Forensics

Manuel García-Cervigón

Agenda

- Introducción
- Aspectos Legales
- Forensics Readiness
- Adquisición de datos
- Sistemas de Ficheros y análisis postmortem
  - FAT12
  - NTFS
  - Ext
- Análisis en vivo
- Análisis de Malware

Forensics

INTRODUCCIÓN

Introducción

- Conocimiento del sistema del archivos
- Conocimiento del entorno
- Conocimiento de vulnerabilidades
- Conocimiento de pentesting

- Ejemplos:
  - http://www.youtube.com/watch?v=WkrPlJcr8w0
  - http://www.youtube.com/watch?v=XUZqKQj4lok

Introducción

INVESTIGACION FORENSE
(des de el punto de vista LEGAL)

1. Preparación
2. Identificación
3. Adquisición
4. Agregación
5. Análisis
6. Seguimiento y presentación

Introducción

INVESTIGACION FORENSE

(des de el punto de vista TÉCNICO)

Introducción

INVESTIGACION FORENSE
(des de el punto de vista del ciclo de la seguridad)

1. Análisis de riesgos
2. Política de seguridad
3. Implantación
4. Monitorización
5. **Respuesta**

Introducción

- Un forense se basa en la investigación de un incidente de seguridad donde interviene información digital.

- Un incidente de seguridad es un evento adverso en el cual algún aspecto de la seguridad del ordenador puede estar amenazado: pérdida de confidencialidad o integridad de los datos, interrupción del sistema e interrupción o denegación del servicio disponible.

Introducción

- Antes: Chicos malos
- Ahora: Mafias
- Consecuencias:
  - 55.000 muestras NUEVAS de malware al día
  - Ataques sobre infrastructuras críticas
  - Ciberterrorismo

Introducción

Pre-Internet…

- **ARPANET** ((*Advanced Research Projects Agency Network*))
- **DARPA** (Defense Advanced Research Projects Agency), departameno de **defensa** de Estados Unidos.
- **Objetivo**: mantener a Estados Unidos como primer pais en desarrollo tecnológico y responder de esta forma a las crecientes investigaciones de la Union Sovietica (Sputnik fue lanzado el 4 de Octubre de 1957).
- En 1983 se implantó TCP/IP -un conjunto de protocolos desarrollados por Vinton Cerf y Robert Kahn- sobre la red de ARPANET

Introducción

Primer ataque…

- En 1988 existían unos 70.000 hosts interconectados y hasta el momento la seguridad no había sido un aspecto importante pero el 2 de Noviembre de 1988 aparece el GUSANO MORRIS.
- Creado por el estudiante predoctoral Robert T. Morris como experimento, el gusano usaba un defecto del sistema operativo Unix para reproducirse hasta bloquear el ordenador.
- **Las copias del virus llegaban a través del correo electrónico!**
- La fiscalía argumentó que el gusano "no se trató de un error, sino de un **ataque contra el gobierno de los Estados Unidos**".
- **RESULTADO**: Tres años de libertad condicional, una multa de 10.000 dólares y 400 horas de servicio as la comunidad.

Introducción

Organización...

- A raiz del gusano en Diciembre de 1988 se crea CERT Coordination Center (http://www.cert.org/) en la universidad Carnegie Mellon seguido de otros equipos de seguridad estadounidenses.

- Un año despues, en 1989, nació CIAC (http://ciac.llnl.gov), Computer Incident Advisory Capability perteneciente departamento de Energia de Unidos. Ese mismo año aparece el gusano WANK.

- El principal objetivo de los CERTs o IRT es responder de forma óptima antes una incidendia donde interviene información digital

Introducción

Organización...(II)

- 1990: FIRST. (Forum of Incident Response and Security Teams) con 9 equipos de seguridad de EEUU y 1 equipo europeo.
- A partir de 1991 el sistema CERT se empieza a expandir a otras regiones y FIRST crece rápidamente
- 1992: Se funda GOVCERT-NL (http://www.govcert.nl/), equipo de respuesta a incidentes del gobierno Holandes y uno de los más activos en Europa.
- 1993: Se funda AUSCERT ((http://www.auscert.org.au/), primer IRT en la zona Asia-Pacífico.
- 1995: Se crean esCERT-UPC y RedIris!!!

