

MSAB

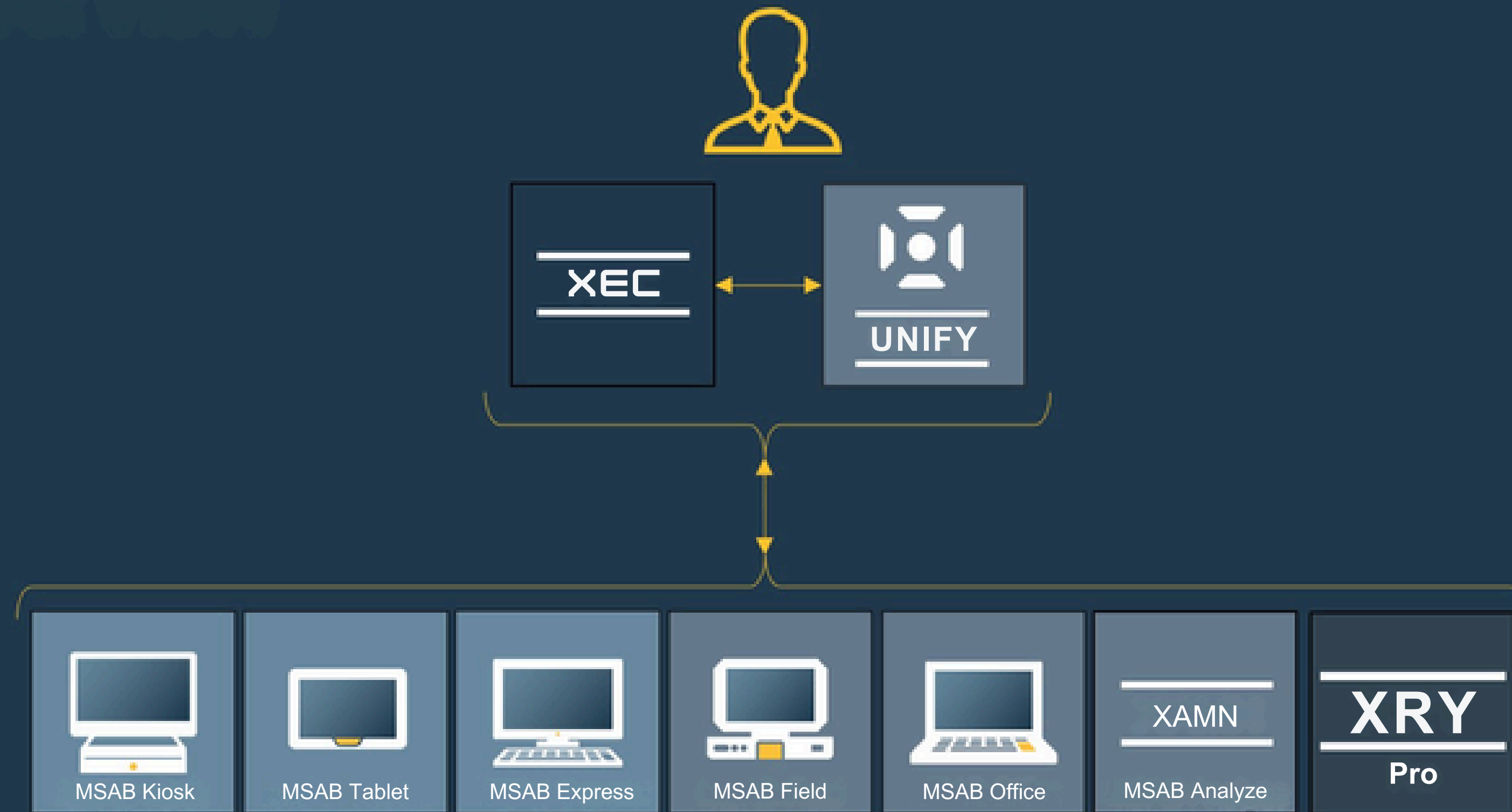
Trusted Partner in Digital Forensics

Sobre a MSAB

- A MSAB é uma empresa sueca
 - As soluções MSAB são desenvolvidas com orgulho na Suécia/UE
- Pioneira em perícia forense móvel por volta de 2005 com a XRY
- Uma das pouquíssimas empresas globais de Forense Móvel "impulsionada" pelo talento do nosso próprio departamento de Pesquisa e Desenvolvimento
 - A única sediada na UE



Ecosystem MSAB



* Os recursos de gerenciamento variam entre as plataformas

MSAB

Principais soluções de software da MSAB

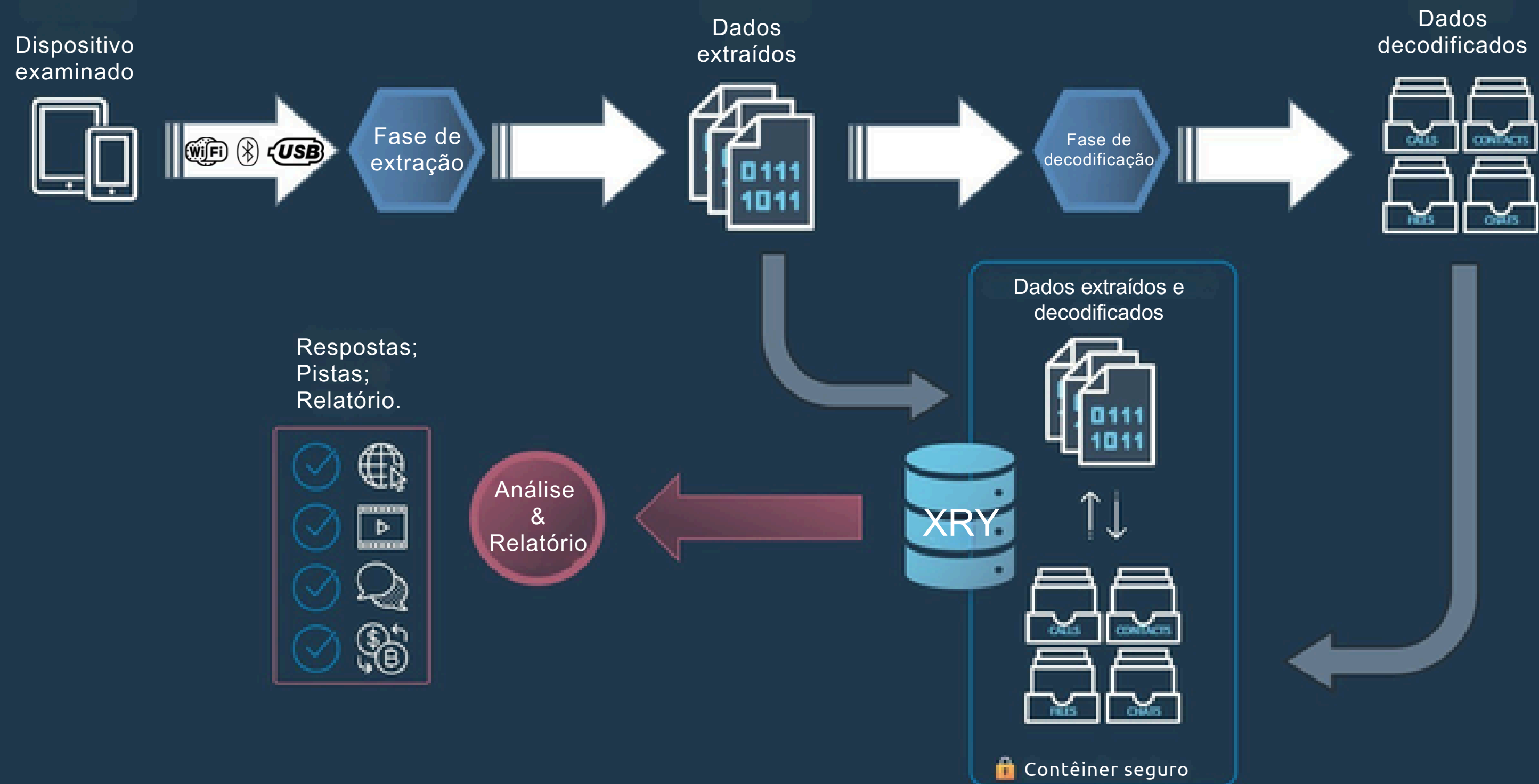


Extração/Decodificação

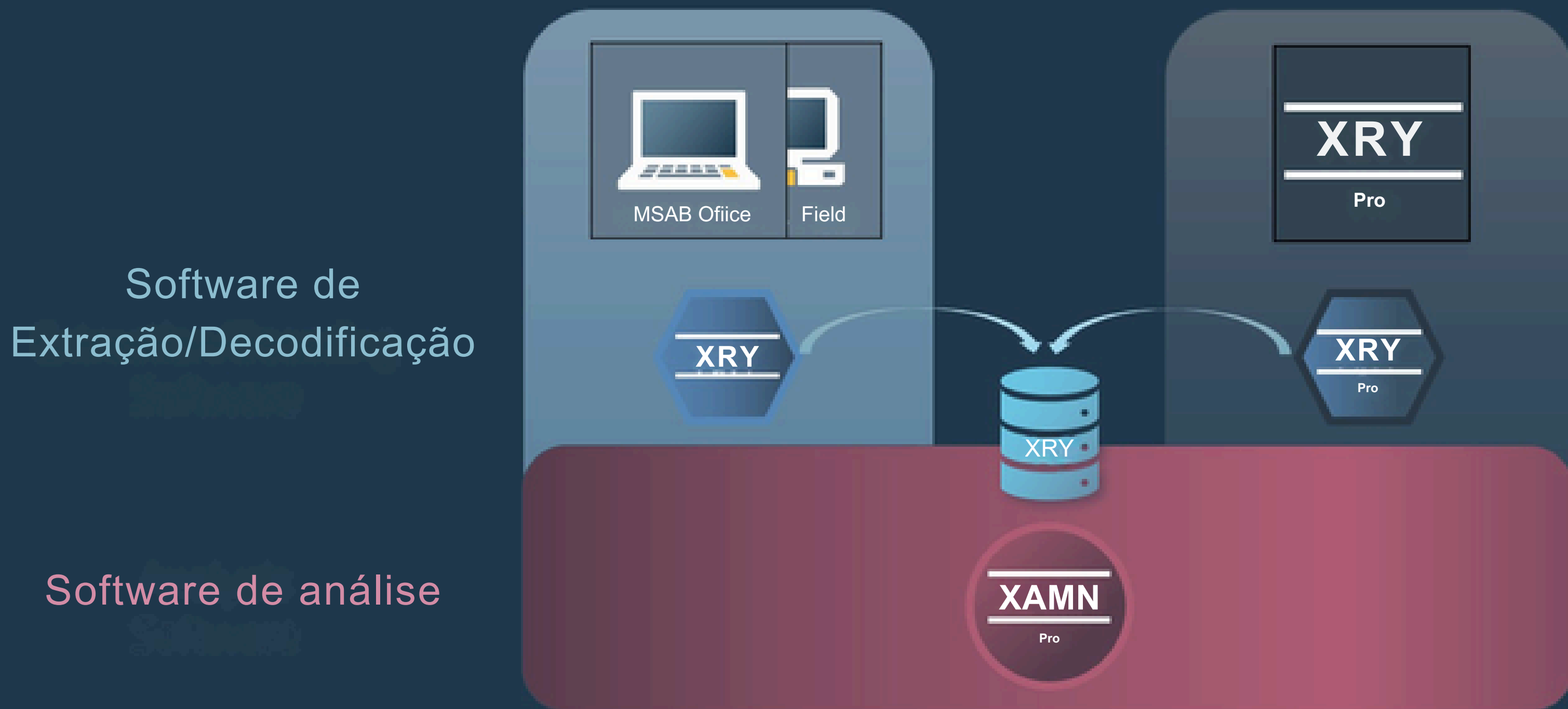


Análise/Relatório

Análise Forense Móvel: Um fluxo de trabalho típico



MSAB Office (Field) e XRY Pro - Ambos incluem a mesma excelente ferramenta de análise: O XAMN Pro



O que são XRY Office e XRY Pro? (comparado)

Extração++

Explorações exclusivas adicionais (Android)

Tools++

XRY BruteStorm, XRY RAMalyzer, etc.

XRY

Pro

Fundação de Extração

Mais de 51.070 perfis de dispositivos

Fundação Decodificando

501 aplicativos, processamento de IA (STT, OCR, reconhecimento de imagem) e muito mais.

XRY®

O que é o XRY Pro?

- XRY Pro é uma solução de extração/decodificação da MSAB
- Herda todas as capacidades de extração/decodificação disponíveis no XRY
- + Adiciona mais exploits e ferramentas (exclusivas)
- Extrações ilimitadas com a licença anual
- Operação offline, sem geofencing, sem coleta de dados
- Ciclo de lançamento adicional para XRY Pro:
 - As "Liberações de Impacto"
 - Além dos lançamentos padrão XRY Major/Micro

XRY

Pro

XRY Pro - Visão geral dos principais recursos

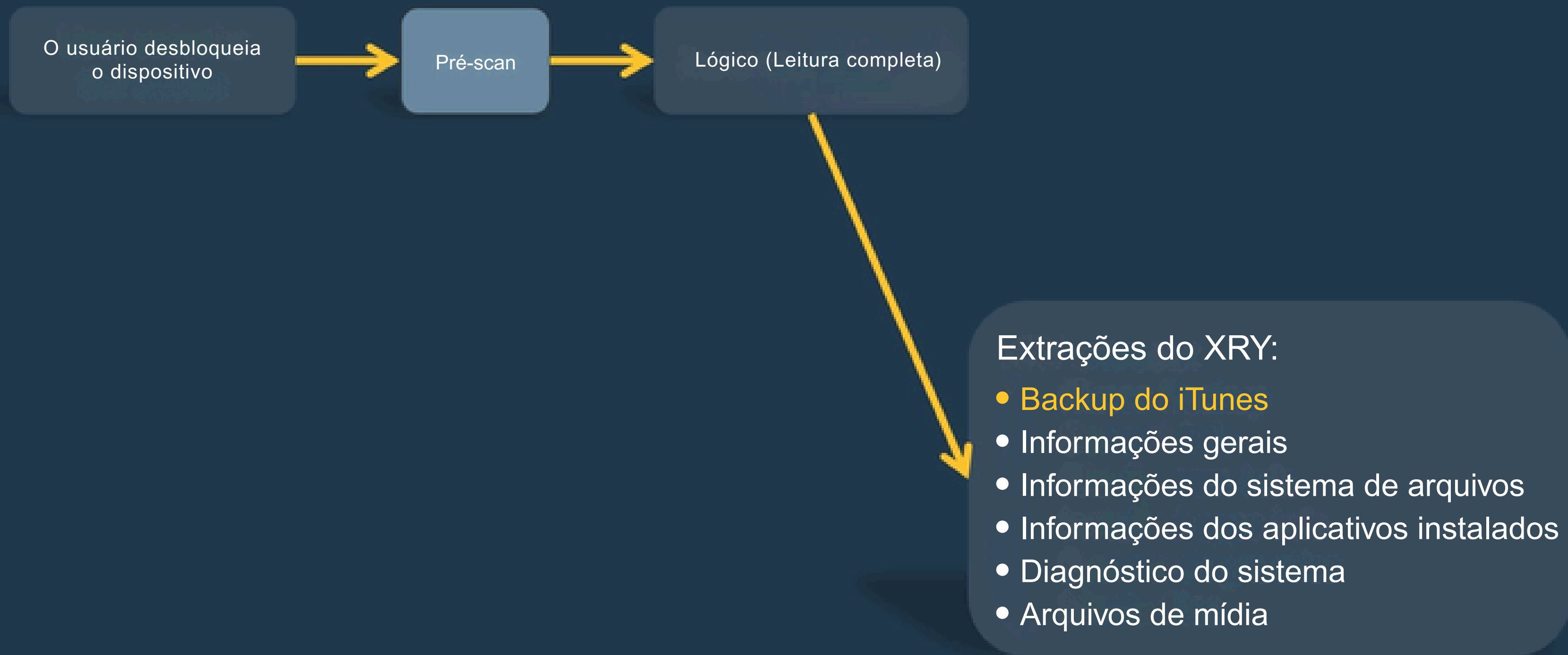
- Melhor suporte da categoria para Samsung (Qualcomm)
- Melhor suporte da categoria para Unisoc
- Suporte preferido pelos usuários para MTK, Kirin e dispositivos Android mais antigos
- Vários outros métodos de extração exclusivos
- Velocidades de força bruta incomparáveis em um único PC
 - Pode ser acelerado pelo XRY BruteStorm (ferramenta de força bruta distribuída)
 - E acelerado mais ainda pelo XRY BruteStorm Surge (GPU)
- Ainda produz extrações físicas em Androids FBE em 2025
- Fornece extrações físicas/FFS completas em AFU e BFU
- Capacidade exclusiva de dump e análise de RAM
- Velocidades de extração líderes da categoria

XRY

Alguns exemplos de extração e decodificação de recursos

iOS (Desbloqueado)

Processo de extração lógica



iOS (Desbloqueado)

