# 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

**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: 2° 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 consequentemente 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 2: Estatísticas dos Incidentes Reportados e Confirmados.       2         Figura 3: Disco rígido como um planeta de dados.       9         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       29         Figura 17: Finalização da tela de criação da imagem.       30         Figura 20: Configurando a quantidade de memória para uso do Java.       32         Figura 21: Diretórios e arquivos extraídos pelo IPED.       33         Figura 22: Arquivos de configuração do IPED.       33         Figura 23: Visualizando o IPEDConfig.       34
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       29         Figura 16: Iniciando a geração da imagem.       20         Figura 17: Finalização da tela de criação da imagem.       30         Figura 20: Configurando a quantidade de memória para uso do Java.       31         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: Execut
Figura 4: Disco rígido como um planeta de dados
Figura 5: Diretórios e arquivos gerados pelo IPED após indexação da imagem
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       29         Figura 16: Iniciando a geração da imagem       20         Figura 17: Finalização da tela de criação da imagem       30         Figura 18: Site de localização do IPED       31         Figura 20: Configurando a quantidade de memória para uso do Java       32         Figura 21: Diretórios e arquivos extraídos pelo IPED       33         Figura 23: Visualizando o IPED       33         Figura 24: Executando o IPED       36         Figura 25: Processamento de indexação do IPED       36         Figura 26: Informação de término de indexação do IPED       36         Figura 26: Informação de término de indexação do IPED       36
Figura 7: Interface do FTK após processamento da imagem
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       29         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 20: Configurando a quantidade de memória para uso do Java.       32         Figura 21: Diretórios e arquivos extraídos pelo 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.       36         Figura 27: Diretórios e arquivos gerados pelo IPED.       36 <t< td=""></t<>
Figura 9: Visualização da mídia
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       28         Figura 16: Iniciando a geração da imagem.       29         Figura 17: Finalização da tela de criação da imagem.       29         Figura 18: Site de localização do IPED.       31         Figura 20: Configurando a quantidade de memória para uso do Java.       32         Figura 21: Diretórios e arquivos extraídos pelo IPED.       33         Figura 23: Visualizando o IPEDConfig.       34         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.       36         Figura 23: Visualizando o IPED.       36         Figura 24: Executando o IPED.       36         Figura 25: Processamento de indexação do IPED.       36         Figura 26: Informação de término de indexação do IPED.       36         Figura 27: Diretórios e arquivos g
Figura 11: Selecionando a mídia física
Figura 12: Selecionando o drive da mídia.26Figura 13: Selecionando o tipo de saída da imagem, no caso RAW (bit a bit).27Figura 14: Atribuindo informações à imagem a ser gerada.28Figura 15: Informando o local onde será salva a imagem, seu o nome e que será28gerada em um único arquivo.28Figura 16: Iniciando a geração da imagem.29Figura 17: Finalização da tela de criação da imagem.30Figura 18: Site de localização do IPED.31Figura 20: Configurando a quantidade de memória para uso do Java.32Figura 21: Diretórios e arquivos extraídos pelo IPED.32Figura 23: Visualizando o IPEDConfig.34Figura 24: Executando o IPED.35Figura 25: Processamento de indexação do IPED.36Figura 26: Informação de término de indexação do IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED.37
Figura 13: Selecionando o tipo de saída da imagem, no caso RAW (bit a bit)
Figura 14: Atribuindo informações à imagem a ser gerada.28Figura 15: Informando o local onde será salva a imagem, seu o nome e que será28gerada em um único arquivo.28Figura 16: Iniciando a geração da imagem.29Figura 17: Finalização da tela de criação da imagem.30Figura 18: Site de localização do IPED.31Figura 20: Configurando a quantidade de memória para uso do Java.32Figura 21: Diretórios e arquivos extraídos pelo IPED.32Figura 23: Visualizando o IPEDConfig.34Figura 24: Executando o IPED.35Figura 25: Processamento de indexação do IPED.36Figura 26: Informação de término de indexação do IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED.36Figura 26: Informação de término de indexação do IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED.37
Figura 15: Informando o local onde será salva a imagem, seu o nome e que será gerada em um único arquivo
gerada em um único arquivo.28Figura 16: Iniciando a geração da imagem.29Figura 17: Finalização da tela de criação da imagem.30Figura 18: Site de localização do IPED.31Figura 19: Verificando a versão do Java.31Figura 20: Configurando a quantidade de memória para uso do Java.32Figura 21: Diretórios e arquivos extraídos pelo IPED.32Figura 22: Arquivos de configuração do IPED.33Figura 23: Visualizando o IPEDConfig.34Figura 24: Executando o IPED.35Figura 25: Processamento de indexação do IPED.36Figura 26: Informação de término de indexação do IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED após indexação da imagem.37
Figura 16: Iniciando a geração da imagem.29Figura 17: Finalização da tela de criação da imagem.30Figura 17: Finalização da tela de criação da imagem.30Figura 18: Site de localização do IPED.31Figura 19: Verificando a versão do Java.31Figura 20: Configurando a quantidade de memória para uso do Java.32Figura 21: Diretórios e arquivos extraídos pelo IPED.32Figura 22: Arquivos de configuração do IPED.33Figura 23: Visualizando o IPEDConfig.34Figura 24: Executando o IPED.35Figura 25: Processamento de indexação do IPED.36Figura 26: Informação de término de indexação do IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED após indexação da imagem.37
Figura 17: Finalização da tela de criação da imagem
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 19: Verificando a versão do Java.31Figura 20: Configurando a quantidade de memória para uso do Java.32Figura 21: Diretórios e arquivos extraídos pelo IPED.32Figura 22: Arquivos de configuração do IPED.33Figura 23: Visualizando o IPEDConfig.34Figura 24: Executando o IPED.35Figura 25: Processamento de indexação do IPED.36Figura 26: Informação de término de indexação do IPED.36Figura 27: Diretórios e arquivos gerados pelo IPED após indexação da imagem37
Figura 20: Configurando a quantidade de memória para uso do Java
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 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 arguivos gerados pelo IPED após indexação da imagem       37
Figura 23: Visualizando o IPEDConfig
Figura 24: Executando o IPED
Figura 25: Processamento de indexação do IPED
Figura 26: Informação de término de indexação do IPED
Figura 27 <sup>•</sup> Diretórios e arquivos gerados pelo IPED após indexação da imagem 37
Figura 28: Site para download do FTK - Forensic Toolkit
Figura 29: Acessando o FTK
Figura 30: Criando um case
Figura 31: Configurando a case
Figura 32: Inclusão da imagem na case40
Figura 33: Tela de final de processamento da imagem pelo FTK40
Figura 34: Diretórios e arquivos gerados pelo FTK41
Figura 35: Interface do FTK42
Figura 36: Tela do relatório gerado pelo FTK43
Figura 37: Diretórios recuperados pelo IPED
Figura 38: Arguivos de vídeos recuperados pelo IPED
Figura 39: Arquivos de fotos recuperados pelo IPED45
Figura 40: Arquivos de slides recuperados pelo IPED45
Figura 41: Planilha recuperada pelo IPED
Figura 42: Sistema de arquivos da imagem46

#### 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 FTF	<b>۲</b> 18

# LISTA DE GRÁFICOS

Gráfico 1: Quantidade de dados originais vs quantidade de dados recu	uperados pelo
IPED	16
Gráfico 2: Quantidade de dados originais vs quantidade de dados rece	uperados 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
Apêndice A - Procedimentos executados desde a sanitização da mídia, criação e	.23
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	40
de relatorios	.43
Apenuice O - Telas da analise da imayem yeradas pelo IF LD	. <del>4</del> J

# 1 INTRODUÇÃO

Áreas como comunicação, ciência, economia, dentre outras, têm sido impulsionadas pela evolução tecnológica. Fato decorrente da democratização do acesso às tecnologias e consequentemente 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 (Tecmundo, 2018), conforme demonstrado na figura 1.

