Anais do I Congresso de Ciência e Tecnologia da PUC Goiás
Disponível em: http://pucgoias.edu.br/ucg/prope/pesquisa/anais/2015/index.htm
ISSN: 2177-3327

MINERAÇÃO DE DADOS APLICADOS À ANALISE DE LINHA DE TEMPO EM SISTEMAS DE ARQUIVOS

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

Objetivo: O objetivo geral desse trabalho é utilizar técnicas de mineração de dados para análise e investigação da confiabilidade dos rótulos de tempo dos arquivos e estudar as propriedades dos sistemas de arquivos. **Método:** Foram efetuados testes em sistemas de arquivos NTFS (New Technologies File System), que é o sistema de arquivos padrão da família Windows NT, em sistemas de arquivos FAT32 (File Allocation Table), que são utilizados geralmente em flash drives e cartões de memória, para os quais utiliza-se e uma tabela representativa que possui a capacidade de indicar onde estão os dados de cada arquivo. Também foram testados os sistemas de arquivos UDF (Universal Disk Format), utilizados em DVD, CD-R e CDRW, sistemas de arquivos CDFS (Compact Disk File System), que também são utilizados em DVD, CD-R e CDRW. **Resultados:** Uma vez realizados todos os experimentos, os rótulos de tempo foram coletados e documentados em uma tabela de resultados. As tabelas 1 e 2 apresentam resultados para pastas e arquivos. Os rótulos de tempo estão presentes em dois atributos chamados $STANDARD_INFORMATION e $FILE_NAME, sendo que estes atributos por sua vez estão localizados em uma estrutura denominada entrada MFT (Master File Table). A entrada MFT consiste em uma tabela que contém informações sobre todos os arquivos e diretórios do sistema de arquivos NTFS, inclusive as informações dela mesma, porque como todas as estruturas do sistema de arquivos NTFS, a entrada MFT também é um arquivo. **Conclusão:** Este trabalho tem como objetivo analisar a utilização de técnicas de mineração de dados para análise e investigação da confiabilidade dos rótulos de tempo e estudo das propriedades dos sistemas de arquivos, onde os arquivos e pastas foram submetidos a operações por meio de testes e definição de linha do tempo, e os resultados foram condicionados em duas tabelas apresentando relações cronológicas entre os rótulos de tempo e os dois atributos estudados da entrada MFT.

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