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

HUMBERTO BATISTA DA SILVA

PERÍCIA FORENSE COMPUTACIONAL EM DISPOSITIVOS MÓVEIS

Assis

2015

HUMBERTO BATISTA DA SILVA

PERÍCIA FORENSE COMPUTACIONAL EM DISPOSITIVOS MÓVEIS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas.

Orientador: Me. Fábio Eder Cardoso

Área de Concentração: Análise e Desenvolvimento de Sistemas

Assis

2015

FICHA CATALOGRÁFICA

SILVA, Humberto Batista

Perícia Forense Computacional em Dispositivos Móveis / Humberto Batista da Silva. Fundação Educacional do Município de Assis -- Assis, 2015.

80 p.

Orientador: Me. Fábio Eder Cardoso

Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

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

CDD: 001.61

Biblioteca da FEMA

PERÍCIA FORENSE COMPUTACIONAL EM DISPOSITIVOS MÓVEIS

HUMBERTO BATISTA DA SILVA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, analisado pela seguinte comissão examinadora:

Orientador: Me. Fábio Eder Cardoso

Analisador: Dr. Almir Rogério Camolesi

Assis
2015

DEDICATÓRIA

Dedico este trabalho a minha família e aos meus amigos, que de muitas formas sempre incentivaram e acreditaram para que eu pudesse vencer mais uma etapa da minha vida.

AGRADECIMENTOS

Agradeço primeiramente a Deus por estar presente em todos os momentos da minha vida dando força e sabedoria para superar as dificuldades.

Aos meus familiares, especialmente minha mãe Marina Magali de Moura, pelo apoio e incentivo nas horas difíceis.

As minhas madrinhas Sandra Regina de Souza e Selma Aparecida Bernardo, por estarem ao meu lado nos momentos de angústia e felicidade, pela motivação e dedicação para a realização dos meus sonhos.

Agradeço minhas amigas Marcela Mantovani e Polyana Gatto, por estarem sempre ao meu lado incentivando a chegar a mais uma conquista e acreditarem em minhas escolhas.

Aos meus amigos de perto e de longe pela torcida, amizade e por compreenderem a importância dessa conquista aceitando minha ausência quando necessário.

Agradeço a todos os professores por me proporcionar o conhecimento no processo de formação profissional.

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

Atualmente com a evolução da tecnologia em aparelhos celulares por meio do uso de sistemas operacionais agregados aos serviços disponibilizados pelas operadoras de telefonia celular, milhares de pessoas estão fazendo uso desta nova plataforma, gerando assim um grande repositório 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.EDU.BR).

Neste presente trabalho será descrito os processos executados durante uma investigação e exibir técnicas na coleta, preservação de evidências e análise dos dados coletados através da ferramenta *Santoku* Linux que auxilia o profissional na investigação em um *smartphone* com sistema *Android*.

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

ABSTRACT

Currently the evolution of technology in mobile devices through the use of aggregate operation systems to services provided by mobile operators, thousands of people are making use of this new platform, generating a extensive repository of information. The computational expertise in practical ways, to prove crime, collecting proof and digital evidence on suspicious devices, helping to clarify justice crime (EDUVALESL.EDU.BR).

In this work will be described processes executed during an investigation and display techniques in collecting, preserving evidence and analysis of data collected by *Santoku* Linux tool that helps professional research on a *smartphone* with Android system.

Keywords: Forensics, Evidence, Research and *Santoku* Linux tool.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACPO – *Association of Chief Police Officers*

ADB - *Android Debug Bridge*

APP - Aplicativo

AVD - *Android Virtual Device*

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*

PIN – *Personal Identification Number*

PUK – *Unlock Key*

RAM - *Random Access Memory*

ROM - *Read Only Memory*

SD - *Secure Digital*

SDK- *Software Development Kit*

SIM – *Subscriber Identily Module*

SMS- *Short Message Service*

SO – *Sistema Operacional*

UID - *User IDentification*

USB – *Universal Serial Bus*

SUMÁRIO

1. INTRODUÇÃO

Na atualidade os aparelhos celulares fazem parte de milhões de pessoas trazendo recursos cada vez mais sofisticados e mais comodidade aos seus usuários através da massificação da internet nestes dispositivos. Vivemos em uma sociedade completamente voltada a informação, e a disseminação de crimes virtuais vem crescendo periodicamente através destes aparelhos. Para combater esse tipo de crime, não basta apenas usar meios convencionais de investigação, mas também é necessário o conhecimento das tecnologias computacional.

“Mesmo já fazendo parte das nossas vidas há algum tempo e nos mantendo em comunicação constante, os dispositivos móveis estão atuando, entre outras funções, como escritório portátil, ferramenta social e entretenimento” (Speckmann, 2008).

A internet tem encontrado formas de inovar para deixar as pessoas conectadas, e permitindo entretê-las e permitir a troca de informações. “Mas nenhum deles é capaz de chegar a cada pessoa em qualquer lugar e a qualquer hora como o telefone celular faz” (Speckmann, 2008).

1.1 OBJETIVOS

“Examinadores forenses devem seguir, de forma clara e bem definida, metodologias e procedimentos que podem ser adaptados para situações específicas” – *National Institute of Standarts and Technology* (NIST) (Ayres, Jansen, Moenner e Delaitre,2007).

Este trabalho tem como objetivo fundamentar conceitos sobre Perícia Forense Computacional, e suas áreas de análise pericial em dispositivos móveis exemplificando por meio de um estudo de caso, os procedimentos necessários, as principais técnicas e exames periciais no dispositivo, afim de extrair as informações possíveis de acordo com o equipamento, mostrando também o conhecimento que o profissional precisa ter para a utilização da ferramenta e metodologia em Análise

Digital Forense, visando estimular o leitor a buscar novos conhecimentos nesta área de pesquisa pouco explorada.

1.2 JUSTIFICATIVAS

“Os aparelhos e a internet móveis são o presente e o futuro da tecnologia” (Tensamani,2011).

Com quantidade diversificada de funcionalidades disponíveis nos aparelhos celulares, produz um grande desafio para a análise forense que necessita avançar por vários obstáculos, a fim de acompanhar os avanços da tecnologia.

Neste estudo será apresentado práticas de perícia, com foco principal no 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 procedimentos homologados e bem fundamentados, alinhados a metodologias de análise pericial aceitas pelas entidades profissionais, possibilitam produzir o conhecimento necessário para a condução de investigações forenses.

1.3 MOTIVAÇÕES

Devido ao aumento considerável de ações ilícitas realizadas no uso dos aparelhos *Smartphones* e com uma pequena demanda de profissionais capacitados nesta área, faz-se necessário estudar e aprimorar cada vez mais os conhecimentos, métodos e ferramentas na área Forense, pois com o surgimento de novas tecnologias, novos desafios e técnicas necessitam ser desenvolvidas

1.4 PERSPECTIVAS DE CONTRIBUIÇÃO

A perspectiva é de levar o leitor a conhecer mais sobre a Perícia Forense Computacional e que o Brasil possa vir a investir mais nesta área no combate de identificar, julgar e penalizar a prática de crimes virtuais, pois atualmente a realidade está relativamente longe do ideal e que no futuro este estudo possa servir de fonte de pesquisa.

1.5 METODOLOGIA DE PESQUISA

Para o desenvolvimento deste trabalho optou-se por realizar uma revisão da literatura de qualidade e produzidos por profissionais na área, pesquisas na Internet para informações complementares através de sites, apostilas, artigos e trabalhos de conclusões e também o uso do *Santoku* versão 0.5 – Lubunto simulando a coleta, e análise de dados, assemelhando uma perícia forense computacional. A partir de então, foram estudadas as características voltada para *smartphones* relacionados à forense em telefones celulares.

O método proposto para realizar uma análise pericial em um *smartphone* está baseado nas melhores práticas utilizadas atualmente pela Polícia Federal do Brasil, pelo NIST (JANSON e AYRES, 2007), pelo Departamento de Justiça dos Estados Unidos (ASHCROFT, 2001), pela polícia Inglesa (Association of Chief Police Officers, 2008) e Instituto Forense da Holanda (Netherlands Forencis Institute, 2007).

1.6 RECURSOS NECESSÁRIOS

Os recursos necessários para a realização deste trabalho, primeiramente foi o levantamento bibliográfico de obras de qualidade e produzidas por profissionais

renomados na área, Computador, Máquina Virtual e a ferramenta *Santoku* versão 0.5 – Lubunto Linux.

1.7 ESTRUTURA DO TRABALHO

Este trabalho descreve alguns procedimentos necessários para a correta análise forense em *smartphone*, baseado nas melhores práticas usadas pelas entidades acadêmicas e profissionais.

Além da presente introdução, que pretende contextualizar o tema, sua perspectiva, objetivos e justificativas, o trabalho se estrutura da seguinte forma:

- O Capítulo 2 apresenta conceitos relevantes sobre perícia forense computacional, bem como a evolução forense, um referencial teórico importante sobre definição forense, profissional computacional, legislação, evidência digital e uma breve contextualização sobre cadeia de custódia.
- O Capítulo 3 será abordado sobre os dispositivos móveis e coleta de dados digitais, procedimentos de busca, apreensão e preservação, aquisição de dados, um referencial teórico sobre ferramenta de extração, memórias dos dispositivos móveis, códigos de segurança e controle de acesso e também sobre memórias removíveis.
- O Capítulo 4 apresenta conceitos importantes no exame do telefone celular, obtenção e cópia forense dos dados, requisição forense, preparação e extração dos dados, identificação e relatório do caso.
- O Capítulo 5 é a seção que referência perícia forense em *Android*, apresentando também a metodologia para aquisição de dados em *smartphones* com a o software *Android* SDK (*Software Development Kit*) na ferramenta *Santoku.* Traz também especificações do ADB (*Android Debug Bridge*), modelo de segurança e permissões de super usuário.
- O Capítulo 6 exibe a seção de referência à perícia forense *Android* com avaliação do cenário, metodologia para aquisição de dados de aparelhos *smartphones.* Mostra também como configurar a máquina virtual e a instalação

da ferramenta forense *Santoku,* bem como fazer o gerenciamento do SDK, construção de um dispositivo virtual, instalação do emulador e do *AFLogical-OSE* e também a extração dos dados do dispositivo móvel.

- Por fim, o Capitulo 7 apresenta as conclusões e uma síntese dos resultados obtidos com o desenvolvimento do estudo de caso.

2. COMPUTAÇÃO FORENSE

A computação forense tem por objetivo criar metodologias e acumular conhecimentos para a aquisição, manipulação e análise de evidências determinando se houve ou não atividades ilegais.

Segundo 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.

De acordo com Eleutério, Machado (2011):

> Tem como objetivo primário determinar a dinâmica, materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo.

2.1 EVOLUÇÃO FORENSE

“As grandes civilizações da Idade Antiga, evoluíram os conceitos norteando a forense primitiva, visando os diferentes modos de pensar e agir, cada uma dessas civilizações gerou diferentes códigos de leis escritas para reger seus cidadãos” (RUIZ,2005).

“O primeiro registro da Ciência Forense vem da China onde Ti Yen Chieh, tornou-se famoso ao fazer uso dos vestígios do crime para resolvê-los, e também da lógica, utilizando diversos métodos e ferramentas” (LUQUE,2002).

Por volta do século XIII, o juiz Song Ts´Eu, escreveu o primeiro compêndio conhecido de medicina legal no campo do Direito. “Nesse compêndio, o juiz explicava como se reconhecer os sinais de estrangulamento e afogamento e ferimentos poderia se chegar a determinar o tipo e o tamanho da arma utilizada no crime” (WILK,2005).

“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).

No início do século XX, 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.

O campo da pesquisa sobre investigação digital surgiu na década de 80, sendo que em 1984 foi criado um programa dentro do FBI.

Segundo Cummings (2010):

> Este programa era conhecido apenas como sendo um grupo de análises e estudos sobre mídias magnéticas. Alguns anos após a criação do programa, o agente especial Michael Anderson, o qual é considerado o “Pai da Forense Computacional”, começou a trabalhar neste departamento do FBI.

Este agente trabalhou no programa até a década de 90 e, 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).

Muitos foram os esforços dos cientistas que estudaram, pesquisaram e desenvolveram alguma prática forense, sem medir esforços para que de alguma maneira viesse a contribuir com suas descobertas para o avanço dos profissionais em gerações posteriores. Mesmo após muito tempo as estes estudos, os conceitos e as bases sobre perícia continuam atuais e largamente utilizadas ao longo de um processo investigativo. Atualmente as principais diferenças são os equipamentos utilizados, e os conceitos que estão mudando devido a chegada da informática e o grande número de informações em que hoje se trabalha. Os cenários dos crimes estão além de sangue, fios de cabelos, fluidos corporais e corpos físicos, mas também em identidades virtuais e informações contidas através dos números binários.

2.2 DEFINIÇÃO DE COMPUTAÇÃO FORENSE

Devido ao surgimento de crimes envolvendo o meio computacional, tornou-se necessário o desenvolvimento da perícia forense computacional.

Segundo Freitas (2006):

> Como a aplicação de conhecimento de informática e técnicas de investigação com a finalidade de obtenção de evidências, além de, para o autor, ser uma área relativamente nova e em grande ascensão; justamente por isso tornou-se uma prática importante nas corporações e polícias, que utilizam resultados científicos e matemáticos estudados na ciência da computação.

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.

Ainda, segundo Bustamante (2006):

> Tal função deve-se ao fato de que o juiz, pessoa dotada de grande conhecimento jurídico, não dispõe de grande saber científico, o que torna obrigatório a presença dos Peritos, profissionais detentores de grande conhecimento em áreas científicas e de confiança do juiz, o qual utilizará de seus conhecimentos para realização da perícia no objeto questionado (indício), sendo que o resultado de seu trabalho será exposto por meio de um laudo, o qual deve ter uma linguagem simples, mas sem omitir dados técnicos, que possam ser compreendidos por não especialistas.

