QUEBRA DE SENHAS APLICADAS À PERÍCIA CRIMINAL EM DISPOSITIVOS MÓVEIS

PASSWORD CRACKING APPLIED TO MOBILE DEVICE FORENSIC EXAMINATION.

Juliane Neves Vilela, Fatec Ministro Ralph Biasi - Americana,
juliane.vilela@fatec.sp.gov.br
Tamires de Carvalho Pereira, Fatec Ministro Ralph Biasi - Americana,
tamires.pereira4@fatec.sp.gov.br
Marcus Vinícius Lahr Giraldi, Fatec Ministro Ralph Biasi - Americana,
marcus.lahr@fatec.sp.gov.br

Resumo

A área de perícia forense computacional desempenha um papel fundamental na investigação de crimes cibernéticos, com um enfoque específico no desbloqueio de dispositivos móveis que frequentemente contêm evidências de grande valor probatório. Neste artigo, apresentamos uma análise dos avanços tecnológicos que impulsionaram o aumento significativo da criminalidade digital e discutimos a importância de preservar a cadeia de custódia. Fornecemos insights sobre os procedimentos envolvidos na perícia digital criminal, com especial atenção ao processo de quebra de senhas. Além disso, abordamos os princípios e implicações legais relevantes para a obtenção de informações de dispositivos móveis, somado a uma visão geral dos principais softwares utilizados nesse contexto. Identificamos métodos de desbloqueio e descrevemos os desafios enfrentados na quebra de senhas. Este estudo contribui significativamente para o avanço do conhecimento na área de forense computacional, fornecendo informações relevantes sobre as complexidades da investigação de crimes digitais e destacando a importância de abordagens eficazes na obtenção de evidências essenciais para o sistema de justiça.

Palavras-chave: Forense computacional, desbloqueio de dispositivos móveis, quebra de senhas, cadeia de custódia, perícia forense.

Abstract

The area of computer forensics plays a fundamental role in the investigation of cybercrimes, with a specific focus on unlocking mobile devices that often contain evidence of great probative value. In this article, we present an analysis of the technological advances that have driven the significant increase in digital crime and discuss the importance of preserving the chain of custody. We provide insights into the procedures involved in digital criminal forensics, with special attention to the password cracking process. Furthermore, we address the principles and legal implications relevant to obtaining information from mobile devices, in addition to an

overview of the main software used in this context. We identify unlocking methods and describe the challenges faced in cracking passwords. This study contributes significantly to the advancement of knowledge in the area of computer forensics, providing relevant information about the complexities of investigating digital crimes and highlighting the importance of effective approaches in obtaining essential evidence for the justice system.

***Keywords**: Computer forensics, mobile device unlocking, password cracking, chain of custody, forensics.*

1. Introdução

Este artigo científico tem como objetivo abordar de forma objetiva a importância da área de perícia forense computacional e seu papel fundamental na investigação de crimes digitais, especialmente no contexto do desbloqueio de dispositivos móveis. Tais dispositivos frequentemente contêm evidências de valor significativo, o que torna crucial a preservação da cadeia de custódia, o processo de perícia digital criminal e o processo de quebra de senhas, bem como a compreensão dos princípios e implicações legais envolvidos.

1.1. Problema:

No cenário atual, a investigação de crimes digitais enfrenta desafios significativos, especialmente quando se trata do desbloqueio de dispositivos móveis protegidos por senhas complexas. A dificuldade em acessar esses dispositivos pode prejudicar a obtenção de evidências vitais para a resolução de casos, levando à necessidade de explorar soluções alternativas para a quebra de senhas em casos onde os softwares existentes não obtêm sucesso.

1.2. Hipótese:

A hipótese subjacente a este estudo é que, ao abordar as limitações existentes nos métodos tradicionais de desbloqueio de dispositivos móveis, é possível encontrar soluções adicionais que contribuam para a obtenção de evidências em casos de crimes digitais.

