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



Pruebas de Seguridad Ofensiva a Teléfonos Cifrados.





Contenidos

Introducción	3
Datos del equipo en custodia	3
4 algoritmos criptográficos utilizados:	4
Fase de pruebas y metodología aplicada	5
Resonancias (Passive Footprinting)	5
Resonancias (Active Footprinting) mediante BLE Sniffer	10
Enumeración Bluetooth	11
Pruebas de de-autenticación a red Wireless	14
Artefactos para la prueba	14
Comprobación y decodificación del handshake	
Conclusión de la prueba	21
Enumeración de puertos y servicios	22
Enumeración de puertos GALAXY S20 FE 5G	23
Enumeración de Puertos Galaxy S22 Ultra	24
Proceso de Extracción Forense	25
Introducción	25
Extracción Física Forense SAMSUNG Galaxy S20 FE 5G	35
Extracción Forense Lógica y Sistema de Archivos SAMSUNG S20 FE 5G	
Proceso para habilitar el modo desarrollador	
Extracción Física Forense Samsung Galaxy S22 Ultra	
Extracción Lógica Avanzada SAMSUNG GALAXY S22 Ultra	
Conclusiones del proceso de extracción forense	



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 У 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, está encriptado porque 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 <u>https://phonescoop.com/</u>

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:
	AT&T Crieket
	Verizon
	Boost Mobile Discontinued
	Metro Discontinued
	T-Mobile Discontinued
	<u>U.S. Certular</u> Discontinued
Procesador	Qualcomm Snapdragon 865
	6 GB <u>RAM</u>
	LPDDR5
Sistema Operativo	Android version 10
Bandas de operación (opera muchas otras)	5G: 2, 5, 25, 41, 66, 71, 260, 261 • more detail
	4G LTE: 2 4 5 7 12 13 14 25 26 29 30 38 40 41
	66, 71
	WCDMA: 2, 4, 5
	CDMA: 800, 850, 1900
	GSM: 850, 900, 1800, 1900
	overseas bands not shown; 5G 260, 261 (mmWave) only
Tecnología de Datos	<u>NR</u> (5G)
	plus Cat. 20 <u>LTE</u>
SIM Card	Nano 4FF
Pluotooth	Summerted Brofilers LICD, LICD, ODD, DDA, AODD, AV(DC, LICD
Bidelootii	PAN MAP
	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
	A3LSMG781V » approved Sep 22, 2020
	Macamororo //

View FormDisplay DisplayDisplay Applicant	Address	City	<u>StateCountry</u>	Zip CodeFCC ID	Application	Final	Lower Upper
Exhibits Grant Corresp- <u>Name</u>					Purpose	Action	FrequencyFrequency
	49 Matches	tound for	FCC ID A3LSM	IG781U			
View Attachment			Exhibit	<u>Type</u>	Date Submitted t	o FCCDisplay	TypeDate Available
Attestations 20200827 v1 - A3LSMG781U Au	uthorization Letter FCC		Cover Le	etter(s) (09/11/2020	pdf	09/17/2020
Attestations 20200827 v1 - A3LSMG781U H/	AC MIF Letter FCC		Cover Le	etter(s) (09/11/2020	pdf	09/17/2020
Attestations 20200828 v1 - A3LSMG781U Re	equest for confidentiality I	etter FCC	Cover Le	etter(s) (09/11/2020	pdf	09/17/2020
Attestations 20200908 v1 - A3LSMG781U LT	E Attestation letter FCC I	C Rev.1	Cover Le	etter(s) (09/11/2020	pdf	09/17/2020
ID Label & Location Info. 20200827 v1 - A3L	SMG781U E-Label Attesta	tion Letter	FC Cover Le	etter(s) (09/11/2020	pdf	09/17/2020
External Photos 20200828 v1 - A3LSMG781U	EXTERNAL PHOTO		Externa	Photos (09/11/2020	pdf	03/16/2021
ID Label & Location Info. 20200908 v1 - A3L	SMG781U E-label and Lo	cation FCC	Rev. ID Labe	//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 - A3LSMG78	1U SAR Report 3 of 6		RF Expo	sure Info (09/11/2020	pdf	09/17/2020

Soluciones simples, accesibles y confiables





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

This document is watermarked because certain important information in the document has not yet been verified. This document has been sent to you as a draft and for informational purposes only.

The document should only be used for internal purposes and may not be distributed outside of the company. Distributing the document outside of the company could result in legal exposure to the company if the preliminary,

unverified information in the draft turns out to be inaccurate.

SAMSUNG Galaxy S20 FE 5G



GALAXY S22 ULTRA

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

View FormDisplay DisplayDisplay <u>Applicant</u> Exhibits Grant Corresp- <u>Name</u> ondence	Address <u>Cit</u>	<u>y StateCountry</u>	<u>Zip CodeFCC ID</u>	Application Purpose	Final Lower Action Frequent Date In MHz	<u>Upper</u> cyFrequency In MHz
Detail Samsung Electronics Co L	td19 Chapin Rd., Building DPir	e BrookNJ United States	07058 A3LSMS908	BEOriginal Equipment	01/07/202213.56	13.56
View Attachment	Evhibit Type	Date Submitted to F	CCDisplay Type	aDate 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		

Soluciones simples, accesibles y confiables



FCC ID : A3LSMS908E

Internal Photographs



Soluciones simples, accesibles y confiables



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**.

