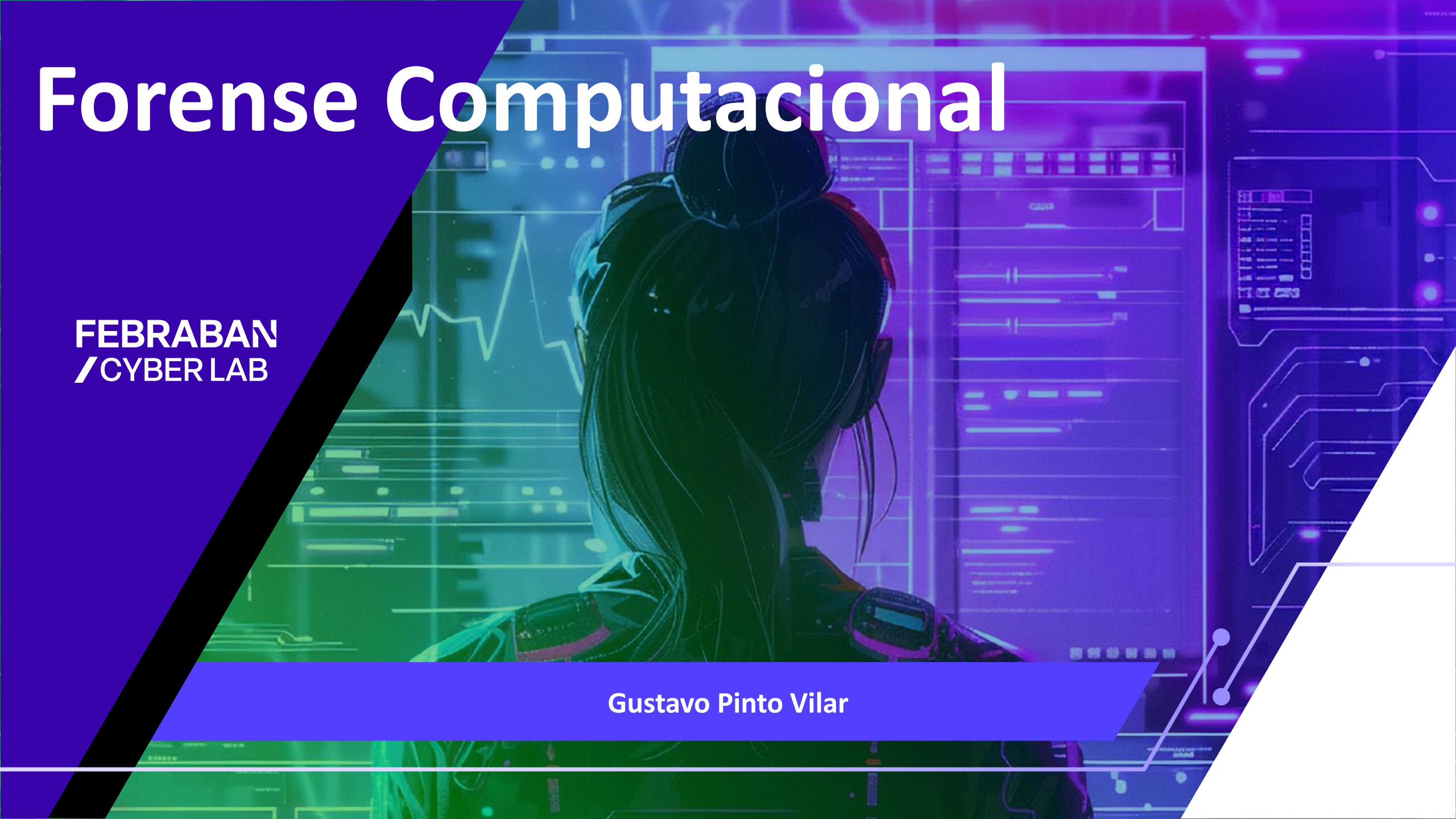
Forense Computacional



FEBRABAN
/CYBER LAB

Gustavo Pinto Vilar

Forense Computacional

Agenda

Módulo 1: Conceitos Básicos de Investigação Digital

Módulo 2: Preservação e Cadeia de Custódia de Evidências

Módulo 3: Coleta e Análise de Logs e Dispositivos

Módulo 4: Ferramentas de Forense Digital

Módulo 5: Relatórios e Boas Práticas de Documentação

Forense Computacional

Agenda

Módulo 1: Conceitos Básicos de Investigação Digital

- Forense Computacional: O Que É e Por Que É Essencial
- Objetivos de uma Investigação Digital
- As Fases da Investigação Digital (Modelo Geral)
- Considerações Legais e Éticas
- Tipos de Evidências Digitais
- O Princípio de Locard na Era Digital
- Desafios na Forense Digital
- Forense Digital vs. Resposta a Incidentes (IR)
- Papéis e Responsabilidades do Investigador Digital
- Tipos de Investigações Forenses Digitais
- Técnicas de Ocultação de Dados (Anti-forense)
- Importância da Forense Computacional na Segurança Pública

Forense Computacional: O Que É e Por Que É Essencial

FEBRABAN
CYBER LAB

- Definição: A ciência de recuperar e investigar materiais encontrados em dispositivos digitais.
- Objetivo Principal: Identificar, preservar, coletar, analisar e apresentar evidências digitais de forma legalmente aceitável.
- Campo de Atuação: Incidentes cibernéticos, crimes digitais, litígios civis, investigações corporativas.
- Importância: Essencial para a justiça criminal, segurança corporativa e defesa nacional.
- Pilares: Integridade, autenticidade, confiabilidade e admissibilidade da evidência.

Objetivos de uma Investigação Digital

FEBRABAN
CYBER LAB

- Identificar o Ocorrido: O que aconteceu, quando, como, onde e por quem (se possível).
- Preservar Evidências: Proteger a integridade e autenticidade dos dados digitais.
- Recuperar Dados: Restaurar informações deletadas, ocultas ou corrompidas.
- Analisar Evidências: Interpretar os dados para reconstruir eventos e extrair informações relevantes.
- Documentar e Relatar: Registrar o processo e as descobertas de forma clara e compreensível.
- Apoiar Processos Legais/Internos: Fornecer base para ações judiciais, políticas de segurança ou resposta a incidentes.

