Perícia Forense Digital

Prof.ª Crishna Irion
Prof.ª Fernanda Rosa da Silva

Indaial – 2021
1ª Edição

Elaboração:
Prof.ª Crishna Irion
Prof.ª Fernanda Rosa da Silva

Revisão, Diagramação e Produção:
Equipe Desenvolvimento de Conteúdos EdTech
Centro Universitário Leonardo da Vinci – UNIASSELVI

Ficha catalográfica elaborada pela equipe Conteúdos EdTech UNIASSELVI

I68p

Irion, Crishna

Perícia forense digital. / Crishna Irion; Fernanda Rosa da Silva. – Indaial: UNIASSELVI, 2021.

205 p.; il.

ISBN 978-65-5663-889-8
SBN Digital 978-65-5663-887-4

1. Prática forense. - Brasil. I. Silva, Fernanda Rosa da. II. Centro Universitário Leonardo da Vinci.

CDD 340

Impresso por:

APRESENTAÇÃO

Olá, acadêmico! Seja bem-vindo ao Livro Didático Perícia Forense Digital. Neste livro, estudaremos os conceitos fundamentais acerca do processo de investigação forense.

Na Unidade 1, abordaremos a necessidade da perícia forense, a organização e a condução do processo por parte do perito, assim como os aspectos legais que envolvem a prática investigatória. Conheceremos, portanto, os conceitos básicos da **análise forense digital**, que compreendem um conjunto de técnicas para coleta, exame de evidências digitais, reconstrução de ataques, identificação de invasores, ameaças e recuperação de dados. Será importante discorrermos, ainda, sobre a **ética**, uma característica fundamental para profissionais de segurança e para peritos que atuam na investigação forense.

Em seguida, na Unidade 2, observaremos os padrões de exame forense, como a segurança dos dados, a qual envolve **técnicas de hash** para a preservação de provas. Também conheceremos a análise de evidências digitais e os equipamentos essenciais utilizados para preservar, coletar e tratar as provas, além dos quesitos técnicos utilizados na produção de provas e laudos, sendo o principal recurso do perito para o esclarecimento de fatos no processo.

Analisaremos, então, os objetos de exame, como mídias e dispositivos de armazenamento, tipos de exame e coleta de evidências digitais, que abrange desde a coleta até a duplicação de provas em mídias. Recursos como tráfego de rede e memória também são recursos computacionais importantes na extração de dados, portanto, estudaremos como eles podem ser utilizados, além das técnicas complementares aplicadas para facilitar o processo de análise.

Por fim, na Unidade 3, conheceremos as práticas de perícia digital aplicadas em diferentes sistemas operacionais e cenários de rede. Além disso, entenderemos como a **coleta de evidências digitais** é uma etapa fundamental, explorando ferramentas e recursos nativos que servem como arma aos peritos digitais.

Desse modo, poderemos assimilar a importância da análise de logs e registros para rastrear o atacante, a quebra de chaves em redes sem fio e a análise de tráfego em sistemas VOIP. Finalizaremos nossos estudos revisando as práticas forenses.

Bons estudos!

Prof.ª Crishna Irion
Prof.ª Fernanda Rosa da Silva

GIO

Você lembra dos UNIs?

Os UNIs eram blocos com informações adicionais – muitas vezes essenciais para o seu entendimento acadêmico como um todo. Agora, **você conhecerá a GIO**, que ajudará você a entender melhor o que são essas informações adicionais e por que poderá se beneficiar ao fazer a leitura dessas informações durante o estudo do livro. Ela trará informações adicionais e outras fontes de conhecimento que complementam o assunto estudado em questão.

Na Educação a Distância, o livro impresso, entregue a todos os acadêmicos desde 2005, é o material-base da disciplina. A partir de 2021, além de nossos livros estarem com um novo visual – com um formato mais prático, que cabe na bolsa e facilita a leitura –, prepare-se para uma jornada também digital, em que você pode acompanhar os recursos adicionais disponibilizados através dos QR Codes ao longo deste livro. O conteúdo continua na íntegra, mas a estrutura interna foi aperfeiçoada com uma nova diagramação no texto, aproveitando ao máximo o espaço da página – o que também contribui para diminuir a extração de árvores para produção de folhas de papel, por exemplo. Assim, a UNIASSELVI, preocupando-se com o impacto de ações sobre o meio ambiente, apresenta também este livro no formato digital. Portanto, acadêmico, agora você tem a possibilidade de estudar com versatilidade nas telas do celular, tablet ou computador.

Junto à chegada da **GIO**, preparamos também um novo layout. Diante disso, você verá frequentemente o novo visual adquirido. Todos esses ajustes foram pensados a partir de relatos que recebemos nas pesquisas institucionais sobre os materiais impressos, para que você, nossa maior prioridade, possa continuar os seus estudos com um material atualizado e de qualidade.

QR CODE

Olá, acadêmico! Para melhorar a qualidade dos materiais ofertados a você – e dinamizar, ainda mais, os seus estudos –, a UNIASSELVI disponibiliza materiais que possuem o código QR Code, um código que permite que você acesse um conteúdo interativo relacionado ao tema que está estudando. Para utilizar essa ferramenta, acesse as lojas de aplicativos e baixe um leitor de QR Code. Depois, é só aproveitar essa facilidade para aprimorar os seus estudos.

ENADE

Acadêmico, você sabe o que é o ENADE? O Enade é um dos meios avaliativos dos cursos superiores no sistema federal de educação superior. Todos os estudantes estão habilitados a participar do ENADE (ingressantes e concluintes das áreas e cursos a serem avaliados). Diante disso, preparamos um conteúdo simples e objetivo para complementar a sua compreensão acerca do ENADE. Confira, acessando o QR Code a seguir. Boa leitura!

LEMBRETE

Olá, acadêmico! Iniciamos agora mais uma disciplina e com ela um novo conhecimento.

Com o objetivo de enriquecer seu conhecimento, construímos, além do livro que está em suas mãos, uma rica trilha de aprendizagem, por meio dela você terá contato com o vídeo da disciplina, o objeto de aprendizagem, materiais complementares, entre outros, todos pensados e construídos na intenção de auxiliar seu crescimento.

Acesse o QR Code, que levará ao AVA, e veja as novidades que preparamos para seu estudo.

Conte conosco, estaremos juntos nesta caminhada!

SUMÁRIO

INTRODUÇÃO À COMPUTAÇÃO FORENSE

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- conhecer a necessidade da perícia forense;
- conceituar os principais elementos da análise forense computacional;
- compreender a importância dos aspectos legais da computação forense, como o perito, os cenários e a prática forense;
- analisar as características básicas e o processo que envolve o uso de evidências digitais;
- diferenciar os tipos de perícia e a análise dos quesitos técnicos na perícia forense;
- descrever os conceitos de ética e legislação aplicados à computação forense.

PLANO DE ESTUDOS

A cada tópico desta unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – A NECESSIDADE DA PERÍCIA FORENSE
TÓPICO 2 – ANÁLISE FORENSE COMPUTACIONAL
TÓPICO 3 – ASPECTOS LEGAIS NA COMPUTAÇÃO FORENSE
TÓPICO 4 – EVIDÊNCIAS DIGITAIS
TÓPICO 5 – TIPOS DE PERÍCIA E QUESITOS
TÓPÍCO 6 – ÉTICA E LEGISLAÇÃO APLICADA À COMPUTAÇÃO FORENSE

CHAMADA

Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

CONFIRA A TRILHA DA UNIDADE 1!

Acesse o
QR Code abaixo:

A NECESSIDADE DA PERÍCIA FORENSE

1 INTRODUÇÃO

Acadêmico, no Tópico 1, a respeito da **necessidade** da perícia forense, notaremos que com a transformação digital e a expansão do uso de redes de internet, os recursos tecnológicos estão cada vez mais inseridos no nosso cotidiano e em diversos segmentos do negócio, por isso a investigação forense se torna cada vez mais necessária.

Com o advento de **plataformas** e **aplicações** que trazem inúmeras possibilidades para o tratamento de informações, não somente os dispositivos estão cada vez mais conectados, as práticas ilícitas e aquelas conduzidas por criminosos digitais também crescem cada vez mais.

Para compreendermos todos os recursos, componentes e técnicas que compõem o processo de investigação forense, precisamos entender como surgiu a necessidade da perícia forense e a sua importância. Vamos lá?

2 A NECESSIDADE DA PERÍCIA FORENSE

Com o passar do tempo, pessoas com os mais diversos objetivos passaram a usar a rede mundial de computadores, a qual conhecemos como internet, se familiarizando, assim, cada vez mais com a tecnologia, principalmente como o uso dos dispositivos móveis e outros que permitem a automação de tarefas em vários setores do mercado. Atualmente, as tarefas cotidianas estão diretamente ligadas com a forma pela qual a tecnologia é aplicada, como a realização de compras on-line (em supermercados, farmácias e grandes redes varejistas). Além disso, grande parte das transações financeiras passa pela internet.

Sendo assim, ao apontarmos a **inteligência** dos dispositivos e a **vulnerabilidade** de sistemas computacionais, podemos afirmar que ambas são frequentemente utilizadas em favor de práticas ilícitas. Eleutério e Machado (2011) apontam que a **principal necessidade** da computação forense é determinar a **dinâmica**, a **importância** e a **autoria** de atividades ilegais relacionadas à tecnologia da informação.

Quanto mais a tecnologia alavanca, crescem também as práticas de espionagens, fraudes bancárias, invasões de computadores e diversos outros casos que podem estar relacionados com os **crimes virtuais**. Em consequência disso, a necessidade de rastrear fraudes e identificar usuários que as cometem, assim como a indispensabilidade de coletar evidências e validar provas, torna-se cada vez mais recorrente.

A **computação forense** é um dos ramos (áreas) da **ciência da computação**. Trata-se do processamento de evidências digitais, como materiais e dispositivos, compondo o segmento da ciência da computação responsável pela **análise de dados eletrônicos** e **investigação de incidentes computacionais**. Isso faz com que a perícia forense precise ser aplicada de forma clara:

- quem;
- quando;
- onde;
- como o ato criminoso foi executado.

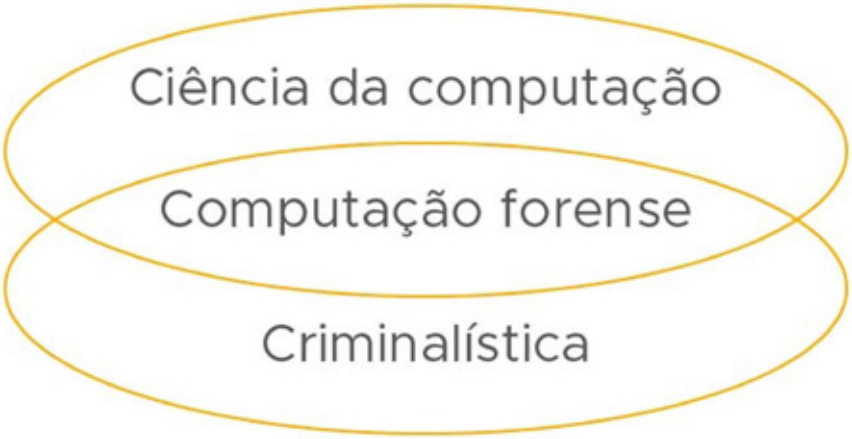
A importância dessa área cresce sob a influência, principalmente, da preocupação de formar profissionais capacitados e representar a relevância da área.

ESTUDOS FUTUROS

Ainda nesta Unidade analisaremos a importância do papel do especialista em computação forense, também conhecido como **perito forense computacional.**

Comparada a outros ramos da **segurança da informação** e áreas correlatas, na imagem a seguir podemos notar de que modo a computação forense vem se encaixando:

FIGURA 1 – ÁREAS DA CIÊNCIA DA COMPUTAÇAO RELACIONADAS À SEGURANÇA DA INFORMAÇÃO



FONTE: Adaptada de Silva (2019)

Podemos definir cada uma dessas áreas da seguinte forma:

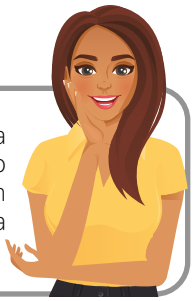
- **Ciência da computação**: ciência que estuda qualquer técnica, metodologia, aplicação ou instrumento que faça parte da transformação tecnológica. O objetivo da ciência da computação é desenvolver soluções e processamento de dados por meio do uso de computadores, algoritmos e telecomunicação.
- **Computação forense**: ramo da ciência da computação caracterizado principalmente pelos métodos aplicados na busca de evidências digitais e criminais, as quais ficam armazenadas em computadores e/ou mídias.
- **Criminalística**: conjunto de procedimentos que compõem as práticas aplicadas pela justiça moderna, com o intuito de averiguar qualquer delito, crime ou circunstância de diversas origens, considerando vestígios de crime, meios e métodos utilizados por cada um deles.

O surgimento da perícia forense deve-se também à necessidade de obtenção de provas sobre a ocorrência de determinadas situações, podendo ter valor probatório em investigações e procedimentos de qualquer campo judicial: civil, criminal, comercial, trabalhista, entre outros.

Sem o **conhecimento técnico** para usar em processos nos quais a tecnologia é a principal ferramenta utilizada para cometer um crime ou infração, juízes e advogados necessitam de um profissional da área técnica para comprovar os fatos. Segundo Franco (2016), a **informática forense** está relacionada com a **criminologia** porque extrai informações de qualquer evidência para tirar **conclusões técnicas** sobre um crime específico.

ATENÇÃO

Uma grande variedade de dispositivos disponíveis no mercado tornou a vida mais fácil, mas inevitavelmente acabou se tornando uma brecha para a execução de crimes. Esse fato decorre da facilidade do anonimato e da simplicidade em ocultar evidências, tornando o processo de omissão de qualquer prova ainda mais realizável.



Contudo, o uso do computador ou dispositivo vai além disso, isto é, no cenário do crime pode ser um agente facilitador, um atacante ou uma vítima. Em resumo, vejamos algumas das razões que tornam o conhecimento digital importante:

- intrusão de computador;
- criação de comunidades virtuais para defender o uso de drogas;
- introdução de vírus em sistemas computacionais por meio de ferramentas corporativas, como e-mail;
- promoção de crimes antigos, como pornografia infantil, corrupção e engenharia social, em que o usuário pode ser enganado, provendo informações privilegiadas sem ao menos perceber.
- O crime cibernético pode assumir várias formas e acontecer a qualquer hora e em qualquer lugar. Os **cibercriminosos** usam métodos diferentes, conforme suas habilidades e objetivos. Considerando os diferentes tipos, podemos definir o crime cibernético com precisão utilizando ferramentas como computadores, redes ou dispositivos de hardware.

De acordo com Silva (2019), o termo **crime digital** engloba toda e qualquer infração originada de computadores, estejam eles conectados ou não a uma rede local ou internet, ou seja, o uso de um meio virtual apropriado já caracteriza tal feito. Todavia, nem sempre é possível afirmar a verdadeira intenção de quem praticou o crime e se realmente houve intenção de causar qualquer dano ao bem, informação ou a um terceiro, e para isso a computação forense permeia sob tal esfera criminal.

Assim, para distinguir se a invasão foi executada por meio de um ataque, como no caso de DDoS (em que comandos podem ser direcionados por meio de "computadores zumbis", o que torna a análise ainda mais complexa), surgiu a necessidade não somente da perícia forense, mas também da atuação de profissionais especializados, além de equipamentos e sistemas desenvolvidos para o uso da computação forense e até mesmo da apresentação de testemunhas (usuários comuns).

O *Código de Processo Civil* versa que "as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz" (BRASIL, 2015, Art. 339).

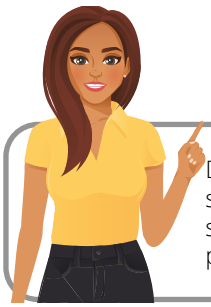
ATENÇÃO

Ainda que a investigação tenha como informação a origem do crime cometido (IP do computador e localização), a identidade do cibercriminoso é uma informação mais complexa de ser desvendada, pois qualquer pessoa com acesso a determinado dispositivo pode cometer um crime digital e despistar os profissionais responsáveis pela rede. Portanto, acaba sendo necessário realizar a perícia para averiguar registros, logs e recursos de forma aprofundada.

A ação dos criminosos ainda pode ser facilitada pelo anonimato promovido pela internet, como já mencionamos, fazendo com que o receio de agir contra a vítima fique cada vez menor, já que a **punição** se apresenta mais incerta. Um bom exemplo desse caso envolve a criação (e abuso) de perfis falsos em redes sociais em algumas práticas, como engenharia social e outros mecanismos empregados por quem pretende se aproveitar de qualquer pessoa conectada à internet sem devida proteção.

Segundo essas definições, o crime cibernético pode apresentar uma ampla variedade de ataques. Por isso, é importante conhecermos os diferentes tipos de crime, já que cada um deles exige práticas de segurança diferentes. A demanda pela perícia digital forense e por profissionais especializados é imprescindível para investigar quem, como e quando o crime cibernético ocorreu.

Podemos observar, então, que o profissional com conhecimento em **perícia forense** e aplicação da mesma em **investigação** e **produção de laudos** (os quais podem provar a autoria e materialidade de um delito eletrônico), tem sido cada vez mais procurado. Isso significa que reconstruir o passado, constatar a materialidade e apurar a autoria de incidentes cometidos com o requinte dos bits é uma necessidade no mundo atual.



ATENÇÃO

Devemos considerar que a cada dia os criminosos cometem seus delitos sem deixar vestígios, por isso é necessário reconstituir fatos em laboratórios, seguindo as normas e os padrões estabelecidos e, portanto, importantes para o julgamento (FRANCO, 2016).

A computação forense se tornou um evento importante na **identificação** de pistas virtuais que descrevem o autor de ações ilícitas, a fim de suprir as necessidades das instituições legais, no que se refere à manipulação de evidências eletrônicas.

Diante disso, a investigação forense é indispensável para a comprovação de um crime, ou seja, de um processo que envolve uma série de análises de equipamentos computacionais e eletrônicos. Hoje em dia, a perícia digital faz parte do cotidiano de advogados, policiais, juízes e de outros profissionais que atuam em conjunto com a lei, principalmente na condução de processos e aplicação de punições por meio do tribunal de justiça.

Na transformação digital, tornou-se comum encontrar um ou mais computadores na cena do crime, os quais, geralmente, são os principais recursos utilizados para o armazenamento e processo de informações (ferramentas importantes para qualquer segmento do negócio). A necessidade da perícia, então, requer definição de **leis**, **processos**, **regras**, **métodos** e **profissionais** que possam investigar e inspecionar os respectivos equipamentos, a fim de determinar, com base nas informações encontradas, o que é considerado ou não um crime de informática.

Agora que compreendemos a importância da perícia forense, estudaremos como a análise é realizada e quais são as ferramentas e etapas que a caracterizam.

RESUMO DO TÓPICO 1

Neste tópico, você aprendeu:

- A área de segurança abrange diversos segmentos de aplicação.
- A tecnologia requer atenção para a preservação de dados.
- Os crimes cibernéticos são uma ameaça para a organização.
- As informações devem estar devidamente protegidas na internet.
- Os profissionais de informática são tão importantes quanto os de direito.

AUTOATIVIDADE

1 A perícia forense nasceu da necessidade de controlar atos ilícitos originados por usuários mal-intencionados e atacantes que utilizam internet, redes e dispositivos para praticar atividades prejudiciais às informações gerenciadas por meio digital. Sobre os principais motivos que tornam a perícia forense uma ferramenta útil, assinale a alternativa CORRETA:

a) ( ) Para resolver problemas e incidentes resultantes de intrusão em computadores e dispositivos digitais.
b) ( ) Reforçar a importância da criação de comunidades virtuais a fim de incentivar práticas clandestinas.
c) ( ) Descobrir práticas e identidade de quem realizou qualquer intrusão de vírus ou malware.
d) ( ) Identificar vulnerabilidades do sistema, as quais resultaram em danos ou vazamento de informações.

2 A ciência da computação é uma área extensa, de modo que possui diversos ramos, como análise de sistemas, redes de computadores, sistemas de informação, entre outros. Dessa forma, emergiram também subáreas, como a computação forense, relacionadas aos segmentos que não fazem parte das tecnologias que visam atender às novas necessidades de preservação de dados. Com base nas definições e considerando a computação forense, a ciência da computação e criminalística, analise as sentenças a seguir:

I- As evidências e os métodos aplicados em diversos cenários para comprovar um crime são definidos pela ciência da computação.
II- A computação forense trata do processamento de dados em computadores e dispositivos móveis, com o objetivo de aprimorar o desempenho de tarefas cotidianas com o uso da tecnologia.
III- A criminalística trata de crimes como roubos e assassinatos, e a maneira como a investigação é conduzida deu origem à forma como a computação forense é aplicada aos crimes digitais.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença III está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Diversas abordagens geraram a necessidade de aprimorar a prática forense, além da adaptação de leis e regras para investigar crimes digitais. Considerando que as pessoas se tornam cada vez mais vulneráveis ao utilizar recursos computacionais, leia as sentenças abaixo e classifique V para as verdadeiras e F para as falsas:

( ) Para se expor a qualquer risco, tanto o computador quanto a pessoa precisam, necessariamente, de conexão à internet, pois somente assim os acessos indevidos acontecem.
( ) Mesmo sem conhecimento técnico necessário, um atacante pode ter informações privilegiadas e cometer crimes digitais, aproveitando-se do conhecimento da vítima.
( ) Assim como fraudes bancárias, com o objetivo de coletar informações com fins lucrativos, as redes sociais também sofrem crimes digitais, o que ocorre a partir de perfis falsos.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) F – V – V.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 Sabemos que a computação pode facilitar os processos, mas sofre com diversos métodos de ataque desenvolvidos para prejudicar, acessar e roubar informações em diferentes meios digitais, sendo hoje um dos principais recursos utilizados para o processamento de dados, resultado da tecnologia moderna. Disserte sobre a relação entre a ciência da computação, a computação forense e a criminalística, justificando a relação entre elas.

5 Algumas informações sobre computadores utilizados para cometer crimes digitais, como a identificação do equipamento, podem ser facilmente encontradas na rede em que a prática ocorreu. Contudo, a identificação de quem praticou o ataque, muitas vezes é uma tarefa difícil, o que demanda a perícia forense. Disserte sobre o assunto.

ANÁLISE FORENSE COMPUTACIONAL

1 INTRODUÇÃO

A análise forense digital consiste em utilizar ferramentas e técnicas para recuperar, preservar e analisar dados armazenados ou transmitidos em formato binário, ou seja, contidos em qualquer dispositivo computacional, sendo capaz de interpretar informações criadas digitalmente

Desse modo, no Tópico 2, conheceremos as principais atividades que caracterizam a análise forense digital, ou seja, as peculiaridades do processo e como um ambiente periciado deve ser tratado, considerando os diversos tipos de fraudes eletrônicas aplicados atualmente.

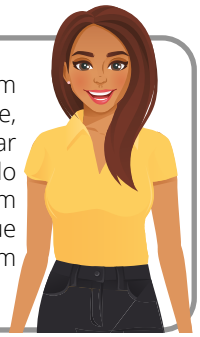
Compreenderemos, então, como a necessidade da perícia forense fez a análise forense computacional evoluir junto a recursos utilizados pelos peritos digitais, visando a execução de suas tarefas. Está preparado? Vamos lá!

2 ANÁLISE FORENSE COMPUTACIONAL

A **análise forense** é a principal atividade que compõe a **perícia forense**. Nessa etapa, o perito executa suas atividades com base em perguntas-chave. Adaptadas ao ambiente periciado, todas elas fazem parte da **análise de segurança** de determinado sistema computacional, devendo considerar que o perito seja capaz de aplicar seu conhecimento, estando apto para defender argumentos importantes no processo.

INTERESSANTE

Considere a seguinte situação hipotética: uma fraude foi conduzida a um sistema de banco, de modo que informações privilegiadas vazaram e, consequentemente, os clientes tiveram prejuízos milionários. Para desvendar o crime, alguns fatores imprescindíveis devem ser analisados: a versão do sistema operacional utilizado; os últimos usuários que logaram ou realizaram tentativas recentes de acesso ao computador ou rede alvo; os arquivos que foram acessados pelo suspeito; se existem portas lógicas abertas que possam ter originado o crime; se algum arquivo ou diretório foi excluído.



Se o crime digital ocorre em um ambiente virtual, em que há interação entre pessoas reais, é comum que seja considerado um crime como qualquer outro. E para todos os tipos de crime, parte-se da premissa que, com vestígios a serem analisados, o exame pericial é obrigatório. No *Código de Processo Penal* (BRASIL, 1941, Art. 158) está explicitado que "quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado".

Na investigação forense de **crimes computacionais**, na maioria dos casos, o primeiro passo é a busca e apreensão dos equipamentos ou a vistoria no local ou rede da organização. Respectivamente, as ações envolvem a **emissão de um mandato** ou a presença de um **oficial de justiça** para acompanhar a análise realizada pelo profissional nomeado.

Quando o mandato é expedido, o perito fica liberado para realizar a **identificação** do local do crime, além de iniciar a **seleção** de todo e qualquer equipamento que possa servir como prova e deva ser apreendido, como discos, servidores, pen drives e até mesmo documentos impressos ou copiados por meio de dispositivos de imagem. Durante todo o procedimento de investigação forense, o manuseio das informações deve seguir leis, normas e padrões estabelecidos, a fim de garantir que a análise forense seja realizada corretamente.

2.1 TIPOS DE SISTEMAS ANALISADOS

Após a **coleta de vestígios** (possíveis provas), inicia-se o **processo de análise**, isto é, etapa em que é possível identificar se o objeto realmente tem algum vínculo com o evento ocorrido e se encaixa com o objetivo da perícia ou com o crime cometido. De acordo com Velho (2016), os sistemas analisados pela perícia forense podem ser classificados da seguinte maneira:

FIGURA 2 – SISTEMAS DA ANÁLISE FORENSE

FONTE: Adaptada de Velho (2016)

Vamos, agora, analisar as características de cada um deles, segundo o mesmo autor:

- **Sistemas integrados**: têm como função realizar uma tarefa específica, sendo que sua estrutura é composta por hardware e software. Podemos citar, como exemplo, um terminal para monitoramento de um ambiente, controlado por um programa instalado e baseado em sistema operacional, cuja função é realizada por meio de periféricos e conexão com interface de rede. Sistemas integrados têm características semelhantes às de um computador comum, de modo que são projetados para tarefas próprias. Outro exemplo comum é o televisor (Smart TV) projetado com inteligência computacional.
- **Sistemas embutidos**: caracterizam-se por um dispositivo computacional incorporado como parte integrante de outro sistema de controle, fragmento essencial para possibilitar operações lógicas, embora sejam utilizados, em sua maioria, recursos de processamento e armazenamento reduzidos, além de pouca capacidade ligada a componentes internos, como memória. A existência desses sistemas, geralmente passa despercebida, mas estão presentes em máquinas industriais, equipamentos médicos, eletrodomésticos e até mesmo em veículos.
- **Sistemas embarcados**: Velho (2016) aponta os sistemas embarcados como uma subcategoria de sistemas embutidos, em que sua utilização está diretamente ligada aos veículos por meio de sistemas desenvolvidos, com interfaces de controle web, conexões de redes e podem ser criados com um custo não tão elevado. Além disso, não representam alto índice de manutenção, recuperando-se de falhas até mesmo de forma automática.

Agora que conhecemos a classificação dos sistemas que demandam análise forense, cabe destacar que a **coleta de vestígios cibernéticos** deve ser realizada com **extrema cautela**, pois a maioria das informações é crítica, frágil e/ou privada, principalmente em **sistemas embarcados**. Já para os sistemas embutidos, existe um empecilho por parte da liberação de informações, além da dificuldade na liberação de dados por parte dos fabricantes, o que acarreta problemas e torna o processo de análise lento, estendendo a perícia forense além do esperado. Ademais, existe a questão **operacional**, fazendo com que os dispositivos sejam praticamente únicos em sua arquitetura, e não existem muitas ferramentas de análise voltadas especialmente para as suas características, limitando, portanto, as possibilidades.

INTERESSANTE

Existem fontes de consulta que podem facilitar o processo de análise forense, como a Biblioteca Nacional de Referência do Software (RDS), em que estão disponíveis assinaturas digitais de arquivos conhecidos e rastreáveis, podendo ser utilizados em busca de sua origem (VELHO, 2016).

Outro fator que dificulta a análise forense diz respeito aos **sistemas criptografados**, afinal, como o atacante precisa de um bom conhecimento para se infiltrar em sistemas e coletar informações privadas, também pode adicionar recursos criptográficos para dificultar a mitigação de provas, o que pode levar tempo para ser desvendado, antes mesmo que se possa ter acesso às informações de fato.

Compreendo a infinidade de dispositivos e sistemas que podem estar envolvidos no local do crime, fica evidente que a análise pode ser a fase mais demorada de todas as que compõem a investigação, de modo que é preciso ter tempo e realizar testes com aplicação de diversas técnicas, até que o resultado esperado possa ser alcançado.

IMPORTANTE

Existem casos em que o processo de análise forense se torna impossível, gerando um resultado inconclusivo por parte do perito em decorrência do prazo ou da falta de recursos para analisar devidamente todos os artefatos suspeitos.

Na etapa final, o perito deve redigir o **laudo pericial**, comprovando todas as observações e apresentando provas e evidências a serem utilizadas no processo judicial. O laudo deve conter, então, todos os detalhes para auxiliar o Judiciário na análise do crime. Para tanto, o documento deve ser compreensível e conter as principais atividades que foram executadas na análise forense.

FIGURA 3 – ETAPAS DA ANÁLISE FORENSE

FONTE: A autora

Seguir à risca todas as etapas garante que não ocorram imprevistos no final da perícia, portanto, a análise deve estar completa para responder todos os **quesitos** do processo.

ESTUDOS FUTUROS

Não se preocupe! Ainda nesta Unidade estudaremos a respeito dos quesitos.

Nitidamente, a análise forense precisa ser adaptada de acordo com o ambiente periciado, trata-se, afinal, de uma etapa da computação forense que requer diversos componentes, habilidades e muita atenção por parte dos envolvidos, visando utilizar as provas de maneira adequada, sem que sejam recusadas devido ao manuseio ou tratamento incorreto. Além disso, o processo de análise forense envolve uma série de **aspectos legais**, os quais iremos analisar adiante.

RESUMO DO TÓPICO 2

Neste tópico, você aprendeu:

- Os sistemas possuem características próprias que devem ser analisadas na perícia forense.
- As etapas devem ser executadas em ordem cronológica, a fim de obter sucesso na perícia.
- Nem sempre a análise é possível, pois depende do cenário e da complexidade dos fatos.
- Sistemas, equipamentos e pessoas envolvidas são fatores importantes na análise forense.
- O crime digital deve ser tratado como qualquer outro crime.

AUTOATIVIDADE

1 Os sistemas estruturam a funcionalidade dos equipamentos computacionais, sendo responsáveis por executar logicamente as funções para as quais os equipamentos foram projetados. Sabemos, portanto, que existem diferentes sistemas, e entre os principais estão os sistemas embutidos. Sobre os sistemas embutidos, assinale a alternativa CORRETA:

a) ( ) São utilizados em dispositivos que apresentam características semelhantes às dos computadores, podendo utilizar rede, periféricos e até mesmo sistemas operacionais.
b) ( ) São sistemas projetados especificamente para televisores comuns, os transformando em dispositivos inteligentes, ou seja, alvos para ataques.
c) ( ) São sistemas utilizados para controlar ambientes, por isso são alvos comuns quando o objetivo é a invasão de um ambiente de rede.
d) ( ) São todos os sistemas espiões que passam despercebidos aos usuários e servem como ferramenta de apoio para coletar evidências no processo de análise forense.

2 A análise forense é composta por diversas etapas, permitindo ao perito e aos profissionais envolvidos uma coleta organizada de provas, servindo como principal elemento para o processo e o local do crime analisado. Com base nas definições de cada uma delas, analise as sentenças a seguir:

I- O levantamento envolve qualquer atividade que o perito execute para unir as provas necessárias, comprovando os fatos levantados sobre determinada situação.
II- O laudo técnico é a documentação final, em que o perito documenta tudo o que foi visto, descrevendo a verdade dos fatos e os vestígios encontrados.
III- A coleta ocorre somente quando as informações são extraídas de sistemas operacionais, sem que os equipamentos sejam recolhidos da cena do crime.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Quando falamos de dados importantes para o processo de análise forense, principalmente em softwares, sistemas e aplicações, algumas informações devem ser coletadas como base principal de investigação. De acordo com a influência desses fatores, analise as sentenças a seguir e classifique V para as verdadeiras e F para as falsas:

( ) Alguns detalhes são importantes, como a versão do sistema operacional e a identidade dos usuários que logaram ou realizaram tentativas de acesso no sistema.
( ) Arquivos que foram acessados não são importantes para a análise forense, desde que não tenham sido modificados ou executados por usuários externos.
( ) O risco de manter as portas lógicas é mínimo, porque crimes de informática geralmente não exploram as vulnerabilidades do sistema.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) V – F – V.
c) ( ) V – F – F.
d) ( ) F – F – V.

4 A análise forense é importante para evidenciar provas, desvendar crimes digitais e padronizar os processos que envolvem a computação forense, como o combate de crimes na internet. Disserte sobre a importância de documentar todos os fatores obtidos no processo de análise.

5 Existem muitas maneiras de analisar um local de crime, mas para que isso seja possível, é necessário obter uma autorização por parte do juiz, garantindo que todas as práticas sejam executadas dentro da lei. Considerando tais aspectos, descreva qual documentação autoriza o perito a realizar a análise forense.

ASPECTOS LEGAIS DA COMPUTAÇÃO FORENSE

1 INTRODUÇÃO

Acadêmico, no Tópico 3, analisaremos os aspectos legais que envolvem todas as etapas da estrutura do processo de análise forense, incluindo aquisição, preservação, recuperação e análise de dados mantidos ou armazenados por sistemas computacionais.

É importante lembrar que a perícia forense surgiu com o objetivo de suprir as necessidades referentes à manipulação de evidências eletrônicas, entretanto existem leis a serem consideradas antes mesmo de qualquer ação judicial e de verificação a ser tomada.

Sendo assim, regras, normas e obrigações fazem parte do papel do perito digital, o qual deve cumprir suas obrigações de acordo com o que é definido pela legislação. Vamos conhecer esses aspectos!

2 ASPECTOS LEGAIS DA COMPUTAÇÃO FORENSE

Quando um crime precisa ser **detectado** e **analisado**, algumas habilidades técnicas são importantes para determinar a forma como a **máquina suspeita** pode ser considerada um alvo de ataques cibernético. Para tanto, a visão de um usuário comum não é suficiente para coletar os vestígios e produzir provas capazes de desvendar um mistério computacional, principalmente quando a situação envolve um ambiente de alta complexidade.

NOTA

A lei descreve os **crimes informáticos** como **comportamento intrusivo**, prática que envolve o uso de equipamentos conectados a uma rede de computadores ou não, a fim de obter benefícios ilegais por meio da violação indevida de mecanismos de segurança (SANTOS; MIRANDA, 2019).

Para observar o sistema como um detetive que examina a cena de um crime, a visão de **programadores** e **especialistas** é muito importante, sobretudo quando consideramos que erros e rastros minimamente esquecidos por um atacante precisam ser analisados de forma aprofundada, mas os aspectos legais e o uso de informações privadas precisam ser atendidos.

Seja pela análise de um código-fonte ou aplicando corretamente o raciocínio lógico, o entendimento das relações de causa e efeito capazes de gerar panes e problemas de funcionalidade em sistemas computacionais, entre outras consequências, as tarefas sempre devem ser executadas com total legalidade sobre os métodos e práticas da perícia forense.

Contudo, uma perícia em um computador suspeito de invasão (ou mesmo um computador apreendido em alguma batida policial) não envolve apenas uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para análise, mas também a **preservação da privacidade** da vítima, já que a intenção é investigar o atacante e a prática, e não pesquisar informações pessoais do usuário que está geralmente sob proteção da lei. Na maioria dos casos, o equipamento analisado tem a função de servidor, armazenando serviços importantes, como e-mails ou arquivos. Deve-se, portanto, tomar uma série de cuidados, a fim de evitar a invasão da privacidade dos usuários do sistema.

O ideal é que se defina um **escopo** antes mesmo de iniciar a investigação, restringindo ao máximo a área de **atuação da análise**, evitando violar a privacidade e vazamento de informações de forma desnecessária. Para desviar de problemas como esses, as políticas de segurança de conhecimento de todos os usuários envolvidos, podem ser aplicadas.

3 CENÁRIOS DE PERÍCIA EM INFORMÁTICA

Depois de analisarmos a importância da perícia forense e os aspectos legais que envolvem os crimes ocorridos na internet, conheceremos alguns dos **principais cenários** que envolvem a **aplicação da perícia em informática**. Faremos esse estudo acompanhando alguns exemplos de casos comuns, em que se julga necessário realizar a **análise pericial** e a **atuação do perito** como profissional especializado no ramo de tecnologia.

3.1 JOGOS

Pode parecer que o motivo não esteja relacionado a um cenário de perícia em informática, mas com o avanço da tecnologia junto a cenários em que os usuários passam a utilizar ainda mais os computadores para lazer (como na pandemia de COVID-19), um grande público acaba sendo inserido no contexto dos jogos on-line.

Além dos aspectos citados, muitos usuários também jogam profissionalmente, de modo que existem crimes voltados para roubo de jogadores. Nesse caso, o hacker pode, por exemplo, roubar moedas, burlar as regras do fabricante ou até mesmo prejudicar outros jogadores, o que resulta em usuários banidos. Porém, em casos mais críticos, a situação pode gerar um processo contra quem praticou tais atividades ou a favor de um usuário banido indevidamente. Fica a cargo do perito analisar se o que aconteceu, está de acordo e coletar informações necessárias para comprovar a verdade.

3.2 LICENCIAMENTO

Muitas empresas utilizam software não licenciado, alteram as características das licenças de uso com o uso de crackers (simulando uma chave de ativação falsa como verdadeira), usam licenças expiradas ou replicam em um número excessivo de computadores. Essa prática é ilegal e frequentemente analisada em casos de perícia forense.

3.3 COMPRA DE EQUIPAMENTOS

Nesse caso, um consumidor adquire um equipamento que apresenta problemas durante a garantia, mas a loja ou o fabricante nega a substituição dentro do prazo legal. Tal situação pode causar grande transtorno e dar origem a um processo, em que o perito precisará analisar se o problema relatado realmente existe. Essa análise é feita com base nos **quesitos** levantados para verificar a integridade ou não do equipamento em questão.

3.4 USO INADEQUADO DE COMUNICAÇÃO

Ocorre quando o remetente de um e-mail encaminha uma mensagem inapropriada, ferindo os direitos de outras pessoas. Essa mensagem pode ser utilizada como prova e gerar um processo por **danos morais**. No entanto, é responsabilidade do perito averiguar se o e-mail realmente saiu da caixa do remetente, se sofreu alteração antes de ser reenviado e quais são as informações que realmente estavam contidas na mensagem.

3.5 FALSIFICAÇÃO IDEOLÓGICA

Com o crescimento das *Fintechs*, os bancos sofrem diversas fraudes, assim como seus usuários. Ficou mais fácil abrir uma conta digital no nome de outra pessoa e utilizar serviços como cartão de crédito, limite especial e cheques sem sair de casa. Nesse caso, uma análise no dispositivo, na conta e na documentação emitida precisa ser feita pelo perito especializado, que deve identificar como o caso ocorreu.

ATENÇÃO

Devemos observar o quanto os cenários mencionados se diferem entre si, por isso é necessário que o perito forense tenha um amplo conhecimento da área.

A seguir, analisaremos as características atribuídas ao perito forense para que ele atue forma adequada e satisfatória em processos, causas e investigações de cenários suspeitos.

4 O PERITO DA COMPUTAÇÃO FORENSE

Inicialmente, ao estudarmos sobre a perícia forense, podemos perceber que o **procedimento forense computacional**, para alcançar o sucesso no resultado, deve envolver diversos profissionais, como: juízes, advogados, delegados, promotores e demais profissionais da área de direito, além de profissionais da área de TI, como os auditores de sistemas. Apesar disso, focaremos em compreender o ofício do profissional perito forense ou digital, assim como seu papel junto com a atuação de todos os demais profissionais.

Embora a profissão de perito forense ainda se apresente como uma novidade para muitas pessoas que ingressam no mercado de trabalho, principalmente na área de TI (tecnologia da informação), a função desse profissional é de extrema importância devido à necessidade de combate aos **crimes eletrônicos**.

Como os profissionais da área podem ser chamados em diversos locais, eles precisam prestar diferentes serviços na área de TI, envolvendo:

- redes de computadores;
- segurança da informação;
- análise de sistemas.

As atividades envolvem habilidades como o manuseio de equipamentos de informática, mas também deve haver disposição para seguir regras e medidas, visando a qualidade e credibilidade de seu trabalho. Para tanto, é necessário ser eficiente em vistorias, confecção de laudos, perícias técnicas e audiências judiciais que demandam relatórios técnicos, por exemplo.

O perito forense é o responsável por **selecionar** e **preservar** as evidências, além de coordenar a equipe para realizar tais atividades. Também pode realizar exames forenses no local de crime, devido à sensibilidade e volatilidade dos materiais e dispositivos.

Com relação ao trabalho executado pelo **perito digital**, podemos citar técnicas, conhecimentos e práticas executadas para manusear os dados com responsabilidade e dentro dos limites da lei, por meio da análise de informações que de alguma forma foram ocultadas pela capacidade de tecnologias computacionais, com o objetivo de vincular dados originários de ações, como chamadas, mensagens e compartilhamento de informações que podem ter sido utilizadas de forma indevida, provando tal crime digital (SANTOS; MIRANDA, 2019).