Devices	Alerts	SSIDs	ADSB Live		
All devices	1	Ŧ]		
Name			🔺 Туре	ŧ	Phy
Tim's S22	Ultra		BR/EDR		Bluetooth
Galaxy S2	0 FE 5G		BR/EDR		Bluetooth

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

Find MAC Address Vendors. Now.	Find MAC Address Vendors. Now.
Enter a MAC Address	Enter a MAC Address
44:EA:30:C4:64:7E	DC:CC:E6:DB:A4:3B
Samsung Electronics Co.,Ltd	Samsung Electronics Co.,Ltd

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.

DEVICE: GALAXY S20 FE	5G	X
Name 😡	Galaxy S20 FE 5G 企	
Notes 🔞	Empty	
MAC Address 💿	DC:CC:E6:DB:A4:3B 🖉	
Manufacturer 📀	Samsung Electronics Ltd	
Туре	BR/EDR	
First Seen	Sat Oct 15 2022 22:28:48 GMT-0500 (Central Daylight Time)	
Last Seen	Sat Oct 15 2022 22:29:17 GMT-0500 (Central Daylight Time)	
Frequencies		
Channel 📀	FHSS	
Main Frequency 🔞	2.400 GHz	
	Packet frequency distribution	
30.0		
29.8		
29.6		
29.4		
29.2		
29.0		
28.8		
28.6		
28.4		
28.2		
28.0		
1		

Soluciones simples, accesibles y confiables



2400000:	29
description.kismet.device.base.crypt:	"string, printable encryption type"
kismet.device.base.crypt:	
description.kismet.device.base.key:	"devicekey, unique device key across phy and server"
kismet.device.base.key:	"B603E01100000000_3BA4DBE6CCDC"
description.kismet.device.base.packets.crypt:	"uint64_t, data packets using encryption"
kismet.device.base.packets.crypt:	U
description.kismet.device.base.packets.total:	"uint64_t, total packets seen of all types"
kismet.device.base.packets.total:	29
description.kismet.device.base.manuf:	"stringmanufacturec_pame".
kismet.device.base.manuf:	"Samsung Electronics Ltd"
description.kismet.device.base.basic_type_set:	"uint64_t, bitset of basic type"
kismet.device.base.basic_type_set:	8
description.kismet.device.base.seenby:	"map[int, x], sources that have seen this device"
description kismet common seenby unid-	Callas, BUD of Source"
kismat common seenby uuid	"910094E4_0000_0000_0000_878928419558"
description kisset serves wide	
description.kismet.server.uuid:	-uuld, unique server uuld
kismet.server.uuid:	"739E9B10-8E84-11EC-98B7-4B49534D4554"
description.kismet.device.base.packets.llc:	"uint64_t, observed protocol control packets"
kismet.device.base.packets.llc:	29
description.kismet.device.base.type:	"string, printable device type"
kismet.device.base.type:	"BR/EUK"
description.kismet.device.base.basic_crypt_set:	"uint64 t, bitset of basic encryption"

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.

DEVICE: TIM'S S22 ULTRA		×
Name Notes MAC Address Manufacturer Type First Seen Last Seen Frequencies Channel Channel	Tim's S22 Ultra (2) Empty 44:EA:30:C4:64:7E (2) Samsung Electronics Ltd BR/EDR Sat Oct 15 2022 22:40:24 GMT-0500 (Central Daylight Time) Sat Oct 15 2022 22:40:51 GMT-0500 (Central Daylight Time) FHSS 2 400 CUI-	
Pa	cket frequency distribution	
15.0 14.8 14.6 14.4 14.2 14.0 13.8 13.6 13.4 13.2		
13.0		



2400000:	34
description.kismet.device.base.crypt:	"string, printable encryption type"
kismet.device.base.crypt:	H-
description.kismet.device.base.key:	"devicekey, unique device key across phy and server"
kismet.device.base.key:	"B603E01100000000 7E64C430EA44"
description.kismet.device.base.packets.crypt:	"uint64 t, data packets using encryption"
kismet.device.base.packets.crypt:	Ð
description.kismet.device.base.packets.total:	"uint64 t, total packets seen of all types"
kismet.device.base.packets.total:	_14
description.kismet.device.base.manuf:	"string, manufacturer name"
kismet.device.base.manuf:	"Samsung Electronics Ltd"
description.kismet.device.base.basic_type_set:	"uint64_t, bitset of basic type"
kismet.device.base.basic_type_set:	8
description.kismet.device.base.seenby:	"map[int, x], sources that have seen this device"
<pre>w kismet.device.base.seenby:</pre>	
- 0:	
description.kismet.common.seenby.first_time:	"uint64_t, first time seen time_t"
kismet.common.seenby.first_time:	1665891624
description.kismet.common.seenby.last_time:	"uint64_t, last time seen time_t"
kismet.common.seenby.last_time:	1665891651
description.kismet.common.seenby.num_packets:	"uint64_t, number of packets seen by this device"
kismet.common.seenby.num_packets:	14
description.kismet.common.seenby.uuid:	"alias, UUID of source"
kismet.common.seenby.uuid:	"91DD0AE4-0000-0000-0000-8C882B41955B"
description.kismet.server.uuid:	"uuid, unique server UUID"
kismet.server.uuid:	"739E9B10-8E84-11EC-9887-4B49534D4554"
description.kismet.device.base.packets.llc:	uinto4_t, observed protocol control packets"
kismet.device.base.packets.llc:	14
description.kismet.device.base.type:	"string, printable device type"
kismet.device.base.type:	BR/EDR-
description.kismet.device.base.basic_crypt_set:	"uint64 t. bitset of basic encryption"
kismet.device.base.basic_crypt_set:	
description.kismet.device.base.frequency:	"double, frequency"

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.