As Fases da Investigação Digital (Modelo Geral)

FEBRABAN
CYBER LAB

- Preparação: Desenvolvimento de kits forenses, planos de resposta a incidentes, treinamento.
- Identificação: Reconhecimento do incidente e dos sistemas envolvidos.
- Preservação: Isolamento e proteção das fontes de evidências.
- Coleta (Aquisição): Criação de cópias forenses íntegras das evidências.
- Análise: Exame sistemático das evidências para extrair informações relevantes.
- Documentação: Registro detalhado de todas as ações e descobertas.
- Relato (Reporting): Elaboração de um relatório compreensível para stakeholders.
- Apresentação (Testemunho): Se necessário, explicação das descobertas em juízo.

Considerações Legais e Éticas

FEBRABAN
CYBER LAB

- Legalidade: Necessidade de autorização (mandados judiciais, políticas internas) para acesso a dados.
- Jurisdição: Leis variam entre países e estados.
- Privacidade: Respeito à legislação de proteção de dados (LGPD, GDPR).
- Ética Profissional: Imparcialidade, objetividade, confidencialidade, competência.
- Consequências: Investigação ilegal ou antiética pode anular evidências e resultar em sanções

Tipos de Evidências Digitais

FEBRABAN
/CYBER LAB

- Evidências Voláteis: Dados que se perdem ao desligar o sistema (ex: RAM, registros de CPU, conexões de rede ativas).
- Evidências Persistentes: Dados armazenados em mídias não voláteis (ex: discos rígidos, SSDs, pendrives, cartões de memória).
- Evidências Latentes: Dados que não são imediatamente visíveis ou acessíveis, mas podem ser recuperados (ex: arquivos deletados, metadados, slack space).
- Evidências de Rede: Logs de firewall, registros de tráfego, capturas de pacotes.
- Evidências em Nuvem: Dados armazenados em serviços de nuvem (IaaS, PaaS, SaaS).

O Princípio de Locard na Era Digital

FEBRABAN
CYBER LAB

- Princípio Original (Edmond Locard): "Todo contato deixa um rastro." (When two objects come into contact, a transfer of material occurs.)
- Contexto Digital: Toda interação com um sistema digital deixa um rastro ou modifica o ambiente.
- Transferência Digital: Acesso a um arquivo, modificação de um registro, navegação web, execução de programas.
- Vestígios: Logs, metadados, arquivos temporários, entradas de registro, históricos.
- Aplicação na Forense: Busca por esses "rastros digitais" para reconstruir eventos e identificar ações.

Desafios na Forense Digital

FEBRABAN
CYBER LAB

- Volatilidade: Dados efêmeros que podem ser perdidos rapidamente.
- Volume de Dados: Lidar com terabytes de informação.
- Criptografia: Dificuldade em acessar dados protegidos.
- Anti-forense: Técnicas para ocultar, destruir ou confundir evidências.
- Jurisdição e Fronteiras: Incidentes que atravessam múltiplas geografias e leis.
- Tecnologias em Evolução: Constante necessidade de atualização de ferramentas e conhecimentos.
- Fragmentação: Evidências espalhadas por múltiplos sistemas e locais (nuvem, dispositivos móveis).

Forense Digital vs. Resposta a Incidentes (IR)

FEBRABAN
CYBER LAB

- Resposta a Incidentes (IR):
  - Foco: Conter, erradicar e recuperar rapidamente de um incidente.
  - Prioridade: Restaurar a operação normal do negócio.
  - Tempo: Ações rápidas, em tempo real ou quase.
  - Exemplo: Bloquear um ataque, restaurar backups.
- Forense Digital:
  - Foco: Investigar a fundo o que aconteceu, como e por quem, para fins legais ou de aprimoramento de segurança.
  - Prioridade: Preservar a integridade da evidência.
  - Tempo: Processo metódico, pode ser mais demorado.
  - Exemplo: Reconstruir a timeline do ataque, identificar a origem.
- Interligação: IR pode gerar a necessidade de FC; FC fornece informações para IR.

Papéis e Responsabilidades do Investigador Digital

FEBRABAN
CYBER LAB

- Conhecimento Multidisciplinar: TI, Direito, Criminologia, Psicologia (para engenharia social).
- Competências Técnicas: Sistemas operacionais, redes, segurança, formatos de arquivo, análise de malware.
- Competências Metodológicas: Raciocínio lógico, atenção aos detalhes, organização, documentação.
- Competências Comportamentais: Integridade, ética, imparcialidade, comunicação.
- Certificações: GCFE, GCFA, CCE, EnCE, ACE.

Tipos de Investigações Forenses Digitais

FEBRABAN
/CYBER LAB

- Criminosa: Crimes digitais (fraude, extorsão, pedofilia, terrorismo, invasão). Evidências para processos criminais.
- Civil: Litígios entre partes (disputas de propriedade intelectual, divórcios, quebra de contratos).
- Administrativa/Corporativa: Violação de políticas internas, assédio, espionagem industrial, vazamento de informações.
- Regulatória: Conformidade com leis e regulamentos (LGPD, normas setoriais).
- Militar/Inteligência: Ciberguerra, espionagem, proteção de infraestrutura crítica.

Técnicas de Ocultação de Dados (Anti-forense)

FEBRABAN
CYBER LAB

- Criptografia: Proteger o conteúdo de arquivos ou discos inteiros com senhas/chaves.
- Esteganografia: Ocultar dados dentro de outros arquivos (imagens, áudios) de forma imperceptível.
- Exclusão Segura/Limpeza de Disco: Sobrescrever dados múltiplas vezes para dificultar a recuperação.
- Ofuscação/Renomeação: Alterar nomes de arquivos/pastas, tipos de arquivo para disfarçar.
- Uso de Máquinas Virtuais/Containers: Isolar atividades em ambientes descartáveis.
- Anti-Forense para Segurança Pública: Conhecer essas técnicas é fundamental para combatê-las.

Importância da Forense Computacional na Segurança Pública

FEBRABAN
CYBER LAB

- Combate ao Crime Cibernético: Investigação de fraudes, ataques, extorsões, crimes contra menores.
- Inteligência Policial: Análise de dados digitais para prevenção e elucidação de crimes.
- Provas Judiciais: Geração de evidências robustas para processos criminais.
- Segurança Nacional: Investigação de ciberataques contra infraestruturas críticas, espionagem.
- Desenvolvimento de Políticas: Informações forenses que ajudam a criar leis e políticas de segurança mais eficazes.
- Proteção à Sociedade: Identificação e responsabilização de criminosos digitais.

