**UNIVERSIDADE DO SAGRADO CORAÇÃO**

**ÉDER LOURENÇO**

# ESTUDO COMPARATIVO ENTRE SOFTWARES LIVRES PARA PERÍCIA FORENSE BASEADOS EM LINUX

BAURU
2013

**ÉDER LOURENÇO**

# ESTUDO COMPARATIVO ENTRE SOFTWARES LIVRES PARA PERÍCIA FORENSE BASEADOS EM LINUX

Trabalho de Conclusão de Curso, apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título em bacharel em Ciência da Computação sob orientação do Prof. Esp. Henrique Pachioni Martins.

BAURU
2013

Lourenço, Eder
L982e

Estudo comparativo entre softwares livres para perícia forense baseados em Linux / Eder Lourenço -- 2013.
145f. : il.

Orientador: Prof. Esp. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Informação. 2. Segurança da informação. 3. Perícia forense. 4. Software livre. I. Martins, Henrique Pachioni. II. Título.

**ÉDER LOURENÇO**

# ESTUDO COMPARATIVO ENTRE SOFTWARES LIVRES PARA PERÍCIA FORENSE BASEADOS EM LINUX

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título em Bacharel em Ciência da Computação sob orientação do Profº Esp. Henrique Pachioni Martins.

Banca examinadora:

_____
Prof. Esp. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

_____
Prof. Ms. Patrick Pedreira Silva
Universidade do Sagrado Coração

Bauru, 4 de dezembro de 2013.

## AGRADECIMENTOS

Agradeço a todos os amigos que fiz durante o curso de Ciência da Computação, a atenção dos professores durante o curso em especial ao Prof. Esp. Henrique Martins pela paciência e pelo incentivo nas dificuldades que tive durante a pesquisa. A minha família pelo apoio nos momentos bons e também nos momentos difíceis, sempre me incentivando e me mostrando a importância dos estudos na nossa vida. A minha tia Neuza com muita saudade. E também agradeço a Deus por todas coisas boas que tem feito por mim.

## RESUMO

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação. Confidencialidade, Integridade e Disponibilidade representam atualmente, os principais atributos que orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Por isso é cada vez mais necessário para profissionais da área de computação sejam organizações públicas e privadas o domínio de técnicas de análise forense, aplicadas no âmbito computacional. A análise forense computacional consiste em um conjunto de técnicas para coleta e exame de evidências digitais, reconstrução de dados e ataques, identificação e rastreamento de invasores. Hoje em dia há diversos softwares livres baseados em Linux disponíveis para pericia e com diversas ferramentas disponíveis para análise forense computacional. Entre elas podemos citar o BackTrack 5 R3, CAINE 4.0 Pulsar e o FDTK 3.0 e que serão descritas neste trabalho.



**Palavras-chave:** Informação. Segurança da Informação. Perícia Forense. Software Livre.

## ABSTRACT

Shall mean all information and any content or data that has value for any organization or person. It can be stored for restricted use or exposed to the public for inspection or purchase. The security of certain information can be affected by behavior and use of those factors it uses, the environment or infrastructure that the fence or by malicious people who aim to steal, destroy or modify such information. Confidentiality, Integrity and Availability currently represent the main attributes that guide the analysis, planning and implementation of security for a given set of information to be protected. So it is increasingly necessary for computing professionals in both public and private domain of technical forensics organizations, applied in the computational framework. The computer forensics is a set of techniques for collection and examination of digital evidence, data and reconstruction attacks, identification and tracking of intruders. Nowadays there are many free software available for Linux-based and skill with various tools available to computer forensics. Among them we can mention the Backtrack 5 R3, Pulsar and FDTK CAINE 4.0 and 3.0 which are described in this paper.



**Keywords**: Information. Information Security. Forensics. Free Software.

## LISTA DE ILUSTRAÇÕES

**SUMÁRIO**

# 1 INTRODUÇÃO

Na atualidade, um dos bens mais importantes que temos, sem dúvida nenhuma, é a informação. A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias e, portanto, a proteção e segurança destes dados é muito importante. (BASTO, 2012).

A segurança da informação é um conjunto de medidas constituídas basicamente de controles e da política de segurança objetivando a proteção das informações dos clientes e da empresa a fim de garantir a continuidade do negócio e minimizar os riscos de revelação ou alteração por pessoas não autorizadas. (LINS, 2009). A segurança está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou para uma organização. Possui alguns aspectos básicos de confidencialidade, integridade e disponibilidade da informação que ajuda a entender as necessidades de sua proteção e que não se aplica ou está restrita a sistemas computacionais, nem a informações eletrônicas ou qualquer outra forma mecânica de armazenamento, ela se aplica a todos os aspectos de proteção e armazenamento de informações e dados, em qualquer forma lógica ou física, em trafego, processamento ou armazenado. (CAMPOS, 2006).

Existem hoje, diversos sistemas operacionais baseados em Linux e Software Livre, desenvolvidos exclusivamente para profissionais e estudiosos de Segurança da Informação e Computação Forense. Os sistemas possuem ferramentas e aplicativos exclusivos para realização de testes, análises e atividades da área, tais como: recuperação de arquivos apagados, analisadores de logs do sistema e programas, engenharia reversa, testes de invasão, vasculhador de tarefas executadas no sistema, analisador de protocolos enviados e recebidos na rede, programas de força bruta para quebrar senhas, entre outras coisas. Nesta era, em que estamos conectados em todos os lugares, os problemas e incidentes tendem a aumentar. (BASTO, 2012). Esse trabalho tem por objetivo utilizar as ferramentas gratuitas de pericia forense baseadas em Linux e testar suas ferramentas para análise além de colaborar com área de pericia forense e com os peritos a ter um comparativo entre os softwares Linux disponíveis.

## 2 JUSTIFICATIVA

Atualmente existem diversos softwares que reúnem ferramentas e um conjunto de aplicativos customizados para profissionais da área de segurança da informação e também para usuários  e que podem ser utilizados para pericia forense computacional. Com isso a utilização de ferramentas que auxiliam e dão suporte à investigação é de suma importância, pois estas conseguem garimpar informações de forma eficaz e ágil, primando pela integridade e minimizando os riscos da perda de dados.

# 3 OBJETIVOS

## 3.1 GERAL

O objetivo desse trabalho é apresentar e testar o funcionamento de diferentes softwares de pericia forense, no intuito de demonstrar as características desses softwares e demonstrar uma comparação entre elas.

## 3.2 ESPECÍFICOS

- Pesquisar referencias bibliográficas sobre ferramentas forenses;
- Estudar diferentes softwares livres para pericia forense e suas ferramentas disponíveis;
- Configurar os diferentes softwares utilizando uma máquina virtual
- Testar e descrever as principais funcionalidades de cada software**;**
- Fazer um comparativo entre as ferramentas utilizadas.

# 4 FUNDAMENTAÇÃO TEÓRICA

## 4.1 INFORMAÇÃO

O conceito de informação deriva do latim e significa um processo de comunicação ou algo relacionado com comunicação. (ZHANG, 1988). Mas na realidade existem muitas e variadas definições de informação, cada uma mais complexa que outra. Ainda segundo o Aurélio (1995), informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza. A informação tornou-se uma necessidade crescente para qualquer setor da atividade humana e é indispensável mesmo que a sua procura não seja ordenada ou sistemática, mas resultante apenas de decisões casuísticas ou intuitivas.

## 4.2 ETAPAS DO CICLO DE VIDA DA INFORMAÇÃO

De acordo com Sêmola (2003) estágios do ciclo de vida da informação são os seguintes:

- **Manuseio**: É o momento em é criada e manipulada seja, por exemplo, ao digitar informações recém-geradas em uma aplicação internet, ou, ainda, ao utilizar sua senha de acesso para autenticação;
- **Armazenamento**: É o momento no qual a informação é armazenada seja em um banco de dados compartilhado, mídia removível como, por exemplo, um pen drive, e posteriormente depositada na gaveta da mesa de trabalho;
- **Transporte**: Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico, telefone, ofícios, telegramas, etc;
- **Descarte**: Momento em que a informação é descartada, seja ao depositar na lixeira da um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa.

## 4.3 SEGURANÇA DA INFORMAÇÃO

Segurança de Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. O conceito de segurança se aplica a todos os aspectos de proteção de informações e dados, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si. Sêmola (2003) define Segurança da Informação como a área de conhecimento que se dedica à proteção de ativos da informação contra acessos não autorizados e alterações indevidas. Segundo Abrahão (2003), a Segurança da informação é alcançada a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais ou ainda funções de software. De acordo com a norma ABNT NBR ISO/IEC 27002, 2005, alguns princípios básicos devem ser respeitados para que se possa garantir a segurança da informação:

- **Confidencialidade:** significa que a informação deve ser protegida contra sua divulgação para pessoas não autorizadas – interna ou externamente. Assegurar que a informação só pode ser acessada por pessoas autorizadas;
- **Integridade:** consiste em garantir que a informação gerada não será modificada sem a devida autorização da(s) pessoa(s) responsáveis por ela. Com isso garante que a informação efetivamente foi criada ou manipulada por quem reivindica sua autoria como, por exemplo, uso de uma senha de acesso.
- **Autenticidade:** o controle de autenticidade está ligado ao fato da informação que esteja sendo trafegada seja de fato originada do proprietário a ela relacionado. Não deve ser permitida a violação da origem da informação.
- **Disponibilidade:** Consiste em garantir que a informação esteja disponível às pessoas autorizadas sem nenhum tipo de modificação e sempre que elas necessitarem. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

## 4.4 Pericia Forense Aplicada A Informática

De acordo com o Mini Dicionário Aurélio (2010, p. 579, grifo nosso) a palavra pericia significa "*habilidade, destreza, conhecimento, ciência*", como também "*vistoria ou exame de caráter técnico e especializado*". Já a palavra forense de acordo com o Mini Dicionário Aurélio (2010, p. 357, grifo nosso) significa "Que se refere ao foro judicial" ou "relativo aos tribunais". Dessa forma, a técnica forense diz respeito à aplicação de recursos científicos em um processo jurídico, sendo que essas práticas valem-se da perícia para alcançar os objetivos de prova, visto que muitas provas não são perceptíveis a olho nu nem estão disponíveis a pessoas desprovidas de conhecimentos técnicos necessários.

A Perícia Forense Aplicada à Informática, também é referenciada como computação forense, forense computacional, criminalística computacional, forense digital, investigação eletrônica e perícia eletrônica, é a aplicação de conhecimentos em informática e técnicas de investigação com a finalidade de obtenção de evidências. (FREITAS, 2006).

Para Bustamante (2006), a perícia forense pode ser definida como coleção e análise de dados de um computador, sistema, rede ou dispositivos de armazenamento, de forma que sejam admitidos em juízo, sendo que as evidências que um criminalista ou expert (também chamado perito) encontra geralmente não podem ser vistas a olho nu, dependendo de ferramentas e meios para a sua obtenção.

Nesse contexto, cabe ao profissional de informática coletar as evidências e produzir um laudo pericial com as evidências e técnicas abordadas na coleta. Para que o perito conduza uma análise forense computacional de maneira eficaz é necessário que ele tenha uma série de habilidades, como, por exemplo, raciocínio lógico, mente aberta e o entendimento das relações de causa e efeito. Todas essas habilidades (que são encontradas nos programadores) são utilizadas durante a busca de um erro em um programa. (REIS; GEUS, 2001).

## 4.5 Procedimentos Para Pericia Forense

De acordo com Huebner (2007), a primeira coisa de que um investigador deve estar ciente é sobre o Princípio da Troca de Locard, segundo o qual qualquer pessoa ou coisa entrando em uma cena de crime leva algo da cena consigo ou deixa algo de si para trás quando sai da cena. Nesse sentido, um princípio básico é o da preservação dos vestígios originais. Os padrões metodológicos seguem o princípio de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiabilidade e a precisão das evidências.

A Computação Forense faz parte de um processo investigativo, que tem com objetivo provar os fatos ocorridos com a maior clareza possível. Para que isso ocorra o perito que for nomeado para realizar a perícia deve trabalhar de uma forma sistemática e cuidadosa com as evidências com o intuito de sempre preservar a integridade dos dados e detalhar toda a atividade executada no laudo final. Todo esse processo pericial na forense computacional é divido em quatro etapas conforme a seguir:

- **Coleta de dados**: É considerada a etapa mais importante de todo o processo, ou seja, a que mais precisa de cuidados. É nessa etapa que os dados serão coletados, sendo necessário cuidado especial para manter a integridade das informações. Outras atividades que são realizadas nesta etapa são relacionadas ao equipamento questionado, que deve ser identificado, devidamente embalado de uma forma segura, etiquetado as suas partes e suas identificações registradas no documento de cadeia de custódia;
- **Exame dos dados**: nesta segunda etapa o objetivo principal é separar as informações relevantes ao caso de outras sem importância, como os arquivos do próprio sistema. Nesta fase, deve-se identificar, extrair, filtrar e documentar os dados relevantes à apuração. Antes de iniciar o processo é preciso definir quais as ferramentas que serão utilizadas para o exame dos dados.
- **Análise das Informações**: nesta fase todas as informações anteriormente separadas serão analisadas com o intuito de encontrar dados úteis e

relevantes que auxiliem na investigação do caso para que assim seja possível realizar a conclusão;

- **Interpretação dos resultados**: nesta última etapa, o objetivo é apresentar um laudo que deve informar com toda a veracidade possível o que foi encontrado nos dados analisados. Neste laudo deve-se também relatar todas as ferramentas e documentos utilizados. (FREITAS, 2006).

De acordo com o descrito nas etapas anteriormente apresentadas, a Figura 1 demonstra de forma gráfica como é todo o processo de investigação em computação forense.

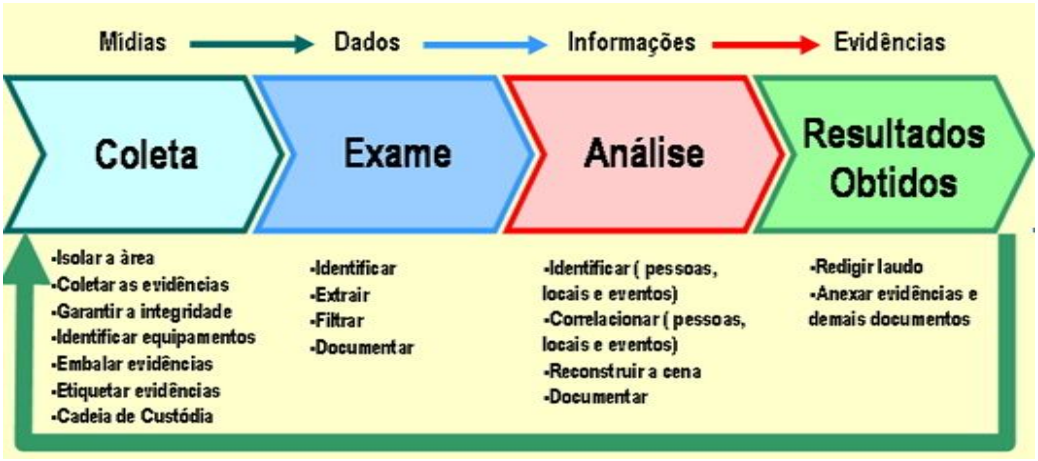
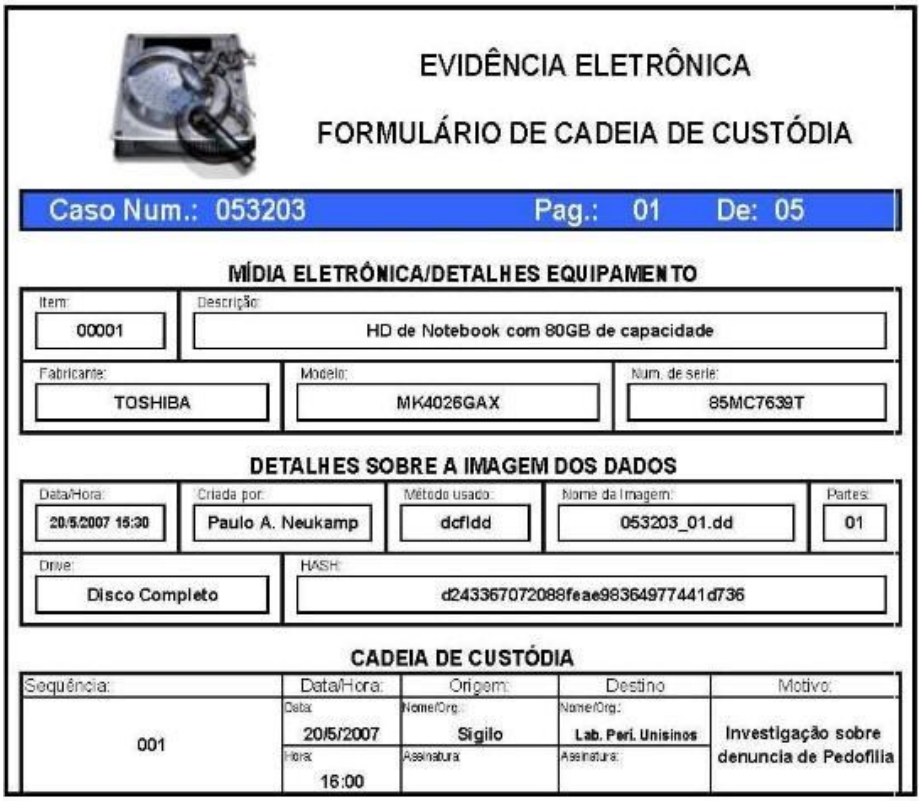



Figura 1 - Fases do processo de investigação.
Fonte: Autores Della Vecchia, E.; Fagundes, L.; Neukamp, P.; Ludwig, G.; Konrath, M (2007).
**VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (2007).**

## 4.6 Cadeia de Custódia

A cadeia de custódia trata dos procedimentos que buscam garantir a idoneidade das evidências através da descrição e documentação detalhada de como a evidência foi encontrada e de como foi tratada dali por diante. Devido ao usual exercício do contraditório, a defesa poderá questionar no tribunal a legitimidade dos resultados da investigação, alegando que as evidências foram alteradas ou substituídas por outras. Devido à importância das evidências, é indispensável que o perito mantenha a cadeia de custódia. (FREITAS, 2006).

A cadeia de custódia prova onde as evidências estavam em um determinado momento e quem era o responsável por ela durante o curso da perícia. Ao documentar estas informações, você poderá determinar que a integridade das suas evidências não foi comprometida. A cada vez que as evidências passarem de uma pessoa para outra ou de um tipo de mídia para outro, a transação deverá ser registrada. Ao final deverá ser incluído um formulário de cadeia de custódia que será a documentação oficial quanto a quem manipulou o computador em toda a investigação. (FREITAS, 2006).



EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 053203 Pag.: 01 De: 05

**MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO**

| Item: | Descrição: | | |
|---|---|---|---|
| 00001 | HD de Notebook com 80GB de capacidade | | |
| Fabricante: | Modelo: | Num. de serie: | |
| TOSHIBA | MK4026GAX | 85MC7639T | |

**DETALHES SOBRE A IMAGEM DOS DADOS**

| Data/Hora: | Criada por: | Método usado: | Nome da Imagem: | Partes: |
|---|---|---|---|---|
| 20/5/2007 15:30 | Paulo A. Neukamp | dcfldd | 053203_01.dd | 01 |
| Drive: | HASH: | | | |
| Disco Completo | d243367072088feae98364977441d736 | | | |

**CADEIA DE CUSTÓDIA**

| Sequência: | Data/Hora: | Origem: | Destino | Motivo: |
|---|---|---|---|---|
| 001 | Data: 20/5/2007 | Nome/Org.: Sigilo | Nome/Org.: Lab. Peri. Unisinos | Investigação sobre denuncia de Pedofilia |
| | Hora: 16:00 | Assinatura: | Assinatura: | |

Figura 2 - Exemplo de formulário de cadeia de custódia (2013).
Fonte: Monteiro [2007].

De acordo com Silva (2010), uma cadeia de custódia deve conter o histórico de toda a manipulação ocorrida com a evidência na qual devem constar:

- Local onde a evidência quando foi coletada.
- Quando foi coletada.

- Quem entregou a evidência para especialista.
- Dados sobre o equipamento (desktop, laptop, celular, etc.) e a mídia (HD, CD, Pendrive, etc.) onde estava armazenada a evidência original.
- Como foi feita imagem forense (softwares, formato da imagem, etc.).
- Mudanças na custódia da evidência.

## 4.7 Ata Notarial

Tomaszewski (2008, p. 164), define Ata Notarial como:

> […] um documento que contém a narração imparcial, portanto sem juízo de valores, e minuciosa de fatos jurídicos adrede solicitados e que não sejam de atribuição de outro profissional registrador.[...] Este profissional deve ater-se em sua atividade a relatar aquilo que ouve, vê ou como anotado, ainda pode perceber pela audição ou olfato. Este documento pode servir de base probante de fatos jurídicos, assim entendido como aqueles relevantes para o Direito e que por previsão no ordenamento jurídico produzem efeitos a que a ordem jurídica entende sendo dignos de regulamentação.

De acordo com Queiroz e Vargas (2010), os fatos que devemos estar atentos e podemos utilizar em uma ata notarial são:

- Acontecimentos na internet;
- Uso indevido de música armazenado em HD;
- Imagens de pedofilia infantil acessados com auxilio da internet;
- Acesso Indevido a sites pornográficos pela internet;
- Outros.

## 4.8 Aspectos Legais No Brasil

Não existem normas específicas que regem a forense computacional, contudo existem normas gerais que abrangem todos os tipos de perícia (ditadas no Código de Processo Penal), podendo ser adotadas no âmbito computacional, salvo algumas peculiaridades. No caso de uma pericia criminal existe a figura de um Perito Oficial

(dois para cada exame), onde seu trabalho deve servir para todas as partes interessadas (Polícia, Justiça, Ministério Público, Advogados, etc.).

A responsabilidade do Perito no exercício da sua função deve ser dividida em duas partes distintas: aquele do ponto de vista legal, onde lhe são exigidas algumas formalidades e parâmetros para a sua atuação como perito e as de ordem técnica, necessárias para desenvolver satisfatoriamente os exames técnico-científicos que lhe são inerentes. O Perito deve seguir a risca as normas contidas no Código de Processo Penal, dentre elas pode-se destacar duas para exemplificar a sua possível abordagem computacional:

> - Art. 170. Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.
> - Art. 171. Nos crimes cometidos com destruição ou rompimento de obstáculo a subtração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado. (BRASIL, 1941).

Recentemente foram sancionadas duas leis que falam sobre a tipificação de crimes informáticos:

### 4.8.1 Lei 12.737/12 Ou Lei “Carolina Dieckmann”

A chamada Lei Carolina Dieckmann acrescenta artigos ao Código Penal especificando que invadir computadores ou outros dispositivos eletrônicos – conectados ou não à Internet – é crime sujeito a prisão e multa.

O apelido da lei faz referência à atriz, que teve 36 fotos íntimas roubadas de seu computador e divulgadas na internet em maio passado. Uma pessoa passou a chantageá-la por email e exigiu o pagamento de R$ 10 mil para que as imagens não fossem divulgadas.

### 4.8.2 Lei Nº 12.735/12 ou “Lei Azeredo”

Esta lei foi proposta em 1999 pelo então deputado federal Eduardo Azeredo - PSDB. O principal ponto aprovado determina que a polícia estruture setores especializados no combate a crimes informáticos. Poucas cidades possuem delegacias especializadas em crimes eletrônicos. Onde não tem, a indicação é procurar qualquer delegacia da Polícia Civil. O outro ponto da Lei Azeredo em vigor inclui na legislação sobre os crimes resultantes de preconceito de raça ou de cor que um juiz pode determinar que qualquer publicação racista, eletrônica ou em qualquer meio, seja interrompida.

## 4.9 Técnicas Forenses

Nessa Seção serão apresentados algumas técnicas forenses, utilizadas pelos peritos.

### 4.9.1 Dump De Memória

Cópia parcial ou completa da memória física do sistema. Consegue capturar informações como a memória de processos, senhas em texto puro e arquivos descriptografados temporariamente. (MACEDO, 2007 apud SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, 2007; SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, 2007).

> Criando uma imagem da memória, ou dump de memória pode-se identificar os arquivos (processos) em processos pais e processos filhos. Tornando-se possível verificar como estava sendo a utilização do equipamento no momento do dump de memória, quais programas estavam sendo executados e provavelmente algumas senhas também ficam temporariamente na memória. (SOARES; FIRME, 2012).

### 4.9.2 Funções de Hash

Um dos mecanismos mais utilizados para se assegurar que os dados coletados não sejam modificados é calcular sua função de hash. O HASH é uma

função matemática que realiza o cálculo à partir de uma entrada de qualquer tamanho gerando em uma saída de tamanho fixo, pequena sequência de bits conhecida como valor do hash, de acordo com o algoritmo utilizado para o cálculo. (ELEUTÉRIO; MACHADO, 2011). Ao alterar o arquivo, por menor que seja a alteração, o valor do hash para o mesmo arquivo será diferente do valor calculado anteriormente à alteração, garantindo assim a integridade da informação à ser periciada. O hash é uma solução é muito utilizada nos meios computacionais já que é possível reconstruir a cadeia de caracteres original a partir do algoritmo hash criado. Assim caso haja qualquer tipo de mudança no arquivo original, mesmo que de um único bit, o hash resultante no destino será diferente e o documento resultante se tornará inválido. (PAGANELLI, 2012). Você pode utilizar *hash* para:

- verificar a integridade de um arquivo armazenado em seu computador ou em seus *backups*;
- verificar a integridade de um arquivo obtido da Internet (alguns *sites*, além do arquivo em si, também disponibilizam o *hash* correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);
- gerar assinaturas digitais.

O hash é uma função unidirecional e por isso possibilita retornar a informação original a partir do valor do hash. Os algoritmos utilizados para a realização do cálculo de hash são o MD5, SHA1 (gera valores de hash de 160 bits), SHA256 (gera valores de hash de 256 bits) e o SHA512(gera valores de hash de 512 bits). (ELEUTÉRIO; MACHADO, 2011).

### 4.9.3 Mactimes

MACtimes referem-se a três atributos de tempo: mtime, atime e ctime, que são anexados a qualquer arquivo ou diretório no Linux, Windows e em outros sistemas de arquivo.

- mtime (Modification time): mostra a última data e hora em que o arquivo foi modificado;
- atime (Access time): mostra a última data e hora em que um diretório ou arquivo foi acessado/lido;
- ctime (Creation time): mostra a data e hora em que arquivo foi criado.

### 4.9.4 Log de arquivo

De acordo com o Comissão Especial de Regimes de Trabalho (2012):

> Logs são o registro de atividade gerado por programas e serviços de um computador que podem ficar armazenados em arquivos, na memória do computador ou em bases de dados. A partir da análise desta analise podemos ser capazes de:
> - detectar o uso indevido do seu computador, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema;
> - detectar um ataque, como de força bruta ou a exploração de alguma vulnerabilidade;
> - rastrear (auditar) as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema;
> - detectar problemas de hardware ou nos programas e serviços instalados no computador.

## 4.10 Técnicas Anti-Forenses

Nessa seção serão apresentadas técnicas anti-forenses.

### 4.10.1 Esteganografia

De acordo com Jascone (2003, p.34),

> A esteganografia é a arte de comunicar-se secretamente, ocultando uma mensagem sigilosa dentro de outra informação sem importância, de maneira que não exista forma de detectar que há uma mensagem escondida. Na computação essa outra informação pode ser um arquivo de som, imagem ou texto".

Atualmente utilizam-se recursos como imagens, áudios e vídeos como meios de mensagem de cobertura (KESLER, 2007).

## 4.11 Criptografia

Segundo Peterson (2004), criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- autenticar a identidade de usuários;
- autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- proteger a integridade de transferências eletrônicas de fundos.

## 4.12 Códigos Maliciosos – Malwares

De acordo com o CERT (2012), códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Entre as diversas motivos pelos quais os códigos maliciosos podem infectar ou comprometer um computador podemos citar (CERT 2012):

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como pen-drives;
- pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

### 4.12.1 Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de

outros programas e arquivos. Ainda segundo Goodrich e Tamassia (2013), outra propriedade discriminante de um vírus é que essa replicação requer algum tipo de assistência do usuário como, por exemplo, clicar em um anexo de email ou compartilhar uma unidade USB. Muitas vezes um vírus também pode realizar alguma tarefa maliciosa como eliminar arquivos importantes ou roubar senhas. De acordo com o CERT (2012) alguns dos tipos de vírus mais comuns são:

- **Vírus propagado por *e-mail*:** recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador.
- **Vírus de *script*:** escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador *Web* e do programa leitor de *e-mails* do usuário.
- **Vírus de macro:** tipo específico de vírus de *script*, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).
- **Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (***M**ultimedia **M**essage **S**ervice*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

### 4.12.2 Worm

De acordo com o CERT (2012) um worm é um programa que possui a capacidade se propagar automaticamente pelas redes, enviando copias de si mesmo de computador para computador.

Diferentemente do vírus, o worm não se propaga por meio de copias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores. São notadamente responsáveis por consumir muitos recursos, devido a grande quantidade de copias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores. Um worm pode ter as mais diversas finalidades, como simplesmente espalhar-se consumindo largura de banda, causar ataques de negação de serviço, apagar arquivos, enviar arquivos por e-mail e, principalmente, instalar outros malwares como keyloggers, rootkits e backdoors.

