UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

GUSTAVO ZANIN COPETTI

PERÍCIA FORENSE EM REDES SOCIAIS: ANÁLISE DE EVIDÊNCIAS NO FACEBOOK E WHATSAPP

CRICIÚMA
2018

GUSTAVO ZANIN COPETTI

PERÍCIA FORENSE EM REDES SOCIAIS: ANÁLISE DE EVIDÊNCIAS NO FACEBOOK E WHATSAPP

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. MSc. Paulo João Martins

CRICIÚMA

2018

GUSTAVO ZANIN COPETTI

PERÍCIA FORENSE EM REDES SOCIAIS: ANÁLISE DE EVIDÊNCIAS NO FACEBOOK E WHATSAPP

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para a obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Perícia Forense em Redes Sociais.

Criciúma, 28 de junho de 2018

BANCA EXAMINADORA

Prof. MSc. Paulo João Martins – (Unesc) – Orientador

Prof. MSc. Rogério Antônio Casagrande – (Unesc) – Membro Banca

Prof. MSc Gustavo dos Santos De Lucca – (Faculdade SATC) – Membro Banca

Agradecer a minha mãe e meu pai por sempre estarem do meu lado, me apoiando e me auxiliando nos momentos bons e ruins, agradecer a minha irmã e a todos os parentes e amigos.

AGRADECIMENTOS

Agradecer principalmente aos meus país, Eliane Zanin e Francisco Copetti, por terem me concedido a total confiança no curso escolhido, e por proporcionarem-me os melhores caminhos de forma a obter sempre uma educação de melhor qualidade. E agradecer por eles não desistirem dos meus sonhos, sempre acreditando no meu potencial e da minha irmã.

A minha irmã Chailane Zanin Copetti, pelo apoio constante, sendo fundamental a não permitir a minha desistência do curso de Ciência da Computação. Aos meus tios Elaine Zanin e Reginaldo Folchini, padrinhos Jucerlei de Jesus e Rosane Zanin de Jesus compreendendo a ausência em alguns momentos. Aos meus Avós José Zanin e Salete Bez Batti, que estiveram presentes o tempo todo, na minha formação profissional e educacional, auxiliando na formação da pessoa que me tornei hoje.

Não esquecendo das pessoas que me auxiliaram nessa caminhada, minha namorada Helena Sartor Ronsani que disponibilizou ferramentas para o desenvolvimento do TCC e por estar sempre do meu lado nos piores e melhores momentos. Agradecer aos meus amigos: Lucas Felisbino, Gabriel Talamini, Augusto Sorato, Jhonatan Frasson Melo, João Gabriel Felisbino, Angelo Bratti e em especial para Alécio Andrade Filho onde sempre esteve preocupado e ao me lado se tornando um grande amigo para todos os momentos e Andrey Andrade pelo auxílio na pesquisa e apoio ao desenvolvimento do trabalho.

Agradecer a Universidade do Extremo Sul Catarinense (UNESC), pelo apoio acadêmico, aos professores por todo o conhecimento passado, em especial ao meu orientador e professor Paulo João Martins.

“É genial festejar o sucesso, mas é mais importante aprender com as lições do fracasso.”

Bill Gates

RESUMO

As redes sociais vêm se sobressaindo na era digital, aplicativos que atuam com diferentes níveis do meio de comunicação, entretenimento e profissional, proporcionando praticidade para os usuários. Com o passar do tempo apresentam-se novas redes sociais, porém com desafios a serem vencidos, tais como a aquisição de dados forenses e a realização da perícia forense. Os crimes em redes sociais vêm aumentando significativamente, desta forma surgindo a necessidade de combater esses crimes, portanto, auxiliando a perícia forense. O objetivo da pesquisa foi abordar perícia forense em redes sociais empregando um estudo de caso para relatar um método e realizar uma análise forense. Para a realização do seguinte trabalho utilizou-se a metodologia SOP aplicada em 7 etapas: autorização, preparação do equipamento, coleta e preservação, imagem forense, exame e análise, documentação, relatório e revisão. Com a conclusão, conseguiu-se estudar e aplicar os conceitos de perícia forense em redes sociais, utilizando a ferramenta *AccessData FTK Imager*, logrando êxito na análise dos arquivos.

Palavras-chaves: Redes Sociais. Pericia Forense. Segurança. Crimes Digitais.

ABSTRACT

Social networks have been standing out in the digital era, being applications that act with different levels, such as a means of communication, entertainment and professional, providing practicality for the users. As time goes by, new social networks have been presented, but with challenges to be overcome, such as the acquisition of forensic data and forensic expertise. Crimes in social networks have been increasing significantly, thus arising the need for new techniques to fight these crimes, therefore, aiding forensic expertise. The objective of the research was to approach forensic expertise in social networks, employing a case study to report a method and perform a forensic analysis. In order to accomplish such work, the SOP methodology was applied in 7 steps: authorization, preparation of the equipment, collection and preservation, forensic image, examination and analysis, documentation, report and revision. After the conclusion, we were able to study and apply the concepts of forensic expertise in social networks, using the AccessData FTK Imager tool, succeeding in the analysis of the files.

Keywords: Social Networks. Forensic Expertise. Safety. Digital Crimes.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ARPA	*Advanced Research Project Agency*
CCJ	Comissão de Constituição de Justiça
CSI	*Computer Security Institute*
DFRWS	*Digital Forensics Research WorkShop*
ENIAC	*Eletronic Numerical Integrator and Computer*
GECAT	Gerência de Combate a Crimes de Alta Tecnologia
HDFS	*Hadoop Distributed File System*
HTTPS	*HyperText Transfer Protocol Secure*
IHCFC	*International Hi – Tech Crime and Forensics Conference*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
MIM	*Mobile Instant Messaging*
RFC	*Request for Comments*
SOP	*Standard Operating Procedures*
TIC	Tecnologias de Informação e Comunicação
URL	*Uniform Resource Locator*
Wi-Fi	*Wireless Fidelity*

SUMÁRIO

1 INTRODUÇÃO

As redes sociais na atualidade vêm se tornando a forma de comunicação mais eficiente da Internet. Como a comunicação é imediata, altera a cultura social, fazendo as pessoas estruturarem suas vidas reais na rede virtual.

Uma das características das redes sociais é a possibilidade de abertura, onde viabiliza relacionamentos horizontais e não hierárquicos, ou seja, facilita a aproximação das pessoas, troca de conteúdos entre outras características que fazem com que elas tenham um crescimento.

No decorrer dos tempos o surgimento de novas tecnologias, e consequentemente, a evolução da Internet tem incorporado novas atividades dentre elas: a prática de crimes digitais, a utilização de redes sociais como Facebook, WhatsApp, entre outras. Com a melhoria e evolução das redes sociais, bem como os softwares e as pessoas com más intenções, procuram mascarar os crimes.

Por outro lado, tem-se a Perícia Forense Digital, que tem contribuído para a análise, interpretação e apresentação de evidências, com o intuito de tentar localizar vestígio dos crimes, utilizando algumas técnicas para tornar a descoberta possível, para os profissionais da área (SOUZA, 2018).

Devido a esse aumento nas redes sociais os crimes cibernéticos como, roubo de informações confidenciais, pedofilia, fraudes, sequestros, homicídios entre outros tem sido cada vez mais constante e são casos como os citados que necessitam saber como analisar e buscar vestígios com o intuito de comprovar e desvendar o suposto crime, trabalho este executado por um perito em tecnologia forense.

Segundo os dados da Norton, empresa de soluções em segurança cibernética, em 2016 houve um crescimento de 10% no número de brasileiros que foram vítimas de crimes virtuais, deixando o país com um prejuízo segundo a pesquisa de 10,3 bilhões de reais. A perícia forense busca nesses casos, vestígios que na maioria das vezes são deixados pelos criminosos.

Os Crimes Digitais, conhecidos como Crimes Cibernéticos ou Crimes de Alta Tecnologia, representam as condutas criminosas cometidas com o uso das tecnologias de informação e comunicação, e também os crimes nos quais o objeto da ação criminosa é o próprio sistema informático (CARVALHO, 2013), nas redes sociais também ocorrem

essas infrações, e podem ser realizadas em território nacional ou Internacional, neste caso dificultando muito os peritos na descoberta do réu, sendo que é necessário almejar um acordo internacional para buscar favorecer a vítima do furto.

Este trabalho tem como propósito, retratar metodologias e software, para resgatar evidências de crimes em redes sociais, sendo que o mesmo especifica como descrever e aplicar os conceitos sobre redes sociais, relatar conceitos de perícia forense em redes sociais, aplicar software de perícia forense em redes sociais, enumerar os métodos para que o usuário possa se proteger no uso de redes sociais e por fim especificar os crimes mais comuns em redes sociais.

Tendo em vista o meio virtual, onde se busca a informação referente a teoria forense em redes sociais, nota-se que essa área é necessitada de estudos, sendo que este trabalho vem para contribuir, demonstrando os sinais da falta de segurança da informação, caso contrário o usuário acaba com informações particulares expostas, podendo então trazer informações para o desenvolvimento de novos serviços e produtos.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Descrever e relatar metodologias e software para resgatar evidências de crimes digitais, em redes sociais.

1.1.2 Objetivo Específico

Os objetivos específicos desta pesquisa foram:

a) descrever e aplicar os conceitos sobre redes sociais;
b) relatar conceitos de perícia forense em redes sociais;
c) aplicar software de perícia forense em redes sociais;
d) enumerar os métodos para que o usuário possa se proteger no uso de redes sociais;
e) especificar os crimes mais comuns em redes sociais.

1.2 JUSTIFICATIVA

A computação forense tem como conceito segundo (LOPES, 2018) uma ciência multidisciplinar, que por sua vez aplica técnicas investigativas para determinar e analisar evidências, diferentemente dos outros tipos de perícias forense conhecidos, a análise forense computacional produz resultados diretos e não interpretativos conforme os outros modelos, sendo por sua vez decisivos em um caso.

O crescimento de crimes cibernéticos pelas redes sociais foi muito relevante, segundo a 18ª edição anual da pesquisa Global de segurança da Informação, lançada pela PricewaterhouseCoopers (PwC), uma das maiores prestadora de serviços profissionais do mundo nas áreas de auditoria, consultoria entre outros serviços, o número de ataques médios revelados no mundo subiu 38%, e no Brasil aumentou 274%, e a mesma pesquisa justifica que este crescimento, impõem as empresas um investimento maior, de forma a conseguir detectar os ataques, e em seguida responder a ele.

Devido à incidência de crimes por meio das redes sociais, a empresa BitDefender afirma que os incidentes vêm acontecendo com uma frequência alta, com os usuários que as utilizam, principalmente para fins comerciais, e assim os mesmos disponibilizam informações que deveriam ser confidenciais, muitas das vezes por questões de comodidade. Por outro, lado os *hackers* procuram obter informações destes usuários, onde tentam utilizar isto em benefício próprio, tentando extorquir dinheiro ou mais informações, e assim prejudicar a vítima.

Considerando o número de usuários em redes sociais segundo a BitDefender, o vasto crescimento de usuários justifica o porquê do aumento de roubo das informações, sendo que 80% das atividades dos usuários na internet são realizadas em redes sociais. Atividades compostas por compras de produtos pelas redes sociais podem acarretar no desvio de informações para clonagem dos seus dados, informações confidenciais que podem ser utilizadas para práticas de chantagens e extração de bens da suposta vítima.

1.3 ESTRUTURA DO TRABALHO

A presente pesquisa teve como objetivo descrever métodos e ferramentas para perícia forense em redes sociais. O trabalho está dividido em sete capítulos. O primeiro capítulo é a introdução, nela é encontrada a definição do problema, objetivo geral, objetivos específicos e a justificativa do trabalho. O segundo capítulo aborda sobre as redes sociais sendo elas o Facebook, WhatsApp e os recursos que as mesmas proporcionam, também aborda o tema do hadoop, como se utiliza o hadoop e como integrar a estrutura com a perícia forense nas redes sociais. O terceiro capítulo aborda a segurança das redes sociais, as ameaças a essa segurança e as políticas referente a segurança da informação possuindo no capitulo três tema referente aos crimes digitais e algumas leis relacionando os crimes específicos, crimes digitais e algumas leis referente aos seus crimes.

Quarto capítulo aborda a perícia forense em redes sociais, o framework Volatility buscando inovação para a perícia forense, a aquisição dos dados, pool de dados, que são as informações retiradas das redes sociais, como utilizar a perícia forense em redes sociais, as redes sociais a serviço da justiça e a investigação forense.

Os trabalhos correlatos usados para o desenvolvimento da pesquisa são abordados no sexto capítulo. O sétimo capítulo trata a temática da metodologia utilizada para a análise de evidências, ambientes utilizados para desenvolvimento, procedimento para a realização da perícia utilizando uma metodologia e por fim os resultados e discussão. A conclusão é o último capítulo desta monografia.

2 REDES SOCIAIS

Embora até hoje não tenha uma teoria referente as redes sociais, Barnes (1972) relata que sua compreensão pode ser diferente para diversas áreas de estudo. Diante desta tolerância, pode-se reconhecer que as redes sociais são constituídas por um vínculo complexo que podem acontecer entre pessoas, grupos ou organizações, os quais buscam interesses, valores ou crenças sem comum (MARTELETO,2001).

As redes sociais Segundo Marteleto (2001, p.72), tem a possibilidade de ser descrita como “um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados”. Por sua vez Downes (2005), subjuga que “uma rede social é um conjunto de indivíduos ligados entre si por um conjunto de relações”. Redes sociais também podem ser compreendidas como um aglomerado de relações sociais presente entre um grupo de pessoas e também entre estas pessoas individualmente (COLONOMOS,1995; ACIOLI, 2007).

Segundo Tomaél (2007), “A multiplicação da informação em grupos é comum nas redes, isto se compreende na sublimidade das pessoas terem confiança e se aproximarem de pessoas que as inspiram, ou terem uma familiaridade e alguma relação profissional”. Nesta circunstância, a pessoa possui uma característica de dispor de inúmeras relações, podendo ser originada pela amizade, relações de trabalho ou simplesmente pela troca de informação entre os indivíduos.

Com essas informações as redes sociais vão tendo um crescimento à proporção que os contatos vão sendo feitos, ocasionando na idealização social dos indivíduos, de forma que as igualdades resultam em um corpo social, onde as unidades são as redes sociais (TOMAÉL,2007).

“As relações que são feitas nas redes sociais muitas vezes são tão unidas que, na grande maioria das vezes é difícil de saber como começou ou com quem”, Tomaél (2007), sendo que as amizades constituídas nas redes sociais podem irem se reforçando ou se danificando, neste último caso ocasionando no conflito (ACIOLI,2007).

A análise de redes sociais, em muitos casos pode ser utilizada para o aprendizado dos movimentos sociais mais completos (MARTELETO,2001) quanto para o conhecimento das redes temáticas ou de relacionamentos informais, ou ainda de relacionamentos técnicos (ACIOLI, 2007).

Segundo Aguiar (2006), uma rede social é caracterizada por dois fundamentos principais: a estrutura e a dinâmica.

Uma rede social é uma estrutura composta por pessoas ou organizações, conectadas por um ou vários tipos de relações que partilham valores e objetivos comuns (DUARTE; QUANT, 2008).

Um dos principais fundamentos da definição das redes sociais é sua abertura e porosidade, possuindo a viabilidade de relacionamentos entre pessoas semelhantes e sem um nível de classe entre os indivíduos. As redes sociais podem ser classificadas como uma forma não estruturada partindo da habilidade de fazer e desfazer rapidamente, podendo ser classificada como uma forma de constituir conhecimento coletivo, onde os indivíduos utilizam as redes sociais como uma forma de se comunicar compartilhando informações.

As redes sociais podem ser utilizadas de diferentes formas como por exemplo as redes de relacionamento (Facebook, WhatsApp, Snapchat), redes profissionais (Linkedin), redes comunitárias (redes sociais em bairros ou cidades), redes políticas, dentre outras, que disponibilizam possibilidades de explorar as formas como a sociedade aprimora suas atividades, como os usuários atingem suas metas.

O conceito de rede social teve seu início há aproximadamente um século atrás, para denominar um conjunto confuso de relações entre diferentes indivíduos da sociedade, segundo Aristóteles (III a.C.), “o homem é um ser social”, ou seja, ele tem a necessidade de interagir, comunicar-se e manter relacionamentos.

Relações estabelecidas entre indivíduos com interesses em comum em um mesmo ambiente, sendo que usuários se comunicam e compartilham informações e interesses semelhantes.

As redes sociais, são organizações sociais compostas por um grupo de pessoas ou instituições conectadas por um ou diversos tipos de relações, que coparticipam de valores e propósitos em comum.

O acesso às redes sociais já faz parte do cotidiano de muitos usuários da Internet. Por meio delas, pode-se ter informação sobre os assuntos do momento, saber o que seus amigos estão fazendo, onde estão e o que estão pensando, também pode ver assuntos relacionados à seleção e vagas de empregos, pesquisas de opinião e mobilizações sociais.

Usar as redes sociais com segurança, é muito importante para isso é preciso que se esteja ciente dos riscos que elas podem representar e possa, assim, tomar medidas preventivas para evitá-los, pois a questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam. (SILVA; COSTA, 2009 apud QUALMAN, 2011).

Inclusão social e as rápidas transformações trazidas pela globalização - em que hoje é possível, praticamente, “nascer conectado” (GIDDENS, 2012).

2.1 FACEBOOK

Considerada a maior rede social do mundo na atualidade, (figura 1) o Facebook, foi fundado em 2004, por Mark Zuckerberg, ex-estudante de Harvard nos Estados Unidos. No início o projeto era restrito apenas para os estudantes da Universidade, obteve uma expansão para outras áreas até atingir o grupo secundarista, hoje utilizado por mais de 2 bilhões de usuários ativos por dia. Para competir com a outra rede social concorrente, a rede social incentivou os usuários desta a “importar” seus amigos através de um anúncio na sua página principal, onde disponibilizou um tutorial explicativo para extrair os contatos. O Facebook é no fundo mais um serviço de rede social que funciona bem (FACEBOOKINC, 2018).