Forense Computacional

Agenda

Módulo 2: Preservação e Cadeia de Custódia de Evidências

- Preservação de Evidências: O Imperativo da Integridade
- Integridade da Evidência: Hashing Criptográfico
- Cadeia de Custódia: Definição e Propósito
- Elementos Essenciais da Cadeia de Custódia
- Dispositivos Write-Blockers: Protegendo o Original
- Métodos de Aquisição de Evidências: Dead vs. Live
- Ordem de Coleta de Evidências Voláteis (ORDEM DE VOLATILIDADE)
- Aquisição de Imagem de Disco (Forensic Imaging)
- Aquisição de Memória RAM (Memory Forensics)
- Aquisição de Evidências em Nuvem
- Aquisição de Evidências em Dispositivos Móveis
- Coleta de Evidências de Rede (Network Forensics)

Preservação de Evidências: O Imperativo da Integridade

FEBRABAN
CYBER LAB

- Definição: Proteger a evidência digital contra qualquer alteração, destruição ou corrupção.
- Objetivo Primordial: Manter a autenticidade e a integridade da evidência desde a coleta até a apresentação.
- Princípio Básico: "Não modifique o original." Trabalhe sempre com cópias.
- Consequência de Falha: Evidência pode ser invalidada e não ser aceita em juízo.

Integridade da Evidência: Hashing Criptográfico

FEBRABAN CYBER LAB

- Hashing: Função matemática que gera uma "assinatura digital" única para um dado.
- Propriedades:
  - Determinístico: Mesma entrada sempre gera a mesma saída.
  - Único (quase): Pequena alteração na entrada gera uma saída completamente diferente.
  - Não Inversível: Não é possível reconstruir a entrada a partir do hash.
- Algoritmos Comuns: MD5 (obsoleto para segurança), SHA1 (desaconselhado), SHA256 (comumente usado), SHA512.
- Uso na Forense: Calcular o hash da evidência original ANTES e DEPOIS da aquisição, e da cópia adquirida.

Cadeia de Custódia: Definição e Propósito

FEBRABAN
CYBER LAB

- Definição: Registro cronológico e documentado de todas as pessoas que tiveram posse da evidência, da coleta à apresentação.
- Propósito: Provar que a evidência não foi alterada, contaminada ou substituída.
- Fundamento Legal: Garante a admissibilidade da evidência em juízo.
- Elementos Chave: Quem, o quê, quando, onde, por que e como cada evidência foi tratada.

Elementos Essenciais da Cadeia de Custódia

FEBRABAN
CYBER LAB

- Identificação da Evidência: Número de identificação único, descrição detalhada do item.
- Local e Data/Hora da Coleta: Precisão de onde e quando a evidência foi encontrada.
- Pessoa que Coletou: Nome, assinatura, função.
- Local de Armazenamento: Onde a evidência foi guardada após a coleta.
- Transferências de Posse: Registro de quem recebeu a evidência de quem, quando e por que.
- Ações Realizadas: Cada acesso, análise, cópia ou extração, com data/hora e nome do responsável.
- Hashing da Evidência: Registros do hash do original e da cópia forense.

Dispositivos Write-Blockers: Protegendo o Original

FEBRABAN
CYBER LAB

- Função: Impedir que qualquer dado seja escrito ou modificado no dispositivo de evidência original.
- Operação: Atuam como uma "barreira de hardware" ou "software" entre o dispositivo original e o sistema do perito.
- Tipos:
  - Hardware Write-Blockers: Dispositivos físicos (portas USB, SATA, IDE) com firmware dedicado. Preferidos pela segurança e confiabilidade.
  - Software Write-Blockers: Soluções baseadas em software (ex: modo somente leitura de SO, ferramentas de linha de comando). Menos robustos, mas úteis em algumas situações.
- Importância: Garantem a não contaminação da evidência original durante a aquisição.

Métodos de Aquisição de Evidências: Dead vs. Live

FEBRABAN
/CYBER LAB

- Aquisição Dead (Forensic Acquisition):
  - Método: Desligar o dispositivo e adquirir os dados de uma mídia não volátil.
  - Vantagem: Maior integridade dos dados, menos risco de contaminação.
  - Desvantagem: Perda de evidências voláteis (RAM, processos ativos).
  - Uso: Discos rígidos, pendrives, dispositivos com armazenamento persistente.
- Aquisição Live (Live Forensics):
  - Método: Coletar dados de um sistema em execução.
  - Vantagem: Captura de evidências voláteis (RAM, conexões de rede, processos).
  - Desvantagem: Maior risco de modificar a evidência, processo complexo.
  - Uso: Análise de malware, sistemas comprometidos.

Ordem de Coleta de Evidências Voláteis (ORDEM DE VOLATILIDADE)

- Princípio: Coletar as evidências mais voláteis primeiro, antes que sejam perdidas.
- Sequência Típica (do mais volátil para o menos volátil):
  1. Registros de CPU e Cache: Quase impossíveis de capturar sem equipamentos especializados.
  2. Conteúdo da Memória RAM: Processos ativos, chaves, senhas.
  3. Estado da Rede: Conexões abertas, tabelas de roteamento, ARP cache.
  4. Processos em Execução: Lista de processos, serviços, handles abertos.
  5. Conteúdo de Disco Temporário/Swap: Dados que foram para o arquivo de paginação.
  6. Logs do Sistema: Event logs, logs de segurança (em alguns casos, podem ser mais persistentes).
- Objetivo: Maximizar a captura de dados que desapareceriam com o desligamento.

Aquisição de Imagem de Disco (Forensic Imaging)

FEBRABAN CYBER LAB

- Definição: Criação de uma cópia bit a bit exata de uma mídia de armazenamento.
- Diferença de Cópia Simples: Inclui espaço não alocado, slack space, e setores ocultos (Host Protected Area - HPA).
- Formatos Comuns: E01 (EnCase Forensic Image File), AFF (Advanced Forensic Format), RAW (dd image).
- Ferramentas: FTK Imager, AccessData Imager, EnCase Forensic, Guymager (Linux), dd.
- Processo:
  1. Conectar disco original a write-blocker.
  2. Conectar disco de destino (vazio, maior que o original).
  3. Executar ferramenta de imagem forense.
  4. Calcular hash da fonte e destino.

Aquisição de Memória RAM (Memory Forensics)

FEBRABAN CYBER LAB

- Objetivo: Capturar o conteúdo da memória volátil de um sistema em execução.
- Informações Fundamentais: Processos ativos, conexões de rede abertas, senhas em plaintext, chaves de criptografia, atividade de malware.
- Ferramentas: Volatility Framework, WinPMEM, LinPMEM, DumpIt.
- Processo:
  1. Executar a ferramenta de aquisição de RAM (localmente ou via rede).
  2. Salvar o dump da memória em uma mídia de destino externa e limpa.
  3. Calcular o hash do dump.
- Desafio: O próprio ato de coletar altera a memória.

