INSTITUTO ENSINAR BRASIL
FACULDADES DOCTUM DE CARATINGA

RAIMYSSON HENRIQUE DE OLIVEIRA SILVA

ANÁLISE DE FERRAMENTAS LIVRES PARA RECUPERAÇÃO DE DADOS

CARATINGA
2019

INSTITUTO ENSINAR BRASIL

FACULDADES DOCTUM DE CARATINGA

RAIMYSSON HENRIQUE DE OLIVEIRA SILVA

ANÁLISE DE FERRAMENTAS LIVRES PARA RECUPERAÇÃO DE DADOS

Monografia apresentada ao Curso de Ciência da Computação das Faculdades Doctum de Caratinga, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

Área de concentração: Computação Forense

Orientador (a): Msc Fabrícia Pires Souza

DOCTUM/CARATINGA

2019

rede de ensino DOCTUM	FACULDADES DOCTUM DE CARATINGA	FORMULÁRIO 9
	TRABALHO DE CONCLUSÃO DE CURSO	
TERMO DE APROVAÇÃO		

TERMO DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado: ANÁLISE DE FERRAMENTAS LIVRE PARA RECUPERAÇÃO DE DADOS, elaborado pelo(s) aluno(s) RAIMYSSON HENRIQUE DE OLIVEIRA SILVA foi aprovado por todos os membros da Banca Examinadora e aceito pelo curso de CIÊNCIA DA COMPUTAÇÃO das FACULDADES DOCTUM DE CARATINGA, como requisito parcial da obtenção do título de

BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Caratinga 05/12/2019

FABRÍCIA PIRES
Prof. Orientador

ELIAS DE SOUZA
Prof. Avaliador 1

MAICON RIBEIRO
Prof. Examinador 2

DEDICATÓRIA

Dedico este trabalho a minha mãe Sônia Maria de Oliveira e ao meu Pai Sidnei Lima da Silva que foram minha força durante toda essa caminhada.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me permitido alcançar esse objetivo, e por sempre ter estado comigo me dado forças para enfrentar as dificuldades encontradas nessa caminhada.

Agradeço aos meus pais Sônia Maria de Oliveira e Sidnei Lima da Silva, por sempre me apoiarem e por me ensinarem o valor do trabalho e dos estudos. Muito obrigado, por acreditarem em mim.

Agradeço a minha orientadora Msc. Fabrícia Pires de Souza que foi excepcional para que esse objetivo fosse concluído, e também aos meus amigos e companheiros de turma por todo o tempo de convivência e experiência compartilhada.

Agradeço também aos professores, todos aqueles que já se foram e aos que continuam lecionando na instituição, agradeço por todo o conhecimento que foi passado, foi de grande valia para alcançar meus objetivos.

Agradeço a todos que diretamente e indiretamente tenham contribuído para que fosse possível minha chegada aqui!

LISTA DE ABREVIATURAS E SIGLAS

3GP – *Third Generation Partnership Project*

7z – *Sevenzip*

AAC – *Advanced Audio Coding*

AIFF – *Audio Interchange File Format*

AVI – *Audio Video Interleave*

BLU-RAY – *Digital Optical Disc Data Storage*

BMP – *Bitmap*

CD-ROM – *Compact Disc*

DOC – *Document*

DOCX – *Document*

DVD – *Digital Video Disc*

EXE – Executável

FLAC – *Free Lossless Audio Codec*

FLV – *Flash Video*

GIF – *Graphics Interchange Format*

GB – *Gigabyte*

GPL – *General Public License*

JPEG – *Joint Photographic Experts Group*

M4A – *MPEG-4 Audio*

MKV – *Matroska Video*

MP3 – *MPEG Layer 3*

MP4 – *MPEG Layer 4*

PDF – *Portable Document Format*

PNG – *Portable Network Graphics*

PPT – *Microsoft PowerPoint*

RAR – *Roshal Archive*

RAM – *Random Access Memory*

SQL – *Structured Query Language*

TAR – *Tape Archive*

TIF – *Tagged Image File Format*

TXT – *Text*

VM – *Virtual Machine*

VOB – *Video Object*

WMA – *Windows Media Audio*

WMV – *Windows Media Video*

XML – *Extensible Markup Language*

XLS – *Microsoft excel*

ZIP – Fechar (tradução)

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

RESUMO

Com os avanços tecnológicos, estão surgindo pessoas mal-intencionadas, que querem apossar de informações sigilosas, realizando procedimentos para roubar essas informações, para a segurar de que sejam encontrados os respectivos autores dos fatos ocorridos, os peritos forense que utilizam um conjunto de técnicas, procedimentos e conhecimentos científicos para coletar, extrair, analisar e apresentar evidências que possam ser utilizadas para julgar o autor. Sendo essencialmente a busca minuciosa com base em determinados eventos para uma investigação criminal. Durante as investigações o especialista realiza diversos exames forenses e dentre os mais requisitados destes são os realizados em dispositivos de armazenamento de dados onde uma das técnicas utilizadas nestes é a recuperação de dados. Existem várias ferramentas forenses de licença gratuita para recuperação de dados, portanto este trabalho analisou duas dessas ferramentas, concluindo qual das ferramentas foi mais eficiente no método de recuperação dos arquivos, levando em consideração o tempo de execução e a quantidade de arquivos recuperados, as ferramentas analisadas foram *Foremost* e *Photorec*. Com base nos resultados obtidos após a realização dos testes pode-se chegar à conclusão que a ferramenta *Photorec* apresentou um melhor desempenho perante os requisitos analisados, também foi analisado os resultados para determinar qual sistema operacional obteve os melhores resultados chegando à conclusão que o caine apresentou os melhores resultados.

Palavras-chave: Computação Forense. Recuperação de Arquivos e Análise de Dados.

ABSTRACT

With technological advances, malicious people are emerging who want to get hold of sensitive information, performing procedures to steal that information, to ensure that the respective perpetrators, forensic experts using a set of techniques, are found, procedures and scientific knowledge to collect, extract, analyze and present evidence that can be used to judge the author. Being essentially the thorough search based on certain events for a criminal investigation. During the investigations the specialist performs several forensic examinations and among the most requested of these are performed on data storage devices where one of the techniques used in these is data recovery. There are several free license forensics tools for data recovery, so this paper analyzed two of these tools, concluding which of the tools was the most efficient in the file recovery method, taking into account the runtime and the amount of files recovered, the tools analyzed were Foremost and Photorec. Based on the results obtained after the tests, it can be concluded that the Photorec tool presented the best performance against the analyzed requirements. The results were also analyzed to determine which operating system obtained the best results. the best results.

Keywords: Computer Forensics. File Recovery and Data Analysis.

SUMÁRIO

1 INTRUDUÇÃO

Após o surgimento dos primeiros computadores, não demorou muito para que os mesmos fossem desenvolvidos para se tornarem cada vez mais, velozes, eficientes e menores, e aumentando o uso dos mesmos na sociedade, pois ficaram mais acessíveis, deixando de serem utilizados apenas por empresas e corporações. Ao decorrer desse desenvolvimento foram surgindo, em paralelo, meios ou formas de se trocar informações de formas mais práticas e mais rápidas do que o antigo meio da época, onde se usavam cartas e tinha que esperar dias para se receber uma determinada resposta, com o aumento dessas trocas de informações, despertou em algumas pessoas o interesse de interceptá-las obtendo sem consentimento dos proprietários das informações, esse ato é considerado crime, onde o autor do crime acessa um determinado dispositivos sendo computadores, celulares, quaisquer meio de mídia, para obter as informações e salva-las, podendo envia-las ou simplesmente apaga-las, sem que o proprietário saiba ou dê a devida autorização.

Com tudo para combater esse tipo de crime, surge a computação forense que para QUEIROZ E VARGAS (2010), não define apenas em investigação, mas sim de várias metodologias para investigação e armazenamento de provas, podendo também utilizar ferramentas e conhecimentos específicos para auxiliar no procedimento. Quando se quer encontrar esses criminosos é realizado uma convocação de um perito que realiza todos os processos de perícia, onde passa coletando todas as mídias de armazenamento de dados, passando por uma extração dos dados contidos nelas, e analisando os dados obtidos para que enfim possa apresentar se de fato ocorreu esse crime.

Este trabalho consiste em analisar a eficiência de ferramentas livres, para atender os objetivos, observando qual ferramenta desenvolve o melhor tempo de execução e a quantidade de arquivos recuperados, para isso foram escolhidos os sistemas operacionais KALI e o CAINE, que visam auxiliar nos processos de recuperação, através de um vasto conjunto de ferramentas que atendem às diversas etapas das computação forense, seguindo este princípio, as ferramentas escolhidas foram a *Photorec* e *Foremost*, definido os principais equipamentos foram realizados 3 testes para cada ferramenta com o objeto de estudo em duas situações onde a primeira tratava o objeto com os arquivos apagados e o segundo tratava do objeto com os arquivos formatadas, esse processo se repete em ambos os sistemas operacionais.

2 REFERENCIAL TEÓRICO

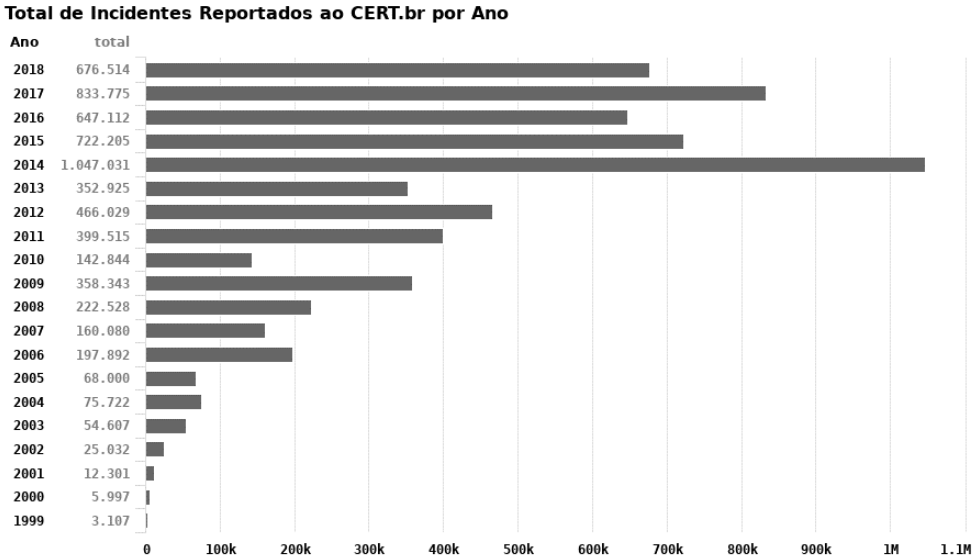
Este capítulo tem o objetivo de mostrar uma breve explicação sobre a Computação Forense, crimes cibernéticos, abordando um pouco sobre as etapas da recuperação de dados e sobre as ferramentas forense de *softwares* livres, sendo estes os tópicos principais para a realização deste estudo.

2.1 Crimes Cibernéticos

Segundo SAVEGNAGO e WOLTMANN (2015), a definição de cibercrimes ou crimes cibernéticos se diverge entre diversos autores, porém todos apontam que os crimes cibernéticos são aqueles que tem vínculo direto com a internet, e aprofundando um pouco mais relata que são cometidos no espaço virtual, alguns crimes que são mais populares de se encontrar são os de pedofilia virtual, invasão, divulgação da vida de outras pessoas e invasão de sites bancários.

O website Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) apresenta uma relação de ataques de crimes cometidos na internet, conforme demonstra o gráfico 1.

Gráfico 1 - Quantidade de crimes reportados ao Cert



Fonte: https://www.cert.br/stats/incidentes/

No gráfico 1, são apresentados a quantidade de casos reportados por ano desde 1999 até o ano de 2018, pode se observar que o maior índice de casos reportados foi durante o ano de 2014 chegando a 1.047.031 de casos reportados.

2.2 Computação Forense

O termo computação forense aparece desde os primórdios da nação, onde julgavam as pessoas pelos crimes cometidos, mas havia um problema onde o que prevalecia eram as palavras dos poderosos, por causa da falta de evidências que pudesse provar o que de fato havia acontecido.

Segundo QUEIROZ e VARGAS (2010), a computação forense é uma mesclagem de procedimentos e metodologias com a função de investigar e armazenar evidências que possam apontar se houve ou não um crime, tendo como base a análise de dispositivos como computadores pessoais, *laptops*, servidores, estações de trabalho ou outras mídias eletrônicas.

Já FARMER e VENEMA (2006), aponta que a computação forense é o recolhimento e análise de dados de forma a investigar e reconstruir as situações acontecidas no passado.

No entanto REIS e GEUS (2002) consideram que o propósito principal da computação forense consiste na extração de evidências relacionadas a um caso investigado, para que propicie conclusões sobre o desfecho do delito.

Para que possa ser possível realizar uma perícia forense é necessário ter um ambiente de trabalho, pensando nisso foram criados para alguns sistemas operacionais que possuem ferramentas voltadas para auxiliar o perito forense em seu trabalho.

Esses sistemas podem ser instalados tanto em computadores físicos ou lógicos, onde os físicos utilizam o disco rígido podendo ocupar todo o seu espaço de armazenamento, já os lógicos são instalados através de máquinas virtuais (*softwares*), que alocam parte do armazenamento do disco rígido assim como memória e processador, na seção a seguir é abordado mais detalhadamente sobre o assunto.

2.3 Máquinas Virtuais

Para poder entender sobre as máquinas virtuais ou VM (*Virtual Machine*), deve-se primeiro compreender o conceito de virtualização, que é um processo realizado pelas VMs. MATTOS (2008) aponta que a empresa IBM foi a primeira a relatar algo sobre as virtualizações, esse fato foi apresentado nos anos 60, tendo foco de realizar a virtualização de várias máquinas virtuais em apenas um único dispositivo, para redução de custos.

Para LAUREANO (2006) as máquinas virtuais são ambientes criados por um monitor VMM (*Virtual Machine Monitor*), também denominado "sistema operacional para sistemas operacionais". Onde esse monitor criar uma ou mais máquinas virtuais sobre uma única máquina real (computadores ou notebooks). Conseguindo executar no sistema operacional *Windows* uma versão do sistema operacional *Linux*.

Existem diversos softwares desenvolvidos que realizam os processos de virtualização de sistemas operacionais, alguns exemplos deles são o virtualbox e vmware. Tendo uma melhor visão sobre as máquinas virtuais, a seção a seguir abordará uma melhor explicação sobre os sistemas operacionais, mostrando quais foram escolhidos para a realização desse trabalho.

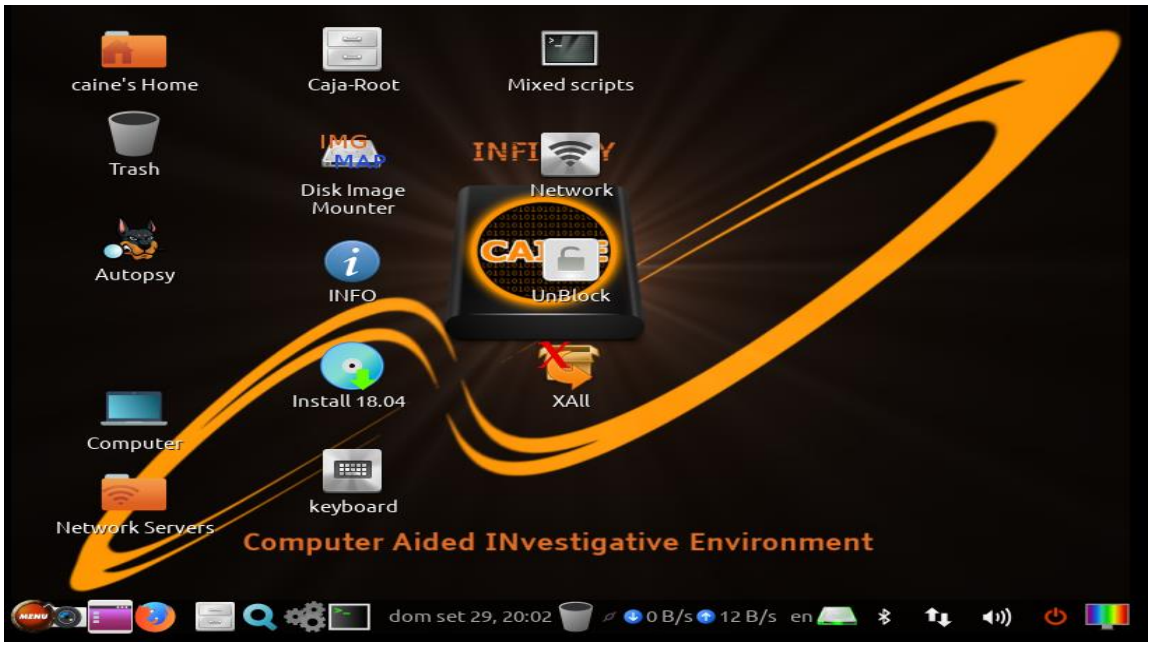
2.4 Sistemas Operacionais

Para MAZIERO (2019) um sistema de computação é constituído por *hardware* e *software*, onde o *hardware* é composto por: processador, memórias e por alguns periféricos como: teclados, mouse. Já o *software* é constituído por programas destinados aos usuários dos sistemas, que são a razão final de seu uso. Entre os aplicativos e o *hardware* reside uma camada de *software* multifacetada e complexa, denominada genericamente como Sistema Operacional. Ele é responsável pela comunicação do usuário com o *hardware*, onde ele realiza uma tradução do que o usuário quer, e envia ao *hardware* comando exigido. Tendo entendido um pouco sobre os sistemas operacionais as seções a seguir trará um detalhamento mais rico sobre os sistemas escolhidos, para a realização dos testes.

2.4.1 Caine

A seção 2.4.1 traz uma apresentação sobre o sistema operacional caine realizando um detalhamento mais aprofundado sobre o mesmo, onde a Fig. 1, demonstra sua área de trabalho.

Figura 1 - Área de trabalho do sistema operacional caine



Fonte: Autor

Esse sistema foi desenvolvido a partir do sistema operacional Linux, e segundo o website do Caine, ele é voltado especificamente para a computação forense, onde é apontado que ele apresenta um ambiente forense completo, sendo organizado para integrar ferramentas de *software* existentes como módulos, possui uma interface gráfica amigável e de fácil entendimento, esse sistema é uma distribuição do sistema Linux que tem o seu código aberto onde usuários tem livre acesso para modificá-lo.

Tendo apresentado o sistema operacional caine a seção a seguir abordará sobre o sistema operacional Kali demonstrando com melhor detalhamento o mesmo.

2.4.2 Kali

A presente seção abordará um pouco mais acerca do sistema operacional Kali, fazendo um detalhamento maior sobre o mesmo, onde a Fig. 2, apresenta sua área de trabalho.

