AS DIFICULDADES DO PROFISSONAL FORENSE NO BRASIL

DANIELE RIBEIRO DOS SANTOS, DAVID BUENO MARTINS DE RAMOS, DIEGO ANTUNES MUNIZ, GABRIEL DAMASCENO CUNHA, KENNEDY PASSOS DA SILVDA SANTOS, NARUMI ABE, ELIANE CRISTINA AMARAL, ELINEY SABINO

RESUMO

O presente artigo, estuda a perícia forense aplicada à informática e suas implicações visando o perfil do perito computacional forense para a sociedade, dentre problemas enfrentados pelo profissional e características de sua função, destacando a importância do profissional no setor exercido e a carência de normas e padronizações no Brasil, levando a categoria enfrentar dificuldades. Para tanto, são apresentados estudos de caso relevantes, procedimentos e ferramentas que possibilitaram analisar eventos em que a perícia se fez necessária, mitigando riscos e possibilitando ações proativas por parte da perícia.
Palavras-chave: Perícia forense, Leis e crimes digitais, Ferramentas de segurança.

ABSTRACT

This present article studies the forensic expertise applied to informatics and its implications aiming at the profile of the forensic computational expert for the society, among the problems faced by the professional and the characteristics of its function, highlighting the importance of the professional in the sector practiced and the lack of norms and standardizations In Brazil, leading the category to face difficulties. In order to do so, we present relevant case studies, procedures and tools that enable us to analyze events in which the expertise was necessary, mitigating risks and enabling proactive actions by the expertise.
Keywords: Forensic expertise, Laws and digital crimes, Security tools.

1 INTRODUÇÃO

Ao decorrer dos anos, a tecnologia está mais presente na rotina das pessoas, e com isso, o crescimento e a necessidade do uso da tecnologia passam despercebido para muitos. Fazer compras por um dispositivo com dados de um cartão; se relacionar com pessoas por meios virtuais; procurar empregos em sites; praticar educação à distância com recursos multimídia; usar Global Positioning System (GPS) que os possibilitam, através de sistemas, chegar a qualquer lugar do planeta. E a Computação Forense faz a sua parte. A palavra forense vem de foro, e podemos entender como meio policial onde é feita uma análise minuciosa de todo material capturado em cena de crime. Computação forense é então o ramo da criminalística que compreende a descoberta, preservação, restauração e análise de evidências computacionais. Computadores podem ser usados para cometer crimes, como, por exemplo, aliciamento

de menores. Podem conter evidências de crimes, como dados de contas bancárias fraudadas. Ou ainda ser alvos de crimes, quando armazenam informações sigilosas de grandes instituições. O objetivo do presente artigo é compreender o perfil do profissional computacional forense, a maneira como a profissão é desempenhada, estudar as dificuldades que existem na profissão do Perito Computacional Forense no Brasil. Alavancar possíveis sugestões de melhorias com base em pesquisas, características, dentre outros aspectos do perito profissional. A seguir apresentamos alguns procedimentos e ferramentas, seguido de métodos forenses utilizados atualmente.

Este artigo tem por objetivo estudar as dificuldades que existem na profissão do Perito Computacional Forense no Brasil. Alavancar possíveis sugestões de melhorias com base em pesquisas bibliográficas. Contudo, destacaremos a importância deste profissional na busca e nas soluções de fraudes ligadas a informática, como é efetuada as perícias: procedimentos, técnicas, métodos, metodologias e programas, que utilizam.

Neste artigo, justifica-se na intenção de ajudar o profissional Perito Computacional Forense a encontrar soluções e melhorias na sua profissão. Assim, sendo de base de pesquisas para outros alunos de universidades e profissional da área especifica, a fim de ampliar e aprofundar conhecimentos de uma forma geral para a sociedade.

2 COMPUTAÇÃO FORENSE

Segundo Macêdo (2012), os crimes eletrônicos aumentaram em 1970, principalmente no setor financeiro. A maioria dos computadores era mainframe, utilizados por pessoas treinadas para trabalhar em finanças, engenharia e academia. Nessa época, os policiais não conheciam computadores; e não sabiam realizar as perguntas corretas para descobrir o crime, ou para preservar as provas para o julgamento. Muitos começaram a participar do Federal Law Enforcement Training Center (FLETC), que eram destinados a treinar a aplicação da lei na recuperação de dados digitais.

