Aula 17 – Processo de Aquisição de Evidências Digitais - Parte 2: Mídia Não Volátil

Bem-vindos à segunda parte da nossa jornada pelo fascinante e crítico universo da aquisição de evidências digitais. Na aula anterior, exploramos a natureza efêmera das mídias voláteis, como a memória RAM, e a urgência que as caracteriza. Agora, viramos nossa atenção para um tipo de evidência que, embora não desapareça com um simples desligamento, exige uma metodologia igualmente rigorosa e um cuidado extremo para garantir sua integridade e admissibilidade em um processo legal ou investigativo.

Imagine que você é um detetive digital, e a cena do crime não é um local físico, mas um disco rígido, um SSD ou um pendrive. Diferente de uma cena que pode ser isolada com fitas, o ambiente digital é invisível e incrivelmente frágil a alterações. Qualquer passo em falso pode destruir ou contaminar a prova, tornando-a inútil. É por isso que a aquisição de evidências em mídias não voláteis é um pilar fundamental da forense digital, exigindo precisão cirúrgica e conhecimento técnico aprofundado.

Nesta aula, desvendaremos os segredos por trás da criação de imagens forenses, uma técnica que nos permite "fotografar" digitalmente o estado exato de um dispositivo sem alterá-lo. Abordaremos a importância vital dos conceitos de hash para garantir a autenticidade dessas imagens, o papel protetor dos bloqueadores de escrita e, finalmente, exploraremos as ferramentas essenciais que todo especialista em forense digital deve dominar, como Guymager, dd e FTK Imager. Ao final, você estará apto a compreender e aplicar as melhores práticas para coletar evidências digitais de forma íntegra e confiável.

A Essência da Evidência Digital Não Volátil: Onde os Dados Resistem

No vasto campo da forense digital, a distinção entre mídias voláteis e não voláteis é crucial, pois define as estratégias e a urgência de cada etapa da investigação. Enquanto as mídias voláteis, como a memória RAM, perdem seus dados ao serem desligadas, as mídias não voláteis são projetadas para reter informações mesmo sem energia. Elas são o "arquivo morto" digital, o local onde a história de um sistema é escrita e armazenada de forma mais permanente.

Pense em um disco rígido (HDD) ou um Solid State Drive (SSD) como o diário de bordo de um navio. Cada entrada, cada registro, cada arquivo salvo é uma página desse diário. Mesmo que o navio pare de navegar (o computador seja desligado), o diário permanece intacto, contendo as informações cruciais sobre sua jornada. É nesse diário que os investigadores forenses buscam as pistas mais duradouras e reveladoras de atividades maliciosas ou de eventos específicos.

Discos Rígidos (HDD)

Armazenamento magnético tradicional com grande capacidade

Solid State Drives (SSD)

Armazenamento em memória flash, mais rápido e resistente

Dispositivos Portáteis

Pendrives, cartões SD e outros meios removíveis

A importância dessas mídias reside na sua capacidade de armazenar grandes volumes de dados por longos períodos, incluindo sistemas operacionais, programas, documentos, e-mails, históricos de navegação e muito mais. Esses dados podem ser a chave para desvendar um crime cibernético, identificar um invasor ou reconstruir uma sequência de eventos. Contudo, a persistência desses dados não significa que eles são imunes a danos ou alterações, o que nos leva ao próximo desafio: como coletá-los sem contaminá-los.

O Desafio da Preservação: Por Que Imagens Forenses?

O Problema

Quando nos deparamos com uma cena de crime digital envolvendo mídias não voláteis, a primeira e mais importante regra é: "não faça mal". Qualquer interação direta com o dispositivo original pode alterar os metadados, sobrescrever arquivos ou, de alguma forma, contaminar a evidência. É como um arqueólogo que, ao invés de escavar cuidadosamente, usa uma pá mecânica, destruindo artefatos valiosos no processo.

O problema central é que, mesmo ao ligar um computador, o sistema operacional já começa a escrever dados no disco, alterando o estado original. Abrir um arquivo, navegar por pastas ou até mesmo visualizar uma imagem pode deixar rastros que comprometem a integridade da evidência. Para que a prova seja aceita em um tribunal ou para que a investigação seja robusta, é imperativo que o processo de coleta seja impecável e que a evidência original permaneça intocada.

A Solução

A solução para esse dilema é a criação de uma **imagem forense**. Imagine que você precisa estudar um documento antigo e frágil. Você não o manusearia diretamente, mas faria uma cópia exata, talvez uma fotografia de alta resolução, para trabalhar com ela. No mundo digital, a imagem forense é essa "fotografia perfeita", uma cópia bit a bit, setor por setor, do dispositivo original. Ela replica não apenas os arquivos visíveis, mas também os espaços não alocados, os arquivos deletados e até mesmo os artefatos de sistemas de arquivos, preservando o estado exato da mídia no momento da aquisição.

Criando a Cópia Fiel: O Conceito de Imagem Forense

A imagem forense é a pedra angular da análise de mídias não voláteis. Ela não é uma simples cópia de arquivos e pastas, como faríamos ao copiar documentos para um pendrive. Pelo contrário, é uma réplica exata, bit a bit, de todo o conteúdo do dispositivo de armazenamento, incluindo áreas que o sistema operacional normalmente esconde ou não acessa diretamente. Isso significa que cada zero e cada um do disco original é copiado para um novo arquivo de imagem.