Figura 2 - Área de trabalho sistema operacional kali

Fonte: Autor

O sistema Kali também pertence a uma distribuição do sistema operacional Linux, ele foi fundado e é mantido pela *Offensive Secutiry*. Ele é um sistema operacional voltado para área de segurança de informações, mas contém diversas ferramentas para análise forense.

Tendo obtido os conhecimentos necessários sobre os sistemas operacionais chega o momento abordar sobre as ferramentas contidas neles, a seção a seguir abordará sobre as ferramentas escolhidas dentre várias opções existentes nos sistemas operacionais apontados, trazendo um detalhamento de cada uma delas.

2.5 Ferramentas Forense

Nessa seção serão apresentadas as ferramentas forenses escolhidas para a realização do estudo, onde são detalhadas as suas características e suas principais funções.

2.5.1 Dd_Rescue

Segundo o website Gnuorg, a ferramenta realiza uma cópia de arquivos dos dispositivos como disco rígido (Hard Disc), CD's ROMs, para outros dispositivos, ela tenta recuperar esses dados primeiramente nos setores que estão em perfeito estado em caso de erros de leitura. A ferramenta não grava nada quando encontra setores defeituosos na entrada e não separa o arquivo de saída, a menos que seja solicitado. Portanto, toda vez que é executada no mesmo arquivo de saída, ele tenta preencher os espaços vazios sem eliminar os dados já resgatados. O Quadro 1 apresenta com mais clareza algumas informações que não foram apresentadas no texto, demonstrando sobre a licença que a ferramenta utiliza, o atual mantedor como a atual versão.

Quadro 1 - Especificações da ferramenta dd_rescue

DDRESCUE	
Mantedor:	Antônio Diaz Diaz
Gênero:	Recuperação de Dados
Sistema Operacional:	Linux
Linguagem de Programação:	C++
Versão Atual:	1.23
Licença:	GLP

Fonte: Autor

A próxima seção traz o detalhamento da ferramenta *Foremost*, explicando qual a função realizada por ela entre outras informações relevantes, para o estudo.

2.5.2 Foremost

Segundo o website FDTK (*Forense Digital Toolkit*) a ferramenta conta com um arquivo de configuração onde são especificados arquivos a serem recuperados. Conforme os resultados vão aparecendo, as informações coletadas são colocadas dentro da pasta output, essa pasta é criada por padrão, seu caminho e nome podem ser alterados. São criados, então, subdiretórios identificados com a extensão dos arquivos. O Quadro 2 apresenta informações sobre a ferramenta, onde demonstra quem é o atual mantedor, como a linguagem a qual foi programada, a atual versão e sobre a licença que possui.

Quadro 2 - Especificações da Ferramenta Foremost

FOREMOST	
Mantedor:	Kris Kendall e Jesse Kornblum
Gênero:	Recuperação de Dados
Sistema Operacional:	Linux
Linguagem de Programação:	C
Versão Atual:	1.5.7
Licença:	GLP

Fonte: Autor

Na seção a seguir será apresentado um detalhamento sobre a ferramenta *Photorec*, dando exemplos de quais mídias a ferramenta podem ser aplicadas.

2.5.3 Photorec

Segundo o website CgSecurity essa ferramenta é capaz de recuperar dados mesmo se o sistema de arquivos ao qual será realizada a recuperação de dados estiverem comprometidos ou danificados. A ferramenta pode ser aplicada em dispositivos como discos rígidos, CD-ROMs, cartões de memória, *Smart Media*, *Micro drives*, entre outros dispositivos de armazenamento de dados.

Quadro 3 - Especificações da ferramenta Photorec

PHOTOREC	
Mantedor:	Christophe Grenier
Gênero:	Recuperação de Dados
Sistema Operacional:	Multi-plataforma
Linguagem de Programação:	C
Versão Atual:	7.0
Licença:	GLP

Fonte: Autor

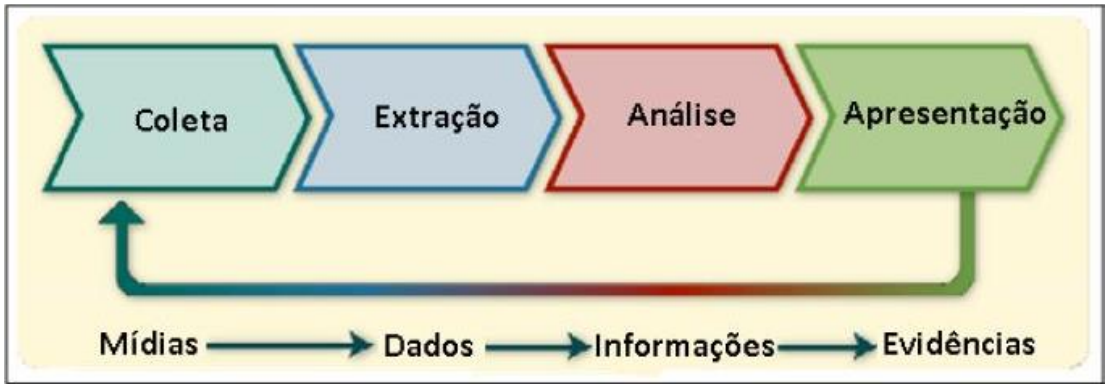
Sabendo sobre as ferramentas, é necessário ter o conhecimento das etapas da perícia forense, para então poder realizar uma, na seção a seguir são detalhadas as etapas e o que é a perícia forense para alguns autores renomeados na área da computação forense.

2.6 Perícia Forense

Para KENT (2006) a perícia forense, busca compreender um determinado evento, encontrando e analisando casos relacionados ao objeto em si analisado, para alcançar esse feito ele sugere que a perícia siga quatro etapas sendo elas a coleta, extração, analise e apresentação.

Menciona também que a perícia forense computacional não tem um procedimento padronizado de como deve ser realizada, sendo assim, o processo pode ser ajustado para a realização de uma perícia adequada às características dos dispositivos de armazenamento ao quando deseja utilizar para tal. A Fig. 3 ilustra as etapas do processo forense (KENT et al, 2006) em um contexto computacional.

Figura 3 - Etapas dos processos forenses



Fonte: Adaptação de Kent et al (2006)

A Fig. 3, apresenta o processo que deve ser seguido em uma perícia forense, onde primeiramente se deve recolher todas as mídias para realizar a análise, em seguida deve ser aplicado o método de recuperação, tendo obtido os dados das mídias é realizado uma análise para filtrar os resultados que são relevantes para que possam ser apresentados. Essas etapas são detalhadas nas seções a seguir.

2.6.1 Etapa de Coleta

A etapa de coleta trata-se da primeira etapa a qual, nas quais se realiza a coleta de fontes que contenham evidências digitais ou que possuam alguma relação acerca da investigação. É

desejável que essa etapa ocorra de forma rápida, logo após o conhecimento do incidente e siga os procedimentos que preservem a integridade do material coletado. Para KENT (et al 2006), a etapa de coleta pode ser subdividida em outras quatro etapas sendo elas a identificação, aquisição, preservação e verificação de integridade.

A etapa de identificação visa reconhecer os materiais poderão ser úteis ou necessários para a perícia, ou seja, materiais que possam conter evidências para agregar na perícia podendo ser computadores, servidores, elementos de rede, celulares e outros dispositivos de armazenamento. Já ELEUTÉRIO e MACHADO (2011) destacam que os dispositivos de armazenamento mais comuns em exames forenses são discos rígidos, CDs, DVDs, *pendrives*, cartões de memória, Blu-Rays.

Após o término da identificação dos dispositivos de armazenamento úteis para a investigação, é realizado uma aquisição (apreensão) desses materiais. É de suma importância que as características de cada dispositivo sejam observadas, e que a apreensão seja realizada com procedimentos e técnicas para garantir a integridade de todos os dados e informações (KENT et al, 2006).

ELEUTÉRIO e MACHADO (2011) aponta que os dispositivos mais comuns de apreensão possuem a característica de fragilidade, facilidade de cópia e sensibilidade ao tempo de vida e de uso. Com isso, a preservação desses dispositivos garante que as informações armazenadas permaneçam inalteradas. Assim é necessário realizar uma cópia fiel e segura dos dados contidos no dispositivo original apreendido, utilizando técnicas, equipamentos e softwares específicos.

Tendo identificado e apreendido os dispositivos, é recomendado que as fontes de dados sejam verificadas e preservadas. Para MODESTO JUNIOR e MOREIRA (2014) a verificação da integridade dos dados pode ser realizada com funções matemáticas. A segunda etapa aborda sobre a extração dos arquivos, dados ou informações, apontando uma breve explicação sobre a mesma sendo apresentada na seção a seguir.

2.6.2 Etapa de Extração

Após realizar a apreensão dos dispositivos é realizada cópias dos dados ou informações, em seguida é necessário recuperar toda a informação contida nas cópias e extrair dados úteis

para a investigação, assim sendo normal que no início da etapa de extração, exista uma grande massa de arquivos as vezes ocultos ou corrompidos para serem analisados.

Para KENT (et al 2006), um dispositivo pode conter milhares de arquivos de dados, sendo sua maioria irrelevante para a investigação em si. Levando em consideração a quantidade de arquivos irrelevantes, o perito realiza aplicação de ferramentas e técnicas para o auxiliar na filtragem dos dados que sejam importantes. ELEUTÉRIO e MACHADO (2011) relata que pode ser interessante na etapa de extração utilizar padrões de busca em textos, referenciando um nome ou assunto; filtragem por determinados tipos de arquivos, como texto ou vídeo; exclusão de arquivos desnecessários; procedimentos de recuperação de arquivos apagado. Tendo entendido sobre a etapa de extração, é chegado o momento de entender melhor sobre como é realizada a análise dos resultados obtidos, a seção a seguir apresenta exatamente isso.

2.6.3 Etapa de Análise

Para ELEUTÉRIO e MACHADO (2011), a análise consiste em realizar um exame sobre as informações extraídas do material apreendido buscando a identificação de evidências que possuam relação com a investigação. Já KENT (et al 2006), aponta que a perícia forense utiliza uma base metódica para tomar as conclusões adequadas às informações disponíveis. analisando e estudando as informações objetivando algumas conclusões como a identificação de pessoas, locais e a relação entre esses elementos.

ELEUTÉRIO e MACHADO (2011), rela que embora na etapa de extração tenha recuperado e identificado às informações mais relevantes de um determinado dispositivo, a quantidade de arquivos é um fator a ser considerado, pois em dispositivos com uma capacidade de (80GB) de armazenamento que é pequena se comparada com os demais existentes nos dias que hoje que chegam a mais de 1TB (*terabyte*), mesmo tendo realizado o processo de separação dos arquivos relevantes, pode conter muitos arquivos de dados que necessitam ser analisados manualmente, ou seja, examinando visualmente cada conteúdo. Durante a etapa de análise, é normal encontrar arquivos que contenha senhas, criptografia e esteganografia que dificulta ainda mais o processo da perícia. Para superar tais desafios, existem diversos métodos, procedimentos, técnicas e ferramentas para auxiliar nesta etapa. Continuando para agregar ainda mais os conhecimentos gerados nas seções anteriores, a seção a seguir apresenta a última etapa da perícia trata-se da apresentação das informações obtidas e analisadas.

2.6.4 Etapa de Apresentação

Essa é a etapa final da perícia, KENT (et al 2006) aponta que é necessário realizar uma documentação das evidências encontradas e apresentá-las e que deve constar neste documento os aspectos relativos às etapas anteriores como: método de coleta e extração, análise dos dados e informações assim como o valor técnico do conteúdo analisado.

Já os autores MODESTO JUNIOR e MOREIRA (2014), relata que a documentação normalmente é realizada através de um laudo técnico pericial e deve apresentar com precisão todas as ações realizadas na perícia e os resultados obtidos, pois esse laudo pode provar a ocorrência ou não do fato em investigação. Ainda continua dizendo que o laudo técnico pericial deve ser conciso; apresentando uma leitura adequada ao público, descrevendo com maior clareza os métodos, ferramentas e exames realizados durante o processo forense.

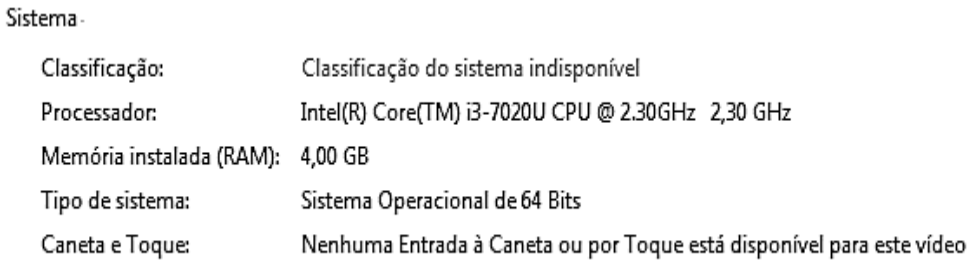
Tendo gerado conhecimento das etapas da perícia forense, das ferramentas a serem utilizadas e dos sistemas operacionais, a seção a seguir trata-se de como foi realizado o processo de recuperação para obtenção de resultados a fim de determinar qual ferramenta tem melhor desempenho para o a realização dos procedimentos forenses.

3 METODOLOGIA

Nesse capítulo serão apresentados os procedimentos realizados para chegar ao objetivo proposto, demonstrando o método utilizado para análise forense, visando a recuperação de dados e o tempo gasto, de forma a discutir os resultados obtidos e apresenta-los no próximo capítulo.

Para chegar ao objetivo proposto sendo necessário a utilização de um notebook com o sistema operacional *Windows* 7 *Ultimate* com o *Service Pack* 1 com a linguagem "português brasil" e com norma de teclado ABNT2, tendo as seguintes configurações de *hardware*, com demonstra a Fig. 4.

Figura 4 - Especificações de hardware do notebook



Fonte: Autor

Também foi utilizado um *software* de máquina virtual, onde foram virtualizados os sistemas operacionais, para que pudesse ser acessado as ferramentas, junto foi utilizado um *pendrive* da marca *SanDisk* com a capacidade de armazenamento de 4GB, foi realizado a instalação da máquina virtual Vmware, em seguida realizado as configurações dos sistemas operacionais na mesma, onde foram definidos que as configurações para cada sistema seriam as mesma para ambos sistemas operacionais, sendo então configurados com 1GB de memória RAM, com disco rígido (*Hard Disc*) de 40GB de armazenamento e com 1 processador de 2 núcleos. Realizado os procedimentos de instalação e configuração, foi necessário criar um banco de arquivos, onde a seção a seguir aborda detalhadamente os arquivos e como foi realizado a etapa.

3.1 Banco de Arquivos

Para realizar o processo de recuperação dos dados, antes de iniciar todo o processo, foi gerado um banco de dados onde foram salvos todos os arquivos, para que não sofressem nenhuma alteração indesejada, sendo possível acessá-lo através do link https://www.dropbox.com/sh/0l8wd6ekmgxo3fn/AAAWmOh7qmtPqNpoUvKXHtD_a?dl=0. Foram armazenados diversos tipos de arquivos no banco de dados, como áudios, vídeos, executáveis, imagens, também arquivos word, powerpoint, excel e pdf.

Quadro 4 - Lista dos arquivos do banco de recuperação

Tipo de Arquivos	Extenções	Quantidade
Áudio	mp3	10
	m4a	2
	ogg	2
	wma	1
	flac	2
	aiff	1
	aac	2
Vídeos	avi	1
	mp4	4
	flv	3
	mkv	2
	3gp	2
	mpg	3
	vob	3
	wmv	2
Imagens	bmp	4
	gif	4
	png	4
	jpg	5
	tif	3
Compactados	Zip	5
	Tar	4
	Rar	6
	7z	5
Executáveis	exe	20
Documentos	pdf	4
	ppt	3
	sql	3
	txt	3
	xls	4
	doc	1
	docx	2

Fonte: Autor

O Quadro 4, apresenta todos os arquivos armazenado no banco, separados por tipos como áudio ou vídeo, imagens ou documentos, e também detalhando quais suas respectivas extensões e por fim apresenta a quantidade em que cada uma possui no banco de dados.

A seção a seguir apresenta com detalhes como foi realizado o processo de recuperação dos arquivos, para cada ferramenta e para cada sistema operacional, sendo separados por estado do objeto de estudo, com arquivos excluídos e com arquivos formatados. Vale ressaltar que o tempo foi medido para identificar qual dos sistemas operacionais é mais eficiente durantes a realização dos testes e não apenas para saber qual das ferramentas pode ser mais eficientes e atender a uma perícia.

3.2 Recuperação dos arquivos

Para realizar o processo de recuperação foram definidos, dois estados para o objeto de estudo, onde no primeiro os arquivos foram excluídos (apagados) do objeto, e no segundo os o objeto foi formatado, para cada estado foram realizados 3 recuperações, e anotados os tempos gastos e a quantidade de arquivos recuperados, assim como os arquivos perdidos, visando ter uma boa base de resultados para chegar em uma conclusão mais satisfatória, esse processo foi executado para ambos os sistemas operacionais.

Dando início aos testes, após iniciar a sessão na máquina virtual do sistema Kali ou do Caine, foi realizado o *download* do banco de arquivos através do link (https://www.dropbox.com/sh/0l8wd6ekmgxo3fn/AAAWmOh7qmtPqNpoUvKXHtD_a?dl=0), na máquina virtual e ao término o arquivo foi descompactado, pois o *download* do banco de arquivos foi efetuado com formato ZIP (extensão de arquivos compactados), em seguida os arquivos foram copiados para o objeto de estudo, sendo nesse momento necessário escolher qual dos estados o objeto seria utilizado, aplicando a exclusão dos arquivos ou a formatação dos mesmos.

Os testes foram realizados de maneira alternada entre as ferramentas, e executadas primeiramente no sistema operacional Kali para depois ser executado no sistema operacional caine, sendo também separados em duas etapas onde a primeira consiste em executar o processo

de recuperação com o objeto de estudo com os arquivos apagados (excluídos) e a segunda realizada com os arquivos do objeto de estudo formatados, esses procedimentos foram apresentados nas seções a seguir.

