UNIVERSIDAD NACIONAL AUTONÓNOMA DE NICARAGUA, MANAGUA
UNAN-MANAGUA
CONGRESO DE LA RED DE COMPUTACIÓN PARA EL DESARROLLO, COMPDES 2014
Del 23 al 25 de julio de 2014
"Investigando e Innovando para el Desarrollo Tecnológico"

Benchmarking de Herramientas Forenses para Móviles

Presentado por : Elmer Arturo Carballo Ruiz
Pedro Eliseo Peñate.

Objetivos

Objetivo General

Comparar tres herramientas para el uso de un análisis forense informático en tecnologías móviles

Objetivos Específicos

- Investigar herramientas a nivel de open source para el análisis forense de dispositivos móviles.
- Establecer una comparación en base a criterios técnicos sobre las herramientas forenses para móviles.

Alcance y Limitaciones

- **Alcance**
- Este estudio estaría basado sólo en el uso de herramientas forenses open source para dispositivos móviles sobre plataforma Android, y lo que se pretende es brindar una comparación de las ventajas y desventajas entre ellas y su aplicabilidad en el análisis forense.

- **Limitaciones**
- El proyecto se ha delimitado a la extracción de datos de dispositivos Android con herramientas Open Source de Adquisición Lógica.
- Una herramienta de adquisición requiere que la versión de Android sea desde la 1.5 hasta la 4.1 en el caso de la otra herramienta evaluada la versión de Android requerida es 2.x.

Marco Conceptual

- Demanda de consumo de dispositivos móviles en los que muchos fabricantes han posicionado sus marcas tomando buena parte de este mercado. Entre las 5 marcas mayormente comercializadas a finales del 2012 se encuentran: Samsung, Nokia y Apple

Top Five Worldwide Total Mobile Phone Vendors, Q4 2012			
Rank	Manufacturer	Gartner[22]	IDC[23]
1	Samsung	22.7%	23.0%
2	Nokia	18.0%	17.9%
3	Apple	9.2%	9.9%
4	ZTE	3.4%	3.6%
5	LG	3.2%	-
5	Huawei	-	3.3%
	Others	43.5%	42.3%

Tabla 1. Top Five Worldwide Total Mobile Phone Vendors (Wikipedia The Free Encyclopedia, 2014)

Sistema de Archivos de Android

- Android utiliza los sistemas de archivo EXT, FAT32 y YAFFS2 tanto para la inicialización como para el almacenamiento de archivos. Aunque recientemente el sistema de archivos de Android que se utiliza más en estos dispositivos móviles es EXT4, debido a la capacidad de los procesadores de varios núcleos y el uso de tarjetas de memoria.

