CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
Recredenciado pela Portaria Ministerial nº 1.162, de 13/10/16, D.O.U nº 198, de 14/10/2016
ASSOCIAÇÃO EDUCACIONAL LUTERANA DO BRASIL

Dennis Dyodi Kawakami

COMPARATIVO ENTRE FERRAMENTAS DE EXTRAÇÃO DE DADOS DO WHATSAPP EM SISTEMAS ANDROID PARA INVESTIGAÇÃO FORENSE

Palmas – TO

2018

Dennis Dyodi Kawakami

COMPARATIVO ENTRE FERRAMENTAS DE EXTRAÇÃO DE DADOS DO WHATSAPP EM SISTEMAS ANDROID PARA INVESTIGAÇÃO FORENSE

Trabalho de Conclusão de Curso (TCC) II elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Ciência da Computação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. M.e Madianita Bogo Marioti.

Palmas – TO
2018

Dennis Dyodi Kawakami

COMPARATIVO ENTRE FERRAMENTAS DE EXTRAÇÃO DE DADOS DO WHATSAPP EM SISTEMAS ANDROID PARA INVESTIGAÇÃO FORENSE

Trabalho de Conclusão de Curso (TCC) II elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Ciência da Computação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. M.e Madianita Bogo Marioti.

Aprovado em: _____/_____/_____

BANCA EXAMINADORA

_____

Prof. M.e Madianita Bogo Marioti

Orientador

Centro Universitário Luterano de Palmas – CEULP

_____

Prof. M.e Fabiano Fagundes

Centro Universitário Luterano de Palmas – CEULP

_____

Prof. Heloise Acco Tives Leão

Centro Universitário Luterano de Palmas – CEULP

Palmas – TO

2018

RESUMO

KAWAKAMI, Dennis Dyodi. **Comparativo entre ferramentas de extração de dados do WhatsApp em sistemas Android para investigação forense**. 2018. 51 f. Trabalho de Conclusão de Curso (Graduação) – Curso de Ciência da Computação, Centro Universitário Luterano de Palmas, Palmas/TO, 2018.

A Computação Forense é uma área da Ciência Forense cujo objetivo é realizar investigações de crimes cometidos com a utilização de equipamentos computacionais, podendo ser microcomputadores, celulares ou quaisquer outros dispositivos que armazenem informações. Os principais exames forenses em informática que são realizados atualmente são os exames em locais de crime, exames em dispositivos de armazenamento computacional, exames em aparelhos de telefone celular e exames em *sites* da *Internet*. O *WhatsApp* é um aplicativo de Mensagens Instantâneas que armazena grandes quantidades de informações no *Smartphone* em que estiver instalado, podendo ser mensagens de mídias (áudios, imagens, vídeos) ou de textos, tornando-se assim um objeto de estudo da Computação Forense, devido a possibilidade de seus dados serem utilizados como evidências de crimes. Para o auxílio da perícia sob o aplicativo, existem várias ferramentas no mercado, podendo ser gratuitas ou proprietárias, que capturam as informações do *WhatsApp*. Neste contexto, o presente trabalho teve por objetivo comparar ferramentas de extração de dados de *Smartphones*, que consigam extrair os dados do aplicativo *WhatsApp* em sistemas *Android*, visando buscar informações que auxiliem uma investigação forense. O desenvolvimento deste trabalho está organizado em seis etapas, sendo elas: reuniões com especialista do domínio com objetivo de compreender o contexto do projeto e o problema a ser solucionado; revisão de literatura tendo como propósito buscar obras publicadas sobre Perícia Forense Computacional, documentos que esclarecessem sobre a perícia no *WhatsApp* e ferramentas utilizadas para captura de dados do aplicativo; definição de ferramentas de extração de dados do *WhatsApp* na qual foram definidas quais das ferramentas encontradas na fase anterior poderiam ser utilizadas no projeto*;* definição dos critérios de comparação entre as ferramentas, onde foram avaliados parâmetros utilizados por outros autores para elaboração dos critérios; utilização de ferramentas de extração de dados do *WhatsApp* definidas na terceira etapa para realizar a extração dos dados do *WhatsApp* e elaboração de um paralelo entre as ferramentas baseando-se nas características e nas informações extraídas por cada uma delas.

Palavras-chave: WhatsApp. Computação Forense. Extração de Dados.

LISTA DE FIGURAS

Figura 1: Etapas da Perícia Forense 15
Figura 2: Estrutura de armazenamento dos arquivos wa.db e msgstore.db 18
Figura 3: Passos para extração de dados utilizando ferramentas forenses 20
Figura 4: Metodologia 22
Figura 5: Softwares para extração de dados do WhatsApp 24
Figura 6: Tela inicial da ferramenta Elcomsoft eXplorer for WhatsApp 28
Figura 7: Extração das mensagens do WhatsApp 29
Figura 8: Lista de contatos do WhatsApp 30
Figura 9: Extração dos arquivos de mídias do WhatsApp 31
Figura 10: Extração de ligações no WhatsApp 32
Figura 11: Tela inicial da ferramenta Andriller 33
Figura 12: Menu de funcionalidade da ferramenta 34
Figura 13: Mensagens extraídas pela ferramenta 35
Figura 14: Mensagens de mídias 35
Figura 15: Contatos 36
Figura 16: Extração das chamadas 37
Figura 17: Extração do banco de dados do WhatsApp com WhatsApp Key Extractor 38
Figura 18:Arquivos extraídos utilizando o WhatsApp Key Extractor 39
Figura 19: Tela inicial da ferramenta WhatsApp Viewer 39
Figura 20: Lista de contatos e mensagens 40
Figura 21: Imagens recuperadas pela ferramenta 41

LISTA DE TABELAS

Tabela 1: Diretório do WhatsApp em SO Android 18
Tabela 2: Apresentação dos critérios de comparação entre as ferramentas 25
Tabela 3: Tabela comparativa entre as ferramentas preenchida 41
Tabela 4: Pontos fortes e fracos das ferramentas utilizadas 43

LISTA DE ABREVIATURAS E SIGLAS

CD – Compact Disc

CD - RW – Compact Disc ReWritable

CPP – Código de Processo Penal

DB – Data Base

DoS – Denial of Service

DVD – Digital Video Disc

DVD - RW – Digital Video Disc ReWritable

HD – Hard Disc

IM – Instant Messenger

NCFS – National Commission Foresensic Science

SO – Sistema Operacional

SMS – Shot Message Service

TCC – Trabalho de Conclusão de Curso

USB – Universal Serial Bus

SUMÁRIO

1 INTRODUÇÃO 8

2 REFERENCIAL TEÓRICO 11

2.1 COMPUTAÇÃO FORENSE 11

2.1.1 Crimes cometidos com o uso de equipamentos computacionais 12

2.1.2 Principais exames forenses em informática 13

2.1.3 Etapas da perícia forense 14

2.2 PERÍCIA FORENSE NO WHATSAPP 16

2.2.1 Arquivos e diretórios do Android 17

2.2.2 Passos para extração de dados utilizando ferramentas forenses 20

3 MATERIAIS E MÉTODOS 22

3.1 DESENHO DE ESTUDO 22

3.2 MATERIAL 23

3.2.1 Hardware 23

3.2.2 Software 23

3.3 DEFINIÇÃO DOS CRITÉRIOS DE COMPARAÇÃO 25

4 RESULTADOS E DISCUSSÃO 27

4.1 ELCOMSOFT 27

4.2 ANDRILLER 33

4.3 WHATSAPP KEY EXTRACTOR 37

4.4 COMPARAÇÃO ENTRE AS FERRAMENTAS 41

5 CONSIDERAÇÕES FINAIS 45

REFERÊNCIAS 46

ANEXOS 48

1 INTRODUÇÃO

Nos últimos anos os *Smartphones* passaram por uma grande evolução tecnológica, permitindo que os usuários se comuniquem através de mensagem de texto, envio de imagens, áudios, vídeos e documentos diversos. Esses serviços, conhecidos como mensagens instantâneas (*Instant Messaging* - IM), são um dos meios mais utilizados entre as pessoas para a comunicação, visto que, o envio e o recebimento das mensagens podem ser realizados para múltiplos participantes ao mesmo tempo e acontece em tempo real (ROSLER, MAINKA e SCHWENK, 2017, tradução). Uma ferramenta popular que oferece serviço de IM é o *WhatsApp*, um aplicativo muito utilizado atualmente.

De acordo com os dados fornecidos pelo site oficial do *WhatsApp* com acesso em outubro de 2017, o *WhatsApp* é um aplicativo de troca de mensagens gratuito que permite envios e recebimentos de multimídias (fotos, vídeos, áudios e documentos) e a realização de chamadas de voz. Segundo Thakur (2013, tradução), a maioria dos arquivos enviados e/ou recebidos pelo aplicativo ficam armazenados na memória interna e/ou na memória *flash* do dispositivo em que o utilitário estiver instalado.

O *WhatsApp* é um aplicativo que pode ser utilizado como ferramenta para prática de crimes eletrônicos devido a facilidade de compartilhar conteúdos de natureza ameaçadora, difamatória, ofensiva, matérias de intolerância e pedofilia. Além dos conteúdos citados, também contribui com outros tipos de delitos como, por exemplo, o tráfico de drogas, que pode ser realizado através das trocas de mensagens entre os usuários. Dessa forma, o *WhatsApp* torna-se uma fonte muito rica de informações e evidências de práticas criminosas, dessa forma é uma área de estudos para a análise forense.

Para realizar o esclarecimento de crimes existe um campo de estudo denominado Ciência Forense, que, segundo a Comissão Nacional de Ciências Forenses (*National Commission on Forensic Science* - NCFS), é a "aplicação de práticas científicas ou técnicas para reconhecimento, coleta, análise e interpretação de evidências de direito penal e civil ou questões regulatórias" (NATIONAL COMMISSION ON FORENSIC SCIENCE, 2016, tradução). Existem algumas áreas que são relacionadas a Ciência Forense como a antropologia, biologia, computação, matemática, psicologia, química entre outras, que buscam comprovar o modo em que um crime foi cometido por meio de metodologias específicas de cada área de atuação. A Computação Forense, especificamente, tem como principal objetivo determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de Informática (ELEUTÉRIO e MACHADO, 2011).

A Perícia Forense computacional pode usar os dados do *WhatsApp* para buscar evidências de crimes, devido à grande quantidade de informações armazenadas no aplicativo. Para o auxílio do perito na investigação, existem várias ferramentas forenses que permitem realizar a perícia em dispositivos móveis, tendo como objetivo a extração dos dados dos *Smartphone*s. Conhecer quais são essas ferramentas, o seu funcionamento e as potencialidades delas é importante, pois cada uma possui uma forma distinta de utilização, podendo ser executadas em diversos SOs (Windows, Linux, mac OS) e apresentar diferentes tipos de informações. Realizar o estudo das ferramentas permite esclarecer as funcionalidades e quais tipos de informações são retornadas por elas, tornando-o muito útil para auxiliar nas investigações forenses sobre o *WhatsApp*.

O objetivo geral deste trabalho é comparar ferramentas de extração de dados do aplicativo *WhatsApp* em Sistemas *Android*, visando buscar informações que auxiliem uma investigação Forense. Além disto, tem-se os objetivos específicos, os quais apresentam os propósitos de forma mais precisa, que são:

- apresentar conceitos relacionados à Computação Forense, enfocando a Perícia Forense sobre dados extraídos do *WhatsApp*;
- descrever o armazenamento das informações do *WhatsApp* em Sistemas *Android*;
- descrever as funcionalidades de três ferramentas de extração de dados de dispositivos móveis;
- apresentar os dados do *WhatsApp* extraídos pelas ferramentas;
- comparar os resultados obtidos pelas ferramentas.

O presente trabalho visa esclarecer o seguinte problema de pesquisa: é possível obter informações de ferramentas de extração de dados do *WhatsApp* que auxiliem na resolução de crimes? Para responder o problema de pesquisa proposto foi levantada a hipótese de que os dados capturados do *WhatsApp* pelas ferramentas podem apresentar várias informações como: imagens comprometedoras, data de ações ilícitas, conversas sobre atos ilícitos, nomes de envolvidos em crimes, entre outros que podem auxiliar na resolução de crimes. A partir dos estudos e resultados obtidos pelas ferramentas, a hipótese proposta foi validada, conseguindo apresentar diversas informações do aplicativo.

Neste contexto, o presente trabalho apresenta conceitos relacionados à Computação Forense possibilitando uma melhor compreensão sobre a área, apresenta como o Sistema Operacional (SO) *Android* armazena as informações do *WhatsApp* nos *Smartphones*, descreve as funcionalidades das ferramentas Andriller, Elcomsoft e *WhatsApp Key Extractor*, que

foram utilizadas para extração de dados de dispositivos móveis, apresenta os dados do *WhatsApp* que foram extraídos pelas ferramentas e compara os resultados obtidos pelas ferramentas.

2 REFERENCIAL TEÓRICO

Existe uma área da Ciência Forense, a Computação Forense, que tem como objetivo investigar crimes que foram cometidos utilizando equipamentos computacionais e elaborar o laudo pericial, contendo todas as informações e procedimentos que foram obtidos e realizados, respectivamente, durante todas as etapas da perícia. Neste trabalho, foi estudado o conceito de Computação Forense, os crimes que ela investiga, as principais etapas de uma investigação e, também, como as informações retiradas do *WhatsApp* em SO *Android* podem ser utilizadas na Perícia Forense.

Assim, esta seção está estruturada da seguinte forma: na subseção 2.1 são apresentados os conceitos de Computação Forense, como os principais crimes utilizando equipamento computacional, os principais exames forenses em informática e as etapas da Perícia Forense; subseção 2.2 apresenta a Perícia Forense usando o *WhatsApp*, trazendo algumas informações como os armazenamentos e diretórios e os procedimentos para realizar a análise forense a partir das informações obtidas.

2.1 COMPUTAÇÃO FORENSE

Segundo Costa (2011), os primeiros crimes envolvendo computadores foram as fraudes na contabilidade bancária, realizadas pelos funcionários dos bancos, fraudes contra o governo e contra o usuário. No Brasil, em 2016, conforme os dados disponibilizados pelo CERT.br, houve o total de 647.112 incidentes de segurança em computadores, em que, segundo a análise feita pelo próprio *site*, alguns desses eventos foram os ataques de negação de serviço (DoS), tentativa de fraude, varreduras e propagação de códigos maliciosos, ataques a servidores web, computadores comprometidos e outros incidentes reportados. Desse modo, os equipamentos eletrônicos, como computadores e celulares, podem ser utilizados de duas formas, tanto como ferramenta de apoio aos crimes quanto como meio para realização do crime.