Analogia: Para entender melhor, imagine um livro. Uma cópia comum seria apenas o texto das páginas. Uma imagem forense, por outro lado, copiaria não só o texto, mas também as margens, as anotações feitas nas bordas, as páginas arrancadas (mas que deixaram um rastro), e até mesmo o tipo de papel e a encadernação. Ela captura a estrutura completa do "livro", não apenas seu conteúdo legível.

Cópia Lógica

Apenas arquivos visíveis e acessíveis

Cópia Bit-Stream

Todos os setores, incluindo dados deletados e espaços vazios

Imagem Forense

Réplica exata e verificável para análise

Existem diferentes tipos de cópias, mas na forense, a **cópia bit-stream** (ou cópia setor a setor) é o padrão ouro. Ela garante que cada setor do disco original seja copiado para o arquivo de imagem, independentemente de conter dados ativos, dados deletados ou espaço vazio. Essa abordagem contrasta com uma cópia lógica, que apenas copia os arquivos visíveis e acessíveis pelo sistema operacional. Ao trabalhar com a imagem forense, o analista pode explorar o dispositivo sem o risco de alterar a evidência original, garantindo a integridade e a validade da investigação.

Integridade Acima de Tudo: A Função do Hashing

Depois de criar uma imagem forense, surge uma questão fundamental: como podemos ter certeza de que essa cópia é *exatamente* igual ao original e que não foi alterada, intencionalmente ou acidentalmente, desde o momento da aquisição? É aqui que entram os conceitos de **hashing**, uma ferramenta criptográfica indispensável na forense digital para garantir a integridade da evidência.

O que é Hash?

Pense no hashing como a criação de uma "impressão digital" única para um conjunto de dados. Assim como cada pessoa tem uma impressão digital distinta, cada arquivo ou conjunto de dados tem um valor de hash exclusivo. Se até mesmo um único bit for alterado no arquivo original, o valor de hash resultante será completamente diferente. É uma forma de verificar a autenticidade e a imutabilidade dos dados.

Aplicação Forense

No contexto da aquisição de evidências, calculamos o valor de hash do dispositivo original *antes* de iniciar o processo de imagem. Em seguida, calculamos o valor de hash da imagem forense *após* a sua criação. Se os dois valores de hash forem idênticos, temos uma prova matemática de que a imagem é uma réplica exata do original. Essa correspondência é vital para a cadeia de custódia e para a admissibilidade da evidência em um tribunal, pois demonstra que a prova não foi adulterada.

01

Calcular Hash Original

Antes da aquisição, gerar hash do dispositivo de evidência

02

Criar Imagem Forense

Realizar cópia bit a bit usando ferramentas apropriadas

03

Calcular Hash da Imagem

Após aquisição, gerar hash do arquivo de imagem

04

Comparar e Validar

Verificar se os hashes são idênticos para confirmar integridade

MD5 e SHA-256: Comparando Impressões Digitais

No universo do hashing forense, dois algoritmos se destacam: MD5 (Message-Digest Algorithm 5) e SHA-256 (Secure Hash Algorithm 256). Ambos geram uma sequência alfanumérica de tamanho fixo a partir de um conjunto de dados, mas possuem características e níveis de segurança distintos.

MD5

O **MD5** gera um hash de 128 bits (32 caracteres hexadecimais). Por muitos anos, foi o padrão da indústria para verificação de integridade. No entanto, com o avanço da capacidade computacional, foram descobertas "colisões" para o MD5, o que significa que é possível encontrar dois conjuntos de dados diferentes que geram o mesmo valor de hash. Embora isso não invalide completamente seu uso para verificação de integridade em cenários onde a alteração maliciosa é menos provável, sua segurança criptográfica para fins de autenticidade é questionável.

SHA-256

Já o **SHA-256**, parte da família SHA-2, gera um hash de 256 bits (64 caracteres hexadecimais). Ele é consideravelmente mais robusto que o MD5, com uma resistência muito maior a colisões. Por essa razão, o SHA-256 (e outros da família SHA-2, como SHA-512) é amplamente recomendado e utilizado como padrão atual para garantir a integridade e autenticidade de evidências digitais em investigações forenses e processos legais. A escolha do algoritmo de hash é um detalhe técnico que pode ter grandes implicações na credibilidade da evidência.

Conceito	Âmbito/Aplicação	Base/Origem	Exemplo (Hash de "Olá Mundo!")
MD5	Verificação de integridade (legado), checksums rápidos	Algoritmo de 128 bits	`3e25960a79dbc69b674cd4ee196323ff`
SHA-256	Verificação de integridade (atual), segurança criptográfica, blockchain	Algoritmo de 256 bits	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b27796fc19a216

A Barreira Protetora: Bloqueadores de Escrita (Write Blockers)

Imagine que você está em uma cena de crime e precisa examinar um objeto frágil, mas não pode tocá-lo diretamente para não deixar suas próprias impressões digitais ou danificá-lo. Você usaria luvas e ferramentas especiais para manuseá-lo indiretamente. No mundo digital, os **bloqueadores de escrita (write blockers)** desempenham um papel análogo, atuando como uma barreira protetora entre o analista e a evidência digital original.

