ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO

Cap QCO Infor Lamartine de Oliveira Medeiros

ANÁLISE DE FERRAMENTAS *OPEN SOURCE* UTILIZADAS PARA A PERÍCIA FORENSE COMPUTACIONAL

Brasília
2020

Cap QCO Infor Lamartine de Oliveira Medeiros

ANÁLISE DE FERRAMENTAS *OPEN SOURCE* UTILIZADAS PARA A PERÍCIA 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 Infor ANDERSON BARROS TORRES

Brasília
2020

ANÁLISE DE FERRAMENTAS *OPEN SOURCE* UTILIZADAS PARA PERÍCIA FORENSE COMPUTACIONAL

Lamartine de Oliveira Medeiros[a]
Anderson Barros Torres[b]

RESUMO

Com o avanço da tecnologia, os ataques cibernéticos aumentaram em número e gravidade. Umas das respostas a estes tipos de ataques são as perícias forenses computacionais, que ajudam na investigação e na recuperação das evidências deixadas pelos criminosos. A investigação realizada pela forense computacional inclui a perícia em computadores e dispositivos de armazenamento, dispositivos móveis, banco de dados e memórias *RAM*, redes de computadores e análise de dados. Nesse contexto, o estudo busca avaliar a aderencia das ferramentas, procedimentos e metodologias utilizadas no Exército Brasileiro com as melhores práticas e tecnologias de investicação digital. A metodologia emprega uma pesquisa de campo junto ao 7º Centro de Telemática de Área (7º CTA) e ao Núcleo de Perícia Forense do Centro de Defesa Cibernética (CD Ciber), além de pesquisa bibliográfica em bibliotecas digitais. O trabalho concluiu que a questão normativa e metodológica do Exercito Brasileiro estão de acordo com os padrões nacionais e internacionais de perícia computacional forense, no entanto existem oportunidades de melhorias quanto às ferramentas utilizadas nas unidades pesquisadas.

Palavras-chave: *Open Source*, Perícia Forense Computacional, Cibernética

ABSTRACT

With the advancement of technology, cyber attacks have increased in number and severity. One of the responses to these types of attacks is computer forensic expertise, which helps in investigating and recovering evidence left by criminals. The investigation carried out by computer forensics includes expertise in computers and storage devices, mobile devices, databases and RAM memories, computer networks and data analysis. In this context, the study seeks to assess the adherence of the tools, procedures and methodologies used in the Brazilian Trade with the best practices and technologies of digital research. The methodology employs field research at the 7th Area Telematics Center (7th CTA) and the Center for Forensic Expertise at the Cyber Defense Center (CD Ciber), in addition to bibliographic research in digital libraries. The work concluded that the normative and methodological question of the Brazilian Army are in accordance with the national and international standards of computer forensic expertise, however there are opportunities for improvement regarding the tools used in the units surveyed..

Keywords: Open Source, Computer Forensic Expertise, Cybernetics

---

[a] Especialista em Guerra Cibernética pelo Centro Integrado de Guerra Eletrônica em 2017.

[b] Mestre em Ciência da Informação pela Universidade de Brasília em 2005.

SUMÁRIO

1. INTRODUÇÃO

Com o avanço da tecnologia e a criação e propagação da Internet, ocorreu uma expressiva transformação no modo como as pessoas interagem. Distâncias foram encurtadas, a condução de negócios tornou-se menos burocrática, e o acesso as informações e a possibilidade de entretenimento de forma *on-line* permitiu a entrada na chamada Era Digital. (MABEY, 2017)

A evolução da tecnologia computacional contribui para o desenvolvimento social, no entanto, veio acompanhada de inúmeros incidentes, como infrações, invasões, pirataria, tentativas de acessos indevidos a organizações ou até mesmo a pessoas comuns. Essas práticas são constantemente aprimoradas, e com isso, há a necessidade do auxílio de ferramentas mais modernas para a busca e identificação dos infratores (VARGAS, 2011).

No contexto do Exército Brasileiro (EB) a preocupação com o Setor Cibernético tornou-se o principal ponto estratégico da Instituição, conforme estabelecido na Estratégia Nacional de Defesa (END), com o objetivo de garantir a segurança do espaço cibernético brasileiro (BRASIL, 2008).

A atividade de Perícia Forense Computacional (PFC) a ser realizada internamente, quando solicitada, faz parte das atividades dos Centros de Telemática de Área (CTA) e dos Centros de Telemática (CT) em virtude da peculiaridade das informações que compõem a rotina do EB.

A problemática proposta pelo estudo é: O 7º Centro de Telemática de Área (7º CTA) e o Núcleo de Perícia Forense do Centro de Defesa Cibernética (CD Ciber) estão aderentes quanto às normas e ferramentas adotadas, em relação às melhores praticas normativas/procedimentais e tecnologias mais utilizadas pela investigação forense?

Nesse sentido, o estudo propõe a definição de requisitos para avaliar a questão problema, ao mesmo tempo que apresenta as principais ferramentas e padrões metodológicos para a perícia forense computacional no referencial teórico discorrido no Capítulo 3.

Inicialmente o trabalho aborda o histórico da perícia forense computacional, a importância desta recente área de conhecimento humano, partindo em seguida para

tratar de aspectos legais, aspectos nos quais o trabalho do perito deve estar respaldado, e aspectos técnicos, que envolvem a metodologia e as ferramentas de apoio.

A Capítulo 4 apresenta-se os resultados da pesquisa de campo nos Setores responsáveis pela perícia no 7º Centro de Telemática de Área (7º CTA) e no Núcleo de Perícia Forense do Centro de Defesa Cibernética (CD Ciber).

No Capítulo 5 ocorre a discussão da problemática do estudo, e é desenvolvida uma análise dos aspectos levantados durante a pesquisa, em relação ao referencial teórico do estudo, de maneira a indicar se as melhores práticas e ferramentas forenses estão disponíveis e aderentes com as práticas do EB.

