INSTITUTO ENSINAR BRASIL
FACULDADES DOCTUM DE CARATINGA

JOÃO PEDRO MONTEIRO CAMPOS

COMPUTAÇÃO FORENSE: ANÁLISE E COMPARAÇÃO DE DESEMPENHO DAS FERRAMENTAS FORENSIC TOOLKIT 4 E RECOVERIT 6

CARATINGA
2018

JOÃO PEDRO MONTEIRO CAMPOS
FACULDADES DOCTUM DE CARATINGA

COMPUTAÇÃO FORENSE: ANÁLISE E COMPARAÇÃO DE DESEMPENHO DAS FERRAMENTAS FORENSIC TOOLKIT 4 E RECOVERIT 6

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
30 / 11 / 2018

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: COMPUTAÇÃO FORENSE: ANÁLISE E COMPARAÇÃO DE DESEMPENHO DAS FERRAMENTAS FORENSIC TOOLKIT 4 E RECOVERIT 6, elaborado pelo(s) aluno(s) JOÃO PEDRO MONTEIRO CAMPOS 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 17/12/2018

FABRICIA PIRES
Prof. Orientador

Maicon Ribeiro
MAICON RIBEIRO
Prof. Avaliador 1

ELIAS DE SOUZA GONÇALVES
Prof. Examinador 2

DEDICATÓRIA

Dedico este trabalho a minha avó Odineia Maria Soares e ao meu avô Alcileo Mageste de Carvalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me permitido alcançar meu objetivo, e sempre ter me dado forças para enfrentar todas as dificuldades encontradas durante minha jornada.

Agradeço aos meus avós Odineia Soares e Alcileo Mageste, por sempre me apoiarem, me ensinando desde cedo o valor do trabalho e dos estudos, sempre estando ao meu lado me incentivando a sempre buscar mais. Muito obrigado, por acreditarem em mim.

Aos meus pais Jossiney Soares e Ana Paula Monteiro, por sempre me ajudarem e estarem comigo nos momentos bons e ruins, sempre me apoiando da melhor maneira possível.

Agradeço a minha madrinha Katia Couto e Alexandre Oliveira, que também foram duas pessoas que estiveram presente e acompanharam toda essa minha trajetória, 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 com a gente, agradeço por todo o conhecimento que foi passado e que ajudará a alcançar todos os meus objetivos.

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

LISTA DE ABREVIATURAS E SIGLAS

AVI- *Audio Video Interleave*

BIOS- *Basic Input / Output System*

CD- *Compact Disc*

DOC- *Document*

DVD- *Digital Video Disc*

EXE- Executável

FTK- *Forensic Toolkit*

GB- *Gigabyte*

GIF- *Graphics Interchange Format*

HD- *Hard Drive*

JPEG- *Joint Photographic Experts Group*

MP3- *MPEG Layer 3*

MP4- *MPEG Layer 4*

NTFS- *New Technology File System*

PDF- *Portable Document Format*

PNG- *Portable Network Graphics*

RMVB- *Real Media Variable Bitrate*

RTF- *Rich Text Format*

SO- Sistema Operational

TXT- *Text*

USB- *Universal Serial Bus*

WMA- *Windows Media Audio*

WMV- *Windows Media Video*

XML- *Extensible Markup Language*

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE GRÁFICOS

RESUMO

A computação forense pode ser definida como um conjunto de técnicas e procedimentos que utilizam conhecimento científico para coletar, analisar e apresentar evidências que possam ser utilizadas em um tribunal. Sendo essencialmente a busca minuciosa com base em determinados eventos para uma investigação criminal. Durante as investigações o perito realiza diversos exames forenses e dentre os mais requisitados destes são os realizados em mídias de armazenamento de dados onde uma das técnicas utilizadas nestes é a recuperação de dados. Existem várias ferramentas forenses de licença paga e licença gratuita para recuperação de dados, sendo assim este trabalho analisou uma de cada dessas ferramentas, concluindo quais ferramentas são eficientes no processo de recuperação dos dados. As ferramentas analisadas foram *Forensic Toolkit* 4 e *RecoverIt* 6, sendo uma de licença paga e a outra gratuita, respectivamente nesta ordem. A análise destas ferramentas levou em consideração a praticidade da interface, as extensões dos arquivos, o tempo de retorno e o percentual de recuperação de cada uma das ferramentas, e com esses dados foi possível determinar qual ferramenta apresentou melhor resultado.

.

Palavras-chave: Computação Forense. Recuperação. Análise. Dados.

ABSTRACT

Forensic computing can be defined as a set of techniques and procedures that use scientific knowledge to collect, analyze, and present evidence that can be used in court. Being essentially the thorough search based on certain events for a criminal investigation. During the investigations the expert performs several forensic examinations and among the most requested of these are those performed in data storage media where one of the techniques used in these is data recovery. There are several forensic tools for paid license and free license for data recovery, so this work has analyzed one of each of these tools, concluding which tools are efficient in the data recovery process. The tools analyzed were Forensic Toolkit 4 and RecoverIt 6, one being paid license and the other free, respectively in this order. The analysis of these tools took into consideration the practicality of the interface, the file extensions, the time of return and the percentage of recovery of each of the tools, and with these data it was possible to determine which tool presented the best result.

Keywords: Forensic Computing. Recovery. Analysis, Data.

SUMÁRIO

INTRODUÇÃO

A computação forense pode ser definida como um conjunto de técnicas e procedimentos que utilizam conhecimento científico para coletar, analisar e apresentar evidências que possam ser utilizadas em um tribunal. Sendo essencialmente a busca minuciosa com base em determinados eventos para uma investigação criminal.

Com o avanço tecnológico de ferramentas para intrusões de sistemas, os crimes virtuais obtiveram força e, consequentemente, êxito nos ataques efetuados. Para prevenir e até mesmo extinguir os ataques virtuais, peritos especializados utilizam técnicas e ferramentas forenses como forma de combate.

A Computação Forense é formada por quatro etapas de investigação:

1. Coleta, onde é realizada a coleta das evidências na cena do crime garantindo a integridade das evidências.
2. Exame, que consiste em filtrar, extrair, identificar e documentar.
3. Análise, onde identifica e correlaciona pessoas reconstruindo a cena e documentando os resultados.
4. Resultados obtidos, onde é realizado um laudo anexando as evidências.

De acordo com o tipo de investigação diversos exames forenses são realizados: em locais de crime de informática, em dispositivos de armazenamento digital, em *smartphones*, em sites e mensagens eletrônicas (ELEUTÉRIO; MACHADO, 2011).

Vacca (2005) define que a recuperação de dados é o processo no qual são recuperados os dados apagados ou que não podem ser mais acessíveis em mídias computacionais.

Existem várias ferramentas para recuperação de dados, ferramentas proprietárias e ferramentas livres. O foco deste trabalho foi na comparação entre uma ferramenta de licença paga que é a *Forensic Toolkit* (FTK), e uma de licença gratuita que é a *RecoverIt*.

As ferramentas foram utilizadas no Sistema Operacional (SO) *Windows*, com o objetivo de determinar qual ferramenta apresentou melhores resultados de desempenho e percentual de recuperação de dados.

Com base nos resultados obtidos dos testes de recuperação realizados foi possível determinar qual ferramenta apresentou melhores resultados, mesmo apresentando problemas de recuperação em alguns testes.

1. REFERENCIAL TEÓRICO

Este capítulo tem o objetivo de mostrar uma breve explicação sobre computação forense, mostrar um pouco sobre as etapas de investigação da forense computacional e recuperação de dados, sendo estes conceitos relevantes para o entendimento e realização deste estudo.

1.1 Perícia Forense Computacional

A Computação Forense se apresenta como sendo uma ciência de investigação criminal aplicada em sistemas digitais. Ela objetiva-se em utilizar métodos técnico-científicos para preservar, coletar, validar, identificar, analisar, interpretar e documentar as evidências conferindo-lhe validade probatória em juízo (ELEUTÉRIO; MACHADO, 2011).

A perícia forense aplicada à computação é ligada a investigação de crimes cibernéticos colhendo dados para identificação, preservação, análise e documentação com a finalidade de obtenção de evidências digitais. Alguns procedimentos devem ser seguidos pelo perito para assegurar que a evidência não seja comprometida, substituída ou perdida (FREITAS, 2007).

Os profissionais na área têm regras a seguir, providências definidas a tomar, para obter credibilidade no que faz, artigos específicos de como um capacitado deve proceder em uma investigação para que seu trabalho não tenha sido em vão e desconsiderado em uma audiência judicial, nas quais um parecer técnico será necessário. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados (QUEIROZ; VARGAS, 2010).

Segundo Eleutério e Machado (2011), apesar de a utilização de computadores não ser uma prática tão recente no mundo do crime, a legislação brasileira ainda não está preparada para tipificar todas as modalidades específicas de crimes cibernéticos.

A legislação brasileira necessita de muitos avanços na área. Assim, torna-se

importante diferenciar se o computador é utilizado apenas como ferramenta de apoio à prática de delitos convencionais ou se é utilizado como meio para a realização do crime (ROSA, 2005).

Assim, Eleutério e Machado (2011) afirmam ainda que se torna importante diferenciar se o computador é utilizado apenas como ferramenta de apoio à prática de delitos convencionais ou se é utilizado como meio para a realização do crime.

Segundo Eleutério e Machado (2011), o computador está associado ao *modus operandi* do crime. Assim, em muitos casos, exames forenses nesses objetos são uma excelente prova técnica e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença.

O uso de equipamentos computacionais como ferramenta de apoio aos crimes convencionais corresponde a cerca de 90% dos exames forenses realizados na área da informática, excluindo-se dessa estatística os exames forenses em aparelhos celulares (ELEUTÉRIO; MACHADO, 2011).

O computador é a peça central para a ocorrência do crime, ou seja, se o dispositivo não existisse, tal crime não seria praticado (ELEUTÉRIO; MACHADO, 2011).

O aumento da inovação tecnológica beneficia muito as pessoas, porém, com essa inovação sempre surgem práticas ilegais e criminosas.

De acordo com Eleutério e Machado (2011) o Código de Processo Penal (CPP) determina em seu artigo 158 que: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado. ” Dessa forma, surge a necessidade de um profissional qualificado, que examine vestígios e produza laudos de interesse à justiça na apuração de um delito, conforme definidos nos caputs dos artigos 159 e 160 do CPP, que dizem, respectivamente: “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior. ” e “Os peritos elaborarão o laudo pericial, no qual descreverão minuciosamente o que examinarem e responderão aos quesitos formulados.”

No caso específico da computação, quem realiza esse trabalho de forma oficial no âmbito criminal é o Perito Criminal em Informática. Entretanto, diversos outros profissionais podem ter a necessidade de realizar exames em computação. São eles: peritos particulares, auditores de sistemas e profissionais de TI. Além disso, juízes, advogados, delegados, promotores e demais profissionais da área de direito também devem conhecer como evidências e provas digitais devem ser corretamente coletadas, apuradas e apresentadas.

Segundo Ramalho Terceiro (2002) enquanto houver por parte da legislação penal tal omissão, não serão considerados crimes, como de fato são. Destarte, seus agentes sempre serão agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena, ou impor uma sanção, a uma conduta que o ordenamento penal não considere expressamente como criminosa, mesmo que tal conduta produza prejuízos financeiros ou atente contra a integridade humana, bens resguardados pelo direito penal.

No entanto, segundo Blum (2009), a legislação ordinária brasileira cobre, total ou parcialmente, 95% dos crimes eletrônicos. Os demais 5% que ainda não têm previsão legal são motivos de grande preocupação. “É um mundo sem leis”.