1.3. Objetivo Principal:

O objetivo principal deste artigo é analisar de forma objetiva a área de perícia forense computacional, com foco especial no desbloqueio de dispositivos móveis, e explorar possíveis soluções alternativas para a quebra de senhas em casos onde as abordagens convencionais falham.

1.4. Objetivos Específicos:

- Examinar os avanços tecnológicos na área de forense computacional.
- Discutir a importância da preservação da cadeia de custódia.
- Investigar os procedimentos envolvidos na perícia digital criminal, com destaque para o processo de quebra de senhas.
- Explorar os princípios e implicações legais relacionados à obtenção de informações de dispositivos móveis.
- Apresentar uma visão geral dos principais softwares utilizados no contexto da perícia forense computacional.
- Identificar os desafios enfrentados na quebra de senhas.

1.5. Justificativa:

Este estudo se justifica pela crescente importância da forense computacional na era digital, onde a obtenção de evidências é essencial para a aplicação eficaz da justiça. A abordagem de soluções alternativas para a quebra de senhas pode preencher lacunas críticas na investigação de crimes digitais, garantindo que nenhum caso seja deixado sem solução devido a desafios técnicos. Além disso, a pesquisa busca contribuir para o avanço contínuo das técnicas empregadas na forense computacional, beneficiando tanto os profissionais da área quanto o sistema de justiça como um todo.

2. Referencial Teórico

2.1. Aumento da Criminalidade Cibernética

Com os avanços dos sistemas tecnológicos, incluindo a Internet das Coisas (IoT), houve um aumento gradual no número de dispositivos conectados à rede de internet. Segundo a CETIC (2020), o acesso à internet teve um crescimento significativo em relação ao ano anterior, especialmente devido à pandemia da COVID-19, que levou as pessoas a ficarem mais conectadas à internet. O número de pessoas acessando a internet aumentou em 83%, totalizando cerca de 61,8 milhões de pessoas na área de Tecnologia da Informação e Comunicação (TIC). Esse aumento nas conexões proporcionou oportunidades para criminosos cibernéticos realizarem ataques.

Independentemente de ser terrorismo cibernético, cibercrime, hacktivismo ou até mesmo cyber extremismo, a definição é clara, tratando-se de uma conspiração, ameaça, ato malicioso ou violência com o objetivo de afetar o psicológico das pessoas, utilizando o ciberespaço como arma (AKHGAR et al., 2014). Conforme a tecnologia avança, os criminosos estão se tornando cada vez mais criativos em seus ataques para alcançar seus objetivos.

A perícia forense criminal aplicada à informática não se limita apenas a crimes cometidos por meio de meios tecnológicos, mas também utiliza dispositivos e tecnologias de suspeitos (independentemente do tipo de crime) para localizar evidências que comprovem um crime, seja ele cibernético ou não.

2.2. Cadeia de Custódia

Para que a perícia possa atuar diante do crime, os termos do artigo 6º do Código de Processo Penal devem ser obedecidos. A preservação das provas e a comprovação dos fatos dependem fundamentalmente da cadeia de custódia. A norma ISO/IEC 27037 (Diretrizes para identificação, coleta, aquisição e preservação de evidência digital) regula a evidência digital e estabelece boas práticas.

Tomlinson et al. (2006) e Kleypas e Badiye (2021) afirmam que a cadeia de custódia deve documentar minuciosamente todo o processo, desde a coleta até a transferência da evidência, registrando informações sobre as pessoas que tiveram contato com a evidência, o tempo em que foi guardada, as condições durante a coleta e o manuseio, a fim de evitar a obstrução ou extravio da evidência durante o percurso, no laboratório ou por parte dos funcionários da lei e também impedir o acesso de pessoas não autorizadas.