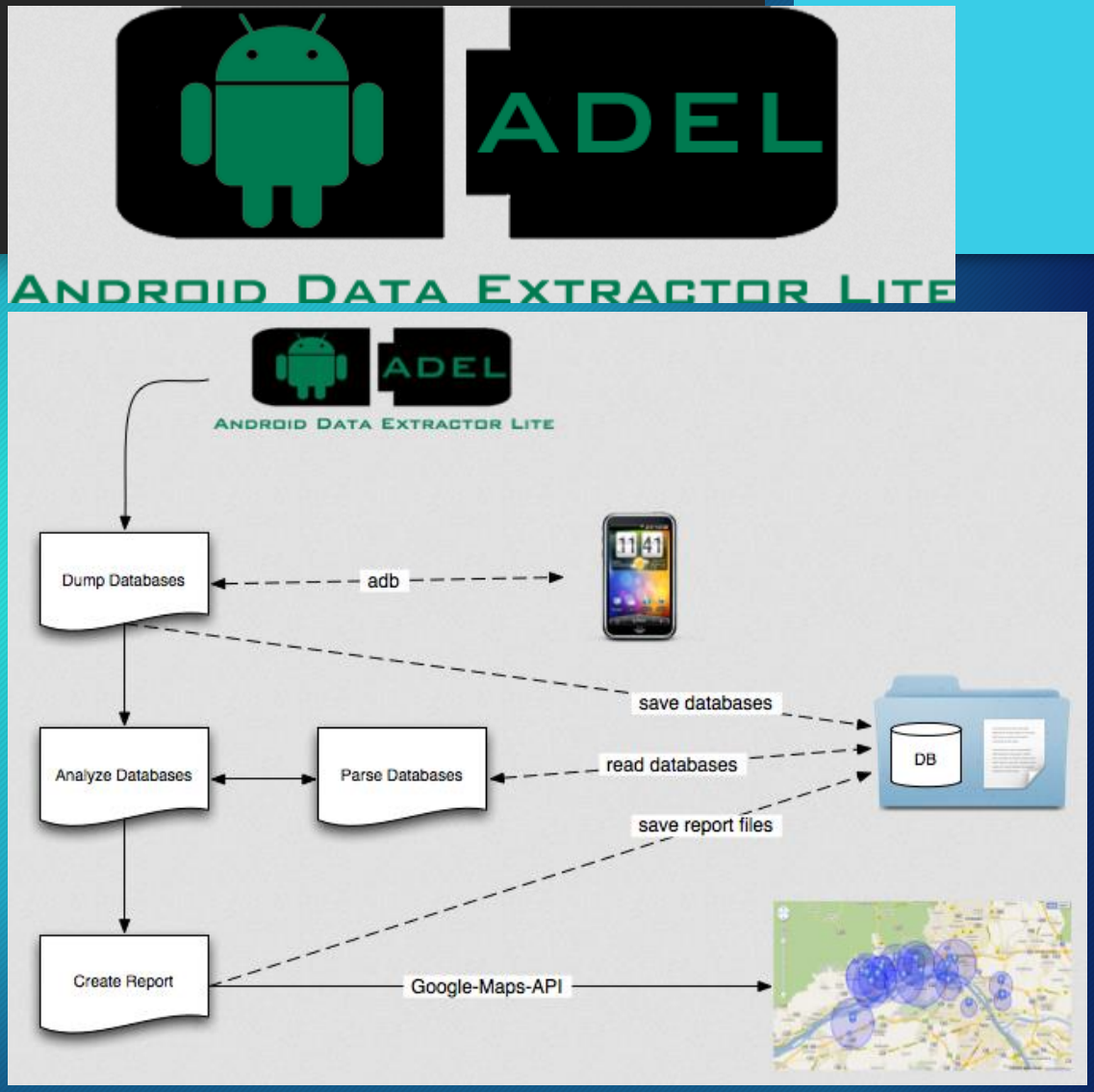
Path	Name	File System	Mount point	Description
/dev/mtd/mtd0	pds	yaffs2	/config	Configuration data
/dev/mtd/mtd1	misc	–	N/A	Memory Partitioning data
/dev/mtd/mtd2	boot	bootimg	N/A	Bootable (typical boot)
/dev/mtd/mtd3	recovery	bootimg	N/A	Bootable (recovery mode)
/dev/mtd/mtd4	system	yaffs2	/system	System files, Applications, Vendor additions, Read-Only,
/dev/mtd/mtd5	cache	yaffs2	/cache	Cache Files
/dev/mtd/mtd6	user data	yaffs2	/data	User data (Applications)
/dev/mtd/mtd7	kpanic	–	N/A	Crash Log

Herramientas Forenses

- El nombre de Santoku, se traduce libremente como “tres virtudes” o “tres usos” (Santoku) y es un homenaje a un cuchillo japonés multiuso. Santoku está dedicado a los forenses móviles, análisis y seguridad empaquetados en un formato fácil de usar en una plataforma de código abierto

ADEL

- **ADEL** que se entiende como una abreviatura de “ **Android Data Extractor Lite** ”.
- El programa está desarrollado en Python (Lakhoua, 2013). ADEL interactúa con los dispositivos utilizando el Android Software Development Kit (SDK de Android) y especialmente el demonio adb para volcar los archivos de base de datos en el equipo del investigador