A Computação Forense tem como principal objetivo “determinar a dinâmica, a materialidade e autoria de ilícitos ligado à área de informática” (ELEUTÉRIO e MACHADO, 2011, p.16). Assim, seu papel é determinar metodologias que ajudem os profissionais que atuam na área da informática a buscarem por evidências de crimes, para que tenham

informações para elaborar laudos contendo os dados dos possíveis crimes que foram cometidos.

Essa área tornou-se uma prática importante tanto para empresas quanto para órgãos públicos, pois utiliza-se de métodos científicos para identificar, preservar, analisar e documentar evidências localizadas em computadores e ou em dispositivos eletrônicos (FREITAS, 2006). Os responsáveis por realizar as investigações em busca de evidências e elaborar os laudos são os peritos criminais, que necessitam possuir de diploma de nível superior na área em que atuará realizando as pericias.

Segundo Costa (2011), o dever do perito criminal em informática é realizar a investigação de crimes cometidos com o uso de equipamentos eletrônicos ou que envolvam a computação como meio. Logo, é de extrema importância distinguir os modos que os equipamentos computacionais são utilizados para a prática de crimes virtuais, elas podendo ser utilizadas como ferramenta ou como meio para execução dos delitos, assim a seção 2.1.1 explica a diferença entre as modalidades em que os crimes são cometidos com a utilização do equipamento computacional.

2.1.1 Crimes cometidos com o uso de equipamentos computacionais

Os equipamentos computacionais, quando manipulados para cometer algum tipo de crime virtual, podem ser utilizados tanto como ferramenta para apoio a prática de crime quanto como um meio para realização de crime. Ou seja, os equipamentos computacionais podem ser utilizados de formas distintas, com o propósito de realizar de crimes.

De acordo com Eleutério e Machado (2011), a utilização do computador como ferramenta de apoio aos crimes consiste em usar o equipamento em alguns momentos da prática de delitos, ou seja, o equipamento computacional é apenas uma ferramenta que auxilia o infrator, de forma que o crime poderia ser cometido com ou sem a utilização do computador. Um exemplo de crime nesta modalidade é a utilização do computador para o tráfico de entorpecentes, em que o traficante pode utilizar o equipamento para armazenar informações sobre os usuários e a venda das drogas, trocar informações com outros traficantes, entre outros atos que não sejam o delito propriamente dito. A aplicação de exames forenses em equipamentos que são usados para cometerem esses crimes, pode ser uma forma eficiente de se obter provas técnicas e, assim, elaborar relatórios para o convencimento do magistrado que irá formular a sentença.

Já a utilização de equipamentos eletrônicos como meio para realização do crime utiliza o computador como peça fundamental para a ocorrência do crime, ou seja, caso o dispositivo

não existisse a infração não seria cometida (ELEUTÉRIO e MACHADO, 2011). Neste caso, os infratores utilizam o computador e/ou a *Internet* para cometerem crimes contra pessoas ou instituições tanto públicas quanto privadas, usando os dispositivos de informática para obter informações de um determinado computador ou de uma rede de computadores, ou até mesmo para cometer fraudes, seja comprometendo algum *site* ou clonando contas bancárias de terceiros. Um exemplo de crime nesta modalidade é o ataque de negação de serviços, também conhecido como *Denial of Service* (DoS), onde segundo Costa (2011, p. 33) são "Ataques utilizando um ou mais computadores para interromper um determinado serviço, computador ou rede".

As duas modalidades de crimes utilizando o equipamento computacional podem ser periciadas, tendo em vista que existem ferramentas e metodologias a disposição do perito para o auxiliar no processo de investigação. Segundo Queiroz e Vargas (2010) os casos são diferentes um do outro e nem sempre uma ferramenta utilizada em casos anteriores irá servir para futuras investigações. Desse modo, é necessário ter o conhecimento de quais são as principais formas de realizar perícias na área de informática para que o perito esteja preparado para atuar na cena do crime em busca de evidências e comprovação de crimes digitais. Assim, a próxima seção apresenta os principais exames forenses em informática.

2.1.2 Principais exames forenses em informática

Um dos principais princípios da análise forense é a Teoria da Troca de Locard, que diz que "qualquer um, ou qualquer coisa, que entra em um local de crime leva consigo algo do local e deixa alguma coisa para trás quando parte" (HOLPERIN e LEOBONS, 2017). No caso dos crimes que envolvem equipamentos computacionais, pode-se associar esse princípio ao fato de que mesmo os crimes virtuais deixam rastros, que são evidências físicas ou virtuais no local do crime, podendo ser utilizado como provas os dispositivos computacionais encontrados no local de crime ou as análises de *logs*, *sites* visitados entre outros respectivamente. Isso porque "o local físico é considerado o espaço real que abriga as evidências; e o local virtual é onde se abrigam as informações voláteis, sem registro definitivo" Costa (2011, p.36).

Assim, o perito forense possui o desafio de analisar uma grande variedade de equipamentos computacionais que armazenam dados em busca de rastros deixados pelo criminoso e que sirvam de evidências para comprovar o delito. Eleutério e Machado (2011) apresentam os principais exames forenses em informática dentro de sua experiência profissional, que são:

- **Exames e procedimentos em locais de crime de informática**: consistem principalmente no mapeamento, identificação e preservação dos equipamentos computacionais de forma correta, visando obter melhor seleção do material a ser apreendido para análise que serão examinados em laboratório. Dependendo do caso é necessário que se faça o exame no local de crime;
- **Exames em dispositivos de armazenamento computacional**: consistem em analisar arquivos, sistemas e programas instalados no discos rígidos (HD), CD's, DVD's, *Blu-Rays, pendrives* e outros dispositivos de armazenamento digital de dados. Esses exames possuem 4 fases que serão melhor explicados na seção 2.1.3 deste trabalho e utilizam de algumas ferramentas e técnicas para realizar a investigação nos dispositivos;
- **Exames em aparelhos de telefone celular**: tem como objetivo realizar a extração de dados dos aparelhos celulares, recuperando e formalizando as informações armazenadas em sua memória (lista de contatos, ligações, fotos, mensagens, etc.). A metodologia utilizada para realizar os exames em aparelhos celulares assemelham-se com os exames em dispositivos de armazenamento computacional;
- **Exames em sites da Internet**: consiste em analisar os conteúdos existentes na *internet* como *sites*, servidores remotos dos mais variados serviços com o objetivo de descobrir os responsáveis que cometeram algum tipo de crime utilizando a *internet*.

O perito forense, ao realizar os exames citados, precisa seguir etapas pré-definidas, de forma que cada etapa possui procedimentos básicos para a manipulação de evidências digitais, que devem ser realizados com cuidados rigorosos para não correr o risco de comprometer o resultado do trabalho. Estas etapas são apresentadas na próxima seção.

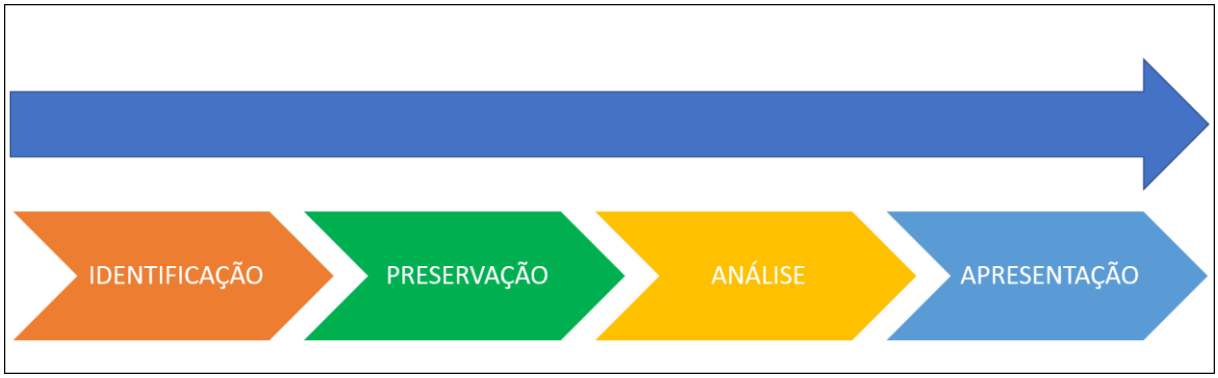
2.1.3 Etapas da perícia forense

Durante todo o desenvolvimento de uma Perícia Forense, desde o momento da chegada ao local de crime até a entrega do laudo pericial, é recomendado seguir as etapas indicadas na Figura 1, para que as análises das evidências sejam bem-sucedidas, diminuindo a probabilidade de ocorrer imprevistos que possam prejudicar a investigação.

A figura 1 apresenta as etapas da Perícia Forense Computacional, que devem ser seguidas adequadamente, tendo em vista que o profissional que irá realizar a perícia deve obter resultados convincentes e claros para interpretação do órgão que irá julgar o infrator.

Queiroz e Vargas (2010) alegam que o profissional deve estar preparado ao realizar uma perícia para que não seja surpreendido com situações que possam influenciar o resultado da análise negativamente. Uma ocorrência apresentada por Eleutério e Machado (2011) que pode comprometer o resultado de uma perícia é ligar um computador com SO *Windows*, pois ao ligar, alguns arquivos temporários são modificados e outros criados sem que o utilizador realize alguma operação, assim realizando alterações em relação as informações "originais" do dispositivo.

Figura 1: Etapas da Perícia Forense



A etapa da identificação inicia-se no momento em que é emitido o mandado de busca e apreensão, momento em que o perito deve determinar o que será apreendido para investigação, realizando a coleta e identificação dos equipamentos apreendidos. Segundo Costa (2011, p. 48) "Ao executar a busca e apreensão, as evidências serão identificadas, documentadas e apreendidas". Essa etapa é considerada uma das mais importantes, pois é nela que serão identificados e coletados os equipamentos que contém possíveis provas de crimes, exigindo muita cautela para manter a integridade dos dados. Nesta fase o profissional responsável pela investigação deve adotar alguns procedimentos que o auxiliem na coleta e identificação de evidências no local de crime como, por exemplo, determinar quais ferramentas podem ser utilizadas no local do crime; verificar se é possível remover as evidências digitais do local, entre outras (COSTA, 2011).

A etapa da preservação, segundo Eleutério e Machado (2011), consiste em garantir que as informações do material apreendido não sejam alteradas, pois eles contêm as evidências que devem ser mantidas intactas, para que possam ser usadas como provas de em uma investigação. Alguns dispositivos computacionais que podem ser encontrados e devem possuir atenção especial são as mídias regraváveis (CD-RW e DVD-RW) e dispositivos de armazenamentos portáteis (pen drives, cartões de memória e HDs externos), pois estes podem ter seus dados apagados caso sejam manuseados de forma incorreta.

Para manter a veracidade dos dados nos dispositivos apreendidos e evitar que eles sejam comprometidos durante o transporte e ou durante a perícia, são necessários tomar alguns cuidados como: armazenar HDs em sacos antiestática evitando danos ao periférico, preservando o conteúdo armazenado; realizar cópias ou imagens das mídias originais, fazendo os exames forenses nas cópias; todas as evidências devem ser lacradas em sacos contendo sua identificação (COSTA, 2011).

A etapa da análise consiste em "tentar identificar quem fez, quando fez, que dano causou e como foi realizado o crime" (FREITAS, 2006, p. 4). Ou seja, a fase da análise tem como propósito analisar as informações encontradas no equipamento apreendido buscando evidências de crimes para que seja possível responder questões como: quem estava utilizando o equipamento no momento do crime?; quais tipos de arquivos o suspeito estava utilizando?; quais arquivos foram excluídos? Lembrando que as evidências devem ser autentica, exata, completa e estar em conformidade com a lei (FREITAS, 2006). Durante a análise das evidências é de extrema importância manter a integridade dos dados a serem analisados para que não haja danos, evitando, assim, que os materiais sejam comprometidos.

A última etapa, a apresentação, consiste na elaboração do laudo pericial, também conhecida como cadeia de custodia, definida por Ronzani (ano, p. 24 apud PIRES, 1996) como o relatório elaborado pelo perito, no qual ele resume tudo o que foi observado durante a perícia. Costa (2011) menciona que os laudos devem ser claros, concisos, estruturados e sem ambiguidade para que não haja a incerteza de sua veracidade. Além disso, devem ser informados os métodos, procedimentos, *softwares* e *hardwares* utilizados na perícia e o laudo deve conter apenas afirmações e conclusões que possam ser provadas e demonstradas técnica e cientificamente.

2.2 PERÍCIA FORENSE NO WHATSAPP

O *WhatsApp* é um aplicativo de troca de mensagens instantâneas que armazena os dados (conversas, imagens, vídeos, áudios) no dispositivo em que estiver instalado (Thakur, 2013, tradução). Esse fator faz com que a Perícia Forense Computacional tenha um novo objeto de estudo, devido ao fato do aplicativo conter informações que podem ser extraídas através do exame forense no aparelho e serem utilizadas como fonte de provas/evidências em uma investigação de crime.

De acordo com informações na página *WhatsApp* (2016, tradução), as novas versões do aplicativo, disponibilizadas após 31 de março de 2016, possuem criptografia ponta-a-ponta, projetada pela empresa Open Whisper Systems, com objetivo de impedir que terceiros

e até mesmo o próprio *WhatsApp* tenha acesso as mensagens trocadas pelos usuários. Essa criptografia funciona como um cadeado, onde apenas o remetente e o(s) destinatário(s) que possuem a chave privada para destranca-lo podem ter acesso a mensagem, sendo que cada mensagem possui um cadeado e uma chave privada específica. Assim, os dados que são trocados pela rede de comunicação, mesmo que capturados enquanto são trocados, não poderão ser compreendidos, devido a necessidade de possuir a chave privada para decodificação da mensagem, que é enviado do autor para o contato ou grupo que ele deseja que receba a conversa.