Embora não haja limite para a transferência da evidência, é crucial manter seu percurso o mais curto possível. As evidências requerem cuidado e a cadeia de custódia garante sua integridade, fornecendo controle de registro, transferência, análise e transparência no procedimento (BÓRQUEZ, 2011).

A integridade é fundamental e a documentação desempenha um papel vital, pois todos os exames e análises probatórias devem ser autorizados e registrados. A responsabilidade por qualquer incidente recai sobre todos os envolvidos, e a única defesa é a documentação adequada.

2.3. Processo da Perícia Digital Criminal

A perícia digital criminal é um processo sistemático e cuidadoso que envolve várias etapas. De acordo com Casey (2011), as principais etapas desse processo são a identificação e preservação de evidências, a aquisição de dados, a análise forense e a apresentação de resultados.

Uma vez que o perito obtém as evidências, elas passam por uma análise minuciosa e são submetidas à perícia. Nesse contexto, são realizadas diversas atividades fundamentais, como a recuperação de evidências apagadas, a busca por arquivos em dispositivos que podem armazenar até dezenas de terabytes de dados, a decodificação e interpretação dos dados encontrados, o tratamento de criptografias que visam impedir o acesso não autorizado e a extração de informações sem comprometer sua integridade, como ocorre no processo de quebra de senhas.

Essas etapas e atividades são essenciais para garantir a integridade e a confiabilidade das evidências durante o processo de perícia, contribuindo para uma investigação bem-sucedida e a apresentação de resultados consistentes.

2.4. Processo da Quebra da Senhas

A quebra de senhas de dispositivos móveis é uma atividade complexa e requer o uso de softwares especializados. Autores como Sammons (2016) e Quick (2017) destacam a importância de abordagens forenses adequadas e o uso de ferramentas específicas para a extração e quebra de senhas em dispositivos móveis.

Essa prática consiste em um método empregado com o intuito de conseguir realizar a quebra de senhas. Com base no crime ou ataque, são testados todos os conjuntos possíveis de senhas até que a correta seja identificada para desbloqueio ou até que todas as possibilidades sejam esgotadas. Diversas técnicas e estratégias podem ser aplicadas, levando em consideração informações obtidas sobre a senha, como comprimento máximo, tipo de caracteres, idioma e até mesmo a verificação de sua existência em dicionários. Vale ressaltar que o tamanho e a quantidade de caracteres exercem um impacto significativo no grau de complexidade de todo o processo (HRANICKÝ et al., 2017).

Além disso, softwares computacionais são empregados, os quais fazem uso de diferentes algoritmos criptográficos para a verificação de cada senha. Essas ferramentas especializadas desempenham um papel fundamental na análise e na quebra das senhas, auxiliando os peritos digitais

no processo de obtenção de acesso aos dispositivos móveis e no acesso aos dados protegidos por senha.

É fundamental enfatizar que o uso de técnicas de desbloqueio de dispositivos móveis em investigações criminais deve ser realizado dentro dos limites estabelecidos pela lei e com autorização judicial. É imprescindível seguir os procedimentos adequados e garantir a legalidade das evidências obtidas durante todo o processo.

De acordo com os autores Figueiredo e Júnior (2022), é importante ressaltar que, nesses casos, há situações em que é necessária a intervenção pericial propriamente dita, já que a simples análise documental ou jurídica frequentemente se confunde com a perícia.

2.5. Princípios e Implicações Legais

Não obstante, todos os aspectos mencionados anteriormente devem estar em conformidade com os princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD). Em caso de infração penal relacionada à LGPD, o tratamento de dados será regido pela legislação específica da infração, conforme estipulado no artigo 4º, III da LGPD. No entanto, essas interpretações não se afastam dos princípios fundamentais da LGPD, como indicado no parágrafo 1º do art. 4º da referida lei. Além disso, caso o Anteprojeto da LGPD Penal, ou norma equivalente, seja aprovado, há a possibilidade de que ele prevaleça sobre a LGPD, seguindo os critérios mencionados anteriormente (LOUZADA; ROHDEN, 2022).