2.METODOLOGIA

O presente trabalho, quanto a finalidade, caracteriza-se por uma pesquisa aplicada, uma vez que procura adquirir conhecimento com o objetivo de empregar em uma situação específica. O propósito do estudo é exploratório, pois baseou-se em levantamento bibliográfico, e coleta de dados a partir de entrevistas, numa abordagem qualitativa, visando responder a questões subjetivas.

Para isso, realizou-se uma revisão teórica do assunto com uma pesquisa bibliográfica tendo como fonte acervos em bibliotecas digitais com artigos científicos, legislação e publicações literárias compreendidas nos últimos 20 anos. Além disso foi realizada uma consulta ao Portal da intranet do 1º Centro de Telemática de Área com o objetivo de obter dados referentes as Normas Técnicas e Legislação utilizada pelo Exército Brasileiro, relacionados à Perícia Forense Computacional.

Foi realizada uma pesquisa de campo com questionário estruturado e entrevistas nos setores responsáveis pela perícia no 7º Centro de Telemática de Área (7º CTA) e no Núcleo de Perícia Forense do Centro de Defesa Cibernética (CD Ciber), visando compreender a realidade de cada Organização Militar.

3. REFERENCIAL TEÓRICO

A revisão de literatura foi realizada com o intuito de reunir e expor os conceitos relativos à Perícia Forense Computacional (PFC), além de abordar de forma sucinta as

técnicas e as ferramentas livres utilizadas para a realização de uma investigação digital.

3.1 HISTÓRICO DA PERÍCIA FORENSE COMPUTACIONAL

Segundo Eleutério e Machado (2011, apud SOUZA, 2015) a Computação Forense é um conjunto de procedimentos e metodologias utilizadas que devem assegurar a validade das ações perante a justiça, com o objetivo de preservar e documentar evidências de dispositivos de armazenamento digital como computadores , PDAs, câmeras digitais, telefones celulares e vários dispositivos de armazenamento de memória.

Entre 1960 e 1980 os computadores eram considerados aparelhos industriais, em que apenas centros de pesquisa, grandes corporações, universidades e órgãos do governo operavam e tinham acesso. Estes equipamentos basicamente trabalhavam no processamento de dados (POLLITT, 2010). O autor acrescenta que o livro de Donn Parker de 1976, "*Crime by Computer"* trata sobre os primeiros registros de informações computacionais utilizadas para investigação de crimes realizados com auxílio de computadores. Nesse sentido, Prasanthi (2016) ressalta que, com a popularização dos computadores pessoais no início da década de 1980 cresceram os crimes digitais. Fato este que levou as organizações aos primeiros esforços de treinamentos em investigação computacional.

A partir de então organizações como o Departamento de Defesa Americano, o Serviço da Receita Federal dos EUA e o *Federal Bureau of Investigation* (FBI) passaram a criar grupos de agentes voluntários (POLLITT, 2010). Para o autor, esses agentes ajudariam os outros investigadores a obter dados armazenados e analisar os *logs* dos equipamentos. Segundo Pollitt (2011), faziam parte destas equipes investigadores como Jim Christy e Karen Matthews do Departamento de Defesa Americano; Ron Peters e Jack Lewis do Serviço Secreto dos EUA entre outros que se tornaram membros fundadores da *International Association of Computer Specialists* (IACIS), primeira fundação dedicada à ciência forense digital.

O termo "Computação Forense" foi utilizado pela primeira vez em 1991, em uma sessão de treinamento realizada pela IACIS em Portland, Oregon (ARTHUR e VENTER, 2004). Desde então, o assunto Computação Forense tornou-se cada vez mais popular nos grupos interessados em segurança de computadores e na

comunidade jurídica. Como qualquer outra ciência forense, a Computação Forense lida com a aplicação da lei a uma ciência. (NTI, 1996?)

Ainda na década de 1990, o uso da Internet e o aumento do consumo de tecnologias facilitaram ainda mais os ataques cibernéticos. Por conta disso a *Scientific Working Group Digital Evidence* (SWGDE) passou a desenvolver padrões para a Computação Forense (PRASANTHI, 2016). O autor ainda ressalta que o crime cibernético explode, a partir de 2000, em virtude da integração de tecnologias como os dispositivos móveis, expandindo exponencialmente os tipos de fontes primárias de tecnologia usados pela criminalidade.

Assim a Computação Forense evoluiu de técnicas investigativas para uma ciência forense completa. Tudo devido ao esforço conjunto de pesquisadores, indústria, criação de ferramentas e militares para enfrentar o desafio da Perícia Forense Computacional (PRASANTHI, 2016).

Desse modo, segundo Freitas (2003), todas as evidências precisam ser legítimas, ou seja, quando apresentadas a uma autoridade legal precisam ter validade jurídica. E isso só é possível quando o perito obedece rigorosamente os aspectos legais e técnicos de uma PFC. Na próxima seção serão abordados estes dois aspectos.

3.2 ASPECTOS TÉCNICOS E LEGAIS DA PERÍCIA FORENSE COMPUTACIONAL

De acordo com COSTA (2011 apud RAMOS, 2014) dois aspectos principais norteiam a PFC: os aspectos técnicos e os aspectos legais. Os aspectos técnicos são aos parâmetros técnicos que corresponderão às etapas ou fases da PFC. Já os aspectos legais estão ligados com a legislação envolvida. Esses dois aspectos devem estar bem alinhados, tendo em vista que uma PFC tecnicamente bem executada, porém com a inobservância dos aspectos legais inviabilizará as provas obtidas, comprometendo todo o trabalho.

Em relação aos aspectos legais, o trabalho do perito deve estar respaldado na legislação pertinente, tendo como referência básica leis, normas, decretos, políticas e diretrizes, além de documentos infra-legais (OLIVEIRA, 2018).