ATENÇÃO

O perito precisa sempre ter em mente o objetivo da investigação, por exemplo:em casos de suspeita de manipulação de arquivos, o foco está em apreender dispositivos de armazenamento computacional. Já em casos de falsificação de documentos, equipamentos como scanners, impressoras e máquinas fotográficas também devem ser apreendidos.

Por ser o profissional responsável por analisar ambientes digitais (sistemas, hardware, software e mídias), a fim de detectar fraudes e levantar evidências que possam servir como provas de possíveis crimes, as pistas virtuais devem ser utilizadas para que o perito possa **descrever o autor** das ações ilícitas.

IMPORTANTE

Devemos observar o quanto os cenários mencionados se diferem entre si, por isso é necessário que o perito forense tenha um amplo conhecimento da área.

Algumas precauções também devem ser tomadas durante a coleta, o transporte e armazenamento de informações e evidências. A **perícia digital forense** é um campo dedicado à **varredura de ameaças e ataques** que podem comprometer os meios eletrônicos. Cabe ressaltar que o perito atual, com a intenção de encontrar evidências de crimes digitais e virtuais, tem sua profissão reconhecida desde a publicação da Lei n° 12.737 (BRASIL, 2012).

Compete ao perito analisar como os recursos podem ter sido utilizados para obter, adulterar ou destruir dados ou informações sem autorização expressa. De modo geral, além de comprovar o conhecimento na área profissional, os especialistas digitais também precisam ter formação acadêmica em **tecnologia da computação**. Adicionalmente, certificação técnica comprovando suas habilidades no campo é essencial para a prática de perícia forense (SANTOS; MIRANDA, 2019).

Levando em consideração que as cenas de crime podem ter múltiplas características, esses profissionais possuem uma ampla gama de habilidades, são denominados peritos justamente pelo alto nível de conhecimento em computação e realização de investigações acerca da natureza tecnológica. Nesse contexto, vejamos algumas características essenciais desses profissionais:

- estar familiarizado com as ferramentas técnicas, estratégias e métodos de ataques conhecidos, incluindo aqueles que não foram relatados, mas são considerados como potencial ameaça ou vulnerabilidade conhecida para determinado sistema;
- desenvolver habilidade em encontrar traços sutis de comportamento malicioso, com foco na perfeição e nos detalhes. Sempre existem rastros, por mais sutis que sejam;
- compreender as causas e consequências de tudo o que acontece no sistema para construir um histórico lógico formado por comportamentos maliciosos, causas e ações executadas no cenário;
- compreender a legislação envolvida na prática executada e de que forma foram afetados os favores que envolvem a privacidade, confidencialidade e restrições ao âmbito da ação ou jurisdição;
- manusear evidências legais com cuidado, além de examinar a trajetória do evento de qualquer complexidade, indo além do nível de experiência do invasor.

Além disso, alguns conhecimentos técnicos são imprescindíveis, tais como:

- **Linguagens de programação**: desenvolver habilidades para revisar e analisar códigos-fonte maliciosos.
- **Competência para identificar malware**: vulnerabilidades em redes, dispositivos e computadores.
- **Conhecimento na depuração**: analisar a segurança, além da aplicação de práticas que possam solucionar ou identificar restrições de segurança da informação.
- **Revisão de logs**: identificar atividades maliciosas e inconformidades na rede, isso envolve verificar a integridade de sistemas, redes que utilizam tecnologias sem fio e LAN (rede local), assim como qualquer recurso que possa ser utilizado para explorar a vulnerabilidade de um sistema.
- **Verificação de serviços**: analisar acessos à internet, correio eletrônico e servidores que possam ter influenciado com a injeção de ameaças, como vírus e trojans.

- **Análise de força de senha**: os usuários representam o elo mais fraco da rede, por isso é necessário avaliar a força das senhas utilizadas, identificando se foi a causa do que está sendo analisado no cenário.
- **Gerenciamento de sistemas operacionais**: gerenciar os sistemas operacionais, como Linux, Windows e até mesmo sistemas de dispositivos móveis, incluindo Android e iOS, identificando vulnerabilidades nativas.
- **Sistemas de telefonia**: revisar os sistemas de telefonia e aplicar sistemas e barreiras de segurança na rede, como firewalls e ACL (Access Control List, ou seja, lista de controle de acessos).
- **Conhecimento e entendimento em direito digital**: reconhecer as características de funcionamento de sistemas de arquivos, programas de computador e padrões de comunicação em redes de computadores em relação às leis de proteção ao usuário e crimes na internet.

Precisamos lembrar que, além de obedecer ao princípio básico de mínima interferência no ambiente, o profissional dessa área deve respeitar as **normas** no que diz respeito à **legitimidade** e **licitude** da prova. Dessa forma, é possível evitar que uma prova possa ser negada em juízo e servir, de fato, para solucionar um crime.

É de suma importância que o perito tenha uma excelente **postura comportamental**, além de ser **imparcial** em relação às análises realizadas. Por ser um profissional ético, não deve ter antecedentes que possam levantar qualquer suspeita a seu respeito. Caráter e ética profissional são características chaves.

ATENÇÃO

De acordo com Reis *et al*. (2001), em casos de perícia criminal, o profissional responsável é o **perito oficial**, pois o seu trabalho serve para todas as partes interessadas (polícia, justiça, ministério público, advogados, entre outros). Nesse caso, é indispensável ter graduação completa, e em seguida, é necessário prestar concurso público para cumprir tal função.

Na Lei n° 3.689 (BRASIL, 1941, Art. 477), está definido que outro requisito para prosseguir com a **intimação** do perito, para comparecer em juízo e prestar esclarecimentos, é a preexistência do **laudo pericial** já anexo ou em processo. Caso haja necessidade de esclarecimentos, as partes solicitarão ao juiz a participação de peritos ou assistentes técnicos nas audiências de instrução e de julgamento, elaborando perguntas.

Em outras palavras, o perito forense computacional **identifica** e **processa evidências** em provas materiais de crimes. Assim, contribui para determinar a materialidade, a dinâmica e a autoria de vestígios ilícitos digitais que possam contribuir para a decisão final da perícia e investigação forense.

5 PERÍCIA FORENSE COMPUTACIONAL

No Brasil, não existem normas específicas que regem a forense computacional, mas existem **normas gerais** que abrangem a perícia (ditadas no *Código de Processo Penal*), e que devem ser adotadas no âmbito computacional, salvo exceções que não se adequem a área de atuação do perito (REIS *et al.*, 2001).

O perito deve seguir corretamente as normas contidas no *Código de Processo Penal*, visto que sua nomeação é responsabilidade da justiça, e nessa função, ele precisa atuar como um profissional ético, protegido pela lei. Entre as normas, podemos destacar duas que dizem respeito à abordagem computacional na perícia forense (REIS *et al*., 2001):

- **Art. 170**: para perícias que envolvem provas em forma de ilustração, prints ou fotografias, o perito deverá armazenar o material necessário para uma nova perícia (se necessário), mantendo recursos adicionados aos laudos técnicos. Além disso, cópias de ambientes, máquinas virtuais e sistemas operacionais devem ser mantidas para futuras atividades de laboratório, quando for realizada a investigação, sem que a prova original seja alterada indevidamente.
- **Art. 171**: quando qualquer mídia, dispositivo ou equipamento for danificado, corrompido ou se torne inutilizável, o perito deve ser capaz de apontar quais ferramentas foram utilizadas para tais práticas.

Além de descrever as ferramentas que possivelmente foram utilizadas para cometer a prática ilegal, o perito precisa documentar quais as ferramentas de software foram usadas por ele para fazer a análise, bem como a possível identificação de uma **linha de tempo**, descrevendo como o processo foi executado. Todos esses detalhes garantem que **o valor judicial** de uma prova digital válida, enquanto não há uma padronização metodológica de análise forense.

Existem também **políticas internas de segurança**, as quais são adotadas, principalmente, por organizações privadas, a fim de garantir a privacidade dos seus dados. Sendo assim, o primeiro passo, ao identificar um ato de uma intrusão na rede ou qualquer atividade suspeita, é realizar o contato imediatamente com a organização ou setor de suporte, relatando quaisquer incidentes de segurança, para que as medidas legais cabíveis sejam tomadas.

6 TERMINOLOGIA NA COMPUTAÇÃO FORENSE

Assim como em todas as áreas, sejam elas tecnológicas ou não, a perícia forense adota alguns termos para facilitar o entendimento de todos os componentes, dispositivos e ferramentas de análise dos meios (e crimes) digitais. De acordo com Sampaio (2011), os principais termos são:

- **Provas digitais**: qualquer informação que esteja armazenada ou tenha sido transmitida no formato binário, servindo como prova de um crime digital.
- **Mídias de provas**: objetos em que as provas digitais são encontradas e servem como evidência para que o perito possa analisar a origem dos dados.
- **Duplicação pericial**: ato em que o perito duplica o cenário, sistema ou mídia para um ambiente seguro, de modo que ele possa explorar sem causar qualquer dano ao ambiente original, mantendo um conteúdo idêntico, em que os testes serão submetidos
- **Imagem pericial**: imagem gerada a partir de mídias de provas.
- **Mídia de destino**: mídia para onde as provas são replicadas, podem ser um dispositivo móvel, disco rígido, máquina virtual ou outro dispositivo.
- **Imagem restaurada**: restauração dos dados ou sistema para a sua forma original, excluindo ou desfazendo qualquer alteração.
- **Análise on-line**: coleta de dados realizada em um computador funcional.
- **Análise off-line**: coleta de dados em mídia duplicada, com menor risco de alterar a prova original do crime.

ESTUDOS FUTUROS

Alguns desses termos já foram abordados nos tópicos anteriores, por isso ao se deparar com a definição, já conseguimos relacionar como esses recursos são utilizados na prática. Quanto aos ainda não mencionados, ainda aparecerão no decorrer da disciplina. Além disso, a seguir, iremos aprofundar nosso conhecimento sobre **evidências digitais**. Por enquanto, teste seus conhecimentos na autoatividade que preparamos!

RESUMO DO TÓPICO 3

Neste tópico, você aprendeu:

- O perito representa um papel importante nas decisões judiais ligadas à perícia forense.

- É necessário ter conhecimento técnico profundo, inclusive sobre a inovação tecnológica.

- O perito é um profissional ético que precisa ter conhecimento em questões legais em relação ao tratamento de informações.

- Todo cuidado é pouco durante a manipulação de informações mantidas em sistemas computacionais.

- Termos técnicos facilitam o entendimento acerca da funcionalidade de cada componente pericial.

AUTOATIVIDADE

1 Com base nos diversos cenários analisados pelo perito forense, o profissional precisa estar atento ao seu objetivo em relação às provas e evidências, para definir adequadamente os equipamentos a serem analisados. Em casos de investigação de falsificação de documentos, assinale a alternativa CORRETA:

a) ( ) É preciso analisar alguns equipamentos utilizados, como scanners, impressoras, copiadoras e seus respectivos logs.
b) ( ) É preciso avaliar apenas dispositivos como computadores e notebooks, os quais necessitam de autenticação de usuários internos.
c) ( ) É preciso identificar os sistemas de telefonia VoIP instalados e telefones móveis, utilizados, geralmente, para esse fim.
d) ( ) É preciso avaliar toda a documentação física, assim como os documentos armazenados em servidores e *storages,* ou seja, criados em formato digital.

2 A respeito das aptidões de um perito forense, precisamos considerar que seu perfil deve ser composto tanto por habilidades técnicas como por conhecimento sobre o processo de perícia, além dos direitos que englobam a utilização de dados na internet. Com base nas definições sobre o perito na computação forense, analise as sentenças a seguir:

I- Um perito precisa ter conhecimento em linguagens de programação para analisar possíveis informações maliciosas embutidas no código-fonte.
II- Um perito deve ter competência para identificar vulnerabilidades em redes, dispositivos e computadores como vírus e malwares.
III- Um perito deve ter conhecimento na depuração que envolve análise de segurança, mas não precisa solucionar qualquer restrição de segurança da informação, pois essa é uma responsabilidade do analista de segurança.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 A ética é uma característica essencial para o perito digital, uma vez que ele deve agir de acordo com a lei, com as regras e com os objetivos propostos pelos autos do processo por meio da investigação forense. Considerando os princípios e as funções do perito forense, analise as sentenças e classifique V para as verdadeiras e F para as falsas:

( ) Faz parte das habilidades ligadas à legislação, analisar o comportamento malicioso de uma aplicação ou sistema operacional, e para isso basta o conhecimento judicial.
( ) O perito precisa entender de que forma a legislação está envolvida com os princípios de privacidade, confidencialidade e integridade das informações.
( ) Manusear evidências legais, independente da complexidade do sistema investigado e do que precisa ser evidenciado no processo, deve ser uma preocupação do perito.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) F – V – V.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 O perito, para atuar na computação com ênfase em investigação forense, precisa comprovar seu conhecimento sobre a coleta de informações e análise de crimes. Explique como tal comprovação deve ser feita.

5 Embora as tecnologias e os dispositivos eletrônicos caracterizem os pontos mais importantes a serem analisados pelo perito, os usuários também podem ser ponto fraco para o sistema, gerando vulnerabilidades a serem exploradas pelo atacante por meio de práticas não padronizadas, ou seja, seriam brechas que facilitam as infrações e crimes na internet. No contexto da perícia forense, disserte sobre as preocupações acerca das senhas fracas utilizadas na rede.

EVIDÊNCIAS DIGITAIS

1 INTRODUÇÃO

Acadêmico, no Tópico 4, conheceremos os conceitos básicos que envolvem as evidências digitais, assim poderemos compreender a importância de coletar e documentar as provas de maneira adequada, sendo um processo decisivo para o sucesso da perícia forense.

Devemos considerar que o perito digital precisa defender sua visão sobre os fatos, de modo que e é por meio das evidências digitais que qualquer informação relevante pode comprovar o que foi analisado no cenário do crime, seja essa informação armazenada ou transmitida por meio digital.

Sabendo disso, analisaremos a relevância das **evidências digitais** e as **características** dos locais em que os crimes de informática mais comuns são executados.

2 CONCEITOS DE EVIDÊNCIAS DIGITAIS

Uma **evidência digital** é definida como **qualquer dado armazenado**, **processado** ou **transmitido** por meio de um dispositivo digital ou eletrônico, podendo ser utilizado como informação de apoio ou refutação em relação a um incidente a ser comprovado por um álibi ou comprovação (CASEY, 2011).

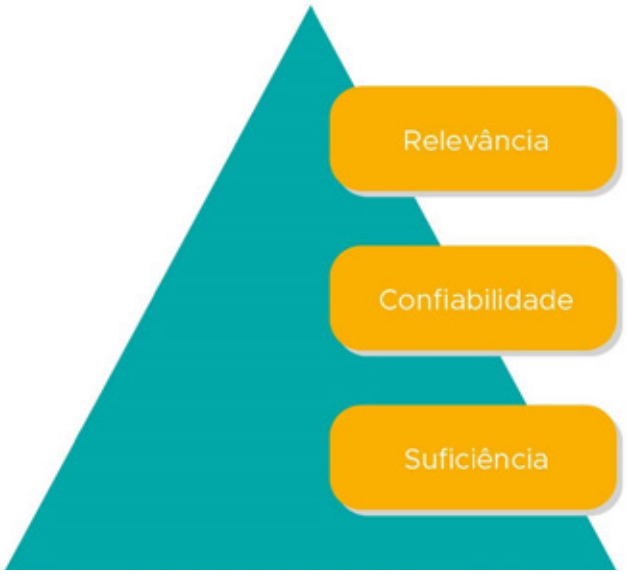
Nesse contexto, os dados são, essencialmente, uma **combinação de informações** de tipos diferentes: texto, imagens, áudios e vídeos recuperados de várias fontes e denominados, em conjunto, de **evidência digital**. Os sistemas computacionais em que as evidências podem ser coletadas, de acordo com Henseler (2000), costumam ser categorizados nos seguintes grupos:

- **Sistema de computador aberto**: um sistema de discos rígidos, teclados e monitores, como laptops, desktops e servidores, em conformidade com o padrão. Esses sistemas se tornaram indispensáveis à medida que o espaço de armazenamento continua aumentando. Arquivos simples podem conter informações criminais e atributos relevantes para as investigações.
- **Sistema de comunicação**: corresponde aos sistemas tradicionais de telefonia, sistemas de telecomunicações sem fio, internet e redes gerais. Para acessar esse tipo de informação, pode ser necessário verificar os arquivos de log de servidores intermediários e roteadores que processam mensagens específicas.

- **Sistemas integrados**: são dispositivos móveis, cartões inteligentes e outros sistemas com computadores integrados. Eles podem conter comunicações, fotos, vídeos e outros dados pessoais, assim como os sistemas de navegação podem ser usados para determinar o caminho do veículo.

Além disso, toda evidência digital é formada por **três pilares** fundamentais, conforme podemos observar:

FIGURA 4 – PILARES FUNDAMENTAIS DE UMA EVIDÊNCA DIGITAL



FONTE: A autora

Desse modo, caracterizaremos cada um dos pilares considerando os fundamentos sobre evidências apresentados pela Associação Brasileira de Normas Técnicas (2013):

- **Relevância**: recomenda-se a comprovação da importância do material obtido para a investigação, ou seja, se contém dados relevantes que auxiliam na investigação de um evento específico e se apresenta um bom motivo para ser obtido.
- **Confiabilidade**: recomenda-se que todos os processos usados para processar a evidência digital sejam auditáveis e repetíveis. Espera-se que os resultados da aplicação desses procedimentos sejam reproduzíveis.
- **Adequação**: é recomendado considerar que os materiais suficientes foram coletados para conduzir uma investigação apropriada. Espera-se que as partes envolvidas sejam capazes de passar por auditorias e certificações, a fim de indicar quantos materiais são considerados e quais procedimentos são utilizados para determinar a quantidade e as características dos materiais obtidos.

Nesse contexto, os peritos devem seguir procedimentos documentados para garantir que as evidências sejam **íntegras** e **confiáveis**, além disso, devem ser consideradas tanto as diretrizes de tratamento quanto as fontes, os rastros e as evidências que estejam de acordo com os princípios fundamentais para minimizar a manipulação nos dispositivos originais.

ATENÇÃO

Todas as ações e alterações, à medida que forem acontecendo em cumprimento com a legislação local sobre as evidências, devem ser documentadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

A análise forense dos equipamentos de armazenamento precisa ser minunciosamente examinada pelos peritos digitais, buscando informações relevantes para o caso e cenário suspeito.

Algumas etapas podem facilitar tal análise de dispositivos de armazenamento, desde que sejam consideradas da seguinte forma:

FIGURA 5 – ETAPAS DA PRESERVAÇÃO DE EVIDÊNCIAS

FONTE: Araújo (2020, p. 23)

O comprometimento das provas pode resultar da coleta de informações, dados ou provas realizadas de maneira incorreta, causando o fracasso da perícia, por isso é importante que as etapas sejam seguidas como passos essenciais de uma investigação forense (VELHO, 2016).

A fase de **preservação** tem como papel fundamental evitar que qualquer alteração seja realizada no ambiente, prova ou dispositivo, por isso o perito deve ser capaz de criar um ambiente fidedigno, em que possa explorar as vulnerabilidades sem qualquer risco ou ameaça.

Na **extração de dados**, o exame da mídia ou rede deve ser realizado, mas apenas informações pertinentes serão copiadas ou replicadas para iniciar a análise de evidências. Ao iniciar a análise, o **principal objetivo** é **reconhecer informações** e **recuperar dados** que foram de alguma forma deletados pelo atacante para despistar o perito e entender qual a importância dos dados para desvendar o crime.

Por último, na fase de **apresentação**, podemos considerar que as evidências, devidamente identificadas, são formalmente adicionadas como conclusivas ao exame realizado pelo perito, tendo esse o principal propósito de **elaborar o laudo técnico**, prova importante nos autos do processo.

Quando o perito se torna responsável por produzir evidências técnicas sobre o caso a ser analisado, o primeiro passo é analisar a documentação recebida, em que todas as características, tanto do cenário quanto das práticas e dos envolvidos estão descritas. De acordo com Araújo (2020), nessa documentação estão as informações que representam a mídia, sistema ou informação digital para que o perito possa utilizá-las como um direcionamento na identificação das características de tal cenário.

IMPORTANTE

Quando a análise é realizada, por exemplo, em uma aplicação, na qual o fabricante acusa o réu de utilizar licenciamento de forma indevida, o perito já possui conhecimento sobre qual software (parte lógica ou programa) precisa analisar, e para tornar as provas legítimas, deve incluir no laudo informações como versão, atualização, computador e data de expiração do software, além de fotografar qualquer evidência que permita ao fabricante analisar se a chave utilizada é ou não falsa. Outra prática importante é fotografar os equipamentos, o local, o número de série e qualquer outro elemento capaz de provar que o ambiente periciado realmente não está em conformidade com a lei e extensão dos fatos.

Com essas informações, precisamos considerar as evidências lógicas e também físicas, como análise de equipamentos, devendo comprovar o estado de conservação. Em alguns casos, as perícias servem para comprovar a **funcionalidade** de um equipamento, para isso deve-se analisar as características físicas, como amassamentos, riscos, marcas de má utilização e ausência de componentes.

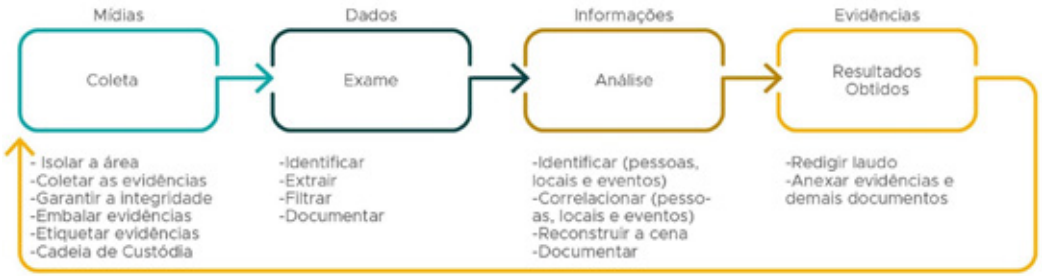
NOTA

Em alguns casos, o perito precisa comprovar a funcionalidade de um dispositivo, por exemplo. Isso envolve verificar se a falha está relacionada com o mau uso do equipamento. Imaginemos que um usuário comprou um equipamento com problemas de carregamento e o fabricante nega a troca em garantia de fábrica. Sendo assim, o perito precisa comprovar a causa e as condições de uso, por exemplo: se o usuário fez a utilização correta do dispositivo; analisar o tempo de vida de bateria; verificar as aplicações utilizadas no equipamento; analisar se há existência de vírus; e verificar o comportamento de testes de hardware (parte física de um equipamento computacional) do fabricante.

Todos os aspectos mencionados são fundamentais para comprovar a origem do problema relatado. E para entendermos a importância das evidências digitais, podemos compará-las com os vestígios encontrados nas cenas de crime, os quais não podem ser alterados quando existe a necessidade de identificar o criminoso.

Os autores Lopes, Gabriel e Bareta (2006) afirmam que a **fase de preservação** também integra o processo de cadeia de custódia, ou seja, é um processo realizado para manter e documentar a história (cronologicamente), visando garantir a confiabilidade e o rastreamento das evidências. O processo tem também outros objetivos, como garantir a **integridade** dos equipamentos e dos dados coletados. A cadeia de custódia pode ser vista da seguinte maneira:

FIGURA 6 – PROCESSOS QUE ENVOLVEM A CADEIA DE CUSTÓDIA



FONTE: Adaptada de Lopes, Gabriel e Bareta (2006)

Evidentemente o processo de produção, coleta e análise de evidências é bastante metódico, de modo que o principal objetivo do perito é apresentar resultados com base em provas reais, tomando todo o cuidado necessário para preservar as evidências e apresentá-las sem correr qualquer risco de negação decorrente de algum tipo de violação. O laudo mostra a verdade dos fatos e descreve o que foi constatado pelo perito, podendo servir como recurso de prova para o caso e cenário analisado.

3 LOCAIS DE CRIME DE INFORMÁTICA

O local de um crime pode ser descrito como o lugar em que ocorreu (ou supostamente ocorreu) um determinado ataque, situação ou prática digital ilegal. Esse local será auditado pelo perito forense, nele estão grandes possibilidade de localização das evidências, as quais representam grande relevância para que o crime seja desvendado.

NOTA

Para que um local seja explorado com a finalidade de levantamento de provas e análise de qualquer vestígio de crime, é necessário a emissão de um mandato de busca e apreensão. Esse documento representa uma diligência policial, permitindo legalmente que o perito (ou profissional responsável pelo processo de investigação) possa procurar e apreender objetos e dispositivos de interesse judicial.

Três fatores são considerados essenciais para o cenário que pode conter evidências: quem, como e onde. Os fatores compreendem informações sobre quem executou o crime digital, quais ferramentas e ações descrevem o planejamento ou execução do crime e qual é o local de ocorrência. Desse modo, o local envolve todas as provas, componentes, pessoas e dispositivos computacionais relacionados ao delito, e requer do perito forense todos os cuidados necessários para que o processo represente transparência (REIS; GEUS, 2013).

Sobre a prática mais importante a ser executada no local do crime, denominada **apuração dos fatos**, é imprescindível o isolamento do local, a análise da cena, uma documentação minuciosa dos vestígios encontrados e a coleta. Por isso, Reis e Geus (2013) reforçam a respeito da importância de identificar e recolher os equipamentos computacionais, além de compreender a função e o conhecimento de cada usuário presente, ou seja, quem utilizou os dispositivos ou quem tem acesso.

Para manter o foco no local do crime, o **objetivo da investigação** deve ser devidamente determinado. Por exemplo: quando o foco é identificar documentos adulterados ou softwares falsos, é necessário apreender dispositivos de armazenamento computacional; já em casos de falsificação de documentos, são analisados dispositivos que possam ser utilizados para tal fim; e em casos de identificação de uma ligação, existe a possibilidade de analisar dispositivos móveis (como smartphones) ou a infraestrutura VoIP, se for a tecnologia utilizada pela organização.

RESUMO DO TÓPICO 4

Neste tópico, você aprendeu:

- As evidências digitais são provas unidas pelo perito.
- O local em que ocorre o crime de informática não deve ser modificado.
- Todas as etapas são essenciais para provar a veracidade dos dados.
- As evidências precisam ser comprovadas por meio do laudo da coleta de informações.
- Os sistemas de informação são fontes importantes de evidências.

AUTOATIVIDADE

1 Os processos da cadeia de custódia envolvem mídias, dados, informações e evidências, de modo que cada um desses aspectos compreende diferentes abordagens e devem ser tratados até que o resultado seja alcançado. Sobre uma das etapas que faz parte do processo de exame, assinale a alternativa CORRETA:

a) ( ) Isolar a área do crime e coletar as evidências necessárias.
b) ( ) Extrair as informações do sistema e filtrar somente as evidências úteis para o caso analisado.
c) ( ) Identificar pessoas que estejam no local e sirvam como elemento para reconstruir uma cena.
d) ( ) Redigir o laudo, anexando todas as evidências coletadas para que a decisão seja tomada.

2 Para comprovar as causas e condições de uso de um determinado equipamento, é necessário realizar uma análise inicial sobre as características dos dispositivos. Com base nas definições comuns para a perícia forense de um equipamento que não carrega, analise as sentenças a seguir:

I- É importante determinar se o equipamento foi utilizado de maneira correta ou sofreu danos em decorrência de mau uso por parte do usuário, isentando o réu de qualquer relato.
II- O tempo de vida da bateria não é importante, pois é uma característica que não define a sua funcionalidade.
III- O uso de ferramentas que provem o mau funcionamento do dispositivo deve ser aplicado para dar embasamento ao cenário, uma vez que o perito precisa ser imparcial.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Entre as etapas que compreendem o tratamento de evidências, temos a extração de dados como o segundo passo a ser dado. Considerando as atividades que a definem, classifique V para as sentenças verdadeiras e F para as falsas:

( ) As mídias devem ser examinadas, de modo que informações pertinentes serão copiadas ou replicadas para um ambiente seguro, podendo ser analisadas.
( ) É importante reconhecer quais informações e dados são importantes, e até mesmo recupera-los caso tenham sido deletados como parte do crime.
( ) A extração é a prática cometida pelo atacante, pois ele recolhe informações com má intenção e sem a devida autorização.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – F.
b) ( ) V – F – F.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 Assim como o laudo é fundamental para comprovar a atuação do perito, a documentação dos equipamentos analisados é importante para que o perito possa entender as características nativas previstas pelo fabricante, e assim comparar o comportamento atual de recursos computacionais tratados como evidências ativas. Explique a importância da documentação em casos de perícia forense.

5 A relevância está entre os pilares que sustem a maneira como as evidências são tratadas em um cenário de crime digital. Fale sobre suas características.

TÍPOS DE PERÍCIA E QUESITOS

1 INTRODUÇÃO

Os quesitos servem para orientar o perito sobre as informações pertinentes que precisam ser inseridas no processo, isto é, informações relevantes. Desse modo, as partes conseguem analisar os elementos do processo e elaborar uma defesa na condução da causa.

Por isso, no Tópico 5, abordaremos a função e as características dos quesitos, além disso, conheceremos os tipos mais comuns de perícias.

Sobre os quesitos, iremos compreender como essa ferramenta é significativa para o perito, uma vez que ela ajuda a determinar o que precisa ser coletado e como as evidências precisam ser apresentadas.

2 TIPOS DE PERÍCIA E QUESITOS

Para compreendermos como o quesito compõe os laudos periciais e auxilia na decisão de um processo, iremos defini-lo como qualquer questão ou dúvida que possa ser levantada em um processo. Em casos de perícias forenses, dizem respeito aos **sistemas computacionais** e **dispositivos**, portanto, são analisados por alguém para responder perguntas específicas.

De acordo com Avatec (2020), os **quesitos** podem ser caracterizados como inquirições ou **questões essenciais**. Por meio de respostas aos quesitos, o perito digital é capaz de opinar sobre pontos específicos que o ato processual deseja submeter tecnicamente, direcionando tais dúvidas a fim de realizar a **prova pericial**.

IMPORTANTE

Apesar de responder aos quesitos propostos, como forma de organizar e entregar as provas encontradas, o perito forense precisa ser imparcial, ou seja, não pode adicionar opiniões pessoais sobre qualquer recurso analisado. O perito não tem o poder de tomar a decisão e nem mesmo de apoiar qualquer parte envolvida no processo, apresentando apenas provas concretas em seu laudo, de forma neutra, pois essas provas serão utilizadas pelo juiz na análise e decisão final do caso.

Nem sempre o quesito é uma pergunta direta ao perito, pode também ser redigida em formado de sugestão, provocação ou solicitação, como "analisar o número de licenças e versão do sistema utilizado" ou "o cliente recebeu um e-mail que fere sua índole". Nesses casos, o perito precisa utilizar suas habilidades técnicas e buscar provas pertinentes para responder ao quesito mencionado de forma imparcial, apresentando somente a verdade dos fatos.

DICAS

Na totalidade dos casos, de acordo com o Art. 465, §1º, inciso III do *Código de Processo Civil* (redação dada pela Lei nº 13.105), o cumprimento dos quesitos técnicos deve ocorrer dentro do período de quinze dias contados da intimação do despacho de nomeação do perito por parte do juiz, e envolve as seguintes condições (BRASIL, 2015): I - arguir o impedimento ou a suspeição do perito, se for o caso; II - indicar assistente técnico; III - apresentar quesitos.

Para conhecer essa Lei na íntegra, acesse: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.

2.1 TIPOS DE PERÍCIA

Como o nosso foco é conhecer os conceitos acerca da perícia forense, precisamos também estudar outros tipos de perícia, pois assim conseguiremos comparar as características da computação forense com outros tipos de perícias. Iremos, então, analisar alguns deles:

- **Perícia médica**: tem como objetivo a emissão de pensões por invalidez, licença médica ou laudos para liberar o trabalhador em decorrência de qualquer problema de saúde.

- **Perícia ambiental**: atua na área da criminologia ambiental, responsável pela fiscalização e denúncia de crimes envolvendo o meio ambiente.
- **Perícia criminal**: essa área é baseada no ambiente do crime. Os vestígios encontrados são coletados e utilizados como prova, geralmente após serem analisados em laboratório.
- **Perícia em veículos**: atualmente, muitos crimes estão voltados para veículos, incluindo alterações no veículo, sendo necessário analisar sua estrutura e identificar também objetos e bens que podem ser ocultados nos compartimentos internos.

IMPORTANTE

Cabe lembrar que os veículos utilizam sistemas embarcados, então a perícia forense pode ser necessária se o caso estiver relacionado com invasão ou problemas técnicos que envolvam a parte lógica do veículo.

- **Perícia em balística**: responsável por validar evidências de crime envolvendo o uso de armas e a identificação de relíquias culturais. No geral, armas e munições precisam ser inspecionadas mais detalhadamente.

2.2 QUESITOS

Analisaremos, agora, como os quesitos podem ser categorizados de acordo com o tipo, características e objetivos para os quais se aplicam (AVATEC, 2020).

A começar pelos **quesitos preliminares**, eles estão relacionados aos processos abertos e devem ser definidos de maneira **simplificada**. Tais quesitos referem-se às **proposições iniciais**, sendo redigidos e apresentados entre as partes no prazo de quinze dias contados da intimação do despacho, que prevê a nomeação do perito, para que o profissional possa avaliar a solicitação antes mesmo de aceitar o encargo ao qual foi intimado. Essa definição está prevista pelo Art. 465, §1°- III_do *Código de Processo Civil* (BRASIL, 2015).

Em tal circunstância, além dos quesitos levantados pelas partes acusada e acusadora, também são classificados os quesitos apresentados pelo juiz do caso, conforme Art. 473-IV do *Código de Processo Civil* (BRASIL, 2015). Os quesitos preliminares, dessa forma, podem ser definidos como pontos essenciais que, no prazo assinalado pela legislação, foram apresentados pelas partes e/ou pelo julgador da causa e precisam ser minunciosamente analisados.

IMPORTANTE

Ao analisar os quesitos preliminares, o perito pode aceitar ou apresentar escusa ao encargo pericial oferecido. Caso não tenha conhecimento técnico suficiente para embasamento dos quesitos, deve manifestar-se, apresentando justificativa plausível para isentar-se de tal responsabilidade (REIS et al., 2001).

Antes ou após o retorno do perito sobre os quesitos preliminares anexados ao caso, as partes podem complementar os quesitos, isto é, adicionar nova solicitação a respeito de outros quesitos considerados importantes para a conclusão do juiz. São esses denominados **quesitos suplementares**, ou seja, são pontos levantados posteriormente pelas partes e submetidos à apreciação do perito durante as diligências.

INTERESSANTE

O perito não é um profissional exclusivo de qualquer parte do processo, por isso deve responder aos quesitos levantados por ambos. É permitido ao réu nomear um assistente técnico para acompanhar o perito na análise do caso, exame ou perícia quando previamente avisado sobre a ação. Porém, quando a causa corre sob sigilo e envolve a atuação de um oficial de justiça que acompanha o perito ao local, a parte ré toma conhecimento da ação movida apenas na vistoria, para que não haja risco de apagarem as provas. Nesse caso, não apresenta quesitos.

Nem sempre os quesitos direcionados ao profissional pelas partes e pelos advogados estão ligados com a sua área de atuação, nesse caso, pode o perito esquivar-se de responder. Quando os **quesitos são impertinentes**, entende-se por inadequados e podem ser descartados.

Em alguns casos, torna-se necessário levantar outras questões para elucidar os quesitos já apontados. Muitas vezes, ao apresentar os quesitos, as partes acrescentam "e outros quesitos que o perito considere necessário", esses quesitos podem estar embutidos na prova pericial se decisivos para o processo, portanto, são denominados **quesitos de esclarecimento**.

Portanto, a condição para definir os quesitos é simplesmente a necessidade de qualquer esclarecimento de questões relevantes para a perícia forense, para isso devem ser resolvidas no laudo pericial apresentado, mesmo que não sanem todas as dúvidas das questões analisadas.

RESUMO DO TÓPICO 5

Neste tópico, você aprendeu:

- Os quesitos envolvem pontos importantes a serem compreendidos no local do crime.
- Os quesitos são utilizados para direcionar o curso do projeto.
- Por meio do laudo pericial, o perito deve responder aos quesitos.
- A classificação dos quesitos ocorre conforme o momento em que são solicitados.

AUTOATIVIDADE

1 Quando o perito é nomeado e intimado para apresentar seus honorários e avaliar a proposta do encargo a ele oferecido, existem condições prévias que servem como orientação para que ele compreenda qual será sua função. Sobre a maneira como esses quesitos são denominados, assinale a alternativa CORRETA:

a) ( ) Quesitos complementares.
b) ( ) Quesitos preliminares.
c) ( ) Quesitos de esclarecimento.
d) ( ) Quesitos impertinentes.

2 Considerando a simplicidade e nitidez com que os quesitos preliminares são apresentados, estando ou não em forma de questionamento, acabam instigando o perito a buscar evidências que comprove um fato. Com base nas definições de quesitos, analise as sentenças a seguir:

I- Quando recebe os quesitos, o perito também fica ciente do prazo apresentar as respostas em forma de laudo pericial anexo ao processo.
II- O juiz também pode solicitar quesitos preliminares quando achar relevante, sendo imparcial e buscando apenas compreender os fatos.
III- A parte acusadora é responsável por definir os quesitos, enquanto a parte acusada pode apenas consultá-los e definir se aceita ou não o que foi solicitado.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Nem todos os tipos de perícias estão ligados com a perícia forense, mas é importante conhecê-los, entendendo também se utilizam a tecnologia a seu favor. De acordo com os princípios e as normativas, classifique V para as sentenças verdadeiras e F para as falsas:

( ) A perícia em veículos investiga a ocultação de provas, mas pode tornar-se um processo forense caso envolva a funcionalidade dos sistemas embarcados.
( ) A perícia criminal analisa crimes como assassinatos, roubos, entre outros. Faz parte de uma das áreas definidas junto com a computação forense, utilizando como principal recurso a fotografia.
( ) A perícia médica envolve qualquer situação voltada para causas em que são necessários laudos médicos, atestados e licenças, sendo realizada por um profissional de medicina devidamente especializado.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) V – V – V.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 Conforme o processo, os laudos e as evidências são analisados, pode surgir a necessidade de expandir a visão acerca do andamento do processo, analisando, portanto, novas provas e avaliações sobre o que foi coletado. Sendo assim, discorra sobre os quesitos suplementares.

5 Qual é a importância da definição de quesitos preliminares para o perito?

ÉTICA E LEGISLAÇÃO APICADA À COMPUTAÇÃO FORENSE

1 INTRODUÇÃO

No Tópico 6, estudaremos a ética e a legislação aplicadas em computação forense. Como observamos no decorrer dos tópicos anteriores, frequentemente as organizações de todos os portes sofrem tentativas de invasões e ataques cibernéticos, esse tipo de situação prejudica as informações sigilosas que trafegam nas redes de computadores.

Por esse motivo, a computação forense tornou-se uma área importante na solução de problemas e casos de crimes na internet, portanto, devem seguir leis que garantem a preservação das informações, das vítimas e de todos os profissionais envolvidos.

2 ÉTICA E LEGISLAÇÃO APICADA À COMPUTAÇÃO FORENSE

Para compreendermos como são aplicadas as leis em torno da legislação e da defesa de crimes digitais, antes de tudo, devemos considerar a **complexidade do processo**, pois a internet pode ser uma porta para a comunicação sem fronteiras, dando acesso a infinitos conteúdos compartilhados por todo o mundo.

O termo que define essa circunstância é **ciberespaço ou espaço cibernético**, em que diversas redes de computadores estão conectadas, de modo que as pessoas podem se comunicar por meios comuns, o que ocorre com a troca de mensagens, salas de bate-papo, uso de e-mails e outros aplicativos (SANTOS; MIRANDA, 2019).

DICAS

Para garantir os parâmetros de defesa aplicados contra diversos ataques cibernéticos, a lei e os conceitos de ética ganharam reforço com a aprovação do Decreto n° 10.222/2020 (BRASIL, 2020). Para aprofundar o conhecimento sobre esse assunto, acesse o link: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

Por proporcionar múltiplos serviços no mesmo ambiente, em que as informações trafegam de forma livre, os usuários e governos temem pela insegurança das informações. Desse modo, considerando a importância das informações privadas atualmente confiadas à internet, é impossível discorrer sobre os desafios éticos da tecnologia e da computação forense sem citar a LGPD, isto é, a *Lei Geral de Proteção de Dados* (BRASIL, 2018).

ATENÇÃO

A LGPD é a legislação que garante o tratamento adequado dos dados pessoais, evitando que os dados sejam violados. Isso passou a ser aplicado também aos meios digitais quando as informações são tratadas por pessoas jurídicas, tanto de direito público como privado (MOURA, 2020).

Com a intenção de diminuir as ocorrências de perícia forense, ou até mesmo definir regras para que elas sejam executadas quando necessário, a LGPD estabeleceu princípios, direitos e deveres para o uso de dados no Brasil, visando proteger os direitos fundamentais de liberdade e privacidade (BRASIL, 2018).

A disseminação da tecnologia e o crescimento acelerado da internet geraram uma séria de **confrontos éticos**, resultando em muitos conflitos a respeito da maneira como as novas tecnologias são utilizadas, causando graves consequências para a privacidade dos dados. Ao próprio perito forense, são atribuídas diversas funções éticas, garantindo a conformidade dos processos de computação forense. Verifiquemos algumas das funções:

QUADRO 1 – A ÉTICA DO PERITO FORENSE

Atribuições técnicas	Resultado ético
Mitigação de riscos	Explorar as vulnerabilidades e brechas dos sistemas, identificando os impactos causados.
Conformidade com as normas de segurança	Garantir que ferramentas e boas práticas sejam aplicadas adequadamente às evidências coletadas.
Atender aos requisitos previstos na legislação.	Garantir a confiabilidade de qualquer informação que tenha acesso durante a análise forense.
Evitar o vazamento de informações.	Utilizar mídias seguras e garantir a confiabilidade do ambiente onde os testes serão executados.

