Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LEONARDO DE CASTRO PALMA

PERíCIA DIGITAL EM DISPOSITIVOS MÓVEIS ANDROID

Assis/SP
2018

Av. Getúlio Vargas, 1200 – Vila Nova Santana – Assis – SP – 19807-634
Fone/Fax: (0XX18) 3302-1055 homepage: www.fema.edu.br

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LEONARDO DE CASTRO PALMA

PERíCIA DIGITAL EM DISPOSITIVOS MÓVEIS ANDROID

Projeto de pesquisa apresentado ao Curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Leonardo de Castro Palma
Orientador(a): Prof. Me. Fábio Eder Cardoso

Assis/SP
2018

FICHA CATALOGRÁFICA

PALMA, Leonardo de Castro.

PERÍCIA DIGITAL EM DISPOSITIVOS MÓVEIS ANDROID / Leonardo de Castro Palma. Fundação Educacional do Município de Assis –FEMA – Assis, 2018.

Número de páginas.

1. Investigação. 2. Santoku Linux. 3. Perícia Forense. 4. Evidência

CDD: 001.61
Biblioteca da FEMA

PERÍCIA DIGITAL EM DISPOSITIVOS MÓVEIS ANDROID

LEONARDO DE CASTRO PALMA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Me. Fábio Eder Cardoso

Examinador: _____
Dr. Luiz Carlos Begosso

Assis/SP
2018

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus e a minha família e amigos, que me incentivaram nos momentos difíceis e acreditaram em mim para que eu pudesse vencer mais uma etapa na minha vida.

AGRADECIMENTOS

Primeiramente quero agradecer a Deus que em meio as lutas esteve comigo me apoiando e me concedendo sabedoria para continuar.

Aos meus familiares, em especial a minha mãe Silvia Helena Dias de Castro Palma e ao meu pai José Américo de Castro Palma que me incentivaram quando inúmeras vezes pensei em desistir.

Agradeço também a minha querida e amada namorada Laura Silva Candido, que em meio a devaneios e impaciência esteve junto comigo me apoiando e acalmando para que eu prosseguisse.

Aos meus melhores amigos Vinicius Gutierres Mello Fachiani e Igor Delgado que estiveram ao meu lado me ajudando diversas vezes com pesquisas e me incentivando para que eu não desistisse das minhas conquistas

E por ultimo ao meu orientador Fábio Eder Cardoso, pelo empenho, paciência, confiança e pela seriedade em compartilhar seus conhecimentos e experiência para a elaboração deste trabalho.

RESUMO

Nos dias de hoje com a grande evolução da tecnologia em dispositivos móveis, muitas pessoas no mundo todo têm feito o uso dessa plataforma que são os *Smartphones* com o sistema operacional *Android*, gerando assim uma grande quantidade de informações. “A perícia computacional em meios práticos, busca formas de comprovar um crime, coletando provas e evidências digitais em aparelhos suspeitos, auxiliando a justiça esclarecer o delito”. (Eduvales, 2012).

Neste trabalho foram apresentados processos e métodos realizados durante uma análise forense e foram apresentados técnicas na preservação de evidência e a extração de dados analisada pela ferramenta *Santoku* Linux que irá ajudar o profissional da área na investigação em um *smartphone* com sistema *Android.*

Palavras-chaves: Investigação, Ferramenta *Santoku* Linux, Perícia Forense e Evidência.

Abstract

These days with the great evolution of technology on mobile devices, many people around the world have made use of this platform are Smartphones with Android operating system, thus creating a large amount of information. "The computational expertise in practical ways, seeking ways to prove a crime, collecting evidence and digital evidence on suspects, assisting the justice to clarify the offence". (Eduvales, 2012).

This work will be presented procedures and methods made during a forensic analysis and show evidence preservation techniques and data extraction analyzed by Santoku Linux tool will help the professional in research in a Smartphone with Android system.

Keywords: Research, Tool Santoku Linux, Forensics and Evidence.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

ADB – *Android Debug Bridge*

APP – Aplicativo

FBI – *Federal Bureau of Investigation*

GSM – *Global System for Mobile Communications ou Groupe Special Mobile*

GPS – *Global Positioning System*

IrDA – *Infrared Data Association*

MMS – *Multimedia Messaging Service*

NFI – *Netherlands Forensic Institute*

NIST – *National Institute of Standards and Technology*

PDAs – *Personal Digital Assistants*

RAM – *Random Access Memory*

ROM – *Read Only Memory*

SD – *Secure Digital*

SDK – *Software Development Kit*

SMS – *Short Message Service*

SO – *System Operational*

USB – *Universal Serial Bus*

SUMÁRIO

1. INTRODUÇÃO

A computação forense é uma área da computação científica na qual o objetivo é examinar dispositivos computacionais procurando preservar, identificar, recuperar e apresentar evidências digitais que possam provar crimes tecnológicos. Estes dispositivos são destacados por computadores, *notebooks, laptops*, *tablets*, *telefones celulares, máquinas fotográficas* dentre outros. De acordo com (GROSSMAN, 2015) o número de linhas ativas de telefones celulares, em 2015, é estimado em pouco mais de 7,1 bilhões, com isso, o telefone celular é um importante ativo da análise forense.

Hoog (2011) descreve que, desde 2011 o sistema operacional *Android* tem se tornado o dispositivo móvel mais popular do mundo. Sendo assim é normal que a quantidade de aparelhos apreendidos para perícia seja proporcionalmente grande. O sistema operacional *Android* possui um recurso interno usado para segurança do mesmo que é o bloqueio de tela com senha numéricas, alfanuméricas, padrões, dentro outros. Os desenvolvedores *Android* usam de um recurso para poder fazer o acesso ao telefone celular por meio de um computador, este recurso é a ativação da depuração USB, usada também pelos peritos criminais, para fazer a extração de dados como imagens, vídeos, mensagens.

O perito, quando recebe o dispositivo para ser analisado, inicialmente realiza a extração dos dados do aparelho para o computador, de forma que haja toda cautela para preservar o artefato original. “Existem duas formas para extração, a forma física e a lógica. A extração física é mais complexa, pois envolve *hardwares* especiais e conhecimento em eletrônica” (HOOG,2011). A extração lógica é feita por meio de *softwares* que se conectam ao dispositivo utilizando a aplicação *Android Debug Bridge* (ADB), serviço usado no *Android* quando a função depuração USB está ativada. Sendo assim, existem várias técnicas e ferramentas para executar a extração de dados utilizando da depuração USB. Porém, ocorre um problema quando essa opção está desabilitada e não é possível habilitá-la, tornando o trabalho do perito mais difícil, impedindo, assim, a extração dos dados.

O presente trabalho abordou pesquisas em sistema de arquivo e dados armazenados como imagens, vídeos e mensagens.

1.1. OBJETIVO

O objetivo desse trabalho foi explanar conceitos voltados à Perícia Forense Computacional, e suas áreas de análise pericial em dispositivos móveis, mostrando por meio de um estudo de caso, alguns procedimentos necessários e as principais técnicas e exames periciais no dispostivo, sendo assim extraindo as possíveis informações de acordo com cada equipamento utilizado na hora do teste, mostrando também como um examinador deve seguir de forma clara e bem definida, metodologias e procedimentos em determinadas situações de uma análise forense, procurando instigar a curiosidade e a busca por conhecimento do leitor pela área.

1.2. JUSTIFICATIVAS

Hoje existe uma quantidade muito vasta de funcionalidades disponiveis em um aparelho celular, e com isso proporciona ao examinador um grande desafio na hora da análise forense que necessita avançar por vários obstaculos, a fim de acompanhar os avanços tecnologicos.

Neste estudo foram abordadas práticas de perícia, visando principalmente o processo de recuperação de mensagens SMS (*Short Message Service)* e MMS (*Multimedia Messaging Service)*, mostrando a importância de utilização de técnicas corretas bem como de procedimento homologados e bem fundamentados, de acordo com a metodologia de análise pericial aceitas pelas entidades profissionais, procurando o melhor conhecimento necessário para conduzir muito bem uma investigação forense.

1.3. MOTIVAÇÕES

O aumento excessivo de ações ilícitas e crimes digitais realizadas no uso dos aparelhos *Smartphones* e com pequena quantidade de profissionais capacitados nesta área, faz-se necessário o estudo e o aprimoramento de conhecimentos, métodos e ferramentas de perícia forense, pois com as novas técnologias do mundo de hoje, novos desafior e técnicas precisam ser desenvolvidas.

1.4. PERSPECTIVA DE CONTRIBUIÇÃO

A perspectiva de contribuição é levar ao público um pouco mais de conhecimento sobre Perícia Forense Computacional, e espera-se que o Brasil possa invertir mais nesta área no combate de identificar, julgar e penalizar a prática de crimes virtuais, e quer no futuro possa vir servir de fonte de pesquisa.

1.5. METODOLOGIA DE PESQUISA

Para atingir os objetivos propostos nesta pesquisa, uma metodologia foi definida com base em pesquisas na Internet a partir de apostilas, artigos, sites e trabalhos de conclusões e também vai ser utilizado para a extração e análise de dados o sistema operacional *Santoku* versão 0.5 – Lubuntu. Portanto, foram analisadas características em *Smartphones* para ser realizada a perícia forense em dispositivos móveis.

Um dos métodos proposto para realizar uma análise pericial em um *smartphone* será baseado nas melhores práticas utilizadas pela Polícia Federal do Brasil, por meio de pesquisas para conclusões de análise.

1.6. RECURSO NECESSÁRIOS

Foram analisados recursos para realizar este trabalho, que foi o levantamento de obras de qualidade produzidas por profissionais bastante conhecidos na área, o trabalho foi elaborado com um Computador, uma Máquina Virtual e a ferramenta *Santoku* versão 0.5 – Lubunto Linux.

1.7. ESTRUTURA DO TRABALHO

Este trabalho apresenta alguns procedimentos necessários para uma análise forense perfeita em *smartphone*.

Ele foi composto de seis capitulos divididos em:

O Capítulo 1 apresenta a introdução e os objetivos da pesquisa para poder efetuar um trabalho bem elaborado.

O capítulo 2 abrange um pouco do conceito de computaçao forense, falando um pouco sobre sua evolução, sobre definições forense, mostrando um pouco dos trabalhos de alguns profissionais e também sobre a sua legislação.

O capítulo 3 será abordado sobre os dispositivos móveis e coleta de dados digitais, procedimentos de busca, apreensão e preservação, aquisição de dados e um pouco sobre memórias dos dispositivos móveis.

O capítulo 4 é a parte que vai referenciar a perícia forense em *Android*, apresentando algumas metodologias e softwares utilizados para a extração. Traz por sua vez especificações sobre o comando ADB.

O capítulo 5 abordará um pouco do cenario forense com metodologias. Mostra também como configurar uma maquina virtual e como fazer a instalação da ferramente *Santoku*, e por fim nos mostra como fazer a extração completa de dados.

Por fim, o capítulo 6 apresenta as conclusões do trabalho.

2. COMPUTAÇÃO FORENSE

O objetivo da computação forense é em base criar metodologias e também acumular conhecimentos para a obtenção, manipulação e análise de proeminências mostrando se houve ou não atividades ilegais.

De Acordo com Freitas (2006):

> A perícia forense computacional, também conhecida como computação forense, informática forense ou forense digital, dentre outros termos, tem ganhado importância cada vez maior para as autoridades policiais e judiciárias, assim como para empresas e organizações, à medida que utiliza conhecimentos em informática aliados a técnicas de investigação a fim de obter evidências sobre a ocorrência de incidentes de segurança em sistemas computacionais. A forense computacional propõe métodos científicos para identificar, coletar, preservar, analisar e documentar evidências digitais em dispositivos eletrônicos.

A perícia forense por sua vez tem como objetivo não só analisar os dados, mas também prezar pela integridade dos mesmos, fazendo então uma extração limpa sem qualquer falha ou dano de dados.

2.1. A EVOLUÇÃO

“No século XIII, através dos Decretos do Papa Gregório IX, eram determinadas perícias médicas nos casos de morte violenta, lesões corporais, cujas consequências pudessem ser de interesses jurídicos” (GONZÁLES,2004).

Dentre as evoluções forense teve também no século XX, onde o cientista Leone Lattes descobriu que os tipos sanguíneos poderiam ser divididos em grupos de acordo com características próprias.

De acordo com (PROBST et al, Qperito.com):

> A partir dessa pesquisa surgiram os grupos sanguíneos A, B, AB e O. Já nesta época esses grupos passaram a auxiliar as ciências forenses na identificação de criminosos, quando a cena do crime continha evidências de sangue. Essa prática permitiu diminuir a quantidade de suspeitos simplesmente a partir de uma análise de seus tipos sanguíneos. Também no início do século XX, Calvin Goddard desenvolveu um estudo comparando diferentes projéteis de armas de fogo. Este estudo possibilitou a detecção da arma que disparou o projétil existente em uma cena de crime e tornou-se um marco para a solução de inúmeros casos julgados. No mesmo período, Albert Osborn desenvolveu uma pesquisa sobre as características e metodologias para análise de documentos, o que ajudou a identificação e comprovação de fraudes e falsificações.