OSAF

- OSAF (Open Source Android Forensics) (OSAF Community, 2012) Es un proyecto de software libre para Análisis Forense de Androids, su objetivo fue crear un marco unificado para análisis forense de Androids centrándose principalmente en el malware dentro de las aplicaciones de Android.
- Su enfoque en primer lugar, la creación de una compilación fuente totalmente abierta de la ciencia forense y análisis de malware de software en la forma de Toolkit OSAF. En segundo lugar, el objetivo era crear un proceso estandarizado para el uso del kit de herramientas y un conjunto de mejores prácticas para el análisis de las aplicaciones de Android

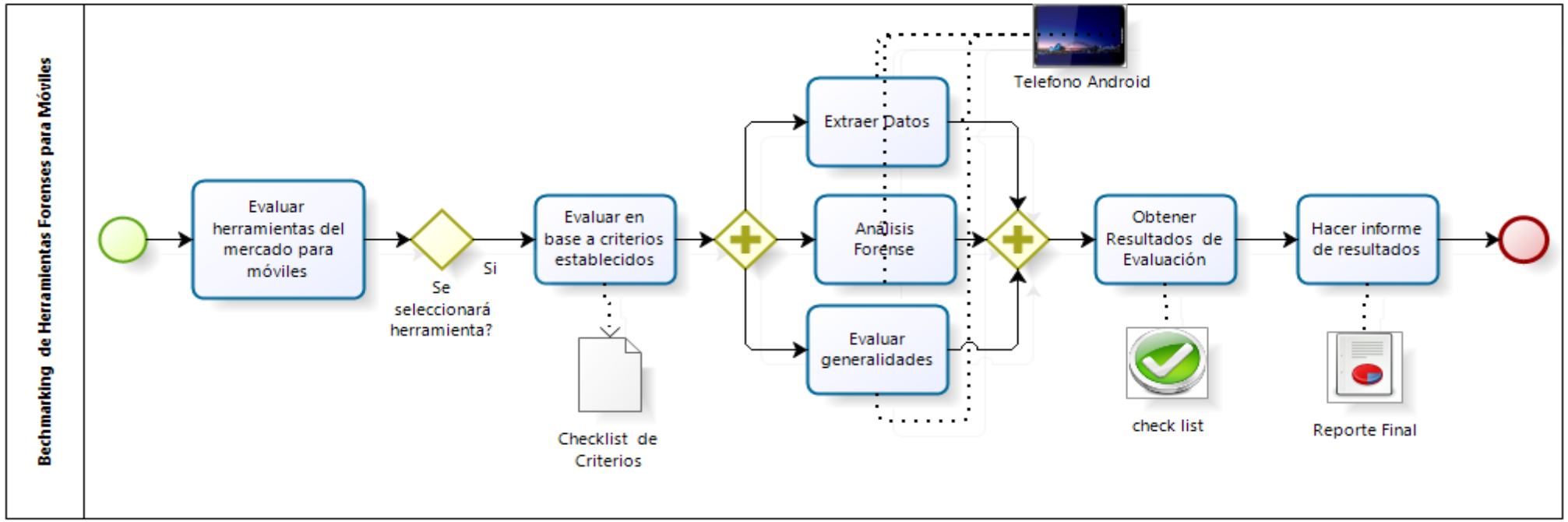
AF Logical

- AFLogical es una herramienta de extracción lógica para el análisis forense de Androids, fue lanzado en diciembre de 2011, desarrollado por viaForensics y ahora está alojado en GitHub.
- AFLogical realiza una adquisición lógica de cualquier dispositivo Android con Android 1.5 o posterior. (ViaForensics, 2014) Los datos extraídos se guardan en la tarjeta SD del examinador en formato csv (valores separados por comas), que se puede importar fácilmente en un software de hoja de cálculo, por lo que es fácil de extraer y analizar los datos de Android
- Esta herramienta puede encontrarse dentro de la suite de OSAF y SANTOKU

