

**INSTITUTO ENSINAR BRASIL
FACULDADES DOCTUM DE CARATINGA**

CÍCERO DE SALES COSTA

CARATINGA

2018

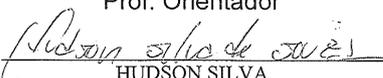
CÍCERO DE SALES COSTA
FACULDADES DOCTUM DE CARATINGA

**PERÍCIA FORENSE EM DISPOSITIVOS MÓVEIS, ESTUDO DE CASO:
SMARTPHONE MOTO G6 COM ANDROID 8.0**

Monografia apresentada ao Curso de
Ciência da Computação das Faculdades
Doctum de Caratinga, como requisito
parcial à obtenção do título de Bacharel
em Ciência da Computação.

Área de Concentração: Computação
Forense
Orientador (a): Msc. Fabrícia Pires Souza

CARATINGA
2018

	FACULDADES DOCTUM DE CARATINGA	FORMULÁRIO 9
	TRABALHO DE CONCLUSÃO DE CURSO	
TERMO DE APROVAÇÃO		
TERMO DE APROVAÇÃO		
<p>O Trabalho de Conclusão de Curso intitulado: PERÍCIA FORENSE EM DISPOSITIVOS MÓVEIS, ESTUDO DE CASO: SMARTPHONE MOTO G6 COM ANDROID 8.0, elaborado pelo(s) aluno(s) CÍCERO DE SALES COSTA foi aprovado por todos os membros da Banca Examinadora e aceito pelo curso de CIÊNCIA DA COMPUTAÇÃO das FACULDADES DOCTUM DE CARATINGA, como requisito parcial da obtenção do título de</p>		
<p>BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.</p>		
<p>Caratinga 18/12/2018</p>		
<p> FABRÍCIA PIRES Prof. Orientador</p>		
<p> HUDSON SILVA Prof. Avaliador 1</p>		
<p> ELIAS DE SOUZA GONÇALVES Prof. Examinador 2</p>		

DEDICATÓRIA

Dedico este trabalho aos meus pais Cecílio Costa Neto (in memoriam) e Maria Helena de Sales Costa, minha esposa Pâmella Aparecida Cler Costa e meu irmão Cássio de Sales Costa.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado forças para não desistir dos meus objetivos.

Aos meus pais Cecílio Costa Neto (in memoriam) e Maria Helena de Sales Costa por terem me dado total apoio para que eu pudesse fazer uma faculdade muitas vezes abrindo mão de comprar alguma coisa para eles para que pudessem me ajudar com os gastos da faculdade.

Ao meu irmão Cássio de Sales Costa por ter ficado ao meu lado no momento mais difícil das nossas vidas quando perdemos nosso pai, mesmo morando longe me incentivava a estudar e dava total apoio a nossa mãe.

Agradeço aos meus professores que por muitas vezes pensei que estavam exagerando na quantidade de conteúdo passado em sala de aula, mas hoje vejo que a cobrança é consequência de um aprendizado avançado.

Por último não menos importante a minha esposa Pamella Aparecida Cler Costa que me ajudou a retomar os estudos para conseguir o tão sonhado diploma.

RESUMO

A evolução e mobilidade alcançada pelos dispositivos móveis trouxe à tona um novo tipo de crime, baseado nessa mobilidade e conectividade. Os smartphones são capazes de armazenar grandes quantidades de informações de grande valor para investigação de crimes. Dessa forma, foi necessário adequar técnicas da ciência forense de forma a preservar as evidências de crimes digitais para que as mesmas possam ser utilizadas como prova judicial. Nesse trabalho foi abordado a evolução dos sistemas móveis, os desafios da computação forense, o campo de trabalho e as etapas necessárias para realizar uma perícia digital tal como coleta de dados, preservação das evidências e análise dos dados. Por fim, é apresentado um estudo de caso baseado na ferramenta Santoku Linux com as técnicas utilizadas na realização de uma correta perícia em um dispositivo com sistema operacional Android. Conclui-se com essa pesquisa que a ferramenta Santoku Linux é uma poderosa aliada do perito forense, se mostrando de fácil manuseio e adequada para o tipo de serviço. Que essa pesquisa sirva de base para outros estudantes para uma pesquisa mais profunda dessa ferramenta.

Palavras-Chaves: Santoku Linux. Mobile. Perícia forense.

ABSTRACT

The evolution and mobility achieved by mobile devices has brought to the forefront a new type of crime, based on such mobility and connectivity. Smartphones are capable of storing large amounts of valuable information for crime investigation. Thus, it was necessary to adapt techniques of forensic science in order to preserve evidence of digital crimes so that they can be used as evidence. In this work, the evolution of mobile systems, the challenges of forensic computation, the field of work and the steps necessary to perform a digital expertise such as data collection, evidence preservation and data analysis were discussed. Finally, a case study based on the Santoku Linux tool is presented with the techniques used to perform a correct skill on a device with an Android operating system. It concludes with this research that the Santoku Linux tool is a powerful ally of the forensic expert, if it is easy to handle and suitable for the type of service. That this research serve as a basis for other students for a deeper research of this tool.

Keywords: Santoku Linux. Mobile. Forensic expertise.

LISTA DE SIGLAS

ADB – Android Debug Bridge (Ponte de Depuração Android)

BR – Brasil

CD – Compact Disc (Disco Compacto)

CDMA – Code Division Multiple Access (Acesso múltiplo por divisão de código)

DVD – Digital Video Disc (Disco Digital de Vídeo)

ExFAT – Extended File Allocation Table (Tabela de Alocação de Arquivos Estendida)

FAT – File Allocation Table (Tabela de Alocação de Arquivos)

FBI – Federal Bureau of Investigation (Departamento Federal de Investigação)

FGV – Fundação Getúlio Vargas

GPS – Sistema de Posicionamento Global

IOS – Sistema Operacional móvel da Apple

MMS – Multimedia messaging Service (serviço de mensagens multimídia)

NTFS – New Technology File System (Novo Sistema de Tecnologia de Arquivos)

OSE – Open Source Edition (Edição de Código Aberto)

PT – Português

SDK – Software Development Kit (Pacote de desenvolvimento de software)

SIM – Módulo de identificação do assinante

SMS – Short Message Service (Serviço de Mensagens Curtas)

USB – Universal Serial Bus (Porta Universal)

VDI – Virtual Desktop Infrastructure (Infraestrutura de Desktop Virtual)

LISTA DE FIGURAS

Figura 1: Fraudes mais comuns no meio digital.....	14
Figura 2: Popularidade dos sistemas mobile a nível Brasil e Mundo.....	17
Figura 3: Arquitetura do sistema Android.....	19
Figura 4: Arquitetura do iOS.....	20
Figura 5: Ciclo de vida Perícia Forense Computacional.....	23
Figura 6: Etapa de aquisição de dados de um telefone celular com sistema operacional Android.....	25
Figura 7: Passos na investigação forense em dispositivos mobile.....	26
Figura 8: Tela inicial do Santoku Linux.....	31
Figura 9: Print da tela com as informações do dispositivo.....	34
Figura 10: Criando nova máquina virtual no Virtual Box.....	35
Figura 11: Alocando memória na máquina virtual.....	36
Figura 12: Criar Disco Rígido.....	37
Figura 13: Tipo de arquivo de Disco Rígido.....	37
Figura 14: Armazenamento em Disco Rígido Físico.....	38
Figura 15: Criar Disco Rígido Virtual.....	39
Figura 16: Atribuindo o Santoku a Máquina Virtual.....	40
Figura 17: Inserindo o Arquivo Santoku.....	40
Figura 18: Instalando o Santoku.....	41
Figura 19: Passos para atualizar o Android SDK Manager.....	42
Figura 20: Atualizando o Android SDK Manager.....	43
Figura 21: Permissão de Depuração USB.....	45
Figura 22: Com esse comando, você tem uma visão geral de todos os dispositivos conectados ao computador.....	46

Figura 23: Comando “adb backup”, extração lógica de dados do Android.....	47
Figura 24: Permissão de backup dos dados no dispositivo periciado.....	48
Figura 25: Backup gerado pelo comando “adb backup”	48
Figura 26: Extraíndo dados da pasta “data”, do dispositivo.....	49
Figura 27: Extração de arquivos via Santoku Linux.....	49
Figura 28: Caminho para a ferramenta AF LOGICAL OSE no Santoku Linux	50
Figura 29: Extração de dados via ferramenta AF LOGICAL OSE.....	51
Figura 30: Apresentação dos dados extraídos com a ferramenta AF LOGICAL OSE.....	51
Figura 31: Fotos encontradas dentro da pasta “data”.....	52
Figura 32: SMS entre suspeito de pedofilia e a vítima.....	53
Figura 33: Registro de ligações do dispositivo periciado.....	54
Figura 34: Contatos extraídos do dispositivo periciado.....	55

LISTA DE TABELAS

Tabela 1: Comparativo de vendas por sistema operacional.....	18
Tabela 2: Procedimentos para isolamento de dispositivos de conexões de rede	27

SUMÁRIO

INTRODUÇÃO	13
1 REFERÊNCIAL TEÓRICO	16
1.1 Sistemas Operacionais	16
1.1.1 Android	17
1.1.2 iOS.....	19
1.1.3 Outros Sistemas Operacionais	20
1.2 Computação forense	21
1.3 Evolução forense	22
1.4 Etapas da perícia	22
1.4.1 Apreensão Isolamento e Identificação	26
1.4.2 Aquisição da Evidência.....	29
1.4.3 Exame e Análise.....	29
1.5 Ferramentas Forenses	29
1.5.1 Encase.....	30
1.5.2 Kali Linux	30
1.5.3 Santoku Linux.....	31
1.5.4 Autopsy.....	32
2 METODOLOGIA	34
2.1 Configurando a máquina virtual	35
2.2 Instalação e configuração do Santoku	41
2.3 Preparação do dispositivo	43
2.4 Aquisição dos dados	44
2.4.1 Manual.....	44
2.4.2 Aquisição Lógica	44
3 RESULTADOS	52
3.1 Extração de dados por meio do adb	52
3.2 Extração de dados por meio do AF Logical OSE	53
4 CONCLUSÃO E TRABALHOS FUTUROS	56
5 REFERÊNCIAS BIBLIOGRÁFICAS	57

INTRODUÇÃO

O uso de *smartphones* em todo o mundo cresceu nos últimos anos, e com isso também cresceu o número de práticas ilícitas que podem ser cometidas com o uso dos aparelhos.

Segundo uma pesquisa realizada pela Fundação Getúlio Vargas (FGV), o Brasil já tem mais *smartphones* ativos que pessoas, sendo 220 milhões de celulares ativos no país contra 207,6 milhões de habitantes. A FGV também aponta que em torno de 70% dos aparelhos que são usados para conexão com a internet em nosso país são *smartphones* (FGV, 2017).

Pode-se apontar esse crescimento com o aumento dos recursos dos aparelhos, que funcionam para receber e fazer chamadas, enviar e receber mensagens, para utilização de diversos aplicativos de troca de mensagens como Whats App, Telegram ou Skype, uso de aplicativos de texto para edição de documentos, uso de redes sociais, entre várias outras funcionalidades como ouvir música, tirar fotos e GPS.

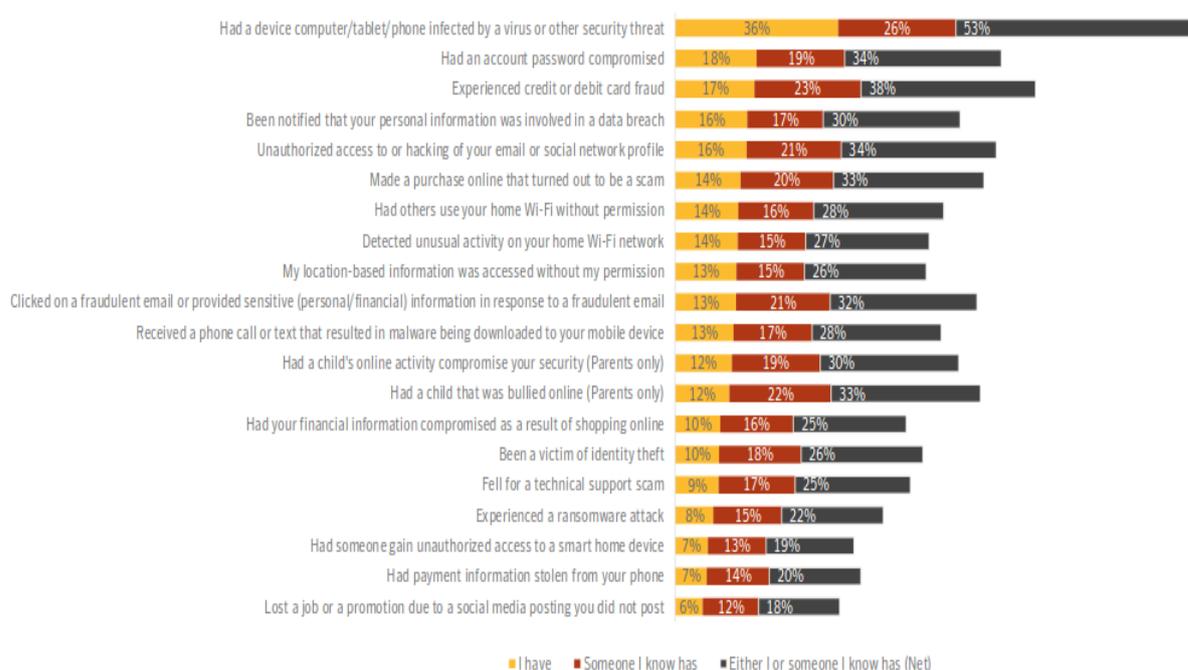
Mas todo esse crescimento também atrai pessoas mal-intencionadas que veem ali um meio para aplicar seus golpes, segundo um relatório da Norton Cyber Security. Em 2017 o Brasil se tornou o segundo país do mundo com maior número de casos de crimes cibernéticos, o que afeta 62 milhões de pessoas, ficando atrás somente da China (NORTON, 2017).

Outro ponto que a pesquisa da Norton (2017), aponta, é que 87% das pessoas tem internet via *wireless* em suas casas, e também há o grande acesso à internet em demais locais como cafés, bibliotecas, universidades, entre outros ambientes. Muitas dessas redes são desprotegidas o que acaba abrindo brechas para hackers.

A seguir apresenta-se uma lista dos principais crimes que vem sendo cometidos digitalmente, tendo como destaque algum dispositivo ser infectado por vírus, ter perdido o acesso a alguma conta devido a uso de senhas fracas, fraude em cartão de crédito, recebimento de e-mails fraudulentos (*phishing*).

De acordo com o gráfico apresentado na Figura 1, temos que 36% dos entrevistados já tiveram seus dispositivos infectados por vírus, 18% já tiveram suas senhas comprometidas e 17% já passaram por fraudes de cartão de créditos. Além do número de pessoas que já tiveram esses problemas, temos ainda que 53% afirmam ter conhecidos que tiveram seus dispositivos infectados por vírus, 34% de conhecidos que tiveram suas senhas comprometidas e 38% de conhecidos que já passaram por fraude de cartão de crédito. Esse número, entre vários outros apresentados, apenas demonstra a grande área de atuação e abrangência desses criminosos.

