METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE

CLAUDINEI MORIN DA SILVEIRA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM ENGENHARIA ELÉTRICA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

METHODOLOGY FOR FORENSICS DATA RECONSTRUCTION ON MOBILE DEVICES WITH ANDROID OPERATING SYSTEM APPLYING IN-SYSTEM PROGRAMMING AND COMBINATION FIRMWARE

METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE

CLAUDINEI MORIN DA SILVEIRA

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR, DR.
COORIENTADOR: ROBSON DE OLIVEIRA ALBUQUERQUE, DR.

DISSERTAÇÃO DE MESTRADO PROFISSIONAL
EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.004

BRASÍLIA/DF: AGOSTO - 2020

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE

CLAUDINEI MORIN DA SILVEIRA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

_____

Prof. Dr. Rafael Timóteo de Sousa Júnior – ENE/Universidade de Brasília
Orientador

_____

Prof.ª Dra. Edna Dias Canedo – ENE/Universidade de Brasília
Membro Interno

_____

Prof.ª Dra. Ana Paula Bernardi da Silva – PPGTI/Universidade Católica de Brasília
Membro Externo

BRASÍLIA, 17 DE AGOSTO DE 2020.

FICHA CATALOGRÁFICA

MORIN DA SILVEIRA, CLAUDINEI
METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE [Distrito Federal] 2020.
xiv, 72p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2020).
Dissertação de Mestrado Profissional – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. forense de dispositivos móveis
2. In-System Programming
3. aquisição de dados
4. Combination Firmware
I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

MORIN DA SILVEIRA, C. (2020). METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE . Dissertação de Mestrado Profissional em Engenharia Elétrica, Publicação PPEE.MP.004, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 72p.

CESSÃO DE DIREITOS

AUTOR: Claudinei Morin da Silveira
TÍTULO: METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE .
GRAU: Mestre ANO: 2020

Claudinei Morin da Silveira

Departamento de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

"Deixem que o futuro diga a verdade e avalie cada um de acordo com o seu trabalho e realizações. O presente pertence a eles, mas o futuro pelo qual eu sempre trabalhei pertence a mim" (Nikola Tesla)

AGRADECIMENTOS

Agradeço primeiramente a Deus, pelo dom da vida, pela saúde, pela serenidade, por ter me feito capaz de perseverar. Agradeço pela oportunidade de ajudar a tranformar a sociedade onde vivo em um lugar melhor.

Agradeço a minha esposa Neliza, que sempre esteve presente, seja para celebrar momentos de euforia por bons resultados obtidos, para confessar nervosismos ou mesmo para compartilhar frustrações, por sempre ter me dado atenção e ouvidos. Obrigado por estar ao meu lado em todas essas etapas, obrigado pelas orações, paciência, companheirismo e fé. Você foi fundamental para que mais esse desafio fosse superado.

Agradeço aos filhos meus Anna Karolina e Petrus por terem suportado, de forma muito compreensiva e amorosa, minha ausência em muitos momentos onde gostariam de contar com minha presença.

Agradeço aos meus pais Salete e Edil, minha avó Geny, e minha irmã Edilaura, pelo apoio, mesmo à distância, e por sempre acreditaram na minha capacidade.

Agradeço ao meu orientador, Prof. Dr. Rafael, ao meu Coorientador, Prof. Dr. Robson, por terem aceitado este desafio, pelo constante apoio, paciência, dedicação, disponibilidade e profissionalismo, essenciais para a realização deste trabalho. Agradeço também ao Prof. Dr. Georges, pelo profissionalilsmo e pelo incentivo.

Gratidão também não pode faltar ao amigo Gildásio, pelo incentivo, apoio, e pelas conversas que me proporcionaram reflexões importantes.

Agradeço ainda ao amigo Djalma, por compartilhar seus conhecimentos, pela ajuda e pelas inúmeras madrugadas discutindo possibilidades.

Não poderia deixar de agradecer a todos aqueles que me acompanham desde minha chegada à Brasília, e que também acompanharam os passos dados ao longo deste mestrado: Adriano, Carlos Sydrião, Edson, Felipe, Francisco Régis, Júlio Adilson, Marco Antonio, Rafael e Rômulo. Amigos, muito obrigado!

RESUMO

Título: METODOLOGIA PARA RECONSTRUÇÃO DE DADOS EM DISPOSITIVOS MÓVEIS COM SISTEMA OPERACIONAL ANDROID MEDIANTE APLICAÇÃO DE TÉCNICAS ISP E COMBINATION FIRMWARE
Autor: Claudinei Morin da Silveira
Orientador: Rafael Timóteo de Sousa Júnior, Dr.
Coorientador: Robson de Oliveira Albuquerque, Dr.
Programa de Pós-Graduação Profissional em Engenharia Elétrica – Área de Concentração em Segurança Cibernética
Brasília, 17 de agosto de 2020

Este trabalho propõe uma nova metodologia de análise forense que combina processos, técnicas e ferramentas para aquisição física e lógica de dados de dispositivos móveis. A metodologia proposta integra o emprego da técnica de *In-System Programming* (ISP) com o uso de *Combination Firmware*, elementos que são alinhados com processos específicos de coleta e análise. Para efeito de validação da proposta, as experiências realizadas demonstram que a nova metodologia proposta é praticável e fornece novas possibilidades para aquisição de dados em dispositivos que executam o Sistema Operacional Android com mecanismos avançados de proteção. A metodologia é viável mesmo em dispositivos que utilizam memória principal do tipo *Embedded Multimedia Card* (eMMC) ou *Embedded Multi-Chip Package* (eMCP), e que sejam compatíveis com o emprego das técnicas ISP. As técnicas incluídas na metodologia são eficazes em dispositivos criptografados onde a técnica de JATG e *Chip-Off* se mostram ineficazes, principalmente os que possuem mecanismo de proteção de acesso não autorizado ativados, tais como senha de bloqueio de tela, *bootloader* bloqueado e *Factory reset Protection* (FRP) ativo. Os estudos também demonstram que a metodologia é aplicável a cerca de 70% dos dispositivos móveis com Sistema Operacional (SO) Android em uso atualmente, preservando a integridade dos dados, o que é fundamental para um processo de forense digital.

Palavras-chave: Forense de dispositivos móveis, *In-System Programming*, *Combination Firmware*, Aquisição de dados.

ABSTRACT

Title: METHODOLOGY FOR FORENSICS DATA RECONSTRUCTION ON MOBILE DEVICES WITH ANDROID OPERATING SYSTEM APPLYING IN-SYSTEM PROGRAMMING AND COMBINATION FIRMWARE
Author: Claudinei Morin da Silveira
Supervisor: Rafael Timóteo de Sousa Júnior, Dr.
Co-Supervisor: Robson de Oliveira Albuquerque, Dr.
Professional Post-Graduate Program in Electrical Engineering – Cybersecurity Concentration Area
Brasília, August 17th, 2020

This work proposes a new forensic analysis methodology that combines processes, techniques and tools for physical and logical data acquisition from mobile devices. The proposed methodology integrates the use of the In-System Programming (ISP) technique with the use of Combination Firmware, elements that are aligned with specific collection and analysis processes. For the purpose of validating the proposal, the experiments carried out demonstrate that the new proposed methodology is feasible and provides new possibilities for data acquisition on devices that run the Android Operating System with advanced protection mechanisms. The methodology is feasible even on devices that use Embedded Multimedia Card (eMMC) or Embedded Multi-Chip Package (eMCP) main memory, and that are compatible with the use of ISP techniques. The techniques included in the methodology are effective on encrypted devices where the JATG and Chip-Off technique are ineffective, especially those that have protection mechanisms for unauthorized access enabled, such as screen lock password, blocked bootloader and Factory reset Protection (FRP) active. Studies also show that, the methodology is applicable to about 70 % of mobile devices with an Operating System (SO) Android currently in use, preserving data integrity, which is essential for a digital forensics process.

Keywords: Mobile Device forensics, In-System Programming, Combination Firmware, Data acquisition.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS E ABREVIA CÕES

ADB Android Debug Bridge. 25, 36, 37, 58
AOSP Android Open Source Projec. 16
ART Android Runtime. 26
AVB Android Verified Boot. 18–21, 38, 43, 66

BGA Ball Grid Array. 11

CAS Cellebrite Advanced Service. 32
CC Common Criteria. 23

EDL Emergency Download Mode. 14, 23
eMCP Embedded Multi-Chip Package. i, 11, 37, 61
eMMC Embedded Multimedia Card. i, 11, 22, 25, 37, 43, 45, 46, 50, 54, 55, 58, 59, 61
EXT4 Fourth Extended Filesystem. 7, 23, 43, 50, 54, 61

F2FS Flash-Friendly File System. 7, 58, 61
FBE File-Based Encryption. 5, 17, 24, 39, 45, 59, 61
FDE Full-Disk Encryption. 16, 17, 39, 52, 55, 61
FRP Factory Reset Protection. i, 35, 39, 43, 44, 47, 51, 55, 56, 58

GPS Global Positioning System. 4, 30
GSI Generic System Image. 16
GSM Global System for Mobile. 30, 31

IMEI International Mobile Equipment Identity. 31
IMSI International Mobile Subscriber Identity. 31
IPED Indexador e Processador de Evidências Digitais. 21
ISP In-System Programming. xi, xii, 3, 6, 7, 9–14, 18, 24, 27, 33, 35, 37–39, 43, 46, 56, 63, 64

JATG Joint Test Action Group. i, 9, 10, 21, 24–27, 37, 38, 45, 55, 59

LCD Liquid Crystal Display. 10, 36
LLDA-ISPCF Low Level Data Acquisition with In-System Programing and Combination Firmware. 5, 6, 33, 62, 65

MMS Multimedia Messaging Service. 31

NFC Near Field Communication. 35
NIST National Institute of Standards and Tecnology. 9, 21, 25, 37

OEM Original Equipment Manufacturer. 18
OMA Open Mobile Alliance. 15
OTA Over-the-air. 15

PBL Primary Bootloader. 18

RAM Random Access Memory. 15, 26, 27
ROM Read-Only Memory. 15
RoT Root of Trust. 19, 20

SE Secure Element. 17
SMD Surface-Mount Device. 10
SMS Short Message Service. 4, 17, 30, 31
SO Sistema Operacional. i, 1, 3, 5–7, 18, 19, 22–27, 31, 34, 36–40, 42, 43, 45, 51, 54, 59–63
SoC System on a chip. 1, 14, 17, 18, 23, 34, 39, 42, 43, 48, 50, 54, 57, 58, 61, 66

TAP Test Acess Point. xi, xii, 10, 11, 13, 14, 35–38, 43, 45, 46, 55, 56, 59, 63
TEE Trusted Execution Environment. 17, 18

UFED Universal Forensic Extraction Device. 3, 14, 21, 24–26, 31–33, 43, 48–50, 53, 54, 57, 60, 62, 63
UFS Universal Flash Storage. 11, 37, 63, 66
USB Universal Serial Bus. 10, 13, 23, 25, 35, 36, 40, 43, 44, 51, 55, 58, 62

1 INTRODUÇÃO

Nos últimos anos, a sociedade tem experimentado um acelerado processo de informatização, tornando-se cada vez mais interconectada. Com a evolução dos dispositivos móveis, grande parte da população vem substituindo o computador pelo *smartphone* para a execução da maioria das tarefas que usam tecnologia como ponto de partida, por exemplo, troca de mensagens, envio de correio eletronico, pagamentos *on-line*, etc. De acordo com o StatCounter[1] [4], os *smartphone*s correspondem a 51,69% dos dispositivos computacionais (*smartphone*s, tablets e computadores) em uso.

Em maio de 2019, somente no Brasil, os registros públicos apontaram para mais de 230 milhões de *smartphones* em uso. Se somarmos *Laptops* e *Tablets* a esse número, havia 324 milhões de dispositivos portáteis, ou seja, aproximadamente 1,6 dispositivos portáteis por habitante [5].

Os dispositivos móveis são utilizados para uma diversidade de tarefas, como enviar ou receber mensagens de texto, voz ou imagens, conversar por chamadas de voz ou vídeo, assistir vídeos, enviar ou receber *e-mails*, efetuar transações bancárias, realizar a captura e manipulação de imagens, uso de aplicativos para cuidados com a saúde, relacionamento, redes sociais, monitoramento de atividades físicas, mobilidade e trânsito e até mesmo, para armazenar exibir documentos digitais. No Brasil, podemos citar como exemplo algumas aplicações de serviços de interesse do cidadão, tais como o Título de Eleitor, o Certificado de Registro e Licenciamento de Veículos e Carteira Nacional de Habilitação.

Inúmeros fabricantes já produziam telefones celulares e os comercializavam globalmente antes do surgimento do Sistema Operacional (SO) Andorid. Após isso, passaram a investir no desenvolvimento de *hardware* para que seus dispositivos passassem a executar o novo SO. Surgiram também novos fabricantes, com foco no mercado global ou no mercado asiático, cujo público conumidor tem números bastante expressívos. A sul-coreana *Samsung* é a fabricante que detém a maior fatia do mercado global [6] de dispositivos móveis e que executam o SO Android, tornando-o o mais utilizado mundialmente [7].

Com os avanços tecnológicos, os fabricantes investem no aprimoramento de *hardware* e *software* dos dispositivos móveis. A cada novo dispositivo lançado, são empregados novos *System on a chip* (SoC), mais modernos, rápidos e energeticamente mais eficientes, maior capacidade de armazenamento e maior velocidade de acesso à memória, mais opções de

[1] Sitío de análise de tráfego da web criado em 1999, sediado em Dublin, Irlanda, que fornece ferramentas gratuitas de estatísticas on-line baseadas nos dados agregados coletados em uma amostra superior a 10 bilhões de visualizações de página por mês, coletadas em mais de 2 milhões de sites, atualizadas e disponibilizadas todos os dias.

conectividade e principalmente a capacidade de realizar multitarefas, o que os tornam a primeira opção de uso de inúmeros usuários. Além disso, novos mecanismos de proteção contra acesso indevido ou não autorizado também são implementados ou aprimorados frequentemente.

Dispositivos móveis modernos são uma fonte riquíssima de dados que podem constituir evidências forenses em processos de investigação e análise de segurança. Atualmente, dispositivos que executam o Sistema Operacional Android e suas variações são os mais acessíveis no mercado global. Isso os transformam em candidatos naturais em processos de análise e investigação forense devido a sua ampla abrangência.

Os arquivos armazenados em formato digital são considerados evidências digitais, incluindo os de áudio, vídeo e imagem, podendo ser ainda um *software* ou o próprio *hardware*. Ressalta-se que tais arquivos e dispositivos podem fazer parte da investigação da maioria dos crimes, sejam eles relacionados ao ambiente digital ou não e, portanto, devem ser adequadamente periciados e protegidos contra alteração, mantendo a proteção sob a cadeia de custódia.

No que se refere a parte de segurança e forense digital, os analistas se esforçam para adquirir e analisar dados de dispositivos móveis. A diversidade da tecnologia empregada em dispositivos móveis, o acúmulo de evidências digitais, a falta de metodologias padronizadas de extração e a falta de capacitação necessária caracterizam desafios que dificultam ou impedem a aquisição de dados [8].

As empresas que desenvolvem tecnologias para forense digital também são afetadas pela diversidade de componentes e fabricantes de dispositivos móveis, pois não podem ser eficazes e eficientes em todos os modelos ou em todos os fabricantes. As lacunas deixadas por essas empresas também constituem uma barreira para as forças de aplicação da lei.

Atualmente, figura como maior problema ou desafio a ser superado, o contorno ou eliminação do bloqueio de tela do dispositivo, pois tal mecanismo impede o acesso e aquisição dos dados contidos no dispositivo ou às configurações que permitam tais ações. Além do bloqueio de tela, há ainda a criptografia da memória principal do dispositivo, que também impede que dados adquiridos via chipp-off sejam decodificados. Ferramentas foresnses já consagradas no mercado tem se mostrado ineficazes quanto ao contorno ou quebra de tais mecanismos em inúmeros modelos existentes no mercado, sendo capazes de adquirir dados somente de deispositivos desbloqueados e ou ainda contornar tais mecanismos de apenas alguns modelos de dispositivos móveis.

A Forense em Dispositivos móveis é caracterizada por dificuldades no acesso aos dados do dispositivo, pelo esforço para desbloquear ou ignorar os mecanismos de segurança e obter dados e, muitas vezes, pela incapacidade de obter todo o volume de dados contidos no dispositivo. Também caracteriza-se pelo fato de ser mais complexa do que a forense com-

putacional tradicional, exigindo equipes mais bem treinadas e equipamentos especializados para obter resultados legalmente aceitáveis.

Diferentemente da computação forense tradicional, onde qualquer intervenção no sistema deve ser evitada a todo custo, na forense em dispositivos móveis, é necessário realizar o acesso e fazer intervenções diretamente no *hardware* para tentar contornar os mecanismos do bloqueio de acesso e também para instalar aplicativos de elevação de privilégio. No entanto, o uso correto das técnicas permite preservar a evidência e, consequentemente a legitimidade da evidência obtida.

A metodologia desenvolvida combina o emprego de *In-System Programming* (ISP) e uso de *Combination Firmware* para efetuar o contorno do bloqueio de tela. Após isso, seguem-se procedimentos específicos e mediante uso de ferramentas próprias para o trabalho de análise forense tanto em *hardware* quanto em *software*. A metodologia é aplicável a cerca de 70% dos dispositivos móveis com Sistema Operacional (SO) Android em uso atualmente.

Para efeito de validação, a metodologia foi aplicada em 4 (quatro) dispositivos, o que permitiu que fosse realizada a aquisição dos dados dos mesmos, com o uso do *Uiversal Forensic Extraction Device* (UFED) *Touch 2*, preservando a integridade dos dados, e, por fim, os dados adquiridos foram analisados no *UFED Physical Analyzer*. Vale ressaltar que a metodologia desenvolvida não se limita às ferramentas usadas. Isso significa que outras ferramentas, no mercado, podem executar as tarefas no processo de análise forense de dispositivos móveis.

No entanto, visando facilitar o entendimento do emprego da metodologia proposta no contexto das ciências forenses, são apresentadas a seguir as etapas gerais de uma possível metodologia forense para aplicação, especificamente, na forense de dispositivos móveis, conforme a Figura 1.1. Vale notar, com relação à análise forense de dispositivos móveis, que o cenário de obtenção de evidências também pode ser diferente, entretanto cada uma das etapas da metodologia observa e zela pela legalidade das ações, assim procedendo:

Figura 1.1 – Passos da metodologia forense.

1. *Identificação da evidência*: por tratar-se de um dispositivo móvel, sua identificação

pode ser mais difícil, pois o infrator poderá tentar entregar outro dispositivo no lugar daquele que realmente contém a evidência. Portanto, é essencial determinar o fato que precisa ser esclarecido e quais dispositivos devem ser analisados. É importante registrar todos os detalhes do local e dos itens apreendidos.

2. *Preservação de evidência*: o dispositivo a ser analisado sempre deve ser manuseado com luvas para que as impressões digitais do usuário do dispositivo sejam preservadas. Embora não faça parte da aquisição e análise de evidências digitais, essas evidências podem ser relevantes para outras ciências forenses. O dispositivo deve ser mantido, sempre que possível, no estado em que foi apreendido. Se for apreendido desligado, deverá permanecer desligado. Caso contrário, também é importante colocar o dispositivo no modo avião, para impedir que ele receba novas chamadas, *Short Message Service* (SMS), crie novos registros de itinerário pelo *Global Position System* (GPS), evitando falsos positivos durante o processo de análise, ou ainda que os dados possam ser apagados remotamente. Se isso não for possível, uma *faraday bag* deve ser utilizada para transportar o dispositivo até o laboratório onde os dados serão adquiridos. Todos os recursos do dispositivo devem ser documentados.

3. *Cadeia de custódia*: a cadeia de custódia, no contexto jurídico, refere-se ao registro cronológico ou histórico que registra a sequência de custódia, controle, transferência, análise e disposição das evidências, sejam físicas ou eletrônicas e é de fundamental importância em casos criminais.

4. *Método de aquisição da evidência*: o analista forense deve avaliar a melhor ferramenta ou metodologia para aquisição dos dados, preferencialmente iniciando pelos métodos menos invasivos, que podem ser usados de acordo com a necessidade .

5. *Pergunta investigativa*: a autoridade responsável por elucidar o caso deve formular as perguntas para as quais o analista forense deve buscar nas evidências, respostas que satisfaçam as perguntas da autoridade.

6. *Processo de análise*: esses são os processos, ferramentas ou metodologias através das quais as evidências adquiridas serão analisadas para responder às questões investigativas.

7. *Relatório conclusivo*: é o documento que inclui todos os registros feitos nas etapas anteriores e, principalmente, responde às perguntas investigativas feitas pela autoridade competente.

1.1 PRINCIPAIS CONTRIBUIÇÕES

Em artigo publicado no *Journal Applied Sciences* [9], vinculado à presente dissertação, uma síntese da metodologia proposta é apresentada com um estudo de caso considerado o de maior impacto do estudo de validação realizado, tendo em vista o número de dispositivos comercializados. No presente texto, o conteúdo de artigo publicado é extendido para dar maior detalhamento das informações. No que se refere às contribuições da solução proposta, podemos citar como principais as seguintes:

- Possibilitar o contorno do bloqueio de tela, em dispositivos com SO até a versão 9 (Pie);
- Comprovar a eficácia da metodologia LLDA-ISPCF em dispositivos com *File-Based Encryption* (FBE);
- Possibilitar a aquisição de dados de uma vasta gama de dispositivos móveis, independente do fabricante;
- Permitir a aquisição dos dados do dispositivo com o uso de ferramentas especializadas, proprietárias e *open sourse* preservando a integridade dos dados;
- Permitir que seja habilitado o usuário *root* sem o risco da perda dos dados do usuário, o que permite a extração física em modelos cujo processo de aquisição somente é possível com o dispositivo rooteado;
- Permitir a aquisição e análise dos dados por qualquer ferramenta forense com capacidade para tal, observando a compatibilidade da ferramenta de análise com o formato gerado pela ferramenta de aquisição.;

1.2 OBJETIVO DO TRABALHO

Tornou-se comum encontrar relatórios públicos que mostram que o uso dos *smartphones* na prática de atos ilícitos vem aumentando. Cada vez mais, estes dispositivos são usados como meio para prática de atividades criminosas e se tornam evidências digitais relevantes para investigações criminais. Devido a uma participação mais significativa no mercado, a aquisição e análise forense dos dados de dispositivos Android ganhou significativa importância no campo da investigação forense digital [10].

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é desenvolver uma nova metodologia que permita a aquisição de dados de dispositivos móveis com SO Android até a versão 9 e que estejam com mecanismo de bloqueio de tela ativado.

1.2.2 Objetivos Específicos

A metodologia denominada *Low-Level Data Acquisition with In-System Programming and Combination Firmware* (LLDA-ISPCF) tem como objetivos específicos combinar o emprego de *In-System Programming* (ISP) e de *Combination Firmware*, além de outras ferramentas para manutenção de dispositivos móveis de modo que possam ser utilizadas como ferramentas forenses ou como complemento para outras ferramentas na aplicação de técnicas forenses para o contorno ou remoção de bloqueio de tela e criptografia da memória principal de dispositivos móveis com SO Android até a versão 9, e após seu emprego, e assim, proporcionar o uso das funcionalildades de aquisição e análie das ferramentas forenses, uma vez que sem o emprego da metodologia, tais funcionalidades são ineficazes, pois necessitam que a maioria dos aparelhos esteja desbloqueado para que a aquisição seja possível.

Embora muitas ferramentas forenses já possuem essa capacidade para alguns modelos de dispositivo, as mesmas não são capazes de contornar tal mecanismo de um número muito grande de modelos de fiferentes fabricantes, realizar a aquisição quando estes dispositivos apresentam um mecanismo de bloqueio de acesso (senha de tela). O emprego da metodologia proposta possibilita o contorno de tal mecanismo, além do mecanismo de criptografia implementado para proteger os dados armazenados na memória principal, aplicável em dispositivos com SO Android até a versão 9, garantindo assim que as aquisições forenses possam ser realizadas e empregadas para os fins determinados pelas autoridades.

