**UNIVERSIDADE FEDERAL DE SANTA MARIA**
**COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA**
**CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES**

# PERÍCIA FORENSE COMPUTACIONAL: PROCEDIMENTOS, FERRAMENTAS DISPONÍVEIS E ESTUDO DE CASO

**TRABALHO DE CONCLUSÃO DE CURSO**

**PAULO FRANCISCO CRUZ DE SOUZA**

**Santa Maria, RS, Brasil**

**2015**

| | | | |
|---|---|---|---|
| CTISM/UFSM, RS | FRANCISCO CRUZ DE SOUZA, Paulo | Graduado | 2015 |

# Perícia Forense Computacional: procedimentos, ferramentas disponíveis e estudo de caso

**Paulo Francisco Cruz de Souza**

Trabalho apresentado ao Curso de Graduação em Tecnologia em Redes de Computadores, Área de concentração em Informática Forense e Segurança da Informação, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Tecnólogo em Redes de Computadores**

**Orientador: Prof. Me. Tiago Antônio Rizzetti**

**Santa Maria, RS, Brasil**

**2015**

**Universidade Federal de Santa Maria**
**Colégio Técnico Industrial de Santa Maria**
**Curso Superior de Tecnologia em Redes de Computadores**

A Comissão Examinadora, abaixo assinada,
aprova a Monografia

**PERÍCIA FORENSE COMPUTACIONAL: PROCEDIMENTOS, FERRAMENTAS DISPONÍVEIS E ESTUDO DE CASO**

elaborada por
**Paulo Francisco Cruz de Souza**

como requisito parcial para obtenção do grau de
**Tecnólogo em Redes de Computadores**

**COMISSÃO EXAMINADORA**

**Tiago Antônio Rizzetti, Me.**
(Presidente/Orientador)

**Renato Preigschadt de Azevedo, Me.** (UFSM)

**Simone Regina Ceolin, Dra.** (UFSM)

Santa Maria, 08 de junho de 2015

# RESUMO

Monografia
Universidade Federal de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores

## PERÍCIA FORENSE COMPUTACIONAL: PROCEDIMENTOS, FERRAMENTAS DISPONÍVEIS E ESTUDO DE CASO

AUTOR: PAULO FRANCISCO CRUZ DE SOUZA
ORIENTADOR: TIAGO ANTÔNIO RIZZETTI
Data e Local da Defesa: Santa Maria, 12 de junho de 2015

Na computação, os vestígios de um crime são digitais (em forma de *bits*), podendo ser encontrados em dispositivos de armazenamento ou trafegando em rede. Por sua natureza, esse tipo de vestígio talvez não possa ser coletado e examinado através de métodos tradicionais. Nesse sentido, são abordadas neste trabalho, as fases da perícia, os principais procedimentos, as técnicas e as ferramentas normalmente utilizadas em exames periciais forenses envolvendo vestígios digitais, como dados de dispositivos de armazenamento, por exemplo. São construídas tabelas comparativas contendo as técnicas e ferramentas discutidas em cada etapa da perícia forense. Ao final, é realizado um estudo de caso no qual é verificada a aplicabilidade prática dos conceitos e ferramentas apresentadas neste trabalho.

**Palavras-chave**: perícia forense computacional. Vestígios digitais. Processo forense. Procedimentos, técnicas e ferramentas forenses. Estudo de caso.

# ABSTRACT

Monography
Federal University of Santa Maria
Superior Course of Technology in Computer Networks

## COMPUTER FORENSICS: PROCEDURES, AVAILABLE TOOLS AND CASE STUDY

AUTHOR: PAULO FRANCISCO CRUZ DE SOUZA
ADVISER: TIAGO ANTÔNIO RIZZETTI
Defense Place and Date: Santa Maria, june 12th, de 2015

In computing, the traces of a crime are digital and can be found in storage devices or network. This kind of trace might not be collected and examined through traditional methods. This course conclusion work shows the stages of expertise, the main procedures, techniques and tools commonly used in forensic expert examinations involving digital traces as data storage devices, for example. Comparative tables showing the techniques and tools discussed at every stage of forensics are presented. Finally, a case study is conducted to verify the practical applicability of the concepts and tools presented in this work.

**Keywords:** computer forensics. Digital traces. Process forensics. Procedures, techniques and forensic tools. Case study.

# LISTA QUADROS

# LISTA DE ILUSTRAÇÕES

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| DNS | *Domain Name Server* |
| HD | *Hard Disk* |
| IP | *Internet Protocol* |
| LIBPCAP | *Packet Capture Library* |
| NFAT | *Network Forensics Analysis Tools* |
| PCAP | *Packet Capture* |
| RAM | *Random Access Memory* |
| TCP | *Transmission Control Protocol* |

# SUMÁRIO

# 1 INTRODUÇÃO

Após seu rápido desenvolvimento e popularização, os computadores e a internet tornaram-se mais presentes em diversas atividades desempenhadas pelo ser humano, inclusive em atividades ilegais ou criminosas.

Segundo Priberam (2015), “perícia” significa “exame técnico realizado por perito”; “forense” é a aplicação de conhecimentos científicos a questões criminais. Assim, a perícia forense computacional é uma fusão entre conhecimentos da área da informática e da área jurídica. Seu objetivo é coletar evidências digitais, analisar dados e apresentar provas perante um ambiente jurídico, visando sempre à elucidação de um fato.

“Crimes sempre deixam vestígios” é uma frase bastante dita popularmente (ELEUTÉRIO; MACHADO, 2011). No caso da informática, os vestígios deixados por um crime estão na forma digital (armazenados em um disco, por exemplo). Assim, a perícia forense computacional tem como questão principal a identificação e o processamento de tais vestígios, através de procedimentos, técnicas e ferramentas adequadas.

Segundo Eleutério e Machado (2011), exames forenses na área de informática podem ser realizados em dispositivos de armazenamento, em aparelhos de telefone celular, em sites da internet, entre outros. Galvão (2013) ressalta, no entanto, que na maior parte das vezes a perícia tem como objetivo a análise de dados armazenados em dispositivos de armazenamento (discos rígidos, CDs, DVDs, cartões de memória, etc.).

Tarefas envolvendo computadores e redes aumentam em ritmo acelerado. Ações ilícitas utilizando esses meios, também. Segundo o Centro de Estudos, Resposta e tratamento de Incidentes de Segurança no Brasil (CERT.br), o número de fraudes na internet cresceu 6.513% no país entre 2004 e 2009. Em 2013, foram 352.925 incidentes reportados ao CERT.br (CERT, 2014).

Dado o aumento dos incidentes e fraudes envolvendo meios computacionais, há a necessidade de técnicas investigativas para a apuração dessas atividades ilícitas. A perícia forense computacional busca a coleta e a análise de dados e informações, ou seja, de vestígios digitais deixados na ocorrência de uma atividade criminosa ou fraudulenta envolvendo meios computacionais (ERBACHER; CHRISTIANSEN; SUNDBERG, 2006).

## 1.1 Objetivos

### 1.1.1 Objetivo geral

Investigar a metodologia da Perícia Forense Computacional envolvendo dispositivos de armazenamento e dados interceptados.

### 1.1.2 Objetivos específicos

Verificar na bibliografia quais são os procedimentos e os aspectos a serem observados em uma perícia forense computacional envolvendo dispositivos de armazenamento e dados interceptados;

Apresentar comparativamente as principais técnicas e ferramentas disponíveis;

Elaborar um estudo de caso para verificar, em um cenário prático, a aplicabilidade dos procedimentos discutidos e das ferramentas disponíveis para exames periciais em dispositivos de armazenamento de dados voláteis e não voláteis;

## 1.2 Justificativa

A evolução da tecnologia acompanha desde sempre a evolução humana. No âmbito computacional não é diferente, seu ritmo de evolução é acentuado e aumenta cada vez mais. A busca é pelo desenvolvimento de novas tecnologias da informação, pela disseminação do acesso à internet, pela promoção de novas demandas e correspondência com novas ofertas tecnológicas.

O avanço da computação e da comunicação em rede proporciona comodidade às pessoas. A realização de uma tarefa escolar pode ser feita de forma online (através da internet). O estudo e formação em um curso pode ser EaD (Educação à Distância). A compra de um produto pode ser realizada pelo site (página web). Enfim, atividades que antes eram realizadas presencialmente, agora podem ser realizadas de qualquer lugar e a qualquer hora, inclusive crimes.

No caso de prática de crime, o Código de Processo Penal Brasileiro (BRASIL, 1941) determina que: quando a infração deixar vestígios, será indispensável o

exame de corpo de delito (artigo 158); o exame de corpo de delito e outras perícias serão realizados por perito oficial (artigo 159); os peritos elaborarão o laudo pericial, no qual descreverão o que examinarem e responderão aos quesitos formulados (artigo 160).

Na computação, os vestígios de um crime são digitais (em forma de *bits*), podendo ser encontrados em dispositivos de armazenamento ou trafegando em rede. De acordo com Eleutério e Machado (2011), na maioria dos casos, exames forenses nesses dispositivos resultam em uma excelente prova técnica e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença.

## 1.3 Estrutura do trabalho

Este trabalho de conclusão de curso está dividido em quatro capítulos: introdução, metodologia da perícia forense computacional, estudo de caso e conclusão.

No capítulo dois é apresentada a metodologia da perícia forense computacional: os procedimentos forenses, ou seja, as etapas de uma perícia forense computacional. Após isso, as três primeiras etapas serão detalhadas nos próximos subcapítulos. Ao final de cada subcapítulo, será apresentada uma tabela comparativa contendo as técnicas e ferramentas discutidas.

No capítulo três é realizado um estudo de caso. Através de um cenário hipotético, serão aplicados os procedimentos, as técnicas e as ferramentas discutidas neste trabalho.

No capítulo quatro é apresentado uma conclusão, relacionando o que foi possível compreender e contribuir com a realização deste trabalho.

# 2 METODOLOGIA DA PERÍCIA FORENSE COMPUTACIONAL

Neste capítulo, são apresentadas as principais etapas e aspectos a serem observados em uma perícia forense computacional envolvendo dispositivos de armazenamento ou tráfego de rede. Ao final de cada subcapítulo, é construído um quadro comparativo contendo as técnicas e ferramentas discutidas.

## 2.1 Trabalhos relacionados

Na literatura relacionada ao assunto, há uma diversidade de técnicas e ferramentas (em *hardware* e *software*) que são sugeridas e aplicadas em exames periciais na área da informática. Além disso, há modelos de processos forenses e questões a serem observadas durante a realização de uma perícia.

De acordo com Kent et al. (2006), a perícia forense não segue procedimentos rígidos bem definidos. Independente da área de aplicação (isto é, da natureza das evidências), é sugerido, no entanto, que o exame pericial forense seja segmentado em quatro etapas, de forma a torná-lo mais organizado e consistente (KENT et al., 2006).

Junior e Moreira (2014) propõem um roteiro básico de investigação pericial em redes. A proposta dos autores é formular um roteiro base, descrevendo os procedimentos a serem realizados em casos de intrusão ou invasão de redes. Junior e Moreira (2014) ressaltam que, por se tratar de um roteiro básico e objetivar a construção de uma linha mestra para a atuação da perícia, possíveis alterações e incrementos podem ser aplicados, de modo a adequar a perícia ao contexto da investigação.

Weyer (2011) apresenta um estudo sobre as ferramentas computacionais baseadas em *software* livre e as principais técnicas disponíveis para uma perícia forense computacional.

Segundo Eleutério e Machado (2011), os computadores podem ser utilizados como ferramenta de apoio ou como meio para a realização de crimes. A partir da experiência profissional dos autores, o uso de computadores como ferramenta de apoio à prática de crimes representa a maior parte dos casos investigados. Além disso, exames em dispositivos de armazenamento

computacional são os exames periciais mais solicitados na computação forense (ELEUTÉRIO; MACHADO, 2011).

Galvão (2013) adverte que, embora existam procedimentos padrões e sequências sugeridas semelhantes em perícias na área da informática, há algumas particularidades a serem observadas em cada tipo de perícia (em dispositivos de armazenamento ou em redes, por exemplo).

Nesse sentido, este trabalho apresentará os principais procedimentos, técnicas e ferramentas para uma perícia forense computacional.

## 2.2 Procedimentos forenses

A realização de uma perícia forense é justificada pela busca de uma melhor compreensão de um determinado evento, encontrando e analisando outros fatos e eventos relacionados ao objeto de análise. Para alcançar esse objetivo, Kent et al. (2006) sugere que a perícia siga um processo forense composto por quatro etapas: coleta, extração, análise e apresentação.

O processo sugerido pode ser utilizado para perícias forenses em diversas áreas científicas, inclusive em computação. A perícia forense computacional não segue procedimentos rígidos bem definidos (KENT et al., 2006). Assim, o processo pode ser seguido e ajustado para a realização de uma perícia adequada às características dos dispositivos de armazenamento computacional a serem apreendidos e periciados (JUNIOR; MOREIRA, 2014). A Figura 1 ilustra as etapas do processo forense (KENT et al., 2006) em um contexto computacional.

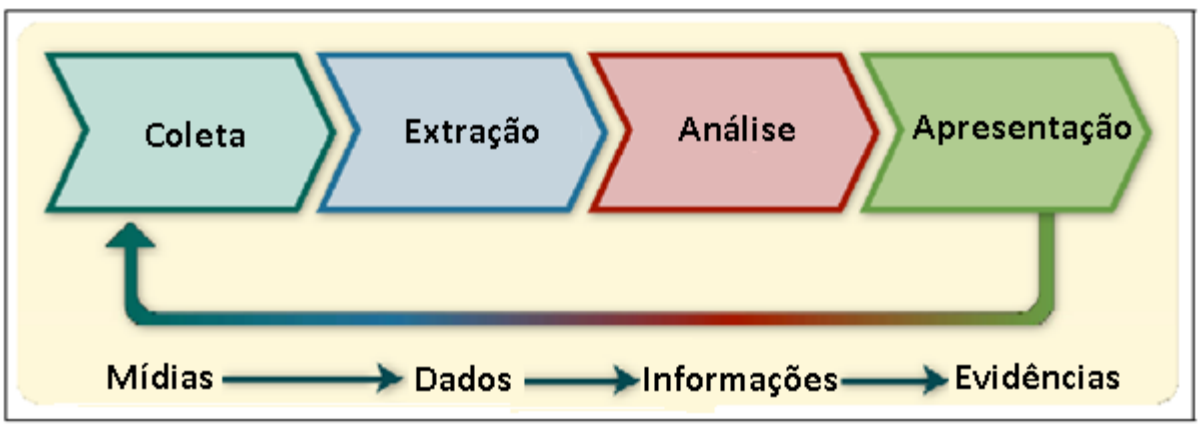


Figura 1 – Etapas do processo forense
Fonte: Adaptado de Kent et al. (2006).

### 2.1.1 Etapa de coleta

Nesta primeira etapa, é realizada a coleta de fontes que provavelmente contenham evidências digitais ou que possuam alguma relação com o evento investigado. É de fundamental importância que esta etapa ocorra de maneira rápida – se possível, logo após o conhecimento do incidente – e que siga procedimentos que preservem a integridade do material coletado. Para KENT et al. (2006), a etapa de coleta pode ser subdividida em identificação, aquisição, preservação e verificação de integridade.

Na identificação, há a necessidade de reconhecer quais materiais podem ser úteis para a perícia, ou seja, o que pode ser uma possível fonte de evidências digitais. Computadores pessoais, servidores, elementos de rede, câmeras digitais, celul*Ares*, dispositivos de armazenamento, entre outros, são dispositivos que podem conter informações digitais – documentos, fotos, vídeos, registros, entre outros – e, a princípio, são de fácil reconhecimento. Entretanto, com os avanços tecnológicos, novos dispositivos e possíveis fontes de informação surgem rapidamente demandando uma forte atualização por parte da perícia forense para que esses materiais sejam efetivamente identificados (KENT et al., 2006).

Eleutério e Machado (2011) ressaltam que os dispositivos de armazenamento mais comuns em exames forenses são os discos rígidos, CDs, DVDs, *pen drives,* cartões de memória, *Blu-Rays,* entre outros. A identificação deverá ocorrer de forma precisa, pois os dispositivos computacionais e de armazenamento só deverão ser apreendidos se houver desconfiança de que eles contenham evidências relevantes para a investigação. Ao contrário, serão apreendidos dispositivos e materiais irrelevantes para a perícia, que não possuem qualquer relação com o evento investigado, resultando em exames periciais demorados e desnecessários.

Depois de realizada a identificação dos dispositivos computacionais e de armazenamento úteis para a investigação, será realizada a aquisição – apreensão – desses materiais. Para isso, é de suma importância que as características de cada provável fonte de evidências digitais sejam observadas e que a apreensão seja balizada por procedimentos e técnicas que garantam a integridade dos dados e das informações (KENT et al., 2006).

Para Kent et al. (2006), os principais fatores que devem ser levados em conta no momento da aquisição de dispositivos computacionais são: volatilidade – dados e informações digitais podem ser perdidas devido à passagem do tempo, à interrupção do fornecimento de energia ou às ações realizadas no sistema; valor provável da fonte – com base em experiências anteriores e situações semelhantes, estimar a utilidade provável da fonte de dados para a investigação; quantidade de esforço necessário para aquisição da fonte – fontes de dados que demandam esforços de aquisição distintos, como registros de um roteador e de um provedor de acesso, podem fornecer evidências equivalentes.

Em relação ao grau de volatilidade das informações, Eleutério e Machado (2011) ressaltam que esse fator dependerá do dispositivo de armazenamento computacional. Os dispositivos mais comuns de serem apreendidos possuem as seguintes características: fragilidade, facilidade de cópia e sensibilidade ao tempo de vida e de uso. Com isso, a preservação desses dispositivos – garantia de que as informações armazenadas permaneçam inalteradas – é fundamental. Nesse sentido, será necessário realizar uma cópia fiel e segura dos dados digitais contidos no dispositivo original apreendido. Para isso, deverão ser utilizadas técnicas, equipamentos e *softwares* específicos que realizem não só uma cópia fidedigna, mas que também preservem e mantenham inalterada a fonte original dos dados.

Assim, considerando tais fatores – volatilidade, valor provável e esforço necessário –, além de preservar a integridade das potenciais fontes de dados, será possível aplicar uma priorização no momento da apreensão de forma a determinar quais fontes são mais relevantes para a investigação.

Depois de identificadas e adquiridas, é de suma importância que as fontes de dados (originais e cópias) sejam verificadas e preservadas. A verificação da integridade dos dados poderá ser feita através de funções matemáticas de comparação que determinarão a correspondência entre a fonte de evidências e a cópia realizada (JUNIOR; MOREIRA, 2014).

Segundo Eleutério e Machado, ao final da etapa de coleta, a equipe pericial terá em seu poder uma cópia integral e fidedigna das fontes de dados apreendidas. O material original deverá ser preservado. Para isso, o mesmo deverá ser lacrado e acondicionado em lugar apropriado. As próximas etapas do processo forense de investigação serão realizadas sobre as cópias realizadas.

### 2.1.2 Etapa de extração

Após coletadas as prováveis fontes de vestígios e realizadas as respectivas cópias seguras, a próxima etapa é recuperar toda a informação contida nas cópias e extrair dados úteis para a investigação. As cópias seguras – realizadas na etapa de coleta – são cópias integrais, ou seja, contêm todos os arquivos, dados e configurações do material original que foi apreendido. Assim, é natural que ao início da etapa de extração, exista uma grande quantidade de arquivos e dados – às vezes ocultos ou até corrompidos – para serem analisados pelo perito. Identificar e recuperar arquivos que possam conter informações relevantes para a investigação é o objetivo da etapa de extração.

Segundo Kent et al. (2006), um disco rígido pode conter milh*Ares* ou até milhões de arquivos de dados, sendo a maioria deles irrelevantes para a investigação – arquivos do sistema operacional e de aplicativos, isto é, programas diversos de computador. Além disso, podem existir mecanismos de controle de acesso, de compressão de dados e de criptografia dificultando o acesso às informações de interesse. Kent et al. (2006) ressalta ainda que arquivos de interesse podem conter informações desnecessárias. Um log de acesso de um *firewall*, por exemplo, pode conter milhões de registros, mas talvez somente alguns deles tenham relação com o fato investigado.

Levando-se em consideração a quantidade de arquivos irrelevantes, será necessário ao perito aplicar ferramentas e técnicas que o auxiliem a peneirar e identificar os dados que sejam pertinentes à investigação. Pode ser útil na etapa de extração a utilização de padrões de busca em textos, referenciando um nome ou assunto; filtragem por determinados tipos de arquivos, como texto ou vídeo; exclusão de arquivos irrelevantes, como arquivos do sistema operacional; procedimentos de recuperação de arquivos apagados e de indexação de dados (ELEUTÉRIO; MACHADO, 2011); entre outras ferramentas e técnicas auxili*Ares* à etapa de extração que serão apresentadas mais adiante.