Por Que São Essenciais?

A função primordial de um write blocker é garantir que nenhum dado seja acidentalmente (ou intencionalmente) gravado na mídia original durante o processo de aquisição. Mesmo uma simples visualização de arquivos pode fazer com que o sistema operacional crie arquivos temporários ou atualize metadados, alterando a evidência. Sem um write blocker, a integridade da prova pode ser comprometida, levantando dúvidas sobre sua autenticidade em um tribunal.

Como Funcionam?

Esses dispositivos ou softwares funcionam permitindo apenas operações de leitura na mídia conectada, bloqueando qualquer tentativa de escrita. É como uma rua de mão única: os dados podem sair do dispositivo (ser lidos), mas nada pode entrar (ser escrito). Essa medida de segurança é tão fundamental que a ausência de um write blocker em uma aquisição de evidências digitais é frequentemente um ponto de questionamento em processos judiciais, podendo invalidar a prova coletada.

Tipos e Funcionamento dos Write Blockers

Os bloqueadores de escrita podem ser classificados em duas categorias principais: **hardware** e **software**. Cada um tem suas vantagens e cenários de uso, mas o princípio fundamental de proteger a mídia original contra alterações permanece o mesmo.

Write Blockers de Hardware

Os **write blockers de hardware** são dispositivos físicos, geralmente externos, que se conectam entre a mídia de evidência (como um HD ou SSD) e o computador forense. Eles possuem circuitos eletrônicos dedicados que interceptam e bloqueiam todos os comandos de escrita, permitindo apenas os comandos de leitura. São considerados o padrão ouro na forense digital devido à sua confiabilidade e à sua natureza independente do sistema operacional. Eles eliminam a possibilidade de um software malicioso ou um erro do sistema operacional contornar a proteção.

Write Blockers de Software

Já os **write blockers de software** são programas que rodam no sistema operacional do computador forense. Eles configuram o sistema para montar a mídia de evidência em modo somente leitura. Embora sejam mais flexíveis e muitas vezes mais acessíveis, dependem da correta configuração e do bom funcionamento do sistema operacional. Há um risco inerente de que um erro no software ou no sistema possa falhar em bloquear a escrita, tornando-os menos preferíveis para evidências críticas, mas ainda úteis em cenários específicos ou como uma camada adicional de proteção. A escolha entre hardware e software depende da criticidade da evidência, dos recursos disponíveis e da política da equipe forense.

Ferramentas do Ofício: Guymager – O Aliado Gráfico

Com a teoria da aquisição e da proteção da evidência bem estabelecida, é hora de conhecer as ferramentas que transformam esses conceitos em prática. Uma das opções mais amigáveis e eficientes para a criação de imagens forenses em ambientes Linux é o **Guymager**. Se você já se sentiu intimidado por linhas de comando, o Guymager é como um farol de simplicidade em um mar de complexidade.

Interface Gráfica Intuitiva

Imagine que você precisa operar uma máquina complexa, mas ela vem com um painel de controle intuitivo, com botões claros e indicadores visuais. O Guymager é exatamente isso para a aquisição de imagens forenses. Ele oferece uma interface gráfica de usuário (GUI) que simplifica o processo de seleção da mídia de origem, configuração dos parâmetros da imagem e monitoramento do progresso. Isso o torna uma excelente escolha para iniciantes e para situações onde a rapidez e a clareza visual são importantes.

Recursos Forenses Completos

Desenvolvido para sistemas Linux, o Guymager permite criar imagens forenses de discos rígidos e outros dispositivos de armazenamento de forma segura e eficiente. Ele suporta a criação de imagens em formatos populares como E01 (EnCase) e RAW (dd), e o mais importante, ele calcula os hashes (MD5 e SHA-256) da imagem *durante* o processo de aquisição, garantindo a integridade desde o primeiro momento. Sua facilidade de uso não compromete a robustez forense, tornando-o uma ferramenta valiosa no arsenal de qualquer investigador.

O Poder Bruto do Terminal: dd (Disk Duplicator)

Se o Guymager é o painel de controle intuitivo, o comando **dd** (disk duplicator) é a ferramenta cirúrgica de linha de comando: poderosa, precisa e, se usada incorretamente, potencialmente destrutiva. O dd é um utilitário Unix/Linux que permite copiar e converter arquivos em nível de bloco, o que o torna ideal para a criação de imagens forenses bit a bit.

Pense no dd como um robô que pode copiar qualquer coisa de um lugar para outro, byte por byte, sem fazer perguntas. Ele não se importa com o que são os dados – se é um arquivo, um sistema operacional ou um espaço vazio – ele simplesmente os copia. Essa característica o torna incrivelmente versátil para tarefas como criar imagens de discos, restaurar backups ou até mesmo apagar dados de forma segura. No entanto, essa mesma versatilidade exige um conhecimento profundo de seus parâmetros, pois um erro de digitação pode resultar na sobrescrita do disco errado, causando perda irreparável de dados.