Para Macêdo (2012), em 1980 os Computadores Pessoais começaram a ter popularidade e vários sistemas operacionais apareceram, Apple 2E em 1983 e o Macintosh em 1984, pela Apple. E depois surgiram Sistemas Operacionais de Disco (DOS), incluindo Personal Computer Disk Operating System (PC-DOS), Quick and Dirty Operating System (QDOS), Digital Research (DR-DOS), an acronym for IBM Personal Computer Disk Operating System (IBMPC-DOS) e MicroSoft Disk Operating System (MS-DOS). Nessa época, as ferramentas forenses eram simples, criadas pelas agências governamentais: Royal Canadian Mounted Police, (RCMP), U.S. Internal

Revenue Service (IRS) e não eram fornecidas ao público. No meio de 1980 surgiu no mercado o Xtree Gold, que reconhecia tipos de arquivos, recuperava arquivos perdidos ou apagados e permitia ver o código de um binário, convertendo seus bytes para American Standard Code for Information Interchange (ASCII). No início de 1990 ferramentas especializadas para computação forense foram disponibilizadas, a International Association of Computer Investigative Specialists (IACIS) iniciou o treinamento sobre softwares de investigações forenses e o IRS criou programas de pesquisa de produtos sob garantia de licença, então surgiu o primeiro software não comercial com modo gráfico, o Data Forensiscs Software services and Training (ASR-Data) criado para peritos Macintosh. Até que um dos patrocinadores saiu do projeto e criou o EnCase, que se tornou a ferramenta forense mais popular da época.

Afirma Macêdo (2012), que no Brasil a empresa TechBiz Forense Digital é a maior integradora das tecnologias de computação forense e possui um amplo portfólio de ferramentas, que são fornecidas para órgãos públicos e privados e forças da lei de todo o Brasil. No caso de prática de crime, o Código de Processo Penal Brasileiro (BRASIL, 1941), determina que: quando a infração deixar vestígios, será indispensável o exame de corpo de delito (artigo 158); o exame de corpo de delito e outras perícias serão realizados por perito oficial (artigo 159); os peritos elaborarão o laudo pericial, no qual descreverão o que examinarem e responderão aos quesitos formulados (artigo 160). Na computação, os vestígios de um crime são digitais (em forma de bits), podendo ser encontrados em dispositivos de armazenamento ou trafegando em rede, na maioria dos casos, exames forenses nesses dispositivos resultam em uma excelente prova técnica e os laudos produzidos tornam-se peças fundamentais para o convencimento do juiz na elaboração da sentença.

De acordo com Gonçalves, Amadio, Gavilan, e Santos (2012), muitos são os casos em que são solicitados os trabalhos do Profissional Forense. Porém, na maioria das vezes o mesmo não é de fácil resolução, tendo a investigação dificuldade pelo investigado. Como por exemplo, a tentativa de ocultação de provas, com a formatação de periféricos e até computadores para mascarar o crime ou destruição dos mesmos. Também é bastante utilizada técnicas para ocultar localização e Internet Protocol (IP), com a ajuda de Virtual Private Network (VPNS) e outros programas para o mesmo fim. No entanto, será que mesmo com todas as dificuldades apresentadas ao Profissional Forense, consegue solucionar esses casos?

Segundo Bustamante (2006), vemos abaixo uma ocasião em que o Profissional Forense foi de total importância para elucidar os casos a ele proposto.

Caso real: Crime solucionado com ajuda da Computação Forense.

Para Bustamante (2006), no Brasil um corretor de imóveis foi condenado por homicídio tendo como meio de prova um laudo pericial que indicava a localização do suspeito no momento do crime. Neste caso o Profissional Forense conseguiu através de informações dadas pela empresa de telefonia captada pela estação rádio-base (Erb) ou antena de celular, informações essas de total confiança e autenticidade. Na qual apontava o investigado próximo ao local do crime, o que contrariava o depoimento do mesmo. Tendo essa informação como prova, o acusado foi condenado pelo crime.

Conforme Guimarães, Reis, Oliveira e Geus (2001), no Brasil não existem normas próprias para Computação Forense, apenas trabalhos feitos a pedido da polícia federal. Esses trabalhos são direcionados ao público leigo composto por promotores e juízes federais.