### 2.1.3 Etapa de análise

Nesta etapa, serão analisados os dados e informações extraídas da etapa anterior. Para Eleutério e Machado (2011), a análise consiste em um exame realizado sobre as informações extraídas do material apreendido buscando a identificação de evidências digitais que possuam relação com o fato investigado.

Segundo Kent et al. (2006), a ciência forense usa uma base metódica para chegar a conclusões adequadas às informações disponíveis. Assim, dados e informações serão analisadas e estudadas objetivando algumas conclusões como a identificação de pessoas, locais e eventos, e a correlação entre esses elementos e o fato investigado. Contudo, na realização de exames envolvendo dispositivos de armazenamento, há diversos desafios a serem superados pela perícia como, por exemplo, a quantidade de arquivos. (ELEUTÉRIO; MACHADO, 2011).

Embora a etapa anterior – extração – tenha recuperado e identificado as informações mais relevantes de um determinado dispositivo de armazenamento, a quantidade de arquivos ainda é um fato a ser considerado. Em alguns casos, um dispositivo com capacidade de armazenamento de oitenta Gigabytes (80GB) – uma capacidade pequena se comparada a discos com mais de um *Terabyte* (1TB) existentes atualmente (ELEUTÉRIO; MACHADO, 2011) –, após ser peneirado pela etapa de extração de arquivos relevantes, ainda contém milh*Ares* de arquivos de dados. Analisar de forma manual, ou seja, examinar visualmente o conteúdo de cada arquivo em busca de vestígios, pode se tornar uma tarefa inviável para a perícia forense.

Durante a etapa de análise, é comum a existência de senhas, criptografia e esteganografia dificultando o exame pericial. Evidências importantes contidas em programas e arquivos podem estar protegidas por senha; uma informação útil para a investigação pode estar criptografada; através da esteganografia, uma mensagem incriminadora pode estar camuflada dentro de outra aparentemente irrelevante.

Para superar tais desafios, existem métodos forenses – procedimentos, técnicas e ferramentas – que podem auxiliar nesta etapa. A utilização de procedimentos básicos como a utilização de filtros de arquivos e pesquisas por palavras-chave, ou até suítes de ferramentas de exames forenses, viabiliza e torna mais eficiente a análise forense computacional. Os principais métodos que podem ser utilizados na análise forense serão mais bem explicados em um próximo tópico.

### 2.1.4 Etapa de apresentação

A apresentação (ou documentação) é a etapa final do processo forense. Nesta etapa, a tarefa da perícia é documentar as evidências digitais encontradas e apresentá-las às autoridades competentes. Constarão da documentação aspectos relativos às etapas anteriores como: método de coleta e extração, análise dos fatos e o valor técnico do conteúdo analisado (KENT et al., 2006).

Segundo Junior e Moreira (2014), a documentação – normalmente realizada através de um laudo técnico pericial – deve apresentar com precisão todas as ações realizadas e os resultados obtidos das etapas anteriores, uma vez que nesta etapa há a possibilidade de provar a ocorrência ou não de um fato inicialmente investigado. O laudo técnico pericial deve ser conciso; apresentar uma leitura adequada ao público não ligado à área da informática; descrever de forma objetiva e clara os métodos, ferramentas e exames realizados durante o processo forense.

Essa metodologia é fundamental para manter a segurança, a transparência e a validade de eventuais evidências digitais encontradas nos materiais examinados. Geralmente, os laudos periciais possuem a seguinte estrutura: preâmbulo, histórico, material, objetivo, considerações técnicas ou periciais, exames e respostas aos quesitos formulados ou conclusões (ELEUTÉRIO; MACHADO, 2011). Essa estrutura é apresentada e explicada de forma breve no Quadro 1.

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

Quadro 1 – Seções do laudo técnico pericial
Fonte: Adaptado de Eleutério e Machado (2011).

## 2.2 Principais aspectos, técnicas e ferramentas para coleta

Nesta seção são apresentadas as principais técnicas e ferramentas (*hardware* e *software*) utilizadas na etapa de coleta e preservação de uma perícia forense computacional. É de suma importância que os dados contidos nos materiais (mídias digitais e dispositivos de armazenamento) e os dados voláteis (presentes na memória RAM ou trafegando em rede), possíveis fontes de evidências digitais, sejam corretamente coletados e preservados, de modo a garantir sua inalterabilidade.

É da fase de coleta e preservação que será possível colher elementos (dados digitais, dispositivos e mídias de armazenamento, etc.) de modo a formar uma base investigativa para as demais fases da perícia.

### 2.2.1 Técnicas de espelhamento e de imagem

Em regra, os exames forenses devem ser realizados sobre cópias fiéis obtidas dos materiais questionados – material original apreendido e submetido a exames forenses. Para isso, deverão ser aplicadas técnicas e ferramentas que realizem uma duplicação fidedigna dos dados e preservem a integridade do material apreendido (ELEUTÉRIO; MACHADO, 2011).

Espelhamento e imagem são técnicas de duplicação utilizadas na etapa de coleta do processo forense. Segundo Eleutério e Machado (2011), os materiais coletados mais comuns são dispositivos de armazenamento – mídias ópticas, discos magnéticos e cartões de memória. A falta de cuidado no manuseio desses materiais pode acarretar alteração ou até a perda de informações. O espelhamento e a imagem, quando realizadas através de equipamentos e *softwares* forenses específicos, permitem uma duplicação fiel dos dados e a preservação do material apreendido.

O espelhamento é uma técnica de duplicação que realiza uma cópia exata e fiel dos dados contidos em um dispositivo de armazenamento computacional para outro (ELEUTÉRIO; MACHADO, 2011). O espelhamento possui algumas peculiaridades: exigência de um dispositivo de destino dedicado para um dispositivo de origem; o dispositivo de destino deve ter capacidade igual ou superior ao de

origem; o dispositivo de destino não pode possuir conteúdo, pois eventuais resquícios de dados podem ser confundidos na etapa de análise; a técnica de espelhamento realiza uma cópia bit-a-bit para o dispositivo de destino, logo eventuais setores defeituosos em dispositivos de destino podem acarretar a perda de dados.

A técnica de imagem, por sua vez, também realiza uma cópia fiel dos dados contidos em um dispositivo de armazenamento digital. Contudo, com os dados copiados, é gerada uma imagem de disco – arquivo único que contém toda a estrutura e conteúdo de um dispositivo de armazenamento de dados.

De acordo com Eleutério e Machado (2011), a técnica de imagem possui algumas vantagens se comparada com o espelhamento: um dispositivo de destino pode armazenar diversas imagens de disco, se houver capacidade; possibilidade de compactação dos arquivos de imagem; facilidade de replicação das imagens de disco, uma vez que podem ser copiadas por qualquer sistema operacional; eventuais setores defeituosos no dispositivo de destino são tratados pelo sistema operacional.

Devido às vantagens apresentadas, a técnica de imagem normalmente é a escolhida para a duplicação dos dados. Contudo, é importante que, independentemente da técnica utilizada, a duplicação seja realizada com a garantia de que as informações contidas no dispositivo a ser copiado mantenham-se inalteradas (ELEUTÉRIO; MACHADO, 2011). Para isso, alguns equipamentos e *softwares* forenses são apresentados na seção 2.2.2 – como bloqueadores de escrita, duplicadores, *softwares* e sistemas operacionais – que podem ser utilizados nesta etapa de coleta e preservação de dados.

### 2.2.2 Equipamentos para bloqueio de escrita e duplicação forense

De acordo com Eleutério e Machado (2011), existem diversos equipamentos em *hardware* que auxiliam na preservação dos dados durante a realização do espelhamento ou da imagem. Os principais são os bloqueadores de escrita e os duplicadores forenses.

Os bloqueadores de escrita, segundo Eleutério e Machado (2011), são dispositivos simples utilizados para garantir que, durante o processo de cópia ou de acesso, as informações e os dados digitais contidos no dispositivo de

armazenamento computacional permaneçam inalterados. Essa garantia é dada pelo hardware que, uma vez conectado entre o computador e o dispositivo questionado (dispositivo de origem), bloqueia operações de escrita no material a ser copiado, sem a necessidade software adicional.

Os dispositivos Espion Forensics FastBlock 3 FE (para discos), *Forensic Bridge Tableau* (para discos) e *ICS Write Protect Card Reader* (para cartões de memória) são exemplos de bloqueadores de escrita bastante utilizados em processos de duplicação forense (ELEUTÉRIO; MACHADO, 2011). A Figura 2 ilustra o uso de um equipamento dessa natureza.

Figura 2 – Bloqueador de escrita Forensic Bridge Tableau
Fonte: adaptado de QPERITO (2013)

Os duplicadores forenses são dispositivos mais avançados, pois além de realizarem o bloqueio de escrita, permitem a realização de cópias simultâneas e oferecem suporte a múltiplas interfaces de disco (conectores). Através da técnica de espelhamento ou de imagem, os duplicadores realizam cópias de um ou mais discos de origem diretamente para um ou mais discos de destino.

De acordo com Eleutério e Machado (2001), a utilização de duplicadores forenses no processo de duplicação de dados resulta em algumas vantagens, dentre elas: maior velocidade na cópia dos dados; suporte a uma diversidade de interfaces (conectores) de discos; dispensa do uso de computador para realizar a interface entre os discos questionados (discos de origem) e os discos de destino.

Os dispositivos *Intelligent Computer Solutions Solo III* e *Tableau TD2u* são exemplos de duplicadores forenses que podem ser utilizados no processo de duplicação forense.

A Figura 3 ilustra a organização física dos dispositivos de armazenamento em um processo de duplicação forense através do duplicador Tableau TD2u.

Figura 3 – Duplicação forense através do Tableau TD2u
Fonte: Adaptado de Techbiz (2015)

### 2.2.3 *Softwares* e sistemas operacionais para duplicação forense

A etapa de coleta de dados não exige necessariamente o uso de equipamentos de bloqueio de escrita ou de duplicação forense. Embora o uso desses equipamentos facilite o processo de cópia de discos, por exemplo, Eleutério e Machado (2011) defendem a possibilidade do uso de alguns *softwares* específicos ou de sistemas operacionais que não acessem o dispositivo de armazenamento questionado (dispositivo a ser duplicado).

O *software Symantec Norton Ghost* é uma alternativa ao uso de bloqueadores ou de duplicadores forenses. Através desse programa, é possível realizar uma cópia dos dados contidos em um disco, seja pela técnica de espelhamento, seja pela técnica de imagem. O processo é simples: após conectar o disco questionado e o disco de destino ao computador, a inicialização deve ser feita via mídia de armazenamento contendo o *Symantec Norton Ghost*. Inicializado o computador, o programa disponibiliza as opções de duplicação, espelhamento ou imagem, e requisita a indicação do disco a ser copiado (origem) e do disco a receber a cópia (destino). Eleutério e Machado (2011) advertem sobre a possibilidade de erro na operação de indicação de disco de origem e de destino, pois haverá perda

de evidências caso ocorra inversão dos discos, visto que o disco questionado sofrerá alteração.

Segundo Eleutério e Machado (2011), o *Forensic ToolKit* (*FTK*) e o *Encase* são soluções comerciais compatíveis com o sistema operacional *Windows*. Ambas reúnem um conjunto de funcionalidades que permitem a realização das principais técnicas para perícia forense computacional. Além disso, essas suítes de aplicativos disponibilizam recursos que podem ser utilizados em todas as etapas da perícia, inclusive na etapa de coleta (seja na coleta ou na preservação dos dados). Outras funcionalidades dessas suítes serão apresentadas nas próximas etapas.

De acordo com Silva e Oliveira (2014), as distribuições baseadas no sistema operacional *Linux CAINE* e *FDTK-UbuntuBr* possuem diversas ferramentas que auxiliam os peritos nas diversas etapas da investigação forense. Após analisar a eficiência das ferramentas presentes nessas distribuições, Silva e Oliveira (2014) destacam a utilidade de algumas para a etapa de coleta e preservação: *DC3DD* e *Guymager*, ambas do sistema *CAINE*.

A distribuição livre baseada no GNU/*Linux* chamada de *CAINE* – acrônimo de *Computer Aided Investigative Environment*, ou então, “ambiente investigativo auxiliado por computador” (*CAINE*, 2015, tradução nossa) – foi criada com foco na área de forense digital e oferece um ambiente completo para a realização de atividades periciais. Essa distribuição integra diversos *softwares* e ferramentas para a perícia forense digital. Os principais objetivos que essa distribuição se propõe a prover são: um ambiente que suporte as quatro fases da investigação digital; interface gráfica e ferramentas de uso amigável (*CAINE*, 2015).

A ferramenta *DC3DD* é uma versão baseada no aplicativo *duplicate disk* (*dd*), possui novas funcionalidades e está presente na distribuição *CAINE*. O principal recurso dessa ferramenta é a criação de imagens forenses (cópias integrais, ou seja, bit-a-bit) de um dispositivo de armazenamento. Silva e Oliveira (2014) ressaltam que o dispositivo ou a mídia de armazenamento de destino (que receberá a imagem do dispositivo questionado) deve, previamente, passar por um processo de sanitização, isto é, uma formatação completa sem recuperação de dados. Para isso, a ferramenta *DC3DD* possui o recurso de *wipe* que, além de realizar uma formatação completa do dispositivo, apresenta o percentual real do processo. Funcionalidades como a quebra de imagens e a geração de logs de erros também estão presentes nessa ferramenta (SILVA; OLIVEIRA, 2014).

Segundo Silva e Oliveira (2014), a ferramenta *Guymager* do sistema *CAINE* é uma opção válida para a criação de imagens forenses. Além de realizar uma cópia integral dos dados e de possuir uma interface gráfica amigável (onde é possível verificar e acrescentar uma série de informações relativas aos dispositivos de armazenamento, como número de série e observações), essa ferramenta oferece cálculo de *hash* (sequência de bits, calculada através de uma função, que resume de forma unidirecional um arquivo ou uma informação) – importante técnica para preservação, isto é, para verificação de inalterabilidade da mídia ou do dispositivo de armazenamento duplicado. Embora existam diversos *softwares* e algoritmos para cálculo de *hash*, a ferramenta *Guymager* oferece essa comparação e validação de integridade dos dados de forma nativa, através de uma opção de *hash* (MD5 ou SHA – algoritmos de *hash*). Assim, o *Guymager* do sistema *CAINE* é uma ferramenta válida para o processo de duplicação forense.

As distribuições baseadas em *Linux* voltadas para a computação forense, como o Knoppix e o Helix, representam outra opção para a duplicação de discos. No caso do Helix, é possível utilizá-lo como uma ferramenta instalável em sistemas operacionais como *MAC OS X*, *Windows* e *Linux*. Ambas contêm a ferramenta *dd* (*duplicate disc*) e dispensam o uso de bloqueadores de escrita ou de duplicadores forenses, pois o acesso aos discos ocorre de forma somente leitura.

Com a ferramenta *dd* é possível criar a imagem ou o espelho do disco questionado. O processo de duplicação ocorre da seguinte forma: após conectar os discos de origem e de destino ao computador, a inicialização é feita através da mídia que contenha o sistema operacional forense; depois, a ferramenta *dd* é utilizada (através do comando *dd if=<origem> of=<destino>*) para criar a imagem ou o espelho do disco de origem (questionado) para o disco de destino. O processo de duplicação é simples, mas Eleutério e Machado (2011) ressaltam a importância da escolha correta dos discos de origem e de destino, visto que a escolha incorreta ou invertida, acarretará a alteração do disco questionado e a perda de evidências digitais.

Equipamentos como bloqueadores de escrita ou duplicadores forenses não são obrigatórios no momento da duplicação de discos. Conforme apresentado, o uso de *softwares* específicos ou de sistemas operacionais forenses no processo de duplicação também permite a criação de cópias integrais dos discos. No entanto,

havendo a possibilidade do uso desses equipamentos, o processo de duplicação se torna mais simples e seguro.

A utilização de um bloqueador de escrita, por exemplo, permite o uso de programas e sistemas operacionais com interface gráfica mais amigável. Nesse sentido, *softwares* como o Symantec Norton Ghost, *DC3DD*, *dd* e *Guymager* se tornam uma opção mais segura para o processo de duplicação quando utilizados em conjunto com um bloqueador de escrita..

Além disso, Eleutério e Machado (2011) destacam que, embora a seleção de disco de origem e de destino no processo de duplicação seja uma etapa crítica, eventuais enganos não resultariam perda de dados digitais, visto que o disco questionado estaria protegido pelo *hardware* (bloqueador de escrita) utilizado.

### 2.2.4 Ferramentas para coleta de dados voláteis

A etapa de coleta de evidências em estado digital para a realização de uma perícia forense computacional divide-se em dois tipos, diretamente relacionados à volatilidade dos dados: coleta *post-mortem* – realizada sobre diversos tipos de fontes de dados que contenham informações não voláteis, ou seja, que independam de fornecimento de energia para que mantenham os dados e as informações digitais – e coleta *live* (em tempo real) – realizada sobre fontes que contenham informações voláteis (armazenadas temporariamente), ou seja, que dependam do fornecimento de energia para a manutenção e a existência dos dados e informações digitais (LILLARD et al., 2010).

As principais técnicas e ferramentas para a realização de uma coleta p*ost-mortem* já foram apresentadas. Dispositivos e mídias de armazenamento secundário – discos rígidos, CDs, DVDs, cartões de memória – eram as principais fontes de dados não voláteis. De acordo com Galvão (2013), a grande maioria das atividades periciais forenses na área computacional tem como objetivo principal a coleta de evidências digitais nessas fontes.

Nesse sentido, ainda que as atividades do tipo p*ost-mortem* representem a maior parte das ações periciais, existem casos em que a coleta do tipo *live* (em tempo real) é imprescindível de ser realizada. Situações em que existam evidências digitais armazenadas na memória principal do sistema computacional, *Random Access Memory* (RAM), ou indícios de atos ilícitos trafegando em uma rede de

computadores justificam a necessidade de uma coleta do tipo *live,* ou seja, sobre dados voláteis.

A memória principal do sistema computacional é um dispositivo de armazenamento primário que contém, dentre outras informações, os processos em execução, as conexões de rede, os arquivos abertos e os dados que estão sendo manipulados, mas que ainda não foram salvos no disco ou em outra memória secundária (WEYER, 2011). A aplicação de uma abordagem correta, que preserve e capture o estado atual dessa memória volátil, é necessária nos casos em que esse dispositivo contenha informações relevantes para a perícia.

O primeiro aspecto a ser observado para a geração de uma cópia do conteúdo da memória RAM é que o eventual desligamento ou até mesmo o manuseio incorreto do sistema computacional investigado ocasionará a perda dessas informações. Embora esse aspecto pareça óbvio, Galvão (2013) adverte para os casos em que exista a necessidade de apreensão de dispositivos ou coleta de dados em locais de alta periculosidade. Nessas situações, de acordo com Galvão (2013), é indicado que seja realizado um treinamento para que outros profissionais, que não possuam conhecimentos avançados na área de informática, realizem a coleta e a preservação, a fim de evitar a exposição desnecessária do perito.

Após observar esse primeiro aspecto, será possível, com o uso de ferramentas adequadas, gerar uma cópia integral do conteúdo da memória RAM do sistema. Essa cópia também é conhecida como *dump* de memória e é semelhante à técnica de imagem de discos apresentada anteriormente. O *dump* de memória, segundo Weyer (2011), é um arquivo criado para receber todo o conteúdo da memória do sistema. Para auxiliar na geração desse arquivo, existem algumas ferramentas específicas como: *dd* (para ambiente *Linux*) e m*dd* (para ambiente *Windows*).

A ferramenta conhecida como *dd* permite a criação de uma cópia integral dos dados contidos em um disco. No entanto, é possível, por meio de opções existentes nesse utilitário baseado em *software,* gerar imagens (cópias integrais) de diversos tipos de dispositivos de armazenamento. Através do comando *dd if=/dev/fmem of=*<*arquivo-dump-destino*>, os dados presentes na memória principal podem ser copiados para um arquivo de destino, ou seja, pode ser gerada uma imagem (*dump*) do conteúdo da memória RAM. No caso da ferramenta m*dd*, o

mesmo processo de geração de imagem é realizado através do comando *mdd.exe -o arquivo-dump-destino* (JUNIOR et al., 2009). A Figura 4 ilustra a realização de um *dump* de uma memória de 512MB.

```
root@desktop-VirtualBox:/# dd if=/dev/fmem of=/home/memoria.dump bs=1M
 count=512
512+0 registros de entrada
512+0 registros de saída
536870912 bytes (537 MB) copiados, 31,0341 s, 17,3 MB/s
root@desktop-VirtualBox:/#
```

Figura 4 – Exemplo de *dump* de memória
Fonte: do Autor.