De Acordo com Rezende (2008):

> O cargo de Perito Criminal é dotado de fé pública e não abriga o significado de representação exata e correta da realidade, de certeza ideológica, mas também de um sentido altamente jurídico, ou seja, fornece evidência e força

> probante atribuída pelo ordenamento, quanto à intervenção do oficial público em determinados atos ou documentos. O valor jurídico e a certeza implicam que a fé pública pressupõe a correspondência da realidade, cuja firmeza é tutelada pelo Direito.

Ainda, Palmer and Corporation (2001):

> Destacam que a Forense Computacional pode ser definida como a inspeção científica e sistemática em ambientes computacionais, com o objetivo de angariar evidências derivadas de fontes digitais, tendo como objetivo promover a reconstituição dos eventos encontrados (dessa forma, pode-se determinar se o ambiente em análise foi utilizado na realização de atividades ilegais ou não autorizadas.

O objetivo da perícia forense é criar metodologias e acumular conhecimentos para a aquisição, manipulação e análise de 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.

Segundo Oliveira, Guimarães e Geus (2002):

> Para resolver um mistério computacional é necessário examinar o sistema nos mínimos detalhes, ou seja, da maneira que um detetive examina a cena de um crime. Dessa forma, o perito que está realizando a análise deve conhecer profundamente o sistema operacional em que está trabalhando para identificar e entender as relações de causa e efeito de todas as ações tomadas durante a análise.

De acordo com Reis e Geus (2001):

> Para que o perito conduza uma análise forense computacional de maneira eficaz é necessário que ele tenha uma série de habilidades, como, por exemplo, raciocínio lógico, mente aberta e o entendimento das relações de causa e efeito. Todas essas habilidades (que são encontradas nos programadores) são utilizadas durante a busca de um erro em um programa.

Segundo Zillo Neto (2008):

> Todos os dias novas tecnologias surgem e daí a necessidade de novas preocupações com segurança, novas especificações, novos padrões, e antes mesmo de implementarmos novas tecnologias seguras, aparecem outras, depois outras e sucessivamente, realmente vira uma corrida contra o tempo [...].

"A Forense Computacional é uma área de pesquisa muito recente e poucos são os trabalhos sobre esse assunto no Brasil. É importante que esta área se desenvolva, aja vista que muitos *hackers* utilizam os computadores em atividades criminosas" (VARGAS, QUINTÃO e GRIZENDI, 2007).

2.3 PROFISSIONAL DA PERÍCIA FORENSE

"O profissional ou equipe de trabalho, deve-se contar com profissionais que conheçam o máximo possível das tecnologias da informática, procurando capacitar-se para o trabalho de investigação, levantamento e preservação das provas materiais" (ELEUTÉRIO E MACHADO, 2011, p. 14).

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 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 abaixo ilustra o mapa mental de um perito.

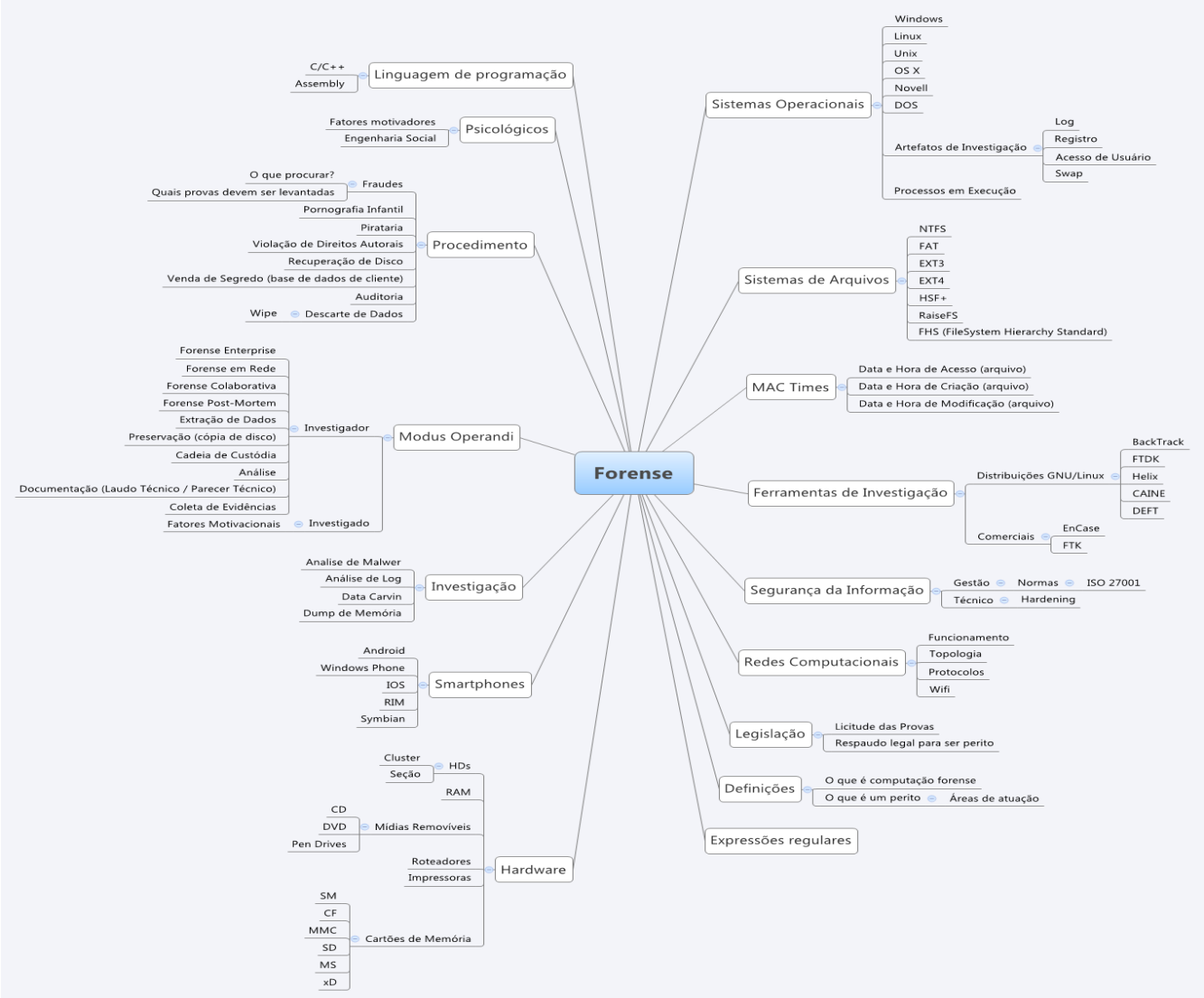

Figura 1- Mapa mental conhecimento perito forense computacional (https://4en6br.files.wordpress.com/2012/05/forense1.png)

“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

As legislações vigentes sobre crimes que são cometidos com computador não possuem nenhuma tipificação própria.

Segundo Queiroz e Vargas (2010):

> Os mesmos crimes são tipificados com a legislação de crimes comuns, onde apenas o resultado do crime é caracterizado a um crime comum, então o meio utilizado pelo autor do crime é ignorado no caso quando é utilizado o computador como meio de praticar o delito.

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 [1]dispositivo 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).

Cuidando-se de nova lei incriminadora, a Lei nº 12.737/2012 que, em seu art. 4º estabelece uma *vacatio legis*[1] de 120 (cento e vinte) dias, não poderá retroagir para alcançar condutas pretéritas.

Assim, a nova lei incrimina 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.),

[1] Vacatio legis é o prazo legal que uma lei tem para entrar em vigor, ou seja, de sua publicação até o início de sua vigência (Dicionário Informal).

desde que a finalidade do criminoso seja obter, adulterar ou destruir dados ou informações.

- Instalar no dispositivo informático qualquer vulnerabilidade com o fim de obter uma vantagem ilícita (patrimonial ou não).
- Produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a invasão de dispositivo informático ou a instalação de vulnerabilidades.
- O crime é qualificado, com penas que vão 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 comunicações eletrônicas privadas, segredos comerciais ou industriais, informações definidas em lei como sigilosas. Se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas, a pena do crime qualificado será também aumentada de 1/3 a 2/3.
- Se a conduta for mais grave que a simples invasão com a finalidade de obtenção, adulteração ou destruição dos dados ou informações, ou a instalação de vulnerabilidades, como por exemplo, fraudes em *netbanking* (furto qualificado), estelionato ou extorsão, interceptação de comunicação telemática, o crime de invasão de dispositivo informático será desconsiderado, porque constituirá somente um meio para o cometimento daquelas condutas.

Como visto, 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 propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos.

O legislador não contemplou a invasão de sistemas, como os de *clouding computing* (computação em nuvem), optando por restringir o objeto material aquilo que denominou dispositivo informático, sem, contudo, defini-lo. Atividades de comercialização de *cracking codes* (quebra de códigos) e de engenharia reversa de

software também não foram objeto da norma. Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira. Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo). Numa síntese, os tipos e penas da Lei nº 12.737/2012 não conseguem dar as respostas esperadas pela Sociedade para desestimular aqueles que abusam das facilidades tecnológicas (MPSP.MP.BR).

De acordo com Silva (2003):

> O aparecimento da informática no meio social ocorreu de forma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso a necessidade social aparenta estar desprovida da tutela de direito.

2.5 EVIDÊNCIA DIGITAL

A evidência digital abrange periféricos e dispositivos ligados à cena do crime, onde se pode coletar e averiguar dados ali contidos, seja em um computador ou um dispositivo móvel.

De acordo com Lisita; Moura; Pinto (2009, p.23):

> O aparecimento da informática no meio social ocorreu de forma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso a necessidade social aparenta estar desprovida da tutela de direito.

É dito que 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 de através de técnicas e ferramentas de perícia digital” (LISITA; MOURA; PINTO, 2009).

Como descreve a ACPO em seu segundo princípio, em um exame mais específico 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. Como os telefones celulares possuem diferentes softwares, hardwares e funcionalidades, vê-se a necessidade de escrever procedimentos específicos para diferentes categorias de aparelhos.

2.6 CADEIA DE CUSTÓDIA

O Departamento de Justiça dos Estados Unidos (MUKASEY, SEDGWICK e HAGY, 2001), sugere, 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 probatório;
- 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 COLETA DE DADOS

“A Computação Móvel proporciona a capacidade de mover fisicamente serviços computacionais junto aos usuários, permitindo ao ser humano ter acesso a recursos oferecidos por um sistema computacional” (WIESER, 1993).

Na Publicação Especial 800-101 do NIST (*National Institute of Standards and Technology*) (JANSON e AYRES 2007) os autores sugerem que a chave para o sucesso na análise forense de dispositivos móveis é a compreensão das características de *hardware* e *software* dos telefones celulares. Os dados dos assinantes e suas atividades por meio de celulares são muitas vezes uma fonte valiosa de provas em uma investigação. Portanto, para que a produção de provas possa ser realizada, conta-se com um conjunto básico de características, obtido a partir da maioria dos celulares, sendo este conjunto comparável entre diferentes aparelhos. Como exemplos de características podem ser citados: 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 ou 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.

Os autores recomendam sempre fazer a aquisição de dados física antes da aquisição lógica.

Ainda segundo Jansen e Ayres (2007):

> As ferramentas forenses adquirem informações dos dispositivos sem alterar o conteúdo, ou seja, em modo somente de leitura, utilizando equipamentos

> denominados de *Write Blocker* (ou bloqueadores de escrita). E, ainda, fazendo a geração de *hash* de modo a garantir a integridade dos dados coletados. Tal característica é muito importante perante um Juiz, sendo que cabe ao perito garantir a integridade das provas digitais por ele coletadas ou a ele confiadas.

As melhores práticas de análise forense em telefones celulares 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.

“Ao descrever as melhores práticas da análise forense digital, existem princípios fundamentais para todos os exames forenses e eles podem ser separados em fatores chaves e principais responsabilidades de todos os profissionais envolvidos:

- 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.

Além disso, descreve que na realização de um exame forense, o especialista forense 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 registro. 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.

De acordo com Craiger (2005):

> Documentar todas as atividades realizadas é crucial, por diversas razões. Em primeiro lugar, permite que o investigador possa manter atualizado o registro do que deve ser usado em depoimento e em segundo, permite ao tribunal (ou a quem estiver julgando) a possibilidade de verificar se os procedimentos forenses foram realizados corretamente. Finalmente, permite a recriação das atividades que foram realizadas durante todo o exame.

Como descreve a ACPO em seu segundo princípio, em um exame mais específico onde há necessidade de extração da informação direta do dispositivo, o examinador deve ter as competências e expertise necessária a fim de obter a informação e explicar a relevância e implicações dos procedimentos utilizados. Como os telefones celulares possuem diferentes softwares, hardwares e funcionalidades, vê-se a necessidade de escrever procedimentos específicos para diferentes categorias de aparelhos.

3.1 PROCEDIMENTOS DE BUSCA, APREENSÃO E PRESERVAÇÃO

Antes efetivamente de extrair os dados dos telefones celulares, 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 por objetivo preservar as evidências de tal forma a evitar a perda ou 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 questão mais importante é preservar de forma adequada os dispositivos que forem apreendidos, documentando-os conforme preconiza 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, documentá-la, coletar as evidências, realizar o acondicionamento, transporte e armazenamento da evidência de forma confiável, evitando danificá-la, primando pela sua preservação.

De acordo com Jansen e Ayres (2007):

> No processo de busca e apreensão, acena poderá ser fotografada e, se houver a presença de um perito na equipe, em havendo necessidade, será realizado um laudo local onde constarão informações acerca de todas evidências coletadas. Deve-se atentar também para os dispositivos móveis que estiverem conectados às *docking stations* ou ao computador, pois pode estar ocorrendo transferências de dados que, caso sejam interrompidas, poderão cessar a transferência de dados ou sincronização.

As abordagens propostas pelo NIST, ACPO e NFI descrevem a importância de isolar o dispositivo móvel da rede de comunicação. Assim, evita-se que dados recebidos pelo dispositivo após a sua apreensão não sobrescrevam dados já existentes. Pode-se citar o exemplo de das mensagens de texto SMS que, em alguns modelos de telefones celulares, sobrescrevem automaticamente as mais antigas quando uma nova mensagem chega. Assim, pode-se utilizar um invólucro que bloqueia o

recebimento dos dados para acondicionamento ou deve-se desligar o aparelho no momento em que for apreendido. Outra opção seria ativar o modo avião (*off-line*) nos dispositivos que tiverem tal opção, afim de evitar o desligamento completo do equipamento, inclusive economizando o consumo de bateria.