### 4.12.3 Spyware

De acordo com Moraes (2011), *spyware* são arquivos espiões que se infiltram no computador quando acessamos sites não confiáveis, podendo vir escondidos inclusive quando instalamos alguns aplicativos. A maioria dessas ameaças tem a função de coletar dados de suas vítimas desde um endereço de site visitado até dados bancários do usuário. Segundo o CERT (2012) existem 3 tipos de spyware:

- ***Keylogger*:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*.
- ***Screenlogger***: similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*.

- ***Adware*:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

### 4.12.4 Backdoor

De acordo com Lovinson (2012), backdoor é um programa instalado pelo invasor que garante o acesso futuro a máquina invadida sem grandes esforços, permitindo o retorno do mesmo de maneira prática e rápida. Geralmente os backdoors são incluídos por outro malware no momento da infecção da máquina, mas também podem ser instaladas depois da instalação de uma vulnerabilidade.

### 4.12.5 Cavalo De Troia

De acordo com o CERT (2012), cavalo de troia, trojan ou trojan-horse, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Alguns exemplos de trojans que podemos citar são programas que você recebe ou obtém de sites na Internet, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas (CERT, 2012).

### 4.12.6 Rootkit

De acordo com Rosanes (2011), rootkit é um conjunto de programas utilizados para impedir a detecção de atividades maliciosas no sistema, como a presença de usuários não autorizados. Costumam ser usados por invasores de sistemas para manterem acesso após um ataque bem sucedido. De acordo com Melo (2009) Rootkits são um tipo de Malware muito arrojado, sua engenharia normalmente prevê a instalação de binários, módulos, bibliotecas que disponibilizam os mais variados recursos como backdoors e keyloggers. Os rootkits usam técnicas para esconder processos e outras informações inerentes ao mecanismo, o que dificulta sua identificação. Ainda segundo Rosanes (2011) alguns dos principais procedimentos feitos pelos rootkits são:

- Esconder informações sobre os processos referentes;
- Esconder seus arquivos;
- Esconder sockets criados para comunicação em rede;
- Modicar ou restringir o acesso aos arquivos de log;

## 4.13 Tipos De Análise

Ao iniciar o procedimento de perícia em um equipamento questionado, o perito deve fazer a escolha de qual metodologia será empregada em seu trabalho: se a **Live Analysis** ou se a **Post Mortem Analysis**. A escolha da metodologia adequada vai depender do tipo de delito que será investigado. Por exemplo, em um suposto crime de pedofilia, onde arquivos de imagens gravados em disco são evidências, o perito fará uso da metodologia Post Mortem Forensics. Já para crimes de estelionato praticados por meios eletrônicos, poderão ser utilizadas as duas metodologias, a Post Mortem Forensics para a busca de dados que indiquem que o acusado tenha, por exemplo, invadido o sistema de uma empresa, e a Live Forensics para averiguar conexões estabelecidas no instante da investigação.

### 4.13.1 Live Analysis

Nomeia-se Live Analysis, o processo realizado sem o desligamento da máquina vítima (PEREIRA, 2007). A importância deste tipo de investigação consiste na existência de informações voláteis, as quais serão perdidas com o desligamento da máquina. Informações como conexões de redes e processos em execução são exemplos de dados coletados durante este tipo de análise. Ocorrem situações onde a máquina analisada ainda pode estar sobre domínio do atacante, desse modo o sistema pode estar executando programas que escondam informações e dificultem o trabalho do perito. Baseando-se neste fato, o perito necessita usar um conjunto de ferramentas confiáveis e assim poderá garantir a integridade das tarefas realizadas com o auxílio das mesmas (PEREIRA, 2007).

Segundo Anson & Bunting (2007), os ingredientes principais para realizar uma análise live bem sucedida são:

a) Interagir o mínimo possível com o sistema em análise;
b) Utilizar ferramentas confiáveis;
c) Pensar e repensar, pois uma vez feito o procedimento em um sistema em execução, o sistema modificará o estado atual, sendo impossível retornar ao estado inicial;
d) Documentar todo o procedimento.

Informações como conexões de redes e processos em execução são exemplos de dados coletados durante este tipo de análise. Para evitar novas escritas no disco, remoção de arquivos temporários ou qualquer modificação no sistema, aconselha-se desligar o computador utilizando o procedimento pull the plug. Esse procedimento consiste na interrupção do fornecimento de energia ao equipamento pela retirada do cabo de energia da tomada. Após a coleta do equipamento computacional, uma cópia integral do disco rígido do sistema é realizada e, a partir daí, essa imagem é analisada em laboratório, utilizando-se um sistema operacional e aplicações forenses confiáveis (CARRIER, 2006).

### 4.13.2 Post Mortem Analysis

A forense Post-Mortem inclui técnicas de varredura por documentos, logs, imagens (fotografias), identificação de data e hora de arquivos, análise de trilhas de uso do computador e recuperação de dados excluídos (CARVEY 2007). Este tipo de análise é executado com o auxílio de um computador, denominado estação forense, preparada com ferramentas apropriadas, além de sistema operacional adequado e uma grande capacidade de armazenagem de dados (PEREIRA, 2007). De acordo com Vacca (2005), devem ser feitas pelo menos duas cópias da mídia original em análise sendo uma das cópias lacrada na presença do responsável pelo material (dono) e guardada em local seguro, podendo ser aberto somente sob determinação judicial e a segunda seria utilizada para a pesquisa e recuperação de dados.

## 4.14 Ferramentas Linux para Pericia Forense

De acordo com Campos (2006) software livre é o software que pode ser usado, copiado, estudado, modificado e redistribuído sem restrição. A forma usual de um software ser distribuído livremente é sendo acompanhado por uma licença de software livre (como a GPL ou a BSD), e com a disponibilização do seu código-fonte.

A seguir serão apresentadas algumas das ferramentas que reúnem um conjunto de aplicativos customizados para profissionais da área de segurança da informação, que trabalham com forense computacional Linux utilizados para perícia forense:

### 4.14.1 Backtrack

Distribuição Linux com foco em segurança da informação e computação forense, o BackTrack possui um arsenal de ferramentas para testes que auxiliam os profissionais na realização de avaliações de segurança. O sistema é destinado a todos os públicos, dos profissionais de segurança mais experientes aos novatos. Pode ser utilizado para análises diversas, avaliação de aplicação web e sistemas, aprender sobre segurança da informação, estudos de engenharia social, realizar

testes de penetração e vários outros aplicativos. O Backtrack foi evoluído da combinação de duas distribuições bem difundidas, voltadas também para segurança, Whax e Auditor Security Collection. Atualmente o BackTrack e atualmente possui mais de 300 ferramentas diferentes e atualizadas, que são logicamente estruturadas de acordo com o fluxo de trabalho de profissionais de segurança. Essa estrutura permite até novatos encontrar as ferramentas relacionadas a uma tarefa específica para ser cumprida. Novas tecnologias e técnicas de teste são combinadas no BackTrack o mais rápido possível para mantê-lo atualizado.

Possui ferramentas de Coleta de Informações, Mapeamento de Rede, Identificação de vulnerabilidade, Analise de Redes, Penetração, Escalação de Privilégio, Ferramentas de Acesso, Ferramentas para Encobrir Rastros.


Figura 3 - Página inicial do Backtrack 5 R3
Fonte: http://www.backtrack-linux.org/screenshots/(2013)

### 4.14.2 FDTK – Forense Digital Toolkit

O FDTK-UbuntuBr, é um projeto livre que objetiva produzir e manter uma distribuição para coleta e análise de dados em Perícias de Forense Computacional. Surgiu durante a elaboração da monografia da primeira turma do curso de Graduação em Segurança da Informação da Universidade do Vale do Rio dos Sinos – Unisinos situada no Rio Grande do Sul. A proposta inicial deste trabalho era um estudo das técnicas mundialmente utilizadas para a prática Forense Computacional com o intuito de esclarecer e desmistificar esta que é uma área ainda pouco conhecida pelos profissionais ligados a Tecnologia da Informação. É uma distribuição Linux criada a partir da já consagrada distribuição Ubuntu, e reúne mais de 100 ferramentas capazes de atender a todas as etapas de um investigação em Forense Computacional, oferecendo a possiblidade de ser utilizada como LiveCD e também ser instalada em um equipamento transformando-o em uma estação Forense. Essa distribuição está em constante desenvolvimento e caracteriza-se não apenas pela quantidade de ferramentas, mas também por uma interface amigável, estruturada conforme as etapas do processo de perícia e, ainda pela preocupação por ser distribuída no idioma português.


Figura 4 - Página Inicial do FDTK
FDTK. Fonte: http://fdtk.com.br/www/wp-content/uploads/2008/12/Tela1.png (2013)

### 4.14.3 Caine

Software de origem italiana cujo gerente do projeto é Nanni Bassetti. Caine (Computer Aided Investigativo Environment) é uma Distribuição baseada em Linux Ubuntu que oferece um ambiente completo forense que está organizado para integrar ferramentas de software existentes como módulos de software e para fornecer uma interface gráfica amigável. Os objetivos principais do projeto que visa a garantir Caine são os seguintes: um ambiente que suporta o investigador digital durante as quatro fases da investigação digital; uma interface gráfica amigável; uma compilação semi-automatizada do relatório final.


Figura 5 - Página inicial do CAINE
Fonte: http://www.caine-live.net/page4/page4.html (2013)

# 5 METODOLOGIA

Como proposta para o presente estudo, inicialmente foi realizada uma pesquisa bibliográfica que segundo Domingues; Heubel; Abel (2003) as pesquisas devem conter assuntos gerais e particulares podendo ser localizadas em diversas fontes de pesquisas como periódicos livros e materiais digitais nos quais tende a ter a facilidade em encontrar assuntos sobre softwares livres utilizados em pericia forense. Para consulta das funcionalidades foram utilizados diversos meios tais como, manual de usuário, forum de discussão e tutoriais disponíveis na internet entre outros.

Após o término da pesquisa o próximo passo foi instalar um sistema uma máquina virtual VMPlayer 6.0 onde foram instalados os softwares de pericia forense. Para esse trabalho utilizamos os softwares livres Backtrack 5 R3, FDTK V-3.0 e C.A.IN.E 4.0, todos compatíveis com o Linux Ubuntu. A lista de softwares a serem avaliados foi baseada em buscas feitas em sites voltados aos softwares livres. Além disso, autores e revistas digitais especializadas também foram consultados.

Depois de instalados e corretamente configurados, o próximo passo foi testar e descrever as funcionalidades que cada software possui e suas aplicações em testes de pericia computacional com o objetivo de determinar as principais características de cada software utilizado. Para maior compreensão essas características de softwares foram divididas em tópicos com o objetivo de facilitar o trabalho do perito em Forense Computacional.

Após os testes realizados nos softwares, será feito um quadro comparativo, destacando as principais características de cada um deles, como por exemplo, manuais e tutorias disponíveis, configuração mínima exigida, entre outras características que ainda serão analisadas e verificadas. Ao término dessa pesquisa espera-se proporcionar maiores detalhes de informações dos softwares analisados, permitindo aos peritos forenses maior facilidade de escolha quanto ao software com o qual ele deseja utilizar.

# 6 TESTE DAS FERRAMENTAS

## 6.1 Exemplo de uso de ferramentas forenses usando o live cd CAINE

### 6.1.1 PHOTOREC

Esta ferramenta útil para recuperar arquivos excluídos dentro de uma partição ou algum dispositivo de armazenamento como cartões de memoria ou pendrives. Neste exemplo utilizou-se um pendrive de 4Gb. Conforme figura 9, primeiramente foi selecionada a ferramenta dentro da distribuição C.A.IN.E através do menu forensics>Photorec.


Figura 6 – Selecionando a ferramenta Photorec

Em seguida, foi selecionado o dispositivo no qual se quer recuperar estes dados, neste caso o pendrive Kingston DT 102 G2 (capacidade de 4Gb), conforme figura 10.

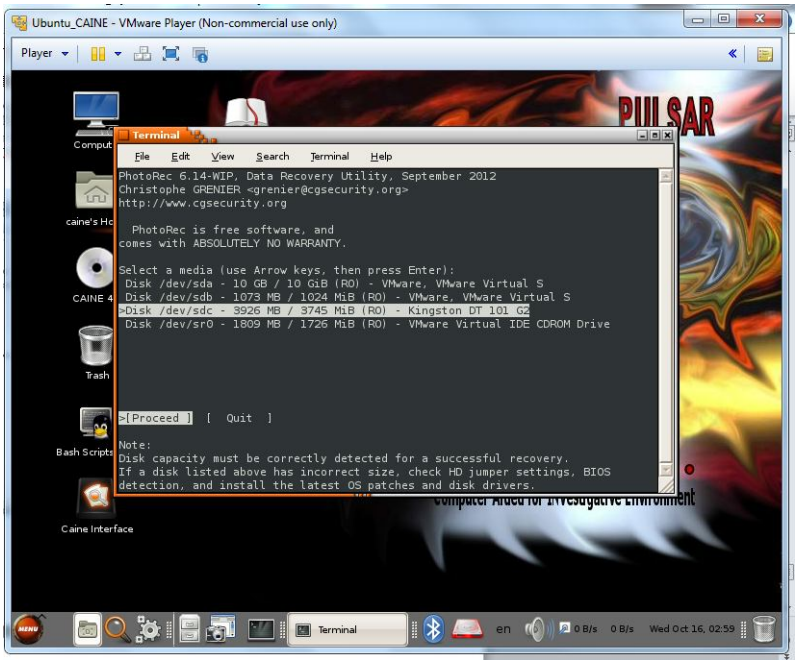



Figura 7 – Escolhendo a unidade a ser verificada

Após a escolha do dispositivo a ser a analisado, a ferramenta pergunta se será analisada uma partição do disco ou a unidade inteira. No exemplo citado opta-se por escolher toda a partição (FAT32 LBA) conforme é exibido na figura 11.

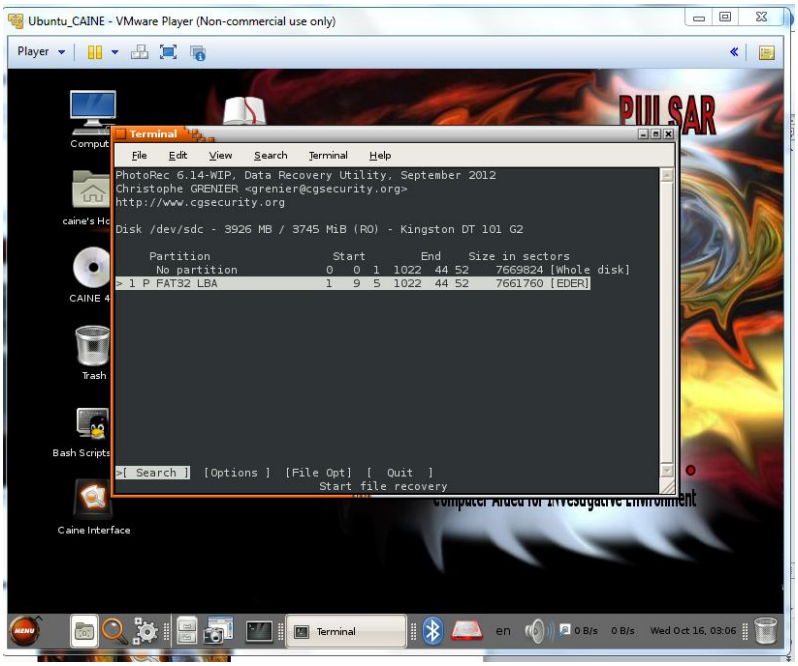



Figura 8– Escolhendo a partição a ser analisada

Após a confirmação da unidade a ser analisada a ferramenta foi solicitada a confirmação do sistema de arquivos a ser analisado. Neste caso o sistema utilizado foi FAT  32, utilizado em pendrives, conforme exibido na figura 12.

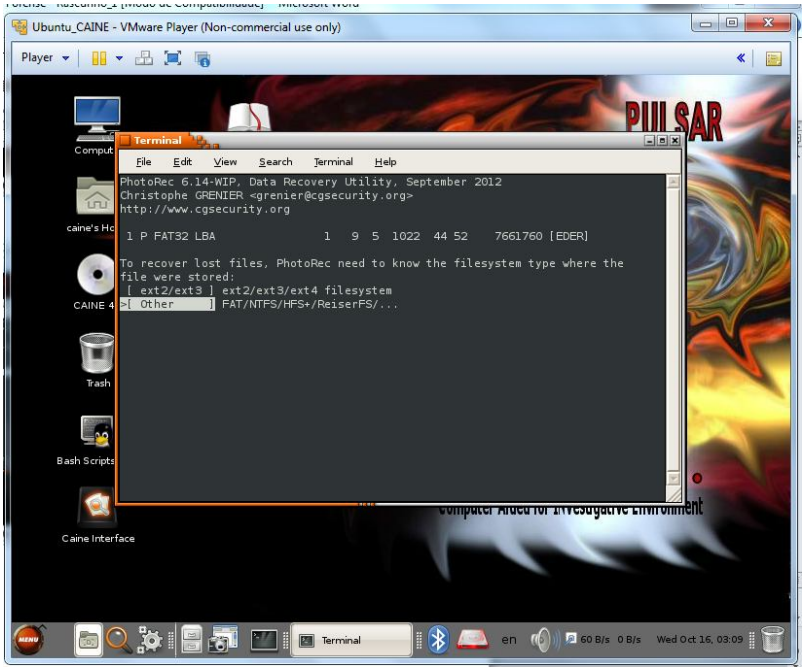



Figura 9 – Confirmando o Sistema de arquivos da unidade (Neste caso FAT).

Em seguida, foi escolhido o local onde os arquivos recuperados deverão ser armazenados. Se escolher “Free”, o PhotoRec colocará os arquivos em uma área vazia da própria unidade. Neste caso foi utilizada a opção “Whole”, e logo em seguida salvar os arquivos na área de trabalho. Em seguida foi pressionada a tecla C para confirmação. Este processo é exibido abaixo nas figuras 13,14, 15 e 16.

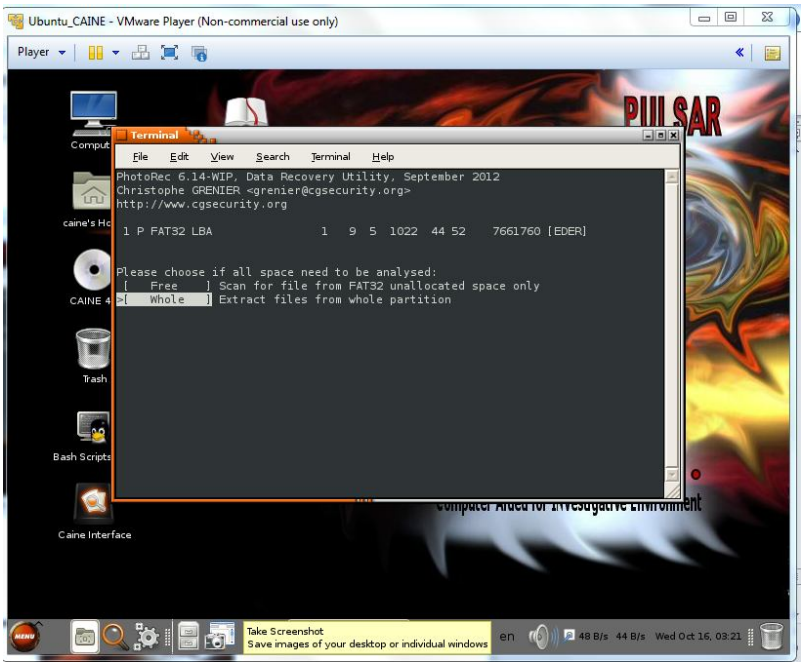



Figura 13 – Escolhendo a opção Whole para escolhermos onde os arquivos recuperados serão armazenados

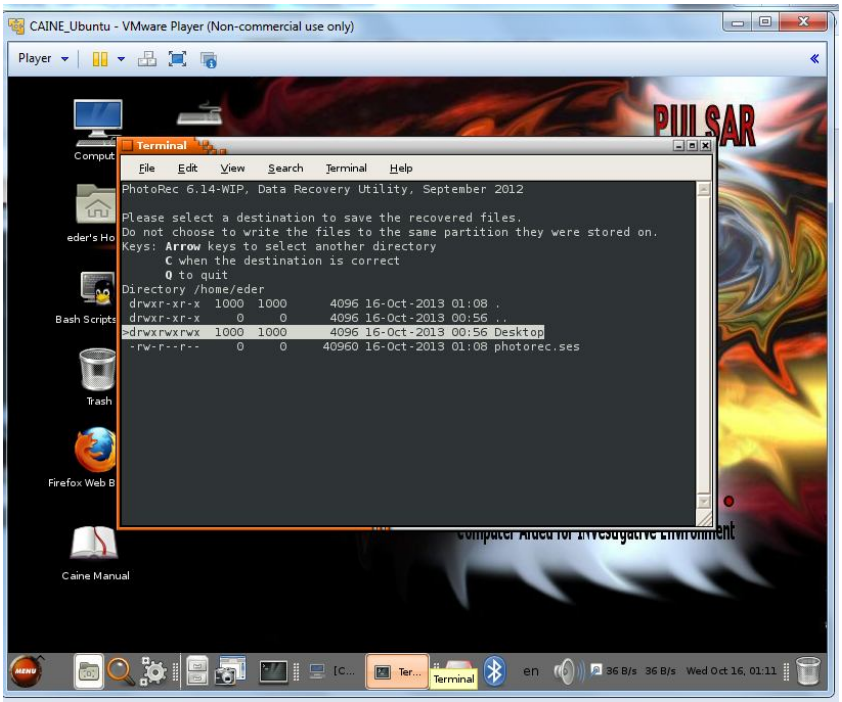



Figura 14 – Selecionando o local onde os arquivos serão salvos

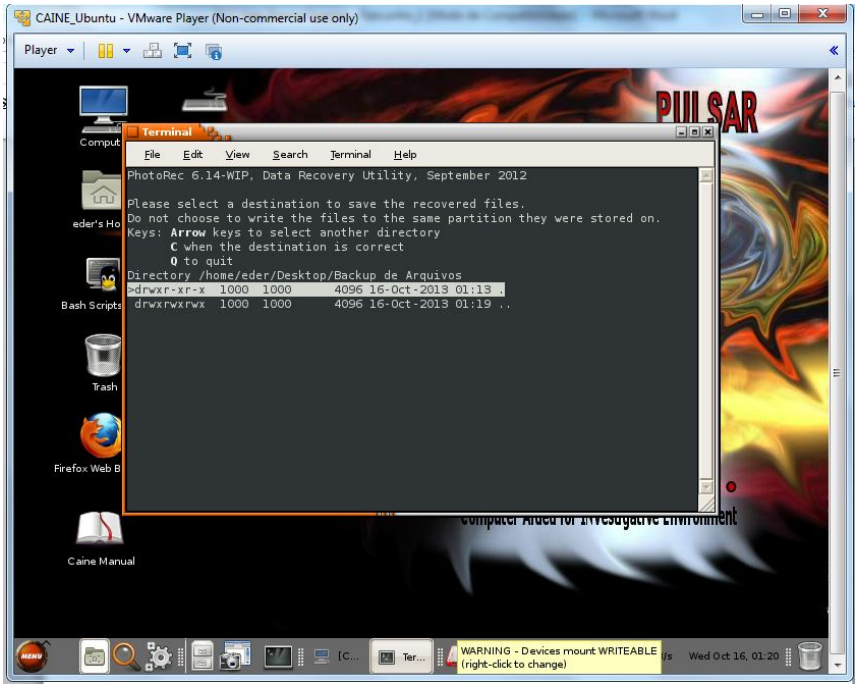



Figura 15 – Confirmando se o endereço de arquivos a ser recuperado está correto.

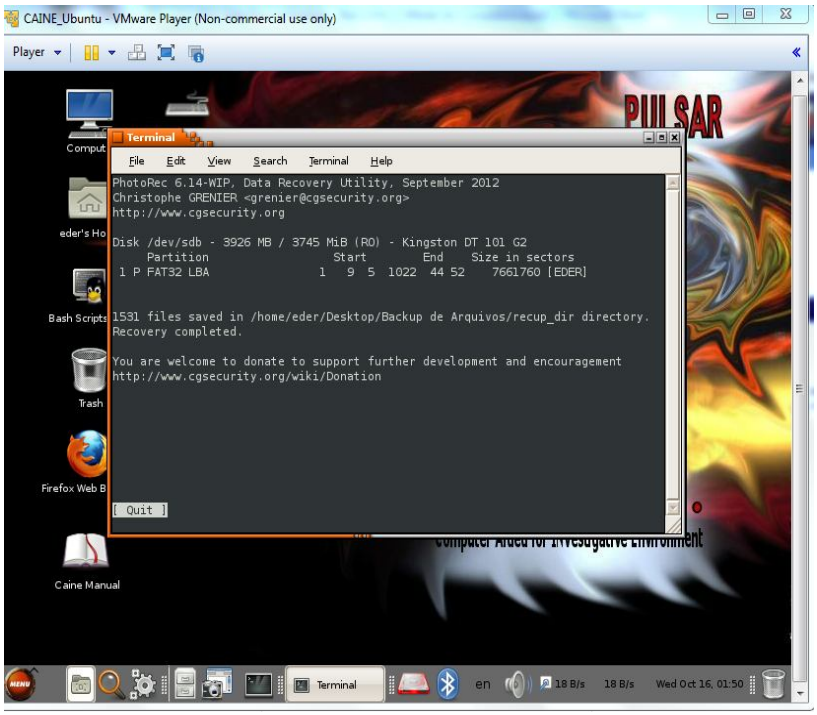



Figura 16 – Lista da quantidade de arquivos recuperados.

Ao final, conforme exibido na figura 17, foi acessado o local  onde os arquivos foram recuperados, neste caso a área de trabalho (Desktop). Foram recuperados 1531 arquivos organizados em 3 pastas de 500 arquivos cada e uma de 31 arquivos.

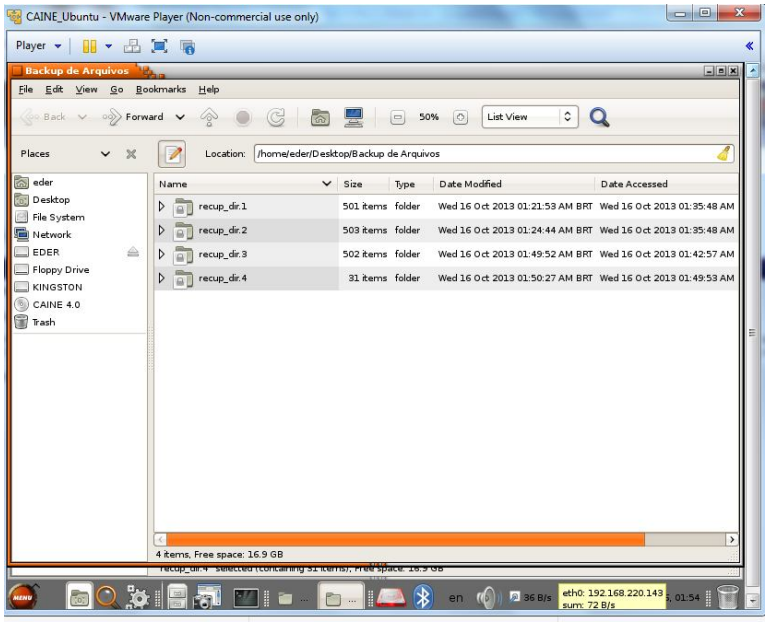



Figura 107 – Arquivos recuperados pela ferramenta.

Ao final a ferramenta lista os arquivos recuperados, conforme mostrado na figura.

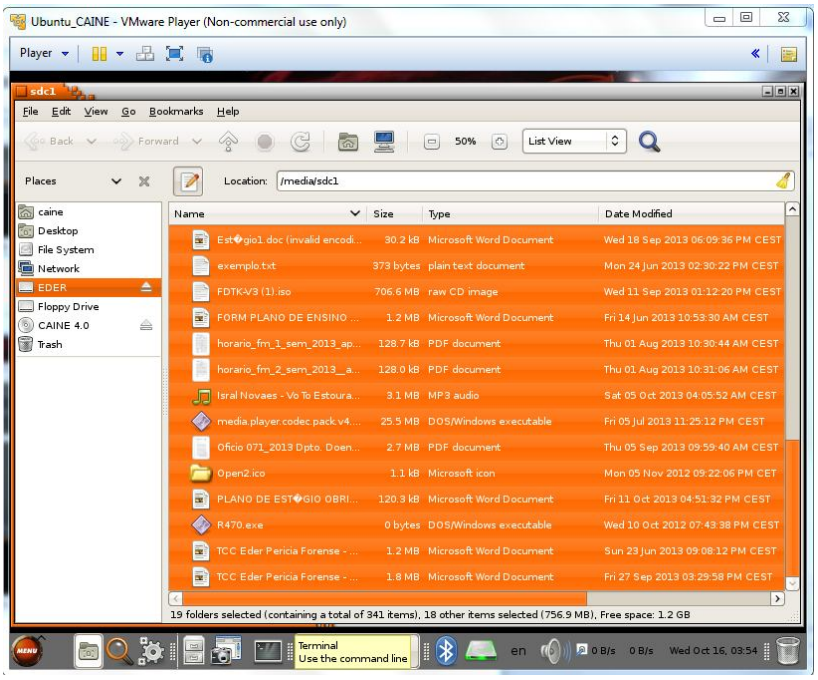



Figura 18 – Pasta com arquivos salvos pela ferramenta.

