SERGIPE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA JUSTIÇA
E DE DEFESA DO CONSUMIDOR

PROCESSO Nº: **3292/2024-COMP.CON.DIRETA-SEJUC**
FORMA DE CONTRATAÇÃO: **Inexigibilidade**
BASE LEGAL: **74, I, da Lei nº 14.133/2021.**

RATIFICO EM 5 de dezembro de 2024

e-doc SERGIPE ASSINADO ELETRONICAM
Verificar autenticidade conforme me
apresentada no rodapé do docum

VIVIANE CRUZ PESSOA
Secretário(a) de Estado

JUSTIFICATIVA

No dia 10 de novembro do corrente ano, o Núcleo de Inteligência, junto à empresa UTI dos Dados, realizou uma apresentação e prova de conceito da ferramenta PC-3000 Mobile Pro da empresa ACELab, especialista reconhecida mundialmente em recuperação de dados. No Brasil, a ferramenta é representada exclusivamente pela empresa UTI DOS DADOS PERÍCIAS DIGITAIS, SOLUÇÕES DE DADOS E IMPORTAÇÃO LTDA, inscrita sob o CNPJ 16.946.935/0001-03, situada na Av. Trindade, 254 - Salas 714 / 715 – Bethaville I, Barueri – SP, CEP 06404-326.

Considerando o aumento do uso de dispositivos móveis portáteis nos últimos anos, há um grande número de marcas e modelos de dispositivos. Esses dispositivos armazenam grande quantidade de dados e por vezes possuem evidências de práticas criminosas, gerando provas que são imprescindíveis nos processos criminais.

Os projetos eletrônicos desses dispositivos utilizam diversas tecnologias, como sistemas operacionais e processadores (*chipsets*), e estes representam um enorme desafio ao acesso de dados destes aparelhos. Os dispositivos da marca *Apple,* por exemplo, possuem *chipsets* produzidos com sua tecnologia proprietária e as demais marcas utilizam *chipsets* produzidos por outras diversas empresas. Os *chipsets* mais utilizados no sistema operacional Android são *Qualcomm*, *Exynos*, *MediaTek* e *Unisoc* (Spreadtrum). Em geral, os dispositivos, com custo reduzido, utilizam os chipsets *MediaTek* e *Unisoc*.

O Núcleo de Inteligência Penal – NIP, em Sergipe, recebe os aparelhos apreendidos nas unidades prisionais de todo o Estado para a realização de extração e analise de aparelhos apreendidos, possuindo um Laboratório de Extração de Dados dedicado para tal função.

Com a grande variedade de materiais encaminhados, torna-se imprescindível a disponibilidade de diversas ferramentas forenses de extração, a fim de aumentar a probabilidade de êxito na obtenção dos dados.

SERGIPE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA JUSTIÇA
E DE DEFESA DO CONSUMIDOR

Este documento faz referência ao teste e prova de conceitos da ferramenta PC-3000 Mobile PRO, da fabricante ACELAB.

DA FERRAMENTA

O principal objetivo da ferramenta é o desbloqueio e extração de dados de aparelhos celulares. As principais funcionalidades da ferramenta PC-3000 Mobile PRO que são de interesse às atividades do laboratório de extração são:

a) Possui compatibilidade com diversas plataformas e dispositivos Android baseados em *Unisoc*, *Mediatek* e *Qualcomm*. (lista de fabricantes suportados: ASUS, Alcatel, Ark, BQ, Blackfox, Blackview, Caterpillar, CUBOT, DIGMA, FLY, Ginzzu, INFINIX, Itel, Hammer, Highscreen, HTC, HONOR, Huawei, Lenovo, LG, Meizu, ;Motorola, Nokia, OPPO, Philips, POCO, Prestigio, Realme, Redmi, Samsung, Sony, Sony Ericsson, TP-LINK, TCL, Tecno, Vivo, Xiaomi, ZTE, entre outros.)

c) A ferramenta utiliza comunicação direta com o *chipset* do telefone, necessitando funcionamento mínimo dos componentes eletrônicos do aparelho, como circuitos de alimentação e dos circuitos integrados de processamento e memória. Com testes, inclussive, em aparelho totalmente desligados, que é uma ferramenta não suportada em equipamentos como o Celebrite.

d) Diferente das ferramentas tradicionais, **ele possibilita a comunicação com o celular sem a inicialização do sistema operacional Android, realizando quebra de senha e extração de dados sem afetar a integridade dos vestígios computacionais, tais como *logs*, rotinas de *backups*** e entre outras informações com maior grau de volatilidade.

e) A ferramenta executa o procedimento de quebra de senhas utilizando os recursos computacionais na qual está instalada, possibilitando um alto número de tentativas de senhas, dependendo somente da capacidade de processamento da máquina, **independente do celular**, este recurso técnico é um avanço e um diferencial muito importante da ferramenta.

