doi.org/ 10.51891/rease.v7i12.3503

A IMPORTÂNCIA DA COMPUTAÇÃO FORENSE NO COMBATE ACRIMES CIBERNÉTICOS

Amanda Barbosa Costa[1]
Fernando Bezerra da Silva[2]
Helton Girio Matos[3]
Italo Luan Cavalcante Freire[4]

RESUMO: Com a tecnologia em ascensão e o aumento de usuários, a internet e os dispositivos eletrônicos têm se tornado uma arma poderosa na atualidade. Conectando cada vez mais as pessoas umas às outras e disponibilizando informações sobre elas sem burocracia. O que resulta em algo mais grave, partindo de aproveitadores criminosos no mundo da internet, que cometem os crimes fazendo uso dessas informações. Este trabalho tem como objetivo realizar o estudo das ferramentas utilizadas na computação forense. Foi realizada uma pesquisa bibliográfica sobre o tema abordado e foram testadas algumas das principais ferramentas e concluiu-se que juntas atendem às etapas do processo de análise forense para o resultado final.

Palavras-Chave: Crime Cibernético. Evidência Digital. Computação Forense.

ABSTRACT: With technology on the rise and the increase of users, the internet and electronic devices have become a powerful weapon nowadays. Increasingly connecting people to each other and making information about them available without bureaucracy. What results in something more serious, from criminal profiteers in the internet world, who commit crimes using this information. This work aims to study the tools used in computer forensics. Bibliographical research on the approached theme was carried out and some of the main tools were tested in which, it was concluded that together they meet the stages of the forensic analysis process for the final result.

Keywords: Cyber Crime. Digital Evidence. Computer Forensics.

[1] Bacharel em Sistemas de Informação – Centro de Ensino Unificado do Piauí (CEUPI). E-mail: amanda119155@ceupi.com.br
[2] Bacharel em Sistemas de Informação – Centro de Ensino Unificado do Piauí (CEUPI). E-mail: Fernando120730@ceupi.com.br
[3] Sistemas de Informação – Centro de Ensino Unificado do Piauí (CEUPI). E-mail: helton.matos@ceupi.com.br
[4] Bacharel em Sistemas de Informação – Centro de Ensino Unificado do Piauí (CEUPI). Digital Solutions Analyst at capgemini. E-mail: italo120224@ceupi.com.br.

INTRODUÇÃO

Atualmente, percebe-se uma maior interação entre o homem e a tecnologia. O que antes era mero acessório, passa a ser fundamental no cotidiano das pessoas (GOMES, 2017). Torna-se cada vez mais comum o uso de dispositivos tecnológicos com capacidade para armazenar dados e informações que estejam conectados através da internet.

Na medida em que os seres humanos alimentam esse universo de dados e informações, a tecnologia modificou a natureza do diálogo humano (COLOMBO; NETO, 2017). Crime cibernético é uma atividade criminosa que o alvo usa ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado à rede. Na maioria desses crimes cibernéticos são cibercriminosos ou hackers que buscam adquirir dinheiro. O crime cibernético é realizado por pessoas ou organizações (MELO, 2020).

Os criminosos que praticam insultos e ataques dessa natureza, se aproveitam do "ocultismo" das telas para cometer tais delitos e levarem vantagem sobre a situação. Para combater esses atos e "desmascarar" os criminosos, a computação forense tem avançado cada vez mais, utilizando de tecnologias inteligentes para chegar a evidências dessas práticas ilícitas.

É papel da Forense Computacional investigar, identificar, coletar, analisar, interpretar, preservar, periciar, documentar e apresentar os fatos que ocorreram mediante a utilização de evidências digitais (SILVA, 2017). Quando um crime é cometido no mundo físico, várias vezes a evidência pode ser encontrada em dispositivos digitais de um suspeito ou na internet (UBALDO, 2017). Busca-se, como objetivo, mostrar a importância da computação forense através dessas evidências encontradas em dispositivos eletrônicos.

Busca-se no objetivo geral, realizar o estudo das ferramentas utilizadas na forense computacional, para em seguida aplicá-las seguindo as etapas do processo de análise forense em um laboratório de um caso hipotético de um crime. O objetivo específico tem como finalidade colocar em uso as ferramentas FTK Imager, Autopsy,

ImageJ e FotoForensics. Usando-as em conjunto é esperado conseguir aspectos técnicos do processo de análise e mostrar que juntas, geram informações de forma clara para a conclusão do caso.

