MSAB

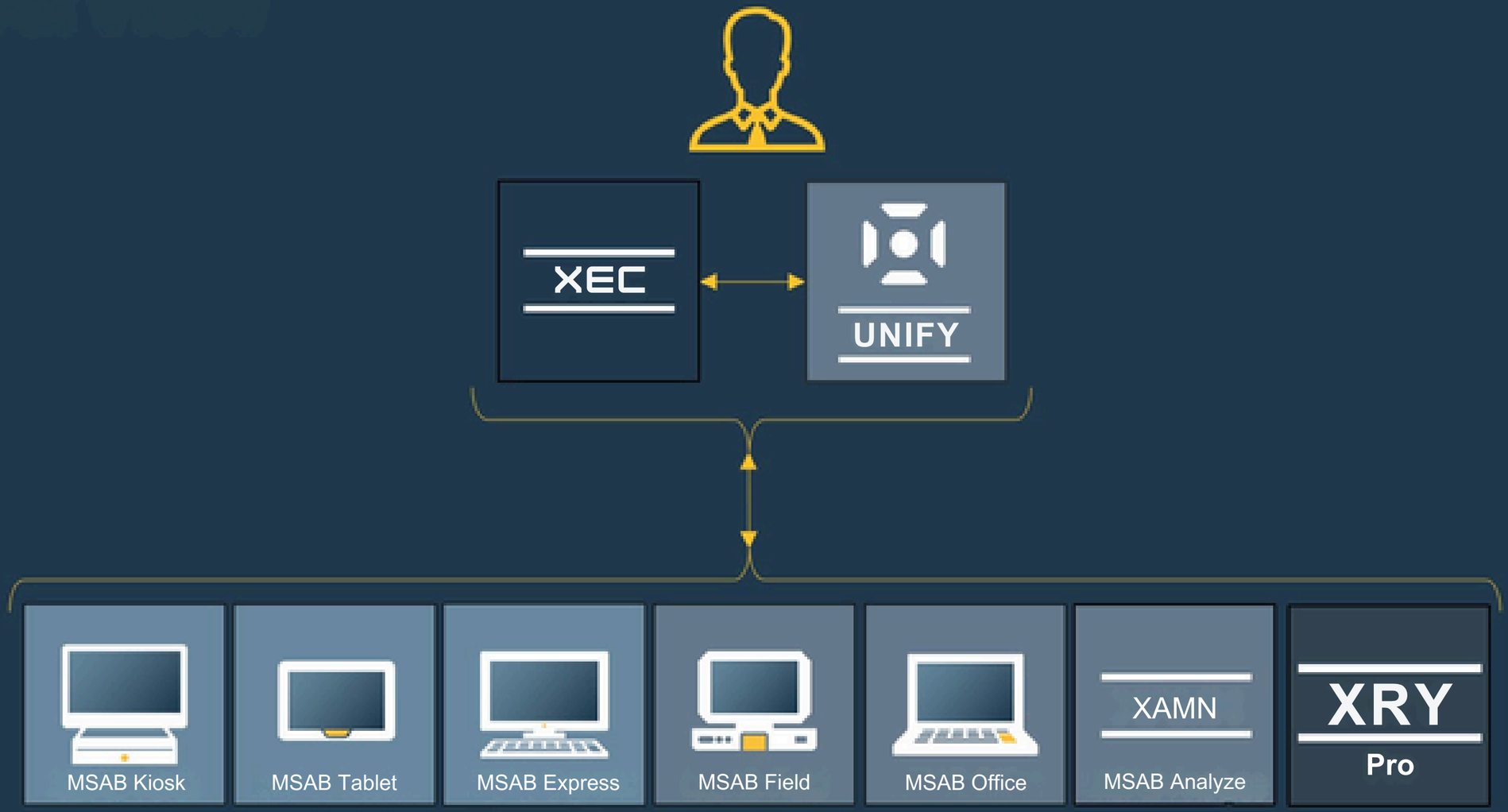
Trusted Partner in Digital Forensics

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

MSAB

Ecossistema MSAB



* Os recursos de gerenciamento variam entre as plataformas

MSAB

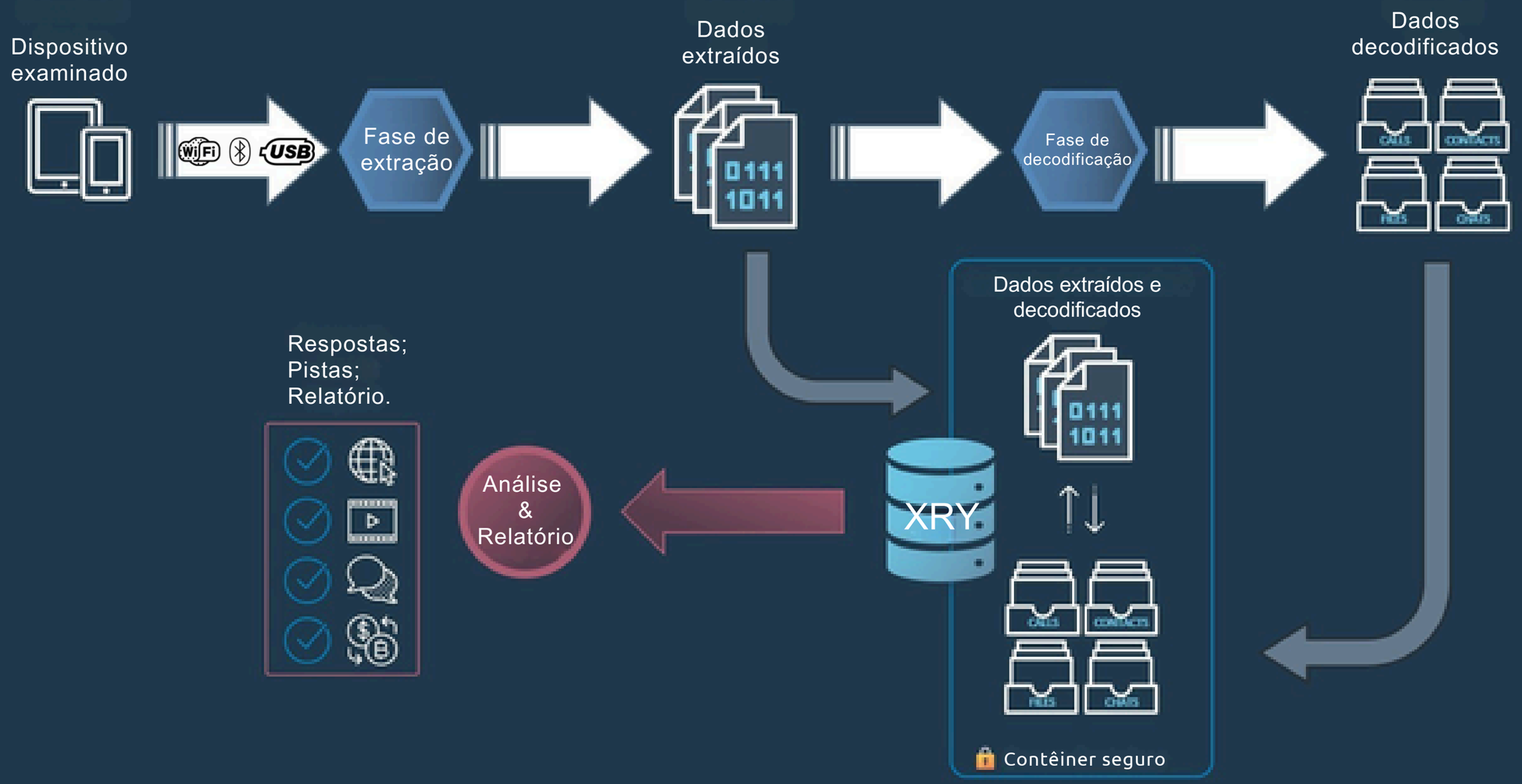
Principais soluções de software da MSAB

Extração/Decodificação

Análise/Relatório

MSAB

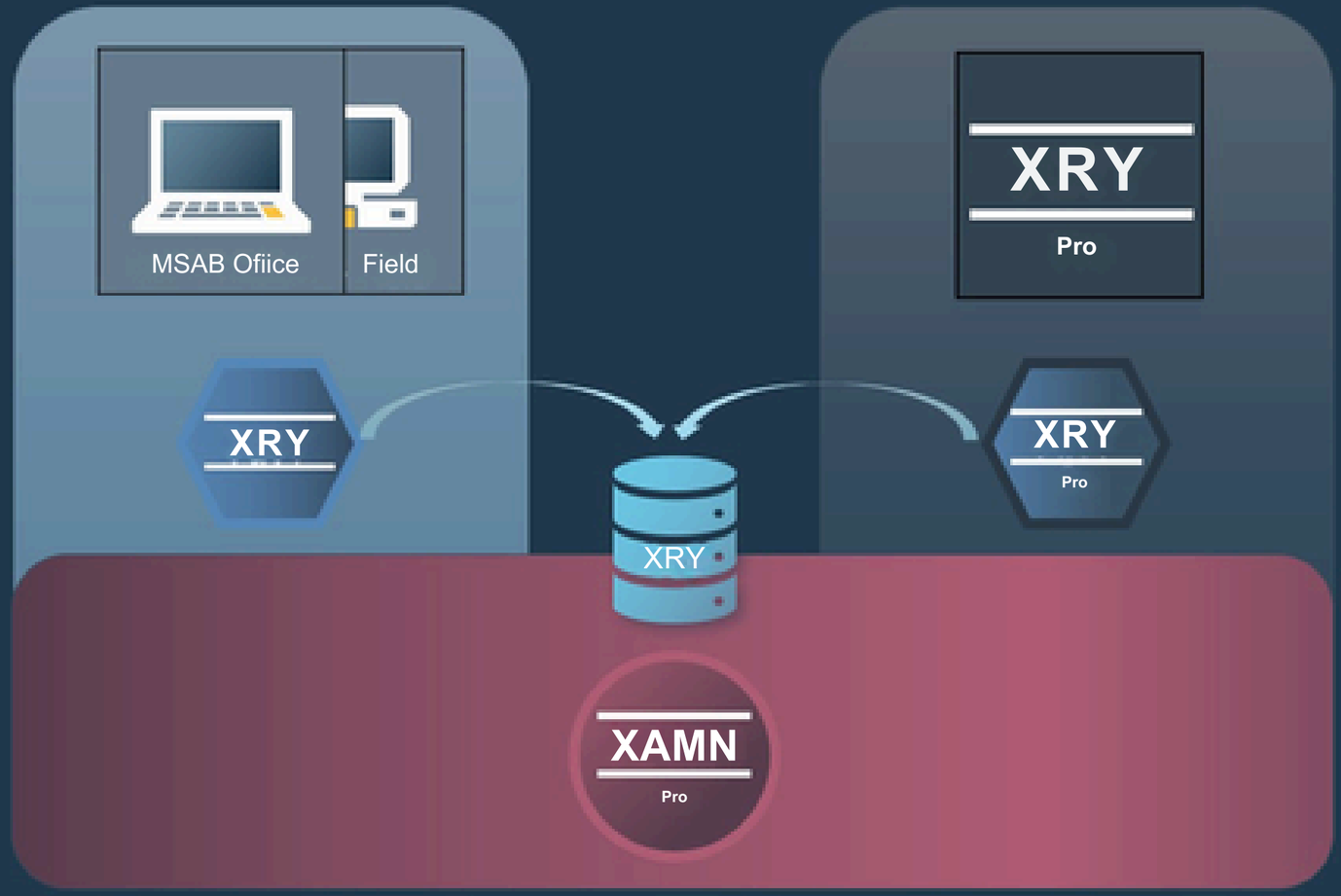
Análise Forense Móvel: Um fluxo de trabalho típico