Aquisição de Evidências em Nuvem

FEBRABAN
/CYBER LAB

- Desafio: Falta de acesso físico direto aos servidores.
- Abordagens:
  - Acordos com Provedores (Legal): Mandados judiciais ou requisições legais para acesso aos dados.
  - APIs e Ferramentas do Provedor: Uso de APIs e ferramentas específicas para exportar logs, snapshots de VMs, volumes de armazenamento.
  - Aquisição Live (em VMs): Se tiver acesso à VM, coletar memória/disco dentro do ambiente em nuvem.Considerações: Termos de serviço do provedor, jurisdição, privacidade.
- Exemplos: AWS S3 buckets, Google Drive, Microsoft Azure Storage.

Aquisição de Evidências em Dispositivos Móveis

FEBRABAN
CYBER LAB

- Desafio:
  - Diversidade de sistemas (iOS, Android), modelos, hardwares.
  - Criptografia de disco completa (FDE) padrão.
  - Bloqueios de tela (PIN, biometria).
  - Conexão constante à rede, alterando evidências.
  - Dificuldade de acesso físico (soldado, baterias internas).
- Métodos:
  - Logical Acquisition: Extração de dados visíveis (arquivos, contatos, SMS).
  - Physical Acquisition: Cópia bit a bit da memória flash (exige root/jailbreak, ou ferramentas forenses).
  - Chip-off Forensics: Remoção física do chip de memória.
  - JTAG/ISP: Acesso à memória via pinos de teste.
- Ferramentas: Cellebrite UFED, XRY, Oxygen Forensics.

Coleta de Evidências de Rede (Network Forensics)

FEBRABAN
CYBER LAB

- Objetivo: Monitorar e analisar o tráfego de rede para identificar atividades suspeitas ou maliciosas.
- Fontes de Dados:
  - Capturas de Pacotes (Packet Capture): Dados brutos de tráfego de rede (full content).
  - Dados de Fluxo (Flow Data): Metadados de conexão (quem, quando, para onde, quanto). Ex: NetFlow, IPFIX.
  - Logs de Dispositivos de Rede: Firewalls, roteadores, IDS/IPS.
- Ferramentas: Wireshark, tcpdump (captura); Zeek (Bro), Suricata (análise IDS); ELK Stack (logs).
- Desafio: Volume de dados, criptografia de tráfego (HTTPS).

Forense Computacional

Agenda

Módulo 3: Coleta e Análise de Logs e Dispositivos

- Coleta e Análise de Logs: O Diário do Sistema
- Fontes de Logs Comuns
- Coleta de Logs: Estratégias e Ferramentas
- Análise de Logs: Técnicas e Insights
- Análise Forense de Discos Rígidos: Fundamentos
- Sistemas de Arquivos: A Organização dos Dados
- Recuperação de Arquivos Deletados e Espaços Residuais
- Análise do Registro do Windows (Registry Forensics)
- Forense de Navegadores Web
- Forense de E-mails
- Ferramentas de Forense Digital: Visão Geral

Coleta de Evidências de Rede (Network Forensics)

FEBRABAN
CYBER LAB

- Objetivo: Monitorar e analisar o tráfego de rede para identificar atividades suspeitas ou maliciosas.
- Fontes de Dados:
  - Capturas de Pacotes (Packet Capture): Dados brutos de tráfego de rede (full content).
  - Dados de Fluxo (Flow Data): Metadados de conexão (quem, quando, para onde, quanto). Ex: NetFlow, IPFIX.
  - Logs de Dispositivos de Rede: Firewalls, roteadores, IDS/IPS.
- Ferramentas: Wireshark, tcpdump (captura); Zeek (Bro), Suricata (análise IDS); ELK Stack (logs).
- Desafio: Volume de dados, criptografia de tráfego (HTTPS).

Coleta e Análise de Logs: O Diário do Sistema

FEBRABAN
CYBER LAB

- Logs: Registros gerados por sistemas operacionais, aplicações e dispositivos de rede.
- Conteúdo: Eventos do sistema, ações do usuário, erros, tentativas de acesso, atividades de segurança.
- Importância: Base para reconstruir eventos, identificar atividades suspeitas e determinar a causa raiz.
- Desafio: Volume, heterogeneidade de formatos, tempo de retenção.

Fontes de Logs Comuns

FEBRABAN
CYBER LAB

- Sistemas Operacionais (SO):
  - Windows: Event Logs (Segurança, Sistema, Aplicação), logs do PowerShell, logs de Firewall.
  - Linux: Syslog, logs de autenticação (auth.log), logs de kernel (kern.log), logs de aplicações (Apache, Nginx).
- Aplicações:
  - Servidores Web (Apache, Nginx, IIS): Acessos, erros, requisições.
  - Bancos de Dados (SQL Server, MySQL, PostgreSQL): Acessos, alterações, erros.
  - Aplicações Legadas/Customizadas: Logs específicos da aplicação.
- Dispositivos de Rede: Firewalls, IDS/IPS, roteadores, switches, balanceadores de carga.
- Serviços em Nuvem: CloudTrail (AWS), Stackdriver (Google Cloud), Azure Monitor (Azure).

Coleta de Logs: Estratégias e Ferramentas

FEBRABAN
CYBER LAB

- Coleta Local (Manual): Acessar diretamente o dispositivo e copiar os arquivos de log.
  - Vantagem: Dados brutos originais.
  - Desvantagem: Lenta, escala mal, altera a evidência (se o SO está ligado).
- Coleta Remota (Agent-based): Agentes instalados nos dispositivos enviam logs para um servidor central.
  - Vantagem: Automatizada, escalável, menos intrusiva.
  - Desvantagem: Depende da instalação e configuração do agente.
- Centralização de Logs (SIEM/ELK): Sistemas que agregam, armazenam e analisam logs de múltiplas fontes.
  - Vantagem: Visão unificada, correlação de eventos, alertas.
  - Desvantagem: Complexidade de implantação, custo.
- Ferramentas: Syslog-ng, rsyslog (Linux), Winlogbeat, nxlog (Windows), Splunk, ELK Stack (Elasticsearch, Logstash, Kibana).

