TÉCNICAS AVANÇADAS DE EXTRAÇÃO DE DADOS

ADVANCED DATA EXTRACTION TECHNIQUES

STANLEY GUSMÃO DE PAIVA[1]

Resumo

Este ensaio tem o objetivo apresentar diferentes técnicas de extração de dados que podem ser utilizadas em dispositivo eletrônico, além de discorrer sobre quais delas devem ser usadas considerando-se os tipos de aparelhos, técnicas de segurança de acesso e das condições físicas dos equipamentos apreendidos. Sugere-se uma triagem para definição de quais processos devem ser empregados a cada dispositivo eletrônico, para que não ocorra perda de dados, e salienta-se a importância da instauração da cadeia de custódia que demostra o histórico da apreensão até o descarte dos dispositivos. Os resultados demonstram que sem o emprego das técnicas corretas as informações constantes nos dispositivos podem ser perdidas, não contribuindo dessa forma para a resolução de crimes ou antecipação de tomadas de decisões por parte das autoridades competentes.

Palavras-chave: Inteligência penitenciária. Extração de dados. Dispositivos eletrônicos.

Abstract

This essay aims to present different data extraction techniques that can be used in electronic devices, in addition to discussing which of them should be used considering the types of devices, access security techniques and the physical conditions of the seized equipment. A screening is suggested to define which processes should be used for each electronic device, so that data loss does not occur, and the importance of establishing the chain of custody is highlighted, which demonstrates the history of the seizure until the disposal of the devices.The results show that without the use of correct techniques, the information contained in the devices can be lost, thus not contributing to the resolution of crimes or anticipation of decision-making by the competent authorities.

***Keywords**: Penitentiary intelligence. Data extraction. Electronic devices.*

1 Policial Penal da Secretaria de Estado da Administração Penitenciária da Paraíba – SEAP/PB. Graduado em Sistema de Informação pela Faculdade Joaquim Nabuco, MBA Executivo em Gestão da Tecnologia da Informação pela Universidade Federal de Pernambuco, Pós-Graduação Inteligência Prisional, de Segurança Pública e de Estado pela Faculdade de Comunicação Tecnológica de Olinda – Facottur. E-mail: stanley-pe@hotmail.com. ORCID: 0000-0002-0874-2805.

ISSN 2675-1895
ISSN Eletrônico 2675-1860

INTRODUÇÃO

O ensaio objetiva demonstrar as metodologias de extração de dados avançadas como ferramenta de apoio, que subsidiará com os dados extraídos, ações preventivas, ostensivas e a tomada de decisões em prol do Sistema Penitenciário e da segurança pública. Sem a utilização da técnica apropriada, dados relativos às facções, cometimentos de crimes, faltas disciplinares e a interlocução entre apenados podem ser perdidos.

O ensaio apresenta ainda os processos, as técnicas, os possíveis dados que podem ser extraídos dos dispositivos, a implementação da perícia forense digital, a cadeia de custódia e seu embasamento jurídico. Serão apresentadas as técnicas utilizadas e os resultados obtidos em 3 anos de atuação da Gerência de Inteligência e Segurança Orgânica Penitenciária (GISOP) e da Secretária de Estado da Administração Penitenciária da Paraíba (SEAP/PB).

Desde o final de 2018 a SEAP/PB, junto com a GISOP vem selecionando policiais penais que tenham a expertise em técnicas de extração de dados e uso de tecnologia correlacionadas, para que possam estar buscando um diferencial na área entre membros da inteligência. A busca contínua de qualificação de seus profissionais tem o intuito de buscar a excelência na obtenção de dados extraídos, onde mais dados extraídos, analisados, podem gerar mais informações e conhecimento, que além de facilitar a tomada de decisão no combate criminal a partir das prisões podem auxiliar toda a cadeia de segurança pública estadual.

O texto está dividido em quatro blocos: (I) Pericia forense, que realiza um pequeno resgate da etimologia da palavra, além de contextualizar temas imbricados em sua realização, como perícia forense digital, cadeia de custódia e as fases da investigação forense; (II) Técnicas de extração de dados, onde são abordados as principais técnicas utilizadas para a realização da extração de dados, além de apresentar algumas delas, como a manual, lógica, física, avançada (*chip off, JTAG, e ISP) e Micro leitura; (III) Possíveis dados extraídos e (IV) Discussão.*

1. A PERÍCIA FORENSE

Cretella e Cintra (1959), define a perícia como ciência experimental, como conhecimento, já o termo forense é definido como foro judicial. Segundo o autor, a ciência forense é atividade do perito, o co-

nhecedor, o inteligente, o sábio. Logo, a ciência forense é o conjunto de métodos e técnicas cientificas aplicadas para a resolução de crimes, que abrange diversas áreas afins. O termo vem sendo usado desde a antiguidade e sofreu transformações com o tempo como exposto a seguir:

- Archimedes (287-212 a.C.) verificava a quantidade real de ouro da Coroa calculada pela teoria do peso específico dos corpos.