Por ser uma das últimas inovações em redes sociais, a mesma possui um diferencial dos seus concorrentes, com um design elaborado possui características que fazem com que seus usuários necessitem explorar os links existentes. Essa tem sido uma das principais razões para algumas pessoas utilizarem ainda mais o Facebook.
Algumas vantagens:

a) encontrar amigos e colegas de escola e trabalho;
b) compartilhar;
c) chamadas de voz – serviços como o Skype podem ser utilizados sem maiores problemas. Tudo o que o usuário precisa é ter uma conta.

Figura 1 - O Facebook domina o panorama das redes sociais

Fonte: Statista (2017).

O Facebook, sendo a rede social mais utilizada do mundo, com uma enorme quantidade de usuários ativos todos os dias. Possuindo vários dados pessoais dos usuários, ferramentas que são utilizadas tanto para localização quanto para armazenagem de fotos e vídeos. Tendo como principal alvo a questão “o que você está pensando?”, fazendo com que os usuários sejam induzidos a compartilhar sua vida pessoal em público, fazendo com que sua vida passe de privada para pública, somente “sua”, visível a todos os usuários por meio de um clique.

2.1.1 RECURSOS FACEBOOK

Sendo a rede social mais escolhida pelos usuários, conforme a figura 1, o Facebook possui alguns recursos a serem explorados pelos usuários conforme os exemplos a serem citados:

a) *games e chatbots*: os usuários do Facebook além de conversar com outros amigos iniciar jogos desde clássicos como *PAC-man* até *Space Invaders*. Ainda com a possibilidade de utilizar um recurso chamado *ChatBot* basta entrar em contato com uma marca escolhida para que se comece uma

conversa com o *chatbot* sem precisar de nenhuma instalação bastando enviar uma mensagem privada para o *bot* responder;

b) possibilidades de propaganda: o Facebook buscando se tornar uma rede social para todos os gostos está proporcionando a exposição de propagandas e anúncios, durante e depois de transmissões e vídeos ao vivo;
c) grupos de chat com vídeo: embutido diretamente na interface do Messenger permite que até 50 pessoas participem de uma ligação com vídeo;
d) facebook live 2.0: buscando ainda mais o englobamento de outras redes sociais o Facebook criou a *Live* onde você pode realizar a transmissão da sua rotina diretamente do seu desktop a qualquer momento;
e) workplace do facebook: o objetivo do *Workplace* é auxiliar na sua rotina de trabalho, estando conectado com seus colegas de trabalho, muito semelhante ao Facebook, com *feed* de notícias, *chat* ou *live* permitindo os colegas de trabalho falarem uns com os outros;
f) facebook 360: com grande repercussão e o vasto avanço da tecnologia com a possibilidade de postar uma imagem 360. Segundo o site do Facebook até o momento, já foram publicadas na rede social mais de 25 milhões de fotos 360 e 1 milhão de vídeos 360;
g) messenger day: o Messenger Day é uma função muito parecida com o famoso Snapchat e as *Stories* do Instagram, tendo como diferencial verificar quem está *online* no momento de enviar a *storie* funcionando em tempo real.

2.2 WHATSAPP

Sendo a segunda rede social mais acessada no mundo (figura 1), o WhatsApp é um aplicativo de mensagens instantâneas para dispositivos móveis, conforme a descrição do produto em sua página virtual:

> Esse tipo de aplicativo permite trocar mensagens pelo celular sem pagar por SMS (Short Message Service). O recurso é disponível para iPhone, BlackBerry, Android, Windows Phone e Nokia e esses telefones podem trocar mensagens entre si. Como o WhatsApp Messenger usa o mesmo plano de dados de internet que se utiliza para e-mails e navegação, não há custo para enviar mensagens. Além das mensagens básicas, os usuários do WhatsApp podem criar grupos, enviar mensagens ilimitadas com imagens, vídeos e áudio (WHATSAPP).

O WhatsApp foi lançado em 2009 por dois amigos universitários funcionários da empresa Yahoo!, Jon Koum e Brian Acton, onde possuíam um problema pois não era permitido o uso de celulares na universidade, criando então a solução para as ligações perdidas. O nome do aplicativo vem da expressão em inglês *What's up?* que significa, em tradução livre, E aí? ou Tudo bem?. O aplicativo disponibiliza a troca de mensagens de texto, vídeos, áudios, imagens (WHATSAPP).

Todas as possibilidades citadas impulsionam a comunicação entre os indivíduos, depois da instalação o aplicativo utiliza o número de celular para criar uma conta, em seguida ocorrendo a sincronização com a agenda do smartphone. Como todos os usuários são registrados com o número do smartphone, o aplicativo reconhece todos os usuários que utilizam o WhatsApp, fazendo com que o aplicativo faça uma comparação na sua agenda com quem possui ou não a rede social.

Para o envio ou recebimento de mensagens a rede social utiliza os planos da operadora de telefonia ou simplesmente conecta em alguma rede Wi-Fi disponível, se por um acaso não possui nenhuma das possibilidades o aplicativo salva as conversas que são reapresentadas ao usuário.

O aplicativo ainda disponibiliza sinais onde verifica se a postagem foi enviada, recebida ou lida pelo usuário, sendo um se foi enviada, dois se a mensagem foi recebida e dois sinais na cor azul se a mensagem foi lida. Além deste recurso o aplicativo disponibiliza verificar se o interlocutor está online, se está digitando alguma mensagem e quando foi a última vez que o mesmo acessou a rede social. Como principais concorrentes dessa rede social, no Brasil pode-se citar: Viber, Telegram, ZapZap, Snapchat, Wechat, Google Hangouts, Line e Kik Messenger (CANEQUELA, 2015). Todos os aplicativos citados possuem diferenças, as quais cada usuário deve verificar qual está mais de acordo com suas necessidades. Todos esses aplicativos de troca de mensagens por meio de conversas são denominados por Church e Oliveira (2103) como *Messaging Instant Meaning* (MIM), sendo o WhatsApp o mais utilizado.

Outros quesitos que depõem contra o WhatsApp, segundo os autores, vêm da possibilidade de as pessoas enviarem ou receberem a mensagem sem conhecer quem enviou a mensagem, além de tudo vendo a foto que está disponível no seu perfil. A falta de segurança na leitura das mensagens na rede social WhatsApp foi resolvida

em uma atualização de abril de 2016 onde o mesmo começou a criptografar as conversas

Ao possibilitar a socialização de textos, muitas vezes híbridos (MARCUSCHI, 2004) em seus elementos, e o diálogo entre interlocutores, o WhatsApp (além de outros meios de interação social pela Internet) produz criatividade, estimula o raciocínio, constrói conceitos e estratégias de leitura, de escrita e de interação.

O site oficial do WhatsApp Messenger o descreve como:

> Um aplicativo de mensagens multiplataforma que permite trocar mensagens pelo celular. (...) não há custo para enviar mensagens e ficar em contato com seus amigos. Além das mensagens básicas, os usuários do WhatsApp podem criar grupos, enviar (...) imagens, vídeos, local, contatos e áudio.

Alguns de seus momentos mais importantes são compartilhados no WhatsApp. E por isso foi implementado uma criptografia nas versões mais recentes do aplicativo. Depois de ocorrer a criptografia das mensagens, as mesmas estão seguras fazendo com que somente o remetente e o destinatário possam lê-las ou ouvi-las nem mesmo o WhatsApp.

2.2.1 RECURSOS DO WHATSAPP

O WhatsApp permite com que você verifique se as chamadas que você fizer e as mensagens que você enviar estão criptografadas de ponta-a-ponta. Você consegue encontrar este indicador ao acessar a tela de dados do contato ou dados do grupo.

Chamadas de voz, você pode conversar com sua família e seus amigos gratuitamente, mesmo que eles estejam em outro país. E com as chamadas de vídeo, que também são gratuitas, você poderá conversar cara a cara quando as mensagens de voz ou de texto não forem suficientes. As chamadas de voz e vídeo do WhatsApp utilizam a conexão de Internet do seu telefone, ao invés de usar os minutos de voz do plano do seu celular, assim você não precisa se preocupar com altos custos de chamadas.

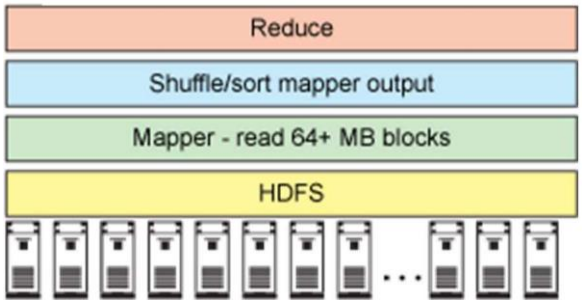
2.3 HADOOP

Criado em 2005 pela empresa Yahoo o Hadoop é considerado uma das mais significativas invenções de big data, projeto adquirido pela Apache está sendo utilizado por muitas empresas para analisar informações com grande quantidade de dados não estruturados, ou seja, elementos de difícil acesso que não podem ser organizados e dificilmente recuperados (APACHE, 2014).

De acordo com o Gartner, Big Data são grandes quantidades de dados, em alta velocidade, gerados por uma multiplicidade de fontes. Por serem criados de forma quase aleatória, esses dados não possuem estrutura. Podendo ser analisadas para auxiliar em algumas decisões mais eficazes no processo das informações. O Hadoop se encaixa em Big Data pois para o processamento dessas informações é necessário a utilização de ferramentas e técnicas singulares.

O Hadoop conforme o site oficial da Apache é uma estrutura que permite o processamento distribuído de grandes conjuntos de dados em clusters de computadores usando modelos de programação simples, sendo um software de código aberto do paradigma de programação Map-Reduce. Map-Reduce é um modelo de framework introduzido pelo Google para verificar e examinar grandes quantidade de dados. Todos os programas que são implementados nesse framework utilizam o paralelismo, que consiste na execução de uma grande quantidade de informações sem a necessidade de um servidor muito potente.

Figura 2 - Arquitetura Hadoop



Fonte: DevelopersWorks (2013)

Um grande processamento de dados se segmenta em vários outros processamentos (figura 2) que são executados em paralelo em diferentes “máquinas” para no fim encontrar uma única solução dada no início do processo. Um exemplo desse processo são os grafos de recomendações do Facebook, simplificando os problemas pois o desenvolvedor não irá incomodar-se com problemas de demora ou lentidão no processamento das informações.

A rede social Facebook utiliza o Apache para armazenar cópias de fontes internas de dados de registro e dimensão e usá-lo como fonte de relatórios (BORBOLO, 2010), análises e aprendizado de máquinas, sendo que os próprios utilizam um cluster de 1100 máquinas com 8800 núcleos e cerca de 12 GB de armazenamento bruto. Um cluster de 300 máquinas com 2400 núcleos e cerca de 3 GB de armazenamento bruto. Cada nó (*commodity*) possui 8 núcleos e 12 TB de armazenamento.

O Facebook ainda utiliza uma estrutura criada por eles de *data warehousing* de nível superior chamada de HIVE e outra implementação FUSE sobre o HDFS. O HIVE é um projeto, também de código aberto, do Hadoop de armazenamento para análise, redação e gestão de uma quantidade massiva de dados utilizando *querys* para fazer armazenamento de dados.

2.3.1 COMO UTILIZAR O HADOOP

Para utilizar o Hadoop pode ser recorrido a alguns centros de distribuição, como por exemplo a Empresa Cloudera Hadoop, onde a mesma possui suporte para várias distribuições Linux, ideal para iniciantes na plataforma, levando em consideração que a máquina já possua a tecnologia Java e cURL instalado. As recomendações são para utilizar o Ubuntu para realizar a instalação pois a utilização do APT facilita muito e permite usar o pacote binário sem detalhes de realizar o download e geração de origens.

O próximo passo é informar o APT da distribuição, sendo que dependendo do release utilizado pode alterar o código para a geração do Hadoop, e em seguida gerar um arquivo.

2.3.2 INTEGRAÇÃO DO HADOOP COM PERÍCIA FORENSE EM REDES SOCIAIS

O Hadoop na perícia forense em redes sociais é um projeto que vem sendo desenvolvido ao passar dos anos que irá permitir o processamento de uma grande

quantidade de dados, TSK é uma biblioteca e uma coleção de instrumentos de comando que permite a investigação de imagens de disco, tendo como principal recurso a análise de volume e dados do sistema de arquivos podendo ser implementada diretamente para encontrar evidências na perícia forense digital (MILAGRE, 2014).

3 SEGURANÇA DAS REDES SOCIAIS

É chamada de Segurança da Informação, o resguardo sobre as informações de uma pessoa ou empresa. Pressupondo que informação é todo e qualquer conteúdo ou conhecimento que tenha valor para pessoa ou organização, sendo que essa informação pode estar armazenada para uso pessoal ou exposta (BROSTOFF, 2004).

Contudo, pode ser estabelecido regras para a definição do nível de segurança presente, assim estabelecendo critérios para uma posição melhorada ou piorada da circunstância existente. A segurança de uma estabelecida informação pode ser atingida por fontes comportamentais e de aplicação de quem manipula a mesma, pelo ambiente ou infraestrutura que a cerca, ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação (COLAÇO, 2010).

O relacionamento com a proteção e o conjunto de dados, no sentido de proteger o valor que conservam para uma pessoa ou organização, são características essenciais da segurança de informação os atributos de confidencialidade, integridade e disponibilidade, não estando está segurança restrita somente a sistemas computacionais.

Segundo Colaço (2010), que gerencia softwares de segurança on-line no Facebook. "Consideramos que a educação dos adolescentes sobre a segurança da informação é responsabilidade que os encarregados políticos, defensores da segurança, pais e os serviços como Facebook devem participar," disse ele. "O Facebook confia no tratamento da segurança, o assédio moral e o assédio de forma proativa – pois a idealização de um universo de confiança é essencial para a sua missão assegurando uma experiência assertiva para os usuários do site."

Para que o usuário se sinta seguro nas redes sociais, os mesmos podem levar em consideração algumas dicas para proteger a privacidade (PSAFE, 2015):

a) Utilização de senhas fortes: na atualidade é de suma importância o a criação de uma senha complexa, diminuindo a probabilidade de sofrer golpes;
b) Download de aplicativos: é importante saber quais as permissões que o aplicativo tem acesso e quem desenvolveu o mesmo, possibilitando vírus no download dos aplicativos;
c) Utilização de autenticação de contas: com a frequência de ataques cibernéticos é válido a ativação de autenticações, como por exemplo,

impressões digitais, reconhecimento facial ou a utilização de *tokens* no caso de acessos a contas bancárias;

d) Instalação de Antivírus: para a proteção em redes sociais de malwares e vírus, a instalação de um antivírus pode auxiliar na preservação de informações;
e) Realizar *Logout* depois que acessar as redes sociais: a desatenção de uma rede social conectada, deixa seus dados vulneráveis para qualquer pessoa mal-intencionada, podendo acessar informações e sequestra-las, prejudicando o réu;
f) Ter cuidado com quem adiciona nas redes sociais: *Hackers* buscam informações para a prática de golpes, a aceitação de um convite faz com que o criminoso tenha acesso à dados confidenciais;
g) Conhecimento em redes sociais: é importante ter conhecimento nas configurações das redes sociais, definindo quem pode ter acesso as informações, deixando o perfil resguardado de desconhecidos.

3.1 AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

Os riscos referentes a segurança da informação estão associados diretamente ao extravio de suas três características ou atributos essenciais:

a) perda de confidencialidade: é quando ocorre um fracionamento da privacidade de uma estabelecida informação (exemplo a senha de administrador de um sistema), consentido que as informações restritas sejam liberadas, sendo que somente seriam acessadas apenas pelos usuários autorizados;
b) perda de integridade: ocorre quando estipulada informação fica evidenciada por um usuário não autorizado, podendo efetuar alterações que não são consentidas e não estão perante a gestão do proprietário da informação;
c) perda de disponibilidade: ocorre quando a informação não pode mais ser acessada por quem precisa dela. Exemplo seria a falta de comunicação de um sistema valoroso para a empresa, devido a uma falha ou erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

Em atos de ameaças à rede de computadores ou a um sistema, as ações podem acontecer por agentes maliciosos, muitas vezes conhecidos como *crackers*, (*hackers* não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Os *crackers* são instigados a realizar ilegalidades por vários fatores, os principais são: notoriedade, autoestima, vingança e o dinheiro. De acordo com pesquisa elaborada pelo CSI, mais de 70% dos ataques partem de usuários legítimos de sistemas de informação (*Insiders*), o que motiva corporações a investir largamente em controles de segurança para seus ambientes corporativos (Intranet) (ROSA, 2010).

3.2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

De acordo com o RFC 2196 (*The Site Security Handbook*), as políticas de segurança compõem de um aglomerado formal de normas que devem ser empregadas por quem utiliza os patrimônios de uma organização. As mesmas necessitam dispor de práticas realistas, e determinar nitidamente as áreas de responsabilidade dos indivíduos que utilizam, tendo que além de tudo se adaptar com as alterações da organização. Os princípios da segurança oferecem um âmbito para a execução dos mecanismos, apontam processos corretos, processos de auditoria e constituem uma base para metodologias legais na sequência de ataques.

O documento que descreve os princípios de segurança deve deixar de fora todas as questões técnicas relacionadas a execução dos mecanismos de defesa, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de ter as informações resumidas. Existem algumas normas que apontam o que deve ser julgados na elaboração das políticas de segurança. Entre essas normas estão a BS 7799 (é uma norma elaborada pela *British Standards Institution*) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e, por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

3.3 CRIMES DIGITAIS

O antecedente histórico mais remoto do surgimento da informática ocorreu em 1946, quando foi construído o primeiro computador digital, denominado ENIAC (WENDT; JORGE, 2012).