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

Software de Extração/Decodificação

Software de análise



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

XRY

Fundação Decodificando

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

MSAB

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

MSAB

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

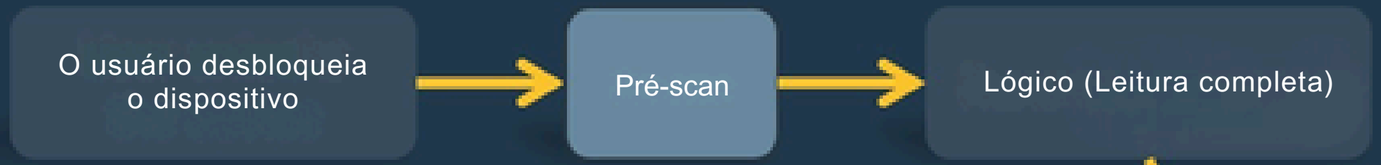
MSAB

XRY

Alguns exemplos de extração e decodificação de recursos

MSAB

iOS (Desbloqueado)
Processo de extração lógica



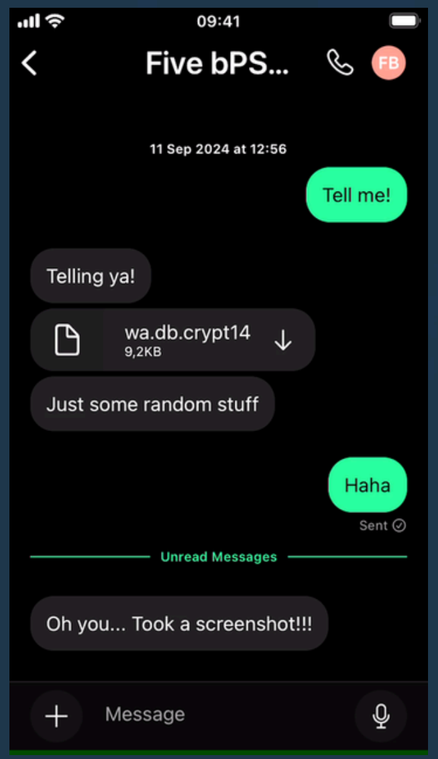
Extrações do XRY:

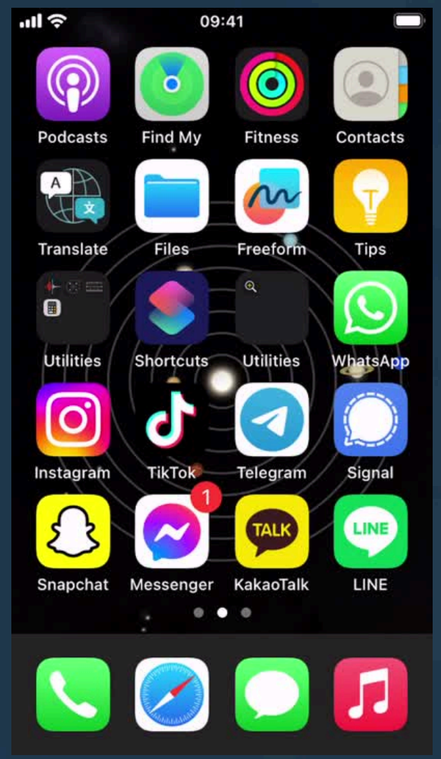
- Backup do iTunes
- Informações gerais
- Informações do sistema de arquivos
- Informações dos aplicativos instalados
- Diagnóstico do sistema
- Arquivos de mídia

MSAB

iOS (Desbloqueado)
Extração lógica \ Captura de tela e vídeo

O usuário desbloqueia o dispositivo → Pré-scan → Captura de tela



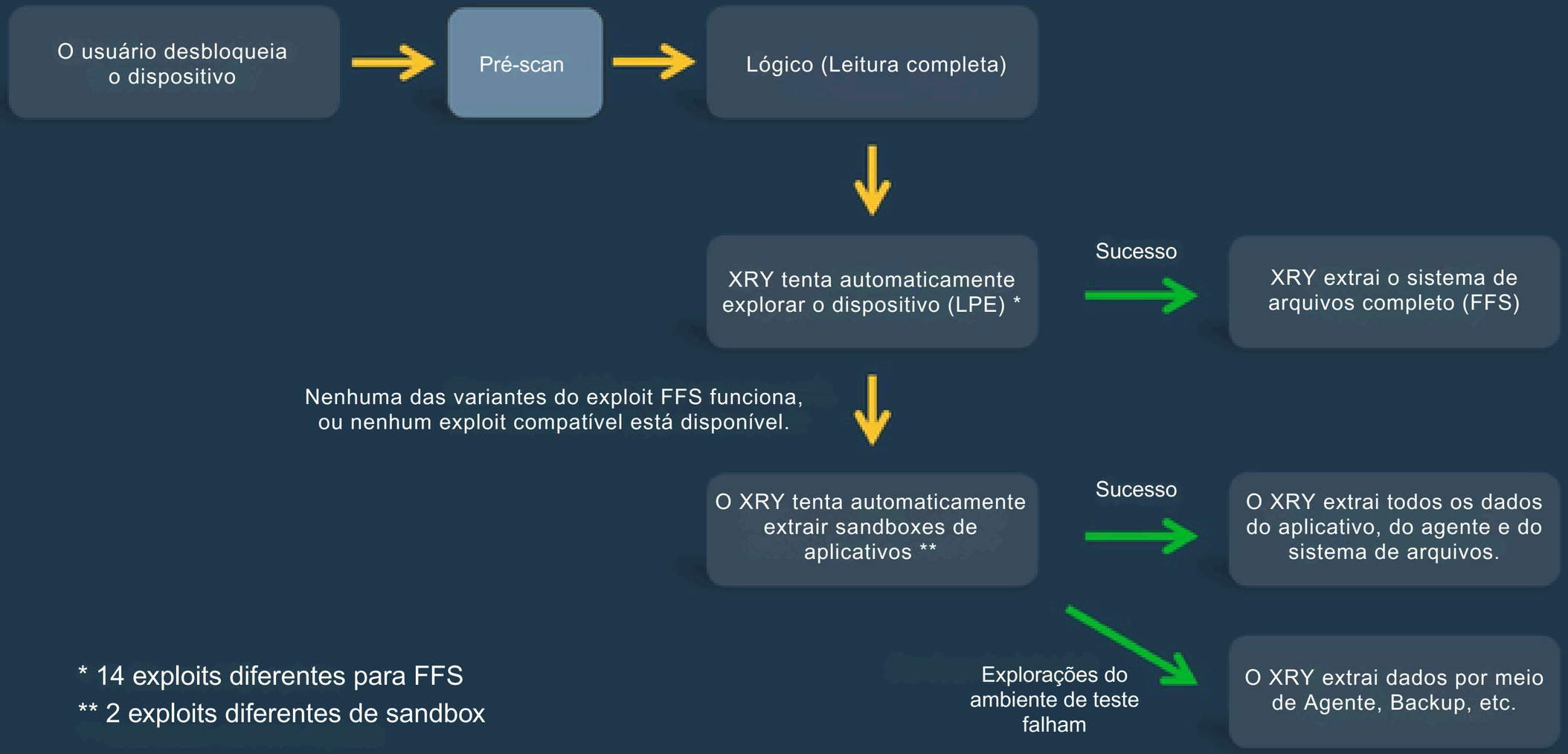


Extrações do XRY:

- Capturas de tela do iOS
- Gravação de vídeo do iOS

(sem instalação de aplicativos adicionais!)

Android (Desbloqueado)
Processo de extração lógica



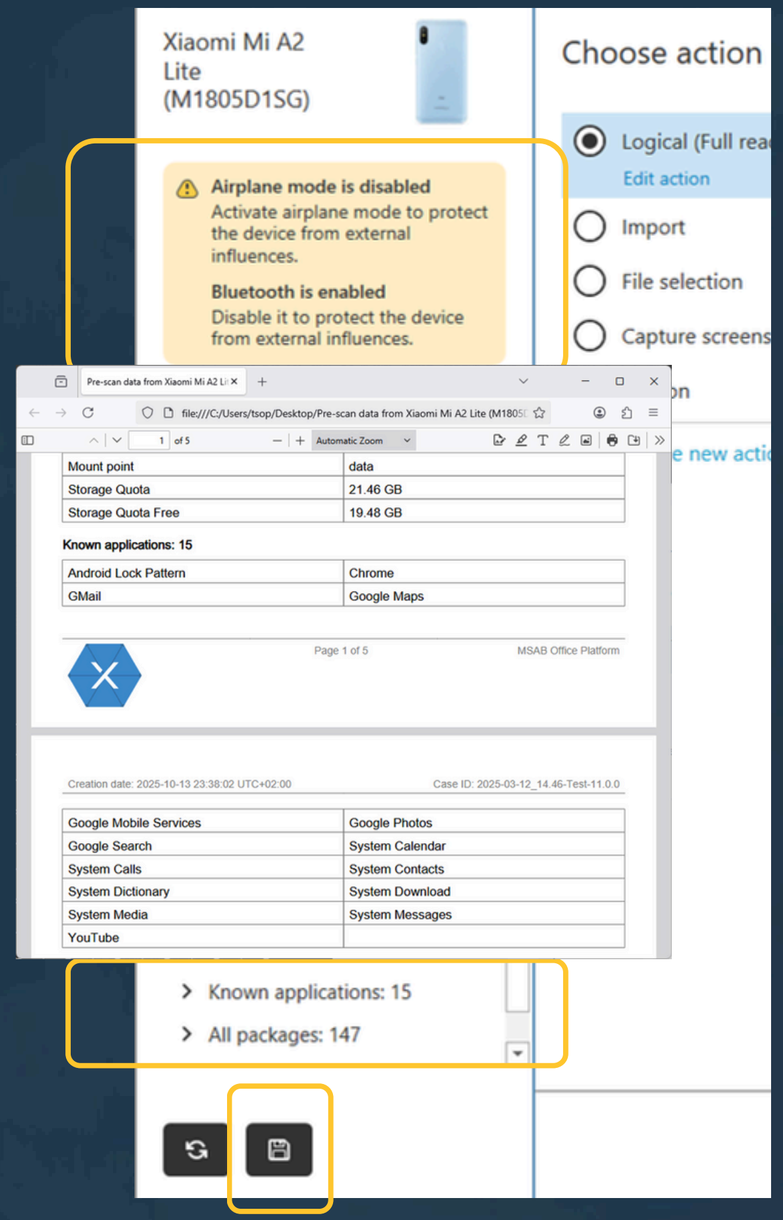
* 14 exploits diferentes para FFS

** 2 exploits diferentes de sandbox

MSAB

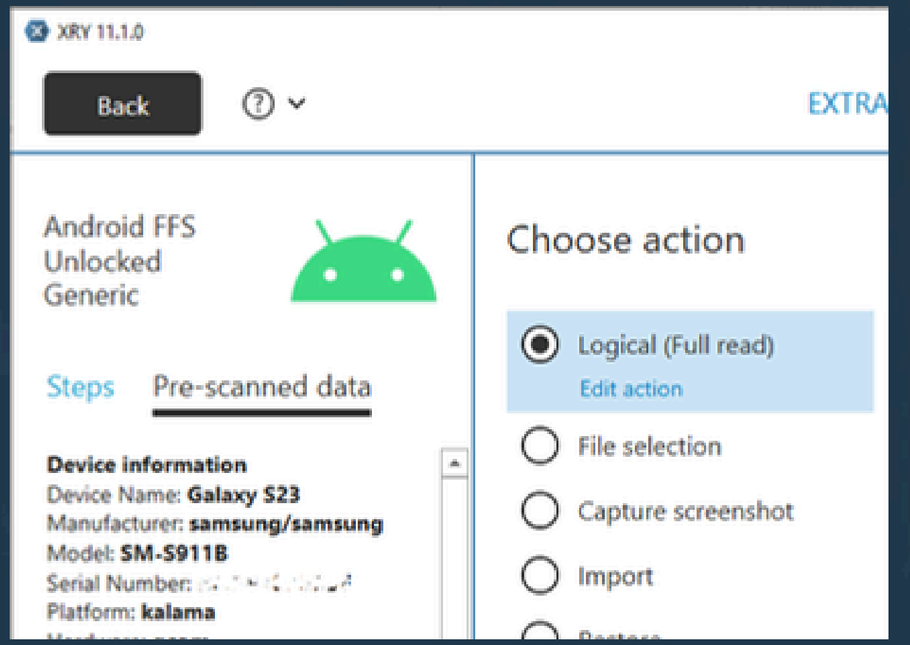
Pré-scan

- 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



XRY tenta automaticamente explorar o dispositivo (LPE) *

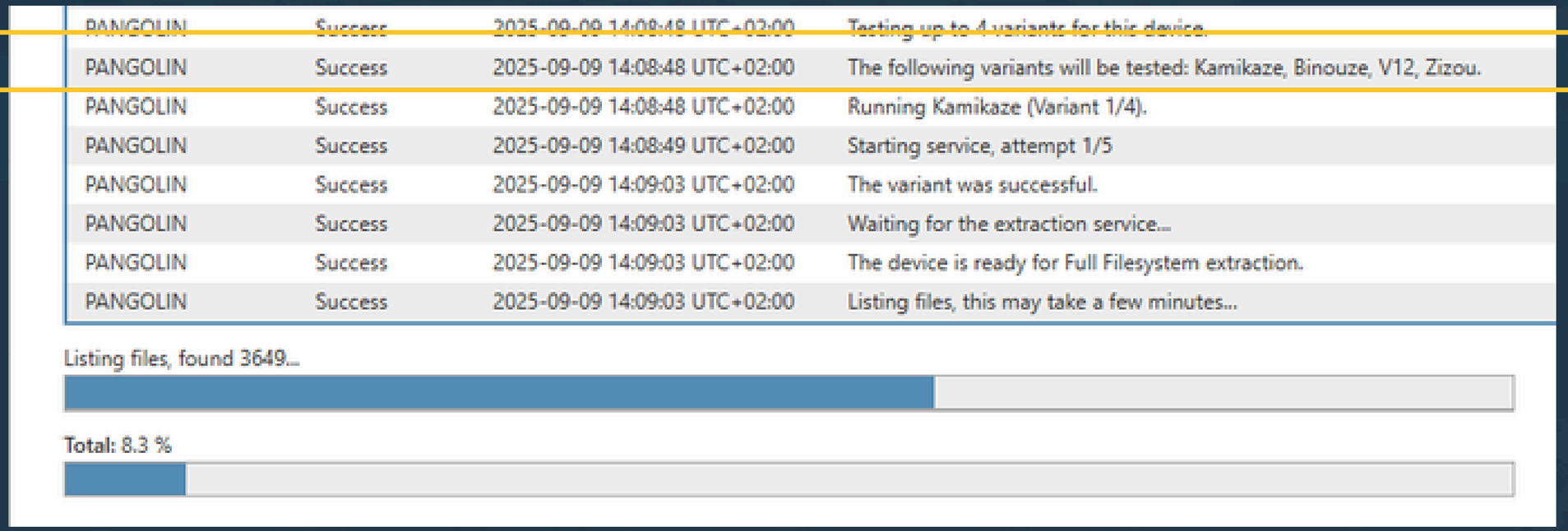
Sucesso

Extratos XRY FFS

MSAB

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...