Devido essa nova segurança adotada pelo aplicativo, a única maneira para investigar os dados enviados/recebidos pelo *WhatsApp* é com a obtenção do aparelho através de um mandado judicial e com a utilização de ferramentas/técnicas específicas para a extração das informações armazenadas nos dispositivos capturados. Assim, é necessário que o perito tenha domínio dos formatos dos arquivos e dos principais diretórios do aplicativo, para que seja possível realizar a captura de dados que podem servir de evidências de atos ilícitos.

Nesse contexto, o perito, antes de utilizar quaisquer ferramentas/técnicas para obtenção dos dados armazenados no aplicativo, precisa garantir a integridade dessas informações, ou seja, assegurar que os dados originais não sofram nenhum tipo de alterações, pois, caso exista alguma modificação nos conteúdos extraídos eles tornam-se inválidos para utilização como evidência de crime. Por isso é de suma importância o perito compreender onde são armazenados os arquivos que possuem mais relevância em uma investigação, para não o comprometer. Dessa forma a subseção a seguir apresenta os principais arquivos do *WhatsApp* e os diretórios em que são armazenados.

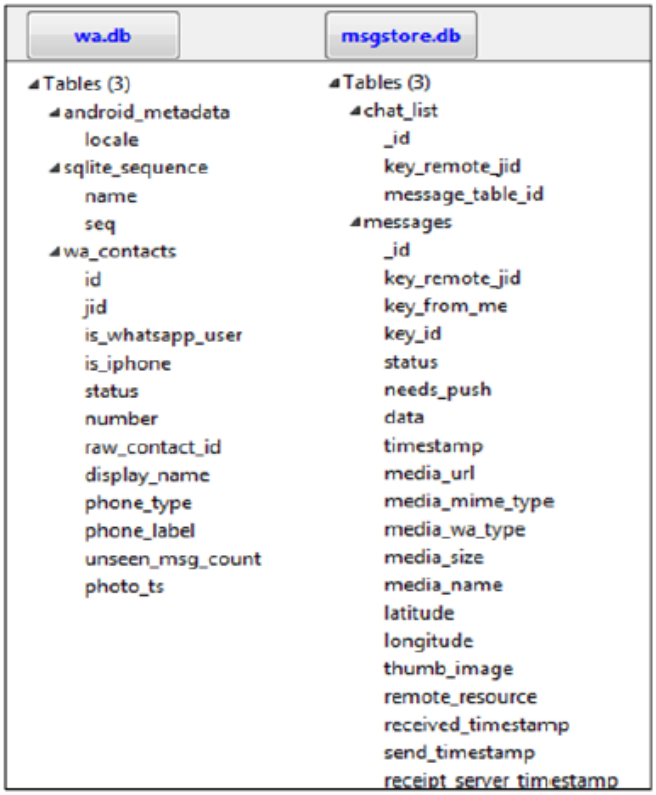
2.2.1 Arquivos e diretórios do Android

Os locais de armazenamento de arquivos do *WhatsApp* variam de acordo com a plataforma, por exemplo, *Android* e iOS possuem uma estrutura de diretórios distintos para o armazenamento das pastas que contêm os arquivos utilizados pelo aplicativo. Neste trabalho serão apresentados apenas os diretórios de dispositivos com a plataforma *Android*, tendo em vista que o presente projeto possui o foco em capturar os dados do *WhatsApp* apenas em SO *Android*.

Segundo Thakur (2013, tradução), o *WhatsApp* em sistemas *Android* armazena os dados de usuário em um Banco de Dados (DB) SQLite, que possui dois arquivos de base de dados, “msgstore.db” e “wa.db” que se encontram criptografados. Segundo Sandrim (2014), esses arquivos armazenam as mensagens e os contatos, respectivamente, podendo ser

encontrados originalmente no diretório "/sdcard/whatsapp/Databases" conforme mostra a figura 2.

Figura 2: Estrutura de armazenamento dos arquivos wa.db e msgstore.db



Fonte: Thakur (2013)

A figura 2 retrata a estrutura dos arquivos "wa.db" e "msgstore.db". Nesta figura, pode-se observar quais informações cada um dos arquivos armazena, sendo que "wa.db" disponibiliza três tabelas contendo informações dos contatos do *WhatsApp* como identificador, número do telefone, nome do contato, foto de perfil do contato etc. Já o arquivo "msgstore.db" disponibiliza três tabelas que armazenam informações das mensagens trocadas entre os usuários, como identificador do bate papo, mensagens relacionadas ao bate papo, horário de envio, horário de recebimento, as mídias que foram enviadas etc.

Além do diretório de armazenamento de DB do usuário, o *WhatsApp* utiliza outros diretórios, que são apresentados e descritos na tabela 1.

Tabela 1: Diretório do WhatsApp em SO Android

Diretório	Conteúdo
/sdcard/whatsapp/databases	Diretório que contém as bases de dados

	com o *backup* das mensagens e dos contatos do *WhatsApp* criptografados.
/sdcard/whatsapp/media	Diretório onde estão armazenados todos os tipos de arquivos de áudio, vídeo e imagens que foram enviados e recebidos.
/sdcard/whatsapp/Profile Pictures	Diretório onde as imagens que se referem aos perfis dos contatos estão armazenadas.
/data/data/com.whatsapp	Diretório acessado somente se o dispositivo estiver rooteado. Contém os subdiretórios abaixo.
/data/data/com.whatsapp/databases	Diretório onde estão armazenados a base de dados com as mensagens trocadas msgstore.db e os contatos ambos sem criptografia.
/data/data/com.whatsapp/files	Diretório onde estão armazenados diversos dados com a imagem dos perfis dos contatos, estatísticas, log e *timestamps*.

Fonte: Sandrim (2014)

Os diretórios apresentados na tabela 1 guardam arquivos criptografados e arquivos em texto plano, ou seja, sem criptografia. Um dos diretórios que pode ser acessado sem necessidade de decodificar os arquivos armazenados é o diretório onde estão localizadas as mídias (áudios, imagens e vídeos), sendo necessário apenas seguir o caminho "/sdcard/whatsapp/media" para ter acesso ao conteúdo armazenado. Já os arquivos criptografados, se encontram no diretório "/sdcard/whatsapp/databases", que armazenam os arquivos de DB do usuário, sendo esses arquivos "msgstore.db" e "wa.db" por exemplo, explicado anteriormente.

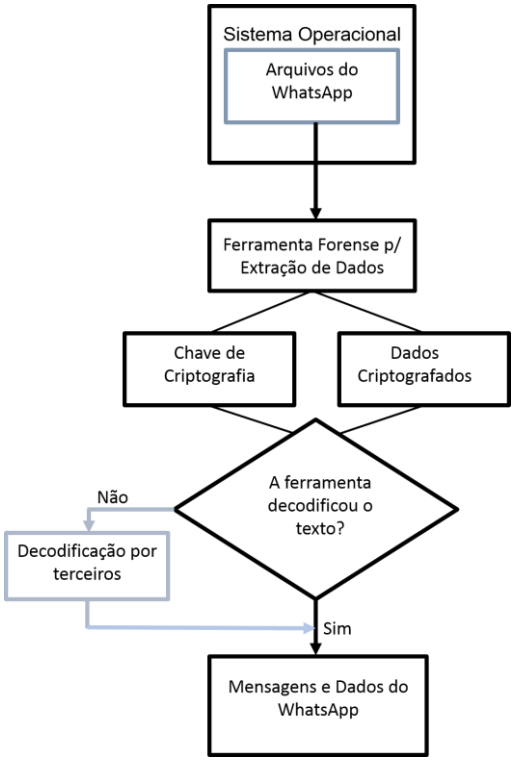
Ter conhecimento dos diretórios e saber o que cada um deles armazena faz com que o perito agilize o processo de extração de dados, em busca de evidências de crime. Isto é muito importante, tendo em vista que o prazo máximo para elaboração de laudo pericial é de 10 dias, segundo o art. 160, parágrafo único do Código de Processo Penal (CPP).

Para a captura dos dados, são utilizadas ferramentas que consigam, também, realizar a decodificação dos arquivos criptografados sem que estes sejam comprometidos. A seção 2.2.2 apresenta algumas etapas básicas que uma ferramenta forense deve realizar para que seja possível fazer a extração dos dados do *WhatsApp*.

2.2.2 Passos para extração de dados utilizando ferramentas forenses

Para definir quais *softwares* serão utilizados para extrair os dados do aplicativo é fundamental observar as funcionalidades do mesmo, tendo em vista que nem sempre uma ferramenta específica atenderá todas as necessidades apresentas durante a investigação. A figura 3, disponibilizada por Shortall e Azhar (2015, tradução), apresenta algumas etapas que devem ser seguidas na utilização de ferramentas forenses para a extração de dados do *WhatsApp*.

Figura 3: Passos para extração de dados utilizando ferramentas forenses



Fonte: Shortall e Azhar (2015, tradução)

A figura 3 mostra um fluxograma dos procedimentos para realização da extração de dados utilizando as ferramentas forenses. A figura 3 deve ser lida de cima para baixo, tendo o seu início na etapa "Sistema Operacional", em que é analisado o telefone celular que será periciado, pois cada SO (*Android*, iOS, *BlackBarry*) possui uma arquitetura diferente. Nesta primeira etapa, deve ser feito um levantamento de quais ferramentas conseguem atuar sobre o SO do dispositivo que será periciado para, assim, definir a(s) ferramenta(s) que serão utilizadas pelo perito, tendo em vista que esta é uma etapa que precede as atribuições da ferramenta, sendo realizado pelo perito.

A etapa da "Ferramenta Forense" consiste em utilizar a(s) ferramenta(s) definida(s) na etapa anterior para realizar a captura dos dados do *WhatsApp*, podendo esses dados estarem

criptografados, sendo necessário obter a chave de criptografia, que é utilizada para decodificar os dados.

Algumas ferramentas de extração oferecem a funcionalidade de decodificar os dados, mas, caso a que esteja sendo utilizada não ofereça suporte a esse serviço, é possível utilizar *softwares* de terceiros para realizar a decodificação dos dados. Quando os arquivos extraídos estiverem em texto plano, decodificados, o perito poderá realizar a busca por dados que sejam evidências de crimes cometidos pelo dono do dispositivo móvel periciado.

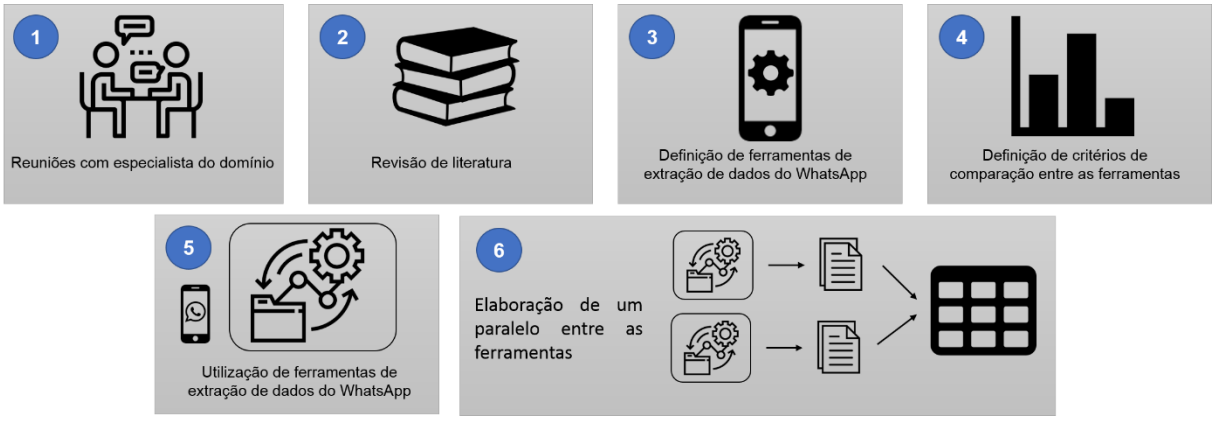
3 MATERIAIS E MÉTODOS

Esta seção apresenta a metodologia do trabalho, que engloba o desenho de estudo, demonstrando as etapas que foram seguidas para chegar no objetivo do projeto; os materiais que foram utilizados durante todo o processo da utilização da ferramenta; a descrição das ferramentas que foram utilizadas para captura dos dados do *WhatsApp* e a definição dos critérios de comparação entre as ferramentas.

3.1 DESENHO DE ESTUDO

Esta subseção apresenta o Desenho de Estudo, figura 4, que retrata a estrutura que o trabalho seguiu até chegar no objetivo final, que foi a elaboração de um paralelo entre as ferramentas utilizadas neste projeto. O desenvolvimento do trabalho foi composto por seis etapas, sendo que as etapas 1 a 4 foram realizadas para a elaboração do projeto do trabalho e as etapas 5 e 6 foram seguidas posteriormente para realização do trabalho proposto neste projeto.

Figura 4: Metodologia



A primeira etapa foi a realização de reuniões com o especialista do domínio, com o objetivo de compreender o contexto do projeto e o problema a ser solucionado. Nesta etapa, também foi realizado um levantamento das ferramentas que realizam a extração de dados de *Smartphones* mais utilizadas em trabalhos encontrados na *Internet* e de ferramentas indicadas por um profissional que atua na área de Perícia Forense Computacional.

A segunda etapa consistiu na elaboração da revisão de literatura. Essa fase teve como objetivo buscar obras publicadas sobre Perícia Forense Computacional, documentos que

esclarecessem sobre a perícia no *WhatsApp*, que apresentassem quais são os principais arquivos a serem extraídos, seus diretórios e as ferramentas utilizadas para captura de dados do aplicativos. A partir das obras encontradas, foi escrita uma seção para contextualizar o trabalho.

A terceira etapa foi a definição das ferramentas de extração de dados do *WhatsApp*. Nesse estágio foram feitas pesquisas sobre as ferramentas que foram encontradas no levantamento realizado na primeira etapa do projeto para saber quais poderiam ser utilizadas. Devido ao fato de algumas ferramentas serem proprietárias, foram escolhidas as duas que oferecem uma versão *trial*, que é uma distribuição da ferramenta para testes, e uma ferramenta gratuita, que oferece mais recursos que as demais gratuitas encontradas.

A quarta etapa teve como propósito definir critérios de comparação entre as ferramentas, o que é apresentado na seção 3.3.

A quinta etapa teve como objetivo a utilização de ferramentas de extração de dados do *WhatsApp*. Nesta etapa, foram utilizadas três ferramentas, definidas na terceira etapa, para realizar a extração dos dados do *WhatsApp* de um *Smartphone* com SO *Android*.

