

Práctica 10: Forense Móvil

Nombre: Juan Monserrat González García **Fecha:** 15/02/2020

1. OBJETIVO:

El participante aprenderá la extracción forense en un dispositivo celular, eso nos permitirá saber información que creíamos ya no existía con dos herramientas muy sencillas de utilizar y que son legalmente permitidas ante un juicio.

2. INTRODUCCIÓN:

Hoy en día el uso de los dispositivos móviles celulares se vuelve cada vez más común y es por eso que debemos aprender la extracción de la información de manera segura con técnicas forense.

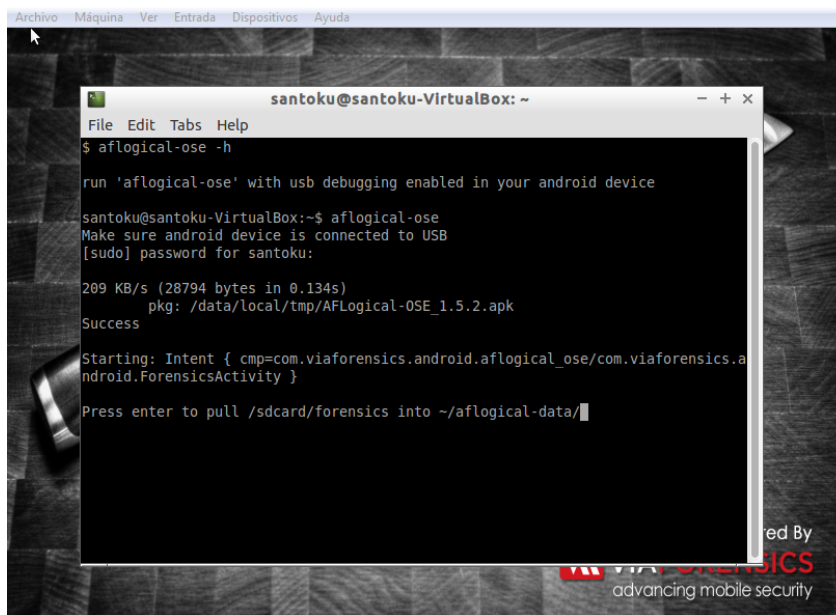
La preparación es un componente clave para responder a cualquier tipo de incidente. Parte de ese paso implica la creación de un entorno que contiene todas las herramientas que el primer respondedor ante un incidente móvil podría necesitar para responder adecuadamente a una situación. Esta práctica proporcionará las herramientas necesarias para proporcionar respuesta a incidentes en un teléfono móvil. Se enfoca al uso de software libre y / o de código abierto.

3. MATERIAL:

- Kali Linux o Santoku.
- VirtualBox
- Cable USB
- Celular con S.O. Android.
- Gnumeric

4. DESARROLLO:

- Si los prefieres puedes descargar Santoku¹ .iso ó .ova ó utilizar la máquina virtual con Kali Linux he instalar el paquete de AF Logical OSE².
- Habilitar el modo depuración en el celular revisa en internet como activarlo en el tuyo.
- Conectar el dispositivo a la USB y después agregarlo a la máquina virtual, de Santoku o Kali Linux, asegurando su montaje.
- Inicie la aplicación AF Logical OSE, en ella podrán ejecutar la instrucción \$aflogical-ose.



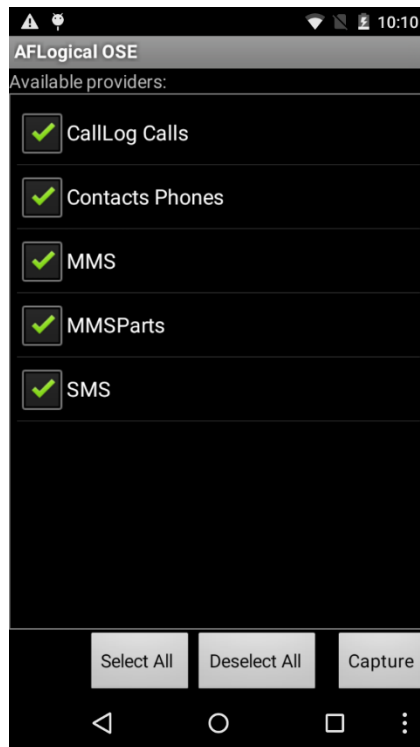
```
santoku@ santoku-VirtualBox: ~  
File Edit Tabs Help  
$ aflogical-ose -h  
  
run 'aflogical-ose' with usb debugging enabled in your android device  
  
santoku@ santoku-VirtualBox:~$ aflogical-ose  
Make sure android device is connected to USB  
[sudo] password for santoku:  
  
209 KB/s (28794 bytes in 0.134s)  
pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk  
Success  
  
Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a  
ndroid.ForensicsActivity }  
  
Press enter to pull /sdcard/forensics into ~/aflogical-data/
```

