FACULDADE DE TECNOLOGIA DE AMERICANA
CENTRO PAULA SOUZA

VAMILE SANTOS FEIJÓ

PERICIA FORENSE DIGITAL
Recuperação de Imagens com a ferramenta Autopsy

Americana -SP
2020

VAMILE SANTOS FEIJÓ

PERICIA FORENSE DIGITAL
Recuperação de Imagens com a ferramenta Autopsy

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Professor Henry Godoy

Americana -SP
2020

VAMILE SANTOS FEIJÓ

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

F328p FEIJÓ, Vamile Santos

Pericia forense digital: recuperação de Imagens com a ferramenta Autopsy. / Vamile Santos Feijó. – Americana, 2020.

36f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Henri Alves de Godoy

1 Perícia digital 2. Segurança em sistemas de informação I. GODOY, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.3

VAMILE SANTOS FEIJÓ

PERICIA FORENSE DIGITAL
Recuperação de Imagens com a ferramenta Autopsy

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Professor Henry Godoy

Americana, 30 de Junho de 2020

BANCA EXAMINADORA

_____

Prof. Henri A. Godoy
Fatec Americana

_____

Prof. José Martins Junior
Fatec Americana

_____

Prof. Elton Rafael M. De S. Pereira
Fatec Americana

Dedico este trabalho a minha mãe por ter sido a mulher mais forte e inspiradora que eu já conheci.

AGRADECIMENTOS

Agradeço aos meus professores e colegas por me ajudarem a desenvolver este trabalho. E ao meu esposo Danilo por acreditar em mim e me apoiar acima de tudo.

RESUMO

De acordo com ao grande avanço tecnológico e a grande necessidade de empresas e pessoas do uso equipamentos e sistemas, os crimes cibernéticos também evoluíram e assumiram esses equipamentos como ferramenta para suas práticas. Portanto, para que esses crimes sejam investigados, tanto no âmbito judicial, quanto comercial, é necessário um profissional qualificado, sendo esse o Analista Forense , ou Perito Forense. A pesquisa a seguir demonstra alguns procedimentos e ferramentas presentes no ciclo da Perícia Forense Computacional, os procedimentos de coleta, exame, análise e resultados são mostradas ao longo do projeto. Bem como a abordagem de ferramentas utilizadas em alguns desses processos e um estudo de recuperação de arquivos apagados utilizando a ferramenta Autopsy em um dispositivo formatado.

Palavras-chave: Forense. Análise. Evidência. Crimes. Digital.

ABSTRACT

According to the great technological advance and the great need of companies and people to use equipment and systems, cybercrimes also evolved and started to use these equipments as tools for their practices. Therefore, for these crimes to be investigated, both in the judicial and commercial spheres, a qualified professional is required, being this the Forensic Analyst, or Forensic Expert. The following research demonstrates some procedures and tools present in the Computer Forensic Expertise cycle, the procedures for collection, examination, analysis, and results are shown throughout the project. As well as the tools approach used in some of these processes and a study of recovering deleted files using the Autopsy tool on a formatted device.

Keywords: *Forensics. Analysis. Evidence. Cyber Crime.*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Com o grande avanço da tecnologia na área informática, as empresas estão aderindo a medidas tecnológicas para aumentar o seu potencial de mercado, assim como as pessoas estão cada vez mais utilizando computadores e smartphones para fazer coisas que antigamente só eram possíveis presencialmente. Hoje pode-se pagar contas via internet, fazer compras online utilizando apenas o número do cartão de crédito e até mesmo requisitar serviços sem ao menos sair de casa.

Tanta tecnologia e praticidade nos leva a questionar se estamos seguros ao informar nossos dados a sites e aplicativos e a verdade é que nem sempre estamos, uma vasta quantidade de dados importantes e sensíveis fluem no chamado Ciberespaço a todo momento, dando oportunidade a cibercriminosos, utilizarem esses dados para cometer os mais variados crimes virtuais. Antigamente, quando não existia tanta tecnologia, a chave para que todos os crimes fossem resolvidos eram: exames toxicológicos, coleta de impressões digitais, análise de rastros, documentos e outros meios tradicionais. Hoje, com o avanço na área de informática, foi necessário que a área de perícia se adaptasse para que Crimes Cibernéticos fossem resolvidos, surgindo assim a Perícia Forense aplicada à Informática.

A Perícia Forense aplicada à informática possui várias técnicas e métodos que auxiliam os profissionais nas investigações a encontrar evidências deixadas pelos invasores como por exemplo; a identificação da máquina invasora. As análises feitas por um computador, são mais eficazes que impressões digitais, tanto em crimes cibernéticos como em crimes considerados normais, pois uma história inteira de um crime pode ser contada através da recuperação de um arquivo que foi apagado.

Devido ao surgimento e a popularização da internet nas redes no cotidiano da sociedade, especialmente nos últimos anos, a Segurança da Informação está sendo colocada em evidência cada vez mais, pois crimes virtuais têm sido cometidos com maior frequência. A segurança da Informação por sua vez, salienta a ocorrência de crimes virtuais e maneiras de evitá-los ou mesmo minimizá-los. Esses crimes são motivados pela ideia de baixa exposição do criminoso dando a sensação de anonimato, e pelo fato de o criminoso ver a internet como um campo farto de vítimas descuidadas o que facilita a sua ação criminosa sem a utilização de meios violentos.

Diante desse problema, nota-se a importância da ação de uma perícia específica e rigorosa para a determinação de indícios que mostrem o rumo da investigação e processo penal. Nesse aspecto, a perícia forense computacional vem a ser indispensável para a investigação dos crimes virtuais.

Desta forma, com o propósito de levantar e evidenciar conhecimentos que atuam na área da perícia forense computacional na investigação do crime virtual, trazendo concepções de segurança da informação dentro e fora da rede de computadores, dá-se a construção deste estudo a fim de produzir e comprovar conhecimentos nas áreas mencionadas, levando ao entendimento do que envolve o crime virtual e seu método de investigação, proporcionando maior compreensão de áreas de conhecimento pouco mostradas no cotidiano.

Objetivo Geral

O objetivo dessa pesquisa é apresentar passo a passo de que forma é feita a recuperação de arquivos apagados de dispositivos formatados com base no estudo de caso feito com a ferramenta de Perícia Forense Autopsy.

Objetivos Específicos

Pesquisar de que forma é realizado o processo de investigação.

Conceituar ferramentas utilizadas no processo de investigação.

Analisar como é realizado o processo feito pela ferramenta Autopsy

Apresentar resultados obtidos pela ferramenta através de estudo de caso.

Método científico

Para a realização desse projeto foiutilizado o método de estudo de caso por ser o mais viável para esse assunto. Segundo Fachin (2005):

> Este método é caracterizado por ser um estudo intensivo. No método do estudo de caso, leva-se em consideração, principalmente, a compreensão, como um todo, do assunto investigado. Todos os aspectos do caso são investigados. Quando o estudo é intensivo, podem até aparecer relações que, de outra forma, não seriam descobertas. O direcionamento desse método dá-se com a obtenção de uma descrição e compreensão completas das relações dos fatores em cada caso, sem contar o número de casos envolvidos. Conforme o objetivo da investigação, o número de casos pode ser reduzido a um elemento caso ou abranger inúmeros elementos, como grupos, subgrupos, empresas, comunidades, instituições e outros. Algumas vezes, uma análise detalhada desses casos selecionados pode contribuir para a obtenção de ideias sobre possíveis relações. (FACHIN, 2005, p.45)

2 REVISÃO BIBLIOGRÁFICA

2.1 COMPUTAÇÃO FORENSE

Segundo Eleutério e Machado (2011) a Computação Forense é a ciência que usa técnicas especializadas, para coletar, preservar e analisar os dados digitais de um computador ou computadores suspeitos de serem utilizados em um crime virtual, sendo assim apresentados para a justiça através de um laudo pericial. Da mesma forma que a perícia convencional, ela trata de buscar evidências para a solução de um crime.

A Computação Forense é a ciência que, através de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo. (ELEUTÉRIO E MACHADO, 2011, p. 31).

> De acordo com Eleutério e Machado (2011) para a perícia criminal da polícia, a computação forense envolve o trabalho investigativo e todo o trabalho pericial, para desvendar os crimes cometidos através do uso do computador. Ela pode ser empregada tanto para fins legais como exemplo investig (ELEUTERIO; MACHADO, 2011)() ar espionagem industrial, como também para ações disciplinares internas, por exemplo, uso indevido de recursos de uma empresa.