- Impressões digitais utilizadas no século VII como comprovação de débito.

- Medicina e Entomologia – afogamento e estudos pulmonares e cartilagens do pescoço e sobre insetos na cena do crime que podem datar dia e hora do acontecido.

- Evolução da Ciência Forense – identificação de tipos sanguíneos publicação de normas que referenciam as investigação e utilização de técnicas forenses em diversas áreas criada pelo Polícia Federal Norte Americana.

Atualmente, a forense é dividida em diversos segmentos por área de atuação cada vez mais específica como são os casos da forense toxicológica, podologia, patologia, optometria, odontologia, linguística, geologia, entomologia, engenharia, análise de *DNA*, botânica, arqueologia, antropologia, criminalística e a digital dentre outras.

1.1 Perícia Forense Digital

Inicialmente necessitamos compreender a definição da ciência forense digital Casey (2011) a define como um ramo da Ciência Forense que trata da análise e investigação de conteúdos associados a dispositivos digitais. E, em complemento, Carrier (2006) define a investigação forense digital sendo um processo de responder perguntas sobre estados e eventos digitais, onde os resultados são conseguidos de maneira forense os procedimentos e técnicas utilizados permitem obter resultados a serem utilizados em tribunal.

Desde a década de 1970, com a evolução das tecnologias, a investigação forense digital passa por diversos desafios, como o crescimento na capacidade de armazenamento, segurança, meios de comunicação social e armazenamento em algum tipo de mídia. Segundo Carrier (2006), as perícias forenses digitais podem ser utilizadas em investigações em geral, espionagem, roubo de identidade e de informações, extorsão, ameaça,

uso indevido de recursos, chantagem, calúnia, difamação, injúria por meio virtual, pedofilia, fraudes, tráfico de drogas, remoção de arquivos, dentre outros.

1.2 Cadeia de Custódia

A cadeia de custódia é um procedimento de grande importância para uma investigação, desde a etapa de coleta até o descarte da evidência que deve ser utilizada em todo processo, embasando os procedimentos de investigação que se baseiam na Lei 13.964/19 – Capítulo II. A lei estabelece diretrizes acerca, do exame de corpo de delito, da cadeia de custódia e das perícias em geral onde em seu artigo 158-A até o 158-F, *in verbis*, bem como a ISO/IEC 27037, 2012 tratam sobre o assunto.

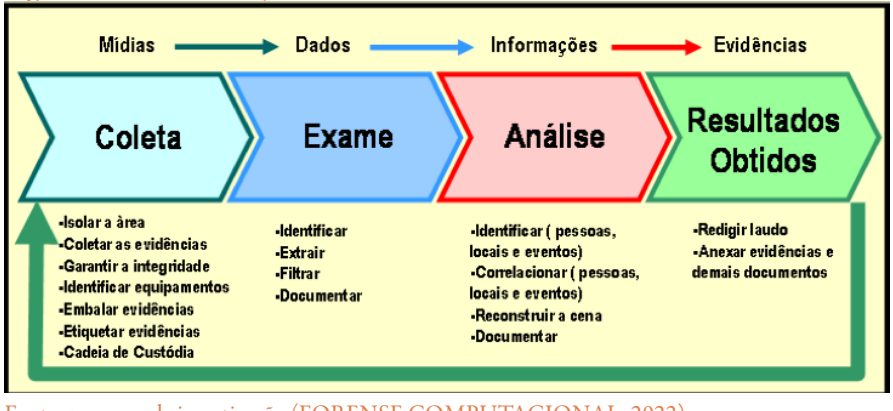
> Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. E seus parágrafos tratam da descrição, do agente público e dos vestígios.
>
> Art. 158-B. A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas: I – reconhecimento; II – isolamento; III – fixação; IV – coleta; V – acondicionamento; VI – transporte; VII – recebimento; VIII – processamento; IX – armazenamento e X – descarte.
>
> Art. 158-C. A coleta dos vestígios deverá ser realizada preferencialmente por perito oficial, que dará o encaminhamento necessário para a central de custódia, mesmo quando for necessária a realização de exames complementares. E seus parágrafos tratam do tratamento dos vestígios.
>
> Art. 158-D. O recipiente para acondicionamento do vestígio será determinado pela natureza do material. E seus parágrafos tratam dos recipientes para o acondicionamento.
>
> Art. 158-E. Todos os Institutos de Criminalística deverão ter uma central de custódia destinada à guarda e controle dos vestígios, e sua gestão deve ser vinculada diretamente ao órgão central de perícia oficial de natureza criminal. E seus parágrafos tratam dos locais de armazenamentos.
>
> Art. 158-F. Após a realização da perícia, o material deverá ser devolvido à central de custódia, devendo nela permanecer. E seus parágrafos tratam do retorno do material após a perícia, sua guarda até o seu descarte.