ENCRYPTED	×
-----------	---

Encrypted

Some data frames can be identified by Kismet as carrying encryption, either by the contents or by packet flags, depending on the phy type

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



BSSID	PWR RXQ Beacons	#Data, #/s CH MB	ENC CIPHER AUTH ESSID
50:D4:F7:53:6D:FC	-34 96 297	56 0 3 270	WPA2 CCMP PSK Test24
BSSID	STATION	PWR Rate Lost	Frames Notes Probes
50:D4:F7:53:6D:FC	6E:50:CF:52:BB:F2	-24 1e-1 0	75
50:D4:F7:53:6D:FC	DE:3A:51:F8:25:FD	-32 1e- 6e 291	48
50:D4:F7:53:6D:FC	0C:72:D9:5A:E9:9C	-40 12e- 6e 0	27

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.

(root®	hskali)-[~]
🖵 🗰 airepl	lay-ng -0 10 -a 50:D4:F7:53:6D:FC -c 6E:50:CF:52:BB:F2 wlan0mon
12:39:31	Waiting for beacon frame (BSSID: 50:D4:F7:53:6D:FC) on channel 3
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 0
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 1
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 2
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 3
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 4
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 5
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 6
12:39:31	Sending 64 directed DeAuth (code 7). STMAC: [6E:50:CF:52:BB:F2] [0 7

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).**

BSSID	PWR RXQ Be	acons	#Data	a, #/s	СН МВ	ENC CIPHER	AUTH ESSID
50:D4:F7:53:6D:FC	-36 100	2566	461	1 0	3 270	WPA2 CCMP	PSK Test24
BSSID	STATION		PWR	Rate	Lost	Frames Note	es Probes
50:D4:F7:53:6D:FC	6E:50:CF:52	:BB:F2	-36	1e- 1	1582	5434 EAP	OL
50:D4:F7:53:6D:FC	DE:3A:51:F8	:25:FD	-36	1e- 1e	. 0	12918	rest24
50:D4:F7:53:6D:FC	0C:72:D9:5A	:E9:9C	-34	1e- 6e	: 0	372	



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 f	for beacon f	frame (B	BSSID:	50:[04:F7:53	3:6D:FC)	on channel 3	3		
12:38:11	Sending 6	64 directed	DeAuth	(code	7).	STMAC:	[DE:3A:5	1:F8:25:FD]	[0	0
12:38:11	Sending 6	64 directed	DeAuth	(code	7).	STMAC:	[DE:3A:5	1:F8:25:FD]	[1	Ø
12:38:11	Sending 6	64 directed	DeAuth	(code	7).	STMAC:	[DE:3A:5	1:F8:25:FD]	[1	1
12:38:11	Sending 6	64 directed	DeAuth	(code	7).	STMAC:	[DE:3A:5	1:F8:25:FD]	[2	1
12:38:11	Sending 6	64 directed	DeAuth	(code	7).	STMAC:	[DE:3A:5	1: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	#Dat	a, #/s	СН	MB	ENC CI	PHER	AUTH	ESSID
50:D4:F7:53:6D:FC	-37 100	5820	88	2 2	3	270	WPA2 C	CMP	PSK	Test24
BSSID	STATION		PWR	Rate	Lo	st	Frames	Note	s Pr	obes
50:D4:F7:53:6D:FC	DE:3A:51	:F8:25:FD	-22	1e- 6	e	2	25752	EAPO	L Te	st24
50:D4:F7:53:6D:FC	0C:72:D9	:5A:E9:9C	-38	1e- 6	e	0	936	EAPO	L Te	st24

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.	l 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"						
Assoc	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=		
۸.	م مامر										

Authentication

W	lan.fc.t	ype_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.

<pre>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 GNUL General Public License v3+</pre>
This code is distributed under the GNO deneral Public Elcense VS+
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').
<pre>#1: Station 6e:50:cf:52:bb:f2, 9 handshake(s):</pre>
<pre>#1: HMAC_SHA1_AES, good*, spread 1</pre>
#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.



Cor	npro	ba	ció	n y	/ d	eco	odi	fic	aci	ón	de	el k	nar	nds	sha	ake
Land Read Rese Rese Read	aircr ding p ning c etting etting d 1132	ack ack apt EAI EAI	-ng ets ura2 POL POL pacl	-J , p 24-(Har Har kets	caj lea: 01.0 ndsl ndsl s.	ptu se v cap hake hake	raha wait e de e de	ash t eco	<u>ca</u> der der	sta sta	ate	4-01	1.ca	<u>ap</u>		
1	# BSS	ID					ESS	SID								Encryption
:	1 50:	D4:	F7:	53:0	5D:	FC	Tes	st24	4						l	WPA (1 handshake)
Cho	osing	fir	st i	netı	vor	k as	s ta	arge	et.							
Rea Oper Res Res Rea	ding p ning c etting etting d 1132	ack apt EAI EAI 58	ets ura2 POL POL pacl	, p ¹ 24-(Han Han kets	lea: 01.0 ndsl ndsl s.	se w cap hake hake	wait e de e de	ecoe	der der	sta sta	ate. ate.	•				
1 p	otenti	al	tarı	gets	s											
Bui ¹ [*] [*] [*] [*]	lding ESSID Key v BSSID STA: anonc	Has (l ers : 5 DE: e:	hcat engt ion: 0:D4 3A:S	t f: th: : 2 4:F7 51:I	ile 6) 7:5: F8:2	···· : Te 3:6[25:1	est2 D:F0 FD	24								
	49 82 77 70	6A	EF F1	42 F2	94 71	25 6D	51 54	46 06	D5 BC	47 81	2B ∆2	FA 20	ED E6	45 1 D	DA	
[*]	snonc	e:		L2	/1				DC		A 2	20	LU			
	6F 92 AE 47	D4 0B	77 97	BØ FD	1F D2	6C D6	3B 33	8B 67	03 0E	FØ 28	0A 0C	24 06	96 9B	D8 DD	7F 4F	
[*] [*]	Key M 28 D4 eapol	IC: 06 :	DE	06	8B	C6	60	58	9E	94	A2	85	88	92	27	
	01 03	00	75 D	02	01	0A	00	00	00	00	00	00	00	00	00	
	01 6F 7F AE	92 47	04 08	// 97	Б0 FD	1F D2	6С D6	3В 33	8B 67	03 0E	FØ 28	0A 0C	24 06	96 9B	D8 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	16	30	14	01	00	00	06 0F	AC	00 04	01	00	00	06 0F	AC	
	04 01	00	00	ØF	AC	02	00	00								
Suc	cessfu	11v	wrj	itte	en i	to	capt	tura	ahas	sh.	hcca	ap				

