UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

EDUARDO NOVAK DE CASTRO

ANÁLISE DE FERRAMENTAS PARA COMPUTAÇÃO FORENSE APLICADA A REDE SOCIAL FACEBOOK

CRICIUMA

2019

EDUARDO NOVAK DE CASTRO

ANÁLISE DE FERRAMENTAS PARA COMPUTAÇÃO FORENSE APLICADA A REDE SOCIAL FACEBOOK

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Me. Paulo João Martins

CRICIUMA

2019

EDUARDO NOVAK DE CASTRO

ANÁLISE DE FERRAMENTAS PARA COMPUTAÇÃO FORENSE APLICADA A REDE SOCIAL FACEBOOK

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Criciúma, 24 de junho de 2019.

BANCA EXAMINADORA

Prof. Paulo João Martins - Mestre - (UNESC) - Orientador

Prof. Rogério Antônio Casagrande - Mestre - (UNESC)

Prof. Sergio Coral - Especialista - (UNESC)

Meus pais, grandes incentivadores e maiores exemplos, este trabalho é dedicado a vocês.

AGRADECIMENTOS

A Universidade do Extremo Sul Catarinense – UNESC, pelo ambiente criativo e recursos disponibilizados.

Ao Prof. Me. Paulo João Martins pela orientação e apoio.

A minha família pelo incentivo, dedicação e amor incondicional.

.

“A privacidade está morta, e a mídia social é a principal suspeita.”
Pete Cashmore

RESUMO

Redes sociais se tornaram parte da vida das pessoas no decorrer da última década. Sua popularização se tornou ainda mais massiva após a introdução de novos dispositivos que facilitam seu acesso, como *smartphones* e *tablets*. Destacando-se como a principal destas plataformas sociais, o Facebook possibilita o compartilhamento de qualquer tipo de informação e interação com outros usuários das mais variadas formas, por esse motivo se tornou também um ambiente propício para a ação de criminosos. Crimes contra a honra, falsidade ideológica, tráfico de drogas e pedofilia são alguns dos diversos delitos que podem ser cometidos utilizando esta rede social.

A computação forense, em meios práticos, busca formas de comprovar um crime, coletando provas e evidências digitais, auxiliando a justiça esclarecer quais sejam os delitos ou conduta criminosa praticada pelo uso da rede social.

O presente trabalho tem por finalidade apresentar ferramentas utilizadas para a coleta de evidências especificamente direcionadas ao Facebook, bem como produzir uma análise comparativa sobre os resultados da aplicação destas.

Palavras-chaves: Redes Sociais, Facebook, Crimes Virtuais, Forense Computacional.

ABSTRACT

Social networking has become a part of people's lives over the last decade. Its popularization improved even more massive after the introduction of new devices that facilitate its access, such as smartphones and tablets.
Standing out as the main of these social platforms, Facebook enables the sharing of any kind of information and interaction with other users in a wide variety of ways, which is why it has also become a conducive environment for criminals. Crimes against honor, ideological falsehood, drug trafficking and pedophilia are some of the various crimes that can be committed using this social network.
Computational forensics, in practical ways, looks for ways to prove a crime, collecting proofs and digital evidence, helping justice clarify what are the crimes or criminal conduct practiced by the use of the social network.
The present work has the purpose of presenting tools used to gather evidence specifically directed to Facebook, as well as to produce a comparative analysis on the results of the application of these.

Keywords: Social Networks, Facebook, Virtual Crimes, Computational Forensics.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BEF	*Belkasoft Evidence Finder*
CEO	*Chief Executive Officer*
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CGI	Conselho Gestor de Internet
EUA	Estados Unidos da América
FJF	*Facebook JPG Finder*
FTK	*Forensic ToolKit*
GB	*Giga Byte*
GSM	*Global System for Mobile Communications*
GUI	*Graphic User Interface*
HTML	*Hypertext Markup Language*
IBGE	Instituto Brasileiro de Geografia Estatística
ID	*Identity*
IEF	*Internet Evidence Finder*
IP	*Internet Protocol*
JPG	*Joint Photographic Group*
JSON	*JavaScript Object Notation*
PC	*Personal Computer*
RSA	*Rivest-Shamir-Adleman*
SMS	*Short Message Service*
USB	*Universal Serial Bus*

SUMÁRIO

1. INTRODUÇÃO

Os números de crimes virtuais têm crescido de forma crítica nos últimos anos, dessa forma, fez-se necessário o desenvolvimento de um método de investigação voltado ao meio digital. Apesar de a legislação brasileira não especificar claramente esse tipo de crime, de acordo com Pereira (2010), é possível constatar que os crimes são praticamente os mesmos descritos no Código de Processo Penal, todavia cometidos por meio de computadores e dispositivos semelhantes.

A computação forense tem a alçada de provar que um delito foi cometido utilizando recursos computacionais, de um modo onde os resultados obtidos com a perícia técnica não despertem dúvidas em relação a sua integridade. A crescente leva de crimes cometidos por meios informáticos é motivada, em grande parte das ocasiões, pelo fato das vítimas se tratarem de pessoas leigas no que se refere à segurança de seus dados pessoais em sistemas computacionais. Além disso, existe o fato de as pessoas acreditarem que possuem o anonimato garantido na Internet, estando livres para fazer qualquer coisa, e que não haverá punição fora dela. (LISITA; MOURA; PINTO, 2009).

No passado, a prática de crimes não era possível sem que existisse uma ação humana direta, atualmente essa concepção foi alterada. Um simples acesso à Internet e a utilização de programas de computador especificamente construídos, em diversos casos, é o bastante para qualquer indivíduo praticar um crime. Invasão, acesso indevido ou furto de dados, sabotagem, espionagem, destruir ou adulterar informações, ataques contra ambientes de rede, retenção e compartilhamento de vídeos ou fotos contendo pedofilia, envio não solicitado de anúncios, monitoramento de tráfego de informações e comunicação podem ser alguns dos cenários possíveis.

Da mesma forma que em crimes comuns, o tratamento de crimes cibernéticos requer a coleta de evidências e provas fortes de sua ocorrência, que possa convencer de forma completa os representantes dos poderes eleitos para julgar e punir tais crimes. A composição de provas em crimes virtuais é feita por meio da identificação, coleta e diferenciação de vestígios digitais, ou seja, de informações e dados trocados pelos sistemas computacionais em periféricos,

aparelhos de armazenamento e na própria memória volátil do computador. (SILVA; LORENS, 2009).

Em um mundo contemporâneo e totalmente informatizado, a Internet é hoje ferramenta primordial que proporciona novos padrões de relacionamento social. Nos dias atuais é mecanismo de primeira necessidade, pois, por meio dela, pode-se vender, comprar, fechar negócios e fazer reuniões. Pessoas se conhecem e se relacionam pelas redes sociais, em uma velocidade nunca imaginada há alguns anos. Neste mesmo contexto e velocidade crescem também os crimes virtuais, principalmente os relacionados às redes sociais. Estes crimes tiveram grande aumento, pois sua prática se tornou muito mais fácil, onde diversas informações particulares ficam disponíveis na rede. Dessa forma, os criminosos realizam a coleta dos dados e informações privilegiadas para chantagear ou apenas prejudicar o outro, lesando-o moral e financeiramente.

Ao mesmo tempo, os profissionais da área de computação forense têm desenvolvido e aperfeiçoado uma infinidade de ferramentas que auxiliam na busca pelos vestígios deixados por criminosos, sejam eles físicos ou digitais. Aplicações de código aberto ou contratadas estão disponíveis aos investigadores que devem avaliar o melhor momento para sua utilização e de que forma pode combiná-las a fim de obter os melhores resultados.

1.1 OBJETIVO

1.1.1 Objetivo Geral

O objetivo geral deste estudo compreende a aplicação e análise de ferramentas forense a fim da obtenção de evidências em dispositivos com acesso a rede social Facebook.

1.1.2 Objetivos Específicos

Os objetivos específicos dessa pesquisa consistem em:

- Descrever o conceito de perícia forense computacional e suas áreas de atuação.
- Compreender o funcionamento da rede social *Facebook*, bem como os elementos que compõem uma página de perfil do usuário.
- Aplicar a perícia forense para localizar evidências especificamente na rede social Facebook.
- Utilizar ferramentas forense e realizar uma análise comparativa destas na execução de perícia aplicada ao *Facebook*.

1.2 JUSTIFICATIVA

A Forense computacional é a parte da criminalística que compreende a aquisição, preservação, restauração e análise de evidências digitais, podendo estas estarem em dispositivos físicos ou processadas e armazenadas em ambiente virtual.

As provas em crimes cometidos em ambiente digital se dão através da identificação, aquisição e definição dos vestígios, ou seja, de rastros com dados e informações que ficam contidos na memória física ou volátil dos dispositivos.

Em decorrência do uso da Internet destacam-se o crescimento explosivo do uso das redes sociais como *Whatsapp*, *Facebook*, *Twitter*, *Instagram*, *Linkedin*, *Instagram,* entre diversas outras tão comuns na vida de qualquer pessoa, resultando, dessa forma, em um aumento significativo de sua utilização como atrativo para atividades criminosas e consequentemente na qual um grande manancial de informações é possível de ser encontrado em um determinado perfil de rede social e que, por sua vez, pode ter um amplo valor na apuração de crimes em juízo, assim como qualquer outro meio de armazenamento de dados já habitualmente analisados pela pericia forense computacional.

Uma página do *Facebook*, por exemplo, pode ser usada para planejar um assalto, homicídio, ou um grupo de pessoas mal-intencionadas pode usá-lo para reunir novos membros e defender suas intenções criminais. Apresentar muitas informações a respeito de um suspeito, associadas a conhecidos, amigos, família, mensagens, grupos, entre outros, através das quais é possível criar uma

teia detalhada de informações de relacionamentos acerca do que, ou de quem, se está investigando, podendo colaborar na descoberta de um círculo criminoso inteiro.

A mídia social tornou-se o meio preferido de comunicação para muitos, superando até mesmo o tão conhecido *e-mail* em termos de popularidade e, por consequência disso, qualquer tipo de comunicação inevitavelmente leva à possibilidade de evidência. Como decorrência à popularidade dos meios de comunicações social, encontram-se sujeitos dotados de má índole que passam a ter na mídia social, uma ferramenta oportuna para estreitar a amizade entre criminosos e promover ações delitivas.

A partir desse fundamento surge a necessidade de uma perícia em mídia social, considerando a evolução dos sistemas, ferramentas e técnicas para sua aplicação.

1.3 ORGANIZAÇÃO DO TRABALHO

O presente trabalho está distribuído em 8 capítulos. No primeiro capítulo apresenta-se o projeto, expondo uma breve contextualização e apresentação do problema, assim como os objetivos geral e específicos.

O segundo capítulo é destinado aos conceitos da ciência forense. É realizada uma revisão da literatura sobre o forense computacional e explanado seus principais aspectos. Por fim, uma abordagem sobre crimes virtuais.

O terceiro capítulo analisa especificamente a rede social Facebook. Detalha desde sua criação, passando pelas principais funcionalidades até chegar em telefonia móvel.

No quarto capítulo estão listados os trabalhos correlatos. Com a descrição de suas problemáticas e resultados obtidos.

Um aprofundamento detalhado dos crimes cometidos através das redes sociais é o que apresenta o quinto capítulo. Com uma revisão da literatura do código penal brasileiro e informações sobre os crimes praticas diretamente na rede social tema deste trabalho.

O sexto capítulo descreve os métodos e as ferramentas utilizadas, bem como o detalhamento dos testes com as mesmas.

No sétimo capítulo são abordados os resultados obtidos e confrontados de forma comparativa.

Finalmente, o oitavo capítulo traz a conclusão do trabalho.

2. PERÍCIA FORENSE

O direito e as ciências sempre foram instituições que caminharam em paralelo. Com o passar do tempo, começaram a desenvolver suas próprias características e se entrelaçando. Deve-se isso ao fato de o direito ter adentrado no meio científico e a ciência, por sua vez, no setor jurídico, de acordo com Costa (2002).

Este relacionamento salta ainda mais aos olhos quando falamos da Ciência Forense. Na visão de Sebastiany (et al., 2012), a Ciência Forense é definida como um setor multidisciplinar, que pode abranger tanto a biologia, química, física, informática, entre diversas ciências e sua meta principal é fornecer auxílio às investigações das justiças civil e criminal.

2.1 FORENSE COMPUTACIONAL

Na era tecnológica em que a sociedade atualmente está inserida, o acesso e a dependência da informação nas organizações e computadores pessoais levantam questões complexas quanto à segurança dos dados neles contidos (DIAS, 2000). Erros nos sistemas informatizados podem, de acordo com Dias (2000), afetar a sociedade de inúmeras formas, bem como comprometer informações de instituições financeiras, indústrias, sistemas de telecomunicação entre outros.

Com a crescente disponibilidade de ferramentas de comunicação e interação, a tecnologia, além de trazer benefícios, cria um ambiente para a realização de práticas ilegais e criminosas, conforme Eleutério e Machado (2010). Para Ng (2007), além da acessibilidade ocasionada pela tecnologia digital, tornou-se necessário a inserção de novos conceitos em todas as áreas, bem como a investigação no campo digital. Surgiu, assim, a disciplina forense computacional.

A disciplina de forense computacional produz informações diretas, que podem ser decisivas em um dado caso, ao contrário das demais áreas forenses, que em sua maioria produzem resultados apenas interpretativos, como afirmam Noblett e Pollit (2000).

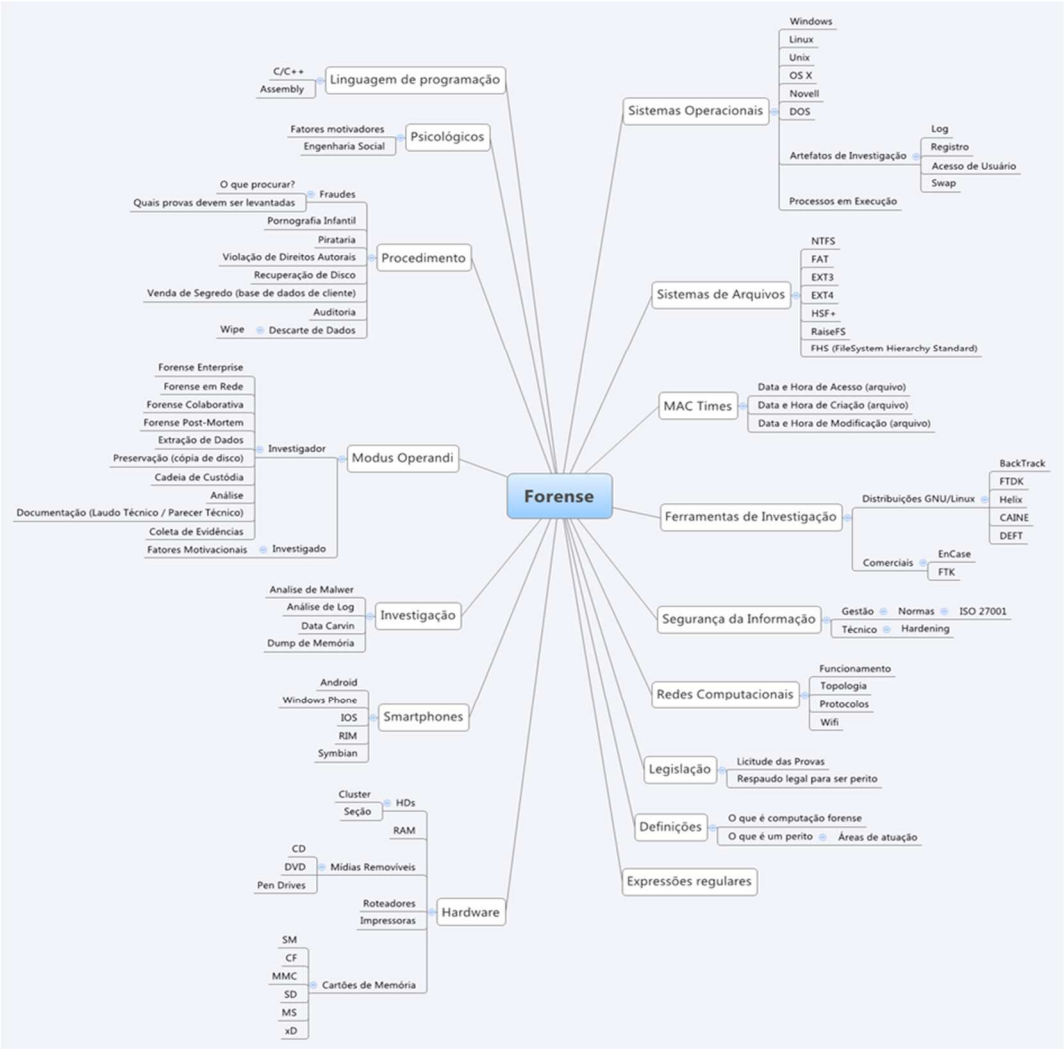
As necessidades jurídicas e de tecnologia da informação se complementam, quando:

> A Computação Forense pode ser definida como uma área da Ciência da Computação que se desenvolve gradualmente para atender à demanda oriunda da área da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação. (MELO, 2009, p. 13).

Da mesma forma, Ng (2007) expõe como objetivo do processo de análise forense computacional o levantamento de materiais válidos para apresentação no âmbito jurídico, apesar da não obrigatoriedade de tal fato.

Na Figura 01 abaixo, é possível observar as diversas ramificações que a perícia forense aplicada à computação pode proporcionar:

Figura 1 - Ramificações da Forense Computacional



Ramificações da Forense Computacional

(*https://4en6br.files.wordpress.com/2012/05/forense1.png*/Brainstorming do Estudo Forense)

Adentrando no âmbito da perícia forense, Freitas (2006, p. 1) afirma que a mesma “é uma área relativamente nova e tornou-se uma prática investigativa importante tanto para as empresas quanto para a polícia”.

Freitas (2006) ainda assegura que alguns procedimentos devem ser seguidos para que as evidências coletadas não sejam contestadas em juízo, comprovando assim, sua legitimidade. Ng (2007) ratifica tal fato afirmando que a perícia forense computacional necessita de metodologia definida e elaboração de estratégia de atuação, para que ocorra o melhor aproveitamento possível do tempo e das evidências em uma investigação.

Assim, a Perícia Forense tem por objetivo principal “a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de

métodos técnico-científicos, conferindo-lhes validade probatória em juízo.” (ELEUTÉRIO; MACHADO, 2010, p. 17).

2.2 APLICAÇÃO

O investigador forense computacional tem como principal objetivo relatar a origem e os eventos pertinentes a um crime ou ato malicioso e encontrar quem o praticou, seguindo uma metodologia de investigação estruturada.

Na visão de Noblett e Pollitt (2000), esse processo se produz pela aquisição, preservação, recuperação e exibição de informações gravadas em formato digital, onde a mesma levanta evidências e recria situações para auxiliar na resolução de possíveis delitos.

2.2.1 Aquisição

O momento da aquisição de provas é de suma importância e a primeira fase do processo. Na visão de Melo (2009), consiste na reunião do máximo possível de provas (elementos a serem analisados). O sucesso de uma análise pericial depende fundamentalmente da qualidade do material coletado e da validade dos procedimentos adotados.

O perito deve se pautar de uma metodologia clara e objetiva de coleta de dados. Para Freitas (2006), a identificação de evidências dependerá da habilidade do perito na busca por dados em fontes diversificadas e de sua familiaridade com o tipo de crime cometido.

Assim, como em uma cena de crime convencional na qual as evidências e provas presentes devem ser guardadas, os dados que constam nos materiais que são enviados para uma análise forense jamais podem sofrer qualquer alteração. Segundo Almeida (2011), deve-se garantir a proteção e idoneidade da prova, para dessa forma evitar quaisquer dúvidas quanto à sua ascendência ou estado inicial, pois a menor suspeita pode ocasionar em sua anulação e colocar toda a investigação em cheque.