A lei é sábia em especificar de forma detalhada a cadeia de custódia, demonstrando o histórico da evidência desde a coleta até o descarte definitivo, sendo exposto as datas e pessoas que tiveram acesso com suas fases bem discriminadas, acondicionamentos de acordo com os materiais e armazenamento em locais apropriados, conferindo credibilidade às evidências, podendo ou não serem utilizadas novamente em novas situações ou contraprova, as quais veremos mais detalhados adiante.

1.3 Fases da investigação

As fases de uma investigação forense digital devem ser bem divididas e seus subitens respeitados para gerar evidências robustas sem vícios e com resultados satisfatórios que possam ser repetidas.

Figura 1: Fases da extração de dados



Fonte: processo de investigação (FORENSE COMPUTACIONAL, 2022).

- Coleta

Considerada uma fase de grande importância, tem início no isolamento da área, da coleta das evidências, da garantia da integridade do material coletado, prosseguindo para as fases futuras, as coletas não devem sofrer nenhum tipo de alteração durante todo o processo, devendo ser criada uma cópia idêntica a original *bit a bit*, efetuando a extração do código de verificação conhecido como hash. Após a finalização da coleta realiza-se a identificação e acondiciona o dispositivo eletrônico, lacrando e guardando em local apropriado até decisão superior do que será realizado, mantendo sempre a cadeia de custódia atualizada as informações e manuseios registrados.

- Exame

É nessa fase em que ocorre efetivamente a extração de dados digital, estágio em que se realiza a recuperação e catalogação de tudo que for encontrado no dispositivo eletrônico, recordando continuamente que deve ser utilizada a cópia feita na fase da coleta, objetivando manter a integridade do material original. Como orienta Franco (2016), nessa fase se busca o maior número de informações possíveis, visíveis ou ocultas, podendo utilizar a técnica de *Data Carving*, que busca recuperar os dados apagados tornando visível.

- Análise

Etapa onde é feita uma busca detalhada no material extraído na fase anterior, devendo ser mais delicada e atenciosa. Esta etapa pode ser refinada com programas que filtram palavras-chave, programas escondidos, arquivos com estenografia e ou criptografia. Busca-se identificar pessoas, locais e eventos bem como correlacionar situações e tentar reconstruir o cenário do fato (BRASIL, 2013).

- Resultado

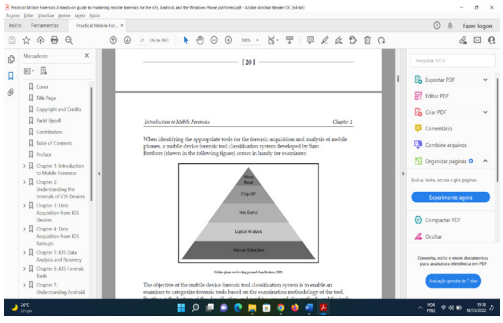
Última fase da perícia, onde ocorre a elaboração do relatório em que são transcritas as evidências analisadas que serão levadas às vias judiciais, devendo ser redigido com maior clareza e concisão, apresentando uma conclusão imparcial (BRASIL, 2013).

2. TÉCNICAS DE EXTRAÇÃO DE DADOS

São várias as técnicas que podem ser utilizadas para a extração de dados, sendo citado pelo prof. Jorge que a "melhor técnica com o menor risco possível, mesmo que dela resulte um padrão de dados não ideal ao que deseja, mas que ela seja segura e os dados estejam preservados." (RAMOS,2022). Sempre obedecendo do menor risco para o mais arriscado e que os privilégios devem ser ultrapassados com cautela desde uma simples acesso por senha, implementação de acesso root, extração manual, por software e técnicas avançadas.