A investigação digital surgiu na década de 80, constituindo que em 1984 veio a ser criado o programa de investigação dentro do FBI. Este era um programa muito conhecido por ser um grupo de análises e estudo sobre mídias magnéticas. Logo depois de alguns anos da criação do programa o agente especial Michael Anderson, o grande “Pai da Forense Computacional” entrou para o quadro de especialista deste programa.

Na década e 90 este agente especial Michael Anderson trabalho no programa, mas posteriormente começou sua própria empresa de investigação forense. “O termo Forense Computacional foi mencionado pela primeira vez em 1988, no primeiro treinamento realizado pela Associação Internacional de Especialistas em Investigação Computacional (IACIS) em Portland, Oregon” (ARTHUR, 2004).

Os cientistas estudaram, pesquisaram e desenvolveram alguma prática forense, sem medir esforços para que de alguma maneira eles pudessem contribuir com descobertas para o avanço e qualificação de profissionais para gerações posteriores. Logo após muito tempo a estes estudos, conceitos e bases sobre perícia continuam muito atuais e vastamente é utilizadas em um longo processo investigativo. Uma das principais diferenças nos dias de hoje são sem dúvida os equipamentos utilizados para a perícia, e o também fortemente o

conceitos que por sua vez estão mudando devido a chegada da informática e o grande número de informações em que hoje se trabalha. Hoje os cenários dos crimes estão muito além de sangue, fios de cabelo, fluidos corporais e corpos físicos, mas também em identidades virtuais e informações contidas através dos números binários.

2.2. DEFINIÇÕES FORENSE

Pelo vasto surgimento de crimes envolvendo o meio computacional, foi necessário por sua vez o desenvolvimento da perícia forense computacional.

De acordo com Bustamante (2006):

> A perícia forense pode ser definida como coleção e análise de dados de um computador, sistema, rede ou dispositivos de armazenamento, de forma que sejam admitidos em juízo, sendo que as evidências que um criminalista ou expert (também chamado perito) encontra geralmente não podem ser vistas a olho nu, dependendo de ferramentas e meios para a sua obtenção. Nesse contexto, cabe ao profissional de informática coletar as evidências e produzir um laudo pericial com as evidências e técnicas abordadas na coleta.

Um dos destaques da Forense Computacional é a inspeção cientifica e sistemática em ambientes computacionais, com o objetivo de granjear evidências derivadas de fontes digitais, tendo como um dos principais objetivos promover a reconstituição dos eventos encontrados.

A perícia forense tem como objetivo desenvolver metodologias e acumular grandes conhecimentos para adquirir, manipular e analisar evidências digitais.

De acordo com Vargas, Quintão e Grizendi (2007):

> A Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, que podem ser os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.

Hoje todos os dias novas tecnologias surgem e por isso são necessárias as preocupações com segurança, novas especificações, novos padrões, e antes mesmo de começar uma implementação de uma nova tecnologia segura, é preciso estudar e procurar maneiras, métodos, e habilidade para desvendar o novo objetivo com um equipamento e com mais segurança.

A forense computacional em 2007 era uma área de pesquisa muito recente e eram poucos os trabalhos sobre esse assunto no Brasil. Nos dias de hoje pode se dizer que a área está mais forte e proporcionando mais trabalhos.

2.3. PROFISSIONAL DA PERÍCIA FORENSE

Um bom profissional ou equipe de trabalho, deve ser montado com profissionais capacitados que conheçam o máximo possível das tecnologias da informática, e pessoas que tem o desejo de se capacitar a cada novo trabalho de investigação, levantamento e preservação das provas materiais.

Segundo Beebe e Clark (2005):

> O profissional da área de perícia forense computacional precisa estar atento aos detalhes, bem como nos procedimentos, quanto as escolhas de melhores práticas na conduta de uma investigação, de forma sistemática e cuidadosa com as evidências. As investigações digitais, sejam de natureza forense ou não, devem ter o rigor científico e seguir processos padronizados, pelas facilidades que eles propõem.

A habilidade de um perito de um perito digital é algo que faz parte do seu dia a dia, pois em seu trabalho lida com códigos binários que formam arquivos e para isso é necessário que se tenha conhecimento para se fazer a análise.

Com base há uma grande variedade de assuntos que envolve a perícia no sistema computacional, a figura 1 ilustra o mapa mental de um perito.

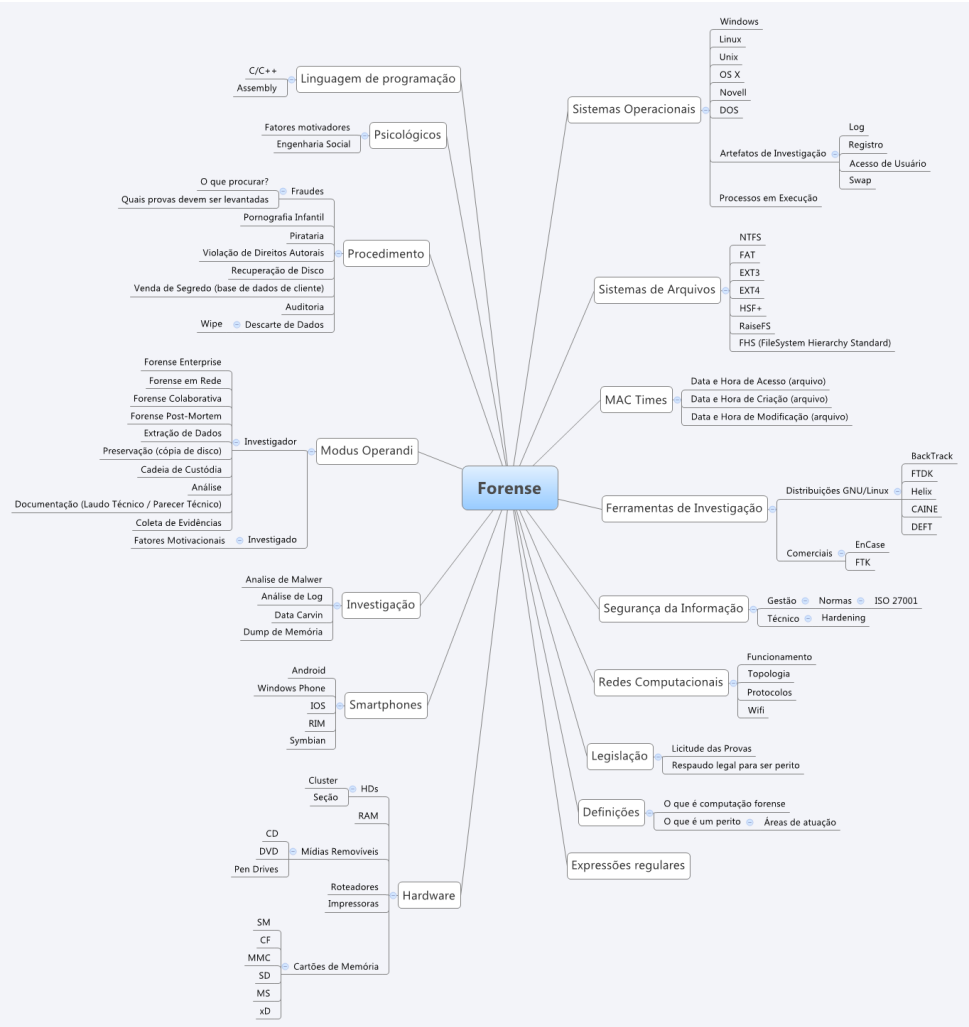

Figura 1 - Mapa mental conhecimento perito forense computacional (https://4en6br.files.wordpress.com/2012/05/forense1.png)

“Para se trabalhar com forense computacional é bom ter, não somente, uma visão superficial e sim uma visão mais profunda das armas reais e das armas hipotéticas possíveis” (VARGAS, 2007).

2.4. LEGISLAÇÃO

A legislação vigente sobre crimes que são cometidos com computador não possuem nenhuma tipificação própria.

Na atualidade apelidada de “Lei Carolina Dieckmann”, a Lei nº 12.737, de 30 de novembro de 2012, entrou em pleno vigor no dia 3 de abril de 2013, alterando o Código Penal para tipificar os crimes cibernéticos propriamente ditos (invasão de 1dispositivo telemático e ataque de denegação de serviço telemático ou de informação), ou seja, aqueles voltados contra dispositivos ou sistemas de informação e não os crimes comuns praticados por meio do computador. Colateralmente equiparou o cartão de crédito ou débito como documento particular passível de falsificação (MPSP.MP.BR).

Assim, a lei citada acima penaliza as condutas de invasão de dispositivo informático:

- Invadir dispositivo informático alheio de qualquer espécie, conectados ou não em rede, desde que violado mecanismo de segurança (senha, firewall etc.), desde que tenha como finalidade obter, adulterar ou destruir dados ou informações.
- Instalar no dispositivo qualquer software de vulnerabilidade com o intuito de obter uma vantagem ilícita (patrimonial ou não).
- Fazer qualquer tipo de comercio de dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivos ou a instalação de vulnerabilidade.
- A penalização desses crimes vai de 6 (seis) meses a 2 (dois) anos de reclusão e multa, caso a conduta não configure outro crime mais grave, quando a invasão resultar a obtenção de conteúdo de comunicação eletrônicas privadas, segredos comerciais ou industriais, informações definidas em lei como sigilosas. Se houver qualquer tipo de divulgação, comercialização das informações obtidas, a pena do crime qualificado será também aumentada de 1/3 a 2/3.

Como visto acima, a Lei nº 12.737/2012, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores.

Os crimes cibernéticos são como uma porta de entrada para o abuso de outras condutas criminosas, deixando de livre acesso a utilização do computador como instrumento para cometer crimes.

2.5. EVIDÊNCIAS

A evidência digital abrange periféricos e dispositivos ligados à cena do crime, aonde com isso pode coletar e averiguar dados ali contidos, seja tanto um computador, ou um dispositivo móvel.

A evidência digital não deixa de ser um tipo de evidência física, embora não seja palpável. “Este tipo de evidência é formado por campos magnéticos, campos elétricos e pulsos eletrônicos que podem ser coletados e analisados através de técnicas e ferramentas de perícia digital” (LISITA; MOURA; PINTO, 2009).

A ACPO em seu segundo princípio, em um exame mais especifico onde há necessidade de extração de informação direta do dispositivo, o examinador deve ter as competências e expertise necessárias a fim de obter a informação e explicar a relevância e implicações dos procedimentos utilizados. Os aparelhos celulares possuem diferentes softwares, hardwares e funcionalidades, e com isso é importante escrever os métodos e procedimentos específicos para cada aparelho.

2.6. CADEIA DE CUSTÓDIA

O Departamento de Justiça dos Estados Unidos (MUKASEY, SEDGWICK e HAGY, 2001), recomenda, dentre outros, os seguintes pontos chaves ao se aproximar de uma cena de crime digital:

- Proteger e avaliar a cena: Devem ser tomadas medidas que garantam a segurança das pessoas; identificar e proteger a integridade das potenciais provas;
- Documentar a cena: Deve-se criar um registro permanente da cena, registrando precisamente tanto provas digitais quanto provas convencionais relacionadas;

- Coletar as evidências: Deve-se coletar evidências tradicionais e digitais, preservando sua integridade e valor provatório;
- Embalar, transportar e Armazenar: Deve-se tomar precauções adequadas para embalar, transportar e armazenar as evidências, mantendo sempre a cadeia de custódia.

Segundo Lopes, Gabriel e Bareta (2006):

> Todos os procedimentos relacionados à evidência, desde a coleta, o manuseio e análise, sem os devidos cuidados e sem a observação de condições mínimas de segurança, podem acarretar na falta de integridade da prova, provocando danos irrecuperáveis no material coletado, comprometendo a idoneidade do processo e prejudicando a sua rastreabilidade.

3. DISPOSITIVOS MÓVEIS E PERÍCIA

Na Publicação Especial 800-101 do NIST (*National Institute of Standards and Technology*) (JANSON e AYRES 2007) os autores mostram que para ter um sucesso na análise forense de dispositivos móveis é saber compreender e aperfeiçoar as características de *hardware* e *software* dos aparelhos celulares. Por muitas vezes os dados do usuário e suas atividades efetuadas por meio de celulares são por sua vez uma fonte muito valiosa de provas em uma investigação. Portanto, para se ter uma produção de provas realizada com sucesso, existem um conjunto de características obtido a partir da maioria dos celulares como por exemplo: microprocessador, memória ROM, memória RAM, módulo de rádio, processador de sinal digital, alto falante, tela, sistema operacional, bateria, PDAs, GPS, câmera, entre outros recursos.

