1BYTE 100110 101010

EDUCAÇÃO DIGITAL EM 8 BLOCOS

25 DE NOVEMBRO DE 2024 - 4ª edição

Núcleo de Inovação e Tecnologia

PROVA DIGITAL CONCEITOS FUNDAMENTAIS

1) O que é uma prova digital? É qualquer evidência armazenada ou transmitida em meio eletrônico, que tenha valor probatório em processos judiciais ou administrativos (artigo 4º do PL 4939/2020).

2) Quais leis, normas e padrões regulamentam as provas digitais no Brasil? As principais normas são Código de Processo Penal (arts. 158-A e seguintes), o Código de Processo Civil (art. 195 e art. 411), a Lei 11.419/2009 (Processo Eletrônico) e o Decreto 10.046/2019, Lei 12.965/2014 (Marco Civil da Internet), ISO/IEC 27037 (Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais) e ISO/IEC 27041 (Orientações para avaliação de processos de investigação digital).

3) Quais são os elementos essenciais de uma prova digital? **1-Autenticidade:** É a propriedade que garante que a prova é o que afirma ser, comprovando sua origem e autoria; **2-Integridade:** Refere-se à garantia de que a prova não foi modificada ou alterada desde a sua coleta. Isso pode ser assegurado por técnicas como algoritmos de hash e padrões de segurança; **3-Completude:** Significa que todos os dados relevantes foram coletados, incluindo os contextos necessários para interpretação; **4-Auditabilidade:** É a capacidade de verificar, passo a passo, o processo pelo qual a prova foi coletada, analisada e apresentada, assegurando transparência e rastreabilidade; **5-Preservação da Cadeia de Custódia:** É o controle rigoroso e documentado de todas as etapas pelas quais a prova passou, desde a coleta até a apresentação no tribunal.

4) Quais são as 10 etapas da cadeia de custódia digital? **1- Reconhecimento:** Identificação do objeto da produção probatória e delimitação do que será coletado; **2- Isolamento:** Preservação do ambiente físico ou eletrônico onde ocorrerá a coleta; **3-Fixação:** Descrição detalhada do objeto, incluindo seu estado e o meio em que se encontra; **4-Coleta:** Recolhimento da evidência de forma adequada, respeitando as melhores práticas forenses; **5-Acondicionamento:** Armazenamento da prova em mídia compatível ou embalagem apropriada, preservando sua integridade; **6-Transporte:** Transferência da prova coletada de forma segura, garantindo que não seja alterada ou danificada; **7-Recebimento:** Registro protocolar da entrega da evidência no local de análise ou armazenamento; **8-Processamento:** Análise técnica ou pericial da prova para elaboração de laudos e conclusões; **9-Armazenamento:** Guarda da evidência bruta para eventuais contraperícias; **10-Descarte:** Inutilização do vestígio de acordo com a legislação.

5) Quais os desafios específicos das provas digitais? A volatilidade dos dados digitais, a necessidade de ferramentas forenses adequadas e a preservação da integridade e autenticidade ao longo do processo judicial.

6) O que são metadados de arquivos? Metadados são informações descritivas que fornecem detalhes sobre um arquivo digital, como sua origem, propriedades e histórico. Eles não fazem parte do conteúdo principal do arquivo, mas registram informações auxiliares que são fundamentais para entender como, quando e por quem o arquivo foi criado, modificado ou acessado.

7) Como garantir a autenticidade e a integridade de uma prova digital? Utilizando ferramentas certificadas, como **algoritmos de hash (ex. MD5, SHA256, CRC)** que comprovam que os dados não foram modificados desde sua coleta, ou uma timestamp (estampa de tempo), que registra a data e a hora exatas de um evento ou ação em um sistema eletrônico, são alguns padrões de segurança recomendados pela doutrina.

8) Quais são as feramentas forenses mais populares para produção de provas digitais? Ferramentas forenses digitais, como **EnCase Forensic**, **FTK** e **Autopsy**, são essenciais para coletar, analisar e preservar evidências eletrônicas de forma técnica e juridicamente válida. Outras, como **Cellebrite** e **Magnet AXIOM**, destacam-se na análise de dispositivos móveis e dados na nuvem, enquanto **Wireshark** e **Volatility** são usadas para redes e memória volátil. Open-source como **Autopsy** e especializadas como **X-Ways Forensics** e **Oxygen Forensics** abrangem desde a recuperação de dados apagados até a análise de mensagens em aplicativos.

Gostou do conteúdo? Siga-nos em nossas rede:

@osinquietosmp @Osinquietosmp

@carmaidigital @julia_schutt @marcioafcunha