Análise de Logs: Técnicas e Insights

FEBRABAN
/CYBER LAB

- Filtragem: Reduzir o volume de logs para eventos relevantes (por data/hora, IP, usuário).
- Correlação de Eventos: Relacionar eventos de diferentes fontes para reconstruir uma sequência de ataque.
- Detecção de Anomalias: Identificar padrões incomuns que podem indicar atividades maliciosas.
- Pesquisa de Palavras-Chave: Buscar termos específicos (malware, erros, logins falhos).
- Análise de Tendências: Observar o comportamento ao longo do tempo.
- Timeline Analysis: Criar uma linha do tempo detalhada dos eventos.

Análise Forense de Discos Rígidos: Fundamentos

FEBRABAN
CYBER LAB

- Objetivo: Extrair e interpretar informações de mídias de armazenamento persistente.
- Conteúdo Analisado:
  - Sistema de Arquivos (FAT, NTFS, ext4, HFS+).
  - Arquivos e Pastas (visíveis, ocultos, protegidos).
  - Arquivos Deletados e Dados Residuais.
  - Metadados de Arquivos (timestamps, autor, software).
  - Registros do Sistema Operacional (Registry no Windows).
  - Artefatos de Internet (histórico de navegador, cache, cookies).
- Fase: Geralmente realizada após a aquisição da imagem forense.

Sistemas de Arquivos: A Organização dos Dados

FEBRABAN
/CYBER LAB

- Função: Estrutura lógica que o sistema operacional usa para organizar e gerenciar arquivos e diretórios em uma mídia.
- Informações fundamentais:
  - Tabela de Alocação de Arquivos: Onde os arquivos estão fisicamente no disco.
  - Metadata: Atributos de arquivos (nome, tamanho, datas de criação/modificação/acesso).
  - Estrutura de Diretórios: Hierarquia de pastas.
- Tipos Comuns e Suas Peculiaridades:
  - FAT (File Allocation Table): Mais antigo, simples, menos robusto.
  - NTFS (New Technology File System - Windows): Robusto, segurança, journaling, compressão, criptografia.
  - ext4 (Linux): Comum em Linux, journaling, grande volume.
  - HFS+ / APFS (macOS): Específicos da Apple.
- Importância Forense: O conhecimento do sistema de arquivos é essencial para recuperar dados e entender como o SO interage com o disco.

Recuperação de Arquivos Deletados e Espaços Residuais

FEBRABAN
CYBER LAB

- Princípio: Quando um arquivo é "deletado", seus dados raramente são apagados imediatamente.
- Áreas de Interesse:
  - Espaço Não Alocado (Unallocated Space): Áreas do disco que o sistema de arquivos considera vazias. Podem conter dados de arquivos deletados.
  - Slack Space: Espaço não utilizado no último cluster alocado para um arquivo. Pode conter resíduos de dados anteriores.
  - MFT (NTFS) / Inodes (ext4): Registros que armazenam metadados de arquivos, mesmo após a exclusão lógica.
- Técnicas: File Carving (busca por cabeçalhos/rodapés de arquivos), análise de tabelas de alocação.
- Ferramentas: PhotoRec, Foremost, EnCase, FTK.

Análise do Registro do Windows (Registry Forensics)

FEBRABAN
/CYBER LAB

- Registro (Registry): Banco de dados hierárquico que armazena configurações de baixo nível para o sistema operacional Windows, hardware, software e perfis de usuário.
- Informações Chave:
  - Programas instalados e executados recentemente (MRU - Most Recently Used).
  - Dispositivos USB conectados (Plug and Play - PnP).
  - Contas de usuário, senhas (hashing).
  - Configurações de rede, firewalls.
  - Histórico de pesquisa, documentos recentes.
  - Horários de boot e shutdown do sistema.
- Ferramentas: Registry Explorer, RegRipper, Autoruns.
- Importância: Tesouro de artefatos para a reconstrução de atividades do usuário e do sistema.

Forense de Navegadores Web

FEBRABAN
/CYBER LAB

- Objetivo: Analisar os artefatos deixados por navegadores web para reconstruir a atividade online do usuário.
- Artefatos Comuns:
  - Histórico de Navegação: URLs visitadas, timestamps.
  - Cache: Cópias locais de páginas web, imagens, scripts.
  - Cookies: Pequenos arquivos que armazenam informações de sessão, preferências, rastreamento.
  - Downloads: Lista de arquivos baixados.
  - Bookmarks/Favoritos: Sites salvos pelo usuário.
  - Autocompletar: Dados preenchidos automaticamente em formulários.
- Navegadores: Chrome, Firefox, Edge, Safari, Opera (cada um com formatos de armazenamento diferentes).

Forense de E-mails

FEBRABAN
CYBER LAB

- Objetivo: Investigar comunicações por e-mail para encontrar provas de fraude, assédio, espionagem, vazamento de dados.
- Fontes de E-mails:
  - Cliente de E-mail Local: Outlook (PST/OST), Thunderbird (MBOX).
  - Servidor de E-mail (Webmail/Corporativo): Caixa de entrada/saída em servidores (requer acesso legal).
  - Logs de Servidor de E-mail: Registros de envio, recebimento, tentativas de login.
- Análise de Cabeçalhos:
  - Remetente/Destinatário: Real, não apenas o que aparece na interface.
  - Rotas: Servidores pelos quais o e-mail passou.
  - Timestamps: Horários precisos de envio/recebimento.
  - IPs de Origem: Endereço IP do remetente original.
  - Conteúdo: Corpo da mensagem, anexos.

Ferramentas de Forense Digital: Visão Geral

FEBRABAN
/CYBER LAB

- Categorias:Aquisição: Criar cópias forenses (hardware write-blockers, FTK Imager).
- Análise: Examinar e extrair dados da imagem forense (EnCase, Autopsy, Volatility).
- Recuperação: Restaurar dados deletados (PhotoRec, Foremost).
- Visualização/Relato: Apresentar as descobertas (EnCase, FTK, Ferramentas de timeline).
- Tipos:
  - Open Source: Acessíveis, flexíveis, comunidade ativa.
  - Comerciais: Robustas, certificadas, suporte especializado.
- Importância: A escolha da ferramenta certa é fundamental para a eficiência e validade da investigação.