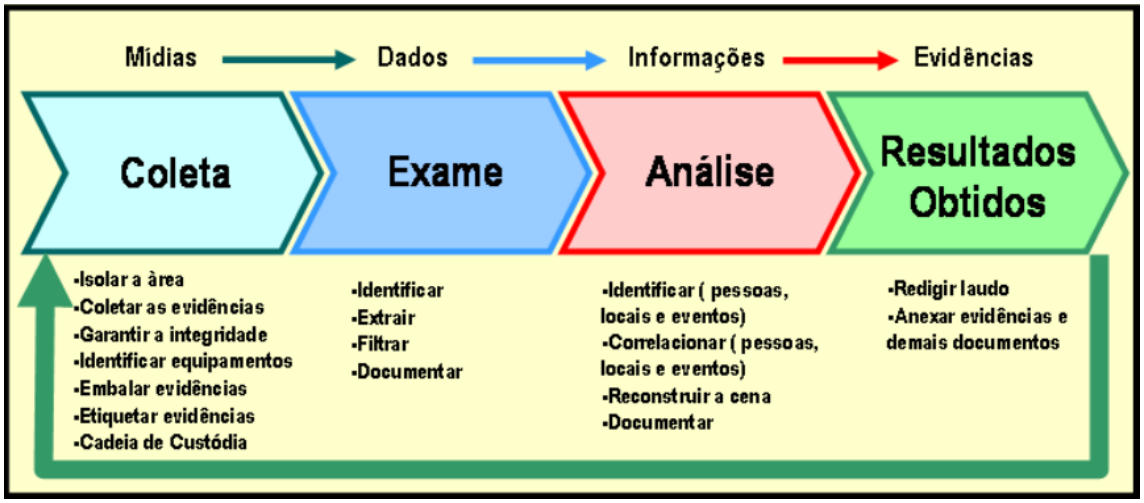
1.2 Etapas de Investigação

A execução de uma perícia se distribuí em quatro fases, nas quais as informações devem ser levantadas, examinadas e analisadas, gerando a partir daí a documentação técnica que é o resultado de todo o processo.

Sendo a computação forense uma ciência investigativa, tendo como objetivo provar os acontecimentos através de métodos técnico-científicos, sendo nomeado um perito que será o responsável por aplicar esses métodos preservando a integridade das evidências e detalhar tudo o que for realizado da investigação através de um laudo pericial (PEREIRA et al., 2007).

Para que seja possível realizar todos esses passos descritos acima, os mesmos são divididos em quatro etapas como pode ser observado na FIG. 1.

FIGURA 1 - Etapas de investigação na computação forense



Fonte: Pereira et al.(2007)

Para que seja possível um melhor entendimento das quatro etapas observadas acima, elas serão explicadas nos tópicos a seguir.

1.2.1 Coleta dos Dados

A etapa de coleta dos dados é a etapa mais importante das quatro etapas de investigação precisando assim de muita atenção para executar a mesma. Essa etapa tem essa atenção toda pelo fato de ser o marco inicial de toda investigação sendo necessário garantir a integridade de todas as evidências.

A chegada ao local da investigação é um passo pré-coleta, no qual alguns cuidados são tomados tais como isolar a área ou local do crime, visando impedir que algum tipo de alteração ou contaminação ocorra com as evidências e caso necessário, fotografar e/ou filmar o ambiente ou equipamento para amparar necessidades de alguma análise futura nas próximas etapas do processo.

A fase de coleta de dados é dividida em: identificação de possíveis fontes de dados e aquisição de dados (KENT et al., 2006).

1.2.1.1 Identificação das fontes de dados

Com relação aos equipamentos a serem investigados: computadores pessoais, CDs, DVDs, relógio com comunicação via USB, entre outros equipamentos podem conter informações de suma importância para a investigação. E como pode se perceber cada vez mais surgem novos equipamentos capazes de armazenar informações havendo a necessidade de atualização das tecnologias por parte do perito (KENT et al., 2006).

1.2.1.2 Aquisição de dados

A aquisição dos dados dividiu-se em três partes: plano para aquisição dos dados, aquisição propriamente dita e verificação de integridade (KENT et al., 2006).

1.2.1.2.1 Plano para aquisição de dados

O plano para aquisição dos dados consiste em uma sequência de passos que o perito determina para realizar a coleta dos dados seguindo três fatores: valor da fonte, volatilidade e quantidade de esforço requerido (KENT et al., 2006).

1.2.1.2.1.1 Valor da fonte

O perito determina valores para as fontes de dados, sendo estes valores responsáveis por determinar a sequência que deve ser respeitada durante o processo de investigação das fontes de dados (KENT et al., 2006).

1.2.1.2.1.2 Volatilidade

Os dados voláteis são dados que quando uma máquina é desligada esses dados são perdidos temos como exemplos de dados voláteis: dados da memória e conexões de rede. Assim para conseguir esses dados é necessário que o perito faça a coleta das informações com os equipamentos ainda ligados (KENT et al., 2006).

1.2.1.2.1.3 Quantidade de esforço requerido

Tem a ver além do tempo que o perito leva para realizar a coleta dos dados, o custo da utilização de equipamentos e serviços de terceiros, caso necessário (KENT et al., 2006).

1.2.1.2.2 Aquisição propriamente dita

A aquisição ou coleta dos dados pode ser realizada localmente aonde o perito vai até o local da investigação para realizar a perícia agindo de forma direta ao sistema ou remotamente, porém a aquisição dos dados realizada localmente é mais aconselhável para ser realizado pelo fato de o perito ter maior controle de todas as operações que estão sendo realizadas (KENT et al., 2006).

1.2.1.2.3 Verificação de integridade

Através de funções matemáticas de resumo é realizada uma correspondência de informações entre a fonte dos dados com os dados coletados. Quando é realizada a coleta dos dados deve-se manter a integridade dos dados coletados e essa integridade seria a integridade dos tempos de criação de cada arquivo (KENT et al., 2006).

1.2.2 Exame dos dados

O objetivo da fase de exame é avaliar, extrair, filtrar e documentar somente as informações relevantes à investigação levantadas na fase de coleta, uma tarefa bastante trabalhosa tendo em vista a grande capacidade de armazenamento dos dispositivos atuais, variedade de sistemas operacionais e a enorme quantidade de diferentes formatos de arquivos existentes.

Depois de realizada a coleta dos dados é realizado o exame dos dados coletados sendo realizado um filtro determinando quais dados são relevantes para a investigação e quais não são, onde estas determinações variam de investigação para investigação de acordo com o tipo de informação que está sendo investigada (KENT et al., 2006).

O objetivo principal é mapear, identificar e mostrar a forma correta de preservar os equipamentos computacionais sendo assim mais fácil de realizar a seleção desses equipamentos a serem periciados futuramente em laboratório. Porém dependendo do tipo de investigação pode ser necessário que o perito responsável pela investigação tenha que realizar a perícia no local do crime (ELEUTÉRIO, MACHADO, 2011).

Estes exames são realizados em quatro frases: preservação, extração, análise e formalização e utilizam algumas técnicas que auxiliam na realização destes exames sendo quebra de senhas, virtualização e recuperação de dados (ELEUTÉRIO, MACHADO, 2011).

1.2.3 Análise de Dados

Depois de examinado os dados onde foi realizado um filtro para determinar as informações relevantes, na etapa de análise é realizado uma correlação entre as informações relevantes que foram encontradas na etapa de análise com as informações da investigação, sendo possível assim realizar a conclusão da investigação (PEREIRA et al., 2007).

Além de consumir muito tempo, a análise de informações está muito suscetível a equívocos, pois depende muito da experiência e do conhecimento dos peritos e não há muitas ferramentas de apoio para esta fase, dada sua complexidade, e as que existem, não possuem um bom grau de precisão.

A análise pericial é o processo usado pelo investigador para descobrir informações valiosas, a busca e extração de dados relevantes para uma investigação. O processo de análise pericial pode ser dividido em duas camadas: análise física e análise lógica. (FREITAS, 2007).

A análise física é a pesquisa de sequências e a extração de dados de toda a imagem pericial, dos arquivos normais às partes inacessíveis da mídia.

Já a análise lógica consiste em analisar os arquivos das partições. O sistema de arquivos é investigado no formato nativo, percorrendo-se a árvore de diretórios do mesmo modo que se faz em um computador comum.

1.2.4 Resultados Obtidos

Depois de realizadas todas as três etapas (coleta, exame e análise dos dados), realiza-se a última etapa de investigação que são os resultados, apresentados na forma de um laudo pericial, onde o perito forense computacional responsável pela investigação descreverá da forma mais detalhada possível tudo o que foi realizado desde o início garantindo assim a veracidade das informações e apresentando uma conclusão sobre a investigação. Constarão da documentação aspectos relativos às etapas anteriores como: método de coleta e extração, análise dos fatos e o valor técnico do conteúdo analisado (KENT et al., 2006).

Geralmente, os laudos periciais possuem a seguinte estrutura: preâmbulo, histórico, material, objetivo, considerações técnicas ou periciais, exames e respostas aos quesitos formulados ou conclusões (ELEUTÉRIO, MACHADO, 2011). Essa estrutura é apresentada e explicada de forma breve no Quadro 1.

Quadro 1 - Seções do laudo técnico pericial

Laudo Técnico Pericial – Perícia Forense Computacional	
Preâmbulo	Identificação do laudo
Histórico	Fatos anteriores e de interesse ao laudo. Quesitos concisos e objetivos.
Material	Descrição do material examinado.
Objetivo	Principais objetivos da perícia.
Considerações técnicas/periciais	Conceitos e informações que podem ser úteis para o entendimento do laudo.
Exames	Parte descritiva e experimental do laudo.
Respostas aos quesitos/conclusões	Resumo objetivo dos resultados obtidos.

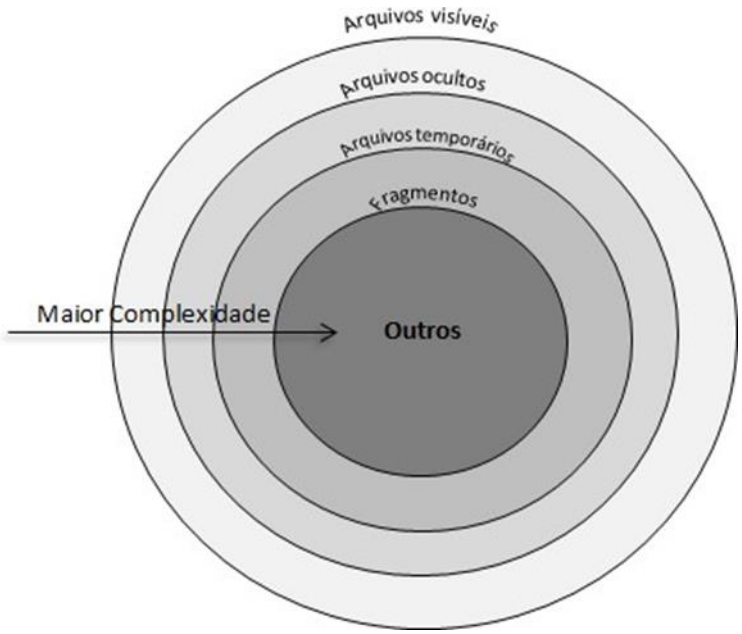
Fonte: Eleutério e Machado (2011)

No Quadro 1 podem ser observados os passos que um perito forense deve seguir para a finalização de um laudo pericial. Nesta pesquisa foi feita a penúltima etapa do laudo, a etapa de “Exames”, sendo onde são feitos os testes necessários para a conclusão do laudo, variando o tipo de teste em cada caso. Por fim o teste utilizado nesta pesquisa foi o de recuperação de dados.

1.3 Recuperação de Dados

Atualmente os dispositivos de armazenamento podem guardar muitas informações que não são visíveis aos usuários comuns, e esse fato ocorre devido ao tipo de organização de dados adotado nesses materiais. Eleutério e Machado (2011) apresentam, de forma ilustrativa, um comparativo entre um disco rígido e um planeta de dados conforme mostra a FIG.2. A exploração das camadas dos arquivos de um sistema de armazenamento fica mais complexa quanto mais interna na ilustração.

FIGURA 2 - Disco rígido como um planeta de dados



Fonte: Eleutério e Machado (2011)

Na região mais interna da Fig.2 são classificados outros arquivos e dados, representados principalmente por arquivos apagados e por arquivos protegidos por senhas. Segundo Kent et al (2006), arquivos comprimidos, criptografados ou protegidos por mecanismos de controle de acesso também fazem parte dessa classificação.

A recuperação de informações dessa região é complexa, exige tempo e uso de técnicas e ferramentas específicas. No entanto, a recuperação eficaz dessas informações pode resultar em evidências elucidativas para a perícia forense (ELEUTÉRIO; MACHADO, 2011).

São vários os fatores que afetam a integridade, disponibilidade e confiabilidade dos dados presentes nas mídias de armazenamento não volátil que são mídias onde o seu conteúdo não é perdido quando desligado.

Vacca (2005) define a recuperação de dados como sendo um processo em que se busca os dados que foram apagados nas mídias de armazenamento computacional ou que não são mais acessíveis pelas mídias.

Para Vacca (2005) são vários os motivos para os dados se tornarem inacessíveis: realizado através de um ato humano deliberadamente, por falha mecânica ou elétrica, problemas no software ou simplesmente um vírus de computador.

