

UNIVERSIDADE DO SAGRADO CORAÇÃO

RAFAELA TEREZA VENERANDO

**COMPARAÇÃO DE FERRAMENTAS POR MEIO DA
ANÁLISE DAS FASES DE UMA PERÍCIA FORENSE
COMPUTACIONAL PARA OBTENÇÃO DE
EVIDÊNCIAS**

BAURU
2014

RAFAELA TEREZA VENERANDO

**COMPARAÇÃO DE FERRAMENTAS POR MEIO DA
ANÁLISE DAS FASES DE UMA PERÍCIA FORENSE
COMPUTACIONAL PARA OBTENÇÃO DE
EVIDÊNCIAS**

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2014

V456a Venerando, Rafaela Tereza.

Comparação de ferramentas por meio da análise das fases de uma perícia forense computacional para obtenção de evidências / Rafaela Tereza Venerando. -- 2014.

83f. : il.

Orientador: Prof. Esp. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Perícia Forense. 2. Tecnologia. 3. Evidências. 4. Investigação. 5. Dispositivos de Armazenamento. I. Martins, Henrique Pachioni. II. Título.

RAFAELA TEREZA VENERANDO

**COMPARAÇÃO DE FERRAMENTAS POR MEIO DA ANÁLISE DAS
FASES DE UMA PERÍCIA FORENSE COMPUTACIONAL PARA
OBTENÇÃO DE EVIDÊNCIAS**

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Martins.

Banca examinadora:

Prof. Me. Henrique Pachioni Martins
Universidade do Sagrado Coração

Prof. Me. Patrick Pedreira Silva
Universidade do Sagrado Coração

Prof. Esp. André Luiz Ferraz Castro
Universidade do Sagrado Coração

Bauru, 26 de Novembro de 2014.

Dedico este trabalho a minha família, em especial minha mãe Luceli Venerando pelo amor, dedicação e por sempre me incentivar nos estudos, e a todos os envolvidos que de muitas formas me incentivaram e ajudaram para que fosse possível a concretização desta etapa.

AGRADECIMENTOS

A Deus pela força que nunca me faltou e por permitir que eu concluísse uma etapa tão importante em minha vida.

Agradeço especialmente e carinhosamente aos meus pais, Luceli Luiza da Silva Venerando e Adilson Carlos Venerando, que sempre me incentivaram a estudar. Sou grata pelo amor incondicional, pela confiança, pelo respeito, pelos conselhos em me orientar e por acreditar em minhas escolhas.

A Clara Mariana Venerando, pela honra e alegria de ser minha irmã.

A minha avó paterna, por todo amor, carinho e companheirismo prestado no decorrer do curso, no qual é de extrema importância.

Agradeço a todos os professores do curso de Ciência da Computação da Universidade, que no decorrer de todo o curso empenharam-se compartilhando o conhecimento e contribuindo para meu crescimento; especialmente ao Coordenador e Prof. Me. Patrick Pedreira pelas dicas e paciência prestada; ao Prof. Me. Henrique Pachioni Martins, meu orientador, que inspirou e valorizou meus esforços, não permitindo assim que eu desistisse mesmo quando acreditava não ser possível realizar tal tema e claro por toda sabedoria, confiança e apoio prestado.

Agradeço aos professores que compõem a banca examinadora pela contribuição dedicada a este estudo.

Agradeço a Universidade do Sagrado Coração (USC), pela satisfação em poder fazer parte desse time de profissionais e conviver durante a realização deste curso.

Agradeço aos meus grandes amigos que fiz no decorrer do curso, Diego Regys, Guilherme Lacerda e John Bezerra pelo apoio, críticas, sugestões, empenho, dedicação e por ajudarem a tornar esse período muito mais divertido.

E por último, e nem por isso menos importante, agradeço Franciele Vieira e Anne Caroline Nascimento pela amizade excepcional, pelo carinho, paciência em momentos difíceis, compreensão em sempre estarem dispostas a ajudar e pelo apoio em torno desses quatro anos, por me fazerem acreditar que eu era capaz.

E a todos que contribuíram de alguma forma e, por algum motivo não foram citados, meu obrigado. Sou grata a cada um.

RESUMO

As proporções alcançadas por meio da tecnologia são enormes. Praticamente tudo em um mundo informatizado funciona a base de dispositivos de armazenamento, desenvolvimento de software e meios de comunicação online onde estão todos interligados a um único ponto: a tecnologia. Com esta atuando de forma tão imponente no mundo nos deparamos com os criminosos que a usam para cometer delitos, desta forma, tornando primordial a análise de computadores pela perícia forense computacional. O presente trabalho teve como objetivo expor, de forma sucinta, a importância da perícia forense digital no cenário de avanços tecnológicos que auxiliam a vida do ser humano e acabam por ser usados contra ele mesmo. Serão abordados tópicos ao leitor bem como a definição do termo computação forense, os procedimentos realizados em uma investigação em dispositivos de armazenamento e a solução de crimes na área de informática. A perícia computacional traz ao mercado da tecnologia a solução criminalística, sendo um auxiliar da justiça na coleta de provas através de evidências digitais. Em meios práticos, a finalidade da perícia computacional é buscar formas para comprovar um crime de informática e levar a justiça até o autor. Nesse contexto, o trabalho analisou técnicas de perícia forense computacional para recuperação de arquivos em dispositivos de armazenamento, são elas: busca e preservação de evidências, extração, análise, laudo pericial, ferramentas que auxiliam o perito no trabalho de investigação e também a importância do perito forense em desvendar crimes aparentemente impossíveis. A metodologia utilizada para o desenvolvimento do trabalho foi através de pesquisas bibliográficas em livros, monografias, teses, dissertações e artigos científicos para enriquecimento do trabalho proposto. Deste modo o trabalho evidenciou que o Helix e Forensic Toolkit são duas ferramentas de grande importância ao perito forense digital, visto na parte de análise que as duas ferramentas exploram basicamente os mesmos contextos, porém o Helix atende ao maior tipo de necessidade de um perito forense na hora da investigação, enquanto o Forensic Toolkit é um pouco falho em análise de arquivos com esteganografia e entre outros.

Palavras-Chave: Perícia Forense. Tecnologia. Evidências. Investigação. Dispositivos de Armazenamento.

ABSTRACT

The proportions achieved through technology are huge. Virtually everything in a computerized world works based on storage devices, software development and online media, all interconnected to a single point: technology. With this acting as imposing form in the world, we are faced with criminals who use it to commit crimes. For this reason, it's really important to make primary analysis of computers by computer forensics. This paper aimed to explain, briefly, the importance of digital forensics at the scene of technological advances that help the human being's life, and end up being used against him. Topics will be addressed to the reader as well as the definition of computer forensics, the procedures in an investigation on storage devices and solving crimes in informatics. The computational technology expertise brings to market a forensic solution, being an auxiliary of justice in gathering evidence on digital evidence. In practical ways, the purpose of computer forensics is to seek ways to prove a digital crime and bring justice to the perpetrator. In this context, the paper analyzed the computational forensics techniques evidence the files on storage devices, such as: search and preservation of evidence, extraction, analysis, expert opinion, the expert tools that assist in research work, and also the importance of forensic expert unravel seemingly impossible crimes. The methodology used for the development of labor was through literature searches in books, monographs, theses, dissertations and scientific enrichment for the proposed work items. Thus the work showed that the Helix and Forensic Toolkit are two very important tools to digital forensics expert, seen on the analysis that the two tools basically exploit the same contexts, but the Helix serves the higher type of need for a forensic expert at the time of research, while the Forensic Toolkit is a bit flawed in analysis files with steganography and others.

Keywords: Expert Forensic. Tech. Evidence. Investigation. Storage devices

LISTA DE FIGURAS

| | |
|---|----|
| Figura 1 - Macroprocesso simplificado do evento até a sentença final | 17 |
| Figura 2 - Etapas do processo de investigação..... | 20 |
| Figura 3 - Processo de investigação | 23 |
| Figura 4 – Ferramenta Helix com o terminal aberto | 29 |
| Figura 5 – Tela Forensic Toolkit | 30 |
| Figura 6 - Arquivos inseridos no <i>pen drive</i> antes da análise oficial..... | 33 |
| Figura 7 - Criação da imagem | 36 |
| Figura 8 - Extração dos dados | 37 |
| Figura 9 - Análise dos dados..... | 38 |
| Figura 10 - Terminal do Ubuntu criando a imagem | 40 |
| Figura 11 - Terminal do Ubuntu copiando os dados do dispositivo..... | 41 |
| Figura 12 - Criação da Imagem com a ferramenta FTK | 43 |
| Figura 13 - Destino da imagem criada na ferramenta FTK..... | 43 |
| Figura 14 - Status de criação da imagem obtida na ferramenta FTK..... | 44 |
| Figura 15 - Informações obtida da imagem com a ferramenta FTK | 44 |
| Figura 16 - Tela inicial do AutoPsy para criação do caso a ser investigado..... | 45 |
| Figura 17 - Caminho da imagem criada com a ferramenta Helix | 45 |
| Figura 18 - Confirmação da imagem criada no Helix | 46 |
| Figura 19 - Busca por palavra chave na ferramenta Helix..... | 46 |
| Figura 20 - Criação da evidência com a ferramenta FTK..... | 47 |
| Figura 21 - Arquivos encontrados da imagem pela ferramenta FTK | 47 |
| Figura 22 - Comparativo da MD5 pela ferramenta Helix | 48 |
| Figura 23 - Resultado na busca do nome do dispositivo com a ferramenta Helix..... | 49 |
| Figura 24 - Arquivos deletados encontrados na ferramenta Helix..... | 49 |
| Figura 25 - Categoria de arquivos encontrados com..... | 50 |
| Figura 26 - Relatório das MD5 criado na ferramenta Helix..... | 50 |
| Figura 27 - Análise de arquivo na ferramenta Helix. | 51 |
| Figura 28 - Resultado da análise de esteganografia na ferramenta Helix..... | 51 |
| Figura 29 - Análise hexadecimal no Helix com arquivo esteganografado. | 52 |
| Figura 30 - Informações obtidas do arquivo com esteganografia..... | 52 |
| Figura 31 - Arquivo encontrado dentro do arquivo com esteganografia..... | 53 |
| Figura 32 - Imagem encontrada dentro do arquivo com esteganografia..... | 53 |

| | |
|---|----|
| Figura 33 - Resultado da análise de um arquivo .txt na ferramenta Helix | 53 |
| Figura 34 - Dado encontrado na análise hexadecimal de um arquivo .ppt..... | 53 |
| Figura 35 - Informações do áudio com esteganografia na ferramenta Helix..... | 54 |
| Figura 36 - Resultados na ferramenta Helix do áudio com esteganografia..... | 54 |
| Figura 37 - Total de arquivos recuperados com a ferramenta Helix..... | 55 |
| Figura 38 - Arquivos deletados recuperados pela ferramenta Helix..... | 55 |
| Figura 39 - Arquivos encontrados dentro do arquivo esteganografado..... | 56 |
| Figura 40 - Arquivo encontrado dentro do audio esteganografado | 56 |
| Figura 41 - arquivo contido dentro da esteganografia aberto..... | 57 |
| Figura 42 - Tela inicial do FTK para exportação da imagem criada | 57 |
| Figura 43 - Resultado na busca do nome do dispositivo na ferramenta FTK..... | 58 |
| Figura 44 - Arquivos encontrados dentro da imagem pela ferramenta FTK..... | 59 |
| Figura 45 - Arquivo deletado e aberto pela ferramenta FTK | 59 |
| Figura 46 - Análise de arquivo na ferramenta FTK..... | 60 |
| Figura 47 - Análise de arquivo com esteganografia na ferramenta FTK. | 60 |
| Figura 48 - Evidência dentro do arquivo com esteganografia na ferramenta FTK. ... | 61 |
| Figura 49 - Evidência encontrada na ferramenta FTK de um arquivo .txt | 61 |
| Figura 50 - Evidência na ferramenta FTK de um arquivo .ppt..... | 62 |
| Figura 51 - Evidência encontrada na ferramenta FTK de um áudio | 62 |
| Figura 52 - Resultado das ferramentas utilizadas no trabalho | 63 |

LISTA DE ABREVIATURAS E SIGLAS

| | |
|--------------|--|
| 3GP | <i>Third Generation Partnership</i> |
| ADJ | <i>Adjetivos</i> |
| AVI | <i>Audio video interleave</i> |
| BMP | <i>BitMap</i> |
| COC | <i>Chain of Custody</i> |
| CD | <i>Compact disc</i> |
| CPU | <i>Central processing unit</i> |
| DD | <i>Data description</i> |
| DVD | <i>Digital versatile disc</i> |
| DOC | <i>Document</i> |
| DOCX | <i>Document Extended</i> |
| FTK | <i>Forense toolkit</i> |
| GB | <i>Gigabyte</i> |
| HD | <i>Hard disk</i> |
| HOST | <i>Hospedeiro</i> |
| IBAPE | <i>Instituto brasileiro de avaliações e perícias de engenharia</i> |
| IF | <i>Input File</i> |
| IOCE | <i>The international organization of computer evidence</i> |
| JPG | <i>Joint photographic group</i> |
| JPEG | <i>Joint photographic experts group</i> |
| MP3 | <i>Moving picture experts group 1(mpeg) audio layer 3</i> |
| MP4 | <i>Moving picture experts group 1(mpeg) audio layer 4</i> |
| OF | <i>Output File</i> |
| PC | <i>Personal computer</i> |
| PDA | <i>Personal digital assistant</i> |
| PDF | <i>Portable Document Format</i> |
| PNG | <i>Portable Network Graphics</i> |
| PPT | <i>Power Point</i> |
| RAM | <i>Random Access Memory</i> |
| SWGDE | <i>Scientific working group on digital evidence</i> |
| TXT | <i>Text</i> |
| WAV | <i>Waveform Audio</i> |
| XLSX | <i>Excel Microsoft Office Open XML Format Spreadsheet</i> |

SUMÁRIO

| | |
|---|-----------|
| 1 INTRODUÇÃO | 12 |
| 2 OBJETIVOS..... | 14 |
| 2.1 OBJETIVO GERAL..... | 14 |
| 2.2 OBJETIVOS ESPECÍFICOS | 14 |
| 3 ORGANIZAÇÃO DO TRABALHO | 15 |
| 4 REFERENCIAL TEÓRICO..... | 16 |
| 4.1 DEFINIÇÃO DE PERÍCIA..... | 16 |
| 4.2 PERÍCIA FORENSE COMPUTACIONAL..... | 16 |
| 4.2.1 Investigação Forense Computacional | 18 |
| 4.2.2 Procedimentos e Métodos aplicados a Perícia Forense Computacional .. | 19 |
| 4.2.3 Perito Forense Computacional..... | 22 |
| 4.3 FASES E ETAPAS DA PERÍCIA FORENSE COMPUTACIONAL | 22 |
| 4.3.1 Preservação | 23 |
| 4.3.2 Extração | 25 |
| 4.3.3 Análise das Evidências..... | 26 |
| 4.3.4 Formalização | 27 |
| 4.4 PRINCIPAIS DIFICULDADES DURANTE A INVESTIGAÇÃO | 27 |
| 4.5 FERRAMENTAS DE COMPUTAÇÃO FORENSE..... | 28 |
| 4.5.1 Forense ToolKit | 28 |
| 4.5.2 Helix..... | 28 |
| 5 METODOLOGIA | 30 |
| 5.1 PRESERVAÇÃO | 36 |
| 5.2 EXTRAÇÃO..... | 37 |
| 5.3 ANÁLISE DAS EVIDÊNCIAS | 38 |
| 5.4 FORMALIZAÇÃO | 39 |
| 6 RESULTADOS..... | 40 |
| 6.1 PRESERVAÇÃO | 40 |
| 6.1.1 Utilizando a ferramenta Helix | 40 |
| 6.1.2 Utilizando a ferramenta FTK..... | 43 |
| 6.2 EXTRAÇÃO..... | 45 |
| 6.2.1 Utilizando a ferramenta Helix | 45 |
| 6.2.2 Utilizando a ferramenta FTK..... | 47 |
| 6.3 ANÁLISE DAS EVIDÊNCIAS | 48 |
| 6.3.1 Utilizando a ferramenta Helix | 48 |
| 6.3.2 Utilizando a ferramenta FKT | 57 |
| 6.4 FORMALIZAÇÃO | 63 |
| 7 CONCLUSÃO | 64 |
| 8 TRABALHOS FUTUROS..... | 66 |
| REFERÊNCIAS..... | 67 |

| | |
|--|-----------|
| APÊNDICE A - TABELA DADOS GERADOS COM A FERRAMENTA FTK..... | 69 |
| APÊNDICE B - MODELO DE LAUDO JUDICIAL | 72 |

1 INTRODUÇÃO

Com o avanço tecnológico de ferramentas para invasão de sistemas, os crimes virtuais obtiveram força e, conseqüentemente, êxito nos ataques efetuados. Para prevenir e até mesmo extinguir os ataques virtuais, peritos especializados utilizam técnicas forenses como forma de combate. Visto que a perícia forense aplicada à computação é ligada à investigação de crimes cibernéticos colhendo dados para identificação, análise e documentação, com a finalidade de obtenção de evidências digitais. (SOUZA, 2011).

Devido ao aumento na procura de dispositivos de armazenamento computacionais, os próprios dispositivos ficam vulneráveis a métodos de cópia ou técnicas *cracker* por pessoas supostamente maliciosas, lembrando que é necessário diferenciar crackers de hackers. Gonçalves et al., (2012), define *hackers* sendo indivíduos virtuais conhecidos por invadirem sistemas, para desafiar suas próprias habilidades e conhecimentos. Já Assunção (2002 apud GONÇALVES et al., 2012, p.9), define *crackers* como *hackers* antiéticos, que utilizam o seu conhecimento para fazer invasão em sistemas, furtar informações, adulterar dados, e o que for necessário para obter o que desejam, causando prejuízo as vítimas e a sociedade.

Segundo Eleutério e Machado (2011), a computação forense é a ciência que usa técnicas especializadas, para coletar e analisar dados digitais de um ou mais computadores suspeitos de serem utilizados em um crime virtual. Sendo que existem etapas que servem para combater supostas ameaças em vários tipos de dispositivo de armazenamento.

Gonçalves et al. (2012) cita outros tipos de dispositivos de armazenamento que podem ser analisados numa perícia forense computacional, como: *pen drives*, CDs, DVDs, cartões de memória, mp3, câmeras digitais, celulares, dentre outros. Dispositivos esses que passarão por uma análise completa e rigorosa, pois deverão cumprir etapas para chegarem a uma conclusão que comprovarão ou não um crime.

Deste modo, existem procedimentos em casos específicos de análise de mídia de armazenamento digital que devem ser seguidos pelo perito, para assegurar que a evidência não seja comprometida, substituída ou perdida. (FREITAS, 2007).

Relatadas de forma sucinta no trabalho como quatro fases, descritas como: preservação; extração; análise e formalização, a fim de explicar o manuseio correto de cada uma.

A perícia forense computacional abrange questões relacionadas de como coletar evidências de crimes, analisar e documentar casos e, desta forma, torna-se um tema totalmente escasso, superficial ou até mesmo incompleto em muitos objetos de pesquisa, pois aborda apenas uma das vertentes dessa área, e com base neste contexto, este estudo teve por finalidade aprimorar o conhecimento das fases relacionadas à investigação digital em um dispositivo de armazenamento e comparar as ferramentas utilizadas, resultando na confecção de um comparativo com informações sobre as características dos *softwares* analisados e suas potencialidades.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Identificar as etapas de uma perícia forense em ferramentas, abordando técnicas utilizadas em cada fase de um dispositivo de armazenamento.

2.2 OBJETIVOS ESPECÍFICOS

- Estudar as fases da perícia forense.
- Levantar estratégias para análise pericial.
- Identificar as técnicas utilizadas em cada fase estudada.
- Pesquisar *softwares* específicos das técnicas de cada fase.
- Verificar os recursos que cada ferramenta apresenta.
- Estabelecer um comparativo, evidenciando as potencialidades de cada ferramenta.

3 ORGANIZAÇÃO DO TRABALHO

O Capítulo 1 contém a introdução do trabalho juntamente com a justificativa para desenvolvimento deste trabalho

O Capítulo 2 relata os objetivos gerais e específicos que foram adotados.

O Capítulo 3 contém a organização do trabalho.

O Capítulo 4 abrange o referencial teórico, relativo à perícia forense computacional, procedimentos e métodos que compõem uma investigação.

Já o Capítulo 5 apresenta a metodologia, elencando como foi o desenvolvimento do objetivo proposto.

No Capítulo 6 estão descritos a análise e os resultados obtidos na realização deste trabalho.

O Capítulo 7 contém as considerações finais sobre os resultados apresentados no capítulo anterior.

Por fim, o Capítulo 8 contém a sugestão de possíveis trabalhos futuros.

4 REFERENCIAL TEÓRICO

4.1 DEFINIÇÃO DE PERÍCIA

Perícia, do latim *perícia*, é definida por (PERICIA, c2013) “sabedoria, prática, experiência, habilidade em alguma ciência ou arte.”, vista como qualidade de perito e citada no glossário (INSTITUTO BRASILEIRO DE AVALIAÇÕES E PERÍCIAS DE ENGENHARIA DE SÃO PAULO - IBAPE) por Neto (2011), define *perícia* como atividade profissional especializado, legalmente habilitado a esclarecer um fato.

Já o termo Forense, do latim *forense* (FORENSE, c2013), “adj. Relativo ao foro judicial. / Que se usa nos tribunais: expressão forense”,

Segundo Farmer e Venema (2007), a perícia é considerada a ciência de coletar e analisar evidências, reconstruindo ataques e recuperando dados.

O perito forense computacional consiste em um analista de sistemas, especialista em metodologias laboratoriais e padronização da investigação, aquisição, análise e manuseio de evidências em inquéritos, forense digital, inteligência e contra inteligência, como definem vários autores. (FAERMER e VENEMA, 2007).

A perícia age quando é necessário um laudo de um especialista no assunto, a busca de fatos e provas para esclarecer o que aconteceu no local, como afirma Mello, Silva e Tolentino, (2011). Conceitos devem ser entendidos, sugerido por Farmer e Venema (2007), como: a volatilidade dos dados, a coleta de quantidade máxima de evidências confiáveis e a recuperação de informações destruídas com o intuito de manter a credibilidade das informações analisadas. Deste modo a perícia forense deve seguir fases denominadas (seção 4.3).

4.2 PERÍCIA FORENSE COMPUTACIONAL

Segundo Faria (2011), a perícia forense computacional é a ciência que através de técnicas investiga computadores e equipamentos digitais, com o intuito de recriar e obter o mais próximo do cenário de um crime para a obtenção de evidências computacionais, tomando o cuidado de preservar os dados processados eletronicamente e armazenados em dispositivos, possibilitando uma análise

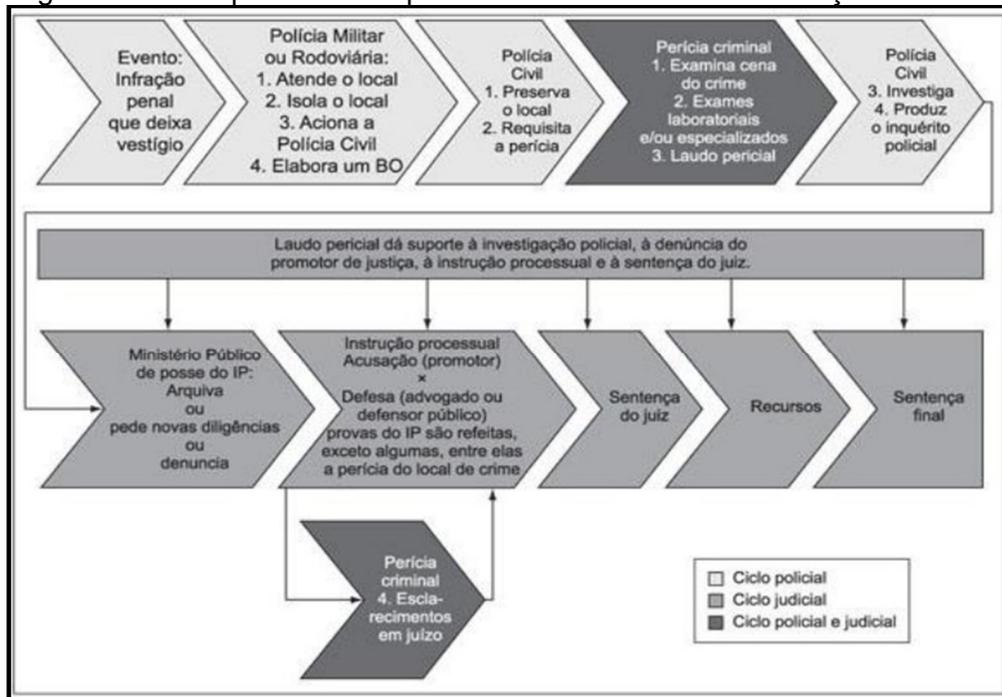
detalhada das evidências encontradas e a confecção de documentação que possa servir de provas para serem utilizadas em processos judiciais.

Freitas (2006 apud AZEVEDO et al., 2011, p. 6) afirma que, a aplicação de conhecimento de informática e técnicas de investigação com a finalidade de obtenção de evidências, além de ser uma área relativamente nova e em grande ascensão, tornou-se uma prática importante nas corporações policiais e judiciais que utilizam esses resultados científicos para achar o real culpado do crime (figura 1).