Forense Computacional

Agenda

Módulo 4: Ferramentas de Forense Digital

- Write-Blockers: Hardware vs. Software (Revisão e Comparação)
- Ferramentas de Imagem de Disco (Aquisição)
- Suítes Forenses Digitais (Análise Abrangente)
- Ferramentas de Memória Forense (RAM)
- Ferramentas de Rede Forense (Network Forensics)
- Ferramentas de Análise de Logs Centralizadas
- Ferramentas de Forense Móvel
- Ferramentas de Forense Open Source vs. Comerciais
- Virtualização e Contêineres em Forense Digital
- Hardware Forense Especializado

Write-Blockers: Hardware vs. Software (Revisão e Comparação)

Característica	Write-Blocker de Hardware	Write-Blocker de Software
Natureza	Dispositivo físico externo	Aplicação ou driver de SO
Nível de Operação	Nível físico/controlador de disco	Nível do sistema operacional
Confiabilidade	Alta (firmware dedicado, independente do SO)	Menor (depende da integridade do SO, pode ser burlado)
Custo	Mais elevado	Geralmente gratuito (modo somente leitura do SO)
Uso Comum	Aquisição forense padrão, em laboratório	Análise de disco em sistemas operacionais "vivos", emergências
Recomendação Forense	Preferencial (maior garantia de não modificação)	Uso limitado, com riscos maiores

Ferramentas de Imagem de Disco (Aquisição)

FEBRABAN
CYBER LAB

- FTK Imager (AccessData Imager):
  - Tipo: Ferramenta comercial gratuita.
  - Funções: Cria imagens forenses (E01, RAW, AD1), monta imagens, recupera arquivos deletados de forma limitada.
  - Interface: Gráfica, intuitiva.
- Guymager (Linux):
  - Tipo: Ferramenta open source.
  - Funções: Cria imagens forenses (E01, RAW) em ambiente Linux.
  - Interface: Gráfica.dd (Disk Dump - Linux):
  - Tipo: Ferramenta de linha de comando (open source).
  - Funções: Copia dados bit a bit de um dispositivo para outro.
  - Vantagem: Universal, poderoso.
  - Desvantagem: Requer conhecimento preciso da sintaxe, perigoso se usado incorretamente.
- EnCase Forensic / Magnet Acquire: Ferramentas comerciais líderes para aquisição e análise.

Suítes Forenses Digitais (Análise Abrangente)

FEBRABAN
CYBER LAB

- EnCase Forensic (OpenText):
  - Tipo: Comercial, uma das ferramentas mais antigas e abrangentes.
  - Funções: Aquisição, análise de sistema de arquivos, recuperação de dados, análise de artefatos, criação de relatórios.
  - Reconhecimento: Padrão da indústria, frequentemente usado em tribunais.
- FTK (Forensic Toolkit - AccessData):
  - Tipo: Comercial, similar ao EnCase em funcionalidade.
  - Funções: Processamento de imagens, indexação, pesquisa, análise de e-mails, análise de artefatos.
  - Vantagem: Integração com FTK Imager.
- Autopsy (The Sleuth Kit):
  - Tipo: Open Source, construída sobre o The Sleuth Kit.
  - Funções: Interface gráfica para análise de discos, recuperação de arquivos, análise de artefatos, timeline.
  - Vantagem: Gratuita, poderosa, extensível via módulos.

Ferramentas de Memória Forense (RAM)

FEBRABAN
CYBER LAB

- Volatility Framework:
  - Tipo: Open Source, uma das ferramentas mais completas para análise de dump de RAM.
  - Funções: Extrai processos, conexões de rede, chaves de registro, senhas, código de malware da memória.
  - Plataformas: Windows, Linux, macOS.
  - Interface: Linha de comando.
- LiME (Linux Memory Extractor):
  - Tipo: Open Source.
  - Funções: Ferramenta para criar dumps de RAM de sistemas Linux.
  - Vantagem: Pode ser carregada como módulo de kernel, minimizando a contaminação.
- WinPMEM / LinPMEM / MacPMEM (Google):
  - Tipo: Open Source.
  - Funções: Ferramentas de aquisição de RAM para diferentes sistemas operacionais.
  - Vantagem: Simples e eficaz.

Ferramentas de Rede Forense (Network Forensics)

FEBRABAN
CYBER LAB

- Wireshark:
  - Tipo: Open Source, analista de protocolo de rede gráfico.
  - Funções: Captura e análise detalhada de pacotes de rede.
  - Vantagem: Filtros poderosos, reconstrução de sessões, análise de protocolos.
- tcpdump:
  - Tipo: Open Source, ferramenta de linha de comando para captura de pacotes.
  - Funções: Captura pacotes brutos, ideal para automação e servidores remotos.
- Zeek (Bro):
  - Tipo: Open Source, IDS/IPS e sistema de monitoramento de segurança de rede.
  - Funções: Geração de logs detalhados de rede, detecção de intrusão, análise de protocolo.
  - Vantagem: Foco em metadados de conexão, scripts personalizados.
- Suricata:
  - Tipo: Open Source, IDS/IPS/NSM (Network Security Monitoring).
  - Funções: Detecção de intrusão (baseada em regras), análise de tráfego.

Ferramentas de Análise de Logs Centralizadas

FEBRABAN
CYBER LAB

- ELK Stack (Elasticsearch, Logstash, Kibana):
  - Tipo: Open Source, suite completa para ingestão, armazenamento, busca e visualização de logs.
  - Elasticsearch: Banco de dados distribuído para busca de logs.
  - Logstash: Pipeline de ingestão para coletar, transformar e enriquecer logs.
  - Kibana: Interface gráfica para visualização, dashboards e relatórios.
- Splunk:
  - Tipo: Comercial, líder de mercado em SIEM (Security Information and Event Management).
  - Funções: Ingestão de logs, monitoramento em tempo real, detecção de ameaças, correlação de eventos, relatórios forenses.
  - Vantagem: Poderoso, escalável, rico em funcionalidades.
  - Desvantagem: Alto custo.
- Graylog:
  - Tipo: Open Source (com versão Enterprise).
  - Funções: Gerenciamento centralizado de logs, análise, alertas.

Ferramentas de Forense Móvel

FEBRABAN
CYBER LAB

- Cellebrite UFED (Universal Forensic Extraction Device):
  - Tipo: Comercial, líder de mercado.
  - Funções: Extração lógica e física de dados de milhares de modelos de celulares.
  - Avançado: Desbloqueio de dispositivos, bypass de criptografia.
- XRY (MSAB):
  - Tipo: Comercial, concorrente do Cellebrite.
  - Funções: Extração e análise de dados de dispositivos móveis.
- Oxygen Forensics Detective:
  - Tipo: Comercial.
  - Funções: Análise de dados de celulares, tablets, drones e dispositivos de IoT.
- Magnet AXIOM:
  - Tipo: Comercial, suite forense que inclui análise de mobile.
  - Funções: Análise de artefatos de dispositivos móveis e computadores.

