LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

HERBERT WAGNER VIANA MORAIS

COMPUTAÇÃO FORENSE E SUAS FERRAMENTAS DE INVESTIGAÇÃO CRIMINAL

NATAL
2020

HERBERT WAGNER VIANA MORAIS

COMPUTAÇÃO FORENSE E SUAS FERRAMENTAS DE INVESTIGAÇÃO CRIMINAL

Trabalho de Conclusão de Curso apresentado ao Centro Universitário do RN, como requisito final para obtenção do título de Bacharel em Sistemas da Informação.

Orientador: Prof. Alexandre Damasceno

Natal

2020

AGRADECIMENTO

Agradeço primeiramente a deus, por essa nova fase em minha vida. A minha mãe Maria Dalva e a minha esposa Renata, por sempre me motivarem. A o Prof. Alexandre damasceno pelo seu empenho em me orientar durante a realização desse trabalho.

RESUMO

Neste artigo vamos abordar a temática sobre a computação forense, o que é, quais são as suas ferramentas e seus métodos que são usados nas pericias computacionais. Em tese a computação forense é a ciência cujo se compreende a aquisição, prevenção, recuperação e análise de evidências computacionais, dados que foram processados eletronicamente e armazenados em arquivos. Esse artigo foi baseado no estudo da computação forense. Para adquirir o conhecimento necessário para elaboração do projeto, foram estudados os assuntos sobre forense computacional, suas implicações legais, como adquirir, preservar, analisar e apresentar os dados de uma investigação. Sobre analise de evidências de um crime cibernético, seus conceitos, suas características, mecanismos, suas políticas de segurança e formas de proteção. Em Cada etapa, foi descrito detalhadamente e apresentada através de fluxogramas para melhor entendimento. No fim da abordagem desse artigo vamos poder te uma certa noção do importante papel desse assunto na sociedade tecnologicamente desenvolvida. Iremos saber o real valor do assunto, já que cada dia mais o ser humano está fortemente ligado a tecnologia, que além de trazer vários benefícios, como conexão, automação entre outros, também traz o lado ruim de se tornar alvo de crimes virtuais.

Palavras-chave: Computação forense. Evidências. Dados.

ABSTRACT

In this article we will talk about forensic computing, what it is, what are its tools and its methods that are used in computer experts. In thesis, forensic computing is the science that comprises the acquisition, prevention, recovery and analysis of computational evidence, data that have been electronically processed and stored in files. This article was based on the study of forensic computing. To acquire the necessary knowledge to elaborate the project, the subjects about forensic computation, its legal implications, how to acquire, preserve, analyze and present the data of an investigation were studied. About the analysis of evidence of a cyber-crime, its concepts, characteristics, mechanisms, security policies and forms of protection. In each step, it was described in detail and presented through flowcharts for better understanding. At the end of this article we will be able to give you a certain notion of the important role of this subject in the technologically developed society. We will know the real value of the subject, since every day the human being is strongly linked to technology, which besides bringing several benefits, such as connection, automation among others, also brings the bad side of becoming a target of virtual crimes.

Keywords: Forensic computing. Evidence. Data.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Nesses artigos vamos demonstrar como nos últimos anos, vem crescendo utilização da tecnologia na qual tem sido de uma grande valia em todas as áreas da vida do ser humano. Com a criação da internet foi associado vários benefícios para a humanidade, mas, também surgiram práticas ilícitas como malwares (tipos de softwares maliciosos) e *Phishing* (captação de dados de forma fraudulenta) que afetam computadores pessoais e corporativos. Através de ataques aos usuários e sistemas, o cyber crime (crime cibernético) está ficando cada vez mais difícil de ser investigado e chegar ao infrator, devido à condição do anonimato, tornando-se mais comum que os próprios crimes convencionais. Entre as ocorrências mais comuns dos ataques praticados estão, a perda ou alteração de dados importantes para uma organização, roubo de informações confidenciais e outros crimes como pedofilia e fraudes.