1.3 ESTRUTURA E ORGANIZAÇÃO DO TRABALHO

O restante do trabalho está organizado da seguinte maneira: A Seção 2 apresenta alguns conceitos básicos importantes para a compreensão da metodologia proposta, como a revisão do estado da arte e alguns trabalhos correlatos. A Seção 3 apresenta a descrição do problema, a proposta de solução, a nova metodologia criada e suas respectivas fases. A Seção 4 mostra uma prova de conceito e os resultados da metodologia proposta. Por fim, a Seção 5, traz algumas conclusões sobre a metodologia e trabalhos futuros.

2 REVISÃO BIBLIOGRÁFICA E TRABALHOS RELACIONADOS

Esta seção apresenta as diferentes técnicas de aquisição padrão, ciclo de vida forense, algumas ferramentas e softwares para reparo de smarthones, um breve descritivo sobre *In-System Programming* (ISP), Swap Físico e Lógico, *Combination Firmware*, criptografia dos dados aplicadas ao contexto forense, bootloader em smartphones com SO Android. Além disso, revisa os principais trabalhos relacionados, bem como as limitações desses trabalhos e o principal diferencial da nossa proposta.

2.1 PROCESSOS DE AQUISIÇÃO DE DADOS

O termo *processo de aquisição* é usado para designar o ato de realizar a cópia do conteúdo do dispositivo de origem (fonte) para um dispositivo de destino (alvo). Como já dito anteriormente, a aquisição de dados de dispositivos móveis se difere da aplicada à computação forense tradicional, pois nesta última, qualquer intervenção no sistema deve ser evitada, já na forense em dispositivos móveis, o acesso e intervenções diretamente no hardware são necessárias. No entanto, o uso correto das técnicas e o emprego de ferramentas adequadas garantem a preservação da evidência e, consequentemente sua legitimidade.

2.1.1 Aquisição Física

A aquisição física em dispositivos móveis consiste em copiar informações do dispositivo por acesso direto a memória de armazenamento interno. O processo cria uma cópia *bit a bit* do sistema de arquivos inteiro. Tal abordagem é semelhante a adotada em investigações forenses realizadas em computadores. Uma aquisição física é capaz de adquirir todos os dados presentes em um dispositivo de armazenamento, incluindo os dados excluídos que ainda não foram sobrescritos, além de copiar o espaço não alocado [11]. É considerada como a mais efetiva em termos forenses e é realizada mediante o uso de ferramentas específicas.

De acordo com Mota Filho [12], a menor quantidade de informações que um SO consegue ler em um sistema de arquivos é um bloco que, em nível físico de disco, equivale a um *cluster*. As cópias e leituras são feitas bloco a bloco no nivel de filesystem. Os Sistemas de Arquivo usados em larga escala pelos dispositivos Android foram o Flash-Friendly File System (F2FS), e atualmente o Fourth Extended Filesystem (EXT4). Ambos os sistemas de

arquivos adotam blocos lógicos com tamanho de 4KB. Ainda segundo Mota Filho [12], existem softwares como o *dd* e o *dc3dd* que conseguem ler um setor físico, que possui 512 bytes por padrão, e é a menor unidade de informação que se pode ler em um HD ou dispositivo de armazenamento em massa pela sua controladora.

2.1.2 Aquisição do Sistema de Arquivos

A aquisição do sistema de arquivos é tecnicamente vista como um tipo de aquisição lógica [11]. No entanto, é mais abundante em dados, pois todo o sistema de arquivos do dispositivo é copiado. Ela contém os arquivos e diretórios que o dispositivo usa para preencher aplicativos, configurações do sistema e configurações do usuário, juntamente com as áreas de armazenamento do usuário. Ainda inclui arquivos não acessíveis diretamente ao usuário através da interface do dispositivo, o que requer ferramentas especializadas para acessar tais artefatos. Porém, diferentemente da aquisição física, este tipo de aquisição não copia o espaço não alocado da memória física.

2.1.3 Aquisição Lógica

A aquisição lógica é uma cópia dos objetos de armazenamento lógico, como sistema de arquivos, diretórios e arquivos. São copiados os dados dos espaços alocados em disco, ainda acessíveis ao usuário no sistema de arquivos. Tais dados incluem a agenda telefônica, as chamadas, as mensagens, alguns dados de aplicativos e outros dados que se pode esperar de um backup do softwares com o iTunes ou o próprio Android, ou seja, o que você pode ver se examinar manualmente o dispositivo [13]. É vista como a mais rápida e menos invasiva, porém é a mais limitada das aquisições.

2.1.4 Comparação dos processos de aquisição

A Figura 2.1 apresenta os diferentes dados que podem ser adquiridos pelos diferentes tipos de aquisições apresentadas.

Figura 2.1 – Resumo dos tipos de dados em cada tipo de aquisição.

2.2 CICLO DE VIDA DA FORENSE DIGITAL

Ajijola et al. [14] apresentaram uma avaliação comparativa das diretrizes forenses do NIST SP 800-101 Rev.1: (Guidelines on Mobile Device Forensics) [15] e International Organization for Standardization (ISO)/IEC 27037: 2012 (Guidelines for identification, collection, acquisition and preservation of digital evidence) [16]. O estudo resultou na proposta de uma implementação integrada das duas diretrizes forenses.

Considerando os padrões mencionados, nenhum deles trata de todos os processos de investigações forenses digitais. Existem diretrizes forenses comuns aos dois padrões, e outras que apenas um dos padrões contempla, expondo suas limitações que atingem questões mais autais de processos forenses. De acordo com Neumer e Weippl [17], outra diretriz que pode ser aplicada em conjunto é a RFC 3227 (Guidelines for Evidence Collection and Archiving) [18], que também fornece diretrizes para boas práticas de forense digital.

A Figura 2.2 representa o ciclo de vida típico ou as principais etapas da forense digital.

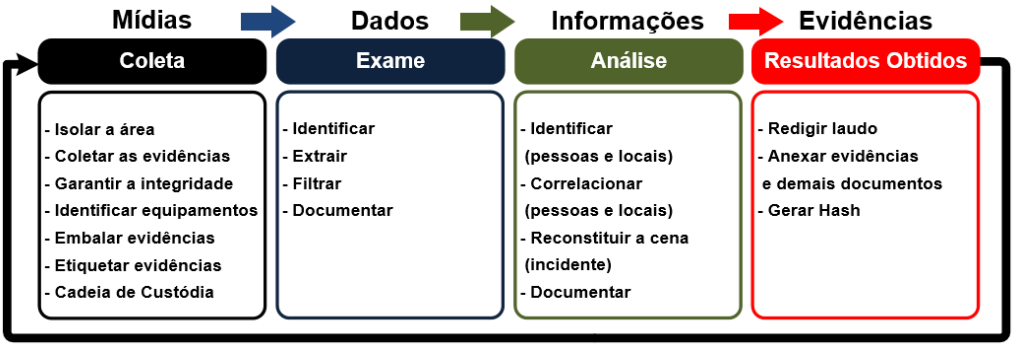

Figura 2.2 – Ciclo de vida da Forense digital.[Fonte: Adaptado de [1]]

2.3 FERRAMENTAS E SOFTWARES PARA REPARO DE SMARTHONES

Segundo Yang et al. [19], empresas que prestam serviço de assistência técnica ou que realizam reparos em dispositivos móveis, utilizam ferramentas conhecidos como *Box* (Figura 2.4). São interfaces dotadas de funcionalidades que possibilitam a execução de leitura e escrita em áreas da memória de armazenamento interno dos dispositivos móveis que não são acessíveis para o usuário e também podem ser utilizadas como ferramentas forenses.

Dentre os diversos modelos utilizados, podemos citar a Octoplus Pro [20], UFI [21] e Easy JTAG Pro [22] e seus respectivos softwares. Embora essas Box tenham recuros para execução de ISP, JATG e Chip-Off, raramente são empregadas para esse fim. Elas são amplamente empregadas para reparos de software e hardware de dispositívos móveis, tendo

em vista que o foco das empresas que prestam serviços de assistência técnica é devolver ao usuário um dispositivo em perfeito funcionamento, sem se preocupar com os dados do contidos no mesmo.

Existem outras ferramentas e softwares usados para reparos, tanto físicos quanto lógicos, em dispositivos móveis. Para reparos a nível de software, podemos citar as interfaces conhecidas como Dongles, que consistem de uma interface USB que serve para ler um smartcard e validar a licença do software. Para reparos físicos, são empregadas as mesmas ferramentas necessárias na preparação do dispositivo para a execução de ISP, JATG e Chip-Off. As técnicas forenses de Chip-Off e ISP usam Soldering Station, Surface-Mount Device (SMD) Rework, pinças antiestáticas, manta antiestática, estanho para solda, fluxo de solda, microscópio estereoscópico, microscópio eletrônico, suportes para placas e memórias de dispositivos móveis, sondas e espátulas, micro retífica, multímetro digital de alta precisão, LCD Disassembly Machine, entre outros.

A Figura 2.3 ilustra um dos modelos de Dongles disponíveis no mercado para reparo de software de dispositivos móveis.

Figura 2.3 – EFT Dongle.

2.3.1 In-System Programming

In-System Programming (ISP) é uma técnica que pode ser empregada para aquisição de dados para análise forense de dispositivos móveis. No entanto, neste trabalho será abordado o udo de ISP não apenas como ferramenta para leitura de dados da memória principal, mas também como ferramenta de escrita de dados, o que nos permite alterar partições da memória principal do dispositivo, algo que ainda - no melhor do conhecimento do autor e até a elaboração deste trabalho - não foi explorado. Seu uso não será como ferramenta principal, mas como componente de uma metodologia que combina o uso de outras ferramentas para a aquisição bem-sucedida de dados.

Segundo Afonin e Katalov [23], a análise forense que emprega a técinca ISP é uma variação menos invasiva ou destrutiva que a técnica de *Chip-Off*. A técnica ISP envolve um processo avançado de aquisição, entre o *Joint Test Action Group* (JATG) e o *Chip-Off*.

De acordo com Pappas [11], ISP é uma técnica de aquisição semelhante ao JATG, porém mais rápida, cuja principal diferença é que no ISP, a conexão é feita diretamente à memória flash, ignorando o processador, por meio dos *Test Acess Point* (TAP), e pode ser usado quando o dispositivo não é compatível com JATG. A aquisição via ISP se aplica a qual-

quer memória flash eMMC ou eMCP, não limitando-se apenas a smartphones, podendo ser empregada em qualquer dispositivo que utilize esses tipos de memórias, como exemplo, os cartões SD.

No ISP, é necessário conhecer os TAPs que se conectam à memória flash. É necessário o uso da *Box* para fazer a conexão do computador onde será executado o software com a placa do dispositivo. Existem no mercado vários modelos de *Box* com capacidade de executar ISP, sendo as mais conhecidas a Easy JTAG Plus e a Z3X Pro. A Figura 2.4, mostra uma *Box* Easy JATG Plus.

Figura 2.4 – Easy JTAG Plus.

Para a técnica forense ISP, durante o processo de aquisição, o conteúdo da memória interna é copiado sem se remover o chip. O emprego desta técnica depende do acesso aos TAPs necessários. Em muitos dispositivos, por questões de projeto, o fabricante opta por não deixar o TAP na camada mais externa da placa, ou seja, embora exista, está em uma das camadas internas. A técnica de aquisição usando ISP é mais comum em dispositivos que utilizam memórias flash do tipo Embedded Multimedia Card (eMMC) ou Embedded Multi-Chip Package (eMCP) de encapsulamento tipo Ball Grid Array (BGA). Não foram encontrados registros sobre ISP em dispositivos que utilizam memória do tipo UFS, mesmo exintindo leitor para Chip-Off para este tipo de memória.

Com maiores detalhes, a execução do ISP é um processo que requer vários passos. Primeiro, deve-se conectar os TAPs de acesso à memória flash a um adaptador. Segundo solda-se uma das extremidades de um condutor metálico no TAP e a outra extremidade no adpatador. Terceiro, se conecta os TAPs à *Box*.

O Software da *Box* disponibiliza o diagrama dos TAPs da maioria dos Smartphones. Também existem sites especializados que disponibililzam tais imagens. A Figura 2.5 exemplifica as soldas no adaptador e nos TAPs da placa.

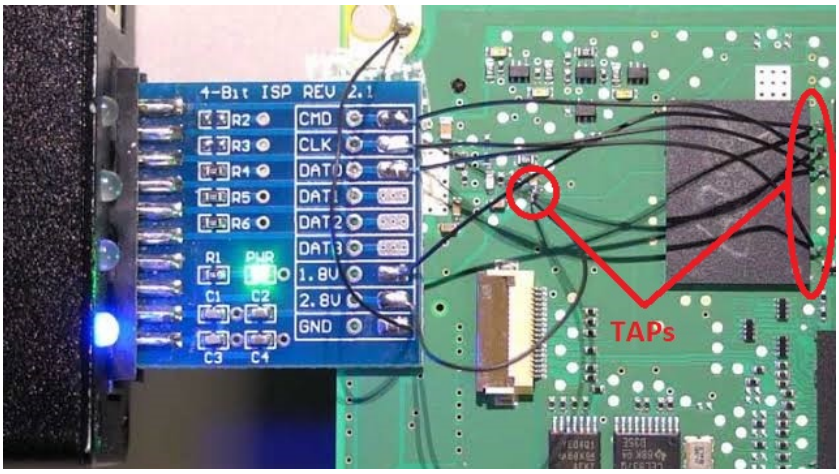

Figura 2.5 – Placa pronta para execução de ISP.

O uso da técnica ISP permite que outro analista reproduza ou repita todas as etapas do processo para aquisição de dados, pois o dispositivo permanece funcional e com todos os componentes na placa. No entanto, mesmo quando a técnica Chip-Off é aplicada, é possível retornar o componente ao seu local original executando o processo de resolda da memória principal, conhecido como *reballing*, fazendo com que o dispositivo volte a funcionar normalmente.

É possivel ainda fazer uso de uma interface chamada VR-TABLE, que possui braços articulados, dotados de sondas metálicas de alta precisão, que dispensam a solda dos condutores na placa do dispositivo móvel, eliminando a possibilidade de danos causados pelo superaquecimento. A Figura 2.6 demonstra o uso de uma VR-Table.

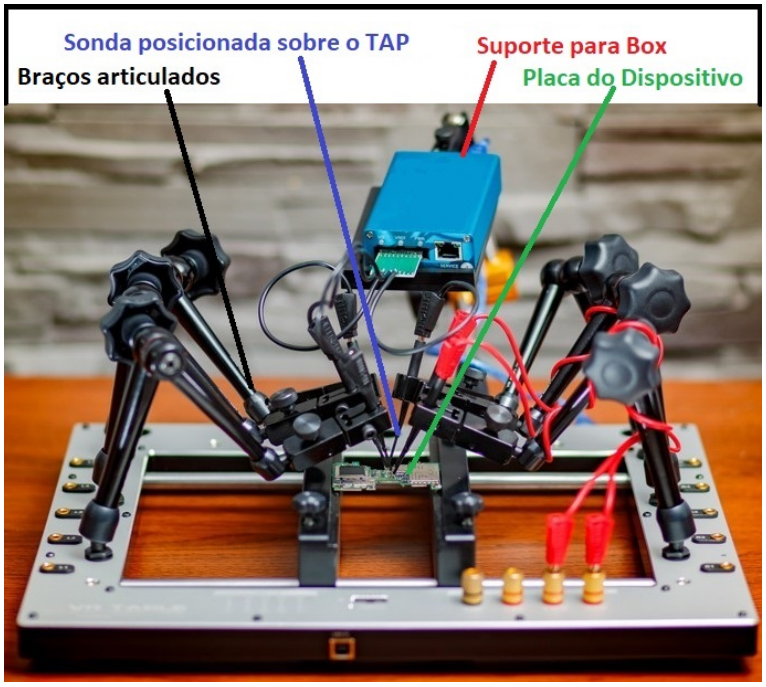

Figura 2.6 – VR-Table. [Fonte: Adaptado de [2]]

Os softwares da *Box* são capazes de realizar operações de leitura/escrita diretamente na memória principal do dispositivo. Após efetuar a solda de todos os condutores necessários, a *Box* é conectada ao computador por meio de um cabo USB. Concluida essa etapa, é necessário selecionar o software correto a ser utilizado e configurar os parâmetros necessários. Quando tudo estiver conectado, o software com os parâmetros corretamente configurados, a conexão entre a *Box* e a memória pode então ser estabelecida e o conteúdo da mesma pode ser acessado ou manipulado.

No ISP, é possível manipular os dados usando larguras de banda de 1 ou 4 bits. O mais comum, é a utilização do valor "1 bit", pelo fato de ser menos suscetível a erros durante a cópia, e por reduzir a exposição da placa ao calor, já que para a execução com largura de banda de "4 bit" é necessário soldar 3 condutores a mais.

Na Tabela 2.1, estão descritos os TAPs que obrigatóriamente devem ser conectados para a execução do ISP.

Tabela 2.1 – Funções dos TAPs no ISP. [Fonte: Adaptado de [3]]

ISP Pinout	
TAP	Function
CMD	Command in/Response out
DAT0	Data input/output
CLK	Clock
VCC	Supply voltage for Core (2.8/3.3V)
VCCQ	Supply voltage for I/O (1.8/3.3V)
GND	Ground

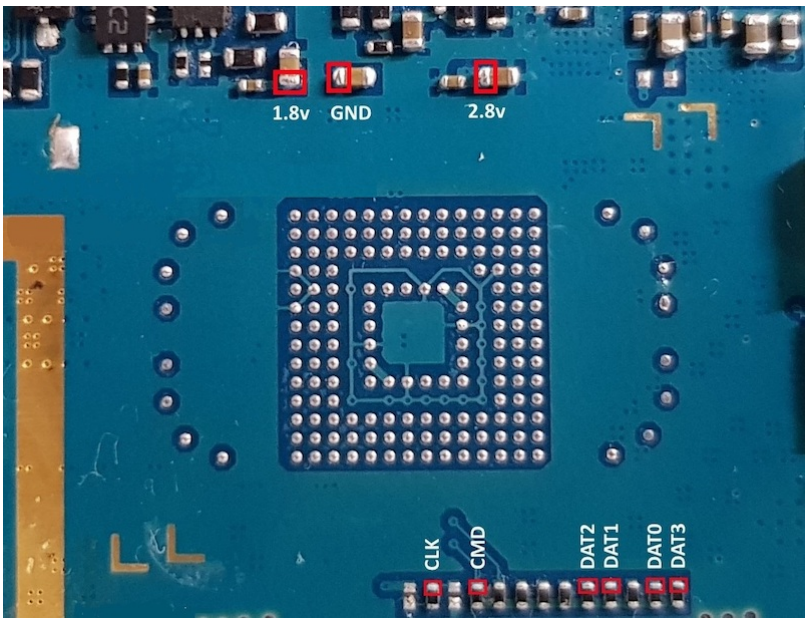

Figura 2.7 – Pinout Samsung GT-N8000.

Na Figura 2.7, estão identificados os TAPs da placa de um dispositivo móvel Samsung modelo GT-N8000. Neste exemplo, DAT1, DAT2 e DAT3, que possibilitam a execução de ISP com largura de banda de 4 bit, também estão identificados. A taxa de transferência pode variar de 1.2 a 1.8 Kbps, de acordo com a frequência selecionada. Se a largura de banda for de 4 bit, multiplica-se a taxa de transferência por 4.

Também é possível criar uma imagem binária da memória principal do dispositivo utilizando o software da *Box*. Esta imagem pode ser analisada por ferramentas forenses como o UFED [24], XRY [25] ou AXIOM [26].

O processo de preparação do dispositivo móvel para a execução de ISP também propicia a aquisição física em dispositivos equipados com SoCs produzidos pela Qualcomm. Usando o Emergency Download Mode (EDL), método proposto por Wu et al [10], é necessário soldar um condutor no TAP **CMD** do dispositivo para realizar a Aquisição Física. Em dispositivos de alguns fabricantes, a exemplo da XIAOMI, há também a possibilidade de fazer com que se entre em modo EDL de maneira lógica, digitando um código no teclado do aplicativo de chamadas. No caso dos dispositivos da XIAOMI o código é ***#*#717717#*#***.

2.3.2 Swap Lógico e Swap Físico

O Swap lógico consiste em realizar uma copia forense de todo o conteúdo da memória principal de um dispositivo danificado via ISP, se possível, via Chip-Off e posteriormente gravar o conteúdo na memória principal de um dispositivo exatamente do mesmo modelo, que está funcionando normalmente. Assim, todo o conteúdo do dispositivo danificado, passará a ser executado no disposivitvo saudável, preservando o sistema de arquivos, critpografia e mecanismos de bloqueio.

O Swap físico consiste em remover o SoC e a memória principal da placa de um dispositivo danificado, remover os mesmos componentes da placa de um dispositivo funcional exatamente do mesmo modelo, que será o receptor, e posteriormente efetuar o *reballing* (ressoldagem) na placa deste.

Ambos os procedimentos podem ser usados na fase que antecede o emprego da metodologia proposta, servindo como modo de reparo para permitir a aquisição de dados em dispositivos danificados.

Para a leitura e escrita dos dados da memória principal, pode ser utilizada a Box Easy JTAG Plus.

2.3.3 Combination Firmware

Um Firmware de Engenharia ou Firmware de Serviço Especial é um firmware desenvolvido para realizar a leitura do hardware do dispositivo, exibindo informações completas, além de permitir testes de hardware e execução de aplicativos e funcionalidades básicas do dispositivo. É possível obter o firmware especial para dispositivos de vários fabricantes, no entanto, eles são encontrados com diferentes nomenclaturas. Para dispositivos Xiaomi, eles são conhecidos como *ENG Firmware* ou *Engineering Rom* e para dispositivos Samsung, embora eles tenham a mesma funcionalidade, são conhecidos como *Combination Firmware*. É importante esclarecer que o uso mais comum desses Firmwares é a manutenção de dispositivos móveis.

De acordo com Morgillo e Viola [27], a Read Only-Memory (ROM), é um tipo de memória geralmente usada em sistemas embarcados para armazenar com segurança todos os arquivos que fazem parte do núcleo sistema. O Firmware que executa o sistema operacional Android nos dispositivos móveis, é armazenado em uma área da memória cuja permisão é "Somente Leitura", e por isso esse firmware é popularmente conhecido como ROM. Existe um esforço por parte dos fabricantes para garantir a maior integridade possível do sistema, fazendo com que o sistema principal permaneça intacto durante a reinicialização do dispositivo e seja tolerante a falhas. No entanto, com uso de ferramentas específicas, é possível manipular essa área da memoria interna e instalar um firmware personalizado.

Considera-se que tal personalização é possível pelo fato de que o Android é um dos projetos de código aberto mais populares e, de modo geral, as *ROMs customizadas* que corrigem erros específicos para cenários específicos são versões otimizadas do sistema original. Neste último caso, sobrescrevem todas as áreas da memória interna quando substituem o firmware original.

Segundo Parry e Carter [28], a atualização do firmware de dispositivos móveis pode ser realizada por uma conexão sem fio, conhecida como Over-the-air (OTA). A Open Mobile Alliance (OMA) desenvolveu técnicas para atualização de firmware que podem exigir dezenas, centenas ou até milhares de arquivos, e algumas soluções agrupam todos os arquivos de atualização necessários em um único arquivo para serem baixados diretamente no dispositivo móvel. A substituição do firmware original por outro, desenvolvido por terceiros, necessita de ferramenta específica e é feito por meio de um computador.

Para a instalação de um *Combination Firmware* é necessário a utilização de software específico, que realiza a reescrita do firmware. Uma vez substituido o firmware original do dispositivo pelo Combination Firmware, é possível verificar todos os recursos de hardware, como câmera traseira, câmera frontal, sensores, memória RAM, memória ROM, além de executar um teste que mostra os resultados do diagnóstico do telefone.

Engenheiros e técnicos utilizam amplamente os Firmwares Especiais e, embora não

exista documentação oficial sobre os mesmos, há muitos tópicos em fóruns especiaizados, como o *XDA Developers* [29] sobre seu emprego. Os arquivos podem ser baixados de sites especializados em ferramentas para manutenção de dispositivos móveis.

