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**

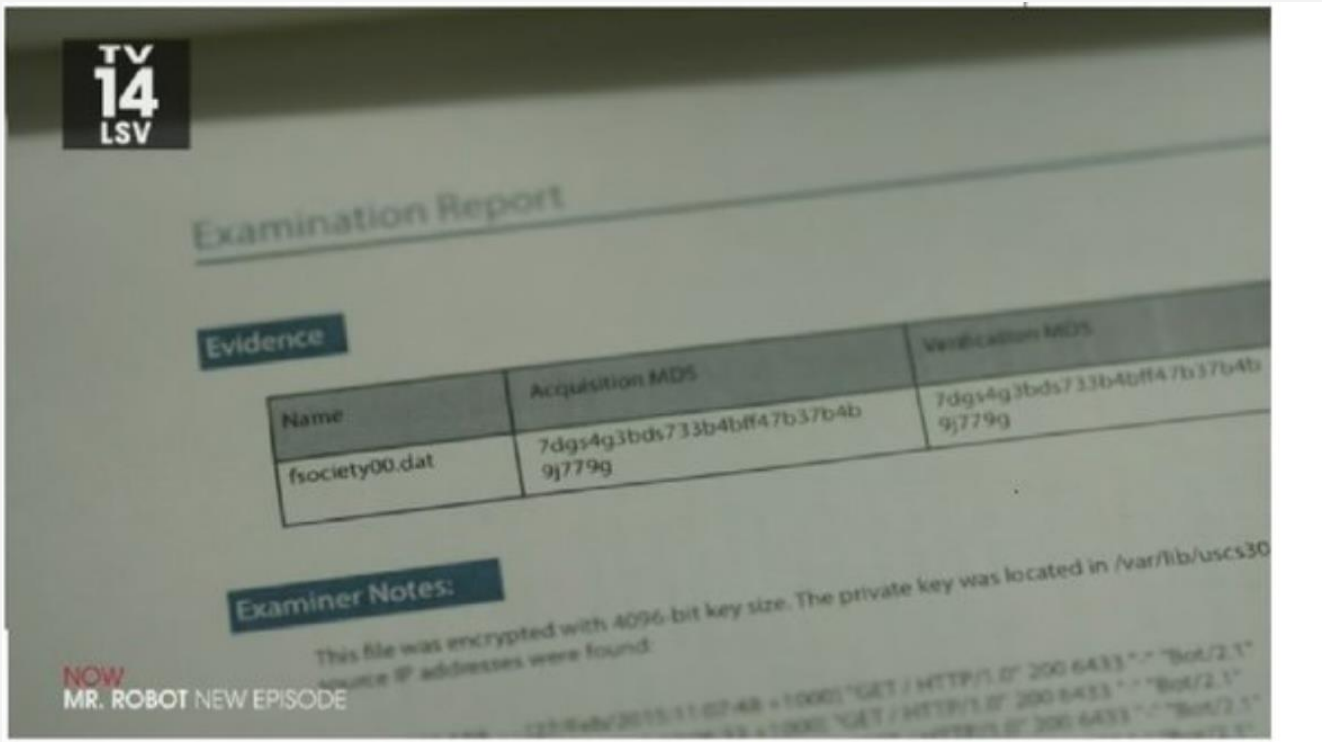
EKOPARTY HACKADEMY

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 . Analisis de casos

EKOPARTY HACKADEMY

ES LA INFORMATICA FORENSE LO QUE VEMOS EN TV ?



EKOPARTY HACKADEMY

ES LA INFORMATICA FORENSE LO QUE VEMOS EN TV ?

CONCEPTOS PRELIMINARES

INFORMATICA FORENSE

(Ciencia criminalistica)

=

INFORMATICA + BASE LEGAL

Actuación en:

- **AMBITO JUDICIAL → Perito Informático**
- **AMBITO CORPORATIVO → Analista Forense**

EKOPARTY HACKADEMY

ACTUACIÓN PERICIAL SEGÚN AMBITO

AMBITO JUDICIAL

- Mediante Requerimiento Judicial u Oficio del Juzgado
- Actuación acotada y definida con un cuestionario pericial
- Existen procedimientos y plazos procesales según fuero y jurisdiccion (códigos procesales)
- Derecho a percibir honorarios en el momento procesal oportuno

AMBITO EXTRAJUDICIAL

- Generado por un Encargo con el requirente
- La actuación se define en función de las necesidades del caso y el requirente
- Los plazos para la actuación vienen determinados por los intereses del requirente
- El encargo se enmarca en una relación comercial entre el perito y el requirente