### 6.1.2 GUYMAGER


Figura 11 – Selecionando Guymager

Para este exemplo, mostrado na figura 20 utilizou-se duas partições do hd nomeadas de hd01 e hd02 respectivamente com 2gb e 1gb, dentro de segundo HD criado com tamanho de 8gb.


Figura 120 – Selecionando as partições HD_PART01 e HD_PART02

Em seguida, conforme mostrado na figura 20, tudo o conteúdo do hd denominado HD_PART2 foi copiado em um arquivo de imagem no formato dd para o hd denominado HD_PART01 através da ferramenta Guymager. Para se encontrar o hd desejado, deve-se acessar o menu *devices>add especial device* e depois digitar dev6 (caminho para encontrar o dispositivo neste caso). Após o dispositivo encontrado, clicar-se com o botão direto do mouse selecionando posteriormente a opção acquire image conforme mostrado na figura 21:

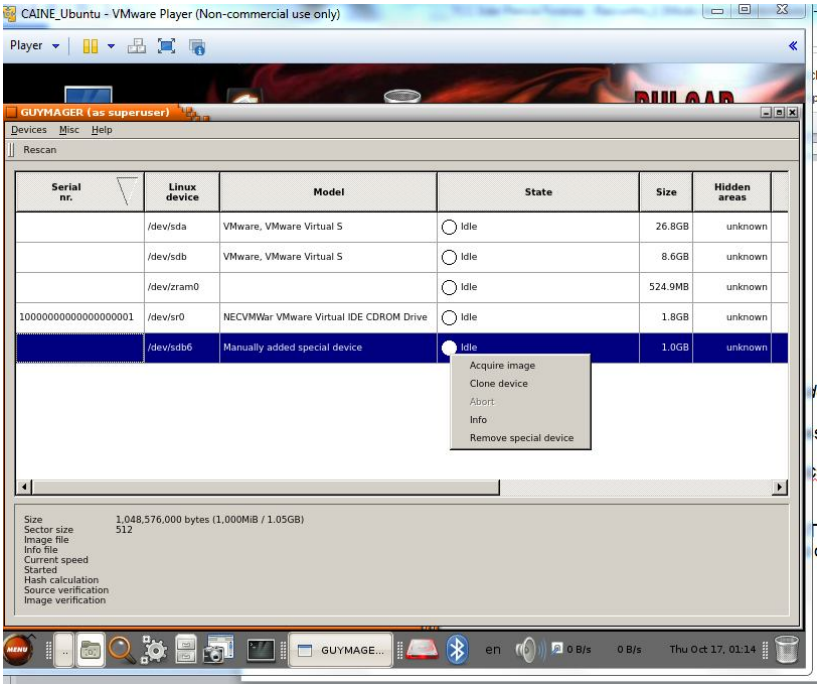



Figura 131 – Selecionando o dispositivo /dev/sdb6 que será copiado.

Para criar a imagem será utilizada a opção *Linux dd raw image (file extension .dd or .xxx).* O arquivo de imagem será salvo no hd denominado HD_PART02. Ao final foi selecionado o arquivo de hash que queremos escolher, neste caso a hash sha-256. O arquivo da imagem gerada foi denominado caso01. Clicar em start para iniciar a cópia. Este processo é mostrado na figura 22.

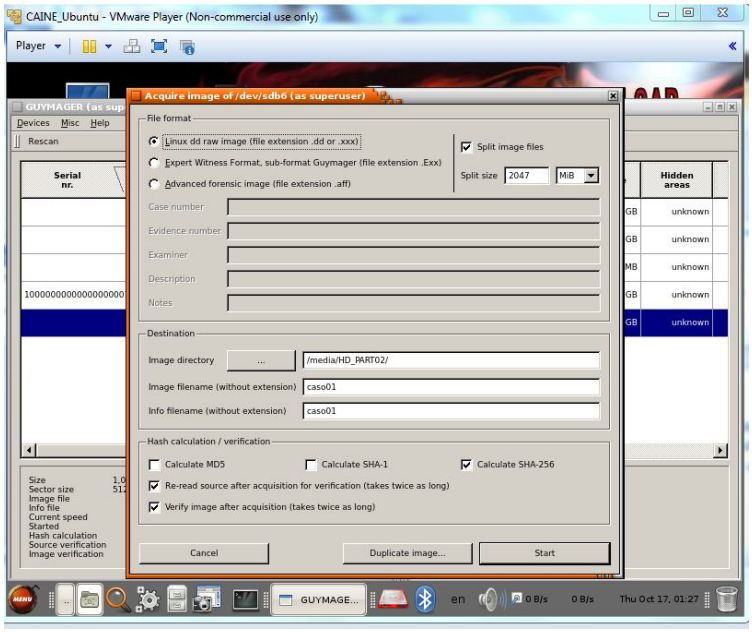



Figura 142 – Definindo parâmetros para criação da imagem a ser gravada.

Conforme figura 23 é exibido o arquivo com as informações sobre a imagem gerada:

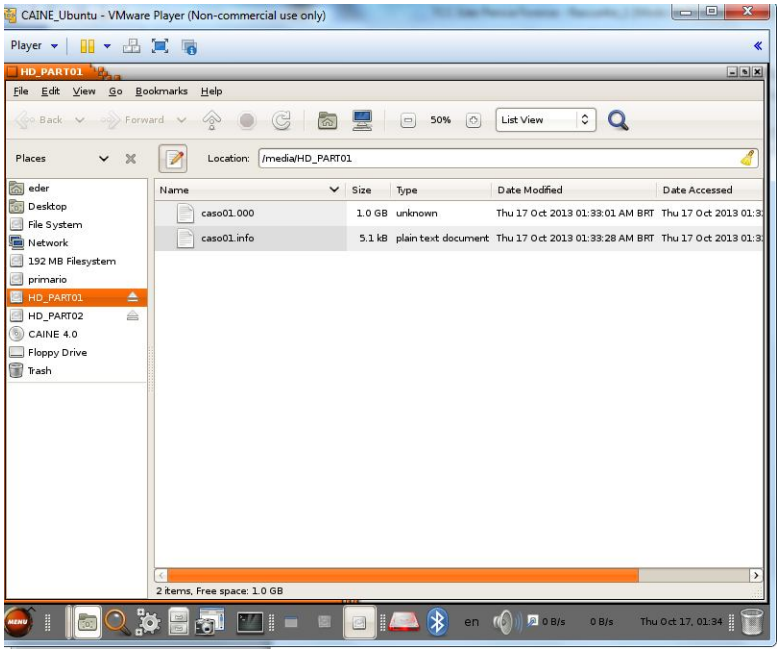



Figura 153 – Imagem gravada com o nome de caso01.

Ao final do processo um arquivo é exibido com informações gerais, bem como o hash gerado sobre o arquivo gerado de acordo com a figura 24.

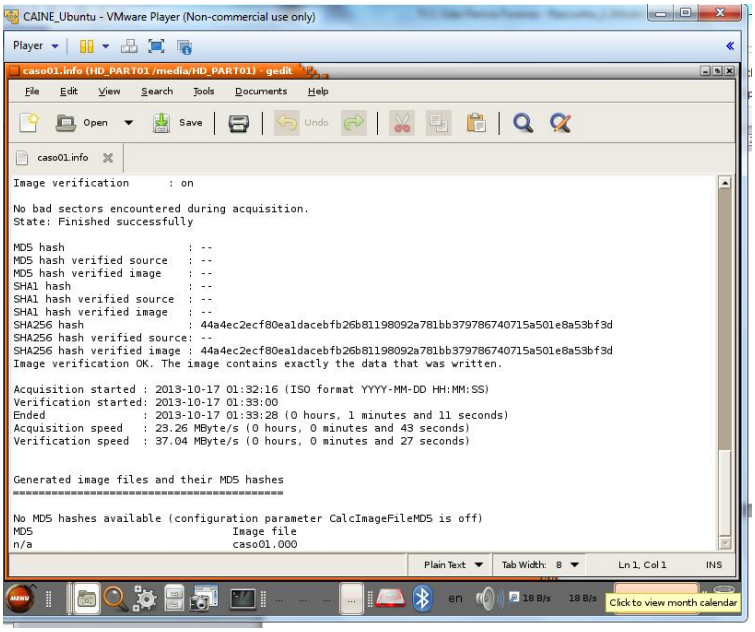



Figura 24 – Arquivo gerado com informação sobre o imagem gerada e também com o hash gerado.

## 6.2 Exemplo de uso de ferramentas forenses usando o live cd FDTK

### 6.2.1 Stegdetect

Usa-se esta ferramenta para detectar esteganografia em imagens jpg.

**Exemplo**

Primeiramente acessa-se a pasta Esteganografia criada na área de trabalho e que contém os arquivos futebol.jpg, paisagem.jpg e peixes.jpg e texto.txt. O arquivo texto.txt não será analisado, apenas os arquivos de extensão .jpg. Este processo é mostrado na figura 25.

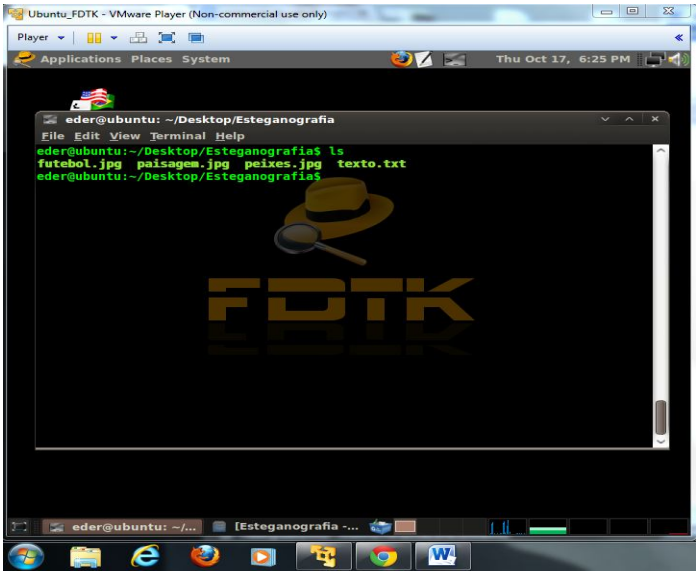



Figura 25– Listagem dos arquivos futebol.jpg, paisagem.jpg, peixes.jpg

Conforme figura 26, utilizou-se novamente a ferramenta com o valor de sensibilidade alto ( -s ) e o valor para habilitar a verificação de falsos positivos ( -n )

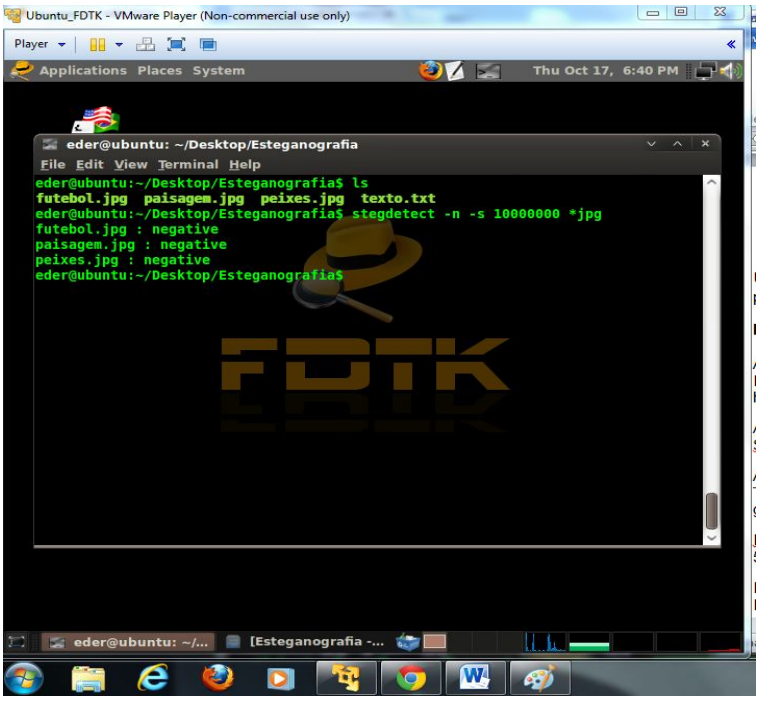



Figura 166 – Utilizando os parâmetros –n –s para descobrir se há esteganografia nas imagens.

Conforme mostrado na figura 27 comando cat foi utilizado para mostrar o conteúdo do arquivo texto.txt

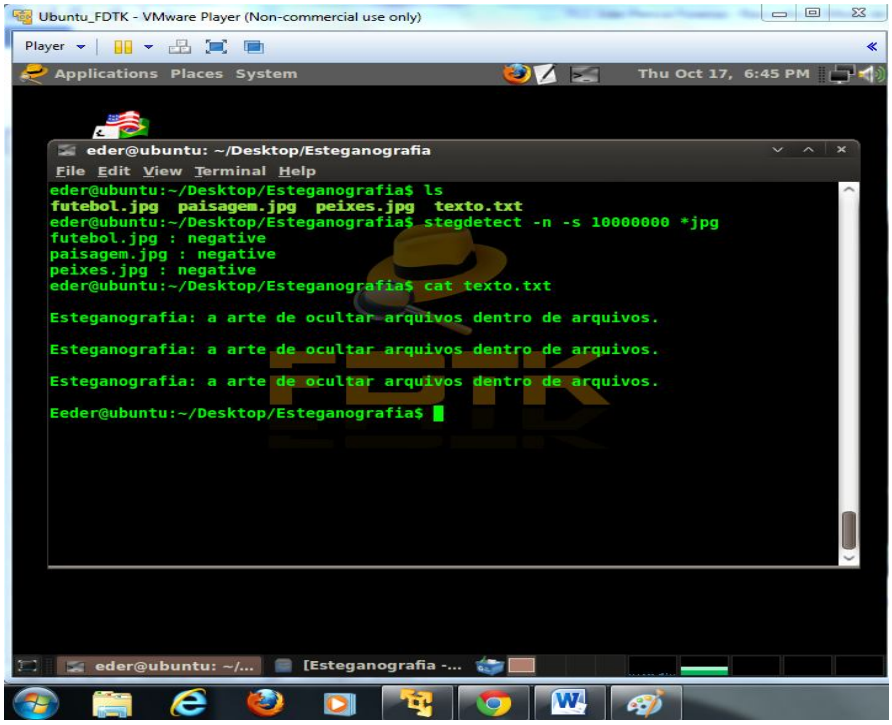



Figura 177 – Acesso ao conteúdo do arquivo texto.txt, através do comando cat.

Agora conforme mostrado na figura 28 utiliza-se a ferramenta outguess para adicionar à imagem futebol.jpg o arquivo texto.txt e criar o arquivo futebolnovo.jpg.

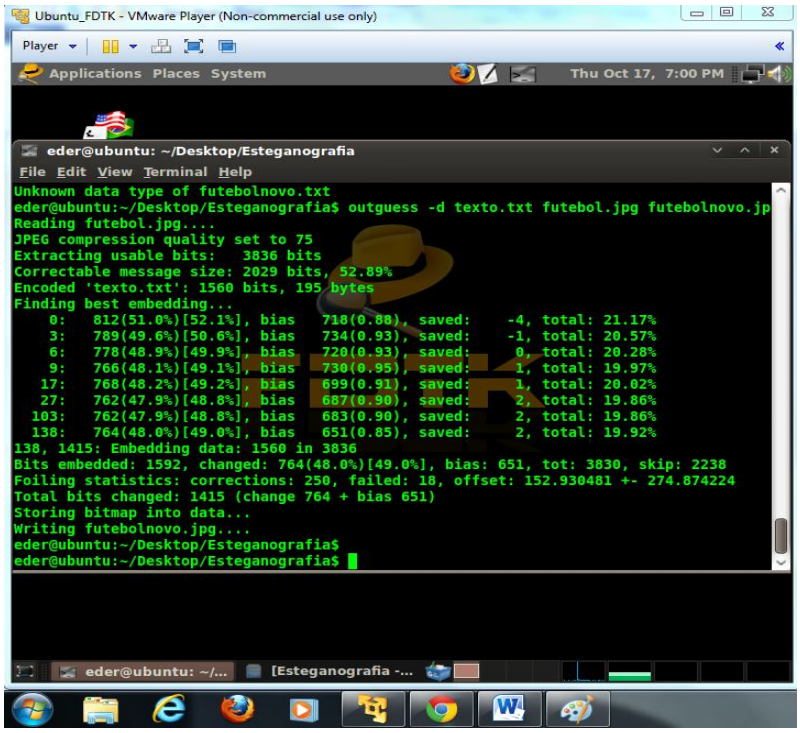



Figura 188 – adicionando o conteúdo do arquivo texto.txt ao arquivo futebol.jpg criando o arquivo futebolnovo.jpg.

Agora, conforme mostrado na figura 30 os arquivos na pasta Esteganografia forão novamente listados através do comando stegdetect e pôde-se ver que o mesmo não detecta esteganografia nas imagens.

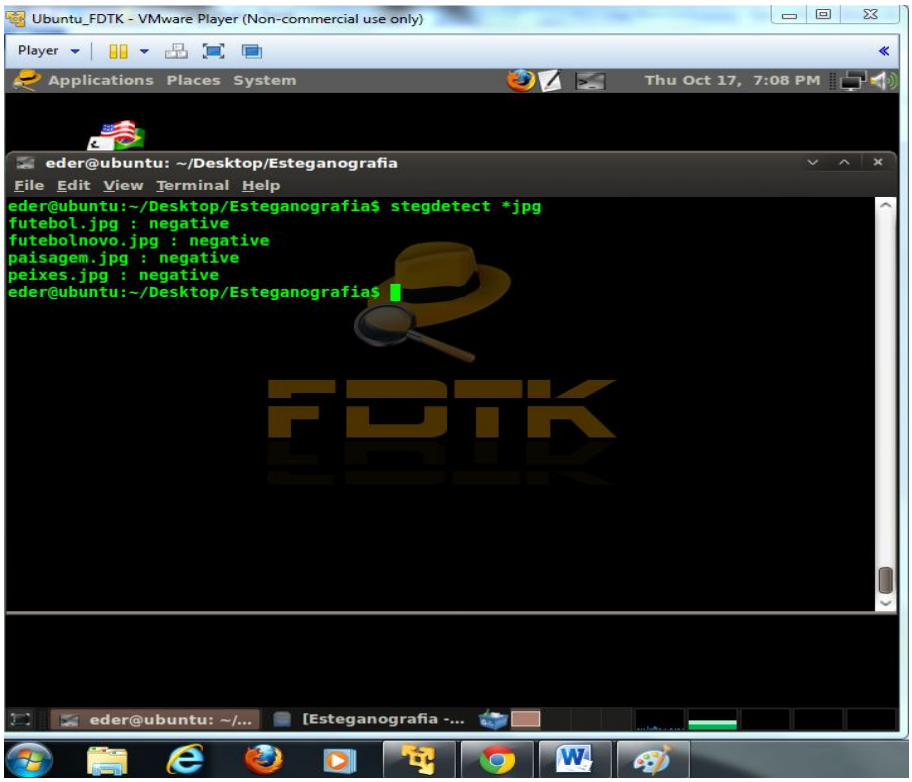



Figura 19 – Listando novamente os arquivos através do comando ls.

Posteriormente os arquivos foram novamente listados novamente com o comando stegdetect mas desta vez com o parâmetro –s para aumentar a sensibilidade da ferramenta e verificamos que ela detecta esteganografia no arquivo futebolnovo.jpg, conforme mostrado na figura 31.

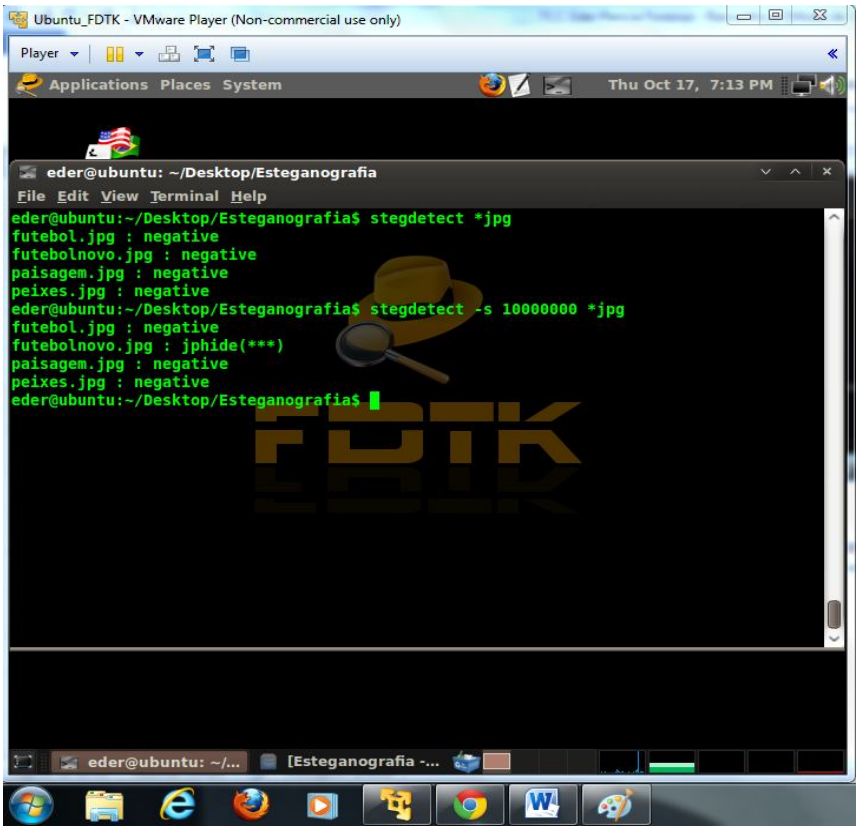



Figura 20 – Detectando esteganogragria no arquivo futebolnovo.jpg através dos parâmetros -n e –s.

Na figura 32 mostra-se o acesso feito à pasta Esteganografia que contém o arquivo futebolnovo.jpg

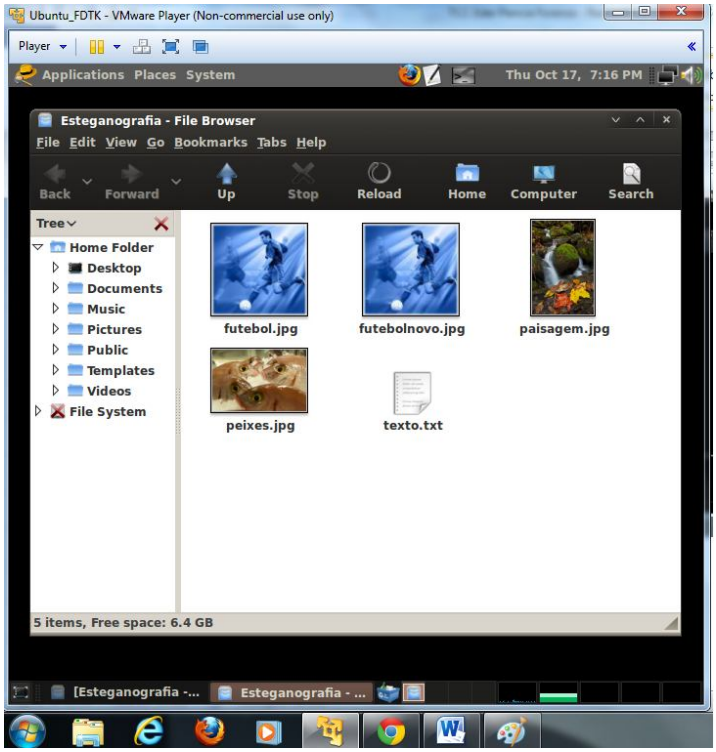



Figura 21 – arquivos usados neste exemplo

### 6.2.2 Galleta

Ferramenta usada para analisar cookies no navegador Internet Explorer. Cookie é o pequeno arquivo e que é enviado ao seu computador quando você acessa um site. Para utilizarmos a ferramenta primeiramente foram coletados estes pequenos arquivos no navegador internet explorer no notebook onde foram instalado a maquina virtual Vmware. A figura 33 exibe a tela inicial do Internet Explorer.

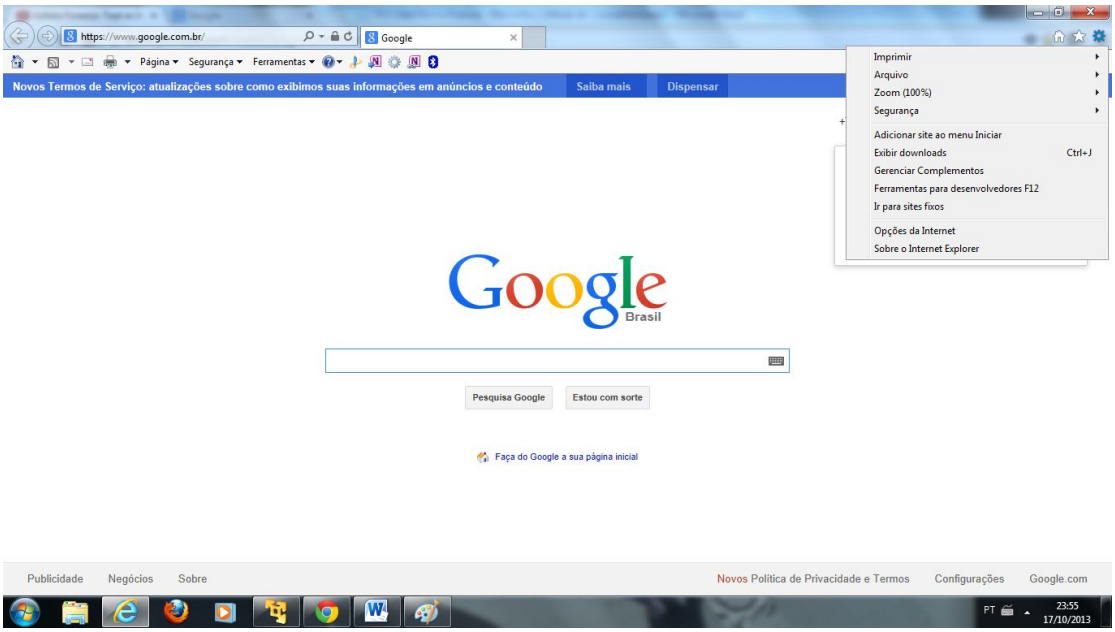



Figura 22 - Tela inicial do internet explorer

Posteriormente foi acessado, dentro do negador Internet Explorer o item configurações e depois em exibir arquivos, conforme mostrado na figura 34.

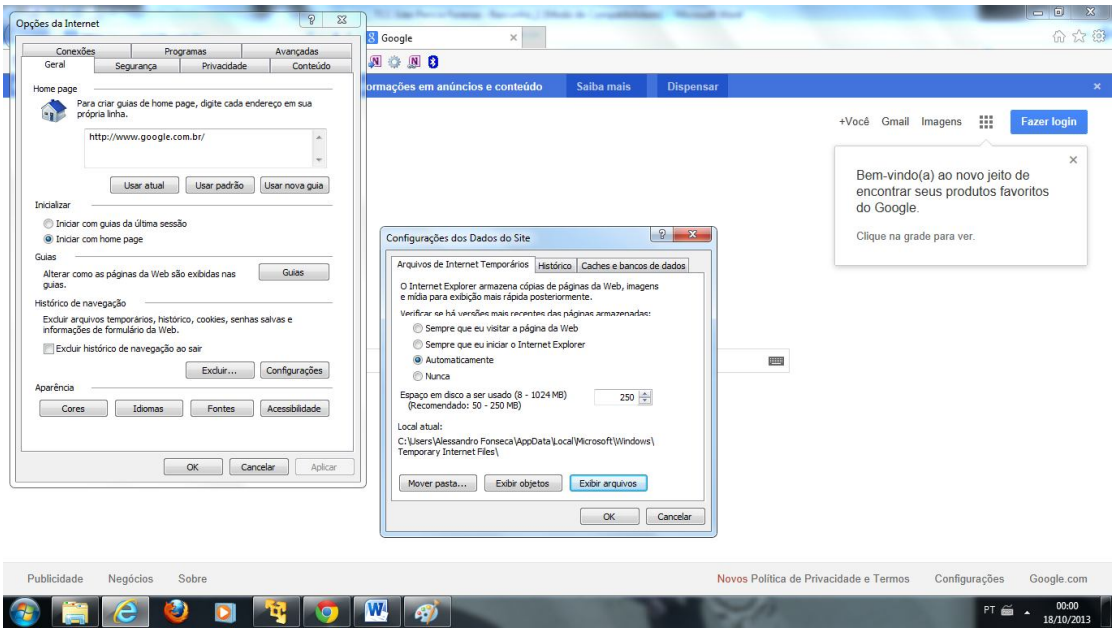



Figura 23 – Acessando o item Configurações de Dados do Site do Internet Explorer.

Depois deve-se acessar a pasta Temporary Internet Files do internet explorer onde se encontram os cookies, como mostrado na figura 35.