A aquisição de dados a partir de um dispositivo pode ser física como também lógica.

De acordo com Jansen e Ayres (2007):

> A aquisição física tem vantagens sobre a aquisição lógica, uma vez que permite que os arquivos apagados e alguns dados restantes possam ser examinados, por exemplo, na memória não alocada ou em espaço do sistema de arquivos.

E como vimos os profissionais recomendam sempre fazer o método físico antes de fazer o lógico.

Hoje as melhores práticas de análise forense definem procedimentos para apreensão, aquisição, exame e documentação (geração de relatório/laudo). “Estas etapas são importantes, entretanto, existe um histórico de terem sido definidas a partir de procedimentos utilizados em forense de computadores” (OWEN, THOMAS e MCPHEE, 2010).

Segundo (ISFS, 2009):

> O objetivo de ter um conjunto de melhores práticas e metodologias é estabelecer parâmetros e princípios de qualidade e abordagens para obtenção, identificação, preservação, recuperação, exame, análise e uso das evidências digitais. Altos padrões de qualidade e consistência são vitais para manter o valor probatório dos elementos encontrados em uma investigação digital.

Existem princípios fundamentais para um exame forense e são separados em alguns fatores:

- Fatores Chaves: Manter a integridade e a autenticidade dos dados; preservar e minimizar riscos de contaminação dos dados; criar uma documentação apropriada e abrangente, implementar metodologias sistemáticas e com bases científicas.
- Principais responsabilidades dos peritos: Manter a objetividade; apresentar fatos com precisão e não reter quaisquer conclusões que possam distorcer ou depurar fatos; opinar somente com base no que se pode demonstrar; nunca mentir em suas qualificações e estar disposto a trabalhar em equipe, quando o caso exigir.

Na realização de um exame forense, o profissional deve:

- Aplicar todas as regras e princípios gerais de como lidar com as evidências digitais;
- Não executar qualquer ação que possa mudar provas encontradas;
- Certificar-se de que apenas pessoas qualificadas possam acessar as evidências digitais;
- Documentar todas as atividades relacionadas com a apreensão, acesso, armazenamento e transferência de evidências digitais e preservar um registo. Qualquer terceiro que seja relacionado à investigação deve ser capaz de examinar os procedimentos documentados e repetir o processo, alcançando o mesmo resultado;
- Garantir que as melhores práticas de Forense Computacional sejam cumpridas.

3.1. BUSCA, APREENSÃO E PRESERVAÇÃO

Antes de extrair os dados de um aparelho celular, deve-se fazer a correta preservação do dispositivo para que chegue a um analista pericial na melhor condição possível para se realizar o exame. A apreensão tem o objetivo de preservar as evidências muito bem evitando a perda ou a alteração da prova a ser apreendida. Também envolve a busca por mídias eletrônicas que possam possuir informação útil a respeito do que está sendo investigado. A parte mais importante numa investigação é preservar de uma forma adequada todos os dispositivos que foram apreendidos, sendo assim deixando tudo documentado conforme com o Código de Processo Penal Brasileiro (Brasil, 2003) e os normativos vigentes (DITEC/DPF, 2010).

Segundo o Departamento de Justiça Norte Americano (ASHCROFT, 2001), na etapa de apreensão, a equipe tem o dever de avaliar e preservar a cena, documenta-la, coletar as evidencias, realizar o acondicionamento, transporte e armazenamento da evidencia de forma confiável, evitando danifica-la privando pela sua preservação.

Após a apreensão de um dispositivo móvel, é muito importante isolar o aparelho de qualquer tido de comunicação de rede, pois assim evita que os dados que são recebidos após a apreensão não sobrescrevam os dados já existentes. Alguns aparelhos celulares têm por costume apagar os SMS antigos assim quando a nova chega quando a caixa está muito cheia. Uma opção bastante usada por especialista é a ativação do modo avião (*off-line*) que assim deixa o aparelho totalmente bloqueado para qualquer tipo de comunicação usando somente quem está de posse dele, no caso o investigador. Outra opção é o invólucro que bloqueia o recebimento dos dados para acondicionamento ou deve-se desligar o aparelho no momento em que for apreendido.

Cada uma das três alternativas tem sua vantagens e desvantagens, que devem ser levadas consideração a depender do caso ou alvo investigado. O desligamento do dispositivo pode dificultar o seu acesso quando da realização dos exames, uma vez que códigos de autenticação podem ser solicitados quando reiniciado. Já o isolamento em uma sacola de bloquei de sinal, pode aumentar significativamente o consumo da bateria do dispositivo, uma vez que o mesmo aumentará a potência de sua antena para tentar encontrar uma torre mais distante (*Association of Chief Police Officers,* 2008). A ativação do modo avião exigirá

uma interação de um agente da lei com o dispositivo, sendo q nem sempre esta pessoa está habilitada para realiza-la, o que feriria uma das premissas da preservação, uma vez que o dispositivo só poderia ser manuseado por uma pessoa habilitada, pois uma interação antes da realização dos exames pode não ser adequada.

3.2. AQUISIÇÃO DE DADOS

Quando é feito uma aquisição de dados, o mesmo é feito em um ambiente totalmente isolado da rede de comunicação do dispositivo, e é feito isso através de hardware e software adequados para obtenção de dados.

No momento da extração o examinador não pode esquecer de verificar se o dispositivo está se comunicando com a rede de telefonia ou realizando conexões com a rede WI-FI, Bluetooth, IrDA (Infravermelho), se caso esteja se comunicando deve-se para imediatamente antes de começar a extração.

O perito deve iniciar os trabalhos de extração de preferencia com a bateria do celular totalmente carregada ou com o carregador ligado na energia para evitar perca de dados.

A interação do telefone celular com os softwares forenses deve ser a menor possível, por isso deve-se tentar estabelecer uma conexão primeiramente via cabo) USB ou portas seriais ou paralelas), depois infravermelho, *bluetooth* e por último Wi-Fi (*Association of Chief Officers*, 2008).

De acordo com Simão (2011):

> Em algumas situações, tais softwares podem não funcionar adequadamente em alguns equipamentos, sendo necessária a extração com a utilização dos aplicativos proprietários dos fabricantes do dispositivo móvel ou uma extração manual do conteúdo, que deve ser realizada por analista pericial com conhecimentos específicos sobre a plataforma do telefone celular em questão.

“O chip ou cartão SIM (*Subscriber Identity Module*) é um cartão inteligente que possui microprocessador, usado para implementar segurança (autenticação e geração de chaves criptografadas” (QUIRKE, 2004).

Ainda Segundo Quirke (2004):

> Além das informações de habilitação da rede de telefonia celular contidas em um chip, este é capaz de armazenar dados correspondentes à agenda telefônica, últimas chamadas, mensagens de texto, dentre outros. Cada chip possui um código IMSI (*International Mobile Subscriber Identity*), que é um código único, de 15 dígitos, utilizados para identificar um único usuário em rede GSM (*Global System for Mobile Communications / Group Special Mobile*).

3.3. FERRAMENTAS DE EXTRAÇÃO

É de inteira importância que sejam seguidos alguns critérios fundamentais para ferramentas forenses, pois deve apresentar dados de tal forma que sejam uteis e necessários ao investigador.

Hoje alguns critérios são fundamentais para ferramentas forenses, devendo apresentar dados de tal forma que sejam uteis e necessários ao investigador, com a finalidade de determinar ou não a autoria e culpabilidade; ser precisa, determinística, apresentando os mesmos resultados da mesma entrada, e verificável, garantindo a precisão da saída, fornecendo acesso a etapas intermediarias e apresentação dos resultados. Tudo isso de acordo com Janson e Ayres (2007).

Devido à grande diversidade de dispositivos, modelos, versões e fabricantes, e à necessidade do mercado de ter ferramentas forenses atualizadas e compatíveis com sua realidade, as ferramentas forenses devem ser validadas por uma equipe de examinadores.

Segundo Simão (2011):

> Pode haver situações em que uma determinada ferramenta pode ser muito útil na extração dos dados de uma agenda, entretanto pode falhar na recuperação das datas dos registros e até mesmo conseguir extrair com sucesso os dados de um modelo específico e não obter sucesso em outros

> modelos. Com a chegada ao mercado de aparelhos sem fabricantes conhecidos, e de baixo custo, a adequabilidade e compatibilidade das ferramentas forenses podem não conseguir acompanhar a realidade do mercado, devendo o examinador conhecer a ferramenta forense, estando apto a observar comportamentos não desejáveis que não se adequem aos critérios definidos.

3.4. MEMÓRIAS DO DISPOSITIVO

Os dispositivos móveis têm em sua estrutura de hardware memórias voláteis e não voláteis. Toda estrutura do sistema dos aparelhos utiliza memória para armazenar dados relativos aos aplicativos instalados, assim como informações relativas ao próprio Sistema Operacional.

Hoje cada fabricante e modelo podem utilizar uma versão de sistema operacional, alterando a forma com que são armazenadas informações de agenda, textuais, imagens, vídeos, calendários e registros de chamadas. Informações que usualmente são focos das extrações. Diz Simão (2011).

4. FORENSE EM ANDROID

Todo tipo de exame forense necessita ter informações detalhadas sobre a plataforma na qual especialistas iram examinar. Conceitos teóricos, arquitetura, recursos, ferramentas utilizadas, detalhes sobre segurança e funcionalidade de plataforma, são algumas das informações indispensáveis para um perito mesmo antes da realização de qualquer análise forense.

Sobre as amplas literaturas especializadas, está entre elas (Simão, 2011) e (Hoog, 2011), afirmam que em uma análise forense em dispositivos móveis, sobretudo aqueles com a plataforma *Android*, é praticamente impossível que não haja algum impacto ao dispositivo, pois quase todos os procedimentos necessários nos diversos cenários para um exame forense, o perito certamente vai impactar o dispositivo ou de seus dados de alguma forma. Isto por sua vez concretiza a importância da documentação adequada e dos registros das ações tomadas pelo perito em todas as fases de uma metodologia.

Com o crescimento de dados possíveis de extração é importante entender como estas informações podem estar dispostas e quais são elas.

De acordo com Hoog (2011):

> Os aplicativos instalados no Android podem armazenar informações de cinco maneiras: por meio de preferências de compartilhamento, que são basicamente arquivos XML (Extensible Markup Language); por meio de armazenamento interno, armazenamento externo e por meio do banco de dados SQLite.

Existe um vasto número de ferramentas disponíveis para a extração e análise forense em dispositivos móveis, inclusive para os que utilizam *Android*, entre elas as ferramentas forenses comerciais e ferramentas *open-source*.

Figura 2 - Imagem de Cellebrite - UFED Touch Ultimate

Fonte:< http://www.bitmag.com.br/2017/04/solucoes-cellebrite-agilizam-investigacoes-forenses-por-meio-de- tecnologia-analitica/ > Acesso em: 04AGO18.

Atualmente o *UFED Touch Ultimate*, é umas das ferramentas comerciais que permite a extração, decodificação, análise e criação de relatórios tecnologicamente mais avançados a partir de dados móveis, realizando a extração física, lógica, de sistemas de arquivos e de senhas de todos os dados, mesmo os que foram excluídos, de uma ampla gama de dispositivos acelerando o processo de investigação, atendendo as necessidades do setor forense móvel.

