

CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA

CAPITÃO DE CORVETA (T) MARIA REJANE LEITE DO AMARAL

**ANÁLISE COMPARATIVA QUANTO AO DESEMPENHO DOS SOFTWARES DE
FORENSE DIGITAL IPED E FTK NA RECUPERAÇÃO DE DADOS EXCLUÍDOS
EM DISPOSITIVOS DE ARMAZENAMENTO DE INFORMAÇÕES DIGITAIS**

**Brasília
2019**

CAPITÃO DE CORVETA (T) MARIA REJANE LEITE DO AMARAL

**ANÁLISE COMPARATIVA QUANTO AO DESEMPENHO DOS SOFTWARES DE
FORENSE DIGITAL IPED E FTK NA RECUPERAÇÃO DE DADOS EXCLUÍDOS
EM DISPOSITIVOS DE ARMAZENAMENTO DE INFORMAÇÕES DIGITAIS**

Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais apresentado ao Centro de Instrução de Guerra Eletrônica como requisito para obtenção do Grau de Pós-Graduação *Lato Sensu*, nível de especialização em Guerra Cibernética.

Orientador: Cap VASCONCELLOS

Coorientador: 2º Sgt Com Vinícius Emiliano dos Santos

**Brasília
2019**

Ficha catalográfica

Deve ser feita por bibliotecário.
Tamanho fixo de 7,5 x 12,5 cm

Ficha Catalográfica Elaborada pela Biblioteca
do Centro de Instrução de Guerra Eletrônica (CIGE)
Bibliotecária Responsável: 2º TenThaís Moraes CRB1/1922

M314e

Leite do Amaral, Maria Rejane

Análise comparativa quanto ao desempenho dos softwares de forense digital IPED e FTK na recuperação de dados excluídos em dispositivos de armazenamento de informações digitais. / Maria Rejane Leite do Amaral – Brasília, 2019. 61f.; il.

Trabalho de conclusão apresentado ao Curso de Guerra Cibernética para Oficiais – Centro de Instrução de Guerra Eletrônica, Brasília, 2019.

Bibliografia: f. 59-61.

1. Bloqueio Eletrônico. 2. Sistema Rádio Digital Troncalizado. I Marcelino, Thiago. da Silva. II. Centro de Instrução de Guerra Eletrônica. III. Título.

CDD355

CAPITÃO DE CORVETA (T) MARIA REJANE LEITE DO AMARAL

ANÁLISE COMPARATIVA QUANTO AO DESEMPENHO DOS SOFTWARES DE FORENSE DIGITAL IPED E FTK NA RECUPERAÇÃO DE DADOS EXCLUÍDOS EM DISPOSITIVOS DE ARMAZENAMENTO DE INFORMAÇÕES DIGITAIS

Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais apresentado ao Centro de Instrução de Guerra Eletrônica como requisito para obtenção do Grau de Pós-Graduação *Lato Sensu*, nível de especialização em Guerra Cibernética.

Aprovado em: 20 de novembro de 2019.

Vasconcellos - Cap
Orientador

Vinícius Emiliano dos Santos - 2º Sgt Com
Coorientador

Nome Completo do membro
Membro da comissão de avaliação

Nome Completo do membro
Membro da comissão de avaliação

**Brasília
2019**

Dedico este trabalho integralmente ao Senhor Deus que com sua graça e misericórdias permitiu-me concluí-lo. Assim, expresso minha alegria por meio de sua Palavra que diz: “Então a nossa boca se encheu de riso e a nossa língua de cântico; então se dizia entre os gentios: Grandes coisas fez o SENHOR a estes. Grandes coisas fez o SENHOR por nós, pelas quais estamos alegres.” (BÍBLIA, Salmos, 126-2:3).

AGRADECIMENTOS

Louvarei ao SENHOR em todo o tempo porque o busquei e Ele me respondeu e me livrou dos meus temores.

Na minha necessidade, clamei ao SENHOR e Ele salvou-me de todas as minhas angústias. Eu vi que o SENHOR é bom e bem-aventurado é aquele que Nele confia.

Também agradeço aos instrutores do Centro de Instrução de Guerra Eletrônica pelo carinho, atenção, esmero e espírito de corpo, demonstrados cotidianamente no trato com os alunos. Era visível o entusiasmo, o esforço e a preocupação em fazer todos chegarem juntos ao coroamento do Curso de Guerra Cibernética para Oficiais 2019, que é a formatura e o recebimento do brevê de conclusão.

A esses bravos e incansáveis militares e a toda tripulação do Centro de Instrução de Guerra Eletrônica, todo o meu respeito e admiração por terem sido BRAÇO FORTE MÃO AMIGA ao longo dessa desafiadora jornada. O Exército Brasileiro é mais forte por tê-los em suas trincheiras. Bravo Zulu!

Uns confiam em carros e outros em
cavalos, mas nós faremos menção do
nome do SENHOR nosso Deus.
Uns encurvam-se e caem, mas nós nos
levantamos e estamos de pé.
BÍBLIA, Salmos, 20-7:8.

RESUMO

Leite do Amaral, Maria Rejane. Análise comparativa quanto ao desempenho dos softwares de forense digital IPED e FTK na recuperação de dados excluídos em dispositivos de armazenamento de informações digitais. Brasília, 2019.

A evolução tecnológica democratizou o acesso às tecnologias e conseqüentemente à Informação, possibilitando a inclusão de mais e mais pessoas no mundo digital. Paralelo a esse crescimento, também tem aumentado o número de crimes no mundo virtual. Para apoiar tecnicamente o Judiciário, surge a computação forense, um dos ramos mais tradicionais da Forense Digital, com o objetivo de recuperar a maior quantidade possível de arquivos excluídos, tendo em vista que a maioria das atividades periciais em computadores são voltadas para análise de mídias de armazenamento. Neste sentido, foram elencados para este trabalho, o software comercial *Forensic Toolkit* (FTK), desenvolvido pela empresa *AccessData*, e o software livre, Indexador e Processador de Evidências Digitais (IPED), desenvolvido pela Polícia Federal, a fim de verificar a eficiência de ambas as ferramentas forenses quanto a porcentagem de recuperação de arquivos excluídos, concluindo-se que, neste laboratório, o IPED foi aproximadamente 86% mais eficiente na recuperação de arquivos excluídos que o FTK.

Palavras-chave: Software livre. Computação forense. Recuperação de dados.

ABSTRACT

Technological evolution has democratized access to technologies and, consequently, to information, enabling the inclusion of more and more people in the digital world. Parallel to this growth, the number of crimes in the virtual world has also increased. To technically support the judiciary comes computer forensics, one of the most traditional branches of Forensic Digital, with the goal of recovering as many deleted files as possible, given that most computer forensic activities are focused on media analysis. of storage. For this purpose, the commercial software Forensic Toolkit (FTK), developed by AccessData, and the free software, Indexer and Digital Evidence Processor (IPED), developed by the Federal Police, were listed for this purpose, in order to verify the efficiency of both forensic tools for percentage of deleted file recovery, concluding that in this lab IPED was approximately 86% more efficient in recovering deleted files than FTK.

Keywords: Free software. Computer forensics. Data recovery.

LISTA DE ILUSTRAÇÕES

Figura 1: Digital in 2018 revela as estatísticas globais da Internet.....	1
Figura 2: Estatísticas dos Incidentes Reportados e Confirmados.....	2
Figura 3: Disco rígido como um planeta de dados.....	4
Figura 4: Disco rígido como um planeta de dados.....	9
Figura 5: Diretórios e arquivos gerados pelo IPED após indexação da imagem.....	14
Figura 6: Interface do IPED para análise da imagem.....	15
Figura 7: Interface do FTK após processamento da imagem.....	17
Figura 8: Preenchendo a mídia com zeros.....	24
Figura 9: Visualização da mídia.....	24
Figura 10: Criando uma imagem comAccessData FTK Imager 4.2.1.4.....	25
Figura 11: Selecionando a mídia física.....	25
Figura 12: Selecionando o drive da mídia.....	26
Figura 13: Selecionando o tipo de saída da imagem, no caso RAW (bit a bit).....	27
Figura 14: Atribuindo informações à imagem a ser gerada.....	28
Figura 15: Informando o local onde será salva a imagem, seu o nome e que será gerada em um único arquivo.....	28
Figura 16: Iniciando a geração da imagem.....	29
Figura 17: Finalização da tela de criação da imagem.....	30
Figura 18: Site de localização do IPED.....	31
Figura 19: Verificando a versão do Java.....	31
Figura 20: Configurando a quantidade de memória para uso do Java.....	32
Figura 21: Diretórios e arquivos extraídos pelo IPED.....	32
Figura 22: Arquivos de configuração do IPED.....	33
Figura 23: Visualizando o IPEDConfig.....	34
Figura 24: Executando o IPED.....	35
Figura 25: Processamento de indexação do IPED.....	36
Figura 26: Informação de término de indexação do IPED.....	36
Figura 27: Diretórios e arquivos gerados pelo IPED após indexação da imagem.....	37
Figura 28: Site para download do FTK - Forensic Toolkit.....	38
Figura 29: Acessando o FTK.....	39
Figura 30: Criando um case.....	39
Figura 31: Configurando a case.....	39
Figura 32: Inclusão da imagem na case.....	40
Figura 33: Tela de final de processamento da imagem pelo FTK.....	40
Figura 34: Diretórios e arquivos gerados pelo FTK.....	41
Figura 35: Interface do FTK.....	42
Figura 36: Tela do relatório gerado pelo FTK.....	43
Figura 37: Diretórios recuperados pelo IPED.....	44
Figura 38: Arquivos de vídeos recuperados pelo IPED.....	44
Figura 39: Arquivos de fotos recuperados pelo IPED.....	45
Figura 40: Arquivos de slides recuperados pelo IPED.....	45
Figura 41: Planilha recuperada pelo IPED.....	46
Figura 42: Sistema de arquivos da imagem.....	46

LISTA DE QUADROS

Quadro 1: Características das ferramentas selecionadas.....	6
Quadro 2: Configuração do laptop.....	8
Quadro 3: Base de dados.....	8
Quadro 4: Descrição da mídia de armazenamento.....	9
Quadro 5: Quantidade de arquivos recuperados pelo IPED.....	15
Quadro 6: Quantidade de arquivos com conteúdo exibido corretamente.....	16
Quadro 7: Quantidade de arquivos recuperados pelo FTK.....	17
Quadro 8: Quantidade de arquivos com conteúdo exibido corretamente pelo FTK...	18

LISTA DE GRÁFICOS

Gráfico 1: Quantidade de dados originais vs quantidade de dados recuperados pelo IPED.....	16
Gráfico 2: Quantidade de dados originais vs quantidade de dados recuperados pelo FTK.....	18
Gráfico 3: Comparativo entre IPED e FTK.....	20
Gráfico 4: Percentual de arquivos recuperados pelo IPED e FTK.....	21

SUMÁRIO

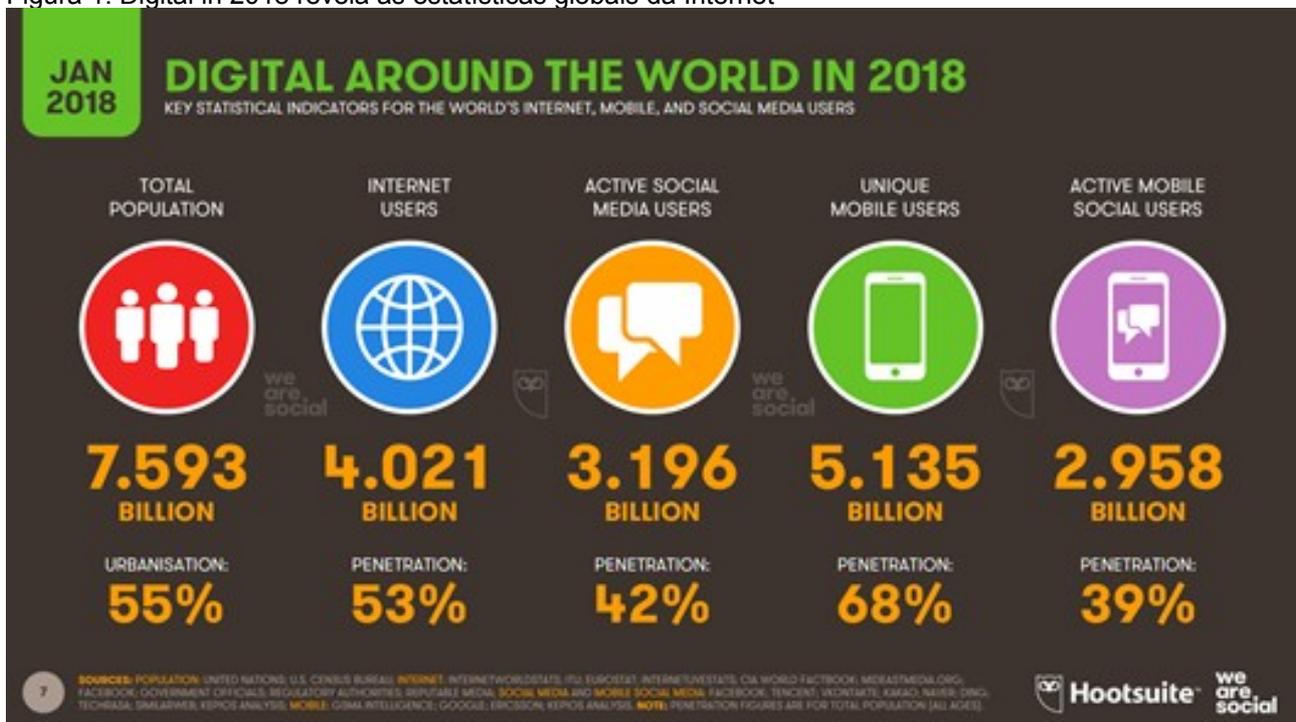
1 INTRODUÇÃO.....	1
1.1 DELIMITAÇÃO DO TEMA.....	3
1.2 PROBLEMA.....	4
1.3 HIPÓTESE.....	5
1.4 JUSTIFICATIVA.....	5
1.5 OBJETIVO GERAL.....	7
1.5.1 OBJETIVOS ESPECÍFICOS.....	7
1.6 MÉTODO DE PESQUISA.....	7
1.7 ESTRUTURA DO TRABALHO.....	10
2 SOBRE O IPED.....	11
2.1 SOBRE O FTK.....	13
3 RESULTADOS.....	14
3.1 RESULTADO APRESENTADO PELO IPED.....	14
3.2 RESULTADO APRESENTADO PELO FTK.....	17
4 CONCLUSÃO.....	19
5 TRABALHOS FUTUROS.....	22
REFERÊNCIAS BIBLIOGRÁFICAS.....	23
Apêndice A - Procedimentos executados desde a sanitização da mídia, criação e submissão da mesma para análise pelas ferramentas IPED e FTK.....	24
Apêndice B – Interface gráfica do FTK versão 7.1.0 e apresentação de um modelo de relatórios.....	43
Apêndice C - Telas da análise da imagem geradas pelo IPED.....	45

1 INTRODUÇÃO

Áreas como comunicação, ciência, economia, dentre outras, têm sido impulsionadas pela evolução tecnológica. Fato decorrente da democratização do acesso às tecnologias e conseqüentemente à Informação, possibilitando a inclusão de mais e mais pessoas no mundo digital (Própria autora, 2019).

O relatório *Digital in 2018*, divulgado pelos serviços online *Hootsuite* e *We Are Social*, informa que são mais de 4 bilhões de pessoas conectadas à rede, em relação a uma população global de 7,6 bilhões de seres humanos (Tecnundo, 2018), conforme demonstrado na figura 1.

Figura 1: Digital in 2018 revela as estatísticas globais da Internet

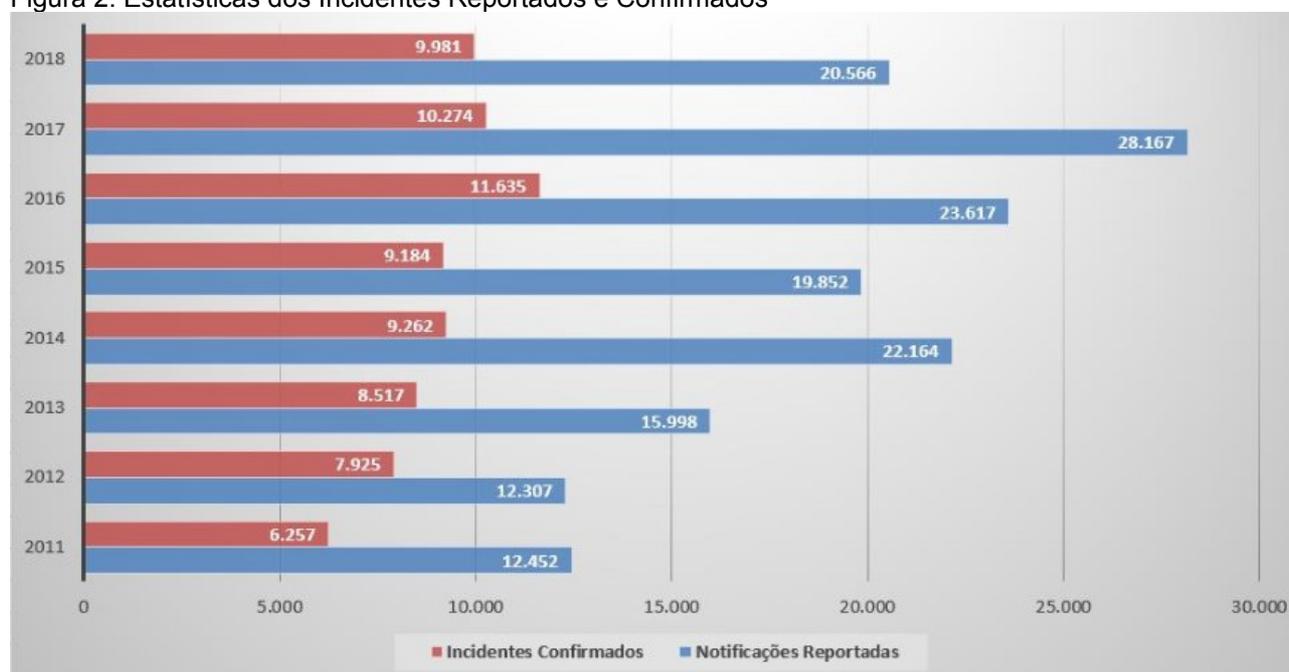


Fonte: Tecnundo, 2018.

Paralelo ao crescimento supracitado, também tem sido observado o aumento exponencial de incidentes da segurança das informações digitais (Própria autora, 2019). No que diz respeito ao Brasil, segundo GOMES (UOL, 2019), o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) divulgou relatório mostrando que, em 2018, foram reportados 20.566 eventos adversos, relacionados à segurança dos sistemas de computação ou das redes de computadores, que comprometeram a segurança digital na Administração Pública Federal. Desses eventos, 9.981 foram

confirmados (GOMES, UOL, 2019). A figura 2, apresenta a quantidade de eventos reportados e confirmados que ocorreram entre os anos de 2011 até 2018, relacionados a segurança digital na Administração Pública Federal.