⚠️ **ATENÇÃO:** Apesar de sua curva de aprendizado mais íngreme e da ausência de uma interface gráfica, o dd é amplamente utilizado por profissionais forenses devido à sua ubiquidade (presente em quase todas as distribuições Linux), sua leveza e sua capacidade de ser integrado em scripts automatizados. Ele é a espinha dorsal de muitas operações de aquisição, oferecendo controle granular sobre o processo e sendo fundamental para a criação de imagens RAW, que são o formato mais básico e universalmente compatível para análise forense.

Comandos Essenciais com dd para Aquisição Forense

Para utilizar o dd de forma eficaz na aquisição forense, é crucial entender seus parâmetros básicos. A sintaxe fundamental envolve if (input file, a origem dos dados) e of (output file, o destino dos dados). Para a aquisição de um disco rígido, o if será o caminho para o dispositivo de disco (ex: /dev/sda), e o of será o caminho para o arquivo de imagem que você deseja criar.

Comando Típico de Aquisição

```
sudo dd if=/dev/sda of=/mnt/evidencia/imagem_forense.dd bs=4M conv=noerror,sync status=progress
```

sudo

Executa o comando com privilégios de superusuário, necessários para acessar dispositivos de disco.

if=/dev/sda

Define o disco /dev/sda como a fonte de entrada. ⚠️ **ATENÇÃO:** Substitua /dev/sda pelo identificador correto do disco de evidência. Um erro aqui pode apagar seu próprio sistema!

of=/mnt/evidencia/imagem_forense.dd

Define o arquivo imagem_forense.dd no diretório /mnt/evidencia como o destino da imagem. Certifique-se de que o destino tenha espaço suficiente e esteja em um disco diferente do de evidência.

bs=4M

Define o tamanho do bloco de leitura/escrita para 4 megabytes. Isso otimiza a velocidade de cópia.

conv=noerror,sync

noerror continua a cópia mesmo se encontrar erros de leitura no disco de origem (útil para discos danificados). sync preenche blocos de entrada com zeros se houver erros de leitura, mantendo o tamanho do bloco consistente.

status=progress

Exibe o progresso da cópia, o que é muito útil para operações longas.

Verificação de Integridade

Após a criação da imagem, é vital calcular o hash para verificar a integridade. Você pode usar ferramentas como md5sum ou sha256sum:

```
md5sum /mnt/evidencia/imagem_forense.dd
sha256sum /mnt/evidencia/imagem_forense.dd
```

Compare o hash gerado com o hash do disco original (calculado antes da aquisição) para confirmar a integridade.

FTK Imager: A Suíte Completa para Windows

Enquanto Guymager e dd são predominantes em ambientes Linux, o **FTK Imager** é a ferramenta de escolha para muitos profissionais forenses que operam em sistemas Windows. Desenvolvido pela AccessData (agora parte da Exterro), o FTK Imager é uma aplicação gratuita e robusta que oferece uma gama completa de funcionalidades para a aquisição e pré-análise de evidências digitais.

Funcionalidades Principais

- Criação de imagens forenses em múltiplos formatos
- Montagem de imagens como unidades virtuais
- Visualização de conteúdo de discos e arquivos
- Exploração de sistemas de arquivos
- Recuperação básica de arquivos deletados
- Cálculo de hashes (MD5, SHA-1)

Por Que Usar?

Imagine que você tem uma caixa de ferramentas completa, onde cada ferramenta é projetada para uma tarefa específica, mas todas trabalham em conjunto. O FTK Imager é assim: ele não apenas cria imagens forenses, mas também permite montar essas imagens como unidades virtuais, visualizar o conteúdo de discos e arquivos, explorar o sistema de arquivos e até mesmo recuperar arquivos deletados em um nível básico. É uma verdadeira "suíte suíça" para a forense em Windows, oferecendo uma interface gráfica intuitiva que facilita o trabalho.

Sua popularidade se deve à sua versatilidade e à sua capacidade de lidar com diversos formatos de imagem (RAW, E01, AD1), além de calcular hashes (MD5 e SHA-1, embora SHA-256 seja mais recomendado hoje e possa ser integrado com outras ferramentas). O FTK Imager é uma ferramenta indispensável para quem trabalha com forense digital em ambientes Windows, seja para aquisição em campo ou para análise inicial em laboratório, complementando as capacidades oferecidas por ferramentas baseadas em Linux.

Passo a Passo com FTK Imager: Criando uma Imagem

Criar uma imagem forense com o FTK Imager é um processo relativamente simples e guiado pela interface gráfica. Aqui está um passo a passo conceitual de como você faria:

Iniciar o FTK Imager

Abra o programa. Você verá uma interface com menus e painéis.

Selecionar a Fonte da Evidência

No menu "File", escolha "Create Disk Image". Uma janela de assistente será aberta.

Escolher o Tipo de Fonte

O assistente perguntará qual tipo de fonte você deseja imaginar. As opções incluem "Physical Drive" (para discos rígidos, SSDs, pendrives), "Logical Drive" (para partições), "Image File" (para criar uma imagem de outra imagem) ou "Contents of Folder" (para criar uma imagem de uma pasta). Para a maioria das aquisições de mídia não volátil, você selecionará "Physical Drive".