Para Freitas (2006), quando tratamos de análise forense, o Profissional Computacional Forense segue alguns fundamentos básicos que são comuns às análises de qualquer programa computacional, que foram originalmente herdados de bases da Ciência Forense em geral. Basicamente estes fundamentados buscam dar confiabilidade aos resultados, fornecendo técnicas para a verificação da integridade das evidências e correção nos procedimentos adotados. A documentação das atividades é fundamental para que uma análise possa ser aceita, mesmo que o stress causado por um incidente de segurança torne difícil à atividade de documentar as decisões e ações, o que pode prejudicar uma futura ação judicial contra os responsáveis, pois pode tornar inviável a avaliação das evidências.

Além da documentação, Freitas (2006), cita alguns princípios através dos métodos computacionais:

- Réplicas: É recomendado há realizar a duplicação do laudo pericial para que seja possível a repetição dos processos e a busca por resultados, sem que ocorra o dano à evidência original. Normalmente é necessária a obtenção de uma imagem *bit-a-bit* dos sistemas, tarefa esta, que muitas vezes toma um grande tempo.

- Garantia de Integridade: Deve haver procedimentos de modo prévio que visem garantir a integridade das evidências coletadas. No mundo real as evidências são armazenadas em ambientes cuja entrada é restrita, são tiradas fotos, detalhe das peças coletadas são escritas com o intuito de verificar sua autenticidade. No mundo virtual a autenticidade e a integridade de uma evidência podem ser verificadas através da utilização de algoritmos de *hash* criptográfico como *o Message-Digest algorithm 5* (MD5), *secure hash algotithm* (SHA-1) e o (SHA-2). Além disso, é possível armazená-las em mídias para somente leitura, como Compact *Disc Read-Only* (CD-ROMs).

- Ferramentas Confiáveis: É necessário usar programas computacionais capazes de garantir resultados confiáveis, o mesmo ocorre no mundo real onde os experimentos de uma análise laboratorial devem ser conduzidos em ambientes controlados e comprovadamente seguros a fim de que os resultados não possam ser contaminados por alguma influência externa.

Segundo Machado (2011), a perícia forense operada na computação, tem a precisão de melhorias nos métodos, técnicas e recursos. Justamente com o aumento de investigações a perícia forense busca ajustar tarefas legais e administrativas na busca por vestígios. O crescente uso dos computadores e da popularização dos dispositivos computacionais tornaram ferramentas de apoio á práticas de crimes acerca de sonegação fiscal, compra de votos em eleições, tráfico de entorpecentes e falsificação de documentos. Porém, os computadores tornaram-se também um excelente mecanismo de investigações, sendo fundamentais para solucionar vários tipos de crime.

> Um local de crime de informática nada mais é do que um local de crime convencional acrescido de equipamentos computacionais que podem ter relações com o delito investigado. São comuns nos dias de hoje, assim como o cumprimento de mandados de buscas e apreensão envolvendo equipamentos computacionais. (Machado, 2011,25)

Destaca Machado (2011), que o uso dos equipamentos computacionais como ferramentas de apoio aos crimes convencionais, representam 90% dos exames forenses realizados no campo de informática.

> Um exemplo de má utilização de computadores é o compartilhamento de arquivos de pornografias infanto-juvenil por meio da internet. Muitos pedófilos e usuários baixam e compartilham fotos vídeos com esse tipo de conteúdo de acordo o artigo 241- A do estatuto da criança e do adolescente. Se o computador e a internet não existissem, tal conduta seria impossível. (Machado, 2011, 19)

De acordo com Palmer (2001), a computação Forense pode ser entendida como reconhecimento científico e sistemático, com a intenção de coletar evidência de fontes digitais, para favorecer a remontagem dos fatos encontrados.

Conforme Machado (2011), o perito é responsável em orientar a equipe durante a seleção, preservação e coletas dos equipamentos computacionais para decorrente realização de exames forenses. Cuidados devem existir com a coleta dos vestígios digitais, pelo nível de sensibilidade e

responsabilidade ao fato. O impacto, umidade, afundamento em água, o calor excessivo pode causar perdas das informações digitais.

Para Erbacher; Christiansen e Sundberg (2006), questões são essenciais, a saber, quando relacionadas à perícia forense computacional:

- Responsável por executar os ataques?
- Qual a dimensão dos danos?
- Qual o fundamento do ataque?
- Qual categoria de acesso alcançado pelo executor?
- Há intenção de direção de ameaças?
- Há intenção de seguimento do negócio?