No século 19, surge um dos primeiros pesquisadores, Francis Galton, que elabora um estudo complexo sobre as impressões digitais. Tal estudo serve como base para as investigações que diferenciam um ser humano do outro, baseado em uma característica única que não se repete. O grande problema, é que após algumas décadas, descobriu-se que pelo menos 5% da população mundial não possui digitais, seja por problemas genéticos, seja por suas atividades profissionais que fazem com que as digitais de uma pessoa se desgaste com o tempo, tais como: professores (as), pedreiros, faxineiras (os) e pessoas que manipulam produtos químicos abrasivos.

Já no início do século 20, o cientista Leone Lattes descobre que os tipos sanguíneos podem ser divididos em grupos de acordo com características próprias. E a partir de sua pesquisa surgem os grupos A, B, AB e O. Isso auxilia na ciência forense quando há cenas de crimes envolvendo sangue, o que já permite diminuir a quantidade de suspeitos, puramente a partir de uma análise do tipo sanguíneo. Também no início do século 20, Calvin Goddard desenvolve um estudo sobre a comparação entre projéteis de armas de fogo o que possibilita a detecção da arma que disparou o projétil existente em uma cena onde há a necessidade de uma análise forense. Esse estudo torna-se um marco para a solução de inúmeros casos julgados em um tribunal. No mesmo período, Albert Osborn desenvolve uma

pesquisa sobre as características e metodologias para análise de documentos, o que pode comprovar fraudes, falsificações e veracidade dos mesmos. Outro cientista que nessa mesma época contribui com seus estudos para a área de forense é Hans Gross, que desenvolve o método científico para a realização de investigações criminalísticas.

E em 1932, no FBI, um laboratório foi organizado para prover serviços de análise forense a todos os agentes de campo e outras autoridades legais de todo os EUA.

Todos esses estudos, pesquisas e desenvolvimentos, se devem aos esforços de cientistas que atuavam na área da ciência forense ou não, mas que de alguma forma suas descobertas contribuíram para o avanço no trabalho dos profissionais de gerações posteriores. Tanto que, mesmo após um século dos primeiros estudos, as bases e conceitos desenvolvidos por esses pioneiros continuam atuais e amplamente utilizadas ao longo de um processo de análise. A única diferença são os equipamentos utilizados. No entanto, a maioria dos conceitos e métodos permanecem os mesmos. Isso só começa a mudar com o advento da informática e o crescente nível de importância da informação no contexto da atualidade. Essas mudanças surgem, por conta de um novo paradigma, onde os crimes são realizados de uma outra maneira e as cenas não são mais aquelas tradicionais, com sangue, fios de cabelo e fluidos corporais. E as vítimas não são mais os corpos físicos dos denunciantes, mas suas identidades e vidas virtuais. E ainda podemos acrescentar que o objetivo básico da mesma é a determinação do valor das evidências relacionadas à cena de um crime.

Contudo, com o passar do tempo, os artefatos utilizados em um crime tornaram-se mais sofisticados e um criminoso não precisa mais sair do conforto de seu lar para causar milhões de prejuízos às suas vítimas. Não temos mais sangue envolvidos numa cena de um crime, apenas 0’s e 1’s, ou seja, bits.

2.2 CRIME CIBERNÉTICO

Segundo (FELIPE, 2012, com adaptações).

Um crime cibernético é qualquer ato ilegal envolvendo um computador, seu sistema ou suas aplicações. E para ser considerado um crime, o ato deve ser intencional, e não acidental.

E um crime cibernético possui três diferentes aspectos a serem analisados:

Ferramentas do crime, quais hardwares foram utilizados para cometer o ato

Alvo do crime , a vítima do crime

Tangente do crime , segundo (DORIGÃO, 2015, p. 1). ocorre quando numa

ação existe uma questão prejudicial, onde uma esfera jurídica depende da solução em outra para decidir a ação principal.

E o mesmo deve ser de duas categorias diferentes:
Ataque interno
Ataque externo

2.2.1 Exemplos de crimes cibernéticos

Alguns exemplos de crimes cibernéticos são:

Roubo de propriedade intelectual , também conhecido como plágio, onde o indivíduo, copia o trabalho de outra pessoa e apresenta como sendo seu.

Fraude financeira , qualquer ação, irregularidade, ou infração de natureza financeira.

Distribuição e compartilhamento de pornografia infantil

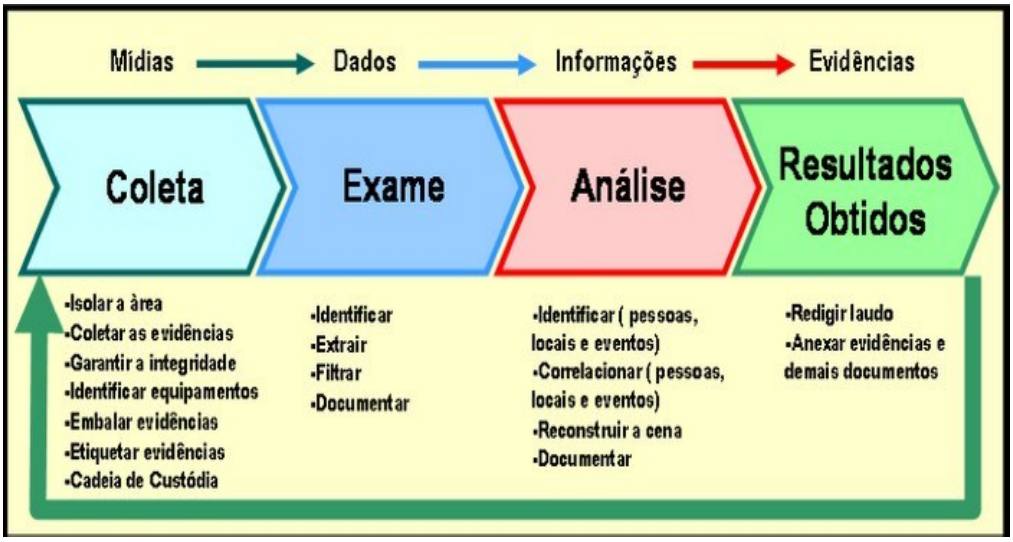
A motivação para esses crimes são as mais variadas, dentre elas podemos destacar;

Testes, ou tentivas de aprender na prática, por script kiddies
Necessidade psicológica
Vingança ou outras razões maliciosas
Desejo de causar problemas para o alvo
Espionagem – corporativa ou governamental

3 INVESTIGAÇÃO

Uma investigação computacional é iniciada através de denúncias anônimas à Polícia Federal ou através de relatórios de redes sociais como o Facebook e Instagram com páginas e perfis que contêm possíveis imagens de conteúdo criminoso encontradas em seus servidores. Redes sociais como o Facebook coletam dados de perfis contendo por exemplo; divulgação de conteúdo de pornografia infantil e disponibiliza essas informações que dispõem quem as publicou, e quais foram as imagens. Essas informações são enviadas a Ong (Nicmec - National Center for Missing & Exploited Children) que repassa as informações para os países de onde as imagens foram enviadas. Após a denúncia, ou o recebimento dessas informações a Polícia Federal emite um mandado de busca e apreensão aos dispositivos identificados pelo número de IP (número que cada dispositivo conectado à internet possui) e uma investigação é iniciada através de etapas chamadas Ciclo de Investigação Computacional Forense (figura 1) que será abordado detalhadamente nesse capítulo. Se caso no final da investigação, for confirmado através de laudo pericial que o suspeito é culpado, o o mesmo será preso em flagrante

Figura 1 - - Ciclo da Investigação Computacional Forense



Fonte: J. Rover (2011)

Após executar a ordem de busca e apreensão, como mencionado anteriormente, é necessário enviar os hardwares confiscados para um laboratório de informática especializado para que seja feita uma análise mais específica.

Ao receber um dispositivo de armazenamento de computação para análise, seja um disco rígido, DVD, unidade flash, cartão de memória ou outra mídia, os

especialistas devem seguir uma série de etapas do Ciclo de Investigação, que serão descritas abaixo em detalhes.

3.1 COLETA

A coleta de material para o início de uma investigação dá-se após denúncias a Polícia Federal, para que essa coleta seja realizada, é necessário que procedimentos de segurança sejam feitos. É imprescindível que a área seja isolada evitando assim que terceiros possam danificar alguma evidência mesmo que não intencionalmente.

Após o isolamento da área é necessário fazer a coleta das evidências, no caso de uma investigação de pornografia infantil, essas evidências podem estar em hardwares como computadores, aparelhos celulares, câmeras fotográficas, pen drives entre outros. Dentro dessa coleta é necessário estabelecer prioridades de acordo com a volatilidade dos dados, sendo que os dados que podem ser perdidos com maior facilidade precisam ser priorizados. Após a priorização por volatilidade, os dados onde as coletas são de menor esforço, devem ser priorizados. Por fim, a coleta deve ser priorizada por valor estimado, o valor das fontes dos dados deve ser estimada.