Para manipular os objetos em questão, deve-se tomar uma série de precauções, porquanto, até operações simples podem modificar as evidências

ali contidas. Quando se liga o computador, por exemplo, alguns arquivos são alterados, datas de último acesso são modificadas e arquivos temporários são criados, mesmo que nenhuma ação seja tomada por parte do usuário, afirma Almeida (2011). Até mesmo a corriqueira conexão de um *pendrive* na porta USB pode ocasionar o armazenamento de novos dados. Levando isso em conta, todas as atividades devem ser realizadas após se garantir que as informações armazenadas não serão alteradas de nenhuma forma.

Assim, “para que as provas sejam válidas, é de fundamental importância que nenhum dado seja alterado, para que possam ser utilizados numa apresentação judicial. Essa etapa baseia-se em recuperar, reunir e organizar os dados obtidos.” (VIEIRA et al., 2013. p. 6).

Dessa forma, conforme os itens citados anteriormente, Almeida (2011) conclui que o exame forense deve sempre ser realizado em cópias fiéis do material original. As técnicas que são mais utilizadas para este procedimento são a de espelhamento e imagem.

2.2.2 Preservação

Na visão de Melo (2009), a identificação consiste na análise pericial que objetiva organizar os artefatos encontrados, englobando tanto os artefatos identificados no processo antes do desligamento, como também depois do desligamento.

Para Almeida (2011), ao examinar o material, é muito importante que a extração dos dados seja feita com muita atenção e minuciosamente, uma vez que as evidências da prática do delito podem estar nas áreas mais complexas do disco ou até mesmo excluídas.

Assim como na fase anterior, o perito deve continuar sendo metódico no processo de identificação de cada entidade digital. Um elemento crucial para a elaboração do laudo é uma documentação clara. Melo (2009) ainda afirma que dependendo do propósito da perícia, os dados disponíveis no objeto analisado podem expor fatores determinantes para uma investigação, além de criar ligações, mesmo que este objeto não tenha nenhum vinculo com o dispositivo principal.

Após a varredura completa de todos os *bits* do dispositivo, incluindo os arquivos já removidos, é feita também, uma indexação das informações que estão nele contidas. Almeida (2011, p. 24) informa que essa varredura consiste em encontrar todas as assinaturas de arquivos que são conhecidas e deixá-las organizadas de forma que possam ter seu acesso e recuperação da maneira mais veloz possível. Uma vez executado este processo, é possível saber quais são e a quantidade das ocorrências de cada uma das cadeias alfanuméricas.

Deve ser criada uma espécie de catálogo, que teve ter todas as cadeias encontradas e suas respectivas localizações, possibilitando dessa forma a realização de buscas por palavras-chaves nos dispositivos examinados.

2.2.3 Recuperação

Um Perito Forense Computacional experiente, de acordo com Kerr (2011), terá de ter certeza de que uma evidência extraída deverá ser adequadamente manuseada e protegida para garantir que nada seja danificado, destruído ou até comprometido pela execução de maus procedimentos durante a análise e que não seja feita a introdução de nenhum vírus ou código mal-intencionado.

A parte de Recuperação, conforme Melo (2009), consiste na análise de artefatos e da enumeração dos mesmos em uma linha do tempo. É nessa fase em que o perito forense deve mostrar suas principais habilidades.

“A análise de dados é a fase que consiste no exame das informações extraídas na etapa anterior, a fim de identificar evidências digitais presentes no material examinado que tenham relação com o delito investigado.” (ALMEIDA, 2011, p. 24).

Seguindo nessa linha, Almeida (2011) também relata que essa relação é estabelecida pelos pontos organizados pela autoridade solicitante presentes no laudo. Esses precisam ser claros e bem definidos, pois se tornaria inviável analisar de forma individual todo o conteúdo de dispositivo de armazenamento computacional, tomando um tempo relativamente grande do perito e ocasionando uma redução na eficiência dos exames forenses.

2.2.4 Exibição

Essa é a fase final de uma análise forense, onde o perito responsável constrói um laudo de acordo com os resultados encontrados durante toda a análise, juntamente com as técnicas utilizadas na aquisição, recuperação e preservação. É feito uma cópia das evidências, que são armazenadas em mídias digitais, como CDs ou DVDs.

De acordo com Constantino (2012), o laudo pericial é um documento técnico-científico e deve ser escrito de forma que fique claro e objetivo, detalhando todos os processos e métodos dos exames realizados, para que o mesmo não venha a gerar dúvidas em relação a sua veracidade. O laudo tem uma estrutura própria e bem definida, formada por seções, são elas:

- Preâmbulo – identificação do laudo;
- Histórico – é opcional, caso o perito julgue necessário, são informados os fatos e interesses que levaram ao laudo;
- Material – onde descreve detalhadamente o que foi analisado;
- Objetivo – qual o objetivo desse laudo;
- Considerações técnicas/periciais – também opcional, algum detalhe importante que o perito identificou durante a análise,
- Exames – descreve os passos e procedimentos realizados;
- Respostas aos quesitos/conclusões – resumo dos resultados.

Essa estrutura é utilizada em qualquer tipo de laudo pericial computacional.

2.3 TIPIFICAÇÃO DOS CRIMES VIRTUAIS

Conforme Eleutério e Machado (2010), crimes sempre deixam vestígios e, no âmbito da computação, os vestígios são digitais e precisam de um profissional qualificado para o exame e a elaboração de laudos específicos.

Para os autores, os crimes podem ser definidos de duas formas. A primeira é a utilização de computadores para a realização de crimes já existentes, como sonegação fiscal, falsificação de documentos e tráfico de entorpecentes. Já na segunda modalidade, o computador age como o item

principal para a realização do crime, bem como: ataques a *sites*, roubo de informações, *phishing*[1], roubo de senhas através de programas mal-intencionados, entre outros novos delitos advindos do uso de computadores e Internet. (ELEUTÉRIO; MACHADO, 2010).

No texto da Lei n. 12.737 de 30 de Novembro de 2012, que descreve a tipificação criminal de delitos informáticos e altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal, acrescenta a pena de detenção de 3 (três) meses a 1 (um) ano, e multa para o seguinte artigo:

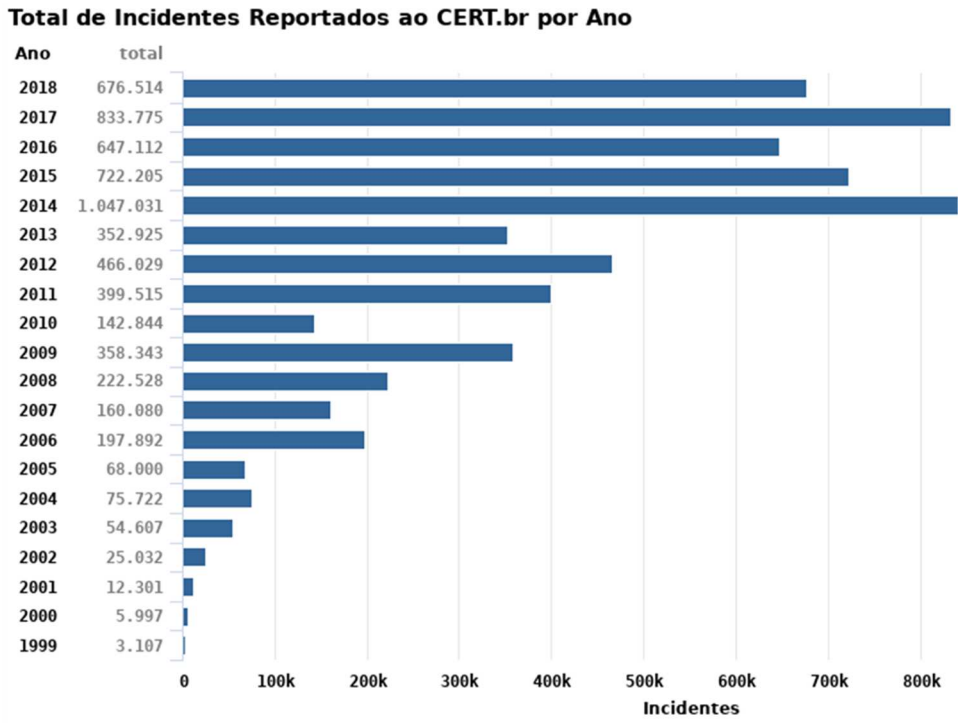
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

No mesmo Decreto-Lei, discorre-se a pena para os atos de “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”, com pena de detenção de 1 (um) a 3 (três) anos, e multa e “Falsificação de documento particular” ou “Falsificação de cartão”, com pena de reclusão de 1 (um) a 5 (cinco) anos, e multa. (BRASIL, Decreto-Lei n. 2.848, de 7 de dezembro de 1940).

O Grupo de Resposta a Incidentes de Segurança no Brasil (CERT.br) é mantido pelo Conselho Gestor de Internet no Brasil (CGI.br) e responsável por analisar os incidentes de segurança de computadores conectados à Internet brasileira. (CERT.br, 2014).

Segundo o gráfico abaixo, com informações recolhidas pelo CERT.br desde 1999, o pico de alertas recebidos foi no ano de 2014, chegando a mais de um milhão incidentes reportados:

Figura 2 - Incidentes de segurança reportados ao CERT.br



Fonte: CERT.br (2019).

3. FACEBOOK

3.1 HISTÓRICO

A história do *Facebook* tem início em Harvard, no ano de 2003. Então com 20 anos, Mark Zuckerberg cursava o segundo ano de Psicologia e, em um momento de puro tédio, decidiu utilizar um código que havia escrito para criar um *site* para comparar seus colegas de quarto. Ele utilizou fotos de animais com os nomes de seus amigos e comparava qual seria o mais bonito.

Dessa brincadeira entre companheiros de classe surgiu o *Facemash*. Zuckerberg decidiu utilizar seu conhecimento em segurança de dados e redes de computador para acessar sem permissão o servidor da universidade e utilizar as fotos de todas as estudantes. Através da pergunta "*Who's Hotter? Click to Choose*", o site apresentava duas imagens com um símbolo de versus entre eles, como uma disputa. Depois de o usuário selecionar qual das opções

apresentadas julgava mais atraente, o voto era contabilizado para o ranking principal e uma nova disputa surgia.

De acordo com López (2017a), menos de vinte e quatro horas depois de sua publicação, o *Facemash* já havia sido acessado por mais de quatrocentos e cinquenta pessoas, que por sua vez emitiram mais de vinte e dois mil votos, além de iniciarem a divulgação através de seus *e-mails*. Poucos dias depois, o novo *site* tornara-se febre dentre os alunos e inevitavelmente passou a ser conhecido também pelas autoridades de Harvard. O Conselho de Administração de Harvard acusou formalmente Mark por violação de segurança, direitos autorais e privacidade individual de seus estudantes. Sob uma enxurrada de críticas e na iminência de ser expulso, Zuckerberg encerrou a página e pediu desculpas públicas pelo ocorrido.

O código do *Facemash* seguiu sendo desenvolvido mesmo após o encerramento da plataforma, seu formato e identidade visual passaram por modificações e, em fevereiro de 2004, foi publicado sua segunda versão. Dessa vez o título, ao invés de "*Who's Hotter?"* apresentava "*Welcome to Thefacebook*" (Figura 3).

Figura 3 - Thefacebook

Página inicial do Thefacebook; Fonte: entrepreneur.com (2017).

Segundo Cassidy (2006), a nova página foi divulgada pela lista de *e-mails* da universidade e em menos de vinte e cinco horas o *Thefacebook* já possuía mais de mil e quinhentos registros. Outro fator determinante para a rápida popularização desta nova plataforma, aliado a repercussão obtida pelo *Facemash*, foi a acusação recebida de três acadêmicos sênior de Harvard.

Uma semana após o lançamento, Cameron Winklevoss, Tyler Winklevoss e Divya Narendra acusaram Mark de tê-los enganado. Segundo eles, Zuckerberg foi contratado para desenvolver uma rede social denominada "*HarvardConnection.com"* e, posteriormente, teria abandonado o projeto e roubado a ideia para criar sua própria rede social. A acusação deflagrou um processo de investigação sobre o caso e acabou com os três veteranos movendo uma ação judicial contra Mark Zuckerberg. Por fim, segundo McGinn (2004) ambas as partes chegaram a um acordo no ano de 2008.

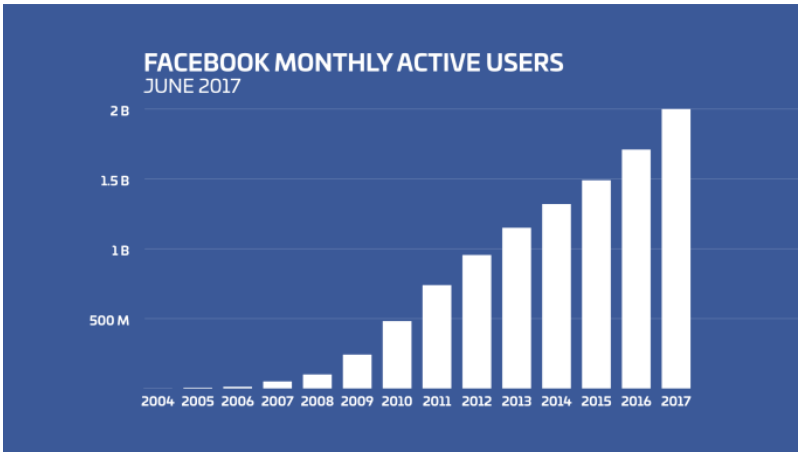
Com pouco mais de trinta dias a pleno funcionamento, mais da metade dos estudantes de Harvard já tinha uma conta no *TheFacebook*, bem como a rede social já se fazia presente em outras universidades, em uma franca expansão. O empreendimento crescia de forma exponencial e Mark decidiu montar uma equipe com seus colegas de classe Dustin Moskovitz e Chris Hughes para uma gestão mais assertiva.

Conforme Phillips (2007), o criador do *software* de compartilhamento de arquivos *Napster*, Sean Parker demonstrou interesse pelo promissor projeto e decidiu oferecer seus serviços à recém-formada equipe. Acabou tornando-se, de maneira informal, um assessor de Zuckerberg em busca de novas conexões no mercado e práticas de negócio. No verão de 2004 a empresa saiu do campus da Universidade de Harvard e passou a ter sede na cidade de Palo Alto, na Califórnia, e Parker foi oficializado no cargo de primeiro presidente do *TheFacebook*.

No ano seguinte, mais de oitocentas redes universitárias estavam conectadas através desta rede social. Foi quando surgiu a necessidade da troca do domínio do *site* para um novo mais robusto. Com movimento, o endereço passou a ser apenas "*facebook.com"* e a empresa passou a se chamar simplesmente *Facebook*.

A última grande expansão ocorreu no ano de 2006. Segundo Brown (2008), foi a partir desta data que se tornou permitido que qualquer usuário de Internet com idade superior a treze anos e com um endereço de *e-mail* válido possa criar uma conta. Como fica evidenciado na Figura 04, a rápida expansão das redes com acesso liberado ao *Facebook* implicou em um crescimento exponencial em seu número de usuários ativos, com raros índices de queda de popularidade.

Figura 4 - Usuários Ativos Facebook



Fonte: techcrunch.com (2017)

3.2 FUNCIONALIDADES

Juntamente com a rápida popularização entre os usuários de Internet por todo o mundo, o *Facebook* também passou por diversas modificações e atualizações em sua lista de funcionalidades. A fim de promover uma melhor experiência para seu público, melhorando e reinventando os quesitos de interação entre as pessoas e compartilhamento informações entre as partes mostrados nas demais redes sociais da época.

Enviar mensagens simples, compartilhar imagens ou vídeos, ler notícias e interagir com o conteúdo publicado pelos outros, volveu-se muito intuitivo e simples por conta desses mecanismos. De acordo com Donelly (2018), hoje setenta e nove por cento da população dos Estados Unidos possui um perfil no *Facebook* e destes, cinquenta e três por cento o utilizam por diversas vezes ao dia. Todos os dias, trinta e cinco milhões de pessoas atualizam seus *status* em um dos cento e um idiomas que a rede social disponibiliza.

A seguir, serão descritas as funcionalidades que forma a base da rotina de acesso para a maioria dos usuários e de que forma se dá seu funcionamento.

3.2.1 Pedidos de Amizade

Na visão de Heussner (2009), esta é a funcionalidade base do *Facebook*. Pedidos de amizade é a essência desse negócio, pois é através deles que você tem a oportunidade de se conectar com os demais usuários da rede e torná-la, de fato, social.

O mecanismo é bem simples, segundo Galanes (2009) consiste no envio de uma requisição para outra pessoa solicitando uma conexão entre as partes. No caso da resposta positiva do destinatário, ambos se tornam amigos e todas as informações de seus perfis e futuras atualizações ficam visíveis.

É também possível rejeitar a requisição de amizade ou até excluir a amigo já aceito, bem como bloquear esse amigo, caso não queira mais ser incomodado por ele. Em ambos os casos o utilizador rejeitado não recebe qualquer notificação sobre o ocorrido (Facebook, 2018a).

3.2.2 Reações

Descritas como uma forma de “fazer comentários e conectar-se com coisas importantes para você” (Facebook, 2018b), as reações transformaram-se em peças chaves para o funcionamento dos algoritmos e das interações entre os clientes do *Facebook*.

Criado em 2009, o botão *Like* que significa a palavra “Curtir” foi a primeira das reações a ser inserida. Os usuários passaram a utilizar essa funcionalidade para avisar as demais pessoas de sua rede quando “gostou” ou ‘’curtiu’ determinada foto, alteração de *status* ou publicação. (Facebook, 2018c)

No ano seguinte, o botão “Curtir” ficou disponível também para uso em *sites* fora da rede social. Dessa forma o *Facebook* recebia informações de perfil de seus usuários através de páginas que eles interagiam sem estarem em sua plataforma (Facebook Developers, 2011). Segundo Albanesius (2009), tal ação gerou alguns problemas com países como Alemanha e Canadá que alegaram

sobre a referida forma de coleta de dados na qual infringia as políticas de proteção de informação desses países.

A mais recente atualização desta funcionalidade sobreveio no ano de 2016, na qual foram inseridos mais cinco modos de se reagir a postagens. Sendo elas as de “*Love*”,” *Ha-ha*”, “*Wow*”, “*Sad*” e “*Angry*” (Facebook, 2018d).

Figura 5 - Tipos de Reação Facebook

Fonte: facebookbrand.com (2016)

3.2.3 *Feed* de Notícias

Inicialmente, após inserir seus dados de usuário e senha e acessar a rede social, era mostrada a tela principal. Nela estavam contidas suas informações de perfil para atualização e personalização. No entanto, caso optasse por outras formas de interação, era necessário buscar manualmente por essas novas páginas.

Segundo Costine (2016), com a introdução do *NewsFeed* (algo como “abastecimento de notícias”, em português) em 2006 a página inicial do *Facebook* foi totalmente reconstruída para mostrar as últimas atualizações de status e fotos das outras pessoas que fazem parte da sua rede. A página de perfil do usuário também recebeu uma *mini-feed* com suas últimas postagens e passou a ser chamada de “mural”.

De acordo com Clark (2018a), dois anos após sua criação o *Feed* de Notícias sofreu sua primeira grande alteração. No ano de 2009, através de informações coletadas pelos recursos de “curtir” e “compartilhamentos”, as postagens, antes mostradas na ordem de a mais recente para a mais antiga, agora passaram a ser exibidas por ordem de popularidade. Quesito que era baseado no nível de engajamento recebido pela publicação, sendo ele contabilizado através de visualizações, comentários, entre outros.