3.1.1 Recuperação apagados

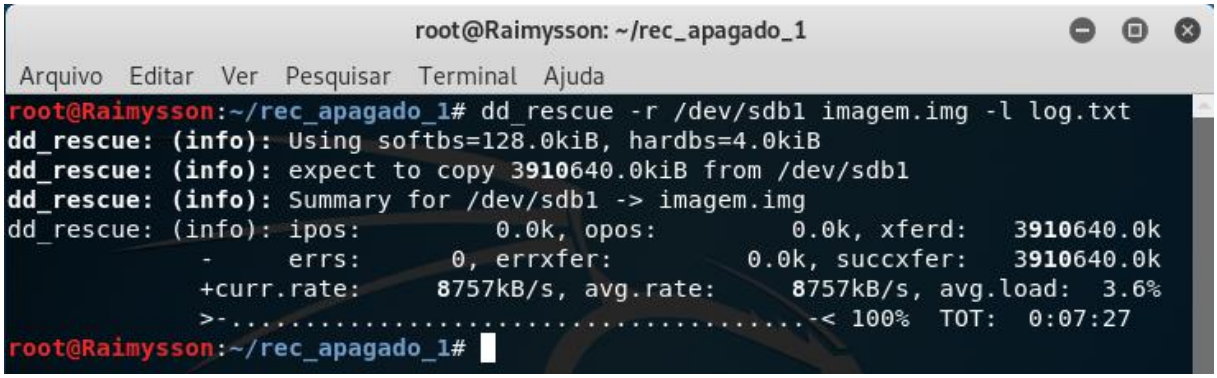
Tendo realizado o procedimento da seção 3.2, onde trata do *download* e cópia dos arquivos para o objeto de estudo, foi selecionado então o procedimento de exclusão dos arquivos para a realização dos primeiros testes com as ferramentas *Foremost* e *Photorec*, os testes foram bem similares para ambos os sistemas operacionais, por serem ferramentas que não possuem interface gráfica, foi necessário realizar os comandos via terminal, podendo ser aberto com as teclas de atalho "Ctrl+Alt_T". Para criar as pastas de armazenamento das imagens e dos arquivos recuperados, o comando "mkdir" foi executado, e junto inserido o nome da pasta desejada, foram criado as pastas "rec_apagado_" sendo diferenciadas por apenas o número final entre 1 à 6, para diferenciar os dois sistemas operacionais, sendo de 1 à 3 foram criadas para o sistema operacional Kali e de 4 à 6 foram criadas para o sistema operacional Caine. Também foram criadas as pastas "*Foremost*" e "*Photorec*" em ambos os sistemas para armazenar as pastas criadas para as recuperações separadamente, de forma que ao final das recuperações cada pasta da ferramenta tivesse três subpasta com os respectivos nomes.

Após a criação das pastas, foi executado o comando "fdisk -l", para listar as mídias de armazenamento ligadas na máquina, e observando foi encontrado o diretório "/dev/sdb1" referenciando ao objeto de estudo, em posse dessa informação, foi executado o comando "dd_rescue -r /dev/sdb1 imagem.img -l log,txt" para criar as imagens de recuperação, tendo a imagem criada, o comando "Foremost -Q imagem.img" foi executado realizando enfim o processo de recuperação, esse processo cria uma pasta "output" e armazena os arquivos recuperados dentro nela, esses passos foram realizados para a ferramenta *Foremost*.

Para a recuperação com a ferramenta *Photorec* alguns passos foram diferentes, mantendo os mesmo para a criação das pastas para o armazenamento dos arquivos e das imagens, em seguida foi executado o comando "Photorec" que realiza um chamado para a ferramenta, após abertura da ferramenta já são listados as mídias de armazenamentos disponíveis na máquina, sendo mais fácil de encontrar o objeto de estudo, pois é apresentado a

marca da mídia como se fosse o nome do mesmo, para navegar na ferramenta foi necessário utilizar o teclado, mas especificamente as setas direcionais, a tecla “Enter” e a tecla “C”, após selecionar o objeto de estudo foi necessário selecionar a pasta de armazenamento, confirmando a seleção é iniciado o processo de criação de imagem e de recuperação, a ferramenta cria uma subpasta com nome “recup_dir”, para salvar os arquivos recuperados.

Figura 5 - Criação da imagem para apagado_1 Foremost Kali



Fonte: Autor

Na Fig. 5, são apresentados os dados de criação da imagem de recuperação, no topo pode ser observado a pasta que está recebendo a imagem, pode ser observado o andamento do processo de criação, assim como quanto tempo a imagem demorou para ser criada, o tempo foi anotado para realizar a análise dos resultados posteriormente, a primeira imagem foi criada com 7 minutos e 27 segundos, e a imagem chegou aos 4GB conforme o tamanho do *pendrive*.

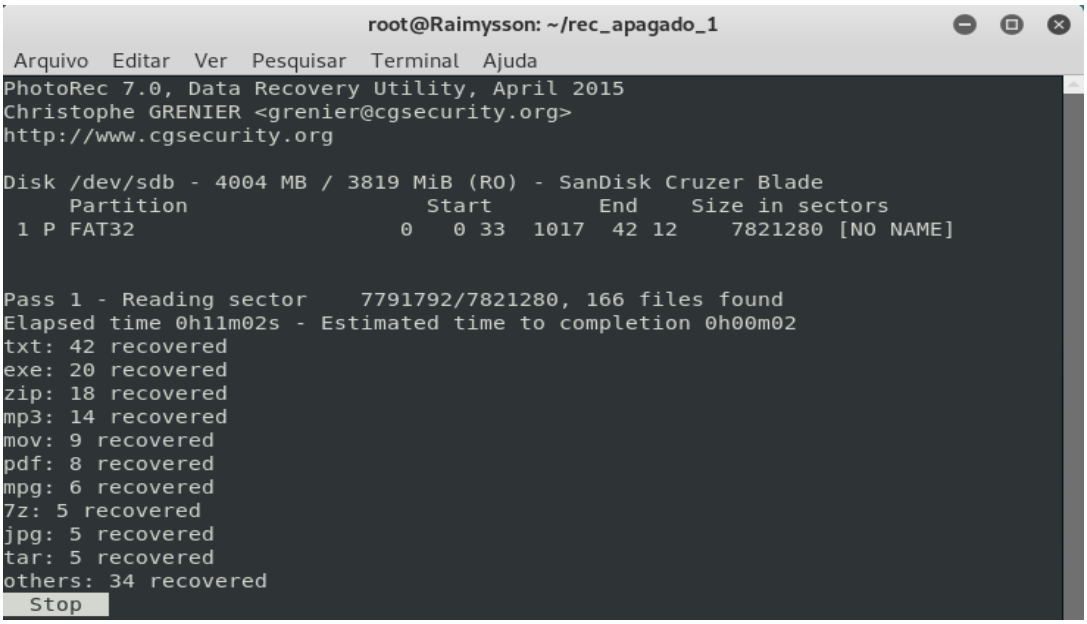
Figura 6 - Recuperação para apagado_1 Foremost Kali

Fonte: Autor

Continuando o primeiro teste, como demonstra a Fig. 6, foi chamada a ferramenta *Foremost* e solicitado a recuperação da imagem, mas é muito difícil entender o que está sendo

exibido na tela durante o procedimento, a ferramenta não retorna o tempo de execução, tendo isso em mente o tempo foi marcado em um cronômetro, e para a primeira recuperação o tempo foram gastos 3 minutos e 4 segundos.

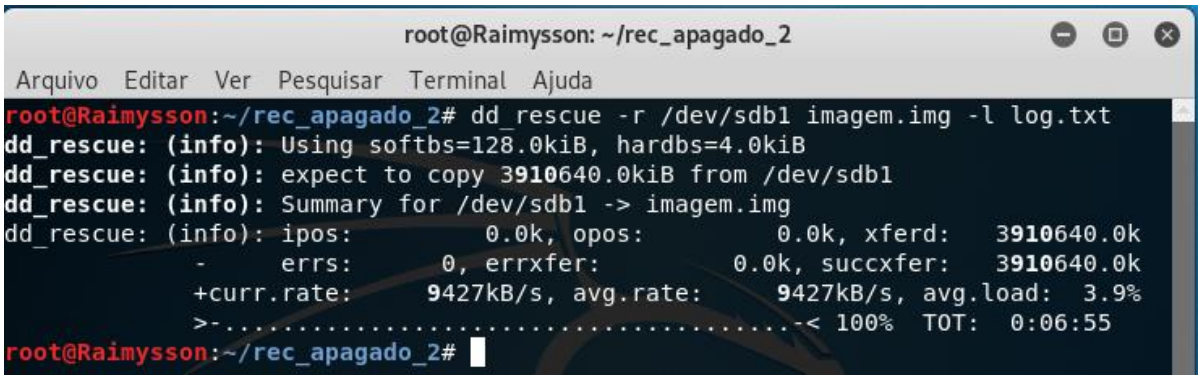
Figura 7 - Criação de imagem e recuperação apagado_1 Photorec Kali



Fonte: Autor

É possível observar na Fig. 7 que se trata da ferramenta *Photorec*, nela é possível saber pra onde estão sendo enviados os arquivos recuperados e a imagem de recuperação, a ferramenta também retorna o tempo total gasto para a realização do procedimento, levando 11 minutos e 4 segundos para criar a imagem e recuperar os arquivos, em teoria recuperando 166 arquivos.

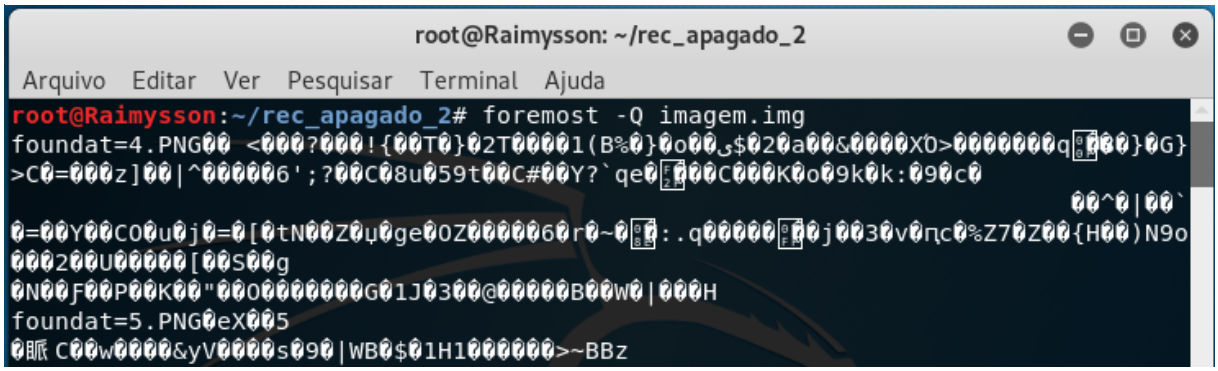
Figura 8 - Criação da imagem para apagado_2 Foremost Kali



Fonte: Autor

Continuando o procedimento do segundo teste no sistema Kali, na Fig. 8 é possível observar que a imagem foi criada na pasta “rec_apagado_2”, pois foi o segundo teste da ferramenta *Foremost* no sistema Kali, o procedimento demorou 6 minutos e 55 segundos para ser realizado.

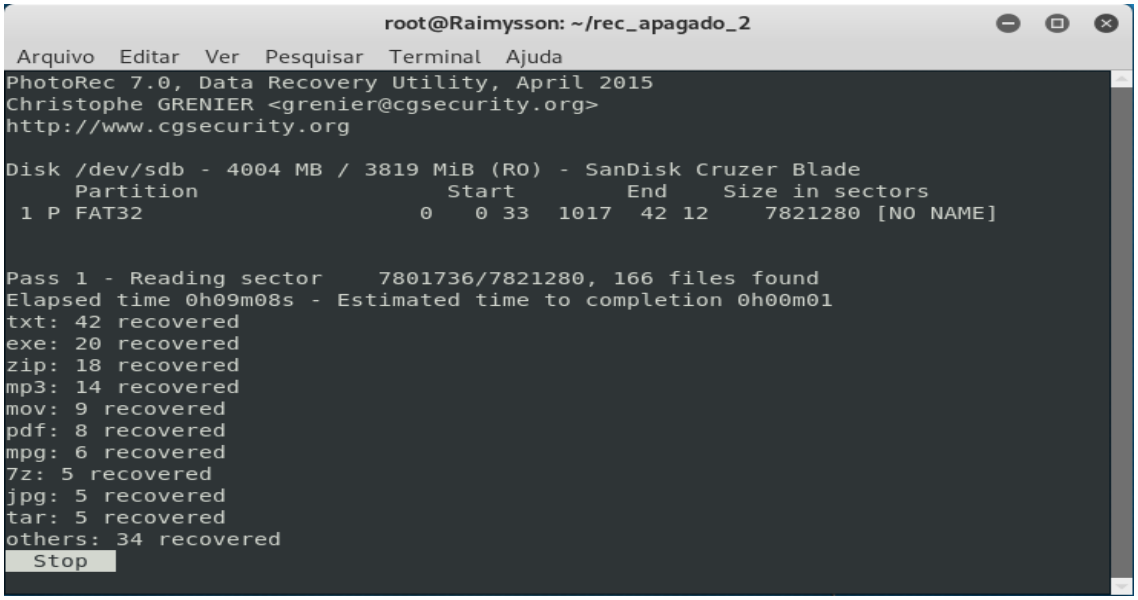
Figura 9 - Recuperando para apagado_2 Foremost Kali



Fonte: Autor

Na Fig. 9, foi realizado a recuperação dos arquivos na pasta “rec_apagado_2”, como é possível notar a ferramenta não retorna o tempo de execução, tendo cronometrado a ferramenta gastou 3 minutos na recuperação dos arquivos através da imagem criada anteriormente na Fig. 8.

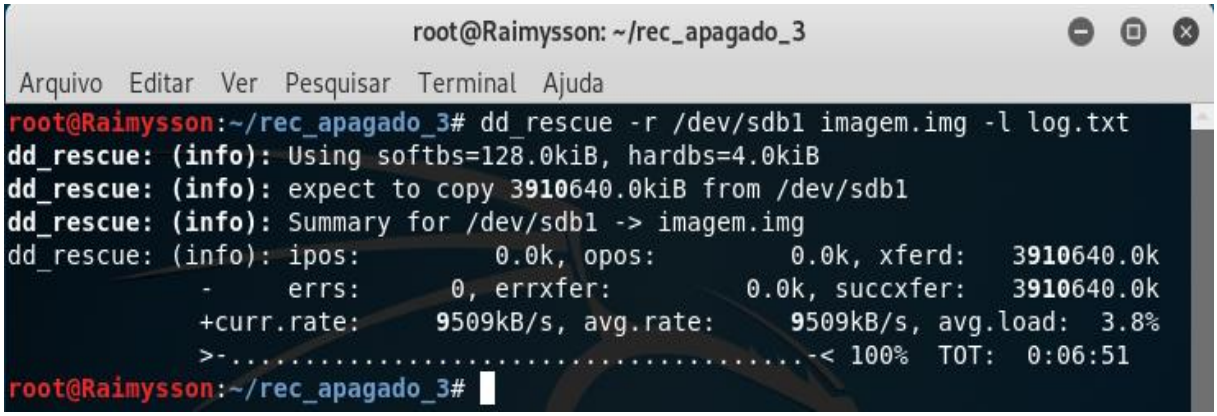
Figura 10 - Criação da imagem e recuperação apagado_2 Photorec Kali



Fonte: Autor

Na Fig. 10 é apresentado as informações do segundo teste com a ferramenta *Photorec*, criando a imagem de recuperação e a recuperação dos arquivos, o processo demorou 9 minutos e 9 segundos para finalizar o processo, recuperando em tese 166 arquivos.

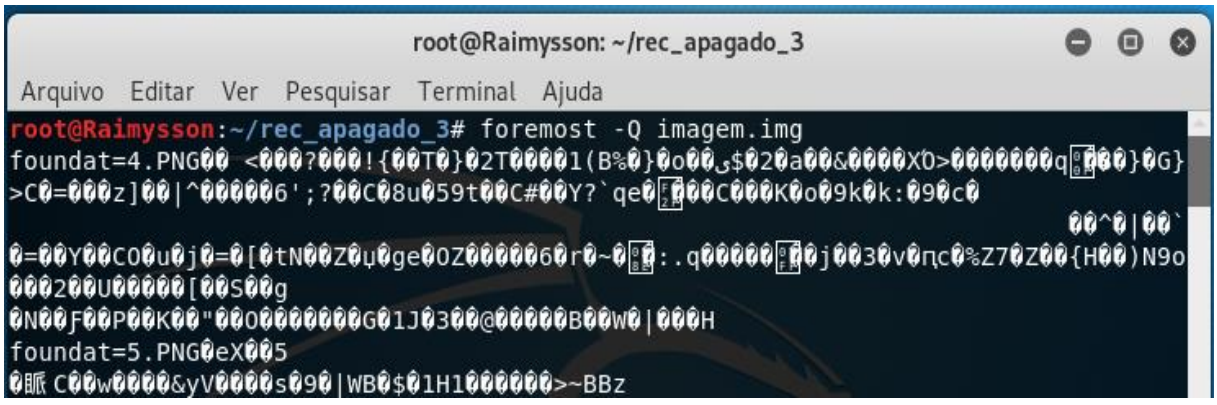
Figura 11 - Criação da imagem para apagado_3 Foremost Kali



Fonte: Autor

Na Fig.11 já é mostrado os resultados do terceiro teste com a ferramenta *Foremost* demonstrando que a imagem foi criada na terceira pasta, levando 6 minutos e 51 segundos para criar a imagem do objeto de estudo.

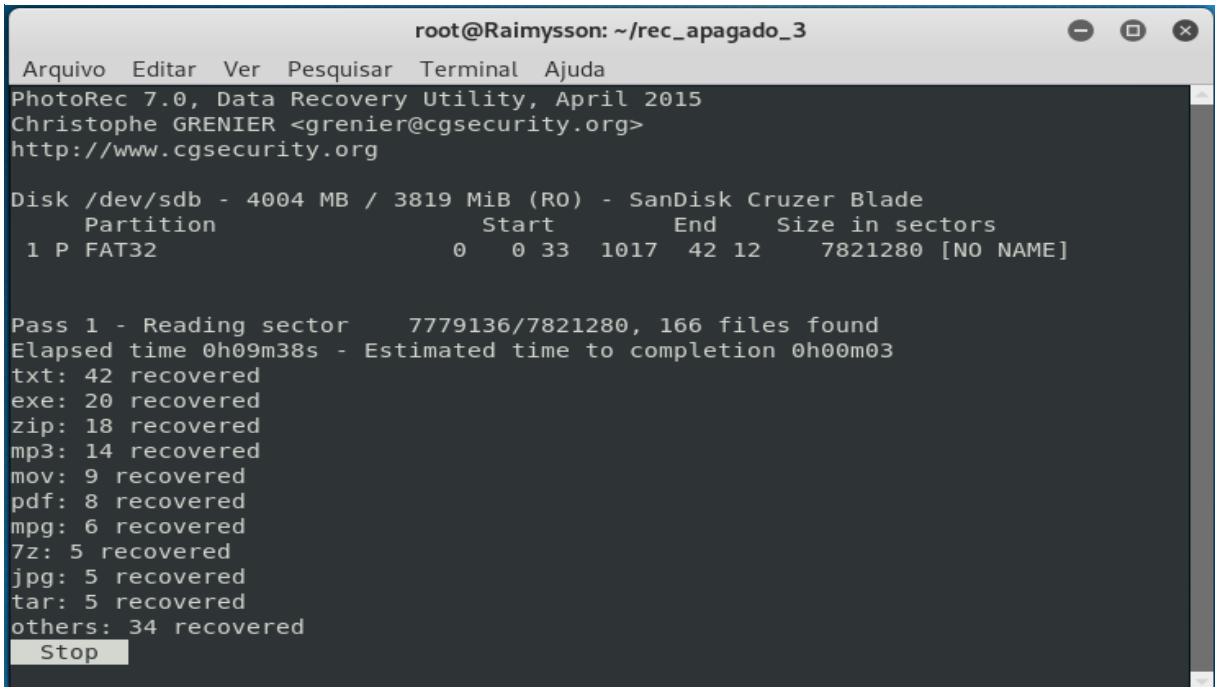
Figura 12 - Recuperando para apagado_3 Foremost Kali



Fonte: Autor

Completando a Fig. 11 a Fig. 12 realiza o processo de recuperação para o terceiro teste da ferramenta *Foremost* no sistema Kali, realizando o processo em 3 minutos e 8 segundos, por não retornar o tempo após a execução.