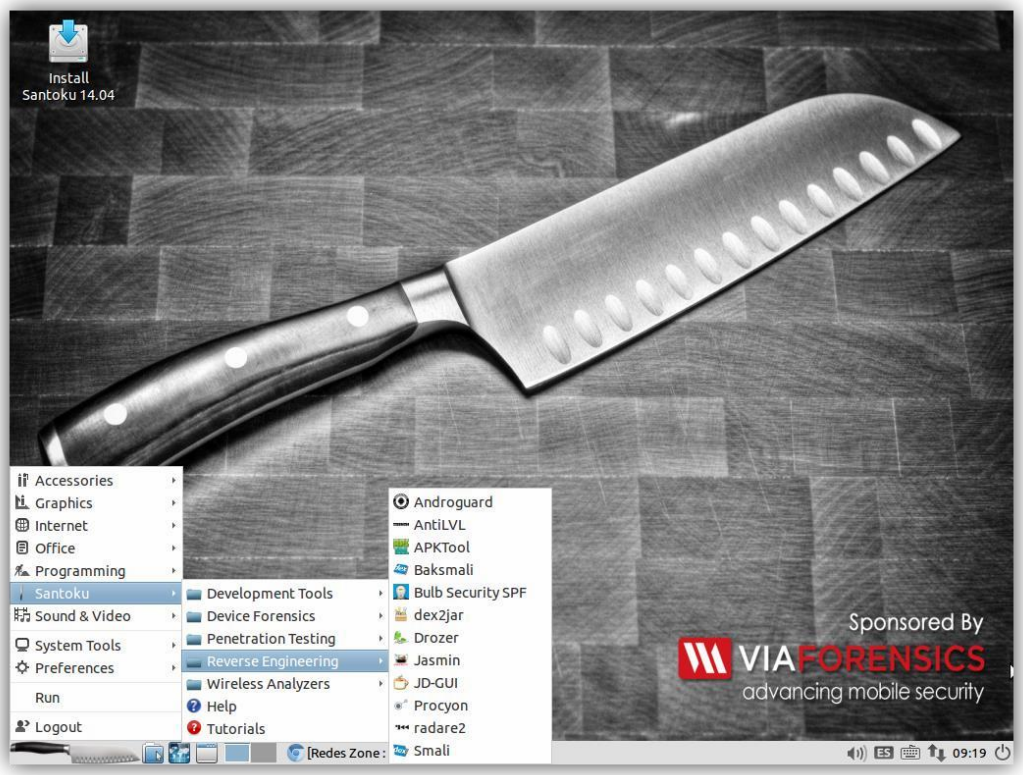

Figura 3 - Sistema Operacional Santoku – Lubunto

Fonte: (https://www.redeszone.net/app/uploads/2015/03/Santoku-Linux-foto-1.png**).**

Já o Linux Forense permite soluções alternativas pelo fato de ser um software livre, que contém diversos recursos para cada necessidade. O *Santoku* Linux uma plataforma operacional baseada no Ubunto que foi desenvolvida pela organização *Via Forensic* com todo foco voltado exclusivamente para análise de telefone celulares para adquirir e analisar dados em múltiplos aparelhos, ferramentas de imagem, cartões de mídia, e memória RAM, emuladores de dispositivos móveis, simulador de rede para análise dinâmica, ferramenta de decodificação, acesso a dados de *malware* e scripts para descompactar dados.

De acordo com Jansen e Ayres (2007):

> Embora a maioria dos peritos e examinadores tenham sua coleção de ferramentas, tanto aceitas, quanto as ferramentas sem aceitação

> ou de desenvolvimento próprio, ao considerar o uso de cada uma delas, o cuidado com o impacto dos procedimentos tomados durante o exame é essencial. Em alguns cenários, as ferramentas não validadas podem ser o único meio de recuperar dados relevantes em um dispositivo.

No entanto para que os infratores que cometem crimes computacionais sejam punidos a perícia forense em informática conta com as ferramentas que auxiliam na busca e padronização de evidências, sendo algumas ferramentas de âmbito comercial ou software livre.

4.1. METODOLOGIA PARA AQUISIÇÃO DE DADOS

A metodologia para aquisição de dados evidenciado nesta seção foi desenvolvida por (Simão, 2011) considerando as características do *Android* e baseada nas melhores práticas utilizadas atualmente pela Polícia Federal do Brasil, pelo NIST (Jansen e Ayres, 2007).

Segundo Lessard e Kessler (2010):

> O Android está cada vez mais poderoso, complexo, com múltiplas funcionalidades, bem estruturado e com implementações constantes. A padronização de métodos e procedimentos poderá transformar a forense em dispositivos móveis um processo mais simples, preciso e menos demorado.

Pelos diversos cenários apresentados, e os respectivos procedimentos a serem adotados por um perito.

De acordo com Simão (2011):

> O método foi proposto com o objetivo de obter a maior quantidade de informações possíveis, levando em conta a preocupação com a documentação e os processos de extração e análise das evidências digitais de forma segura e com o mínimo de intervenção possível.

Pelo *Android* ser em vista uma ferramenta muito complexa, o perito necessita levar em consideração a padronização de métodos e procedimentos para fazer a extração dos dados de forma segura.

De acordo com (Simão, 2011), na Figura 4 mostra a etapa para aquisição de dados de um telefone celular com sistema operacional *Android.*

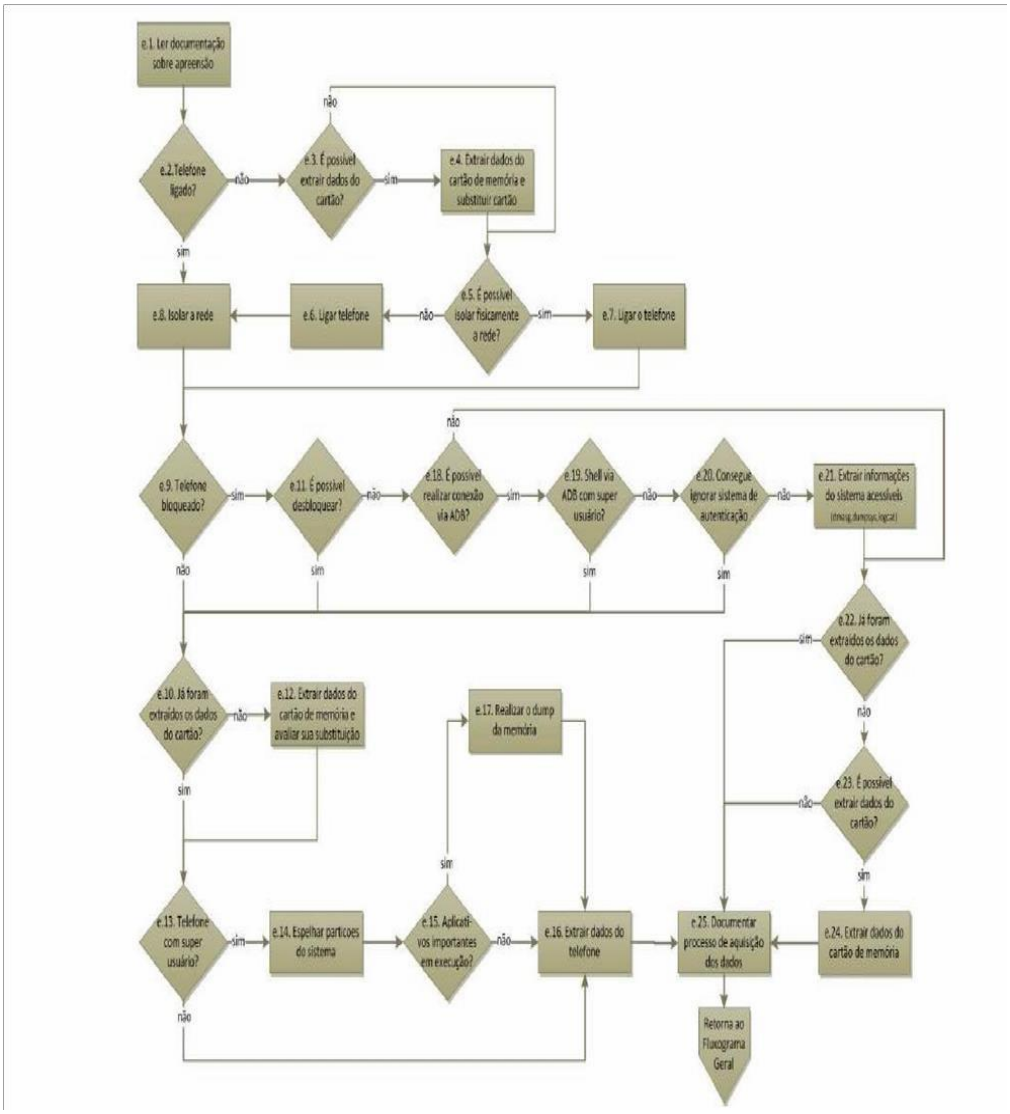

Figura 4 - Procedimento de Aquisição de Dados de um Telefone Celular com Sistema Android (Simão, 2011).

4.2. SDK DA FERRAMENTA SANTOKU

O *Santoku* Linux do *Android* é distribuído gratuitamente pelo GNU/Linux e é uma poderosa ferramenta forense que pode ser utilizada em diversas funções e cenários, onde há necessidade de um exame pericial e os peritos devem instalá-lo. O SDK é um dos recursos necessário para desenvolvimento de aplicativos *Android*, que inclui, entre outras ferramentas e funcionalidades as bibliotecas de software, APIs, material de referência para desenvolvedores e emulador.

Duas ferramentas importantes do SDK são: o emulador *Android*, onde é feito uma configuração da máquina virtual projetada para rodar em um computador de desenvolvimento e é usado para testar e depurar as aplicações. O ADB (*Android Debug Bridge*) é um aplicação cliente-servidor que é usada para fazer a comunicação com um emulador ou um dispositivo *Android* em modo de depuração através da porta USB, permitindo a cópia dos arquivos e pastas.

Segundo Hoog (2011):

> O SDK do Android proporciona um conhecimento mais abrangente sobre a plataforma Android e fornece ferramentas poderosas para investigar um dispositivo. Ao ter o SDK instalado em uma estação de trabalho forense, o perito tem a capacidade de interagir com dispositivo conectado via USB (com o recurso de depuração ativo) podendo consultar informações do dispositivo, instalar e executar aplicações e extrair dados.

4.3. ANDROID DEBUG BRIDGE

A ferramenta Android Debug Bridge (ADB) é uma ferramenta versátil que disponibiliza uma interface para um emulador ou para um dispositivo Android conectado ao computador.

Consiste em uma aplicação cliente-servidor combinada por três partes (Google Inc. 2012e):

- Cliente: roda na máquina à qual o dispositivo está conectado e sua maneira de trabalho é por terminal ou linha de comando através da ferramenta ADB (comando adb);
- Servidor: é executado em segundo plano como se fosse um serviço e fica na máquina à qual o dispositivo está conectado gerenciando a comunicação entre o cliente e o serviço na qual está sendo executado;
- Serviço: também é executado em segundo plano em cada emulador ou instância de dispositivo.

De acordo com Simão (2011):

> A conexão via ADB em um dispositivo físico é realizada com o usuário "shell", com poucos privilégios e um acesso limitado aos dados. Nas conexões feitas através de um emulador a permissão é de super usuário (root). Para ter acesso a um shell com permissões de super usuário em um dispositivo físico, é preciso que o sistema esteja com acesso à root instalado.

O comando *adb* é usado digitando *adb* no *prompt* de comando, e então será apresentada uma lista de comando disponíveis no ADB, entre eles são:

- **Adb devices:** Exibe a lista de dispositivos conectados ao ADB;
- **Adb logcat:** Permite a visualização dos dispositivos *Android* conectados ao ADB;
- **Adb shell:** Cria uma conexão *shell* para um dispositivo *Android* e permite a interação com o sistema;
- **Adb shell chmod:** Altera a permissão de arquivos;
- **Adb reboot:** Reinicia o sistema;
- **Adb install:** Instala um aplicativo direto da pasta do adb;
- **Adb pull e adb push:** Usado para copiar pastas ou arquivos para um diretório no sistema operacional *Android* em uma instância do emulador ou dispositivo.

4.4. SEGURANÇA ANDROID

O sistema operacional *Android* é baseado em Linux e, por isso, muitos conceitos do modelo de segurança aplicado nele foram adaptados. Por exemplo um dos conceitos central já abordado é o de usuários e grupos, onde cada usuário utilizador recebe um ID de usuário (*user* ID – UID) quando é criado.

Toda vez que um aplicativo (*app*) é instalado no *Android*, é gerado um novo ID de usuário (único no dispositivo) e esse novo *app* é executado sob esse UID, que a partir disso, relaciona todos os dados armazenados pelo *app*, sejam arquivos, base de dados ou qualquer outro recurso, a este UID criado.

De Acordo com Six (2012):

> A segurança é baseada em permissões de recursos, para este app recém instalado é configurada uma permissão total para todos os dados com o UID associado e nenhuma permissão de outro modo, ou seja, o sistema impede que outros aplicativos (UID diferente) acessem dados relacionados a ele.

Quando é instalado um *.apk* em um dispositivo *Android* pela primeira vez o mesmo confere o arquivo para garantir que ele tem uma assinatura digital válida que identifica o desenvolvedor. Com esse arquivo *.apk* validado, são verificados também os acessos que a aplicação precisa ter para funcionar (Hoog, 2011) notificando o usuário do dispositivo e pedindo uma aceitação para determinados acessos. Após a instalação do aplicativo e as permissões concedidas, nenhuma configuração de permissão pode ser alterada.

4.5. PERMISSÕES DE SUPER USUÁRIO

Como todos sabem, todos os dispositivos *Android* contém uma grande quantidade de informações por exemplo, lista de contatos, chamadas, banco de dados e mensagens de texto em seu diretório.

É um dispositivo capaz de armazenar vários se não todos os tipos de informações, no meio de um mundo criminalista, o dispositivo *Android* é uma ferramenta muito forte pois serve para o manuseio de muitas informações, e dependendo muito de como esse dispositivo é destruído, dificulta muito o trabalho do Perito para a extração de dados, deixando muitas vezes impossível a extração do mesmo.