FONTE: Adaptado de Moura (2020)

Sendo assim, a LGPD promoveu algumas mudanças no gerenciamento e manipulação de dados pessoais, pois garantir a segurança dos dados se tornou a principal preocupação em relação ao uso da tecnologia e importância do compartilhamento de informações em plataformas digitais. Assim, após a publicação da referida lei, diversas exigências foram relacionadas com a legalidade e ética no uso da tecnologia.

Além da LGPD, existem outros decretos pensados para garantir a ética no que diz respeito à computação forense. O Decreto n° 10.222/2020, por exemplo, descreve dez ações que precisam ser implementadas para a computação forense (BRASIL, 2020). Podemos analisar tais ações na imagem a seguir:

FIGURA 7 – AÇÕES ÉTICAS PARA COMPUTAÇÃO FORENSE

FONTE: Adaptada de Brasil (2020)

Dessa maneira, a ética e as leis voltadas para o tratamento de dados são mais do que apenas uma "boa prática", tornaram-se fundamentais para manter a reputação das organizações, dos usuários e punir de forma adequada os que infringirem as leis, ferindo os direitos do próximo por meio do uso de ferramentas tecnológicas e de comunicação. Nesse ponto, não consideramos somente o armazenamento de dados, mas também o uso inadequado de informações derivadas de sistemas internos e de terceiros, o vazamento e qualquer ação ilícita que não se justifique com ética em relação às funcionalidades dos sistemas computacionais.

LEITURA COMPLEMENTAR

CIÊNCIAS FORENSES: PRINCÍPIOS ÉTICOS E VIESES

Franciéllen de Barros
Barbara Kuhnen
Mônica da Costa Serra
Clemente Maia da Silva Fernandes

Introdução

As ciências forenses são compostas por todos os conhecimentos científicos e técnicas utilizados para apurar crimes e assuntos legais diversos (cíveis, penais ou administrativos). Esse campo tem a função de estudar e interpretar os vestígios que caracterizam as infrações para esclarecer os atos delituosos e colaborar com as autoridades responsáveis pela aplicação da lei. Nas investigações criminais, a principal tarefa do perito forense é confirmar a autoria do delito ou excluir o envolvimento do(s) suspeito(s) – evitando a condenação injusta de inocentes – por meio de métodos que permitem determinar com relativa precisão, por exemplo, se uma pessoa estava na cena do crime.

Segundo Silva e Rosa (2013), o principal papel desta ciência é auxiliar as investigações relativas às justiças civil e criminal, empregando métodos científicos para averiguar danos, mortes e crimes inexplicados. A partir do estudo das evidências colhidas no âmbito da investigação, as ciências forenses ajudam a identificar suspeitos e a elucidar determinado crime, criando hipóteses sobre o ocorrido. Têm, portanto, o objetivo principal de pesquisar nos vestígios do fato criminoso os elementos necessários para formalizar o exame de corpo de delito, produzindo a prova para instruir o processo penal.

Nos primórdios da estruturação do campo, as práticas forenses eram desempenhadas por profissionais de formação genérica. Porém, com a evolução tecnológica, certos crimes tornaram-se mais complexos, tornando necessária a participação de profissionais especializados em outras áreas da ciência, com o intuito de realizar investigações policiais mais eficazes 6. Dessa forma, muitas áreas – como antropologia, criminologia, entomologia, odontologia, toxicologia, engenharia, patologia, psicologia e medicina, entre outras – passaram a compor e auxiliar as ciências forenses, consideradas como campo interdisciplinar. Sua área de atuação é, portanto, bastante abrangente, buscando servir à Justiça e à sociedade.

A interdisciplinaridade do campo engendra diversas metodologias para a execução dos exames periciais. Assim como o juiz lança mão de vários elementos para aplicar a lei, os peritos utilizam os conhecimentos das diversas áreas da ciência para analisar os vestígios encontrados na cena de um crime.

Diferentemente de outras disciplinas científicas, o Direito é ferramenta usual no campo forense. Apesar disso, a ciência e o Direito obtêm informações e resultados de maneiras diferentes. Durante a investigação, uma hipótese é proposta e experimentos são realizados para testá-la; se os dados encontrados não a contrapõem, ela ganha suporte, fundamentando-se e sendo aceita como razoável e confiável. Porém, o perito trabalha com certas limitações da própria ciência, pois mesmo com os avanços tecnológicos nem sempre as conclusões são precisas, o que pode levar as descobertas a serem questionadas. O Direito opera de forma contraditória, atuando às vezes sem exigir quaisquer dados de apoio para fundamentar dúvidas trazidas por advogado de defesa. Em outros momentos, há casos em que a acusação pode não validar a admissibilidade do método proposto pela defesa. Contudo, os métodos das ciências forenses têm sido validados e testados continuamente na arena científica.

Assim como todas as atividades profissionais, as ciências forenses são regidas por princípios e práticas éticas que visam delinear os deveres e as responsabilidades de cada trabalhador para agregar qualidade não somente à área técnica, mas também humana do ofício. Os peritos que não seguem princípios éticos violam as normas deontológicas, independentemente do campo em que atuam.

Com isso, este trabalho objetiva analisar aspectos éticos e deontológicos da atuação profissional em ciências forenses. Para fundamentar esta reflexão foi realizado levantamento em três bases de dados – PubMed, Web of Science e Embase –, utilizando os descritores "ciências forenses", "ética", "vieses", "deontologia", "princípios éticos", "bioética", "ética profissional" e "perito". Foram selecionados artigos em inglês ou português que discutissem dilemas éticos e vieses nas ciências forenses, assim como capítulos de livros que abordassem o tema.

Ética e ciências forenses

Segundo Dinkar (2005), Frabkena descreveu a ética como filosofia da moralidade ou pensamento filosófico sobre moral, problemas morais e julgamento moral. Contudo, ética, em sentido restrito, é diferente de moral. A ética se baseia em conhecimento e pensamento; moralidade se baseia em crença e sentimento.

A ética estipula o comportamento correto do indivíduo, permitindo ao ser humano discernir o certo do errado, e a transgressão de regras ou normas vigentes na sociedade resulta em atitudes pouco éticas. O comportamento de cada pessoa é modulado desde o nascimento pelos pais, mas influências externas presentes no cotidiano interferem nesse comportamento e na própria personalidade.

Durante a vida, as pessoas são limitadas tanto por regras particulares quanto profissionais, sendo a prática trabalhista regida por normas deontológicas. O profissional que emite resultado falso trai a confiança pública, prejudica outros profissionais e coloca a justiça em risco. Uma das maneiras mais eficazes de se proteger de violações éticas é estar atento aos caminhos que levam ao erro.

O perito deve ser imparcial ao transmitir informações à Justiça, pois a sociedade, as vítimas e os suspeitos têm direitos relacionados aos deveres deste profissional. Para a sociedade, o principal dever do perito se baseia na confiança nele depositada. Para a acusação, a vítima e o suspeito, esse profissional é responsável pelo resultado correto da investigação, que deve ser conduzida de maneira eficiente e eficaz. Muitas vezes, a acusação pode depender completamente do relatório apurado pelo perito.

Portanto, o sistema judicial deve poder contar inteiramente com o trabalho dos especialistas, pois são encarregados de estabelecer parâmetros úteis para identificar a autoria do crime ou isentar o suspeito da responsabilidade penal. Neste sentido, além da obediência à legislação pertinente, entende-se que a atuação dos peritos deve se pautar na observância de normas deontológicas e princípios éticos.

Prática ética e o perito

Nas ciências forenses existem muitas áreas que atuam separadamente, mas que se unem no final para fornecer resultados precisos e, assim, confirmar a autoria do crime ou descartar o envolvimento do(s) suspeito(s). Para que seu trabalho tenha autoridade, o perito deve ter experiência em sua área, mas para se tornar especialista é necessário que tenha conhecimento amplo e aprofundado, sendo desta forma competente para formular seu relatório final.

Magistrados confiam em peritos. Os tribunais costumam aceitar sem contestação laudos periciais, sobretudo devido à dificuldade que leigos em temas técnicos têm para questionar as informações fornecidas. Assim, é primordial que as evidências apresentadas pelos peritos sejam confiáveis, precisas e o mais livre de vieses possível.

A complexidade da análise e interpretação de dados forenses é tema bastante debatido. Preocupações sobre a admissibilidade de evidências e depoimentos de especialistas foram amplamente expressas em relação às taxas de validação e erro em métodos usados nas investigações. Segundo Hiss, Freund e Kahana, quando um perito é chamado a fornecer opinião especializada sobre assunto fora do escopo de sua área profissional, espera-se que seja honesto o suficiente para recusar seus serviços. Os autores revisaram a competência de peritos-testemunhas em diversos casos forenses e encontraram incongruências e discrepâncias nos resultados das análises clínicas e forenses nas áreas analisadas.

Para Dinkar (2005), o problema ético mais significante no campo forense, identificado em pesquisa feita com advogados e peritos associados à Academia Americana de Ciências Forenses, é a competência. Neste contexto, o autor sugere dois requisitos éticos: emprego de métodos confiáveis e relatório restrito à área de atuação do perito, redigido com honestidade quanto à sua qualificação ou experiência.

O perito deve apresentar comportamento eticamente correto ao testemunhar sobre assunto específico, não podendo avultar suas qualificações ou experiência. Não é ético – tampouco legal – dar falsas declarações sobre sua carreira, e assumir a responsabilidade de analisar uma investigação sem possuir experiência para isso contraria os valores éticos das ciências forenses. Não sendo qualificado para determinado assunto, o perito não deve apresentar sua opinião científica.

Este tipo de profissional cotidianamente se depara com criminalidade, violência e morte. Devido à urgência e complexidade das atividades desenvolvidas nesta seara, Walterscheid acredita que questões políticas, o elevado nível de estresse e vieses pessoais podem dar margem para imprudência. Com isso, o autor entende que o cientista forense deve possuir habilidades e conhecimento técnico, educação e treinamento adequados. Nesses casos, a ética apresenta padrões de conduta sustentados por justiça e coerência.

Na mesma linha, Murdock e Holmes entendem que os profissionais que atuam em ciências forenses devem ser objetivos, demostrando como chegam às conclusões apresentadas em seus laudos. Neste sentido, treinamento e adesão ao código de ética profissional são importantes. O profissional ético obtém resultados de forma clara e explícita, sem qualquer viés, não se estendendo além de suas habilidades, competências ou conhecimentos, reconhecendo a importância de realizar investigação minuciosa antes de chegar a uma conclusão. Yadav, por sua vez, lembra que resultados periciais, bem como a opinião de peritos, jamais devem ser falsificados, recortados, adaptados ou de forma alguma modificados para atender a terceiros, seja por questão política, militar, racial, financeira ou outras.

FONTE: Adaptado de <https://www.scielo.br/j/bioet/a/GYNrWJgbtfwQskD5TR7dCGN>. Acesso em: 21 set. 2021.

RESUMO DO TÓPICO 6

Neste tópico, você aprendeu:

- A ética protege os direitos de usuários na era digital.
- Diversas leis foram criadas e adaptadas para o tratamento de crimes cibernéticos.
- É importante que o perito tenha ética, antes mesmo de conhecimento técnico.
- A computação forense envolve práticas homologadas e apoiadas pela legislação do país em que é aplicada.

AUTOATIVIDADE

1 A Lei Geral de Proteção de Dados foi idealizada no Brasil para garantir a privacidade dos dados de terceiros, uma vez que essas informações são processadas em qualquer rede ou trafegadas na internet. Sobre o principal objetivo da LGPD, assinale a alternativa CORRETA:

a) ( ) Aumentar a recorrência de perícia forense para desvendar crimes e aplicar a punição correta a quem praticar ações ilícitas.
b) ( ) Garantir o tratamento adequado dos dados violados quando referentes a qualquer pessoa jurídica ou governo.
c) ( ) Oferecer proteção pessoal apenas para informações de pessoas físicas, sendo responsabilidade do governo preservá-las.
d) ( ) Garantir que o perito forense trate as informações de forma confiável, sem externá-las por meio de dispositivos suspeitos.

2 A ética não deve ser seguida somente por quem utiliza a internet e trata de dados de terceiros, mas sim por todos os profissionais envolvidos nas práticas da computação forense, principalmente pelos peritos responsáveis por manipular evidências. Com base no que define a perícia forense, de acordo com a conformidade da ética e legislação, analise as sentenças a seguir:

I- Identificar os impactos causados deve ser uma prática realizada com atenção aos requisitos previstos na legislação.
II- O uso de mídias não é uma prática aceitável, pois aumenta o risco de vazamento de informações.
III- Em relação à ética, o perito precisa seguir as normas de segurança, com o objetivo de aplicar boas práticas na coleta de evidências.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 O Decreto n° 10.222/2020 descreve dez ações a serem implementadas para que a ética seja devidamente aplicada às informações tratadas digitalmente. Sobre tais ações, classifique V para as sentenças verdadeiras e F para as falsas:

( ) A proteção aplicada devidamente às infraestruturas que tratam de informações críticas, minimizam a necessidade de perícia forense, pois protegerem os dados nos meios digitais.
( ) Nem sempre o incentivo de soluções inovadoras é um caminho promissor, uma vez que as tecnologias atuais abrem brechas para o vazamento de informações.
( ) Ao fortalecer ações de governança cibernética a nível mundial, é possível ter mais controle sobre o uso de informações na internet.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) V – F – V.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 Considerando a importância da computação forense, sabemos que existe um foco em aplicar boas práticas e ferramentas de segurança nas análises, afinal, os maiores alvos são os crimes cometidos na internet. Com base nos seus conhecimentos, explique o conceito de ciberespaço.

5 Com suas palavras, explique como a ética pode ser importante para minimizar problemas tratados atualmente pela computação forense.

REFERÊNCIAS

ARAÚJO, S. **Computação forense**. Curitiba: Contentus, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27037:2013**: tecnologia da informação, técnicas de segurança, diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Acesso em: 21 set. 2021.

AVATEC. **O que são espécies de quesitos periciais**. 2020. Disponível em: https://avatec.com.br/o-que-sao-especies-de-quesitos-periciais. Acesso em: 21 set. 2021.

BRASIL. **Decreto-lei nº 3.689 de 3 de outubro de 1941**. Código processo penal. Brasília, DF: Presidência da República, [1941]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 20 set. 2021.

BRASIL. **Lei nº 12. 737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 set. 2021.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de processo civil. Brasília, DF: Presidência da República, [2015]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 20 set. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 set. 2021.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a estratégia nacional de segurança cibernética. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 21 set. 2021.

CASEY, E. **Digital evidence and computer crime**: forensic science, computers, and the internet. 3. ed. Cambridge: Academic Press, 2011.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense**. São Paulo: Novatec, 2011.

FRANCO, D. P. **A Atuação do perito forense computacional na investigação de crimes**. 2016. Disponível em: https://cryptoid.com.br/banco-de-noticias/atuacao-do-perito-forense-computacional-na-investigacao-de-crimes-ciberneticos/. Acesso em: 20 set. 2021.

HENSELER, J. Computer crime and computer forensics. *In*: SIEGEL, J.; SAUKKO, P. (Org.) **The encyclopedia of forensic science**. Cambridge: Academic Press, 2000.

LOPES, M.; GABRIEL, M. M.; BARETA, G. M. S. **Cadeia de custódia uma abordagem preliminar**. 2006. Disponível em: https://revistas.ufpr.br/academica/article/view/9022/6315 . Acesso em: 21 set. 2021.

MOURA, K. **Ethical hacker**: profissão de segurança da informação. 2020. Disponível em: https://engenharia360.com/ethical-hacker-profissao-seguranca-de-infomacao. Acesso em: 20 set. 2021.

REIS, M. A. *et al*. **Forense computação**: aspectos legais e padronização. 2001. Disponível em: https://lasca.ic.unicamp.br/paulo/papers/2001-WSeg-flavio.oliveira-marcelo.reis-forense.pdf. Acesso em: 20 set. 2021.

REIS, M. A.; GEUS, P. L. **Análise forense e intrusões em sistemas computacionais**: técnicas, procedimentos e ferramentas. 2013. Disponível em: https://www.lasca.ic.unicamp.br/paulo/papers/2002-Pericia-marcelo.reis-forense.tecnicas.procedimentos.pdf. Acesso em: 20 set. 2021.

SAMPAIO, M. **Terminologia pericial**. 2011. Disponível em: https://www.infocrime.com.br/2011/07/terminologia-pericial. Acesso em: 20 set. 2021.

SANTOS, V. C. M.; MIRANDA, W. G. **A proteção do direito a intimidade segundo a lei 12.737**. 2019. Disponível em: https://jus.com.br/artigos/73475/a-protecao-do-direito-a-intimidade-segundo-a-lei-n-12-737-2012. Acesso em: 20 set. 2021.

SILVA, J. C. **Crime digital**: cibercrime – uma realidade e suas motivações. 2019. Disponível em: https://www.teleco.com.br/tutoriais/tutorialalcrimedig/pagina_3.asp. Acesso em: 20 set. 2021.

VALLIM, A. P. A. **Forense computacional e criptografia**. São Paulo: Editora Senac, 2019.

VELHO, J. A. **Tratado de computação forense**. Campinas: Millennium, 2016.

PADRÕES DE EXAME FORENSE COMPUTACIONAL

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- compreender os padrões e as técnicas utilizados na perícia forense;
- abranger acerca da segurança dos dados (técnicas de hash como preservação de provas);
- compreender o processo e as técnicas de análise de evidências digitais e os equipamentos essenciais utilizados para preservar, coletar e tratar as provas;
- entender o principal recurso do perito para o crescimento de fatos no processo.

PLANO DE ESTUDOS

A cada tópico desta unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – USO DE HASH PARA PRESERVAÇÃO DE EVIDÊNCIAS
TÓPICO 2 – TIPOS DE EXAME (ANÁLISE AO VIVO X ANÁLISE OFF-LINE)
TÓPICO 3 – ANÁLISE DE EVIDÊNCIAS DIGITAIS
TÓPICO 4 – RECUPERAÇÃO DE DADOS: TÉCNICA DE DATA CARVING
TÓPICO 5 – TÉCNICAS COMPLEMENTARES

CHAMADA

Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

CONFIRA A **TRILHA** DA UNIDADE 2!

Acesse o
QR Code abaixo:

USO DE HASH PARA PRESERVAÇÃO DE EVIDÊNCIAS

1 INTRODUÇÃO

Os últimos tempos têm sido marcados pelas transformações tecnológicas e sua evolução em um espaço de tempo muito pequeno. O computador faz parte da vida de milhões de pessoas no mundo (talvez bilhões após a pandemia de 2020, que inseriu a tecnologia na maior parte das relações humanas no período).

A massificação do uso da internet e os dispositivos que a conectam aproximou o uso de recursos importantes para a sociedade. As instituições utilizam cada vez mais a tecnologia para melhorias em suas operações e potencialmente se posicionarem no mercado.

Todos os tipos de transações (comerciais – compra e venda, bancárias, divulgação e marketing, comunicações etc.) ocorrem na internet atualmente. Inclusive o crime. O crime virtual tem crescido exponencial e proporcionalmente à evolução tecnológica. E para combater esse tipo de crime, é fundamental que a Perícia Forense evolua na mesma proporção, utilizando análises e métodos para identificar e coletar evidências eficientes, com a finalidade de coletar provas que possam comprovar os crimes cometidos e seus autores.

Computação forense é a aplicação de técnicas de investigação e análise para reunir e preservar evidências de um dispositivo de computação específico de uma forma que seja adequada para apresentação em um tribunal. O objetivo da computação forense é realizar uma investigação estruturada e manter uma cadeia documentada de evidências para descobrir exatamente o que aconteceu em um dispositivo de computação e quem foi o responsável por isso.

Para Eleutério e Machado (2012), a Computação Forense é a ciência que usa técnicas especializadas para identificar e processar evidências digitais, da mesma forma que a perícia convencional busca evidências para a solução de um crime, procurando coletar, preservar e analisar os dados digitais de dispositivos suspeitos de terem sido utilizados em um crime virtual, sendo, assim, apresentados para a justiça por meio de um laudo pericial.

Reis e Geus (2004) definem a Computação Forense como objeto do processo de investigação. Esse processo deve ser muito transparente e com todas as garantias de manter intactas as provas e os fatos que ocorreram, ou seja, a preservação das evidências é a principal meta do perito ao ter contato com elas.

São considerados quatro princípios a respeito da computação forense:

- Não se pode alterar, em qualquer hipótese, os dados que serão analisados e que possam ser usados em ação judicial.
- Se for necessário acessar os dados como análise de evidências, deve-se fazer uma cópia legítima dos dados e trabalhar na imagem gerada.
- A evidência eletrônica deve ser criada, preservada e auditada, para a garantia de que se algum terceiro analisar a mesma evidência, os mesmos resultados serão encontrados.
- O perito é legalmente responsável pela garantia desses princípios.

A perícia digital começa com a coleta de informações de uma forma que mantenha sua integridade. Os investigadores analisam os dados ou sistema para determinar se foram alterados, como foram alterados e quem o fez.

O uso de computação forense nem sempre está vinculado a um crime. O processo forense também é usado como parte dos processos de recuperação de dados para coletar dados de um servidor travado, unidade com falha, sistema operacional reformatado (SO) ou outra situação em que um sistema tenha parado de funcionar inesperadamente.

Informações podem ser críticas na solução de uma questão legal ou um crime, e a computação forense frequentemente desempenha um papel na identificação e preservação dessas informações.

A evidência digital não é apenas útil na solução de crimes do mundo digital, como roubo de dados, violações de rede e transações ilícitas on-line. Também é usada para solucionar crimes do mundo físico, como roubo, assalto, acidentes de atropelamento e assassinato.

Empresas, atualmente, usam computação forense para rastrear informações relacionadas a sistemas ou redes comprometidos, que pode ser usada para identificar e processar invasores cibernéticos. As empresas também podem usar especialistas e processos forenses digitais para ajudá-los com a recuperação de dados no caso de uma falha de sistema ou rede causada por um desastre natural ou outro.

2 PLANEJAMENTO DA INVESTIGAÇÃO

O planejamento da investigação deve definir o melhor formato para a investigação, identificando as principais atividades que precisarão ser executadas, de acordo com as informações obtidas inicialmente, buscando aproveitar da melhor forma a coleta de dados.

Para Wendt (2020), o local de crime é o lugar onde a suposta infração penal ocorreu, pois podem ser encontradas evidências importantes à investigação, já que mesmo sendo um crime de informática, sempre há um local em que os equipamentos estão localizados e em que foi cometido, de fato, o crime.

2.1 PADRÕES DE EXAME FORENSE COMPUTACIONAL

Segundo o Código de Processo Penal brasileiro, em que está regulamentada a função do Estado de julgar as infrações penais e de aplicar punições a quem as pratica. Em seu texto, define-se como primeira etapa a investigação do crime, que se inicia após uma denúncia ou suspeita de crime, buscando esclarecer a materialidade, a forma e o autor do fato ou crime.

Os procedimentos executados pela autoridade policial devem ser:

- preservar o local e garantir legitimidade das provas até a chegada dos peritos;
- confiscar objetos e dispositivos que possam ter alguma ligação com o ocorrido, assim como coletar as provas para análise e verificação;
- identificar as pessoas envolvidas no local;
- definir quaisquer exames iniciais ou corpo de delito, se necessário.

A investigação e a análise de dispositivos computacionais são divididas em quatro etapas:

1- Coleta: isolamento da área de ação, identificando dispositivos, assim como coletar, guardar e identificar as evidências, como garantia da sua integridade.
2- Exame: é a identificação, extração e documentação dos dados.
3- Análise: a apuração, verificação e o desenvolvimento dos envolvidos e suas relações com pessoas e locais, assim como a reconstrução da cena e toda a documentação.
4- Resultado: é o relatório final construído com a documentação extraída e organizada, com as evidências e demais documentos anexados.

FIGURA 1 – CICLO DE VIDA DA PERÍCIA FORENSE COMPUTACIONAL

FONTE: <https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao>. Acesso em: 14 ago. 2021.

2.2 EQUIPE DE INVESTIGAÇÃO

A equipe de investigação desempenha um papel importante na resolução de um caso e é responsável por avaliar o crime, as evidências e os criminosos. A organização deve atribuir tarefas específicas a cada membro da equipe, apoiada em seus dados e habilidades para formar o processo.

As diretrizes para formar a equipe de investigação são as seguintes:

- Os membros da equipe de investigação forense devem ter dados bastante abrangentes de princípios, diretrizes, procedimentos, ferramentas e técnicas forenses, da mesma forma que as ferramentas e técnicas antiforenses, que podem ocultar ou destruir dados.
- Os membros da equipe de investigação forense precisam ser treinados sobre ameaças de segurança existentes e crescentes.
- Organize os membros da equipe e forneça responsabilidades a cada membro da equipe.
- Elenque alguém como um líder técnico entre os membros da equipe.
- A equipe de investigação deve ser tão pequena quanto o potencial para realizar a confidencialidade.
- Cada membro da equipe deve ter a autorização obrigatória para concluir as tarefas atribuídas.
- Recrute um facilitador de uma equipe de investigação externa, se necessário.

2.3 MÉTODO DE INVESTIGAÇÃO FORENSE COMPUTACIONAL

A Investigação forense computacional deve seguir algumas fases:

- Fase de pré-investigação: esta fase envolve todas as tarefas realizadas antes do início da investigação real. Envolve a criação de um laboratório de informática forense, a construção de uma estação de trabalho forense, um kit de ferramentas de investigação, a equipe de investigação, a obtenção da aprovação da autoridade competente e assim por diante.
- Fase de investigação: é a fase principal da investigação forense na informática, envolve a aquisição, preservação e análise dos dados probatórios para identificar a origem do crime e também o autor do crime. Essa fase envolve a implementação do conhecimento técnico para localizar as evidências, examinar, documentar e preservar as descobertas também como evidências.

Depois de obter as permissões especificadas e avaliar as condições do caso, o investigador está preparado para pesquisar o incidente. A parte de investigação inclui várias etapas e processos que requerem uma execução cuidadosa e sistemática para obter resultados superiores.

O método de investigação forense por computador é uma grande coleção de um tipo de processos, que vão desde a resposta a incidentes até a análise da cena do crime, coleta de provas para sua análise e desde a documentação até as notícias. Cada etapa durante esse processo é igualmente crucial para a aceitação das provas em um tribunal de justiça e o processo contra os perpetradores.

As etapas envolvidas na fase de investigação incluem:

1- Iniciar o processo de investigação.

Os responsáveis pelo incidente devem ter uma ideia clara sobre os objetivos do exame antes de conduzir a investigação. Eles devem ter um conhecimento técnico profundo sobre o funcionamento interno do que está sendo examinado. Devem, ainda, ser capazes de exigir, ou fazer, uma abordagem científica para examinar as provas que fundamentam a solicitação.

2- Realizar investigação forense de computador.

Esta etapa inclui as fases subsequentes:

- Resposta inicial: a primeira resposta refere-se à ação primária, realizada quando da ocorrência de um incidente de segurança. Contando com o tipo de reação, a resposta primária facilitará à vítima evitar danos futuros e pode ajudar os responsáveis pelo incidente a rastrear facilmente o suspeito.

- Busca e apreensão: os investigadores devem ter dados precisos de todos os dispositivos que teriam competido uma parte no envio dos dados de ataque para o dispositivo da vítima. Devem ser capazes de pesquisar todos os dispositivos envolvidos e apreendê-los de maneira formal para analisá-los em busca de dados probatórios.

- Coletar as provas: as evidências são as informações cruciais que facilitarão aos investigadores compreender o método de ataque rastreando o agressor. Portanto, o investigador deve apreender onde quer que observe a prova e a forma de montá-la.

- Garantir a prova: a evidência é um conhecimento frágil, fácil de manipular, alterar e destruir. Portanto, os invasores estão sempre tentando encontrar maneiras de quebrá-la em cada forma potencial. Logo, é importante armazenar e proteger as evidências de maneira econômica.

- Aquisição de dados: durante a investigação de dispositivos digitais, todas as provas podem estar presentes no tipo de informação. Portanto, os investigadores devem ter experiência na aquisição de dados armazenados em vários dispositivos em diferentes formas.

- Análise de dados: a análise de dados refere-se ao método de navegar nos dados das informações e encontrar os dados comprovativos relevantes e sua relevância para o crime. Essa análise ajuda a provar o crime e, portanto, o agressor.

- Fase pós-investigação: esta fase envolve o relato e a documentação de todas as ações realizadas e também dos resultados ao longo de uma investigação. O relatório deve ser realizado com muita clareza e alinhamento porque ele fornece provas adequadas e aceitáveis.

As etapas envolvidas na parte pós-investigação incluem:

- Avaliação da Prova: a avaliação da prova é o método de relacionar as informações comprobatórias obtidas com o incidente para compreensão, entretanto, o incidente completo ocorreu. A avaliação da prova pode ser um estágio crucial dentro do método forense.

A avaliação da prova depende do tipo de incidente, dos objetivos necessários para realizar o incidente, das brechas presentes para a prevalência do incidente e assim por diante.

Ao longo da avaliação, é necessário avaliar a prova digital em correlação com o âmbito do caso para se chegar a uma decisão sobre o curso da ação.

- Documentação e relatórios: documentar é o método de escrever todas as ações que os investigadores realizaram durante a investigação para obter os resultados especificados.

Os investigadores devem mantê-lo na ordem correta e submetê-lo ao tribunal durante todo o julgamento. Eles têm que documentar todos os processos forenses aplicados para detectar, reunir, analisar, preservar e relatar as provas, de modo a fornecer um relatório honesto ao tribunal e facilitar o processo.

- Testemunho de especialista:

O advogado, os promotores e todos os agentes de um tribunal de justiça não têm conhecimento dos dados técnicos sobre o crime, evidências e perdas, logo, os investigadores devem abordar pessoal especializado que possa esclarecer todos os aspectos sobre a investigação dentro do tribunal para confirmar a exatidão do processo e o conhecimento.

Uma testemunha pode ser aquela que contém dados completos sobre um tema, cujas credenciais convencerão outros a acreditar em suas opiniões sobre o assunto em um tribunal.

2.4 USO DE *HASH* PARA PRESERVAÇÃO DE EVIDÊNCIAS

Para Araújo (2020), a preservação das evidências inicia com os processos de análise e verificação do material inicialmente recebido. Essa documentação tem os dados característicos individuais e o estado de conservação da mídia.

A preservação compõe o processo da cadeia de custódia, que trata do processo de manutenção e documentação histórico-cronológica da evidência para manter o rastreio e a legitimidade no processo legal.

Os vestígios digitais devem ser preservados e cuidados para que se possa validar a cena do crime. Em uma investigação, ainda para o autor, não se deve efetuar a investigação diretamente na evidência original, deve-se garantir uma cópia de dados exatamente igual ao original. Essa garantia é realizada por meio de algoritmos de *hash*, os quais são validados ao final da cópia.

2.4.1 Hash

Hashing é uma técnica de programação na qual uma *string* de caracteres (uma mensagem de texto, por exemplo) é convertida em um valor menor, também conhecido como chave ou valor *hash*. Essa chave, que é sempre única e tem um comprimento fixo, representa a *string* original.

No entanto, a chave não pode ser usada para recuperar a mensagem original. Isso garante privacidade e segurança ao compartilhar a mensagem. É usado, em geral, para indexar e acessar itens em um banco de dados, pois encontrar uma chave *hash* mais curta do item é mais rápido do que localizar os dados originais diretamente. Na perícia digital, entretanto, as funções *hash* são usadas para garantir a integridade das evidências.

O hash é uma sequência de números e letras de comprimento fixo gerada a partir de um algoritmo matemático e um arquivo de tamanho arbitrário, como um e-mail, documento, imagem ou outro tipo de dado. A string gerada é exclusiva para o arquivo que está sendo analisado pelo hash e é uma função unilateral (um hash computado não pode ser revertido para encontrar outros arquivos que podem gerar o mesmo valor de hash).

O algoritmo da função hash é especialmente usado em TI e perícia digital. O valor da função hash é usado na autenticação de mensagens, assinaturas digitais e várias autenticações, como códigos de autenticação de mensagens (MACs) etc. Eles também são usados em hash para impressão digital, identificações, identificação de arquivos, somas de verificação e detecção de duplicatas.

O hash é comumente usado para criptografia de dados. Alguns algoritmos de função hash forense populares são MD5, SHA1 e SHA256. Na próxima seção, descreveremos cada um deles em detalhes.

Em termos simples, um valor *hash* é uma *string* numérica específica, criada por meio de um algoritmo e associada a um arquivo específico. Se o arquivo for alterado de alguma forma e o valor for recalculado, o *hash* resultante será diferente. Em outras palavras, é impossível alterar o arquivo sem alterar, também, o valor de *hash* associado. Portanto, se houverem duas cópias de um arquivo e ambas tiverem o mesmo valor de *hash*, pode ter certeza de que são idênticas.

Um valor ***hash*** garante autenticidade graças a quatro características particulares:

- É determinístico, o que significa que uma entrada (ou arquivo) específica sempre fornecerá o mesmo valor de *hash* (*string* numérica). Isso significa que é fácil verificar a autenticidade de um arquivo. Se duas pessoas independentemente (e corretamente) verificarem o valor de *hash* de um arquivo, elas sempre obterão a mesma resposta.
- As chances de "colisões" são baixas. Isso significa que as chances de duas entradas (arquivos) diferentes coincidentemente terem o mesmo valor de *hash* são incrivelmente pequenas – praticamente inexistentes.
- Um ***hash*** pode ser calculado rapidamente. Gerar um valor de *hash* é rápido e fácil (desde que seja usada a ferramenta certa). O tamanho do arquivo em questão também é irrelevante – gerar um valor *hash* para um arquivo grande é tão simples quanto criar um para um arquivo pequeno.

Qualquer mudança na entrada mudará a saída. Mesmo a menor alteração no arquivo de entrada resultará em uma alteração no valor de *hash* resultante. Isso significa que é impossível alterar um arquivo sem alterar o valor de *hash* associado, o que torna muito fácil provar (ou refutar) a autenticidade de uma peça de evidência digital.

2.4.2 Função *hash*

Um algoritmo usado em *hash* é chamado de função ***hash*** e o valor retornado por essa função é chamado de resumo da mensagem ou valor ***hash***.

Características das funções *hash*:

- As funções de *hash* são funções unilaterais, o que significa que não se pode reverter um processo de hash para extrair dados originais de um valor de *hash.*
- O tamanho do valor do *hash* é sempre fixo e é independente do tamanho dos dados de entrada.
- Dois arquivos de entrada diferentes não podem produzir o mesmo valor de *hash.*

FIGURA 2 – TRABALHO DE UM ALGORITMO DE HASH

FONTE: <https://privacycanada.net/hash-functions/>. Acesso em: 15 ago. 2021.

2.4.3 Algoritmos de *hash* MD5, SHA1 e SHA256

- MD5 (*Message Digest* 5)

Na criptografia, o MD5 é um dos algoritmos de *hash* criptográficos mais populares e amplamente usados, que produz valor de *hash* de 128 bits.

O *hashing* MD5 em computação forense é empregado em vários aplicativos de segurança. É uma função *hash* unilateral, especialmente usada para verificar a integridade dos dados dos arquivos. Geralmente, não é possível descriptografar o *hash* MD5 para obter a mensagem original.

É uma das funções *hash* criptográficas mais conhecidas, que foi usada e ainda está em uso. É usado exclusivamente para verificar os dados contra corrupção não intencional. Além da verificação da integridade dos dados, também ajuda a verificar se os dados do e-mail não foram adulterados, uma vez carregados na pasta Caixa de entrada. Ajuda a validar os e-mails de forma contínua.

- SHA1 Secure Hash Algorithm

SHA1 é o algoritmo criptográfico que pega um arquivo de entrada e produz um valor *hash* desse arquivo. Ele gera uma *string* de 160 bits (20 bytes) de comprimento.

Essa função *hash* na segurança da rede também é conhecida como resumo da mensagem. Normalmente, é representado como um número hexadecimal de 40 caracteres na forma hexadecimal.

O algoritmo de *hash* criptográfico SHA1 é mais usado para verificar se os arquivos são alterados ou não. Esse processo ocorre produzindo a soma de verificação antes da transmissão dos arquivos de dados.

Depois que o arquivo chega ao destino, o valor do *hash* na análise forense digital produz novamente um valor para verificar a soma de verificação do mesmo arquivo.

- SHA256 (*Secure Hash Algorithm* 256)

O *hash* criptográfico SHA256 (às vezes chamado de "*digest*") também é conhecido como *hash* unilateral. É quase impossível reverter o valor do *hash* do arquivo original, e ele funciona como assinatura de um texto ou conjunto de dados. Ele converte um texto de qualquer comprimento em uma *string* exclusiva de 356 *bits* (32 *bytes*) de tamanho.

O algoritmo de função *hash* forense SHA-256 é usado principalmente para verificar a integridade dos arquivos de dados, incluindo assinaturas digitais, verificação de transação. Além disso, ele não pode descriptografar os dados de volta à sua forma original.

QUADRO 1 – PRINCIPAIS DIFERENÇAS ENTRE OS ALGORITMOS MD5 E SHA1

Fator Diferenciador	MD5	SHA1
Comprimento do valor de hash	128 bits	160 bits
Nível de segurança	Pobre	Moderado
Velocidade	Rápido	Lento
Complexidade do algoritmo	Simples	Complexo

FONTE: A autora

O uso de algoritmos *hash* MD5 e SHA1 é uma prática padrão em análise forense digital. Esses algoritmos permitem que os investigadores preservem as evidências digitais desde o momento em que as adquirem até o momento em que são apresentadas no tribunal.

2.5 USANDO VALORES DE *HASH* PARA AUTENTICAR EVIDÊNCIAS

O valor de *hash* atua como uma assinatura digital (ou impressão digital) que autentifica a evidência. Contanto que uma parte da evidência tenha sido coletada e processada corretamente, qualquer outra parte examinando independentemente o valor de *hash* encontrará a mesma sequência de números.

Em outras palavras, se uma pessoa usa uma ferramenta para autenticar uma evidência com um algoritmo de *hash* durante a coleta, qualquer pessoa que use o mesmo algoritmo para autenticá-la em um estágio posterior verá exatamente o mesmo valor de *hash* resultante – e qualquer alteração nos dados resultará na alteração do valor do *hash*.

É por isso que os valores de hash são tão cruciais: eles fornecem evidências incontestáveis e facilmente verificáveis de que as evidências não foram adulteradas.

3 OBJETOS DO EXAME (MÍDIA DE PROVA X MÍDIA DESTINO)

Segundo Jorge (2018), é fundamental a realização de um registro inicial dos fatos criminosos (Boletim de Ocorrência) e elaborar um Auto de Materialização de Evidência Eletrônica para garantia e segurança das evidências coletadas, assim como evitar que a evidência seja apagada antes de que a sua existência possa ser usada como prova no inquérito policial e na ação penal.

> O Auto de Materialização de Evidência Eletrônica é um documento que tem a finalidade de descrever como se deu o acesso às evidências, bem como informar data, horário e fuso horário do acesso e formalizar o conteúdo criminoso indicado pela vítima ou por outra pessoa que tenha permitido que o fato criminoso fosse investigado. É importante não se esquecer de apresentar todos os links que tenham relação com o fato em investigação – por exemplo, os links do perfil do Facebook, do Twitter, do blog e do site que tenham publicado o conteúdo de interesse policial (JORGE, 2018, s.p.).

O autor ainda recomenda que ao envolver som ou imagem, a investigação deve armazenar o conteúdo em mídias, de preferência não regravável ou em mídias que permitam a geração de *hash*, com chave criptográfica capaz de comprovar a autenticidade do arquivo.

3.1 ASSINATURA DE MÍDIAS DE PROVA

Com o uso de algoritmo de *hash*, é possível garantir a integridade dos dados a serem analisados. A função *hash* mapeia um conjunto de *bits* e gera uma assinatura no arquivo, pois caso haja alguma alteração, será possível identificá-la.

3.2 OBJETO FÍSICO DA INVESTIGAÇÃO

É o equipamento ou seus periféricos e mídias, que podem conter as provas da investigação, entre eles, arquivos em disco ou memória, dados trafegados na rede.

3.3 MÍDIA DE DESTINO

É o destino dos dados capturados ou copiados da mídia de provas. É a imagem pericial sobre a qual serão realizados os procedimentos de análise e busca por provas. Nesse momento, é necessário o uso de assinatura *hash* para garantir a integridade, de preferência, nesse momento, deve-se arrolar testemunhas para a execução do procedimento.

RESUMO DO TÓPICO 1

Neste tópico, você aprendeu:

- Planejar a investigação é o ponto de partida para a perícia forense. Ela deve ser seguida da proteção da integridade das evidências coletadas, a qual é vital para a aplicação da lei.

- Se a integridade das provas for posta em dúvida, seu uso em processos judiciais pode ser comprometido, possivelmente permitindo que um culpado escape da acusação.

- Aspectos importantes como o uso do Hash para proteger o material digital e a preservação dos objetos de exame são técnicas necessárias para o processo de preservação das evidências.

AUTOATIVIDADE

1 O planejamento da investigação deve definir o melhor formato para ela, identificando as principais atividades que precisarão ser executadas, de acordo com as informações obtidas inicialmente, buscando aproveitar da melhor forma a coleta de dados. A preservação das evidências deve ser garantida em todas as etapas da investigação. Sobre a preservação das evidências na investigação, analise as sentenças a seguir:

I- Análise é a pesquisa sobre as evidências do crime e a análise do local.
II- Preservação é o ato de identificar e manter a integridade das possíveis evidências no local do crime.
III- Coleta é a ação de extrair as informações necessárias dos itens identificados como possíveis evidências.