Figura 13 - Criação da imagem e recuperação apagado_3 Photorec Kali

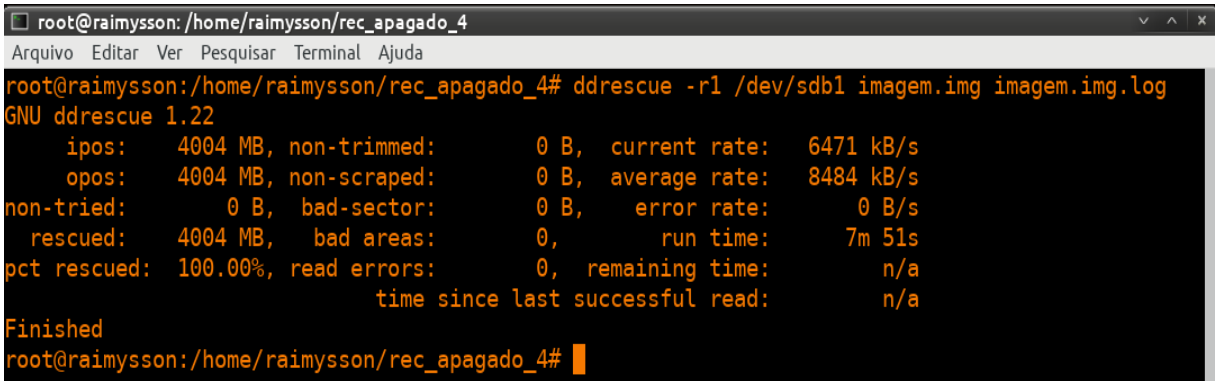


Fonte: Autor

Na Fig. 13 é apresentado o terceiro teste da ferramenta *Photorec* para o sistema operacional Kali, sendo executado com o tempo de 9 minutos e 41 segundos, recuperando em tese cerca de 166 arquivos.

A partir da Fig. 14 foram apresentados as recuperações do sistema operacional caine, e como pode ser observado na mesma, é apresentado a pasta criada para o primeiro teste da ferramenta *Foremost* no sistema, a criação de imagem demorou 7 minutos e 51 segundos para ser finalizada, e foi armazenada na pasta "rec_apagado_4".

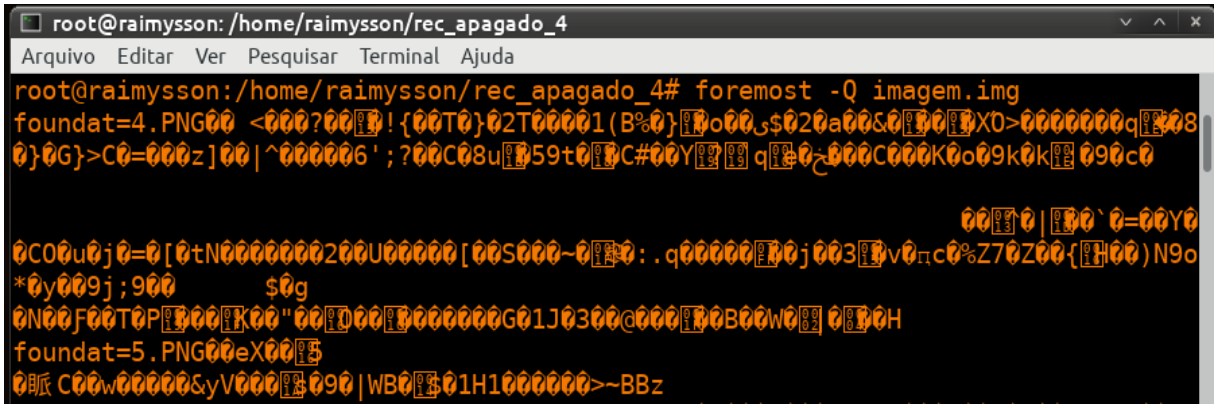
Figura 14 - Criação da imagem para apagado_4 Foremost Caine



Fonte: Autor

Dando continuidade no primeiro teste para o sistema caine com a ferramenta *Foremost* a Fig. 15 apresenta os resultados, que não são compreensíveis por se tratar da recuperação dos arquivos, no entanto é possível ver que a recuperação foi armazenada na pasta da imagem criada, a ferramenta realizou o processo em 2 minutos e 15 segundos, mesmo não tendo retornado na tela, foi possível saber realizando a marcação através de um cronômetro.

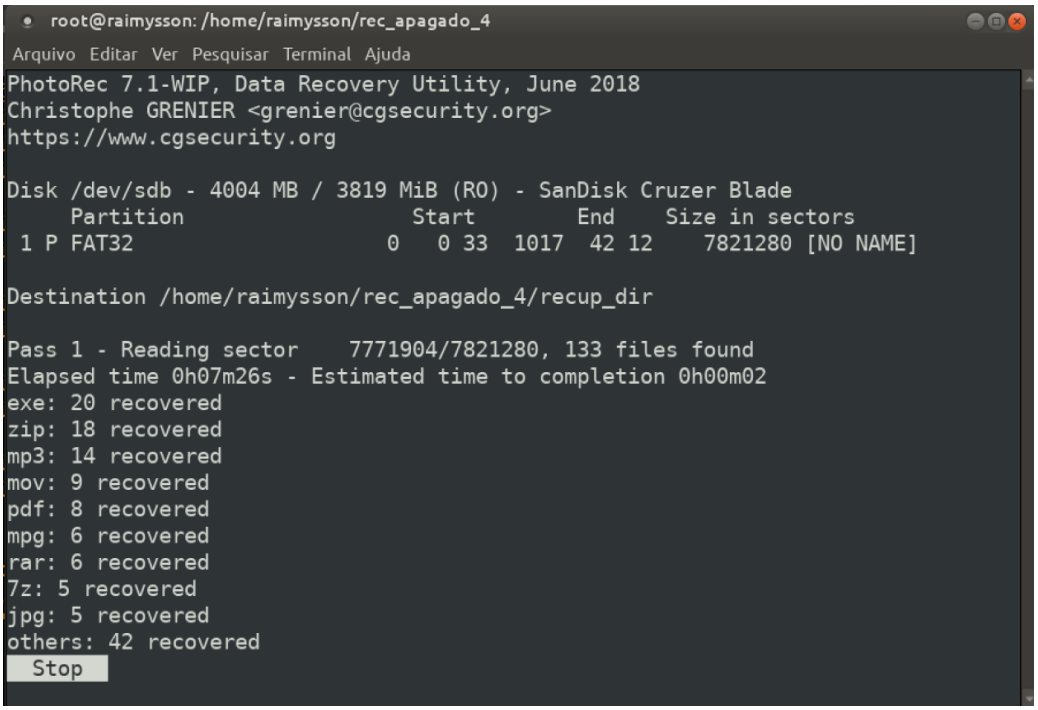
Figura 15 - Recuperação apagado_4 Foremost Caine



Fonte: Autor

Tendo terminado o primeiro teste de recuperação com a ferramenta *Foremost* no sistema caine, foi iniciado o processo com a ferramenta *Photorec*.

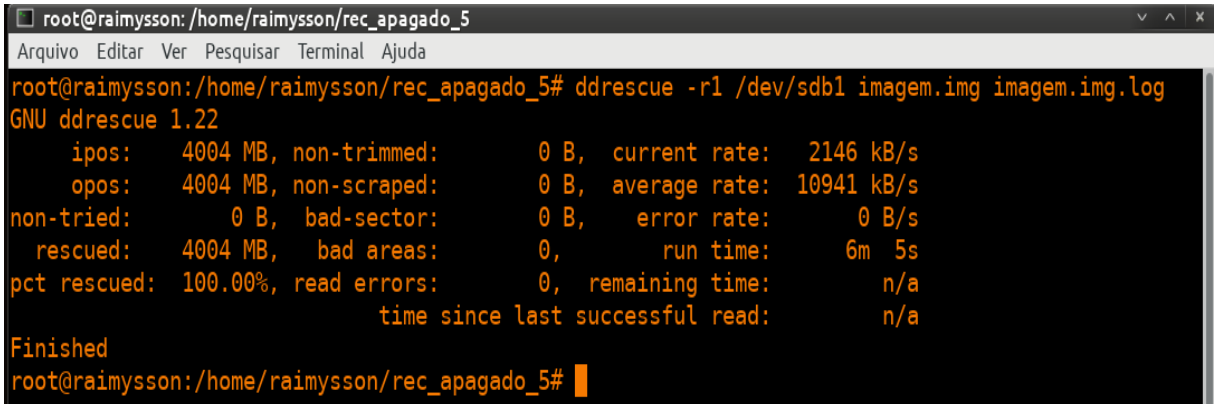
Figura 16 - Criação da imagem e recuperação para apagado_4 Photorec Caine



Fonte: Autor

Na Fig. 16 é possível observar o primeiro teste realizado com a ferramenta *Photorec* no sistema operacional caine, onde o procedimento foi executado dentro de 7 minutos e 28 segundos, recuperando em tese 133 arquivo.

Figura 17 - Criação da imagem para apagado_5 Foremost Caine

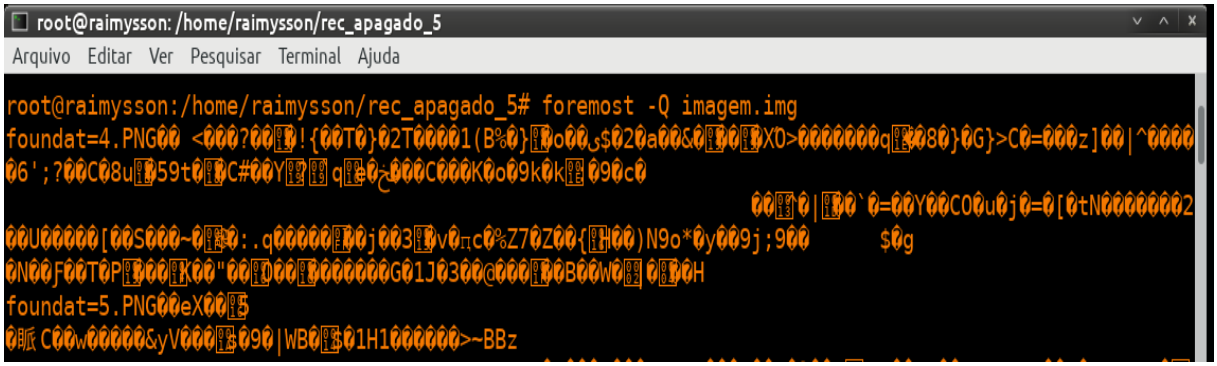


Fonte: Autor

Na Fig. 17 são apresentados o tempo de criação da imagem e a pasta a qual foi armazenada, segunda recuperação da ferramenta *Foremost*, sendo realizado em 6 minutos e 5 segundos.

Continuando a segunda recuperação após o processo de criação é possível observar na Fig. 18, o processo de recuperação com a ferramenta *Foremost*, como a ferramenta retorna o tempo de execução o mesmo foi realizado com a ajuda de um cronômetro, onde o processo foi concluído em 2 minutos e 7 segundos.

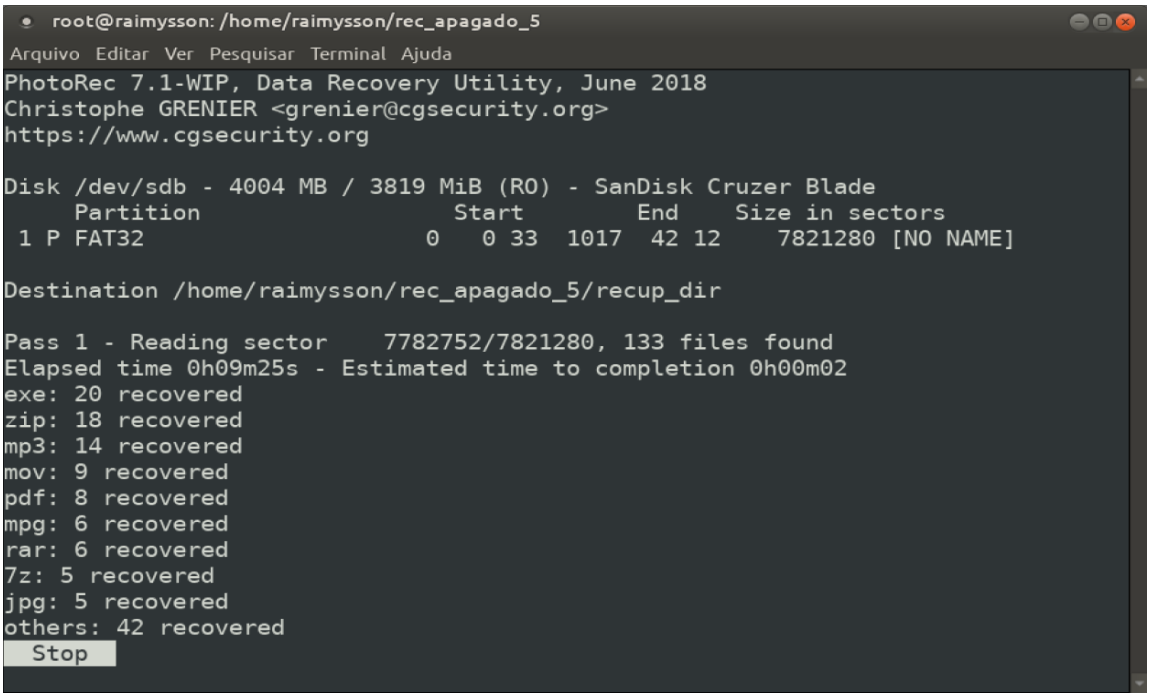
Figura 18 - Recuperação apagado_5 Foremost Caine



Fonte: Autor

Na Fig. 19, são apresentados a pasta onde foi armazenado a imagem de recuperação e os arquivos recuperados, para a segunda recuperação com a ferramenta *Photorec*, o processo foi realizado em 9 minutos e 27 segundos, recuperando em tese 133 arquivos.

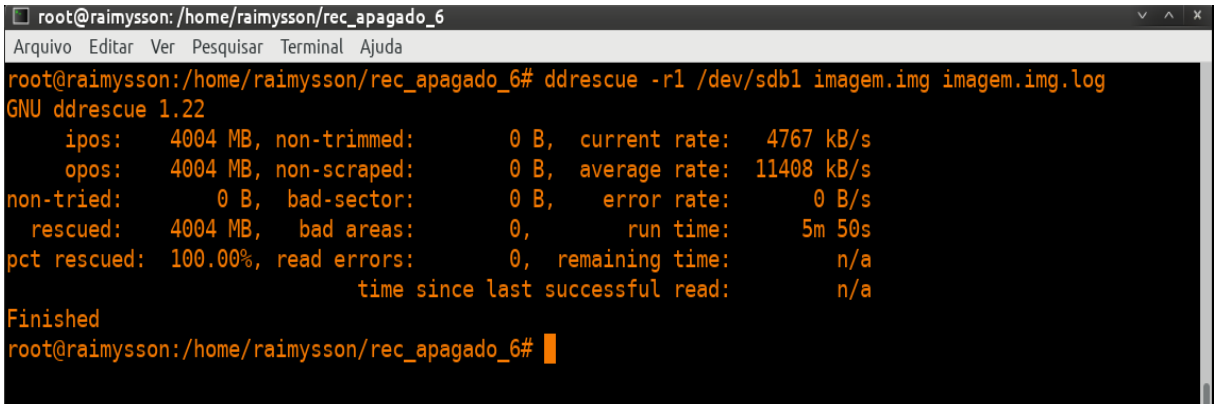
Figura 19 - Criação da imagem e recuperação apagado_5 Photorec Caine



Fonte: Autor

Na Fig. 20, são apresentados os dados de criação da imagem do terceiro e último teste de recuperação no sistema caine com o objeto de estudo com os arquivos apagados, onde o processo demorou 5 minutos e 50 segundos para a finalização.

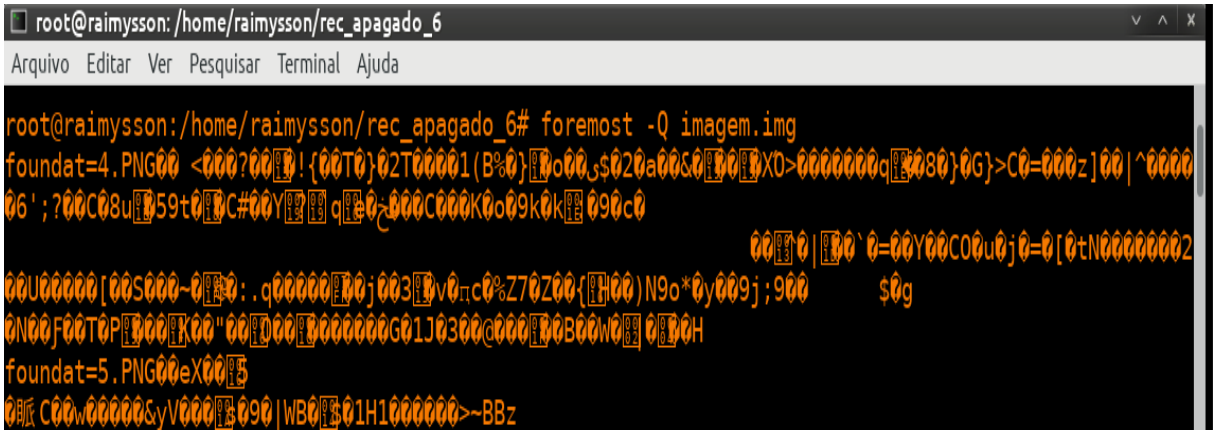
Figura 20 - Criação da imagem para apagado_6 Foremost Caine



Fonte: Autor

Continuando terceiro teste da ferramenta *Foremost*, é apresentado na Fig. 21 que a recuperação foi realizada na pasta "rec_apagado_6", sendo executado em 1 minuto e 57 segundos, sendo cronometrados pela ferramenta não retornar ao término de sua execução como é feito na criação de imagem.