Ainda segundo Clark (2018b), apesar das reclamações de muitos usuários que preferiam o modo cronológico do *Feed* e assim usavam

paralelamente a nova atualização, o *Facebook* ignorou tais reivindicações e decidiu unir os dois modos. Dessa forma, lançou uma terceira versão onde eram apresentadas primeiramente as publicações das pessoas mais próximas ao usuário, como familiares e companheiros, e logo depois viriam as mais recentes. A partir deste movimento, foi instituído o uso de algoritmos para a montagem do *feed* do utilizador, uma vez que a ordem era apresentada dependendo de quanto tempo se passara desde seu último acesso.

Em constante evolução, o mural de notícias tornou-se o carro chefe do *Facebook.* Em 2015, de acordo com Hillstead-Jones (2018a), ganhou a função *See First* (ver primeiro) onde o utilizador seleciona quais páginas deseja acompanhar e recebe notificações sempre que surgir um novo conteúdo. Nesse mesmo ano, também foram implementados os suportes a *gifs* e compartilhamento de *links*.

Ciente da dimensão e do alcance se sua plataforma, segundo Hillstead-Jones (2018b), o *Facebook* direcionou seu foco para o conteúdo publicado por seus utilizadores. Foram criados recursos para denunciar boatos e notícias falsas, onde os usuários podem reportar a uma equipe de mediadores qualquer postagem que julgarem inverdade ou até mesmo ofensiva. Dessa forma podendo ser retirado o engajamento da publicação ou até mesmo a remoção, dependendo da gravidade.

3.2.4 *Fan pages*

À medida que o serviço se popularizava, os perfis criados passaram a apresentar uma maior diversidade. Quando no início se tratava exclusivamente de indivíduos, ou seja, pessoa física, o *Facebook* passou a receber em sua plataforma também marcas, bandas, empresas, instituições, organizações e figuras públicas.

Em 2007, percebeu-se uma oportunidade de atender a esta emergente demanda bem como uma forma de trazer dinheiro para a empresa com uma alternativa a clássica página de perfil do usuário: as *Fan Pages*.

De acordo com Beese (2016a), as *Fan Pages* do *Facebook* são uma forma de representar uma organização ou companhia. Para quem visita,

assemelha-se ao perfil comum, no entanto, possui uma infinidade de ferramentas para gerenciamento e rastreamento do engajamento obtido.

Outra grande vantagem é o número ilimitado de seguidores. Enquanto nos perfis convencionais se faz necessário a solicitação de amizade para um limite de cinco mil amigos, nas *fan pages* basta clicar no botão “Curtir” (*Like*).

Segundo Ayres (2013a), os principais fatores que diferenciam os dois modelos de apresentação são anúncios, agendamento de postagens, informações demográficas e interação facilitada**.**

As dez maiores *fan pages* registradas no *Facebook* possuem, somadas, mais de 970 milhões de seguidores (SocialBakers, 2018a). O jogador português Cristiano Ronaldo é a figura pública que possui a maior audiência, falando diretamente para 122 milhões de contas.

Discorrendo exclusivamente de marcas, a atual líder é a austríaca *Red Bull*. A fabricante de bebidas energéticas tem quase cinquenta milhões seguidores em sua conta, seguida pela sul-coreana Samsung com cinco milhões de fãs a menos (SocialBakers, 2018b).

3.2.5 Grupos

Lançados em 2006, os grupos são páginas destinadas aos usuários com interesses em comum, no qual podem compartilhar informações e conhecimentos. Qualquer pessoa pode criar um grupo sobre qualquer tópico, causa ou evento.

De acordo com Martín (2019), os grupos no *Facebook* são classificados com base em dois tipos: tópicos e privacidade. O primeiro define o tipo, ou seja, sobre o que se trata o grupo em sua essência, podendo este ser sobre: jogos, viagens, música, empregos e diversos outros tipos. O segundo trata-se das propriedades de privacidade, ou seja, as regras de acesso para os membros e não membros do grupo podendo elas ser do tipo público, fechado ou secreto. Quando público, a visualização das informações é permitida a qualquer usuário, assim como o de ingressar no grupo sem qualquer tipo de autorização. No caso de um grupo definido como fechado, a autorização de um dos administradores é necessária. Por fim, um grupo do tipo secreto não pode ser visualizado por um

não membro e a única forma de ingresso é por meio de convite dos criadores ou membros do grupo.

3.3 MOBILE

Durante as duas últimas décadas, as redes de comunicação móveis passaram por mudanças bastante significativas, com o aperfeiçoamento da tecnologia no segmento. Segundo Vora (2015a), as redes de telefonia móvel sem fio são divididas em gerações (G) na qual cada uma se refere a alterações em sua natureza de sistema, velocidade, tecnologia, frequência, capacidade de armazenamento, latência, entre outros padrões que as diferenciam das anteriores.

A primeira geração (1G), conforme descreve Vora (2015b), era analógica e utilizada somente para chamadas de voz. Essa geração estendeu-se entre o fim dos anos 70 e o início dos anos 90, quando foi substituída por sua sucessora.

A segunda geração (2G) foi introduzida com três grandes alterações em relação a anterior, destaca Kumar (2018a). A comunicação passou a ser de forma digital, adotando o padrão GSM (*Global System for Mobile Communications* ou Sistema Global para Comunicações Móveis) e os sistemas se tornaram muito mais efetivos quando comparados aos da primeira geração. Além disso, também foi incorporado o recurso de SMS (*Short Message Service* ou Serviço de Mensagens Curtas). As redes de comunicação 2G duraram, em sua maioria, até o início dos anos 2000.

Sucedendo a segunda geração até o início da década de 2010, as redes 3G trouxeram uma taxa de transmissão de dados muito maior, conforme afirma Vora (2015b), bem como melhoras em termos de capacidade e introdução do suporte para multimídia. Na visão de Kumar (2018b), a terceira geração tornou possível a navegação *web*, chamadas de voz por Internet sem fio (*wireless*) e chamadas de vídeo.

A quarta geração (4G), por sua vez, contempla todos os recursos apresentados na geração que a antecede além de inserir novas funcionalidades para garantir o suporte a redes móveis sem fio e, dessa forma, acompanhar a evolução dos aparelhos celulares em termos de velocidade de conexão e taxa

de transmissão de dados, que estavam limitados ao alcance que obtinham com a 3G. As redes de comunicação da quarta geração são as que se encontram vigentes no mercado, pelo menos durante os próximos dois anos, quando se prevê o lançamento da próxima geração.

Com início da implantação previsto para 2020, a quinta geração (5G) promete alçar as potencialidades utilizadas atualmente em padrões altíssimos de velocidade de conexão e de usuário simultâneos. Conforme Helerbrock (2019), as redes 5G devem consumir até 90% menos energia, diminuir em até seis vezes o tempo de conexão entre os aparelhos e dobrar o número de usuários conectados por área.

3.3.1 *Facebook Mobile*

Com a chegada da terceira geração das redes de telefonia móvel (3G) e a constante evolução das tecnologias contempladas nos aparelhos, tornou-se cada vez mais comum as pessoas utilizarem seus celulares para outras tarefas, além de realizar chamadas de voz ou enviar mensagens de texto. Agora era possível controlar os *e-mails*, realizar vídeo conferências, acessar *sites* da Internet para ler notícias e atualizar a sua rede social.

Percebendo a demanda cada vez maior nos acessos por Internet móvel, em 2007 o *Facebook* divulgou em seu blog que o site *m.facebook.com* estava disponível e que estaria disponível para cada usuário que possuísse um telefone. De acordo com Casti (2013a), o primeiro *website* móvel oferecia uma navegação otimizada para telas pequenas, permitindo ao usuário subir fotos, postar mensagens, solicitar amizades e “cutucar” através de SMS.

Ainda em 2007, conforme relata Casti (2013b), o mercado foi revolucionado com o lançamento do *iPhone*. O smartphone da *Apple* introduziu as telas grandes e sensíveis ao toque (*touchscreen*), e rapidamente foi seguida pelas demais marcar fabricantes. Iniciava-se a era dos *smartphones*. Desta forma, foram lançados os sites *iphone.facebook.com* e posteriormente o *x.facebook.com*, para contemplar os demais *smartphones*.

Dois anos depois já era possível encontrar aplicativos (*App’s*) do *Facebook* em quase todas as plataformas disponíveis, além do acesso via navegador, representando mais de 100 milhões de acessos por mês. Estava

claro que a companhia precisava tornar sua presença no mercado móvel muito mais robusta.

Segundo Casti (2013c), em 2010, o *Facebook* lançou seu aplicativo próprio. Esse não foi bem recebido pelo mercado devido aos constantes erros que apresentava e por não se tratar de uma versão nativa para os sistemas dos aparelhos da época. O *Facebook App* não decolou até a empresa decidir em 2012 que a parte de tecnologia móvel se tornaria sua prioridade. Adquiriu por um bilhão de dólares o aplicativo de fotos *Instagram* e reformulou completamente o *Facebook App* para a plataforma *iPhone*.

Atualmente, Bullas (2019) afirma que mais de noventa por cento dos usuários ativos acessam o *Facebook* através de dispositivos móveis. Índia, Estados Unidos, Brasil e Indonésia são os campeões de acessos, com mais de 100 milhões usuários cada. Com exceção dos EUA, todos os demais países são mercados emergentes onde o acesso por dispositivos móveis é muito superior aos demais, em que na maioria das vezes a primeira experiência do usuário com a Internet é através de um dispositivo de baixo valor com um plano de dados também pouco caro.

4. TRABALHOS CORRELATOS

A perícia forense computacional, apesar das poucas publicações oficiais encontradas, atualmente vem apresentando uma grande diversidade de estudos acadêmicos. A seguir, apresentam-se alguns trabalhos que são correlatos ao tema abordado nesta pesquisa.

4.1 USO DE APLICAÇÕES OPEN SOURCE NA PRÁTICA DE PERÍCIA FORENSE COMPUTACIONAL

Este trabalho de conclusão de curso foi desenvolvido por Sergio Rosa da Silva Júnior e apresentado ao curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, em 2012.

O objetivo principal do autor foi abordar exemplos de métodos de análise forense e fazer um estudo comparativo entre estes métodos, viabilizando a melhor técnica em torno das mais variadas formas de análise utilizando a ferramenta FTDK (Forense digital Toolkit), uma distribuição livre UbuntuBR que possui em seu conteúdo um conjunto de mais de 100 (cem) ferramentas voltadas a perícia forense computacional, dessa forma, simulando o uso da ferramenta, coletando dados, examinando, analisando e recuperando arquivos.

Os resultados obtidos mostraram que a computação forense não é focada somente na área de investigação e criminalista, uma vez que grandes empresas estão surgindo com o propósito de recuperar dados valiosos que foram perdidos de forma acidental ou maliciosa. A ferramenta utilizada, FDTK-UbuntuBR, mostrou-se bastante eficaz na simulação da busca feita em imagens, incluindo sua facilidade de uso. Sendo assim, a ferramenta fez jus a sua fama, tornando-se um fato e verídico na sua aceitação pelos peritos e seus numerosos downloads, tornando-se, dessa forma, recomendada a profissionais ingressantes e experientes na área.

4.2 COMPUTAÇÃO FORENSE: EXAMINANDO DISPOSITIVOS DE ARMAZENAMENTO COMPUTACIONAL.

Este trabalho constituiu em uma monografia desenvolvida em 2012 por Luan Francisco da Silva Ramos e Wanderson Flores de Matos requisito parcial para obtenção do grau em Bacharelado em Ciência da Computação do Centro Universitário do Estado do Pará – CESUPA.

Os autores tomaram por objetivo principal desenvolver um estudo sobre Forense Computacional, mais especificamente sobre as fases de uma investigação computacional, deixando esclarecida as suas funções, e a importância de cada uma delas em processos de crimes computacionais. Bem como estudar conceitos, conhecer tipos de evidências e questões jurídicas.

Ao final, expuseram as dificuldades para encontrar materiais envolvendo o assunto, principalmente em português. Enfatizando que a escassez de literaturas sobre Forense Computacional se deve muito ao fato de ser um assunto ainda muito novo.

Finalmente, conseguiram provar a eficácia de exames forense através de evidências coletadas pelas ferramentas abordadas durante o trabalho.

4.3 TÉCNICAS DA COMPUTAÇÃO FORENSE

Trabalho de conclusão de curso de Bacharelado em Ciência da Computação do Instituto de Ensino Superior de Assis (IMESA) e Fundação Educacional do Município de Assis (FEMA). Desenvolvido por Diego Zaratini Constantino, no ano de 2012.

Objetivou-se com este trabalho um melhor entendimento sobre a computação forense e levantamento de evidências. A necessidade de um maior conhecimento dos profissionais da área tecnológica em segurança e o crescimento dos conceitos sobre computação forense tornaram-se fundamentais para o desenvolvimento deste trabalho. Também foram abordadas as técnicas e metodologias de uma análise forense, iniciando-se pela coleta dos materiais e equipamentos até à extração de arquivos e dados e a partir de um estudo de caso, foi confeccionado um laudo pericial.

Ao término do trabalho, foi possível identificar a função e fundamentação da computação forense em dispositivos computacionais, bem como tudo e qualquer tipo de informações que são ou foram transmitidas de um dispositivo, pois tudo o que é feito em quaisquer desses dispositivos, deixa algum vestígio ou rastro. Estes que, através dos tópicos abordados, foram identificados.

4.4 O PAPEL DO ETHICAL HACKING NA FORENSE COMPUTACIONAL:RESPECTIVAS CONTRIBUIÇÕES EM PROCESSOS INVESTIGATIVOS

O título acima foi um trabalho de Conclusão de Curso, desenvolvido em 2013 por Sidney Akira Hakata e apresentado a FACSENAC-DF, Faculdade Senac do DF, como requisito para a obtenção do título de Especialista em Segurança da Informação.

A finalidade do artigo é explicar a relação entre Forense Computacional e Ethical Hacking, e suas respectivas contribuições para a sociedade, por meio de ferramentas e técnicas específicas reconhecidas e validadas perante diretrizes estabelecidas, apoiadas ainda na legislação.

Foram definidos como resultados demonstrar os aspectos operacionais e investigativos da Forense Computacional e a respectiva associação com técnicas de Ethical Hacking, utilizando ferramentas de auditoria, detecção e correção de vulnerabilidades, propondo-se que para trabalhos futuros os profissionais de áreas como tecnologia e segurança da informação utilizem como documento de referência em suas atividades.

4.5 ANÁLISE E COMPARAÇÃO DE SOFTWARES PARA PERÍCIA FORENSE EM AMBIENTES *LINUX* BASEADO NA MÉTRICA *FUNCTION POINT ANALYSIS*

Este é um trabalho de conclusão de curso desenvolvido por Paula Porfírio Teixeira para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense – UNESC, apresentando em Junho de 2010.

Teve por objetivo principal fazer uma comparação de softwares para perícia forense voltados ao ambiente *Linux*, baseado em métricas de software. Especificamente voltado para descrição e definição destas métricas, delimitação de ambientes e realização de testes, e posteriormente a análise dos resultados.

A pesquisa apresentou conceitos de perícia forense computacional, aplicando-os na análise das ferramentas *The Sleuth Kit*, versão 3.1.2, utilizando a sua interface gráfica *Autopsy*, e o *SMART Linux*.

A análise foi realizada baseando-se na métrica de software Pontos de Função (FPA), com o objetivo de medir a qualidade do software. Também foi realizada uma segunda análise levando em consideração a quantidade de recursos que as ferramentas disponibilizam. Por fim foram comparados os resultados de ambas as ferramentas, quantidade de recursos de cada uma e a qualidade dos mesmos, segundo a métrica FPA. Baseando-se no resultado desta comparação é possível observar que a ferramenta *The Sleuth Kit* é a que possui uma maior quantidade de recursos e detém uma maior qualidade dos mesmos, de acordo com a métrica citada.

5. REDES SOCIAIS COMO MEIO PARA CRIMES

Com a chegada da Internet, a comunicação entre as pessoas e as instituições passou a se dar de forma muito mais ágil, limites geográficos foram superados, em poucos minutos milhões de pessoas interagem através de seus computadores seja comprando, vendendo ou se comunicando, em tempo real, com uma ou várias pessoas, através dos correios eletrônicos (*e-mail*), páginas eletrônicas, bate-papo, aplicativos de mensagens entre outros.

De acordos com uma pesquisa do Instituto Brasileiro de Geografia Estatística (IBGE), postada no site da ITMÍDIA, em 20 de dezembro de 2018, o Brasil possui 145,2 milhões de pessoas com acesso à Internet. O que coloca o país à frente do Canadá, México e Argentina no número de usuários, sendo o décimo colocado em todo o mundo.

Esse capítulo tem o objetivo de evidenciar a importância de um estudo sobre os crimes digitais, os quais já se fazem presentes no cotidiano da sociedade, prejudicando desde cidadãos comuns até grandes corporações, devido ao cenário propenso que os criminosos, muitas vezes definidos como *hackers*, encontram para efetuar suas ações e não arcarem com alguma represália pelo delito cometido. Também discorre sobre arquétipos do modo que crimes podem ser praticados utilizando computadores, a *Internet* e as redes sociais e o que a legislação brasileira e mundial vem fazendo para não perder o controle sobre esse tipo de infração. Após o advento da *Internet*, várias outras modalidades de crimes que, dentro do nosso ambiente jurídico, não possuem uma resolução bem definida para esse tipo de exercício que vem acontecendo em todos os lugares.

Assim, faz-se necessário dissertar algumas considerações sobre a definição de um crime, ou, o que o sistema jurídico avalia como crime.

5.1 CONSIDERAÇÕES SOBRE CRIME NA LEI PENAL BRASILEIRA

De acordo com a definição analítica de crime, é necessário que o agente tenha executado uma ação composta de três características imprescindíveis,

são elas: Tipicidade (fato típico), Antijuridicidade (antijurídico) e Culpabilidade.

> Fato típico – é o padrão de conduta que o Estado, através da lei, visa impedir que seja praticada. Tipo é a descrição precisa do comportamento humano feita pela lei penal.
> O fato típico possui os seguintes elementos: - conduta dolosa ou culposa, comissiva ou omissiva; - resultado (nos crimes onde se exija um resultado naturalístico.) - nexo de causalidade entre conduta e resultado; -tipicidade (formal e conglobante).
> Antijuridicidade ou ilicitude – é a relação de contrariedade que existe entre a conduta que o agente realiza e o ordenamento jurídico.
> Culpabilidade é a reprovação pessoal que se faz sobre a conduta ilícita do agente.
> A culpabilidade possui os seguintes elementos: - imputabilidade; - potencial consciência sobre a ilicitude do fato; - exigibilidade de conduta diversa. (GRECO, Rogério. Curso de direito penal - parte geral, v. I, p.158-159).

Precisa-se seguir uma determinada sequência durante a análise do delito praticado por um agente para concluir se é ou não crime, ou seja, deve-se verificar inicialmente a tipicidade da conduta, em seguida a antijuridicidade e por final a possibilidade de culpa.

A *Internet* passou a fazer parte de nosso quadro social e desde então o Direito se fez necessário para assegurar estas relações e proteger o bem jurídico quando este é lesado. O Direito penal foi criado para proteger os bens jurídicos avaliados como de maior importância para a sociedade, a vida é um dos principais exemplos desta categoria de proteção. A definição de crime não possui diferença entre delitos comuns e para os crimes cibernéticos, isto é, ação humana que ocasione lesão ou ameaça contra os bens de maior importância para a sociedade, o comportamento do ser humano nos dois casos está sujeito a uma punição prevista em lei.

O art 1° do Código Penal discorre que: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”. Este artigo pode ser aplicado tanto para os crimes por meio digital quanto para os crimes comuns, porque, não é possível punir uma pessoa se o ocorrido não for considerado crime pelo nosso ordenamento jurídico. O Código Penal admite que diversos crimes cometidos utilizando um computador possam ser inseridos nos tipos penais descritos, pois no momento em que a conduta humana se ajusta de uma forma repressiva ela está apta a uma sanção penal.