Assinale a alternativa CORRETA:

a) ( ) Somente a sentença I está correta.
b) ( ) As sentenças II e III estão corretas.
c) ( ) As sentenças I e II estão corretas.
d) ( ) Somente a sentença III está correta.

2 Existem alguns procedimentos executados pela autoridade policial para a investigação do crime. Pensando nesses procedimentos, assinale a alternativa CORRETA:

a) ( ) Dirigir-se ao local e preservar o estado e a conservação das coisas até a chegada dos peritos criminais.
b) ( ) Apreender os objetos que tiverem relação com o fato antes de serem liberados pelos peritos.
c) ( ) Alterar os dados de um computador ou mídia de armazenamento para que possam ser posteriormente invocados em tribunal.
d) ( ) Não é necessário o reconhecimento de pessoas e coisas envolvidas.

3 A investigação envolvendo uma análise de dispositivos computacionais está dividida em quatro etapas, sendo que três delas são essenciais para a investigação. Pensando nas etapas da investigação envolvendo análise, classifique V para as sentenças verdadeiras e F para as falsas:

( ) Coleta.
( ) Exame.
( ) Análise.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – V.
b) ( ) F – F – V.
c) ( ) V – V – F.
d) ( ) F – F – F.

4 O que é *hash* e qual sua importância para a perícia forense computacional?

5 A computação forense é uma área muito importante para a atualidade. Defina o conceito e comente o objetivo da computação forense.

TIPOS DE EXAME (ANÁLISE AO VIVO X ANÁLISE OFF-LINE)

1 INTRODUÇÃO

Proteger a integridade das evidências coletadas é vital para a aplicação da lei. Se a integridade das provas for posta em dúvida, seu uso em processos judiciais pode ser comprometido, possivelmente permitindo que um culpado escape da acusação.

Os países com um histórico de Estado de Direito têm uma estrutura de regras e procedimentos que estipulam como as evidências devem ser coletadas, usadas e preservadas. A prova é admissível em tribunal apenas se as regras forem seguidas. Os acusados têm direitos processuais, dando-lhes proteção contra adulteração de provas para manipular o resultado de uma investigação ou um julgamento.

É importante que qualquer pessoa que lida com as provas durante uma investigação conheça e siga as regras relativas à admissibilidade das provas e à análise dos exames. Eleutério e Machado (2012) apresentam os seguintes tipos de exames ligados à área da Perícia Forense Computacional, conforme o Quadro 2.

QUADRO 2 – TIPOS DE EXAMES LIGADOS À ÁREA DA PERÍCIA FORENSE COMPUTACIONAL

TIPOS DE EXAMES	
No local do crime computacional	São executados no local do crime, em que o perito criminal mapeia e identifica para futura análise em laboratório.
Dispositivos computacionais	Análise de todos os equipamentos de armazenamento e tráfego.
Smartphone	Dados e arquivos são extraídos para possíveis análises.
Sites e navegadores	Todos os históricos e fluxos de navegação são analisados.
Mensagens de correio eletrônico	Identificação de remetentes e conteúdos dos e-mails dos investigados, com possíveis extrações de dados e informações relevantes ao processo.

FONTE: Eleutério e Machado (2012, s.p.)

2 COLETA DE EVIDÊNCIAS DIGITAIS

A coleta de evidências digitais é fundamental ao processo de investigação. Os computadores são usados para cometer crimes e, graças à ciência da perícia de evidências digitais, a polícia tem utilizado computadores para combater o crime.

Provas digitais são informações armazenadas ou transmitidas em forma binária que podem ser consideradas em tribunal. Podem ser encontradas no disco rígido de um computador, um telefone celular, entre outros locais. A evidência digital é comumente associada ao crime eletrônico ou e-crime, como pornografia infantil ou fraude de cartão de crédito. No entanto, as evidências digitais têm sido usadas para processar todos os tipos de crimes, não apenas os crimes eletrônicos.

A coleta dos dados digitais é a aquisição dos dados que podem ser relevantes para a investigação. A coleta pode envolver a remoção de dispositivos eletrônicos da cena do crime ou do incidente e, em seguida, a imagem, a cópia ou a impressão de seu conteúdo.

QUADRO 3 – PRÁTICAS QUE DEVEM ANTECEDER A COLETA DE DADOS

Esterilização das mídias ou uso de novas mídias a cada investigação.
As ferramentas a serem utilizadas devem ser licenciadas e devem estar prontas para utilização.
Nada deve ser alterado sem a anuência do perito.
Registros devem ser feitos, ou seja, deve-se filmar ou fotografar o local para registrar detalhes.

FONTE: A autora

Uma atividade crucial que acompanha as primeiras etapas é fazer anotações históricas. Essa é a documentação do que foi feito imediatamente após a coleta, com detalhes suficientes para que outra pessoa possa reproduzir todo o procedimento apenas a partir das anotações.

O armazenamento adequado das informações é muito importante para garantir a integridade e veridicidade das provas. O armazenamento delas deve ser feito de forma segura, em local íntegro, por profissionais éticos, para que de forma alguma caia em mãos erradas.

A coleta de dados deve iniciar com a manutenção do estado do equipamento, que deve ser mantido ligado ou desligado, de acordo com seu estado atual. Assim, não será feita nenhuma adulteração nas evidências.

O material coletado deve ser mantido íntegro nessa fase, garantindo que as informações não sofram modificações durante a investigação e processo.

É muito importante fazer uma cópia *bit* a *bit* ou um espelhamento de todo o material lógico, fidelizando a imagem obtida na fase de coleta, assim como efetuar a extração de *hashes* de verificação.

A fase de extração tem como principais ações a recuperação de arquivos apagados e a indexação de dados. Existem ferramentas que fazem esse procedimento. O processo de cópia das informações pode ser feito através de softwares que duplicam disco ou softwares específicos para perícia. Com as ferramentas adequadas, a evidência não será comprometida durante a cópia, mantendo a sua integridade.

O dispositivo de armazenamento computacional deverá ser lacrado e guardado em local apropriado, ao fim do processo de coleta, aguardando a autorização por parte da justiça para encerramento do uso, assim como o destino que pode ser o descarte ou a devolução.

2.1 ANÁLISE AO VIVO

É a realização da perícia em tempo real. A análise é feita diretamente sobre a mídia de provas. Esse procedimento não é considerado ideal para a garantia da integridade das provas, pois pode ser contestado, podendo ser considerado como delito não comprovado e, ainda, a manipulação de evidências pode inviabilizar uma perícia posterior, caso haja uma alteração de mídia de provas.

A análise ao vivo é o processo de coleta de evidências forenses do sistema do computador do suspeito quando ele está em execução. Porém, esse processo não é amplamente aceito como um procedimento cibernético forense em muitos países.

Em vez de começar com um procedimento forense ao vivo, geralmente, uma análise off-line tradicional é adotada, de acordo com o procedimento forense cibernético aceito. Isso envolve puxar o plugue de alimentação do sistema do suspeito e criar imagens da mídia de armazenamento.

A evidência crucial disponível no sistema em execução é perdida para sempre ao desligar o sistema. As informações mais importantes que podem ser coletadas em análises forenses ao vivo são as evidências disponíveis na memória de acesso aleatório de um sistema.

Como um sistema operacional Windows adiciona pegadas de cada uma de suas atividades atuais na RAM, analisar seu conteúdo é indispensável em uma análise cibernética forense. E isso pode fornecer informações que podem ser cruciais para a realização de investigações adicionais.

Como o conteúdo da RAM é altamente volátil, seu conteúdo completo é perdido ao desligar o sistema. Nesse artigo, é explicada uma metodologia para recuperar artefatos forenses de memória, ao mesmo tempo em que adota uma análise forense off-line tradicional. Isso é feito analisando o arquivo de hibernação disponível na partição de diretório do Windows dentro do disco rígido do sistema do suspeito.

2.2 ANÁLISE OFF-LINE

A perícia digital tradicional é realizada por meio de análise estática de dados preservados em mídia de armazenamento permanente. Nem todos os dados necessários para entender o estado do sistema examinado existem na memória não volátil.

A análise ao vivo usa o sistema em execução para obter dados voláteis para uma compreensão mais profunda dos eventos que estão acontecendo. A amostragem do sistema em execução pode alterar irreversivelmente seu estado, tornando as evidências coletadas inválidas.

A virtualização é usada para dar vida aos dados estáticos. O despejo de memória volátil é usado para permitir a análise off-line de dados ativos. Usando dados de despejo de memória, a máquina virtual criada a partir de dados estáticos pode ser ajustada para fornecer uma melhor imagem do sistema ativo quando o despejo foi feito.

O investigador pode ter uma sessão interativa com a máquina virtual sem violar a integridade da evidência. Também conhecida como análise "Post Mortem". A análise off-line é feita após a coleta de dados e é operacionalizada sobre a mídia de destino.

3 DUPLICAÇÃO FORENSE EM MÍDIAS (LOCAL E REMOTA)

É fundamental lembrar da máxima de que todos os procedimentos periciais devem estar subsidiados juridicamente para que possam ser eficazes no processo investigativo. Perícias sem amparo legal se tornam tão ou mais ilegais que as suspeitas investigadas.

A cópia de um dispositivo para a geração da imagem é uma das ações de início da investigação. A técnica "dead analysis" é aquela em que o dispositivo a ser verificado deve ser copiado com fidelidade *bit a bit* e todos os exames e análises devem ser feitos nessa imagem, mantendo íntegro o dispositivo.

Muitas vezes a evidência não está numa mídia estática, está em uma memória RAM do computador ou trafegando na rede. Para tanto, deve-se optar pela coleta live para a captura dos dados que trafegam na rede usando ferramentas que analisem os protocolos de rede e verifiquem pacotes.

4 COLETA DE DADOS VOLÁTEIS: TRÁFEGO DE REDE

Essa análise forense digital se preocupa em monitorar e analisar o fluxo de tráfego em redes de computadores para extrair evidências, como, por exemplo, descobrir a fonte de ataques de segurança, a fim de incriminar o causador do dano ou para detectar intrusões. A análise forense de redes lida basicamente com dados voláteis, ao contrário de outros tipos forenses digitais.

As redes apresentam aos investigadores uma série de desafios. Quando as redes estão envolvidas em um crime, as evidências são frequentemente distribuídas em muitos computadores, tornando a coleta de todo o hardware, ou mesmo de todo o conteúdo de uma rede, inviável.

Além disso, as evidências estão frequentemente presentes em uma rede por apenas uma fração de segundo – as janelas de oportunidade para coletar tais evidências voláteis são muito pequenas.

O software de criptografia está se tornando mais comum, permitindo que os criminosos embaralhem as evidências incriminatórias usando esquemas de codificação muito seguros. Além disso, ao contrário do crime no mundo físico, um criminoso pode estar em vários lugares em uma rede a qualquer momento. Uma sólida compreensão de redes de computadores e a aplicação dos princípios da ciência forense a essa tecnologia é um pré-requisito para qualquer pessoa responsável por identificar, proteger e interpretar evidências em uma rede.

4.1 CAPTURA DE TRÁFEGO

Interceptação de tráfego de rede, para posterior extração de dados considerados relevantes:

- Origem e destinos da comunicação.
- Protocolos e serviços utilizados.
- Remontagem dos fluxos de dados.
- Análise do seu conteúdo.

Interceptação de tráfego é considerada legal quando realizada por agente ou perito (autorizado). A Lei n° 9.296/96 regulamenta a “interceptação do fluxo de comunicações em sistemas de informática e telemática”. Nela é citada a definição da interceptação das comunicações:

> Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.
> Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:
> I- da autoridade policial, na investigação criminal;
> II- do representante do Ministério Público, na investigação criminal e na instrução processual penal.
> Art. 4° O pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.
> § 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo (BRASIL,1996).

4.2 INTERCEPTAÇÃO ILEGAL

Entre as modalidades de Interceptação ilegal, existem: o *pharming*, o *Session hijacking* (sequestro de cookies) e o "*man-in-the-middle*".

Pharming é uma prática fraudulenta na qual um código malicioso é instalado em um computador pessoal (PC) ou servidor, direcionando os usuários para sites fraudulentos sem o seu conhecimento ou consentimento. O objetivo é que os usuários insiram suas informações pessoais. Depois que informações, como número de cartão de crédito, número de conta bancária ou senha, são inseridas em um site fraudulento, os criminosos as possuem e o roubo de identidade pode ser o resultado.

O *Session hijacking* é o sequestro de uma sessão. Um usuário em uma sessão pode ser sequestrado por um invasor e perder o controle da sessão por completo, onde seus dados pessoais podem ser facilmente roubados. Depois que um usuário inicia uma sessão, como fazendo *login* em um site de banco, um invasor pode sequestrá-lo.

Para sequestrar uma sessão, o invasor precisa ter um conhecimento substancial da sessão de cookie do usuário. Embora qualquer sessão possa ser hackeada, é mais comum em sessões de navegador em aplicativos da web.

A sessão pode ser sequestrada de várias formas, dependendo da posição e do vetor do invasor. Aqui estão algumas das maneiras pelas quais uma sessão pode ser sequestrada:

QUADRO 4 – MANEIRAS PELAS QUAIS UMA SESSÃO PODE SER SEQUESTRADA

Cross-site scripting (XSS)	Os invasores exploram vulnerabilidades em servidores ou aplicativos para injetar scripts Java do lado do cliente nas páginas da web dos usuários, fazendo com que seu navegador execute código arbitrário ao carregar uma página comprometida. Se o servidor não definir o HTTPOnly nos cookies de sessão, os scripts injetados podem obter acesso à sua chave de sessão, fornecendo aos invasores as informações necessárias para o sequestro de sessão.
Session side jacking	Ao usar o packet sniffing, um invasor pode monitorar o tráfego na rede e interceptar os cookies de sessão do usuário depois de autenticá-los. Se o site seguir o caminho mais barato de usar criptografia SSL/TLS apenas para suas páginas de login, o invasor pode usar a chave de sessão que derivou da detecção de pacotes para sequestrar a sessão do usuário e personificá-lo para executar ações no aplicativo da web. Isso geralmente pode acontecer no caso de um Hotspot WiFi inseguro para obter acesso à rede, monitorar o tráfego e configurar seus próprios pontos de acesso para realizar o ataque.
Fixação de sessão	Os invasores fornecem uma chave de sessão e enganam o usuário para que ele acesse um servidor vulnerável.

FONTE: A autora

A ameaça de sequestro de sessão existe devido ao protocolo sem status. Esses protocolos têm limitações, por isso são vulneráveis a ataques.

Já o ataque *man-in-the-middle* é um tipo de ataque em que os invasores interceptam uma conversa ou intercâmbio de dados existente. Nesse processo, fingem ser o participante real da outra ponta da conversa. Isso permite que um invasor intercepte informações e dados de qualquer uma das partes e, ao mesmo tempo, envie links maliciosos ou outras informações para os dois participantes legítimos, de uma forma que pode não ser detectada até que seja tarde demais.

Em um ataque *man-in-the-middle,* o "espião" manipula a conversa desconhecida para qualquer um dos dois participantes legítimos, agindo para recuperar informações confidenciais e, de outra forma, causar danos. Abreviações comuns para um ataque *man-in-the-middle são* MITM, MitM, MiM e MIM.

4.3 PRINCIPAIS CARACTERÍSTICAS DE UM ATAQUE *MAN-IN-THE-MIDDLE*

QUADRO 5 – CARACTERÍSTICAS DO ATAQUE

Man-in-the-middle
É um tipo de sequestro de sessão.
Envolve invasores que se inserem como retransmissores ou proxies em uma conversa ou transferência de dados legítima em andamento.
Explora a natureza em tempo real das conversas e transferências de dados para passar despercebido.
Permite que invasores interceptem dados confidenciais.
Permite que invasores insiram dados e links maliciosos de uma forma indistinguível de dados legítimos.

FONTE: A autora

Esse tipo de ataque é facilitado pelo uso de redes Wi-Fi abertas e sem criptografia. A interceptação legal, ou grampo legal, como também é conhecida, apareceu na apresentação dos sistemas utilizados pela polícia brasileira. Um desses sistemas é o Guardião, utilizado pela polícia civil para monitorar de maneira autorizada pela justiça.

INTERESSANTE

O sistema Guardião ficou conhecido ao aparecer no filme Tropa de Elite 2, em que conversas interceptadas em um computador são apresentadas por subordinado ao capitão Nascimento.

4.4 FERRAMENTA FORENSE

As ferramentas forenses comumente disponíveis hoje têm recursos robustos para identificar e recuperar arquivos excluídos no curso normal do processamento.

As ferramentas forenses são valiosas para análise e automatização de grande parte do processo de análise, como:

- Identificar e recuperar fragmentos de arquivos e arquivos e diretórios ocultos e excluídos de qualquer local (por exemplo, espaço usado e espaço livre).
- Examinar estruturas de arquivos, cabeçalhos e outras características para determinar que tipo de dados cada arquivo contém, em vez de depender de extensões de arquivo (por exemplo, .doc, .jpg, .mp3).
- Exibir o conteúdo de todos os arquivos gráficos.
- Realizar pesquisas complexas.
- Exibir graficamente a estrutura de diretório da unidade adquirida.
- Gerar relatórios.

Existem muitas ferramentas de hardware projetadas e construídas especificamente para análise forense digital. Algumas dessas ferramentas incluem dispositivos de clonagem, dispositivos de aquisição de telefones celulares, bloqueadores de gravação, dispositivos de armazenamento portáteis, adaptadores, cabos e muito mais.

O processo de definição e posicionamento da ferramenta de interceptação e captura ou de monitoramento de redes segue passos bem definidos, como conter um SWITCH com porta de monitoramento ou HUB que devem estar conectados: na máquina alvo da investigação e no roteador de saída da rede para a Internet. Normalmente será necessária a instalação de *software* e/ou hardware (cooperação).

4.5 FERRAMENTA FORENSE AVANÇADA OWASP SSL/ AUDITORIA OWASP

Um exemplo de ferramenta avançada é o O-Saft, uma ferramenta fácil de usar para mostrar informações sobre o certificado SSL e testar a conexão SSL de acordo com determinada lista de cifras e várias configurações SSL. Ele é projetado para ser usado por testadores de penetração, auditores de segurança ou administradores de servidor. A ideia é mostrar as informações importantes ou as verificações especiais com uma simples chamada da ferramenta. No entanto, ele oferece uma ampla gama de opções para que possa ser usado para verificações abrangentes e especiais por pessoas experientes.

O-Saft é uma ferramenta de linha de comando, portanto, pode ser usada off-line e em ambientes fechados. Também existe uma GUI baseada em Tcl/Tk. No entanto, pode simplesmente ser transformado em uma ferramenta CGI on-line.

Outro exemplo de *software* é o Wireshark, que coloca a rede em modo promíscuo, possibilitando a análise e captura dos pacotes que circulam na rede. É uma ferramenta *Open Source* e muito robusta, que possui uma interface gráfica bem intuitiva para quem trabalha com redes e está familiarizado com as camadas dos protocolos.

5 COLETA DE DADOS VOLÁTEIS: MEMÓRIA

A análise forense de memória pode fornecer percepções exclusivas sobre a atividade do sistema em tempo de execução, incluindo conexões de rede abertas e comandos ou processos executados recentemente. Em muitos casos, os dados críticos relativos a ataques ou ameaças existirão apenas na memória do sistema – os exemplos incluem conexões de rede, credenciais de conta, mensagens de bate-papo, chaves de criptografia, processos em execução, fragmentos de código injetados e histórico da Internet que não pode ser armazenado em cache. Qualquer programa – malicioso ou não – deve ser carregado na memória para ser executado, tornando a análise forense crítica para identificar ataques de outra forma ofuscados.

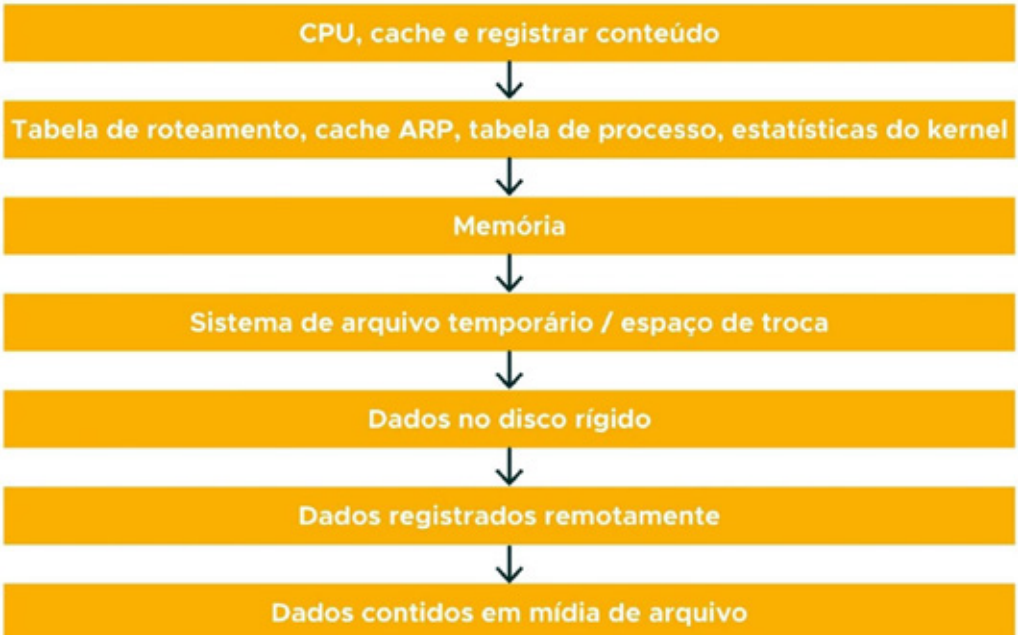
A evidência que está presente apenas enquanto o computador está funcionando é chamada de evidência volátil e deve ser coletada usando métodos forenses em tempo real. Isso inclui evidências de que estão na RAM (memória de acesso aleatório) do sistema, como um programa que está presente apenas na memória do computador.

Um despejo de memória (também conhecido como despejo de núcleo ou despejo do sistema) é uma captura instantânea dos dados da memória do computador de um instante específico. Um despejo de memória pode conter dados forenses valiosos sobre o estado do sistema antes de um incidente, como uma falha ou comprometimento da segurança. Os despejos de memória contêm dados de RAM que podem ser usados para identificar a causa de um incidente e outros detalhes importantes sobre o que aconteceu.

A ordem de volatilidade é importante para priorizar as evidências a serem coletadas. Geralmente, o ideal é começar com as evidências mais voláteis primeiro, processo conhecido como a ordem da volatilidade.

A ordem da volatilidade, do mais volátil (RAM) ao menos volátil (dados arquivados), pode ser vista no Quadro 6:

QUADRO 6 – ORDEM DA VOLATILIDADE



FONTE: A autora

Para Eleutério e Machado (2012, s.p.), "a Memória RAM é volátil, e seus dados são perdidos quando o computador é desligado. Assim, caso o perito suspeite que evidências estejam contidas nesse tipo de memória, ferramentas próprias podem ser utilizadas para realizar tal cópia".

A RAM é a fonte mais "rica" para a coleta de dados voláteis, pois nela estão contidos:

- Processos (e sua memória).
- Arquivos abertos.
- Conexões de rede.
- Usuários conectados.

Os programas que estão presentes apenas na memória do computador são considerados TSRs ou programas *Terminate and Stay Resident*. Vários tipos de *malware*, como programas cavalo de Tróia, vírus e Worms, são projetados para serem apenas programas residentes na memória, presentes na memória do computador durante a operação e desaparecem quando o computador é desligado, em muitos casos sem deixar rastros.

Existem, também, muitos tipos de outras evidências voláteis que estão disponíveis apenas enquanto o computador está em execução, incluindo determinados arquivos temporários, arquivos de log, arquivos em cache e senhas.

A RAM é apagada quando o computador é desligado e todos os dados presentes são perdidos. Essa pode ser uma etapa crítica se houver suspeita de que qualquer tipo de criptografia de dados está habilitado para evitar que o disco rígido ou partes do disco sejam visualizados.

Em muitos casos, a única maneira de recuperar a senha necessária para remover a criptografia em um disco rígido é coletar a "memória ativa" antes que o computador seja desligado. Além disso, se o computador estiver funcionando, a parte criptografada do armazenamento de dados estará acessível, mas apenas até que o computador seja desligado, tornando essencial que o disco rígido seja copiado enquanto o computador ainda estiver ligado.

Existem ferramentas disponíveis para fazer cópias de RAM e discos rígidos em computadores em execução e servidores de linha de negócios que não podem ser desligados e, ainda assim, garantir que essas cópias sejam válidas do ponto de vista jurídico.

RESUMO DO TÓPICO 2

Neste tópico, você aprendeu:

- Os exames são parte crucial da investigação. Para que sejam analisados adequadamente, a coleta dos dados digitais relevantes precisa ser minuciosa. Ela pode envolver a remoção de dispositivos eletrônicos da cena do crime ou do incidente e, em seguida, a imagem, a cópia ou a impressão de seu conteúdo.

- O armazenamento adequado das informações é muito importante para garantir a integridade e veridicidade das provas e deve ser feito de forma segura, em local íntegro, por profissionais éticos, para que de forma alguma não caia em mãos erradas.

- A coleta de dados deve se iniciar com a manutenção do estado do equipamento, garantindo que nenhuma adulteração seja feita nas evidências.

- Na perícia de rede, a análise de pacotes pode ser usada para coletar evidências para investigações de atividades digitais e para detectar tráfego e comportamento de rede malicioso, incluindo tentativas de intrusão e uso indevido de rede, e identificar ataques *man-in-the-middle* e *malware*, como *ransomware*.

AUTOATIVIDADE

1 Na investigação forense, existem alguns tipos de exames de objetos caracterizados. Pensando nesses exames, assinale a alternativa CORRETA:

a) ( ) Exames e procedimentos nos locais do crime de informática.
b) ( ) Exames em dispositivos de armazenamento em papel.
c) ( ) Exames médicos.
d) ( ) Exames em bibliotecas físicas.

2 A análise ao vivo é muito importante para a investigação, pois nela podem ser encontrados indícios recentes do suposto crime. Sobre a análise ao vivo de evidências, classifique V para as sentenças verdadeiras e F para as falsas:

( ) É o processo de coleta de evidências forenses do sistema do computador do suspeito quando ele está em execução.
( ) As informações mais importantes que podem ser coletadas em análises forenses ao vivo são as evidências disponíveis na memória de acesso aleatório de um sistema.
( ) É um processo amplamente aceito como um procedimento cibernético forense em muitos países.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – V.
b) ( ) F – F – V.
c) ( ) V – V – F.
d) ( ) V – F – F.

3 É fundamental lembrar da máxima de que todos os procedimentos periciais devem estar subsidiados juridicamente para que possam ser eficazes no processo investigativo. Perícias sem amparo legal se tornam tão ou mais ilegais que as suspeitas investigadas. Tendo a duplicação forense de mídias em mente, sobre a preservação das evidências na investigação, analise as sentenças a seguir:

I- A técnica "*dead analysis*" determina que o disco a ser analisado deve ser clonado bit a bit e qualquer análise deve ser feita nessa cópia, de forma a manter a mídia analisada íntegra.
II- A imagem deve ser uma cópia fiel de todos os dados do disco, incluindo as partes não utilizadas.
III- A fase de coleta de evidências digitais é aquela que é realizada sobre fontes não voláteis, que independem de energia para armazenar os dados.

Assinale a alternativa CORRETA:

a) ( ) Somente a sentença I está correta.
b) ( ) As sentenças II e III estão corretas.
c) ( ) As sentenças I e II estão corretas.
d) ( ) Somente a sentença III está correta.

4 A coleta digital é uma fase fundamental ao processo de investigação. Qual a sua definição?

5 Como é possível garantir a assinatura de mídia de prova?

ANÁLISE DE EVIDÊNCIAS DIGITAIS

1 INTRODUÇÃO

Para que as provas digitais sejam aceitas em um tribunal, elas devem ser tratadas de maneira muito específica, de modo que não haja oportunidade para os criminosos cibernéticos adulterarem as provas.

Para tanto, alguns passos devem ser seguidos:

1- Identificação – encontrar a evidência, observando onde ela está armazenada.
2- Preservação – isolar, proteger e preservar os dados. Isso inclui evitar que as pessoas possam adulterar as evidências.
3- Análise – reconstrução dos fragmentos de dados e tirar conclusões com base nas evidências encontradas.
4- Documentação – registro de todos os dados para recriar a cena do crime.
5- Apresentação – resumo e conclusão.

Na análise de dados, a equipe responsável examina os dados adquiridos para identificar as informações probatórias que podem ser apresentadas ao tribunal. Essa fase trata de examinar, identificar, separar, converter e modelar dados para transformá-los em informações úteis.

2 FERRAMENTA DE ANÁLISE HD

O Sleuthkit é um *framework* de ferramentas voltadas à análise forense computacional, que somente aceita a participação de ferramentas livres. Esse kit possui várias ferramentas importantes para a análise forense, entre elas o Autopsy. O Autopsy é uma interface de trabalho do Sleuthkit, bem visual e mais automatizada. Esse kit trabalha com a análise do HD, automaticamente reconhecendo as partições do disco rígido.

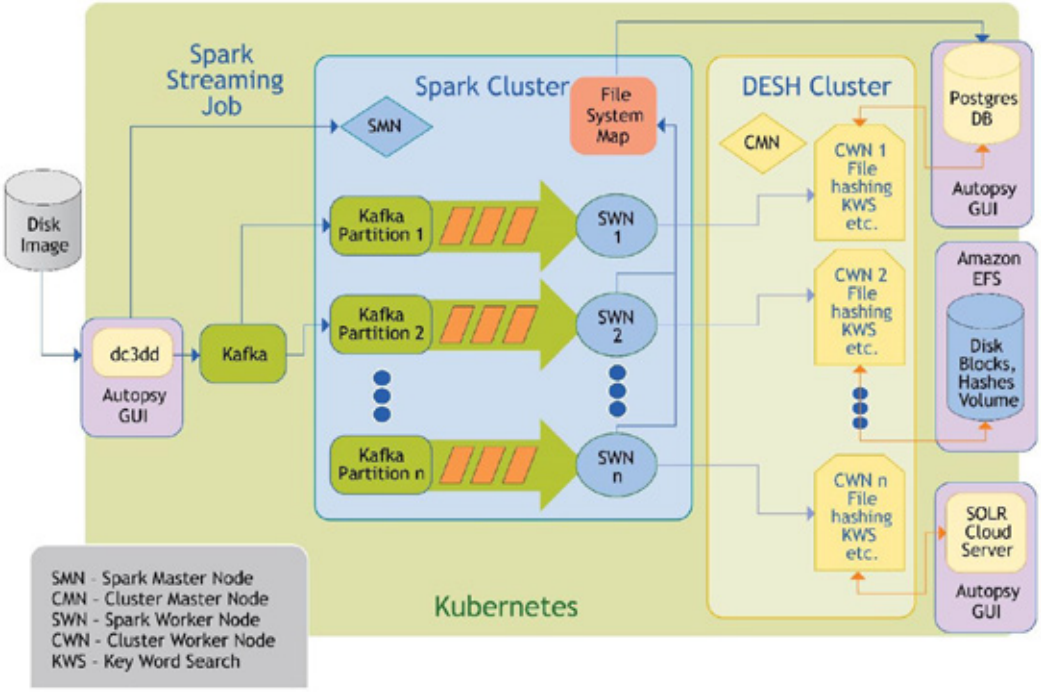
O Encase é outra ferramenta de análise em que se consegue identificar o autor da utilização do disco rígido, por meio do acesso a servidores de instalação de aplicativos, chaves de registro e backup de sistema. Esse sistema ainda permite identificar endereço de rede de servidores acessados na Internet e os dados de autenticação (usuário e senha) deles.

O site do Encase apresenta como características do software:

- Coleta completa de evidências – aquisição de evidências de múltiplas fontes para descobrir, coletar e preservar informações potencialmente relevantes.
- Fluxos de trabalho personalizáveis – eficiência na investigação com fluxos de trabalho otimizados do investigador com condições e filtros predefinidos ou personalizados para localizar evidências rapidamente.
- Relatórios abrangentes – resultados de evidências.

Outra ferramenta importante para a análise de evidências é o projeto DFORC2, um projeto de código aberto. Os usuários interagem com o DFORC2 também por meio do Autopsy. O DFORC2 foi projetado para que o aplicativo também possa usar o Kubernetes Cluster Manager, um projeto de código aberto que fornece recursos de escalonamento automático quando implantado em serviços de computação em nuvem apropriados.

FIGURA 3 – ARQUITETURA DO SISTEMA DFORC2



FONTE: <https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis>. Acesso em: 18 ago. 2021.

A principal vantagem do DFORC2 é que ele reduzirá significativamente o tempo necessário para analisar e processar a evidência digital.

A vantagem de velocidade do DFORC2, no entanto, dependerá de dois fatores. O primeiro fator é a velocidade e a memória do servidor. Para servidores menores (aqueles com 16 GB de RAM ou menos e um microprocessador mais antigo), a versão independente original do Autopsy terá um desempenho melhor do que o DFORC2. Em um servidor maior (um com 28 GB de RAM ou mais e um novo microprocessador multicore de última geração), o DFORC2 será mais rápido.

O segundo fator é o número de nós de trabalho que podem ser alocados aos *clusters*. DFORC2 organiza recursos em um gerenciador de *cluster* e nós de trabalho. Os nós de trabalho executam tarefas de computação atribuídas a eles pelo gerenciador de *cluster*. Mais nós de trabalho reduzirão significativamente os tempos de ingestão e processamento de evidências.

No entanto, há um limite para o número de nós de trabalho que podem ser implementados em um servidor, mesmo aquele equipado com um microprocessador multicore de última geração.

Para obter o benefício total de um grande número de nós de trabalho, a versão baseada em nuvem do DFORC2 é necessária; o Kubernetes Cluster Manager pode distribuir tarefas de processamento de dados por várias máquinas na nuvem.

3 EXTRAÇÃO DE DADOS (ANÁLISE DE MÍDIAS DE DESTINO)

Para a extração de dados, deve-se seguir uma ordem de investigação. A primeira etapa em qualquer processo forense é a validação de todo o hardware e software, para garantir que funcionem corretamente. As organizações devem validar cada software e hardware antes de usá-los, assim como devem testar novamente após qualquer atualização, patch ou reconfiguração.

Quando a plataforma forense do perito está pronta, ele duplica os dados forenses fornecidos na solicitação de perícia e verifica sua integridade. Esse processo pressupõe que a aplicação da lei já obteve os dados por meio de um processo legal apropriado e criou uma imagem forense.

Uma imagem forense é uma cópia *bit* a *bit* dos dados existentes na mídia original, sem acréscimos ou exclusões. Também se presume que o perito forense recebeu uma cópia de trabalho dos dados apreendidos. Se os peritos obtiverem evidências originais, eles precisam fazer uma cópia de trabalho e proteger a cadeia de custódia do original.

Os peritos certificam-se de que a cópia em sua posse está intacta e inalterada. Eles normalmente fazem isso verificando um *hash* ou uma impressão digital das evidências. Se houver algum problema, os peritos consultam o solicitante sobre como proceder.

Após a verificação de integridade dos dados a serem analisados, um plano é desenvolvido para extrair os dados. São organizados em relação à solicitação forense com perguntas claras. As ferramentas forenses permitem responder a essas perguntas selecionadas.

Os peritos têm ideias preliminares sobre o que procurar, com base na solicitação. Eles os adicionam a uma "Lista de objetivos de pesquisa", que é uma lista contínua de itens solicitados. Por exemplo, a solicitação pode fornecer o objetivo: "pesquisar pornografia infantil". A lista leva explicitamente a ajudar a enfocar o exame. À medida que desenvolvem novos objetivos, eles os adicionam à lista e, conforme eles os atendem, os marcam como "processados" ou "concluídos".

Para cada objetivos de pesquisa, os peritos extraem dados relevantes e marcam como processado. Adicionam qualquer coisa extraída a uma segunda lista chamada "Lista de dados extraídos". Os peritos perseguem todos os objetivos de pesquisa, adicionando resultados a essa segunda lista. Em seguida, eles passam para a próxima fase da metodologia, a identificação

4 RECUPERAÇÃO DE DADOS APAGADOS (SISTEMA DE ARQUIVOS)

A maneira mais comum de as pessoas perderem dados é excluindo acidentalmente um arquivo. Arquivos frequentemente perdidos dessa forma incluem documentos, imagens, histórico do navegador da web, e-mails, logs de bate-papo de mídia social, vídeos e arquivos relacionados ao trabalho. Quando os backups não existem, há de se usar ferramentas e a experiência dos profissionais para encontrar os dados perdidos e recuperar a maior parte ou a totalidade deles.

4.1 RECUPERAÇÃO FORENSE

Às vezes, os arquivos excluídos não são acidentais. Principalmente quando há uma perícia a respeito de um possível crime. Se há alguém envolvido em comportamento ilícito, é comum que se esforce para excluir qualquer evidência desse comportamento.

Nesses casos, os dados não são apenas excluídos, mas esforços adicionais são feitos para limpar completamente o dispositivo de armazenamento dos dados. Esses esforços podem incluir a reformatação de um disco rígido, reescrever novos dados sobre os dados antigos várias vezes ou até mesmo danificar intencionalmente o dispositivo de armazenamento

4.2 UNIDADES DANIFICADAS E COM FALHA

As unidades de armazenamento de dados são altamente suscetíveis a danos e falhas. Muitos discos rígidos padrão falham em menos de uma década, apenas com o uso normal. Além disso, danos de superaquecimento e picos de energia também são bastante comuns.

A recuperação de dados de dispositivos de armazenamento que foram fisicamente danificados ou degradados requer ferramentas e habilidades específicas.

Os peritos copiam o dispositivo que desejam examinar e trabalham na criação de uma imagem em outro sistema, instantânea e exata de todos os dados contidos na unidade original. Esse método permite que eles examinem os dados sem fazer nenhuma alteração na unidade. E se fizerem alterações na cópia, não haverá prejuízo, pois poderão fazer uma nova cópia do original.

Para a recuperação, o perito pode fazer a substituição de um disco rígido inteiro, caso esteja formatado, por exemplo, e preencher todos os blocos endereçáveis com zeros (*bytes* ASCII NUL). Porém, existem ferramentas de apagamento seguro de unidade, que são usadas como antiforense e que podem apagar arquivos e pastas específicos, sobrescrevendo-os, com finalidade de atingir uma alta taxa de eficiência quando usadas várias vezes na mesma unidade. Nesse ponto, não há como recuperar os dados sobrescritos.

4.3 PROBLEMAS: IDENTIFICAÇÃO E RECUPERAÇÃO

Para reconstruir arquivos excluídos dentro de um ambiente forense, três problemas fundamentais devem ser resolvidos por uma ferramenta de recuperação de arquivo excluído (DFR). Primeiro, os arquivos que foram excluídos devem ser identificados e localizados. Embora isso possa ser tão simples quanto digitalizar o diretório de entradas para uma chave específica (por exemplo, '0xE5' em Fat 32), pode, também, ser mais complexo.

Esse processo é fundamental para que qualquer ferramenta de recuperação funcione corretamente. Caso os arquivos não sejam devidamente identificados e localizados, não farão parte do processo de recuperação.

O segundo problema, do ponto de vista do sistema de arquivos, é que os dados a serem recuperados são latentes, e precisam do auxílio de uma ferramenta para recuperar os dados. Como acontece com a maioria das recuperações de dados, uma vez que os resultados dependem da saída de uma ferramenta particular, a ferramenta deve ser apresentada para operar corretamente (ou seja, recuperar arquivos corretamente).

O terceiro problema é que a incerteza, presente em qualquer esforço de recuperação, leva a um nível reduzido de confiança nas informações recuperadas. Especificamente com a recuperação de arquivo excluído, os dados recuperados podem ser misturados com dados de outros arquivos excluídos, arquivos alocados ou até mesmo de espaço não alocado.

4.4 RECUPERAÇÃO DE DADOS: TÉCNICA DE DATA CARVING

Data Carving é a técnica que possibilita a recuperação de arquivos apagados, realizada através da localização de assinaturas conhecidas, como, por exemplo, a identificação do tipo de arquivo em seus cabeçalhos.

4.5 FERRAMENTAS DE RECUPERAÇÃO

No mercado atual existem muitas ferramentas de recuperação. Aqui serão apresentadas algumas atuais, no momento da construção desse material.

4.5.1 Kernel para Linux Data Recovery

O software de recuperação de dados Kernel para Linux pode gerenciar a recuperação de arquivos de dados do Linux que estão danificados ou corrompidos pela corrupção do bloco descritor de grupo, bloco super ou tabela danificada. A ferramenta pode reparar qualquer coisa, incluindo as partições excluídas do Linux.

O aplicativo está disponível em três classes, cada versão é responsável pela recuperação de arquivos de dados de sistemas de arquivos Ext2, Ext3, ReiserFS e JFS. Essas partições danificadas complexas e sofisticadas podem ser facilmente verificadas pelo software com a ajuda de algoritmos inteligentes e dinâmicos que tornam a recuperação possível.

4.5.2 Disk Drill

O Disk Drill é uma ferramenta de recuperação de dados com foco na recuperação de dados em dispositivos de armazenamento dos mais diversos tipos.

4.5.3 System Rescue CD

É um sistema Linux projetado para recuperar dados após uma falha no sistema ou nos dados. Seu objetivo é fornecer uma abordagem simples para executar as tarefas de administração, como a criação e edição de partições do disco rígido.

Essa ferramenta é desenvolvida no SO Linux e pode recuperar sistemas e entre as suas utilidades pode-se encontrar uma ferramenta de remoção de vírus e *malware*, assim como restauração de backup, cópia de disco e solução de problemas de rede.