A coleta do tipo *live* caracteriza-se por ser aplicada sobre dados altamente voláteis. Na memória principal do sistema computacional, os dados e informações (possíveis evidências digitais) permanecem temporariamente, enquanto houver energia ou utilidade. Em redes de computadores, esses mesmos dados e informações apenas trafegam de um ponto de origem para um ponto de destino. Essa característica resulta em um maior índice de volatilidade e, consequentemente, um menor tempo hábil para a realização de uma coleta.

De acordo com Junior e Moreira (2014), a coleta *live* realizada em redes de computadores normalmente ocorre através da captura dos dados que trafegam pela entrada ou pela saída de tráfego entre computadores e redes distintas. Cabe ressaltar que a captura é apenas a primeira etapa de uma perícia forense envolvendo dados trafegados em rede, a qual é composta pelas seguintes etapas: captura de tráfego (coleta), extração, análise e apresentação. Nesse sentido, Singh (2009) discorre sobre as principais funções das ferramentas utilizadas na perícia forense de redes, também conhecidas como *Network Forensic Analysis Tools* (NFAT) – Ferramentas para Análise Forense em Redes, em tradução livre.

As funções básicas das NFAT, de acordo com Singh (2015), são: captura de tráfego ou *traffic sniffing*, análise do tráfego capturado e interação entre o profissional que fará a análise e a ferramenta. Tais ferramentas podem abarcar outras funções úteis para a perícia em redes. Assim, uma mesma ferramenta pode ser utilizada nas diversas etapas e atividades periciais.

Segundo Galvão (2013), o agente principal envolvido em uma atividade de captura de dados é o *sniffer* – ferramenta que envolve componentes de *hardware* e *software* para realizar a captura de tráfego em uma rede de computadores. A captura de tráfego consiste em inspecionar ou capturar, através de *softwares* específicos (*sniffers*), os dados trafegados em uma rede de computadores (CERT, 2015). Os dados são capturados na forma como trafegam. Com isso, caso estejam criptografados, só serão úteis caso sejam decodificados (CERT, 2015).

Existem diversos *sniffers* disponíveis que, para Galvão (2013), podem se diferenciar em inúmeras características – operacionalização em linha de comando ou através de interface gráfica, sistemas operacionais compatíveis, licença de uso, entre outras. No entanto, o procedimento realizado pela ferramenta é o mesmo: alterar o comportamento padrão da interface de rede de forma a ativar o modo de captura de pacotes, também conhecido como modo promíscuo (em redes cabeadas) ou modo monitor (em redes sem fio) (GALVÃO, 2013). De acordo com Junior e Moreira (2014), as principais NFAT que podem ser utilizadas na captura de tráfego são: *NetworkMiner*, *tcpdump* e *Wireshark*.

O *software NetworkMiner*, no que tange à etapa de coleta, é uma ferramenta capaz de interceptar e registrar o tráfego de dados de uma rede de computadores (NETRESEC, 2015). O processo ocorre de forma passiva, ou seja, sem colocar qualquer tipo de tráfego na rede. Através dessa ferramenta é possível detectar sistemas operacionais, nomes de host e portas abertas. Além disso, é possível capturar e armazenar o tráfego da rede no formato *packet capture* (*pcap*) para uma posterior remontagem e análise dos arquivos transmitidos.

O *NetworkMiner* é uma ferramenta compatível com diversos sistemas operacionais – entre eles *Windows*, *Linux* e *MAC OS X* – e possui as versões *Open Source* (código-fonte aberto, sem restrições de cópias ou modificações) e comercial.

A depender da versão, essa ferramenta possui a opção de interação via linha de comando ou interface gráfica. O NETRESEC é o fornecedor responsável pelo software que, além de realizar pesquisa e desenvolvimento na área de análise de tráfego e segurança de rede, disponibiliza produtos, treinamentos e um blog, todos relacionados à perícia em redes ou à ferramenta *NetworkMiner* (NETRESEC, 2015).

A Figura 5 ilustra uma captura de tráfego de rede realizada através do *software NetworkMiner* em sua versão comercial.

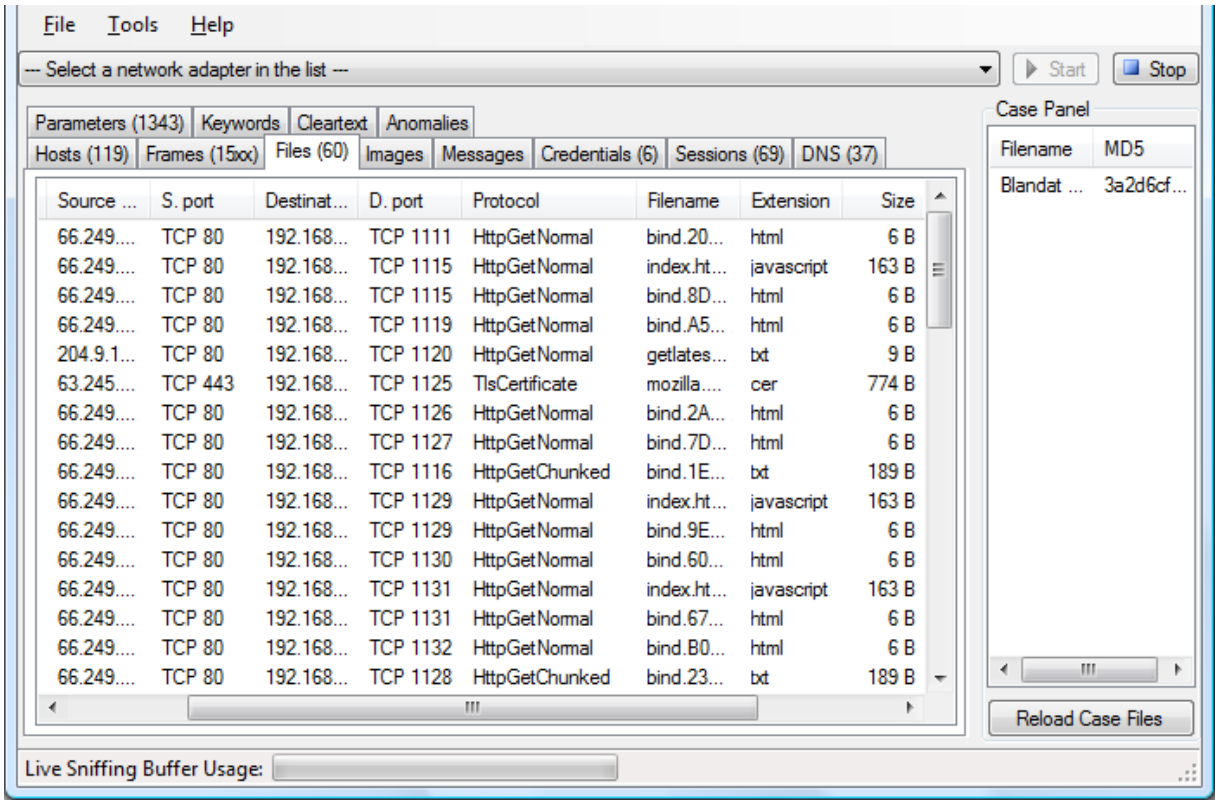


Figura 5 – Captura de tráfego através do *NetworkMiner*
Fonte: Adaptado de Netresec (2015).

O *software tcpdump*, de acordo com Galvão (2013), é o *sniffer Open Source* mais conhecido e utilizado atualmente. Essa ferramenta provê uma interface de interação entre o usuário e a biblioteca *libpcap* – biblioteca *Open Source* utilizada por diversas ferramentas NFAT, que oferece uma infraestrutura flexível para captura e monitoramento de pacotes em redes de computadores (GALVÃO, 2013). O processo de captura ocorre da seguinte forma: a biblioteca *libpcap* altera o funcionamento padrão da placa de rede; os pacotes que trafegam pela interface de rede são capturados e repassados ao *tcpdump*; a ferramenta realiza uma filtragem, definindo quais campos ou informações serão exibidas ou gravadas em um arquivo de extensão *pcap* (GALVÃO, 2013).

O *tcpdump* é compatível com as principais versões baseadas no sistema operacional Unix (*Linux*, *Solaris*, *MAC OS X*, entre outros). Além disso, há a versão chamada *WinDump* (que interage com a biblioteca *winpcap*) para o sistema operacional *Microsoft Windows*. Tanto o *tcpdump* quanto o *WinDump* possuem

documentação completa, fórum de discussão e de suporte. No entanto, de acordo com Galvão (2013), há algumas exigências e limitações, entre elas: são ferramentas executadas em linha de comando, portanto exigem o conhecimento da sintaxe para a execução de uma captura; capturam, em regra, somente os pacotes que efetivamente trafegam pela interface de rede do dispositivo computacional que executa a ferramenta. A Figura 6 ilustra uma captura e gravação (em um arquivo de formato *pcap)*, e posterior análise, através da ferramenta *tcpdump*, de um tráfego de rede envolvendo o próprio *host.*

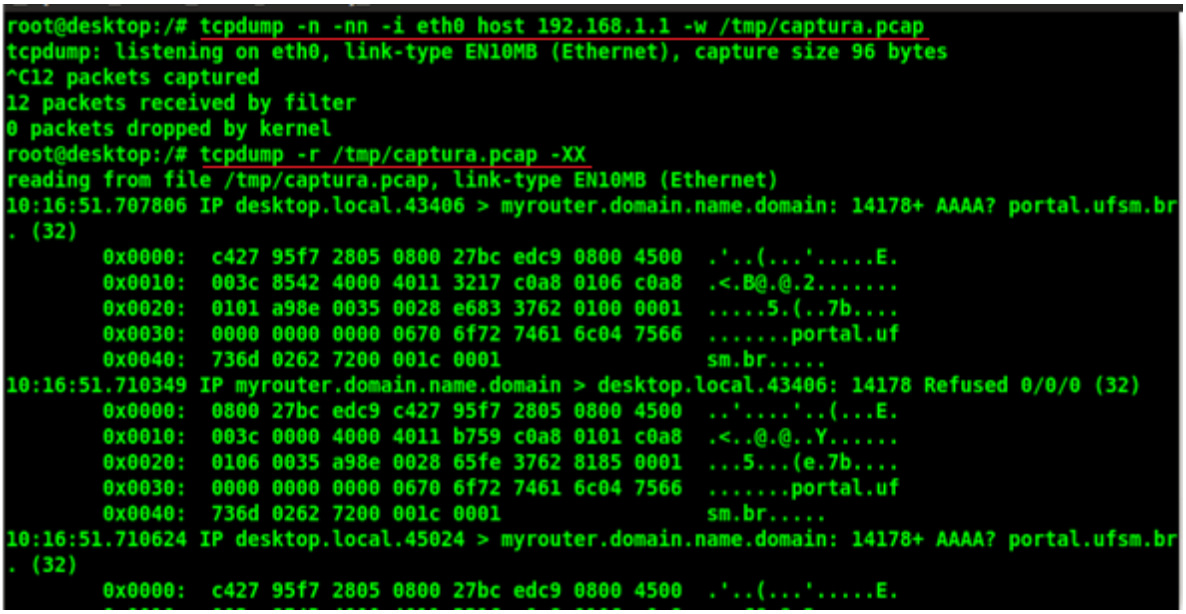

Figura 6 – Captura de tráfego com *tcpdump*
Fonte: do Autor.

Segundo Galvão (2013), a limitação de capturar, em regra, somente os pacotes que trafegam pela interface de rede ocorre devido às soluções de conectividade e segurança que limitam ou bloqueiam o tráfego, como no caso de redes com *switch.* Esse equipamento limita por padrão o tráfego de pacotes aos *hosts* envolvidos no processo de comunicação. Essa limitação pode ser contornada, no entanto, através do uso de portas de monitoramento presentes no *switch* (GALVÃO, 2013).

O *software Wireshark* é o principal analisador de protocolo de rede existente (*WIRESHARK*, 2015). Em relação à etapa de coleta, essa ferramenta também possui a funcionalidade de captura de pacotes. Ao utilizar a biblioteca *libpcap*, o

*Wireshark* modifica o funcionamento padrão da interface de rede (alterando-a para o modo promíscuo), permitindo a captura do tráfego de rede, acompanhamento em tempo real (através de sua interface gráfica) e gravação no formato *pcap* para posterior análise.

O *Wireshark* é uma ferramenta *Open Source*, disponível para diversas plataformas – *Microsoft Windows*, *Linux*, *MAC OS X*, entre outras. De acordo com Galvão (2013), uma das principais vantagens em utilizar o *Wireshark* para a captura e análise de tráfego de rede é a possibilidade de acompanhar detalhadamente, através de sua interface gráfica e em tempo real, os pacotes capturados.

Galvão (2013) adverte que, em ambientes de grande volume de tráfego de dados, a utilização do *Wireshark* em modo gráfico para o acompanhamento da captura em tempo real pode gerar um consumo excessivo ou até mesmo a exaustão dos recursos do sistema computacional (processamento, memória, etc.), implicando no descarte de pacotes e no comprometimento da coleta de dados. Nesse sentido, Galvão (2013) recomenda que, para a captura de dados, o *Wireshark* seja utilizado em modo linha de comandos ou, então, seja utilizada outra ferramenta para a captura do tráfego. A Figura 7 ilustra uma captura de um tráfego de rede realizada pelo *software Wireshark* sobre a interface do próprio *host*.

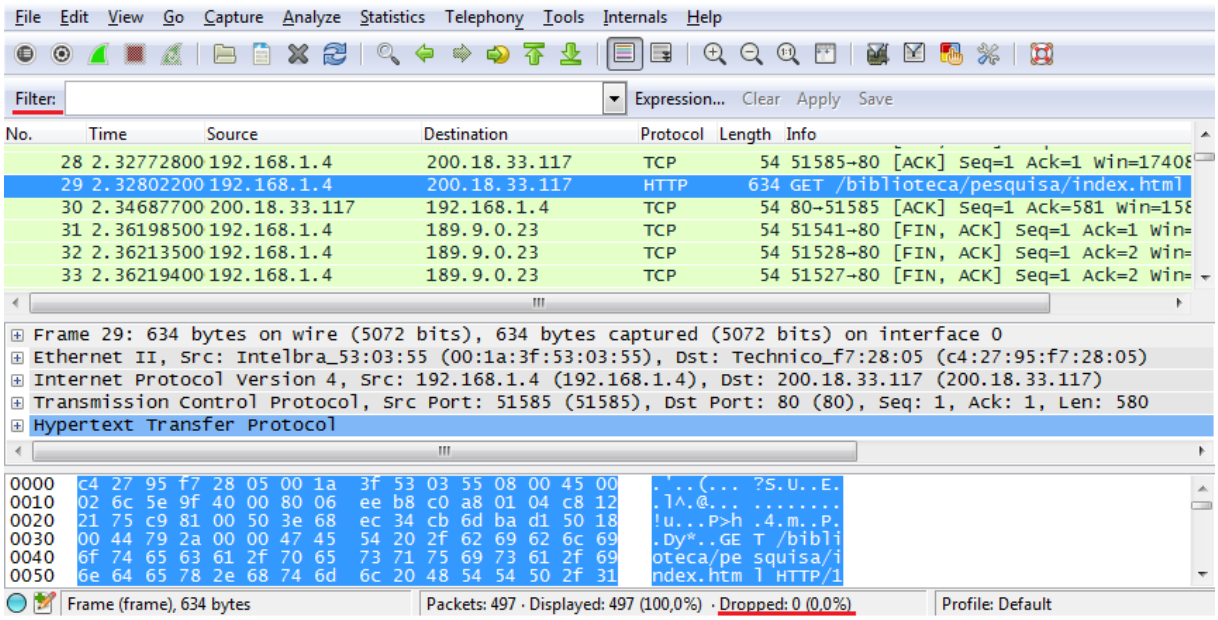


Figura 7 – Captura de tráfego com *Wireshark*
Fonte: do Autor.

É possível notar (através dos campos marcados em vermelho) que, nesse caso, embora todo o tráfego tenha sido capturado (campo *Filter* em branco, ou seja, não foram aplicados filtros) e mostrado em tempo real, não houve descarte de pacotes (ou seja, campo *Dropped* permaneceu em zero).

Na seção 2.2.5 é apresentado um quadro comparativo contendo as técnicas e ferramentas discutidas neste subcapítulo. Nesse quadro, os campos “Família”, “Tipo” e “Nome” são utilizados para uma melhor organização de acordo com a utilização ou com a natureza da técnica ou ferramenta. O campo “Família” é dividido conforme a volatilidade dos dados a serem coletados. No campo “Tipo”, são formados conjuntos de técnicas ou ferramentas em *hardware* ou *software* para uma determinada operação de coleta – no conjunto do “Tipo” *dump* de memória, são apresentados os *softwares* que podem ser utilizados para uma coleta de dados envolvendo memória principal, por exemplo. No campo “Nome”, é apresentado o nome da técnica ou ferramenta.

Os campos “*Graphical User Interface”* (GUI), “Multiplataforma”, “*Open Source”* e “Suporte” são utilizados para classificar as técnicas e ferramentas quanto a algumas importantes características para a atividade da forense computacional – a classificação foi feita através da pesquisa por informações em sites oficiais de desenvolvedores e fornecedores. No campo “GUI”, é sinalizado se há uma interface gráfica para o usuário interagir com a ferramenta. No campo “Multiplataforma”, é sinalizado se a técnica ou ferramenta pode ser utilizada em diversos sistemas operacionais, isto é, se a ferramenta não é exclusiva de um determinado sistema. No campo “*Open Source”,* é sinalizado se a versão completa da ferramenta, além de ser “*Open Source”,* é disponibilizada de forma totalmente gratuita. No campo “Suporte”, a técnica ou ferramenta é classificada, de forma cumulativa, de acordo com o nível de suporte que é oferecido. Uma classificação nível um (“**+**”), significa que o desenvolvedor oferece suporte através de documentação ou contato – através de *e-mail* ou telefone, por exemplo. Uma classificação nível dois (“**++**”), significa que há suporte através de fóruns de discussão ou *blogs*, ou então que há atualizações periódicas com notícias e promoção de cursos para o aperfeiçoamento do uso da ferramenta. Uma classificação nível três (“**+++**”), significa que há suporte disponível em língua portuguesa, seja pelo desenvolvedor, seja por fóruns de discussão ou *blogs* brasileiros.

### 2.2.5 Comparativo entre as principais técnicas e ferramentas para coleta

| **Família** | **Tipo** | **Nome** | **GUI** | **Multi plataforma** | ***Open Source*** | **Suporte** |
|---|---|---|---|---|---|---|
| Coleta de dados não voláteis | Técnica para Duplicação | Espelhamento | | ✔ | | + |
| | | Imagem | | ✔ | | + |
| | *Hardware* Bloqueador de Escrita | Espion Forensics FastBlock 3 | | ✔ | | + |
| | | Forensic bridge Tableau | | ✔ | | + |
| | | ICS Write Protect Card Reader | | ✔ | | + |
| | | Intelligent Computer Solutions Solo III | | ✔ | | ++ |
| | | Tableau TD2u | | ✔ | | ++ |
| | *Software* Duplicação Forense | Symantec Norton Ghost | ✔ | ✔ | | +++ |
| | | Forensic ToolKit | ✔ | *Windows* | | ++ |
| | | EnCase | ✔ | *Windows* | | ++ |
| | | *dd* | | *Linux* | ✔ | +++ |
| | | *DC3DD* | | ✔ | ✔ | +++ |
| | | *Guymager* | ✔ | *Linux* | ✔ | +++ |
| | Sistema Operacional / Distribuição Forense | *CAINE* | ✔ | *Linux* | ✔ | ++ |
| | | *FDTK* | ✔ | *Linux* | ✔ | + |
| | | Knoppix | ✔ | *Linux* | ✔ | ++ |
| | | Helix | ✔ | *Linux* | | ++ |
| Coleta de dados Voláteis | *Dump* de Memória | *dd* | | *Linux* | ✔ | +++ |
| | | m*dd* | | *Windows* | ✔ | +++ |
| | Captura de Tráfego de Rede | *NetworkMiner* | ✔ | ✔ | | ++ |
| | | *Tcpdump* | | *Linux* | ✔ | +++ |
| | | *WinDump* | | *Windows* | ✔ | +++ |
| | | *Wireshark* | ✔ | ✔ | ✔ | +++ |

Quadro 2 – Comparativo de técnicas e ferramentas para coleta
Fonte: do Autor.

## 2.3 Principais aspectos, técnicas e ferramentas para extração

Depois de realizada a coleta, a próxima etapa é extrair dados e informações pertinentes para uma posterior análise. Essa etapa envolve a avaliação e extração do que pode ser útil para a investigação (*FDTK*-WIKI, 2015) – dados irrelevantes para a perícia (arquivos de programas, por exemplo) podem ser ignorados; possíveis fontes de evidências podem estar inacessíveis, devido à prévia exclusão ou à proteção por senha. Nesse sentido, as principais técnicas e ferramentas utilizadas na etapa de extração do processo forense são apresentadas no subcapítulo 2.3.