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



Fonte: Tecmundo, 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.





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 minimante 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

Fonte: CTIR Gov, 2019.

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).



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, concluise 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 grade volume de dados	Detecção de nudez			
	Interface intuitiva	Identificação de criptografia			
	Multiplataforma (Windows, Linux e Mac OS)	Localização de palavras			
	Portabilidade e	Rastreamento de locação			
	processamento em batch	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.

Com o objetivo de atingir os objetivos acima apresentados, o seguinte laboratório foi utilizado:

Quadro 2: Configuração do laptop

HOST HOSPEDEIRO			SISTEMAS VIRTUALIZADOS		
HARDWARE	S.O.	PROGRAMA DE VIRTUALIZAÇÃO	HARDWARE	S.O.	SW FORENSE
- processador	Debian	Oracle VM	- processador	Windows 7	
Intel Core i7-	GNU/Linux	VirtualBox 6.0.14	Intel Core i7-	Professional	
7700HQ	10 (buster)		7700HQ	(service	FTK 7.1
2,80GHz * 8			2,80GHz * 2	pack 1)	
			- 8GB de		
- 16GB de			memória RAM		
memória					
RAM					IPED
					3.15.6
- disco rígido					
de 1 TB					

Fonte: Própria autora, 2019.

Em um dispositivo de 32GB, conforme as especificações apresentadas no quadro 3, foram armazenados 323 arquivos, distribuídos em 6 diretórios, totalizando 21GB em dados, distribuídos da seguinte forma:

Quadro 3: Base de dados

DIRETÓRIOS	QUANTIDADE DE ARQUIVOS	TIPO DOS ARQUIVOS
1. DOC	79	.doc / .odt
2. FOTOS	105	.jpeg
3. VIDEOS	71	.mp4 / .mp3 / .wmv
4. PLANILHA	01	.ods
5. PDF	62	.pdf
6. PPT	05	.ppt / .odp / .pptx

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 S01<sup>1</sup>.

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.

<sup>1</sup> Para obter informações sobre os formatos de arquivos de imagens forense, acesse https://kb.digitaldetective.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, consequentemente, 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 ο cálculo de hash, indexação do conteúdo dos arquivos(indexFileContents), indexação do espaco não alocado (indexUnallocated), cálculo de assinatura (processFileSignatures), carving (enableCarving), expansão decontainers (expandContainers), dentre diversas outras opcões comentadas no próprio arguivo (IPED - Manual, 2019).

Outro arquivo importante de configuração é o LocalConfig.txt onde são definidas configurações específicas do ambiente, como diretório temporário indexTemp, se odiretório 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, comoresolução, 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, decriptografar 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

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.

🔎 Indexador e Processador de Evidências Digitais 3	3.15.6 [Case: Z:\analise_iped]							
[No filter]	ed Duplicates Search:						Optic	ons Help 🗹 1/4
×								
	Gallery Map							
Categories	62 Score Name	Type Siz	ize (84M Deleted	Category	Created	Modified	Accessed	Hash
Documents (94)	1 11% 7 - Subprogramas.pdf	pdf	931,947 true	PDF Do	11/14/2019 12:43:39 UTC	08/31/2016 19:35:38 UTC	11/15/2019	73BF7FC986A803
PDF Documents (62)	2 11% 7_Curriculo CC T REJANE A.	. pdf	82,553 true	PDF Do	11/14/2019 12:43:39 UTC	02/27/2019 12:33:18 UTC	11/15/2019	B1C076225701B2
Text Documents (32)	4 11% Todos juntos odf	pdf 12	4 407 530 true	PDF Do	11/14/2019 12:43:40 UTC	07/22/2019 08:02:58 UTC	11/15/2019	B7C57520CAE0B
Empty Files (2)	5 11% Todos os slides.pdf	pdf 2	2,422,490 true	PDF Do	11/14/2019 12:43:41 UTC	07/23/2019 09:54:18 UTC	11/15/2019	4B66767F6D6456
Folders (11)	6 🔲 11% 📑 tudao_ataque1.pdf	pdf 21	1,373,587 true	PDF Do	11/14/2019 12:43:41 UTC	10/02/2019 02:22:44 UTC	11/15/2019	465FFF519E6596
Image Disks (1)	7 11% Tunelamento SSH.pdf	pdf	878,208 true	PDF Do	11/14/2019 12:43:42 UTC	08/14/2019 07:24:44 UTC	11/15/2019	8C628A2DEA8BF
Other Disks (1)	8 11% tutorialebaula.pdf	pdf 5	5,232,089 true	PDF Do	11/14/2019 12:43:42 UTC	05/31/2019 00:57:00 UTC	11/15/2019	531DA390FA55C
Multimedia (185)	9 11% Verificação de Aprendizagem. 10 11% Vi Eirowall Cabarito pdf	par	33,189 true	PDF Do	11/14/2019 12:43:43 UTC	08/27/2019 17:49:52 UTC 09/27/2019 16:25:20 LITC	11/15/2019	508544520FE4EA
Audios (1)	11 11% VolP1.pdf	pdf	716.514 true	PDF Do	11/14/2019 12:43:43 UTC	08/21/2019 17:33:38 UTC	11/15/2019	48C825B86E6B0
Images (113)	12 11% VOIP gciber2.pdf	pdf	28,551 true	PDF Do	11/14/2019 12:43:43 UTC	09/02/2019 15:15:20 UTC	11/15/2019	16F66B66F8CFEE
L Videos (71)	13 11% Volatility-Cheatsheet.pdf	pdf	849,883 true	PDF Do	11/14/2019 12:43:43 UTC	09/01/2018 00:55:24 UTC	11/15/2019	CFD181A053BEC
Other Files (155)	14 11% Warranty.pdf	pdf 1	1,172,289 true	PDF Do	11/14/2019 12:43:44 UTC	07/26/2018 07:31:46 UTC	11/15/2019	B5FB47D0642043
Plain Texts (45)	15 11% Windows-Forensics-Poster.p	df pdf 1	1,444,142 true	PDF Do	11/14/2019 12:43:44 UTC	03/07/2019 20:00:58 UTC	11/15/2019	6600EAA3E6BE34
Dther Texts (45)	16 11% Windows_gciber15.pdf	par	50,909 true	PDF Do	11/14/2019 12:43:44 UTC	09/04/2019 15:31:36 UTC 11/20/2016 02:12:19 UTC	11/15/2019	4AEDDD058C114
Presentations (5)	18 11% 01 - Capa pdf	ndf	4 074 true	PDF Do	11/14/2019 12:43:36 UTC	09/04/2017 21:21:18 UTC	11/15/2019	48CB0A5BBA882
Spreadsheets (1)	19 11% 01 ARSF - Fundamentos.pdf	pdf	571,951 true	PDF Do	11/14/2019 12:43:36 UTC	09/25/2019 11:18:28 UTC	11/15/2019	B6916029D4B660
	20 11% 01-anonimizacao.pdf	pdf 6	6,600,839 true	PDF Do	11/14/2019 12:43:36 UTC	09/27/2018 12:04:20 UTC	11/15/2019	3636C4CFE80CF
	21 11% 01-SGM-105-REV5.pdf	pdf 7	7,758,320 true	PDF Do	11/14/2019 12:43:36 UTC	07/25/2019 19:03:58 UTC	11/15/2019	75DE8EBE9E82B
	22 11% 01_02_2010_MetodologiaEs.	pdf	343,179 true	PDF Do	11/14/2019 12:43:37 UTC	05/25/2010 02:05:34 UTC	11/15/2019	A09BC85E99B0E
								7 F
📋 Bookmarks 📃 Metadata 📃 🗗 🗖	Attachs/Subitems Parent Item Duplicates	N	- 🗗 🗖 🔍 💷	The prev	iew may be inaccurate. Doub	le click to open the file extern	ally.	Fix Viewe
				Taut Mater	data Draview			
[No Rookmarks]			Hex	Text Meta	uata Preview			
relation1				b 🐻 🗈	1 of 58	■ ■ 104%	• +	
					ମ୍ବ ଦ୍ରା 📄			
								4
								~
						Capit	ulo 🥑	
						-		
						Subprog	gramas	;
				-				· 8

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				

Quadro 5: Quantidade de arquivos recuperados pelo IPED

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

Quadro 6: Quantidade de arquivos com conteúdo exibido corretamente

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.