As técnicas foram evoluindo com o advento das tecnologias para obter melhores resultados, de acordo com as características e estado de cada dispositivo. As técnicas podem ser Manual, Lógica, Física, Avançada (Chip Off, JTAG e ISP) e Micro Leitura, como demostra a figura.

Figura 2: Tipos de técnicas de extração de dados



Fonte: *Introduction to Mobile Forensics - Chapter* 1, pag. 21.

2.1 Técnica Manual

O método busca analisar o dispositivo móvel de forma manual, adentrando em seus aplicativos através de teclado ou tela. Todo procedimento é registrado por fotos e *backup d*e forma manual, extraído em mídia de armazenamento externo, executada de forma rápida e fácil. Nessa etapa pode ocorrer falhas, visto que se trata de processo manual, realizado por efetivo humano.

Tamma (2018) ratifica que a técnica manual não permite que sejam recuperados dados apagados pelo usuário e só deve ser usada em último caso pois tem como falha o fator humano que é suscetível a erros e consome muito tempo.

2.2 Técnica Lógica

Como parte do processo de extração, os dados são recolhidos por meio de uma conexão USB *(Universal Serial Bus)* ou *bluetooth*, via *software* forense, onde há comunicação de envio e recebimento de comandos que realizam a extração de dados para uma análise futura, sendo compatíveis com a maioria dos dispositivos e requer pouco treinamento para executá-la. Como a técnica manual, essa técnica não consegue recuperar dados apagados pelo usuário.

Segundo Tamma (2016) são usados *Application Programming Interface* (API's), aplicativos das fabricantes dos softwares instalados nos aparelhos, os quais possuem arquivos do sistema, montando assim as partições do sistema operacional, podendo trazer dados apagados.

2.3 Técnica Física

A extração é realizada por meio de *software* forense conectado ao dispositivo. Nessa técnica ocorre troca de comandos em baixo nível, extraindo na forma binária (*bit-a-bit*), que permite a recuperação de dados excluídos em espaço não alocado, trazendo o conteúdo de memória do dispositivo.

Tamma (2016), esclarece que é o procedimento mais utilizada hexadecimal[2] *Dump* que envia o programa *bootloader* para a *Random Access Memory* (RAM) do dispositivo, que consegue superar o bloqueio do dispositivo, e, em alguns casos em que o sistema não aceita o *bootloader* são instalados outros programas temporários para ter acesso aos dados (TAMMA, 2016).

2.4 Extração avançada: *ChipOff*, JTAG e ISP

A extração de dados mobile em ambiente avançado pode ser definida como sendo aquela em os níveis de conhecimento e ferramentas clássicas de extração não conseguem surtir efeito necessário ao resultado esperado pelas forças da lei. (RAMOS,2022)

As técnicas avançadas, possibilitam o acesso direto à memória do dispositivo, podem ocorrer de 3 (três) modos ChipOff, JTAG e ISP.

As técnicas começaram a ganhar maior ênfase na década de com a utilização de celulares para detonar artefatos explosivos à distância nas investigações do *Federal Bureau of Investigation* (FBI), na tentativa de reconstruir aparelhos e conseguir extrair os dados, pois a técnica de *Chip Off*[3] [2] só era utilizada para ter acesso aos dados dos dispositivos. A tabela 1 mostra a evolução das técnicas avançadas de extração de dados, suas utilidades e características (Academia Forense Digital – AFD, 2020).

2 O Hexadecimal é o sistema de numeração muito utilizado na programação de microprocessadores, em especial nos equipamentos e máquinas de estudo e sistemas de desenvolvimento. Trata-se de um sistema de numeração posicional que representa os números em base 16, sendo assim, utilizando 16 símbolos. Este sistema utiliza os símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 do sistema decimal, além das letras A, B, C, D, E e F.

3 *Chip Off* é uma técnica de extração avançada de dados em dispositivos eletrônicos que consiste na retirada do chip conhecido como Emmc e acondicionado em adaptadores para a extração binária.