A computação forense é definida por Silva Filho (2009 apud FARIA, 2011, p.17), como uma área de estudos da investigação que vem se expandindo com o avanço dos crimes cibernéticos.

Faria (2011), afirma que os principais objetivos da computação forense é observar as descobertas de novas fontes desde que a análise e a perícia dos computadores tenham passado por algum tipo de violação ou ataque, pois passam a tornar-se uma matéria importante no conjunto de ações no processo de segurança, possibilitando assim o entendimento do ocorrido de forma a corrigir falhas.

Figura 1 - Macroprocesso simplificado do evento até a sentença final



Fonte: Faria (2011, p.18).

Em casos de crimes computacionais Costa (2011), relata que as provas são classificadas pelas normas SWGDE (*Scientific Working Group on Digital Evidence*) e IOCE (*The International Organization of Computer Evidence*) em:

- **Provas digitais:** informação de valor para um processo penal que está armazenado ou transmitido de forma digital;
- **Dados de objetos:** consiste em objetos de valor para um processo penal o qual está associado a itens físicos;
- **Itens físicos:** consiste nas mídias físicas onde a informação digital é armazenada ou pelo qual é transmitido ou transferido.

4.2.1 Investigação Forense Computacional

Em alguns casos, a perícia forense responde quesitos pré-estabelecidos, como por exemplo “descrever o conteúdo para um exame”, entretanto são muitas as informações da análise em um sistema computacional. ADAMS (2000).

Segundo Pereira (2010 apud FARIA, 2011, p.32), diferentemente das provas físicas pertinentes aos crimes convencionais, às comprovações que são encontradas em mídias magnéticas são digitais, podendo existir de diversas formas como: arquivos, dispositivos, fragmentos de logs e outros indícios residentes em uma mídia que podem estar relacionados criando uma evidência que indique a ocorrência de um crime ou auxilie a identificação de um criminoso.

O processo de investigação de uma perícia computacional, citado por Faria (2011), ocorre de forma cuidadosa, procurando preservar as características originais para que não haja interferência alguma nas evidências do ato ilícito.

De acordo com Rodrigues e Foltran (2010 apud FARIA, 2011, p.32), o processo investigativo da forense computacional deve assegurar a integridade dos vestígios coletados, porém devido à volatilidade das evidências eletrônicas essa tarefa é considerada difícil, deste modo o perito forense deve seguir procedimentos e protocolos reconhecidos pela comunidade científica. No qual deve detalhar e revisar a documentação desenvolvida para que evite erros durante a investigação.

Neukamp (2007 apud GONÇALVES et al., 2012, p.5), define o sistema de arquivos de um computador em vários tipos de dados: binário, textos, imagens, áudios, sendo que todos eles precisam ser analisados e identificados com relação a sua funcionalidade dentro do sistema investigado.

Além de alterações, exclusão ou até mesmo incluso de modificações inesperadas em diretórios, arquivos (especialmente aqueles cujo acesso é restrito) podem caracterizar-se como indícios para uma infração. Exemplo: arquivos do tipo DOC, TXT, imagens, programas executáveis, aplicações instaladas (exe), dentre outras. (FREITAS, 2006, p. 73).

Outro ponto na investigação, segundo Neukamp (2007 apud GONÇALVES et al., 2012, p.6), é a memória, por conter arquivos voláteis do sistema usados pelos programas em funcionamento no disco rígido. Sendo assim possível recuperar dados por um processo conhecido com dump¹ de memória, onde é gravado todo o conteúdo da memória para um arquivo de imagem como forma de Backup.

4.2.2 Procedimentos e Métodos aplicados a Perícia Forense Computacional

Para uma boa execução da perícia forense computacional segundo Eleutério e Machado (2011), existem quatro fases primordiais a serem cumpridas:

- Preservação
- Extração
- Análise
- Formalização

Logo, Freitas (2007 apud MELLO et al., 2011, p. 27) afirma que perícia forense possui quatro procedimentos básicos e que todas as evidências devem ser:

- A. Identificadas
- B. Preservadas
- C. Analisadas
- D. Apresentadas

Almeida (2011) descreve que uma investigação envolvendo análise de dispositivos computacionais deve cumprir quatro etapas: (Seção 4.3).

- **Preservação:** O perito deve isolar a área; identificar equipamentos; coletar; etiquetar e garantir a integridade das evidências.
- **Extração:** Nesta fase, deve-se identificar extrair e documentar os dados relevantes a fim de apreender os objetos que tiverem relação com o fato.

¹ Técnica de Backup

- **Análise:** Os dados transformam-se em informações que o perito deve identificar; correlacionar pessoas; locais; eventos; reconstruir as cenas e documentar os fatos;
- **Formalização:** Deve-se redigir o laudo; anexar às evidências e demais documentos.

Para uma melhor compreensão do ciclo dos procedimentos forenses Goldini, Pereira e Weber (2009 apud FARIA, 2011, p.33) demonstram (figura 2), como ocorrem as duas transformações da mídia em evidência:

Figura 2 - Etapas do processo de investigação



Fonte: Faria (2011, p. 33).

Explicação das duas transformações (figura 2):

- I. A transformação ocorre quando os dados coletados são examinados e as informações extraídas da mídia são analisadas por ferramentas forenses;
- II. Depois a análise dos dados cria informações que processadas resultam em evidências.

Na identificação da primeira fase Mello, Silva e Tolentino, (2011), afirmam que o perito deve atentar para o tipo de crime praticado, por exemplo: crime de pornografia com menores; o perito deve identificar imagens; o computador ou dispositivo apreendido; vídeos; histórico e arquivos temporários do navegador.

Portanto, ao identificar uma evidência digital, a parte física de um computador ou qualquer dispositivo de equipamento digital, é de muita importância para descobrir novas pistas.

A Cadeia de Custódia² (coc), segundo Lopes et al., (2008 apud MELLO, SILVA E TOLENTINO, 2011, p.27) viabiliza o controle sobre a amostra com a

² Documentar a história cronológica da evidência

identificação nominal das pessoas envolvidas em todas as fases do processo, caracterizando responsabilidades nas quais são reconhecidas institucionalmente. Sendo assim, o cuidado com a evidência deve ser extremamente alto durante o seu transporte, uma vez que quedas, alta temperatura, líquidos e poeira causam danos à evidência acarretando a não veracidade da mesma.

A prova após ter sido transportada deverá estar em local seguro e monitorado para garantir a inviolabilidade. Freitas (2007, apud Mello, Silva e Tolentino, 2011, p. 27), cita que a análise é uma das etapas mais importantes da perícia forense.

Os primeiros a chegarem à cena do crime devem tomar algumas precauções segundo Mello, Silva e Tolentino (2011), para que possa garantir a integridade das evidências e dependendo do perito, identificar evidências depende da sua familiaridade com o tipo de crime cometido, dos programas e sistema operacional.

Shinder (2002 apud COSTA, 2008, p.27) afirma que se devem ter os primeiros cuidados ao procurar evidências, sendo:

- **Identificar a cena/lugar do crime:** Verificar a extensão da cena do crime e definir um perímetro. Isso pode incluir desde uma sala até edifícios inteiros.
 - **Procurar por dispositivos de armazenamento (*hardwares*):** *laptops*, HDs, Cds, DVDs, drives, *pen drives*, câmeras digitais, MP3, celulares, smartphones, dispositivos de backup ou qualquer equipamento que possa armazenar evidências;
- **Proteger a cena do crime:** Todos os equipamentos laptops, notebooks, dispositivos de armazenamento, desktops, PDA's entre outros devem ser protegidos. Estes itens podem ser limitados devido ao mandado, mas até que o investigador chegue ao local nada pode ser descartado.
 - **Procurar por informações relacionadas:** anotações, nomes de pessoas, datas, nomes de empresas, instituições, números de telefones e documentos impressos.
- **Preservar as evidências temporárias:** Evidências que possam desaparecer antes dos investigadores chegarem, como informações sendo exibidas no monitor e mudando constantemente, os primeiros a chegar ao local do crime devem tomar quaisquer medidas possíveis para preservar as evidências.

Toda evidência encontrada precisa ser documentada para validação. Para isso, segundo Mello, Silva e Tolentino (2011), afirmam que existem duas separações por prioridade das evidências (irrelevante e relevante), onde cada uma dessas evidências é usada como provas no tribunal.

A apresentação da análise é feita através do laudo técnico em que devem constar os fatos; as evidências; os procedimentos e os resultados. O laudo terá que ser o mais claro possível e objetivo de forma que apresente as ideias mais formais.

4.2.3 Perito Forense Computacional

O perito forense investiga fatos de ocorrência e propõe um laudo técnico para o entendimento de um episódio comprovado através de provas. Um perito é chamado quando a resolução de um delito não fica clara e em casos de ações judiciais, é escolhido por um juiz para o caso específico. (MELLO, SILVA E TOLENTINO, 2011).

Trata-se de um profissional que tende a ter maior responsabilidade em uma cena pós-crime, pois comprova através do ocorrido e quem é o devido culpado.

Queiroz e Vargas (2010) fazem uma lista com dicas importantes para ajudar a traçar o perfil do profissional:

- Ter formação superior em tecnologia;
- Possuir mestrado acadêmico ou profissional (dentro da área);
- Ter especialização;
- Ter conhecimento das leis que envolvam crimes praticados
- Ter boa redação (estudar concordância e verbos é fundamental);
- Estudar técnicas de redação jurídica;

4.3 FASES E ETAPAS DA PERÍCIA FORENSE COMPUTACIONAL

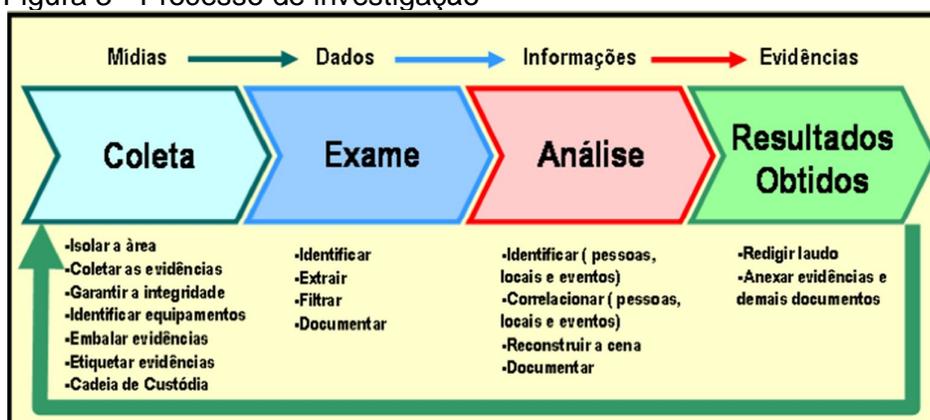
Após o cumprimento do mandado de busca e apreensão, segundo Almeida (2011), o perito deve encaminhar o material confiscado para um laboratório capacitado a fim de realizar os exames necessários e ao receber o dispositivo de armazenamento computacional, independente se for um disco rígido, *pen drive* ou

outra mídia, o perito deve concluir uma série de etapas que são descritas a seguir, porém serão melhores detalhadas ao longo desse capítulo.

Abaixo a figura 3, exemplifica como é um processo de investigação forense;

- I. **Coleta:** Garantir as informações armazenadas no material.
- II. **Exame:** Execução de procedimentos.
- III. **Análise:** Exame de informações do material
- IV. **Resultado:** Formação do laudo.

Figura 3 - Processo de investigação



Fonte: Pereira (2010).

4.3.1 Preservação

Assim como em um local de crime convencional cujas provas existentes devem ser preservadas, Almeida (2011) relata que os dados do material enviado para exames forenses jamais devem ser alterados. Pois a garantia da cadeia de custódia é uma das principais obrigações do perito, ele deve assegurar a proteção da prova a fim de evitar questionamentos quanto à sua origem, vendo que qualquer suspeita pode anulá-la e colocar em risco toda a investigação.

Almeida (2011), ainda descreve que precauções especiais devem ser tomadas ao manipular equipamentos, pois operações simples podem modificar as evidências armazenadas. Situações básicas como ligar o computador, por exemplo, alterará alguns arquivos, datas de último acesso e criam arquivos temporários, mesmo que o usuário não execute nenhuma ação no computador. Até a conexão de um *pen drive* na porta USB pode gerar gravação de dados no dispositivo.

Eleutério e Machado (2011) descrevem que há dois métodos mais utilizados para a preservação.

Os exames forenses devem sempre ser realizados em cópias fiéis obtidas a partir do material original. Para conceber tais cópias, os peritos utilizam, principalmente, duas técnicas de espelhamento ou imagem. (ELEUTÉRIO E MACHADO, 2011, p.54).

Já Newkamp (2007 apud GONÇALVES et al., 2012. P.11), relata a preservação ou por ele chamada coleta de dados, é a etapa em que devem ser identificadas e processadas as evidências.

O processo de identificação, processamento e documentação de possíveis provas, ocorre no primeiro passo de uma investigação criminal, ou seja, durante o processo de coleta de evidências, sendo esta, considerada a mais vital das etapas da investigação. (NEUKAMP, 2007, p. 26).

Almeida (2011) descreve os métodos da preservação sendo o espelhamento a primeira técnica que consiste na cópia exata e fiel dos dados contidos em um dispositivo de armazenamento computacional para outro, ou seja, a duplicação.

O segundo método, que foi a proposta do trabalho, como citado por Almeida (2011), é a chamada técnica de dump, ou gerador de imagem, que consiste na duplicação de discos feita bit a bit, ou seja, processo semelhante ao espelhamento que se copia dados encontrados do sistema operacional, programas, drivers, configurações e todo tipo de arquivo, originando assim uma reprodução exata e fiel do disco. Almeida (2011) afirma que o método de cópia bit a bit dos dados é a mais segura, pois é feita uma cópia real do dispositivo. Vantagens dessa técnica segundo Eleutério e Machado (2011):

- Possibilidade de copiar o disco inteiro ou uma de suas partições;
- Possibilidade do dispositivo de destino ser utilizado para receber distintas imagens de dispositivos variados.
- Facilidade em manipular os dados.
- Capacidade de compactar os arquivos de imagens.

Almeida (2011) contextualiza que a cópia dos dados deve ser efetuada de forma que as informações contidas no material questionado não sejam alteradas.

Após o término da preservação, o dispositivo de armazenamento deverá ser lacrado e guardado em um local apropriado até que haja a autorização por parte da justiça permitindo o seu descarte. (ELEUTÉRIO E MACHADO, 2011).

4.3.2 Extração

No processo de perícia computacional segundo Gonçalves et al. (2012), a fase de extração é a mais trabalhosa.

O ato de extrair, localizar e filtrar somente as informações que possam contribuir, de forma positiva, em uma investigação ocorre na segunda etapa, denominada “exame de evidências”. Considera-se esta, a etapa mais trabalhosa do processo de investigação criminal, principalmente pela quantidade de diferentes tipos de arquivos existentes (áudio, vídeo, imagem, arquivos criptografados, compactados, etc.) que facilitam o uso de esteganografia, o que exige que o perito esteja ainda mais atento e apto a identificar e recuperar esses dados. (FARMER; VENEMA, 2007 p. 41).

Almeida (2011) relata que a fase de extração consiste na recuperação e organização das informações contidas na cópia do passo anterior, ou seja, a ação executada da imagem do disco (.dd) mantendo o material original intacto.

Etapas importantes para o processo investigativo, pois as análises serão realizadas a partir de seu resultado. E de acordo com Almeida (2011) ao examinar o material (imagem criada), é importante que a extração dos dados seja feita de forma minuciosa e com atenção, pois uma das evidências podem estar em áreas improváveis do disco.

Silva Filho (2009 apud FARIA, 2011 p.35) afirma que os técnicos devem levar em conta a natureza volátil dos artefatos e antes de iniciar o processo de busca é preciso definir quais ferramentas serão utilizadas para a extração dos dados, relacionando com o tipo de investigação e os tipos de informações procuradas.

Baseado em métodos de busca, Almeida (2011) define um sistema de arquivo como o conjunto de estruturas lógicas que verifica o modo como os arquivos são estruturados, nomeados, acessados, utilizados, protegidos e manipulados pelo sistema operacional, por armazenar arquivos como sequência de bytes e organizar dentro de um diretório, gerenciando nomes, conteúdos de acesso, data e hora da última modificação. Causando assim felicidade em buscar conteúdos.

Outra técnica que Almeida (2011), cita é pesquisar o conteúdo de um dispositivo de armazenamento por palavras-chave, extensão ou permissões de acesso. Pois a pesquisa por palavras-chave é um meio eficiente para encontrar a maioria das evidências digitais necessárias para elaboração de laudo forense.

Diante disso, essa etapa usou dois tipos de ferramentas para extrair as imagens criadas na fase de preservação, sendo o Helix e o FTK; (seção 4.5).

4.3.3 Análise das Evidências

O objetivo da análise das evidências, segundo Pereira (2010 apud FARIA 2011, p.37) é examinar dados e separar as informações relevantes.

Almeida (2011) relata que analisar o conteúdo de arquivos extraídos da fase anterior, olhando um a um, levará muito tempo e tornará o exame impraticável, com o objetivo de auxiliar o perito nessa tarefa, procedimentos e técnicas podem ser utilizados para tornar esse processo mais eficiente. Um deles é utilizar filtro de arquivos conhecidos para eliminar da análise àqueles que não são importantes para a investigação, mas extrair os dados relevantes, não é o suficiente, pois segundo Sá (2013), o perito forense deve interpretar essas informações de forma correta.

Sá (2013) afirma que se devem identificar características que indiquem relações com a área do crime, como pessoas, e-mails, telefones, locais, vídeos, ou seja, expor tudo que foi buscado na fase da extração.

Logo após a criação de imagem houver fixado as provas do sistema (fase 1) e extraído todos os conteúdos relevantes dos dados (fase 2), o perito pode então analisar os processos por vários métodos e verificar tudo que possa existir dentro de cada arquivo, de acordo com as evidências encontradas como por exemplo, a extensão dos arquivos no formato .doc, .mp3, .avi, .jpg, .txt entre outros.

É permitido ao perito realizar a impressão dos arquivos extraídos, segundo Almeida (2011) além de impresso podem ser reproduzidos em papel sem a perda de informações, como textos, planilhas, figuras e relatórios de sistemas. No entanto, quando se trata de uma grande quantidade de dados como sequências de vídeo, faz-se necessária a utilização de um computador. Deste modo, uma solução viável é a gravação das evidências digitais encontradas pelo perito em mídias computacionais ópticas, como *pen drives*, CDs, que permitem o encaminhamento dos arquivos em seu formato original e sem perda de informações. Deste modo

Almeida (2011) relata que o material, seja um *pen drive*, um disco rígido ou um cartão de memória, não armazena somente o conteúdo de seus arquivos e por isso, deve haver uma atenção para o correto manuseio do material onde deve ser livre do calor excessivo, da alta umidade, atrito e campos magnéticos.

Sendo assim, nessa etapa a proposta foi utilizar novamente as ferramentas FTK e o Helix para expor métodos encontrados para uma análise forense.

4.3.4 Formalização

O laudo técnico ou formalização consiste no último processo da perícia forense computacional, que segundo Freitas (2003 Apud SÁ, 2013, p.15) descreve sendo um relatório gerado a partir da análise, destinado às pessoas leigas e, por isso, a linguagem técnica deve ser simples, para que todos possam compreender.

O perito deve utilizar análises gráficas e visuais com o objetivo de facilitar a compreensão do crime para demonstrar como foi feito o crime. Caso o laudo não for entendido pelos julgadores, pode ser requerido que seja novamente escrito e até mesmo ser pedido à troca do perito.

Um laudo pericial segundo Mello, Silva e Tolentino (2011), deve ser claro levando em conta que o juiz responsável pelo caso só entende do código de lei vigente e não de termos técnicos. O laudo constatará com as conclusões tomadas após minuciosas investigações através das comprovações, detalhando do que foi recolhido e investigado, forma de investigação, de como será provada a veracidade dos artefatos recolhidos e as devidas conclusões tomadas pelo perito.

Mediante ao prazo do laudo pericial, é estimado no prazo máximo de 10 dias, podendo ser prorrogado em casos excepcionais, a requerimento dos peritos (QUEIROZ E VARGAS, 2010 apud MELLO, SILVA E TOLENTINO, 2011).

Deste modo o laudo pericial nada mais é que a conclusão da perícia forense computacional no caso investigado.

4.4 PRINCIPAIS DIFICULDADES DURANTE A INVESTIGAÇÃO

Segundo Almeida (2011), afirma-se que durante todo o processo investigativo, o perito depara-se com diversos desafios que podem atrapalhar ou impossibilitar a apuração dos fatos. Essas dificuldades, quando impostas

explicitamente pelos usuários, são conhecidas comumente na área pelo termo Anti Forense³ e consistem em métodos de remoção ou ocultação das evidências com o objetivo de mitigar os resultados de uma análise forense computacional.

Os termos mais conhecidos é a esteganografia (ESTEGANOGRAFIA, c2013), substantivo feminino do grego descrito; arte de escrever em cifra, escrita encoberta. Almeida (2011) a define; como sendo o estudo e o uso de técnicas para fazer que uma forma escrita seja disfarçada em outra a fim de mascarar o seu verdadeiro sentido. A esteganografia pode ter uma mensagem escondida dentro de arquivos considerados comuns para uso convencional do computador, como imagens, vídeos.

Almeida (2011) também cita que existem atualmente várias outras técnicas de esteganografia, desde mais simples a muito mais complexas do que as apresentadas, o que acaba dificultando o trabalho do perito forense. Caso ele não descubra o tipo utilizado para ocultar a mensagem, uma alternativa é verificar se há *softwares* específicos instalados no dispositivo examinado, pois, desse modo, pode ser possível determinar a técnica praticada, ou até mesmo, usar o próprio *software* para descobrir o conteúdo do arquivo.

4.5 FERRAMENTAS DE COMPUTAÇÃO FORENSE

Existem ferramentas no mercado criadas especificamente para Perícia Computacional e segundo Eleutério e Machado (2011 apud GONÇALVES et al., 2012, p.12), algumas são de uso específico em uma determinada fase e outras que podem ser utilizadas em todas as etapas da investigação, abaixo mostra as ferramentas escolhida para realização do trabalho

4.5.2 Helix

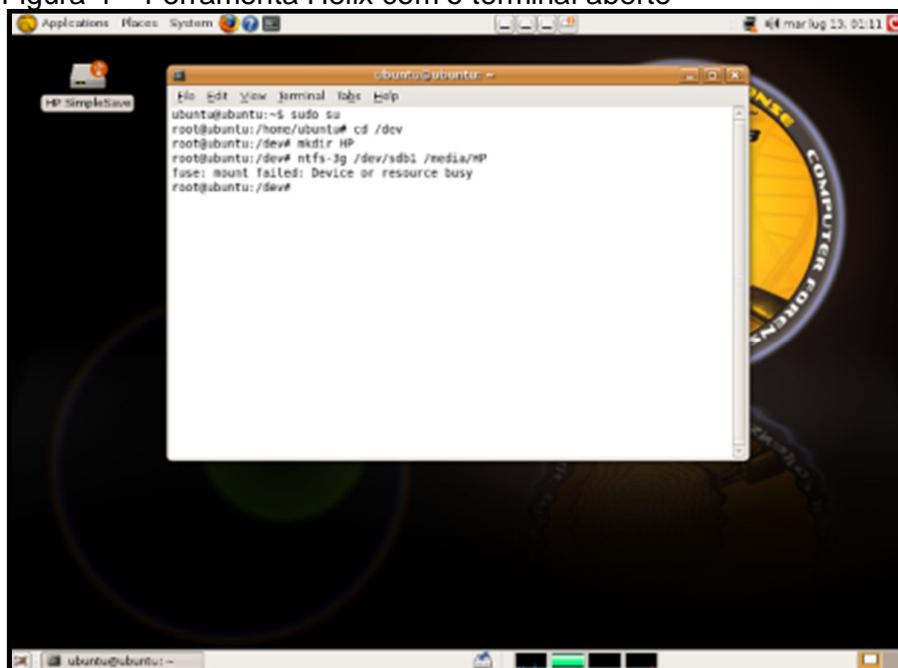
O Helix é uma ferramenta utilizada para análise de exames forense, de uso gratuito, disponível em sistema Linux onde possui opções importes para análise forense como a extração de dados forense, listagem de processos e análise de dados coletados, entre outros itens importantes durante uma análise pericial.

³ Ocultação de dados

O Helix pode ser executado a partir de um CD, ou com o computador ligado como pode ser utilizado de forma inicializável, ou seja, pode ser iniciado ao ligar o computador, onde é carregado no equipamento sua versão em Linux, a ferramentas Helix contem recursos disponíveis para análises dos casos e alguns programas que não estão disponíveis em sua versão Windows, como o Autopsy.

Através do terminal no Helix é possível buscar a validade da MD5 de cada arquivo encontrado em sua raiz, comprovando deste modo à veracidade dos dados encontrados. Como mostra a Figura 4.

Figura 4 – Ferramenta Helix com o terminal aberto



Fonte: Helix (2014).