Na legislação brasileira consta punição para tais delitos, mesmo que com lentidão, proporciona uma área responsável por proteger as informações, conforme a Lei de Software 9609/98. Todavia, bastante ainda precisa ser feito para que os crimes digitais tenham as punições desejadas pela sociedade. Alterada em 1998, a Lei do Software discorre sobre a proteção da propriedade intelectual de programas de computador e seu comércio. Contratos de licença de utilização, direitos autorais, registros de sistemas, garantias para usuários, compra e venda, transferência de tecnologia são alguns dos itens tratados na lei. Também estão previstas as infrações e penalidades, principalmente para quem não cumpre as regras de proteção da propriedade intelectual.

A lei recém citada explicou algumas condutas, sendo correto que elas não são exaustivas nas formas do indivíduo praticar crimes virtuais, mas certamente foi o pontapé para a elaboração de uma codificação. Os crimes efetuados utiliando a *Internet* trazem um grande problema para o Direito em virtudo do vasto universo em que trabalham os criminosos e o nível intelectual elevado que estes possuem.

A facilidade no compartilhamento de informações que a rede proporciona vem ocasionando um desconforto nos legisladores de todo o mundo. Sendo que os criminosos cibernéticos estão, em grande parte dos casos, protegidos pelo anonimato, o que torna mais difícil a sua identificação e localização. O criminoso não aparece fisicamente e pode agir de qualquer localidade do planeta, por este motivo tem a impressão de que estão operando imunes às leis.

Através da *Internet*, uma pessoa que reside em outro continente pode cometer um crime no Brasil. De que forma se pode punir este tipo de ação? Em nosso ordenamento jurídico existe o princípio da territorialidade, isto é, o local onde o delito foi realizado. O mesmo é dividido em três teorias: Teoria da atividade; Teoria do resultado e Teoria mista ou ubiquidade. Conforme esclarece GRECO.

> A teoria da atividade diz que lugar do crime seria o da ação ou da omissão, mesmo que outro fosse o da ocorrência do resultado. A teoria do resultado despreza o lugar da conduta e defende a tese de que lugar do crime é onde ocorre o resultado, e teoria mista ou da ubiqüidade adota as duas posições anteriores e diz que lugar do crime será o da ação ou da omissão, bem como onde se produziu ou deveria produzir-se o resultado. (GRECO, Rogério. Curso de Direito penal – parte geral, v. I, p.136).

O Código Penal brasileiro considera a teoria mista ou da ubiquidade conforme o art 6° 9 aduz: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Considera-se também neste caso o princípio da extraterritorialiedade, que se trata da aplicação da lei penal brasileira àqueles que executarem crimes fora dos limites territóriais do Brasil. As variantes de extraterritorialidade são apresentadas no inciso I, alínea b, art 7° do Código Penal que diz:

> Art 7º – Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
> I – os crimes:
> a) [...}
> b) contra patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; (BITENCOURT, 2004, op-cit, p.20).

5.2 EXEMPLOS DE CRIMES DIGITAIS

A *Internet* proporcionou uma quantidade absurda de informações para todo tipo de pessoa que demonstre interesse em procurar sobre um determinado tema, da mesma forma abriu caminho para numerosos tipos de crimes efetuados por meio dessa gigantesca ferramenta de informação cujo acesso é disponível para todos.

Entre os principais delitos cometidos constam, por exemplo: a exibição de sites contendo pornografia infantil, que pode ser enquadrada no art 241 do Estatuto da Criança e do Adolescente – pedofilia; além desse, o plágio de textos de terceiros que se enquadra no art 184 do Código Penal – violação de direito de autor. Também são delitos comuns: falsa identidade, crime contra a segurança nacional, preconceito ou discriminação de raça/cor/etnia, lavagem de dinheiro, apropriação indevida, calúnia, estelionato, difamação, divulgação de segredo, injúria, incitação ao crime, adulteração de dados em sistemas de informações, ameaça, violação do direito autoral, furto, favorecimento da prostituição, dano, apologia ao crime ou criminoso, escrito ou objeto obsceno, crime contra a propriedade industrial, escárnio por motivo de religião, falso

testemunho, ato obsceno, jogo de azar, exercício arbitrário das próprias razões, interceptação de comunicações de informática, pirataria de software e inserção de dados falsos em sistemas de informações.

Os comportamentos que prejudicam o direito relativo a bens ou informações informáticas não recebem nenhuma forma de punição dentro de nossa legislação, essas condutas são denominadas crimes digitais, também podendo ser descritos como crimes informáticos, crimes da *Internet*, crimes cibernéticos, ou *cybercrimes*. Para esta modalidade de crimes, não se faz necessário uma nova legislação específica, uma vez que já estão sob o domínio da legislação atual, salvo que necessitem de atualizações da lei para se adaptar aos novos processos da *Internet.*

Existe uma diferença entre crimes de informática e crimes cibernéticos, segundo Quintiliano (2007) os crimes de informática são práticas nativas, antijurídicas e passíveis de culpa executadas a partir do uso de computadores e/ou de outros dispositivos semelhantes. Já crimes cibernéticos são aqueles cometidos utilizando a Internet, ou seja, o crime cibernético é espécie do crime de informática, uma vez que se utiliza de computadores para acessar a *Internet*.

5.2.1 Crimes Frequentes no Facebook

Em 2016, Mark Zuckerberg, CEO do *Facebook,* comemorou a marca de 1,8 bilhão de usuários em atividade, ou seja, aproximadamente ¼ da população mundial utiliza regularmente o *Facebook*. No Brasil, também em 2016, a rede social já registrava 102 milhões de brasileiros mensalmente ativos, o que representa mais de 50% da população do país.

O *Facebook* disponibiliza diversas ferramentas em seu ambiente, sendo possível a criação de páginas pessoais e profissionais, divulgação de marketing, vídeos ao vivo, criação de grupos temáticos e também a comunicação entre os usuários em tempo real.

Decorrente ao crescimento de usuários do *Facebook* é o aumento de infrações penais ocorridas neste ambiente. A prática de crimes, cada vez mais

corriqueira, sobrevém contra a honra, ameaças, pornografia infantil, estelionato, falsidades em geral, comércio de drogas e armas entre outros.

O comércio de drogas e armas acontece na Internet, muitas vezes, restringem-se a *Dark Web* (“Internet Obscura”), a qual somente pode ser acessada com configurações e softwares especiais. Este setor da Internet, por ser anônimo e com uma criptografia que dificulta o rastreio dos usuários, é bastante utilizada por criminosos para o comércio de drogas, armas, compartilhamento de pornografia infantil e pirataria de softwares e mídias.

Outro delito comum na Internet – e não menos grave –, que também passou a ocorrer no *Facebook*, é a pornografia infantil, tipificado no art. 241-A, do Estatuto da Criança e do Adolescente. De acordo com a lei, a condenação criminal do agente infrator, por clara ofensa aos direitos da adolescente a exposição vexatória, principalmente quando envolve nudez ou cenas sexuais, aduz:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente; (Artigo 241A da Lei nº 8.069 de 13 de Julho de 1990); Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008).

Notoriamente, toda a agressão a crianças e adolescentes deve ser combatida na forma da lei. Se um adulto toma conhecimento de imagens envolvendo menores, é seu dever comunicar as autoridades competentes, e não dar ainda mais publicidade a elas, através de novos compartilhamentos. A rede social, igualmente, deve fazer uma fiscalização constante dos conteúdos postados, especialmente quando há denúncias contra os mesmos e, assim que identificá-los, deve removê-los sob pena de transformar-se em responsável pelo ilícito, perante sua negligência.

Os crimes praticados na esfera do *Facebook* também impetraram o campo eleitoral, principalmente após a polarização das últimas eleições e o consequente acirramento de ânimos, o que ocasionou diversas denúncias de crimes contra a honra. Para tais delitos há um recurso criminal que consta na ementa do Código Eleitoral nos Art. 325 e 326, sendo a pena privativa de

liberdade substituída por uma restritiva de direitos, consistente no pagamento de 10 salários mínimos à vítima pela Difamação Eleitoral ou por Injúria Eleitoral.

> Art. 325. Difamar alguém, na propaganda eleitoral, ou visando a fins de propaganda, imputando-lhe fato ofensivo à sua reputação: Pena - detenção de três meses a um ano, e pagamento de 5 a 30 dias-multa.
> Parágrafo único. A exceção da verdade somente se admite se ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.
> Art. 326. Injuriar alguém, na propaganda eleitoral, ou visando a fins de propaganda, ofendendo-lhe a dignidade ou o decoro: Pena - detenção até seis meses, ou pagamento de 30 a 60 dias-multa. (Lei nº 4.737 de 26 de Dezembro de 1996)

Ofensas proferidas em pleno período de campanha e por intermédio de redes sociais assumem conotação de delitos eleitorais, uma vez que praticadas em cerne de propaganda eleitoral, o que atrai a competência da Justiça Especializada. A restrição do *Facebook* é relativa, pois existem maneiras de se configurar um perfil nele inserido como “público”, justo que, qualquer usuário da rede social possa ter acesso às informações. Logo, configura-se um meio de comunicação de massa.

Os crimes de falsidade e contra o patrimônio estão também nas redes sociais. Algumas condutas no *Facebook* podem configurar falsidade ideológica, estelionato e extorsão. No Brasil não há legislação específica para tal delito. Observando a legislação penal, pode-se constatar que o furto mediante fraude está descrito no inciso II do §2º do art.155 do Código Penal. O agente engana a vítima, visando reduzir seu cuidado sobre o item, o qual é tomado. Pode-se notar que o agente apenas aplica o “golpe patrimonial imperceptível” que é empregado sobre determinado item da vítima. Contudo, o inciso não precede a danos realizados no âmbito virtual. O legislador pátrio, recentemente, atualizou o capítulo do Código Penal referente aos crimes de falsidade, a fim de equiparar os cartões de débito e crédito a documento particular, permitindo a punição a quem realiza clonagem de cartões magnéticos.

Outro delito comum está na criação de perfis falsos na Internet. Dependendo do animus do agente e dos desdobramentos de suas ações, resultam em punição por falsidade ideológica, pois aquele que constrói um perfil inverídico está inserindo informações falsas (nome, idade, localização, etc.) e, se em razão desta conduta houver prejuízo de direitos, criação de obrigações ou

alteração da verdade sobre fato juridicamente relevante, o agente será punido com até três anos de prisão e multa, nos termos do art. 299, do Código Penal.

> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante: Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa.(CP - Decreto Lei nº 2.848 de 07 de Dezembro de 1940).

5.2.2 Sensibilidade ao Tempo de Uso

As informações publicadas em redes sociais podem ser apagadas pelo usuário a qualquer momento. É possível recuperá-las através de ferramentas específicas para tal, no entanto as chances são reduzidas a medida em que o tempo passa e os arquivos alocados vão se perdendo.

5.2.3 Possibilidade do Inverídico

Informações publicadas podem ser manipuladas, como na criação de um perfil falso para fins ilegais, a fim de alguém se passar por quem que não é. Um pedófilo, por exemplo, pode criar um perfil falso no Facebook se passando por uma criança, ou um indivíduo pode fazer *check-in* em um determinado país estando em outro diferente, ou seja, é possível manipular essa informação, e isso vai da criatividade ou do objetivo de se dizer onde se está, seja no país de origem, ou fora dele, isto é, em qualquer lugar.

Sendo assim, é possível que o investigador obtenha informações a partir de um perfil criado no Facebook as quais não correspondam a real identidade de quem criou e usa tal página. Felizmente, é possível se obter outras informações relevantes tais como endereço IP de um titular de conta usada durante a sua criação original ou os endereços IP do titular da conta usada efetuar o acesso.

6. METODOLOGIA E APLICAÇÃO DAS FERRAMENTAS FORENSE

Neste trabalho será apresentado a descrição e aplicação de algumas ferramentas forense para a aquisição, preservação, análise e apresentação de evidências especificamente direcionada a rede social Facebook.

Os meios de pesquisa utilizados para a redação deste trabalho podem ser encontrados em livros desta mesma área, documentos existentes como artigos, monografias, dissertações e teses onde se fez presente o tema do forense computacional.

Os ambientes em que os testes foram realizados, as ferramentas escolhidas e a aplicação das mesmas serão descritas nos capítulos seguintes.

6.1 RECURSOS UTILIZADOS

Para a execução dos testes propostos neste trabalho, foram utilizados dois computadores com ambiente Windows, um smartphone Android e seis ferramentas forense diferentes. Todos os ambientes se encontram em plenas condições, em seu modo padrão de uso e acesso.

Foram também instalados todos os softwares auxiliares necessários para o funcionamento das ferramentas forense.

6.1.1 Equipamento

Tabela 1 - Especificações Equipamento

Computador	Desktop
Memória	2 GB
Processador	Intel Core2Duo
Disco	500 GB
Sistema Operacional	Windows 7 Ultimate
Notebook	Acer Aspire A515
Memória	8 GB
Processador	AMD A12
Disco	1 TB
Sistema Operacional	Windows 10 Home
Smartphone	Samsung Galaxy S8
Memória	4 GB
Processador	Exynos 8895
Disco	64 GB
Sistema Operacional	Android 9.0

6.1.2 Softwares Utilizados

Na tabela abaixo temos a descrição das ferramentas utilizadas e suas versões.

Tabela 2 - Versões Software

Software	Versão	Contrato
FTK Imager	4.2.0.13	Free
Autopsy	4.11.0	Trial
Belkasoft Evidence Center	9.5.3532	Trial
Facebook JPG Finder	v1.2	Free
Internet Evidence Finder	v6.26.0.16919	Trial
Andriller	3.1.0	Free

Para a instalação dos softwares no ambiente Windows 7 se fez necessário o download de alguns outros programas auxiliares, como o *.NET Framework 4.5*. Os demais programas auxiliares necessários já se encontravam embutidos no instalador do software principal e suas instalações foram todas realizadas.

No caso do *Adriller*, foi necessário também algumas configurações diretamente no smartphone. São elas:

- Ativar modo desenvolvedor
- Ativar depuração USB
- Autorizar RSA Fingerprint

6.2 LOCALIZAÇÃO DE EVIDÊNCIAS

6.2.1 Identificação de um Perfil

A identificação de um usuário no Facebook pode acontecer de duas maneiras: a primeira representada numericamente por quinze dígitos após o ID (https://www.facebook.com/profile.php?id=números) ou simplesmente (https://www.facebook.com/números). Esta identificação é única e não pode ser alterada, ou seja, mesmo que o indivíduo mude seu nome de perfil, o ID continuará o mesmo.

Na primeira, a visualização do ID é possível de ser verificado quando se posiciona o cursor do mouse em cima da foto de perfil ou da capa. O último bloco de números representa o ID, conforme é mostrado na Figura 06. Sendo que ainda é possível descobrir o ID de um usuário através de sites que oferecem serviço para tal como o *Find My Facebook ID* (http://findmyfacebookid.com).

Figura 6 - Identificação Facebook ID

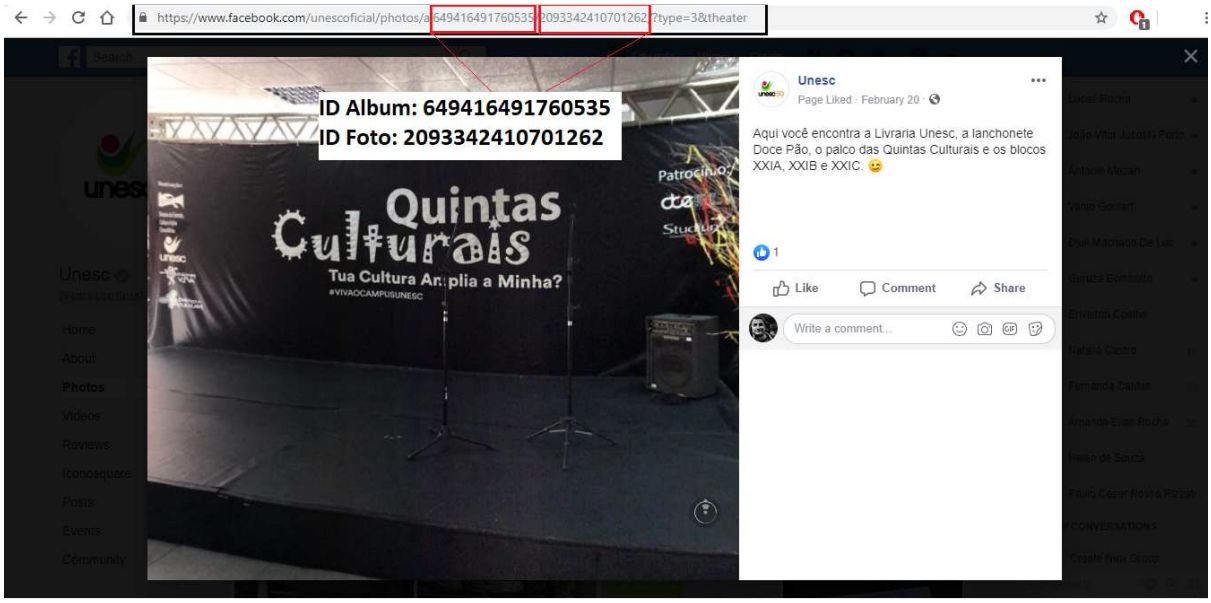
Fonte: *Print Screen* criado pelo autor da página da universidade no Facebook.

A segunda forma é a mais amigável e de fácil visualização, onde a identificação se dá através do nome do próprio usuário após o endereço do site no navegador (https://www.facebook.com/nomedousuario), sendo permitido alterar este nome apenas uma vez para a inclusão do nome real. Importante destacar que as duas maneiras correspondem à identificação do usuário. Entretanto, a segunda é a mais utilizada devido sua facilidade de percepção, afinal basta estar no perfil do usuário para visualizá-la.

6.2.2 Identificação de Fotos

As fotos que são publicadas carregam consigo uma identificação numérica (ID) após o “fbid” (https://www.facebook.com/photo.php?fbid= números) e que fica visível ao se passar o mouse por cima de uma foto, ou ao expandi-la, como mostrado na Figura 07.

Figura 7 - Identificação de Fotos



Fonte: *Print Screen* criado pelo autor da página da universidade no Facebook.

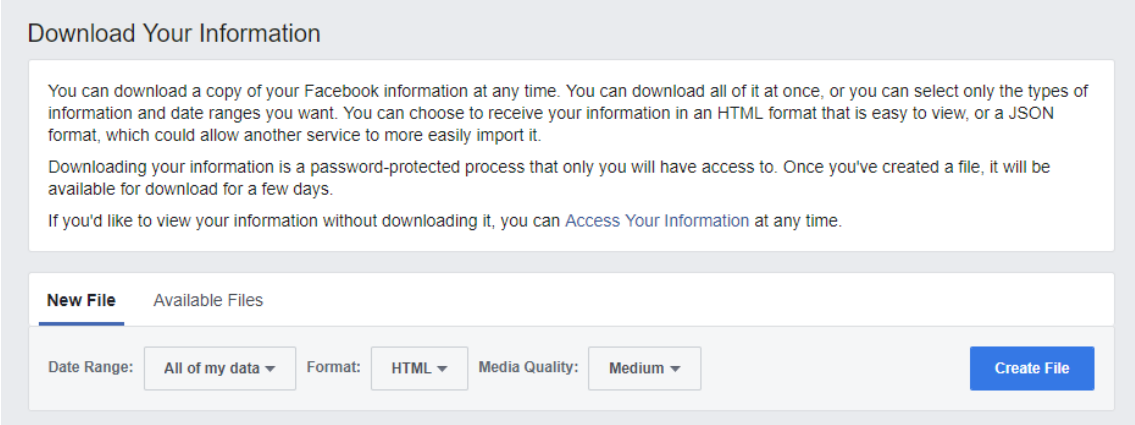
Esta identificação possibilita saber de qual usuário do Facebook a imagem teve origem, tornando possível extrair esta informação através do download de uma foto do Facebook, na ocasião em que a mesma é salva, por padrão, com um nome que apresenta uma numeração específica para cada foto, a qual é composta por 3 blocos de números como, por exemplo, “60441844_2093342410701262_3818474858153508864_n”, onde o segundo bloco (“2093342410701262” neste caso) indica o ID da imagem. Quando este ID é recolocado na barra de endereços do navegador, é possível visualizar sua origem (para o exemplo em questão, dessa forma: https://www.facebook.com/2093342410701262).