Extração lógica \ Captura de tela e vídeo

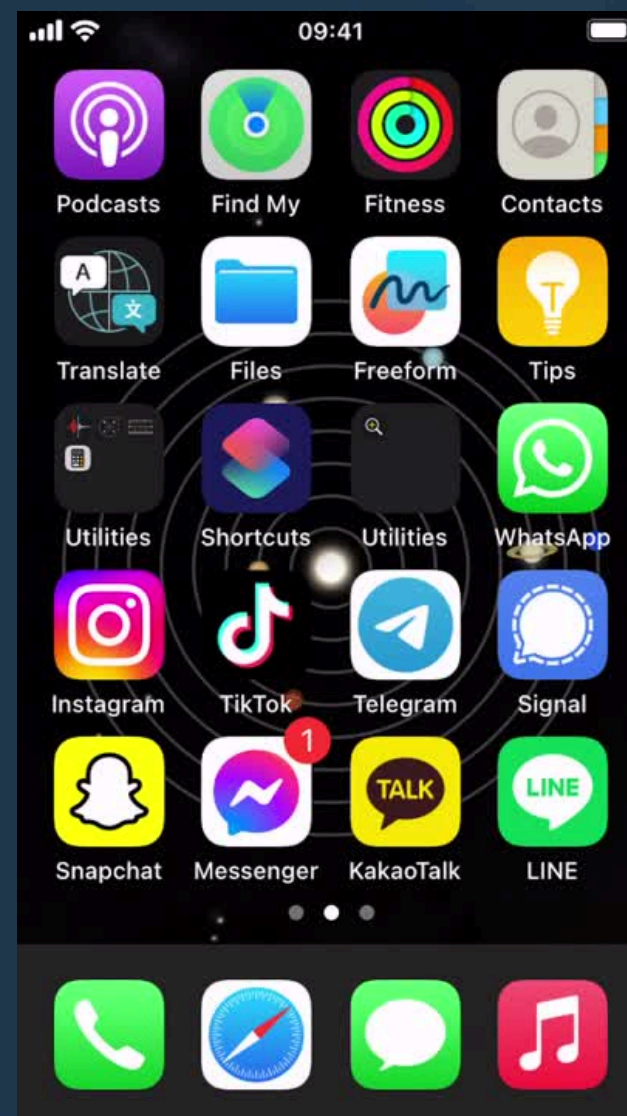
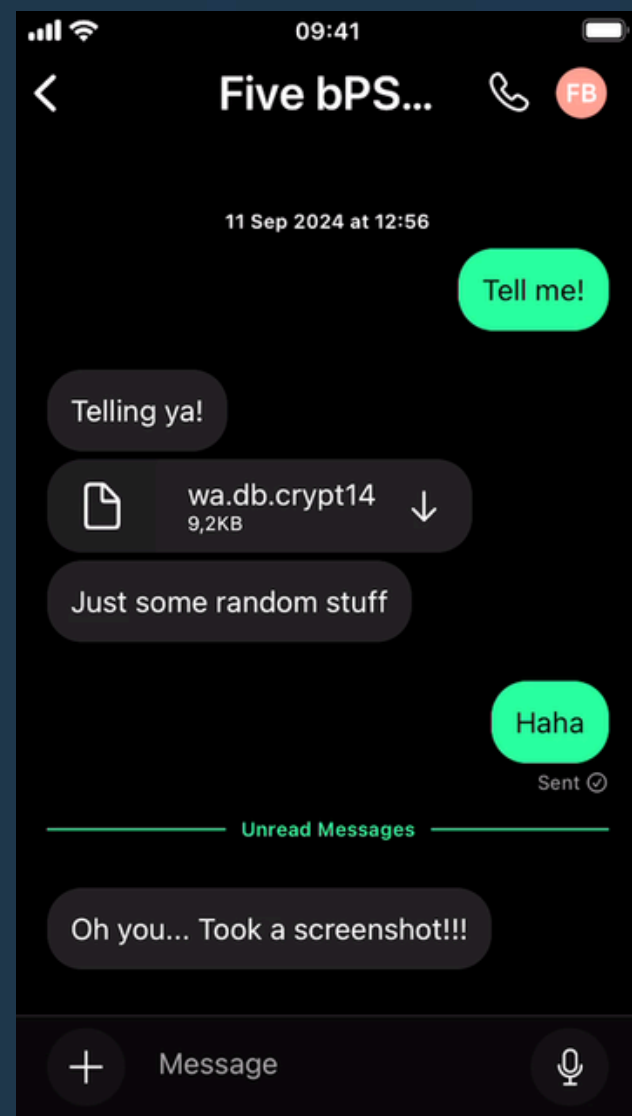
O usuário desbloqueia o dispositivo

Pré-scan

Captura de tela

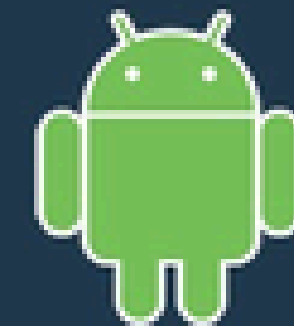
Extrações do XRY:

- Capturas de tela do iOS
 - Gravação de vídeo do iOS
- (sem instalação de aplicativos adicionais!)



Android (Desbloqueado)

Processo de extração lógica



O usuário desbloqueia o dispositivo



Pré-scan

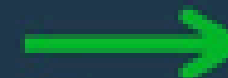


Lógico (Leitura completa)



XRY tenta automaticamente explorar o dispositivo (LPE) *

Sucesso



XRY extrai o sistema de arquivos completo (FFS)

Nenhuma das variantes do exploit FFS funciona, ou nenhum exploit compatível está disponível.



O XRY tenta automaticamente extrair sandboxes de aplicativos **

Sucesso



O XRY extrai todos os dados do aplicativo, do agente e do sistema de arquivos.

Explorações do ambiente de teste falham



O XRY extrai dados por meio de Agente, Backup, etc.

* 14 exploits diferentes para FFS

** 2 exploits diferentes de sandbox

Pré-scan

➤ Apresenta informações essenciais em tempo real sobre o dispositivo analisado:

➤ Modelo, número de série, IMEI, etc

➤ Níveis de patches de segurança e do sistema operacional

➤ Modo avião, status do Wi-Fi e do Bluetooth

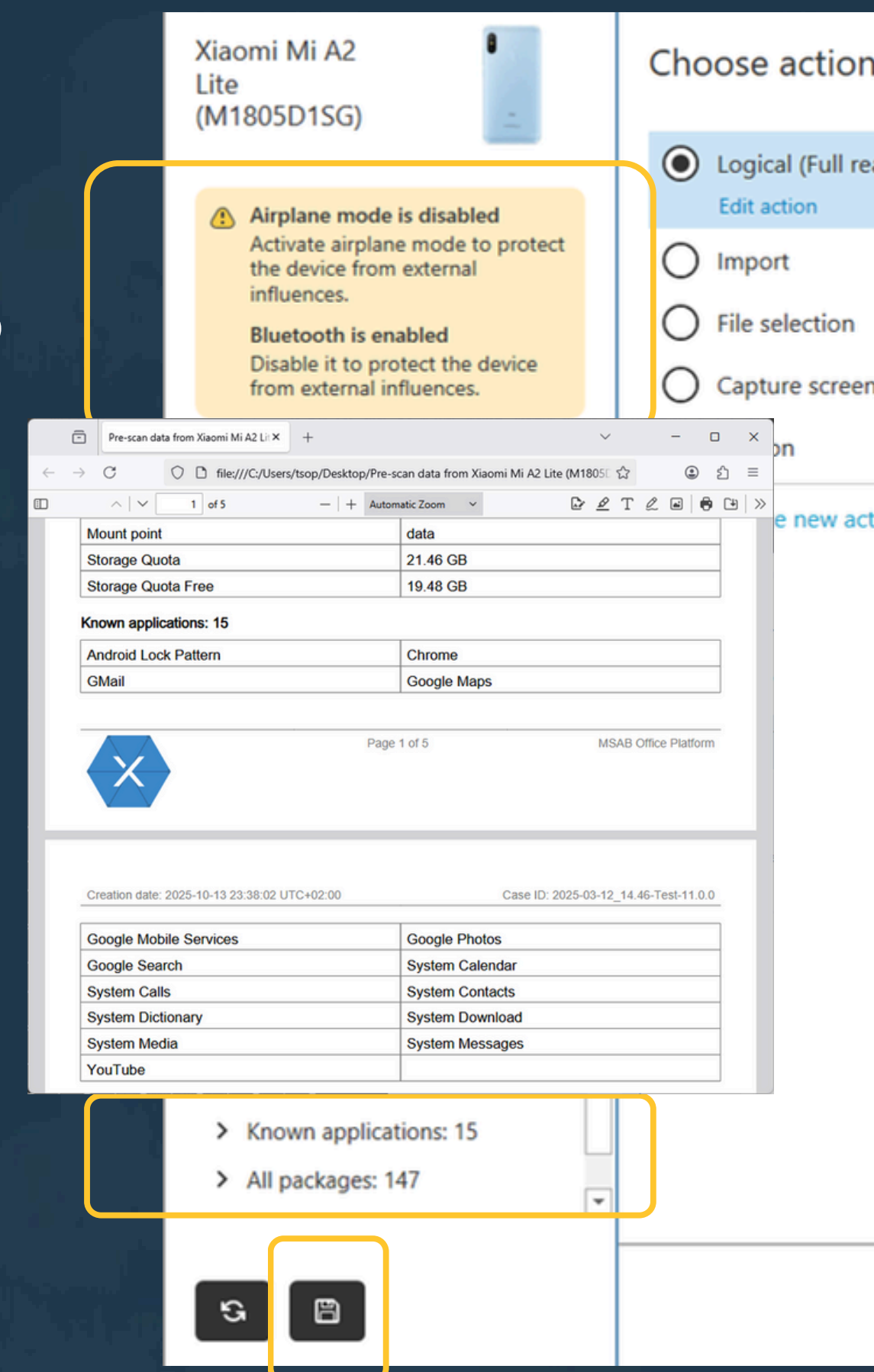
➤ Informações de armazenamento do dispositivo

➤ Aplicativos instalados (compatíveis e não compatíveis)

➤ Etc

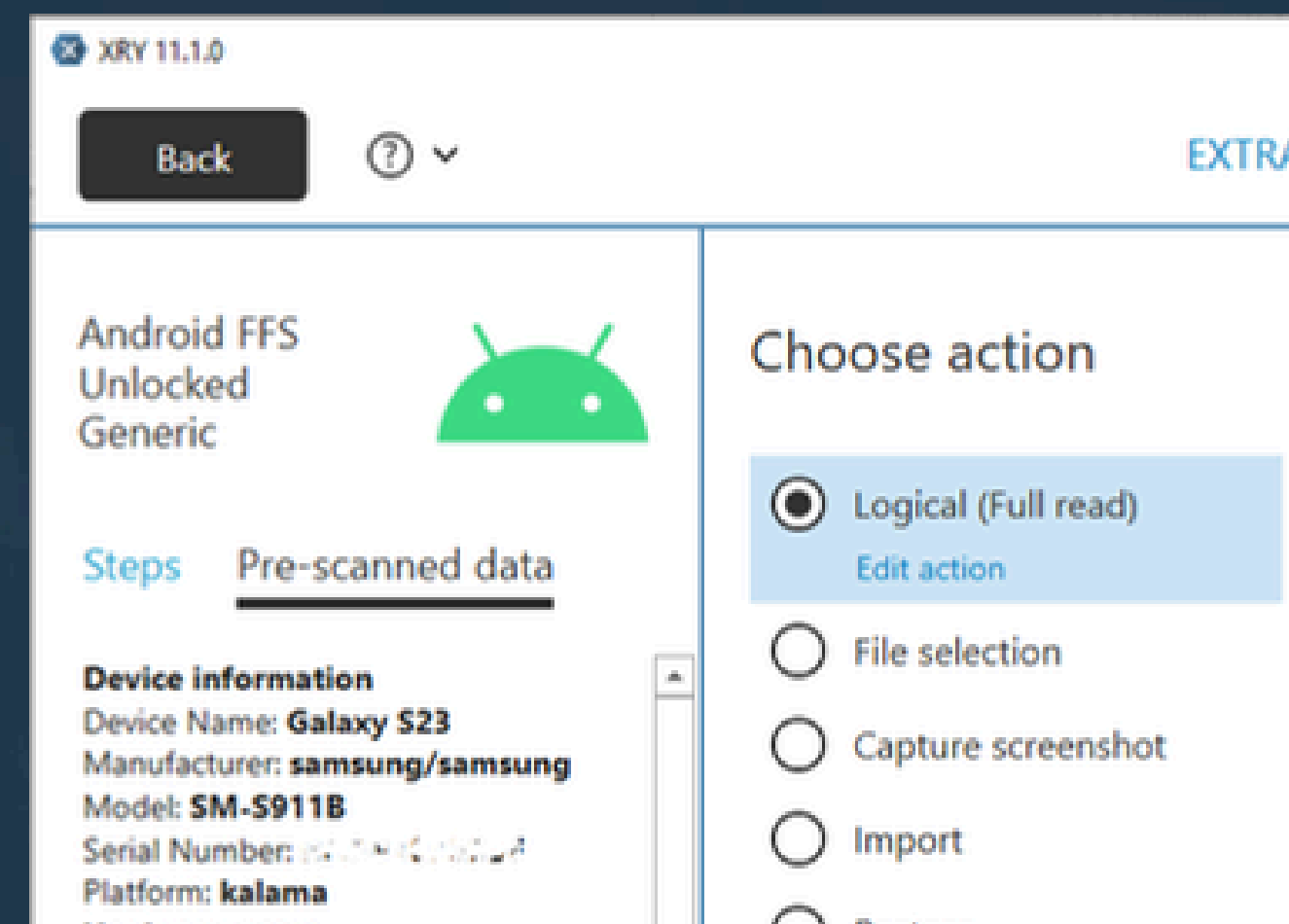
➤ Essas informações podem ser exportadas para PDF

➤ Não é necessária extração



Perfil genérico desbloqueado do Android FFS

- Um perfil genérico que incorpora 14 variantes de exploração diversas direcionadas a diferentes plataformas (a partir do XRY 11.2.0)
- Por exemplo, a partir da versão 11.2.0 do XRY, uma das variantes suporta FFS em dispositivos Samsung de última geração
- O primeiro módulo que é testado ao realizar uma extração de "Leitura Lógica Completa"
- Quando/se alguma das variantes do exploit for bem-sucedida, o usuário obtém uma extração completa do sistema de arquivos



Sistema de arquivos completo desbloqueado do Android

- Variantes de exploração aplicadas de forma inteligente a parâmetros específicos do dispositivo (por exemplo, SO, SPL, chipset)
- Antes de aplicar as variantes, o XRY realiza um teste de compatibilidade e limita o número de tentativas de exploração apenas às “compatíveis” [1]

PANGOLIN	Success	2025-09-09 14:08:48 UTC+02:00	Testing up to 4 variants for this device.
PANGOLIN	Success	2025-09-09 14:08:48 UTC+02:00	The following variants will be tested: Kamikaze, Binouze, V12, Zizou.
PANGOLIN	Success	2025-09-09 14:08:48 UTC+02:00	Running Kamikaze (Variant 1/4).
PANGOLIN	Success	2025-09-09 14:08:49 UTC+02:00	Starting service, attempt 1/5
PANGOLIN	Success	2025-09-09 14:09:03 UTC+02:00	The variant was successful.
PANGOLIN	Success	2025-09-09 14:09:03 UTC+02:00	Waiting for the extraction service...
PANGOLIN	Success	2025-09-09 14:09:03 UTC+02:00	The device is ready for Full Filesystem extraction.
PANGOLIN	Success	2025-09-09 14:09:03 UTC+02:00	Listing files, this may take a few minutes...

Listing files, found 3649...

Total: 8.3 %

[1]

Perfil genérico desbloqueado do Android FFS

- Recuperação do keystore de aplicativos suportados [1]
- Velocidades de extração rápidas [2]

PANGOLIN	Success	2025-09-09 14:11:37 UTC+02:00	Extracting keystore keys...
PANGOLIN	Success	2025-09-09 14:11:37 UTC+02:00	Extracting keystore data for user 0 from Session...
PANGOLIN	Success	2025-09-09 14:11:44 UTC+02:00	Extracting keystore data for user 0 from SimpleX...
PANGOLIN	Success	2025-09-09 14:11:48 UTC+02:00	Extracted keystore data: pref_attachment_encrypted_secret from network.loki.messenger
PANGOLIN	Success	2025-09-09 14:11:48 UTC+02:00	Extracted keystore data: pref_database_encrypted_secret from network.loki.messenger
PANGOLIN	Success	2025-09-09 14:11:48 UTC+02:00	Extracted keystore data: EncryptedDBPassphrase from chat.simplex.app
PANGOLIN	Success	2025-09-09 14:11:48 UTC+02:00	Extracting files...

Progress: 15.50% Time Elapsed: 00:00:29 Time Remaining: 00:02:40 Average Speed: 37603 KiB/s Current Speed: 43851 KiB/s Read: 1080 MiB

Total: 12.5 %

Abort

Exploração de vulnerabilidades de extração em sandbox no exemplo XRY

- Caso nenhuma das variantes de exploração do FFS funcione (ou nenhuma variante compatível seja encontrada), o XRY tentará uma das explorações de extração do sandbox
- Atualmente, existem 2 variantes
- Em caso de sucesso, o usuário obtém os dados do ambiente de teste (sandbox) dos aplicativos
- O ambiente de teste contém dados essenciais do aplicativo, como mensagens de bate-papo do WhatsApp, chamadas etc
- Extrações de agentes e do sistema de arquivos padrão também são realizadas com esses métodos

The screenshot displays the XRY application's extraction results. A table lists 10 successful extractions of various Android applications. A yellow box highlights the last row, which shows the extraction of WhatsApp. Below the table, a progress bar indicates the current status of the extraction process, with a label 'Preparing com.instagram.android for extraction (sandbox 11 out of 21)'. The progress bar shows a completion of 32.9%. An 'Abort' button is visible in the bottom right corner.