1. REFERENCIAL TEÓRICO

Os tópicos a seguir, conceituam crime cibernético, computação forense e mostram detalhes das etapas de investigação e algumas das principais ferramentas usadas.

1.1 Crimes cibernéticos

Os crimes virtuais são, assim como os crimes comuns, condutas típicas, antijurídicas e culpáveis, contudo todos são praticados contra ou com a utilização dos sistemas da informática (MENESES, 2019). Em suma, qualquer ação ilegal, que utiliza-se de recursos tecnológicos como meio para a prática delituosa ou voltada contra computadores, sistemas e dados não autorizados, pode ser caracterizado como crime cibernético (MATSUYAMA; LIMA, 2017).

Segundo Régis (2018), os crimes virtuais no Brasil têm crescido gradativamente, á medida que os meios tecnológicos se tornam cada vez mais acessíveis, caindo, por vezes, em mãos erradas. No ano de 2020, a Polícia Federal intensificou operações ao combate ao crime virtual, especialmente os crimes relacionados a pornografia infantil (CHAVES, 2020). De acordo com Moraes (2019) Dentre os crimes mais comuns, destacam-se: Fraudes eletrônicas em sistema bancário; Mídias e ou redes sociais; Vídeos e fotos na internet (impróprios ou sem o consentimento da vítima); Atuação de grupos racistas ou organizações criminosas; Cyberbullying.

Crimes virtuais ou cibernéticos são atos praticados ilicitamente com o intuito de furtar, ofender, denegrir, prejudicar, abusar psicológica ou fisicamente de outro indivíduo. Por meio da rede Mundial estes atos podem ser realizados contra uma pessoa ou contra bens materiais e imateriais (LEMOS; COSTA; PINTO; NUNES, 2017).

1.1.1. Computação forense

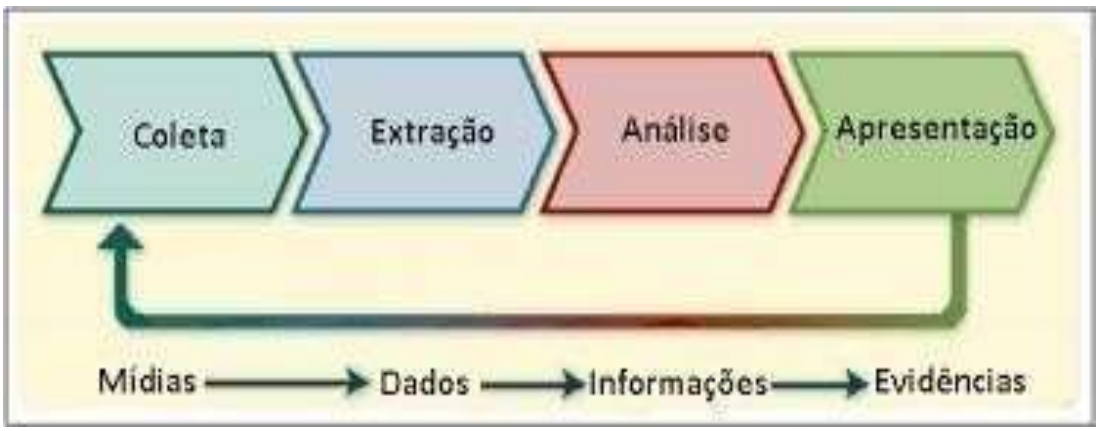
A computação forense examina toda forma de dispositivo computacional, identificando, preservando, recuperando e apresentando evidências digitais para classificação de crimes (BORGES; PRADO, 2017). De acordo com Silva Filho (2016) os cuidados devem ser tomados para garantir a preservação e coleta dos dados digitais: isolar olocal; evitar acessos remotos; utilizar funções de hash para garantir a integridade dos dados e a cadeia de custódia.

Através desses conceitos, é possível verificar a importância que a computação forense tem na busca da verdade dos fatos, sendo esse um motivo relevante para revisar suas etapas, seus aspectos, e aplicações (SOUSA, 2016).