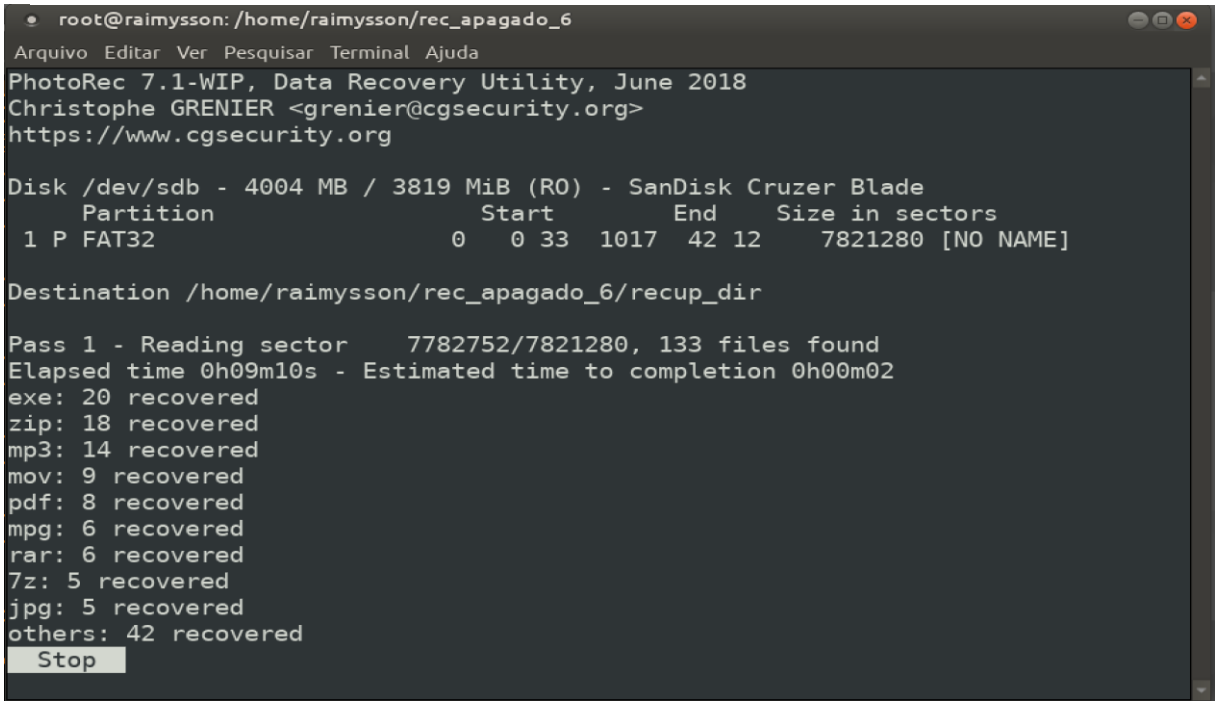
Figura 21 - Recuperação apagado_6 Foremost Caine



Fonte: Autor

Para terminar os testes com o objeto de estudo com os arquivos apagados, foi realizado o último teste com a ferramenta *Photorec*, como demonstra Fig. 22, onde o procedimento demorou 9 minutos e 12 segundos sendo salvado os arquivos na pasta “rec_apagado_6”.

Figura 22 - Criação da imagem e recuperação apagado_6 Photorec Caine



Fonte: Autor

Após a conclusão de todos os testes com o objeto de estudo com os arquivos excluídos, foram iniciados os preparativos para realizar os testes com o objeto formatado, dificultado ainda mais o processo de recuperação, a seção a seguir aborda sobre os passos realizados para consiguir esse feito.

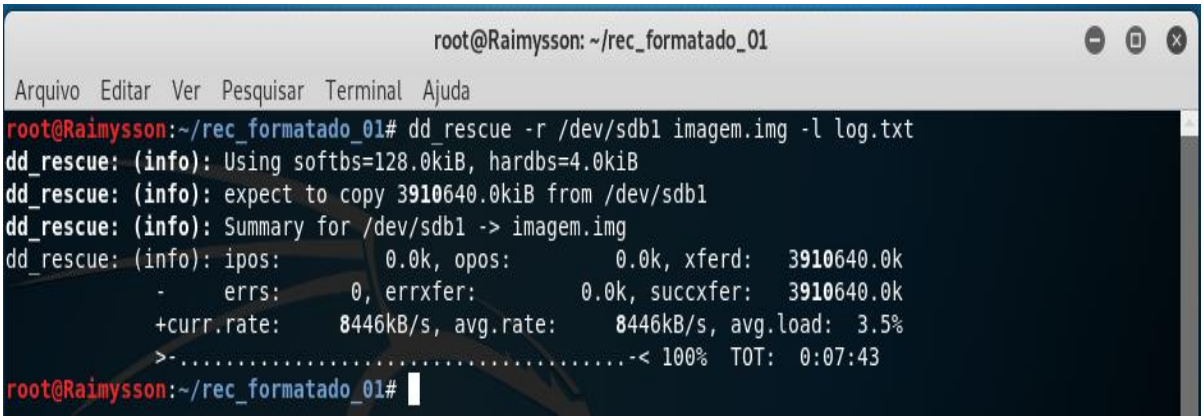
3.2.1 Recuperação formatados

Tendo executado o processo da seção 3.2, onde é realizado o *download* e a cópia dos arquivos para o objeto de estudo, foi selecionado o processo de formatação dos arquivos, para a execução dos primeiros testes com as ferramentas *Foremost* e *Photorec*, os testes foram bem similares em ambos os sistemas operacionais, por serem ferramentas que não possuem interface gráfica, os teste foram realizados através de comandos no terminal, podendo ser aberto com as teclas de atalho "Ctrl+Alt_T". Para gerar as pastas de armazenamento dos arquivos e das imagens recuperadas, foi executado o comando "mkdir", e junto o nome da pasta desejada, foram criado as pastas "rec_formatado_" sendo diferenciadas por somente o número final entre 1 à 6, onde os finais 1 à 3, estão ligados ao sistema operacional Kali, já os finais de 4 à 6 foram ligados ao sistema operacional Caine, também foram criadas as pastas "*Foremost*" e "*Photorec*" para armazenar as pastas criadas para a recuperações separadamente de forma que ao final das recuperações cada pasta da ferramenta tivessem três subpasta com os respectivos. Após a geração das pastas, foi executado o comando "fdisk -l", para listar as mídias de armazenamento ligadas na máquina, e observando foi encontrado o diretório "/dev/sdb1" referenciando ao objeto de estudo, em posse dessa informação, foi executado o comando "dd_rescue -r /dev/sdb1 imagem.img -l log,txt" para gerar as imagens de recuperação, tendo a imagem de recuperação criada, o comando "Foremost -Q imagem.img" foi executado realizando o processo de recuperação, tendo executado o comando o processo criou uma subpasta "output" armazenando os arquivos recuperados, esses trechos foram realizados para a ferramenta *Foremost*.

Para a recuperação com a ferramenta *Photorec* alguns passos foram diferentes, no entanto a criação das pastas para o armazenamento dos arquivos e das imagens foram as mesmas conforme realizado para a ferramenta *Foremost*, em seguida a ferramenta foi chamada através do comando "*Photorec*", posteriormente a ferramenta ser aberta, foram listados as mídias de armazenamentos disponíveis na máquina, na primeira interface, sendo mais fácil de descobrir o objeto de estudo, pois informa a marca da mídia como se fosse o nome, para navegar na ferramenta foi preciso usar o teclado, mas especificamente as setas direcionais, a tecla "Enter" e a tecla "C", depois de selecionar o objeto de estudo foi necessário escolher a pasta de armazenamento, confirmando a seleção foi iniciado o processo de criação de imagem e de recuperação, a ferramenta assim como o *Foremost* criou uma subpasta "recup_dir", para armazenar os arquivos recuperados. Dando início aos testes, primeiro foram realizados os testes

com o sistema Kali, para os três testes com as ferramentas *Foremost* e *Photorec*, os testes foram alternados entre as ferramentas, sendo executando em primeiro o *Foremost* e depois o *Photorec*, em seguida os testes com o sistema Caine foram realizados, também sendo alternados entre as ferramentas, os resultados foram exibidos nas imagens a seguir.

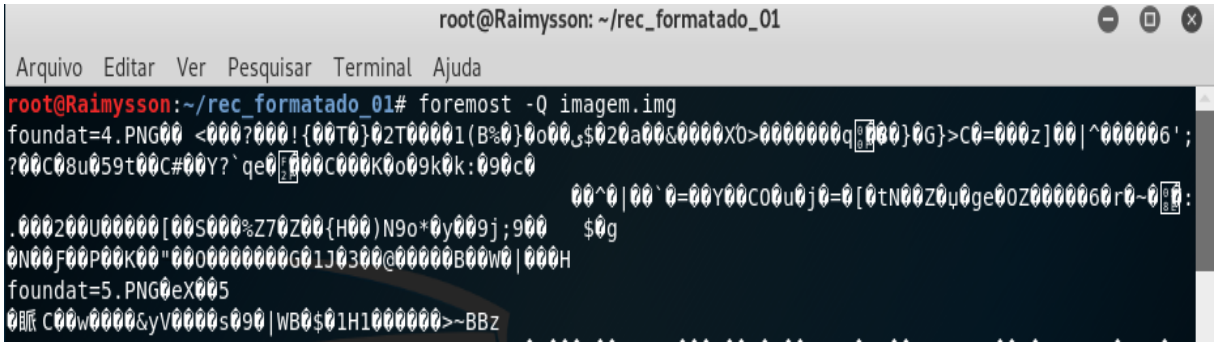
Figura 23 - Criação da imagem para formatado_1 Foremost Kali



Fonte: Autor

Na Fig. 23, são apresentados os dados da criação da imagem para o primeiro teste com a ferramenta *Foremost*, é possível observar a pasta que foi armazenada a imagem o dispositivo que foi utilizado no processo, a ferramenta conseguiu realizar a criação com 7 minutos e 43 segundos.

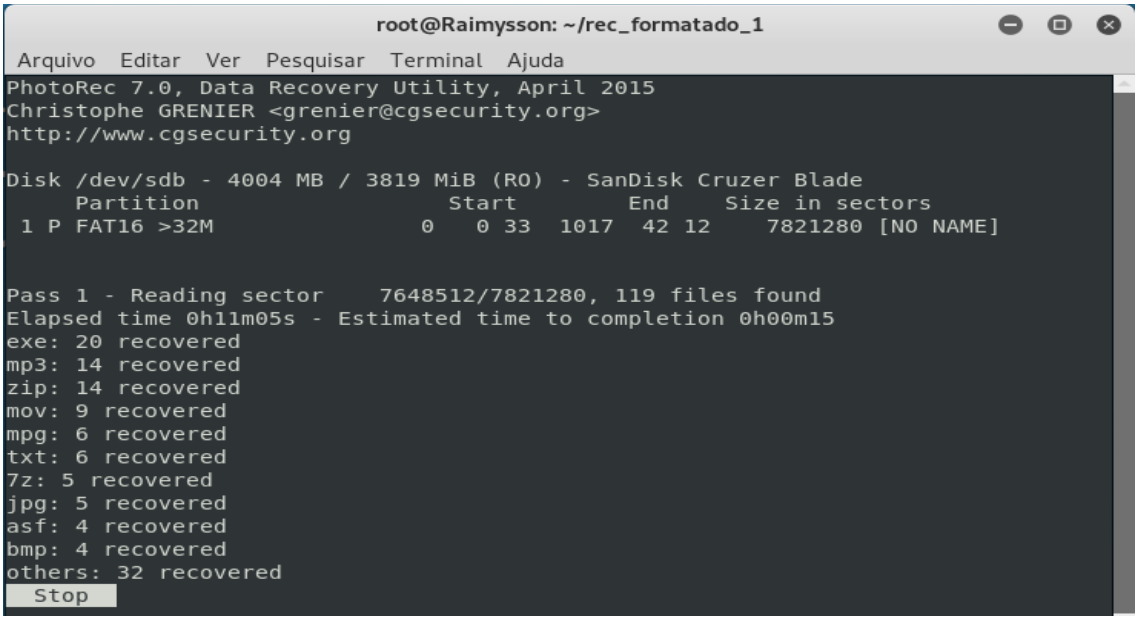
Figura 24 - Criação da imagem e recuperação formatado_1 Foremost Kali



Fonte: Autor

Continuando o primeiro teste, na Fig. 24, são apresentados a pasta que recebeu os arquivos recuperados, com a ferramenta não retorna o tempo como na Fig. 23, o tempo foi marcado através de um cronômetro, onde a o processo foi realizado com 3 minutos e 31 segundos.

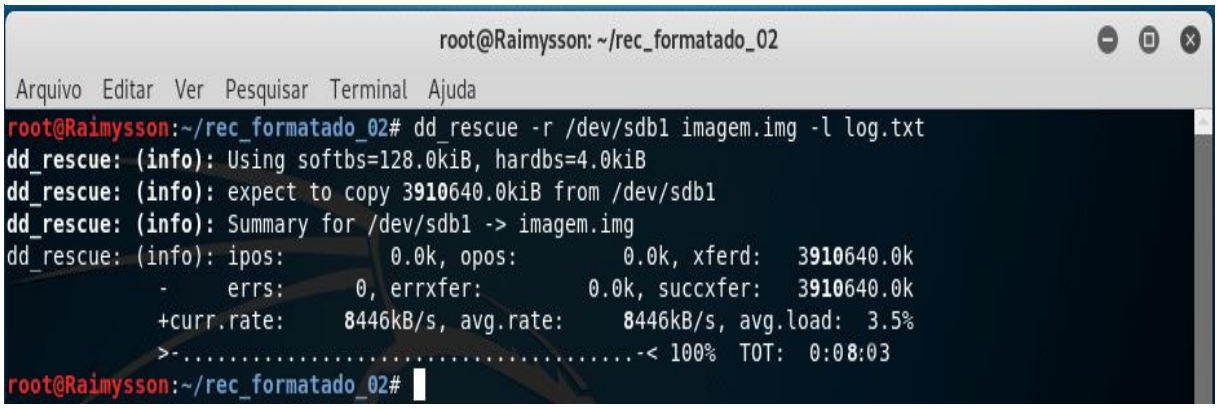
Figura 25 - Criação da imagem e recuperação formatado_1 Photorec Kali



Fonte: Autor

Na Fig. 25, são apresentados os dados do primeiro teste da ferramenta *Photorec* no sistema Kali, onde demonstra a pasta a qual os arquivos de recuperação foram salvos junto com a imagem criada, a ferramenta executou o processo em 11 minutos e 20 segundos, recuperando em tese 119 arquivos.

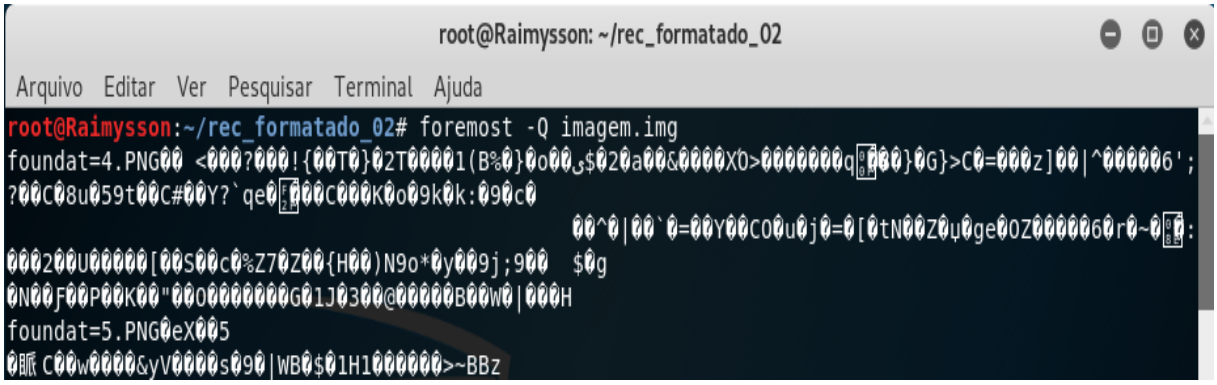
Figura 26 - Criação da imagem para formatado_2 Foremost Kali



Fonte: Autor

Na Fig. 26, são apresentados os dados da criação de imagem, para o segundo teste da ferramenta *Foremost*, é possível ver que a imagem está sendo realizada do *pendrive*, o processo foi executado em 8 minutos e 3 segundos.

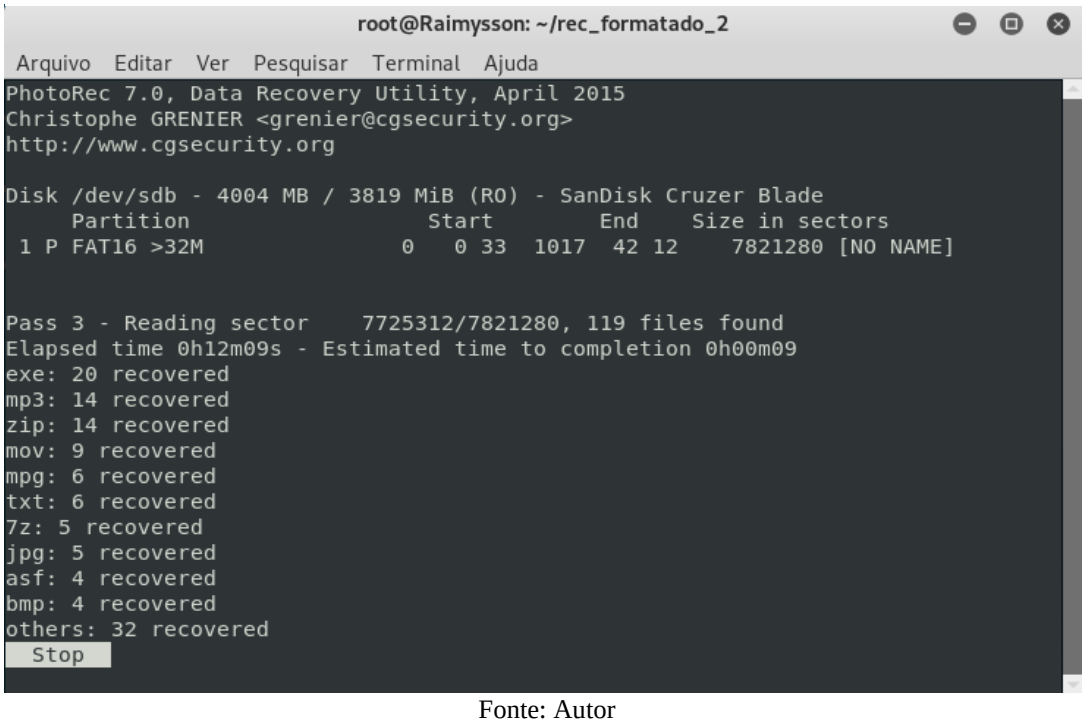
Figura 27 - Recuperação formatado_2 Foremost Kali



Fonte: Autor

Continuando o segundo teste a Fig. 35, demonstra o processo de recuperação a partir da imagem criada na Fig. 27, o processo demorou 3 minutos e 8 segundos para ser concluído, a marcação do tempo foi realizada com auxílio de um cronômetro.