De acordo com Racioppo e Murthy (2012):

> O Android armazena a maioria das informações importantes como contatos, chamadas, banco de dados e mensagens de texto no diretório raiz (/). Para obter acesso a este diretório é preciso realizar um procedimento no dispositivo conhecido como “Rooting”, que consiste entre outras características, obter permissões de super usuário (root) e um maior controle sobre o sistema operacional. As técnicas para obtenção de acesso root no Android variam conforme fabricante, modelo do telefone celular e versão do sistema. Muitas dependem de softwares de terceiros, sem validação, ou são invasivas, podendo comprometer a integridade dos dados armazenados no dispositivo.

O *Rooting* é necessário, pois os usuários usados por padrão pelos aplicativos não possuem permissões para realizar modificações no sistema operacional. São usuários com muitas restrições e que realizam apenas as interações específicas do aplicativo, que como citado anteriormente não podem modificar e às vezes até ter acesso a algumas partes do sistema operacional.

5. ESTUDO DE CASO

Neste capítulo foi abordado um estudo de caso mais detalhado sobre alguns métodos usados e os procedimentos mais importantes necessários para fazer uma análise pericial completa em um *Smartphone*.

Apresenta-se um cenário um pouco mais comum como quando um *smartphone* é apreendido e é necessário extrair dados para um exame, onde o aparelho é de um usuário comum, e o dispositivo encontra-se ligado, sem qualquer tipo de restrição de acesso e sem permissões de super usuário. Neste estudo explica-se como é feita a extração de SMS, MMS e extração logica de dados do *smartphone*.

5.1. AVALIAÇÃO DO EQUIPAMENTO

Este estudo de caso leva em consideração apenas a solicitação para aquisição/extração de dados armazenados no aparelho celular, percorrendo superficialmente os outros processos normais de uma metodologia de análise forense em dispositivos móveis, que são as fases de preservação e apreensão do aparelho, exame, análise, documentação e formalização do laudo pericial.

Segundo Simão (2011):

> Em um primeiro momento, o analista pericial deve se inteirar sobre o processo de apreensão, lendo a documentação produzida nesta etapa e se informar a respeito da solicitação, a fim de subsidiar as decisões a serem tomadas no processo de extração de dados do sistema Android.

As informações encontradas no caso apresentado, serão baseadas nos dados possíveis de serem extraídos. As informações mais comuns são registros de chamadas, mensagens, vídeo, imagens e áudios.

Utiliza-se dois modelos de *Smatphones* com as características a seguir:

- Fabricante e Modelo: ASUS Zenfone 3 – ASUS_Z017DC (Software: WW_15.0410.1806.68_0);
- Versão do Android: 8.0.0;
- Versão do Kernel: 3.18.66-perf-g55b9fd2;
- Condições: Aparelho ligado, sem bloqueio de acesso, sem super usuário, em modo avião e sem danos.

Essas informações são muito importantes para constar no processo de documentação da apreensão e deve estar inteiramente disponível para o perito.

5.2. METODOLOGIA PARA AQUISIÇÃO DE DADOS

Conforme ressalta Simão (2011), O fluxo que tem que ser seguido no processo de aquisição de dados para o cenário proposto munido de base para ilustração do estudo de caso e a descrição das etapas previstas é o de acordo com a figura 5.

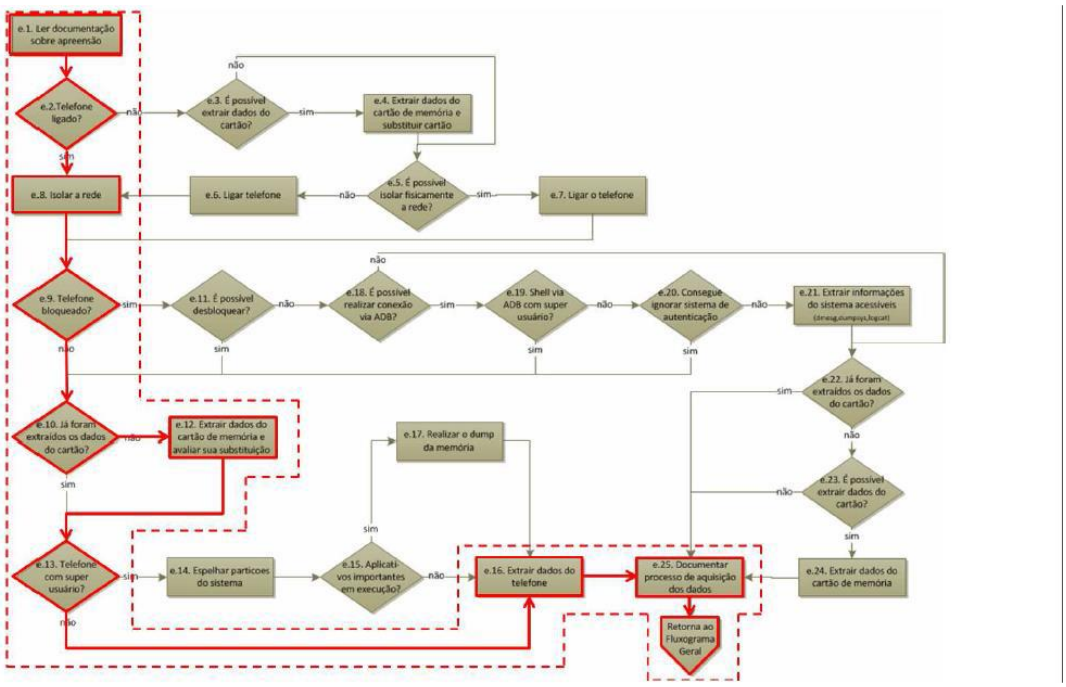

Figura 5 - Etapa a ser seguida para uma aquisição de Dados

Para fazer uma extração de dados em um dispositivo móvel existe algumas etapas para fazer no processo de investigação.

Após o perito ler a documentação e ver que o dispositivo está em modo aviação e ver também a descrição completa do aparelho o analista irá ver que o aparelho está ligado e sem bloqueio de acesso. A partir desse momento, poderá começar com a extração de dados.

5.3. MÁQUINA VIRTUAL

Nesta etapa será mostrado como se configura uma máquina virtual com o sistema operacional indicado para a investigação. Para ser instalado o *Santoku* deve em primeiro lugar fazer o download do mesmo que está disponível em (https://santoku-linux.com/download/). Para executar o *Santoku* é necessário usar um software de máquina virtual na versão mais recente do Virtual Box, disponível em (https://www.virtualbox.org/wiki/Downloads). Após o download, instale o software em sua estação de trabalho, logo após, siga os passos para iniciar a máquina virtual.

No virtual box localize o botão “Novo” para criar uma nova VM, logo em seguida seleciona o Linux/Ubunto de 64 bits. Veja na figura 6.

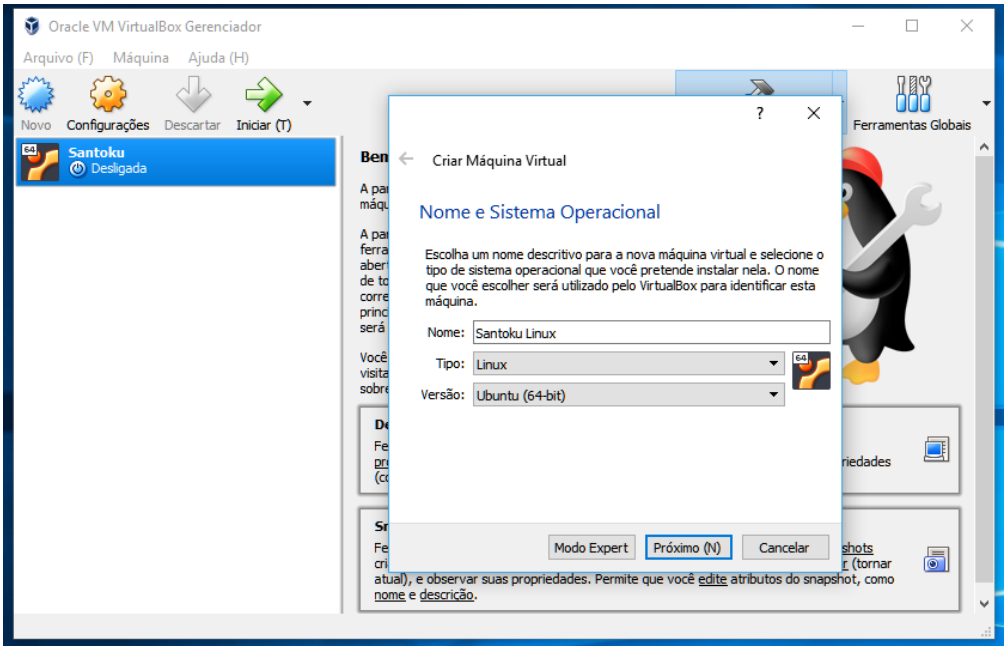

Figura 6 - Nova Virtual Box

Na próxima etapa será solicitado a quantidade de memória que irá disponibilizar para a máquina virtual, por padrão a mesma recomenda 512 MB de memória, mas para deixar a máquina virtual mais rápida aumentaremos a dimensão de memória para 1024 MB. Para utilizar o Android Virtual Device (AVD), é recomendado pelo menos 4 GB de memória, em seguida vamos clicar em “Próximo”. Veja na figura 7.

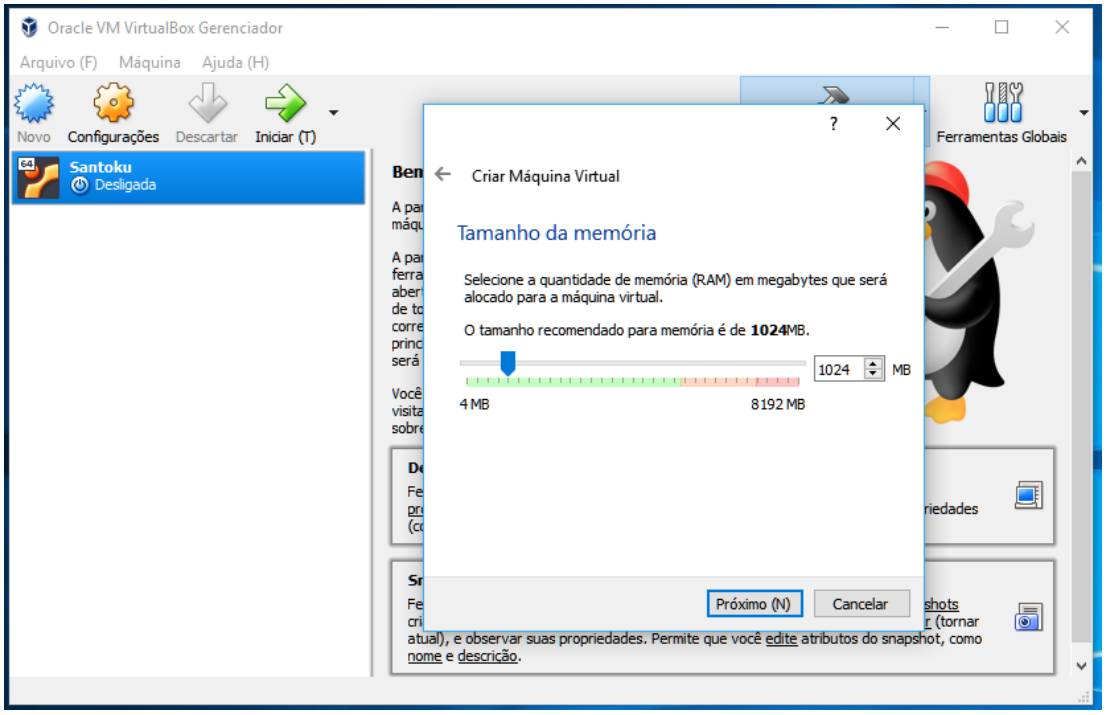

Figura 7 - Memória Virtual

Para prosseguir tem que certificar se o disco de inicialização (*Disk Startup*) está marcado, em seguida, escolha criar novo disco rígido e a opção VDI (*Virtual Box Disk Image*) e clicamos em “Próximo” como mostra a figura 8.