Segundo Moura (2021), derivou-se disso algumas considerações da Secretaria Nacional de Segurança Pública (SENASP), que, a partir de 2013, passou a abordar o assunto de forma semelhante à ISO/IEC 27037, embora sem o peso da imposição legal. Somente no final de 2019, com a aprovação do pacote da Lei anticrime nº 13.964/2019, que entrou em vigor em janeiro de 2020, foi estabelecido um marco legal que aprimorou a legislação penal e processual penal do país. Essa alteração modificou o código de processo penal, especificamente o artigo 158 (de A a F), tratando de forma mais específica a coleta de vestígios em locais de crime.

A partir de então, existe um arcabouço jurídico que determina a atuação do perito e dos agentes da lei no tratamento e apreensão de vestígios em cena de crime, conforme estabelecido pelo Art. 158-A da referida lei.

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. (Lei nº 13.964/2019).

2.6. Principais Softwares

A utilização de softwares na quebra de senhas de dispositivos móveis é fundamental para o sucesso da investigação. Existem várias ferramentas disponíveis, como:

- Cellebrite, desenvolvido por uma empresa israelense em 2007, conhecido por sua capacidade de desbloquear, extrair dados de forma forense e recuperar informações apagadas. Ganhou notoriedade no Brasil por possibilitar a obtenção de provas na Operação Lava Jato em 2016 e no Caso do menino Henry em 2021;
- Avilla Forensics, ferramenta forense móvel gratuita, criada em fevereiro de 2021 pelo perito forense Daniel Avilla e que atualmente está concorrendo ao prêmio Forensic 4:Cast; projetada para auxiliar os investigadores a obterem informações e evidências de um dispositivo móvel;
- FTK Imager, criado pela empresa Access Data em 2013, permite a criação de imagens de disco e análises periciais nas imagens geradas;
- Magnet AXIOM, desenvolvida pela empresa Magnet Forensics, é uma plataforma digital abrangente que possibilita a visualização, análise e integração de dados e imagens de diversas fontes;
- Oxygen Forensic Detective, ferramenta especializada em extração e análise avançada de dados de dispositivos móveis, incluindo mensagens, chamadas, mídia e histórico de navegação;
- MSAB XRY, desenvolvida pela empresa MSAB, possibilita a extração e análise de dados como mensagens, contatos, registros de chamadas e arquivos de mídia, com recursos avançados de decodificação e análise forense;
- X-Ways Forensics, criado pela empresa X-Ways Software Technology AG, é um software forense versátil e poderoso, oferecendo recursos de extração de dados de dispositivos móveis, análise forense avançada e suporte a diversos formatos de arquivo para garantir a eficiente recuperação e análise de dados.

Além disso, também é utilizado o método de ataque de força bruta, que basicamente emprega um software ou programa para testar todas as senhas existentes em um dicionário, utilizando uma lista de palavras (Wordlist). É possível encontrar Wordlists na internet, que são listas de senhas e suas variações possíveis, para realizar os testes e, potencialmente, quebrar a senha.

2.7. Desafios da Quebra de Senhas

A quebra de senhas em dispositivos móveis apresenta diversos desafios para os peritos digitais criminais. Algumas das principais dificuldades encontradas nesse processo.

Uma das dificuldades está relacionada à criptografia avançada utilizada nos dispositivos móveis modernos. Essa criptografia utiliza algoritmos complexos para proteger as senhas e os dados armazenados, o que dificulta a quebra de senhas pelos softwares forenses. Casey (2011) ressalta que a criptografia forte pode ser um desafio significativo para os peritos digitais.

Outro desafio é a criação de senhas complexas pelos usuários. As senhas tendem a conter combinações de letras, números e caracteres especiais, além de serem longas e incluírem combinações aleatórias de caracteres. Essa complexidade aumenta a dificuldade de quebrar as senhas, mesmo com o uso de softwares avançados. Sammons (2016) destaca a importância de abordagens forenses adequadas para lidar com a complexidade das senhas.