De acordo com Eleutério e Machado (2011), os principais aspectos a serem observados são os seguintes: o sistema operacional sabe (através da tabela de controle, em discos rígidos) quais partes do dispositivo de armazenamento estão ocupadas ou não; ao apagar um arquivo do computador, o sistema operacional não remove os dados referentes a esse arquivo, mas altera o status do espaço anteriormente ocupado para disponível; uma vez classificado como disponível, o espaço ocupado pelos dados do arquivo pode ser sobrescrito a qualquer momento, seja por novos arquivos salvos pelo usuário, seja por ações do sistema operacional. Nesse sentido que quanto mais recente for a exclusão de um determinado arquivo, maior será a probabilidade de sucesso na recuperação.

A recuperação dos dados além de levar em consideração a forma como os dados se perderam leva em consideração também o tipo de informação a ser recuperada, pelo fato de que arquivos contendo certos tipos de informações não são recuperadas totalmente, mas para a computação forense qualquer fragmento de arquivos influencia na investigação (VACCA, 2005).

Segundo Altheide e Carvey (2011), quando se analisa uma mídia de armazenamento computacional (HDs, CDs, DVDs, cartões de memória dentre outras mídias de armazenamento) o que se espera com este processo é fazer uma análise, extração e identificação dos arquivos e dos sistemas de arquivos das mídias. A extração dos dados é feita utilizando técnicas de recuperação, existem várias técnicas, mas as mais utilizadas são duas: recuperação lógica e *data carving*, que a seguir são apresentadas.

1.3.1 Recuperação Lógica

Segundo Mota Filho (2012) os “arquivos ou áreas de disco só serão realmente apagados se escrevermos dados por cima dos que já existem”.

Segundo Vacca (2005) os dados nos sistemas de arquivos não são sobrescritos podendo ser recuperados utilizando ferramentas específicas.

Os sistemas de arquivos não utilizam a exclusão definitiva dos arquivos, apenas uma exclusão lógica pelo fato de o tempo que se leva para sobrescrever um arquivo chega a ser maior que o tempo de escrita do arquivo. Utilizando a exclusão lógica o bloco recebe simplesmente o status de livre podendo ser utilizada para receber novos dados (MOTA FILHO, 2012).

Segundo Carrier (2005) a recuperação lógica tenta recuperar os dados que estavam nas mídias de armazenamento utilizando informações do próprio sistema de arquivos que cada uma das mídias de armazenamento computacional está utilizando.

Este tipo de recuperação consegue recuperar os metadados dos arquivos (nome, data entre outras informações sobre os metadados) sendo a sua maior vantagem, porém esse tipo de recuperação não se torna tão eficiente quando as mídias são formatadas, pelo fato de ser criada uma nova tabela de dados de controle (CARRIER, 2005).

1.3.2 *Data Carving*

A técnica de *data carving* também chamada de *file carving* diferente da recuperação lógica, não leva em consideração a estrutura do sistema de arquivos presente nas mídias de armazenamento, por conta deste fato não são recuperados os metadados (nomes, datas e outras informações que compõem os metadados) controlados pelo sistema de arquivos (CARRIER, 2005).

Esta técnica busca por padrões e estes padrões são assinaturas que os arquivos deixam quando são apagados sejam de forma acidental ou por ter sido realizado formatações, essa técnica compara essas assinaturas achando um padrão ela começa a

fazer o processo de recuperação, recuperando os dados totalmente ou parcialmente (CARRIER, 2005).

A data carving consegue recuperar dados que não são mais reconhecidos pelos sistemas de arquivos, porém não são eficientes para arquivos fragmentados (CARRIER, 2005).

Como o foco deste estudo é na recuperação de dados em mídias digitais, na próxima seção é relatado um pouco sobre as ferramentas forenses utilizadas.

1.4 FERRAMENTAS FORENSES

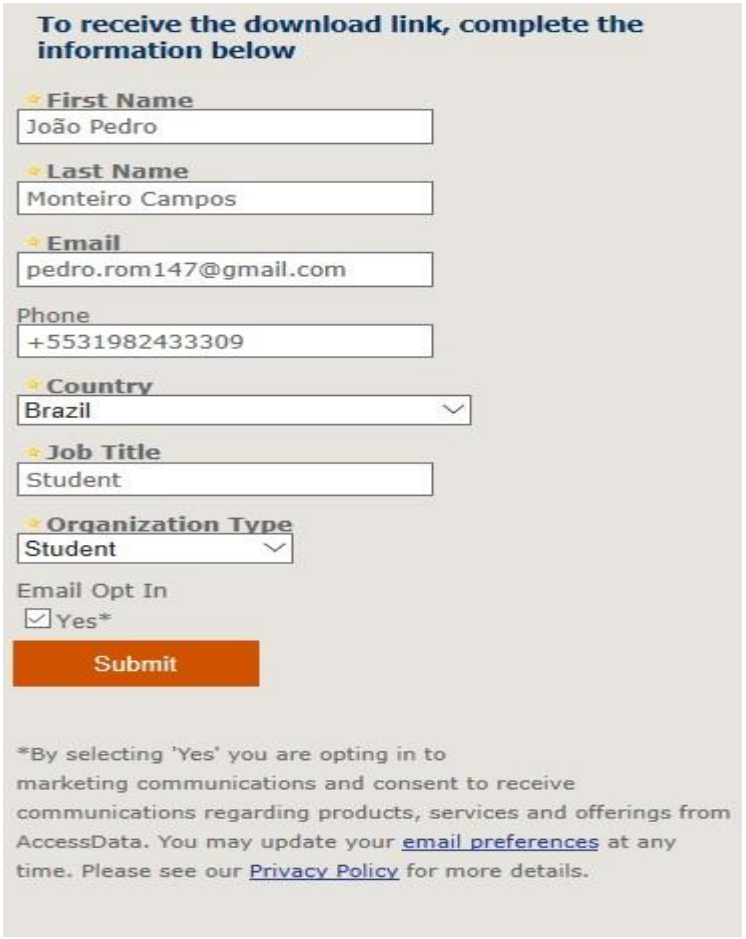
Existem várias ferramentas para recuperação de dados, ferramentas pagas e ferramentas gratuitas. O foco deste trabalho foi na comparação entre uma ferramenta de licença paga e uma de licença gratuita.

Diante das várias ferramentas existentes foram selecionadas duas levando em consideração o tipo de técnica que elas utilizam para a recuperação dos dados, sendo essa técnica a recuperação lógica, uma das técnicas mais utilizadas na área. A ferramenta de licença paga é a *Forensic Toolkit* (FTK), e de licença gratuita que é a *RecoverIt*.

O FTK é uma ferramenta muito conhecida e bem-conceituada entre os peritos forense. Na sua atual versão 4.2.0, liberada em dezembro de 2017, é um software de licença paga custando em média $ 3.995,00 na sua versão mais completa.

Mas para o estudo foi utilizado a versão disponibilizada para estudantes, que possui as mesmas funcionalidades da versão completa, mas tem um prazo de validade para este uso gratuito. Esta versão gratuita da ferramenta está disponível no próprio site da fabricante *Access Data*, mediante ao preenchimento de um formulário conforme mostra a FIG.3.

FIGURA 3 - Formulário para recebimento do link de download do FTK



Fonte: Autor

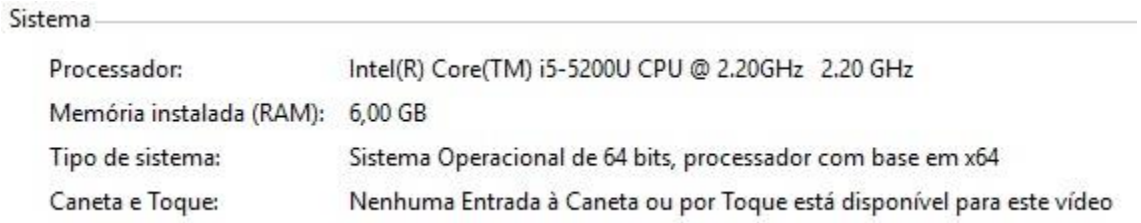
O *RecoverIt* é uma ferramenta bastante conhecida no meio como a melhor ferramenta de licença gratuita. Em suas versões mais antigas possui o nome de *Recovery Data*, a empresa fabricante da ferramenta *Wondershare*, garante que a mesma seja capaz de recuperar até 96% dos arquivos deletados do seu dispositivo, isso acaba a tornando um dos softwares mais potentes do mercado a possuir uma versão gratuita.

As ferramentas foram utilizadas no Sistema Operacional (SO) *Windows*, e o objetivo desse estudo foi executar uma análise geral dessas ferramentas em testes de recuperação de dados, tendo como foco não desvalorizar nenhuma das ferramentas, mas sim apontar as vantagens e desvantagens entre elas, desde a interface para o usuário, como a complexibilidade, o desempenho e principalmente a taxa de sucesso na recuperação dos dados, auxiliando na tomada de decisão sobre qual ferramenta deve ser utilizada para a execução de determinada tarefa.

2 METODOLOGIA

Para analisar as ferramentas forense de recuperação de dados FTK e *RecoverIt* foi utilizado o SO de 64 bits *Windows* 10 *Home Single Language*, versão 1809, compilação 17763.134. Na FIG.4 são mostradas as especificações de *Hardware* utilizadas.

FIGURA 4 - Exibição das especificações de Hardware



Fonte: Autor

Foi necessário a realização de alguns passos para efetuar a análise das ferramentas, e estes passos foram relatados nas próximas seções.

2.1 DETALHAMENTO DA ESTRUTURA

As ferramentas forenses de recuperação de dados podem ser utilizadas em diversos tipos de mídias de armazenamento. Mas neste estudo foi utilizado um HD como mídia de armazenamento, possuindo uma capacidade de armazenamento de 931 GB com o sistema de arquivos NTFS.

Tendo o HD devidamente formatado, foi transferido para o mesmo o banco de arquivos que foram utilizados nos testes para análise, que será melhor explicado nos tópicos a seguir.

2.2 ARMAZENAMENTO DOS ARQUIVOS NO HD

Para execução dos testes foram utilizados 120 arquivos, divididos em 20 arquivos de 06 tipos e 23 extensões diferentes, que podem ser visualizados no Quadro 2.

Quadro 2 - Tipos e extensões dos arquivos utilizados

Tipos de arquivos	Extensões
Áudios	MP3, WMA e M4A
Compactados	ZIP e RAR
Documentos	PDF, DOCX, LOG, TXT, DOC, XML, RTF e XLSX
Executáveis	EXE
Imagens	JPG, PNG, GIF e JPEG
Vídeos	MP4, RMVB, WMV, 3GP e AVI

Fonte: Autor

As extensões de dados utilizadas foram escolhidas de maneira aleatória, de modo a não favorecer nenhuma ferramenta.

Para manter a integridade dos arquivos para os próximos testes, foi feito o *upload* de todos eles para um servidor gratuito que pode ser acessado pelo seguinte *link: "https://mega.nz/#F!gBtC3QTB!T3M3hq25J8w68C8UEZKd9g".*

Tendo feito o upload do banco de arquivos, ao final de cada etapa de testes foi efetuado o download do mesmo diretamente no HD, visando manter a integridade de todos os dados ali contidos para que não houvesse diferenças nos resultados finais.

2.3 RECUPERAÇÃO DOS ARQUIVOS

Depois de criado o banco de arquivos e o HD preparado, foi iniciado à parte dos testes, sendo dividida nos seguintes tópicos: Recuperação da exclusão direta, recuperação da restauração do dispositivo e recuperação da formatação do dispositivo.

2.3.1 Recuperação da exclusão direta

Nessa etapa com o HD formatado sem nenhum arquivo em sua memória, foi efetuado o *download* do banco de arquivos diretamente no dispositivo. Com a finalização do download, foi conferido se todos os arquivos estavam no dispositivo por completo, tendo feita essa conferência o próximo passo é a exclusão direta dos arquivos. Essa exclusão direta é a exclusão dos dados com a utilização das teclas *shift* e *delete*.

Com os arquivos excluídos inicia o processo de recuperação com as ferramentas, que será descrito nos próximos tópicos.

2.3.1.1 Recuperação com a ferramenta FTK

A ferramenta FTK possui uma determinada complexidade em sua instalação, sendo uma instalação mais custosa, pois antes de instalar a ferramenta é necessário a instalação de um banco de dados *PostgreSQL*, que vem junto com o pacote baixado no site da *AccessData*, conforme mostra a FIG.5.