Introducción

Creando nuestro propio equipo

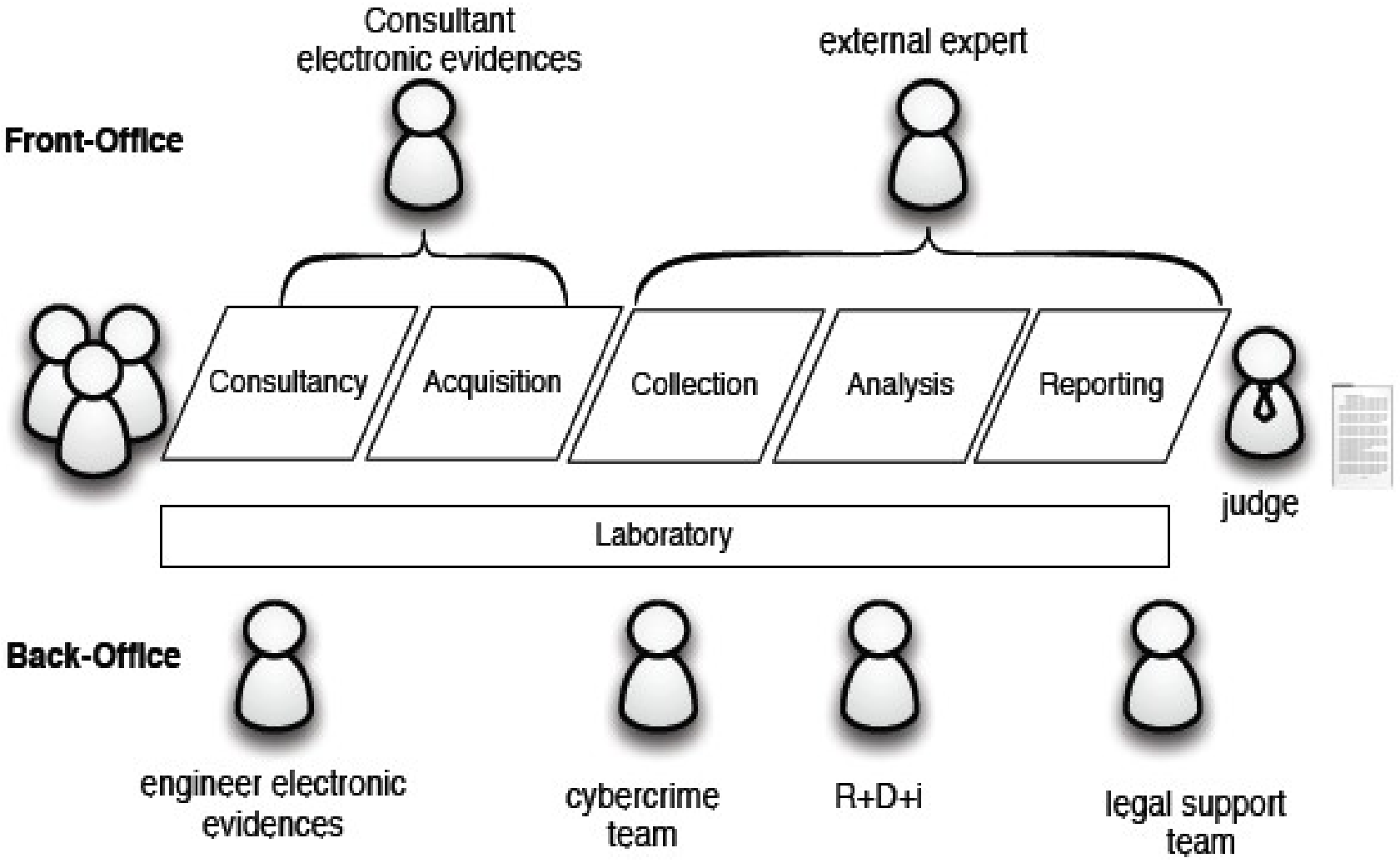
Las siguientes preguntas deben de analizarse antes de crear un equipo de respuesta a incidentes:

- ¿Estructura organizativa y técnica de la organización?
- ¿A qué comunidad se va a dar servicio? (constituency)
- ¿Cuáles son las metas y objetivos del IRT?
- ¿Cuál es el **nivel de autoridad** que posee el IRT?
- ¿Qué servicios se van a proporcionar?
- ¿Cuál es el modelo organizativo o estructura operativa?
- ¿Qué equipamiento e infraestructura de red se necesita para dar soporte a sus funciones diarias?
- ¿Cómo se va a financiar y sustentar?