A sexta etapa teve como finalidade realizar um paralelo entre as ferramentas, baseando-se nas características e nas informações extraídas por cada uma delas. O paralelo será apresentado através de uma tabela comparativa entre as ferramentas com os critérios levantados na quarta etapa que é apresentado na subseção 3.4

3.2 MATERIAL

3.2.1 Hardware

Para o desenvolvimento do presente projeto foi utilizado um *Smartphone* com sistema *Android*, com o aplicativo *WhatsApp* instalado, através do qual foram trocadas mensagens diversas pelo aplicativo (áudios, chamadas, imagens, textos e vídeos), com diferentes contatos. Além disso, foi utilizado um microcomputador onde foram instaladas as ferramentas que foram usadas neste projeto. Os bancos de dados do celular foram copiados para o microcomputador e as ferramentas foram utilizadas para extrair informações relevantes desses BDs.

3.2.2 Software

Os *softwares* que realizam a extração de dados do aplicativo *WhatsApp* que foram utilizados neste trabalho são: Andriller, Elcomsoft e WhatsApp Key Extractor. A figura 5 ilustra as ferramentas que foram utilizadas.

Figura 5: Softwares para extração de dados do WhatsApp

- **Elcomsoft**: é uma ferramenta para *Windows* (*Windows* 10, 8.1, 8, 7, Vista; *Windows Server* 2012, 2008) que realiza a extração de conversas do *WhatsApp* tanto de dispositivos *Android* quanto iOS. Essa ferramenta conta com um visualizador onde são apresentados os resultados da extração (mensagens de texto, lista de contatos, imagens enviadas e recebidas etc.). Ela oferece a funcionalidade de decodificar os arquivos de banco de dados criptografados pelo *WhatsApp* e de *backups* realizado na nuvem da Apple iCloud, além da funcionalidade de quebrar senhas de bloqueio do *Smartphone*, sendo elas senhas numéricas ou desenho (ELCOMSOFT,2017, tradução). A Elcomsoft disponibiliza esse *software* em uma versão paga, sendo que o custo da edição padrão da ferramenta é de $79 (acessado em 24/11/2017), e uma versão para avaliação, em que algumas funcionalidades da ferramenta são liberadas por um tempo determinado.
- **Andriller**: é um aplicativo multiplataforma, podendo ser utilizado tanto em *Windows* quanto em Ubuntu Linux. O Andriller possui uma coleção de ferramentas forenses para S*martphones* que oferecem várias funcionalidades: extração e decodificação automatizada de dados, decodificação de DB criptografados do *WhatsApp*, bloqueio e desbloqueio para senha, padrão ou PIN e capturas de telas de exibição do dispositivo. Essa ferramenta possui três opções de licença, sendo elas: a licença de teste, que

liberam algumas funcionalidades para teste durante 14 dias podendo ser prorrogado por mais 14 dias; compra da licença, com valor anual de $99,99 (acesso em 24/11/2017) por estação de trabalho; e a licença LEA/ Polícia, para governo ou os órgãos da lei, que recebem uma licença gratuita de 6 meses para a utilização da ferramenta (ANDRILLER, 2017, tradução).

- **WhatsApp Key Extractor:** é um *script* cujo objetivo é extrair a chave criptográfica do *WhatsApp* em dispositivos *Android* não roteados. A chave é utilizada para decodificar os arquivos de banco de dados do *WhatsApp* que são criptografados. Além da chave criptográfica, o script também extrai o banco de dados "msgstore.db" e "wa.db" mais recente do aplicativo.

3.3 DEFINIÇÃO DOS CRITÉRIOS DE COMPARAÇÃO

Os critérios de comparação das ferramentas utilizadas neste trabalho foram selecionados entre os critérios apresentados nos trabalhos de Shortall e Azhar (2015), Sandrim (2014) e Thakur (2013). O anexo A apresenta a tabela comparativa entre as ferramentas utilizada por Sandrim (2014). O anexo B apresenta a tabela desenvolvida por Thakur (2013) em seu trabalho. O anexo C apresenta a tabela com os critérios de comparação utilizado por Shortall e Azhar (2015) em seu trabalho.

A partir das informações apresentadas nos anexos citados, definiram-se os critérios para o paralelo a ser apresentado neste trabalho, levando em consideração que os critérios elaborados pelos autores apresentam os resultados obtidos pelas ferramentas utilizadas por eles. Dessa forma, foram avaliados os critérios mais relevantes, disponibilizados nas obras dos autores, para que assim, fossem definidas as regras de comparação entre as ferramentas utilizadas neste projeto, não sendo necessário elaborar novos critérios. Esses critérios são apresentados na tabela 2.

Tabela 2: Apresentação dos critérios de comparação entre as ferramentas

Critério	Descrição	Possíveis Respostas
Licença	Qual tipo de licença a ferramenta possui?	Gratuito, versão de teste, pago
Criptografia	A ferramenta consegue realizar a decodificação dos arquivos?	Sim, não
Mensagens	Consegue apresentar as mensagens extraídas do aplicativo?	Sim, não

Mensagens excluídas	Consegue apresentar mensagens que foram excluídas do aplicativo?	Sim, não
Arquivos de mídias	Consegue apresentar os arquivos de mídias do aplicativo?	Sim, não
Arquivos de mídias excluídas	Consegue apresentar os arquivos de mídias que foram excluídas do aplicativo?	Sim, não
Chamadas	Consegue apresentar as chamadas realizadas e recebidas do aplicativo?	Sim, não
Contatos	Consegue apresentar a lista de contatos do aplicativo?	Sim, não
Foto de perfil	Consegue apresentar a foto de perfil dos contatos adicionados no aplicativo?	Sim, não
Relatórios	Gera relatórios em mais de um formato?	Sim, não
Necessidade de o dispositivo estar desbloqueado	O dispositivo necessita estar desbloqueado para que possa ser realizado a perícia?	Sim, não
Complexidade de uso da ferramenta	Qual a complexidade de se utilizar a ferramenta para realizar a extração e visualização dos dados do *WhatsApp*?	Baixa complexidade, média complexidade ou alta complexidade
Compatível com *Android* e iOS	A ferramenta é compatível com os SOs *Android* e iOS?	Compatível com *Android*, compatível com iOS, compatível com *Android* e iOS

Para analisar a complexidade de uso da ferramenta foi observado o quão difícil foi realizar a extração e visualização dos dados recuperados do *WhatsApp*. Para essa avaliação foi levado em conta os passos para extração de dados, que é apresentado na seção 2.2.2 deste trabalho. Um dos fatores relevantes foi se as ferramentas conseguiam realizar a decodificação e apresentação das informações extraídas ou se necessitavam de *softwares* de terceiros para realizar a apresentação.

4 RESULTADOS E DISCUSSÃO

O intuito deste trabalho foi realizar o comparativo entre ferramentas de extração de dados do *WhatsApp*, apresentando suas principais funcionalidades, os tipos de informações elas retornam para uma investigação forense e uma tabela com o paralelo das informações obtidas. Esta seção apresenta os resultados da extração dos dados do *WhatsApp* utilizando as ferramentas Elcomsoft eXplorer for WhatsApp, Andriller e WhatsApp Key Extractor. As ferramentas mencionadas possuem funcionalidades que permitem recuperar algumas informações do *WhatsApp*, como: mensagens trocadas entre os usuários, arquivos de mídias (áudio, imagem e vídeo), contatos do *WhatsApp* e as chamadas realizadas ou recebidas no aplicativo.

Nas próximas seções são apresentados os resultados obtidos de cada ferramenta, sendo a seção 4.1 a Elcomsoft, 4.2 a Andriller e 4.3 o WhatsApp Key Extractor. Também, na seção 4.4, será apresentada uma tabela comparativa entre as ferramentas, que mostram as informações levantadas sobre os *softwares* de acordo com os critérios definidos na seção 3.3, e considerações sobre os resultados apresentados.

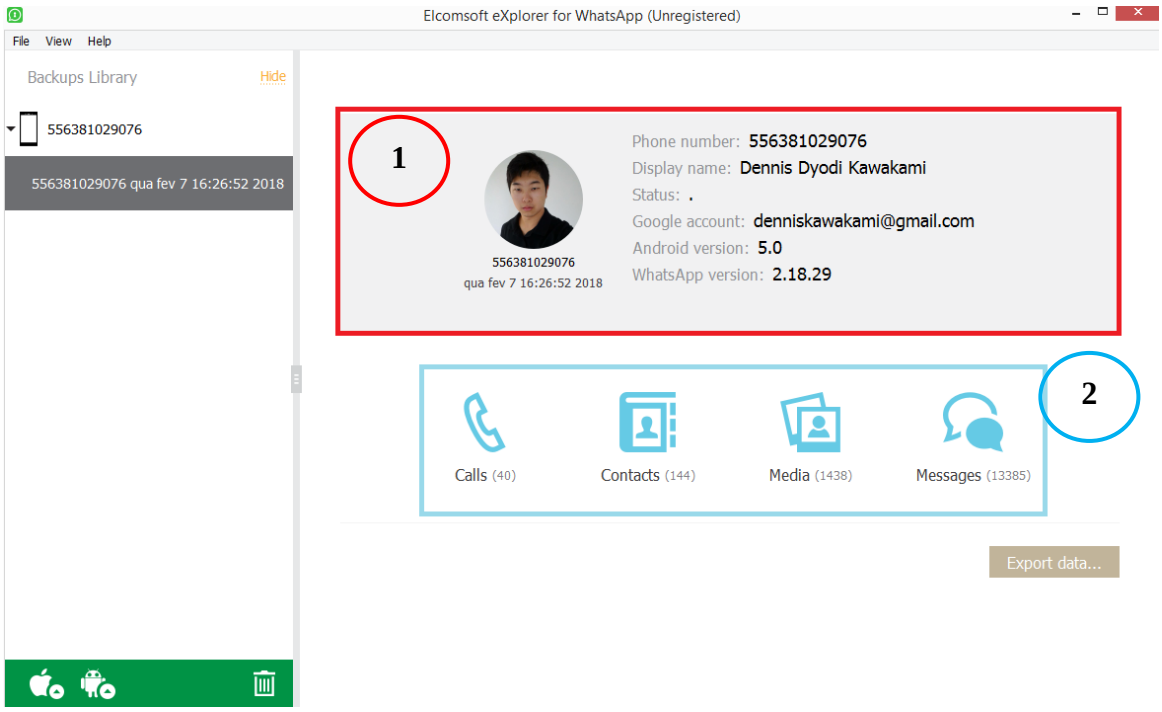
4.1 ELCOMSOFT

A Elcomsoft, descrita na seção 3.2.2, é uma ferramenta proprietária para realizar a extração de dados do *WhatsApp*, tanto em SO *Android* quanto em iOS, que retornam informações que auxiliam na investigação forense. Neste trabalho, foi utilizada a versão de teste, que possibilita utilizar todos os recursos disponíveis na ferramenta, com a limitação de retornar apenas parte do conteúdo do *WhatsApp* armazenado no dispositivo, sendo necessário adquirir a sua versão paga para obter as informações completas.

A limitação da versão teste não afeta o desenvolvimento do trabalho, tendo em vista que todas as funcionalidades da ferramenta são liberadas, restringindo apenas a quantidade de conteúdo apresentado. Diferente de uma perícia forense, que necessita ter acesso a todos os dados para uma investigação, o presente trabalho precisa apresentar as funcionalidades que a ferramenta disponibiliza.

A figura 6 apresenta a tela inicial do *software* “Elcomsoft eXplorer for WhatsApp”, que é exibida após o processo de carregamento e de *backups* dos dados do *WhatsApp*, que é realizado pela própria ferramenta.

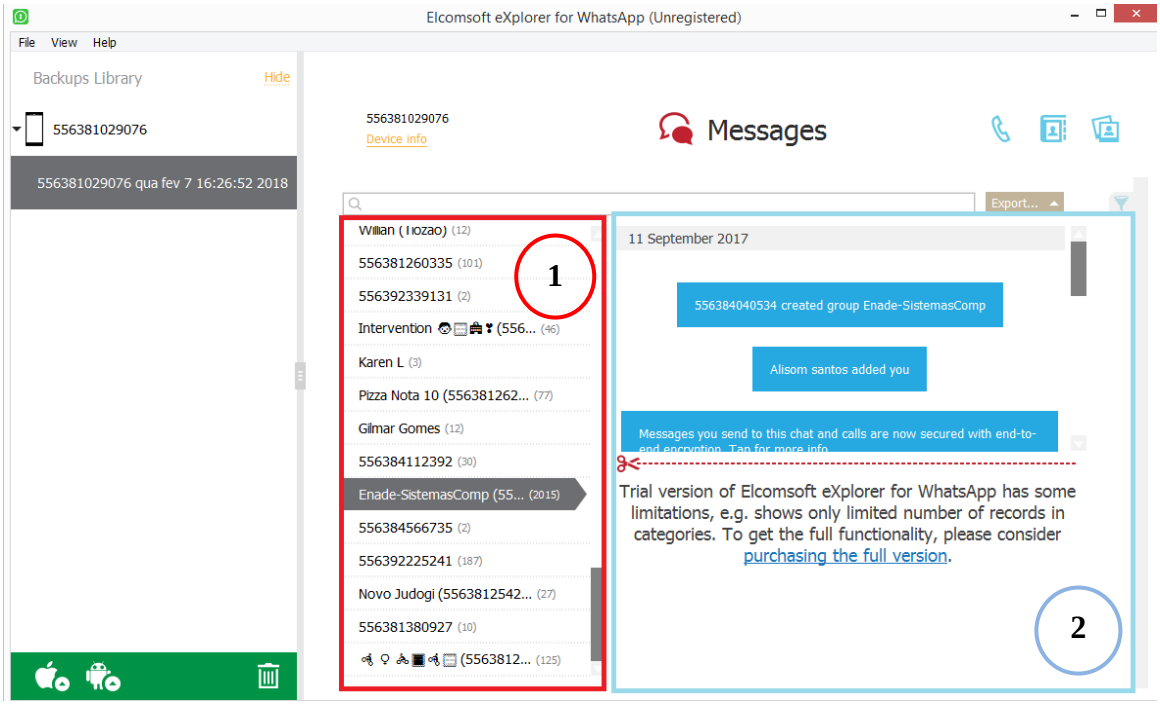
Figura 6: Tela inicial da ferramenta Elcomsoft eXplorer for WhatsApp



Conforme apresentado na figura 6, a tela inicial da ferramenta exibe diversas informações sobre o *WhatsApp* periciado. O bloco contornado pela cor vermelha e com a marcação de número 1 mostra as informações relacionadas à conta do usuário no aplicativo, como: número do telefone, nome que aparece no *WhatsApp*, *status* do usuário, conta da *Google*, versão do *Android* e a versão do *WhatsApp*. Já o bloco contornado pela cor azul e com a marcação de número 2 exibe um menu no qual é possível acessar as chamadas, os contatos, os arquivos de mídias (áudios, imagens e vídeos) e as mensagens do usuário, respectivamente.