1.1.2 Etapas do processo de Análise Forense

A computação forense é balizada por métodos e procedimentos específicos que permitem que o perito chegue a um resultado esperado, seguindo as etapas de coleta, extração, análise e apresentação conforme a representado na Figura 1.

Figura 1. Etapas do processo da Análise Forense



Fonte: Souza, 2015

Coleta: é o processo de isolamento da área que deve ser analisada posteriormente para que mantenha seu estado original sem interferências ou modificações depois que o processo de investigação iniciar. Quando a área tiver sido isolada, as evidências deverão ser coletadas nas mídias apontadas como parte do

cenário, sempre visando garantir sua integridade;

Extração: na etapa de extração serão identificados, extraídos, filtrados os dados que foram coletados na primeira etapa. Sendo extraídos e filtrados somente os dados que serão relevantes no processo de resolução do crime;

Análise: no processo de análise em si, que é a mais primordial de todas as etapas, os dados examinados na fase anterior deverão formar informações que promovam a identificação dos possíveis envolvidos, permitindo que seja feita a reconstituição do cenário;

Apresentação: também conhecida como a etapa de relatório, essa é a última fase desse processo, e consiste na demonstração das evidências obtidas, através da redação de um laudo que deve ter como anexo todas as evidências encontradas nas mídias examinadas e os demais documentos que foram produzidos durante o processode Análise Forense.

1.1.1 Principais ferramentas usadas

Após as pesquisas, foi citada algumas das ferramentas usadas nesse processo de análise forense. Por se tratar de ferramentas gratuitas, acabam sendo uma das mais usadas tanto por peritos iniciantes quanto pelos mais experientes.

FTK Imager:

O ForensicToolKit Imager, ou FTK Imager , foi desenvolvido pela AccessData,e neste software podemos encontrar as principais funcionalidades para a realização de exames forenses em dispositivos de armazenamento de dados. Este aplicativo possui uma switch com vários recursos que podem ser utilizados em todas as fases de um exame computacional forense (AccessData, 2021).

Autopsy:

Autopsy é um software de computador que simplifica a implantação de muitos dos programas e plugins de código aberto usados no The Sleuth Kit. A interface gráfica do usuário exibe os resultados da pesquisa forense do volume subjacente, tornando mais fácil para os pesquisadores sinalizar seções pertinentes de dados (*Copyright 2012-2021 Basis Technology*).

ImageJ:

ImageJ é um programa de processamento de imagem Java de domínio público inspirado no NIH Image para Macintosh. Ele é executado, seja como um mini aplicativoonline ou como um aplicativo para download, em qualquer computador com uma máquina virtual Java 1.4 ou posterior. Distribuições para download estão disponíveis para Windows, Mac OS, Mac OS X e Linux.

Ele pode exibir, editar, analisar, processar, salvar e imprimir imagens de 8, 16 e 32 bits, calcular estatísticas de área e valor de pixel de seleções definidas pelo usuário, medir distâncias e ângulos, criar histogramas de densidade e gráficos de perfil de linha, faz transformações geométricas, como escala, rotação e inversões. A imagem pode ser ampliada até 32: 1 e até 1:32. Todas as funções de análise e processamento estão disponíveis em qualquer fator de ampliação.

FotoForensics:

FotoForensics fornece aos pesquisadores iniciantes e investigadores profissionais acesso a ferramentas de ponta para análise forense de fotos digitais. A hospedagem, administração e desenvolvimento de sites não são gratuitos, o site é patrocinado pela Hacker Factor,