		- 1-		· · J ·				
essData Forensic Toolkit	Version: 7.1.0.290 Da	tabase: localho	ost Case: 01					ð 🗾
Edit View Evidence	Filter Tools M	anage <u>H</u> elp						
Titure land			The Manager 1 🛋 🛧 1771 - 2	2				
Hiter: jpeg		٣	Filter Manager	8				
ore Overview Email	Graphics Video Int	ernet/Chat B	Bookmarks Live Search Index Search System	Information				4
vidence Items			d b	File Content				
Nuterice items			4.9		red Natural			
Evidence imagem02.001				Thex Text Thite	Ted Traction			
	2]							
🖻 🖵 🧰 [root]								L L
	IA .							ed
-C) 75 IOC								
								Wet
🖻 🖵 🛅 IPT								Ē
System	Volume Information							
	apacej							
						-		
					Capíti			
							_	
					Nome	es. Vinculações e	Escopos	
				5				
				File Content	Properties	Hex Interpreter		
a 🖊 🍇 💶 🔳	-	<b>≣</b> • A A	Normal	one: E. South America	Davlight Time (From	local machine)		<u>*×0</u>
Name	Label Item #	Evt.	Path	Category	P-Size L-Size	MD5	SHA1	Cre A
20160805 141854 inc	1078	ing	imagem02.001/NONAME [EAT32]/[root]/IDE/201/	6080 IPEG EXTE	3056 KB 3048 k	B ef18b54848fc8e1e832a502587db8a71	8a4c6baa8f1048db27c15de3dd5eec94360d225e	11/
20160805 143050.ipg	1079	ipg	imagem02.001/NONAME [FAT32]/[root]/IDF/2010	6080 JPEG EXIF	3008 KB 3004 K	B b83ee3eca92f80220294671283d922d3	1089ffb5268e550a5fba2aaccbd87cf24c3cfc64	11/
20160805_144248.jpg	1080	jpg	imagem02.001/NONAME [FAT32]/[root]/IDF/2016	6080 JPEG EXIF	3072 KB 3068 K	B b5a701f87fafb33ac74ced26ba8f345d	a6dab6340c1829b6e7fbeeb1a790e2dd509f997d	d 11/
20160809_091951.jpg	1081	ing	imagem02.001/NONAME [EAT32]/[root]/IDE/2016	6080 1PEG EXTE	2040 KR 2020 K	// -476620222204-10650-08	and the second sec	
		76.41	indigenerative strength of the statistic statistics of the statist		30-10 KD 3023 H	CHC91002399976529650HC1096020C30	9fe156058a74724b233cb3f25ec6b04ceb5bee88	3 11/
20160809_142332.jpg	1082	jpg	imagem02.001/NONAME [FAT32]/[root]/!DF/2016	6080 JPEG EXIF	3072 KB 3068 K	B ed5751a298c18bbe7431d26606f90980	9fe156058a74724b233cb3f25ec6b04ceb5bee88 8d8c3ef94ace72f1df65624d46143323122a28bb	3 11/ 11/
20160809_142332.jpg 2_Historico_Escolar_Gra	1082 . 1083	jpg pdf	imagem02.001/NONAME [FAT32]/[root]/IDF/2016 imagem02.001/NONAME [FAT32]/[root]/IDF/2_Hi	6080 JPEG EXIF istori Adobe Ac	3072 KB 3068 k 80.00 KB 65.97	05         C+C476539435CE354220+C104e550C98           08         ed5751a298c18bbe7431d26606f90980           KB         6c7bfec0477e27049cadf30a121a7504	9fe156058a74724b233cb3f25eC6004ce55bee88 8d8c3ef94ace72f1df65624d46143323122a28bb b74601c9dd15e157075b0583ee75266e4538e	3 11/ 11/ 11/ ≡
	eessData Forensic Toolkit Edit View Evidence Filter: peg Ore Overview Email Evidence Items © Underce Items © Item (International International Internatione Internationa	Personal Astronomic Toolkit Version: 7.10.290 Da Edit View Evidence Filter Iools M Filter: peg tore Overview Email Graphics Video Int Evidence Items  Evidence Items  Evidence Tools  Filter: peg tore Overview Email Graphics Video Int Evidence Items  Evidence Items  Evidence  Filter: peg tore Overview Email Graphics Video Int Evidence Items  Evidence Items  Evidence  Filter: peg tore Overview Email Graphics Video Int Evidence Items  Evidence Items  Evidence  Filter: peg tore Overview Email Graphics Video Int Evidence Items  Evidence  Evidence Evidence  Evidence  Evidence Evidence  Evidence Eviden	EeseBata Forensi: Toolkit Version: 71.0.290 Database: localh Edit View Evigence Filter Iools Manage Help Filter: peg  Tore Overview Email Graphics Video Internet/Chat E Evidence Items  Evidence Items Evidence Items Evidence Items Evidence Items  Evidence Items Evidence Items Evidence Items Evidence Evidence Evidence Evidence Evidence Evidence Evid	ExestData Forensic Toolkit Version: 7.1.0.290 Database localhost Case 01         Edit View Evidence Filter Tools Manage Help         Filter:       peg         Filter:       peg         Evidence       Image: Tools Manage Help         Evidence Items       Image: Tools Manage Help         Image: Tool Item       Image: Tool Item         Image: Tool Item       Image: Tool Item	ExcessData Forensic Toolkit Version: 71.0.290 Database: localhoot Case 01         Edit View Evidence Filter Iools Manage Help         Filter:       peg         Filter:       peg         Filter:       Pilter Manager         Evidence       Image: State Filter:         Image: State Filter:       Image: Stat	ExestData Forensi: Toolkit Version: 7.1.0.290 Database: localhost Case 01         Edit Yiew Evidence Filter Jools Manage Help         Filter:       peg         Filter Source Filter       Filter Manager.         Image:       Image:         Evidence Items       Image:         Evidence       Filter Manager.         Evidence       Filter Manager.         Evidence       Image:         Evidence       Image:	reseData Forensic Toolkit Version: 7.1.0.290 Database localhost Case 01  file View Evidence Filter Iools Manage Help  Filer: peg  Filer: peg  File Content  File Content File Content	eexbats forenisis Toolist Version: 7.10.200 Database localhost Case (1)

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: Quantida	de 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

Quadro 8. Quantida	ide de arquivos com conteudo 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:

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

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

 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:



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 o programa recuperaou aproximadamente 86% em relação aos 57% recuperados pelo

#### FTK, conforme demonstrado no gráfico 4.





Legenda:

PERCENTUAL DE ARQUIVOS RECUPERADOS PELO IPED PERCENTUAL DE ARQUIVOS RECUPERADOS PELO FTK

#### **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 pro 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.

ACESSDATA. Product Downloads. Disponível em: https://accessdata.com/productdownload/forensic-toolkit-ftk-version-7.1.0. Acesso em: 11 nov. 2019.