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



—(root⊛hskali)-[~]

hccap2john capturahash.hccap > capturahandshake

—(root®hskali)-[~]

- —# du -hc <u>capturahash.hccap</u>
- 4.0K capturahash.hccap

4.0K total

—(root⊛hskali)-[~]

L <mark>#</mark> hccap2john <u>capturahash.hccap</u>
Test24:\$WPAPSK\$Test24#IBHrIqrwrXdFy0LxPt9IRv.TP1i9.z.877PMTut50tTxohMnNksc1.0PrIx7UafjEdEZ
IIPJFmjuvILORrbKwS7lPJE4j94W6CMRnE21.5I0.Ec/Pt9IRv.TP1i9.z.877PMTut50tTxohMnNk
sc1.0PrIw3X.I.E1uk2.E
1uk2.E1uk0
/tV0XI/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)-[~]

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	1	
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:

펜 [Client-Lan] - 192.168.0.149	8E:AF:6A:69:0A:E0
Щ [Client-Lan] - 192.168.0.179	CA:DD:5D:91:FE:17

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 elansed Imap 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.



 Image: Constrained state sta

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.

🗑 Cellebrite UFE	D 7.53.0.24					-	
	zte maven 3	X	VICE WIZARD Beta		Ø	≡	
	All	Vendors	Generic profiles	Recently used			
	ZTE GSM Z8 <u>3</u> 5 <u>Maven</u> 3						
	ABORT				ВАСК		

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.*



Soluciones simples, accesibles y confiables



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

Cellebrite UFB	D 753024				-	0 ×
	SELECT MODE				=	
	Cable A with black tip T-2	n 3 100				
	Advanced ADB	ADB (Rooted)	Decrypting Boot Loader (Recommended) Lock Bypass			c
	ABORT			ВАСК		

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.

Cellebrite UFED 7.53.0.24					-	\times
WAITING FOR DEVI	CE			⊙ ≡		
Cable A with blac	Maven 3 sk tip T-100					
Connect the source device	to a USB port.					
Z835 Maven 3: To enable device connection The battery should be fully of 1. Remove the battery and SD 2. Re-insert the battery (with * If the battery is not remova 3. Leave the device powered 4. Simultaneously, press and (while holding the buttons) u 5. Press Continue.	: harged. IM card from the device. Jout the SIM card). able, power off the device. off. hold the Volume Up + Volume Down keys and con Intil the Continue button is enabled.	nect the device to the Ce	llebrite UFED. Then wait for	at least 10 seconds		
ABORT		ВАСК	CONSOLE	CONTINUE		

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.

Soluciones simples, accesibles y confiables



Cellebrite UFED 7.53.0.24



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.



Please Wait. Initializing step 4 out of 6.



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

Cellebrite UFED 7.53.0.24		-	
EXTRACTION IN PROGRESS	0	≡	
ZTE GSM Z835 Maven 3 Cable A with black tip T-100			
Please wait, this can take some time			
Please Wait			
Preparing to execute, this can take a few minutes			пх
EXTRACTION IN PROGRESS	0	≡	
ZTE GSM Z835 Maven 3 Cable A with black tip T-100			
Please wait, this can take some time			
DIKU_mmcDikU.bin 1/2		-	0 X
EXTRACTION SUMMARY	O	=	
Extraction completed successfully			
Source: Z835 Maven 3			
Target: Local Drive (Physical Decrypting Boot Loader (Recommended) 01)			

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.



Cellebrite PHYSICAL ANALYZER				 10 1 1 0 1 0 0 1 1 1 1 0 0 1 0 1 0 1 0	000100001100011100011100	000010111100000000000000000000000000000				010100000000000000000000000000000000000	0 0 1 0 0 0 0 1 1 1 1 1 0 0 1 0 0 0 1	
🗘 Cellebrite		-			c	ell	eb	rite	2 C	020)22	14%