Escenario

- Para realizar el benchmarking se tomaran diferentes teléfonos celulares reales con sistema Android debido a que una de las herramientas es necesario que este en modo recovery y dentro del modo se puedan montar algunas carpetas principales del sistema de archivos de Android, para el caso OSAF y Santoku no es necesario que el dispositivo ingrese en modo recovery debido a que AFLogical se instala en sistema Android del dispositivo

PROCESO DE EVALUACIÓN DE LAS HERRAMIENTAS SANTOKU, ADEL Y OSAF



Powered by bizagi Modeler

Resultados

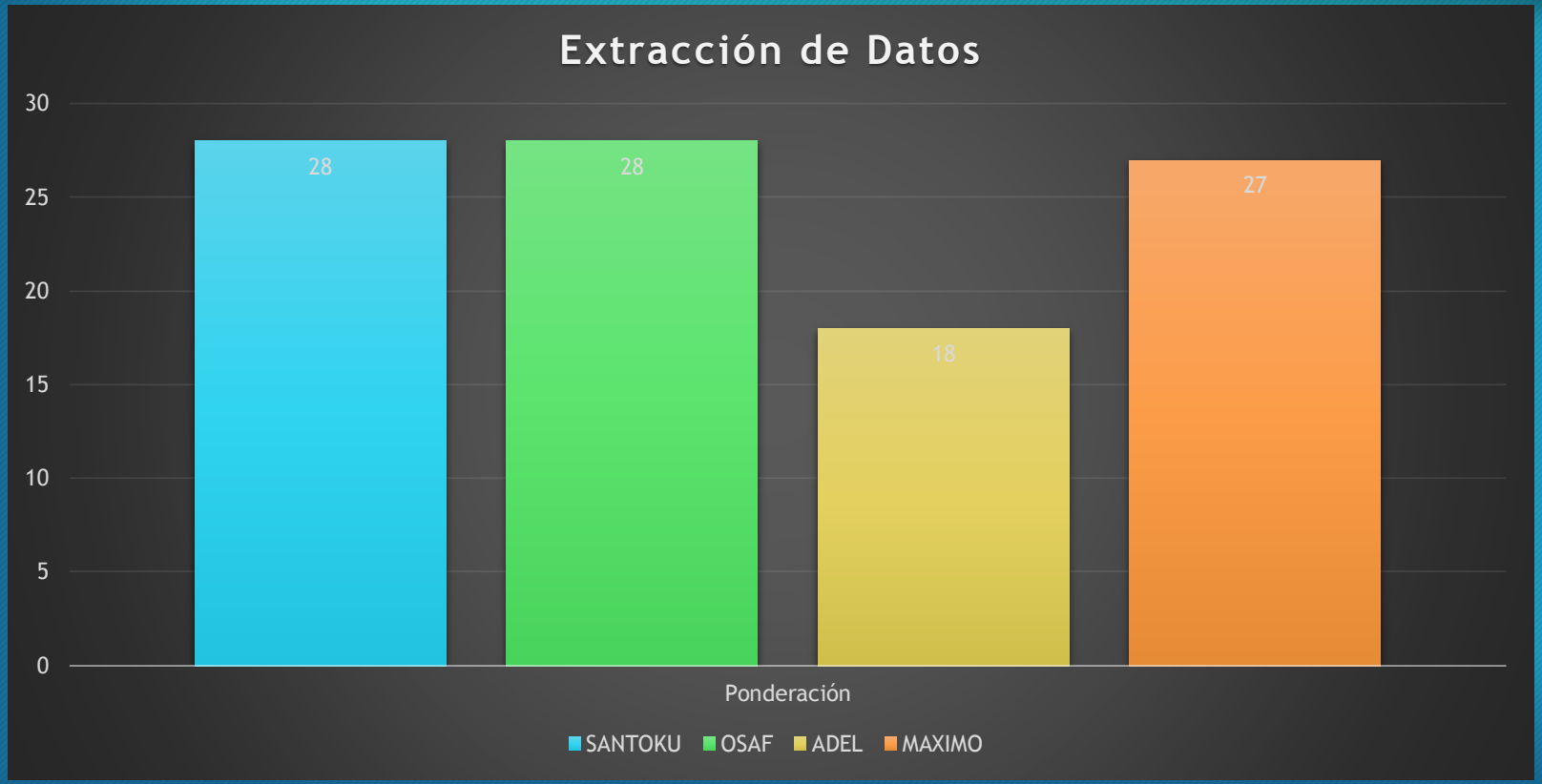
RESULTADO									
CATEGORIA :	ANALISIS FORENSE								
Criterio de Evaluación	SANTOKU			OSAF			ADEL		
	ALTA	MODERADA	BAJA	ALTA	MODERADA	BAJA	ALTA	MODERADA	BAJA
Relevancia	2			2			3		
Confiabilidad	3			3			3		
Suficiencia	1			1			2		
TOTAL	6			6			8		