Cada uma das três alternativas tem suas 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 bloqueio 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 que 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 pessoa habilitada, pois uma interação antes da realização dos exames pode não ser adequada.

3.2 AQUISIÇÃO DE DADOS

“A aquisição consiste em extrair do telefone celular a informação para posterior análise” (SIMÃO,2011). A aquisição é realizada em um ambiente isolado da rede de comunicação do dispositivo por meio de hardware e software adequados para obtenção dos dados.

Antes de realizar a extração dos dados, o examinador deve evitar que o dispositivo se comunique com a rede de telefonia ou realize conexões com a rede Wi-Fi, *Bluetooth*, IrDA (Infravermelho). Para tanto, pode-se utilizar equipamentos específicos para isolar tal comunicação ou realizar intervenção direta no dispositivo, desabilitando tais serviços como já descrito na fase de apreensão e preservação.

O perito examinador deve iniciar os trabalhos de extração preferencialmente com a bateria do celular totalmente carregada e, quando for o caso, com uma fonte direta de

energia conectada. Desta forma evita-se a corrupção ou perda de dados durante o processo.

Para realizar a extração de forma adequada, deve-se observar que os dispositivos atuais possuem, além de memória interna, cartões de memória, e, a depender do dispositivo, dados armazenados na Internet por meio de aplicativos instalados (computação em nuvem), que não são citadas nas abordagens usadas atualmente. Assim o perito examinador deve levar em conta o objetivo dos exames que serão realizados, para avaliar até onde poderá extrair informações que se encontram disponíveis por meio do dispositivo.

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.

Segundo Janson e Ayres (2007):

> Também é importante a correta identificação do equipamento a ser periciado. A descrição do equipamento com dados do fabricante, marca, modelo e operadora podem ajudar na extração dos dados do dispositivo e na sua cadeia de custódia. A identificação dos telefones celulares pelo IMEI (*International Mobile Equipment Identifier*) faz-se necessária uma vez que esta numeração consiste em um número de 15 dígitos, cujos 8 iniciais indicam o TAC (*Type Allocation Code*), fornecendo o modelo e a origem, e os demais dígitos são uso do fabricante.

“ O chip ou cartão SIM (*Subscriber Identity Module*) é um cartão inteligente que possui microprocessador, usado para implementar segurança (autenticação e geração de chaves criptográficas” (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 suma importância que alguns critérios sejam fundamentais para ferramentas forenses, pois deve-se apresentar dados de tal forma de sejam úteis e necessários ao investigador.

De acordo com Janson e Ayres (2007):

> Alguns critérios são fundamentais para ferramentas forenses, devendo apresentar dados de tal forma que sejam úteis 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 intermediárias e apresentação dos resultados.

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 DOS DISPOSITIVOS MÓVEIS

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

De acordo com Simão (2011):

> 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. Em resumo, nem todos os dados armazenados na memória dos telefones celulares estão armazenados da mesma forma, mudando de acordo com o fabricante e modelo do telefone celular.

3.5 CÓDIGOS DE SEGURANÇA E CONTROLE DE ACESSO

Os dispositivos móveis possuem muitas formas de controles de acesso às suas aplicações para maior segurança aos seus usuários.

De acordo com Simão (2011):

> Muitos dispositivos móveis possuem formas de controles de acesso às suas funcionalidades, assim como os dispositivos GSM com PIN ativado que é um tipo de bloqueio de dispositivos, cujo o acesso só é concedido aquelas pessoas que conheçam a senha de quatro dígitos a ser fornecida. Além de bloqueios fornecidos pelo cartão SIM, há também aqueles fornecidos pelo sistema operacional do equipamento.

Um cartão SIM bloqueado só poderá ser acessado através da digitação do código PIN, que normalmente é configurado pelo usuário, e, caso este código seja digitado incorretamente por três vezes, o cartão solicitará o código PUK. O PUK vem pré configurado de fábrica e é fornecido no momento da aquisição do cartão SIM. Outra forma de obter o PUK é por meio de informação da operadora de telefonia ao qual o cartão está vinculado. Caso o PUK seja digitado errado por dez vezes o cartão SIM é definitivamente bloqueado. Assim é recomendável que o analista pericial verifique a quantidade de vezes que o PIN foi digitado incorretamente, e apenas tente a utilização de códigos PIN padrão se não restar apenas uma tentativa de erro (*Association of Chief Police Officers*, 2008).

Segundo ainda Simão (2011):

> Os controles de acesso fornecidos em nível de sistema operacional, em alguns modelos de dispositivos, podem ser contornados afim de fornecer o acesso ao telefone. Desta forma, caso o examinador se depare com este tipo de bloqueio deve se pesquisar sobre o modelo do dispositivo e seu SO, afim de tentar burlar o sistema de controle de acesso, ou buscar soluções alternativas, a exemplo de interrogar o proprietário do equipamento.

De acordo com Janson e Ayres (2007):

> Os métodos baseados em hardware e software são específicos para cada dispositivo aonde algumas abordagens devem ser observadas a exemplo de contatar o fabricante ou a operadora de telefonia, afim de descobrir possíveis *backdoors* ou vulnerabilidades do equipamento em questão; verificar a documentação do dispositivo fornecida pelos fabricantes para saber quais medidas tomar; verificar se existem profissionais no mercado especializados em recuperação das evidências; contatar equipes de assistência técnica especializada a fins de descobrir se há alguma forma de obter as evidências a partir de informações técnicas do equipamento.

"Outras abordagens usam procedimentos específicos, em nível de software, para burlar o sistema de autenticação dos dispositivos, podendo variar muito a depender da marca, modelo e versão do dispositivo e do sistema operacional instalado" (CANNON,2011).

Segundo Knijff (2001):

> Seria ler o chip de memória diretamente do circuito de memória, nesta abordagem, a especificação de hardware do equipamento influencia na forma como os dados serão obtidos, sendo mais complexa tanto no processo de obtenção bem como no de análise dos dados, uma vez que deverão ser reorganizados em um ambiente diferente disponibilizado pelo dispositivo móvel.

3.6 MEMÓRIAS REMOVÍVEIS

As memórias removíveis na atualidade são muito utilizadas em celulares, pois sua capacidade de armazenamento de dados de um dispositivo móvel é grande.
Segundo Jansen e Ayres (2007):

> A aquisição das informações presentes nestas memórias pode se dar através de ferramentas utilizadas comumente em pericias de computadores. Nem todas a ferramentas forenses de extração de dados de telefone celular

> possuem a capacidade de obter as informações armazenadas no cartão de memória, devendo o examinador saber o funcionamento destas ferramentas e complementar a aquisição de dados, quando for o caso, utilizando outros meios.

De acordo com Simão (2011):

> Deve-se atentar que as boas práticas exigem que na aquisição dos dados de memórias removíveis, utilize-se leitor de cartões compatíveis com a mídia em questão, devendo o examinador proteger a memória da escrita indesejada usando bloqueadores de escrita, seja por software ou hardware.

4 EXAME DO TELEFONE CELULAR

O exame é uma etapa onde o analista pericial extrairá as informações relevantes dos dados que foram adquiridos.

Segundo Ashcroft (2001):

> Há uma necessidade que o especialista tenha o conhecimento necessário para lidar com a evidência, devendo ter treinamento específico para esta finalidade. Os exames realizados em telefones celulares devem ter um objetivo claro daquilo que se está buscando, onde o examinador deve ter conhecimento do caso em questão. Caso contrário, o relatório (laudo) descrevendo o resultado dos exames não passará de uma simples extração das informações que estavam no dispositivo para outro tipo de suporte.

Observando o que ocorre atualmente no processo investigativo brasileiro, a autoridade que realiza a solicitação formal do exame deve buscar esclarecer ao máximo em tal documento o motivo que ensejou o pedido.

De acordo com Simão (2011):

> Há casos que, a depender daquilo que está sendo apurado, o exame pode seguir paradigmas diferentes na análise dos dados extraídos do telefone celular. Por exemplo, em um caso de abuso sexual infantil, o examinador deve iniciar o exame buscando imagens e vídeos que possam ter relação com o objeto da solicitação. Já em casos de tráfico de drogas, a troca de mensagens e relação dos contatos pode ser o primeiro passo.

Segundo Jansen e Ayres (2007):

> Na análise dos dados extraídos, o examinador deve basicamente se atentar as configurações como data e hora, linguagem, configurações regionais,

> contatos, agenda, mensagens textuais, chamadas (realizadas, recebidas e não atendidas), imagens, vídeos, áudio e mensagens multimídia.

De acordo com Simão (2011):

> Entretanto, com a evolução dos dispositivos móveis, a complexidade dos exames tem aumentado, uma vez que os analistas devem buscar também e-mails, históricos de navegação web, documentos, informações de GPS, aplicativos específicos, informações relativas à computação em nuvem, e também examinar a mídia removível que está sendo usada pelo telefone celular, devendo, a depender da situação, fornecer subsídios à autoridade que coordena a investigação para solicitar mais exames.

“O analista pericial deve buscar informações sobre os eventos envolvidos, determinar a natureza dos eventos, buscar cronologia dos eventos, determinara motivação e como o ato delituoso ocorreu” (JANSEN e AYRES, 2007).

Dada a grande variedade de telefones celulares e sistemas operacionais voltados para estes tipos de dispositivos, vê-se então que são necessários métodos de análise forense específicos, que serão utilizados a depender da marca, modelo e sistema operacional do dispositivo. “Ante o exposto, é necessário que o examinador se especialize em específicos tipos de telefones celulares, uma vez que o método utilizado em uma situação pode não ser adequado em outra” (ASHCROFT, 2001).

4.1 EXTRAÇÃO E CÓPIA FORENSE DE DADOS

O analista pericial para ter acesso a evidência digital faz se necessário criar uma cópia, verificando e certificando-se que a cópia esteja íntegra e idêntica.

De acordo com Carroll, Brannon e Song (2008):

> Se os peritos tiverem acesso a evidência original, precisa-se criar uma cópia de trabalho e guardar o original da cadeia de custódia, verificando e certificando que a cópia em sua posse está intacta e inalterada (costuma-se fazer isso verificando um *hash* da evidência).

Segundo Craiger (2005):

> Criar uma imagem forense é importante por várias razões, inclusive do ponto de vista jurídico, onde os tribunais as aceitam, pois demonstra que todas as provas foram capturadas. Em uma perspectiva de investigação, nessas imagens é possível que se possa encontrar conteúdo de arquivos excluídos anteriormente e outros dados do ambiente em questão. Essa informação poderá não estar disponível caso apenas uma cópia lógica da evidência for feita.

De acordo com Eleutério e Machado (2011):

> Criar uma imagem forense de um dispositivo a partir da cópia para arquivos, em um processo semelhante à cópia bit a bit ou espelhamento. Existem algumas vantagens ao usar este tipo de procedimento, entre elas está a possibilidade de compactar os arquivos de imagem, economizando a utilização do disco de destino (exigindo mais processamento durante a extração) e a maior facilidade de replicação dos dados, uma vez que os arquivos podem ser facilmente copiados para outros dispositivos e em quaisquer outros sistemas operacionais.

4.2 REQUISIÇÃO FORENSE

Segundo a CCIPS (CARROLL, BRANNON e SONG, 2008), o exame deve começar pela verificação da existência de informações suficientes para prosseguir com todo o processo de perícia. Deve-se ainda, certificar-se de que existe um pedido claro para

realização da perícia, além da existência de dados suficientes para a tentativa de obtenção das respostas as perguntas do pedido.

4.3 PREPARAÇÃO/EXTRAÇÃO

Segundo a CCIPS (CARROLL, BRANNON e SONG, 2008), após a requisição forense e verificação da integridade dos dados a serem analisados, é necessário a criação de um plano para extração dos dados, além da organização e refinamento do pedido em perguntas. Com um plano de atuação estipulado e focado nas especificidades do caso requerido, são escolhidas as ferramentas forenses que melhor permitirem responder ou ajudar na obtenção de informações importantes para a construção das respostas as perguntas do pedido.

Segundo Eleutério e Machado (2011):

> Os principais procedimentos atrelados a esta fase são, a recuperação de arquivos apagados e a indexação de dados, que consiste em varrer todos os dados (bits) do dispositivo, localizando todas as ocorrências alfanuméricas, organizando-as de forma que seja possível acessá-las e recuperá-las rapidamente.

“Em segundo princípio para Evidências Digitais, no exame onde há necessidade de extração da informação direta do dispositivo, o perito deve ter as competências necessárias para obter a informação e ser capaz de explicar a relevância” (ACPO, 2008).

4.4 IDENTIFICAÇÃO

Nesta fase se realiza a busca por informações e dados, que posteriormente serão utilizados para análise pericial.

Segundo Ruback (2011):

> Nesta etapa, será feito um pré-processamento, que consiste na realização de procedimentos automatizados para processar os dados extraídos na etapa anterior facilitando o processo do perito. Dentre outros procedimentos citados, são efetuados os cálculos dos *hashes* de todos os arquivos encontrados, categorização dos arquivos de acordo com a assinatura e geração de índices de palavras para utilização em buscas automatizadas.

Ainda de acordo com Ruback (2011):

> Com os dados processados, podem ser realizados procedimentos de filtragem, para que se possa separar dados considerados irrelevantes ao exame e destacar os mais relevantes. O objetivo é reduzir a quantidade de informações a analisar na próxima fase.

De acordo com Carroll, Brannon e Song (2008):

> Neste ponto do processo, é aconselhável que os peritos informem aos requerentes suas conclusões iniciais, informalmente, pois, dependendo do estágio do processo, os dados relevantes extraídos e identificados podem dar ao solicitante informações suficientes para continuar o caso, fazendo com que os peritos não precisem mais prosseguir.

4.5 RELATÓRIO/LAUDO

Mediante a todo trabalho já realizado o relatório é importante para dar valor a todo o processo forense. É a finalização de todos esforço do processo, traduzido com clareza, através da apresentação dos resultados e das conclusões obtidas.