Com a necessidade maior de cada dia em se intercomunicar, trocar dados, realizar transações da forma mais rápida possível, isso vem acarretando em um grande número de pessoas utilizando a internet (no termo em inglês web) que por consequência podem-se tonar alvos fáceis para criminosos popularmente conhecido como Hacker, ou até mesmo por maquinas programadas para realizar certos tipos de ataques cibernéticos.

Segundo (QUEIROZ e VARGAS, 2010), a forense computacional é um conjunto de procedimentos e metodologias com a funcionalidade de investigar e armazenar evidências que possam provar se houve ou não um crime cibernético, levando como base de análise equipamentos de processamento de dados (computadores pessoais, laptops, servidores, estações de trabalho ou outras mídias eletrônicas).

(SILVA e OLIVEIRA, 2014) desenvolveram um estudo sobre as ferramentas computacionais baseadas em software livre e também as principais técnicas disponíveis para uma perícia forense computacional. Para isso foram utilizadas as ferramentas Forense Digital *ToolKit* (FDTK-*UbuntuBr*) e Computer *Aided Investigative Environment (CAINE)*, duas distribuições Linux que possuem um vasto conjunto de ferramentas que atendem aos diversos

processos de investigação. Dentre algumas ferramentas apresentadas, foram utilizadas ferramentas para a recuperação de dados de ambas as plataformas, realizando ao final um comparativo entre as ferramentas. Neste artigo, o objetivo é realizar a recuperação de arquivos já deletados da memória de dispositivos de armazenamento mais comuns, assim sendo possível fazer com que provas apagadas de algum dispositivo, por exemplo, sejam novamente coletadas para a montagem de um dossiê de uma investigação criminal.

2.1. COMPUTAÇÃO FORENSE

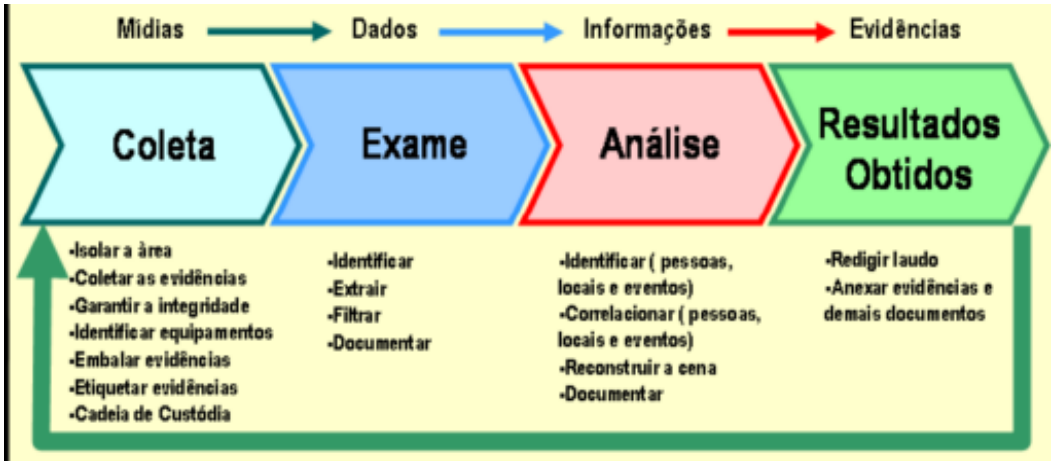
A computação forense tem como base a investigação de crimes cometidos através de quaisquer equipamentos eletrônicos, no qual é utilizado um conjunto de técnicas que coleta, recupera, analisa e preserva evidências digitais a fim de solucionar crimes. Podemos citar como exemplo Computadores, notebooks, tablets, celulares e GPS. Primeiramente vamos entender em que tipificações de crimes é necessário o trabalho de um perito em computação. Notoriamente é necessário a perícia computacional em crimes que envolvam diretamente ou indiretamente, qualquer tipo de aparelho eletro/eletrônico que tenham a capacidade de armazenar dados.