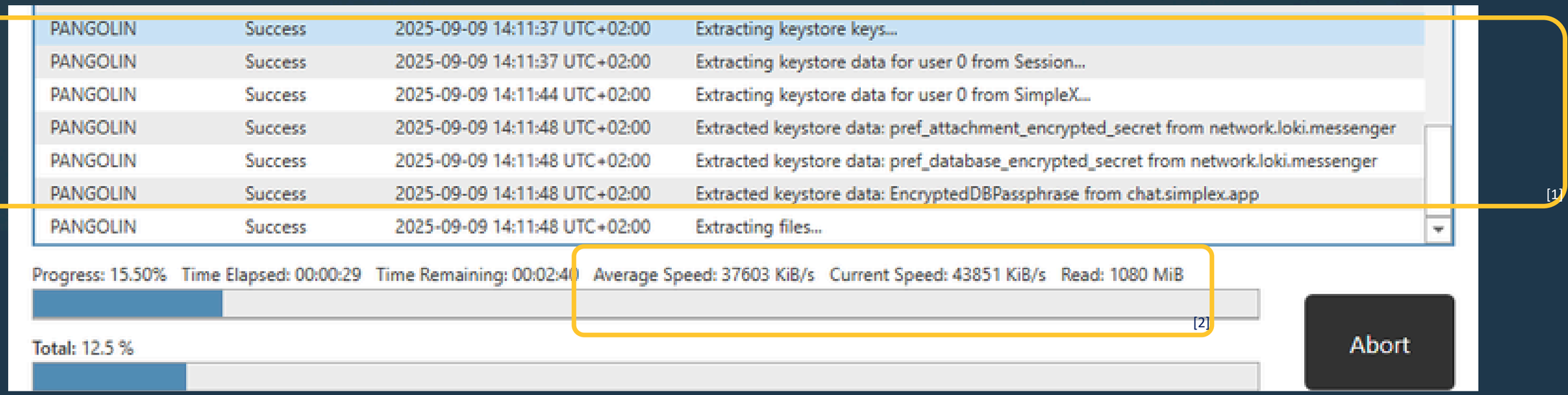
Listing files, found 3649...

Total: 8.3 %

[1]

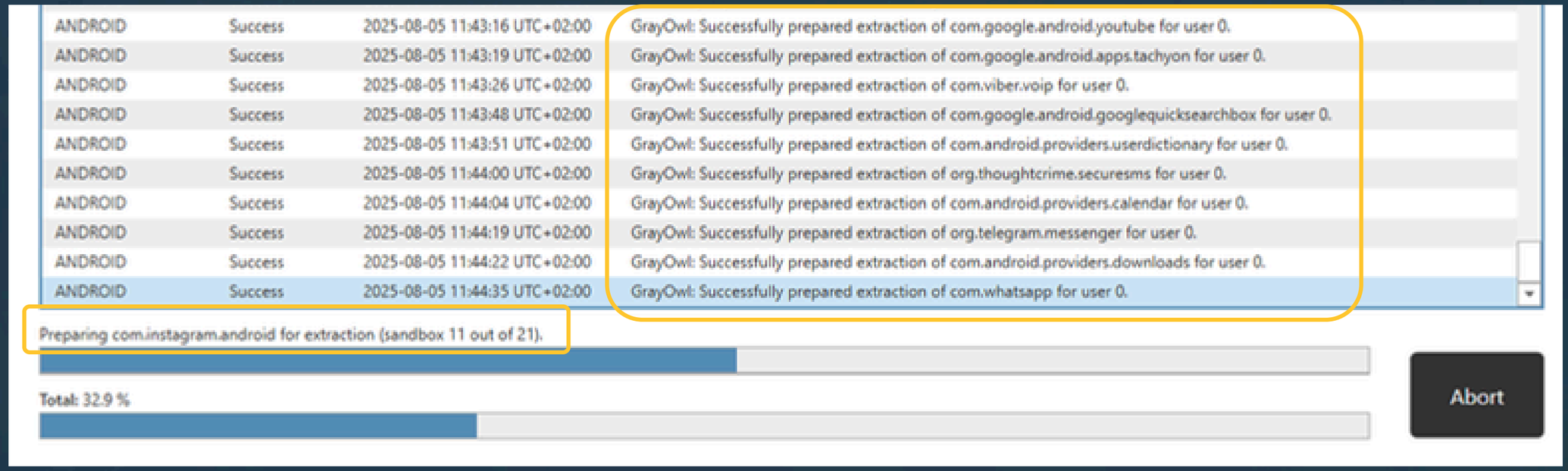
Perfil genérico desbloqueado do Android FFS

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



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



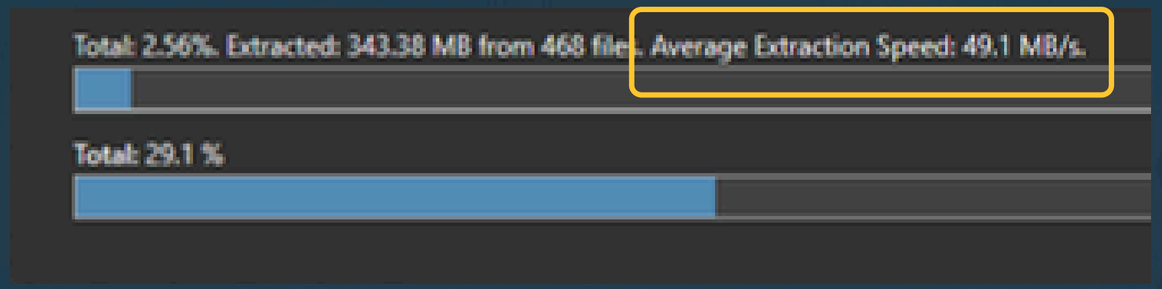
Extração lógica padrão (clássica)
Agente, backup, sistema de arquivos

- 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)

MSAB

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)

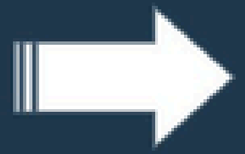
Android MediaTek Generic

MSAB

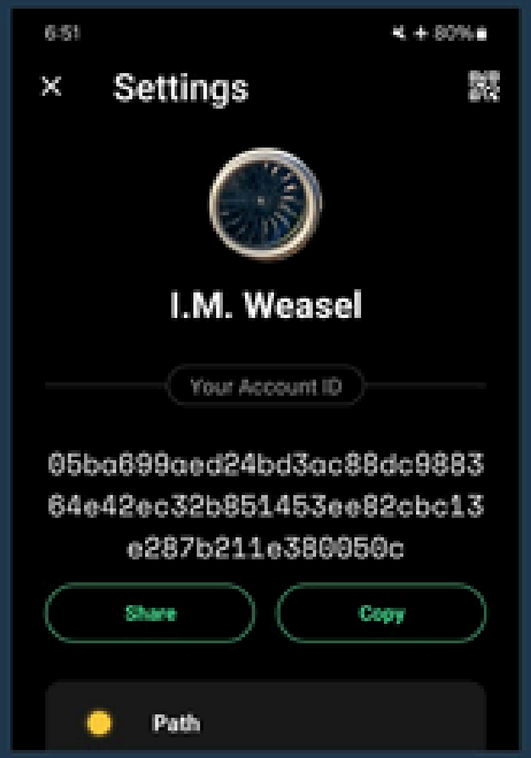
A extração por si só não basta: Decodificação de dados