- En el teléfono aparecerá un mensaje de permiso, debemos aceptarlo para poder continuar de lo contrario no podremos entrar.
- Ahora manejaremos todo desde el celular dándole permiso a todo lo que queremos extraer del celular y comenzara la extracción

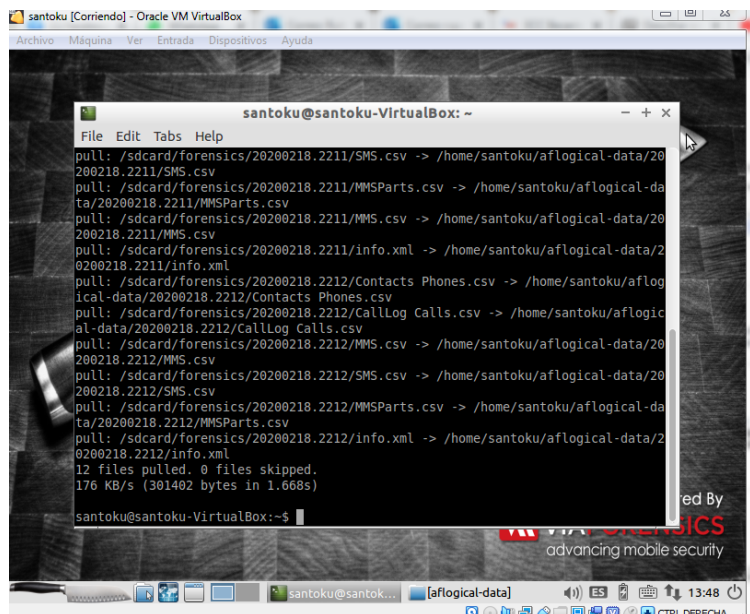
¹ <https://santoku-linux.com/download/>

² <https://github.com/nowsecure/android-forensics>

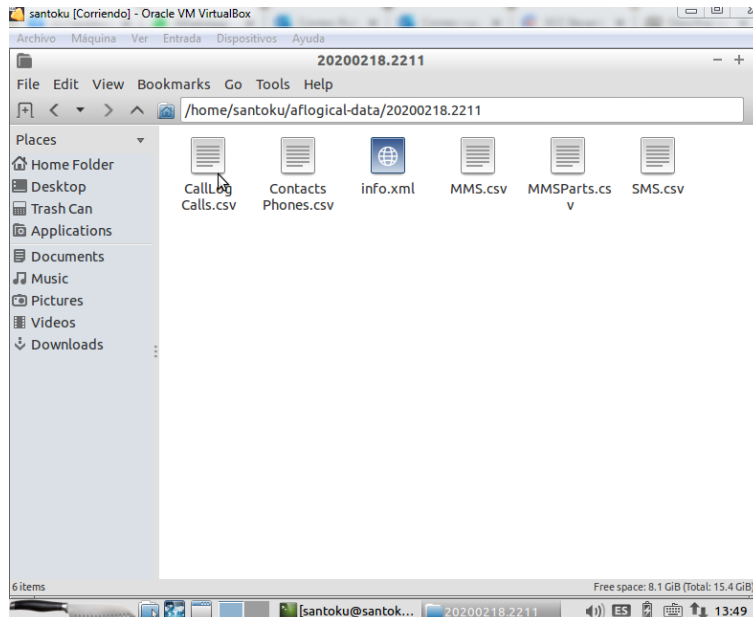
Aquí seleccionamos lo que queremos que se extraiga del celular.



Y enseguida dentro del programa hace la extracción de datos.



- g. La carpeta en donde se realizará el respaldo regularmente es en santoku
“/home/Santoku/aflogicaldata/...”, donde contendrá archivo con extensión
.CSV



- h.
i. ¿Qué es la extensión csv?