Além disso, a quebra de senhas em dispositivos móveis pode exigir um tempo considerável e recursos computacionais significativos. O número de combinações possíveis a serem testadas pode ser enorme, o que demanda um esforço computacional considerável. O tempo necessário para quebrar uma senha depende de vários fatores, como a complexidade da senha e a capacidade de processamento do hardware utilizado, como mencionado por Quick (2017).

As atualizações de software nos dispositivos móveis também podem representar um desafio, pois podem introduzir novas medidas de segurança que dificultam a quebra de senhas. Novos algoritmos criptográficos ou técnicas de proteção de senhas podem ser implementados, exigindo que os peritos digitais acompanhem constantemente as mudanças e atualizem seus conhecimentos e ferramentas. Casey (2011) ressalta a importância de se manter atualizado com as últimas tecnologias e técnicas de quebra de senhas.

É importante destacar que a proteção contra tentativas de quebra de senha também representa

uma limitação adicional. Os dispositivos móveis podem ser configurados para bloquear ou apagar automaticamente os dados após um determinado número de tentativas incorretas, o que os peritos digitais precisam levar em consideração ao realizar a quebra de senhas. Quick (2017) ressalta a importância de conhecer as políticas de bloqueio e os mecanismos de proteção dos dispositivos analisados.

Durante uma entrevista conduzida por Ricardo (2022), com Alan Martins, um especialista forense sênior, ele ressalta que a perícia em dispositivos móveis apresenta uma série de desafios. Entre eles, destacam-se a ampla variedade de hardwares utilizados nesses dispositivos, as robustas medidas de segurança implementadas pelos próprios smartphones, a escassez de softwares e ferramentas específicas para essa área da investigação digital, a presença de técnicas antiforenses em alguns desses dispositivos, bem como as dificuldades enfrentadas na obtenção de senhas pessoais, mesmo com solicitações judiciais direcionadas aos fabricantes.

Conforme mencionado por BOMMISETTY (2020, p. 18), a obtenção e análise de dados em telefones móveis envolve diversas abordagens, assim como ocorre em qualquer investigação forense. O processo forense adotado é determinado pelo tipo de dispositivo celular, sistema operacional e configuração de segurança. É importante ressaltar que cada investigação é única, com suas próprias circunstâncias, o que impossibilita a definição de uma abordagem processual única para todos os casos.

Em resumo, a quebra de senhas em dispositivos móveis é um processo desafiador para os peritos digitais criminais. A complexidade das senhas, a criptografia avançada, as limitações de tempo e recursos computacionais, as alterações nas versões do software e a proteção contra tentativas de quebra de senha são alguns dos desafios enfrentados nesse processo.

3. Metodologia

A metodologia adotada neste estudo consiste em uma abordagem exploratória, qualitativa e descritiva, utilizando diversas técnicas de pesquisa. Foram realizadas pesquisas bibliográficas em livros, publicações, artigos científicos e dissertações relevantes ao tema em questão.

Outro aspecto importante da metodologia foi a realização de conversas com profissionais especializados na área, a fim de obter insights valiosos e informações atualizadas sobre o assunto em estudo. Além disso, foram realizados levantamentos de dados em bases acessíveis e observações diretas de casos práticos.

Os conhecimentos adquiridos ao longo do curso de Segurança da Informação, abrangendo disciplinas como Fundamentos de Perícia Forense, Criptografia, Programação, Administração de Sistemas Operacionais e Fator Humano, foram aplicados de forma prática na condução desta pesquisa.

No decorrer do trabalho, foi apresentado um embasamento teórico consistente, referenciando pesquisas que evidenciam o aumento da criminalidade cibernética. Também foi abordado o funcionamento da cadeia de custódia das provas adquiridas, bem como os processos e desafios enfrentados pelos peritos criminais na quebra de senhas.