Figura 2: Estatísticas dos Incidentes Reportados e Confirmados



Fonte: CTIR Gov, 2019.

Face ao exposto, percebe-se que assim como no mundo real, no digital também ocorrem crimes – os chamados crimes digitais ou cybercrimes ou crimes cibernéticos. Termos usados para crimes praticados em ambiente virtual (Própria autora, 2019). Segundo o conselho nacional de justiça, “apesar de ser um assunto relativamente novo, a legislação tem avançado com textos específicos para cada propósito” (AGÊNCIA CNJ DE NOTÍCIAS, 2018).

Contudo, segundo Galvão (2013, p. 15), “a computação segue trazendo novos desafios quase sempre sem a normatização e o amparo técnico e legal minimamente satisfatórios diante da complexidade que o seu uso exige”.

Enquanto o judiciário caminha para prover amparos jurídicos sobre os delitos relacionados à tecnologia, surge “a perícia forense em computação ou computação forense responsável por dar respostas ao judiciário em questões envolvendo sistemas computacionais, sem os objetos de investigação equipamentos, mídias, estruturas computacionais ou que tenham sido utilizados como meio em atividades sobre investigação. Envolve, pois, a obtenção e análise de informações digitais e/ou equipamentos, infraestrutura e mídias computacionais para o uso como evidências em

casos cíveis, criminais ou administrativos” (GALVÃO, 2013, p. 19).

Cabe ressaltar que “a computação forense é um dos ramos mais tradicionais da Forense Digital” que, por sua vez, “é a ciência responsável pela investigação forense de evidências tecnológicas”. Ela tem como objetivo a preservação, coleta, análise e apresentação de resultados de análise das evidências digitais”. A Computação Forense uma subárea da forense digital (ACADEMIA DE FORENSE DIGITAL, 2017).

Situações nas quais seja necessário o suporte da computação forense para procedimentos de recuperação de dados vão além do uso de ferramentas de recuperação; envolvem toda uma estratégia de suporte com foco na preservação de evidências, definição prévia de técnicas e ferramentas, coleta e análise de dados, primando pela integridade e pelo detalhamento dos processos utilizados, finalizando com um laudo ou parecer técnico sobre o processo. (GALVÃO, 2013, p. 20).

Contudo, tendo em vista que

a grande maioria das atividades periciais em computadores tem como objetivo a análise de mídias de armazenamento (discos rígidos internos e externos, pendrives CD, DVD, cartões de memória flash de vários tipos e a própria memória com suas informações voláteis armazenadas temporariamente) em processos de recuperação de arquivos (GALVÃO, 2013, p. 24)

este trabalho tem como objetivo recuperar dados excluídos em mídias de armazenamento utilizando, não sendo objeto desta pesquisa o detalhamento das fases que envolvem o exame forense em dispositivos de armazenamento de informações digitais (Própria autora, 2019).

Para a recuperação dos dados excluídos, dentre as ferramentas gratuitas e/ou comerciais existentes no mercado, foram selecionadas *Forensic Toolkit* (FTK), software comercial desenvolvido pela empresa *AccessData*, e o Indexador e Processador de Evidências Digitais (IPED), software livre, desenvolvido pela Polícia Federal (Própria autora, 2019).

1.1 DELIMITAÇÃO DO TEMA

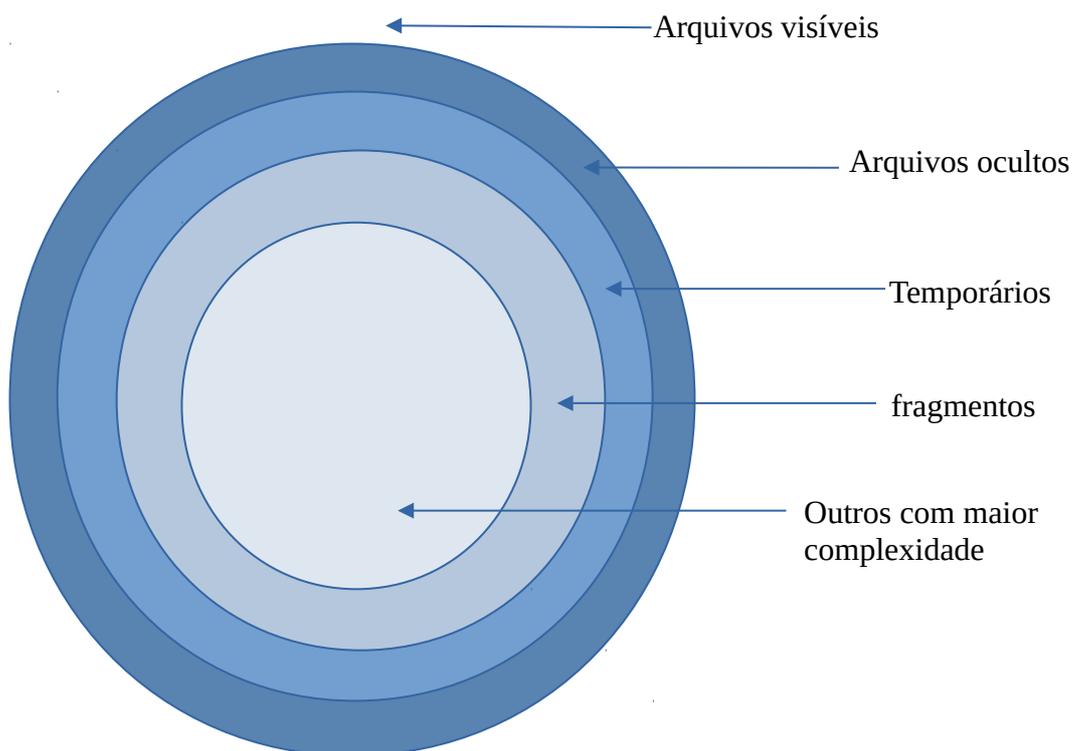
Análise comparativa da eficiência dos softwares para computação forense IPED e FTK quanto a porcentagem de recuperação de dados excluídos em dispositivos de armazenamento de informações digitais.

1.2 PROBLEMA

“Os dispositivos de armazenamento de dados digitais podem guardar muito mais informações do que as visíveis pelos usuários comuns. Isso ocorre basicamente devido ao tipo de organização dos dados dentro desses dispositivos” (ELEUTÉRIO; MACHADO, 2011, p. 62).

Conforme a figura abaixo, “os dados contidos em um disco rígido podem ser divididos em camadas” e as camadas mais internas do disco são mais difíceis de serem exploradas, conforme demonstrado na figura 3. “Os usuários comuns de computadores conseguem enxergar apenas a parte superficial” [...] os chamados arquivos visíveis, que podem ser visualizados com softwares como o Windows Explorer” (ELEUTÉRIO; MACHADO, 2011, p. 62).

Figura 3: Disco rígido como um planeta de dados



Fonte: ELEUTÉRIO; MACHADO, 2011.

“Ao apagar um arquivo de um computador,” [...] “o sistema operacional apenas altera o status do espaço de ocupado para livre (disponível)” (ELEUTÉRIO; MACHADO, 2011, p. 63) e

os dados referentes aos arquivos apagados continuam armazenados no disco rígido e podem ser recuperados por meio de técnicas específicas. Entretanto, esses dados também podem ser sobrescritos a qualquer momento pelo sistema operacional, uma vez que o espaço está disponível para utilização. Logo, conclui-se que, quanto mais recentemente um arquivo foi apagado, maiores são as chances de recuperá-lo, uma vez que será menor a probabilidade de sobrescrita do espaço utilizado no disco rígido por algum novo arquivo a ser gravado ou por alguma ação realizada pelo próprio sistema operacional (ELEUTÉRIO; MACHADO, 2011, p. 63),

concluindo-se que o tempo é um fator de extrema importância na forense digital.

Diante do exposto, qual a eficiência quanto a porcentagem de recuperação de arquivos excluídos, ao se utilizar o software livre IPED em relação a ferramenta comercial FTK?

1.3 HIPÓTESE

Por ser baseado em software livre, é possível o IPED ser mais eficiente na recuperação de dados excluídos em dispositivos de armazenamento de informações digitais, uma vez que por ser de código-fonte aberto tem maior probabilidade de receber adaptações/atualizações pela comunidade de interesse em relação a ferramenta comercial FTK, desenvolvida para funcionar dentro de um escopo para o qual foi projetada.

1.4 JUSTIFICATIVA

Diante da existência de uma gama de ferramentas voltadas para realizar forense computacional em mídias de armazenamento, sejam sob os termos da GNU *General Public License* ou comerciais, foram escolhidos o software comercial *Forensic Toolkit* (FTK), desenvolvido pela empresa *AccessData*, e o livre, *Indexador e Processador de Evidências Digitais* (IPED), desenvolvido pela Polícia Federal para serem submetidas a um laboratório de testes, a fim de se verificar qual obteve melhor eficiência quanto ao percentual de recuperação de dados excluídos em dispositivos de armazenamento digital.

O quadro 1 apresenta algumas das principais características e funcionalidades das ferramentas supracitadas.

Quadro 1: Características das ferramentas selecionadas

FERRAMENTAS FORENSES	CARACTERÍSTICAS	FUNCIONALIDADES
IPED	Alta escalabilidade	Análise integrada dos dados armazenados nos dispositivos digitais
	Arquitetura multithread	Cruzamento de informações
	Ideal para a análise de grande volume de dados	Detecção de nudez
	Interface intuitiva	Identificação de criptografia
	Multiplataforma (Windows, Linux e Mac OS)	Localização de palavras
	Portabilidade e processamento em batch	Rastreamento de locação e Recuperação de arquivos deletados
FTK	Fácil operação	Criação de filtros para gerenciamento de evidências relevantes
		Escaneamento de disco rígido para coleta de informações
		Gráficos e imagens
		Processamento e análise de documentos
		Recuperação de arquivos

Fonte: MERCADO EM FOCO.

1.5 OBJETIVO GERAL

Realizar uma análise comparativa entre as ferramentas IPED e FTK para se verificar a eficiência quanto a porcentagem de recuperação de informações excluídas em dispositivos de armazenamento de informações digitais.

1.5.1 OBJETIVOS ESPECÍFICOS

Ao objetivo geral agregam-se os seguintes objetivos específicos:

- 1) Delimitar uma amostra de base de dados que contemple arquivos de tipos diferentes;
- 2) Selecionar e sanitizar uma mídia para armazenamento;
- 3) Copiar a base de dados para a mídia sanitizada, após excluí-la;
- 4) Criar uma imagem da mídia, utilizando software forense que a preserve de possíveis alterações de escrita;
- 5) Submeter a imagem às ferramentas IPED e FTK;
- 6) Analisar a eficiência das ferramentas quanto a recuperação da base de dados; e
- 7) Apresentar os resultados.

1.6 MÉTODO DE PESQUISA

Essa pesquisa caracteriza-se por ser uma análise dos dados, com objetivo realizar uma comparação quanto ao desempenho de cada ferramenta no que se refere a recuperação de dados excluídos em uma mídia de armazenamento digital, dentro de uma abordagem qualitativa de interpretação das informações coletadas para encontrar resposta ao problema proposto.

Tem ainda como finalidade aplicada escolher a ferramenta mais adequada para realizar a referida recuperação em tais dispositivos, ainda que por meio do método hipotético-dedutivo, onde a hipótese apresentada possa ser confirmada ou refutada.

Para alcançar o objetivo geral, os dados foram coletados a partir da instalação e estudo das ferramentas IPED e FTK..

Esse trabalho, também, foi elaborado por meio de pesquisas as legislações, documentos, artigos e trabalhos de conclusão de curso.

Para alcançar o objetivo geral, foram excluídos todos os diretórios e respectivos arquivos do dispositivo, deixando-o vazio.

Quadro 4: Descrição da mídia de armazenamento

TIPO	CARACTERÍSTICAS
Dispositivo USB	Marca: Lexar Modelo: JDS75 Capacidade: 32GB Interfaces: USB 3.0 P/N: 1000-106 A S/N: 34302-32GBGA País de fabricação: CHINA

Fonte: ELEUTÉRIO; MACHADO, 2011

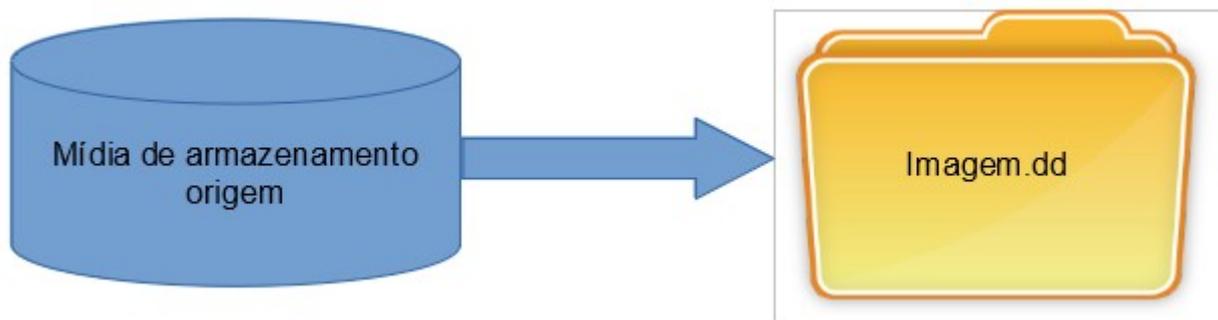
“Os dispositivos de armazenamento computacional são sensíveis e devem ser manuseados com cuidado”. Eles possuem características de “interesse para a computação forense”, tais como “fragilidade, facilidade de cópia, sensibilidade ao tempo de vida e sensibilidade ao tempo de uso” (ELEUTÉRIO; MACHADO, 2011, p. 51).

Segundo ELEUTÉRIO e MACHADO (2011, p. 54)

Devido à fragilidade e sensibilidade das mídias de armazenamento computacional, os exames forenses devem, sempre que possível, ser realizados em cópias fiéis obtidas a partir do material original. Assim, deve-se realizar a duplicação do equipamento original com uma das seguintes técnicas computacionais: espelhamento ou imagem. Para isso, devem ser utilizados equipamentos ou softwares forenses específicos.

Para este laboratório, a técnica utilizada foi a de imagem, quando, segundo Eleutério e Machado (2011, p. 56), os dados são copiados para arquivos, conforme demonstrado na figura 4, com a vantagem de “maior facilidade em replicar os dados, uma vez que são arquivos que podem ser copiados facilmente por qualquer sistema operacional”.

Figura 4: Disco rígido como um planeta de dados



Fonte: ELEUTÉRIO e MACHADO (2011).

Assim, para evitar algum processo de escrita durante a cópia, foi utilizada a ferramenta gratuita *AccessData FTK Imager*, desenvolvida pela *AccessData*, para Sistemas operacionais Windows XP/Vista/7/8/10, que suporta imagens forenses dos tipos AFF, DD, RAW, 001, E01 e S01¹.

Ao final do processo de criação da imagem, o programa apresenta o cálculo do *hash*, MD5, de 128 bits, e SHA1, de 160 bits, útil para o caso de verificações da integridade do conteúdo em processos investigatórios futuros.

Na fase de análise, o foco deste trabalho foi analisar comparativamente a eficiência de cada ferramenta em relação ao maior percentual de recuperação dos arquivos excluídos, bem como a exibição correta do conteúdo, conforme o tipo de cada arquivo.

A fase de formalização apresenta o resultado obtido na fase de análise.

No apêndice A são demonstrados os procedimentos executados, desde a sanitização da mídia até a submissão da imagem para análise pelas ferramentas IPED e FTK.

1.7 ESTRUTURA DO TRABALHO

No primeiro capítulo são apresentadas as definições e os conceitos gerais sobre computação forense, bem como o método de pesquisa e o laboratório utilizado.

No segundo capítulo são apresentadas as ferramentas IPED e FTK.

No terceiro capítulo é apresentada a análise dos resultados comparativos entre as ferramentas IPED e FTK.

Por fim, no quarto capítulo é apresentada a conclusão deste trabalho.

¹ Para obter informações sobre os formatos de arquivos de imagens forense, acesse <https://kb.digital-detective.net/display/HstExV4/Supported+Source+Data+Formats#SupportedSourceDataFormats-ForensicImageFileFormats>

2 SOBRE O IPED

Segundo MONTEIRO (2018), o “IPED é um indexador de evidências, de software livre desenvolvido pela Polícia Federal para tratar de uma grande quantidade de dados, organizando-os por tipos de informações”.

Foi desenvolvido em Java 64bits, tipo portable, conseqüentemente, não necessita ser instalado. Para bom desempenho do IPED, as configurações ideais são um computador com sistema operacional 64bits, java 64bits, 32GB de memória RAM e processador com 8 núcleos. As configurações mínimas são sistema operacional 64bits, java 64bits, 8GB de memória RAM e processador com 4 núcleos (TI FORENSE, 2019).

Segundo IPED – Manual (2019), o “programa linha de comando em java originalmente desenvolvido para indexar relatórios do FTK 1.8 (convertidos pelo AsAP3) e relatórios do FTK 3+.”, em sua versão 3.15.6, “apresenta diversas funcionalidades presentes em softwares forenses comerciais, servindo como alternativa eficiente e de código aberto na maioria dos casos”, como “em casos que necessitem de função de busca por palavras-chave ou recuperação de dados apagados”.

O principal arquivo de configuração da ferramenta é o IPEDConfig.txt. Lá pode ser configurado o cálculo de hash, indexação do conteúdo dos arquivos(indexFileContents), indexação do espaço não alocado (indexUnallocated), cálculo de assinatura (processFileSignatures), carving (enableCarving), expansão decontainers (expandContainers), dentre diversas outras opções comentadas no próprio arquivo (IPED – Manual, 2019).

Outro arquivo importante de configuração é o LocalConfig.txt onde são definidas configurações específicas do ambiente, como diretório temporário indexTemp, se o diretório temporário está em SSD, número de workers de processamento, e caminhos para as bases de hashes do IPED (NSRL do NIST), de pornografia infantil doLED, base de detecção de nudez do LED, e caminho para o TskDatamodel.jar compilado em sistemas Linux (IPED – Manual, 2019).

Segundo IPED – Manual (2019), quanto ao processamento de imagens, o IPED “é capaz de acessar o conteúdo de dispositivos físicos e imagens forenses gerados até o FTKImager 3.4.0.5, normalmente por meio da suíte forense *The Sleuthkit* (TSK) e Libewf, utilizados para acessar o conteúdo das imagens e decodificação dos sistemas de arquivos”, bem como há a funcionalidade de “extração de cenas de vídeos (enableVideoThumbs), a qual utiliza o software MPlayer. Os parâmetros da extração de cenas, como resolução, número de quadros extraídos, podem ser alterados no arquivo conf/VideoThumbsConfig.txt” (IPED – Manual, 2019).