Platform	Status	Timestamp	Message
ANDROID	Success	2025-08-05 11:43:16 UTC+02:00	GrayOwl: Successfully prepared extraction of com.google.android.youtube for user 0.
ANDROID	Success	2025-08-05 11:43:19 UTC+02:00	GrayOwl: Successfully prepared extraction of com.google.android.apps.tachyon for user 0.
ANDROID	Success	2025-08-05 11:43:26 UTC+02:00	GrayOwl: Successfully prepared extraction of com.viber.voip for user 0.
ANDROID	Success	2025-08-05 11:43:48 UTC+02:00	GrayOwl: Successfully prepared extraction of com.google.android.googlequicksearchbox for user 0.
ANDROID	Success	2025-08-05 11:43:51 UTC+02:00	GrayOwl: Successfully prepared extraction of com.android.providers.userdictionary for user 0.
ANDROID	Success	2025-08-05 11:44:00 UTC+02:00	GrayOwl: Successfully prepared extraction of org.thoughtcrime.securesms for user 0.
ANDROID	Success	2025-08-05 11:44:04 UTC+02:00	GrayOwl: Successfully prepared extraction of com.android.providers.calendar for user 0.
ANDROID	Success	2025-08-05 11:44:19 UTC+02:00	GrayOwl: Successfully prepared extraction of org.telegram.messenger for user 0.
ANDROID	Success	2025-08-05 11:44:22 UTC+02:00	GrayOwl: Successfully prepared extraction of com.android.providers.downloads for user 0.
ANDROID	Success	2025-08-05 11:44:35 UTC+02:00	GrayOwl: Successfully prepared extraction of com.whatsapp for user 0.

Preparing com.instagram.android for extraction (sandbox 11 out of 21).

Total: 32.9 %

Abort

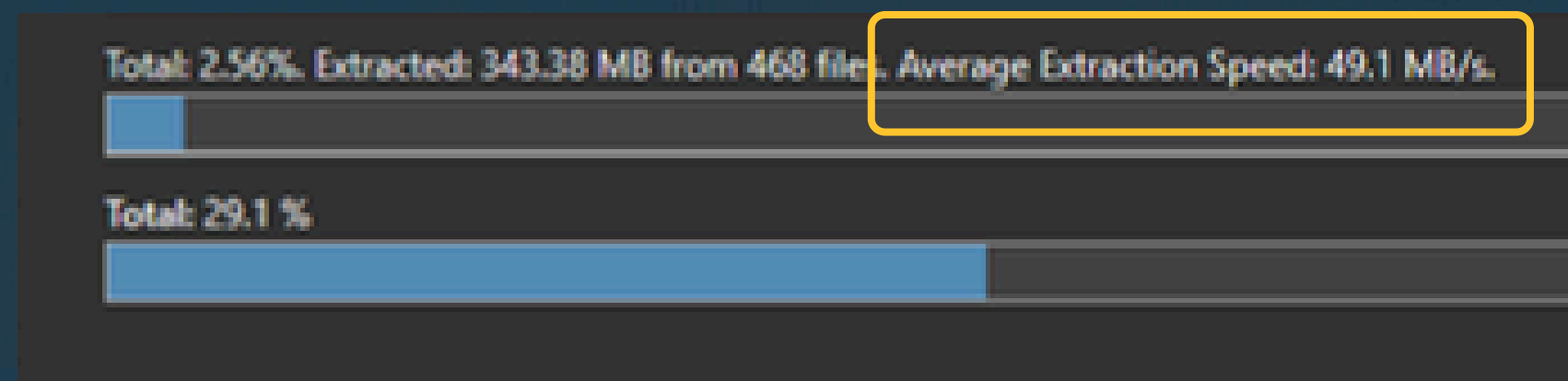
Extração lógica padrão (clássica)

Agente, backup, sistema de arquivos

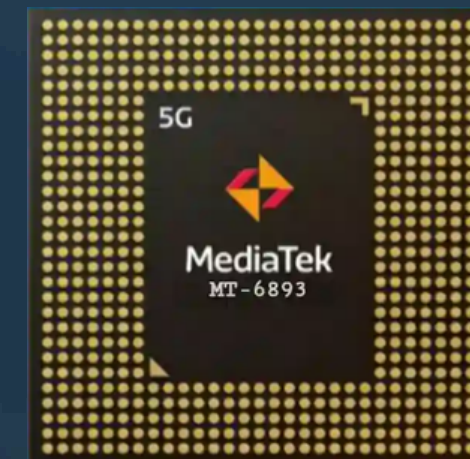
- Se nem a variante FFS e nem a variante Sandbox forem bem-sucedidas, o XRY realiza a extração lógica "clássica" por meio de:
 - Agente
 - Backup (com ou sem downgrade do aplicativo)
 - Sistema de arquivos (padrão)
- A extração lógica padrão também pode ser realizada em dispositivos Android com portas danificadas via Wi-Fi (veja o próximo slide)

Extrações de Wi-Fi do Android

- Quando a conectividade USB não é uma opção
- Suporta até Wi-Fi 7
- Extração lógica padrão
- Altas velocidades de extração



[Bloqueado] Android MediaTek Genérico Físico (Bypass/Força Bruta)



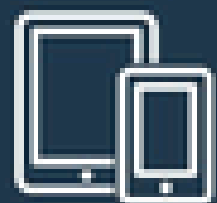
- Entrada: Dispositivos baseados em MTK bloqueados (e desbloqueados) no estado BFU
- Saída: Extração física (!)
- Processamento da criptografia: via ataque de força bruta ao código de bloqueio, executado no PC do usuário (no caso do XRY Pro, pode ser em PCs)
- Mais de 500 telefones já foram oficialmente testados/verificados com este método:
 - Mais de 20 chipsets, incluindo MT6833p, MT6833v, MT6853, MT6853v, MT6893, MT6899 e outros (no caso do XRY Pro, também inclui os mais recentes chipsets MTK 5G)
 - Todas as principais marcas baseadas em MTK: Alcatel, AT&T, BBK Vivo, Blackview, BLU, Cricket, Cubot, Huawei, Infinix, LG, Nokia, Oppo, OUKITEL, TCL, Tecno, T-Mobile, Ulefone, WIKO, Xiaomi, ZTE, Samsung, etc...
- Perfil genérico MediaTek para Android: pode ser testado em dispositivos MTK não testados (com os chipsets acima e/ou combinações de fornecedores)



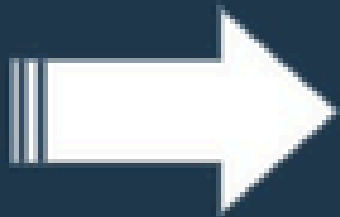
Android MediaTek Generic

A extração por si só não basta: Decodificação de dados

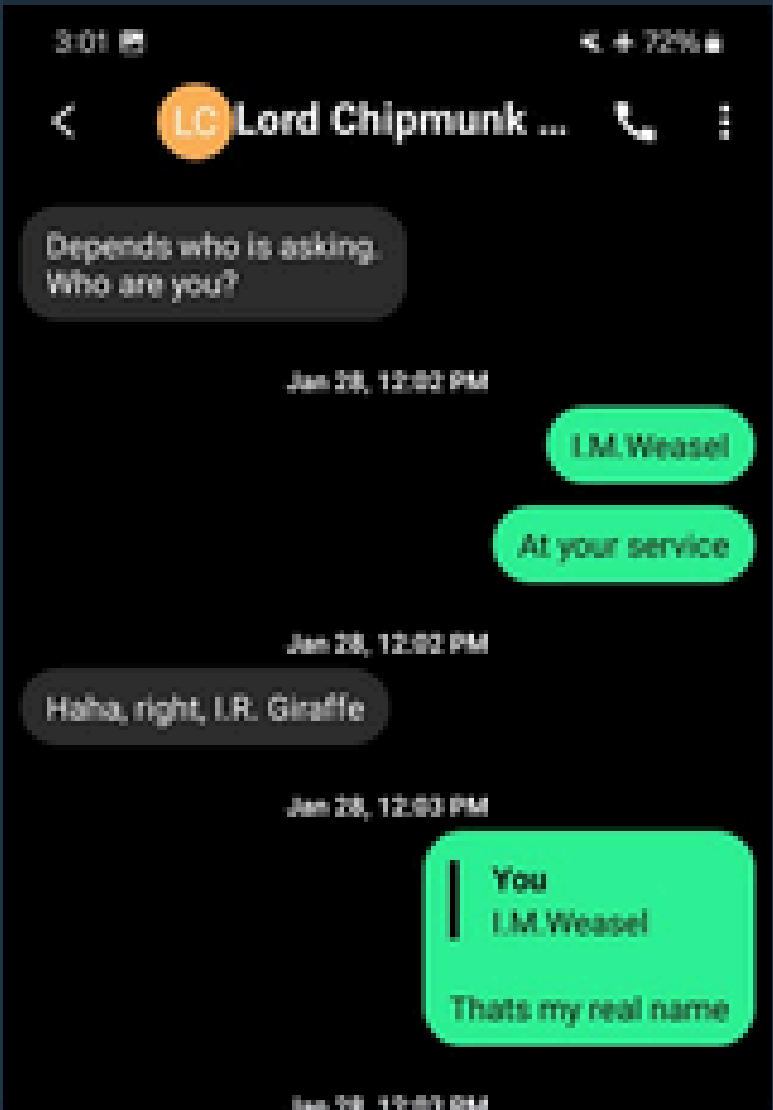
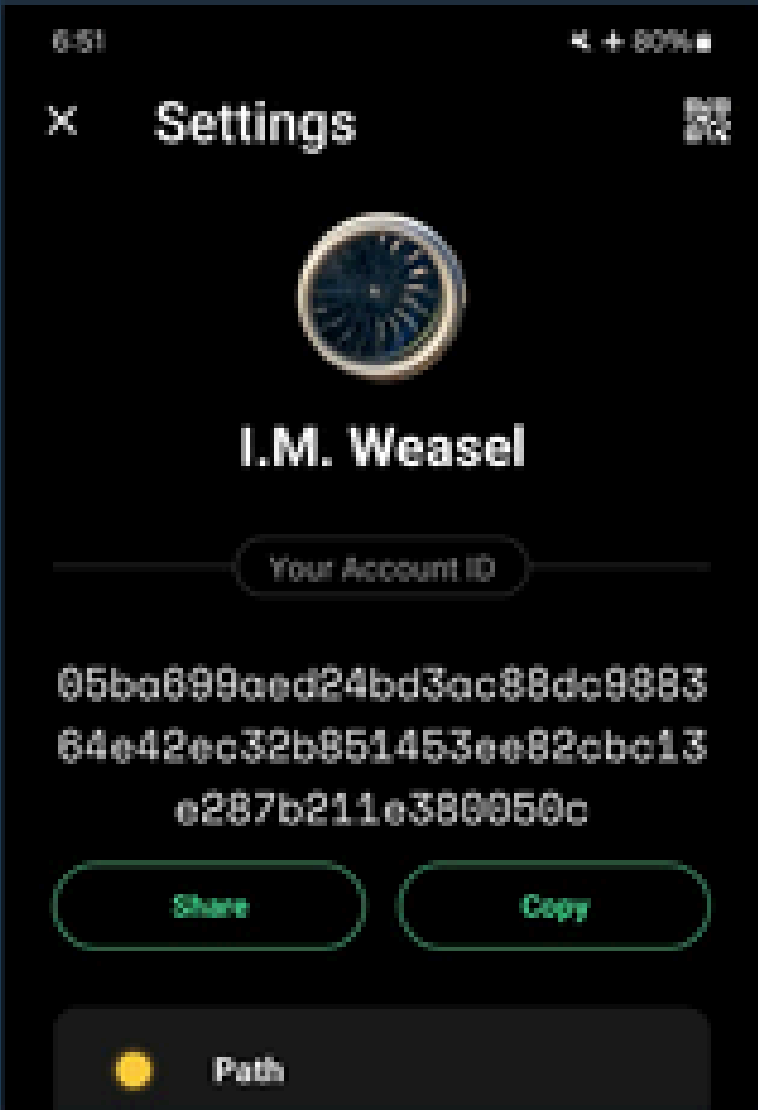
Dispositivo
examinado



Fase de
Extração



Dados
extraídos



TABLES |←

Select a table to view data

table	count
sms	7 (0)
sms_fts_config	1 (-)

TABLES |←

Select a table to view data

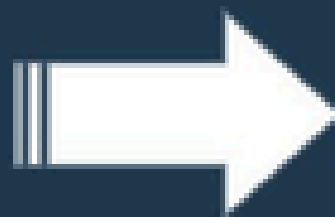
table	count
sms	4 (0)
msms_fts_config	1 (-)
msms_fts_data	1 (-)
msms_fts_doc1	1 (-)
msms_fts_idx	1 (-)
open_group_a	1 (-)
open_group_b	1 (-)
open_group_c	1 (-)

XML viewer

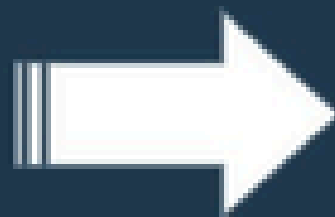
```
<boolean name="has_viewed_seed" value="true" />
<string
  name="pref_local_number">05ba699aed24bd3ac88dc988364e42ec3
<string name="pref_database_encrypted_secret">
  {"data":"RecTaDWnf4E9QOstyVGgBQV7gUB1SHcdBm3U08h3ds4oM
</string>
<int name="pref_notification_channel_version" value="3" />
<string name="pref_profile_name">I.M. Weasel</string>
<int name="pref_local_registration_id" value="15106" />
<string name="pref_profile_avatar_url">http://filev2.getsession.org/fi
<long name="pref_last_version_check" value="1738088422913" />
</map>
```

A extração por si só não basta: Decodificação de dados

Dados extraídos



Fase de decodificação



Dados decodificados



TABLES |←

Select a table to view data

name 7

TABLES |←

Select a table to view data

name 4

XML viewer

```
<boolean name="has_viewed_seed" value="true" />
<string
  name="pref_local_number">05ba699aed24bd3ac88dc988364e42ec3
<string name="pref_database_encrypted_secret">
  ("data":"RucTaDWnf4E9QOstyVGgBQV7gUB15HcDBm3U08h3ds4oNU
  </string>
<int name="pref_notification_channel_version" value="3" />
<string name="pref_profile_name">I.M. Weasel</string>
<int name="pref_local_registration_id" value="15106" />
<string name="pref_profile_avatar_url">http://filev2.getsession.org/fi
<long name="pref_last_version_check" value="1738088422913" />
</map>
```

Timeline Maps

Thread

Lord Chipmunk I.M. Weasel

0579483026b15c416c2c2e7734 05ba699aed24bd3ac88dc9883

12:01:46

Depends who is asking. Who are you?

12:01:17

I.M. Weasel

12:00:37

All your service

12:00:32

That's my real name

12:00:09

Guess where

OK

Person

Person of interest

Join with person...

I.M. Weasel

Edit name... Edit picture...

