PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA DA PUC GOIÁS
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

ESTUDO SOBRE COMPUTAÇÃO FORENSE COM O USO DE FERRAMENTAS LINUX

GUSTAVO GOMES CARDOZO DOS SANTOS

GOIÂNIA
2022

GUSTAVO GOMES CARDOZO DOS SANTOS

ESTUDO SOBRE COMPUTAÇÃO FORENSE COM O USO DE FERRAMENTAS LINUX

Trabalho de Conclusão de Curso apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Me. Claudio Martins Garcia

GOIÂNIA
2022

GUSTAVO GOMES CARDOZO DOS SANTOS

ESTUDO SOBRE COMPUTAÇÃO FORENSE COM O USO DE FERRAMENTAS LINUX

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenhariade Computação, em_____/_____/_____.

_____

Prof. Ma. Ludmilla Reis Pinheiros dos Santos
Coordenador de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientador: Prof. Me. Claudio Martins Garcia
Pontifícia Universidade Católica de Goiás

_____

Prof. Dr Nilson Cardoso Amaral
Pontifícia Universidade Católica de Goiás

_____

Prof. Dr Gustavo Siqueira Vinhal
Pontifícia Universidade Católica de Goiás

GOIÂNIA
2022

AGRADECIMENTOS

Dedico o trabalho a minha mãe e a meu pai e todos os amigos e professores que estive presente em minha jornada .

RESUMO

O trabalho a ser apresentado mostra o passo a passo de como um perito forense se porta durante uma investigação, e quais são as ferramentas utilizadas para obter evidências suficientes para compor um laudo pericial, além de descrever as leis que permitem que esse perito realize essa prática e quais áreas do *hardware* e sistema, geralmente são mais utilizadas durante a obtenção de evidências. Tambem, foi demonstrado um caso no qual as ferramentas de forense são aplicadas de forma coordenada e seguindo um padrão logico para que o fluxo de obtenção de evidencias e analise das mesmas entrega-se um conjunto final de provas que pudessem compor um laudo pericial.

Palavras-Chave: Forense. Ferramentas. Evidências.

ABSTRACT

The work to be presented shows step by step how a forensic expert behaves during an investigation, and what are the tools used to obtain enough evidence to compose an expert report, in addition to describing the laws that allow this expert to carry out this practice. and which areas of the hardware and system are most used during evidence gathering. Also, a case was demonstrated in which the forensic tools are applied in a coordinated way and following a logical pattern so that the flow of obtaining evidence and analyzing it delivers a final set of evidence that could compose an expert report.

Keywords: Forensics. Tools. Evidence.

LISTA DE FIGURAS

LISTA DE SIGLAS

AMD	–	Advanced Micro Devices
ANAPD	–	Autoridade Nacional de Proteção de Dados
ARPANET	–	Advanced Research Projects Agency Network
CD	–	Compact Disc
CISC	–	Complex Instruction Set Computer
CPU	–	Central Processing Unit
DRAM	–	Dynamic Random Acess Memory
DVD	–	Digital Versatile Disc
EXT4	–	Fourth Extended File System
FAT	–	File Allocation Table
FNC	–	Federal Networking Council
HD	–	Disco Rígido
HD	–	Hard Disk
Kb	–	KiloByte
Lgpd	–	Lei Geral de Proteção de Dados
MS-DOS	–	Microsoft Disk Operating System
NTFS	–	New Technology File System
RAM	–	Random Access Memory
RISC	–	Reduced Instruction Set Computer
SO	–	Sistema Operacional
SRAM	–	Static Random Acess Memory
SSD	–	Unidade de Estado Sólido
TB	–	TeraByte
TCP/IP	–	Protocolo de Controle de Transmissão/Protocolo de Internet
ULA	–	Unidade Lógica Aritmética
VM	–	Máquina Virtual

SUMÁRIO

1 INTRODUÇÃO

No início dos anos 80, iniciou-se um esforço por parte das grandes empresas de tecnologia para tornar os computadores pessoais mais acessíveis para o público consumidor, e como consequência desse aumento na quantidade de usuários, surgiram novas modalidades de crimes computacionais, os quais foram denominados "*cracking*", que ocorre quando alguém realiza a quebra de um sistema de segurança de forma ilegal (DELLA VECCHIA, 2019).

O profissional que atua com Computação Forense e Perícia Digital é encarregado de investigar, recuperar e analisar informações que podem estar em dispositivos mobile, computadores, servidores ou ativos de rede. Ele deverá procurar por evidências de vazamento de dados ou invasões que possam ter ocorrido no ambiente ao qual o crime ocorreu (DELLA VECCHIA, 2019).

A Lei Geral de Proteção de Dados Pessoais (LGPD, 2018), em seu Art. 5º, estabelece que o tratamento de dados deve ser organizado em: Dado Pessoal, Dado Pessoal Sensível, Banco de Dados, Titular, Controlador, Operador, Encarregado, Agentes de tratamento, Tratamento, Anonimização, Consentimento, Bloqueio, Eliminação, Transferência Internacional de Dados, Uso Compartilhado de Dados, Relatório de Impacto à Proteção de Dados Pessoais, Órgão de Pesquisa e Autoridade Nacional. O objetivo é estabelecer regras para empresas e organizações sobre coleta, uso, armazenamento e compartilhamento de dados pessoais, impondo multas e sanções no caso de descumprimento.

Basicamente, a área relacionada à segurança da informação já possuía normas, requisitos e boas práticas para manter um ambiente de proteção por meio da confidencialidade, integridade e disponibilidade, sendo esse conjunto anterior à própria Lei Geral de Proteção de Dados Pessoais (LGPD, 2018). Porém, agora a LGPD fornece um conjunto de regras que devem ser seguidas pelas empresas,e seu descumprimento pode gerar multas ou até mesmo a suspensão de suas atividades.

Segundo levantamento de dados realizado pela Autoridade Nacional de Proteção de Dados (ANAPD, 2020) durante o período da pandemia, os crimes cibernéticos tiveram um aumento de 300%, sendo que no primeiro semestre de 2020 a maioria desses ataques era voltada a órgãos públicos, e a partir do segundo semestre, os cibecriminosos voltaram seus esforços para os cidadãos, com o intuito de obter dados pessoais para a realização de fraude.

Tendo como base os dados apresentados no parágrafo anterior, pode-se deduzir que surgiu a necessidade de analisar e descobrir quem são esses cibercriminosos, sendo esse o principal objetivo deste trabalho de pesquisa, onde serão aplicadas técnicas de investigação forense dentro de um ambiente de testes, para obter dados suficientes para compor um laudo pericial (ANAPD, 2020).

Diante desse contexto, esta pesquisa pretende responder a seguinte questão: **Como identificar falhas e obter os dados necessários para elaborar o laudo de um crime cibernético?**

1.1 Objetivo Geral

Realizar um estudo e teste de ferramentas de forense digital, utilizando técnicas de perícia para compor um laudo pericial.

1.2 Objetivo Específico

- Entender como funciona o processo de perícia digital;
- Exibir os procedimentos e etapas realizados em uma perícia;
- Apresentar a legislação que vigora diante crimes cibernéticos;
- Demonstrar os tipos de peritos existentes;
- Apresentar os conceitos e as diferenças dos atuais sistemas de arquivos (NTFS, FAT e EXT4);
- Expor os conceitos e as diferenças entre a perícia em equipamento desligado e equipamento ligado;
- Descrever os métodos de recuperação de dados;
- Realizar um estudo de caso localizando um arquivo nos dois dos principais sistemas de arquivos atuais (NTFS e EXT4) e, consequentemente, demonstrando sua estrutura de organização.

2 PROCEDIMENTOS METODOLÓGICOS

Este trabalho é um resumo de assunto, no qual, conforme Wazlawick (2014, p. 21), busca “[...] apenas sistematizar uma área de conhecimento, usualmente indicando sua evolução histórica e estado da arte”.

Quanto aos objetivos, esta é uma pesquisa exploratória, pois foram utilizados ferramentas e métodos para levantamento e análise de dados (WAZLAWICK, 2014). Ela se caracteriza por uma pesquisa exploratória pois busca “examinar um conjunto de fenômenos, buscando anomalias que não sejam ainda conhecidas e que possam ser, então a base para uma pesquisa mais elaborada” (WAZLAWICK, 2014, p. 22). Os dados obtidos passaram por uma perícia para identificar possíveis falhas e indícios de crimes que constituíram um laudo pericial (VECCHIA, 2019).

Quanto aos procedimentos e técnicas utilizadas, a pesquisa é bibliográfica e experimental. De acordo com Gil (2017, p. 34):

> A pesquisa bibliográfica é elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui material impresso, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos. Todavia, em virtude da disseminação de novos formatos de informação, estas pesquisas passaram a incluir outros tipos de fontes, como discos, fitas magnéticas, CDs, bem como o material disponibilizado pela Internet.

Durante a elaboração do trabalho, foi realizada uma pesquisa bibliográfica relacionada a área de forense digital e arquitetura de computadores, realizando uma análise teórica de ferramentas e procedimentos relacionados a crimes cibernéticos. Wazlawick (2014) sugere que a pesquisa bibliográfica deve seguir os seguintes passos:

a) Realizar uma listagem dos periódicos e eventos relevantes ao tema da pesquisa, verificando se existe algum artigo na área do tema a ser pesquisado;
b) Organizar uma lista de todos os artigos relacionados à área da pesquisa e que foram publicados nos últimos cinco anos;
c) Realizar a leitura de artigos relacionados ao tema de pesquisa;
d) De acordo com o material já pesquisado, o aluno pode decidir se quer ou não elaborar sua pesquisa.

De acordo com Wazlawic*k* (2014), a pesquisa experimental geralmente partilha de aspectos da realidade do pesquisador. Neste trabalho, por exemplo, as evidências que serão coletadas viram de um HD, que é um produto eletrônico comum na maioria dos computadores.

De acordo com Gil (2017, p. 34), a pesquisa experimental consiste em realizar o estudo de um objeto e utilizar variáveis para realizar a sua manipulação, obtendo os resultados por meio da observação. De acordo com Gil (2017), para realizar uma pesquisa experimental é necessário seguir os seguintes passos:

a) Formulação do problema: **Como identificar falhas e obter os dados necessários para elaborar o laudo de um crime cibernético?**
b) Definição do plano experimental: foi descrito quais são os componentes e ferramentas que foram utilizados para realizar a cópia e obtenção dos dados de um HD;
c) Determinação do ambiente: O ambiente foi composto por uma máquina rondando a distribuição Linux Caine e um HD com as informações que foram coletadas.

- Configuração da máquina de teste:
  I. Computador HP com processador Intel Xeon e5-2650v2 de 2.6GHz, placa mãe Kllisre, Placa de vídeo Nvidea Gt 710 2gb e 16b de Memória de Acesso Randômico (RAM);
  II. Cabo de transferência de dados tipo SATA;
  III. HD de 500gb.

d) Coleta de Dados: a coleta dos dados foi realizada por meio da cópia do HD e geração de uma imagem com a ferramenta Guymager, que já vem instalada na distribuição Linux Caine;
e) Análise e interpretação dos dados: a análise foi realizada com a ferramenta Autópsia, que é uma plataforma forense de código aberto, rápida, fácil de usar e capaz de analisar diversos tipos de mídias.