Do ponto de vista forense, outros recursos interessantes podem ser exploradas com o uso de Firmwares Especiais. Com ele é possível ignorar e remover a proteção de redefinição de fábrica ou a verificação ou a proteção da conta do Google. Contudo, o principal ponto de interesse é permitir acesso total ao conteúdo do dispositivo, uma vez que a substituição do firmware original pelo Firmware Especial não altera a partição de dados do usuário, preservando a integridade dos mesmos e permitindo que sejam feitas aquisições físicas, aquisições do sistema de arquivos e aquisições lógicas com o uso de ferramentas forenses. Também é possível habilitar o usuário root caso seja necessário. Segundo Almehmadi e Batarfi [30] - que investigaram o impacto na integridade dos dados do usuário ao habilitar o usuário *root* em um smartphone Android - as modificações nos dados do dispositivo não afetam os dados do usuário e concluíram que tal processo é, portanto, legalmente válido e que as evidências extraídas dos dispositivos Android como resultado do processo de rooteamento é uma evidência robusta e confiável para sentença em casos criminais.

Ressalta-se que um os Firmwares Especiais, como o Combination Firmware utilizados em dispositivos Samsung, não são destinado ao usuário final, e sim para as tarefas especializadas de acordo com a necessidade. Utilizar tais técnicas sem o devido conhecimento pode invalidar as provas provenientes de dados adquiridos de um dispositvo, quando tratamos de um processo de investigação criminal, eliminando evidências substanciais para apuração de crimes. É necessário ainda observar que o Combination Firmware sempre executa a mesma versão do Android do firmware original. É importante frisar que o Firmware Especial de que trata este trabalho, é diferente do Generic System Image (GSI), uma imagem genérica do sistema que é uma implementação de Android puro com código do Android Open Source Project (AOSP) não modificado e pode ser executada em vários dispositivos Android ou ainda de firmwares disponibilizados pelo projeto LineageOS.

Quando não há firmware especial para o dispositivo de destino, é possível fazer o download da imagem das partições *boot*, *Recovery* e *System*, também desenvolvido para reparar dispositivos móveis, e fazer adaptações para que sejam semelhantes às encontradas no firmware especial. No entanto, isso requer análise individual para cada dispositivo. Este procedimento não será descrito neste artigo.

2.4 USO DE CRIPTOGRAFIA NO ANDROID

Segundo Loftus e Baumann [31], a Google disponibilizou desde a versão 3.0 (Honeycomb) do Aindroid, o modelo de criptografia Full-Disk encryption (FDE), que permite crip-

tografar a partição */data*, também chamada de "user data".

Depois de ligar o dispositivo, todos os dados na partição */data* ficam inacessíveis até que o usuário forneça as credenciais para autenticação. Mesmo usando tais avanços, isso não impediu que ataques como *Evil Maid Attack* e o *Cold Boot* obtivessem êxito contra a FDE. Numa perspectiva de segurança e forense, há ainda outros inconvenientes decorrentes do uso do FDE. Por exemplo, após a reinicialização, várias funções críticas do dispositivo não podem ser usadas sem a interação do usuário. Cofdeexemplo, podemos citar a impossibilidade de pode receber chamadas após uma reinicialização inesperada.

Ainda de acordo com Loftus e Baumann [31], a File-Based Encryption (FBE) foi introduzida para superar esse problema como parte do lançamento do Android 7.0 (Nougat). A FBE protege os dados do usuário, criptografando cada arquivo com uma chave exclusiva. Essa chave é composta com base na combinação de uma chave de hardware com a entrada do usuário (senha alfanumérica, PIN, etc.), associada a proteção da Inicialização Segura (Direct Boot). Mesmo assim tem a comodidade de não sofrer limitações, corrigindo a falha mencionada do FDE, além de permitir um controle mais refinado do que é cifrado.

O Direct Boot pode ser definido durante a configuração inicial e enquanto se especifica a senha da tela de bloqueio. Quando a opção de inicialização segura está ativada, e o usuário informa sua chave de acesso, durante a inicialização, a partição de dados é montada e decifrada e alguns aplicativos podem iniciar e acessar seus dados, mesmo que não ocorra o desbloqueio da tela. A solicitação da chave ocorre antes que a maioria dos serviços e aplicativos do Android tenha permissão para iniciar. A credencial é necessária para gerar a chave de criptografia real.

Alguns casos de apps que são executados no modo de inicialização segura incluem Apps com notificações programadas, como apps de despertador, apps de SMS e apps que fornecem serviços de acessibilidade, como o Talkback. De acordo com Alendal [32], esse mecanismo de segurança pode ser contornado.

Nos dispositivos fabricados pela Samsung, a criptografia do tipo FBE está presente apenas em dispositivos Samsung Galaxy enviados com Android 9.0 ou superior, com Knox 3.3 ou superior. Nos demais, a criptografia ainda é do tipo FDE [33].

Segundo Ribunov et al.[34], a coexistência de aplicativos críticos e não críticos está se tornando comum em dispositivos móveis. Os aplicativos críticos devem ser executados isoladamente em Trusted Execution Environment (TEE), para que o código e os dados associados possam ser protegidos contra aplicativos mal intencionados.

De acordo com Leignac et al.[35] o TEE foi criado para melhorar a segurança dentro do SoC com base na arquitetura ARM. Ele oferece um compromisso entre a funcionalidade do Rich Operating System (Rich OS), a exemplo do Android, e a segurança de um Secure Element (SE). O ARM TrustZone separa o SoC entre dois ambientes, considerado seguro e

outro não tão seguro.

As chaves são derivadas das informações armazenadas no TEE, bem como as credenciais do usuário (PIN, senha, etc.) usados para desbloquear o telefone. Se a Criptografia baseada em arquivo for empregada, o telefone poderá inicializar e acessar os dados armazenados na área cifrada específica do dispositivo, protegida com chaves de hardware. A maioria das informações, no entanto, é armazenada na area cifrada com as diversas credenciais. Essa área é protegida com chaves basedas nas credenciais do usuário.

Deste modo, uma aquisição feita por meio do software de uma Box, seja por ISP ou Chip-Off, não trará resultados satisfatórios, pois o dispositivo está desligado, e consequentemente, cifrado.

2.5 BOOTLOADER

De acordo com Hay [36], existe uma cadeia de gerenciadores de inicialização que se originam do Original Equipment Manufacturer (OEM) ou do fabricante do SoC. O carregador de inicialização primário *(Primary Bootloader - (PBL)*, que é escrito pelo fabricante do chipset, que aciona o Bootloader (ABOOT). Ainda se tem o TrustZone, que fornece mecanismos de segurança como o Secure Boot.

Os dispositivos Android vem de fábrica com o bootloader bloquedo para garantir a integridade do SO. Para desbloquear o bootloder, o que permite a instalação de um bootloader alternativo e a instalação de um firmware personalizado, alguns dispositivos requerem um código de autorização pelo fabricante. Em alguns dispositivos ocorre a redefinição de fábrica, isto é, os dados do usuário serão perdidos, o que não é interessante do ponto de vista forense.

2.5.1 Android Verified Boot

De acordo com Weiss [37], o Android Verified Boot (AVB) é um recurso de segurança implementado nas versões 8.0 do SO Android e superiores. Seu principal objetivo é garantir que todo o código executado venha de uma fonte confiável, e não de atacante que tenha adulterado arquivos do dispositivo. O mecanismo usa um modelo de cadeia de confiança, a partir do gerenciador de inicialização (bootloader), passando para a partição de inicialização (boot) e outras partições verificadas, como a *System*, *Vendor* e *OEM*. Quando o dispositivo é iniciado, cada estágio verifica criptograficamente a integridade e autenticidade da próxima etapa antes de prosseguir, assegurando que é autêntico e não possui falhas de segurança conhecidas.

O suporte à inicialização verificada foi adicionado na versão 4.4 do Android. Na versão Android 7.0 do SO Android, foi implementada a função que garante que dispositivos comprometidos não inicializem . No entamto, o AVB funciona com a arquitetura do Project Treble, que separa a estrutura do Android da implementação do fabricante, podendo este implementar ou não, ou ainda elencar apenas determinados modelos de dispositivos para implementação. É integrado ao Android Build System e ativado por uma única linha, que cuida da geração e assinatura de todos os metadados necessários do *dm-verity*.

o AVB é implementado dentro do *libavb*, uma biblioteca C para ser usada no momento da inicialização para verificar o Android, e que pode ser usada tanto dentro dos programas do espaço do usuário (avbctl do Android) quanto pelo espaço do kernel (carregador de inicialização). O coração do sistema é o *VBMeta struct*, que contém os hashs de verificação do conteúdo de várias partições importantes, como boot, recovery, dtbo, vendor e system e a chave pública usada para assiná-las criptograficamente. A chave pública deve ser verificada pelo gerenciador de inicialização incorporada a ele, para que as partições citadas sejam consideradas confiáveis. É possível integrar o *libavb* ao bootloader implementando uma funcionalidade específica da plataforma para E/S (I/O), fornecendo o Root of Trust (RoT) e obtendo ou configurando metadados de proteção de reversão [38].

Para entender o AVB, o conceito de estado do dispositivo deve ser definido. O estado indica se o software do dispositivo pode ser atualizado. Os dispositivos bloqueados seguem as etapas de verificação de inicialização. Dispositivos com bootloader desbloqueado não realizam tais verificações. O bootloader pode ser bloqueado ou desbloqueado usando o fastboot.

Root of Trust RoT é a chave criptográfica usada para assinar a versão do Android no dispositivo. Dispositivos com vários gerenciadores de inicialização podem ter várias chaves para verificar. Os usuários podem definir sua própria RoT para alguns dispositivos. Isso permite que versões personalizadas do Android sejam usados sem perder os benefícios de segurança do AVB.

O AVB verifica criptograficamente o código executável antes de ser executado, incluindo o kernel, a árvore de dispositivos e as partições do Systeme Vendor. Pequenas Partições, como boot (kernel) e dtbo (árvore de dispositivos) são verificadas usando hash. Toda a partição é carregada na memória, o hash é calculado e comparado com o valor conhecido, e se o hash não corresponder, o SO não será carregado.

Partições maiores que não podem ser carregadas na memória (por exemplo, sistemas de arquivos) precisam usar um árvore de hash em que a verificação acontece continuamente à medida que os dados são carregados na memória. A raiz hash é comparada a um valor já conhecido. Se os valores não corresponderem, o SO entra em estado de erro. Os hashes conhecidos são armazenados no início ou no final de cada partição verificada ou em um partição dedicada, dependendo da implementação. Esses hashes devem ser assinados pelo

RoT para garantir a integridade.

O AVB também verifica a versão correta do android, como proteção contra reversão. A proteção contra reversão funciona usando o tamper-evident storage (armazenamento inviolável) para gravar a versão atual do Android. Quando o sistema é inicializado, a versão é verificada para garantir que não seja menor que a versão gravada. Se for, o dispositivo se recusará a inicializar. Isso evita que invasores instalem uma versão mais antiga do Android com vulnerabilidades para depois explorá-las, comprometendo o sistema.

2.5.2 VBMeta struct

O completo entendimento da estrutura e funcionamento do VBMeta, em todos os seus detalhes, não é o objetivo principal deste trabalho. No entanto, para que se tenha condições de entender uma das etapas da metodologia, se faz necessária uma breve explicação sobre tal partição.

De acordo com Elenkov [39], a estrutura de dados central usada no AVB é a estrutura do *vbmeta*. Essa estrutura de dados contém descritores e outros metadados, todos assinados criptograficamente. Os descritores são usados para hashes de imagem, metadados de hashtree de imagem e para as partições encadeadas.

Na partição *vbmeta* está o hash da partição *boot* em um descritor de hash. Para as partições *system* e *vendor*, um hashtree dos dados da sistema de arquivos e a partição vbmeta mantém o root hash, salt e o deslocamento do hashtree nos descritores. O VBMeta struct na partição vbmeta é assinado criptograficamente, o carregador de inicialização pode verificar a assinatura e verificar que foi feito pelo proprietário key0 (por exemplo incorporando a parte pública key0) e, assim, confiar os hashes utilizados para nas partições *boot*, *system* e *vendor*.

A estrutura vbmeta é descrita em *libavb/avb_vbmeta_image.h*. Ela contém cabeçalho, dados de autenticação (referência à chave pública) e referências a descritores para várias partições.

Para desabilitar o AVB é necessário setar os seguintes sinalizadores na partição *vbmeta*: - *-disable-veritye* e - *-disable-verification*.

Quando o dispositivo está bloqueado, o carregador de inicialização carrega o VBMeta struct da partição vbmeta e chama *avb_slot_verify()* para cada partição mencionada dentro do vbmeta struct. Se alguma partição falhar nessa verificação, o gerenciador de inicialização identificará que os arquivos do sistema foram modificados. A partir deste resultado, o carregador de inicialização define o estado de inicialização, exibindo avisos na tela que remetem ao o estado de inicialização na linha de comando do kernel, a exemplo de *androidboot.verifiedbootstate=orange*.

- AMARELO: Tela de aviso para dispositivos bloqueados com *trust set* personalizado;

- LARANJA: Tela de aviso para dispositivos desbloqueados;

- VERMELHO: (eio): tela de aviso para corrupção do *dm-verity*;

- VERMELHO: nenhum sistema operacional válido encontrado: nenhum sistema operacional válido encontrado.

A melhor solução encontrada até a presente data é utilizar uma imagem modificada da partição *vbmeta*, que desativa os sinalizadores, fazendo com que a imagem de inicialização personalizada e as demais partições não sejam verificadas pelo AVB.

2.6 SUITES FORENSES ESPECIALIZADAS EM DISPOSITIVOS MÓVEIS

Existem no mercado inúmeras ferramentas e suites forenses voltadas para a aquisição e análise de dados de dispositivos móveis. O estudo de Rao e Chakravarthy, [13], Khan e Mansuri [40] apontam algumas delas e as que são usadas pelo National Institute of Standards and Technology (NIST [41]: SAFT, AFLogical, LiME Module, Nandroid Backups, Open Source Android Forensics - Tool Kit (OSAF-TK), Santoku Linux, Andriller, JATG, Chip-Off, Cellebrite UFED, Mobile Oxygen Forensics, Paraben, Mobile Device Seizure, MOBILedit Forensic, MPE+, XRY, AXIOM, EnCase Forensic, X-Ways, XRY, UFED, Paraben e Final Mobile Forensics.

Podemos ainda citar o Indexador e Processador de Evidências Digitais (IPED), que pode ser obtido gratuitamente no site do Departamento de Polícia Federal do Brasil [42].

Segundo Pappas [11], qualquer ferramenta ou software usado para aquisição e análise de dados deve ser testado e verificado anteriormente à sua utilização em casos reais, para que possa garantir seu desempenho e que os documentos relacionados ao software/hardware devem ser revistos periodicamente. O NIST disponibiliza em seu site[1] relatórios de validação de algumas ferramentas. Os relatórios apontam recursos e limitações de tais ferramentas.

2.7 TRABALHOS RELACIONADOS

Esta seção apresenta alguns trabalhos relacionados, onde os esforços foram voltados para a aquisição de dados de dispositivos móveis por meio de metodologias e técnicas diferentes das apresentadas por já serem existentes no mercado.

Segundo Martelli [43] o conceito de Metodologia pode ser atribuido ao estudo do ca-

[1] https://www.dhs.gov/science-and-technology/nist-cftt-reports

minho escolhido para a busca na solução de problemas, e que com o decorrer dos anos as metodologias de pesquisas vem sendo modificadas com a iniciação de novos pesquisadores e com o tipo de pesquisa a ser realizado, e que a pesquisa científica é um processo de construção de conhecimento baseado no método científico, o que nos permite solucionar problemas em qualquer área do conhecimento.

Ainda de acordo com Martelli [43], a pesquisa exploratória é uma metodologia que permite encontrar a solução de problemas sobre temas pouco conhecidos ou explorados.

Quanto a definição da estratégia de pesquisa, de acordo com Lacerda, [44], uma vez determinada a área de conhecimento, devem ser elencadas as palavras-chave que serão utilizadas na busca de referências, podendo ainda utilizar a lógica booleana para a construção da árvore de palavras-chave.

Durante a seleção dos artigos que compõem o portfólio, o motor de busca padrão adotado foi o *Google Acadêmico*, uma vez que o mesmo é capaz de indexar uma imensa gama de repositórios. Os artigos foram avaliados quanto à relevância em relação a três eixos principais: tema, autores e periódico. Os artigos selecionados foram ordenados segundo critérios científicos, sem vieses na escolha, tendo sido adotado um método multicritério de apoio.

Baseado nesses conceitos, a formulação da pergunta racional sobre o problema é objetiva e direta e fundamentada com referências bibliográficas confiáveis, o que garante uma resposta com base científica e técnica.

Os trabalhos formam agrupados de acordo com as técnincas e metodologias aplicadas pelos autores.

2.7.1 Aquisições baseadas em ataque ao firmware do dispositivo

Yang et al. [19] propuseram um método de aquisição baseado na análise dos protocolos de atualização de firmware dos smartphones Android dos fabricantes Samsung, LG e Pantech. Afirmaram ser possível realizar a aquisição física de smartphones Android usando o comando de leitura da memória flash, fazendo engenharia reversa do protocolo de atualização de firmware no carregador de inicialização. No entanto, à época da realização do trabalho, os dispositivos Android utilizados foram os modelos LG G3 (F400S, D851), Optimus G (F180S, E975), R3 (IM-A850S), Iron2 (IM-A910S) e Nexus 4/5 (E960, D821), que ainda não encriptavam, por padrão, a memória principal. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Li et al. [45] apresentaram uma ferramenta forense com base na substituição do Recovery Mode, com foco nas memórias do tipo *flash* e eMMC. Foi explorada a possibilidade de recuperação de dados após a desinstalação de um aplicativo em dispositivos Android com

sistema de arquivos no formato EXT4. Dos dispositivos submetidos à extração de dados, a versão mais recente do Android foi a 4.4.X, com kernel 3.4.39. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Wu et al. [10] propuseram uma aquisição forense para smartphones Android com Processadores Qualcomm em uma abordagem usando modos especiais. Abordaram os modos especiais 9008 e 9006 do Processador Qualcomm para extrair a partição de dados. Esse modo também é conhecido como Emergency Download Mode (EDL). Adquirindo a imagem de dados usando o Modo Qualcomm 9008, não se faz necessário o desbloqueio do gerenciador de inicialização. É preciso apenas inicializar o dispositivo em modo fastboot e definir o telefone no modo Qualcomm 9008. O Modo 9006 é aplicado causando danos intencionais na partição de inicialização, após isso um computador pode ser usado para ler os dados da partição. Nos experimentos, também foi comprovada a integridade dos dados e a possibilidade de executar os métodos propostos. Todavia, o experimento foi feito em dispositivos com SO Android Versão 5.1.1, e a abordagem proposta alcança somente dispositivos que utilizam SoCs Qualcomm. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal e a aplicabilidade somente em dispositivos que utilizam SoCs Qualcomm.

Alendal et al. [32], exploraram o Common Criteria (CC), que é um recurso que aumenta o nível de segurança dos dispositivos Samsung e, portanto, dificulta a aquisição forense para a aplicação da lei. Devido a impossibilidade de obter acesso às especificações, documentação e código fonte do projeto, os autores realizaram a engenharia reversa da implementação do modo CC e como é protegido pelo gerenciador de inicialização seguro da Samsung. Apresentaram como esse modo de segurança é aplicado, suas vulnerabilidades e como elas podem ser usadas para contornar o modo CC aumentando a superfície de ataque para posterior aquisição forense. Contudo, o trabalho limita-se a dispositivos fabricados pela Samsung e é incapaz de contornar a criptografia da memória principal.

Dave et al. [46] recuperaram 3.500 comandos AT de mais de 2.000 imagens de firmware de smartphones Android de onze fornecedores. Os comandos foram testados em oito dispositivos Android de quatro fornecedores diferentes por meio da interface USB. Os autores identificaram a possibilidade de reescrever o firmware do dispositivo, ignorar os mecanismos de segurança do Android, obter informações confidenciais do dispositivo, executar desbloqueios de tela, e injetar eventos de toque apenas através do uso de comandos AT. Ainda segundo Dave et al. [46], há ainda outras funcionalidades que podem ser exploradas pelo comando AT, não descritas no trabalho analisado, o que caracterizaria uma maior superfície de ataque em dispositivos Android. Os comandos AT foram escritos no início da década 80, cujo objetivo era o de controlar modems, mas ainda podem ser usados na maioria dos smartphones com SO Android. A técnica mostrou-se eficaz somente em dispositivos Sam-

sung até o modelo Galaxy S7 Edge com SO Android até versâo 7.0. Testado em um modelo Galaxy S8 Plus, a técnica mostrou-se inificaz, assim como em modelos Google Nexus 6P e Google Pixel, o que limita a metodologia a apenas um fabricante.

2.7.2 Aquisições empregando *ISP, JTAG e Chip-Off*

Pappas [11] realizou um estudo focado nas técnicas de aquisição física JATG e ISP, com objetivo de provar que estas técnicas forenses são equivalentes quando comparadas a qualquer outro método. Para tanto, propos três testes. O primeiro teste mostrou as diferenças nos resultados da análise forense quando se realiza uma aquisição física, Sistema de arquivos e aquisição Lógica, usando o UFED Touch e posteriormente comparando os resultados usando o Physical Analyzer. Os resultados apontam que a extração física é mais vigorosa e, em termos forenses, recupera um número maior de evidências.

O segundo teste [11] visou provar que todas as aquisições físicas são equivalentes comparando os dados adquiridos do mesmo dispositivo usando o UFED Touch e a ferramenta “dd”. O resultado aponta que houve diferença no *hash* de dois arquivos, no entanto o autor explica que a diferença se deve as diferenças em “user data” se devem ao espaço não alocado e alterações nos arquivos do "Fyle System", como "inode table" e "superblock".

O terceiro teste [11] consistiu no exame do conteúdo de um dispositivo cifrado para mostrar se é possível encontrar evidências que foram adquiridas usando a ferramenta "dd", com o objetivo de verificar se uma aquisição física de um dispositivo cifrado pode fornecer alguma informação útil. Concluiu-se que se o dispositivo estiver cifrado, a aquisição física produzirá um código criptografado completo, inútil para a análise forense, pois nenhuma informação que faça sentido pode ser encontrada.

No caso de dispositivos Android antigos ou desatualizados, existe a possibilidade de quebra da criptografia. O autor [11] descreve ainda um passo a passo da aquisição de um dispositivo móvel usando ISP e JATG e sua posterior análise no UFED Physical Analyzer. O autor [11] buscou ainda evidenciar os diferentes graus de dificuldade ao se utilizar diferentes ferramentas, como o UFED Touch, que é de fácil uso, comparando-a ao ISP e JATG, onde há o risco de danificar o dispositivo. O foco principal do estudo foi fornecer uma visão geral da aquisição de JATG e ISP, apresentar algumas informações sobre essas técnicas e para mostrar que o UEFD Physical Analyzer pode ler o produto da extração.