4.5.1 Forense ToolKit

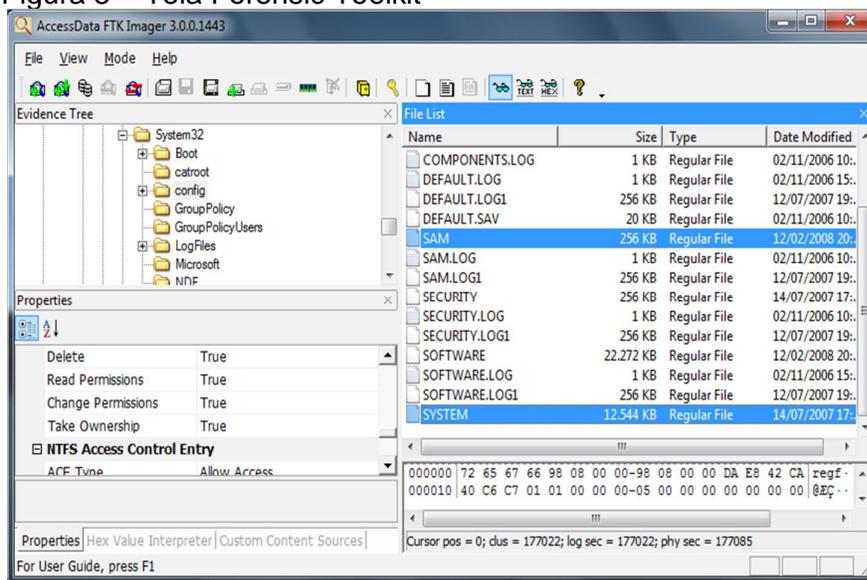
Outra ferramenta utilizada no trabalho foi o ForensicToolKit, conhecido por FTK, disponível em sistema WINDOWS e de uso gratuito, desenvolvida pela AccessData, ferramenta essa que pode-se encontrar as principais funcionalidades para a realização de exames forenses em dispositivos de armazenamento de dados.

O FTK possui vários recursos disponíveis para análise pericial, um dos mais elencados é de criar imagens forense de disco, realizar dumps de memória e realizar

a análise forense na imagem criada, como mostra a figura 5. E por esse modo foi selecionado como uma das ferramentas do trabalho, por ser capaz de atender todas as necessidades do trabalho.

Utilizando a ferramenta FTK, o trabalho buscou analisar todos os recursos que a ferramenta trás, para comprovar que a ferramenta realiza todas as fases do exame computacional forense até a concretização do mesmo.

Figura 5 – Tela Forensic Toolkit



Fonte: FTK (2013).

As ferramentas acima citados, são indispensáveis e contribuem imensamente na solução de casos forense, agilizando assim o processo de investigação e garantindo a integridade da análise desenvolvida pelo perito.

5 METODOLOGIA

O objetivo de uma pesquisa exploratória é proporcionar ao investigador maior familiaridade com um determinado problema, e torná-lo mais explícito ou construir hipótese. Uma pesquisa de aparência exploratória tende a ser bastante flexível, pois leva em consideração os mais variados relatos ao problema estudado, sendo assim pesquisas realizadas com propósitos acadêmicos, assumem caráter exploratório, pois neste momento é pouco provável que o pesquisador tenha uma definição clara e ampla do que irá investigar. (GIL, 2010).

Desse modo, a produção deste trabalho exhibe etapas que devem ser seguidas até a obtenção dos resultados, concretizando, deste modo, a análise da perícia forense computacional em um *pen drive*. Considerando a natureza delicada de se realizar uma série de procedimentos que devem ser seguidos, para que evidências não sejam perdidas ou invalidadas.

Assim, o projeto é inicialmente uma pesquisa exploratória, pois explora as fases para obtenção de evidências digitais em dispositivos de armazenamento, relatando uma pesquisa e produzindo um levantamento de técnicas. Foram feitas pesquisas abordando o tema "perícia forense" e uma revisão literária sobre o tema proposto. Em relato (seção 4.1) também foram feitos um breve resumo sobre o que é a perícia forense, que tem como objetivo informar a importância da perícia atualmente, sendo que é pouco conhecida e explorada hoje em dia. Também foram detalhadas as principais características das etapas que compõe o processo investigativo (seção 4.2.2), visando futuramente à utilização de ferramentas de perícia para a realização das análises em dispositivos de armazenamento.

Um tópico (seção 4.4) sobre as dificuldades durante a investigação foi descrito, com propósito de explicar os problemas que pode surgir no campo investigativo como técnicas de esteganografia, para ter conhecimento sobre os arquivos que pode estar oculto dentro do *pen drive* apreendido.

No campo da perícia forense computacional, peritos devem saber como agir, quais os passos a seguir para que nenhum dano ao equipamento utilizado ocorra, e desse modo, o trabalho deixou claros os passos para preservar o material encontrado e o que fazer no seu estado de pesquisa/análise.

O trabalho foi desenvolvido em duas etapas distintas até a obtenção dos resultados sendo:

A primeira etapa foi feito um levantamento das principais ideias sobre o termo perícia forense, o funcionamento das fases e aspectos das técnicas forenses. E segunda etapa teve como objetivo, a aplicação de técnicas contida no contexto, comprovando através da teoria e de ferramentas o levantamento geral do trabalho, proporcionando dados comparativos e uma conclusão para obter-se um laudo gratificante sob o suposto crime concluído.

Para atingir os objetivos práticos deste trabalho foi usado um *Pen drive* de 4GB para análise forense e as ferramentas, Helix para sistema operacional UBUNTU, o Forensic Toolkit para sistema operacional WINDOWS e o OpenPuff para extração de dados em arquivos com esteganografia .

Os mesmos foram escolhidos por serem gratuitos e de fácil localização em sistemas de buscas. Abaixo informações sobre as ferramentas utilizadas no trabalho.

- Forensic Toolkit - FTK
 - ✓ Versão: 2.5.1
 - ✓ Licença: Free
 - ✓ Sistema Operacional compatível: WINDOWS

- Helix
 - ✓ Versão: 2009R1
 - ✓ Licença: Free
 - ✓ Sistema Operacional compatível: UBUNTU

- OpenPuff
 - ✓ Versão: v4.00
 - ✓ Licença: Free
 - ✓ Sistema Operacional compatível: WINDOWS

O desenvolvimento do tema ocorreu em um ambiente criado para fins forenses, utilizando um notebook com as seguintes configurações:

- Microsoft Windows 7 32-bits
- Intel Pentium Dual-Core CPU T4200 @2.00Ghz
- 3,00GB RAM
- Intel Semp Toshiba IS 1412 - 20ga & ICH9M Chipset

Para a realização dos testes no sistema operacional Linux, o mesmo foi virtualizado no ambiente Windows pelo *software* VirtualBox⁴ - v. 4.3.15 for Windows hosts, x86/amd64. O sistema Linux utilizado foi através do LiveCD (boot pelo CD) com uma distribuição Helix-2009.

Inicialmente foram feitas duas bases de testes com o *pen drive* formatado no modo FAT-32, por se tratar de uma partição convencional, pois nem todos os sistemas operacionais suportam os dois tipos de partição existentes (FAT-32 e NTFS). A partição NTFS, por exemplo, é reconhecida apenas pelo WinNT, Win2000, WinXP, Vista, Windows 7 e Windows Server (2003, 2008) - enquanto a partição FAT32 é reconhecida por todos sistemas operacionais, exceto o WinNT, deste modo tomou-se como escolha o modo de partição FAT-32, sendo da seguinte forma:

- 1 – Formatação rápida (FAT-32)
- 2 – Formatação completa (FAT-32)

Para realizar a montagem do objeto de pesquisa, foram inseridos arquivos com vários tipos de extensões dentro do *pen drive* e, em seguida, formatados no modo de formatação rápida e formatação completa. Com a finalidade de verificar se as ferramentas forenses conseguem visualizar ou até recuperar arquivos deletados.

Desse modo foram inseridos sete arquivos de acesso comum ao dia-a-dia de qualquer pessoa, com extensão do tipo png, jpg, jpeg, docx, pdf e avi, como mostra a figura 6 e em seguida esses arquivos foram deletados.

Figura 6 - Arquivos inseridos no *pen drive* antes da análise oficial

| Nome | Tipo |
|---|-----------------------------|
|  Crian_Imagem1 | Arquivo PNG |
|  Crian_Imagem2 | Arquivo JPG |
|  Imagem3 | Arquivo JPEG |
|  Texto_Teste 1 | Documento de Texto |
|  Texto_Teste 2 | Foxit Reader PDF Document |
|  TextoNumero1 | Documento do Microsoft Word |
|  Video1 | Videoclipe |

Fonte: Elaborado pela autora.

⁴ É um programa que cria máquinas virtuais, que utiliza um sistema operacional dentro de outro, maiores informações acesse o site: <https://www.virtualbox.org>

Com o *pen drive* vazio, os testes foram realizados em um *pen drive* (4Gb - *SanDisk*), contendo diferentes tipos de arquivos, sendo divididos nas seguintes categorias com suas devidas extensões.

Foram inseridos 25 arquivos com o tamanho total de 22,3 MB, para a análise forense como mostra abaixo:

- **Figuras;**
 - (3) três arquivos com extensão .bmp;
 - (3) três arquivos com extensão .png;
 - (3) três arquivos com extensão .jpeg;
 - (4) quatro arquivos com extensão .jpg;

- **Executável;**
 - (1) um arquivo com extensão .exe;

- **Texto;**
 - (1) um arquivo com extensão .docx;
 - (1) um arquivo com extensão .txt;
 - (1) um arquivo com extensão .pdf;
 - (1) um arquivo com extensão .ppt;
 - (1) um arquivo com extensão .xlsx;

- **Áudio;**
 - (1) um arquivo com extensão .wav;
 - (2) dois arquivos com extensão .mp3;

- **Vídeo;**
 - (1) um arquivo com extensão .3gp;
 - (1) um arquivo com extensão .avi;
 - (1) um arquivo com extensão .mp4;

A quantidade de arquivos utilizados descritos acima tem como base uma quantidade significativa para o desenvolvimento do trabalho.

Para todas as fases descritas (seção 4.3) foram utilizado o mesmo ambiente.

Para uma melhor análise de tempo na criação das imagens, foram feitos três testes a fim de medir a divergência de tempo que cada *software* leva para criar a mesma imagem.

Após a criação do ambiente foi dado início aos testes, de três maneiras diferentes utilizando dois tipos de ferramentas forenses;

1 - Realização da cópia e criação da imagem (.dd) com os arquivos inseridos no *pen drive* utilizando a ferramenta Helix e, em seguida, a execução das quatro fases existentes na perícia forense computacional (preservação, extração, análise e formalização).

2 - Realização da imagem (.dd) dos arquivos inseridos no *pen drive* utilizando o Forensic Toolkit (FTK) e em seguida, a execução novamente das quatro fases existentes na perícia forense computacional.

3 - Comparação das imagens criadas no modo (1 e 2), ou seja, abrir, ler e analisar a imagem do Helix no FTK e abrir, ler e analisar a imagem do FTK no Helix.

A escolha das ferramentas Helix, FTK e OpenPuff teve por finalidade comparar os resultados obtidos pelas mesmas e analisar qual a melhor em determinados quesitos de um perito forense computacional. Visto que o OpenPuff tem a função de analisar arquivos esteganografado no formato áudio e figuras, no qual foi utilizado no decorrer do trabalho. As ferramentas foram selecionadas por ser uma das mais conhecidas na área de forense.

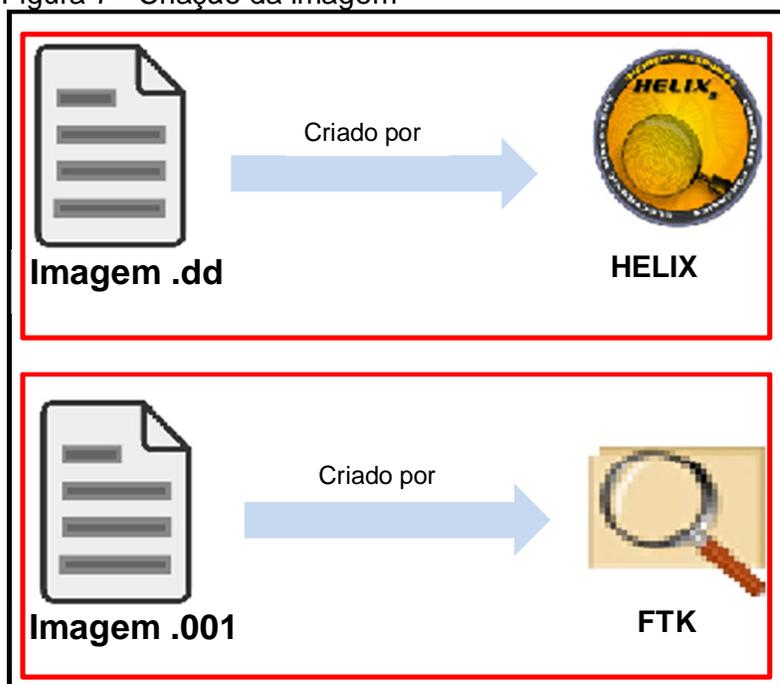
Para execução do objeto de pesquisa, abaixo mostra as divisões das fases forense da seguinte forma:

5.1 PRESERVAÇÃO

A preservação denomina realizar a duplicação de discos, ou seja, é feita uma cópia fiel dos dados encontrado no *pen drive*, também chamada fase de coleta como mostra a figura 3, sendo assim é gerada exatamente uma cópia dos arquivos contido no *pen drive* em um único arquivo de imagem com extensão *.dd*.

Deste modo para realização dos procedimentos nessa fase foram usados às ferramentas Helix (que gerou uma imagem do *pen drive* apreendido) e FTK (que gerou outra imagem do mesmo *pen drive*), como apresentado na figura 7.

Figura 7 - Criação da imagem



Fonte: Elaborado pela autora.

5.2 EXTRAÇÃO

A extração ou exame como mostra a figura 3, consiste na recuperação e organização das informações contidas nas cópias dos dados descritos na fase de preservação, ou seja, foi examinada a imagem (.dd) e a imagem (.001) mantendo o material original intacto.

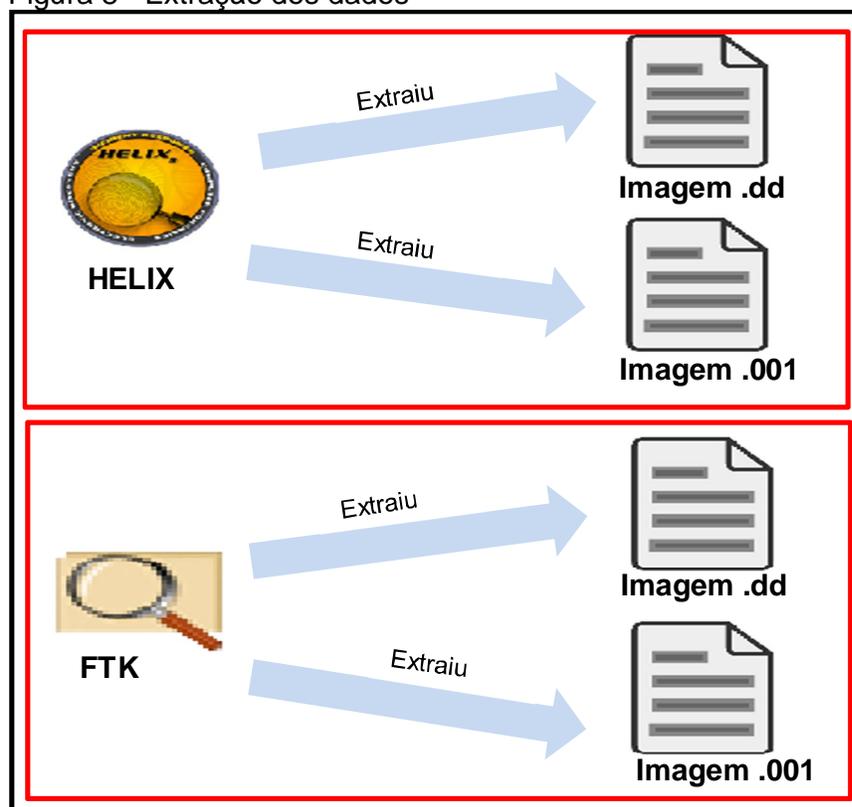
Assim, foram coletadas as informações das duas imagens geradas na fase anterior, sendo:

- 1) Imagem.dd – Utilizando a ferramenta Helix.
- 2) Imagem.001 – Utilizando o ferramenta FTK.

Deste modo, o Helix fez a leitura do arquivo por ele próprio gerado (imagem.dd) e a leitura da imagem criada pelo FTK (imagem.001).

E o FTK fez o mesmo procedimento, leu sua própria imagem (imagem.001) e a criada pelo Helix (imagem.dd) como mostra a figura 8.

Figura 8 - Extração dos dados



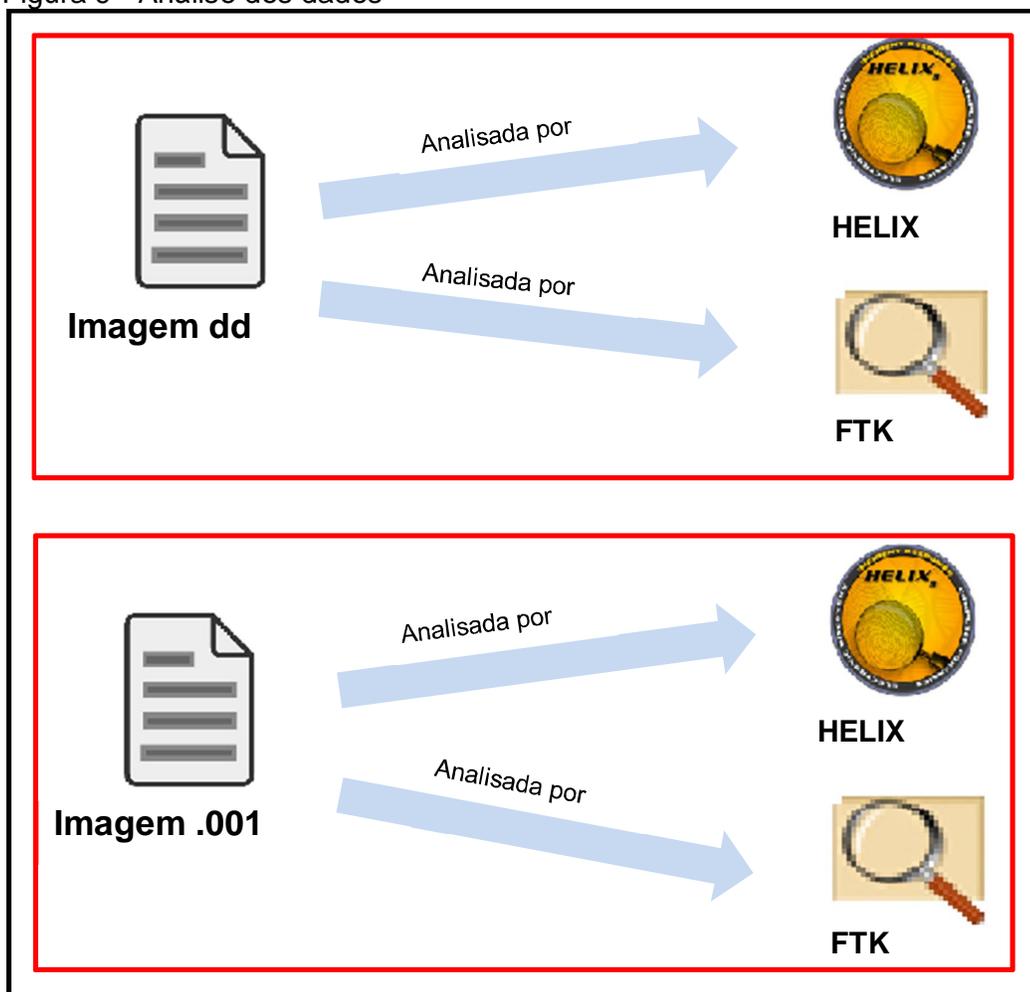
Fonte: Elaborado pela autora.

5.3 ANÁLISE DAS EVIDÊNCIAS

A fase de análise requer analisar as evidências e separar as informações relevantes, através de identificação e características que mostre relações com a área do crime, como pessoas, imagens, nomes, locais, horários, vídeos, ou seja, expor tudo que foi buscado na fase da extração.

Deste modo, como mostra a figura 9, cada imagem criada foi lida e analisada com as duas ferramentas, ou seja, a imagem.dd foi analisada pela ferramenta Helix e pelo FTK, e a imagem.001 foi analisada pelo FTK e pelo Helix.

Figura 9 - Análise dos dados



Fonte: Elaborado pela autora.

5.4 FORMALIZAÇÃO

Para descrever a fase da formalização, foi necessário utilizar os recursos disponíveis pelas ferramentas Helix e FTK, a fim de estruturar um laudo pericial.

O conteúdo que abrange o laudo pericial foi feito com base em análises de investigação, pois assim as informações relevantes comprovarão o real autor do crime.

Eleutério e Machado (2011) afirmam que a formalização é a elaboração do laudo pericial, onde o perito deve se atentar, pois o laudo é um documento técnico-científico e deve ser com objetividade e clareza os métodos e os exames realizados, para segurança e transparência do processo forense.

Deste modo, o laudo pericial tem uma estrutura própria, formada geralmente pelas seguintes seções:

- **Preambulo:** Identificação do laudo
- **Histórico:** Fatos de interesse ao laudo
- **Material:** Descrição detalhada do material examinado
- **Objetivo:** Objetivo do laudo
- **Considerações técnicas:** Conceitos e informações relacionadas ao exame pericial realizado, que podem ser importantes para o entendimento do laudo.
- **Exames:** Parte descritiva e experimental do laudo.
- **Conclusões:** Resumo objetivo dos resultados obtidos no exame.

Sendo assim, foi criado um laudo pericial (APÊNDICE B), abrangendo os tópicos acima citados com as devidas informações baseadas na análise das imagens realizadas em cada fase.

6 RESULTADOS

Após os testes realizados, obteve-se os resultados que serão descritos a seguir.

Utilizando a formatação completa, concluiu-se que os arquivos inseridos vistos na figura 6, foram completamente apagados do dispositivo após a formatação, não deixando vestígios de nenhum arquivo.

E utilizando a formatação rápida, pode-se concretizar que os mesmos arquivos deletados estavam visíveis no modo de análise do dispositivo.

Deste modo, o método de formatação rápida deixa vestígios de arquivos “deletados”. Abaixo, serão apresentados os resultados colhidos em cada fase forense.

6.1 PRESERVAÇÃO

6.1.1 Utilizando a ferramenta Helix

Utilizando o terminal da ferramenta Helix, foi possível levantar os primeiros dados relevantes da fase da preservação.

A figura 10 mostra os dados colhidos para essa fase sendo: Item 1: **/dev/sdb1** entrada que se encontra o dispositivo corresponde ao que acondicionou a cópia, com o nome do *pen drive* **/media/FORENSE** e o tamanho do dispositivo.

Figura 10 - Terminal do Ubuntu criando a imagem

```
ubuntu@ubuntu:~$ sudo -i
root@ubuntu:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           252M  18M  235M   7% /lib/modules/2.6.24-19-generic/volatile
varrun         252M  112K  252M   1% /var/run
varlock         252M     0  252M   0% /var/lock
devshm          252M   12K  252M   1% /dev/shm
gvfs-fuse-daemon 252M  5.8M  247M   3% /home/ubuntu/.gvfs
/dev/sdb1       3.8G   23M   3.8G   1% /media/FORENSE
/dev/sdc1       7.5G   4.0K   7.5G   1% /media/LU
root@ubuntu:~# cd /home
root@ubuntu:/home# cd ubuntu
root@ubuntu:/home/ubuntu# dc3dd if=/dev/sdb1 of=/home/forensehelic.dd progress=on hash=md5 log=forensehelic.log conv=noerror
```

Fonte: Elaborado pela autora.

Já o item 2: representa a linha de comando que gerou a cópia de todos os dados existente no *pen drive* e criou a imagem forense.

Sendo: **“dc3dd if=/dev/sd1 of=home/forenseheliX.dd progress=on hash=md5 log=forenseheliX.log conv=noerror”**

Abaixo estão as informações sobre os comandos utilizados no UBUNTU para criação da imagem.

- ✓ dc3dd - Cópia exata de um intervalo de dados
- ✓ /dev/sd1 - Diretório dos arquivos de dispositivos do sistema
- ✓ If - Define o endereço da entrada /
- ✓ of - Define o endereço da saída.
- ✓ progress - Mostra o progresso na tela
- ✓ hash - Calcula o hash da origem
- ✓ log - Gera arquivo de log com etapas do procedimento.
- ✓ conv - Ignora blocos defeituosos
- ✓ df-h - Verifica os discos conectados

Visto que antes de confirmar o comando deve-se garantir que o campo **if** aponta para o disco que será copiado (disco original), enquanto o campo **of** aponta para o disco que acondicionará a cópia.

O *pen drive* localizado na entrada **/dev/sd1** foi copiado para um único arquivo chamado forenseheliX.dd, junto com um log⁵, chamado forenseheliX.log , deste modo, deu-se início a cópia dos arquivos.