ACESSDATA. 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-quaisleis-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-dadoscresce-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-peritodigital-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-eforense-computacional-conheca-os-softwares-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/126654-4bilhoes-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 writ <mark>ing '/dev/adb'. Na space left en device</mark>
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 c	la mídia				
Filesystem	Size	Used	Avail	Use%	Mounted on
udev	7.8G	Θ	7.8G	0%	/dev
tmpfs	1.6G	9.7M	1.6G	1%	/run
/dev/sda2	92G	7.8G	79G	9%	/
tmpfs	7.8G	Θ	7.8G	0%	/dev/shm
tmpfs	5.0M	4.0K	5.0M	1%	/run/lock
tmpfs	7.8G	Θ	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	0326	3106	613G	35%	/media/user/Seagate Exp
/dev/sdc	30G	22G	8.8G	71%	/media/user/F613-7B26

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 comAccessData FTK Imager 4.2.1.4

9						AccessData FTK Imager 4.2.1.4
Ei	e <u>V</u> iew <u>M</u> ode <u>H</u> elp	_				
	<u>A</u> dd Evidence Item	•   🖸 🕄   🗋 🖻 🔤   🐱	के रेड्से सेड्रे 💡 🔒			
	Add All Attached Devices	× File List				
6	Image Mou <u>n</u> ting	Name	Size	Туре	Date Modified	
9	<u>R</u> emove Evidence Item					
4	Remove All Evidence Items					
	<u>C</u> reate Disk Image					

Fonte: Própria autora, 2019.

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

Name		Size Type	
S	elect Source		
Please Select the Source Evi Physical Drive Logical Drive Image File Contents of a Folder (logical file-level analysi	dence Type s only; excludes d	leleted, unallocate	ed, etc.)
O Femico Device (multiple	e CD/DVD)		
< Back	Next >	Cancel	Help
	Name Si Please Select the Source Evi Physical Drive Logical Drive Image File Contents of a Folder (logical file-level analysi Femico Device (multiple)	Name         Select Source         Please Select the Source Evidence Type <ul> <li>Physical Drive</li> <li>Logical Drive</li> <li>Image File</li> <li>Contents of a Folder (logical file-level analysis only; excludes of Femico Device (multiple CD/DVD)</li> </ul> < Back     Next >	Name       Size       Type         Select Source         Please Select the Source Evidence Type <ul> <li>Physical Drive</li> <li>Logical Drive</li> <li>Image File</li> <li>Contents of a Folder (logical file-level analysis only; excludes deleted, unallocate</li> <li>Femico Device (multiple CD/DVD)</li> </ul> < <ul> <li>Back</li> <li>Next &gt;</li> <li>Cancel</li> </ul>

Figura 11: Selecionando a mídia física

Figura 12: Se	ecionando o drive da mídia
	Select Drive
Sou	rce Drive Selection ease select from the following available drives:
X	\.\PHYSICALDRIVE3 - Lexar USB Flash Drive USB Device [32 ∨
	< Back Finish Cancel Help

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

	Create Image	×
Image Source		
\\. \PHYSICALDRIVE3		
Image Destination(s)	Starting Evidence Number: 1	
Add	Edit Domovo	
Add	Euit Remove	
	Select Image Type	>
Please Select the Desti	ination Image Type	
Please Select the Desti	ination Image Type	
Please Select the Desti	ination Image Type	
Please Select the Desti	ination Image Type	
Please Select the Desti Raw (dd) SMART E01	ination Image Type	
Please Select the Destine Raw (dd) SMART E01 AFF	ination Image Type	
Please Select the Desti Raw (dd) SMART E01 AFF	ination Image Type	
Please Select the Desti Raw (dd) SMART E01 AFF	ination Image Type	
Please Select the Desti Raw (dd) SMART E01 AFF	ination Image Type	

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

6) Em seguida, foi criada um case para a imagem, conforme demonstrado na figura14.

	Evidence Item Information
Case Number:	02
Evidence Number:	02
Unique Description:	
Examiner:	
Notes:	
	< Back Next > Cancel

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.

G: \IMAGENS				Browse
(mage Filename (E	xcluding Extension)			
imagem02				
	Image	in a mont Cine /		
For Raw, E0	1, and AFF formats: 0	= do not fragm	ent 0	
Compress	ion (0=None, 1=Faste	st,, 9=Smalle	est) 0	l
		Use AD Encryp	tion	

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.

	Create Image	
Image Source		
\\. PHYSICALDRIVE3		
	Starting Evidence Number:	1
Cr/IMACENS/imagem02	[raw/dd]	
or prince to prince inor	[ anyog	
Add	Edit	Remove
Add	Edit	Remove
Add	Edit Add Overflow Location	Remove
Add	Edit Add Overflow Location	Remove
Add	Edit Add Overflow Location y are created Precalculate	Remove Progress Stati
Add Verify images after the Create directory listings	Edit Add Overflow Location y are created Precalculate s of all files in the image after the	Remove Progress Stati

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.

ura 1	7: Finalização da	tela de criação da ima	agem	
		AccessData FTK In	nager 4.2.1.4	
3, 3	• 🛲   📴 🥄   [ ×   File List	) 🖹 📾 <del>o <u>R</u> 22</del>	8.	
		Creating Im	age – 🗆 🗙 Modi	
	Image Source:	\\. \PHYSICALDRIVE2		
	Destination:	G: \imagem		
	Status:	Image created successfu	ly	
	Progress			
Elapsed time: 0:44:56 Estimated time left:				
	Image Summar	y Close		
	1			
		Drive/Image Ve	rify Results 🛛 🗕 🗖 🗙	
	Sector count	4852	28544	
	MD5 Hash			
	Computed hash	4749	3991c147d018e3446357f5b0f1ad	
	Report Hash	4749	3991c147d018e3446357f5b0f1ad	
	Verify result	Mat	ch	
	SHA1 Hash			
	Computed hash	a041	ce6f2ce94c6432951c6e263af0b539d48	
	Computed hash Report Hash	a041 a041	ce6f2ce94c6432951c6e263af0b539d48 ce6f2ce94c6432951c6e263af0b539d48	
	Computed hash Report Hash Verify result	a041 a041 Mat	ce6f2ce94c6432951c6e263af0b539d48 ce6f2ce94c6432951c6e263af0b539d48 ch	
	Computed hash Report Hash Verify result Bad Blocks List	a041 a041 Mat	ce6f2ce94c6432951c6e263af0b539d48 ce6f2ce94c6432951c6e263af0b539d48 ch	

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.

	C' û	🔽 🔒 ht	tps://servicos	.dpf.gov	v.br/ferra	amentas/IP	ED/3
🐻 Centr	o de Instrução d	Captive Portal	Login P  🖈	SIMOC	- Simula	dor de 🏾 🌍	CIGE
POLICIA	MJ - Departan	nento de Polícia	Federal				
	CGTI - Coorde	enação Geral de	Tecnologia	da Info	rmação	)	
FEDERAL	Domingo, 17 d	le Novembro de	2019				
Name	1		Last modif:	ied	<u>Size</u>	Descripti	on
-							
Pare Pare	ent Directory				-		
Pare Pare	ent Directory )-3.15.6-with-e	xtra-tools.zip	2019-05-23	01:35	- 367M		
Pare Pare IPEI	ent Directory )-3.15.6-with-e )-Manual_pt-BR.	xtra-tools.zip pdf	2019-05-23 2019-02-27	01:35 15:16	- 367M 1.1M		
Pare IPEL IPEL Lice	ent Directory )-3.15.6-with-e )-Manual_pt-BR. ense.txt	xtra-tools.zip pdf	2019-05-23 2019-02-27 2019-03-29	01:35 15:16 09:53	- 367M 1.1M 1.0K		

Fonte: Própria autora, 2019.