Figura 1: Fraudes mais comuns no meio digital



Fonte: Norton (2017)

Devido a esse crescimento de crimes digitais, foi necessário criar métodos de coleta e análise de evidências, para que pudessem ser consideradas e apresentadas no meio jurídico, dessa forma surge a Análise Forense em Dispositivos Móveis, que, segundo (JANSEN, 2008), é o uso dos valores e técnicas da ciência forense para providenciar evidências legais para investigações relacionadas.

A análise forense em dispositivos móveis é a ciência de recuperar evidências digitais de um celular (CURRAN, 2010), e é uma área recente e com um procedimento que exige muita atenção, pois por exemplo, caso a bateria do aparelho seja retirada pode-se perder dados de chamadas recebidas ou perdidas, ou pode-se alterar a hora do sistema, fazendo com que algumas evidências possam ser perdidas. Outro ponto que aumenta a dificuldade do trabalho é a diversidade de dados que podem ser analisados, como: fotos, áudio, *logs* de sistema, números, mensagens privadas, dados excluídos.

O presente trabalho apresenta um estudo de caso através da ferramenta Santoku Linux que serve para realizar perícias em dispositivos móveis. E quanto aos objetivos específicos, pode-se destacar:

- Apresentar a evolução dos dispositivos móveis;
- Apresentar as particularidades dos principais sistemas operacionais disponíveis no mercado;
- Apresentar as etapas de trabalho e coleta de evidências de um perito digital;
- Descobrir o desempenho da ferramenta Santoku mediante alguns casos de uso de uma perícia forense em um smartphone moto g6 com android 8.0.

Esse trabalho tem a seguinte estrutura: no capítulo 1 conta o embasamento teórico em que esse curso é baseado, tratando da evolução dos dispositivos móveis, dos principais sistemas operacionais disponíveis no mercado e das etapas em que uma perícia é baseada, de forma a preservar as evidências. No capítulo 2 é apresentado um estudo de caso baseado no Santoku Linux e explicações sobre o porquê da escolha do sistema para investigação, no capítulo 3 é apresentado a Análise de Resultados e por fim no capítulo 4 é apresentada a conclusão e trabalhos futuros.

1 REFERÊNCIAL TEÓRICO

1.1 Sistemas Operacionais

“É o conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos. O sistema que faz comunicação entre o hardware e os demais softwares. O Sistema Operacional cria uma plataforma comum a todos os programas utilizados. Exemplos: Dos, Unix, Linux, Mac OS, OS-2, Windows NT.”

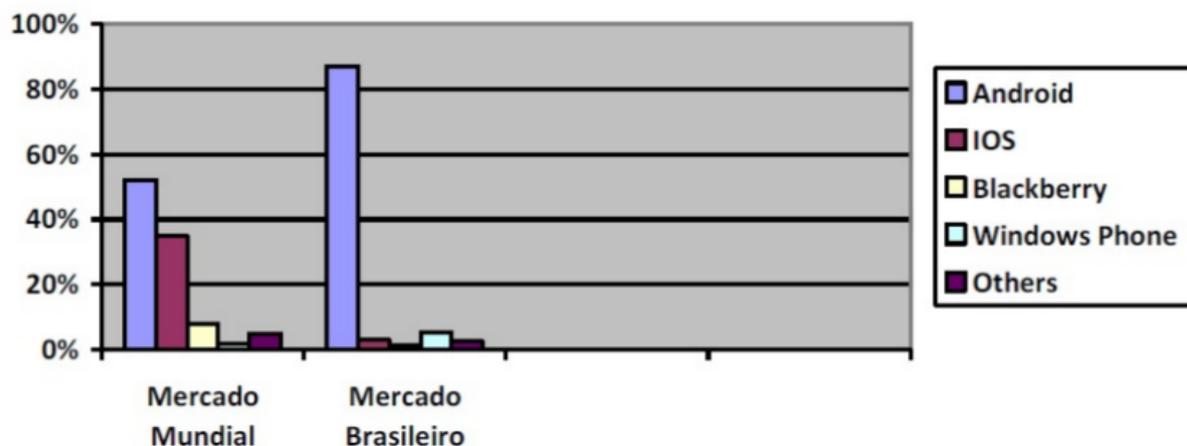
De acordo com (Stallings, 2004; Tanenbaum, 1999), possui dois modos diferentes de conceituar um sistema operacional:

Pela visão do programador é uma abstração do hardware, fazendo o papel de mediador entre o aplicativo (programa) e os elementos físicos do computador (hardware).

Em outra perspectiva, é um administrador de recursos, controla quais processos serão executados e quando, e quais recursos (memória e etc) serão utilizados nesse processo.

Um sistema operacional é responsável por gerenciar o *hardware* e *software* do aparelho, e hoje os principais sistemas operacionais móveis disponíveis no mercado são: Android, iOS e Windows Phone. A Figura 2 demonstra a popularidade desses sistemas a nível Brasil e Mundial em um estudo realizado por De Almeida et al (2014).

Figura 2: Popularidade dos sistemas mobile a nível Brasil e Mundo



Fonte: De Almeida et al. (2014)

Cada sistema operacional tem características próprias e determinado público-alvo, algumas dessas características serão discutidas a seguir.

1.1.1 Android

O Android é um sistema operacional baseado em Linux (Linux é um termo popularmente empregado para se referir a sistemas operativos ou sistemas operacionais que utilizam o Kernel Linux), tendo início em 2003 com a Android Inc., uma empresa de Palo Alto, Califórnia, USA, que em 2005 foi adquirida pela Google.

A principal característica do Android é que, por ter seu núcleo baseado em Linux, seu código fonte é aberto, o que abre a possibilidade para que demais desenvolvedores possam criar novas funcionalidades ou corrigir falhas na plataforma (LECHETA 2017). Isso abre diversas possibilidades para fabricantes de *smartphones* e contribui para a popularidade do sistema e viabilidade de custos com tecnologia.

Segundo o relatório do *International Data Corporation* (IDC) publicado em maio de 2017 e apresentado de forma mais detalhada na Tabela 1, o Android possui 85% do mercado de *smartphones* e vendeu um total de 344,3 milhões de

smartphones em todo o mundo no primeiro trimestre de 2017. Em segundo lugar, aparece o iOS com 14.7%, que é o sistema operacional da Apple.

Tabela 1: Comparativo de vendas por sistema operacional

Period	Android	iOS	Windows Phone	Others
2016Q1	83.4%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%
2016Q3	86.8%	12.5%	0.3%	0.4%
2016Q4	81.4%	18.2%	0.2%	0.2%
2017Q1	85.0%	14.7%	0.1%	0.1%

Fonte: IDC (2017)

Por meio da tabela pode - se observar como aumentou as vendas do Android, saindo de 83,4% e indo para 85%, enquanto as vendas do iOS caíram de 15,4% para 14,7% e do Windows Phone caíram 0,7% nesse mesmo período. Esses dados demonstram o crescimento de vendas do Android frente a seus concorrentes.

Na Figura 3 é apresentado a arquitetura do sistema Android. A última camada é a mais abstrata, onde os desenvolvedores dos aplicativos irão atuar, inclusive quando for necessário criar ligações com o hardware. Na 2 camada temos o *Framework*, que será utilizado quando o desenvolvedor precisar acessar serviços do *kernel* do Android, tal como notificações, chamadas telefônicas, câmera, entre outros. Na terceira camada temos a ligação do hardware com os serviços do sistema tal como funções e mídia. Na quarta e última camada temos o acesso ao *kernel* do Linux, responsável pelo gerenciamento de todo o sistema, tal como memória, aplicativos, armazenamento, entre outros.

Figura 3: Arquitetura do sistema Android



Fonte: Android (2005)

1.1.2 iOS

O iOS é um sistema desenvolvido para o iPhone, lançado em 29 de junho de 2007, e como o sistema ainda não tinha um nome, no seu lançamento foi rotulado de iPhone Operating System (iOS), segundo (GARCIA 2013).

O sistema foi baseado no Mac OS X, e passou a ser o principal sistema da empresa, sendo utilizado nos iPods, iPads e até mesmo na Apple TV (MILANI 2012).

A arquitetura do sistema também é composta por 4 camadas, e apresentada na Figura 4. A primeira camada, conhecida como *Cocoa Touch* é a camada de mais

alto nível, responsável pela interação do usuário com o aparelho, essa também é a camada onde os desenvolvedores atuam. A segunda camada trabalha com as mídias em geral, tal como áudio, vídeo e tecnologias utilizadas em jogos. A terceira camada é onde dá-se o acesso aos serviços, tal como o acesso ao banco de dados e a manipulação de arquivos. Por fim, a última camada responsável pelo núcleo do sistema, fazendo todo o gerenciamento de tarefas, energia, segurança.

Figura 4: Arquitetura do iOS



Fonte: Apple (2015)

1.1.3 Outros Sistemas Operacionais

Além dos dois mais populares sistemas citados, temos alguns outros, citados abaixo:

- Windows Phone: Segundo Nunes (2014), entre os principais sistemas, esse foi o último a ser lançado, em 21 de outubro de 2010, tendo uma padronização de *hardware* por parte dos fabricantes e uma área específica para interação do usuário.
- BlackBerry: Uma linha de celulares criados pela Research in Motion com foco no mercado corporativo, tendo funções que permitissem que se produzisse conteúdo em qualquer local. Foi descontinuado em 2016.

- Ubuntu Touch: Sistema operacional desenvolvido pela Canonical, baseado no kernel do Ubuntu e adaptado para celulares. O projeto também foi descontinuado.

Desse modo pode – se concluir que o sistema operacional mais utilizado em dispositivos móveis no mundo é o Android, o que consequente o faz ser o sistema com o maior número de ataques sofridos entre outros.

1.2 Computação forense

De acordo com Lopes (2002), “a Perícia Forense Computacional é definida como ciência multidisciplinar, ela por sua vez aplica técnicas investigativas para determinar e analisar evidências, diferentemente dos outros tipos de perícias forense conhecidos, a análise forense computacional produz resultados diretos e não interpretativos conforme os outros modelos, sendo por sua vez decisivos em um caso”.

Segundo o Colégio Notarial do Brasil (CNB) em 2014, de acordo com os registros, somente no estado de São Paulo, o total de atos criminosos no Brasil chegou a 18.820 em 2012 a 32.011 em 2013, com um aumento muito preocupante de 70%, já que a cada dia mais, brasileiros utilizam desses meios para trabalho.

De acordo com Eleutério; Machado (2011), o artigo 159 do Código de Processo Penal Brasileiro, estabelece que “O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior”. Significando que o processo de Análise Forense Computacional somente poderá ser realizado por profissional devidamente qualificado e habilitado, “destinada a determinar a dinâmica, a 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 crimes, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo”

1.3 Evolução forense

De acordo com Ruiz (2005), “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”.

Segundo Luque (2002), “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”.

O ramo da pesquisa sobre investigação digital apareceu na década de 80, em 1984 foi criado um programa dentro do FBI. Segundo Cummings (2010), era conhecido somente como conjunto de análise de estudos sobre mídias. Alguns anos depois a criação do programa, o agente especial Michael Anderson, o qual é chamado de o “Pai da Forense Computacional”.

Posteriormente Michael Anderson 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).

1.4 Etapas da perícia

Segundo Reis e Geus (2004) a computação forense tem como objetivo realizar uma investigação com a maior transparência possível, para que possa com excelência provar os fatos ocorridos, sem comprometer os resultados obtidos.

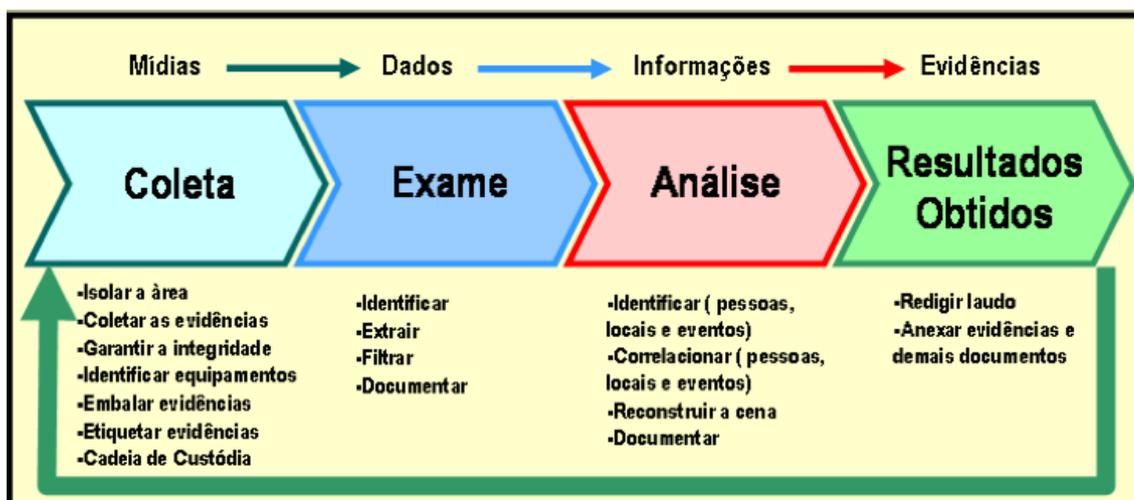
“Na fase de planejamento, tem que se definir a melhor abordagem para a investigação, identificando as principais atividades que precisarão ser executadas, de acordo com as informações obtidas preliminarmente, de modo a aproveitar melhor a coleta de dados. Dar início a criação de uma cadeia de custódia, ou seja, um histórico dos passos tomados na investigação, reunindo informações sobre os procedimentos,

pessoas envolvidas e evidências recolhidas”. (REIS e GEUS, 2004, p.54)

Já para Farmer (2007, p.5) a verificação pericial de um sistema compõe - se de um ciclo de coleta (mídias), Exame (dados), Análise (informações) e Resultados Obtidos (evidências). Quanto maior a precisão e riqueza dos dados, melhor será a perícia.

Na figura 5 são apresentadas as etapas para realização de uma perícia forense em dispositivos, mesmo que cada caso seja diferente, é importante que a sequência de passos seja mantida de forma a preservar as evidências e que os resultados possam ser utilizados em meio jurídico.

Figura 5: Ciclo de vida da Perícia Forense Computacional



Fonte: Pereira et al.(2007)

De acordo com Eleutério e Machado (2001) na fase de coleta dos dados, a finalidade é identificar, separar, etiquetar, armazenar, colher as evidências físicas relacionadas à investigação, e manter a integridade das provas coletadas.