Tabela 1: Técnicas de extração de dados

Chip Off **Chip Fora**	**JTAG** - ***Join Test Action Group*** **Grupo de Ação de Teste Conjunto**	**ISP** - ***In System Programming*** **Programação no Sistema**
1980	1985	1990
Criado para ter acesso a dados armazenados ao eMMC	Criado para ter acesso a placa e testar algum tipo de defeito.	Evolução do protocolo JTAG
Utilizado	Ainda utilizado	Utilizado
Retirada do e*MMC* a frio (raspagem) e a calor	12 a 20 pontos de conexão	06 pontos de conexão
Velocidade alta	Velocidade baixa	Maior velocidade
Não precisa da placa e nem do processador	Placa, Processador e e*MMC* tem que estar funcionando	Placa e eMMC tem que estar funcionando

Fonte: produzido pelo autor, baseadas nas características propostas pela apostila da Academia Forense Digital.

2.4.1 Intervenção *Chip Off*

Técnica mais antiga, teve início na década de 1980. Criada para ter acesso aos dados diretamente armazenados, consiste na retirada física da memória do *Embedded Multimedia Card* (eMMC), que é um tipo de memória *flash*, onde o acesso é realizado por meio de pontos na placa do dispositivo.

Considerada uma técnica destrutiva e de alto risco é realizada manualmente usando calor, meio de ondas de radiação ou raspagem da placa para a retirada da memória, que posteriormente é lida por um adaptador via USB ou outro dispositivo. Essa técnica só é utilizada em último caso, visto que perde todo o funcionamento do dispositivo, exigindo cautela em sua extração para não danificar a eMMC, que passa pelo processo de análise, decodificação e interpretação.

A técnica é a única opção em dispositivos eletrônicos danificados fisicamente por oxidação, por contato com água ou fogo por longos períodos ou por contato com material corrosivo. Após a extração é criado o código *hash* de imagem binária para comprovar a integridade dos dados. A técnica de *Chip Off* só é utilizada para aparelhos que possuam instalados as versões do sistema Android 7, por conta do sistema de segurança dos dados (Academia Forense Digital – AFD, 2020) (TAMMA, 2018).

A sigla eMMC refere-se ao cartão multimídia embutido que possui diversas capacidades de armazenamento, variando de 4 Gb a 128 Gb, e é capaz de atingir velocidade de transferência de até 400 MB/s com um valor de baixo custo, sendo considerada um tipo de memória *flash* embarcada não volátil, presente *pen drives*, *smartphones*, televisores e geladei-

ras inteligentes, central multimídia, *tablets, notebooks smartwatch*, drones e outros dispositivos eletrônicos e usados no IoT (Internet das Coisas).

Figura 3: Dispositivos Eletrônicos que utilizam eMMC

Fonte: produzida pelo autor, baseado em imagens disponíveis do Google

Existem diversos modelos de adaptadores de eMMC (100, 153, 162, 168,169,186,221, 254 e 529), que modificam pela pinagem e pelo tamanho.

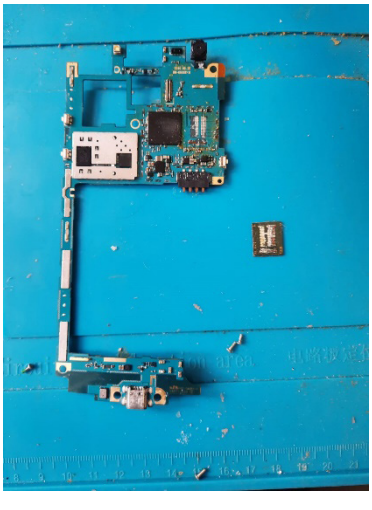
Figura 4: Aparelho celular apreendido em unidades prisionais que foram submetidos à técnica Chip-Off

Fonte: produzida pelo autor.

Figura 5: Aparelho celular desmontado

Fonte: produzida pelo autor.

Figura 6: Extração da eMMC da placa



Fonte: produzida pelo autor.

2.4.2 Técnica *Join Test Action Group* (JTAG)

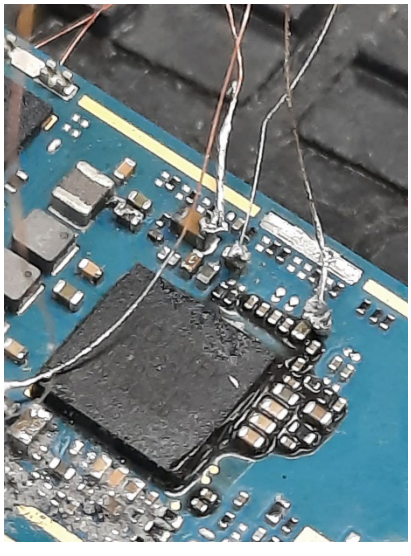
Essa técnica foi criada em 1985 com o intuito obter acesso físico ao circuito integrado do dispositivo e verificar algum tipo de defeito com comunicação em duas vias, lendo e gravando, cujos dados podem ser acessados de 12 a 20 pontos de conexão em determinadas portas de acesso e pela troca de comandos induz o processador a extrair os da-