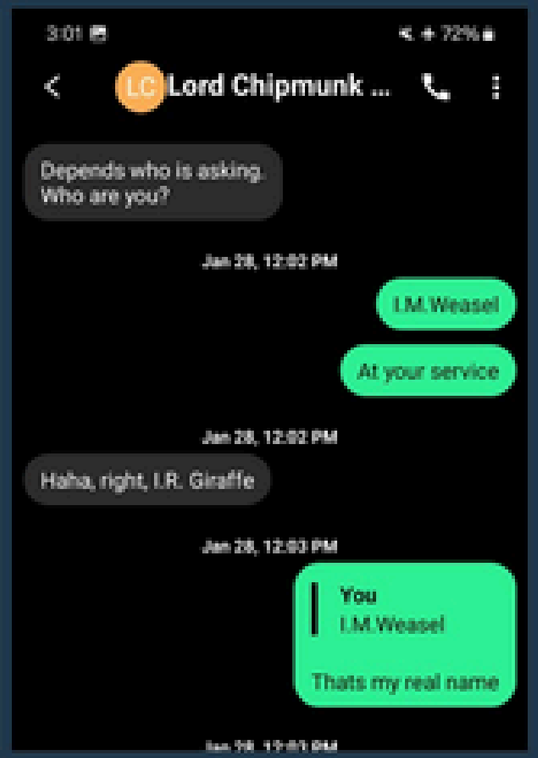
Dispositivo examinado

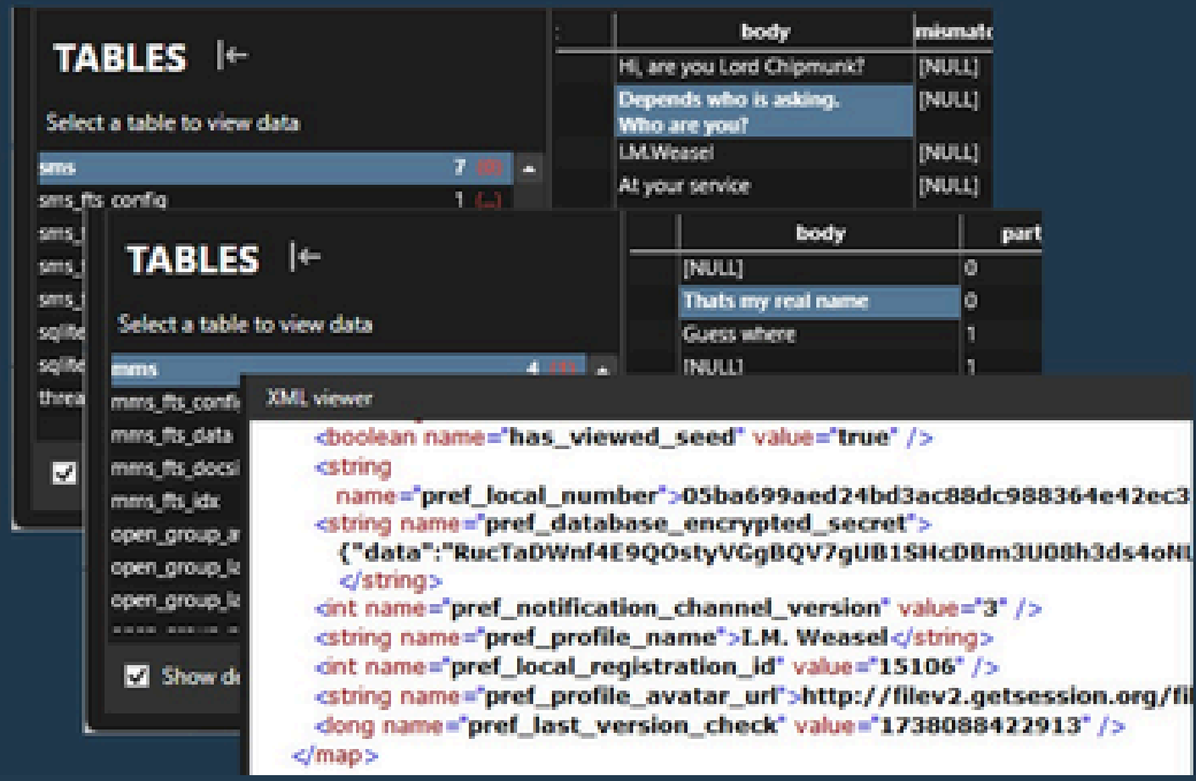
Fase de Extração



Dados extraídos





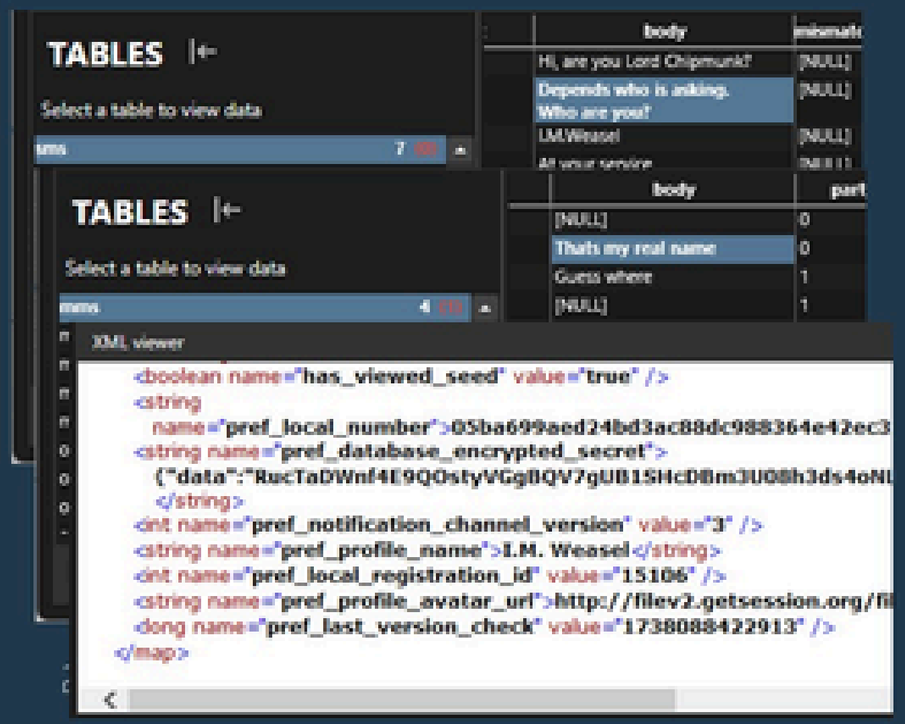


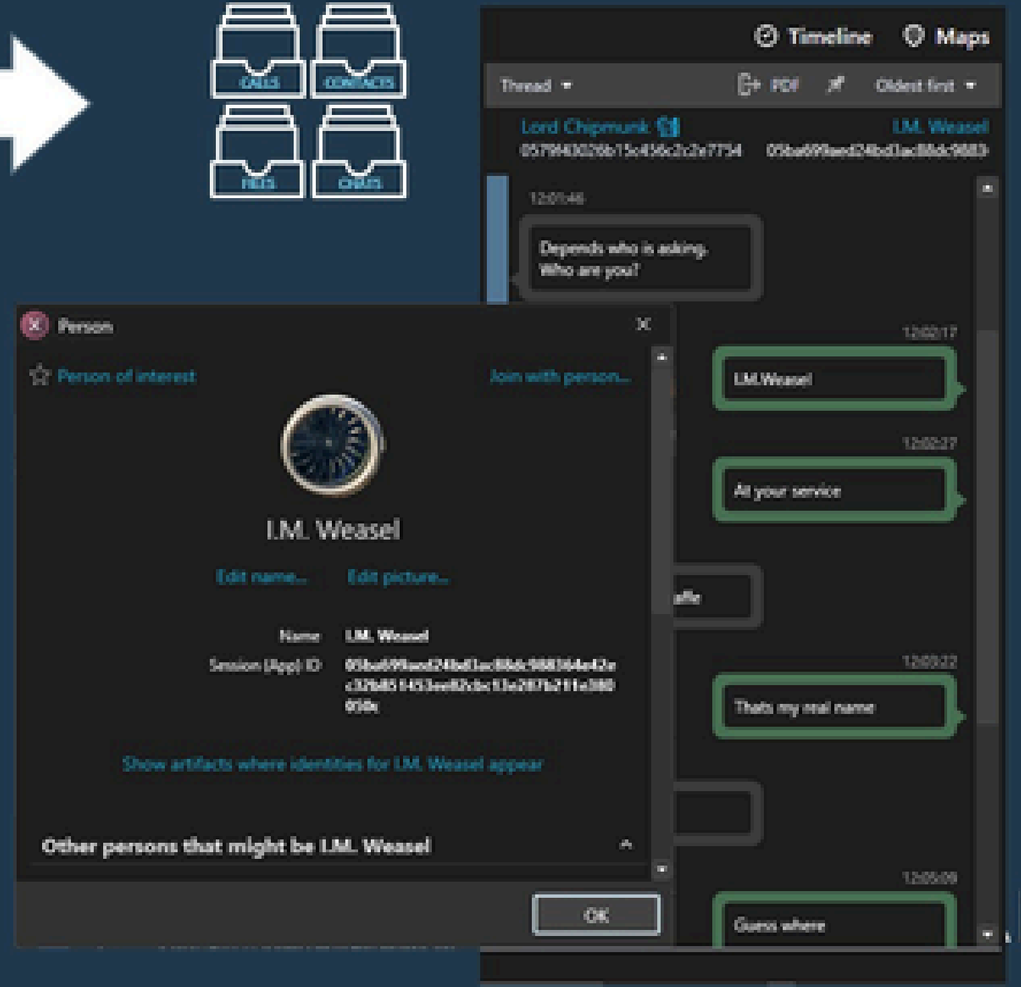
A extração por si só não basta: Decodificação de dados