RESUMO DO TÓPICO 3

Neste tópico, você aprendeu:

- A análise de evidências digitais trabalha com os dados, em que a equipe responsável examina os dados adquiridos para identificar as informações probatórias que podem ser apresentadas ao tribunal. É a fase que trata de examinar, identificar, separar, converter e modelar dados para transformá-los em informações úteis.

- Existem problemas para reconstrução dos arquivos excluídos dentro de um ambiente forense, como os arquivos que foram excluídos devem ser identificados e localizados, os dados a serem recuperados são latentes, e precisam do auxílio de uma ferramenta para recuperar os dados e ainda a incerteza na recuperação, que leva a um nível reduzido de confiança nas informações recuperadas.

AUTOATIVIDADE

1 A maneira mais comum de as pessoas perderem dados é excluindo acidentalmente um arquivo. Arquivos frequentemente perdidos dessa forma incluem documentos, imagens, histórico do navegador da web, e-mails, logs de bate-papo de mídia social, vídeos e arquivos relacionados ao trabalho. Quando os backups não existem, há de se usar ferramentas e a experiência dos profissionais para encontrar os dados perdidos e recuperar a maior parte ou a totalidade deles. Sobre o Data Carving, assinale a alternativa CORRETA:

a) ( ) Data Carving é a técnica que possibilita a recuperação de arquivos apagados, realizada através da localização de assinaturas conhecidas, como por exemplo, a identificação do tipo de arquivo em seus cabeçalhos.
b) ( ) O carving de arquivos, porém, não recupera espaços alocados em um disco ou partição baseados na estrutura do arquivo e do seu conteúdo.
c) ( ) O método de carving tem pouca ou nenhuma utilidade nas análises forenses, pois faz com que dados sejam escondidos ou deletados.
d) ( ) Data carving é um processo de fragmentação de arquivos, na ausência de metadados de sistema de arquivos.

2 Para a extração de dados, deve-se seguir uma ordem de investigação. A primeira etapa em qualquer processo forense é a validação de todo o hardware e software, para garantir que funcionem corretamente. As organizações devem validar cada software e hardware antes de usá-los, assim como devem testar novamente após qualquer atualização, patch ou reconfiguração. Sobre as ferramentas de análise de mídias, classifique V para as sentenças verdadeiras e F para as falsas:

( ) O Sleuthkit é um framework de ferramentas voltadas à análise forense computacional, que somente aceita a participação de ferramentas livres.
( ) O Autopsy é uma interface de trabalho do Sleuthkit, bem visual e mais automatizada que trabalha com a análise do HD, automaticamente reconhecendo as partições do disco rígido.
( ) O Encase é uma ferramenta de análise em que se consegue identificar o autor da utilização do disco rígido através do acesso a servidores de instalação de aplicativos, chaves de registro e backup de sistema, ele permite identificar endereço de rede de servidores acessados através da Internet e os dados de autenticação (usuário e senha) deles.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – V.
b) ( ) F – F – F.
c) ( ) V – V – F.
d) ( ) V – F – F.

3 Às vezes, os arquivos excluídos não são acidentais. Principalmente quando há uma perícia a respeito de um possível crime. Se há alguém envolvido em comportamento ilícito, é comum que se esforce para excluir qualquer evidência desse comportamento, e é aí que entra o papel do perito forense de recuperar essas evidências. Sobre a preservação das evidências na investigação, analise as sentenças a seguir:

I- Sempre que há uma perícia a respeito de um possível crime, são feitos muitos esforços para limpar completamente o dispositivo de armazenamento dos dados. Esses esforços podem incluir a reformatação de um disco rígido, reescrever novos dados sobre os dados antigos várias vezes ou até mesmo danificar intencionalmente o dispositivo de armazenamento.
II- Existem ferramentas de apagamento seguro de unidade, que são usadas como antiforense e que podem apagar arquivos e pastas específicos, sobrescrevendo-os, com finalidade de atingir uma alta taxa de eficiência quando usadas várias vezes na mesma unidade.
III- A fase de coleta forense é uma cópia *bit* a *bit* dos dados existentes na mídia original, porém com alguns acréscimos ou exclusões.

Assinale a alternativa CORRETA:

a) ( ) Somente a sentença I está correta.
b) ( ) As sentenças II e III estão corretas.
c) ( ) As sentenças I e II estão corretas.
d) ( ) Somente a sentença III está correta.

4 Quando os backups não existem, há de se usar técnicas e a experiência dos profissionais para encontrar os dados perdidos e recuperar a maior parte ou a totalidade deles. Tendo isso em mente, disserte sobre o que é data carving.

5 Quais os problemas para reconstrução de arquivos recuperados?

RECUPERAÇÃO DE DADOS: TÉCNICA DE DATA CARVING

1 INTRODUÇÃO

"Carving é feito em um disco quando o arquivo está em um espaço não alocado do sistema de arquivos" (MEROLA, 2008, p. 4). O carving não é identificado por conta da falta de informação sobre sua alocação, ou, ainda, ao se fazer capturas de rede em que se extrai os arquivos do tráfego capturado utilizando-se as mesmas técnicas.

Infelizmente, o carving é muito menos eficaz para recuperar arquivos de despejos de memória. Muitos sistemas operacionais, incluindo o Windows, tentam evitar a fragmentação de arquivos no disco, o que torna o entalhe linear relativamente eficaz.

Assim como um disco rígido é dividido em setores, a memória é dividida em páginas. Essas estruturas são alocadas de *pools* de memória. Um *pool* de memória é uma área de memória dinâmica alocada pelo kernel onde ele armazena estruturas administrativas. O tipo de uma estrutura de *pool* pode ser determinado por meio de um número mágico de quatro bytes, chamado de *tag pool* (por exemplo, Proc, Obtb e MmCa).

Os dados na memória mostram muita fragmentação. Quando um fragmento com blocos consecutivos de dados de um arquivo é definido, ele fica separado em páginas consecutivas da memória. É possível que o gerenciador de memória carregue apenas partes de um arquivo na memória. Se um bloco de um arquivo mapeado na memória ainda não foi carregado, isso também é definido como um fragmento

2 DATA CARVING EM MEMÓRIA

Data carving é uma técnica amplamente utilizada na recuperação de dados e na perícia digital. Ao usar carving, essencialmente é realizada uma varredura de baixo nível da mídia (ou na memória ou na própria rede) em busca de vários artefatos, procurando assinaturas (sequências específicas de *bytes*), características desse ou daquele tipo de dados.

2.1 FERRAMENTAS DE DATA CARVING

Existem vários softwares no mercado que recuperam arquivos apagados de forma automática. Eles recuperam arquivos baseando-se na estrutura e não na assinatura, o que é muito interessante para a perícia.

2.1.1 Scalpel

Uma das ferramentas de data carving é o Scalpel, que é uma ferramenta de código aberto, a qual analisa o bloco do armazenamento do banco de dados e identifica os arquivos deletados e os recupera.

O Scalpel usa uma técnica de carving linear, eficaz apenas para arquivos contíguos. Quando um arquivo está fragmentado, os algoritmos de carving linear falham em reconstruir o arquivo e o arquivo ficará incompleto após o primeiro fragmento. Algoritmos de carving inteligente podem ser capazes de recuperar arquivos fragmentados, conforme descrito por Garfinkel (2007).

A ferramenta analisa a imagem e retorna com o descritivo, apresentando os tipos de arquivos identificados que foram recuperados e, também, a sua quantidade. A pasta em que é armazenada a saída, com as informações coletadas, apresenta os resultados divididos de acordo com seu formato de arquivo e, também, se apresenta um registro com a descrição dos resultados. Porém, acontece de alguns arquivos serem completamente recuperados, enquanto outros podem não ser recuperados.

2.1.2 Foremost

A ferramenta Foremost é muito similar à Scalpel, pois utiliza o mesmo método Data carving de arquivos. É possível adaptar a vários tipos de formatos, ajustando a ferramenta. Após as configurações serem finalizadas, pode-se descobrir os parâmetros que podem ser utilizados na análise das imagens.

O arquivo de configuração pode ser utilizado, porém não é o obrigatório, e a ferramenta pode ser usada sem especificações e com qualquer formato, somente informando-se o local em que a imagem está localizada para análise. Os resultados ficam armazenados de forma independente em pastas de acordo com seu formato específico. O relatório de registros é criado e são organizados seus dados de maneira visual.

2.2 ESTRUTURAS DE MAPEAMENTO DE ARQUIVO ALOCADO

Usando o algoritmo de carving é possível identificar as estruturas de processo em execução, ocultas e encerradas. Os processos em execução e ocultos contêm indicadores específicos contidos na tabela de objetos.

Os processos que foram encerrados têm esses ponteiros definidos como zero. Os arquivos compartilhados são carregados pelo kernel e podem ser acessados por qualquer processo em execução. Percorrendo a tabela de objetos é possível reconstruir arquivos privados; arquivos que só podem ser acessados pelo processo que mapeou o arquivo.

2.3 ESTRUTURAS DE MAPEAMENTO DE ARQUIVO NÃO ALOCADAS

Quando os identificadores de arquivo são fechados por processos, os dados do arquivo ainda podem ser retidos na memória. Eles não podem ser vinculados às estruturas do processo, porque os ponteiros para as estruturas do arquivo mapeado são definidos como zero quando o identificador é fechado.

Essa situação é semelhante a rastros deixados por arquivos excluídos em um sistema de arquivos. O alto grau de fragmentação da memória torna mais difícil reconstruir a ordem lógica das páginas, portanto, determinar essa ordem olhando a Tabela de páginas pode possibilitar a reconstrução de arquivos.

O carving pode ser usado para estruturas relacionadas a esses arquivos. Os arquivos fechados às vezes podem ser recuperados pela criação de estruturas de Área de Controle e Tabela de Página. A primeira estrutura pode fornecer informações detalhadas sobre o arquivo, como o nome do arquivo. Ele também contém um ponteiro para a Tabela da Página.

Como é possível que uma Tabela de Página ainda esteja presente na memória depois que uma Área de Controle foi sobrescrita, o carving para Tabelas de Página pode ser útil. Depois que a ordem das páginas foi reconstruída e o arquivo extraído, às vezes é possível determinar o tipo de arquivo olhando as informações do cabeçalho. Uma ferramenta comumente usada para isso é o comando de arquivo do Unix.

2.4 PÁGINAS DE ARQUIVO NÃO IDENTIFICADAS

Ainda é possível que as páginas usadas anteriormente para armazenar dados de arquivo mapeado não tenham mais estruturas apontando para elas. Os dados do arquivo ainda estão presentes na página e podem ser identificados combinando o *hash* MD5 dos dados da página com *hashes* de blocos de 4K de arquivos no disco rígido.

Os últimos blocos de arquivos são preenchidos até 4K (tamanho da página da memória) com zeros antes de calcular o *hash*. A correspondência de *hashes* é genérica e não requer conhecimento sobre a estrutura da memória.

Há razões para não usar esse método primeiro, pois os *hashes* correspondentes requerem acesso ao sistema de arquivos. Outro problema é que essa técnica não vincula informações sobre processos para os arquivos e, ainda, os arquivos que foram alterados na memória não serão reconhecidos.

3 DATA CARVING EM TRÁFEGO DE REDES

Informações sobre redes às quais os dispositivos se conectam e os padrões de comunicação desses dispositivos podem fornecer aos investigadores forenses uma rica fonte de informações.

Beverly *et al*. (2011) afirmam que o conjunto de endereços de protocolo da Internet (IP) de origem que um dispositivo adquiriu ao longo do tempo pode fornecer pistas sobre seus pontos de conexão de rede física e padrões de mobilidade.

Os endereços de destino dos pacotes IP podem fornecer uma imagem dos sites mais visitados, das transferências de arquivos ou troca de e-mail. Como resultado, a prática forense comumente vasculha o dispositivo de um sujeito em busca de informações de rede e apresentar essas informações a analistas e investigadores.

Os endereços Ethernet Media Access Control (MAC) também podem ter um valor forense significativo. Os três primeiros octetos de um MAC Ethernet são atribuídos a fornecedores de equipamentos específicos e podem ser usados para inferir informações sobre o equipamento usando um endereço MAC específico. Mas os endereços MAC de outras máquinas na sub-rede do dispositivo do sujeito também podem ser reveladores, pois podem ser usados para determinar a localização física de um dispositivo. O simples fato de um computador ter sido associado a uma rede física (com ou sem fio) também pode ser usado para inferir a associação em uma organização ou o acesso a um local físico.

Para uma análise de tráfego de rede há que analisar aspectos mais profundos, pois essa análise depende de assinaturas de rede binárias de camada inferior, como estruturas de dados de pacote e soquete. Essas estruturas são criadas na memória e mantidas pelo sistema operacional durante o curso normal da atividade da rede. No entanto, as estruturas de rede não estão confinadas a imagens de memória, pois são invariavelmente gravadas em armazenamento fixo de um computador.

Além disso, programas de rede (clientes e servidores de domínio, clientes e servidores DHCP) podem usar estruturas de dados de rede binárias ao armazenar configurações ou resultados de cache no sistema de arquivos, tornando esses arquivos fontes de dados úteis.

A comunicação entre os dispositivos da rede é facilitada por meio de protocolos, ou seja, mecanismos para identificar e estabelecer conexões, regras de formatação e convenções especificadas para transferência de dados.

Para Chapman (2016), os dados da rede podem ser analisados e o tráfego da rede segregado por tipo, usando um software específico. Os analisadores de protocolo projetados para análise de pacotes são chamados de analisadores de pacotes (farejadores de pacotes ou analisadores de rede). Essas ferramentas de software interceptam e registram o tráfego de rede que atravessa uma rede digital ou parte de uma rede por meio do processo de captura de pacotes. Os pacotes capturados podem, então, ser analisados pela decodificação dos dados brutos dos pacotes e visualizados por meio da exibição de vários campos para interpretar o conteúdo.

Ao colocar um controlador de interface de rede com fio (NIC) ou controlador de interface de rede sem fio (WNIC) em modo promíscuo, todo o tráfego de rede recebido pode ser passado para a unidade de processamento central (CPU) em vez de apenas aqueles quadros que o controlador está especificamente programado para receber.

Disponível na maioria das distribuições Linux, o Berkeley Packet Filter (BPF) oferece suporte à filtragem de pacotes, como receber apenas os pacotes que iniciam uma conexão TCP. Como o BPF retorna apenas os pacotes que passam pelo filtro, os pacotes irrelevantes não precisam ser copiados do sistema operacional para o kernel para serem processados, melhorando significativamente o desempenho.

Um aprimoramento do BPF original é o BPF estendido (eBPF), que oferece suporte não apenas para saltos para a frente, mas também para trás, permitindo assim os loops. Usando armazenamentos de dados globais chamados mapas, o eBPF também pode ser usado para agregar estatísticas de eventos.

Em um ambiente de rede comutada, a visibilidade de um farejador de pacote é limitada à porta a que está conectada. Existem quatro maneiras principais de capturar o tráfego de um dispositivo de destino:

- espelhamento de porta (*port spanning*);
- *hubbing out*;
- usando um tap;
- e ARP *cache poisoning* (*spoofing* ARP).

A escolha da técnica depende do cenário:

- O primeiro é uma opção apenas se há acesso à linha de comando ou à interface de gerenciamento baseada na web do switch, no qual o computador de destino está localizado. O switch suporta espelhamento de porta e tem uma porta vazia na qual se pode conectar o sniffer.
- O segundo precisa de acesso físico ao switch, ao qual o dispositivo de destino está conectado.
- O terceiro requer uma ferramenta de *hardware* especial (tap de rede) para ser conectado à rede.
- E o quarto requer que sejam coletadas informações, como o endereço IP do sistema analisador, o sistema remoto ao qual é necessário capturar o tráfego e o roteador do qual o sistema remoto está *downstream*.

Os pacotes de rede contêm informações úteis sobre as atividades da rede e sua análise ajuda a reunir e relatar estatísticas de rede e depurar as comunicações cliente-servidor.

Os arquivos de captura de pacote de rede armazenam muitas informações sobre a atividade do usuário online que podem ser úteis na análise forense da rede, como sites visitados e o tempo gasto para navegar neles, tentativas de login, credenciais, downloads ilegais de arquivos, abuso de propriedade intelectual, bem-sucedidos e malsucedidos fluxos, fluxos e sessões

RESUMO DO TÓPICO 4

Neste tópico, você aprendeu:

- Existem dois tipos de data Carving: de memória e de tráfego de redes.

- Quando os identificadores de arquivo são fechados por processos, os dados do arquivo ainda podem ser retidos na memória. Eles não podem ser vinculados às estruturas do processo porque os ponteiros para as estruturas do arquivo mapeado são definidos como zero quando o identificador é fechado, mas podem ser recuperados com data Carving.

- Os dados de uma rede podem ser analisados e o tráfego da rede segregado por tipo, usando um software específico, os analisadores de pacotes (farejadores de pacotes ou analisadores de rede). Essas ferramentas de software interceptam e registram o tráfego de rede que atravessa uma rede digital ou parte de uma rede por meio do processo de captura de pacotes.

- Os pacotes capturados podem, então, ser analisados pela decodificação dos dados brutos dos pacotes e visualizados por meio da exibição de vários campos para interpretar o conteúdo.

AUTOATIVIDADE

1 Sobre o Data Carving de tráfego de redes, assinale a alternativa CORRETA:

a) ( ) Informações sobre redes às quais os dispositivos se conectam e os padrões de comunicação desses dispositivos não fornecem aos investigadores forenses fonte de informações, devendo ser evitados.
b) ( ) Os endereços de destino dos pacotes IP podem fornecer uma imagem dos sites mais visitados, das transferências de arquivos ou troca de e-mail.
c) ( ) A prática forense, em geral, não vasculha dispositivos de um suspeito em busca de informações de rede, pois não poderá apresentar essas informações a analistas e investigadores, muito menos no julgamento.
d) ( ) Para uma análise de tráfego de rede há, são dispensadas assinaturas de rede binárias de camada inferior, como estruturas de dados de pacote e soquete.

2 Sobre as técnicas de recuperação com o Data Carving de memória, classifique V para as sentenças verdadeiras e F para as falsas:

( ) Páginas usadas anteriormente para armazenar dados de arquivo mapeado podem não ter mais estruturas apontando para elas. Os dados do arquivo ainda estão presentes na página e podem ser identificados combinando o *hash* MD5 dos dados da página com *hashes* de blocos de 4K de arquivos no disco rígido.
( ) Se os identificadores de arquivo são fechados por processos, os dados do arquivo ainda podem ser retidos na memória. Eles não podem ser vinculados às estruturas do processo, porque os ponteiros para as estruturas do arquivo mapeado são definidos como zero quando o identificador é fechado.
( ) Rastros deixados por arquivos excluídos em um sistema de arquivos não podem mais ser recuperados, pois o alto grau de fragmentação da memória torna impossível a sua reconstrução.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – V.
b) ( ) F – F – V.
c) ( ) V – V – F.
d) ( ) V – F – F.

3 Sobre a preservação das evidências na investigação, analise as sentenças a seguir:

I- O Scalpel analisa o bloco do armazenamento do banco de dados e identifica os arquivos deletados e os recupera; usa uma técnica de carving linear, eficaz apenas para arquivos contíguos. Quando um arquivo está fragmentado, os algoritmos de carving linear falham em reconstruir o arquivo e o arquivo ficará incompleto após o primeiro fragmento.
II- O Scopel é uma ferramenta tão robusta que consegue recuperar todos os arquivos apagados ou danificados. Os dados encontrados são armazenados e os resultados são salvos separados por pastas de acordo com os formatos de arquivos.
III- A ferramenta Foremost analisa a imagem e retorna com o descritivo, apresentando os tipos de arquivos identificados que foram recuperados e, também, a sua quantidade. Porém, infelizmente, a ferramenta não gera relatório de registro dos arquivos.

Assinale a alternativa CORRETA:

a) ( ) Somente a sentença I está correta.
b) ( ) As sentenças II e III estão corretas.
c) ( ) As sentenças I e II estão corretas.
d) ( ) Somente a sentença III está correta.

4 Qual a diferença do Data Carving de memória e de tráfego de redes?

5 Quais as formas de captura de tráfego de rede de um dispositivo de destino?

TÉCNICAS COMPLEMENTARES

1 INTRODUÇÃO

As investigações forenses por computador usam uma combinação de técnicas e conhecimento especializado. Algumas técnicas comuns incluem o seguinte:

- Esteganografia reversa: a esteganografia é uma tática comum usada para ocultar dados dentro de qualquer tipo de arquivo digital, mensagem ou fluxo de dados. Especialistas em computação forense revertem uma tentativa de esteganografia analisando o hashing de dados que o arquivo em questão contém. Se um cyber criminoso ocultar informações importantes dentro de uma imagem ou outro arquivo digital, pode parecer o mesmo antes e depois para o olho não treinado, mas o *hash* subjacente ou sequência de dados que representa a imagem mudará.
- Forense estocástica: os investigadores analisam e reconstroem a atividade digital sem o uso de artefatos digitais. Artefatos são alterações não intencionais de dados que ocorrem em processos digitais. Os artefatos incluem pistas relacionadas a um crime digital, como alterações nos atributos do arquivo durante o roubo de dados. A perícia estocástica é frequentemente usada em investigações de violação de dados em que o invasor é considerado um invasor, que pode não abandonar artefatos digitais.
- Análise de *cross-drive*: esta técnica correlaciona e cruza informações encontradas em várias unidades de computador para pesquisar, analisar e preservar informações relevantes para uma investigação. Os eventos que levantam suspeitas são comparados com informações em outras unidades para procurar semelhanças e fornecer contexto. Isso também é conhecido como detecção de anomalias.
- Análise ao vivo: com essa técnica, um computador é analisado de dentro do sistema operacional enquanto o computador ou dispositivo está em execução, usando ferramentas de sistema no computador. A análise analisa os dados voláteis, que geralmente são armazenados em cache ou RAM. Muitas ferramentas usadas para extrair dados voláteis exigem que o computador esteja em um laboratório forense para manter a legitimidade de uma cadeia de evidências.
- Recuperação de arquivo excluída: essa técnica envolve a busca em um sistema de computador e memória por fragmentos de arquivos que foram parcialmente excluídos em um lugar, mas deixam rastros em outro lugar na máquina. Isso às vezes é conhecido como carving de arquivo ou carving de dados.

2 ESTERILIZAÇÃO DE MÍDIAS

Um método de esterilização de mídias é uma maneira específica pela qual um programa de destruição de dados ou destruidor de arquivos sobrescreve os dados em um disco rígido ou outro dispositivo de armazenamento.

A maioria dos programas de destruição e fragmentação de dados oferece suporte a vários métodos de sanitização de dados. Esses métodos também são frequentemente chamados de métodos de eliminação de dados, algoritmos de eliminação e padrões de eliminação de dados.

A limpeza e esterilização de discos é o conjunto de técnicas utilizadas para eliminar as informações armazenadas em um disco.

Para Reis (2019), o funcionamento do processo de formatação de um arquivo, ou mesmo sua exclusão, acontece com a informação do Sistema Operacional ao sistema de arquivos que o espaço em disco reservado para armazenar o conteúdo daquela partição do disco está liberado e pode ser reaproveitado. Porém, os dados continuam gravados em disco e podem ser recuperados utilizando técnicas específicas para recuperação de dados, como o Data Carving. Os dados apagados se mantêm no disco até que o Sistema Operacional os sobrescreva.

O projeto para aumento no desempenho do sistema de arquivos procura reduzir a realização de movimentos do cabeçote do disco, o que leva à organização de dados lado a lado no armazenamento do disco, reduzindo a fragmentação dos arquivos, ou seja, quanto mais recente foi executada a exclusão do arquivo, maior é a chance de recuperação.

Existem no mercado atual muitos dispositivos e forenses que auxiliam na realização do processo de espelhamento e cópia de dados, como sistemas que definem o acesso somente leitura das informações em discos rígidos e para duplicação. Os bloqueadores de escrita em disco rígido são os sistemas mais usados, pois ficam conectados entre o material questionado e o computador, tendo garantia, certificada em hardware, não haverá dado gravado, somente precisando usar um programa próprio para a cópia do disco. Já os duplicadores forenses são equipamentos muito mais avançados que bloqueiam a escrita como cópias para outros discos rígidos, por técnica de espelhamento ou imagem.

Na verdade, existem várias maneiras de apagar completamente um disco rígido, mas usar um software de destruição de dados é o mais fácil e ainda permite que o disco rígido seja usado novamente.

2.1 APAGAMENTO SEGURO

O Apagamento seguro é o nome dado a um conjunto de comandos disponíveis no *firmware* em discos rígidos com base em PATA e SATA.

Usar o apagamento seguro para apagar os dados de um disco rígido geralmente é considerado a melhor maneira de fazer isso porque a ação é realizada a partir da própria unidade, o mesmo *hardware* que gravou os dados em primeiro lugar. A técnica Wipe é uma representação de um método de apagamento seguro.

2.2 WIPE

Wipe é um processo para apagar dados no disco rígido, *bit* a *bit*, de forma que substitua toda a área reservada para alocação de um arquivo. Os dados armazenados nos setores apagados são substituídos por zeros ou números aleatórios. Isso garante que não há possibilidade de dados serem recuperados por descuido ou sem intenção.

O *Department of Defense* Americano desenvolveu um método de sanitização de mídia, conhecida como DoD 5220.22-M, que consiste em realizar três formas distintas de gravação nos bytes endereçáveis do disco:

- Gravar "zeros" (0x00) e verificar o que foi escrito.
- Gravar "uns" (0xff) e verificar o que foi escrito.
- Gravar valores aleatórios e verificar o que foi escrito.

Algumas técnicas de wipe sobrescrevem toda a área proposta com caracteres específicos por até sete vezes. Porém, para o NIST (2006), a maioria das mídias atuais podem ser sanitizadas com apenas uma sobrescrita. O grande problema é que a técnica Wipe pode ser utilizada para limpeza de discos como pode ser usada como um método antiforense para eliminar vestígios de um crime.

2.3 GUTMANN

O método Gutmann, desenvolvido por Peter Gutmann em 1996, usa um caractere aleatório, ao invés de apenas o zero usado em outras técnicas, aplicando um padrão complexo de substituição dos dados. Ele grava um total de 35 passos de substituição.

Esse método foi desenvolvido no final do século XX. Os discos rígidos em uso naquela época usavam métodos de codificação diferentes dos que são usados hoje, portanto, a maioria das passagens que esse método executa são completamente inúteis para discos rígidos modernos. Sem saber exatamente como cada disco rígido armazena os dados, a melhor maneira de apagá-los é usar padrões aleatórios.

Porém, cada disco rígido usa apenas um método de codificação para armazenar dados, então apesar de o método de Gutmann não ser adequado às mídias atuais, enquanto técnica, pode-se perceber que escrever dados aleatórios é tudo o que realmente precisa para ser feito.

2.4 WRITE ZERO

O método de sanitização de dados Write Zero é geralmente implementado com apenas um passo: escreve um zero. Esse método pode ser implementado com a inclusão de uma validação após a primeira vez que for executado, escrevendo caracteres diferentes ou iguais a zero (este últimos com várias execuções).

Algumas técnicas de sanitização de dados alteram seus dados com caracteres randômicos. A técnica Write Zero usa somente zeros para sua implementação.

A sua principal característica em relação a técnicas de dados randômicos é que não importa somente o caractere que está sendo definido, mas sua eficiência na sobrescrita dos dados. Se a técnica Write Zero é utilizada, com certeza será feita a verificação dos dados sobrescritos e, provavelmente, a recuperação desses dados será bem reduzida em relação à técnica de dados randômicos (ou aleatórios).

Algumas técnicas têm uma maior privacidade que outras, ou seja, se o algoritmo de recuperação identifica que foi feita a técnica de substituição por zeros, o exame dos dados será muito mais eficiente na restauração do que se não for percebido o tipo de alteração feita.

Outra razão para todos os outros métodos de limpeza de dados é que algumas organizações querem provar que suas informações estão sendo apagadas de uma maneira específica, o que provavelmente evita a recuperação, então eles usam um determinado método de limpeza de dados com certos parâmetros para todas as suas necessidades de limpeza de dados.

3 SANITIZAÇÃO DE TRÁFEGO DE REDE

Galvão (2015) cita a norma NBR ISO/IEC 27002:2005, a qual afirma que a:

> segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos (ABNT, 2005b *apud* GALVÃO, 2015, s.p.).

Para compreender quais controles e ferramentas podem ser utilizados, é preciso compreender os princípios de segurança:

- Identificação – reconhecimento da entidade – conhecer a origem e dados que afirmem quem é essa entidade.
- Autenticação – averiguar e solicitar uma comprovação para certificar que as informações obtidas na identificação são verdadeiras.
- Autorização – consentir e permitir que a entidade realize uma ação solicitada por ela.
- Não repúdio – não dar chances que determinada entidade negue que foi ela quem realizou um ato específico, ou seja, através da autenticação e da identificação pode-se saber quem realizou tal ato e poder provar isso.

Os tipos de ataque que um sistema pode enfrentar também devem ser compreendidos antes de se definir modelos, conceitos e ferramentas de segurança da informação.

Galvão (2015) cita:

- Interrupção – quando ocorrer este tipo de ataque, a informação ficará indisponível, isto é, ninguém mais conseguirá acessá-la.
- Interceptação – neste tipo de ataque, informações confidenciais poderão ser visualizadas por pessoas sem permissão e autorização para visualizá-las.
- Fabricação – neste tipo de ataque, o indivíduo que cometê-lo irá alterar a autenticidade da informação, isto é, poderá se fazer passar por outra pessoa.

Para a limpeza do tráfego de rede, é fundamental ter todos os conceitos compreendidos.

3.1 FERRAMENTA DE SANITIZAÇÃO

Metadefender Cloud: ferramenta de segurança gratuita para verificar vulnerabilidades e sanitizar arquivos.

A maioria dos malware encontrados nos computadores é resultado de anexos de e-mail não detectados, abertos pelo usuário sem perceber. O *Metadefender Cloud* remove este tipo de malware. Deve-se carregar o arquivo afetado na ferramenta; o Metadefender irá então higienizar o conteúdo e tornar um arquivo mais seguro para download. O recurso atende aos formatos de arquivo mais comuns, como .DOC, PPT, .XLS, PDF, .JPG, .BMP e .SVG. Contém um processo de CDR, que ativa 90 mecanismos de sanitização de dados (CDR), suporta ainda animação.

O processo de "sanitização" é uma peça-chave no tratamento de dispositivos para evitar "infecções" que podem colapsar as redes das companhias, causando uma série de prejuízos incalculáveis.

Algumas tecnologias e cuidados que devem ser seguidos para proteger o tráfego de dados e não colocar em risco a segurança das redes:

- VPN: tecnologia Virtual Private Network (VPN), é uma rede privada virtual, ou uma conexão criptografada pela Internet de um dispositivo a uma rede. A conexão criptografada ajuda a garantir que os dados confidenciais sejam transmitidos com segurança. Ele evita que pessoas não autorizadas espionem o tráfego e permite que o usuário conduza o trabalho remotamente. A tecnologia VPN é amplamente utilizada em ambientes corporativos.
- Criptografia de Dados: a criptografia de dados deve ser usada para a proteção do HD. As técnicas de codificação protegem informações confidenciais de ameaças e exploração por malware e acesso não autorizado de terceiros.
- Segundo Fator de Autenticação: o controle do acesso, através de uma senha por si só, não garante a proteção. Pode-se usar ferramentas de segundo fator de autenticação como opção de garantia e controle de acesso à rede, protegendo informações sigilosas.
- DLP: Data Loss Prevetion (DLP), ou Prevenção de Perda de Dados, analisa os arquivos acessados por um usuário e verifica todos os logs de acesso. É um processo de classificação da informação, que pode ter uma complexidade maior, porém tem como objetivo gerar um registro confiável dos acessos, para garantir o rastreamento e a verificação da origem de um acesso.
- Firewall: o firewall é um processo de proteção através de hardware, software ou os dois, que através de um conjunto de regras, analisa o tráfego da rede, podendo verificar ou definir os dados que entram ou saem dela. Os firewalls conseguem executar funções de segurança, política e gerenciamento de ferramentas.

Os riscos de segurança à investigação precisam ser minimizados a fim de evitar alterações e ataques antiforenses a qualquer momento do processo de perícia

LEITURA COMPLEMENTAR

A INTERNET COMO INSTRUMENTO UTILIZADO PELA PERÍCIA PARA RESOLUÇÃO DE CRIMES

Débora Aparecida Miranda Benetti
Rodrigo Plotze

INTRODUÇÃO

A internet hoje é um dos instrumentos mais utilizados pelas pessoas do mundo todo, proporcionando a resolução de vários problemas. Hoje, as Fontes Abertas já fazem parte das nossas vidas. Tais fontes de informações estão disponíveis ao público sem restrição ao seu acesso. Jornais, bibliotecas digitais, livros estão abertos sem nenhuma dificuldade de acesso. Vivenciamos, cada vez mais, a privacidade das pessoas sendo invadida com muita facilidade, obrigando, assim, que a polícia busque formas e modos para investigar e solucionar problemas. O Código Penal atual (BRASIL, 2019), de forma muito tímida, apresenta alguns artigos para punir condutas criminosas envolvendo o acesso à internet.

Este artigo tem como objetivo apresentar algumas definições sobre computação forense e os aspectos associados ao modo de investigação. Além disso, são relatadas como as investigações digitais em fontes abertas podem ser importantes para a prisão de determinados indivíduos, bem como para a identificação de suspeitos, testemunhas e foragidos.

A internet possibilita que a própria polícia, juntamente com outros meios de provas, solucione vários casos. Este artigo apresentará também alguns crimes que ocorreram na internet, seja no Brasil ou em outros países, descrevendo suas soluções e investigações, através de vários instrumentos, sejam e-mails, *pendrive*, redes sociais, entre outros, como, por exemplo, instrumentos como esteganografia. Por fim, serão citados dados estatísticos do CERT.br (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil).

COMPUTAÇÃO FORENSE

O objetivo da computação forense segundo os autores Pedro Monteiro da Silva Eleutério e Marcio Pereira Machado (2010, p. 16):

> [...] A Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhes validade probatória em juízo.

Ainda segundo os autores já citados, podemos elencar os cinco principais exames forenses de informática de forma sucinta. O primeiro deles constitui-se pelos exames e procedimentos em locais de crime de informática, que consiste principalmente no mapeamento, identificação e correta preservação dos equipamentos computacionais, a fim de permitir melhor seleção do material apreendido, para serem examinados posteriormente em laboratório.

Também, em segundo, há os exames em dispositivos de armazenamentos computacionais: são os exames periciais mais solicitados na Computação Forense e consistem basicamente em analisar arquivos, sistemas e programas instalados em discos rígidos, CD, DVD, Blu-ray, *pendrives* e outros dispositivos de armazenamentos digitais de dados. Em terceiro, podemos citar os exames em aparelhos de telefone celular, que compreendem basicamente a extração dos dados desses aparelhos, a fim de recuperar e formalizar as informações armazenadas em suas memórias (lista de contatos, ligações, fotos, mensagens etc.), de acordo com as necessidades de cada caso.

O quarto tipo de exame forense que mencionaremos são os exames em sites da internet, que consistem principalmente na verificação de cópia de conteúdo existente na internet, em *sites* e servidores remotos dos mais variados serviços. Além disso, trata-se da investigação do responsável por um domínio de um *site* e/ou endereço IP. Por fim, o quinto tipo, os exames em mensagens eletrônicas (e-mails): corresponde basicamente à análise das propriedades das mensagens eletrônicas, a fim de identificar hora, data, endereço IP e outras informações do remetente da mensagem.

Assim, concluímos que o computador é um instrumento que também é utilizado para a prática de vários crimes em todas as suas dimensões.

CRIMES SOLUCIONADOS NA INTERNET E REDES SOCIAIS

O primeiro caso que podemos destacar ocorreu no próprio Facebook: um assaltante foi preso no México por causa de informações postadas no Facebook. A prisão foi bem-sucedida porque o criminoso adicionou como amigo um integrante do Departamento de Defesa norte-americano (BBC Brasil, 2009).

Um dos cem criminosos mais procurados da Itália foi preso em Isola Capo Rizzuto, graças a seu "amor" pelo Facebook. "Segundo a polícia, a detenção só foi possível porque Manfredi costumava acessar sua página no Facebook de seu esconderijo. Ele usava o apelido de *Scarface*, apelido do personagem mafioso Tony Montana, interpretado por Al Pacino em filme de 1983" (G1, 2010).

Robert Powell foi preso pelo assassinato do seu amigo ao postar frases no Myspace com mensagem de "Descanse em paz" antes de o fato ter chegado ao conhecimento da polícia (SOUZA, 2010).

A polícia suíça apreendeu 1,2 toneladas de maconha com o auxílio do *software* de imagens da Google Earth. A investigação resultou na prisão de 16 pessoas e na localização da plantação, medindo aproximadamente 7.500 metros quadrados, que estava camuflada em uma plantação de cereais (G1, 2009).

O colombiano Juan Carlos Ramírez Abadía foi preso em São Paulo. Os delegados da Polícia Federal ficaram intrigados com a quantidade de imagens da gatinha japonesa *Hello Kitty* que ele tinha no seu computador.

Na verdade, a gatinha *Hello Kitty* possuía mensagem de voz e textos escondidos na sua imagem. Tal técnica é conhecida como esteganografia. A Al Qaeda utilizou essa técnica para preparar os atentados em 2001 (FOLHA DE SÃO PAULO, 2019).

A nossa antiga primeira-dama, Marcela Temer, também foi vítima desses problemas na Internet. "Silvonei José de Jesus Souza pediu R$ 300 mil para não vazar fotos íntimas e áudios de Marcela" (G1, 2016).

Pendrive USB pode ter infectado usina nuclear russa com devastador Stuxnet

O Stuxnet, para quem não conhece, é a primeira 'super-arma cibernética': um worm criado pelos governos dos EUA e Israel para atacar usinas nucleares do Irã. Ele foi implantado em 2008, através de espiões americanos armados com pendrives. Inicialmente, o alvo era a planta nuclear iraniana de Natanz, mas o Stuxnet escapou de lá e começou a se replicar.

A usina da Rússia não estava conectada à internet quando foi infectada. Kaspersky disse que isso ocorreu 'durante a época do Stuxnet', mas não entrou em detalhes sobre o efeito do malware na planta nuclear russa (ESTES, 2013).

O caso do subtenente acusado de matar o filho e tentar suicídio foi solucionado a partir de provas relacionadas à modificação de mensagem e pesquisa de veneno para rato. Uma mensagem na rede social alterada quando o subtenente estava em coma gerou desconfiança sobre a autoria do crime. Após uma pesquisa, a polícia constatou que a esposa do subtenente havia estudado veneno para ratos, instrumento usado para a prática do crime. No fim, a autora do crime era sua mulher (G1, 2015).

Por fim, podemos destacar o estupro virtual. Um caso em especial ocorreu em 2017, quando um juiz do Piauí decretou a primeira prisão por estupro virtual no Brasil (JUSBRASIL, 2017).

Com relação ao crime de estupro expresso no Código Penal, devemos primeiramente apresentar o artigo para uma melhor compreensão do tema. Assim, determina o artigo 213 do Código Penal: "constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou permitir que com ele se pratique outro ato libidinoso" (BRASIL, 2019).

Os autores Eleutério e Marcio Machado (2010) definem o papel dos provedores de acesso à internet como sendo um papel importantíssimo nas investigações. Assim, explicam os autores,

> [...] a maioria dos usuários utiliza os serviços de Internet a partir de sua residência e/ou pequenas empresas. Nesses casos, o computador pessoal (PC) de cada usuário não pode ter um endereço de IP reservado exclusivamente, pois a quantidade de endereços IPs disponíveis no mundo se esgotaria rapidamente. O que ocorre é que, para os usuários acessarem a Internet, eles precisam contratar um provedor, que será o responsável em atribuir um endereço IP válido para aquela conexão, possibilitando a entrada daquele computador na grande rede mundial.

Em território nacional, os provedores geralmente contratam uma faixa de endereços IP com Registro.br e, posteriormente, "emprestam" aos seus usuários. Cada vez que um usuário se conecta a um provedor, geralmente recebe um endereço IP diferente. Em um exemplo hipotético, um crime foi cometido por um usuário que acessou a Internet por meio de provedor, e sabe-se que o endereço IP utilizado foi AAA.BBB.CCC.DDD. Nesse caso, algumas informações cruciais para a investigação e a determinação da autoria estão em poder do Registro.br e, em alguns casos, também do provedor utilizado. O grande objetivo será descobrir qual computador estava utilizando os endereços IP naquele momento. Para isso, deve-se verificar no Registro.br para quem está registrado o endereço IP investigado. No caso de estar associado a um provedor de acesso (uma empresa de telefonia, por exemplo), será necessária uma nova etapa que consiste em obter com o provedor as informações sobre qual cliente utilizava aquele IP na data e hora de interesse nas investigações. (ELEUTÉRIO; MACHADO, 2010, p. 108).

Enfim, a internet é um campo perigoso, mas a tecnologia usada pelo criminoso também é utilizada pela polícia, sendo, assim, possível resolver alguns crimes cibernéticos.

CONSIDERAÇÕES FINAIS

Hoje, o avanço da tecnologia facilita a vida da sociedade, compras pela internet, vídeos para conversarmos com colegas e entes queridos, bancos oferecendo milhares de serviços, enfim, uma enormidade de facilidades. Por outro lado, nossa intimidade é exposta constantemente, os crimes cibernéticos aumentam, o grande problema é que hoje somos vítimas de vários crimes dentro da nossa própria casa. Antes não era seguro sair de casa, hoje a segurança acabou até mesmo em nossas residências. O que nos conforta é que a tecnologia não está apenas nas mãos dos infratores, mas também da polícia, assim, como apontamos nos artigos elencados neste trabalho, vários crimes são solucionados em virtude da evolução da internet.