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

Case wiza	ard						
Op	pen case	<u>Help</u>	Load evidence Select the extractions				۵. ۱
•	Load evidence		+ Add + Add password list				
	Select import lo	ocation					\times
	$\leftarrow \rightarrow \star \uparrow$	📜 « Z1	TE > UFED ZTE GSM Z835 N	/laven 3 2022_07 →	ب ن	Buscar en UFED ZTE	E GSM Z8
	Organizar 🔻	Nueva ca	rpeta				•
	SAS	^	Nombre		Fecha de modificación	Тіро	Tamaño
	. 🗢 Este equipo		📒 Physical Decrypting Bo	oot Loader (Recom	22/07/2022 04:28 p.m.	Carpeta de archivos	5
	🖊 Descargas		EvidenceCollection		22/07/2022 04:28 p.m.	UFED Multiple Du	1
			Música Objetos 3D Videos Windows (C:) HS-Data (D:) V				
			Nombre de archivo:		 All Suppo Abrii 	rted Files V Cancelar	÷
	Back					Next	

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



✓ Extractions: 1

ZT endert Size uns uzaut Alar Alar Den versität Den ve	Physical ZTE GSM Z835 Maven 3 Physical Extraction start date/time 22/07/2022 04:17:01 p. m.(UTC-5) Extraction end date/time 22/07/2022 04:28:07 p. m.(UTC-5)	Image Hashes Hash data is available for this extraction.
Proc. Bassing Sal. Rand Gala		Verify image hash

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

Analyzed Data				
>	::	Application (193)		
>	بر	Calls (180) (7)		
>	9	Contacts (1272) <mark>(155)</mark>		
>	((†))	Devices & Networks (3617)		
>	Ŷ	Location Related (20) (1)		
>	0	Media (12778) <mark>(595)</mark>		
>	Þ	Messages (1964) <mark>(6)</mark>		
>	۹	Search & Web (845) (1)		
>	2 t	User Accounts & Details (368)		

Data fi	iles
	Applications (2140) (55)
	Archives (31) (12)
¢	Configurations (38)
₹	Databases (390) <mark>(3)</mark>
8	Documents (1)
5	Exchange (1)
T	Text (1714) <mark>(99)</mark>
۳	Uncategorized (18173) (7419)
Mes	sages (1964) <mark>(6)</mark>

~	Chats (156) (5) (10253 messages)
	> 📮 Instagram (29) (281 messages)
	Native Messages (29) (3) (162 messages)
	> 📮 WhatsApp (98) (2) (9810 messages)
>	🖾 Emails (1808) (1)



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.



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.



Cellebrite UFED 7.53.0.24					- 🗆 X
🎲 Cellebrite UFED				⊙ ≡	
			_		
	SIM	card	Ma	ss storage	
Mobile device					
			<u> </u>		
	UFED camera	a Quicl	к сору	Drone	
				R D	
				S	
Device tools					
Version 7.53.0.24			(⁽) 03:11:41 p. m	າ. │ [ະີະີ] 22/07/2022	2
Callabeles (IEED 752.0.24					
	DEVICE WIZARD	Beta		⊙ ≡	
	T				1
	l			EXTRACTION FLOW] -
		🗙 AUTO DETEC	TION TIPS		
		Android devices			
		2. Enable USB del	bugging	and Number 7 times)	
		 Enable stay aw Set USB connet 	ake (if available) ction to enable file	e transfers (MTP/Media))
		iOS devices	a ali		
	Ţ	1. Disable auto-le	DCK		
)				
ABORT	BACK	CONSOLE	BROWSE DEVICE	ES AUTO DETECT	

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.

🗑 Cellebrite UFE	0 7.53.0.24				-	\times
	SELECT EXTRACTION TYPE				≡	
	Samsung GSM SM-G7 USB cable 170 or Original	81U Galaxy S20 FE 5G Cable				
	i Advanced Logical	File system	i Physical (Rooted)	Camera		
	Screenshot	Chat Capture				

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.

	ABORT		ВАСК	CONSOLE	USE BLUETOOTH	
--	-------	--	------	---------	---------------	--

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.



Cellebrite UF	ED 7.58.0.172	×
	DETECT DEVICE	⊙ ≡
	CONNECT DEVICE TO AUTO DETECT	
		 ★ AUTO DETECTION TIPS Android devices 1. Enable developer options (tap Build Number 7 times) 2. Enable USB debugging 3. Enable stay awake (if available) 4. Set USB connection to enable file transfers (MTP/Media) iOS devices 1. Disable auto-lock
	ABORT	BACK CONSOLE AUTO DETECT

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"

🝘 Cellebrite UFE	D 7.580.172	- 🗆 ×
	DETECT DEVICE	
	CONNECT DEVICE TO AUTO DETECT	
	Auto detect didn't find the device	
	1 Disconnect the device 2 Android only: Turn on USB Debug and enable Media Device mode (MTP) 3 Wait 5 seconds and reconnect the device (Auto detect will start)	iuild Number 7 times) Ie transfers (MTP/Media)
	Tried the steps, and the device wasn't found? FIND DEVICE MANUALLY CONSOLE	
	ABORT BACK CONS	OLE AUTO DETECT

Soluciones simples, accesibles y confiables



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.

Samsung GSM SM-S9080 C USB cable 170 or Original Cable	Galaxy S22 Ultra	
	Extraction to Local Drive	
	D:\Cellebrite\S22	



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.