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

F (11 (1010 1.1.4 (

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) <u>64-Bit</u> Server VM (build 25.221-b11, mixed mode)

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.

		l Inve Co	untral Dana	1					
ſ		eperal I	Indate 13	a Security /	Vdvanced				~
			opuate sa	Security 7	kuvanceu				
		View and	manage Ja	va Runtime ver	sions and settin	ngs for Java applications ar	nd applets		
								View	
	4	Java Ru	ntime Envi	ronment Settir	ngs				×
		Lines a							
		User S	/stem						
		Pla	Product	Location	Path	Runtime Parameters	Enabled	Archite	
		1.8	1.8.0_231	http://java	C:\Program	-Xmx6144m		x86_64	
/									
						Find	Add	Remove	
							ОК	Cancel	
									_

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: Arc	uivos d	le confi	guração	do	<b>IPED</b>
				J		

e ► Downloads ► IPED-3.15.6-with-extra-tools ►	iped-3.15.6 🕨
Share with  Print New folder	
Name	Date modified
퉬 bin	5/23/2019 1:14 AM
퉬 conf	5/23/2019 1:14 AM
퉬 htm	5/23/2019 1:14 AM
퉬 htmlreport	5/23/2019 1:14 AM
퉬 jre	5/23/2019 1:14 AM
\mu lib	5/23/2019 1:14 AM
퉬 licenses	5/23/2019 1:14 AM
퉬 log	9/16/2019 12:00 AM
🌗 profiles	5/23/2019 1:14 AM
\mu sources	5/23/2019 1:14 AM
퉬 tools	5/23/2019 1:14 AM
🔎 iped	3/29/2019 9:53 AM
📓 iped	3/29/2019 9:53 AM
IPEDConfig	11/12/2019 11:38
IPED-Manual_ptBR	2/27/2019 3:16 PM
License	3/29/2019 9:53 AM
LocalConfig	11/12/2019 9:33 PM
Release Notes_ptBR	3/29/2019 9:53 AM
Third party licenses	3/29/2019 9:53 AM

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.

I	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	
1	# Enables dettection of more than 70 idioms in document files. enableLanguageDetect = false	
	<pre># 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 insatisfatory # 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</pre>	
	<pre># Indexes files contents. If disabled, indexes only the properties of files. indexFileContents = true</pre>	
	# 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 (64К) of the file. # It's necessary to enable "addUnallocated" and to configure "ledwkffPath". enableKFFCarving = false	
I	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:

.\iped.jar -d <CaminhoDeLocalizaçãoDaImagem> java -jar -0 <CaminhoDeLocalizaçãoDoDiretório\_indexIPED>

COO - De Computer + Sy	vstem Reserved (E:) index iped		Computer >	System Reserved (E:) > temp_index	✓ 4y Search tem	p_index
Organize   Include in library	✓ Share with ✓ New folde	r	Organize   Include in libra	ry 🔻 Share with 👻 New folder		
✓ Favorites ■ Desktop 30 Downloads 30 Recent Places	Name	Date moo This fold	☆ Favorites ■ Desktop ♪ Downloads > Recent Places	Name	Date modified Type This folder is empty.	Size
<ul> <li>Libraries</li> <li>Documents</li> <li>Music</li> </ul>			Documents			
Pictures     Videos	Windows PowerShell PS C:\Users\rejane\Dowr Directory: C:\Users	loads\IPED-3.15	.6-with-extra-tools\iped ls\IPED-3.15.6-with-extra	-3.15.6> dir a-tools\iped-3.15.6		
Computer Comput	$\begin{array}{c c c c c c c c c c c c c c c c c c c $	ttyriteTime ) 11:14 AM 11:14 AM 11:14 AM 11:14 AM 11:14 AM 11:14 AM 11:14 AM 11:14 AM 11:14 AM 12:00 AM 12:00 AM 12:14 AM 12:14 AM 12:14 AM 12:00 AM 12:03 AM 1	Length Name bin conf tion lite lite lite lite lite lite lite lite	odf		

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.

								×
🕘 🔍 🔻 🚺 🕨 Libraries	s 🕨 Document	s ▶ temp_iped ▶		<b>- - </b> <sup>4</sup> <del>•</del>	Search temp_ip	ed		٩
Organize 👻 Share wi	ith 🔻 New	folder				== -		0
✓ ★ Favorites ■ Desktop	Docume	nts library			,	Arrange by: F	older 🔻	
Downloads     Recent Places     Documents     My Docume     Difference     Mysic	Name Mane indexador-temp1573829554930 indexador-temp1573829557805		1	Date modified 11/15/2019 12:52 11/15/2019 12:53	Type File folder File folder	Size		
Indexador e Processad	lor de Evidência Wait, dec	s Digitais 3.15.6 oding image Z:\imagem\im	agem.00	01	F	Preview Case	- C	ause
Processing Time	0h 2m 41s	IgnoreHardLinkTask	05 (0%)	Worker-0	S. Waiting Item			
Estimated Finish	-	TempFileTask		Worker-1	Waiting Item			
Mean Speed	0 GB/h	SignatureTask	0s (0%)		g tottai			
Current Speed	0 GB/h	SetTypeTask	0s (0%)					=
Volume Found	0 MB	SetCategoryTask	0s (0%)					
Volume Processed	0 MB	RefineCategoryTask	0s (0%)					
Items Found	0	HashTask	0s (0%)					
Items Processed	0	KFFTask						_ L
Actual items process	ed 0	LedKFFTask	-					
Subitems Processed	0	DuplicateTask	0s (0%)					
Carved items	0	ParsingTask	0s (0%)					
Carved discarded	0	RegexTask	0s (0%)					
Exported items	0	LanguageDetectTask	0s (0%)					
Exported items Ignored items	0	LanguageDetectTask NamedEntityTask	0s (0%) -					

Figura 25<sup>.</sup> 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 :\Users\rejane\Downloads\IPED-3.15.6-with-extra-tools\iped-3.15.6> java -jar .\iped.jar -d Z:\imagem\imagem.001 alise\_iped finished. k 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

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

#### **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.



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

igura 29: Acessando	o o FTK					
🚾 AccessData Forensic Toolkit	t Version: 7.1.0.290					23
File Database Case Tools	Manage Help					
Cases						
Name D	ate Modified		Case ID	n/a		
			Case Owner	n/a		
			Reference	n/a		
			Date Modified	n/a		
			Date Accessed	n/a		
			Date Created	n/a		
			Case Path	n/a		
			Description File	× n/a		
	Please Authenticate		<b>—</b>			
	User Name:					*
	user					
	Password:					
	***					
	'					
			OK Cancel			
	Figura 29: Acessando             AccessData Forensic Toolkit         File       Database         Cases         Name       D	Figura 29: Accessando o FTK         AccessData Forensic Toolkit Version: 7.1.0.290         File Database Case Tools Manage Help         Cases         Name         Date Modified         Please Authenticate         User Name:         user         Password:         ****	Figura 29: Accessando o FTK         AccessData Forensic Toolkit Version: 7.1.0.290         File Database Case Tools Manage Help         Cases         Name         Date Modified         Please Authenticate         User         Password:         ****	Figura 29: AccessData Forensic Toolkit Version: 7.1.0.290         File       Database       Case       Tools       Manage       Help         Cases       Name       Date Modified       Case ID       Case Owner         Reference       Date Modified       Date Accessed       Date Accessed         Date Created       Case Path       Description File         Viser       Please Authenticate       Viser         Viser       Password:       ***	Figura 29: Accessando o FTK         AccessData Forensic Toolkit Version: 7.1.0.290         File       Database         Cases         Name       Date Modified         Case Owner       n/a         Date Modified       Case Owner         Date Modified       n/a         Date Modified       n/a         Date Modified       n/a         Date Accessed       n/a         Date Accessed       n/a         Date Created       n/a         Description File          User Name:          User Name:          OK       Cancel	Figura 29: AccessData Forensic Toolkit Version: 7.1.0.290         File Database Case Tools Manage Help         Cases         Name       Date Modified         Case Owner       n/a         Date Modified       n/a         Date Accessed       n/a         Date Created       n/a         Date Nodified       n/a         Date Nodified       n/a         Date Created       n/a         Date Name:       x         User Name:       x         OK       Cancel