“O ato de extrair, localizar e filtrar somente as informações que possam contribuir, de forma positiva, em uma investigação ocorre na segunda etapa, denominada “exame de evidências”. Considera-se esta, a etapa mais trabalhosa do processo de investigação criminal, principalmente pela quantidade de diferentes tipos de arquivos existentes (áudio, vídeo, imagem, arquivos criptografados, compactados, etc.) que facilitam o uso de esteganografia, o que exige que o perito esteja ainda mais

atento e apto a identificar e recuperar esses dados” (FARMER, VENEMA, 2007, p.41)

De acordo com Almeida (2011) a etapa de análise baseia-se em examinar as informações coletadas na etapa anterior de extração verificando evidências digitais, analisando com relação ao fato apurado. De posse dessas informações é possível seguir com o inquérito, podendo responder as perguntas relevantes ao caso. Sendo assim, é de grande importância que as autoridades saibam exatamente o que procura, para que possa evitar desperdício de trabalho e tempo dos peritos.

Afirma ainda Eleutério; Machado (2011), mesmo um disco rígido nos padrões micros que se utilizam atualmente, contem milhões de arquivos, sendo assim, consumiria muito tempo e trabalho, se não tiver um objetivo ou saiba o que procura, acaba tornando o exame inviável.

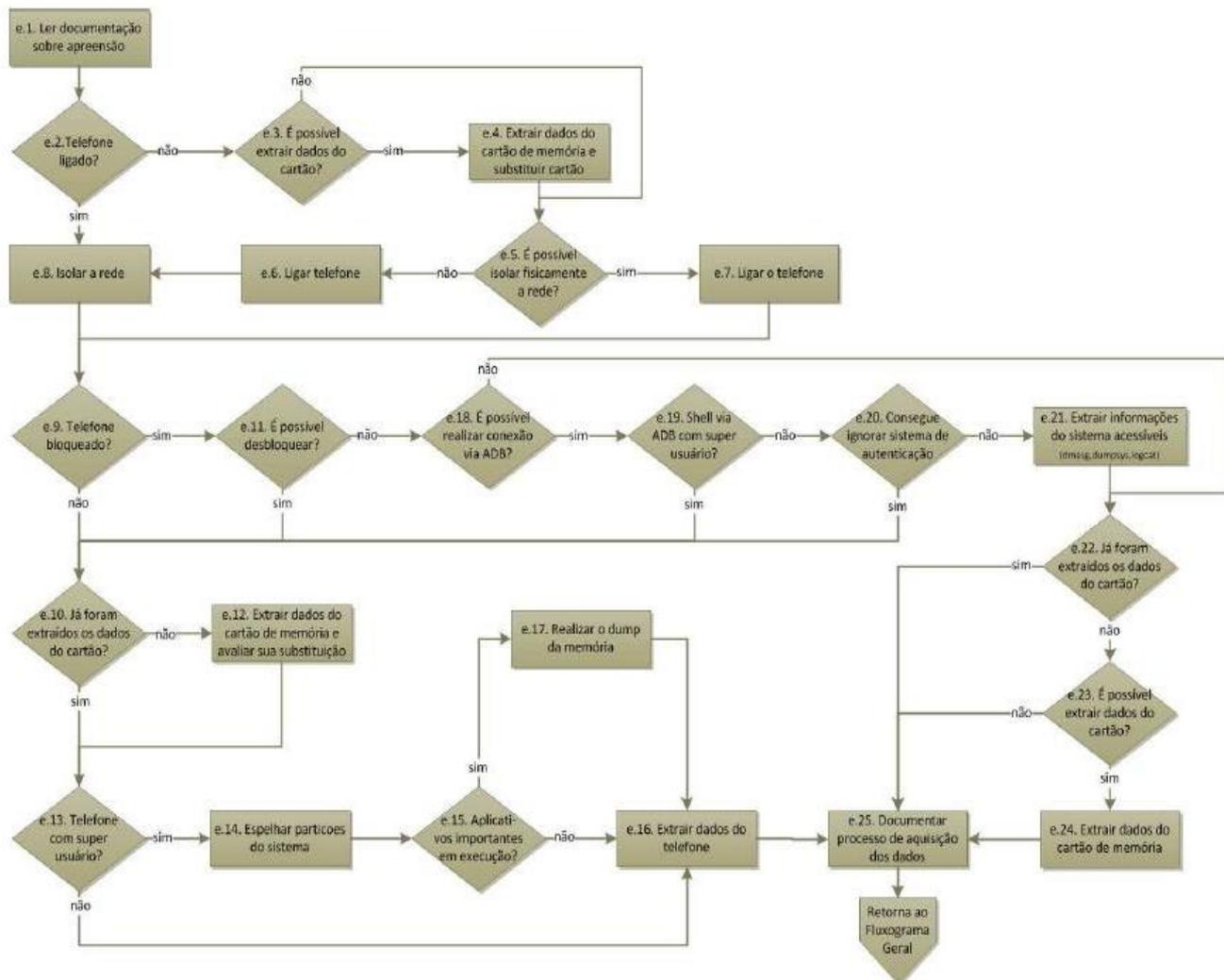
“O examinador só deve criar o relatório quando esgotarem todas as possibilidades de interpretação dos dados extraídos do dispositivo móvel e já tiver conclusões pertinente sobre elas” (SIMÃO, 2011).

Afirma ainda Carroll; Brannon; SONG (2008), “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”.

Porém, a área mobile tem algumas características que exigem atenção do perito, pois de acordo com (Joseph e Sing, 2017), a facilidade dos dados armazenados em um telefone serem comprometidos ou perdidos é enorme, por exemplo ao retirar a bateria do aparelho, diversos dados de chamada ou mensagens podem ser perdidos, bem como o horário registrado no aparelho, comprometendo as evidências.

Outro ponto de destaque é que o aparelho deve ser isolado de sinal de redes de telecomunicações ou wi-fi, pois existem diversos programas que podem, remotamente, apagar os dados do aparelho, dessa forma podemos agrupar os 4 passos anteriores nos 3 passos apresentados na Figura 7, e também podemos apresentar como um passo a passo de procedimento a tomar a Figura 6.

Figura 6: Etapa de aquisição de dados de um telefone celular com sistema operacional Android



Fonte: Simão (2011)

A imagem acima descreve sucintamente cada etapa a ser executada para a coleta de dados de um aparelho móvel, podendo assim, ter um passo a passo, ou seja, uma noção bem explicativa.

Figura 7: Passos na investigação forense em dispositivos mobile



Fonte: Joseph e Sing (2017).

Tradução do esquema a cima:

Apreensão		Exame
Isolamento	----->	Aquisição de Evidencia ---->
Identificação		Reportar

Vamos observar as seguintes etapas a seguir.

1.4.1 Apreensão/ Isolamento e Identificação

Nessa etapa é preciso garantir que as informações não sejam perdidas nem adulteradas, para isso temos que executar alguns passos, tais como os descritos a seguir:

- Coletar e catalogar todos os cabos e cartões;
- O aparelho deve ser mantido no estado em que se encontra, por exemplo, se estiver ligado, deve ser mantido dessa forma e com a bateria carregada;
- O aparelho deve ser protegido de influências externas, tal como: receber ligações, GPS e wi-fi. Para isso pode-se utilizar o modo avião.

Na Tabela 2 é apresentado o procedimento para isolar o aparelho com sistema operacional Android de conexões de rede, de acordo com a versão de sistema operacional.

Tabela 2: Procedimentos para isolamento de dispositivos de conexões de rede

Versão do Android	Técnica	Vantagem	Desvantagem
3.0 ou inferior	Colocar o dispositivo em Modo Avião (Airplane mode).	Requer acesso completo ao dispositivo. Os processos do dispositivo continuam a rodar e dados temporais permanecem intactos.	Modificação de configuração do dispositivo.
3.0 ou superior	Colocar o dispositivo em Modo Avião (Airplane mode). Não requer acesso especial	Não requer acesso aos menus internos do sistema operacional. Os processos do dispositivo continuam a rodar e dados temporais permanecem intactos. Desabilita conexões Wi – fi	Modificação de configuração do dispositivo.
Qualquer versão	Remoção do cartão SIM em caso de dispositivos GSM	Fácil de remover, efetivo em desabilitar as conexões de voz, SMS e transmissão de dados.	Não desabilita conexões Wi - fi, Bluetooth e outros tipos de conexões. Pode não funcionar em dispositivos que não sejam GSM, incluindo dispositivos CDMA e IDEN

Qualquer versão	Suspender a conta de celular na operadora	Efetivo em desabilitar toda transmissão de voz, SMS e transmissões de dados de qualquer telefone	O processo demanda tempo e depende de uma ordem judicial para ser executada pela operadora. Não desabilita conexões Wi-fi e bluetooth
Qualquer versão	Inserir o dispositivo em um invólucro de isolamento, como uma sacola ou caixa.	Previne vários tipos de transmissão de redes	Ao impedir que os sinais de transmissão cheguem ao dispositivo, o mesmo continuará a procurar redes disponíveis, o que consome consideravelmente a bateria do dispositivo.
Qualquer versão	Desligar o dispositivo	Totalmente efetivo em prevenir toda forma de comunicação em rede	O estado do dispositivo é alterado e dados temporais (voláteis) são perdidos. Possibilidade de travamento do dispositivo através de mecanismo de criptografia e/ou bloqueio de tela

Fonte: Hogg,(2012)

1.4.2 Aquisição da Evidência

Para a extração de dados do SIM card é necessário um hardware específico, já os dados armazenados no cartão de memória podem ser extraídos de acordo com um dos 5 tipos de aquisição abaixo:

- Manual: Os dados são extraídos de forma manual diretamente do dispositivo;
- Lógica: Dessa forma a cópia é feita bit a bit, e uma cópia fiel é feita dos dados;
- Força – bruta: Essa forma é necessária quando o dispositivo está bloqueado com senha. Para o caso dos dispositivos Android pode-se utilizar a ferramenta ADB, disponível no SdK do Android, para os dispositivos iOS utiliza-se a ferramenta libimbledevice, essa ferramenta pode ser baixada e integrada com o Santoku Linux, por exemplo.
- Metadados: são arquivos copiados diretamente do banco de dados e logs do sistema.
- Física: Dessa forma são adquiridos os binários do sistema, que contém as informações dos objetos deletados.

1.4.3 Exame e Análise

Após a coleta dos dados, pode-se realizar o exame em alguns dos seguintes itens: chamadas, SMS, calendário, e-mail, aplicativos de mensagens, downloads, documentos, imagens, vídeos, áudios, localizações registradas, redes salvas, entre outros.

Após o exame e análise, deve-se escrever o laudo pericial, que deve conter, de forma imparcial, as evidências digitais encontradas. Também é aconselhável manter as cópias realizadas para perícia.

1.5 Ferramentas Forenses

Existem inúmeras ferramentas forenses disponíveis no mercado. Nesse trabalho são apresentadas 4 dessas ferramentas forenses, são elas: Encase, Kali Linux, Santoku Linux e Autopsy. A seguir é descrito brevemente as características de cada uma de forma a justificar a escolha do Santoku Linux como instrumento de análise.

1.5.1 Encase

O Encase é um produto da Guidance Software, ele tem vários produtos projetados para o uso forense, segurança cibernética, análise de segurança e descoberta eletrônica.

Vargas (2007) salienta que a ferramenta EnCase é uma das mais completas quando o assunto trata-se de perícia forense computacional, o autor justifica sua afirmativa baseado nos seguintes pontos:

- Padronização de laudos periciais;
- Organização do banco de dados ligado às evidências;
- Fornece senhas ou às quebras;
- Recuperação de arquivos excluídos.
- Analisa hardwares;
- Analisa e-mails;

O EnCase Forensic possibilita também, através de utilitários internos, identificar arquivos criptografados e protegidos com senha, localizar conversas em mecanismos de bate-papo, localizar logs e proporcionar ao usuário a análise de forma abrangente dos arquivos contidos na lixeira e arquivos de link (VARGAS, 2011).

Com ele também é possível adquirir dados diretamente dos principais *smartphones* e tablets. Ele também tem diversos templates já prontos de relatórios. É uma ferramenta poderosa, porém com custo elevado.

1.5.2 Kali Linux

O Kali Linux conforme cita Pritchett; Smet (2013) é uma distribuição do Linux baseada no Debian e cuja finalidade é oferecer ferramentas para a utilização na auditoria e em testes de invasão, coleta de informações, identificação de vulnerabilidade, exploração, escalação de privilégios.

O Kali Linux possui vários softwares pré-instalados como:

- NMAP: escaneador de portas em uma rede.
- Wireshark: é um programa que analisa o tráfego de rede.
- John the Ripper: software de quebra de senhas.
- Aircrack: software para testes de segurança em redes sem fios.

O sistema pode ser instalado como sistema operacional e também pode ser utilizado a partir de um Live CD ou live-usb.

Embora seja uma ferramenta muito conhecida, seu foco não é forense, e sim auditorias e segurança de computadores em geral, onde é possível analisar portas de rede e fazer diversos testes quanto a invasão.

1.5.3 Santoku Linux

O Santoku Linux é uma ferramenta especializada na análise forense de dispositivos móveis, podendo fazer a análise de *malwares*, engenharia reversa e testes de segurança. Sua tela inicial é apresentada na Figura 8.

Figura 8: Tela inicial do Santoku Linux.



Fonte: Próprio autor

Para Neves (2012) a distribuição possui alguns recursos tais como: emuladores de dispositivos móveis, utilitários para simular serviços de rede para análise dinâmica, scripts para detectar problemas comuns em aplicações móveis, descriptografar binários, entre outros.

A ferramenta também conta com emuladores para as seguintes plataformas, como: BlackBerry JDE, Apple Xcode IDE, BlackBerry Tablet OS SDK, BlackBerry WebWorks, DroidBox, Eclipse IDE, e Windows Phone SDK.

Para análise de *malwares* mobile, ele possui uma base de dados contendo informações dos principais tipos de *malwares* existentes.

Também é gratuita e pode rodar como um *live-cd*, não sendo necessário realizar sua instalação.

Dessa forma, o Santoku Linux torna-se a melhor opção para análise de dispositivos mobile, devido a quantidade de ferramentas já incluídas na distribuição e pelo mesmo ser gratuito. Uma análise mais aprofundada em diversas de suas ferramentas será feita no próximo capítulo, e abaixo detalharemos alguns processos referentes ao Android.

Para o Android, o sistema já apresenta o SDK e o emulador, com isso é possível trabalhar com um aparelho real ou então utilizar o emulador para simular diversas configurações de aparelhos, desde tamanho do cartão de memória, até processadores, câmeras, entre outros.

O Android trabalha com o ADB (Android Debug Bridge) que consiste em um cliente-servidor utilizado para conectar-se a um dispositivo (real ou emulado) Android através do modo de depuração USB. Abaixo apresentamos a lista de comandos disponíveis.

Segundo M.Droid (2017) comandos úteis para utilização em android:

- adb devices: mostra uma lista dos dispositivos conectados ao computador que estejam com o modo de depuração USB ativado.
- adb logcat: mostra os dispositivos conectados ao ADB.
- adb shell: cria uma conexão com o dispositivo, permitindo a interação dos comandos com o sistema.
- adb shell chmod: muda a permissão dos arquivos.
- adb reboot: reinicia o sistema.
- adb install: instala um aplicativo direto da pasta do adb.
- adb pull e adb push: faz a cópia de arquivos e pastas do computador para o aparelho e vice-versa.