Figura 11 - Terminal do Ubuntu copiando os dados do dispositivo

```

root@ubuntu:/home/ubuntu# dc3dd if=/dev/sdb1 of=/home/forenseheliX.dd progress=on
n hash=md5 log=forenseheliX.log conv=noerror
257736704 bytes (246 M) copied, 286.591 s, 878 K/s
dc3dd: writing to '/home/forenseheliX.dd': No space left on device
503393+0 records in
503392+0 records out
257736704 bytes (246 M) copied, 286.628 s, 878 K/s
root@ubuntu:/home/ubuntu# cat /home/* | md5deep -e
stdin: 236MB done. Unable to estimate remaining time.
me/ubuntu: Is a directory
0b5cab2b156dd472306636472f769128
  
```

Fonte: Elaborado pela autora.

A figura 11 - item 1, mostra a quantidade de bits copiados (1 à 1), pois dessa forma comprova que todos os dados estão sendo copiados fielmente, seguidos do tamanho do arquivo copiado (246 M) e o tempo que foi calculado para copiar os bits 286.591 s, 878 K/s.

⁵ Arquivo que contém as informações realizadas da imagem

Já a figura 11 - item 2, mostra como foi feito a geração da hash⁶, visto que o usuário precisa estar dentro do diretório que se encontra o arquivo forensehelix.dd (figura 10 - item 2), sendo **/home/ubuntu** para dessa forma executar o comando **cat /<caminho_da_imagem> /* | md5deep -e**.

Comando esse que calcula a hash da imagem, ou seja, o parâmetro hash é calculado no hashcode do disco original e compara a veracidade da cópia feita.

Abaixo, são exibido detalhes dos comandos usados, e se caso for os mesmos arquivos copiados, assim é gerada a MD5⁷.

- ✓ **cat** - Exibe o conteúdo do arquivo na tela de forma contínua.
- ✓ **/<caminho_da_imagem> /*** - Caminho da imagem gerada
- ✓ **md5deep** - Calcula e compara a MD5
- ✓ **-e** - Mostra um indicador de progresso e estimativa do tempo restante do arquivo.

A figura 11 - item 3, mostra a MD5 do arquivo já criado chamado de forensehelix.dd, para garantir a integridade dos dados.

Sendo que a imagem forensehelix.dd criada servirá para análise forense em tópicos abaixo.

Deste modo a primeira fase utilizando a ferramenta Helix foi concluída.

⁶ Linha de código que garante a integridade dos dados copiados

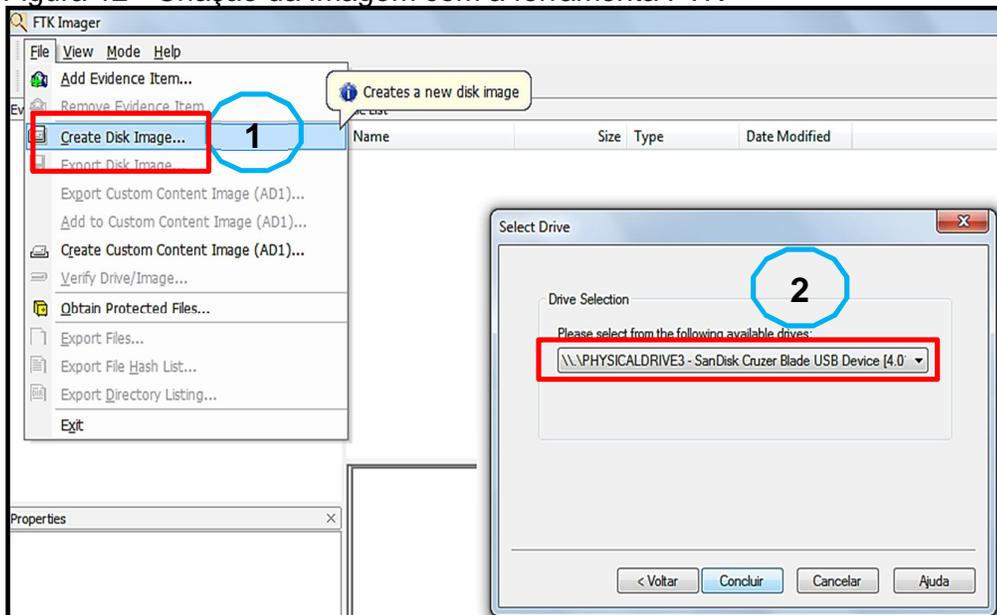
⁷ Esquema de encriptação de dados, que transforma dados em um código.

6.1.2 Utilizando a ferramenta FTK

A ferramenta FTK utilizada na plataforma WINDOWS, realizou o mesmo procedimento que a ferramenta Helix, criou uma imagem idêntica do dispositivo.

A figura 12 - Item 1, mostra a criação da imagem e o item 2, exemplifica a escolha da entrada do dispositivo

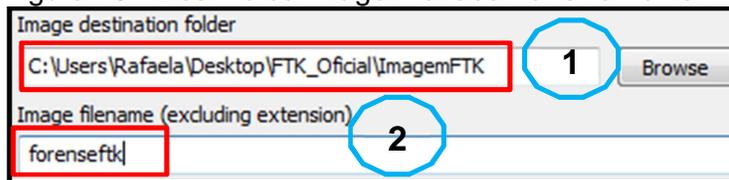
Figura 12 - Criação da Imagem com a ferramenta FTK



Fonte: Elaborado pela autora.

Após escolher o caminho da imagem, foi feita a escolha do tipo de extensão da mesma, visto que o trabalho busca comparar as imagens criadas, deste modo foi usada à mesma extensão da ferramenta Helix, ou seja, extensão.dd.

Figura 13 - Destino da imagem criada na ferramenta FTK

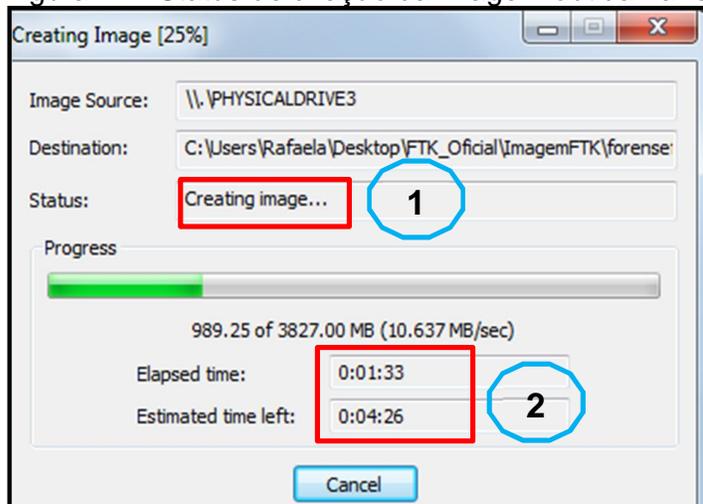


Fonte: Elaborado pela autora.

A figura 13 - item 1, mostra o destino da imagem criada e o item 2, o nome da imagem criada forensftk, lembrando que a imagem oficialmente analisada no decorrer do trabalho é chamada "forensftk.001" devido a outras criações de

imagem feitas com o mesmo nome como “forenseftk.002”, “forenseftk.003” porém com locações vazia ou seja não existe arquivos dentro para ser analisado.

Figura 14 - Status de criação da imagem obtida na ferramenta FTK



Fonte: Elaborado pela autora.

A figura 14 - item 1, representa o status da criação da imagem. Passo importante a ser observado, seguido da quantidade de arquivos, o tempo decorrido e o tempo estimado para a conclusão da cópia como mostra a figura 14 - item 2.

Figura 15 - Informações obtida da imagem com a ferramenta FTK

| General | |
|---------------|---|
| Name | forenseftk.001 (circled in red and labeled '1') |
| Sector count | 7837696 |
| MD5 Hash | |
| Computed hash | ec912fcc6c79d07b3f2cab7afc40c63e (circled in red and labeled '2') |
| Report Hash | ec912fcc6c79d07b3f2cab7afc40c63e |
| Verify result | Match |
| SHA1 Hash | |
| Computed hash | 1a9d9c41c681a91afd1d8e4296294ea00ac66b44 |
| Report Hash | 1a9d9c41c681a91afd1d8e4296294ea00ac66b44 |
| Verify result | Match |

Fonte: Elaborado pela autora.

A figura 15 - item 1, mostra o nome da imagem criada “forenseftk.001” sendo a extensão “.001” correspondente a extensão “.dd”. E o item 2, mostra o código da MD5 dos dados copiados: “ec912fcc6c79d07b3f2cab7afc40c63e”

Deste modo a fase da preservação foi finalizada, as cópias dos dados foram feitas e o material original pode ser apreendido e guardado até a resolução do laudo.

6.2 EXTRAÇÃO

6.2.1 Utilizando a ferramenta Helix

Após a criação da “forensehelix.dd” foi extraído as informações da imagem, para isso utilizou-se a ferramenta disponível no próprio Helix, chamada AutoPsy, que consiste em analisar imagens para fins forense. Como mostra a figura 16.

Figura 16 - Tela inicial do AutoPsy para criação do caso a ser investigado

Fonte: Elaborado pela autora.

A tela principal do AutoPsy vista na figura 16, tem a finalidade de analisar a imagem forense, para isso é preciso criar o caso a ser investigado, como mostra o item 1: Nome do caso investigado; Item 2: Descrição do caso e o item 3: Nomes dos peritos envolvidos no caso.

Figura 17 - Caminho da imagem criada com a ferramenta Helix

Fonte: Elaborado pela autora.

A figura 17 - item 1: mostra o caminho da imagem para a extração dos dados; Item 2: mostra o tipo do disco a ser analisado e o item 3: mostra os métodos que podem ser importados a imagem.

Figura 18 - Confirmação da imagem criada no Helix



Fonte: Elaborado pela autora.

A figura 18 mostra a imagem selecionada para serem extraídas as informações.

Figura 19 - Busca por palavra chave na ferramenta Helix

| KEYWORD SEARCH | FILE TYPE | IMAGE DETAILS | META DATA | DATA UNIT | HELP | CL |
|--------------------------------|------------------------------|------------------------------|------------------------------|-----------|------|----|
| 1 | 2 | 3 | 4 | 5 | | |
| NAME | WRITTEN | ACCESSED | CREATED | SIZE | | |
| \$FAT1 | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 3909120 | | |
| \$FAT2 | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 3909120 | | |
| \$MBR | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 512 | | |
| \$OrphanFiles/ | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0 | | |
| Color.jpg | 2014-09-06 12:59:44 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 950013 | | |
| Crianca1.bmp | 2014-09-06 | 2014-09-06 | 2014-09-06 | 6334 | | |

Fonte: Elaborado pela autora.

A figura 19, mostra todos os arquivos contidos dentro da pasta “Busca por palavra chave”, da imagem forensehelix.dd;

Item 1 - *Name*: o nome do arquivo

- ✓ *\$fat* - sistema de ficheiros
- ✓ *\$OrphanFiles* – arquivos deletados

Item 2 - *Written*: a data que o arquivo foi escrito.

Item 3 - *Accessed*: a data que o arquivo foi acessado.

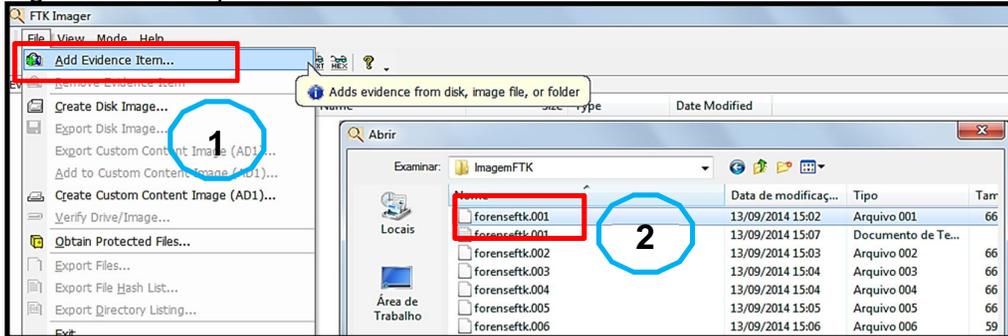
Item 4 - *Created*: a data que o arquivo foi criado.

Item 5 - *Size*: tamanho dos arquivos.

6.2.2 Utilizando a ferramenta FTK

Utilizando a ferramenta FTK, com sua imagem criada forenseftk.001, foi preciso criar uma evidência para serem extraídas as informações figura 20 - item 1.

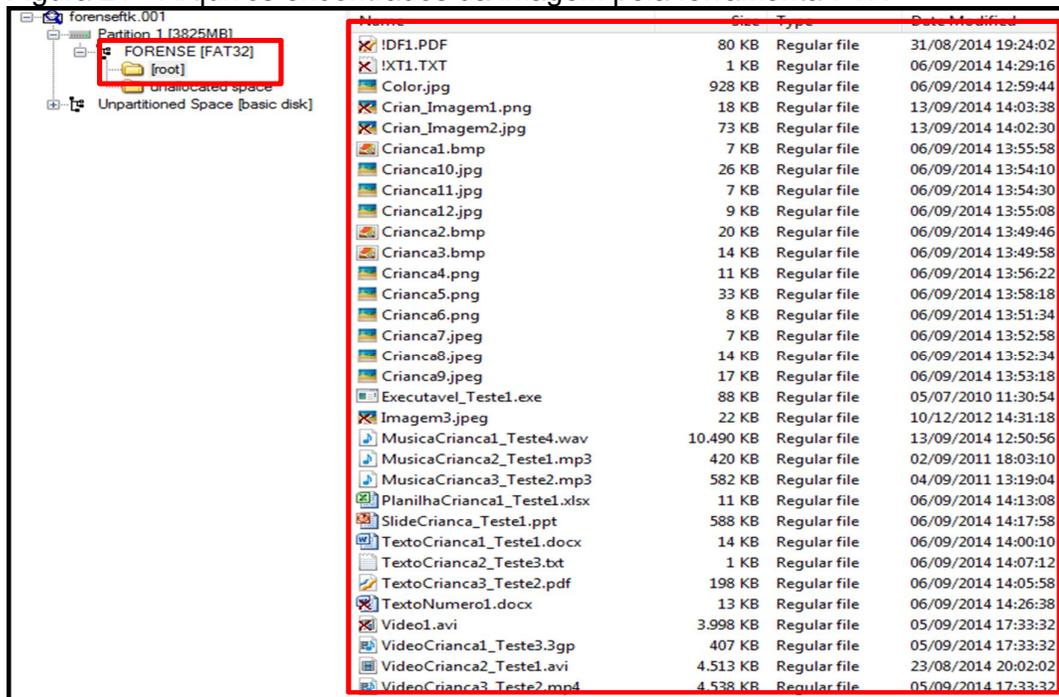
Figura 20 - Criação da evidência com a ferramenta FTK



Fonte: Elaborado pela autora.

Depois de criar a evidência, foi preciso direcionar o caminho da imagem lembrando que o arquivo correto é “.001”, visto na figura 20 - item 2.

Figura 21 - Arquivos encontrados da imagem pela ferramenta FTK



Fonte: Elaborado pela autora.

A figura 21, mostra os arquivos a serem analisados encontrados dentro da imagem criada forenseftk.001, onde contém informações que o perito precisa examinar como nome do arquivo, extensão, hora, data e tamanho do arquivo.

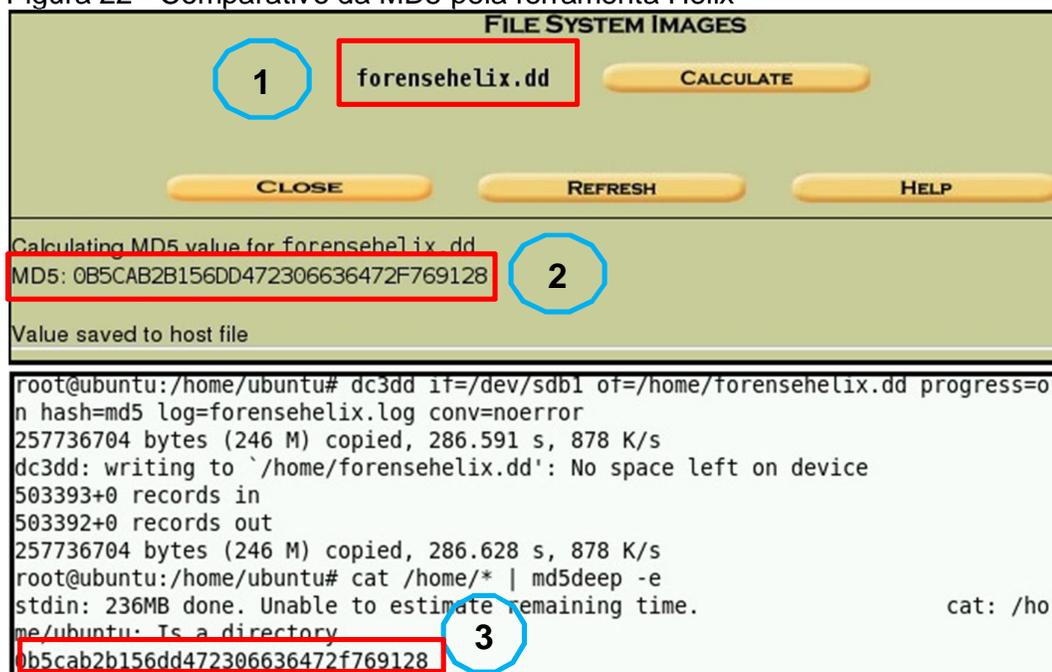
6.3 ANÁLISE DAS EVIDÊNCIAS

6.3.1 Utilizando a ferramenta Helix

Utilizando a ferramenta AutoPsy com a imagem criada forenseheliX.001, todos os passos seguintes foram analisados por essa imagem.

O primeiro tópico a ser processado foi a validação da imagem investigada, para isso obteve-se a comparação das MD5 para exemplificar a veracidade das evidências coletadas, a fim de analisar se são as mesmas cópias feitas na fase de preservação utilizando a ferramenta Helix, como mostra a figura 22.

Figura 22 - Comparativo da MD5 pela ferramenta Helix



Fonte: Elaborado pela autora.

O item 1: Mostra o nome da imagem analisada; item 2: mostra o código da MD5; e o item 3: é o comparativo da MD5 do item 2, para verificar se não existe a possibilidade de fraude ou de alterações no material coletado.

Note que o código da MD5 do item 1, é o mesmo código da criação da imagem forenseheliX.dd exibido na figura 11 - item 3.

Deste modo, ficou válido o código da MD5 e comprova que não houve alteração alguma na imagem. A partir desse tópico importante encontrado, pode-se dar continuidade a análise da imagem.

Figura 23 - Resultado na busca do nome do dispositivo com a ferramenta Helix

| Type | NAME | WRITTEN | ACCESSED | CREATED | SIZE |
|--------|---------|------------------------------|------------------------------|------------------------------|------|
| dir/in | FORENSE | 2014-09-06 15:28:56 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0 |

Fonte: Elaborado pela autora.

A figura 23 - item 1, mostra o nome do *pen drive* copiado na fase de preservação descrito na figura 10 - item 1. E o item 2 da figura 23, comprova o mesmo nome do dispositivo, encontrado na análise do *pen drive*.

Deste modo, foi encontrada uma prova coerente e correta pelo perito.

A figura 24 abaixo, deixou claro a análise da imagem forensehelix.dd com um arquivo deletado encontrado dentro da pasta "\$OrphanFiles", representado com um dos nomes visto na figura 6.

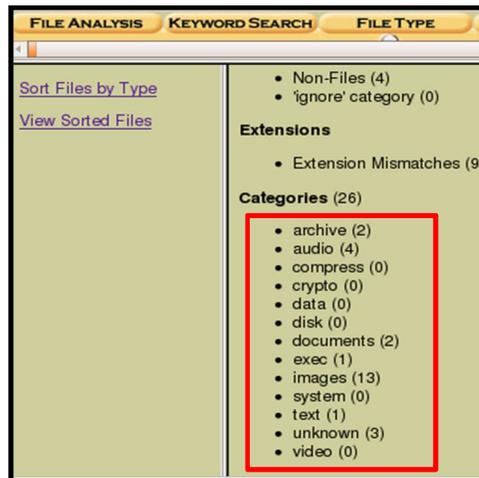
Deste modo, conclui que os arquivos deletados foram encontrados na imagem forense utilizando o Helix, arquivos esses que não podem ser recuperados e nem visualizados, pois é preciso outro tipo de ferramenta além do AutoPsy, visto que a função principal da ferramenta é de apenas mostrar o nome dos arquivos deletados, como mostra a figura 24.

Figura 24 - Arquivos deletados encontrados na ferramenta Helix



Fonte: Elaborado pela autora.

Figura 25 - Categoria de arquivos encontrados com ferramenta Helix



Fonte: Elaborado pela autora.

A figura 25 mostra, o resultado da análise feita sobre a imagem forensehelix.dd, contendo as categorias de arquivos;

Figura 26 - Relatório das MD5 criado na ferramenta Helix

```

MDS Values for files in C:/ (forensehelix.dd-0-0)
FORENSE      (Volume Label Entry)
995669292cd30b990e27f32454307bfd - Color.jpg
94294266efc9f10cd399c54d9c6c6965 - Crianca1.bmp
a5b461b6f0481ea9c0509ab285a8ef62 - Crianca2.bmp
1d28906563d4c19fd47ec3b89447aa94 - Crianca3.bmp
67b562b4d94b664f612b8994d35f58b1 - Crianca4.png
ac5cec107e182c9b8af3276bb4d8f281 - Crianca5.png
1af220ba16d5565c762d942744c850e9 - Crianca6.png
b087eaff85befa723dc31fcc6bad71bc - Crianca7.jpeg
47b70157300b64a8f2621e8f0249cce - Crianca8.jpeg
4231df773f6ad0742cea3dff08c7feac - Crianca9.jpeg
400ac588b11fd6a66b5ad766df93fd3f - Crianca10.jpg
3e57c01d52a178fb621429133437a5c9 - Crianca11.jpg
23f2727b3a45b8a26cdebc5bbebfd271 - Crianca12.jpg
e69624ef8bb880ba6eff3871e044cac0 - Executavel_Testel.exe
1b6d4597c85e526f21b869a5e53893f5 - MusicaCrianca1_Testel4.wav
3fffcad2d3940f9415f4bed30e8f7df72 - MusicaCrianca2_Testel.mp3
2e028cf85da0e0feddbfdb9c465061b0 - MusicaCrianca3_Testel2.mp3
85d52febbf97dd63e8da25e2dfe5fbef - PlanilhaCrianca1_Testel.xlsx
da0399ed1e395982dbc3307414bb2c50 - SlideCrianca_Testel.ppt
af11dd5f138f3c469140102f311e60a1 - TextoCrianca1_Testel.docx
05dd222e1b2c610551d0175aa55c08e7 - TextoCrianca2_Testel3.txt
1b2ad27f985bf95ea4e5b1be8f2ec7e9 - TextoCrianca3_Testel2.pdf
42c3f8b5d1d6f592c60109293379b527 - VideoCrianca1_Testel3.3gp
44b33be5f2d8814074973216a5a55477 - VideoCrianca2_Testel1.avi
5998c043dced50dabf39a89402736213 - VideoCrianca3_Testel2.mp4

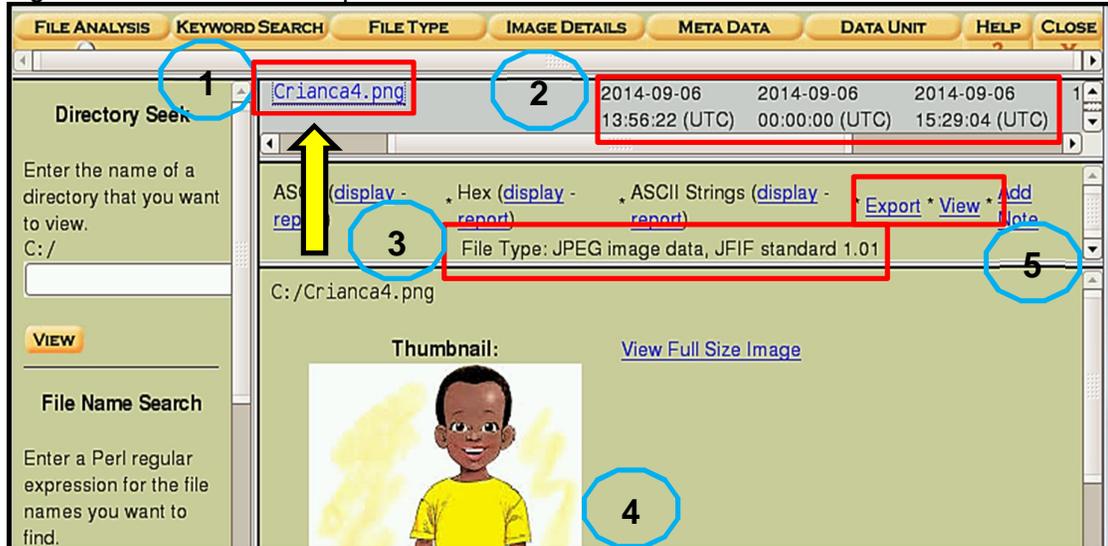
```

Fonte: Elaborado pela autora.

A figura 26, resulta em um relatório gerado pela própria ferramenta Helix, que contém todos os arquivos que estão dentro na imagem forensehelix.dd, seguidas de suas respectivas MD5, comprovando a integridade de cada arquivo através do seu próprio código.

A figura 27 abaixo mostrou como é o processo da análise de um arquivo comum de uma figura a ser analisada.