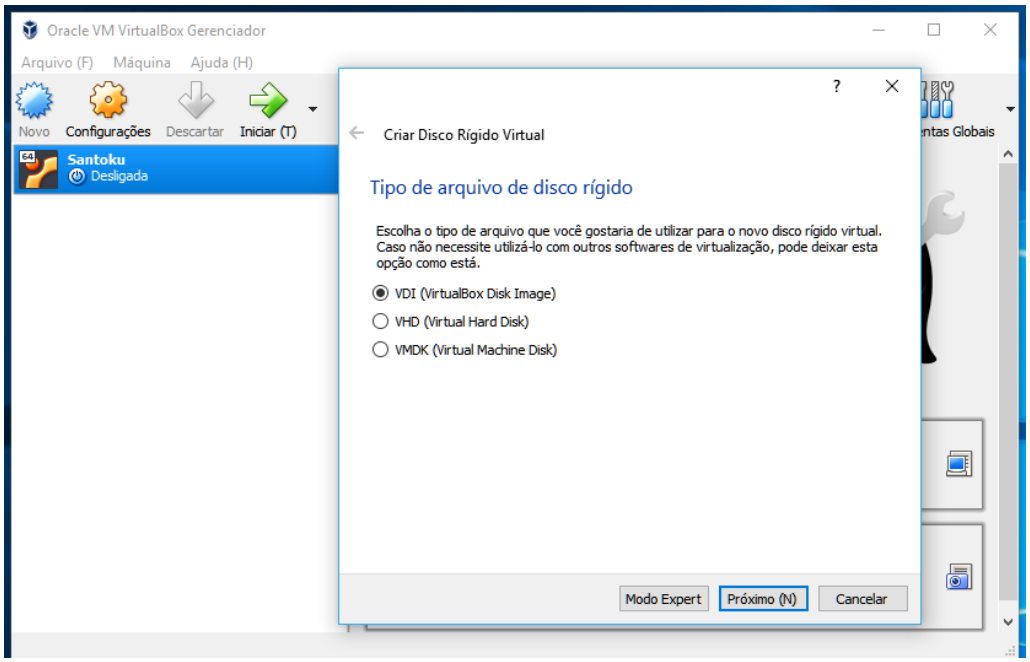

Figura 8 - Criando Disco Rígido

Agora escolha o local do disco rígido virtual, para salvar qualquer tipo de alteração e clique em salvar. Depois ajuste o tamanho do seu disco, é recomendado 40 gigas, então por fim clique em “Criar” como mostra a figura 9.

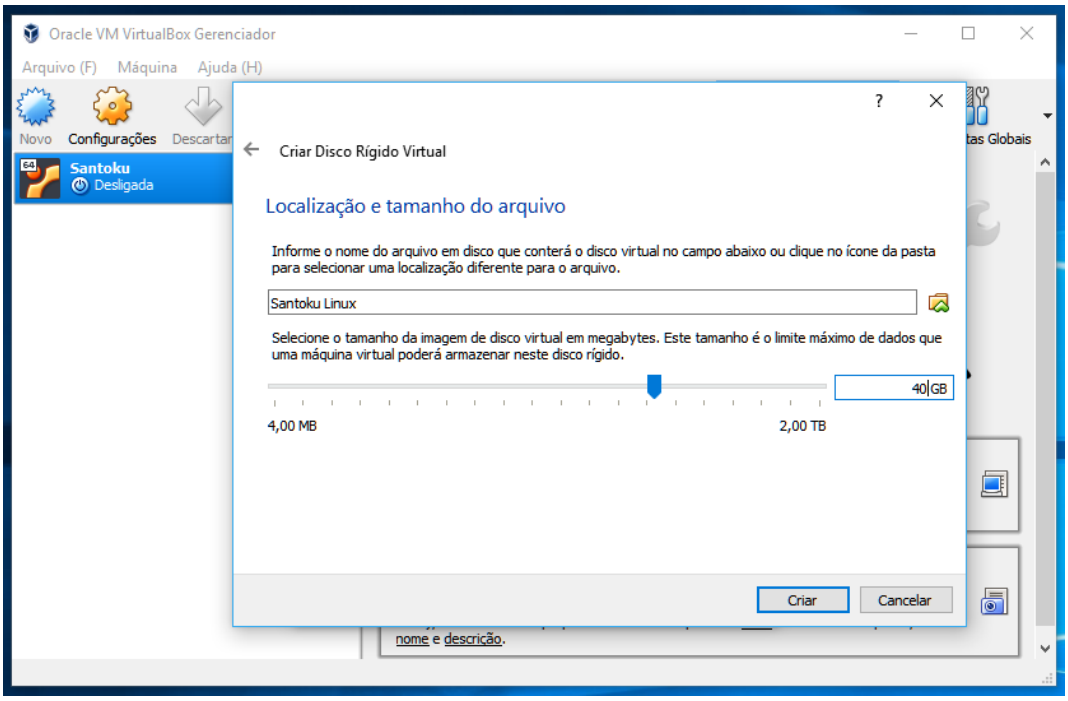

Figura 9 - Local e Tamanho Disco

Após feito toda a configuração, vamos inserir a imagem do Santoku-Linux à máquina virtual. Para inserir selecione o arquivo criado e clique na opção “Configurações”. Procure pela aba “Armazenamento” e depois clique no ícone em forma de CD que encontra ao lado do “Controlador IDE”. Logo após um aviso irá aparecer, escolha a opção “Escolha disco”, em seguida abrira a janela do Windows Explorer navegue até onde está a imagem do Santoku e cliquei em “Abrir” e depois “Ok”, de acordo com a figura 10.

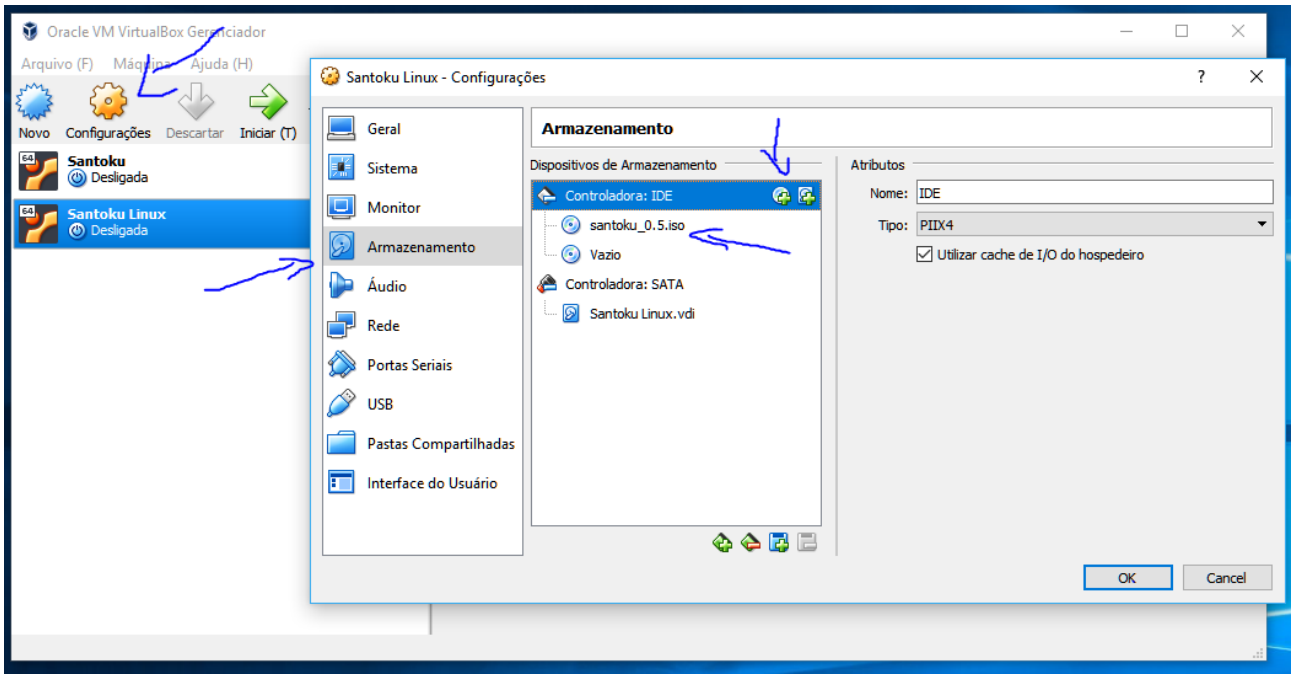

Figura 10 - Inserindo Santoku

5.4. INSTALANDO SISTEMA OPERACIONAL

Depois de ter configurado a virtual box podemos iniciar a mesma selecionando a máquina virtual e clicando no botão de “Iniciar”. Quando a VM foi iniciada vai aparecer na tela as opções de instalação do sistema operacional Santoku, escolha a opção “*Install – start the installer directly*”. Veja na figura 11.

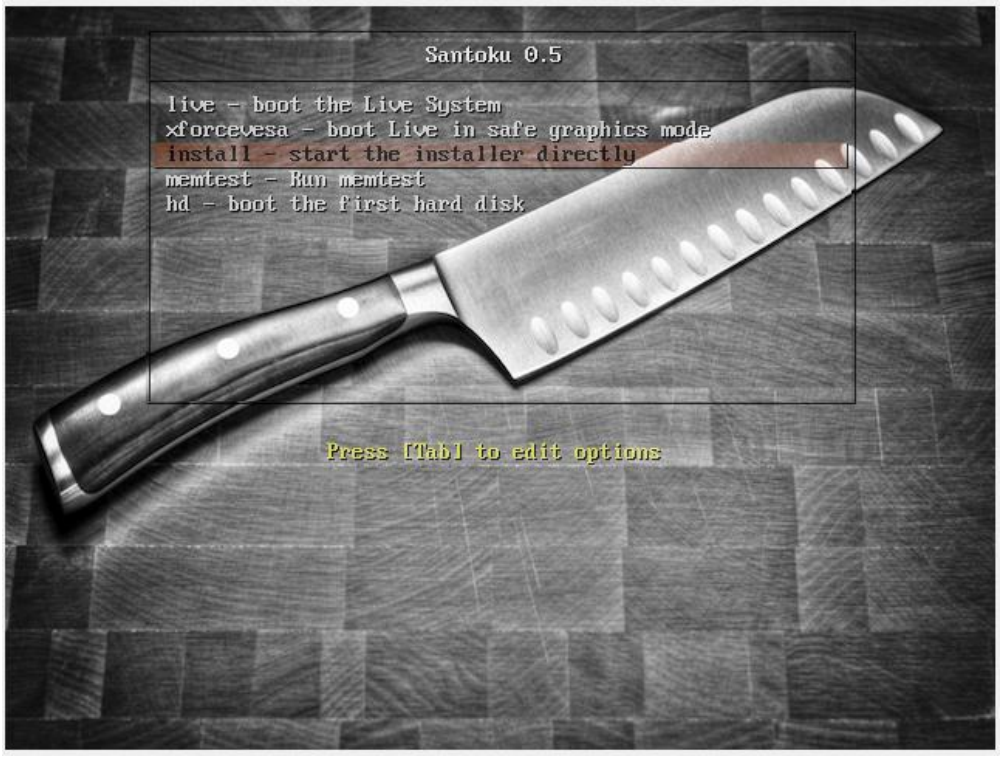

Figura 11 - Instalação Santoku

Após de concluir a instalação abrira a tela para escolher o idioma, fuso horário e configurações de relógio, depois disso escolha a opção “apagar o disco e instalar o Santoku”. Logo após escolha um nome de usuário e senha de administrador para dar mais segurança a sua máquina virtual e por fim clique em “Instalar”.

5.5. SDK

A ferramenta *Santoku* vem com o SDK instalado, porém o mesmo está todo desatualizado o SDK Manager tendo que por sua vez atualizar. Para fazer a atualização clique no logo do *Santoku* depois navegue até ferramentas de desenvolvimento e depois clique na opção gerenciador SDK, terá várias versões de Android para escolher, selecione a que será utilizada na investigação, cliquei em “Instalar pacotes” e em seguida aceite tudo para instalar.