De acordo com Janson e Ayres (2001):

> O momento para se redigir o relatório é quando o examinador já esgotou todas as possibilidades de interpretar os dados extraídos do telefone celular e já possui as conclusões pertinentes que devem ser agora documentadas de forma clara, objetiva e conclusiva. Todo o recurso disponível deve ser utilizado pelo examinador para poder passar aos leitores as informações obtidas no decorrer dos exames. Figuras, tabelas, anexos, mídias, óticas com vídeos extraídos, devem ser utilizados para evitar que informações importantes, evidenciadas pelo examinador durante as outras etapas, não deixem de ser documentadas, tendo em mente que o resultado de todo seu trabalho é o relatório.

"O examinador só deve criar o relatório quando esgotarem todas as possibilidades de interpretação dos dados extraídos do dispositivo móvel e já tiver conclusões pertinente sobre elas" (SIMÃO, 2011).

Segundo Eleutério e Machado (2011):

> O laudo é um documento técnico-científico, que deve descrever com objetividade e clareza os métodos e exames realizados e são formandos geralmente pelas seguintes partes: preâmbulo (identificação do laudo), histórico, material (descrição do material analisado), objetivo, considerações técnicas/periciais (conceitos e informações relevantes), exame (parte descritiva e experimental do laudo) e respostas aos quesitos/conclusões (um resumo objetivo dos resultados obtidos).

"Esta é a fase na qual é criado o documento ou laudo pericial com as conclusões dos peritos, de modo que o solicitante do pedido possa entender e utilizar essas conclusões no caso" (CAROLL, BRANNON e SONG,2008).

5 FORENSE EM ANDROID

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

Várias literaturas especializadas, 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 somente consolida ainda mais a importância da documentação adequada e dos registros das ações tomadas pelo perito em todas as fases de uma metodologia.

Com a grande quantidade 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.

De acordo com a NIST (Jansen e Ayres, 2007) e (Hoog, 2011), há duas maneiras possíveis para extrair dados de um dispositivo: aquisição física e aquisição lógica. A aquisição consiste na cópia forense bit a bit de um dispositivo de armazenamento inteiro (um cartão SD por exemplo), não contando com sistemas de arquivos para acessar os dados, que são disponibilizados em forma mais bruta. Desta forma, é possível obter uma quantidade significativa de dados excluídos que podem ser

analisados, porém este tipo de extração pode demorada e mais difícil de ser executada.

No caso de aquisição lógica, ocorre a extração de dados alocado, acessíveis ao sistema de arquivo do dispositivo, por exemplo, diretórios arquivos e partições. Neste tipo de extração, a análise pode ser mais rápida, pois seus procedimentos são mais fáceis de executar.

Segundo Hoog (2011):

> No Android, a extração lógica não fornece acesso direto ao sistema de arquivos e opera em um nível abstrato e menos eficaz do que as técnicas tradicionais em outros dispositivos ou computadores, mesmo assim, ainda é eficaz, pois retorna dados importantes.

Há um vasto número de ferramentas disponíveis para extração e análise forense em dispositivos móveis, inclusive para os que utilizam *Android*, entre elas as ferramentas forenses comerciais e ferramentas *open-surce*[2]. As ferramentas forenses são aceitas por diversos órgãos e são projetadas para o exame forense nos dispositivos móveis com nenhum ou o mínimo de impacto na interação.

Atualmente o *UFED Touch Ultimate*[3], é a ferramenta comercial 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.

[2] Open-surce é um termo em inglês que significa código aberto. Isso diz respeito ao código fonte de um software, que pode ser adaptado para diferentes fins (Softwarelivre.org).
[3] http://www.cellebrite.com/Mobile-Forensics/Products/ufed-touch

Figura 2- Imagem da Cellebrite - UFED Touch Ultimate

O Linux Forense permite soluções alternativas baseadas em software livre, com diversos recursos para as mais variadas necessidades. As distribuições Linux forenses são customizações de distribuições conhecidas geralmente voltadas para a produção de imagens periciais de dispositivos de armazenamento de dados e memória, assim como análise completa destes dispositivos. O *Santoku*[4] Linux baseada no Ubuntu foi desenvolvido pelo *Via Forensic* com foco voltado para análise de telefones 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*[5] e *scripts* para descompactar dados.

[4] https://santoku-linux.com

[5] O termo *malware* é proveniente do inglês "*malicious software*" ("Software malicioso"); é um software destinado a infiltrar em um sistema de computador alheio de forma ilícita, com intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não) https://pt.wikipedia.org/wiki/Malware.

Figura 3- Imagem da Ferramenta Santoku

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.

Portanto com a grande necessidade de se identificar os infratores que cometem crimes computacionais e para que os mesmos sejam punidos a perícia forense em informática conta com as mais diversas ferramentas que auxiliam na busca e padronização de evidências, sendo algumas ferramentas de âmbito comercial e ou por meio de software livre.

5.1 METODOLOGIA PARA AQUISIÇÃO DE DADOS EM *SMARTPHONES*

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), pelo Departamento de Justiça dos Estados Unido, pela *Association of Chief Police Officers* (ACPO, 2008) e *Netherlands Forensic Institute* (Instituto Forense da Holanda).

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.

Diversos são 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.

Tendo em vista à complexidade do *Android*, 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 apresenta a etapa para aquisição de dados de um telefone celular com o sistema operacional *Android.*

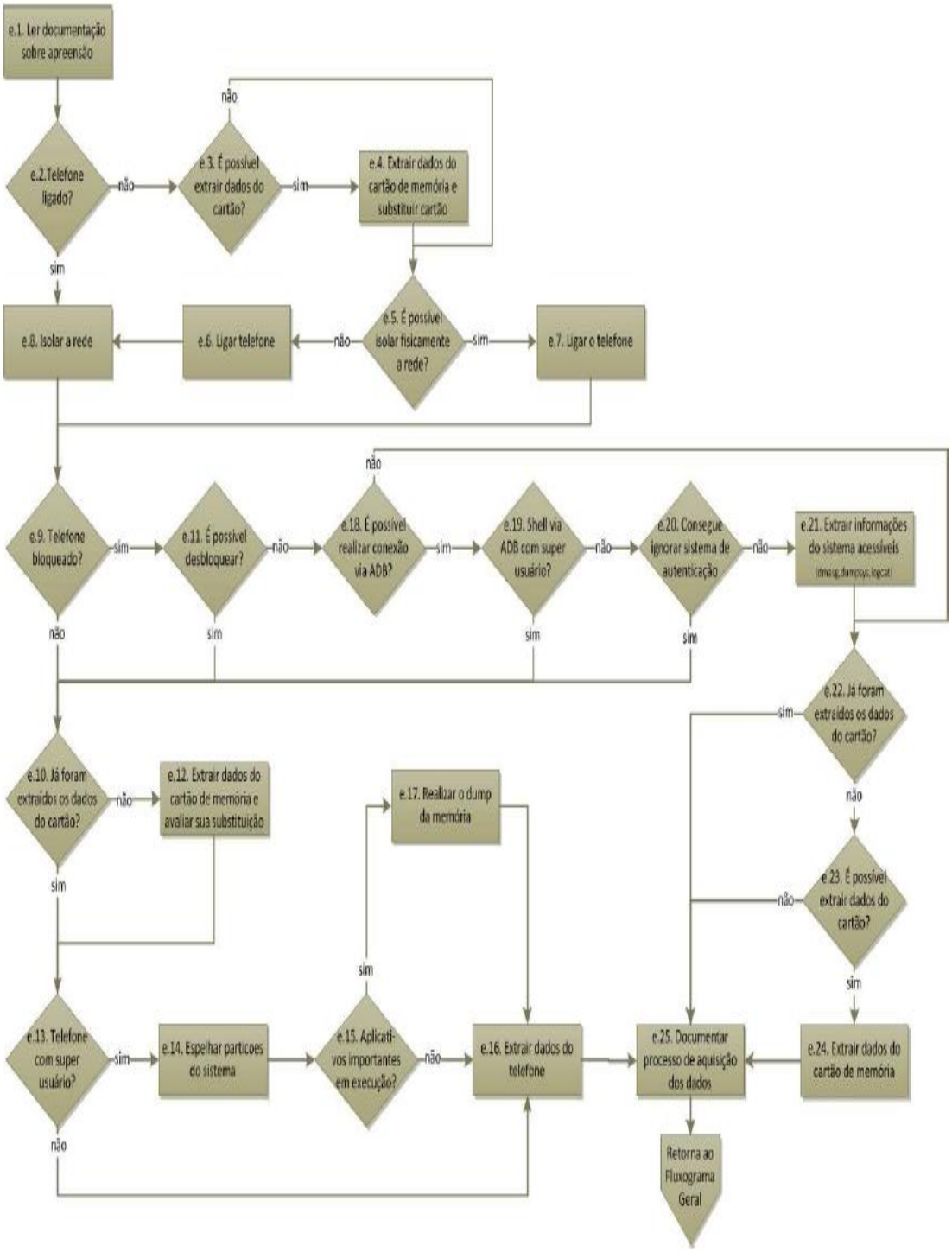

Figura 4- Etapa de aquisição de dados de um telefone celular com sistema operacional Android (Simão, 2011).

5.2 SOFTWARE ANDROID 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 recurso necessário para o desenvolvimento de aplicativos *Android*, que inclui, entre outras ferramentas e funcionalidades as bibliotecas de software, APIs, material de referência para desenvolvedores e emulador. É gratuito e pode ser utilizado nos principais ambientes operacionais como Linux e Windows.

Duas ferramentas importantes do SDK são: o emulador *Android*, onde é possível ter uma implementação 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*) consiste em uma aplicação cliente-servidor usada para conectar a 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.

5.3 O ANDROID DEBUG BRIDGE

O *Android Debug Bridge* (ADB) é uma ferramenta versátil que disponibiliza uma interface para um emulador ou para um dispositivo *Android* conectado ao computador. É uma aplicação cliente-servidor composta por três componentes (Google Inc, 2012e):

- Cliente: roda na máquina à qual o dispositivo está conectado e é utilizado por um terminal ou linha de comando através da ferramenta ADB (comando adb);
- Servidor: é executado em segundo plano como um serviço e fica na máquina à qual o dispositivo está conectado gerenciado a comunicação entre o cliente e o serviço (daemon) que está em execução;
- Serviço (daemon): 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 "s*hell*", 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.

Digitando *adb* no *prompt* de comando, será apresentada uma lista de comandos disponíveis no ABD, 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.

5.4 MODELO DE SEGURANÇA ANDROID

O *Android* é baseado no Linux e, por isso, muitos conceitos do modelo de segurança aplicado nele foram adaptados. Um conceito central já abordado é o de usuários e grupos, onde cada usuário utilizador recebe um ID de usuário (*user ID – UID*) quando é criado.

No *Android*, quando um aplicativo (*app*) é instalado, um novo ID de usuário (único no dispositivo) é criado 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.

Durante a instalação, o sistema cria um diretório específico no dispositivo para armazenar os dados do aplicativo, permitindo que somente a aplicação criadora possa acessar os dados. Este é um padrão, mas várias exceções deste modelo são possíveis.

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 uma aplicação é instalada pela primeira vez o *Android* confere o arquivo .*apk* para garantir que ele tem uma assinatura digital válida que identifica o desenvolvedor. Com o 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.

De acordo com Lessard e Kessler (2010):

> Os mecanismos de segurança implementados no Android podem impedir um determinado exame forense, desta maneira, é recomendado que o primeiro passo no exame seja a análise dos cartões SD, caso estejam disponíveis, pois geralmente usam sistema de arquivos FAT32, que são mais fáceis de visualizar e analisar utilizando ferramentas tradicionais.

5.5 PERMISSÕES DE SUPER USUÁRIO

O *Android* armazena a maioria das informações tais como, contatos, chamadas, banco de dados e mensagens de texto em seu diretório.

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.

Segundo Hoog (2011):

> Se houver a necessidade de realizar o *rooting* em um aparelho novo ou com uma nova versão do Android, é preciso que o processo seja realizado em um aparelho separado para que as técnicas sejam testadas e o seu funcionamento validado. A perda de informações ou comprometimento de dados do dispositivo tem que ser avaliada antes da execução em um aparelho apreendido.

De acordo som Simão (2011):

> Com acesso de super usuário é possível, por meio de um shell, realizar qualquer tarefa dentro do sistema operacional, a exemplo de realizar overclocks, backups de aplicativos restritos, acessar diretórios das partições do sistema, acessar partições de sistema e dados do usuário através da ferramenta ADB. Alguns aplicativos também podem ser executados com perfil de root, perdendo as restrições impostas por padrão do sistema.

6 ESTUDO DE CASO

Este capítulo apresenta um estudo de caso detalhando alguns métodos usados e os principais procedimentos necessários para uma correta análise pericial em um *smartphone* com sistema operacional *Android.*

Este estudo de caso apresenta um cenário mais comum quando um *smartphone* é apreendido e é necessário extrair dados para um exame, ou seja, onde o aparelho é de um usuário comum, encontra-se ligado, sem restrições de acesso e sem permissões de super usuário. Serão relatadas como se dá a extração de SMS, MMS e extração lógica de dados do *smartphone*, com exemplos de procedimentos necessários para análise de dados.

6.1 AVALIAÇÃO DO CENÁRIO

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.

De acordo com Simão (2001):

> 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 buscadas no caso apresentado, são baseadas nos dados possíveis de serem extraídos, sem a relação com um caso específico real ou fictício. As informações mais comuns são registros de chamadas, mensagens, vídeo e imagens.

Neste cenário, será utilizado o modelo de *smartphone* com as seguintes características:

- Fabricante e Modelo: LG Electronics – LG-E612f (Software: LG-E612f-v10b);
- Versão do Android: 4.0.3;
- Versão do *Kernel*: 3.0.8-perf lgeletronics@lgcmp09-sp;
- IMEI: 352623052850685;
- Condições: Aparelho ligado, sem bloqueio de acesso, sem permissões de super usuário instaladas, em modo avião e sem danos aparentes.

É de suma importância enfatizar que estas informações devem constar no processo de documentação da apreensão e deve estar disponível para o perito.