3 REFERENCIAL TEÓRICO

3.1 Internet

A internet é um meio de comunicação eletrônica. Inicialmente, elar era restrita a ser utilizada por militares na “Guerra Fria”, que foi um cenário onde as duas maiores potências da época, Estados Unidos da América (EUA) e União das Repúblicas Socialistas Soviéticas (URSS), brigavam para ver quem era a maior potência tecnológica e armamentista mundial, gerando um cenário de polarização de poderes. Nesse período, qualquer meio de inovação era motivo de impor superioridade diante de seu país inimigo (DEMENTSHUK; HENRIQUES, 2019).

E assim, diante de um eminente ataque Soviético, o exército dos Estados Unidos da América (EUA) ficou preocupado quanto a segurança de seus dados, que eram guardados apenas localmente, o que os tornavam vulneráveis, uma vez que se os dados fossem perdidos em um ataque, não poderiam ser recuperados (DEMENTSHUK; HENRIQUES, 2019).

Diante disso, foi criada na *Advanced Research Projects* Agency (ARPA) a *Advanced Research Projects Agency Network* (ARPANET), com o intuito de interligar as bases militares americanas, de forma que seus dados fossem compartilhados, solucionando o problema de perda de dados mediante a um ataque Soviético. Porém, esse ataque nunca aconteceu e o Departamento de Defesa dos Estados Unidos mal sabia que havia criado uma das maiores redes de comunicação do século 20 (KLEINROCK; CERF; KAHN, 2003).

Com a evolução das tecnologias de transmissão de dados, a ARPANET se tornou obsoleta em 1990 e foi fechada. No entanto, a internet já estava sendo utilizada desde 1983 e utilizava novos protocolos de rede, como o Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP), e em 24 de outubro de 1995, a *Federal Networking Council* (FNC) aprovou por unanimidade o nome Internet como a sucessora da ARPANET (KLEINROCK; CERF; KAHN, 2003).

3.2 *Hardware*

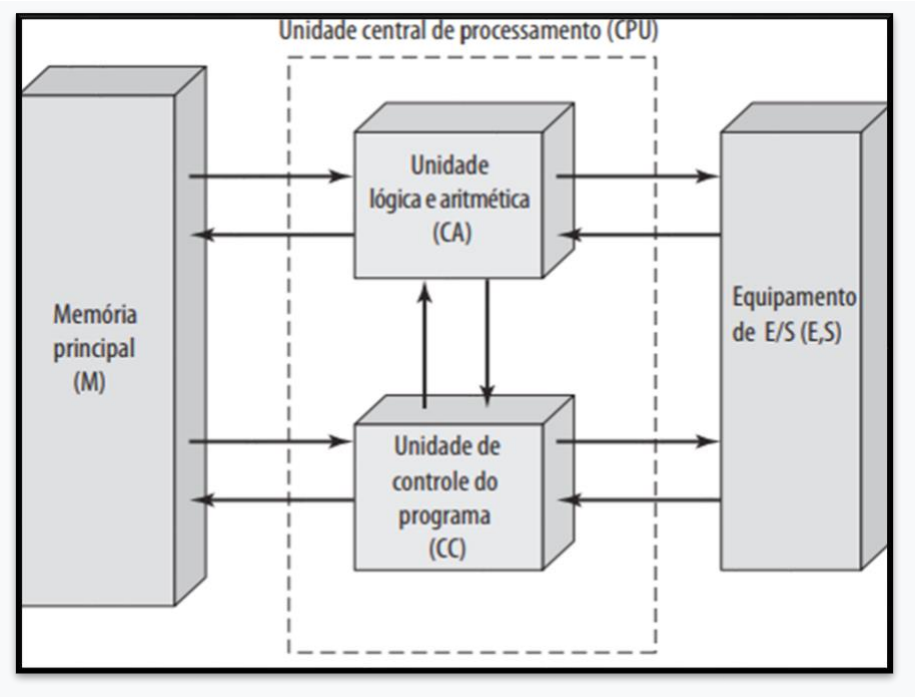
No início da computação, em meados de 1940, havia apenas dois níveis e linguagem de programação: a linguagem de máquina, que era programada a nível de

lógica digital, onde cada instrução era efetivamente executada. Nesse sentido, o *hardware* a executava de forma direta sem a utilização de compiladores ou interpretadores (BRASIL, 2021).

Em 1951, surgiu a ideia de projetar um novo tipo de *hardware* onde se usava uma arquitetura mais simples e na qual suas instruções poderiam ser primeiramente interpretadas antes que o *hardware* as executasse. Nesse modelo de *hardware*, apenas um pequeno conjunto de instruções armazenadas era executado por vez, o que exigia uma menor quantidade de circuitos, diminuindo a complexidade da arquitetura (BRASIL, 2021).

Dentre esse cenário de evolução do *hardware*, um matemático húngaro chamado John von Neumann desenvolveu uma arquitetura que possibilitava o armazenamento de seus programas no mesmo espaço físico que os dados, permitindo a manipulação desses programas. Para que essa arquitetura funcionasse, era necessário que o *hardware* fosse composto por: uma Unidade Lógica Aritmética (ULA), onde todas as operações matemáticas seriam executadas; uma controladora, que organizaria os dados em uma sequenciação apropriada para a execução das operações, sendo que qualquer dispositivo que precisasse realizar a execução de sequências extensas ou cálculos matemáticos necessitava de uma maior quantidade de memória. Esses dados seriam transferidos por barramentos, sendo eles divididos em: barramento de dados, que é bidirecional, ou seja, faz a entrada e saída de dados; barramento de controle, que realiza o agrupamento de sinais elétricos, que são comandos para leitura ou escrita; e barramento de endereços; que agrupa todos os endereços da memória facilitando seu acesso a figura 1 mostra a unidade logica aritimetica (ULA) (STALINGS, 2015).

Figura 1 - Unidade central de processamento



Fonte: Stallings, 2015.

3.2.1 Processador

Com a criação do transistor, foi aberto uma infinidade de possibilidades de novas arquiteturas de *hardware*, transformando as válvulas termiônicas em transistores que consumiam significativamente menos energia e tinham uma a vida útil de *hardware* maior, por não gerar tanto calor. Como consequência disso, houve uma menor deterioração de seus materiais e a miniaturização dos componentes (ALMEIDA, 2012).

No ano de 1971, foi lançado comercialmente o primeiro *microchip* produzido pela Intel, o qual tinha o nome de Intel4004 e era um processador que possuía cerca de 2000 transistores. Sua rival, *Advanced Micro Devices* (AMD), até o ano de 1978 criou seus próprios *chips* e desenvolveu projetos a partir da tecnologia de outras empresas, por meio de licenças, produzindo, inclusive, *chips* para a própria Intel (ALMEIDA, 2012).

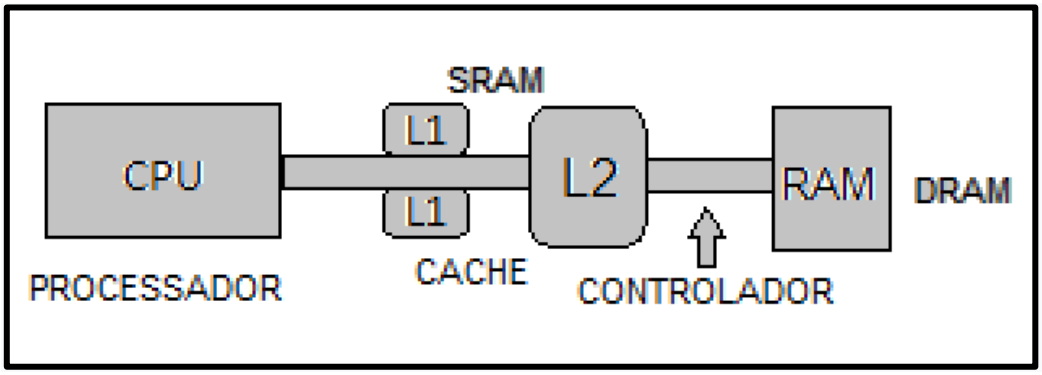
Os processadores funcionam executando os seguintes passos:

- Busca de uma instrução que estão na memória;
- Interpretação das instruções obtidas;
- Obtenção de um determinado dado da memória caso a instrução exija;

- Processamento do dado que pode ser uma operação aritmética;
- Gravação de dados na memória ou em um dispositivo de entrada e saída de dados.

Alguns dados processados são guardados temporariamente em uma memória especial, que se localiza no próprio corpo do processador, tem o nome de memória “cache” e geralmente é dividida entre cache L1 e L2, sendo a L1 a memória de maior velocidade e a L2 de menor velocidade entre as duas. A controladora decide se vai utilizar o dado novamente ou se ele pode ir para a memória de *Random Access Memory* (RAM), que se encontra a um nivel abaixo do *cache* L2 a figura 2 mostra como é composta a ligação entre memoria *cache* o controlador e a memoria *RAM* (STALLINGS, 2015).

Figura 2 - Hierarquia de memória



Fonte: Adaptado de Samsung, 2020.

Para que um sistema operacional funcione sobre uma camada de *hardware*, emprega-se uma hierarquia de memória. Essa hierarquia funciona como uma pirâmide que escala da memória de menor velocidade até a de maior velocidade, e dentro dos processadores existe um tipo de memória que opera na mesma frequência do processador e que tem o nome de registrador (STALLINGS, 2015).

Existem registradores visíveis ao usuário, os quais permitem que o programador de uma determinada linguagem de programação reduza as referências à memória. Devido a otimização do uso de registradores, eles são divididos em:

- Registrador de uso Geral: categoria de registrador que pode trabalhar operando para qualquer opcode que é a referência à instruição na qual o processador recebe para realizar uma determinada tarefa, ou seja, pode armazenar dados de execução do programa, e seu uso dentre um determinado conjunto de

instruções é ortogonal;

- Registrador de dados: são especialmente utilizados para armazenamento e dados, e não podem realizar cálculos de um endereço relacionado a um operando;
- Registrador de endereços: podem ser utilizados como registradores de uso geral, mas podem operar em modo de endereçamento;
- Registrador de índice: são dedicados a realizar a indexação dos endereços;
- Ponteiros de segmento: geralmente guardam o endereçamento de um segmento, tendo o endereço base como ponto de referência;
- Registradores de controle de estado: tipo de registrador o qual, quando autorizado pelo Sistema Operacional ou por programas com privilégios de administração, permite que algumas operações do processador sejam manipuladas (STALLINGS, 2015). Portanto, para que as instruções sejam executadas, é fundamental que existam os seguintes registradores:
    - Contador de programas (PC): armazena uma instrução a que será lida;
    - Registrador de instrução (IR): guarda a instrução que foi lida mais recentemente;
    - Registrador de *buffer* de memória (MBR): armazena um dado a ser escrito ou o dado que foi lido mais recentemente.

Existem duas principais arquiteturas que dominam o mercado de processadores: a *Reduced Instruction Set Computer* (RISC), que consiste em processadores no quais suas instruções são reduzidas e mais simples, e levam à mesma quantidade de tempo para serem executadas, ou seja, não possuem micro programação; a arquitetura *Complex Instruction Set Computer* (CISC), que contém um conjunto de instruções complexas, além de sustentar a micro programação, ou seja, as instruções são gravadas no processador, o que fornece a possibilidade interpretar comandos de programas e executá-los a partir das instruções já gravadas no processador, quebrando esses comandos e transformando-os em instruções de baixo nível (STALLINGS, 2015).