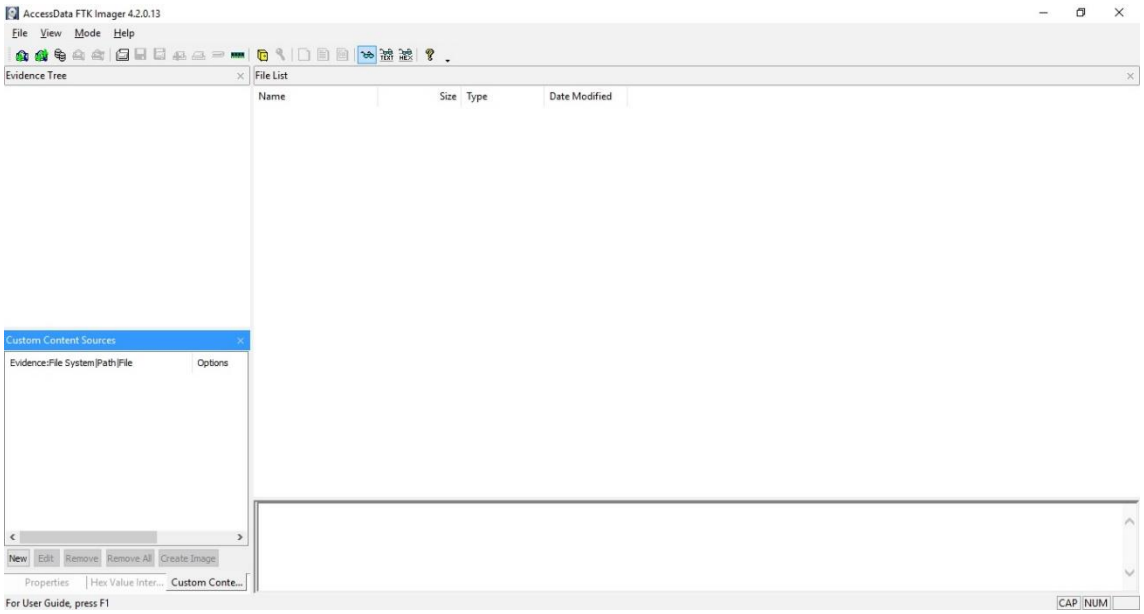
FIGURA 5 - Tela de instalação da ferramenta FTK

Fonte: Autor

Conforme mostra a FIG.5, a primeira opção selecionável é "*Database Install 64bit*". Essa opção vem em destaque acima e em coluna única, de modo a instruir o usuário que é necessário executar esse procedimento primeiro.

Após a instalação do banco de dados e da ferramenta, já é possível a utilização da mesma. O FTK possui uma interface complexa, mas com diversas funções, permitindo que o perito trabalhe com mais de uma evidência simultaneamente.

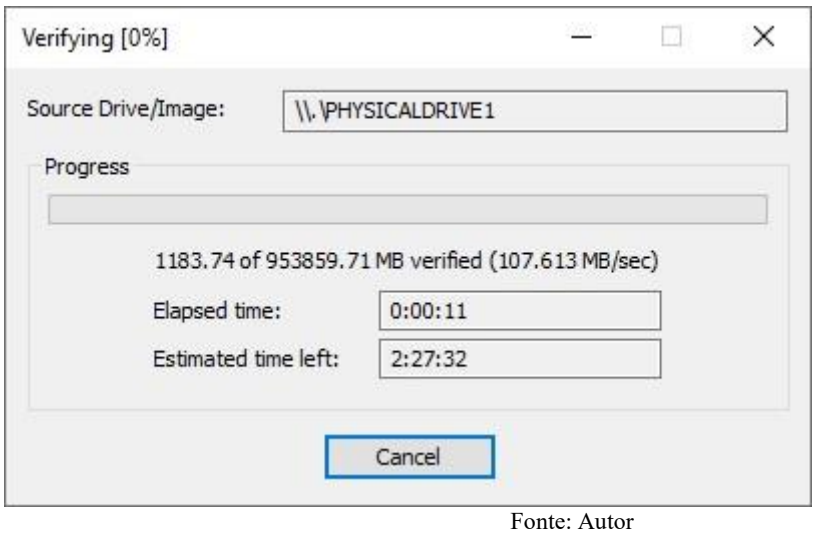
FIGURA 6 - Tela inicial do FTK



Fonte: Autor

Como mostrado na FIG.6, na tela inicial do FTK é iniciado uma nova análise de evidências, e no canto superior esquerdo é selecionado dispositivo de mídia onde será efetuada a análise. Iniciado a análise aparece uma nova janela mostrada na FIG.7.

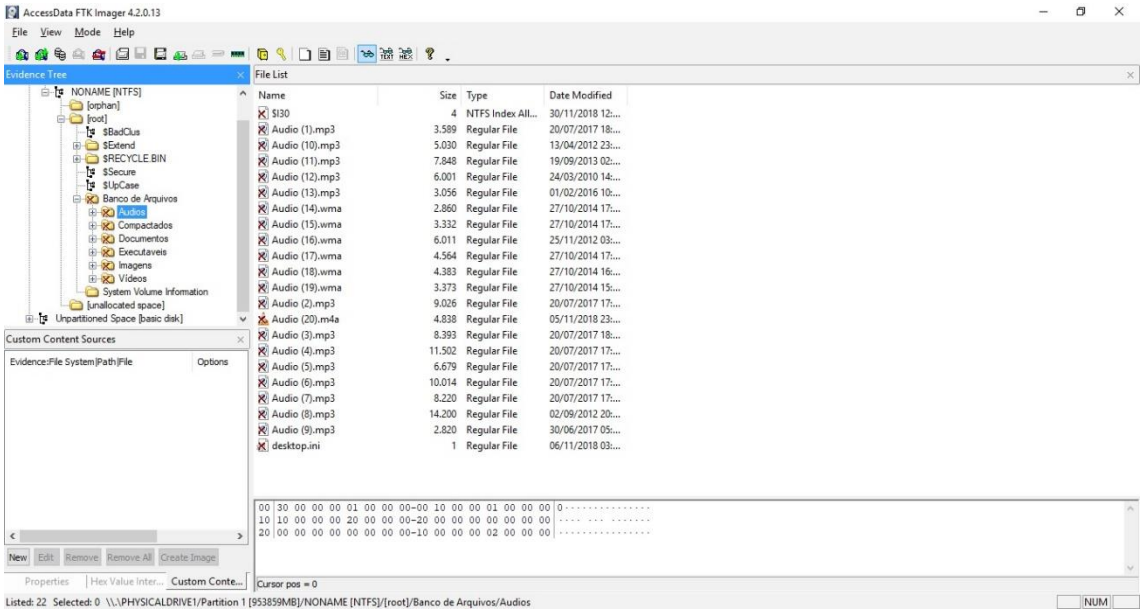
FIGURA 7 - Janela de verificação FTK



Fonte: Autor

Após o fim da verificação a janela fecha e são exibidos todos os dados recuperados do dispositivo de mídia, conforme pode ser visto a seguir na FIG.8.

FIGURA 8 - Janela de exibição de dados recuperados



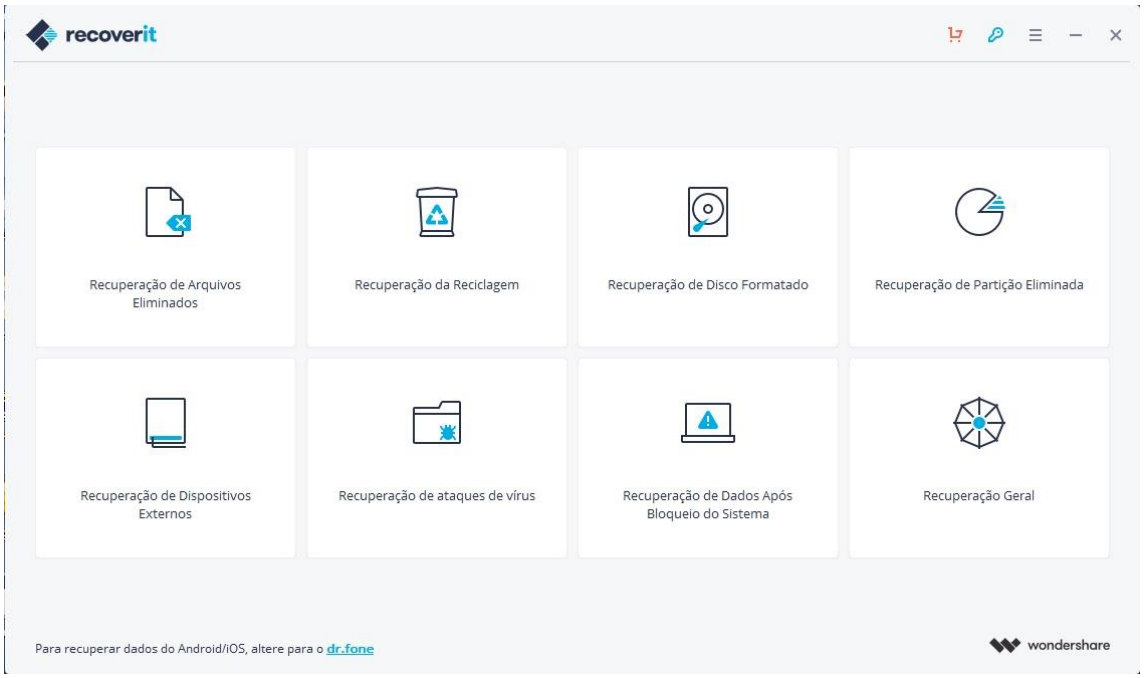
Fonte: Autor

Por fim com os arquivos recuperados, seus dados foram inseridos nas tabelas, para que fosse feita a análise posteriormente.

2.3.1.2 Recuperação com a ferramenta *RecoverIt*

A ferramenta *RecoverIt*, é uma ferramenta que possui uma interface simples e intuitiva em relação ao FTK, sendo de rápida e fácil instalação, tendo somente que fazer o download do arquivo .exe no site da fabricante.

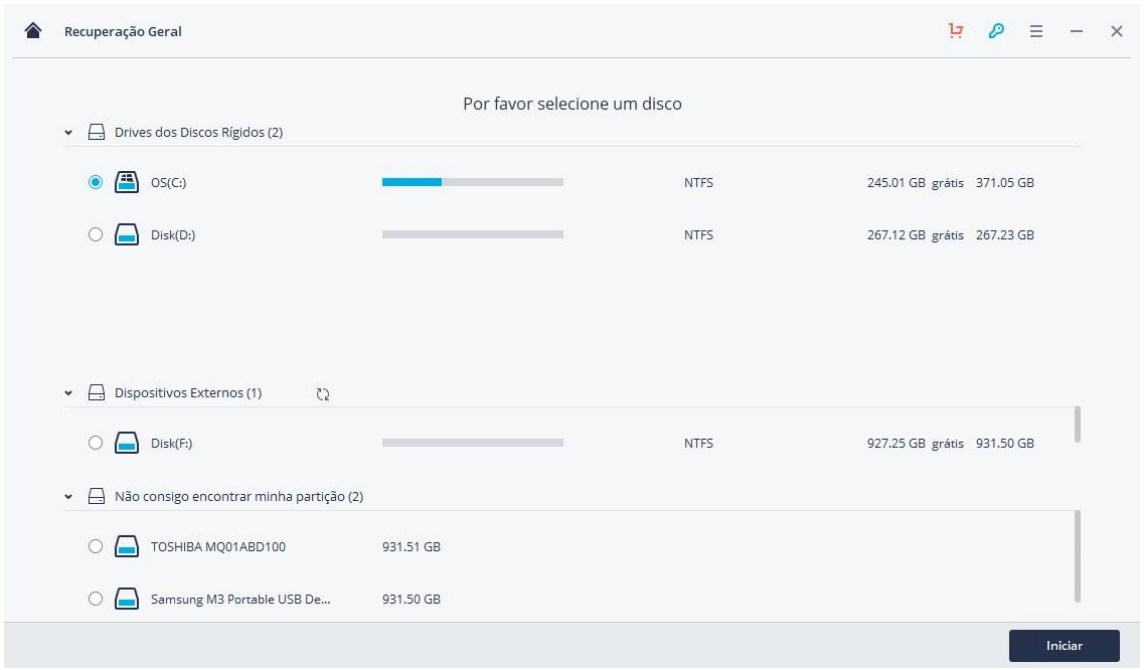
FIGURA 9 - Interface inicial da ferramenta *RecoverIt*



Fonte: Autor

Conforme mostra na FIG.9, o *RecoverIt* possui uma interface moderna e intuitiva. Na tela inicial do *RecoverIt*, foi utilizada no estudo sua função “Recuperação Geral”, onde a tela é mostrada na FIG.10.