No que diz respeito a detecção de nudez, há

um filtro "Imagens com Possível Nudez", que realiza um corte simplista de imagens com scoreNudez acima de 500, mas não é recomendado seu uso indiscriminado devido a falsos negativos, considere o uso da ordenação”.Nos

testes o algoritmo de detecção mostrou uma ótima relação precisão x cobertura comparativamente a outros softwares forenses comerciais e de código aberto (IPED – Manual, 2019).

Ainda sobre imagens, o IPED possui a função de georreferenciamento de Imagens, onde

imagens com informações de GPS nos metadados exif são renderizadas no painel "Mapa", permitindo visualizar sua localização de origem. Também foi incluído um filtro "Itens Georreferenciados" para facilitar a localização de itens contendo informações de GPS (IPED – Manual, 2019).

“Por meio do *Sleuthkit*, é realizada automaticamente a recuperação simples de arquivos apagados das tabelas de arquivos dos sistemas de arquivos” e também “é acessado o espaço não alocado, o qual é indexado e submetido a data carving otimizado pelas tarefas de processamento específicas do IPED” (IPED – Manual, 2019).

Quanto ao suporte a relatórios XML/UFDR do UFEDA,

o IPED exibe apropriadamente as categorias, itens e propriedades exibidos no UFEDReader. Logo, a ferramenta serve como alternativa em casos grandes inviáveis de analisar pelo UFEDReader, que é ineficiente. Além disso, as demais funções podem ser usadas em dados extraídos de celulares, como OCR, pesquisa em bases de *hashes*, detecção de nudez, etc, (IPED – Manual, 2019).

porém a “versão 3.15 do IPED atualmente não suporta relatórios UFDR segmentados (divididos)” (IPED – Manual, 2019).

“A categorização dos arquivos é realizada principalmente via análise de assinatura pela biblioteca Apache Tika (<http://tika.apache.org>). [...] “Além disso, a categoria dos arquivos pode ser refinada com base em qualquer propriedade, como caminho, tamanho, datas, deletado, etc, por meio do arquivoconf/CategoriesByPropsConfig.txt, que utiliza linguagem javascript para permitir flexibilidade nas definições” (IPED – Manual, 2019).

A detecção de arquivos criptografados “é realizada automaticamente para os arquivos dos tipos: pdf, office97 (doc, xls, ppt), office2007 (docx, xlsx, pptx),openoffice (odt, ods, odp), zip, rar, 7z e pst e os arquivos identificados como cifrados podem ser acessados por um filtro pré-configurado” (IPED – Manual, 2019).

Para a expansão de containers, é utilizada a biblioteca Apache Tika (<http://tika.apache.org>), que fornece suporte para zip, tar, ar, arj, jar, gzip, bzip, bzip2, xz, 7z, z,cpio, dump, formatos office, rtf e pdf. Caso se queira extrair imagens embutidas em PDFs, é necessário habilitar a opção processImagesInPDFs emconf/AdvancedConfig.txt (IPED – Manual, 2019).

Para o cálculo de múltiplos *Hashes*, “o software suporta os seguintes algoritmos de *hashes* criptográficos: md5, sha-1, sha-256, sha-512, edonkey” (IPED – Manual, 2019).

Para obter mais informações sobre outras funcionalidades do sistema deve-se consultar o manual.

2.1 SOBRE O FTK

Segundo ELEUTÉRIO e MACHADO (2011, p. 77), o FTK “reúne as principais funcionalidades para a realização de exames forenses em dispositivos de armazenamento de dados”.

Sua interface gráfica (Apêndice B) possibilita uma visão geral do conteúdo a ser analisado. “Das principais funcionalidades, é possível indexar dados, realizar Data Carving, recuperar arquivos e visualizar imagens, [...] entre outras” (ELEUTÉRIO; MACHADO 2011, p. 77).

“Ao identificar arquivos de interesse, é possível categorizá-los em *bookmarks*”. A ferramenta também possui “um módulo gerador de relatório (Apêndice B) que cria arquivos em *Hypertext Markup Language* (HTML)”, permitindo visualizar os resultados por meio de *browsers*” (ELEUTÉRIO; MACHADO 2011, p. 77).

É possível

criar imagens, processar uma variedade de tipos de dados, de várias fontes, desde dados do disco rígido a dispositivos móveis, dados de rede e armazenamento na Internet em um local centralizado, descriptografar arquivos, decifrar senhas, gerar relatórios e recuperar senhas de mais de 100 aplicativos. A ferramenta ainda possui biblioteca de *known file filter* (kff) com 45 milhões de *hashes*” (ACCESSDATA, 2019).

“O FTK é orientado por banco de dados, para evitar perdas em caso de falhas da GUI e os componentes do FTK são compartimentados, permitindo a continuidade do processamento dos dados sem interrupção (ACCESSDATA, 2019).

A versão do FTK utilizada neste trabalho é a versão 7.1, desenvolvida para a “” plataforma Windows nas seguintes versões Windows Server 2016; Windows Server 2012 R2; Windows 10 / 8.1 / 7 64-bit” (ACCESSDATA, 2019).

3 RESULTADOS

Conforme apresentado no item 1.6, em um dispositivo de 32GB foram armazenados 323 arquivos, distribuídos em 6 diretórios, totalizando 21GB em dados.

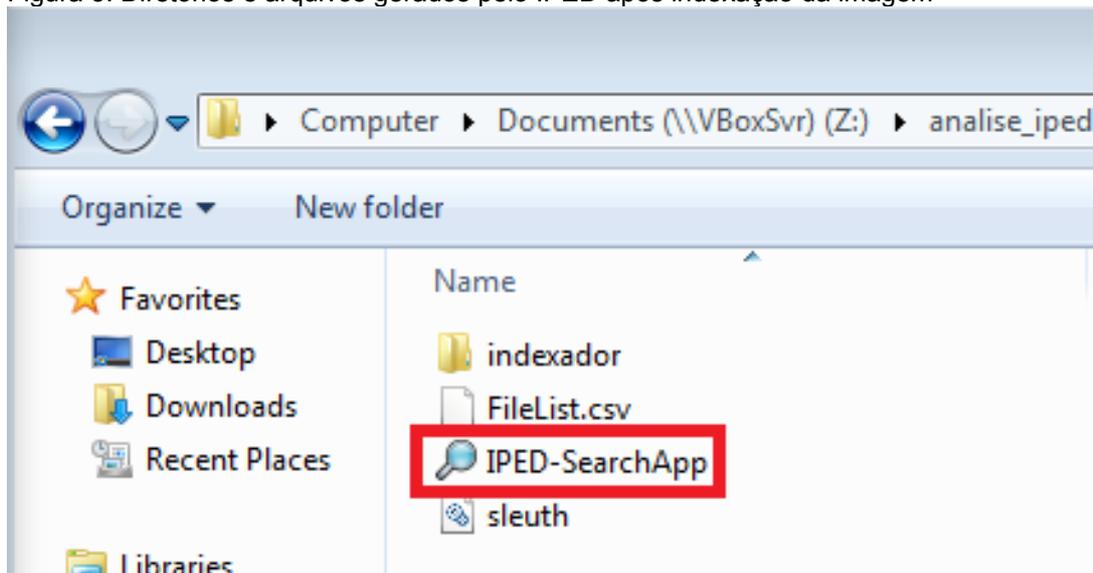
Para confirmar ou refutar a hipótese apresentada no item 1.3, todos os dados foram excluídos do dispositivo, sendo gerada uma imagem do mesmo, a qual foi submetida para análise pelas ferramentas forenses IPED e FTK, a fim de se verificar a eficiência quanto a porcentagem de recuperação de arquivos excluídos.

Face ao exposto, os seguintes resultados foram obtidos.

3.1 RESULTADO APRESENTADO PELO IPED

Ao finalizar o processo de processamento da imagem, o IPED gerar os diretórios e arquivos, conforme demonstrado na figura 5.

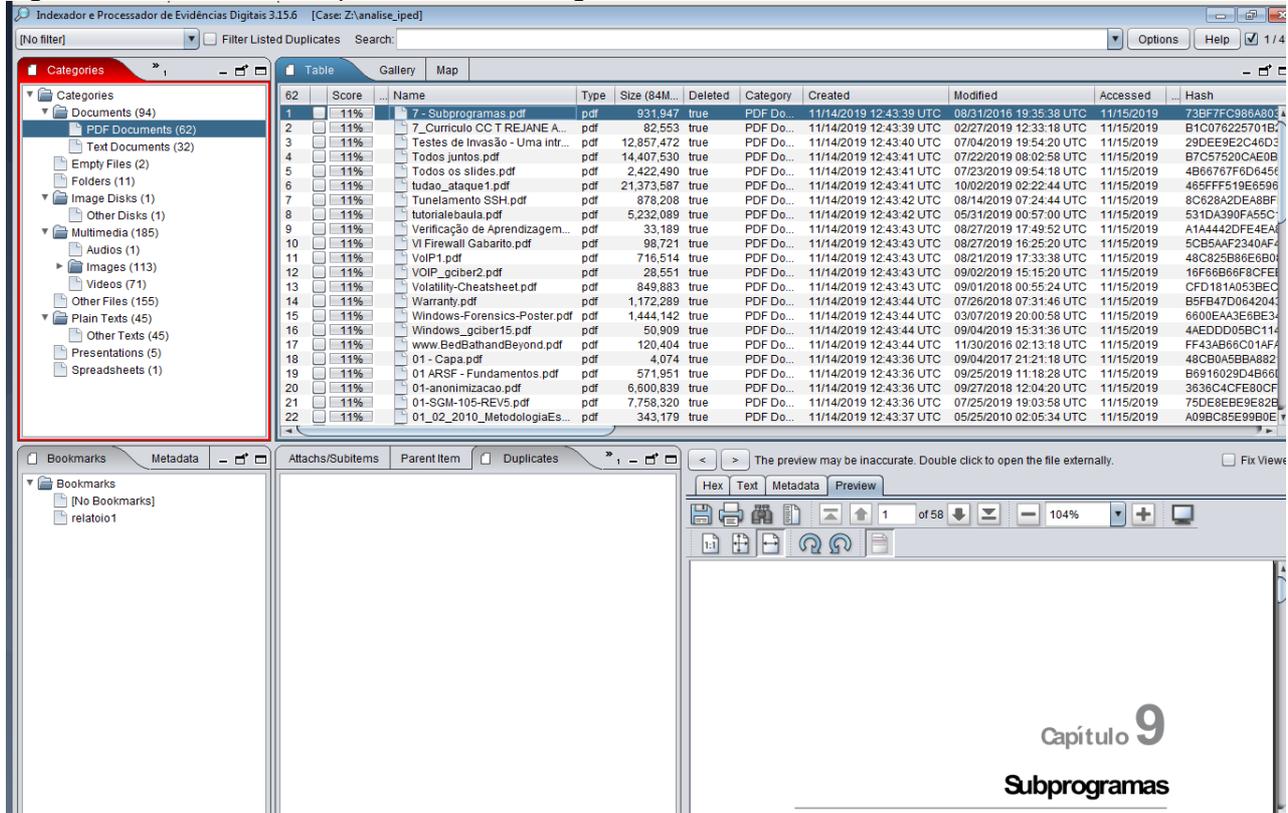
Figura 5: Diretórios e arquivos gerados pelo IPED após indexação da imagem



Fonte: Própria autora, 2019.

Ao abrir o programa IPED-SearchApp, o IPED apresenta a indexação da imagem, conforme demonstrado na figura 6, contendo os dados que foram interpretados e recuperados.

Figura 6: Interface do IPED para análise da imagem



Fonte: Própria autora, 2019.

Observa-se que o IPED conseguiu recuperar 279 arquivos dos 323 que originalmente existiam na mídia, conforme demonstrado no quadro 5, porém, dos 279 arquivos recuperados, somente 176 tiveram seus conteúdos exibidos corretamente, conforme demonstrado no quadro 6.

Quadro 5: Quantidade de arquivos recuperados pelo IPED

DIRETÓRIOS	QUANTIDADE DE ARQUIVOS RECUPERADOS
1) DOC	32
2) FOTOS	108
3) VIDEOS	71
4) PLANILHA	01
5) PDF	62
6) PPT	05
TOTAL	279

Fonte: Própria autora, 2019.

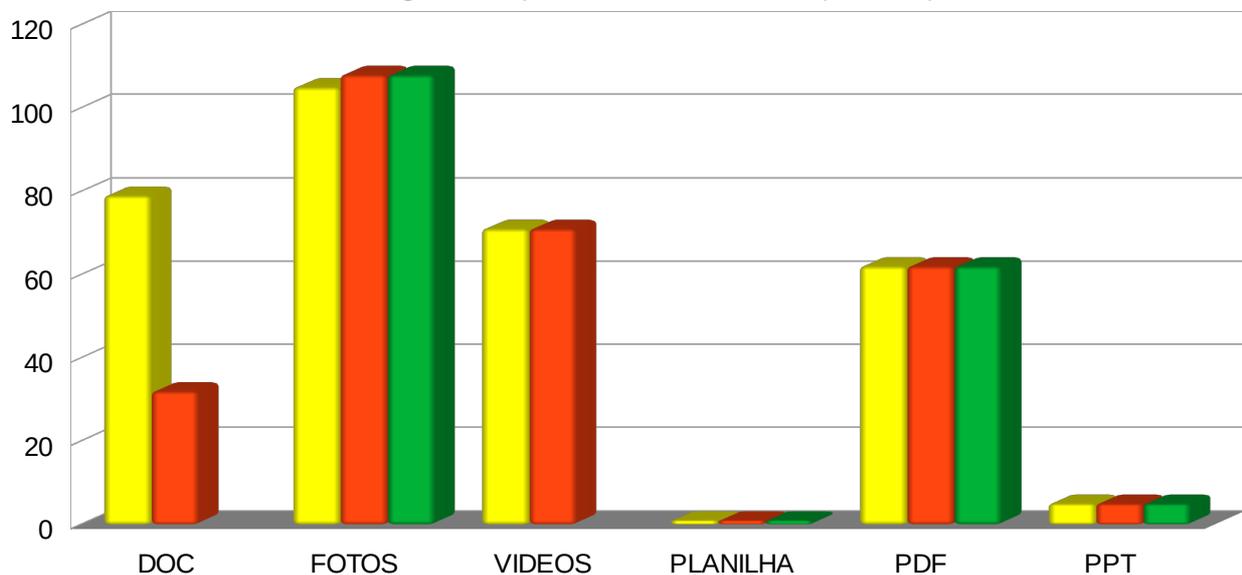
Quadro 6: Quantidade de arquivos com conteúdo exibido corretamente

DIRETÓRIOS	QUANTIDADE DE ARQUIVOS CUJO CONTEÚDO FOI VISUALIZADO CORRETAMENTE
1) DOC	0
2) FOTOS	108
3) VIDEOS	0
4) PLANILHA	01
5) PDF	62
6) PPT	05
TOTAL	176

Fonte: Própria autora, 2019.

O gráfico 1 demonstra em amarelo a quantidade de arquivos de existiam na mídia original, por tipo, em vermelho a quantidade de arquivos recuperados pelo IPED e em verde a quantidade de arquivos cujos conteúdos foram corretamente exibidos.

Gráfico 1: Quantidade de dados originais vs quantidade de dados recuperados pelo IPED



Legenda:

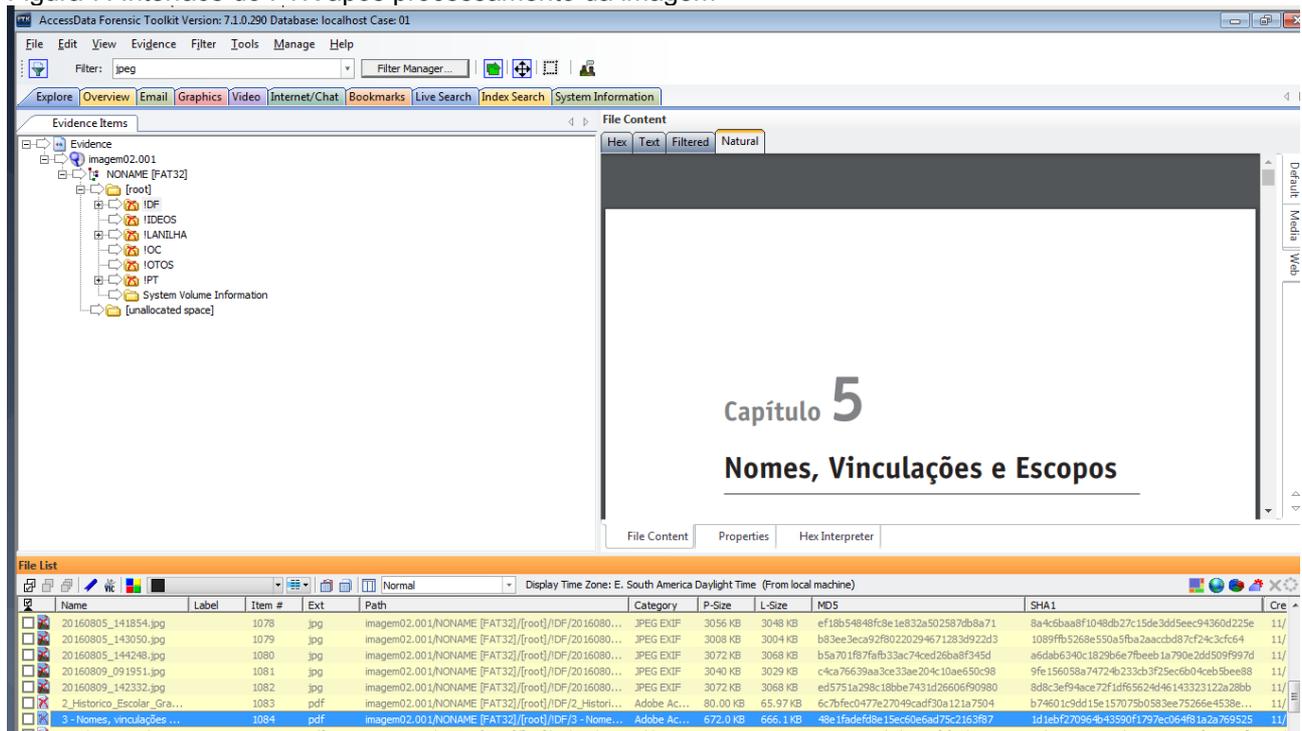
- QUANTIDADE DE ARQUIVOS EXCLUÍDOS DA MÍDIA ORIGINAL
- QUANTIDADE DE ARQUIVOS RECUPERADOS
- QUANTIDADE DE ARQUIVOS CUJO CONTEÚDO FOI VISUALIZADO CORRETAMENTE

O Apêndice C apresenta algumas telas da análise da imagem geradas pelo IPED.

3.2 RESULTADO APRESENTADO PELO FTK

O FTK apresentou a seguinte interface, conforme a figura 7, contendo os dados que foram interpretados e recuperados.

Figura 7: Interface do FTK após processamento da imagem



Fonte: Própria autora, 2019.

Observa-se que o FTK conseguiu recuperar e ler corretamente o conteúdo de 186 arquivos dos 323 que originalmente existiam na mídia, conforme demonstrado nos quadros 7 e 8.