FONTE: <https://profdebora.jusbrasil.com.br/artigos/1109384866/a-internet-como-instrumento-utilizado--pela-pericia-para-resolucao-de-crimes>. Acesso em: 8 out. 2021.

RESUMO DO TÓPICO 5

Neste tópico, você aprendeu:

- É fundamental seguir princípios de segurança da informação para a garantia da limpeza e sanitização de mídias e redes.

- Um método de esterilização de mídias é uma maneira específica pela qual um programa de destruição de dados ou destruidor de arquivos sobrescreve os dados em um disco rígido ou outro dispositivo de armazenamento.

- Uma conexão criptografada ajuda a garantir que os dados confidenciais sejam transmitidos com segurança. Evita que pessoas não autorizadas espionem o tráfego e permite que o usuário conduza o trabalho remotamente.

- A tecnologia VPN é amplamente utilizada em ambientes corporativos.

AUTOATIVIDADE

1 Sobre o método de esterilização Write Zero, assinale a alternativa CORRETA:

a) ( ) Write Zero substitui seus dados legíveis regulares pelo número 1.
b) ( ) Esse método pode incluir uma verificação após a primeira passagem, pode escrever um caractere diferente de zero ou pode escrever zeros em várias passagens, sendo essas maneiras comuns de fazer isso.
c) ( ) A diferença do Write Zero para os métodos aleatórios é que não é apenas o caractere que está sendo escrito que importa, mas a eficiência do método em sobrescrever os dados. Se apenas uma única passagem de gravação for feita e o software não verificar se todos os dados foram apagados, o método não será tão eficaz quanto os métodos que o fazem.
d) ( ) Quando o profissional limpa um disco rígido com zeros e, em seguida, joga fora, quem encontrar seu lixo, será capaz de recuperar de seus dados excluídos se usar uma anti técnica imediatamente.

2 Sobre as técnicas de apagamento seguro de dados, classifique V para as sentenças verdadeiras e F para as falsas:

( ) Wipe é um processo para apagar dados no disco rígido, *bit* a *bit*, de forma que substitua toda a área reservada para alocação de um arquivo. Os dados armazenados nos setores apagados são substituídos por zeros ou números aleatórios. Isso garante que não há possibilidade de dados serem recuperados por descuido ou sem intenção.
( ) Todo Wipe sobrescreve a área proposta inteira com caracteres específicos por até dezessete vezes. A maioria das mídias atuais podem ser sanitizadas com apenas sete sobrescritas.
( ) O grande problema da técnica Wipe é que pode ser utilizada para limpeza de discos como pode ser usada como um método antiforense para eliminar vestígios de um crime.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – V.
b) ( ) F – F – V.
c) ( ) V – V – F.
d) ( ) V – F – V.

3 A partir do que você aprendeu dentro dos princípios da segurança da informação, sobre a preservação das evidências na investigação, analise as sentenças a seguir:

I- Não repúdio é o processo de averiguar e solicitar uma comprovação para certificar que as informações obtidas na identificação são verdadeiras.
II- Autorização é validar e não dar chances que determinada entidade negue que foi ela quem realizou um ato específico, ou seja, através da autenticação e da identificação pode-se saber quem realizou tal ato e poder provar isso.
III- Identificação ou reconhecimento da entidade busca conhecer a origem e dados que afirmem quem é essa entidade.

Assinale a alternativa CORRETA:

a) ( ) Somente a sentença I está correta.
b) ( ) As sentenças II e III estão corretas.
c) ( ) As sentenças I e II estão corretas.
d) ( ) Somente a sentença III está correta.

4 O que significa esterilização de mídia?

5 Como método de sanitização de mídia, o DoD 5220.22-M, realiza três formas distintas de gravação nos bytes endereçáveis do disco. Quais são elas?

REFERÊNCIAS

ARAÚJO, S. de. **Computação Forense**. Curitiba: Contentus, 2020.

BEVERLY R.; GARFINKEL, S.; CARDWELL, G. Forensic Carving Of Network Packets And Associated Data Structures, **Digital Investigation**, v. 8, p. S78-S89, 2011. Disponível em: https://doi.org/10.1016/j.diin.2011.05.010. Acesso em: 8 out. 2021.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF: Diário Oficinal [da] República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 19 ago. 2021.

CHAPMAN, C. Using Wireshark and TCP dump to visualize traffic. **Network Performance and Security**, v. 2, p. 195-225, 2016. Disponível em: https://www.researchgate.net/publication/312132633_Using_Wireshark_and_TCP_dump_to_visualize_traffic. Acesso em: 8 out. 2021.

ELEUTÉRIO, P. M. D. S.; MACHADO, M. P. **Desvendando a Computação Forense**. São Paulo: Novatec, 2012.

ENCASE. **OpenText EnCase Forensic**, c2021. Software de Evidências Forenses. Disponível em: https://security.opentext.com/encase-forensic. Acesso em: 14 ago. 2021.

GALVÃO, M. da C. **Fundamentos Em Segurança Da Informação**. Recife: Pearson, 2015.

GARFINKEL, S. L. Carving Contiguous And Fragmented Files With Fast Object Validation Digital Investigation, **4S**, 2007, p. S1-S12. Disponível em: https://doi.org/10.1016/j.diin.2007.06.017. Acesso em: 2 set. 2021.

JORGE, H. V. N. **Investigação Criminal Tecnológica**. Volumes I e II. Rio de Janeiro: Brasport, 2018.

LOPES, P. **Forense Digital**, 2016. Perícia Forense Computacional. Disponível em: https://periciacomputacional.com/pericia-forense-computacional-2/. Acesso em: 13 ago. 2021.

MEROLA, A. **Data Carvingconcepts**, 2008. Sans Infosec Reading Room.Disponível em: https://www.sans.org/reading-room/whitepapers/forensics/data-carving-concepts-32969. Acesso em: 15 ago. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Computer Security: Guidelines For Media Sanitization. **Gaithersburg**, 2006. Disponível em: https://nvlpubs.nist.gov. Acesso em: 10 ago. 2021.

REIS, F. M. dos. Forense computacional: técnicas para preservação de evidências em coleta e análise de artefatos. **Brasil Escola**, 2019. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/forense-computacionaltecnicas-para-preservacao-evidencias-coleta-analise-artefatos.htm. Acesso em: 19 ago. 2021.

REIS, M. A dos GEUS, P. L. de. **Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos E Ferramentas**. Instituto de Computação. Universidade Estadual de Campinas, 2004.

TAMMA, R.; TINDALL, D. **Learning Android Forensics**. 1. ed. Birmingham, UK: Packt Publishing, 2015.

WENDT, E., BARRETO, A. **Inteligência E Investigação Criminal**. Rio de Janeiro: Brasport. 2020.

PRÁTICA EM COMPUTAÇÃO FORENSE

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- compreender as principais práticas da análise forense em sistema operacional *Linux*;
- reconhecer as características de ataques realizados em servidores *Linux*;
- entender o processo de coleta de informações do registro;
- identificar aspectos de redes de dados, tráfego e criptografia;
- investigar tráfego VOIP, identificando características da perícia forense;
- analisar processos de quebra de chaves na prática.

PLANO DE ESTUDOS

A cada tópico desta unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – ANÁLISE DE MÁQUINAS COM SISTEMA OPERACIONAL LINUX
TÓPICO 2 – ANATOMIA DE ATAQUES A SERVIDORES LINUX
TÓPICO 3 – COLETA DE INFORMAÇÕES DO REGISTRO
TÓPICO 4 – QUEBRA DE CHAVES WEP/WAP – PERSONAL
TÓPICO 5 – ANÁLISE DE TRÁFEGO VOIP
TÓPICO 6 – PRÁTICAS DE COMPUTAÇÃO FORENSE

CHAMADA

Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

CONFIRA A **TRILHA** DA UNIDADE 3!

Acesse o
QR Code abaixo:

ANÁLISE DE MÁQUINAS COM SISTEMA OPERACIONAL *LINUX*

1 INTRODUÇÃO

Acadêmico, no Tópico 1, abordaremos os principais pontos relacionados com análises forenses em máquinas com sistema operacional *Linux*. Analisando os atores e fatores envolvidos nesse cenário e características que devem ser notadas em ataques voltados para esse cenário.

Devemos considerar que a privacidade em sistemas operacionais é uma das maiorias preocupações quando o assunto é a segurança da informação e por isso, um profissional de TI deve estar atento aos métodos de análise de evidências como a coleta de log.

Sabendo disso, analisaremos a importância dos logs e os diretórios que devem ser explorados no sistema operacional *Linux* para extrair informações necessárias em uma prática forense.

2 ANÁLISE DE MÁQUINAS COM SISTEMA OPERACIONAL *LINUX*

Atualmente, assim como os especialistas em segurança dispõe de diversos motivos para proteger um sistema, os ataques também são motivados por uma variedade de fatores, dessa forma análises forenses acabam se tornando necessárias. As categorias que segmentam a análise forense, de acordo com Nikkel (2021), são duas:

- Vítimas, parte que sofre com os ataques cibernéticos de diversas origens como intrusões e incidentes conduzidos através do conhecimento do atacante sobre a vítima, a fim de a influenciar em dar-lhe informações como a engenharia social.
- Perpetradores, categoria que representa qualquer sistema de computador apreendidos por autoridades ou equipes de investigação à resposta a incidentes corporativos. Geralmente coletados para análise de atividade maliciosa ou criminosa, estando em posse de alguém mal-intencionado.

Com relação ao lado que representa as vítimas, ele cita as seguintes formas de ataques, que devem ser consideradas em uma análise forense voltada para servidores *Linux*:

- Servidores que foram *hackeados* ou comprometidos pela exploração técnica de brechas de segurança no sistema ou configuração incorreta servindo como base para um ataque.
- Acesso não autorizado a servidores usando credenciais roubadas de usuários devidamente cadastrados ou desvendadas através de ataque de força bruta.
- Usuários acessando conteúdo comprometedor, onde como consequência, o computador tenha sido invadido por malware, ou qualquer vírus que tenha sido executado através de scripts maliciosos camuflados em programas.
- O atacante induz o usuário do sistema através de engenharia social, coletando informações de acesso ao sistema operacional.
- Sistemas de computador que precisam ser analisados como parte de uma investigação maior em uma organização vitimizada ou tomou alguma ação que prejudique outra organização como uso de *software* pirata ou não licenciado, por exemplo.

No caso de perpetradores, a análise normalmente envolve as seguintes práticas:

- Servidores são especificamente configurados para hospedar sites de phishing, distribuir *malwares* e gerenciar *botnets*, redes gerenciadas remotamente com o intuito de infectar a rede alvo através de *softwares* maliciosos, ataques DDoS e *spam*.
- Os próprios usuários autorizados podem ser tornar perpetradores, utilizando de informações privilegiadas para atacar por algum motivo à organização através de atividades ilegais.

Sistemas operacionais *Linux* precisam ser analisados e diversos fatores que envolvem má funcionamento do sistema, detecção de atividades suspeitas e irregularidades na operação da rede servem como base para fornecer evidências ao perito.

Quando os sistemas *Linux* são legalmente apreendidos por autoridades ou organizações devidamente autorizadas, ou até mesmo disponibilizados de forma voluntaria pelas vítimas, tornam-se imagens forenses, sendo o principal recurso do investigador que precisa coletar informações e detectar o problema ocorrido na infraestrutura e que serviu como fonte do ataque ou cibercrime.

IMPORTANTE

Nem sempre um único usuário faz o uso do sistema *Linux* e nesses casos, Nikkel (2021), afirma que as evidências e a análise de registros acabam envolvendo um grande volume de dados. Outro ponto importante é que devido aos ataques ocorridos em relação ao sistema operacional *Linux*, muitas vezes um usuário pode se passar por outro e ser dessa forma, acusado indevidamente ou estar sob suspeita, a atividade de análise forense em sistemas operacionais, dessa forma, também pode fornecer evidência de inocência.

A principal ferramenta nativa do sistema, que permite ao perito forense a coleta de informações e análise de atividades, são os logs. Por isso, analisaremos sua importância a seguir.

2.1 ANÁLISE DE LOGS

Acadêmico, antes de mais nada vamos definir o que são Logs: registros, geralmente armazenados em arquivos do tipo *ascii* (codificação utilizada para representar textos em computadores) ou de texto simples. A principal funcionalidade dos logs é armazenar o status de execução de sistemas e estatísticas ou comportamentos inesperados que ocorrem nos serviços de rede.

Os logs são de grande importância para a segurança e a privacidade dos dados, revelando eventos importantes para os processos de auditoria, reconstituindo cenários importantes para o reestabelecimento de serviços e identificando ataques que precisam ser explorados pela perícia forense.

Apesar da importância dos logs, existem diversas tarefas importantes que devem ser levadas em consideração pelos especialistas para analisar corretamente o comportamento de determinado sistema. Os logs quando são simplesmente armazenados não resolvem o problema, por isso tomar ações que vão além do armazenamento no disco como despejo de memória e congelamento de processos, são ações que devem estar relacionadas entre si. Nikkel (2021) aponta que os especialistas devem estar familiarizados com a coleta de dados em sistemas *Linux* a partir de diversos aplicativos como o *squid.*

NOTA

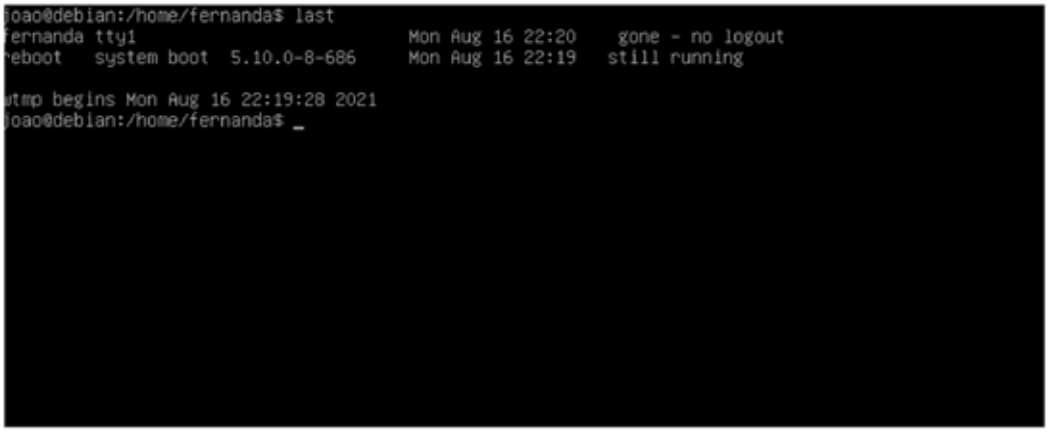
Não se preocupe, entenderemos a funcionalidade do squid e suas características básicas ainda nesse livro.

O *Linux* oferece diversos comandos nativos e diretórios que armazenam registros e retornam informações sobre o sistema. Vamos conhecer alguns deles:

2.1.1 Comando LAST

Utilizado para identificar os últimos usuários que realizaram *login* na rede, apresentando o histórico de acessos por meio de listagem, conforme ilustra a Figura 1:

FIGURA 1 – COMANDO LAST



FONTE: A autora

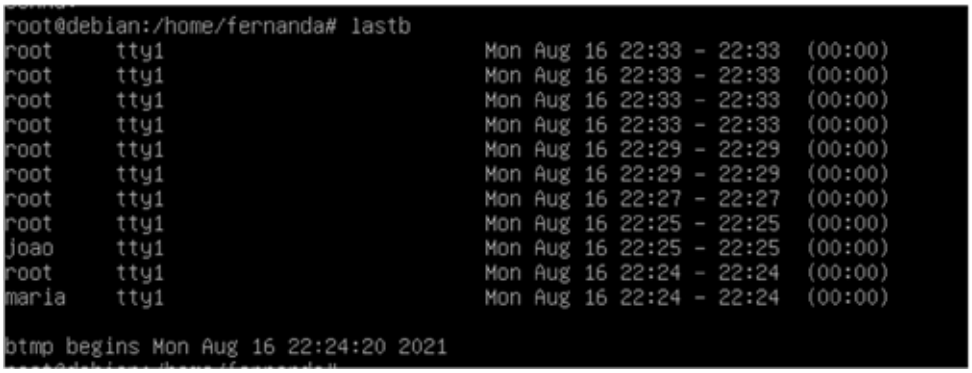
Nesse exemplo, é possível notar que Fernanda esteve logada as 22:20 do dia 16 de agosto e que o usuário root está logado no momento que as informações são coletadas.

Algumas informações importantes para a perícia forense são retornadas ao utilizar o comando, como data e hora, considerando que seja necessário comprovar se este acesso deve ser considerado como evidência em determinada situação.

2.1.2 Comando LASTB

Agora, analisando a Figura 2, podemos analisar a execução do comando *lastb,* que ao contrário do comando anterior, lista as tentativas de login mal-sucedidas de usuários que por algum motivo, foram barrados no seu acesso ao sistema:

FIGURA 2 – COMANDO LASTB



FONTE: A autora

Além de visualizar as informações no próprio terminal, é possível realizar acesso direto aos registros no arquivo de logs armazenado no diretório /var/log/btmp.

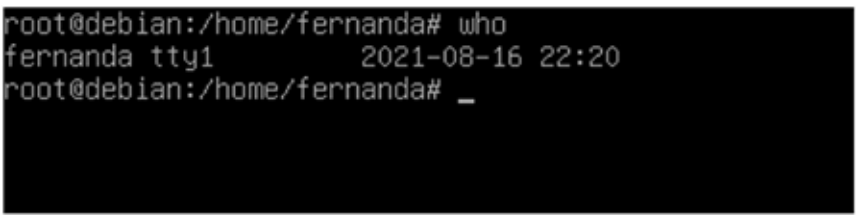
ATENÇÃO

O comando **cat** é utilizado no *Linux* para exibir o conteúdo armazenado em um ou mais arquivos de texto, permitindo ainda combinar as informações e criar novos arquivos com a saída resultante.

2.1.3 Comando WHO

Com esse comando, a análise de logs considera os usuários logados na máquina, no momento em que a evidência foi coletada. Acompanhe na Figura 3:

FIGURA 3 – COMANDO WHO



FONTE: A autora

Nesse exemplo, temos apenas um usuário, mas em redes complexas, analisar os usuários logados pode ser um processo que requer algum tempo.

2.1.4 Comando *history*

Na maioria das vezes, o perito vê a necessidade de analisar o histórico completo de comandos que foram executados no sistema na seção atual, a partir deles, é possível direcionar corretamente o processo de auditoria. A Figura 4 ilustra o histórico:

FIGURA 4 – COMANDO HISTORY

FONTE: A autora

Acadêmico, agora que já conhecemos alguns dos comandos nativos do sistema operacional *Linux* para coletar evidências importantes para a perícia forense. Vamos falar sobre os processos. Nem sempre somente acompanhar as atividades já executadas ou quais usuários estão utilizando o sistema é necessário, até porque essas são tarefas normais em um ambiente de rede.

É necessário analisar os processos que estão sendo executados em um sistema operacional *Linux* e que em muitas vezes estão camuflados através de outros processos, fazendo-se parecer que não é uma atividade suspeita, como por exemplo em segundo plano.

2.1.5 Monitoramento de processos e diretórios importantes

Ao citar o monitoramento de processos como uma prática importante na análise de evidências, Nikkel (2021) aponta que determinados arquivos podem ser implantados no sistema com o objetivo de executar ameaças como *trojans,* sendo esses configurados para chamar os processos. Por isso, além dos recursos como *logs,* históricos e *status* dos usuários, o comando *ps-aux* é útil para identificar processos que estão sendo executados no *Linux*.

Através do PID de um processo, é possível identificar qual programa está sendo executado. Portanto se a política da empresa não permite a utilização de *softwares* homologados, por exemplo, é possível filtrar aplicações executadas e identificar qualquer ação não autorizada, com o uso do comando lsof -p por exemplo apontando para determinado processo.

ATENÇÃO

O comando deve ser executado da seguinte forma:

admin@Linux: /var/log$ lsof -p 11098

No comando, "11098" é o número do processo.

Geralmente, a intenção de uma perícia forense é identificar o usuário que executou determinada ação, por isso, além de identificar o ID do processo, é importante identificar qual usuário está relacionado com o processo executado através do ID único para identificá-lo. Assim como o PID está para o processo, o UID está para o usuário. O comando lsof pode ser adaptado para esse fim: **admin@*Linux*: /var/log$ lsof –U UID**.

INTERESSANTE

Sabia que no Linux por padrão, os registros são mantidos no diretório /var/log?

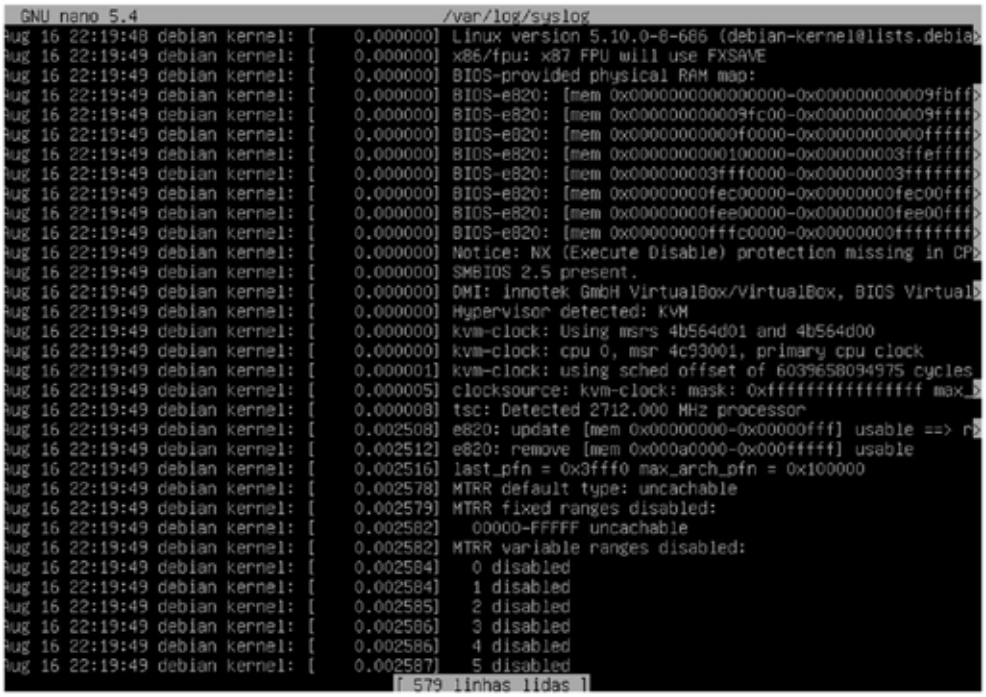
Por isso, mesmo sem rodar nenhum comando, o perito pode analisar o arquivo completo de acessos.

No entanto, em alguns casos, logs mais completos são necessários, para que se possa analisar outros serviços como:

- Logs de rede.
- Requisições de conexões aos servidores.
- IPs atribuídos aos *hosts*.
- Identificar se dispositivos móveis foram conectados por exemplo, o que é um grande indício de que a cópia de alguma informação ou arquivo foi feito ou algum *software* foi adicionado ao sistema.

Para isso o arquivo daemon.log no diretório /etc/log pode ser útil, como ilustra a Figura 5:

FIGURA 5 – ARQUIVO SYSLOG



FONTE: A autora

É possível notar que diversos eventos são registrados como:

- Inicialização do sistema e a versão do Kernel.
- Inicialização da BIOS.
- Execução do sistema operacional com base no Virtual Box.
- Especificações de memória e processamento.

Para complementar nosso conhecimento, no Quadro 1, iremos analisar outros diretórios importantes na análise de log:

QUADRO 1 – DIRETÓRIOS IMPORTANTES

Diretório	Funcionalidade
messages/syslog	Armazena eventos e informações do sistema Linux e dos aplicativos hospedados.
boot.log/dmesg	Registra qualquer informação relacionada com os processos e com a inicialização do sistema.
Secure	Guarda mensagens privadas utilizadas pelos problemas, além de permissões que autorizam os usuários a acessar os arquivos.
Syslog	Registra o uso do comando su. O comando su é utilizado para alterar credenciais de usuários.
/etc/syslog.conf	Arquivo de configuração de logs principal, que registras as mensagens do sistema.

FONTE: Adaptado de Nikkel (2021).

Na maioria dos casos, em que a perícia é necessária, não são de fato os logs internos da rede que são os mais importantes. Ainda mais quando se trata do vazamento de informações por exemplo, compartilhamento de dados privados ou roubo de informações privadas, recursos como proxys de cache podem ser úteis em cenários como estes.

2.1.6 *Proxy* de cache

O administrador de rede mantém além das políticas e boas práticas, soluções de hardware e software (componentes lógicos do computador*)* que auxiliam na produção de provas, segurança da rede e armazenamento de *logs,* como um *proxy* de *cache.*

Quando visitamos um site, o cache eventualmente é copiado e armazenado temporariamente ao utilizar um *proxy* de cache, sendo assim, as informações carregadas dentro de determinado período pelos usuários, podem ser revistas pelo administrador. Outra vantagem é que ao armazenar esses dados, os próximos acessos dos usuários são facilitados, resultando em menor tempo para o carregamento da página, minimizando o número de solicitações ao servidor, aumentando assim a velocidade de acesso (INTNET, 2018).

NOTA

O *Squid* é um dos servidores proxy mais comuns baseados em sistemas Linux e extremamente úteis na análise de logs.

Assim como todos os logs que citamos até agora, em um servidor *proxy,* os registros também são armazenados em um diretório específico, nesse caso, a análise deve ser voltada para /etc/squid/squid.conf. Além disso, Nikkel (2021) aponta que podemos dividir os logs da seguinte forma:

- No diretório /var/log/squid/access.log está armazenado um arquivo contendo o registro de todas as conexões http;
- No diretório /var/log/squid/cache.log, podem ser encontradas informações sobre hora e data em que o arquivo cache foi iniciado;
- No diretório /var/log/squid/store.log são registradas as atividades de usuários que envolvem acessos e pesquisas aos sites, incluindo o conteúdo armazenado como vídeos, conteúdos proibidos, mp3s e imagens e servem como parâmetro para auditoria, quando os padrões de segurança e políticas de acesso são bem estabelecidos.

2.1.7 Programa GREP

Já falamos dos *logs,* dos diretórios que os armazenam e da importância dos registos em uma perícia forense. Mas ainda é importante falarmos sobre o *Grep (global regular expression print),* que de acordo com Morimoto (2010), pode ser descrito com um programa que pode ser encontrado na maioria das distribuições do sistema *Linux,* utilizado para filtrar informações de um arquivo de log, retornando apenas determinadas *stings*, facilitando as perícias e auditorias.

Um perito, administrador ou investigador pode encontrar uma grande dificuldade em analisar arquivos de *log* muito extensos, além disso, muito tempo seria consumido desnecessariamente e isso pode ser resolvido com o uso do *Grep.* Aqui geralmente temos uma ferramenta útil, em casos que o perito já sabe pelo que busca e pode utilizar termos específicos para garantir uma filtragem enxuta nos registros.

Na investigação de incidentes eletrônicos e crimes digitais, a análise de logs é muito importante, pois se a função do perito é investigar a ocorrência de um fato e determinar seu autor, então a função do log é atuar como "testemunha eletrônica", servindo como prova para justificar as ações que determinam ações maliciosas de forma concreta.

RESUMO DO TÓPICO 1

Neste tópico, você aprendeu:

- É possível realizar a verificação de integridade do sistema operacional Linux através da análise de logs.

- Podemos identificar conexões de rede de origens suspeitas estabelecidas ou serviços sendo executados sem permissão adequada.

- Reconhecer atividades atípicas de usuários ou atacantes através de registros e diretórios do sistema Linux se torna mais simples.

- Podemos analisar inconsistências nos arquivos e processos, utilizando-os como evidências.

AUTOATIVIDADE

1 Diretórios são locais onde por padrão o sistema estrutura sua funcionalidade e em relação ao registro de logs. Assim como qualquer serviço, os repositórios principais utilizados por um servidor *squid* podem ser classificam de acordo com as informações armazenadas, entre eles está o que armazenada os registros das conexões HTTP estabelecidas pelos usuários. Sobre esses diretórios, assinale a alternativa CORRETA:

a) ( ) /var/log/squid/access.log.
b) ( ) /var/log/squid/cache.log.
c) ( ) /var/log/squid/store.log.
d) ( ) /var/log/squid.log.

2 As análises periciais tratam de uma séria de informações que precisam ser coletadas e analisadas e em alguns casos, o cenário é de grande complexidade, necessitando o perito de ferramentas mais complexas. De forma nativa, os sistemas *Linux* oferecem o daemon.log como recurso. Com base em suas características, analise as sentenças a seguir:

I- Diversas práticas podem ser facilitadas com o uso do arquivo *daemon.log*, entre elas podem citar a análise de estatísticas e requisições de rede como conexões estabelecidas aos servidores e endereçamento IPs dos hosts que realizaram o acesso.
II- Somente pode ser utilizado quando o armazenamento das informações foi configurado pelo administrador previamente através de um plugin compatível com a versão do sistema utilizado.
III- Por meio desse arquivo, é possível identificar dispositivos móveis que foram conectados ao sistema e que podem representar qualquer ameaça aos serviços e aos usuários da rede.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Quando falamos de ataques em sistemas *Linux,* podemos citar como partes envolvidas, as vítimas que sofrem os ataques e os perpetradores que conduzem e executam práticas de ataques. De acordo com classifica a categoria dos perpetradores, classifique V para as sentenças verdadeiras e F para as falsas:

( ) É induzido através da engenharia social, onde fornece credenciais e informações privilegiadas favorecendo os ataques e o acesso ao sistema através de recursos de autenticação verídicos.
( ) Utiliza softwares piratas com a intenção de prevenir ataques e garantir que informações privilegiadas não sejam externadas ou utilizada contra os princípios da organização.
( ) Configura servidores utilizados para hospedar sites falsos, encaminhar mensagens de *Phishing* e distribuir *malwares* e ataques bem sucedidos.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) F – F – V.
c) ( ) F – V – F.
d) ( ) V – F – V.

4 A análise de logs é um dos primeiros passos seguidos pelo perito para coletar o máximo de informações no ambiente corporativo quando sistemas *Linux* são utilizados. Apesar disso, em alguns casos existe um grande volume de dados e ferramentas, como o Grep, que podem facilitar o processo de análise. A partir deste contexto, disserte sobre a funcionalidade do Grep.

5 A vítima é um dos fatores causadores dos ataques em sistemas *Linux* sendo reconhecidas como o principal alvo dos atacantes. A partir deste contexto, disserte sobre a forma como os atacantes utilizam as vítimas para realizar essas ações que representam também pontos de atenção para os peritos.

ANATOMIA DE ATAQUES A SERVIDORES *LINUX*

1 INTRODUÇÃO

Acadêmico, no Tópico 2, abordaremos as características principais de ataques que são cometidos em sistemas operacionais *Linux*, além de compreender quais são os principais fatores que influenciam na segurança dos sistemas em relação à essas ameaças.

É importante levar em consideração que existem diversos tipos de ataque e que cada um explora vítimas, alvos e vulnerabilidades especificas, por isso iremos abordar alguns deles.

Sabendo disso, analisaremos os locais clássicos para busca de evidências e que facilitam a forma como o perito forense coleta informações, alimentando também nosso conhecimento sobre os *rootkits.*

2 ANATOMIA DE ATAQUES EM SERVIDORES *LINUX*

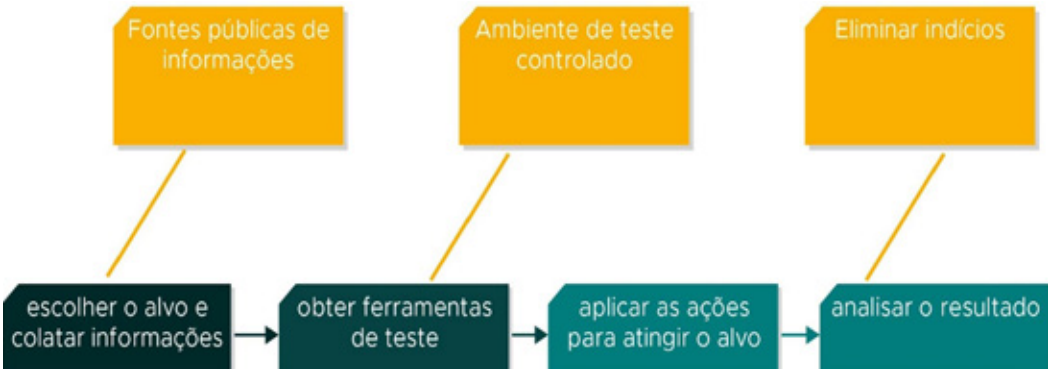
Cada vez mais, o número de ataques a redes de computadores conectadas à Internet cresce. Os ataques DDoS são os mais frequentes e ocorrem na maioria das redes locais. Muitos problemas de segurança estão relacionados com os protocolos e serviços da Internet e ainda não estão ligados às soluções definitivas. Nesse cenário, não estamos falando apenas das vítimas diretas do ataque, mas também discutindo principalmente sobre a forma como os dados estão expostos devido à forma como as informações são disponibilizadas através dos sistemas.

Os administradores de rede sabem que esses problemas de segurança são principalmente incidentes do sistema operacional, mas também acreditam que, quanto menos os hackers souberem sobre o seu sistema, menos vulneráveis eles serão a ameaças externas e em muitos casos, acabam por não tomar os cuidados necessários para evitar que as tentativas de intrusão sejam bem-sucedidas.

Apesar de a privacidade dos dados ser um fator importante na visão do administrador de rede, com tantas tarefas atribuídas, nem sempre a atenção necessária é direcionada para os problemas de segurança, a menos que eles aconteçam e aí entra a função do perito forense, para descobrir o que causou o incidente, principalmente quando estão ligados aos privilégios de superusuário, quando o assunto é o sistema *Linux*.

Na Figura 6, podemos compreender melhor como a anatomia de um ataque é definida:

FIGURA 6 – ANATOMIA DE UM ATAQUE



FONTE: A autora

O fluxo que prevê a anatomia de um ataque é bastante claro e composta por etapas que precisam ser executadas de forma sincronizada para que se possa alcançar o resultado esperado.

2.1 ETAPAS DE UM ATAQUE

Um ataque geralmente inicia quando o *hacker* utiliza uma ferramenta de scanner, de acordo com Sobral (2021a), que ainda afirma que existem diversos recursos que podem oferecer essa funcionalidade e permitindo que seja possível identificar quais as aplicações e serviços estão disponíveis em um sistema operacional e podem ser explorados.

Tendo conhecimento sobre os serviços e suas versões, o atacante pode pesquisar e estudar sobre as suas vulnerabilidade e falhas que ainda não foram resolvidas pelos seus fabricantes. Sobral (2021a) aponta que os ataques podem ser definidos em três etapas, que analisarem a seguir:

- **Footprint**

Primeira fase do ataque, em que as informações são coletadas de forma passiva (sem que o administrador perceba) ou de forma ativa (sem uso de qualquer camuflagem). No segundo caso, fica mais fácil identificar quando um ataque está ocorrendo, já que atividades suspeitas podem ser identificadas no sistema, como o uso de credenciais desconhecidas, por exemplo. Quanto mais informações forem coletadas, mais críticas se tornam as consequências do ataque.

E quais são as informações uteis em um ataque executado ao sistema? Bom, isso depende tanto do objetivo quanto das funcionalidades do sistema operacional na rede. Todavia, de forma genérica podemos citar algumas delas:

- Endereços IPs de *hosts* alvos;
- Informações de acessos dos usuários;
- Segmento de atuação da organização, domínio e endereços de e-mail;
- Versões dos serviços utilizados.

Todas essas informações podem servidor como porta para acesso ao sistema operacional.

- **Fingerprint**

Enquanto *footprint* definem as informações coletadas, *fingerprint* definem as ferramentas utilizada para essa coleta. Por isso, recursos que auxiliam na coleta de tráfego são importantes armas utilizadas no ataque da rede.

DICAS

Ferramentas como *NMAP*. *Wireshark* e *Xprobe2* podem ser utilizadas, principalmente quando a varredura de portas e encaminhamento de pacotes forem atividades que precisam ser realizadas pelos atacantes.

- **Enumeração**

Enumeração é o processo de extrair informações de um sistema de destino para entender melhor o que está presente em sua configuração e ambiente. Sobral (2021a) acredita que esta fase requer mais tempo de análise, e é nesta fase que as informações sobre o usuário, comutadores e sistemas, como credenciais do sistema, nome do host, compartilhamentos e serviços. No entanto, essas informações dependem do sistema operacional usado e de sua versão de lançamento.

As ferramentas disponíveis para realização de ataques estão cada vez mais poderosas e não se fazem tão complexas como antes, podendo ser executada por qualquer pessoa que tenha interesse e disciplina para entender como funcionam. Os próprios atacantes criam e melhoram as ferramentas para que possam atender às suas necessidades, cada vez que seu conhecimento é reforçado em relação as características dos sistemas *Linux.*

2.2 ATAQUE *SCRIPT KIDDIE*

Sempre que possa existir qualquer bug de segurança relacionado com determinada versão de algum serviço em sistemas *Linux* é de conhecimento público e para os atacantes fica mais fácil utilizar *exploits* como ferramenta.

O *Script Kiddie* é basicamente alguém que procura, nas diversas redes de computadores conectadas à Internet, certas vulnerabilidades que facilitariam uma invasão e para isso não é necessário possuir um nível alto de conhecimento técnico ou atuar como profissional de segurança.

O objetivo não é atacar uma rede ou *host* específico, mas sim qualquer alvo que possua deficiências de segurança e muitas vezes as práticas representam um *hobby* ou a vontade de adquiri conhecimento em determinada técnica, sem qualquer objetivo específico (SOBRAL, (2021b)).

NOTA

Um *exploit* determina qualquer ataque em que as vulnerabilidades de aplicações, redes e sistemas operacionais sejam exploradas. Na verdade, *exploits* não são voltados somente para ataques em *software*, mas também em *hardware* (componentes físicos do computador). Geralmente os *exploits* são soluções em forma de código que possibilitam controlar sistemas e como consequência permitir o roubo de informações. (LATTO, 2020).

Para exemplificar essas características, a Figura 7 pode ser analisada:

FIGURA 7 – ANATOMIA DE UM ATAQUE SCRIPT KIDDIE

FONTE: Sobral (2021, s.p.)

Suponha que um Script Kiddie utilizou uma ferramenta de scanner para identificar portas abertas e protocolos utilizados em uma rede. Podemos assumir que as seguintes informações podem retornar como saída do que foi coletado de forma genérica:

<[tcp port: 80 (http)]> <[tcp port: 23 (telnet)]>
<[tcp port: 143 (imap)]> <[tcp port: 110 (pop-3)]>
<[tcp port: 111 (sunrpc)]> <[tcp port: 79 (finger)]>
<[tcp port: 53 (domain)]> <[tcp port: 25 (smtp)]>
<[tcp port: 21 (ftp)]>
–<[*OS*: máquina: os detected: redhat *Linux* 5.1
máquina: VULN: *Linux* box vulnerable to named overflow.
-<[*CGI*: IP_da_máquina: tried to redirect a /cgi-bin/phf request.
-<[*FINGER*: máquina: root: account exists.
–<[*VULN*: máquina: sendmail will 'expn' accounts for us
–<[*VULN*: máquina: *Linux* bind/iquery remote buffer overflow
–<[*VULN*: máquina: *Linux* mountd remote buffer overflow
––––––––––––<[* scan of máquina completed *

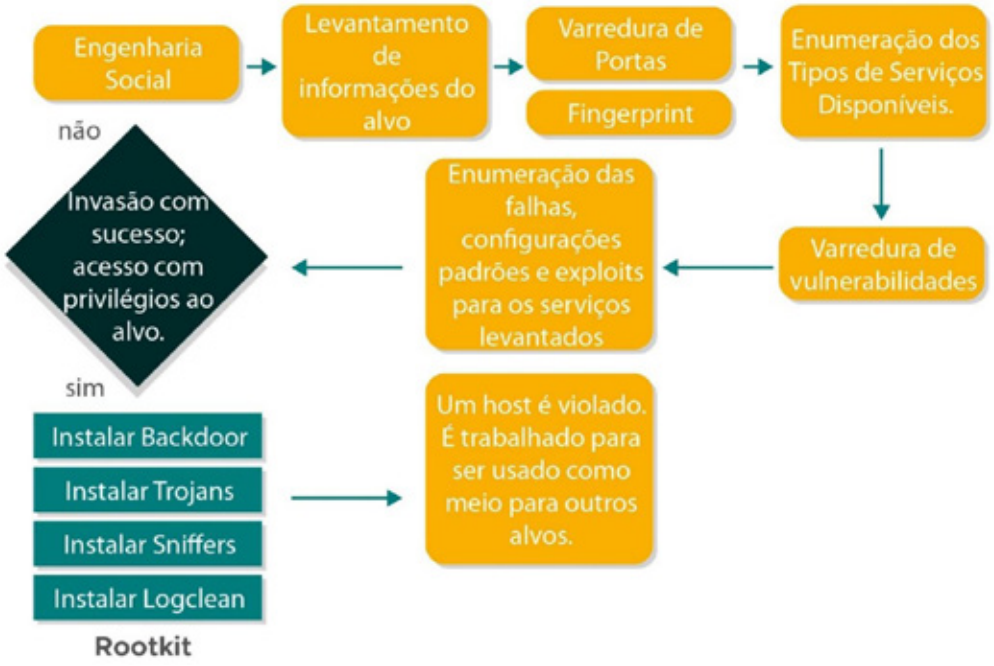
Observe que na saída além de identificar as portas e serviços ativos na rede, a versão do sistema operacional também foi detectada e a conta de usuário root. Ao final do que foi coletado, algumas linhas estão identificadas com a tag VULN, o que aponta para vulnerabilidades encontradas e que podem servir como chave de entrada para o atacante como o nome da máquina, o aceso de root e os serviços mal configurados como o *bind* e o *mountd* (sistema de arquivos).