Quanto aos aplicativos que são instalados, cada um deles recebe um novo ID de usuário no momento da instalação, esse ID relaciona todos os dados armazenados referentes a esse aplicativo, sejam pastas, arquivos, base de dados ou quaisquer outros recursos. Outro ponto é que somente a aplicação criadora pode acessar esses dados. Quando o aplicativo é instalado, ele também solicita a confirmação de diversas permissões, que após a instalação não podem ser alteradas.

1.5.4 Autopsy

De acordo com Sleuthkit (2018) Autopsy é uma ferramenta forense digital gratuita utilizada por policiais e peritos forenses. É uma aplicação gráfica que faz uso de um conjunto de ferramentas em linha de comando. Segundo o site do fabricante do Autopsy ele possui os seguintes recursos:

- Web Artifacts: Mostra atividades recentes de usuários em navegadores.
- Registry Analysis: Mostra documentos recentes usado pelo dispositivo USB.
- Link File Analysis: Identifica atalhos e documentos acessados.
- Email Analysis: Analisa mensagens no formato MBOX, como Thunderbird.
- EXIF: Extrai geo localização de imagens.

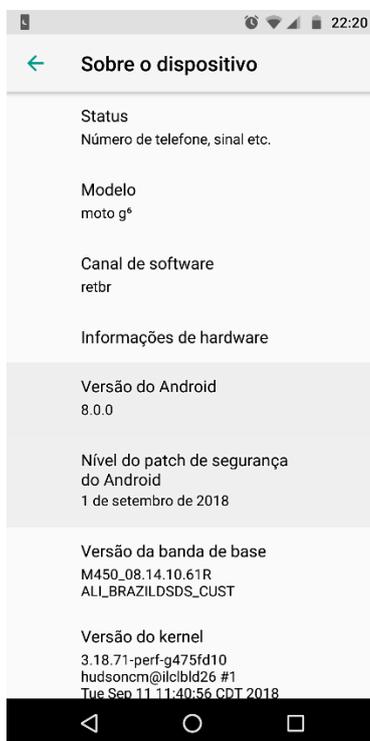
- File Type Sorting: Pesquisar documentos e imagens a partir do seu nome ou grupo.
- Media Playback: Veja os vídeos e imagens acessadas do play padrão do Windows.
- Thumbnail viewer: Exibe miniaturas de imagens para ajudar nos relatórios.
- Robust File System Analysis: Suporte para os sistemas de arquivos comuns, incluindo NTFS, FAT12, FAT16, FAT32, HFS +, ISO9660 (CD-ROM), ext2, ext3, e UFS a partir do kit Sleuth.

O software Autopsy é utilizado principalmente pelos peritos para realizar a análise de imagens de disco, unidades locais ou uma pasta de arquivos locais.

2 METODOLOGIA

Nesse capítulo são apresentadas algumas das técnicas e métodos utilizados na realização de uma perícia em um smartphone com sistema operacional Android de forma a discutir os resultados no próximo capítulo. Os testes foram executados em um aparelho MOTO G6, da Motorola com sistema operacional Android versão 8.0. Sem restrição de acesso e sem permissões de usuário root. Conforme mostrado na figura 9 a seguir.

Figura 9: Print da tela com as informações do dispositivo



Fonte: Próprio autor

Neste estudo de caso simula uma situação a qual um smartphone de uma determinada pessoa é apreendido e necessita ter seus dados extraídos para uma análise. Será descrito como se dá a extração de imagens, vídeos, SMS, MMS, e demais dados lógicos.

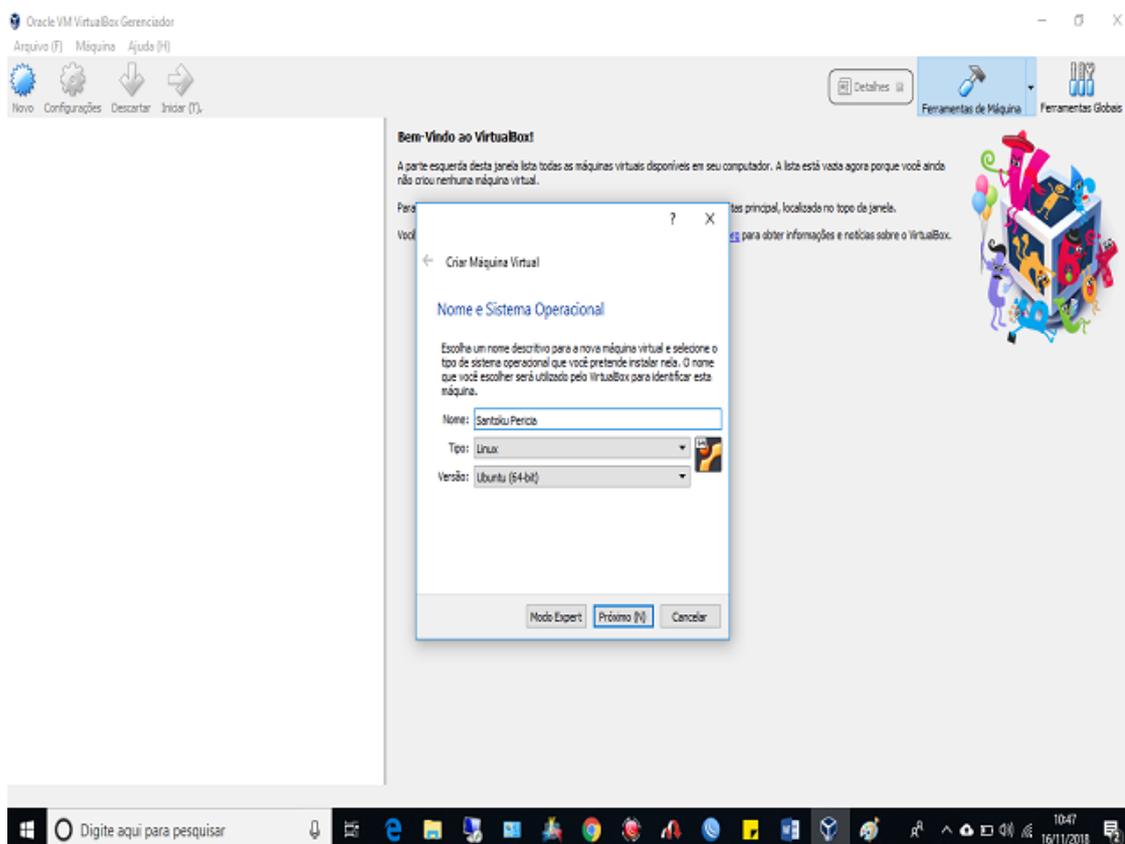
2.1 Configurando a máquina virtual

Para a realização desse trabalho foi necessário realizar a configuração da ferramenta Santoku Linux em uma máquina virtual utilizando o virtual box. É apresentado o passo a passo de como essa configuração deve ser feita.

Primeiramente deve-se fazer o download do arquivo de instalação do sistema Santoku disponível (<https://santoku-linux.com/download/>) e também do arquivo de instalação mais recente do Virtual Box 5.2.22 disponível em (<https://www.virtualbox.org/wiki/Downloads>). Após o download, deve-se instalar o virtual box em seu computador.

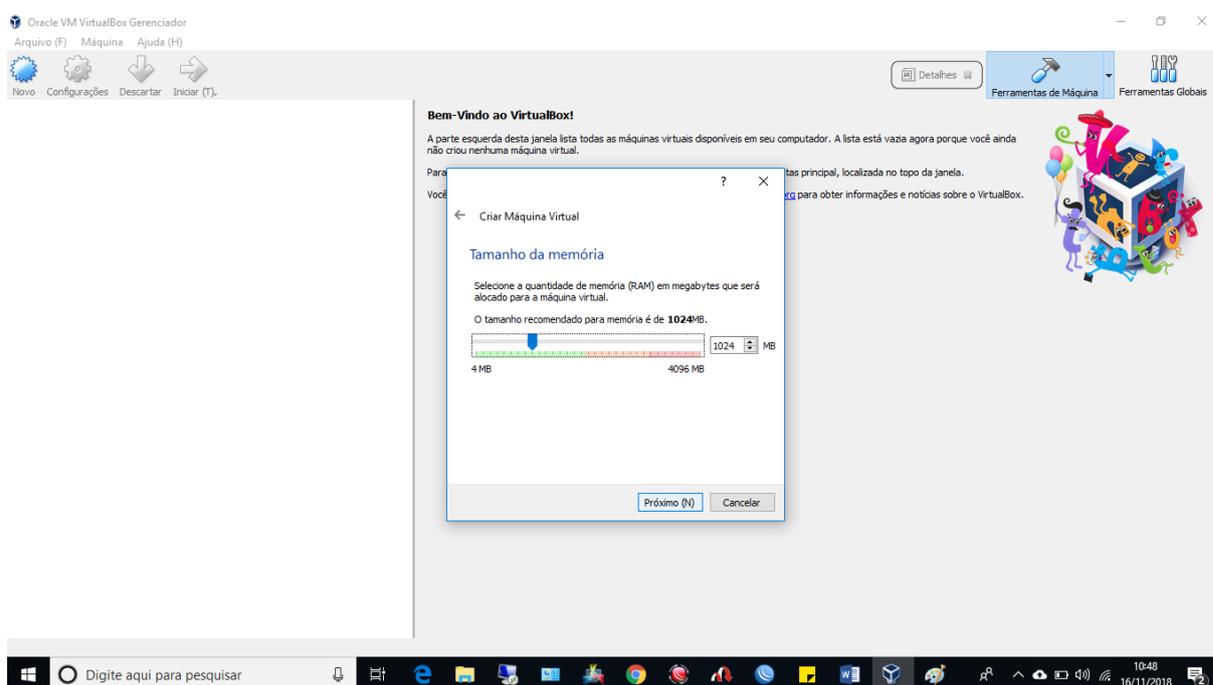
Em seguida execute o Virtual Box, deve-se clicar em “Novo”, criar um nome para a máquina virtual em seguida em tipo selecione o Linux e versão Ubuntu 64 bits. É preciso definir o tipo de versão do sistema para 64 bits pois o arquivo de instalação.

Figura 10: Criando nova máquina virtual no Virtual Box



Nesta próxima etapa aparecerá na tela a caixa de memória, na qual se deve selecionar uma quantidade adequada, pois o tamanho para a máquina virtual 512 MB é o recomendado, no entanto foi aumentada a dimensão da memória para 1024 MB para deixar a máquina virtual mais rápida. Para utilizar o Android Virtual Device (AVD), recomenda-se selecionar ao menos 4 GB de memória, em seguida avance clicando em “Próximo”.

Figura 11: Alocando memória na máquina virtual

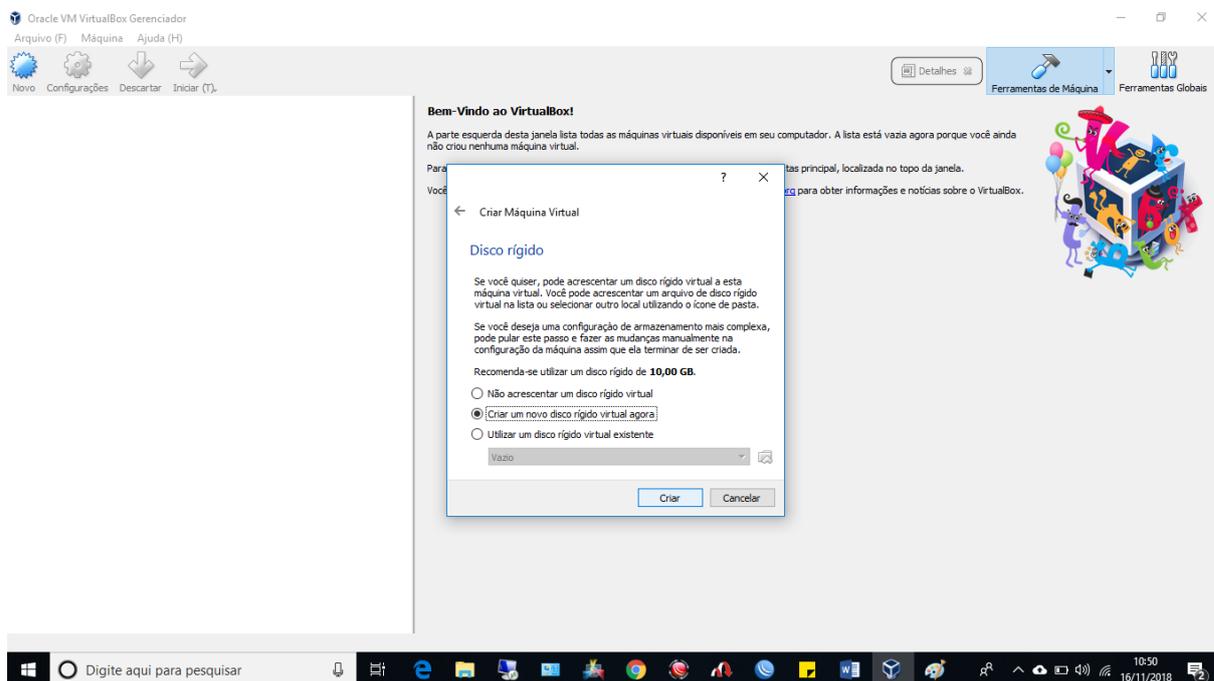


Fonte: Próprio autor

Na figura anterior foi definido o tamanho para 1024MB para dar mais velocidade a máquina virtual. O tamanho máximo de memória disponível para alocar na máquina virtual é de 4GB, porém esse número pode variar de computador para computador.

A seguir deve-se criar um disco rígido virtual onde o sistema Santoku é instalado e configurado.

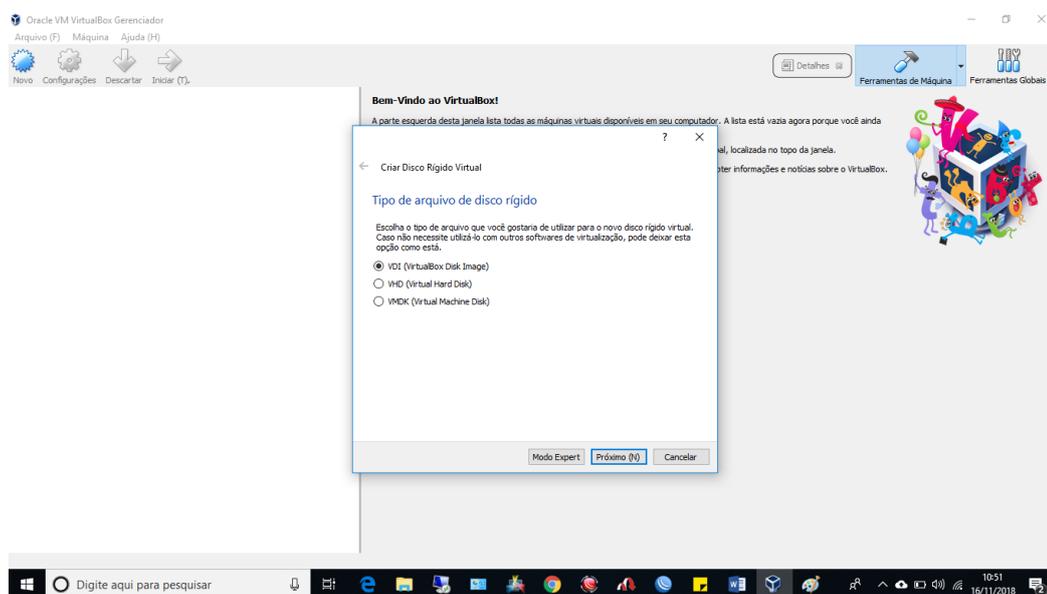
Figura 12: Criar Disco Rígido.