dos binários, porém a placa deve estar funcionando. O processador e o eMMC possui a característica da velocidade de extração muito baixa e se faz necessário a desmontagem parcial do dispositivo. Ainda é utilizada, porém a técnica foi aprimorada com o surgimento da técnica *In System Programming*, utilizada até o Android 7 para alguns modelos, versões e atualizações de segurança (TAMMA,2018).

2.4.3 *In System Programming (ISP)*

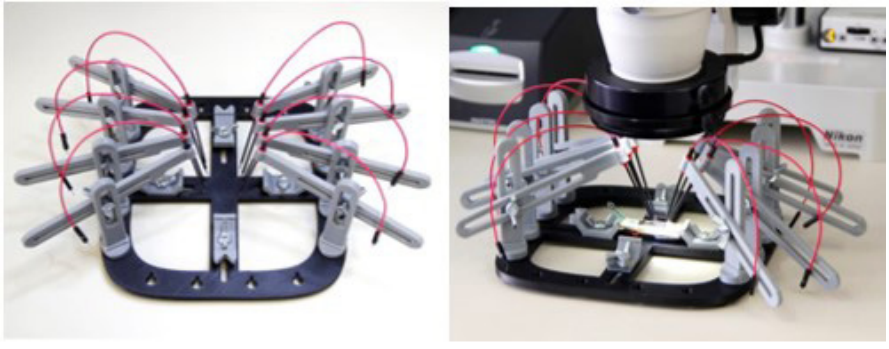
É a evolução da técnica JTAG, que foi criada em 1990, superando os limites de velocidade se tornando mais rápida, minimizando os pontos de conexão de 12 a 20 pontos, dependendo da placa, para 06 pontos. Outro ganho em relação à técnica anterior foi a superação da necessidade de funcionamento do processador, permanecendo somente a necessidade da placa do dispositivo e do eMMC, podendo ler e escrever direto na memória sem a intervenção do processador utilizado até Android 6 (TAMMA, 2018).

Figura 7: Processo de ISP por micro solda



Fonte: produzida pelo autor.

Figura 8: Processo de ISP sem a necessidade de micro solda



Fonte: PCB *Workstation with Crane Arms* (MAKERBOTE THIGIVERSE), 2022.

Vale salientar que a utilização das técnicas avançadas é necessária grande intervenção humana na extração de dados, aumentando risco de perda de dados e danificação do dispositivo eletrônico, deve ser utilizada em última instância, porém possui grande efetividade em seu emprego e devem ser implementadas após esgotar todas as técnicas menos invasivas tentando preservar ao máximo as evidências.

2.5 Técnica de Micro Leitura

Técnica altamente especializada com interpretação manual, na qual o *chip* da memória é analisado utilizando um microscópio eletrônico, verificando as portas físicas e traduzindo o estado da porta em zeros e uns para configurar os caracteres *American Standard Code for Information Interchange* (ASCII) como resultado. Processo muito demorado e com alto custo tendo que ter autoconhecimento em memória *flash* [4]e sistema de arquivo, deve ser utilizada em casos extremos, são escassos os profissionais com conhecimento técnico para realizá-la e pouca literatura bibliografia (TAMMA,2018).

Em todas as técnicas citadas ratifica-se a importância do cuidado nos procedimentos da cadeia de custódia e nas fases de extração de dados, para a produção de dados concisos que poderão ser utilizados na esfera judicial ou como subsídio de contrainteligência. O conhecimento das técnicas garante uma maior efetividade no ganho de conhecimento

4 A memória flash é uma memória do tipo EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), cujos chips são semelhantes ao da Memória RAM, que permite que diversos endereços sejam apagados ou escritos numa só operação.

dos dados extraídos e habilita o profissional de inteligência para a escolha da ferramenta que mais se adequa ao fato.