6.2 METODOLOGIA PARA AQUISIÇÃO DE DADOS

De acordo com (Simão ,2011), a Figura 5 demonstra o fluxo a ser seguido no processo de aquisição de dados para o cenário proposto servindo como base para ilustração do estudo de caso e a descrição das etapas previstas.

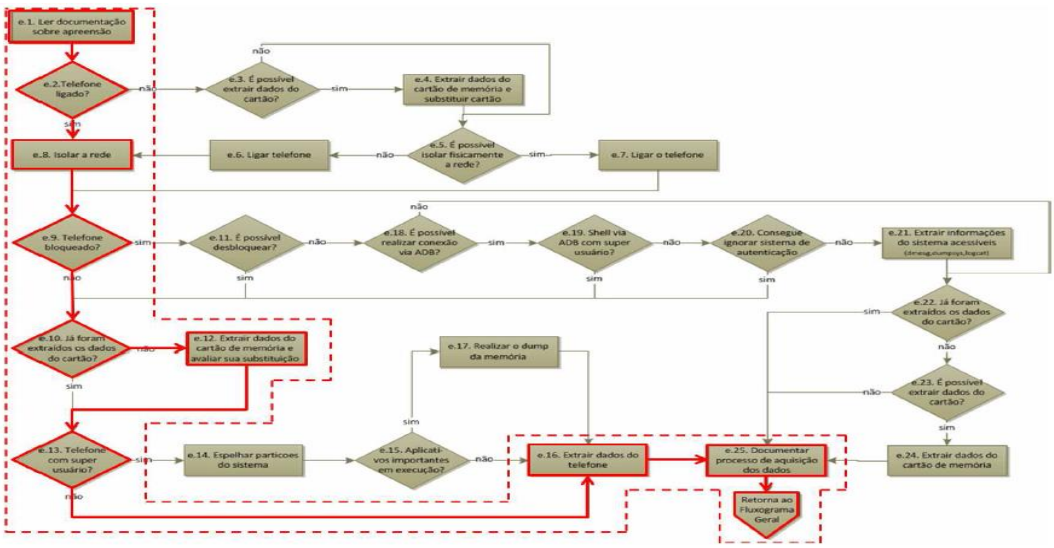

Figura 5- Etapa de aquisição dos dados de um telefone com o sistema operacional Android, sem bloqueio e sem super usuário. (Simão,2011).

Para obter as informações de um dispositivo móvel é necessário que haja um caminho para cada etapa no processo de investigação.

Nos processos descritos por (Simão, 2011), após ler a documentação e obter, entre outras informações, a anotação de que o dispositivo está em modo avião e a descrição completa do aparelho encaminhado para a extração dos dados, o analista ou perito constatará que este encontra-se ligado e sem bloqueio de acesso. A partir deste ponto, pode realizar a aquisição dos dados.

6.3 CONFIGURANDO A MÁQUINA VIRTUAL

Para instalar o *Santoku* deve-se primeiro fazer o download do arquivo disponível em (https://www.santoku-linux.com/download). Para executar o *Santoku* devemos instalar o software de máquina virtual na versão mais recente do Virtual Box 4.1.18, disponível no site (https://www.virtualbox.org/wiki/Downloads). Após o download, instale o software em sua estação de trabalho forense, em seguida, siga os passos passa iniciar a máquina virtual.

Localize na virtual box “Novo” para criar uma nova VM, logo em seguida selecione o Linux/Ubunto de 64 bits.

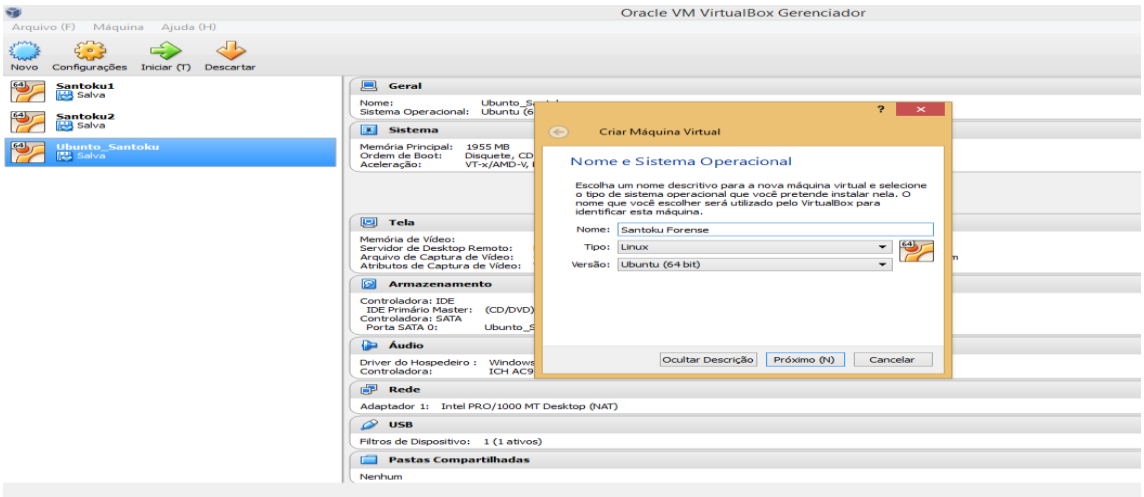

Figura 6-Criando Nova Virtual Box

Nesta próxima etapa aparecerá na tela a caixa de memória, na qual deve-se selecionar uma quantidade adequada, pois o tamanho para a máquina virtual 512 MB é o recomendo, no entanto aumentaremos a dimensão da memória para 1024 MB para deixar a máquina virtual mais rápida. Para utilizarmos o Android Virtual *Device* (AVD), recomenda-se selecionar ao menos 4 Giga de memória, em seguida vamos clicar em “Próximo”.

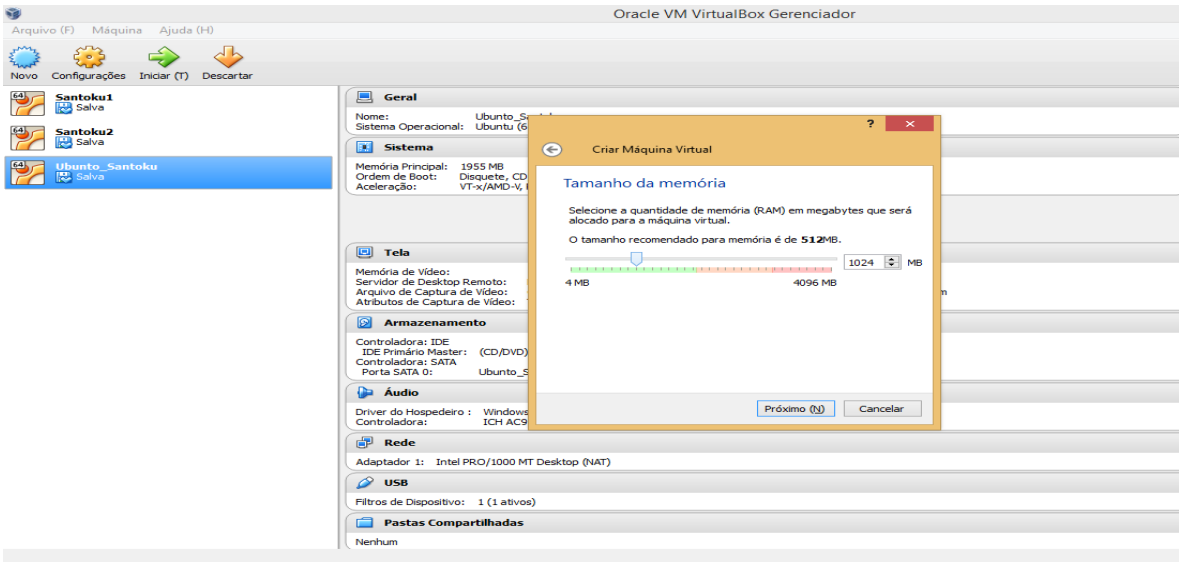

Figura 7-Alocando memória no Virtual Box

Na próxima tela temos que nos certificar se o disco de inicialização (*Disk Starup*) está marcado, em seguida, selecione criar novo disco rígido e a opção VDI (*Virtual Box Disk Image*) e clicamos em “Próximo”.

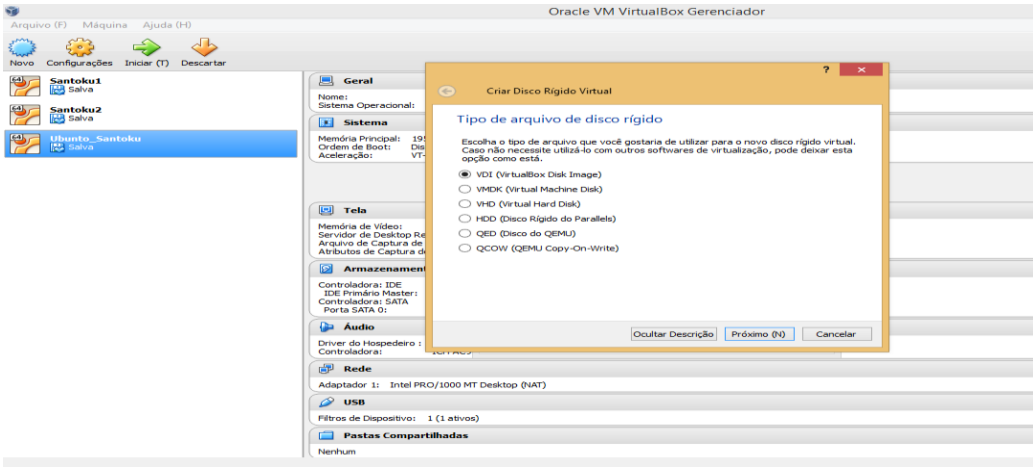

Figura 8-Criando tipo de arquivo de Disco Rígido

Nesse instante selecione o item dinamicamente alocado e clica em continuar, na próxima etapa escolha o local do disco rígido virtual, para armazenar o mesmo em seguida clicar em salvar. Posteriormente ajuste o “tamanho” para alocar o disco, onde o recomendado é de 40 gigas. Ao terminar, clica em “Criar”.

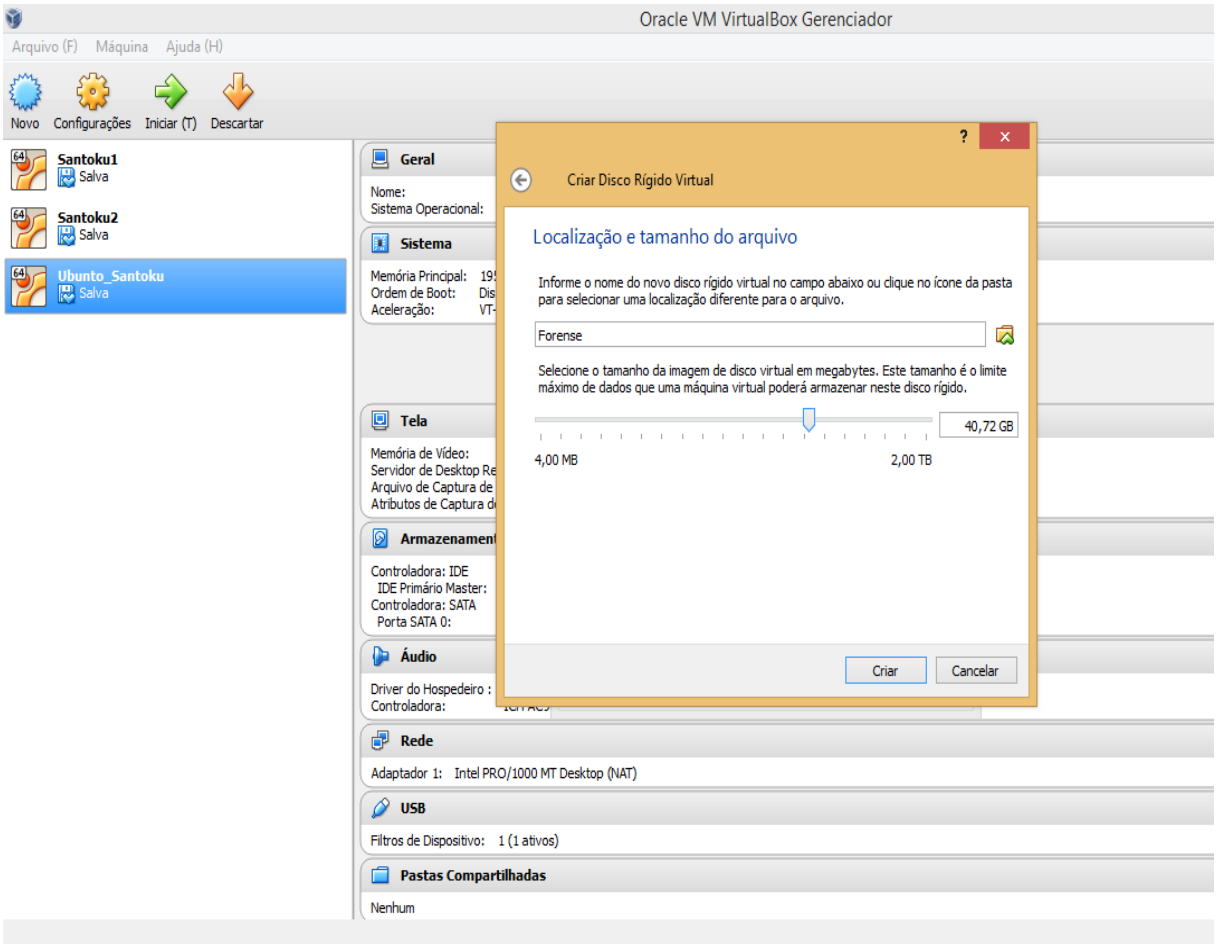

Figura 9-Localização e tamanho do disco rígido

Após feito as configurações necessárias, insira o *Santoku*-Linux à máquina virtual recém-criado. Isto é o mesmo que colocar um CD (*Compact Disc*) ou DVD (*Digital Versatile Disc*) para inicializar e instalar um novo sistema operacional. Para isso, selecione o arquivo criado e vá em “Configurações” no topo da tela. Selecione a opção

de “Armazenamento” e em seguida clica em ícone do CD ao lado do “Controlador IDE”.