### 2.3.1 Recuperação de arquivos

Os dispositivos e mídias de armazenamento podem guardar muitas informações que, a princípio, não estão visíveis aos usuários comuns. Esse fato ocorre devido ao tipo de organização de dados adotado nesses materiais. Eleutério e Machado (2011) apresentam, de forma ilustrativa, um comparativo entre um disco rígido e um planeta de dados conforme mostra a Figura 8. A exploração das camadas de um planeta (ou dos arquivos de um sistema de armazenamento) fica mais complexa quanto mais interna na ilustração.

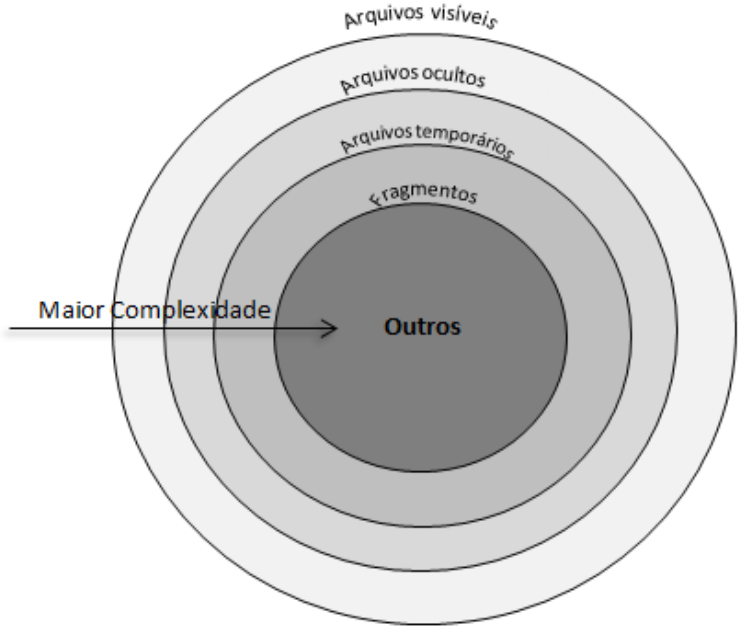


Figura 8 – Disco rígido como um planeta de dados
Fonte: Adaptado de Eleutério e Machado (2011).

Nesse sentido, assim como um planeta pode ser dividido em camadas, os arquivos e dados contidos em um disco rígido, por exemplo, também podem ser classificados desta maneira. Na camada mais externa estão os arquivos visíveis, que podem ser visualizados e acessados normalmente por um usuário comum, sem a necessidade de técnicas, procedimentos ou ferramentas específicas. Os arquivos ocultos estão uma camada abaixo – arquivos não visíveis em um diretório ou em uma pasta, mas comuns em todos os outros aspectos. Depois, aparecem os arquivos e dados salvos temporariamente – registros de impressão, *swap* de memória, entre outros – e os fragmentos de arquivos, que são partes isoladas de um arquivo.

Na região mais interna da Figura 8 são é classificado outros arquivos e dados, representados principalmente por arquivos apagados e por arquivos protegidos por senhas. Segundo Kent et al (2006), arquivos comprimidos, criptografados ou protegidos por mecanismos de controle de acesso também fazem parte dessa classificação. A recuperação de informações dessa região é complexa, exige tempo e uso de técnicas e ferramentas específicas. No entanto, a recuperação eficaz dessas informações pode resultar em evidências elucidativas para a perícia forense (ELEUTÉRIO; MACHADO, 2011).

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

A recuperação de arquivos apagados, também chamada de *Data Carving*, ocorre através da busca de assinaturas conhecidas (cabeçalhos que contêm o formato dos arquivos, entre eles *JPEG, AVI, DOC, PDF,* etc.) (ELETÉRIO; MACHADO, 2011). Essa busca é realizada em toda a área classificada como disponível no dispositivo de armazenamento. Ao encontrar uma assinatura

conhecida, o restante do conteúdo do arquivo é procurado e recuperado. A recuperação poderá ser integral (caso as informações do arquivo apagado estejam preservadas) ou parcial (caso as informações tenham sido sobrescritas por outro arquivo). O processo de busca e recuperação de arquivos apagados é realizado de forma automática por diversas ferramentas, entre as principais estão o *Ontrack Easy Recovery* e o *Photorec*.

A ferramenta *Ontrack Easy Recovery* é um *software* para recuperação de dados que possui uma interface amigável e realiza diversos tipos de recuperação de arquivos. Segundo Eleutério e Machado, o *software* realiza recuperação de arquivos não só através da busca por assinaturas (formatos de arquivos) conhecidas, mas também com base na estrutura de arquivos utilizada pelo sistema operacional presente no dispositivo a ser recuperado. Além disso, essa ferramenta possui um módulo de recuperação de mensagens eletrônicas e de arquivos compatíveis com o pacote de aplicativos *Microsoft Office*. O *software Ontrack Easy Recovery* é compatível com os sistemas operacionais *Windows* e *MAC OS X* e é disponibilizado em três versões comerciais.

A ferramenta *Photorec* é um *software Open Source* para recuperação de arquivos e dados compatível com diversas assinaturas (mais de 440 formatos), sistemas de arquivos (*FAT, NTFS, EXT,* etc*.)*, dispositivos e mídias de armazenamento (SILVA; OLIVEIRA, 2014). Embora o *software* seja executado em linha de comando, ele é multiplataforma, compatível com diversos sistemas operacionais, entre eles *Windows*, *Linux* e *MAC OS X* (CGSECURITY, 2015).

Além da recuperação de arquivos apagados, é comum que os peritos se depararem com arquivos e programas protegidos por senha durante a etapa de extração. Uma vez que tais arquivos podem ocultar evidências, é necessário aplicar técnicas e ferramentas que possibilitem o acesso ao conteúdo desses arquivos e programas. Ataque de força bruta, ataque de dicionário, engenharia social*, RainBow Tables* e engenharia reversa são as principais técnicas que permitem a quebra ou a descoberta de senhas em arquivos ou em *softwares* (ELEUTÉRIO; MACHADO, 2011).

Ataque de força bruta e de dicionário são técnicas semelhantes para descoberta, por tentativa e erro, de nomes de usuários ou senhas (CERT, 2015). No caso da força bruta, um domínio é predefinido e todas as combinações possíveis são testadas até que se acerte a senha. Esse domínio pode ser especificado entre

um número mínimo e máximo de caracteres, existência de letras e números, letras maiúsculas e minúsculas, entre outros. É importante que o domínio seja bastante específico, caso contrário, este tipo de ataque pode tornar-se inviável devido ao grande número de combinações possíveis e ao esforço computacional para processá-las e testá-las. No segundo caso, o processo de tentativa e erro se utiliza de um dicionário, ou seja, de uma lista de possíveis senhas. O ataque de dicionário costuma ser mais eficaz que o de força bruta, pois utiliza padrões de senha normalmente utilizados (senhas no formato de datas, por exemplo). Entre as principais ferramentas para ataque de força bruta ou de dicionário estão os *softwares ElcomSoft Password Recovery Bundle* e o *John the Ripper*.

O *software ElcomSoft Password Recovery Bundle* é uma solução comercial para recuperação de arquivos protegidos por senha. O programa possui interface gráfica, é compatível com o sistema operacional *Windows* e possui três versões disponíveis para diferentes necessidades. O *software John the Ripper* é uma solução *Open Source* e gratuita, operado através de linha de comandos e compatível com diversos sistemas operacionais, entre eles *Linux*, *MAC OS X* e *Windows*. Ambas as soluções apresentam escalabilidade linear, isto é, permitem a utilização de processadores ou *chips* gráficos em série para aumentar a capacidade de recuperação de senhas.

A técnica de descoberta de senhas através *RainBow Tables* (tabelas pré-compiladas de *hashes*) é mais eficiente do que um ataque de força bruta (ELEUTÉRIO; MACHADO, 2011). Um ataque de força bruta é uma tentativa de descoberta de uma chave criptográfica ou senha, gerando computacionalmente todas as combinações de caracteres possíveis até que a correta seja encontrada – fato que dependerá do tamanho da chave ou senha e dos recursos computacionais aplicados (ACCESSDATA-A, 2015). Em tabelas RainBow Tables, todas as chaves ou senhas possíveis já estão calculadas. Assim, descobrir uma senha de 40 *bits* com o uso de *RainBow Tables* levaria segundos ou minutos, enquanto um ataque de força bruta poderia levar dias a depender do sistema computacional aplicado (ACCESSDATA-B, 2015). O *software Ophcrack* é um exemplo de ferramenta que usa tabelas *RainBow Tables* para descoberta de senhas. O *software* possui interface gráfica, é *Open Source* e é multiplataforma (compatível com *Windows*, *Linux* e *MAC OS X*).

A engenharia social pode ser definida como um conjunto de atos que influenciam uma pessoa a realizar uma determinada ação de interesse (SOCIAL-ENGINEER, 2015). De acordo com Eleutério e Machado (2011), em um ambiente no qual a recuperação de arquivos protegidos é o objetivo da perícia, a engenharia social seria um processo de obtenção de senhas realizada com os usuários. Em sua forma mais simples, bastaria perguntar ao usuário e contar com a sua colaboração (ELEUTÉRIO; MACHADO, 2011). Em sua forma mais complexa, a engenharia social poderia envolver técnicas de *phishing* (influenciando ou obtendo informações através do envio de *e-mails* de origem aparentemente confiável), *vishing* (através do telefone) ou *Impersonation* (através da interação pessoal com um círculo social ou profissional) (SOCIAL-ENGINEER, 2015).

A engenharia reversa de um *software* é um processo de desmontagem e análise. Seu objetivo é analisar e construir um modelo representativo em alto nível de um determinado programa para que ele possa ser entendido (PINHEIRO, 2013). De acordo com Eleutério e Machado (2011), a partir do conhecimento da estrutura de um determinado programa é possível detectar a parte responsável pela autenticação de usuários (requisição de senhas, por exemplo). Em muitos casos, será possível modificar a senha ou até excluir sua necessidade, através do processo de alteração do código-fonte (ELEUTÉRIO; MACHADO, 2011). Para auxiliar nesse processo minucioso, que pode envolver análise de executáveis em programação de baixo nível, há ferramentas em *software* como o *Olly Debugger* (compatível com *Windows*) e o *IDA Pro Disassembler and Debugger* (multiplataforma), ambas comerciais e operadas através de interface gráfica. No caso do IDA Pro Disassembler and Debugger, a *Hex-Rays* (desenvolvedora do *software*) disponibiliza diversas opções de suporte, como contato através de *e-mail*, fórum, *blog*, treinamentos, tutoriais e documentação.

### 2.3.2 Indexação de dados

A indexação é uma técnica de organização de dados em um dispositivo de armazenamento. De acordo com Eleutério e Machado (2011), o processo de indexação funciona da seguinte forma: após percorrer todos os dados (*bits*) presentes em um dispositivo ou em uma base de dados, todas as ocorrências

alfanuméricas são localizadas e organizadas de forma que seja possível acessá-las ou recuperá-las de forma rápida.

A indexação dos dados cria uma espécie de catálogo, contendo todas as cadeias alfanuméricas encontradas, assim como a localização de cada uma delas. Depois de realizada, permite que o processo de *Data Carving* seja feito de forma rápida e eficiente, uma vez que todo o conteúdo do dispositivo de armazenamento foi percorrido e as ocorrências alfanuméricas (inclusive as assinaturas conhecidas) foram organizadas. Além disso, será possível realizar buscas rápidas, através de palavras-chave, no conteúdo dos dispositivos examinados. Essa busca é uma das técnicas utilizadas na análise, próxima etapa da perícia forense computacional (ELEUTÉRIO; MACHADO, 2011).

Existem diversas ferramentas em *software* disponíveis para a indexação de dados, entre as principais estão: Forensic TooKit (*FTK*), Encase e Forensic Digital ToolKit (*FDTK*). Segundo Eleutério e Machado (2011), o *FTK* e o Encase, além de realizarem a recuperação e a indexação de dados, são soluções comerciais que oferecem, de forma integrada, diversas ferramentas que podem ser utilizadas em todas as etapas da perícia forense. Já o *FDTK*, de acordo com Weyer (2011), é uma distribuição *Linux* que reúne diversas ferramentas – entre elas o *slocate*, *software Open Source* utilizado para a localização e indexação de arquivos e dados – capazes de atender a todas as etapas periciais. O *FDTK* foi criado a partir da distribuição Ubuntu, possui uma interface amigável (estruturada conforme as etapas do processo pericial) é distribuído em português e está em constante desenvolvimento pela comunidade *Linux* (WEYER, 2011).

A seção 2.3.3 apresenta um quadro comparativo contendo as técnicas e ferramentas discutidas neste subcapítulo. No Quadro 3, os campos “Família”, “Tipo” e “Nome” são utilizados para uma melhor organização de acordo com a utilização ou com a natureza da técnica ou ferramenta. O campo “Família” é dividido conforme a volatilidade dos dados a serem coletados. No campo “Tipo”, são formados conjuntos de técnicas ou ferramentas em *software* para uma determinada operação de extração – no conjunto do “Tipo” *Software* para indexação de dados, são apresentados os *softwares* que podem ser utilizados para organizar os dados, de forma alfanumérica, em um dispositivo de armazenamento, por exemplo. No campo “Nome”, é apresentado o nome da técnica ou ferramenta.

Os campos “*Graphical User Interface”* (GUI), “Multiplataforma”, “*Open Source”* e “Suporte” são utilizados para classificar as técnicas e ferramentas quanto a algumas importantes características (como existência ou não de interface gráfica para o usuário, por exemplo) para a atividade da forense computacional – a classificação foi feita através da pesquisa por informações em sites oficiais de desenvolvedores e fornecedores. No campo “GUI”, é sinalizado se há uma interface gráfica para o usuário interagir com a ferramenta. No campo “Multiplataforma”, é sinalizado se a técnica ou ferramenta pode ser utilizada em diversos sistemas operacionais, isto é, se a ferramenta não é exclusiva de um determinado sistema. No campo “*Open Source”,* é sinalizado se a versão completa da ferramenta, além de ser “*Open Source”,* é disponibilizada de forma totalmente gratuita. No campo “Suporte”, a técnica ou ferramenta é classificada, de forma cumulativa, de acordo com o nível de suporte que é oferecido. Uma classificação nível um (“**+**”), significa que o desenvolvedor oferece suporte através de documentação ou contato – através de *e-mail* ou telefone, por exemplo. Uma classificação nível dois (“**++**”), significa que há suporte através de fóruns de discussão ou *blogs*, ou então que há atualizações periódicas com notícias e promoção de cursos para o aperfeiçoamento do uso da ferramenta. Uma classificação nível três (“**+++**”), significa que há suporte disponível em língua portuguesa, seja pelo desenvolvedor, seja por fóruns de discussão ou *blogs* brasileiros.

### 2.3.3 Comparativo entre as principais técnicas e ferramentas para extração

| **Família** | **Tipo** | **Nome** | **GUI** | **Multi plataforma** | ***Open Source*** | **Suporte** |
|---|---|---|---|---|---|---|
| Recuperação de arquivos | *Software* - recuperação de arquivos apagados | *Ontrack Easy Recovery* | ✔ | ✔ | | **++** |
| | | *Photorec* | | ✔ | ✔ | **++** |
| | Técnica - recuperação de arquivos protegidos | Ataque de força bruta | | ✔ | | **+** |
| | | Ataque de dicionário | | ✔ | | **+** |
| | | RainBow Tables | | ✔ | | **+** |
| | | Engenharia social | | ✔ | | **+** |
| | | Engenharia reversa | | ✔ | | **+** |
| | *Software* - recuperação de arquivos protegidos | ElcomSoft Password Recovery Bundle | ✔ | *Windows* | | **++** |
| | | *John the Ripper* | | ✔ | ✔ | **+++** |
| | | *Ophcrack* | ✔ | ✔ | ✔ | **+** |
| | | *Olly Debugger* | ✔ | *Windows* | | **+** |
| | | IDA Pro Disassembler and Debugger | ✔ | ✔ | | **++** |
| Indexação de dados | *Software* - indexação de dados | Forensic ToolKit (*FTK*) | ✔ | *Windows* | | **++** |
| | | Encase | ✔ | *Windows* | | **++** |
| | | Forensic Digital ToolKit (*FDTK*) | ✔ | *Linux* | ✔ | **+** |

Quadro 3 – Comparativo de técnicas e ferramentas para extração
Fonte: do Autor.

## 2.4 Principais aspectos, técnicas e ferramentas para análise

A etapa de análise consiste em examinar os dados extraídos da etapa anterior (etapa de extração), identificar evidências digitais e verificar a relação com o fato investigado (KENT et al., 2006).

De acordo com Almeida (2011), a partir da identificação e da avaliação das evidências presentes no material analisado, será possível responder aos quesitos elaborados pela autoridade solicitante. Nesse sentido, é recomendado que a autoridade solicite detalhadamente os tipos de arquivos procurados e utilize quesitos com nomes de pessoas, empresas ou documentos específicos; ou seja, apresente claramente o que deve ser procurado pelo perito, de forma a evitar trabalhos desnecessários (ALMEIDA, 2011).

### 2.4.1 Análise de dados provenientes de dispositivos de armazenamento

Segundo Eleutério e Machado (2011), um disco rígido de 80 GB, considerado pequeno nos padrões atuais, pode conter milhões de arquivos. Analisar o conteúdo de todos os arquivos, verificando-os um a um, pode levar muito tempo e tornar o exame inviável (ELEUTÉRIO; MACHADO, 2011).

Nesse sentido, além da solicitação através de quesitos objetivos e detalhados pela autoridade, Eleutério e Machado (2011) discorrem sobre alguns procedimentos, técnicas e ferramentas que podem ser utilizadas para tornar a etapa de análise viável e eficiente, entre elas: utilização de filtros Known File Filter, pesquisas por palavras-chave, navegação pelo sistema de pastas e arquivos, visualização adequada de arquivos e virtualização.

O *Known File Filter* (KFF) é uma lista de valores *hash* (resumos unidirecionais) de arquivos ou informações conhecidas que pode ser utilizada para filtrar o conteúdo de um dispositivo analisado, ignorando arquivos irrelevantes ou detectando arquivos de interesse à perícia (ACCESSDATA-A, 2015).

Com a utilização de KFF é possível: diminuir o número de arquivos ignorando, por exemplo, o sistema operacional ou programas diversos conhecidos que estejam instalados no dispositivo de armazenamento analisado; verificar a existência de um determinado arquivo de interesse à perícia, como nos casos em que um mesmo

arquivo conhecido (um vídeo de pornografia infantil, por exemplo) está presente em vários dispositivos de armazenamento. Assim, a aplicação do KFF contendo previamente o que se deve filtrar, será possível realizar uma análise mais eficiente, seja descartando arquivos irrelevantes, seja detectando a existência de um arquivo ou informação útil para a perícia(ELEUTÉRIO; MACHADO, 2011).

A pesquisa por palavras-chave em um dispositivo de armazenamento computacional é uma técnica bastante eficaz para localizar arquivos de interesse à perícia (ELEUTÉRIO; MACHADO, 2011). Após o dispositivo ser estruturado e organizado (através da indexação de dados), diversas buscas podem ser realizadas por todo o seu conteúdo de forma rápida. Uma busca pela palavra “contatos”, por exemplo, retornaria todos os arquivos e fragmentos de arquivos que contenham essa palavra, inclusive os recuperados na etapa de extração. Eleutério e Machado (2011) ressaltam, no entanto, que caso o conteúdo dos arquivos esteja criptografado, a pesquisa por palavras-chave não encontrará os valores ou as palavras procuradas. Além disso, buscas em dispositivos não indexados podem levar um tempo a mais (a depender da capacidade de armazenamento ou velocidade de leitura), pois, a cada pesquisa, todo o seu conteúdo terá de ser percorrido.

A navegação pelo sistema de arquivos e pastas do dispositivo é uma técnica interessante para encontrar vestígios de interesse à perícia (ELEUTÉRIO; MACHADO, 2011). As pastas “Meus Documentos” e “*Desktop*” (em sistemas *Windows*), ou então o diretório “/home” (em sistemas *Linux*), por exemplo, são locais onde geralmente os usuários guardam seus arquivos pessoais. De acordo com Eleutério e Machado (2011), identificar e analisar os arquivos presentes nesses locais é de suma importância para a investigação.

A visualização adequada dos arquivos é fundamental para a etapa de análise de dados da perícia forense computacional (ELEUTÉRIO; MACHADO, 2011). Segundo Eleutério e Machado (2011), possíveis evidências podem passar despercebidas caso o perito não disponha de ferramentas que interpretem e mostrem corretamente o conteúdo de um determinado arquivo.