No entanto, o marco inicial do desenvolvimento tecnológico propriamente dito, e considerado assim por muitos autores, teria se dado em 1957, quando, o então presidente dos Estados Unidos, John Kennedy, em contrapartida ao lançamento do primeiro satélite artificial pela antiga União Soviética, prometeu enviar um americano para a lua e criar um sistema de defesa à prova de destruição. Dessa forma, tendo em vista tal objetivo, foi criada a ARPA.

Os primeiros casos de uso do computador para a prática de delitos datam da década de 50. Os crimes virtuais, ou cibercrimes, que são quaisquer atos ilegais onde o conhecimento especial de tecnologia de informática é essencial para as suas execuções, consistiam basicamente, nessa época, em programas que se autorreplicavam, ou seja, defeituosos (FERREIRA, 2000). Não houve, num primeiro momento, a intenção de se criar um vírus. Na verdade, o que ocorreu foi uma falha na compilação de determinado código fonte (instrução de comandos que faz um programa funcionar de determinada forma) gerando algum tipo de transtorno, o que se assemelha ao resultado danoso que o vírus que conhecemos hoje proporciona (SZNICH, 1995; WENDT; JORGE, 2012).

O comércio de drogas e armas acontece na Internet e é de conhecimento das autoridades, porém, se restringiam a *Dark Web*, 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. Há sites na *Dark Web*, que disponibilizam a contratação de assassinos de aluguel, para se ter uma ideia do conteúdo disponível neste porão da rede mundial de computadores (BBC, 2014). Contudo há muitos relatos de venda de drogas, injuria racial, e sequestros, principalmente na maior rede social do mundo, segundo pesquisa realizada pela empresa Statista, o Facebook.

De acordo com Paul Zak, professor da Universidade Claremont College, nos Estados Unidos, golpistas preferem usar a Internet para enganar pessoas para evitar o contato pessoal com elas. "É mais fácil prejudicar alguém quando não está olhando para esta pessoa", disse o professor. Segundo ele, pesquisas em neurociência mostram que violações morais são menos comuns em interações pessoais porque se cria uma empatia maior com quem se vê ao vivo.

Foi aprovado em 2015 na Comissão de Constituição e Justiça (CCJ) da Câmara dos Deputados, em Brasília, o Projeto de Lei n.º 7758/2014 que criminaliza as condutas ilícitas de usuários maledicentes, inclusive a falsa identidade nas redes sociais.

Dessa forma, o infrator, por exemplo, pode ser condenado, ser preso de três meses a um ano, simplesmente por ter criado um perfil falso (“*fake*”) no Facebook.

Além do Facebook outras redes sociais são utilizadas para a prática de crimes como por sua vez o WhatsApp um dos mais populares aplicativos no Brasil. Cresceu ao integrar o celular à comunicação via Internet, de forma gratuita. Não se justifica mais o envio de torpedos SMS pagos se é possível se comunicar com maior eficiência em uma interface gratuita. Além disso, o aplicativo permite o envio de conteúdo multimídia, áudio e vídeo e a criação de grupos. A aplicação diz ter 38 milhões de usuários no Brasil e 430 milhões de usuário no mundo. Há possibilidade de criar grupos privados e compartilhar.

3.4 LEIS PARA CRIMES DIGITAIS

Em abril de 2012 entra vigor a Lei 12.737/2012, que modificou o Código Penal e determinou o futuro para os crimes cibernéticos no Brasil. Quem invadir dispositivo informático alheio (computadores, tablets, notebooks, celulares, entre outros), conectados ou não à Internet, desenvolver programas para roubar dados ou divulgar e comercializar as informações obtidas de forma ilícita, a pessoa pode ser punida com multa ou poderá até ir para a prisão. As penas aplicadas variam de três meses a dois anos de reclusão, podendo ter uma pena maior caso o determinado crime resultar em um detrimento financeiro ou for cometido contra políticos como vereadores, deputados federais e estaduais, senadores e o presidente da República.

O grande problema da prova no meio informático é que ela é muito volátil. A investigação é mais complexa, porque envolve um caminho longo. É preciso preservar a prova para que ela se torne idônea. Para isso é necessário obter o endereço IP, que é a identidade virtual. Na maioria das vezes é necessário recorrer à Justiça para que o provedor forneça o IP, fazendo com que muitas vítimas desistam de procurar a Polícia.

O ideal em casos como esse é que ocorra a promulgação de uma lei processual no sentido de obrigar os provedores a informar a autoridade policial os dados, o que facilitaria a apuração da autoria dos crimes.

A proposta, que está na Câmara Federal, prevê que os provedores de Internet guardem os chamados logs (dados de conexão do usuário, que incluem endereço IP, data e hora do início e término da conexão, por um ano.

Conforme os dados do Tribunal de Justiça do Mato Grosso, atualmente 25 investigações de crimes virtuais estão em andamento na GECAT, da Polícia Judiciária Civil de Mato Grosso, sendo que 70% deles são de crimes contra honra, como calúnia, difamação e racismo, que já estão contidos na legislação e no Código Penal.

Os outros 30% são de crimes contra o patrimônio, ameaça, entre outros, explica o delegado, completando que apesar da falta de legislação que facilite o trabalho da Polícia, o GECAT, instalado há um ano, tem conseguido em 70% dos casos chegar ao autor do crime virtual. Nos próximos meses o GECAT, que até então trabalhou no assessoramento das unidades da Polícia Civil no Estado, passará a instaurar inquéritos policiais (TJMT, 2013).

Mesmo não sendo possível se proteger 100% dos crimes cibernéticos, é viável que o usuário tome algumas medidas de segurança. Primeiro é preciso ter cautela no uso de equipamentos informáticos. Ter um uso comedido, principalmente das redes sociais. Não precisa postar tudo, contar tudo, deixar o conteúdo aberto ao público, deixe apenas seus amigos terem acesso. São medidas que parecem simples, mas que surtem efeito. Segundo Elisa Mombelli (2014), a prevenção de crimes, acabam transformando a ficção em realidade com solução em Big Data, o *predictive policing* equivale em análise de dados que são obtidas de fontes variadas, suspeitando também das redes sociais. A utilização do Hadoop pode auxiliar no grande processamento de dados, por se tratar de uma grande quantidade de informações.

4 PERICIA FORENSE NAS REDES SOCIAIS

A pesquisa forense digital vem sendo destaque, pelo fato de crimes serem cada vez mais evidenciados na mídia, sendo que os mesmos ocorrem unicamente ou com auxílio de computadores. Vestígios deixados auxiliam tribunais e agências que executam as leis para a apreensão de provas para as investigações (LUIS, 2015).

Com o número elevado de pessoas compartilhando e se comunicando, a perícia se torna muito importante para a busca de informações nas redes sociais e em nuvem.

Grande parte dos provedores de redes sociais possuem serviços dedicados para atender os pedidos de aplicação da lei. Por exemplo o Facebook oferece informações de assinantes básicos e estendidos.

A investigação forense digital em muitos casos tem de confiar em um aglomerado limitado de informações, em qualquer caso, o investigador pode enviar solicitações ao operador e pode ou não receber todos os dados relevantes (por exemplo, escrito na aplicação da lei do Facebook diretrizes publicadas pelo EFF) (FACEBOOKINC, 2010). Isso está em clara contradição às diretrizes para a coleta de evidências, uma vez que o investigador não consegue mostram que a evidência é autêntica, completa e confiável (BREZINSKI, 2002). Rede forense o framework Volatility simplesmente não podem ver ou acessar todos os dados, uma vez que são apenas passivos.

4.1 VOLATILITY

O framework foi lançado em 2007 sendo que a primeira versão foi chamada de The Volatility, publicamente lançado na Black Hat DC. Constituído principalmente com base de vários anos de pesquisas acadêmicas que foram publicadas em análises avançadas de memória forense. Antes do lançamento do framework as investigações digitais eram ligadas ao tráfico de imagens armazenadas em discos rígidos. A volatilidade introduziu as pessoas no poder de analisar o estado de tempo de execução de um sistema usando os dados encontrados no armazenamento volátil (RAM) (VOLATILITY, 2014). O framework também disponibilizou uma multiplataforma, sendo extensível e modular para encorajar os trabalhos na área forense de pesquisa, outro

principal objetivo do framework era o incentivo, a colaboração, a inovação e acessibilidade ao estudo comum nas organizações de softwares.

Desde o surgimento do framework, a análise de memória forense vem se tornando um dos assuntos mais importantes para o futuro da perícia forense, sendo que o projeto é apoiado por uma das maiores comunidades ativas de forense. O Volatility oferece também uma plataforma onde possibilita realizar pesquisas avançadas e enviadas para os pesquisadores digitais (VOLATILITY, 2013).

No decorrer do tempo a construção do framework foi administrado pela The Volatility Foundation, uma organização independente sem fins lucrativos, que foi fundada para propiciar um uso da volatilidade e analise de memória no corpo social forense, para defender a propriedade intelectual do projeto (marcas registradas, licenças) e longevidade e, finalmente, para auxiliar na pesquisa de análise de memória inovadora. Nesse segmento, a organização foi trabalhando para auxiliar na proteção dos privilégios dos criadores do projeto onde tornaram a plataforma forense de memória gratuitamente e com código aberto (VOLATILITY, 2013).

4.2 AQUISIÇÃO DE DADOS

Antes de poder analisar os dados das redes sociais, os dados devem ser reunidos e adquiridos, embora os métodos forenses tradicionais possam ser usados para extrair artefatos do *cache* do *webbrowser* local, são possíveis inúmeras outras formas na camada de comunicação (ALTHEIDE; CARVEY; DAVIDSON, 2011). Estes variam desde o ataque passivo na rede para ativos como *sniffing Wi-Fis* não criptografado ou em combinação com *spoofing* ARP em *LANs*.

O rastreamento, no entanto, é limitado, pois metadados e *timestamps* precisos não são mostrados em páginas da *web*. Eles só estão disponíveis usando as APIs de rede social, que estendem os dados disponíveis da *interface web*. Embora seria possível usar o registro passivo na camada de comunicação, além disso, muitas redes sociais oferecem a possibilidade de criptografar dados na camada de comunicação usando HTTPS.

Em geral, não é possível um usuário baixar tudo o que está conectado ao seu perfil na rede social. Outro recurso interessante do Facebook Linha do tempo, usá-la

como um arquivo histórico. Se tornando interessante para exames forenses, uma vez que o usuário tem menos probabilidade de excluir dados.

4.3 POOL DE DADOS DE REDE SOCIAL

Embora as redes sociais variem em características e arquitetura, foi identificado as seguintes fontes genéricas de dados que interessam em exames forenses em questões sociais (BONNEAU, 2009):

a) o rastro social: qual é o gráfico social do usuário, com quem ele ou ela está conectado ("amigo")?;
b) padrão de comunicação: como é utilizada a rede para comunicação, qual método é usado e com quem o usuário está se comunicando?;
c) imagens e vídeos: quais fotos e vídeos foram carregados pelo usuário, em que fotos de outras pessoas ele ou ela é marcada?;
d) tempos de atividade: quando é um usuário específico conectado à rede social, quando exatamente aconteceu uma atividade específica de interesse?;
e) aplicativos: quais aplicativos o usuário usa, qual é o propósito deles e o que? a informação pode ser inferida no contexto social?.

Toda essa informação não pode ser encontrada no disco rígido de um suspeito, como é exclusivamente armazenado no operador. Especialmente para pessoas que usam a rede social em uma base diária, uma infinidade de informações é armazenada no operador. O Facebook afirma que mais de 50% de seus usuários use-o em qualquer dia, o que seria algo em torno de 400 milhões de usuários.

Maioria das vezes as informações são armazenadas em cache localmente, mas esta não é uma fonte confiável de informações como não são completas nem armazenadas de forma persistente. Dependendo a implementação, a disponibilidade de dados em si e a possibilidade de recuperar os dados através de chamadas de API pode variar entre diferentes redes sociais. No entanto, a maioria desses dados pode ser extraída diretamente, ou inferido com baixa sobrecarga sem a colaboração da rede social operador.

Embora os dados possam ser facilmente analisados manualmente, a enorme quantidade de dados requer automatização de ferramentas para um examinador forense ver a imagem completa.

4.4 COMO UTILIZAR A PERÍCIA FORENSE EM REDES SOCIAIS

Conforme os dados apontam o Facebook possui mais de 2 bilhões de usuários ativos, as informações postadas na rede social são muito importantes para a investigação forense. O compartilhamento de informações do seu dia a dia é uma forma de conseguir alguma pista sobre os suspeitos de algum crime em investigação.

O monitoramento das informações se dá com as postagens públicas que o usuário realiza, são analisadas e servem como provas, por esse fato o Facebook é rico em informações. Conforme Farmer (2007), “a análise forense de um sistema envolve um ciclo de coleta de dados e processamento das informações coletadas”. A linha de tempo de determinado usuário concede um histórico de vida, fotos, postagens, localização, onde comentários e curtidas podem auxiliar como provas para esclarecer um crime.

No fim da investigação essas informações geram um conjunto detalhado dos dados, onde esses dados são incorporados as ferramentas e sistemas utilizados pela autoridade buscando a resolução do caso (QUEIROZ, 2010).

4.5 REDES SOCIAIS A SERVIÇO DA JUSTIÇA

Nas redes sociais não ocorrem somente crimes cibernéticos, crimes como pedofilia, abuso sexual, sequestro, roubo, estelionato, homicídio e outros diversos também podem deixar vestígios, sendo que o criminoso pode fazer uso da rede social como meio ou apoio para praticar o ato ilegal (NOGUEIRA, 2009).

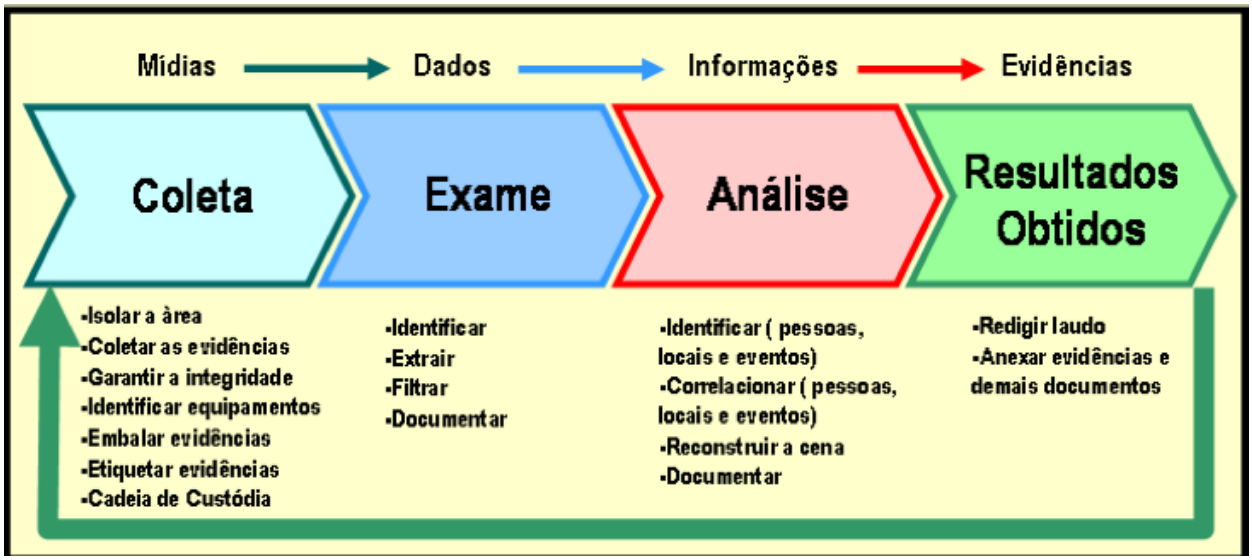
De acordo com Nogueira (2009, p. 42), “a internet está sendo usada há vários anos pelos terroristas do mundo todo, devido a sua rapidez na propagação de mensagens e alcance de milhões de pessoas rapidamente”.

Sendo assim, seja qual for a investigação pode ser realizada uma análise forense para a descoberta de vestígios e tentativa de desvendar crimes, além de que nos dias atuais as redes sociais possuem ainda mais pessoas compartilhando informações, estando mais conectadas.

A prática de coletar informações pessoais podem acrescentar à uma investigação que já teve início, ou dar um ponto de partida. Sabendo que é necessária uma autorização judicial para se aprofundar em dados protegidos.

Para realizar uma investigação forense pode ser levado em consideração algumas fases (Figura 3).