Selecionar o Dispositivo Físico

Uma lista de todos os dispositivos físicos conectados ao seu sistema será exibida. ⚠️ **ATENÇÃO:** Identifique cuidadosamente o disco de evidência correto. Um erro aqui pode levar à aquisição do disco errado ou, pior, à sobrescrita de dados.

Adicionar Destino da Imagem

Clique em "Add" para configurar onde a imagem será salva. Você precisará escolher o formato da imagem (E01 é comum, RAW é universal), fornecer informações sobre o caso (número do caso, evidência, examinador, notas) e especificar o caminho e o nome do arquivo de destino.

Configurar Opções Adicionais

Você pode definir o tamanho dos segmentos da imagem (para dividir um arquivo grande em partes menores), o nível de compressão (se usar E01) e se deseja calcular hashes (MD5 e SHA-1 são padrão, mas você pode usar outras ferramentas para SHA-256).

Iniciar a Aquisição

Após revisar todas as configurações, clique em "Start". O FTK Imager começará a criar a imagem, exibindo o progresso e os hashes calculados em tempo real.

Desafios na Aquisição de Mídias Não Voláteis

Embora o processo de aquisição de mídias não voláteis pareça direto, a realidade forense apresenta uma série de desafios que exigem flexibilidade, conhecimento e, por vezes, criatividade. Nem toda evidência digital está em um disco rígido saudável e facilmente acessível.

Mídias Danificadas ou Corrompidas

Um dos maiores desafios são as **mídias danificadas ou corrompidas**. Discos com setores defeituosos, placas controladoras queimadas ou danos físicos podem tornar a aquisição uma tarefa árdua, exigindo ferramentas e técnicas especializadas de recuperação de dados antes mesmo que a imagem forense possa ser criada. Nesses casos, a prioridade é obter o máximo de dados possível, mesmo que a imagem não seja 100% completa.

Criptografia

Outro ponto complexo é a **criptografia**. Discos rígidos ou partições criptografadas (como BitLocker, VeraCrypt, LUKS) representam uma barreira significativa. A aquisição da imagem ainda é possível, mas o conteúdo permanecerá ilegível sem a chave de descriptografia. Isso adiciona uma camada de complexidade à investigação, exigindo a obtenção da chave ou a aplicação de técnicas de quebra de criptografia, o que pode ser demorado ou até impossível.

Grandes Volumes de Dados

Além disso, a crescente capacidade de armazenamento e a proliferação de dispositivos (smartphones, IoT) significam que os analistas frequentemente lidam com **grandes volumes de dados**, tornando a aquisição e a análise mais demoradas e exigindo infraestrutura robusta.

A Importância da Documentação no Processo de Aquisição

No mundo da forense digital, a aquisição de evidências é apenas metade da batalha; a outra metade, igualmente crucial, é a **documentação meticulosa** de cada passo do processo. Imagine um detetive de cena de crime que coleta uma arma, mas não anota onde a encontrou, quem a tocou ou como a transportou. Essa evidência, por mais relevante que seja, perderia sua credibilidade no tribunal.

Da mesma forma, na aquisição de evidências digitais, cada ação deve ser registrada com precisão cirúrgica. Isso inclui detalhes como a data e hora da aquisição, o nome do examinador, o número do caso, a identificação exata do dispositivo de evidência (número de série, modelo), o tipo de bloqueador de escrita utilizado, a ferramenta de imagem e seus parâmetros, e, crucialmente, os valores de hash (pré e pós-aquisição). Essa documentação forma a **cadeia de custódia**, um registro ininterrupto que prova que a evidência foi manuseada de forma adequada e que sua integridade foi mantida desde a coleta até a apresentação.

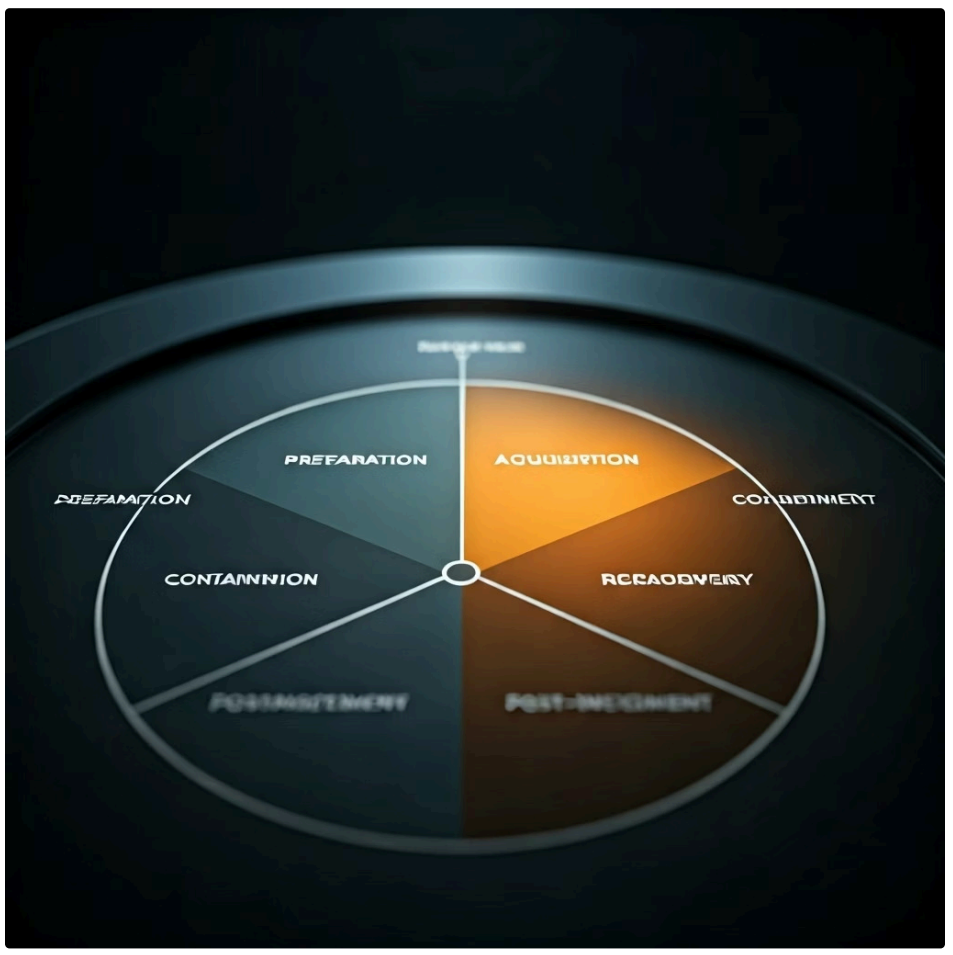
Validade Legal Documentação completa valida a evidência em processos judiciais	**Transparência** Permite que outros especialistas revisem e repliquem o processo
Reprodutibilidade Garante que a investigação possa ser verificada independentemente	**Credibilidade** Prova que o analista seguiu as melhores práticas