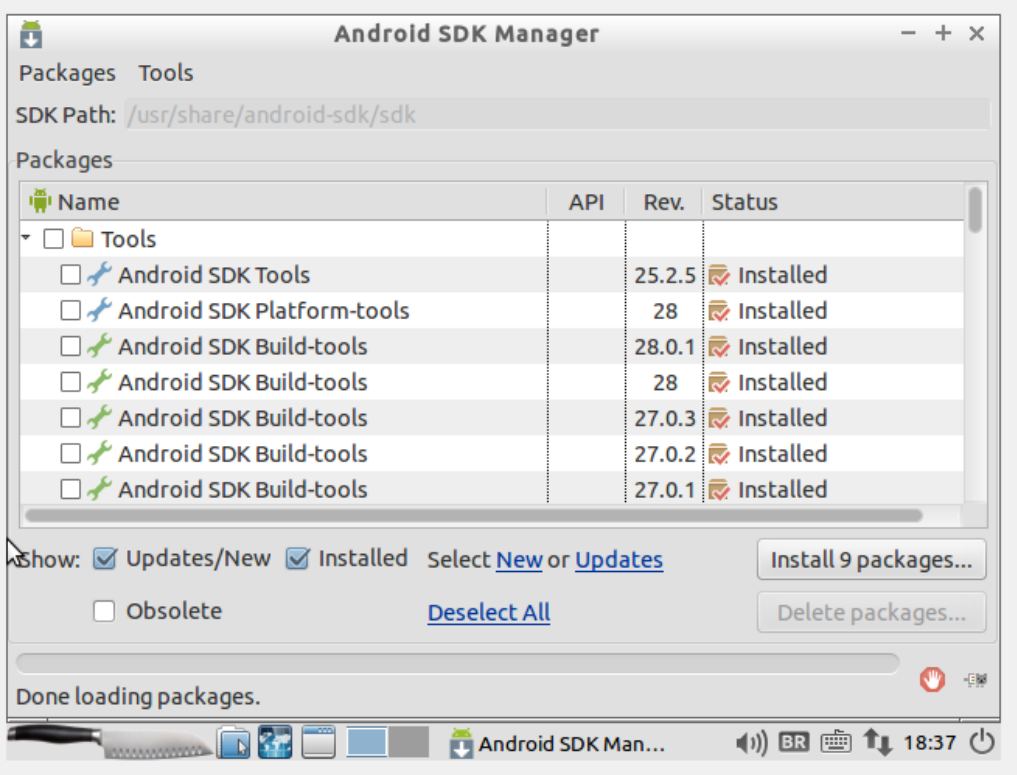

Figura 12 - Gerenciador SDK

5.6. INSTALANDO E EXECUTANDO O AFLOGICAL-OSE

O próximo passo é instalar o *AFLogical Ose,* mas para isso é necessário que o dispositivo esteja conectado ao terminal via cabo USB. Após conectar o cabo é recomendado verificar se o mesmo foi reconhecido, para isso vá até a barra de tarefas e clique na opção “Dispositivos”, escolha a opção “USB” que irá abrir uma janela mostrando que o dispositivo está conectado como mostra a figura abaixo.

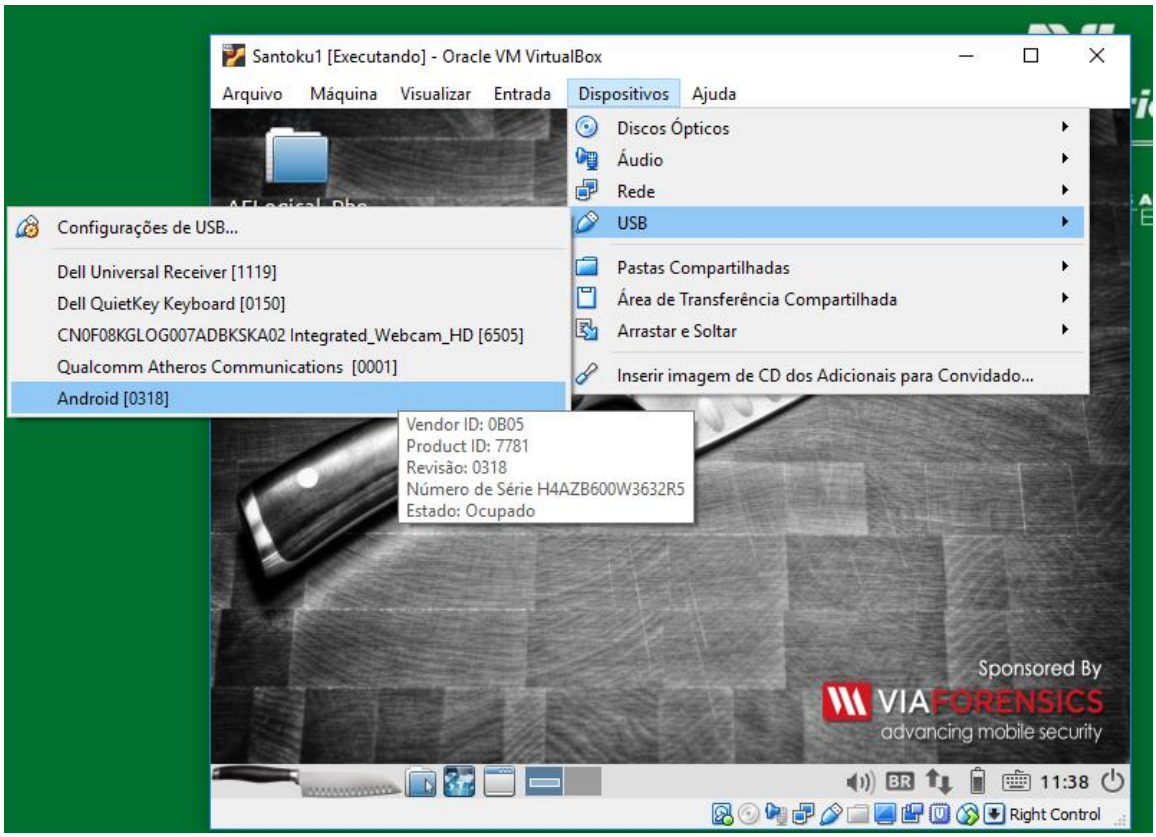

Figura 13 - Reconhecendo o Dispositivo

Após verificar se o dispositivo está conectado ao *Santoku*, é preciso isolar o aparelho de qualquer tipo de comunicação, para isso coloque-o em “Modo Avião”, e depois habilite o “Depuração USB” em “Configurações”, “Opções do desenvolvedor. Depois dessas etapas o aparelho já está pronto para fazer a extração.

Figura 14 - Habilitando Depuração USB

Depois de fazer todos esses passos chegou a hora de instalar o APK no dispositivo e começar a extração. Para isso vá para o terminal no diretório *Santoku* em seguida "*Devices Forensics"* e por fim AFLogical.

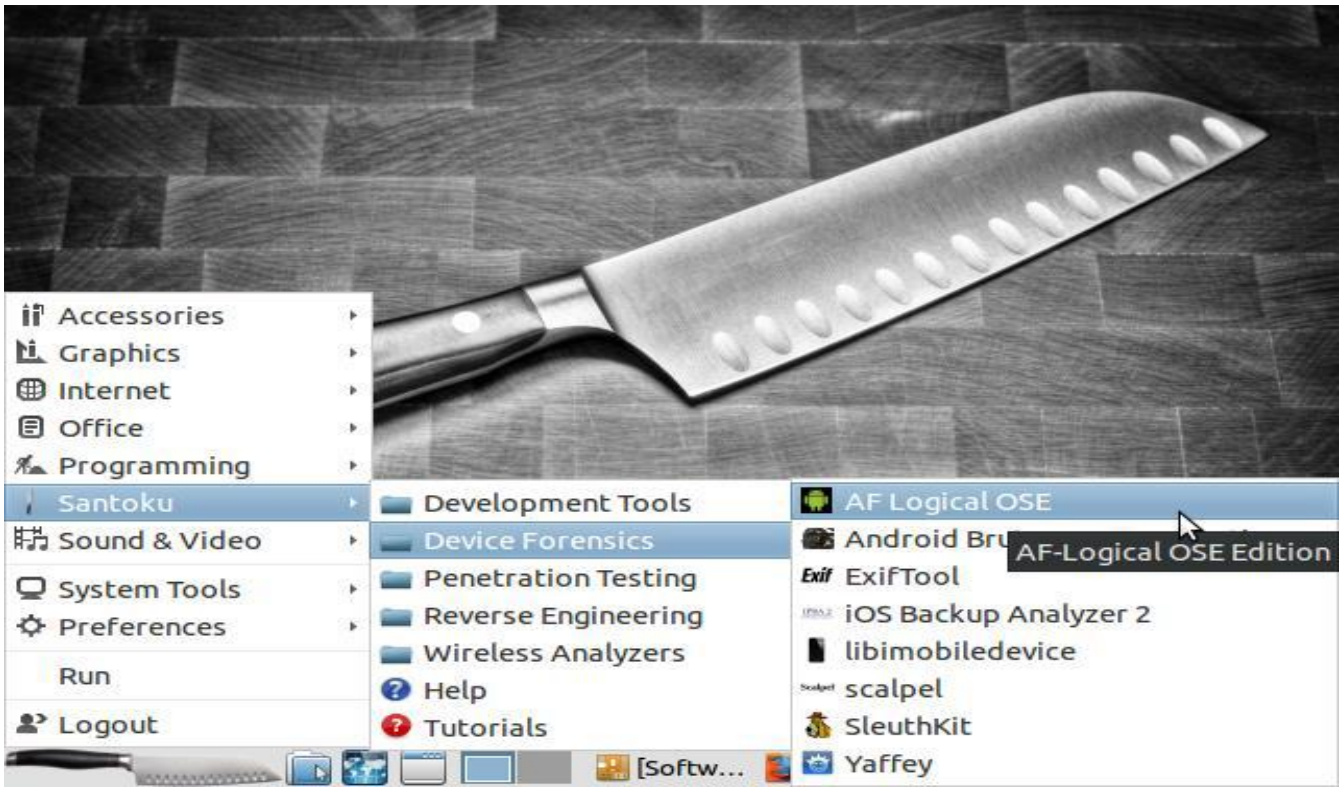

Figura 15 - Terminal AFLogical

Para prosseguir deve-se verificar se a ferramenta forense se comunica com o dispositivo Android. Para verificar bastar dentro do terminal AFLogical digitar o seguinte comando:

$ sudo adb devices

Será necessário colocar a senha que foi criada quando você instalou o sistema operacional e então aparecerá no terminal a mensagem abaixo.

[sudo] password for "Nome da Máquina"*:*

daemon not running. Starting it now on port 5037

daemon started successfully

List of devices attached

H4AZB600W3632R5 device

O próximo passo é instalar o AFLogical.apk, ainda com o terminal aberto digite:

$ adb install AFLogical-OSE_1.5.2.apk

Irá aparecer a seguinte informação na tela:

296 KB/s (28794 bytes in 0.094s)

Pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk, Sucess.

Agora no dispositivo que está sendo investigado procure pelo aplicativo “AFLogical OSE” que foi instalado e escolha os dados que deseja extrair.

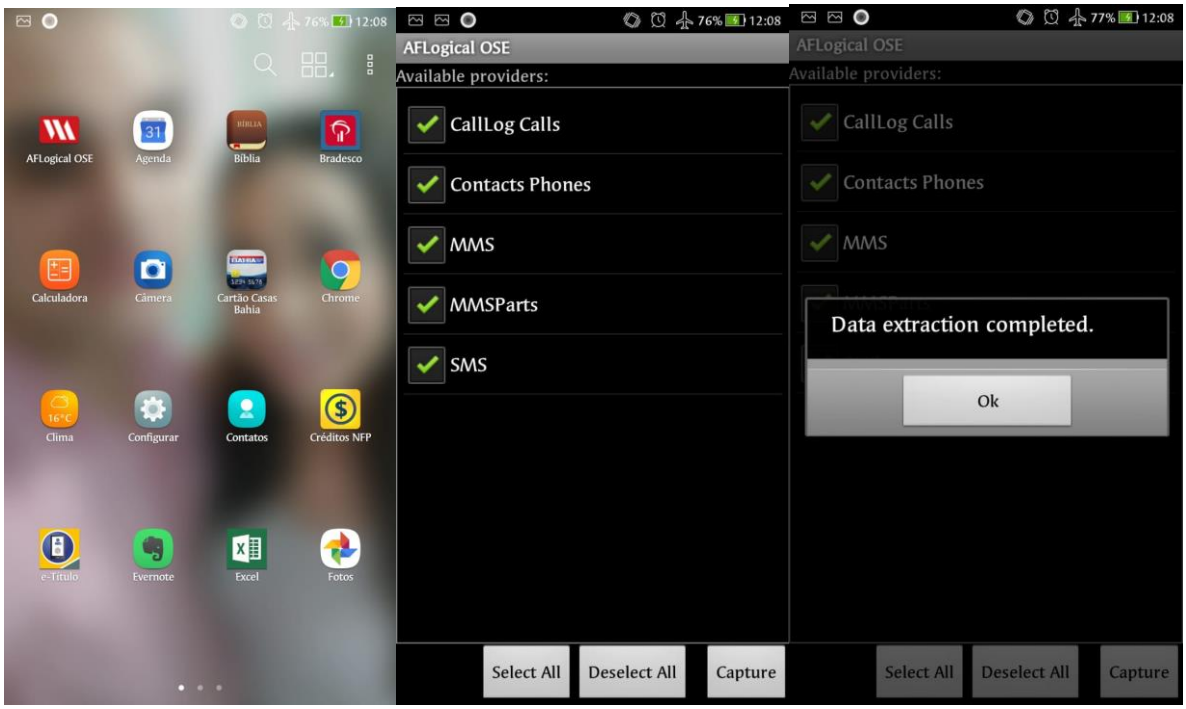

Figura 16 - Extraindo os dados do Celular

Agora o próximo passo a ser tomado é puxar os dados do Cartão SD para a Máquina *Santoku*, para fazer esse procedimento segue os comandos abaixo:

$ mkdir ~/Desktop/AFLogical_Phone_Data

$adb pull /sdcard/forensics/ ~/Desktop/AFLogical_Phone_Data

Pull: building file list...