MOTIVAÇÃO

Apesar das ferramentas forenses disponíveis no laboratório de extração atenderem às expectativas com relação a seu funcionamento, há desafios encontrados em alguns casos que fazem com que outras soluções sejam buscadas para suprir a lacuna de suporte.

SERGIPE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA JUSTIÇA
E DE DEFESA DO CONSUMIDOR

Os principais desafios da extração dos dados são:

- Desbloqueio de aparelhos celulares com *chipsets* como *MediaTek* e *Unisoc*, em especial os que são vendidos exclusivamente no mercado brasileiro, vez que possuem suporte reduzido nas ferramentas forenses comerciais de grande nome, como exemplo a **UFED 4PC da empresa Cellebrite,** que já possuímos em nosso laboratório.

- Desbloqueio e extração de dados de aparelhos danificados que dependem de tela funcional: Apesar de o laboratório de extração contar com uma equipe especializada no reparo de dispositivos danificados, alguns modelos exigem uma tela funcional para viabilizar o uso de determinadas ferramentas de extração. Quando a tela está danificada ou indisponível, o processo pode ser inviabilizado. No contexto do sistema penitenciário, essa situação é ainda mais desafiadora, dado o número significativo de aparelhos danificados devido à prática frequente de internos em tentar inutilizá-los durante abordagens.

- Desbloqueio de aparelhos com senha alfanumérica (letras, números e caracteres especiais): utilizando-se as ferramentas disponíveis atualmente no laboratório, o processo de quebra de senhas é realizado no celular e, portanto, a velocidade do processo depende da capacidade de processamento do aparelho, limitando muito o número de possibilidades.

No caso concreto, é possível citar o aparelho marca SAMSUNG modelo A01 Core, aparelho de custo reduzido (em média R$600), com *chipset Mediatek*, o qual possui uma lacuna de suporte nas ferramentas forenses e em técnicas de extração disponíveis no laboratório, que não são capazes de realizar o processo de quebra de senha nele. No laboratório de extração, cerca de 60% desses aparelhos não são extraídos devido a essa lacuna de suporte. O restante é extraído devido a não utilização de senha no equipamento ou a informação dela por parte da autoridade requisitante.

Considerando somente o ano de 2023, no sistema penitenciário de Sergipe, foram apreendidos cerca de 400 dispositivos. Desses, a maioria é composta por aparelhos com *chipsets Unisoc* ou *Mediatek*. No entanto, aproximadamente 70% desses dispositivos não são extraídos devido à falta de suporte adequado para esses modelos.

Entre os dispositivos com *chipsets Unisoc* e *MediaTek* encaminhados bloqueados, a maioria não foi extraída com sucesso, evidenciando uma limitação nas ferramentas disponíveis. Apesar de nosso laboratório dispor de equipamentos capazes de realizar tentativas de desbloqueio e extração de dados utilizando altas taxas de processamento e diversas possibilidades, ainda não conseguimos obter êxito na extração de informações de grande parte desses *chipsets*.

SERGIPE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA JUSTIÇA
E DE DEFESA DO CONSUMIDOR

Com o uso da ferramenta PC-3000 Mobile PRO, seria possível superar a marca de 1 bilhão de tentativas em computadores de alto desempenho, ampliando significativamente as chances de sucesso na extração de dados desses dispositivos.

A motivação para o teste da ferramenta se baseia nos desafios citados, visando complementar as ferramentas disponíveis no laboratório de extração.

DOS TESTES

MARCA	MODELO	CHIPSET	TIPO DE SENHA
XIAOMI	A2	Mediatek	GEOMETRICA
XIAOMI	NOTE 8	Qualcom	ALFANÚMERICA
SAMSUNG	A032	Unisoc	NUMERICA
MOTOROROLA	E7 POWER	Mediatek	GEOMETRICA
SAMSUNG	A01 CORE	Mediatek	ALFANUMERICA
SAMSUNG	A15	Mediatek	GEOMETRICA
SAMSUNG	A12	Mediatek	NUMERICA

Os testes foram realizados em 10 de novembro de 2024. A Tabela a seguir apresenta os aparelhos cujas senhas foram determinadas com a ferramenta PC-3000 Mobile PRO no teste.