Conforme Erbacher; Christiansen e Sundberg (2006), há dificuldades ao encontrar a identificação correta do atacante. Tendo como exemplo, o Spoofing é um ataque que consiste em ocultar pacotes (IP) utilizando endereços de remetentes falsificados, isso dificulta o trabalho dos peritos. Mesmo assim a investigação consiste na procura de fontes da ocorrência que facilita na identificação de falhas, as quais podem ser realizadas em novos ataques. É muito importante identificar o foco do ataque, assim permite definir as ações a serem realizadas. São ações verídicas que ajudam na hora de possíveis medias (administrativas e /ou jurídicas) serem tomadas.

Todo o trabalho feito deve possibilitar após o encerramento da perícia, que as devidas providências administrativas e legais sejam tomadas. Visto a crescente quantidade de ataques em rede e recursos de comunicações é possível identificar as necessidades de melhorias dos recursos, métodos e práticas utilizadas nas investigações.

Segundo Melo (2005), recomenda que o trabalho da perícia seja realizado baseando-se em quatro etapas: coleta, extração, análise e documentação. Sendo assim, a perícia forense faz uso deste processo em sua investigação. Coleta diz respeito ao reconhecimento e coleta de informações que podem envolver provas digitais. Este procedimento deve ocorrer imediatamente após o conhecimento do incidente, tendo em vista reduzir perdas de informações. O analista deve ser apto para reconhecer e levantar todas as prováveis fontes de dados, como computadores, laptops, servidores, dispositivos de armazenamento, celulares entre outros. É importante, também, investigar as informações válidas em outros locais, por exemplo, possíveis conexões de rede suspeitas.

De acordo com Modesto e Moreira (2014) a coleta de dados se divide em três partes: desenvolvimento de plano para https://www.sinonimos.com.br/adquiricao/obter informações devidamente dita e verificação dos dados. Este desenvolvimento faz combinação com os seguintes fatores: valor da fonte, volatilidade e quantidade de esforço requerido. Obter dados pode ser realizado localmente, funcionando nos sistemas que se encontram em analises, o processo também pode ser realizado remotamente, mas o trabalho localmente permite maior controle do perito sobre as operações. A verificação da integridade dos dados pode-se utilizar funções matemáticas de comparações.

Segundo Melo (2005), a extração de informações utiliza-se métodos forenses, tendo em vista resguardar todo o a coletado. Essa análise é feita através de cópia forense, para preservar as evidências digitais. Análise tem por objetivo de se basear em análises já realizadas, utilizando ferramentas e metodologias propícias antes de quaisquer conclusões. Por fim é necessário fazer a documentação, realizar relatórios técnicos, para documentar e apresentar os resultados alcançados.

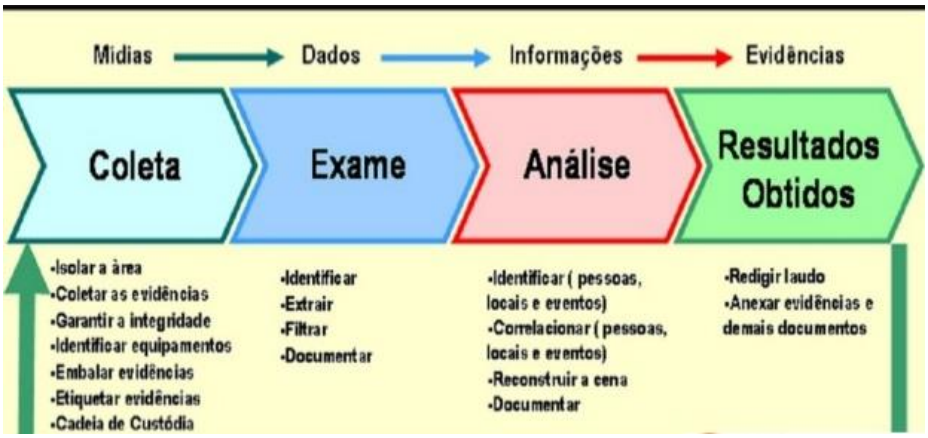

Figura 1. Fases de Verificação
Fonte: Pereira, Fagundes, Neukamp, Ludwig, Konrath (2017 s/n)

Na figura 1, descreve as fases expostas acima, como o modo de investigação é feito. A investigação se inicia com o aprisionamento dos dispositivos e armazenamentos de dados, logo depois os dados armazenados passam pela fase de exame, nesta fase o perito utiliza ferramentas para extrair somente informações relevantes no caso investigado. A análise é feita para a criação de relatório de investigação, assim as evidencias são descritas.