Dados extraídos

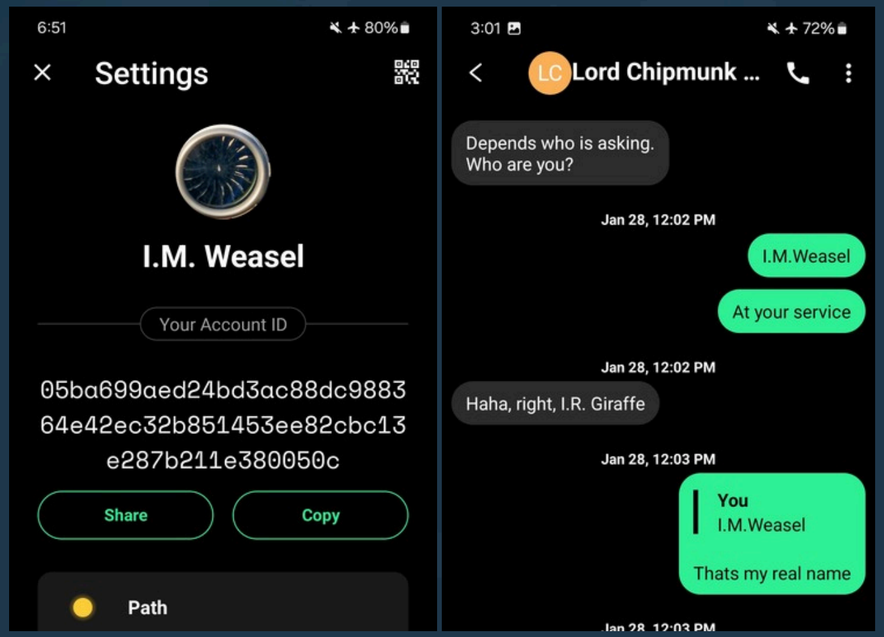
Fase de decodificação

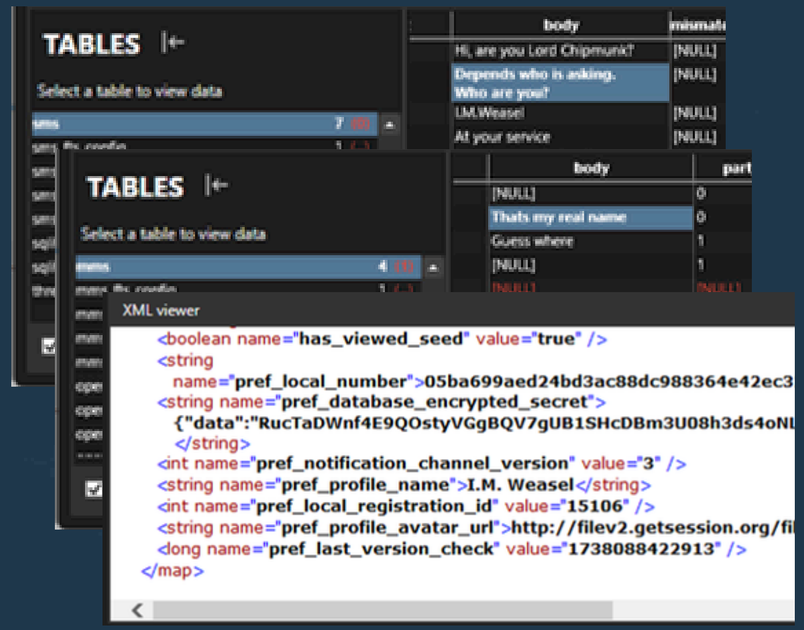
Dados decodificados

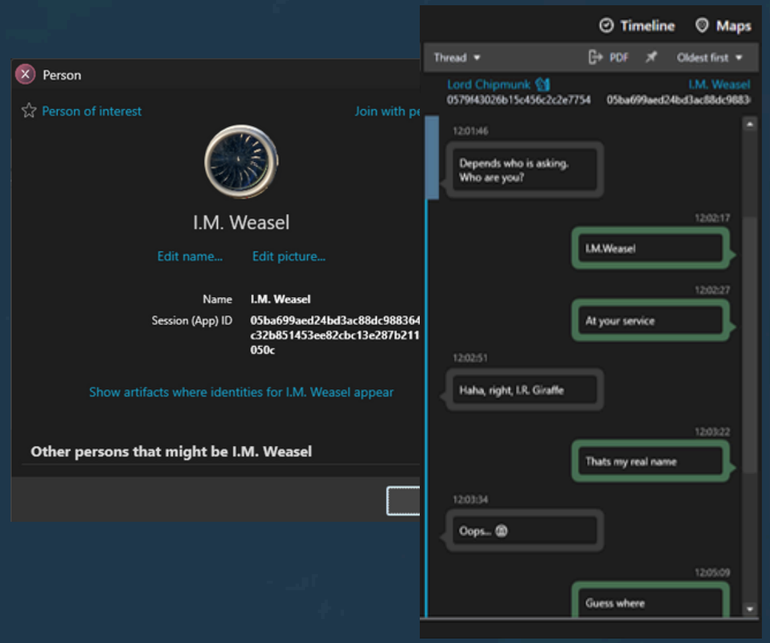




XRY: Extração e Decodificação



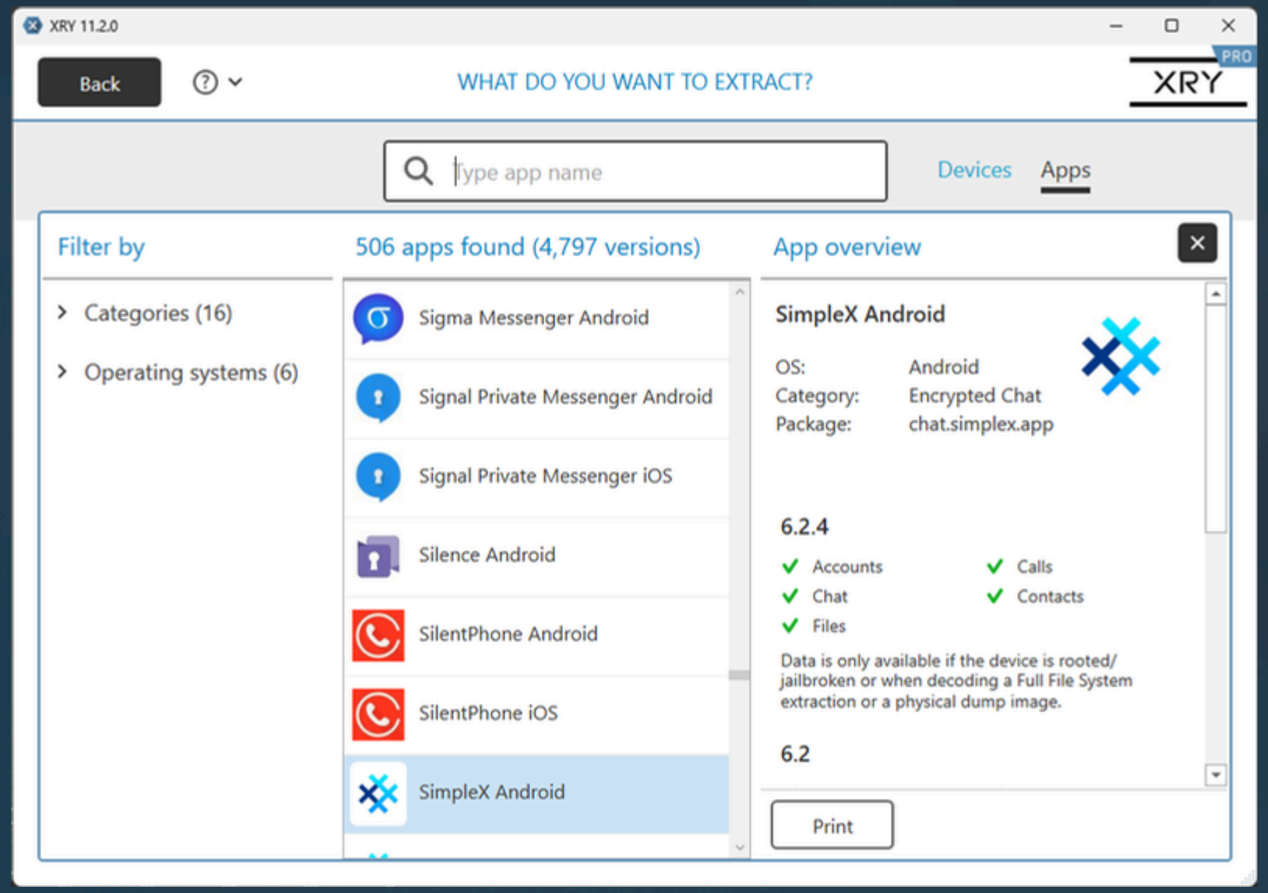




MSAB

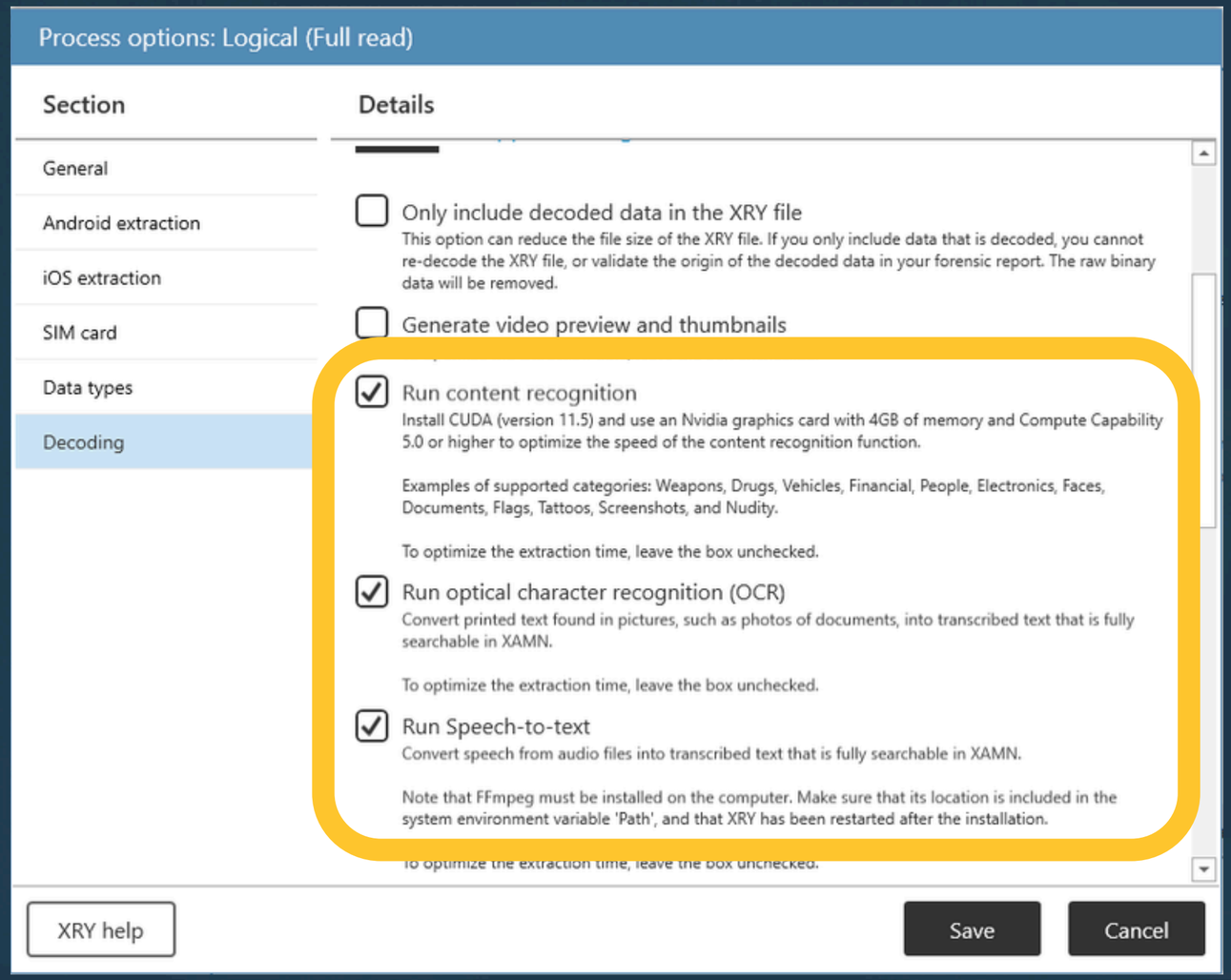
Decodificação do aplicativo XRY

- 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



MSAB

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



Alguns exemplos de recursos avançados XRY Pro

XRY Pro: Plataformas e fabricantes de dispositivos compatíveis

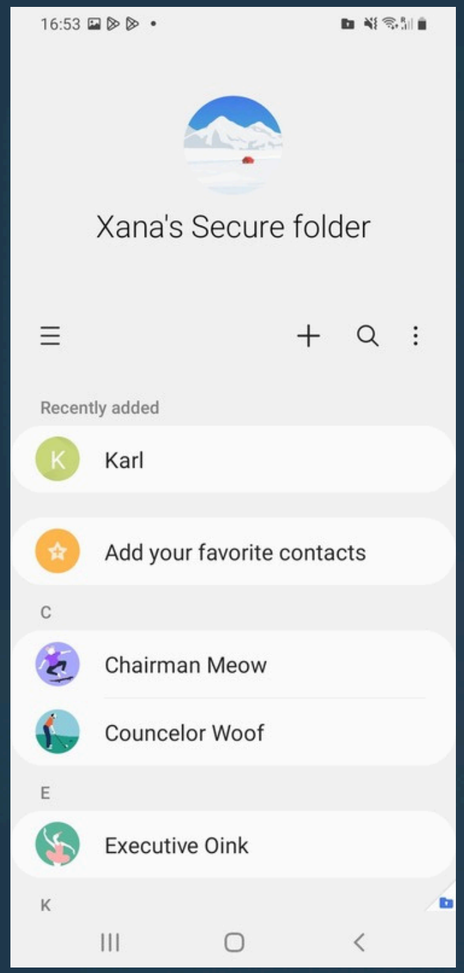
XRY Pro: Plataformas e fabricantes de dispositivos compatíveis

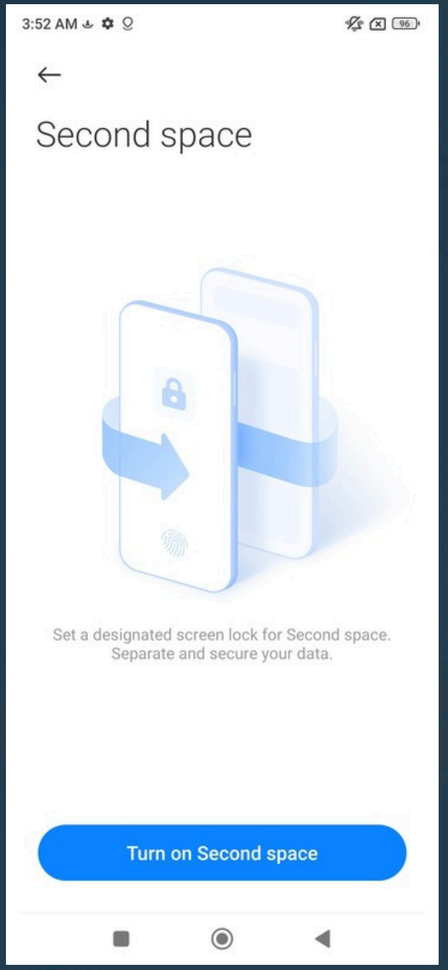
- Suporte à plataforma Unisoc (incluindo Samsung, Oppo, Realme, Motorola, Nokia e outras)
- Exploração de vulnerabilidades AFU e BFU para dispositivos Samsung/Exynos das séries A, J, S, Note e Ultra até a série S24 (incluindo Plus e Ultra)
- Explorações de segurança da Samsung/Qualcomm para dispositivos 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

MSAB

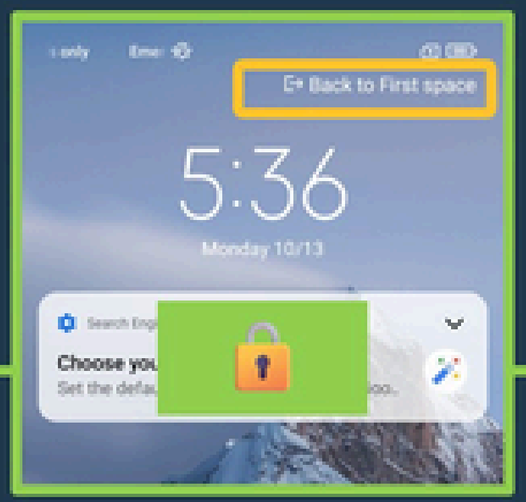
XRY Pro: Suporte para armazenamento oculto/seguro (também conhecido como Android multiusuário)

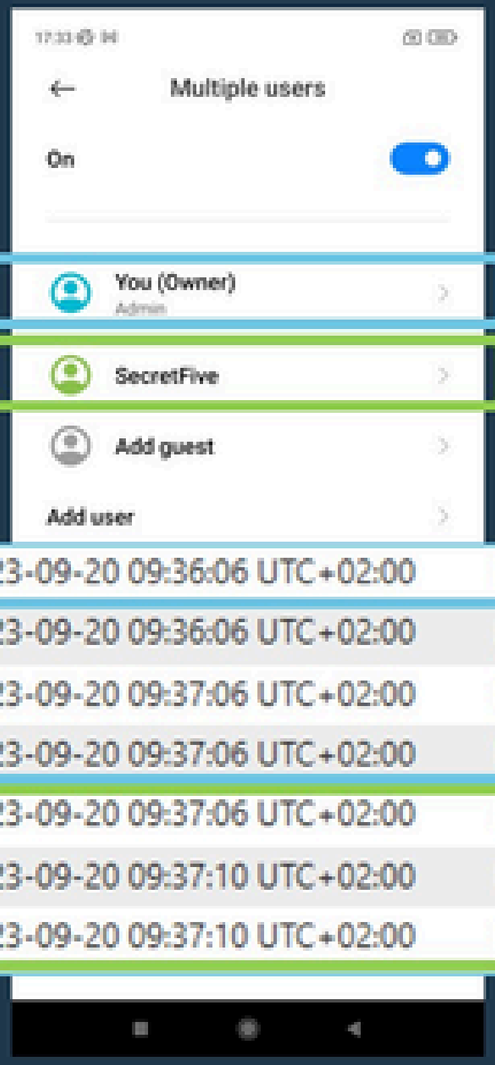
- O XRY Pro suporta a detecção e a quebra de senha de armazenamento seguro do fornecedor por força bruta ou mesmo a sua evasão
- Alguns exemplos de armazenamento seguro/oculto suportados:
  - Pasta Segura Samsung
  - Xiaomi Second Space
  - Implementações de outros fornecedores para multiusuário