Figura 27 - Análise de arquivo na ferramenta Helix.



Fonte: Elaborado pela autora.

A figura 27 mostra a principal tela do AutoPsy na fase de análise, onde conteve várias informações importantes para a investigação sendo: Item 1: Nome do arquivo investigado e a extensão; Item 2: Data da figura, data que foi acessada, data que foi criada; Item 3: Tipo do arquivo; Item 4: O Arquivo analisado; Item 5: Local para o perito salvar o arquivo;

A figura 28 mostra um arquivo chamado “Color.jpg”, no qual foi feita a análise em vários tópicos. Arquivo esse que contém uma esteganografia, ou seja, arquivos ocultos dentro de outro arquivo.

Figura 28 - Resultado da análise de esteganografia na ferramenta Helix.



Fonte: Elaborado pela autora.

Através da análise no modo hexadecimal foi possível comprovar a existência da esteganografia citada, para isso foi preciso abrir uma nova aba no AutoPsy para obter uma análise mais precisa do arquivo, como mostra a figura 29.

Figura 29 - Análise hexadecimal no Helix com arquivo esteganografado.

```

GENERAL INFORMATION
1
File: C://Color.jpg 2
MD5 of file: 995669292cd30b990e27f32454307bfd
SHA-1 of file: b8413e6731cc1f5e52c526bf35f8e1eccc876bb5

Image: '/var/lib/autopsy/Pedofilia/maquina_02/images/forensehelix.dd' 3
Offset: Full image
File System Type: fat32

Date Generated: Sun Sep 7 23:01:27 2014
Investigator: PeritoForense2088 4

```

Fonte: Elaborado pela autora.

Deste modo, na aba de análise hexadecimal é possível notar algumas informações do arquivo, como mostra a figura 29.

O item 1: Nome do arquivo analisado; Item 2: Código da MD5 desse arquivo (comparando o mesmo código da MD5 vista na figura 26); Item 3: Caminho da imagem (NomeCaso/NomeMaquina/Análise/NomeImagem) como visto na figura 16; Item 4: Nome do perito que está analisando o caso.

Figura 30 - Informações obtidas do arquivo com esteganografia.

```

18240 18241 18242 18243 18244 18245 18246 18247
File Type: JPEG image data, JFIF standard 1.02
-----
CONTENT
00000000: FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 00 64 .....JFIF.....d

```

Fonte: Elaborado pela autora.

Ainda na análise hexadecimal do arquivo “Color.jpg”, note que o arquivo contém um tipo JFIF⁸, como mostra a figura 30. E deste modo fica nítido que existe um arquivo dentro de outro arquivo, uma vez que a sequencia de hífen implica a presença de outros arquivos, porem só foi possível verificar o que contém dentro dessa esteganografia nos tópicos abaixo.

⁸ Extensão associada e complementar de JPEG

Figura 31 - Arquivo encontrado dentro do arquivo com esteganografia.

```

000CEE00: 0000 D033 0000 02A0 4761 3083 6626 451D ...3...Ga0.T&E.
000CEE10: 330D 0020 0000 0043 6F6E 7461 746F 732E 3.. ...Contatos.
000CEE20: 646F 6378 00B0 8650 9214 1D0C D14C D155 docx...P....L.U
000CEE30: 5C11 0196 106B 1285 811A BCD6 0569 26AF

```

Fonte: Elaborado pela autora.

Ainda na análise hexadecimal do arquivo “Color.jpg”, como mostra a figura 31, existe uma evidência encontrada, um arquivo chamado “Contatos.docx.”, comprovando a existência de esteganografia dentro do arquivo, sendo as demais informações em hexadecimal desnecessária para análise.

Figura 32 - Imagem encontrada dentro do arquivo com esteganografia.

```

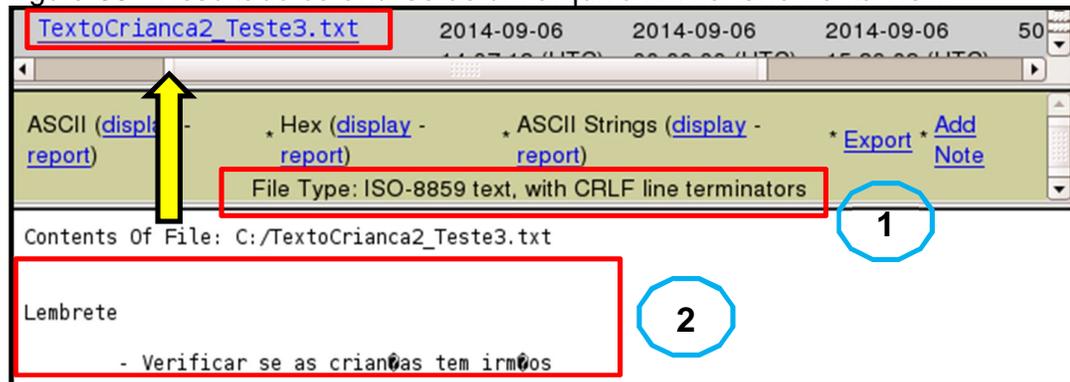
000D1720: 5F28 6526 451D 3314 0020 0000 004E 6F6D (e&E.3...Nom
000D1730: 6554 6573 7465 4372 6961 6E63 612E 6A70 eTesteCrianca.jp
000D1740: 6700 F047 6772 1619 5115 089D D599 D161 g Ggr 0...a

```

Fonte: Elaborado pela autora.

Ainda na análise hexadecimal do arquivo “Color.jpg”, a figura 32 comprova outra evidência encontrada, pois foi localizado uma figura com o nome de “NomeTesteCrianca.jpg”, ou seja existe uma figura dentro da figura “Color.jpg”.

Figura 33 - Resultado da análise de um arquivo .txt na ferramenta Helix



Fonte: Elaborado pela autora.

A figura 33 acima, mostra a análise de um arquivo com formato “.txt”, encontrado uma evidência no corpo do texto.

A figura 34 abaixo, mostra a análise hexadecimal de um arquivo com formato “.ppt”, onde foi localizada uma nova evidência dentro do arquivo.

Figura 34 - Dado encontrado na análise hexadecimal de um arquivo .ppt

```

0007E370: 0F10 0000 0050 6F72 7175 6520 4372 6961 ....Porque Cria
0007E380: 6EE7 6173 3F00 00A1 0F1C 0000 0011 0000 n.as?.....

```

Fonte: Elaborado pela autora.

A figura 35 abaixo, mostra a análise hexadecimal de um arquivo com formato “.wav”, com a MD5, o caminho da imagem e o nome do perito responsável do caso.

Figura 35 - Informações do áudio com esteganografia na ferramenta Helix.

```
File: C://MusicaCrianca1 Teste4.wav
MD5 of file: 4c775aa46b7175ded84f47957d6fb48f -
SHA-1 of file: 139acd690da1c489839424f3a29613b898ea7df8 -

Image: '/var/lib/autopsy/Pedofilia/maquina_02/images/forensehelix.dd'
Offset: Full image
File System Type: fat32

Date Generated: Sun Sep 7 17:00:54 2014
Investigator: PeritoForense2088
```

Fonte: Elaborado pela autora.

Após analisar o arquivo “.wav”, foi encontrada uma esteganografia na evidência como mostra a figura 36 , sendo um áudio com tipo RIFF⁹, visto que uma vez que a sequência de hífen implica a presença de outros arquivos dentro do analisado, comprovando, assim, a existência de esteganografia dentro do arquivo.

Ainda na análise do arquivo “.wav”, foi encontrada outra evidência. O nome do áudio antes de ser renomeada, como mostra a figura 36.

Figura 36 - Resultados na ferramenta Helix do áudio com esteganografia.

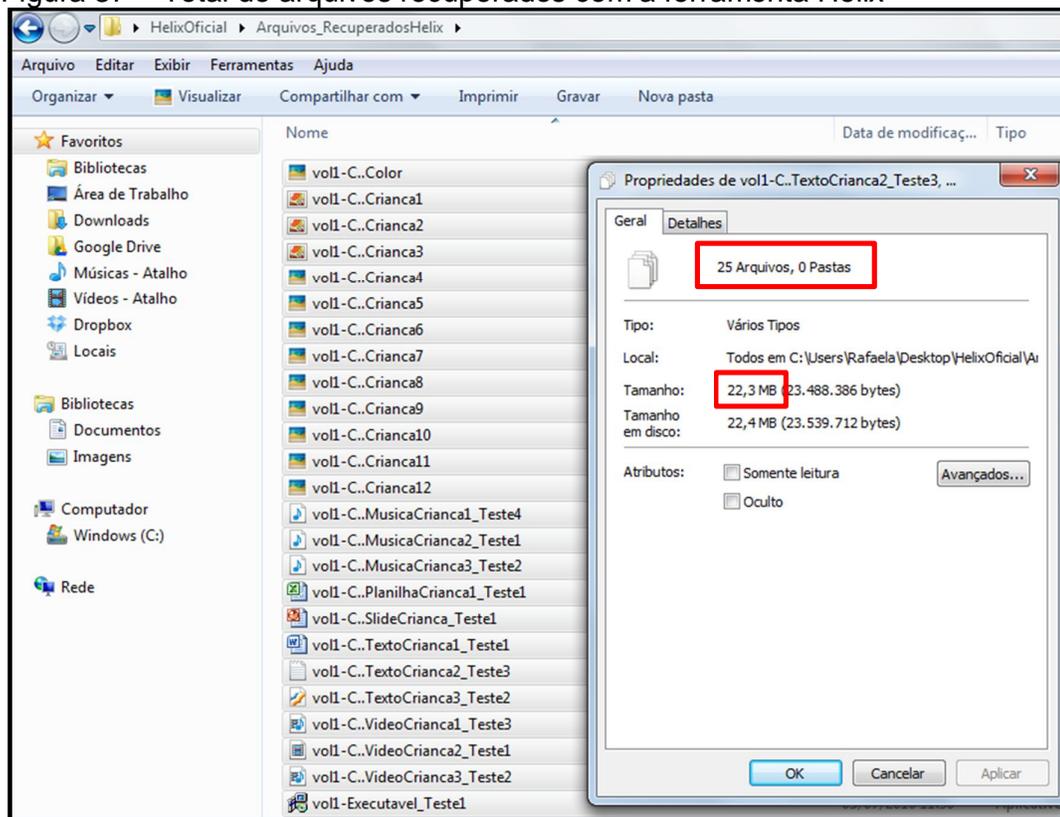
```
22712 22713 22714 22715 22716 22717 22718 22719
File Type: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz
-----
CONTENTS
00000000: 5249 4646 826F 3100 5741 5645 666D 7420 RIFF.o1.WAVEfmt
00000010: 1200 0000 0100 0200 44AC 0000 10B1 0200 .....D.....
00000020: 0400 1000 0000 4C49 5354 9800 0000 494E .....LIST....IN
00000030: 464F 4941 5254 0C00 0000 4C69 6E6B 696E FOIART...Linkin
00000040: 2050 6172 6B00 4943 5244 0B00 0000 3230 Park.ICRD...20
00000050: 3130 2D30 392D 3134 0000 4947 4E52 0500 10-09-14..IGNR..
```

Fonte: Elaborado pela autora.

Após a análise da imagem forensehelix.dd, a figura 37, mostra os arquivos salvos e recuperados. Totalizando 25 arquivos recuperados e mantidos em plataforma WINDOWS para maior facilitação e conclusões finais das análises.

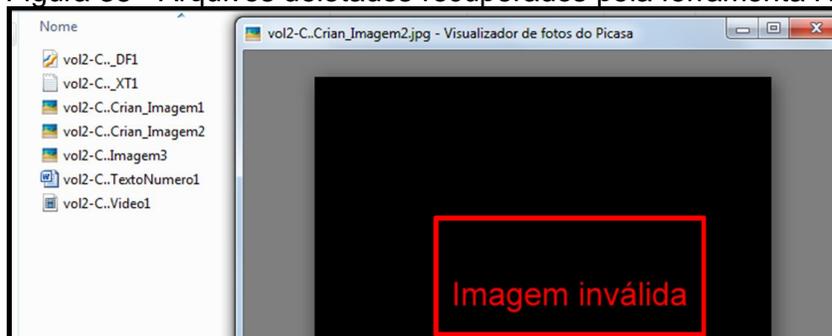
⁹ Extensão de compartilhamento de áudio

Figura 37 - Total de arquivos recuperados com a ferramenta Helix



Fonte: Elaborado pela autora.

Figura 38 - Arquivos deletados recuperados pela ferramenta Helix



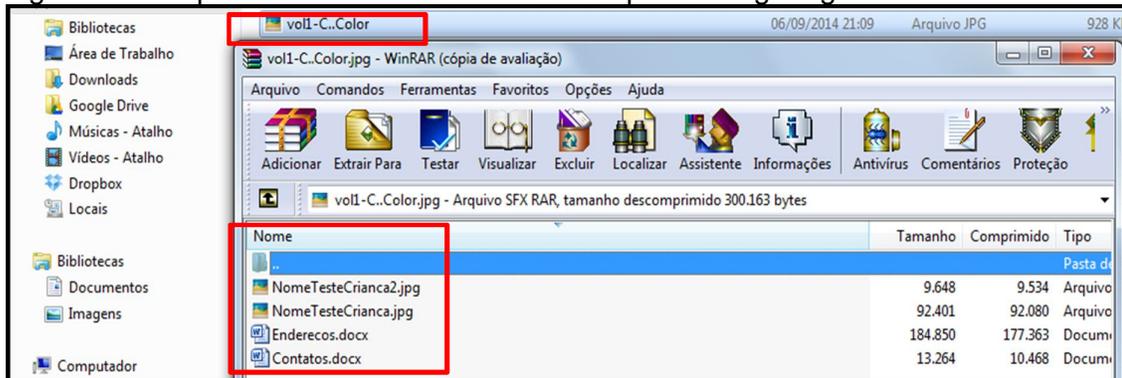
Fonte: Elaborado pela autora.

A figura 38, mostra os arquivos recuperados da imagemforensehelix.dd contidas na pasta “\$orphan file” (arquivos deletados), ou seja, são os mesmos arquivos vistos na figura 6, comprovando que a formatação rápida, deixou vestígios de arquivos deletados do dispositivo. Porém os arquivos recuperados não podem ser abertos e nem visíveis, pois o trabalho busca apenas analisar as imagens forenses.

Após localizar os arquivos com esteganografia sendo, “Color.jpg” e o áudio “.wav”, foi preciso verificar o que contém dentro desses arquivos.

O primeiro a ser analisado foi o “Color.jpg”, visto na figura 30, para recuperar esse arquivo foi utilizado o método de extração, como mostra a figura 39.

Figura 39 - Arquivos encontrados dentro do arquivo esteganografado

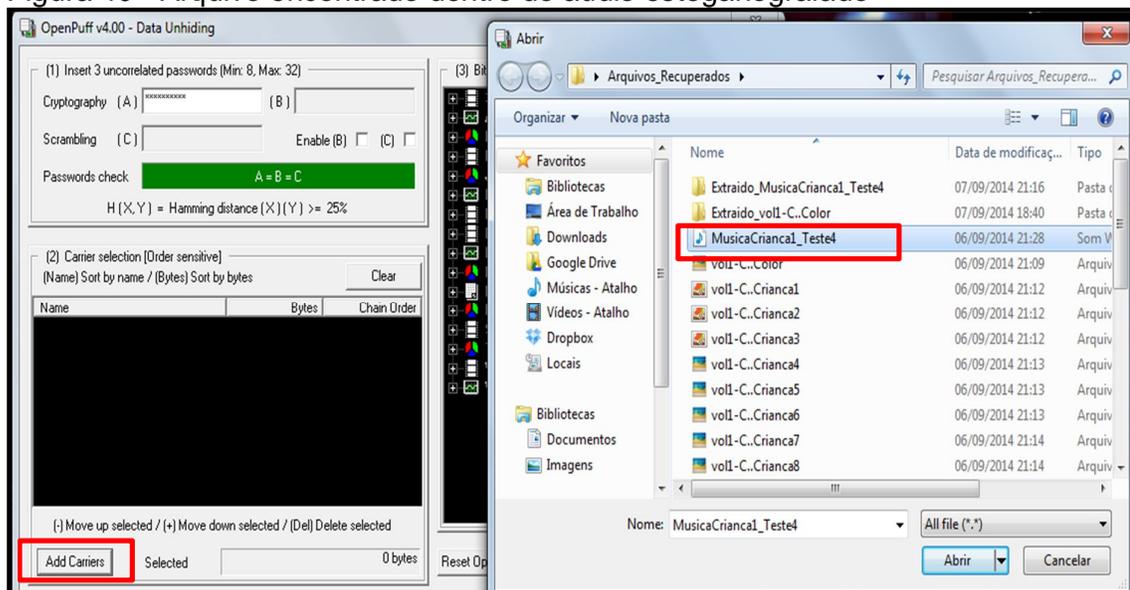


Fonte: Elaborado pela autora.

Deste modo utilizando o método de extração, pode-se ver quatros arquivos encontrados dentro do arquivo “Color.jpg”, as mesmas evidências encontradas nas figura 32 e figura 31.

E para analisar o áudio “. wav”, foi preciso usar o *software* OpenPuff, como visto na figura 40.

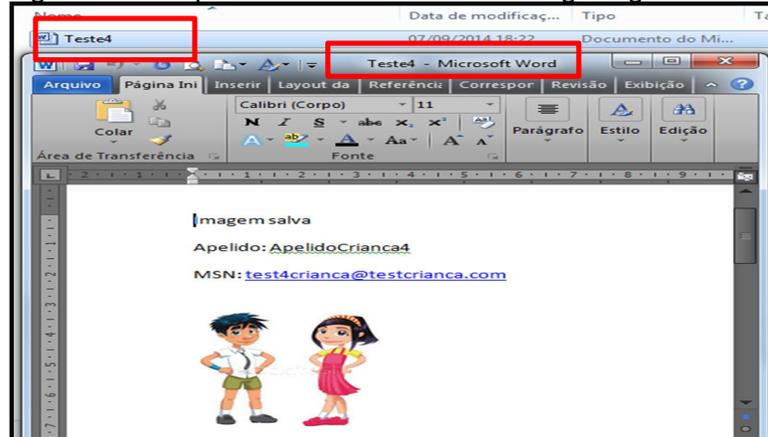
Figura 40 - Arquivo encontrado dentro do audio esteganografado



Fonte: Elaborado pela autora.

Após aberta a ferramenta OpenPuff, o próprio *software* gerenciou o destino do arquivo contido dentro do áudio “.wav”, e após escolher o destino basta abrir o arquivo e concluir a análise, como mostra a figura 41.

Figura 41 - arquivo contido dentro da esteganografia aberto



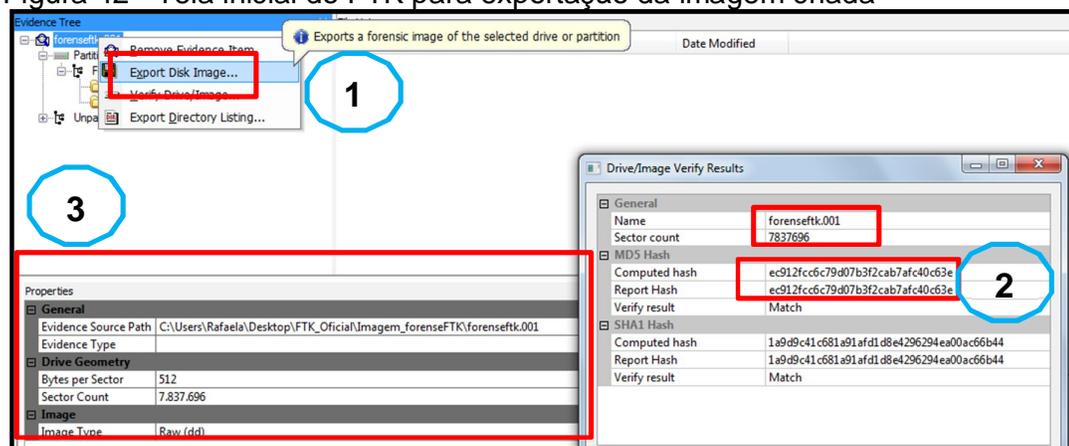
Fonte: Elaborado pela autora.

6.3.2 Utilizando a ferramenta FKT

Após extrair as informações da imagem forensftk.001, visto na fase de extração figura 21, foi feita a análise das evidências utilizando a ferramenta FTK.

Inicialmente precisou verificar a veracidade da imagem analisada vista na figura 42, para deste modo ser comprovado que nenhum dado foi modificado e comparar o código da MD5 com o mesmo proposito, como mostra a figura 15.

Figura 42 - Tela inicial do FTK para exportação da imagem criada



Fonte: Elaborado pela autora.

A figura 42 mostra a tela inicial do FTK pronto para iniciar a análise da imagem, para isso algumas informações são importantes, como:

Figura 44 - Arquivos encontrados dentro da imagem pela ferramenta FTK

| Name | Size | Type | Date Modified |
|------------------------------|-----------|--------------|---------------------|
| !DF1.PDF | 80 KB | Regular file | 31/08/2014 19:24:02 |
| !XT1.TXT | 1 KB | Regular file | 06/09/2014 14:29:16 |
| Color.jpg | 928 KB | Regular file | 06/09/2014 12:59:44 |
| Crian_Imagem1.png | 18 KB | Regular file | 13/09/2014 14:03:38 |
| Crian_Imagem2.jpg | 73 KB | Regular file | 13/09/2014 14:02:30 |
| Crianca1.bmp | 7 KB | Regular file | 06/09/2014 13:55:58 |
| Crianca10.jpg | 26 KB | Regular file | 06/09/2014 13:54:10 |
| Crianca11.jpg | 7 KB | Regular file | 06/09/2014 13:54:30 |
| Crianca12.jpg | 9 KB | Regular file | 06/09/2014 13:55:08 |
| Crianca2.bmp | 20 KB | Regular file | 06/09/2014 13:49:46 |
| Crianca3.bmp | 14 KB | Regular file | 06/09/2014 13:49:58 |
| Crianca4.png | 11 KB | Regular file | 06/09/2014 13:56:22 |
| Crianca5.png | 33 KB | Regular file | 06/09/2014 13:58:18 |
| Crianca6.png | 8 KB | Regular file | 06/09/2014 13:51:34 |
| Crianca7.jpeg | 7 KB | Regular file | 06/09/2014 13:52:58 |
| Crianca8.jpeg | 14 KB | Regular file | 06/09/2014 13:52:34 |
| Crianca9.jpeg | 17 KB | Regular file | 06/09/2014 13:53:18 |
| Executavel_Testel.exe | 88 KB | Regular file | 05/07/2010 11:30:54 |
| Imagem3.jpeg | 22 KB | Regular file | 10/12/2012 14:31:18 |
| MusicaCrianca1_Testel.wav | 10.490 KB | Regular file | 13/09/2014 12:50:56 |
| MusicaCrianca2_Testel.mp3 | 420 KB | Regular file | 02/09/2011 18:03:10 |
| MusicaCrianca3_Testel.mp3 | 582 KB | Regular file | 04/09/2011 13:19:04 |
| PlanilhaCrianca1_Testel.xlsx | 11 KB | Regular file | 06/09/2014 14:13:08 |
| SlideCrianca_Testel.ppt | 588 KB | Regular file | 06/09/2014 14:17:58 |
| TextoCrianca1_Testel.docx | 14 KB | Regular file | 06/09/2014 14:00:10 |
| TextoCrianca2_Testel.txt | 1 KB | Regular file | 06/09/2014 14:07:12 |
| TextoCrianca3_Testel.pdf | 198 KB | Regular file | 06/09/2014 14:05:58 |
| TextoNumero1.docx | 13 KB | Regular file | 06/09/2014 14:26:38 |
| Video1.avi | 3.998 KB | Regular file | 05/09/2014 17:33:32 |
| VideoCrianca1_Testel3.gp | 407 KB | Regular file | 05/09/2014 17:33:32 |
| VideoCrianca2_Testel1.avi | 4.513 KB | Regular file | 23/08/2014 20:02:02 |
| VideoCrianca3_Testel2.mpl | 4.538 KB | Regular file | 05/09/2014 17:33:32 |

Fonte: Elaborado pela autora.