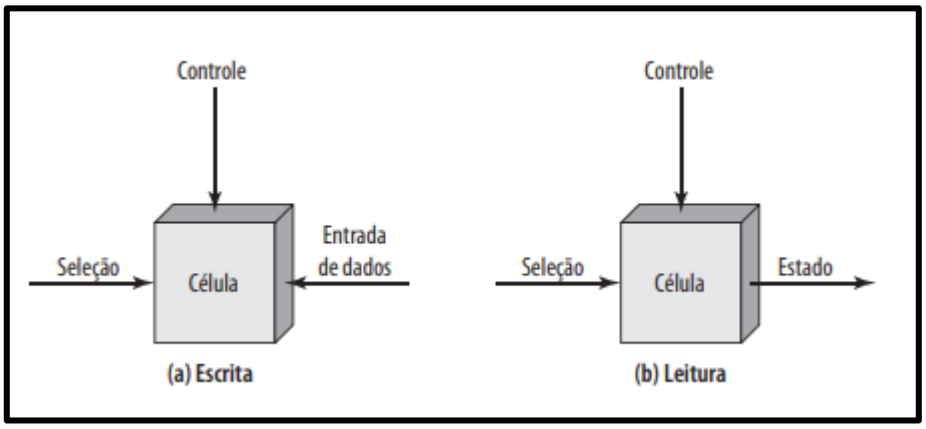
3.2.2 Memória

3.2.2.1 Memória Interna

Nos primores da computação, havia uma ideia de que os programadores desejariam uma quantidade cada vez maior de memória rápida para a programação de suas aplicações. Essa ideia virou uma realidade, na qual a cada dia os computadores pessoais precisam de uma quantidade maior de memória para poder rodar suas aplicações de maneira estável. Porém, quanto maior a velocidade da memória, maior é o custo de sua fabricação, uma vez que para obter um nível mais alto de velocidade são necessários materiais de valor alto e um nível de tecnologia de construção elevado, o que, como consequência, gera um produto mais caro. Para baratear os custos desses componentes, a memória foi dividida em partes, sendo que quanto mais próxima a velocidade do processador, menor é a quantidade de armazenamento, maior é sua velocidade, priorizando as atividades mais críticas: as memórias de maior velocidade. No oposto dessa hierarquia estão as memórias de maior quantidade de armazenamento e que possuem menor velocidade de leitura e escrita, sendo as mais baratas e tendo sua utilidade voltada para atividades de uso geral (HENNESSY; PATTERSON, 2019).

A memória semicondutora tem como elemento principal a célula de memória e apresenta dois estados estáveis, que são 0 e 1, além de possuir a capacidade de receber escrita a ser lida para verificação de estado. Outra característica dessas memórias é que seu tipo de acesso é aleatório, comumente chamadas de memória *Static Random Acess Memory* (SRAM). Para isso, é necessário uma lógica de endereçamento interna para a localização de um determinado dado, não tendo a necessidade de realizar atualizações constantes e sendo mais rápida e econômica que a memória do tipo (DRAM). Sua leitura e escrita é realizada por meio de sinais elétrico. Figura 3 mostra como é realizado esse controle (STALLINGS, 2015).

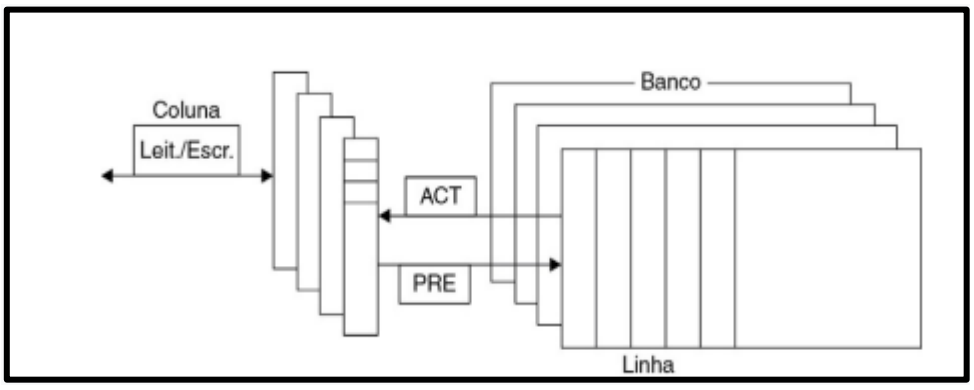
Figura 3 – Registrador



Fonte: Stallings, 2015.

Além da memória (SRAM), também há outra tecnologia de memória interna denominada *Dynamic Random Acess Memory* (DRAM), que possui uma fabricação bem mais barata que as do modelo (*SRAM*), mas que entregam um menor nível de velocidade, além de possuírem a necessidade de realizar constantes atualizações de pulsos para manter seu funcionamento e seus dados carregados a figura 4 apresenta a estreutura da *SRAM* (HENNESSY; PATTERSON, 2019).

Figura 4 - Estrutura da SRAM



Fonte: Hennessy e Patterson, 2019.

As memórias (DRAM) atuais possuem uma arquitetura, onde sua matriz tem uma densidade máxima de 64gb, o que é quatro vez maior que sua antecessora.

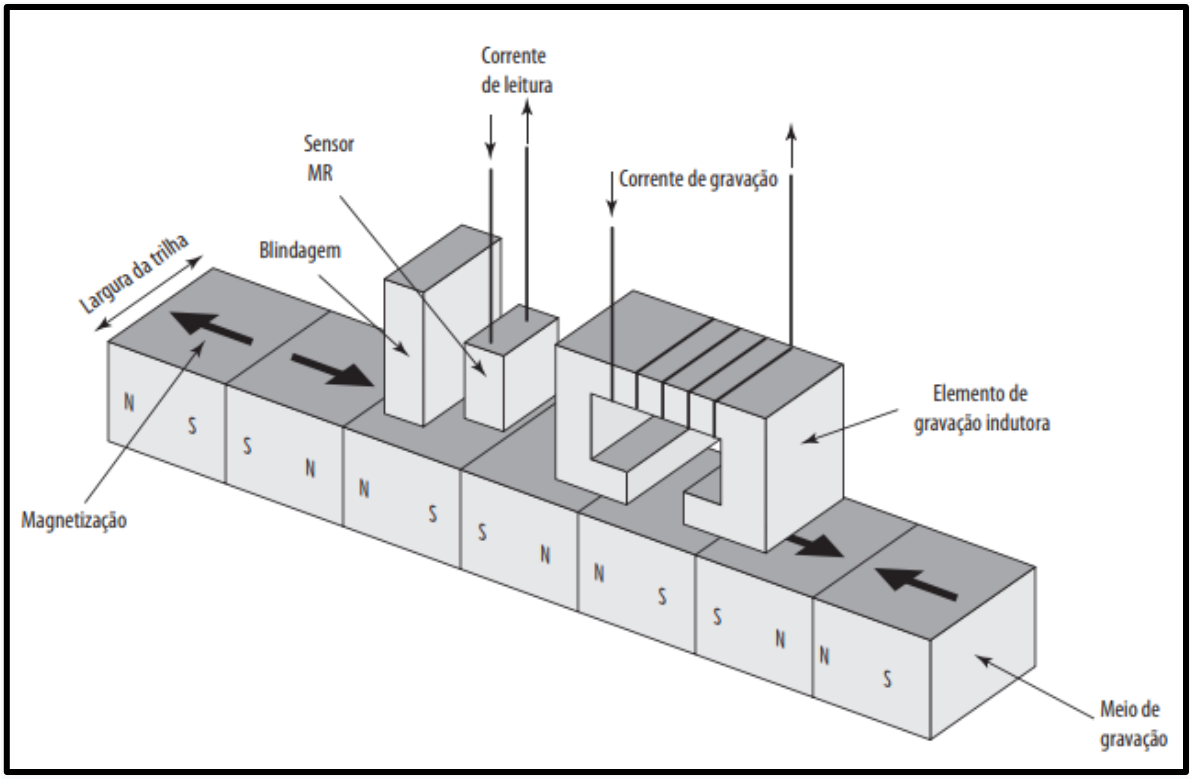
3.2.2.2 Memória Externa

A memória externa é geralmente utilizada para armazenamento de arquivos,

uma vez que não perde seus dados quando não está energizada. A maioria dos computadores ainda utiliza o *Hard Disk* (HD), que consiste em um disco magnético onde os dados são gravados por meio de magnetismo. Dentro do HD existem algumas estruturas que, em conjunto, realizam a leitura e escrita desses dados. O mecanismo possui uma bobina que produz um campo magnético. Os pulsos elétricos são direcionados à cabeça, que realiza a gravação com diferentes padrões, oscilando entre zeros e uns. Para a leitura dos dados gravados, o disco gira e seu movimento gera uma corrente que possui a mesma polaridade daquela já gravada (STALLINGS, 2015).

Em um HD, os dados são organizados em trilhas. Cada trilha possui a mesma largura da cabeça ,que realiza a leitura e escrita, sendo que existem milhares de trilhas dentro de um disco rígido, que são separadas por pequenos espaços para impedir que haja alguma falha de alinhamento da cabeça, geralmente ocorrida em função de uma interferência entre os campos magnéticos e as trilhas, a figura 5 apresenta um sistema de gravação magnética (STALLINGS, 2015).

Figura 5 - Sistema de gravação magnética

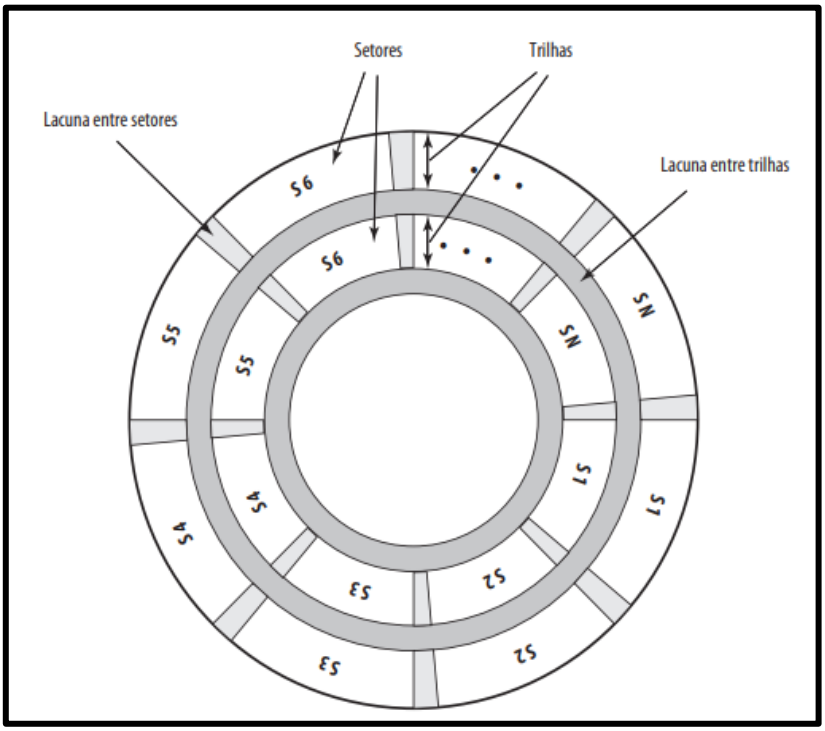


Fonte: Stallings, 2015.