Name I.M. Weasel

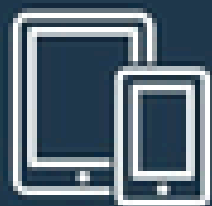
Session (App) ID 05ba699aed24bd3ac88dc988364e42ec326851453aed2c6c13e287b211e588050a

Show artifacts where identities for I.M. Weasel appear

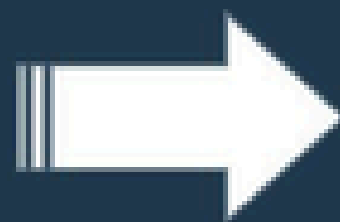
Other persons that might be I.M. Weasel

XRY: Extração e Decodificação

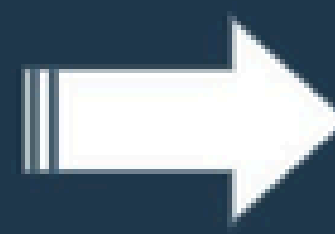
Dispositivo
examinado



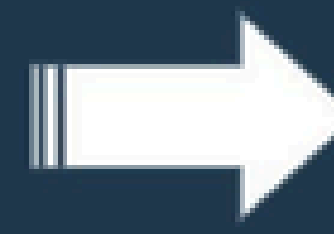
Fase de
Extração



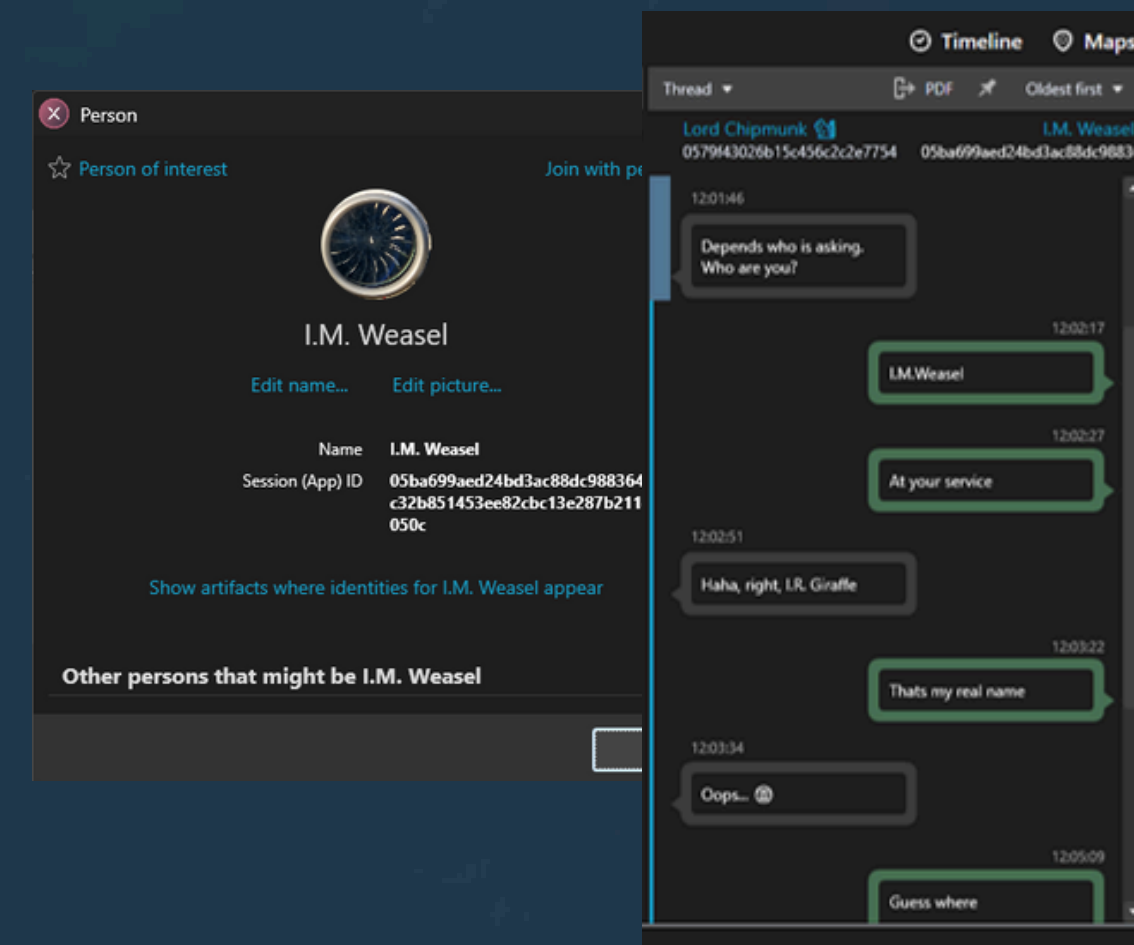
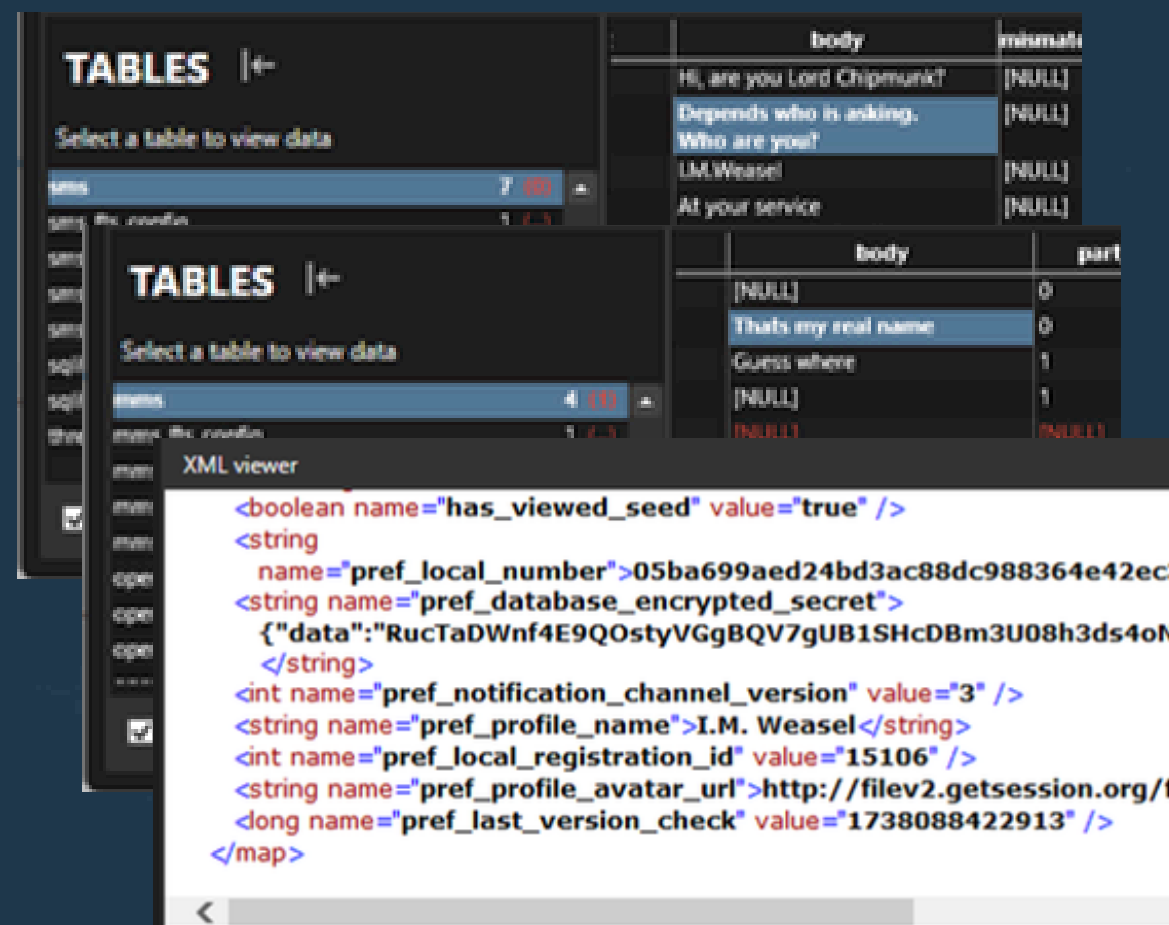
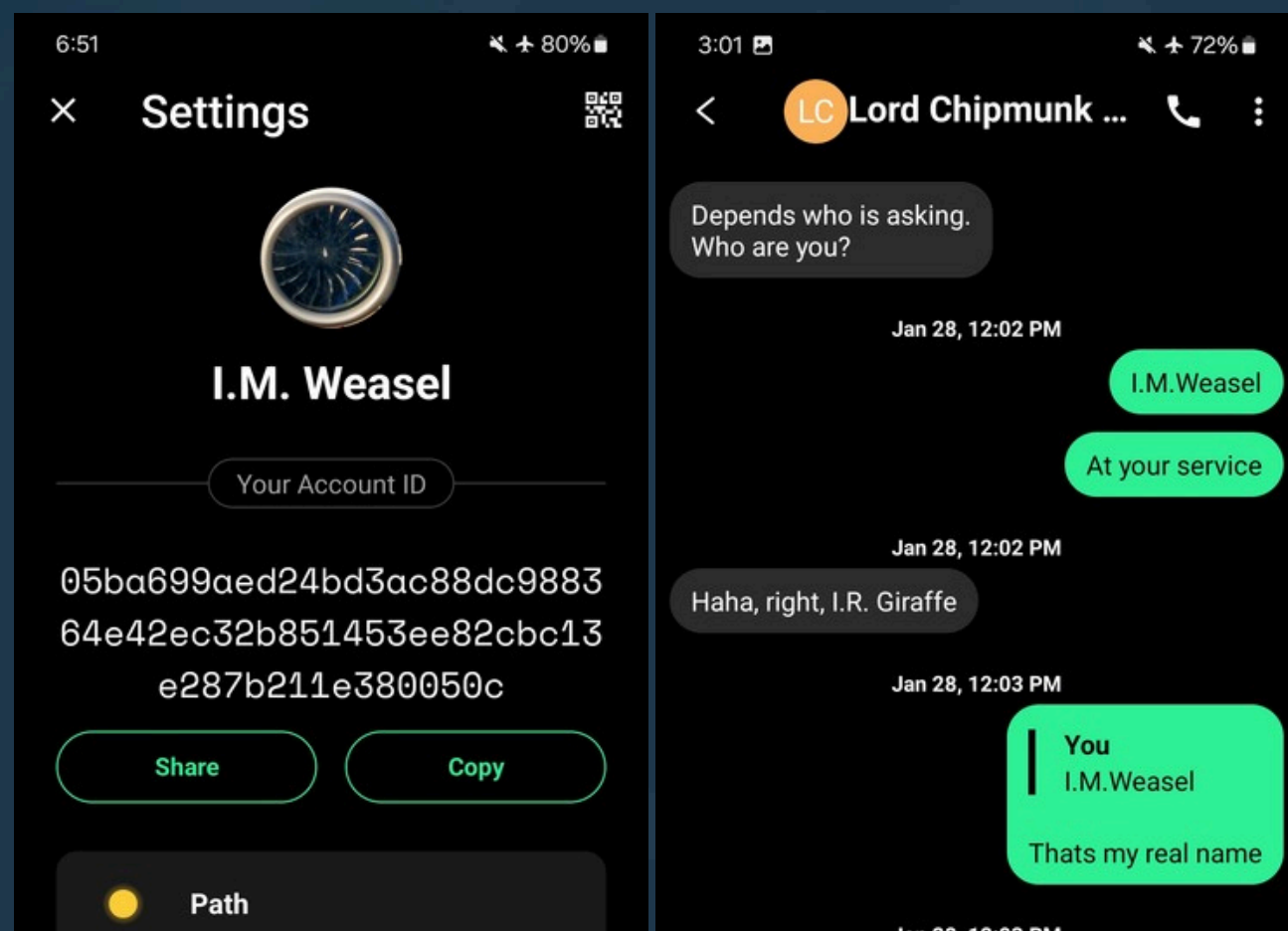
Dados
extraídos



Fase de
decodificação

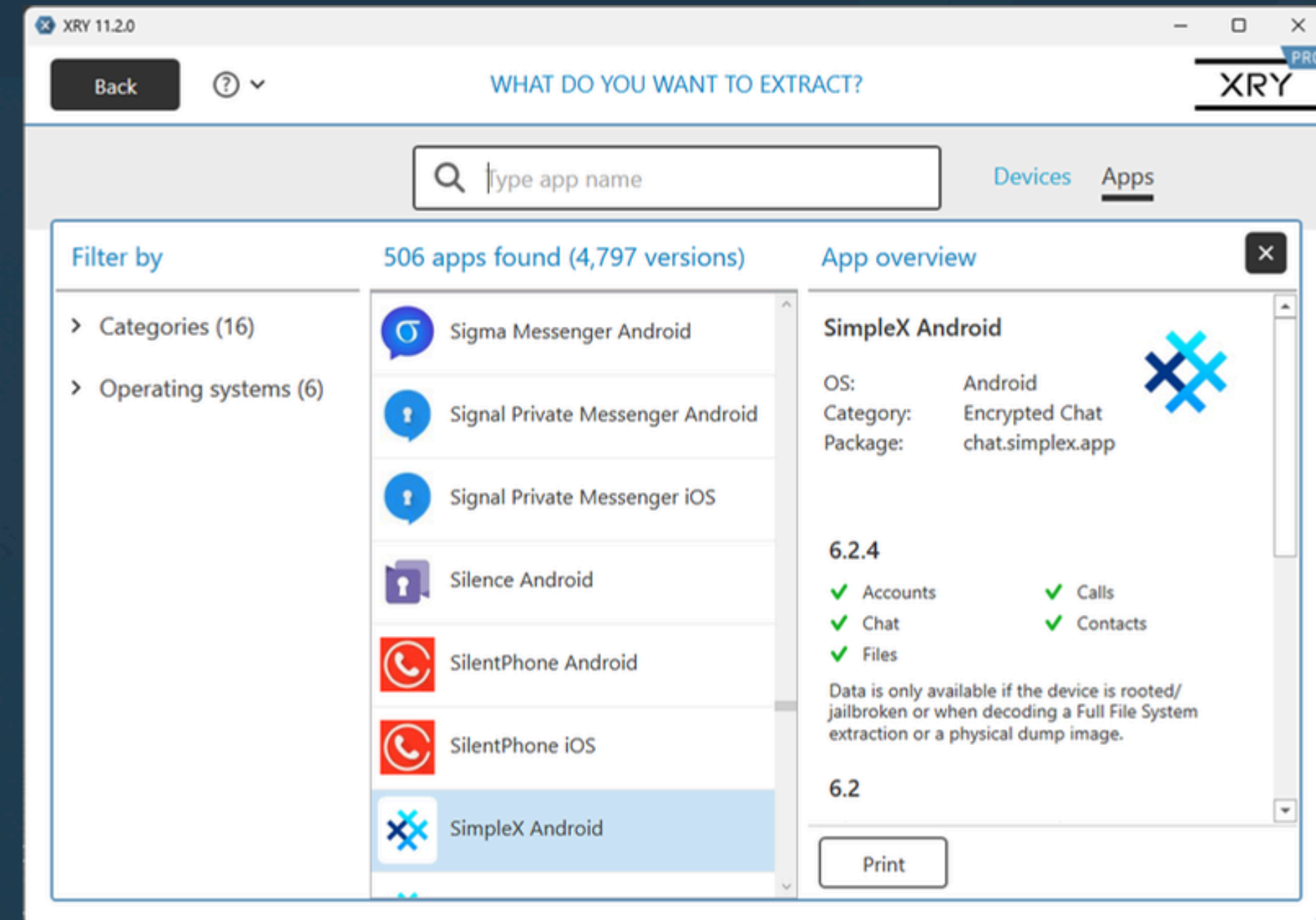


Dados
decodificados



Decodificação do aplicativo XRY

- O XRY Pro suporta nativamente a decodificação de mais de 500 aplicativos (e mais de 4700 versões)
- Além disso, o XRY decodifica dados importantes de aplicativos do sistema para Android e iOS



Recursos adicionais de decodificação (conversão de voz em texto, OCR, ImgRec)

Process options: Logical (Full read)

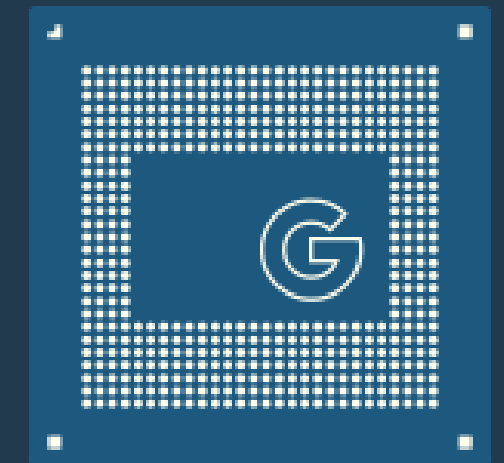
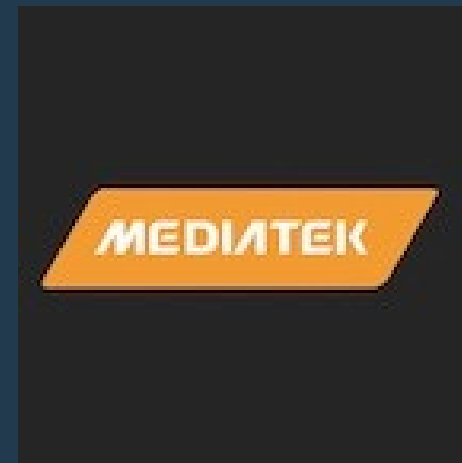
Section	Details
General	
Android extraction	☐ Only include decoded data in the XRY file This option can reduce the file size of the XRY file. If you only include data that is decoded, you cannot re-decode the XRY file, or validate the origin of the decoded data in your forensic report. The raw binary data will be removed.
iOS extraction	
SIM card	☐ Generate video preview and thumbnails
Data types	
Decoding	☒ Run content recognition Install CUDA (version 11.5) and use an Nvidia graphics card with 4GB of memory and Compute Capability 5.0 or higher to optimize the speed of the content recognition function. Examples of supported categories: Weapons, Drugs, Vehicles, Financial, People, Electronics, Faces, Documents, Flags, Tattoos, Screenshots, and Nudity. To optimize the extraction time, leave the box unchecked. ☒ Run optical character recognition (OCR) Convert printed text found in pictures, such as photos of documents, into transcribed text that is fully searchable in XAMN. To optimize the extraction time, leave the box unchecked. ☒ Run Speech-to-text Convert speech from audio files into transcribed text that is fully searchable in XAMN. Note that Ffmpeg must be installed on the computer. Make sure that its location is included in the system environment variable 'Path', and that XRY has been restarted after the installation. To optimize the extraction time, leave the box unchecked.