Introducción

Niveles de Autoridad	Relación con la comunidad
Completa	Los miembros del IRT tienen la autoridad de llevar a cabo cualquier acción o decisión relativas a un incidente en nombre de su comunidad.
Compartida	Los miembros del IRT tienen influencia en las decisiones de su comunidad, pero éstas siempre son compartidas.
Sin autoridad	No tienen autoridad sobre su comunidad. Se limitan a aconsejar y diseminar información.

Introducción
Fases de un forense



- Entender el problema
- Determinar dónde se almacena la información importante
- Determinar lo objetivos

Introducción
Fases de un forense. 2 Agregación (collection)

- Agregar la información relevante obtenida anteriormente
- Filtrar información:
  - Palabras clave
  - Información temporal
- Obtener los datos relevantes
  - Extraer el mailbox de un usuario de una base de datos

Fases de un forense. 3 Análisis

- Analizar el conocimiento extraido de los datos preprocesados
  - Respetando la legalidad
  - Investigando UNICAMENTE lo que estamos autorizados

Introducción
Fases de un forense. y 4 Reporting

- Expresar en un documento los hechos
  - Contrastados
  - Relacionados con la investigacion
- No incluir datos subjetivos
- Si se expresa una hipótesis, comentarlo claramente

FORENSICS

ASPECTOS LEGALES

Aspectos Legales

- La mayoría de las veces que se realiza un análisis forense es para determinar actividades que se presumen delictivas o ilegítimas, aunque cabe la obtención de pruebas simplemente a título informativo para conocimiento exclusivo del cliente.

- Es importante conocer la legislación y así evitar el rechazo de pruebas en un juicio por haber infringido la ley.

Aspectos legasles
Aportacion de pruebas

- La prueba es el instrumento que tienen las partes para acreditar los hechos en los que basan sus pretensiones.
- Cuándo se presentan? Depende de la jurisdicción
- Prueba pericial en jurisdicción civil
  - Pericial de parte: Se adjunta a la demanda o contestación
  - Pericial judicial: Lo pueden pedir las partes antes de la vista

Aspectos Legales

Jurisdicción civil

- Regulado por la **Ley de Enjuiciamiento Civil**

- Cabrá la realización de actuaciones en ámbitos tales como la demostración de realización de **daños en equipos informáticos, actuaciones relativas a competencia desleal**, así como cualquier otra acción que pretenda demostrar la identidad de un sujeto que haya cometido un ilícito civil, que afectará generalmente a empresas.

- Áreas especializadas: **mercantil y familiar**

Aspectos Legales

Jurisdicción Laboral o Social

- Sometidos a la **Ley de Procedimiento Laboral**

- La finalidad de estos procedimientos consistirá, de modo mayoritario, en obtener información acerca del **uso correcto o incorrecto por parte de los trabajadores de los medios telemáticos** titularidad del empresario.

Jurisdicción Laboral o Social (II)

- Son aquellos procedimientos en que existe una relación laboral entre las partes denunciante y denunciada. Se **limita la capacidad de control del empresario**, en favor de los derechos fundamentales de los trabajadores.

Art. 90.1 Ley de Procedimiento Laboral:

- "Las partes podrán valerse de cuantos medios de prueba se encuentren regulados en la Ley, admitiéndose como tales los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan **violación de derechos fundamentales** o libertades públicas."

Jurisdicción Laboral o Social (III)

Punto 3 del Artículo 20 (Dirección y control de la actividad laboral) del Estatuto de los Trabajadores:

- "El empresario podrá adoptar las medidas que estime más oportunas de **vigilancia y control** para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su **dignidad humana** y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso."