Cada trilha, geralmente, possui centenas de setores de tamanho fixo ou

variável. Na maioria dos casos, esses setores são de tamanho fixo para evitar que o seja imposto níveis de precisão excessivos no sistema. Entre os setores, existem lacunas denominas de intersetores, na figura 6 é demonstrada a organização de um HD (STALLINGS, 2015).

Figura 6 - Organização do HD



Fonte: Stallings, 2015.

As trilhas de um HD possuem dois pontos que delimitam o ponto inicial e final. Para realizar a localização desses pontos, cada um possui um endereço, tendo um *byte SYNCH* com padrão especial que limita o início e fim do campo. Quando uma formatação é realizada, o que o SO mostra para o usuário é que todos os arquivos foram apagados. Porém, há algumas ferramentas que conseguem resgatar esses dados apagados por meio de algoritmos que identificam o id inicial da trilha apagada e fazem a engenharia reversa dos endereços de cada espaço de memória (STALLINGS, 2015).

3.2.2.3 Sistema de Arquivo FAT

O *File Allocation Table* (FAT) surgiu em 1977 e era utilizado *no Microsoft Disk Operating System (MS-DOS)*. Seu funcionamento consistia em uma tabela que indica

onde cada arquivo está localizado. Esse esquema se mostra eficiente, uma vez que a gravação dos blocos pode variar de tamanho e posição e a tabela funciona como um guia para a localização desses blocos na figura 7 mostra um modelo de organização do sistema de arquivos *FAT* (ALECRIM, 2011).

Figura 7 - Sistema de arquivos *FAT*

Fonte: Microsoft Learn, n.d.

Com o passar do tempo, o sistema de arquivos *FAT* foi ganhando atualizações para acompanhar as novas tecnologias e o aumento da capacidade de armazenamento dos dispositivos. Uma das atualizações mais significativas foi do FAT16, o qual utilizava 16 bits para realizar o endereçamento, o que limitava o tamanho de suas partições a apenas 2GB, sendo necessário um upgrade de sua capacidade. A partir disso, seu sucessor nasceu, o *FAT32*, o qual resolveu o problema de armazenamento que seu antecessor possuía, pois trabalhava com 32bits de endereçamento, passando de uma capacidade máxima de 2GB para 2TB (ALECRIM, 2011).

Uma das desvantagens principais do FAT é a sua fragmentação. Uma das recomendações para quem utilizava o Windows 95 era utilizar uma aplicação que realizasse a desfragmentação, pois, com o passar do tempo, os fragmentos de dados ficavam por todo o disco, tornando-o mais lento (ALECRIM, 2011).

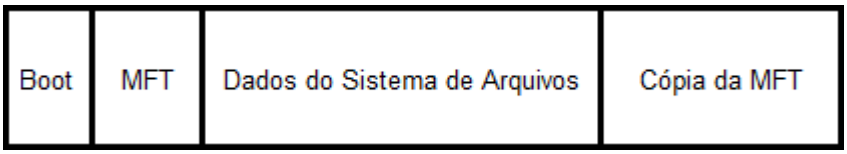
3.2.2.4 Sistema de Arquivo NTFS

O *New Technology File System* (NTFS) é o sistema de arquivos mais utilizado pelo sistema operacional da Microsoft, o *Windows.* O NTFS foi criado para substituir o FAT, que possuía muitas limitações. Ele veio para fazer parte do *Windows* NT, que era o novo sistema operacional da Microsoft, feito para fazer frente ao crescimento das soluções com base no *Unix* (ALECRIM, 2011).

O NTFS utiliza 64bits para realizar o endereçamento dos dados e sua capacidade máxima por partição é de 256TB, mostrando-se superior ao FAT32, que é de apenas 2TB. Para manter sua integridade, o NTFS realiza: verificação do log com o objetivo de identificar quais cluster devem ser corrigidos e reversão de

procedimentos não concluídos. Outra vantagem do NTFS é que o sistema operacional pode definir grupos de usuários para acessar um determinado arquivo ou pasta, a figura 8 apresneta a organização do sistema de arquivos NTFS (ALECRIM, 2011).

Figura 8 - Sistema de arquivos NTFS



Fonte: Microsoft Learn, n.d.

3.2.2.5 Sistema de Arquivo EXT4

O sistema de arquivos EXT4 é dividido em grupos de blocos que são alocados dentro do mesmo grupo, o que reduz o tempo de busca e minimiza a fragmentação do disco. Cada bloco é composto por um grupo de setores entre1KiB e 64KiB, sendo que a quantidade de setores deve ser uma potência integral de 2. Esses blocos são agrupados em unidades maiores denominadas de grupos de blocos. O tamanho da página de memória deve ser maior ou igual ao do bloco, para evitar conflitos na hora da montagem (DJWONG, 2017). O EXT4 pode trabalhar com arquivos de 32 ou 64 bits, sendo que seus limites são os seguintes (Figura 9) para 32bits:

Figura 9 - Limite de trabalho ext4 32bits

Item	1 KiB	2 KiB	4 KiB	64 KiB
Blocos	2^32	2^32	2^32	2^32
Inodes	2^32	2^32	2^32	2^32
Tamanho do sistema de arquivos	4TiB	8TiB	16TiB	256TiB
Blocos por grupo de blocos	8.192	16.384	32.768	524.288
Inodes por grupo de blocos	8.192	16.384	32.768	524.288
Tamanho do grupo de blocos	8 MiB	32MiB	128MiB	32 GiB
Blocos por arquivo, extensões	2^32	2^32	2^32	2^32
Blocos por arquivo, mapas de blocos	16.843.020	134.480.396	1.074.791.436	4.398.314.962.956 (realmente 2^32 devido a limitações de tamanho de campo)
Tamanho do arquivo, extensões	4TiB	8TiB	16TiB	256TiB
Tamanho do arquivo, mapas de blocos	16 GiB	256 GiB	4TiB	256TiB

Fonte: Linux, n.d.

E para 64bits são:

Figura 10 - Limite de trabalho ext4 64bits

Item	1 KiB	2 KiB	4 KiB	64 KiB
Blocos	2^64	2^64	2^64	2^64
Inodes	2^32	2^32	2^32	2^32
Tamanho do sistema de arquivos	16ZiB	32ZiB	64ZiB	1YiB
Blocos por grupo de blocos	8.192	16.384	32.768	524.288
Inodes por grupo de blocos	8.192	16.384	32.768	524.288
Tamanho do grupo de blocos	8 MiB	32MiB	128MiB	32 GiB
Blocos por arquivo, extensões	2^32	2^32	2^32	2^32
Blocos por arquivo, mapas de blocos	16.843.020	134.480.396	1.074.791.436	4.398.314.962.956 (realmente 2^32 devido a limitações de tamanho de campo)
Tamanho do arquivo, extensões	4TiB	8TiB	16TiB	256TiB
Tamanho do arquivo, mapas de blocos	16 GiB	256 GiB	4TiB	256TiB

Fonte: Linux, n.d.

3.3 Forense Digital

Uma perícia digital tem como finalidade realizar a identificação das ações que foram realizadas dentro de um determinado dispositivo digital, sendo necessária a utilização de ferramentas e um conjunto de metodologias científicas (DELLA VECCHIA, 2019).

Para a realização de uma perícia forense, é de suma importância seguir um processo, que pode ser aplicado não somente na área digital, mas em diversas áreas de perícia, e geralmente seu fluxo é seguido como o disposto na Figura 11, a seguir:

Figura 11 - Etapas da Perícia forense

Fonte: Adaptado de Della Vecchia, 2014, p. 82.

3.3.1 Identificação

Para realizar a identificação de qualquer objeto que possa conter evidências de um crime, é necessário um mandado judicial de busca e apreensão, que pode ser expedido por um magistrado ou juiz que autoriza os policiais da ocorrência a conduzir a busca (DELLA VECCHIA, 2014).

Com o mandato, o perito realiza a identificação dos objetos que possam conter evidências do crime, tais como: hd, pendrive, cd, fita e vários outros dispositivos que armazenam dados. O criminoso pode também camuflar os dispositivos com o intuito de enganar o perito e investigadores que participem do caso (DELLA VECCHIA, 2014).

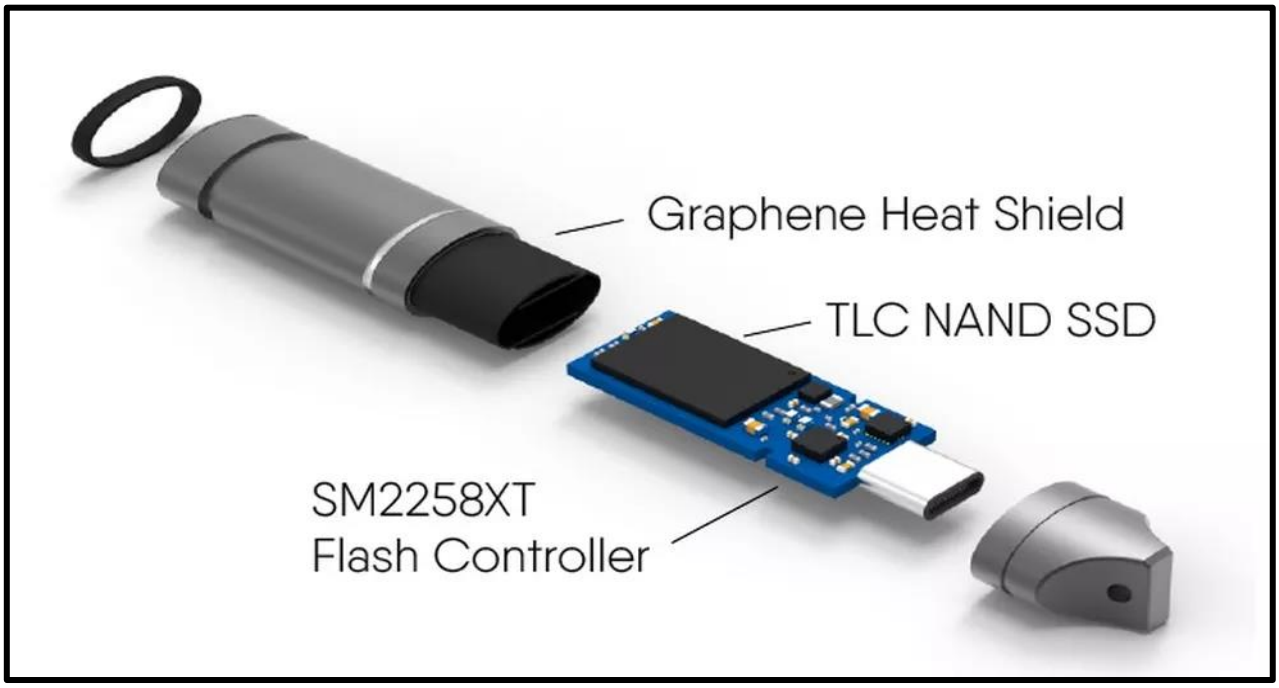
Figura 12 - SSD camuflado em chaveiro

Fonte: KICKSTARTER, n.d.

Na Figura 12, pode-se ver um chaveiro com alguns itens como fones de ouvido, chaves e um item metálico muito pequeno que poderia passar despercebido ao olhar

da maioria das pessoas. Nentanto esse é uma Unidade de Estado Sólido (SSD), que tem a capacidade de armazenar 2TB de memoria (KICKSTARTER, 2021).

Figura 13 - SSD Aberto



Fonte: Kickstarter, n.d.