Diante dos desafios encontrados, foram exploradas alternativas para lidar com situações em que a quebra de senha não é possível. Essas alternativas foram discutidas e analisadas à luz das melhores práticas e técnicas atualmente disponíveis na área da Segurança da Informação.

4. Resultados e Discussões

A quebra de senhas em dispositivos móveis apresenta desafios significativos para os peritos digitais criminais, mesmo quando utilizam softwares especializados. Autores como Jonathan Zdziarski, autor do livro "iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets" (2008), e Oleg Afonin e Vladimir Katalov, autores do livro "Mobile Forensics Cookbook" (2018), destacam estratégias que podem ser adotadas para enfrentar essas dificuldades.

Uma abordagem fundamental é a análise detalhada da criptografia utilizada nos dispositivos móveis. Como mencionado por Zdziarski (2008), os peritos devem estudar e compreender os algoritmos criptográficos avançados empregados. Isso permite que eles desenvolvam técnicas específicas para descriptografar ou contornar as medidas de segurança, facilitando a quebra de senhas.

Outra estratégia essencial é a utilização de softwares especializados, como o Cellebrite UFED e o Oxygen Forensic Detective, mencionados por Afonin e Katalov (2018). Essas ferramentas são projetadas para auxiliar na recuperação de dados e na quebra de senhas em dispositivos móveis. Elas oferecem recursos avançados de criptoanálise e técnicas específicas para superar as barreiras criptográficas.

Além disso, os peritos digitais devem manter-se atualizados constantemente, acompanhando as atualizações de software e as novas medidas de segurança implementadas nos dispositivos móveis, conforme ressaltado por Zdziarski (2008). Isso envolve estar atualizado com

as últimas tecnologias e técnicas de quebra de senhas, bem como aprimorar constantemente suas habilidades e conhecimentos.

Os peritos também podem recorrer a técnicas forenses adequadas para lidar com a complexidade das senhas, conforme sugerido por Afonin e Katalov (2018). Isso inclui a utilização de dicionários de senhas, ataques de força bruta otimizados e técnicas de análise de metadados. Cada caso pode exigir uma estratégia diferente, e os peritos devem ser capazes de selecionar as técnicas mais eficazes com base na situação específica.

Em resumo, os peritos digitais criminais podem superar as dificuldades encontradas na quebra de senhas de dispositivos móveis, mesmo utilizando softwares específicos. A análise da criptografia, o uso de softwares especializados, a atualização constante de conhecimentos, o emprego de técnicas forenses adequadas e o acompanhamento das atualizações de software são algumas das estratégias que podem ser adotadas com base nas abordagens sugeridas por Zdziarski, Afonin e Katalov.

Essas estratégias são essenciais para garantir o sucesso na investigação de crimes digitais envolvendo dispositivos móveis e demonstram a importância da adaptação contínua dos peritos às novas tecnologias e desafios que surgem nesse campo em constante evolução.

5. Considerações Finais

Este artigo científico abordou de forma abrangente os métodos e desafios relacionados à quebra de senhas em dispositivos móveis no contexto da forense computacional. Foi discutida a importância da forense computacional na investigação de crimes digitais e a relevância de obter acesso aos dispositivos móveis para a obtenção de evidências relevantes.

Foi destacado que, apesar da disponibilidade de softwares especializados no mercado, a quebra de senhas apresenta desafios significativos, especialmente devido à criptografia avançada e à complexidade das senhas criadas pelos usuários. A utilização de softwares foi mencionada como ferramentas importantes na análise forense e na quebra de senhas.

Foi ressaltada a importância de garantir a conformidade com os princípios legais e a integridade da cadeia de custódia durante o processo de quebra de senhas. A documentação adequada e a adoção de procedimentos adequados foram enfatizadas como aspectos essenciais para a obtenção de evidências válidas e confiáveis.