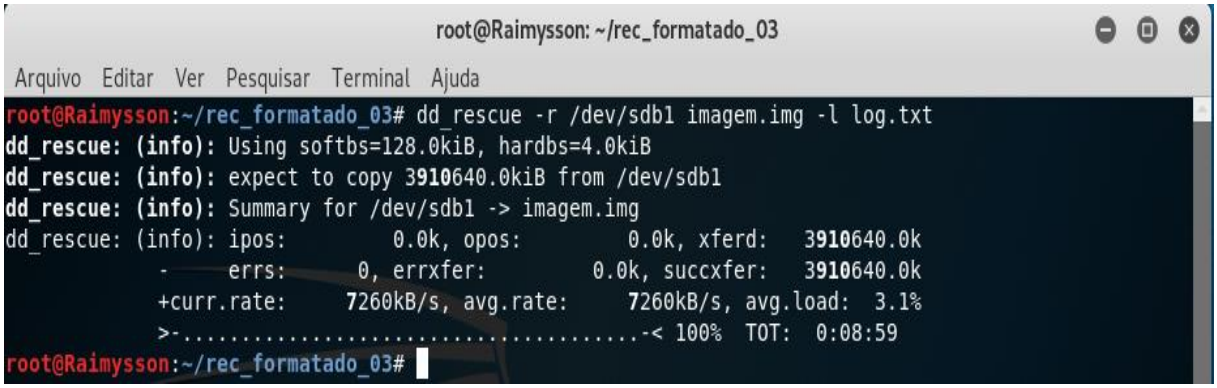
Figura 28 - Criação da imagem e recuperação formatado_2 Photorec Kali



Fonte: Autor

Na Fig. 28, são apresentados os dados da criação de imagem assim como a recuperação do segundo teste com a ferramenta *Photorec*, também é possível ver qual a mídia selecionada para ser feita a imagem, o processo foi realizado em 12 minutos e 18 segundos, recuperando em tese 119 arquivos.

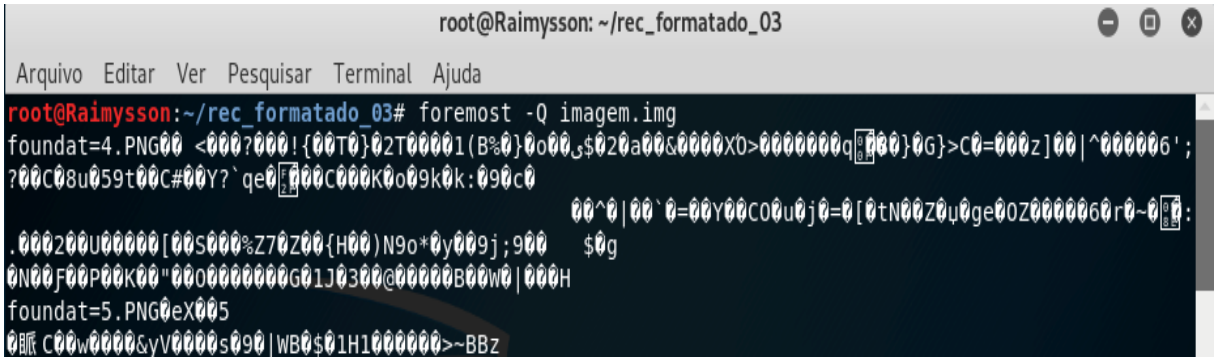
Figura 29 - Criação da imagem para formatado_3 Foremost Kali



Fonte: Autor

Na Fig. 29, são apresentados os dados de criação de imagem do objeto de estudo para o terceiro teste da ferramenta *Foremost*, o processo demorou 8 minutos e 59 segundos para ser finalizados, é possível ver que a imagem foi salva a pasta do 3 teste.

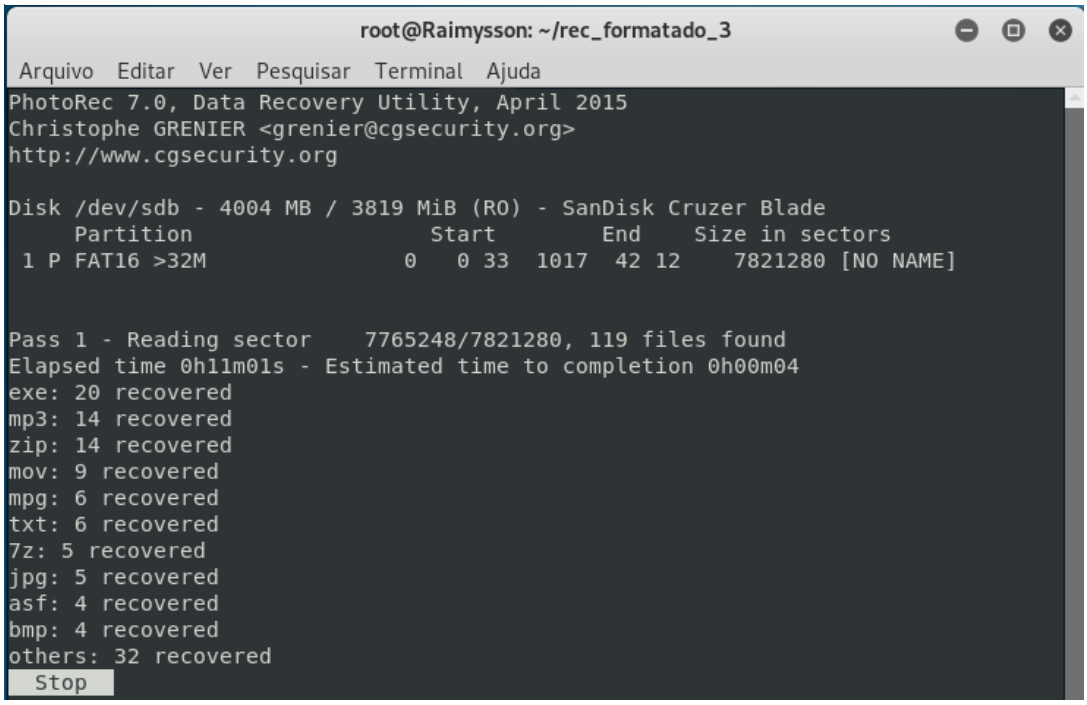
Figura 30 - Recuperação formatado_3 Foremost Kali



Fonte: Autor

Continuando o último teste da ferramenta *Foremost* no sistema Kali, a Fig. 30 demonstra a ferramenta sendo executada a realização da recuperação dos arquivos, não é possível entender o que está passando na tela durante o processo de recuperação, a ferramenta demorou 3 minutos e 8 segundos na recuperação.

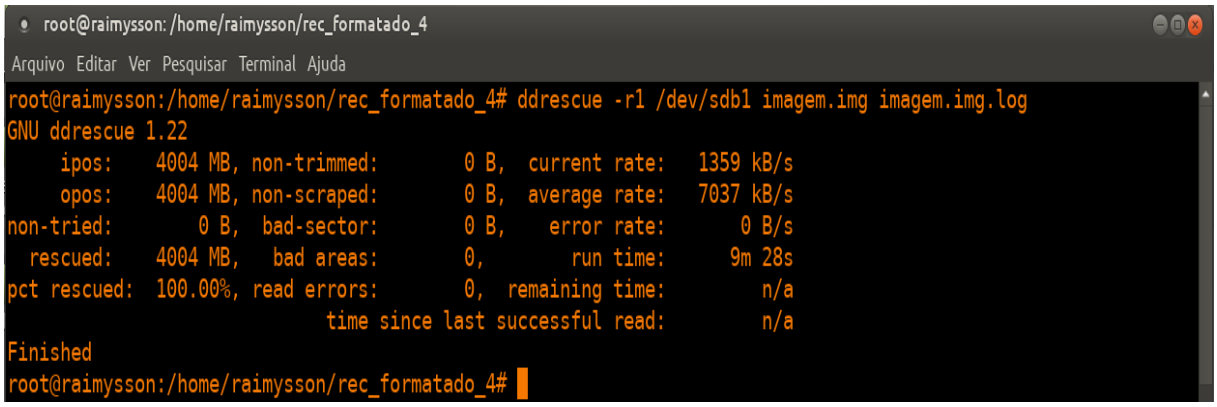
Figura 31 - Criação da imagem e recuperação formatado_3 Photorec Kali



Fonte: Autor

Como pode ser observado na Fig. 31, são apresentados os dados de criação da imagem, como também de recuperação, é possível observar que a imagem foi criada a partir do objeto de estudo, o pricedimento demorou 11 minutos e 5 segundos, e recuperou em tese 119 arquivos.

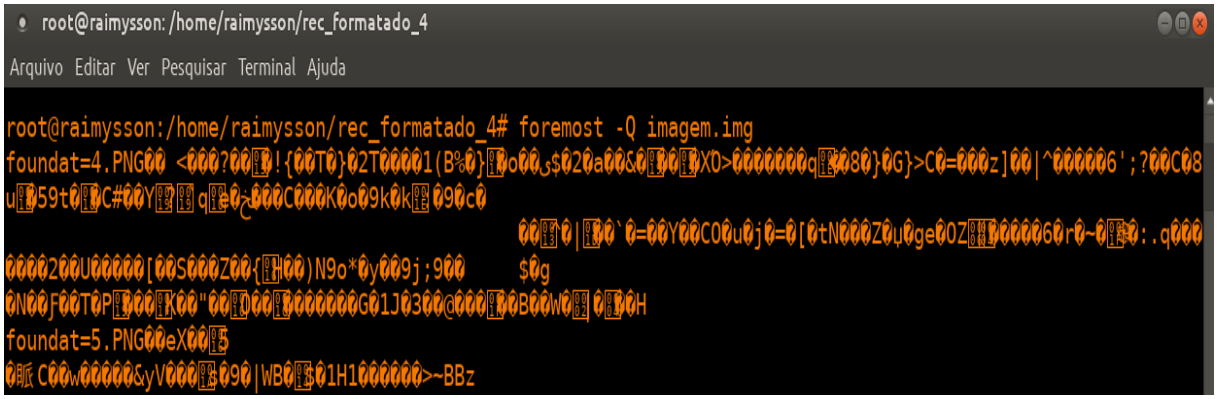
Figura 32 - Criação da imagem para formatado_4 Foremost Caine



Fonte: Autor

O primeiro teste do sistema caine foi realizado com a ferramenta *Foremost*, como pode ser observado na Fig. 32, são apresentados os dados de criação da imagem, onde o processo foi realizado em 9 minutos e 28 segundos.

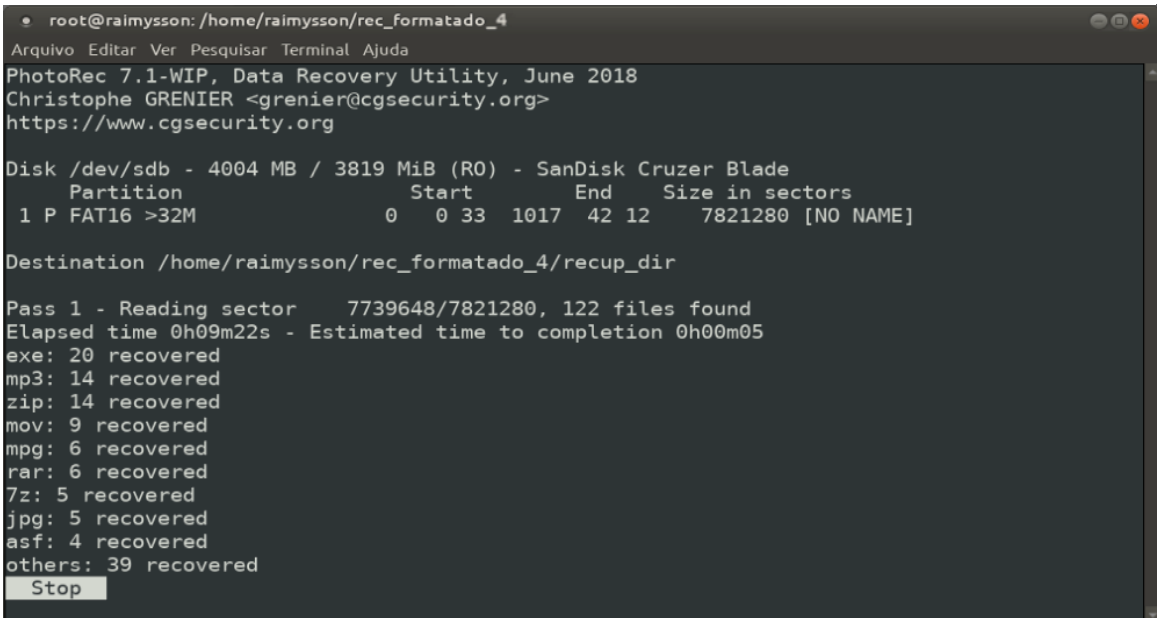
Figura 33 - Recuperação formatado_4 Foremost Caine



Fonte: Autor

Continuando o primeiro teste da ferramenta *Foremost*, na Fig. 33 é possível observar o processo de recuperação, onde o processo teve a duração de 2 minutos e 15 segundos, o tempo foi cronometrado, pois a ferramenta não retorna o tempo de execução.

Figura 34 - Criação da imagem e recuperação formatado_4 Photorec Caine

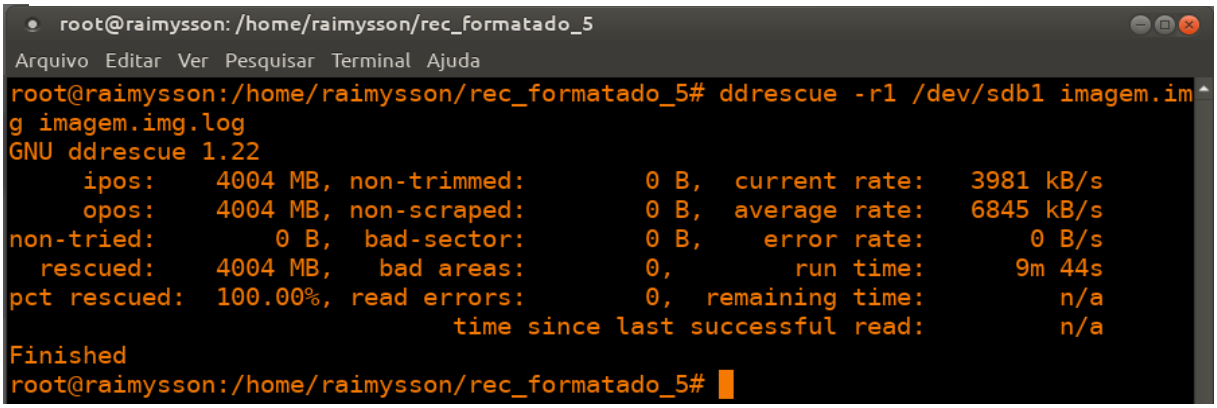


Fonte: Autor

Na Fig 34, são apresentados as informações da criação de imagem e também a recuperação dos arquivos com a ferramenta *Photorec*, onde o processo demorou 9 minutos e 27 segundos para ser concluido, recuperando em teoria 122 arquivos.

Na Fig. 35 é possível observar os dados da criação de imagem, para o segundo teste da ferramenta *Foremost*, onde o processo de execução demorou 9 minutos e 44 segundos para ser finalizado, é possível ver a pasta a qual recebe a imagem e tamém de onde essa imagem esta saindo, no caso da mídia de estudo como demonstrado no início da seção.

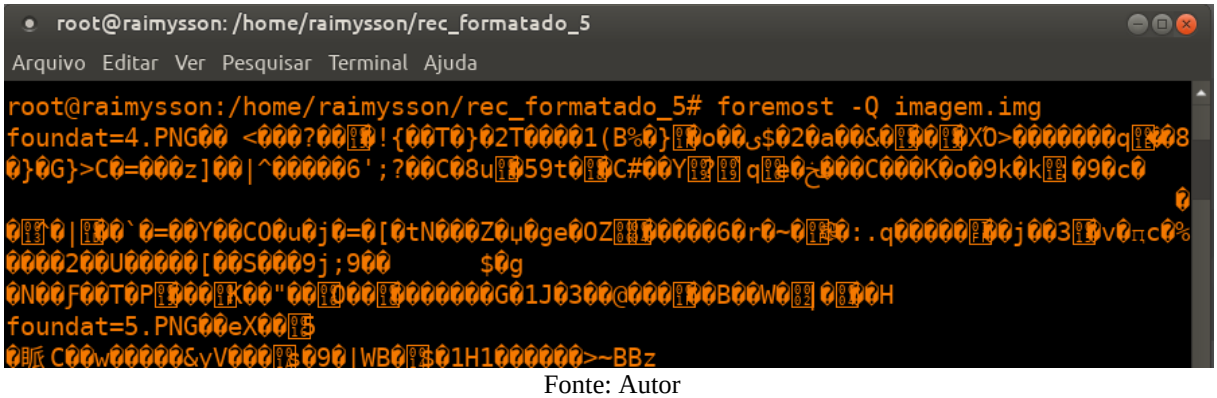
Figura 35 - Criação da imagem para formatado_5 Foremost Caine



Fonte: Autor

Continuando o segundo teste na Fig. 36, é possível observar o processo de recuperação da imagem criada na Fig. 35, o processo teve a duração de 2 minutos e 18 segundos, o processo teve o tempo cronometrado, pois a ferramenta não retorna o tempo de recuperação, e nem a quantidade de arquivos recuperados.