A Figura 13 apresenta a estrutura interna do dispositivo. Um perito deve saber identificar esses itens, pois esses podem conter informações valiosas para compor uma determinada investigação. Ressalta-se que a cada dia dispositivos mais compactos estão sendo criados, fazendo com que o perito tenha que se atualizar sobre as novas tecnologias (DELLA VECCHIA, 2014).

Geralmente, o perito deve apreender somente o dispositivo que contem as evidências. Um computador é composto por diversos componentes. No entanto, somente o itens que possam conter evidências devem ser coletados para realizar a etapa de exame (DELLA VECCHIA, 2014).

Em qualquer mandado de busca de um dispositivo eletrônico, é necessário que a hora atual do equipamento seja devidamente arquivada e mantida para evitar alguma inconsistência que possa prejudicar as evidências.

Quando o dispositivo está ligado, é possível obter as horas antes de realizar seu desligamento, podendo realizar a retirada de seu dispositivo de armazenamento

com segurança. Porém, há situações onde o perito não encontra a máquina ligada ou ela está impossibilitada de realizar sua inicialização, fazendo-se necessária a retirada do dispositivo de armazenamento sem a marcação do horário atual de funcionamento. Nesse caso, a obtenção de seu horário para verificação da hora é realizada por meio do *setup* (DELLA VECCHIA, 2014).

3.3.2 Coleta

Na etapa de coleta, o perito deve realizar a coleta das evidências, fotografando, filmando ou etiquetando cada equipamento para compor a análise. Isso possibilita identificar detalhes que não foram avaliados no momento da coleta, mas que posteriormente e com as devidas ferramentas, podem ser obtidos.

Figura 14 - Exemplo de etiquetas usadas na coleta

Equipamento: Gabinete 7 **Fabricante:** LG **Número de Série:** 788985 **Cor:** Preto **Observação:** Possui adesivo com nome da empresa
Armazenamento: HD **Fabricante:** Western Digital **Níúmero de Série:**4G2D58S14D

Fonte: Adaptado de Della Vecchia, 2014, p. 86.

Para manter a integridade dos arquivos contidos na mídia, é realizada uma cópia *bit* a *bit* dos dados do dispositivo. Com esse procedimento, se obtem uma cópia idêntica das evidências do dispositivo e o trabalho de perícia deverá ser realizado a partir dessa cópia, com o intuito de manter a total integridade dos dados da mídia original. Esse arquivo de cópia é chamado de imagem e apresenta o mesmo tamanho da original (DELLA VECCHIA, 2014).

3.3.3 Exame

A partir das imagens geradas na etapa de coleta, o perito pode utilizar ferramentas para realizar buscas de evidências. Para isso, os peritos utilizam alguns sistemas operacionais especializados em forense que vêm com os *softwares* adequados para realizar a busca e análise dos dados (DELLA VECCHIA, 2014).

3.3.4 Análise

A analise é uma etapa que não possui um padrão especifico ou seja ela deve girar em torno das informações obtidas durantes as etapas anteriores. Uma sequência de passos deve ser montada a partir das evidencias coletadas sendo necessário que a autoridade responsável pelo caso delimite o escopo ao qual o perito deve elaborar a sequência de perguntas a ser respondida. Muitos filtros devem ser aplicados com o intuito de refinar as informações tornando assim muito difícil automatizar essa etapa do processo de perícia (DELLA VECCHIA, 2014)

3.3.5 Resultados

Na fase de resultados, o laudo é gerado, apresentando-se um relatório da investigação. Nesse, devem estar os procedimentos metodológicos e todas as ferramentas e técnicas utilizadas durante o processo de investigação (DELLA VECCHIA, 2019).

Esses dados devem ser distribuídos de forma clara e de fácil compreensão, pois, geralmente, quem realizar a avaliação do caso após a entrega do laudo pericial é alguma autoridade, que muitas vezes não está familiarizada com determinadas teologias e técnicas de forense digital. Nesse sentido, termos técnicos devem ser evitados (DELLA VECCHIA, 2019).

O laudo deve demonstrar, de forma imparcial e transparente, os resultados da investigação, mostrando a metodologia utilizada e a relação de evidências encontradas, já que quem decidirá o rumo do processo é a autoridade da área jurídica (DELLA VECCHIA, 2019).

A estrutura do laudo é composta por uma introdução, que deve conter o número do protocolo, da ocorrência e do inquérito e muitos outros dados de identificação. A metodologia utilizada, que descreve os procedimentos utilizados no período em que o trabalho de perícia foi realizado, possui o objetivo de consolidar o laudo pericial, protegendo-o de uma futura contraprova (DELLA VECCHIA, 2019).

A conclusão do laudo pericial, geralmente, é composta por um questionário, que deve ser respondido de forma imparcial, levando apenas em consideração os dados obtidos na investigação (DELLA VECCHIA, 2019).

3.3.6 Máquina Virtual

A máquina virtual ou VM simula um computador virtual com CPU, memória e discos para armazenamento de arquivos. Ela permite que um sistema rode dentro de outro sistema, podendo usufruir de todas as suas funcionalidades. A vantagem de utilizar uma máquina virtual é que com ela pode-se manipular arquivos de maneira isolada do sistema principal do computador. Nesse sentido, se houver algum arquivo que possa infectar e comprometer o sistema operacional ao qual a máquina virtual está rodando em cima, o invasor não conseguirá atingir o sistema externo, pois a VM em *sandbox* é um ambiente controlado e seguro para realização de testes.

Um exemplo de software de virtualização é o Virtual Box. Nesse, a criação de uma máquina virtual é simples e rápida, permitindo que o usuário configure a quantidade de núcleos que o processador da máquina física deve dedicar à máquina virtual a quantidade de memória RAM, além alocar, de maneira estática ou dinâmica, o armazenamento de dados.

3.3.7 Caine

Caine é um sistema Linux baseado em Ubuntu, e foi criado pelo gerente de projeto Nanni Bassetti, com o intuito de oferecer um sistema com ferramentas simples e práticas como o Guymager, que realiza a criação de imagens forenses por meio de uma interface amigável. Os dados das cópias são idênticos aos originais, podendo acrescentar algumas informações relativas à mídia de armazenamento e realizar cálculos de hash (CAINE, 2021).

O Caine também possui uma poderosa fermenta de código aberto, que pode realizar a análise de mídias, o Autopsy, que pode abrir diversos tipos de imagens geradas de dispositivos de armazenamento e obter evidências dentre essas imagens, como tipo de sistema operacional utilizado, data de login de usuários, histórico de navegação de internet e até mesmo se um arquivo foi copiado para outro dispositivo externo a máquina apreendida. A figura 16, a seguir, apresenta a tela inicial do Caine Linux.

Figura 15 - Caine Linux

Fonte: Sidereal, n.d.

4 PERÍCIA

Para realização da pericia, foi montado um ambiente em uma máquina virtual (VM) com distro Linux Caine em modo live dedicando 4 núcleos de processamento, 2 GB de memória RAM e 30 gb de armazenamento no formato ext4 . Com o intuito de aproximar-se ao máximo de um teste real, a distro está em modo live, pois muitos peritos utilizam essa abordagem como forma de manter a integridade dos dados da máquina ou dispositivo removível em que as evidências estão contidas.

O processo de instalação de um sistema na máquina em que a perícia será realizada pode gerar alguma inconsistência nos dados a serem avaliados. Além disso, uma distro em live se mostra bem mais prática e rápida ainda, mantendo todas as ferramentas que teria se ela fosse instalada na máquina a qual a perícia será realizada.

A imagem utilizada foi obtida do site “Cfreds”, que disponibiliza arquivos de imagem gerados sinteticamente com o intuito de auxiliar peritos no treinamento e aprendizado forense. A abordagem utilizada para obtenção da imagem foi definida para que não houvesse qualquer tipo de violação dos dados pessoais de qualquer que fosse o dispositivo abordado, seguindo as normas estabelecidas pela Lei geral de proteção de dados (LGPD).

O arquivo de imagem *data duplicato* (DD) foi gerado com base em uma história fictícia, onde uma multinacional estava desenvolvendo novas tecnologias que eram de extremo sigilo. No entanto, um de seus diretores foi subornado por uma empresa rival que queria obter as informações sobre a multinacional. Quando o diretor estava saindo da empresa, foi barrado pela equipe de segurança, que desconfiou de sua recente utilização de um computador, ao qual ele não era autorizado a utilizar, e por sua saída de forma repentina. Com ele, foi encontrado um HD externo, que foi analisado pela equipe de segurança, não sendo identificado nenhum arquivo sigiloso. No entanto, a política de segurança da empresa deixa bem claro que em caso de possível vazamento de dados, é necessária a verificação dos dispositivos por um profissional da área forense, e assim se iniciou a análise do HD externo confiscado.

4.1 Identificação

Na primeira etapa, é realizada a identificação de todos os possíveis detalhes

que possam conter evidências, como dispositivos camuflados, um pendrive conectado ou não na máquina, dentre outros detalhes. Tudo é fotografado e devidamente organizado para que o ambiente possa ser reavaliado em uma futura investigação detalhada. Como a imagem foi criada sinteticamente, essa etapa está descrita para complementar o laudo geral de forma sequencial e coerente, uma vez que se trata de uma simulação.

4.2 Coleta

Na etapa de coleta, as identificações sobre o dispositivo são reunidas, tais como: número de série, marca configuração e qualquer tipo de dado que possa auxiliar na obtenção de evidências. Como se trata de uma imagem sintética, os dados obtidos são do site “Cfreds”. Nas Figuras 17 e 18 são apresentados os detalhes dos dispositivos nos quais as imagens DD foram geradas.

Figura 16 - Computador Diretor

Equipamento: Gabinete **Fabricante:** Asus **Número de Série:** 846185 **Cor:** Preto **Observação:** Adesivo de identificação de patrimônio da empresa
Armazenamento: HD **Fabricante:** Western Digital **Número de Série:**652D58S14D
Sistema Operacional: Windows 7 **Versão do Sistema**: 6.1 **Raiz do Sistema**: C:\\Windows

Fonte: Elaboração própria.

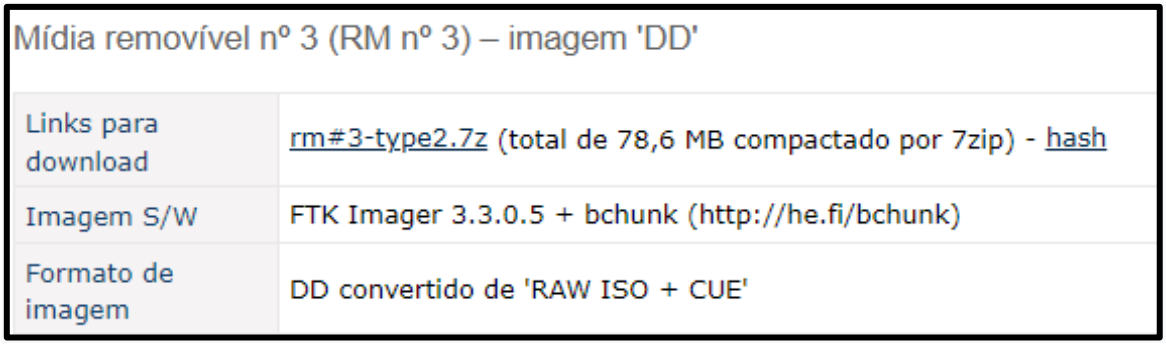
Figura 17 - CD Diretor

Equipamento: CD **Fabricante:** Sony **Cor:** branco **Tamanho do armazenamento:** 700mb **Observação:** Adesivo com etiqueta com nome sigiloso

Fonte: Elaboração própria.