Na Figura 9, por exemplo, um arquivo foi recuperado na etapa de extração (através do processo de recuperação de arquivos apagados) e, posteriormente, analisado.

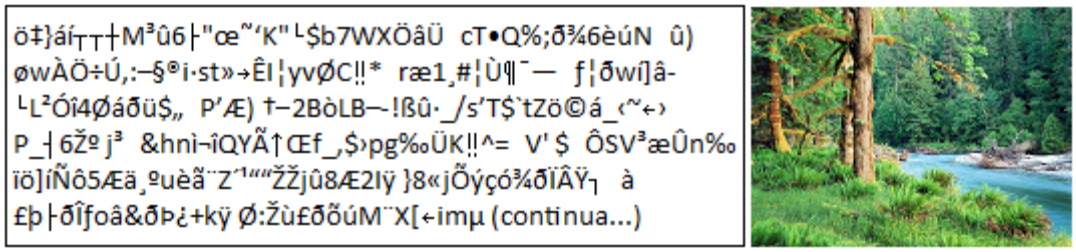


Figura 9 – Visualização de um arquivo na forma textual e na forma gráfica
Fonte: Adaptado de Eleutério e Machado (2011).

Quando visualizado na forma gráfica, o arquivo ilustrado pela Figura 9 faz mais sentido, isto é, trata-se de uma imagem. Isso pode ocorrer devido à recuperação incompleta dos dados – o cabeçalho e o rodapé do arquivo, contendo informações sobre seu formato, podem ter sido sobrescritos –, ou devido à incompatibilidade entre imagem e ferramenta de visualização – a extensão ou o formato da imagem serem desconhecidos ou não suportados.

De acordo com Eleutério e Machado (2011), o Forensic ToolKit (*FTK*) e o EnCase são exemplos de *softwares* que podem auxiliar na etapa de análise, seja através da aplicação de filtros KFF, de pesquisas por palavras-chave, da navegação pelo sistema de arquivos ou da visualização adequada de arquivos. Tanto o *FTK* quanto o EnCase são soluções comerciais que disponibilizam funções úteis a todas as etapas de uma perícia forense envolvendo equipamentos de informática.

A virtualização é uma técnica interessante nos casos em que se deseje entender as operações realizadas pelo s usuários dos computadores e dispositivos examinados (ELEUTÉRIO; MACHADO, 2011). Uma vez apreendido um equipamento computacional (um computador, por exemplo), o mesmo não pode ser ligado pelas vias normais, pois isso pode acarretar alterações ou perdas de informações devido à inicialização do sistema. Nesse sentido, depois de realizados os procedimentos da etapa de coleta, o sistema operacional contido no espelho ou na imagem poderá ser inicializado de forma segura através de um *software* de virtualização.

Para Eleutério e Machado (2011), a virtualização, além de ser interessante para visualizar o ambiente do sistema operacional e para entender as operações realizadas pelo usuário, é bastante útil nos casos em que o dispositivo de armazenamento analisado contenha programas específicos instalados, que demandem muitas configurações e ajustes para serem executados a partir de outro ambiente computacional. Assim, com a virtualização, a execução e a análise desses programas podem ser realizadas de forma mais simples pelo perito.

Entre os programas mais utilizados na operação de virtualização estão o Virtual Box e o VMWare. O *software* Virtual Box é a única solução profissional de virtualização disponível para empresas e para uso doméstico de forma gratuita e *Open* Source (VIRTUALBOX, 2015). O VMWare é uma opção comercial que realiza o processo de virtualização sem alterar os dados contidos nas cópias provenientes da etapa de coleta e preservação, pois uma camada intermediária de dados é utilizada entre a máquina virtual e a cópia analisada (ELEUTÉRIO; MACHADO, 2011). Ambas alternativas de *software* para virtualização são multiplataforma (compatíveis com *Windows*, *Linux*, *MAC OS X*, entre outros) e são atualizadas periodicamente.

### 2.4.2 Análise do tráfego de rede

Segundo Junior e Moreira (2014), a análise forense de redes possibilita a reunião de informações sobre o tráfego e colabora para a elaboração de respostas aos quesitos levantados pela investigação. O objetivo é examinar eventuais dados e informações que tenham relação com o incidente, de forma a elucidar o fato investigado (ERBACHER; CHRISTIANSEN; SUNDBERG, 2006).

A análise do tráfego de uma rede pode ser em tempo real – a captura e a análise dos pacotes trafegados são simultâneas – ou a partir de um arquivo *pcap* – arquivo *packet capture* oriundo da etapa de coleta. Independente do tipo de análise empregada, a identificação da origem e do destino de um pacote pode ser um fator importante para a perícia. As principais informações que auxiliam na identificação dos *hosts* (um computador servidor e outro cliente, por exemplo) envolvidos em uma comunicação são: endereço de IP de origem e de destino; porta de origem e de destino; protocolo de transporte (GALVÃO, 2013). O Quadro 4 organiza, de forma justificada, a interpretação dessas informações através do *software Wireshark* –

*software* para captura e análise de pacotes, multiplataforma, *Open Source* e com interface gráfica amigável – a partir da análise de um pacote capturado.

```
Internet Protocol Version 4, Src: 192.168.1.4 (192.168.1.4), Dst: 200.18.33.117 (200.18.33.117)
Transmission Control Protocol, Src Port: 51585 (51585), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 580
```

| Informações | Justificativa |
|---|---|
| Endereço de IP de origem: 192.168.1.4 | Campo Src (*Source*) |
| Endereço de IP de destino: 200.18.33.117 | Campo Dst (*Destiny*) |
| Porta de origem: 51585 | Src Port (*Source Port*); Porta alta não padrão |
| Porta de destino: 80 | Dst Port (*Destiny Port*); Porta padrão |
| Protocolo de transporte: TCP | Transmission Control Protocol |

Quadro 4 – Identificação da origem e do destino de um pacote
Fonte: Adaptado de Galvão (2013).

Segundo Galvão (2013), essas informações podem ser usadas para otimizar o processo de captura de pacotes – através da definição de filtros, indicando *hosts*, portas ou serviços específicos –, ou na escolha das técnicas e ferramentas que serão usadas para a análise da camada de aplicação.

Existem algumas técnicas indispensáveis para a análise de pacotes. Entre elas estão o casamento de padrões (*pattern matching*) e a filtragem de pacotes (*packet filter*), que podem ser aplicadas através de algumas ferramentas NFAT como *Wireshark* e *tcpdump* (GALVÃO, 2013).

A técnica de *pattern matching* consiste na busca de pacotes relevantes através do casamento de padrões ou expressões regul*Ares*. A Figura 10 ilustra o uso dessa técnica através da ferramenta ngrep – *software* para análise de pacotes, executado em linha de comando, multiplataforma e *Open Source*.

```
^Croot@desktop-VirtualBox:/# ngrep -I /tmp/captura.pcap 'ufsm'
input: /tmp/captura.pcap
match: ufsm
#
U 10.0.2.15:25823 -> 192.168.1.1:53
  ............site.ufsm.br.....
```

Figura 10 – Exemplo de busca de padrão com ngrep
Fonte: do Autor.

Na Figura 10 é ilustrada uma busca pelo padrão “ufsm” em um arquivo contendo um tráfego de rede capturado anteriormente. É possível notar que houve casamento (*match*) do padrão “ufsm” na comunicação entre o *host* com IP 10.0.2.15 (origem) e o *host* com IP 192.168.1.1 (destino). Além disso, é possível perceber que se trata de informações de DNS (devido ao “:53” no IP de destino, ou seja, porta de destino).

A técnica *packet filtering* permite a separação de pacotes através de filtros pré-definidos. É possível, por exemplo, especificar (através da definição de filtros como endereço de origem ou de destino, portas de comunicação utilizadas, entre outros) o que será capturado (ou descartado) para ser analisado.

A Figura 11 ilustra a especificação de alguns filtros para a realização de uma captura e análise através da ferramenta *tcpdump*. No exemplo, são especificados: o filtro *host 192.168.1.1* – determina que a captura será de pacotes que tenham como origem ou destino o dispositivo  com IP 192.168.1.1; o filtro *and port 53* – determina que a captura seja de pacotes que trafeguem pela porta 53, ou seja, de serviço DNS. Assim, só serão capturados os pacotes que satisfaçam, de forma cumulativa, os requisitos dos dois filtros especificados.

```
root@desktop:/# tcpdump -n -nn -i eth0 host 192.168.1.1 \ and port 53 -w /tmp/captura2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes


^C140 packets captured
140 packets received by filter
0 packets dropped by kernel
root@desktop:/# tcpdump -n -nn -i eth0 host 192.168.1.1 -r /tmp/captura2.pcap -XX | more
reading from file /tmp/captura2.pcap, link-type EN10MB (Ethernet)
22:16:53.468596 IP 192.168.1.6.55247 > 192.168.1.1.53: 21633+ AAAA? www.ufsm.br. (29)
        0x0000:  c427 95f7 2805 0800 27bc edc9 0800 4500  .'..(...'.....E.
        0x0010:  0039 0c34 4000 4011 ab28 c0a8 0106 c0a8  .9.4@.@..(......
        0x0020:  0101 d7cf 0035 0025 7c79 5481 0100 0001  .....5.%|yT.....
        0x0030:  0000 0000 0000 0377 7777 0475 6673 6d02  .......www.ufsm.
        0x0040:  6272 0000 1c00 01                        br.....
22:16:53.471222 IP 192.168.1.1.53 > 192.168.1.6.55247: 21633 Refused 0/0/0 (29)
        0x0000:  0800 27bc edc9 c427 95f7 2805 0800 4500  ..'....'..(...E.
        0x0010:  0039 0000 4000 4011 b75c c0a8 0101 c0a8  .9..@.@..\......
        0x0020:  0106 0035 d7cf 0025 fbf3 5481 8185 0001  ...5...%..T.....
        0x0030:  0000 0000 0000 0377 7777 0475 6673 6d02  .......www.ufsm.
        0x0040:  6272 0000 1c00 01                        br.....
22:16:53.471666 IP 192.168.1.6.37091 > 192.168.1.1.53: 21633+ AAAA? www.ufsm.br. (29)
        0x0000:  c427 95f7 2805 0800 27bc edc9 0800 4500  .'..(...'.....E.
        0x0010:  0039 0c35 4000 4011 ab27 c0a8 0106 c0a8  .9.5@.@..'......
        0x0020:  0101 90e3 0035 0025 c365 5481 0100 0001  .....5.%.eT.....
        0x0030:  0000 0000 0000 0377 7777 0475 6673 6d02  .......www.ufsm.
        0x0040:  6272 0000 1c00 01                        br.....
```

Figura 11 – Exemplos de filtros na captura e análise de tráfego com *tcpdump*
Fonte: do Autor.

A Figura 12 ilustra a especificação de alguns filtros para a realização de uma captura e análise através da ferramenta *Wireshark*. Nesse caso, são especificados: o filtro *ip.addr == 192.168.1.4* – determina que a captura será de pacotes que tenham como origem ou destino o dispositivo com IP 192.168.1.4; o filtro *and !(dns)* – determina que serão descartados pacotes de serviço DNS; o filtro *and tcp contains "aluno"* determina que serão capturados pacotes que contenham a *string* "aluno". Assim, só serão capturados os pacotes que satisfaçam, de forma cumulativa, os três filtros especificados.

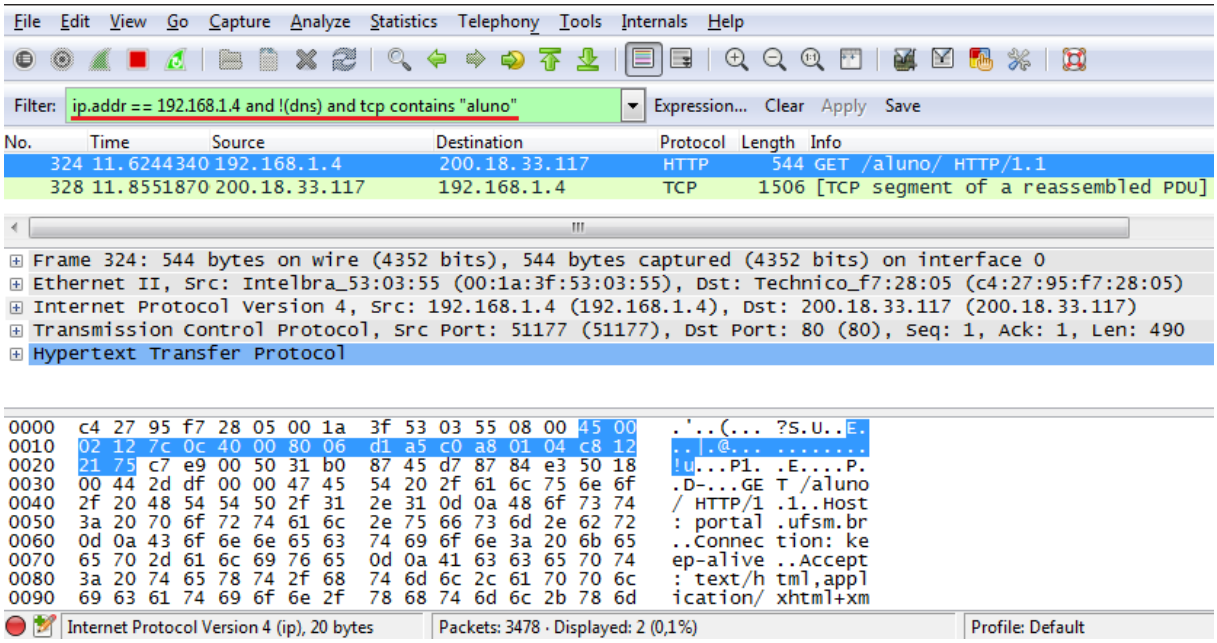


Figura 12 – Exemplos de filtros na captura e análise de tráfego com *Wireshark*
Fonte: do Autor.

Na seção 2.4.3 é apresentado um quadro comparativo contendo as técnicas e ferramentas discutidas neste subcapítulo. No Quadro 5, os campos "Família", "Tipo" e "Nome" são utilizados para uma melhor organização de acordo com a utilização ou com a natureza da técnica ou ferramenta. O campo "Família" é dividido conforme a volatilidade dos dados a serem coletados. No campo "Tipo", são formados conjuntos de técnicas ou ferramentas em *software* para uma determinada operação de análise – no conjunto do "Tipo" *Software* para análise de arquivos são apresentados os *softwares* que podem ser utilizados na correta visualização de um determinado arquivo ou na virtualização de um sistema operacional, por exemplo. No campo "Nome", é apresentado o nome da técnica ou ferramenta.

Os campos “*Graphical User Interface”* (GUI), “Multiplataforma”, “*Open Source”* e “Suporte” são utilizados para classificar as técnicas e ferramentas quanto a algumas importantes características para a atividade da forense computacional – a classificação foi feita através da pesquisa por informações em sites oficiais de desenvolvedores e fornecedores. No campo “GUI”, é sinalizado se há uma interface gráfica para o usuário interagir com a ferramenta. No campo “Multiplataforma”, é sinalizado se a técnica ou ferramenta pode ser utilizada em diversos sistemas operacionais, isto é, se a ferramenta não é exclusiva de um determinado sistema. No campo “*Open Source”,* é sinalizado se a versão completa da ferramenta, além de ser “*Open Source”,* é disponibilizada de forma totalmente gratuita. No campo “Suporte”, a técnica ou ferramenta é classificada, de forma cumulativa, de acordo com o nível de suporte que é oferecido. Uma classificação nível um (“**+**”), significa que o desenvolvedor oferece suporte através de documentação ou contato – através de *e-mail* ou telefone, por exemplo. Uma classificação nível dois (“**++**”), significa que há suporte através de fóruns de discussão ou *blogs*, ou então que há atualizações periódicas com notícias e promoção de cursos para o aperfeiçoamento do uso da ferramenta. Uma classificação nível três (“**+++**”), significa que há suporte disponível em língua portuguesa, seja pelo desenvolvedor, seja por fóruns de discussão ou *blogs* brasileiros.

### 2.4.3 Comparativo entre as principais técnicas e ferramentas para análise

| **Família** | **Tipo** | **Nome** | **GUI** | **Multi plataforma** | ***Open Source*** | **Suporte** |
|---|---|---|---|---|---|---|
| Análise de dispositivos de armazenamento | Técnicas úteis na análise de arquivos | Known File Filter | | ✔ | | **+** |
| | | Pesquisas por palavras-chave | | ✔ | | **+** |
| | | Navegação pelo sistema de arquivos | | ✔ | | **+** |
| | | Visualização adequada de arquivos | | ✔ | | **+** |
| | | Virtualização | | ✔ | | **+** |
| | *Software para análise de arquivos* | Forensic ToolKit (*FTK*) | ✔ | *Windows* | | **++** |
| | | Encase | ✔ | *Windows* | | **++** |
| | | VMWare | ✔ | ✔ | | **+++** |
| | | VirtualBox | ✔ | ✔ | ✔ | **+++** |
| Análise de tráfego de rede | Técnicas úteis na análise de pacotes | *Pattern matching* | | ✔ | | **+** |
| | | *Packet Filtering* | | ✔ | | **+** |
| | *Software para captura ou análise de pacotes* | *Wireshark* | ✔ | ✔ | ✔ | **+++** |
| | | *tcpdump* | | *Linux* | ✔ | **+++** |

Quadro 5 – Comparativo de técnicas e ferramentas para análise
Fonte: do Autor.

# 3 ESTUDO DE CASO

O objetivo deste capítulo é verificar, através de um cenário hipotético, a aplicabilidade prática das etapas de coleta, extração e análise do processo forense e de algumas técnicas e ferramentas descritas no Capítulo 2.

## 3.1 Justificativa e cenário proposto

A computação forense tem como questão principal a identificação e o processamento de evidências digitais em provas materiais de um crime (ELEUTÉRIO; MACHADO, 2011). De acordo com Eleutério e Machado (2011), os exames periciais em dispositivos de armazenamento computacional são os mais solicitados na computação forense. Nesse sentido, o estudo de caso será realizado sobre um cenário hipotético em que a realização desse tipo de exame seja relevante.

Segundo os artigos 241-A e 241-B do Estatuto da Criança e do Adolescente (BRASIL-B, 2015), são crimes em espécie (dentre outras condutas): disponibilizar, transmitir, possuir ou armazenar, por qualquer meio, inclusive por meio de informática, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

No cenário proposto, obviamente, não há arquivo nem qualquer outra forma de registro ligado à pornografia infantojuvenil. Assim, será considerado ilegal a disponibilização, a transmissão ou o armazenamento de imagens ou vídeos que contenham explicitamente cenas de árvores.

Em outras palavras, há um determinado computador (com diversos arquivos e programas instalados), de um suposto infrator, que foi encontrado ligado e precisa ser periciado. A partir da aplicação das etapas do processo forense e da análise dos dados presentes na memória volátil e no disco rígido, os seguintes quesitos deverão ser respondidos: havia arquivos ilegais (fotos ou vídeos de árvores) armazenados? Os referidos arquivos estavam disponíveis para compartilhamento ou transmissão?

Para a realização da perícia serão aplicadas as quatro etapas do processo forense (coleta, extração, análise e apresentação), assim como algumas ferramentas em *software*, entre elas a distribuição *CAINE*, que proporciona um ambiente amigável para a realização de exames periciais.

## 3.2 Metodologia

O estudo de caso envolverá dados de memória e de disco. Serão realizadas, de forma prática, as etapas de coleta, extração e análise do processo forense (KENT et al., 2006), sendo apresentadas de forma cronológica em subcapítulos. Algumas ferramentas em *software* serão utilizadas e ilustradas através de figuras.

## 3.3 Processo forense nos dados da memória

A seguir, são apresentados os procedimentos e os *softwares* utilizados durante os exames forenses nos dados da memória do computador investigado.

### 3.3.1 Coleta

Será realizada, neste primeiro momento, a coleta dos dados contidos na memória RAM do computador investigado. *SoftwAres* específicos serão utilizados para garantir a geração de uma cópia fiel e a correta preservação dos dados.

O primeiro passo da perícia é realizar a captura dos dados presentes na memória RAM do computador investigado. No cenário em estudo, o computador a ser investigado foi encontrado ligado e será chamado de *netDesktop*. A Figura 13 ilustra o processo de criação do *dump* de memória, que foi realizado e salvo (como *NETDESKTOP-20150526-124458.RAW)* em um *pen drive* que continha a ferramenta DumpIt.