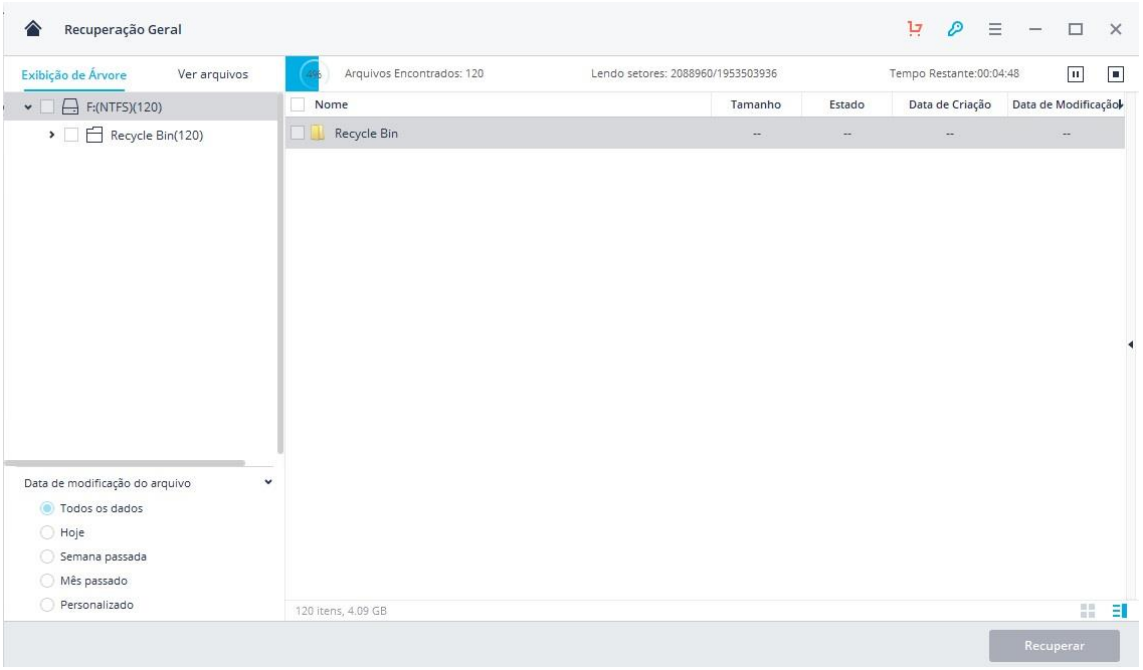
FIGURA 10 - Interface Recuperação Geral da ferramenta *RecoverIt*



Fonte: Autor

Na tela apresentada na FIG.10, é selecionado o dispositivo de mídia a ser examinado, e em seguida selecionada a opção iniciar. Que redireciona para uma nova tela apresentada na FIG.11.

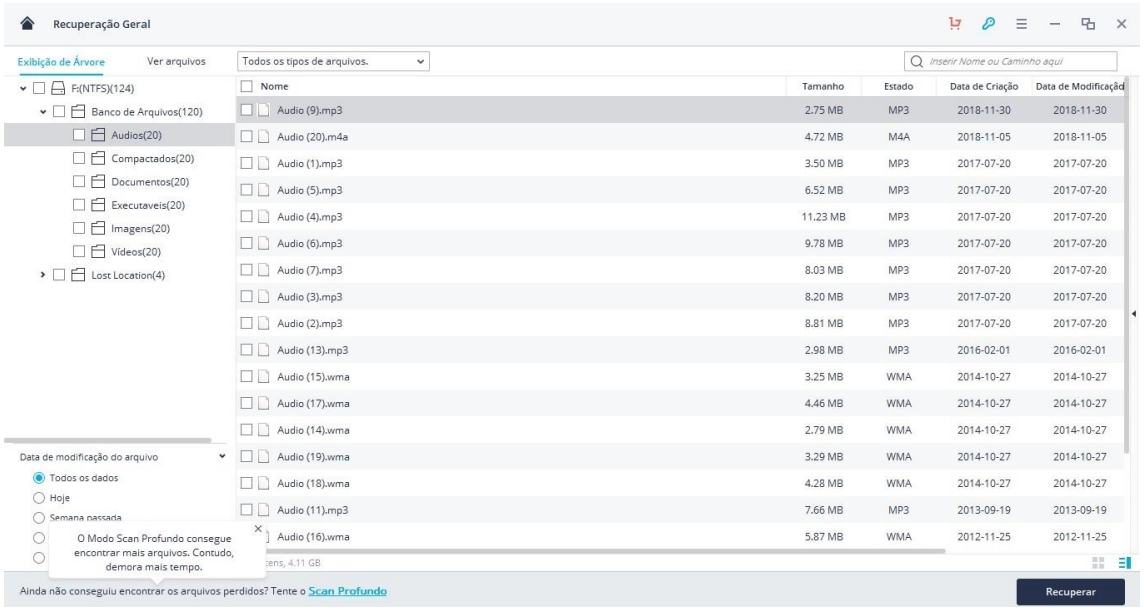
FIGURA 11 - Tela final de análise do *RecoverIt*



Fonte: Autor

A tela apresentada na FIG.11, é a tela final de análise do *RecoverIt*. Após a conclusão do exame efetuado na mídia, nessa mesma tela são exibidos todos os dados recuperados, como mostra a FIG.12.

FIGURA 12 - Tela de dados recuperados *RecoverIt*



Fonte: Autor

Por fim com os arquivos recuperados, seus dados foram inseridos nas tabelas, para que fosse feita a análise posteriormente.

2.3.2 Recuperação da restauração do dispositivo

Após ter a finalização das etapas anteriores, foi efetuado novamente o *download* do banco de arquivos no dispositivo. Finalizado o *download*, o SO instalado no dispositivo de mídia foi restaurado para as configurações de fábrica, utilizando a própria opção de restauração nativa do *Windows*. Finalizada a restauração do dispositivo, se repete os processos descritos nas seções 2.3.1.1 e 2.3.1.2.

Os resultados obtidos foram apresentados e discutidos na seção 3 Análise de resultados.

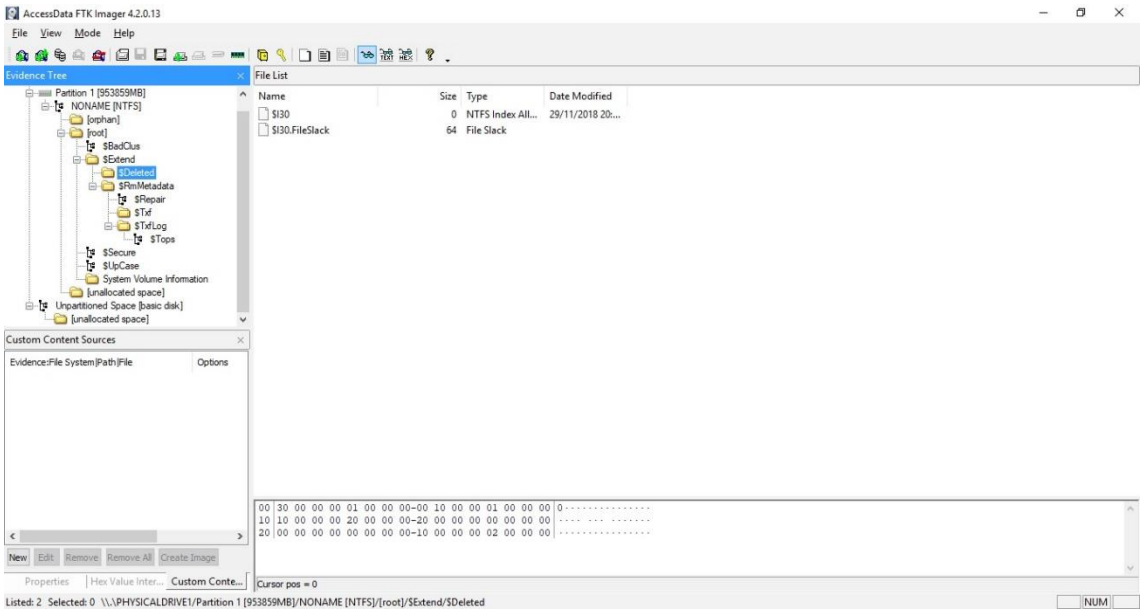
2.3.3 Recuperação da formatação do dispositivo

Após ter a finalização das etapas anteriores, foi efetuado novamente o *download* do banco de arquivos no dispositivo. Finalizado o *download*, o SO instalado no dispositivo de mídia foi formatado através da BIOS. Finalizada a formatação do dispositivo, se repete os processos descritos nas seções 2.3.1.1 e 2.3.1.2.

Porém ao final da execução dos testes de recuperação da formatação do dispositivo o resultado foi diferente em relação as seções anteriores, pois nenhuma das ferramentas foram capazes de recuperar os dados.

A ferramenta FTK exibiu na tela de recuperação arquivos de LOG do dispositivo de mídia, conforme mostra a FIG.13.

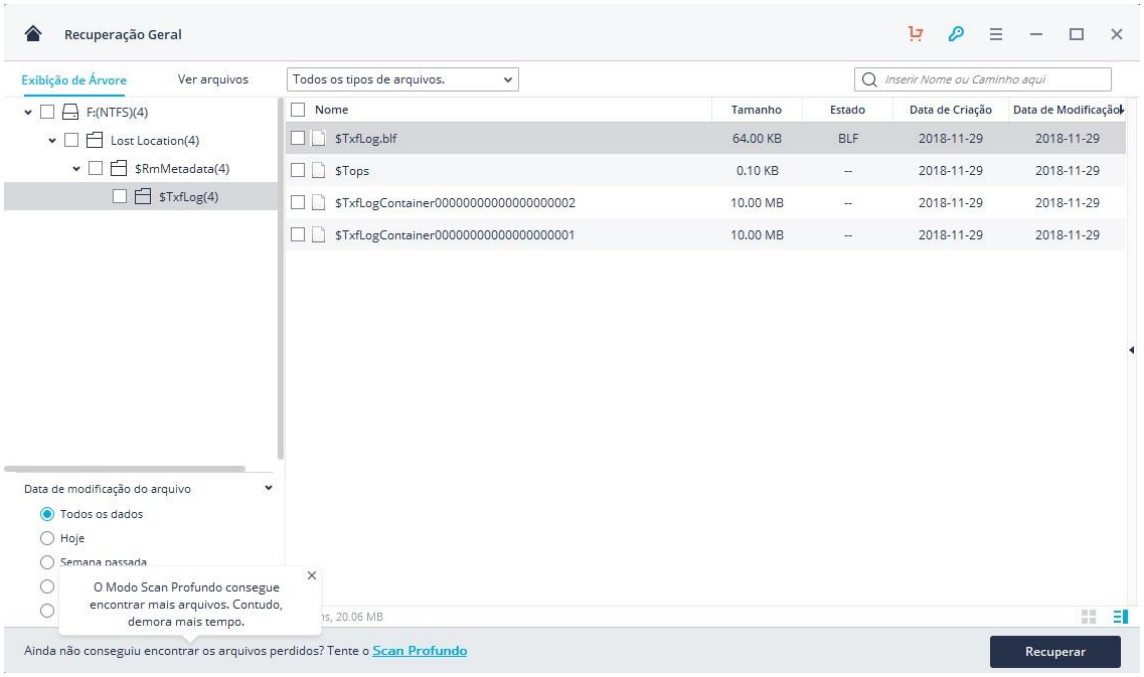
FIGURA 13 - Tela de exibição da análise final com FTK



Fonte: Autor

A mesma coisa ocorreu com a ferramenta *RecoverIt*, conforme mostra a FIG.14.

FIGURA 14 - Tela de exibição da análise final com *RecoverIt*



Fonte: Autor

Esse erro deve-se ao fato de ambas as ferramentas utilizarem a técnica de recuperação lógica dos arquivos.

Elas não conseguem recuperar arquivos em mídias que foram formatadas, pois quando são formatadas a tabela de partição da mídia é perdida, e como o método de recuperação lógica necessita desta tabela para realizar as recuperações, as ferramentas não conseguem recuperar os dados devido a criação de uma nova tabela.