Fonte: Próprio autor

É possível utilizar um disco rígido existente, ou seja, caso haja um backup da máquina virtual. Não é o caso, pois o sistema está sendo instalado pela primeira vez no virtual box.

Figura 13: Tipo de arquivo de Disco Rígido.

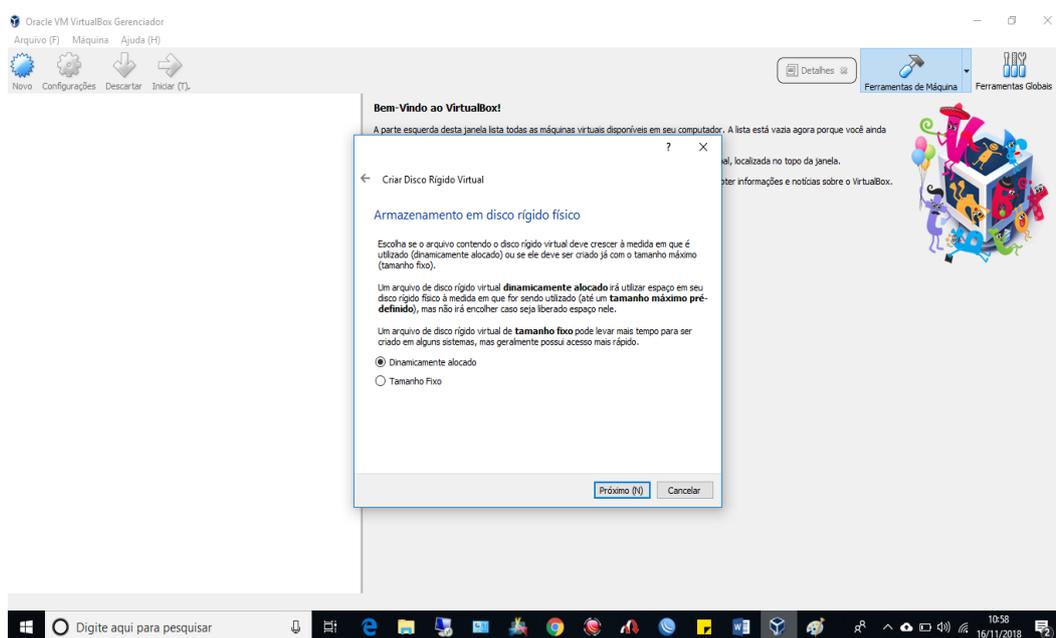


Fonte: Próprio autor

O Virtual Box oferece suporte a discos em vários formatos, tais como discos criados no Paralles e no VMWare da Microsoft, porém por ser o formato nativo do Virtual Box o mais indicado é o VDI (Virtual Disc Image).

Nessa etapa deve-se selecionar qual o tipo de armazenamento em disco rígido físico. O recomendado é “Dinamicamente alocado” pois irá utilizar o espaço em seu disco rígido físico a medida que for sendo utilizado (até um tamanho pré-definido).

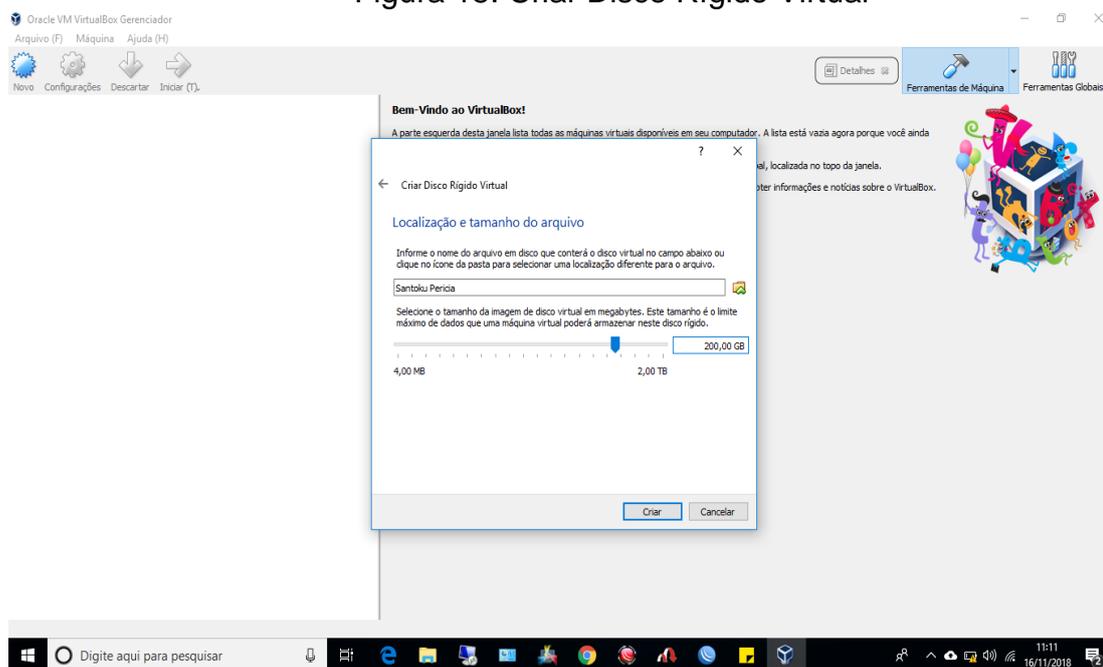
Figura 14: Armazenamento em Disco Rígido Físico



Fonte: Próprio autor

Por fim escolha o local onde o disco rígido virtual será armazenado e clique em salvar. Defina o tamanho para o disco, onde o recomendado é de 40 GB.

Figura 15: Criar Disco Rígido Virtual

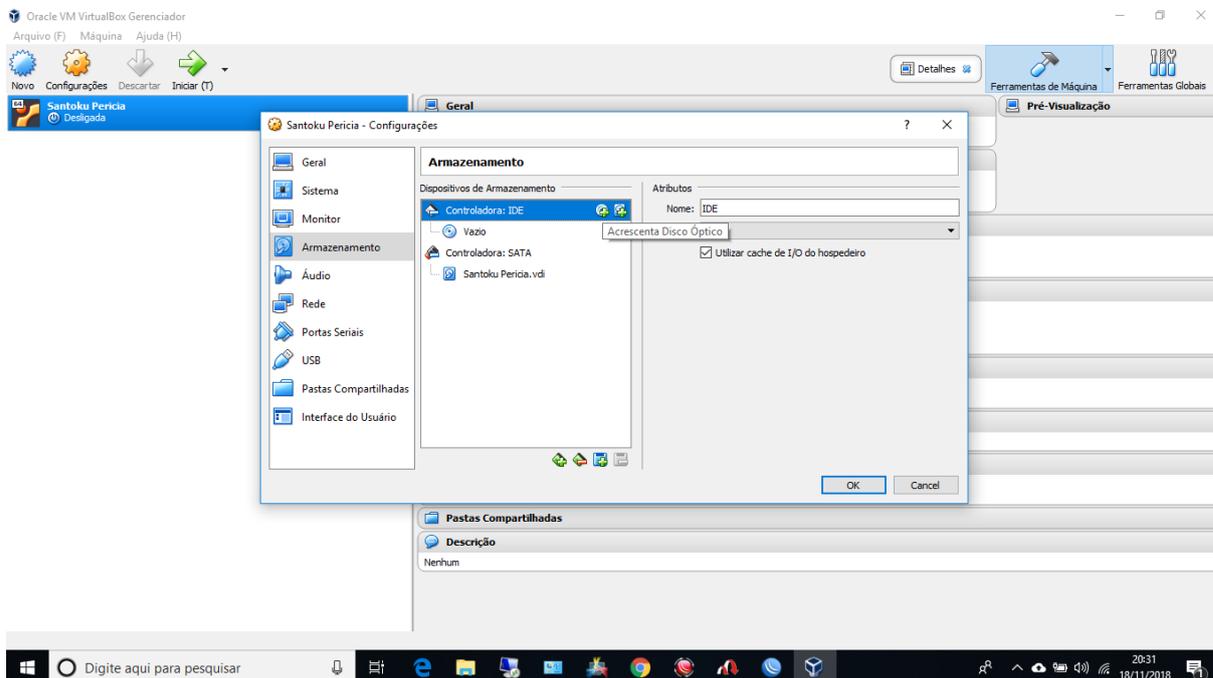


Fonte: Próprio autor

Para não haver problemas futuros por falta de capacidade de armazenamento foi definido o tamanho do disco de 200 GB. Para terminar clique em “Criar”.

Para que o Santoku seja executado no Virtual Box é preciso que seja feita a seguinte configuração. Na máquina virtual em “Configurações”, selecione-se a opção “Armazenamento” e em seguida clique no ícone do CD ao lado do “Controlador IDE”. Esses passos são necessários para vincular o Santoku à Máquina Virtual. É o mesmo que colocar um CD para iniciar um sistema.

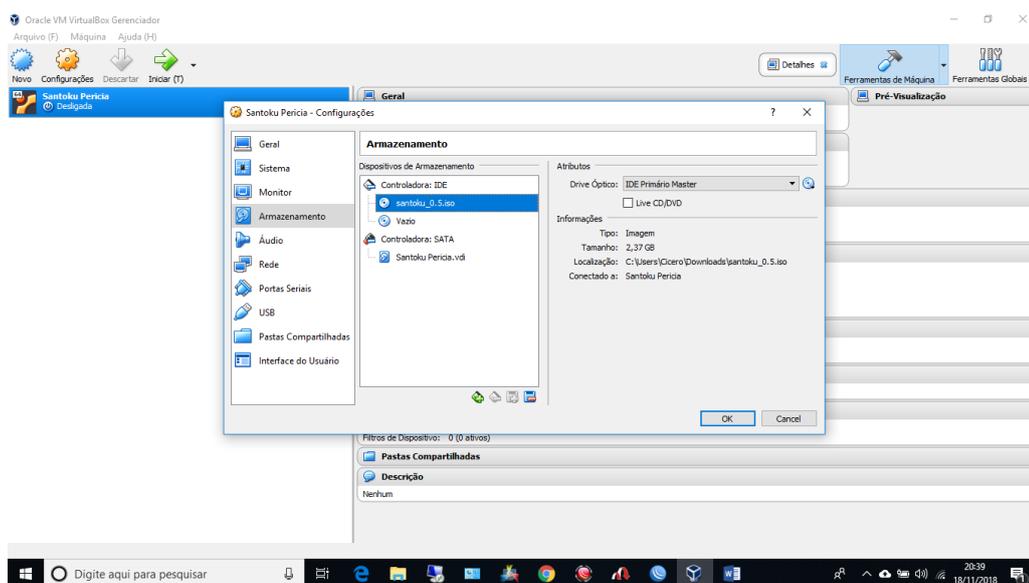
Figura 16: Atribuindo o Santoku a Máquina Virtual



Fonte: Próprio autor

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

Figura 17: Inserindo o Arquivo Santoku.



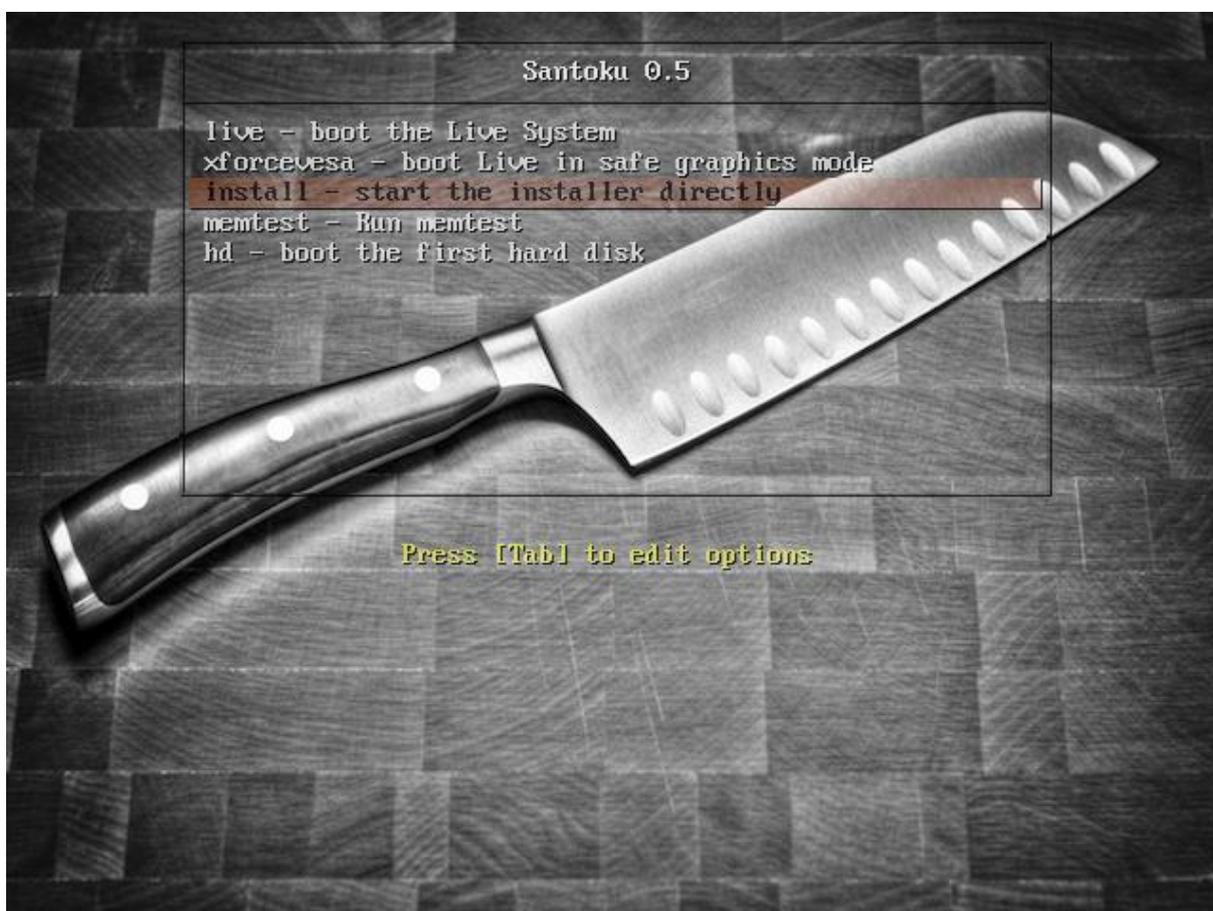
Fonte: Próprio autor

Após todos esses passos a máquina virtual está pronta para ser executada. A seguir o passo a passo da instalação e configuração do Santoku.