Samsung GSM SM-S9080 Galaxy S22 Ultra USB cable 170 or Original Cable								
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.								
Android 4.2 and Higher	4.1.2 and Lower	_						
	🗟 Tutorial Video							
1 . Enable Developer options	How to?							
2 . Enable Stay awake and US	B debugging modes How to?							
3 . Verify screen lock mode	How to?							
4. Connect the device to the	unit.							
ABORT		ВАСК	CONSOLE	CONTINUE				

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

Samsung GSM SM-S90	080 Galaxy S22 Ultr ^{Cable}	а		
v	Varning			
A Tr C	device restart may be o continue with the exi lick "Abort" to end the	required during the traction select "Cont e extraction.	extraction process. tinue".	
	[ABORT	CONTINUE	



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

 $\mathsf{Menu} \ (\mathsf{Apps}) \rightarrow \mathsf{Settings} \ (\mathsf{More}) \rightarrow \mathsf{Security} \ \mathsf{and} \ \mathsf{confirm} \ \mathsf{any} \ \mathsf{pop-up} \ \mathsf{that} \ \mathsf{appears} \ \mathsf{during} \ \mathsf{the} \ \mathsf{start} \ \mathsf{of} \ \mathsf{the} \ \mathsf{transaction}.$

To enable the Developer options, go to

Menu (Apps) \rightarrow Settings (More) \rightarrow About (Software information) \rightarrow More, and tap the "Build number" 7 times until they are enabled. To enable "USB Debugging", go to:

 $\mathsf{Menu} \rightarrow \mathsf{Settings} \rightarrow \mathsf{Applications} \rightarrow \mathsf{Development} \rightarrow \mathsf{select} \ \mathsf{the} \ \mathsf{checkbox} \ "\mathsf{USB} \ \mathsf{debugging}".$

• -- OR ----

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

Extraction Error

Cannot connect to device (13)

• -- OR ----

 $\mathsf{Menu}\ (\mathsf{Apps}) \rightarrow \mathsf{Settings}\ (\mathsf{More}) \rightarrow \mathsf{Developer}\ \mathsf{options} \rightarrow \mathsf{select}\ \mathsf{the}\ \mathsf{checkbox}\ "\mathsf{USB}\ \mathsf{debugging}".$

• -- OR ----

 $\mathsf{Menu} \rightarrow \mathsf{Settings} \rightarrow \mathsf{More} \rightarrow \mathsf{Development} \rightarrow \mathsf{select} \ \mathsf{the} \ \mathsf{checkbox} \ "\mathsf{USB} \ \mathsf{debugging}".$

• -- OR ----

 $\mathsf{Menu} \rightarrow \mathsf{Settings} \rightarrow \mathsf{select} \ \mathsf{General} \ \mathsf{tab} \rightarrow \ \mathsf{Developer} \ \mathsf{options} \rightarrow \mathsf{select} \ \texttt{"USB} \ \mathsf{debugging"} \ \mathsf{check} \ \mathsf{box}.$

• -- OR ----

Menu \rightarrow Settings \rightarrow General \rightarrow Applications \rightarrow Development \rightarrow USB debugging \rightarrow Switch to ON * And if exists:

 $\label{eq:Menu} Menu \rightarrow Settings \rightarrow select Networks tab \rightarrow PC connection \rightarrow clear the checkbox from "Ask on connection" Please dial ##8778# or *#7284# on phone's dial pad, if the 'PhoneUtil' menu appears, please set USB to 'PDA'. Then reboot the phone.$

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.

Cellebrite UFED	7.58.0.172			_	L X
	SELECT EXTRACTION TYPE			⊙ ≡	
	Samsung GSM SM-S USB cable 170 or Origin	9080 Galaxy S22 Ultra al Cable			
	i Advanced Logical	File system	Physical (Rooted)	Camera	
	Screenshot	Chat Capture			
	ABORT			ВАСК	

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

Cellebrite UFED 7.58.0.172		- 🗆 ×
SELECT EXTRACTION LOCATION	◎ =	
Samsung GSM SM-S9080 Galaxy S22 Ultra USB cable 170 or Original Cable		_
Extraction to Local Drive		
D:\Extraccion\S22 Ultra		
ABORT	NEVT	



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.

Cellebrite UFED 7.58.0.172					-	\Box \times
WAITING FOR DEVICE					=	
Samsung GSM SM-S9080 Gala USB cable 170 or Original Cable	axy S22 Ultra					
Connect the source device to a USB port.						
 SM-S9080 Galaxy S22 Ultra: 1. To enable the Developer options, go to Menu (A) 2. Go to Menu (Apps) → Settings → Developer opti To enable multimedia transfer, please set the follow When the device is connected, press and hold the select Transfer files on the phone also set: Menu (Apps) → Settings → Lock screen → Select sc This phone needs a client in order to communicate The application has to upload the client to the phone 	pps) → Settings → About pl ions → select check boxes " wing: status bar, then slide your fi creen lock → select "None". with the application. ne prior to using it.	none → tap the "Build nun USB debugging" and "Stay inger downward:	nber" 7 times until they are awake".	enabled.		
ABORT	ВАСК	CONSOLE	USE BLUETOOTH	CONTINU	JE	

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.

19:56	\$ a b •	al 87% 💼	19:56 🕲 뎒 🔒 🔹	.ıll 87% 🖬
Set	tings	Q	< About phone	Q
0	Digital Wellbeing and parental of Screen time • App timers • Bedtime mo	controls	Tim's S	22 Ultra
0	Battery and device care Storage • Memory • Device protection		E	idit
	Appo		Phone number	Unknown
	Default apps • App settings		Model name	Galaxy S22 Ultra
			Model number	SM-S908E/DS
A	General management		Serial number	RFCT31GQL2D
-	Language and keyboard * Date and time		IMEI (slot 1)	354862740043349
Ŕ	Accessibility TalkBack • Mono audio • Assistant mer	าน	IMEI (slot 2)	354955820043344
0	Software update		Status information	
			Legal information	
	User manual Learn more		Software information	
0	Remote support Remote support		Battery information	
0	About phone		and the second second	
0	Status • Legal information • Phone nam	le	Looking for someth	ing else?
	111 0 <		111	0 <

Soluciones simples, accesibles y confiables





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.