De de acordo com Eleutério e Machado (2011 apud ALMEIDA, 2011), o Código de Processo Penal Brasileiro (CPP) através dos seus Artigos 158º e 159º

definem respectivamente que toda investigação conduzida por autoridade competente deve iniciar pela apuração e análise dos vestígios deixados; bem como toda a atividade de perícia deve ser realizada por profissional especialista (perito) legalmente habilitado, por meio de métodos técnico-científicos, a fim de conferir-lhe validade probatória em juízo.

Além do CPP, o arcabouço legal relacionado à perícia forense abrange a seguinte relação de leis e decretos:

Tabela 1: Legislação relacionada à Perícia Forence Computacional

Competência legal	**Vinculação**
LEI Nº 13.709, de 14 de agosto de 2018.	Lei Geral de Proteção de Dados Pessoais (LGPD).
LEI Nº 12.965, de 23 de abril de 2014	Marco Legal da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
LEI Nº 12.737, de 30 de novembro de 2012	Lei Carolina Dieckman. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
LEI Nº 12.735, de 30 de novembro de 2012	Tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares
LEI Nº 12.527, de 18 de novembro de 2011	Lei de Acesso a Informação - Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal
LEI Nº 12.030, de 17 de setembro de 2009	Lei das Perícias Oficiais. Dispõe sobre as perícias oficiais e dá outras providências
LEI Nº 9.609 , de 19 de fevereiro de 1998	Lei do Software. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
DECRETO Nº 10.046, de 9 de outubro de 2019	Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
DECRETO Nº 9.637, de 26 de dezembro de 2018	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.
DECRETO Nº 8.771, de 11 de maio de 2016	Decreto Regulamentador do Marco Civil da Internet.
DECRETO Nº 7.845, de	Regulamenta procedimentos para credenciamento de segurança e

14 de novembro de 2012	tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Fonte: Adaptado de Oliveira (2018).

As normas relativas à PFC referem-se às diretrizes e procedimentos para a condução de uma investigação forense computacional, e servem de parâmetro para que as organizações responsáveis pela perícia a executem amparadas em requisitos mínimos de boas práticas, requisitos essenciais para a qualidade e eficácia do trabalho pericial.

Nesse sentido, numa abrangência nacional, destacam-se as normas NBR 16386:2015, que estabelece orientações para a interceptação telemática oriunda de ordem judicial, e a norma NBR 27037:2013, que fornece instruções para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório.

Dentro do Exército Brasileiro as normas para o planejamento e a execução do serviço de Perícia Forense Computacional, no âmbito do Sistema de Telemática do Exército (SisTEx) são reguladas pelo Anexo H - NORMAS PARA REALIZAÇÃO DE PERÍCIA FORENSE COMPUTACIONAL NO SISTEMA DE TELEMÁTICA DO EXÉRCITO (NRPFC/SisTEx), da DIRETRIZ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO SISTEMA DE TELEMÁTICA DO EXÉRCITO. (DSIC/SisTEx). (BRASIL, 2012).

O Anexo H determina que as Perícias Forenses Digitais devem ser conduzidas por militares especializados e que constituem o Centro de Coordenação para tratamento de Incidentes de Rede do Exército (CCTIR/EB) ou ainda as Seções de Tratamento de Incidentes de Rede (STIR), sendo estas últimas orgânicas do CITEx ou subseções dos Centro de Telemática de Área (CTA) e Centro de Telemática (CT). É definido também, que todas as perícias no âmbito do SisTEx devem ser executadas preconizando o previsto no Código de Processo Penal Militar (CPPM), além das normas e diretrizes aprovadas pelo Escalão Superior e pelo DSIC/SisTEx. (BRASIL, 2012)

De acordo com Adams (2000 apud VARGAS, 2011) os aspectos técnicos são definidos pelo *Scientific Working Group Digital Evidence* (SWGE), que é o órgão

norte-americano representante na *International Organization on Computer Evidence* (IOCE). Segundo o autor, esses aspectos técnicos seguem um único princípio que é manter um elevado nível de qualidade, de modo que sejam asseguradas a confiabilidade e a precisão das evidências juntamente a correta observância dos aspectos legais. Para VARGAS (2011) o nível de qualidade pode ser atingido ao serem elaborados *Standard Operating Procedures* (SOPs), que devem conter os procedimentos para todo o tipo de análise a ser realizada, observando metodologias aceitas e adotadas pela comunidade científica internacional.

A Norma Técnica da *U.S. Homeland Security* (2006) estabelece que existem cinco principais ramos da forense computacional e eles são categorizados por onde os dados estão armazenados ou como os dados são transmitidos.

Prasanthi (2016) ressalta que a PFC é enquadrada nas seguintes categorias:

a) forense de computadores – tem como foco a recuperação de evidências em computadores e dispositivos de armazenamento, como discos rígidos e memórias *flashes* por exemplo.

b) forense em dispositivos móveis – tem como alvo a recuperação e preservação de evidências digitais em dispositivos móveis, como *smartphones* e tablets.

c) forense em redes: consiste na análise do tráfego de rede.

d) forense em banco de dados e memória: estudo de banco de dados, nessa categoria se enquadram investigações em conteúdos de banco de dados, arquivos de *logs* e dados de memória *Randon Access Memory* (RAM).

e) forense em análise de dados - tem como foco a investigação a análise dos dados visando a busca de um padrão de ataque.

3.3 METODOLOGIA DA PERÍCIA FORENSE COMPUTACIONAL.

Na busca por uma padronização da metodologia relacionada à Perícia Forense Computacional, diversos organismos desenvolveram conjuntos de orientações, procedimentos e boas práticas para a atividade forense.

