COMPUTAÇÃO FORENSE:
PROCEDIMENTOS TÉCNICOS E OPERACIONAIS

Autores

Jean Aleff Dorneles Borges - Nicholas Prado

jean_aleff@hotmail.com - nickprado@msn.com

Orientador

Antônio Manoel Batista da Silva

antonio.manoel@uniube.br

RESUMO

Crimes que ocorrem no meio da computação, deixam vestígios em forma de dados, sendo encontrados em diversos dispositivos de armazenamento ou de tráfegos em rede. Por utilizar-se de técnicas e procedimentos específicos, destina-se esse tipo de investigação aos peritos computacionais. Por meio deste trabalho, destacaremos as fases do processo de investigação forense, as técnicas utilizadas em cada etapa, como também as principais ferramentas e softwares periciais realizados na coleta, extração e análise de dados. Como proposta de efetivar esses procedimentos na prática, iremos realizar um estudo de caso verificando a aplicabilidade dos conceitos estudados neste trabalho.

Palavras-chave: Peritos computacionais; investigação forense; principais ferramentas; softwares periciais.

FORENSIC COMPUTING:
TECHNICAL AND OPERATIONAL PROCEDURES

ABSTRACT

Crimes that occur in computing tend to leave traces in the form of data found in multiple storage devices or network traffic. By using specific techniques and procedures, this type of investigation is intended for computer forensics specialists. Throughout this article, the steps of a forensic investigation procedure are going to be highlighted, as well as the techniques used in each step and the tools and forensic software used in the acquisition, extraction and data analysis. As a proposal to show how these procedures work in practice, a case study will be performed to verify the applicability of the concepts studied in this article.

Keywords: Computer forensics; forensic investigation; forensic tools; forensic software.

1. INTRODUÇÃO

Com seu rápido desenvolvimento, os aparelhos eletrônicos, celulares, computadores e meios de trafego de informações – hoje comumente chamada de “nuvem” – tornaram-se essenciais nas diversas atividades desempenhadas pelo ser humano, como também nas atividades criminosas e ilegais. Podemos citar crimes exequíveis atualmente como: roubos de identidade, pedofilia virtual, calúnia e difamação, ameaças, discriminação, espionagens, entre outros.

Como forma de provar a ocorrência desses crimes, a justiça requisita peritos computacionais para que analisem os computadores, celulares e equipamentos eletrônicos dos suspeitos e apurem se haviam suficientes indícios de materialidade e autoria, realizando assim, indiciamento dos criminosos. Estes peritos são de suma importância na solução de crimes virtuais, de modo que acessam e analisam às informações e dados em relação ao indivíduo indiciado, que podem se mostrar evidências digitais, de grande valor à investigação.

A computação forense examina toda forma de dispositivo computacional, identificando, preservando, recuperando e apresentando evidências digitais para classificação de crimes. A presença de uma forma de armazenamento, a memória, seja ela volátil ou não, nos dispositivos computacionais, sejam eles computadores, celulares, notebooks, câmeras e diversos outros, favorece a análise dos peritos. Para Junior e Moreira (2014), a computação forense consiste em um ramo que alia elementos jurídicos e computacionais, visando coletar e analisar informações de dispositivos e sistemas, possibilitando assim a apresentação de evidências no âmbito jurídico.

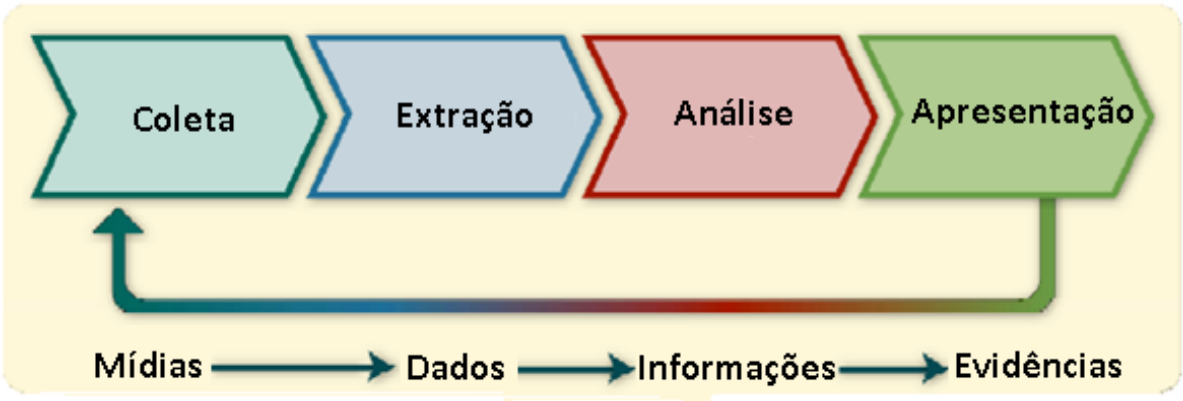
O objetivo geral deste trabalho de conclusão de curso é conceituar Perícia Forense Computacional e demonstrar os conceitos e técnicas das perícias computacionais, singularizando os métodos de aquisição, extração, análise e apresentação; utilizar da aplicação de softwares de perícia forense, visando resultados concisos para uma documentação objetiva dos fatos e verificar a aplicabilidade prática das etapas discutidas através de um estudo de caso, evidenciando a utilização das ferramentas e softwares periciais em dispositivos computacionais.

2. METODOLOGIA

A perícia computacional utiliza de procedimentos e técnicas para que seja realizada de forma concisa, tendo suas etapas estruturadas e obedecendo padrões específicos para não infringir a legislação.

O método de identificação é o princípio básico para deferimento da perícia e, a partir de então surgem as perguntas a serem respondidas por meio da investigação, que são denominados quesitos. Definimos em etapas o processo posterior, sendo fundamental para seu desenvolvimento, são elas: coleta, extração, análise e apresentação (KENT et al., 2006), apresentadas na Figura 1.

Figura 1 - Etapas do processo de perícia



Fonte: Adaptado de Kent et al. (2006)

2.1 Identificação

Inicia-se o processo de perícia com a ocorrência de um determinado crime e a constatação de informações digitais. A investigação forense vem por meio dessas informações, recriar a verdade diante dos acontecimentos. Assim, o examinador descobre a verdade expondo os vestígios deixados nos sistemas, visando formar uma trilha de auditoria, capaz de elucidar e averiguar possíveis atividades criminosas e/ou fraudulentas ligadas ao incidente.

Independente das circunstâncias, o processo subsequente é exercido após se estabelecer hipóteses, ou seja, perguntas-chave, que permitem estruturar o contexto de atuação da perícia. São elas: O que aconteceu? Por que aconteceu? Quando aconteceu? Como aconteceu? (ERBACHER; CHRISTIANSEN; SUNDBERG, 2006).

Essas questões são relacionadas, de forma geral, a todos os tipos de pericias computacionais.

2.2 Coleta

Nesta etapa, realiza-se a coleta de dispositivos que possam ser providos de evidências digitais ou relacionados com o caso investigado. Essa etapa deve ocorrer de forma rápida – se possível, instantes após o conhecimento do incidente – e sempre sendo seguidos os devidos procedimentos para preservar a integridade do material coletado. Para Kent et al. (2006), a etapa de coleta pode ser subdividida em aquisição, preservação e verificação de integridade dos dados.

> As duas atividades são interdependentes, principalmente pelo cuidado em tornar o processo auditável e reproduzível. De nada adianta coletar os dados se estes se perderem total ou parcialmente ou sofrerem modificações, perdendo seu valor como prova, ou, ainda, o trabalho ser questionado. (MADEIRA, 2012, p. 53).