Figura 45 - Arquivo deletado e aberto pela ferramenta FTK

| Name | Size | Type | Date Modified |
|-----------------------|--------|--------------|---------------------|
| !DF1.PDF | 80 KB | Regular file | 31/08/2014 19:24:02 |
| !XT1.TXT | 1 KB | Regular file | 06/09/2014 14:29:16 |
| Color.jpg | 928 KB | Regular file | 06/09/2014 12:59:44 |
| Crian_Imagem1.png | 18 KB | Regular file | 13/09/2014 14:03:38 |
| Crian_Imagem2.jpg | 73 KB | Regular file | 13/09/2014 14:02:30 |
| Crianca1.bmp | 7 KB | Regular file | 06/09/2014 13:55:58 |
| Crianca10.jpg | 26 KB | Regular file | 06/09/2014 13:54:10 |
| Crianca11.jpg | 7 KB | Regular file | 06/09/2014 13:54:30 |
| Crianca12.jpg | 9 KB | Regular file | 06/09/2014 13:55:08 |
| Crianca2.bmp | 20 KB | Regular file | 06/09/2014 13:49:46 |
| Crianca3.bmp | 14 KB | Regular file | 06/09/2014 13:49:58 |
| Crianca4.png | 11 KB | Regular file | 06/09/2014 13:56:22 |
| Crianca5.png | 33 KB | Regular file | 06/09/2014 13:58:18 |
| Crianca6.png | 8 KB | Regular file | 06/09/2014 13:51:34 |
| Crianca7.jpeg | 7 KB | Regular file | 06/09/2014 13:52:58 |
| Crianca8.jpeg | 14 KB | Regular file | 06/09/2014 13:52:34 |
| Crianca9.jpeg | 17 KB | Regular file | 06/09/2014 13:53:18 |
| Executavel_Testel.exe | 88 KB | Regular file | 05/07/2010 11:30:54 |
| Imagem3.jpeg | 22 KB | Regular file | 10/12/2012 14:31:18 |

| Properties | |
|--------------------|--------------------------|
| General | |
| Name | !DF1.PDF |
| File Class | Regular file |
| File Size | 81.629 |
| Physical Size | 81.920 |
| Start Cluster | 33 |
| Date Accessed | 13/09/2014 |
| Date Created | 13/09/2014 15:00:33 |
| Date Modified | 31/08/2014 19:24:02 |
| DOS Attributes | |
| 8.3 Short Filename | !DF1.PDF |
| Hidden | <input type="checkbox"/> |
| System | <input type="checkbox"/> |

<vazio>

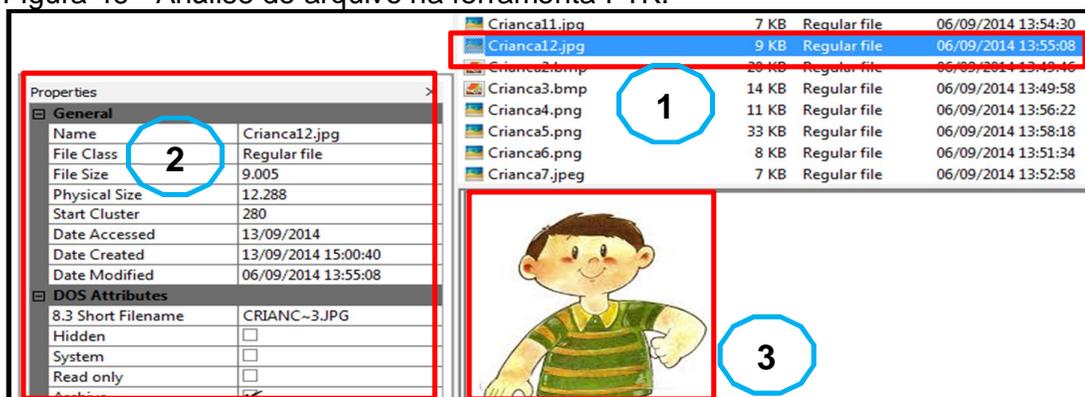
Fonte: Elaborado pela autora.

A figura 45 - item 1, mostra a análise de um arquivo deletado, que corresponde a um dos arquivos inseridos no *pen drive* antes de inserir os itens reais para análise forense, como comprovados na figura 6. Já o item 2, mostra o que

contém dentro do arquivo deletado, como já informado o trabalho não busca recuperar arquivos deletados, desse modo apenas pode-se ver o nome do arquivo.

Existem dois tipos de analisar o arquivo utilizando o FTK, sendo o modo automático e o hexadecimal, visto que um exibe o modo padrão e outro específico.

Figura 46 - Análise de arquivo na ferramenta FTK.



Fonte: Elaborado pela autora.

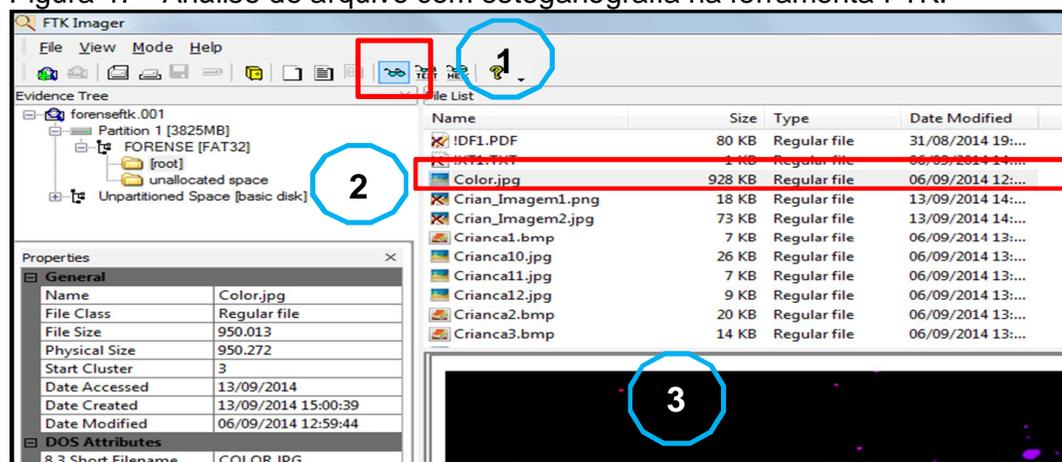
A figura 46 mostra a análise de uma figura no modo automático. Para isso algumas informações são importantes para análise forense, sendo:

Item 1: Informações da figura; Item 2: Propriedades da figura e o item 3: O arquivo selecionado, visível para análise do perito.

A figura 47 - item 1: Analisa a figura no modo automático; item 2: Nome do arquivo; e o item 3: O arquivo aberto para visualização.

Lembrando que o arquivo "Color.jpg" é o mesmo arquivo analisado na ferramenta Helix, deste modo os arquivos contêm esteganografia.

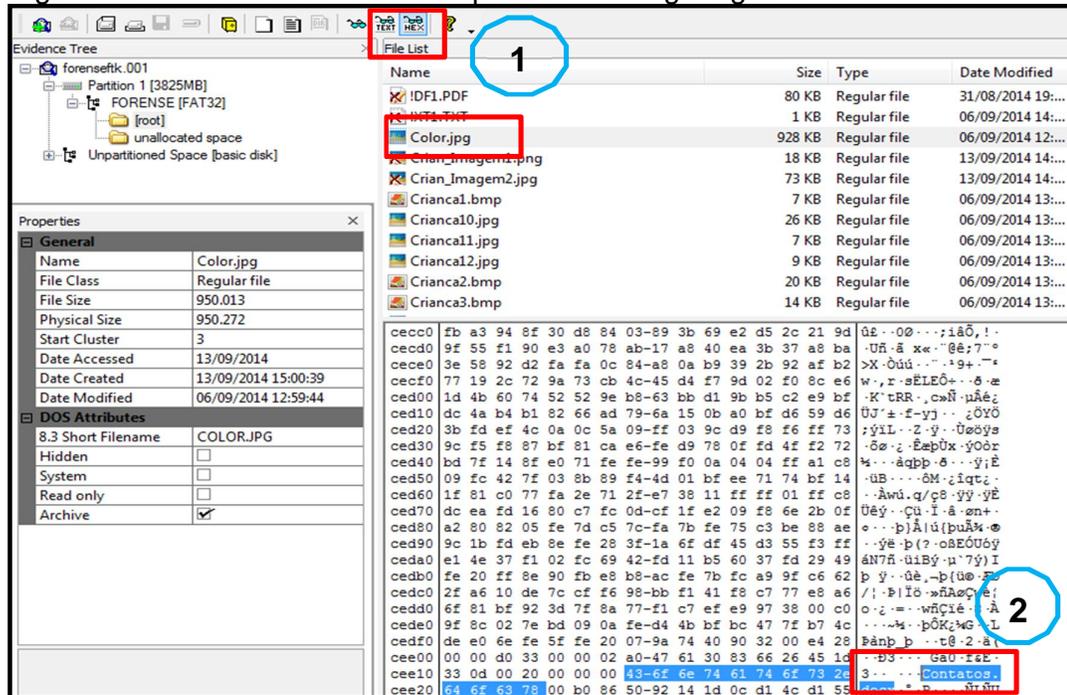
Figura 47 - Análise de arquivo com esteganografia na ferramenta FTK.



Fonte: Elaborado pela autora.

Ainda na análise do arquivo “Color.jpg”, foi utilizado o segundo método em seu modo hexadecimal, como mostra a figura 48.

Figura 48 - Evidência dentro do arquivo com esteganografia na ferramenta FTK.

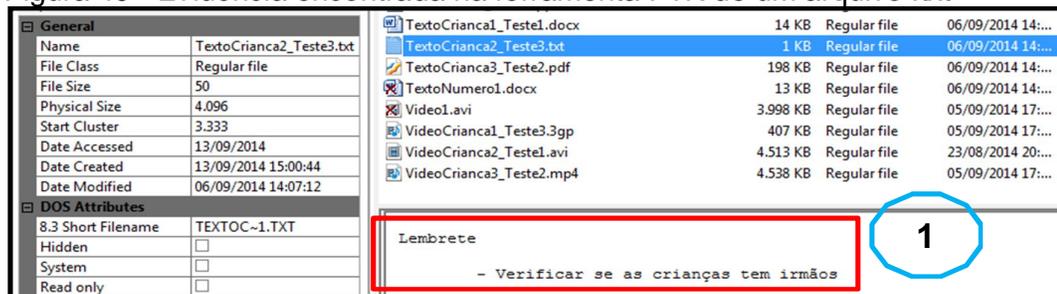


Fonte: Elaborado pela autora.

O modo hexadecimal verificou de forma mais específica as informações contida no arquivo, como mostra o item 1; e o item 2, mostra a primeira evidência encontrada no arquivo “Color.jpg”, sendo um “.docx”.

Após concluir a existência de esteganografia no arquivo “Color.jpg”, precisou verificar qual o seu conteúdo, que por sua vez foram utilizados os mesmos recursos da ferramenta Helix, e obtiveram o mesmo resultado (figura 39).

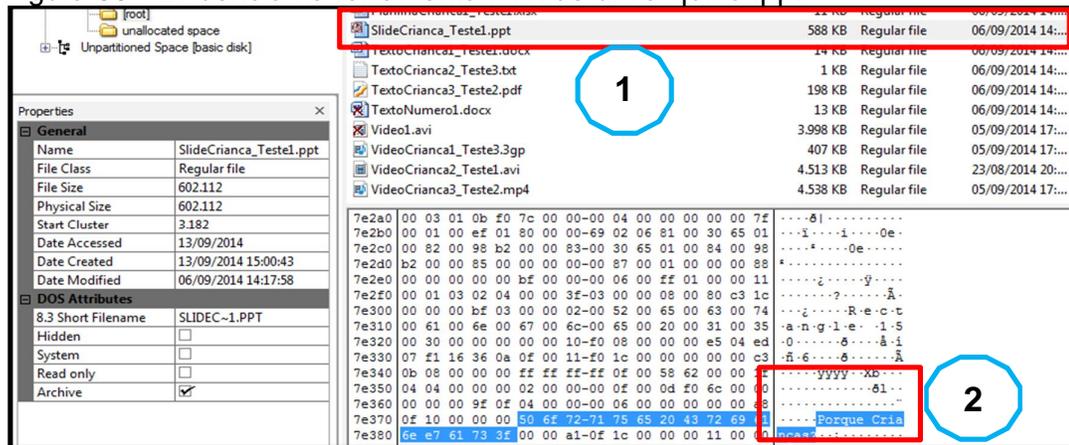
Figura 49 - Evidência encontrada na ferramenta FTK de um arquivo .txt



Fonte: Elaborado pela autora.

A figura 49, mostra a análise de um arquivo “.txt”, com a comprovação através do modo automático, uma evidência encontrada no corpo do arquivo (item 2).

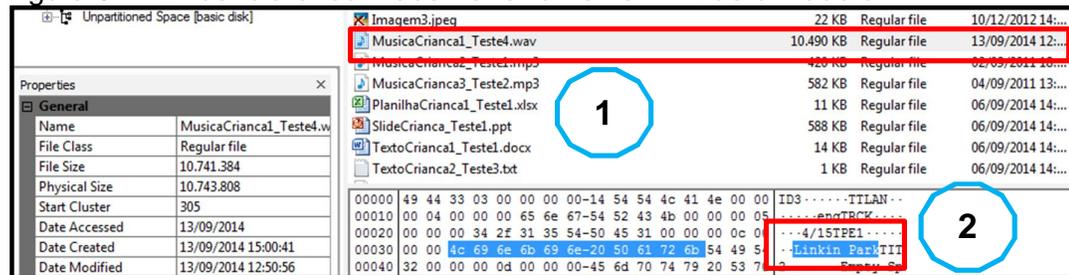
Figura 50 - Evidência na ferramenta FTK de um arquivo .ppt



Fonte: Elaborado pela autora.

A figura 51 mostra a análise de um arquivo “.ppt”, visto no item 1, e o item 2 mostra, o modo hexadecimal aberto com a análise feita, onde foi comprovado a existência de uma mensagem dentro do arquivo.

Figura 51 - Evidência encontrada na ferramenta FTK de um áudio



Fonte: Elaborado pela autora.

A figura 51, mostra a análise do arquivo “.wav” no modo hexadecimal vista no item 1, e assim pode-se concluir apenas uma evidência encontrada, sendo o nome da música antes de ser renomeada vista na figura 51 - item 2.

Os demais arquivos, que não foram apresentados nenhum tipo de resultado na análise referem-se às ferramentas que não foram compatíveis para comprovar nenhuma evidência encontrada.

Após terminar a análise das duas imagens feitas forensehelix.dd e o forenseftk.001, pode-se concluir que obteve-se provas o suficiente para formular um laudo, como foi apresentado abaixo.

6.4 FORMALIZAÇÃO

A fase da formalização conhecida também por fase dos resultados obtidos, exibida na figura 3, levou a conclusão de todas as análises feitas no dispositivo, a fim descrever e comprovar a evidência encontrada do caso relatado.

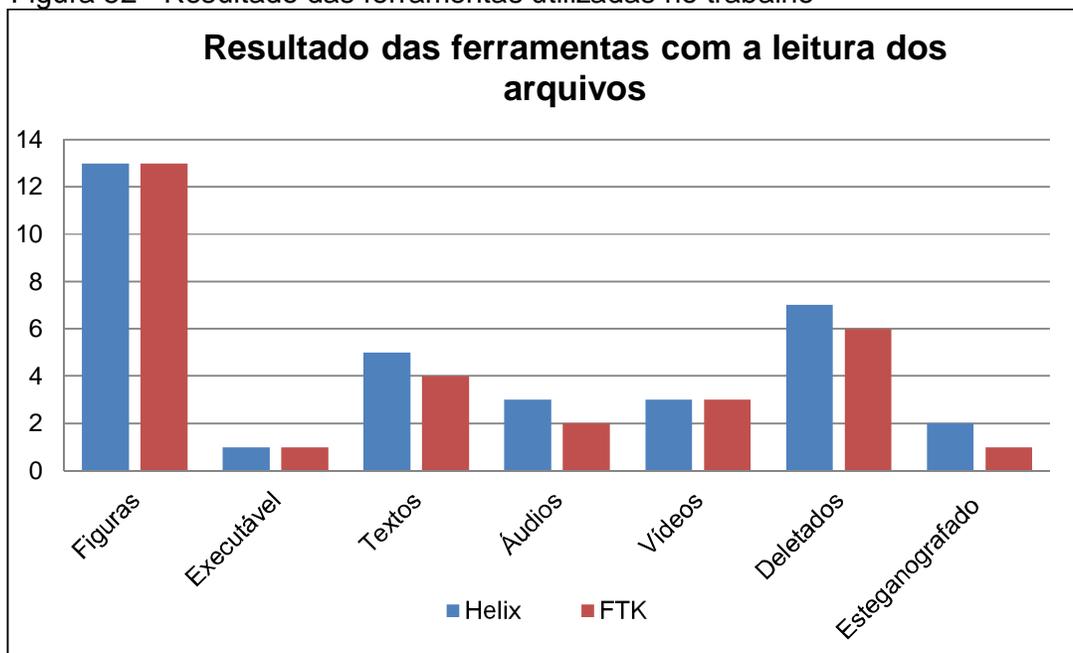
Deste modo foi feito um laudo pericial contendo as informações da análise feita, vista no APÊNDICE B.

Após exibir os resultados encontrados do presente trabalho, abaixo (figura 52) mostra a repercussão que cada ferramenta teve em ler determinados tipos de arquivos.

Através do gráfico abaixo, fica nítido que as duas ferramentas tiveram basicamente as mesmas repercussões com alguns tipos de arquivos, como: figuras, executáveis e vídeos.

Já para os demais arquivos, a ferramenta Helix mostrou estar sempre à frente da ferramenta FTK no quesito leitura de arquivos, exibida com arquivos do tipo: texto, áudio, deletados e os principais, arquivos com esteganografia.

Figura 52 - Resultado das ferramentas utilizadas no trabalho



Fonte: Elaborado pela autora.

7 CONCLUSÃO

Considerando o grande avanço tecnológico de ferramentas para invasões de crimes virtuais, existem ferramentas que buscam reconhecer autores desse tipo de ataque, deste modo muitas ferramentas são desenvolvidas atualmente com a finalidade de reconhecer esses autores, tanto para uso pessoal quanto corporativo. A perícia forense fica cada vez mais evidente no mercado devido a estes fatos, e cada vez mais precisa de *softwares* com estas funções.

O trabalho por ser um tema de grande escassez e até mesmo incompleto em muitos objetos de pesquisa abordou uma das vertentes da área forense computacional digital, obter evidência em dispositivos.

Com esse intuito, foram usadas algumas ferramentas forenses em dois tipos de sistemas operacionais utilizados no dia-a-dia, sendo Windows e Linux.

As ferramentas foram criadas cada uma em um sistema operacional, e depois testada em outro sistema operacional com a intenção de comparar qual delas obtém o maior número de informações relevantes sobre o dispositivo analisado.

O trabalho concluiu inicialmente qual o melhor tipo de formatação para o perito encontrar evidência em um dispositivo. E deste modo foram realizados testes com arquivos antes de ser analisado o dispositivo com os reais arquivos. Assim foi relatado que a formatação rápida deixou vestígios de arquivos deletados dentro do *pen drive* e a formatação completa apagou literalmente todos os arquivos que estavam dentro o *pen drive*.

Devido à formatação rápida apagar apenas onde estão localizadas as informações dos arquivos, permite assim que os arquivos ainda continuem lá (apesar de não estarem mais listados). E a formatação completa apaga tudo quanto à trilha zero quantas todas as outras trilhas.

Detalhes importantes foram visto em cada plataforma. Na plataforma Linux, utilizando o Helix, a ferramenta conseguiu realizar todas as fases forenses e alcançar a expectativa do trabalho, pois criou, analisou e concluiu todo o trabalho da análise da imagem. Visto que os arquivos contidos dentro do dispositivo foram abertos e analisados devidamente por peritos. O único problema encontrado na ferramenta Helix foi que não é possível recuperar arquivos deletados encontrado dentro do dispositivo, pois para esse tipo de técnica é preciso o estudo de outras ferramentas forense. O Helix além de ser gratuito provou que é uma ótima

ferramenta para análise de arquivos com esteganografia, tanto para arquivos quanto para áudios, pois foram analisados e encontrados todos os arquivos inseridos no objeto de pesquisa.

Já a ferramenta Forensic Toolkit utilizada na plataforma WINDOWS realizou todas as fases, porém deixou a desejar em alguns procedimentos importantes para um perito forense como, a não análise de arquivos com esteganografia. Visto que a ferramenta apenas encontrou evidências em arquivo com formato JPEG (figura), e no formato WAV (áudio) não foi encontrado nenhum tipo de evidência.

Um fator importante em relação ao Forensic Toolkit, é o modo como são gerados os formulários com as informações que compõe os arquivos dentro na imagem, sendo gerado no formato de tabela com extensão .xlsx onde é notável uma estrutura mais clara e fácil visualização para o perito.

Outro fator importante é que o Forensic Toolkit não conseguiu atingir, é a validação da imagem gerada pelo Helix. Pois dessa forma não se pode comparar o MD5 gerada pelo Helix e acabou não garantindo a integridade da imagem feita. Já o Helix, conseguiu comparar a MD5 dele próprio e a do Forensic Toolkit para assim validar a integridade da imagem.

Levando em consideração à questão do tempo na criação de cada imagem, o Helix copiou bit a bit e tornou o processo mais lento, porém muito mais seguro. E o Forensic Toolkit torna a criação mais rápida, porém no padrão normal de cópia.

Os arquivos lidos por cada ferramenta revelam que as duas ferramentas conseguem ler sem nenhum tipo de problema qualquer extensão de figuras; a ferramenta Helix mostrou ter maior desempenho em arquivos texto; em áudios a ferramenta Helix novamente mostrou ter maior desempenho; em arquivos deletados as duas ferramentas conseguem visualizar, entretanto nenhuma delas consegue recuperá-los e arquivos com esteganografia o Helix tem mais desenvoltura na leitura.

Para formalização do laudo pericial, foi feito com base na ferramenta que teve o melhor desempenho no decorrer do trabalho, sendo o Helix. Visto que o mesmo consegue atingir todos os recursos precisos em uma análise forense.

Um ponto observado foi que o Helix é uma ferramenta estruturada para não montar automaticamente nenhuma unidade de disco, pois preserva a integridade dos dados e é por essa razão que o *software* é um dos mais utilizado para análise forense.

8 TRABALHOS FUTUROS

Como possíveis trabalhos futuros, pode-se apontar:

- Procurar novas ferramentas forenses que possam analisar arquivos com esteganografia;
- Conhecer novas ferramentas forenses que possam analisar arquivos em dispositivos móveis;
- Explorar outros tipos de ferramentas forenses que façam cópia bit a bit;
- Aprofundar a análise na ferramenta Helix, para que seja possível mostrar outros recursos disponíveis na ferramenta;
- Estudar outras fases forenses para obtenção de evidência digital;
- Procurar ferramentas que possam recuperar arquivos deletados dentro de dispositivos;

REFERÊNCIAS

AZEVEDO, M. T.; PEGETTI, A. L.; SANTOS, K. M. Técnicas de perícia forense como ferramentas de prevenção de incidentes de segurança. **Revela**, v. 5, n. 12, dez. 2011. Disponível em: <http://www.fals.com.br/revela16/artigo2_12.pdf> Acesso em: 25 maio 2014.

ALMEIDA, R.N. **Perícia Forense Computacional**: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais. 2011. 48 f. monografia (Tecnólogo em Processamento de Dados) - Faculdade De Tecnologia De São Paulo. São Paulo. 2011.

COSTA, D.M. **Boas Práticas Para Perícia Forense**. 2008. 44 f. monografia (Curso de Ciência da Computação) – Faculdade de Jaguariúna. Jaguariúna. 2008.

ELEUTÉRIO, P. M. S; MACHADO, M.P. **Desvendando a Computação Forense**. 1. Ed. São Paulo: Novatec, 2011.

ESTEGANOGRAFIA. In: **Dicionário Pribeam da Língua Portuguesa**, c2013. Disponível em: < <http://www.priberam.pt/dlpo/esteganografia>>. Acesso em: 02 nov. 2014.

FARIA, R.F. **Analisando Os Riscos De Uma Invasão Para Testar O Desempenho De Um Banco De Dados**. 2011. 75 f. Trabalho de conclusão de curso. (Tecnólogo em Banco de Dados) – Centro Estadual De Educação Tecnológica “Paula Souza”, Faculdade De Tecnologia De Lins. Lins. 2011.

FARMER, D.; VENEMA, W. **Perícia Forense Computacional**: Teoria e Prática Aplicada. São Paulo: Pearson Prentice Hal, 2007.

FORENSE. In: **Dicionário Pribeam da Língua Portuguesa**, c2013. Disponível em: <<http://www.priberam.pt/dlpo/forense>>. Acesso em: 30 maio 2014.

FORENSE DIGITAL TOOLKIT. **Site oficial da ferramenta Forense Digital ToolKit para download**, c2014. Disponível em: <<http://fdtk.com.br/www/download/>> Acesso em: 8 nov. 2014.

FREITAS, A. R. **Perícia Forense Aplicada à Informática**: Ambiente Microsoft. 1. Ed. Rio de Janeiro: Brasport, 2006.

GIL, A.C. **Como Elaborar Projetos de Pesquisa**. 4. Ed. São Paulo: Atlas, 2002.

GONCALVES, M. et al., **Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas**. **Net**. Jaciara-Mato Grosso, nov. 2012. Disponível em: <<http://www.eduvalesl.edu.br/site/edicao/edicao-74.pdf>> acesso em: 08 nov. 2014.

HELIX. **Site oficial da ferramenta Helix para download**, c2001-2014. Disponível em: <<https://e-fenseinc.sharefile.com/d/sda4309a624d48b88>> Acesso em: 8 nov. 2014.

NETO, A. F. et al. **Instituto Brasileiro de Avaliações e Perícias de Engenharia de São Paulo**. c2011. Conhecimento de termos. Disponível em: <http://www.ibape-sp.org.br/arquivos/09_CARTILHA_DE_AVALIACAO_O_QUE_E_E_COMO_CO_NTRATAR.pdf> acesso em: 10 set. 2014.

OPENPUFF. **Site para download da ferramenta OpenPuff**. Disponível em: <http://embeddeds.w.net/OpenPuff_Steganography_Home.html> Acesso em: 8 nov. 2014.