6.3 AQUISIÇÃO DOS DADOS

Conforme descrito nos itens anteriores, quando o perito possui acesso às informações da conta do investigado no Facebook é possível navegar por entre as funcionalidades da rede social em busca de evidências. Ou seja, analisar diretamente na página da Internet as publicações enviadas, fotos postadas e mensagens trocadas pelo investigado. Entretanto, este processo além de possuir um certo grau de amadorismo é também bastante moroso.

A partir de 2010 o Facebook passou a fornecer uma opção bastante interessante para seus usuários e, consequentemente, aos investigadores forense. Na sessão de opções, em ‘Configurações’, é possível solicitar uma cópia de todos os seus dados, postagens, mensagens, curtidas, pedidos de amizade, grupos, histórico de pesquisa e locais desde o dia em que sua conta foi criada até o presente momento. O pedido é avaliado pela administração da rede social e o tempo de resposta pode variar de usuário para usuário, compreendendo-se entre horas ou até mesmo dias. É possível escolher o período de coleta dos dados, a qualidade das informações e também o formato do arquivo de saída, podendo ele ser HTML ou JSON.

Figura 8 - Solicitação Arquivo de Informações



Fonte: *Print Screen* criado pelo autor.

No entanto, na grande maioria dos casos os investigadores não possuem as credenciais de acesso ao perfil do investigado, ficando impossibilitados de solicitar o arquivo de atividades. Os dados, então, devem ser adquiridos das outras fontes possíveis como o histórico de navegação do browser, arquivos temporários de Internet, arquivos de cache do navegador e até mesmo em informações guardadas em memória volátil. Para este tipo de extração, os peritos são auxiliados por softwares de análise forense desenvolvidos para buscar as informações nestes locais.

6.4 FERRAMENTAS DE EXTRAÇÃO E ANÁLISE

6.4.1 Gerando o HASH

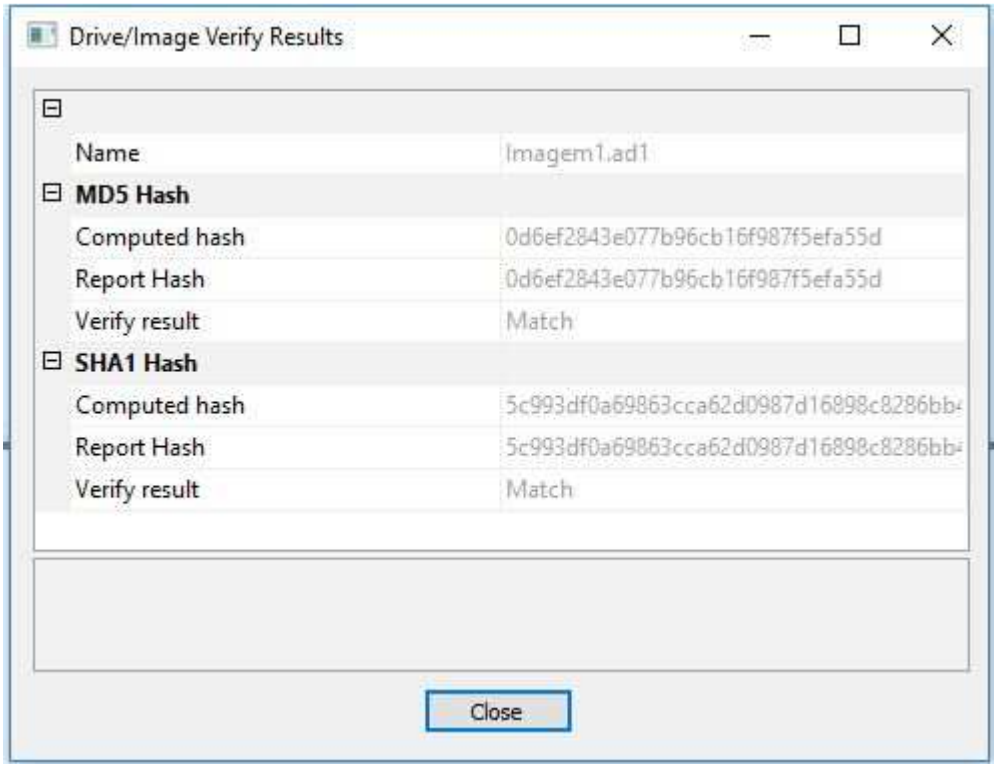
Em toda perícia forense é de extrema importância garantir que o conteúdo do material não sofra qualquer modificação e nem trocado até que se conclua o inquérito e, dessa forma, o processo se finalize.

Sendo assim, surge a necessidade do emprego de métodos que permitam a averiguação da integridade e da legitimidade das informações. O principal destes métodos é o cálculo feito a partir de funções de autenticação unidirecionais definidas como *hash*. Tais funções, utilizando uma entrada de qualquer tamanho, produzem uma saída de tamanho fixo, isto é, convertem uma grande quantidade de dados em uma pequena sequência de bits.

Esta função é a mais utilizada para a verificação de integridade de dados computacionais em virtude de que uma simples modificação na informação de entrada do algoritmo produzirá um valor *hash* (sequência de bits) totalmente diferente. Ou seja, caso o teor de um arquivo seja processado por uma função unidirecional e em seguida ter o seu conteúdo modificado em um apenas um bit, ao ser rodada novamente a função, serão alcançadas como resultado duas sequências de bits totalmente distintas. Uma outra vantagem adquirida com o uso das funções unidirecionais é que não é possível executar o processo inverso, isto é, não é possível retroceder à informação inicial a partir de um valor *hash*. Isso faz com que estas funções sejam de frequentemente utilizadas em algoritmos de criptografia.

Para a geração da imagem dos dados extraídos do perfil do facebook, foi utilizada a ferramenta da AccessData, o FTK ® Imager. Na figura abaixo podes observar o valor *hash* obtido.

Figura 9 - Valor HASH Obtido



Fonte: *Print Screen* criado pelo autor.

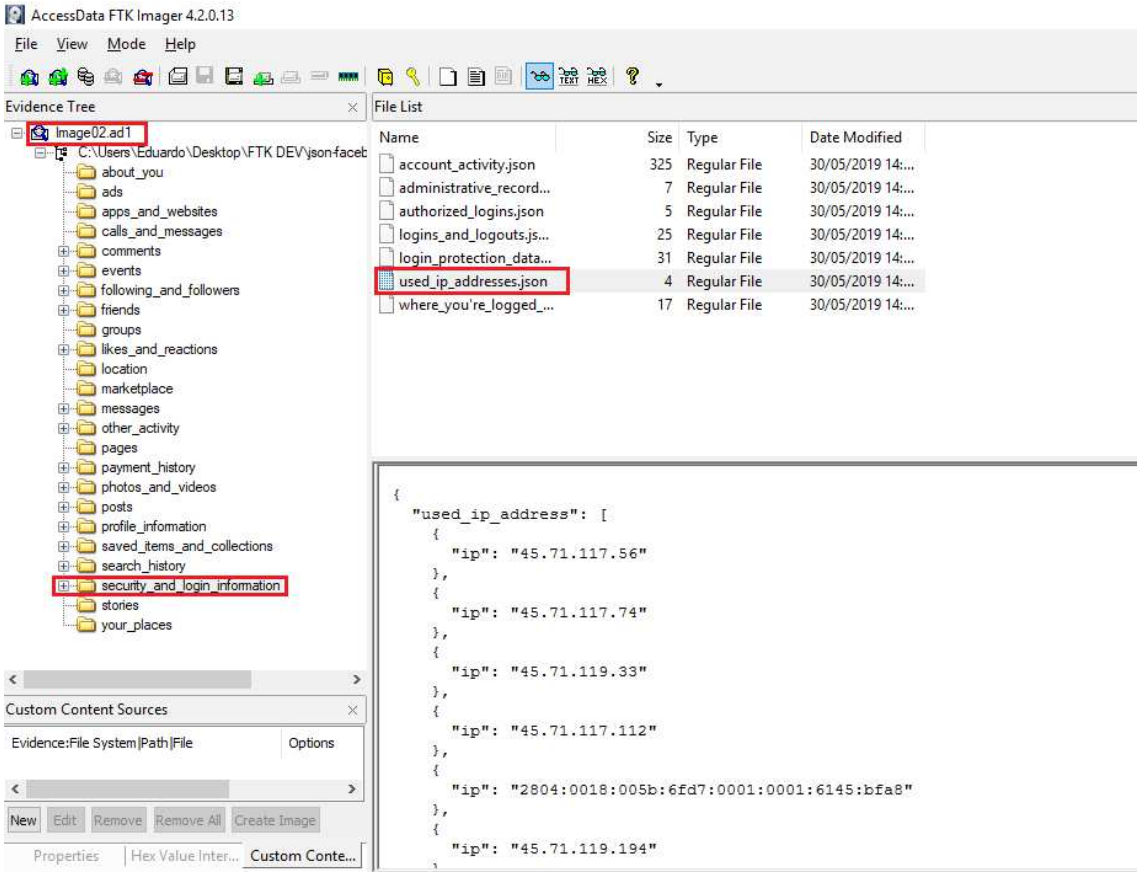
6.4.2 FTK ® Imager

Desenvolvido pela empresa norte americana AccessData, o FTK® Imager se trata de uma ferramenta para montagem de imagens de forma que possam ter suas informações apenas lidas, sem permitir qualquer tipo de alteração. Além da criação das imagens, sejam elas de discos rígidos, CDs ou dispositivos USB, o FTK Imager também oferece recursos de visualização de dados. Isso pode ser usado para visualizar os arquivos e pastas e os conteúdos que residem nesses arquivos. O FTK Imager também suporta a montagem de imagens, o que aumenta sua portabilidade. A ferramenta é uma das poucas que podem criar vários formatos de arquivo: EO1, SMART ou DD raw. Também é possível acompanhar facilmente as atividades por meio de um arquivo de log de texto básico.

Ao criar cópias de unidades de disco originais, um aspecto crítico é verificar a integridade dos arquivos. O FTK Imager também auxilia nesta área, com suporte para a criação de *hashes* MD5 e SHA1, conforme mostrado anteriormente. Além disso, pode-se gerar relatórios de *hash* que podem ser arquivados para uso posterior. Por exemplo, se você quiser verificar se uma imagem foi alterada desde a sua aquisição. A versão do aplicativo utilizada no teste foi a 4.2.

Na figura a seguir temos um exemplo da visualização da imagem gerada do arquivo solicitado ao Facebook, contendo todas as informações do perfil. Na sessão de Segurança e Informações de *Login*, pode-se observar todos os endereços de Internet (IP) já utilizados pelo usuário. Durante os nove anos desde a criação da conta, foram utilizados mais de oitenta endereços diferentes.

Figura 10 - Visualização no FTK Imager



Fonte: Print Screen criado pelo autor.

6.4.3 Autopsy

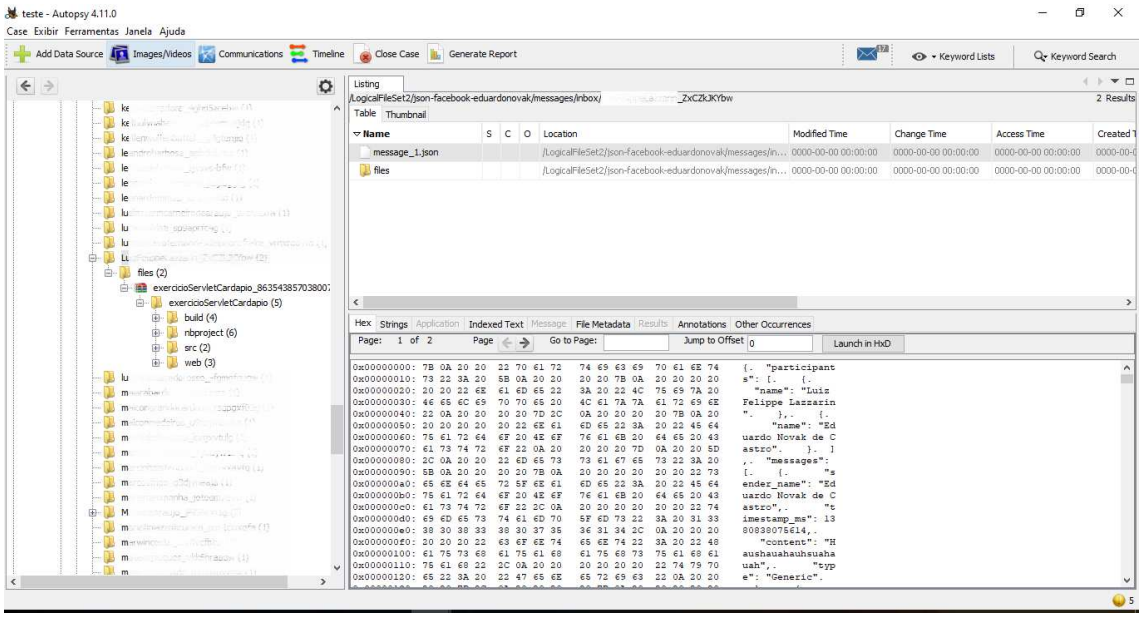
O *Autopsy* é a interface gráfica para usuário (*Graphic User Interface* - ou GUI) usada no *The Sleuth Kit*, uma biblioteca de ferramentas de linha de comando que permitem investigar imagens de disco.

O software possui código aberto e vem pronto para funcionar em qualquer plataforma Windows ou Mac (Apple). A abordagem *Open Source* (código fonte aberto) permite ao usuário verificar todos os aspectos da captura, processamento e análise de dados, fornecendo transparência e essencialmente colocando o controle totalmente nas mãos do utilizador. Nesse sentido, o software é educacional e informativo.

Um ótimo recurso é a capacidade da *Autopsy* de produzir resultados em tempo real, transmitindo resultados de palavras-chave à medida que aparecem nos dados pesquisados. Um rápido clique com o botão direito abre um arquivo relevante. Isso significa pouco ou nenhum tempo de espera para descobrir se há termos específicos de pesquisa no disco, no telefone ou no computador que está sendo pesquisado.

Na figura 11 podemos observar o arquivo recebido do Facebook sendo processado pelo *Autopsy*, em sua versão 4.11.0.

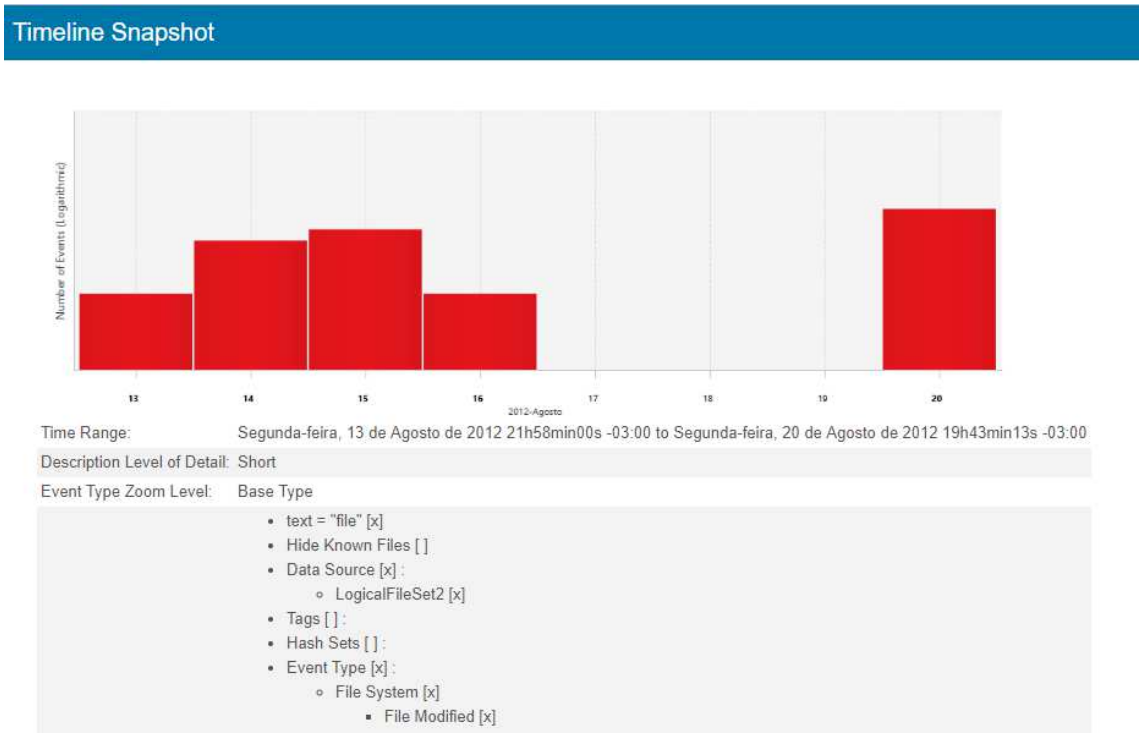
Figura 11 - Arquivo Aberto no Autopsy



Fonte: Print Screen criado pelo autor.

A imagem mostra a navegação entre as subpastas até uma conversa onde ocorreu um compartilhamento de arquivos, pesquisado através da palavra chave “*file*”. A ferramenta para a perícia conseguiu resgatar na íntegra o conteúdo do arquivo, bem como gerou um relatório com a linha do tempo do compartilhamento deste na conversa. O relatório apresenta as palavras chave procuradas, o registro de data e hora e a descrição dos filtros utilizados.

Figura 12 - Relatório Autopsy



Fonte: Print Screen criado pelo autor.

6.4.4 Belkasoft Evidence Center

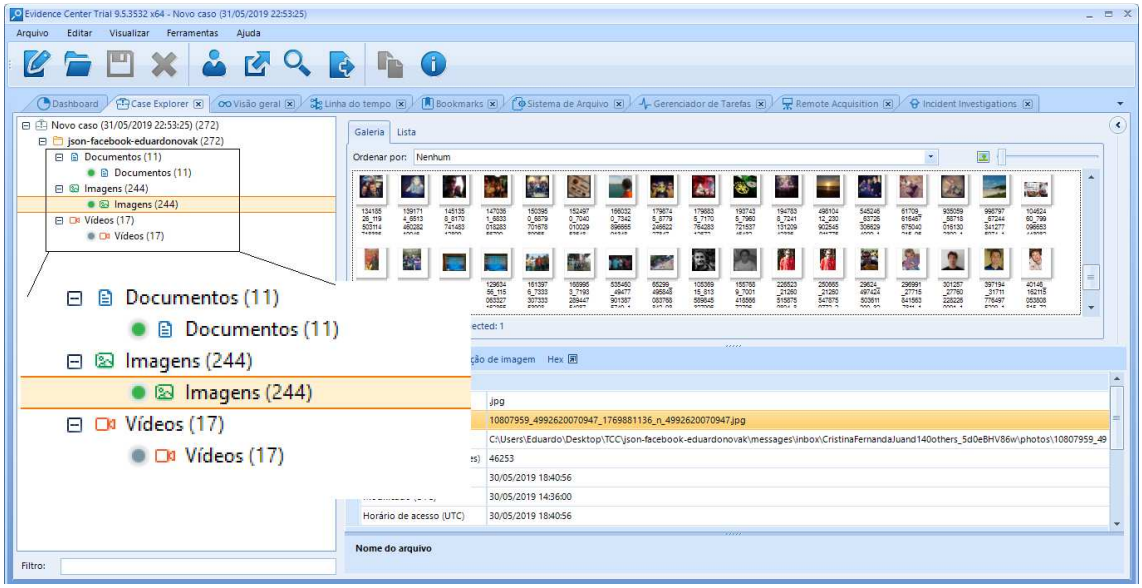
Fundada em 2002, a Belkasoft é líder global em tecnologia forense digital, conhecida por suas ferramentas sólidas e abrangentes. Com uma equipe de profissionais em análise forense digital, recuperação de dados e engenharia reversa, a Belkasoft se concentra na criação de produtos tecnologicamente avançados, com fácil usabilidade, para investigadores e especialistas forenses, tornando seu trabalho mais fácil, rápido e eficaz.