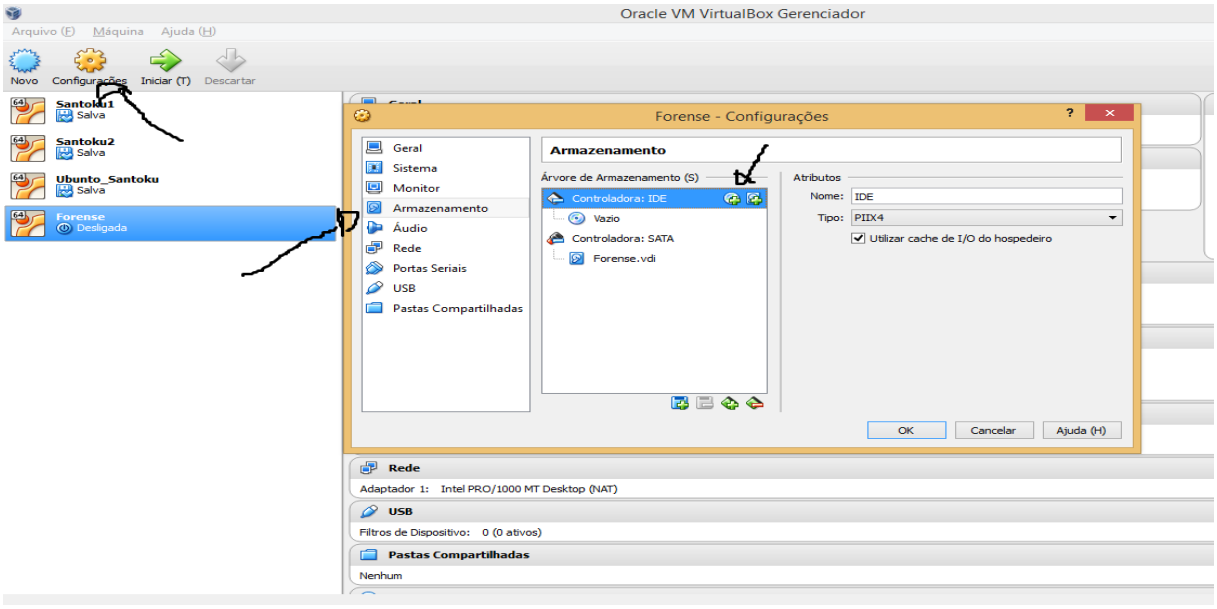

Figura 10-Atribuindo o *Santoku* a máquina virtual

Um aviso aparecerá pedindo para escolher um DVD virtual, selecione “Escolha disco” neste momento abrirá à pasta onde está alocado o *download* do arquivo *Santoku*, clica em “Abrir” e depois “Ok”.

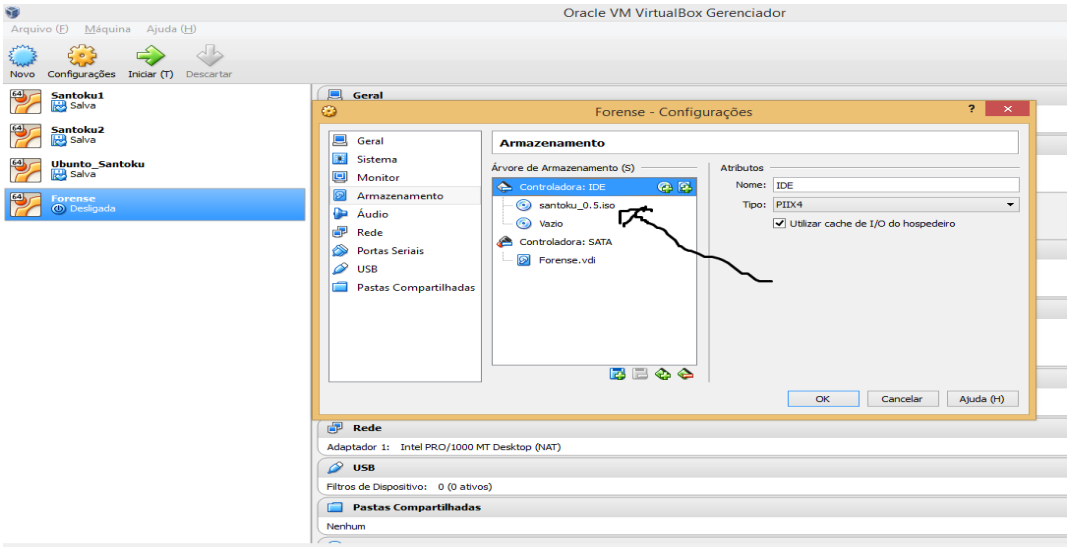

Figura 11-Inserindo o arquivo *Santoku*

6.4 INSTALANDO O *SANTOKU*

Agora já podemos clicar em “Iniciar” na tela principal do virtual box para carregar a máquina virtual. Quando iniciada a VM vai aparecer na tela algumas opções de instalação do *Santoku,* no entanto selecione a opção “*Install – start the installer directly*”.

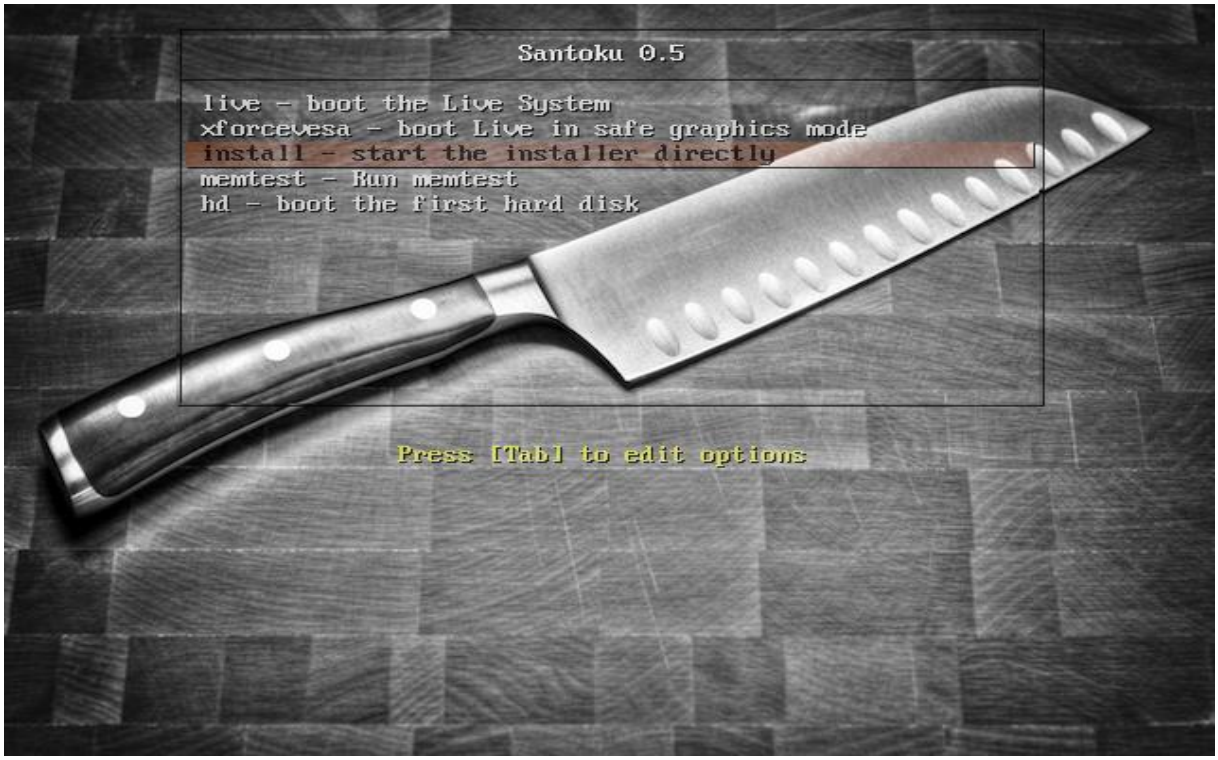

Figura 12- Instalação do *Santoku.*

Após ter concluído a instalação abrirá a tela para a escolha do idioma, fuso horário e configurações de relógio, após isso selecione “apagar o disco e instalar o *Santoku*” na tela de instalação. A partir daí, adicione seu nome de usuário e senha e clique em “instalar”.

6.5 GERENCIANDO O SDK

A ferramenta *Santoku* vem previamente com SDK instalado, porém é necessário atualizar as plataformas do SDK Manager. Para fazer a atualização vá até ao *Santoku* logo em seguida ferramentas de Desenvolvimento e por fim gerenciador *SDK,* marque a caixa ao lado das versões do Android e selecione “instalar pacotes”, em seguida aceite tudo para instalar.

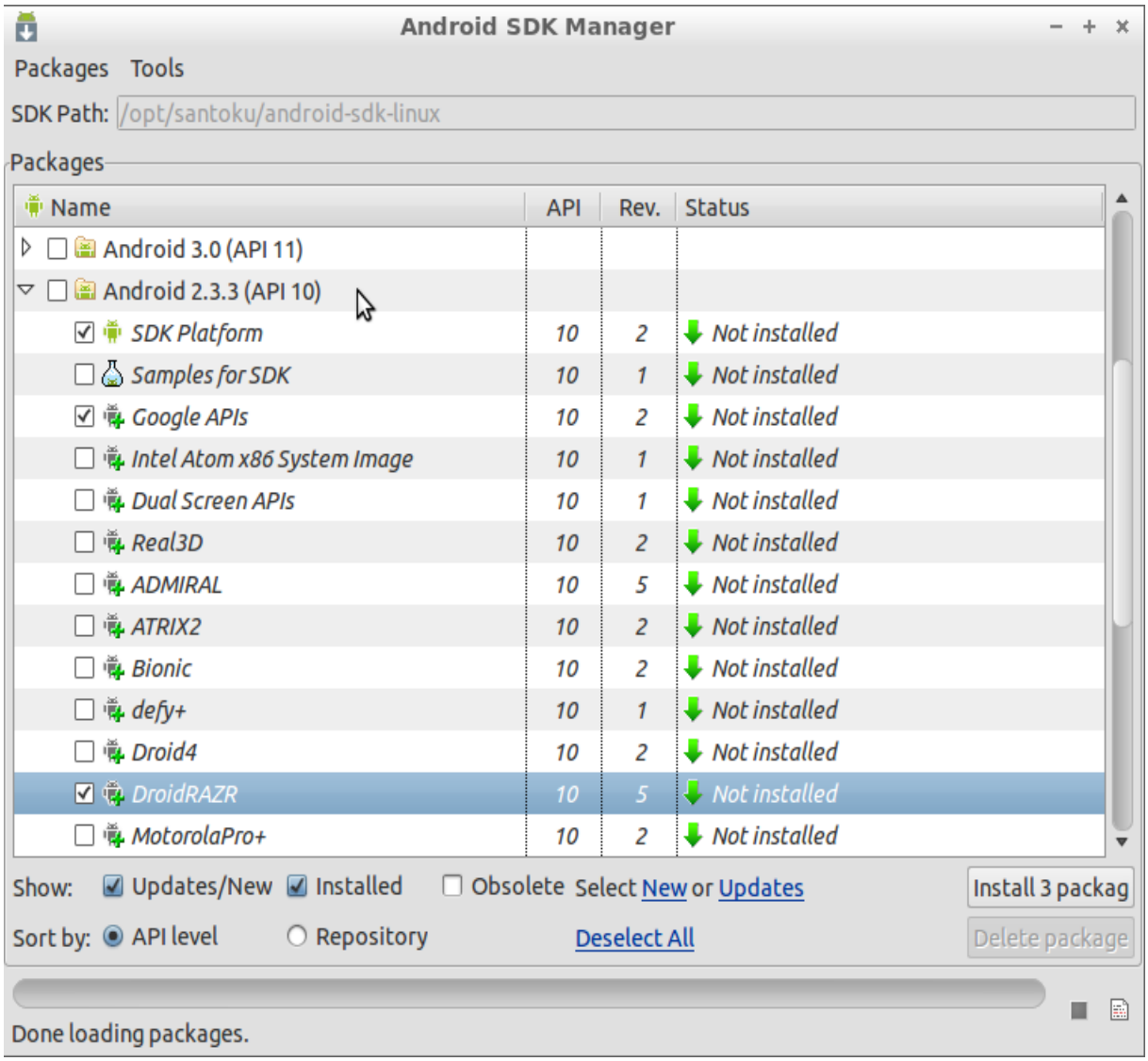

Figura 13-Gerenciando e instalando *SDK*

6.6 CONTRUINDO UM DISPOSITIVO VIRTUAL

Para construir um dispositivo virtual selecione “ferramentas” em seguida “criar AVDs”, logo depois clica em “novo”. O “*Targe*t” permite escolher o sistema operacional em nosso AVD. Se desejar podemos escolher o tamanho do SD, e ainda adicionar recursos de *hardware* expandidos além do que está na tela do *Android Virtual Device.* Neste caso escolha o Android 2.2, no entanto pode-se escolher qualquer tipo do mesmo que esteja disponível na ferramenta, em seguida retornará à janela como mostra a figura abaixo.