El informe puede ser utilizado como parte de un proceso judicial

DEFINICION DE INFORMATICA FORENSE

" **Es la ciencia de adquirir , preservar , obtener y presentar datos que han sido procesados electronicamente y almacenados o transmitidos a través de un medio informático**"

*** Adaptada de : http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm**

EKOPARTY HACKADEMY

DEFINICION DE INFORMATICA FORENSE

" Es la ciencia de adquirir , preservar , obtener y presentar datos que han sido procesados electronicamente y **almacenados o transmitidos a través de un medio informático**"

EVIDENCIA DIGITAL

INVESTIGACION INFORMATICA

DELITOS CON TI Vs. DELITOS INFORMATICOS

- **Investigación Judicial** : Causas en todos los fueros (Civiles , comerciales , laborales , penales....) **PERITO JUDICIAL EN INFORMATICA**

- **Investigación Extra Judicial**: Investigación de seguros . Temas Corporativos : Comportamientos desleales . Espionaje Industrial . Auditorías Internas . Preparacion de casos .Preconstitución de prueba. **INVESTIGADOR O ANALISTA FORENSE INFORMATICO**

INVESTIGACION INFORMATICA

- **Investigación Judicial** : Reglas de buena práctica . Códigos Procesales ?

- **Investigación Corporativa**: Libre

CAMBIO DE ESCENARIO

CORPORATIVO A JUDICIAL

Normativa aplicable para el tratamiento de Evidencia Digital

BUENAS PRÁCTICAS / GUIAS

- Best Practices
- Protocolos

Organismos nacionales e internacionales principalmente LE

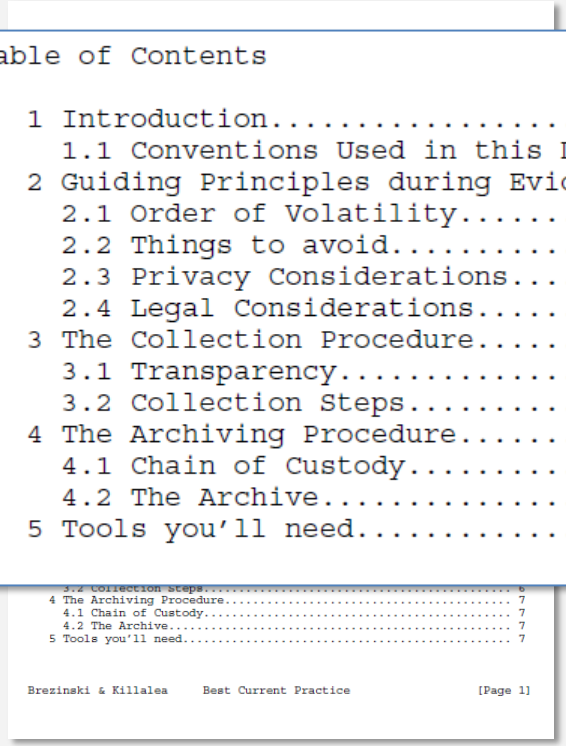
NORMAS

- *RFC 3227 - "Guidelines for evidence Collection and Archiving" (2002)*
- *ISO/IEC 27037:2012/2018 - "Guidelines for identification, collection, acquisition and preservation of digital evidence"*
- *ISO/IEC 27042:2015 – "Guidelines for the analysis and interpretation of digital evidence*

EKOPARTY HACKADEMY

RFC 3227

Table of Contents



EKOPARTY HACKADEMY

ISO 27037

ROLES

- DEFR
- **DFS**

PROCESOS

- METODOLOGICO
- AUDITABLE
- REPRODUCIBLE
- DEFENDIBLE

ROLES ISO 27037

DEFR ***: Digital Evidence Forensic Responder***

Individuo autorizado, entrenado y calificado para actuar en la escena del hecho con capacidad de recolección y adquisición de evidencia digital

DES*: Digital Evidence Specialist*

DEFR + Capacidades de Análisis

PROCESOS ISO 27037

Proceso metodológico

La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y obteniendo copias de respaldo (?) – Enmarcado en la normativa especifica

Proceso auditable

Los procedimientos y la documentación generada deben haber sido validados y basados en buenas prácticas, protocolos o normas

Proceso reproducible

Los métodos y procedimientos deben poder ser verificados y sostenidos científicamente

Proceso defendible

Las herramientas utilizadas deben de ser descriptas y validadas y el analista o perito debe acreditar conocimiento de las mismas y metodología empleada (*not push button Forensics*)