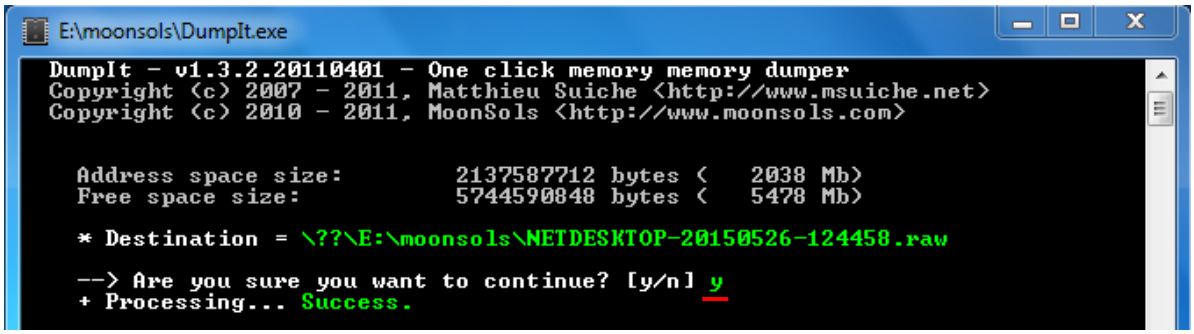


Figura 13 – Criação do d*ump* de memória
Fonte: do Autor.

Foi possível perceber que o *software* DumpIt realiza o processo de *dump* de forma bastante automatizada, requisitando apenas uma confirmação (sublinhada em vermelho) para iniciar o processo de captura.

Depois de realizada a captura dos dados da memória, o fornecimento de energia ao computador investigado foi cortado e o disco rígido, apreendido. O arquivo de *dump NETDESKTOP-20150526-124458.RAW* (salvo em um *pen drive*) e o disco rígido são considerados como materiais originais apreendidos e, portanto, devem ser preservados.

Nesse sentido, todos os demais procedimentos envolvendo os dados da memória ou do disco serão realizados em um ambiente controlado e seguro, que preserve a integridade dos dados envolvidos na investigação e disponibilize ferramentas adequadas para os exames forenses. A Figura 14 apresenta o ambiente de trabalho do sistema que foi utilizado: *CAINE*, uma distribuição *Linux* que oferece diversas ferramentas para atividades forenses.


Figura 14 – Ambiente de trabalho *CAINE*
Fonte: do Autor.

O próximo passo é realizar uma cópia fiel e garantir a correta preservação dos dados presentes nos materiais apreendidos. A Figura 15 apresenta, em três

passos sublinhados em vermelho, o procedimento de cópia do arquivo de *dump* de memória para um diretório do *CAINE* e a geração de valores *hash*, tanto para o arquivo original quanto para sua cópia.

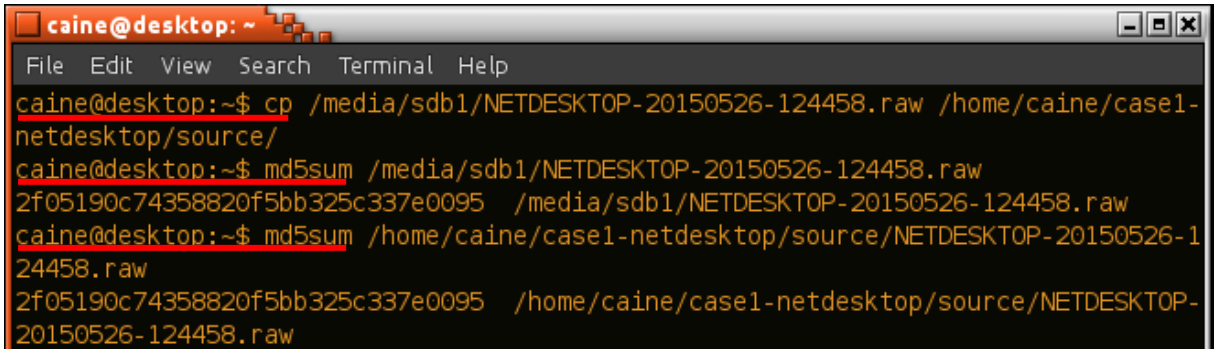

Figura 15 – Cópia e geração de *hash* do *dump* de memória
Fonte: do Autor.

É possível notar que, através do programa md5sum (*software open source* utilizado para verificação de integridade de dados através de *hash* criptográfico MD5 de 128 *bits*), foram gerados valores *hash* idênticos, tanto para o arquivo original quanto para sua cópia. Com a comparação dos valores é possível confirmar que a integridade do arquivo foi mantida após o processo.

Para encerrar a etapa de coleta de dados da memória, o material original (*pen drive* contendo o arquivo de *dump* de memória) foi lacrado e guardado. As demais etapas e procedimentos forenses serão aplicados sobre o arquivo cópia, armazenado em um diretório do *CAINE*. Posteriormente, uma nova comparação será realizada para verificar a inalterabilidade desse arquivo.

### 3.3.2 Extração

O objetivo desta etapa é reunir informações, através da extração de dados do *dump* de memória, que possam ser úteis para a perícia. Para isso, será utilizada a ferramenta Volatility, *software open source* e multiplataforma capaz de extrair informações sobre os processos em execução, as conexões de rede e os arquivos em uso.

A Figura 16 apresenta, em quatro passos sublinhados em vemelho, os procedimentos realizados para extrair algumas informações úteis do arquivo de *dump.* No primeiro passo, a opção *imageinfo* foi utilizada para verificar qual sistema

operacional era utilizado pelo computador investigado. No campo *Suggested Profile(s),* a ferramenta sugere o sistema operacional que era utilizado pelo computador investigado. A sugestão dada pela ferramenta foi necessária e utilizada como parâmetro (*--profile=Win7SP1x86)* nos outros passos realizados.

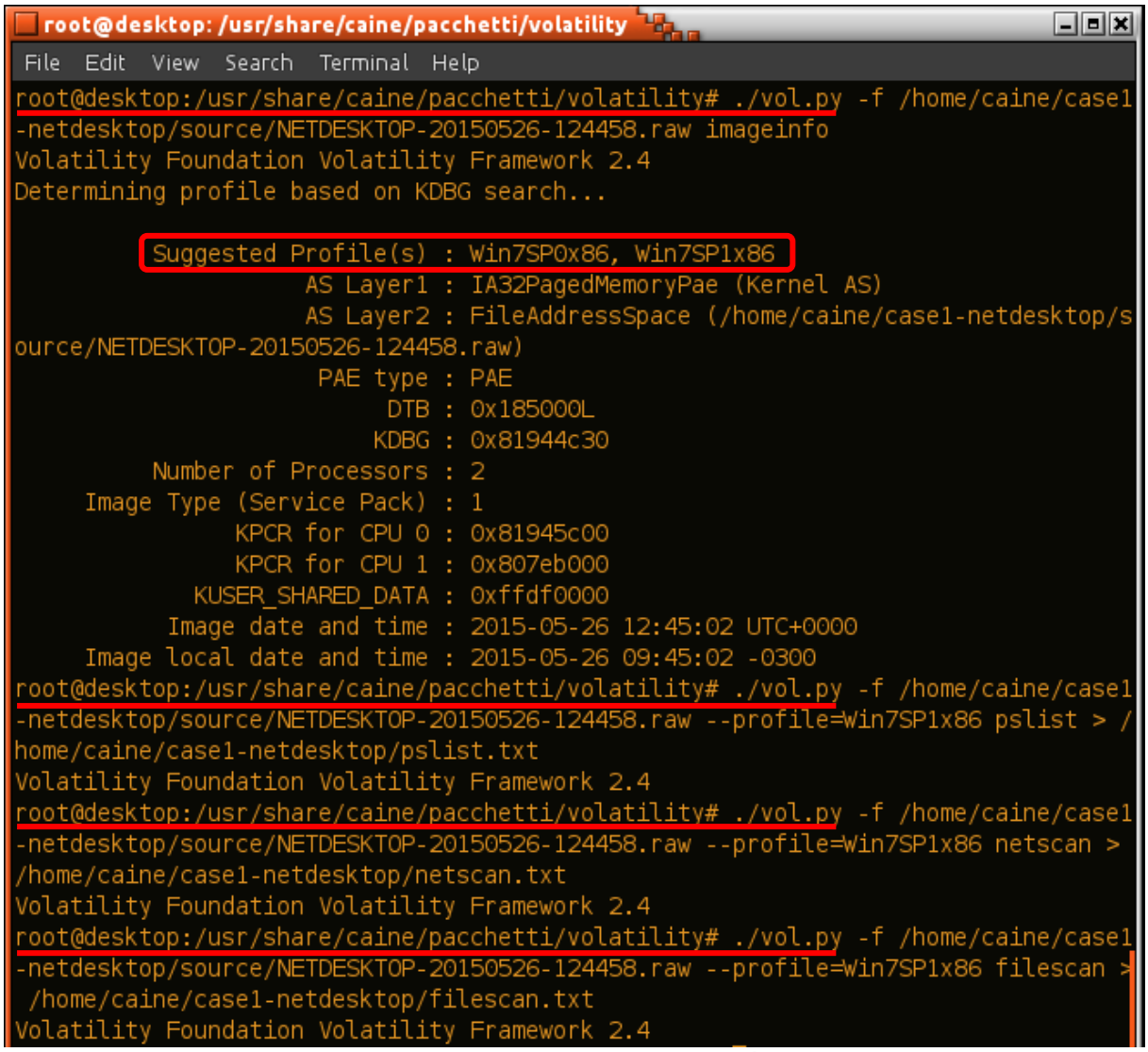

Figura 16 – Extração de informações do *dump* de memória
Fonte: do Autor.

No segundo passo, foi extraída (e salva para posterior análise em *pslist.txt*) uma lista dos processos que estavam sendo executados através da opção *pslist*. No terceiro passo, foram extraídas e salvas informações sobre as conexões de rede ativas através da opção *netscan*. No quarto passo, foram extraídas e salvas informações sobre os arquivos que estavam em uso através da opção *filescan*.

A próxima etapa da perícia forense é realizar a análise dessas informações.

### 3.3.3 Análise

Nesta etapa serão analisadas as informações anteriormente extraídas do arquivo de *dump.* O objetivo é verificar se existem informações que tenham relação com o fato investigado e responder aos quesitos inicialmente levantados: havia arquivos ilegais (fotos ou vídeos de árvores) armazenados? Os referidos arquivos estavam disponíveis para compartilhamento ou transmissão?

No que tange ao segundo quesito, a existência de uma forma de compartilhamento de dados ou até de uma conexão com a internet, por exemplo, são meios necessários para uma transmissão ou um compartilhamento de arquivos. A análise dos dados de memória pelo perito permite que seja verificada a existência ou não desses meios.

A primeira análise foi realizada sobre o arquivo *pslist.txt*. Nesse arquivo, foram buscados processos relacionados a programas de compartilhamento de arquivos, como *Ares*, *eMule*, *LimeWire*, entre outros. Na Figura 17 é possível perceber que, em uma das buscas realizadas (sublinhado em vermelho), o processo *Ares.exe* (provavelmente relacionado ao programa *Ares*) foi encontrado dentre os processos que estavam em execução no computador investigado.

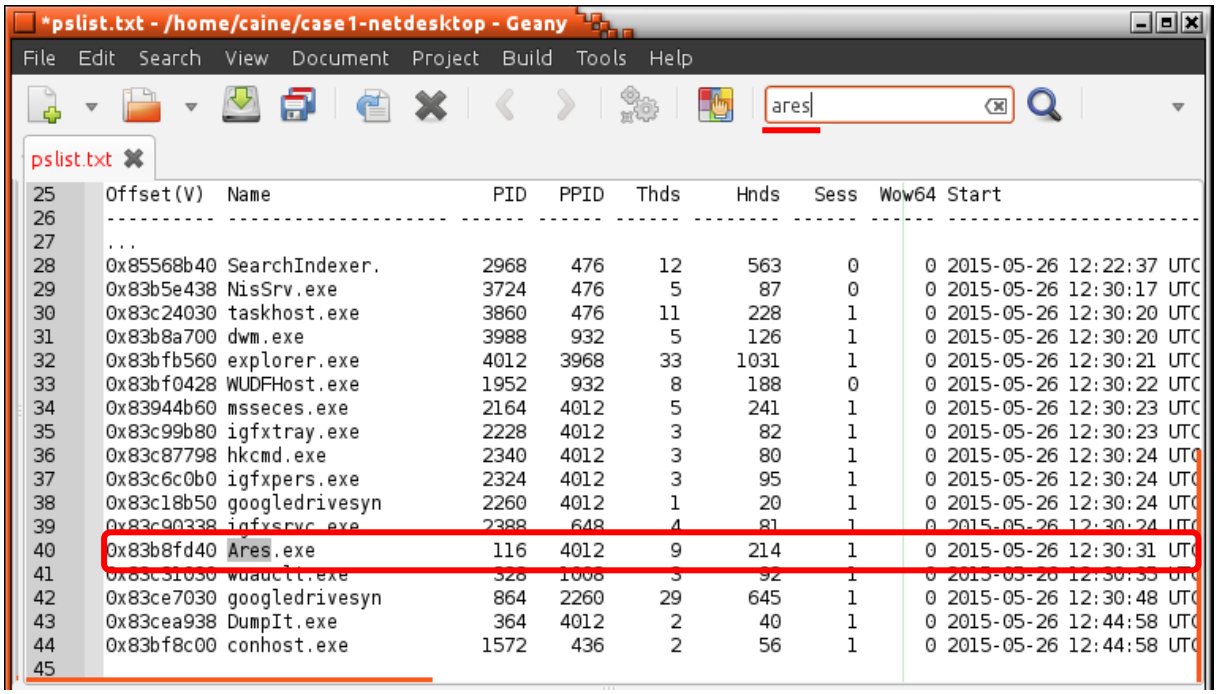


Figura 17 – Análise dos processos que estavam em execução
Fonte: do Autor.

Na Figura 18 é ilustrada a segunda análise, realizada sobre o arquivo *netscan.txt*. Através da busca (sublinhado em vermelho) pelo padrão *Ares*, foi possível perceber que havia algumas conexões de rede relacionadas ao processo *Ares.exe*, dentre elas diversas conexões estabelecidas com diferentes IP's.

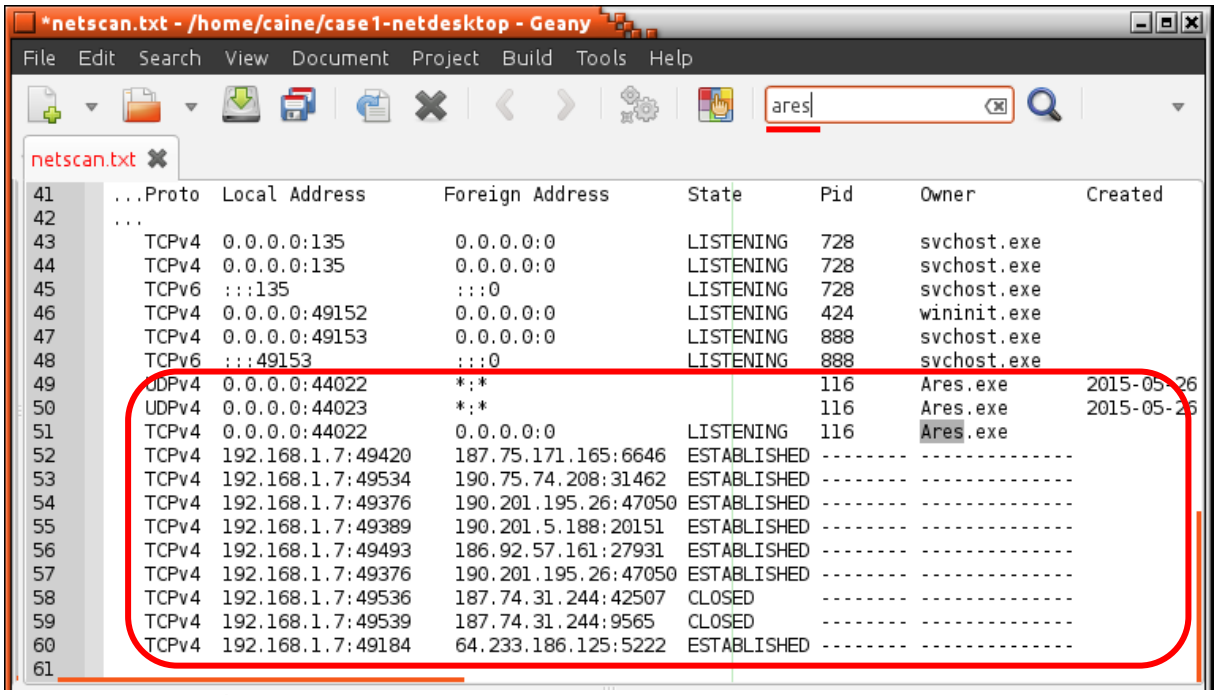


Figura 18 – Análise das conexões de rede
Fonte: do Autor.

A partir dos indícios existentes (processo *Ares.exe* em execução a conexões de rede relacionadas a esse processo), foram buscadas no site do desenvolvedor algumas informações a respeito do programa de compartilhamento de arquivo chamado *Ares*. Na documentação correspondente ao processo de instalação desse *software,* foi encontrado que a pasta utilizada por padrão para compartilhar arquivos é denominada como *My Shared Folder*, normalmente localizada no diretório do usuário do sistema.

A terceira e última análise de dados de memória foi realizada sobre o arquivo *filescan.txt* (arquivo que contém a lista dos arquivos que estavam em uso no momento da geração do *dump*, seja por processos em segundo plano, seja por programas utilizados pelo usuário).

Na Figura 19 é ilustrada uma busca (sublinhada em vermelho) pelo padrão *my shared folder*. É possível notar que o padrão foi encontrado: havia um ou mais arquivos dessa pasta que estavam em uso.

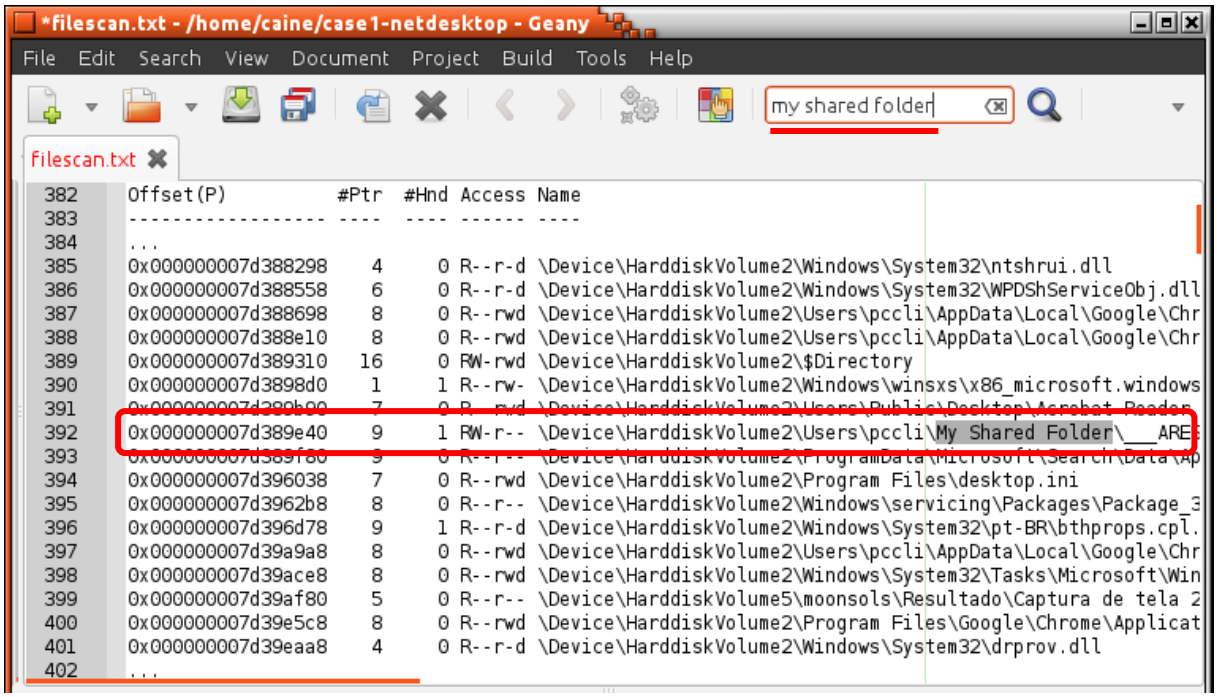

Figura 19 – Análise dos arquivos em uso
Fonte: do Autor.

Na Figura 19 é possível perceber ainda que a pasta que é usada por padrão para o compartilhamento de arquivos está localizada no diretório do usuário *pccli.*

Essas e outras informações levantadas pela perícia nos exames envolvendo dados da memória RAM poderão ser utilizadas nas próximas etapas, agora envolvendo dados do disco rígido.

