Computação Forense e Investigação Digital

Fundamentos da Computação Forense

PETTER ANDERSON LOPES

FORENSE NA HISTÓRIA

O forense existe desde os primórdios da justiça.

Francis Galton (**1822–1911**) fez o primeiro estudo registrado de **impressões digitais**, Leone Lattes (**1887–1954**) descobriu **agrupamentos sanguíneos** (A, B, AB e 0), Calvin Goddard (**1891–1955**) permitiram armas de fogo e comparação de balas para resolver muitos processos judiciais pendentes, Albert Osborn (**1858-1946**) desenvolveu características essenciais do **exame documental**, Hans Gross (**1847–1915**) fez uso de estudo científico para liderar **investigações criminais**.
E em **1932**, o **FBI** criou um laboratório para fornecer serviços forenses a todos os agentes de campo e outras autoridades jurídicas em todo o país.

COMPUTAÇÃO FORENSE

A atividade cibernética tornou-se uma parte importante da vida cotidiana do público em geral. Smartphones, Drones, IoT, SmartTVs, etc...

O exame da **evidência digital** forneceu um meio para investigadores forenses focar depois que um incidente ocorreu. **O objetivo final de um investigador em computação forense é determinar a natureza e os eventos relativos a um crime e localizar o perpetrador seguindo um procedimento investigativo estruturado**.

O que é computação forense? Uma série metódica de técnicas e procedimentos para coleta de evidências, de equipamentos de computação e vários dispositivos de armazenamento e mídia digital, que podem ser apresentados em um tribunal de justiça em um formato coerente e significativo.
—Dr. H.B. Wolfe

COMPUTAÇÃO FORENSE - OBJETIVO

Determinar a natureza e os eventos relativos a um crime e localizar o perpetrador seguindo um procedimento investigativo estruturado.

Por meio de uma série metódica de técnicas e procedimentos para coleta de evidências, de equipamentos de computação e vários dispositivos de armazenamento e mídia digital, que podem ser apresentados em um tribunal de justiça em um formato coerente e significativo.

COMPUTAÇÃO FORENSE

Os investigadores devem aplicar **dois testes** para obter evidências tanto em ambiente virtual quanto ambiente físico para sobreviver em um tribunal:

■ Autenticidade: De onde vem a evidência?
Obtida do dispositivo original...

■ Confiabilidade: A evidência é confiável e isenta de falhas?
Foi coletada de forma correta...

COMPUTAÇÃO FORENSE

Computação forense está constante desenvolvimento.
Diferencia-se de outras ciências forenses como evidência digital é examinada.
Há um pouco de conhecimento teórico para basear suposições para análise e teste de hipóteses empíricas padrão quando realizado falta treinamento adequado ou padronização de ferramentas e, finalmente, é ainda mais "arte" do que "ciência".

NIST's "**Computer Security Incident Handling Guide**," SP800-61, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST's "**Guide to Integrating Forensic Techniques into Incident Response**," SP800-96, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

RFC 3227, "**Guidelines for Evidence Collection and Archiving**," www.faqs.org/rfcs/rfc3227.html

---

CRIMES NO AMBIENTE VIRTUAL

Dos crimes mais comumente cometidos no meio virtual temos:

Calúnia, Insultos, Difamação, Divulgação de material confidencial, Ato obsceno, Apologia ao crime, Perfil falso, Preconceito ou discriminação, Pedofilia, Distribuição de malware, Distribuição de ransomware, CryptoJacking, Ataques de injeção, Pharming, Phishing, E-mail Bombing and Spamming, Phishing, Identity Theft, Cyberstalking, Uso ilegal da internet, DDoS Attacks, Social Engineering.

OBJETIVOS

O principal objetivo da **análise forense digital** é investigar crimes cometidos usando dispositivos de computação como **computadores**, **tablets**, **telefones celulares** ou qualquer outro dispositivo que pode armazenar/processar dados digitais e extrair evidências digitais de uma forma que possa ser apresentada em um tribunal.

OBJETIVOS

- Encontrar evidências legais em dispositivos de computação e preservar sua integridade de uma forma que seja considerada admissível em um tribunal de justiça.
- Conservação e recuperação de provas, após aceitação dos procedimentos técnicos pela corte.
- Atribuir uma ação ao seu iniciador.

OBJETIVOS

- Identificando vazamentos de dados dentro de uma organização.
- Acessando possíveis danos ocorridos durante uma violação de dados.
- Apresentar os resultados em um relatório formal adequado para ser apresentado em corte.
- Fornecer um guia para testemunho de especialistas em tribunal.

CATEGORIAS

Computação Forense

Este é o tipo mais antigo de análise forense digital, é a área que aborda a investigação digital evidências encontradas em computadores **desktop**, **laptops**, dispositivos de armazenamento digital (como **discos rígidos** externos, **pen drives** e **cartões SD**) e na **memória RAM**, SO e rastreamentos de aplicativos instalados e logs associados. Uma das atividades recorrentes é **recuperar dados excluídos** e analisá-los para **incriminar** ou **exonerar** evidências.

CATEGORIAS

Forense Móvel ou Mobile

É a análise forense digital voltada para a obtenção de evidências digitais de **dispositivos móveis**, bem como dispositivos computacionais como telefones, smartphones, tablets e dispositivos portáteis, como relógios inteligentes.

A proliferação desta tecnologia **poderá** tornar a forense em dispositivos móveis o **ramo mais utilizado** entre outros tipos forenses digitais.

CATEGORIAS

Forense de rede

Análise forense digital que 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** afim 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

CATEGORIAS

Forense em Banco de dados

Nesta modalidade ocorre a **análise de dados** e **metadados** existentes dentro de um banco de dados, como Microsoft SQL Server, Oracle, MySQL e outros.

Banco de dados forense procura quem acessa um banco de dados e quais ações são executadas para ajudar a descobrir atividades maliciosas realizadas.

CATEGORIAS

Forense em Banco de dados

Nesta modalidade ocorre a **análise de dados** e **metadados** existentes dentro de um banco de dados, como Microsoft SQL Server, Oracle, MySQL e outros.

Banco de dados forense procura quem acessa um banco de dados e quais ações são executadas para ajudar a descobrir atividades maliciosas realizadas.

Petter Anderson Lopes
DPO (LGPD e GDPR), Perito Digital, Hacker Ético, Árbitro (Juiz Arbitral)

P +55 (54)99645-0777 E petter@periciacomputacional.com
W www.periciacomputacional.com
Skype petter.lopes

Microsoft
Specialist

Programming in HTML5 with JavaScript and CSS3 Specialist

EXIN
Privacy & Data Protection
FOUNDATION
Certified by EXIN

CERTIFIED EXAMINER
ACE
ACCESSDATA