O Belkasoft Evidence Center, seu principal produto, trata-se de uma solução integrada para coleta e análise de evidências digitais de dispositivos móveis e de computadores. Clientes em agências policiais, militares, comerciais, agências de inteligência e laboratórios forenses em mais de 130 países usam produtos Belkasoft para combater homicídios, crimes contra crianças, tráfico de drogas, vazamento de dados, fraude e outros crimes on-line e off-line.

A versão utilizada nos testes foi a 9.5.3, de demonstração. Obtida após o preenchimento de um cadastro de solicitação no site da fabricante. Após esse procedimento, é enviado o link para download juntamente com uma chave para registro.

Apesar da robustez da ferramenta, os testes encontraram poucas evidências ligadas exclusivamente a rede social Facebook. Foram retornados apenas os arquivos de fotos e vídeos postados na linha do tempo, além dos documentos compartilhados com outros usuários, conforme evidencia a figura 13 abaixo.

Figura 13 - Belkasoft Análise Arquivo Facebook

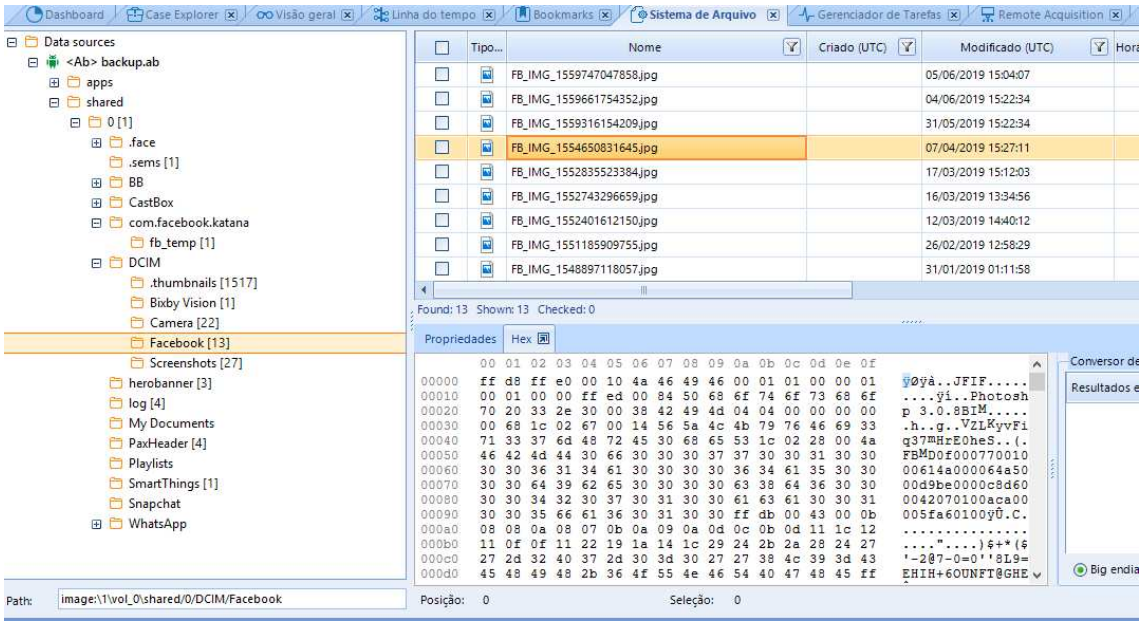


Fonte: Print Screen criado pelo autor.

A análise em dispositivo móvel, por sua vez, se mostrou muito mais frutífera no que tange o número de resultados retornados. No entanto, quanto aos dados com origem restrita ao Facebook, o Belkasoft Evidence Center

retornou apenas a imagens que foram baixadas da rede social para o aparelho móvel, conforme figura 14. A coleta foi feita a partir do aparelho Samsung Galaxy S8, que opera com o sistema operacional é o Android versão 9.

Figura 14 - Belkasoft Análise Dispositivo Móvel



Fonte: Print Screen criado pelo autor.

6.4.5 Facebook JPG Finder

O Facebook JPG Finder, ou FJF, é uma ferramenta desenvolvida pela empresa canadense JADSoftware no final da década de 2000. Escrito na linguagem de programação Visual Basic exclusivamente para ambiente Microsoft Windows, o sistema foi projetado visando a otimização do tempo de extração das informações, o que o torna apto a funcionar com excelente performance até nas máquinas de configuração mais defasadas.

O funcionamento se dá através de uma que pesquisa uma pasta selecionada, e consequentemente suas subpastas, por possíveis imagens JPG oriundas do Facebook. Essas imagens são identificadas executando vários filtros no nome do arquivo. Conforme visto anteriormente, o nome do arquivo contém o ID do usuário/perfil na rede social e, portanto, pode indicar de qual usuário do Facebook a foto veio. Um arquivo de relatório HTML é criado na pasta de saída selecionada pelo examinador contendo o nome do arquivo, os horários de

criação, modificação e último acesso. Também é gerado um link para o possível perfil do Facebook, um *hash* MD5 da imagem e a própria imagem. Todas as imagens localizadas também são copiadas para a pasta de saída, configurada na tela inicial ao iniciar o programa. A versão utilizada nos testes foi a 1.2.

Figura 15 - Facebook JPG Finder

Fonte: Print Screen criado pelo autor.

O projeto do Facebook JPG Finder foi descontinuado no início da década de 2010, dando lugar a outro projeto muito mais abrangente e complexo que será explicado no próximo item.

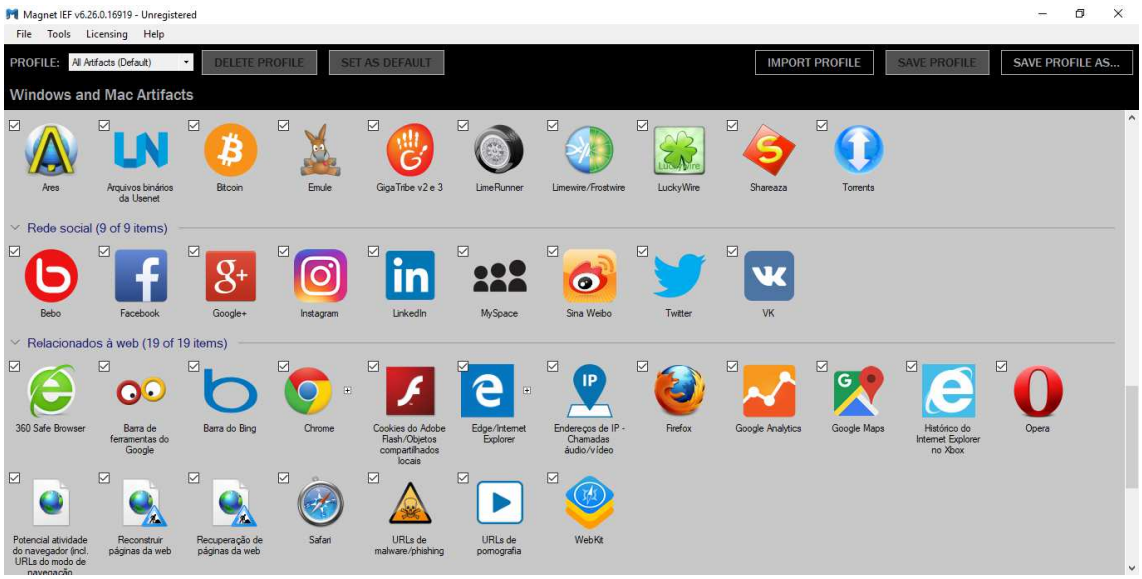
6.4.6 Internet Evidence Finder

A *Magnet Forensics* é responsável pelo desenvolvimento de sistemas forenses completos, de fácil usabilidade e que possibilitam aos analistas acessar de forma rápida as evidências produzidas pelo uso da *Internet*. O *Internet Evidence Finder* (IEF), desenvolvido por um policial aposentado e carro chefe da empresa, surgiu da unificação dos produtos da JADSoftware, sua antiga empresa. Atualmente é referência em investigação para milhares de agências de polícia, governos e corporações em mais de 90 países do mundo.

Trata-se de uma ferramenta para forense computacional utilizada por inúmeros investigadores a fim de encontrar artefatos de *Internet* e avaliar evidências digitais armazenadas em computadores, smartphones e tablets. O software é capaz de recuperar evidências de mais de 265 tipos de artefatos de Internet em sistemas operacionais Windows e Mac. As buscas tem seus resultados apresentados no IEF *Report Viewer* – que permite aos analistas identificar as evidências relevantes – e são exportados em vários formatos de relatórios, de fácil compreensão.

O IEF permite a seleção de diversos tipos de plataformas para a busca de evidências, conforme a figura 15 abaixo. Ele possui em seu acervo não só aplicativos correspondentes a redes sociais, encontra-se também gerenciadores de e-mail, mensageiros instantâneos (como whatsapp), compartilhadores de arquivos e todos os tipos de navegadores conhecidos. Para os testes foi marcado somente a opção que representa o Facebook.

Figura 16 - IEF Aplicativos Disponíveis

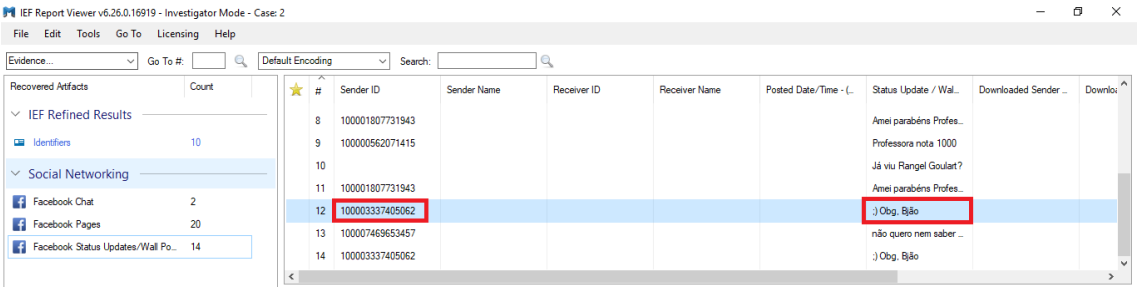


Fonte: Print Screen criado pelo autor.

O primeiro teste foi realizado em um computador pessoal. A busca foi feita em todo o disco da máquina, atrás dos arquivos de Internet que apresentariam qualquer ligação com a rede social em questão. O IEF conseguiu encontrar informações referentes a conversas, alterações de status e publicações no

mural. A parte de pré-visualização permite que se verifique o ID do usuário e o conteúdo da postagem.

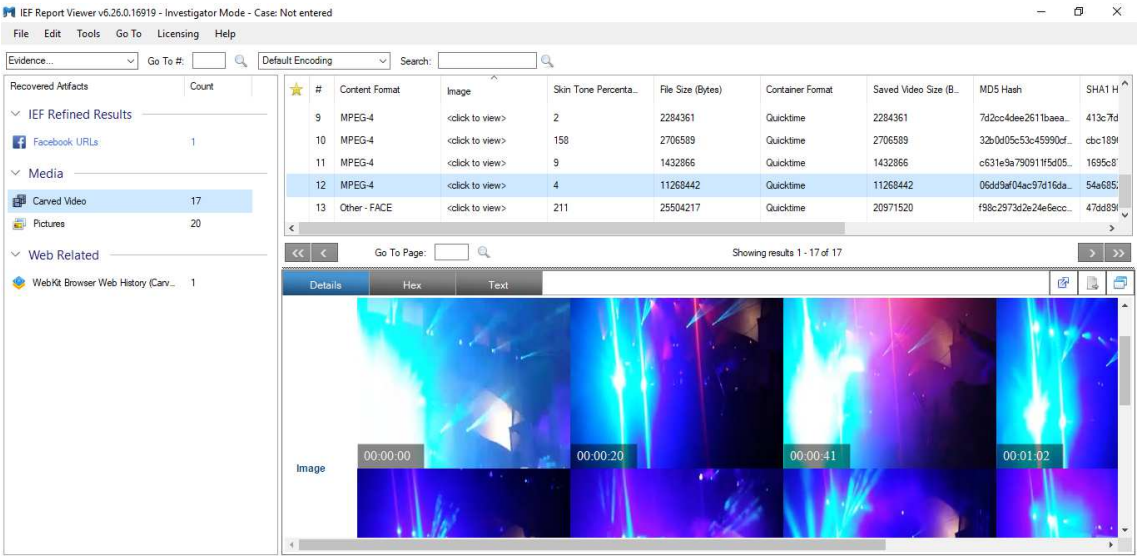
Figura 17 - IEF Dados Recuperados Disco



Fonte: Print Screen criado pelo autor.

No segundo teste a ferramenta foi utilizada para executar a pesquisa sobre o arquivo de informações solicitado ao Facebook. Como retorno foi obtido um endereço de perfil, mídias de vídeo e imagens. Conforme a figura 17, são apresentadas imagens miniaturas a cada vinte segundos da reprodução do vídeo, facilitando percepção do examinador e otimizando o tempo de pesquisa.

Figura 18 - IEF Dados Recuperados Arquivo



Fonte: Print Screen criado pelo autor.

6.4.7 Andriller

Esta ferramenta se trata de um software utilitário com uma coleção de ferramentas forenses para smartphones. Ela realiza aquisição não-destrutiva,

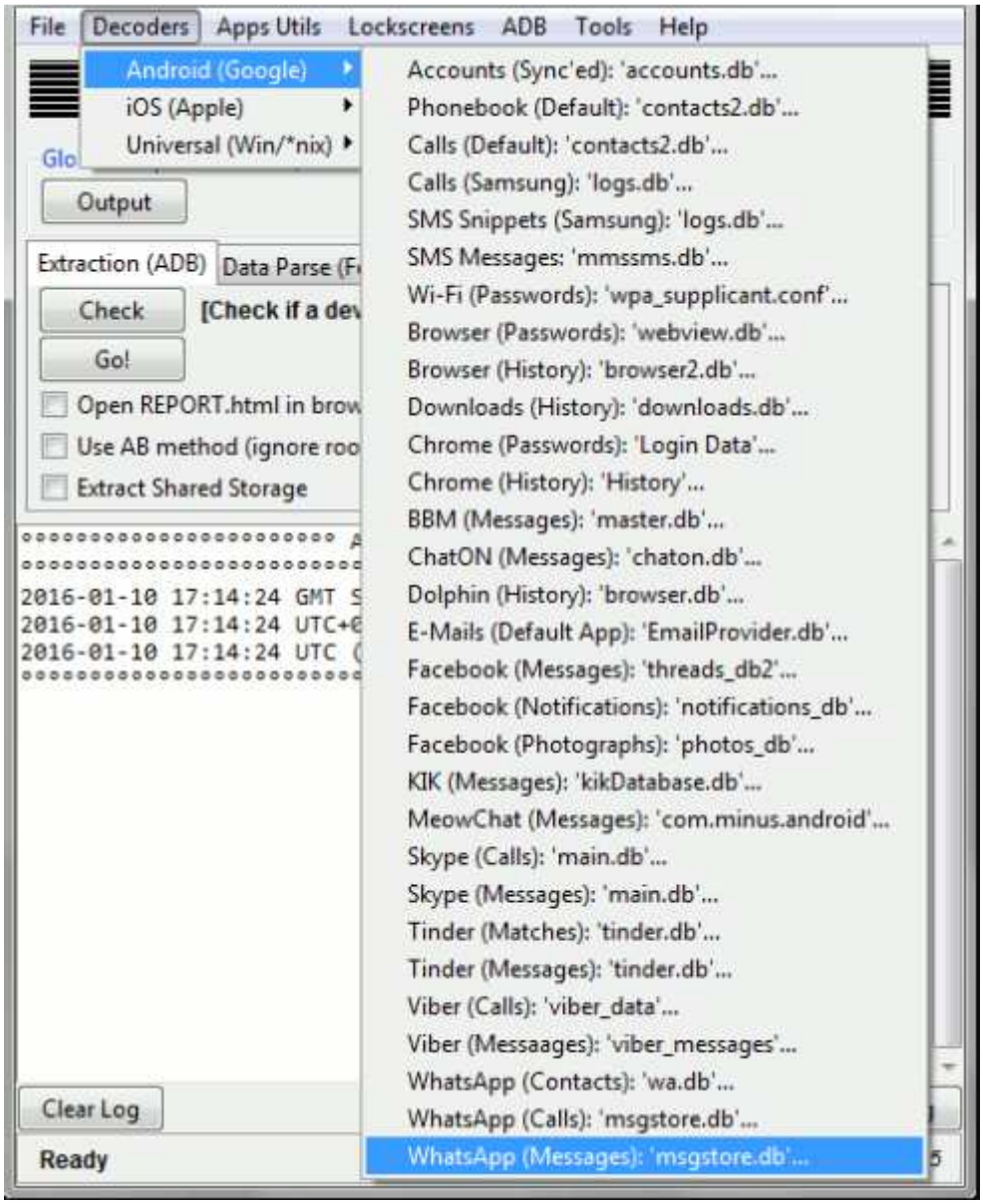
somente leitura e forense de dispositivos Android. Ele tem recursos, como poderoso sistema para quebra de bloqueio de tela, código PIN ou senha; decodificadores personalizados para dados do Google Apps a partir de bancos de dados Android (alguns do Apple iOS e Windows) para comunicação codificada. Extração e decodificadores produzem relatórios em formatos HTML e Excel.

Primeiro, deve-se selecionar o diretório onde se pretende salvar os dados de extração. Após isso, utilizar o botão para verificar se a ferramenta encontrou o seu dispositivo móvel conectado. Finalmente, após definição do local de saída para o relatório, é iniciada a varredura. O *Andriller* executa a busca, o download e a decodificação tudo de uma só vez.

Após a conclusão da extração de dados, todos os dados são salvos na pasta no diretório especificado antes da extração. O principal arquivo de índice de extração é “REPORT.html”. Nele estará contido o resumo do dispositivo examinado e uma lista com todos os dados extraídos. Um excel “REPORT.xlsx” também é produzido simultaneamente, o qual contém todos os dados em um arquivo.

Foram utilizados os decodificadores específicos para Facebook (ver figura 18). A análise retornou os arquivos de imagens e vídeos que foram baixados do Facebook.

Figura 19 - Decodificadores Andriller



Fonte: Print Screen criado pelo autor.

7. ANÁLISE COMPARATIVA DOS RESULTADOS

Neste capítulo serão analisados os resultados obtidos com os testes realizados com as ferramentas forense. No primeiro momento será analisado a capacidade de cada software em resgatar as informações referentes ao Facebook por categoria. Posteriormente as ferramentas serão confrontadas quanto ao tempo de execução que apresentaram.

7.1 ARQUIVO FACEBOOK

A tabela a seguir apresenta quais categorias de dados da rede social foram apresentadas ao fim da execução dos testes. As ferramentas *Belkasoft Evidence Finder*, *Facebook JPG Finder* e *Internet Evidence Finder* tiveram seus nomes abreviados para BEF, FJF e IEF respectivamente.

Tabela 3 - Arquivo Facebook

Arquivo Facebook	FTK Imager	Autopsy	BEF	FJF	IEF
Eventos Linha do Tempo	✓	✓	✓	✗	✓
Conversas	✓	✓	✓	✗	✗
Mídia	✓	✓	✓	✗	✓
Reações	✓	✓	✓	✗	✗
Documentos	✓	✓	✓	✗	✓

Fonte: Elaborado pelo autor.