Cellebrite UFED 7.58.0.172			- 🗆 ×
SELECT EXTRACTION	ТҮРЕ		◎ ≡
Samsung GSM USB cable 170 or	SM-S9080 Galaxy S22 Ultra Original Cable		
Advanced Logical	i File system	• Physical (Rooted)	Camera
Screenshot	Chat Capture		
ABORT			ВАСК

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



SELECT CONTENT TYPE				⊚ ≡
Samsung GSM SM-SS USB cable 170 or Origina	9080 Galaxy S22 Ultra al Cable			
🕝 Extract from				
Device	B SIM			
B Choose data types to	extract			🔲 All
₽, Call Logs	O Locations	<u> </u> Advertising ID	<u></u> co	ntacts
ଣ୍ଟି sms	[р ммs	👬 Calendar	🛃 Pic	tures
f Audio/Music	Dideos	Ringtones	E Do	cuments
Archives				owsing Data
ABORT			BACK	NEXT
Archives	🚊 Email	2, ім	E Bro	wsing Data
🔐 User Dictionary	iies			
ABORT			BACK	NEXT

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

Warning

The following content types may require a device restart during the extraction process:

Files.

Select "Continue" to continue with the extraction.

Select "Exclude content" and avoid a device restart during the extraction.





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.

Extra Info Read Failed

SM-S9080 Galaxy S22 Ultra (USB cable 170 or Original Cable): Cannot connect to device (13) SM-S9080 Galaxy S22 Ultra: If any prompt messages display on the device, press Allow or Yes 1. To enable the Developer options, go to Menu (Apps) → Settings → About phone → tap the "Build number" 7 times until they are enabled. 2. Go to Menu (Apps) → Settings → Developer options → select check boxes "USB debugging" and "Stay awake". To enable multimedia transfer, please set the following: When the device is connected, press and hold the status bar, then slide your finger downward: select Transfer files on the phone also set: Menu (Apps) → Settings → Lock screen → Select screen lock → select "None". This phone needs a client in order to communicate with the application. The application has to upload the client to the phone prior to using it.

ABORT SKIP RETRY

SKIP

RETRY

RETRY

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.

Connection Failure - Cannot Read Phonebook

SM-S9080 Galaxy S22 Ultra (USB cable 170 or Original Cable):
Cannot connect to device (13)
SM-S9080 Galaxy S22 Ultra:
If any prompt messages display on the device, press Allow or Yes
1. To enable the Developer options, go to Menu (Apps) $ ightarrow$ Settings $ ightarrow$ About phone $ ightarrow$ tap the "Build number" 7 times until they are enabled.
2. Go to Menu (Apps) \rightarrow Settings \rightarrow Developer options \rightarrow select check boxes "USB debugging" and "Stay awake".
To enable multimedia transfer, please set the following:
When the device is connected, press and hold the status bar, then slide your finger downward:
select Transfer files on the phone
also set:
Menu (Apps) $ ightarrow$ Settings $ ightarrow$ Lock screen $ ightarrow$ Select screen lock $ ightarrow$ select "None".
This phone needs a client in order to communicate with the application.
The application has to upload the client to the phone prior to using it.

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

ABORT

Calendar read failed

SM-S9080 Galaxy S22 Ultra (USB cable 170 or Original Cable): Cannot connect to device SM-S9080 Galaxy S22 Ultra: If any prompt messages display on the device, press Allow or Yes 1. To enable the Developer options, go to Menu (Apps) \rightarrow Settings \rightarrow About phone \rightarrow tap the "Build number" 7 times until they are enabled. 2. Go to Menu (Apps) \rightarrow Settings \rightarrow Developer options \rightarrow select check boxes "USB debugging" and "Stay awake". To enable multimedia transfer, please set the following: When the device is connected, press and hold the status bar, then slide your finger downward: select Transfer files on the phone also set: Menu (Apps) \rightarrow Settings \rightarrow Lock screen \rightarrow Select screen lock \rightarrow select "None". This phone needs a client in order to communicate with the application. The application has to upload the client to the phone prior to using it. ABORT SKIP RE

Soluciones simples, accesibles y confiables



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.

SMS Read Failed

SM-S9080 Galaxy S22 Ultra (USB cable 170 or Original Cable): Cannot connect to target (13) SM-S9080 Galaxy S22 Ultra: If any prompt messages display on the device, press Allow or Yes 1. To enable the Developer options, go to Menu (Apps) \rightarrow Settings \rightarrow About phone \rightarrow tap the "Build number" 7 times until they are enabled. 2. Go to Menu (Apps) \rightarrow Settings \rightarrow Developer options \rightarrow select check boxes "USB debugging" and "Stay awake". To enable multimedia transfer, please set the following: When the device is connected, press and hold the status bar, then slide your finger downward: select Transfer files on the phone also set: Menu (Apps) \rightarrow Settings \rightarrow Lock screen \rightarrow Select screen lock \rightarrow select "None". This phone needs a client in order to communicate with the application. The application has to upload the client to the phone prior to using it. ABORT SKIP RETRY

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.