Ferramentas de Forense Móvel

FEBRABAN
/CYBER LAB

- Ferramentas Open Source:
  - Vantagens: Gratuito, código aberto (transparência), flexibilidade, comunidade ativa, inovação.
  - Desvantagens: Sem suporte formal, curva de aprendizado, exige maior conhecimento técnico.
  - Exemplos: Autopsy/TSK, Volatility, Wireshark, dd, Guymager, ELK Stack.
- Ferramentas Comerciais:
  - Vantagens: Suporte técnico, interfaces amigáveis, automação, certificação, aceitação legal.
  - Desvantagens: Alto custo, código fechado (black box), menos flexibilidade.
  - Exemplos: EnCase, FTK, Cellebrite, XRY, Splunk.Melhor
- Prática: Combinar o uso de ambas para aproveitar os benefícios de cada uma.

Virtualização e Contêineres em Forense Digital

FEBRABAN CYBER LAB

- Uso: Criar ambientes isolados e controlados para análise de malware, engenharia reversa e testes.
- Máquinas Virtuais (VMs):
  - Vantagens: Isolamento completo do sistema host, fácil criação de snapshots (pontos de restauração).
  - Uso: Análise de malware com segurança, testes de ferramentas.
- Contêineres (Docker):
  - Vantagens: Leves, rápidos para iniciar e descartar, ideal para ferramentas forenses.
  - Uso: Empacotar e executar ferramentas forenses em ambientes consistentes.
- Benefício: Proteção da estação de trabalho forense contra códigos maliciosos e garantia de um ambiente de análise limpo.

Hardware Forense Especializado

FEBRABAN
CYBER LAB

- Uso: Criar ambientes isolados e controlados para análise de malware, engenharia reversa e testes.
- Máquinas Virtuais (VMs):
  - Vantagens: Isolamento completo do sistema host, fácil criação de snapshots (pontos de restauração).
  - Uso: Análise de malware com segurança, testes de ferramentas.
- Contêineres (Docker):
  - Vantagens: Leves, rápidos para iniciar e descartar, ideal para ferramentas forenses.
  - Uso: Empacotar e executar ferramentas forenses em ambientes consistentes.
- Benefício: Proteção da estação de trabalho forense contra códigos maliciosos e garantia de um ambiente de análise limpo.

Forense Computacional

Agenda

Módulo 5: Relatórios e Boas Práticas de Documentação

- Relatórios Forenses: Propósito e Audiência
- Componentes Essenciais de um Relatório Forense
- Boas Práticas de Documentação Durante a Investigação
- Linguagem e Objetividade no Relato
- Reconstrução da Linha do Tempo (Timeline Analysis)
- Visualização de Dados Forenses
- Admissibilidade Legal da Evidência Digital
- Considerações Éticas no Relato Forense
- O Papel do Testemunho e do Perito Expert
- Desafios Contemporâneos na Forense Digital
- Desenvolvimento Profissional Contínuo
- Boas Práticas Essenciais em Forense Computacional
- Resumo Geral: Forense Computacional - Uma Perspectiva Integrada
- Futuro da Forense Computacional: Novos Horizontes
- Perguntas e Discussão

Relatórios Forenses: Propósito e Audiência

FEBRABAN
/CYBER LAB

- Propósito Primordial: Comunicar as descobertas da investigação de forma clara, objetiva e imparcial.
- Fundamentação: Apresentar fatos e análises técnicas que suportem conclusões.
- Audiências Diversas:
  - Técnica: Outros peritos, analistas de segurança.
  - Gerencial/Executiva: Diretores, gerentes (foco no impacto).
  - Jurídica: Advogados, juízes, júri (foco na admissibilidade e peso da prova).
- Qualidade: O relatório é o "produto final" da investigação e deve ser impecável.

Componentes Essenciais de um Relatório Forense

FEBRABAN
CYBER LAB

- Sumário Executivo: Breve visão geral do incidente, metodologia e principais conclusões (para gerentes/executivos).
- Informações do Investigador: Nome, credenciais, certificações.
- Escopo da Investigação: Limites, objetivos, autorização legal.
- Metodologia: Ferramentas, técnicas e procedimentos utilizados.
- Cadeia de Custódia: Registro detalhado da evidência.
- Descobertas (Findings): Apresentação dos fatos relevantes e evidências (objetivo, detalhado, com referências).
- Conclusões: Respostas aos objetivos da investigação, baseadas nas descobertas.
- Opinião Pericial: Se aplicável, a interpretação do perito sobre as descobertas.
- Apêndices: Evidências em formato bruto (logs, capturas de tela, hashes).

Boas Práticas de Documentação Durante a Investigação

FEBRABAN / CYBER LAB

- Registros Contemporâneos: Documentar cada passo à medida que ele acontece.
- Detalhe: Registrar comandos, outputs, configurações, datas/horas, nomes de arquivos, hashes.
- Coerência: Usar um formato padronizado (modelos, formulários).
- Anotações Claras: Manter um log de investigação detalhado, legível e organizado.
- Capturas de Tela/Vídeos: Registrar o estado do sistema, a execução de ferramentas.
- Backup Regular: Salvar a documentação e os dados da investigação em local seguro.
- Objetivo: Reconstruir o processo de investigação se necessário, garantir transparência.

Linguagem e Objetividade no Relato

FEBRABAN
CYBER LAB

- Linguagem Clara e Concisa: Evitar jargões técnicos excessivos, usar termos simples quando possível.
- Público-Alvo: Adaptar a linguagem ao nível de compreensão da audiência.
- Objetividade: Apresentar apenas os FATOS e as EVIDÊNCIAS.
- Neutralidade: Evitar julgamentos de valor, opiniões pessoais ou especulações.
- Formato Consistente: Usar formatação padrão, tabelas, gráficos para clareza.
- Gramática e Ortografia: Revisão rigorosa para garantir profissionalismo e credibilidade.

Reconstrução da Linha do Tempo (Timeline Analysis)

FEBRABAN
CYBER LAB

- Definição: Construção de uma representação cronológica de eventos a partir de múltiplas fontes de evidência.
- Fontes de Dados: Timestamps de arquivos, logs de sistema, logs de aplicações, eventos de rede, entradas de registro.
- Objetivo: Reconstruir a sequência de ações e identificar o momento exato de cada evento.
- Importância:
  - Identificar a causa raiz de um incidente.
  - Determinar a extensão da intrusão.
  - Correlacionar eventos de diferentes fontes.
  - Comprovar ou refutar alegações.
  - Ferramentas: Plaso/log2timeline, Autopsy, EnCase.