Esta extensión significa "valores separados por comas" debido a que los datos de estos archivos CSV son detalles dividido por comas en conjuntos particulares de información. Estas piezas de datos se pueden introducir los usuarios de hojas de cálculo y edición de texto de aplicaciones integradas con soporte para la creación y modificación de documentos CSV. Filas base de datos independientes están representados por cada línea de texto que se almacena en un archivo CSV. Estas filas de bases de datos se implementan con uno o más campos de datos, y estos se dividen por comas.

- j. Estamos listos para la investigación de los archivos con el programa Gnumeric que nos mostrara las llamadas realizadas de ese celular.



santoku [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

*CallLog Calls.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

Sans 10 a a a

B1 number

	B	C	D	E	F	G	H	I	J
	number	date	duration	type	new	name	number	numberlabel	
1	4.64E+09	1492357841260	20	2	0	Mama	2		
2	4.64E+09	1492369518382	0	2	0	Mama	2		
3	4.65E+09	1492441743501	11	1	0		0		
4	4.64E+09	1492482932270	29	2	0	Mama	2		
5	4.64E+09	1492528140556	91	2	0	Cinthia	2		
6	1.8E+10	1492541688574	165	2	0		0		
7	4.65E+09	1492546676848	7	1	0		0		
8	4.65E+09	1492546702793	19	1	0		0		
9	4.64E+09	1492556701154	31	2	0	Mama	2		
10	4.64E+09	1492558519556	29	1	0	Paola	2		
11	4.65E+09	1492566681901	38	1	0		0		
12	4.64E+09	1492628291391	14	2	0	Paola	2		
13	4.64E+09	1492632718572	19	2	0	Mama	2		
14	4.64E+09	1492633829701	21	2	0	Mama	2		
15	4.64E+09	1492634674721	0	2	0	Mama	2		
16	4.64E+09	1492651305765	0	3	0	Paola	2		
17									

CallLog Calls.csv Sum = 0

CallLog Calls.csv (15.4 KiB) CSV document

Free space: 15.4 GiB (Total: 15.4 GiB)

2020... SMS.c... *CallL... 22:48

santoku [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

20200218.2211

File Edit View Bookmarks Go Tools Help

SMS.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

Sans 10 a a a

A1 _id

	A	B	C	D	E	F
	id	thread_id	address	person	date	date_sent
1	58	42	UNOTV.COM		1534809172627	1534805547000
2	57	42	UNOTV.COM		1534725916141	1534725913000
3	56	26	Telcel		1534656803332	1534656800000
4	55	26	Telcel		1534650794601	1534650790000
5	54	42	UNOTV.COM		1534638101185	1534638098000
6	53	1	45578		1534635713581	1534635709000
7	52	26	Telcel		1534624907584	1534624905000
8	51	42	UNOTV.COM		153455571909	1534555567000
9	50	42	UNOTV.COM		1534553713516	1534553708000
10	49	51	4641194953		1534477051305	0
11	48	42	UNOTV.COM		1534467361854	1534467358000
12						

SMS.csv Sum = 0

"SMS.csv" (12.8 KiB) CSV document

Free space: 8.1 GiB (Total: 15.4 GiB)

san... 20... *Ca... [Co... SM... 23:30

5. CONCLUSIONES:

Para esta práctica muy interesante del cómputo forense, me agrada que pudiéramos explorar un celular para poderle extraerle los datos y observar la información que maneja este dispositivo.

Hoy en día es muy fácil poder acceder a datos personales, desde el acceso a cosas sencillas como a cuentas de banco importantes, poder hackear a un apersona es una tarea no muy fácil pero que no es realizada por personas honestas, el querer hacerle daño o querer invadir su privacidad es además de un delito una situación muy grave, el clonar tarjetas, el clonar teléfonos, el extraer información por diferentes medios está al alcance de todos, es importante saber para qu se utiliza y de esta manera proteger nuestros archivos e información, no con el afán de hacer lo mismo sino de protegernos de estas personas, el hackeo es una práctica muy utilizada hoy en día así que nos compete estar a la vanguardia para proteger nuestra información incluso en situaciones donde los componentes físicos ya parecen no funcionar, ahí es donde también puede haber información valiosa que los hackers pueden obtener.