O *National Institute of Standards and Technology* (NIST) é um órgão norte-americano que faz parte do Departamento de Comércio dos Estados Unidos, sendo considerado um dos mais antigos laboratórios de ciências físicas do país (EUA, 2006). Este órgão publicou um Guia de Integração de Técnicas Forenses para

Respostas a Incidentes. Este Guia possui recomendações de aspectos técnicos que devem ser observadas e utilizadas para a realização de investigações de incidentes de segurança de computadores, bem como apoiar na solução de problemas operacionais de tecnologia da informação. (KENT et al., 2006)

De acordo com Kent et al. (2006), o processo de perícia digital compreende as seguintes fases básicas:

> **Coleta**: identificação, rotulagem, registro e aquisição de dados das possíveis fontes de dados relevantes, seguindo procedimentos que preservam a integridade dos dados. Cópias integrais, ou seja, contêm todos os arquivos, dados e configurações do material original que foi apreendido
>
> **Exame ou Extração**: processamento forense de dados coletados usando uma combinação de dados automatizados e métodos manuais e avaliação e extração de dados de interesse particular, preservando o integridade dos dados. Identifica e recupera arquivos que possam conter informações relevantes para a investigação, descartando dados irrelevantes (arquivos de aplicativos, sistema operacional, etc)
>
> **Análise**: análise dos resultados do exame, utilizando métodos legalmente justificáveis e técnicas, para obter informações úteis que abordem as questões que foram o ímpeto para realização da coleta e exame.
>
> **Relatório**: relatar os resultados da análise, que pode incluir a descrição das ações utilizadas, explicando como as ferramentas e procedimentos foram selecionados, determinando quais outras ações precisam ser realizada (por exemplo, exame forense de fontes de dados adicionais, proteção identificada vulnerabilidades, melhorando os controles de segurança existentes) e fornecendo recomendações para melhoria de políticas, procedimentos, ferramentas e outros aspectos do processo forense. 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).

No Brasil, a Norma ABNT ISO/IEC 27037:2013 padroniza as atividades específicas no tratamento de evidências digitais que vão desde a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório, auxilia as organizações em seus procedimentos disciplinares na facilitação de

intercâmbio de evidências digitais entre jurisdições. De maneira sintética, as fases pode ser assim descritas (OLIVEIRA, 2019):

a) Identificação: envolve a pesquisa, reconhecimento e documentação da evidência digital. Convém que durante este processo se identifique os dispositivos de armazenamento de mídia digital e os dispositivos de processamento que podem conter a evidência digital relevante para o caso

b) Coleta: consiste em recolher o dispositivo questionado de sua localização original para um laboratório ou outro ambiente controlado para posterior aquisição e análise. Deve-se observar a documentação de toda abordagem (cadeia de custódia), bem como o devido acondicionamento destes dispositivos antes do transporte.

c) Aquisição: O processo de aquisição consiste na produção da cópia da evidência digital e documentação dos métodos usados e atividades realizadas.

d) Preservaçao: Convém que a evidência digital seja sempre preservada para garantir sua integridade como “objeto” questionado. O processo de preservação envolve a guarda da potencial evidência digital assim como o dispositivo digital que pode conter a evidência digital contra espoliação ou adulteração.

Conforme leciona Eleutério e Machado (2011), o exame forense em dispositivos de armazenamento computacional também deve ser executado em quatro fases, nessa ordem: preservação, extração, análise e formalização. Em resumo, a preservação consiste basicamente em realizar o espelhamento ou imagem dos dados. Os principais procedimentos para a realização da fase de extração são a recuperação de arquivos apagados e a indexação de dados. A etapa de análise consiste em examinar os dados e informações obtidos e resultantes da etapa da coleta. Por fim, apresenta-se a formalização do resultado através da elaboração do laudo ou parecer técnico.

Assim, para que o perito construa artefatos com credibilidade através das evidências encontradas é necessário que se percorra todos os passos propostos pela metodologia e que se utilize de ferramentas adequadas. Segundo Arthur e Vender (2004) as ferramentas geralmente que dão suporte à metodologia diferem em funcionalidade, complexidade e custo. Os autores afirmam que estes três fatores

limitantes devem ser avaliados de acordo com a criticidade do crime, quando da escolha das ferramentas.

Observa-se que as etapas propostas para o desenvolvimento de padrões metodológicos e procedimentos de boas práticas para a perícia forense assemelham-se em suas fases e abordagens, sugerindo a existência de um senso comum quanto ao método de investigação judicial para crimes computacionais.

3.4 O USO DE FERRAMENTAS *OPEN SOURCE*

A evolução da tecnologia computacional contribui para o desenvolvimento social, no entanto, veio acompanhada de inúmeros incidentes, como infrações, invasões, pirataria, tentativas de acessos indevidos a organizações ou até mesmo a pessoas comuns. Essas práticas são constantemente aprimoradas, e com isso, há a necessidade do auxílio de ferramentas mais modernas para a busca e identificação dos infratores (VARGAS, 2011).

Segundo Kyk (2017) a literatura classifica as ferramentas em comerciais e não-comerciais, ou licenciados e *open source*. O autor ainda afirma que ferramentas comerciais normalmente são desenvolvidas para plataforma Windows com diversos módulos integrados em um único programa, sendo bastante caras. Já as ferramentas não-comerciais funcionam em Linux que as origens das PFC não estão ligadas ao Windows, mas sim aos sistemas UNIX, que possuem suas raízes no início da década de 1970.