Visualização de Dados Forenses

FEBRABAN
/CYBER LAB

- Propósito: Tornar dados complexos mais compreensíveis e insights mais evidentes.
- Tipos de Visualização:
  - Gráficos de Linha do Tempo: Representação cronológica de eventos.
  - Gráficos de Barras/Pizza: Distribuição de tipos de arquivos, atividades.
  - Mapas de Calor: Concentração de atividades em áreas do disco ou rede.
  - Diagramas de Rede: Fluxo de comunicação, topologia de ataque.
  - Mapas Geográficos: Localização de IPs, dispositivos (se disponível).
- Ferramentas: Kibana (ELK), Maltego, Gephi, Excel/PowerBI.
- Importância: Facilitar a comunicação no relatório e no testemunho.

Admissibilidade Legal da Evidência Digital

FEBRABAN
/CYBER LAB

- Requisitos Legais:
  - Autenticidade: Provar que a evidência é o que alega ser.
  - Integridade: Provar que a evidência não foi alterada.
  - Relevância: Provar que a evidência se relaciona com o caso.
  - Confiabilidade: Provar que a metodologia de coleta e análise é sólida.
- Cadeia de Custódia: Registro detalhado e ininterrupto para comprovar integridade e autenticidade.
- Perícia Oficial: No Brasil, a prova pericial é produzida por peritos oficiais (Polícia Federal, Polícia Civil).
- Juízo Crítico: O juiz, em última instância, decide sobre a admissibilidade da prova.

Considerações Éticas no Relato Forense

FEBRABAN
CYBER LAB

- Imparcialidade: Apresentar os fatos de forma neutra, sem favorecer nenhuma parte.
- Objetividade: Basear as conclusões em evidências concretas, não em suposições.
- Confidencialidade: Proteger informações sensíveis, dados pessoais e segredos comerciais.
- Competência: Não apresentar conclusões fora da área de expertise.
- Honestidade: Não omitir ou distorcer fatos.
- Integridade: Manter a honestidade intelectual e profissional.
- Evitar Vieses: Reconhecer e mitigar vieses pessoais que possam afetar a análise.

O Papel do Testemunho e do Perito Expert

FEBRABAN
CYBER LAB

- Testemunho em Juízo: O perito pode ser chamado a depor em tribunal para explicar o relatório e suas conclusões.
- Perito Expert: Pessoa com conhecimento, habilidade, experiência, treinamento ou educação especializada.
- Função: Ajudar o juiz ou júri a entender provas técnicas complexas.
- Qualidades:
  - Clareza na comunicação.
  - Capacidade de simplificar conceitos complexos.
  - Firmeza e convicção (baseada em fatos).
  - Integridade e imparcialidade.
- Desafio: Resistir ao questionamento (contraditório) da parte adversa.

Desafios Contemporâneos na Forense Digital

FEBRABAN
CYBER LAB

- IoT (Internet das Coisas): Milhões de dispositivos conectados, novos tipos de evidência (dados de sensores, câmeras inteligentes).
- Inteligência Artificial (IA): Análise de dados massivos, mas também IA como ferramenta de ataque ou defesa.
- Big Data: Volume colossal de informações a serem processadas.
- Blockchain e Criptomoedas: Transações pseudo-anônimas e descentralizadas.
- Deepfakes e Fraudes Avançadas: Dificuldade em distinguir conteúdo real de sintético.
- Privacidade e Criptografia Generalizada: Balancear segurança com capacidade de investigação.
- Recursos Limitados: Necessidade de constante investimento em treinamento e ferramentas.

Desenvolvimento Profissional Contínuo

FEBRABAN
CYBER LAB

- Aprendizagem Contínua: Novas tecnologias, técnicas e ferramentas surgem constantemente.
- Treinamento e Certificações: Manter-se atualizado com as melhores práticas (SANS, GIAC, EC-Council).
- Comunidade: Participar de fóruns, conferências, grupos de estudo.
- Pesquisa: Contribuir para o avanço da área através de estudos e experimentos.
- Ética: Reafirmar constantemente os princípios éticos e legais.

Boas Práticas Essenciais em Forense Computacional

FEBRABAN
/CYBER LAB

- Preparação: Ter planos de resposta, kits forenses e equipe treinada.
- Isolamento: Desconectar imediatamente o dispositivo da rede (mas não desligar, se houver evidência volátil).
- Preservação: Usar write-blockers e coletar do mais volátil para o menos.
- Hashing: Calcular e registrar hashes antes e depois da aquisição.
- Cadeia de Custódia: Documentar cada movimento e ação sobre a evidência.
- Análise Criteriosa: Trabalhar em cópias, usar ferramentas validadas, manter objetividade.
- Documentação Detalhada: Registrar tudo, de forma contemporânea.
- Relato Claro: Apresentar as descobertas de forma imparcial e compreensível.
- Atualização: Manter-se sempre atualizado com as tecnologias e leis.

Resumo Geral: Forense Computacional - Uma Perspectiva Integrada

FEBRABAN / CYBER LAB

- Ciência e Arte: Combina metodologia científica, conhecimento técnico e arte da investigação.
- Processo Multidisciplinar: Integra TI, Direito, Ética e habilidades de comunicação.
- Ciclo Contínuo: Identificação -> Preservação -> Coleta -> Análise -> Documentação -> Relato.
- Foco na Integridade: Autenticidade, confiabilidade e admissibilidade da evidência são imperativos.
- Dinâmico: Adaptação constante a novas tecnologias e ameaças.
- Impacto Social: Ferramenta fundamental para a justiça, segurança e proteção no mundo digital.

Futuro da Forense Computacional: Novos Horizontes

FEBRABAN
/CYBER LAB

- Automação e IA: Ferramentas inteligentes para processamento e correlação de evidências.
- Forense em Nuvem: Padronização de metodologias e cooperação com provedores.
- Forense de IoT: Desafios de escala, diversidade de dispositivos e padrões de dados.
- Forense de Dados Criptografados: Pesquisa contínua em métodos de recuperação ou bypass legal.
- Forense Comportamental: Análise de padrões de uso para identificar intenção.
- Resposta a Incidentes Proativa: Integração mais profunda com IR e Threat Hunting.
- Educação e Padrões: Necessidade de mais profissionais qualificados e normas internacionais.

Perguntas e Discussão

FEBRABAN
/CYBER LAB

- Conceitos Fundamentais: Estamos prontos para identificar, preservar, coletar e analisar evidências digitais?
- Desafios Reais: Como aplicaremos esses conhecimentos na prática, especialmente em Segurança Pública?
- Próximos Passos: O que mais você gostaria de explorar sobre este tema?

FEBRABAN
/CYBER LAB

Muito Obrigado!!!