Figura 36 - Recuperação formatado_5 Foremost Caine

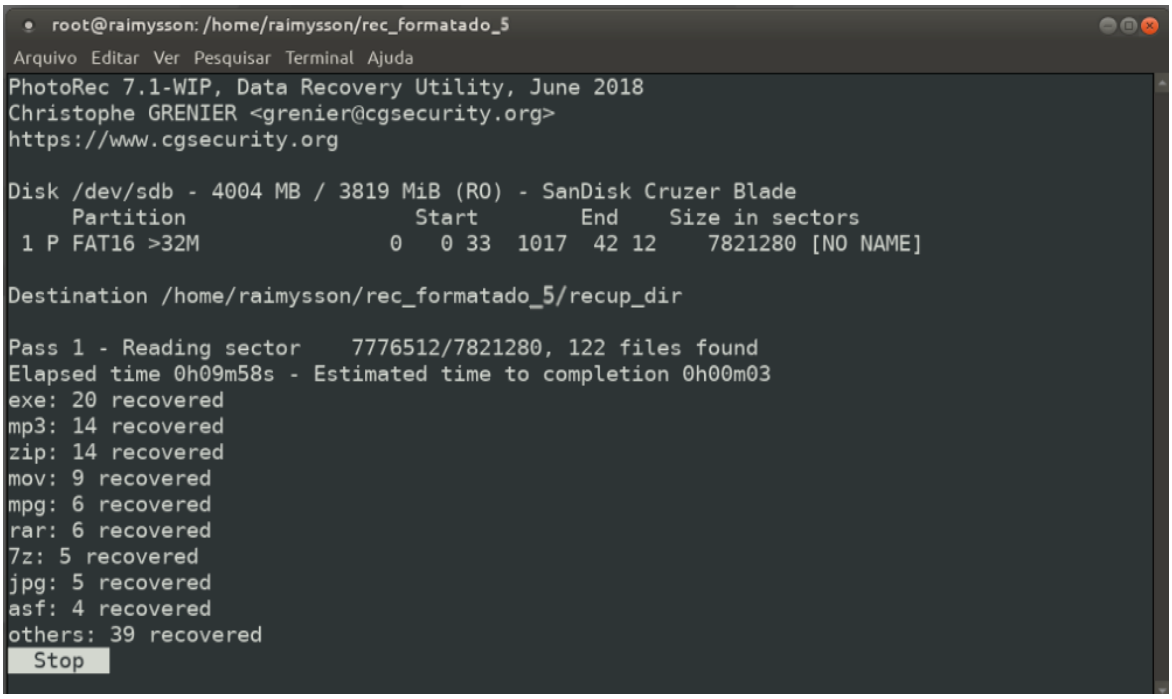


Fonte: Autor

Ao fim da recuperação com a ferramenta *Foremost*, foi iniciado o segundo teste da ferramenta *Photorec* a Fig. 37, apresenta os dados, onde foram criados a imagem do objeto de

estudo e a recuperação dos arquivos e armazenado na devida pasta, o processo foi executado em 10 minutos e 1 segundo.

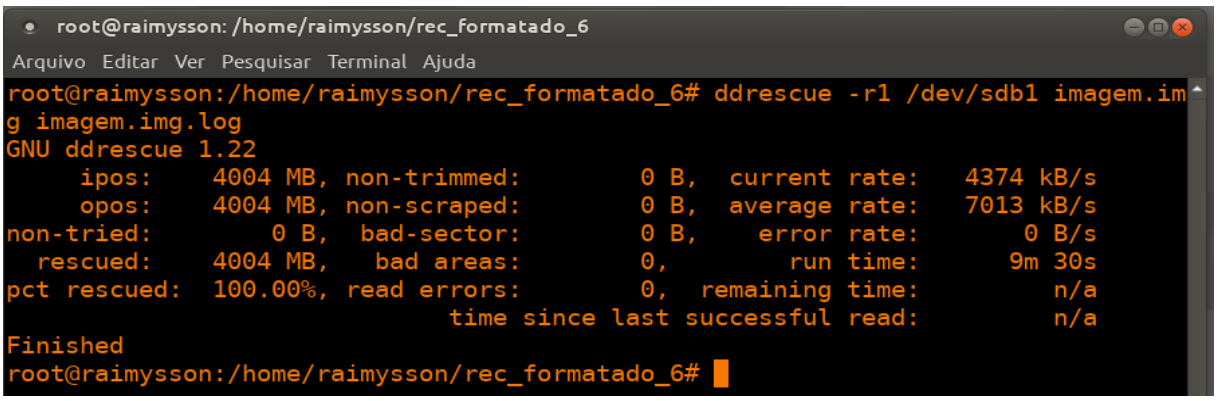
Figura 37 - Criação da imagem e recuperação formatado_5 Photorec Caine



Fonte: Autor

Na Fig. 38, são apresentados os dados o último teste com a ferramenta *Foremost*, onde foi gerado a imagem de recuperação, com tempo de execução de 9 minutos e 30 segundos, sendo armazenada na devida pasta como mencionada na seção.

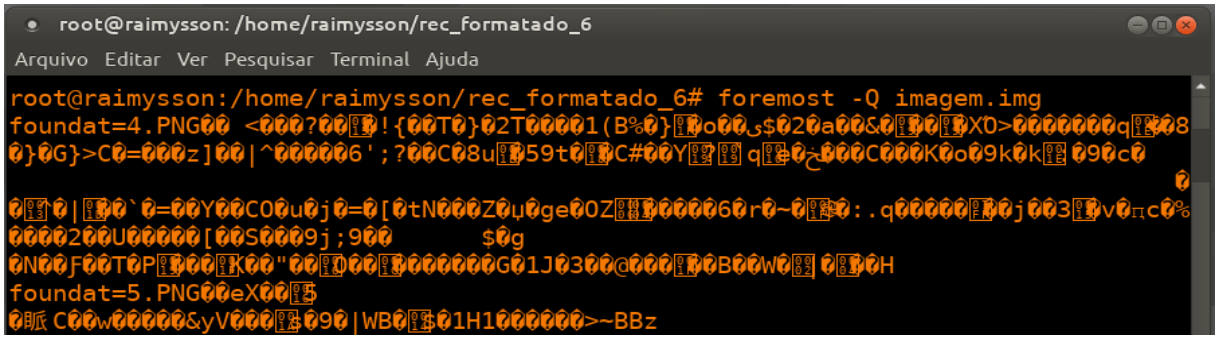
Figura 38 - Criação da imagem para formatado_6 Foremost Caine



Fonte: Autor

Continuando o último teste, a Fig. 39 demonstra o processo de recuperação dos arquivos, ondo o tempo de execução foi de 2 minutos e 11 segundos, o tempo foi medido com auxílio de um cronômetro, pois a ferramenta não retorna o tempo de execução.

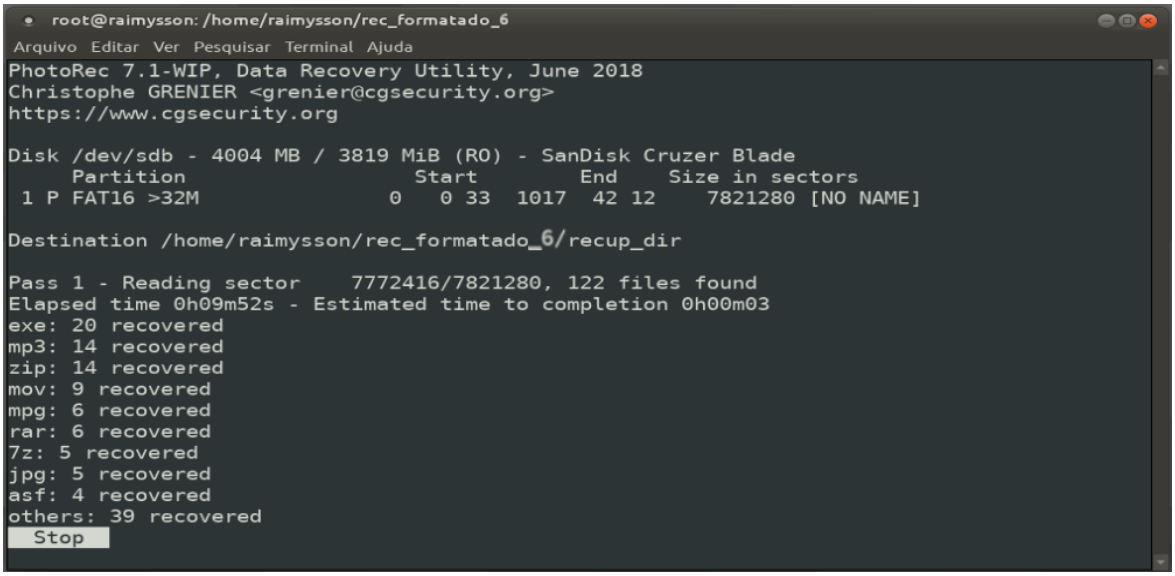
Figura 39 - Recuperação formatado_6 Foremost Caine



Fonte: Autor

Na Fig. 40, são apresentados os dados do último teste com a ferramenta *Photorec*, onde é possível observar, a criação da imagem e da recuperação de dados, o processo demorou 9 minutos e 55 segundos para ser finalizados, é possível observar que a imagem foi criada do objeto de estudo, recuperando 122 arquivos em tese.

Figura 40 - Criação da imagem e recuperação formatado_6 Photorec Caine



Fonte: Autor

Após conclusão de todos os testes, os resultados foram recolhidos, para serem analisados e apresentados no capítulo a seguir.

4 ANÁLISE DOS RESULTADOS

Esse capítulo apresentará os resultados obtidos a partir dos testes realizados com as ferramentas em cada sistema operacional, analisando detalhadamente os tempos de cada ferramenta, também a quantidade de arquivos recuperados e pôr fim a quantidade de arquivos perdidos.

Quadro 5 - Especificações dos dados obtidos dos arquivos apagados

QUANTIDADE DE ARQUIVOS UTILIZADO PARA O TESTE = 120								
RECUPERAÇÃO APAGADO								
CASO	TEMPO	FERRAMENTA	RECUPERADOS	PERDIDOS	SISTEMA	MÉDIA TEMPO	MÉDIA RECUPERADO	MÉDIA PERDIDO
rec_apagado_1	10,31	Foremost	47	73	KALI	10,22	47,00	73,00
rec_apagado_2	9,55	Foremost	47	73	KALI			
rec_apagado_3	9,59	Foremost	47	73	KALI			
rec_apagado_4	10,06	Foremost	45	75	CAINE	8,42	46,33	73,67
rec_apagado_5	8,12	Foremost	47	73	CAINE			
rec_apagado_6	7,07	Foremost	47	73	CAINE			
rec_apagado_1	11,04	Photorec	107	13	KALI	10,25	106,33	13,67
rec_apagado_2	9,09	Photorec	106	14	KALI			
rec_apagado_3	9,41	Photorec	106	14	KALI			
rec_apagado_4	7,26	Photorec	109	11	CAINE	8,55	109,00	11,00
rec_apagado_5	9,27	Photorec	109	11	CAINE			
rec_apagado_6	9,12	Photorec	109	11	CAINE			

Fonte: Autor

O Quadro 5, apresenta os resultados obtidos durante os testes com a mídia com arquivos deletados, exibindo o tempo gasto, quantidade de arquivos recuperados e quantidade dos arquivos perdidos, sendo separados pelos sistemas.

Já o Quadro 6 apresenta os resultados obtidos com a mídia de estudo formatada, apontando o tempo gasto nos processos de recuperação, também a quantidade de arquivos recuperados e os arquivos perdidos, sendo separados pelo sistema operacional e pela ferramenta, por fim apresenta as médias, calculadas para o tempo, arquivos recuperados e arquivos perdidos.

Quadro 6 - Especificações dos dados obtidos dos arquivos formatados

QUANTIDADE DE ARQUIVOS UTILIZADO PARA O TESTE = 120								
RECUPERAÇÃO FORMATADO								
CASO	TEMPO	FERRAMENTA	RECUPERADOS	PERDIDOS	SISTEMA	MÉDIA TEMPO	MÉDIA RECUPERDO	MÉDIA PERDIDO
rec_formatado_01	10,74	Foremost	43	77	KALI	11,17	45,67	74,33
rec_formatado_02	11,11	Foremost	47	73	KALI			
rec_formatado_03	11,67	Foremost	47	73	KALI			
rec_formatado_04	11,43	Foremost	49	71	CAINE	11,49	47,67	72,33
rec_formatado_05	11,62	Foremost	47	73	CAINE			
rec_formatado_06	11,41	Foremost	47	73	CAINE			
rec_formatado_01	11,20	Photorec	110	10	KALI	11,48	108,00	12,00
rec_formatado_02	12,18	Photorec	107	13	KALI			
rec_formatado_03	11,05	Photorec	107	13	KALI			
rec_formatado_04	9,27	Photorec	107	13	CAINE	10,01	109,00	11,00
rec_formatado_05	10,01	Photorec	110	10	CAINE			
rec_formatado_06	9,55	Photorec	110	10	CAINE			

Fonte: Autor

Conforme pode-se observar nas tabelas apresentadas, foram separadas em duas, onde a Tabela 1 apresenta os resultados das recuperações com objeto de estudo com os dados apagados, sendo separado pela numeração dos casos, sistema operacional e ferramentas utilizadas, para fins foram recolhidos os tempos gastos, e expostos conforme na coluna tempo, também foram expostos a quantidade de arquivos recuperados e a quantidade de arquivos perdidos, sendo que ao total foram utilizados 120 arquivos. Na Tabela 2, são apresentadas as recuperações com o objeto de estudo com os arquivos formatados, sendo separados pela numeração dos casos, sistema operacional e ferramentas utilizadas, foram expostos os tempos, os resultados de arquivos perdidos e recuperados e demonstrado nas respectivas colunas.

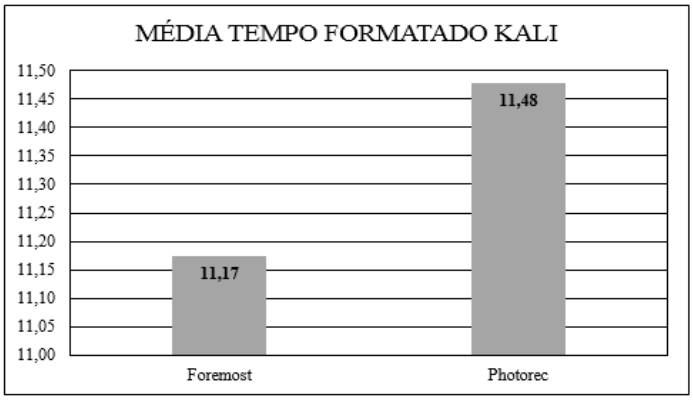
Foram medidos os tempos e analisados a quantidades de arquivos, para obter resultados que pudessem comprovar que as ferramentas em estudo, tem o potencial de serem utilizadas em perícias forenses em busca de informações que possam ajudar na decisão de um crime ou em uma sentença.

Tendo em mente os dados principais foi necessário realizar as análises dos resultados separadamente, para isso foram os mesmos foram separados e apresentados nas seções seguintes.

4.1 Análise dos tempos gastos pelas ferramentas

O Gráfico 2, apresenta a comparação das ferramentas para o sistema Kali. como o objeto formatado, podendo observar uma diferença considerável entre elas.

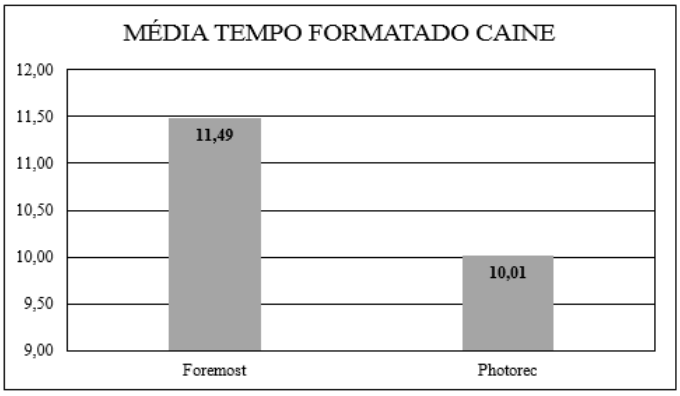
Gráfico 2 - Média do tempo gasto na recuperação com arquivos formatados no Kali



Fonte: Autor

O Gráfico 3 apresenta comparação das ferramentas no sistema operacional caine, com o objeto formatado, podendo ser observado uma diferença enorme entre elas no quesito tempo.

Gráfico 3 - Média do tempo gasto na recuperação com arquivos formatados no Caine

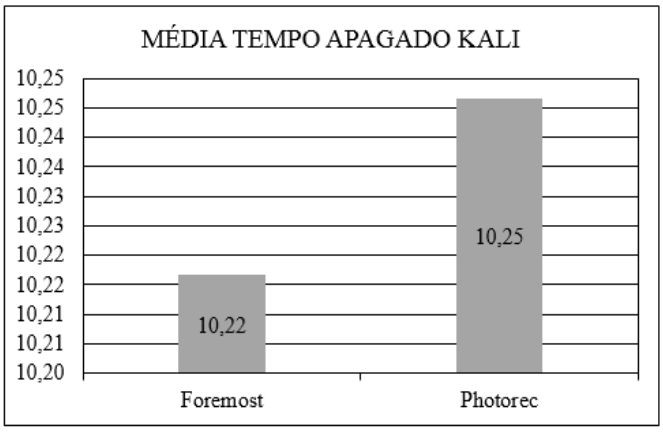


Fonte: Autor

Analisando os gráficos 2 e 3, onde foram expostas as médias dos tempos gasto pelas ferramentas na recuperação dos arquivos com a objeto de estudo devidamente formatado, neles podemos observar que as duas ferramentas tiveram uma média de desempenho acima de 10 minutos, mas

ao somar as duas médias obtidas do sistema caine e do sistema Kali, para a mesma ferramenta, pode-se observar que a ferramenta *Photorec* obteve um melhor desempenho, ficando com uma média de 21 minutos e 49 segundos, enquanto a ferramenta *Foremost* obteve uma média de 23 minutos e 06 segundos. O Gráfico 4 apresenta uma comparação das ferramentas no quesito tempo, com o objeto de estudo onde os arquivos foram deletados, para o sistema Kali.

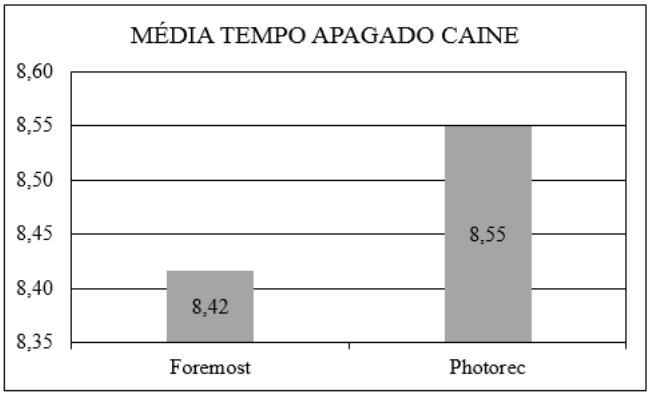
Gráfico 4 - Média do tempo gasto na recuperação com arquivos apagados no Kali



Fonte: Autor

O Gráfico 5 apresenta a média de tempo em que as ferramentas executaram os processos de recuperação com o objeto de estudo como os arquivos deletados.

Gráfico 5 - Média do tempo gasto na recuperação com arquivos apagados no Caine



Fonte: Autor

Os resultados exibidos nos gráficos 4 e 5, foram gerados a partir da recuperação de dados, onde o objeto de estudo teve os arquivos deletados, como é possível ler nos gráficos as ferramentas tiveram um desempenho semelhante em ambos os sistemas operacionais, mas ao

realizar a soma os tempos de ambas podemos observar que a ferramenta *Foremost* obteve uma média melhor onde realizou o processo com 19 minutos e 04 segundos, porém a ferramenta *Photorec* realizou o mesmo processo em 19 minutos e 20 segundos alguns segundos depois.