A primeira análise foi feita sobre a performance das ferramentas sobre o arquivo enviado pelo Facebook, contendo todas as atividades do usuário desde a criação da conta.

Os aplicativos capazes de ler arquivos de imagem de disco não tiveram problemas e apresentaram todas as informações fornecidas pelo Facebook. Este também não possui controle das fotos que os usuários fazem download, por este motivo o FJF não mostrou qualquer resultado.

Por sua vez, o IEF se mostrou capaz de catalogar vídeos e fotos enviados e identificar o perfil cujos dados pertencem.

7.2 DISCO LOCAL

Os resultados das análises feitas diretamente no disco se encontram na tabela a seguir:

Tabela 4 - Análise Disco PC

Disco PC	FTK Imager	Autopsy	BEF	FJF	IEF
Eventos Linha do Tempo	✗	✗	✗	✗	✓
Conversas	✗	✓	✗	✗	✓
Mídia	✗	✓	✓	✓	✗
Reações	✗	✗	✗	✗	✓
Documentos	✗	✓	✓	✗	✗

Fonte: Elaborado pelo autor.

Tratando-se unicamente de um gerador e leitor de imagens de disco, o FTK não foi capaz de encontrar algum resultado nos testes.

Os aplicativos BF e *Autopsy* trouxeram praticamente os mesmos resultados. Localizaram documentos compartilhados em conversas, fotos e vídeos postados. Com a diferença de que os chats onde ocorreram os compartilhamentos também foram localizados pelo *Autopsy*.

Por fim, as ferramentas da *Magnet*, FJF e IEF, cumpriram seu papel. O primeiro localizou as imagens que foram baixadas da rede social, com as respectivas datas e ID dos perfis. O IEF trouxe a tona comentários de linha do tempo, troca de mensagens por chat e também curtidas do usuário analisado.

7.3 DISPOSITIVO MÓVEL

Os testes realizados em dispositivo móvel deixaram bem claro como a política de segurança do Facebook mudou para melhor após os escândalos com vazamento de dados dos últimos anos. Apenas em 2019, Mark Zuckerberg anunciou um investimento de quase 4 bilhões de dólares. A título de comparação, esse valor é equivalente ao faturamento total da empresa no ano de 2011, antes de abrir o capital.

As ferramentas utilizadas não foram capazes de captar nenhum outro dado além de fotos e vídeos armazenados no dispositivo que foram postados na rede social, com exceção do *Autopsy* que também resgatou documentos de texto

compartilhados. Arquivos referentes a pedidos de amizade, comentários, postagens, dentre outros tipos não foram encontrados. Softwares pagos, como o *Autopsy*, *Internet Evidence Finder* e *Belkasoft Evidence Finder* garantem que as versões vendidas a empresas especializadas e secretarias de Estado possuem o desempenho infinitamente superior ao de suas versões de teste.

Tabela 5 - Dispositivo Móvel

Dispositivo Android	Autopsy	BEF	FJF	IEF	Andriller
Eventos Linha do Tempo	✗	✗	✗	✗	✗
Conversas	✗	✗	✗	✗	✗
Mídia	✓	✓	✓	✓	✓
Reações	✗	✗	✗	✗	✗
Documentos	✓	✗	✗	✗	✓

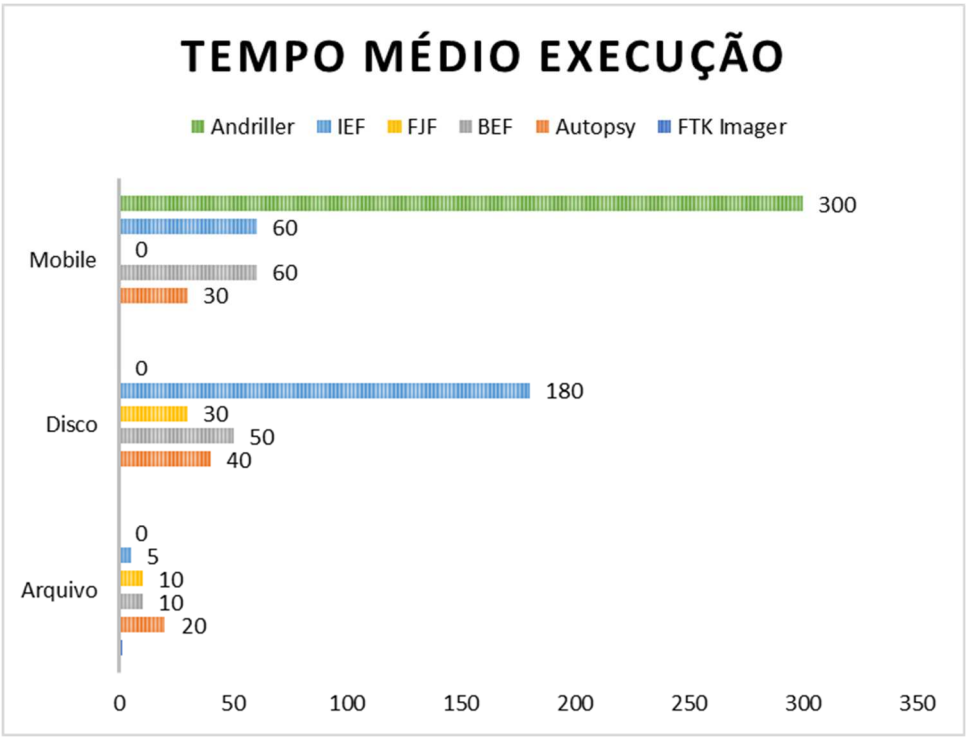
Fonte: Elaborado pelo autor.

7.4 TEMPO DE EXECUÇÃO

Fator de extrema importância na arquitetura dos softwares, o tempo de execução das varreduras podem ser fatores determinantes para uma perícia forense, principalmente quando se lida com dados temporários ou voláteis.

Podendo variar de acordo com o ambiente em que é executado e a quantidade de dados processados, na imagem a seguir temos o tempo médio, em minutos, de execução de cada ferramenta.

Figura 20 - Tempo Médio Execução



Fonte: *Print Screen* tirado pelo autor.

Pode-se constatar que as ferramentas *Belkasoft Evidence Finder* e *Autopsy* mantém o padrão de duração independente do ambiente de execução. Com destaque para a última, que apresentou a melhor performance nos testes realizados.

8. CONCLUSÃO

O combate aos crimes efetuados por meios cibernéticos necessita de uma legislação específica. Países como os Estados Unidos, Canadá e Alemanha já alteraram suas leis a respeito deste assunto. Enquanto isso, se encontra em discussão a Convenção Sobre o Cibercrime, também conhecida como Convenção de Budapeste, que propõe regular o combate a tais delitos em âmbito mundial, estimulando uma política de colaboração recíproca entre as polícias, entretanto o Brasil ainda não é signatário.

Para as práticas de Forense Computacional é de suma importância a utilização de técnicas e procedimentos homologados e bem fundamentados para que todo o processo de investigação se torne seguro e válido.

Pode-se afirmar que as normas penais que existem no Brasil não se fazem suficientes para penitenciar os comportamentos danosos que ocorrem na *Internet*, pois necessitam mais especificidade, incluindo ocasiões agravantes ou aumento de penas aos crimes digitais, definindo as competências de razão da matéria e razão do lugar. Da mesma forma, aperfeiçoar e manter sempre atualizado o corpo policial bem como as políticas de incentivo e proteção do Estado.

Foram apresentados desafios que ainda estão por vir para a área computacional forense, dentre eles a evolução tecnológica, que diariamente propõe novas ferramentas e sistemas a serem questionados. Os quesitos para a prática da perícia forense computacional, área esta que compreende o exame e a coleta de evidências digitais em dispositivos computacionais inseridos em procedimentos ilícitos ou qualquer natureza de crime, foram descritas no presente trabalho.

O profissional da computação forense se difere dos demais profissionais da área da tecnologia por, além de se fazer necessário o domínio da antigas e as novos procedimentos, ou ao menos ter o poder de entende-las de forma rápida, precisa atentar-se também, durante todo o processo investigativo, a utilização de técnicas que não comprometam o estado das evidências encontradas, pois, uma vez comprometidas, todo o restante do trabalho pode ser invalidado.

O principal objetivo deste trabalho foi apresentar uma análise a respeito de ferramentas de Computação Forense e sua aplicação direcionada a rede social Facebook. Um assunto que atualmente levanta muitas questões no meio tecnológico, onde apesar de recente, possui uma grande perspectiva de crescimento. Trata-se de uma área que vem se tornando muito utilizada, devido principalmente ao grande aumento do número de pessoas com acesso a esta rede e, por consequência, nos crimes envolvendo este meio.

Também foi de intuito informar a grande quantidade de ferramentas disponíveis no mercado para a análise forense. Muitas delas gratuitas, com um robusto poder análise e de usabilidade simplificada. Podendo assim auxiliar desde o perito mais capacitado até o usuário inicial.

Um fator que impôs limites ao estudo foi versão utilizada nos testes. Boa parte das ferramentas utilizadas liberaram versões com capacidade de processamento limitado em suas versões de demonstração, pois negociam seu produto apenas com pessoa jurídica.

Através deste estudo pode-se constatar que a computação forense tem muito que desenvolver e inovar. É necessário muito aperfeiçoamento no que se refere a métodos e tecnologias na obtenção das evidências necessárias para a solução dos crimes de informática. Ainda se conclui que estamos servidos de diversas ferramentas para o auxílio nas buscas, podendo elas serem específicas a apenas um tipo de evidência e trabalharem em conjunto durante a análise.

Um trabalho futuro, adquirindo por completo a licença de um kit de ferramentas para a análise forense e o aplicando em um caso específico de crime virtual, objetivando a identificação dos criminosos e a apresentação do laudo, seria de grande valia para o entendimento do papel do perito em uma investigação e do método de aplicação dos softwares por agências especializadas.

REFERÊNCIAS

ALMEIDA, Rafael Nader de. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais**. 2011. 48 f. TCC (Graduação) - Curso de Ciência da Computação, Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

AMARI, Kristine. **Techniques and Tools for Recovering and Analyzing Data from Volatile Memory.** Sans Institute Infosec Reading Room, Us, v. 1, p.9-35, mar. 2009.

BITENCOURT, Cezar Roberto. *Código Penal comentado*. 2. ed. atual. São Paulo; Saraiva, 2004.

CARTER, Nicholas. **Teoria e problemas de arquitetura de computadores.** Porto Alegre: Bookman, 2003.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. **Metodologia científica.** 5 ed. São Paulo: Prentice Hall, 2002.

CONSTANTINO, Diego Zaratini. **Técnicas da Computação Forense.** 2012. 66 f. TCC (Graduação) - Curso de Ciência da Computação, Instituto de Ensino Superior de Assis (imesa), Assis, 2012.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense.** São Paulo: Novatec Editora, 2010.

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

GRECO, Rogério. *Curso de direito penal*. 5. ed. Rio de Janeiro: Impetus, 2005.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. **Metodologia da investigação científica para ciências sociais aplicadas.** 2. ed. São Paulo: Atlas, 2009.

MELO, Sandro. **Computação forense com software livre.** Rio de Janeiro: Alta Books, 2009.

MONTEIRO, Mário A. **Introdução à organização de computadores.** 3. ed. Rio de Janeiro: ITC, 1996.

MURDOCCA, Miles J.; HEURING, Vincent P. **Introdução à arquitetura de computadores.** Rio de Janeiro: ed. Campus, 2000.

NG, Reynaldo. **Forense computacional corporativa.** Rio de Janeiro: Brasport, 2007.

PROCURADORIA GERAL DA REPÚBLICA: Centro de Cooperação Jurídica Internacional. Cibercrime. Disponível em: http://ccji.pgr.mpf.gov.br/institucional/informes/cibercrime Acesso em: 18 abril.2019.

STALLINGS, William; FIGUEIREDO, Carlos Camarão de; FIGUEIREDO, Lucília Camarão de. **Arquitetura e organização de computadores: projeto para o desempenho.** 5.ed. São Paulo: Prentice Hall, 2002.

TANENBAUM, Andrew S. **Organização estruturada de computadores.** 5. ed. Rio de Janeiro: Pearson Prentice Hall, 2007.

Vade Mecum Acadêmico de Direito - CD. **Novo Dicionário da Língua Portuguesa**. São Paulo: Rideel, 2007.

VASCONCELOS, Laércio; ASSUMPÇÃO FILHO, Milton Mira de (Editor). **Hardware total**. São Paulo: Makron Books, 2002.

ZANELLATO, Marco Antônio. Condutas Ilícitas na sociedade digital, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, n. IV, Julho de 2012.

FIELD, Hayden. **Facemash, la red ilegal que se convirtió en Facebook.** 2017. Disponível em: <https://www.entrepreneur.com/article/288398>. Acesso em: 12 mar. 2019.

COSTINE, Josh. **Facebook now has 2 billion monthly users… and responsibility.** 2017. Disponível em: <https://techcrunch.com/2017/06/27/facebook-2-billion-users/>. Acesso em: 12 mar. 2019.

CLARK, Kei Akoi; HILLSTEAD-JONES, Nicole. **Facebook Newsfeed Algorithm History.** 2019. Disponível em: <https://wallaroomedia.com/facebook-newsfeed-algorithm-history/>. Acesso em: 13 mar. 2019.

ALBANESIUS, Chloe. **News & Analysis / German Agencies Banned From Using Facebook, 'Like' Button.** 2011. Disponível em: <https://www.pcmag.com/news/286591/german-agencies-banned-from-using-facebook-like-button>. Acesso em: 13 mar. 2019.

GALANES, Philip. **De-Friend Me? I Don't Think So.** 2009. Disponível em: <https://www.nytimes.com/2009/05/24/fashion/24social.html>. Acesso em: 16 mar. 2019.

BEESE, Jennifer. **Facebook Fan Page vs. Profile: Know the Difference.** 2016. Disponível em: <https://sproutsocial.com/insights/facebook-fan-page/>. Acesso em: 16 mar. 2019.

AYRES, Scott. **Facebook Profile or Fan Page -- Which Should I Use for My Business?** 2015. Disponível em: <https://www.postplanner.com/facebook-profile-or-fan-page-which-should-i-use-for-my-business/>. Acesso em: 18 mar. 2019.

SOCIALBAKERS. **Facebook Statistics.** 2019. Disponível em: <https://www.socialbakers.com/statistics/facebook/pages/total/>. Acesso em: 18 mar. 2019.

WIKIPEDIA. **Red Bull.** 2016. Disponível em: <https://pt.wikipedia.org/wiki/Red_Bull>. Acesso em: 18 mar. 2019.

HELERBROCK, Rafael. **Rede 5G.** 2018. Disponível em: <https://mundoeducacao.bol.uol.com.br/informatica/rede-5g.htm>. Acesso em: 22 mar. 2019.

KUMAR, Ram. **A Recent Review on Growth of Mobile Generations-Case Study.** 2018. Disponível em: <https://www.researchgate.net/publication/327861617_A_Recent_Review_on_Growth_of_Mobile_Generations-Case_Study>. Acesso em: 22 mar. 2019.

VORA, Lopa J.. **EVOLUTION OF MOBILE GENERATION TECHNOLOGY: 1G TO 5G AND REVIEW OF UPCOMING WIRELESS TECHNOLOGY 5G.** 2015. Disponível em: <https://pdfs.semanticscholar.org/4dfd/40cc3a386573ee861c5329ab4c6711210819.pdf>. Acesso em: 12 abr. 2019.

CASTI, Taylor. **The Evolution of Facebook Mobile.** 2013. Disponível em: <https://mashable.com/2013/08/01/facebook-mobile-evolution/>. Acesso em: 22 abr. 2019.

APÊNDICE(S)

APÊNDICE A – ARTIGO CIENTÍFICO

Análise de Ferramentas para Computação Forense Aplicada a Rede Social Facebook

Eduardo Novak de Castro[1], Paulo João Martins[2]

[1]Acadêmico do Curso de Ciência da Computação – Unidade Acadêmica de Ciências, Engenharias e Tecnologias (UnaCET) – Universidade do Extremo Sul Catarinense (UNESC) Av. Universitária, 1105 - Bairro Universitário – Criciúma – SC – Brasil

[2]Professor do Curso de Ciência da Computação – Unidade Acadêmica de Ciências, Engenharias e Tecnologias (UnaCET) – Universidade do Extremo Sul Catarinense (UNESC) Av. Universitária, 1105 - Bairro Universitário – Criciúma – SC – Brasil

eduardonovakdc@gmail.com, pjm@unesc.net

Abstract. *Social networks, especially Facebook, have become part of people's routine. Accompanying this growth came criminals and malicious people, who use the platform to harm others. Faced with this problem it is necessary to investigate and punish such crimes. This article describes some tools capable of searching for evidence for crimes committed through Facebook and presents a comparative analysis of the results obtained by them.*

Resumo. *As redes sociais, com destaque para Facebook, tornaram-se parte da rotina das pessoas. Acompanhando este crescimento vieram os criminosos e as pessoas mal-intencionadas, que utilizam a plataforma para prejudicar os outros. Diante deste problema se faz necessário a investigação e a punição de tais delitos. Este artigo descreve algumas ferramentas capazes de buscar evidências para crimes cometidos através do Facebook e apresenta uma análise comparativa dos resultados obtidos por elas.*

1. Introdução

Da mesma forma que em crimes comuns, o tratamento de crimes cibernéticos requer a coleta de evidências e provas fortes de sua ocorrência, que possa convencer de forma completa os representantes dos poderes eleitos para julgar e punir tais crimes. A composição de provas em crimes virtuais é feita por meio da identificação, coleta e diferenciação de vestígios digitais, ou seja, de informações e dados trocados pelos sistemas computacionais em periféricos, aparelhos de armazenamento e na própria memória volátil do computador. (SILVA; LORENS, 2009).

Em um mundo contemporâneo e totalmente informatizado, a Internet é hoje ferramenta primordial que proporciona novos padrões de relacionamento social. Neste mesmo contexto e velocidade crescem também os crimes virtuais, principalmente os relacionados às redes sociais. Estes crimes tiveram grande aumento, pois sua prática se tornou muito mais fácil, onde diversas informações particulares ficam disponíveis na rede.

Ao mesmo tempo, os profissionais da área de computação forense têm desenvolvido e aperfeiçoado uma infinidade de ferramentas que auxiliam na busca pelos vestígios deixados por criminosos, sejam eles físicos ou digitais. Aplicações estão

disponíveis aos investigadores que devem avaliar o melhor momento para sua utilização e de que forma pode combiná-las a fim de obter os melhores resultados.

2. Forense Computacional

Na visão de Sebastiany (et al., 2012), a Ciência Forense é definida como um setor multidisciplinar, que pode abranger tanto a biologia, química, física, informática, entre diversas ciências e sua meta principal é fornecer auxílio às investigações das justiças civil e criminal.

A disciplina de forense computacional produz informações diretas, que podem ser decisivas em um dado caso, ao contrário das demais áreas forenses, que em sua maioria produzem resultados apenas interpretativos, como afirmam Noblett e Pollit (2000).

A Forense computacional é a parte da criminalística que compreende a aquisição, preservação, restauração e análise de evidências digitais, podendo estas estarem em dispositivos físicos ou processadas e armazenadas em ambiente virtual.

3. Crimes Virtuais

Os crimes podem ser definidos de duas formas. A primeira é a utilização de computadores para a realização de crimes já existentes, já na segunda modalidade, o computador age como o item principal para a realização do crime, bem como: ataques a sites, roubo de informações, roubo de senhas, entre outros novos delitos advindos do uso de computadores e Internet. (ELEUTÉRIO; MACHADO, 2010).

A definição de crime não possui diferença entre delitos comuns e para os crimes cibernéticos, isto é, ação humana que ocasione lesão ou ameaça contra os bens de maior importância para a sociedade, o comportamento do ser humano nos dois casos está sujeito a uma punição prevista em lei.