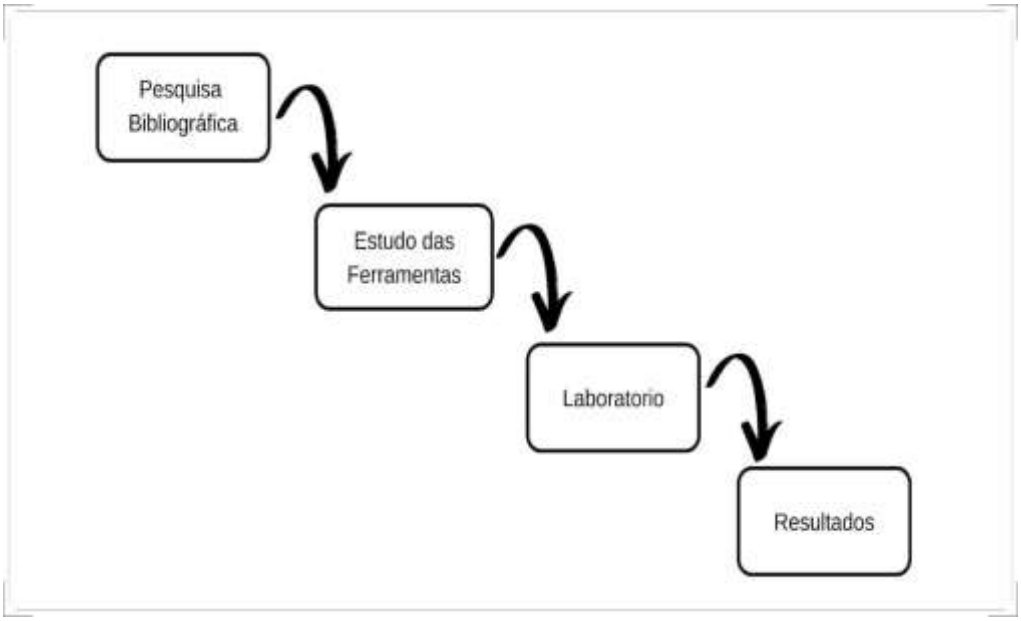
possuindo diversas funcionalidades como ajuste de cor, digerir, ELA, pixels ocultos, JPEG%, efeitos de lente, metadados e strings (Copyright 2012-2021 Hacker Factor).

METODOLOGIA

A evolução desta pesquisa se deu em 4 fases conforme citado. Inicialmente foi realizadauma revisão bibliográfica de artigos científicos sobre o tema na Internet e, em seguida, um estudo das ferramentas supracitadas foi realizado com a finalidade de aplicá-las em laboratório. Todo este estudo fundamentou-se nas etapas do processo de análise forense.

Seguindo o esquema exemplificado no diagrama da Figura 2 a seguir, foi trabalhado na elaboração de um laboratório com o intuito de demonstrar uma situação hipotética.

Figura 2. Fluxo da metodologia



Fonte: Próprio autor.

Em seguida, a fase de estudos das ferramentas se deu a partir da leitura da documentação de cada ferramenta encontrada nos seus respectivos sites, podendo assim aprofundar no conhecimento teórico essencial para o desenvolvimento da etapa seguinte.

Na etapa de laboratório, que corresponde aos testes, foi criado um cenário hipotético onde a polícia vai realizar uma coleta na casa do principal suspeito de cometer um crime. Baseado nisso, executado em laboratório os procedimentos de análise forense usando as ferramentas supracitadas no tópico 2.1.3

O laboratório inicia após o perito in-loco concluir a fase de coleta e iniciou a partir da segunda etapa, em que foi realizada o Dump (extração lógica) da unidade de armazenamento, procedimento de cópia bit a bit do disco rígido com o intuito de preservar a integridade das evidências contidas na unidade original. Para esse procedimento foi utilizado o FTK Imager. Após a conclusão foi gerado um arquivo contendo o hash e outras informações a fim de garantir a confiabilidade dos dados. Esta ferramenta é extremamente versátil e pode ser usada em diversas fases da

análise.

A realização da análise das evidências ocorreu a partir da cópia lógica obtida na etapa anterior. A princípio, usamos o Autopsy para checar a existência de arquivos excluídos, sejam eles fotos, vídeos, documentos ou até mesmo mensagens de texto.

Dando continuidade à análise, foi encontrada uma imagem jpg, tal arquivo correspondia a expectativa da análise e prosseguiu-se com a recuperação dela, usando e analisando de forma minuciosa como uso do ImageJ uma ferramenta de código aberto para análise de vetores.

Feita a análise e vetorização com ImageJ, foi preciso passar a imagem por uma segunda análise diferente para que fosse consolidada as informações obtidas. Dessa forma, afastando qualquer dúvida que pudesse ofuscar o caso e, para isso, foi usado o FotoForensics.

Terminada a etapa de análise fazendo uso dessas ferramentas, foi possível gerar um laudo preliminar para ser usado na etapa seguinte de apresentação que será discutidano tópico 4.