Figura 3 - Fases Investigação Computacional Forense



Fonte: Petter (2010)

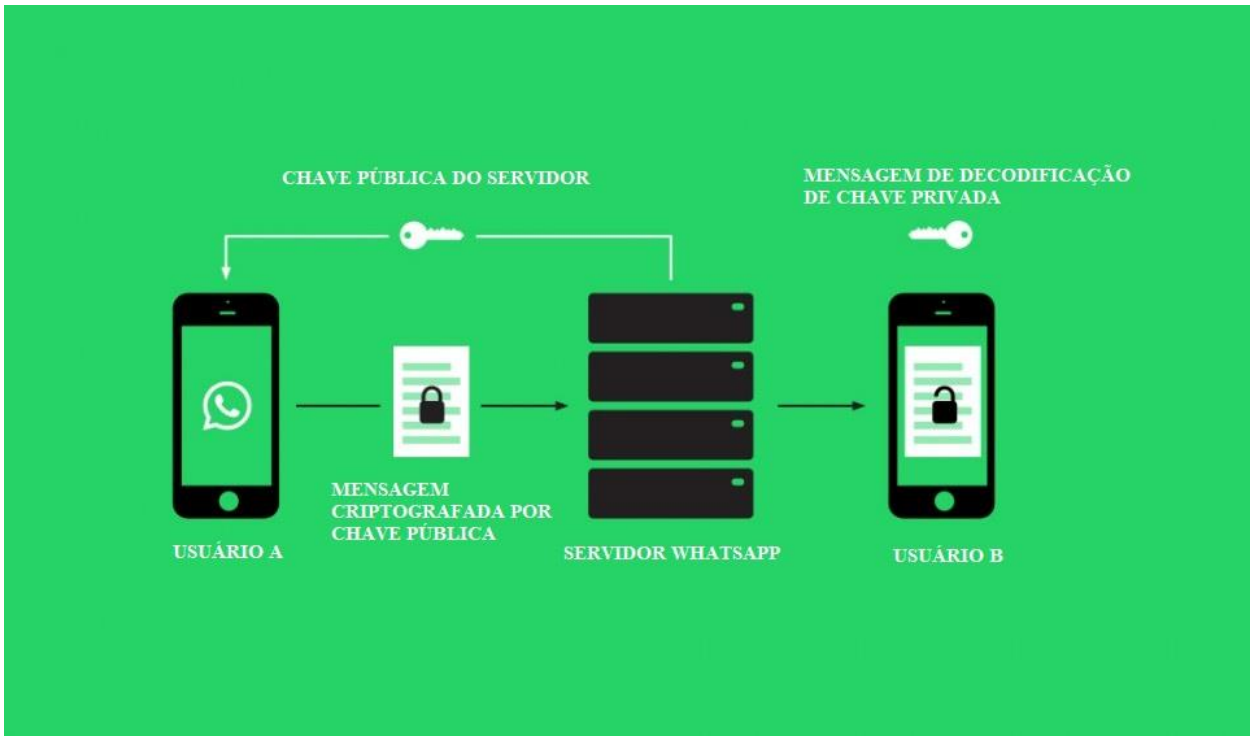
Para a resolução dos crimes digitais é necessário que ocorra constante evolução, para isso existem alguns processos que tendem a ter o objetivo de desvendar e expor as evidências do crime ou desfecho com informações de como, onde e quando aconteceu (CASEY,2004). Levando em consideração duas principais, a metodologia *Digital Forensics Research WorkShop* (DFRWS), possuindo sete etapas, identificação, preservação, coleta, exame, analise, apresentação e decisão (BERTOGLIO, 2008). A metodologia utilizada é conhecida por *Standard Operating Procedures* (SOP) sendo formada por seis etapas, preparação, identificação, coleta, analise, documentação e reconstituição, fazendo com que a metodologia tenha unificação com procedimentos e conceitos de perícia forense (WEBBA,2010).

4.6 INVESTIGAÇÃO FORENSE NO WHATSAPP

Nos anos de 2015 e 2016 ocorreu o bloqueio do aplicativo WhatsApp onde a mesma se negou a liberar as conversas trocadas entre dois suspeitos envolvidos em uma investigação.

O WhatsApp depois das últimas atualizações começou a usar recursos de criptografia assimétrica. Exemplificando na figura 4, a mensagem é enviada ao servidor do WhatsApp que mistura os caracteres com a utilização de um código. A mensagem só pode ser lida pelo destinatário onde o mesmo recebe uma chave criptográfica, dificultando muito a leitura da conversa.

Figura 4 - Criptografia do WhatsApp



Fonte: Wired (2011)

A criptografia criada pelo WhatsApp continua sendo um amplo desafio para as investigações, sendo ainda mais dificultoso para a justiça (FRANCO, 2016), não tornando possível ainda quebrar a criptografia sem a obtenção do equipamento, sendo estudado por muitos investigadores forenses. Em casos que os investigadores possuem acesso ao aplicativo, é possível realizar a investigação analisando as informações.

5 TRABALHOS CORRELATOS

No decorrer da pesquisa realizada, foram analisados alguns trabalhos com temas similares referente a perícia forense e redes sociais. A seguir será realizado um resumo breve de alguns trabalhos.

5.1 FORENSE COMPUTACIONAL: MÉTODO PROCEDIMENTO E FERRAMENTAS PARA PERÍCIA FORENSE EM CLOUD COMPUTING

O trabalho realizado por Célio Fabricio da Conceição Filipe, no curso de Ciência da Computação, pela Universidade do Extremo Sul Catarinense, como Trabalho de Conclusão do Curso, para obtenção do grau de Bacharel, sob orientação do Prof. MSc. Paulo João Martins.

O trabalho teve como objetivo demonstrar e realizar procedimentos de perícia forense em *Cloud Computing* tendo como foco a recuperação dos dados para realizar a perícia. O trabalho também possui a elaboração de um estudo de caso aplicando a metodologia SOP, contendo sete etapas: autorização, preparação do equipamento, coleta e preservação, imagem forense, exame e análise, documentação, relatório e revisão.

Com o fim do trabalho concluiu-se que foi possível analisar e estudar os conceitos de perícia forense computacional referente a Cloud Computing utilizando o ambiente Deft 7.2, as ferramentas *AccessData* FTK *Imager*, *Autopsy* e a pasta de sincronização do Google Drive.

5.2 PERÍCIA FORENSE COMPUTACIONAL: ESTUDO DAS TÉCNICAS UTILIZADAS PARA COLETA E ANÁLISE DE VESTÍGIOS DIGITAIS

O trabalho realizado por Rafael Nander de Almeida, no tecnólogo em Processamento de Dados, pela Faculdade de Tecnologia de São Paulo, para a obtenção do grau de tecnólogo em Processamento de Dados, sob orientação do Prof. Rodrigo Zuolo Carvalho.

O trabalho tem como objetivo qualificar Pericia Forense Computacional, descrever os processos que são aplicados na investigação, buscar os crimes cometidos utilizando ferramentas e equipamentos, descrever as dificuldades que surgem com o

decorrer da investigação como quantidade de arquivos, existência de senhas, criptografia e esteganografia.

Com o fim do trabalho foi possível concluir os principais conceitos de perícia forense, descrevendo onde um perito deve atuar em uma investigação, incluindo 43 procedimentos que podem ser realizados em uma investigação e por fim foi relacionando os aspectos jurídicos e legais com relação em crimes cibernéticos na Perícia Forense Computacional.

5.3 CRIMES CIBERNETICOS

O trabalho realizado por Kleber Assunção do Espirito Santo, no Curso de Direito, pela Faculdade de Ciências Jurídicas da Universidade Tuiuti do Paraná, para a obtenção do grau de Bacharelado, sob orientação do Prof. Dr. André Peixoto de Souza.

O trabalho tem como objetivo tentar responder algumas perguntas que são consideradas problemáticas segundo o autor, “quais os principais crimes praticados na internet?”, “Como o ordenamento jurídico pátrio e o de outros países tratam sobre os crimes perpetuados na internet?” e “o que já vem sendo feito no nosso ordenamento jurídico para abranger os crimes cibernéticos?”, também relatando na monografia a evolução do direito digital.

Com o fim do trabalho foi possível concluir que o aumento dos crimes cibernéticos é importante analisar sobre o Direito Penal, o vasto crescimento tecnológico vindo junto com a globalização o crime pode ser executado de todos os lugares em que tem rede disponibilizada.

5.4 UM ESTUDO DA INFLUÊNCIA DE REDES SOCIAIS NO DESENVOLVIMENTO DE ESTRATÉGIAS DE MARKETING

O trabalho realizado por Dean Costa Pinto, no curso de Desenvolvimento de Sistemas, pela Universidade Estadual de Maringá para a obtenção do grau de Especialista, sob orientação do Prof. Dr. Wesley Romão.

O trabalho teve como objetivo empregar um questionário a 115 usuários, demonstrando os potenciais das redes sociais como veículo de comunicação e marketing para empresas, realizando um compartilhamento de informações que sejam importantes para um processo de marketing empresarial. Realizando esse processo com

base na modalidade de pesquisa exploratória, abordando também no trabalho a importância da Web 2.0 buscando oportunidades de negócios e processos de Marketing justamente com o contexto de redes sociais.

Com o fim do trabalho foi possível concluir que os usuários realizam o acesso as redes sociais grande maioria das vezes em suas casas, onde possuem maior tempo vago possuindo mais tempo para o consumo, sendo assim facilitando a exposição de produtos e serviços.

6 MÉTODO, PROCEDIMENTO E FERRAMENTA UTILIZADA PARA PERICIA FORENSE EM REDES SOCIAIS

Segundo o Perito Judicial e Assistente Técnico em Informática, Marketing, Propriedade Intelectual e Crimes Informáticos José Milagre quando se trata em pericia forense em redes sociais tem de haver a distinção de duas áreas, uma utilizando uma grande coleta de dados e a outra a utilização de data mining em sua aplicação, sendo áreas incipientes e parando em questões de privacidade. Através da Lei 12.737/2012 pode-se achar fundamentos para investigação de vários ataques, com o mesmo sentido porem possuindo outros nomes, como por exemplo “Invasão de Dispositivo Informático” ou “invasão de e-mails e redes sociais”. Sendo que cada ataque *hacker*, possui diversas técnicas para utilizar, deixando assim, tipos diferentes de vestígios (ACADEMIA FORENSE DIGITAL, 2017).

O trabalho proposto aborda sobre pericia forense em redes sociais especificando o WhatsApp e o Facebook, considerada por peritos uma área científica recente, buscando realizar a integração da perícia forense com as redes sociais, em seguida realizando um estudo de caso onde teve a aplicação de um método, técnica e ferramenta para a busca e coleta de informações para a resolução de um suposto crime que ocorreu tanto no Facebook quanto no WhatsApp, visto que o trabalho é apenas um estudo de caso buscando as informações na arvore de amigos do determinado perfil.

Neste estudo foi realizada a criação de uma imagem forense e em seguida a busca das evidências de um crime nas redes sociais, com o objetivo de cooperar com a comunidade científica, com a elaboração de um trabalho possuindo diversas informações na perícia forense em redes sociais, com apoio nas metodologias e recursos buscando evidências.

Para a pesquisa, foram realizados estudos referentes as redes sociais mais utilizadas por usuários e as que possuíam mais indícios de crimes digitais, além das redes escolhidas, possuí também o Twitter e SnapChat. Foi então escolhido o Facebook e WhatsApp para realizar a pesquisa, pois os mesmos possuem maior incidência de crimes e quantidade de usuários ativos (ROZA, 2016).

Depois de escolher as redes sociais onde realizar a pesquisa, foi criado um estudo de caso onde evidenciasse um processo de perícia forense em redes sociais.

6.1 ESTUDO DE CASO

Foi realizado um estudo de caso baseado em alguns crimes que podem ocorrer nas redes sociais, buscando as informações em uma rede de amigos associados ao usuário conectado, permitindo acessar as redes sociais propostas e buscar as evidências conforme a ferramenta utilizada, não foi realizado a utilização de um caso verídico buscando a integridade, compreendendo que para ter acesso a dados é necessário uma autorização colocando em risco a segurança no desenvolvimento da monografia.

No presente caso um usuário no Facebook realiza postagens com apologia as drogas dando a entender que o mesmo possui ligação com o tráfico de drogas, realizando vendas e compras de entorpecentes via redes sociais, podendo apresentar provas pelo Facebook ou até mesmo possuindo conversas com outros integrantes no aplicativo do WhatsApp, sendo que para isso os responsáveis pelo caso entraram em contato com um perito Forense para encontrar evidências que levem a confirmação da suspeita.

Ao tomar posse do caso, o perito constatou que há vestígios de ligação com o tráfico nas redes sociais, por se abordar de um crime digital praticado em redes sociais, foi solicitado o computador apreendido para a realização das análises e aplicar todos os procedimentos para encontrar o máximo de evidências para servir de prova.

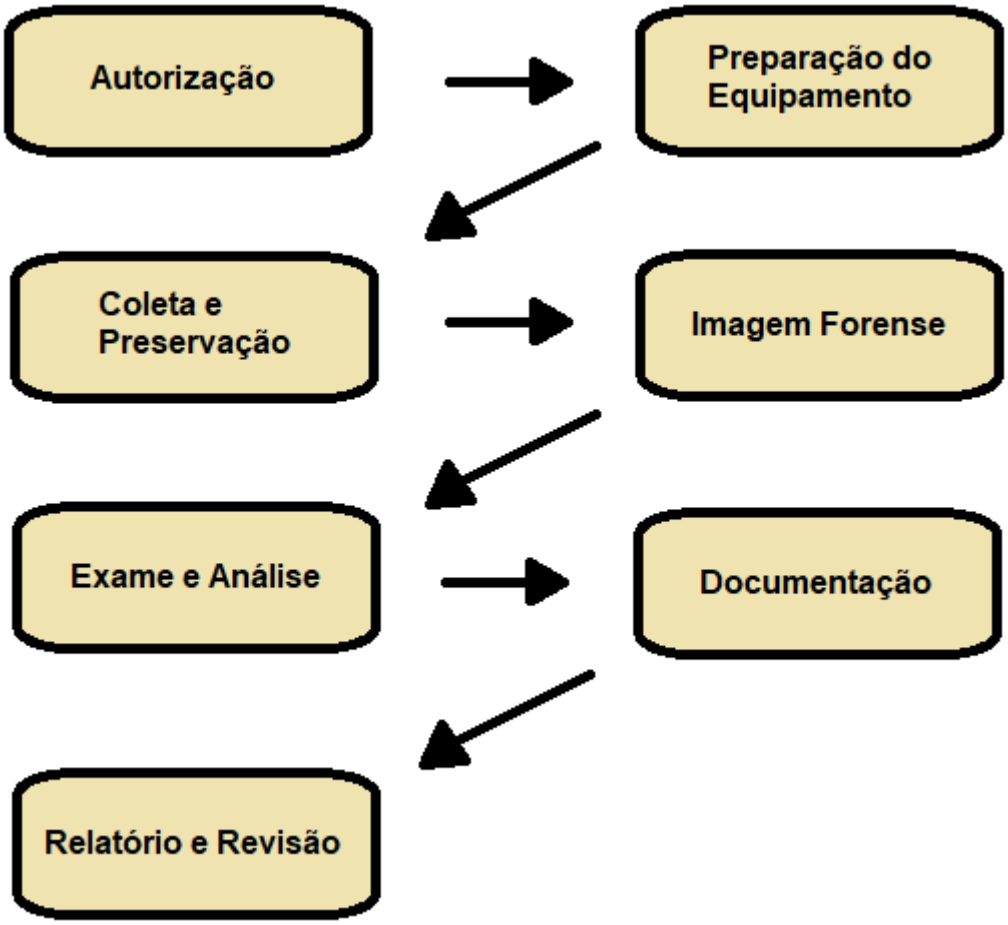
6.2 METODOLOGIA

Para o desenvolvimento do trabalho foram adotadas as seguintes metodologias: Na primeira etapa foi realizado o levantamento bibliográfico, redes sociais, crimes digitais entre outros, maior parte do trabalho dispõe de artigos científicos, livros, monografias e da Academia de Forense Digital.

Segundo Martins e Theóphilo (2009) afirmam que estudo de caso são expressões sinônimas que designam um método da abordagem de investigação em ciências sociais ou aplicadas. Consiste na utilização de um ou mais métodos qualitativos de recolha de informação e não segue uma linha rígida de investigação. Caracteriza-se por descrever um evento ou caso de uma forma longitudinal. O caso consiste geralmente no estudo aprofundado de uma unidade individual, tal como: uma pessoa, um grupo de pessoas, uma instituição, um evento cultural, etc. Quanto ao tipo de casos estudo, estes podem ser exploratórios, descritivos ou explanatórios.

Quando é realizada a analise referente a perícia forense, dependendo do caso levasse em consideração diferentes formas de analise, para a análise do caso apresentado foi utilizado a metodologia SOP (*Standard Operating Procedures*), sendo a mais utilizada no Brasil e apresentada pela *International Hi-Tech Crime and Forensics Conference* (IHCFC), como padrão internacional desde 1999. A metodologia utilizada possui várias etapas conforme a figura 5, sendo elas, Autorização, Preparação do Equipamento, Coleta e Preservação, Imagem Forense, Exame e Analise, Documentação, Relatório e Revisão.

Figura 5 - Etapas metodologia SOP



Fonte: Vargas (2007).

6.2.1 Autorização

Com o desenvolvimento do trabalho para fins acadêmicos não foi necessário a realização da prática de autorização, que consiste na busca das informações da rede

social para que o perito realize a busca das evidencias, porém foi utilizado o restante das etapas conforme consta na metodologia SOP.

6.2.2 Preparação do Equipamento

Para que o perito realize uma análise com completas condições é necessário que o mesmo possua equipamentos que condizem com as ferramentas e softwares utilizados no processo, possuindo então os pré-requisitos para que seja realizada a investigação forense computacional em redes sociais. Os computadores utilizados para realizar a análise (figura 6) apresentem as seguintes configurações:

a) ultrabook LG U460:
    a) disco rígido 280 GB,
    b) memória SSD 128 GB,
    c) memória RAM 4 GB,
    d) sistema operacional Windows 10 *Home Single Language*,
    e) processador core i3 – 3227U CPU @ 1.90GHz;
b) notebook Dell Inspiron 14:
    a) disco rígido 280 GB,
    b) memória SSD 256 GB,
    c) memória RAM 16 GB,
    d) sistema operacional Windows 10 Pro,
    e) processador i5 – 4210U CPU @ 2.40 GHz;

No notebook Dell Inspiron foi realizado a análise, sendo realizada a instalação do software *Forensic Toolkit Imager* (FTK Imager), onde foi realizada a busca de evidências, sendo que o notebook LG, foi utilizado para a utilização das redes sociais, onde foi criado a imagem para a análise.