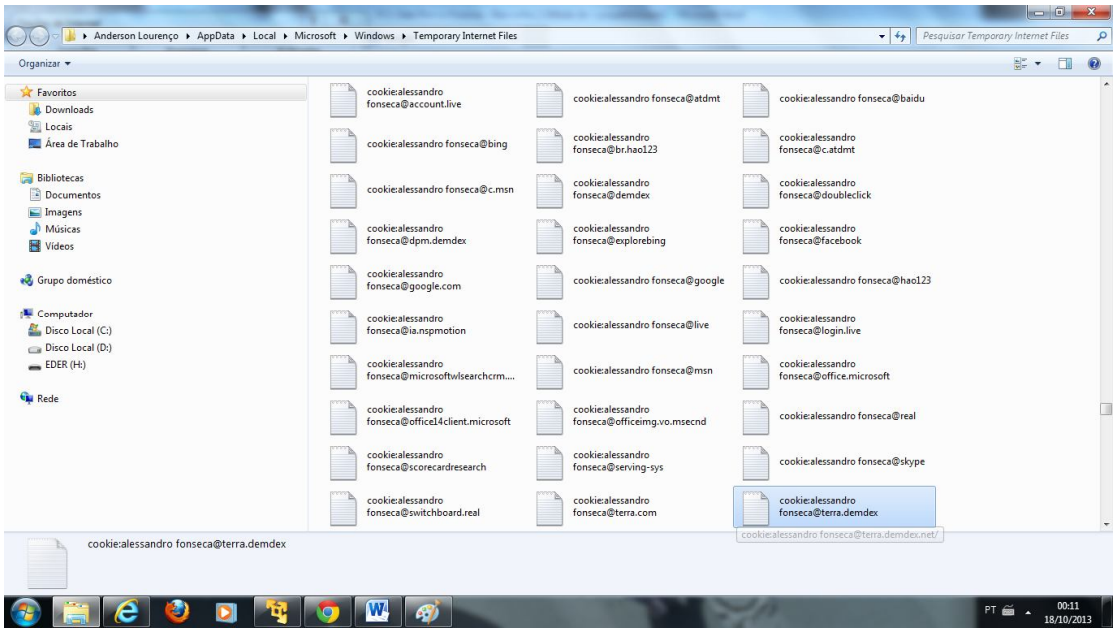



Figura 24 – Pasta Temporary Internet Files onde se encontram os arquivos a serem analisados

### 6.2.3 Usando Galleta

Conforme mostrado na figura 36 selecionados na pasta Temporary Internet Files os arquivos em uma pasta chamada Cookies e salvamos na área de trabalho da ferramenta FDTK. Para fazer o teste será usado o arquivo ZJRPC4VD.txt.

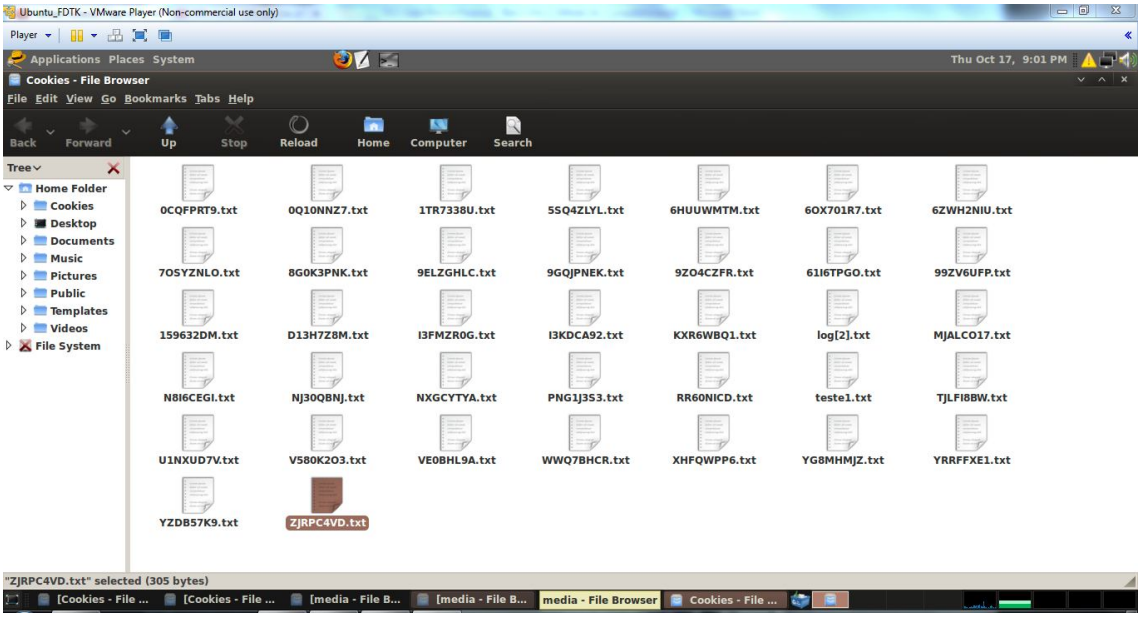



Figura 25 - Arquivos cookies copiados para maquina virtual FDTK

Arquivo aberto antes de usarmos a ferramenta galleta, mostrado na figura 37, usando o editor de texto gedit.

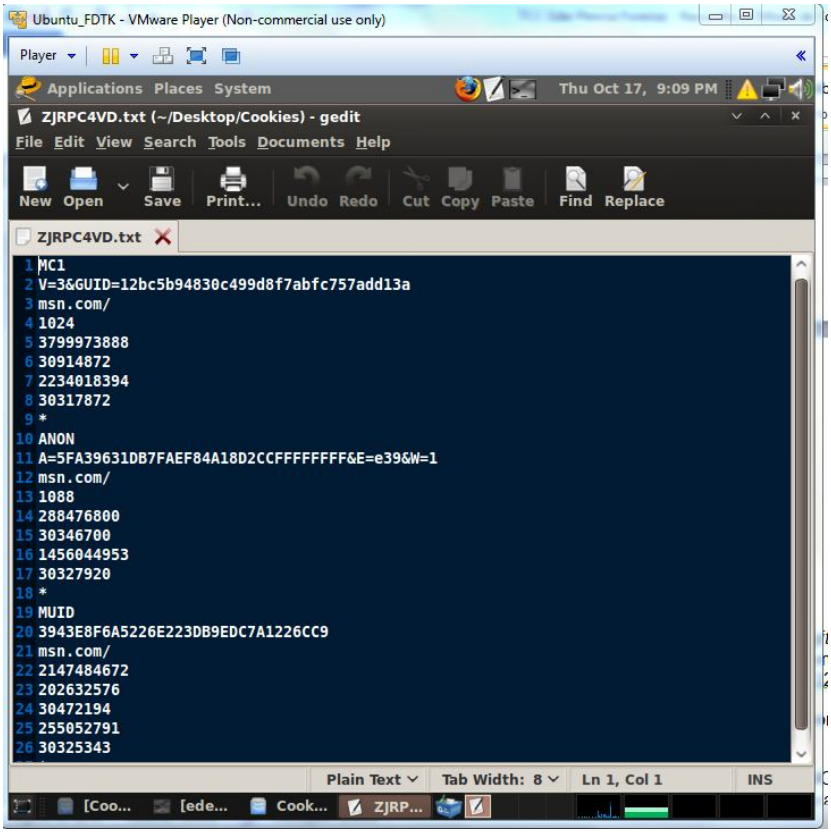



Figura 26 - Arquivo ZJRPC4VD.txt aberto com o editor de texto gedit

Posteriormente foi criado um novo arquivo denominado arquivo_novo.txt utilizando a ferramenta galleta e o arquivo ZJRPC4VD.txt utilizando a linha de comando: galleta ZRJPC4VD.txt > novo_arquivo.txt, mostrado abaixo na figura 38.

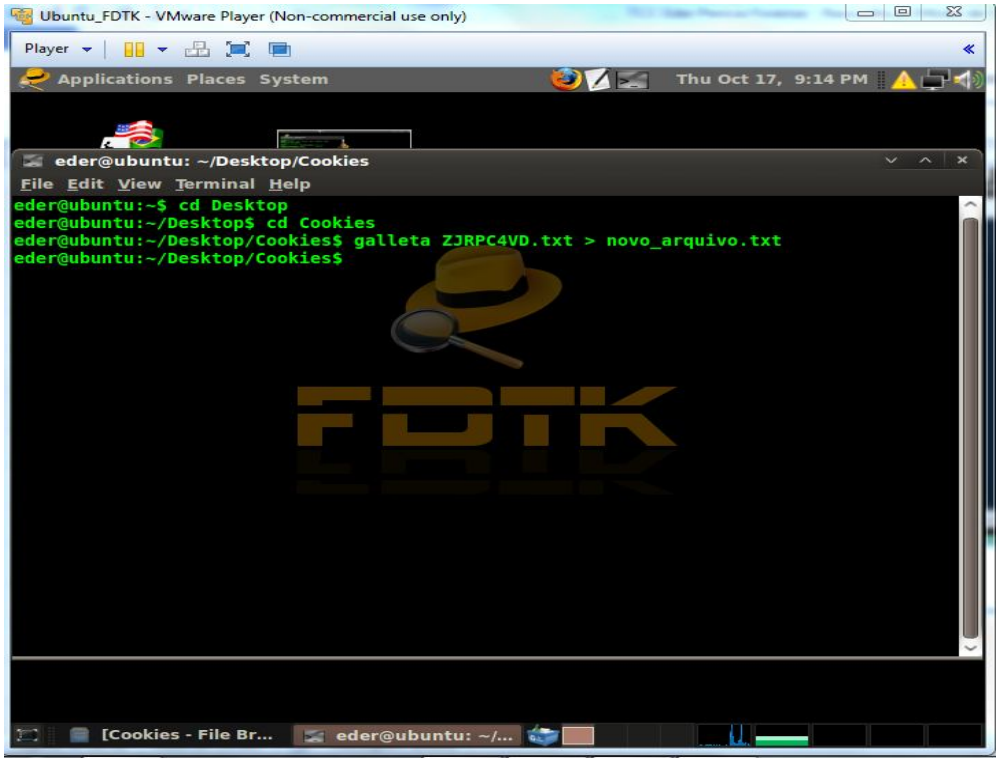



Figura 27 – Gerando o arquivo novo_arquivo.txt.

Conforme mostrado na figura 39, depois de criado o arquivo foi acessado acessá-lo para ver os resultados obtidos.

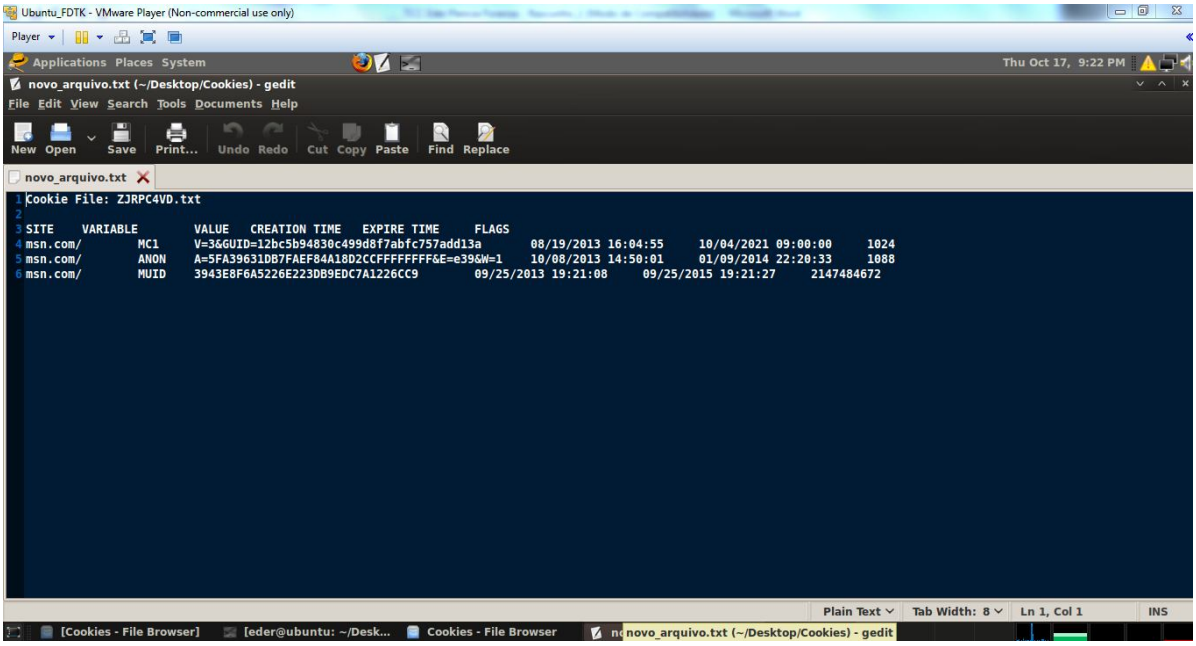



Figura 28 – Acessando arquivo_novo.txt

### 6.2.4 Comando DD

Para o uso deste comando foi utilizado um pendrive de 4gb para fazer a aquisição da imagem, conforme mostrado na figura 40.

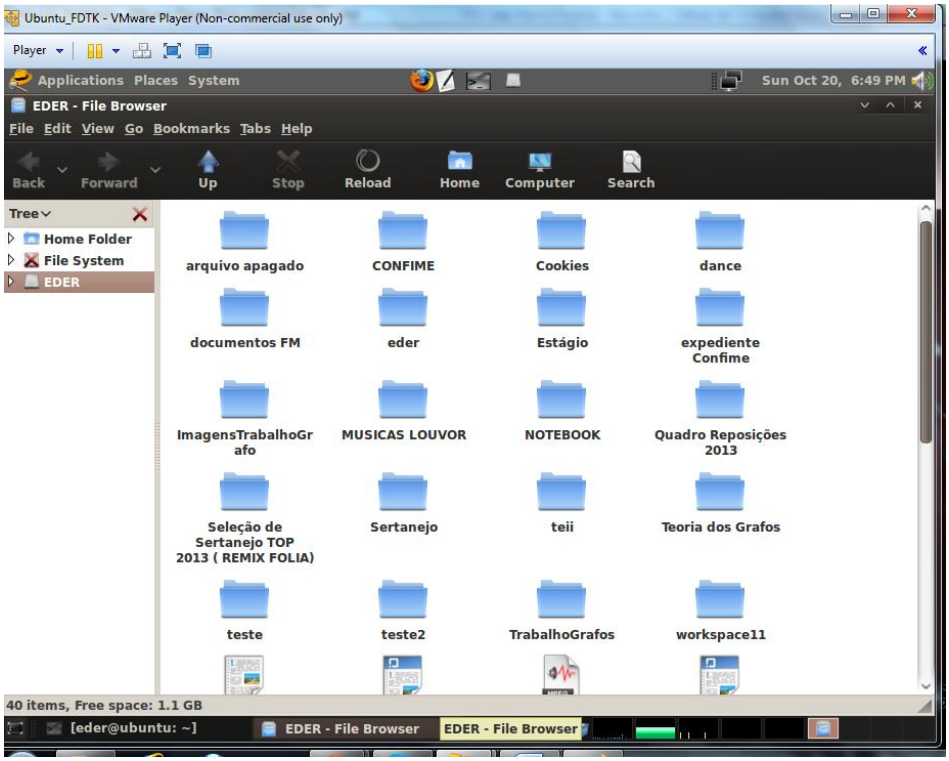



Figura 29 – pendrive de 4Gb utilizado para a aquisição da imagem

Conforme exibido na figura41, para fazer a cópia do arquivo primeiramente utilizou-se o camando fdisk para listar a localização do pendrive.

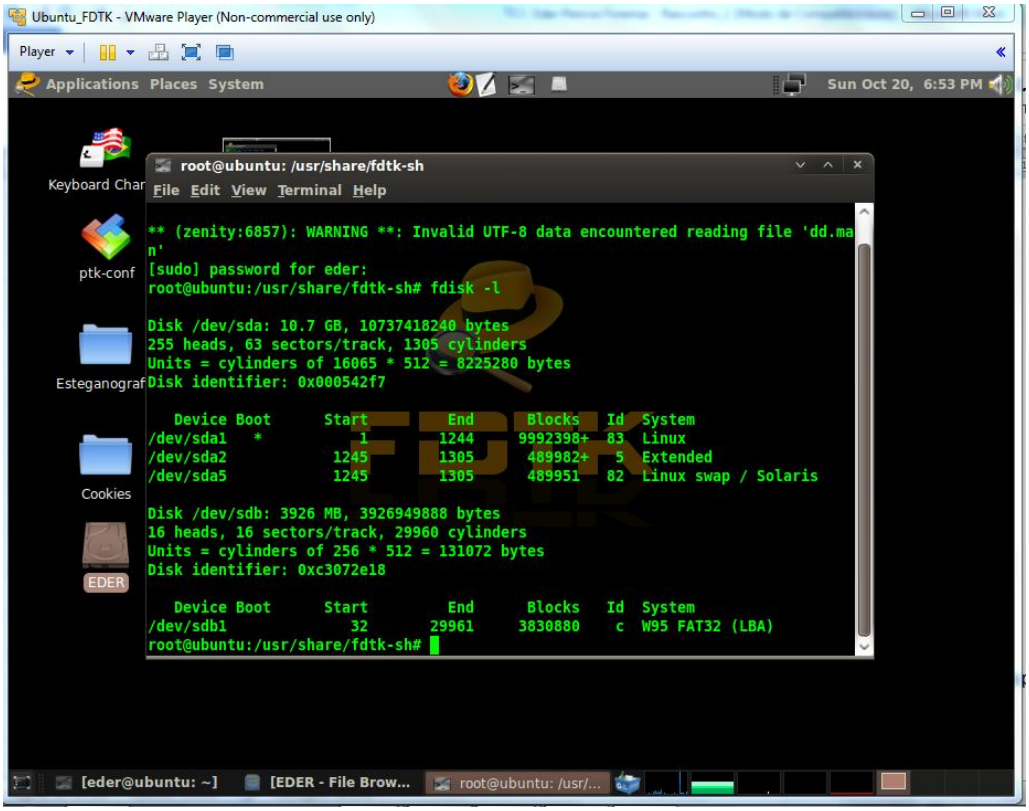



Figura 30 – Listando os dispositivos através do comando fdisk –l.

Conforme mostrado na figura 42, através do comando fdisk –l lista-se a localização do pendrive: /dev/sdb1. Para a fazer a cópia da mídia física utilizou-se o comando DD no qual a imagem gerada na pasta home eder com o nome imagem.img foi salva. A sintaxe usada para a captura foi dd if=dev/sdb1 of=home/eder/imagem.img.

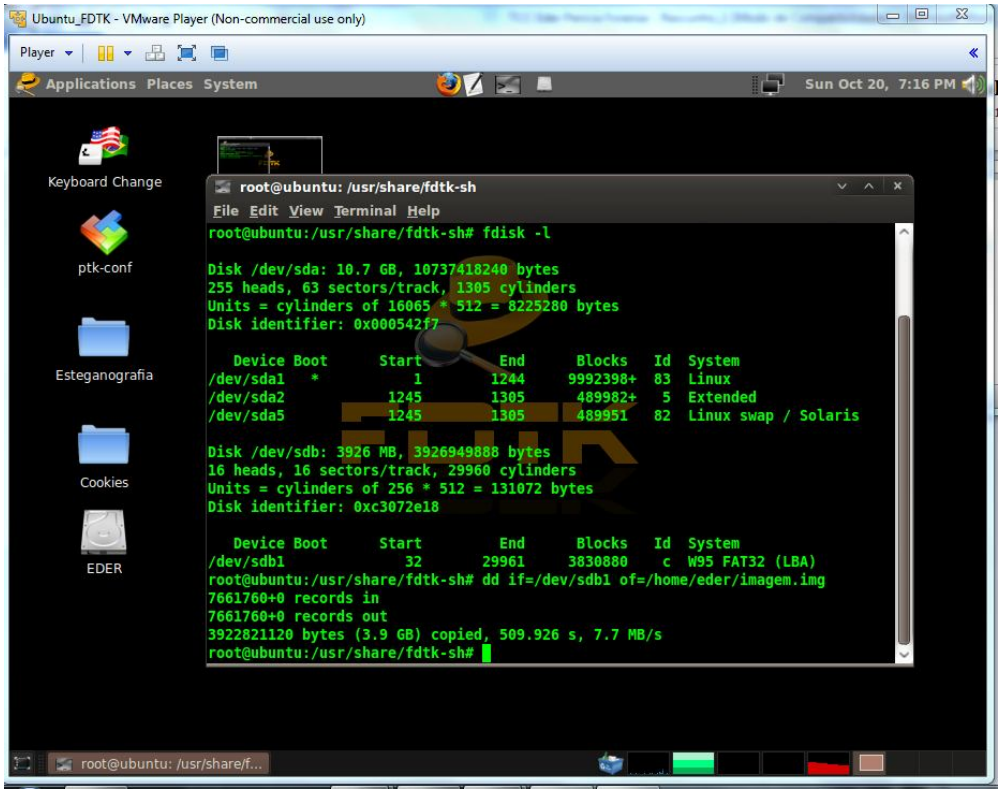



Figura 31 – Gerando a imagem através do comando dd.

Arquivo gerado e exibido na figura 43.

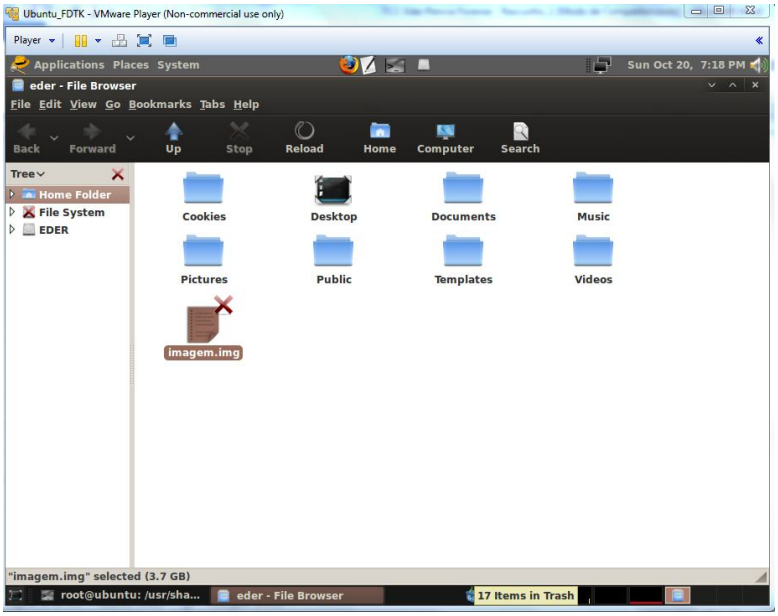



Figura 32 – Arquivo imagem.img gerado.

## 6.3 Exemplo de uso de ferramentas forenses usando o live cd BACKTRACK

### 6.3.1 Md5deep

Primeiramente cria-se um arquivo denominado arquivo_hash conforme mostrado na figura 44.


Figura 33 – Criando arquivo_hash.txt

Posteriormente serão adicionadas algumas informações dentro do arquivo_hash.txt e mostrado abaixo na figura 45 através do comando vi.

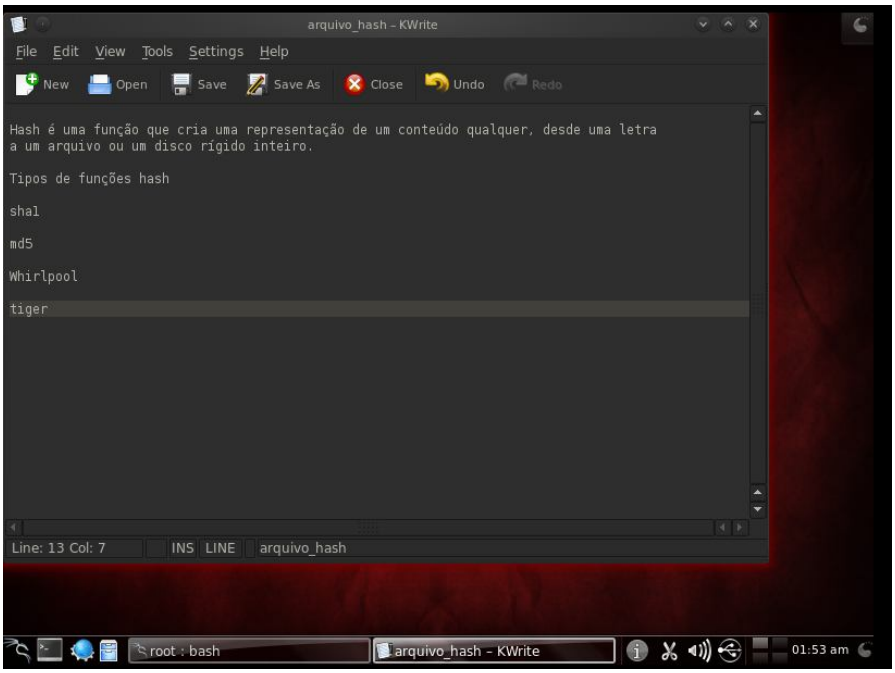



Figura 34 – Acessando o arquivo através do comando VI

Arquivo criado com a assinatura hash md5 e mostrado na figura 46.

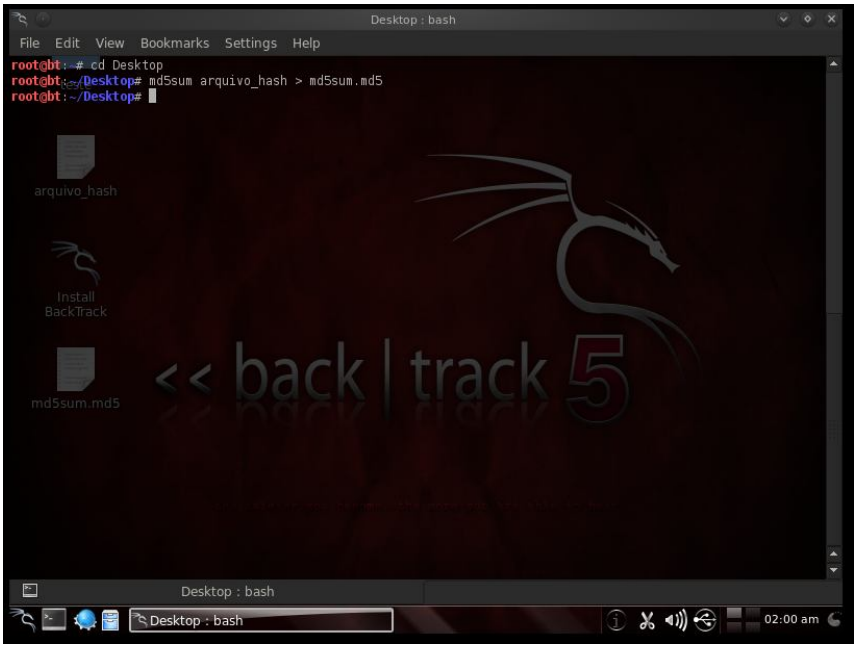
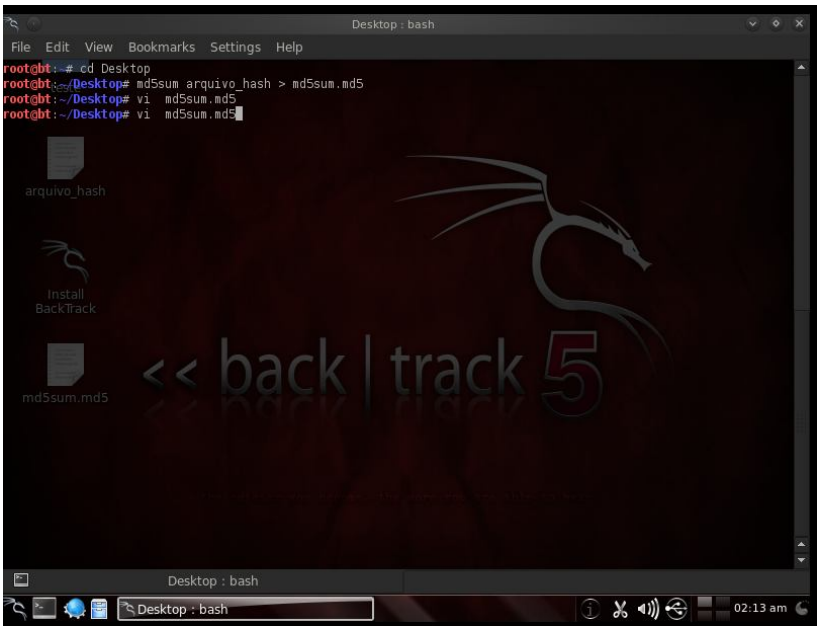
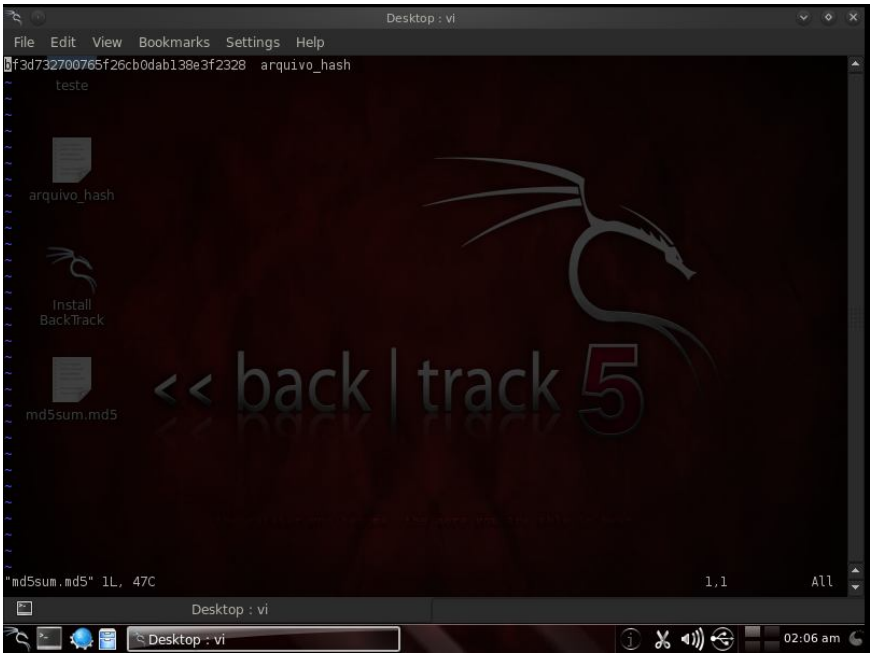



Figura 35 – Gerando o hash do arquivo através do comando md5sum.