RESULTADOS

A ferramenta se mostrou amplamente eficaz no desbloqueio dos aparelhos celulares de *chipset Unisoc* testados. Especificamente sobre os aparelhos Samsung SM-A032, cuja extração nas ferramentas não é possível sem o conhecimento prévio da senha. Estas evidências tiveram suas senhas determinadas pela ferramenta PC-3000 Mobile Pro, possibilitando, assim, a extração pelas ferramentas tradicionais. Vale ressaltar que também seria possível realizar a extração via PC-3000, contudo não se optou para tal devido ao curto espaço de tempo de testes.

Já as marcas Motorola e XIAOMI, que possuem modelos com suporte limitado na ferramenta presentes no laboratório, tiveram êxito em dois modelos, testados com sucesso, cujas senhas foram determinadas, inclusive uma alfanumérica.

SERGIPE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA JUSTIÇA
E DE DEFESA DO CONSUMIDOR

Conforme Atestados de Capacidade Técnica de órgãos como Ministério Público do Mato Grosso, Ministério da Justiça e Segurança Pública, a ferramenta se mostrou como uma alternativa competitiva para utilização de desbloqueio de *smartphones* Android, tendo de se destacado em desbloqueio em aparelhos que ferramentas "Tradicionais" como Cellebrite "UFED 4 PC" e "UFED PREMIUM", não foram capazes de realizar o desbloqueio e extração.

Por fim, importante ressaltar que é uma ferramenta com proposta única de desbloqueio de celulares fisicamente danificados e bloqueados por senha, principalmente dos *chipsets Mediatek, Unisoc e Spreadtrum,* além disso, o método de extração e desbloqueio é realizado com o celular desligado, com situação de zero logs, perfeito para setores de inteligência, e sem alteração do sistema Android, evitando qualquer tipo de questionamento quanto à veracidade das informações.

É uma ferramenta capaz de realizar a extração de celulares bloqueados por *Knox* Samsung e *Second Space* Xiaomi, e um método de extração que utiliza somente a placa do celular, sem a necessidade do de uso de tela, câmera, bateria etc.

Assim sendo, é uma ferramenta que trabalha apenas com a placa do celular, não sendo necessário que o aparelho celular esteja funcionando, como é o caso do equipamento Celebrite, então é uma proposta única de complementação de laboratório como uma ferramenta pra extração de dados, de desbloqueio e de lidar com celulares danificados, e como um dos principais diferenciais é o zero log, vez que o melhor método forense é quando não realizamos o ligamento de HD, celular, fazendo uma cópia sem necessidade de subir um sistema operacional, evitando questionamentos sob o estado da coisa, com o celular totalmente desligado durante o processo, sem necessidade de bateria, tela, câmera, etc.

Ademais, importante frisar que o equipamento X1 Discovery, não é uma ferramenta pra celular com proposta de desbloqueio; já o GrayChift é uma ferramenta vendida apenas pra Polícia Federal, e mesmo assim não tem a completude do PC-3000 Mobile Pro.

CONCLUSÃO

A ferramenta PC3000 Mobile Pro foi eficaz na determinação das senhas de sete aparelhos testados, que não possuem suporte de força bruta de senha nas ferramentas presentes no laboratório, possibilitando a extração dos dados desses equipamentos.

A ferramenta realiza a força bruta utilizando o processador do computador na qual está instalada, o que agiliza o processo, especialmente nos casos de senha alfanumérica. Como o acesso ao equipamento é realizado utilizando-se a interface USB e placa-mãe, há a facilidade de extração em equipamentos danificados, que por vezes são encaminhados com a tela destruída, por exemplo.

SERGIPE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA JUSTIÇA
E DE DEFESA DO CONSUMIDOR

Ao final, juntamos o Contrato Exclusivo nº 80, redigido originalmente em inglês, bem como a versão traduzida para português por tradutor público juramentado, conforme documentos.

Aracaju, 4 de dezembro de 2024

e-doc SERGIPE
ASSINADO ELETRONICAMENTE
Verificar autenticidade conforme mensagem apresentada no rodapé do documento

ADRIANO DIAS DE OLIVEIRA

Diretor(a)

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço http://edocsergipe.se.gov.br/consultacodigo e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: BQWV-BIQ7-S7ST-LVQZ

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 17/12/2024 é(são) :

Legenda: Aprovada Indeterminada Pendente

- ADRIANO DIAS DE OLIVEIRA - 05/12/2024 09:20:28 (Docflow)
- VIVIANE CRUZ PESSOA - 05/12/2024 10:04:00 (Docflow)