No estudo [11] o dispositivo utilizado para aquisição dos dados no experimento foi um Samsung GT-I9505 (Galaxy S4) com SO Android Versão 5.0.1 rooteado, com memória principal criptografada, e um Nokia Lumia 635, com Windows Phone 8.1. Como principais limitações podemos citar a impossibilidade de contornar a criptografia do tipo FBE, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Sathe e Dongre [47] realizaram em estudo comparativo de requisitos, capacidades e limitações de técnicas forenses de aquisição lógica e física de dados de dispositivos móveis, sendo utilizado um dispositivo Samsung Galaxy Grand Duos GT-I9082 para a realização dos testes comparativos. Foram analisadas as seguintes suítes e ferramentas forenses UFED, MOBILedit, Oxygen Forensics e XRY, ADB Pull, Backup Analysis, AFLogical, Wondershare Dr. Fone for Android, JATG e Chip-Off. Embora abordem o uso de JATG e Chip-Off, o dispositivo analizado foi lançado com SO Android Versão 4.1.2 e foi atualizado até a verão 4.2.2, ambas não proviam, por padrão, a criptografia da memória principal. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Chanajitt et al. [48] analisaram sete aplicativos de m-banking para Android na Tailândia e descreveram os artefatos forenses que podem ser recuperados dos aplicativos e também os resultados da avaliação dos aplicativos no que se refere à segurança. Descrevem o JATG como método de aquisição de dados fisicamente invasivo, mas que possibilita o acesso aos dados sem a exigencia de que a depuração USB esteja habilitada, ou sem que o usuário root esteja habilitado (não rooteado) e ainda pode burlar o bloqueio de senha, ignorando o mecaninsmo de segurança do SO. No experimento realizado, foram usados um Samsung GT-I9500 (Galaxy S4) rooteado e um Samsung GT-I9190 (Galaxy S4 Mini) não rooteado, ambos com SO Android na Versão 4.4.2 com a memória principal não criptografada. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Fonseca [49] empregou a técnica de Chip-Off para recuperação dos dados de um disposivivo móvel severamente danificado. Os dados da eMMC, após adquiridos, foram analisados com o Cellebrite UFED Physical Analyzer. O dispositivo analisado foi um LG K8, com Android na versão 6. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Fonseca [50] empregou novamente a técnica de Chip-Off para recuperação dos dados de um disposivivo móvel severamente danificado pela oxidação da água ou outro líquido não identificado. Os dados da eMMC, após adquiridos, foram analisados no SO Ubuntu, onde a imagem da eMMC foi montada e acessada como se fosse outro dispositivo de armazenamento qualquer. O dispositivo analisado foi um Moto G1, com Android na versão 4.4.4. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Em 28 de janeiro de 2020, o NIST divilgou o resultado de testes realizados empregando

JATG e Chip-Off para adquirir dados de dispositivos móveis danificados [51]. O objetivo era testar a validade dos métodos, para saber se produzem resultados precisos com confiabilidade. Após a aquisição dos dados, foram usadas as seguintes suites forenses para a análise: AXIOM, EnCase Forensic, X-Ways, XRY, UFED, Paraben e Final Mobile Forensics, sendo identificados, locais, textos, fotos, dados de mídia social e outros. Os dados extraídos foram comparados aos dados carregados inicialmente em cada telefone, comprovando que JATG e chip-off extraíram os dados sem alterá-los, e que algumas das ferramentas utilizadas são mais eficientes para a análise dos dados do que outras, especialmente para dados de aplicativos de mídia social. Os dispositivos analisados eram de diferentes fabricantes, sendo a versão mais recente do SO Android a 5.1. Os resultados são publicados em uma série de relatórios on-line disponíveis gratuitamente [41]. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

2.7.3 Aquisições de dados da memória RAM

Soares e Sousa Júnior [52] apresentaram uma técnica de análise de dados de objetos Java provenientes da extração de memória RAM de dispositivos com arquitetura ARM 32-bits, mas com flexibilidade para serem adaptadas para outras arquiteturas (inclusive de 64-bits). Os autores desconsideraram os dados de objetos grandes ou alocados por bibliotecas de código nativo presentes no sistema operacional Android, versão 5.0, executado em um emulador. Para o processo de análise foi utilizado o *framework* Volatility. Os autores ainda criaram um conjunto de extensões para o Volatility que possibilitaram a recuperação das informações sobre o ambiente de execução e a recuperação de objetos Java alocados, além de mapeamentos para interpretação dos dados dos arquivos Android Runtime (ART), OAT e DEX, o que permitiu a recuperação das estruturas de dados do ambiente de execução. Para validação experimental, fizeram a emulação de um dispositivo Nexus 5 com a Vesão 5.01 do SO Android, utilizando o *goldfish*. Para análise dos dados, utilizaram a versão 0.4 da Distribuição Linux Santoku, especializada em forense de dispositivos móveis. Como resultado, os autores conseguiram extrair e analisar objetos Java com entendimento das estruturas de armazenamento, superando as técnicas tradicionais baseadas na detecção de padrões intrínsecos aos artefatos. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, a impossibilidade de ser aplicado a dispositivos reais além dos da impossibilidade de contornar os mecanismos de segurança implementados a partir da versão 7 do SO Android.

Soares e Sousa Júnior [53] descrevem um caso de transição resultante de uma nova versão do ART. Aprimoraram a técnica desenvolvida anteriormente [52], validando as ferramentas propostas em dispositivos emulados e reais, com SO Android versão 5.0.1, sendo o dispositivo físico rooteado, ilustrando as dificuldades relacionadas à análise forense, devido às

diferentes implementações específicas por vários fabricantes de dispositivos móveis. Como principais limitações podemos citar a impossibilidade de contornar a criptografia da memória principal, além dos mecanismos de segurança implementados a partir da versão 7 do SO Android.

Na Tabela 2.2 apresentamos um resumo das diferentes técnicas e metodologias empregadas em trabalhos relacionados.

Tabela 2.2 – Técnicas e metodologias empregadas em trabalhos relacionados.

	Aquisições baseadas em ataque ao firmware do dispositivo	Aquisições usando JATG, ISP e Chip-Off	Aquisição de dados da memória RAM
[19]	X	-	-
[10]	X	-	-
[32]	X	-	-
[46]	X	-	-
[45]	X	-	-
[11]	-	X	-
[47]	-	X	-
[48]	-	X	-
[49]	-	X	-
[50]	-	X	-
[51]	-	X	-
[52]	-	-	X
[53]	-	-	X

Diferentemente dos trabalhos correlatos apresentados na Tabela 2.2, este trabalho irá empregar a combinação das técnicas de ISP e Combination Firmware, sendo este o principal diferencial dos demais, que na sua maioria só aplicam uma técnica, não contemplando dispositivos de fabricação mais recente nem os novos mecanismos de bloqueio, criptografia e implementações de segurança, contemplados pela metodologia proposta.

3 DELIMITAÇÃO DO PROBLEMA E PROPOSTA DE SOLUÇÃO

A Legislação brasileira, no que se refere ao Direito Digital, é brevemente analisada neste trabalho, tendo em vista o objetivo de caráter mais técnico do mesmo. No entanto, se faz necessário abordar alguns pontos que são esssenciais para que as provas obtidas com o emprego da metodologia proposta estejam de acordo com o que preconiza a legislação vigente.

De acordo com Velho [54], a informatização da sociedade trouxe inúmeros benefícios e facilidades, mas com eles vieram também novos desafios. Tal mudança obrigou também o Direito a mudar, evoluir, acompanhar a transformação social causada pelo advento das novas tecnologias. O estudo do Direito Cibernético tornou-se essencial como ferramenta técnica-jurídica para vários setores, e fundamental para analistas forenses, pois seu domínio possibilita o desencadeamento de ações de prevenção e combate aos crimes cujo *modus operandi* exige alguma ação ou atividade através de uso de recursos informáticos ou telemáticos, ou gera algum tipo de registro eletrônico, seja de sua autoria, ocorrência ou resultado, bem como a responsabilidade gerada por tais ações, não obedecendo limites geográficos nem temporais.

O Direito Digital [1] é o conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital. Essa nova ramificação jurídica corresponde ao conjunto de normas que visam tutelar as relações humanas e as violações comportamentais em ambientes digitais. São as regras e princípios que orientem a conduta nesse meio.

No que diz respeito ao Direito Digital, algumas leis devem ser observadas:

- Decreto n° 9.637 - 26 de dezembro de 2018 (Política Nacional de Segurança da Informação);

- LEI n° 13.709 - 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);

- Lei n° 12.846 - 1º de agosto de 2013 (Lei Anticorrupção);

- Lei n° 12.850 - 02 de agosto de 2013 (Lei de Provas Eletrônicas);

- Decreto n° 7.962 - 15 de março de 2013 (Contratação no Comércio Eletrônico);

- Lei n° 12.737 - 30 de novembro de 2012 (Tipificação criminal de delitos informáticos);

- Leis de n° 12.735 - de 30 de novembro de 2012 (Tipificação criminal de delitos infor-

[1] O Direito Digital, também conhecido e citado como Direito Cibernético, Direito Eletrônico, Direito da Informática, Direito da Tecnologia da Informação [54].

máticos);

- Decreto n° 7.845 - de 14 de novembro de 2012 (Lei de Tratamento da Informação Classificada);

- Lei n° 12.551 - 15 de sezembro de 2011 (Lei Home Office e Teletrabalho);

- Lei n° 12.527 - 18 de novembro de 2011 (Lei de Acesso à Informação);

- Lei n° 10.764 - 12 de novembro de 2003 (Lei de Pornografia Infantil na Internet);

- Lei n° 9.610 - 19 de fevereiro de 1998 (Lei de Direitos Autorais);

- Lei n° 9.609 - 19 de fevereiro de 1998 (Lei de Software);

- Lei n° 9.296 - 24 de julho de 1996 (Lei de Interceptação);

- Lei n° 9.279 - 14 de maio de 1996 (Lei de Propriedade Industrial).

Dentre as classificações adotadas na literatura para esses crimes, destacam-se duas. Uma que faz referência a crimes cibernéticos puros, mistos e comuns, e outra que classifica tais infrações como próprios e impróprios. No Brasil, a categorização mais aceita é a dos crimes puros, mistos e comuns. De acordo com Pereira e Oliveira [55], podemos assim definir tais crimes:

- **Crimes cibernéticos puros ou exclusivamente cibernéticos:** são aqueles que somente podem ser cometidos através do ambiente computacional;
- **Crimes cibernéticos mistos:** são aqueles onde se faz uso da internet para realizar o ato ilícito, mas o foco não é o computador da vitima;
- **Crimes cibernéticos comuns:** são aqueles onde o ambiente computacional é utilizado como ferramenta ou como meio para facilitar ou potencializar o ato ilícito;

Conforme descrito na metodologia aplicada à forense de dispositivos móveis (Figura 1.1), para que as evidências digitais sejam consideradas válidas, há requisitos a serem cumpridos para obtenção da prova digital, tendo em vista que é necessário garantir a autenticidade e a integridade da prova. No que diz respeito à identificação da evidência, segundo Velho [54], a autenticidade é a garantia de que a evidência tem origem no autor nela indicado e quanto a preservação da evidencia, também de acordo com Velho [54], a integridade é a garantia de que a informação não sofreu nenhuma alteração ao longo do processo.

No tocante à Cadeia de custódia, o Ministério da Justiça e Segurança Pública estabeleceu por meio da Portaria n° 82, de 16 de julho de 2014 [56], diretrizes a serem observadas pelos profissionais e Órgãos de segurança pública no que se refere à cadeia de custódia, que é um complemento essencial para garantir a integridade, pois envolve a documentação da cronologia dos vestígios e do controle do acesso aos mesmos, tornando possível a rastreabilidade.

No que diz respeito ao método de aquisição da evidência, na computação forense tradicional, a ordem de volatilidade, desrita na RFC 3227-2002 [18], é uma referência para profissionais da área, tanto da área técnica quanto do direito. Quando tratamos da forense de dispositivos móveis, mais especificamente smartphones, a volatilidade pode englobar outros fatores, pois deverão ser preservadas as impressões digitais do usuário do dispositivo e ainda materiais genéticos, como sangue ou outros fluídos, pois podem ser usadas em outra fase do processo por outras ciências forenses. Sempre que possível, o dispositivo deve ser mantido no estado em que foi apreendido. Se for apreendido desligado, deverá permanecer desligado, ou ainda, se o mesmo estiver ligado, é desejável adicionar uma fonte de energia externa, como um *powerbank*, para que o mesmo não desligue por falta de alimentação. É importante colocar o dispositivo no modo avião, que desativa conexões Wi-Fi, GPS, bluetooth e a comunicação com a rede Global System for Mobile GSM, para impedir que ele receba novas chamadas, SMS, crie novos registros de itinerário pelo *gps*, evitando falsos positivos durante o processo de análise, ou ainda que os dados possam ser apagados remotamente por um comando recebido pela rede de dados. Se isso não for possível, é aconselhável o uso de uma *faraday bag* para transportar o dispositivo até o laboratório onde os dados serão adquiridos, ou ainda a utilização de um *radio jammer* (bloqueador de sinal). No entanto, as *faraday bag* devem ser testadas constantemente, pois as memas perdem a eficácia com o decorrer do uso. Se não dispuser destes meios ou ainda o acesso aos controles de tais funções no aparelho estejam indisponíveis em virtude do bloqueio de tela imposto pelo usuário, pode ser adotado o procedimento de remover o SIM Card do dispositivo. Tal procedimento evitará que o dispositivo receba comandos remotos entre outros já citados. Todos os recursos e acessórios do dispositivo devem ser documentados. Após essa etapa, caberá ao especialista definir quais ferramentas utilizará para realizar a aquisição dos dados. É sempre desejável realizar a aquisição física (Figura 2.1), que é mais vigorosa em termos forenses. No entanto, o processo de aquisição dependerá das ferramentas disponíveis, e do modelo do dispositivo, pois nem sempre a aquisição física, pode ser possível, ou ainda qualquer tipo de aquisição, caso o telefone esteja com mecanismo de bloqueio de acesso ativado.

Outro fator determinante para o sucesso de uma forense digital, são as perguntas investigativas. Tais perguntas, elaboradas pela autoridade que requisita o exame pericial, indicarão a direção dos esforços ao analista forense. Se as perguntas investigativas forem mal formuladas ou vagas, este poderá direcionar seus esforços para vestígios e evidências que não levarão à solução do caso.

Já durante o processo de análise, após ter adquirido os dados do dispositivo móvel e de posse das perguntas investigativas, o analista forense buscará respostas às perguntas que lhe foram feitas. O processo de análise dependerá também das ferramentas que o mesmo tem à disposição. Salvo algumas exceções, as ferramentas forenses tem a capacidade ou oferecem a possibilidade de portar a aquisição para a análise em ferramenta de outro fabricante. Tal

situação não ocorre entre as Suites XRY e UFED, pois o XRY consegue processar e analisar dados adquiridos pelo UFED, enquanto o inverso não é verdadeiro, devido à criptografia imposta pelo XRY no momento da aquisição.

A maioria das Suites forenses consegue categorizar uma vasta gama de dados adquiridos dos dispositivos. É necessário observar que o volume de dados depende do processo de aquisição realizado (Figura 2.1). Os mais comuns, considerando a Aquisição Física (Subseção 2.1.1), são dados de identificação do equipamento (International Mobile Subscriber Identity - IMSI, International Mobile Equipment Identity - IMEI, modelo do dispositivo, número de série, versão do SO, entre outros); dados relativos ao usuário (contas, senhas, contatos, agenda, calendários, anotações, número da linha telefônica e *tokens* para acesso a serviços hospedados em núvem); dados relativos à telefonia (registros de chamadas, Multimedia Messaging Service - MMS, Short Message Service - SMS); histórico de comunicação em comunicadores instanâneos (WhatsApp, Telegram, Snapshat, Signal, entre outros); histórico de navegação na internet (cookies, histórico de buscas, favoritos); arquivos de áudio e vídeo; informações de geolocalização (registrado em deslocamentos ou registro de imagens); registros de conexão com redes Wi-fi, pareamentos Bluetooth e Rede GSM GSM; dados de aplicativos; e, ainda todo o histórico de atividades da Google Account, que pode ser solicitado pelo Google Takeout. É possível ainda, realizar a análise usando ferramentas *Open Source*, seguindo o mesmo processo de documentação dos procedimentos realizados.

Por fim, os resultados obtidos devem ser documentados. Tal documentação inclui todos os registros realizados em todas as etapas da Metodologia forense empregada 1.1. Devem ser registradas também, quaisquer danos ou alterações ocorridas durante o processo de aquisição dos dados, visando possibilitar a repetição da análise por outro especialista forense, caso seja solicitado. A maioria das suites forenses comerciais oferece a função de geração de relatório, com uma vasta gama de possibilidades de formato de saída, inclusive podendo exportar dados e arquivos, sempre com a possibilidade de gerar *hash* dos mesmos. Quando ferramentas *Open Source* são empregadas, caso esta não possuam um módulo para geração do relatório, o mesmo deverá ser confeccionado manualmente. Neste documento, serão respondidas as perguntas investigativas feitas pela autoridade solicitante do exame.

3.1 DELIMITAÇÃO DO PROBLEMA

Uma das óticas equivocadas sobre a análise forense é a de que sempre se busca algo para incriminar o proprietário do dispositivo. No entanto, existem outras razões para a análise de um dispositivo. É o que ocorre nos casos de pedofilia, assédio (tanto moral quanto sexual), ameaças, onde o dispositivo a ser analisado inicialmente é geralmente o da vítima e ainda, há casos em que o dispositivo pertence a alguém que veio à óbito em virtude de ação delituosa,

e a análise do dispositivo da vítima pode ser de fundamental importância na elucidação do crime ou para previnir futuras ações de mesma natureza. Há ainda casos em que o dispositivo a ser analisado busca evidenciar a inocência de arrolado, ratificando a importância da correta análise dos dados obtidos.

A título de ilustração, é possível citar dois exemplos recentes de evidências cruciais encontradas em dispositivos móveis. O primeiro pode ser visto no caso do atirador Mohammed Saeed Al Shamrani, que em 6 de dezembro de 2019 matou três marinheiros americanos em uma base militar na Flórida. As autoridades descobriram contatos entre Mohammed Saeed Alshamrani e agentes da *Al Qaeda* depois de ter acesso ao conteúdo dos dispositivos móveis do franco-atirador [57].

O segundo exemplo, ocorrido no brasil, refere-se à aquisição dos dados de um smartphone, o que foi crucial para a elucidação do caso, onde a Policial Militar do Estado de São Paulo, Juliane dos Santos Duarte, assassinada por membros de uma organização criminosa, foi solucionado graças às conversas de WhatsApp obtidas depois da quebra de sigilo do celular de um dos suspeitos [49].

Embora os estudos não apontem de maneira explícita, observa-se que a dificuldade mais significativa encontrada pelos profissionais de forense digital, no que se refere à aquisição de dados de dispositivos móveis, são os bloqueios de tela configurados pelo usuário. Tal restrição impede a aquisição dos dados pelas ferramentas forenses usualmente empregadas, de uma extensa lista de modelos de diferentes fabricantes.

Corrobora com a afirmação o fato de que a Cellebrite [2] [58] já possui 11 laboratórios espalhados pelo mundo, especializados em serviços de desbloqueio e extração avançadas que utilizam o UFED Ultimate, sendo um destes instalado no Brasil [59]. O serviço oferecido por esses laboratórios é chamado de Cellebrite Advanced Service (CAS) CAS, cujo principal objetivo é o desbloqueio do dispositivo por meio da quebra de senha por ataque de força bruta. Tal técnica é passível de emprego em dispositivos da Apple com iOS, dispositivos Samsung, Huawei e LG [60], com um custo aproximado de $ 2.500,00 (Dois mil e quinhentos dólares) por desbloqueio.

Outra empresa que oferece uma solução semelhante é a GaryShitf, que desenvolveu um produto denominado GrayKey [61], destinado exclusivamente ao desbloqueio de iPhones. Além da remoção ou contorno *(bypass)* do bloqueio de tela, é pode ser necessário ainda fazer a aquisição física dos dados do dispositivo, para ter acesso ao conteúdo excluido pelo usuário e conteúdo de mensageiros instantâneos como o WhatsApp, sem contaminar a prova

[2] A Cellebrite DI é uma empresa israelense fundada em 1999 e sediada em Petah Tikva, que fabrica dispositivos de extração e análise de dados de dispositivos móveis, dispositivos de armazenamento em massa e drones. A empresa é uma subsidiária da Sun Corporation, do Japão. A Cellebrite DI possui duas subsidiárias, a Cellebrite USA Corp. e a Cellebrite GmbH, baseadas respectivamente em Parsippany, Nova Jersey, USA e Munique, na Alemanha.

e possibilitar a análise por ferramentas especializadas, comerciais ou não. No caso dos dados do aplicativo *WhatsApp* em dispositivos Android, é possível utilizar uma ferramenta específica, como a *Forensic Tools*. Neste aspecto, cada modelo deve ser individualmente analisado para identificar possibilidades e limitações de aquisição.

Em alguns casos, mesmo com o dispositivo desbloqueado, pode não ser possível realizar a aquisição física, sendo necessário ainda, habilitar o usuário *root* no dispositivo para tal. Em alguns modelos de dispositivos Android, durante o procedimento realizado para *rootear* o disposito, ocorre o apagamento seguro da memoria interna, o que não é viável do ponto de vista forense.

Considerando estes aspectos, esta seção delimita o problema abordado nesse trabalho e apresenta uma proposta de solução. Esta solução resultará no contorno da senha de bloqueio de tela, na possibilidade de rootear o dispositivo (se necessário) sem o risco de perda ou contaminação dos dados do usuário e a posterior aquisição dos dados por ferramenta forense especializada em dispositivos móveis e, por fim, a análise dos dados adquiridos.

A cada nova atualização de software, fabricantes de dispositivos móveis disponibilizam mecanismos de segurança aperfeiçoados para impedir ou dificultar o acesso não autorizado aos dados do dispositivo. Atualmente, o usuário dispõe de mecanismos de criptografia, mecanismos para bloqueio de tela que automaticamente impedem que outras alterações que poderiam permitir acesso aos dados sejam feitas, além de outros mecanismos de segurança.

A implementação e aprimoramento de tais mecanismos impede ou dificulta o trabalho de agências da aplicação da lei do estado. As polícias judiciária e científica encontram dificuldade para realizar a aquisição os dados dos dispositivos móveis que podem constituir evidências, tendo em vista que as atuais suites forenses, tanto proprietárias quanto *Open Source* não conseguem contornar (*bypassar*) os mecanismos de bloqueio de tela de alguns modelos de dispositivos móveis.

3.2 PROPOSTA DE SOLUÇÃO E JUSTIFICATIVA

Embora ferrametas como UFED, XRAY, AXIOM, BelcaSoft e outras sejam capazes de realizar a aquisição de dados de uma vasta gama de dispositivos móveis, bloqueados ou não, muitos modelos, principalmente de marcas com expressiva participação no mercado, não são suportados por tais ferramentas ou estas não são capazes de contornar os mecanismos de bloqueio de tela. Esta lacuna deixada pelas ferramentas forenses comerciais, motivou o desenvolvimento de uma solução que combina o uso de ISP e Combination Firmware, denominada Low-Level Data Acquisition with In-System Programming and Combination Firmware (LLDA-ISPCF), visando contornar o bloqueio de tela do dispositivo, permitindo

que sejam realizadas a aquisição física, com a possibilidade de *rootear* o dispositivo caso haja necessidade, a aquisição do sistema de arquivos e a aquisição lógica dos dados. Após as respectivas aquisições, o perito pode realizar sua a análise usando ferramentas forenses especializadas.

Durante a execução do processo da metodologia proposta, é possível ainda realizar o backup das partições que serão alteradas para o emprego do Firmware Especial. Este backup pode ser restaurado após a aquisição dos dados, deixando o dispositivo exatamente como original, com o mesmo bloqueio de tela configurado pelo usuário.

Esta metodologia é aplicável à uma vasta gama de dispositivos, independente da versão do SO (testado com eficácia até a versão 9), do modelo ou fabricante do SoC ou do sistema de arquivos.

As possibilidades forenses oferecidas pela metodologia proposta são de grande importância para a forense digital, pois pode possibilitar a aquisição de dados contidos em dispositivos móveis para elucidação dos mais variados crimes. A capacidade de adquirir dados de dispositivos móveis com as últimas versões do SO Android, já que um pequeno número de dispositivos executa a Versão 10 do Android, representa um avanço significativo no que diz respeito à forense de dispositivos móveis, principalmente considerendo o cenário atual.

Depois de verificar se a fase de coleta dos dados do dispositivo está em conformidade com o estágio do ciclo de vida da forense digital apresentado na Figura 2.2, a metodologia proposta neste trabalho pode ser empregada na fase de aquisição, seja ela física, de sistema de arquivos ou lógica.