A Figura 19 registra os detalhes da imagem DD que foi gerada para a perícia referente ao HD externo o qual o diretor estava portando durante a abordagem pela segurança.

Figura 18 - Imagem DD

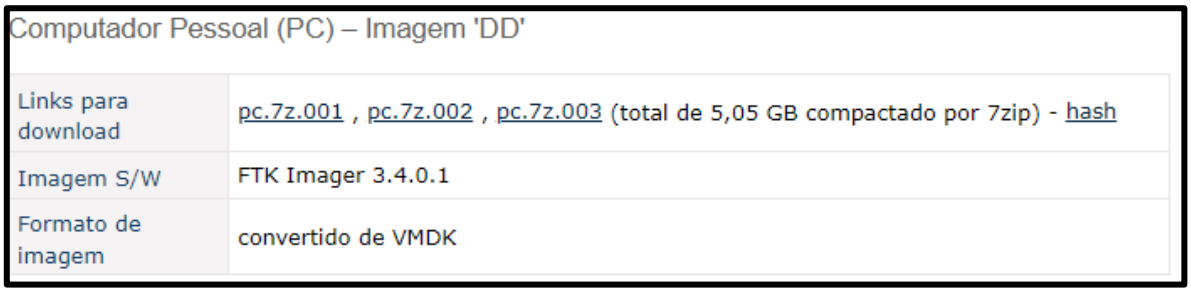


Mídia removível nº 3 (RM nº 3) – imagem 'DD'	
Links para download	rm#3-type2.7z (total de 78,6 MB compactado por 7zip) - hash
Imagem S/W	FTK Imager 3.3.0.5 + bchunk (http://he.fi/bchunk)
Formato de imagem	DD convertido de 'RAW ISO + CUE'

Fonte: Cfredsm, n.d.

A Figura 20 mostra as informações de compactação e formato da imagem DD gerada a partir do computador do diretor envolvido no caso.

Figura 19 - Imagem DD Computador Diretor

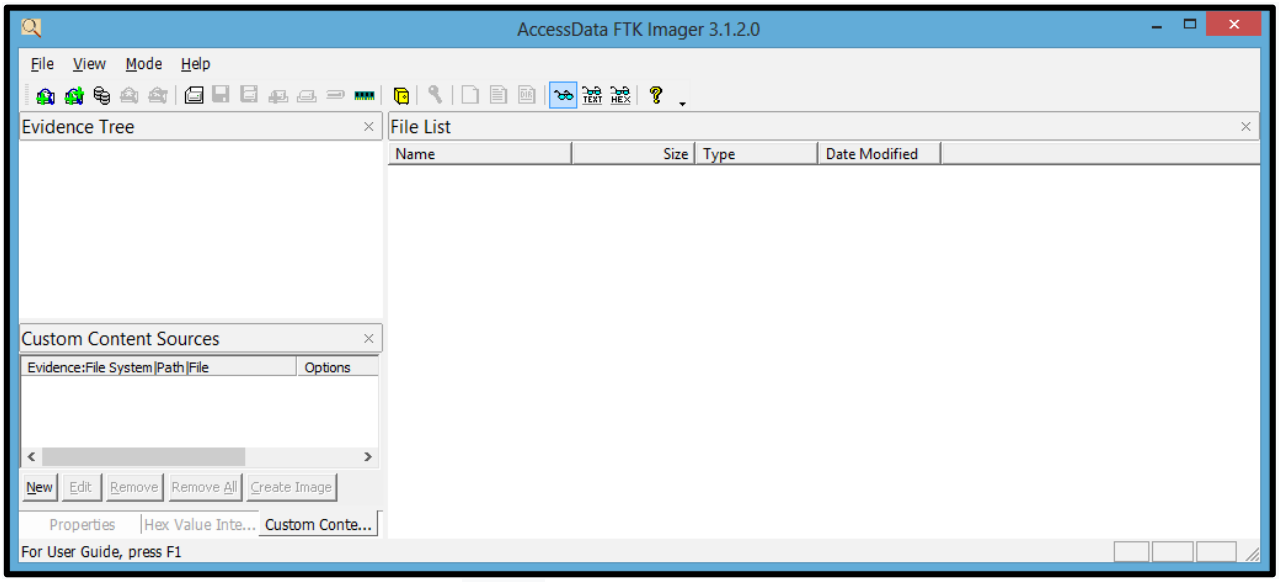


Computador Pessoal (PC) – Imagem 'DD'	
Links para download	pc.7z.001 , pc.7z.002 , pc.7z.003 (total de 5,05 GB compactado por 7zip) - hash
Imagem S/W	FTK Imager 3.4.0.1
Formato de imagem	convertido de VMDK

Fonte: Cfredsm, n.d.

As imagens foram criadas a partir da ferramenta FTK *Imager* (Figura 21), que é um *software* criado pela empresa Acess Date e possui várias funcionalidades para criação de imagens de disco e realizar *dumps* de memória, sendo amplamente utilizado em perícias a figura 4.2.5 apresenta a tela inicial do FTK *Imager*.

Figura 20 - Figura 4.2.5 FTK Imager

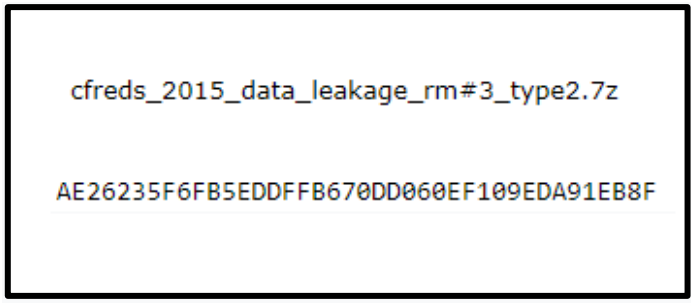


Fonte: Lau e Jasper, n.d

4.3 Exame

O primeiro ponto do exame compreende verificar se o Hash sh1 da cópia realizada é o mesmo da imagem original. A partir dessa comparação, busca-se identificar se houve alguma alteração no arquivo de imagem. Essa comparação é necessária, pois no processo de cópia alguma evidência pode ser perdida ou mesmo o próprio dispositivo verificado pode conter um mecanismo que altere os dados em caso de cópia como modo de defesa. A Figura 22 mostra *hash sh1* e nome do arquivo da imagem original.

Figura 21 - Hash sh1

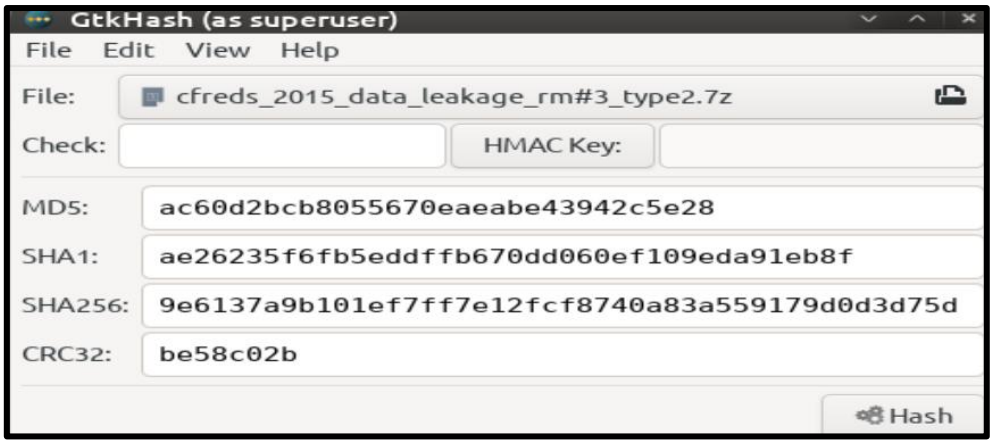


Fonte: CFREDS, n.d.

Para a verificação da cópia, foi utilizado o *software* GTKhash, que utiliza a biblioteca Mhash e no qual todos os cálculos da hash são realizados. A ferramenta, além do *hash sh1*, também mostra os valores do *hash md5*, *sha256* e *crc32*, como é

mostrado na Figura 23.

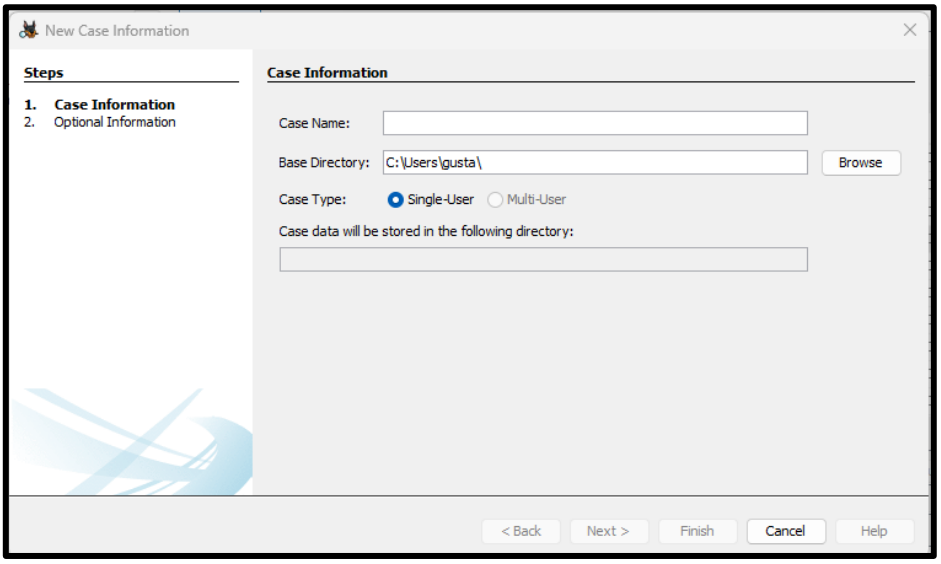
Figura 22 - GtkHash



Fonte: Elaboração própria.

Com a comparação do *sha1* original com a cópia, pode-se identificar que a cópia é fiel à imagem original do dispositivo. Em seguida, deve-se realizar a análise do conteúdo da mídia que foi obtida. Para essa análise, deve ser utilizada a ferramenta Autopsy, que pode identificar partições, arquivos ocultos, localização, dentre outros aspectos de uma imagem. A Figura 24, a seguir, mostra a interface do programa Autopsy.