Quadro 7: Quantidade de arquivos recuperados pelo FTK

DIRETÓRIOS	QUANTIDADE DE ARQUIVOS RECUPERADOS
1) DOC	0
2) FOTOS	118
3) VIDEOS	0
4) PLANILHA	01
5) PDF	62
6) PPT	05
TOTAL	186

Fonte: Própria autora, 2019.

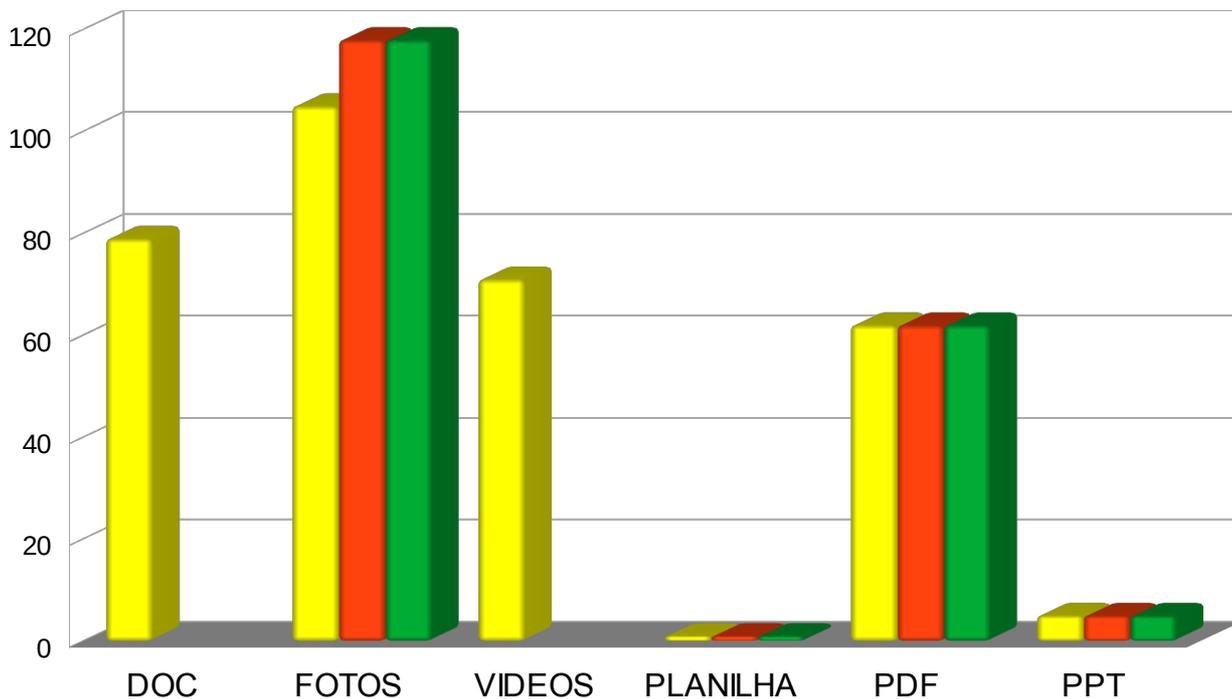
Quadro 8: Quantidade de arquivos com conteúdo exibido corretamente pelo FTK

DIRETÓRIOS	QUANTIDADE DE ARQUIVOS CUJO CONTEÚDO FOI VISUALIZADO CORRETAMENTE
1) DOC	0
2) FOTOS	118
3) VIDEOS	0
4) PLANILHA	01
5) PDF	62
6) PPT	05
TOTAL	186

Fonte: Própria autora, 2019.

O gráfico demonstra em amarelo a quantidade de arquivos de existiam na mídia original, por tipo, em vermelho a quantidade de arquivos recuperados pelo FTK e em verde a quantidade de arquivos cujos conteúdos foram corretamente exibidos.

Gráfico 2: Quantidade de dados originais vs quantidade de dados recuperados pelo FTK



Fonte: Própria autora, 2019.

Legenda:

- QUANTIDADE DE ARQUIVOS EXCLUÍDOS DA MÍDIA ORIGINAL
- QUANTIDADE DE ARQUIVOS RECUPERADOS
- QUANTIDADE DE ARQUIVOS CUJO CONTEÚDO FOI VISUALIZADO CORRETAMENTE

4 CONCLUSÃO

Conforme o problema apresentado no item 1.2, os arquivos apagados somente podem ser recuperados por meio de técnicas específicas. Neste trabalho foram utilizadas as ferramentas para forense computacional IPED e FTK, apresentadas no item 2, para as quais foi levantada a seguinte hipótese: Por ser baseado em software livre, é possível o IPED ser mais eficiente na recuperação de dados excluídos em dispositivos de armazenamento de informações digitais, uma vez que por ser de código-fonte aberto tem maior probabilidade de receber adaptações/atualizações pela comunidade de interesse em relação a ferramenta comercial FTK, desenvolvida para funcionar dentro de um escopo para o qual foi projetada. Tal hipótese foi confirmada, em virtude das seguintes análises:

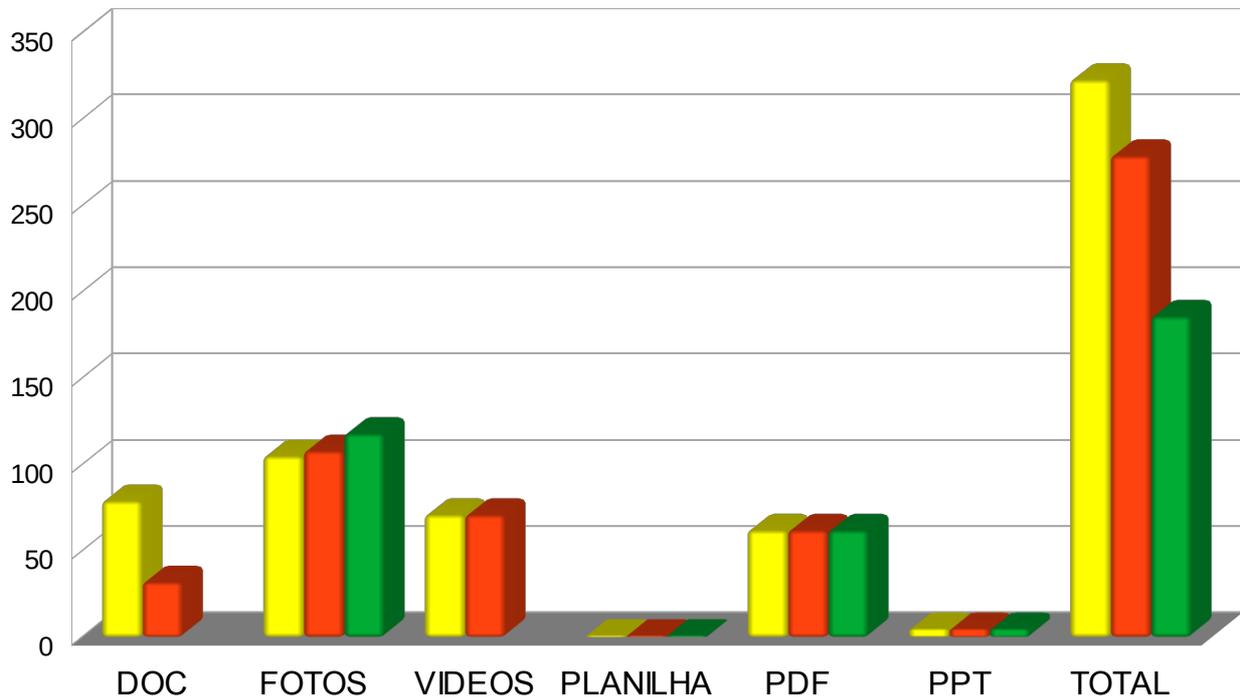
1) Em um dispositivo de 32GB foi armazenado 323 arquivos, distribuídos em 6 diretórios, conforme o tipo de cada arquivo, totalizando 21GB em dados, conforme demonstrado no quadro 3;

2) Os diretórios/arquivos foram excluídos da mídia e o dispositivo foi submetido a um processo de sanitização; e

3) Foi tirada uma imagem da mídia para ser submetida às ferramentas IPED e FTK, a fim de se verificar a eficiência quanto a porcentagem de recuperação de arquivos excluídos.

Conforme o gráfico 3, observa-se que o IPED, relação ao FTK, conseguiu recuperar e exibir corretamente o conteúdo de uma maior quantidade de arquivos.

Gráfico 3: Comparativo entre IPED e FTK



Fonte: Própria autora, 2019.

Legenda:

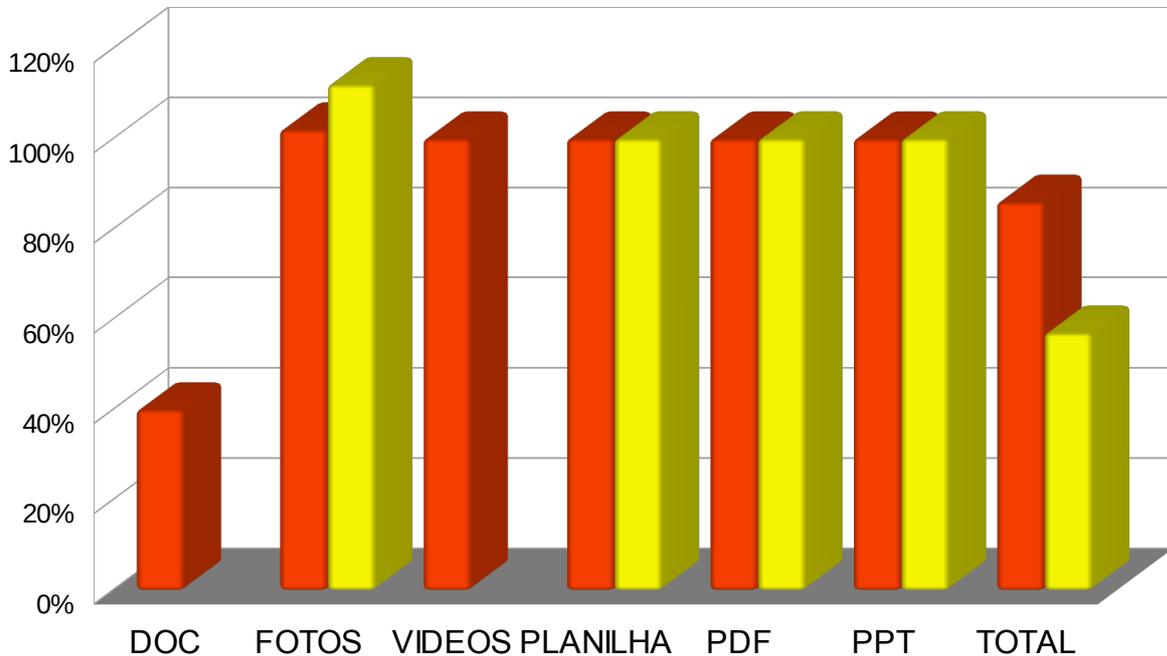
- QUANTIDADE DE ARQUIVOS EXISTENTES NA MÍDIA ORIGINAL
- QUANTIDADE DE ARQUIVOS RECUPERADOS PELO IPED
- QUANTIDADE DE ARQUIVOS RECUPERADOS PELO FTK

Conforme demonstrado no gráfico 3, apesar de o FTK ter, também, interpretado as fotos das apresentações existentes no diretório PPT, não foi capaz de interpretar, recuperar e exibir os arquivos de vídeo e de texto que estavam armazenados nos diretórios VIDEOS e DOC, respectivamente.

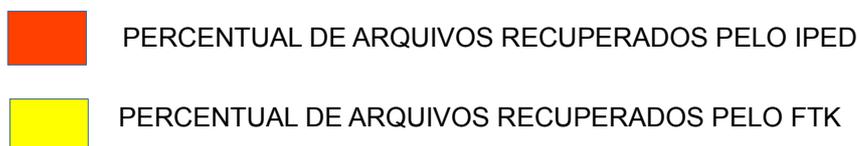
Ainda que o IPED não tenha conseguido apresentar corretamente o conteúdo dos arquivos de vídeo e de texto, o programa foi capaz de informar que havia arquivos nos diretórios, possibilitando, portanto, o uso de outras técnicas para extração dos mesmos e consequente verificação de seus conteúdos. Conclui-se, portanto, que o IPED apresentou melhor resultado na recuperação de arquivos, uma vez que dos 323 arquivos originais, o programa recuperou aproximadamente 86% em relação aos 57% recuperados pelo

FTK, conforme demonstrado no gráfico 4.

Gráfico 4: Percentual de arquivos recuperados pelo IPED e FTK



Legenda:



5 TRABALHOS FUTUROS

Finalmente, diante do vertiginoso aumento de crimes virtuais e da utilização de dispositivos computacionais seja como meio ou como apoio para o cometimento de crimes cibernéticos ou convencionais, espera-se que este trabalho contribua para fomentar o aprimoramento das ferramentas utilizadas em computação forense, de forma que se tornem cada vez mais precisas no que se refere ao exame forense em equipamentos computacionais.

Cabe, ainda, salientar que esta pesquisa não representa um fim em si mesma, antes busca incentivar que outros laboratórios sejam realizados com o intuito de nortear o

esforço conjunto das Organizações jurídicas, colaboradores e peritos digitais a alcançarem um nível eficiente e eficaz no combate aos crimes cibernéticos por meio do uso de ferramentas forense cada vez mais eficientes e eficazes, pois conforme ELEUTÉRIO e MACHADO (2011, p. 17), “Crimes sempre deixam rastros!”. “No caso da computação, os vestígios de um crime são digitais, uma vez que toda a informação armazenada dentro desses equipamentos computacionais é composta por bits (números zeros e uns), em uma sequência lógica.”

Desse modo, tendo em vista que este trabalho realizou uma análise comparativa das ferramentas quanto a recuperação de dados excluídos em mídias de armazenamento de informações digitais, para futuras pesquisas sugerem-se os seguintes temas com foco em análise comparativa de ferramentas forense quanto:

- 1) Ao processamento distribuído, no sentido de aferir a agilidade das ferramentas no processamento distribuído de evidências;
- 2) Ao processo de indexação, no sentido de aferir a agilidade de resultados quando se aplicam filtros;
- 3) A remontagem hexadecimal, no sentido de aferir a correta remontagem de arquivos corrompidos que, por ventura, forem encontrados em uma evidência;
- 4) Ao processamento personalizado, no sentido de aferir a versatilidade das ferramentas quanto ao estabelecimento de padrões e customização para processamento e análise de evidências; e
- 5) Ao reconhecimento de imagens *Optical character recognition* ou optical character reader (OCR), no sentido de aferir a qualidade das imagens escaneadas por reconhecimento ótico.

REFERÊNCIAS BIBLIOGRÁFICAS

- ACADEMIA DE FORENSE DIGITAL, 2017. Disponível em: <https://www.academiadeforensedigital.com.br/o-que-e-forense-digital/>
Acesso em: 2 jul. 2019
- ACCESSDATA. FTK Imager. Disponível em: <https://marketing.accessdata.com/ftkimager4.2.0>. Acesso em: 11 nov. 2019.
- ACCESSDATA. Product Downloads. Disponível em: <https://accessdata.com/product-download/forensic-toolkit-ftk-version-7.1.0>. Acesso em: 11 nov. 2019.
- ACCESSDATA. Disponível em: <https://accessdata.com/products-services/forensic-toolkit-ftk>
Acesso em: 5 ago. 2019.
- BRASIL. Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Estatísticas Anuais de Tratamento de Incidentes Computacionais de Governo. 2019. Disponível em: <https://www.ctir.gov.br/estatisticas/>. Acesso em: 2 set. 2019.
- BRASIL. Conselho Nacional de Justiça. Crimes digitais: o que são, como denunciar e quais leis tipificam como crime? Disponível em: <https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/>. Acesso em: 5 ago. 2019.
- DEPARTAMENTO DE POLÍCIA FEDERAL. SEPINF:IPED. Disponível em: https://servicos.dpf.gov.br/ferramentas/IPED/3.15.6/IPED-Manual_pt-BR.pdf. Acesso em: 11 nov. 2019.
- DIGITAL DETECTIVE, 2018. Disponível em: <https://kb.digital-detective.net/display/HstExV4/Supported+Source+Data+Formats#SupportedSourceDataFormats-ForensicImageFileFormats>. Acesso em: 19 nov. 2019.
- ELEUTÉRIO, Pedro M. da S.; MACHADO, Marcio P. Desvendando a computação forense. São Paulo: nov.atec, 2011.
- GALVÃO, Ricardo Kléber M. Introdução à análise forense em redes de computadores: Conceitos, técnicas e ferramentas para “grampos digitais”. São Paulo: nov.atec, 2013.
- GOMES, Helton Simões, 2019. Disponível em: <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/06/16/vazamento-de-dados-cresce-e-ja-e-2-maior-ataque-digital-ao-governo-federal.htm>
Acesso em: 2 jul. 2019.
- MILAGRE, José Antonio, 2017. Disponível em: <https://josemilagre.com.br/blog/2017/07/31/a-profissao-do-futuro-como-ser-um-perito-digital-ou-perito-em-informatica-e-iniciar-na-carreira-2017/>. Acesso em: 2 jul. 2019.
- Mercado em foco. Cyber security e forense computacional: conheça os softwares mais utilizados no mercado. Disponível em: <https://mercadoemfoco.unisul.br/cyber-security-e-forense-computacional-conheca-os-sofwarees-mais-utilizados-no-mercado/>. Acesso em: 11 nov. 2019.
- MONTEIRO, Marcos, 2018. Indexador IPED. Disponível em: <https://www.youtube.com/watch?v=A1NDvVtdEJY>. Acesso em: 11 nov. 2019.
- GALVÃO, Ricardo Kléber M. Perícia Forense Computacional. Disponível em: <https://www.passeidireto.com/arquivo/23009002/pericia-forense-computacional-seg-info>. Acesso em: 11 nov. 2019.
- TECMUNDO, 2018. Disponível em: <https://www.tecmundo.com.br/internet/126654-4-bilhoes-pessoas-usam-internet-no-mundo.htm>. Acesso em: 2 jul. 2019.
- TI FORENSE, 2019. Demonstração de uso básica do IPED. Disponível em: <https://www.youtube.com/watch?v=7x3JISpj8qY&t=1082s>. Acesso em: 11 nov. 2019.

Apêndice A - Procedimentos executados desde a sanitização da mídia, criação e submissão da mesma para análise pelas ferramentas IPED e FTK

1) Antes de copiar a base de dados, mídia foi sanitizada com zeros para evitar contaminação da imagem por usos anteriores do dispositivo, conforme demonstrado na figura 8.

Figura 8: Preenchendo a mídia com zeros

```
root@debian:~#
root@debian:~# dd if=/dev/zero of=/dev/sdb bs=1M count=40000
dd: error writing to /dev/sdb: No space left on device
30527+0 records in
30526+0 records out
32008830976 bytes (32 GB, 30 GiB) copied, 1929.61 s, 16.6 MB/s
```

Fonte: Própria autora, 2019.