Visualizando a hash criada através do comando VI conforme mostrado nas figuras 47 e 48.




Figuras 36 e 48 – Visualizando a hash do arquivo gerado através do comando VI

Ao final foi conferida a assinatura com o arquivo criado, conforme mostrado na figura 49.

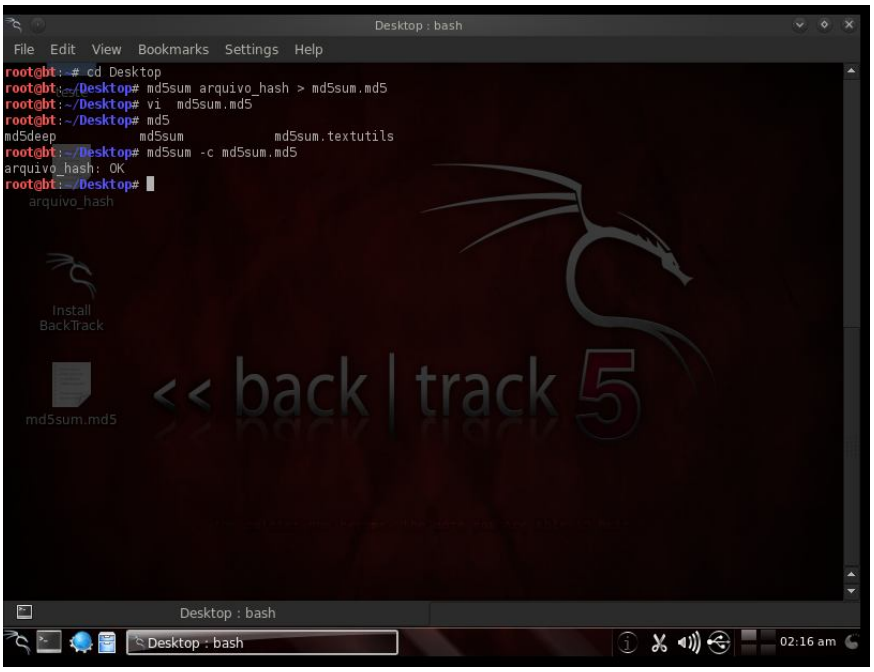



Figura 37 – Verificando a integridade da hash gerada.

### 6.3.2 Xplico

Primeiramente selecionada-se a ferramenta dentro da distribuição Backtrack 5 conforme exibido na figura 50.

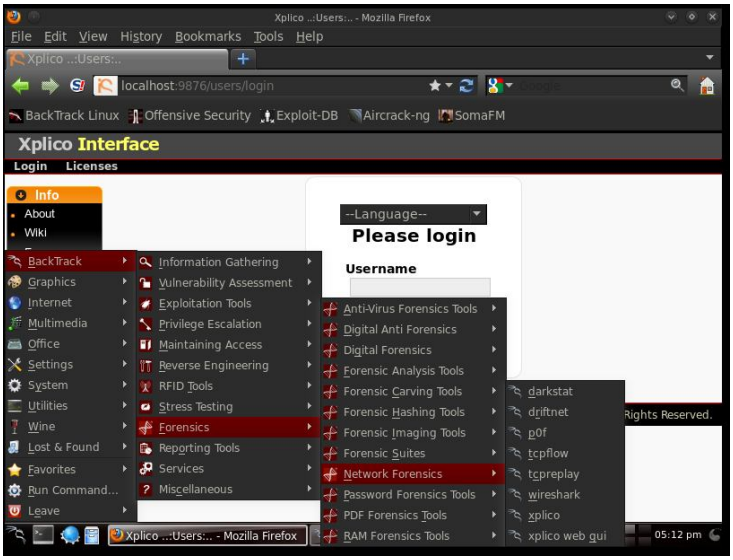



Figura 38 – Selecionando a ferramenta Xplico.

Em seguida foi feito o acesso a ferramenta através de um usuário e senha padrão, como mostrado na figura 51. Usuário: Xplico. Senha: Xplico:

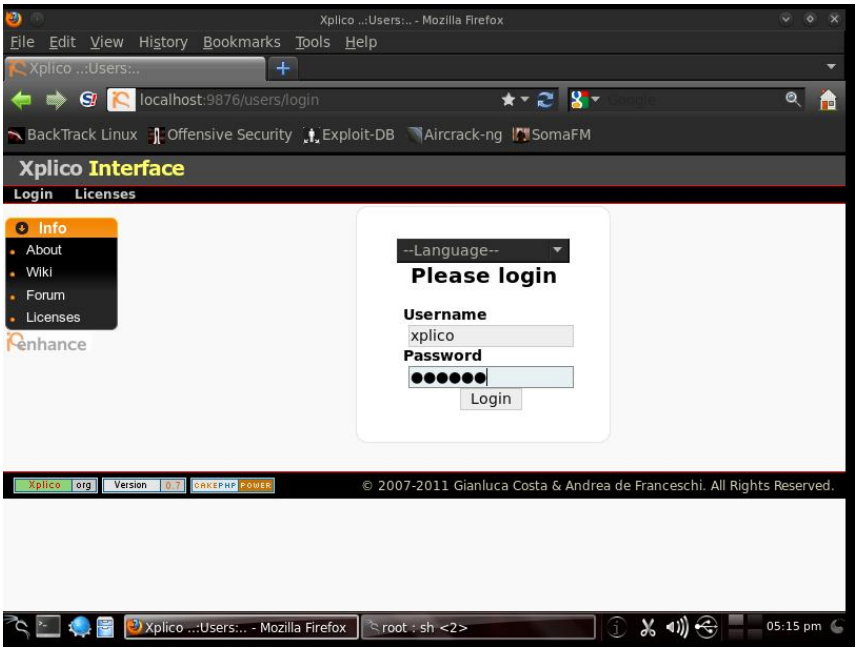



Figura 39 - Acessando a interface da ferramenta xplico.

Posteriormente, clicou-se em New Case e depois em criar um novo caso. Este exemplo foi denominado Caso01. Depois utilizou-se a opção Criate. Em DATAACQUISITION, clicou-se em Live acquisition para captura dos arquivos acessados na internet. Este processo é mostrado nas figuras 52 e 53.

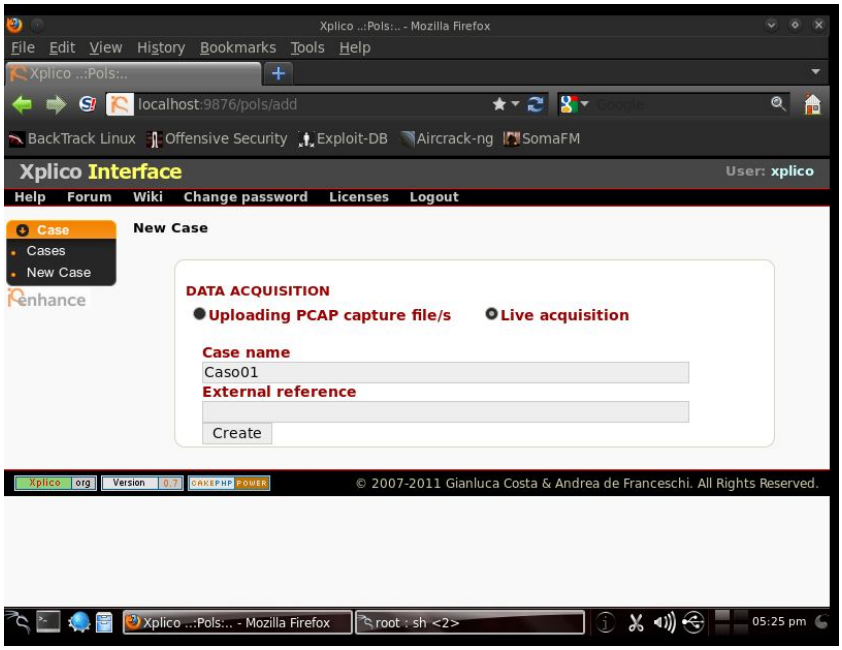



Figura 40 – Criando um arquivo de extensão .pcap de nome Caso01.

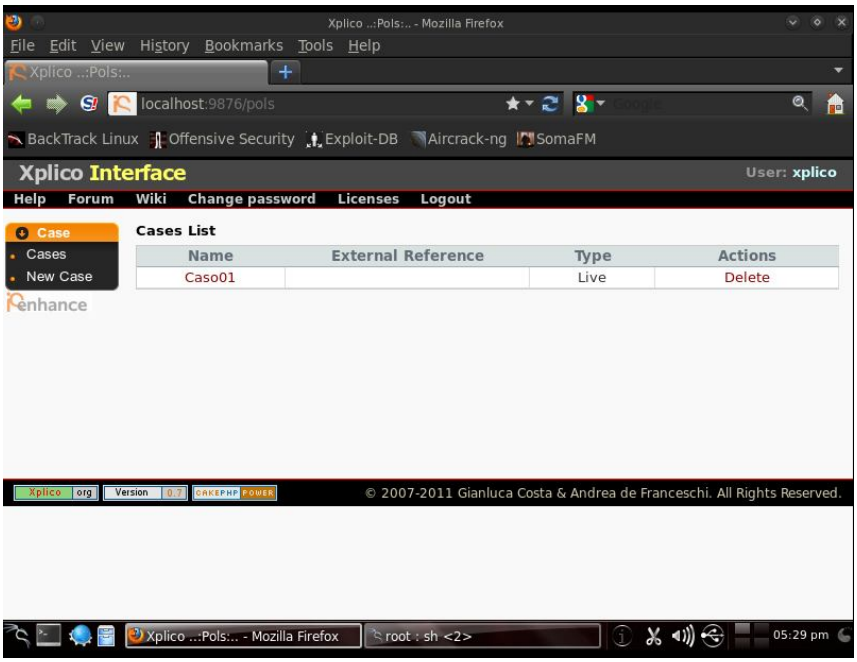



Figura 41 – Criando um arquivo de extensão .pcap de nome Caso01.

Ao final foi criada uma nova sessão denominada Evidencia01 conforme mostrado na figura 54.

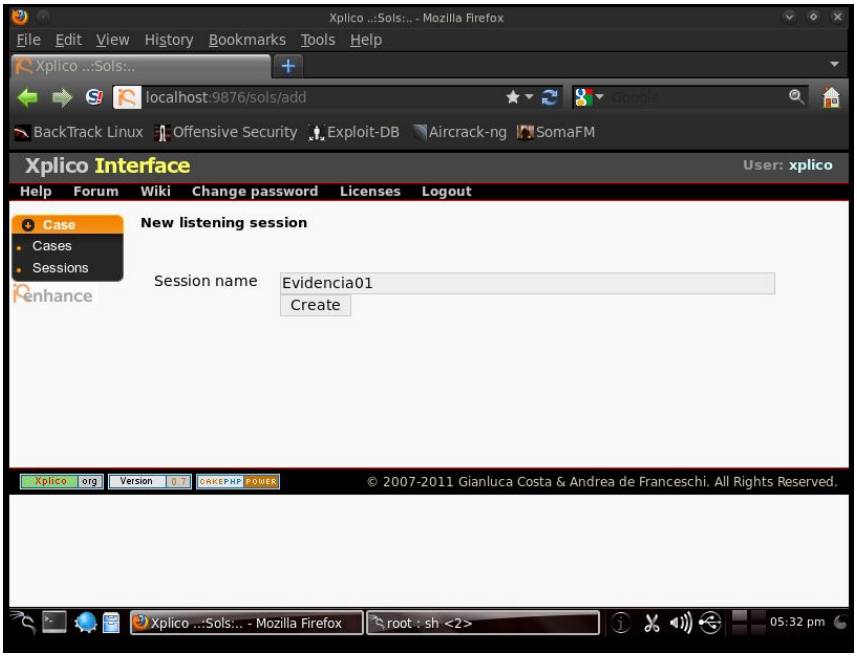



Figura 42 – Criando uma nova seção dentro do arquivo Caso01 com o nome de Evidencia01.

Ao final foi clicado em Evidencia01 para iniciar a captura mostrado na figura 55.

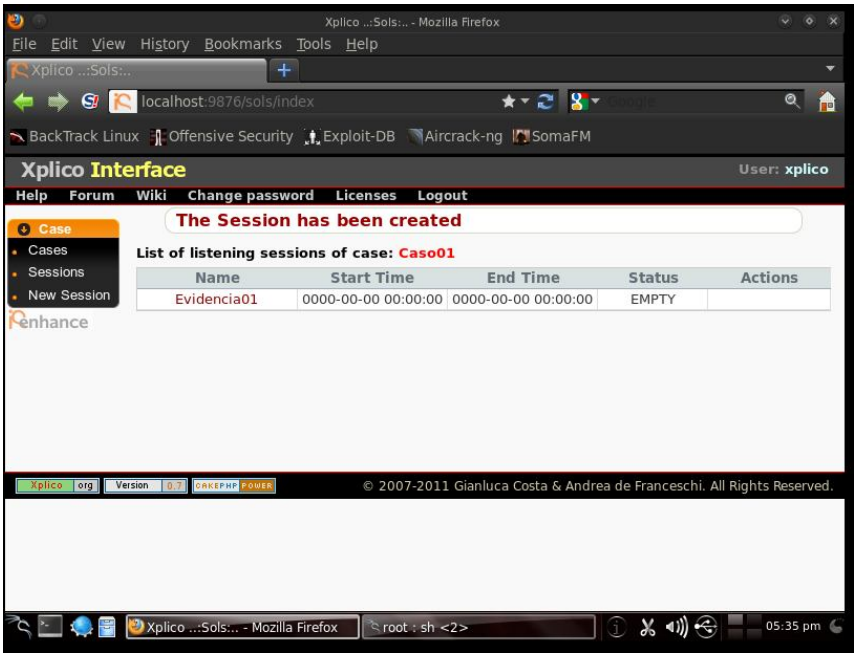



Figura 43 – Sessão Evidencia01 criada dentro o arquivo Caso01.

No item interface selecionou-se o adaptador de rede que será utilizado para captura. Neste caso como estamos utilizando um sistema Linux foi selecionado a interface eth0 e em seguida clicar em start para iniciar. Este processo é mostrado na figura 56.

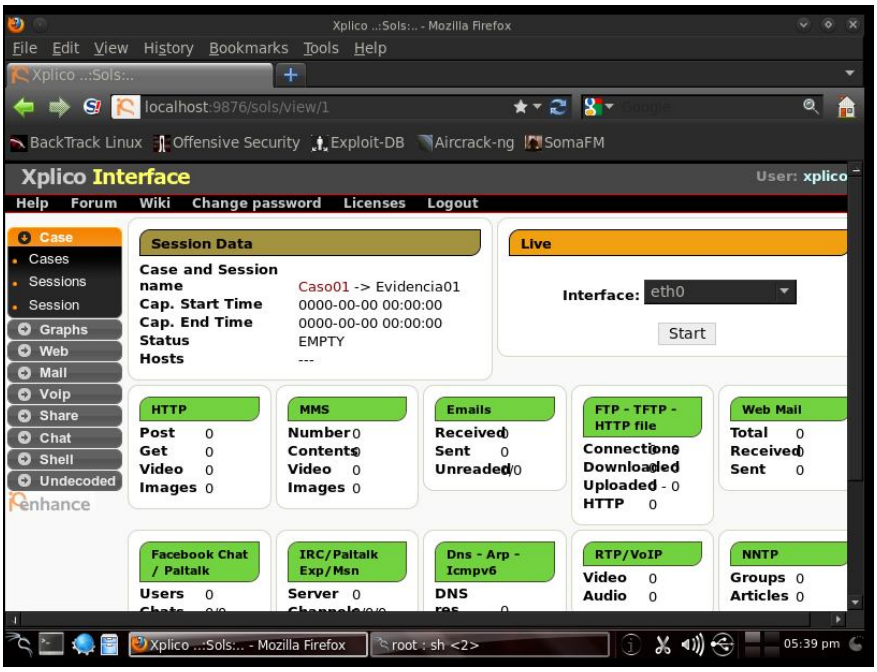



Figura 44 – Opções de captura dentro da ferramenta Xplico e inicio da captura dos dados.

Para a analise foi utilizada outra maquina virtual instalada, neste caso uma maquina virtual Ubuntu 12.04 onde foram acessados diversos sites para que a ferramenta fizesse a coleta dos pacotes. Diversos sites foram acessados para a captura dos dados, conforme figuras 57, 58, 59 e 60.

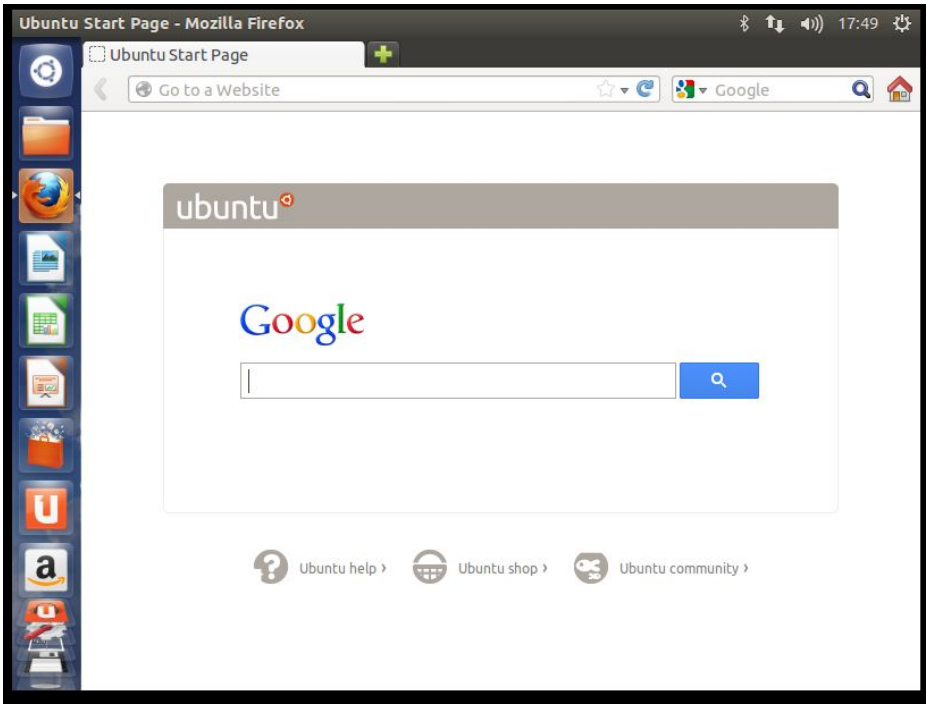



Figura 45 – Sites acessados

Sites acessados:


Figura 46 - Site do portal Uol – www.uol.com.br


Figura 47 – Página da Microsoft – www.microsoft.com.br


Figura 48 – Página da USC – www.usc.br

Conforme figura 61 clicou-se em Stop para finalizar a coleta dos dados na rede.

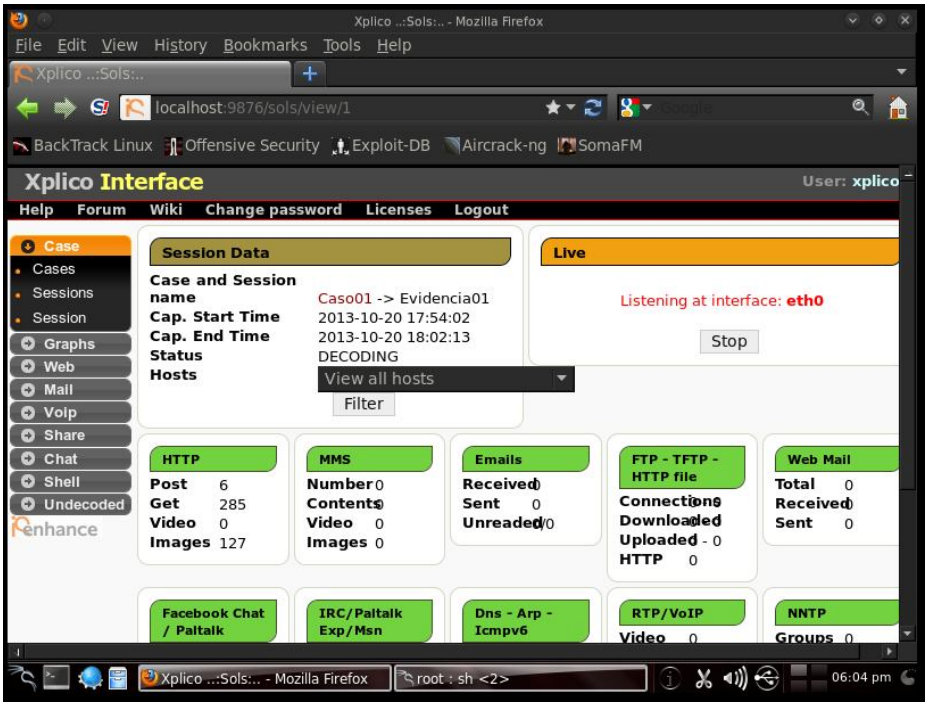



Figura 49 – Término da captura dos dados e listagem dos arquivos capturados.

Ao final, conforme mostrado na figura 62 foi feita a análise dos dados coletados. Existem diversas opções. Neste caso, foi acessado o item Web, depois clicamos em site e selecionamos o item Html. Na figura 63 é mostrado o email acessado durante a captura dos pacotes.

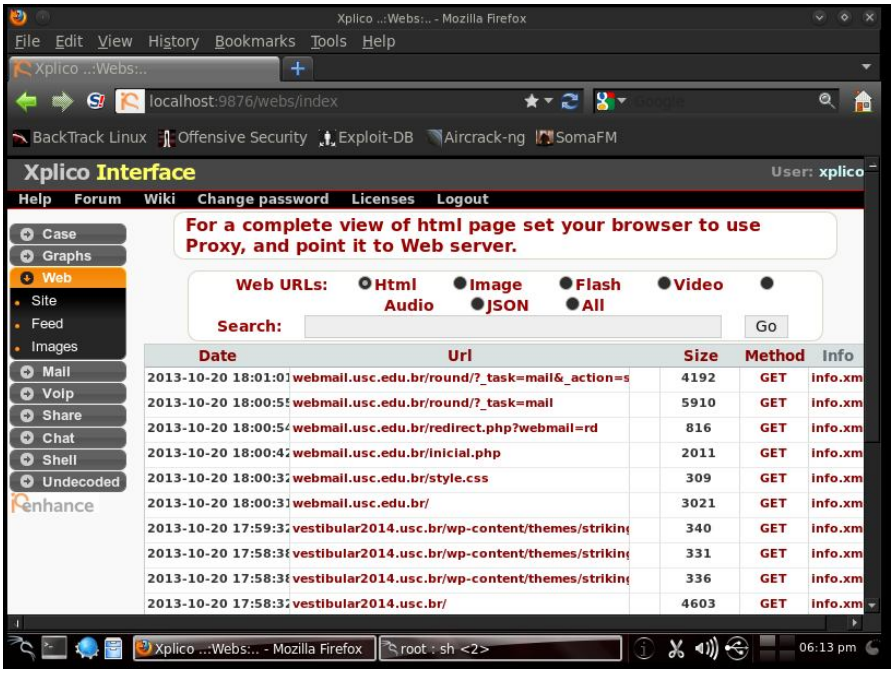



Figura 50 – Arquivos capturados pela ferramenta Xplico.


Figura 51 – Acessando email USC capturado através da ferramenta Xplico

# 7 Quadro comparativo das distribuições analisadas

Ao final dos testes foi feito um quadro comparativo com as ferramentas disponíveis para pericia forense nas distribuições estudadas.

| Quadro Comparativo das distribuições de Live CD de Pericia Forense Analisados | | | |
|---|---|---|---|
| Ferramentas Disponíveis | | | |
| | FDTK 3.0 | Backtrack 5 | C.A.IN.E. 4.0 |
| Criação de Imagens de Dados | aimage, air, btktool, dc3dd, dc3dd GUI, dd, ddrescue, dd_rescue, mondoarchive, mondorestore rdd, rddi, sdd 13 | air, dc3dd, ddrescue, ewfacquire | Guymager,air |
| Captura tela | Take-Screenshot | | |
| Análise de memoria RAM | Memdump | pdfbook, pdgmail, volafox, volatility | |
| Geração de Hash | md5sum, sha1sum | hashdeep, md5deep, sha1deep, sha256deep, tigerdeep, whirlpooldeep | quickhash |
| Identificação de Hardware | Discover, Gráfic-lshw, Hardinfo, Sysinfo, Xsysinfo | Bulk-extractor | |
| Limpar mídias | Wipe | | |
| AFFTools | Afcat, afcompare, afconvert, afinfo, afstats, afxml | | |
| Antivírus e Malware | Clamav, Nephentes | | |
| Arquivos Compactados | Cabextract, orange, p7zip, unace, unrar-free, unshield, Xarchiver, zoo | | |
| Arquivos de | Dcraw, exif, exifautotran, exifprobe, | Exiftool | |

| | | | |
|---|---|---|---|
| Imagem | exiftags,exiftran exiv2, jhead, jpeginfo | | |
| Visualizar Imagens | commix, F-Spot Photo Manager, gthumb, imageindex | | |
| Análise de Arquivos Microsoft | Antiword, Dumpter, fccu-docprop, mdb-hexdump, readpst, regLookup, reglookup-recover, reglookup-timeline, regp, tnef, ntfscat, ntfsclone, ntfsinfo, ntfslabel, eindeutig, fccu-evtreader, galleta, Ggrokervtg-builddb, Grokevt, grokevt-aadlog, grokevt-findlogs, grokevt-parselog, grokevt-ripdll | readpst, evtparse.pl, misidentify, pref.pl, reglookup | |
| Quebra de Senha | fcrackzip, john the Ripper, medussa, ophcrack | Cmospwd, fcrackzip, samdump | |
| RootKits | chkrootkit, Rkhunter | chkrootkit, Rkhunter | |
| Cripto-Stegano | Bcrypt, ccrypt, Gdecrypt, Outguess, stegcompare, stegdeimage, stegdetect, xsteg | TrueCrypt, stegdetect, | xsteg |
| Editor Hexa | Bless, ghex2, hexdump | Hexedit | gtkhash, hexeditor |
| Restaurar dados | E2undel, Foremost, gzrecover, MagicRescue, recover, recoverjpeg, scrounge-ntfs | Extundelete, fatback, foremost, magicrescue, recoverjpeg, safecopy, scalpel, scrounge-ntfs, testdisk | Photorec, testdisk, |
| Linha do Tempo – Mactimes | mac-robber, mactime | | |
| Localizar dados | Blkcalc, blkcat, blkid, blkstat, glark, gnome- | | |

| | | | |
|---|---|---|---|
| | search-tool, Meld Diff Viewer, slocate | | |
| Arquivos Pdf | | Pdfid, pdf-parser, peeddf | |
| Coleção de scripts para análise forense | | | bash scripts tools, idevice tools |
| Rede e Internet | Traceroute, mork, cookie_cruncher | Darkstat, driftnet, p0f, tcpflow, tcpreplay,wireshark, xplico, xplico web gui, mork, ptk | netdiscover, network, networktools, sharedfolders, warishark, zenmap |
| ToolKits | autopsy, ptk, | Autopsy, dff cli, dff ui, ptk, sleuthkit | Autopsy, mobius |
| Forense para dispositivos móveis | | | IphoneBackupAnalyzer, BlackberryToll, IDevicetools |
| **Total de Ferramentas Forenses disponíveis nesta versão** | 115 | 57 | 21 |

**Criação de Imagens de Dados**: Através desses ferramentas pode-se criar cópias de dispositivos de armazenamento de arquivos como hd e pendrives. Essas ferramentas podem ser usadas em modo gráfico, ou seja, através de interfaces gráficas que interagem com o usuário, como telas e menus ou através de linhas de comando onde o usuário deve fornecer os comandos necessários para a realização das tarefas. Dentre os softwares de pericia forense Linux analisadas, a ferramenta FDTK foi a que apresentou a maior quantidade de ferramentas disponíveis tanto em modo gráfico quanto através de linhas de comando. O software Backtrack 5 apresentou duas ferramentas sendo duas em modo gráfico e duas em modo de linha de comando. Já a ferramentas C.AI.N.E apresentou duas ferramentas, ambas em modo gráfico.

**Captura de tela:** Através dessa ferramenta pode-se criar cópias das telas utilizadas. Apenas a ferramenta FDTK disponibiliza esta ferramenta no conjunto de ferramentas forenses.

**Análise de memoria RAM:** Esse tipo de análise permite que dados voláteis sejam coletados, ou seja, enquanto a máquina estiver ligada. O software FDTK possui um ferramenta para esse tipo de análise enquanto a ferramenta Backtrack 5 apresenta uma ferramenta disponível. Já o software C.A.IN.E não apresentou ferramenta disponível.

**Geração de Hash:** Ferramenta utilizada para geração de Hash ou seja algoritmos que garantam a integridade dos arquivos analisados, ou seja, garante que estes arquivos não foram modificados. A ferramenta FDTK apresentou duas ferramentas. Já a ferramenta C.AIN.E apresentou uma ferramenta.