Temos como exemplo os Crimes cibernéticos mais praticado na atualidade, como fraudes bancárias e roubo de identidade , mas a computação forense não é só utilizada para investigar crimes cometidos no mundo virtual, assim como também no mundo físico , fazendo a análise de informações digitais também envolvidas no ato criminoso, que podemos ter como exemplo, de uma organização criminosa que venha a desviar verbas públicas, recuperando dados ou outras informações já apagadas de um computador e que podem ser vitais para a resolução do caso.

2.2. ETAPAS DA COMPUTAÇÃO FORENSE

A perícia computacional é uma área da computação forense, sendo um processo investigativo. Ao início de uma investigação um perito especialista é acionado e o mesmo precisa ter várias precauções e também necessita ser disciplinado para que todas as evidências permaneçam totalmente íntegras para assim não comprometer o andamento da investigação e o laudo ao final do processo. Esse processo todo é dividido em quatro etapas: Coleta de dados, exame dos dados, análise das informações e interpretação dos resultados (PEREIRA, 2010), como pode ser observado na Figura abaixo.

Figura 1 – Etapas da computação forense



Fonte: https://periciacomputacional.com/wp-content/uploads/2016/06/ciclo-2.png

• **Coleta de Dados:** a etapa de coleta é considerada a primordial durante o processo de investigação, pois é nessa fase que é adquirido uma grande quantidade de dados da investigação, desta forma é preciso ter muita cautela para manter a integridade dos dados e não afetar o resultado final. Além disso, outras atividades como coleta de equipamento, e identificação são realizadas nesta etapa.

• **Exame dos Dados:** Nessa etapa pode-se dizer que é separado os principais dados do demais, pois o objetivo é de filtrar as informações mais importantes para o caso, e deixar os irrelevantes de lado, como por exemplo, arquivos do sistema. Ao início do processo é definida as ferramentas utilizadas, e essa escolha é relativa ao tipo de investigação e informações que estão sendo buscadas.

• **Análise das Informações:** Nessa terceira etapa, todas as informações já obtidas anteriormente são analisadas com a finalidade de encontrar informações significativas para a investigação do caso. Todos os dados importantes são relacionados com informações que são referentes à investigação, para que dessa forma seja possível realizar a conclusão.

• **Interpretação dos Resultados:** Na última etapa, é apresentado pelo perito um relatório técnico que tem a finalidade de repassar com toda a precisão e embasamento possível do que foi descoberto durante a investigação nos dados analisados. Todo o processo pericial deve estar presente nesse relatório, informações contidas no laudo.

3. Ferramentas e Equipamentos da Computação Forense

Para comentar algumas dentre as várias ferramentas utilizadas por peritos e investigadores em informática, vamos usar uma cena de crime hipoteticamente envolvendo pornografia infantil armazenada em um disco rígido pessoal. Na maioria dos casos, os investigadores primeiro removeriam o disco rígido do PC e o conectariam em um dispositivo que bloqueia a gravação de dados no hardware. Esse dispositivo torna completamente impossível alterar os dados do disco rígido de qualquer maneira, permitindo que os pesquisadores capturem e visualizem o conteúdo do disco.

Uma cópia muito precisa do disco pode ser feita com uma variedade de ferramentas especializadas. Existem excelentes e enormes *Frameworks* e softwares para computação forense, além de inúmeros aplicativos menores. O primero grupo inclui o *Digital Forensics Framework, o Open Computer Forensics Architecture, o CAINE (Computer Aided Investigative Environment), o X-Ways Forensics, o SANS Investigative Forensics Toolkit (SIFT), EnCase, The Sleuth Kit, Llibforensics, Volatility, The Coroner's Toolkit, Oxygen Forensic Suite, o Computer Online Forensic Evidence Extractor (COFEE), HELIX3 ou Cellebrite UFED.*

Essas soluções de software e suítes forenses incluem uma ampla gama de serviços de dados forenses em um único pacote. No entanto, muitos especialistas forenses preferem criar as suas próprias caixas de ferramentas personalizadas a partir de ferramentas e utilitários individuais que atendem

exatamente às suas necessidades e preferências. As opções são abundantes para cada etapa do processo de recuperação de dados forenses, incluindo análise forense de disco rígido e análise forense de sistemas de arquivos.