Uma documentação completa e precisa não apenas valida a evidência em um processo legal, mas também permite que outros especialistas revisem e repliquem o processo, garantindo a transparência e a reprodutibilidade da investigação. É a prova de que o analista seguiu as melhores práticas e que a evidência apresentada é autêntica e confiável. Sem ela, mesmo a aquisição tecnicamente perfeita pode ser questionada e desconsiderada.

Frameworks em Ação: NIST SP 800-61 e SANS PICERL na Aquisição

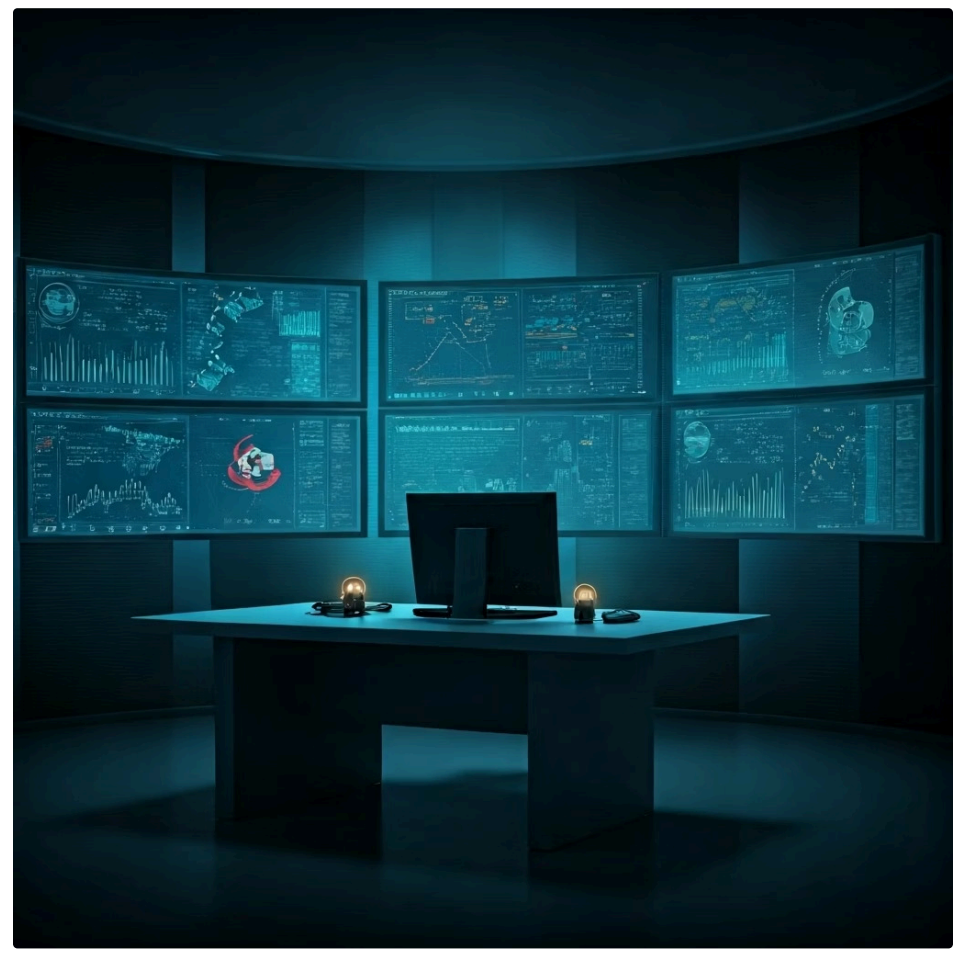
A aquisição de evidências digitais não ocorre em um vácuo; ela é uma etapa crítica dentro de um processo maior de resposta a incidentes. Frameworks consolidados, como o **NIST SP 800-61** e o **SANS PICERL**, fornecem uma estrutura organizada para gerenciar incidentes de segurança, e a aquisição de mídias não voláteis se encaixa perfeitamente em suas fases.

