UNIVERSIDADE ESTADUAL JULIO MESQUITA FILHO

Trabalho 2

Diego Pereira dos Reis

Presidente Prudente

2024

Introdução

Para esta auditoria, o programa Autopsy foi escolhido porque tem uma interface simples e uma grande variedade de funcionalidades para análise forense digital. Autopsy é uma plataforma de código aberto que facilita a investigação de dispositivos de armazenamento digital. Ele permite a recuperação de dados apagados, análise de histórico de navegação, extração de metadados e muitas outras funções importantes para uma auditoria detalhada.

Contextualização do Caso

Fui convocado para conduzir uma auditoria na empresa Reis devido à suspeita de vazamento de informações confidenciais. A empresa informou que informações confidenciais, como dados financeiros e de clientes, podem ter sido acessadas e copiadas de forma não autorizada.

O objetivo desta auditoria é determinar se houve o vazamento, os dados acessados ou copiados e em qual horários foram realizados. Um computador específico que é suspeito de ter sido usado para esse propósito será usado para realizar a auditoria. Vamos nos concentrar na análise do disco rígido deste computador para encontrar arquivos apagados e outros artefatos digitais que possam sugerir atividades suspeitas.

Relatório da Auditória

1. **Recuperação de arquivos apagados**: foi identificado um arquivo apagado “DadosClientes - Copia.txt”.
2. **Analise do conteúdo de arquivo recuperados**: uma vez feita uma análise do conteúdo do arquivo, foi comprovado a existência de dados confidenciais de clientes da empresa.
3. **Análise dos MetaDados de arquivos recuperados**: ao analisar o arquivo recuperado é possível identificar seu horário de criação “2024-06-04 15:11:43 BRT”, também é identificado que este arquivo teve sua última modificação “2024-06-04 15:08:22 BRT”. Com isso é possível identificar que este arquivo é uma cópia de outro arquivo, pois seu horário de criação é posterior a sua última modificação.
4. **Conclusão**: Foi identificado uma cópia seguida de uma exclusão de um arquivo confidencial da empresa, às 15:08:22 na seguinte data 04/06/2024.