As informações que podem ser acessadas pelo menu, marcação de número 2, foram extraídas dos arquivos "msgstore.db" e "wa.db". A ferramenta possui recursos para decodificar os arquivos criptografados, como é o caso das mensagens e contatos. As figuras 7 e 8 apresentam as informações contidas nesses dois arquivos após a decodificação, sendo elas as mensagens e os contatos, que podem ser acessadas através do menu "*Messages*" e "*Contacts*", destacados na figura 6.

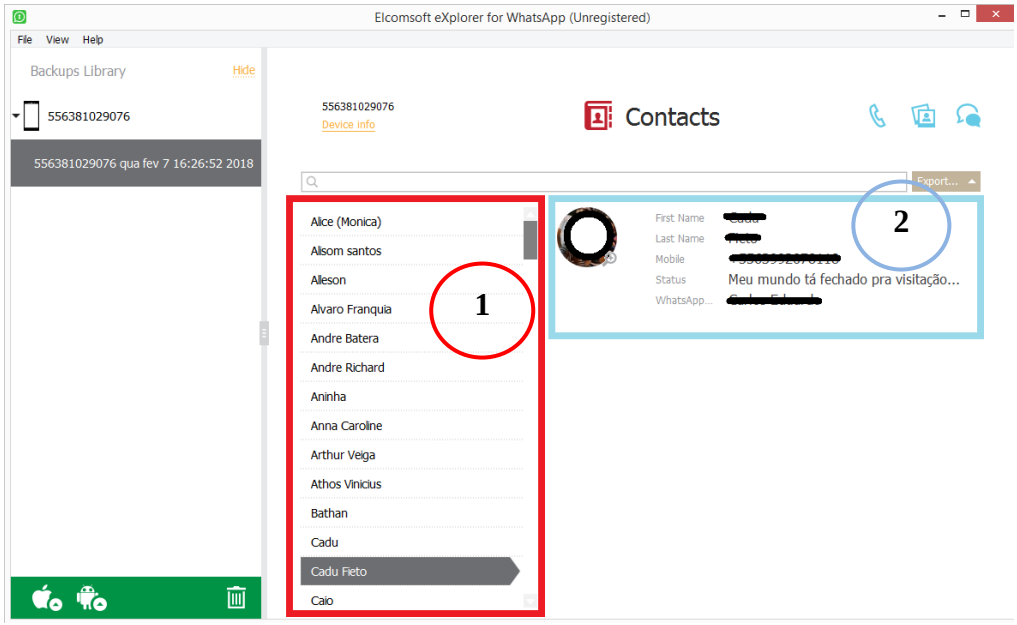
Figura 7: Extração das mensagens do WhatsApp



Conforme mostra a figura 7, o aplicativo consegue extrair as mensagens trocadas pelo usuário. O bloco contornado pela cor vermelha e com a marcação de número 1 apresenta uma lista dos contatos e grupos com os quais o usuário trocou mensagens. O bloco contornado pela cor azul e com marcação de número 2 apresenta a conversa contendo as mensagens trocadas com o contato/grupo selecionado, no caso, grupo “Enade-SistemasComp”.

A figura 8 apresenta os contatos que foram extraídos do arquivo “wa.db”, que armazena o *backup* dos contatos salvos pelo usuário no *WhatsApp*. Após a decodificação desse arquivo foi possível obter informações como o número do telefone, nome e outros dados referente às configurações do contato.

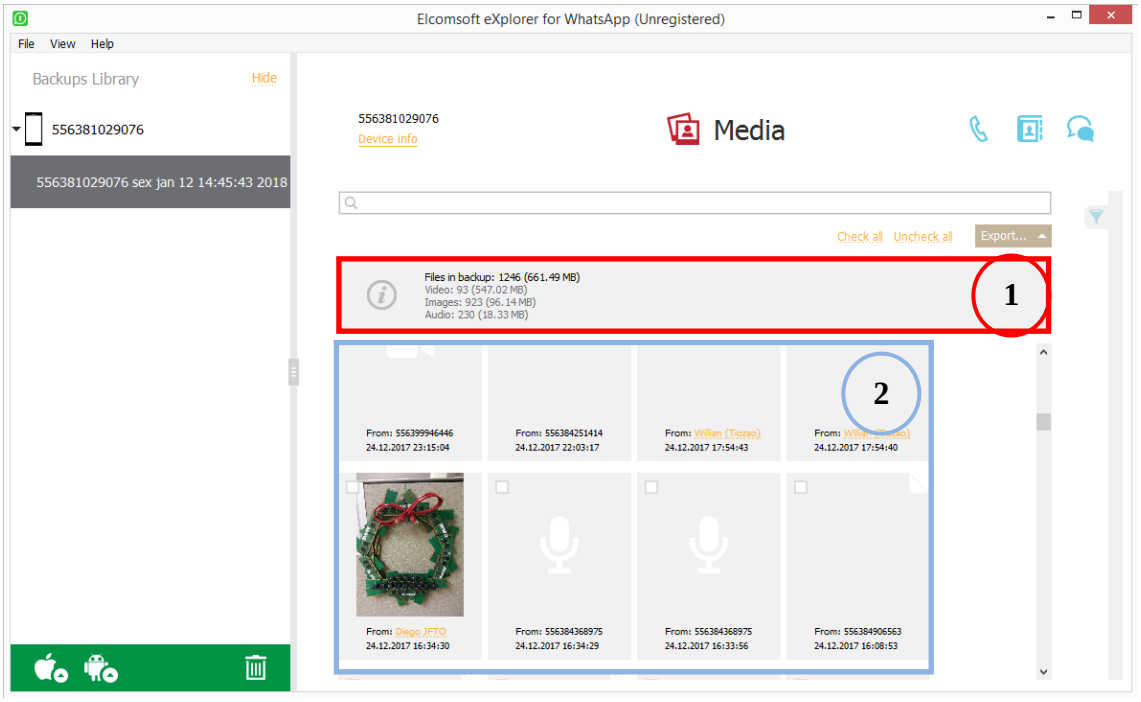
Figura 8: Lista de contatos do WhatsApp



. Na figura 8, o bloco contornado pela cor vermelha e com a marcação de número 1 exibe uma lista de contatos que o usuário possui adicionado no *WhatsApp*. Quando um contato é selecionado, são exibidas as informações referentes a ele no bloco contornado pela cor azul e com marcação de número 2, como: primeiro e último nome do contato, número do telefone, status e o nome que aparece no *WhatsApp*. No exemplo da imagem, após selecionar o contato "Cadu Fieto" foram exibidas algumas informações referentes a ele como sua foto de perfil e outros dados que foram mencionadas antecipadamente.

Além de apresentar as informações descritas anteriormente, a ferramenta, recupera as mídias (áudios, imagens e vídeos) que foram enviadas ou recebidas pelo *WhatsApp*. A figura 9 exibe algumas dessas mídias, que podem ser acessadas através do menu "*Media*", apresentado na figura 6.

Figura 9: Extração dos arquivos de mídias do WhatsApp

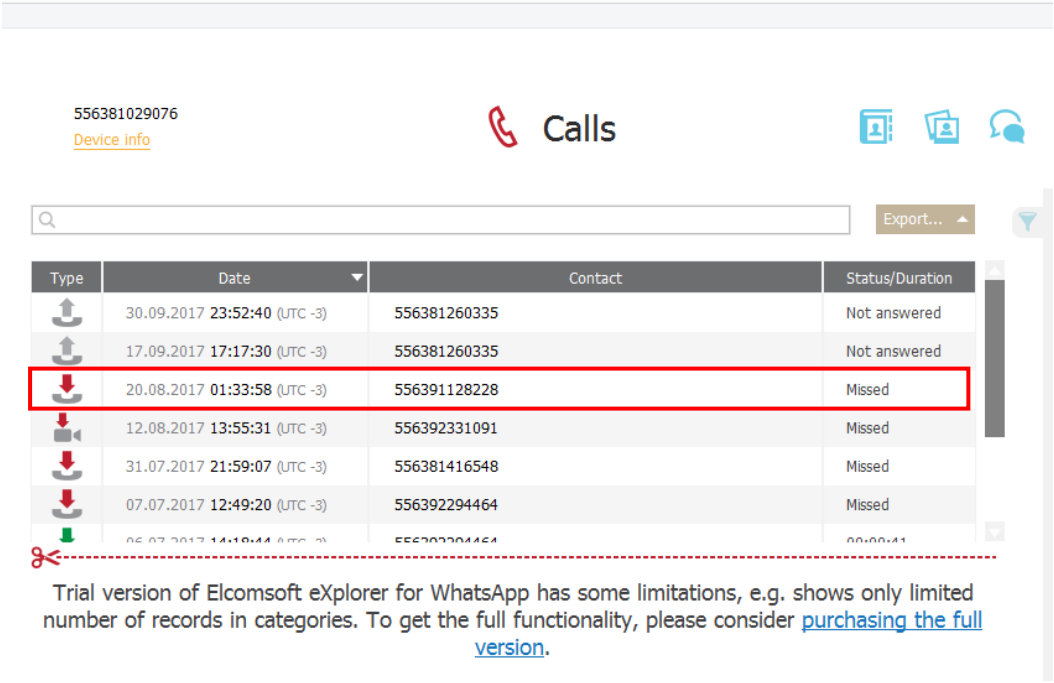


A figura 9 apresenta os arquivos de mídias enviados ou recebidos, que foram extraídos do *WhatsApp*. O bloco contornado pela cor vermelha e com a numeração 1 apresenta informações sobre os arquivos de mídias, como: a quantidade total de arquivos que foram extraídos e o seu tamanho total em *megabytes* (MB) e as informações individuais de cada tipo de arquivos (vídeo, imagens e áudios). Já o bloco contornado pela cor azul e com a numeração 2 apresenta a própria mídia, contendo informações do destinatário e sua respectiva data e horário.

Nem todos os arquivos de mídias extraídos pela ferramenta podem ser visualizados ou reproduzidos, devido ao fato da ferramenta recuperar essas mídias dos arquivos de *backup*, ou seja, caso não tenha sido feito o *backup* da mídia e o usuário apagá-la, apenas será informado que foi enviado um áudio, imagem ou vídeo, não sendo possível visualizá-lo ou reproduzi-lo.

O *software* "Elcomsoft eXplorer for WhatsApp" também possui uma funcionalidade que apresenta as chamadas que o usuário efetuou ou recebeu no *WhatsApp*. A figura 10 apresenta a tela referente ao item "*Calls*", chamadas, do menu mostrado na figura 6.

Figura 10: Extração de ligações no WhatsApp



A figura 10 exibe as chamadas de voz ou de vídeo que o usuário efetuou ou recebeu no *WhatsApp*. Na imagem são apresentadas diferentes informações que podem ser analisadas, como:

- Tipo de chamada (*Type*): a ferramenta distingue os tipos de chamadas por meio de ícones, sendo eles um telefone ou uma filmadora. O ícone do telefone indica que o tipo de ligação foi a de voz, já o ícone de filmadora indica que foi uma chamada de vídeo. As cores das setas indicam se a chamada foi perdida, não respondida ou aceita, sendo vermelho, cinza e verde suas respectivas cores;
- Data da chamada (*Date*): outra informação apresentada são as datas das chamadas, onde são exibidas o dia e a hora em que a chamada foi efetuada ou recebida;
- Contatos (*Contact*): também são apresentados os contatos que o proprietário efetuou ou recebeu as chamadas;
- *Status*/Duração da chamada (*Status/Duration*): a última coluna apresenta informações referente ao *status*/duração da chamada. O status "*not answered*" indica que que o proprietário do *Smartphone* realizou algum tipo de chamada para um determinado usuário, mas não foi respondido. O status "*missed*" indica que algum contato realizou uma chamada para o proprietário do *Smartphone*, mas não foi atendido. Caso a chamada seja atendida, é apresentado a duração da chamada.

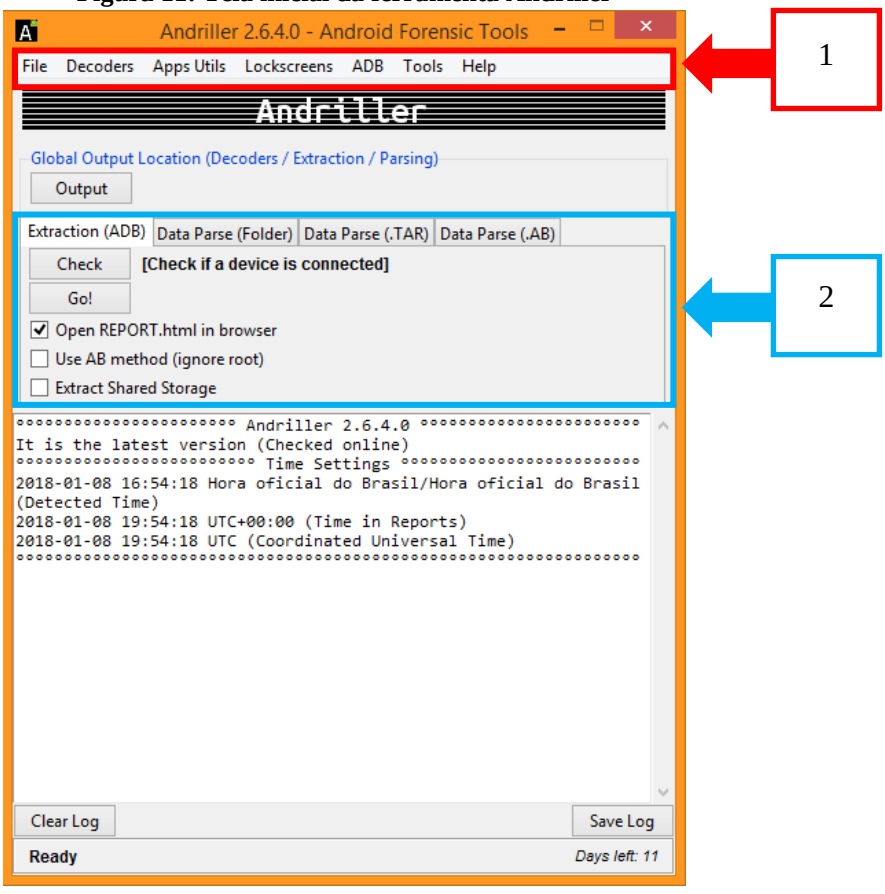
O bloco contornado destaca uma chamada, para qual são apresentadas as informações citadas anteriormente. Na chamada pode-se observar que se trata de uma chamada de voz recebida. A seta para baixo simboliza que uma chamada foi realizada para o proprietário do *Smartphone*, do contrário, indicaria que o proprietário efetuou uma chamada para um determinado contato. A data e a hora da chamada correspondem ao dia 20/08/2017 no horário de 01:33:58 e seu status foi "*missed*", ou seja, uma chamada perdida.