2.2 Instalação e configuração do Santoku

Para realizar a instalação do Santoku deve-se primeiramente clicar em “Iniciar” na tela principal do virtual box para carregar a máquina virtual.

Figura 18: Instalando o Santoku



Fonte: Próprio autor

Na figura 18 é apresentada a tela inicial da instalação do Santoku. Ao carregar o sistema seleciona-se “*install -start the installer directy*”.

No decorrer da instalação será pedido que o usuário defina o idioma, fuso horário e configurações de relógio. No último passo da instalação defina um nome de usuário e senha e clique em “instalar”. Será pedido para reiniciar o sistema e estará pronto para uso.

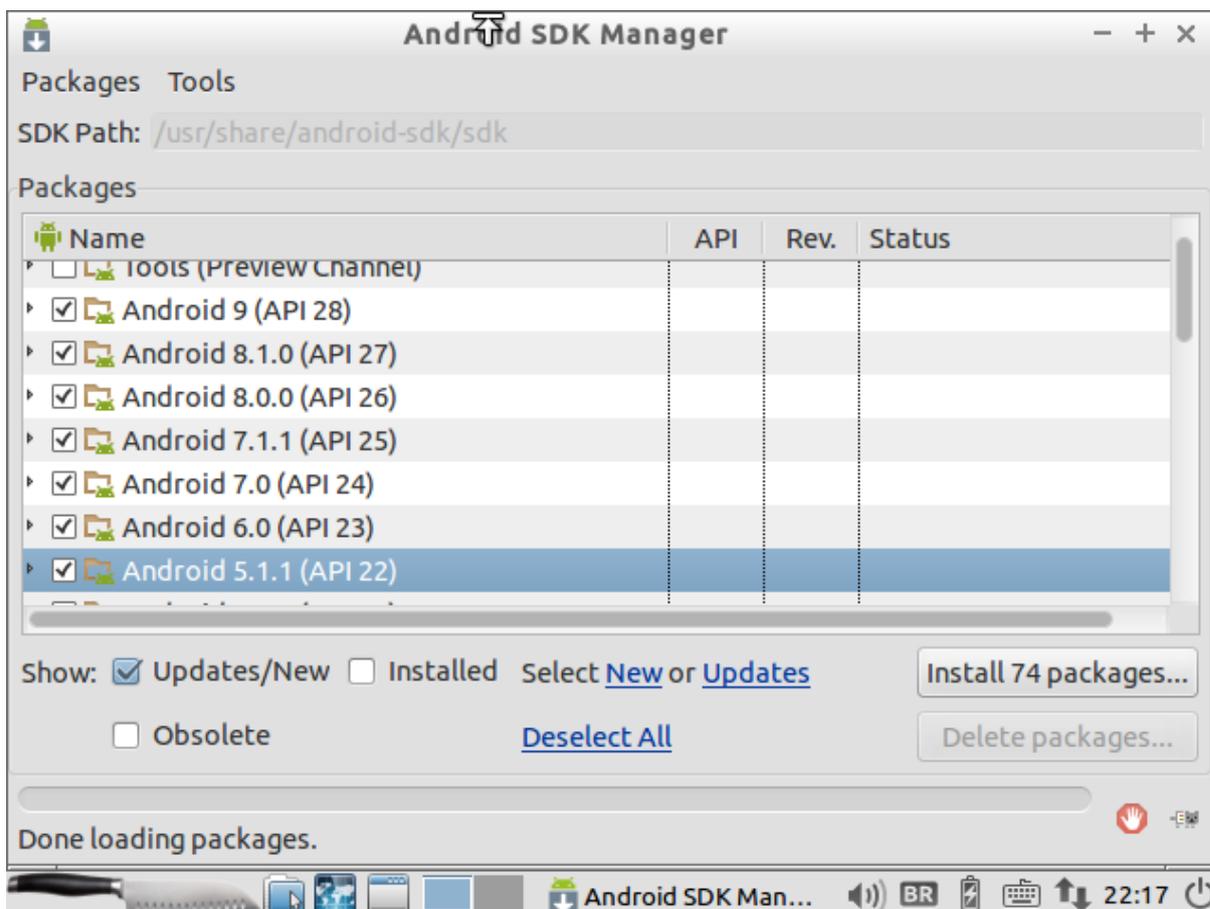
Figura 19: Passos para atualizar o Android SDK Manager



Fonte: Próprio autor

Após iniciado o sistema pela primeira vez é importante que seja atualizado o SDK Manager, para isso deve-se ir até ao “Santoku” em seguida “Development Tools” e por fim “Android SDK Manager”. Conforme mostrado na figura 19.

Figura 20: Atualizando o Android SDK Manager



Fonte: Próprio autor

É importante que seja atualizado o Android SDK Manager para as versões mais recentes do Android. Para tal marque a caixa ao lado das versões do Android e clique em "install packages". Na figura 20 é possível observar que o Santoku oferece suporte para vários tipos de Android.

2.3 Preparação do dispositivo

Conforme apresentado no capítulo 1, a primeira etapa da perícia consiste em proteger os dados que estão no aparelho de interferências externas, dessa forma, como o mesmo encontra-se ligado com cartão de memória e chip SIM, o mesmo foi colocado no modo avião e teve qualquer conexão wi-fi ou bluetooth desligada.

Também é preciso manter o celular carregando para não acabar a bateria e correr o risco de perda de dados armazenados na memória.

2.4 Aquisição dos dados

Os dados podem ser adquiridos de 3 formas, manual, lógica e física. Nesse trabalho foi realizada a aquisição dos dados pelo método manual e lógico, pois o método de aquisição física é mais complexo pois envolve hardwares especiais e conhecimento em eletrônica. Esse método faz uma cópia bit-a-bit de todo o sistema de arquivos, deve ser feita sempre que possível de forma a preservar as evidências. A seguir é explicado como se dá a aquisição dos dados pelos métodos manual e lógico.

2.4.1 Manual

A aquisição manual é feita quando os dados são coletados manualmente navegando pelo dispositivo. Nessa etapa não há necessidade de ferramentas envolvidas, e esse tipo de aquisição tem grandes dificuldades devido a quantidade de conteúdo que pode estar envolvida, pela demora no processo e porque nem todos os dados podem ser coletados.

O indicado nesse método é apenas como forma de uma análise geral do aparelho, do que se tem instalado nele, fotos que são tiradas, vídeos, entre outros. Após isso deve-se partir para uma análise mais aprofundada conforme descrito a seguir.

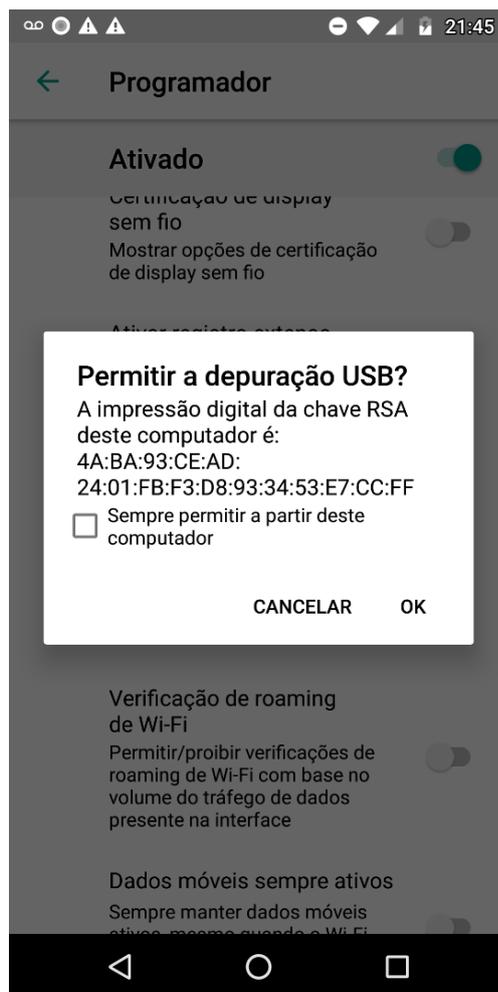
2.4.2 Aquisição Lógica

Nesse tipo de aquisição o conteúdo do telefone é sincronizado com o computador por meio de uma interface, não apaga nem altera os dados. Essa forma de aquisição depende do sistema operacional do aparelho. Conforme descrito na metodologia a aquisição lógica será realizada em um dispositivo com Android 8.0, será utilizado o ADB, que compõe o SDK do Android e possibilita interagir com o dispositivo através dos passos executados abaixo:

1. Conectar o dispositivo no computador;
2. Ativar as opções de desenvolvedor no celular;
3. Ativar a depuração via cabo USB dentro das opções de desenvolvedor;
4. Abrir o terminal no Santoku Linux e entrar com o usuário root;

5. Digitar *adb devices* (Ao digitar o comando “adb devices”, será aberta uma janela no celular periciado com a mensagem perguntando ao usuário se deseja permitir a “Depuração USB” conforme mostrado na figura 21.

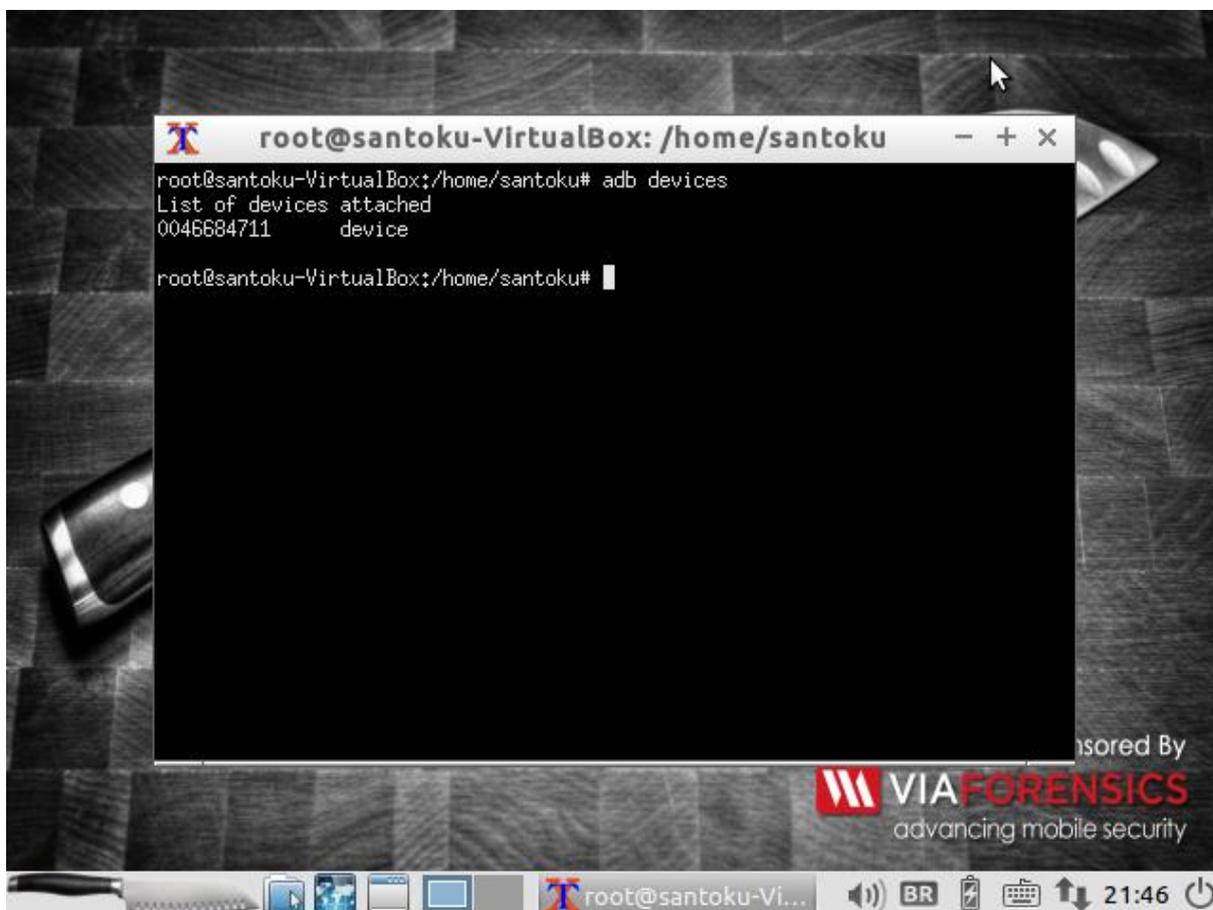
Figura 21: Permissão de Depuração USB



Fonte: Próprio autor

É importante que seja permitido a “Depuração USB” pois caso contrário não será possível extrair os dados do celular.

Figura 22: Com esse comando, você tem uma visão geral de todos os dispositivos conectados ao computador

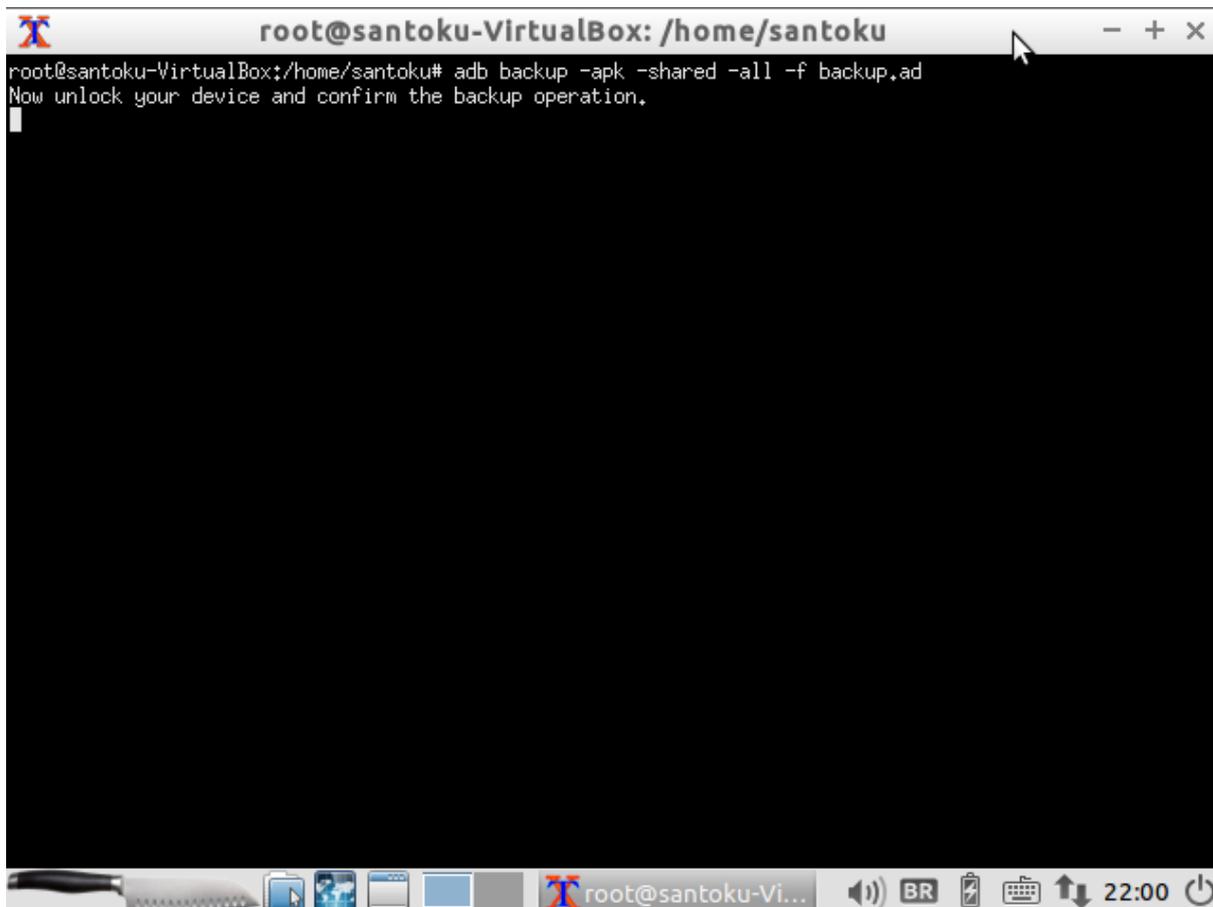


Fonte: Próprio Autor

Dessa forma pode-se conferir que o dispositivo foi identificado pelo sistema operacional;

O próximo passo é extrair os dados do dispositivo, foi utilizado o comando “adb backup”, que é utilizado para realizar uma extração lógica de todo o conteúdo do dispositivo Android, é muito útil para os peritos forenses. A figura 23 mostra o comando em ação.