2) Os diretórios e arquivos, apresentados no item 1.6, foram copiados para a mídia, ocupando 22G de um total de 32GB, conforme demonstrado na figura 9.

Figura 9: Visualização da mídia

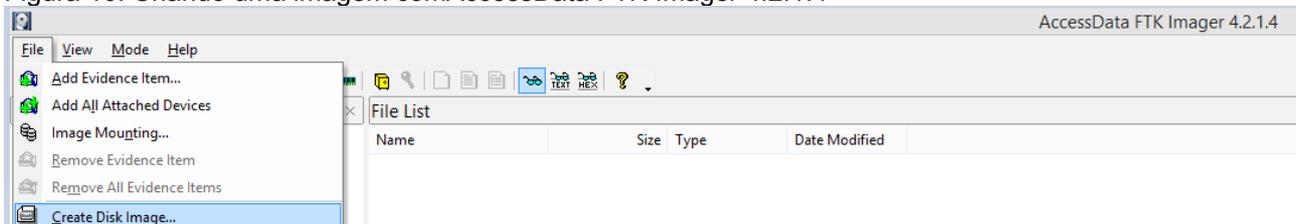
Filesystem	Size	Used	Avail	Use%	Mounted on
udev	7.8G	0	7.8G	0%	/dev
tmpfs	1.6G	9.7M	1.6G	1%	/run
/dev/sda2	92G	7.8G	79G	9%	/
tmpfs	7.8G	0	7.8G	0%	/dev/shm
tmpfs	5.0M	4.0K	5.0M	1%	/run/lock
tmpfs	7.8G	0	7.8G	0%	/sys/fs/cgroup
/dev/sda1	952M	5.1M	947M	1%	/boot/efi
/dev/sda3	37G	49M	35G	1%	/tmp
/dev/sda5	782G	53G	690G	8%	/home
tmpfs	1.6G	16K	1.6G	1%	/run/user/117
tmpfs	1.6G	40K	1.6G	1%	/run/user/1000
/dev/sdb1	932G	319G	613G	35%	/media/user/Seagate Exp
/dev/sdc	30G	22G	8.8G	71%	/media/user/F613-7B26

Fonte: Própria autora, 2019.

3) Em seguida, todos os dados foram excluídos da mídia para posterior criação da imagem

4) A criação da imagem da mídia ocorreu na sequência das figuras abaixo:

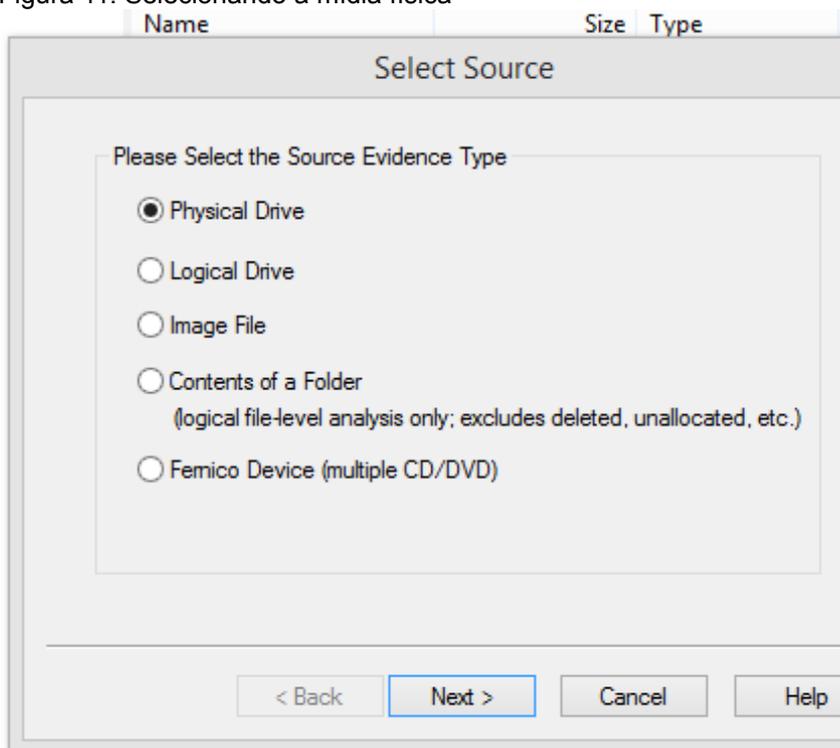
Figura 10: Criando uma imagem com AccessData FTK Imager 4.2.1.4



Fonte: Própria autora, 2019.

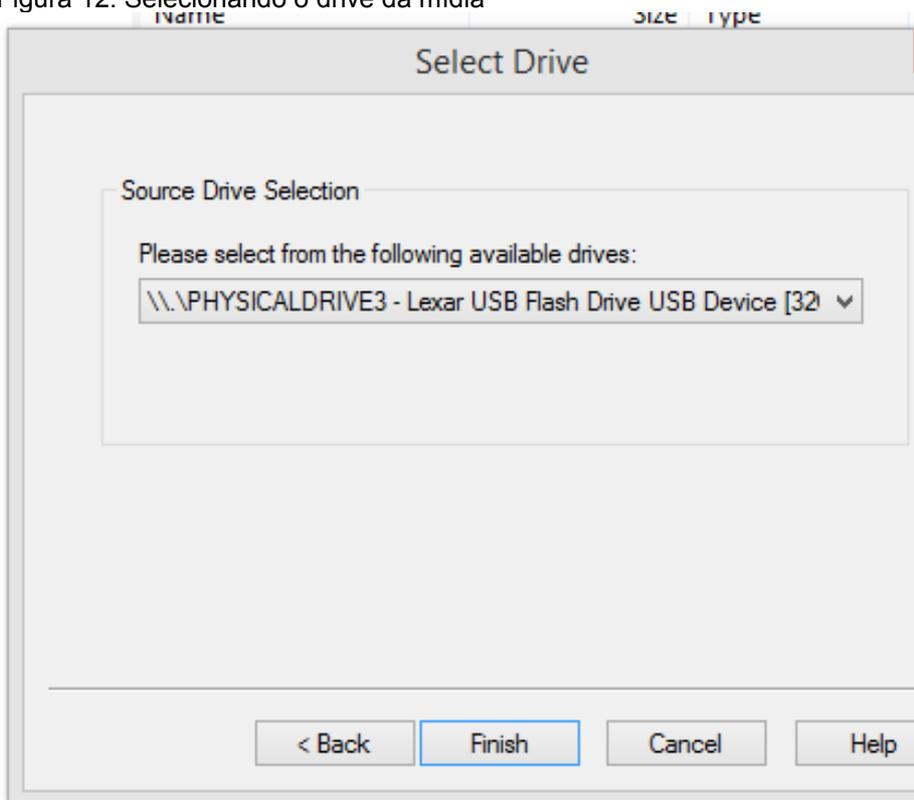
4.1) As figuras 11 e 12 mostram a seleção da mídia com drive físico

Figura 11: Selecionando a mídia física



Fonte: Própria autora, 2019.

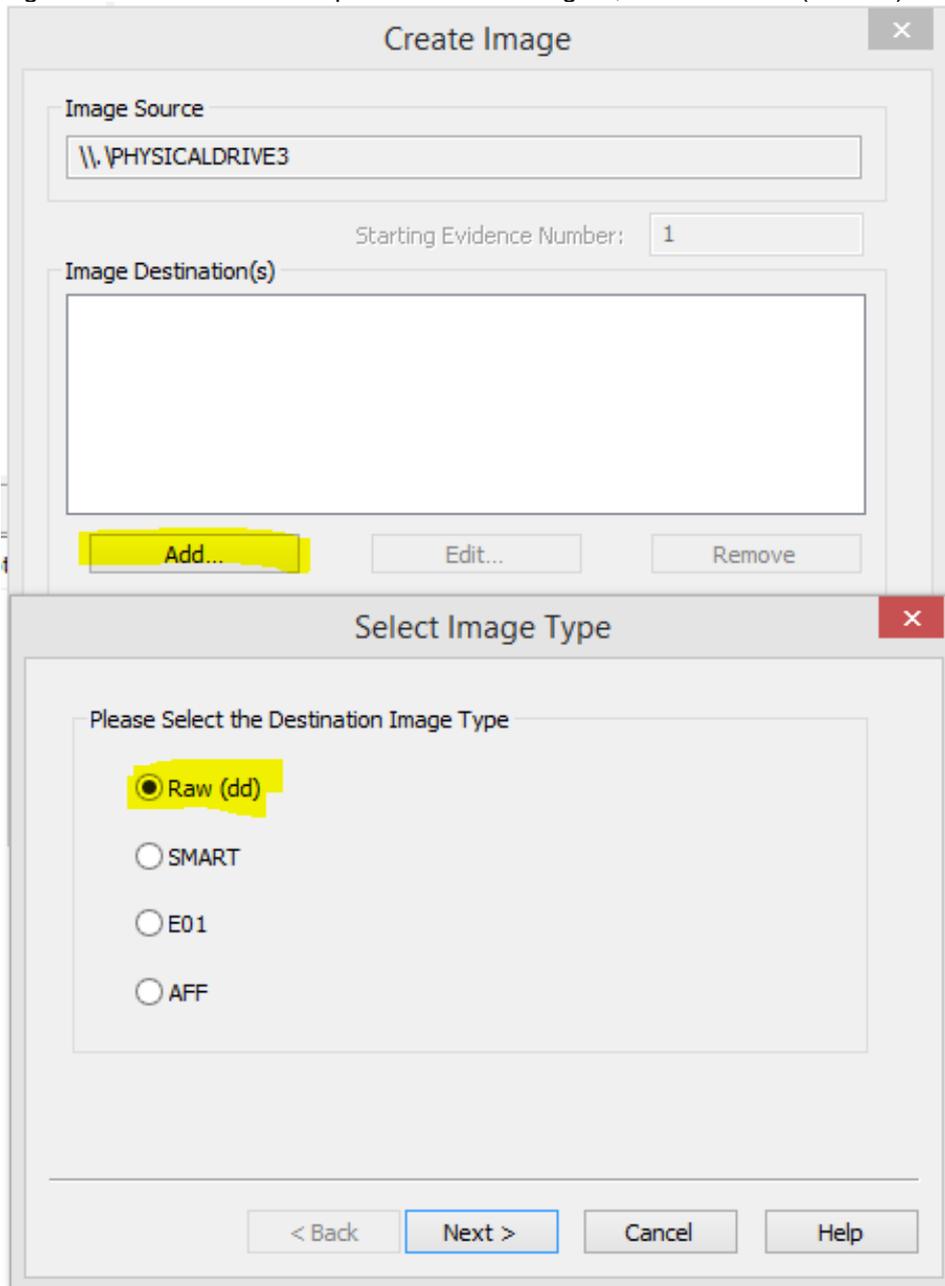
Figura 12: Selecionando o drive da mídia



Fonte: Própria autora, 2019.

5) Em seguida foi selecionado o tipo de saída do arquivo de imagem, conforme demonstrado na figura 13.

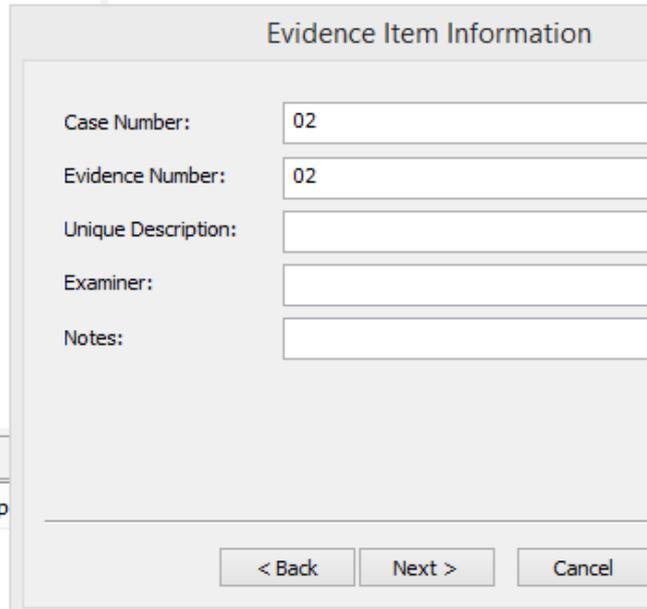
Figura 13: Selecionando o tipo de saída da imagem, no caso RAW (bit a bit)



Fonte: Própria autora, 2019.

6) Em seguida, foi criada um case para a imagem, conforme demonstrado na figura 14.

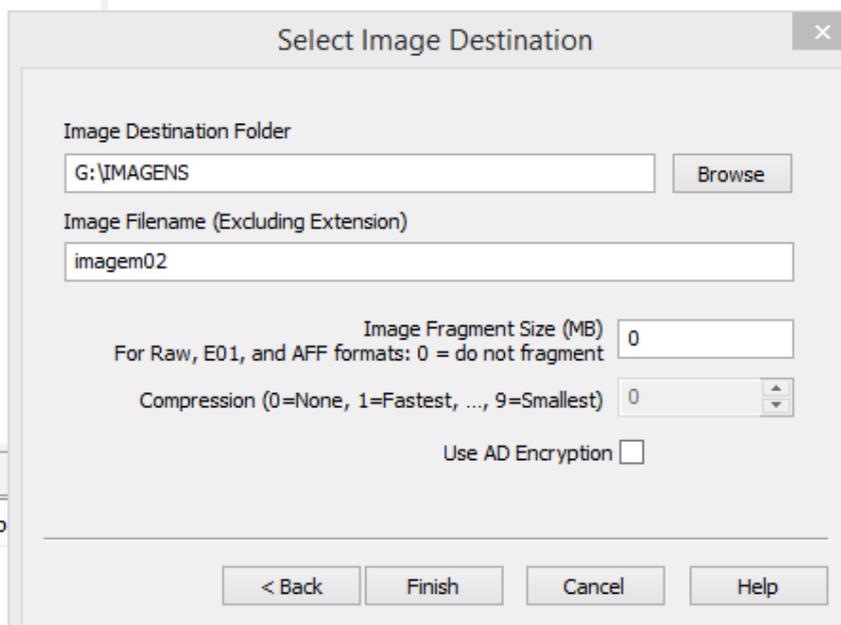
Figura 14: Atribuindo informações à imagem a ser gerada



Fonte: Própria autora, 2019.

7) Na figura 15 são informados o destino para criação da imagem e o nome da mesma, optando a criação de um único arquivo para a imagem, que pelo tamanho da mídia não havia necessidade de fragmentá-la.

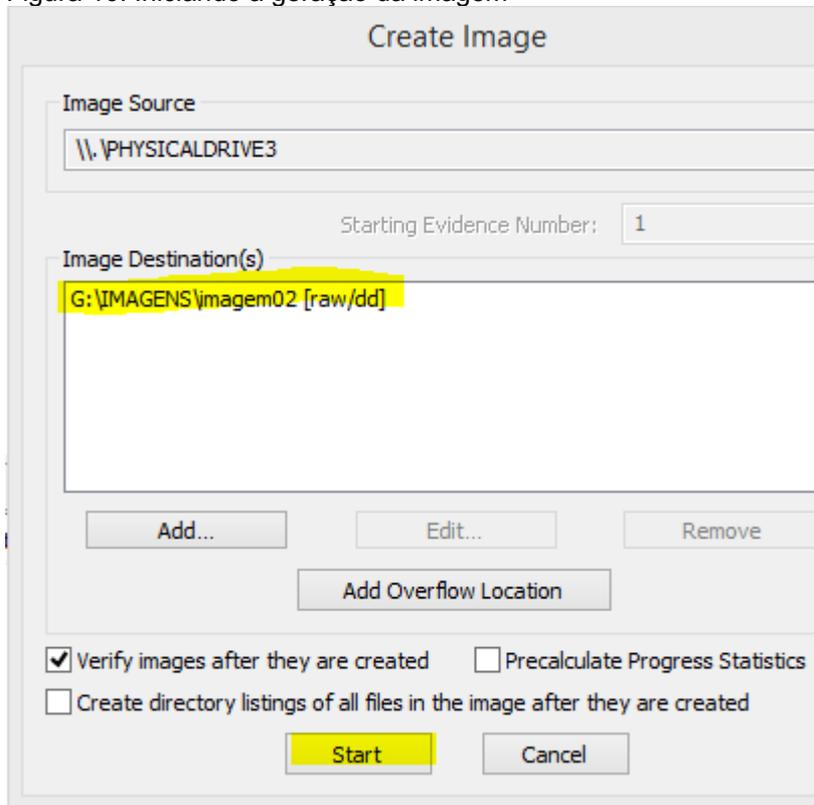
Figura 15: Informando o local onde será salva a imagem, seu o nome e que será gerada em um único arquivo



Fonte: Própria autora, 2019.

8) Ao final das configurações, é apresentada o formato da imagem e o local onde será criada, conforme demonstrado na figura 16.

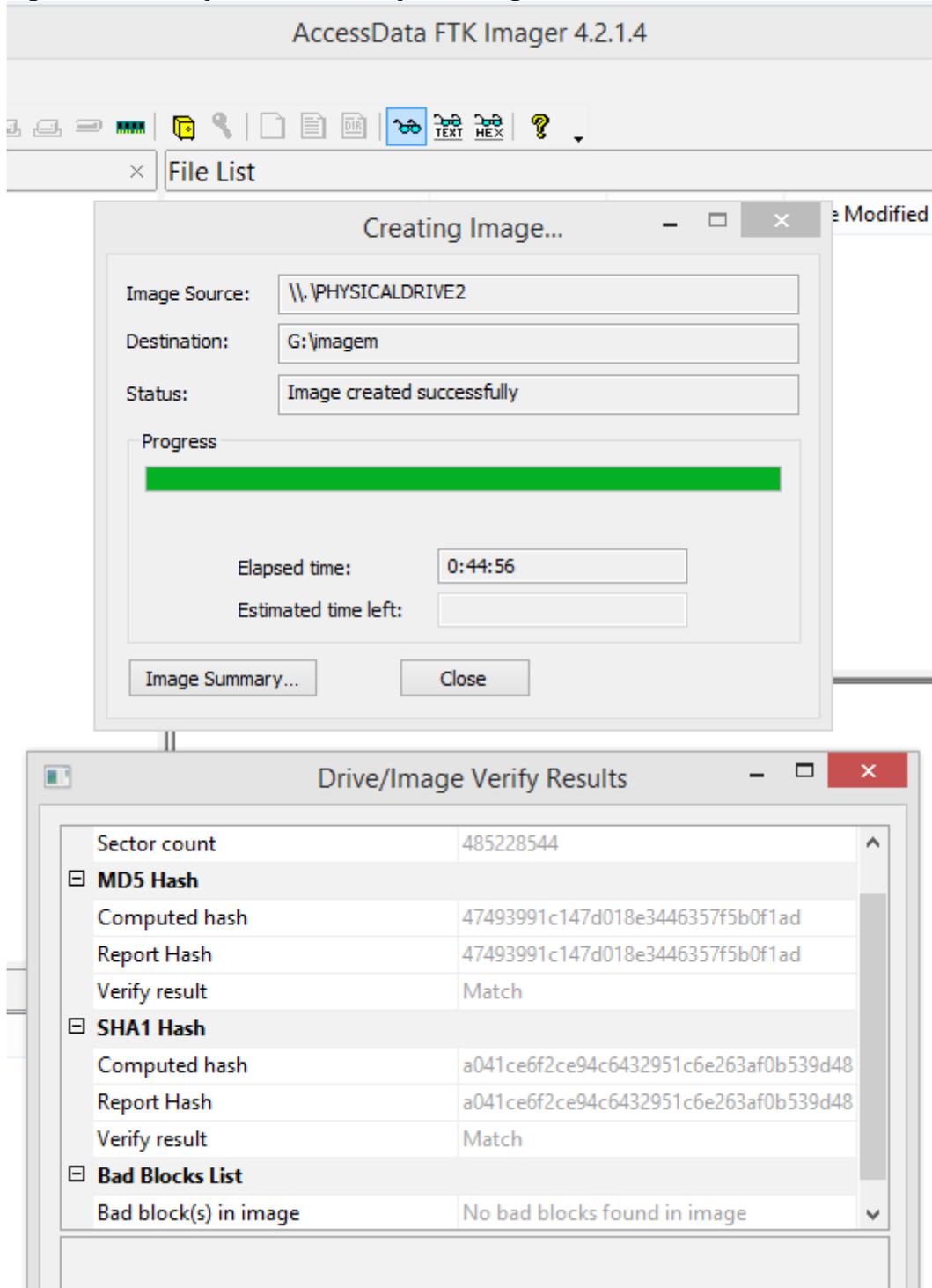
Figura 16: Iniciando a geração da imagem



Fonte: Própria autora, 2019.

