Resumos AFD

Investigação Digital:

Técnicas e ferramentas que permitem recuperar, preservar e analisar evidências digitais armazenadas em, ou transmitidas por dispositivos digitais.

Evidência Digital:

Objeto digital que contém informação fidedigna que suporte ou refute uma hipótese.

A Investigação Digital tenta identificar:

- Quais os dispositivos envolvidos no incidente;
- Qual o uso dado aos dispositivos;
- Qual o motivo por detrás do incidente;
- Quem causou o incidente;

Investigação Digital Forense:

- Forma mais restrita de investigação digital
- Possui requisitos legais (validade em tribunal)

Onde se Aplica:

Recuperação de Dados:

- Falhas em equipamentos centrais à operação;
- Não existência de mecanismos de redundância
- Catástrofes naturais (não previstas)

(Foco na continuidade do negócio)

Atividades não autorizadas:

- Natureza não técnica;
- Ações ilícitas mal-intencionadas;
- Visam corromper, danificar, impedir operação, etc., de sistemas informáticos

(Foco na prova pericial (policias))

Onde procura evidencias:

- Todo e qualquer suporte de armazenamento de informação (volátil ou permanente)
- Ficheiros recuperados após eliminação (e respetiva informação)
- Windows Registry (histórico de dispositivos USB, últimos ficheiros acedidos, ...)
- Ficheiros de serviços de impressão (spool)
- Ficheiros de hibernação e de memoria virtual (swap)
- Espaço livre, ficheiros temporários, cache de browsers
- ...

Que evidências é possível obter:

- Ficheiros eliminados
- Dados temporários (data de eliminação, modificação, acesso, criação,...)
- Identificar que dispositivos de armazenamento (ex: USB) estavam ligados a um PC específico
- Histórico de navegação de internet
- ...

Exemplos de evidencias digitais:

- Documentos (docx, pptx, xlsx, ...)
- Emails (ameaças, divulgação de informação confidencial)
- Software malicioso
- Mensagens
- Trabalhos de impressão eliminados
- ...

Processo de analise forense digital:

1 – Identificação de fontes de evidencias digitais

- Que equipamentos foram utilizados pelo suspeito?

2 – Preservação e copia de evidencias digitais

- Se é possível, fazer cópias fidedignas para analise posterior

3 – Análise minuciosa das evidencias digitais

- Recuperação de ficheiros (undele, file carving)
- Pesquisa por palavras-chave
- Inspeção do Windows Registry
- Geração de diagramas temporais (timelines)

4 - Documentação e apresentação dos resultados

- Elaboração de relatórios periciais
- Depoimento ou testemunho em tribunal

Princípios orientadores:

1- As ações desencadeadas pelos investigadores não podem alterar os dados em análise que possam vir a ser usados como prova.

2- Em circunstâncias excecionais, caso seja necessário aceder aos dados originais, quem o fizer deve ter competência para tal e ser capaz de explicar a relevância e implicações das suas ações.

3- Deve ser criada e preservada uma cadeia de auditoria, registando-se todos os processos aplicados aos dados, possibilitando a verificação por repetição.

4- A pessoa responsável pelo inquérito deve garantir a observância da lei e destes princípios.

Técnicas anti-forenses:

Conjunto de ferramentas que visam dificultar ou impedir a analise de evidencias

- Ferramentas que escondem informação (encriptação, estenografia, ...)
- Ferramentas que removem evidencias (limpeza de discos ou ficheiros, destruição de discos, ...)
- Ferramentas que escondem registos (alteração de timestamps em ficheiros, alteração de cabeçalhos de ficheiros, ...)

Funções de Hash e Integridade de Dados

- MD5 e SHA-1 → Já não são considerados seguros devido a colisões.
- SHA-256 e SHA-512 → Algoritmos recomendados para garantir integridade