Mesmo que ao utilizar um scanner, o atacante não tenha vulnerabilidades reveladas à seu favor, outra estratégia que deve ser conhecida na perícia forense, se deve ao fato de o atacante criar um banco de dados com as informações obtidas para utilizar à seu favor, tendo acesso constantemente as máquinas que possuem vulnerabilidades e de que forma elas podem ser exploradas

2.3 ATAQUE *CRACKER*

Nesse ataque uma máquina ao ser atacada, pode ser utilizada como fonte para gerar ataque à outras máquinas. Com a execução desse ataque, é possível que a vítima seja atacada várias vezes sem ao menos perceber, já que de acordo com Sobral (2021), o atacante é capaz de apagar seus rastros sem aos menos ser identificado. A anatomia de um ataque cracker pode ser visto na Figura 8, assim como comparado com um ataque do tipo Script Kiddie.

FIGURA 8 – ANATOMIA DE UM ATAQUE CRACKER



FONTE: Sobral (2021)

É possível concluir que para perícias forenses sejam bem-sucedidas, assim como os atacantes, os peritos forenses precisam entender sobre os protocolos e serviços usados na rede e também ter o conhecimento necessário para identificar locais clássicos para busca de evidências, como veremos no próximo tópico.

3 LOCAIS CLÁSSICOS PARA BUSCA DE EVIDÊNCIAS

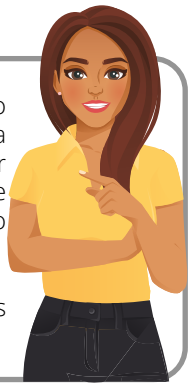
Quando um perito, precisa investigar um sistema, o primeiro passo é obter a imagem original ou ISO, que estaria sendo utilizada antes que os serviços fossem afetados, adulterados ou danificados, para que seja possível evidenciar as causas a partir das provas coletadas. A originalidade do material é importante para garantir que o que precisa ser descoberto, de fato seja.

Após a montagem da imagem em um servidor ou computador seguro, o perito deve iniciar a análise dos logs e dos diretórios.

ATENÇÃO

É necessário prezar pela integridade da imagem analisada, por isso Argolo (2005) afirma que é importante o perito montar o sistema em uma mídia ou dispositivo somente em modo de leitura, evitando que qualquer alteração acidental ou atualização do sistema possa interferir no ambiente a ser investigado. O comando a ser executado nesse caso é: # mount -o ro,noexec,nodev,loop hdc_img.dd /mnt/analise

Isso irá impedir qualquer instalação que possa influenciar nas evidências digitais a serem produzidas.



Por onde começar? Afinal, existe uma infinidade de diretórios na estrutura de um sistema. Por isso, o perito deve conhecer os principais locais, onde as informações podem estar armazenadas, localizando a fonte de dados de forma facilitada, evitando a necessidade de avaliar arquivos desnecessários.

Antes de qualquer coisa, é necessário relembrar que os atacantes possuem um bom conhecimento técnico e por isso nem sempre apenas analisar os diretórios e logs será a solução para um caso baseado em evidências, considerando que eles apagam seus rastros sempre que possível, então o controle de acesso e de credenciais deve ser rígido no sistema, através de políticas implementadas pelo administrador de rede, para evitar que as provas sejam descartadas de maneira mais simples, o que dificulta o trabalho do perito por exemplo.

Já na sua função, o perito deve estar atendo ao analisar o sistema comprometido focando em tipos de arquivos importantes, para entender qual foi a intenção do atacante ao comprometer a máquina e quais as ações que ele executou para efetivar o ataque.

Vamos analisar alguns locais que devem ser de atenção dos peritos

3.1 ARQUIVOS TEMPORÁRIOS

Geralmente quando o usuário está mal-intencionado, mas não possui conhecimento necessário para livrar-se das provas. Os arquivos suspeitos são deletados superficialmente. E, por mais provável que seja, os diretórios temporários devem ser analisados, entre eles podemos citar o /tmp e o /usr/tmp, que armazenam arquivos excluídos pelo próprio sistema, mas que podem ser bastante úteis para rastrear determinadas atividades.

3.2 DIRETÓRIO /dev

O diretório /dev é um diretório que, em regra, possui mais de mil arquivos e é pouco acessado pelos administradores, já que é um diretório de dispositivo bastante utilizado pelo próprio sistema operacional. Por esses motivos, esse diretório torna-se interessante para um invasor que deseja guardar arquivos maliciosos no sistema sem alertar o administrador.

Pelo fato do diretório /dev ser um diretório de dispositivos, qualquer arquivo regular presente em seu conteúdo pode ser uma evidência. Scripts criados pelos atacantes, geralmente são armazenados nesse diretório e rodam em segundo plano.

3.3 ESTRATÉGIAS DE OCULTAÇÃO DE PROVAS

Arquivos e diretórios ocultos são bastante comuns quando servem como ferramenta do atacante para executar comandos, scripts e instruções no sistema, sendo comumente utilizados para enganar os administradores e despistar os peritos na investigação de provas.

Nomes não usuais também são adotados, renomeando e criando arquivos com padrões de nomes incomuns, contendo espaços, caracteres especiais, espaços em brancos ou pontos. No entanto, ferramentas e comandos nativos do *Linux* podem auxiliar na localização desses arquivos.

root@debian: /home/admin: #ls -la | cat -A

O comando permite visualizar as linhas com caracteres especiais, garantindo que a varredura seja completa, evitando que algumas evidências passem despercebidas.

3.4 DIRETÓRIOS BINÁRIOS E BIBLIOTECAS

Não somente os arquivos de texto devem ser revisados, pelo contrário, outras extensões de programas e aplicativos são ainda mais importantes e precisam ter seus rastros devidamente analisados. Arquivos binários do sistema geralmente são armazenados em diretórios padrões, entre eles: /bin, /sbin, /usr/bin e /usr/sbin.

NOTA

Um arquivo binário é qualquer arquivo de computador em um formato não textual. Podem ser programas de computador, arquivos de imagem digital, arquivos de som, bibliotecas compartilhadas, arquivos de dados e vários outros arquivos. Qualquer arquivo em um formato não textual é considerado um arquivo binário.

É possível que provas falsas sejam criadas pelo atacante ou que alguma evidência precise ser verificada à nível de integridade por isso é preciso utilizar de marcas como os *hashs,* que definem se um arquivo é de fato original, isso pode ser feito manualmente com os devidos conhecimentos sobre criptografia ou automatizando o processo através de ferramentas específicas que geram o *hash* criptográfico do arquivo, permitindo a comparação e análise (ARGOLO, 2005).

3.5 ÁREAS NÃO ACESSÍVEIS

Infelizmente não se pode ter um controle sobre as áreas não acessíveis, de acordo com Argolo (2005), aqui podemos considerar os arquivos apagados e a referência que também é removida da estrutura do sistema operacional. Entretanto, como sabemos, mesmo quando as informações sejam removidas do sistema, ainda permanecem localizadas no disco, existem diversos métodos de recuperação à baixo nível.

A estrutura de um disco rígido, mantem os dados até que eles sejam sobrescritos por outros arquivos, por isso a recuperação do arquivo ou de parte dele ainda é possível á nível de hardware, por isso, chamamos de área inacessíveis.

Apesar de o administrador ser responsável por garantir a integridade dos logs do sistema e o perito forense de analisar as evidências considerando seu conhecimento na coleta de informações, o atacante também é um *expert* e utiliza diversas ferramentas a seu favor, algumas delas conhecidas como *rootkits*, geralmente utilizadas para esconder seus rastros, consequências dos atos. Iremos analisar a funcionalidade dos *rootkits* no próximo tópico.

4 ANÁLISE DE ROOTKITS

Os *rootkits* são utilizados para auxiliar o atacante na ocultação dos seus rastros, seja alterando ou apagando logs no sistema. Além disso também é útil para modificar arquivos binários, criar contas de usuários fictícias para despistar o investigador e alterar o cenário do crime digital. *Backdoors* também são ocultadas.

NOTA

Backdoors como o próprio nome diz são portas dos fundos, por onde o atacante se infiltra na rede. Esse método de entrada permite que através de um malware, o atacante possa entrar no sistema sem o uso de qualquer recurso de autenticação, contornando a necessidade de identificação no sistema.

Na verdade, os *rootkits* permitem que até mesmo atacantes com pouca experiência possam ocultar sua identidade e intenções. A detecção desse recurso geralmente é complexa e as soluções se tornam cada vez mais complexas através de melhorias que possam torná-los imperceptíveis.

Para justificar como isso ocorre, Argolo (2005) afirma que alguns *rootkits* usam a técnica LKM (*Loadable Kernel Module*) para tornar isso possível. A principal ação dessa técnica é alterar as chamadas do sistema(syscalls).

É possível notar que assim como os atacantes, os peritos podem utilizar as características nativas do sistema ao seu favor. Sistemas operacionais *Linux* possuem diversas ferramentas de segurança implementadas para proteger os serviços e informações armazenados, por isso mesmo contendo vulnerabilidades assim como os demais recursos computacionais, o *Linux* pode permitir que a perícia forense possa ser executada com base em diversas possibilidades de análise desde simples arquivos e diretórios até o uso de ferramentas capazes de avaliar ameaças e ataques a partir de ações mais complexas.

RESUMO DO TÓPICO 2

Neste tópico, você aprendeu:

- Os comandos nativos do *Linux* são ferramentas poderosas na perícia forense.
- Existem diferentes ataques que podem ser executados em sistemas operacionais *Linux*.
- A análise de logs se torna mais simples com o conhecimento de locais comuns a serem analisados.
- Rootkits auxiliam os atacantes a se camuflarem.

AUTOATIVIDADE

1 Ataques podem ser definidos de acordo com a experiência do atacante, complexidade do ambiente de rede e sistema operacional e objetivo final para qual está sendo executado. Porém independente de ser um ataque *Cracker* ou do tipo *Script Kiddle*, pode ser definido em três etapas. Sobre a enumeração, assinale a alternativa CORRETA:

a) ( ) Processo final, onde as informações são excluídas para ocultar a identidade do atacante que não quer ser descoberto.
b) ( ) Processo onde as informações são extraídas para outro sistema, garantindo que o perito forense analise as características do ambiente.
c) ( ) Todos os passos do atacante são enumerados por ele antes de iniciar o ataque para garantir que o processo esteja minunciosamente organizado.
d) ( ) É a etapa mais breve de um ataque, onde apenas as informações sobre o endereçamento do host e domínio são analisadas.

2 Nem sempre as versões e distribuições dos sistemas estão integras em toda a sua estrutura e serviços, por esse motivo, os fabricantes frequentemente lançam atualizações e correções para respectivamente reforçar a segurança do sistema e corrigir *bugs* identificados. Com base nas definições dos *exploit*, analise as sentenças a seguir:

I- Um *exploit* é aplicado quando as vulnerabilidades de aplicações, sistemas e redes passam a ser conhecidas, passando a facilitar a exploração da falha.
II- Os *exploits* são voltados para ataques direcionados para software, já que o hardware geralmente não é um alvo de ataques.
III- *Exploits* são soluções lógicas, que permitem ao atacante aplicar um código pré-definido a fim de tomar posse sobre o controle do sistema, destruí-lo ou roubar informações.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 A estrutura de um sistema operacional *Linux,* envolve diversos diretórios e entre eles estão aqueles que armazenam os arquivos temporários. De acordo com as características dos arquivos temporários, classifique V para as sentenças verdadeiras e F para as falsas:

( ) São arquivos mantidos pelo próprio sistema com o objetivo de armazenar algumas informações do sistema antes de apaga-las definitivamente para o caso de serem úteis ao administrador, usuário ou perito.
( ) Podem ser pistas utilizadas contra o atacante, quando por falta de conhecimento, os arquivos foram excluídos superficialmente e ainda puderem ser localizados.
( ) Determina que um arquivo estará no sistema somente por um período e caso não exista rotina de backup, informações importantes serão perdidas.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) V – F – V.
c) ( ) V – V – F.
d) ( ) F – F – V.

4 Quando os logs já foram analisados, mas ainda não foram coletadas informações suficientes, os diretórios precisam ser revisados, porém o atacante geralmente se livra das provas após realizar o ataque. Neste contexto, disserte sobre as áreas não acessíveis.

5 Na fase de *footprint* em um ataque, as informações são coletadas, esse processo pode ser realizado tanto manualmente, quanto com uso de ferramentas como NMAP ou *wireshark*. Neste contexto, disserte sobre algumas informações geralmente coletas em cenários de rede.

ANÁLISE DE MÁQUINAS COM SISTEMA OPERACIONAL *WINDOWS*

1 INTRODUÇÃO

Acadêmico, no Tópico 3, abordaremos sobre a análise forense em sistemas operacionais *Windows*, analisando a prática de coleta de informações do registro e de que forma esse componente pode oferecer dados sobre os serviços e a estrutura de cada um deles.

É importante lembrar que analisar a forma como os ataques alteram o comportamento de um sistema operacional é essencial para reconhecer as consequências de um ataque. Por isso abordaremos análise de *malware* em memória.

Assim como as redes locais, as redes sem fio representam ameaças e se tornam ainda mais vulneráveis à ataques por não serem implementadas contando com recursos de segurança reforçados em alguns casos, como nas redes domésticas ou de pequenas organizações. Sendo assim, iremos tratar sobre a coleta de tráfego em redes *wireless.*

2 ANÁLISE DE MÁQUINAS COM SISTEMA OPERACIONAL *WINDOWS*

Sistemas operacionais Windows são soluções proprietárias, diferente dos sistemas operacionais *Linux*, que são de código aberto, isso significa que para adquirir o sistema é necessário comprar uma licença. Esse fato faz com que ao invés de as vulnerabilidades e brechas serem identificadas pela comunidade de desenvolvedores que utiliza o software e tem a liberdade de alterá-lo aplicando melhorias, a responsabilidade é do fabricante, a Microsoft.

O primeiro conhecimento que o perito deve ter é sobre a versão do sistema operacional que está sendo utilizada, o que facilita o entendimento sobre a forma como as informações podem ser coletadas, agilizando as fases de aquisição e análise dos dados.

NOTA

Compreender as características do protocolo IP também é um pré-requisito.

Versões mais recentes do *Windows* fornecem suporte para *hardware* de ponta e tarefas de computação intensivas, trazendo maior segurança para as informações tratadas pelas aplicações e tráfego de rede.

Hassan (2019) afirma que as versões Pro for Workstations e *Windows* 10 Enterprise são altamente recomendados, a primeira oferece recursos avançados, que permitem que o próprio sistema se recupere de falhas automaticamente.

É importante ressaltar que existem versões do *Windows* voltadas para *workstations* como essas, que servem como base para usuários e versões especificamente instaladas em servidores e que são mantidas e gerenciadas pelo administrador de rede, por armazenarem serviços críticos.

Existem requisitos mínimos e recomendados para qualquer sistema operacional *Windows* funcionar. A alocação de recursos recomendados influencia em maior desempenho dos serviços. Mas e para máquinas forenses, utilizadas pelo investigador, qual seria a recomendação ideal para que se tenha um dispositivo poderoso e que possa processar e analisar as evidências digitais da melhor forma?

Computadores forenses requerem poder de processamento de alto nível, além de uma quantidade de memória RAM expressiva. Dispor de espaço de armazenamento necessário para coletar as provas é essencial no trabalho do perito e além disso, *slots* de expansão devem estar disponíveis para conectar diferentes tipos de dispositivos, já que pen drivers, discos externos e outras mídias, representam grande parte dos dispositivos utilizados e que compreendem um processo de perícia. Hassan (2019) citou recomendações de hardware:

1- **Memória RAM**: pelo menos 24 GB (DDR4).
2- **CPU**: pelo menos duas CPUs, considerando também modelos de processadores de alto nível como, por exemplo Intel i9 de 8ª geração, que possuem múltiplos núcleos de processamento em sua arquitetura.
3- **Placa mãe**: compatível com os demais dispositivos internos de *hardware*.
4- **Discos rígidos**: uma combinação de SSD e HDD - pelo menos 512 GB de SSD e 4 TB de HDD. O primeiro deles traz maior desempenho e rapidez para os processos e o segundo geralmente oferece maior armazenamento.

5- **Controlador de vídeo**: existem placas específicas para suportar processos pesados com as oferecidas pela Nvidia por exemplo.
6- **Proteção contra gravação**: para garantir a integridade das provas, principalmente das imagens do sistema a serem analisadas.

O disco rígido é o componente interno de mais interesse em perícias forense e Hassan (2019) afirma que o *Windows* organiza s discos com base em setores que formam um cluster. Ou seja, o disco é logicamente segmentado e os dados vão sendo gravados sempre em setores específicos. O mesmo ocorre quando as informações são excluídas e novos dados são reescritos no mesmo disco, mas que ainda podem ser restaurados através de *softwares* de recuperação, mesmo que deletados do sistema.

Assim como o sistema de logs do *Linux,* o *Windows* oferece diversas ferramentas nativas para coleta e análise de dados como o registro, que iremos analisar no próximo tópico.

3 COLETA DE INFORMAÇÕES DE REGISTRO

A coleta de informações é feita a partir do registro do *Windows*, um dos seus componentes centrais, ainda mais quando o assunto é a análise digital, apesar de exigir um certo conhecimento para que se possa compreender a sua funcionalidade, visto que não é um recurso frequentemente utilizado pelos usuários comuns.

O registro do *Windows* pode fornecer uma grande quantidade de informações valiosas sobre configurações do sistema, importantes no contexto digital, algumas delas são citadas por Carvey (2016):

- Histórico de informações sobre as atividades dos usuários.
- Informações sobre aplicações instaladas e acessadas pelos usuários.
- Características da conta do usuário que envolvem inclusive a aparência do desktop.
- Alterar o encapsulamento do sistema de arquivos, ou seja, evitar que sofram acessos indevidos.
- Definir que o usuário não seja capaz de remover arquivos de forma permanente, ou seja, a lixeira não pode ser ignorada, o que traz mais chances na recuperação dos dados.
- Modificar despejo de falha do sistema e configurar opções de restauração do sistema.
- Limpar o arquivo de paginação quando o sistema for desligado. O sistema de paginação representa uma extensão da memória RAM através do disco rígido, para atender as necessidades de armazenamento temporário do sistema.
- Habilitar ou desabilitar a auditoria do Registro de Eventos que exibe informações sobre atividades realizadas no sistema como adicionar, alterar ou excluir um usuário, remover de um grupo, alterar a senha, entre outros.
- Ativar ou desativar o firewall do *Windows*, o que pode afetar a segurança do sistema *Windows* e deve ser um ponto de atenção.

O registro do *Windows* é bem semelhante à um arquivo de *log,* mas é importante considerar que para analisar informações gravadas no sistema por exemplo ou análise à nível de administração do sistema, existem outras ferramentas como por exemplo, o Log de eventos.

Apesar de nem todas as informações serem armazenadas no registro, esse recurso é muito valioso para as atividades forenses. De acordo com Hassan (2019), um grande volume de informações que passa despercebido pelos analistas, pode retornar através desse componente, tendo um impacto positivo em relação às evidências coletadas.

Por exemplo, se o sistema tenta executar uma atualização, mas no registro há um valor especificado para que ela seja interrompida, alterando o seu comportamento, essa regra que vale. Outro exemplo que está diretamente ligado com a perícia forense é o seguinte: Um arquivo é criado e toda a vez que ele for acessado, irá armazenar a data, hora e usuário que o visualizou. Onde isso está definido? No registro do *Windows!*

Quando uma tarefa é executada no sistema, principalmente tendo origem da interface gráfica, algum rastro poderá ser identificado. No entanto, o registro é uma ferramenta de apoio, por isso utilizar soluções que auxiliem nessa busca, pode facilitar o trabalho de investigação.

4 ANÁLISE DE MALWARE EM MEMÓRIA

A tecnologia usada a favor da computação forense é essencial para identificar invasões de dispositivos, coletar materiais e preparar evidências, porque uma invasão é um crime.

A análise de malware na memória é um fator muito importante neste processo. Para entendê-lo, vamos primeiro definir o que é *malware:* um termo geral que inclui especificamente projetado para executar ações maliciosas em dispositivos de computação (como *phishing* e vírus) todos os tipos de programas.

4.1 TIPOS DE ANÁLISES

Sabendo disso, compreenderemos diferentes tipos de análises a partir de Lopes (2019).

4.1.1 Análise estática

Um método de investigação que envolve a análise estática pode ser aplicado à um programa ou à um código do computador sem executar qualquer programa, utilizando como recurso principal a engenharia reversa.

NOTA

Engenharia reversa é o processo de decompilar o código binário em linguagem *assembly* ou mesmo em linguagem de programação, para chegar à forma como ele foi criado.

4.1.2 Análise dinâmica

Nesse caso, o ambiente analisado é modificado, já que depende da execução de programas para ser compreendido. Dessa forma, geralmente os testes são voltados para máquinas virtuais e para não danificar o sistema ou torná-lo inutilizado, o recurso de *Snapshot* pode ser utilizado. Com isso é possível criar recortes do status da máquina e retornar para o ponto anterior, caso por algum motivo, o sistema seja danificado.

Na análise dinâmica, o comportamento do malware é avaliado de forma real, onde as ações realizadas por ele são fielmente simuladas e é possível reconhecer a forma como ele se comporta. Com esse tipo de análise é possível:

- Coletar *dumps* de memória, ou seja, mensagens de erro e logs relacionados à sua causa. Um exemplo claro está na famosa tela azul, onde é possível extrair um relatório e analisar se ela foi causada por uma atualização ou falha em *hardware* por exemplo.
- Analisar tráfego de rede.
- Monitorar operações realizadas em disco ou até mesmo injeção de código.

Na análise dinâmica, é possível avaliar o comportamento do *malware*, já que estaremos testando o ambiente e identificando quais são as tarefas responsáveis por sua execução. Por exemplo, o *malware* será executado quando o navegador for iniciado. Ou ainda, pode depender de privilégios de administradores ou ainda exigir reinicializações no sistema em determinado período para que possa aplicar suas alterações.

Ao simular o ataque identificado, é necessário descobrir as dependências impostas pelo *malware,* além disso, também é possível coletar informações sobre o atacante, como o endereçamento IP. Sendo assim, precisamos considerar alguns fatos com relação à análise de tráfego WI-FI, que iremos analisar no próximo tópico.

5 ANÁLISE DE TRÁFEGO WI-FI

É cada vez mais comum a utilização de dispositivos móveis, usuários conectam seus dispositivos de qualquer local em pontos de acesso sem fio disponíveis e com a necessidade de manter as pessoas conectadas através da internet, e possível afirmar que a segurança das informações é cada vez mais necessária. Para ferir a integridade dos dados que trafegam nesse tipo de rede, os atacantes utilizam *sniffers*.

ESTUDOS FUTUROS

Vamos falar sobre esse recurso e sobre as técnicas aplicadas, ainda neste Tópico.

As redes sem fio são representadas por um conjunto de tecnologia, conectados entre si, garantindo a transmissão de informações sobre eles sem o uso de cabeamento estruturado.

As redes *Wireless* compreendem uma das opções de conectividade mais exploradas atualmente pelos usuários, isso envolve a mobilidade, facilidade de conexão e acima de tudo a simples implementação de sua infraestrutura. Organizações mantem cada vez mais redes híbridas que envolvem parte da sua infraestrutura cabeada e pontos móveis disponíveis para conexão dos usuários e visitantes.

Todavia, o que nos importa agora, é entender como essas redes são investigadas pelos profissionais de análise digital. Tanto os atacantes como os profissionais forenses utilizam farejadores quando o assunto é análise de tráfego da rede sem fio.

IMPORTANTE

Sniffers podem ser definidos, de acordo com Basta, Basta e Brown (2015), como um farejador (em português), por isso, possui uma aplicação versátil, sendo utilizado tanto para capturar, monitorar e filtrar pacotes com a intensão de explorar vulnerabilidades e efetivar uma intrusão como para farejar pacotes suspeitos que trafegam na rede, analisando problemas e detectando anomalias. Isso tudo considerando as redes Wi-fi!

Ainda de acordo com Basta, Basta e Brown (2015) farejadores são programas inteligentes que trabalham geralmente em modo promíscuo, ou seja, utilizam uma interface camuflada na rede para detectar o tráfego de todas as demais. Um investigador é capaz de analisar pacotes de dados e detectar rastros da invasão em computadores de diversos sistemas operacionais como *Linux* e *Windows*, com o uso de *sniffers*.

A desvantagem desse tipo de ferramenta é que os mesmos softwares, com mesma arquitetura foram idealizados tanto para explorar falhas como para identificar informações sensíveis, por isso pode servir para objetivos diferentes. Ora protegendo a rede e ora tornando-a vulnerável.

Segundo Wendt (2020), o *sniffer* é uma ferramenta poderosa, mas também pode representar grande perigo quando estiver utilizada pelos cibercriminosos, com o objetivo de detectar dados de acesso de usuários, senhas, conteúdo de e-mails, arquivos, diretórios e até mesmo sites acessados.

Vamos analisar rapidamente as características dos farejadores, de acordo com a categorização definida por Basta, Basta e Brown (2015):

- Farejadores integrados: também denominados embutidos, são aqueles integrados ao sistema operacional e que podem ser utilizados de forma nativa. Alguns exemplos são *Network Monitor* (*Windows*) e o TcpDump (*Linux*).
- Farejadores comerciais, são aqueles comercializados por fabricantes terceiros compatíveis com um ou mais sistemas e que permitem customização do ambiente de acordo com a necessidade da análise e coleta de dados.
- Farejadores livres, oferecidos de forma gratuita. O mais conhecido é o *Wireshark*, que oferece uma gama de recursos e ambiente de simples manipulação.

De forma geral, os farejadores são capazes de atuar com diversos protocolos do modelo TCP/IP apesar de uma interface de rede. Ainda de acordo com Basta, Basta e Brown (2015), um farejador é definido por cinco componentes:

a) Hardware: identifica a placa de rede. Nesse caso podemos considerar também as redes cabeadas, mas nesse caso, estamos falando especificamente das redes sem fio.
b) Drive de captura. Aqui temos o software utilizado para captura seja ele nativo, comercial ou livre.
c) Buffer. Quando os dados são capturados, o armazenamento ocorre na memória temporária, denominada *buffer.*
d) Decodificador: trata de traduzir os dados compreendidos pelo computador (binários) para informações que possam ser entendidas na linguagem humana.
e) Análise de pacotes. A análise de pacotes envolve todos os componentes.

Concluímos que analise de *malwares* e de vulnerabilidades que rodeiam as redes sem fio pode ser realizada através de ferramentas especificas, porém também é necessário ter o conhecimento necessário sobre as ações que eles executam para poder combatê-los.

Ferramentas anti-*malware* representam uma ótima alternativa para aplicar ações como detecção, análise e exclusão de malware em computadores e ataques à criptografia. Alguns exemplos clássicos são os antivírus.

RESUMO DO TÓPICO 3

Neste tópico, você aprendeu:

- Os *malwares* podem causar prejuízos à rede.
- Existem diversos tipos de análises para identificar os *malwares*.
- Análise de tráfego WI-FI pode minimizar problemas de confiabilidade.
- *Sniffers* podem ser utilizados para atacar ou proteger a rede.

AUTOATIVIDADE

1 As redes sem fio trazem diversas facilidades na conexão dos usuários e são utilizadas devido a mobilidade oferecida e disponibilidade de acesso à Internet de qualquer lugar, porém existem vulnerabilidades exploradas frequentemente pelos atacantes, assinale a alternativa CORRETA:

a) ( ) A maior vulnerabilidade é em relação aos sniffers que são utilizados para quebra de criptografia que utilizam protocolos como o WEP.
b) ( ) Sniffers são utilizados para coletar informações da rede como credenciais de acesso e dados de usuários conectados à rede.
c) ( ) Diferente das redes que utilizam criptografia WEP, quando a criptografia WAP é aplicada à rede, ataques não podem ser utilizados, pois sua camada de segurança é totalmente resistente.
d) ( ) Redes sem fio geralmente são exploradas através de outra rede sem fio, sem o uso de qualquer placa de rede para detecção de SSIDs.

2 O registro de informações do *Windows* é uma ferramenta bastante útil na investigação forense e tão importante quanto arquivos de log, pois permite que alterações no sistema sejam controladas, assim como as vulnerabilidades. Com base na sua utilidade, analise as sentenças a seguir:

I- Coleta de informações e histórico de atividades de usuários cadastrados na rede com acessos devidamente criados e que utilizem logins para acesso ao sistema;
II- Permite que o administrador possa identificar qualquer software que foi instalado ou acesso pelo usuário em determinado período;
III- As atividades de usuário que podem ser monitoradas estão voltadas para processos executados via linha de coando, sem envolver informações sobre o uso da interface gráfica.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Um *siniffer* ou farejador é composto por diversos componentes que permitem que as informações possam ser coletas e analisadas na rede, classifique V para as sentenças verdadeiras e F para as falsas:

( ) Um farejador utiliza uma placa de rede para capturar o tráfego de pacotes e representa o componente físico responsável por monitorar o tráfego.
( ) Sistemas operacionais como *Linux* e *Windows* oferecem drivers de captura comerciais para atuar junto ao hardware na análise de informações.
( ) As informações tratadas pelos sistemas e aplicações precisam ser decodificadas pra que sejam compreendidas à nível da linguagem humana, por isso um decodificador é um dos componentes utilizados.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) V – F – V.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 A análise forense está diretamente ligada com a coleta de evidências e em casos onde malwares são utilizados como fonte de ataque, existem tipos de análises especificas a serem consideradas pelo perito digital. Disserte sobre esta área de concentração e sobre as diferenças entre a análise estática e dinâmica.

5 Assim como os atacantes têm o objetivo de levar vantagem com a coleta de informações em uma rede, infiltrando-se e tendo acesso a informações privilegiadas. O perito precisa ter habilidade para coletar informações e identificar de que forma as ações mal-intencionadas foram aplicadas na rede. Neste contexto, disserte sobre o uso do *sniffer* realizado por ambas as partes para diferentes fins

QUEBRA DE CHAVE WEP/WPA

1 INTRODUÇÃO

Acadêmico, no Tópico 3 discutimos sobre diversos fatores ligado com a análise e coleta de informações, inclusive da análise em redes sem fio. Uma das principais práticas em uma rede sem fio, envolve a coleta de chave de acesso para que se possa ter acesso à rede e posteriormente cometer outras ações que envolvem o cibercrime.

No Tópico 4, analisaremos o processo de quebra de chave na prática.

2 QUEBRA DE CHAVE WEP/WPA

A quebra da criptografia em rede sem fio, esteja a rede utilizando protocolos WEP e WPA, pode ser realizada com o uso de diversas técnicas. Comandos diferentes podem ser aplicados em sistema operacionais *Linux* ou *Windows,* apesar de os objetivos serem os mesmos, coletar a chave de acesso da rede.

IMPORTANTE

Existem métodos diferentes de métodos de criptografia em redes sem fio, entre eles WAP (*Wi -Fi Protected Access*) e WEP (*Wired Equivalent Privacy*). O protocolo WEP surgiu antes, porém apresentou diversos problemas de segurança, dando origem ao WAP que recebeu diversas melhorias e passou a oferecer maior privacidade aos ambientes de rede sem fio.

Segundo Wrightson (2012, tradução nossa) para que seja um atacante, capaz de quebrar a criptografia de uma rede sem fio, por mais que ela apresenta fatores evidentes de segurança, os seguintes passos precisam serem considerados:

1. Identificar a rede alvo.
2. Adicionar uma placa de rede em modo de monitoramento (promiscuo) para coletar o tráfego.
3. Armazenar tráfego coletado na rede.
4. Realizar o processo de quebra de criptografia.

Antes de conhecermos o processo de quebra de criptografia, precisamos conhecer alguns comandos, descritos no Quadro 2:

QUADRO 2 – COMANDOS *LINUX*

Comando	Descrição	Sintaxe
aircrack-ng	Quebra de encriptação de protocolos WEP e WAP.	aircrak-ng <opções><arquivo. cap>
aireplay-ng	Gerador de tráfego por meio da injeção de pacotes.	aireplay-ng <ataque><opções><monitor>
airodump-ng	Realiza a captura de pacotes	airodump-ng <opções><monitor>
airmon-ng	Habilita o modo de monitoramento na interface.	airmon-g start/stops <interface_ wireless< <canal>

FONTE: Adaptado de Wrightson (2012).

2.1 QUEBRA DE CRIPTOGRAFIA WEP

Agora considerando os passos, vamos assumir que estejamos iniciando a quebra de criptografia em uma rede sem fio que utiliza criptografia WEP. O computador utilizado pelo usuário alvo possui o sistema operacional *Linux* instalado, na distribuição *Kali Linux*, por isso iremos utilizar comandos compatíveis com esse ambiente.

IMPORTANTE

Sistemas *Windows* também permitem a aplicação dessa prática e geralmente é realizada com o uso de softwares. Outra prática é descobrir a senha através do WPS (Wi-Fi Protected Setup), ferramenta presente em roteadores que permite a descoberta da senha.

O primeiro passo é a **Identificação da rede:** Lembra que o primeiro passo em um ataque de penetração é o *scanner*? root@kali: wlist wlan0 scanning 2.

Depois a configuração correta da **placa de rede em modo de monitoramento:** Vamos iniciar a interface para que seja capaz de capturar os pacotes necessários: root@ kali: airmon-ng start wlan0.

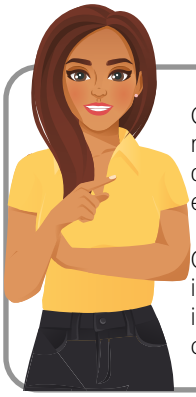
É necessário garantir que o **armazenamento do tráfego coletado** esteja ocorrendo corretamente**:** root@kali: airodump-ng -c 11 --bssid BA:66:85:1A:CB:04 -w rede _ wep wlan0. Por último, se executa o comando para efetivar a **quebra de criptografia:** aircrack-ng *.cap

DICAS

Com o parâmetro -w, os dados capturados são armazenados em um arquivo .cap

2.2 QUEBRA DE CRIPTOGRAFIA WAP

Atualmente, com a descontinuidade da criptografia WEP, algumas outras técnicas foram desenvolvidas. Por ser essa criptografia mais complexa, um passo adicional deve ser implementado no processo.



IMPORTANTE

Considerando que as redes sem fio que utilizam o protocolo WPA, são mais seguras, para descriptografar senhas nesse cenário, necessitamos da informação do *handshake*, processo que ocorre quando os dispositivos estabelecem uma conexão com o ponto de acesso.

O *handshake* pode ser entendido como um acordo em que as máquinas que irão se comunicar, afirmam que reconheceram umas às outras e aceitam o início da comunicação. O *handshake* é utilizado em diversos protocolos de comunicaão além do WAP, entre eles: FTP, TCP, HTTP e SMTP.

O primeiro passo é a **identificação da rede**: lembra que o primeiro passo em um ataque de penetração é o *scanner*? root@kali: airmon-ng

Aqui estamos coletando informações sobre a placa de rede que iremos utilizar para buscar as redes sem fio, identificando as que estão nas proximidades, escolhendo o alvo: root@kali: iwlist wlan0 scanning

Depois é necessário configurar a **placa de rede em modo de monitoramento,** iniciando a interface para que seja capaz de capturar os pacotes necessários: O modo promiscuo é habilitado com o comando airmon-ng.

Nesse cenário, primeiramente vamos utilizá-lo para analisar se algum processo pode vir a interferir no processo de invasão, com o seguinte comando: root@kali: airmon-ng check kill. Após, é necessário identificar se existe algum processo em andamento. Caso haja, basta encerrá-lo através do seu PID:root@kali: airmon-ng check kill 1022.

Para **armazenar o tráfego coletado**, o que garante receber as informações a serem armazenadas, podemos utilizar o seguinte comando: root@kali: airodump-ng -c 11 --bssid C0:3D:D9:69:3E:90. -w. Com esse comando é possível validar todos os dispositivos que estão conectados no ponto de acesso da rede.

Diferente do que ocorre na quebra de chave WEP, nesse caso, teremos um passo adicional, a desautenticação de dispositivo. O processo acontece quando um usuário se conecta na rede e sua reconexão é forçada, assim é possível coletar informações como endereço do ponto de acesso e do dispositivo: root@kali: aireplay-ng --deauth 0 -a C0:3D:D9:69:3E:90 -c C8:F7:33:7B:65:3D wlan0

Se tudo ocorrer como planejado, ao rodar o comando, assim que o dispositivo for reconectado, uma mensagem retorna no terminal.

Por último, temos a quebra de criptografia, onde o processo de força bruta é aplicado. Esse tipo de ataque é executado através da execução de uma séria de combinações possíveis em determinados parâmetros serão testadas no arquivo criptografado com a informação do *handshake*.

A lista de palavras geralmente é armazenada em um arquivo no formato .txt e pode ser executada em paralelo com a quebra da senha. O comando crunch pode ser utilizado para criação da lista de palavras. Atente-se a seguinte linha de comando: root@kali: crunch 10 10 ABCDEFGHIJKLMNO0123456789 -t FBA4E@@@@@ | aircrack-ng /home/kali/exemplo-01.cap -w - -e VIVOFIBRA-3E90

Nesta linha de comando, o parâmetro -w indica o caminho da lista de palavras que usaremos para quebrar a senha, e o comando -e indica qual a rede sem fio a ser criptografada (quebra a rede utilizando seu nome). O tempo que será gasto no processo depende da complexidade da senha e do tamanho. Se existem caracteres especiais, letras e números, provavelmente a quebra será um pouco mais difícil e até mesmo não ser possível.

Como vimos, existem técnicas de ataque a redes sem fio voltadas para características e protocolos diferentes, o que também ganha mais complexidade considerando o nível de segurança aplicado a rede, minimizando e muitas vezes impedindo que ações mal-intencionadas ocorram.

Conhecemos também algumas ferramentas (comandos nativos) utilizados no sistema *Linux* que servem como facilitadora para os ataques, estabelecendo um processo que envolve desde a identificação da rede até a desautenticação de dispositivos e a quebra das redes criptografas encontradas. Um exemplo passo a passo reforçou nosso conhecimento.

É importante lembrar que em muitos casos, a perícia forense envolve a exploração de ambientes, por isso, atividades como essas não são apenas utilizadas por cibercriminosos mas também por profissionais da segurança, que precisam ter acesso à determinada rede e utilizam os recursos para alcançar seus objetivos

RESUMO DO TÓPICO 4

Neste tópico, você aprendeu:

- É possível realizar a quebra dos protocolos WAP e WEB com ferramentas nativas.
- Descobrir a senha de um usuário conectado à rede sem fio.
- Explorar informações criptografadas para acessar uma rede protegida.
- Coletar tráfego de rede através do sistema operacional *Linux*.

AUTOATIVIDADE

1 Existem situações em que processos específicos que estejam rodando na rede possa interferir na quebra de criptografia de uma rede sem fio, como por exemplo um antivírus. Sobre a forma como um software que está rodando no sistema pode ser encerrado através do terminal, assinale a alternativa CORRETA:

a) ( ) airmon-ng check kill 1054.
b) ( ) airmon-ng check process 1054.
c) ( ) airmon-ng create process 1054.
d) ( ) airmon-ng kill 1054.

2 Existem algumas características no ambiente que tornam a quebra da segurança de uma rede sem fio, um processo mais demorado ou até mesmo a impossibilidade de furar a criptografia, interceptando a senha do usuário, analise as sentenças a seguir:

I- O protocolo WAP possui uma estrutura mais complexa que o protocolo WEP, por isso, atacar uma rede sem fio com esse protocolo, torna-se mais difícil.
II- A complexidade da senha define a duração do processo de quebra de senha, por isso quanto mais caracteres e variedade de elementos da senha, se tornam mais trabalhoso.
III- Somente o sistema operacional *Linux* permite a quebra de criptografia tanto para o protocolo WEP ou WAP, por ser mais vulnerável.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Na quebra de senha do protocolo WAP, um processo adicional compõe o passo a passo estabelecido para a quebra de senha, denominado desautenticação, analise as sentenças a seguir:

I- Ocorre um processo denominado *handshake, responsável* por estabelecer a confiabilidade entre as duas pontas e estabelecer a comunicação.
II- O dispositivo do cliente é desconectado e a reconexão é restabelecida, esse tempo é utilizado para que se possa interceptar as informações.
III- Desautenticação é o processo no qual o perito desabilita o acesso do atacante através das credenciais coletadas e armazenadas no processo de quebra de senha.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

4 O primeiro passo na quebra de criptografia é identificar a rede que será atacada, utilizando a placa em modo de monitoramento, porém existe outro passo importante, no qual o comando root@kali: iwlist wlan0 scanning é utilizado. Disserte sobre a sua funcionalidade.

5 Protocolos de criptografia por mais que tenham a mesma finalidade, possuem características importantes, em relação a quebra de uma chave WAP, o procedimento requer mais conhecimento e tempo para efetivar o processo. Neste contexto, disserte sobre como o ataque de força bruta é aplicado.

ANÁLISE DE TRÁFEGO VOIP

1 INTRODUÇÃO

Acadêmico, no Tópico 5, abordaremos algumas características importantes no sistema VoIP, entendendo as semelhanças dos ataques e vulnerabilidades com outros dispositivos e recursos computacionais. Iremos revisar passos importantes da análise forense e do tratamento das evidências.

Relacionaremos as etapas de perícia forense aplicadas aos sistemas operacionais *Linux* e *Windows,* aos PBX e como as boas práticas podem auxiliar o perito no processo de análise forense.

2 A SEGURANÇA DO SISTEMA VoIP

A evolução dos sistemas VoIP (voz sobre IP) foi essencial para a modernização dos telefones e comunicação realizada através de dispositivos analógicos, que deram origem a era da comunicação.