Figura 23: Comando “adb backup”, extração lógica de dados do Android.



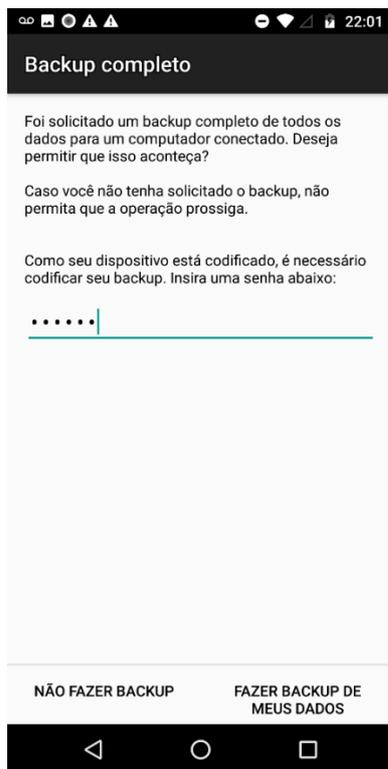
Fonte: Próprio autor

Note que foram acrescentados vários parâmetros junto ao comando "adb backup":

- -apk: Ativa o backup dos arquivos * .apk.
- -shared: Permite o backup do armazenamento compartilhado dos dispositivos / conteúdo do cartão SD.
- -all: Permite o backup de todos os aplicativos instalados.
- -f <arquivo> .ad: grava um arquivo dos dados do dispositivo em um arquivo * .ab especificado.

Ao executar o comando é aberto uma tela no dispositivo solicitando permissão para efetuar o backup. Também oferece a opção de definir uma senha para o backup. Na figura 24 é mostrado a tela do dispositivo solicitando a permissão para o backup.

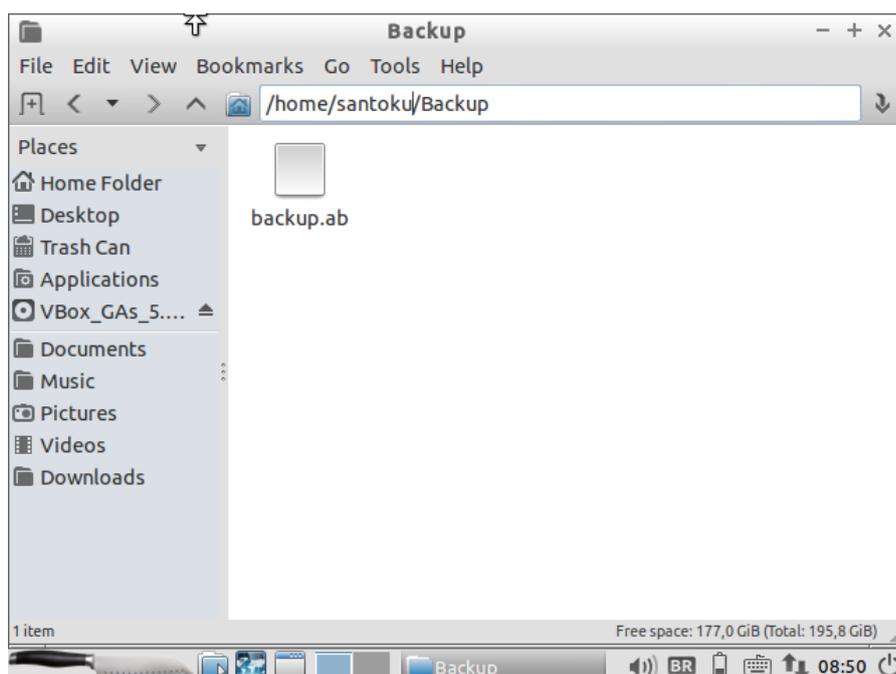
Figura 24: Permissão de backup dos dados no dispositivo periciado



Fonte: Próprio autor

O comando "adb backup" é comumente usado pelos peritos para criar uma imagem lógica do dispositivo Android. Dessa forma não há risco de prejuízo a perícia caso aconteça algo com o dispositivo.

Figura 25: Backup gerado pelo comando "adb backup"



Fonte: Próprio autor

Por fim é gerado o arquivo de backup conforme mostrado na figura 25. Para restaurar o backup deve-se abrir o terminal e digitar `adb restore backup.ab`.

A seguir é apresentado o comando “adb pull”, ele permite que seja feita a cópia de um arquivo ou diretório do dispositivo para o computador. É muito útil caso o perito deseje copiar apenas dados específicos.

Figura 26: Extraindo dados da pasta “data”, do dispositivo

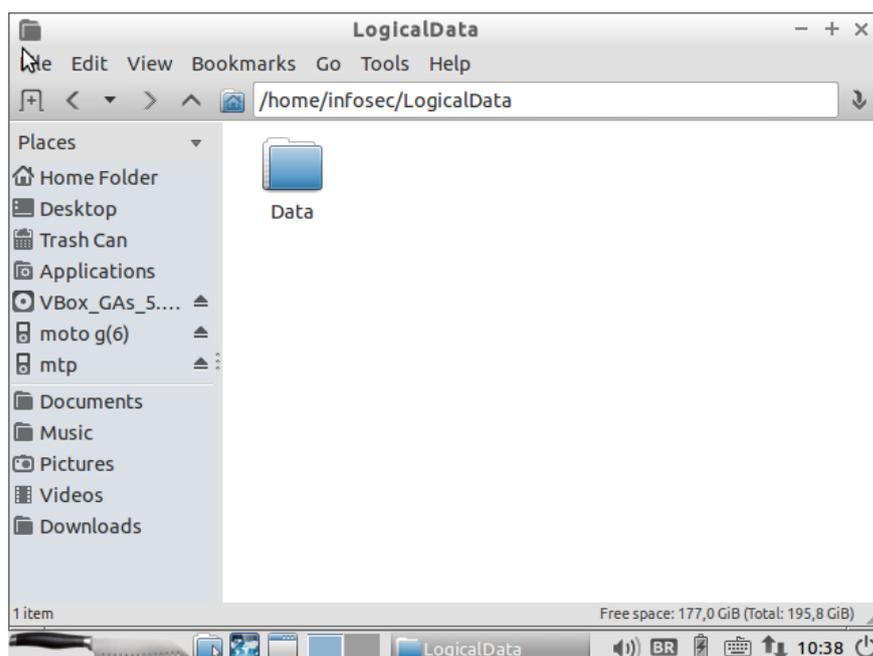
```
infosec@infosec-santoku:~$ adb pull /data /home/infosec/LogicalData
pull: building file list...
pull: /data/app/test_sstream_host -> /home/infosec/LogicalData/app/test_sstream_
host
pull: /data/app/test_char_traits_host -> /home/infosec/LogicalData/app/test_char
_traits_host
pull: /data/app/CubeLiveWallpapers.apk -> /home/infosec/LogicalData/app/CubeLive
Wallpapers.apk
pull: /data/app/test_iomanip_host -> /home/infosec/LogicalData/app/test_iomanip_
host
pull: /data/app/test_string_host -> /home/infosec/LogicalData/app/test_string_ho
st
pull: /data/app/test_vector_host -> /home/infosec/LogicalData/app/test_vector_ho
st
pull: /data/app/test_limits_host -> /home/infosec/LogicalData/app/test_limits_ho
st
```

Fonte: Próprio autor

O objetivo da extração realizada é copiar a pasta “data” do dispositivo, pois é onde estão localizados os dados do WhatsApp.

Após a execução do comando “adb pull”, pode-se abrir a pasta diretamente pelo gerenciador de arquivos do computador.

Figura 27: Extração de arquivos via Santoku Linux



Fonte: Próprio autor

Conforme visto a pasta “data” foi extraída do dispositivo para o computador e agora pode-se analisar o conteúdo da mesma.

Outra extração que pode-se fazer são os contatos, históricos de ligações e mensagens, através da ferramenta “AF LOGICAL OSE” disponível no Android, e apresentado na Figura 28 a seguir.

Figura 28: Caminho para a ferramenta AF LOGICAL OSE no Santoku Linux



Fonte: Próprio autor

Para essa etapa é utilizado o AF Logical OSE que é uma poderosa ferramenta de extração de dados. Abra o terminal do Santoku e digite o comando: “sudo adb devices” para conferir se o dispositivo está conectado no computador. Será aberto uma tela no dispositivo solicitando ao usuário que autorize a depuração USB conforme visto anteriormente na figura 24.

Após a permissão da depuração usb, deve-se digitar no terminal: “aflogical-ose”, nesse momento será instalado um aplicativo no dispositivo (que deve ser removido posteriormente), ele irá possibilitar a extração dos dados de contatos, sms, registro de ligações, MMS. Ao terminar a instalação, automaticamente é aberto no celular o aplicativo para que se selecione o que desejamos extrair, conforme apresentado na Figura 29.

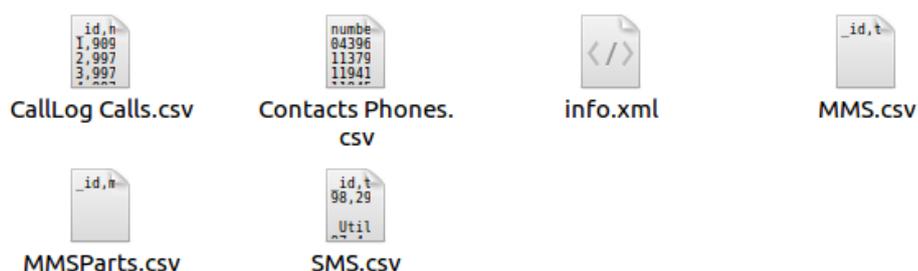
Figura 29:Extração de dados via ferramenta AF LOGICAL OSE



Fonte: Próprio autor

Apos a execução do programa é gerado uma pasta com os dados extraídos, eles aparecem em formato .csv e .xml, conforme apresentado na Figura 30.

Figura 30:Apresentação dos dados extraídos com a ferramenta AF LOGICAL OSE.



Fonte: Próprio autor

Os dados extraídos com a extensão “.csv” agora podem ser abertos através do programa nativo do Santoku GNUmeric, que é similar ao Excel do Windows. O arquivo “info.xml”, contém informações sobre o dispositivo, tais como dados do fabricante, versão do sistema operacional, data de fabricação. Para abrir o arquivo info.xml é necessário um software leitor de xml. No próximo capítulo são apresentados os resultados da perícia nos arquivos extraídos.

3 RESULTADOS

Com base nos resultados da seção 2.4 a perícia foi realizada por meio da aquisição manual e lógica.

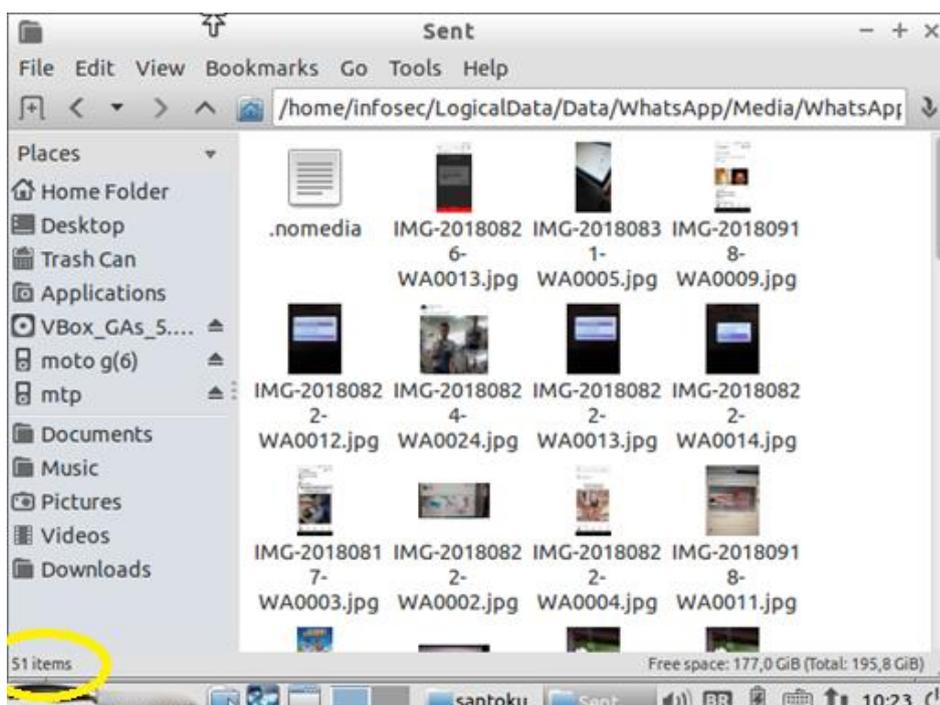
A aquisição manual consistiu em realizar uma verificação superficial dos dados de forma rápida no smartphone navegando manualmente por ele. Foi aberto as conversas do WhatsApp, a galeria de fotos do dispositivo, foi verificado vídeos, porém como o processo foi todo manual não foi possível apresentar os resultados nessa sessão. A aquisição lógica foi realizada de duas formas:

1. Por meio da ferramenta "adb", utilizando o comando "adb pull".
2. Por meio da ferramenta AF Logical OSE.

3.1 Extração de dados por meio do adb.

Primeiramente a extração dos dados se deu por meio da ferramenta "ADB", onde foi realizado a extração da pasta "data" com o objetivo de extrair fotos enviadas pelo WhatsApp conforme a figura 31 a seguir revela.