3.3 DESCRIÇÃO DA METODOLOGIA PROPOSTA

A metodologia é apresentanda na Figura 3.1 e suas fases estão detalhadas abaixo:

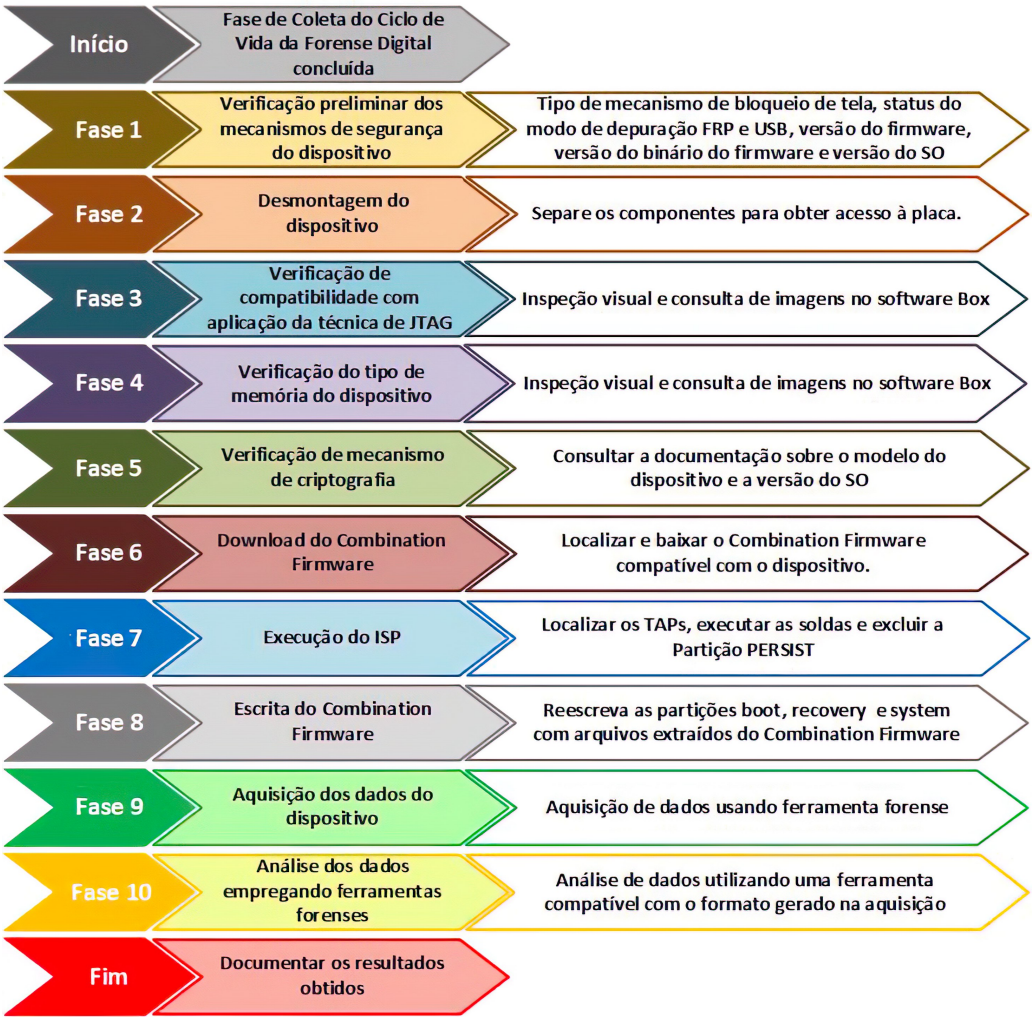

Figura 3.1 – Fluxo de execução da metodologia proposta.

3.3.1 Fase 1: Verificação Preliminar dos mecanismos de segurança do dispositivo

Esta fase, embora de simples execução, é de fundamental importância para a execução da metodologia porposta, pois a partir dos dados dela obtidos, é possível saber se as demais fases poderão ser executadas.

O primeiro passo é verificar no software da Box, se o dispositivo possui os TAPs para a execução do ISP. Caso possua, deve-se verificar se o dispositivo possui algum tipo de mecanismo de bloqueio de tela. Os mais comuns Encontrados nos dispositivos Android são o PIN padrão, senha alfanumérica, biometria, reconhecimento facial e leitura de íris. Existem ainda mecanismos de bloqueios apoiados em hardware, como Tokens NFC e USB, embora sejam menos comuns. Se o dispositivo estiver protegido pelo mecanismo de bloqueio de tela, será necessário iniciar o dispositivo em Modo Recovery para obtermos informações sobre o status do bootloader do dispositivo (bloqueado ou debloqueado), Modo de depuração USB (habililtado ou desabilitado), status do FRP (On ou OfF) e a versão do Firmware do dispositivo, com atenção especial à versão do binário do Fiwmware. Dispositivos Xiaomi

não exibem tais informações quando inicializados em Modo Recovery, o que inviabiliza a obtenção de tais informações.

Com o dispositivo bloqueado, é necessário utilizar uma combinação de teclas físicas presentes no dispositivo, sendo que tal combinação varia de acordo com o fabricante e com o modelo. A maneira mais comum, é partindo da situação em que o dispositivo encontra-se desligado, pressionar simultaneamente as teclas Power e Volume Up e mantê-las pressionadas por cerca de 3 segundos. Recomenda-se tomar nota de todas as informações, inclusive a versão do SO que é executada no dispositivo, pois esses dados serão utilizadas as próximas fases. Se o dispositivo estiver com o modo de depuração USB desabilitado, quando for conectado ao computador, embora seja reconhecido, não será possível acessar nenhuma partição do sistema de aquivos. O smartphone apenas recarregará a bateria pela porta USB. Se o modo de depuração USB estiver habilitado, pode ser explorada a técnica do uso do Android Debug Bridge (ADB) [62]. Esta técnica usa uma ferramenta de linha de comando que fornece acesso a um shell Unix que pode ser usado para executar diversos comandos em um dispositivo com SO Android, mas que não será abordada neste trabalho.

Caso o dispositivo não possua mecanismo de bloqueio de tela, poderão ser empregadas outras ferramentas ou até mesmo passos da metodologia proposta. Contudo, esta hipótese não será detalhada neste trabalho, já que não trata do mecanismo de segurança habilitado.

3.3.2 Fase 2: Desmontagem do dispositivo

Esta fase também é muito importante. Embora aqui o conhecimento exigido seja mais voltado à eletrônica ou manutenção de dispositivos móveis, se faz necessário enfatizar a fragilidade e tamanho diminuto dos componentes, o que exige paciência, conhecimento e habilidade manual, evitando danos aos componentes, o que poderia impossibililtar ou dificultar ainda mais a aquisição dos dados. O primeiro passo é a adoção do uso de uma pulseira antiestática, evitando que a energia estática presente no corpo ocasione a queima de algum componente. O objetivo é acessar os TAPs na placa do dispositivo. Em alguns modelos, é necessário remover o display e separar componentes para ter acesso a placa. Além do display, é necessário remover a bateria, cabos, dissipadores, blindágens e o que mais for necessário para ter acesso aos TAPs, possibilitando assim a soldagem com precisão adequada, sem risco de danificar o equipamento e inviabilizar a aquisição. É altamente recomendável uma pesquisa prévia sobre como proceder a desmontagem do modelo que será submetido à metodologia proposta.

Para a remover o display, é ideal o uso de um *LCD Disassembly Machine*, equipamento que aquece a tela de maneira uniforme, com a possibilidade de regulagem da temperatura, encontrando o ponto de fusão da cola usada no display, fazendo com que a mesma se solte com mais facilidade e reduzindo a possibilidade de quebra do mesmo. Em alguns dispositi-

vos, pode ser necessário remover segmentos da blindagem metálica de alguns componentes para se ter acesso aos TAPs.

3.3.3 Fase 3: Verificação de compatibilidade com aplicação da técnica de JTAG

Embora eteja presente apenas em dispositivos mais antigos, é necessário verificar se o mesmo possui os TAPs para a execução do JATG. Essa verificação pode ser realizada de modo visual. Caso o analista forense não consiga localizar os TAPs padrão JATG, pode consultar o software da Box e verificar o Diagrama dos TAPs do dispositivo no qual fará a aquisição.

É importante ratificar que os dispositivos mais recentes não incluem TAPs padrão JATG. Se o dispositivo a ser analizado possuir os TAPs, pode ser utilizada a técnica de JATG, conforme os trabalhos de Pappas [11], Sathe e Dongre [47], além dos testes realizados pelos NIST [51], cujos dispositivos eram dotados de TAPs para JATG. Caso contrário, outra técnica deve ser empregada.

3.3.4 Fase 4: Verificação do tipo de memória do dispositivo

O ISP, até a elaboração deste trabalho no melhor conhecimento do autor, só é compatível com memórias do tipo eMMC e eMCP, e já foi empregado na forense de dispositivos móveis, conforme o trabalho de Sathe e Dongre [47] e dos testes realizados pelos NIST [51]. Embora exista o leitor para Chip-Off de memórias do tipo UFS, não foram encontrados registros sobre ISP em dispositivos que utilizam tal tipo de memória.

3.3.5 Fase 5: Verificação de mecanismo de criptografia

Para verificar se memória principal está protegida com criptografia e qual o modelo foi aplicado, é necessário consultar a documentação referente ao modelo do dispositivo, ou ainda a versão do SO executada no aparelho, dado já obtido na Fase 1 (3.3.1) e buscar informações técnicas e respeito do SO do modelo a ser analisado em disopositivos desbloqueados, o tipo de criptografia pode ser verificado usando conectando o dispositivo a um computador com Windows ou Linux, com a ferramenta ADB instalada, executando o comando *adb shell getprop ro.crypto.type*, cujo saída será *file* ou *block*. O Android, por padrão, criptografa a partição *userdata* de todos os dispositivos com SO acima da versão 6, inclusive.

Faz-se necessário ratificar que o emprego da técnica de Chip-Off irá realizar a aquisição de dados criptografados, e que as suites forenses podem não ser capazes de descritografar tais dados. Se a memória principal não estiver protegida por nenhum tipo de criptografia, é possível utilizar o software da Box para realizar a aquisição física do dispositivo, sem a

necessidade do emprego do Combination Firmware.

3.3.6 Fase 6: Download do *Combination Firmware*

Nesta fase, de posse dos dados da versão do firmware do dispositivo e da versão do binário do mesmo, obtidos na Fase 1 (3.3.1), é necessário localizar e fazer o download do Firmware Especial (Combination Firmware para dispositivos Samsung), compatível com o dispositivo.

Existem sites que disponibilizam tais arquivos gratuitamente. No entanto, é aconselhavel efetuar o download de sites especializados, diminuindo a probabilidade de obter arquivos corrompidos ou infectados por malwares. Um dos sites mais conhecidos que disponibiliza acesso à ferramentas para manutenção de dispositivos móveis é o *Halabtech Support* [63]. Uma consideração importante sobre dispositivos Xiaomi, é que além do Firmware Especial, que traz apenas a informação do modelo do dispositivo, é necessário realizar o download do arquivo *vbmeta.img*, para desabilitar o funcionamento do AVB.

Para dois modelos usados no estudo de caso (Motorola XT 1640 - Moto G4 Plus e Samsung J260M/DS - J2 Core), os Firmwares Especiais foram desenvolvidos e cedidos por Fonseca [3], que atualmente trabalha no desenvolvimento de uma ferramenta (hardware e software) para fosense de dispositivos móveis.

3.3.7 Fase 7: Execução do ISP

Quando se chega até esta fase, significa que já foi identificado que o dispositivo é compatível com ISP. Com o dispositivo já desmontado, é importante verificar novamente, e se possível em mais de uma fonte de consulta (software da Box e outra fonte, a exemplo dos sites especializados em arquivos para manutenção de dispositivos móveis) o diagrama contendo a localização dos TAPs do modelo do dispositivo. Após identificar os TAPs na placa, é necessário realizar a soldagem dos condutores. Uma das extremidades dos condutores é soldada nos TAPs, a outra extremidade é fixada, também por meio de solda, no adaptador que posteriormente será conectado à ISP.

O passo seguinte é plugar o conector ISP na Box. Neste ponto, é possível utilizar a ferramenta *eMMC Tool Suite* para fazer a aquisição física da memória interna do dispositivo. No entanto, os dados criptografados que forem adquiridos somente poderão ser analisados se a suite forense usada para análise tiver capacidade de realizar a descriptografia dos dados adquiridos. Caso não seja possível descriptografar os dados, o software *JTAG Classic Suite*

[3]DJALMA BARBOSA FONSECA é especialista em dispositivos móveis. Atua na área forense de dispositivos móveis e possui muitos anos de experiência em reparo de microeletrônica. Atua como perito assistente para Forças da lei. É especialista e instrutor de cursos para aquisição de dados de dispositivos com SO Android empregando JATG, ISP, Chip-Off, Logical e Physical Swap.

será utilizado para manipular os dados da partição *Persist*, sem alterar a partição onde estão os dados do usuário.

Dispositivos Android possuem várias partições que tem diferentes funções [64]. No entanto, por tratar-se de um projeto *Opens Source*, os fabricantes podem efetuar alterações ou modificações à vontade. Dessa forma, teremos um número direferente de partições nos diferentes modelos de dispositivos que executam o SO Android. Assim, as partições podem variar em função do SoC, da marca, da versão do SO entre outras.

Para que seja possível instalar o Combination Firmware, ou seja, sobrescrever as partições *boot*, *recovery* e *system*, nos dispositivos Samsung é necessário anteriormente sobrescrever com 0 (zeros) a área onde está gravado o FRP, sendo que, em dispositivos mais atuais e novos, a FRP normalmente fica na Partição *Persist*). Enquanto o FRP estiver ativo, não é possível sobrescreve as partições *boot*, *recovery* e *system*.

Todas os valores para configuração do software necessários para a execução do ISP foram obtidos em *Seeking the Truth from Mobile Evidence.* [3].

3.3.8 Fase 8: Escrita do *Combination Firmware*

Seguindo as fases propostas na metodologia, a escrita do Combination Firmware é a última fase que antecede a aquisição propriamente dita. É necessário reescrever as partições *boot*, *recovery* e *system*. Tais partições terão seu conteúdo original substituido pelos arquivos contidos no Combination Firmware previamente obtido. É aconselhável efetuar um backup das partições que serão sobrescritas antes de realizar a operação. Pode-se ainda extrair o conteúdo do arquivo com extensão *MD5* e gerar um novo arquivo compactado com o mesmo nome do arquivo completo, sobrescrevendo o mesmo. Isso facilitará o processo de uso do softwre para a escrita do firmware.

Para a operação de escrita, podem ser empregadas tanto a *Box Octoplus Pro* quanto a ferramenta *Odin* ou ainda a própria Easy JTAG Plus. Os procedimentos necessários para a escrita do Combination Firmware usando a Box podem ser obtidos em *Seeking the Truth from Mobile Evidence.* [3].

Após a substituição das partições citadas acima, o dispositivo irá inicializar normalmente, sem solicitar a senha ou mecanismo imposto pelo usuário, exceto no dispositivo Motorola usado no estudo de caso, onde se faz necessário reiniciar o dispositivo mais uma vez.

Os dispositivo nos quais foram aplicados a metodologia proposta, empregam criptografia do tipo FBE e FDE. Nos dispositivos que usam criptografia FBE, quando o dispositivo é inicializado, o sistema acessa os dados armazenados na área cifrada especial do dispositivo, protegida com chaves de hardware. Todos os dados na partição *data* ficam inacessíveis até que o usuário forneça as credenciais para autenticação, pois essa área é protegida com chaves

baseadas nas credenciais do usuário. A senha do usuário é uma das chaves criptográficas e quando esta deixa de existir, resta somente a senha do sistema, definida no código-fonte pelos desenvolvedores. Como existe apenas a chave padrão do sistema, não ocorre a troca de chaves e a partição é descriptografada automaticamente. O processo é transparente e assim que o processo de inicialização for concluido, o sistema exibe a tela inicial.

Após a inicialização, o dispositivo exibe uma tela com funções essenciais, sendo possível visualizar fotos, explorar o conteúdo (arquivos) presentes no dispositivo, registrar imagens entre outras operações básicas.

A partir desse ponto, o dispositivo está pronto para aquisição dos dados, sendo possível ativar o Modo de Depuração USB, ativar a opção *Permanecer Ativo*, e ainda, se necessário para a aquisição, rootear o dispositivo. É importante ressaltar que o firmware agora instalado executa a mesma versão do Android que é executado no firmware original.

Assim sendo, os métodos de aquisição devem ser compatíveis com a versão do SO, caso o dispositivo não seja *rooteado*. A escolha da ferrameta forense para aquisição fica a critério do especialista executando o procedimento em questão.

3.3.9 Fase 9: Aquisição dos dados do dispositivo

Tão importante quanto as fases que a antecedem, nesta fase, o analista forense poderá selecionar a ferramenta mais adequada para a aquisição dos dados do dispositivo que estiver em processo de aquisição. É de fundamental importância que o profissional conheça minuciosamente todas as possibilidades da ferramenta, para que possa explorar ao máximo o seu potencial e obter o melhor resultado possível.

A necessidade de *rootear* ou não o dispositivo deve ser cuidadosamente avaliada pelo analista, cuja decisão poderá depender do modelo do dispositivo, das capacidades das ferramentas forenses que estiverem a sua disposição e das evidências que estiver buscando.

3.3.10 Fase 10: Análise dos dados empregando ferramentas forenses

Após a aquisição dos dados, esta etapa marca o fim das fases anteriores propostas pela metodologia. O analista forense realizará a análilse dos dados adquiridos, podendo valer-se de quaisquer ferramentas forenses que dispor para tal, desde que sejam compatíves com o formato dos dados gerados pela ferramenta que realizou a aquisição.

Cabe ressaltar que de uma aquisição física, é possível obter arquivos que contém as credenciais do usuário para acesso à serviços online e redes sociais, a exemplo dos serviços da Google (Keep, Photos, Google Drive, etc.), Facebook, Twitter, Instagram, entre outros. Essas credenciais quando extraídas, e quando inseridas em um software para busca e análise

de dados em *nuvem*, funcionam como "tokens", provendo acesso legitimo a tais serviços, aumentando consideravelmente a volume de dados obtidos.

Nesta fase, ressalta-se a importância da correta formulação das perguntas investigativas (Figura 1.1), pois é norteado por elas que o analista direcionará seus esforços.

4 ESTUDOS DE CASO: APLICAÇÃO DA METODOLOGIA PROPOSTA

Nesta seção serão detalhados quatro estudos de caso, e as ações em cada fase da metodologia proposta empregada a cada dispositivo. Não serão detalhados em todos os casos, a análise dos dados.

4.1 ESCOLHA DOS DISPOSITIVOS PARA VALIDAÇÃO DA METODOLOGIA PROPOSTA

Para fins de estudo, selecionamos quatro modelos de dispositivos para aplicação da metodogia proposta. A escolha do dispositivo foi feita levando em consideração o SoC, SO, o tipo de memória utilizado, o tipo de criptografia empregada e o fabricante. Os modelos selecionados representam, no que diz respeito aos aspectos supracitados, do ponto de vista da problemática para a aquisição de dados forenses, algo em torno de 70% dos dispositivos móveis com SO Android em uso atualmente.

Os modelos usados nos experimentos foram o Samsung J2 Prime (SM-G532MT - Android 6, SoC Mediatek), Samsung J2 Core (J260M/DS - Android 8.0, SoC Exynos), Motorola Moto G4 Plus (XT1640, Android 8.1, SoC Qualcomm), e Samsung Galaxy A10 (A105M/DS - Android 9.0, SoC Exynos). É importante deixar claro que como se trata de uma metodologia que aborda a utilização de várias ferramentas, em determinados dispositivos, pode não ser necessário o emprego de todas as ferramentas ou execução de todos os passos. Os tipos de aquisição de dados realizados serão descritos nos respectivos Estudos de Caso.

No entanto, para a escolha do modelo Samsung Galaxy A10 (A105M/DS), outros quatro fatores foram levados em consideração.

O primeiro foi a abrangência e o volume de vendas global. De acordo com a Counterpoint[1] [65] o Samsung Galaxy A10 (A105M) foi o smartphone Android mais vendido no mundo no terceiro trimestre do ano de 2019, e segundo colocado no volume geral de vendas, ficando apenas atrás do iPhone XR.

O segundo critério foi a versão do Android utilizada no dispositivo, uma vez que quanto mais atual for o smartphone, mais camadas de segurança são implementadas e mais seguro

[1]Empresa sediada em Hong Kong especializada em análise mercadológica e assessoria de negócios.

tende a ser o sistema. Neste caso, o modelo SM-A105M/DS executa a versão 9.0 (Pie) do SO Android, que é a executada na maioria (41,9%) dos dispositivos Android [66].

O terceiro critério foi a dificuldade para execução das soldas na placa, tendo em vista que o dispositivo tem componentes co mdimenões ainda mais reduzidas, quando comparados aos outros dispositivos. Mesmo sem a adoção do uso de uma VR-Table para a realização de ISP, é possível efetuar solda dos condutores nos TAPs.

O quarto critério é o fato de que os dados do modelo SM-A105M/DS tem a criptografia de dispositivo ativada automaticamente (Direct Boot).

Dos Smartphones usados nos Estudos de Caso, nenhum possui o AVB implementado.

Antes do emprego da metodologia proposta, realizamos tentativas de aquisição de dados usando todos os métodos disponíveis no UFED Touch 2 (software versão 7.32.0.68). Todos os dispositivos encontravam-se com bloqueio de tela (caracteres alfanuméricos) ativado, *bootloader* bloqueado, modo de depuração USB desabilitado e FRP ativo. Infelizmente, percebemos que nenhum dos métodos disponíveis na ferramenta conseguiu realizar a aquisição dos dados nem foi possível remover ou ignorar o bloqueio imposto pelo usuário. A exceção fica por conta do Samsung J2 Prime (SM-G532MT), que no início dos estudos para confecção desse trabalho, quando bloqueado não permitia a aquisição dos dados com o uso do UFED. No entanto, a versão 7.32.0.68 permite a aquisição dos dados mesmo com o dispositivo bloqueado.

Embora não faça parte da metodologia, em todos os dispositivos, exceto os danificados que foram submetidos à técnica de Swap 2.3.2, foram realizadas aquisições sem que o mecanismo de bloqueio estivesse ativado, para fins de comparação posterior com a aquisição após a remoção do mecanismo de bloqueio empregando a metodologia proposta. Nos dispositivos danificados, foi realizado somente a aquisição após o emprego da metologia para tornar o cenário o mais realista possível. O resultado das comparações serão descritos nos estudos de caso.

4.2 ESTUDO DE CASO 1

A seguir, serão descritas as fases da metodologia executadas para possibilitar o *bypass* do bloqueio de tela e a aquisição dos dados do dispositivo.

O Samsung Galaxy A10 sai de fábrica com Android 9.0 (Pie), e em alguns países o modelo já recebeu upgrade para Android 10, com One UI 2.0. O SoC é o Exynos 7884 (14 nm), e a capacidade de armazenamento interno é de 32GB, providos por uma eMMC 5.1, com sistema de arquivos EXT4.

Todas as etapas ilustradas na Figura 4.1 foram aplicadas para validar a metodologia proposta. O experimento foi repetido cinco vezes no mesmo dispositivo.

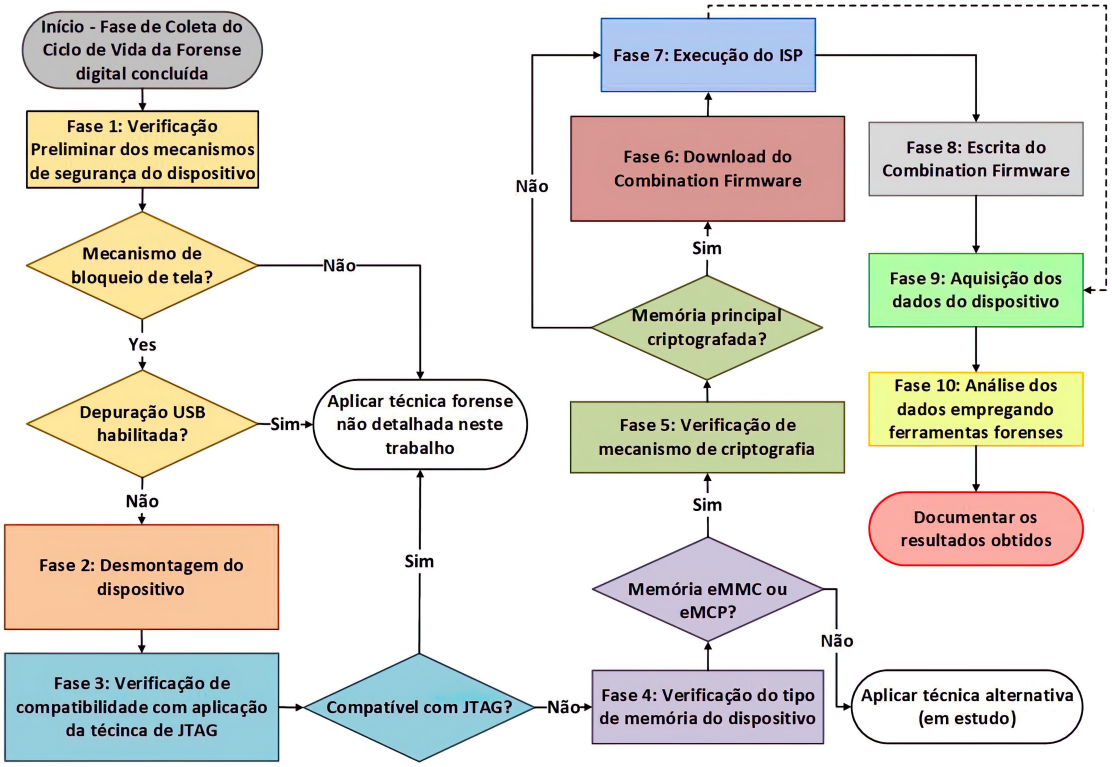

Figura 4.1 – Fluxograma de aplicação da metodologia no estudo de caso.

