



MINERAÇÃO DE DADOS APLICADOS À ANÁLISE FORENSE

MARIANE MOREIRA BATISTA; SIBELIUS LELLIS VIEIRA.
mbatista1711@gmail.com

Na era da informação atual, em que há um maior índice na inclusão digital e maior acessibilidade aos computadores, é também possível se deparar com o crescimento do índice de atividades ilícitas (disseminação de pornografia infantil, fraudes financeiras, furto de informações, invasão dos sistemas por parte dos hackers). Neste sentido, é importante poder realizar uma análise mais detalhada de equipamentos computacionais utilizando técnicas da computação forense para a investigação desses crimes. A computação forense mescla a formação jurídica com a tecnologia da informação e se baseia na análise de dados armazenados em um sistema operacional, computador ou rede na busca por evidências da prática de crimes. O objetivo do trabalho apresentado é utilizar técnicas de mineração de dados para extrair vestígios relacionados a um crime específico. Nesse primeiro momento, a pesquisa foi direcionada para a análise da eficácia das ferramentas forenses utilizadas na análise das evidências deixadas pelos serviços de webmail e programas de mensagens instantâneas, no qual foi montada uma linha do tempo e uma tabela com os resultados obtidos. Foram criadas três imagens que foram analisadas, procurando evidências dos serviços de webmail, para cada imagem analisada foi criada uma tabela de resultados, sendo que em cada imagem foi utilizado um navegador web diferente. Foi possível recuperar algumas informações com as ferramentas testadas neste trabalho, mas elas não se mostraram 100% eficazes, mesmo utilizando palavras chaves que foram utilizadas nos conteúdos das mensagens enviadas de um email para outro. A análise de conteúdos de webmail possui um papel importante na análise de dados, e a recuperação dessas informações é possível. No entanto, não é uma tarefa simples e requer um trabalho maior por parte dos peritos, que devem escolher as ferramentas e técnicas forenses corretas para fazê-lo.

Palavras-chave: Análise Forense. Artefatos da Web. Crimes Virtuais.