6.2.3 Coleta e Preservação

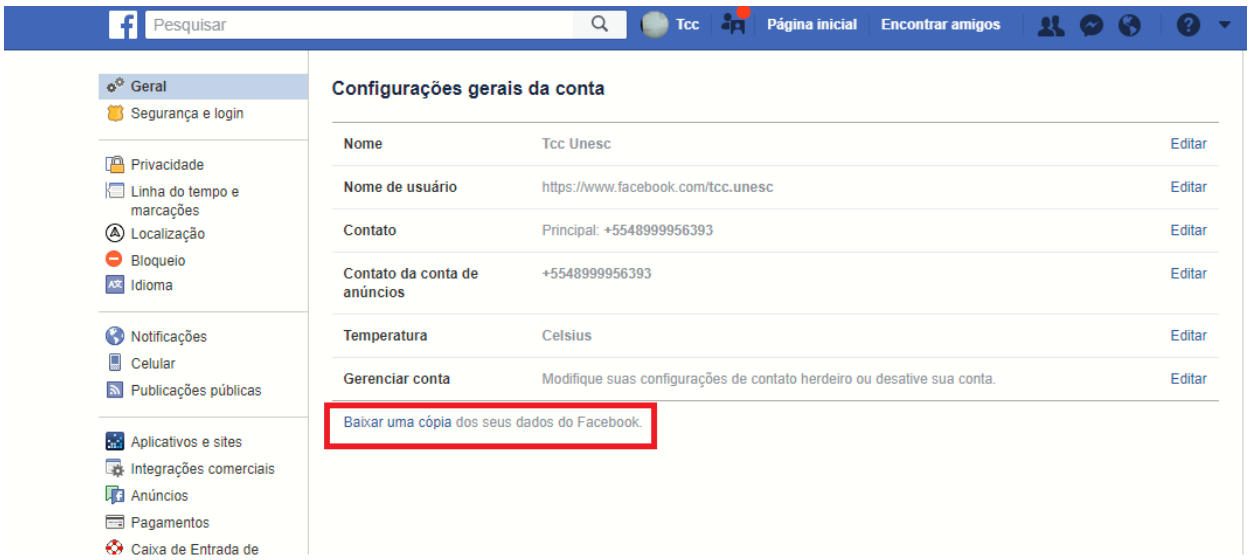
A coleta é entendida como a apreensão de informações físicas e lógicas, sendo que deve ser de forma cuidadosa por se tratar de dispositivos frágeis como computadores (RODRIGUES, 2017). Depois de realizar a coleta, vem a necessidade de

transporte do material, sendo meios eletrônicos se tornam sensíveis, exigindo do perito um maior cuidado para não danificar nenhum meio de prova (RODRIGUES,2017).

Sendo realizada, a perícia em redes sociais, muitas vezes se encontra o desafio de como acessá-las, e para acessar os dados de usuário no Facebook, por exemplo, é necessário seguir uma série de regras pré estabelecidas pela equipe do Facebook, descrito no documento “Requisito Legal de Processo Internacional”, para fins acadêmicos foi realizado um novo cadastro, porém para a busca das informações antigas o Facebook disponibilizou uma função onde é requerido os dados (figura 7).

Já no caso do WhatsApp a ferramenta possui uma função parecida com o Facebook, onde o usuário pode realizar o download do backup das conversas, porem sendo necessário que o proprietário realize um backup para futuramente usufruir do mesmo.

Figura 6 – Download informações do Perfil Facebook



Fonte: Do Autor.

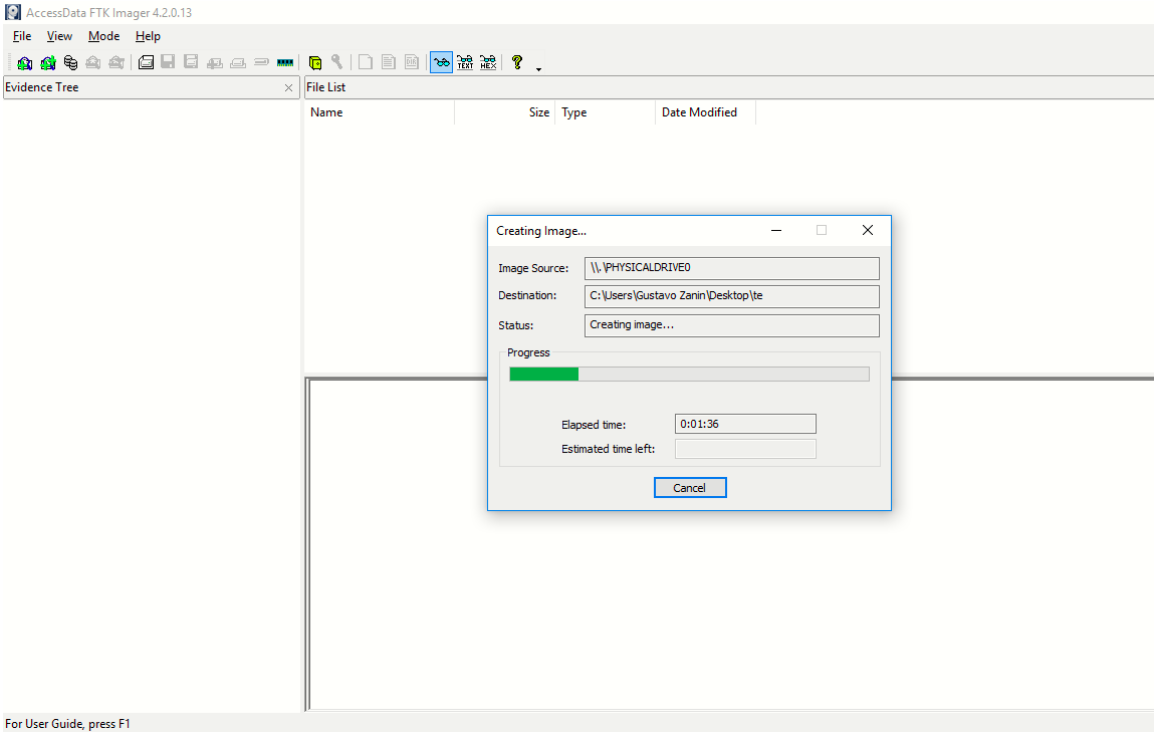
Com o requerimento das informações o Facebook necessita de um tempo para disponibilizar o link para realizar o download do que foi solicitado, dependendo da quantidade de informações. Antes de efetuar o processo é possível realizar o procedimento de sanitização, consiste em realizar uma limpeza em algum caractere específico (0x00) por exemplo, de acordo com o documento SP 800-80, publicado pelo *National Institute of Standarts and Technology*, em 11 de setembro de 2006, estudos tem mostrado que a maioria das mídias atuais podem ser efetivamente sanitizadas com apenas uma sobrescrita (PETTER, 2018).

6.2.4 Imagem Forense

Para a realização da análise forense das redes sociais, foi utilizado o software para a criação *AcessData Forense Toolkit Imager*, o mesmo possui a opção para a criação de uma imagem e captura de memória para que seja analisado. Ao fim do processo de geração da imagem, foi constituído um arquivo *Hash* com o algoritmo Md5 e Sha1 e em seguida transferido para a máquina onde houve a análise forense no Facebook e no WhatsApp com o mesmo arquivo. Na sequência da criação da imagem forense, é apresentado o sumário onde demonstra as informações do arquivo criado (figura 9). Seguindo a análise foi realizado, a criação de um arquivo *hash* (figura 10), onde busca armazenar a informação para uma possível verificação em alterações nas evidências.

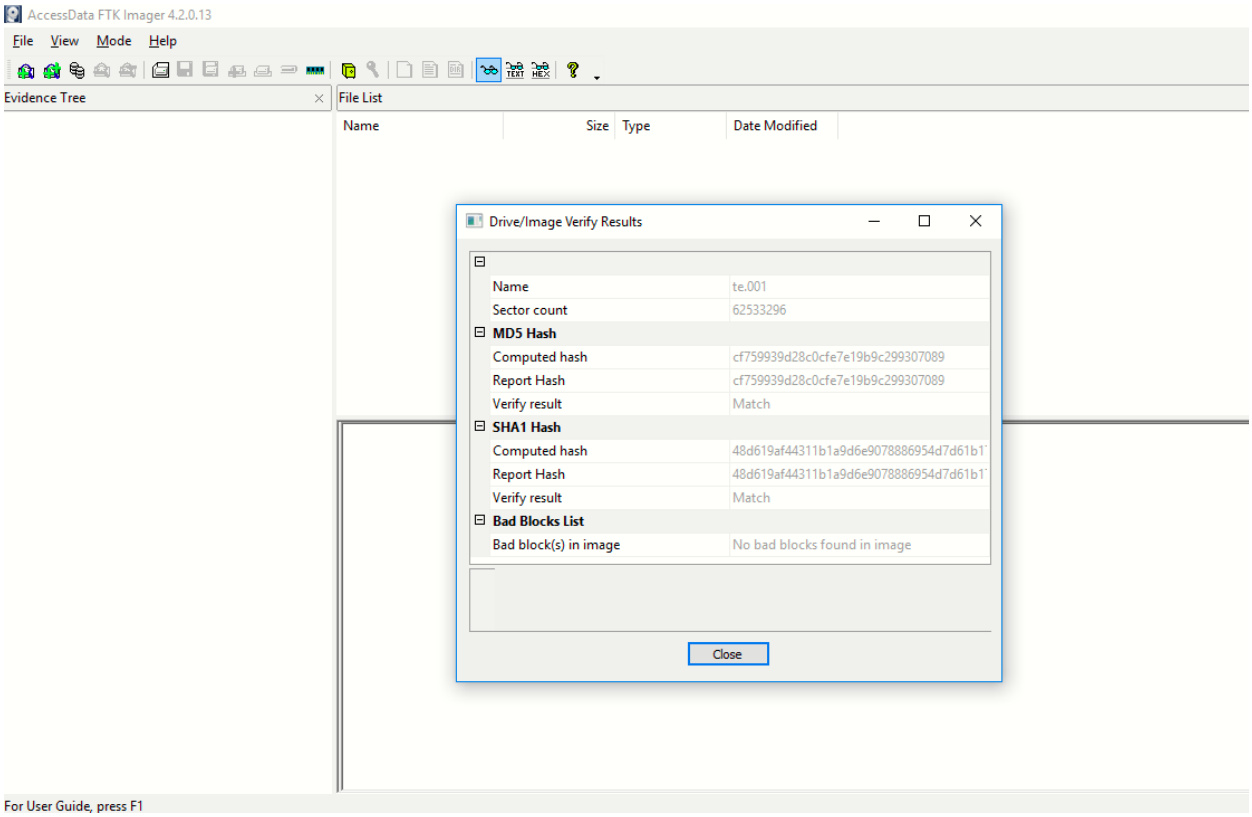
Na figura 8 demonstra a geração de uma imagem forense, depois de finalizado vai ser utilizado para buscar informações referente a investigação forense.

Figura 7 - Criação da Imagem Forense



Fonte: FTK Imager

Figura 8 - Criação da Imagem e Hash



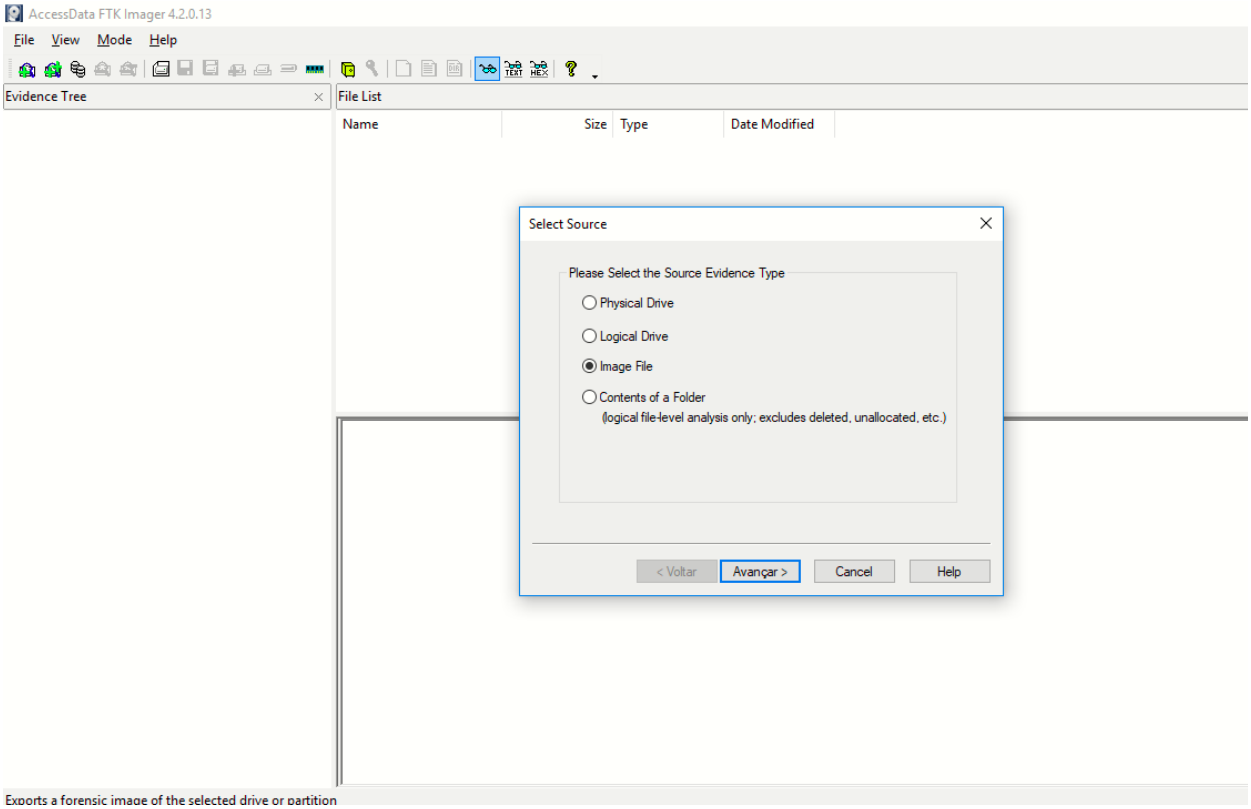
Fonte: FTK Imager

6.2.5 Exame e análise

Para realizar o exame e a análise, para que não ocorra a perda das informações é necessário realizar uma cópia dos dados, para não ocorrer o extravio ou alteração da imagem. Depois desta ser realizada, foi adicionado a imagem na ferramenta FTK Imager onde é possível visualizar as informações, conversas e imagens para a análise.

Depois de adicionar a imagem, basta realizar as configurações do software, escolhendo se vai ser realizado as evidências, física, lógica, imagem ou alguma pasta disponível (figura 12).

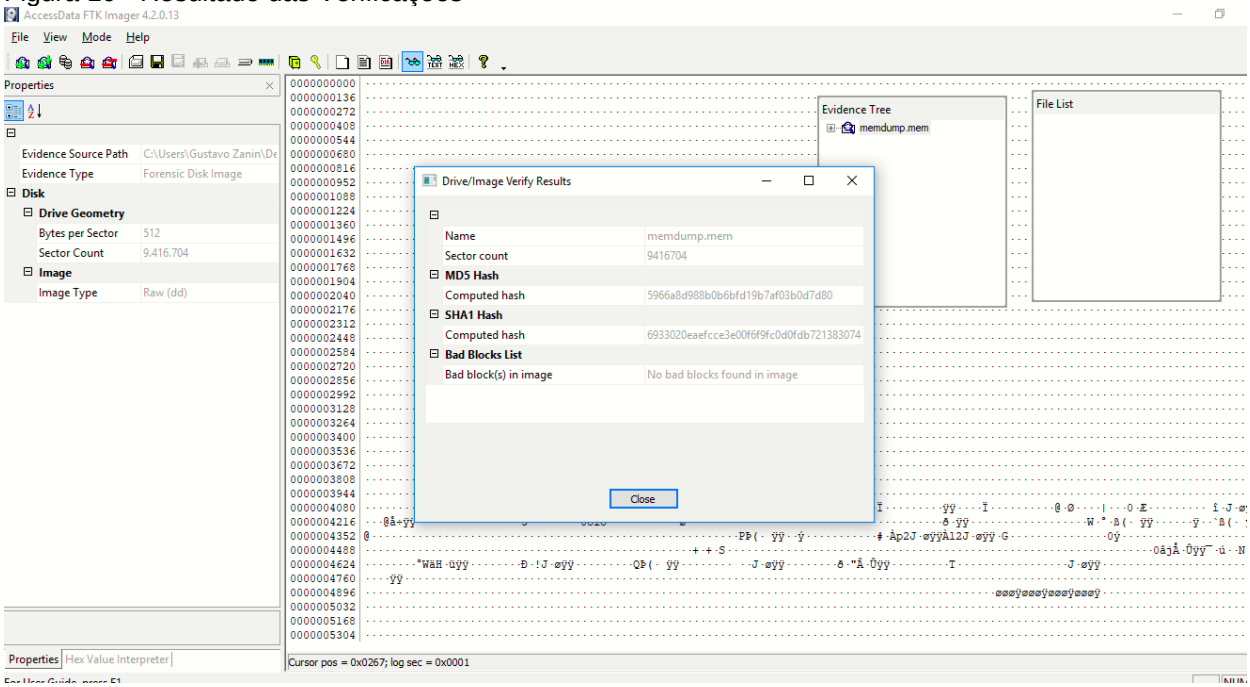
Figura 9 - Opções de análise



Fonte: FTK Imager.

Com a imagem importada, existem duas formas que demonstram as informações, uma coluna em hexadecimal e outra o mesmo texto corrente. Nesse caso busca-se informações para solucionar um crime utilizando a opção de busca nos textos. Anterior a isto, é necessário verificar a possibilidade de alguma alteração no arquivo, pelo comando *Verify Drive/Image* (figura 13), no fim do processo apresentando se houve alteração de blocos. No resultado (figura 14) demonstrou que o arquivo não ocorreu nenhuma modificação.