A captura de dados pode ser feita com a ajuda do *EnCase Forensic Imager, FTK Imager, Live RAM Capturer* ou *Disk2vhd* da Microsoft. Os e-mails são analisados com ferramentas como EDB Viewer, Mail Viewer ou MBOX *Viewer*. Algumas ferramentas são feitas especificamente para certos sistemas operacionais, enquanto outras suportam múltiplas plataformas. Ferramentas populares para Mac OS X incluem Disk Arbitrator, Volafox e ChainBreaker, que analisa a estrutura keychain e extrai informações do usuário. Não há necessidade em dizer que nenhuma analista forense pode ocorrer sem uma grande variedade de ferramentas de análise de internet, como o Dumpzilla do Businidre, o Chrome Session Parser, o IEPassView, o OperaPassView e o Web Page Saver da Magnet Forensics.

3.1 Características das Ferramentas Forenses Profissionais

Podemos dizer que as características mais requisitadas dos programas forenses profissionais podem ter variações de acordo com os principais pontos da análise forense e da forma que elas são destinadas e ao seu mercado alvo. Comumente, os grandes suítes de softwares forenses necessitam ter a capacidade de realizar os seguintes pontos:

•Oferecer suporte hash de todos os arquivos, o que permite a filtragem comparativa.

•Hash completo do disco para poder confirmar que os dados não foram alterados (normalmente uma ferramenta é usada para adquirir e outra é usada para confirmar o hash do disco).

•Localizadores de caminho exatos.

•Registro de hora /datas.

•Incluir um recurso de aquisição.

•Pesquisa e filtragem de itens.

•A capacidade de carregar backups do iOS e analisar seus dados.

Em comparação com as agências de aplicação da lei, as empresas geralmente não estão preocupadas com a captura da memória volátil RAM. Eles pretendem sempre adquirir as provas para investigação privada e/ou para entregar a justiça. Eles geralmente também não estão interessados na capacidade de visualização.

3.2 PRICIPAIS FORNOCEDORES DE SOFTWARE

A área de software de analise forense é onusto de empresas inovadoras e prolificas, que estão prontas para ampliar a sua operação. Os grandes fornecedores de sotware forense tendem a aparecer em grandes encontros industriais, como a High tech Crime Investigation Association Conference. Existem muitas dessas conferencias em toda a América do Norte.