O próximo passo é preservar a integridade dos dados, para que isso seja feito é necessário gerar provas que os dados estão íntegros (HASH). Esse é o passo mais importante para a admissibilidade das evidências.

Depois de coletar as evidências e garantir que os dados estão seguros e são íntegros, é necessário fazer a identificação dos equipamentos para que não se percam, e embalar as evidências, nesse caso os hardwares, etiquetar cada um deles e fazer uma cadeia de custódia.

Segundo Aury Lopes Junior:

> “A cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico.
> A preservação da cadeia de custódia exige grande cautela por parte dos agentes do estado, da coleta à análise, de modo que se exige o menor número de custódios possível e a menor manipulação do material. O menor número de pessoas manipulando o material faz com que seja menos manipulado e a menor manipulação, conduz a menor exposição. Expor menos é proteção e defesa da credibilidade do material probatório.”

Uma cadeia de custódia deve conter os seguintes itens:

1. Data e hora de coleta da evidência

2. De quem a evidência foi apreendida
3. Informações sobre o hardware, como fabricante, modelo, número de série etc.
4. Nome da pessoa que coletou a evidência
5. Descrição detalhada da evidência.
6. Nome e assinatura das pessoas envolvidas
7. Identificação do caso e da evidência (tags)
8. Assinaturas MD5/SHA1 das evidências.
9. Informações técnicas pertinentes.

3.2 EXAME

O segundo passo para uma investigação consiste no exame dos dados encontrados, no processo de exame as informações são filtradas e avaliadas para que apenas os dados mais importantes e relevantes sejam analisados. Para esse processo são utilizadas ferramentas e recursos específicos como : dump de memória volátil, segundo Marcos Monteiro:

> "Fazer um dump da memória RAM é como "congelar" o estado da memória e salvá-la num arquivo, que nada mais é, que um clone fidedigno da memória RAM, salvando assim todos os dados que estavam alocados na memória no momento do dump.
> Um dump de memória RAM, serve para análise de possíveis malwares alojados na RAM, como também para descobrir o que estava sendo feito naquele dispositivo utilizando os dados voláteis encontrados.
> Todas as informações presentes em memória RAM, por serem voláteis serão perdidas assim que o dispositivo em questão for desligado, e qualquer ação no dispositivo ligado altera o estado da memória, pois estará enviando novos dados a memória, como por exemplo ao executar um programa.
> A volatilidade dá-se pela perda de informação ao ser desligado um dispositivo tecnológico, assim como a capacidade de recuperação ou validação dos dados, diminuindo a veracidade e possivelmente impedindo que tenha algo de valor probatório em juízo" (MONTEIRO, 2018, p. 1).

Também é necessário a recuperação e análise de dados persistentes e um conjunto de assinaturas de softwares e documentos disponibilizado para filtragem de dados.

3.3 ANÁLISE

A análise é feita através da interpretação dos dados coletados, para que seja feita a identificação dos envolvidos nos crimes. Após a identificação, é estabelecida a ordem cronológica dos crimes e um levantamento dos eventos e locais também é feita para que possa ser traçada uma rota de onde essas imagens possam ter sido

espalhadas ou se houve divulgação das mesmas. Um cruzamento de informações também é feito para que levem a provas concretas ou evidências dos crimes cometidos e todas as evidências são documentadas.

3.4 RESULTADOS OBTIDOS

É a fase final dos exames forenses e é composta pela preparação do laudo pelo perito, expondo o resultado e explicitando as evidências digitais descobertas nos materiais avaliados

Após a realização da coleta, exame e análise dos dados e a identificação da violação da lei, um laudo pericial é redigido para documentar tudo o que foi feito. Um laudo pericial precisa conter uma conclusão imparcial, clara e concisa, precisa expor os fatos e todos os métodos utilizados, deve expor todos os métodos utilizados, e deve ser de fácil interpretação.

4 FERRAMENTAS DE INVESTIGAÇÃO

Muitos softwares são utilizados para a diferentes tipos de casos de investigação relacionados à crimes cibernéticos, para crimes de pornografia infantil, uma ferramenta que se mostra muito eficaz é a ferramenta Sistema IPED, que foi idealizada e desenvolvida por um perito da Polícia Federal Brasileira. Outras ferramentas também se mostram muito eficazes em investigações de crimes cibernéticos relacionados a pornografia infantil, dentre elas estão a ferramenta Nu detective que é um software que faz um reconhecimento de assinatura de arquivos digitais e ferramenta Autopsy.

4.1 SISTEMA IPED

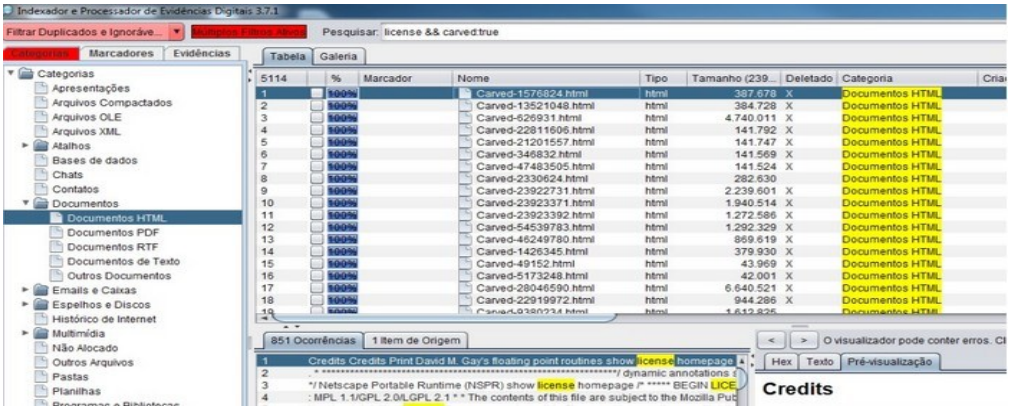
O Sistema IPED (Indexador e Processador de Evidências Digitais) é um software que foi idealizado e desenvolvido por um perito da Polícia Federal Brasileira, é utilizado em algumas perícias da Lava Jato e comparado com outros softwares é considerado excelente nas questões desempenho e velocidade de processamento. Ele é um software desenvolvido em java com foco na velocidade de processamento e exame detalhado. Na interface do software, é possivel identificar quais foram o tipo de arquivos encontrados em categorias (figura 2).

Resumo das principais funcionalidades segundo (TI FORENSE, 2018, p. 1).

> Decodificação de imagens dd, 001, e01 e iso via Sleuthkit 4.2 e Libewf
> Acesso a arquivos apagados e espaço não alocado (via Sleuthkit)
> Categorização por análise de assinatura e propriedades e filtro por categoria (ver seção Categorização)
> Expansão de containers (ver seção Expansão de Containers)
> Indexação (ver seção Indexação) e pesquisa por palavras-chave no conteúdo e propriedades dos arquivos.
> Data Carving eficiente sobre itens não alocados e alocados (ver seção Data Carving)
> Visualização em árvore dos dados (não implementada para relatórios, atualmente)
> Cálculo de hash e filtro de duplicados
> OCR de imagens e PDFs e detecção de imagens contento textos como digitalizações (metadado OcrCharCount)
> Detecção de documentos cifrados
> Consulta a base de hashes (KFF) para alertar ou ignorar arquivos
> Visualização integrada de dezenas de formatos.
> Visualizador de texto filtrado para qualquer formato.
> Galeria multithread para visualizar miniaturas de dezenas de formatos de imagens (via Image/GraphicsMagick)
> Geração de miniaturas de vídeos (contribuição PCF Wladimir)
> Ordenação por propriedades, como nome, tipo, datas e caminho.
> Marcação, exportação e cópia de propriedades dos arquivos

Geração de arquivo CSV com as propriedades de todos os itens
Extração automática de categorias para casos de extração automática de dados
Extração e reindexação de itens selecionados pela interface de pesquisa após análise do perito
Geração de relatório HTML (contribuição PCF Wladimir)

Figura 2 - IPED - Processador de evidencias digitais



Fonte: Polícia Federal (2018)

Existem varios softwares importantes para o processo de investigação forense, porém o sistema IPED possui uma vantagem frente as outras devido ao seu desempenho e alta velocidade de processamento, que é necessária para grandes volumes de dados em mídias de alta capacidade como as que tem sido usadas por peritos brasileiros.

Este software possui uma interface simples, intuitiva e integrada para análises e exames periciais detalhados dos dados armazenados em diferentes mídias, como: computadores, pendrives, cartões de memória, CD's, DVD's, entre outros dispositivos, facilitando assim o trabalho dos peritos no processamento de dados em varios dispositivos diferentes.

Apesar de ser uma ferramenta gratuita, o sistema IPED requer um bom conhecimento computacional para que possa ser utilizada.