NIST SP 800-61



O **NIST SP 800-61** (Computer Security Incident Handling Guide) descreve quatro fases principais: Preparação, Detecção e Análise, Contenção, Erradicação e Recuperação, e Atividades Pós-Incidente. A aquisição de evidências digitais se situa principalmente na fase de **Contenção**. Uma vez que um incidente é detectado e analisado, a contenção visa limitar o dano e impedir que o incidente se espalhe. Parte essencial dessa contenção é a coleta de evidências para entender o que aconteceu e para futuras análises. A aquisição de mídias não voláteis é fundamental para preservar o estado do sistema afetado antes de qualquer tentativa de erradicação ou recuperação.

SANS PICERL



De forma similar, o modelo **SANS PICERL** (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) também posiciona a aquisição na fase de **Contenção**. Após a identificação de um incidente, a contenção é o momento de isolar os sistemas afetados e, crucialmente, coletar as evidências. A aquisição de imagens forenses de discos rígidos e outros dispositivos não voláteis é uma ação primária para garantir que os dados relevantes sejam preservados antes que qualquer ação de remediação possa potencialmente alterá-los. Esses frameworks garantem que a aquisição seja uma etapa planejada e integrada, não uma ação isolada.

Inteligência de Ameaças (CTI) e a Proatividade na Aquisição

A forense digital tradicionalmente atua de forma reativa, investigando um incidente *após* sua ocorrência. No entanto, a integração da **Inteligência de Ameaças (Cyber Threat Intelligence - CTI)** está transformando essa abordagem, permitindo uma postura mais proativa, inclusive na fase de aquisição de evidências.

> **Analogia:** Imagine que, antes de investigar um crime, você já tem informações sobre os métodos preferidos do criminoso, as ferramentas que ele usa e os locais onde ele costuma deixar rastros. A CTI oferece exatamente isso para o mundo digital. Ela fornece informações contextuais sobre ameaças cibernéticas, incluindo táticas, técnicas e procedimentos (TTPs) de adversários, indicadores de comprometimento (IoCs) e vulnerabilidades.

Identificação de Ameaças

CTI fornece informações sobre TTPs e IoCs de adversários conhecidos

Aquisição Direcionada

Analista prioriza áreas específicas do disco baseado em inteligência

Resposta Otimizada

Redução de tempo e recursos, aumentando eficácia da investigação

Ao incorporar a CTI, um analista forense pode antecipar *onde* e *o que* procurar durante a aquisição de evidências. Por exemplo, se a inteligência de ameaças indica que um determinado grupo de ataque usa um tipo específico de malware que armazena seus logs em um diretório não padrão, o analista pode priorizar a aquisição e a análise desse diretório ou de áreas específicas do disco. Isso otimiza o tempo e os recursos, tornando a aquisição mais direcionada e eficiente. A CTI transforma a aquisição de uma busca genérica para uma caça cirúrgica, aumentando significativamente as chances de encontrar evidências relevantes e de responder a ataques de forma mais rápida e eficaz.

Forense em Ambientes Modernos: Nuvem e Virtualização

O cenário da computação evoluiu drasticamente, e com ele, os desafios da forense digital. A aquisição de evidências em ambientes tradicionais de discos físicos é bem estabelecida, mas o advento da **computação em nuvem** e da **virtualização** introduz novas complexidades e metodologias.

Ambientes Virtualizados

Em ambientes virtualizados, como máquinas virtuais (VMs) rodando em um hypervisor, a "mídia não volátil" não é um disco físico, mas um arquivo de imagem de disco virtual (ex: VMDK, VHD, QCOW2). A aquisição forense aqui envolve copiar esse arquivo de imagem virtual. Embora o conceito de cópia bit a bit permaneça, o desafio é acessar o hypervisor de forma segura e sem interrupções, garantindo que a VM não seja alterada durante o processo. Ferramentas específicas e APIs dos provedores de virtualização são frequentemente necessárias.

Computação em Nuvem

Ainda mais complexa é a forense em nuvem. Em vez de ter acesso direto ao hardware, o analista depende dos provedores de serviços em nuvem (CSPs) para obter acesso a logs, snapshots de discos virtuais ou até mesmo imagens de memória. A aquisição de evidências em nuvem é frequentemente uma "aquisição lógica" de dados fornecidos pelo CSP, regida por contratos de serviço e requisitos legais. Isso exige uma colaboração estreita com o provedor e um entendimento das suas capacidades forenses. A tendência é que a forense em nuvem se torne cada vez mais importante, exigindo novas habilidades e abordagens dos especialistas.

Boas Práticas e Erros Comuns a Evitar

Para garantir o sucesso e a validade de qualquer aquisição de evidências digitais em mídias não voláteis, é fundamental aderir a um conjunto de boas práticas e estar ciente dos erros comuns que podem comprometer todo o processo.