3. POSSÍVEIS DADOS EXTRAÍDOS

A extração de dados fornece uma grande gama de dados que podem ser filtrados de maneira a ajudar na identificação de vestígios importantes, trazendo evidências de **quem** utilizou o dispositivo, **o que** ocorreu, **quando** ocorreu, o **porquê** da utilização, **como** foi realizado e **onde** aconteceu o uso, gerando assim informações importantes que possam corroborar com investigações ou para assessorar tomadas de decisões. Vários desafios são impostos, alguns descritos anteriormente e outros como a evolução das técnicas com o objetivo de inviabilizar, dificultar, iludir e até impossibilitar o acesso aos dados através de criptografia, esteganografia, senha de acesso e de inicialização e de aplicativos.

Abaixo estão relacionados os dados que podem ser obtidos no processo de extração:

Dados de identificação do dispositivo e componentes: *International Mobile Equipment Identity* (IMEI), *Integrated Circuit Card Identifier* (ICCID), *International Mobile Subscriber Identity* (IMSI), modelo, fabricante, versão e número de série;
Dados de usuários: contas, senhas e número da linha;
Contatos: números dos contatos, endereços de e-mail armazenados;
Histórico de chamadas: discadas, recebidas, perdidas e durações de chamadas;
Short Message Service (**SMS**): mensagens de texto enviadas e recebidas;
MultimediaMessage System (**MMS**): arquivos de mídia, como fotos e vídeos enviados e recebidos;
E-mail: mensagens de e-mail enviadas, escritas e recebidas;
Histórico do navegador: histórico de sites que foram navegados;
Fotos: imagens da câmera, as baixadas e os transferidos de aplicativos;
Vídeos: vídeos da câmera, baixados e os transferidos de aplicativos;
Música: arquivos de música baixados e os transferidos de aplicativos;
Documentos: documentos criados, os baixados e os transferidos de aplicativos;
Calendário: compromissos agendados;
Comunicação de rede: localizações *Global Positioning System* (GPS);

Mapas: rotas e mapas pesquisados e baixados;
Dados de redes sociais: dados de aplicativos;
Dados excluídos: dados apagados no dispositivo;
Dados de conexão: registro de rede, *bluetooth* previamente conectados ou pareados e dados de aplicativos instalados: registro de banco de dados, arquivos de configuração e temporários (BRASIL, 2013).

4. DISCUSSÃO

Desde sua criação a GISOP consolida técnicas utilizadas na extração de dados e a utilização de tecnologia em prol da Secretaria Penitenciária, com ações voltadas a manter a integridade dos ilícitos aprendidos, criando a cadeia de custódia para manter todo o histórico e integridade dos dispositivos eletrônicos e de armazenamento de acordo com a Portaria nº 017/GS/SEAP/2021.

Em 14 de Janeiro de 2021, no âmbito da SEAP/PB, foram elaboradas políticas internas para que a GISOP se adequasse a portaria, definindo-se parâmetros para serem seguidos nos procedimentos e nos materiais aprendidos.

Foi criado um laboratório para a extração de dados, que está em fase final de aquisição de materiais, os profissionais recebem treinamento e os resultados obtidos demonstram a evolução na quantidade e qualidade de dados extraídos conforme apresentado na tabela 2.

Tabela 2 – Dados extraídos em dispositivos eletrônicos e de armazenamento

ANO	2018	2019	2020	2021
Armazenamento em Gigabyte	65 G	296 G	743 G	1.834 G

Fonte: produzida pelo autor.

Outro item que se conseguiu dados relevantes foi a extração de informações contidas nos drones apreendidos, de onde é possível obter pontos de geolocalização, fotos e vídeos em seu cartão de memória externa e interna.

Tabela 3 – Aeronave não tripulada – Drone apreendida

ANO	2018	2019	2020	2021
Drone	0	1	2	5

Fonte: produzida pelo autor.

No que diz respeito à identificação de apenados após as extrações de dados dos dispositivos eletrônicos e de armazenamentos as informa-

ções são enviadas para as unidades prisionais que efetuaram as apreensões por meio de um ofício com um relatório técnico com dados que embasam o processo administrativo de sindicância para apurar o uso.

Tabela 4 – Apenados identificados após extração de dados

ANO	2018	2019	2020	2021
Apenados Identificados	0	228	261	313

Fonte: produzida pelo autor.

O setor de inteligência da SEAP/PB promove a especialização dos profissionais e utiliza a tecnologia para combater a entrada de materiais ilícitos, apresentação de indícios de crimes cometidos e fornecendo informações que podem dar subsídios para ações de contrainteligência e contribuindo para a segurança pública da Paraíba.