Figura 10 - Resultado das Verificações

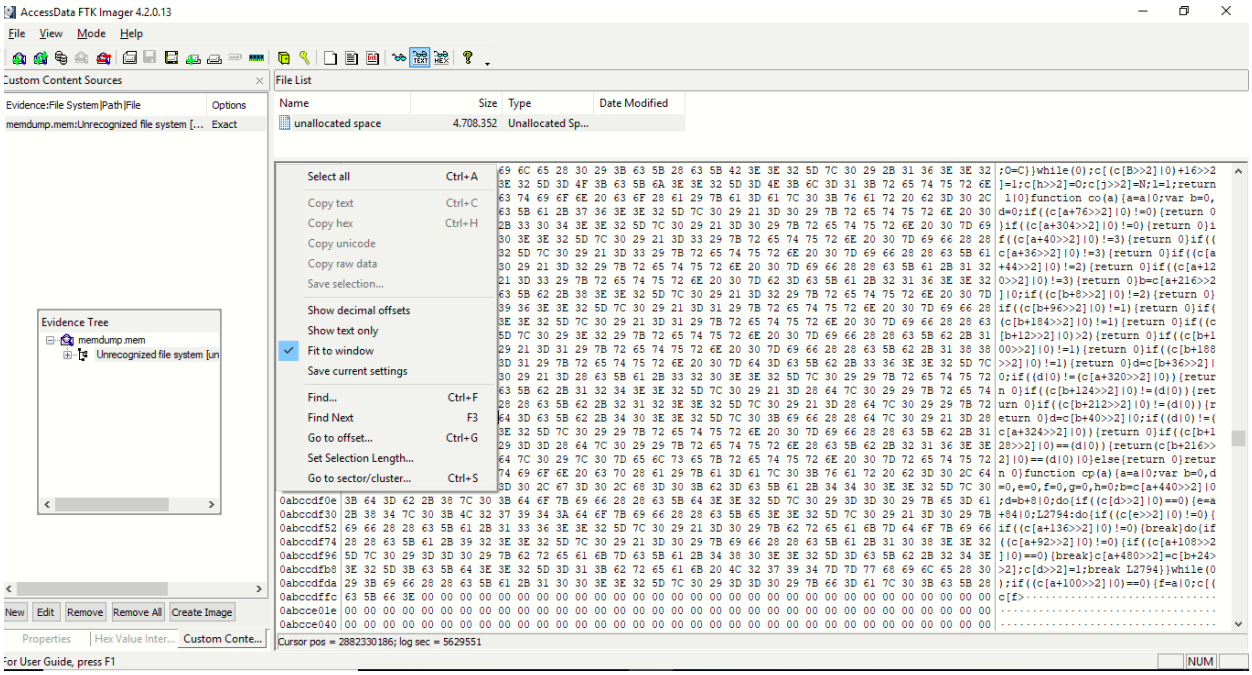


Fonte: FTK Imager.

Uma vez realizado a verificação, basta escolher a opção para a demonstração, texto ou hexadecimal. Há a possibilidade de descobrir se alguma informação possui criptografia com a opção *Detect EFS Encryption*, no caso da imagem criada não possui nenhuma informação criptografada.

O usuário entrou com uma conta na rede social Facebook e realizou uma publicação referente a venda de entorpecentes, com essa informação o perito realizou uma busca com a imagem gerada conforme a figura 15.

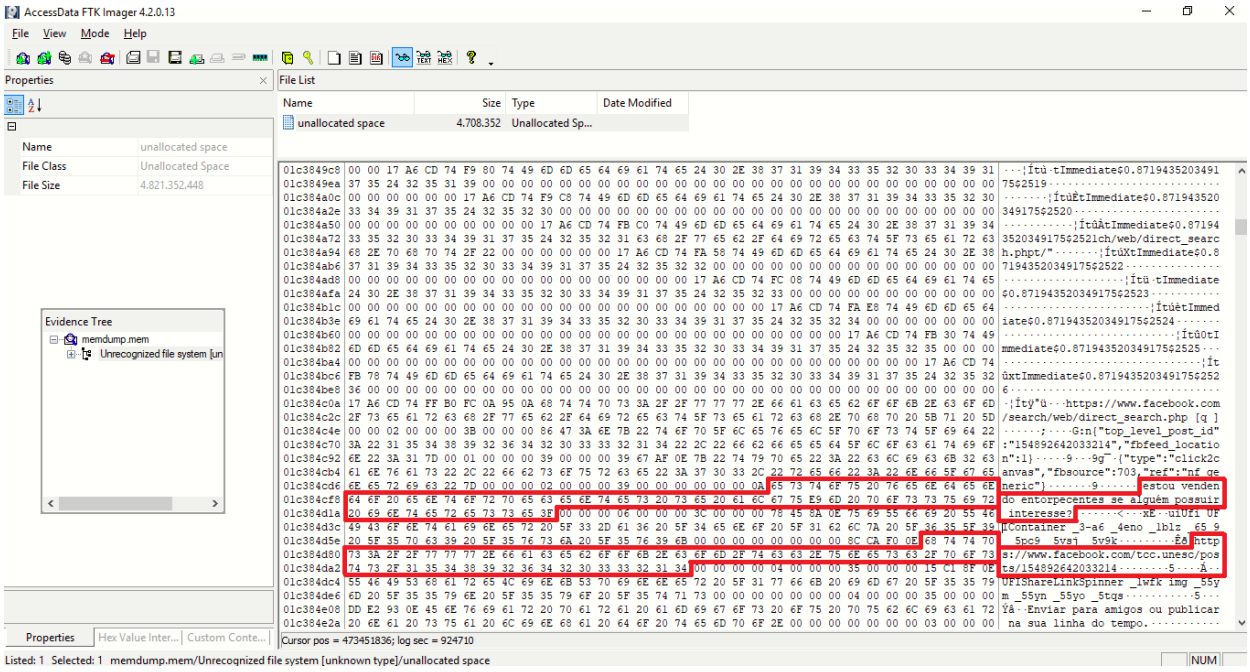
Figura 11 - Busca de Informações



Fonte: FTK Imager.

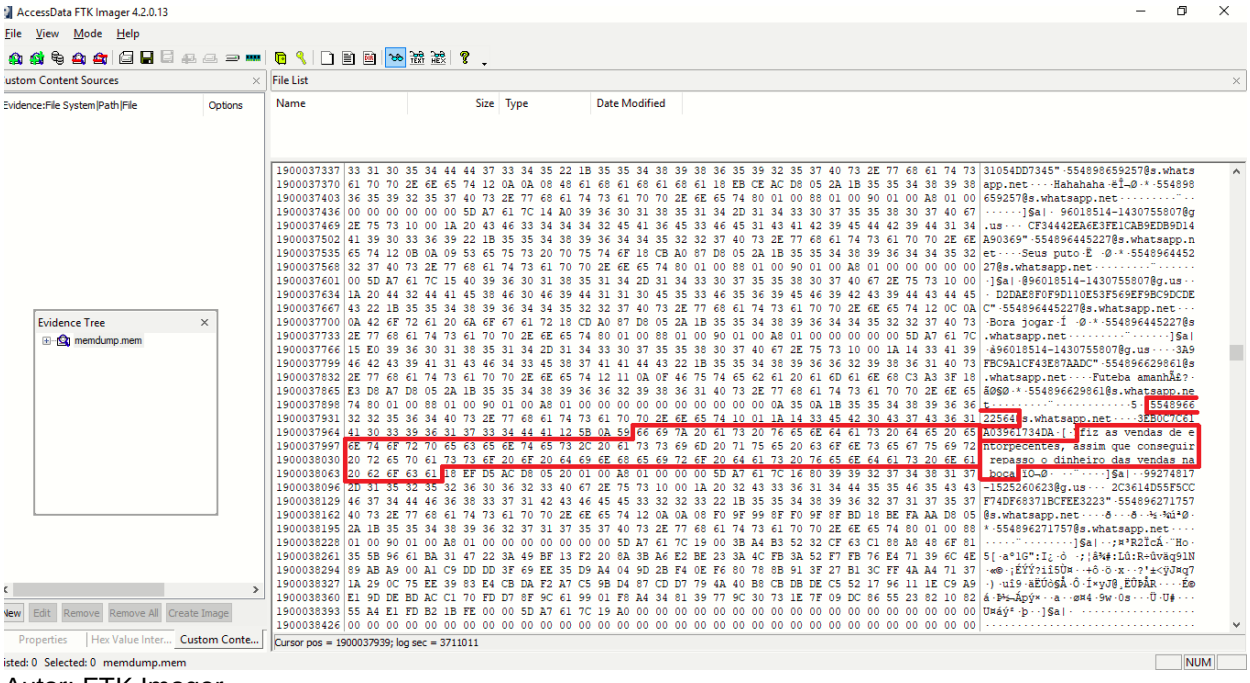
Com a pesquisa realizada pelo perito foi encontrado evidências no Facebook conforme a figura 16, referente a venda de entorpecentes e uma conversa no WhatsApp (figura 17) onde demonstra que o suspeito possui ligação com uma facção criminosa para vendas de materiais ilícitos. Esta pesquisa é realizada por meio da importação de expressões junto ao software, de forma a facilitar a busca de palavras para a investigação.

Figura 12 - Informação encontrada como texto e hexadecimal



Autor: FTK Imager.

Figura 13 - Informação encontrada como texto e hexadecimais WhatsApp



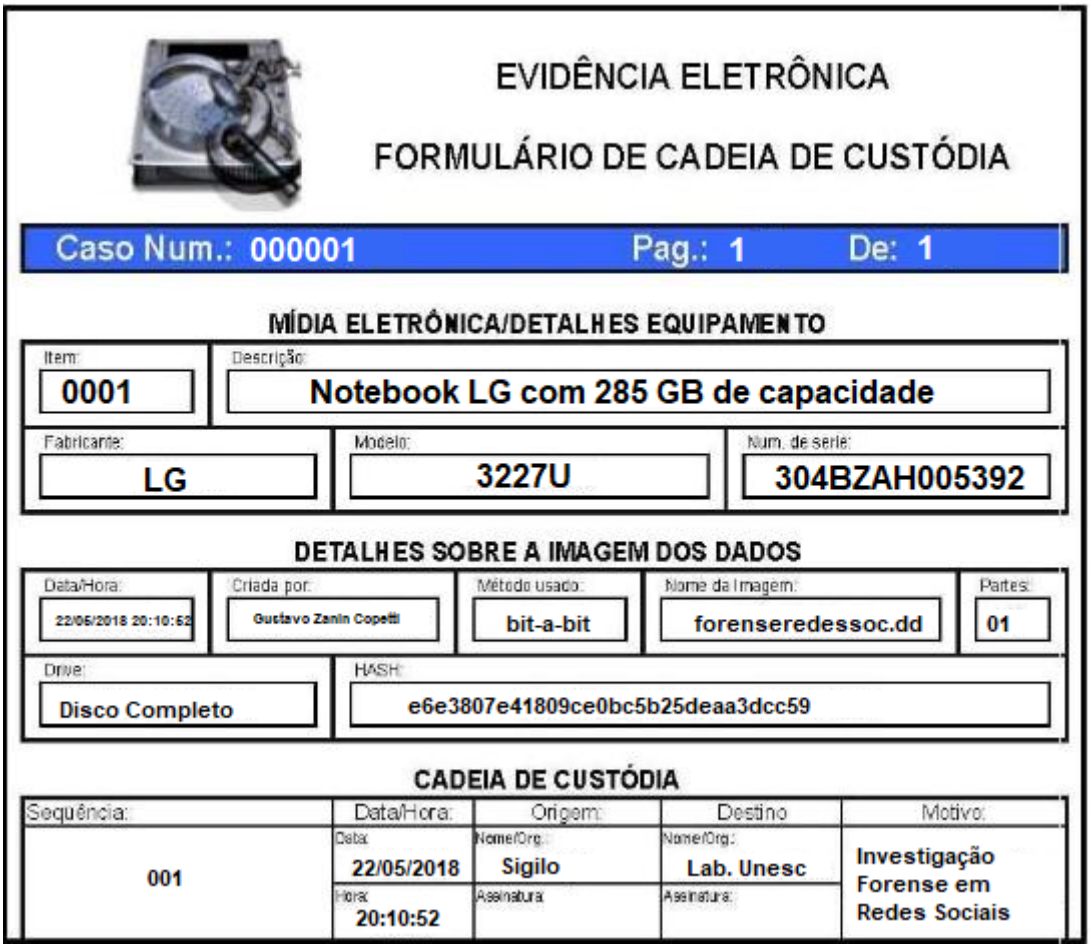
Autor: FTK Imager.

Realizando a busca das informações no WhatsApp, percebe-se como resultado a informação e o número do telefone de destino.

6.2.6 Documentação

Por se tratar de um caso para a apresentar no trabalho proposto não é necessário, juntar essa documentação, uma autorização judicial para coletar evidências. Mesmo assim foi realizado a geração de um formulário com base nas informações coletadas no estudo de caso e nos utensílios utilizados para criar o cenário. Para a geração do arquivo são necessárias algumas informações, como o nome do arquivo *HASH*, nome da imagem, motivo da investigação entre outros.

Figura 14 - Formulário de Evidências Eletrônicas



Fonte: Do Autor.

O processo de perícia forense foi levando em consideração as informações das redes sociais, Facebook e WhatsApp, realizando a validação pelo algoritmo de *hash* md5, onde os valores obtidos ficaram iguais, assim caracterizando que não houve alteração nas imagens. Para todo o processo gerado foi utilizado a metodologia SOP.

6.2.7 Relatório e Revisão

Nesse tópico pode-se encontrar dados que ajudem os profissionais, pesquisadores e comunidade em geral. O estudo de caso baseado nas redes sociais, tanto Facebook quanto WhatsApp, demonstrando os passos para a busca de evidências e informações referente a um crime que ocorreu nas redes citadas. A ferramenta utilizada foi o *AccessData FTK Imager*, software para a criação de imagem e podendo utilizá-lo para análise de evidências, buscando respostas referente ao crime.

No caso investigado foram encontradas evidências de que houve a tentativa de venda de entorpecentes no Facebook e uma conversa onde demonstrou que o usuário entrou em contato pelo WhatsApp para uma entrega, sendo que essas provas podem ser utilizadas para a instauração de um processo contra o usuário e ser aplicada como prova no crime.

6.3 RESULTADOS OBTIDOS

No decorrer da pesquisa, com o estudo de caso realizado foi buscado a solução de um crime digital, levando em consideração a busca de informações na árvore de amigos do perfil analisado, com isso foram alcançados os seguintes objetivos específicos:

a) descrever e aplicar os conceitos sobre redes sociais – descrevendo os conceitos referentes as redes sociais abordadas, buscando um tratamento instrutivo sobre o assunto, sendo realizado com sucesso no capítulo dois;
b) enumerar os métodos para que o usuário possa se proteger no uso de redes sociais – o segundo objetivo alcançado, buscando apresentar as ameaças à segurança nas redes sociais demonstrados no capítulo três;
c) especificar os crimes mais comuns em redes sociais – foi o terceiro objetivo alcançado no capítulo três ponto três, demonstrando os crimes que podem ocorrer nas redes sociais, e compreendendo as leis que são impostas para os determinados crimes;
d) relatar os conceitos de perícia forense em redes sociais – compreendeu-se como buscar os dados das redes sociais, abordando os conceitos de perícia forense em redes sociais para melhor

entendimento acadêmico, reforçando como as redes sociais auxiliam a justiça contra os crimes digitais e com isso instaurado realizado a criação de um estudo de caso para a realização da perícia forense conforme proposto;

e) aplicação de software de perícia forense em redes sociais – foi alcançado o objetivo, realizando a busca da ferramenta que possa atender os requisitos para crimes em redes sociais, buscando auxiliar os peritos na busca de evidências.

Alcançando os objetivos específicos conforme citado acima, julga-se ter um objetivo geral, descrevendo e documentando os métodos, para resgatar evidências de crimes digitais nas redes sociais.

7 CONCLUSÃO

As redes sociais surgiram com o benefício de pessoas se conectarem para manter relações, pessoais ou empresariais, facilitando o compartilhamento e a democratização entre os usuários que utilizam, facilitando o dia-a-dia dos seus usuários possuindo uma ligação social. Porém com um alto crescimento de redes sociais, também cresce as práticas de crimes virtuais com a fragilidade na segurança, mesmo possuindo políticas rigorosas referente a segurança, além disso, a perícia forense vem buscando auxiliar para a busca de evidências dos crimes digitais com ferramentas e mecanismos que auxiliam os mesmos na extração dos dados, assim solucionando crimes e deixando mais simples a perícia forense.

Com o decorrer da pesquisa foram encontradas algumas dificuldades dentre elas a obtenção dos dados das redes sociais, a ferramenta necessária para realizar a obtenção dos crimes em redes sociais que depois de buscar em documentações foi possível solucionar o problema. Com tantos crimes digitais ocorrendo na atualidade, obteve-se dificuldade na escolha do estudo de caso e pela perícia forense em redes sociais ser um assunto considerado novo, tendo grande dificuldade para a busca de provas, se tratando de um trabalho acadêmico, foi realizado uma pesquisa com base em informações criadas diretamente no perfil do usuário, por fim utilizando a metodologia SOP foi possível realizar o processo completo onde o perito visa a busca de evidências do caso.

Concluindo, o trabalho pode contribuir para o desenvolvimento de trabalhos futuros na área de perícia forense em redes sociais contribuindo também como referências bibliográficas. Como ideia para trabalhos futuros, a aplicação da perícia forense buscando informações em celulares com o sistema operacional iOS da Apple.

REFERÊNCIAS

A Prova Nos Crimes Que Se Utilizam Das Redes Sociais. Ufsc: Jorge Luiz Silva da Silva, 26 set. 2016.

A segurança da informação e as redes sociais http://www.tiespecialistas.com.br/2010/11/redes-sociais-e-seguranca-da-informacao-2/. Acesso em 30 Out 2017.

ACIOLI, S. Redes sociais e teoria social: revendo os fundamentos do conceito. Inf & Inf., Londrina: Grafica, 2007.

AGUIAR, S. Redes sociais e tecnologias digitais de informação e comunicação no Brasil (1996-2006). Relatório final de pesquisa. NUPEF Rits. Núcleo de Pesquisas, Estudos e Formação da Rede de Informações para o Terceiro Setor, 2006, 37 p.

ALTHEIDE, C.; CARVEY, H.; DAVIDSON, R. Digital forensics with open source tools: using open source platform tools for performing computer forensics on target systems: Windows, Mac, Linux, Unix, Etc. Elsevier Science, 2011. (Syngress Media). Disponível em: <http://books.google.ca/books?id=J8h8VWUmDuYC>. Acesso em: 10 jan. 2018.