4.2 NUDETECTIVE

O Nudetective é uma software de reconhecimento automatizado de assinaturas de arquivos digitais. O software faz uma triagem na memória da máquina periciada em busca de conteúdos que indiquem a presença de material pornográfico infantil – detecção de nudez em arquivos de imagem como mostrado na figura 3.

Figura 3 - Detecção de Nudez

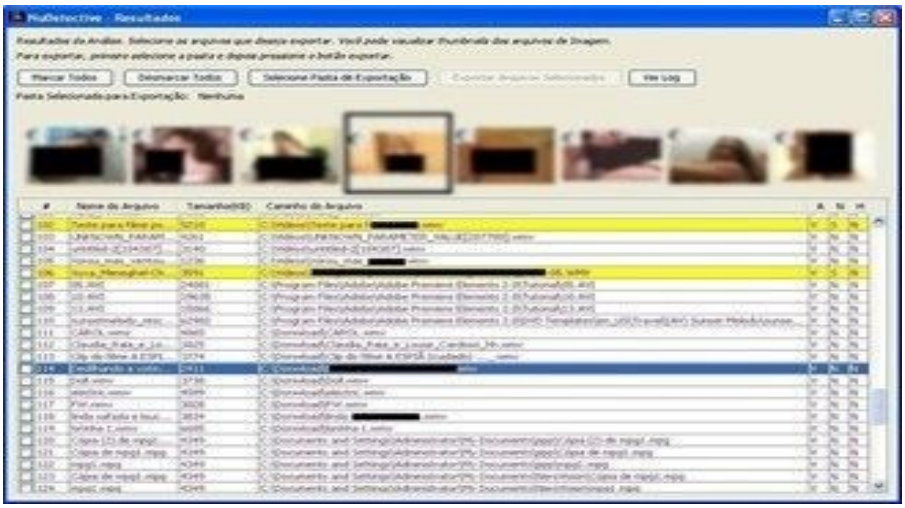
Fonte: Cardozo (2010)

Uma comparação de hashes de arquivos com um banco de dados da Polícia Federal contendo hashes de milhares de arquivos ilegais é feita no dispositivo investigado. Os hashes são comparados com novos arquivos adquiridos em diligências policiais. Uma limitação desse método é que ele detecta apenas arquivos já conhecidos pela PF.

O segundo método de localização é a avaliação de nomes. Por meio de análise de palavras-chave em nomes de arquivos, podemos localizar quais deles contêm conteúdo impróprio. A desvantagem desse método é a geração de falsos positivos, já que muitas vezes os nomes dos arquivos não correspondem ao conteúdo.

O terceiro método, usado pela NuDetective e ferramentas similares, é a detecção de nudez. Ele analisa a foto e procura por áreas com tom de pele humana. A partir daí, o programa faz comparações entre o percentual de pele e o total de bytes do arquivo, entre outras análises como mostrado na figura 4.

Figura 4 - Resultados



Fonte: Payão (2017)

A ferramenta apesar de muito eficaz e gratuita só está disponível para autoridades e instituições públicas.

4.3 AUTOPSY

O Autopsy é uma ferramenta utilizada para análise de mídias que detalha desde a criação até a exclusão dos arquivos, podendo recuperar informações em diversas mídias como por exemplo: pen drives, cartões de memória, dvds e etc.

Para exemplo acadêmico será utilizado uma mídia de 1gb, pois quanto maior o tamanho da unidade a ser examinada maior será o tempo de processamento da ferramenta. Abaixo uma breve descrição de algumas das funcionalidades da ferramenta:

- Colaborar com outros examinadores em casos maiores
- Análise da linha do tempo; exibição de eventos do sistema para a identificação de atividade.
- Pesquisa por palavra chave; permite encontrar arquivos que mencionam expressões específicas.
- Artefatos da WEB; extrai atividade da web de navegadores para identificar a atividade do usuário.
- EXIF: Extrai informações de localização geográfica e câmera de arquivos

JPEG.

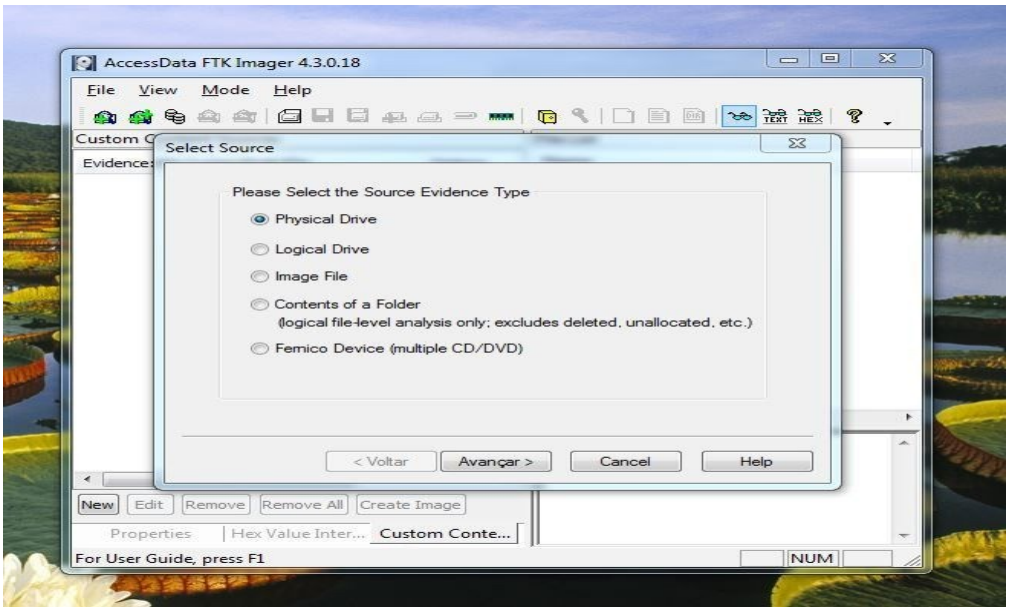
- Reprodução de Mídia; visualização de imagens e vídeos sem a necessidade de sair da ferramenta.
- Exibe miniaturas de imagens para a identificação de conteúdo com maior facilidade.
- Suporte Android; extrai dados de sms, registros de chamadas, contatos e etc.
- Análise de imagens de disco, unidades locais ou pastas específicas.

5 RECUPERAÇÃO DE ARQUIVOS UTILIZANDO A FERRAMENTA AUTOPSY

Para a viabilização desse projeto, foram utilizadas duas ferramentas a ferramenta Autospy já apresentada no capítulo anterior, e a ferramenta FTK Imager versão 4.3.0 como ferramenta de apoio, para a criação da imagem do disco do dispositivo utilizado.

O primeiro passo foi baixar a ferramenta FTK Imager, disponível no site https://accessdata.com. Através de um cadastro rápido na plataforma, um link é enviado ao email cadastrado e a ferramenta pode ser baixada sem nenhuma complicação. Após o download da ferramenta, a imagem do disco pode ser criada clicando em File e depois em Create disk Image (figura 5).

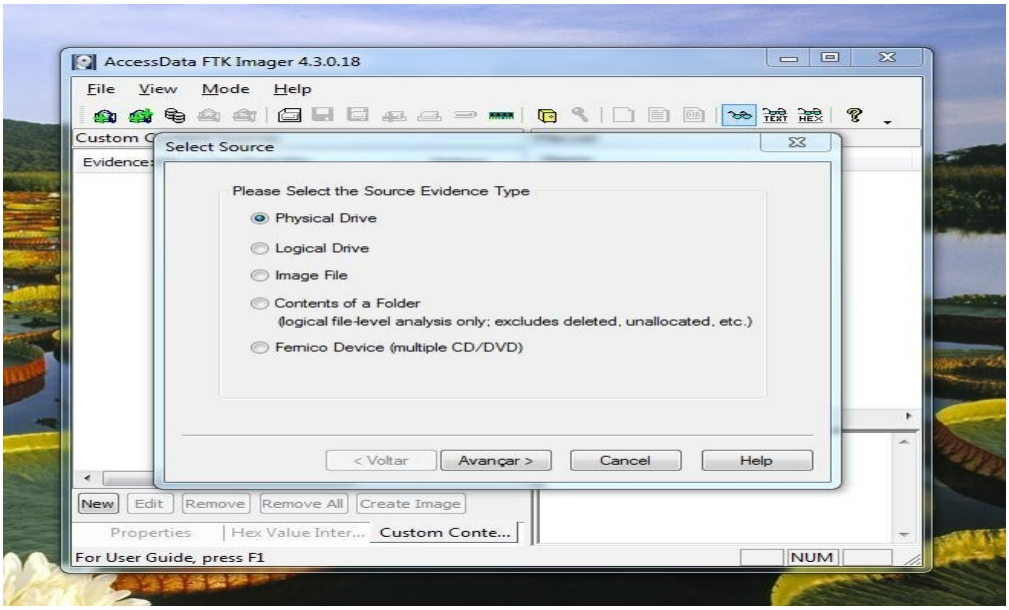
Figura 5 - FTK - Criação de Imagem



Fonte: O autor (2020)

É necessário escolher qual será a fonte de onde o disco virá dentre as opções temos Drive físico, lógico, imagens, conteúdo de uma pasta, entre outros como mostrado na figura 6. Para o experimento será utilizado Drive Físico.