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: Crian	ido um case	Figura 31: Configurando a case
🏧 AccessData F	Forensic Toolkit Version: 7.1.0.290 Database: localhos	2 III New Case Options
File Database	Case Tools Manage Help	) Owner: user
Cases	New	Case Name: 01
Name	Open	Reference:
		Description:
		Description File:
		Case Folder Directory: Z:\analise_ftk
		Processing profile
		Forensic Processing eDiscovery Processing Processing Basic Assessment
		Image Processing Video Processing All Communication
		Customize
		Profile: Forensic Processing

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

Figura 32: Inclusão da image	m na case
🚾 AccessData Forensic Toolkit Version: 7	7.1.0.290 Database: localhost Case: 01
<u>File Edit View Evidence Filter</u>	<u>T</u> ools <u>M</u> anage <u>H</u> elp
Filter: - unfiltered -	<ul> <li>Filter Manager.</li> </ul>
Explore Overview Email Graphics	Video Internet/Chat Bookmarks Live S
Evidence It Manage Evidence	
Evidence     Display Name     imagem02.001	State   +
File List	
	Evid
Add	Remove Choose Restore Poi
Case KFF Op	otions

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

The Data Processing Status		
File Tools		
<ul> <li>□ Add Evidence Jobs</li> <li>imagem02.001 (Finished)</li> <li>□ Additional Analysis Jobs</li> <li>□ Live Search Jobs</li> <li>□ Other Jobs</li> </ul>	Add Evidence Progress         Overall:         Discovered:       662         Processed:       662         Indexed:       662         Process State:       Finished         Evidence Item       Name:         Name:       Imagem02.001         Process Manager:       ocalhost	Messages           Type         Message           TWFO         [9:50 PM 11/16/2019] Using engine localhost           TWFO         [9:50 PM 11/16/2019] Database preparation started           TWFO         [9:50 PM 11/16/2019] Database preparation finished           TWFO         [9:50 PM 11/16/2019] Processing started           TWFO         [9:50 PM 11/16/2019] Processing started           TWFO         [9:51 PM 11/16/2019] Processing finished           TWFO         [9:51 PM 11/16/2019] Database optimization started           TWFO         [9:52 PM 11/16/2019] Database optimization finished           TWFO         [9:52 PM 11/16/2019] Database optimization finished           TWFO         [1:40 PM 11/16/2019] Indexing finished           TWFO         [1:40 PM 11/16/2019] Indexing finished           TWFO         [1:40 PM 11/16/2019] Job Size 2PM to 11/16/2019 11:40:53 PM           Processing:         00:00:21 = 11/16/2019 9:50:22 PM to 11/16/2019 9:51:56 PM           Destpresensing:         00:00:21 = 11/16/2019 9:50:24 PM to 11/16/2019 11:40:53 PM           Indexing time:         01:50:04 = 11/16/2019 9:50:49 PM to 11/16/2019 11:40:53 PM
	Job Eolder Engine Monitor Remove when finished	Pause Cancel <b>Gose</b>

Fonte: Própria autora, 2019.

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

analise_ftk /	01 -	Q <b>∷</b> ▼ Ξ	×
	Name		⇒ S
	5	CaseSettings.xml	1
nts		dts_idx	7
		EvidenceHistory.log	2
		Faulted.bin	С
cations		Jobs	1
		TL	1
	5	Owner_Info.xml	2
		proc_mgr_file.txt	1
		thumbnails	2

Figura 34: Diretórios e arquivos gerados pelo FTK

# 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.



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



Figura 36: Tela do relatório gerado pelo FTK

# 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.

🔎 Indexador e Processador de Evidé	ências Digit	ais 3.15.6 [Case:	Z:\analise_iped]								- 6 <mark>×</mark>
[No filter]	Filter L	Listed Duplicates	Search:							•	Options Help 0 / 497
Categories »1 🔹	Tat	ble Galler	y Map								
🔻 🚞 Categories	11	Score	Name	Туре	Size (30,526	Del	Category	Created	Modified	Accessed	Hash
Documents (94)	1	24%	Ê1		16,384	false	Folders				DF151CFDA404201970
PDF Documents (62)	2	24%	📄 System Volume		16,384	false	Folders	11/14/2019 12:	11/14/2019	11/14/2019	60A2D09E9E0D3609440
Text Documents (32)	3	24%	E _OTOS		16,384	true	Folders	11/14/2019 12:	11/14/2019	11/14/2019	21662002F302D629216
Empty Files (2)	4	24%	0C_ 🍯		16,384	true	Folders	11/14/2019 12:	11/14/2019	11/14/2019	4081281B22390C06E70
Empty riles (2)	5	24%	📄 _LANILHA		16,384	true	Folders	11/14/2019 12:	11/14/2019	11/14/2019	3052A0AF1899198BD31
Folders (11)	6	24%	DF		16,384	true	Folders	11/14/2019 12:	11/14/2019	11/14/2019	DBA51AD1460AE13A19E
Image Disks (1)	7	24%	<u>Грт</u>		16,384	true	Folders	11/14/2019 12:	11/14/2019	11/14/2019	9DCA7CE3FF47EC2BA5
Multimedia (185)	8	24%	DEOS		16,384	true	Folders	11/14/2019 12:	11/14/2019	11/14/2019	23551423327DED30566
Other Files (155)	9	24%	📄 FAT32		32,008,830,9	false	Folders				
► Plain Texts (45)	10	24%	📄 \$OrphanFiles		0	false	Empty Fil				D41D8CD98F00B204E9
Proceedations (5)	11	24%	📄 \$Unalloc		0	false	Empty Fil				D41D8CD98F00B204E9
Presentations (5)											
Spreadsheets (1)											
Fonte: Própria aut	ora, 2	2019.									

