DOCENTE : Gustavo Presman

MATERIA: Computer Forensics

EKOPARTY HACKADEMY

Gustavo Daniel Presman

gpresman@gmail.com

@gpresman

- Ingeniero Electrónico , **UBA** 1987
- Master en Tecnologías de la Información en el programa **GADEX** 2010/2011
- Certificado en Informática Forense **EnCE** , **ACE** , **CCE** , **NPFA** , **FCA , MFCE, CNSS**
- Miembro del capítulo sudamericano **HTCIA**
- Profesor titular de Análisis Forense y Delitos Informáticos en la Maestría de Seguridad Informática **UBA** Profesor titular de la Especialización en Derecho Informático de la **UBA**
- Miembro de numerosos comités académicos de eventos de Seguridad Informática

DISCLAIMER :

- **No soy abogado**
- **Soy entrenador oficial de las herramientas EnCase y AXIOM**

EKOPARTY HACKADEMY

TEMARIO:

- ✓G1: Introducción a la Informatica Forense
- ✓G2: Metodología para la recolección de evidencia digital
- ✓G3: Extracción y preservación de evidencia digital de almacenamiento
- ✓G4: Practica de Imágenes forenses
- ✓G5 y G6: Introducción al análisis forense de evidencia digital

Clase sincrónica: Introducción al análisis forense de dispositivos móviles. Intercambios y Q&A . Análisis de casos

EKOPARTY HACKADEMY

Agenda

- Introducción al análisis forense de dispositivos móviles
- Limitaciones para peritar . Cifrado – Contramedidas de Seguridad- Evolución
- Fases del Análisis- Técnicas de extracción de dispositivos móviles
- Discusión abierta - Q&A

EKOPARTY HACKADEMY

OTRO DISCLAIMER

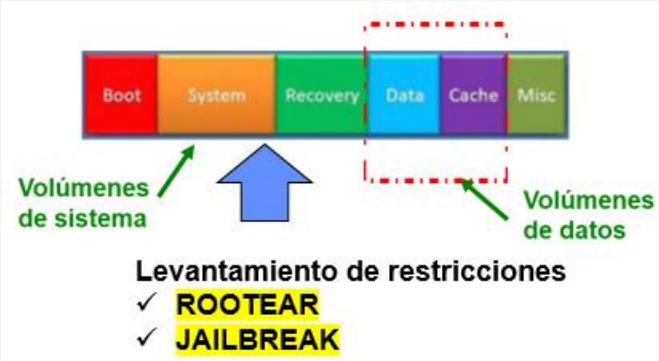
La evolución tecnológica de los dispositivos móviles es aun mas rápida que en otras tecnologías, por lo que algunos aspectos de los temas tratados pueden cambiar debido, entre otras a :

- **Cambios en la tecnología de almacenamiento**
- **Limitaciones del fabricante**
- **Medidas y contramedidas de seguridad**

EKOPARTY HACKADEMY

LIMITACIONES PARA PERITAR UN DISPOSITIVO MÓVIL

- ✓ Bloqueo del dispositivo
- ✓ Cifrado del contenido FDE Vs. FBE
- ✓ Restricción en el acceso a volúmenes de Sistema
- ✓ Cifrado de las aplicaciones
- ✓ Decodificación de los datos
- ✓ Volumen de almacenamiento
- ✓ Datos en la nube



Es la dificultad para acceder a la evidencia digital el desafío mayor ?

EKOPARTY HACKADEMY

LAS DOS BARRERAS

ACCESO FISICO AL DISPOSITIVO

ACCESO LOGICO A LAS APLICACIONES

<u>Barreras dinámicas:</u> Las técnicas de acceso y las aplicaciones cambian todo el tiempo

PUNTOS DE APOYO PARA DESCIFRAR

- ✓Debilidad del algoritmo
- ✓Vulnerabilidad del método o de la Implementación
- ✓Ataque de diccionario
- ✓Ataque de fuerza bruta

Susceptible a contramedidas

QUE ES UNA CONTRAMEDIDA DE SEGURIDAD ?

Es un mecanismo que ataca al proceso de descifrado por fuerza bruta ya sea:

- *Limitando el numero de intentos y wipeando o eliminando la clave privada interna*
- *Incrementando exponencialmente el tiempo de espera entre ingresos de clave*
- *Obligando a utilizar un servicio alternativo con diferentes credenciales de acceso*
- *Impidiendo la instalación de una cuenta (Gmail o Apple ID)*

EVOLUCION DEL CIFRADO EN CELULARES

1) Solo bloqueo
2) FDE por software
3) FDE por hardware
4) Inicio Seguro
5) FBE

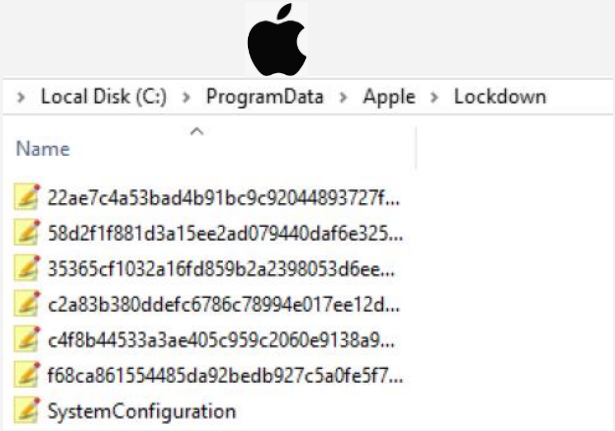
EKOPARTY HACKADEMY

COMO ACCEDER A UN CELULAR BLOQUEADO ?