XRY help Save Cancel



Alguns exemplos de recursos avançados XRY Pro

XRY Pro: Plataformas e fabricantes de dispositivos compatíveis



vivo



xiaomi



ZTE



SONY

alcatel



oppo



HUAWEI



CUBOT

DOOGEE

Blackview

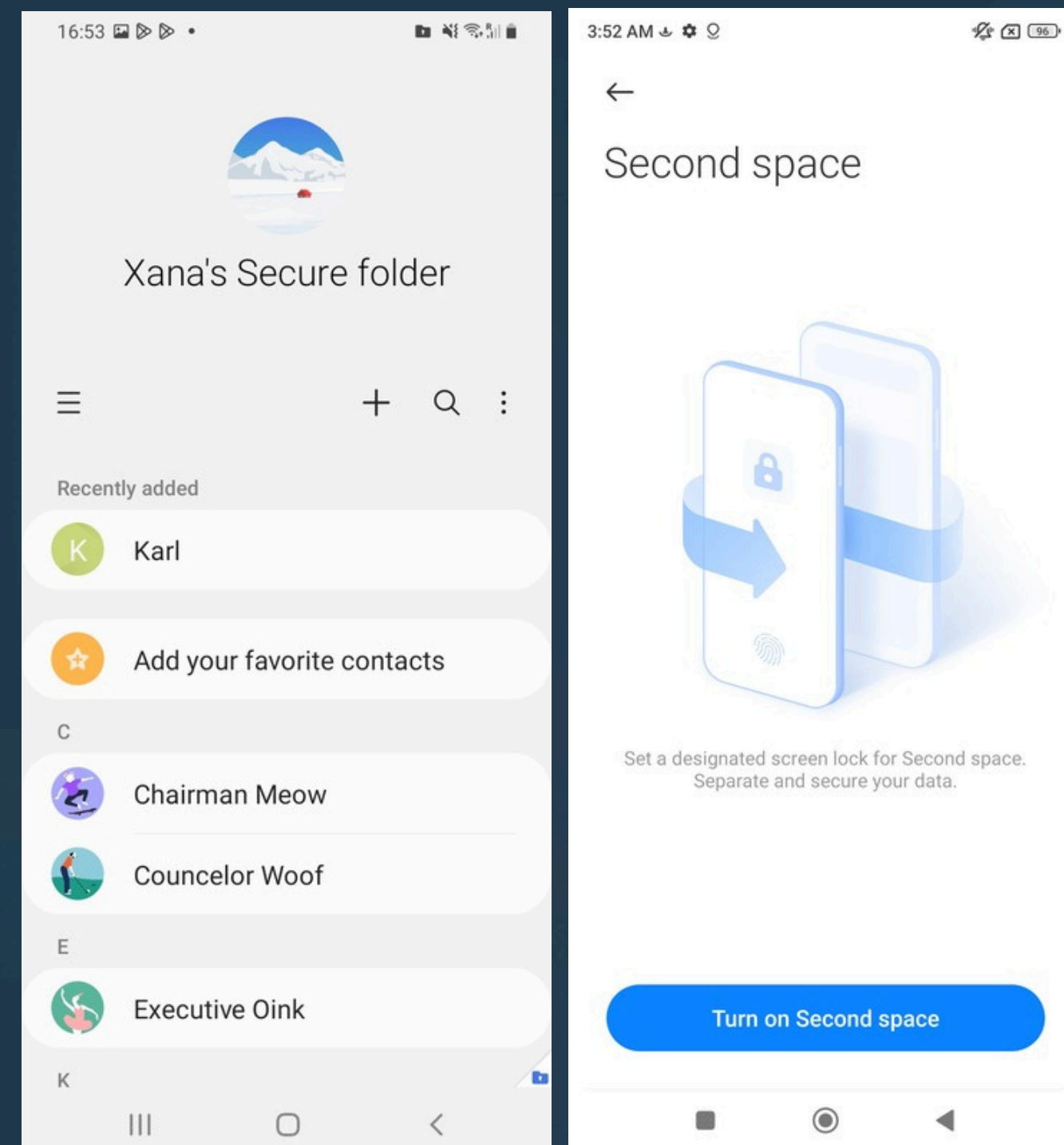


XRY Pro: Plataformas e fabricantes de dispositivos compatíveis

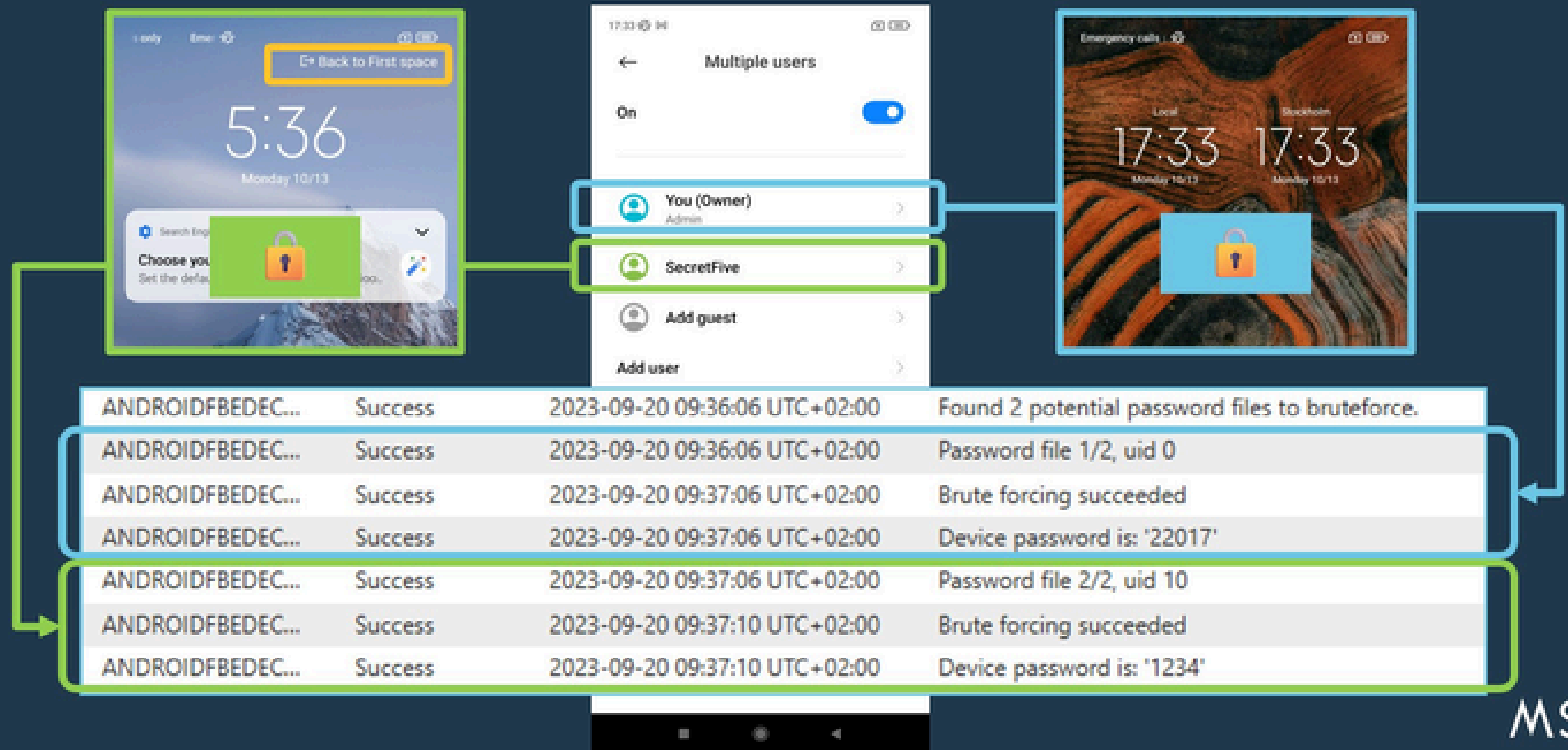
- Suporte à plataforma Unisoc (incluindo Samsung, Oppo, Realme, Motorola, Nokia e outras)
- Exploração de vulnerabilidades AFU e BFU para dispositivos Samsung/Exynos das séries A, J, S, Note e Ultra até a série S24 (incluindo Plus e Ultra)
- Explorações de segurança da Samsung/Qualcomm para dispositivos das séries A, J, S, Note e Ultra até os modelos S22, S23, S24, S25, Z Flip 4-7 e Z Fold 4-7
- Explorações de vulnerabilidades da Qualcomm para outros fornecedores (incluindo Xiaomi, OnePlus, Oppo, Sony, Nokia, LG e outros)
- Chipsets MediaTek 5G mais recentes
- + todos os métodos de extração e recursos de decodificação do XRY Office
 - Incluindo MediaTek, Kirin, Samsung/Exynos, LG e extração FFS desbloqueada
 - Incluindo decodificação por IA, como conversão de fala em texto, OCR e reconhecimento de conteúdo

XRY Pro: Suporte para armazenamento oculto/seguro (também conhecido como Android multiusuário)

- O XRY Pro suporta a detecção e a quebra de senha de armazenamento seguro do fornecedor por força bruta ou mesmo a sua evasão
- Alguns exemplos de armazenamento seguro/oculto suportados:
 - Pasta Segura Samsung
 - Xiaomi Second Space
 - Implementações de outros fornecedores para multiusuário



Exemplo: Gerenciamento de múltiplos usuários do Android no XRY Pro

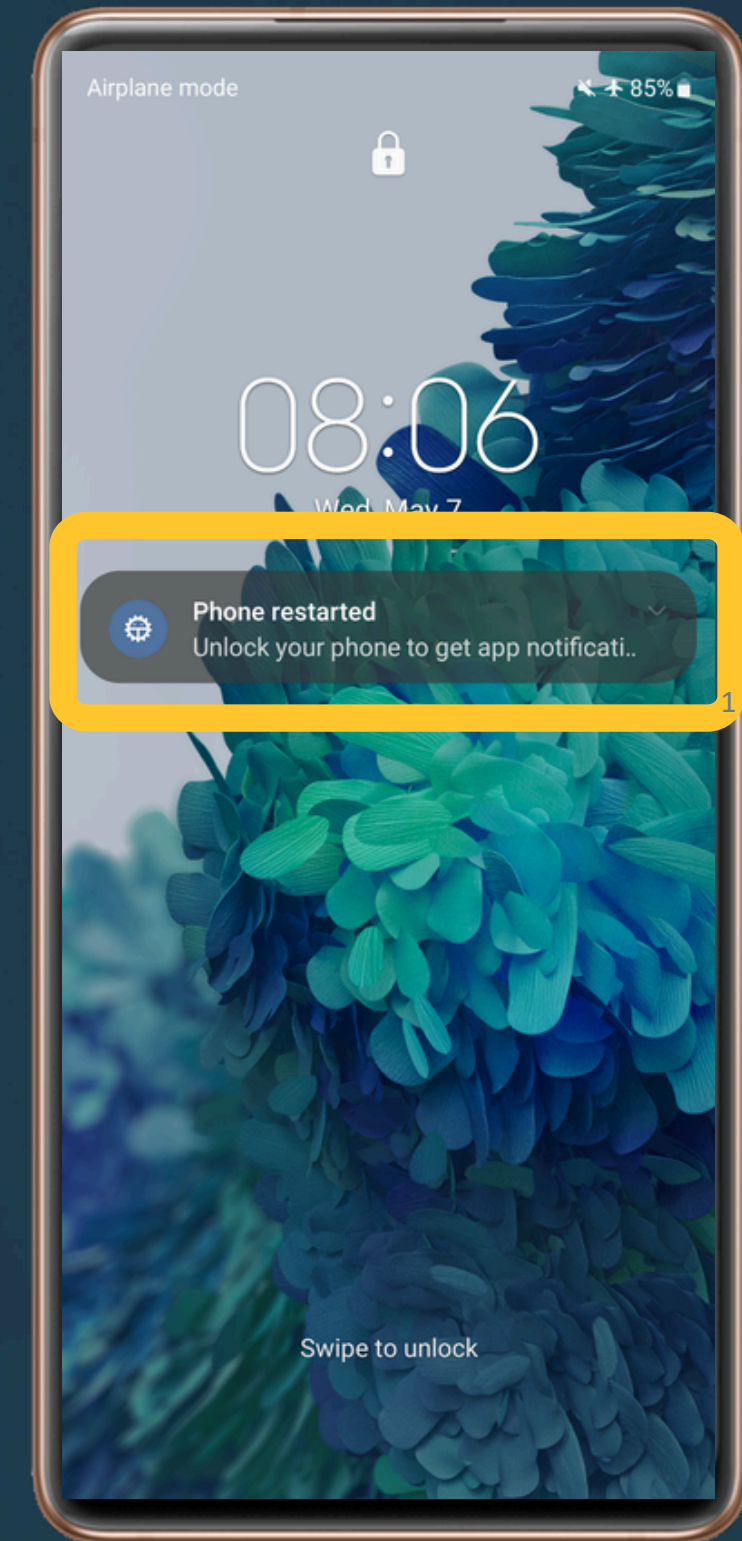


Extrações físicas/FFS com XRY Pro em BFU!

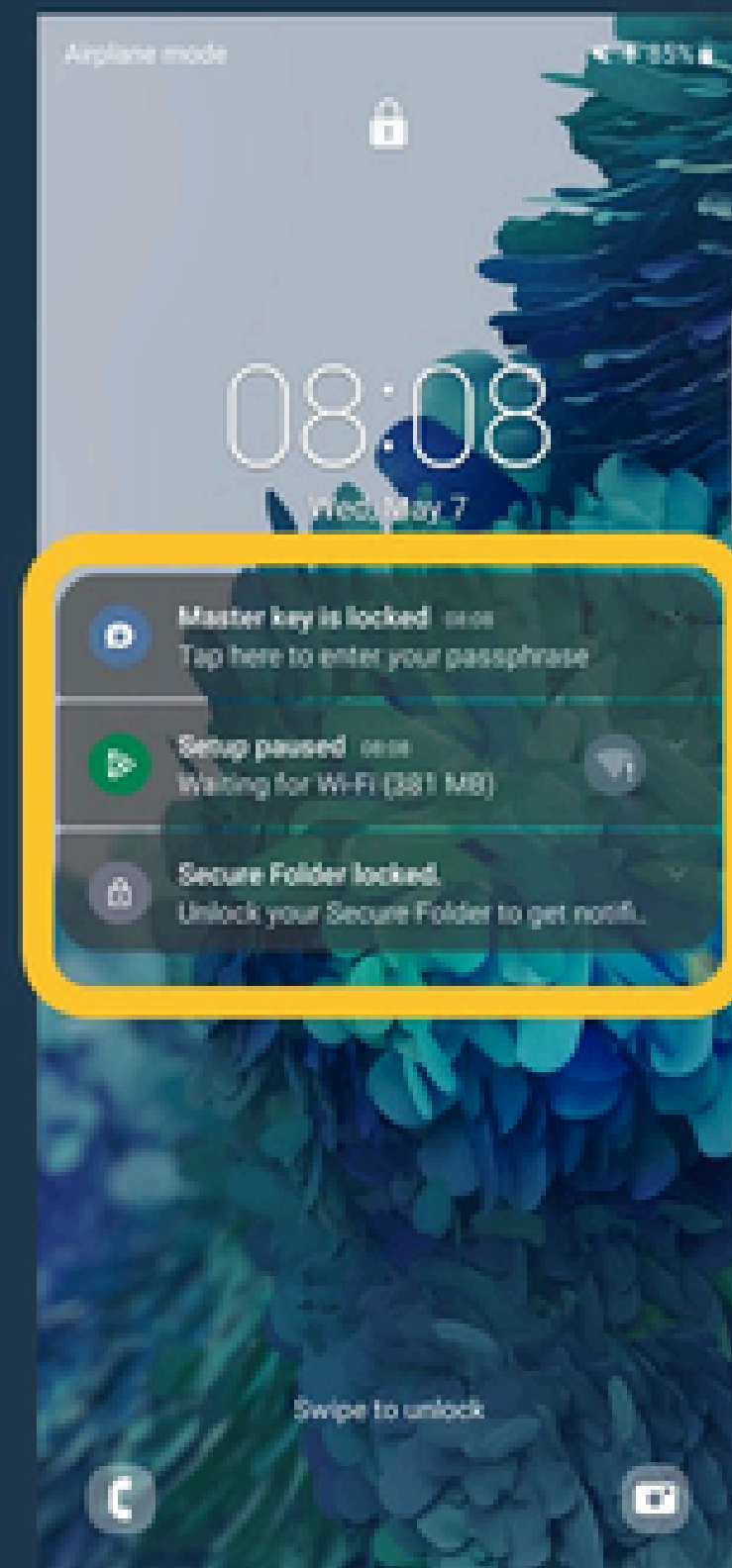
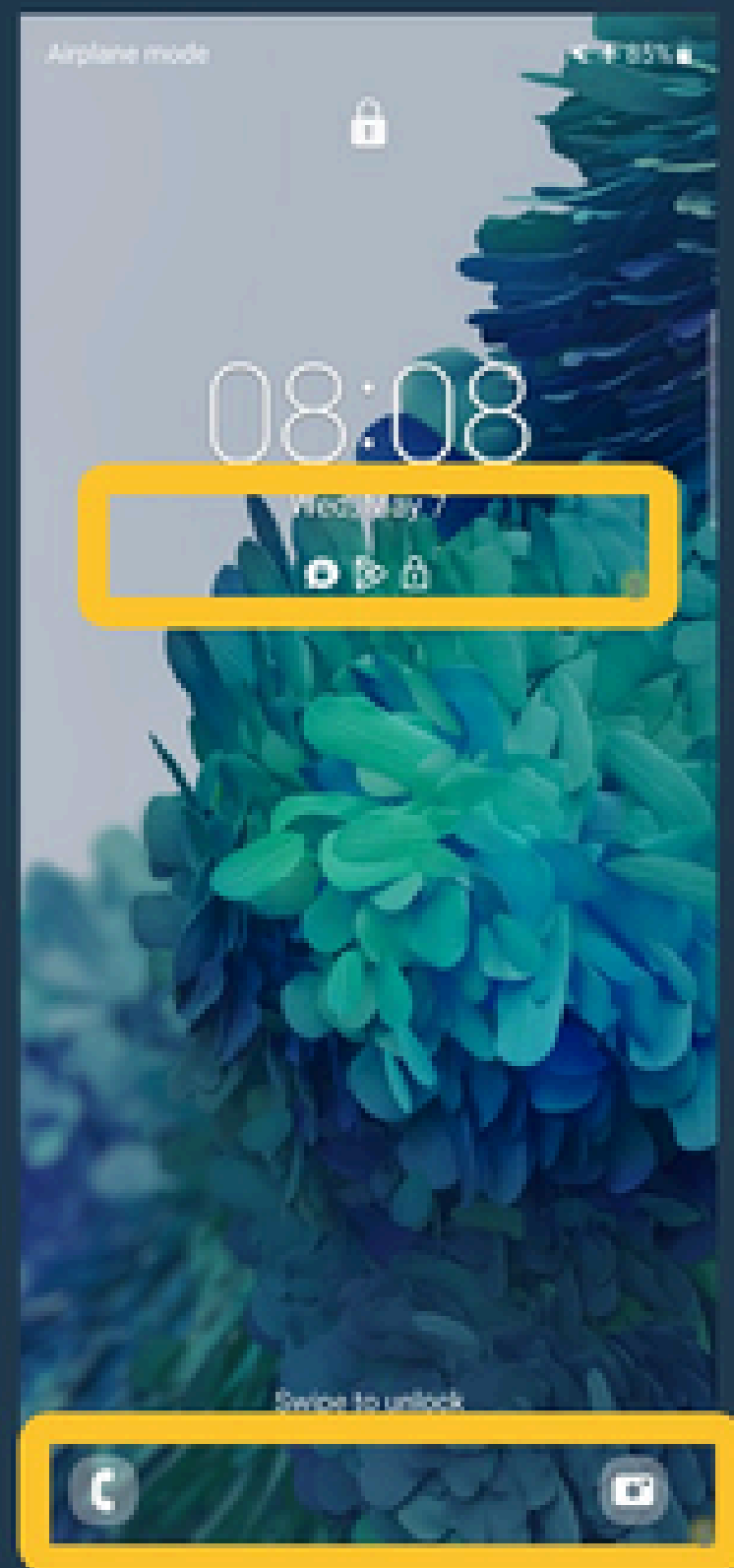
- No "mundo XRY", os dispositivos podem ser suportados nos estados de inicialização AFU, BFU ou em ambos, dependendo da solução/método específico. Mas, independentemente disso,
- **Lembre-se: as extrações BFU no XRY (Pro) são físicas/de sistema de arquivos completos**
- O que é o estado AFU?
 - **AFU = Após o Primeiro Desbloqueio** - o dispositivo está LIGADO e inicializado, e o proprietário do dispositivo fez login (inseriu o código de bloqueio) desde a última inicialização; o dispositivo pode ser bloqueado
 - O dispositivo deve permanecer LIGADO sem ser desligado ou reiniciado para manter o estado AFU!
- O que é o estado BFU?
 - **BFU = Antes do Primeiro Desbloqueio** - o dispositivo está (normalmente) DESLIGADO ou em estado de inicialização a frio, ou seja, o proprietário do dispositivo NÃO fez login (NÃO inseriu o código de bloqueio) desde a última inicialização