4.2.1 Fase 1: Verificação Preliminar dos mecanismos de segurança do dispositivo

O dispositivo encontrava-se com bloqueio de tela (caracteres alfanuméricos) ativado, o *bootloader* bloqueado, modo de depuração USB desabilitado e FRP ativo.

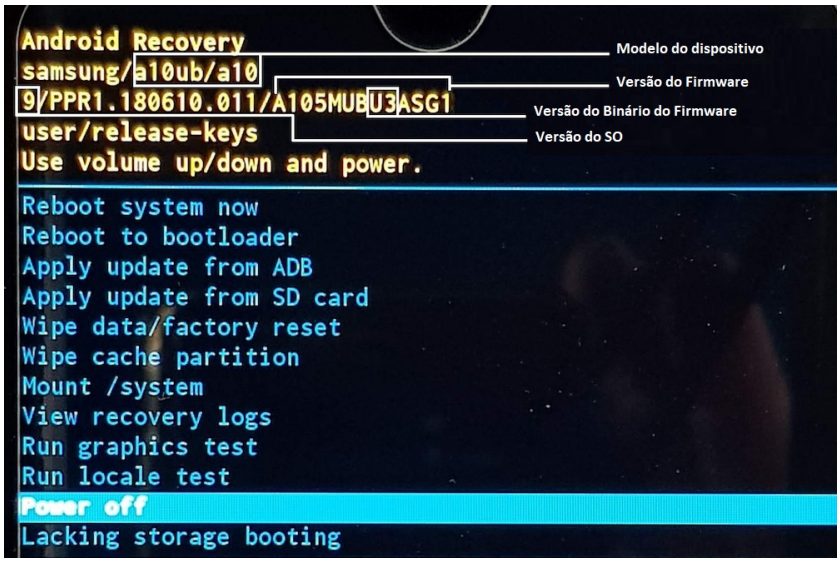

Figura 4.2 – Em destaque, a versão do Binário do dispositivo.

A Figura 4.2 exibe informações sobre a versão do firmware do dispositivo, versão do SO, modelo do dispositivo e versão do Binário do firmware.

4.2.2 Fase 2: Desmontagem do dispositivo

Para acessar a placa deste modelo de Smartphone, foi necessário remover o display. Além deste, foram removidos a bateria, desconectados cabos *flat* e outros conectores para que nenhum componente fosse danificado durante o processo de solda. Devido a dificuldade de acesso aos TAPs, foi necessário remover partes metálicas que servem como proteção para os componentes, como pode ser observado na Figura 4.3.

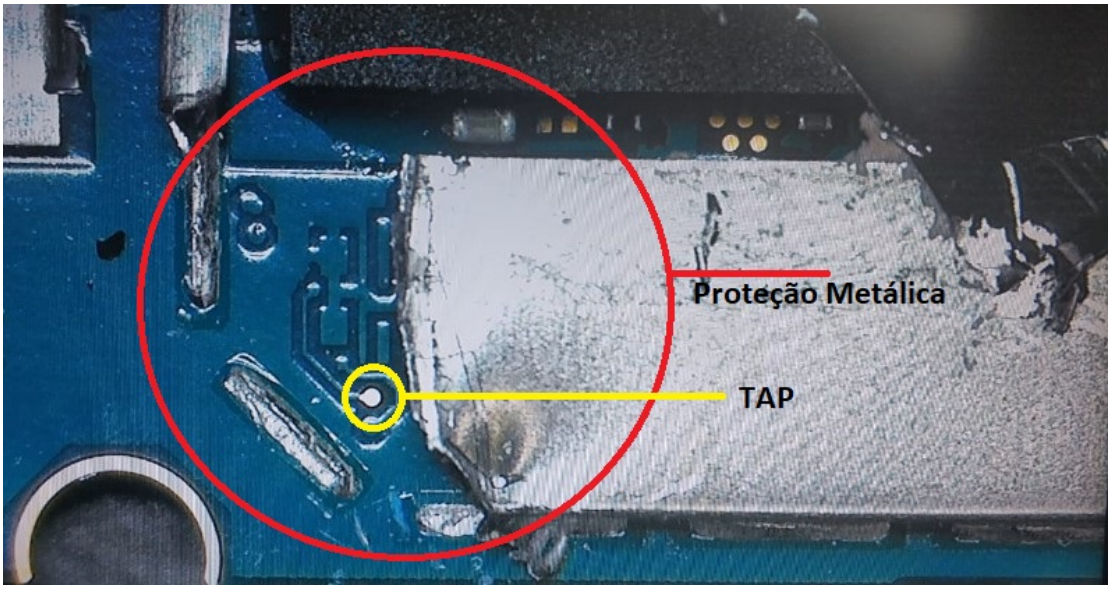

Figura 4.3 – Remoção de parte metálica para acesso ao TAP.

4.2.3 Fase 3: Verificação de compatibilidade com aplicação da técinca de JTAG

Neste estudo de caso, foi observado que o dispositivo, lançado em 2019, não possui TAPs para a execução do JATG (presente apenas em dispositivos mais antigos).

4.2.4 Fase 4: Verificação do tipo de memória do dispositivo

O dispositivo usado no estudo de caso possui memória do tipo eMMC 5.1.

4.2.5 Fase 5: Verificação de mecanismo de criptografia

O dispositivo empregado no estudo de caso (SM-A105M/DS) usa criptografia do tipo FBE.

4.2.6 Fase 6: Download do Combination Firmware

Após a identificação do Combination Firmware necessário, foi realizada a pesquisa para localizar o arquivo e posteriormente foi realizado o download para o computador local. A Figura 4.4 mostra o Combination Firmware selecionado para download.

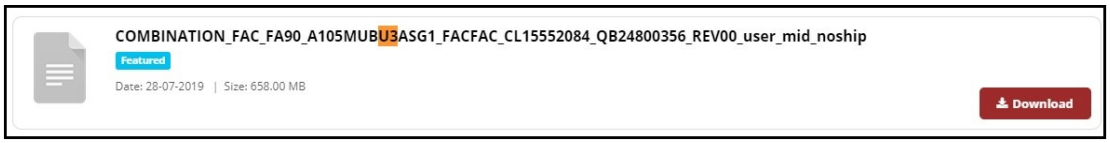

Figura 4.4 – Download do Combination Firmware.

4.2.7 Fase 7: Execução do ISP

Foi realizada a pesquisa no software da Box para ratificar a localização do diagrama contendo a localização dos TAPs na placa do dispositivo. Após a identificação dos TAPs na placa, foram realizadas as soldas dos condutores nos TAPs. A Figura 4.5 mostra, com a ajuda de um microscópio, um dos condutores já soldados.

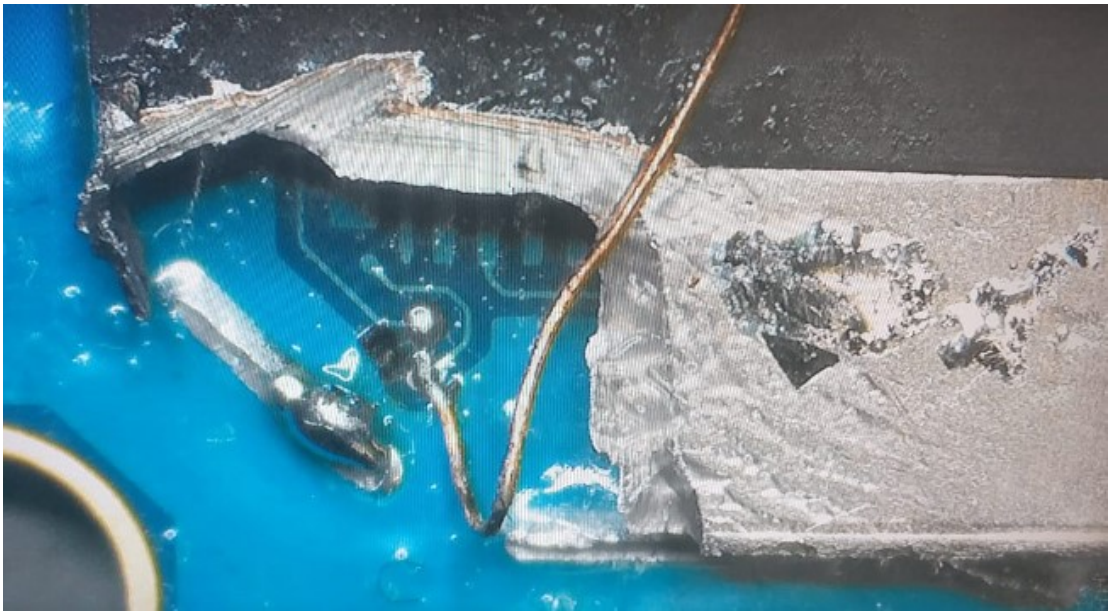

Figura 4.5 – Condutor metálico soldado ao TAP.

Realizada a solda dos condutores necessários, ligando os TAPs aos pontos correspondentes no conector ISP, o mesmo foi conectado à Box. Foi iniciado o utilitário *JTAG Classic Suite*. A Figura 4.6 mostra parte da tela do utilitário *JTAG Classic Suite*, exibindo as partições da memória principal do dispositivo e os valores de cada parâmetro para que se possa manipular a partição *Persist*. Tais valores podem variar de acordo com o dispositivo ou fabricante da eMMC. Os valores referentes aos parâmetros foram obtidos em *Seeking the Truth from Mobile Evidence.* [3].

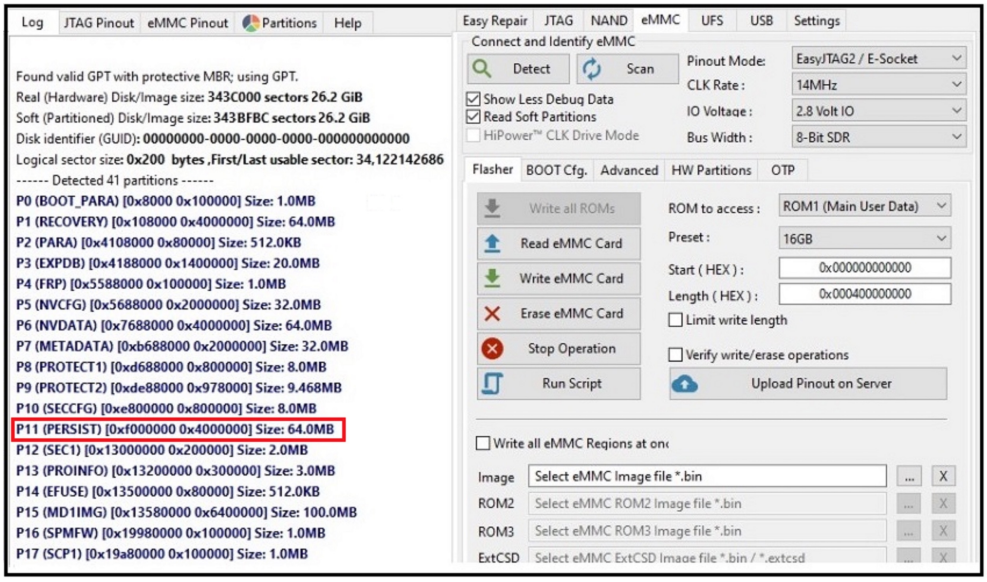

Figura 4.6 – Tela inicial do utilitário *JATG Classic Suite*. [Fonte: Autores]

No Samsung Galaxy A10, a FRP é gravada dentro da Partição *Persist*. Após a configuração dos parâmetros corretos, a partição *Persist* foi sobrescrita. No entanto, a partição que armazena os dados os dados do usuário não foi manipulada, preservando a integridade.

4.2.8 Fase 8: Escrita do Combination Firmware

Para a escrita do Combination Firmware, são necessários somente os arquivos que correspondem às partições (*boot*, *recovery* e *system*). O conteúdo do arquivo com extensão *MD5* pode ser visualizado na Figura 4.7

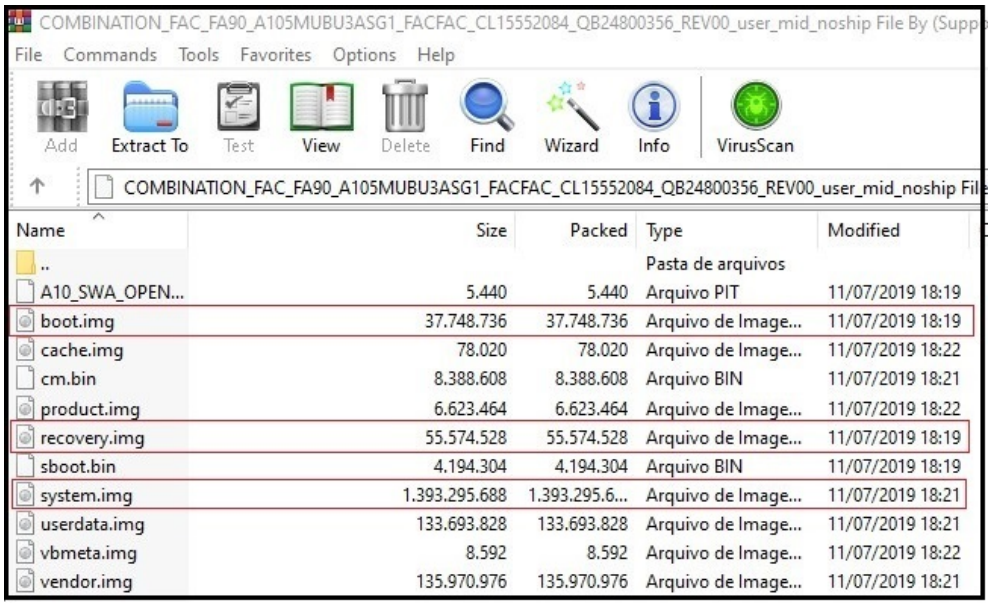

Figura 4.7 – Arquivos do Combination Firmware do SM-A105M/DS.

Em seguida, utilizamos a Box Octoplus Pro, e o utilitário *Octoplus Box Samsung Software* para substituir as partições especificadas na Figura 4.7. A Figura 4.8 exibe a tela inicial da ferramenta *Octoplus Box Samsung Software*. Todas as configurações foram obtidas em *Seeking the Truth from Mobile Evidence.* [3].

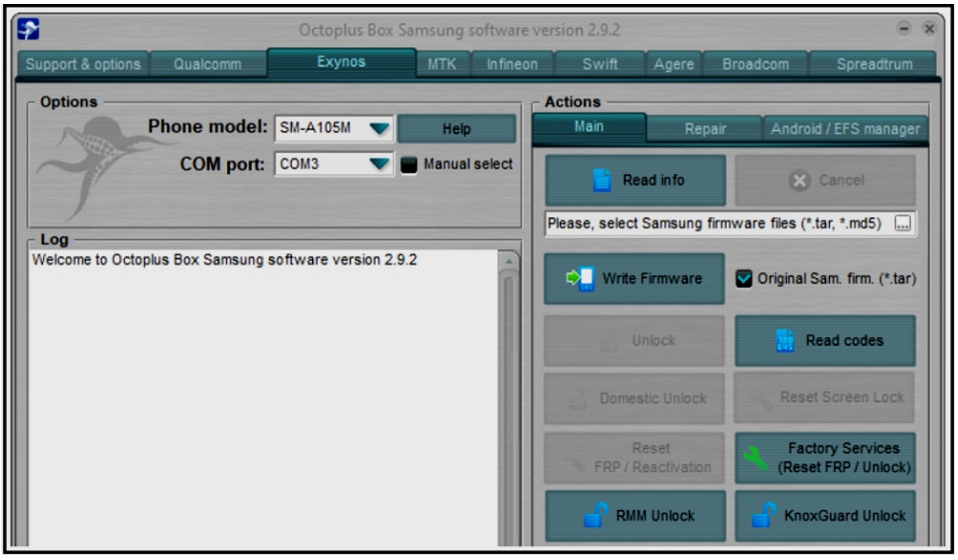

Figura 4.8 – Tela inicial do utilitário *Octoplus Box Sansung Software*.

Após substituir as partições *boot*, *recovery* e *system*, o dispositivo inicializou sem solicitar a senha de bloqueio de tela, permitindo a visualização de arquivos de mídia, aplicativos instalados e todo o conteúdo (arquivos) presente no dispositivo.

Ressalta-se que o firmware recém instalado executa a mesma versão do Android que é executado no firmware original, neste caso, a versão 9.

4.2.9 Fase 9: Aquisição dos dados do dispositivo

A escolha do UFED Touch 2 foi motivada por um anúncio da Cellebrite. Ela declara que a partir da versão 7.23 do UFED Touch 2, 4PC e InField teriam capacidade de realizar a aquisição física de dados de dispositivos Samsung das linhas "A" e "J" equipados com SoC *Exynos*, utilizando um perfil genérico [67].

Com o dispositivo já desbloqueado, foram realizadas tentativas de extração física utilil-zando o UFED Touch 2, com software anteriores à versão 7.32.0.68. Nos testes realizados anteriormente, não foi possível realizar a Aquisição Física sem que o usuário *root* fosse habilitado. Portanto, neste caso, foi possível a Aquisição do Sistema de Arquivos e a Aquisição Lógica sem rootear o dispositivo.

A Figura 4.9 mostra parte da tela do UFED Touch 2. Em destaque, o método que permite a Aquisição Física do SM-A105M/DS habilitando o usuário *root*.

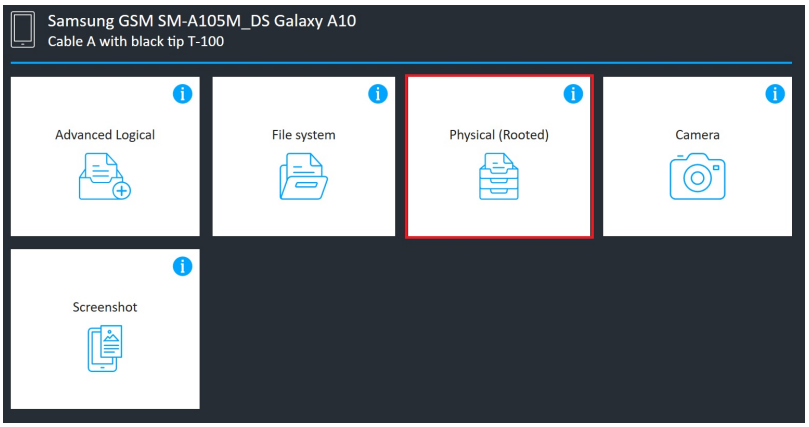

Figura 4.9 – Possibilidade de Aquisição Física do SM-A105M/DS.

Utilizando a versão 7.32.0.68 do software do UFED Touch 2 e selecionando um perfil genérico, foi possível realizar a aquisição física sem a necessidade de habilitar o usuário *root*, além das aquisições de Sistema de Arquivos e Aquisição Lógica. Vale lembrar que o UFED Touch 2 não conseguiu realizar o bypass do bloqueio de tela nos experimentos realizados antes da metodologia proposta neste trabalho, embora a ferramenta prometa fazê-lo.

A Figura 4.10 mostra parte da tela do UFED Touch 2 e, em destaque, a funcionalidade supracitada, permitindo a Aquisição Física do SM-A105M/DS.

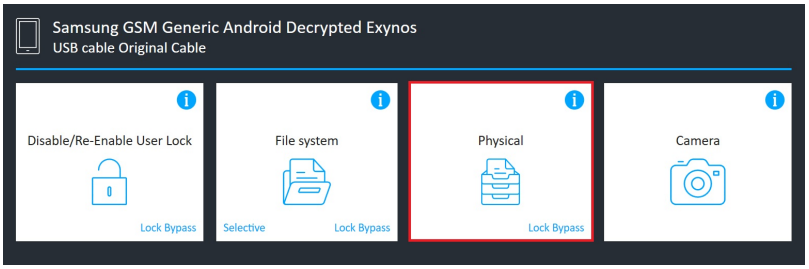

Figura 4.10 – Aquisição Física do SM-A105M/DS.

4.2.10 Fase 10: Análise utilizando o UFED Physical Analyzer

Os dados adquiridos foram analisados usando o software UFED Physical Analyzer Versão 7.32.0.16. A extração foi indexada sem erro e os resultados foram consistentes, incluindo as credenciais para acesso a serviços em *nuvem*, que podem ser utilizadas em aplicativos com capacidade de aquisição especificamente voltados para tais serviços, a exemplo do UFED Cloud Analyzer.

Embora o objetivo deste trabalho não seja o de comparar capacidades de suites forenses, os dados adquiridos foram analisados também com as ferramentas AXIOM Examiner e XRY XAMN, todas apresentando resultados consistentes sob a perspectiva de análise forense. Convém ainda frisar que as aquisições podem ser realizadas com uma ferramenta e a análise

com outra, limitando-se apenas ao formato gerado pela ferramenta de aquisição.

A Figura 4.11 exibe a relação dos arquivos recuperados e que foram analisados, inclusive arquivos excluídos pelo usuário e que ainda não haviam sido sobrescritos. Também se recuperou arquivos de aplicativos de mensagem instantânea, a exemplo do WhatsApp.

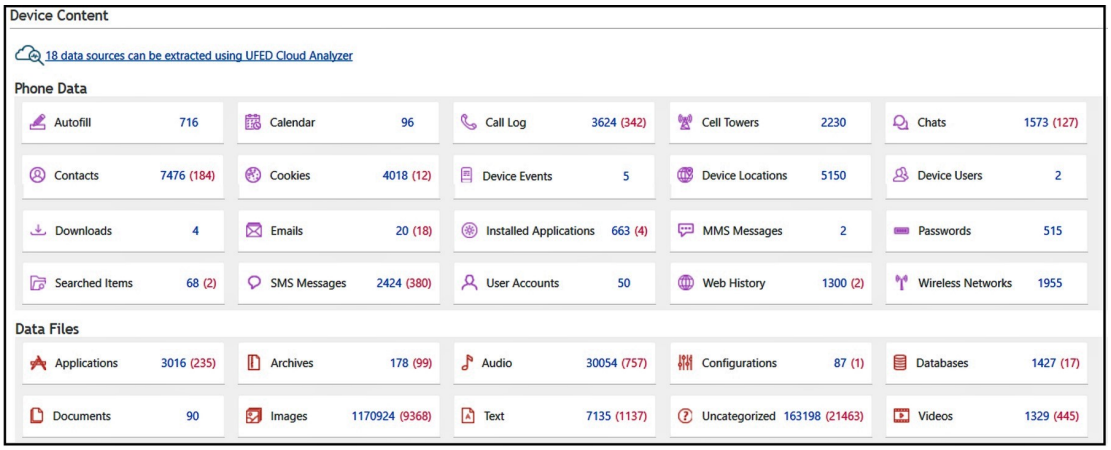

Figura 4.11 – Arquivos recuperados.

4.3 ESTUDO DE CASO 2

Nas versões de software anteriores à 7.23 do UFED Touch 2, a ferramenta não era capaz de realizar a aquisição dos dados deste modelo de dispositivo quando o mesmo se encontrava bloqueado, o que motivou o Estudo de caso. Atualmente, o Cellebrite UFED (Touch 2 ou 4PC) é capaz de realizar a aquisição dos dados com o dispositivo bloqueado.

O J2 Prime (SM-G532MT) sai de fábrica com Android 6, SoC Mediatek MT6737T (28 nm) e memória interna com capacidade de armazenamento de 8GB, providos por uma eMMC 5.0 e sistema de arquivos EXT4. Neste caso, não foi necessário aplicar todos os passos da metodologia para realizar o *bypass* do bloqueio de tela e a aquisição dos dados do dispositivo.

Todas as etapas ilustradas na Figura 4.12 foram aplicadas para validar a metodologia proposta. O experimento foi repetido cinco vezes, em cinco dispositivos diferentes.