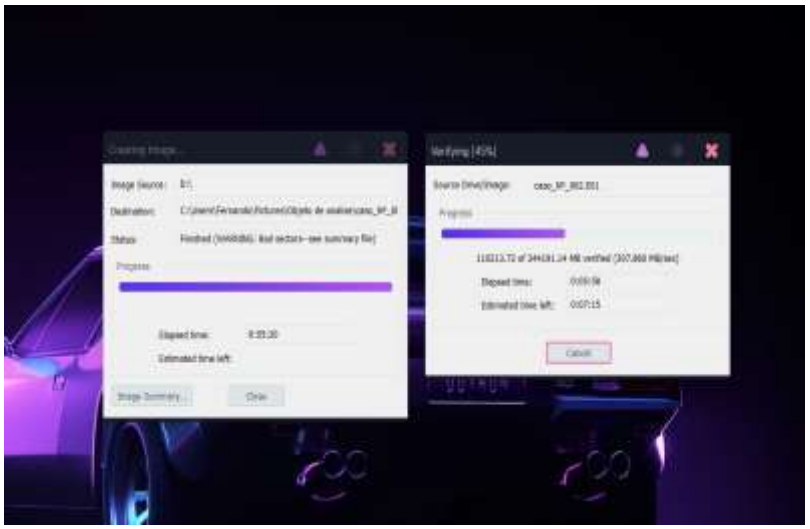
RESULTADOS E DISCUSSÕES

Neste tópico, usou-se um caso hipotético de um crime em que as evidências encontradas são digitais. Foi demonstrado o passo a passo da realização dos testes das ferramentas mencionadas e o resultado final.

1.1 FTK Imager

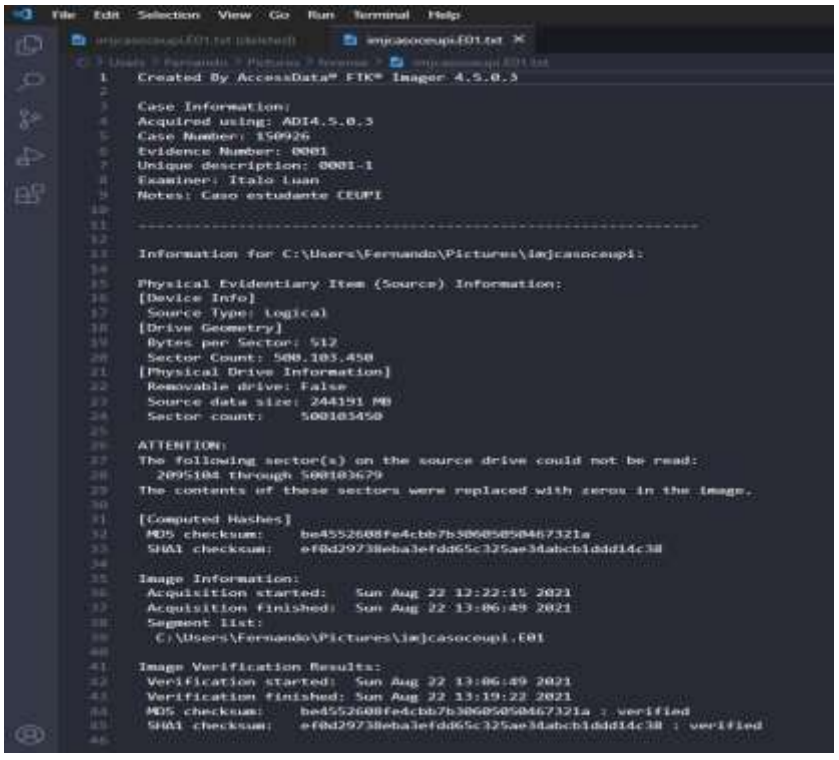
Foi feito o dump (extração lógica) do disco rígido usando o FTK Imager, conforme a Figura 3 em que, por meio dele, pôde-se perceber que o processo é extremamente facilitado, pois a ferramenta entrega funcionalidades como: Amostragem de performance e detalhamento de dados. Mas, o FTK Imager se destaca principalmente por fazer o dump com uma confiabilidade maior pois ao fim da extração é gerado documento que garante a integridade por meio de 2 tipos de hash conforme mostra a figura 4

. **Figura 3.** FTK Imager



Fonte: Próprio autor, 2021

Figura 4. Documento que garante a integridade.