9) Ao final da criação e verificação da imagem, o FTK Imager realiza o cálculo *hash* para garantir a integridade e a autenticidade da mídia original, utilizando para tal as funções MD5, de 128 bits, e SHA1, de 160 bits.

Figura 17: Finalização da tela de criação da imagem



Fonte: Própria autora, 2019.

Observa-se que o FTK Imager levou 8 minutos para gerar uma imagem de 32GB.

2 SUBMETENDO A IMAGEM PARA ANÁLISE PELO IPED

O IPED é um programa de linha de comando, disponível para download no site da Polícia Federal.

Figura 18: Site de localização do IPED



Fonte: Própria autora, 2019.

O programa requer o Java64bits para executar corretamente. Neste sentido, deve-se checar o tipo de java existente no computador onde o IPED será executado.

Figura 19: Verificando a versão do Java

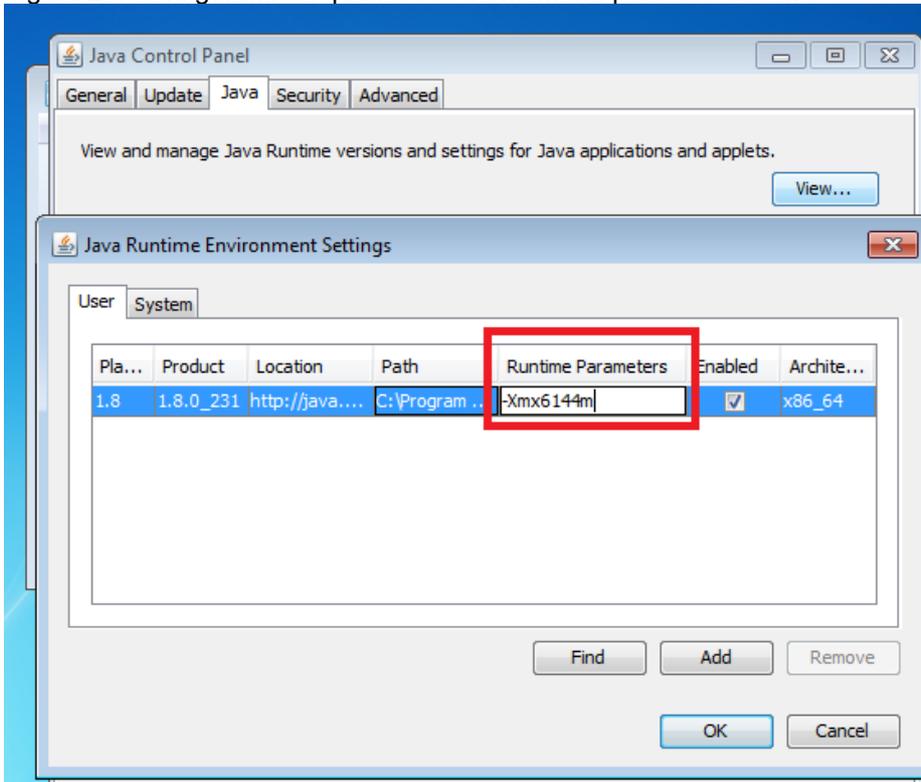
```
Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\rejane> java -version
java version "1.8.0_221"
Java(TM) SE Runtime Environment (build 1.8.0_221-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.221-b11, mixed mode)
```

Fonte: Própria autora, 2019.

Deve-se, também, definir a quantidade de memória RAM que o Java poderá utilizar no processo de indexação da imagem, por meio do parâmetro `-XmxQtdDeMemoria`. Neste laboratório, foi configurado 6GB ($1024 * 6 = 6144$) para uso pelo Java.

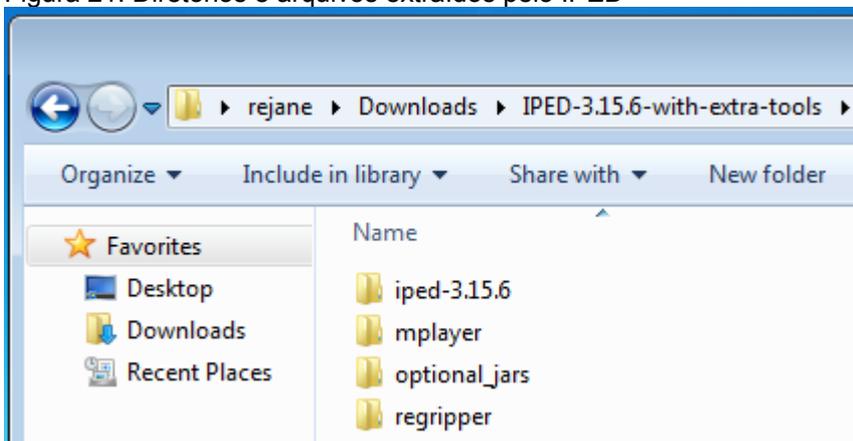
Figura 20: Configurando a quantidade de memória para uso do Java



Fonte: Própria autora, 2019.

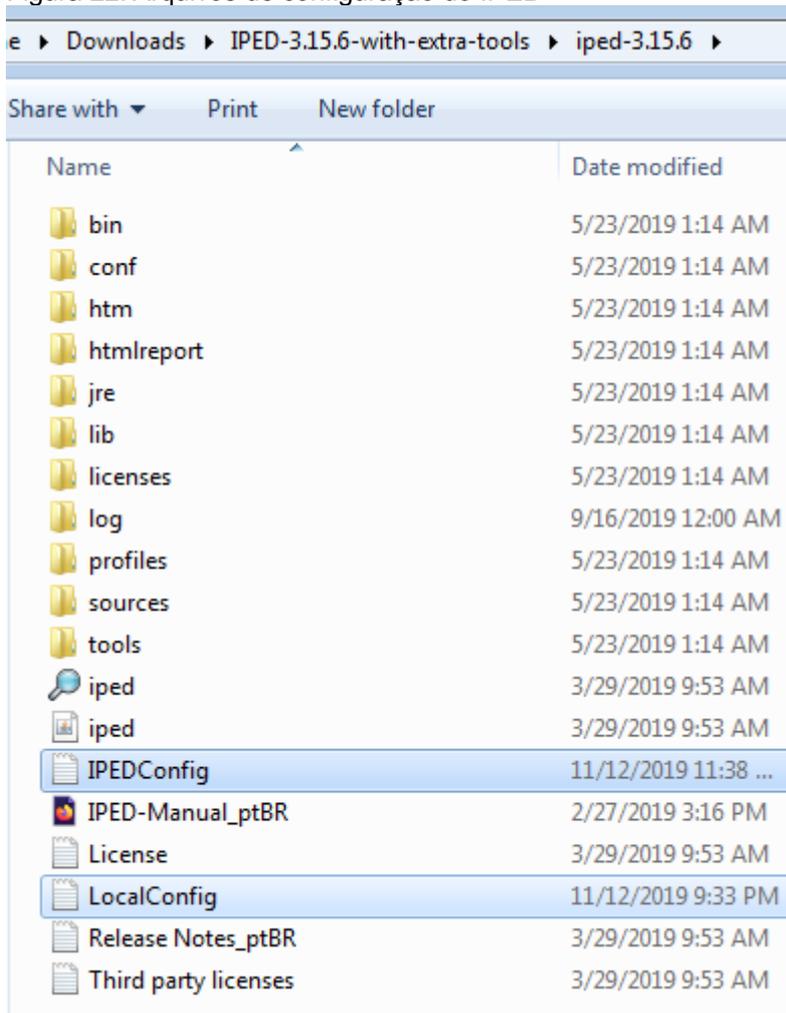
Deve-se selecionar um diretório para extração do programa, onde serão criados diretórios e arquivos, conforme demonstrados nas figuras 21 e 22.

Figura 21: Diretórios e arquivos extraídos pelo IPED



Fonte: Própria autora, 2019.

Figura 22: Arquivos de configuração do IPED



Fonte: Própria autora, 2019.

O IPED é configurado por meio dos arquivos LocalConfig e IPEDConfig, conforme demonstrado na figura 23. No arquivo LocalConfig encontram-se os parâmetros do ambiente do computador, como por exemplo, se existe HD tipo SSD (*solid-state drive*) e no arquivo IPEDConfig estão os parâmetros de funcionalidades do IPED, por exemplo, o tipo de função *hash* a ser utilizada, se habilita detecção de outros idiomas, uso de RegEx, dentre outros.

Para este laboratório, os seguintes parâmetros foram configurados para true no arquivo IPEDConfig:

- a) *enableRegexSearch* que utilizará expressões regulares no processo de indexação;
- b) *enableOCR* para ler os dados contidos em uma imagem, como por exemplo, um documento que pode está um uma foto;

- c) *enablecarving* para fazer recuperação de dados em espaços não alocados na mídia; e
- d) *addunallocated* para áreas não alocadas de imagens.

Figura 23: Visualizando o IPEDConfig

```

IPEDConfig - Notepad
File Edit Format View Help
expandContainers = true

# Searches texts extracted from itens by regular expressions
# like social numbers, emails, URLs, credit cards, money values, etc.
# New expressions can be configured in file "conf/RegexConfig.txt"
enableRegexSearch = true

# Enables detection of more than 70 idioms in document files.
enableLanguageDetect = false

# EXPERIMENTAL function to recognize mentioned entities: names of people, organizations or places.
# Requested models must be downloaded and put in the folder "optional-libs"
# Download requested models from: StanfordCoreNLP 3.8: https://stanfordnlp.github.io/CoreNLP/history.html
# Model for Portuguese language has not be trained, so results may be insatisfactory
# This function uses a lot of CPU, wich can increase processing duration by 4 times.
# Advanced settings can be modified in file "conf/NamedEntityRecognitionConfig.txt"
enableNamedEntityRecogniton = false

# Indexes files contents. If disabled, indexes only the properties of files.
indexFilecontents = true

# Indexes files with no specific decoder, like binaries, unknown, pagefile, unallocated, etc
# In this option, raw strings are extracted from the files and indexed
indexUnknownFiles = true

# Index corrupted files with strings. For example, deleted and partially overwritten imagens
# can have searchable plain text into them.
indexCorruptedFiles = true

# Enables OCR in scanned images and PDFs. It can strongly increase processing time.
# Results depend on the quality and resolution of the images, and on the size and type of the fonts used.
# Advanced OCR options, such as the Tesseract path on Linux, can be modified in "conf/AdvancedConfig.txt"
enableOCR = true

# Adds and processes files fileslacks
addFileslacks = false

# Adds and processes unallocated areas of images, via sleuthkit
addunallocated = true

# Added unallocated space will be indexed. "addunallocated" and "indexUnknownFiles" must be enabled.
indexUnallocated = false

# Enables carving. "addunallocated" must be enabled to unallocated area be searched.
# By default carving runs on almost every item in the case.
# File types to be searched and retrieved can be set in file "conf/CarvingConfig.txt"
enableCarving = true

# Enables carving that retrieves known files from the LED base, based on the beggining (64K) of the file.
# It's necessary to enable "addunallocated" and to configure "ledwkffPath".
enableKFFCarving = false

```

Fonte: Própria autora, 2019.

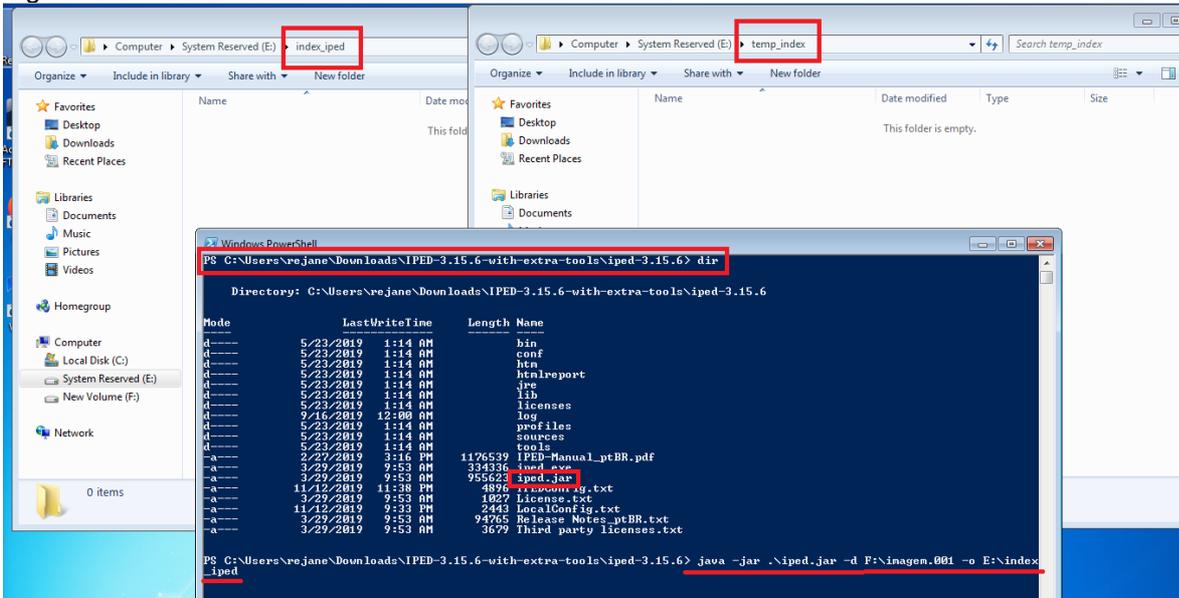
Deve-se criar um diretório indexIPED e outro tempIPED. No indexIPED serão criados arquivos que são resultados do processo de indexação da imagem e no tempIPED serão criados os arquivos temporários, os quais poderão ser excluídos ao término do processo.

Realizada as configurações acima, deve-se abrir o *powershell* ou o cmd do Windows, direcionar para o caminho onde se encontra o arquivo iped.jar e iniciar a execução do IPED para processamento da imagem.

A execução do IPED ocorre por meio do seguinte comando, conforme a figura abaixo, conforme demonstrado na figura 24:

```
java -jar .\iped.jar -d <CaminhoDeLocalizaçãoDaImagem> -o
<CaminhoDeLocalizaçãoDoDiretório_indexIPED>
```

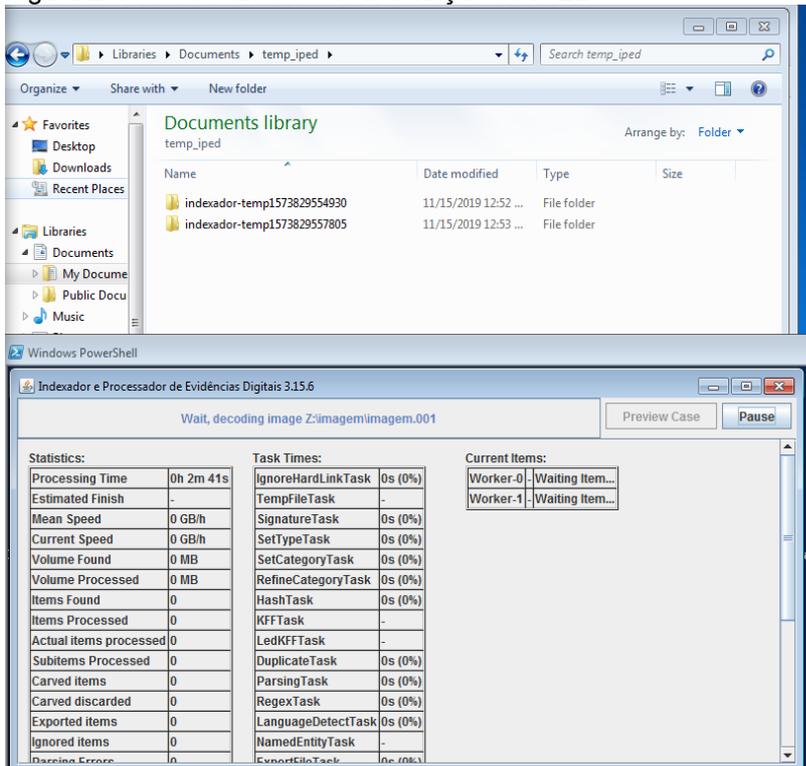
Figura 24: Executando o IPED



Fonte: Própria autora, 2019.

O IPED chama a parte gráfica, conforme demonstrado na figura 25, para o processamento da imagem, onde cada *worker* representa um núcleo do processador destinado ao processo. Neste laboratório, foram configurados 2 núcleos para a máquina virtual Windows.

Figura 25: Processamento de indexação do IPED



Fonte: Própria autora, 2019.