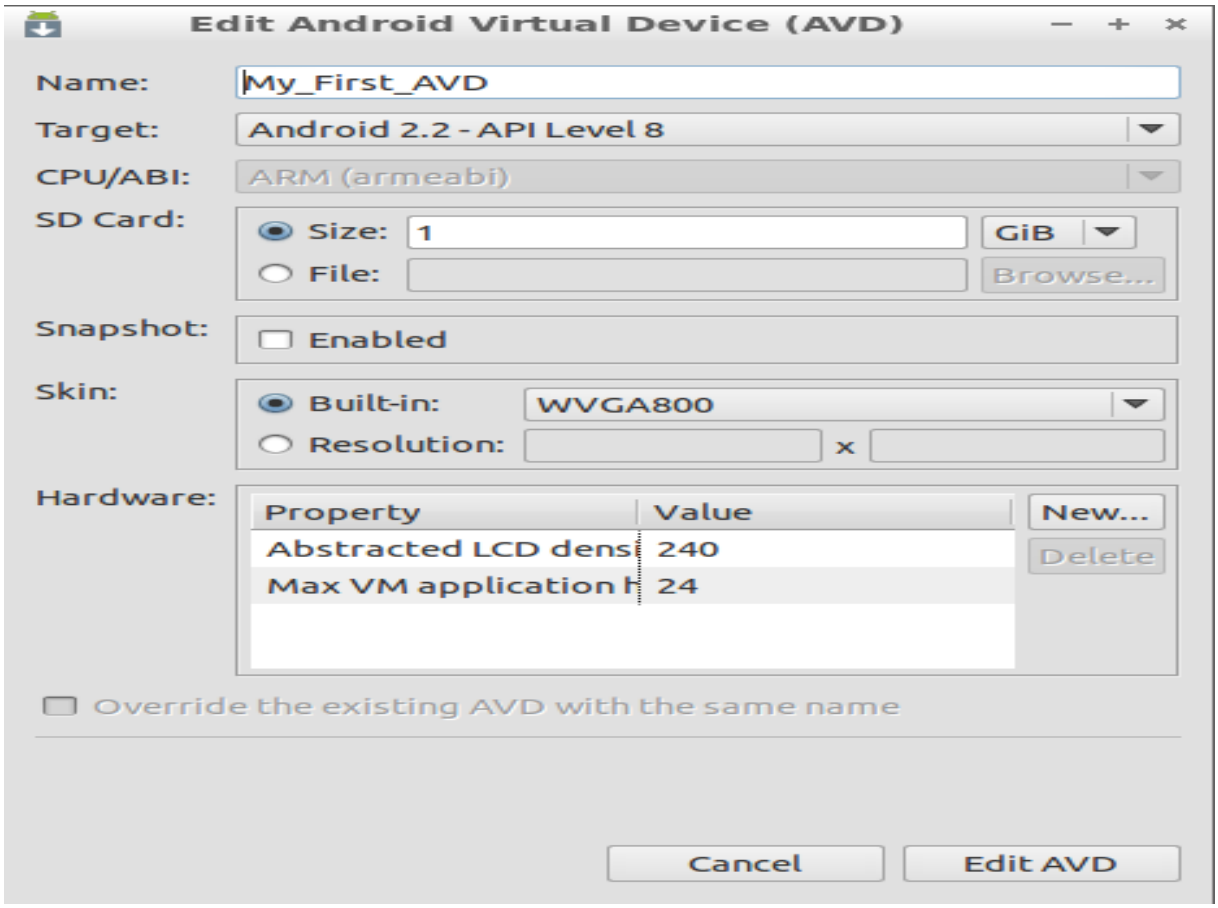

Figura 14- Editando o *Android Virtual Device* (AVD)

No caso de precisar alterar as configurações do *Android Virtual Device* (AVD), vá em “Editar” na janela principal do gerenciador de AVD e ele retornará à janela para realizar

as alterações necessárias. Uma vez criado o *virtual Device*, basta clicar em “Start”. Neste instante selecione as opções aplicáveis na próxima tela e escolher a opção “*Launch*”.

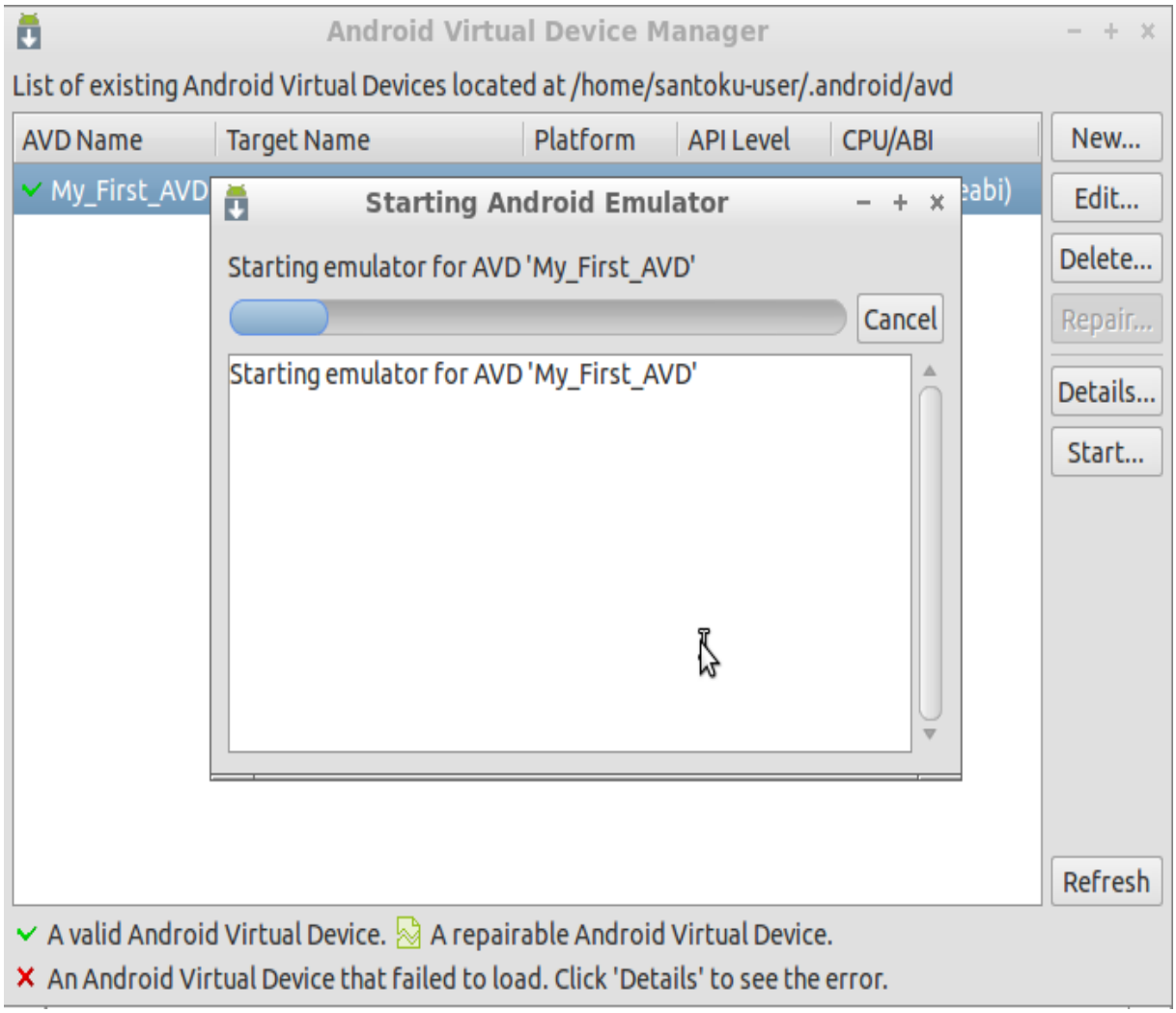

Figura 15-Startando o Emulador *Android Virtual Device*

Em alguns casos pode ocorrer algum erro enquanto o *santoku* está sendo instalado e o recurso SDK pode vir a não fazer as atualizações necessárias. Neste caso deve-se baixar o pacote e instalar junto a ferramenta forense que está sendo utilizada.

6.7 INSTALAÇAO DO APK PARA O EMULADOR

O emulador deve iniciar e ligar imediatamente pela ferramenta *Santoku*. Para testar o emulador e confirmar se o mesmo foi reconhecido, abra o terminal e digite:

"*sudo adb devices".*

Na tela deve aparecer a seguinte mensagem:

"List devices attached emulator-5554 devices".

No entanto se não aparecer esta mensagem e ou aparecer "*off-line*", espere por 60 segundos, pois o reconhecimento ainda não foi feito pelo *Santoku*. Após passado o tempo necessário de espera, novamente no terminal digite: "*sudo adb devices".* Feito o reconhecimento pela ferramenta abrirá na tela o emulador como mostra a figura abaixo.

Figura 16-Inicialização do Emulador

6.8 INSTALANDO E EXECUTANDO AFLOGICAL-OSE

Para instalar o *AFLogical Ose* é necessário que o dispositivo esteja conectado através do cabo USB. Para constatar que o dispositivo foi reconhecido, vá no ícone "*Devices*", escolha a opção "USB *Devices*" que abrirá uma janela mostrando que o dispositivo está conectado como mostra a figura abaixo.

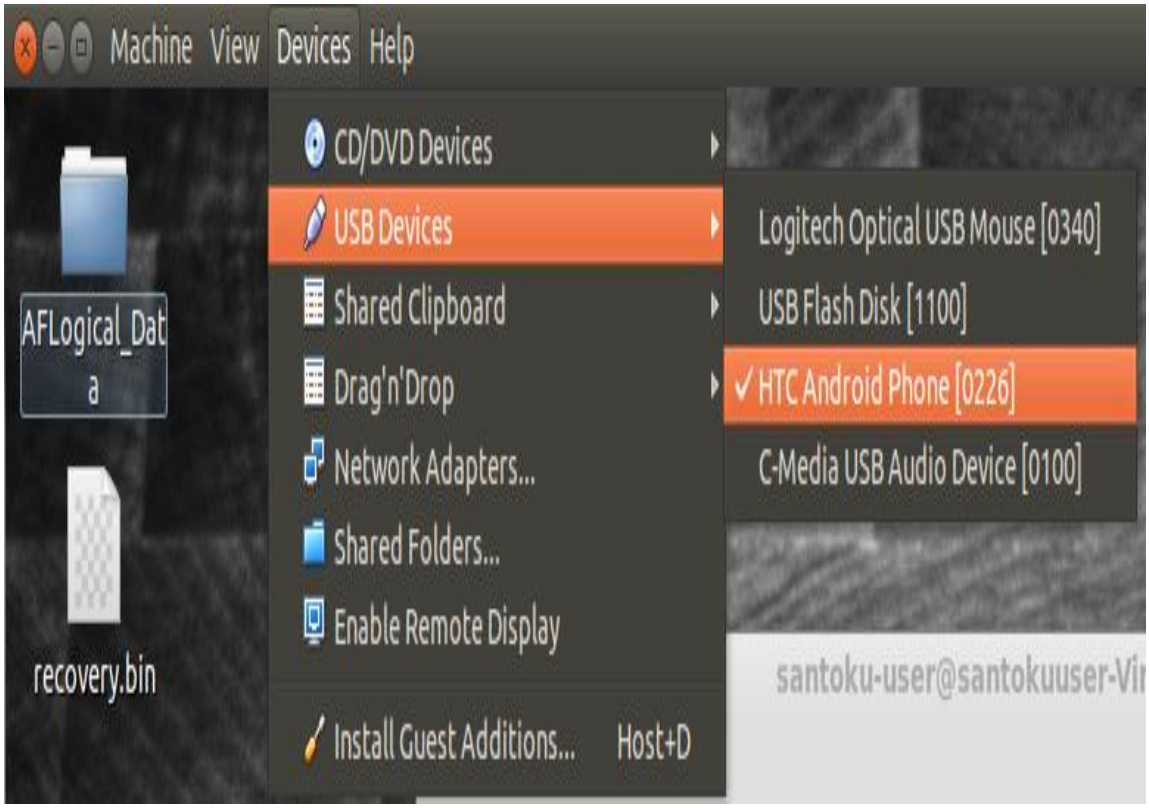

Figura 17-Reconhecendo o Dispositivo na máquina virtual

Após certificar que o aparelho está conectado ao *Santoku*, é necessário isolar o aparelho de qualquer forma de comunicação, para isso coloque o mesmo em "Modo Avião", em seguida vá em "Configurações, "Opções do desenvolvedor" e habilite as seguintes opções: "Depuração USB, permanecer ativo e permitir localizações

fictícias". Habilitando estes módulos do aparelho estará preparado para fazer a extração.

Figura 18-Habilitando o Dispositivo móvel

Seguindo estes passos para o dispositivo ficar sem comunicação vá para o terminal no diretório *Santoku* em seguida "*Devices Forensics*" e por fim AFLogical.

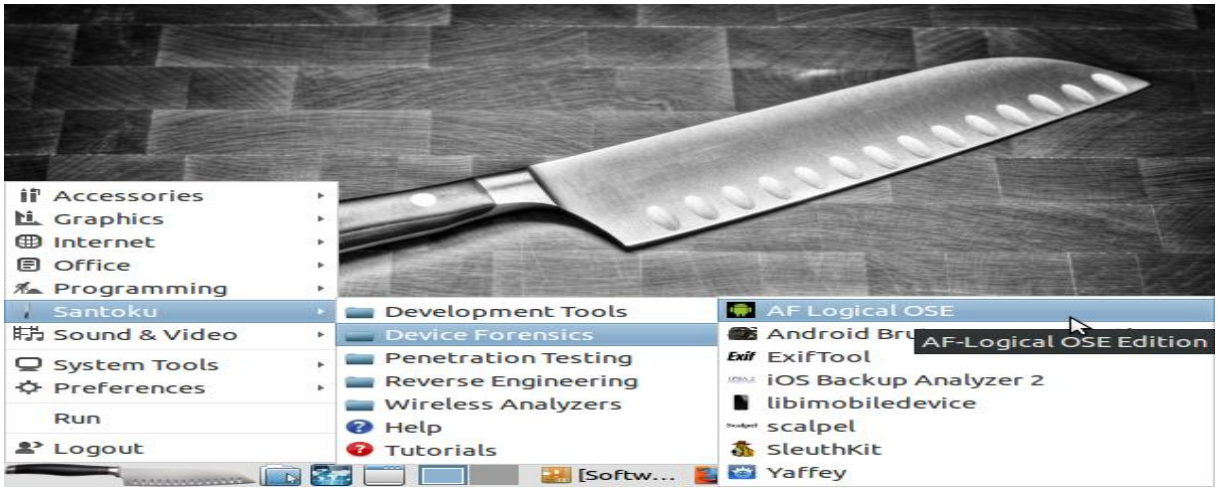

Figura 19-Preparando para a instalação do *AFLogical*

Nessa etapa verifique se a ferramenta forense pode se comunicar com o dispositivo Android. Para isso execute o seguinte comando no terminal:

$ ls -l

Neste momento aparecerá na tela uma lista de dispositivos anexadas da seguinte forma:

“-rw-r--r-- 1 santoku-user santoku-user 28794 Dec 19 2011 AFLogical-OSE_1.5.2.apk

-rw-r--r-- 1 santoku-user santoku-user 35819 Dec 19 2011 GPL

-rw-r--r-- 1 santoku-user santoku-user 1236 Dec 19 2011 README.txt”.