Sistemas VoIP envolvem a padronização de serviços como os PBXs (Private Branch Exchange) tradicionais que utilizavam como base sistemas operacionais proprietários, mas com o passar do tempo, muitas das soluções passaram a ser baseadas em sistemas UNIX – *Linux*, com foco na comunicação de código aberto, fornecendo maior acessibilidade para organizações que precisassem inovar com o uso de VoIP sem precisar arcar com custos altos.

IMPORTANTE

Antes de qualquer coisa é necessário considerar que VoIP é o sistema que funciona por trás de uma estrutura PBX(central telefônica), ou seja, enquanto PBX é um sistema de troca de ramais utilizado exclusivamente por empresas, VoIP é uma tecnologia que utiliza banda larga ou voz sobre banda larga como base para realizar o roteamento de conversação humana através da Internet ou qualquer outra rede de computadores baseada em protocolos que suportem o tráfego de voz e dados.

Por serem soluções bem similares aos computadores, por utilizarem sistemas operacionais e aplicações desenvolvidas por profissionais de TI, contendo também recursos de segurança. É possível que da mesma forma, os atacantes alimentem conhecimento sobre sua estrutura e possam implementar *malware* de forma eficaz.

De acordo com Androulidakis (2016), as interrupções podem ser mais críticas em ambientes de telefonia, uma vez que sua estrutura, isso se deve a convergência de sua infraestrutura, já que apesar de ser adaptada à tecnologia, suas mudanças não ocorrem tão frequentemente como nos computadores, o que traz aos atacantes maior possibilidade de conhecer suas características.

A análise de tráfego em redes VoIP pode ser bastante complexa, uma vez que um malware PBX poderia ser capaz de diversas intervenções como por exemplo, o desligamento de equipamentos e dispositivos de telecomunicações, intercepção de chamadas confidenciais, coleta de dados de registros de chamadas, entre outros.

Com relação aos procedimentos forenses, Androulidakis (2016) afirma que alguns pontos devem ser considerados:

- Questões legais devem ser aplicadas sempre que uma perícia for realizada, para garantir a conformidade com a lei.
- As evidências na análise VoIP não devem ser alteradas, assim como em qualquer outro recurso computacional periciado.
- Qualquer investigador que terá acesso à determinada prova ou ambiente suspeito, deve ser devidamente treinado sobre como prosseguir.
- Qualquer atividade desde a coleta de informações até a análise, deve ser documentada, para que se possa revisar e tomar ações necessárias em relação as provas coletadas.
- O perito sempre será responsável por suas ações, enquanto a prova digital estiver em sua posse.

Com relação aos princípios fundamentais e boas práticas que tangem a análise VoIP, Androulidakis (2016) também aponta os seguintes, relacionados com os pontos necessários:

1. Qualquer ação tomada por agências de aplicação da lei ou seus agentes não deve alterar os dados mantidos e armazenados, seja em um computador ou qualquer outro dispositivo de armazenamento;
2. Em circunstâncias especiais, quando uma pessoa achar necessário acessar os dados originais armazenados em um computador ou meio de armazenamento, a pessoa ser capaz de comprovar a necessidade de acesso e garantir que isso não afete de qualquer forma, as evidências;
3. Todos os processos que descrevam evidências importantes devem ser registrados, a fim de que os resultados possam ser atendidos sempre que necessário;
4. Os princípios precisam ser respeitados por todos os envolvidos no processo de perícia.

Nos próximos tópicos, analisaremos alguns passos importantes na análise de tráfego VoIP.

3 COLETA DE EVIDÊNCIAS

Em exames aplicados às arquiteturas VoIP, é necessário que os dados extraídos garantindo a integridade dos dados. É necessário que a cena seja devidamente protegida e isso envolve tanto as evidências digitais (dados), como as evidências físicas (nesse caso, os aparelhos de telefone).

Quando um sistema VoIP precisa ser analisado, através do reconhecimento de suas características, as ferramentas e metodologias adequadas são selecionadas e o perito deve buscar informações sobre quem, onde e quando os dados serão examinados. É importante que se tenha conhecimento sobre a posse dos telefones no momento que a atividade suspeita ocorreu, antes mesmo de que o exame nos dados seja iniciado. Em um exame minucioso é necessário categorizar os eventos, sem que qualquer evidência seja ocultada.

Todavia, quais são os riscos aos quais um sistema VoIP está exposto? Vamos analisar alguns deles? Diversos motivos levam à ataques em sistemas VoIP como impedir a utilização de serviços, interceptar chamadas de cunho confidenciais com objetivo de utilizar os dados para determinado fim ou utilizá-las indevidamente. Guimarães (2021) cita algumas técnicas:

- *Caller ID Spoofing:* o *hacker* identifica o número utilizado pela organização ou usuário para realização de chamadas VoIP, clonando as informações para fins maliciosos e passa a utilizar as informações a seu favor. Por isso, o termo *spoofing* remete nos ao ato de 'enganar', considerando que os serviços são clonados e um terceiro passa a ter acesso aos e-mails, por exemplo, infiltrando-se na rede e causando danos, muitas vezes irreversíveis.
- *Ataques de DTMF (Dual Tone Multi Frequency):* essa técnica permite que o atacante possa interceptar os números digitados através dos sons digitados no teclado, hackeando a linha e rastreando chamadas, identificando informações como CPF, informações de cartão de crédito, entre outras informações.
- Toll Fraud: nesse caso, ligações de longa distância são realizadas utilizando a linha interceptada, gerando custos que ficam a cargo de quem foi *hackeado.* Esse tipo de ataque se torna mais complexo de ser interceptado pelo perito digital e geralmente são ocasionados por deficiências sérias na segurança do sistema VoIP.
- *Call Hijacking:* o alvo são instituições públicas, governos e figuras de grande importância, que têm suas informações roubadas, por atacantes que se passam pela vítima em chamadas confidenciais para ter acesso às informações privilegiadas.

DICAS

Um recurso bastante útil em análises de sistema VoIP são os logs que garantem o retorno de detalhes de tempo como a hora em que o evento suspeito ocorreu, a ação e seu resultado que gerou como maleficio para a parte que solicita tal análise. Ao seguir as instruções que o log revela, o perito deve ser capaz de chegar ao mesmo resultado, compreendendo como o ataque ocorreu e depois ir atrás de informações que revelem sua fonte.

Quando esse processo é realizado, a gravação em vídeo é essencial para comprovar como a operação foi realizada e a veracidade da simulação. Também pode ser usado para verificar os resultados. As ferramentas e a versão do software devem sempre constar nos relatórios, para que a documentação seja válida.

4 PRESERVAÇÃO DE DADOS NA REDE

O princípio da perícia é a preservação dos dados, por isso, assim como todas as perícias, é necessário garantir que os dados não sofram qualquer alteração que não sejam provenientes do ataque. Para tanto, é aconselhável utilizar somente *softwares* confiáveis que não interfiram na integridade das evidências.

No entanto, Androulidakis (2016) afirma que atualmente, as ferramentas clássicas de TI, especializadas para sistemas operacionais, também podem ser utilizadas para auxiliar em procedimentos forense de tecnologias VoIP.

5 IDENTIFICAÇÃO DE DADOS

A primeira tarefa relacionada com o processo de identificação dos dados está em identificar o modelo do equipamento que será evidenciado, conectar o equipamento no ambiente de testes ou na própria rede de origem onde será analisada, familiarizar-se com os manuais técnicos e preparar os recursos básicos para dar início à análise.

Para atender aos requisitos de segurança e integridade de dados, os examinadores devem compreender o design do dispositivo e explorar os componentes eletrônicos e mecânicos e as interfaces. Ao mesmo tempo, antes de finalmente extrair os dados, deve calcular o tempo necessário para perícia e o custo envolvido no processo.

6 EXAME DE EVIDÊNCIAS

A tarefa real do exame de evidências contém a análise de registros de chamadas, registros de usuários, registros de alterações, conteúdos de memória de telefones e conexões que geralmente estão localizadas no disco rígido (HDD) do servidor configurado para uso de VoIP ou na memória de dispositivos telefones próprios para soluções PABX. Um recurso importante a ser considerado é o *hash.*

NOTA

O hash contém uma assinatura de impressão digital exclusiva para cada arquivo, obtida por algoritmos especiais e garante que os valores e arquivos de configurações não foram alterados para extrair informações ou efetivar o ataque. O hash pode retornar resultados e informações importantes, que não foram coletadas através de softwares ou ferramentas utilizadas.

7 RELATÓRIO DE DESCOBERTAS

O processo termina com um relatório das conclusões da investigação, que regista o processo seguido e as próprias provas. A seguir, apresenta-se o software e as ferramentas usadas, assim como os métodos e etapas executadas.

Os materiais e equipamentos de monitoramento utilizados, bem como a utilização de sistemas automatizados que possam ter sido aplicados para extração de informações, bem como processos manuais. O relatório será encerrado com uma conclusão, o que é fundamental para o processo de julgamento.

Por fim, as evidências extraídas devem ser verificadas. Se possível, uma verificação cruzada pode ser solicitada para o operador de rede, que se vê na obrigação de fornecer qualquer informação. Por exemplo, chamadas registradas na base do provedor, comparadas com os registros coletados, para comprovar a veracidade, evitando qualquer contestação.

RESUMO DO TÓPICO 5

Neste tópico, você aprendeu:

- Soluções VoIP estão suscetíveis aos mesmos problemas técnicos que os computadores.
- A análise deve considerar especificações técnicas em cada cenário.
- Os ataques possuem características diferentes e devem ser devidamente consideradas.
- O relatório deve ser composto de informações completas para auxiliar na análise final.

AUTOATIVIDADE

1 Procedimentos forenses em sistemas VoIP são compostos por diversas etapas a fim de compreender a finalidade dos ataques em relação ao ataque executado pelo *hacker,* que geralmente estão relacionadas com a interceptação de informações importantes que trafegam nas linhas telefônicas e softwares utilizados para transmissão de voz e dados sobre IP. A partir deste contexto, assinale a alternativa INCORRETA:

a) ( ) O perito por estar protegido por lei, pode realizar suas atividades sem precisar adotar qualquer questão legal.
b) ( ) evidências coletas para realização da análise de sistemas VoIP não pode ser alteradas em qualquer hipótese.
c) ( ) a documentação das evidências é uma etapa obrigatório para provar as características do ambiente periciado.
d) ( ) Enquanto as provas estiverem sendo produzidas, qualquer alteração ou incidente que envolva o ambiente VoIP é responsabilidade do perito.

2 Para realizar uma perícia forense, o investigador deve ter conhecimento sobre as técnicas frequentemente aplicadas pelos atacantes e existem métodos específicos que caracterizam o objetivo que o leva a cometer a ação. Com base nas definições das técnicas, analise as sentenças a seguir:

I- Em um caller ID Spoofing, ligações de longa distância são realizadas utilizando informações de telefones ou soluções VoIP clonados.
II- Por meio de um call Hijacking, organizações que hospedam informações importantes são atacadas, suas linhas passam a ser utilizadas para chamadas privadas e coleta de dados.
III- Ataques DTMF permitem que os sons emitidos pelo teclado possam ser interceptados e alterados, direcionando ligações para outros destinatários.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 A análise em um sistema VoIP tem diversas particularidades, assim como ocorrem nas estruturas dos sistemas operacionais *Linux* e *Windows*. Nesse tipo de ataque, quem o executa, encontra uma oportunidade de se infiltrar na rede, estando mal-intencionado e tendo como principal alvo, um ambiente empresarial. Com base no exposto, classifique V para as sentenças verdadeiras e F para as falsas:

( ) O desligamento de equipamentos e dispositivos de telecomunicações é um dos objetivos de ataques em análises de tráfego VoIP.
( ) Ao interceptar chamada confidenciais, diversos prejuízos podem ser causados, sendo o maior deles um risco financeiro, por isso o perito deve rastrear essas ações.
( ) A coleta de dados não pode ser realizada através de um sistema VoIP, mas o perito deve sempre analisar informações como chamadas registradas e histórico de ligações.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – V – F.
b) ( ) V – F – V.
c) ( ) F – V – F.
d) ( ) F – F – V.

4 A perícia forense digital é a área responsável por analisar e investigar crimes na Internet, coletando evidências em sistemas computacionais. Comente sobre qual das técnicas utilizadas é mais difícil de ser interceptada por um perito digital e quais suas características.

5 A coleta de informações é importante, assim como a preservação de provas, porém documentar o cenário, os testes, simulações e resultados, é uma etapa importante. Neste contexto, disserte sobre a documentação na perícia forense na análise de tráfego VoIP.

PRÁTICAS DE COMPUTAÇÃO FORENSE

1 INTRODUÇÃO

Com o avanço da tecnologia e o aumento dos crimes na Internet vem crescendo na mesma proporção que a necessidade de peritos digitais passam a ser procurados para analisar e solucionar os problemas que descrevemos no decorrer dos tópicos. A perícia forense em sistemas operacionais como *Windows* e Linux foi estendida para sistemas de telefonia VoIP que também se tornam cada vez mais essenciais em uma infraestrutura de rede, assim como os roteadores, computadores e outros dispositivos de rede indispensáveis.

Tanto para que se possa realizar corretamente a análise e coleta de evidências, os procedimentos são regularizados por lei, par que possam ser considerados como válidos na etapa de julgamento, por isso toda e qualquer evidência deve ser autenticada por lei.

Sabendo como as evidências são importantes, assim como as ferramentas que envolvem análise de logs, registros e qualquer outra prova digital, é importante sabermos que as provas devem ser corretamente categorizadas. De acordo com Costa (2008), as provas podem ser categorizadas da seguinte forma:

QUADRO 3 – CATEGORIZAÇÃO DE PROVAS

FONTE: Adaptado de Costa (2008)

Costa (2008) ainda aponta que quando o assunto são os crimes computacionais, as provas são classificas pelas normas SWGDE (*Scientific Working Group on Digital Evidence*) / IOCE (*The International Organization of Computer Evidence*), para saber quando essas normas se aplicam, podemos definir as provas digitais como qualquer informação que tenha valor para um processo penal e que esteja armazenada ou sendo transmitida por meio digital em formato de dados.

Por sua vez, dados são qualquer objeto associado à um item físico capaz de dar origem aos dados digitais, aqui se encaixam dispositivos móveis, mídias removíveis ou qualquer outro equipamento que possa ser utilizado de maneira mal-intencionada.

Por mais que já tenhamos conhecimento básico sobre as ferramentas que podem ser utilizadas a favor de descobrir as formas de ataques, suas origens, causas e consequências, precisamos compreender quais são os princípios básicos que envolvem a prática da perícia forense, considerados importantes para os profissionais da área. Vamos revisá-las!

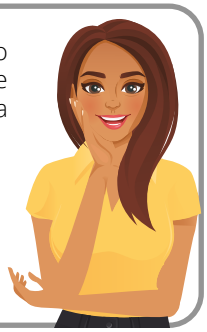
- As provas devem ser obtidas de maneira legal, geralmente por meio de um mandato de busca e apreensão.
- A prova original sempre deve ser preservada, por isso os profissionais protegem o recurso contra alterações ou reproduzem um clono do ambiente para explorar as falhas e provas.
- Quando cópias são realizadas, mídias limpas devem ser utilizadas para não causar mal à integridade da prova e evitar a propagação de vírus.
- As evidências devem ser devidamente etiquetadas, documentadas e preservadas em detalhes a maneira que a perícia evolui.
- Em alguns casos, o desligamento dos equipamentos deve ser evitado, à menos que o profissional tenha pleno conhecimento do cenário em que está lidando. Costa (2008) afirma que essa prática evita que mecanismos implantados pelos criminosos como cavalos de Tróia e outras ameaças programadas possam destruir as provas quando o equipamento for desligado ou manipulado de maneira incorreta.

NOTA

Métodos que envolvam uma ação necessária por parte da vítima como desligar o sistema para aplicar as alterações, é geralmente aplicado aos sistemas baseados em UNIX. Para evitar que as informações sejam perdidas e o sistema danificado, o indicado é alterar conta de usuário através do comando *su*, para um usuário comum sem privilégios de root que possa interferir nessa ação, por um descuido em que o atacante conhecia ou descobriu a senha. Só depois disso, é seguro desligar o equipamento através do comando *halt* via terminal.

O comando *halt* instrui o hardware a finalizar todas as funções que estão sendo executadas pelo CPU, mantendo-o em um estado de manutenção de baixo nível somente rodando os serviços essenciais e confiáveis do sistema antes de desligar ou reiniciar.
Alguns exemplos:

```
# halt -p    >>>executa um poweroff
# halt --reboot    >>> reinicia a máquina
# halt              >>>> desliga a máquina
```



Outra prática que deve ser seguida antes mesmo de iniciar a perícia é medir a extensão da cena a ser analisada, definindo o perímetro. Pois em muitos casos, não existe somente um equipamento a ser periciado, mas uma sala inteira ou até mesmo um prédio inteiro. Essa prática é necessária para medir a complexidade do ambiente.

Sobre as práticas adequadas para se liderar uma equipe que atua em determinado cenário, Costa (2008) acrescenta que é necessário que um policial investigador esteja a frente do time coordenando a operação direcionando a pesquisa e análise das evidências e determinando quais são os fatores importantes que envolvam qualquer atividade relacionada com:

- Equipamentos a serem periciados incluindo notebooks, computadores, scanners, PDA, dispositivos móveis.
- Mídias removíveis como disquetes, cd's, pen drivers, discos externos.
- Manuais, notas e observações que possam ser utilizadas a favor da cena do crime.

IMPORTANTE

É importante salientar que nem sempre é possível preservar as evidências frágeis e temporárias, já que existem casos em que as provas podem desaparecer antes dos investigadores chegarem, como informações dinâmicas que estão sendo exibidas no monitor e podem ser alteradas constantemente, por isso, em alguns casos, a agilidade é essencial para preservar ou gravar estas evidências.

A preservação de evidências deve sempre ser considerada em todas as fases de um caso forense como pudemos observar em todos os tópicos abordados na Unidade 3. O comportamento impróprio de qualquer elemento que faça parte da análise e até mesmo da própria evidência pode fazer com que a outra parte questione os métodos e procedimentos realizados para preservá-los e toda a perícia forense seja desconsiderada.

Por mais precisa que seja a tecnologia de computação, mais relevantes são as evidências encontradas e a forma como são mantidas em sua versão original e corretamente justificadas. A área de computação forense ainda enfrenta desafios, incluindo a transformação e a evolução tecnológica, novos equipamentos e sistemas e até mesmo as metodologias que são aprimoradas a cada dia, por isso todas as etapas do processo realizado por especialistas, principalmente nas etapas de coleta e análise, devem ser realizadas com muito cuidado para aumentar a confiabilidade das evidências.

A computação forense e os profissionais que executam essa profissão, diferente dos demais, precisam dominar novas tecnologias, mas também as obsoletas, ou pelo menos ter a capacidade de entendê-las rapidamente.

Conclui-se que a perícia informática deve estar preparada para assumir a responsabilidade de identificar e preservar os vestígios digitais que possam ser deixados durante a execução de crimes envolvendo informática e tecnologia eletrônica, além de sempre considerar a legislação vigente ao manipular, preservar e analisar recursos computacionais.

LEITURA COMPLEMENTAR

ANÁLISE DE VULNERABILIDADES DA REDE WIRELESS NA FACULDADE DE TECNOLOGIA DA SERRA GAÚCHA

Petter Lopes

RESUMO

O presente artigo tem como objetivo demonstrar visões diversas sobre técnicas de *sniffing* em redes *Wireless*. Com o crescente aumento da necessidade de manter as pessoas conectadas, as redes *Wireless* passam a ser a válvula de escape para solucionar essa demanda. No entanto, como funcionam exatamente essas redes? Questões relacionadas às atividades profissionais de análise digitais com o uso de farejadores de rede, que são programas que tem a função de capturar os pacotes que trafegam na rede, porém fica evidente a dificuldade de manter-se seguro em um ambiente assim. Detectar falhas de segurança, possibilitar invasões e evasão de dados, analisar de forma simples e direta as informações que trafegam na rede em um determinado momento. Obter dados sensíveis de usuários em um ambiente misto, onde todos estão conectados com dispositivos diferentes, porém utilizando a tecnologia *Wireless*. Como funciona o envenenamento da tabela ARP e como utilizar para coletar informações sensíveis.

1 INTRODUÇÃO [...]

2 REFERENCIAL TEÓRICO [...]

2.2 REDE *WIRELESS*

Wireless é conjunto de tecnologias sem fio que podem conectar tudo, desde computadores de escritórios a utensílios domésticos. Segundo Tanenbaum (2003), a comunicação digital wireless não é uma ideia nova, visto que Guglielmo Marconi, no ano de 1901, fez uma demonstração de tráfego wireless de um telégrafo que transmitia informações de um navio para o litoral utilizando código Morse, demonstrando a ideia do funcionamento das redes wireless.

Em um ambiente de rede local seu emprego é importante para que computadores portáteis estabeleçam uma comunicação. Redes wireless passam a ser uma alternativa viável dificultando ou até mesmo impossibilitando a instalação de cabos de fibra ótica ou metálicos. Conforme afirma Soares (1995).

Por outro lado, para Pinheiro (2003), para atender a demanda de comunicação onde a infraestrutura cabeada não pode ser aplicada as redes wireless são soluções normalmente aplicadas, pois viabiliza-se devido ao fato de possuir a mesma eficiência. No entanto deve-se avaliar a relação custo/benefício para que sempre seja menor que a unidade, a fim de tornar o empreendimento viável. Entretanto, para Cardoso (2005), reduções de custos, satisfação do cliente e otimizações do trabalho mostram como a tecnologia wireless torna-se relevante para as organizações.

2.3 FAREJADORES

Segundo Basta e Brown (2015), farejador (sniffer [1], em inglês), mais comumente conhecido como farejador de pacotes, trata-se de uma aplicação desenvolvida para capturar, monitorar e filtrar os pacotes de dados que trafegam em uma rede. Um farejador pode ser implementado tanto para análise de redes para detectar problemas e anomalias quanto para explorar vulnerabilidades nas implementações de protocolos aberto, onde os dados podem ser interpretados em texto puro.

Ainda de acordo com Basta e Brown (2015) farejadores, são programas que trabalham utilizando uma interface de rede do computador em modo promíscuo, o uso de farejadores para analisar os pacotes de dados em um teste de invasão é recomendado pois é quase impossível detectá-lo e pode ser executado em qualquer computador independente de sua plataforma de sistema operacional.

De acordo com Nakamura (2007), farejamento ou sniffing é uma técnica muito utilizada, visto que algumas ferramentas de administração de rede e segurança utilizam os mesmos softwares, os mesmos consistem em capturar os pacotes que trafegam na rede e verificar o seu conteúdo. Os mesmos softwares [2] que foram criados para verificar problemas de rede são utilizados por usuários sem ética para identificar informações sensíveis e explorar falhas em sua proteção.

Segundo Wendt e Nogueira Jorge (2012), cibercriminosos utilizam os sniffers normalmente para detectar dados de acesso de usuários de computador, bem como, senhas, conteúdo de e-mails, sites acessados. Para os autores o sniffer tem como principal objetivo monitorar todo o tráfego da rede, para então, posteriormente analisar todos os dados transmitidos durante a interceptação.

Para Basta e Brown (2015), existem 3 tipos de farejadores, os embutidos que vem instalados no sistema operacional a exemplo do Network Monitor (embutido no Windows) e o TcpDump (embutido no Linux), farejadores comerciais que por sua definição devem ser comprados e possuem algum suporte personalizado e os farejadores livres como por exemplo o Wireshark [3] que não geram custo.

Segundo afirmam os autores Basta e Brown (2015), basicamente os farejadores conseguem trabalhar com todos os protocolos da rede modelo TCP/IP[4], no entanto para observar o tráfego de rede o farejador utiliza o cartão de interface de rede (NIC)

sendo esse responsável por receber o tráfego no segmento de rede em que se encontra. Deste modo o farejador somente conseguirá ler o tráfego no segmento de rede em que o computador estiver conectado, necessitando por sua vez de outras técnicas para alcançar a comunicação dos outros segmentos.

De acordo com Basta e Brown (2015), um farejador é composto por 5 componentes básicos, que são: a) Hardware; b) Drive de captura; c) Buffer; d) Decodificador; e) Análise de pacotes.

Hardware [5] ou o NIC [6], é a própria placa de rede que pode ser cabeada ou Wireless (sem fio).

Driver de Captura, é o programa responsável por capturar o tráfego de rede a partir do hardware, o mesmo filtra as informações e as armazena em buffer [7]**.**

Buffer, após captura os dados o farejador os armazena em um buffer na memória. Se o buffer ficar cheio poderá haver um estouro de buffer, no entanto ainda há uma segunda maneira de armazenar as informações, denomina-se round-robin [8] técnica que gera um buffer circular onde os dados mais antigos serão substituídos pelos mais recentes.

Decodificador, responsável por transformar os dados binários em informações mais legíveis para os seres humanos.

Análise de pacotes, este pode ser em tempo real, ou seja, todos os passos são executados até chegar na análise e exibidos em tempo de execução para o usuário.

2.4 MAN-IN-THE-MIDDLE

Esse ataque consiste em manter o atacante entre a vítima e o serviço a qual ela deseja acessar em um ambiente de rede, por isso dá-se o nome de Man-In-The-Middle ou MITM que na tradução para o português significa "Homem no Meio". O objetivo deste ataque é coletar as informações da vítima de forma precisa.

Para Cunha (2006), este é um ataque que consistem em possibilitar ao atacante a capacidade de ler, modificar e inserir mensagens entre duas entidades, de modo que estas fiquem sem o conhecimento que a ligação entre ambas está comprometida.

Segundo Vieira (2008) o exemplo na Figura 1 (Vieira, 2008) exemplifica o processo do MITM. O atacante que utiliza o dispositivo computacional C, envia uma resposta ARP para dizer à B que o IP de A pertence ao endereço MAC de C, neste momento outra resposta é enviada à A, dizendo que o IP [9] de B pertence ao endereço MAC de C.

Visto que o ARP mantém o cache os dispositivos computacionais A e B confirmam então que o envio da requisição ARP já foi efetuado anteriormente e atualizaram seus caches ARP com esta nova informação. [...]

Neste momento quando A enviar dados para B, ele vai para C. O dispositivo computacional C pode usar esta posição única para direcionar os dados para o dispositivo computacional correto e monitorá-los ou modificá-los à medida que eles passam por C tornando o processo de MITM consolidado como visto na Figura 2 (Vieira, 2008). Ainda para Vieira (2008) o Man-in-The-Middle vem a ser possibilitado por meio do envenenamento da rede com a técnica de ARP Poisoning.

2.5 ARP *CACHE POISONING*

Para Bernal (2000), toda a comunicação baseada na arquitetura TCP/IP é realizada por meio do endereçamento IP, entretanto em redes locais essa comunicação dá-se por meio de pacotes ethernet. Ainda segundo BERNAL (2000), se um pacote é transmitido com endereço IP, faz-se necessário a tradução deste endereço para o endereço físico, para tal processo é utilizado o protocolo ARP [10].

O protocolo ARP (Address Resolution Protocol ou Protocolo de resolução de endereços) foi desenvolvido para mapear endereços IP para endereço físico. Um dispositivo computacional A com a endereço 192.168.0.1 pretende comunicar-se com o dispositivo computacional C de endereço 192.168.0.3, o dispositivo computacional A manda um pacote de broadcast[11] 2 perguntando quem tem o endereço 192.168.0.3, o dispositivo computacional C responde com o seu endereço físico 00:AA:11:BB:22:CC.

Para saber o endereço físico de destino do dispositivo computacional, o protocolo ARP manda um pacote de broadcast. Entretanto, pelo fato do pacote broadcast ocupar muito a rede, torna-se inviável realizar este procedimento toda vez que haja a necessidade de comunicação entre dois pontos da rede. Para isso, utiliza-se o ARP cache, uma lista que armazena os endereços IP's associados aos endereços físicos dos dispositivos computacionais da rede, entretanto vale ressaltar que esta lista é armazenada com requisições anteriores (SOUZA, 2010).

Tanto para Vieira (2008) quanta para Weidman (2014) esta é uma técnica muito precisa, onde todo o tráfego de rede passa a ser redirecionado para o atacante. Deste modo é possível interceptar todo o tráfego da rede e obter dados sigilosos dos usuários, bem como acesso a outros sistemas a exemplo de e-mails, portais de trabalho. É possível também tornar a rede indisponível gerando um alto tráfego de dados aleatórios, bem como a disseminar malwares [12].

Ainda para Weidman (2014) e Vieira (2008), para um teste preciso com informações já filtradas ao que dizem respeito a informações de usuários como dados confidenciais de acesso, o Ettercap é a ferramenta mais recomendada.

3 METODOLOGIA [...]

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Neste capítulo, discutiremos a amostragem dos dados com base nos conceitos das técnicas apresentadas, qualquer dado sensível que seja detectado, será devidamente ocultado para preservação da identidade dos usuários da rede wireless.

Nos testes realizados utilizando a técnica de ARP Poisoning foi possível identificar os dados de autenticação de alguns usuários ativos na rede, entretanto, todos os dados coletados foram mascarados para garantir a confidencialidade das informações.

Dados do Usuário 1

DHCP: [192.168.242.11] ACK : 10.xxx.xxx.xx 255.255.248.0 GW 10.xxx.xxx.x DNS 131.0.152.18 "academic.lc"
HTTP : 131.0.152.66:80 -> USER: xxxxxxx PASS: xxxxxxxx INFO: **aluno/login**.php5?
CONTENT: dbList=192.168.238.19%2FINST01%2FGVCOLLEGE&lstUnidades=12%2C2&
usr=xxxxxxx&passwd=xxxxxxx&base=&postBack=1&acao=login&ViewLoginXmlXsl%5
Bmethod%5D=btnLogin_click&form_key=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Conforme pode ser observado em destaque no resultado acima, a amostragem de informações é referente a um usuário do tipo aluno, o mesmo estava acessando o link de login para entrar na aplicação, utilizando a rota direta identificada conforme o link: http://portalcaxias.ftsg.edu.br/modulos/aluno/login.php5.

Dados do Usuário 2

HTTP : 131.0.152.66:80 -> USER: xxxxxx PASS: xxxxxxx INFO: **formulario_login**.php
CONTENT: usr=013xxxxxx&passwd=xxxxxx%3D%3D&**apsweb_**
tipo=aluno&lstUnidades=12%2C2&ViewLoginXmlXsl%5Bmethod%5D=btnLogin_
click&**acao=login**
Nesta segunda amostragem os dados em destaque também identificam o usuário como sendo um aluno e a ação de login no sistema. Entretanto a rota tomada para acesso foi pelo site da instituição, conforme o link: www.ftsg.edu.br/formulario_login.php.

Dados do Usuário 3

HTTP: 131.0.152.66:80 -> USER: xxxxxxxxxx PASS: xxxxxxxxxx INFO:
CONTENT: usr=09xxxx5&passwd=xxxxxxxxxxxxxx%3D&**apsweb_**
tipo=professor&lstUnidades=12%2C2&ViewLoginXmlXsl%5Bmethod%5D=btnLogin_
click&**acao=login**
Na terceira amostragem é possível identificar a mudança de tipo de usuário, sendo esse um professor conforme destacado. Já o método de acesso segue o padrão, ou seja, pelo site da instituição conforme o link: http://portalcaxias.ftsg.edu.br/modulos/aluno/login.php5.

Dados do Usuário 4

HTTP : 131.0.152.66:80 -> USER: XXXXXXXX PASS: XXXXXXXXX INFO:
CONTENT: usr=02XXXX2&passwd=XXXXXXXXXXXXXX%3D&**apsweb_**
tipo=aluno&lstUnidades=12%2C2&ViewLoginXmlXsl%5Bmethod%5D=btnLogin_
click&**acao=login**
Na quarta e última amostragem o tipo de usuário volta a ser aluno, conforme destacado.

4.1 SUGESTÃO DE MELHORIA E DETECÇÃO

Para uma boa defesa perante um envenenamento de ARP é aconselhável levar em consideração as recomendações do fabricante do equipamento quanto a sua configuração. A configuração de filtro de pacotes, habilitar o MAC Bridging se houver, essa função não permite os endereços MAC associados sejam alterados depois de configurados.

De acordo com Vieira (2008) para detectar ataques de envenenamento de ARP foi que surgiu o programa Arpwatch, esta ferramenta monitora as atividades ethernet e mantém uma base de dados dos pareamentos Ethernet/IP.

Ainda para Vieira (2008) com o Arpwatch também é possível configurar o envio de meio de alertas em caso de alterações na tabela ARP, ou seja, caso algum dispositivo computacional seja adicionado na rede, ele avisa por e-mail o administrador sobre essa atividade, além de informar caso o endereço MAC tenha mudado de IP em algum momento.

Para a detecção de envenenamento de ARP também pode ser usado o RARP (Reverse ARP). Este por sua vez solicita o endereço IP de um endereço MAC conhecido, de modo que ao enviar uma solicitação RARP para todos os endereços MAC existentes na rede, passa a ser possível determinar o momento em que algum computador está realizando a clonagem, e se múltiplas respostas são recebidas por um único endereço MAC.

Além de tomar cuidado com as configurações e monitoramento da rede wireless, é necessário levar em consideração o uso de protocolos seguros como o HTTPS [16]com o certificado S***[17]***SL, que provê a criptografia da comunicação entre os dispositivos.

A prevenção contra o vazamento de informações sigilosas como os dados apresentados na análise, dever ser levada em conta analisando os aspectos jurídicos. Para evitar o vazamento de informações por esse meio, faz-se necessário um desenvolvimento correto do sistema de gestão utilizado pela instituição. Para isso é preciso que as partes envolvidas validem por meio de testes de intrusão a eficiência de sua proteção, no que diz respeito a integridade, confidencialidade e legalidade.

5 CONSIDERAÇÕES FINAIS

Conforme pode ser observado no decorrer da análise, um sniffer pode sim ser utilizado para coletar informações em uma rede Wireless, no entanto somente executá-lo sem a utilização de outras técnicas de invasão não garante uma total satisfação na obtenção de dados mais sensíveis. A ferramenta Ettercap mostrou-se bem eficiente tanto na aplicação da técnica de invasão quanta na técnica de farejamento.

Alguns pontos como a queda constante da rede e poucos acessos ao sistema devido ao fato de ser uma sexta-feira, acabaram dificultando a obtenção de um volume de dados mais significativo para a análise. No entanto não inviabilizou a coleta e nem tão pouco a obtenção de informações relevantes como mostrado na fase de análise. Dados que se divulgados ou coletados por alguém mal-intencionado, pode acarretar problemas catastróficos as partes envolvidas, ou seja, a instituição e o fornecedor do sistema de gestão.

Levando em consideração a importância que a informação representa para as organizações e a fragilidade da rede apresentada neste artigo, é possível sugerir uma futura análise de vulnerabilidades mais completa, abrangendo toda a rede, utilizando também todas as técnicas de intrusão possíveis. A coleta de informações pode ser feita em outro dia da semana, algum dia que tenha mais usuários acessando a rede, levantar esse dado com a direção.

Outra análise de vulnerabilidades pode ser feita diretamente no sistema de gestão, pois encontram-se nele todos os dados dos usuários da instituição, o que o faz ser o principal alvo de atividades maliciosas. Desse modo, é importante que ele seja analisado criteriosamente levando em conta os aspectos jurídicos. Assim como a rede, o sistema de gestão também pode ser analisado completamente com todas as técnicas de intrusão de sistemas cabíveis.

FONTE: <https://periciacomputacional.com/analise-de-vulnerabilidades-da-rede-wireless-na-faculdade-de-tecnologia-da-serra-gaucha/>. Acesso em: 20 ago. 2021.

RESUMO DO TÓPICO 6

Neste tópico, você aprendeu:

- Existem procedimentos e práticas que devem ser seguidos em todos os cenários.
- As práticas forenses exigem alinhamento com a lei.
- As provas são categorizadas de acordo com a sua origem.
- Conservar e alterar as evidências são as práticas mais importantes em uma análise forense.

AUTOATIVIDADE

1 As provas coletas e que identificam as práticas forenses de maneira adequada podem ser categorizadas de acordo com a fonte que as produz e com os argumentos utilizados para sustentar sua integridade, assinale a alternativa CORRETA:

a) ( ) As provas de testemunho direto podem ser definidas pela narração dos fatos ou depoimento de qualquer parte envolvida, que tenha conhecimento sobre cenário investigado.
b) ( ) As provas de testemunho direto são descritas como qualquer objeto ou bem material que possa ser tocado fisicamente.
c) ( ) As provas de testemunho direto são sempre baseadas em algum fator observado pelo indivíduo que tenha pleno conhecimento sobre o que procura, como o próprio perito.
d) ( ) As provas de testemunho direto são identificadas apenas pelo especialista responsável pela análise forense ou um administrador de rede com experiência em tecnologia.

2 O uso de mídias é uma prática que deve ser realizada com cuidado pelo perito, uma vez que também são instrumentos causadores de dados aos sistemas. Por esse motivo, muitas organizações bloqueiam o uso desse tipo de dispositivo, à nível de hardware. Sobre o uso desse recurso, analise as sentenças a seguir:

I- Sendo um perito, um profissional experiente, é aceitável que utilize um dispositivo móvel compartilhado par armazenar imagens relacionadas com diversas análises e perícias diferentes para poupar espaço.
II- O ideal é que uma mídia limpa e formatada seja utilizada, por segurança da imagem e integridade das informações que serão copiadas.
III- Utilizar uma mídia protegida contra gravação depois que a imagem já esteja armazenada, minimiza fortemente os riscos de as informações serem alteradas acidentalmente.

Assinale a alternativa CORRETA:

a) ( ) As sentenças I e II estão corretas.
b) ( ) Somente a sentença II está correta.
c) ( ) As sentenças I e III estão corretas.
d) ( ) Somente a sentença III está correta.

3 Nem sempre somente um dispositivo precisa ser periciado, em alguns casos os problemas precisam ser mitigados em uma rede interna que envolve mais de um local como sala ou prédio que tenha sofrido um ataque ou crime digital. Sobre dispositivos que podem estar inclusos. E casos como estes, classifique V para as sentenças verdadeiras e F para as falsas:

( ) Notebooks e computadores são os principais alvos, mas scanners e dispositivos telefônicos como os que compõe uma estrutura VoIP são totalmente seguros.
( ) Mídias removíveis podem ter sido infectadas e espalharem a ameaça por toda a rede, por isso precisam de atenção, um exemplo são os discos externos.
( ) Mesmo não sendo uma ferramenta de alvo, os manuais são ferramentas importantes, que precisam ser analisados em uma perícia forense, dando confiabilidade aos relatórios finais.

Assinale a alternativa que apresenta a sequência CORRETA:

a) ( ) V – F – F.
b) ( ) V – F – V.
c) ( ) F – V – V.
d) ( ) F – F – V.

4 O desligamento de um dispositivo nem sempre é a melhor ação a ser tomada, apesar de ser muitas vezes a decisão mais rápida a ser tomada com a intensão de interromper um processo de ataque. Disserte sobre os comandos su e halt que pode ser utilizado em sistemas operacionais *Unix,* com o intuito de evitar que *malwares* sejam impulsionados.

5 Sabemos que existem diversos tipos de provas que devem ser juntadas para garantir maior confiabilidade a perícia forense. Neste contexto, disserte sobre a importância de mesclar as diferentes categorias de provas.

REFERÊNCIAS

ANDROULIDAKIS, I. **VoIP and PBX Security and Forensics**. 2. ed. Springer. 2016.

ARGOLO, F. **Análise Forense em sistemas GNU/*Linux***. 2005. Disponível em: https://www.ravel.ufrj.br/sites/ravel.ufrj.br/files/publicacoes/projetofinal_fred.pdf. Acesso em: 23 ago. 2021.

BASTA, A.; BASTA, N.; BROWN, M. **Segurança de Computadores e Testes de Invasão**. Tradução: Lizandra Magnon de Almeida. [S. l]: Cengage Learning Edições LTDA, 2015.

CARVEY, H. ***Windows* Registry Forensics**. 2. ed. Amsterdam: Elsevier, 2016.

COSTA, D. **Boas práticas para perícia forense**. Jaguariúna, 2008. Disponível em: https://www.ethicalhacker.com.br/site/apostilas/PERICIA_FORENSE_COMPUTACIONAL/monografiapericia.pdf. Acesso em: 23 ago. 2021.

GUIMARÃES. **Ameaças VoIP**: tipos de ataques e técnicas usadas por hackers. 2021. Disponível em: https://www.khomp.com/pt/ameacas-ataques-voip. Acesso em: 23 ago. 2021.

HASSAN, N. **Digital Forensecs Basics**: A practical Guide Using *Windows* OS. New York: Apress. 2019.

INTNET. **Proxy e cache**: entenda o que é e como funciona cada um. 2018. Disponível em: https://blog.intnet.com.br/proxy-e-cache-entenda-o-que-e-e-como-funciona-cada-um-2/. Acesso em: 23 ago. 2021.

MORIMOTO, C. **Hardware**: O guia definitivo. 4. ed. Porto Alegre: Sul Editores, 2010.

NIKKEL, B. **Practical *Linux* Forensics**: a guide for digital investigators. 2021.

SOBRAL, B. **Anatomia dos ataques às redes TCP/IP**. c2021a. Disponível em: http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5630/material-seg-redes/Cap3-Anatomia-de-Ataques.pdf. Acesso em: 23 ago. 2021.

SOBRAL, B**. Footprint e Fingerprint**. c2021b. Disponível em: inf.ufsc.br/~bosco.sobral/ensino/ine5630/material-seg-redes/Cap4-Footprint-Fingerprint.pdf. Acesso em: 23 ago. 2021.

WENDT, E.; BARRETO, A. G. **Inteligência e investigação criminal**. Rio de Janeiro: Brasport. 2020.

WRIGHTSON, T. **Wireless network security**: a beginner's guide. New York: McGraw-Hill, 2012.