CONSIDERAÇÕES FINAIS

A ciência forense veio embasar as técnicas e procedimentos que durante anos foram aperfeiçoados para se adaptar as diversas realidades, a fim de buscar vestígios de caráter digital podendo ou não ser usado nos tribunais, mas que é muito utilizado pelos setores de inteligência da segurança pública prestando apoio na tomada de decisões dos gestores com informações importantíssimas.

Para se estabelecer um nível aceitável de confiabilidade nas evidências obtidas se faz necessário a implementação consistente da cadeia de custódia para manter a integridade das extrações embasadas por portarias, regulamentos, procedimentos, manuais e por leis que irão determinar todos os seus históricos do início ao fim da vida da evidência e dos materiais envolvidos.

Todas as técnicas de extração possuem risco em suas extrações de dados devendo obedecer às ordens das menos invasivas as mais complexas tentando preservar ao máximo as evidências em prol do objetivo a ser alcançado.

Por fim os gestores devem buscar soluções tecnológicas e aperfeiçoamentos constantes de seus recursos humanos para que se possa explorar a excelência do serviço público criando espaços de inovações, novas técnicas e procedimentos em prol do Sistema Penitenciário, da Segurança Pública, de Estado e da sociedade como um todo.

REFERÊNCIAS

BRASIL. Secretaria Nacional de Segurança Pública. **Procedimento operacional padrão** – perícia criminal: POP nº 3.2 Exame pericial de equipamento computacional portátil. Brasília, 2013.

BRASIL. **Decreto de Lei n. 17.210, de 11 de outubro de 1984**, aperfeiçoa a legislação penal e processual penal. Disponível em:<https://bityli.com/dFdHY>, acesso em:12 fev. 2021.

BRASIL. **Decreto de Lei n. 13.964, de 24 de dezembro de 2019**, que institui a Lei de Execução Penal. Disponível em:< https://bityli.com/RaWip>, acesso em: 08 mai. 2021.

CARRIER, B. C. ***Basic Digital Forensic Investigation Concepts***. Junho de 2006.Disponível em: <https://digital-evidence.org/di_basics.html>, acesso em: 23 jan. 2022.

CASEY, E. ***Digital Evidence and Computer crime: Forensic Science, Computers, and the Internet***. s.l.: Academic Press, 2011.

CRETELLA JUNIOR, José, e CINTRA, Geraldo de Ulhoa, **Dicionário Latino** – Português, São Paulo, Companhia Editora Nacional, 1956.

FORENSE COMPUTACIONAL, **Processo de investigação**. Disponível em:< https://bityli.com/tfQrLw>, acesso em 02 jul.2022.

FRANCO, Deivison Pinheiro et al. Introdução à Computação Forense. *In*: VELHO, Jesus Antonio (Org.). **Tratado de Computação Forense. Campinas** - Desvendando a Computação Forense. SP: Millenium Editora, 2016. cap. 6, p. 313-385.

ISO/ IEC 27037. *Information technology – Security techniques, Guidelines for collection, aquisition, and preservation of digital evidence. Switzerland: 2012.*

Apostila do **Curso de extração de dados avançados**, ministrado pelo professor Jorge Figueiredo pela Academia Forense Digital – AFD.

MAKERBOTE THIGIVERSE, PCB Workstation with Crane Arms. Disponível em: <https://www.thingiverse.com/thing:2111631>, acesso em: 02 jul. 2022.

RAMOS, de Figueiredo, Jorge FAUSTINO, de França Junior, Fausto. **Extração forense avançada de dados em dispositivos móveis**:

Conceitos, fundamentos técnicos, diretrizes, métodos e documentos legais. - Volume 1. Rio de Janeiro, RJ: Brasport. 2022.

TAMMA, R. Skulkin, O. Mahalik, H. Bommisetty, S. ***Practical Mobile Forensics*** *- A Hands-on Guide to Mastering Mobile Forensics for the iOS, Android, and the Windows Phone Platforms - Third edition: January 2018 - B3 2PB, UK – MAPT – 2018.*

TAMMA, R. Skulkin, O. Mahalik, H. Bommisetty. ***Practical Mobile Forensics*** *Second Edition A Hands-on Guide to Mastering Mobile Forensics for the iOS, Android, and the Windows Phone Platforms - Second published: May 2016 - Published by Packt Publishing Ltd.*