Um trabalho feito pelo ACPO Good Practice Guide foi de extrema importância para a etapa de coleta, e é considerado como referência ao redor de todo o mundo. É um guia de boas práticas para pesquisa, apreensão e exame do vestígio eletrônico, sendo iniciado em 1997, no Reino Unido. Segundo ACPO (2012), esse guia estabelece quatro princípios essenciais para a abordagem no momento da apreensão e coleta de dados:

- **Princípio 1** – Nenhuma ação de algum agente encarregado de trabalhar na investigação pode modificar os dados contidos em um computador ou dispositivo a ser investigado.
- **Princípio 2** – No momento em que uma pessoa tem a necessidade de acessar o conteúdo original mantido no dispositivo, computador ou mídia, essa pessoa deve ser competente para tal e ser capaz de explicar a relevância e as implicações de suas ações.
- **Princípio 3** – Deve ser criado um registro de todos os passos da investigação. Um examinador independente deve ser capaz de usar esses passos e chegar aos mesmos resultados.
- **Princípio 4** – A pessoa a cargo da investigação tem a responsabilidade geral de assegurar que esses princípios sejam condizentes com os preceitos legais aplicáveis.

Esses quatros princípios indicam que o processo vai além da coleta dos vestígios, em direções que implicam na necessidade de rigor na coleta de dados e nas responsabilidades dos envolvidos.

2.2.1. Aquisição

Os principais fatores no momento da aquisição são:

- Volatilidade – dados que se perdem ao decorrer do tempo ou interrupções no sistema, por falta de energia ou por sobrecarga interna; fonte de valor probatório – com base em situações/ problemas anteriores, estipulam as fontes que contenham utilidade provável para a investigação;
- Dificuldade de aquisição – fontes de dados que demandam esforços de aquisição distintos, como registros de provedores e de roteadores, e que podem fornecer evidências de mesmos valores.

"Considerando o grau de volatilidade, define que esse fator é relacionado diretamente com o dispositivo de armazenamento computacional" (ELEUTÉRIO; MACHADO, 2011). Conseguimos definir características dos dispositivos mais comuns, sendo elas: fragilidade, facilidade de cópia e sensibilidade ao tempo de vida e de uso.

Por meio dos demais fatores, é possível priorizar as fontes mais relevantes para o momento da apreensão. Com a capacidade de interpretar as diferentes situações, o perito consegue realizar a aquisição de maneira mais rápida e eficaz, passando mais rápido para os processos subsequentes.

2.2.2. Preservação e verificação de integridade

Em uma investigação forense, na etapa de coleta, a preservação desses dados é crucial, objetivando que a aquisição não seja diferente da fonte original do material. É assim, dever do perito tomar providencias para realizar a idoneidade da prova e sua proteção, evitando questionamentos de autenticidade. Quando se opera com esses dados, independente de quão simples sejam, vale ressaltar cuidados especiais para não alterar significativas evidências e desprover seu valor.

Todas as cópias de dispositivos devem ser realizadas de forma fiel aos dados contidos no material original, utilizando-se de técnicas especificas para tal tarefa. Entre elas, e bastante utilizada pelos peritos, está o espelhamento de imagem. O espelhamento consiste em duplicação

de dados, feito bit a bit, de forma fiel ao material de origem, portanto, a unidade de destino deve ter igual capacidade ou mesmo superior ao original. Deve-se checar se o volume nominal é na realidade o volume real, pois existem vários dispositivos de fabricantes diferentes que afirmam conter determinado espaço de alojamento, quando na realidade é outro. Compara-se o número de setores de cada disco, cuja informação, denominada LBA (Logic Block Addressing), fica na etiqueta do fabricante.

> Logic Block Addressing, é uma organização lógica dos setores, utilizada nos discos rígidos atuais, que faz com que o computador enderece cada setor do disco sequencialmente, ao invés de usar localização física, como cilindro, cabeça e setor. Caso o dispositivo que receberá a cópia seja maior do que o original, é necessário garantir que todo o espaço remanescente esteja limpo, a fim de não sobrar resquícios de dados que possam ser confundidos durante os exames. Esse processo de limpeza é chamado de wipe e consiste em excluir um arquivo ou toda uma partição e gravar bytes na mesma área do disco, desta forma se houver algum software que faça a leitura binária do disco, este verá os dados recém gravados e não os originais (ALMEIDA, 2011).

A técnica de duplicação de discos por imagem é bastante semelhante ao espelhamento. Tem como finalidade a cópia de todo o sistema operacional e seus derivados para um arquivo de imagem, originando uma reprodução exata e fiel do disco (ALMEIDA, 2011). As vantagens são maiores em relação a técnica de espelhamento, pode-se realizar cópia do disco inteiro ou partições individuais, além do mais, caso o local de destino tenha espaço suficiente, podem ser copiados várias imagens de discos diferentes sem que haja interferência entre elas. Por serem arquivos de imagens, podem ser compactados, e assim, ter uma economia de espaço no disco de destino.

Para ter total integridade do material investigado, utilizam técnicas para que impeçam escritas nas cópias e não sofram alterações, definindo os discos para modos de somente leitura. Atualmente utilizam-se bastante os bloqueadores de escritas, hardwares utilizados por peritos que tem como função e garantia principal a inalterabilidade de dados.

Para obter uma garantia de que uma duplicação é feita com exatidão, e até mesmo que ela não sofra alterações futuras perdendo sua legitimidade, utiliza-se de uma função de cálculo de HASH. O hash é uma sequência de bits gerados por um algoritmo de dispersão unidirecional, sendo capaz de cifrar uma sequência de dados de qualquer tamanho em uma sequência de tamanho fixo. Pode-se dizer que o hash é uma impressão digital de um arquivo, será idêntica sua impressão se o conteúdo dos dados for exatamente igual.

O tempo pode ser fator crucial quanto a preservação destes dados. Materiais utilizados na fabricação de dispositivos de armazenamento tendem a ter um tempo de vida útil, podendo assim ocasionar falhas e consequentemente danificando uma fonte de vestígio. Devido a tal fragilidade, torna-se prática a realização cópias de seguranças de variados dados. O tempo interfere quando se pretende apagar dados comprometedores. A restauração torna-se cada vez mais difícil com o passar do tempo e com o passar de que os dados vão sobrescrevendo os anteriores.

Após o término da fase de coleta, o dispositivo de armazenamento computacional deverá ser lacrado e guardado em local apropriado até que haja uma autorização por parte da justiça permitindo o seu descarte ou devolução.

2.2.3. Softwares e hardwares

Na etapa da coleta dispomos de diversos softwares e alguns hardwares que auxiliam o trabalho de um perito computacional. Como a maioria são pagos, e em média valores bem atenuantes, vamos falar do mais utilizado pelos peritos e do utilizado em nosso estudo de caso.

Para o uso da técnica de espelhamento de imagem utilizamos do SYCNBACKSE (versão paga) e do DRIVEIMAGE XML (versão gratuita). O SyncBackSE é bastante utilizado para copiar arquivos seguros, interligar computadores ao um servidor FTP e proteger documentos com criptografia. A proteção é feita por criptografia 256-bit AES e os arquivos também recebem compressão, para ocupar menos espaço em disco. O DriveImage XML permite que se faça uma cópia de segurança de qualquer HD ou partição para um arquivo de imagem, mesmo que o HD ou partição não esteja em uso.

Figura 2 - Softwares para espelhamento de imagem

Fonte: Do autor (2017)

Quando se fala em duplicação de disco, o método mais utilizado não se baseia em software, mas sim em hardwares de fácil manuseio e utilização. Existe hoje no mercado um duplicador bastante funcional chamado UNIDUPDOCK. Ele fornece uma clonagem de disco rápida e completa e pode funcionar de forma autônoma, sem ligação a um computador anfitrião. Fornecendo um clone exato, bit a bit, tem uma taxa de transferência de 72 MB / seg. é composto por duas entradas de HD SATA/IDE, uma tela LCD, onde é possível acompanhar todo o progresso, bem como relatar erros nas unidades. Suportando IDE e SATA, este dispositivo permite a duplicação de SATA para SATA, IDE para SATA ou SATA para IDE e IDE para IDE, desde que a unidade de origem não exceda o tamanho da unidade de destino.

Como no caso dos duplicadores, a maioria dos bloqueadores de escrita são hardwares.

Figura 3 - Duplicadores de disco

Fonte: StarTech

Temos o Ultrablock USB bridge, que traz um bloqueio de escrita seguro, porém serve apenas para armazenamentos em ambientes que suportam USB 2.0. O Ultrablock USB IDE/SATA, que é do mesmo fabricante do anterior, oferece as mesmas funcionalidades, porém é especializado a bloquear as escritas no discos rígidos IDE/SATA.

Figura 4 - Bloquadores de escrita

Fonte: Guidance Software

Listamos apenas alguns dos dispositivos e softwares mais usados nas perícias. Como estamos lidando sempre em paralelo com a lei, é necessário que todos os eles sejam de confiabilidade.

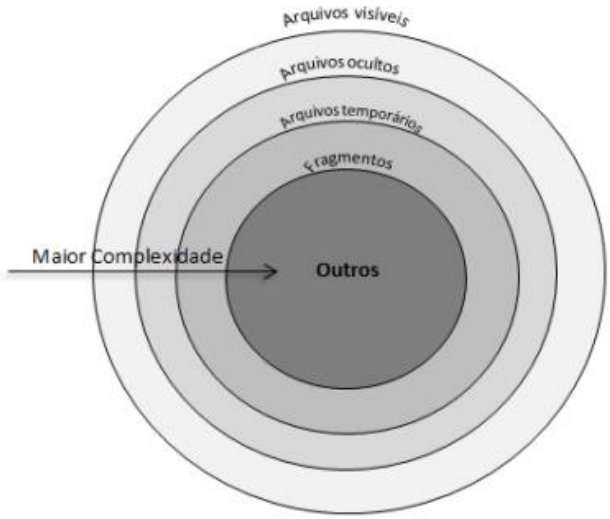
2.3. EXTRAÇÃO

A etapa da extração objetiva a recuperação, reunião e organização das informações coletadas nas cópias realizadas no processo anterior. Toda a investigação deve ser feita no espelho ou imagem do disco, sempre mantendo o material original intacto e protegido (ALMEIDA, 2011).

As cópias recolhem todos os dados do dispositivo, inclusive aqueles que não são necessários. Por isso quando se entra nesta etapa, a quantidade de dados é imensa – às vezes podem estar ocultos ou até corrompidos - para ser analisada pelo perito. Ao examinar o material, sua extração deve ser minuciosa e focada aos detalhes, sendo que na maioria dos casos, as evidências se encontram nas áreas mais improváveis do disco ou até terem sido removidas.

Podemos dividir os discos em camadas, sendo que a mais externa possui arquivos visíveis ao usuário comuns de computador, onde que nas camadas mais internas, encontram-se os arquivos ocultos, criptografados, temporários e apagados, fragmentos de arquivos, entre outros. Para Eleutério e Machado (2011), quanto mais profunda é a camada analisada, maior é o grau de complexidade para exploração, necessitando de técnicas especiais para sua extração.

Figura 5 - Disco rígido dividido por complexidade



Fonte: Adaptado de Eleutério e Machado (2011)

Pode ser útil para diminuir o campo de análise: a utilização de padrões de busca em textos, definindo nomes ou assuntos; filtrar os dados por tipos de arquivos, como áudios, vídeos, documentos de texto; "excluir 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 auxiliares.

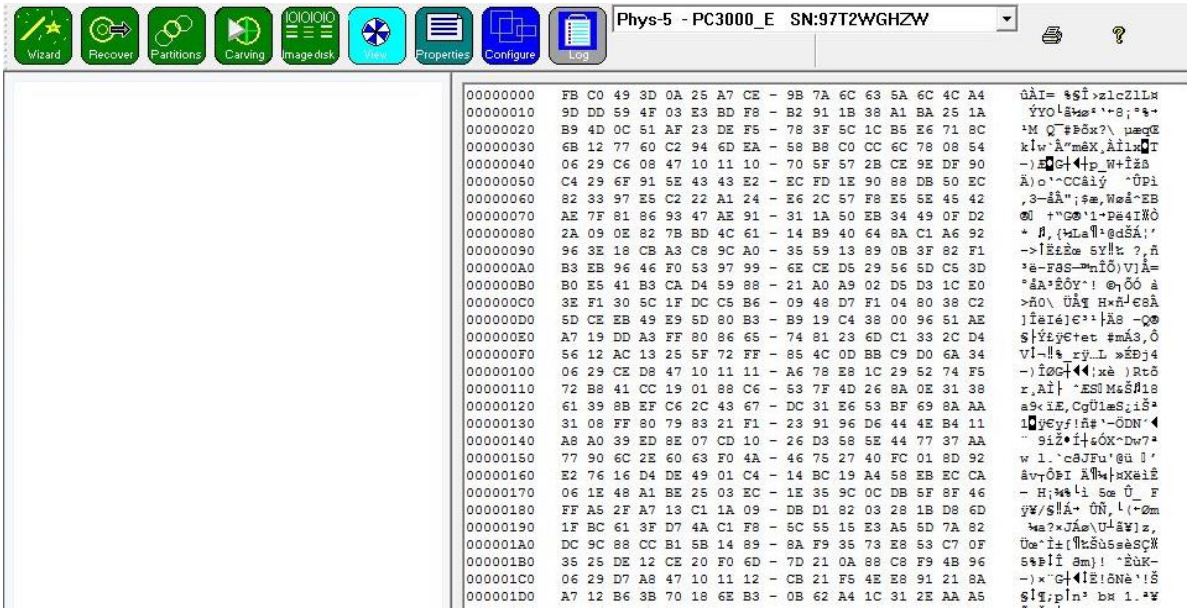
2.3.1. Softwares e hardwares

Alguns dados são irrelevantes para a perícia e podem ser ignorados, como também possíveis fontes de evidencias podem estar inacessíveis, devido a previa exclusão ou a proteção por senha. Vamos listar as principais técnicas e ferramentas utilizadas na etapa da extração.

2.3.1.1. Recuperação de arquivos

Tratamos neste item de um software bastante utilizado no meio forense, o CNW RECOVERY (versão paga). O software é uma caixa de ferramentas que permitem que dados e imagens perdidas, apagadas e corrompidas sejam recuperados e restaurados. Ele gera muitos logs para auxiliar a investigação e ajudar a analisar dados que foram recuperados do sistema. Os logs podem ser classificados, exportados e geralmente revisados. Para o exame pericial, um relatório baseado em XML pode ser gerado, e ajudará na continuidade da evidência.

Figura 6 - Análise de dados em hexadecimal com CNW Recovery

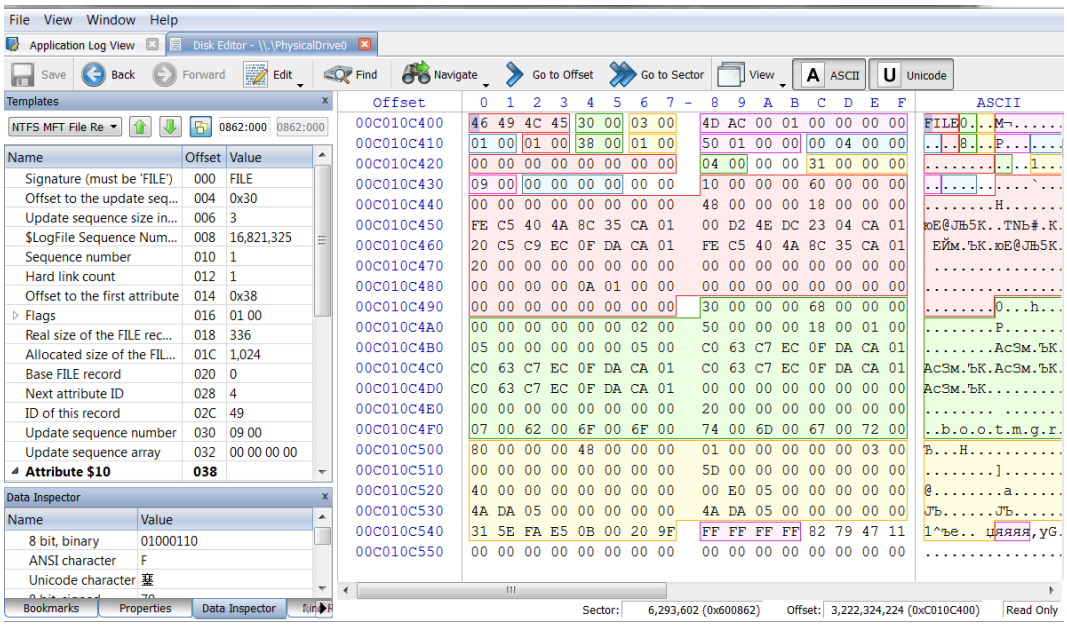


Fonte: Do autor (2017)

Em relação ao tempo necessário para recuperação de arquivos, é um caso relevante, onde levamos em consideração o local onde se quer realizar a ação. Um chip de memória de uma pequena câmera, por exemplo, com todos os arquivos excluídos, a recuperação pode ser de 5-10 minutos. Para uma unidade de 500GB em forma de imagem com vários setores defeituosos, a recuperação pode levar entre algumas horas e alguns dias.

O NTFS Data Recovery Toolkit (versão gratuita) é um conjunto de ferramentas para analisar problemas com partições e arquivos NTFS, fazendo a recuperação de dados nos modos manual e automatizado. Seu principal destaque é o modo manual, que permite analisar as estruturas do disco e definir o problema usando o Freeware Disk Editor. Pode também corrigir o problema usando o Disk Editor, Partition Manager ou Microsoft Windows (c) system utilities. Com esse conjunto de ferramentas pode-se analisar com detalhes cada arquivo e recuperá-lo.

Figura 7 - Análise de dados em hexadecimal com Disk Editor



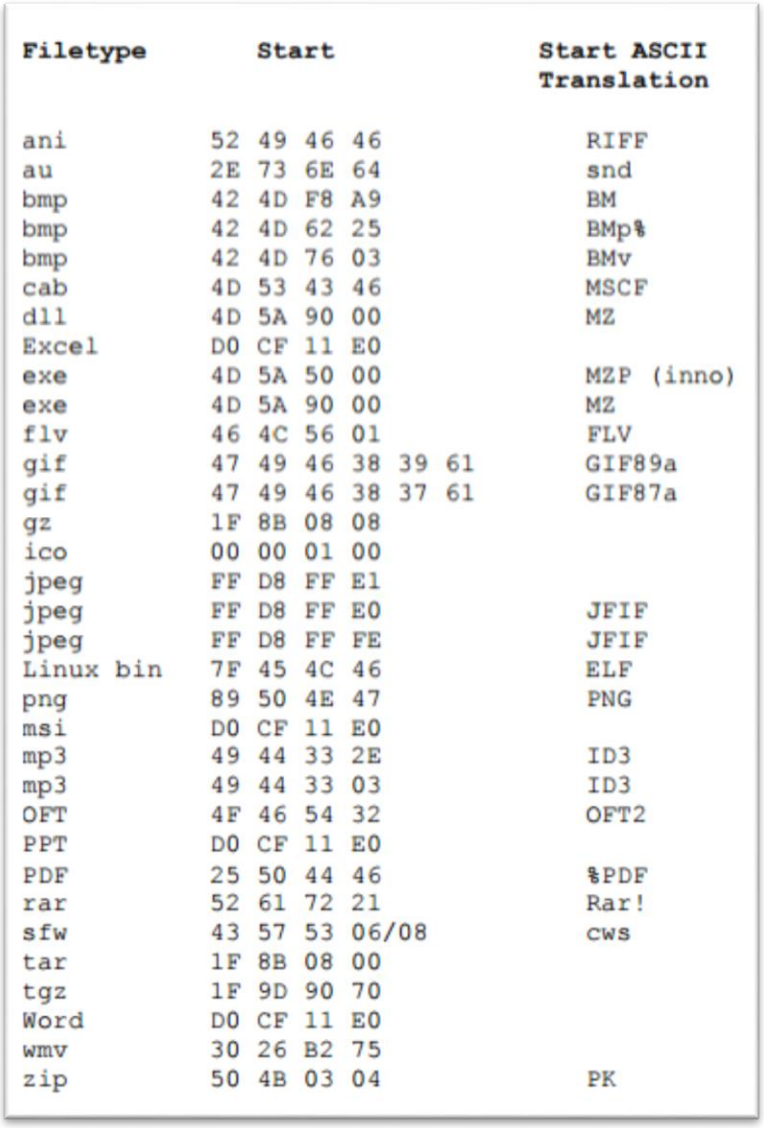
Fonte: Do autor (2017)

2.3.1.2. Indexação de dados

A indexação de dados é a técnica de organização de dados no dispositivo de armazenamento. Cria-se uma espécie de catálogo dividido por tipo de arquivo, onde cada arquivo tem sua característica única de iniciação e fechamento de blocos hexadecimais.

A indexação de dados é a técnica de organização de dados no dispositivo de armazenamento. Cria-se uma espécie de catálogo dividido por tipo de arquivo, onde cada arquivo tem sua característica única de iniciação e fechamento de blocos hexadecimais.

Figura 8 - Indexação de dados



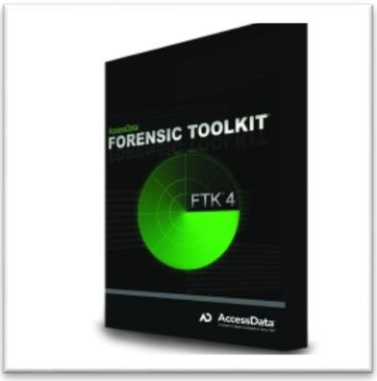
Filetype	Start	Start ASCII Translation
ani	52 49 46 46	RIFF
au	2E 73 6E 64	snd
bmp	42 4D F8 A9	BM
bmp	42 4D 62 25	BMp%
bmp	42 4D 76 03	BMv
cab	4D 53 43 46	MSCF
dll	4D 5A 90 00	MZ
Excel	D0 CF 11 E0	
exe	4D 5A 50 00	MZP (inno)
exe	4D 5A 90 00	MZ
flv	46 4C 56 01	FLV
gif	47 49 46 38 39 61	GIF89a
gif	47 49 46 38 37 61	GIF87a
gz	1F 8B 08 08	
ico	00 00 01 00	
jpeg	FF D8 FF E1	
jpeg	FF D8 FF E0	JFIF
jpeg	FF D8 FF FE	JFIF
Linux bin	7F 45 4C 46	ELF
png	89 50 4E 47	PNG
msi	D0 CF 11 E0	
mp3	49 44 33 2E	ID3
mp3	49 44 33 03	ID3
OFT	4F 46 54 32	OFT2
PPT	D0 CF 11 E0	
PDF	25 50 44 46	%PDF
rar	52 61 72 21	Rar!
sfw	43 57 53 06/08	cws
tar	1F 8B 08 00	
tgz	1F 9D 90 70	
Word	D0 CF 11 E0	
wmv	30 26 B2 75	
zip	50 4B 03 04	PK

Fonte: Do autor (2017)

Na figura 8, descrevemos as os cabeçalhos dos tipos de arquivos mais comuns, assim, os programas utilizam destes padrões para classificar os arquivos e separá-los, como definir seu lugar de alocamento na memória. Com isso é possível realizar buscas nos arquivos de forma rápida, através de palavras-chave, que será visto na etapa de análise.

A FTK (Forensic Toolkit) é uma plataforma de perícia desenvolvida com a finalidade de oferecer velocidade, estabilidade e facilidade de uso ao investigador. Ele fornece indexação de dados, de modo que a filtragem e busca sejam extremamente rápidas em relação a outros processos que não a utilizam.

Figura 9 - Forensic Toolkit (FTK)



Fonte: AccessData

2.4. ANÁLISE

Esta etapa é representada pelos exames dos dados adquiridos na etapa de extração anterior, com intuito de que hajam vestígios que sejam relacionados com o delito investigado. Essa relação ocorre por meio dos quesitos solicitados pela autoridade encarregada da investigação. Necessariamente, os quesitos devem ser bem claros, a fim de que não seja necessário examinar a grande quantidade de dados encontrados.

É recomendado que se busque por um especialista em vestígio de dados, para definir os tipos de arquivos, nomes ou palavras-chave a serem pesquisadas. Com essa ajuda o trabalho do perito fica mais eficaz e traz resultados com maior rapidez.

“Durante a etapa de análise, é comum a existência de senhas, criptografia e esteganografia dificultando o exame pericial” (SOUZA, 2015). Simplificando, arquivos podem estar protegidos por barreiras contra leitura, como algum tipo de senha, informações de texto criptografadas e mensagens dentro de outra sem valor probatório, por meio da esteganografia.

2.4.1. Técnicas e equipamentos

Para quebrar estas barreiras, existem métodos forenses com função de auxiliar nesta etapa. Pode ser por filtros, pesquisas por palavras-chave ou por suítes de ferramentas forenses.

2.4.1.1. Filtros

Um tipo de filtro muito utilizado é o Known File Filter. Ele cria uma lista de hash de arquivos ou informações já conhecidas, para assim realizar uma comparação com os arquivos procurados. Com sua utilização é possível diminuir a quantidade de arquivos ignorando os

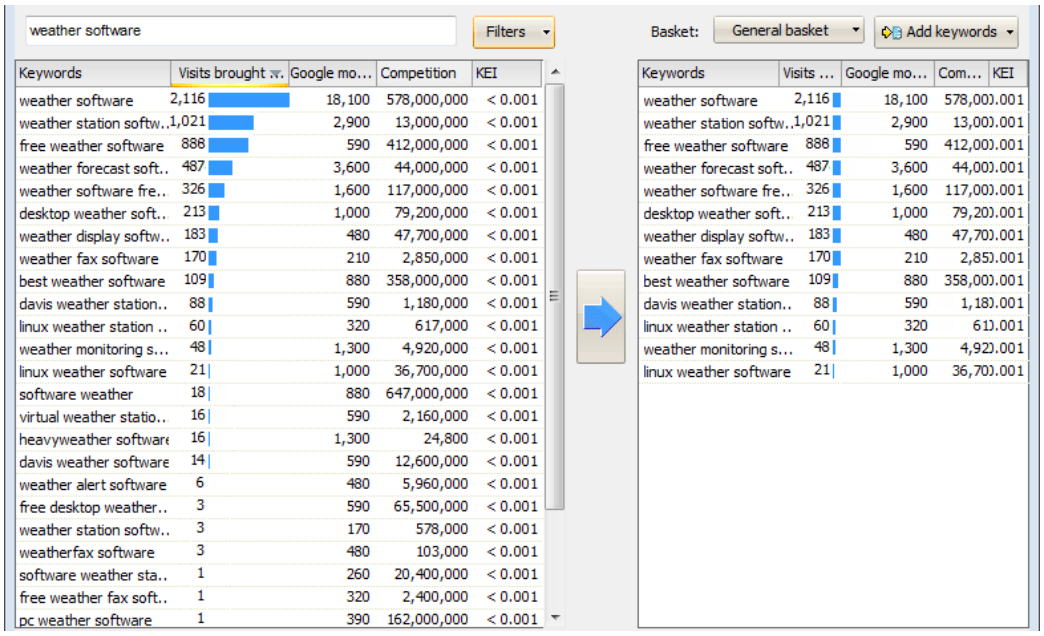
arquivos de programas conhecidos que não alterariam na busca, como por exemplo, os arquivos do sistema operacional.

Quando se já tem em mãos um arquivo ilícito e quer realizar a análise para busca de arquivos iguais em um meio eletrônico coletado, diferente do de sua origem, é possível através do filtro. Por meio da comparação de hash já mencionada anteriormente.

2.4.1.2. Palavras-chave

Com auxílio da indexação de dados essa técnica se torna bastantes eficaz. Como já se tem os dados separados, pesquisas por palavras-chave são mais rápidas, pois analisam apenas os arquivos definidos pelo perito. Como por exemplo, ao se deparar por um quesito de contatos telefônicos de outras pessoas, usamos palavras-chave desse meio : contatos, agenda, telefones, e-mails, entre outros.

Figura 10 - Exemplo de busca por palavras-chave



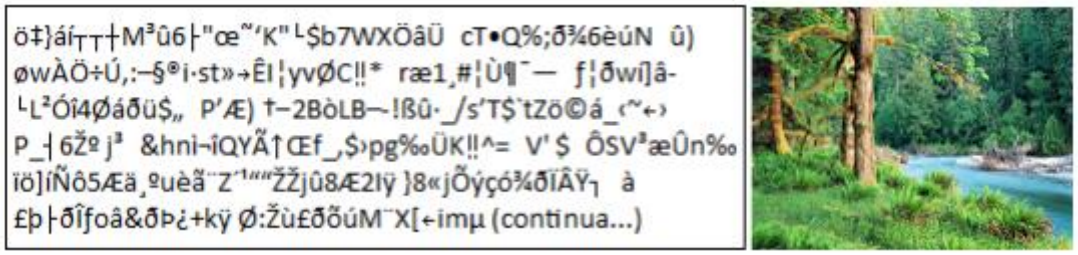
Fonte: Do autor (2017)

2.4.1.3.Visualização gráfica

Arquivos de áudio, imagem e vídeo podem estar representados por formas hexadecimais ou caracteres ASCI, que quando lidas são meramente descartadas por não terem sentido. A maioria das vezes acontece por seus cabeçalhos estarem sobrescritos, impossibilitando sua leitura em softwares convencionais.

Existem programas que convertem esses arquivos para melhor análise de vestígios, como o Forensic Toolkit, já mencionado na etapa anterior.

Figura 11 - Representação de arquivo em formato texto e em formato imagem



Fonte: Adaptado de Eleutério e Machado (2011)

2.4.1.4.Virtualização

Em casos especiais, não podemos abrir imagens de disco de modo convencional, pois podem incorrer na alteração de informações pela inicialização do sistema. Usamos dos ambientes virtuais para essas operações. 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).

Figura 12 - Virtualização de ambiente

Fonte: Do autor (2017)

2.5. APRESENTAÇÃO

A apresentação, ou propriamente dita a documentação, é a última etapa do processo. Sua função é documentar as possíveis evidencias digitais e apresenta-las às autoridades requerentes. 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).

É registrada através do laudo pericial, onde é detalhado minuciosamente todas as ações do perito nas etapas anteriores. Sua escrita deve ser desenvolvida de forma concisa e clara, pois deve ser interpretada por pessoas que não sejam ligadas à área pericial computacional.

Geralmente, os laudos possuem a seguinte estrutura: preâmbulo, histórico, material, objetivo, considerações técnicas ou periciais, exames e respostas aos quesitos formulados.

Quadro 1 - Seções do laudo técnico pericial

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

Fonte: Adaptado de Eleutério e Machado (2011)

3. ESTUDO DE CASO

Para exemplificar o conteúdo abordado neste artigo, foi proposto um estudo, aplicando as práticas comumente empregadas pelos peritos e utilizando um cenário hipotético, onde um perito forense computacional seria necessário, demonstrando assim o uso de algumas das ferramentas apresentadas no trabalho.

3.1. Justificativa e cenário

O crescente uso de aparelhos eletrônicos torna o perito forense computacional cada vez mais requisitado. Segundo Eleutério e Machado (2011), o papel principal da computação forense é a identificação e tratamento de possíveis evidências digitais em provas apreendidas em episódio criminoso.

No cenário em questão, há um dispositivo de armazenamento móvel, o qual foi encontrado em posse de indivíduo suspeito de participação de quadrilha que rouba carros para revenda, durante uma abordagem policial. Através da análise pericial dos dados devem ser respondidas certas questões como: havia informações (vídeos, imagens ou texto) de carros roubados? Havia também informações de possíveis vítimas ou veículos?

A computação forense realiza exames periciais principalmente em dispositivos de armazenamento computacional (ELEUTÉRIO; MACHADO, 2011). Portanto, a aplicação das etapas de coleta, extração, análise e apresentação, tal como alguns softwares utilizados na perícia, são relevantes nesse caso e enriquecem o estudo.

3.2. Processo forense nos dados do dispositivo de armazenamento móvel

É necessário o desenvolvimento de uma metodologia que atenda todos os gêneros de crimes digitais (REITH; CARR; GUNSCH, 2002). Para garantir a correta análise forense do dispositivo em questão, as etapas do processo de perícia foram adotadas como forma de padronização. Os programas utilizados foram listados durante cada uma das primeiras três etapas, que remetem à análise do dispositivo, sendo a etapa de apresentação tratada logo em seguida com os resultados obtidos e apresentados na forma de laudo.

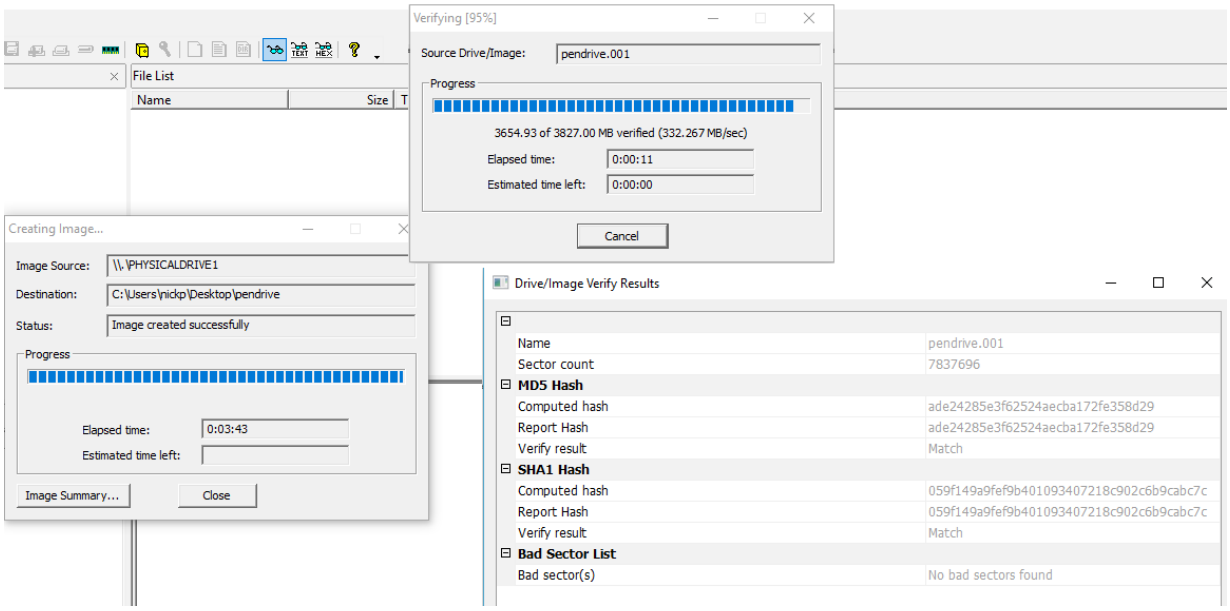
3.3. Coleta

O procedimento de coleta foi iniciado após a obtenção do dispositivo removível. É iniciada então a cópia dos dados contidos nesse dispositivo de forma completa e inalterada.

Como o trabalho tem fins acadêmicos, se torna inviável a obtenção de um bloqueador de escrita devido seu preço, portanto o registro do computador onde o dispositivo seria analisado foi modificado de forma que a entrada USB (Universal Serial Bus) se tornasse somente leitura, impedindo assim a gravação de dados no dispositivo, o que invalidaria possíveis evidências. Lembra-se que essa técnica não é normalmente utilizada pois não garante total segurança dos dados do dispositivo ou da máquina, sendo utilizada aqui somente como forma de ilustrar a metodologia, já que em prática, esses bloqueadores são hardwares que fornecem segurança absoluta.

O passo seguinte foi a criação de cópia fidedigna dos dados do dispositivo. Com o *software* AccessData Forensic Toolkit, foi possível a criação de tal cópia, salva em formato XML para posterior análise. O software traz diversas informações quanto aos dados copiados e oferece também a comparação de *hash* para verificação de inalterabilidade e integridade dos dados.

Figura 13 - Processo de espelhamento e comparação de hash



Fonte: Do autor (2017)

Após finalizado o processo de cópia, a etapa da coleta encerra-se com o dispositivo sendo lacrado e guardado como prova. Todas etapas subsequentes são periciadas sobre a imagem gerada que consiste na cópia fiel dos dados contidos no pen-drive.

3.4. Extração

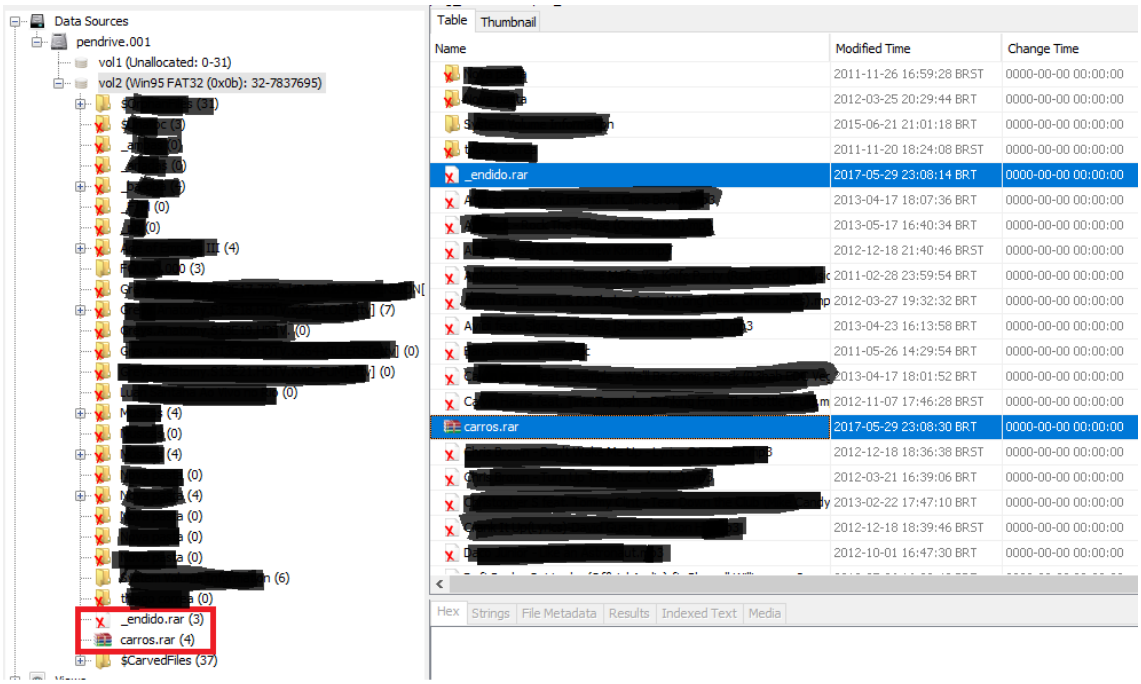
Durante a extração, arquivos e informações contidos na imagem que possam ser de interesse para perícia ou sejam relacionados ao fato são recuperados.

Como modo de responder a uma das questões do caso proposto, é necessário conferir a existência de arquivos que possam comprometer ou incriminar o suspeito, podendo inclusive fornecer informações suficientes para que a investigação continue.

Uma das ferramentas utilizadas neste processo foi a ferramenta *Autopsy*, que permite acesso e extração de arquivos contidos em uma imagem, no caso, do dispositivo móvel. O software permite buscas por formatos específicos de arquivos de imagens (.jpg / .png), vídeos (.mp4), texto (.doc / .txt) e inclusive arquivos compactados (.zip / .rar). No programa, são listados então os resultados da busca feita, marcados da cor vermelha caso tenham sido excluídos do dispositivo, sendo então necessária a utilização de ferramentas e técnicas para recuperar estes arquivos. Alguns podem ser pré-visualizados, mas há também a opção de exportação dos arquivos de interesse do perito para que possam ser melhor analisados e tratados.

Após a extração dos arquivos relevantes, foi verificada a existência de arquivos protegidos por senha que podem ser de interesse da perícia. Existem hoje, diversos programas que forçam a entrada desses arquivos, por um ataque de diversas senhas baseadas em dicionários de senhas já conhecidas ou até mesmo por força bruta, onde tenta uma série de algarismos alfanuméricos até encontrar a sequência correta, quando não um misto de ambos. Para essa finalidade foi empregada a ferramenta *RainbowCrack* (gratuita e open-source), também utilizada em um dos artigos referenciados, e que se mostrou de grande valor.

Figura 14 - Processo de extração dos arquivos suspeitos pelo Autopsy

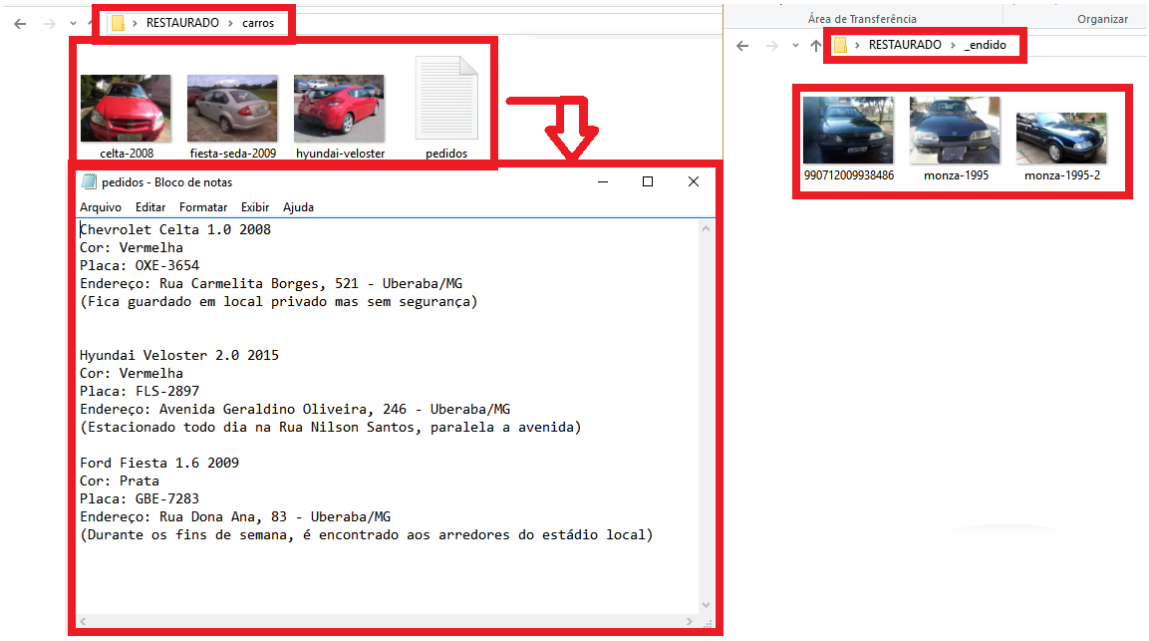


Fonte: Do autor (2017)

3.5. Análise

Foram encontradas dois arquivos compactados, um recentemente excluído e outro presente no dispositivo removível. Após recuperação do arquivo deletado, ambos tiveram suas senhas quebradas e apresentaram conteúdo relevante a investigação. O arquivo deletado continha imagens de um carro apreendido após ter sido roubado e revendido. Já o arquivo que ainda estava presente continha imagens de diversos carros juntos a um arquivo de texto que consistia de uma lista com informações como placa, modelo, cor e endereço.

Figura 15 - Provas após a recuperação confirmam suspeita



Fonte: Do autor (2017)

3.6. Apresentação

Abaixo, foi redigido um modelo de laudo técnico pericial exemplificando o caso.

Quadro 2 - Modelo de laudo pericial com os dados do caso

Preâmbulo	Laudo Técnico Pericial – Caso Revenda de Carros Roubados
Histórico	Foi apreendido um dispositivo de armazenamento removível em posse de indivíduo suspeito de envolvimento com quadrilha de roubo e revenda de carros. A perícia deve responder se havia informações (vídeos, imagens ou texto) de carros roubados e também informações de possíveis vítimas ou veículos.
Material original/ apreendido	Um *pen drive* da marca *SanDisk* (nº de série BH1009OEWB), modelo *Cruzer Blade*, com capacidade de 4GB, apreendido em posse do suspeito.
Objetivo	Identificação e recuperação de possíveis evidências presentes no dispositivo, como fotos, vídeos ou texto de carros roubados ou possíveis vítimas;

	Garantir a integridade do material periciado, preservando os dados nele contido; Apresentar os resultados obtidos à partir da análise forense à autoridade requerente.
Considerações técnicas	- Uma função *hash* gera um resultado chamado de valor *hash*, consiste em uma sequência bits gerados matematicamente, resumindo um arquivo ou informação. Oferece capacidade de detectar erros e é geralmente utilizada na verificação da integridade e autenticação de arquivos. São calculados através de algoritmos, como o MD5 (não mais seguro criptograficamente), SHA-1, SHA-2 e SHA-3. - *Cracking* consiste na quebra de senhas de arquivos protegidos ou sistemas, podendo ser feita através de ataques de dicionário (comparação com senhas já conhecidas), força bruta (tentativa e erro de diversas sequências de algarismos alfanuméricos) ou uma mistura de ambos.
Exames	- Na primeira etapa foi realizada a coleta das possíveis evidências. O uso do registro do computador utilizado como bloqueador de escrita foi a opção viável para garantir a segurança, apesar de não ideal. Foi então realizada cópia do dispositivo adquirido, sendo ele então lacrado e separado. Todos os procedimentos subsequentes foram realizados na imagem gerada pela cópia, garantindo inalterabilidade dos dados originais. Valores de *hash* foram gerados e utilizados para garantir a integridade dos dados. - A segunda etapa se deu através da extração dos dados da imagem do dispositivo removível. Todo e qualquer arquivo que pudesse ter relação com a investigação em questão foi recuperado e tratado com ferramentas específicas. - Durante a terceira etapa foi feita a análise dos dados e informações adquiridas com os arquivos que foram recuperados, para assim então responder os questionamentos relacionados ao caso.
Respostas aos quesitos	- Havia informações (vídeos, imagens ou texto) de carros roubados? Dentre os arquivos analisados, havia um arquivo deletado que foi recuperado e tratado. Este continha três imagens de um veículo previamente apreendido, após ter sido roubado e revendido. - Havia também informações de possíveis vítimas ou veículos?

	O arquivo remanescente no dispositivo constava de três imagens de veículos diversos e um arquivo de texto, o qual continha uma lista com informações dos veículos como placa, modelo e cor, além de endereços de possíveis vítimas.

Fonte: Do autor (2017)

3.7. Resultados

Após concluir o estudo, foi possível compreender melhor o funcionamento das etapas de uma perícia forense computacional e a sua importância. Apesar das dificuldades encontradas, diversas vezes na realização do trabalho, a aplicação das ferramentas se mostrou eficaz e trouxe os resultados esperados.

Por ser inviável a aquisição de um bloqueador de escrita, recorremos ao registro do sistema operacional utilizado para tornar as portas USB somente leitura. Utilizamos então o *software Forensic Toolkit Imager* para duplicar e verificar a integridade dos dados através de valores de *hash*.

Durante a etapa de extração, a ferramenta *Autopsy* se demonstrou muito útil na busca e extração dos arquivos relevantes ao caso. Ao realizar a busca, foi encontrado arquivo deletado, o qual foi necessário ser recuperado, a ferramenta *Data Recovery Toolkit* permitiu a recuperação em relativamente pouco tempo. Após a recuperação do arquivo, este se mostrou estar bloqueado por senha e foi então preciso usar outra ferramenta, o *software RainbowCrack,* que realiza o trabalho sem muitas delongas. Para a quebra da senha foi utilizado um ataque em que a geração de hash feita pelo utilitário compara a senha com diversas outras já conhecidas e utilizadas, e assim que encontrada, é disponibilizada par ao usuário.

Na fase de análise, foi utilizado o software Forensic ToolKit para comparação de hash e geração de novos para os arquivos recuperados e tratados. A análise apesar de pouco complexa nesse caso, foi de fundamental importância para responder as questões propostas.

Apresentamos então um modelo de laudo semelhante ao que deparamos em um dos trabalhos referenciados, o qual preenchemos com os dados encontrados, respondendo todas as questões levantadas e resumindo e simplificando para que possa ser entendido por aqueles que são leigos no que se trata este trabalho.

A confecção do mesmo foi valorosa para adquirir um maior conhecimento na área, pois foi possível um maior aprofundamento num tema que vem crescendo mas que ainda apresenta poucos recursos e poucos profissionais atuantes.

4. CONCLUSÃO

Neste trabalho foi possível conhecer as principais etapas normalmente usadas no exercício de uma perícia computacional, sendo elas voltadas ao âmbito dos dispositivos de armazenamento. Tendo continuidade observaram-se aspectos e procedimentos relevantes, como volatilidade e preservação dos dados.

Foram destacadas as principais ferramentas e técnicas (em hardware e software) utilizadas para as fases da perícia, sendo elas: procedimento para coleta de dados nos principais tipos de fontes de dados existentes atualmente, extração da informação requerente à petição visando preservação da integridade do material, análise minuciosa dos dados para diagnóstico jurídico e por fim documentação de relatório técnico dos resultados.

Embora realizado sem muita complexidade, o fechamento do estudo de caso permitiu a aplicação do processo forense, das técnicas e das ferramentas periciais apresentadas. A análise de possíveis evidências foi feita de forma cômoda ao perito. Ainda que tenha sido possível filtrar e centralizar a análise, a quantidade de arquivos e informações aumenta substancialmente em um cenário real, o que torna a atividade de análise em um processo lento ou até inviável.

Este trabalho não tem pretensão de esgotar as possíveis situações de investigação forense, mas sim ampliar o vago estudo com a proposta de um modelo genérico de roteiro pericial.

Estudos adicionais e futuros podem ser realizados a fim de analisar ambientes mais complexos, onde quantidade e volatilidade das informações são fatores críticos. Outro apêndice importante para realizações futuras é o engajamento da cultura judicial brasileira ao objeto de estudo deste trabalho.

5. BIBLIOGRAFIA

ALMEIDA, R. N. **Perícia forense computacional:** estudo de técnicas utilizadas para coleta e análise de vestígios digitais. 48 p. Processamento de Dados, Faculdade de Tecnologia de São Paulo, 2011.

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 Processes.** In: ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE, 1 ., 2006, Albany. Proceedings of the 1 st. Annual Symposium on Information Assurance. Albany: University at Albany, 2006. p. 72 - 80.

MADEIRA, M. N. **Forense computacional.** Santa Catarina, Universidade do Sul de Santa Catarina, p. 148, 2012.

JUNIOR, C. C. N. M.; MOREIRA, J. **Roteiro Investigativo em Perícia Forense Computacional de Redes:** Estudo de Caso. T.I.S. - Tecnologias, Infraestrutura e Software, São Carlos, v. 3, n. 1, p. 11-23, Jan./Abr., 2014.

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.

REITH, M.; CARR, C.; GUNSCH, G. **An Examination of Digital Forensic Models.** International Journal of Digital Evidence, v. 1, n. 3, 2002.

SAFE E METROPOLITAN POLICE SERVICE UK. **ACPO**: good practice guide for digital evidence. 2012. Disponível em: < http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf >. Acesso em: 16 abr. 2017.

SOUZA, P. F. C. **Perícia forense computacional:** procedimentos, ferramentas disponíveis e estudo de caso. 74 p. Área de Concentração em Informática Forense e Segurança da Informação, Universidade Federal de Santa Maria, 2015.