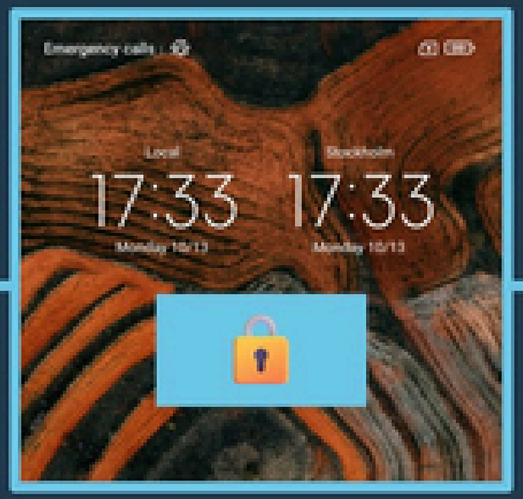




Exemplo: Gerenciamento de múltiplos usuários do Android no XRY Pro







ANDROIDFBEDEC...	Success	2023-09-20 09:36:06 UTC+02:00	Found 2 potential password files to bruteforce.
ANDROIDFBEDEC...	Success	2023-09-20 09:36:06 UTC+02:00	Password file 1/2, uid 0
ANDROIDFBEDEC...	Success	2023-09-20 09:37:06 UTC+02:00	Brute forcing succeeded
ANDROIDFBEDEC...	Success	2023-09-20 09:37:06 UTC+02:00	Device password is: '22017'
ANDROIDFBEDEC...	Success	2023-09-20 09:37:06 UTC+02:00	Password file 2/2, uid 10
ANDROIDFBEDEC...	Success	2023-09-20 09:37:10 UTC+02:00	Brute forcing succeeded
ANDROIDFBEDEC...	Success	2023-09-20 09:37:10 UTC+02:00	Device password is: '1234'

MSAB

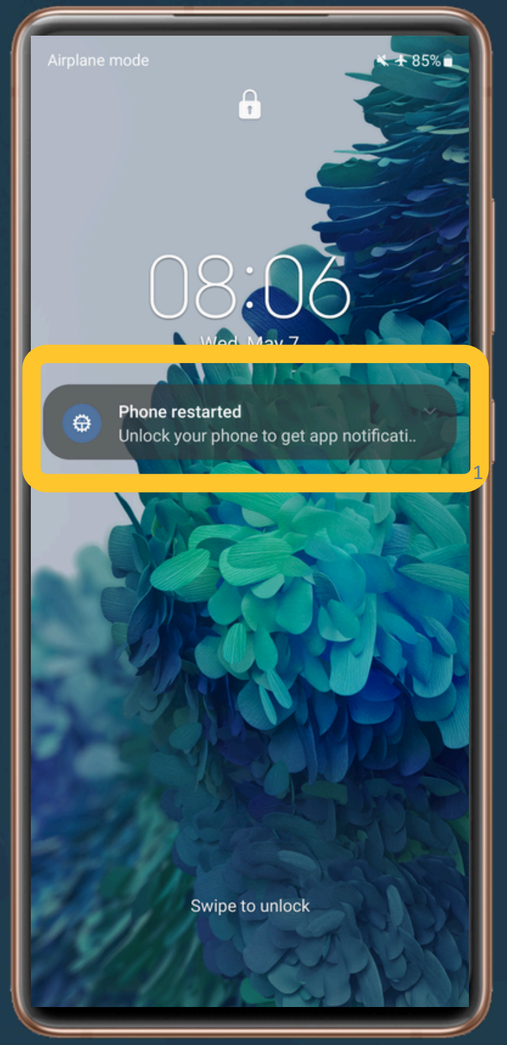
Extrações físicas/FFS com XRY Pro em BFU!

- 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

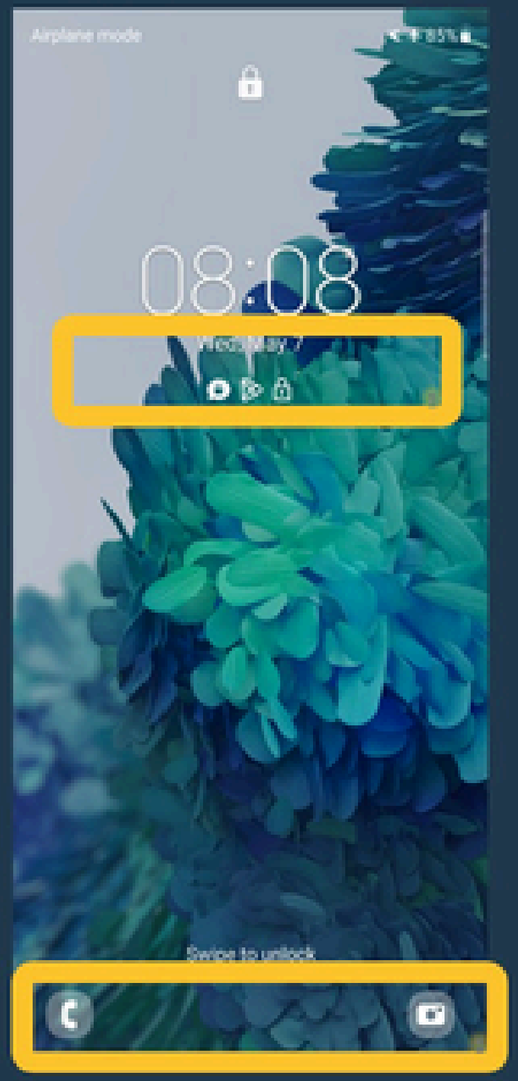
MSAB

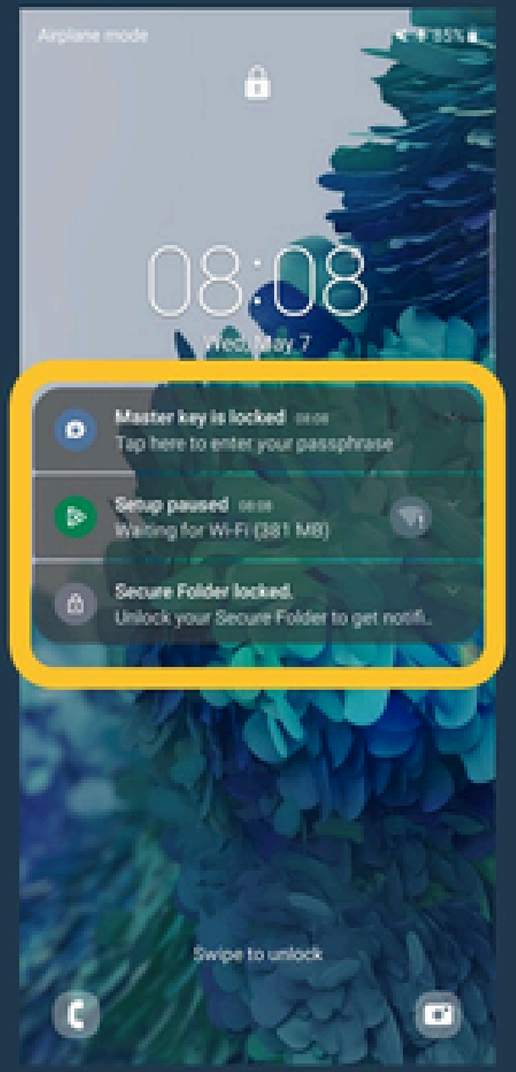
Identificar o estado de inicialização do dispositivo: Antes do primeiro desbloqueio (BFU)

- 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



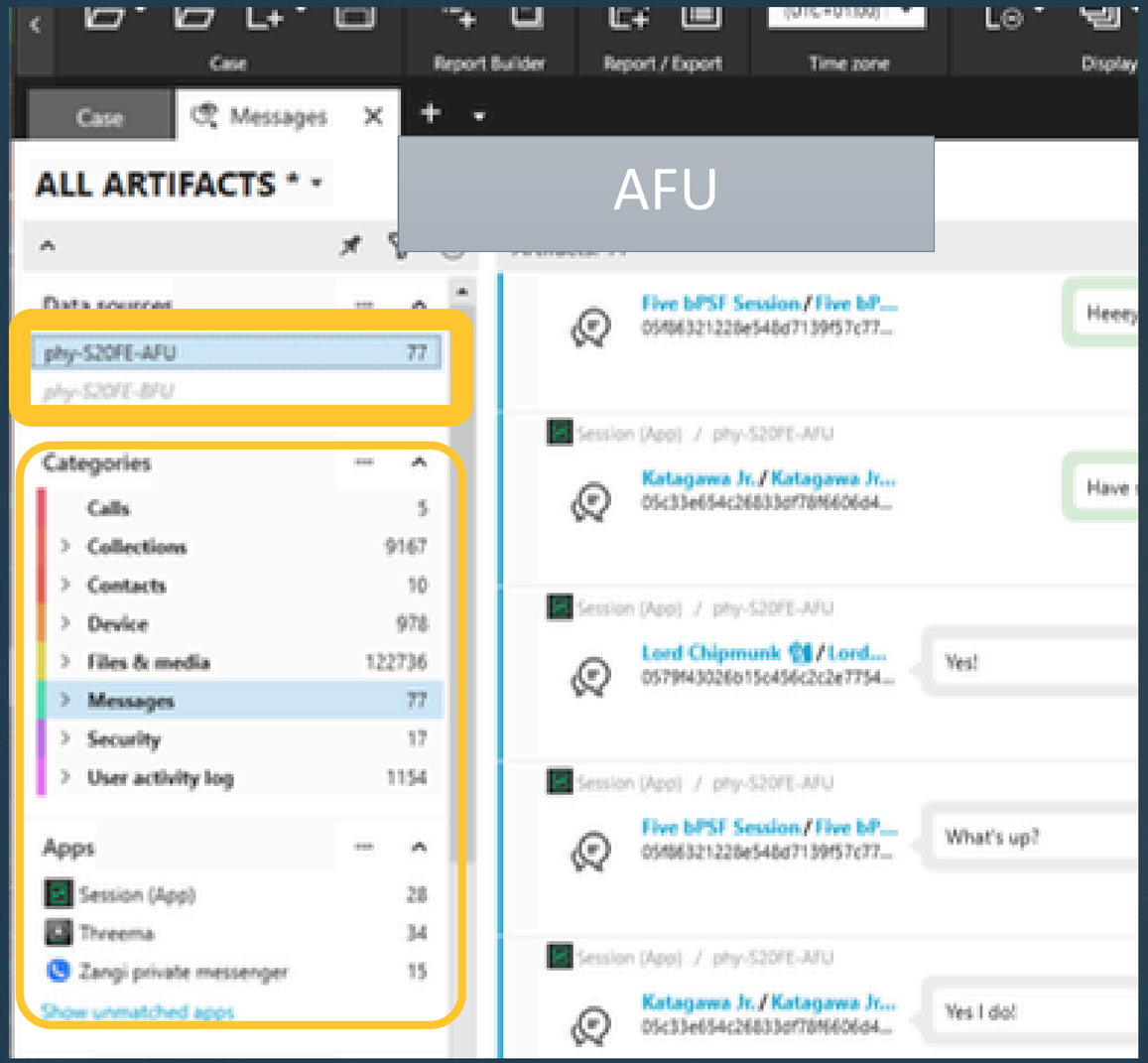
Identificar o estado de inicialização do dispositivo: Após o primeiro desbloqueio (AFU)