APACHE. Apache Hadoop. Disponível em: <http://hadoop.apache.org/>. Acesso em: 15 abr. 2018.

BARNES, J.A. Social networks. (An Addison Wesley Module in Anthropology) Module 26, 1972, p.1-29.

BBC (Londres) (Org.). #SalaSocial: Internet oculta: os segredos de um universo paralelo. 2014. Disponivel em: http://www.bbc.com/portuguese/noticias/2014/07/140701_internet_oculta_mv.shtml. Acesso em: 19 jul 2018.

BITDEFENDER. Vulnerabilidade do Facebook. Disponível em: <https://www.bitdefender.com.br/news/bitdefender-oferece-insights-%C3%A0-recente-descoberta-de-vulnerabilidade-do-facebook-2095.html>. Acesso em: 01 mar. 2018.

BORBOLO, Rafael. Exploring the software behind Facebook, the world's largest site. Disponível em: <https://royal.pingdom.com/2010/06/18/the-software-behind-facebook/>. Acesso em: 25 mar. 2018.

BREZINSKI, Dominique; KILLALEA, Tom. Guidelines for Evidence Collection and Archiving**.** 2002. Disponível em: <https://www.ietf.org/rfc/rfc3227.txt>. Acesso em: 01 fev. 2002.

Casa Civil. Lei Carolina Diekmann. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 06 mar. 2018.

D. Brezinski and T. Killalea. Rfc 3227: Guidelines for evidence collection and archiving, 2002. Online at www.faqs.org/rfcs/rfc3227.html.

DIGITAL INVESTIGATION: Forensic analysis of WhatsApp Messenger on Android smartphones. Italy: Cosimo Anglano, 15 jan. 2014.

DIMITRI, Fazito. A análise de Redes Sociais (ARS) e a Migração: Mito e realidade.UFMG/Cedeplar.Disponível em: <http://www.abep.nepo.unicamp.br/docs/anais/pdf/2002/GT_MIG_ST1_Fazito_texto.pdf>. Acesso em 08 de setembro de 2017.

DUARTE, Fabio; QUANDT, Carlos. O Tempo das Redes. [s.i.]: Perspectiva, 2008.

FACEBOOK. Company Info. Disponível em: <https://br.newsroom.fb.com/company-info/>. Acesso em: 09 abr. 2018.

Facebook Forensics. Hong-kong: Valkyrie-x Security Research Group, 20 jun. 2011.

Facebook: Do You Leave A Trace? A Forensic Analysis Of Facebook Artifacts. Marshall University, Huntington: Katherine Helenek, Bs, Josh Brunty, Ms, Christopher Vance, Bs, Terry Fenger, 25 jul. 2010.

Facebook Law Enforcement Guidelines, retrieved September 15th, 2011. Online at http://www.eff.org/files/filenode/social_network/Facebook2010_SN_LEG-DOJ.PDF.

FELIX RITCHER. Statista. Facebook Inc. Dominates the Social Media Landscape. Disponível em: <https://www.statista.com/chart/5194/active-users-of-social-networks-and-messaging-services/>. Acesso em: 26 jan. 2018.

FERREIRA, Ivette Senise. A criminalidade informática, in: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). Direito e internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000, p. 207-237.

Forensic Analysis Of Social Networking Application On Mobile Devices. Dubai, Emirados Arabes: Digital Investigation, 10 set. 2012.

FRASER, Barbara Y.. RFC 2196. Disponível em: <https://www.ietf.org/rfc/rfc2196.txt>. Acesso em: 01 mar. 2018.

GARTNER. Big Data. Disponível em: <https://www.gartner.com/it-glossary/big-data>. Acesso em: 09 mar. 2018.

LEMIEUX,VINCENT. MATHIEU OUIMET, Sérgio Pereira. Análise Estrutural das Redes Sociais. Instituto Piaget. out 2017. ISBN 9789727719334.

LOPES, Petter Anderson. Forense Digital: Perícia Forense Computacional. Disponível em: <https://periciacomputacional.com/pericia-forense-computacional-2/>. Acesso em: 11 jun. 2016.

MARTELETO, Regina Maria. Análise de Redes Sociais – aplicações nos estudos de transferência da informação. Ci. Inf., Brasília, v.30, n. 1,p. 71-81, jan/abr. 2001.

MARTINS, G. A; THEÓPHILO, C. R. Metodologia da investigação científica para ciências aplicadas – São Paulo: Atlas, 2009.

MILAGRE, Jose. Análise forense de redes sociais e Facebook. Disponível em: <http://josemilagre.com.br/blog/2014/03/20/analise-forense-de-redes-sociais-e-facebook/>. Acesso em: 25 maio 2018.

MOMBELLI, Elisa. O big data e o policiamento preditivo. Disponível em: <https://jus.com.br/artigos/36752/o-big-data-e-o-policiamento-preditivo>. Acesso em: 18 nov. 2017.

NOGUEIRA, Sandro D'Amato. Crimes de informática. São Paulo: BH, 2008.

NORTON SYMANTEC. Cyber Security. Disponível em: <https://br.norton.com/cyber-security-insights>. Acesso em: 04 maio 2018.

QUEIROZ, Claudemir e VARGAR, Raffael; Investigação e Perícia Foresne Computacional. 1. ed. Rio de Janeiro: Brazport, 2010.

RITCHER, Felix. Facebook Inc. Dominates the Social Media Landscape. 2017. Disponível em: <https://www.statista.com/chart/5194/active-users-of-social-networks-and-messaging-services/>. Acesso em: 10 nov. 2017.

ROSA, Bruno Estevão. Segurança da Informação. Disponível em: <http://www.artigos.com/artigos/8642-seguranca-da-informacao>. Acesso em: 14 dez. 2010.

ROZA, Anderson Figueira da. As redes sociais no mundo do crime. Disponível em: <https://canalcienciascriminais.com.br/as-redes-sociais-no-mundo-do-crime/>. Acesso em: 02 jun. 2018.

SOUZA, Tiago. Diretrizes para coleta e arquivamento de evidências. Disponível em: <https://tiagosouza.com/rfc-3227-em-portugues-diretrizes-para-coleta-e-arquivamento-de-evidencias/>. Acesso em: 23 jan. 2018.

VOLATILITY FOUNDATION (Org.). Volatility**.** Disponível em: <http://www.volatilityfoundation.org/faq>. Acesso em: 01 jun. 2018.

TOMAÉL, M.I. Redes Sociais, conhecimento e inovação localizada. Inf. Inf., Londrina, v.12, n. esp., 2017.

TJMT (Org.). Lei de crimes virtuais já está em vigor. Disponível em: <http://www.tjmt.jus.br/noticias/29323#.Wx-uxkgvzIW>. Acesso em: 05 abr. 2018.

WHATSAPP (Org.). Recursos do WhatsApp. Disponível em: <https://www.whatsapp.com/features/>. Acesso em: 01 jan. 2018.

APÊNDICE(S)

PERÍCIA FORENSE EM REDES SOCIAIS: ANÁLISE DE EVIDÊNCIAS NO FACEBOOK E WHATSAPP

Gustavo Zanin Copetti[1], Paulo João Martins[2]

[1]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC - Brasil

[2]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC - Brasil

copeti_gustavo@hotmail.com, pjm@unesc.net

Abstract. *Social networks have been standing out in the digital era, being applications that act with different levels, such as a means of communication, entertainment and professional, providing practicality for the users. As time goes by, new social networks have been presented, but with challenges to be overcome, such as the acquisition of forensic data and forensic expertise. Crimes in social networks have been increasing significantly, thus arising the need for new techniques to fight these crimes, therefore, aiding forensic expertise. The objective of the research was to approach forensic expertise in social networks, employing a case study to report a method and perform a forensic analysis. In order to accomplish such work, the SOP methodology was applied in 7 steps: authorization, preparation of the equipment, collection and preservation, forensic image, examination and analysis, documentation, report and revision. After the conclusion, we were able to study and apply the concepts of forensic expertise in social networks, using the AccessData FTK Imager tool, succeeding in the analysis of the files.*

Keywords: Social Networks. Forensic Expertise. Safety. Digital Crimes.

Resumo. *As redes sociais vêm se sobressaindo na era digital, aplicativos que atuam com diferentes níveis sendo meio de comunicação, entretenimento e profissional, proporcionando praticidade para os usuários. Com o passar do tempo apresentam-se novas redes sociais, porém com desafios a serem vencidos, tais como a aquisição de dados forenses e a realização da perícia forense. Os crimes em redes sociais vêm aumentando significativamente, desta forma surgindo a necessidade de combater esses crimes, portanto, auxiliando a perícia forense. O objetivo da pesquisa foi abordar perícia forense em redes sociais empregando um estudo de caso para relatar um método e realizar uma análise forense. Para a realização do seguinte trabalho utilizou-se a metodologia SOP aplicada em 7 etapas: autorização,*

preparação do equipamento, coleta e preservação, imagem forense, exame e análise, documentação, relatório e revisão. Com a conclusão, conseguiu-se estudar e aplicar os conceitos de perícia forense em redes sociais, utilizando a ferramenta AccessData FTK Imager, logrando êxito na análise dos arquivos.

Palavras-chaves: Redes Sociais. Perícia Forense. Segurança. Crimes Digitais.

1. Introdução

As redes sociais na atualidade vêm se tornando a forma de comunicação mais eficiente da Internet. Como a comunicação é imediata, altera a cultura social, fazendo as pessoas estruturarem suas vidas reais na rede virtual. Uma das características das redes sociais é a possibilidade de abertura, onde viabiliza relacionamentos horizontais e não hierárquicos, ou seja, facilita a aproximação das pessoas, troca de conteúdos entre outras características que fazem com que elas tenham um crescimento.

Com a melhoria e evolução das redes sociais, bem como os softwares e as pessoas com más intenções, procuram mascarar os crimes. Por outro lado, tem-se a Perícia Forense Digital, que tem contribuído para a análise, interpretação e apresentação de evidências, com o intuito de tentar localizar vestígio dos crimes, utilizando algumas técnicas para tornar a descoberta possível, para os profissionais da área (SOUZA, 2018).

Os Crimes Digitais, conhecidos como Crimes Cibernéticos ou Crimes de Alta Tecnologia, representam as condutas criminosas cometidas com o uso das tecnologias de informação e comunicação, e também os crimes nos quais o objeto da ação criminosa é o próprio sistema informático (CARVALHO, 2013), nas redes sociais também ocorrem essas infrações, e podem ser realizadas em território nacional ou Internacional, neste caso dificultando muito os peritos na descoberta do réu, sendo que é necessário almejar um acordo internacional para buscar favorecer a vítima do furto.

Desta forma, o trabalho realizou o estudo de uma ferramenta forense nas redes sociais, definidos no decorrer da pesquisa, buscando à análise das evidências.

2. Redes Sociais

Embora até hoje não tenha uma teoria referente as redes sociais, Barnes (1972) relata que sua compreensão pode ser diferente para diversas áreas de estudo. Diante desta tolerância, pode-se reconhecer que as redes sociais são constituídas por um vínculo complexo que podem acontecer entre pessoas, grupos ou organizações, os quais buscam interesses, valores ou crenças sem comum (MARTELETO,2001). As redes sociais Segundo Marteleto (2001, p.72), tem a possibilidade de ser descrita como “um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados”. Por sua vez Downes (2005), subjuga que “uma rede social é um conjunto de indivíduos ligados entre si por um conjunto de relações”.

2.1. Facebook

Considerada a maior rede social do mundo na atualidade, o Facebook, foi fundado em 2004, por Mark Zuckerberg, ex-estudante de Harvard nos Estados Unidos. No início o projeto era restrito apenas para os estudantes da Universidade, obteve uma expansão para outras áreas até atingir o grupo secundarista, hoje utilizado por mais de 2 bilhões de usuários ativos por dia. Possuindo vários dados pessoais dos usuários, ferramentas que são utilizadas tanto para localização quanto para armazenagem de fotos e vídeos. Tendo como principal alvo a questão “o que você está pensando?”, fazendo com que os usuários sejam induzidos a compartilhar sua vida pessoal em público, fazendo com que sua vida passe de privada para pública, somente “sua”, visível a todos os usuários por meio de um clique.

2.2. WhatsApp

O WhatsApp foi lançado em 2009 por dois amigos universitários funcionários da empresa Yahoo!, Jon Koum e Brian Acton, onde possuíam um problema pois não era permitido o uso de celulares na universidade, criando então a solução para as ligações perdidas. O nome do aplicativo vem da expressão em inglês *What’s up?* que significa, em tradução livre, E aí? ou Tudo bem?. O aplicativo disponibiliza a troca de mensagens de texto, vídeos, áudios, imagens (WHATSAPP). Todas as possibilidades citadas impulsionam a comunicação entre os indivíduos, depois da instalação o aplicativo utiliza o número de celular para criar uma conta, em seguida ocorrendo a sincronização com a agenda do smartphone.

3. Segurança das Redes Sociais

É chamada de Segurança da Informação, o resguardo sobre as informações de uma pessoa ou empresa. Pressupondo que informação é todo e qualquer conteúdo ou conhecimento que tenha valor para pessoa ou organização, sendo que essa informação pode estar armazenada para uso pessoal ou exposta (BROSTOFF, 2004).
Contudo, pode ser estabelecido regras para a definição do nível de segurança presente, assim estabelecendo critérios para uma posição melhorada ou piorada da circunstância existente. A segurança de uma estabelecida informação pode ser atingida por fontes comportamentais e de aplicação de quem manipula a mesma, pelo ambiente ou infraestrutura que a cerca, ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

3.1. Ameaças à Segurança da Informação

Os riscos referentes a segurança da informação estão associados diretamente ao extravio de suas três características ou atributos essenciais, perda de confidencialidade, perda de integridade e perda de disponibilidade. Em atos de ameaças à rede de computadores ou a um sistema, as ações podem acontecer por agentes maliciosos, muitas vezes conhecidos como *crackers*, (*hackers* não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Os

crackers são instigados a realizar ilegalidades por vários fatores, os principais são: notoriedade, autoestima, vingança e o dinheiro.

3.2. Políticas de Segurança da Informação

De acordo com o RFC 2196 (*The Site Security Handbook*), as políticas de segurança compõem de um aglomerado formal de normas que devem ser empregadas por quem utiliza os patrimônios de uma organização. As mesmas necessitam dispor de práticas realistas, e determinar nitidamente as áreas de responsabilidade dos indivíduos que utilizam, tendo que além de tudo se adaptar com as alterações da organização. Os princípios da segurança oferecem um âmbito para a execução dos mecanismos, apontam processos corretos, processos de auditoria e constituem uma base para metodologias legais na sequência de ataques. O documento que descreve os princípios de segurança deve deixar de fora todas as questões técnicas relacionadas a execução dos mecanismos de defesa, pois essa implementação pode variar ao longo do tempo.

3.3. Crimes Digitais

O antecedente histórico mais remoto do surgimento da informática ocorreu em 1946, quando foi construído o primeiro computador digital, denominado ENIAC (WENDT; JORGE, 2012). De acordo com Paul Zak, professor da Universidade Claremont College, nos Estados Unidos, golpistas preferem usar a Internet para enganar pessoas para evitar o contato pessoal com elas. "É mais fácil prejudicar alguém quando não está olhando para esta pessoa", disse o professor. Segundo ele, pesquisas em neurociência mostram que violações morais são menos comuns em interações pessoais porque se cria uma empatia maior com quem se vê ao vivo.

3.4. Leis para Crimes Digitais

Em abril de 2012 entra vigor a Lei 12.737/2012, que modificou o Código Penal e determinou o futuro para os crimes cibernéticos no Brasil. Quem invadir dispositivo informático alheio (computadores, tablets, notebooks, celulares, entre outros), conectados ou não à Internet, desenvolver programas para roubar dados ou divulgar e comercializar as informações obtidas de forma ilícita, a pessoa pode ser punida com multa ou poderá até ir para a prisão. O grande problema da prova no meio informático é que ela é muito volátil. A investigação é mais complexa, porque envolve um caminho longo. É preciso preservar a prova para que ela se torne idônea. Para isso é necessário obter o endereço IP, que é a identidade virtual.

4. Hadoop

Criado em 2005 pela empresa Yahoo o Hadoop é considerado uma das mais significativas invenções de big data, projeto adquirido pela Apache está sendo utilizado por muitas empresas para analisar informações com grande quantidade

de dados não estruturados, ou seja, elementos de difícil acesso que não podem ser organizados e dificilmente recuperados. O Hadoop conforme o site oficial da Apache é uma estrutura que permite o processamento distribuído de grandes conjuntos de dados em clusters de computadores usando modelos de programação simples, sendo um software de código aberto do paradigma de programação Map-Reduce.

4.1. Como Utilizar o Hadoop

Para utilizar o Hadoop pode ser recorrido a alguns centros de distribuição, como por exemplo a Empresa Cloudera Hadoop, onde a mesma possui suporte para várias distribuições Linux, ideal para iniciantes na plataforma, levando em consideração que a máquina já possua a tecnologia Java e cURL instalado. As recomendações são para utilizar o Ubuntu para realizar a instalação pois a utilização do APT facilita muito e permite usar o pacote binário sem detalhes de realizar o download e geração de origens.
O próximo passo é informar o APT da distribuição, sendo que dependendo do release utilizado pode alterar o código para a geração do Hadoop, e em seguida gerar um arquivo.

4.2. Integração do Hadoop com Pericia Forense em Redes Sociais

O Hadoop na perícia forense em redes sociais é um projeto que vem sendo desenvolvido ao passar dos anos que irá permitir o processamento de uma grande quantidade de dados, TSK é uma biblioteca e uma coleção de instrumentos de comando que permite a investigação de imagens de disco, tendo como principal recurso a análise de volume e dados do sistema de arquivos podendo ser implementada diretamente para encontrar evidências na perícia forense digital (MILAGRE, 2014).