PEREIRA, E. D. V. **Investigação Digital: conceitos, ferramentas e estudos de caso**. **Infobrasil.inf.br**, c2010. Disponível em: <<http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao%20Digital.pdf>>. Acesso em: 02 Maio 2014.

PERICIA. In: **Dicionário Priberam da Língua Portuguesa**, c2013. Disponível em: <<http://www.priberam.pt/dlpo/pericia>>. Acesso em: 30 maio 2014.

QUEIROZ, C.; VARGAS, R. **Investigação e Perícia Forense Computacional: Certificações, Leis Processuais, Estudos de Caso**. Rio de Janeiro: Brasport, 2010.

SÁ, G.Z. **Avaliação de técnicas anti-forenses computacionais aplicadas a registros de sistemas Linux**. 2013. 59 f. Trabalho de conclusão de curso. (Graduação em Tecnologia em Sistemas para Internet) - Universidade Tecnológica Federal do Paraná (UTFPR), Campo Mourão.

SOUZA, R. R de. **Revista Tecnologias em Projeção. Bem-Estar Percebido Sobre Funcionalidades e Design De Aparelhos Celulares**, dez. 2011. Disponível em: <<http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/download/167/148>> Acesso em: 10 maio. 2014.

TOLENTINO, L. C.; SILVA, W.; MELLO, P. **Revista Tecnologias em Projeção.v2. A Perícia Forense Computacional**, dez. 2011. Disponível em: <<http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/download/168/149>> Acesso em: 10 maio. 2014.

APÊNDICE A - TABELA DADOS GERADOS COM A FERRAMENTA FTK

Tabela 1 - Dados gerados pela ferramenta FTK

| | MD5 | SHA1 | Nome da Imagem | Partição | Nome Dispositivo | Diretório | Nome Arquivo |
|----|----------------------------------|--|-----------------------|-------------------------|-------------------------|------------------|---------------------|
| 1 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crian_Imagem1.png |
| 2 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crian_Imagem2.jpg |
| 3 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Imagem3.jpeg |
| 4 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | !DF1.PDF |
| 5 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | TextoNumero1.docx |
| 6 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | !XT1.TXT |
| 7 | d41d8cd98f00b204e9800998ecf8427e | da39a3ee5e6b4b0d3255bfef95601890afd80709 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Video1.avi |
| 8 | 995669292cd30b990e27f32454307bfd | b8413e6731cc1f5e52c526bf35f8e11ecc876bb5 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Color.jpg |
| 9 | 94294266efc9f10cd399c54d9c6c6965 | f7a293eb7af87f0cd1d6d10ebecfe656e2f1b0d8 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca1.bmp |
| 10 | a5b461b6f0481ea9c0509ab285a8ef62 | d30e110ab7a1eefab89168431d53cad7dceca0b8 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca2.bmp |
| 11 | 1d28906563d4c19fd47ec3b89447aa94 | 93aba7752c5f534cec3d134c9ab4da87b5b3a27e | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca3.bmp |
| 12 | 67b562b4d94b664f612b8994d35f58b1 | e09694cd08f5538e80995550ca4ce472a1ab7e82 | forensftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca4.png |

| | | | | | | | |
|----|----------------------------------|--|----------------|-------------------------|--------------------|--------|------------------------------|
| 13 | ac5cec107e182c9b8af3276bb4d8f281 | 733d96018147063be29a6051c33b99258ffd42cd | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca5.png |
| 14 | 1af220ba16d5565c762d942744c850e9 | ded1be0a3a8d87641e352fc93fef1599930c998b | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca6.png |
| 15 | b087eaff85befa723dc31fcc6bad71bc | 030fde4a13a496f7ecec0a2def6a9764ba10fe7b | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca7.jpeg |
| 16 | 47b70157300b64a8f26211e8f0249cce | 9099bc69a3f90791c06cca76fa7818211877005c | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca8.jpeg |
| 17 | 4231df773f6ad0742cea3dff08c7feac | 100a2c0364b818e15b0f6863c69cb25aaa0d94de | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca9.jpeg |
| 18 | 400ac588b11fd6a66b5ad766df93fd3f | de5b7116c86b65c579e89b1b8842c7f13eea4b93 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca10.jpg |
| 19 | 3e57c01d52a178fb621429133437a5c9 | 0238111bfbc8cd912272e520ac29da84d57b8458 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca11.jpg |
| 20 | 23f2727b3a45b8a26cdebc5bbebfd271 | 5b0ccaa01164e04d741ba0652d3972e2d417f92a | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Crianca12.jpg |
| 21 | e69624ef8bb880ba6eff3871e044cac0 | c9d032a3975d28fd7eea1be29b4a4a6a414f9b5a | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | Executavel_Teste1.exe |
| 22 | 374ea9c1debee1cde2d5cdab4cbf8956 | e0354bdfdc6a84e11aa50cb0e7aaf119c6c65315 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | MusicaCrianca1_Teste4.wav |
| 23 | 3ffca2d3940f9415f4bed30e8f7df72 | ca7a1c2ed06504caec41a148f8a5ca792d3e1c8b | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | MusicaCrianca2_Teste1.mp3 |
| 24 | 2e028cf85da0e0feddbfdb9c465061b0 | 0315a946033d784441b018b706f6c26cf7f9d961 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | MusicaCrianca3_Teste2.mp |
| 25 | 85d52febbf97dd63e8da25e2dfe5fbef | cd61a281fbb388095f65cbbb7fa3c996189b176 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | PlanilhaCrianca1_Teste1.xlsx |
| 26 | da0399ed1e395982dbc3307414bb2c50 | 4cae5e97859417ac246db0ea047102b59cbb1ae | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | SlideCrianca_Teste1.ppt |
| 27 | af11dd5f138f3c469140102f311e60a1 | 49afe09dc094cbf309363c7a0369fe08037f3e07 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | TextoCrianca1_Teste1.docx |

| | | | | | | | |
|----|----------------------------------|--|----------------|-------------------------|--------------------|-------------------|---------------------------|
| 28 | 05dd222e1b2c610551d0175aa55c08e7 | f4647f2e8e775bc62f2f415c076a43eef4095a1d | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | TextoCrianca2_Testes3.txt |
| 29 | 1b2ad27f985bf95ea4e5b1be8f2ec7e9 | 42f573d3ab863594a6c4978a50ee175fe1c439cd | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | TextoCrianca3_Testes2.pdf |
| 30 | 42c3f8b5d1d6f592c60109293379b527 | a1d070f63840428ea5eb916ac8ced6b0ee10a63b | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | VideoCrianca1_Testes3.3gp |
| 31 | 44b33be5f2d8814074973216a5a55477 | 615f9120bba441fca64ee16f785cf24f363d4df7 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | VideoCrianca2_Testes1.avi |
| 32 | 5998c043dced50dabf39a89402736213 | edc8012be2d062d4726ace0156d228de8970877e | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | [root] | VideoCrianca3_Testes2.mp4 |
| 33 | a63ff86835e3ca13c887a14e729186d3 | 4fa5e33376847680715d3176a30944d02d736adb | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | VBR | |
| 34 | e9eb772461b8d885843fa5d3b11cf9c4 | a5e8607812f951ac8cef094be1d62ec043c6596b | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | reserved sectors | |
| 35 | c12d01eb662a2d72369c3f2966772ea2 | 3185dc2a859f226919ceb34f57d0b71ea29a5f18 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | unallocated space | 005750 |
| 36 | 0f343b0931126a20f133d67c2b018a3b | 60cacbf3d72e1e7834203da608037b1bf83b40e8 | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | file system slack | |
| 37 | db60b895342bb980a71b01b2733220cb | 4218584ffe13439b17cb9868ff023264462804fc | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | FAT1 | |
| 38 | db60b895342bb980a71b01b2733220cb | 4218584ffe13439b17cb9868ff023264462804fc | forenseftk.001 | Partition 1 [3825MB] | FORENSE [FAT32] | FAT2 | |

Fonte: Elaborado pela autora.

APÊNDICE B - MODELO DE LAUDO JUDICIAL

PERÍCIA FORENSE COMPUTACIONAL

LAUDO JUDICIAL

PERITOS RESPONSÁVEIS

Perito Forense 2088

Perito Forense 1878

ESCOPO

Analisar e extrair eventuais evidências que demonstre materialidade de um delito no exame pericial, a fim de descrever provas encontradas que indique a autoria do mesmo para conclusão do processo.

AUTORIDADE SOLICITANTE

Análise vinculada e solicitada pelo Doutor Fulano.

CADEIA DE CUSTÓDIA



EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Número: 82923123428 Pág.: 1 De.: PeritoForense2088

Detalhes da mídia/equipamento

| Item | Descrição | |
|------------|---|-----------------|
| 1 | <i>Pen drive de 4GB com indícios de pedofilia</i> | |
| | | |
| Fabricante | Modelo | Número de Série |
| SanDisk | Cruzer Blade | MBOx20736f63 |

Sobre a imagem dos dados

| Data | Hora | Criado por | Ferramenta |
|----------------|----------------------------------|-------------------|----------------|
| 06/09/2014 | 06h42min | PeritoForense2088 | Helix v.2009R1 |
| | | | |
| Tipo de Cópia | HASH | | |
| Disco Completo | 0b5cab2b156dd472306636472f769128 | | |

Cadeia de custódia

| C ó d. | Origem | Data | Hora | Destino | Data | Hora |
|--------------|-----------------------|----------|----------|------------------|----------|----------|
| 1 | Local de Apreensão | 05/09/14 | 22h30min | Perícia | 06/09/14 | 4h30min |
| 2 | Material entregue | 10/09/14 | 09h25min | Análise | 11/09/14 | 9h22min |
| 3 | Início pericial | 16/09/14 | 21h10min | Emissão Laudo | 28/11/14 | 14h11min |
| 4 | Análise laudo | 30/11/14 | 08h00min | Entrega Juiz | 04/12/14 | 10h40min |

Fonte: Elaborado pelo perito.

OBJETO SUBMETIDO

Indícios: indivíduo denominado fulano com indícios de envolvimento em possíveis crimes relacionados à pedofilia infantil.

Um *pen drive* a ser periciado;

- Fabricante: SanDisk
- Modelo: Cruzer Blade
- Número de Série: MB0x20736f63

Arquivos analisados;

Tamanho do *pen drive* (4GB);

METODOLOGIA

Foram utilizadas as seguintes ferramentas para análise das imagens e arquivos encontrados no *pen drive*:

- ✓ Helix v.2009R1

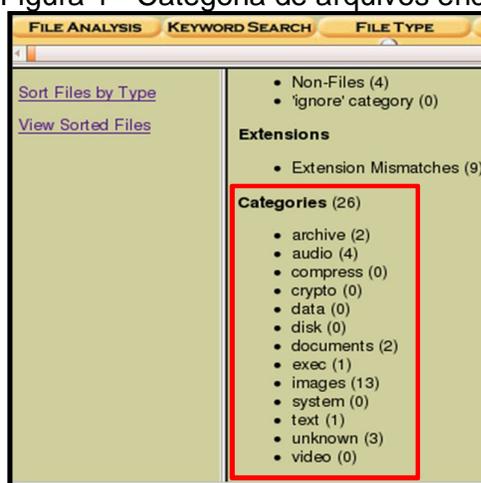
A ferramenta Helix foi utilizada para análise forense por ser uma das melhores ferramentas no campo investigativo com inúmeros recursos disponíveis para analisar imagens.

ANÁLISE DO EVENTO E RESULTADOS OBTIDOS

O primeiro passo executado relativo à perícia forense foi criar uma imagem do disco utilizando a ferramenta Helix, de extrema importância.

Para a extração dos arquivos foi utilizado a ferramenta Helix, e em seu ambiente de análise, denominado Autopsy Forensic Browser, que nada mais é que uma interface gráfica que auxilia a investigação. A figura 1 mostra as categorias dos arquivos encontradas no *pen drive* periciado.

Figura 1 - Categoria de arquivos encontrados com o Helix



Fonte: Elaborado pelo perito.

Vale ressaltar também que foram encontrados alguns arquivos que aparentemente não apresentam indícios que possam comprometer o indivíduo em questão como mostra a figura 2.

Figura 2 – Arquivos encontrados dentro da imagem

| Type | NAME | WRITTEN | ACCESSED | CREATED | SIZE |
|-------|-------------------------------|------------------------------|------------------------------|------------------------------|--------|
| r / r | Color.jpg | 2014-09-06 12:59:44 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 950013 |
| r / r | Crianca1.bmp | 2014-09-06 13:55:58 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 6334 |
| r / r | Crianca10.jpg | 2014-09-06 13:54:10 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 25733 |
| r / r | Crianca11.jpg | 2014-09-06 13:54:30 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 6932 |
| r / r | Crianca12.jpg | 2014-09-06 13:55:08 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 9005 |
| r / r | Crianca2.bmp | 2014-09-06 13:49:46 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 20410 |
| r / r | Crianca3.bmp | 2014-09-06 13:49:58 (UTC) | 2014-09-06 00:00:00 (UTC) | 2014-09-06 15:29:04 (UTC) | 14234 |

Fonte: Elaborado pelo perito.

Através do Helix, foi possível verificar a nome de origem do *pen drive*, sendo assim outra evidência importante a ser descrito nesse laudo, como mostra figura 3.

Figura 3 – Nome encontrado do dispositivo analisado

| Type | NAME | WRITTEN | ACCESSED | CREATED | SIZE |
|--------|------------------------------|------------------------------|------------------------------|------------------------------|------|
| dir/in | FORENSE (Volume Label Entry) | 2014-09-06 15:28:56 (UTC) | 0000-00-00 00:00:00 (UTC) | 0000-00-00 00:00:00 (UTC) | 0 |

Fonte: Elaborado pelo perito.

Dando continuidade nas análises, utilizando a ferramenta Helix, foi possível ter acesso a todas MD5 (hash) de todos os arquivos contidos ou não no *pen drive*, como representa a figura 4.

Figura 4 - Relatório das MD5 criado na ferramenta Helix

```

MDS Values for files in C:/ (forensehelix.dd-0-0)
FORENSE (Volume Label Entry)
995669292cd30b990e27f32454307bfd - Color.jpg
94294266efc9f10cd399c54d9c6c6965 - Crianca1.bmp
a5b461b6f0481ea9c0509ab285a8ef62 - Crianca2.bmp
1d28906563d4c19fd47ec3b89447aa94 - Crianca3.bmp
67b562b4d94b664f612b8994d35f58b1 - Crianca4.png
ac5cec107e182c9b8af3276bb4d8f281 - Crianca5.png
1af220ba16d5565c762d942744c850e9 - Crianca6.png
b087eaff85befa723dc31fcc6bad71bc - Crianca7.jpeg
47b70157300b64a8f26211e8f0249cce - Crianca8.jpeg
4231df773f6ad0742cea3dff08c7feac - Crianca9.jpeg
400ac588b11fd6a66b5ad766df93fd3f - Crianca10.jpg
3e57c01d52a178fb621429133437a5c9 - Crianca11.jpg
23f2727b3a45b8a26cdebc5bbebfd271 - Crianca12.jpg
e69624ef8bb880ba6eff9871e044cac0 - Executavel_Testel.exe
1b6d4597c85e526f21b869a5e53893f5 - MusicaCrianca1_Testel.wav
5ffca2d3940f9415f4bed30e8f7df72 - MusicaCrianca2_Testel.mp3
2e028cf85da0e0feddbfdb9c465061b0 - MusicaCrianca3_Testel2.mp3
85d52febbf97dd63e8da25e2df5fbef - PlanilhaCrianca1_Testel.xlsx
da0399ed1e395982dbc3307414bb2c50 - SlideCrianca_Testel.ppt
af11dd5f138f3c469140102f311e60a1 - TextoCrianca1_Testel.docx
05dd222e1b2c610551d0175aa55c08e7 - TextoCrianca2_Testel3.txt
1b2ad27f985bf95ea4e5b1be8f2ec7e9 - TextoCrianca3_Testel2.pdf
42c3f8b5d1d6f592c60109293379b527 - VideoCrianca1_Testel3.3gp
44b33be5f2d8814074973216a5a55477 - VideoCrianca2_Testel.avi
5998c043dced50daf39a89402736213 - VideoCrianca3_Testel2.mp4

```

Fonte: Elaborado pelo perito.

Utilizando a ferramenta Helix foi encontrado arquivos deletados do *pen drive*, junto com informações de datas e horários, como mostra figura 5.

Figura 5 - Arquivos deletados encontrados pela ferramenta Helix



Fonte: Elaborado pelo perito.

Outra análise importante encontrada foi o arquivo “Color.jpg”, pois está submetido a uma esteganografia, ou seja, contém um arquivo .docx dentro da figura.

Através da análise no modo hexadecimal foi possível comprovar a existência da esteganografia, para isso foi preciso analisar com mais detalhe o arquivo, como mostra a figura 6.

Figura 6 - Análise hexadecimal na ferramenta Helix com arquivo esteganografado.

```

GENERAL INFORMATION
File: C://Color.jpg
MD5 of file: 995669292cd30b990e27f32454307bfd
SHA-1 of file: b8413e6731cc1f5e52c526bf35f8e11ecc876bb5

Image: '/var/lib/autopsy/Pedofilia/maquina_02/images/forensehelix.dd'
Offset: Full image
File System Type: fat32

Date Generated: Sun Sep 7 23:01:27 2014
Investigator: PeritoForense2088
  
```

Fonte: Elaborado pelo perito.

Deste modo, é possível notar algumas evidências do arquivo (figura 6), como:

Item 1: Nome do arquivo; Item 2: Código da MD5 do arquivo; Item 3: Caminho da imagem; Item 4: Nome do perito;

Figura 7 - Informações obtidas do arquivo com esteganografia.

```

18240 18241 18242 18243 18244 18245 18246 18247
File Type: JPEG image data, JFIF standard 1.02
-----
CONTENT
00000000: FF D8 FF E0 00 10 4A 46 49 46 00 01 02 00 00 64 .....JFIF.....d
  
```

Fonte: Elaborado pelo perito.

Ainda na análise hexadecimal do arquivo “Color.jpg”, note que o arquivo contém uma extensão tipo JFIF (extensão associada e complementar de JPEG), como mostra a figura 7 acima. E deste modo fica nítido que existe um arquivo dentro de outro arquivo, uma vez que a sequencia de hífen implica a presença de outros arquivos, porém só foi possível verificar o que contém dentro dessa esteganografia nos tópicos abaixo.

Figura 8 - Arquivo encontrado dentro do arquivo com esteganografia.

```

000CEDF0: DEE0 6EFE 5FFE 2007 9A74 4090 3200 E428  .n._. .t@.2..(
000CEE00: 0000 D033 0000 02A0 4761 3083 6626 451D  ...3...Ga0.f&E.
000CEE10: 330D 0020 0000 0043 6F6E 7461 746F 732E  3.. ...Contatos
000CEE20: 646F 6378 00B0 8650 9214 1D0C D14C D155  docx...P....L.
000CEE30: 5C11 0196 106B 12B5 811A BCD6 0569 26AF  \ k i&

```

Fonte: Elaborado pelo perito.

Na análise hexadecimal do arquivo “Color.jpg”, como mostra a figura 8, a uma evidência foi encontrada, o arquivo chamado “Contatos.docx.”, comprovando a existência de esteganografia dentro do arquivo “Color.jpg”, sendo as demais informações em hexadecimal desnecessária para análise.

Figura 9 - Imagem encontrada dentro do arquivo com esteganografia.

```

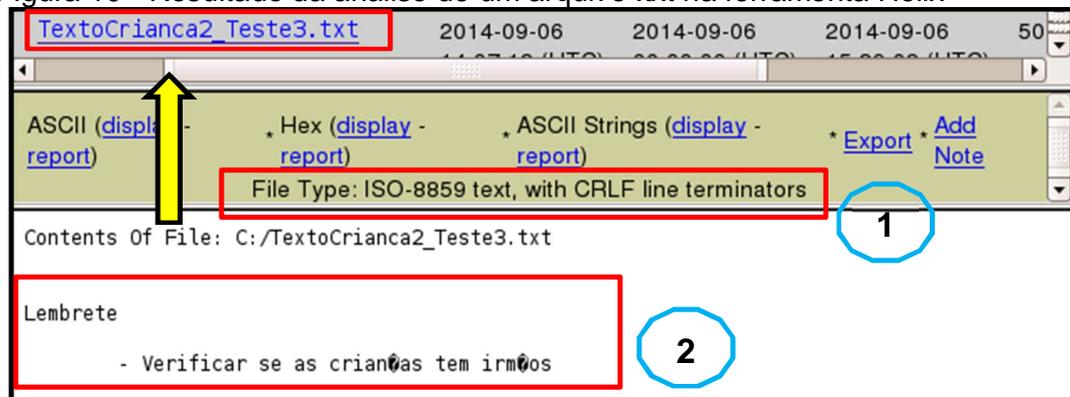
000D1710: 4090 3900 B067 0100 F168 0100 0215 8AFF  @.9..g...h.....
000D1720: 5F28 6526 451D 3314 0020 0000 004E 6F6D  _ (e&E.3... ..Nom
000D1730: 6554 6573 7465 4372 6961 6E63 612E 6A70  eTesteCrianca.jp
000D1740: 6700 F047 6772 1619 5115 089D D599 D161  g..Ggr..Q.....a
000D1750: B555 4517 54B8 96D1 2FA7 01B4 D810 12F2  .UE.T.../.....

```

Fonte: Elaborado pelo perito.

Ainda na análise hexadecimal do arquivo “Color.jpg” a figura 9, comprova outra evidência encontrada, pois foi localizado um figura com o nome de “NomeTesteCrianca.jpg”, ou seja existe uma figura dentro da figura “Color.jpg”.

Figura 10 - Resultado da análise de um arquivo .txt na ferramenta Helix



Fonte: Elaborado pelo perito.

A figura 10, mostra a análise de um arquivo com formato “.txt”, com uma evidência no corpo do texto.

Figura 11 - Dado encontrado na análise hexadecimal do arquivo .ppt na ferramenta Helix.

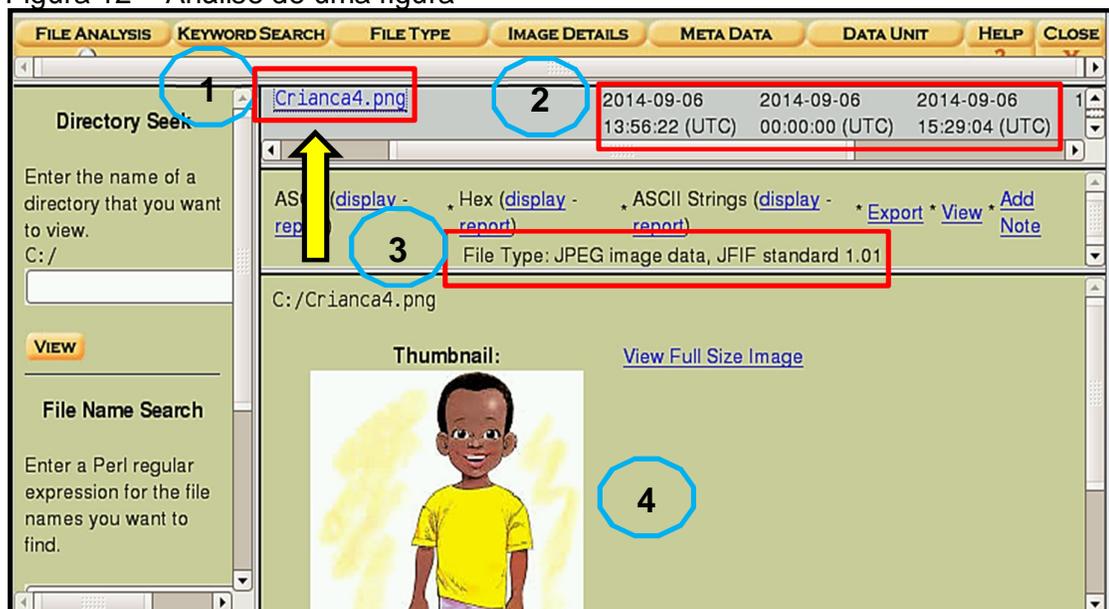
| | | |
|-----------|---|------------------|
| 0007E360: | 0000 009F 0F04 0000 0006 0000 0000 00A8 | |
| 0007E370: | 0F10 0000 0050 6F72 7175 6520 4372 6961 | Porque Cria |
| 0007E380: | 6EE7 6173 3F00 00A1 0F1C 0000 0011 0000 | n.as?..... |
| 0007E390: | 0000 0000 080A 0000 0007 0011 0000 0001 | |

Fonte: Elaborado pelo perito.

A figura 11 acima, mostra a análise hexadecimal de um arquivo com formato “.ppt”, onde foi encontrada uma nova evidência dentro do arquivo, com informações que apontam de fato uma relação duvidosa do individuo.

A figura 12 abaixo mostrou a análise de um arquivo com evidências importantes encontradas.