4.2 ANDRILLER

A Andriller, descrita na seção 3.2.2, é uma ferramenta proprietária que realiza extração de dados do *WhatsApp*, tanto em SO *Android* quando em iOS, assim como a Elcomsoft. Neste trabalho foi utilizada a versão de teste da ferramenta, na qual as funcionalidades são disponibilizadas por quatorze dias, podendo ser prorrogado por mais quatorze, sendo necessário adquirir uma chave de acesso permanente para sua utilização após esse período. Durante o período de teste da ferramenta, todas suas funcionalidades foram disponibilizadas por completo, sendo utilizadas apenas as funcionalidades referentes ao *WhatsApp*.

A figura 11 apresenta a tela inicial da Andriller, que é exibida após a inicialização da ferramenta.

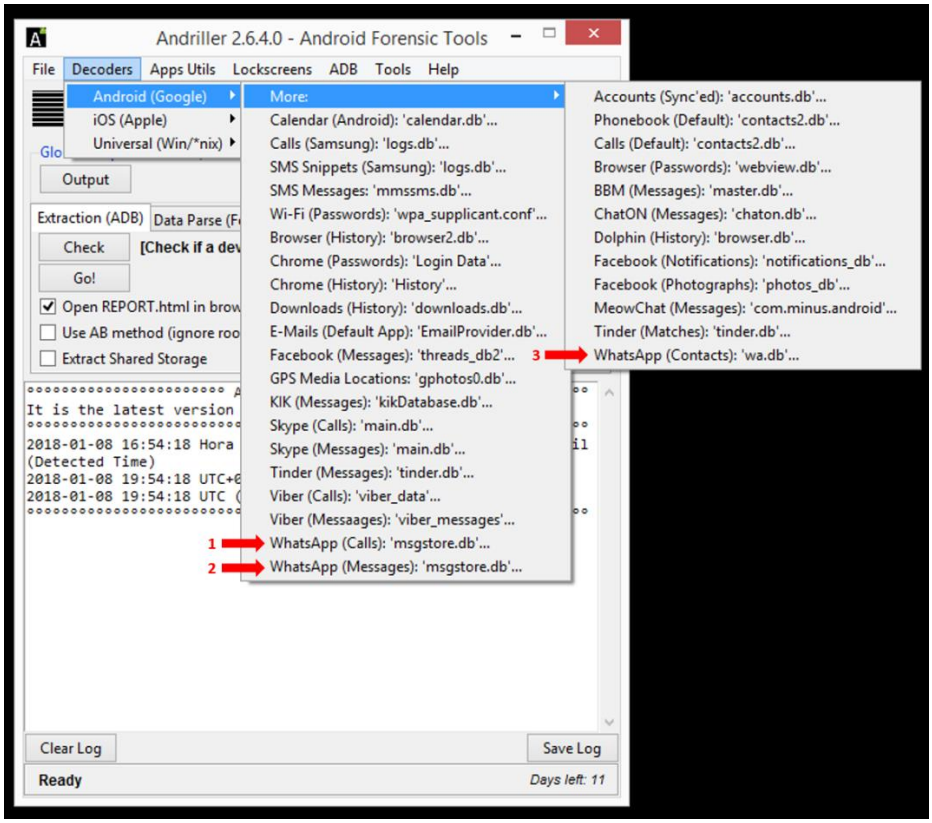
Figura 11: Tela inicial da ferramenta Andriller



Conforme apresentado na figura 11, a tela inicial da Andriller exibe diversas informações sobre suas funcionalidades e configurações. O bloco contornado pela cor vermelha e com a identificação de número 1 mostra uma barra de menus que possibilita acessar suas funcionalidades como abrir um arquivo (*file*), acessar o menu de decodificação (*decoders*), entre outras. Já o bloco contornado pela cor azul e com a identificação de número 2 exibe a funcionalidade de extração de dados do *WhatsApp* (*Extraction ADB*). Dentro desta funcionalidade possui as opções como checar se o *Smartphone* ou o dispositivo a ser periciado está conectado (*Check*) e de iniciar a extração dos arquivos de *backups (Go!).* As demais funcionalidades como *"Data Parse (Folder)"* e *"Data Parse (.TAR)"* não foram utilizadas neste trabalho, por elas não analisarem os arquivos de banco "msgstore.db" e "wa.db".

A maioria das funcionalidades utilizadas para recuperação e decodificação dos dados do *WhatsApp* encontra-se no opção "*Decoders*", que pode ser acessada através da barra de menu, conforme mostrada na figura 11. A ferramenta possui recursos para decodificar os arquivos criptografados, sendo necessário apenas extrair e salvar os arquivos "msgstore.db" e "wa.db" em algum diretório do computador antes de realizar o procedimento de decodificação. A figura 12 apresenta as funcionalidades disponíveis na opção "*Decoders*"

Figura 12: Menu de funcionalidade da ferramenta



Conforme mostrado na figura 12, ao acessar a opção "*Decoders*", são exibidas várias opções referentes ao item "*Android (Google)*", que permite decodificar arquivos ".db" de diferentes aplicativos, além de recuperar outros tipos de informações como SMS e senhas de Wi-Fi. Entre as opções, apenas as três funcionalidades referentes ao *WhatsApp* foram utilizadas, sendo elas: "*WhatsApp (Calls)*", indicada pela numeração 1; "*WhatsApp (Messages)*", indicada pela numeração 2; e "*WhatsApp (Contacts)*", indicada pela numeração 3. As figuras 13, 14, 15 e 16 apresentam os resultados obtidos ao selecionar uma das três opções citadas, que são as mensagens, os arquivos de mídias, os contatos e as chamadas extraídas pela ferramenta.

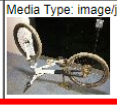
Figura 13: Mensagens extraídas pela ferramenta

#	Sender	Recipient(s)	Message	Type	Time
36557	(This device)	+556381254276	Eu vou ir	Sent	2018-01-08 17:10:23 UTC+00:00
36556	(This device)	+556381254276	Sim	Sent	2018-01-08 17:10:20 UTC+00:00
36555	+556381254276	(This device)	Bora lá hoje?	Inbox	2018-01-08 17:05:15 UTC+00:00
36554	+556381254276	(This device)	Rola de mais	Inbox	2018-01-08 17:05:10 UTC+00:00
36553	+556381254276	(This device)	Blz e vc?	Inbox	2018-01-08 17:05:07 UTC+00:00

A figura 13 apresenta as mensagens trocadas entre os usuários pelo *WhatsApp*. Essas mensagens podem ser recuperadas através do arquivo "msgstore.db" e por meio da funcionalidade "*WhatsApp (Messages)*", conforme destacado na figura 12. A área destacada na figura 13 exibe algumas informações sobre a troca de mensagens. Nas colunas "*Sender*" e "*Recipient(s)*", respectivamente, é informado quem enviou e recebeu a mensagem, sendo apresentado o número do contato. Na coluna "*Message*" é apresentado o conteúdo da mensagem. Na coluna "*Type*", é apresentado se a mensagem foi enviada (*Sent*) ou recebida (*Inbox*) pelo usuário e na coluna "*Time*" são apresentadas a data e hora.

Além de apresentar as informações descritas anteriormente, a ferramenta também recupera imagens que foram enviadas ou recebidas pelo *WhatsApp*. A figura 14 exibe algumas imagens que foram recuperadas junto as mensagens.

Figura 14: Mensagens de mídias

4018	+556 84360818	▸ RCS - JK LESTE I	Media Type: image/jpeg 	Inbox	2016-06-03 09:55:04 UTC+00:00	
4017	+556 84360818	▸ RCS - JK LESTE I	Media Type: image/jpeg 	Inbox	2016-06-03 09:54:58 UTC+00:00	

Os arquivos de mídias também são recuperados através do arquivo "msgstore.db" e por meio da funcionalidade "*WhatsApp (Messages)*", conforme destacado na figura 12. As

colunas apresentadas na área destacada da figura 14 exibem as mesmas informações mencionadas anteriormente sobre as mensagens extraídas. O que difere é que na coluna correspondente a "*Message*" ao invés de apresentar uma mensagem de texto, exibe um arquivo de mídia, no caso, as imagens das bicicletas.

Nem todos os arquivos de mídias extraídos pela ferramenta podem ser visualizados, devido ao fato da ferramenta recuperar essas mídias dos arquivos de *backup*, assim como a Elcomsoft. Além disso a Andriller não possui funcionalidade para reproduzir os arquivos de áudios e vídeos recuperados pelo arquivo de *bakcup* do *WhatsApp*, sendo apenas apresentado como uma imagem e informando o tipo de arquivo (áudio ou vídeo).

Figura 15: Contatos

Name	Number	Status
Aline Diniz	+556384588965	
Alisom santos	981262545	Habacuque 3: 17-18
Alleson	981410033	Olá! Eu estou usando WhatsApp.
Aluga Lado Ortobon	992992191	Hey there! I am using WhatsApp.
Alvaro Franquia	21973439669	Disponível
Andre Batera	981096203	Você pode ter dinheiro, mas tem coisas que nunca vai conseguir comprar. Como um dinossauro, por exemplo.
Andre Richard	04144999283266	

A figura 15 apresenta uma lista dos contatos que foram recuperados do *WhatsApp* através do arquivo "wa.db" e por meio da funcionalidade "*WhatsApp (Contacts)*", conforme destacado na figura 12. A área destacada em vermelho na figura 15 exibe algumas informações sobre o contato. Na coluna "*Name*" é informado o nome do contato adicionado no *WhatsApp*. Na coluna "*Number*" é apresentado o número do telefone referente ao contato e na coluna "*Status*" é apresentado o *status* que o usuário estava utilizando no *WhatsApp*.

Da mesma forma que a ferramenta Elcomsoft, a Andriller oferece a funcionalidade de recuperar as chamadas efetuadas ou recebidas pelo usuário. A figura 16 exibe essa funcionalidade, que pode ser acessada através da opção "*WhatsApp (Calls)*", apresentada na figura 12.

Figura 16: Extração das chamadas

This report was generated using Andriller # (This field is editable in Preferences)

[WhatsApp Calls]

Total items: 32

#	Type	Number	Time	Duration
36391	Dialled	+5516981262677	2018-01-07 02:54:21 UTC+00:00	0:20:51
36390	Dialled	+5516981262677	2018-01-07 02:52:37 UTC+00:00	0:01:13
36255	Dialled	+556392294464	2018-01-06 16:07:08 UTC+00:00	0:00:23
36254	Dialled	+556392294464	2018-01-06 16:05:25 UTC+00:00	0:00:47
36226	Received	+556391128228	2018-01-05 23:49:02 UTC+00:00	0:00:23
36224	Received	+556399960082	2018-01-05 23:48:17 UTC+00:00	0:00:02
36222	Received	+556391128228	2018-01-05 23:37:23 UTC+00:00	0:00:44
36165	Dialled	+556392294464	2018-01-05 13:35:30 UTC+00:00	0:00:00
36051	Dialled	+556392294464	2018-01-03 21:29:17 UTC+00:00	0:00:24
35815	Received	+556392257643	2018-01-01 05:46:31 UTC+00:00	0:00:45
34515	Dialled	+556381260335	2017-12-28 22:04:15 UTC+00:00	0:00:11
31273	Missed	+556392110023	2017-12-03 01:09:49 UTC+00:00	0:00:00
31212	Dialled	+556381262545	2017-12-02 22:21:32 UTC+00:00	0:00:00
28722	Dialled	+556381416548	2017-11-21 00:36:55 UTC+00:00	0:00:40
28713	Received	+556381416548	2017-11-21 00:24:20 UTC+00:00	0:00:29
27744	Received	+556381416548	2017-11-14 00:50:47 UTC+00:00	0:00:27
26809	Dialled	+556381468261	2017-11-04 23:07:20 UTC+00:00	0:00:00
26105	Missed	+556392225241	2017-10-31 22:29:30 UTC+00:00	0:00:00
25562	Missed	+556392294464	2017-10-28 13:01:14 UTC+00:00	0:00:00
25561	Missed	+556392294464	2017-10-28 13:00:49 UTC+00:00	0:00:00
24164	Dialled	+556399662019	2017-10-22 22:48:55 UTC+00:00	0:00:00
21357	Dialled	+556381260335	2017-10-06 23:29:00 UTC+00:00	0:00:00
19446	Dialled	+556381260335	2017-10-01 02:52:40 UTC+00:00	0:00:00
17775	Dialled	+556381260335	2017-09-17 20:17:30 UTC+00:00	0:00:00
14871	Missed	+556391128228	2017-08-20 04:33:58 UTC+00:00	0:00:00