**Identificação de Hardware:** Essa ferramenta permite a identificação do hardware utilizado pela máquina utilizada. A ferramenta FDTK apresentou cinco ferramentas enquanto a ferramenta Backtrack 5 apresentou uma ferramenta enquanto a ferramenta C.A.IN.E não apresentou ferramenta disponível.

**Limpar mídias:** Esta ferramenta permite a completa exclusão dos arquivos dentro de um dispositivo de armazenamento. Dentro das ferramentas analisadas, apenas a FDTK apresenta uma ferramenta para análise forense.

**AFFTools;** Permite a geração de imagem dos dados das mídias utilizando o padrão aff (Advanced Forensic Format). Dentre as ferramentas analisadas, apenas a ferramenta FDTK apresentou ferramentas disponíveis (seis ferramentas no total).

**Antivírus e Malware**: Apenas a ferramenta FDTK apresentou ferramentas disponíveis (duas ferramentas no total).

**Arquivos Compactados:** Permite combinar vários arquivos em uma única pasta compactada para economizar espaço de armazenamento ou para compartilhar estes arquivos. Apenas a ferramenta FDTK apresentou ferramentas disponíveis (oito ferramentas no total).

**Arquivos de Imagem:** Ferramentas usadas para ler, escrever e editar metadados em vários tipos de arquivos. O software FDTK apresentou nove ferramentas e o software Backtrack 5 apresentou uma ferramenta. O software C.A.IN.E não apresentou ferramenta disponível.

**Visualizar Imagens:** Apenas o software FDTK apresentou ferramentas disponíveis (quatro ferramentas no total).

**Análise de Arquivos Microsoft:** Essas ferramentas permitem analisar os diversos formato de arquivos utilizados em sistemas Microsoft Windows durante a investigação. O software FDTK apresentou um total de vinte e três ferramentas enquanto o software Backtrack 5 apresentou um total de 5 ferramentas. A distribuição C.A.IN.E não apresentou nenhuma ferramenta.

**Quebra de Senha:** O software FDTK apresentou um total de quatro ferramentas enquanto a distribuição Backtrack 5 apresentou um total de três ferramentas. A distribuição C.A.IN.E não apresentou nenhuma ferramenta.

**RootKits:** O software FDTK e a distribuição Backtrack 5 apresentaram um total de duas ferramentas. A distribuição C.A.IN.E não apresentou nenhuma ferramenta.

**Cripto-Stegano:** Ferramentas que permitem a detecção técnicas de criptografia e esteganografia usadas em ocultação de dados em arquivos e imagens. O software FDTK apresentou um total de oito ferramentas, o software Bactrack 5

apresentou um total de duas ferramentas, enquanto a distribuição C.A.IN.E apresentou uma ferramenta.

**Editor Hexa:** Estas ferramentas facilitam a compreensão dos dados armazenados e a busca por informações específicas dentro de uma investigação forense. O software FDTK apresentou um total de duas ferramentas, o software Backtrack 5 apresentou uma ferramenta disponível enquanto a ferramenta C.A.IN.E apresentou duas ferramentas disponíveis.

**Restaurar dados:** Estas ferramentas permitem recuperar arquivos que foram perdidos, excluídos ou alterados. O software FDTK apresentou um total de sete ferramentas. O software Backtrack 5 apresentou um total de nove ferramentas. O software C.A.IN.E apresentou um total de duas ferramentas.

**Linha do Tempo – Mactimes:** Apenas o software FDTK apresentou ferramentas disponíveis (duas ferramentas no total).

**Localizar dados:** Apenas a ferramenta FDTK apresentou ferramentas disponíveis (oito ferramentas no total).

**Arquivos Pdf:** Ferramenta usada na visualização de arquivos no formato .pdf. Apenas a ferramenta Backtrack 5 apresentou ferramentas disponíveis (três ferramentas no total).

**Coleção de scripts para análise forense:** Conjunto de códigos usados para análise forense. Apenas o software C.A.IN.E apresentou ferramentas disponíveis (duas ferramentas no total).

**Rede e Internet**: O software FDTK apresentou um total de quatro ferramentas, o software Backtrack 5 apresentou onze ferramentas disponíveis enquanto a ferramenta C.A.IN.E apresentou seis ferramentas disponíveis.

**ToolKits:** Conjunto de ferramentas disponíveis em um software usados para análise dos dados em uma investigação forense. O software FDTK apresentou um total de duas ferramentas, o software Backtrack 5 apresentou cinco ferramentas disponíveis enquanto o software C.A.IN.E apresentou duas ferramentas disponíveis.

**Forense para dispositivos móveis:** Conjunto de ferramentas para cópia de dispositivos de móveis, neste caso principalmente Iphones e Blackberry. Apenas o software C.A.IN.E apresentou ferramentas disponíveis (três ferramentas no total).

## 8. CONSIDERAÇÕES FINAIS

O principal objetivo deste trabalho foi colaborar com estudo sobre Computação forense e softwares livres que podem ser utilizados para estudo desta área da Informática. Um assunto instigante e novo no meio tecnológico, mas com uma grande perspectiva de crescimento. É uma área que vem se tornando muito utilizada, devido principalmente ao grande aumento nos crimes envolvendo o meio informático.

Através do estudo realizado pode-se mostrar a existência de ferramentas gratuitas que facilitam e otimizam as tarefas executadas pelos profissionais de Forense Computacional. Tem a questão econômica como grande vantagem já que são gratuitos. A utilização de máquinas virtuais permite a simulação de diversas máquinas ao mesmo tempo dentro de um mesmo equipamento permitindo utilizar diversas distribuições. Neste caso foram testadas três distribuições baseadas no sistema operacional Linux Ubuntu: Backtrack 5, FDTK e C.A.IN.E. Houve uma grande dificuldade para a elaboração deste trabalho devido à escassez de literatura e materiais pertinentes a este assunto, principalmente na língua portuguesa. A falta de material deve-se a ser uma área recente.

As ferramentas apresentadas possuem diversas ferramentas que podem auxiliar o perito a descobrir informações que podem levar a solução do caso analisado. Estas ferramentas permitem ao profissional a recuperação de diversos tipos de dados dentro dos diversos tipos de aparelhos, sejam dispositivos móveis como celulares e pendrives, computadores e também análise do tráfego de rede e detecção de possíveis ataques realizados por outros usuários.

Dentre as 3 distribuições, a distribuição Backtrack 5 apesar de não possuir a maior quantidade de ferramentas disponíveis especificamente para análise forense,

é aquela que possui a maior quantidade de informações sobre as ferramentas contidas na distribuição permitindo ao usuário utilizar essas ferramentas em situação de investigação forense. Já distribuição FDTK apesar de possuir diversas ferramentas, ainda precisa de maior documentação das funcionalidades delas, bem como correções na funcionalidade das ferramentas contidas na distribuição. O mesmo ocorre com a distribuição Linux C.A.IN.E. que, mesmo com o objetivo de se priorizar o uso interfaces gráficas, possui pouca documentação além de ter a menor quantidade de ferramentas disponíveis em relação as outras ferramentas analisadas o que dificulta o aprendizado e sua utilização. Por fim algumas das ferramentas contidas nestas distribuições foram testadas visando mostrar aplicações das técnicas na análise forense computacional.

Através deste estudo pode-se constatar que a computação forense tem muito que desenvolver e inovar. É necessário muito aperfeiçoamento no que se refere a métodos e tecnologias na obtenção das evidencias necessárias para a solução dos crimes de informática. Apesar de ser uma área recente, já existe muita demanda de profissionais capacitados, que realmente são conhecedores dos procedimentos seguidos pela área cientifica forense. Nesta era, em que estamos conectados em todos os lugares, os problemas e incidentes tendem a aumentar, o mercado de segurança da informação é promissor. Também há necessidade de se atualizar as leis brasileiras para que os crimes de informática possam ser atendidos de uma forma melhor juridicamente falando. A computação forense tem o que contribuir para a sociedade no que se refere a garantia de direitos e deveres por parte dos cidadãos.

## 8.1 TRABALHOS FUTUROS

Em decorrência do desenvolvimento deste trabalho, foi possível perceber que vários assuntos importantes merecem ser melhor detalhados, no entanto, por não pertencerem ao escopo principal ou por serem bastante extensos, a sugestão é que sejam elaborados em trabalhos futuros. Algumas ferramentas foram testadas mas

devido a grande quantidade de ferramentas disponíveis há a necessidade de que mais ferramentas ainda possam ser testadas.

## 9 APÊNDICE

## DESCRIÇÃO DAS FERRAMENTAS FORENSES DAS FERRAMENTAS ANALISADAS

### BACKTRACK LINUX


Figura 1 -Ferramentas forenses do Backtrack 5

No software Backtrack 5 as ferramentas forenses estão divididas nos seguintes tópicos:

### ANTI VIRUS FORENSIC TOOLS (FERRAMENTAS FORENSES ANTI-VÍRUS)

**Chkrootkit**

Chkrootkit é um utilitário que irá verificar se há sinais de que um dispositivo está infectado com um rootkit. Ele usa utlitários padrão para análise, como awk, grep, netstat, cut, echo, entre outros, a fim de detectar as assinaturas que indiquem ser rootkits (NELSON; STEDING-JESSEN, 2009).

**Rkhunter**

Rkhunter é outro utilitário usado para verificar se há sinais de rootkits em sistemas baseados em Unix. Ao final do teste este utilitário gera relatório com logs dos processos dentro da pasta var/log/rhkhunter (BOELEN, 2006).

ANTI DIGITAL FORENSICS (FORENSE ANTI-DIGITAL)

**TrueCrypt**

Este software é usado para criar arquivos criptografados usando várias cifras de criptografia. Ele contém recursos como partições escondidas dentro do arquivo, bem como a capacidade de usar os arquivos e senhas de texto como chaves para a criptografia de arquivos. (LE ROUX, 2000).

DIGITAL FORENSICS (FORENSE DIGITAL)

**Hexedit**

É um programa que dá ao usuário a capacidade de visualizar um arquivo em vista hexadecimal e ASCII. Ele oferece a capacidade de ler um dispositivo como um arquivo. Ele inclui construir em atalhos de teclado para torná-lo rápido e fácil de

editar e analisar arquivos, incluindo pular para posições de memória específicas, cortar e colar, mudar pontos de vista, modos e sintaxes semelhantes ao do emacs (ROGOYSKI, 1999).

## FORENSIC ANALYSIS TOOLS (FERRAMENTAS DE ANÁLISE FORENSE)

### Bulk_extractor

Bulk_extractor é um utilitário que varre muitos tipos de armazenamento de informações (arquivos, pastas) e envia informações de que ele encontra neles sem analisar o sistema de arquivos ou estruturas do sistema de arquivos O que separa bulk_extractor de outras ferramentas similares é a sua velocidade (BRADLEY; GARFINKEL, 2013).

### Evtparse.pl

Este utilitário leva arquivos evt, que contêm informações de log para uso pelo gerente do evento, e analisa-los em algo útil para os investigadores. Especificamente, ele despeja os eventos como uma linha do tempo (CARVEY, 2009).

### Exiftool

Exiftool permite aos usuários ler ou escrever metadados (como EXIF) de imagem, vídeo e arquivos de áudio. O formato exif  permite a gravação pela câmera de informações adicionais no arquivo de imagem gerado (HARVEY, 2003).

### Missidentify

A ferramenta missidentify encontra 32 arquivos executáveis do Windows. É possível pesquisar de forma recursiva através de pastas, a fim de encontrá-los, e, em seguida, exibe os resultados de volta para o usuário (KORNBLUM, 2008).

**Mork.pl**

É um script escrito em linguagem Perl que irá retirar informações de um arquivo de banco de dados Mork. Arquivos mork foram previamente usados por programas Mozilla para armazenar informação, tais como histórico de navegação Firefox, Thunderbird e contatos (ZAWINSKI, 2004).

**Pref.pl**

É um script escrito em linguagem Perl, que pode analisar arquivos prefetch do Windows nas versões XP/Vista/7. Estes são usados para armazenar em cache informações sobre inicialização ou aplicativo de execução (que DLLs, outros arquivos são usados), e, portanto, o sistema operacional pode pré-carregar os arquivos e otimizar a localização dos arquivos no disco rígido, permitindo assim que o aplicativo para iniciar e arrancar para terminar mais rápido. A saída pode ser definida com valores separados por vírgulas (. csv) para facilitar a visualização (GINGRAS, 2009).

**Stegdetect**

Stegdetect é um programa que tentará detectar mensagens estereografadas embutidos na mídia. Ele é capaz de detectar vários métodos de esteganografia diferentes ocultas em imagens JPEG, podendo assim alertar ao usuário de que os dados podem ter sido ser incorporados no arquivo (PROVOS, 2004).

**Vinetto**

Vinetto é uma ferramenta que é utilizada para analisar arquivos thumbs.db. Esse arquivo é responsável por conter informações das imagens do diretório onde

se encontram. Por padrão, este arquivo encontrasse oculto. Ele é capaz de ler esses arquivos thumbs.db e extrair informações sobre as imagens encontradas no sistema (ROUKINE, 2006).

## FORENSIC TOOLS CARVING (EXTRAÇÃO DE DADOS)

### Fatback

Fatback é uma ferramenta que serve para recuperar arquivos apagados do sistema de arquivos FAT. Ele  uma imagem de um sistema de arquivos FAT, e, em seguida, envia todos os arquivos apagados em um diretório determinado pelo usuário. Tabela de Alocação de Arquivos (FAT) é um sistema de arquivos usado pelo MS-DOS e outros sistemas operacionais baseados em Windows para organizar e gerenciar arquivos (HARBOUR, 2005).

### Foremost

Acima de tudo é um utilitário especializado em extração de arquivos. Pode trabalhar com arquivos de imagem, como aqueles criados pelo comando dd e irá procurar por cabeçalhos de arquivo, a fim de recuperar os arquivos. Ele retorna informações para o usuário, a saída de arquivos encontrados em um diretório pré-determinado definido pelo usuário (KENDALL; KORNBLUM, 2001).

### Magicrescue

Magic Rescue é um programa que procura uma imagem de sistema de arquivos através de um "número mágico" de bytes, e tenta recuperá-los. Números mágicos são, basicamente, vários bytes de dados que funcionam como um

identificador de arquivo, dando informações básicas, como tipo de arquivo (JENSEN, 2010).

**Recoverjpeg**

Recoverjpeg é outro utilitário para recuperar imagens JPEG a partir de um sistema de arquivos. Recoverjpeg pode tirar a entrada ou como uma partição (como / dev/sda1) ou um arquivo de imagem, como os produzidos pela dd (TARDIEU, 2004).

**SafeCopy**

Safecopy é um programa usado para recuperar dados tanto quanto possível a partir de um dispositivo danificado, como um disco rígido ou drive USB. Ao contrário de outros programas, como o dd, gato, ou cp, o SafeCopy é especializado em aparelhos danificados. Outros programas vão parar de ler dados de uma vez por área danificada é atingido, enquanto Safecopy vai ler para um ponto designado pelo usuário, independentemente de áreas danificadas. Ele faz isso através da identificação das áreas danificadas e pulando em torno deles (CORAX, 2009).

**Scalpel**

O processo é feito a partir de uma imagem de disco ou partição fazendo analise dos cabeçalhos e rodapés dos arquivos para o reconhecimento dos mesmos. Ele não leva em consideração o sistema de arquivos para extrair os dados, por isso, funciona em todas as partições (FAT, NTFS, Ext2, Ext3 e Ext4). NTFS (New Technology File System – Sistema de Arquivos de Nova Tecnologia) é uma sistema de arquivos baseado em Windows sucessor do FAT usado para organização de dados em dispositivos de armazenamento enquanto o Ext2, Ext3 e

Ext4 (Extended File System) são padrões organização de armazenamento de dados em Linux (RICHARD III, 2005).

### Scrounge-ntfs

Scrounge-ntfs é um utilitário que pode ser usado para recuperar informações de uma partição NTFS. Ele usará as informações fornecidas pelo usuário, a fim de reconstruir a árvore de arquivos, que é coloca em outra partição. Este programa requer que você saiba o início e fim de bloco do sistema de arquivos (VALTER, 2010).

### Testdisk

TestDisk é um programa que se especializou na recuperação de partições de disco perdido, e fazer discos de boot. Ele tem a capacidade de reconstruir tabelas de partição, reconstruir os setores de inicialização, corrigir o Master File Table (MFT), recuperar arquivos, e muito mais. O Master File Table (MFT) é um banco de dados que mantem informações sobre todos os arquivos do sistema de arquivos NTFS. Entre as informações podemos citar hora, tamanho, nome e localização, incluindo do próprio MFT (GRENIER, 2011).

## Ferramentas Hashing forenses

### Hashdeep

Hashdeep é um utilitário que pode calcular hashes para muitos arquivos, olhando de forma recursiva através de diretórios e hashes de computação para cada arquivo encontrado. Ele também contém recursos para comparar e mensagem de

auditoria digere. Por padrão, ele calcula o hash MD5 e SHA256 dos arquivos, embora outros tipos podem ser especificados. Disponíveis tipos de hash são MD5, SHA1, SHA256, Tiger, e Whirlpool. Tiger é uma função hash otimizada para processadores de 64 bits podendo ser utilizada também em processadores de 32 bits. O MD5 (Message-Digest algorithm 5) é um algoritmo de hash de 128 bits unidirecional, usado por softwares com protocolo ponto-a-ponto (P2P) para a verificação de integridade e logins. WHIRLPOOL é uma função hash desenvolvida por Vincent Rijmen e Paulo SLM Barreto que opera em mensagens de menos de $2^{256}$ bits de comprimento, e produz uma compilação de mensagem de 512 bits (KORNBLUM, 2003).

**Md5deep**

Md5deep é uma ferramenta usada para calcular e comparar mensagem do tipo MD5 (KORNBLUM, 2003).

**Sha1deep**

Sha1deep é uma ferramenta usada para calcular e comparar mensagem do tipo sha1 (KORNBLUM, 2003).

**Sha256deep**

Sha256 deep é uma ferramenta usada para calcular e comparar mensagem do tipo sha256 (KORNBLUM, 2003).

**Tigerdeep**

Tigerdeep é uma ferramenta usada para calcular e comparar mensagem do tipo tiger (KORNBLUM, 2003).

### Whirlpooldeep

É uma ferramenta usada para calcular e comparar mensagem do tipo whirlpool (KORNBLUM, 2003).

## FERRAMENTAS DE IMAGEM FORENSE

### Air

AIR, ou Automated Imagem e Restore, é um utilitário usado para criar imagens de disco forense de unidades do dispositivo. É uma interface GUI (Graphical User Interface ou Interface de Usuário Gráfica) para dd/dc3dd, utilizado para criar a imagem (GIBSON; BASSETTI, 2011).

### Dc3dd

Dc3dd é uma versão alterada do dd, que é utilizado para operar as funções de disco de baixo nível. dc3dd contém vários recursos que são de grande utilidade para investigação forense, incluindo recursos que ajudam a proteger o disco original a ser copiado. O programa pode escrever um único valor hexadecimal ou uma cadeia de texto para o dispositivo de saída para fins de limpeza. hashing por partes e, em geral, com vários algoritmos e janelas de tamanho variável. Suporta MD5, SHA-1, SHA-256 e SHA-512. Hashes podem ser calculados antes ou depois de conversões são feitas. metros Progresso com entrada automática / tamanho do arquivo de saída sondagem log combinada para hashes e erros de erro de agrupamento (KORNBLUM, 2002).

### Ddrescue

Ddrescue é uma ferramenta usada para copiar dados de um arquivo ou dispositivo para outro. No caso de um dispositivo danificado, tenta reconstruir as áreas danificadas, ao contrário dd, que simplesmente enche as áreas danificadas com zeros. ddrescue também pode ser usado para mesclar exemplares danificados um arquivo juntos, criaram uma única cópia do arquivo com nenhum dano (DIAZ, 2004)

## Ewfacquire

Ewfacquire é uma ferramenta usada para criar imagens de disco no formato EWF. EWF (Expert Witness Compression Format) imagens são usados em vários kits de ferramentas forenses, incluindo o EnCase eo FTK (Forensic Toolkit). Ele inclui vários sumários de mensagem incluindo MD5 e SHA1(MASTWIJK, 2006).

## FORENSES SUITES

### PTK

PTK é uma ferramenta forense, similar ao kit de ferramentas sleuthkit. Ele contém construído em módulos, a fim de analisar quase qualquer tipo de mídia ou tipo de arquivo que pode ser encontrado em uma investigação forense. Ele é baseado em navegador, e precisa, primeiro, ter um banco de dados MySQL configurado (DFLABS, 2009).

### Autopsy

Autopsy é uma GUI (utiliza interface web) para ferramentas encontradas na forense sleuthkit toolkit. Autopsy é especializada em análise de imagens de disco, e pode recuperar a informação a partir deles usando funções de pesquisa ou de pesquisa (CARRIER, 2008).

## Sleuthkit

Sleuthkit é uma ferramenta forense que contém vários utilitários que podem ser usados em uma investigação forense digital. Sleuthkit em si não é um programa, mas sim é o nome dado à coleção de muitos programas. Alguns desses utilitários incluídos são: ils, blkls, fls, fsstat, ffind, mactime, disk_stat (CARRIER, 2008).

**FORENSE DE REDE**

## Driftnet

Driftnet é um utilitário de rede que fareja o tráfego de imagens e outras mídias, e as exibe em uma janela X. Isso é útil durante as investigações onde os hábitos de Internet dos usuários estão sendo monitorados. Ao invés de sniffer, todo o tráfego usando utilitários como o Wireshark, escolhendo automaticamente as imagens e meios de comunicação e exibi-las ao usuário (LIGHTFOOT, 2001).

## P0f

P0f é um identificador de host passiva. p0f usa a técnica de fingerprinting que olha para a estrutura de pacotes TCP / IP do host, a fim de descobrir o sistema operacional e outras propriedades do host. O que diferencia p0f além de outros analisadores hospedeiras é que p0f é completamente passivo. Todo o exército tem que fazer é conectar-se à mesma rede ou ser contactado por um outro host na rede. Os pacotes gerados por essas transações são o suficiente para dar ao p0f dados suficientes para adivinhar o sistema (ZALEWSKI, 2012).

### Tcpreplay

Tcpreplay é um conjunto de utilitários de rede que podem levar anteriormente cheirou tráfego e repetir os pacotes na rede ao vivo. Isso é muitas vezes usado para dispositivos na rede, como firewalls ou Prevenção / Sistemas (IPS / IDS) de detecção de intrusão de teste. A suíte é composta por tcpprep, tcprewrite, tcpreplay, tcpreplay-edit, tcpbridge e tcpcapinfo. **tcpprep:** analisar arquivos de captura de pacotes para determinar cliente / servidor e criar caches para uso por tcpreplay e tcprewrite **tcprewrite:** editar arquivos de captura de pacotes em cabeçalhos **tcpreplay:** injetar arquivos de captura de pacotes de volta para a rede ao vivo **tcpreplay-edit:** repetição e editar arquivos em a rede **tcpbridge:** ponte duas seções de uma rede em conjunto, utilizando tcprewrite **tcpcapinfo:** arquivos de captura de pacotes matérias decodificar e depurá-los (BING; TURNER, 2001).

### Wireshark

Wireshark é uma ferramenta captura de pacotes e do programa de análise que tem sido usado por milhares de profissionais e amadores. O programa permite aos usuários ouvir em uma interface de rede usando libpcap, e registra o tráfego cheirou. Além de capturar os dados, o Wireshark proporciona, um método gráfica fácil de filtrar e analisar o tráfego. Isso inclui os seguintes fluxos de TCP / IP, filtrando pacotes ARP ou de transmissão, e praticamente qualquer outra opção de filtragem que você pode imaginar (COMBS, 1998).

### Xplico

Xplico é uma Ferramenta de Análise Forense de Rede (NFAT), que é especializada em extração de dados de aplicativos a partir de arquivos de captura de pacotes. Embora inclui um recurso de captura de tráfego ao vivo, é mais

adequado para pcap anaylsis. Xplico pode extrair e-mail, HTTP, VoIP, FTP e outros dados diretamente do arquivo pcap, e apresenta-lo ao usuário como os dados de aplicativos originais. Por exemplo, ele pode reconstruir uma imagem enviada via FTP a partir da captura de pacotes da sessão FTP (COSTA, 2007).

## PASSWORD FORENSICS TOOLS

### Cmospwd

Cmospwd é um cracker de senha BIOS. Com suporte para muitos modelos diferentes de BIOS, cmospwd tem diferentes métodos de quebra para cada tipo de BIOS. Uma vez que uma senha de BIOS impeça de inicializar no computador, ele exige alguma manipulação física (GRENIER, 2006).

#### Fcrackzip

Fcrackzip é um utilitário usado para quebrar a proteção por senha do arquivo Zip (LEHMANN, 1998).

### Samdump

Samdump é um utilitário que pode extrair os hashes de senha de arquivos SAM. Arquivos SAM são os arquivos localizados em sistemas baseados em Windows que contêm as senhas de usuários locais. Usando samdump, você pode recuperar os hashes de senha e, em seguida, usá-los para quebrar com outro programa.

## PDF FORENSIC TOOLS

### Pdfid

Pdfid é um utilitário que pode extrair informações úteis a partir de um arquivo PDF. Especificamente, pdfid extratos informações de cabeçalho do PDF como obj, endobj, fluxo e outras informações. Alguns exploits de PDF alteram esta informação, então pdfid às vezes pode mostrar ao usuário o que exatamente está acontecendo dentro do PDF (STEVENS, 2009).

### Pdf-parser

Pdf-parser é um programa usado para exibir informações detalhadas sobre um arquivo PDF. Um recurso muito útil é a capacidade de executar um fluxo de dados obtener um filtro, como FlateDecode e ASCIIHexDecode. Esses filtros são por vezes usados para ofuscar o código em arquivos PDF, de modo que este recurso pode ajudar a expor as tentativas de exploração. Além disso, pdf-parser pode exibir objetos e fluxos de dados individuais, bem como fornecer estatísticas para o documento PDF (STEVENS, 2009).

### Peepdf

Peepdf é uma utilidade muito completa que é usado para analisar e editar documentos PDF no nível de byte. Ele oferece o uso básico de linha de comando, mas também oferece um console interativo em profundidade. O uso da linha de comando fornece uma visão mais básica do arquivo PDF, enquanto o console interativo oferece funções mais poderosas.

## RAM FORENSICS TOOLS

### Pdfbook.py

Pdfbook.py é um utilitário que reúne informações relativas ao Facebook a partir de um processo de despejo. Em um sistema Linux executar seqüências de "el file.dump> fbookstrings" (BRYNER, 2009 ).

## Pdgmail

Pdgmail.py é um utilitário semelhante ao pdfbook.py, mas em vez de coleta de informações de dumps Facebook do processo, ele reúne informações do Gmail. (BRYNER, 2008 ).

## Volatility

A volatility é um framework escrito em Python que se especializa em análise de memória RAM. O framework volatility pode analisar dumps de memória volátil a partir de qualquer tipo de sistema, e pode fornecer uma visão profunda sobre o estado do sistema enquanto ele estava em execução (SCHUSTER, 2009).

**FERRAMENTAS FDTK**


**Figura 2 -** Ferramentas forenses do FDTK

**Custody Form (Formulário de cadeia de custódia)**

Gera um formulário de cadeia de custódia em arquivo .xls.

**DATA IMAGE GENERATE ()**

**Aimage**

Aimage é uma ferramenta para criar cópias de dispositivos de forma forense. A imagem resultante pode ser em formato bruto, como um dd, ou em formato aff. AFF significa formato forense avançado que é um formato aberto. Geração de imagem dos dados das mídias utilizando o padrão aff (GARFINKEL, 2010).

**Air**

AIR, ou Automated Imagem e Restore, é um utilitário usado para criar imagens de disco forense de unidades do dispositivo. É uma interface GUI para dd/dc3dd, utilizado para criar a imagem (GIBSON; BASSETTI, 2011).

**Blktool**

Exibe ou altera as configurações do dispositivo de bloco (hardware). Pode ser usado em dispositivos SCSI (Small Computer Systems Interface), IDE (Integrated Drive Electronics) e SATA. Deve-se tomar cuidado com o uso deste programa pois ele pode causar danos ao hardware (GARZIK, 2004).

**Dc3ddgui**

Versão gráfica para o programa dd, esta versão tem vários recursos destinados a aquisição forense de dados. (KORNBLUM, 2008).

**Dd**

Ferramenta para geração de imagem dos dados. Os dados em um arquivo ou dispositivo ou partição pode ser despejado em outro arquivo ou dispositivo ou partição (RUBIN, 2013).

**Dd_rescue**

É uma evolução avançada do comando dd, um programa de linha de comando que foi portado apenas para UNIX / Linux. Ao contrário dd, este programa não para se forem encontrados erros, ele apenas retarda o processo. Caso encontre

erros e nulos estes são substituídos. Possui a vantagem de que se pode observar o seu progresso (DIAZ, 2004).

### Mondoarchive

Faz o backup de um subconjunto de seus arquivos, de todo o seu sistema de arquivos, ou mesmo imagens de sistemas de arquivos não Linux para o CD, fita, imagens ISO ou uma montagem NFS (RABSON, 1999).

### Mondorestore

Restaurar dados de fitas, cd's, fitas, imagens isso, salvos anteriormente através do comando mondoarachive (RABSON, 1999).

### Rdd

O rdd é um programa forense utilizado para cópia de discos no Instituto Forense Holandês (Netherlands Forensic Institute [NFI]), ou seja, foi desenvolvido no intuito de facilitar investigações. Conforme a descrição do projeto, a diferença entre o rdd e os demais programas de cópia é a sua alta tolerância a erros de leitura.