### 3.4 Processo forense nos dados do disco

Serão apresentados, neste subcapítulo, os procedimentos e os *softwares* utilizados (todos *open source* e presentes no *CAINE*, sistema utilizado para realizar os exames forenses) durante as três primeiras etapas periciais envolvendo os dados do disco rígido do computador investigado. A etapa de apresentação ou documentação dos resultados obtidos pela perícia será discutida em subcapítulo próprio, ao final dos exames envolvendo dados de disco.

### 3.4.1 Coleta

A etapa de coleta envolvendo dispositivos de armazenamento foi iniciada (após romper o fornecimento de energia) com a retirada e a apreensão do disco rígido do computador investigado. O próximo passo é realizar uma cópia fiel e segura (garantindo a inalterabilidade) dos dados contidos nesse disco.

A Figura 20 ilustra o processo de montagem do disco apreendido com o uso do *Mounter* – *software open source* que permite o acesso a *pen drives* ou a discos de forma somente leitura.

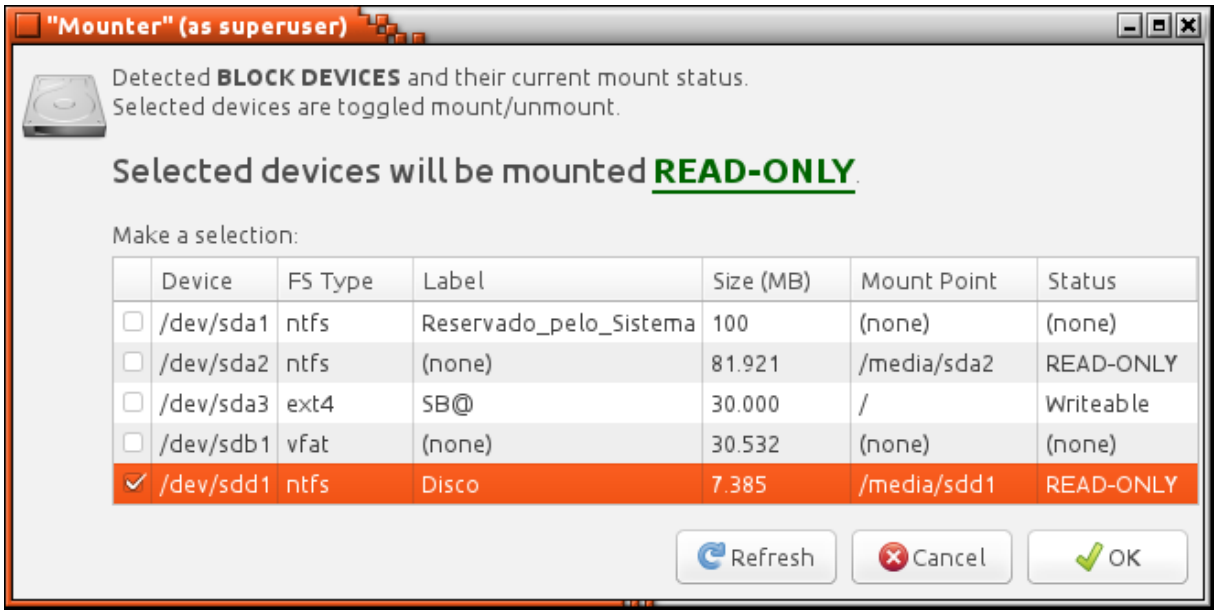

Figura 20 – Montagem do disco de forma somente leitura
Fonte: do Autor.

A montagem de forma somente leitura evita que o sistema operacional ou o perito (por um descuido, por exemplo) realize qualquer procedimento de gravação de dados, alterando ou até invalidando o material apreendido. O próximo passo é criar uma cópia fiel e segura do disco.

Na Figura 21 é ilustrado o procedimento (sublinhado em vermelho) para geração dessa cópia. Através da ferramenta em *software DC3DD*, foi possível gerar uma cópia fidedigna, que foi salva no formato de imagem de disco em um diretório do *CAINE*. O *software* apresenta em tempo real (demarcado em vermelho), dentre outras informações, a quantidade de *bytes* copiados, o progresso, o tempo demandado e a velocidade média do processo. O parâmetro *hash=md5* foi utilizado

para gerar o código *hash* do disco original (apresentado e demarcado em vermelho) para posteriores verificações de integridade e de inalterabilidade dos dados.

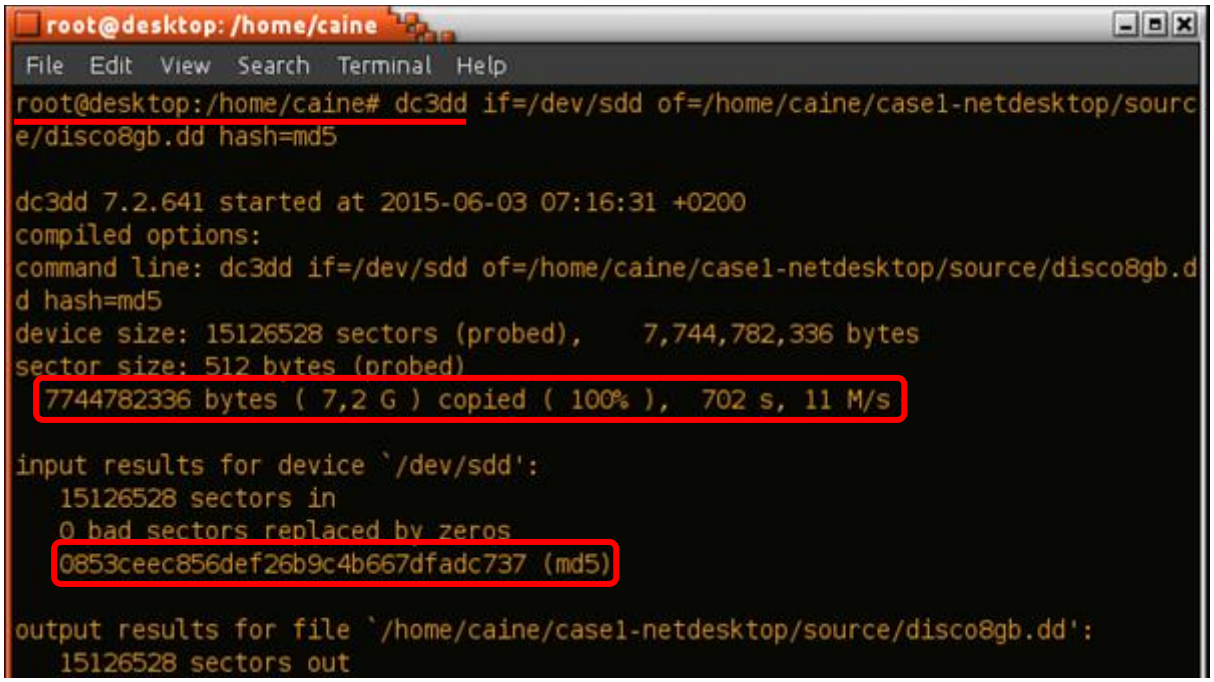

Figura 21 – Criação da imagem do disco apreendido
Fonte: do Autor.

Depois do processo de cópia, a etapa de coleta é encerrada com o disco rígido originalmente apreendido sendo lacrado e guardado. As próximas etapas da perícia serão realizadas sobre a sua imagem, salva como *disco8gb.dd*.

### 3.4.2 Extração

Na etapa de extração envolvendo dados de dispositivos de armazenamento, são recuperados arquivos e informações que sejam relevantes para a perícia ou que tenham relação com o fato investigado.

Nesse sentido, considerando que um dos quesitos inicialmente levantados diz respeito à existência ou não de arquivos ilegais armazenados no computador investigado, a extração será realizada e acordo com este preceito.

Na Figura 22 são apresentados, de forma ilustrativa, alguns procedimentos de extração realizados através da ferramenta *Autopsy*, *software* que permite o acesso e a extração de arquivos contidos em uma imagem de disco. Através da busca utilizando a expressão regular *.jpg|.mp4|.zip (sublinhada em vermelho)* foi

possível encontrar arquivos de imagem, de vídeo e comprimidos (demarcados em vermelho no centro da figura) que podem ter relação ao fato investigado. As letras em vermelho são utilizadas pelo programa para sinalizar os arquivos apagados.

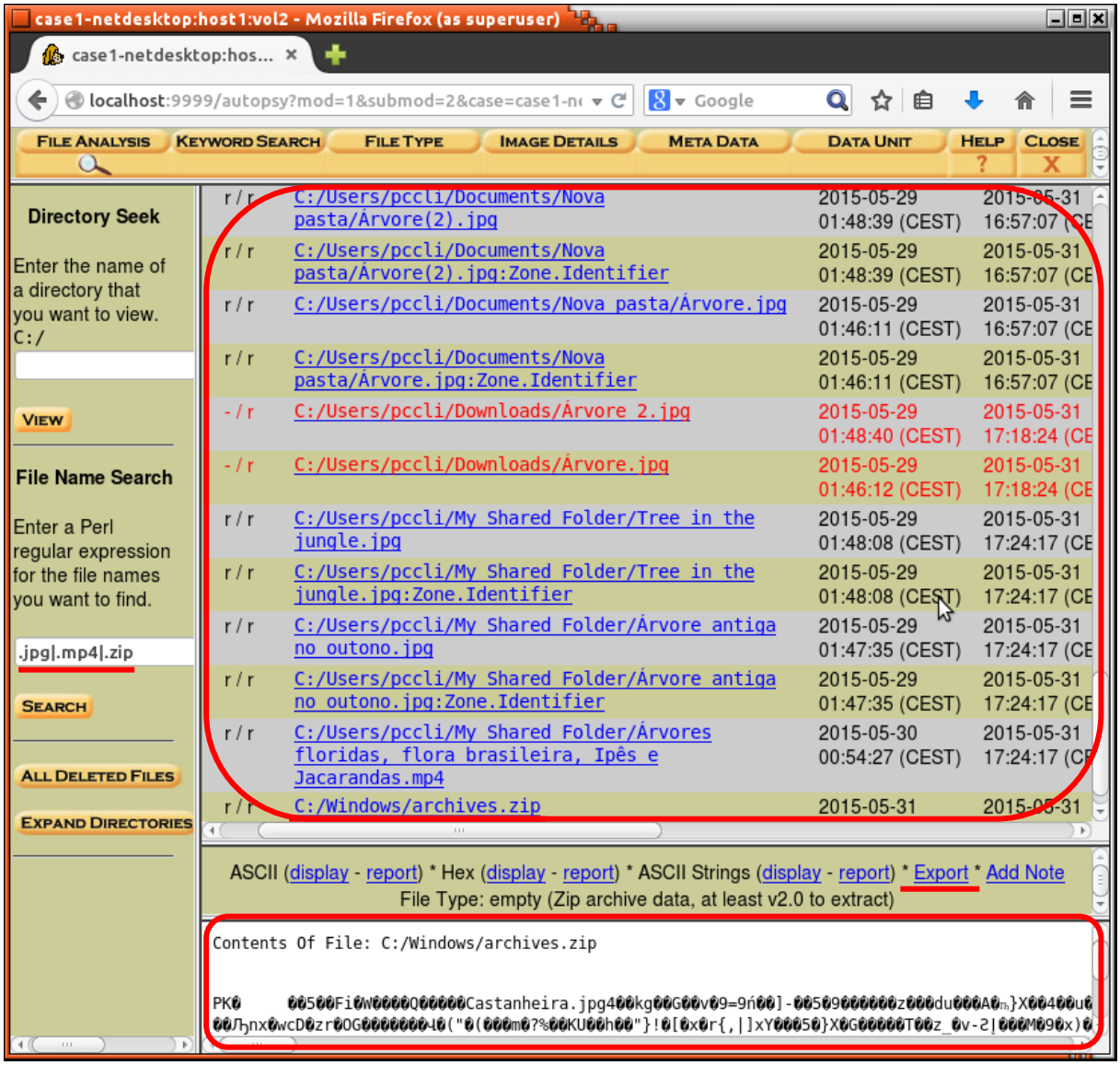


Figura 22 – Busca e extração de arquivos com a ferramenta *Autopsy*
Fonte: do Autor.

É possível perceber que, embora a ferramenta ofereça um espaço para uma pré-visualização (demarcado em vermelho na parte inferior da Figura 22), nem todos os formatos de arquivo são suportados. Assim, a opção *Export* (sublinhada em vermelho) foi utilizada para exportar os arquivos de interesse (inclusive os apagados) para outro diretório do *CAINE*.

A Figura 23 apresenta o conteúdo de *Export*, diretório que contém os arquivos de interesse que foram exportados através da ferramenta *Autopsy*. É possível notar que a localização original do arquivo e sua extensão fazem parte do seu nome.

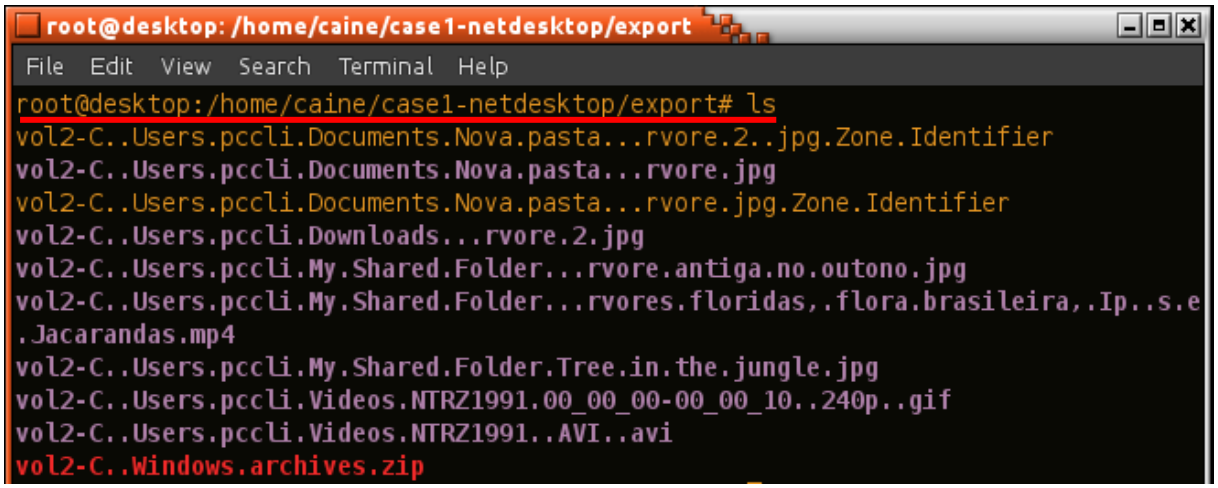

Figura 23 – Arquivos de interesse da perícia
Fonte: do Autor.

Dentre os arquivos apresentados pela Figura 23, além de alguns com nomes bastante sugestivos, o último arquivo (com nome em vermelho e em formato *zip*) chamou a atenção. Conforme o seu nome, ele estava armazenado no diretório *Windows*, com o nome *archives* e comprimido em formato *zip*. Ao acessá-lo foi verificado que havia arquivos protegidos por senha.

O próximo procedimento de extração é recuperar esses arquivos protegidos, pois eles podem conter informações relevantes para a perícia. Para isso, foi utilizado o *software John the Ripper*. A Figura 24 apresenta os dois passos (sublinhados em vermelho) realizados para a descoberta da senha.

No primeiro passo, o utilitário *zip2john* (presente na ferramenta *John the Ripper*) foi aplicado sobre o arquivo protegido para gerar um *hash* de senha que, então, foi salvo em um diretório do *CAINE*. No segundo passo, o *John* foi aplicado sobre o *hash* de senhas. Além disso, o parâmetro *–wordlist* foi usado para definir um dicionário de senhas (uma lista com algumas milh*Ares* de senhas mais usadas). Assim, após executada, a ferramenta testa as senhas uma-a-uma para verificar qual ou quais são compatíveis com o *hash* de senhas. Este método de descoberta de

senhas é conhecido como ataque de dicionário. É possível notar que a ferramenta encontrou a senha que protegia os arquivos (demarcada em vermelho).

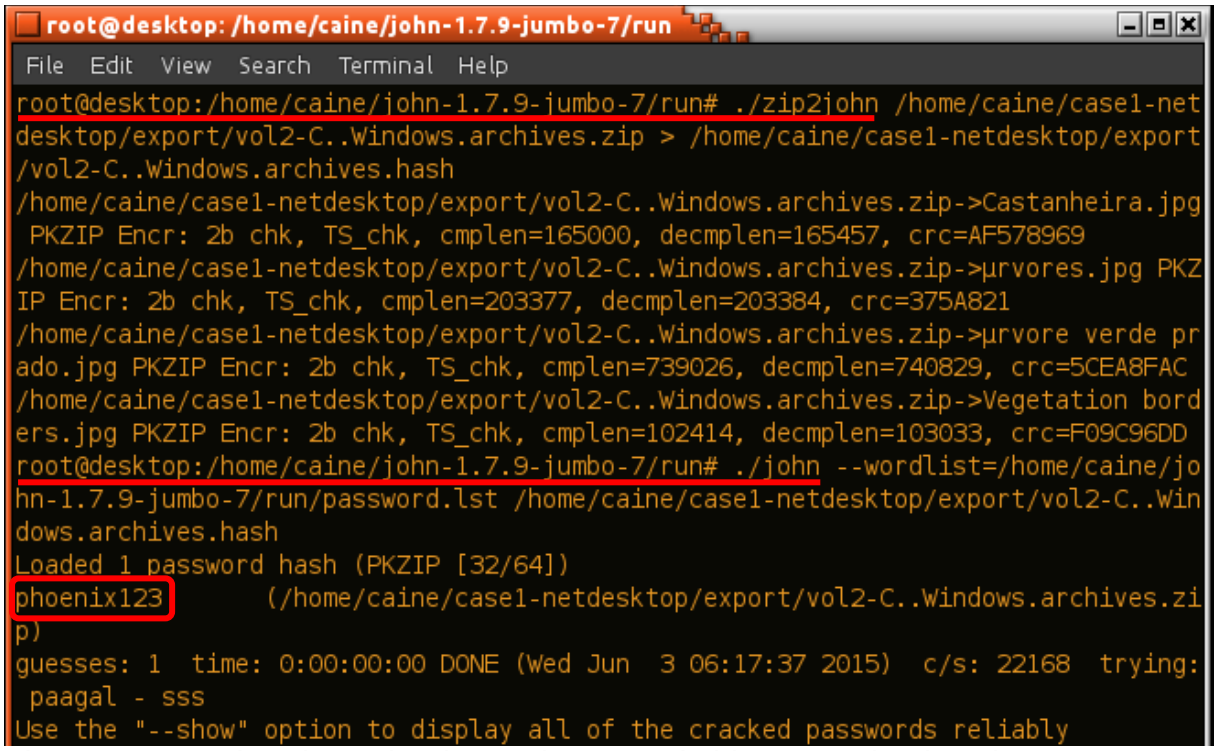

Figura 24 – Quebra da senha do arquivo comprimido com *John the Ripper*
Fonte: do Autor.

Na Figura 25 é apresentado o procedimento de extração (sublinhado em vermelho) dos arquivos protegidos. A senha utilizada foi *phoenix123*. Eram quatro arquivos que estavam protegidos por senha. Todos foram extraídos para o diretório de arquivos relevantes para a perícia.

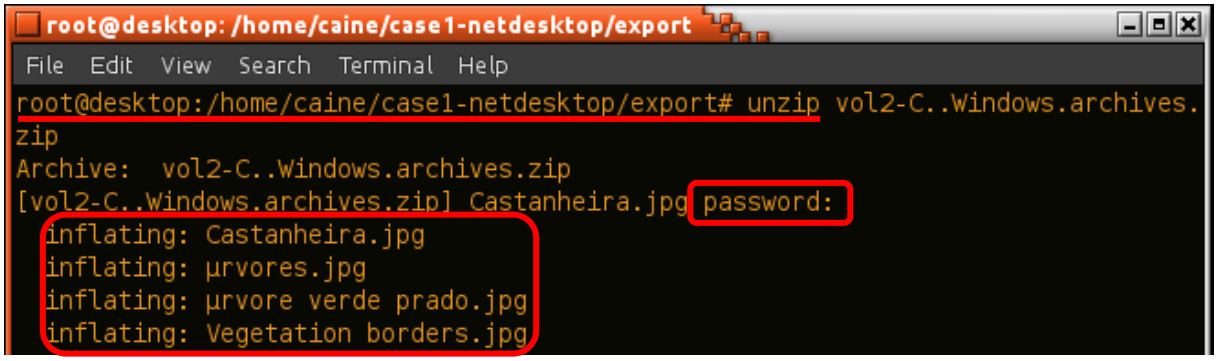

Figura 25 – Extração dos arquivos protegidos
Fonte: do Autor.