Identificar o estado de inicialização do dispositivo: Antes do primeiro desbloqueio (BFU)

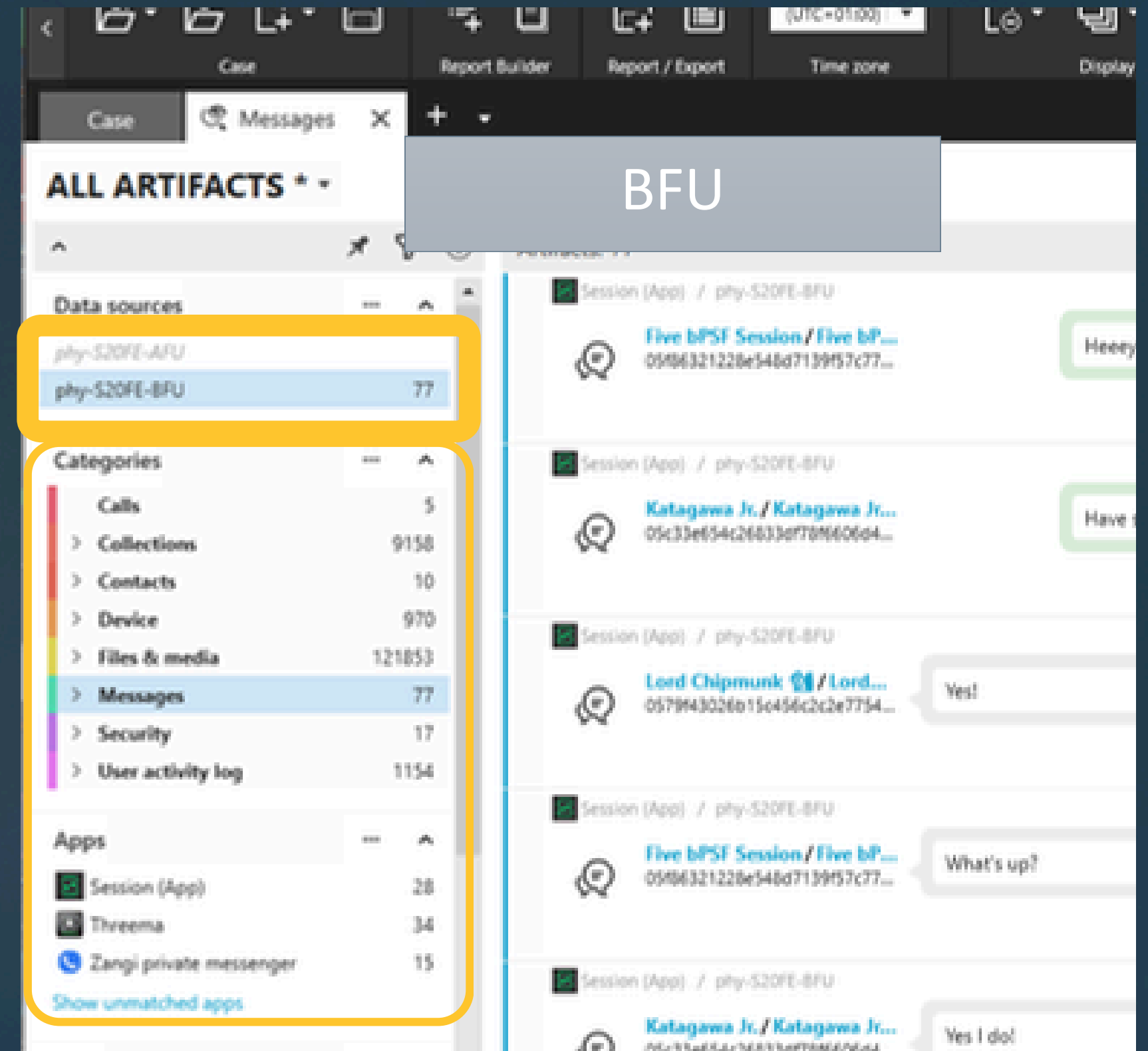
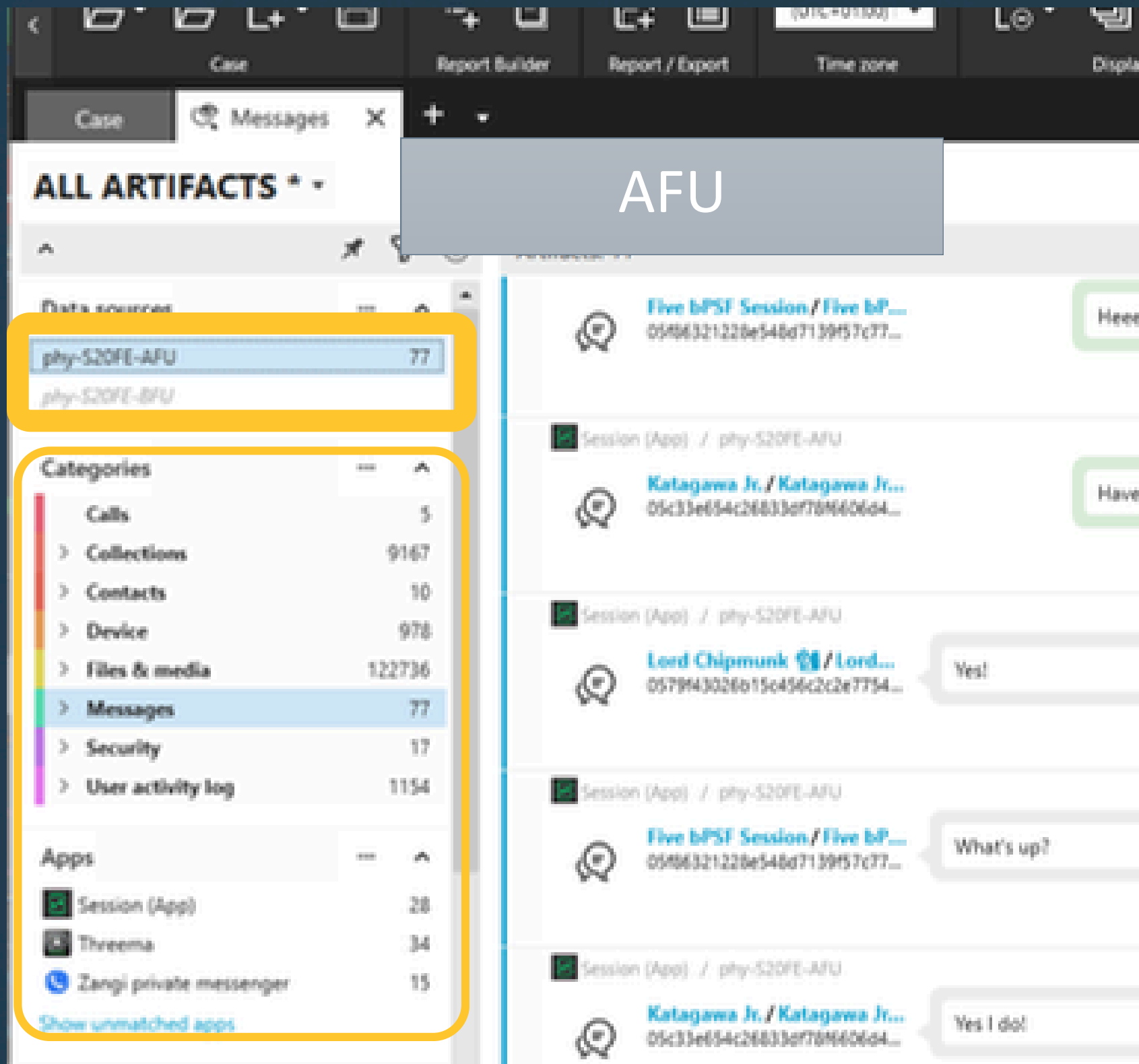
- O dispositivo está no estado de inicialização BFU quando:
 - O dispositivo está DESLIGADO
 - O dispositivo é reiniciado (automático) / inicializado a frio e as credenciais do usuário (PIN/Padrão/Senha, etc.) não foram inserida desde então



Identificar o estado de inicialização do dispositivo: Após o primeiro desbloqueio (AFU)



Exemplo: Extração de AFU e BFU do mesmo dispositivo XRY Pro



Gerenciamento de código de bloqueio e criptografia de dispositivos no XRY Pro

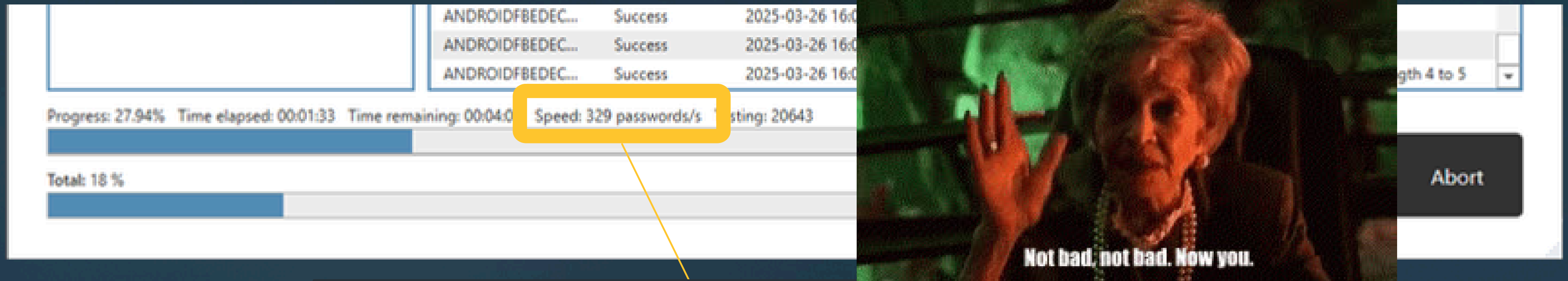
- Alguns métodos de extração XRY (Office/Pro) podem contornar o código de bloqueio (independentemente da complexidade) e descriptografar os dados
- Alguns métodos XRY (Pro) podem contornar e descriptografar os dados e, opcionalmente, realizar um ataque de força bruta ao código de bloqueio
- Alguns métodos XRY (Office/Pro) exigem o uso de força bruta no código de bloqueio para descriptografar os dados

...quão rápido podemos usar o Brute-Force no XRY Pro

- O Brute-Force é uma busca exaustiva por PIN/padrão/senha ("adivinhação"), que pode ser executada em (dependendo do método):
 - Brute-Force no dispositivo = a "tentativa de adivinhação" é executada no telefone analisado
 - A velocidade do Brute-Force geralmente fica entre 10 e 30 combinações por segundo
 - Brute-Force fora do dispositivo = a "tentativa de adivinhação" é executada no(s) computador(es) do examinador
 - Velocidades típicas de BF observadas em máquinas com CPU única: entre 200 e 3500 combinações/segundo (dependendo do desempenho da CPU)
 - A ferramenta XRY Brute Storm (força bruta distribuída) pode ser usada; nesse caso, a velocidade de BF é proporcional ao número de clientes conectados

Exemplo: Velocidade de força bruta XRY (mesma máquina)

Em um PC XRY Pro com i7-1185G7, uma senha de 5 dígitos "22017" é encontrada em aproximadamente 63 segundos.



The screenshot shows the XRY Pro interface with a progress bar at 27.94% and a speed of 329 passwords/s. A yellow box highlights the speed value, with a line pointing to the calculation below. To the right is a video frame of a woman saying "Not bad, not bad. Now you." and an "Abort" button.

Android ID	Status	Time
ANDROIDFBEDEC...	Success	2025-03-26 16:00
ANDROIDFBEDEC...	Success	2025-03-26 16:00
ANDROIDFBEDEC...	Success	2025-03-26 16:00

Progress: 27.94% Time elapsed: 00:01:33 Time remaining: 00:04:00 Speed: 329 passwords/s Testing: 20643

Total: 18 %

Not bad, not bad. Now you.