Se requiere una vulnerabilidad o feature? que permita desbloquear el celular y eso depende de:

- Exploit conocido (que tan conocido?)
- Estado del teléfono

Depuración USB-ADB
GestureKey



Dispositivos de confianza

EKOPARTY HACKADEMY

FASES DEL ANÁLISIS FORENSE DE MÓVILES

Según La NIST 800-101, se recomienda separar el proceso de pericia en 4 grandes fases:

1. Preservación.
2. Adquisición.
3. Análisis.
4. Reportes.

EKOPARTY HACKADEMY

MODOS DE ADQUISICIÓN

Depende del estado del dispositivo

- **Bloqueado/Desbloqueado**
- **Nativo / Rooteado-Jailbreak**

✓ **FISICA : Basada en bloques de almacenamiento**

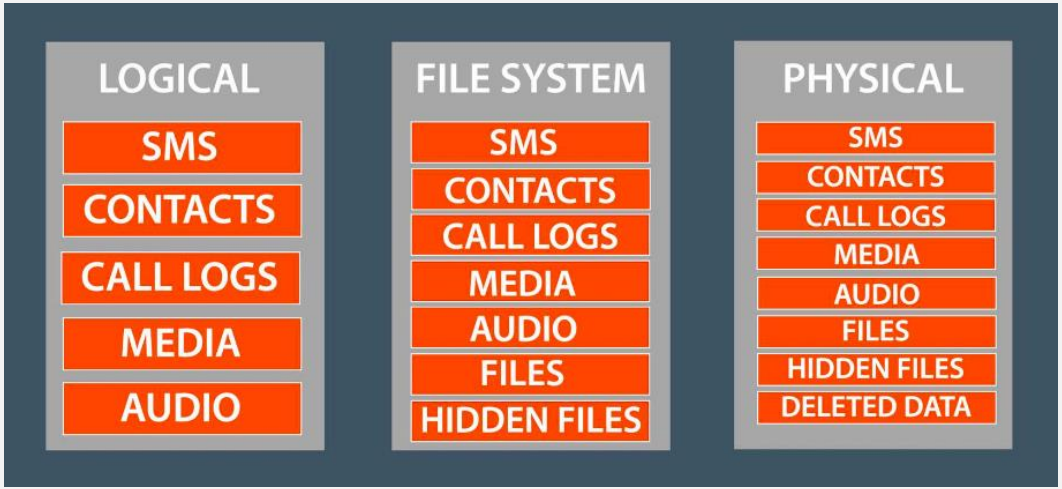
✓ **SISTEMA DE ARCHIVOS : Adquisición del Sistema de archivos**

✓ **LOGICA: Adquisición de objetos o copia de seguridad**

✓ **MANUAL**

EKOPARTY HACKADEMY

TIPOS DE EXTRACCIÓN FORENSE



EKOPARTY HACKADEMY

TÉCNICAS DE ADQUISICIÓN

Segun sea las adquisiciones que se puedan hacer, es el resultado que se puede obtener

Es importante tener presente los siguientes elementos antes de encarar o autorizar un tipo de adquisición:

- **Complejidad del proceso**
- **Dispositivos con pantalla / *touch* dañados**
- **Disponibilidad de recursos (HW/SW/Experticia)**
- **Irreversibilidad del proceso**
- **Riesgo de daño logico permanente (*black screen, bootloop*)**

EKOPARTY HACKADEMY

TECNICAS DE EXTRACCIÓN FORENSE

Extracción física

Extracción lógica y sistema de archivos

Extracción manual y lógica

VALIDEZ DEL PROCESO

La irreversibilidad del proceso exige

A la autoridad Judicial : Autorización en terminos del Código Procesal vigente (Riesgos Vs. beneficios)

Al perito : Extremar los cuidados y documentar, documentar, documentar, documentar, documentar

EKOPARTY HACKADEMY

EL CASO DEL TIRADOR DE SAN BERNARDINO

Apple niega al FBI acceso al iPhone del tirador de San Bernardino

Tim Cook rechaza la orden de una juez al considerar que es un "paso sin seguridad" de sus clientes

108

ROSA JIMÉNEZ CANO

San Francisco - 17 FEB 2016 - 23:13 CET

Finalmente, el FBI accedió al iPhone del terrorista de San Bernardino

Los investigadores del atentado lograron desbloquear el dispositivo móvil sin la ayuda de Apple, luego de que la compañía se negara a colaborar en el descifrado del aparato

28 de marzo de 2016

Compartir en Facebook

Compartir en Twitter

El FBI pagó casi un millón de dólares para desbloquear el iPhone del terrorista de San Bernardino

Matt Novak

5/08/17 11:06AM • Filed to: FBI

11.0K 9 2

Sections

The Washington Post

Democracy Dies in Darkness

Get one year for $29

Sign in

Tech Consumer Tech Future of Transportation Innovations Internet Culture Space Tech Policy Video Gaming

EXCLUSIVE

The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm.

Azimuth unlocked the iPhone at the center of an epic legal battle between the FBI and Apple. Now, Apple is suing the company co-founded by one of the hackers behind the unlock.

EKOPARTY HACKADEMY

Preguntas ?
Intercambios y Q&A

Ing. Gustavo Daniel Presman – MCP , EnCE , CCE, EnCI, ACE,NPFA, FCA, MCFE
ESTUDIO DE INFORMATICA FORENSE

gustavo@presman.com.ar
http://www.presman.com.ar
Linkedin: http://ar.linkedin.com/in/gpresman
@gpresman