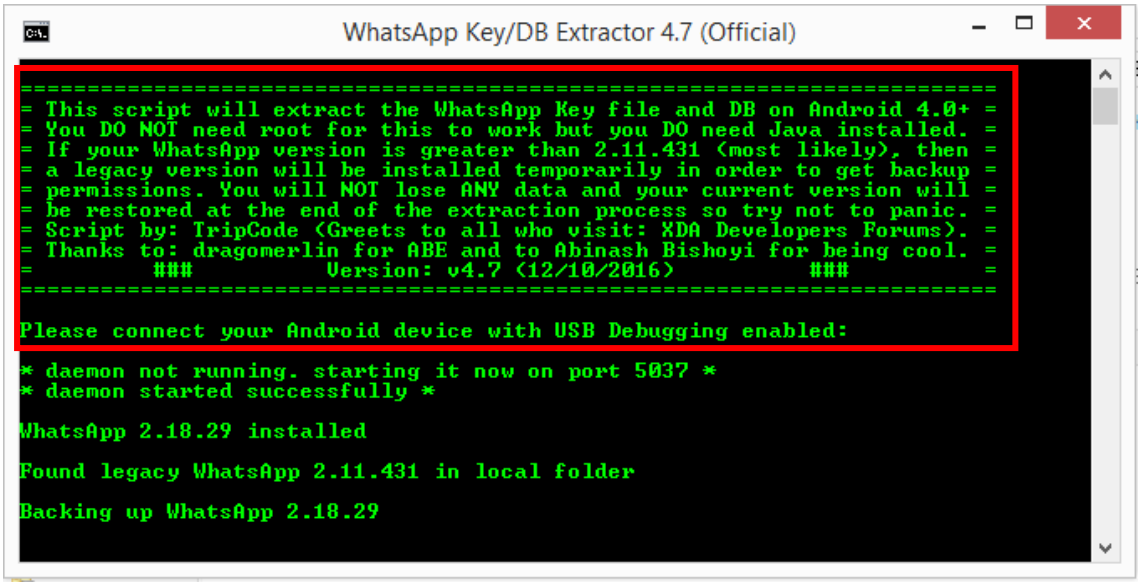
A figura 16 exibe as chamadas que o usuário efetuou ou recebeu no *WhatsApp*. A área destacada em vermelho na figura exibe algumas informações sobre as chamadas. Na primeira coluna é apresentado o ID da chamada. Na coluna "*Type*" é apresentado o tipo da chamada, se ela foi discada (*Dialled*), recebida (*Received*) ou perdida (*Missed*). Na área destacada a chamada foi discada pelo proprietário do *WhatsApp*. Na coluna "*Number*" é apresentado o número do telefone do contato. Na coluna "*Time*" é apresentado a data e a hora que foi realizada a chamada, sendo ela realizada no dia 07/01/2018 no horário de 02:52 e na coluna "*Duration*" é apresentado a duração da chamada, sendo que teve a duração de 0:01:13 (um minuto e treze segundos).

4.3 WHATSAPP KEY EXTRACTOR

O WhatsApp Key Extractor, apresentado na seção 3.2.2, ao contrário da Elcomsoft e Andriller que são proprietárias, é um *script* gratuito que realiza a extração de dados do *WhatsApp* em SO *Android*. Tendo em vista que o WhatsApp Key Extractor apenas realiza a extração dos arquivos de *backups* do aplicativo, para utilizá-la foi necessário obter outra ferramenta para analisar as informações extraídas, o WhatsApp Viewer.

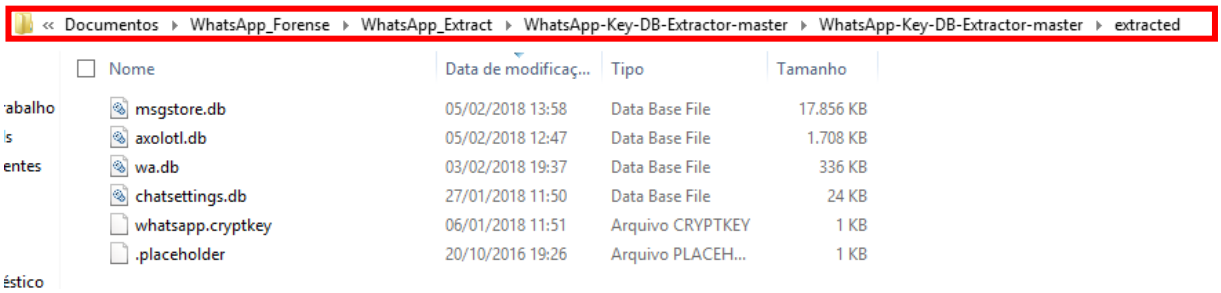
A figura 17 apresenta a tela inicial do WhatsApp Key Extractor, que é aberta após a execução do *script*.

Figura 17: Extração do banco de dados do WhatsApp com WhatsApp Key Extractor



O bloco destacado na figura 17 informa algumas configurações necessárias para realizar a extração dos arquivos de banco de dados do *WhatsApp*, que são: possuir o Java instalado, habilitar o modo de depuração *Universal Serial Bus* (USB) do *Android* e possuir a versão 4.0 ou superior do *Android* instalado no *Smartphone*. O *script* após realizar o processo de extração de dados do *WhatsApp*, armazenam os arquivos extraídos na sua pasta "*extracted*". A figura 18 apresenta os arquivos que foram extraídos após a execução do *script*.

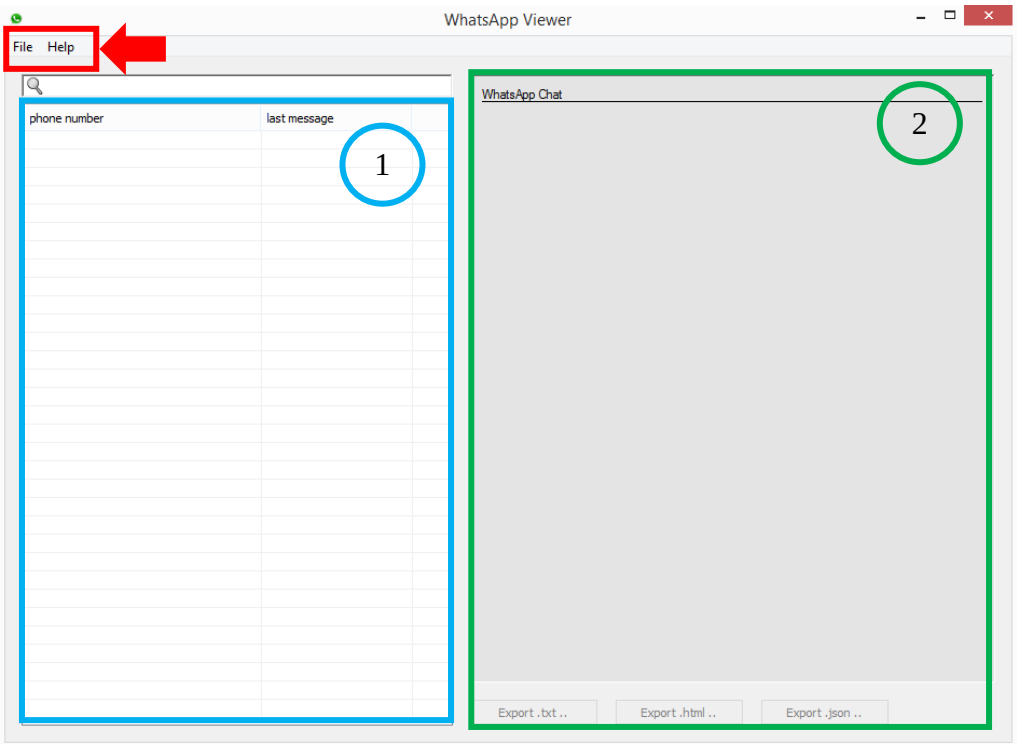
Figura 18:Arquivos extraídos utilizando o WhatsApp Key Extractor



O WhatsApp Key Extractor realiza a extração de alguns arquivos do *WhatsApp* e os salvam na pasta "*extracted*" conforme mostra o diretório da pasta, destacada em vermelho. Os arquivos extraídos pelo *script* são os bancos de dados "msgstore.db" e "wa.db", que são os *backups* das conversas e dos contatos do *WhatsApp* e a chave de decodificação "*whatsapp.cryptkey*", como é apresentado na figura 18.

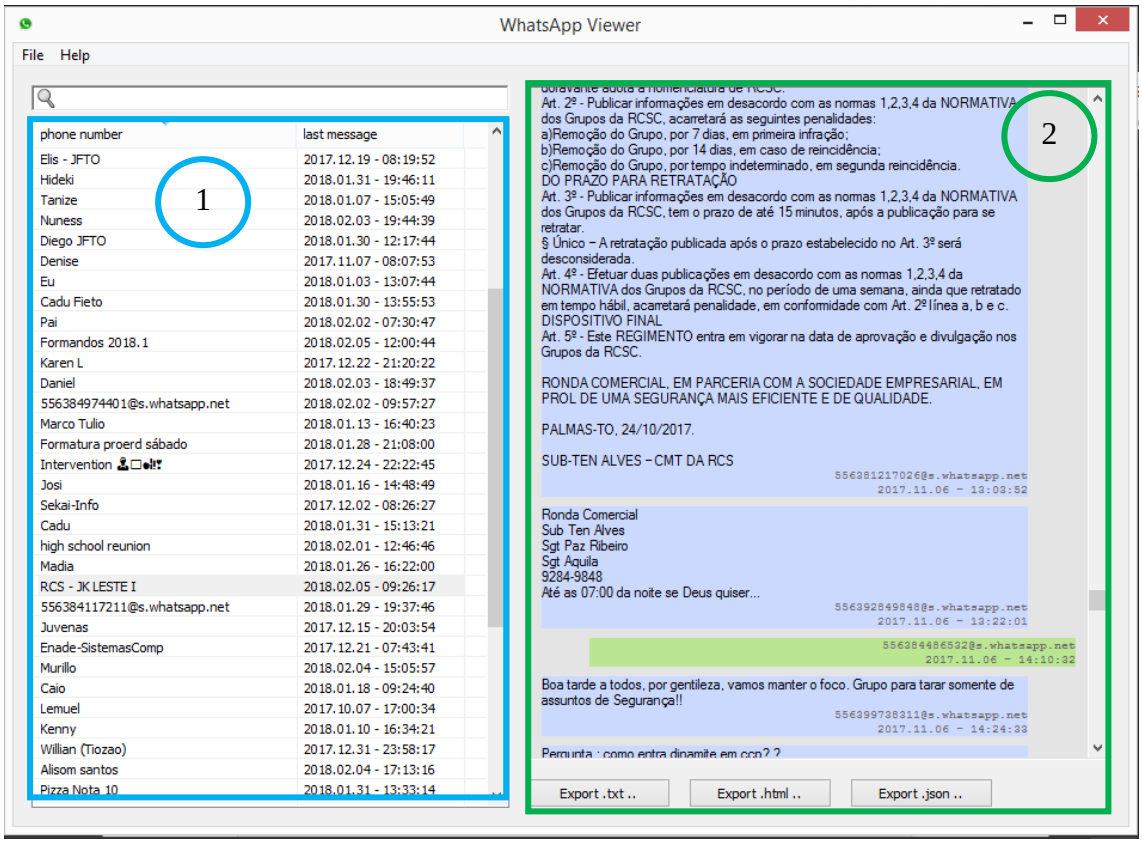
Após a etapa de extração dos bancos de dados, foi necessário utilizar outra ferramenta para analisar os arquivos extraídos. Para isso utilizou-se a ferramenta "WhatsApp Viewer", que permite abrir os arquivos extraídos na etapa anterior. A figura 19 apresenta a tela inicial da ferramenta.

Figura 19: Tela inicial da ferramenta WhatsApp Viewer



Na figura 19, o bloco contornado em vermelho, destacado com a seta, exibe o menu da ferramenta: a opção "*File*" possibilita localizar e abrir os arquivos extraídos, para visualizar os conteúdos; e a opção "*Help*" apresenta informações sobre o *software*. Após abrir o arquivo desejado, o bloco contornado em azul e marcado com a numeração 1 apresentará uma lista de conversas do *WhatsApp.* Já o bloco contornado em verde e marcado com a numeração 2 apresentará as mensagens enviadas e recebidas pelo usuário. A figura 20 apresenta a lista de conversas do *WhatsApp* e as mensagens trocadas, que são apresentadas após a abertura do arquivo "msgstore.db", que é o banco de dados que armazena o *backup* das conversas.

Figura 20: Lista de contatos e mensagens

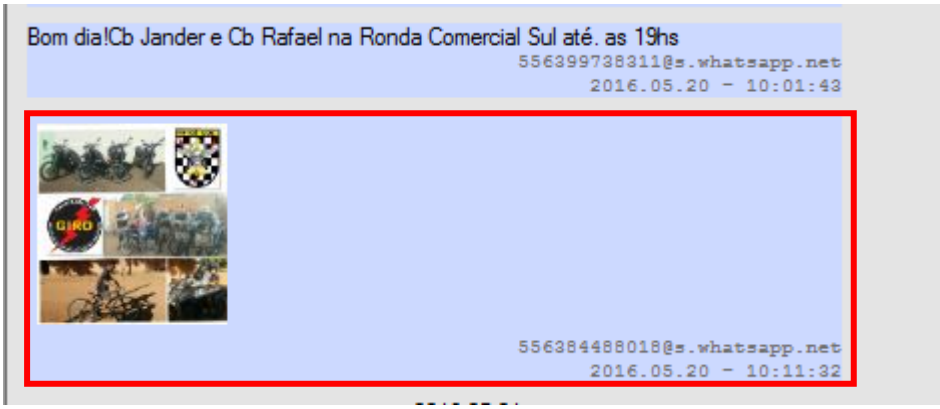


Na figura 20, o bloco contornado em azul e marcado com a numeração 1 exibe uma lista de conversas do *WhatsApp*. Na primeira coluna é apresentada a lista com o número do telefone ou o nome dos contatos com os quais o usuário estava conversando. Na segunda coluna, é exibida a data da última conversa entre os contatos. Ao selecionar alguma das conversas na lista são expostas as mensagens que foram trocadas entre os usuários. O bloco contornado em verde e marcado com a numeração 2 exibe as conversas que foram trocadas

entre o usuário proprietário do *Smartphone* e o contato destacado, RCS – JK LESTE I, que podem ser salvas em arquivos nos formatos “.txt”, “.html” ou “. json”.

Além de apresentar as informações descritas anteriormente, a ferramenta também recupera imagens que foram enviadas ou recebidas pelo *WhatsApp*. A figura 21 exibe algumas imagens que foram recuperadas junto as mensagens.