3 ANÁLISE DE RESULTADOS

Com base nos resultados das seções 2.3.1, 2.3.2 e 2.3.3, estes foram confrontados em duas análises:

1. Na primeira análise serão comparados o tempo de execução gasto por ambas as ferramentas em cada seção.
2. Na segunda análise serão comparadas a porcentagem de dados recuperados, sendo comparados pelo tipo de dado.

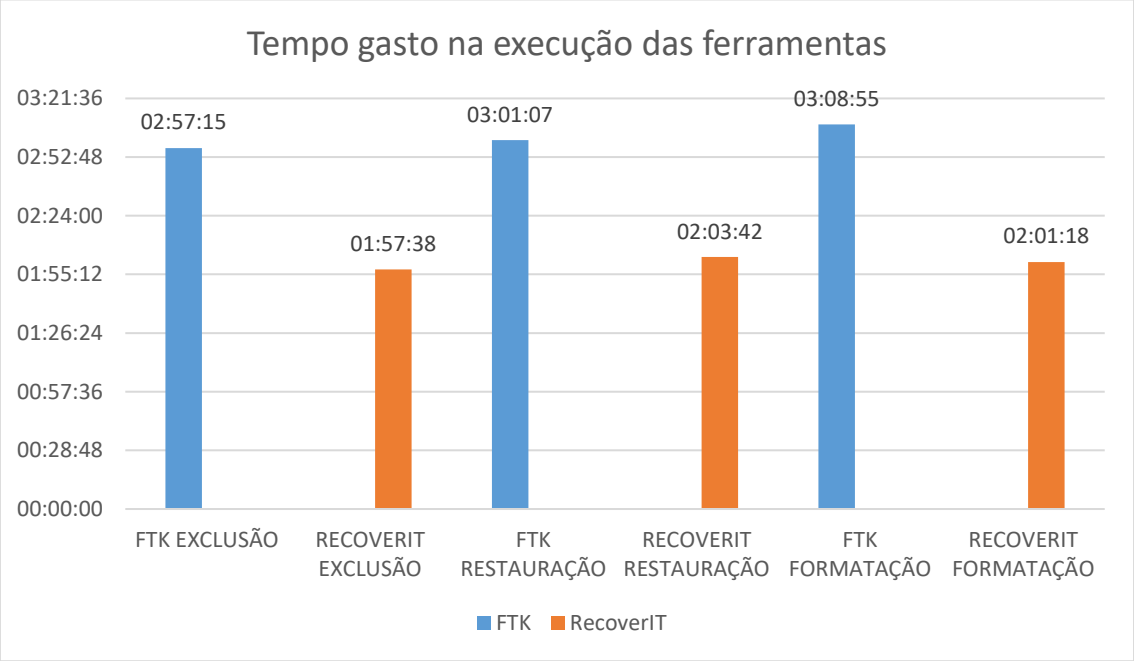
Analisando os resultados será possível concluir qual ferramenta apresentou o melhor resultado.

3.1 Primeira Análise: Análise do tempo de execução

A primeira análise consiste em confrontar o tempo gasto em cada uma das etapas executadas nas seções 2.3.1, 2.3.2 e 2.3.3. Ambas as ferramentas foram executadas de forma alternada, na mesma ordem descrita nas subseções da seção 2.3.

Elas foram executadas de forma alternada pois o dispositivo de mídia não suportaria a execução das duas simultaneamente, pois por ser um dispositivo de mídia mecânica, as ferramentas funcionando separadamente já fazem com que ele funcione em uma frequência alta. O tempo gasto na execução de cada ferramenta foi monitorado utilizando um cronômetro e está descrito a seguir no Gráfico 1 no formato h:m:s.

Gráfico 1 - Tempo gasto na execução das ferramentas



Fonte: Autor

Analisando o Gráfico 1, pode-se chegar à conclusão que a ferramenta *RecoverIt*, executa o processo de recuperação em tempo menor quando comparado com o tempo de execução da ferramenta FTK. Ambas as ferramentas percorrem byte por byte do dispositivo de mídia, o que chega a ser um processo custoso em tempo, dependendo da capacidade do dispositivo.

Por fim é possível inferir que a ferramenta *RecoverIt*, possui um tempo de resposta melhor do que a ferramenta FTK.

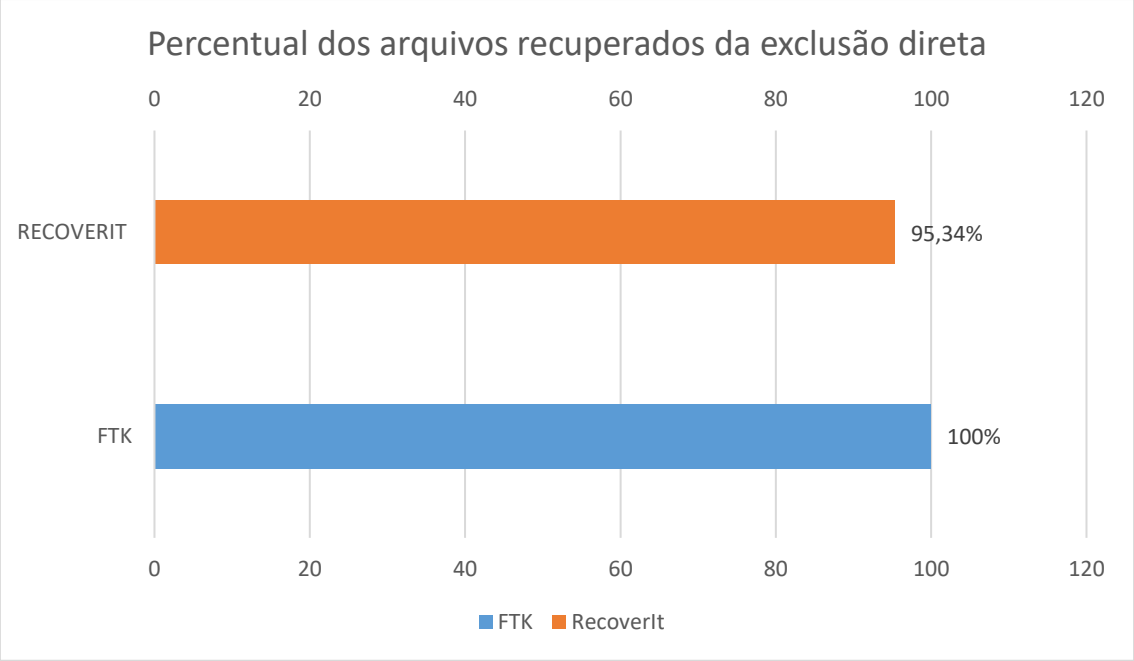
3.2 Segunda Análise: Análise da porcentagem de arquivos recuperados

A segunda análise consiste em confrontar a porcentagem em *bytes* de dados que foram recuperadas, utilizando gráficos para a comparação em relação aos métodos de recuperação utilizados que foram descritos nas seções 2.3.1, 2.3.2 e 2.3.3, e os dados coletados nos testes descritos nessas seções foram dispostos em uma tabela, e feito o uso da regra de 3 simples para chegar nas porcentagens exatas, que podem ser visualizadas nos gráficos presentes nas seções a seguir.

3.2.1 Análise da porcentagem de arquivos recuperados da exclusão direta

A partir dos testes realizados na seção 2.3.1, foi possível coletar os dados descritos na tabela presente no Apêndice B. Os dados coletados foram utilizados para gerar o Gráfico 2, que pode ser observado a seguir.

Gráfico 2 - Percentual dos arquivos recuperados da exclusão direta

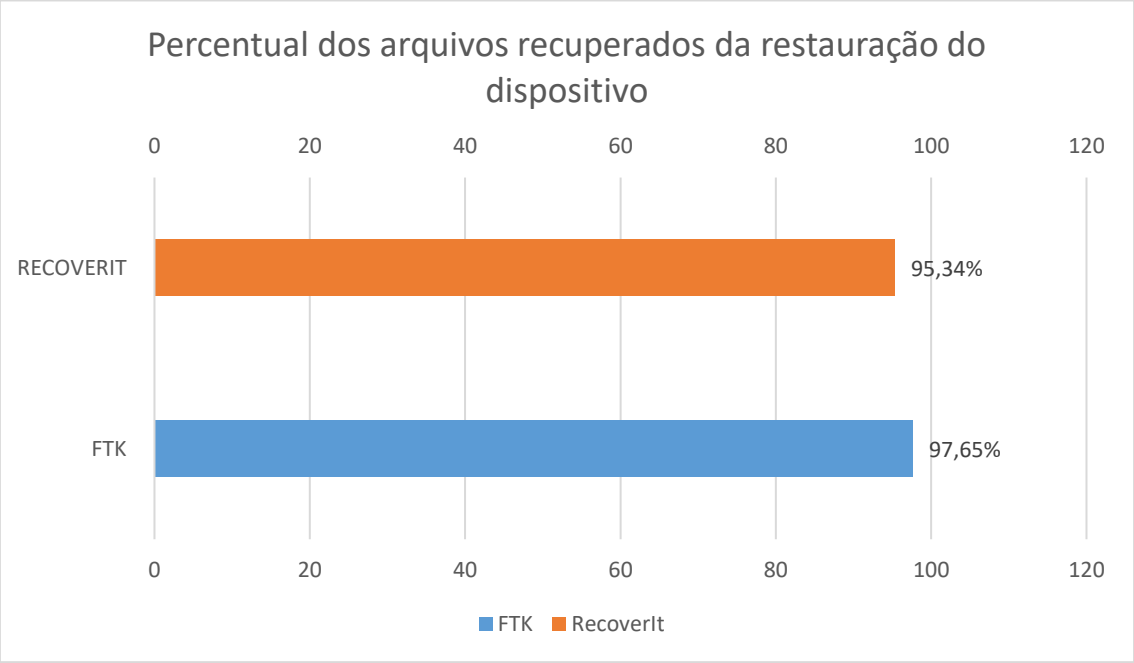


Fonte: Autor

3.2.2 Análise da porcentagem de arquivos recuperados da restauração do dispositivo

A partir dos testes realizados na seção 2.3.2, foi possível coletar os dados descritos na tabela presente no Apêndice C. Os dados coletados foram utilizados para gerar o Gráfico 3, que pode ser observado a seguir.

Gráfico 3 - Percentual dos arquivos recuperados da restauração do dispositivo



Fonte: Autor

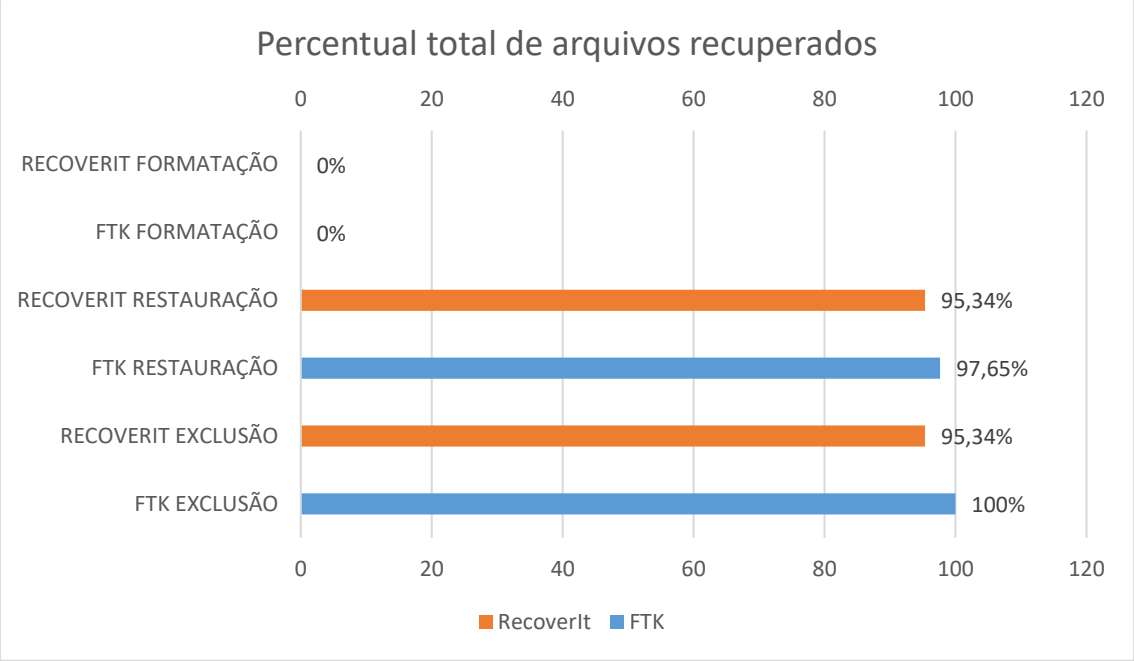
3.2.3 Análise da porcentagem de arquivos recuperados da formatação do dispositivo

Devido ao fato de ambas as ferramentas utilizarem o método de recuperação lógica, elas não são capazes de recuperar dados de dispositivos de mídia formatados devido ao fato da tabela de partição de mídia ser recriada do zero.