Decorrente ao crescimento de usuários do Facebook é o aumento de infrações penais ocorridas neste ambiente. A prática de crimes, cada vez mais corriqueira, sobrevém contra a honra, ameaças, pornografia infantil, estelionato, falsidades em geral, comércio de drogas e armas entre outros.

4. Metodologia e Aplicação das Ferramentas Forense

Os meios de pesquisa utilizados para a redação deste trabalho podem ser encontrados em livros desta mesma área, documentos existentes como artigos, monografias, dissertações e teses onde se fez presente o tema do forense computacional. Para a execução dos testes propostos neste trabalho, foram utilizados dois computadores com ambiente Windows, um smartphone Android e seis ferramentas forense diferentes. Todos os ambientes se encontram em plenas condições, em seu modo padrão de uso e acesso.

4.1. Aquisição dos Dados

Quando o perito possui acesso às informações da conta do investigado no Facebook é possível navegar por entre as funcionalidades da rede social em busca de evidências. Ou seja, analisar diretamente na página da Internet as publicações enviadas, fotos postadas e mensagens trocadas pelo investigado. Entretanto, este processo além de possuir um certo grau de amadorismo é também bastante moroso.

A partir de 2010 o Facebook passou a fornecer uma opção bastante interessante para seus usuários e, consequentemente, aos investigadores forense. Na sessão de opções, em ‘Configurações’, é possível solicitar uma cópia de todos os seus dados desde o dia em que sua conta foi criada até o presente momento. O pedido é avaliado pela administração da rede social e o tempo de resposta pode variar de usuário para usuário, compreendendo-se entre horas ou até mesmo dias.

No entanto, na grande maioria dos casos os investigadores não possuem as credenciais de acesso ao perfil do investigado, ficando impossibilitados de solicitar o arquivo de atividades. Os dados, então, devem ser adquiridos das outras fontes possíveis como o histórico de navegação do browser, arquivos temporários de Internet, arquivos de cache do navegador e até mesmo em informações guardadas em memória volátil.

4.2. Gerando o HASH

É de extrema importância garantir que o conteúdo do material não sofra qualquer modificação e nem trocado até que se conclua o inquérito. Sendo assim, surge a necessidade do emprego de métodos que permitam a averiguação da integridade e da legitimidade das informações. O principal destes métodos é o cálculo feito a partir de funções de autenticação unidirecionais definidas como hash. Tais funções, utilizando uma entrada de qualquer tamanho, produzem uma saída de tamanho fixo, isto é, convertem uma grande quantidade de dados em uma pequena sequência de bits.

Esta função é a mais utilizada para a verificação de integridade de dados computacionais em virtude de que uma simples modificação na informação de entrada do algoritmo produzirá um valor hash (sequência de bits) totalmente diferente. Ou seja, caso o teor de um arquivo tenha o seu conteúdo modificado em um apenas um bit, serão alcançadas como resultado duas sequências de bits totalmente distintas.

Para a geração da imagem dos dados extraídos do perfil do Facebook, foi utilizada a ferramenta da AccessData, o FTK ® Imager.

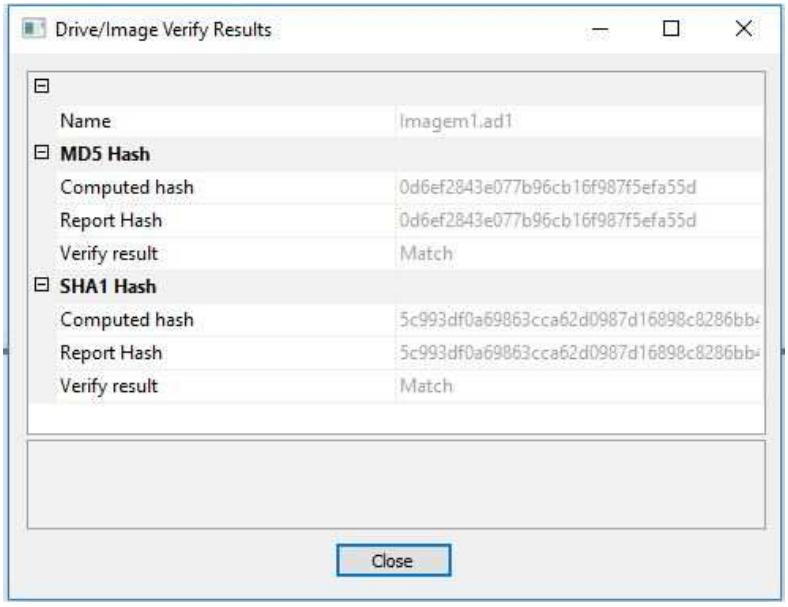


Figura 1. Valor HASH obtido

4.3. FTK Imager

Trata-se de uma ferramenta para montagem de imagens de forma que possam ter suas informações apenas lidas, sem permitir qualquer tipo de alteração. Além da criação das imagens, sejam elas de discos rígidos, CDs ou dispositivos USB, o FTK Imager também oferece recursos de visualização de dados. O FTK Imager também suporta a montagem de imagens, o que aumenta sua portabilidade. A ferramenta é uma das poucas que podem criar vários formatos de arquivo: EO1, SMART ou DD raw.

Ao criar cópias de unidades de disco originais, um aspecto crítico é verificar a integridade dos arquivos. O FTK Imager também auxilia nesta área, com suporte para a criação de hashes MD5 e SHA1. Além disso, pode-se gerar relatórios de hash que podem ser arquivados para uso posterior.

4.4. Autopsy

O software possui código aberto e vem pronto para funcionar em qualquer plataforma Windows ou Mac (Apple). A abordagem Open Source permite ao usuário verificar todos os aspectos da captura, processamento e análise de dados, fornecendo transparência e essencialmente colocando o controle totalmente nas mãos do utilizador. Nesse sentido, o software é educacional e informativo.

Um ótimo recurso é a capacidade da Autopsy de produzir resultados em tempo real, transmitindo resultados de palavras-chave à medida que aparecem nos dados pesquisados. Um rápido clique com o botão direito abre um arquivo relevante. Isso significa pouco ou nenhum tempo de espera para descobrir se há termos específicos de pesquisa no disco, no telefone ou no computador que está sendo pesquisado.

4.5. Belkasoft Evidence Center

O Belkasoft Evidence Center, seu principal produto, trata-se de uma solução integrada para coleta e análise de evidências digitais de dispositivos móveis e de computadores. Clientes em agências policiais, militares, comerciais, agências de inteligência e laboratórios forenses em mais de 130 países usam produtos Belkasoft para combater crimes on-line e off-line.

Os testes encontraram poucas evidências ligadas exclusivamente a rede social Facebook. Foram retornados os arquivos de fotos e vídeos postados na linha do tempo, além dos documentos compartilhados com outros usuários. A análise em dispositivo móvel, por sua vez, se mostrou muito mais frutífera no que tange o número de resultados retornados.

4.6. Facebook JPG Finder

Escrito na linguagem de programação Visual Basic exclusivamente para ambiente Microsoft Windows, o sistema foi projetado visando a otimização do tempo de extração das informações, o que o torna apto a funcionar com excelente performance até nas máquinas de configuração mais defasadas. O funcionamento se dá através de uma que pesquisa uma pasta selecionada por possíveis imagens JPG oriundas do Facebook. Essas imagens são identificadas executando vários filtros no nome do arquivo. O nome do arquivo contém o ID do usuário/perfil na rede social e, portanto, pode indicar de qual usuário do Facebook a foto veio.

Um arquivo de relatório HTML é criado na pasta de saída selecionada pelo examinador contendo o nome do arquivo, os horários de criação, modificação e último acesso. Também é gerado um link para o possível perfil do Facebook, um hash MD5 da imagem e a própria imagem. Todas as imagens localizadas também são copiadas para a pasta de saída, configurada na tela inicial ao iniciar o programa.

4.7. Internet Evidence Finder

O Internet Evidence Finder (IEF) é referência em investigação para milhares de agências de polícia, governos e corporações em mais de 90 países do mundo. Trata-se de uma ferramenta para forense computacional utilizada por inúmeros investigadores a fim de encontrar artefatos de Internet e avaliar evidências digitais armazenadas em computadores, smartphones e tablets. O software é capaz de recuperar evidências de mais de 265 tipos de artefatos de Internet em sistemas operacionais Windows e Mac. As buscas têm seus resultados apresentados no IEF Report Viewer – que permite aos analistas identificar as evidências relevantes – e são exportados em vários formatos de relatórios, de fácil compreensão.

O primeiro teste foi realizado em um computador pessoal. A busca foi feita em todo o disco da máquina, atrás dos arquivos de Internet que apresentariam qualquer ligação com o Facebook. O IEF conseguiu encontrar informações referentes a conversas, alterações de status e publicações no mural. A parte de pré-visualização permite que se verifique o ID do usuário e o conteúdo da postagem. No segundo teste a ferramenta foi utilizada para executar a pesquisa sobre o arquivo de informações solicitado ao Facebook. Como retorno foi obtido um endereço de perfil, mídias de vídeo e imagens.

4.8. Andriller

Esta ferramenta se trata de um software utilitário com uma coleção de ferramentas forenses para smartphones. Ela realiza aquisição não-destrutiva, somente leitura e forense de dispositivos Android. Ele tem recursos, como poderoso sistema para quebra de bloqueio de tela, código PIN ou senha; decodificadores personalizados para dados do Google Apps a partir de bancos de dados Android (alguns do Apple iOS e Windows) para comunicação codificada. Extração e decodificadores produzem relatórios em formatos HTML e Excel.

Primeiro, deve-se selecionar o diretório onde se pretende salvar os dados de extração. Após isso, utilizar o botão para verificar se a ferramenta encontrou o seu dispositivo móvel conectado. Finalmente, após definição do local de saída para o relatório, é iniciada a varredura. O Andriller executa a busca, o download e a decodificação tudo de uma só vez.

Após a conclusão da extração de dados, todos os dados são salvos na pasta no diretório especificado antes da extração. O principal arquivo de índice de extração é “REPORT.html”. Nele estará contido o resumo do dispositivo examinado e uma lista com todos os dados extraídos. Um excel “REPORT.xlsx” também é produzido simultaneamente, o qual contém todos os dados em um arquivo.

5. Análise Comparativa dos Resultados

A seguir serão analisados os resultados obtidos com os testes realizados com as ferramentas forense. No primeiro momento será analisado a capacidade de cada software

em resgatar as informações referentes ao Facebook por categoria. Posteriormente as ferramentas serão confrontadas quanto ao tempo de execução que apresentaram.

5.1. Arquivo Facebook

A tabela a seguir apresenta quais categorias de dados da rede social foram apresentadas ao fim da execução dos testes. As ferramentas Belkasoft Evidence Finder, Facebook JPG Finder e Internet Evidence Finder tiveram seus nomes abreviados para BEF, FJF e IEF respectivamente.

Tabela 1. Arquivo Facebook

Arquivo Facebook	FTK Imager	Autopsy	BEF	FJF	IEF
Eventos Linha do Tempo	✓	✓	✓	✗	✓
Conversas	✓	✓	✓	✗	✗
Mídia	✓	✓	✓	✗	✓
Reações	✓	✓	✓	✗	✗
Documentos	✓	✓	✓	✗	✓

A primeira análise foi feita sobre a performance das ferramentas sobre o arquivo enviado pelo Facebook, contendo todas as atividades do usuário desde a criação da conta.

Os aplicativos capazes de ler arquivos de imagem de disco não tiveram problemas e apresentaram todas as informações fornecidas pelo Facebook. Este também não possui controle das fotos que os usuários fazem download, por este motivo o FJF não mostrou qualquer resultado. Por sua vez, o IEF se mostrou capaz de catalogar vídeos e fotos enviados e identificar o perfil cujos dados pertencem.

5.2. Disco Local

Os resultados das análises feitas diretamente no disco se encontram na tabela a seguir:

Tabela 2. Análise Disco PC

Disco PC	FTK Imager	Autopsy	BEF	FJF	IEF
Eventos Linha do Tempo	✗	✗	✗	✗	✓
Conversas	✗	✓	✗	✗	✓
Mídia	✗	✓	✓	✓	✗
Reações	✗	✗	✗	✗	✓
Documentos	✗	✓	✓	✗	✗

Tratando-se unicamente de um gerador e leitor de imagens de disco, o FTK não foi capaz de encontrar algum resultado nos testes. Os aplicativos BF e Autopsy trouxeram praticamente os mesmos resultados. Localizaram documentos compartilhados em conversas, fotos e vídeos postados. Com a diferença de que os chats onde ocorreram os compartilhamentos também foram localizados pelo Autopsy. Por fim, as ferramentas da Magnet, FJF e IEF, cumpriram seu papel. O primeiro localizou as imagens que foram baixadas da rede social, com as respectivas datas e ID dos perfis. O IEF trouxe a tona comentários de linha do tempo, troca de mensagens por chat e também curtidas do usuário analisado.

5.3. Dispositivo Móvel

As ferramentas utilizadas não foram capazes de captar nenhum outro dado além de fotos e vídeos armazenados no dispositivo que foram postados na rede social, com exceção do Autopsy que também resgatou documentos de texto compartilhados. Arquivos referentes a pedidos de amizade, comentários, postagens, dentre outros tipos não foram encontrados. Softwares pagos, como o Autopsy, Internet Evidence Finder e Belkasoft Evidence Finder garantem que as versões vendidas a empresas especializadas e secretarias de Estado possuem o desempenho infinitamente superior ao de suas versões de teste.

Tabela 3. Dispositivo Móvel

Dispositivo Android	Autopsy	BEF	FJF	IEF	Andriller
Eventos Linha do Tempo	✗	✗	✗	✗	✗
Conversas	✗	✗	✗	✗	✗
Mídia	✓	✓	✓	✓	✓
Reações	✗	✗	✗	✗	✗
Documentos	✓	✗	✗	✗	✓

5.4. Tempo de Execução

Fator de extrema importância na arquitetura dos softwares, o tempo de execução das varreduras podem ser fatores determinantes para uma perícia forense, principalmente quando se lida com dados temporários ou voláteis. Podendo variar de acordo com o ambiente em que é executado e a quantidade de dados processados, na imagem a seguir temos o tempo médio, em minutos, de execução de cada ferramenta.

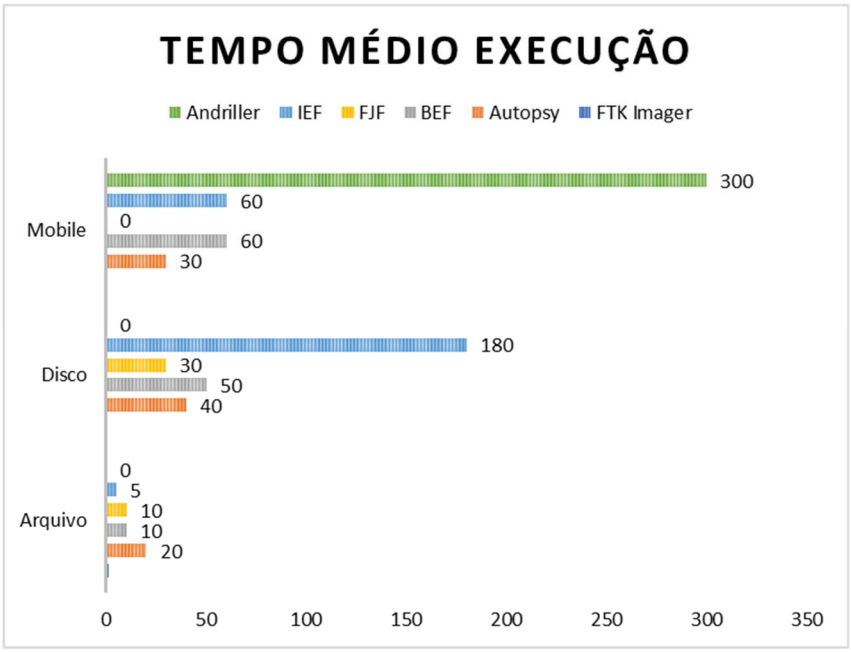


Figura 2. Tempo Médio Execução

Pode-se constatar que as ferramentas Belkasoft Evidence Finder e Autopsy mantém o padrão de duração independente do ambiente de execução. Com destaque para a última, que apresentou a melhor performance nos testes realizados.

6. Conclusão

O profissional da computação forense se difere dos demais profissionais da área da tecnologia por, além de se fazer necessário o domínio da antigas e as novos procedimentos, ou ao menos ter o poder de entende-las de forma rápida, precisa atentar-se também, durante todo o processo investigativo, a utilização de técnicas que não comprometam o estado das evidências encontradas, pois, uma vez comprometidas, todo o restante do trabalho pode ser invalidado.

O objetivo deste artigo foi apresentar uma análise a respeito de ferramentas de Computação Forense e sua aplicação direcionada a rede social Facebook. Também foi de intuito informar a grande quantidade de ferramentas disponíveis no mercado para a análise forense. Muitas delas gratuitas, com um robusto poder análise e de usabilidade simplificada. Podendo assim auxiliar desde o perito mais capacitado até o usuário inicial.

Através deste estudo pode-se constatar que a computação forense tem muito que desenvolver e inovar. É necessário muito aperfeiçoamento no que se refere a métodos e tecnologias na obtenção das evidências necessárias para a solução dos crimes de informática. Ainda se conclui que estamos servidos de diversas ferramentas para o auxílio nas buscas, podendo elas serem específicas a apenas um tipo de evidência e trabalharem em conjunto durante a análise.

7. Referencias

ALMEIDA, Rafael Nader de. Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais. 2011. 48 f. TCC (Graduação) - Curso de Ciência da Computação, Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

AMARI, Kristine. Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. Sans Institute Infosec Reading Room, Us, v. 1, p.9-35, mar. 2009.

BITENCOURT, Cezar Roberto. Código Penal comentado. 2. ed. atual. São Paulo; Saraiva, 2004.

CARTER, Nicholas. Teoria e problemas de arquitetura de computadores. Porto Alegre: Bookman, 2003.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. Metodologia científica. 5 ed. São Paulo: Prentice Hall, 2002.

CONSTANTINO, Diego Zaratini. Técnicas da Computação Forense. 2012. 66 f. TCC (Graduação) - Curso de Ciência da Computação, Instituto de Ensino Superior de Assis (imesa), Assis, 2012.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a computação forense. São Paulo: Novatec Editora, 2010.

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

GRECO, Rogério. Curso de direito penal. 5. ed. Rio de Janeiro: Impetus, 2005.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. Metodologia da investigação científica para ciências sociais aplicadas. 2. ed. São Paulo: Atlas, 2009.

MELO, Sandro. Computação forense com software livre. Rio de Janeiro: Alta Books, 2009.

MONTEIRO, Mário A. Introdução à organização de computadores. 3. ed. Rio de Janeiro: ITC, 1996.

MURDOCCA, Miles J.; HEURING, Vincent P. Introdução à arquitetura de computadores. Rio de Janeiro: ed. Campus, 2000.

NG, Reynaldo. Forense computacional corporativa. Rio de Janeiro: Brasport, 2007.

PROCURADORIA GERAL DA REPÚBLICA: Centro de Cooperação Jurídica Internacional. Cibercrime. Disponível em: http://ccji.pgr.mpf.gov.br/institucional/informes/cibercrime Acesso em: 18 abril.2019.

STALLINGS, William; FIGUEIREDO, Carlos Camarão de; FIGUEIREDO, Lucília Camarão de. Arquitetura e organização de computadores: projeto para o desempenho. 5.ed. São Paulo: Prentice Hall, 2002.

TANENBAUM, Andrew S. Organização estruturada de computadores. 5. ed. Rio de Janeiro: Pearson Prentice Hall, 2007.

Vade Mecum Acadêmico de Direito - CD. Novo Dicionário da Língua Portuguesa. São Paulo: Rideel, 2007.

VASCONCELOS, Laércio; ASSUMPÇÃO FILHO, Milton Mira de (Editor). Hardware total. São Paulo: Makron Books, 2002.