Figura 12 – Análise de uma figura



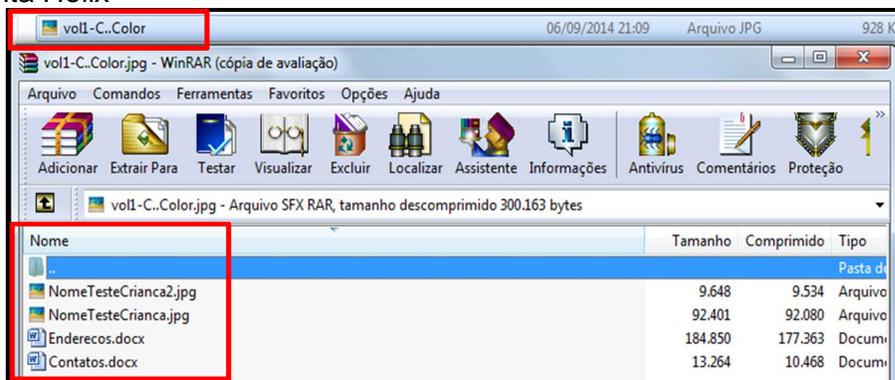
Fonte: Elaborado pelo perito.

A figura 12 mostra as evidências encontradas na figura, pois dará continuidade a investigação sendo:

Item 1: Nome do arquivo; Item 2: Data da figura; Item 3: Tipo do arquivo; Item 4: O Arquivo aberto;

Após analisar o arquivo com esteganografia sendo, “Color.jpg”, faltou verificar o que contém dentro desses arquivos e deste modo conclui-se que o arquivo “Color.jpg” possui técnicas de esteganografia vista no modo hexadecimal (figura 6) e para recuperar foi feito o método de extração. Visto na figura 13.

Figura 13 - Arquivos encontrados dentro do arquivo esteganografado pela ferramenta Helix



Fonte: Elaborado pelo perito.

E utilizando o método de extração, podem-se ver quartos arquivos encontrados dentro de “Color.jpg”, as mesmas evidências encontradas na figura 8 e figura 9.

Foi utilizada a ferramenta Helix para tentativa de detecção de provas sobre análise feita e deste modo foi comprovado que os recursos que as compõe são importantes na área forense.

Vale ressaltar que o *pen drive* estudado foi entregue um dia após a data de emissão do ato de exibição e apreensão e sem o documento intitulado de cadeia de custódia.

Análise das fases de uma perícia forense computacional para obtenção de evidências

Rafaela T. Venerando¹, Henrique P. Martins¹, Patrick P. Silva¹, André L. F. Castro¹

¹Centro de Ciências Exatas e Sociais Aplicadas – Universidade Sagrado Coração (USC)
Bauru 17.011-970 – São Paulo – SP – Brasil

rafaela.venerando@gmail.com

Abstract. *With proportions achieved through technology, everything in a computerized world works based on storage devices and software development, interconnected to a single point: technology. With this acting as imposing form in the world, we are faced with criminals who use it to commit crimes, for this reason, it's really important to make primary analysis of computers by computer forensics. This article aimed to explain, briefly, the procedures in an investigation files storage devices using the tool Helix and Forensic Toolkit. The methodology used for the development of labor was through literature searches in books and monographs. This work shows that the Helix and Forensic Toolkit are two important tools in the digital forensics expert, seen on the analysis that the two tools basically exploit the same contexts, but each with their needs.*

Resumo. *Com as proporções alcançadas por meio da tecnologia, tudo em um mundo informatizado funciona a base de dispositivos de armazenamento e desenvolvimento de software, interligados a um único ponto: a tecnologia. Com esta atuando de forma tão imponente no mundo, nos deparamos com criminosos que a usam para cometer delitos, e desta forma torna-se primordial a presença da perícia forense computacional. O presente artigo tem como objetivo expor os procedimentos realizados da perícia forense computacional para obtenção de evidências em arquivos de um dispositivo de armazenamento, utilizando as ferramentas Helix e Forensic Toolkit. A metodologia utilizada para o desenvolvimento do trabalho foi através de pesquisas bibliográficas em livros e monografias. O trabalho evidenciou que o Helix e Forensic Toolkit são duas ferramentas importantes ao perito forense digital, visto na parte de análise que as duas ferramentas exploram basicamente os mesmos contextos, porém cada uma com suas necessidades.*

1. Introdução

Com o avanço tecnológico em ferramentas para invasão de sistemas, os crimes virtuais obtiveram força e, conseqüentemente, êxito nos ataques efetuados. Para prevenir e até mesmo extinguir os ataques virtuais, peritos especializados utilizam técnicas forenses como forma de combate. Visto que a perícia forense aplicada à computação é ligada à investigação de crimes cibernéticos colhendo dados para identificação, análise e documentação, com a finalidade de obtenção de evidências digitais. (SOUZA, 2011).

Segundo Eleutério e Machado (2011), a computação forense é a ciência que usa técnicas especializadas, para coletar e analisar dados digitais de um ou mais computadores suspeitos de serem utilizados em um crime virtual. Porém existem etapas que servem para combater supostas ameaças em vários tipos de dispositivo de armazenamento. Deste modo, existem procedimentos em casos específicos de análise de mídia de armazenamento digital

que devem ser seguidos pelo perito para assegurar que a evidência não seja comprometida, substituída ou perdida. (FREITAS, 2006).

Relatadas de forma sucinta no trabalho como quatro fases: preservação; extração; análise e formalização.

2. Aporte Teórico

2.1. Investigação Forense Computacional

Segundo Pereira (2010 apud FARIA, 2011, p.32), diferentemente das provas físicas pertinentes aos crimes convencionais, as comprovações que são encontradas em mídias magnéticas são digitais, podendo existir de diversas formas como: arquivos, dispositivos, fragmentos de logs e outros indícios residentes em uma mídia que podem estar relacionados, criando uma evidência que indique a ocorrência de um crime. O processo de investigação da perícia computacional, citado por Faria (2011), ocorre de forma cuidadosa, procurando preservar as características originais para que não haja interferência alguma nas evidências do ato ilícito.

De acordo com Rodrigues e Foltran (2010 apud FARIA, 2011, p.32), o processo investigativo da forense computacional deve assegurar a integridade dos vestígios coletados, entretanto devido à volatilidade das evidências eletrônicas essa tarefa é considerada difícil, deste modo o perito forense deve seguir procedimentos e protocolos reconhecidos pela comunidade científica. No qual deve detalhar e revisar a documentação desenvolvida para que evite erros durante a investigação.

2.2. Procedimentos aplicados a Perícia Forense Computacional

Freitas (2007 apud MELLO et al., 2011, p. 27) afirma que a perícia forense possui quatro métodos básicos e que todas as evidências devem ser:

- Identificadas
- Preservadas
- Analisadas
- Apresentadas

Para uma boa execução da perícia forense computacional segundo Eleutério e Machado (2011), existem quatro fases primordiais a serem cumpridas: Preservação, Extração, Análise e Formalização. Almeida (2011) descreve essas etapas como:

- **Preservação:** Deve isolar a área; identificar equipamentos; coletar evidências.
- **Extração:** Nesta fase, deve-se identificar extrair e documentar os dados relevantes a fim de apreender os objetos que tiverem relação com o fato.
- **Análise:** Os dados transformam-se em informações.
- **Formalização:** Deve-se redigir o laudo; anexar às evidências e documentos.

Toda evidência encontrada precisa ser documentada para validação. Para isso, segundo Mello, Silva e Tolentino (2011), afirmam que existem duas separações por prioridade das evidências (irrelevante e relevante), onde cada uma dessas evidências é usada como provas no tribunal.

A apresentação da análise é feita através do laudo técnico em que devem constar os fatos; as evidências; os procedimentos e os resultados. O laudo terá que ser o mais claro

possível e objetivo de forma que apresente as ideias mais formais.

3. Fases da Perícia Forense Computacional

3.1. Preservação

Assim como em um local de crime convencional cujas provas existentes devem ser preservadas, Almeida (2011) relata que os dados do material enviado para exames forenses jamais devem ser alterados. Newkamp (2007 apud GONÇALVES et al., 2012. P.11), relata que a preservação ou coleta de dados, é a etapa em que devem ser identificadas e processadas as evidências.

O método utilizado para a proposta do trabalho, citado por Almeida (2011), é a chamada técnica de dump, ou gerador de imagem, que consiste na duplicação de discos feita bit a bit, ou seja, um processo de cópia dos dados encontrados no dispositivo, originando assim uma reprodução exata do disco. Almeida (2011) afirma que o método de cópia bit a bit dos dados é a mais segura, pois é feito uma cópia real do dispositivo.

A proposta nessa fase foi à utilização de duas ferramentas forenses, o Helix e Forensic Toolkit (FTK). O Helix permite acessar os dados de forma somente leitura e têm o comando .dd (Extensão do arquivo, duplicar disco) utilizado para criar a imagem do dispositivo com uma cópia fiel. Já o Forensic Toolkit a segunda ferramenta, permite também realizar a cópia dos dados, gerando assim outra imagem com formato.001 (.dd).

Após o término da fase da preservação, o dispositivo deve ser lacrado e guardado em um local apropriado até que haja a autorização por parte da justiça permitindo o seu descarte. (ELEUTÉRIO E MACHADO, 2011).

3.2. Extração

Almeida (2011) relata que a fase de extração consiste na recuperação e organização das informações contidas na cópia da fase anterior.

A extração é uma etapa importante para o processo investigativo, pois as análises serão realizadas a partir de seu resultado e, de acordo com Almeida (2011), ao examinar a imagem criada, é importante que a extração dos dados seja feita de forma minuciosa.

Baseado em métodos de busca, Almeida (2011) define um conjunto de arquivo por nomes, acessos protegidos e manipulados pelo sistema operacional, por armazenar arquivos como sequência de bytes e organizar dentro de um diretório, gerenciando nomes, conteúdos de acesso, data e hora da última modificação. Causando assim felicidade em buscar conteúdos.

Outra técnica que Almeida (2011) cita para facilitar a fase da extração é pesquisar o conteúdo de um dispositivo por palavras-chave, extensão ou permissões de acesso. Pois a pesquisa por palavras-chave é um meio eficiente para encontrar as evidências necessárias para elaboração de laudo. Diante disso, proponha-se utilizar as mesmas ferramentas que a fase de preservação, pois atendem as necessidades descritas.

3.3. Análise das Evidências

O objetivo da análise das evidências, segundo Pereira (2010 apud FARIA 2011, p.37) é examinar dados e separar as informações relevantes.

Almeida (2011) relata que para analisar o conteúdo de arquivos extraídos da fase anterior, um dos métodos é utilizar filtro de arquivos para eliminar da análise àqueles que não

são importantes para a investigação, mas extrair os dados relevantes somente não é o suficiente, pois segundo Sá (2013), o perito forense deve interpretar as informações de forma correta.

A etapa de análise, segundo Sá (2013), afirma que deve identificar características que indiquem relações com a área do crime, como pessoas, e-mails, telefones, locais, ou seja, expor o que foi buscado na fase da extração.

Logo após a criação de imagem houver fixado as provas do sistema (fase 3.1) e extraído todos os conteúdos relevantes dos dados (fase 3.2), o perito pode então analisar os processos por vários métodos um deles é por extensão, como por exemplo: .doc, .mp3, .avi, .jpg, .txt, entre outros.

Deste modo Almeida (2011) relata que o material, seja um pen drive, um disco rígido ou um cartão de memória, não armazena somente o conteúdo de seus arquivos e por isso, deve haver uma atenção para o correto manuseio do material onde deve ser livre do calor excessivo, da alta umidade etc.

Desta forma, a etapa de análise requer utilizar novamente as ferramentas Forensic Toolkit e o Helix para expor os métodos encontrados.

3.4. Formalização

A formalização ou laudo técnico consiste no último processo da perícia forense computacional, descrita por Freitas (2003 Apud SÁ, 2013, p.15) sendo um relatório gerado por algumas ferramentas forense automaticamente ou a próprio punho pelo perito, onde é relatada toda a análise da investigação. O laudo é destinado às pessoas leigas e, por isso, a linguagem técnica deve ser simples, para que todos possam compreender.

O perito deve utilizar análises gráficas e visuais com o objetivo de facilitar a compreensão do crime para demonstrar como ocorreu. Caso o laudo não for entendido pelos julgadores, pode ser requerido que seja novamente escrito e até mesmo ser pedido à troca do perito.

O laudo constatará com conclusões tomadas após minuciosas investigações feitas nas fases anteriores (3.1, 3.2 e 3.3), detalhando o que foi investigado, como será provada a veracidade dos artefatos e as devidas conclusões tomadas.

Mediante ao prazo do laudo pericial, é estimado no prazo máximo de 10 dias, podendo ser prorrogado em casos excepcionais a requerimento dos peritos (QUEIROZ E VARGAS, 2010 apud MELLO, SILVA E TOLENTINO, 2011).

Deste modo o laudo pericial nada mais é que a conclusão da perícia forense computacional no caso investigado.

4. Métodos

No campo da perícia forense computacional, peritos devem saber quais os passos a seguir para que nenhum dano ao equipamento utilizado ocorra, e desse modo o trabalho deixou claros os passos para preservar o material encontrado no estado de pesquisa. O mesmo foi desenvolvido em duas etapas distintas até a obtenção dos resultados.

Na primeira etapa foi feito o levantamento das principais ideias sobre o funcionamento das fases e aspectos das técnicas forenses. A segunda etapa teve como objetivo, a aplicação de técnicas contidas no contexto, comprovando através da teoria e de ferramentas o levantamento geral do trabalho, proporcionando dados comparativos das ferramentas e uma conclusão para obter-se um laudo sob o suposto crime concluído.

Para atingir os objetivos práticos deste trabalho, foi usado um pen drive para análise forense e as ferramentas forenses, Helix para sistema operacional UBUNTU e Forensic Toolkit para sistema operacional WINDOWS. E o OpenPuff para analisar arquivos com esteganografia.

Para realizar a montagem do objeto de pesquisa, foram inseridos arquivos com vários tipos de extensões dentro do pen drive e em seguida formatados no modo de formatação rápida e formatação completa. Com a finalidade de verificar se ao término as ferramentas forenses conseguem visualizar ou até recuperar arquivos deletados.

Os testes reais realizados no pen drive, contiveram diferentes tipos de arquivos para obter melhor resolução na conclusão do trabalho, sendo divididos por extensões.

A escolha das ferramentas Helix, Forensic Toolkit e OpenPuff foram selecionadas a fim de comparar os resultados obtidos pelas mesmas e analisar qual a melhor em determinados quesitos de um perito forense computacional. As ferramentas foram escolhidas por se tratarem de ser uma das mais conhecidas na área de forense.

Para execução do objeto de pesquisa foi exemplificado as fases de análise forense da seguinte forma:

A realização dos procedimentos na fase da preservação, foram usados as ferramentas Helix, que gerou uma imagem exata do pen drive apreendido com o nome forensehelix.dd. E o Forensic Toolkit criou outra imagem do mesmo pen drive com o nome forenseftk.001.

Na fase da extração foi examinada as imagens forensehelix.dd. e forenseftk.001, mantendo o material original intacto. Para isso, o Helix fez a leitura dos dois arquivos criados, uma sendo a imagem por ele próprio gerado (forensehelix.dd) e da imagem criada pelo Forensic Toolkit (forenseftk.001) criada na fase anterior. E o Forensic Toolkit realizou o mesmo procedimento, leu a própria imagem criada (forenseftk.001) e da imagem (forensehelix.dd) criada no Helix na fase anterior.

Após cada imagem ser devidamente criada e extraída, a próxima fase requer analisar as evidências e para isso cada imagem criada foi lida e analisada por sua ferramenta padrão e pela outra ferramenta, ou seja, o Helix fez a análise da imagem forensehelix.dd e também da imagem forenseftk.001 criada pelo Forensic Toolkit. E o Forensic Toolkit fez o mesmo, analisou a imagem forenseftk.001 e também analisou a imagem forensehelix.dd criada no Helix. Tendo assim a finalidade de comparar qual ferramenta conteve o maior número de evidências encontradas.

O conteúdo que abrange a fase da formalização requer a criação de um laudo pericial, deste modo foi criado um laudo com base nas análises feitas da investigação.

Deste modo, Eleutério e Machado (2011) afirmam que um laudo pericial tem uma estrutura própria, formada geralmente pelas seguintes seções: preambulo, histórico, material, objetivo, considerações técnicas, exames, conclusões:

A partir desse tópico, foi criado um laudo pericial, abrangendo os tópicos acima, com as devidas informações baseadas na análise das imagens realizadas em cada fase.

5. Resultados

Inicialmente obteve-se o primeiro resultado utilizando a formatação rápida, pode-se concretizar que arquivos formatados estavam visíveis no modo de análise do dispositivo deixando vestígios dos arquivos e a formatação completa não deixa vestígios de nenhum arquivo deletado, pois apaga literalmente tudo que contém dentro do pen drive.

Na fase da preservação, obteve-se que os resultados foram balanceados nas duas ferramentas, pois o Helix criou a imagem pelo modo tradicional do terminal no UBUNTU com o comando: dc3dd if=/dev/sd1 of=home/forensehelix.dd progress=on hash=md5 log=forensehelix.log conv=noerror. E o Forensic Toolkit criou a imagem pelo próprio *software*, seguindo os passos necessários e mais claros que a ferramenta em WINDOWS proporciona. Ressaltando que todas as imagens criadas foram utilizadas o mesmo ambiente e para cada imagem criada foi gerado automaticamente uma MD5.

A fase de extração não foi tão balanceada em relação às ferramentas quanto à fase da preservação, pois nessa fase o Helix mostrou maior desenho na coleta de dados de ambas as imagens criadas. Visto que para extração é importante colher apenas informações relevantes e de importância para o caso.

Utilizando a ferramenta Helix na extração das imagens forensehelix.dd e forensftk.001, foi possível verificar que a ferramenta extraiu o maior número de informações relevantes, como data de criação, datas de acesso, nomes, tamanhos, diretórios entre outras. E utilizando a ferramenta *Forensic Toolkit* não possível obter os mesmos resultados, pois a ferramenta não atende tamanhas necessidades.

Na fase de análise das evidências, novamente a ferramenta Helix mostrou ter maior desenho em alguns recursos importantes para a análise forense.

Para análise de figura, as duas ferramentas conseguiram abrir e ler normalmente os arquivos, em qualquer tipo de extensão. Para arquivos executáveis, novamente as duas ferramentas conseguiram atingir o objetivo de leitura e análise do arquivo. Em arquivos do formato texto o Helix mostrou ser mais complexo, pois foi possível abrir e analisar normalmente, já a ferramenta *Forensic Toolkit* mostrou algumas dificuldades em abrir determinadas extensões onde aparenta erros na abertura do arquivo.

Para áudio o Helix deixou claro que é possível abrir e analisar qualquer tipo de áudio, e utilizando a ferramenta *Forensic Toolkit*, não foi possível abrir e nem analisar algumas extensões específicas de áudio. Para vídeos as duas ferramentas mostrou ter o mesmo nível de compatibilidade e análise. Para arquivos deletados o Helix mostrou estar á frente apenas no quesito de detalhes importantes ao perito, como datas, nomes, diretórios etc, visto que através de nenhuma das duas ferramentas utilizadas foi possível recuperar arquivos deletados.

Para arquivos com esteganografia, o Helix mostrou ser uma ótima ferramenta na análise forense, pois conseguiu distinguir uma figura e um áudio com esteganografia de uma figura e um áudio comum, através de uma análise no modo hexadecimal, e utilizando a ferramenta *Forensic Toolkit*, não possível analisar que os arquivos continham nenhum tipo de esteganografia. Como mostra (Figura 1).

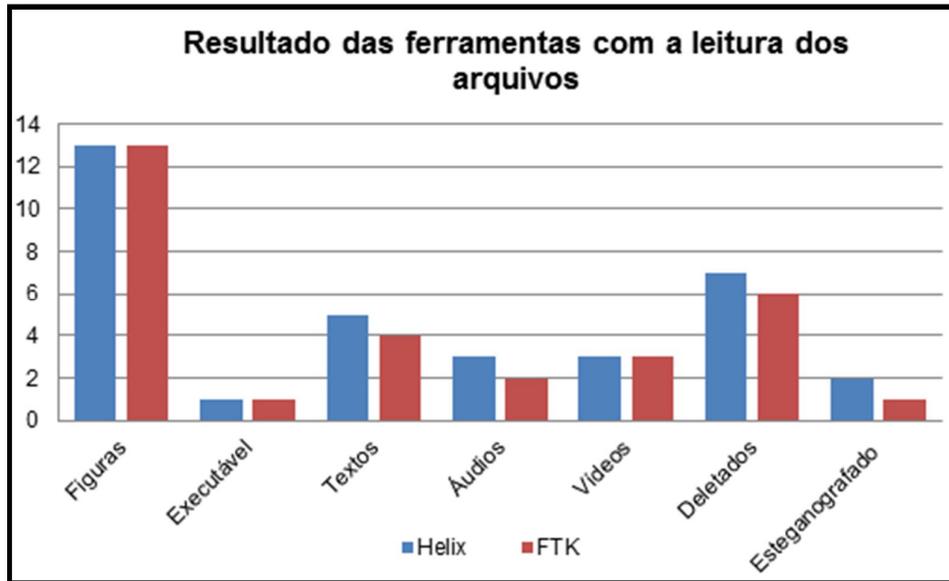


Figura 1. Resultado das ferramentas utilizadas

A fase da formalização levou a conclusão das análises feitas no dispositivo com a ferramenta que mostrou ter o maior desempenho no trabalho, a fim de colocar no papel e comprovar a evidência encontrada do caso relatado. Nesta fase o objetivo era que cada ferramenta gerasse automaticamente o seu próprio laudo, como o Helix e o Forensic Toolkit possuem essa opção automática, foi criado manualmente um laudo pericial abrangendo todas as informações da análise feita, a fim de expor os relatos encontrados pelo perito que comprovam o crime.

6. Considerações Finais

O trabalho por ser um tema de grande escassez e até mesmo incompleto em objetos de pesquisa abordou uma das vertentes da área forense computacional digital, obter evidência em dispositivos. Com esse intuito, foram utilizadas ferramentas forenses em dois tipos de sistemas operacionais, o Windows e Linux, por serem os sistemas operacionais mais utilizados.

O trabalho concluiu qual o melhor tipo de formatação para o perito encontrar evidência em um dispositivo. Como relatado, a formatação rápida deixou vestígios de arquivos deletados dentro do pen drive e a formatação completa apagou literalmente os arquivos que estavam dentro o pen drive.

Detalhes foram vistos em cada plataforma. Na plataforma Linux, utilizando o Helix, a ferramenta conseguiu realizar todas as fases forenses e alcançar a expectativa do trabalho, pois criou, analisou e concluiu as análises das imagens. O único problema foi que a ferramenta Helix não recuperou arquivos deletados encontrados dentro do dispositivo, pois para esse tipo de técnica é preciso o estudo de outras ferramentas forense. O Helix além de ser gratuito provou que é uma ótima ferramenta para análise de arquivos com esteganografia, tanto para figuras quanto para áudios.

E a ferramenta Forensic Toolkit utilizada na plataforma WINDOWS realizou todas as fases, porém deixou a desejar em alguns procedimentos importantes para um perito forense como a não análise de arquivos com esteganografia.

Os arquivos lidos por cada ferramenta revelam que as duas ferramentas conseguem ler

sem nenhum tipo de problema qualquer extensão de figuras; a ferramenta Helix mostrou ter maior desempenho em arquivos texto; em áudios a ferramenta Helix novamente mostrou ter maior desempenho; em arquivos deletados as duas ferramentas conseguem visualizar, entretanto nenhuma delas consegue recuperá-los e arquivos com esteganografia o Helix tem mais desenvoltura na leitura.

E para a formalização do laudo pericial, foi feito com base na ferramenta que teve o melhor desempenho no decorrer do trabalho, pois o Helix conseguiu atingir todos os recursos precisos em uma análise forense.

7. Referências

- Almeida, R.N. “Perícia Forense Computacional”: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais. (2011). 48 folhas. monografia (Tecnólogo em Processamento de Dados) - Faculdade De Tecnologia De São Paulo. São Paulo. (2011).
- Eleutério, P. M. S; Machado, M.P. “Desvendando a Computação Forense”. 1. Ed. São Paulo: Novatec, (2011).
- Faria, R.F. “Analisando os riscos de uma invasão para testar o desempenho de um banco de dados”. (2011). 75 folhas. Trabalho de conclusão de curso. (Tecnólogo em Banco de Dados) – Centro Estadual De Educação Tecnológica “Paula Souza”, Faculdade De Tecnologia De Lins. Lins. (2011).
- Freitas, A. R. “Pericia Forense Aplicada à Informática” Ambiente Microsoft. 1. Ed. Rio de Janeiro: Brasport, (2006).
- Gonçalves, M. et al., Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas. “Net”. Jaciara-Mato Grosso, nov. (2012), <<http://www.eduvalesl.edu.br/site/edicao/edicao-74.pdf>> novembro.
- Sá, G.Z. “Avaliação de técnicas anti-forenses computacionais aplicadas a registros de sistemas Linux”. (2013). 59 folhas. Trabalho de conclusão de curso. (Graduação em Tecnologia em Sistemas para Internet) - Universidade Tecnológica Federal do Paraná (UTFPR), Campo Mourão.
- Souza, R. R de. Revista Tecnologias em Projeção. “Bem-estar percebido sobre funcionalidades e design de aparelhos celulares” dezembro (2011), <<http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/download/167/148>> novembro.
- Tolentino, L. C.; Silva, W.; Mello, P. Revista Tecnologias em Projeção. V.2. “A Perícia Forense Computacional” dez. (2011), <<http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/download/168/149>> novembro.