MMS read failed

SM-S9080 Galaxy S22 Ultra (USB cable 170 or Original Cable): Cannot connect to target (13) SM-S9080 Galaxy S22 Ultra: If any prompt messages display on the device, press Allow or Yes 1. To enable the Developer options, go to Menu (Apps) \rightarrow Settings \rightarrow About phone \rightarrow tap the "Build number" 7 times until they are enabled. 2. Go to Menu (Apps) \rightarrow Settings \rightarrow Developer options \rightarrow select check boxes "USB debugging" and "Stay awake". To enable multimedia transfer, please set the following: When the device is connected, press and hold the status bar, then slide your finger downward: select Transfer files on the phone also set: Menu (Apps) \rightarrow Settings \rightarrow Lock screen \rightarrow Select screen lock \rightarrow select "None". This phone needs a client in order to communicate with the application. The application has to upload the client to the phone prior to using it. ABORT SKIP RETRY

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

Cannot connect to device

SM-S9080 Galaxy S22 Ultra (USB cable 170 or Original Cable):

Connection to Source failed! Make sure Source is attached and ready! (32) SM-S9080 Galaxy S22 Ultra:

If any prompt messages display on the device, press Allow or Yes

1. To enable the Developer options, go to Menu (Apps) \rightarrow Settings \rightarrow About phone \rightarrow tap the "Build number" 7 times until they are enabled.

2. Go to Menu (Apps) \rightarrow Settings \rightarrow Developer options \rightarrow select check boxes "USB debugging" and "Stay awake".

To enable multimedia transfer, please set the following:

When the device is connected, press and hold the status bar, then slide your finger downward:

select Transfer files on the phone

also set:

 $\mathsf{Menu}\ (\mathsf{Apps}) \rightarrow \mathsf{Settings} \rightarrow \mathsf{Lock}\ \mathsf{screen} \rightarrow \mathsf{Select}\ \mathsf{screen}\ \mathsf{lock} \rightarrow \mathsf{select}\ "\mathsf{None"}.$

This phone needs a client in order to communicate with the application.

The application has to upload the client to the phone prior to using it.

ABORT	SKIP	RETRY
-------	------	-------

Soluciones simples, accesibles y confiables



SELECT CONTENT TYPE			⊙ ≡
Samsung GSM SM-S9 USB cable 170 or Origina	080 Galaxy S22 Ultra I Cable		
🕝 Extract from			
Device	SIM		
Choose data types to e	extract		All
ନ୍ଦ୍ରି sms 🔺	[÷ ммs 🔒	🕄 Calendar 🔒	Pictures
f Audio/Music	🗈 Videos 🛕	Pringtones	🗐 Documents 🔒
🗄 Archives			E Browsing Data
	IIII Files		
		В	ACK NEXT

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

EXTRACTION SUN	IMARY			?	=
Extraction aborte	d				
A Contacts	SKIPPED	ନ୍ଦ୍ରି sms	SKIPPED		
டு MMS	SKIPPED	Calendar	SKIPPED		
Pictures	SKIPPED	Ja Audio/Music	SKIPPED		
🔛 Videos	SKIPPED	Ringtones	NOT SELECTED		
🗐 Documents	SKIPPED	Archives	SKIPPED		
🚖 Email	NOT SUPPORTED	<i>Д</i> , ім	NOT SUPPORTED		
کي Call Logs	UNSUCCESSFUL	O Locations	UNSUCCESSFUL		



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.		
 Power on the phone and wait until it's fully booted * Only unlocked phones are supported. 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 p Uncheck the "Verify apps" setting, located in Menu (Apps) → Settings (More) → Security and confirm any pop-up that appears during the start of To enable the Developer options, go to Menu (Apps) → Settings (More) → About (Software information) → More, and tap the "Build numb 	rocedure: the transaction. er" 7 times until they are en	abled.
	ABORT	RETRY

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.



Información Legal: ©2017 NUGA SYS S.A. de C.V. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, fotocopiada, almacenada en un sistema de recuperación de datos o transmitida sin el consentimiento expreso y por escrito del editor. NUGA SYS A.S. de C.V. No hace representaciones o garantías con respecto al contenido o uso de esta documentación, y específicamente renuncia a cualquier garantía expresa o implícita de comerciabilidad o adecuación para un fin determinado. Además, NUGA SYS S.A. de C.V. se reserva el derecho de revisar esta publicación y realizar cambios en su contenido, en cualquier momento, sin obligación de notificar a ninguna persona o entidad de tales revisiones o cambios.

Además, NUGA SYS S.A. de C.V. no hace representaciones o garantías con respecto a ningún software, y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Además, NUGA SYS S.A. de C.V. se reserva el derecho a realizar cambios en cualquiera de todas las partes del documento, en cualquier momento, sin obligación de notificar a ninguna persona o entidad de tales cambios. Se prohíbe exportar o reexportar este producto en violación de cualquier ley o regulación aplicable, incluyendo, sin limitación, regulaciones de exportación de México o las leyes del país en que reside.

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

Un símbolo de marca comercial (®, TM, etc.) indica una marca comercial de NUGA SYS S.A. de C.V. Con pocas excepciones, y salvo aquellas anotadas de otra manera, todos los nombres de productos de terceros se escriben en mayúsculas y de la misma manera el propietario escribe y capitaliza el nombre de su producto. Marcas comerciales de terceros y derechos de autor son propiedad de los titulares de marcas comerciales y derechos de autor. NUGA SYS S.A. de C.V. no asumirá ninguna responsabilidad para la función o el funcionamiento de productos de terceras partes.

Reconocimiento de terceros:

Cellebrite, Shutterstock, Phone Scoop, Apple, Microsoft, Android, BlackBerry, brew, Samsung, Nokia, Eraser, HDDGuru.



Documentos Confidenciales: NUGA SYS S.A. de C.V. Todos los derechos Reservados