Equipamentos computacionais utilizados como ferramentas de apoio aos crimes.

Na atualidade variadas ferramentas está há disposição, tanto proprietárias, quanto em códigos abertos. Normalmente quem tem acesso a ferramentas proprietárias são grandes empresas de perícia ou policias. O perito individual não tem caixa suficiente para comprar essas ferramentas, pois são muito caras, então se utiliza ferramentas livres que são normalmente baseadas em Linux.

Segundo Gibson (2007) softwares são usados com a finalidade de salvar os dados inclusos na maquina suspeita. Uma ferramenta muito utilizada nas investigações é o Automated Image & Restore (AIR), que dá auxilio na formação ou recuperação de imagens das evidencias, além da formação de imagens, produz relatórios incluindo todos os comandos usado durante a execução. A figura 2 descreve a tela inicial desta ferramenta.

Figura 2. Imagem do programa informático para tarefas auxiliares
Fonte: Gibson (2007)

Outro exemplo de ferramenta é o Autopsy, sistema usado pela perícia para a restauração de dados. A figura 3 descreve esse exemplo da tela principal. Pode- se observar que é uma ferramenta que faz comunicação por meio de uma interface Web, assim não é preciso instalar um software exclusivo para esta função.

Figura 3. Imagem Autopsy
Fonte: Gibson (2007)

3 PROCEDIMENTOS E MATERIAIS ANTI- FORENSE

Segundo Harris (2006), existem métodos anti-forense que tem por objetivo eliminar, ocultar ou modificar as evidencias existentes em um sistema, dificultando assim o trabalho dos peritos.

Para dificultar na recuperação de informações os invasores usam materiais para eliminar os dados, para que não fique suspeitas.

> Ferramentas (conhecidas como wiping tools) para remoção dos dados, tais como: wipe, secure-delete, pgp wipe e The Defiler's Toolkit. Essa categoria de ferramentas emprega uma variedade de técnicas para sobrescrever o conteúdo dos arquivos, por exemplo, gravar dados de forma randômica e sobrepor o conteúdo dos arquivos com bytes nulos. Essas ferramentas também alteram o inode dos arquivos o que torna a tarefa de recuperação dos arquivos ainda muito complexa, embora seja possível (Pereira, Fagundes, Neukamp, Ludwig, Konrath. 2014, 31).

Os dados podem ser ocultados de duas maneiras: separando um arquivo e armazenando essas repartições em espaços não alocados ou marcar como bad blocks. Sistema como New Technology File System (NTFS) disponibiliza esconder arquivos para que não sejam visualizados nem por comandos.

> Além desses métodos, a aplicação de criptografia e esteganografia em arquivos de texto, imagem, vídeo e áudio representam uma barreira difícil de ser superada, pois exigem tempo e recursos nem sempre disponíveis para identificação dos dados ocultos. Por exemplo, utilizar ferramentas de estegano análise em uma mídia de 80GB requer muito tempo e na prática nem sempre é algo viável de se realizar. O mesmo ocorre quando se trata de arquivos criptografados (Pereira, Fagundes, Neukamp, Ludwig, Konrath. 2014, 31).

Conforme Harris (2006), a forma mais utilizada para modificar os dados é: Altera a extensão e o conteúdo do cabeçalho dos arquivos. Esses métodos são executados em variadas ferramentas como Metasploit Anti-Forensic Investigation Arsenal (MAFIA) e Windows Memory Forensic Toolkit (WMF).

4 CONSIDERAÇÕES FINAIS

Realizando este artigo, podemos considerar que o perito em computação forense pode ser bem diferente em relação a atividades de outros peritos.

O Perito em computação forense é diferente não só na atividade em si, mas na forma de se atuar. Um perito que precisa coletar DNA de uma amostra, já tem todo o procedimento descrito para fazê-lo com sucesso. Não há como se alterar um DNA do fio de cabelo, ou impedir que sua análise em laboratório seja malsucedida.