3.2.4 Análise da porcentagem total de arquivos recuperados

Contendo a comparação total de todos os arquivos recuperados em relação a cada ferramenta e aos métodos de execução citados nas subseções da seção 2.3, será apresentado no Gráfico 4 a seguir.

Gráfico 4 - Percentual total de arquivos recuperados



Fonte: Autor

Por fim diante dos resultados apresentados pelos gráficos da seção 3.2, pode-se chegar à conclusão que a ferramenta FTK apresentou os melhores resultados na recuperação dos arquivos em relação a ferramenta *RecoverIt*.

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 mídias digitais, levando em consideração o tempo gasto por cada ferramenta e o percentual de arquivos recuperados.

Ambas as ferramentas analisadas utilizavam a técnica de recuperação lógica, o que impossibilitou ambas de recuperarem os arquivos nos últimos testes, os testes de formatação do dispositivo.

Entretanto foi possível a chegar em uma conclusão acerca das ferramentas analisadas. Tendo em vista que, nesse estudo foi levado em consideração somente o valor do tamanho dos arquivos recuperados, chega-se à conclusão de que entre as ferramentas FTK e *RecoverIt* a ferramenta que apresentou um maior percentual de dados recuperados foi FKT. Já a ferramenta *RecoverIt* apresentou uma porcentagem menor de dados recuperados, mas seu tempo de resposta foi mais ágil em relação à FTK.

Chega-se à conclusão que a ferramenta *RecoverIt* é melhor indicada para uso em dispositivos pessoais e domésticos, por ser uma ferramenta com um tempo de resposta melhor em relação ao FTK, possuir uma instalação e interface prática, e também por ser de licença gratuita.

Já a ferramenta FTK recomenda-se o uso profissional, mesmo que possua um tempo de resposta mais custoso, sendo também um software de licença paga custando em média $3.995,00, ela dá uma garantia maior de retorno e devido a necessidade de que os dados apresentados à um tribunal oficial necessita de uma maior integridade. Sendo então a ferramenta FTK melhor indicada para os profissionais da área forense computacional.

TRABALHOS FUTUROS

- Efetuar a análise de cada dado recuperado, verificando se há arquivos corrompidos;
- Efetuar a análise de desempenho em outras formas de mídia de armazenamento;
- Analisar as ferramentas forenses de recuperação levando em consideração SO de *smartphones*;
- Efetuar a análise em um *hardware* de alto nível de desempenho, podendo executar as ferramentas de forma simultânea para uma melhor comparação;
- Efetuar uma análise semelhante a utilizada nesta pesquisa, utilizando diferentes ferramentas.

REFERÊNCIAS

ALTHEIDE, Cory; CARVEY, Harlan. Digital **Forensics with Open Source Tools**. 2011.

BLUM, Renato Opice. ***A era da tecnologia é também a era da insegurança*.** 2009. Disponível em: http://fenapef.org.br/20901/

CARRIER, Brian. **File System Forensic analysis**. 1 ed. Boston: Addison-Wesley, 2005.

ELEUTÉRIO, Pedro e MACHADO, Marcio. **Desvendando a Computação Forense**. 1a ed. Rio de Janeiro: Novatec Editora Ltda, 2011.

FREITAS, Andrey. **Perícia Forense Aplicada à Informatica**. 1ª ed. Brasport, 2007.

KENT, Karen. GRANCE, Timothy. CHEVALIER, Suzanne. DANG, Hung. **Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology.** Gaithersburg: NIST, 2006. Special Publication.

MOTA FILHO, João Eriberto. **Descobrindo o Linux: entenda o sistema operacional GNU/Linux.** 3 ed. São Paulo: Novatec Editora, 2012. 924 p.

PEREIRA, Evandro. FAGUNDES, Leonardo L.;NEUKAMP, Paulo; LUDWIG, Glauco; KONRATH, Marlon. Forense computacional: fundamentos, tecnologias e desafios atuais. In: **Forense Computacional: fundamentos, tecnologias e desafios atuais**, 2007.Disponível em: http://grsecurity.com.br/apostilas/forense/minicurso_forense.pdf

QUEIROZ, Claudemir e VARGAS, Raffael. **Investigação e Pericia Forense Computacional**. 1ª ed. Brasport, 2010.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. ***O problema na tipificação penal dos crimes virtuais*.** 2002. Disponível em: https://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais

ROSA, Fabrizio. **Crimes de Informática**. São Paulo: Bookseller, 2005.

VACCA, John R. Computer forensics: **Computer Crime Scene Investigation**. 2a ed. Boston: Charles River Media, 2005.

APÊNDICE A – TABELA DETALHADA REFERENTE AO TEMPO DE EXECUÇÃO TOTAL GASTO PELAS FERRAMENTAS

ANÁLISE EXECUTADA	TEMPO DE EXECUÇÃO	
FTK EXCLUSÃO	02:57:15	h
RECOVERIT EXCLUSÃO	01:57:38	h
FTK RESTAURAÇÃO	03:01:07	h
RECOVERIT RESTAURAÇÃO	02:03:42	h
FTK FORMATAÇÃO	03:08:55	h
RECOVERIT FORMATAÇÃO	02:01:18	h

APÊNDICE B – TABELA DETALHADA REFERENTE AO TAMANHO TOTAL DOS ARQUIVOS RECUPERADOS NA ANÁLISE DE EXCLUSÃO DIRETA

NOME	EXTENSÃO	TAMANHO REAL	FTK EXCLUSÃO	RECOVERIT EXCLUSÃO	
Audio (1)	.mp3	3.675.111	3.675.111	3.500.000	bytes
Audio (2)	.mp3	9.242.380	9.242.380	8.810.000	bytes
Audio (3)	.mp3	8.594.228	8.594.228	8.200.000	bytes
Audio (4)	.mp3	11.778.028	11.778.028	11.230.000	bytes
Audio (5)	.mp3	6.838.803	6.838.803	6.520.000	bytes
Audio (6)	.mp3	10.254.095	10.254.095	9.780.000	bytes
Audio (7)	.mp3	8.417.027	8.417.027	8.030.000	bytes
Audio (8)	.mp3	14.540.344	14.540.344	13.870.000	bytes
Audio (9)	.mp3	2.887.149	2.887.149	2.750.000	bytes
Audio (10)	.mp3	5.150.649	5.150.649	4.910.000	bytes
Audio (11)	.mp3	8.036.352	8.036.352	7.660.000	bytes
Audio (12)	.mp3	6.144.556	6.144.556	5.860.000	bytes
Audio (13)	.mp3	3.129.156	3.129.156	2.980.000	bytes
Audio (14)	.wma	2.927.740	2.927.740	2.790.000	bytes
Audio (15)	.wma	3.411.796	3.411.796	3.250.000	bytes
Audio (16)	.wma	6.154.919	6.154.919	5.870.000	bytes
Audio (17)	.wma	4.672.732	4.672.732	4.460.000	bytes
Audio (18)	.wma	4.487.476	4.487.476	4.280.000	bytes
Audio (19)	.wma	3.453.628	3.453.628	3.290.000	bytes
Audio (20)	.m4a	4.953.370	4.953.370	4.720.000	bytes
Compactado (1)	.zip	494.487	494.487	482.900	bytes
Compactado (2)	.zip	228.075	228.075	222.730	bytes
Compactado (3)	.zip	441.117	441.117	430.780	bytes
Compactado (4)	.zip	3.869.605	3.869.605	3.690.000	bytes
Compactado (5)	.zip	1.871.471	1.871.471	1.780.000	bytes
Compactado (6)	.zip	3.732.817	3.732.817	3.560.000	bytes
Compactado (7)	.zip	191.493	191.493	187.000	bytes
Compactado (8)	.zip	4.052.252	4.052.252	3.860.000	bytes
Compactado (9)	.zip	206.775	206.775	201.930	bytes
Compactado (10)	.zip	681.764	681.764	665.790	bytes
Compactado (11)	.zip	204.589	204.589	199.790	bytes
Compactado (12)	.zip	4.355.546	4.355.546	4.150.000	bytes
Compactado (13)	.zip	9.858.899	9.858.899	9.400.000	bytes
Compactado (14)	.rar	209.061	209.061	204.160	bytes

Compactado (15)	.rar	472.274	472.274	461.210	bytes
Compactado (16)	.rar	5.493.895	5.493.895	5.240.000	bytes
Compactado (17)	.rar	925.553.255	925.553.255	882.680.000	bytes
Compactado (18)	.rar	1.063.057	1.063.057	1.010.000	bytes
Compactado (19)	.rar	4.377.355	4.377.355	4.170.000	bytes
Compactado (20)	.rar	681.562	681.562	665.590	bytes
Documento (1)	.pdf	346.979	346.979	338.850	bytes
Documento (2)	.pdf	685.955	685.955	669.880	bytes
Documento (3)	.pdf	197.909	197.909	193.270	bytes
Documento (4)	.pdf	424.302	424.302	414.360	bytes
Documento (5)	.pdf	1.204.138	1.204.138	1.150.000	bytes
Documento (6)	.pdf	3.781.889	3.781.889	3.610.000	bytes
Documento (7)	.pdf	2.613.318	2.613.318	2.490.000	bytes
Documento (8)	.pdf	192.719	192.719	188.200	bytes
Documento (9)	.pdf	439.145	439.145	428.850	bytes
Documento (10)	.docx	13.810	13.810	13.490	bytes
Documento (11)	.log	91.048	91.048	88.910	bytes
Documento (12)	.txt	73.729	73.729	72.000	bytes
Documento (13)	.log	192.949	192.949	188.430	bytes
Documento (14)	.docx	70.386	70.386	68.740	bytes
Documento (15)	.doc	321.536	321.536	314.000	bytes
Documento (16)	.xml	79.649	79.649	77.780	bytes
Documento (17)	.xml	78.527	78.527	76.690	bytes
Documento (18)	.rtf	689.922	689.922	673.750	bytes
Documento (19)	.xlsx	1.689.148	1.689.148	1.610.000	bytes
Documento (20)	.xlsx	1.684.026	1.684.026	1.610.000	bytes
Executavel (1)	.exe	4.030.976	4.030.976	3.840.000	bytes
Executavel (2)	.exe	1.090.024	1.090.024	1.040.000	bytes
Executavel (3)	.exe	285.144.256	285.144.256	271.930.000	bytes
Executavel (4)	.exe	11.205.832	11.205.832	10.690.000	bytes
Executavel (5)	.exe	60.074.328	60.074.328	57.290.000	bytes
Executavel (6)	.exe	46.954.408	46.954.408	44.780.000	bytes
Executavel (7)	.exe	120.147.968	120.147.968	114.580.000	bytes
Executavel (8)	.exe	81.400.776	81.400.776	77.630.000	bytes
Executavel (9)	.exe	341.868.448	341.868.448	326.030.000	bytes
Executavel (10)	.exe	118.582.104	118.582.104	113.090.000	bytes
Executavel (11)	.exe	230.883.184	230.883.184	220.190.000	bytes
Executavel (12)	.exe	1.404.640	1.404.640	1.340.000	bytes
Executavel (13)	.exe	1.446.792	1.446.792	1.380.000	bytes
Executavel (14)	.exe	82.312.496	82.312.496	78.500.000	bytes
Executavel (15)	.exe	8.412.624	8.412.624	8.020.000	bytes
Executavel (16)	.exe	73.979.080	73.979.080	70.550.000	bytes
Executavel (17)	.exe	2.370.560	2.370.560	2.260.000	bytes
Executavel (18)	.exe	123.669.848	123.669.848	117.940.000	bytes
Executavel (19)	.exe	38.911.168	38.911.168	37.110.000	bytes