Figura 31: Fotos encontradas dentro da pasta "data"



Fonte: Próprio autor.

Como visto na figura 31 foram encontradas 51 fotos o que mostra a eficácia da ferramenta na extração dos dados.

3.2 Extração de dados por meio do AF Logical OSE

O segundo método teve a extração dos dados através da ferramenta AF Logical OSE. Foi realizado a extração de mensagens, registro de ligações e agenda de contato.

Figura 32: SMS entre o suspeito de pedofilia e a vítima

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	id	thread	address	person	date	date_sent	protocol	read	status	type	callback_n	reply_path	subject	body
1	313	82	5533984258564		1543525397299	1543525395000	0	1	-1	1		0		tá mas não mostra para ninguém tá..
2	312	82	5533984078886		1543525397299	1543525364000	0	1	-1	1		0		Quero ver seu nudes, me manda?
3	311	90	5533984258564		1543525397299	1543498463000	0	0	-1	1		0		tenho 13 e você?
4	310	4	5533984078886		1543525397299	1543498463000	0	0	-1	1		0		Quanto tempo você tem?
5	309	20	5533984078886		1543525397299	1543525395000	0	1	-1	1		0		Que menina linda hein, adoro uma novinha
6	308	25	5533984078886		1543525397299	1543525364000	0	1	-1	1		0		Olá você? refiz as fotos que te enviei?
7	307	88	29090		1543525397299	1543262236000	0	0	-1	1		0		Seu código e 827275 as 2018-11-26 17:57
8	306	88	29090		1543525397299	1543262568000	0	0	-1	1		0		Seu código e 735272 as 2018-11-26 17:58
9	305	89	29097		1543525397299	1543262342000	0	0	-1	1		0		Seu código e 162482 as 2018-11-26 17:58
10	304	88	29090		1543525397299	1543262303000	0	0	-1	1		0		Seu código e 380461 as 2018-11-26 17:55
11	303	87	29095		1543525397299	1543262144000	0	0	-1	1		0		

Fonte: Próprio autor

A análise das mensagens pode revelar muitas informações relevantes em uma investigação policial. Conforme mostrado na figura 32 foi usado como exemplo a troca de mensagens entre um suposto pedófilo e uma menina menor de idade. Em destaque é possível ver que o suspeito pede para a vítima enviar “nudes” (gíria usada para pedir fotos sem roupa).

Através da extração lógica dos dados realizada com o auxílio do AF logical OSE foi possível fazer uma análise do registro de ligações do dispositivo periciado. É uma informação que pode ser útil em casos de sequestro ou de tráfico de drogas onde é possível resgatar todo o histórico de ligações do celular. A figura a seguir mostra o registro de ligações do dispositivo periciado.

Figura 33: Registro de ligações do dispositivo periciado

*CallLog Calls.csv - Gnumeric

Arquivo Editar Visualizar Inserir Formatar Ferramentas Statistics Dados Ajuda

Sans 10

G1 = name

	A	B	C	D	E	F	G	H	I	J	K	L
1	_id	number	date	duration	type	new	name	numbertyp	numberlabel			
2	1	15415265577	1533832174792	39	1	1						
3	2	31994159722	1534087139978	0	3	0						
4	3	984315398	1534115856114	0	2	1	Sabor E I	2				
5	4	84315398	1534115899168	0	2	1	Sabor E I	2				
6	5	33984313719	1534159365001	113	1	1						
7	6	1101396493	1534162219540	0	3	0						
8	7	41997407223	1534359172645	0	3	0	Tio	2				
9	8	41997407223	1534379630911	0	3	0	Tio	2				
10	9	1124483647	1534519681735	0	3	0	English Li					
11	10	1124483647	1534526285358	242	1	1	English Li					
12	11	32984210775	1534890687560	11	1	1	Acesse L	2				
13	12	32984210775	1534895797072	43	1	1	Acesse L	2				
14	13	32984210775	1534896900445	74	1	1	Acesse L	2				
15	14	1148415140	1534946517447	0	5	1	Bradesco					
16	15	1148415140	1534951957680	0	3	0	Bradesco					
17	16	1148415140	1534967486910	1	1	1	Bradesco					
18	17	1148415140	1534968195355	0	3	0	Bradesco					
19	18	1148415140	1534977263318	0	5	1	Bradesco					
20	19	5533999901531	1535144353109	2	2	1	Amor	12				
21	20	1104453392	1535496739494	1	1	1						
22	21	3333227900	1535544154813	121	1	1						
23	22	1148415140	1535722622329	0	3	0	Bradesco					
24	23	1148415140	1535734553063	0	3	0	Bradesco					
25	24	1148415140	1535738195429	0	3	0	Bradesco					
26	25	1148415140	1535744758742	0	5	1	Bradesco					
27	26	33984069149	1535835381880	0	3	0						
28	27	1105756832	1536100221170	0	3	0						
29	28	32984832697	1536190149585	1369	1	1						
30	29	*100	1536322913265	0	2	1						
31	30	5533999901531	1536471589810	0	2	1	Amor	12				

CallLog Calls.csv

Fonte: Próprio Autor

Observa-se que na tabela gerada é possível encontrar o nome e número das pessoas que fizeram contato com o dispositivo periciado.

Por último foi periciado a agenda de contatos no dispositivo. A figura 34 mostra os contatos.

Figura 34: Contatos extraídos do dispositivo periciado

*Contacts Phones.csv - Gnumeric

Arquivo Editar Visualizar Inserir Formatar Ferramentas Statistics Dados Ajuda

Sans 10 100%

L1 number

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	phonetic_r	last_time	send_to_v	custom_rii	notes	label	display_na	type	isprimary	number_key	primary_p	number	starred	person	ni
2		0	0				Acesse Me	2	0	1612782997255		+55 27 992	0	29	Ar
3		0	0				Nem	2	0	466834381355		+55 31 834	0	86	Ni
4		0	0				JV	2	0	227951491355		+55 31 941	0	8	JL
5		0	0				Rafaela	2	0	888203491355		+55 31 943	0	60	Ri
6		0	0				Nayara Le	2	0	142529491355		+55 31 949	0	109	Ni
7		0	0				AndrÃ© A	2	0	676060482355		+55 32 840	0	113	Ar
8		0	0				Acesse Fe	2	0	109012482355		+55 32 842	0	77	Ar
9		0	0				Acesse Lai	2	0	300572482355		+55 32 842	0	34	Ar
10		0	0				Acesse Jaj	2	0	878672482355		+55 32 842	0	52	Ar
11		0	0				Acesse NC	2	0	140792482355		+55 32 842	0	35	Ar
12		0	0				Acesse Ad	2	0	619014482355		+55 32 844	0	27	Ar
13		0	0				Acesse Vir	2	0	796238482355		+55 32 848	0	44	Ar
14		0	0				Acesse Ge	2	0	699360582355		+55 32 850	0	79	Ar
15		0	0			Outros	Dell	0	0	2883192355		+55 32 913	0	45	Dr
16		0	0				Acesse Du	2	0	338804892355		+55 32 984	0	53	Ar
17		0	0			Celular	Casa Lanc	0	0	390114333355		+55 33 334	0	101	Cr
18		0	0			Celular	Celio Tava	0	0	348114333355		+55 33 334	0	17	Cr
19		0	0				Beto	2	0	677360483355		+55 33 840	0	93	Br
20		0	0				Acesse Da	2	0	968360483355		+55 33 840	0	81	Ar
21		0	0				MÃ©e	2	0	757521483355		+55 33 841	0	25	M
22		0	0				Tia DinÃ	2	0	252882483355		+55 33 842	0	43	Ti
23		0	0				AndrÃ©	2	0	578192483355		+55 33 842	0	95	Ar
24		0	0				Acesse Ra	2	0	755503483355		+55 33 843	0	227	Ar

Fonte: Próprio autor

Foram encontrados mais de 200 contatos na agenda do dispositivo periciado, a coluna com número do contato foi diminuída para respeitar a privacidade dos contatos.

4 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho teve por objetivo abordar o tema da Perícia Forense em dispositivos móveis, foi proposto um estudo de caso explicando métodos para aquisição de dados como: mensagens, fotos, agenda de contatos e registro de ligações em um smartphone com Android, listando as principais maneiras necessárias para uma análise correta.

Para a realização do estudo foram efetuadas pesquisas sobre sistemas operacionais, computação forense, perícia forense em dispositivos móveis e ferramentas forenses com o intuito de obter embasamento teórico para essa pesquisa. Posteriormente foi escolhida a ferramenta de análise e optou-se pela escolha do Santoku Linux.

Ao realizar o trabalho de perícia forense em dispositivos móveis é muito importante a utilização de técnicas e procedimentos homologados e bem fundamentados para que todo o processo de investigação se torne seguro e válido.

Os resultados obtidos no estudo de caso evidenciaram os recursos presentes no sistema Santoku Linux pois através das ferramentas presentes no sistema foi possível realizar a extração de fotos enviadas pelo whatsapp, mensagens sms, registro de ligações e agenda de contatos.

Estudos futuros podem ser realizados com smartphones formatados em que os dados necessitariam ser recuperados. Outro aspecto relevante seria realizar uma perícia em um smartphone com segurança biométrica ativa.

Por fim como trabalho futuro desejamos continuar estudando o Santoku Linux, de forma a aplicar os conhecimentos em um estudo de caso envolvendo malwares em celulares Android.

5 REFERÊNCIAS BIBLIOGRÁFICAS

Android. **Android interfaces**. Disponível em <<https://source.android.com/devices/>>. Acesso em 4 de maio de 2018. 2015.

Apple. **About the ios technologies**. Disponível em <>. Acesso em 2 de julho de 2018. 2015.

ARTHUR, K. K. **An Investigation Into Computer Forensic Tools**. Disponível em: <http://www.infosecsa.co.za/proceedings2004/060.pdf,2004>. Acesso em 26/nov/2018.

CAMINHANDO LIVRE. **Santoku linux: perícia forense, análise de malwares e segurança em dispositivos móveis**. Disponível em: <<https://caminhandolivre.wordpress.com/2012/08/26/santoku-inux-pericia-forense-analise-de-malwares-e-seguranca-em-dispositivos-moveis/>>. Acesso em: 22 nov 2018.

CARROLL, O. L.; BRANNON, S. K. e SONG, T. **Computer Forensics: Digital Forensic Analysis Methodology**. The United States Attorneys' Bulletin. 2008

ELEUTÉRIO, P. M. S, MACHADO, M. P. **Desvendando a Computação Forense**. 1ª ed. São Paulo: Novatec, 2011.

ENCASE: Reports. **The Dold Standard in Forense Investios – Including Mobile Acquisiton**. Disponível em: <<https://www.guidancesoftware.com/encase-forensic>>. Acesso em: 29 nov 2018.

FARMER, D. **Perícia forense computacional**. São Paulo: Pearson Prentice Hall, 2007.

FGV. **Pesquisa Anul do Uso do TI**. 2017. Disponível em : <<https://eaesp.fgv.br/ensinoeconhecimento/centros/cia/pesquisa>>. Acesso em 25 de agosto de 2018.

GARCIA, M. A. P. **Filtros de imagens para ios**. Disponível em: <<http://www.tcc-computacao.tiagodemelo.info/monografias/2013/tcc-mario-angel.pdf>>. Acessado em: 22 de abril de 2015. 2013.

HOOG, A. **Android Forensics: Investigation, Analysis and Mobile Security for Google Android** . 1 ed. Editora Elsevier. 2012.

IDH. **Smartphone Market Share**. Disponível em :
<<https://www.idc.com/promo/smartphone-market-share/os>>. Acesso em 28 de agosto de 2018. 2017.

JANSEN, W. & DELAITRE, A. & MOENNER, L. **Overcoming Impediments to Cell Phone Forensics**. Proceedings of the 41 st Annual Hawaii International Conference on System Sciences. 2008.

JOSEPH, A. & SINGH, K. J. **A Study on Digital Forensic in Mobile Devices**. **International Journal Of Electrical, Electronics And Data Communication**. Volume-5, Issue-12. 2017.

KENT, K. et al. **Guide to integrating forensic techniques into incident response: recomendations of the National Institute of Standards and Technology**. Special publication. Gaithersburg: NIST, 2006.

LECHETA, R. **Google Android: “Aprenda a criar aplicações para dispositivos móveis com o Android SDK”**. São Paulo, Novatec Editora, 2017.

LOPES, P . **Forence digital: perícia forense computacional** 11 DE JUNHO DE 2016 . Disponível em: <https://periciacomputacional.com/pericia-forense-computacional-2/>. Acesso em: 30 nov 2018.

M.DROID. **Comandos ABD úteis que você pode fazer no android**. Disponível em: < <http://m-droid.com.br/tutoriais/adb/comandos-adb/comandos-adb-uteis-que-voce-pode-fazer-no-android/>>. Acesso em: 20 nov 2018.

MILANI, A. Programando para iPhone e iPad - **Aprenda a construir aplicativos para o iOS**. São Paulo: Novatec Editora. 2012.

Norton Cyber Security. **Norton Cyber Security Insights Report 2017**. Disponível em <<https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>>. Acesso em 25 de agosto de 2018.

NUNES, F. **Avaliação de técnicas e mecanismos para entrada e saída de informações em dispositivos móveis**. Disponível em:

<[http://aberto.univem.edu.br/bitstream/handle/11077/998/Fernando Nunes.pdf](http://aberto.univem.edu.br/bitstream/handle/11077/998/FernandoNunes.pdf)>. Acessado em: 13 mai. 2018. 2014.

PRITCHETT, WILLIE. L.; SMET, David De. (2013). **Kali Linux CookBook**. Packt Publishing Ltd., Birmingham.

REIS, M. A; GEUS, P. L. **Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas**. Instituto de Computação -Universidade Estadual de Campinas, 2004, p.54.

RUIZ, L. O. A. **Criminalística - Aspectos históricos e evolução no Estado de São Paulo**. Disponível em:

<http://www.revistademedicinalegal.com.br/default.aspx?edicao=&secao=16&subsec%20ao=45&indice=1&indiceSubsecao=1> > Acesso em: 25 outubro 2018.

SIMÃO, A. M. L.; SICOLI, F. C.; MELO, L. P.; SOUSA JR.; R. T. **Acquisition of digital evidence in android smartphones. Proceedings of the 9th Australian Digital Forensics Conference**. Edith Cowan University. 2011.

SLEUTHKIT. **Open Source Digital Forensics**. Disponível em: <<http://www.sleuthkit.org/index.php>>. Acesso em: 25 novembro 2018.

VARGAS. R. G.; QUINTÃO, P.L; GRIZENDI, L.T. **Perícia Forense Computacional**. Anais do I Workshop de Trabalhos de Iniciação Científica e de Graduação da Faculdade Metodista Granbery, pp. 20-29, Juiz de Fora, Maio de 2007.