Para ALTHEIDE e CARVEY (2011) o uso de ferramentas *open source*, em comparação às ferramentas licenciadas, possui os seguintes benefícios:

a) aprendizagem – usar ferramentas de código aberto para aprender PFC tem seus benefícios. Elas permitem que as opções e a saída sejam examinadas e o principal é possível observar a lógica da ferramenta para chegar a determinado resultado.

b) portabilidade e flexibilidade – outro benefício é que grande parte dessas ferramentas são portáteis e flexíveis. Por portátil, entende-se que o kit de ferramentas pode facilmente ser levado de um sistema para outro ou de um trabalho para outro. Ou seja, não há perda de conhecimento caso o perito troque de empresa. Nesse contexto, enquanto portabilidade significa poder escolher onde usar as

ferramentas necessárias; flexibilidade significa como usar essas ferramentas. As ferramentas *open source* podem ser utilizadas no próprio sistema a ser examinado ou instaladas em um servidor e acessadas remotamente. Elas ainda podem ser instaladas em um único sistema ou em vários. E tudo isso pode ser feito sem precisar solicitar a permissão do fornecedor do *software*, sem preencher um pedido de compra e sem precisar integrar uma licença de *software* a um determinado *hardware*.

c) custos – além de serem *open source,* essas ferramentas em sua maioria são *softwares* livres de custo. Isso possibilita que o perito possa montar um kit de ferramentas sem nenhum custo. E mesmo que se utilize ferramentas comerciais, as de código livre podem complementar alguma lacuna de cobertura ou validar alguma descoberta realizada.

A PFC necessita de ferramentas para apoiar o trabalho do perito em todas as suas fases e,de acordo com as recomendações propostas por Kent et al. (2006), seriam as fases de coleta, extração, análise dos dados investigados e relatório. As ferramentas podem ser específicas para determinada fase, ou ainda abranger mais de uma fase, incorporando diversas funcionalidades e programas em um único produto, permitindo agilizar o trabalho pericial.

De acordo com Kiper (2020), dentre os requisitos técnicos relevantes para a seleção de ferramentas, deve ser levado em consideração:

> a) habilidade necessária para uso da ferramenta - algumas ferramentas requerem um alto grau de habilidade no seu uso principalmente em linhas de comando, enquanto outras são totalmente iterativas e intuitivas para o usuário.
> b) qualidade do relatório - algumas ferramentas geram dados brutos que depois precisam ser consolidados e outras ferramentas geram relatórios mais intuitivos e de fácil leitura por parte do perito.
> c) custo - o custo para adquirir e usar uma ferramenta vai do "grátis" (geralmente código aberto) até o "muito caro".
> d) foco do exame - algumas ferramentas focam um artefato específico ou um grupo de artefatos. Enquanto outras são consideradas um "canivete suiço" e analisam uma variedade de artefatos (KIPER, 2020).

O critério para seleção das ferramentas também deve considerar a possibilita de atenderem mais de uma categoria perícia, tais como forense de computadores, dispositivos móveis, redes, banco de dados e analise de dados (padrão de ataques).

A sofisticação dos crimes computacionais exige o uso de ferramentas que agreguem produtos para as mais diversas aplicabilidades em um sistema integrado de análise forense. Nesse sentido, a PFC tem utilizado com frequência ferramentas cada vez mais completas, e que contemplem um número maior de fases da investigação forense computacional.

Grande parte das ferramentas disponíveis para PFC podem ser encontradas em um único produto, conhecidos como sistemas operacionais forenses. Os sistemas operacionais forenses normalmente são gravados de forma que quando os computadores forem inicializados, somente será disponibilizada a leitura dos dados (read-only), para que os discos rígidos possam ser inspecionados (ELEUTÉRIO; MACHADO, 2011).

Além dos sistemas operacionais, as ferramentas forenses são compostas por softwares específicos para ações como coleta de dados voláteis, duplicação, recuperação de arquivos, indexação de dados, análise de arquivos ou análise de tráfego de rede. Essas ferramentas podem ser utilizadas sozinhas, em conjunto ou ainda para complementar o uso de um sistema operacional forense.

Tabela 2 – Principais ferramentas open source e suas caracteristicas.

Software	Descrição	Caracteristicas
Kali	O Kali Linux é um dos sistemas operacionais mais conhecidos no mundo, baseado em Debian, desenvolvido pela Offensive Security, reescrito a partir do sistema BackTrack	Possui mais de 300 ferramentas pré-instaladas; Pode ser instalado como SO da máquina, rodando a partir pendrive ou instalado em VM; Grande número de pacotes e versões customizadas;
Sistema IPED	IPED – Indexador e Processador de Evidências, é um programa computacional forense desenvolvido no Brasil por peritos federais mais utilizados pela Polícia Federal. Foi empregado para a investigação na Operação Lava Jato.	Acesso a arquivos apagados e espaço não alocado (via Sleuthkit); Indexação e pesquisa por palavras-chave no conteúdo e propriedades dos arquivos. Extração e reindexação de itens selecionados pela interface de pesquisa após análise do perito

		Detecção de documentos cifrados
FDTK – UbuntuBR	O projeto FDTK-UbuntuBr uma distribuição Linux criada a partir distribuição Ubuntu	reúne mais de 100 ferramentas capazes de atender a todas as etapas de uma investigação Interface amigável
CAINE	CAINE (Computer Aided INvestigative Environment) é uma distribuição GNU/Linux de origem italiana baseada em Ubuntu 10.04, desenvolvida como um projeto da Digital Forensics.	Ela oferece um ambiente computacional forense completo, organizado para integrar ferramentas de software existentes como módulos, para fornecer uma interface gráfica bastante amigável; Possui ferramentas como nautilus Script, atarrow, bloom, fiwalk, xmount, e sshfs.
PeriBR	Live-CD de perícia digital, desenvolvido como trabalho de pos-graduação em perícia digital da Universidade Católica de Brasília pelos alunos Marcel Carvalho e Jaqueline Carvalho, em 2009. É um sistema baseado no Ubuntu 9.04.	O menu está todo categorizado de acordo com as fases de uma perícia; Estão embutidas ferramentas como PyFlag, PTK , Autopsy, Guymager e Dhash.
DEFT	Distribuição de origem italiana o DEFT (Digital Evidence and Forensic Toolkit) baseado no Xubuntu 9.10 . Mantido pelo escritório de pesquisa e desenvolvimento da Tesla Consulting.	Como ferramentas possui o Autopsy/Sleuthkit; Capacidade de captura de imagem; Pode ser executado ao vivo (via DVDROM ou USB pendrive) e possui interface amigável
Volatility	Coleção de ferramentas open source implementadas em Python, sob a licença GPL, para a extração de artefatos digitais de amostras de memória volátil (RAM)	Determina os processos em execução Apresenta os arquivos abertos para cada processo mapeamento de endereços físicos para endereços virtuais a extração de executáveis de amostras da memória volátil
The Sleuth Kit (TSK)	Conjunto de ferramentas de linha de comando, open source, utilizado em sistemas UNIX (Linux, OS X, FreBSD, OpenBSD e Solaris), e tem a finalidade de recuperar arquivos ocultos ou apagados do disco	Recuperação de arquivos; Recuperação de arquivos sobrescritos; Recuperação de sistemas de arquivos com journaling

Fonte: o autor.