5. Perícia Forense nas Redes Sociais

A pesquisa forense digital vem sendo destaque, pelo fato de crimes serem cada vez mais evidenciados na mídia, sendo que os mesmos ocorrem unicamente ou com auxílio de computadores. Vestígios deixados auxiliam tribunais e agências que executam as leis para a apreensão de provas para as investigações (LUIS, 2015). Com o número elevado de pessoas compartilhando e se comunicando, a perícia se torna muito importante para a busca de informações nas redes sociais e em nuvem. A investigação forense digital em muitos casos tem de confiar em um aglomerado limitado de informações, em qualquer caso, o investigador pode enviar solicitações ao operador e pode ou não receber todos os dados relevantes (por exemplo, escrito na aplicação da lei do Facebook diretrizes publicadas pelo EFF) (FACEBOOKINC, 2010).

5.1. Volatility

O framework foi lançado em 2007 sendo que a primeira versão foi chamada de The Volatility, publicamente lançado na Black Hat DC. Constituído

principalmente com base de vários anos de pesquisas acadêmicas que foram publicadas em análises avançadas de memória forense. Antes do lançamento do framework as investigações digitais eram ligadas ao tráfico de imagens armazenadas em discos rígidos. A volatilidade introduziu as pessoas no poder de analisar o estado de tempo de execução de um sistema usando os dados encontrados no armazenamento volátil (RAM) (VOLATILITY, 2014).

5.2. Aquisição de Dados

Antes de poder analisar os dados das redes sociais, os dados devem ser reunidos e adquirido, embora os métodos forenses tradicionais possam ser usados para extrair artefatos do *cache* do *webbrowser* local, são possíveis inúmeras outras formas na camada de comunicação (ALTHEIDE; CARVEY; DAVIDSON, 2011). Estes variam desde o ataque passivo na rede para ativos como *sniffing Wi-Fis* não criptografado ou em combinação com *spoofing* ARP em *LANs*. O rastreamento, no entanto, é limitado, pois metadados e *timestamps* precisos não são mostrados em páginas da *web*. Eles só estão disponíveis usando a rede social APIs, que estendem os dados disponíveis da *interface web*.

5.3. Pool de Dados de Rede Social

Embora as redes sociais variem em características e arquitetura, foi identificado as seguintes fontes genéricas de dados que interessam em exames forenses em questões sociais como o rastro social, padrão de comunicação, imagens e vídeos, tempos de atividade e os aplicativos (BONNEAU, 2009). Toda essa informação não pode ser encontrada no disco rígido de um suspeito, como é exclusivamente armazenado no operador. Especialmente para pessoas que usam a rede social em uma base diária, uma infinidade de informações é armazenada no operador.

5.4. Como Utilizar a Perícia Forense em Redes Sociais

Conforme os dados apontam o Facebook possui mais de 2 bilhões de usuários ativos, as informações postadas na rede social são muito importantes para a investigação forense. O compartilhamento de informações do seu dia a dia é uma forma de conseguir alguma pista sobre os suspeitos de algum crime em investigação. Conforme Farmer (2007), “a análise forense de um sistema envolve um ciclo de coleta de dados e processamento das informações coletadas”.

5.5. Redes Sociais a Serviço da Justiça

Nas redes sociais não ocorrem somente crimes cibernéticos, crimes como pedofilia, abuso sexual, sequestro, roubo, estelionato, homicídio e outros diversos também podem deixar vestígios, sendo que o criminoso pode fazer uso da rede social como meio ou apoio para praticar o ato ilegal (NOGUEIRA, 2009). De acordo com Nogueira (2009, p. 42), “a internet está sendo usada há vários anos pelos terroristas do mundo todo, devido a sua rapidez na propagação de

mensagens e alcance de milhões de pessoas rapidamente". Sendo assim, seja qual for a investigação pode ser realizada uma análise forense para a descoberta de vestígios e tentativa de desvendar crimes, além de que nos dias atuais as redes sociais possuem ainda mais pessoas compartilhando informações, estando mais conectadas.

6. Método, Procedimento e Ferramenta Utilizada para Perícia Forense em Redes Sociais

Segundo o Perito Judicial e Assistente Técnico em Informática, Marketing, Propriedade Intelectual e Crimes Informáticos José Milagre quando se trata em pericia forense em redes sociais tem de haver a distinção de duas áreas, uma utilizando uma grande coleta de dados e a outra a utilização de data mining em sua aplicação, sendo áreas incipientes e parando em questões de privacidade. O trabalho proposto aborda sobre pericia forense em redes sociais especificando o WhatsApp e o Facebook, considerada por peritos uma área científica recente, buscando realizar a integração da perícia forense com as redes sociais, em seguida realizando um estudo de caso onde teve a aplicação de um método, técnica e ferramenta para a busca e coleta de informações para a resolução de um suposto crime que ocorreu tanto no Facebook quanto no WhatsApp. Neste estudo foi realizado a criação de uma imagem forense e em seguida a busca das evidências de um crime nas redes sociais, com o objetivo de cooperar com a comunidade científica, com a elaboração de um trabalho possuindo diversas informações na perícia forense em redes sociais, com apoio nas metodologias e recursos buscando evidências.

6.1. Estudo de Caso

No presente caso um usuário no Facebook realiza postagens com apologia as drogas dando a entender que o mesmo possui ligação com o tráfico de drogas, realizando vendas e compras de entorpecentes via redes sociais, podendo apresentar provas pelo Facebook ou até mesmo possuindo conversas com outros integrantes no aplicativo do WhatsApp, sendo que para isso os responsáveis pelo caso entraram em contato com um perito Forense para encontrar evidências que levem a confirmação da suspeita.

6.2. Metodologia

Quando é realizada a analise referente a perícia forense, dependendo do caso levasse em consideração diferentes formas de analise, para a análise do caso apresentado foi utilizado a metodologia SOP, sendo a mais utilizada no Brasil e apresentada pela *International Hi-Tech Crime and Forensics Conference* (IHCFC), como padrão internacional desde 1999. A metodologia utilizada possui várias etapas conforme a figura 5, sendo elas, Autorização, Preparação do Equipamento, Coleta e Preservação, Imagem Forense, Exame e Analise, Documentação, Relatório e Revisão.

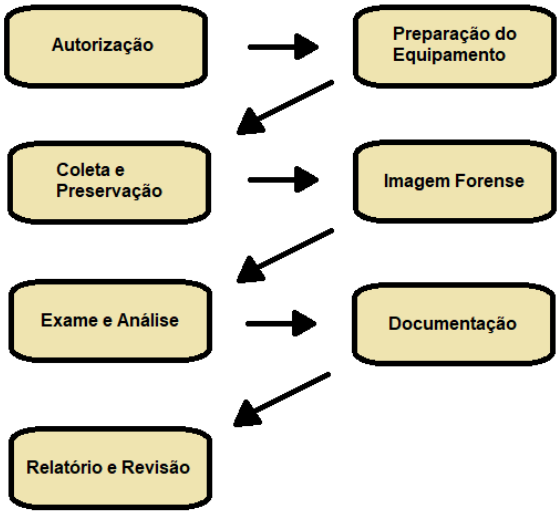


Figura 15 - Metodologia SOP

6.2.1. Autorização

Com o desenvolvimento do trabalho para fins acadêmicos não foi necessário a realização da prática de autorização, que consiste na busca das informações da rede social para que o perito realize a busca das evidências, porém foi utilizado o restante das etapas conforme consta na metodologia SOP.

6.2.2. Preparação do Equipamento

Para que o perito realize uma análise com completas condições é necessário que o mesmo possua equipamentos que condizem com as ferramentas e softwares utilizados no processo, possuindo então os pré-requisitos para que seja realizada a investigação forense computacional em redes sociais.

6.2.3. Coleta e Preservação

A coleta é entendida como a apreensão de informações físicas e lógicas, sendo que deve ser de forma cuidadosa por se tratar de dispositivos frágeis como computadores (RODRIGUES, 2017). Depois de realizar a coleta, vem a necessidade de transporte do material, sendo meios eletrônicos se tornam sensíveis, exigindo do perito um maior cuidado para não danificar nenhum meio de prova (RODRIGUES,2017). Sendo realizada, a perícia em redes sociais, muitas vezes se encontra o desafio de como acessá-las, e para acessar os dados de usuário no Facebook, por exemplo, é necessário seguir uma série de regras pré estabelecidas pela equipe do Facebook, descrito no documento “Requisito Legal de Processo Internacional”, para fins acadêmicos foi realizado um novo cadastro, porém para a busca das informações antigas o Facebook disponibilizou uma função onde é requerido os dados. Já no caso do WhatsApp a ferramenta possui uma função parecida com o Facebook, onde o usuário pode realizar o download do backup das conversas, porem sendo necessário que o proprietário realize um backup para futuramente usufruir do mesmo.

6.2.4. Imagem Forense

Para a realização da análise forense das redes sociais, foi utilizado o software para a criação *AcessData Forense Toolkit Imager*, o mesmo possui a opção para a criação de uma imagem e captura de memória para que seja analisado. Ao fim do processo de geração da imagem, foi constituído um arquivo *Hash* com o algoritmo Md5 e Sha1 e em seguida transferido para a máquina onde houve a análise forense no Facebook e no WhatsApp com o mesmo arquivo. Na sequência da criação da imagem forense, é apresentado o sumário onde demonstra as informações do arquivo criado. Seguindo a análise foi realizado, a criação de um arquivo *hash*, onde busca armazenar a informação para uma possível verificação em alterações nas evidências.

6.2.5. Exame e Análise

Para realizar o exame e a análise, para que não ocorra a perda das informações é necessário realizar uma cópia dos dados, para não ocorrer o extravio ou alteração da imagem. Depois desta ser realizada, foi adicionado a imagem na ferramenta FTK Imager onde é possível visualizar as informações, conversas e imagens para a análise.

Depois de adicionar a imagem, basta realizar as configurações do software, escolhendo se vai ser realizado a evidências, física, logica, imagem ou alguma pasta disponível. Com a imagem importada, existem duas formas que demonstram as informações, uma coluna em hexadecimal e outra o mesmo texto corrente. Nesse caso busca-se informações para solucionar um crime utilizando a opção de busca nos textos.

Anterior a isto, é necessário verificar a possibilidade de alguma alteração no arquivo, pelo comando *Verify Drive/Image,* no fim do processo apresentando se houve alteração de blocos. Uma vez realizado a verificação, basta escolher a opção para a demonstração, texto ou hexadecimal. Com a pesquisa realizada pelo perito foi encontrado evidências no Facebook conforme a figura 2, referente a venda de entorpecentes e uma conversa no WhatsApp (figura 3) onde demonstra que o suspeito possui ligação com uma facção criminosa para vendas de materiais ilícitos.

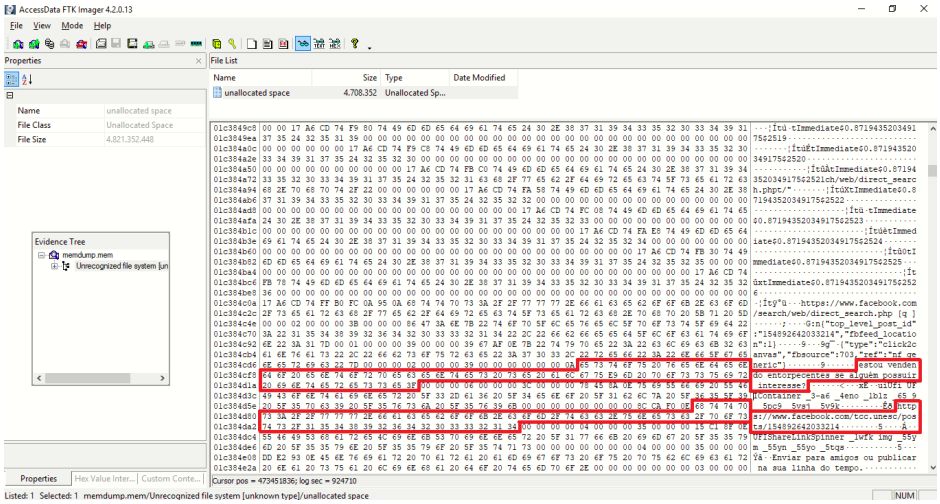


Figura 16 – Resultado Forense Facebook

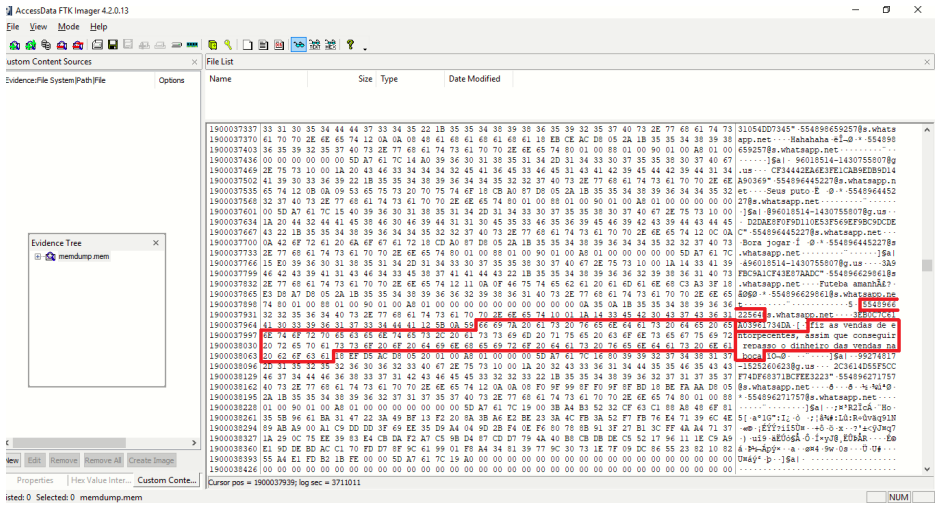


Figura 17 - Resultado Forense WhatsApp

6.2.6. Documentação

Por se tratar de um caso para a apresentar no trabalho proposto não é necessário, juntar essa documentação, uma autorização judicial para coletar evidências. Mesmo assim foi realizado a geração de um formulário com base nas informações coletadas no estudo de caso e nos utensílios utilizados para criar o cenário. Para a geração do arquivo são necessárias algumas informações, como o nome do arquivo *HASH*, nome da imagem, motivo da investigação entre outros.

6.2.7. Relatório e Revisão

O estudo de caso baseado nas redes sociais, tanto Facebook quanto WhatsApp, demonstrando os passos para a busca de evidências e informações referente a um crime que ocorreu nas redes citadas. A ferramenta utilizada foi o *AccessData FTK Imager*, software para a criação de imagem e podendo utiliza-lo para análise de evidências, buscando respostas referente ao crime.

No caso investigado foram encontradas evidências de que houve a tentativa de venda de entorpecentes no Facebook e uma conversa onde demonstrou que o usuário entrou em contato pelo WhatsApp para uma entrega, sendo que essas provas podem ser utilizadas para a instauração de um processo contra o usuário e ser aplicada como prova no crime.

7. Conclusão

O presente artigo buscou apresentar um método, procedimento e ferramenta para retornar evidências sobre um crime realizado em redes sociais, por meio da perícia forense. A pesquisa desenvolvida possibilitou dar uma resposta ao caso, com o decorrer da pesquisa foram encontradas algumas dificuldades dentre elas a obtenção dos dados das redes sociais, a ferramenta necessária para realizar a obtenção dos crimes em redes sociais que depois de buscar em documentações foi possível solucionar o problema. Com tantos crimes digitais ocorrendo na atualidade obteve-se dificuldade na escolha do estudo de caso e pela perícia forense em redes sociais ser um assunto considerado novo, tendo grande dificuldade para a busca de provas, se tratando de um trabalho acadêmico, foi realizado uma pesquisa com base em informações criadas diretamente no perfil do usuário, por fim utilizando a metodologia SOP foi possível realizar o processo completo onde o perito visa a busca de evidencias do caso.
Concluindo, este trabalho apresenta oportunidade para trabalhos futuros em perícia forense em redes sociais, tais como: estudo de outros métodos na área, a utilização da mesma metodologia em outras redes sociais.

8. Referências

ALTHEIDE, C.; CARVEY, H.; DAVIDSON, R. Digital forensics with open source tools: using open source platform tools for performing computer forensics on target systems: Windows, Mac, Linux, Unix, Etc. Elsevier Science, 2011. (Syngress Media). Disponível em: <http://books.google.ca/books?id=J8h8VWUmDuYC>. Acesso em: 10 jan. 2018.

BARNES, J.A. Social networks. (An Addison Wesley Module in Anthropology) Module 26, 1972, p.1-29.

CARVALHO, João. As redes sociais no mundo do crime. Disponível em: <https://canalcienciascriminais.com.br/as-redes-sociais-no-mundo-do-crime/>. Acesso em: 02 jun. 2018.

FRASER, Barbara Y.. RFC 2196. Disponível em: <https://www.ietf.org/rfc/rfc2196.txt>. Acesso em: 01 mar. 2018.

MARTELETO, Regina Maria. Análise de Redes Sociais – aplicações nos estudos de transferência da informação. Ci. Inf., Brasília, v.30, n. 1,p. 71-81, jan/abr. 2001.

MILAGRE, Jose. Análise forense de redes sociais e Facebook. Disponível em: <http://josemilagre.com.br/blog/2014/03/20/analise-forense-de-redes-sociais-e-facebook/>. Acesso em: 25 maio 2018.

NOGUEIRA, Sandro D'Amato. Crimes de informática. São Paulo: BH, 2008.

SOUZA, Tiago. Diretrizes para coleta e arquivamento de evidências. Disponível em: <https://tiagosouza.com/rfc-3227-em-portugues-diretrizes-para-coleta-e-arquivamento-de-evidencias/>. Acesso em: 23 jan. 2018.

VOLATILITY FOUNDATION (Org.). Volatility. Disponível em: <http://www.volatilityfoundation.org/faq>. Acesso em: 01 jun. 2018.

WHATSAPP (Org.). Recursos do WhatsApp. Disponível em: <https://www.whatsapp.com/features/>. Acesso em: 01 jan. 2018.