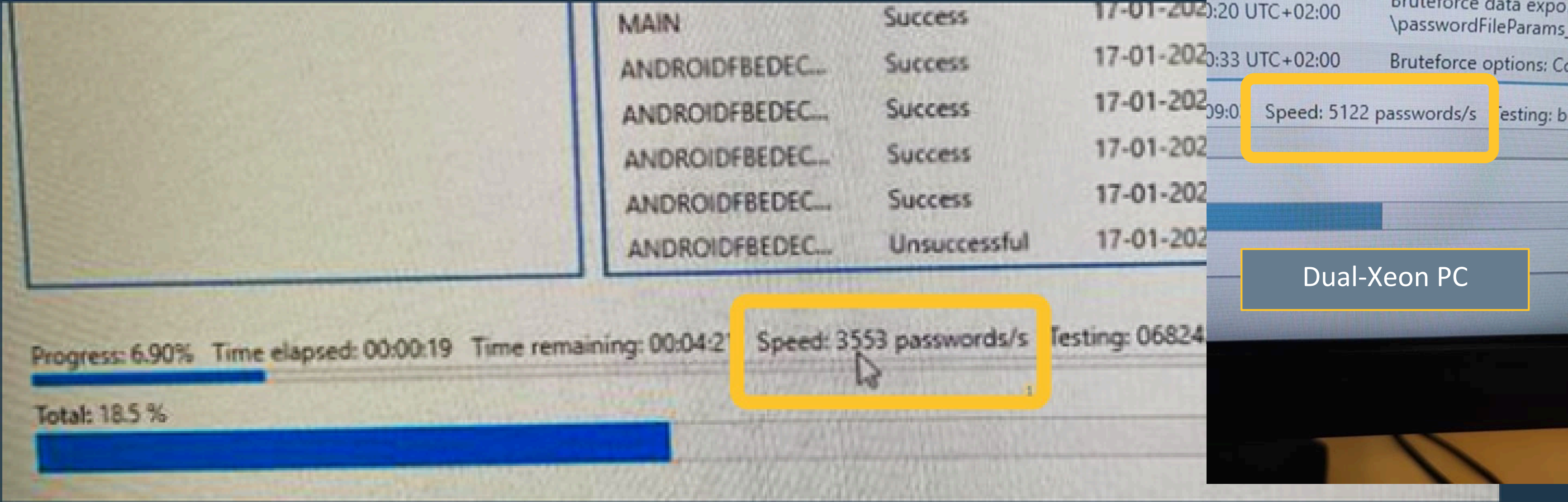
Abort

$329 \text{ PpS (Senhas por segundo)} = 329 * 60 \text{ ApM}$

...19740 ApM

Alguns exemplos relatados por clientes: Velocidades de força bruta

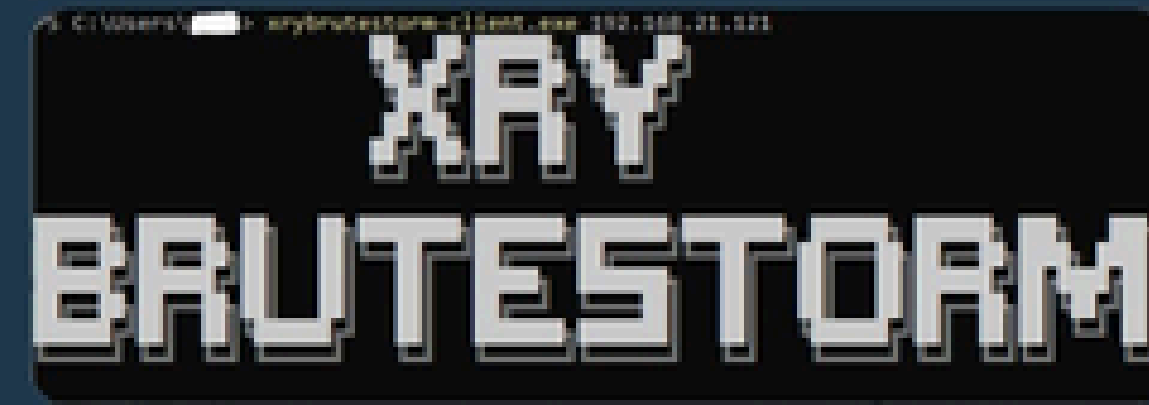
● 19 (13th generation)



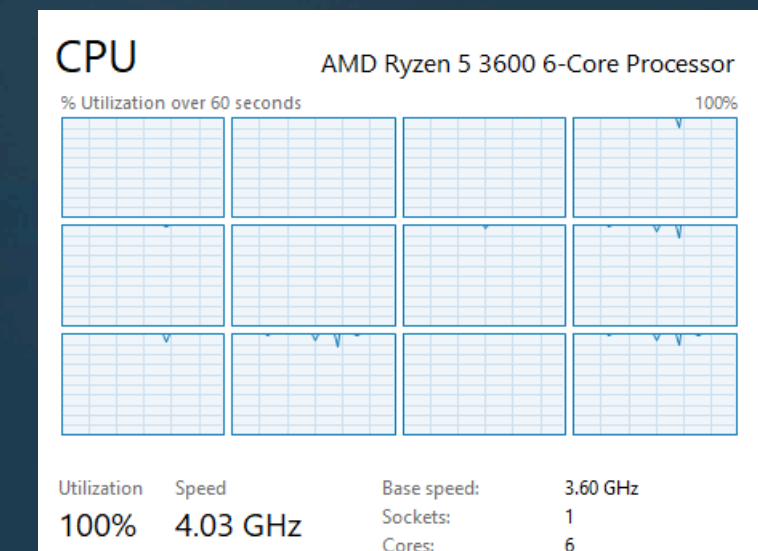
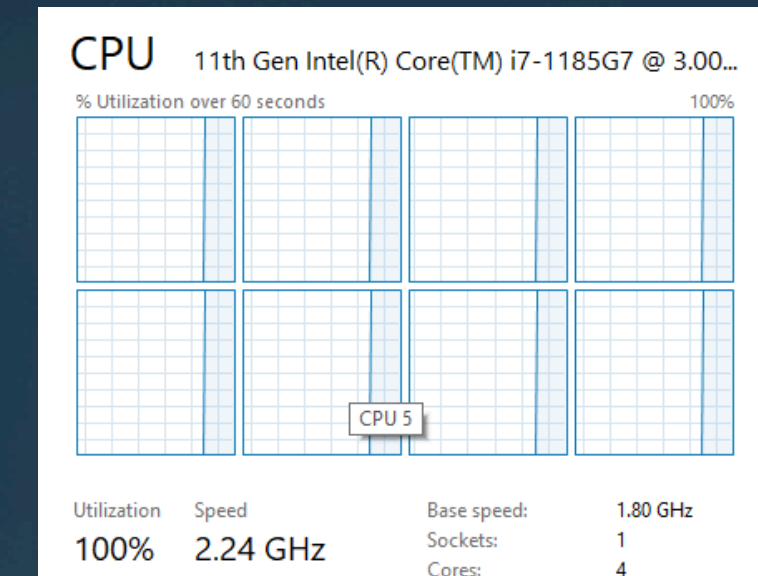
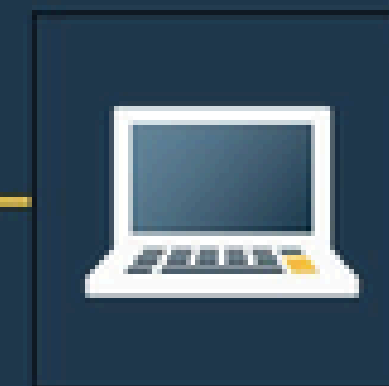
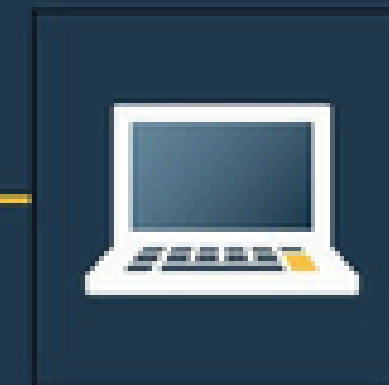
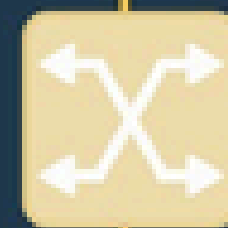
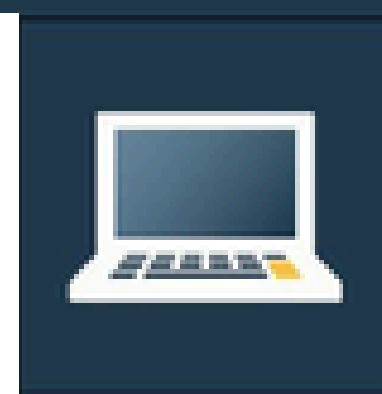
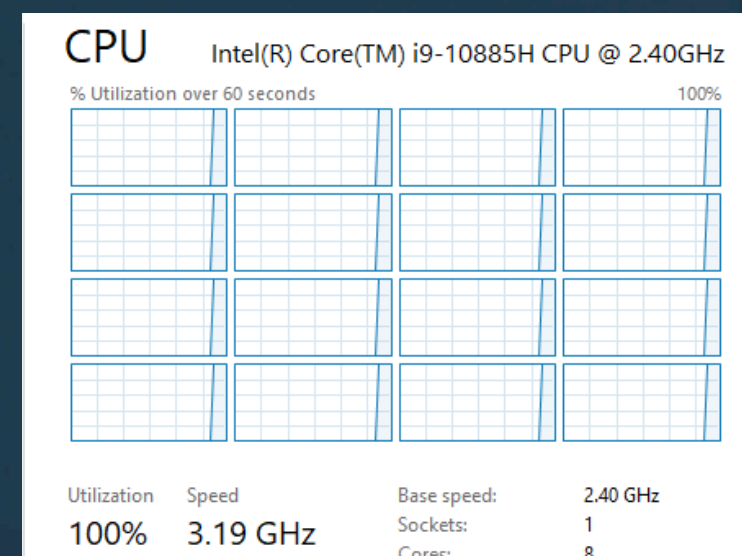


Precisa resolver isso mais rápido?
Apresentamos o XRY BruteStorm

Exemplo XRY BruteStorm (laboratório pequeno)



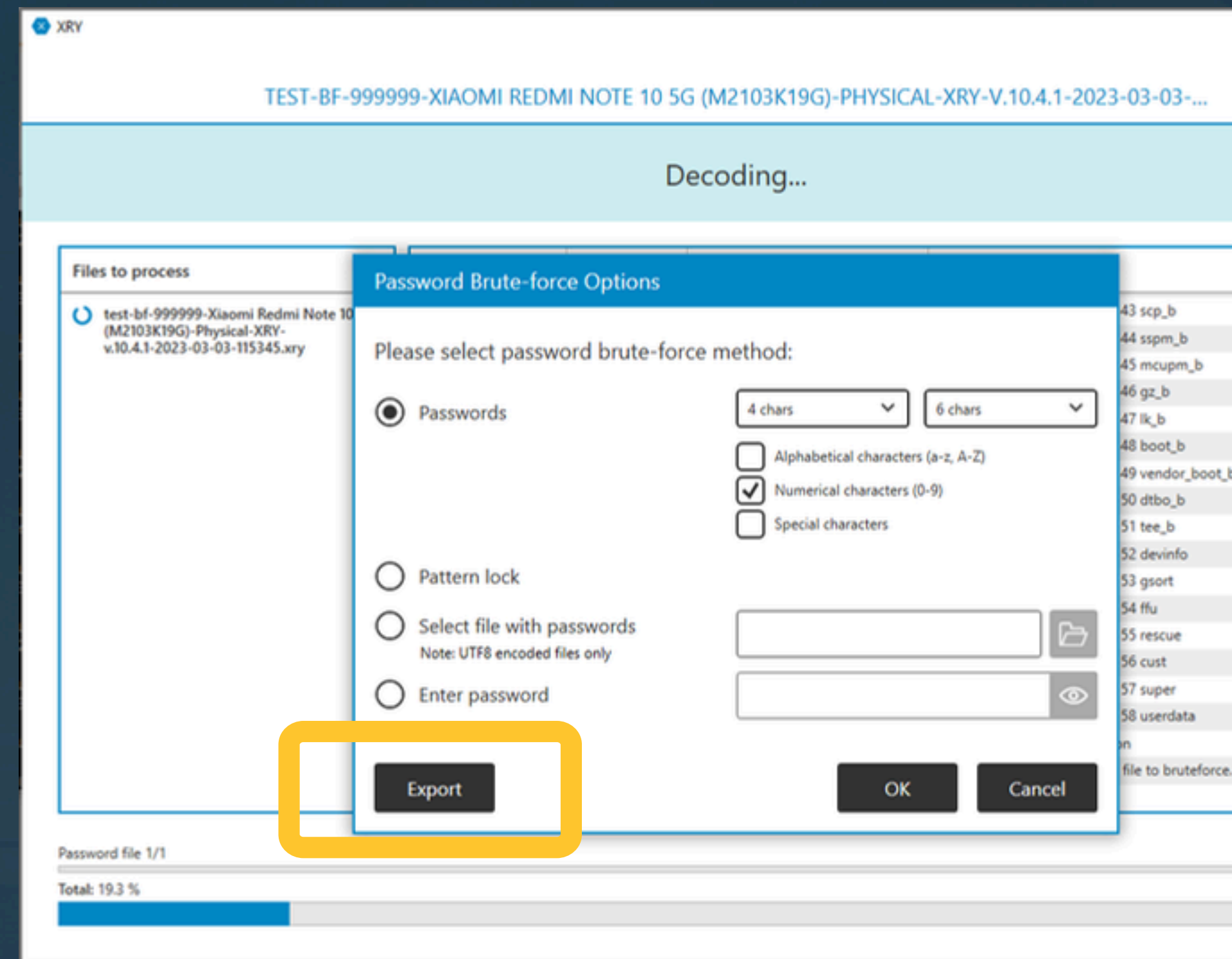
- Uma tarefa BF com PIN de 4 a 6 dígitos leva **22 minutos em um único i9-10885H**
- Mesma tarefa via XRY Brute Storm em 3 PCs em rede:
 - i9-10885H (8 núcleos/16 turbos)
 - +
 - i9-10885H (8 núcleos/16 turbos)
 - i9-10885H (8 núcleos/16 turbos)



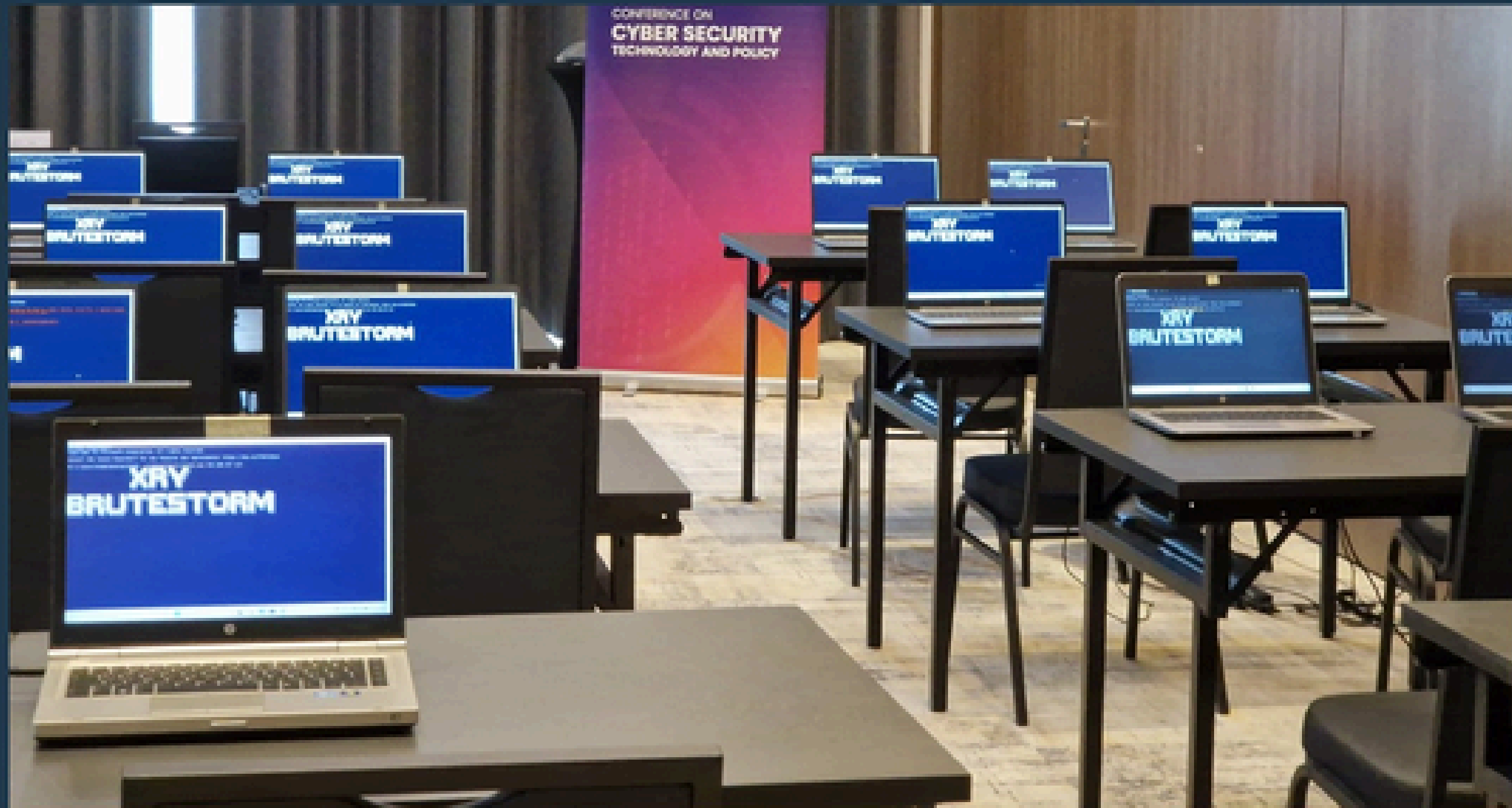
De 22 minutos >>> 8 minutos

Como funciona?

- O método de extração XRY suportado exporta um arquivo de texto especial necessário para executar um ataque de força bruta no código de bloqueio do dispositivo
- Android MediaTek
- Kirin
- Qualcomm
- Unisoc
- Exynos
- ...
- Carregamos este arquivo de texto no servidor XRY BruteStorm (iniciamos a tarefa de força bruta) e definimos uma máscara específica para o ataque de força bruta
- Execute clientes apontando para o endereço IP do servidor BF (computadores com o cliente XRY Brutestorm na mesma rede)
- FEITO!



XRY BruteStorm executado em 20 laptops (Workshop MSAB)

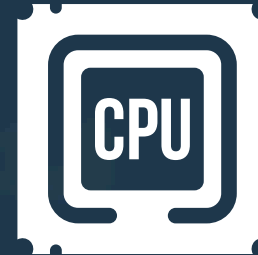


XRY

Precisa resolver isso ainda mais rápido? Apresentamos:
XRY BruteStorm Surge

Exemplo: um dispositivo Flagship FBE Standard (somente CPU) XRY Brute-Force

➤ 2025-09-10, XRY Pro 11.1.1



➤ Intel(R) Core(TM) i9-10885H

➤ Velocidade do BF: ~ 950 senhas/segundo

➤ Protegido por PIN (PIN de 6 dígitos)



➤ Encontrado em 2 minutos e 37 segundos

➤ Suporte para XRY BruteStorm e BruteStorm Surge

2025-09-10 18:32:33 UTC+02:00	Bruteforce options: Numeric pin code, Length 4 to 8
ts) Time Elapsed: 00:00:39 Time Remaining: 1 day, 07:29:25 Speed: 983 passwords/s Testing: 28249	

Success	2025-09-10 18:33:59 UTC+02:00	Bruteforce options: Complex password (Numerical), Length 6
Success	2025-09-10 18:36:36 UTC+02:00	Bruteforcing succeeded
Success	2025-09-10 18:36:36 UTC+02:00	Found password 123321 for user 0
Success	2025-09-10 18:36:36 UTC+02:00	Attempting to unlock user 0 with password 123321
Success	2025-09-10 18:36:39 UTC+02:00	User 0 unlocked
Success	2025-09-10 18:36:39 UTC+02:00	Waiting for initialization of user...