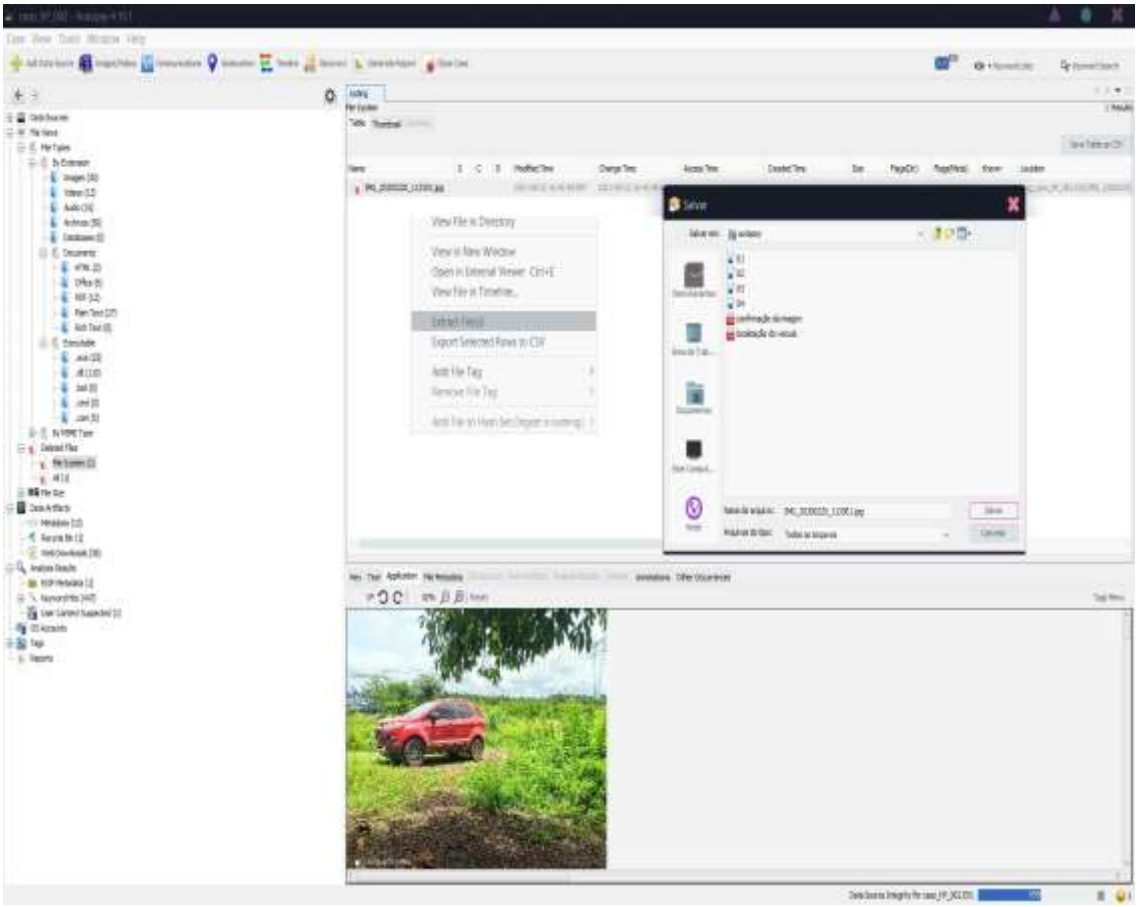
```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 150926
Evidence Number: 0001
Unique description: 0001-1
Examiner: Italo Luan
Notes: Caso estudante CEUPI

--------------------------------------------------------------

Information for C:\Users\Fernando\Pictures\im]casoceupi:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 500.103.450
[Physical Drive Information]
 Removable drive: False
 Source data size: 244191 MB
 Sector count:     500103450

ATTENTION:
The following sector(s) on the source drive could not be read:
  2095104 through 500103679
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
 MD5 checksum:    be4552608fe4cbb7b3060505067321a
 SHA1 checksum:   ef0d2973beba1efdd65c325ae3dabcb1ddd14c38

Image Information:
 Acquisition started:   Sun Aug 22 12:22:15 2021
 Acquisition finished:  Sun Aug 22 13:06:49 2021
 Segment list:
  C:\Users\Fernando\Pictures\im]casoceupi.E01

Image Verification Results:
 Verification started:  Sun Aug 22 13:06:49 2021
 Verification finished: Sun Aug 22 13:19:22 2021
 MD5 checksum:    be4552608fe4cbb7b3060505067321a : verified
 SHA1 checksum:   ef0d2973beba1efdd65c325ae3dabcb1ddd14c38 : verified
```

Fonte: Próprio Autor, 2021.