Figura 21: Imagens recuperadas pela ferramenta



A figura 20 apresenta o arquivo de mídia (imagem) que foi enviado em uma conversa no *WhatsApp*. A área destacada em vermelho apresenta o arquivo de mídia que foi enviado, também apresentando o usuário que enviou a mensagem e a sua respectiva data e hora. Tanto os arquivos de mídias quanto as mensagens de texto são exibidos no bloco contornado em verde e com a numeração 2, conforme apresentando na figura 20.

4.4 COMPARAÇÃO ENTRE AS FERRAMENTAS

Para realizar o paralelo entre as ferramentas utilizadas neste trabalho, foi elaborada uma tabela que elenca os critérios descritos na seção 3.3, que foi formulado levando-se em consideração as funcionalidades das ferramentas e analisando os resultados obtidos em outros trabalhos acadêmicos, apresentados nos anexos deste trabalho.

A tabela 3 mostra a relação entre os critérios que foram definidos (primeira coluna) e as características das ferramentas comparadas, sendo elas a Andriller, Elcomsoft e WhatsApp Key Extractor, respectivamente.

Tabela 3: Tabela comparativa entre as ferramentas preenchida

Critério	Andriller	Elcomsoft	WhatsApp Key Extractor
Licença	Versão de teste	Versão de teste	Gratuito
Criptografia	Sim	Sim	Sim

Mensagens	Sim	Sim	Sim
Mensagens excluídas	Não	Não	Não
Arquivos de mídias	Sim	Sim	Sim
Arquivos de mídias excluídas	Não	Não	Não
Chamadas	Sim	Sim	Não
Contatos	Sim	Sim	Não
Foto de perfil	Sim	Sim	Não
Relatórios	Sim	Não	Sim
Necessidade de o dispositivo estar desbloqueado	Sim	Sim	Sim
Complexidade de uso da ferramenta	Média complexidade	Baixa complexidade	Média complexidade
Compatível com *Android* e iOS	Compatível com *Android* e iOS	Compatível com *Android*	Compatível com *Android*

Conforme apresenta a tabela 3, foram avaliadas a ferramentas de acordo com cada critério definido na primeira coluna. Analisando os resultados da tabela 3, nota-se que em alguns critérios todas as ferramentas obtiveram o mesmo resultado, ou seja, as três ferramentas possuem funcionalidades em comum, como: conseguir realizar decodificação dos arquivos; apresentar as mensagens extraídas do aplicativo; não conseguir apresentar as mensagens que foram excluídas do aplicativo; apresentar arquivos de mídias; não conseguir apresentar os arquivos de mídias excluídos do aplicativo e da necessidade do dispositivo estar desbloqueado para realizar a extração dos dados.

As diferenças entre as funcionalidades das ferramentas é que a Adriller e a Elcomsoft são ferramentas proprietárias, ambas possuindo licença para testes, diferente do WhatsApp Key Extractor que possui licença gratuita para uso. Outra distinção é que as ferramentas proprietárias conseguem recuperar as chamadas, os contatos e as fotos do perfil do *WhatsApp*, já o WhatsApp Key Extractor não possui tal funcionalidade. Além dessas diferenças é possível observar que a Andriller e o WhatsApp Key Extractor conseguem emitir mais de um tipo de relatório, diferente da Elcomsoft que emite apenas um tipo de relatório. As complexidades de uso das ferramentas são diferentes, sendo que a Adriller e o WhatsApp key Extractor possuem média complexidade e a Elcomsoft baixa complexidade. E por fim, a

compatibilidade entre as ferramentas com Andoid e iOS , onde apenas a Andriller é compatível com os dois SOs.

Após utilizar as ferramentas, foi possível notar alguns pontos fortes e fracos de cada uma delas. Esses pontos são apresentados na tabela 4.

Tabela 4: Pontos fortes e fracos das ferramentas utilizadas

Ferramenta	Pontos fortes	Pontos fracos
Elcomsoft	Apresentação das informações extraídas.	Não recupera as informações que foram apagadas do *WhatsApp*
Andriller	Diversidade de funcionalidades.	Forma de apresentação das informações e não recupera informações que foram apagadas do *WhatsApp.*
WhatsApp Key Extractor	Ferramenta gratuita	Depende de outras ferramentas para apresentar os dados extaidos.

Conforme apresentado na tabela 4, as ferramentas utilizadas possuem seus pontos fortes e fracos. A Elcomsoft, por exemplo, tem como ponto forte a apresentação das informações. Ao contrário da Andriller e WhatsApp Key Extractor, que apresentam todos os dados em uma tabela geral, a Elcomsoft exibe os dados extraídos por categoria (chamadas, contatos, mídias e mensagens), facilitando a busca por informações. Além disso, possibilita visualizar os arquivos de mídias, tanto imagens quanto áudio e vídeos de forma clara, característica de grande importância para uma investigação forense. O ponto fraco da ferramenta Elcomsoft é que ela não recupera as informações que foram apagadas do *WhatsApp*, conseguindo recuperar apenas as informações contidas no arquivo de *backup*, ou seja, caso uma informação (mensagens, chamadas ou mídias) tenha sido apagada sem que o *WhatsApp* realizasse o *backup*, essa informação é perdida.

A Andriller possui como ponto forte a diversidade de funcionalidades disponibilizadas pela ferramenta, sendo elas para *Android* ou iOS. Além de conseguir extrair informações dos arquivos de *backup* do *WhatsApp*, recupera as informações de outros aplicativos como *Facebook, Tinder, Skype, Viber,* entre outros. Um ponto fraco da ferramenta é a forma que ela apresenta as mensagens, dificultando a análise das conversas por contato, já que todas as mensagens são apresentadas em uma única tabela. Outro ponto fraco é que ela não recupera informações que foram apagadas do *WhatsApp*, apresentando o mesmo problema mencionando anteriormente sobre a Elconsoft.

O WhatsApp Key Extractor possui como ponto forte ser uma ferramenta gratuita, não sendo necessário adquirir uma versão paga para poder utilizá-la, e, apesar disso, consegue extrair e decodificar os arquivos de banco de dados do *WhatsApp* de forma compatível com as ferramentas proprietárias. O ponto fraco do WhatsApp Key Extractor é que depende de outras ferramentas para apresentar os dados, pelo fato de apenas realizar o processo de extração de decodificação, não realizando a apresentação.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como resultado a comparação entre ferramentas de extração de dados do *WhatsApp* em SO *Android* para investigação forense. Os objetos de estudo foram as ferramentas Elcomsof, Andriller e WhatsApp Key Extractor, das quais foram obtidas informações como: mensagens e arquivos de mídias (áudio, imagem e vídeo) enviadas ou recebidas pelo usuário, além de verificar os contatos salvos no *WhatsApp* e o histórico de chamadas efetuadas ou recebidas no aplicativo.

Os dados recuperados pelas ferramentas podem auxiliar na resolução de crimes pelo fato das informações extraídas poderem apresentar dados como imagens comprometedoras, data de ações ilícitas, conversas sobre atos ilícitos entre outros. Todas as ferramentas utilizadas conseguiram alcançar o objetivo do trabalho, que era apresentar os dados extraídos do *WhatsApp*.

Para verificar as funcionalidades particulares de cada ferramenta e realizar a comparação entre os resultados obtidos, foi realizado um paralelo por meio de uma tabela comparativa, onde foram avaliadas as características individuais através dos critérios de comparação que foram elaborados e são apresentados na seção 3.3. O paralelo entre as ferramentas poderá servir de base para os peritos forenses que buscam ferramentas que realizem extração de dados do WhatsApp em SO Android para que possam o auxiliar em uma investigação.

Dentre as ferramentas utilizadas neste trabalho, foi possível observar que todos os *softwares* recuperavam as informações do *WhatsApp* através dos arquivos de *backups*, ou seja, os dados apagados que não constavam nos arquivos de *backups* não eram recuperados para possível análise. Outra adversidade observada foi a necessidade do dispositivo encontrar-se desbloqueado para que fosse possível realizar a extração dos arquivos de *backup*, pois quando há algum tipo de bloqueio como PIN, não é possível realizar a extração.

Neste trabalho, foram realizadas as extrações de dados do *WhatsApp* apenas em SO *Android*. Para possíveis trabalhos futuros, pode-se realizar o estudo da arquitetura e diretórios do *WhatsApp* em diferentes SO's como iOS e *Windows Phone*, pesquisar for ferramentas que consigam desbloquear os *Smartphones*, tendo em vista que há a possibilidade do aparelho conter uma senha de bloqueio, além de buscar ferramentas mais completas que realizem a extração de dados de *Smartphones* e apresentar suas funcionalidades.

REFERÊNCIAS

COSTA, Marcelo Antonio Sampaio Lemos. **Computação Forense.** 3. ed. Campinas: Millennium, 2011. 158 p.

ELCOMSOFT Explorer for WhatsApp. Disponível em: <https://www.elcomsoft.com/exwa.html>. Acesso em: 27 set. 2017.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** São Paulo: Novatec, 2011. 200 p.

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

HOLPERIN, Marco; LEOBONS, Rodrigo. **Reconhecimento de Evidências.** Disponível em: <https://www.gta.ufrj.br/grad/07_1/forense/reconhecimento.html>. Acesso em: 18 set. 2017.

QUEIROZ, Claudemir; VARGAS, Raffael. **Investigação e Perícia Forense Computacional**: Certificações, Leis Processuais, Estudo de Caso. 2010. Rio de Janeiro: Brasport, 2010.

RICARDO SENRA (São Paulo). BBC Brasil. **Usam WhatsApp para pedofilia, tráfico e assaltos.** 2015. Disponível em: <http://www.bbc.com/portuguese/noticias/2015/02/150227_salasocial_bloqueio_whatsapp_rs>. Acesso em: 26 set. 2017.

ROSLER, Paul; MAINKA, Christian; SCHWENK, Jorg. **More is Less:** How Group Chats Weaken the Security of Instant Messengers Signal, WhatsApp, and Threema. 2017. 29 f. TCC (Graduação) - Curso de Chair For Network And Data Security, Ruhr-universität Bochum, Bochum, 2017. Disponível em: <https://eprint.iacr.org/2017/713.pdf>. Acesso em: 7 nov. 2017.

RONZANI, Maicon Daniel. **Simulação de ferramenta para Perícia Forense em servidor.** 2013. 52 f. TCC (Graduação) - Curso de Tecnólogo em Redes de Computadores, IFC-Instituto Federal Catarinense, Sombrio, 2013. Disponível em: <http://sombrio.ifc.edu.br/download/redes/TCC_2012/TCC_MAICON.pdf>. Acesso em: 10 ago. 2017.

SANDRIM, Alex Masson. **Investigação forense sobre o aplicativo Whatsapp em dispositivo Android.** 2014. 24 f. TCC (Graduação) - Curso de Perícia Digital, Universidade Católica de Brasília, Brasília, 2014. Disponível em: <https://repositorio.ucb.br/jspui/bitstream/10869/5702/1/Alex Masson Sandrim.pdf>. Acesso em: 14 ago. 2017.

SCIENCE, National Commission On Forensic. **Views of the Commission Defining Forensic Science and Related Terms.** 2016. Disponível em: <https://www.justice.gov/archives/ncfs/file/786571/download>. Acesso em: 7 nov. 2017.

SHORTALL, Adam; AZHAR, M A Hannan Bin**. Forensic acquisitions of WhatsApp data on popular mobile platforms**. Sixth International Conference On Emerging Security

Technologies. Canterbury, 10 mar. 2015. Disponível em: <http://ieeexplore.ieee.org/document/7429264/>. Acesso em: 26 out. 2017.

THAKUR, Neha S., **Forensic Analysis of WhatsApp on Android Smartphones** (2013). *University of New Orleans Theses and Dissertations*. 1706. Disponível em: < http://scholarworks.uno.edu/td/1706>. Acesso em: 20 ago. 2017.

ANEXOS

ANEXO A – Representação da tabela comparativa disponibilizado por Sandrim (2014).

Característica	**WhatsApp Extractor**	**UFED 4 PC**
Licença	Gratuito	Pago
Necessidade do dispositivo estar desbloqueado	Sim	Não
Acessa pastas do usuário root	Não	Sim
Apresenta alguma mensagem que foi excluída	Não	Sim
Consegue extrair dados da memória volátil	Não	Sim
Exibe *thumbnail* das imagens enviadas	Sim	Sim
Exibe *thumbnail* da foto dos perfis dos contatos	Não	Sim
Exibe linha do tempo	Não	Sim
Gera relatórios em mais de um formato	Não	Sim
Facilidade de uso	Não	Sim
Necessidade de usuário copiar algum arquivo do dispositivo para o computador	Sim	Não
Compatível com Ios e Android	Sim	Sim

ANEXO B – Representação da tabela comparativa traduzida disponibilizado por Thakur (2013).

	Memoria não volátil (Cartão SD) + não dispositivo de enraizamento	Memoria não volátil (Cartão SD) + rooting	Memoria não volátil (RAM) + rooting do dispositivo
msgstore.db	Encontrado Criptografado	Encontrado Descriptografado	Conteúdo encontrado
wa.db	Não encontrado	Encontrado	Conteúdo encontrado
Número de telefone	Encontrado se db descriptografado*	Encontrado	Encontrado
Mensagens	Encontrado se db descriptografado*	Encontrado	Encontrado
Arquivos de mídia	Encontrado se db	Encontrado	Encontrado

	descriptografado*		
Lista de contatos	Encontrado se db descriptografado*	Encontrado	Encontrado
Localização	Encontrado se db descriptografado*	Encontrado	Encontrado
Consultas SQL	Encontrado se db descriptografado*	Encontrado	Encontrado
Fotos de perfil	Não encontrado	Encontrado	Encontrado
Registro	Não encontrado	Encontrado	Conteúdo encontrado
Estrutura de diretório	Não encontrado	Encontrado	Encontrado
Mensagens deletadas	Não encontrado	Não encontrado	Encontrado
Arquivos de mídias deletadas	Não encontrado	Não encontrado	Encontrado
Android APIs	Não encontrado	Não encontrado	Encontrado

ANEXO C – Representação da tabela comparativa traduzida disponibilizado por Shortall e Azhar (2015).

Dados Encontrados	Android	iOS	WP 8.1
Contatos	✓	✓	×
Mídias	✓	✓	✓
Mensagens Criptografadas	✓	✓	✓
Mensagens Decodificadas	✓	✓	×