Pull: /sdcard/forensics/20120720.1833/Contacts Phone.csv -> /home/Palma/Desktop/AFLogical_Phone_Data/20120720.1833/Contacts Phones.csv

Logo após irá aparecer a contagem de arquivos e o processo de extração na tela do terminal.

40 files pulled. 0 files skipped

410 KB/s (3880025 bytes in 9.229s)

Depois de ter feito todo esse processo, a extração de dados está concluída e para visualizar os dados no terminal é só digitar os seguintes comandos:

"$ cd~/ aflogical-dados /" em seguida o comando "$ ls"

Os dados são extraídos e alocados em uma pasta marcada com hora e data da aquisição no diretório "~/aflogical-data", agora o investigador terá acesso a todos os dados extraídos do dispositivo, dados como: registros de chamadas, MMS/SMS, contatos e informações do dispositivo em formato CSV:

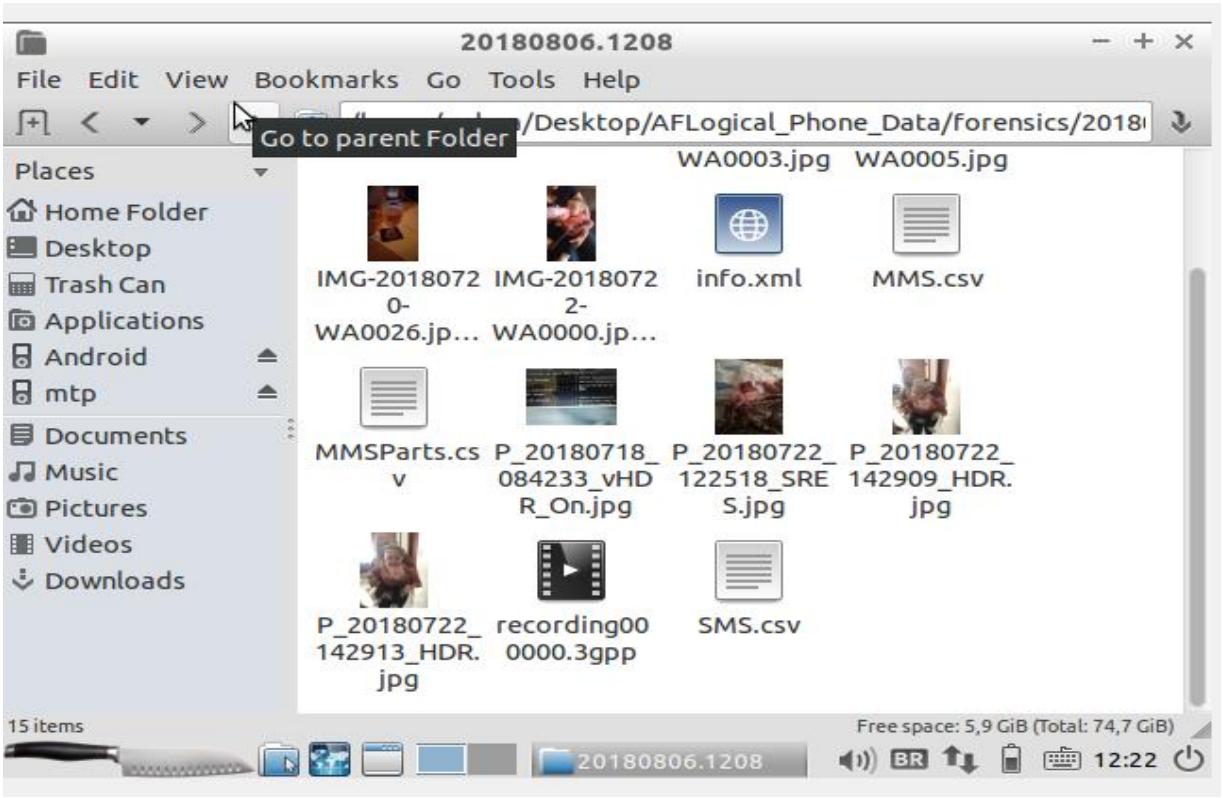

Figura 17 - Resultado da Extração

6. CONCLUSÃO

Nos dias de hoje existem vários métodos que um investigador da área pode usar para examinar e extrair os dados de um dispositivo móvel. Mas é claro que para efetuar uma investigação eficaz é necessário saber e conhecer as plataformas e suas características na qual está trabalhando antes de iniciar a perícia.

Este trabalho proporcionou um estudo de caso mostrando com detalhes um método para aquisição e exame de mensagens (SMS) de um dispositivo móvel com sistema operacional *Android*, mostrando algumas maneiras corretas para uma análise correta. Como todas as pesquisas e trabalhos este estudo não foi diferente, ele apresentou alguns obstáculos na hora do desenvolvimento e execução dificultando a execução de algumas técnicas com o menor impacto no dispositivo.

No aspecto forense esse trabalho teve abordagens de muitos assuntos como, metodologias e possibilidades de aquisição de dados em *Smartphones*, bem como o SDK e o ADB, deixando assim a direção do foco desse trabalho com a utilização da ferramenta *Santoku* Linux.

É de suma importância a utilização de técnicas e procedimentos homologados e principalmente bem fundamentados para se tornar um processo seguro e válido da investigação.

Para finalizar, foram usadas técnicas e procedimentos para obter uma análise forense com intuito de fazer uma coleta e extração de mensagens (SMS) de *smartphones* com sistema operacional Android, isso a partir do momento em que o aparelho se encontra em um contexto comum como mencionado em capítulos acima, sendo assim o dispositivo se encontra ligado, sem restrições de acesso e sem permissões de super usuário para uma investigação completa.

REFERÊNCIAS

ARTHUR, K. K. **Na Investigation Into Computer Forensic Tools**. Disponível em: <http://www.infosecsa.co.za/proceedings2004/060.pdf,2004 > Acesso em 25/06/2018.

ASCROFT, J. Eletronic Crime Scene Investigation: **A Guide for First Responders U.S. Departamento of Justice.** Washington, DC, p.82, 2001.

Association of Chief Police Officers. **Good Practice Guide for Computer-Based Eletronic Evidence.** Versão 4.0, 2008.

BEEBE N. L. e CLARK J. G. **A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. Digital Investigations Process Framework.** Jun. 2005.

BUSTAMANTE, Leonardo. **Computação forense: preparando o ambiente de trabalho. Uol, julho, 2006**. Disponível em:<http://imasters.uol.com.br/artigo/4335/forense/computacao_forensepreparando_o_ambiente_de_trabalho/ > Acesso em: 17 mar 2018.

BRASIL. Lei no. 3.189, de 3 de outubro de 1941, alterada pela lei 10.695, de 1 de julho de 2003. **Código de Processo Penal**, artigos 530-C e 530-D. Brasília, 2003.

Cannon, T. Android Lock Screen Bypass. Thomas Cannon, 2011. Disponível em: <http://thomascannon.net/blog/2011/02/android-lock-screen-bypass/ >. Acesso em: 15/jun/2018.

CARROLL, O. L.; BRANNON, S. K. e SONG, T. **Computer Forensics: Digital Forensic Analysis Methodology. The United States Attorneys' Bulletin.** 2008. Disponível em: <http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf.> Acesso: 20/jun/2018.

CRAIGER, J.P. **Computer forensics procedures and methods**. 2005. H. Bidgoli (Ed.), Handbook of Information Security. New York: John Wiley & Sons, 2005.

CUMMINGS, T. **The History of Computer Forensics**. Disponível em: <http://www.ehow.com/about_5813564_history-computer-forensics.html > Acesso em: 16 mar 2018.

DITEC/DPF. Instrução Técnica no. 003/2010-DITEC**. Dispõe sobre a definição de diretrizes e a padronização de procedimentos em âmbito das perícias de Informática na Policia Federal**. Brasília, 14/jun/2018.

ELEUTÉRIO, Pedro Monteiro da Silva; Machado, Marcio Pereira. **Desvendando a Computação Forense.** 1. Ed. São Paulo: Novatec,2011.

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

Google Inc. **Android Debug Bridge**. Android Developers, 2012e. Disponível em: <http://developer.android.com/tools/help/adb.htm >. Acesso em: 16/03/2018.

González, Elena Labajo. Ciências Antropológicas: **la Antropología Forense. Dez. 2004.** Disponível em: <http://www.p3blog.net/index.php?cat=21 > Acesso em: 18 mar 2018.

GROSSMAN, Luís Osvaldo. **Mundo tem 7,1 bilhões de celulares ativos**. Disponível em:

<http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate = site&infoid=40220&sid=8 >. Acesso em 27 Out 2017.

HOOG, Andrew. **Android Forensics - Investigation, Analysis and Mobile Security for Google Android.** Waltham: Elsevier, 2011.

ISFS. **Computer Forensics. Part 2: Best Practices**. Information Security and Forensics Society, Ago, 2009.

Jansen, W.; Ayers, R. "**Computer Security - guidelines on cell phone forensics**". National Institute of Standards and Technology – NIST, Special Publication 800-101, May 2007, 104 p. Disponível em < http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf > Acesso em: 16 mar 2018.

LESSARD, J. e KESSLER G. C. **Android Forensics: Simplifying Cell Phone Examinations.** Small Scale Digital Device Forensics Journal Vol. 4, No.1, September 2010. ISSN: 1941-6164 1.

Luque, Bartolomé Serrano. **Ciência Forense – como usar la ciência y la tecnologia para desvelar lo ocorrido? Todo-Ciencia.com. 2002.** Disponível em: < http://matap.dmae.upm.es/WebpersonalBartolo/articulosdivulgacion/crimenes_3.htm> Acesso em: 18 mar 2018.

Ministério Público do Estado de São Paulo. **Centro de Apoio Operacional Criminal.** Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf >. Acesso em: 27/jun/2018.

OLIVEIRA, F. S.; GUIMARÃES, C. C.; GEUS, P. L. **Resposta a Incidentes para Ambientes Corporativos Baseado em Windows**. 2002.

PALMER, G. and CORPORATION, M. **A Road Map for Digital Forensic Research**.Technical Report. Disponivel em: < http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf> Acesso em: 18 mar 2018.

Probst, Everson. Et al. Qperito.com. **História das Ciências Forenses**. Disponível em: <http://qperito.com/2014/10/13/queira-o-sr-perito-comentar-sobre-a-historia-dasciencias-forenses-e-as-diferencas-entre-a-computacao-forense-e-investigacaodigital/ > Acesso em: 17 mar 2018.

QUEIROZ, Claudemir e VARGAS, Raffael. **Investigação e Perícia Forense Computacional.** 1. ed. Rio de Janeiro: Brazport, 2010.

QUIRKE, J. **Security in the GSM system.** AusMobile. [S.1], p.26.2004.

RACIOPPO C. e MURTHY N. **Android Forensics: A Case Study of the "HTC Incredible" Phone**. Mai. 2012. Proceedings of Student-Faculty Research Day, CSIS, Pace University. Disponível em: < http://csis.pace.edu/~ctappert/srd2012/b6.pdf> Acesso em: 16 mar 2018.

Revista Científica Eletrônica de Ciências Sociais Aplicadas. **Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas. Nov. 2012.** Disponível em: < www.eduvalesl.edu.br/site/edicao/edicao-74.pdf > Acesso em 30 Out 2017.

REIS, M. A.; GEUS, P. L. **Forense Computacional: Procedimentos e Padrões**. 2001. Disponível em: < https://www.lasca.ic.unicamp.br/paulo/papers/2001-SSI-marcelo.reis-forense.padroes.pdf> Acesso em: 18 mar 2018.

SIMÃO, ANDRÉ MORUM DE L. (2011). **Proposta de Método para Análise Pericial em Smartphone com Sistema Operacional Android.** Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM – 081/2011, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 96p.

SIX, J. **Segurança de Aplicativos Android. Processos, permissões e outras salvaguardas.** 1a. ed. Novatec, 2012. ISBN: 978-85-7522-313-0.

TEMSAMANI, K. **Internet móvel é presente e futuro da tecnologia, diz executiva do Google,** Site IG Tecnologia, Mar. 2011. Disponível em: < http://goo.gl/2bK3U >. Acesso em:10/Jul/2018.

VARGAS. R. G.; QUINTÃO, P.L; GRIZENDI, L.T. **Perícia Forense Computacional**. Anais do I Workshop de Trabalhos de Iniciação Científica e de Graduação da Faculdade Metodista Granbery, pp. 20-29, Juiz de Fora.

WEISER, M. “**Some Computer Science Issues in Ubiquitous Computing”.**

Communications of the ACM, v. 265, n. 3, 1993, p. 137 - 143.