Figura 23 - New case

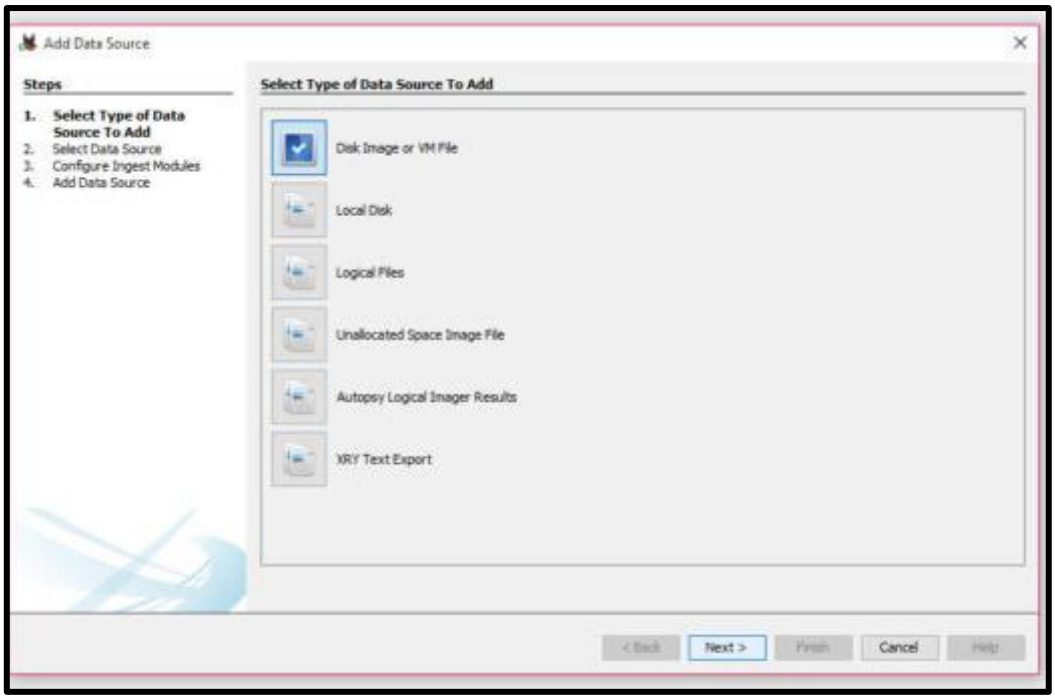


Fonte: Elaboração própria.

Na Figura 24, é mostrada a tela inicial, onde um novo caso é criado. Para dar início, é necessário dar um nome para identificar o projeto de busca na imagem. A

Figura 25 mostra a segunda etapa de configuração do Autopsy.

Figura 24 - Autopsy



Fonte: Elaboração própria.

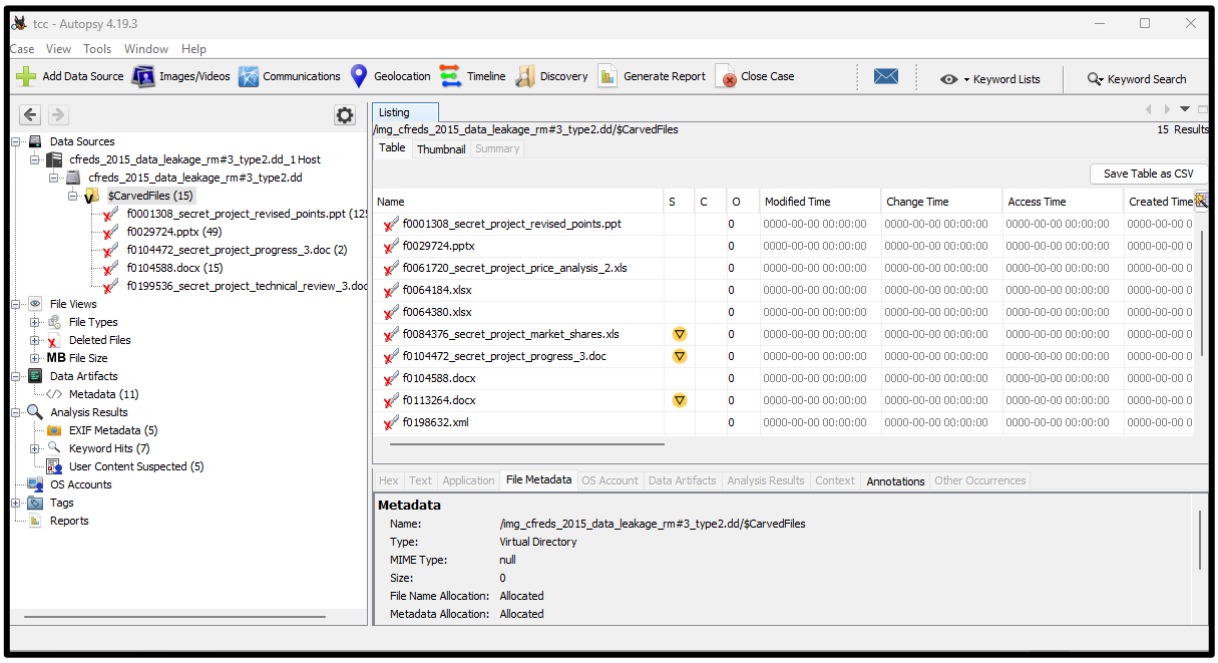
A Figura 25 mostra a tela onde é selecionado o tipo de arquivo de imagem que será utilizado e na Figura 26 se mostra a última etapa de configuração, que é a seleção do arquivo de imagem da raiz do sistema.

Figura 25 - Seleção de Imagem

Fonte: Elaboração própria.

Agora que o Autopsy está configurado, o arquivo de imagem será aberto, e, como se pode visualizar na Figura 27, todos os dados contidos na mídia podem ser manipulados e analisados.

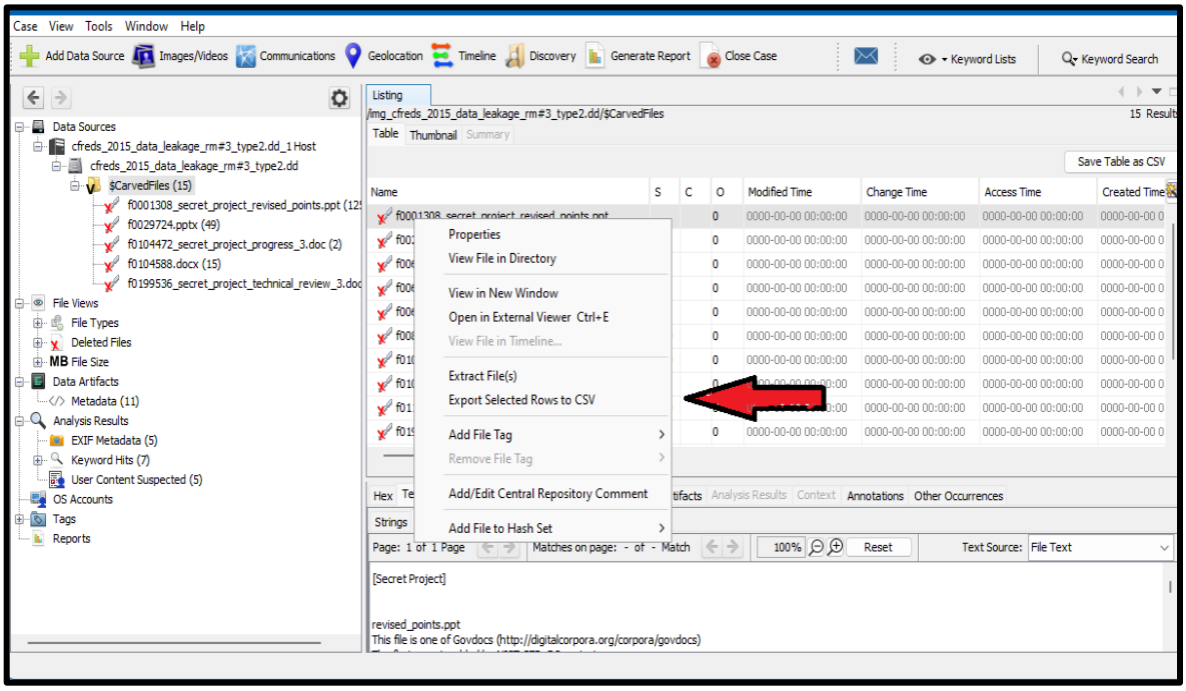
Figura 26 - Imagem montada



Fonte: Elaboração própria.

Na Figura 27, foram identificados 15 arquivos, que t:em tamanho e formato detalhados pela ferramenta de perícia. Dentre esses arquivos, alguns tinham os nomes que fazem referência ao projeto da multinacional. No entanto, apenas o nome não significa que realmente são os projetos que seriam entregues à empresa concorrente. Para ter mais detalhes sobre o conteúdo da empresa, a equipe de perícia convidou os funcionários da empresa responsáveis pelo projeto para que esses verificassem se realmente eram aqueles arquivos que tinham sido vazados Para isso, foi necessária a extração desses, como mostrado na Figura 28.

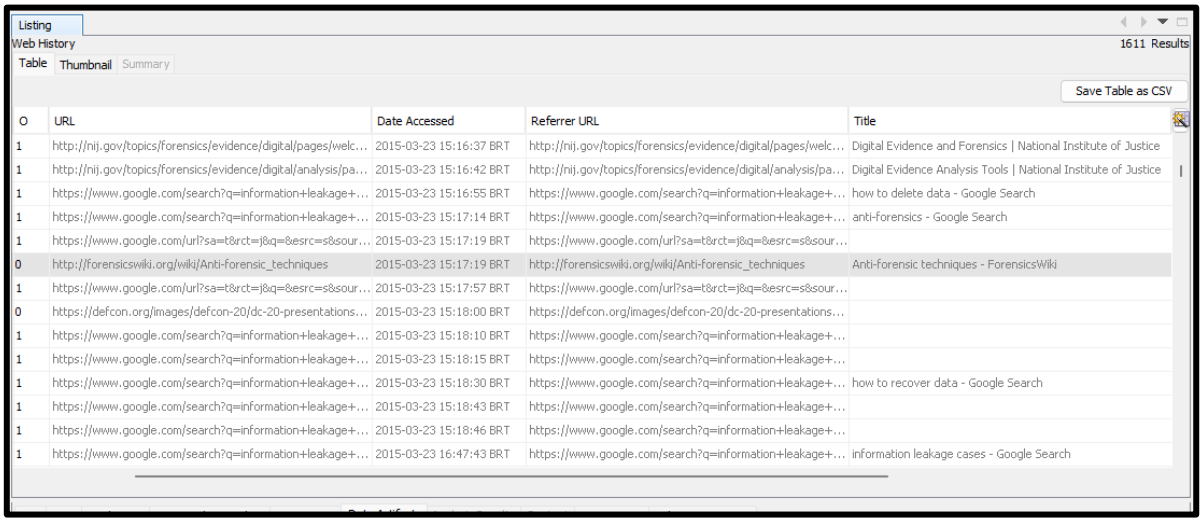
Figura 27 - Extração



Fonte: Elaboração própria.

Uma imagem DD do computador do diretor suspeito de vazamento de dados também foi gerada e examinada. Dentre as evidências verificadas, uma chamou a atenção, sendo o histórico de pesquisa do navegador “Google Chrome”, que apresentava buscas de como burlar técnicas de forense e de identificação de arquivos além de *downloads* de programas de limpeza de disco, o que indica que seu plano de vazamento de dados já tinha sido planejado há algum tempo e que ele temia que alguma equipe forense descobrisse seus planos. Na Figura 29, são mostrados detalhes a respeito, como data, hora e quais foram as pesquisas que o diretor realizou.