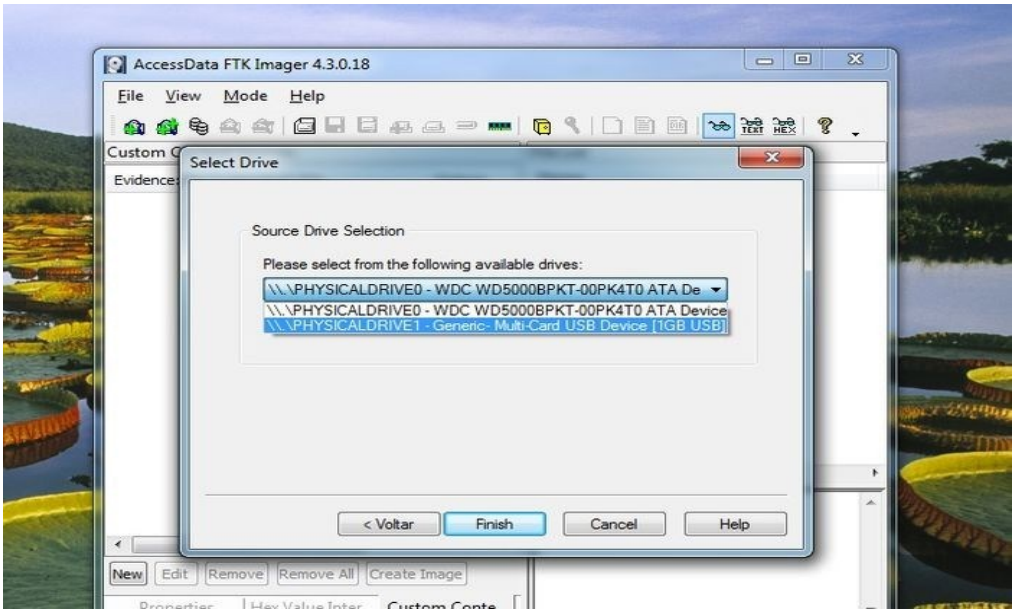
Figura 6 - FTK - Tipo de drive



Fonte: O autor (2020)

O dispositivo utilizado será um cartão de memória de 1gb que foi previamente formatado (Figura 8). É necessário selecionar o drive (Figura 7) e clicar em finish para dar início a criação da imagem de disco.

Figura 7 - Seleção de Drive



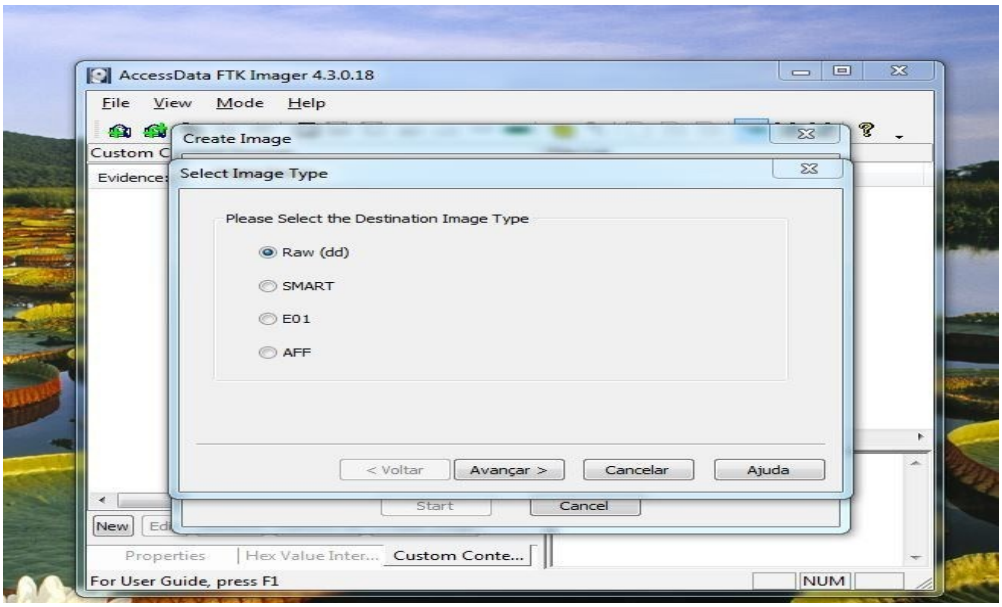
Fonte: O autor (2020)

Figura 8 - Dispositivo Formatado

Fonte: O autor (2020)

Após escolher qual o tipo de drive será utilizado é necessario escolher o tipo de arquivo será gerado nessa imagem. Foi utilizado o tipo Raw (dd) (figura 9) que é o tipo de arquivo mais apropriado para ser lido pelo software Autopsy.

Figura 9 - Tipo de Imagem

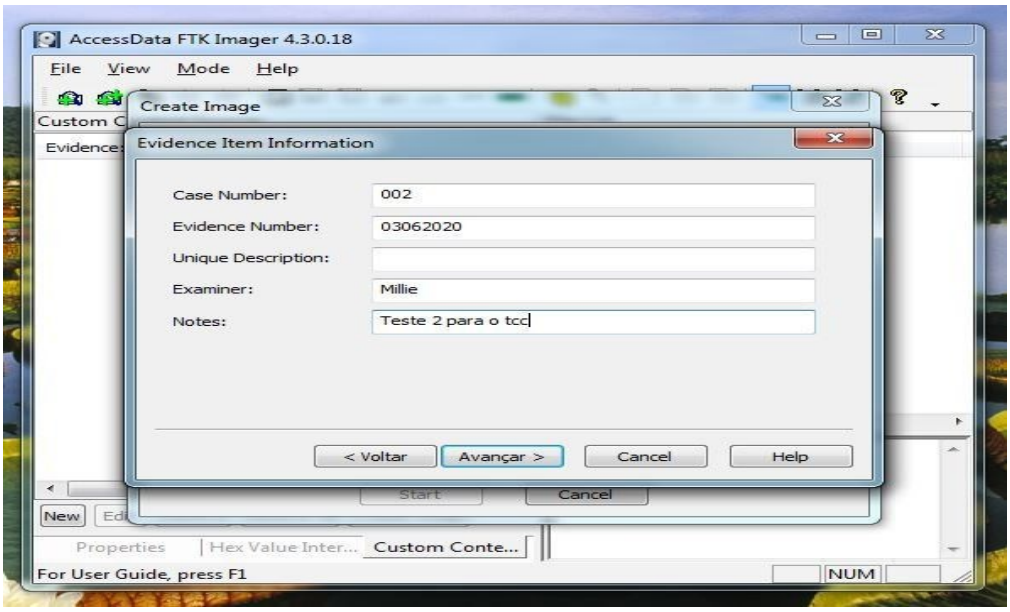


Fonte: O autor (2020)

O próximo passo é colocar as informações como o número do caso, número

da evidência, o nome do examinador (figura 10), acrescentar notas se houver alguma. E escolher a pasta onde essa imagem do disco será salva.

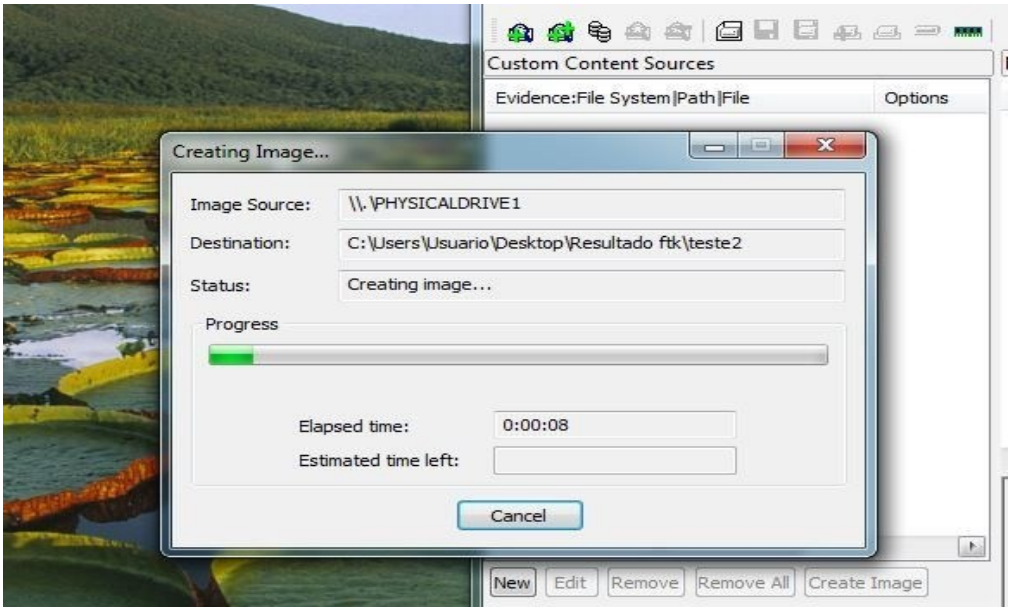
Figura 10 - Informações da evidência



Fonte: O autor (2020)

Após alguns minutos de espera a imagem do disco é criada (figura 11). Como foi dito anteriormente, quanto maior o volume do disco, maior o tempo de processamento da ferramenta no caso do disco utilizado em poucos minutos a imagem foi criada.

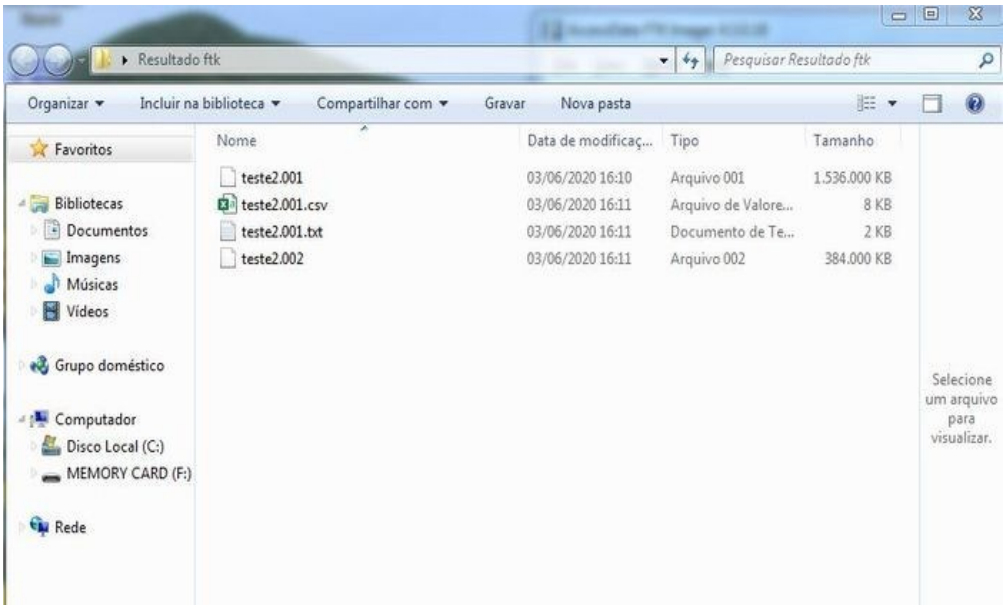
Figura 11 - Criação da Imagem



Fonte: O autor (2020)

Assim como uma pasta com todas as informações e duas imagens do disco (figura 12).

Figura 12 - Pasta com Imagem e informações

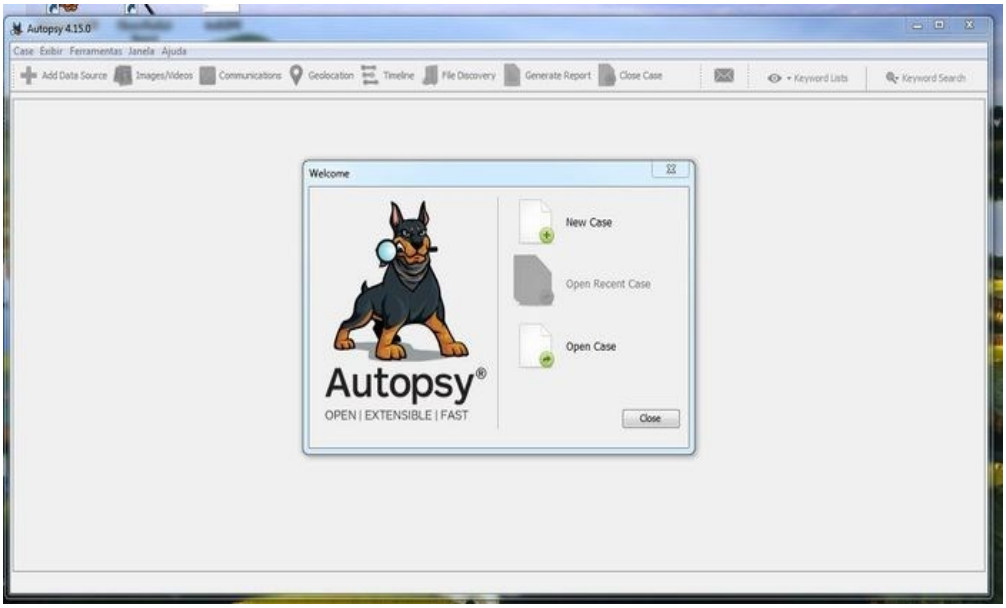


Fonte: O autor (2020)

Uma vez que a imagem foi criada, o próximo passo será o processo de recuperação na ferramenta Autopsy. Onde será iniciado um New Case (Novo Caso)

para iniciar a análise e recuperação como mostra a imagem (figura 13).

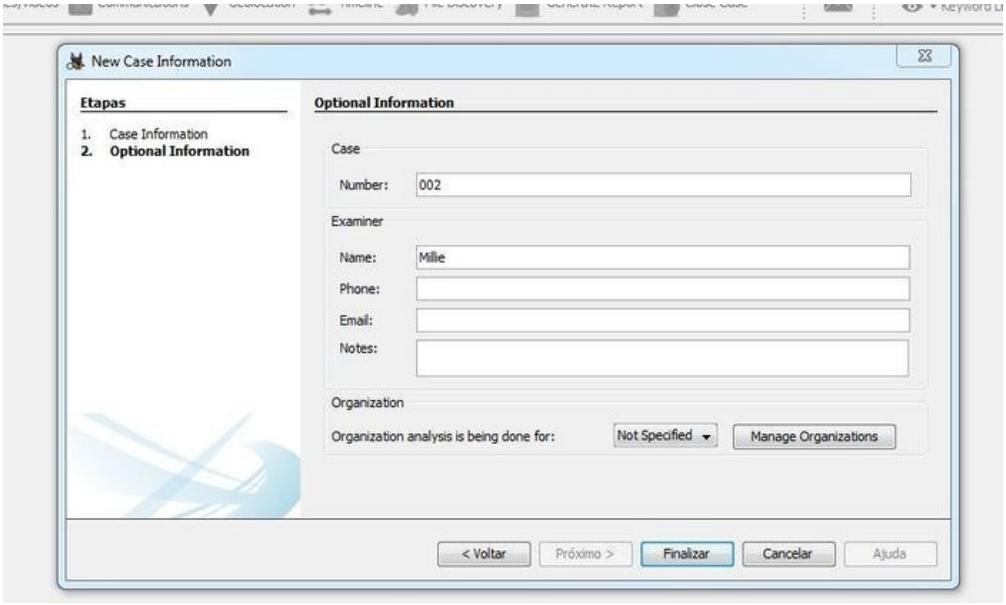
Figura 13 - Autopsy - Novo Caso



Fonte: O autor (2020)

Nesse passo são inseridas as informações do caso (figura 14), assim como no FTK Imager, as informações são opcionais, porém é o que ajuda na identificação das evidências e no controle dos examinadores que terão acesso a esse caso.

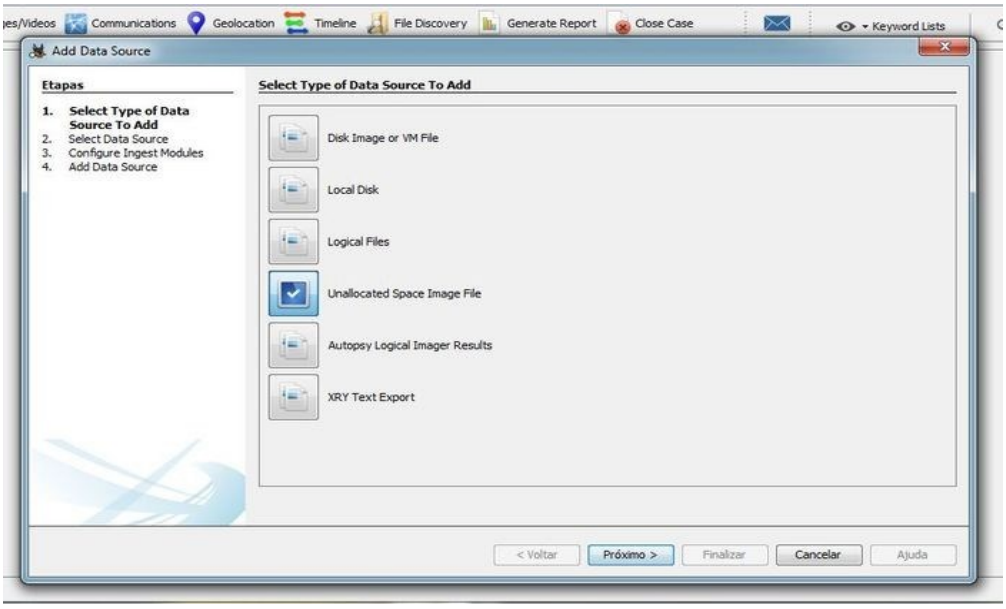
Figura 14 - Autopsy- informações do caso



Fonte: O autor (2020)

O próximo passo consiste em escolher a fonte do dispositivo que será analisado (figura 15), neste experimento será usado a opção espaço de imagem não alocado que será a imagem que foi criada anteriormente no software FTK Imager.

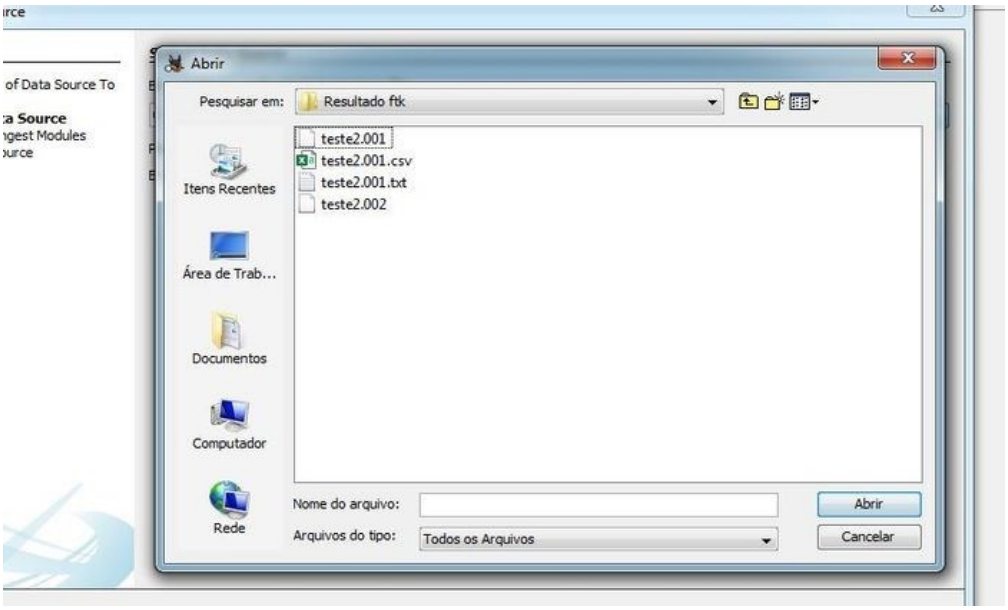
Figura 15 - Espaço de Imagem não alocado



Fonte: O autor (2020)

Agora carrega-se a imagem previamente criada para dar início à analise das evidências, como mostrado na figura 16 a imagem criada está nomeada como teste2.001.

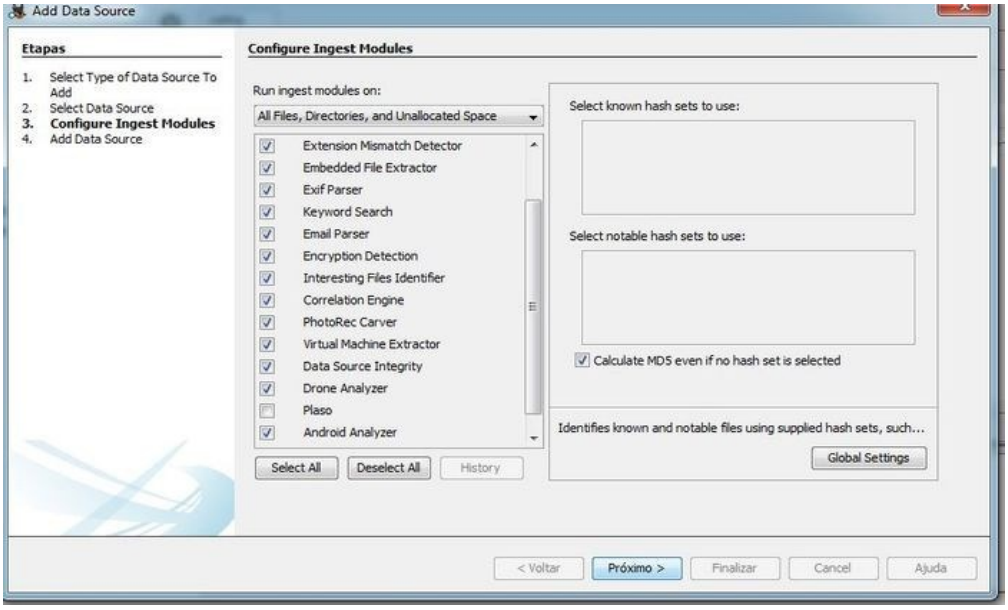
Figura 16 - Inserindo imagem de disco



Fonte: O autor (2020)

É possível escoher quais serão os tipos de arquivos que serão analisados especificamente como mostrado na figura 17.

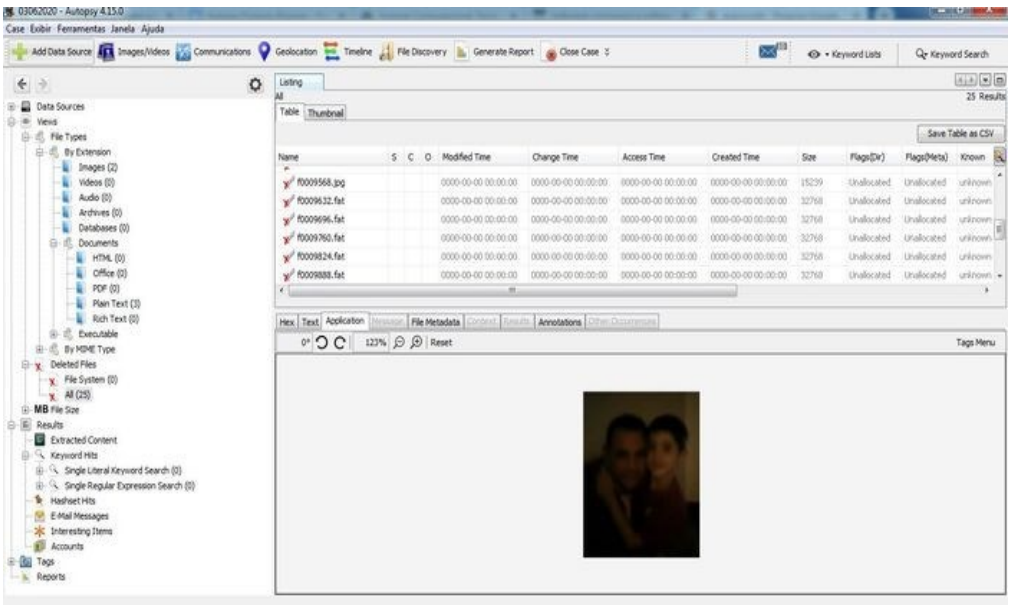
Figura 17 - Análise de Imagem de disco



Fonte: O autor (2020)

É possível notar na figura 18 que o software resgatou 25 arquivos deletados dentre eles fotos na extensão .JPEG mostradas a seguir;

Figura 18 - Analisando Resultado

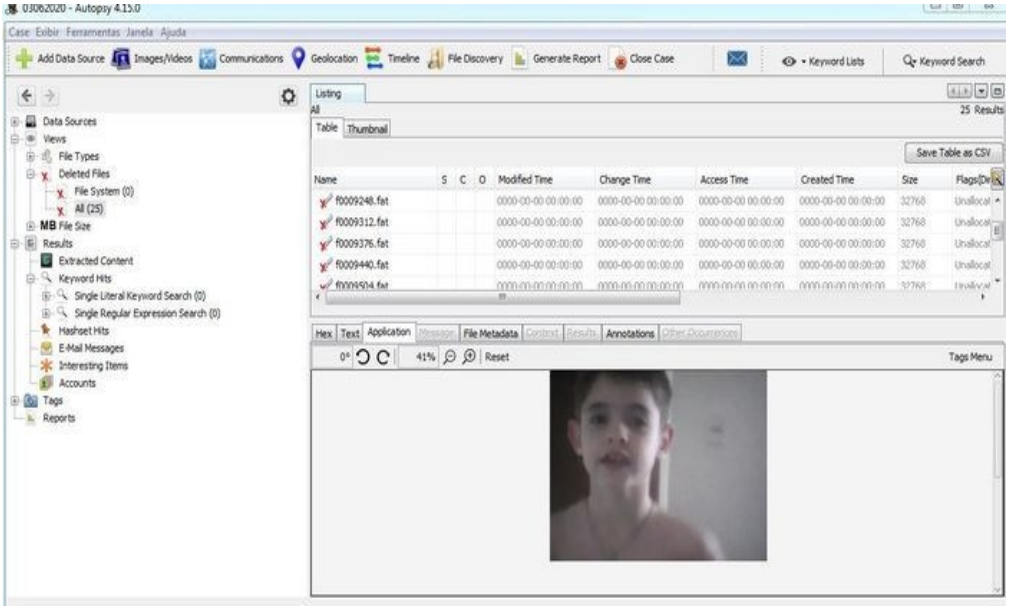


Fonte: O autor (2020)

Como mostra a figura 19 ao clicar no link do arquivo .JPEG é possível

visualizar a imagem e inclusive utilizar o recurso zoom para identificar maiores detalhes.