Figura 37: Diretórios recuperados pelo IPED

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

Indexador e Processador de Evidê	ncias Digitai	s 3.15.6 [Case: Z:\analise_iped]							
[No filter]	Filter Li	sted Duplicates Search:						•	Options Help 0 /
Categories 🔭 🔹	🗋 Tabl	e Gallery Map							- <b>d</b> *
Categories	185	Score Name	Туре	Size (21,055 Del	Category	Created	Modified	Accessed	Hash
Documents (94)	1	EGEND~1.MP3	mp3	8,363,565 true	Audios	11/14/2019 12:	08/20/2014	11/15/2019	A896B71A5E2E34A33
PDF Documents (62)	2	3% _5CURS~1.MP4	mp4	541,028,598 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	AAFF1B308C1259C24
Text Documents (32)	3		mp4	511,704,979 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	E0E9C9838AC92A328
Empty Files (2)	4		mp4	233,976,100 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	0DAF38D0429B1AD1
Enipty riles (2)	5		mp4	631,026,628 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	DC7A1DE47D610CAA
Folders (11)	6	3% _3CURS~1.MP4	mp4	572,247,898 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	7CE5C3984885D389
Image Disks (1)	7		mp4	340,256,863 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	35DC82310AB8816B6
Cther Disks (1)	8		mp4	76,893,303 true	Videos	11/14/2019 12:	08/13/2014	11/15/2019	2E70703D7974B3D29
🔻 🚞 Multimedia (185)	9		mp4	606,773,820 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	F1F5AE9BD1186F249
Audios (1)	10		mp4	702,774,294 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	CA5D5CB3EDA639F6
Images (113)	11		mp4	523,822,878 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	86C03F550BAF650B7
Nidaas (74)	12		mp4	752,247,258 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	7C86CB5FD00DF1AC
Videos (71)	13		mp4	424,804,632 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	DD3E33FB9D17260A
Other Files (155)	14		mp4	319,818,894 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	7B1BD179B5E892EE
Plain Texts (45)	15		mp4	131,421,618 true	Videos	11/14/2019 12:	08/13/2014	11/15/2019	9D69D00A3B7181474
Presentations (5)	16		mp4	677,253,975 true	Videos	11/14/2019 12:	06/21/2019	11/15/2019	2858827D36E00C8B0
Spreadsheets (1)	1/		mp4	80,995,422 true	VIDEOS	11/14/2019 12:	08/12/2016	11/15/2019	E0692233CDA541CD
<u> </u>	18		mp4	396,352,591 true	VIGEOS	11/14/2019 12:	08/12/2016	11/15/2019	3/4A/4/A2/EE/9E3A
	19		mp4	95,485,261 true	VIGEOS	11/14/2019 12:	08/12/2016	11/15/2019	46898FF2A22A4ECA
	20		mp4	283,075,848 true	Videos	11/14/2019 12:	06/22/2019	11/15/2019	50E1D2CD269828CE
	21		mp4	377,268,717 true	videos	11/14/2019 12:	06/22/2019	11/15/2019	BC20B179450CF18A5

Figura 38: Arquivos de vídeos recuperados pelo IPED

Fonte: Própria autora, 2019.

#### Figura 39: Arquivos de fotos recuperados pelo IPED

					•								
🔎 Indexador e Processador de Evidê	ncias Digita	is 3.15.6 [Case: ]	Z:\analise_ip	ed]									
[No filter]	Filter Li	isted Duplicates	Search:								•	Options	Help 0/
Categories »1 🔹	🚺 Tabl	e Gallery	Мар										- 5
Categories	113	Score	Name		Туре	Size (1,055M	Del	Category	Created	Modified	Accessed	Hash	
Documents (94)	1	5%	1 Abdor	minal Ba	jpg	8,376	true	Other Ima	11/14/2019 12:	10/06/2016	11/15/2019	6CADE	8AAD6829DC8
PDF Documents (62)	2	5%	15 - 14,	jpg	jpg	3,981,114	true	Other Ima	11/14/2019 12:	03/08/2017	11/15/2019	D04B5	D7E4733B9403
Text Documents (32)	3	5%	201607	11_140	jpg	2,618,623	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	73C692	2928DA2D7D58
Empty Files (2)	4	5%	201607	11_142	jpg	1,065,931	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	1AE7E/	ADA0750FE408
Empty Files (2)	5	5%	201607 📄	11_190	jpg	1,393,917	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	EFDDE	3EF229FA36E4
Folders (11)	6	5%	201607	11_190	jpg	1,574,813	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	0BF990	05567E80FE55
Image Disks (1)	7	5%	201607 📄	12_135	jpg	1,216,336	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	6C988/	A468DBB5485E
Cther Disks (1)	8	5%	201607	12_151	jpg	1,048,622	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	E361B8	BAB5CEF82454
Multimedia (185)	9	5%	201607	12_171	jpg	692,827	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	99E993	349F1FF773DF
Audios (1)	10	5%	201607	13_114	jpg	1,019,041	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	326703	221EF81CFB7
▼	11	5%	201607	'13_151	jpg	1,130,675	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	EC3822	221FD1C339CI
· · · · · · · · · · · · · · · · · · ·	12	5%	201607	13_151	jpg	853,863	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	DE69D	C048C4E9A8F
Other Images (113	13	5%	201607	13_170	jpg	1,356,963	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	995E1E	EC4D7C1AD18
Videos (71)	14	5%	201607	13_172	jpg	1,749,256	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	94DF61	1A7A35CADD26
Other Files (155)	15	5%	201607	13_192	jpg	1,169,304	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	4E4482	297BDCC6C4F
Plain Texts (45)	16	5%	201607	13_193	jpg	1,600,922	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	EA3450	C01B44D454F9
Presentations (5)	17	5%	201607	13_195	jpg	1,976,552	true	Other Ima	11/14/2019 12:	03/07/2017	11/15/2019	1220E6	6140E02D9CCI
Percendebests (1)	18	5%	201607	14_173	jpg	1,914,733	true	Other Ima	11/14/2019 12:	03/08/2017	11/15/2019	833A5A	D2A23969EE5
opreadsheets (1)	19	5%	201607	14_175	jpg	794,362	true	Other Ima	11/14/2019 12:	10/02/2016	11/15/2019	936BC4	4/3/CDB21CA
	20	5%	201607	14_175	jpg	659,112	true	Other Ima	11/14/2019 12:	03/08/2017	11/15/2019	AF3E34	1348477299AD
	21	5%	201607	15_104	jpg	858,449	true	Other Ima	11/14/2019 12:	03/08/2017	11/15/2019	5882C0	J4/F/DEFB8C4
	22	5%	201607	15_112	Jbd	873,452	true	Other Ima	11/14/2019 12:	03/08/2017	11/15/2019	BD31A/	/F918DE518B1

Fonte: Própria autora, 2019.

#### Figura 40: Arquivos de slides recuperados pelo IPED



Fonte: Própria autora, 2019.

