LAB 04 | Preservação de evidências digitais

Crie um registro de custódia e verifique integridade de um arquivo de demonstração com hash SHA-256.

Uso exclusivo em ambiente próprio, isolado ou expressamente autorizado. Materiais e endereços de teste são fictícios.

Objetivos de aprendizagem

- Gerar hash SHA-256 de um arquivo próprio
- Registrar origem, aquisição e transferências
- Diferenciar integridade, autenticidade e autoria

Procedimento passo a passo

01 Preparar a evidência de teste

Crie um pequeno arquivo de texto fictício, como evidencia_teste.txt, e registre sua origem. Não utilize dados reais de terceiros.

02 Calcular o hash inicial

No Linux, use sha256sum evidencia_teste.txt; no Windows, use certutil -hashfile evidencia_teste.txt SHA256. Copie o valor no registro.

03 Fazer cópia de trabalho

Copie o arquivo para outra pasta sob sua administração. Evite alterar o original e registre data, responsável e finalidade da cópia.

04 Validar integridade

Calcule o SHA-256 da cópia e compare os dois valores. Se forem distintos, identifique possíveis alterações.

05 Documentar a cadeia de custódia

Registre identificador, origem, responsável, hash, armazenamento, acesso e eventuais transferências. Formule conclusões proporcionais à evidência.

Evidências esperadas

- Valores de hash do original e da cópia
- Registro de origem e responsáveis
- Conclusão sobre integridade da cópia

Checklist de execução

[ ] Arquivo de teste identificado

[ ] Hash inicial anotado

[ ] Cópia de trabalho criada

[ ] Hashes comparados

[ ] Registro de custódia preenchido

Questões para discussão

1. Um hash igual demonstra automaticamente quem criou um arquivo?

2. Por que registrar todos os acessos e transferências de evidências?

Registro final

Data: ____ / ____ / _____ Responsável: _____

Resultado, justificativa e limitações: