ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO

Cap QCO Info Wagner Comin Sonáglio

FERRAMENTAS BASEADAS EM SOFTWARE LIVRE PARA ANÁLISE FORENSE COMPUTACIONAL

Florianópolis
2018

Cap QCO Info WAGNER COMIN SONÁGLIO

FERRAMENTAS BASEADAS EM SOFTWARE LIVRE PARA ANÁLISE FORENSE COMPUTACIONAL

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares.

Orientador: Maj QCO Info Luiz Fernando Sousa da Fonte

Florianópolis
2018

Cap QCO Info WAGNER COMIN SONÁGLIO

FERRAMENTAS BASEADAS EM SOFTWARE LIVRE PARA ANÁLISE FORENSE COMPUTACIONAL

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares.

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____
José Roberto Pinho de Andrade Lima – TC QCO Vet – Presidente
Escola de Formação Complementar do Exército

_____
Luiz Fernando Sousa Fonte – Maj QCO Info – Membro
Escola de Formação Complementar do Exército

_____
Marcelo Antonio do Nascimento – Maj QCO Info – Membro
Escola de Formação Complementar do Exército

FERRAMENTAS BASEADAS EM SOFTWARE LIVRE PARA ANÁLISE FORENSE COMPUTACIONAL

Wagner Comin Sonáglio[a]

RESUMO

Com o advento da internet, as pessoas e as organizações no mundo inteiro experimentaram uma nova forma de troca de informações. Com o tempo a internet evoluiu rapidamente e continua crescendo de forma espantosa. Com isso, diversos ramos de atividades passaram a utilizar a internet e as redes de computadores como meio principal de troca e armazenamento de informações. Junto com esta ascensão da internet surgiram também os crimes virtuais e os incidentes de segurança. Para trabalhar com essa nova forma de crime, surgiu um novo ramo de Perícia Forense, chamado de Perícia Forense Computacional, cujo tema se torna importante cada vez mais. Com a Estratégia Nacional de Defesa, o Exército Brasileiro ficou responsável pela Defesa Cibernética. Com o objetivo de se manter uma estrutura interna eficiente quanto à área cibernética, surgiu a necessidade de se analisar as principais ferramentas de análise forense computacional baseadas em *Software* Livre, a fim de classificar qual ferramenta pode ser aplicada em um ambiente militar.

Palavras-chave: *Software* Livre, Perícia Forense, Análise Forense Computacional.

ABSTRACT

With the advent of the internet, people and organizations around the world have experienced a new way of exchanging information. Over time, the internet has evolved rapidly and continues to grow up in a frightening way. As a result, several branches of activities began to use the Internet and computer networks as the main means of exchanging and storing information. Along with this rise of the internet have also emerged virtual crimes and security incidents. To work with this new form of crime, a new branch of Forensic Expertise has emerged, called Computational Forensics, whose subject becomes increasingly important. With the National Defense Strategy, the Brazilian Army was responsible for Cyber Defense. In order to maintain an efficient internal structure in the area of cybernetics, the need arose to analyze the main tools of computational forensic analysis based on Free Software, in order to classify which tool can be applied in a military environment.

Keywords: Free Software, Forensic Expertise, Computational Forensic Analysis.

[a] Capitão QCO de Informática da turma de 2010. Especialista em Aplicações Complementares às Ciências Militares pela EsAEx em 2010.

SUMÁRIO

FERRAMENTAS BASEADAS EM SOFTWARE LIVRE PARA ANÁLISE FORENSE COMPUTACIONAL

1. INTRODUÇÃO

Nos últimos anos, a Internet passou a ser um dos principais meios de comunicação para se trocar informações, adquirir produtos e fazer uso de serviços que até pouco tempo atrás não eram utilizados pelas pessoas por serem pouco comuns. Diante do crescimento da utilização da Internet, foram surgindo novos serviços em vários segmentos, como, por exemplo, no setor bancário, comercial, militar, entre outros. Esta nova fase da Internet serviu como meio para o surgimento de crimes virtuais procurando explorar esses novos tipos de serviços (QUEIROZ E VARGAS, 2010).

Conforme Santos (2008), as organizações atualmente estão preocupadas em utilizar mecanismos para aumentar a segurança dos sistemas computacionais que utilizam a internet e redes locais, porém, não existe garantia de que elas poderão se proteger de ataques virtuais, mesmo que sigam todos as implementações de segurança recomendadas e as tecnologias mais modernas.

Segundo Silva e Oliveira (2014), o uso de ferramentas para atividades como invasão de sistemas, roubo de dados, fraudes, dentre outros, passou a crescer ao longo dos anos. Essas atividades são conhecidas como cibercrimes, sendo que sua principal diferença dos crimes tradicionais é justamente o uso de computadores e outros equipamentos de informática.

Como não existe tecnologia que garanta segurança total, é importante que se encontrem meios para que, no caso de uma ocorrência de invasão, a organização afetada possa agir da melhor maneira possível para evitar o agravamento da situação, colocando em prática, por exemplo, um sistema de resposta a incidentes.

Este sistema é composto por uma equipe de múltiplas especialidades, capaz de atuar de forma integrada e com velocidade para reduzir o tempo de exposição da organização, minimizando os impactos do incidente de segurança.

Essa equipe, em conjunto com as metodologias de análise forense, pode fazer surtir efeitos positivos para a organização no que se refere à resolução de problemas causados pelos ataques virtuais e ações que visem desvendar as causas e os responsáveis pelos mesmos.

Este sistema é definido como Perícia Forense Computacional, também conhecida como Computação Forense ou Forense Computacional. (SANTOS, 2008).

Segundo a Estratégia Nacional de Defesa – END (BRASIL, 2018), lançada em 2008 e revista em 2012, deve-se fortalecer os três setores de importância estratégica: o espacial, o cibernético e o nuclear. Ainda, segundo a END, cabe ao Exército Brasileiro (EB) a responsabilidade pela Defesa Cibernética.

Dentro deste contexto, é de suma importância que o EB deva possuir meios próprios, utilizando ferramentas baseadas em *Software* Livre, para realizar suas perícias computacionais forenses.

Existem muitas ferramentas e sistemas para este fim, inclusive ferramentas baseadas em *Software* Livre para a análise forense digital. Com o surgimento dessas ferramentas, fica a questão de qual delas é a mais indicada para cada caso e qual possui os melhores módulos para análise forense.

Em função da importância do uso da Tecnologia da Informação no Exército Brasileiro, principalmente com a missão da Defesa Cibernética incumbida a esta instituição, o objetivo desse trabalho foi analisar as principais ferramentas de análise forense computacional baseadas em *Software* Livre a serem aplicadas em um ambiente militar como o do EB.

2. METODOLOGIA

O presente trabalho caracteriza-se por ser uma pesquisa que compreende um estudo de natureza aplicada, de abordagem qualitativa, do tipo exploratória. Para tal, realizou-se uma revisão teórica do assunto, através da pesquisa bibliográfica a legislações, documentos e trabalhos científicos (artigos, trabalhos de conclusão de curso, dissertações e teses). Foi feito uma consulta ao sítio eletrônico da Secretaria-Geral do Exército (SGEx), com o objetivo se obter dados referentes à legislações relacionadas à Perícia Forense Computacional no EB. Foi aplicado uma análise de dos principais sistemas e ferramentas baseadas em *Software* Livre para Análise Forense Computacional

As informações obtidas com a pesquisa bibliográfica e documental, e com os testes foram analisados e expostas em subitens dentro do capítulo de Resultados e Discussão (Capítulo 4).

3. REFERENCIAL TEÓRICO

A seguir, serão descritos o referencial teórico sobre análise forense computacional e *Software* Livre.

3.1. CONCEITOS BÁSICOS DE PERÍCIA FORENSE COMPUTACIONAL

Diante de toda as tecnologias desenvolvidas atualmente, a internet foi umas das que mais beneficiou a vida humana e que continua em plena evolução. Atualmente, através de meios eletrônicos e de informática, é possível disponibilizar e consultar todo tipo de informação sempre que for necessário e em qualquer lugar, tudo em tempo real.

Contamos também com o crescimento constante dos serviços disponíveis pela internet, além da ampliação e otimização de sua infraestrutura. No entanto, com isso temos cada vez mais *softwares* com finalidades ilícitas, que podem ser utilizados e acessados facilmente, trazendo o significativo crescimento de invasões de computadores (MELO, 2009).

Por esse motivo, a *internet* pode ser utilizada para diversos objetivos pelos indivíduos e organizações, inclusive para a prática de crimes virtuais.

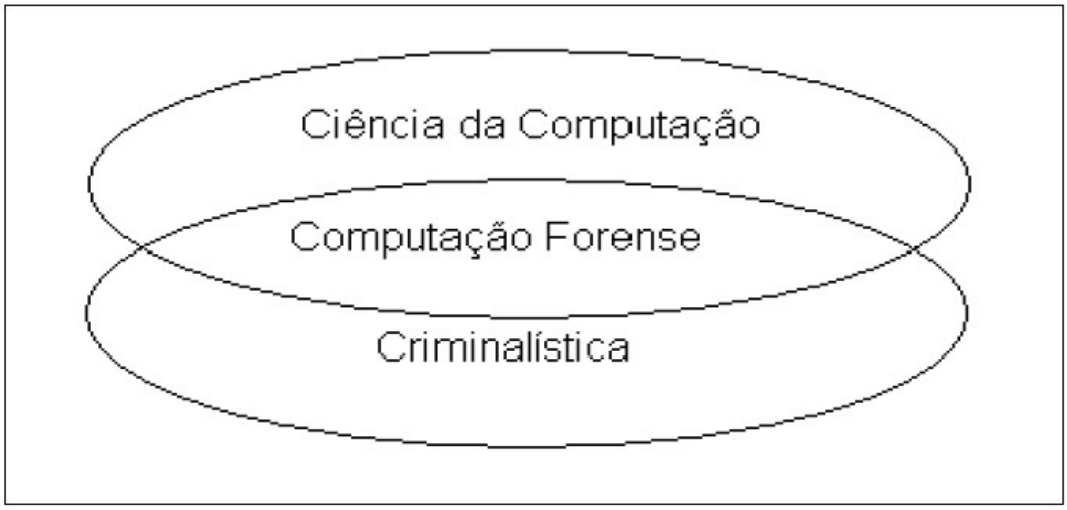
Conforme Santos (2008), a Perícia Forense Computacional tem como objetivo fornecer meios técnicos e legais para a manipulação das evidências digitais. Esta ciência estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional. As informações produzidas podem ser utilizadas para a solução de uma investigação. O técnico responsável por essa perícia é o Perito Forense Computacional.

Melo (2009, p. 13) faz uma definição resumida de computação forense:

> A Computação Forense pode ser definida como uma área da Ciência da Computação que se desenvolve gradualmente para atender à demanda oriunda da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação.

A Figura 1, mostra a relação as áreas de conhecimentos que envolvem a Computação Forense:

Figura 1: Relação entre Ciência da Computação, Criminalística e Computação Forense



Fonte: Melo, 2009.

3.2. CRIMES VIRTUAIS

A utilização de equipamentos de informática para crimes virtuais não é tão recente, porém, a legislação brasileira ainda não está totalmente preparada para tipificar todas as modalidades de crimes cibernéticos, principalmente a do EB, onde, após pesquisa nas legislações em vigor através do REPUBLEx 2018 (BRASIL, 2018), não foram encontradas orientações sobre crimes virtuais, apenas uma orientação de enquadramento de crimes virtuais nos códigos penais, através da Cartilha de Segurança em Redes Sociais, conforme Figura 2 (BRASIL, 2018).

Figura 2: Extrato da Cartilha de Segurança nas Redes Sociais do EB

Enviar vírus, comando, instrução ou programa de computador que destrua equipamento ou dados eletrônicos.	Dano simples.	Art. 259, CPM	Detenção, até seis meses.
	Dano.	Art. 163, CP	Detenção, de 1 a 6 meses, ou multa.
Copiar conteúdo de terceiros sem autorização ou sem mencionar a fonte, baixar MP3 ilegalmente, usar software ou jogo sem licença.	Violação de Direito Autoral.	Art. 184, CP	Detenção, de 3 meses a 1 ano, ou multa.

Fonte: Brasil, 2018.

Atualmente, há um projeto de lei e o Marco Civil da Internet Brasileira tramitando na Câmara dos Deputados e no Senado Federal, porém não há previsão para que sejam apreciados, votados e entrarem em vigor. Tais textos regulamentam, por exemplo, o crime de criação e transmissão de vírus e o tempo mínimo que um provedor de internet deve guardar os registros de acesso de seus usuários. (FILHO, 2016).

Diante dessas dificuldades, as organizações utilizam a estratégia de enquadrar os atos ilícitos em crimes já existentes no Código Penal ou no Código Penal Militar, no caso do EB.

Portanto, é de suma importância diferenciar se o computador é utilizado apenas como ferramenta de auxílio à pratica de delitos convencionais ou se é usado como meio para a realização do crime. Segundo Filho (2016), os equipamentos computacionais podem ser utilizados de duas formas para o cometimento de crimes: ferramenta de apoio à prática de delitos convencionais ou alvo/peça imprescindível da ação criminosa.

Na primeira categoria, os crimes envolvidos são delitos que podem ser cometidos sem o uso de computadores ou outros equipamentos, mas como a sociedade está cada vez mais digital, esses crimes podem deixar vestígios digitais para serem investigados posteriormente.

A outra categoria são os crimes utilizando-se diretamente de equipamentos de informática, nos quais os computadores e outros equipamentos são peças imprescindíveis para o cometimento do crime. Eles são a peça central do crime. Ataques a sites, programas maliciosos para roubo de senhas, programas que sequestram os dados do usuário (*ransomware*), entre outros, são exemplos desse tipo de crime.

3.3. QUESTÃO LEGAL DA ANÁLISE FORENSE DIGITAL

Toda inovação tecnológica traz uma série de benefícios e oportunidades para a sociedade. Porém, surge também a oportunidade para a realização de novos crimes utilizando estes meios. Portanto é necessário que haja uma investigação por parte das autoridades competentes, a qual se inicia sempre com a apuração e análise dos vestígios deixados, conforme determina o Código de Processo Penal Brasileiro (CPP) em seu artigo 158:

> Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

Segundo o dicionário Michaelis da Língua Portuguesa, vestígio é definido como:

> 1 - Sinal deixado pela pisada ou passagem, tanto do homem como de qualquer outro animal; pegada, rasto. 2 - Indício ou sinal de coisa que sucedeu, de pessoa que passou. 3 - Rastros, resquícios, ruínas. Seguir os vestígios de alguém: fazer o que ele fez ou faz; imitá-lo.

No caso da área de informática, os vestígios de um crime são digitais, uma vez que toda a informação armazenada nesses equipamentos computacionais é composta por bits em uma ordem lógica. Já em seu artigo 159, o CPP impõe que:

> O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.

Desta forma, Perícia Forense Computacional é a atividade concernente aos exames realizados por profissional especialista (Perito), legalmente habilitado, destinada a determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crimes, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo (ALMEIDA, 2011).

3.4. METODOLOGIA ENVOLVIDA NA COLETA E NO EXAME DE VESTÍGIOS DIGITAIS

Conforme Silva e Oliveira (2014), é necessário que sejam executados procedimentos e protocolos documentados que assegurem os requisitos legais e técnicos para a evidência pericial digital. Inicialmente é feita a coleta de informações nas mídias digitais. Posteriormente é feito o reconhecimento da evidência, seguido de sua coleta, restauração, documentação e preservação. Finalmente há a correlação das evidências coletadas para que haja a reconstrução dos eventos.

Segundo Queiroz e Vargas (2010), o procedimento que envolve o processo da perícia é composto pela:

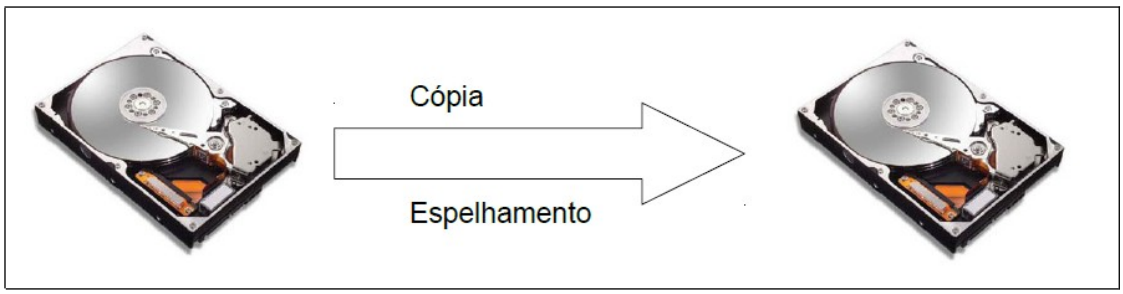
- Identificação da mídia (obtenção das evidências a serem periciadas);
- Coleta (mapeamento de tudo o que foi coletado);
- Preservação da evidência (realização da função *hash* e cópias dos dados para que a original se mantenha segura);
- Análise (onde exige o maior conhecimento do perito, com o uso de ferramentas); e
- Apresentação (criação de um relatório, laudo do perito sobre os dados encontrados durante a análise).

3.5. TÉCNICAS UTILIZADAS NA PERÍCIA FORENSE COMPUTACIONAL

Segundo Constantino (2012), as etapas utilizadas para a parte técnica da Perícia Forense Computacional podem ser classificadas em:

1. Preservação: Nesta etapa o perito deve preservar todas informações que se encontram em um determinador dispositivo. Isso é importante pois caso o perito corrompa os dados durante a perícia a fonte original das informações ainda estará intacta. A fonte original deve ser guardada em local seguro como evidência. A cópia das informações de um disco para outro é um exemplo de preservação (Figura 3).

Figura 3: Cópia de dados de um disco rígido para outro.



Fonte: Constantino, 2012.

2. Extração: nesta fase, após realizar a preservação da fonte original, será iniciado o processo de recuperação de informação da cópia realizada. Durante a fase de extração existe a subfase de a fase de Recuperação de Arquivos. Esta subfase propriamente dita é onde os arquivos são buscados

na mídia a ser analisada. Todo tipo de arquivo possui uma assinatura no início que o identifica e diferencia. Após a busca por assinatura pode-se realizar a busca por conteúdo, pode ser o conteúdo recuperado de forma integral ou parcial.

3. Análise: a fase de análise é onde são feitos os exames nas informações recuperadas na fase de extração. Como podem ser recuperados muitos arquivos, o perito deve utilizar técnicas diversas a fim de facilitar a filtragem pela informação necessária. O principal objetivo desta fase é identificar quem fez, quando fez, que dano causou e como foi realizado o incidente/crime. A partir disso o perito deve-se fazer várias perguntas a fim de se obter as informações necessárias.
4. Formalização: na última fase o perito elabora um documento, o laudo, com os resultados encontrados em toda a análise. Esse documento, ou laudo pericial, é um documento técnico-científico deve ser extremamente detalhado e objetivo, para que o mesmo não gere dúvidas quanto à sua veracidade.

3.6. CONCEITO DE SOFTWARE LIVRE

Atualmente a informática está presente em praticamente todos os setores das mais diversas atividades onde são utilizados diversos *softwares* e sistemas operacionais de diferentes empresas que satisfazem as necessidades dos usuários, seja para trabalhar, estudar ou para lazer. No entanto, poucas pessoas se atentam para o fato de que por trás destes sistemas existem licenças de uso que regulamentam estes programas, onde o não cumprimento destes regulamentos podem gerar processos e condenações.

Segundo o Guia Livre (BRASIL, 2018, p. 27), a definição de *Software* Livre é a seguinte:

> Software Livre é o software disponibilizado, gratuitamente ou comercializado, com as premissas de liberdade de instalação; plena utilização; acesso ao código fonte; possibilidade de modificações e aperfeiçoamentos para necessidades específicas; distribuição da forma original ou modificada, com ou sem custos.

O *Software* Livre proporciona benefícios econômicos maiores do que o licenciamento de *software*. A confiabilidade dos *Softwares* Livres proporcionam

reduções de custos operacionais e a disponibilidade de código-fonte permite a adaptação dos sistemas as necessidades dos usuários. O estudo do código-fonte do programa de código aberto ainda permite condições de aprendizagem que são inviáveis com o *software* fechado (BRASIL, 2018).

O Exército Brasileiro é uma das principais instituições brasileiras que utilizam o *Software* Livre. Segundo o Plano para Migração para *Software* Livre no Exército Brasileiro, um dos grandes objetivos do EB em relação a área de Tecnologia da Informação (TI) é a adoção de soluções livres ou abertas, cuja implantação é considerada definitiva, e a sua utilização deve ser um objetivo permanente para todas as unidades do exército (BRASIL, 2018).

3.7. SEGURANÇA DIGITAL NO EXÉRCITO BRASILEIRO

Conforme a END (BRASIL, 2018), o EB ficou responsável pela área cibernética em relação à Defesa Nacional. Para cumprir esse objetivo o EB publicou e criou diversas legislações, normas e cartilhas a fim de orientar a instituição para esta atividade fim. Entra as principais legislações podemos destacar a EB10-IG-01.014 (Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro), IR 13-09 (Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro), IR 13-15 (Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro) e Cartilha Emergencial de Segurança do Departamento de Ciência e Tecnologia.

Além disso, o EB preocupou-se em adotar o *Software* Livre como objetivo institucional a fim de incrementar a segurança e diminuir custos, conforme explanado no capítulo 3.6.

Porém, mesmo após análise de toda legislação citada acima e em legislações listadas no REPUBLEx 2018 referentes à Tecnologia da Informação e Comunicações, não foram encontradas orientações técnicas ou legais referentes à Análise Forense Computacional, abrindo espaço para a realização do trabalho em questão.

4. RESULTADOS E DISCUSSÃO

Atráves de pesquisas realizadas na bibliografia referenciada, foi possível levantar e descrever os principais sistemas e ferramentas de Análise Forense Computacional em utilização, apresentando suas principais características e finalidade de uso.

4.1. TIPOS DE SISTEMAS E FERRAMENTAS PARA ANÁLISE FORENSE DIGITAL

Para melhor entendimento, podemos dividir os sistemas e ferramentas para perícia forense digital em Distribuições e *Toolkits*.

4.1.1. Distribuições

Um Sistema Operacional é o sistema que trata da operação básica do computador. É ele o responsável pela coordenação do funcionamento de todos os componentes de *hardware* (unidades de disco, placas de rede, som, vídeo, portas seriais, USB, etc), e também dos componentes de *software.* O Sistema Operacional GNU/Linux, por exemplo, é apenas o núcleo de um Sistema Operacional. Além do núcleo, há vários outros componentes, como o *shell*, que faz a interface com o usuário e um enorme conjunto de programas utilitários que formam o Sistema Operacional propriamente dito (PRUDENTE, 2018).

A Distribuição ou “distros”, nada mais é que um conjunto que integra Sistema Operacional e aplicativos, previamente configurados, com ferramentas próprias para facilitar a instalação e desinstalação de novos aplicativos. Por serem compostas por *softwares* livres, cada distribuição tem total liberdade de escolher qual o melhor conjunto de aplicativos e configurações. Cada distribuição tem um objetivo em mente, por exemplo, algumas são direcionadas a aplicações profissionais, como servidores *web* ou computação científica, outras são direcionadas a programadores, outras a jogos, análise forense computacional, entre outros.

Conforme Vieira (2018), podemos citar o *Helix*, FDTK e CAINE como principais distribuições de *Software* Livre para Análise Forense Computacional. Uma distribuição para forense computacional geralmente contém várias ferramentas e *toolkits*.

4.1.2. Toolkits

Toolkit é um único programa utilitário, um conjunto de rotinas de *software* ou um conjunto integrado completo de utilitários de *software* que são usados para desenvolver e manter aplicativos e bancos de dados. Existem kits de ferramentas de *software* para diversos fins, incluindo a perícia digital. Vieira (2018), cita o *Sleuth Kit*, *The Coroner's Toolkit* e o Xplico como os principais *toolkits* baseados em Software Livre para Análise Forense Digital. Uma distribuição pode conter vários *toolkits*.

4.2. ANÁLISE DAS DISTRIBUIÇÕES GNU/LINUX

As principais distribuições baseadas em *Software* Livre para Análise Forense Computacional serão dissecadas nesse capítulo.

4.2.1. FDTK

O *Forense Digital ToolKit* (FDTK) é uma distribuição GNU/Linux baseada em na distribuição GNU/Linux *Ubuntu* criada no idioma português. O FDTK é um projeto que possui um kit com mais de uma centena de ferramentas utilizada para realização de testes, coletas e análises em perícia forense computacional. Possui uma interface gráfica amigável para que o usuário conte com ferramentas forenses de fácil utilização e acessibilidade. O usuário pode instalar a distribuição na sua máquina ou utilizar como *Live-CD*, rodando diretamente da mídia sem necessitar de instalação. Pode realizar análises com o computador alvo desligado (*Post Mortem*) e em equipamentos ligados (*Live Analysis*). Atualmente se encontra na versão 3.0 sempre atualizada pela comunidade Linux e Software Livre (FDTK, 2018).

Figura 4: Tela inicial do FDTK.

Fonte: FDTK, 2018.

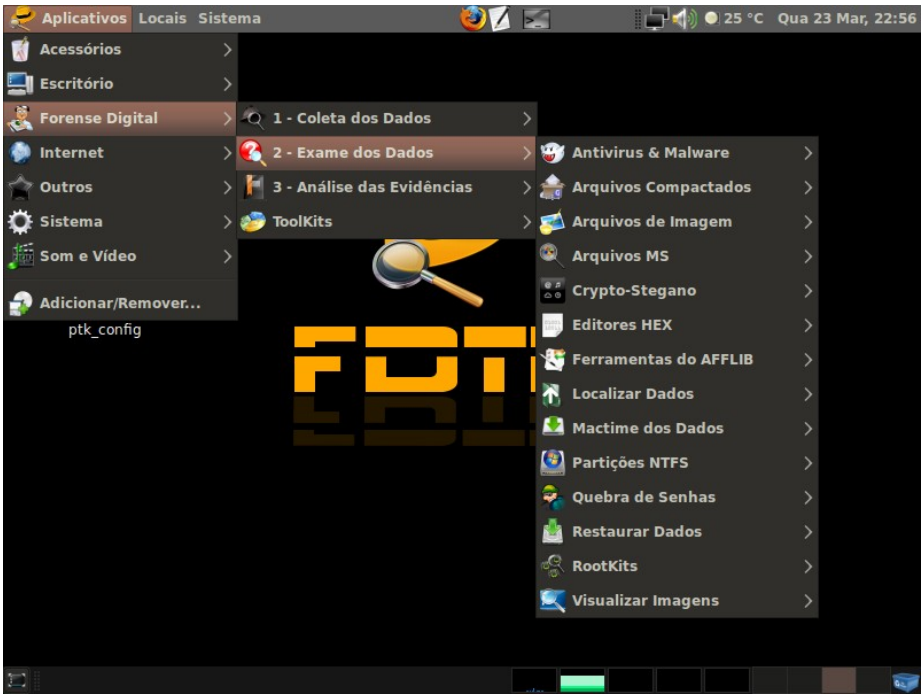
Conforme o site do FDTK, as principais ferramentas de sua distribuição são as seguintes:

- Fase de Coleta: Formulário de Cadeia de Custódia, *gnome-screenshot, aimage, air, dc3ddgui, dcfldd, dd, ddrescue, mondoarquive, mondorestore, rdd, rddi, sdd, memdump, md5sum, sha1sum, discover, hardinfo, lshw-gráfico, sysinfo e wipe*.

- Fase de Exame: *cabextract, 7zip, unace, unrar-free, unshield, xarchiver, zoo, dcraw, exif, exifprobe, exiftran, exiftags, exiv2, dumpster, fccu-docprob, mdb-hexdump, readpst, reglookup, bcrypt, ccrypt, stegcompare, stegdimage, stegdetect, xsteg, ghex2, hexcat, ghexdump, affcat, afcompare, afinfo, afstats, afxml, dcat, glark, slocate, mac-robber, mactime, ntfscat, ntfscluster, fcrackzip, john the ripper, ophcrack, fatback, foremost, magicrescue, ntfsundelete, recover, recoverjpg, scrounge-ntfs e chkrookit*.

- Fase de Análise: *coockie_cruncher, eindeutig, fccu-evtreader, galleta, GrocEVT, mork, pasco, rifiuti, xtraceroute e autopsy*.

Figura 5: Menu de ferramentas inicial do FDTK.



Fonte: FDTK, 2018.

4.2.2. Helix

Distribuição que se baseava na distribuição GNU/Linux *Knoppix* até setembro de 2008, quando uma nova versão baseada na distribuição GNU/Linux *Ubuntu* foi lançada, em formato *Live-CD*. Uma de suas principais características é que não há necessidade de *swap* de disco e não inicializa o disco rígido, garantindo a integridade do disco a ser analise para criação e análise de imagens a partir de sistemas desligados. Atualmente, a versão mais nova do *Helix* (3.0) está com propriedade da empresa *e-Fense*, que atualmente o comercializa (Santos, 2018).

Esta distribuição possui um kit de ferramentas básico que inclui o *Wireshark*, analisador de rede e *sniffer* de pacotes, ferramentas antivírus, recuperadores de senhas, ferramentas para backup e restauração de partições lógicas, visualizador de partições MAC e examinador de arquivos binários. Outras ferramentas inclusas no Helix são: *The Sleuth Kit, dc3dd, dcfldd, LinEn, aimage, FTK Imager, mdd, win32dd, winen, WFT e IRCR*.

Figura 6: Tela inicial do Helix.

Fonte: Helix, 2018

4.2.3. CAINE

O CAINE (*Computer Aided INvestigative Environment*) é uma distribuição *Live-CD* focada em forense digital GNU/Linux, originalmente desenvolvida na Itália. Na última versão lançada (9.0), a distribuição oferece um ambiente forense completo, organizado para integrar ferramentas de *software* existentes com módulos de *software* em uma interface gráfica amigável para o usuário (SANTOS, 2018).

Figura 7: Tela inicial do CAINE.

Fonte: CAINE, 2018.

Dentre as principais ferramentas existentes no CAINE, podem-se destacar as seguintes: *Remote Filesystem Mounter, netdiscover, iphonebackupanalyzer, exiftool phil harvey, tcpflow, tshark, mdbtool, tcpdump, QuickHash, FRED, docanalyzer, knowmetanalyzer, grokevt, nmap, blackberry tools, IDevice tools, AIR 2.0.0, Autopsy, Afflib, Bloom, ByteInvestigator, Cryptcat, Chntpw, Disk Utility, dos2unix, Ddrescue, Dcfldd, dc3dd, Dvdisaster, Exif, Foremost, FileInfo, Fundl 2.0, FKLook, Fatback, Guymager, HDSentinel, Hex Editor, HFSutils, Lnk-parse, Log2Timeline, NBTempo, Offset_Brute_Force, Pasco, Reglookup, Readpst, SFDumper 2.2, SSDeep, SSHFS and SMBFS, Stegbreak, Steghide, TheSleuthKit, Wipe, Xhfs, XNView, XMount e XSteg*.

4.3. ANÁLISE DOS TOOLKITS

4.3.1. The Coroner's Toolkit

The Coroner's Toolkit – TCT é uma coleção de utilitários para forense computacional desenvolvidos por *Wietse Venema* e *Dan Farmer*. A apresentação inicial ocorreu em 1999 no IBM *T.J. Watson Research Center.* A primeira distribuição geral ocorreu em 2000. O *toolkit* foi ampliado em por *Brian Carrier* que disponibilizou a própria versão no *The Sleuth Kit* (VIOTTI, 2005).

O comando *grave-robber* obtêm informações para análise forense e pode ser usado em uma máquina alvo em funcionamento ou numa imagem de disco de um sistema de arquivos sob investigação. Em análises de sistemas em funcionamento o programa procura respeitar a ordem de volatilidade buscando informações, a partir de vários utilitários do TCT, na seguinte ordem:

- atributos de todos os comandos e arquivos que o TCT acessa para obter as informações. Isso é feito primeiro para preservar as respectivas marcas de tempo;
- informações sobre o estado dos processos e, opcionalmente, a memória dos processos em execução;
- arquivos apagados que ainda estão ativos;
- os arquivos executáveis de todos os processos;
- todos os atributos dos arquivos apagados;
- informação sobre o estado da rede;

- informação sobre o estado do *host*, por meio de comandos específicos que fornecem informações sobre a configuração do sistema;
- Atributos dos arquivos existentes; produzindo o corpo do arquivo (*body*) que é usado pela ferramenta *mactime* descrita mais abaixo;
- opcionalmente, informações sensíveis a segurança do sistema controladas pelos usuários, tais como arquivos que permitem acesso remoto a conta do usuário e relativos às tarefas automatizadas programadas pelos usuários.
- cópia dos arquivos de configuração e outros arquivos críticos;

Toda essa informação é armazenada em um “recipiente”, uma estrutura de diretório protegida nomeada com o nome do *host* e o horário de início da obtenção dos dados. Para cada arquivo armazenado no recipiente o *grave-robber* calcula o *hash* MD5. No final, com o recipiente fechado, é calculado o *hash* MD5 de cada arquivo de com os *hashes* individuais.

O comando *mactime* gera um relatório cronológico de todos os acessos aos arquivos a partir das informações dos atributos desses arquivos presentes no arquivo “*body”* produzido pelo *grave-robber*. De forma alternativa o *mactime* pode produzir o arquivo “*body*” no momento da sua execução, enquanto varre o sistema de arquivos.

O *lazarus* é um programa simples cujo objetivo é conferir aos dados sem estrutura uma forma para que possam ser visualizados e editados. Os sistemas de arquivos modernos minimizam o tempo de acesso aos arquivos mantendo próximas informações semelhantes (VIOTTI, 2005). Dentre outras coisas, isso reduz a fragmentação de arquivos individuais. O *lazarus* usa essa característica e outros princípios e heurísticas na tentativa de reconstruir a estrutura do conteúdo de arquivos apagados.

O TCT vem com utilitários que desconsideram a camada do sistema de arquivos. Isso possibilita ao aplicativo acessar arquivos existentes bem como informações de arquivos apagados. Em vez de nomes de arquivos esses programas usam a abstração dos números de *inode* e a representação de alocação de blocos ou mesmo a abstração mais baixa de números de blocos no disco.

O TCT suporta sistemas de arquivos populares no mundo UNIX como UFS (BSD e Solaris) e EXT2FS/EXT3FS/EXT4FS (Linux). O *Sleuth Kit* adiciona suporte adicional que inclui os sistemas de arquivos NTFS, FAT16 e FAT32. Os utilitários para sistema de arquivos do TCT original são (PORCUPINE, 2018):

- *ils* – Acessa os atributos dos arquivos pelo número do *inode*. Por padrão, também são listados os atributos de arquivos não alocados.
- *icat* – Acessa o conteúdo dos arquivos pelo número do *inode*. É o comando preferencial para pesquisar conteúdo de arquivos apagados.
- *unrm* – Acessa blocos do disco pelo número do bloco do disco. Por padrão ão lidos todo o conteúdo de arquivo não alocado e produzida saída para uso dos programas como o *lazarus*.

As ferramentas de baixo nível para memória são mais apropriadas para uso exploratório do que análises consistentes. A razão para isso é que a saída que produzem contem pouca ou nenhuma informação sobre a estrutura, de forma que é adequada apenas para processamento por ferramentas que não fazem uso dessas informações.

- *pcat* – descarrega a memória de um processo em execução.
- *memdump* – descarrega a memória do sistema procurando evitar alterações na mesma. A saída deve ser enviada pela rede para evitar a interação com o cache do sistema de arquivos.

4.3.2. The Sleuth Kit

O (*The Sleuth Kit*) TSK é um *toolkit* baseado no sistema operacional UNIX desenvolvido por *Brian Carrier* e disponibilizado pela primeira vez no início do ano de 2001. Conforme Porcupine (2018), é o sucessor do The Coroner's Toolkit, que teve suas ferramentas incorporadas. TSK é um conjunto de inúmeras ferramentas de linha de comando que possibilitam a análise de discos e sistemas de arquivos a procura de evidências. O *Autopsy* é uma interface gráfica (GUI) para as ferramentas do TSK que pode ser usada para facilitar a análise. O TSK é composto por ferramentas de linha de comando organizadas em grupos, incluindo ferramentas de disco, de volume, de sistema de arquivos e de pesquisa (VIOTTI, 2005).

Figura 8: Tela do *Sleuth Kit*.

Fonte: Sleuth Kit, 2018.

O *diskstat* fornece estatísticas sobre o disco rígido. Ela pode ser usada por exemplo, para pesquisar a *Host Protected Area* – HPA antes de copiar dados de um disco. A ferramenta mostra o número total de setores e quais os setores acessíveis pelos usuários, permitindo concluir se existe a HPA. O comando *disksreset* remove temporariamente a HPA se ela existe. Depois que o disco é reiniciado a HPA retornará (SLEUTH, 2018).

O conteúdo de um disco rígido é organizado em volumes e o TSK inclui uma ferramenta para listar a organização das partições dos volumes. O comando *mmls* suporta partições DOS, APPLE, BSD, SUN e GPT. O tipo da tabela de partições pode ser especificado na linha de comando usando o parâmetro "–t". A saída do *mmls* é ordenada pelo endereço inicial da partição, independente da posição dela na tabela. Também é mostrado quais os setores no volume não estão associados a uma partição. Dentro da maioria dos volumes existe um sistema de arquivos. Grande parte do TSK destina-se ao sistema de arquivos. As ferramentas para o sistema de arquivos do TSK são baseadas nas ferramentas do *The Coroner's ToolKit* – TCT. As principais ferramentas do TSK são listadas na Figura 9.

Conforme o site do TSK (2018), as ferramentas atuais funcionam com partições reais ou imagens de disco. As ferramentas para o sistema de arquivos suportam os formatos EXT2/3/4 FAT, NTFS, UFS1/2. Elas também permitem visualizar páginas individuais do conteúdo real do disco e de partições *swap*. O tipo do sistema de arquivos deve ser especificado com o parâmetro "–f" seguido de um dos tipos informados antes (entre parênteses). As principais ferramentas do *The Sleuth Kit* são os seguintes: As ferramentas para pesquisa incluem o *hfind* (pesquisa *hashes* nas bibliotecas NIST/NSRL, *Hashkeeper* e numa base de dados personalizada criada com o *md5sum*), *mactime*, *sorter* (ordena os arquivos de acordo com o tipo e realiza verificações e pesquisa em bases de *hash*) e o *sigfind* (pesquisa por um valor binário num local específico).

Figura 9: Principais ferramentas do *The Sleuth Kit*.

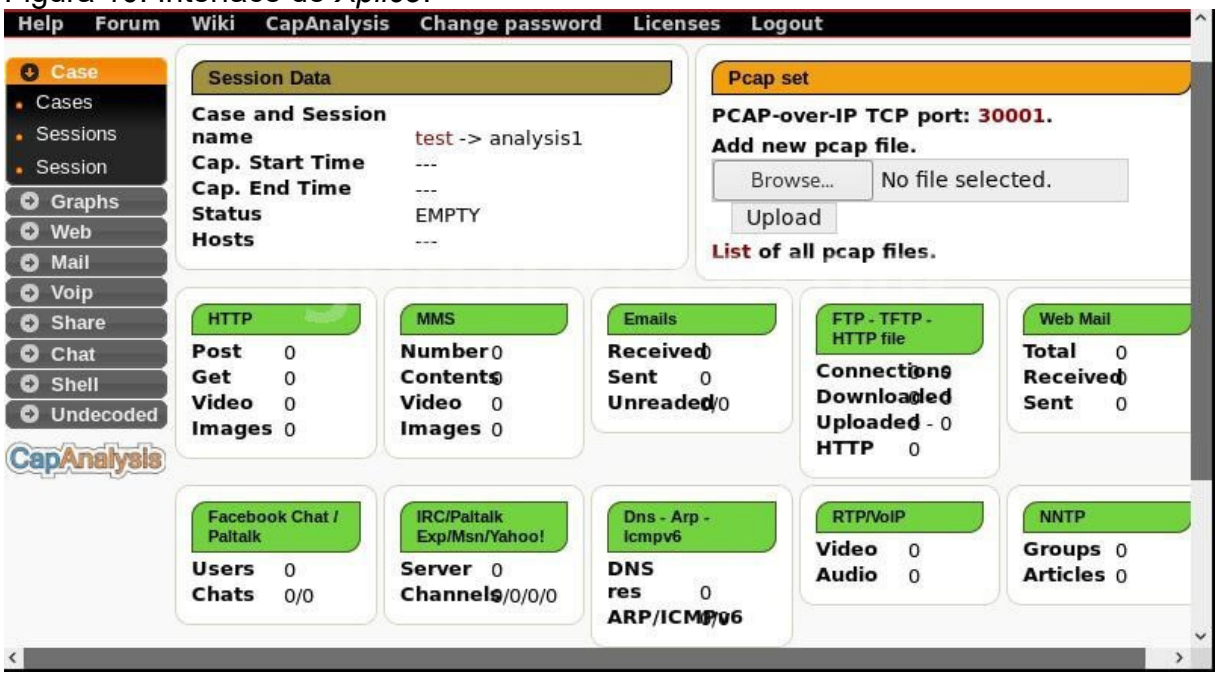
Nome	Descrição
`fsstat`	Mostra estatísticas do sistema de arquivos(e.g. estrutura, tamanho e rótulo).
`ffind`	Encontra nomes de arquivos alocados ou não que apontam para uma determinada estrutura de dados.
`fls`	Lista nomes de arquivos alocados e apagados de um diretório.
`icat`	Extrai unidades de dados de um arquivo, indicado pelo *inode* (no lugar do nome do arquivo).
`ifind`	Encontra a estrutura de meta dados cujo nome de arquivo aponta para ela ou a estrutura de meta dados que aponta para uma unidade de dados.
`ils`	Lista a estrutura e o conteúdo de meta dados.
`istat`	Mostra estatísticas e detalhes sobre uma estrutura de meta dados em um formato de fácil leitura.
`dcat`	Extrai o conteúdo de uma unidade de dados.
`dls`	Lista os detalhes sobre unidades de dados, podendo extrair o espaço não alocado ao sistema de arquivos.
`dstat`	Mostra estatísticas sobre uma unidade de dados num formato claro.
`dcalc`	Calcula a posição dos dados existentes numa imagem encontrados no espaço não alocado (obtidos com o dls). É útil quando uma evidência é encontrada no espaço não alocado.
`jcat`	Mostra o conteúdo de um bloco específico do *journal*.
`jls`	Lista as entradas na base de *journal* do sistema de arquivos.

Fonte: Viotti, 2005.

4.3.3. Xplico

O objetivo do *Xplico* é capturar o tráfego de rede e dados de aplicativos. O *Xplico* trabalha, por exemplo, a partir de um arquivo *.pcap* (arquivo de dados, que contém dados de pacotes de rede) o *Xplico* extrai de cada e-mail (POP, IMAP e SMTP), todo o conteúdo HTTP, cada chamada VoIP (SIP), FTP, TFTP, e assim por diante (XPLICO, 2018).

Figura 10: Interface do *Xplico*.



Fonte: Xplico, 2018.

O *Xplico* não é um analisador de protocolo de redes como o *Wireshark*, por exemplo, ele é uma fonte de Análise Forense de Rede baseada em *Software* Livre. É distribuído sob a GNU e com alguns *scripts* sob *Creative Commons.* Algumas das características mais importantes deste software são listadas a seguir:

- Protocolos suportados: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, entre outros;
- Porta Independente Protocolo de Identificação (PiPi) para cada protocolo de aplicação;
- *Multithreading*;
- Saída de dados e informações em banco de dados SQLite ou banco de dados MySQL e/ou arquivos;
- TCP ACK remontagem com a verificação de qualquer pacote;

- A consulta reversa do DNS dos pacotes DNS contidas nos arquivos de entradas (CPPE), não do servidor DNS externo;
- Não há limite de tamanho para entrada de dados ou o número de arquivos de entrada (o único limite é o tamanho HD);
- Suporte a IPv4 e IPv6;
- Modularidade. Cada componente *Xplico* é modular. A interface de entrada, o decodificador do protocolo e a interface de saída (*dispatcher*) são todos os módulos.

5. CONCLUSÃO

A humanidade atualmente depende das informações para o funcionamento das estruturas que dão suporte as atividades cotidianas. Com isso, os sistemas digitais constituem a infraestrutura por onde dados e informações são obtidos, processados, armazenados e transmitidos.

Como esses sistemas digitais são a base das organizações, é necessário cuidar da segurança da informação desses sistemas, para os que os mesmos sejam confiáveis. O gerenciamento da segurança desses sistemas deve ser um processo contínuo e abrangente de avaliação de riscos e controles para minimizá-los. Nestes processos estão incluídos os tratamentos de incidentes e crimes virtuais que venham a ocorrer, com o objetivo de reavaliar os riscos e as causas que o possibilitaram. Isso pode ser feito através da perícia forense computacional.

Conforme a perícia forense computacional vem se desenvolvendo, novas ferramentas são criadas para atender às diversas etapas que compõem sua metodologia. Muitas dessas ferramentas são proprietárias, porém a utilização de *Softwares* Livres vem crescendo cada vez mais tanto pelos peritos forenses, quanto por usuários comuns.

O EB, que tem como missão constitucional a Defesa Cibernética, delfinada na Estratégia Nacional de Defesa e que tem como objetivo permanente a adoção de *Software* Livre, precisa conhecer as principais ferramentas utilizadas para a forense computacional, por se tratar de importante método no gerenciamento da segurança da informação.

Para aplicar esses métodos e procedimentos de perícia forense, são necessárias ferramentas específicas para cada plataforma ou flexíveis o suficiente

para adaptarem-se às diversas estruturas diferentes existentes no EB. Conforme visto no Capítulo 4, as ferramentas de Software Livre surgem como alternativa preferencial para as investigações digitais.

O objetivo suscitado por este trabalho foi a busca e avaliação de ferramentas baseadas em *Software* Livre usadas na perícia forense computacional, com o intuito de comparar os principais atributos das ferramentas para sua atividade-fim.

Através da pesquisa, pode-se perceber que a distribuição FDTK, abordada no capítulo 4.2.1 é a ferramenta mais indicada para a perícia digital, pois pode ser usada para realizar a investigação sem a necessidade de instalação, podendo realizar perícia em equipamentos ligados (*Live Analysis*) e em equipamentos desligados (*Post Mortem)*, além de possuir muitas ferramentas inclusas por padrão em sua distribuição. Como suplementação e com o objetivo de acrescentar funcionalidades, recomenda-se a instalação do *Sleuth Kit*, que se trata de um *toolkit* que inclui ferramentas adicionais mais completas para a análise de disco e o *Xplico*, utilizado para análise de rede.

Portanto, a principal contribuição deste trabalho foi apresentar e tornar conhecidas as principais ferramentas utilizadas na perícia computacional forense, bem como informar suas principais características. Como contribuição ao EB, o trabalho pretende orientar aos possíveis militar e civis envolvidos em alguma investigação digital, qual a ferramenta e aplicativos recomendados para a perícia computacional.

REFERÊNCIAS

ALMEIDA, Rafael Nader de. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais**. 2011. Monografia - Faculdade de Tecnologia de São Paulo, 2011.

BRASIL. Comando do Exército Brasileiro. **REPUBLEx 2018**. Relação das Publicações do Exército. Portaria Nº 124-SGEx, de 29 de março de 2018. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/boletins.php>. Acesso em: 15 Set 2018.

BRASIL. Comando do Exército Brasileiro. **Cartilha de Segurança nas Redes Sociais**. Disponível em: <http://www.enadciber.eb.mil.br/images/manuais/Livreto_R_Sociais.pdf>. Acesso em: 15 Set 2018.

BRASIL. Comando do Exército Brasileiro. **Plano de migração para Software Livre no Exército Brasileiro**. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=788&act=bre>. Acesso em: 15 Set 2018.

BRASIL. **Guia Livre**. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/E15_469GuiaLivre_v099.pdf>. Acesso em: 15 Set 2018.

BRASIL. Ministério da Defesa. **PND/END**. Política Nacional de Defesa e Estratégia Nacional de Defesa. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 15 Set 2018.

CAINE. **Computer Aided INvestigative Environment**. Disponível em: <https://www.caine-live.net/>. Acesso em: 15 Set 2018.

CONSTANTINO, Diego Zaratini. **Técnicas da Computação Forense**. 2012. 67f. Trabalho de Conclusão de Curso – Fundação Educacional do Município de Assis, 2012.

HELIX. **A Linux Forensics Corkscrew**. Disponível em: <https://www.dedoimedo.com/computers/helix.html>. Acesso em: 15 Set 2018.

FDTK. Forense Digital Toolkit. Disponível em <http://fdtk.com.br/www/>. Acesso em: 15 Set 2018.

FILHO, Wilson Leite da Silva. **Crimes Cibernéticos e Computação Forense**. XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2016, Págs. 44-81, 2016.

GOVERNO DO ESTADO DE GOIÁS**. Plano de Migração para o Software Livre**. Governo do Estado de Goiás, 2007.

HARLEY, Maurício. **Análise Forense Computacional – Referências**. Disponível em: <https://itharley.com/analise-forense-computacional-referencias/>. Acesso em: 10 Jul 2018.

MELO, Sandro. **Computação Forense com Software Livre**. Rio de Janeiro: Alta Books, 2009. 1ª edição.

PRUDENTE, Fábio. **O que é uma distribuição Linux?**. Disponível em: <http://fprudente.blogspot.com/2009/03/o-que-e-uma-distribuicao-linux.html>. Acesso em: 15 Set 2018.

PORCUPINE. **The Coroner's Toolkit**. <http://www.porcupine.org/forensics/tct.html>. Acesso em: 16 Set 2018.

QUEIROZ, C.; VARGAS, R. **Investigação e Pericia Forense Computacional**: Certificações, Leis Processuais, Estudos de Caso. Rio de Janeiro: Ed. Brasport, 2010.

SANTOS, Laudelino Azevedo dos. **Computação Forense em Sistemas GNU/Linux**. 2008. 54f. Monografia - Universidade Federal de Lavras, 2008.

SANTOS, Rodrigo Franco dos. **Ferramentas de Computação Forense Baseadas em Software Livre**. Disponível em: <https://docplayer.com.br/4051996-Ferramentas-de-computacao-forense-baseadas-em-software-livre.html>. Acesso em: 15 Set 2018.

XPLICO. **Xplico, a Open Source Network Forensic Analysis Tool (NFAT)**. Disponível em: <https://www.xplico.org/>. Acesso em: 16 Set 2018.

SILVA, Vinícius Amorim; DE OLIVEIRA, Cleber Henrique. **Análise de Ferramentas Livres para Perícia Forense Computacional**. Caderno de Estudos Tecnológicos da Faculdade de Tecnologia de Bauru, Volume 02, Número 01, Págs. 110-132, Julho/2014.

Sleuth Kit. **The Sleuth Kit**. Disponível em: <https://www.sleuthkit.org/>. Acesso em: 16 Set 2018.

VIEIRA, Luiz. **Forense Computacional com Software Livre**. Disponível em: <https://www.4linux.com.br/noticia/palestra-de-forense-computacional-com-software-livre-em-semana-academica>. Acesso em: 15 Set 2018.

VIOTTI, Alberto Luiz Alves. **Possibilidades de Uso de Software Livre como Ferramentas de Análise em Investigações Digitais**. 2005. 82f. Monografia - Universidade Federal de Lavras, 2005.