Exemplo: um dispositivo Flagship FBE

XRY BruteStorm Surge

- Mesma tarefa com XRY BruteStorm Surge



- Intel(R) Core(TM) i9-10885H + nVidia Quadro T2000 (similar à GTX1650 Ti)

- BF speed: ~ 4300 Passcodes/second

- Protegido por PIN (PIN de 6 dígitos)



- Encontrado em 40 segundos

XRY BruteStorm Surge

- Força bruta acelerada por GPU
- Solução local
 - Disponível como complemento separado para a licença XRY Pro
- Velocidade típica de BF para diferentes GPUs testadas (em dispositivos FBE):
 - 1x nVidia RTX3090: ~ 20.000 pwd/seg
 - 1x nVidia RTX4090: ~ 50.000 pwd/seg
 - 1x nVidia RTX5090: ~ 100.000 pwd/seg
- Em alguns dispositivos FDE, é possível atingir 1.000.000 de gravações por segundo na RTX5090

BruteStorm e BruteStorm Surge

	BruteStorm	BruteStorm Surge
Vinculado ao dispositivo	Não	Não
Funciona em CPU/GPU	CPU apenas	CPU + GPU
Escala	Agregação de múltiplos PCs	Aceleração multi-GPU; (atualmente em um único PC)
Licenciamento	Incluído no XRY Pro	Complemento à licença XRY Pro

XRY Pro: Despejo de RAM

➤ A extração de RAM é suportada no XRY Office e (mais) no XRY Pro

➤ A disponibilidade depende do método de extração

➤ Pode ser analisada no XAMN Pro / visualizador HEX como uma imagem binária normal (cartão microSD)... (a pílula azul)

➤ Bem, quase normal

➤ **XRY RAMalyzer** é a ferramenta XRY Pro que oferece análise detalhada de despejos de RAM

```
0006385744A46347F22A09E92A32E1170282433130878CD4092130A0990283E4A667758D326F2E83432F8F25264E8395F22889C608FD336E10E71E7452C73538E70054F5AB38A90C939E8
F405E354022773A2C290CE246C0E7700A087B0687502090E57F3A938373400F10F68A8E16A07C3981A18D24C337823A64E77708E5169A6789C3DA8E827F21F38E327D7D7E8E16416A0F6
0E7D1D2C08A4090A70057297A6EDC21808C2A277A4A609E45678E4A4CAE72F180876A2722A5608AC4C0257E7E45702A04EC322307295024F6A25F8E7D85F4E8A04A7315008F8FC5
58C28803330074FEEC980A1274FCA3D404E7988520C7706605A19F58F3176C148631157CE52E5AC12A4AC5158020A0090E148C4BC4E28E854F6959A4F9C92AA7A5A00F7E8F7D
5264454005254788E7C9086707AC368FC8E9C8C4A0B529513067000015088CA0C1A761E1F60D1835580094E74A0A03A002830657940CE540C3CCA00D7A688888F328F5802809
208F388C569C2A0C397915F0C8E110F5E5A41CC90B93C9A98FEFC9C880C738022A1E6C870837A53075053483483303088C0A0299337E43980D7A98F831097273A747E9396CE555A
632350A5080A206E034F9F6A180A83D243438CA0D245A3190883DC36A27A8F8E3C43188FCF3A787823F073E607CA0A0A1E171340383484720556574574D4162C00A43889C1CF819C3081E48
A3F5E7A63E5874E366C0D389C85EC69C2F06F04F9E3A5A1253576CA02B60D20C18E1E97581288A28EAD0576D73823C3CAE23004CF97039A0821166850A3E957AC7AC6C090610450
99A018095EAD0121AA008161E1BC3A8D18AF26242AA3D581231310A1F064F0D3D776093570C1044E1A88F48328F842C1E84E4E7829B9A81310D47886143E3D0A0C254889E642872C7C6
337687238E1237E8A674E0F4A1503CA15230077A3140726A681239A39902C008A0F0C0AC470A4870028A3189F3C1318F93C40E4A8F4F8913148891A1E8A79D10C3F7166231
CF8E261C44971C3F3388E81145CC38A6570D86C909F910F1A055C7C87082176A29FED0C4E027C62848050F834FE4852E0000C788133688B11AC6F4713C8A8A620A0A19F31C4F37AC707A
88FDECB81A93A58ED08E751A25E5815F875682F8F880A3C5806F98291B2D952A10188FDD2A206A8BDE66F9CB09C5007E7E60C70A6782A080818869647A3A34794712523825F4E8B885
9088CDD109A088E89C826F4F9823E38072BC1F81864269A53333734CC00A14118AC4F22142A9A985550076654F42A1E6348E337D8A482238F888899A6435D0767E3E8A219F1F06
707D358AC6C9308C10273C656F8890A8E08120A482215003F7743F4004E18F8C6A513CE7729A45AC45532CF44E388091325124F83A453A0727031220816308388
7944520EAAFE590FAD09759986E8F4343C107A08CE26A81A5796C801C4377CB855243C30F89E1A3A4A42208E8077AED8E2A2F2A8FCD871AF8A2D509E6134770072EE6250A8089
608F60AAE3D690D5EE1CC613D10A5ED01927573067CA4E98D16A8C8DF93D255A32A7E1A697D25A8B5F87CD35F388E38816E8548EE697C3E46CA08359CA28E2EE1E018EAA0BC083A
90F4C11E2A879A3637A9A947A90843700A0A47A708EB8EAE072ED073E61E5B7483D7483EAE43A14F8A54200C33A06E4E3952941823CC18831148327B8A51E38821503A502
9E0B3D780992556330A7A08E376C877A8D9331D031A0CA588A03DCE4888CA500E2F8E4624F3D78A0021538C30A8E4391B3A5A38A81728E3551E878805E358F850EC1A2A1D18
A37FA6522EE48457AC8A089A8E826735E2A2267C7BAA831AC68F1580008385516A8387995FACAC66A2222566630F6CD3997A373C35557411662A80F7A17902426C695F7A4D309998
783FF68B3CC0DEE290828944F92F781FF6F1A238806A92453715518878FE9A08E978D38C3DAA6473731106300092734898976AC595227F483849E939A3E7A8A6027821D84C16E37
70278888A062800A4F5C027283A0D7E5A8C4C380523DC8AA54EEF295E355A00CA2E027F66A3381A11F509CE69A4E31306E0817E756D4598F809300A0A0090FAD3678F61
C758EC3F0E530A854FC7A0878C800A558081D02AC3A3F90A90C8B18E4A2310C5CA0618AA2E08E7C5FE7E30A83E16253651A26795AC672CB7A0A08C49A527E88E69FCAB025E59
9C7E4C0A336280F8367113E8655F709F7099C64A2A0C85701A817E69ED72F311F001137F6E1E18C98554D2006F8FC5E1553C8FC9670934064208A05068080FCSF47357A1CB038A450
CD073802808C92A0691C780007E4A9DC13A88318888A84E2245982FC03838F320FCEB48FF92A778C80D32A83EDC460CCAD9337085660971758D4A4009876C030A45CC77880C34
98867EFCB3159C40D20A0A8A70C8809ACCA40005F321E3A873FF7E447F3AC48A12CC8A8C80978DC353728059630C3D0A9F502B38A8C8A350CC708CA4
1A8AC24F8501DC88F8A8A753187C2A38F3382978F708E13289C0436F8C459E39F05FE742386A3AD1E6A636A38778379081305571388262A6573D17C788F520796A0252A3A01
8C075EE38E3C84790855A6A602784D70C13870C7CD6A2626E1E11202C25374C5E4F8F720C6281FD68B4AEBEFC48454FE894CE189FE6AAC8C5787C640879C10815794EEFB8FE4D3
4D1A8FF808CA7A2D7761F3F510A95C4C3D3C8239F4A5D03448A3E3A5F40C2266723135484EEA020A5A528B52A57C30F6A8903501938978F878548C36A04908D9A5A2A1C1C9
A8D308C307A6A6808023A0E8A4C8C6F9FC4EC8E8236A7371418A46A5A3A3E2740B27300280526A597D83287716A1574753F888A63CA78310005106CAAC39038F8B
C1F1164F700C76244682978A36229A36D78C3E35A1A16CC731AC1F8F69598A8388A52054E2D4F8A43F5A1FC05726583A21848DE4F1725292259A6156A8212380026332ED
38EF36D88CA13214E6A8A183F498E2D448D337E425D42CC915F8A6A05323799A3F9D663C8A008E4A51A8A339302568CCCA8188A2E84476A16527812D6D7833646F54EC3008815D
088233AF80861A012A2376E5E1342E8E89FC0AF8A4A4A004C27CECF3E40E48A7E6CC05F0072A1E9E8E4A88093F33B145170395F88330815A0C40002003180A232809394
58805018D24A02187F369FAD85F895210F5F0A550559F148085D2CE82BAE33C54DC584F2C8E78D343C403E88599AA431E583E8168E7F863EE6A4E8F8C3088164C
20030335883EC38F7461A2182740396157807A2A2155916A4459C47C3E2CA37A2978991D89E7389785C156FE4307A18888F86570FCD3FC8E88D781247807FAD79A8A0888A18005C
AF853E87D58250130A6A088C6F857E7615A05078F7F4121E37CD483EAD8A009483472A484EF7F26A6A1D8678782414576A89CA2A494009F96CAB2811925A01D0A9A62A827700C037
83E2A085F99C30A585F81E70FAS1158C18F08A8E3C0A1738820816A21608A8F433EC600799528A238A9C7008733A126C05184F0E28E3E1588865C388F876015D0A2AAS2F
DE8A78B185E868A38F6208D005CE8B39559FC08970A17FB9000087187299F90160741A8365E401C0E1C3A43CC0EAE6A1D0A7C87A8A783E518C5F647809CE889A79C4F08181008E53
C5D2731291550258FECEFB588B45D38BC6085C8E31F6D58E55509F7660A712CA8C7EE55CA28791636858437EAC873558F835570531049F4D615
F08885F014F841E8F2109180A18D2A2E186E7FD38983383C370002A586073C87EECA3A4E809482C1A5A28782E736A0CEC7E2A8A023236F49E08E3E18AAE275C39C089173308
ED4F83A033E586A57A315F8A8E1A8A70914309EC3B3287E35CD972A8F8E991C8E23A31F8A007308518855E88F8FEAC3A88A88A8A08C08073E6681CC00A88793955A4
FAC8A0C7C165E49018E80062F63A07088CEFE1CF775770A8EC03E329E4D42368948CB66740625A7808E3A0C2AEAF1F950A04F4F3E7A3272A5EAC29C559E110838CD6A18676087032
D8582C956154CFE052D0A55918CEFFD5F48C6818CE97CE868A4E7A00A37AC8CB52ED488631E5D67F8093C28E86A9F6A6A4A12F879681BC8EAA6A091CEAE8A33EF017562E031668
47AFCD89779788F8972F5994E24A3A98544DC27332E45A3A05D07E8444A236C0A61B15E218E22E106C006768E7F798CA51081062E83A48A01E8A09A33738823979631733
52510A285A9CECECA8E18F5480E7A05E54A838207E30802F54E620A355E488F4F72192BEE485F0F399A35CE8A69E548484DC3582AC8C795C28F42F8
8935E56808764FABA5885DA0A808D0163471CD858A85A21D9635D2003909112F5AED1A8710A2A2737D5880790378215A46CAE11A01802D06C47498959736A3ED3A53C6FF6A0C595CA
DC66882C9CF839358D58D00A1EACAC38C18742938008E8E0D3146406A1AC969C915A1A7A188995FC9A8206FC18ED0C3A2458ED9D722B061A08A8A9791F88A4C3A4E383897564F02
92EFC8E88A72578E8AC1FA769238E8805157688C4846C154E5A8E0F96A06A0925166ED8A8A028A8A1E7C7E37E8C9770C467A208F1E3204C98D708A88E200A
708F8433A8976C880770AC7767646FC96C8639E29E07F8400A01251CA3384484D731E17A3D21C8E20373A8E4CEDE0A017A80728032515A98A5A4E1FE75257E177338184FE43A6A9
805D00818A658FF520FC27428796398550F5F1FEA271E568F193735A005C395F84725024F40813688E39E03898AF77A45755282125A8A94802F2AE3ACCBAB8A0A9A8AAC99929006
3A36476E727EAE8DE2A1E78D00870145E081D4E0E49F49559368F1C68680A48CAAB8A4C300079E13F7D38C182A8AEEF98CEDC177A88973619C1C561E7A4A5007388F7C9E0200E03A357D38
3AC78E72D30A0CC010A09A8A03F413A7392ACAAE4A5227C8E38F8AC4A8F9F322035C8728C03B35F8E95A0A12439F5A8A0818E7E04F0FC83868F80E28FEDF1A7888
89C7ED38D39327A0C2C85E1868A84CF78C21809327688639387F36657073C6AC4FA33613CF5E1BA0A10464082438A17A0E915ED05A54E150830F487C5C6CC95D8A8F73A68010A0808
F220790C3EF5879A54E7ED47448AD6DA14D22384E5271129A5999C1331CC80933F5890861C77735CF8F4162845FC2923288A707030A07D06641F5151FF19E6071B198F4E4A76954792041
99E3682188D0A88F90A3399A4CD047E36100A04EAF4C5980F3EFF3AED16A13A2897238A8539A5A3A6A3A4A4A4A4E1465A2A259882701A4F1227D1C4D53071A3386887A11DC706124E
42800D1588A867A7AC5A6A4ECC2895A98A9CC6A2168310E1E09389720A8E9677A60A25075387E20C4AC48C43F88891224E58A700C1C6AC8484288A5888C5A871B
CE4F9E9EAC0871C8081702805AAC18639C1AF21091AA3A06288A808585608118DA7429945A889EC588F9880753AF3F68128E1470E408771BE77A25119F5197E457F091A000880A2C
D8028DE28A989CF8F4971D1D61E5CADA0C2CD8A2D39945EE7C96E9E00A0E8FE858EC68F4E12180F2E906A8F138E33738F869E86E29267875852CC1A808FD35808F3A68277A68E5F602B3F
```


Exemplo da ferramenta de análise RAM XRY Ramalyzer

The screenshot displays the XRY Ramalyzer tool interface. On the left, a Windows PowerShell window shows the command `.\RAMalyzer.exe` being executed, which starts analyzing a memory dump. The output shows the tool found 3 tasks and listed them with their PIDs, names, and process types.

The main window shows a memory dump with columns for Address, Hex, and ASCII. A search results table is displayed on the right, showing the results of a search for the string `www.google.com/search?q=london.p`. The table includes columns for PID, Virtual address, File offset, and Strings. The search results show multiple instances of the string `www.google.com/search?q=london.p` at various memory addresses.

A "Go to address" dialog box is open, showing the address `0x00000001c158fe1d` and the option to view the data in Hexadecimal format.

PID	Virtual address	File offset	Strings
25721	0x0000007988307e10	0x00000001c158fe10	www.google
25721	0x0000007988308710	0x00000001c1590710	www.google
25721	0x0000007988308810	0x00000001c1590810	www.google
25721	0x0000007988331510	0x0000000098960510	www.google
25721	0x0000007988332210	0x00000001c5a08210	www.google
25721	0x0000007988332b90	0x00000001c5a08b90	www.google
25721	0x0000007988334710	0x00000000d8133710	www.google
25721	0x0000007988334d90	0x00000000d8133d90	www.google
25721	0x0000007989763910	0x000000002dafa5910	www.google
25721	0x00000079a3981210	0x000000016b00a210	www.google
25721	0x00000079a3981e90	0x000000016b00ae90	www.google
25721	0x0000007a48538110	0x0000000014acf110	www.google
25721	0x0000007a48538910	0x0000000014acf910	www.google
25721	0x0000007a485f5090	0x00000000cc78d090	www.google
25721	0x0000007aa4b9b955	0x00000000d4bfe955	www.google
25721	0x0000007aa505352f	0x00000000c3a4c52f	www.google.com/search?q=

XRY Pro: ...alguns requisitos:

- Treinamento necessário
 - Treinamento XRY
- Treinamento XRY Pro disponível
- Às vezes, equipamentos de laboratório adicionais podem ser necessários



O que está incluído?



Versão Office - XRY Pro (Ilimitado) (Estojo flexível):

1. XRY Pro License (12 months)
2. Licença XRY Lógica e Física (12 meses)
3. Licença XRY Cloud (12 meses)
4. Licença XAMN Pro (12 meses)
5. Licença do pacote XSMN Text Intelligence (12 meses)
6. Licença do Clonador de ID SIM (12 meses)
7. Estojo Office Soft em tecido contendo:
 - Kit de cabos XRY + 3 suportes para cabos RJ45
 - 2 cabos Pro extras (Huawei e EDL)
 - Kit de ferramentas Pro-Tech
 - Outros acessórios (Bolsa Faraday, Leitor de Cartão de Memória (protegido contra gravação), Leitor de Cartão SIM, 3 unidades de cartão SIM clonado Mini/Micro/Nano, Pen Drive USB, Escova de Limpeza)
8. Suporte e manutenção de hardware (12 meses)

XRY

Obrigado!



FORMAX



FORCYBER

MSAB