✅ Boas Práticas

- **Sempre usar bloqueador de escrita**

  Seja hardware ou software, é a primeira linha de defesa contra alteração acidental

- **Calcular e registrar hashes**

  MD5 e SHA-256 do dispositivo original antes e da imagem após aquisição

- **Documentar cada passo**

  Manter cadeia de custódia impecável desde chegada até conclusão

- **Usar ferramentas validadas**

  Utilizar software forense reconhecido e testado pela comunidade

- **Verificar capacidade de destino**

  Garantir espaço suficiente e boas condições do disco de destino

❌ Erros Comuns

- **Não usar write blocker**

  Pode invalidar completamente a evidência coletada

- **Não calcular ou registrar hashes**

  Impossibilita prova de integridade da evidência

- **Sobrescrever disco de evidência**

  Erro fatal, especialmente com dd se parâmetros forem invertidos

- **Espaço insuficiente no destino**

  Interrompe processo e pode corromper imagem parcial

- **Documentação inadequada**

  Compromete cadeia de custódia e validade legal

Princípio Fundamental: Lembre-se, o princípio "do no harm" (não fazer mal) é a bússola que deve guiar todas as suas ações na aquisição de evidências digitais.

Consolidação e Autoavaliação

Chegamos ao fim de mais uma etapa crucial em nossa jornada pela forense digital. Nesta aula, mergulhamos no universo das mídias não voláteis, compreendendo a importância de sua aquisição para a preservação de evidências duradouras. Exploramos o conceito de imagem forense como a cópia bit a bit fiel do original, a função vital dos hashes (MD5 e SHA-256) para garantir a integridade, e a proteção essencial oferecida pelos bloqueadores de escrita. Além disso, conhecemos ferramentas práticas como Guymager, dd e FTK Imager, e discutimos os desafios e as boas práticas, integrando a aquisição aos frameworks de resposta a incidentes e à inteligência de ameaças.

Em prática: A aquisição de evidências digitais de mídias não voláteis é um processo que exige precisão, conhecimento técnico e adesão rigorosa a protocolos. Ao aplicar os conceitos de imagem forense, hashing e bloqueadores de escrita, e ao dominar as ferramentas apresentadas, você estará apto a coletar provas digitais de forma íntegra e admissível. Lembre-se sempre da importância da documentação e da cadeia de custódia para validar seu trabalho.

Autoavaliação

1. Qual é o principal objetivo da criação de uma imagem forense de uma mídia não volátil?
   - a) Acelerar o processo de análise de dados.
   - b) Preservar o estado original da evidência sem alterá-la.
   - c) Reduzir o tamanho dos arquivos para facilitar o armazenamento.
   - d) Converter o formato do sistema de arquivos para um padrão universal.
2. Qual a principal função de um bloqueador de escrita (write blocker) no processo de aquisição de evidências digitais?
   - a) Aumentar a velocidade de cópia dos dados.
   - b) Criptografar a imagem forense para protegê-la.
   - c) Impedir que dados sejam gravados na mídia de evidência original.
   - d) Calcular o hash da imagem durante a aquisição.
3. Em relação aos algoritmos de hash MD5 e SHA-256, qual afirmação está correta para o contexto forense atual?
   - a) MD5 é o algoritmo mais seguro e recomendado devido à sua velocidade.
   - b) SHA-256 é mais robusto e resistente a colisões, sendo o padrão atual.
   - c) Ambos são igualmente seguros e intercambiáveis para qualquer tipo de evidência.
   - d) MD5 é usado para mídias voláteis e SHA-256 para mídias não voláteis.
4. Qual das seguintes ferramentas é mais comumente utilizada em ambientes Linux para criar imagens forenses via linha de comando, apesar de exigir cuidado devido ao seu poder?
   - a) FTK Imager
   - b) Guymager
   - c) dd
   - d) EnCase
5. Descreva a importância da documentação e da cadeia de custódia no processo de aquisição de evidências digitais, explicando como elas contribuem para a validade da prova em um processo legal.

Gabarito e Próximos Passos

1	2	3	4
Resposta: b)	**Resposta: c)**	**Resposta: b)**	**Resposta: c)**
Preservar o estado original da evidência sem alterá-la	Impedir que dados sejam gravados na mídia de evidência original	SHA-256 é mais robusto e resistente a colisões, sendo o padrão atual	dd (Disk Duplicator)

Próxima Aula

Aula 18 – Análise Forense de Sistemas de Arquivos

Na próxima aula, aprofundaremos na estrutura interna das imagens forenses, aprendendo a navegar e extrair informações valiosas dos sistemas de arquivos que as compõem.

Recursos Adicionais

NIST SP 800-61 Rev. 2

Guia oficial para tratamento de incidentes de segurança de computador, essencial para entender o contexto da aquisição.

SANS Institute

Oferece cursos e certificações em forense digital e resposta a incidentes, com materiais aprofundados sobre as ferramentas e técnicas discutidas.

Documentação do FTK Imager

Para explorar em detalhes as funcionalidades e o uso prático da ferramenta.

NOTA IMPORTANTE: As informações regulatórias/legais/técnicas desta aula estão atualizadas até 2025. Consulte sempre fontes oficiais para verificar alterações.