Resultados

RESULTADO									
CATEGORIA :	GENERALIDADES								
Criterio de Evaluación[i]	SANTOKU			OSAF			ADEL		
	ALTA	MODERADA	BAJA	ALTA	MODERADA	BAJA	ALTA	MODERADA	BAJA
Nivel de Experiencia		1			1			2	
Navegabilidad		3			2			1	
Usabilidad		2			2			2	
Multiplataforma		1			1			2	
Estabilidad		3			3			3	
Compatibilidad		3			3			3	
Interoperabilidad		3			3			1	
Facilidad de Instalación		2			2			1	
Estabilidad		3			3			3	
TOTAL		21			20			18	

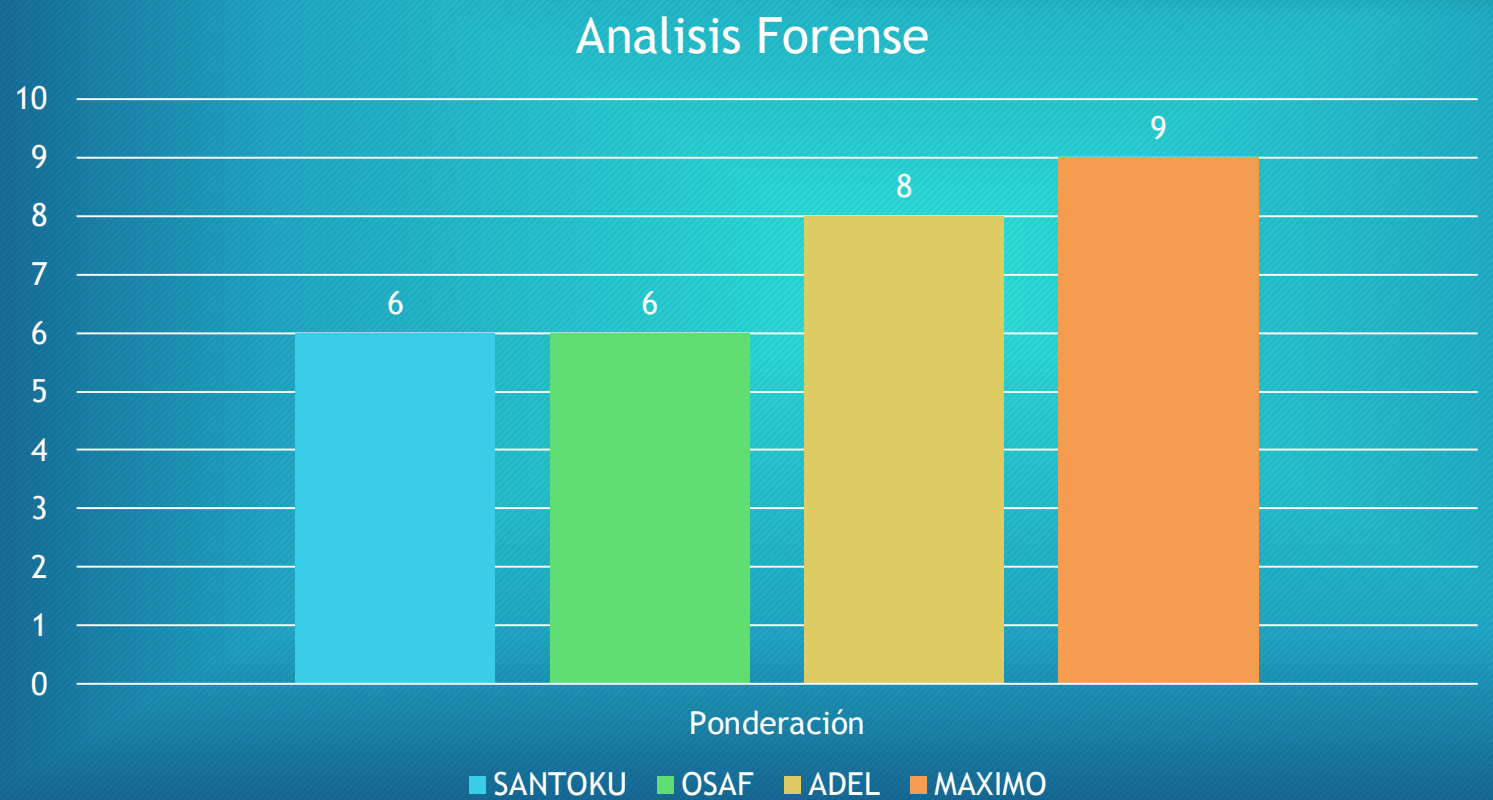
[i] Criterios según ISO/IEC 2500 criterios de calidad.