### 3.4.3 Análise

Na Figura 26 foram demarcados em vermelho os arquivos de imagem e de vídeo que tinham relação com o fato investigado (cenas explícitas de árvores). Seus nomes indicam as pastas onde estavam salvos, entre elas: *Documents, Downloads* e *My Shared Folder*. Cabe ressaltar que havia três arquivos nessa última pasta. Com isso, estavam disponíveis para compartilhamento pelo software *Ares*.

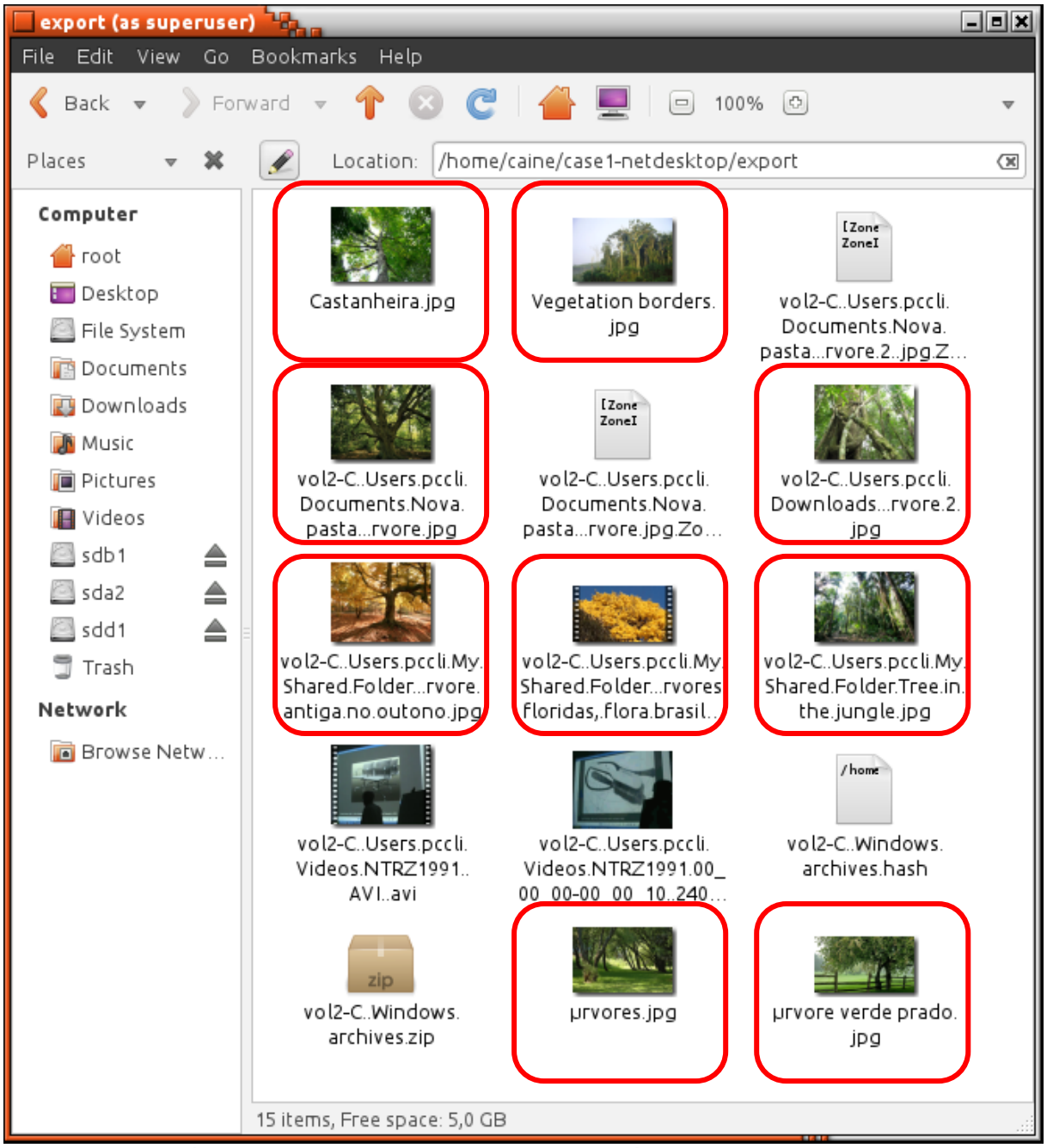


Figura 26 – Análise dos arquivos de imagem e de vídeo
Fonte: do Autor.

Para preservar a integridade dos arquivos analisados e verificar a inalterabilidade da imagem do disco apreendido e da cópia do *dump* de memória, (fontes utilizadas para os exames forenses) foram gerados valores *hash*, ilustradas nas Figuras 27, 28 e 29.

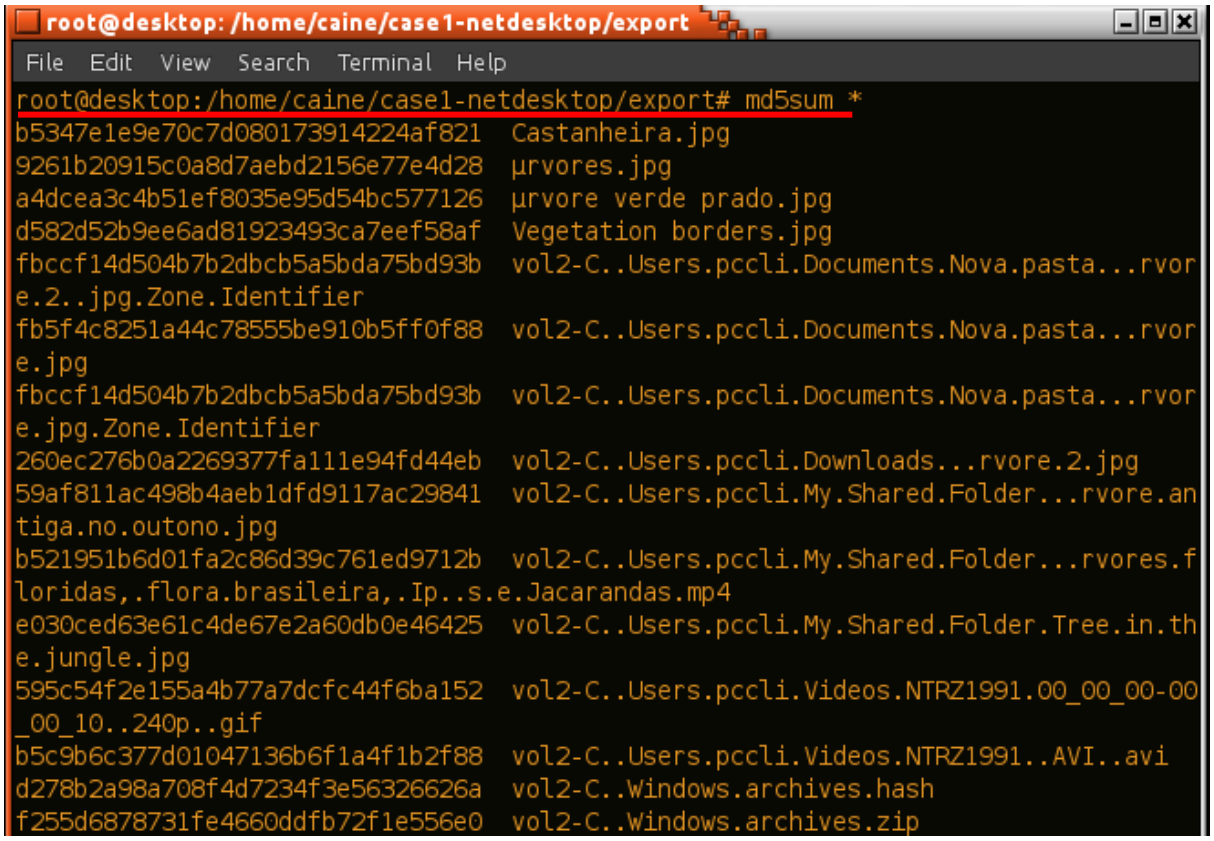


Figura 27 – Geração de *hash* para os arquivos analisados
Fonte: do Autor.

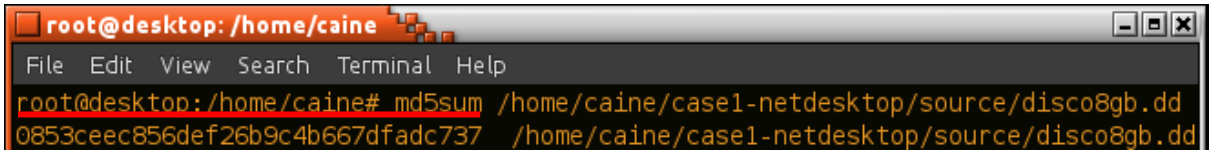


Figura 28 – Geração de *hash* para a imagem do disco
Fonte: do Autor.

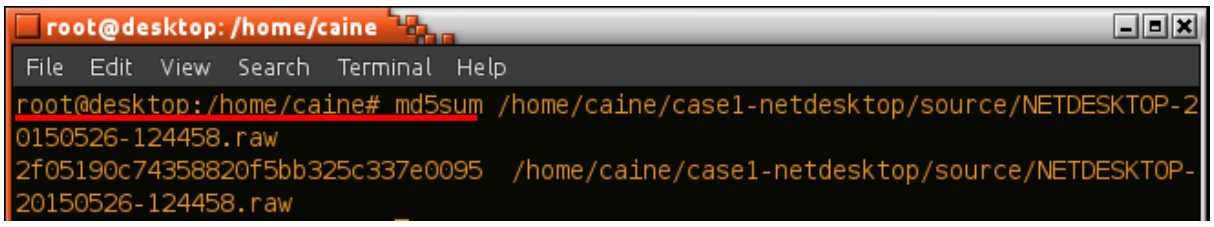


Figura 29 – Geração de *hash* para o *dump* de memória
Fonte: do Autor.

### 3.4.4 Apresentação

No Quadro 6 é apresentado um modelo exemplificado do relatório citado na seção 2.1.4.

(continua)

| Preâmbulo | Laudo Técnico Pericial – Caso 1 (NETDESKTOP) |
|---|---|
| Histórico | Há um determinado computador (com diversos arquivos e programas instalados) que precisa ser periciado. Após a realização da perícia, os seguintes quesitos devem ser respondidos:<br>Havia arquivos ilegais (fotos/vídeos de árvores) armazenados?<br>Os referidos arquivos estavam disponíveis para compartilhamento ou transmissão? |
| Material original/ apreendido | Um *pen drive* da marca *SanDisk* (nº de série 8H1112VWGB), com capacidade de 4GB, contendo um arquivo de *dump* da memória volátil do computador investigado.<br>Nome do arquivo gerado: NETDESKTOP-20150526-124458.raw<br>Valor do *hash* MD5: 2f05190c74358820f5bb325c337e0095<br><br>Um disco rígido da marca Hitachi (nº de série 081224BB6B04WFJXLXVL), com capacidade de 80GB, apreendido do computador investigado.<br>Nome do arquivo gerado: disco8gb.dd<br>Valor do *hash* MD5: 0853ceec856def26b9c4b667dfadc737 |
| Objetivo | Identificar e recuperar possíveis evidências digitais, como fotos ou vídeos contendo cenas explícitas de árvores;<br>Verificar se esses arquivos estavam sendo compartilhados ou disponíveis para compartilhamento;<br>Preservar a integridade dos materiais periciados, garantindo a inalterabilidade dos dados;<br>Apresentar os resultados obtidos à autoridade requisitante. |

(continuação)

| | |
|---|---|
| Considerações técnicas | Um arquivo de *dump* de memória contém todos os dados da memória RAM (memória volátil) de um sistema computacional. Através da análise dos dados da memória, é possível verificar os programas que estavam em execução, os arquivos que estavam em uso pelo usuário ou pelo sistema, as conexões abertas, etc.<br><br>Um valor de *hash* é uma sequência de *bits* gerada por uma função matemática que resume, de forma unidirecional, um arquivo ou uma informação. Valores de *hash* são calculados através de algoritmos (como MD5, por exemplo) para verificar a inalterabilidade de arquivos. |
| Exames | A primeira atividade da perícia foi realizar a coleta de prováveis fontes de evidências digitais. O conteúdo da memória volátil e o disco rígido do computador investigado foram apreendidos e duplicados através de *softwares* de duplicação forense. Os materiais originais foram lacrados e preservados. Os demais procedimentos da perícia foram realizados sobre as cópias dos materiais. Valores de *hash* foram gerados para verificar a inalterabilidade dos dados contidos nos materiais e nas cópias.<br><br>A segunda atividade da perícia foi realizar a extração de dados da memória e do disco. Informações e arquivos que provavelmente tinham relação com o fato investigado foram recuperados através de *softwares* específicos.<br><br>A terceira atividade da perícia foi analisar as informações e os arquivos recuperados, de forma a responder aos quesitos inicialmente levantados. |
| Respostas aos quesitos | 1. Havia arquivos ilegais (fotos/vídeos de árvores) armazenados?<br>Havia oito fotos e um vídeo armazenado no computador investigado, todos contendo cena explícita de árvores. |

(conclusão)

| | |
|---|---|
| | 2. Os referidos arquivos estavam disponíveis para compartilhamento ou transmissão?<br>Dentre os referidos arquivos, havia duas fotos e um vídeo disponível para compartilhamento ou transmissão através de um *software* de compartilhamento de arquivos, o qual estava em execução no momento da apreensão. |

Quadro 6 – Relatório básico da perícia
Fonte: do Autor.

## 4 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Neste trabalho foi possível observar, através da pesquisa na literatura relacionada ao assunto, as quatro etapas que normalmente são realizadas em uma atividade pericial envolvendo dispositivos de armazenamento ou tráfego de rede. Além disso, foram levantados alguns procedimentos e aspectos a serem observados, como volatilidade e relevância da preservação dos dados, durante a realização de exames forenses.

Foram discutidas e posteriormente apresentadas, através de tabelas comparativas, as principais técnicas e ferramentas (em *hardware* e *software*) utilizadas para as fases da perícia. Critérios como quantidade de suporte oferecido foram utilizados para classificar as ferramentas.

Por fim, foi realizado um estudo de caso que, embora conduzido sobre um cenário controlado, permitiu a aplicação do processo forense, das técnicas e das ferramentas periciais apresentadas. No caso estudado, os exames periciais foram realizados manualmente. A análise de possíveis evidências foi feita de forma visual pelo perito. Embora tenha sido possível selecionar e filtrar o que se desejava analisar, a quantidade de arquivos e informações aumenta substancialmente em um cenário real, o que pode tornar a atividade de análise em um processo lento ou inviável.

Estudos futuros podem ser realizados contemplando ambientes mais complexos, em que a quantidade e a volatilidade das informações são fatores críticos. Em um ambiente de comunicação de rede, por exemplo, a análise automatizada das informações e dos pacotes trafegados pode ser um requisito básico para a atividade pericial. Outro aspecto relevante (que demanda o devido aprofundamento) diz respeito às questões legais, ou seja, das leis brasileiras que permeiam as atividades periciais.

Dada à amplitude e a multidisciplinariedade do tema, vale frisar que este trabalho não teve a pretensão de esgotar as possibilidades do assunto, mas sim colaborar através da apresentação de um modelo de roteiro pericial, de um rol exemplificativo de técnicas e ferramentas periciais e de um estudo de caso envolvendo dados de memória e de disco.

## REFERÊNCIAS


ACCESSDATA-A. ***Known File Filter*** **(KFF)**: installation guide 5.6. Disponível em: <www.ad-pdf.s3.amazonaws.com/KFF_Installation_Guide_5_6.pdf>. Acesso em 01 de maio de 2015.

ACCESSDATA-B. **Solutions in digital forensics.** Disponível em: <www.accessdata.com/solutions/digital-forensics/forensic-toolkit-*FTK*>. Acesso em 29 de abril de 2015.

ALMEIDA, R. N. **Perícia forense computacional:** estudo das técnicas utilizadas para coleta e análise de vestígios digitais. 48 f. Monografia (Graduação em Tecnologia em Processamento de Dados)–Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

BRASIL-A. **Código de Processo Penal.** Disponível em: <www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm>. Acesso em 22 de abril de 2015.

BRASIL-B. **Estatuto da Criança e do Adolescente.** Disponível em: <www.planalto.gov.br/CCIVIL_03/leis/L8069Compilado.htm>. Acesso em 16 de maio de 2015.

*CAINE*. COMPUTER FORENSICS *LINUX* DISTRO. **Computer Aided Investigative Environment**. Disponível em: <www.*CAINE*-live.net>. Acesso em 24 de março de 2015.

CERT. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES. **Cartilha de segurança para internet**. Disponível em: <www.cartilha.cert.br/ataques/>. Acesso em 05 de maio de 2015.

CERT. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES. **Estatísticas dos incidentes reportados ao CERT.br**. Disponível em: <www.cert.br/stats/incidentes/>. Acesso em 21 de agosto de 2014.

CGSECURITY. **Digital picture and file recovery:** *Photorec*. Disponível em: <www.cgsecurity.org/wiki/*Photorec*>. Acesso em 15 de abril de 2015.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense.** São Paulo: Novatec, 2011.

ERBACHER, R. F.; CHRISTIANSEN, K.; SUNDBERG, A. **Visual network forensic techniques and process.** In: ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE, 1., 2006, Albany. Proceedings of the 1 st. Annual Symposium on Information Assurance. Albany: University at Albany, 2006

*FDTK*-WIKI**. Centro de consulta sobre ferramentas de forense digital.** Disponível em: <www.*FDTK*.com.br/wiki/tiki-index.php>. Acesso em 29 de abril de 2015.

GALVÃO, R. K. M**. Introdução à análise forense em redes de computadores:** Conceitos, técnicas e ferramentas para “grampos digitais”. São Paulo: Novatec, 2013.

JUNIOR, C. C. N. M.; MOREIRA, J. **Roteiro investigativo em perícia forense computacional de redes:** estudo de caso**.** Departamento de Computação – Universidade Federal de São Carlos: São Carlos, 2014.

JUNIOR, A. P. C. et al. **Forense computacional em memória principal.** FATESG/SENAI, 2009.

KENT, K. et al. **Guide to integrating forensic techniques into incident response:** recomendations of the National Institute of Standards and Technology. Special publication. Gaithersburg: NIST, 2006.

LILLARD, T. et al. **Digital forensics for network, internet and cloud computing:** a forensic evidence guide for moving targets and data. Burlington: Syngress, 2010.

NETRESEC**. Network forensics and network security monitoring:** *NetworkMiner*. Disponível em: <www.netresec.com/?page=*NetworkMiner*>. Acesso em 02 de abril de 2015.

NMAP. **Nmap security scanner.** Disponível em: <www.nmap.org/>. Acesso em 04 de abril de 2015.

PINHEIRO, D. O. **Um estudo experimental das ferramentas de engenharia reversa aplicadas às vulnerabilidades do software.** 42 f. Monografia (Graduação em Sistemas de Informação)–Universidade Federal do Ceará, Quixadá, 2013.

PRIBERAM. **Dicionário da língua portuguesa.** Disponível em: <www.priberam.pt/dlpo/>. Acesso em 11 de maio de 2015.

QPERITO. **Blog sobre computação forense, e-discovery e direito digital:** queira o sr. perito detalhar o procedimento de cópia forense. Disponível em: <www.qperito.com/2013/11/08/queira-o-sr-perito-detalhar-o-procedimento-tecnico-para-realizacao-de-uma-copia-forense/>. Acesso em 06 de maio de 2015.

SILVA, V. A.; OLIVEIRA, C. H. **Análise de ferramentas livres para perícia forense computacional.** Caderno de Estudos Tecnológicos. Faculdade de Tecnologia de Ourinhos: São Paulo, 2014.

SINGH, O. Department of Computer Science and Engineering. Network Forensics. ISEA workshop on network traffic capturing & analysis, 2009. Disponível em: <www.iitg.ernet.in/cse/ISEA/isea_PPT/ISEA_02_09/NForensics-IIT%20Guwahati-21Feb2009OVS.pdf/>. Acesso em 01 de abril de 2015.

SOCIAL-ENGINEER. **Security through education.** Disponível em: <www.social-engineer.org>. Acesso em 22 de abril de 2015.

TECHBIZ. **Forense Digital:** duplicadores e bloqueadores de disco. Disponível em: <www.forensedigital.com.br/product/duplicador-forense-td2u/>. Acesso em 06 de maio de 2015.

VIRTUALBOX. **Full Virtualizer for x86 hardware.** Disponível em: <www.virtualbox.org/>. Acesso em 08 de maio de 2015.

WEYER, A. S. **Perícia computacional – ferramentas, técnicas disponíveis e estudo de caso.** Curso de Tecnologia em Redes de Computadores. Universidade Luterana do Brasil: Canoas, 2011.

*WIRESHARK*. ***Wireshark*** **Foundation.** Disponível em: <www.*Wireshark*.org>. Acesso em 07 de abril de 2015.