Executavel (20)	.exe	3.766.296	3.766.296	3.590.000	bytes
Imagem (1)	.jpg	772.845	772.845	754.730	bytes
Imagem (2)	.jpg	568.460	568.460	555.140	bytes
Imagem (3)	.jpg	612.728	612.728	598.370	bytes
Imagem (4)	.jpg	409.835	409.835	400.230	bytes
Imagem (5)	.jpg	210.647	210.647	205.710	bytes
Imagem (6)	.jpg	565.617	565.617	552.360	bytes
Imagem (7)	.jpg	153.204	153.204	149.610	bytes
Imagem (8)	.jpg	165.786	165.786	161.900	bytes
Imagem (9)	.jpg	109.976	109.976	107.400	bytes
Imagem (10)	.png	315.096	315.096	307.710	bytes
Imagem (11)	.png	137.163	137.163	133.950	bytes
Imagem (12)	.png	1.060.507	1.060.507	1.010.000	bytes
Imagem (13)	.png	1.058.290	1.058.290	1.010.000	bytes
Imagem (14)	.gif	1.131.169	1.131.169	1.080.000	bytes
Imagem (15)	.gif	195.450	195.450	190.870	bytes
Imagem (16)	.gif	215.512	215.512	210.460	bytes
Imagem (17)	.gif	223.813	223.813	218.570	bytes
Imagem (18)	.gif	193.664	193.664	189.120	bytes
Imagem (19)	.jpeg	102.057	102.057	99.670	bytes
Imagem (20)	.jpeg	196.902	196.902	192.290	bytes
Video (1)	.mp4	3.415.981	3.415.981	3.260.000	bytes
Video (2)	.mp4	92.400.005	92.400.005	88.120.000	bytes
Video (3)	.mp4	91.256.099	91.256.099	87.030.000	bytes
Video (4)	.mp4	420.293.294	420.293.294	400.820.000	bytes
Video (5)	.mp4	8.280.369	8.280.369	7.900.000	bytes
Video (6)	.mp4	13.397.681	13.397.681	12.780.000	bytes
Video (7)	.mp4	1.155.756	1.155.756	1.100.000	bytes
Video (8)	.mp4	18.959.281	18.959.281	18.080.000	bytes
Video (9)	.rmvb	170.354.238	170.354.238	162.460.000	bytes
Video (10)	.rmvb	143.580.283	143.580.283	136.930.000	bytes
Video (11)	.rmvb	73.207.715	73.207.715	69.820.000	bytes
Video (12)	.wmv	256.973.357	256.973.357	245.070.000	bytes
Video (13)	.wmv	14.806.653	14.806.653	14.120.000	bytes
Video (14)	.3gp	9.782.246	9.782.246	9.330.000	bytes
Video (15)	.3gp	9.369.061	9.369.061	8.940.000	bytes
Video (16)	.3gp	12.982.917	12.982.917	12.380.000	bytes
Video (17)	.3gp	6.830.621	6.830.621	6.510.000	bytes
Video (18)	.avi	20.751.872	20.751.872	19.790.000	bytes
Video (19)	.avi	134.502.400	134.502.400	126.900.000	bytes
Video (20)	.avi	133.064.704	133.064.704	126.900.000	bytes
TOTAL		4.393.079.034	4.393.079.034	4.188.447.170	bytes

APÊNDICE C – TABELA DETALHADA REFERENTE AO TAMANHO TOTAL DOS ARQUIVOS RECUPERADOS NA ANÁLISE DE RESTAURAÇÃO DO DISPOSITIVO

NOME	EXTENSÃO	TAMANHO REAL	FTK EXCLUSÃO	RECOVERIT EXCLUSÃO	
Audio (1)	.mp3	3.675.111	3.589.000	3.500.000	bytes
Audio (2)	.mp3	9.242.380	9.026.000	8.810.000	bytes
Audio (3)	.mp3	8.594.228	8.393.000	8.200.000	bytes
Audio (4)	.mp3	11.778.028	11.502.000	11.230.000	bytes
Audio (5)	.mp3	6.838.803	6.679.000	6.520.000	bytes
Audio (6)	.mp3	10.254.095	10.014.000	9.780.000	bytes
Audio (7)	.mp3	8.417.027	8.220.000	8.030.000	bytes
Audio (8)	.mp3	14.540.344	14.200.000	13.870.000	bytes
Audio (9)	.mp3	2.887.149	2.820.000	2.750.000	bytes
Audio (10)	.mp3	5.150.649	5.030.000	4.910.000	bytes
Audio (11)	.mp3	8.036.352	7.848.000	7.660.000	bytes
Audio (12)	.mp3	6.144.556	6.001.000	5.860.000	bytes
Audio (13)	.mp3	3.129.156	3.056.000	2.980.000	bytes
Audio (14)	.wma	2.927.740	2.860.000	2.790.000	bytes
Audio (15)	.wma	3.411.796	3.332.000	3.250.000	bytes
Audio (16)	.wma	6.154.919	6.011.000	5.870.000	bytes
Audio (17)	.wma	4.672.732	4.564.000	4.460.000	bytes
Audio (18)	.wma	4.487.476	4.383.000	4.280.000	bytes
Audio (19)	.wma	3.453.628	3.373.000	3.290.000	bytes
Audio (20)	.m4a	4.953.370	4.838.000	4.720.000	bytes
Compactado (1)	.zip	494.487	483.000	482.900	bytes
Compactado (2)	.zip	228.075	223.000	222.730	bytes
Compactado (3)	.zip	441.117	431.000	430.780	bytes
Compactado (4)	.zip	3.869.605	3.779.000	3.690.000	bytes
Compactado (5)	.zip	1.871.471	1.828.000	1.780.000	bytes
Compactado (6)	.zip	3.732.817	3.646.000	3.560.000	bytes
Compactado (7)	.zip	191.493	188.000	187.000	bytes
Compactado (8)	.zip	4.052.252	3.958.000	3.860.000	bytes
Compactado (9)	.zip	206.775	202.000	201.930	bytes
Compactado (10)	.zip	681.764	666.000	665.790	bytes
Compactado (11)	.zip	204.589	200.000	199.790	bytes
Compactado (12)	.zip	4.355.546	4.254.000	4.150.000	bytes
Compactado (13)	.zip	9.858.899	9.628.000	9.400.000	bytes
Compactado (14)	.rar	209.061	205.000	204.160	bytes
Compactado (15)	.rar	472.274	462.000	461.210	bytes

Compactado (16)	.rar	5.493.895	5.366.000	5.240.000	bytes
Compactado (17)	.rar	925.553.255	903.861.000	882.680.000	bytes
Compactado (18)	.rar	1.063.057	1.039.000	1.010.000	bytes
Compactado (19)	.rar	4.377.355	4.275.000	4.170.000	bytes
Compactado (20)	.rar	681.562	666.000	665.590	bytes
Documento (1)	.pdf	346.979	339.000	338.850	bytes
Documento (2)	.pdf	685.955	670.000	669.880	bytes
Documento (3)	.pdf	197.909	194.000	193.270	bytes
Documento (4)	.pdf	424.302	415.000	414.360	bytes
Documento (5)	.pdf	1.204.138	1.176.000	1.150.000	bytes
Documento (6)	.pdf	3.781.889	3.694.000	3.610.000	bytes
Documento (7)	.pdf	2.613.318	2.553.000	2.490.000	bytes
Documento (8)	.pdf	192.719	189.000	188.200	bytes
Documento (9)	.pdf	439.145	429.000	428.850	bytes
Documento (10)	.docx	13.810	13.800	13.490	bytes
Documento (11)	.log	91.048	89.000	88.910	bytes
Documento (12)	.txt	73.729	73.000	72.000	bytes
Documento (13)	.log	192.949	189.000	188.430	bytes
Documento (14)	.docx	70.386	69.000	68.740	bytes
Documento (15)	.doc	321.536	314.000	314.000	bytes
Documento (16)	.xml	79.649	78.000	77.780	bytes
Documento (17)	.xml	78.527	77.000	76.690	bytes
Documento (18)	.rtf	689.922	674.000	673.750	bytes
Documento (19)	.xlsx	1.689.148	1.650.000	1.610.000	bytes
Documento (20)	.xlsx	1.684.026	1.645.000	1.610.000	bytes
Executavel (1)	.exe	4.030.976	3.937.000	3.840.000	bytes
Executavel (2)	.exe	1.090.024	1.065.000	1.040.000	bytes
Executavel (3)	.exe	285.144.256	278.462.000	271.930.000	bytes
Executavel (4)	.exe	11.205.832	10.944.000	10.690.000	bytes
Executavel (5)	.exe	60.074.328	58.667.000	57.290.000	bytes
Executavel (6)	.exe	46.954.408	45.854.000	44.780.000	bytes
Executavel (7)	.exe	120.147.968	117.332.000	114.580.000	bytes
Executavel (8)	.exe	81.400.776	79.493.000	77.630.000	bytes
Executavel (9)	.exe	341.868.448	333.856.000	326.030.000	bytes
Executavel (10)	.exe	118.582.104	115.803.000	113.090.000	bytes
Executavel (11)	.exe	230.883.184	225.472.000	220.190.000	bytes
Executavel (12)	.exe	1.404.640	1.372.000	1.340.000	bytes
Executavel (13)	.exe	1.446.792	1.413.000	1.380.000	bytes
Executavel (14)	.exe	82.312.496	80.384.000	78.500.000	bytes
Executavel (15)	.exe	8.412.624	8.216.000	8.020.000	bytes
Executavel (16)	.exe	73.979.080	72.246.000	70.550.000	bytes
Executavel (17)	.exe	2.370.560	2.315.000	2.260.000	bytes
Executavel (18)	.exe	123.669.848	120.772.000	117.940.000	bytes
Executavel (19)	.exe	38.911.168	38.000.000	37.110.000	bytes
Executavel (20)	.exe	3.766.296	3.679.000	3.590.000	bytes

Imagem (1)	.jpg	772.845	755.000	754.730	bytes
Imagem (2)	.jpg	568.460	556.000	555.140	bytes
Imagem (3)	.jpg	612.728	599.000	598.370	bytes
Imagem (4)	.jpg	409.835	401.000	400.230	bytes
Imagem (5)	.jpg	210.647	206.000	205.710	bytes
Imagem (6)	.jpg	565.617	553.000	552.360	bytes
Imagem (7)	.jpg	153.204	150.000	149.610	bytes
Imagem (8)	.jpg	165.786	162.000	161.900	bytes
Imagem (9)	.jpg	109.976	108.000	107.400	bytes
Imagem (10)	.png	315.096	308.000	307.710	bytes
Imagem (11)	.png	137.163	134.000	133.950	bytes
Imagem (12)	.png	1.060.507	1.036.000	1.010.000	bytes
Imagem (13)	.png	1.058.290	1.034.000	1.010.000	bytes
Imagem (14)	.gif	1.131.169	1.105.000	1.080.000	bytes
Imagem (15)	.gif	195.450	191.000	190.870	bytes
Imagem (16)	.gif	215.512	211.000	210.460	bytes
Imagem (17)	.gif	223.813	219.000	218.570	bytes
Imagem (18)	.gif	193.664	190.000	189.120	bytes
Imagem (19)	.jpeg	102.057	100.000	99.670	bytes
Imagem (20)	.jpeg	196.902	193.000	192.290	bytes
Video (1)	.mp4	3.415.981	3.336.000	3.260.000	bytes
Video (2)	.mp4	92.400.005	90.235.000	88.120.000	bytes
Video (3)	.mp4	91.256.099	89.118.000	87.030.000	bytes
Video (4)	.mp4	420.293.294	410.443.000	400.820.000	bytes
Video (5)	.mp4	8.280.369	8.087.000	7.900.000	bytes
Video (6)	.mp4	13.397.681	13.084.000	12.780.000	bytes
Video (7)	.mp4	1.155.756	1.129.000	1.100.000	bytes
Video (8)	.mp4	18.959.281	18.515.000	18.080.000	bytes
Video (9)	.rmvb	170.354.238	166.362.000	162.460.000	bytes
Video (10)	.rmvb	143.580.283	140.216.000	136.930.000	bytes
Video (11)	.rmvb	73.207.715	71.492.000	69.820.000	bytes
Video (12)	.wmv	256.973.357	250.951.000	245.070.000	bytes
Video (13)	.wmv	14.806.653	14.460.000	14.120.000	bytes
Video (14)	.3gp	9.782.246	9.553.000	9.330.000	bytes
Video (15)	.3gp	9.369.061	9.150.000	8.940.000	bytes
Video (16)	.3gp	12.982.917	12.679.000	12.380.000	bytes
Video (17)	.3gp	6.830.621	6.671.000	6.510.000	bytes
Video (18)	.avi	20.751.872	20.266.000	19.790.000	bytes
Video (19)	.avi	134.502.400	131.350.000	126.900.000	bytes
Video (20)	.avi	133.064.704	129.946.000	126.900.000	bytes
TOTAL		4.393.079.034	4.290.165.800	4.188.447.170	bytes