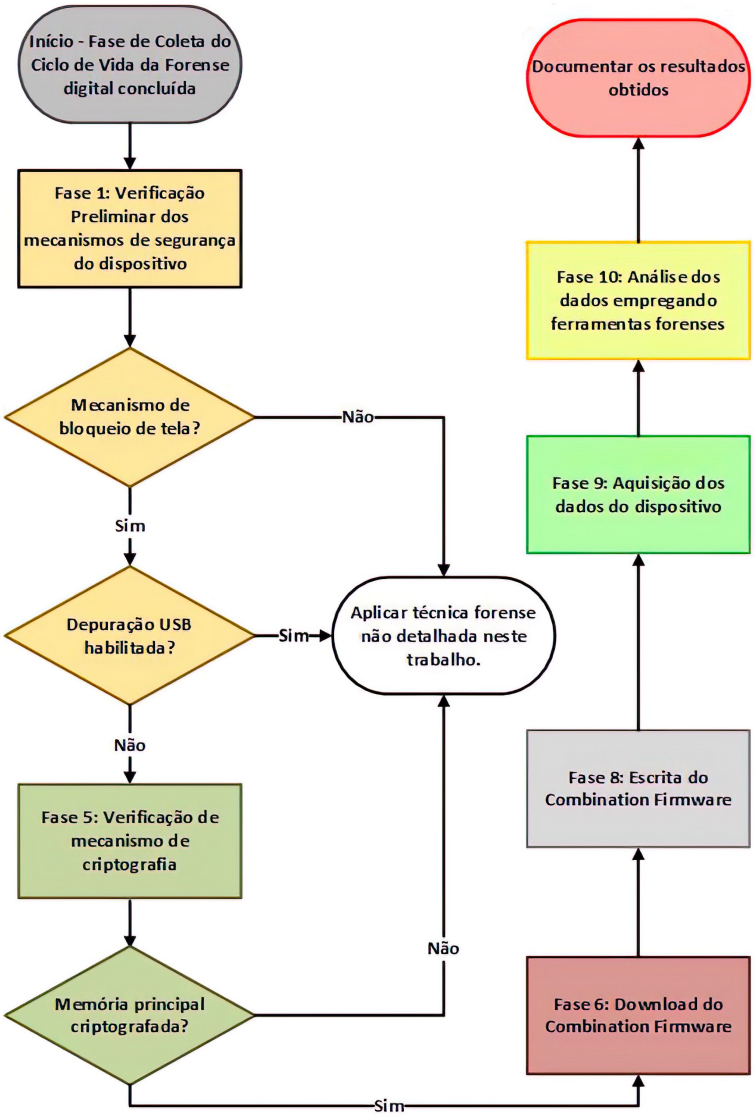

Figura 4.12 – Fluxograma de aplicação da metodologia no estudo de caso 2.

4.3.1 Fase 1: Verificação Preliminar dos mecanismos de segurança do dispositivo

Os dispositivos encontravam-se com bloqueio de tela (caracteres alfanuméricos) ativado, o *bootloader* bloqueado, o modo de depuração USB desabilitado e FRP ativo. Foram identificados o modelo do dispositivo, a versão do SO, versão do Firmware e a versão do binário do Firmware.

4.3.2 Fase 2: Desmontagem do dispositivo

Não se faz necessária a aplicação desta fase para a aquisição dos dados deste modelo de dispositivo.

4.3.3 Fase 3: Verificação de compatibilidade com aplicação da técinca de JTAG

Não se faz necessária a aplicação desta fase para a aquisição dos dados deste modelo de dispositivo.

4.3.4 Fase 4: Verificação do tipo de memória do dispositivo

Não se faz necessária a aplicação desta fase para a aquisição dos dados deste modelo de dispositivo.

4.3.5 Fase 5: Verificação de mecanismo de criptografia

O dispositivo empregado no estudo de caso (SM-G532MT) usa criptografia do tipo FDE.

4.3.6 Fase 6: Download do Combination Firmware

Após a identificação em cada um dos dispositivos usados, foi realizada a pesquisa para localizar o Combination Firmware adequado e posteriormente foi realizado o download dos arquivos para o computador local.

4.3.7 Fase 7: Execução do ISP

Não se faz necessária a aplicação desta fase para a aquisição dos dados deste modelo de dispositivo.

4.3.8 Fase 8: Escrita do Combination Firmware

Para a escrita do Combination Firmware, foram necessários somente os arquivos que correspondem às partições (*boot*, *recovery* e *system*).

Foi utilizada a Box Octoplus Pro, e o utilitário *Octoplus Box Samsung Software* para substituir as partições supracitadas. Todas as configurações foram obtidas em *Seeking the Truth from Mobile Evidence.* [3].

Após substituir as partições *boot*, *recovery* e *system*, os dispositivos inicializaram sem solicitar a senha de bloqueio de tela, permitindo a visualização de arquivos de mídia, aplicativos instalados e todo o conteúdo (arquivos) presente no dispositivo, como pode ser visto na Figura 4.13.

Figura 4.13 – Tela inicial do dispositivo após a inicialização.

4.3.9 Fase 9: Aquisição de dados do dispositivo

Com o dispositivo desbloqueado, foi realizada a aquisição física utililzando o UFED Touch 2, com software versão 7.32.0.68, usando o perfil adequado para o dispositivo e a opção *Decrypted Boot Loader*.

Tal opção possibilita a aquisição com contorno do bloqueio de acesso, mas ficou provado que o emprego da metodologia possibilita a remoção do bloqueio de tela, e consequentemente outras opções de aquisição, embora a desejável é sempre a Física.

A Figura 4.14 mostra parte da tela do UFED Touch 2 e, em destaque, a funcionalidade supracitada, permitindo a Aquisição Física do SM-G532MT.

Figura 4.14 – Aquisição Física do SM-G532MT.

4.3.10 Fase 10: Análise utilizando o UFED Physical Analyzer

Os dados adquiridos foram analisados usando o software UFED Physical Analyzer Versão 7.32.0.16. Foram comparadas as análises de uma aquisição feita após o emprego da metologia proposta com uma aquisição feita antes do emprego da metodologia. O volume de dados foi exatamente o mesmo, provando a eficácia e confiabilidade proporcionada pelo emprego da metologia.

4.4 ESTUDO DE CASO 3

Neste estudo de caso, além da metodologia proposta, foram realizados também, em um dos dispositivos, o Swap lógico e em outro, o Swap físico 2.3.2, tendo em vista que dos cinco dispositivos submetidos ao experimento, dois estavam danificados.

O J2 Core (SM-J260M/DS) sai de fábrica com Android 8.1 Oreo (Go edition) e não recebeu atualização para versão superior do SO. O SoC é o Exynos 7570 Quad (14 nm), e a capacidade de armazenamento interno é de 16GB, providos por uma eMMC 5.0, com sistema de arquivos EXT4.

Todas as etapas ilustradas na Figura 4.15 foram aplicadas para validar a metodologia proposta.

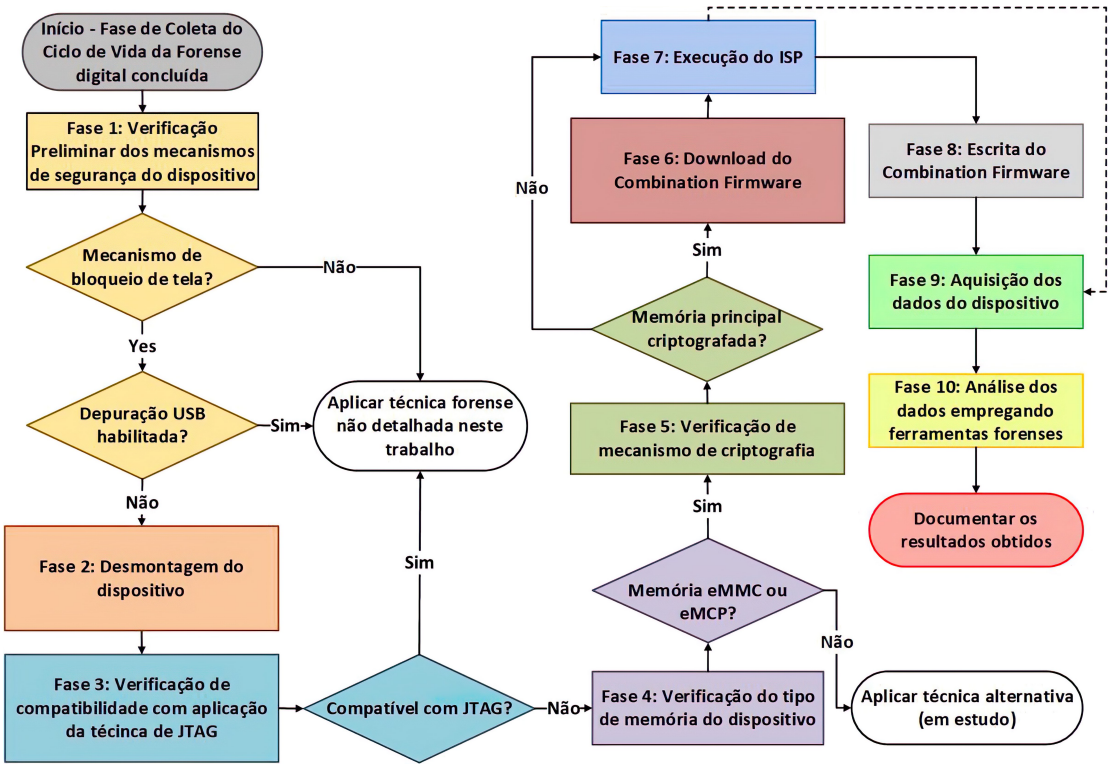

Figura 4.15 – Fluxograma de aplicação da metodologia no estudo de caso 3.

4.4.1 Fase 1: Verificação Preliminar dos mecanismos de segurança do dispositivo

O dispositivos encontravam-se com bloqueio de tela (caracteres alfanuméricos) ativado, o *bootloader* bloqueado, o modo de depuração USB desabilitado e FRP ativo.

4.4.2 Fase 2: Desmontagem do dispositivo

Para acessar a placa deste modelo de Smartphone, foi necessário remover o display, desconectar cabos e outros conectores para que nenhum componente fosse danificado durante o processo de solda. Neste modelo, a bateria é removível. Os TAPs ficam sob uma blindagem, que precisa ser removida para efetuar a solda dos condutores, como pode ser observado na Figura 4.16.

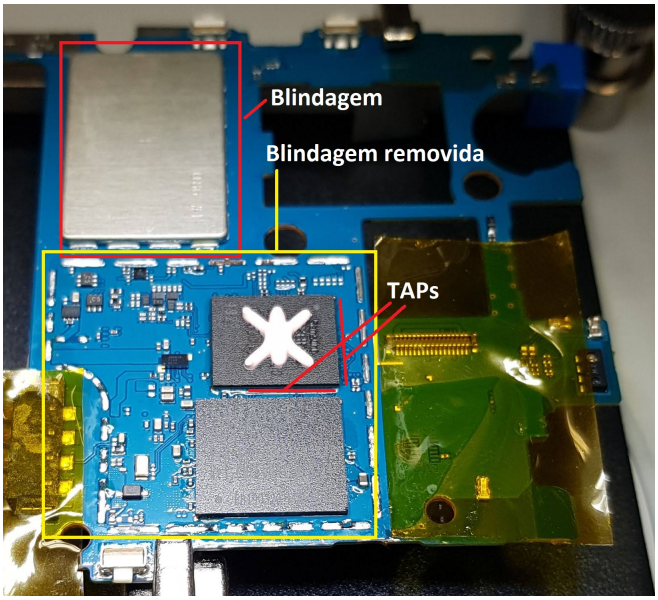

Figura 4.16 – Remoção de blindagem metálica para acesso ao TAP.

4.4.3 Fase 3: Verificação de compatibilidade com aplicação da técinca de JTAG

O modelo em questão não possui TAPs para a execução do JATG.

4.4.4 Fase 4: Verificação do tipo de memória do dispositivo

O dispositivo usado no estudo de caso possui memória do tipo eMMC 5.0.

4.4.5 Fase 5: Verificação de mecanismo de criptografia

O dispositivo empregado no estudo de caso (SM-J260M/DS) usa criptografia do tipo FDE.

4.4.6 Fase 6: Download do Combination Firmware

Após a identificação, foi feito o download do firmware original do dispositivo (na mesma versão). Fonseca [68] compartilhou seu conhecimento com este autor, o que permitiu a alteração de todos os parâmetros que precisavam ser alterados e o resultado foi uma versão aprimorada dos Combination Firmware existentes para download nos sites para manutenção de dispositivos móveis. Por se basear no firmware original, traz apenans as alterações necessárias para o contorno do bloqueio de tela imposto pelo usuário.

4.4.7 Fase 7: Execução do ISP

O procedimento realizado aqui é exatamente o mesmo do Estudo de Caso 1 [4.2]. Após a identificação dos TAPs na placa, foram realizadas as soldas dos condutores nos TAPs. Após ter soldado os condutores necessários, ligando os TAPs aos pontos correspondentes no conector ISP, o mesmo foi conectado à Box. Novamente foi utililzado o utilitário *JTAG Classic Suite*. para manipular a partição *Persist*. Os valores referentes aos parâmetros foram obtidos em *Seeking the Truth from Mobile Evidence.* [3].

No Samsung Galaxy J2 Core, a FRP é gravada dentro da Partição *Persist*. Após a configuração dos parâmetros corretos, a partição *Persist* foi sobrescrita. No entanto, a partição que armazena os dados os dados do usuário não foi manipulada, preservando a integridade.

4.4.8 Fase 8: Escrita do Combination Firmware

Para a escrita do Combination Firmware, foram necessários somente os arquivos que correspondem às partições (*boot*, *recovery* e *system*).

Em seguida, utilizamos a Box Octoplus Pro, e o utilitário *Octoplus Box Samsung Software* para substituir as partições supracitadas. Todas as configurações do software da Box foram obtidas em *Seeking the Truth from Mobile Evidence.* [3].

Após substituir as partições *boot*, *recovery* e *system*, o dispositivo inicializou sem solicitar a senha de bloqueio de tela, permitindo a visualização de arquivos de mídia, aplicativos instalados e todo o conteúdo (arquivos) presente no dispositivo.

Ressalta-se que o firmware recém instalado executa a mesma versão do Andoroid que é executado no firmware original, neste caso, a versão 8.1.

Neste caso em particular, a tela exibida se difere dos demais casos onde foi empregado o Combination Firmware desenvolvido para dispositivos Samsung. Este Firmware aprimorado mantem a aparência do Firmware original, porém não exibe os botões de navegação e ícones da barra de status, como pode ser observado na Figura 4.17.

Figura 4.17 – Galaxy J2 Core após o contorno do bloqueio por senha.

4.4.9 Fase 9: Aquisição de dados do dispositivo

Para a aquisição dos dados foi utilizado o UFED Touch 2, cuja divulgação da Cellebrite assegura que a partir da versão 7.23 do software, o UFED Touch 2, 4PC e InField teriam capacidade de realizar a aquisição física de dados de dispositivos Samsung das linhas "A" e "J" equipados com SoC *Exynos*, utilizando um perfil genérico [67]. Foram realizadas tentativas de aquisição dos dados com o dispositivo bloqueado, antes do emprego da metodologia proposta, no entanto, não houve êxito em nenhuma das tentativas.

Com o dispositivo já desbloqueado, após o emprego da metodologia proposta, utililzando o UFED Touch 2, com software na versão 7.32.0.68, foi possível realizar aquisições de Sistema de Arquivos e Lógica sem que o usuário *root* fosse habilitado.

4.4.10 Fase 10: Análise utilizando o UFED Physical Analyzer

Os dados adquiridos foram analisados usando o software UFED Physical Analyzer Versão 7.32.0.16. As aquisições dos cinco dispositivos foram analilsadas, inclusive os submetidos à técnica de Swap 2.3.2. No entanto, somente as aquisições de três dispositivos puderam ser comparadas, antes e depois do emprego da metodologia, e ambas apresentaram o mesmo

resultado.

4.5 ESTUDO DE CASO 4

Neste estudo de caso, dois dispositivos Motorola Moto G4 Plus (XT1640) foram submetidos ao emprego da metodologia proposta. Este modelo de dispositivo sai de fábrica com Android 6.0, e recebeu atualização para o Android 8.1. O SoC é o Qualcomm MSM8952 Snapdragon 617 (28 nm), e a capacidade de armazenamento interno nos dispositivos usados é de 32GB, providos por uma eMMC 5.1, com sistema de arquivos F2FS.

Todas as etapas ilustradas na Figura 4.18 foram aplicadas para validar a metodologia proposta. O experimento foi repetido cinco vezes no mesmo dispositivo.

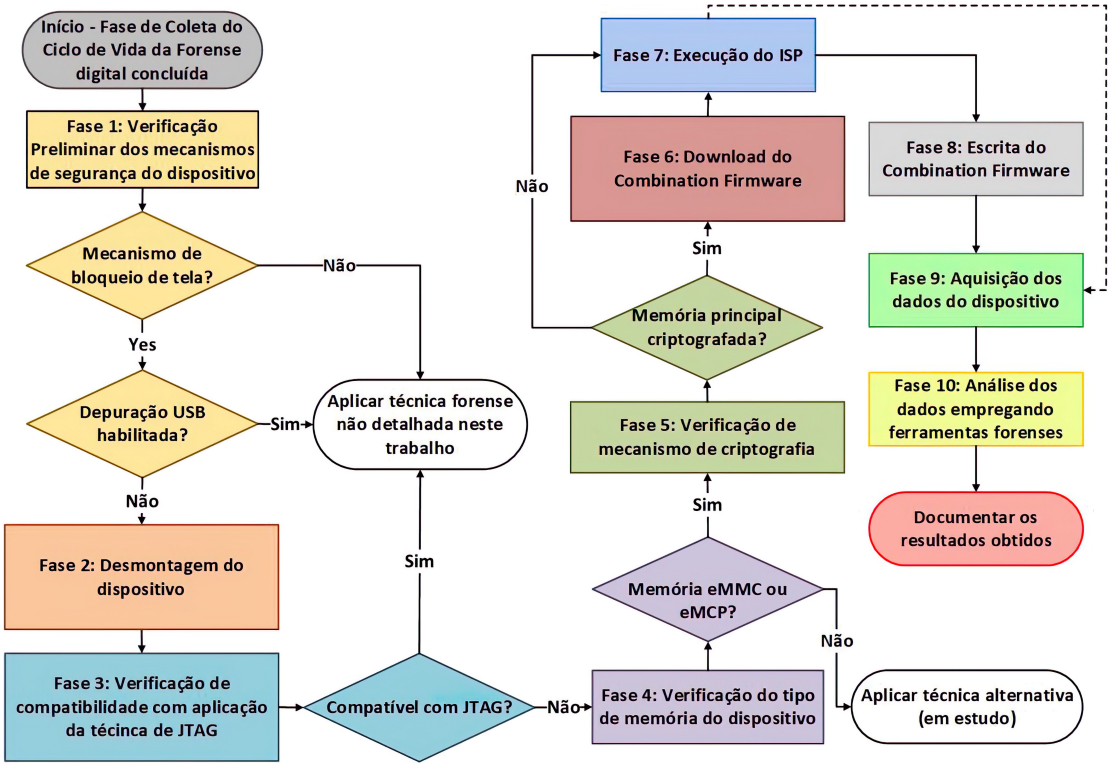

Figura 4.18 – Fluxograma de aplicação da metodologia no estudo de caso.

4.5.1 Fase 1: Verificação Preliminar dos mecanismos de segurança do dispositivo

Os dispositivos encontravam-se com bloqueio de tela (caracteres alfanuméricos) ativado, o *bootloader* bloqueado, modo de depuração USB desabilitado e FRP ativo. Nos dispositivos Motorola, para identificar a versão do Firmware é necessário inicializar em modo *fastboot*, e conectá-lo a um computador Windows ou Linux, com a ferramenta ADB instalada e executar o comando *fastboot getvar all*.

4.5.2 Fase 2: Desmontagem do dispositivo

Para acessar a placa deste modelo de Smartphone, é necessário remover o display. Além deste, foram removidos a bateria, desconectados cabos e outros conectores para que nenhum componente fosse danificado durante o processo de solda.

4.5.3 Fase 3: Verificação de compatibilidade com aplicação da técinca de JTAG

Este modelo de dispositivo não possui TAPs para a execução do JATG.

4.5.4 Fase 4: Verificação do tipo de memória do dispositivo

O dispositivo usado no estudo de caso possui memória do tipo eMMC 5.1.

4.5.5 Fase 5: Verificação de mecanismo de criptografia

O dispositivo empregado neste estudo de caso (XT1640) usa criptografia do tipo FBE, e SO Android 8.1.

4.5.6 Fase 6: Download do Combination Firmware

Neste caso, como não se trata de um dispositivo Samsung, tais firmwares recebem o nome de Firmwares Especiais. No caso deste este modelo específico, não foi necessário o download de um Firmware Especial. Os arquivos utililzados para sobrescrever as partições *boot* e *recovery* são de um firmware original, na mesma versão da usada no dispositivo.

4.5.7 Fase 7: Execução do ISP

Após identificar a localização dos TAPs na placa do dispositivo, foram realizadas as soldas dos condutores nos TAPs. Foi realizada uma aquisição física da memória principal do dispositivo utilizando o software da Box, como backup, para restauração em caso de falha no procedimento.

4.5.8 Fase 8: Escrita do Combination Firmware

Para a reescrita do firmware, são necessários somente os arquivos que correspondem às partições *boot* e *recovery*.

Após realizada a cópia da memória principal, foram sobrescritas as partições *boot* e *recovery* utilizando o software *Easy JTAG Plus*. Os valores referentes aos parâmetros de con-

figuração do software foram obtidos em *Seeking the Truth from Mobile Evidence.* [3].

Após substituir as partições *boot*, *recovery*, o dispositivo inicializou, mas ainda com o bloqueio de tela. Foi necessário reiniciar o aparelho novamente, e após o carregamento completo do SO, a senha de bloqueio de tela deixou de ser exigida.

4.5.9 Fase 9: Aquisição física usando o UFED Touch 2

Embora a Cellebrite alegue que o o UFED Touch 2, 4PC e InField são capazes de efetuar a aquisição dos dados neste modelo de dispositivo com bloqueio de tela ativado, e ainda possuir uma ferramenta para a remoção do bloqueio de tela, ambas as alternativas não funcionam até a versão 7.32.0.68.

Com o dispositivo já desbloqueado, foram realizadas as aquisições Física, de Sistema de Arquivos e Lógica, utililzando o UFED Touch 2, com software versão 7.32.0.68.

4.5.10 Fase 10: Análise utilizanAnalyzer

Os dados adquiridos foram analisados usando o software UFED Physical Analyzer versão 7.32.0.16. Todas as aquisições foram indexadas sem erros e os resultados foram consistentes, comparando as aquisições anteriores e posteriores ao emprego da metodologia proposta, incluindo as credenciais para acesso a serviços em *nuvem*, que podem ser utilizadas em aplicativos com capacidade de aquisição especificamente voltados para tais serviços, a exemplo do UFED Cloud Analyzer.

4.6 ANÁLISE COMPARATIVA E DISCUSSÕES

Após a conclusão dos estudos de caso, os resultados obtidos nas aquisições realizadas antes e depois do emprego da metodologia proposta foram comparados, e comparados também com os trabalhos relacionados. Uma discussão da metodologia proposta em relação à sua eficiência e limitações serão apresentadas.

4.7 ANÁLISE COMPARATIVA DAS CAPACIDADES DAS METODOLOGIAS E TÉCNICAS

A metodologia proposta neste trabalho amplia as possibilidades de extração de dados de dispositivos móveis, podendo a mesma ser empregada em dispositivos com diferentes características. As capacidades de aquisição, em relação às características apresentadas pelos

dispositivos são as seguintes:

- **Capacidade 1 (C1)**: Aquisição de dados de dispositivos que possuem mecanismo de bloqueio de tela ativado;
- **Capacidade 2 (C2)**: Aquisição de dados de dispositivos com criptografia de disco do tipo FDE;
- **Capacidade 3 (C3)**: Aquisição de dados de dispositivos com criptografia de disco do tipo FBE;
- **Capacidade 4 (C4)**: Aquisição de dados de dispositivos com SO até a Versão 9;
- **Capacidade 5 (C5)**: Aquisição de dados de dispositivo com memória do tipo eMMC e eMCP;
- **Capacidade 6 (C6)**: Aquisição de dados independente do fabricante do SoC;
- **Capacidade 7 (C7)**: Aquisição de dados de dispositivos com sistema de arquivos F2FS e EXT4;
- **Capacidade 8 (C8)**: Aquisição de dados de dispositivos físicos;

Com o objetivo de comparar os resultados alcançados empregando a metodologia proposta com os resultados obtidos pelas ferramentas e metodologias apresentadas nos trabalhos relacionados, a Tabela 4.1 apresenta a comparação. No que se refere à aquisição de dados de dispositivos móveis, as capacidades foram sintetizadas para facilitar a visualização do que é comum a cada trabalho referenciado.