No entanto, mesmo com o uso dessas ferramentas e a adoção de procedimentos adequados, existem desafios a serem superados. A criptografia avançada e as senhas complexas continuam sendo obstáculos para os peritos digitais. Portanto, é necessário um desenvolvimento contínuo de técnicas e soluções alternativas para lidar com esses desafios e melhorar a eficácia da quebra de senhas.

Este estudo contribuiu para a compreensão dos desafios enfrentados na quebra de senhas em dispositivos móveis e destacou a importância de abordar essas limitações para avançar no campo da forense computacional. Espera-se que as informações apresentadas neste artigo ofereçam novas perspectivas e alternativas para enfrentar o desafio da quebra de senhas e contribuam para a obtenção de evidências fundamentais para o sistema de justiça.

Em resumo, a quebra de senhas em dispositivos móveis continua sendo uma área de pesquisa e desenvolvimento ativa na forense computacional. É fundamental aprimorar constantemente as técnicas e soluções utilizadas, garantindo a conformidade com os princípios legais e a integridade da cadeia de custódia, a fim de obter sucesso na obtenção de evidências relevantes para a investigação de crimes digitais.

"A computação forense é uma arte de descobrir e recuperar informações sobre um crime de tal forma que se tornem admissíveis em tribunal" (YASINCAC E MANZANO, 2001 apud SOUSA, 2016).

Referências Bibliográficas

AFONIN, Oleg; KATALOV, Vladimir. Mobile Forensics - Advanced Investigative Strategies. [S. L.]: Packt, 2018. 412 p.

AKHGAR, B. et al. Cyber Crime and Cyber Terrorism Investigator's Handbook. Waltham: Elsevier, 2014. 275 p.

BAGGILI, I.; MARRINGTON, A.; FERGUS, P. Investigating Mobile Devices: Tools and Techniques. Syngress, 2014.

BOMMISETTY, Satish. Practical Mobile Forensics (2020, p. 18).

BÓRQUEZ, Pamela. Importance of chain of custody of evidences. Rev Med Chil. 2011.

BRASIL. Constituição (1941). Decreto-Lei nº 3689, de 03 de outubro de 1941. Código De

Processo Penal. Rio de Janeiro, 13 out. 1941.

BRASIL. Lei nº 13853, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 246. ed. Brasília, 20 dez. 2019. Seção 1.

CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3. ed. Baltimore: Academic Press, 2011. 807 p.

CETIC. TIC DOMICÍLIOS: pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros. 2021. Disponível em: < https://cetic.br/media/docs/publicacoes/2/20211124201233/tic_domicilios_2020_livro_eletronico.pdf >. Acesso em: 05 nov. 2022.

FIGUEIREDO, Jorge Ramos de; FRANÇA JÚNIOR, Fausto Faustino de. Extração Forense Avançada de Dados em Dispositivos Móveis: Volume 1: conceitos, fundamentos técnicos, diretrizes, métodos e documentos legais. Rio de Janeiro: Brasport, 2022. 128 p.

HRANICKÝ, R. et al. Distributed Password Cracking in a Hybrid Environment. 2017. Faculty of Information Technology, Brno University of Technology, Božetěchova, 2017. Disponível em: <https://www.fit.vut.cz/research/publication-file/11358/spi2017. pdf >. Acesso em: 20 nov. 2022.

KLEYPAS, Deborah A.; BADIYE, Ashish. Evidence Collection. 2021. Disponível em: < https://www.ncbi.nlm.nih.gov/books/NBK441852/ >. Acesso em: 20 nov. 2022.

LOUZADA, Luiza; ROHDEN, Ana Letícia Manfrim. Bancos de Perfis Genéticos para fins de Investigação Criminal no Brasil. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. Disponível em: < https://www.dataprivacybr.org/wp-content/uploads/2022/10/bancos-perfis-geneticos-vf.pdf >. Acesso em: 20 nov. 2022.