### Rddi

Prompt interativo do rdd.

### Sdd

Cópia o arquivo de entrada especificado para um arquivo de saída especificado para realizar as conversões solicitadas. A entrada e saída padrão são usados por padrão. Após a conclusão, sdd informa o número de registros inteiros, a soma de bytes de entrada parcial e blocos de saída eo valor total em kilo bytes na entrada e saída.

**(HASH GENERATING) GERADORES DE HASH**

## Md5sum

Gerador hash md5.

## Sha1sum

Gerador hash sha 160bits.

**Hardware Identify**

Identificador de Hardware.

## Discover

Fornece uma interface flexível que programas podem usar para relatar uma ampla gama de informações sobre o hardware que está instalado em um sistema linux.

**Hardinfo**

Exibe informações sobre o hardware e o sistema operacional, dispositivos pci, isa pnp, usb, IDE, SCSI, serial e dispositivos de porta paralela.

**Grafic-lshw**

Lista os dispositivos de hardware em formato HTML.

**Sysinfo**

Mostra informações do computador e do sistema.

**Xsysinfo**

Exibe alguns Linux parâmetros do kernel em forma gráfica;

### Memdump

Dumper de memória para sistemas UNIX.

### Take screenshot

Ferramenta utilizada para capturar imagens de tela do computador.

### Wipe

Remove totalmente os dados das Mídias

**EXAME DOS DADOS**

### Afcat

Converte arquivos .aff para o formato raw.

**Afcompare**

Compara dois arquivos .aff ou um arquivo .aff e um arquivo .raw

**Afconvert**

Converte um arquivo .raw em um arquivo .aff

### Afinfo

Exibe informações sobre um arquivo .aff.

### Afstats

Exibe estatísticas sobre um ou mais arquivos .aff.

## Afxml

Exporta arquivos .aff para arquivos no formato xml.

### ANTIVIRUS E ANTI-MALWARE

### ClamAV

Clam AntiVirus é um programa open source (GPL) kit de ferramentas anti-vírus para Unix. Ele fornece uma série de serviços públicos, um scanner de linha de comando e avançado ferramenta para atualizações automáticas do banco de dados.

### Nepenthes

É uma ferramenta que atua como honeypot para emular vulnerabilidades e através dessas vulnerabilidades capturar vírus e worms. Um honeypot é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido (CERT, 2012).

### COMPRESSED FILES

### Cabextract

Acessar conteúdo de arquivos .cab. Arquivos .cab (CABinet file) são arquivos comprimidos que contém um conjunto de arquivos, geralmente, para instalação (CAIE, 2003).

### Orange

Ferramenta usada para manipular arquivos .cab

## P7zip

Utilizado para acessar arquivos zip

**Unace**

Ferramenta para descompactar extensões .ace

**Unrar-free**

Ferramenta para descompactar arquivos rar

**Unshield**

Ferramenta para descompactar arquivos CAB da Microsoft.

**Xarchiver**

Criar, modificar e visualizar arquivos compactados

**Zoo**

Acessar arquivos compactados .zoo

CRYPTO-STEGANO

**Bcrypt**

Usado para encriptar e decriptar arquivos usando o algoritmo blowfish. O Blowfish é um algoritmo de chave simétrica de livre distribuição, desenvolvido por Bruce Schneier, que tem como principais características o fato de possuir diversos tamanhos de chave, variando entre 32 e 448 bits

**Ccrypt**

Encriptar e decriptar arquivos e streams. É baseado no “Rijndael cipher”, algoritmo que é também utilizado pelo governo dos Estados Unidos. Esse algoritmo de mesmo nome é também conhecido como “Advanced Encryption Standard” (ou simplesmente “AES”); este padrão depende de uma chave e de um vetor de inicialização para a execução de operações de criptografia.

**GDecrypt**

Interface gráfica para montar e mapear particções encriptadas

## Outguess

É uma ferramenta universal de esteganografia digital que permite inserção de informações ocultas nos bits redundantes da fonte de dados. Ela também é capaz de extrair essas mensagens (PROVOS, 2004).

**Stegcompare**

Usado para comparar imagens jpeg e detectar a existência de esteganografia.

**Stegdimage**

Utilizado para detectar a existência de esteganografia em imagens jpeg

**Stegdetect**

Utilizada para detectar a existência diferentes tipo de esteganografia em imagens jpeg.

**Xsteg**

Interface gráfica para o comando stegdetect, para análise de imagens jpeg.

DATA MAC-TIME

## Mac-robber

É uma ferramenta de investigação digital que recolhe dados de arquivos alocados em um sistema de arquivos montado. Isso é útil durante a resposta a incidentes quando se analisa um sistema vivo ou quando se analisa um sistema morto em um laboratório.

**Mactime**

É um programa que cria uma lista ordenada cronologicamente por acessos aos diversos arquivos.

**DATA RESTORE**

**E2undel**

É uma ferramenta que recupera os dados de arquivos apagados em um sistema de arquivos ext2 no Linux. E2undel não pode manipular estruturas ext2 internos e requer apenas acesso de leitura para o sistema de arquivos onde os arquivos a recuperar estão localizados (DIEDRICH, 2002).

**Fatback**

Fatback é uma ferramenta que serve para recuperar arquivos apagados do sistema de arquivos FAT. Ele  uma imagem de um sistema de arquivos FAT, e, em seguida, envia todos os arquivos apagados em um diretório determinado pelo usuário (HARBOUR, 2005).

**Foremost**

Acima de tudo é um utilitário especializado em extração de arquivos. Pode trabalhar com arquivos de imagem, como aqueles criados pelo comando dd e irá procurar por cabeçalhos de arquivo, a fim de recuperar os arquivos. Ele retorna informações para o usuário, a saída de arquivos encontrados em um diretório pré-determinado definido pelo usuário (KENDALL; KORNBLUM, 2001)..

**Gzrecover**

Ferramenta para extrair dados de arquivos gzip corrompidos, pulando os setores de arquivos defeituosos.

**Magicrescue**

Magic Rescue é um programa que procura uma imagem de sistema de arquivos através de um "número mágico" de bytes, e tenta recuperá-los. Números mágicos são, basicamente, vários bytes de dados que funcionam como um identificador de arquivo, dando informações básicas, como tipo de arquivo.

**Ntfsundelete**

Usado para recuperar arquivos deletados em partições NTFS.

**Recover**

Ferramenta para recuperar todos inodes deletados de um disco. Inodes são estruturas responsáveis por conter informações básicas sobre seus arquivos e pastas, como permissões de acesso, identificação dos donos dos arquivos, data e hora do último acesso e alterações como também o tamanho dos arquivos.

**Recoverjpeg**

Recoverjpeg é outro utilitário para recuperar imagens JPEG a partir de um sistema de arquivos. Recoverjpeg pode tirar a entrada ou como uma partição (como / dev/sda1) ou um arquivo de imagem, como os produzidos pela dd.

**Scrounge-ntfs**

Scrounge-ntfs é um utilitário que pode ser usado para recuperar informações de uma partição NTFS. Ele usará as informações fornecidas pelo usuário, a fim de reconstruir a árvore de arquivos, que é coloca em outra partição. Este programa requer que você saiba o início e fim de bloco do sistema de arquivos (VALTER, 2010).

**FILE SEARCH**

**Blkcalc**

Cria um mapeamento número da unidade de disco entre duas imagens, uma normal e outra que contém apenas as unidades não afetadas do primeiro.

**Blkcat**

Extrai o conteúdo de uma determinada unidade de dados.

**Blkid**

É um utilitário que permite exibir informações sobre dispositivos existentes. Ele pode determinar o tipo de conteúdo (por exemplo, sistema de arquivos ou swap) que um dispositivo de bloco tem (DILGER, 2004).

**Blkls**

Lista o conteúdo de bloco de disco apagados.

**Blkstat**

Informa sobre detalhes sobre um determinado bloco do disco.

**Glark**

Glark é um programa utilizado para procurar texto em arquivos. Ele pode ser usado a partir da linha de comando ou em scripts.

**Gnome-search-tool**

É um utilitário gráfico usado para encontrar arquivos em seu sistema. A realizar uma pesquisa básica, você pode digitar um nome ou um nome parcial.

**Meld Diff Viewer**

É uma ferramenta gráfica que possibilita a comparação de arquivos ou diretórios.

**Slocate**

Este comando cria um banco de dados contendo a listagem dos arquivos do sistema e sua localização na estrutura de diretórios.

**Bless Hex Editor**

É um editor binário em modo gráfico que permite editar arquivos em uma sequência de bytes.

**Ghex2**

É um editor binário em modo gráfico que permite aos usuários visualizar e editar um arquivo binário. As características incluem localizar e substituir funções, a conversão entre binário, octal e também os valores decimais e hexadecimais.

**Hexcat**

Visualizar arquivos em formato hexadecimal.

**Hexdump**

Visualizar arquivos em formato hexadecimal.

IMAGE FILES

**Dcraw**

Utilizado para acessar imagens de câmeras digitais utilizando o formato RAW

**Exif**

É um pequeno utilitário de linha de comando para mostrar e mudar informações em formato EXIF para arquivos JPEG.

**Exifautotran**

Transforma uma lista de arquivos recebidos na entrada em apenas um.

**Exifprobe**

Lê imagens produzidas por câmeras digitais ou dispositivos semelhantes e relata a sua estrutura e os dados auxiliares e metadados contidos dentro deles.

**Exiftags**

É um programa utilizado para extrair as propriedades EXIF de uma imagem JPEG produzida por uma câmera digital.

**Exiftran**

É um utilitário de linha de comando para transformar imagens jpeg digitais.

**Exiv2**

Ferramenta de linha de comando para linux para editar metadados de fotos. Também é possível inserir, deletar, modificar ou renomear metadados.

**Jhead**

Ferramenta usada para exibir e manipular dados contidos no cabeçalho do arquivo .exif das imagens .jpeg em câmeras digitais. Também é possível inserir, deletar, modificar ou renomear metadados. Metadados são um conjunto de dados estruturados que identificam os dados de um determinado documento e que podem fornecer informação sobre o modo de descrição, administração, requisitos legais de utilização, funcionalidade técnica, uso e preservação.

**Jpeginfo**

Jpeginfo é uma ferramenta de linha de comando usada para gerar informações de arquivos JPEG, e também para verificar nesses arquivos.

**IMAGES VIEWER**

**Comix**

Comix é um visualizador gráfico de imagens principalmente livros de quadrinhos, mas também pode ser usado como um visualizador genérico. Pode ser imagens comprimidas em ZIP, RAR ou arquivos .tar.

**F-Spot Photo Manager**

É um aplicativo de gerenciamento de fotos projetado para Gnome desktop e padrão do Ubuntu. É utilizado para importar e organizar fotos.

**Gthumb**

Aplicativo usado para visualizar imagens e também para edição. Pode-se criar um álbum de imagens para a web, convertê-las para outros tipos de formatos, adicionar comentários nas imagens, etc.

## Imageindex

Usado para criar galerias de imagens em um determinado diretório para ser usado em entradas de diretório dentro do HTML.

**MS FILES MANIPULATE**

**Antiword**

Programa que faz a conversão de arquivos do MSWord para texto puro (.txt) ou .pdf desenvolvido para Linux.

**Dumpster**

Utilitário que permite ao usuário visualizar informações de arquivos através do uso de scripts XML.

**FCCU-Docprop**

É um utilitário de linha de comando que tenta imprimir as propriedades de arquivos do MS OLE. Arquivos MS OLE são principalmente MS Office DOC e XLS. OLE é uma tecnologia que permite que um aplicativo criar documentos compostos que contenham informações de várias fontes, mantendo todas as suas propriedades originais.

**Mdb-hexdump**

Ferramenta para manipulação de arquivos MDB. Arquivos mdb são arquivos usados no aplicativo Microsoft Access.

**Readpst**

Ferramenta para ler arquivos do MS-Outlook.

**Reglookup**

Utilitário em linha de comando para ler e consultar registros do Microsoft Windows NT/2000/XP. Também fornece recursos para filtragem de resultados baseado no caminho e tipo de dado do registro.

**Readpst**

Readpst é um utilitário de linha de comando que leva os arquivos do Microsoft Outlook PST, e os converte em arquivos no formato mbox. Arquivos mbox são mais fáceis de ler e manipular de arquivos PST, de modo que permite aos investigadores para ver o e-mail contidos nos arquivos PST. No exemplo abaixo, e-mail contido no arquivo mail.pst é convertido para o formato mbox e colocado no desktop do usuário root.

## Reglookup

RegLookUp é um utilitário que irá imprimir o conteúdo de entradas de registro em sistemas baseados em Windows NT. Ele produz a informação em um formato que é facilmente legível, o que ajuda na facilidade de pesquisa, e inclui várias opções de filtragem para fazer a saída ainda mais útil. O exemplo a seguir irá imprimir todo o conteúdo do registro encontrado em [Registro-file] path.

### Reglookup-recover

Ferramenta usada para recuperar as tentativas de vasculhar uma seção de registro do Windows para dados apagados estruturas exportando os resultados em um formato CSV.

### Reglookup-timeline

Lê um ou mais arquivos de registro para produzir uma saída classificando os arquivos conforme  atributo de tempo Mtime.

### Regp

Utilizado para cessar o conteúdo de arquivos .dat.

### Tnef

É um programa para descompactar anexos de email do outlook da microsoft.

**NTFS-PARTITIONS**

**Ntfscat**

Esta ferreamenta irá ler um arquivo ou fluxo de um volume NTFS e exibir o conteúdo da saída padrão.

**Ntfsclone**

Clonar um sistema de arquivos NTFS ou somente parte dele

**Ntfscluster**

Identificar os arquivos em uma região especificada de um volume NTFS.

**Ntfsinfo**

Obter informações sobre partições NTFS

**Ntfslabel**

Irá exibir ou alterar rótulo do sistema de arquivos no sistema de arquivos NTFS localizado no dispositivo. Também pode alterar o número de série do dispositivo.

**Ntfsls**

Usado para listar informações sobre os arquivos especificados pela opção PATH (o diretório root por padrão).

**PASSWORD BREAK**

**Fcrackzip**

Ferramenta usada de abrir ficheiros ZIP protegidos com palavra-passe ou password e os quais você perdeu essa mesma palavra-passe.

**John the Ripper**

Software que utilizado para quebrar senhas presentes em um arquivo.

**Medusa**

Crack de senhas.

**Ophcrack**

É um cracker usado para recuperar senhas do Windows.

**ROOTKITS**

## Chkrootkit

Chkrootkit é um utilitário que irá verificar se há sinais de que um dispositivo está infectado com um rootkit. Ele usa utlitários padrão para análise, como awk, grep, netstat, cut, echo, entre outros, a fim de detectar as assinaturas que indiquem ser rootkits (NELSON; STEDING-JESSEN, 2009).

**Rkhunter**

Rkhunter é outro utilitário usado para verificar se há sinais de rootkits em sistemas baseados em Unix. Ao final do teste este utilitário gera relatório com logs dos processos dentro da pasta var/log/rhkhunter (BOELEN, 2006).

**EVIDENCE ANALYZE**

**Cookie_Cruncher**

Ferramenta para análise de cookies no Windows.

## Eindeutig

Analisar bases de dados de email do Outlook Express da Microsoft (arquivos com a extensão .dbx).

**Fccu-evtreader**

É uma ferramenta usada analisar arquivos de log de eventos do Microsoft Windows.

**Galleta**

Ferramenta usada para análise de cookies produzidos pelo Microsoft Internet Explorer.

**GgrokEVT**

Coleção de scripts criados para ler o arquivos de log de eventos do Microsoft Windows NT/2000/XP/2003.

**Gokevt-addlog**

Adiciona arquivo .evt log a base de logs, necessário determinar tipo de log.

**Grokevt-dumpmsgs**

Mostra na tela as informações de mensagens colidas pelo grokevt-ripdll

**Grokevt-parselog**

Usado para analisar um log de eventos do Windows e gerar com base em recursos de mensagens armazenadas em uma base de dados.

**Grokevt-ripdll**

Ferramenta usada para extrair recursos de mensagens a partir de um arquivo PE-formatado (geralmente arquivos com extensão dll) e extrai todos os recursos de mensagens.

**Mork**

É um script escrito em linguagem Perl que irá retirar informações de um arquivo de banco de dados Mork. Arquivos mork foram previamente usados por programas Mozilla para armazenar informação, tais como histórico de navegação Firefox, Thunderbird e contatos (ZAWINSKI, 2004).

**Pasco**

Ferramenta usada que para analisar o histórico de navegação do internet explorer da Microsoft.

**Rifiuti**

Ferramenta para examinar os Info2 arquivos encontrados nas lixeiras do Microsoft Windows. Arquivos info2 são arquivos ocultos que guardam as informações dos arquivos que estão na lixeira.

**Traceroute**

Usado para análise de rede combinando os comandos ping e traceroute no mesmo aplicativo.

**Vinetto**

Vinetto é uma ferramenta que é utilizada para analisar arquivos thumbs.db. Esse arquivo é responsável por conter informações das imagens do diretório onde se encontram. Por padrão, este arquivo encontrasse oculto. Ele é capaz de ler esses

arquivos thumbs.db e extrair informações sobre as imagens encontradas no sistema (ROUKINE, 2006).

## TOOLKITS

### Autopsy

Autopsy é uma GUI (utiliza interface web) para ferramentas encontradas na forense sleuthkit toolkit. Autopsy é especializada em análise de imagens de disco, e pode recuperar a informação a partir deles usando funções de pesquisa ou de pesquisa.

### PTK

PTK é uma ferramenta forense, similar ao kit de ferramentas sleuthkit. Ele contém construído em módulos, a fim de analisar quase qualquer tipo de mídia ou tipo de arquivo que pode ser encontrado em uma investigação forense. Ele é baseado em navegador, e precisa, primeiro, ter um banco de dados MySQL configurado.

## 7.1 CAINE


**Figura 3 - Ferramentas forenses do C.A.I.N.E.**

MOBILE FORENSICS

### IPhone Analyzer

Aplicativo usado recuperar a dados a partir de um dispositivo iOS (Sistema Operacional Apple). Ele trabalha através da importação de backups produzidos pelo iTunes ou software de terceiros permitindo explorar, analisar e recuperar dados em formatos legíveis.

**Blackberry Tool**

Análise de dispositivos móveis Blackberry.

**Idevice Tools**

Conjunto de scripts usado para análise de celulares Iphone.

**NETWORK FORENSICS**

**Netdiscover**

Faz uma busca na rede usando o protocolo ***arp***, ou seja ele faz as buscas de máquinas conectadas à rede através do endereço ***ip*** da própria máquina e também através do seu ***mac adress.***

**Network**

É uma ferramenta de rede que possibilita configurar e modificar as conexões com o seu sistema.

**Networktools**

É um conjunto de ferramentas de rede orientado a cliente que atualmente contém uma ferramenta de informação da rede, um cliente shell e desktop remoto.

**Shared Folders**

Exibe pastas compartilhadas com outros usuários.

**Wireshark**

Wireshark é a famosa captura de pacotes e do programa de análise que tem sido usado por milhares de profissionais e amadores. O programa permite aos usuários ouvir em uma interface de rede usando libpcap, e registra o tráfego cheirou. Além de capturar os dados, o Wireshark proporciona, um método gráfica fácil de filtrar e analisar o tráfego. Isso inclui os seguintes fluxos de TCP / IP, filtrando

pacotes ARP ou de transmissão, e praticamente qualquer outra opção de filtragem que você pode imaginar.

**Zmap**

Aplicativo da ferramenta de nome Nmap. Eles são instalados em conjunto no mesmo pacote a partir das versões mais recentes do Nmap. A função destas ferramentas é o mapeamento da rede e auditoria de segurança ou inventário de rede, por exemplo. Ele faz a verificação de Hosts que estejam disponíveis na rede por meio de pacotes de IP. Entre os resultados disponibilizados pelo programa, ele mostra quais Sistemas Operacionais estão sendo executados nos computadores, se eles possuem firewalls, quais serviços esses hosts disponíveis possuem para disponibilização, entre outras.

**Mounter**

É uma aplicação de montagem do disco que roda na bandeja do sistema.

**Caine Interface**

É uma interface que reúne uma série de ferramentas forenses bem conhecidos, utilizadas durante o processo de pericia forense.

**Guymager**

Aplicativo usado captura de imagens forenses, permitindo obter informações sobre dispositivos conectados ao computador.

**Air**

AIR, ou Automated Imagem e Restore, é um utilitário usado para criar imagens de disco forense de unidades do dispositivo. É uma interface GUI para dd/dc3dd, utilizado para criar a imagem.

**Autopsy**

Autopsy é uma ferramenta GUI (utiliza interface web) encontradas na forense sleuthkit toolkit. Autopsy é especializada em análise de imagens de disco, e pode recuperar a informação a partir deles usando funções de pesquisa.

**Bash Scripts Tools**

Bash é um mecanismo de agregação para as inúmeras ferramentas e métodos disponíveis no linux.

**File Browser Root Mode**

Usado para acessar a pasta de arquivos no modo administrador.

**Gtkhash**

Permite verificar a integridade dos arquivos através das funções de hash. Entre essas funções suportadas incluem: MD5, MD6, SHA1, SHA256, SHA512 entre outros.

**Dvdisaster**

Aplicativo usado para armazenar dados em CD / DVD de uma forma que é totalmente recuperável, mesmo depois terem ocorrido alguns erros de leitura permitindo salvar os dados completos para um novo meio.

**Hex Editor**

Aplicativo que permite ao usuário carregar dados de qualquer arquivo, visualizar e editá-lo em qualquer hexadecimal ou ascii.

**Nbtempo**

Aplicativo usado para verificar a data de criação dos arquivos.

**Remote FileSystem Mounter**

Montagem de arquivos feitos através de modo remoto.

**Photorec**

Software de recuperação de dados de arquivos projetado para recuperar arquivos perdidos, incluindo vídeo, documentos e arquivos de discos rígidos, CD-ROMs, e imagens de memória da câmera digital.

**FRED (Forensic Register Editor)**

Editor de registro.

**Mobius**

Gerencia casos e itens de caso, fornecendo uma interface abstrata para o desenvolvimento de extensões. Casos e categorias de item são definidas usando arquivos XML.

**QuickHash**

Aplicativo usado para calcular hashes de arquivos.

**Testdisk**

Aplicativo usado para recuperar partições formatadas

**TkDiff**

Aplicativo usado para comparar as diferenças entre duas versões do mesmo arquivo.

**Xdeview**

Programa que ajuda a transmitir e receber arquivos binários através da Internet, usando o correio eletrônico ou grupos de noticias. Grupos de notícias são fóruns de discussão pela Internet em que grupos de usuários com interesses comuns se juntam para conversar sobre tudo, de software à politica.

**Xhfs**

Aplicatico gráfico usado para navegar e copiar os arquivos em volumes HFS-formatado.

**Xmount**

Cria um sistema de arquivos virtual.

**Xteg**

É uma interface gráfica para o stegdetect, uma ferramenta automatizada para a detecção de esteganografia em imagens (apenas JPEG).

## 10 REFERÊNCIAS

[DEMPSEY, 1998] DEMPSEY, L. and HEERY, R. Metada: A Current View of Practice and Issues. Journal of Documentation, v. 54, n.2, march 1998.

[TAYLOR, 1999] TAYLOR, Chris. An Introduction to Metadata. University of Queensland Library. Australia, 1999. Disponível em: www.library.uq.edu.au/iad/cteta4.html.

ABRAHÃO, M. S. A *Segurança da Informação Digital na Saúde*. Sociedade Beneficente Israelita Brasileira, 2003. Disponível em http://www.einstein.br/biblioteca/artigos/131%20132.pdf. Acesso em: 28 fev. 2013.

ANSON, S.; Bunting, S. Mastering Windows Network Forensics and Investigation. Sybex, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2005.

BackTrack 5 R3. Disponível em: http://www.backtrack-linux.org/backtrack/backtrack-5-r3-released/. Acesso em: 01 maio 2013.

BARROS, Eduardo Gomes de. Elementos básicos de perícia forense computacional. Disponível em: http://www.mpm.gov.br/mpm/servicos/assessoria-de-comunicacao/anexos/pericia_forense_computacional_conceitos.pdf. Acesso em: 25 mar. 2013.

BASSETTI, Nanni. GIBSON, Steve. Main Page 2011. Disponível em: http://sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page. Acesso em: 18 set. 2013.

BASTO. F. C. Computação Forense com Software Livre, set. 2012. Revista Segurança Digital 8º edição de 30 de setembro de 2012, Disponível em : http://segurancadigital.info/sdinfo_downloads/revista_sd/8_edicao_setembro_30_09_2012.pdf. Acesso em: 20 mar. 2013.

BING, Matt. TURNER, Aaron. History of Tcpreplay, 2001. Disponível em: http://tcpreplay.synfin.net/wiki/History. Acesso em: 18 set. 2013.

BRAGA, Ascenção A Gestão Da Informação. http://repositorio.ipv.pt/bitstream/10400.19/903/1/A%20GEST%C3%83O%20DA%20INFORMA%C3%87%C3%83O.pdf. Acesso em: 02 mar. 2013.

BRASIL. Decreto-lei n. 3689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial [da] República Federativa do Brasil, Rio de Janeiro, RJ, 13 out. 1941.

Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 12 abr. 2013.

BRASIL. decreto-lei nº 3.689, de 3 de outubro de 1941, Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 23 mar. 2013.

BRASIL. Lei Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 mar. 2013.

BRYNER, Jeff. Pdfbook.py, 2009. Disponível em: http://jeffbryner.com/pdfbook. Acesso em: 19 set. 2013.

BRYNER, Jeff. Pdgmail: new tool for gmail memory forensics, 2008. Disponível em: http://computer-forensics.sans.org/blog/2008/10/20/pdgmail-new-tool-for-gmail-memory-forensics/. Acesso em: 19 set. 2013.

BUSTAMANTE, Leonardo. Computação forense: preparando o ambiente de trabalho. Uol, julho, 2006. Disponível em: <http://imasters.uol.com.br/artigo/4335/forense/computacao_forense__preparando_o_ambiente_de_trabalho/>. Acesso em: 06 mar. 2013.

CAINE 4.0 – Pulsar. Disponível em: http://www.caine-live.net/. Acesso em: 01 maio 2013.

CAMPOS, Augusto. O que é software livre. BR-Linux. Florianópolis, março de 2006. Disponível em <http://br-linux.org/linux/faq-softwarelivre>. Acesso em: 05 maio 2013.

Capítulo 6 - Arquivos e daemons de Log. Guia Foca GNU/Linux. Disponível em : http://www.guiafoca.org/cgs/guia/avancado/ch-log.html. Acesso em: 10 maio 2013.

CARRIER, Brian. Autopsy, 2008. Disponível em: http://www.sleuthkit.org/autopsy/history.php. Acesso em: 18 set. 2013.

CARVEY, Harlan. Open source computer forensic tool kit. Revealertoolkit, 2009. Disponível em: https://code.google.com/p/revealertoolkit/source/browse/trunk/tools/evtparse.pl. Acesso em: 18 set. 2013.

CARVEY, Harlan. Windows Forensic Analysis. DVD Toolkit. Syngress Publishing, Inc, 2007

CERT. Cartilha de segurança para Internet. Disponível em: http://cartilha.cert.br/criptografia/. Acesso em: 01 maio 2013.

CLESIO, Flávio. Segurança da Informação: Básico. Revista Info Online, 06 de nov. de 2008. Disponível em: http://info.abril.com.br/forum/viewtopic.php?f=122&t=371#p145. Acesso em: 02 mar. 2013.

COMBS, Gerald. About Wireshark, 1998. Disponível em: http://www.wireshark.org/. Acesso em: 19 set. 2013.

CONGO, Mariana. Lei Carolina Dieckmann e Lei Azeredo entram em vigor hoje; saiba onde denunciar. O Estado de São Paulo, São Paulo, 02 de abr. de 2013. Disponível em: http://blogs.estadao.com.br/radar-tecnologico/2013/04/02/lei-carolina-dieckmann-e-lei-azeredo-entram-em-vigor-hoje-saiba-onde-denunciar/. Acesso em 14 abr. 2013.

CORAX, Corvus. Safecopy, 2009. Disponível em: http://safecopy.sourceforge.net/. Acesso em: 18 set. 2013.

COSTA, Gianluca. Xplico, 2007. Disponível em: http://www.xplico.org/about. Acesso em: 19 set. 2013.

DIAZ, Antônio Diaz. Ddrescue - Data recovery tool, 2004. Disponível em: http://sourceforge.net/p/dc3dd/wiki/Home/. Acesso em: 18 set. 2013.

DIEDRICH, Oliver. E2undel 2002. Disponível em: http://e2undel.sourceforge.net/. Acesso em: 18 set. 2013.

DOMINGUES, Muricy; HEUBEL, Maricê Thereza Corrêa Domingues; ABEL, Ivan José. Bases metodológicas para o trabalho científico. Bauru/SP: Editora Edusc, 2003.

FDTK-UbuntuBr – Forense Digital ToolKit. Disponível em: www,fdtk.com.br. Acesso em: 01 maio 2013.

FERREIRA, Aurélio B. de Holanda. Mini Dicionário Aurélio da Língua Portuguesa. 8. ed. Curitiba: Editora Positivo, 2010.

FREITAS, A. R. de. Perícia Forense Aplicada a Informática: Ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

GARFINKEL, Simson. Aimage, 2010. Disponível em: http://www.forensicswiki.org/wiki/Aimage. Acesso em: 19 set. 2013.