Tabela 4.1 – Capacidades comuns à metodologia proposta e aos trabalhos relacionados.

	C1	C2	C3	C4	C5	C6	C7	C8
LLDA-ISPCF	X	X	X	X	X	X	X	X
[19]	X	-	-	-	-	X	X	X
[10]	X	-	-	-	X	-	X	X
[32]	X	X	X	-	X	-	X	X
[46]	X	X	X	-	X	-	X	X
[45]	-	-	-	-	X	X	-	X
[11]	-	X	-	-	X	X	X	X
[47]	X	-	-	-	X	X	X	X
[48]	-	-	-	-	X	X	X	X
[49]	X	-	-	-	X	X	X	X
[50]	X	-	-	-	X	X	X	X
[51]	X	-	-	-	X	X	X	X
[52]	-	-	-	-	X	X	X	-
[53]	-	-	-	-	X	X	X	X

4.8 DISCUSSÕES

Analisando os trabalhos correlatos, verifica-se que há grande esforço para o aprimoramento de ferramentas, técnicas e metodologias, buscando sempre a aquisição dos dados para a análise forense. Esse esforço se deve ao fato de que a maior dificuldade reside em transpor ou contornar mecanismos de segurança que protegem os dados do dispositivo contra acesso indevido ou não autorizado. Observa-se que tais mecanismos também dificultam a aplicação da lei, pois os especialistas encontram as barreiras citadas enteriormente mesmo quando há dispositivos e mecanismos legais que amparam e permitem ao analista o acesso a tais dados.

Dentre os mecanismos disponíveis em todos os smartphones que executam o SO Android, o bloqueio de tela, quando ativado, impede que se tenha acesso aos dados do dispositivo e suas funcionalidade. Impede ainda a comunicação pela porta USB, pois por padrão, o modo de depuração USB vem desativado. Embora as ferramentas forenses existentes no mercado prometam remover ou contornar o bloqueio de tela da esmagadora maioria dos modelos de smartphones que executam o SO Android, na prática, isso não ocorre. Em uma vasta gama de modelos, o uso das ferramentas de vários fabricantes, tais como o UFED, XRY, AXIOM, BelcaSoft, entre outras, é ineficaz na extração dos dados quando o bloqueio da tela está ativado.

Um exemplo é o modelo SM-A105 e suas variantes, cujo nome comercial é Galaxy

A10. A metodologia proposta no estudo de caso deste trabalho, utilizou esse dispositivo, que é comercializado globalmente, executa a versão 9 (Pie) do SO Android e que foi o segundo smartphone mais vendido no mundo no terceiro trimestre de 2019 [65]. Neste caso, as soluções forense convencionais somente conseguem extrair os dados se o dispositivo estiver desbloqueado.

O emprego da metodologia proposta, que combina o uso de ISP e Combination Firmware, possibilitou o contorno do bloqueio de tela, e a posterior aquisição e análise dos dados. Além disso, ressalta-se que a integridade dos dados foi preservada, o que é fundamental em análise forense.

Levando em consideração que a Samsung é o fabricante que detém a maior fatia de mercado de dispositivos móveis [6], consideramos que seu emprego pode ser uma valiosa contribuição para analistas forenses de forças de aplicação da lei, pela abrangência do número de dispositivos e pela quantidade de barreiras de segurança que seu emprego permite transpor.

No que diz respeito aos aspectos jurídicos, a metodologia proposta perimte cumprir todas as formalidades legais da Metodologia Forense 1.1, garantindo a legalildade da prova.

Do ponto de vista tecnológico, embora as ferramentas apresentadas não sejam novas, não há registrodo emprego de ISP, de Firmwares Especiais, como os Comnbination Firmware, nem acombinação dos mesmos, voltados para a área forense. Se faz necessário ratificar que o emprego da metodologia necessita de mais conhecimento, equipamentos e tempo para uso do que a funcionalidade presente no UFED que remove o mecanismo de bloqueio imposto pelo usuário, mas quenão se mostra eficaz em modelos que possuem alto volume de vendas no mercado interno e a nível global.

4.9 LIMITAÇÕES DA METODOLOGIA PROPOSTA

Em relação às limitações da metodologia, considera-se que – no melhor do conhecimento do autor e até a elaboração deste trabalho – dispositivos que utilizam memória principal do tipo *Universal Flash Storage* (UFS) ou com criptografia apoiada em *hardware* ou que não possuem todos os TAPs necessários para a execução do ISP não são compatíveis com as ferramentas empregadas na metodologia proposta. Futuras atualizações de *firmware* pelos fabricantes, como a ocorrida recentemente e que impossibilitou a aquisição em dispositivos com Android 10, podem inviabilizar o emprego da mesma em outros dispositivos ou versões do SO. Considera-se ainda o fato de que o Firmware Especial, o Combination Firmware, como são chamados os Firmwares Especiais aplicáveis em dispositvos Samsung, podem não estar disponíveis para um modelo ou fabricante específico, e seu uso combinado com

o ISP poderá requerer um estudo específico para ignorar o mecanismo de bloqueio da tela do dispositivo do qual os dados serão adquiridos. Em dispositivos Xiaomi, os resultados poderão não ser eficazes, tendo em vista que não é possível determinar qual a versão do Firmware está sendo utilizada no dispositivo e que, em alguns casos, dispositivos da Xiaomi, de um mesmo modelo, não recebem as atualizações de segurança na mesma data, podendo ocorrer hiatos de tempo de até um ano.

5 CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho, encontra-se proposta uma metodologia, denominada Low Level Data Acquisition with In-System Programing and Combination Firmware (LLDA-ISPCF), que visa contornar o bloqueio de tela de dispositivos móveis, permitindo que sejam realizadas a aquisição física, a aquisição do sistema de arquivos e a aquisição lógica dos dados. Após as respectivas aquisições, o perito pode realizar sua a análise usando ferramentas forenses especializadas.

Durante a execução do processo da metodologia proposta, é possível ainda realizar o backup das partições que serão alteradas para o emprego do Firmware Especial. Este backup pode ser restaurado após a aquisição dos dados, deixando o dispositivo exatamente como original, com o mesmo bloqueio de tela configurado pelo usuário.

A metodologia proposta é aplicável à uma vasta gama de dispositivos, tendo possibilidades de grande importância para a forense digital, pois pode possibilitar a aquisição de dados contidos em dispositivos móveis para elucidação dos mais variados crimes.

Diante dos resultados obtidos no processo de validação, por intermédio de estudos de caso, é possível ratificar a eficiência da metodologia proposta, uma vez que os objetivos propostos foram integralmnete alcançados. Isso se verifica principalmente no que se refere à possibilidade de contornar o mecanismo de bloqueio de tela, que constitui um dos maiores obstáculos no que se refere a execução da forense de dispositivos móveis. Os estudos de caso realizados para validar a metodologia proposta comprovaram que a combinação das técnicas elencadas é exequível e apresenta resultados satisfatórios, pois o emprego da metodologia proposta permitiu a aquisição dos dados do dispositivo.

No que diz respeito à criptografia, com a remoção das credenciais do usuário, a partição de dados *(/data)* é acessada sem a necessidade de realizar ataques de força bruta ou engenharia reversa do algoritmo criptográfico, ocorrendo apenas o contorno (*bypass*) do mecanismo de forma transparente.

É importante reiterar que a ferramenta usada para a extração e análise dos dados (AXIOM, XRY entre outras) fica a critéio do analista ou de acordo com a disponibilidade. Além disso, ainda é possível combinar outras ferramentas para realizar aquisições adicionais.

5.1 TRABALHOS FUTUROS

Convém ainda ressaltar que essa área do conhecimento tem a dinâmica própria de introdução de inovações nos dispositivos no mercado. Assim, em dispositivos com *patch* de segurança ou versão do binário do firmware mais recente, podem ter ocorrido mudanças na arquitetura ou na organização do sistema, cujo estudo não foi contemplado neste trabalho. Essas modificações também podem consistir na implemetação de novos mecanismos de segurança, a exemplo do AVB, que impeçam o funcionamento da metodologia da maneira exata como foi detalhada, necessitando análise de casos específicos, adversos às fases propostas.

Além desse cuidado em manter atualizada a metodologia com relação à evolução do mercado, são interessantes como trabalhos futuros, observando o crescimento do volume de vendas dos dispositivos fabricados pela Xiaomi, se acrescentar ao conjunto de técnicas já aplicadas, a substituição da partição *vbmeta* em um dispositivo Xiaomi Redmi Note 7 (M1901F7H - Android 9, SoC Qualcomm SDM660 Snapdragon 660 (14 nm). Tal estudo já está em andamento, mas não foi possível concluí-lo em tempo hábil, devido à uma atualização do AVB para a versão 2.0. Esforços também serão direcionados no aprimoramento da técnica de *Swap* em *smartphones* danificados. Por fim, pretende-se estudar técnicas que permitam a aquisição de dados de smartphones que utilizam memória do tipo *Universal Flash Storage* (UFS), cortornando o mecanismo de bloqueio de tela e o mecanismo de criptografia.

REFERÊNCIAS BIBLIOGRÁFICAS

1 LOPES, P. A. *Digital Forensic - Computational Forensic Expertise*. 2016. Available online: <https://periciacomputacional.com/pericia-forense-computacional-2/>" (accessed October 20, 2019).

2 COMPANY, M.-C. L. *VR-TABLE EMMC, JTAG, FBUS - User Manual - rev 1.0b*. 2020. Available online: <https://teeltechcanada.com/2015/wp-content/uploads/2016/09/VR-Table_user_manual_EN.pdf>" (accessed abril 20, 2020).

3 BAIR, J. *Seeking the Truth from Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations*. [S.l.]: Academic Press, 2017. ISBN 978-0128110560.

4 STATCOUNTER. *Desktop vs Mobile vs Tablet Market Share Worldwide*. 2020. Available online: <https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet>" (accessed February 28, 2020).

5 VARGAS, F. G. *30ª Pesquisa Anual do FGVcia da FGV/EAESP, 2019*. 2019. Available online: <https://eaesp.fgv.br/sites/eaesp.fgv.br/files/noticias2019fgvcia_2019.pdf>" (accessed January 19, 2020).

6 STATCOUNTER. *Mobile Vendor Market Share Worldwide*. 2019. Available online: <https://gs.statcounter.com/vendor-market-share/mobile>" (accessed February 28, 2020).

7 STATCOUNTER. *Operating System Market Share Worldwide*. 2019. Available online: <https://gs.statcounter.com/os-market-share>" (accessed February 28, 2020).

8 KINGSTON, C. *The Future of Mobile Forensics*. Dissertação (Mestrado) — Utica College, 2018. [Google Scholar].

9 SILVEIRA, C. M. da et al. Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware. *Applied Sciences*, Multidisciplinary Digital Publishing Institute, v. 10, n. 12, p. 4231, 2020.

10 WU, S. et al. A general forensics acquisition for android smartphones with qualcomm processor. In: IEEE. *2017 IEEE 17th International Conference on Communication Technology (ICCT)*. [S.l.], 2017. p. 1984–1988. ISBN 978-1-5090-3944-9. ISSN 2576-7828.

11 PAPPAS, S. *Investigation of JTAG and ISP Techniques for Forensic Procedures*. Dissertação (Mestrado) — University of Tartu, 2017.

12 FILHO, J. E. M. *Discovering Linux-3rd Edition: Understand the GNU/Linux operating system*. [S.l.]: Novatec Editora, 2012. ISBN 978-85-7522-278-2.

13 RAO, V. V.; CHAKRAVARTHY, A. Survey on android forensic tools and methodologies. *International Journal of Computer Applications*, v. 154, n. 8, p. 17–21, 2016. ISSN 0975–8887.

14 Ajijola, A.; Zavarsky, P.; Ruhl, R. A review and comparative evaluation of forensics guidelines of nist sp 800-101 rev.1:2014 and iso/iec 27037:2012. In: IEEE. *World Congress on Internet Security (WorldCIS-2014)*. [S.l.], 2014. p. 66–73. ISBN 978-1-908320-42-1.

15 AYERS, R. P.; BROTHERS, S.; JANSEN, W. *Guidelines on mobile device forensics*. [S.l.], 2014.

16 STANDARDIZATION, I. O. for. *ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. 2012. Available online: <https://www.iso.org/standard/44381.html>" (accessed October 20, 2019).

17 NEUNER, S.; SCHMIEDECKER, M.; WEIPPL, E. Effectiveness of file-based deduplication in digital forensics. *Security and Communication Networks*, v. 9, n. 15, p. 2876–2885, 2016.

18 BREZINSKI, D.; KILLALEA, T. *RFC 3227 - Guidelines for Evidence Collection and Archiving*. 2002. Available online: <https://tools.ietf.org/html/rfc3227>" (accessed October 20, 2019).

19 YANG, S. J. et al. New acquisition method based on firmware update protocols for android smartphones. *Digital Investigation*, Elsevier, v. 14, p. S68–S76, 2015.

20 BOX, O. *Octoplus PRO Box*. 2019. Available online: <https://octoplusbox.com/pt/products/products/>" (accessed October 20, 2019).

21 UFI-BOX. *UFI BOX Overview*. 2019. Available online: <https://www.ufi-box.com/pages/ufi-box-features>" (accessed October 20, 2019).

22 EASYJTAG. *EasyJTAG Plus Box Hardware*. 2019. Available online: <http://easy-jtag.com/easyjtag-2nd-generation-hw/>" (accessed October 20, 2019).

23 AFONIN, O.; KATALOV, V. *Mobile Forensics – Advanced Investigative Strategies*. Packt Publishing, 2016. ISBN 9781786464088. Disponível em: <https://books.google.com.br/books?id=9oVcDgAAQBAJ>.

24 DI, C. *UFED Ultimate*. 2019. Available online: <https://www.cellebrite.com/pt/ufed-ultimate-4/>" (accessed January 22, 2020).

25 SYSTEMATION, M. *XRY*. 2020. Available online: <https://www.msab.com/>" (accessed January 22, 2020).

26 INC., M. F. *Magnet AXIOM*. 2020. Available online: <https://www.magnetforensics.com/products/magnet-axiom/>" (accessed January 22, 2020).

27 MORGILLO, I.; VIOLA, S. *Learning Embedded Android N Programming*. Packt Publishing Ltd, 2016. ISBN 9781785283284. Disponível em: <https://books.google.com.br/books?id=bOrUDQAAQBAJ>.

28 PARRY, T. O.; CARTER, J. L. *Updating firmware on mobile devices*. Google Patents, 2015. US Patent 9,069,641. Disponível em: <https://patentimages.storage.googleapis.com/40/76/1e/206e74a65129e2/US9069641.pdf>.

29 XDA-DEVELOPERS. *xdadevelopers*. 2020. Available online: <https://www.xda-developers.com/>" (accessed January 22, 2020).

30 ALMEHMADI, T.; BATARFI, O. Impact of android phone rooting on user data integrity in mobile forensics. In: IEEE. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. [S.l.], 2019. p. 1–6. ISBN 978-1-7281-0108-8.

31 LOFTUS, R. et al. *Android 7 File Based Encryption and the Attacks Against It*. 2017.

32 ALENDAL, G.; DYRKOLBOTN, G. O.; AXELSSON, S. Forensics acquisition—analysis and circumvention of samsung secure boot enforced common criteria mode. *Digital Investigation*, Elsevier, v. 24, p. S60–S67, 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1742287618300409>.

33 CO., S. E. *File-based encryption (FBE) and full-disk encryption (FDE)*. 2020. Available online: <https://support.samsungknox.com/hc/en-us/articles/360039577713-File-based-encryption-FBE-and-full-disk-encryption-FDE->" (accessed March 28, 2020).

34 RUBINOV, K. et al. Automated partitioning of android applications for trusted execution environments. In: IEEE. *2016 IEEE/ACM 38th International Conference on Software Engineering (ICSE)*. [S.l.], 2016. p. 923–934. ISBN 978-1-4503-3900-1. ISSN 1558-1225.

35 LEIGNAC, P. et al. Comparison of side-channel leakage on rich and trusted execution environments. In: *Proceedings of the Sixth Workshop on Cryptography and Security in Computing Systems*. [S.l.: s.n.], 2019. p. 19–22.

36 HAY, R. fastboot oem vuln: Android bootloader vulnerabilities in vendor customizations. In: *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. Vancouver, BC: USENIX Association, 2017. Disponível em: <https://dl.acm.org/doi/abs/10.5555/3154768.3154790>.

37 WEISS, B. An investigative study on android verified boot process. Creative Components, 2019. Disponível em: <https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1233&context=creativecomponents>.

38 LLC, G. *Android Verified Boot 2.0*. 2020. Available online: <https://android.googlesource.com/platform/external/avb/+/master/README.md>" (accessed June 22, 2020).

39 ELENKOV, N. *Android security internals: An in-depth guide to Android's security architecture*. [S.l.]: No Starch Press, 2014.

40 KHAN, A.; MANSURI, Z. H. Comparative study of various digital forensics logical acquisition tools for android smartphone's internal memory: a case study of samsung galaxy s5 and s6. *International Journal of Advanced Research in Computer Science*, v. 9, n. 1, p. 357–369, 2018. ISSN 0976-5697. Disponível em: <http://www.ijarcs.info/index.php/Ijarcs/article/view/5303>.

41 STANDARDS, N. I. of; TECHNOLOGY. *Test Results for Binary Image JTAG, Chip-Off Decoding and Analysis Tool Paraben's Electronic Evidence Examiner*. 2019. Available online: <https://www.dhs.gov/publication/st-binary-image-jtag-chip-decoding-and-analysis-tool-paraben-s-electronic-evidence>" (accessed February 28, 2020).

42 DEPARTMENT, M. of J. F. P. *CGTI - General Coordination of Information Technology - IPED*. 2020. Available online: <https://servicos.dpf.gov.br/ferramentas/IPED/>" (accessed February 28, 2020).

43 MARTELLI, A. et al. Análise de metodologias para execução de pesquisas tecnológicas/analysis of methodologies for carrying out technological research. *Brazilian Applied Science Review*, v. 4, n. 2, p. 468–477, 2020. ISSN 2595-3621.

44 LACERDA, R. T. d. O.; ENSSLIN, L.; ENSSLIN, S. R. Uma análise bibliométrica da literatura sobre estratégia e avaliação de desempenho. *Gestão & Produção*, SciELO Brasil, v. 19, n. 1, p. 59–78, 2012. ISSN 0104-530X.

45 LI, Z.; XI, B.; WU, S. Digital forensics and analysis for android devices. In: IEEE. *2016 11th International Conference on Computer Science & Education (ICCSE)*. 2016. p. 496–500. ISBN 978-1-5090-2218-2. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7581630>.

46 TIAN, D. et al. Attention spanned: comprehensive vulnerability analysis of at commands within the android ecosystem. In: *Proceedings of the 27th USENIX Conference on Security Symposium*. [s.n.], 2018. p. 273–290. ISBN 978-1-939133-04-5. Disponível em: <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-tian.pdf>.

47 SATHE, S. C.; M., D. N. Data acquisition techniques in mobile forensics. In: ICISSP. *Second International Conference on Inventive Systems and Control*. [S.l.], 2018. p. 280–286. ISBN 978-1-5386-0807-4.

48 CHANAJITT, R.; VIRIYASITAVAT, W.; CHOO, K.-K. R. Forensic analysis and security assessment of android m-banking apps. *Australian Journal of Forensic Sciences*, Taylor & Francis, v. 50, n. 1, p. 3–19, 2018. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/00450618.2016.1182589>.

49 FONSECA, D. B. Mobile forensics extraction from damaged android device. *Digital 4n6 Journal*, Digital 4n6 Journal, v. 4, n. 1, p. 40–43, 2019. Disponível em: <https://www.digital4n6journal.com/product/1_yr_ebook-4-issues/>.

50 FONSECA, D. B. Data extraction from water damaged moto g1. *Digital 4n6 Journal*, Digital 4n6 Journal, v. 4, n. 2, p. 34–36, 2019. Disponível em: <https://www.digital4n6journal.com/product/1_yr_ebook-4-issues/>.

51 STANDARDS, N. I. of; TECHNOLOGY. *NIST Tests Forensic Methods for Getting Data From Damaged Mobile Phones*. 2020. Available online: <https://www.nist.gov/news-events/news/2020/01/nist-tests-forensic-methods-getting-data-damaged-mobile-phones>" (accessed February 28, 2020).

52 SOARES, A. M. M.; JR, R. T. de S. A technique for extraction and analysis of application heap objects within android runtime (ART). In: *ICISSP*. [S.l.: s.n.], 2017. p. 147–156. ISBN 978-989-758-209-7.

53 SOARES, A. M. M.; JR, R. T. de S. Forensic analysis of android runtime (ART) application heap objects in emulated and real devices. In: SPRINGER, CHAM. *International Conference on Information Systems Security and Privacy*. 2017. p. 130–147. ISBN 978-3-319-93354-2. Disponível em: <https://link.springer.com/book/10.1007/978-3-319-93354-2>.

54 VELHO, J. A. et al. Tratado de computação forense–millenium editora. *São Paulo*, 2016.

55 PEREIRA, K. da S.; OLIVEIRA, F. M. de. Perícia forense computacional e crimes cibernéticos. *Revista Interdisciplinar Pensamento Científico*, v. 5, n. 2, 2019.

56 PúBLICA, M. da Justiça e S. *Portaria n° 82, de 16 de Julho de 2014-SENASP/MJ*. 2014. Available online: <https://www.justica.gov.br/Acesso/convenios/portaria-convenios-pericia-2014-versao-29-07-14.doc>" (accessed June 20, 2020).

57 TIMES, T. *F.B.I. Finds Links Between Pensacola Gunman and Al Qaeda.* 2020. Available online: <https://www.nytimes.com/2020/05/18/us/politics/justice-department-al-qaeda-florida-naval-base-shooting.html>" (accessed June 02, 2020).

58 DI, C. *Celebrite - Home*. 2020. Available online: <https://www.cellebrite.com/en/home/>" (accessed January 22, 2020).

59 CELLEBRITE. *Cellebrite Advanced Services Brazil*. 2020. Available online: <https://www.cellebrite.com/en/advanced-services/cas-latam/>" (accessed January 22, 2020).

60 CELLEBRITE. *Serviços avançados da Cellebrite*. 2020. Available online: <https://www.cellebrite.com/pt/cas-sales-inquiry-pt/>" (accessed January 22, 2020).

61 GRAYSHIFT. *Introducing GrayKey*. 2020. Available online: <https://graykey.grayshift.com/>" (accessed January 22, 2020).

62 SKULKIN, O.; TINDALL, D.; TAMMA, R. *Learning Android Forensics: Analyze Android devices with the latest forensic tools and techniques, 2nd Edition*. Packt Publishing, 2018. ISBN 9781789137491. Disponível em: <https://books.google.com.br/books?id=cfOBDwAAQBAJ>.

63 SUPPORT, H. *Halabtech Support - Home*. 2020. Available online: <https://support.halabtech.com/>" (accessed January 22, 2020).

64 PROJECT, A. O. S. *Partições e Imagens*. 2020. Available online: <https://source.android.com/devices/bootloader/partitions-images>" (accessed January 19, 2020).

65 COUNTERPOINT. *iPhone XR was the Top-Selling Model Globally in Q3 2019*. 2019. Available online: <https://www.counterpointresearch.com/iphone-xr-top-selling-model-globally-q3-2019/>" (accessed January 02, 2020).

66 STATCOUNTER. *Mobile & Tablet Android Version Market Share Worldwide*. 2019. Available online: <https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide>" (accessed January 19, 2020).

67 CELLEBRITE. *Exclusive access to untouched evidence in Samsung Exynos devices*. 2019. Available online: <https://www.cellebrite.com/en/productupdates/exclusive-access-to-untouched-evidence-in-samsung-exynos-devices/>.

68 FONSECA, D. B. *Electronic Technician at MDR Service Center*. 2020. Available online: <https://www.linkedin.com/in/djalma-fonseca-49722b113/>" (accessed June 02, 2020).