Considerando as vantagens elencadas das ferramentas *open source*, o Tabela 3 apresenta as principais ferramentas de código aberto utilizadas no PFC, assim como

a existência de funcionalidades para cada fase da investigação forense segundo Kent et al. (2011):

Tabela 3: Principais softwares *open source* e a disponibilidade de funcionalidades para atender as fases da investigação forense

	Fases da investigação*			
Ferramenta	**Coleta**	**Extração**	**Análise**	**Relatório**
Kali	Sim	Sim	Sim	Sim
Sistema IPED	Não	Sim	Sim	Sim
FDTK – UbuntuBR	Sim	Sim	Sim	Sim
CAINE	Sim	Sim	Sim	Sim
PeriBR	Sim	Sim	Sim	Sim
DEFT	Sim	Sim	Sim	Sim
Volatility	Não	Sim	Sim	Não
The Sleuth Kit (TSK)	Não	Sim	Sim	Sim

*Segundo Kent et al. (2011)

Fonte: o autor.

4. RESULTADOS

Através da bibliografia referenciada e de uma pesquisa de campo realizada junto ao 7º Centro de Telemática de Àrea (7º CTA) e ao Núcleo de Perícia Forense do Centro de Defesa Cibernética (CD Ciber) foi possível avaliar os aspectos referentes as ferramentas utilizadas por estes dois órgãos, bem como as características referentes aos peritos no âmbito do Exército Brasileiro.

De acordo com o roteiro da pesquisa, do ponto de vista das ferramentas, foram levantadas quais as ferramentas utilizadas pelas unidades e se as mesmas satisfazem as solicitações de demandas forenses. Em relação aos peritos, critérios como competências, capacitação e experiência foram questionados.

A partir da literatura analisada, foi possível estabelecer um modelo conceitual dos requisitos desejáveis que uma ferramenta deve comportar. Conforme leciona Kent et al. (2011), as fases dentro de um trabalho forense abrangem a coleta, extração,

análise e relatório. Atualmente existem ferramentas que contemplam todas essas fases, ou grande parte das mesmas, sendo esta uma característica desejável para um resultado pericial eficaz e tempestivo. Dessa maneira, verificou-se a aderência das ferramentas pesquisadas no 7º CTA e no CD Ciber a este requisito, conforme apresentado no Tabela 4. Por medida de sigilo não serão divulgados os nomes das ferramentas utilizadas por estes dois órgãos.

Tabela 4: Ferramentas utilizadas no 7º CTA e CD Ciber

Categoria	**Ferramenta**	**Fases contempladas pelas ferramentas**			
		Coleta	**Extração**	**Análise**	**Relatorio**
Forense em computadores e dispositivos de armazenamento	A	Não	Sim	Sim	Não
	B	Não	Sim	Sim	Não
	C	Sim	Não	Não	Não
Forense em dispositivos móveis	D*	Sim	Sim	Sim	Sim
Forense em redes	E	Não	Sim	Sim	Não
Forense em banco de dados e memória	F	Não	Sim	Sim	Não
Forense em análise de dados	Não realizam	-	-	-	-

* Realizam com auxílio de equipamento cedido pelo CIE

Fonte: o Autor

Desde 2007, através da Portaria nº 007-DCT (BRASIL, 2007), o EB vem priorizando o uso de ferramentas *open source* através do seu Plano de Migração para Software Livre, cujos principais objetivos são a economia de custo em aquisições de software, restringir o legado baseado em tecnologia proprietária e fomentar a criação de uma base interna de conhecimento em software livre.

Além do requisito relacionado a necessidade do software utilizado ser *open source*, outros critérios para seleção das ferramentas forenses foram citados pelos peritos pesquisados, como facilidade de uso do programa e qualidade dos relatórios de saída.

Em relação aos requisitos normativos, as Organizações Militares pesquisadas estão amparadas a partir do anexo H das NRPFC/SisTEx do Exército Brasileiro, que orienta a metodologia utilizada para a realização de uma PFC:

> I – Análise do ambiente: consiste na preservação das evidências e dos documentos encontrados. O perito deve evitar o acesso de pessoas não autorizadas, bem como não deixar que as evidências sejam destruídas ou adulteradas.
> II – Coleta de evidências: é o recolhimento de todo o dado armazenado em meio digital. O perito deve observar a ordem decrescente de volatilidade dos dados: 1) memória principal; 2) estado da rede; 3) processos em execução; 4) arquivos temporários; 5) disco rígido; 6) mídias externas regraváveis e 7) mídias somente leitura. A norma orienta que sempre será priorizado o meio de armazenamento mais volátil.
> III – Armazenamento e transporte de evidências: refere-se aos cuidados a serem tomados com as mídias de destino. As mesmas devem ser cuidadosamente embaladas e protegidas contra a luz e umidade devendo ser rotuladas, documentadas e inventariadas. Com relação ao transporte devem ser evitadas exposições a campos eletromagnéticos, variações bruscas de temperatura, umidade e choques físicos.
> IV – Exame e análise em laboratório: consiste na utilização de técnicas e ferramentas para que sejam extraídas as informações julgadas importantes na PFC. A análise por meio de exame e serve para fundamentar as respostas aos questionamentos formulados.
> V – Elaboração do Laudo Pericial: o laudo é o documento que transcreve todo o trabalho realizado pelo perito de acordo com as evidências encontradas.