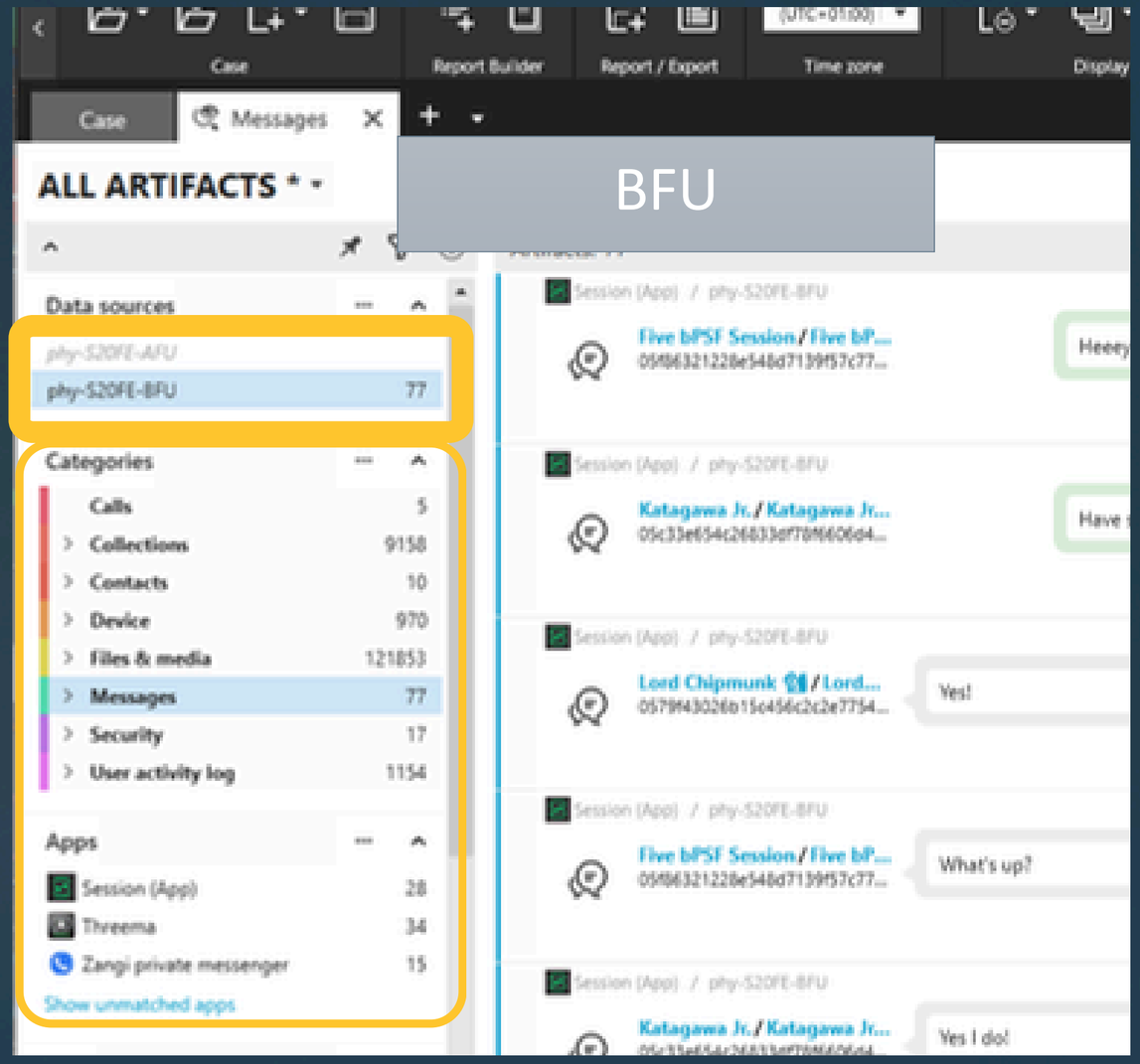




MSAB

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

MSAB

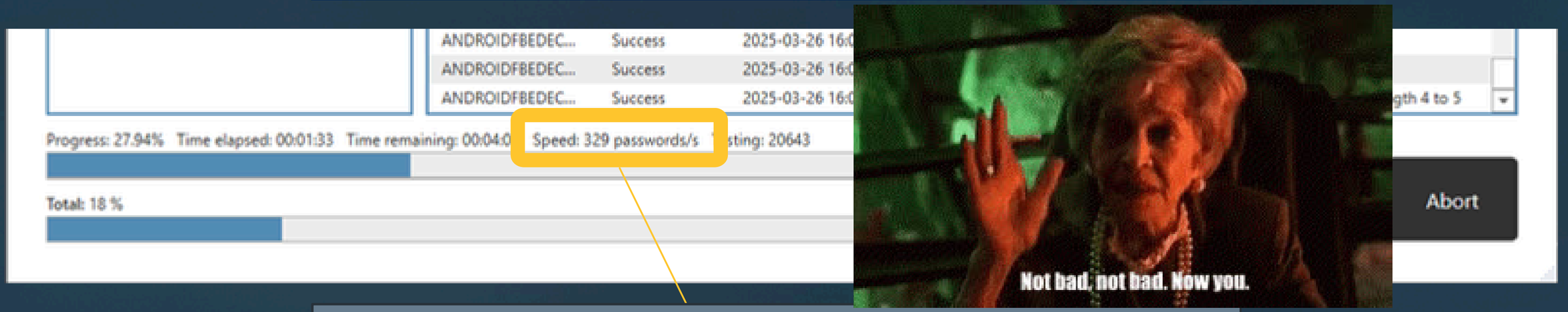
...quão rápido podemos usar o Brute-Force no XRY Pro

- 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

MSAB

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.



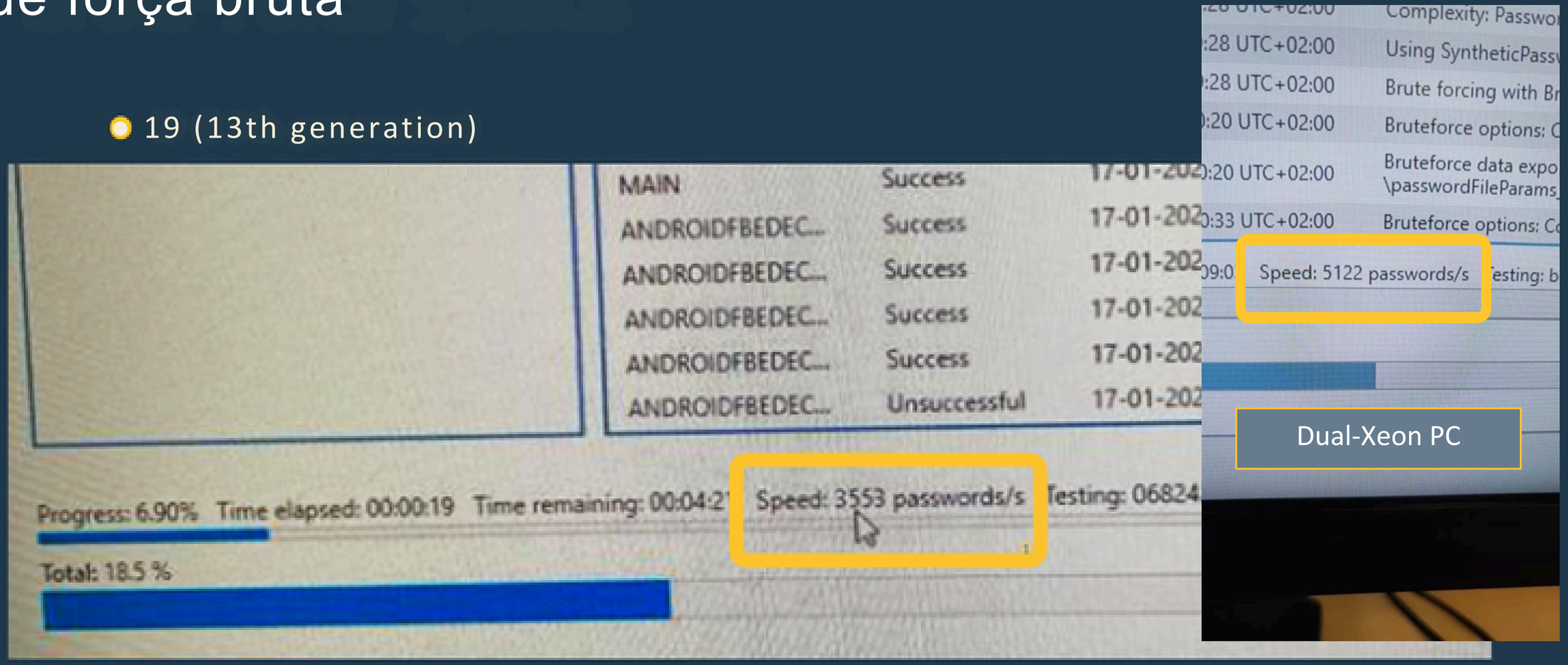
329 PpS (Senhas por segundo) = 329 * 60 ApM

...19740 ApM

MSAB

Alguns exemplos relatados por clientes: Velocidades de força bruta

- 19 (13th generation)



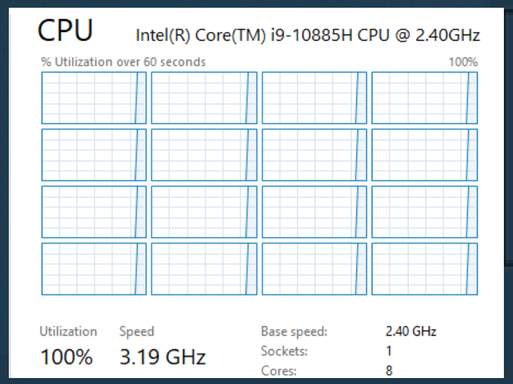
Precisa resolver isso mais rápido? Apresentamos o XRY BruteStorm

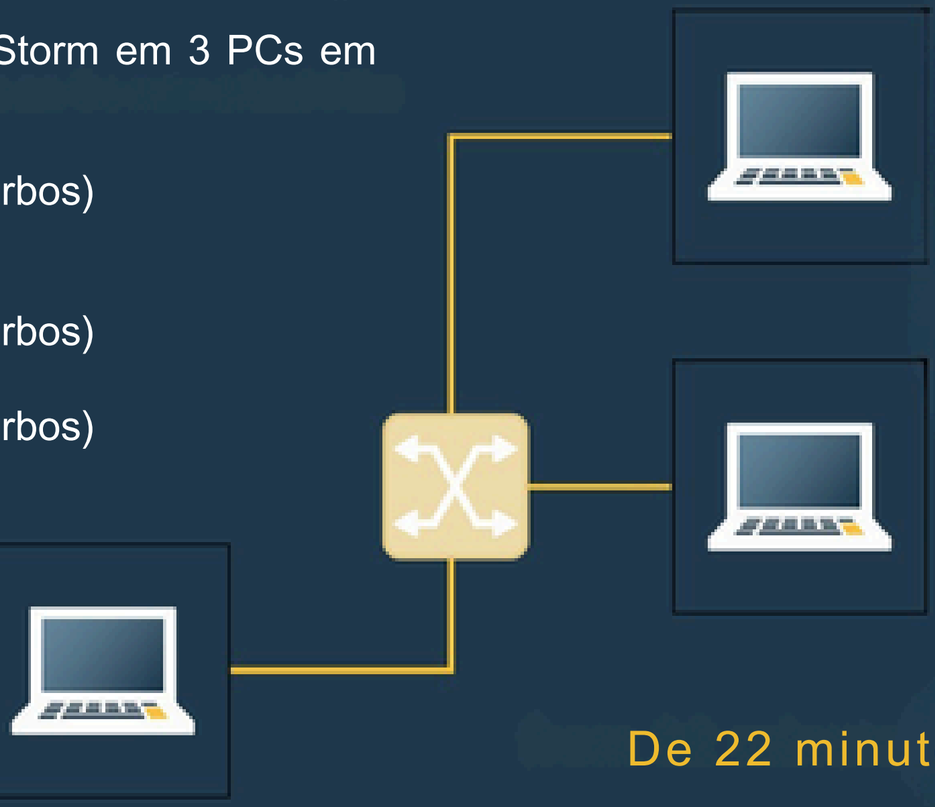
Exemplo XRY BruteStorm (laboratório pequeno)

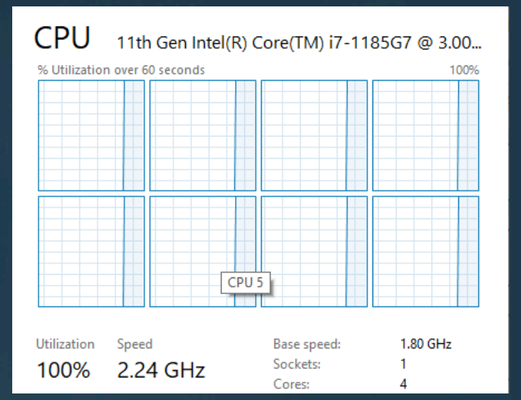
XRY BRUTESTORM

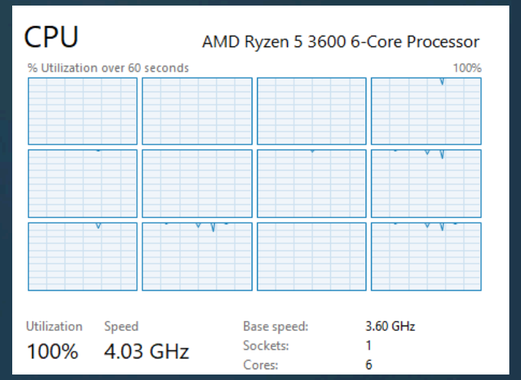
XRY Pro

- 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)