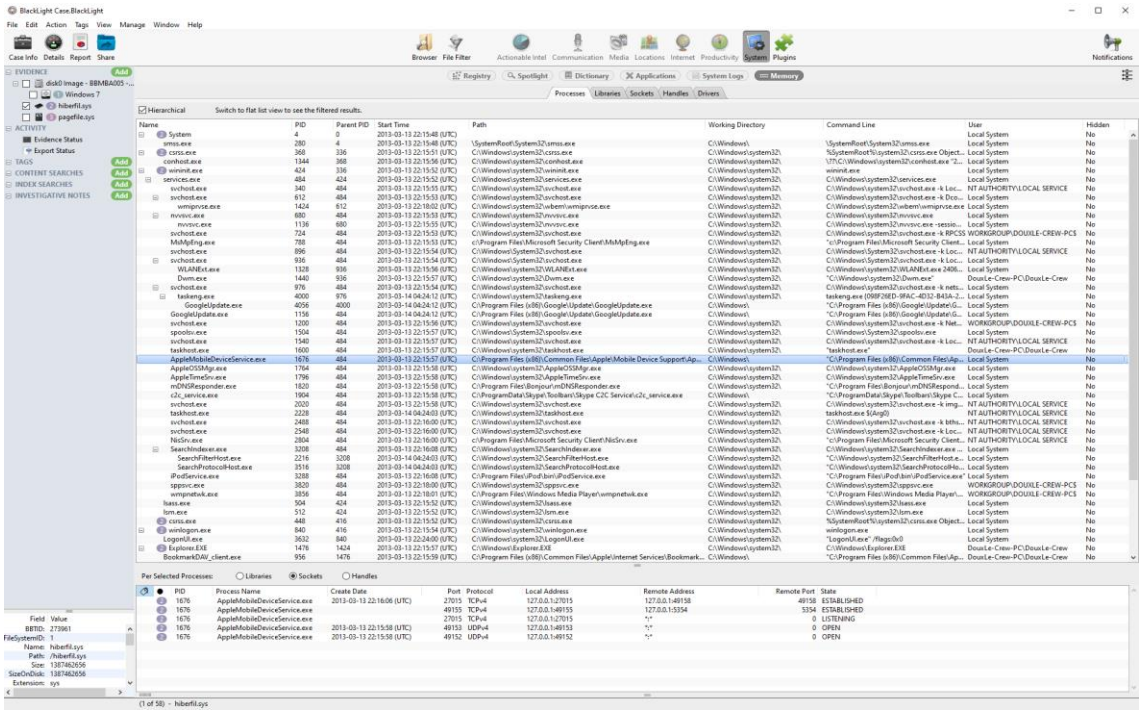
Agora iremos ver alguns dos fornecedores de software forense mais conhecidos e os seus respectivos produtos.

3.3 BlackBag- Blacklight

O Black Light da BlackBag é a principal ferramenta forense para Mac no mercado atualmente e custa aproximadamente U$2600. O Black Light foi lançado há 5 anos como ferramenta forense para Mac. Porém, se tornou também uma boa ferramenta de análise e exame para Windows. Ele também é capaz de analisar todos os dispositivos iOS, bem como, dispositivos Android. No entanto, não é capaz de analisar dispositivos BlackBerry. Uma coisa que o Black light não faz por conta própria é a aquisição forense de bits para clones de bits. Eles têm uma ferramenta adicional para isso chamada MacQuisition.

O MacQuisition executa uma versão simplificada do iOS 10 e custa mais ou menos U$1000 por causa do licenciamento da Apple. Ele faz um bom trabalho em descobrir criptografia e juntar unidades de fusão em um único volume.

Figura 2: Dashboard Blacklight.



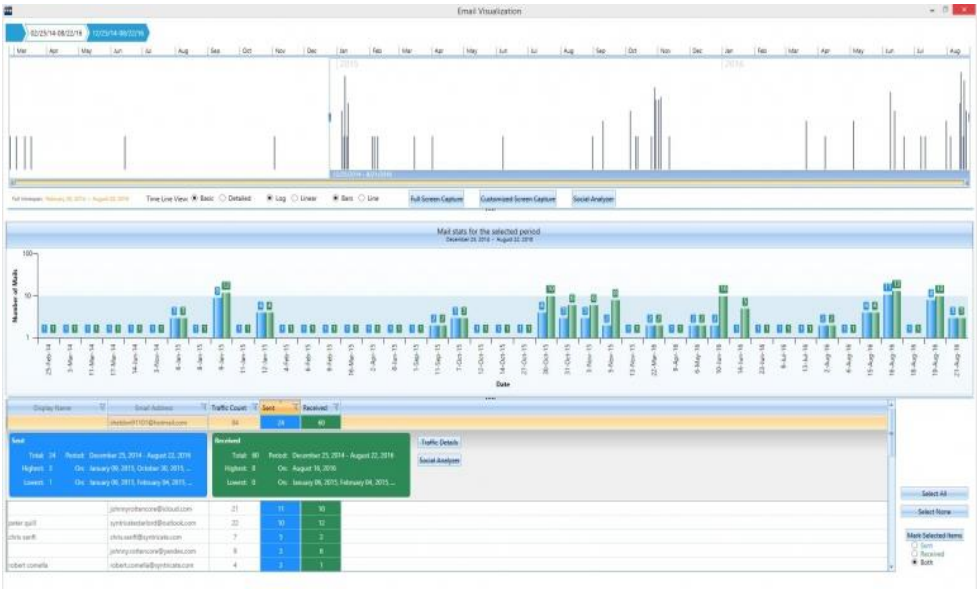
Fonte: Blacklight.