Figura 41:	Planilha recuperada	pelo IPED

PROMINT       Image Details (0)       Preventations (1)       Preventations (2)       First Eact (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)       Image Details (1)         Ima	Indexador e Processador de Evidên	cias Digitais 3.15.6 [Case: Z:\analis	e_iped]						
Categories      Categories      Categories      Categories      POE Documents (4)     POE Documents (2)     Te documents (2)     Te documents (2)     Folders (10)     Poeter Table (2)     Folders (11)     Poeter Table (12)     Poeter Table (13)     Poeter Table (14)     Poeter Table (15)     Poeter Table (14)     Poeter Table (15)     Poeter Table (14)     Poeter Table (15)     Poete	[No filter]	Filter Listed Duplicates Multiple	Filters Applied	Search:				•	Options Help
Categories	Categories »1 🔹	Table Gallery Ma	p						
Documents (4) Port Documents (4) Potential (2) Empty File (2) Folders (1) Potestas (2) Potestas (1) Potestas (2) Potestas (1) Potestas (2) Potestas (2) Potestas (3) Potestas (1) Potestas (2) Potestas (3) Potestas (3) Potestas (4) Potestas (2) Potestas (1) Potestas (2) Potestas (2)<	▼ 🚰 Categories	1 Score Name		A Type Si	ze (OMB) Del.	Category	Created	Modified Accesse	d Hash
Text Documents (2)         Empty Files (2)         Folders (11)         Other Disks (1)         Other Disks (1)         Other Files (2)         Adds (1)         *         Image Disks (13)         Other Files (15)         Plane Tests (45)         Presentations (5)         SpreadSheets (1)         *	PDF Documents (62)	1 <u>44%</u> Cur	sos de 11.ods	ods	14,387 true	Spreadsh	11/14/2019 12:	04/26/2017 11/15/20	19 F652C8
Folders (1)            • Gestão de Riscos em Ativos             • Bookmarks             • Bookmarks             • Bookmarks             • Gestão de Riscos em Ativos             • Security Management (MSISM)         Mestrado         SANS_US,             • CISSP (ISSMP) - Information         Security Management Professional             • Gerência de Redes e Tecnologia Internet             • CISSP (ISSMP) - Information Systems         Security Management Professional             • Gerência de Redes e Tecnologia Internet             • Gerência de Redes e Tecnologia Interne	Text Documents (32)								
The preview may be inaccurate. Double click to open the file externally.     Addios (1)     Addios (1)     Addios (1)     Addios (1)     Addios (1)     Other files (15)     Preview file (15)     Addias (1)     Addias (1)     Addias (1)     Addias (1)     Addias (1)     Addias (1)     Preview file (15)     Preview file (15)     Preview file (15)     Addias     Addias (1)     Addias     Addias (1)     Addias     Adias     Adia     Adias     Adias     Adi	Folders (11)								
Unter Uses (1)         ↓ Autios (1)         ↓ Autios (1)         ↓ Geter Images (11)         ↓ Her, Tent Metadata Preview         ↓ Autil A         ↓ Her, Tent Metadata Preview         ↓ Autil A         ↓ Her, Tent Metadata Preview         ↓ Autil A         ↓ Her, Tent Metadata Preview	Image Disks (1)								
Audios (1)         * Images (113)         Other image	<ul> <li>Other Disks (1)</li> <li>Multimedia (185)</li> </ul>								
Images (113)       Images (113)         Wideos (71)       Other Images (113)         Presentations (5)       Presentations (5)         Spreadsheets (1)       Images (113)         Images (113)       Images (113) <td>Audios (1)</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Audios (1)								
Wdeos (71)       Other Flies (155)         Presentations (5)       Spreadsheets (1)         ■ Bookmarks       *         *       * <t< td=""><td><ul> <li>Images (113)</li> <li>Other Images (113)</li> </ul></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	<ul> <li>Images (113)</li> <li>Other Images (113)</li> </ul>								
Other Files (156) Presentations (5) Spreadsheets (1) Bookmarks *, * Parent Item *, * * * * * * * * * * * * * * * * * *	Videos (71)								
Presentations (5) Spreadsheets (1) ■ Bookmarks No Book	<ul> <li>Other Files (155)</li> <li>Plain Texts (45)</li> </ul>								
Spreadsheets (1) Bookmarks No Bookmarks N	Presentations (5)								
■ Bookmarks Parent Item * The preview may be inaccurate. Double click to open the file externally. ■ Bookmarks ■ Parent Item * Text Metadata Preview ■ A Bookmarks ■ Parent Item * Text Metadata Preview ■ A Bookmarks ■ A B Lockmarks ■ A B L	Spreadsheets (1)								
Bookmarks I Parent Item *a The preview may be inaccurate. Double click to open the file externally. Hex Text Metadata Preview A2 I Star Z = Gestão de Riscos em Ativos A B I CURSO TIPO Lo Universidad Modulo Baster of Science in Information Security Management (MSISM) Mestrado SANS_USJ. 4 Engenharia de Software Pós-Graduação SENAC 5 CISSP (ISSMP) - Information Systems Security Management Professional APERFEIÇOAMENTO ISC2_USA 6 Gerência de Redes e Tecnologia Internet Pós-Graduação UFRJ 7 Gerência de Segurança da Informação Pós-Graduação UFRJ									
Bookmarks       •		-							
Image: Security Management Professional       APERFEIÇOAMENTO       ISC2_USA         Image: Security Management Profesesional       APERFEIÇOAMENTO	🛾 Bookmarks 💦 🔭	📋 Parent Item 💦 🔹 🔻		The preview may l	oe inaccurate. Doul	ble click to open	the file externally.		
A2       fx E = Gestão de Riscos em Ativos         A       B         I       CURSO       TIPO       Lo         2       Gestão de Riscos em Ativos       APERFEIÇOAMENTO       Módulo         3       Master of Science in Information Security Management (MSISM)       Mestrado       SANS_US.         4       Engenharia de Software       Pós-Graduação       SENAC         5       CISSP (ISSMP) - Information Systems Security Management Professional       APERFEIÇOAMENTO       ISC2_USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ	Bookmarks      Ne Bookmarks	1 📄 🕋 _LANILHA	Hex Text	t Metadata Pr	eview				
A     B       1     CURSO     TIPO       2     Gestão de Riscos em Ativos     APERFEIÇOAMENTO       3     Master of Science in Information Security Management (MSISM)     Mestrado       4     Engenharia de Software     Pós-Graduação       5     CISSP (ISSMP) - Information Systems Security Management Professional     APERFEIÇOAMENTO       6     Gerência de Redes e Tecnologia Internet     Pós-Graduação     UFRJ       7     Gerência de Segurança da Informação     Pós-Graduação     UFRJ	[NO BOOKMARKS]		A2	▼ f <sub>X</sub> Σ	E 🗧 🛛 Gestão de	Riscos em Ativo	s		
1       CURSO       TIPO       Lo         2       Gestão de Riscos em Ativos       APERFEIÇOAMENTO       Universida         3       Master of Science in Information       Security Management (MSISM)       Mestrado       SANS_US.         4       Engenharia de Software       Pós-Graduação       SENAC         5       CISSP (ISSMP) - Information Systems       APERFEIÇOAMENTO       ISC²_USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ					A			В	
2       Gestão de Riscos em Ativos       APERFEIÇOAMENTO       Módulo         3       Master of Science in Information       Security Management (MSISM)       Mestrado       SANS_US.         4       Engenharia de Software       Pós-Graduação       SENAC         5       CISSP (ISSMP) - Information Systems       APERFEIÇOAMENTO       ISC2_USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ			1		CURSO			ΠΡΟ	L(
3       Master of Science in Information       Mestrado       SANS_US.         4       Engenharia de Software       Pós-Graduação       SENAC         5       CISSP (ISSMP) - Information Systems       Security Management Professional       APERFEIÇOAMENTO       ISC²_USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ			2 Gest	ão de Risco	s em Ativos		APERE	FICOAMENTO	Universida Módulo
3       Security Management (MSISM)       Mestrado       SANS_US.         4       Engenharia de Software       Pós-Graduação       SENAC         5       CISSP (ISSMP) - Information Systems       Security Management Professional       APERFEIÇOAMENTO       ISC <sup>2</sup> _USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ			Mast	er of Scien	e in Inform	ation	ALLA	LIÇOAMLATO	Wodulo
4       Engenharia de Software       Pós-Graduação       SENAC         5       CISSP (ISSMP) - Information Systems       APERFEIÇOAMENTO       ISC <sup>2</sup> _USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ			<sup>3</sup> Secu	rity Manag	ement (MSI	SM)	Mestrad	0	SANS US.
5       CISSP (ISSMP) - Information Systems Security Management Professional       APERFEIÇOAMENTO       ISC <sup>2</sup> _USA         6       Gerência de Redes e Tecnologia Internet 7       Pós-Graduação       UFRJ			4 Enge	enharia de S	oftware		Pós-Gra	duação	SENAC
2       Security Management Professional       APERFEIÇOAMENTO       ISC2_USA         6       Gerência de Redes e Tecnologia Internet       Pós-Graduação       UFRJ         7       Gerência de Segurança da Informação       Pós-Graduação       UFRJ			CISS	SP (ISSMP)	- Informatio	on System	s		
6 Gerência de Redes e Tecnologia Internet Pós-Graduação UFRJ 7 Gerência de Segurança da Informação Pós-Graduação UFRJ			_ Secu	rity Manag	ement Profe	ssional	APERF	EIÇOAMENTO	ISC <sup>2</sup> _USA
7 Gerência de Seguranca da Informação Pós-Graduação UFRI			6 Gerê	ncia de Red	les e Tecnolo	ogia Intern	et Pós-Gra	duação	UFRJ
· Solution de Segundarde res Staduação - Ories			7 Gerê	ncia de Seg	urança da In	formação	Pós-Gra	duação	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.





Fonte: Própria autora, 2019.