- Normalmente:
  - Registro de **equipos** informáticos
  - En **horario** de trabajo.
  - Dentro de los **locales** de la empresa.
  - En presencia de un **representante** de los trabajadores.

Aspectos Legales

Jurisdicción Penal

- Regulado por la Ley de **Enjuiciamiento Criminal**.
- En él, se deberán aportar pruebas acerca de la comisión de presuntos delitos o faltas y se determinará la forma y presentación de las pruebas, que requerirá en muchos casos la colaboración con órganos judiciales (jueces de instrucción) a la hora de obtener las evidencias.
- 2 fases: **instrucción y enjuiciamiento**

Aspectos Legales

Jurisdicción Contencioso Administrativa

- Litigios de **particulares y empresas contra las Administraciones** públicas (Estado, Comunidades Autónomas y Entidades Locales) y toda clase de entes públicos (Agencia de protección de datos, Servicio de Salud de una Comunidad Autónoma, Universidades públicas …etc).

Aspectos Legales
Inicio de un proceso

- **Procedimientos Penales:**
  - **Denuncia**: Igual no somos las victimas
    - Policía o juzgado
    - No tenemos que ser parte
  - **Querella**: siempre somos el perjudicado. Denunciamos a una persona concreta
    - Por escrito y probado!
    - En juzgado
    - Con abogado y procurador
- **Otros Procedimientos: Demanda**
- **Abogada**: http://www.youtube.com/watch?v=5RTW5eAaF7Q

Aspectos Legales

- **Admisibilidad**
- Asegurar las características de: Autenticidad, Confiabilidad, Suficiencia y conformidad con la leyes y reglas de la administración de justicia
- ¿Cómo se establece la **autenticidad** en medios electrónicos?
- ¿Son **confiables** los registros electrónicos que generan los sistemas electrónicos o informáticos?
- ¿Estarán **completos** los datos que se presentan en los archivos analizados?
- ¿Cómo fueron **obtenidas** estas evidencias digitales?

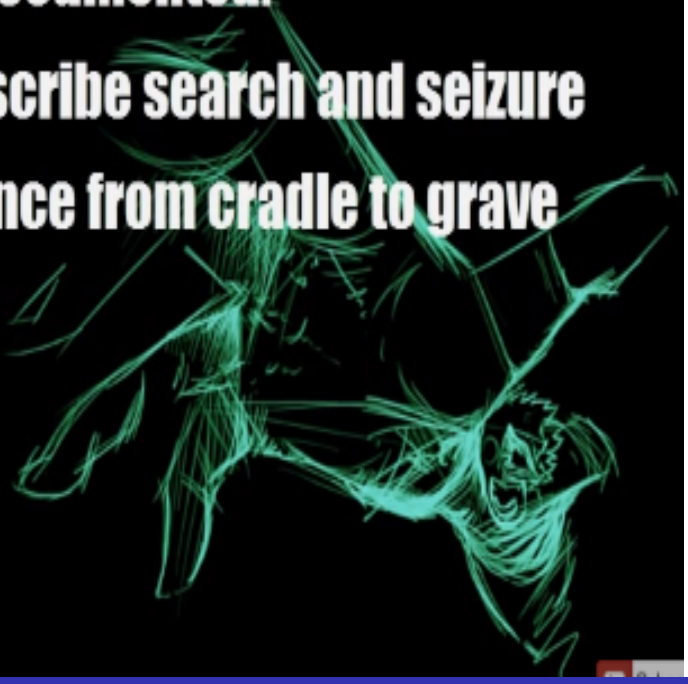
FORENSICS

FORENSICS READINESS

Investigation Check List:

Starting the Investigation

1. Law or Policy needs to be in place
2. Probable cause needs to be determined and documented.
3. Warrent with scope drafted to particularly describe search and seizure
4. Chain of Custody created to accompany evidence from cradle to grave
5. Execute investigation and stay within scope
6. Secure the Evidence
7. Gather first, analyze later



Top 10 Forensic Fouls

- Work on original data when not required
- Break Chain of Custody (CoC) or falsify it
- Modify the data / tamper with after acquisition and/or not document it
- Miss common evidence artifacts do to laziness or lack of understanding
- Fail to understand evidence is NOT 100% reliable
- Do not hash the drive and files
- Do not control access to evidence and/or ducument CoC breaks
- Do not validate and test policies, procedures, and tools
- Rely on only one tool
- Do not stay within scope