Figura 28 - Histórico Navegador

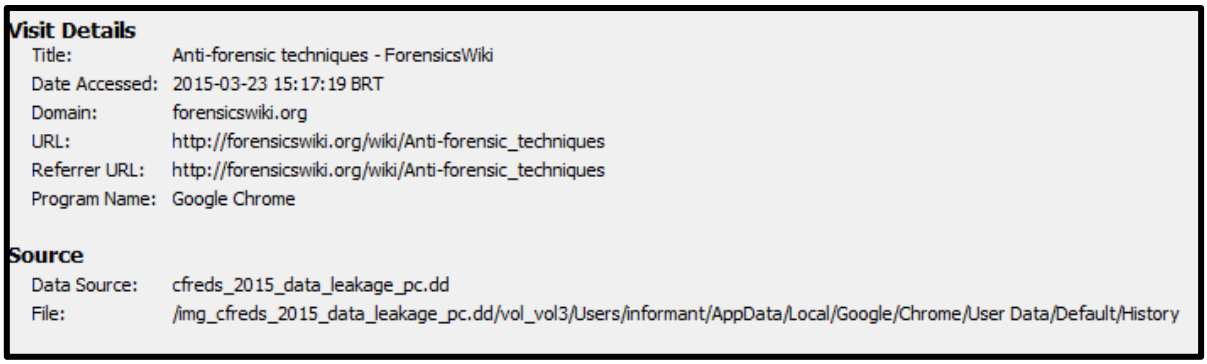


O	URL	Date Accessed	Referrer URL	Title
1	http://nij.gov/topics/forensics/evidence/digital/pages/welc...	2015-03-23 15:16:37 BRT	http://nij.gov/topics/forensics/evidence/digital/pages/welc...	Digital Evidence and Forensics | National Institute of Justice
1	http://nij.gov/topics/forensics/evidence/digital/analysis/pa...	2015-03-23 15:16:42 BRT	http://nij.gov/topics/forensics/evidence/digital/analysis/pa...	Digital Evidence Analysis Tools | National Institute of Justice
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:16:55 BRT	https://www.google.com/search?q=information+leakage+...	how to delete data - Google Search
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:17:14 BRT	https://www.google.com/search?q=information+leakage+...	anti-forensics - Google Search
1	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 15:17:19 BRT	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	
0	http://forensicswiki.org/wiki/Anti-forensic_techniques	2015-03-23 15:17:19 BRT	http://forensicswiki.org/wiki/Anti-forensic_techniques	Anti-forensic techniques - ForensicsWiki
1	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	2015-03-23 15:17:57 BRT	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&sour...	
0	https://defcon.org/images/defcon-20/dc-20-presentations...	2015-03-23 15:18:00 BRT	https://defcon.org/images/defcon-20/dc-20-presentations...	
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:18:10 BRT	https://www.google.com/search?q=information+leakage+...	
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:18:15 BRT	https://www.google.com/search?q=information+leakage+...	
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:18:30 BRT	https://www.google.com/search?q=information+leakage+...	how to recover data - Google Search
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:18:43 BRT	https://www.google.com/search?q=information+leakage+...	
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 15:18:46 BRT	https://www.google.com/search?q=information+leakage+...	
1	https://www.google.com/search?q=information+leakage+...	2015-03-23 16:47:43 BRT	https://www.google.com/search?q=information+leakage+...	information leakage cases - Google Search

Fonte: Elaboração própria.

Na Figura 30, é apresentada uma prova mais detalhada que o diretor estava pesquisando sobre ferramentas que burlassem uma investigação forense.

Figura 29 - Anti-Forense



Fonte: Elaboração própria.

4.4 Análise

Nesta etapa, todos os dados que foram extraídos da imagem DD foram comparados com os originais e todas as informações coletadas na etapa de exame foram analisadas com o intuito de configurar uma sequência de fatores que apontem ou não se o diretor estava realmente fazendo as informações da multinacional.

Dentro da imagem “cfreds_2015_data_leakage_pc_1_dd”, que se refere ao computador no qual o diretor realizou o acesso, foi identificado que pesquisas relacionadas a ferramentas de limpeza de disco e métodos de impedir investigações forenses foram realizadas próximas ao dia no qual o vazamento de dados aconteceu.

Os dados identificados na imagem DD “cfreds_2015_data_leakage_rm#3_type2”, que são do HD externo apreendido pela segurança, foram localizados no computador ao qual o diretor teve acesso e evidências que a cópia dos arquivos para o HD externo foi realizada, e que as datas da cópia e do conjunto de pesquisas são de forma sequencial, o que mostra o planejamento realizado pelo diretor afim de realizar o vazamento dos dados.

O sistema de câmeras também foi avaliado e as imagens mostraram o momento no qual o diretor realizou as pesquisas e o ponto em que ele conectou o Hd externo e realizou a cópia dos arquivos. As datações do navegador Chrome e da cópia dos dados obtidas por meio das imagens DD foram cruzadas com as imagens, e a conclusão foi que os horários foram os mesmos.

4.5 Resultados

Após a reunião de todas as provas, foi possível identificar que o resultado da investigação apontou o diretor como o principal agente de vazamento dos dados da multinacional, tendo em consideração seu histórico de utilização das máquinas da empresa. O CD encontrado em sua bolsa ao sair da empresa e as informações contidas no CD, que eram de mesmo tamanho de *hash* das que estavam no computador da empresa.

As investigações ainda deverão continuar para encontrar quem era o seu contratante na empresa rival e para evitar que novos vazamento ocorram na multinacional. Um relatório com todas as informações do caso foi gerado, contendo nome, telefone, datas de entrada e saída dos funcionários, depoimento das testemunhas, informações de login, navegador, informações do sistema operacional, dentre outras. A partir disso, um laudo foi gerado e enviado para a área judicial, que deverá conduzir o desfecho da investigação.

5 CONCLUSÃO

A computação cresce a cada dia e novas tecnologias estão constantemente surgindo. Com isso, há também uma necessidade de entender como os criminosos atuam diante dessa evolução tecnológica.

Grandes empresas estão a cada dia mais preocupadas com o setor de segurança de dados e o perito de crimes cibernéticos tem um papel fundamental nessa batalha contra esses invasores, uma vez que a cada investigação uma nova técnica de obter evidências pode ser criada, e, por meio dessa, novos meios de prevenir esses crimes podem ser criados.

Foi também identificado que, com ferramentas de código aberto, um perito pode realizar uma investigação sem ter que pagar por ferramentas de forense. A distro Linux Caine mostrou ser uma ótima alternativa para uma investigação no mundo real, apresentando um grande aparato de ferramentas de forense, além de entregar uma interface simples e fácil, não exigindo muito do *hardware*, por ser uma distribuição Linux baseada no Debian que é um dos sistemas operacionais mais consolidados na área de computação. Além disso, concluiu-se que com as ferramentas certas e um seguimento lógico adequado, um perito consegue obter evidências de diversos dispositivos de *hardware* mesmo se estiverem desligados.

Foi apresentado que, com as ferramentas corretas, dados como horário e acesso a navegadores, o que é de suma importância para uma investigação forense, podem ser obtidos e validados de maneira concisa e não muito complexa, o que ajuda a diminuir o tempo da investigação.

Com isso, conclui-se que a cada investigação uma nova técnica e seguimento logico deverá ser utilizado. Nesse sentido, para a devida condução das investigações, o perito deve estar caminhando juntamente à legislação que vigora sobre os dados que estão sendo obtidos. Além disso, em uma investigação, fatores externos à própria informática, como uma movimentação de uma pessoa de um lugar físico para outro, pode ser uma evidência crucial para o desenrolar do caso.

5.1 Trabalhod futuros

Recomenda-se para trabalhos futuros:

● Realizar a análise forense nas demais imagens DD que constituem o caso geral.

● Fazer o uso das demaisferramentas da distro Caine com o intuito de explorar seu potencial.

● Realizar uma busca mais detalhada a fim de identificar programas ant-forese utilizados.

REFERÊNCIAS

ALMEIDA, R. **Evolução dos Processadores Comparação das Famílias de Processadores Intel e AMD.** Campinas: Universidade Estadual de Campinas, 2012. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2009/T2/089065-t2.pdf. Acesso em: 10 ago. 2022.

BRASIL ESCOLA. Revolução do Computador. **Brasil Escola**, n. d. Disponível em: https://brasilescola.uol.com.br/informatica/revolucao-do-computador.htm. Acesso em 24 de maio de 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 mar. 2022.

CFREDS. **Caso de Vazamento de Dados.** n.d. (On-line). Disponível em: https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html. Acesso em: 10 out. 2022.

DELLA VECCHIA, E. D. **Perícia digital:** da investigação à análise forense. São Paulo: Millennium, 2019.

DJWONG. EXT4. **Ext4 Disk Layout.** 2017 (On-line). Disponível em: https://ext4.wiki.kernel.org/index.php? title=Ext4_Disk_Layout&oldid=9077. Acesso em: 20 maio 2022.

GOV.BR. ANPD participa de Seminário que discute o combate aos crimes cibernéticos. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-seminario-que-discute-o-combate-aos-crimes-ciberneticos. Acesso em: 27 mar. 2022.

INTERNET SOCIETY. **Brief History of the Internet.** 1997 (On-line). Disponível em: https://www.internetsociety.org/internet/history-internet/brief-history-internet/#f5. Acesso em: 15 maio 2022.

KICKSTARTER. **Bullet SSD:** unidade minúscula e de alta velocidade - cabe no seu chaveiro. n.d. (On-line). Disponível em: https://www.kickstarter.com/projects/473944941/bullet-ssd-tiny-and-high-speed-drive-fits-on-your-key-chain. Acesso em: 10 out. 2022.

LAU, M.; JASPER, N. FTK Imager: Encontrando arquivos excluídos. **Devmedia**, n.d. (On-line). Disponível em: https://www.devmedia.com.br/ftk-imager-encontrando-arquivos-excluidos/29614. Acesso em: 10 out. 2022.

LINUX. **Sistemas de arquivos no kernel do Linux.** Ext4 estruturas de dados e algoritmos. Projeto de alto nível. n.d. (On-line). Disponível em: https://www.kernel.org/doc/html/latest/filesystems/ext4/overview.html. Acesso em: 10 out. 2022.

MICROSOFT LEARN. **Incentive todas as possibilidades.** n.d. (On-line). Disponível

em: https://technet.microsoft.com/en-us/library/cc776720 (v=ws.10).aspx. Acesso em: 10 out. 2022.

MILAGRE, J. A relação da segurança da informação e perícia em informática com Lei Geral de Proteção de Dados (LGPD). **Jusbrasil**, 2019. Disponível em: https://josemilagre.jusbrasil.com.br/artigos/770656658/a-relacao-da-seguranca-da-informacao-e-pericia-em-informatica-com-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 27 mar. 2022.

SAMSUNG. **Saiba como funciona a memória cache do seu computador.** 2020 (On-line). Disponível em: https://www.sosdigital.com.br/saiba-como-funciona-a-memoria-cache-do-seu-computador/amp/. Acesso em: 10 out. 2022.

SIDEREAL. **Computer Aided Investigative Environment.** n.d. (On-line). Disponível em: https://www.caine-live.net/caine1204.jpg. Acesso em: 10 out. 2022.

SOUZA, P. F. C. Per**ícia Forense Computacional:** procedimentos, ferramentas disponíveis e estudo de caso trabalho de conclusão de curso. 2015. 73f. Trabalho de Conclusão de Curso (Bacharelado e m Tecnologia de Redes de Computadores) – Universidade de Santa Maria, Santa Maria, 2015. Disponível em: http://www.redes.ufsm.br/docs/tccs/Paulo-Souza.pdf. Acesso em: 5 maio 2022.

STALLINGS, W. **Arquitetura e Organização de Computadores.** 10. ed. São Paulo: Pearson, 2017.

WAZLAWICK, R. **Metodologia de pesquisa para ciência da computação**. 2. Ed. Rio de Janeiro: Elsevier, 2014.