5. DISCUSSÃO

O estudo buscou verificar a aderência dos aspectos normativos e técnicos da PFC no 7º CTA e no CD Ciber, em relação a metodologia proposta na literatura para normatização dos procedimentos forenses e aos requisitos desejáveis das ferramentas de apoio à investigação computacional

Em relação às questões normativas, constatou-se que as definições do anexo H das NRPFC/SisTEx do Exército Brasileiro, relativas às etapas para execução de uma PFC, estão de acordo com os padrões metodológicos e procedimentos de boas práticas internacionais para a perícia forense, propostos por Kent et al. (2011), uma vez que as etapas do documento estão em alinhamento com as fases da investigação forense computacional (coleta, extração, análise e relatório). Da mesma forma, a norma definida no NRPFC/SisTEx está aderente a norma NBR 27037:2013, que fornece instruções para atividades específicas no manuseio de evidências digitais que são a

identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório.

Ainda em relação às questões internas para condução da PFC, a opção pelo uso de ferramentas *open source* e livres vai ao encontro dos termos preconizados na Portaria nº 007-DCT (BRASIL, 2007), que ressalta o uso desse tipo de ferramenta no sentido de atender ao Plano de Migração para Software Livre no Exército Brasileiro.

Quanto às ferramentas, o estudo indica que, no sentido atingir resultados positivos, tempestivos e eficazes no trabalho pericial, é essencial o uso de ferramentas para apoiar o trabalho do perito em todas as suas fases, sendo essas ferramentas específicas para cada fase mas, preferencialmente, possam abranger mais de uma fase. Nesse contexto, tornaram-se populares na PFC os sistemas operacionais forenses, com centenas de ferramentas incorporadas em um único produto e com possibilidade de atender a todas as fases da perícia.

As ferramentas utilizadas no 7º CTA e no CD Ciber, apesar de agregarem diversas funcionalidade e programas, estão limitadas a atividades específicas da investigação forense dentro de uma única fase da perícia, ou até em duas fases, no entanto nenhuma ferramenta contempla todas as fases periciais, conforme Tabela 4.

Observou-se inclusive que a ferramenta A, apresentada no Tabela 4, faz parte do Sistema Operacional (SO) forense CAINE, em conjunto com outras ferramentas nativas do SO. Dessa maneira, existe a possibilidade de manter o uso da ferramenta A, a partir de um *upgrade* para um sistema operacional, com ganhos consideráveis nos diversos aspectos da investigação.

Da mesma maneira, as funcionalidades da ferramenta B encontram-se disponíveis em diversos sistemas operacionais forenses, com a mesma facilidade de uso, que foi um dos critérios para sua escolha, mas com opções de relatórios muito mais completos, sendo este outro critério para escolha da ferramenta B. O mesmo ocorre com a ferramenta E, utilizada para forense em redes.

No caso da Ferramenta C, conforme Tabela 4, a mesma é utilizada somente para coleta de dados. O estudo indica que a maioria das principais ferramentas *open source* consideradas sistemas operacionais forenses contemplam a coleta de dados. Dessa maneira, substituir a ferramenta C por um sistema operacional que também

faça a coleta, traria o beneficio de incorporar ao trabalho forense do 7º CTA e do CD Ciber centenas de softwares para ampliar as possibilidades de investigação.

A exceção ocorre em um único programa que pode ser utilizado em todas as fases da perícia, que é a ferramenta D, a qual atende a categoria forense de dispositivos móveis, mas que trata-se de um equipamento pago cedido pelo Centro de Inteligência do Exército (CIE) com *software open source* incorporado.

Contudo, essas possíveis substituições de *sofwares* devem observar a realidade vivenciada por cada Organização Militar. A falta de recursos e treinamento foram citadas durante as entrevistas como barreiras, situações que se deve avaliar e superar antes de se almejar uma substituição de ferramentas.

O aumento exponencial do volume de dados a serem periciados também foi relatado pelos peritos como uma dificuldade, ponto que também pode ser equalizado com a adoção de sistemas operacionais forenses, que garantem escalabilidade em diversas versões.

6. CONCLUSÃO

Com o avanço tecnológico, cresceram também os crimes cibernéticos em virtude da grande quantidade de dispositivos que hoje armazenam ou trafegam dados. Nesse contexto a perícia forense computacional tornou-se importante a partir da busca e da análise das evidências, possibilitando a resolução de crimes que utilizam computadores e equipamentos eletrônicos.

De acordo com o estudo realizado, foram apresentados os aspectos legais e técnicos da PFC, dando ênfase na normatização usada pelo Exército Brasileiro que enquadra todo o trabalho de perícia computacional realizada dentro da Força. Nos aspectos técnicos foram apresentadas as categorias e perícias computacionais e também metodologia básica adotada inclusive pelo EB para a elucidação dos incidentes.

Conforme foi apresentado nos resultados e na discussão, do ponto de vista normativo, a pesquisa identificou que as normas e procedimentos do EB relacionados à PFC, estão de acordo e aderentes com as melhores práticas forenses da atualidade.

Quanto as questões técnicas, especificamente no quesito ferramental, o estudo indicou oportunidades de melhorias na seleção das ferramentas utilizadas pelas Organizações Militares, sugerindo a adoção de sistemas operacionais forenses que, além de contemplar as ferramentas já utilizadas pelo EB, também abarcam de maneira nativa centenas de outras ferramentas que podem ampliar a escalabilidade, qualidade e tempestividade das atividades forenses.

7. REFERÊNCIAS

ALMEIDA, Rafel Nader de. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais.** 2011. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0035.pdf. Acesso em: 16 Ago 2020.