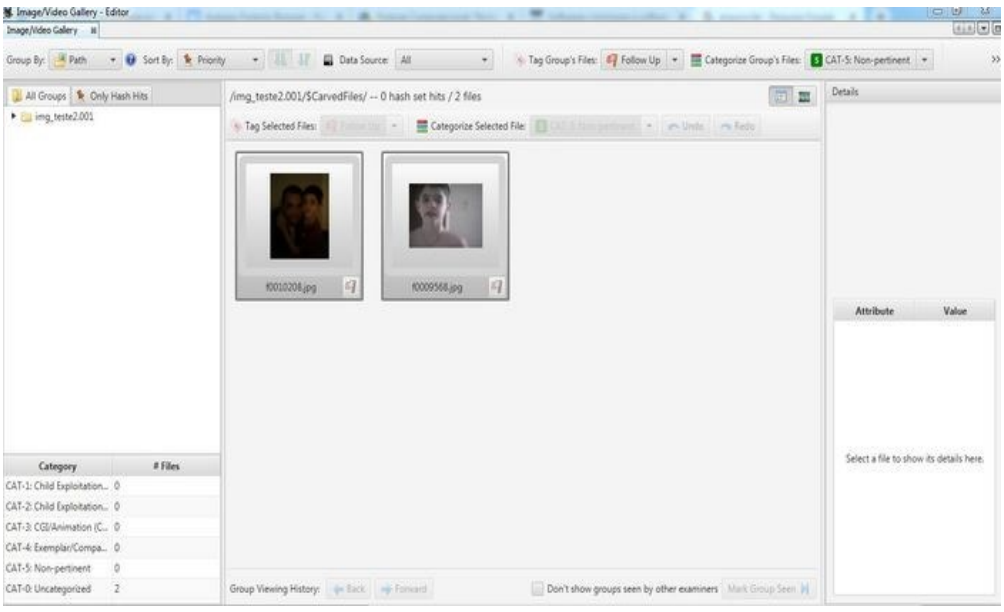
Figura 19 - Resultado 2



Fonte: O autor (2020)

Clicando em galeria, são mostradas todas as imagens e videos recuperados e que não foram corrompidos como é possível identificar na figura 20.

Figura 20 - Resultado 3



Fonte: O autor (2020)

6 CONCLUSÃO

O objetivo desse estudo foi estruturar passo a passo como é realizada uma investigação computacional detalhadamente afim de trazer um entendimento maior do trabalho realizado pela Perícia Forense Computacional, que não é muito divulgado. Com o crescimento exponencial da quantidade de usuários na internet, faz-se necessario um entendimento maior sobre essa área em expansão, para que mais pessoas possam conhecer e eventualmente ingressar na área.

Com base nos dados coletados na pesquisa, é possível apontar que mesmo as ferramentas mais simples, como é o caso da ferramenta Autopsy, é possível obter resultados muito satisfatórios. A recuperação de arquivos feita em dispositivos, pode ajudar na identificação de criminosos como pedófilos e pessoas que fazem distribuição de imagens de pornografia infantil na internet.

Nesse processo de tentativa de recuperação de arquivos apagados houve uma dificuldade em encontrar uma ferramenta que fosse liberada para fins pessoais e de estudo, as melhores ferramentas em termos de processamento e acurácia que foram descritas nesse projeto, são de dificil manipulação ou são disponibilizadas apenas para autoridades e instituições publicas.

Como por exemplo a ferramenta Nudetective, que mesmo sendo a melhor e mais rápida ferramenta para a identificação de pornografia infantil, não está disponível para download, restringindo o seu uso apenas para autoridades. E não existem muitos estudos que possam ajudar na manipulação das ferramentas mais complexas como por exemplo a ferramenta Sistema IPED onde houve uma dificuldade maior em encontrar tutoriais para a manipulação da mesma, apesar de ser uma ferramenta gratuita muito completa e com o processamento mais rápido do que as outras, requer comandos específicos e um conhecimento maior.

Por fim, mesmo com todos os obstáculos, foram obtidos resultados satisfatórios utilizando a ferramenta Autopsy em conjunto com a ferramenta FTK Imager e foi possível demonstrar alguns aspectos principais do processo de investigação forense digital, o que foi muito esclarecedor e ajudou a entender melhor sobre a área de Perícia Forense e seus processos.

REFERÊNCIAS

CARDOZO, André. **Polícia Federal usa detecção de nudez no combate à pedofilia**. **ICCyber**. São Paulo, 2010. Disponível em: https://tecnologia.ig.com.br/noticia/2010/09/17/iccyber+2010+policia+federal+usa+deteccao+de+nudez+no+combate+a+pedofilia+9593758.html. Acesso em: 12 Mai. 2017.

DORIGÃO, Niara Silva . **Tangente no direito processual civil, trabalhista e penal**. **Jurisway**. Porto Velho, 2015. Disponível em: https://www.jurisway.org.br/v2/dhall.asp?id_dh=14358#:~:text=Texto%20enviado%20ao%20JurisWay%20em%2020%2F01%2F2015.&text=Tangente%20%C3%A9%20aquela%20%E2%80%9CQue%20toca,expressa%20no%20dicion%C3%A1rio%20online%20Priberam.. Acesso em: 14 Jun. 2020.

ELEUTERIO, Marcio Pereira; MACHADO, Pedro da Silva . **Desvendando a computação forense**. São Paulo: Novatec, v. 1, 2011.

FACHIN, Odila. **Fundamentos de Metodologia**. 5. ed. São Paulo: Saraiva, 2006.

FELIPE, Nilton. **O que é Forense Computacional**. **Diário de Nilton Felipe**. São Paulo, 2012. Disponível em: https://niltonfelipe.wordpress.com/2012/08/28/o-que-e-forense/. Acesso em: 6 Jun. 2019.

J. ROVER, Aires. **Forense Computacional**: Processo de Investigação. **Forense Computacional**. Santa Catarina, 2011. Disponível em: https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao. Acesso em: 11 Fev. 2020.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de Pesquisa**: Planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretaçãode dados. 7. ed. São Paulo: Atlas, 2008.

MONTEIRO, Marcos. **Computação Forense**: Forense na memória RAM. **Marcos Monteiro**. Ceará, 2018. Disponível em: https://www.marcosmonteiro.com.br/index.php/dicas/dicas/728-forense-na-memoria-ram. Acesso em: 29 Mai. 2020.

PAYÃO, Felipe. **Polícia Federal cria programa que busca pornografia infantil em smartphones**. **Tec Mundo**. São Paulo, 2017. Disponível em: https://www.tecmundo.com.br/seguranca/124311-policia-federal-cria-programa-busca-pornografia-infantil-smartphones.htm. Acesso em: 12 Set. 2018.

POLÍCIA FEDERAL. **Indexador e processador de evidências digitais**: Manual IPED. **Departamento de Polícia Federal**. 2018. 11 p. Disponível em: https://servicos.dpf.gov.br/ferramentas/IPED/3.14.5/IPED-Manual_pt-BR.pdf. Acesso em: 3 Jun. 2020.

TI FORENSE. **AUTOPSY**. **TI FORENSE**. 2018. 1 p. Disponível em: . Acesso em: 29 Mai. 2020.

TI FORENSE. **IPED**: Indexador e processador de evidencias digitais . **TI FORENSE**. São Paulo, 2018. 1 p. Disponível em: https://www.tiforense.com.br/iped-indexador-e-processador-de-evidencias-digitais-dpf/. Acesso em: 29 Mai. 2020.