Resultados



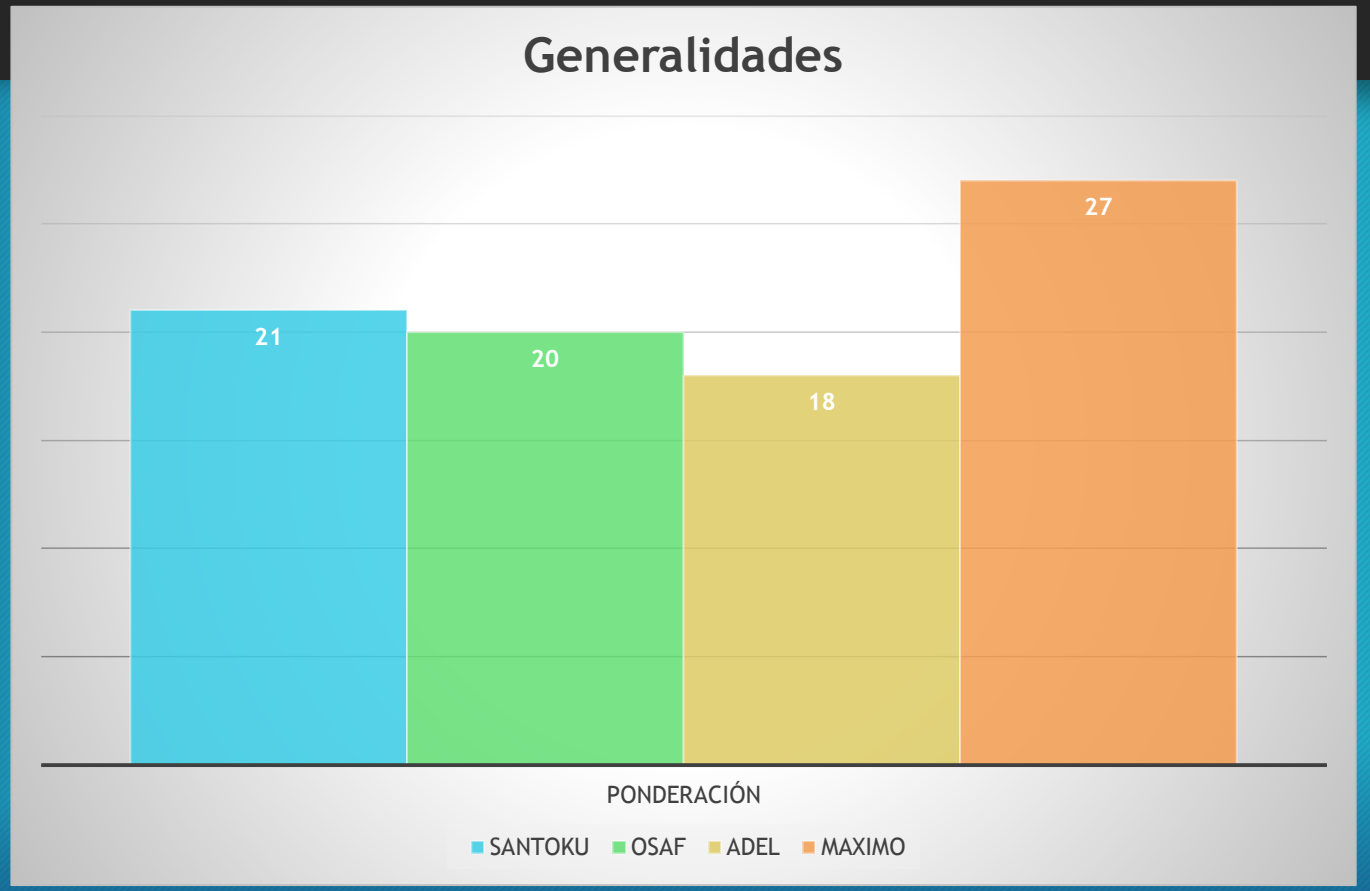
Herramienta	SANTOKU	OSAF	ADEL	MAXIMO
Ponderación	28	28	18	27