ALTHEIDE, Mark; CARVEY, Harlan. **Digital Forensics with Open Source Tools.** 2011. Disponível em:http://index-of.es/Hack/Digital%20Forensics%20with%20Open%20Source%20Tools-slicer.pdf. Acesso em 25 Ago 2020.

ARTHUR, K.K; VENTER, H.S. **An Investigation into Computer Forensic Tools.** 2004. Disponível em : https://digifors.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf. Acesso em 26 Ago 2020.

BRASIL. Comando do Exército Brasileiro. **Plano de Migração de Software Livre no Exército Brasileiro.** 2007. Disponível em: http://www.5cta.eb.mil.br/images/5cta/normasti/Port_n_007_DCT.pdf. Acesso em: 13 Ago 2020.

BRASIL. Ministério da Defesa. **PND/END**. Política Nacional de Defesa e Estratégia Nacional de Defesa, 2008. Disponível em : https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf. Acesso em 13 Ago 2020.

BRASIL. Comando do Exército Brasileiro. **DIRETRIZ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO SISTEMA DE TELEMÁTICA DO EXÉRCITO (DSIC/SisTEx)**, 2012. Disponível em: http://intranet.1cta.eb.mil.br/intranet_nova/images/10-DSIC-DIRETRIZ_SEGURAN%C3%87A_INFORMACAO_COMUNICACOES_SISTEX.PDF. Acesso em 15 Ago 2020.

CARRIER, Brian. **Open Source Digital Forensics Tools: The Argument Legal**, 2002. Disponível em:

https://pdfs.semanticscholar.org/6dd1/b343b01be325147257e364d68b1f983ea4db.pdf?_ga=2.38173216.2050998642.1598368152-816005637.1598368152. Acesso em: 05 Ago 2020.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense**. 11 ed. São Paulo: Novatec. 2011. Disponível em: https://books.google.com.br/books?id=jS2oDwAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_atb#v=snippet&q=operacional&f=false. Acesso em: 10 out. 2002.

EDUARDO, Bruno de Souza; CARVALHO, Fabrício Augusto Beijo; RODRIGUES, André Ricardo Prazeres. **Computação forense: uma aplicação de softwares livres para a recuperação de dados digitais.** Disponível em: https://revistas.setrem.com.br/index.php/reabtic/article/view/300. Acesso em 29 Ago 2020.

EUA. National Institute of Standards and Technology. **About NIST**. 2015. Disponível em:https://www.nist.gov/about-nist. Acesso em: 13 Set 2020.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática.** Rio de Janeiro: Rio de Janeiro, 2003. Disponível em: http://www.truzzi.com.br/blog/wp-content/uploads/2010/08/Monografia.pdf. Acesso em: 22 Jul 2020.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa.** 6ª Edição. Editora Atlas. 2017. São Paulo-SP.

KENT, Karen; CHEVALIER, Suzane; GRANCE, Tim; DANG; Hung. **Guide to Integrating Forensic Techniques into Incident Response.** 2006. Disponível em https://csrc.nist.gov/publications/detail/sp/800-86/final. Acesso em: 29 Ago 2020.

KIPER, J. Richard Rick. **Pick a Tool, the Right Tool: Developing a Practical Typology for Selecting Digital Forensics Tools**. 2020. Disponivel em: https://www.sans.org/reading-room/whitepapers/tools/paper/38345. Acessado em 10 Set 2020.

KYK, K. **INFLUENCE OF OPERATING SYSTEM ON THE FORENSICS TOOLS**. 2017. Disponível em: http://elib.amia.by/bitstream/docs/1627/1/Konferencija-7.pdf. Acesso em: 9 Set 2020.

MABEY, Michael Kent. **Forensic Methods and Tools for Web Environments**. 2017. Disponível em: https://repository.asu.edu/items/46271. Acesso em 22 Ago 2020.

NTI. **Computer Forensics Defined,** 1996? Disponível em: http://www.forensics-intl.com/def4.html. Acesso em 02 Set 2020.

OLIVEIRA, Daniel. Legislação para computação Forense. **TI Forense**. 2018. Disponível em: https://www.tiforense.com.br/legislacao-para-computacao-forense/.

Acesso em: 06 out. 2020.

OLIVEIRA, Vinicius Machado de. Norma NBR ISO/IEC 27037:2013 – Resumo. **TI Forense**. 2019. Disponível em: https://www.tiforense.com.br/norma-nbr-iso-iec-270372013-resumo/. Acesso em: 06 out. 2020.

POLLITT, Mark. **A History Digital Forensics**, 2010. Disponível em: https://link.springer.com/content/pdf/10.1007%2F978-3-642-15506-2_1.pdf. Acesso em 22 Ago 2020.

PRASANTHI, B. V. **Cyber Forensics Tools: A Review**, 2016. Disponível em: http://www.ijettjournal.org/2016/volume-41/number-5/IJETT-V41P249.pdf. Acesso em 27 Ago 2020.

RAMOS, Renato. **SISTEMAS DE LAUDOS FORENSE COMPUTACIONAL: USO NO CONTEXTO DA PERÍCIA CRIMINALÍSTICA**, 2014. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/49546/R%20-%20E%20-%20RENATO%20RAMOS.pdf?sequence=1&isAllowed=y. Acesso em: 29 Ago 2020.

SOUZA, Paulo Francisco Cruz de. **Perícia Forense Computacional: Procedimentos, Ferramentas e Estudo de Caso**. 2015. Disponível em: http://www.redes.ufsm.br/docs/tccs/Paulo-Souza.pdf. Acesso em: 23 Jul 2020.

VARGAS, Raffael Gomes. **Perícia Forense Computacional: Metodologia e Ferramentas Periciais**. Evidência Digital Magazine. 2011. Disponível em: http://dfir.com.br/wp-content/uploads/2013/10/Evidencia_Digital_05.pdf. Acesso em: 2 Set 2020