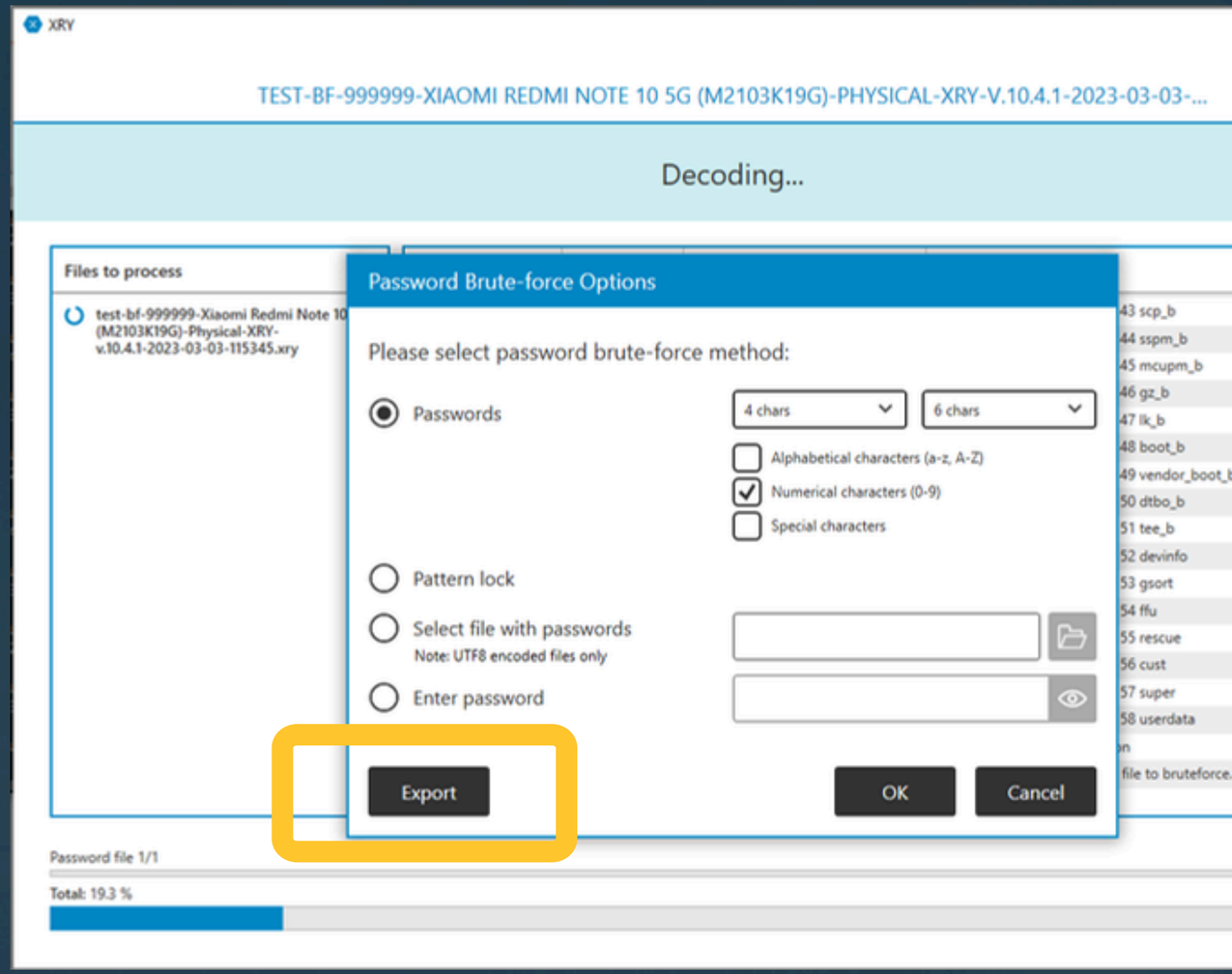


De 22 minutos >>> 8 minutos

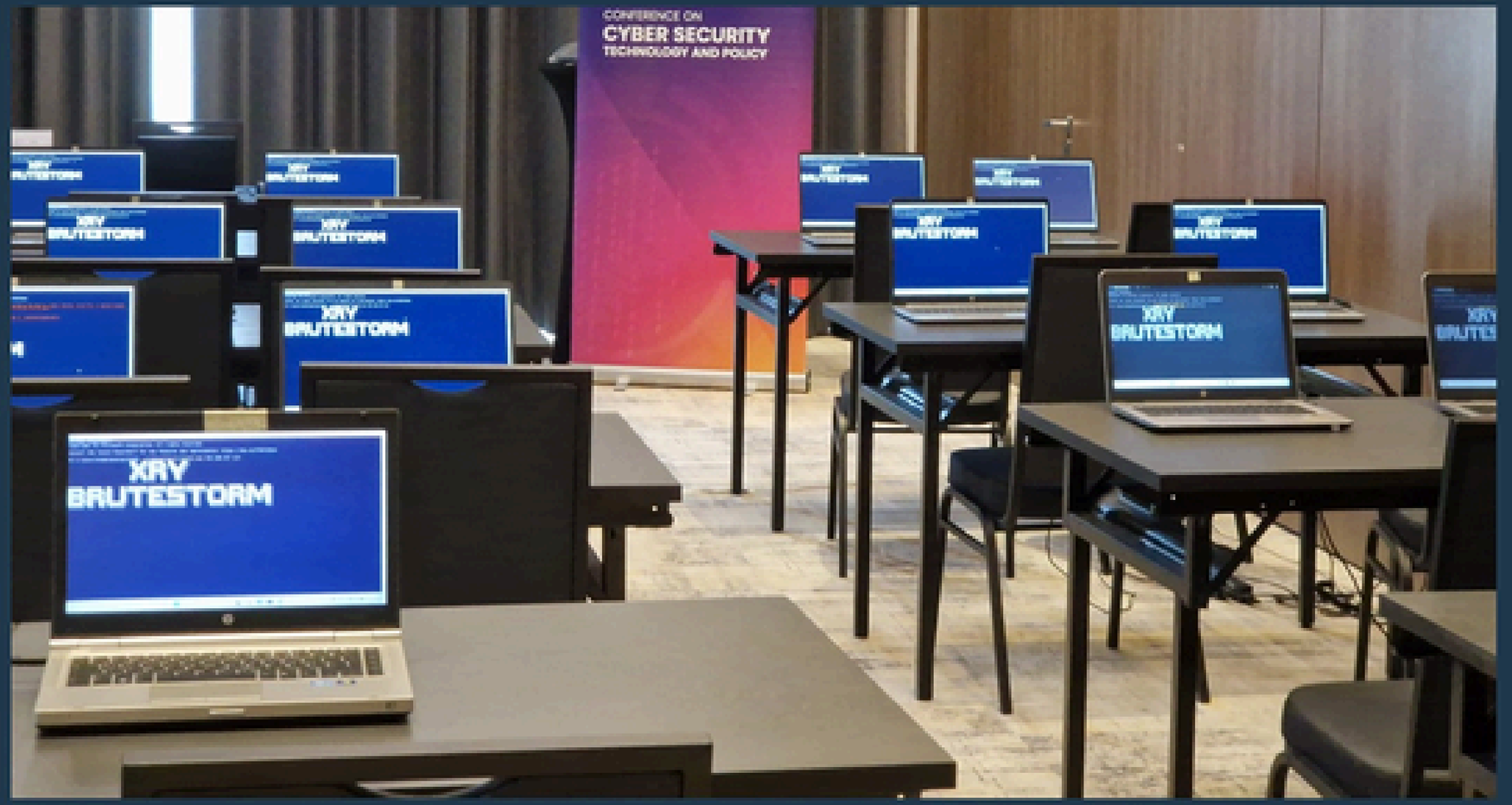
MSAB

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)



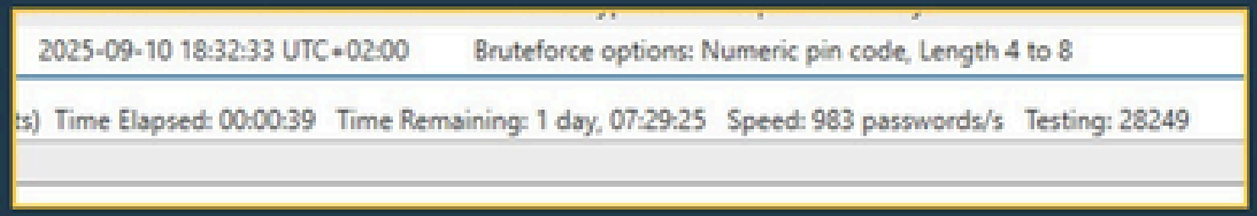
XRY

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

MSAB

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



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...

MSAB

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

MSAB

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

MSAB

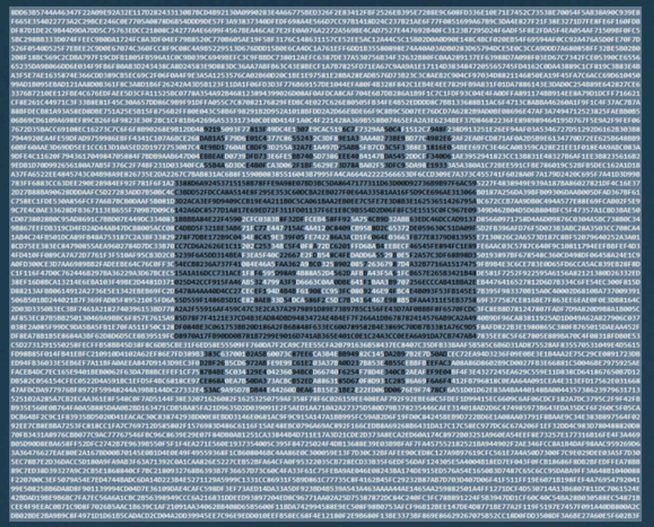
BruteStorm e BruteStorm Surge

	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

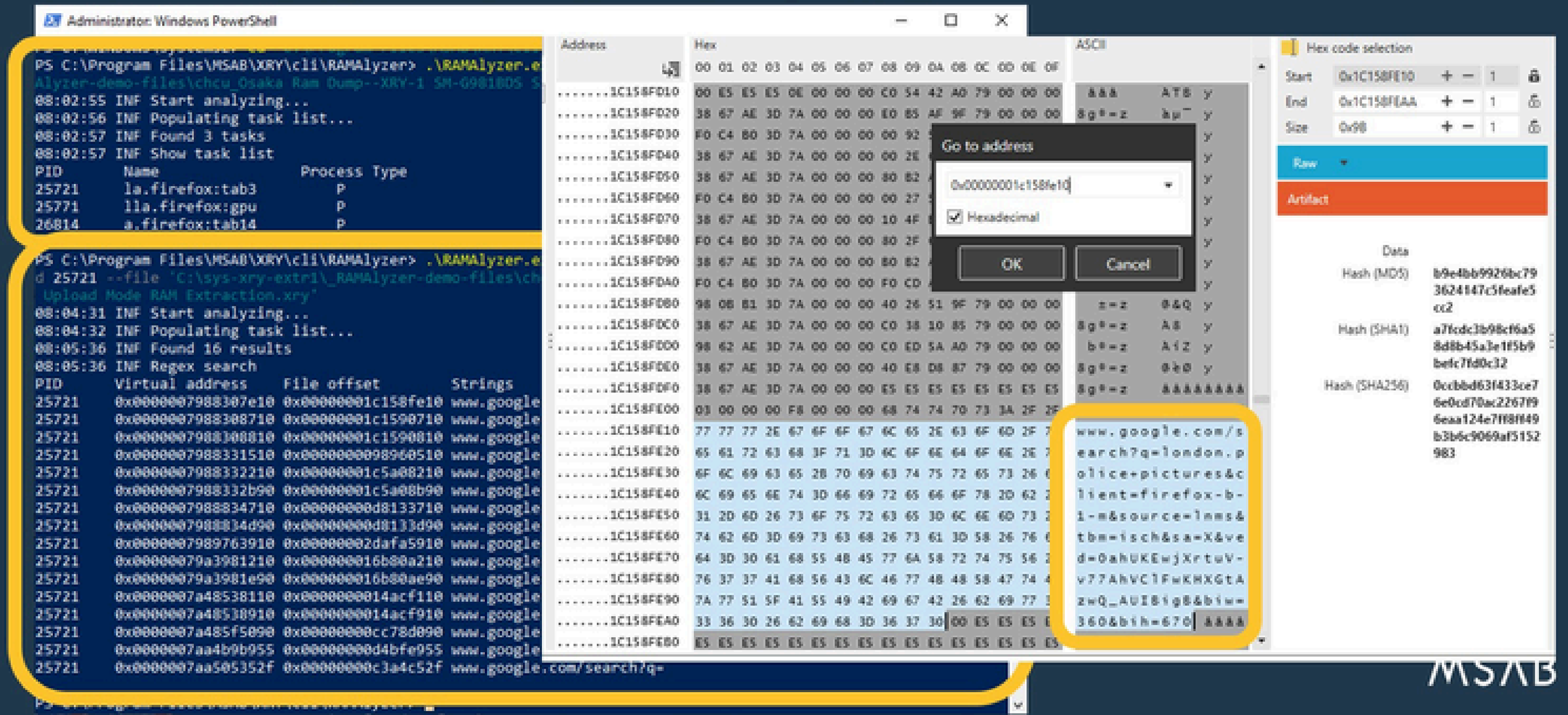
MSAB

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



Exemplo da ferramenta de análise RAM XRY Ramalyzer



XRY Pro: ...alguns requisitos:

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

MSAB

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)

MSAB

XRY

Obrigado!

FORMAX

FORCYBER

MSAB