Resultados



Herramienta	SANTOKU	OSAF	ADEL	MAXIMO
Ponderación	6	6	8	9

Resultados



Herramienta	SANTOKU	OSAF	ADEL	MAXIMO
Ponderación	21	20	18	27

Conclusiones

- Para poder elegir una herramienta de análisis forense es necesario tener bien definidas las necesidades para las que se va utilizar y los criterios que se busca evaluar, la mayoría de veces se utilizan dos o tres herramientas de análisis forense ya que de acuerdo a las necesidades de los casos que se presentan es necesario combinarlas.
- El análisis de forense de dispositivos móviles basado en sistema Android puede facilitarse o complicarse dependiendo de las características del dispositivo como si esta rooteado, si se pueda tener acceso a modos especiales como recovery, fastboot (carga de imagen de SO en RAM, las versiones del sistema Android, si el dispositivo está cifrado, si tiene seguridad de bloqueo de pantalla por PIN o patrón, etc. Para cada caso se debe de tener conocimiento de alguna herramienta que pueda apoyar al propósito de adquirir la información del sistema. Para el caso de las suites evaluadas existen varias herramientas que pueden servir al analista para lograr el objetivo de extraer, analizar y reportar la información de interés. Sobre esto la pericia, experiencia, comprensión del sistema Android del analista puede simplificar o complicar el análisis.

Conclusiones

- Una herramienta fundamental que es utilizada por las herramientas de adquisición de información evaluadas, es el Android Debug Bridge (ADB) que es una herramienta para desarrolladores para el sistema Android y que es parte SDK de Android. ADB sirve de puente de conexión entre el equipo del analista y el dispositivo Android analizado y así como también puede realizar volcados de información e instalación o cargar de programas o información en el dispositivo Android
- Consideramos que el análisis forense a dispositivos móviles hoy día es un tema de gran importancia que tanto las empresas, así como las instituciones que persiguen el delito deberían capacitar a su personal de seguridad o TI para poder realizar este tipo de análisis, ya que en los dispositivos móviles se encuentra mucha información que puede involucrar a una persona en un delito, relacionarlo con personas delictivas o en un procedimiento no adecuado.