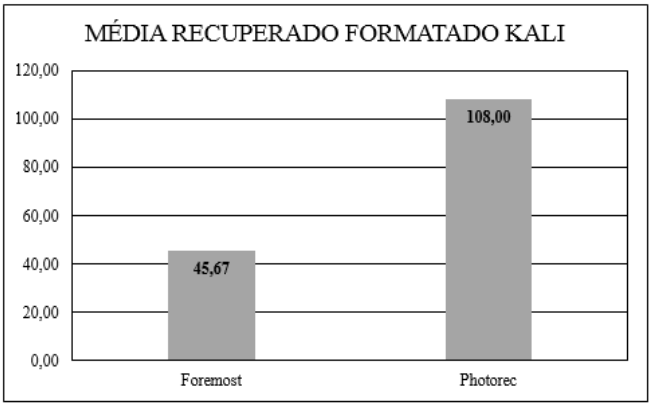
Analisando os resultados da seção 4.1, que trata do tempo de execução das ferramentas, pode-se chegar à conclusão que a ferramenta *Photorec*, executa o processo de recuperação em tempo menor quando comparado com o tempo de execução da ferramenta *Foremost*, porém a ferramenta *Photorec* demonstra um melhor desempenho no sistema operacional caine. Por fim é possível declarar que a ferramenta *Photorec*, possui um tempo de resposta melhor que a ferramenta *Foremost*, sendo mais eficiente no primeiro objetivo.

Após realizar a análise dos tempos de cada ferramenta nos sistemas operacionais, e dando continuidade foram analisados os arquivos recuperados e apresentados na seção 4.2, abordando a média geral de arquivos recuperados. Tendo analisado os resultados dos tempos, a segunda análise foi realizada dos arquivos recuperados, sendo detalhados na próxima seção.

4.2 Análise dos arquivos recuperados

No Gráfico 6, são apresentados as médias de arquivos recuperados, no sistema Kali pelas ferramentas em estudo, podendo observar qual ferramenta demonstrou melhor desempenho nos testes realizados com o objeto formatado.

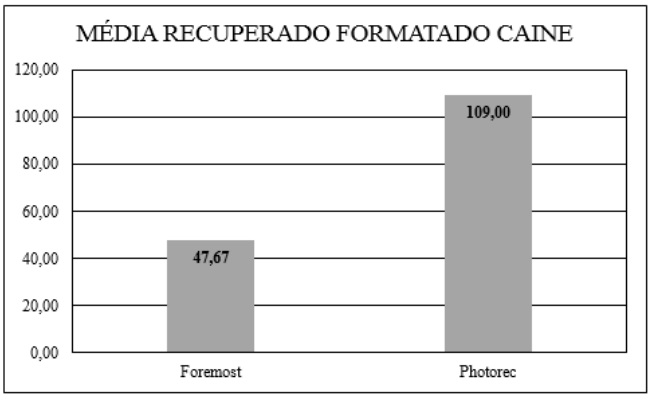
Gráfico 6 - Média de arquivos recuperados com arquivos formatados no Kali



Fonte: Autor

No Gráfico 7 são demonstrados as médias de arquivos recuperados pelas ferramentas para o sistema caine, sendo possível perceber qual ferramenta obteve um melhor resultado com o objeto formatado.

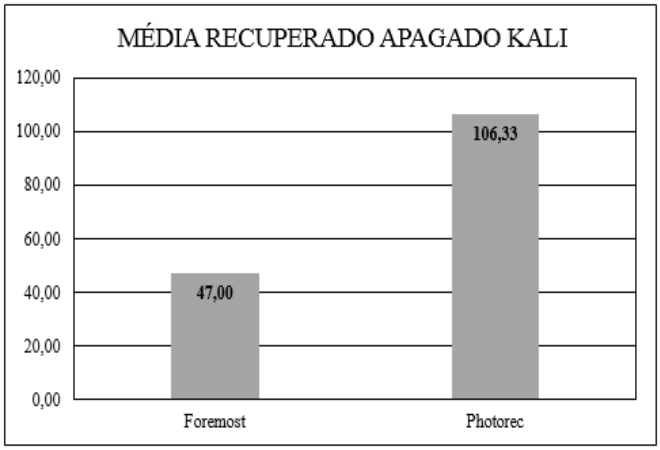
Gráfico 7 - Média de arquivos recuperados com arquivos formatados no Caine



Fonte: Autor

Como pode-se observar nos gráficos 6 e 7, onde foi aplicado a recuperação com o objeto de estudo devidamente formatado, a ferramenta *Photorec* obteve um melhor desempenho em ambos os sistemas operacionais, conseguindo sobressair a ferramenta *Foremost*, com uma média de recuperação muito superior, conseguindo recuperar em média 108 à 109 arquivos dos 120 dispostos, já a *Foremost* conseguiu recuperar em média 45 à 47 arquivos. O gráfico 8, apresenta a média de arquivos recuperados durante a recuperação dos arquivos apagados, com intuído de comprar as duas ferramentas no sistema Kali.

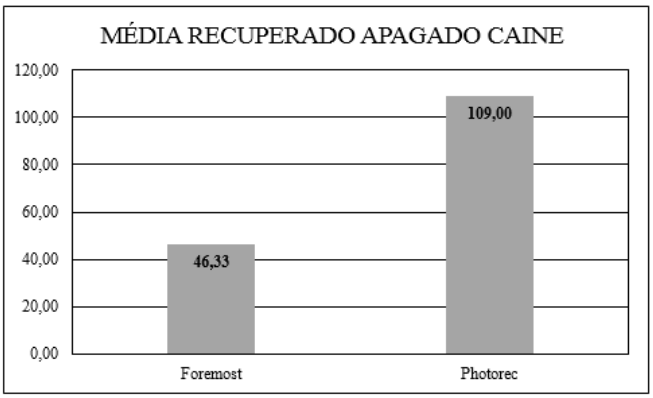
Gráfico 8 - Média de arquivos recuperados com arquivos apagados no Kali



Fonte: Autor

Já no Gráfico 9, são apresentadas as médias dos resultados obtidos da recuperação dos arquivos para comparação do desempenho das ferramentas no sistema caine, onde os arquivos estavam apagados.

Gráfico 9 - Média de arquivos recuperados com arquivos apagados no Caine



Fonte: Autor

Observando atentamente os gráficos a ferramenta *Photorec* conseguiu sobressair a ferramenta *Foremost* mais uma vez, conseguindo recuperar em média 106 a 109 arquivos dos 120 dispostos, já a ferramenta *Foremost* conseguiu recuperar em média 46 a 47 arquivos.

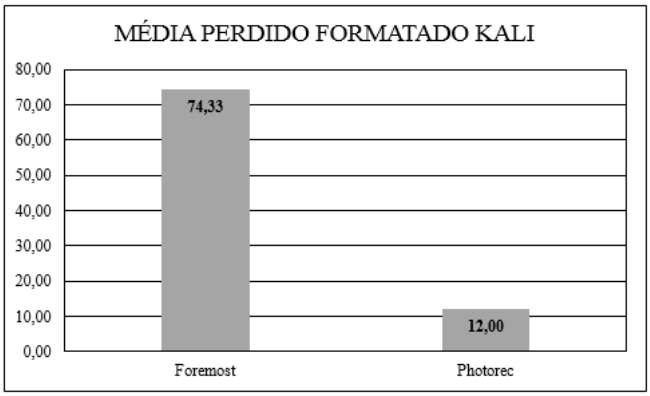
Analisando os resultados dos gráficos da seção 4.2, que trata da quantidade de arquivos recuperados, pode-se chegar à conclusão que a ferramenta *Photorec*, executa o processo de recuperação com maior eficiência comparado com a ferramenta *Foremost*, em ambos os sistemas operacionais, porém a ferramenta demonstra um melhor desempenho no sistema operacional caine. Dito isso a ferramenta que tem o melhor desempenho na recuperação de arquivos é *Photorec*, sendo superior ferramenta *Foremost*.

Ao término da análise dos arquivos recuperados, foi possível descobrir quantos arquivos foram perdidos durante os testes, e a média dos mesmos foram apresentadas na seção 4.3.

4.3 Análise dos arquivos perdidos

O Gráfico 10, exibe a média dos arquivos perdidos durante o processo de recuperação, onde a mídia de estudo teve seus arquivos formatados, realizando uma comparação entre as duas ferramentas para o sistema Kali.

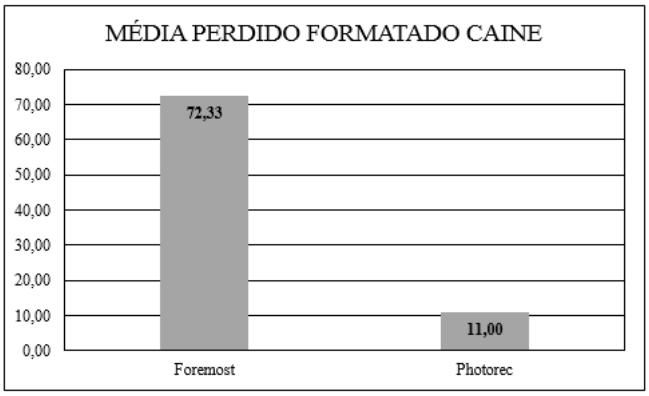
Gráfico 10 - Média de arquivos perdidos na recuperação dos arquivos formatados no



Fonte: Autor

No Gráfico 11, são apontadas as médias dos arquivos perdidos pelas ferramentas, onde a mídia teve os arquivos formatados, mostrando uma comparação entres as ferramentas no sistema caine.

Gráfico 11 - Média de arquivos perdidos na recuperação dos arquivos formatados no Caine

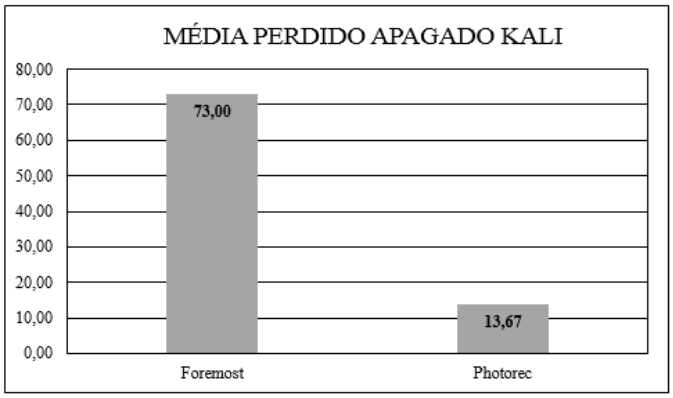


Fonte: Autor

Como pode-se observar, tanto para o sistema Kali quanto ao sistema caine a ferramenta que obteve um melhor desempenho, foi o *Photorec* que perdeu em média de 11 a 12 arquivos perdidos no processo de recuperação enquanto o *Foremost* perdeu em média 72 a 74 arquivos dos 120 dispostos.

O Gráfico 12, apresenta uma comparação dos resultados obtidos pelas ferramentas no sistema Kali durante os testes, onde os arquivos do objeto de estudo foram deletados, mostrando qual ferramenta teve um pior desempenho no momento de recuperação.

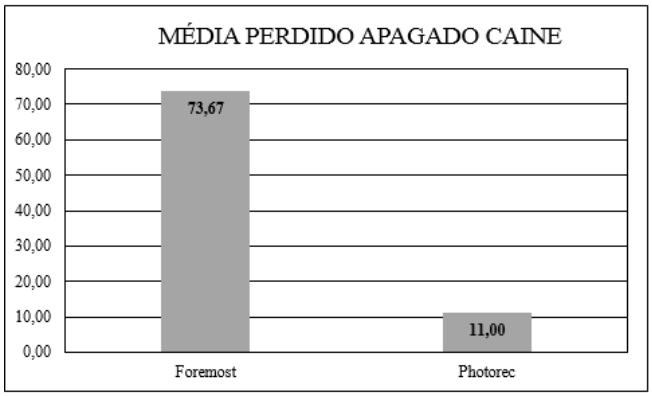
Gráfico 12 - Média de arquivos perdidos na recuperação com arquivos apagados no Kali



Fonte: Autor

No Gráfico 13, são exibidas as médias obtidas pelas ferramentas no sistema operacional caine, apontando qual ferramenta teve um pior desempenho durante a fase de recuperação dos arquivos.

Gráfico 13 - Média de arquivos perdidos na recuperação com arquivos apagados no Caine



Fonte: Autor

Nos gráficos 12 e 13, são dispostos os resultados das médias obtidas após ter realizado a recuperação no objeto de estudo com todos os arquivos deletados, podendo observar que tanto para o sistema caine quanto o sistema Kali a ferramenta *Photorec* teve um melhor desempenho, conseguindo perder durante o processo de recuperação em média 11 à 13 arquivos, enquanto o *Foremost* perdeu uma média de 73 à 74 arquivos.

Analisando os resultados da seção 4.3, que trata da quantidade de arquivos perdidos, pode chegar-se à conclusão que a ferramenta *Photorec,* tem maior eficiência em ambos os

sistemas operacionais, comparado a ferramenta *Foremost*, entre tanto a ferramenta *Photorec* demonstra um melhor desempenho no sistema operacional caine. Dito isso a ferramenta que tem o melhor é a *Photorec*, sendo superior ferramenta *Foremost*, recuperando quase todos os arquivos.

5 CONCLUSÃO

Este estudo teve como objetivo relatar sobre a computação forense e mostrar uma análise do desempenho de duas ferramentas forenses de recuperação de dados em diferentes sistemas operacionais, levando em consideração o tempo gasto por cada ferramenta e a quantidade de arquivos recuperados, assim como a quantidade de arquivos perdidos, o tempo os mesmo requisitos foram utilizado para avaliar os sistemas operacionais em paralelo com as ferramentas.

Após realizar a análise dos testes e realizar uma comparação entre eles foi possível chegar a uma conclusão acerca dos objetivos, tendo em vista que, nesse estudo foi levado em consideração os arquivos recuperados por completo, onde os arquivos corrompidos foram classificados como não recuperados, chega-se à conclusão de que entre as ferramentas *Foremost* e *Photorec*, a ferramenta que apresentou uma taxa maior de dados recuperados foi a *Photorec* tanto para com o objeto de estudo com os arquivos formatados, quanto para os arquivos apagados. Após a analisar os tempos gastos pelas ferramentas, pôde-se concluir que ferramenta com a maior eficiência, sendo 6 minutos e 3 segundos mais rápido, foi a *Photorec*, também apresentou uma qualidade em recuperação, perdendo apenas 11 arquivos dos 120 utilizados no processo.

Da mesma forma, após realizar análise e comparação dos resultados pode-se chegar à conclusão que o sistema operacional mais indicado no momento para a realização de uma perícia com as ferramentas é o sistema operacional Caine, pois ele apresenta na maioria dos resultados um desempenho superior ao sistema operacional Kali.

Sendo o mais indicado utilizar a ferramenta *Foremost* para uso domésticos, por ser uma ferramenta que demanda por mais tempo de execução e por não possuir eficiência nas recuperações em relação a ferramenta *Photorec*, que por sua vez é recomendado para o uso profissional, pois ela dá uma garantia maior de retorno e devido a necessidade de apresentar esses dados à um tribunal é de suma importância garantir a integridade dos dados. Sendo então a ferramenta *Photorec* melhor indicada para os profissionais da área forense, mostrando que as ferramentas livres também podem ser utilizadas em casos real de perícias. Por fim como trabalhos futuros, desejo continuar com esse estudo comparando outras ferramentas e também outros sistemas operacionais, realizando comparações de fermentas com a licença registradas e outra que é de licença livre, utilizando outros dispositivos como objeto de estudo.

REFERÊNCIAS

CAINE. **Computer Ferensics Linux Live Distro**. Página Inicial. Disponível em: <https://www.caine-live.net/index.html>. Acesso em: 15 de Abr. de 2019.

CERT. **CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES. Estatísticas dos incidentes reportados ao CERT.br**, ano 2018. Disponível em: <www.cert.br/stats/incidentes/>. Acesso: 15 de Mar. de 2019

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense**. SP: Novatec, 2011.

FARMER, Dan; VENEMA, Wieste. **Perícia Forense Computacional - Teoria e Prática Aplicada**. 1. Ed. BR: PRENTICE HALL BRASIL, 2006.

GNUOrg Página Inicial disponível em: <https://www.gnu.org/software/ddrescue/>. Acesso em: 07 de Dez. de 2019.

KALI. **By Ofensive Security**. Página Inicial. Disponível em: <https://www.kali.org/>. Acesso em: 28 de Mai. de 2019.

KENT. Karen, CHEVALIE, Suzanne, GRANCE, Tim, DANG, Hung, **GUIDE TO INTEGRATING FORENSIC TECHNIQUES INTO INCIDENT RESPONSE: Recomendations of the National Institute of Standards and Technology. Special publication**. Gaithersburg: NIST, 2006.

LAUREANO, Marcos. **Máquinas Virtuais e Emuladores - Conceitos, Técnicas e Aplicações.** São Paulo: Novatec, 2006. 184 p.

MATTOS, Diogo Menezes Ferrazani. **Virtualização: VMWare e Xen**. UFRJ – CENTRO DE TECNOLOGIA – DEL – 2008. Disponível em:< https://www.gta.ufrj.br/grad/08_1/virtual/artigo.pdf > Acesso em: 20 de Ago. de 2019.

MAZIERO, Carlos Alberto. **Sistemas Operacionais: Conceitos e Mecanismos**. Curitiba: Dinf - Ufpr, 2013-2019. 470 p.

MODESTO JUNIOR, Celso Carlos Navarro, MOREIRA, Jander. **Roteiro investigativo em perícia forense computacional de redes: estudo de caso**. Departamento de Computação – Universidade Federal de São Carlos: São Carlos, 2014.

QUEIROZ, Claudemir; VARGAS, Rafael. I**nvestigação e Pericia Forense Computacional: Certificações, Leis Processuais, Estudos de Caso**. Rio de Janeiro – RJ: Ed Brasport, 2010.

REIS, Marcelo Abdalla dos, GEUS, Paulo Lício de. **Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas**. Instituto de Computação - Universidade Estadual de Campinas, 2002.

SAVEGNAGO, Jéssica Uliana; WOLTMANN, Angelita. A REGULAMENTAÇÃO DOS CIBERCRIMES NO BRASIL: UMA ANÁLISE JURÍDICA DOS "TRÊS PILARES" NORTEADORES DO MARCO CIVIL DA INTERNET. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 3., 2015, Santa Maria. **Congresso iberoamericano de investigadores e docentes de direito e informática.** Santa Maria: Universidade Federal de Santa Maria, 2015. v. 1, p. 1 - 17.

SOURCEFORGE. Página Inicial: Disponível em: <https://sourceforge.net/>. Acesso em: 19 de Abr. de 2019.

SILVA, Gilson Marques, LORENS, Evandro Mário. **Extração e Análise de Dados em Memória na Perícia Forense Computacional**. Disponível em: <http://www.icofcs.org/2009/ICoFCS2009-PP03.pdf>. Acesso em: 10 de Abr. de 2019.

VMWARE Workstation Pro. Página Inicial disponível em: <https://www.vmware.com/br/products/workstation-pro.html> Acesso em: 18 de Jul. de 2019.