Já um perito computacional forense, nunca saberá o que estará em um computador ou em qualquer aparelho eletrônico. Qualquer ação mal pensada pode resultar em perda permanente da evidência, implicando em estrago irreparável para o processo judicial. Por isso a importância de estar sempre a frente quanto a qualquer novidade no mundo tecnológico digital, realizando constantemente estudos na área e bem informado sobre pesquisas atuais, toda e qualquer inovação que possa existir, o que sempre fará a diferença para um perito forense computacional.

5 REFERÊNCIAS BIOGRÁFICAS

ALMEIDA, Rafael Nader de. Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais, 2011.

BESSA, L. (2006). Websense revela suas previsões sobre a segurança da internet para 2007. IMS Marketing. Websense, Inc, CARRIER.B.(2007a). Autopsy forensic browser. SourceForge.net. Disponível em: http://www.sleuthkit.org/autopsy/desc.php. Acessado em: 05/2017.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. 2. Ed. São Paulo: Saraiva (2011). Disponível em: http://imasters.com.br/artigo/4656/gerencia-de-ti/casos-reais-crimes-elucidados-com-ajuda-da-ti. Acessado em: (05/2017).

ELEUTÉRIO, Pedro Monteiro da Silva / MACHADO, Marcio Pereira. Desvendando a Computação Forense. 1ª ed. São Paulo: Novatec, (2011).

ERBACHER, R. F.; CHRISTIANSEN, K.; SUNDBERG, A. Visual Network Forensic Techniques and Processes. In: ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE, 1, 2006, Albany. Proceedings of the 1st. Annual Symposium on Information Assurance. Albany: University atAlbany, (2006) P. 72 - 80.

ESPINDULA, Alberi; A função Pericial do Estado; Pericia Criminal- DF; Disponível em: http://www.apcf.org.br. Acessado em: (05/2017).

FREITAS, Andrey Rodrigues de. Perícia forense aplicada à informática. Rio de Janeiro: Brasport, (2006).

GONÇALVES; Márcio, AMADIO; Renato Arnaut, GAVILAN; Júlio César, SANTOS; Herlones Wuilles (2012). Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas. Disponível em: ttp://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf, Acessado em: (04/2017)

GUIMARÃES, Célio Cardoso; OLIVEIRA, Flávio de Souza; REIS, Marcelo Abdalla; GEUS, Paulo Lício. Forense Computacional: Aspectos legais e padronização. (2001)

PEREIRA; Evandro, FAGUNDES; Leonardo Lemes, NEUKAMP; Paulo, LUDWIG; Glauco, KONRATH; Marlom. Capítulo 1. Forense Computacional: Fundamentos, tecnologias e desafios atuais.

IBSON,S.(2007). Automated image and restore (air).SourceForge.net, Disponível em: https://sourceforge.net/projects/air-imager/. Acessado em: (05/2017).

HARRIS, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. In The 6th Annual Digital Forensic Research Workshop (DFRWS 2006).

MACÊDO, Diego. O que é a computação forense e a sua importância no âmbito empresarial.

Disponível em: http://www.diegomacedo.com.br/o-que-e-a-computacao-forense-e-sua-importancia-no-ambito-empresarial/. Acessado em: 05/2017

MARINO, Aline Marques, GUIDA, Itamara, PASSOS, Jonatas Fonseca, NOGUEIRA, Renan França. Perícia Forense Computacional: Um diálogo interdisciplinar entre a informática e o direito.

MELO Sandro. Disponível em <http//www.linux.com.br>. Acessado em: (05/2017)

MODESTO JUNIOR, Celso Carlos Navarro; MOREIRA Jander. Roteiro Investigativo em Perícia Forense Computacional de Redes: Estudo de Caso (2014).

PALMER, G. A Road Map for Digital Forensic Research. Utica: DFRWS (2001). 48 p. DFRWS Technical Report.

PINHEIRO, Franco Deivison. A atuação do Perito Forense Computacional na investigação de crimes Cibernéticos (2016). Disponível em: https://cryptoid.com.br. Acessado em (04/2017)

TEELINK, S. and ERBACHER, R. F. (2006). Improving the computer forensic analysis process through visualization. Commun. ACM, 49(2):71

QUINTÃO, Patrícia Lima; TEIXEIRA, Carla da Silva: BATISTA, Mônica de Lourdes Souza; VARGAS, Raffael Gomes. Uma abordagem sobre Forense Computacional.