Ao final, o IPED apresenta as seguintes informações, conforme demonstrado na figura 26:

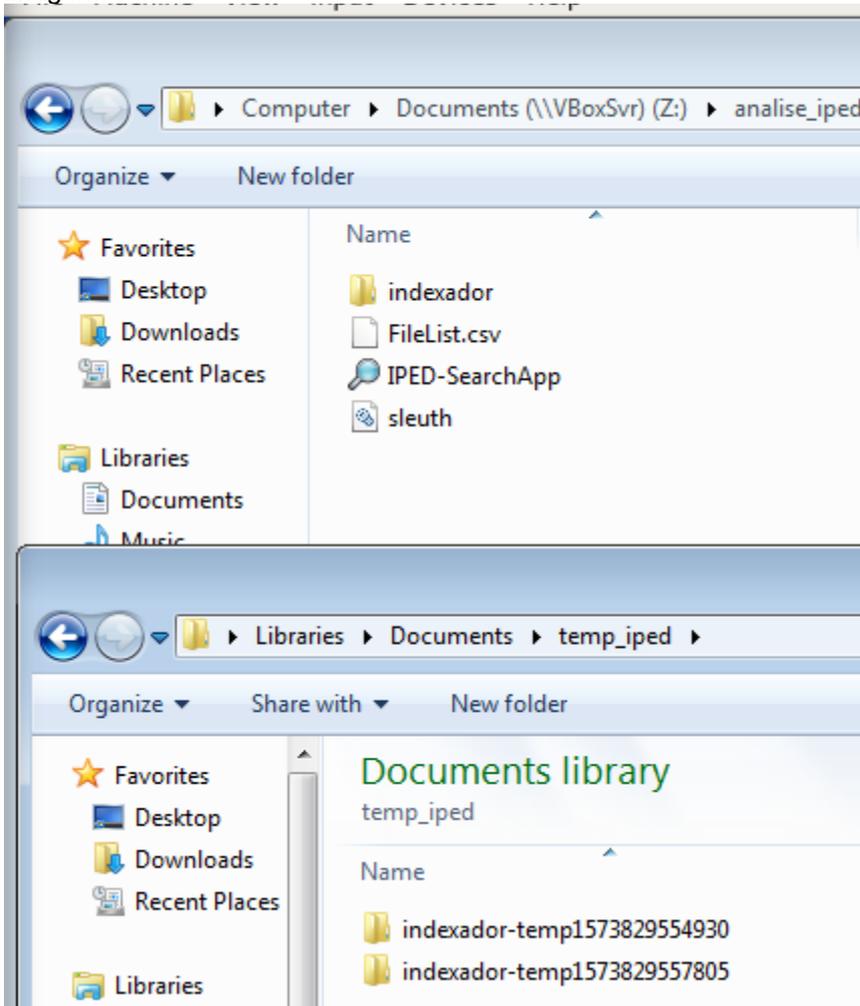
Figura 26: Informação de término de indexação do IPED

```
C:\Users\rejane\Downloads\IPED-3.15.6-with-extra-tools\iped-3.15.6> java -jar .\iped.jar -d Z:\imagem\imagem.001 -o
alipse_iped
finished.
Check the log at C:\Users\rejane\Downloads\IPED-3.15.6-with-extra-tools\iped-3.15.6\log\IPED-2019-11-15-11-52-31.log
```

Fonte: Própria autora, 2019.

Para este laboratório, o programa levou, aproximadamente, 20 minutos para processar a imagem de 32GB, gerando os seguintes diretórios e arquivos, conforme demonstrado na figura 27:

Figura 27: Diretórios e arquivos gerados pelo IPED após indexação da imagem

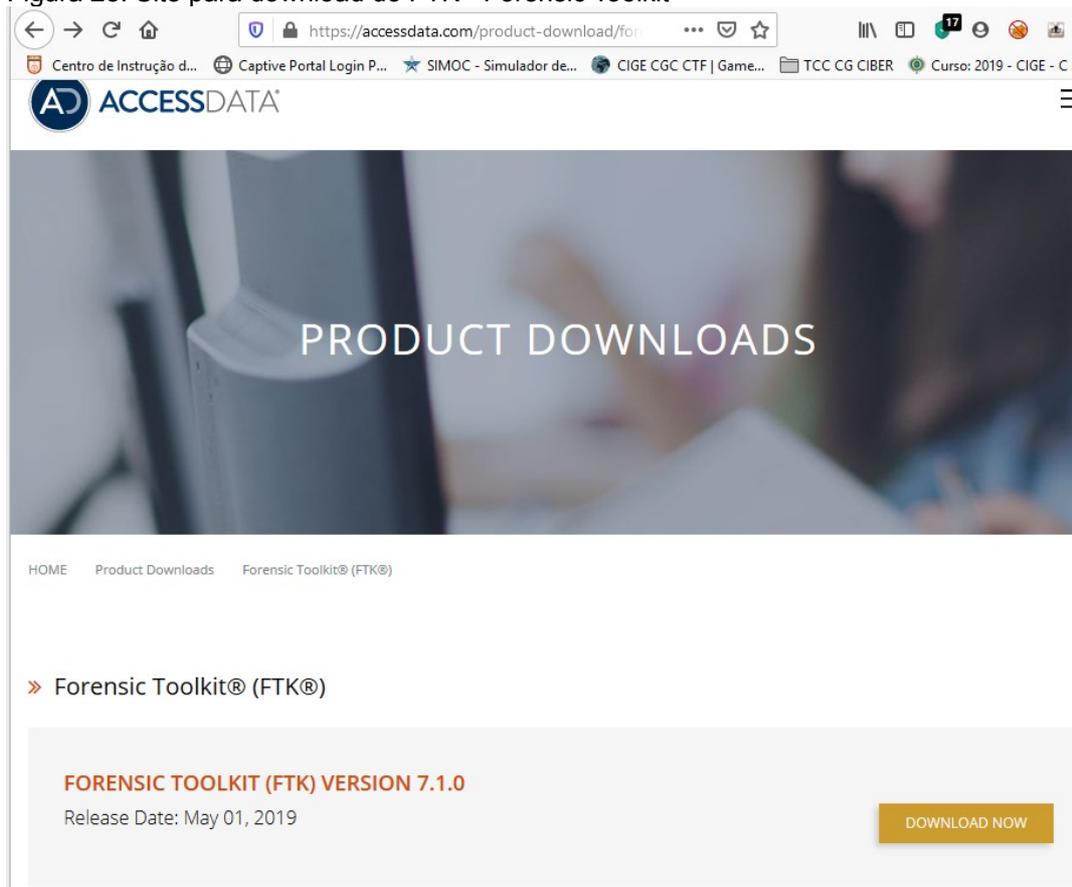


Fonte: Própria autora, 2019.

3 SUBMETENDO A IMAGEM PARA ANÁLISE PELO FTK

A versão utilizada neste laboratório é a 7.1.0, cuja imagem .ISO pode ser obtida do site do desenvolvedor que, embora disponível para download, somente poderá funcionar mediante aquisição da licença para uso do token, tendo em vista que a ferramenta é comercial.

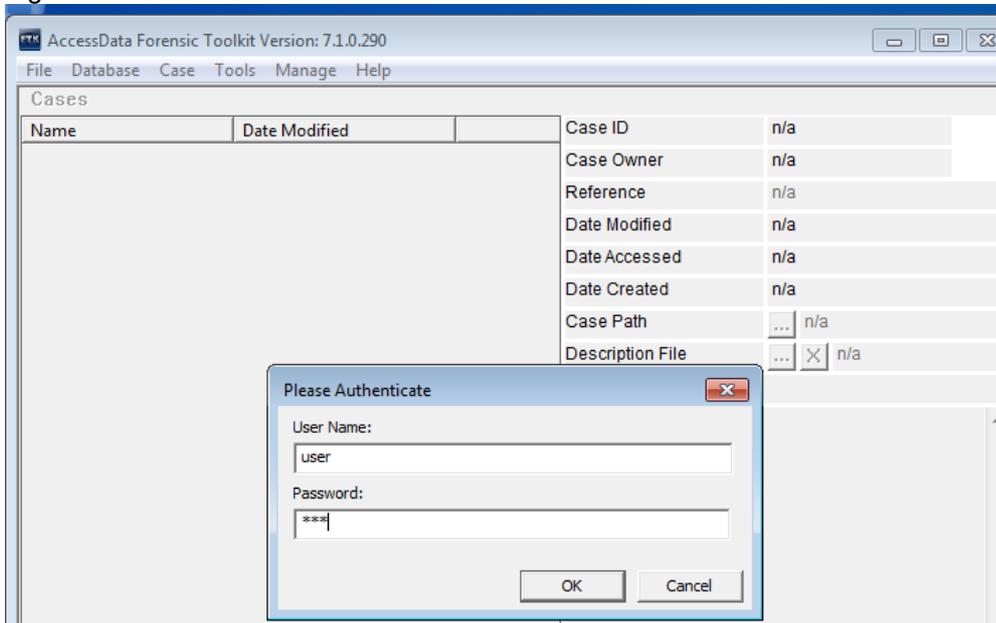
Figura 28: Site para download do FTK - Forensic Toolkit



Fonte: Própria autora, 2019.

Ao abrir o FTK é solicitado a credencial de acesso, conforme demonstrado na figura 29.

Figura 29: Acessando o FTK



Fonte: Própria autora, 2019.

Em seguida, foi criado um case chamado 01, informado o tipo do processo, no caso *Forensic Processing* e o caminho para criação dos arquivos durante o processo de indexação, conforme demonstrado nas figuras 30 e 31.

Figura 30: Criando um case

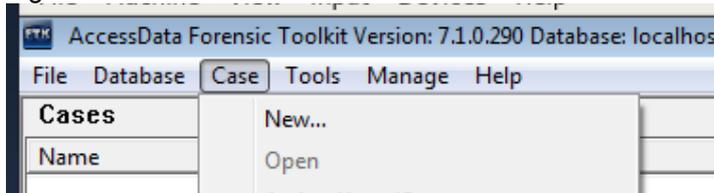
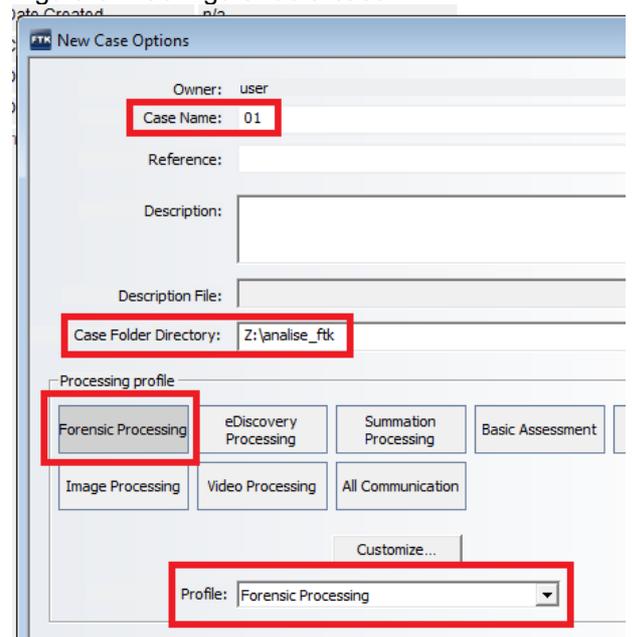


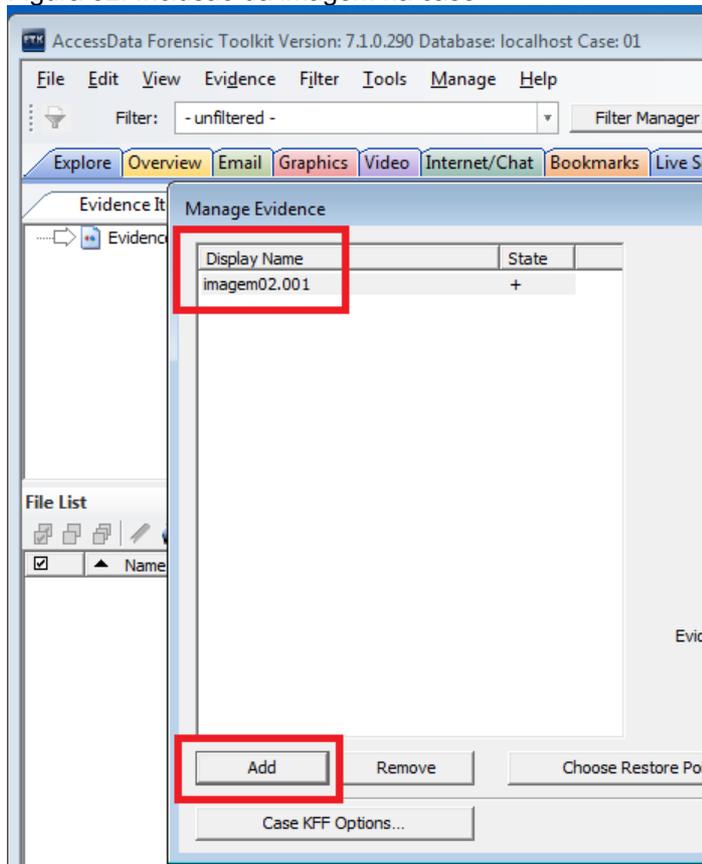
Figura 31: Configurando a case



Fonte: Própria autora, 2019.

Foi incluída a imagem a ser analisada, conforme demonstrado na figura 32.

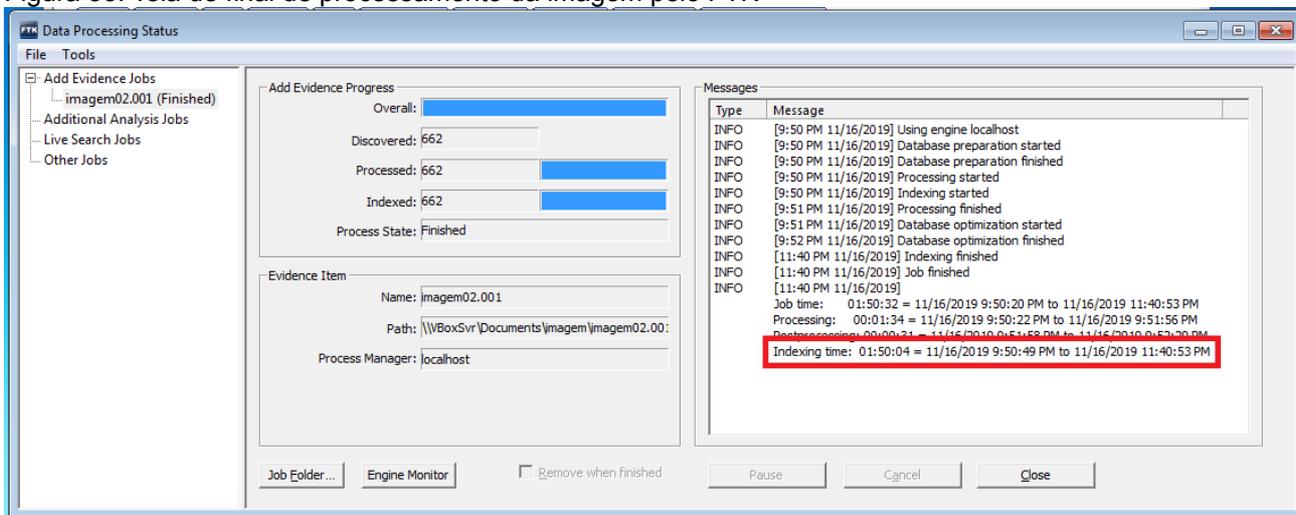
Figura 32: Inclusão da imagem na case



Fonte: Própria autora, 2019.

Conforme demonstrado na figura 33, o FTK levou 1h e 50 minutos para processar a imagem de 32GB

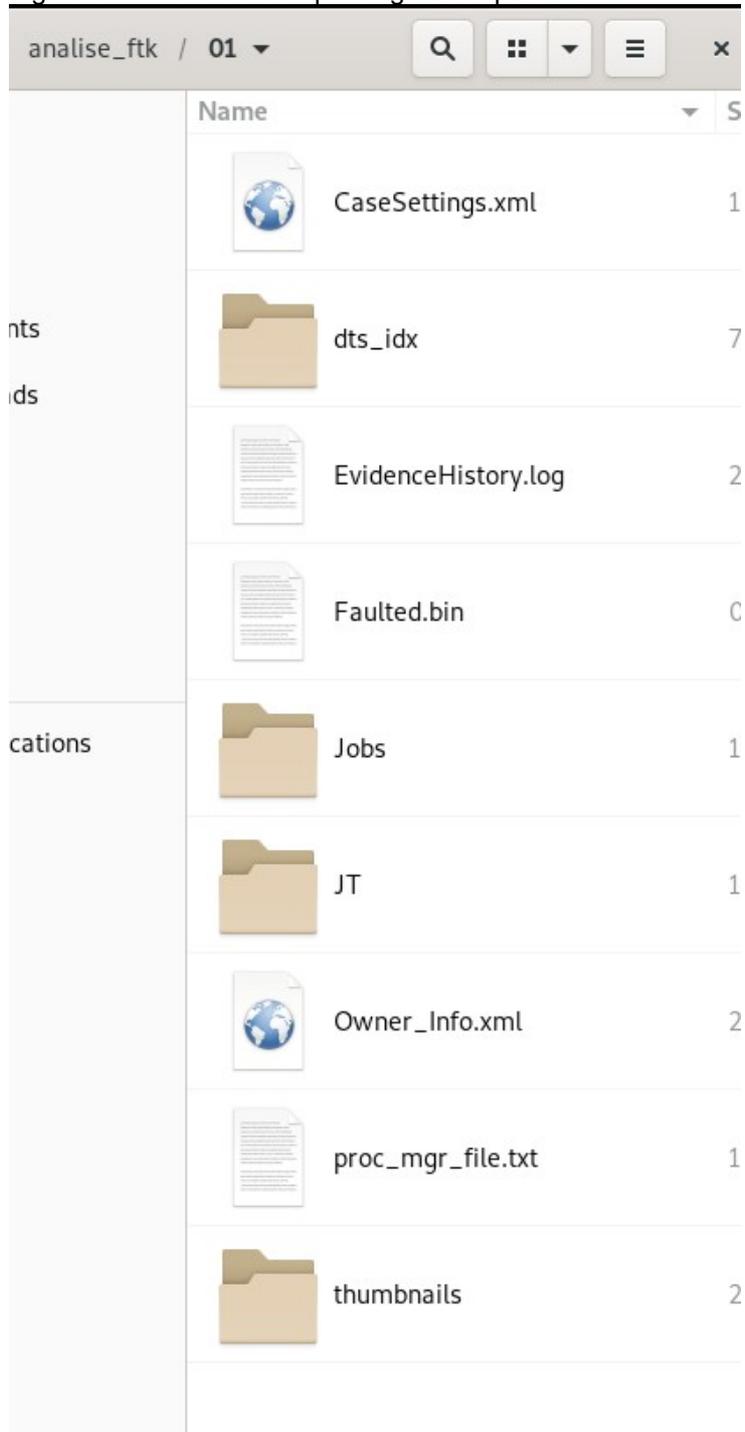
Figura 33: Tela de final de processamento da imagem pelo FTK



Fonte: Própria autora, 2019.

No diretório indicado na figura 31, foram criados os diretórios e arquivos abaixo:

Figura 34: Diretórios e arquivos gerados pelo FTK



The image shows a file explorer window with the address bar set to 'analise_ftk / 01'. The window displays a list of files and folders. The files are: 'CaseSettings.xml' (1 file), 'EvidenceHistory.log' (2 files), 'Faulted.bin' (0 files), 'Owner_Info.xml' (2 files), and 'proc_mgr_file.txt' (1 file). The folders are: 'dts_idx' (7 files), 'Jobs' (1 file), 'JT' (1 file), and 'thumbnails' (2 files). The window also shows a search bar and navigation icons.