Neste momento insira o *AFLogical* para dentro do dispositivo utilizando o comando:

$ sudo adb devices

Agora será necessário inserir a senha criado no momento da instalação da ferramenta e aparecerá a mensagem como está descrita abaixo.

[sudo] password for santoku-user:

** daemon not running. starting it now on port 5037 **

** daemon started successfully **

List of devices attached

aDf1357867 device

Neste momento faça a instalação do *AFLogical.apk*, para isso ainda no terminal digite o seguinte:

$ adb install AFLogical-OSE_1.5.2.apk

Após o comando de instalação na tela aparecerá a seguinte mensagem:

296 KB/s (28794 bytes in 0.094s)

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

No dispositivo do emulador abrirá o aplicativo *AFLogical OSE,* escolha os dados que deseja extrair.

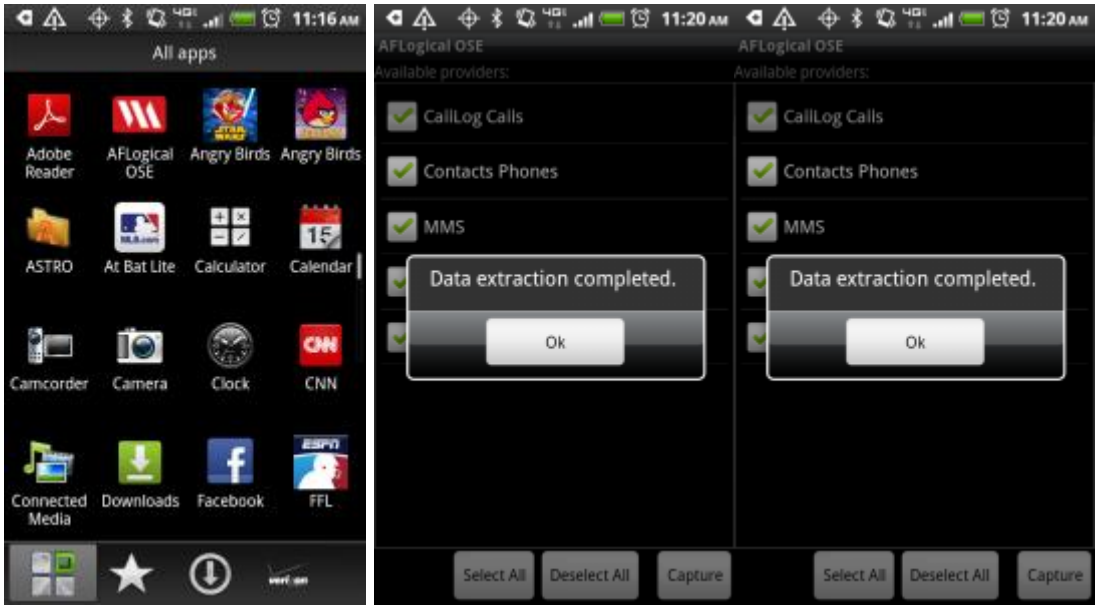

Figura 20-Extração de dados do aparelho celular

Nessa etapa puxe os dados do cartão SD na máquina *Santoku*, para isso digite os seguintes comandos:

$ mkdir ~/Desktop/AFLogical_Phone_Data

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

pull: building file list...

pull: /sdcard/forensics/20120720.1833/Contacts Phones.csv -> /home/santoku-user/Desktop/AFLogical_Phone_Data/20120720.1833/Contacts Phones.csv

Em seguida aparecerá a quantidade de arquivos retirados e de arquivos ignorados bem como está descrito abaixo.

40 files pulled. 0 files skipped.

410 KB/s (3880025 bytes in 9.229s)

Na janela do terminal *AFLocial-ose* no *Santoku* pressione "*Enter*" para puxar os dados para o local "~/aflogical-data", assim a ferramenta extrairá automaticamente todo os dados recuperados a partir do dispositivo para este local.

Para visualizar os dados no terminal é só digitar os seguintes comandos:

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

Os dados são armazenados em uma pasta marcada com hora e data da aquisição no diretório "~/aflogical-data", onde agora já terá acesso aos dados extraídos bem como contatos, registros de chamadas, MMS/SMS, e informações do dispositivo em formato CSV:

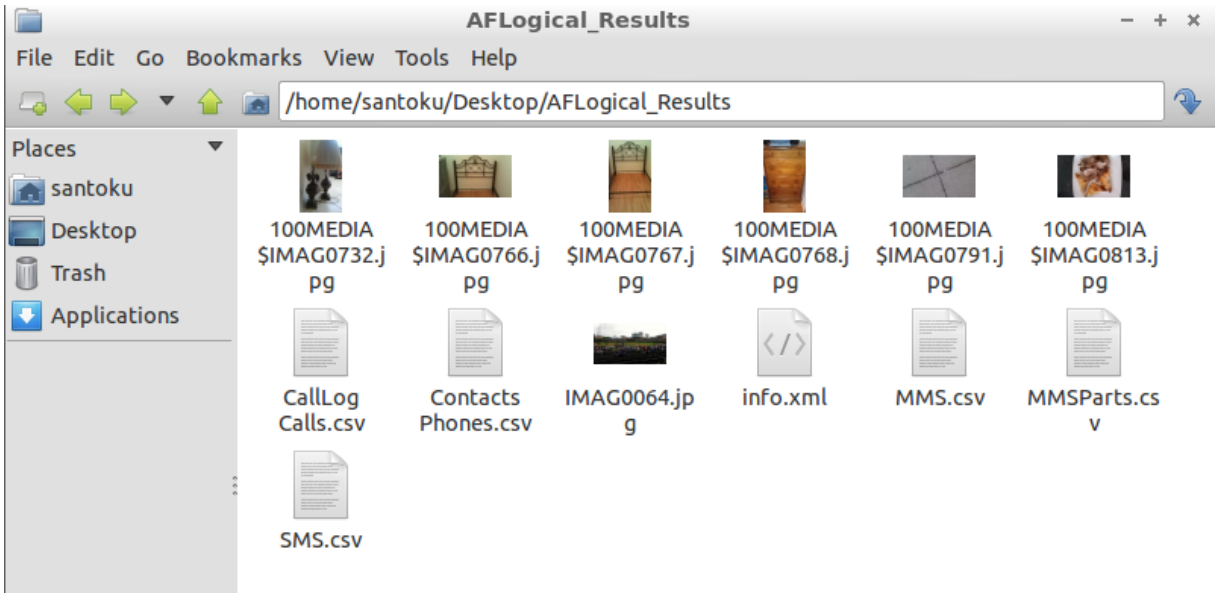

Figura 21- Resultados capturados do Dispositivo móvel

7 CONCLUSÃO

Vários são os métodos que um especialista na área forense pode utilizar para examinar e extrair dados de um dispositivo móvel. No entanto é claro a necessidade de conhecer a plataforma e suas características na qual está trabalhando antes de se iniciar uma investigação.

O presente trabalho propôs um estudo de caso detalhando um método para aquisição e exame de mensagens (SMS) de um dispositivo móvel com sistema operacional *Android*, listando as principais maneiras necessários para uma análise correta. Durante o desenvolvimento e execução deste estudo alguns obstáculos foram encontrados refletindo assim a dificuldade em executar técnicas com o menor impacto possível no dispositivo.

No enfoque forense retrata o contexto e abordagem de assuntos como, metodologias e possiblidades de aquisição de dados em *smartphones* com sistema operacional *Android* bem como o SDK e o ADB e também as permissões de super usuário, tornando assim possível direcionar o foco de pesquisa deste trabalho com a utilização da ferramenta *Santoku* Linux.

Ainda sim outras análises e conceitos são necessários para que se possa aplicar técnicas forenses em uma investigação. O estudo da Forense Computacional e a forma de aplicar suas metodologias voltadas exclusivamente para aparelhos celulares são essenciais e para isso as abordagens utilizadas internacionalmente aceitas e documentadas por algumas das principais entidades profissionais, entre elas a *National Institute of Standards and Technology* (NIST), a *Information Security and Forensics Society* (ISFS), o Departamento de Justiça dos Estados Unidos em conjunto com o Laboratório de Crimes Cibernéticos da *Computer Crime and Intellectual Property Section* (CCIPS) e a *Association of Cheif Police Officers* (ACPO).

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

Por fim, foram explorados técnicas e procedimentos para aquisição e exame de dados com a finalidade de abstração de mensagens (SMS) de *smartphones* com sistema operacional *Android* a partir de um contexto comum, no qual o aparelho, no momento da apreensão, encontra-se ligado, sem restrições de acesso e sem permissões de super usuário.

REFERÊNCIAS

ARTHUR, K. K. **An Investigation Into Computer Forensic Tools**. Disponível em: <http://www.infosecsa.co.za/proceedings2004/060.pdf,2004 > Acesso em 14/fev/2015.

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_forense-preparando_o_ambiente_de_trabalho/ > Acesso em16/fev/2015.

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: 23/fev/2015.

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: 16/fev/2015.

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: 13/fev/2015.

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, 11/mar/2010.

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. Disponivel em: < http://developer.android.com/tools/help/adb.html >. Acesso em: 01/maio/2015.

González, Elena Labajo. Ciências Antropológicas: **la Antropología Forense. Dez. 2004.** Disponível em: <http://www.p3blog.net/index.php?cat=21 > Acesso em: 08/fev/2015.

HOOG, A. **Android Forensics - Investigation, Analisys and Mobile Security for Google Android.** 1a. ed. [S.l.]: Syngress, 2011. ISBN: 978-1-59749-651-3.

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: 26/fev/2015.

KNIJFF, R. V. D. **Handbook of Computer Crime Investigation**, Chapter 11 Embedded System Analysis. Academic Press, 2001.

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.

LISITA, Bruno L; MOURA, Thiago S.M.; PINTO, Tiago J. **Forense computacional em memória principal**. Goiânia. 2009. 66 f. Dissertação (Pós Graduação em Segurança de Redes de Computadores) – Serviço Nacional de Aprendizagem Industrial, Goiânia, 2009.

LOPES, M.; GABRIEL, M. M.; BARETA, G. M. **Cadeia de Custódia: Uma Abordagem Preliminar**, 2006. Disponível em: < http://ojs.c3sl.ufpr.br/ojs2/index.php/academica/article/download/9022/6315 >. Acesso em: 15/fev/2015.

Luque, Bartolomé Serrano. **Ciência Forense - ¿cómo usar la ciencia y la tecnología para desvelar lo ocurrido?. Todo-Ciencia.com. 2002**. Disponível em:<http://matap.dmae.upm.es/WebpersonalBartolo/articulosdivulgacion/crimenes_3.htm > Acesso em: 07/fev/2015.

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/fev/2015.

MUKASEY, M. B., SEDGWICK, J. L. e HAGY, D. W. **Electronic Crime Scene Investigation. A Guide To First Responders, Second Edition**. U.S. Department of Justice.

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

OWEM, P.; THOMAS, P.; MCPHEE,D. **An Analyses of the Digital Forensic Examination of Mobile Phones.** 2010.

PALMER, G. and CORPORATION, M. **A Road Map for Digital Forensic Research**.Technical Report.

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-das-ciencias-forenses-e-as-diferencas-entre-a-computacao-forense-e-investigacao-digital/ > Acesso em 13/fev/2015.

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. Acesso em: 05/out/2012.

REIS, M. A.; GEUS, P. L. **Forense Computacional: Procedimentos e Padrões**. 2001.

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: 06/jan/2015.

REZENDE, A. C. F. **Sobre a Fé Pública**. Disponível em: < http://www.irib.org.br/biblio/Rezende.asp >. Acesso em: 07/jan/2015.

RUBACK, M. C. **Mineração de Dados Aplicada à Construção de Bases de *Hash* em Computação Forense**. 2011. Dissertação de Mestrado, Publicação PPGENE.DM - 84 A/11, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 169p.

Ruiz, Luís Orlando Aponte. **Criminalística - Aspectos históricos e evolução *no* Estado de São Paulo**. Disponível em: <http://www.revistademedicinalegal.com.br/default.aspx?edicao=&secao=16&subsecao=45&indice=1&indiceSubsecao=1 > Acesso em: 05/fev/2015.

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003.

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.

SHINDER, Debra Littlejohn. **Syngress Scene of Cybercrime**: Computer Forensics Handbook. Rockland: Syngress Publishing, Inc, 2002.

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

SPECKMANN, B. **The Android mobile platform.** [S.l.]: Eastern Michigan University, Department of Computer Science, 2008.

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/2015.

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, Maio de 2007.

VARGAS, Raffael Gomes. **Perícia Forense Computacional Metodologias e Ferramentas Periciais**. Revista Evidencia Digital ed. 03, 2004. Disponível em: < http://www.guiatecnico.com.br/EvidenciaDigital/ >. Acesso em: 11/fev/2015.

WEISER, M. "**Some Computer Science Issues in Ubiquitous Computing".** Communications of the ACM, v. 265, n. 3, 1993, p. 137 - 143.

Wilk, Daniel Alejandro. **Análisis de um Caso Real (Instrucción Sumarial o Investigación Penal Preparatoria)**. Disponível em: <http://www.puentes.gov.ar/educar/superior/biblioteca_digital/verdocbiblio1.jsp?url=S_BD_INTERCAMBIOS/R1ENTREWILK_OK.HTM > Acesso em: 07/fev/2015.

ZARZUELA, José Lopes. **Temas Fundamentais de criminalística.** Porto Alegre: Sagra Luzzatto,1996.

ZILLO NETO, Marcello. **Segurança da Informação e Tecnologia**: Disponível em: http://mzillo.blogspot.com/ Acesso em 07/fev/2015.