MOURA, Ana. A Cadeia de Custódia na Perícia Forense Digital. 2021. Disponível em: < https://blog.daryus.com.br/a-cadeia-de-custodia-na-forense-digital/ >. Acesso em: 19 nov. 2022.

QUICK, Donny J. Investigating Digital Crime. Boca Raton: CRC Press, 2017.

RIBEIRO, Ricardo. A importância da perícia forense digital na segurança cibernética. 2022. 1 v. TCC (Especialização) - Curso de Informática Forense., Ipog - Instituto de Pós-Graduação e Graduação, Goiânia, 2022.

SAMMONS, John. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. [S. L.]: Syngress, 2016. 208 p.

SOUSA, Adriano Gomes. ETAPAS DO PROCESSO DE COMPUTAÇÃO FORENSE: UMA REVISÃO. 2016. 13 f. TCC (Graduação) – Curso de Ciência da Computação, Centro Universitário da Bahia (FIB), Salvador, 2016. Disponível em: <http://www.ls.edu.br/actacs/index.php/ACTA/article/viewFile/138/128 >. Acesso em: 19 nov.

2022.

TOMLINSON, J. J. et al. Laboratory Information Management System Chain of Custody: Reliability and Security. Automated Methods And Management In Chemistry. Raleigh, USA, p. 1-4. 18 jan. 2006. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1903459/pdf/S1463924606749070.pdf>. Acesso em: 20 nov. 2022.

ZDZIARSKI, Jonathan. IPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets. Sebastopol: O'Reilly, 2008. 186 p.

Anexo I

Entrevista com Perito Forense Computacional

Entrevista realizada no dia 30/05/2023 com perito da Polícia Técnico-Científica do estado de São Paulo (SPTC).

Qual a maior dificuldade durante uma extração de um dispositivo móvel?

R: Os maiores desafios são os de aparelhos bloqueados por senhas e aplicativos criptografados.

Em termos de porcentagem, quantos % de aparelhos não chegam a ser periciados e extraídos dados, por não ser possível realizar a quebra de senha?

R: Variável devido aos modelos e condições dos aparelhos, mas algo em torno de 50% dos aparelhos não foi possível a extração dos dados.

O quanto impactaria caso houvesse uma ferramenta que tivesse 100% êxito no desbloqueio dos dispositivos móveis?

R: Impacto muito positivo na obtenção de dados para investigação e talvez menor tempo gasto nas tentativas de desbloqueio.

Existe hoje no mercado, alguma ferramenta capaz de realizar o desbloqueio de dispositivos móveis e que não é utilizada pela polícia por algum motivo legal?

R: Existem versões/atualizações dos softwares utilizados, mas que ainda não estão disponíveis para a polícia científica do estado de São Paulo.

Anexo II

NOTA DE DIREITOS AUTORAIS

Nós, abaixo assinados, declaramos que o texto científico submetido à apreciação da Comissão Científica desta publicação é de total autoria nossa.

Estamos cientes de que, caso haja qualquer trecho do texto científico em questão que possa ser considerado plágio (cópia de trechos de livros, artigos, revistas, dissertações, teses, *sites*, blogue, etc., sem a referida citação, de acordo com a ABNT), ou se o mesmo puder ser considerado "comprado" (isso é considerado crime, de acordo com o Código Penal 184, Lei n. 9.610/98), essa Comissão Científica poderá recusar o artigo científico.

Americana, 17 de julho de 2023.

DocuSigned by:
JULIANE NEVES VILELA

Juliane Neves Vilela

RG: 47.521.441-9

DocuSigned by:
MARCUS VINICIUS LAHR GIRALDI

Marcus Vinicius Lahr Giraldi

RG: 40.047.801-8

DocuSigned by:
TAMIRES DE CARVALHO PEREIRA

Tamires de Carvalho Pereira

RG: 55.323.157-1