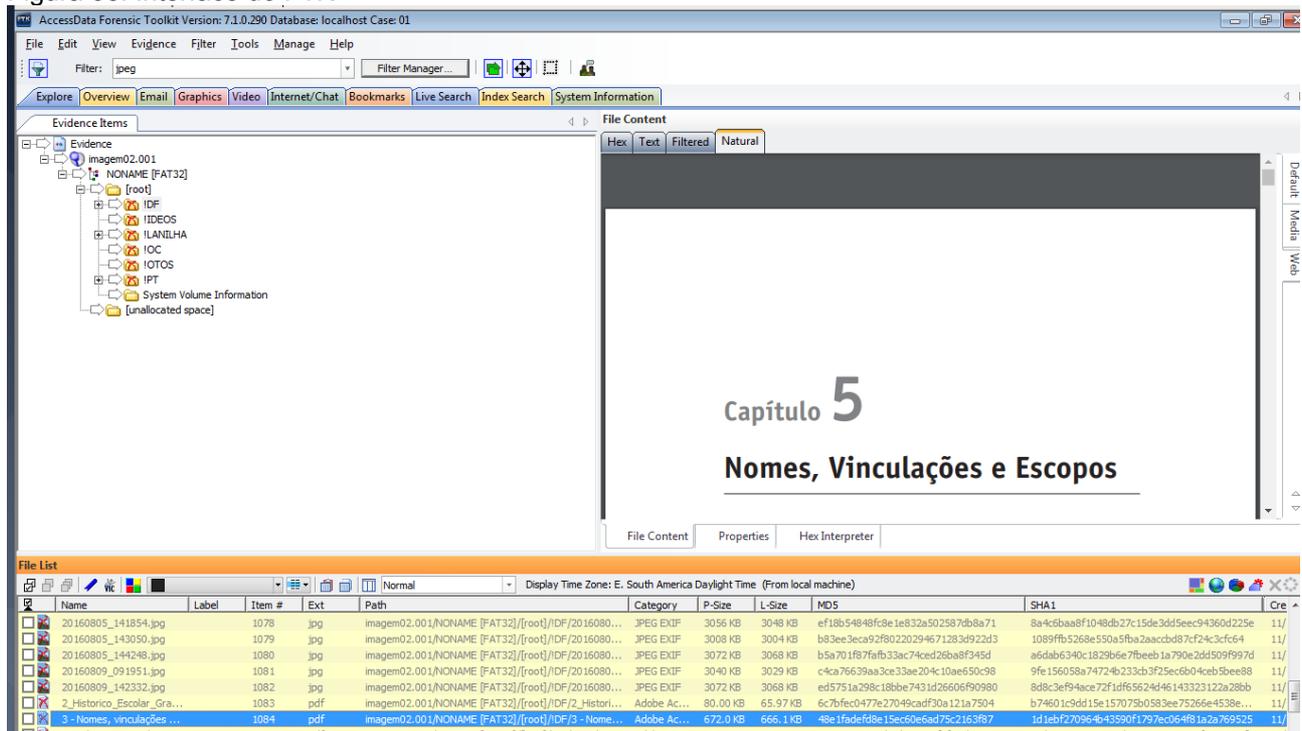
Name	S
 CaseSettings.xml	1
 dts_idx	7
 EvidenceHistory.log	2
 Faulted.bin	0
 Jobs	1
 JT	1
 Owner_Info.xml	2
 proc_mgr_file.txt	1
 thumbnails	2

Fonte: Própria autora, 2019.

Apêndice B – Interface gráfica do FTK versão 7.1.0 e apresentação de um modelo de relatórios

Após o processo apresentado no apêndice A, o FTK apresenta as informações que conseguiu recuperar após processamento da imagem, conforme demonstrado na figura 35.

Figura 35: Interface do FTK



Fonte: Própria autora, 2019.

Conforme demonstrado na figura 36, o FTK gera relatórios em HTML.

Figura 36: Tela do relatório gerado pelo FTK

The screenshot shows a web browser window with the following content:

Report.pdf x +
 file:///C:/Users/rejane/Desktop/teste/Report.pdf
 2 of 5 Automatic Zoom

Case Summary

11/17/2019
 Time zone for display: E. South America Daylight Time

Case Information

11/17/2019
 Time zone for display: E. South America Daylight Time

Version	AccessData Forensic Toolkit Version: 7.1.0.290
Case Owner	user
Case Name	01
Case Reference	
Case Description	
Report Created	11/17/2019 4:57:24 PM

File Overview

11/17/2019

Evidence Groups

Ungrouped: 662

File Items

Evidence Items: 1
 Checked Items: 0
 Unchecked Items: 662

File Category

Archives: 0
 Databases: 0

Fonte: Própria autora, 2019.

Apêndice C - Telas da análise da imagem geradas pelo IPED

Após o processo apresentado no apêndice A, o IPED apresenta as informações que conseguiu recuperar após processamento da imagem, conforme demonstrado na figura 37.

Figura 37: Diretórios recuperados pelo IPED

	Score	Name	Type	Size (30,526...	Del...	Category	Created	Modified	Accessed	Hash
1	24%	/		16,384	false	Folders				DF151CFDA4042019701
2	24%	System Volume ...		16,384	false	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	60A2D09E9E0D360944
3	24%	_OTOS		16,384	true	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	21662002F302D629216
4	24%	_OC		16,384	true	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	4081281B22390C06E7C
5	24%	_LANILHA		16,384	true	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	3052A0AF1899198BD31
6	24%	_DF		16,384	true	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	DBA51AD1460AE13A19E
7	24%	_PT		16,384	true	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	9DCA7CE3FF47EC2BA5E
8	24%	_IDEOS		16,384	true	Folders	11/14/2019 12:...	11/14/2019...	11/14/2019	23551423327DED3056E
9	24%	FAT32		32,008,830,9...	false	Folders				
10	24%	\$OrphanFiles		0	false	Empty Fil...				D41D8CD98F00B204E9
11	24%	\$Unalloc		0	false	Empty Fil...				D41D8CD98F00B204E9

Fonte: Própria autora, 2019.

Conforme demonstrado nas figuras 38-41, o IPED indexa os arquivos por categorias.

Figura 38: Arquivos de vídeos recuperados pelo IPED

	Score	Name	Type	Size (21,055...	Del...	Category	Created	Modified	Accessed	Hash
1	10%	_EGEND~-1.MP3	mp3	8,363,565	true	Audios	11/14/2019 12:...	08/20/2014...	11/15/2019	A896B71A5E2E34A331
2	3%	_5CURS~-1.MP4	mp4	541,028,598	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	AAFF1B308C1259C24
3	3%	_4CURS~-1.MP4	mp4	511,704,979	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	E0E9C9838AC92A32E
4	3%	_CURSO~-1.MP4	mp4	233,976,100	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	0DAF38D0429B1AD19
5	3%	_1CURS~-1.MP4	mp4	631,026,628	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	DC7A10E47D610CAA
6	3%	_3CURS~-1.MP4	mp4	572,247,898	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	7CE5C3984885D389F
7	3%	_2CURS~-1.MP4	mp4	340,256,863	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	35DC82310AB8816B6
8	3%	_EVOL~-1.MP4	mp4	76,893,303	true	Videos	11/14/2019 12:...	08/13/2014...	11/15/2019	2E70703D7974B3D29
9	3%	_0CURS~-1.MP4	mp4	606,773,820	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	F1F5AE9BD1186F249
10	3%	_6CURS~-1.MP4	mp4	702,774,294	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	CA5D5CB3EDA639F6
11	3%	_7CURS~-1.MP4	mp4	523,822,878	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	86C03F550BAF650B7
12	3%	_8CURS~-1.MP4	mp4	752,247,258	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	7C86CB5FD00DF1AC
13	3%	_9CURS~-1.MP4	mp4	424,804,632	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	DD3E33FB9D17260A5
14	3%	_CURSO~-1.MP4	mp4	319,818,894	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	7B1BD179B5E892EE5
15	3%	_JSEGU~-1.MP4	mp4	131,421,618	true	Videos	11/14/2019 12:...	08/13/2014...	11/15/2019	9D69D00A3B7181474
16	3%	_0CURS~-1.MP4	mp4	677,253,975	true	Videos	11/14/2019 12:...	06/21/2019...	11/15/2019	2858827D36E00C8BC
17	3%	_01608~-2.MP4	mp4	80,995,422	true	Videos	11/14/2019 12:...	08/12/2016...	11/15/2019	E0692233CDA541CD
18	3%	_01608~-1.MP4	mp4	396,352,591	true	Videos	11/14/2019 12:...	08/12/2016...	11/15/2019	374A47A27EE79E3A
19	3%	_01608~-3.MP4	mp4	95,485,261	true	Videos	11/14/2019 12:...	08/12/2016...	11/15/2019	46B9BFF2A22A4ECA7
20	3%	_2CURS~-1.MP4	mp4	283,675,848	true	Videos	11/14/2019 12:...	06/22/2019...	11/15/2019	60E1D2CD269828CE
21	3%	_1CURS~-1.MP4	mp4	377,268,717	true	Videos	11/14/2019 12:...	06/22/2019...	11/15/2019	BC20B179450CF18A5

Fonte: Própria autora, 2019.

Figura 39: Arquivos de fotos recuperados pelo IPED

Score	Name	Type	Size (1,055M...)	Del...	Category	Created	Modified	Accessed	Hash
5%	1 Abdominal Ba...	jpg	8,376	true	Other Ima...	11/14/2019 12...	10/06/2016...	11/15/2019	6CADE8AAD6829DC8A
5%	15 - 14.jpg	jpg	3,981,114	true	Other Ima...	11/14/2019 12...	03/08/2017...	11/15/2019	D04B5D7E4733B9405
5%	20160711_140...	jpg	2,618,623	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	73C692928DA2D7D56
5%	20160711_142...	jpg	1,065,931	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	1AE7EAD0750FE408
5%	20160711_190...	jpg	1,393,917	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	EFDDE3EF229FA36E
5%	20160711_190...	jpg	1,574,813	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	0BF99D5567E80FE55
5%	20160712_135...	jpg	1,216,336	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	6C988A488DB5485E
5%	20160712_151...	jpg	1,048,822	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	E361B8AB5CEF82454
5%	20160712_171...	jpg	692,827	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	99E99349F1FF773DF
5%	20160713_114...	jpg	1,019,041	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	326703221EF81CFB7
5%	20160713_151...	jpg	1,130,675	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	EC382221FD1C339C
5%	20160713_151...	jpg	853,863	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	DE69DC048C4E9A8F
5%	20160713_170...	jpg	1,356,963	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	995E1EC4D7C1AD18
5%	20160713_172...	jpg	1,749,256	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	94DF61A7A35CADD2
5%	20160713_192...	jpg	1,169,304	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	4E44829BDCC6C4F
5%	20160713_193...	jpg	1,600,922	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	EA345C01B44D454F9
5%	20160713_195...	jpg	1,976,552	true	Other Ima...	11/14/2019 12...	03/07/2017...	11/15/2019	1220E140E02D9CC
5%	20160714_173...	jpg	1,914,733	true	Other Ima...	11/14/2019 12...	03/08/2017...	11/15/2019	833A5AD2A23989EE5
5%	20160714_175...	jpg	794,362	true	Other Ima...	11/14/2019 12...	10/02/2016...	11/15/2019	936BC4737CDB21CA
5%	20160714_175...	jpg	659,112	true	Other Ima...	11/14/2019 12...	03/08/2017...	11/15/2019	AF3E3434B477299AD
5%	20160715_104...	jpg	858,449	true	Other Ima...	11/14/2019 12...	03/08/2017...	11/15/2019	5882C047F7DEF8BC
5%	20160715_112...	jpg	873,452	true	Other Ima...	11/14/2019 12...	03/08/2017...	11/15/2019	BD31A7F918DE518B

Fonte: Própria autora, 2019.

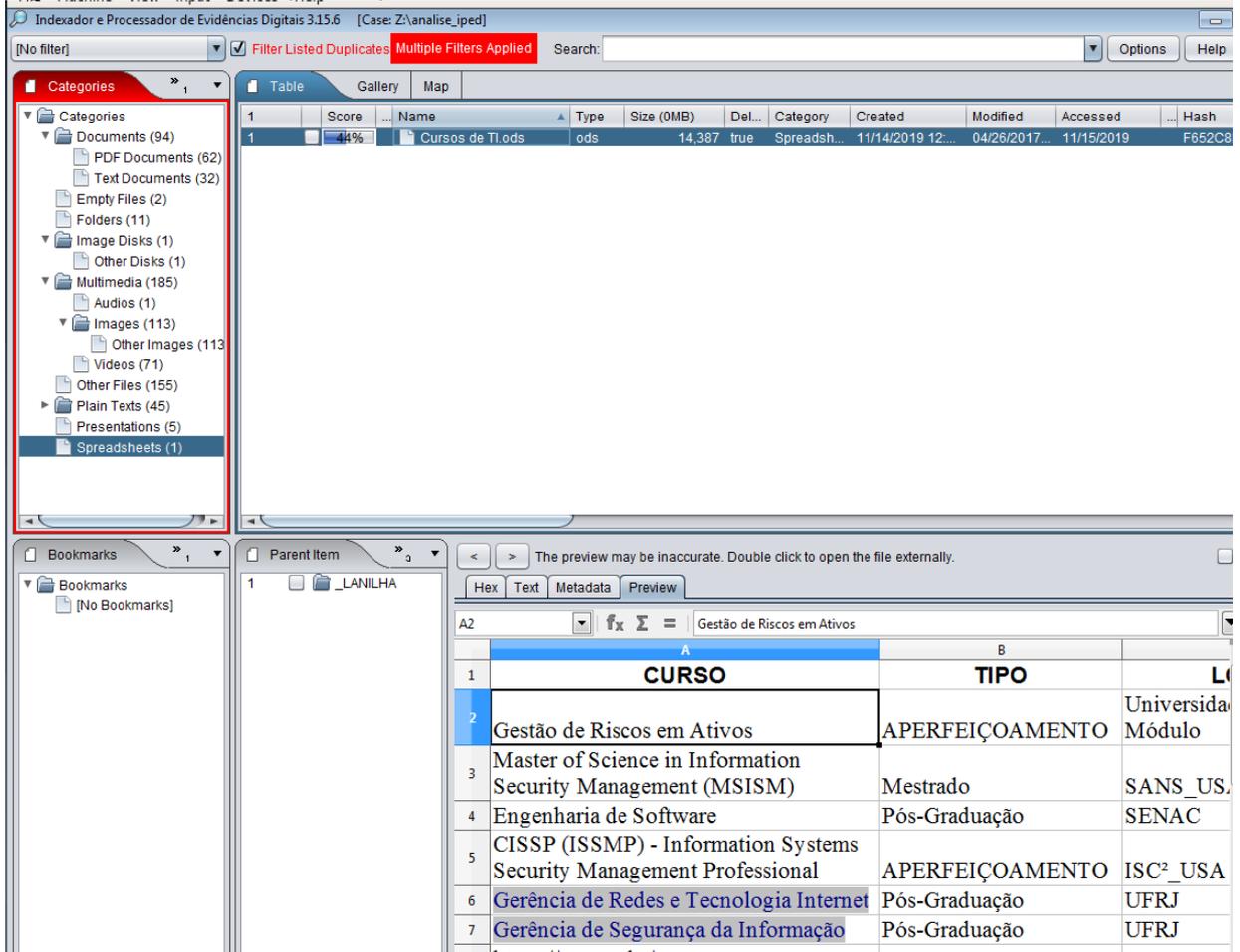
Figura 40: Arquivos de slides recuperados pelo IPED

Score	Name	Type	Size (2,128M...)	Del...	Category	Created	Modified	Accessed	Hash
31%	trato das informações...	ppbx	437,455,083	true	Presentat...	11/14/2019 12...	08/05/2017...	11/15/2019	BAF4137
31%	uso de senhas no am...	ppbx	44,179,296	true	Presentat...	11/14/2019 12...	01/28/2017...	11/15/2019	6266418
31%	VolIP1.odp	odp	1,595,980	true	Presentat...	11/14/2019 12...	09/21/2019...	11/15/2019	E9C5B62
31%	Vuln_Web[1].ppt	ppt	5,221,376	true	Presentat...	11/14/2019 12...	05/16/2019...	11/15/2019	D5FBE17
31%	WHATSAPP.pptx	pptx	1,743,692,199	true	Presentat...	11/14/2019 12...	08/21/2017...	11/15/2019	808BE47

The preview window displays a slide with a key icon and the text: **SENHA a CHAVE para SUAS informacoes**. The slide also features a graphic with a key and two tags labeled 'USUÁRIO' and 'SENHA'.

Fonte: Própria autora, 2019.

Figura 41: Planilha recuperada pelo IPED



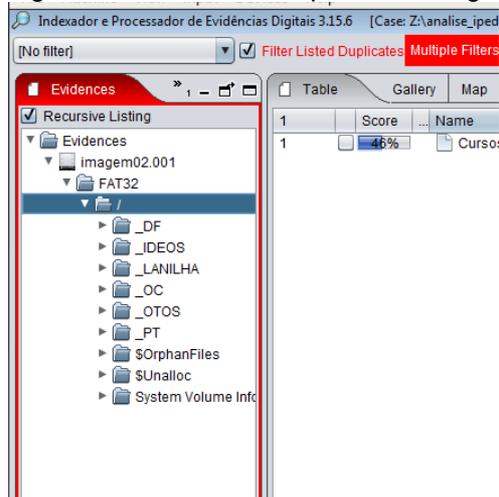
Score	Name	Type	Size (0MB)	Del...	Category	Created	Modified	Accessed	Hash
44%	Cursos de TI.ods	ods	14.387	true	Spreadsh...	11/14/2019 12:...	04/26/2017...	11/15/2019	F652C8

CURSO	TIPO	
Gestão de Riscos em Ativos	APERFEIÇOAMENTO	Universidade Módulo
Master of Science in Information Security Management (MSISM)	Mestrado	SANS_US.
Engenharia de Software	Pós-Graduação	SENAC
CISSP (ISSMP) - Information Systems Security Management Professional	APERFEIÇOAMENTO	ISC²_USA
Gerência de Redes e Tecnologia Internet	Pós-Graduação	UFRJ
Gerência de Segurança da Informação	Pós-Graduação	UFRJ

Fonte: Própria autora, 2019.

Conforme demonstrado na figura 42, ao reconhecer o sistema de arquivos, o IPED permite navegar pela estrutura de diretórios. Neste laboratório, o sistema de arquivos da mídia era FAT32 com a seguinte estrutura de diretórios.

Figura 42: Sistema de arquivos da imagem



Score	Name
46%	Curso:

CURSO	TIPO
Gestão de Riscos em Ativos	APERFEIÇOAMENTO
Master of Science in Information Security Management (MSISM)	Mestrado
Engenharia de Software	Pós-Graduação
CISSP (ISSMP) - Information Systems Security Management Professional	APERFEIÇOAMENTO
Gerência de Redes e Tecnologia Internet	Pós-Graduação
Gerência de Segurança da Informação	Pós-Graduação

Fonte: Própria autora, 2019.