1.1.1 Autopsy

Ao fazer a extração lógica e submeter o dump ao Autopsy, nota-se uma visão ampla doselementos que compõem a massa de dados extraída. Observou-se aspectos técnicos como hash e metadados, inclusive de arquivos deletados. Conforme Figura.5

Figura 5. Autopsy



Fonte: Autor, 2021.Próprio

1.1.2 ImageJ

Com o uso do ImageJ, é possível ampliar a imagem e colocar o frame da placa do carro em uma perspectiva diferente, em que fica claro a numeração da placa, evitando assim, qualquer dúvida ou questionamento. Conforme a Figura 6.

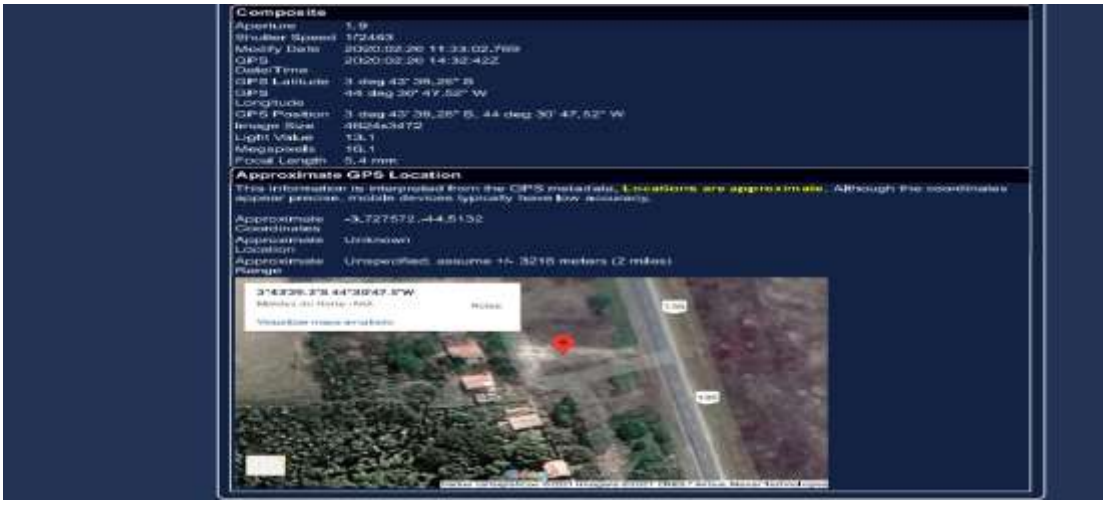
Figura 6. ImageJ

Fonte: Autor, 2021.Próprio

4.1. 3 FotoForensics

Agora, tendo certeza que o modelo do carro e placa conferem com o esperado, usamos oFatoForensics em busca de metadados e conseguimos saber informações do dispositivo que tirou a foto, além da geolocalização que comprovou a presença do suspeito no local do crime. Vê-se exemplificado na Figura 7.

Figura 7. FotoForensics



Fonte: Autor, 2021.Próprio

Por meio do laboratório, nota-se diferenças entre as ferramentas usadas. O FTK Imager, por exemplo, guarda características e funcionalidades parecidas com a doAutopsy, porém, o FTK se destaca em performance e a extração das evidências é feita com mais rapidez. Em contrapartida, o Autopsy gera um caso completo com mais detalhamentos das evidências.

Foram colocadas em prática ferramentas voltadas para forense em imagens como o ImageJ e FotoForensics. Embora, usadas para perícia em imagens, cada uma possui funções que as destacam em determinados empregos. Por exemplo, o ImageJ consegue fazer manipulação da imagem mudando-a de perspectiva, aplicando filtro e pode ser usado inúmeros plugins que aumentam ainda mais suas funcionalidades. Já o FotoForensics, consegue ter acesso a informações das imagens como os metadados e pixels mortos, dessa forma, o perito consegue saber a origem de uma imagem e se ela é ou não é uma montagem.