3.4 AccessData

O AccessData é o fornecedor líder de E-Discovery e Computação Forense para Desktops e Dispositivos Móveis para empresas, escritórios de advocacia e agências governamentais. Suas soluções de computação forense incluem o Forensic ToolKit (FTK), que fornece processamento abrangente e indexação adiantada, de modo que a filtragem e a busca sejam realizadas de forma mais rápida do que qualquer outra solução no mercado.

A empresa é conhecida por suas ferramentas forenses para dispositivos móveis, incluindo o Mobile Phone Examiner Plus (MPE+) e nFIELD. O primeiro permite que os examinadores forenses de dispositivos móveis coletem rapidamente, identifiquem facilmente e obtenham os principais dados que outras soluções não conseguem. O último é uma solução ágil que permite aos usuários realizar aquisições lógicas e físicas de todos os dispositivos móveis compatíveis com MPE+ em apenas 5 etapas.

Figura 3- Dasboard Forensic ToolKit



Fonte: Acessdata

4 CONSIDERAÇÕES FINAIS

O objetivo desse TCC foi demonstrar que a computação forense vem desempenhando um papel importante nos tempos atuais, já que o aumento número de crimes virtuais, vem obrigando as forças de investigação que atuam na área cibernética, a aprimorar as ferramentas utilizadas para combater tais crimes, segundo pesquisas, a grande parte dos crimes como, estelionato, ataques cibernéticos, invasão que são cometidos através de dispositivos eletrônicos, ficam sem resolução. O que aumenta a sensação de impunidade.

Não basta apenas cuidados extras dos usuários dessas tecnologias, também é preciso ter uma busca de aperfeiçoamento dos meios utilizados para as pericias em dispositivos, e assim tornar cada vez mais seguro a utilização da internet, computadores, smartfones. Não só forças policiais como Policia Federal, Agência Brasileira de Inteligência (ABIN), Policia Civil, estão se capacitando mas a cada dia, mas também as empresas como instituições financeiras, grandes multinacionais estão cada vez mais investindo nessa área da T.I , para evitar fraudes, entre outros problemas que venham a afetar a sua estrutura empresarial.

Nesse trabalho estudamos o que é a computação forense, a sua importância, suas etapas e ferramentas para uma análise profunda de objetos relacionados a um crime virtual, com a finalidade de obter provas que possam levar a autoria e responsabilização do crime cometido. Com o assunto visto pode-se ter uma ideia do tamanho do papel de tal área sobre a sociedade na que vivemos em tempos atuais, onde maior parte dos crimes acontecem no ambiente virtual, sendo assim necessário sempre buscar a evolução nesse quesito que se trata de combate aos crimes cibernéticos.

REFERÊNCIAS

QUEIROZ, C.; VARGAS, R. **Investigação e perícia forense computacional: certificações, leis processuais e estudos de caso**. Rio de Janeiro: Brasport, 2010.

SILVA, V. A.; OLIVEIRA, C. H. D. **Análise De Ferramentas Livres Para Perícia Forense Computacional. Caderno de Estudos Tecnológicos** - Faculdade de Tecnologia de Ourinhos, São Paulo, 2014.

ELEUTÉRIO, P. M. D. S.; MACHADO, M. P. **Desvendando a Computação Forense.** São Paulo: Novatec , 2011.