GARZIK, Jeff. Gkernel, 2004. Disponível em: http://sourceforge.net/projects/gkernel/files/?source=navbar. Acesso em: 19 set. 2013.

GINGRAS, Jean Francois. Jaygeeplayground, 2009. Disponível em: https://jaygeeplayground.googlecode.com/svn-history/r4/trunk/prefetch/pref.pl. Acesso em: 18 set. 2013.

GRENIER, Christophe. Manned.org, 2006. Disponível em: http://manned.org/cmospwd/3930865c. Acesso em: 19 set. 2013.

GRENIER, Christophe. TestDisk, Data Recovery, 2011. Disponível em: http://www.cgsecurity.org/wiki/TestDisk/. Acesso em: 18 set. 2013.

HARBOUR, Nicholas. Fatback, 2005. Disponível em: http://sourceforge.net/projects/fatback/. Acesso em: 18 set. 2013.

HARVEY, Phil. Read, Write and Edit Meta Information! ExifTool by Phil Harvey, 2003. Disponível em: http://www.sno.phy.queensu.ca/~phil/exiftool/. Acesso em: 18 set. 2013.

Huebner, E., Bem, D., and Bem, O. (2007). Computer Forensics: Past, Present And Future. Information Security Technical Report, 8(2):32–36.

JASCONE, Fábio Luis Tavares. Protótipo de Software para Ocultar Texto Criptografado em Imagens Digitais. Blumenau, 2003. Trabalho de Conclusão de Curso – Ciências da Computação, Universidade Regional de Blumenau, p.33-40.

JENSEN,Jonas. Magicrescue, 2010. Disponível em: http://sourceforge.net/projects/fatback/. Acesso em: 18 set. 2013.

KENDALL, Kris. KORNBLUM, Jessie. Foremost, 2001. Disponível em: http://www.itu.dk/people/jobr/magicrescue/manpage.html#author. Acesso em: 18 set. 2013.

KESSLER, G. Anti-Forensics and the Digital Investigator. Disponível em http://scissec.scis.ecu.edu.au/conference_proceedings2007/forensics/01_Kessler_Anti-Forensics.pdf. Acesso em: 13 abr. 2013.

KORNBLUM, Jesse. Miss Identify - Latest version 1.0, 2008. Disponível em: http://missidentify.sourceforge.net/. Acesso em: 18 set. 2013.

KORNBLUM, Jessie. dc3dd, 2002. Disponível em: http://sourceforge.net/p/dc3dd/wiki/Home/. Acesso em: 18 set. 2013.

KORNBLUM, Jessie. dc3dd, 2008. Disponível em: http://sourceforge.net/projects/dc3dd/. Acesso em: 18 set. 2013.

KORNBLUM, Jessie. Dd, 2013. Disponível em: http://man7.org/linux/man-pages/man1/dd.1.html#COPYRIGHT. Acesso em: 18 set. 2013.

KORNBLUM, Jessie. md5deep and hashdeep - Latest version 4.3, 2003. Disponível em: http://www.itu.dk/people/jobr/magicrescue/manpage.html#author. Acesso em: 18 set. 2013.

LEHMANN, Marc. Fcrackzip, 1998. Disponível em: http://oldhome.schmorp.de/marc/fcrackzip.html. Acesso em: 19 set. 2013.

LIGHTFOOT, Chris. Driftnet, 2001. Disponível em: http://www.ex-parrot.com/~chris/driftnet/. Acesso em: 18 set. 2013.

LINS, Sérgio. Desafios sistêmicos: lições aprendidas por consultores e executivos que vivenciaram a implantação de sistemas. Rio de Janeiro: E-papers, 2009.

LOVISON, Henrique Dalla Costa, Uma metodologia de análise de Programas Daninhos. Trabalho de Conclusão de Curso, Porto Alegre, 2012. Universidade Federal do Rio Grande do Sul p. 13.

MASTWIJK, Kees. Ewfacquire(1) - Linux man page, 2006. Disponível em: http://sourceforge.net/p/dc3dd/wiki/Home/. Acesso em: 18 set. 2013.

MASTWIJK, Kees. Ewfacquire(1) - Linux man page, 2006. Disponível em: http://sourceforge.net/p/dc3dd/wiki/Home/. Acesso em: 18 set. 2013.

MELO, Sandro. Computação Forense com Software Livre: Conceitos, técnicas, ferramentas e estudos de casos. 1. ed. Rio de Janeiro: Alta Books. 2009.

MONTEIRO, Marcos. Perícia Computacional Forense: identificando o crime. Marcos Monteiro, [2007]. Disponível em: <http://www.marcosmonteiro.com.br/mm/palestras/Realizando_Pericia.pdf>. Acesso em: 15 abr. 2010.

MORAES, Paulo. Mente anti-hacker: proteja-se. Rio de Janeiro, Brasport, 2011.

NICOLAS DE, SOUZA. www.systemice.org.. Disponivel em: http://www.systemice.org/2009/09/principios-basicos-de-seguranca-da_09.html. Acesso em: 09 mar. 2013.

PAGANELLI, Celso Jefferson Messias. O Meio Digital como instrumento da prova. Dissertação(Pós-Graduação em Direito) – Centro Universitario “Euripedes Soares da Rocha”, mantenedora do Centro Universitário Eurípedes de Marília – UNIVEM.

Marília, 2012. Disponível em: http://aberto.univem.edu.br/bitstream/handle/11077/837/Disserta%C3%A7%C3%A3o_Celso%20Jefferson%20Messias%20Paganelli_2012.pdf?sequence=1. Acesso em: 12 maio 2013.

PEREIRA, E; FAGUNDES, L; NEUKAMP, P et al. Forense Computacional: fundamentos, tecnologias e desafios atuais. Em VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais..., p. 3-53, Rio de Janeiro, RJ, 2007.

PETERSON, Larry L.; DAVES, Bruce S. Redes de Computaores: uma bordagem de sistemas. Rio e Janeiro: Elservier, 2004

PROVOS, Niels. Steganography Detection with Stegdetect, 2004. Disponível em: http://www.outguess.org/detection.php. Acesso em: 18 set. 2013.

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

RABELO, Luiz. Cadeia de Custódia. Digital forensics blog // 4n6.cc, 2011. Disponível em: http://forensics.luizrabelo.com.br/2011/08/cadeia-de-custodia.html. Acesso em: 06 abr. de 2013.

REIS, M. A.; GEUS, P. L. Forense Computacional: Procedimentos e Padrões. 2001.

RICHARD III, Golden G. Scalpel, 2005. Disponível em: http://www.digitalforensicssolutions.com/Scalpel/. Acesso em: 18 set. 2013.

ROSANES, Pedro. Rootkits. Universidade Federal do Rio de Janeiro. Grupo de Resposta a Incidentes de Segurança. Rio de Janeiro, 2011. Disponível em: http://www.gris.dcc.ufrj.br/documentos/artigos/rootkits-survey. Acesso em: 25 maio 2013.

ROUKINE, Michel. Vinetto documentation page, 2006. Disponível em: http://vinetto.sourceforge.net/docs.html. Acesso em: 18 set. 2013.

SCHUSTER, Andreas. Windows Memory Forensics with Volatility, 2009. Disponível em: http://computer.forensikblog.de/files/talks/FIRST2009-Windows_Memory_Forensics_with_Volatility.pdf. Acesso em: 19 set. 2013. Scientific Working Groups on Digital Evidense and Imaging Technology. SWGDE and SWGIT Digital & Multimedia Evidence Glossary. 22 de maio de 2009, versão 2.3. Disponível em https://www.swgde.org/documents/swgde2009/SWGDE_SWGITGlossaryV2.3.pdf . In: MACEDO, Guilherme Matte. Investigação Digital de Rootkits em Sistemas Unix, p.20.

SÊMOLA, Marcos. Gestão da Segurança da Informação. Rio de Janeiro: Elsevier, 2003.

SILVA, Mário Bezerra da. Cadeia de Custódia. Disponível em: http://www.viajus.com.br/viajus.php?pagina=artigos&id=3153. Acesso em: 09 abril 2013.

SOARES, Felipe dos Santos. FIRME, Milene Nogueira Ferreira. Melhores práticas para coletar dados para uma perícia computacional usando Software livre. *Revista Eduf@tima, Vol. 3, No 1 (2012)*. Disponível em: http://www.edufatima.inf.br/isf/index.php/es/article/viewFile/96/36. Acesso em: 10 maio de 2013.

STEVENS, Didier PDFiD, 2009. Disponível em: http://blog.didierstevens.com/2009/03/31/pdfid/. Acesso em: 19 set. 2013.

STEVENS, Didier. Pdf-parser, 2009. Disponível em: http://blog.didierstevens.com/2009/03/31/pdfid/. Acesso em: 19 set. 2013.

TARDIEU, Samuel. How recoverjpeg saved my day, 2004. Disponível em: http://www.rfc1149.net/blog/2004/12/29/how_recoverjpeg_saved_my_day/. Acesso em: 18 set. 2013.

TOMASZEWSKI, Adauto de Almeida. Direito civil, notarial e registral. Curitiba, Camões,2008.

VACCA, John R. “Computer forensics: computer crime cene investigation”. 2. ed. Boston: Charles River Media, 2005.

VALTER, Stef. Scrounge-ntfs, 2010. Disponível em: http://thewalter.net/stef/software/scrounge/. Acesso em: 18 set. 2013.

ZALEWSKI, Michal p0f v3 (version 3.06b), 2012. Disponível em: http://lcamtuf.coredump.cx/p0f3/. Acesso em: 18 set. 2013.

ZAWINSKI, Jamie. Jwzhacks, 2004. Disponível em: http://www.jwz.org/hacks/mork.pl. Acesso em: 18 set. 2013.

ZHANG, Y. Definitions and Sciences of information. Information Processing & Management, 1988.

# ESTUDO COMPARATIVO ENTRE SOFTWARES LIVRES PARA PERÍCIA FORENSE BASEADOS EM LINUX

Instituto de Informática – Universidade Do Sagrado Coração (USC) Bauru – SP

Centro de Ciências Exatas e Sociais Aplicadas– Universidade do Sagrado Coração, USC.

{eder.lourenco@usc.br, henrique.martins@usc.br,egsilva@usc.br, patrick.silva@usc.br}

***Abstract.*** *Information is one of the most important assets today, for Both Individuals and companies paras and security of these data is vital. Currently there are several techniques used these data theft. This causes more and more computing professionals are needed to Ensure this security. The forensic computing is an area of computing focused on acquisition, preservation and documentation of evidence from digital storage devices electronics. This paper Analyzed que tools can be used to assist the expert in the collection and analysis of digital evidence.*

**Resumo.** *A informação é um dos bens mais importantes atualmente, tanto para empresas quanto paras pessoas e a segurança da informação destes dados é vital. Atualmente existem diversas técnicas usadas roubo destes dados. Isso faz com que cada vez mais profissionais da área de computação sejam necessários para garantir esta segurança. A perícia forense computacional é uma área da computação voltada para a obtensão, preservação e documentação de evidências a partir de dispositivos de armazenage m eletrônica digital. Neste trabalho são analisadas ferramentas que podem ser utilizadas para auxiliar o perito na coleta e análise de evidências digitais.*

## 1 Introdução

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação. Confidencialidade, Integridade e Disponibilidade representam atualmente, os principais atributos que orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Por isso é cada vez mais necessário para profissionais da área de computação sejam organizações públicas e privadas o domínio de técnicas de análise forense, aplicadas no âmbito computacional. A análise forense computacional consiste em um conjunto de técnicas para coleta e exame de evidências digitais, reconstrução de dados e ataques, identificação e rastreamento de invasores. Hoje em dia há diversos softwares livres baseados em Linux disponíveis para pericia e com diversas ferramentas disponíveis para análise forense computacional. Entre elas podemos citar o BackTrack 5 R3, CAINE 4.0 Pulsar e o FDTK 3.0 e que serão descritas neste trabalho.

## 2 Informação

Segundo o Aurélio (1995), informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza. A informação tornou-se uma necessidade crescente para qualquer setor da atividade humana e é indispensável mesmo que a sua procura não seja ordenada ou sistemática, mas resultante apenas de decisões casuísticas ou intuitivas.

## 3 Segurança da Informação

Sêmola (2003) define Segurança da Informação como "Uma Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou de sua indisponibilidade". De acordo com a norma ABNT NBR ISO/IEC 27002, 2005, alguns princípios básicos devem ser respeitados para que se possa garantir a segurança da informação:

- **Confidencialidade:** significa que a informação deve ser protegida contra sua divulgação para pessoas não autorizadas – interna ou externamente. Assegurar que a informação só pode ser acessada por pessoas autorizadas;
- **Integridade:** consiste em garantir que a informação gerada não será modificada sem a devida autorização da(s) pessoa(s) responsáveis por ela. Com isso garante que a informação efetivamente foi criada ou manipulada por quem reivindica sua autoria como, por exemplo, uso de uma senha de acesso.
- **Autenticidade:** o controle de autenticidade está ligado ao fato da informação que esteja sendo trafegada seja de fato originada do proprietário a ela relacionado. Não deve ser permitida a violação da origem da informação.
- **Disponibilidade:** Consiste em garantir que a informação esteja disponível às pessoas autorizadas sem nenhum tipo de modificação e sempre que elas necessitarem.

## 4 Pericia Forense Aplicada A Informática

A Computação Forense faz parte de um processo investigativo, que tem com objetivo provar os fatos ocorridos com a maior clareza possível. Para que isso ocorra o perito que for nomeado para realizar a perícia deve trabalhar de uma forma sistemática e cuidadosa com as evidências com o intuito de sempre preservar a integridade dos dados e detalhar toda a atividade executada no laudo final. Todo esse processo pericial na forense computacional é divido em quatro etapas conforme a seguir (FREITAS, 2006):

• **Coleta de dados**: É considerada a etapa mais importante de todo o processo, ou seja, a que mais precisa de cuidados. É nessa etapa que os dados serão coletados, sendo necessário cuidado especial para manter a integridade das informações. Outras atividades que são realizadas nesta etapa são relacionadas ao equipamento questionado, que deve ser identificado, devidamente embalado de uma forma segura, etiquetado as suas partes e suas identificações registradas no documento de cadeia de custódia;

• **Exame dos dados**: nesta segunda etapa o objetivo principal é separar as informações relevantes ao caso de outras sem importância, como os arquivos do próprio sistema. Nesta fase, deve-se identificar, extrair, filtrar e documentar os dados relevantes à apuração. Antes de iniciar o processo é preciso definir quais as ferramentas que serão utilizadas para o exame dos dados.

• **Análise das Informações**: nesta fase todas as informações anteriormente separadas serão analisadas com o intuito de encontrar dados úteis e relevantes que auxiliem na investigação do caso para que assim seja possível realizar a conclusão;

• **Interpretação dos resultados**: nesta última etapa, o objetivo é apresentar um laudo que deve informar com toda a veracidade possível o que foi encontrado nos dados analisados. Neste laudo deve-se também relatar todas as ferramentas e documentos utilizados.

De acordo com o descrito nas etapas anteriormente apresentadas, a Figura 1 demonstra de forma gráfica como é todo o processo de investigação em computação forense.

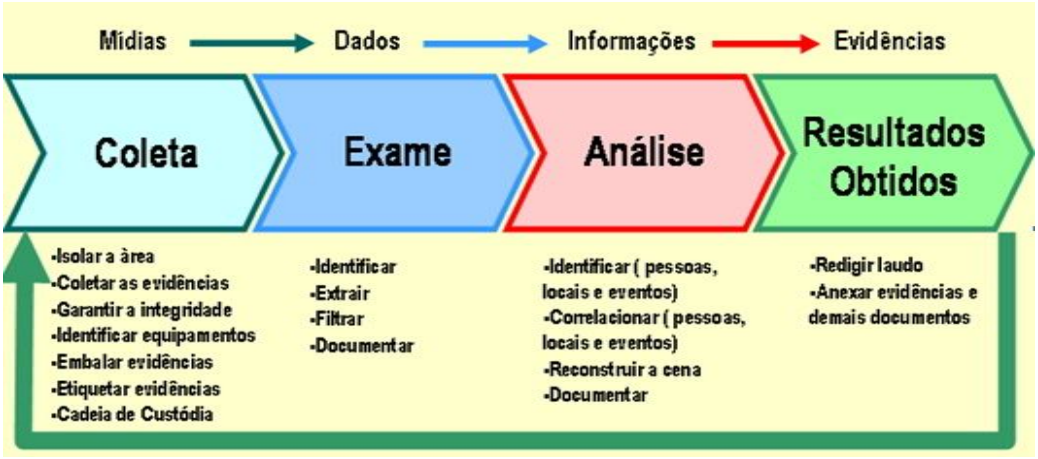



Figura 52 - Fases do processo de investigação
Fonte: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (2007).

## 5 Técnicas Forenses

Nessa Seção serão apresentados algumas técnicas forenses, utilizadas pelos peritos.

### 5.1 Dump De Memória

Cópia parcial ou completa da memória física do sistema. Consegue capturar informações como a memória de processos, senhas em texto puro e arquivos descriptografados temporariamente (MACEDO apud (SWGDE, 2007) e (SWGDE, 2008).

### 5.2 Funções de Hash

O HASH é uma função matemática que realiza o cálculo à partir de uma entrada de qualquer tamanho gerando em uma saída de tamanho fixo, pequena sequência de bits conhecida como valor do hash, de acordo com o algoritmo utilizado para o cálculo. (ELEUTÉRIO; MACHADO, 2011).

### 5.3 Mactimes

MACtimes referem-se a três atributos de tempo: mtime, atime e ctime, que são anexados a qualquer arquivo ou diretório no Linux, Windows e em outros sistemas de arquivo: **Mtime** (Modification time): mostra a última data e hora em que o arquivo foi modificado; **Atime** (Access time): mostra a última data e hora em que um diretório ou arquivo foi acessado/lido; **Ctime** (Creation time): mostra a data e hora em que arquivo foi criado.

### 5.4 Log de arquivo

De acordo com o CERT (2012), logs são o registro de atividade gerado por programas e serviços de um computador que podem ficar armazenados em arquivos, na memória do computador ou em bases de dados.

## 6 Técnicas Anti-Forenses

Nessa seção serão apresentadas técnicas anti-forenses.

### 6.1 Esteganografia

A esteganografia é o estudo ou técnica utilizada para esconder mensagens dentro de outras. Estegano, do grego steganós, significa oculto ou misterioso. Assim, esteganografia seria a “escrita escondida”.

Segundo Peterson (2004), criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias; proteger a integridade de transferências eletrônicas de fundos.

### 6.2 Códigos Maliciosos – Malwares

De acordo com o CERT (2012), códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

### 6.3 Tipos De Análise

Ao iniciar o procedimento de perícia em um equipamento questionado, o perito deve fazer a escolha de qual metodologia será empregada em seu trabalho: se a **Live Analysis** ou se a **Post Mortem Analysis**. A escolha da metodologia adequada vai depender do tipo de delito que será investigado. Por exemplo, em um suposto crime de pedofilia, onde arquivos de imagens gravados em disco são evidências, o perito fará uso da metodologia Post Mortem Forensics. Já para crimes de estelionato praticados por meios eletrônicos, poderão ser utilizadas as duas metodologias, a Post Mortem Forensics para a busca de dados que indiquem que o acusado tenha, por exemplo, invadido o sistema de uma empresa, e a Live Forensics para averiguar conexões estabelecidas no instante da investigação.

## 7 Metodologia

Como proposta para o presente estudo, inicialmente foi realizada uma pesquisa bibliográfica que segundo Domingues; Heubel; Abel (2003) as pesquisas devem conter assuntos gerais e particulares podendo ser localizadas em diversas fontes de pesquisas como

periódicos livros e materiais digitais nos quais tende a ter a facilidade em encontrar assuntos sobre softwares livres utilizados em pericia forense. Para consulta das funcionalidades foram utilizados diversos meios tais como, manual de usuário, forum de discussão e tutoriais disponíveis na internet entre outros.

Após o término da pesquisa o próximo passo foi instalar um sistema uma máquina virtual VMPlayer 6.0 onde foram instalados os softwares de pericia forense. Para esse trabalho utilizamos os softwares livres Backtrack 5 R3, FDTK V-3.0 e CAINE 4.0, todos compatíveis com o Linux Ubuntu. A lista de softwares a serem avaliados foi baseada em buscas feitas em sites voltados aos softwares livres. Além disso, autores e revistas digitais especializadas também foram consultados.

Depois de instalados e corretamente configurados, o próximo passo foi testar e descrever as funcionalidades que cada software possui e suas aplicações em testes de pericia computacional com o objetivo de determinar as principais características de cada software utilizado. Para maior compreensão essas características de softwares foram divididas em tópicos com o objetivo de facilitar o trabalho do perito em Forense Computacional.

Após os testes realizados nos softwares, será feito um quadro comparativo, destacando as principais características de cada um deles, como por exemplo, manuais e tutorias disponíveis, configuração mínima exigida, entre outras características que ainda serão analisadas e verificadas. Ao término dessa pesquisa espera-se proporcionar maiores detalhes de informações dos softwares analisados, permitindo aos peritos forenses maior facilidade de escolha quanto ao software com o qual ele deseja utilizar.

## 8 Quadro comparativo com as ferramentas disponíveis em cada distribuição analisada

| Quadro Comparativo das distribuições de Live CD de Pericia Forense Analisados | | | |
|---|---|---|---|
| Ferramentas Disponíveis | | | |
| | FDTK 3.0 | Backtrack 5 | C.A.IN.E. 4.0 |
| Criação de Imagens de Dados | aimage, air, btktool, dc3dd, dc3dd GUI, dd, ddrescue, dd_rescue, mondoarchive, mondorestore rdd, rddi, sdd | air, dc3dd, ddrescue, ewfacquire | Guymager,air |
| Captura tela | Take-Screenshot | | |
| Análise de memoria RAM | Memdump | pdfbook, pdgmail, volafox, volatility | |
| Geração de Hash | md5sum, sha1sum | hashdeep, md5deep, sha1deep, sha256deep, tigerdeep, whirlpooldeep | Quickhash |
| Identificação de Hardware | Discover, Gráfic-lshw, Hardinfo, Sysinfo, Xsysinfo | Bulk-extractor | |
| Limpar midias | Wipe | | |
| AFFTools | Afcat, afcompare, afconvert, afinfo, afstats, afxml | | |
| Antivírus e Malware | Clamav, Nephentes | | |
| Arquivos Compactados | Cabextract, orange, p7zip, unace, unrar-free, unshield, Xarchiver, zoo | | |
| Arquivos de Imagem | Dcraw, exif, exifautotran, exifprobe, exiftags,exiftran exiv2, jhead, jpeginfo | Exiftool | |
| Visualizar Imagens | commix, F-Spot Photo Manager, gthumb, imageindex | | |
| Análise de Arquivos Microsoft | Antiword, Dumpter, fccu-docprop, mdb-hexdump, readpst, regLookup, reglookup-recover, reglookup-timeline, regp, tnef, ntfscat, ntfsclone, ntfsinfo, ntfslabel, eindeutig, fccu-evtreader, galleta, Ggrokervtg-builddb, Grokevt, grokevt-aadlog, grokevt-findlogs, grokevt- | readpst, evtparse.pl, misidentify, pref.pl, reglookup | |

| | | | |
|---|---|---|---|
| | parselog, grokevt-ripdll, pasco, rifiuti | | |
| Quebra de Senha | fcrackzip, john the Ripper, medussa, ophcrack | Cmospwd, fcrackzip, samdump | |
| RootKits | chkrootkit, Rkhunter | chkrootkit, Rkhunter | |
| Cripto-Stegano | Bcrypt, ccrypt, Gdecrypt, Outguess, stegcompare, stegdeimage, stegdetect, xsteg | TrueCrypt, stegdetect, | Xsteg |
| Editor Hexa | Bless, ghex2, hexdump | Hexedit | gtkhash, hexeditor |
| Restaurar dados | E2undel, , Foremost, gzrecover, MagicRescue, recover, recoverjpeg, scrounge-ntfs | Extundelete, fatback, foremost, magicrescue, recoverjpeg, safecopy, scalpel, scrounge-ntfs, testdisk | Photorec, testdisk, |
| Linha do Tempo – Mactimes | mac-robber, mactime | | |
| Localizar dados | Blkcalc, blkcat, blkid, blkstat, glark, gnome-search-tool, Meld Diff Viewer, slocate | | |
| Arquivos Pdf | | Pdfid, pdf-parser, peeddf | |
| Coleção de scripts para análise forense | | | Bash scripts tools, bash scripts tools, idevice tools |
| Rede e Internet | Traceroute, mork, cookie_cruncher | Darkstat, driftnet, p0f, tcpflow, tcpreplay,wireshark, xplico, xplico web gui, mork, ptk | netdiscover, network, networktools, sharedfolders, warishark, zenmap |
| ToolKits | autopsy, ptk, | Autopsy, dff cli, dff ui, ptk, sleuthkit | Autopsy, Mobius |
| Forense para dispositivos móveis | | | IphoneBackupAnalyzer, BlackberryToll, IDevicetools |
| Total de Ferramentas Forenses disponíveis nesta versão | 115 | 57 | 21 |

Figura 2 – Quadro comparativo das Ferramentas testadas.

## 9 Conclusão

Através do estudo realizado pode-se verificar a existência de ferramentas que facilitam e otimizam as tarefas executadas pelos profissionais de Forense Computacional. Neste caso foram testadas três distribuições baseadas no sistema operacional Linux Ubuntu: Backtrack, FDTK e C.A.IN.E. Houve uma grande dificuldade para a elaboração deste trabalho devido à escassez de literatura e materiais pertinentes a este assunto, principalmente na língua portuguesa. A falta de material deve-se a ser uma área recente.

As ferramentas apresentadas possuem diversas ferramentas que podem auxiliar o perito a descobrir informações que podem levar a solução do caso analisado. Dentre as 3 distribuições, a distribuição Backtrack apesar de não possuir a maior quantidade de ferramentas disponíveis especificamente para análise forense, é aquela que possui a maior quantidade de informações sobre as ferramentas contidas na distribuição permitindo ao usuário utilizar essas ferramentas em situação de investigação forense. Já distribuição FDTK apesar de possuir diversas ferramentas, ainda precisa de maior documentação das funcionalidades delas, bem como correções na funcionalidade das ferramentas contidas na distribuição. O mesmo ocorre com a distribuição Linux C.A.IN.E. que, mesmo com o objetivo de se priorizar o uso interfaces gráficas, possui pouca documentação além de ter a menor quantidade de ferramentas disponíveis em relação as outras ferramentas analisadas o que dificulta o aprendizado e sua utilização. Por fim algumas das ferramentas contidas nestas distribuições foram testadas visando mostrar aplicações das técnicas na análise forense computacional.

Através deste estudo pode-se constatar que a computação forense tem muito que desenvolver e inovar. É necessário muito aperfeiçoamento no que se refere a métodos e tecnologias na obtenção das evidencias necessárias para a solução dos crimes de informática. Apesar de ser uma área recente, já existe muita demanda de profissionais capacitados, que realmente são conhecedores dos procedimentos seguidos pela área cientifica forense. Nesta era, em que estamos conectados em todos os lugares, os problemas e incidentes tendem a aumentar, o mercado de segurança da informação é promissor. Também há necessidade de se atualizar as leis brasileiras para que os crimes de informática possam ser atendidos de uma forma melhor juridicamente falando. A computação forense tem o que contribuir para a sociedade no que se refere a garantia de direitos e deveres por parte dos cidadãos.

## 10 Referencias

ABRAHÃO, M. S. A *Segurança da Informação Digital na Saúde*. Sociedade Beneficente Israelita Brasileira, 2003. Disponível em http://www.einstein.br/biblioteca/artigos/131%20132.pdf. Acesso em: 08 nov. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2005.

BackTrack 5 R3. Disponível em: http://www.backtrack-linux.org/backtrack/backtrack-5-r3-released/. Acesso em: 01 nov 2013.

CAINE 4.0 – Pulsar. Disponível em: http://www.caine-live.net/. Acesso em: 01 nov. 2013.

CERT ADVISORY. **Cartilha de Segurança para Internet.** Disponível em: <http://cartilha.cert.br/malware/sec7.html>. Acesso em: 12 nov. 2012.

ELEUTÉRIO, P.; Machado, M. Desvendando a Computação Forense. Novatec. Brasil, 2011.

FDTK-UbuntuBr – Forense Digital ToolKit. Disponível em: www,fdtk.com.br. Acesso em: 01 nov. 2013

FERREIRA, Aurélio B. de Holanda. Mini Dicionário Aurélio da Língua Portuguesa. 8. ed. Curitiba: Editora Positivo, 2010.

FREITAS, A. R. de. Perícia Forense Aplicada a Informática: Ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

Scientific Working Groups on Digital Evidense and Imaging Technology. SWGDE and SWGIT Digital & Multimedia Evidence Glossary. 22 de maio de 2009, versão 2.3. Disponível em https://www.swgde.org/documents/swgde2009/SWGDE_SWGITGlossaryV2.3.pdf . In: MACEDO, Guilherme Matte. Investigação Digital de Rootkits em Sistemas Unix, p.20.

SÊMOLA, Marcos. Gestão da Segurança da Informação. Rio de Janeiro: Elsevier, 2003.

SILVA, Mário Bezerra da. Cadeia de Custódia. Disponível em: http://www.viajus.com.br/viajus.php?pagina=artigos&id=3153. Acesso em: 09 nov. de 2013.