O conjunto de informações que conseguiu-se obter fazendo uso das ferramentas supracitadas de forma complementar, permitindo uma grande assertividade e um baixo erro de rejeição quando as provas forem expostas a um juiz. O que é de suma importância.

CONCLUSÃO

Este trabalho possibilitou entender como funciona o processo de investigação da perícia computacional forense e sua importância no combate aos crimes cibernéticos. Com isso, pôde-se perceber a necessidade da computação forense que considera as evidências digitais e dispositivos eletrônicos as principais ferramentas para alcançar os criminosos.

O teste começou com o uso do FTK Imager para realizar um Dump (Extração Lógica). Depois, executou-se o Autopsy para a recuperação de um arquivo. Fez-se uso do ImageJ para atingir uma visualização nítida da placa do carro, onde conseguiu chegar ao resultado esperado: que foi ver que o modelo do carro coincidia com o suspeito. Paraalcançar os metadados, incluindo a localização, foi colocada a imagem

no Fotoforensecs. Com essas informações obtidas, foi possível reunir provas de que a pessoa suspeita estava no local do crime.

Observou-se que essas ferramentas são importantes e que, trabalhadas em conjunto, apresentam eficácia nos resultados. Em pesquisas futuras, pretendemos propor esse e outros testes seguindo cada etapa do processo de investigação. O exercício demonstraria a real eficácia da incorporação da computação forense e a importância da utilização da tecnologia na investigação de crimes, sejam eles por meio da internet e/ou redes sociais, ou até mesmo de natureza contrária, mas com evidências em dispositivos, como celular ou computador.

REFERÊNCIAS

Autopsy Developer Documentation: Autopsy Developer's Guide https://www.sleuthkit.org/autopsy/docs/build-docs/4.12.0/index.html 2021 https://ad-pdf.s3.amazonaws.com/Imager/4_3_0/FTKImager_UG.pdf

Chaquian Filho, E., Duarte, S., S. L. O. e Lacerda, L. C. (2018). "A importância da preservação da evidência digital nos crimes cibernéticos", Revista Diálogos: Economia e Sociedade, p. 89-109.

Chaves, S. R. (2020). "Crimes cibernéticos - questionamentos acerca da vulnerabilidade nos crimes virtuais sexuais", https://repositorio.pucgoias.edu.br/jspui/handle/123456789/950, Novembro.

Da Silva Filho, W. L. "Crimes cibernéticos e computação forense", http://sbseg2016.ic.uff.br/pt/files/MC2-SBSeg16.pdf.

Ferreira, J. S. (2021). "Computação forense e a técnica de esteganografia aplicada em imagens digitais: um mapeamento sistemático", http://rdu.unicesumar.edu.br/handle/123456789/7503, Fevereiro.

FotoForensics Tutorials http://ipv4.fotoforensics.com/tutorial.php

Freitas, J. J. D. (2019). "Crimes cibernéticos: uma abordagem sobre a fragilidade penal

brasileira contra os crimes ocorridos nas redessociais e plataformas de compartilhamentos de vídeos", http://repositorio.unifametro.edu.br/jspui/handle/123456789/90, Junho.

ImageJ Documentation https://imagej.nih.gov/ij/docs/index.html

Mesquita, P. (2018). "Desafios da forense em dispositivos móveis", Gestão da Segurança da Informação - Unisul Virtual, https://repositorio.animaeducacao.com.br/handle/ANIMA/3685.

Rodrigues, A. P. S., Costa, E. R., de Sousa, J. F., e Turibus, S. N. (2019). "Análise forense: técnicas e ferramentas aplicadas em reconstituições de ataques cibernéticos em ambientes corporativos", Revista Científica da Faculdade de Balsas, p. 46-58, https://www.unibalsas.edu.br/revista/index.php/unibalsas/article/view/115/95, Maio.

Silva, R. e Marques, D. (2019). "Crimes cibernéticos e sua competência", Encontro deIniciação Científica, http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7911/67648665.

Soares, S. S. B. (2016). "Os crimes contra honra nas perpectiva do ambiente virtual", https://ambitojuridico.com.br/cadernos/direito-penal/os-crimes-contra-honra-na-perspectiva-do-ambiente-virtual/, Janeiro.