Clasificación según funciones

Tipos de Incidentes según IrisCERT:

- Comunicación Ofensiva
- Denegación de Servicio
- Virus
- Otros
- Sondeos o escaneos de puertos
- Acceso a cuentas privilegiadas
- SPAM
- Troyanos
- Gusanos IIS
- Usos no autorizados
- Violaciones de Copyright

Tipos de Incidentes según EsCERT:

- Compromiso root
- Copyright
- Denegación de servicio
- Intento de acceso
- P2p
- Scan
- Spam
- Suplantación
- Virus
- Otros

Clasificación según origen

- **Internos**
  - Uno o más sistemas son utilizados para llevar a cabo ataques fuera de la comunidad (interna-externa) o hacia otros sistemas de la comunidad (interna-interna).
- **Externos**
  - Uno o más sistemas que no pertenecen a la comunidad atacan contra los sistemas propios. En estos casos son necesarias medidas de comunicación fluidas con CERT´s responsables o relacionados con el entorno al que pertenece la máquina atacante.

Clasificación según alcance

Ejemplo 1: esCERT

- **Leves (Nivel 1)**
  - Uno o más sistemas se ven involucrados en una incidencia y el administrador de éstos soluciona el problema por si mismo o mediante soporte telefónico
- **Graves (Nivel 2)**
  - La incidencia precisa de una investigación forense
  - La incidencia puede tener repercusiones en cuanto a sanciones administrativas
  - La incidencia tiene implicaciones legales
  - La incidencia precisa de una investigación a nivel internacional. Ejemplo: Un DoS (Denial of Service) a una máquina de otro País desde UPC
  - Nuevo ataque a nivel global

Ejemplo 2: Iris-CERT

- **Prioridad baja:** Tentativas en las que el atacante no consigue su propósito (p.ej. telnet)
- **Prioridad normal:** Acceso simple al sistema informático o escaneos insistentes de redes
- **Prioridad alta:** Infiltración de una cuenta privilegiada o denegación de servicio
- **Emergencia:** Lo que suponga peligro para vidas humanas, para la seguridad nacional o para la infraestructura de Internet.

Forensic Readiness

"1. Maximizing an environment's ability to collect credible digital evidence minimizing the cost of forensics in an incident response."

[1]Forensic Readiness,John Tan,@stake, Inc.,196 Broadway,Cambridge, MA 02139 USA

Requerimientos

- Conocimiento de la seguridad de entorno: Inventario, avisos, análisis de riesgo
- Monitorización
- Herramientas de gestión de incidentes

¿QUÉ SON LOS AVISOS DE VULNERABILIDADES?

- Recopilación de avisos de seguridad donde se recopila información exhaustiva de la vulnerabilidad, organizada por plataformas afectadas y riesgos asociados que conlleva.

IMPORTANCIA DE LOS AVISOS DE VULNERABILIDADES

- Servicio preventivo
- Aumento del grado de confianza en la seguridad de las redes y sistemas.
- Reducción del riesgo asociado del impacto a las operaciones de la empesa (DOS, reducción de la productividad…)
- Minimización de la mala imagen a terceros.
- Estar al día de las nuevas vulnerabilidades y actualizaciones del software.
- Centralización de las vulnerabilidades (ahorro de tiempo).

ESTÁNDARES

- CVE (Common vulnerabilities and Exposures) de MITRE Corporation, quien establece los indicadores de
- vulnerabilidades utilizados por la mayoría de fabricantes hoy en día. Mediante el identificador es posible relacionar dicho aviso con firmas de Detectores de Intrusiones o Herramientas de Auditoría.
- CPE (Common Plaform Ennumeration) permite identificar de manera única sistemas operativos,aplicaciones y sistemas integrados

ESTÁNDARES

- CVSS (Common Vulnerability Scoring System)
- Se estableció en el 2004 dentro del Foro de Equipos de respuesta a Incidentes y equipos de seguridad FIRST .
- Tiene por objetivo identificar y evaluar las vulnerabilidades que se detectan en los sistemas y programas.

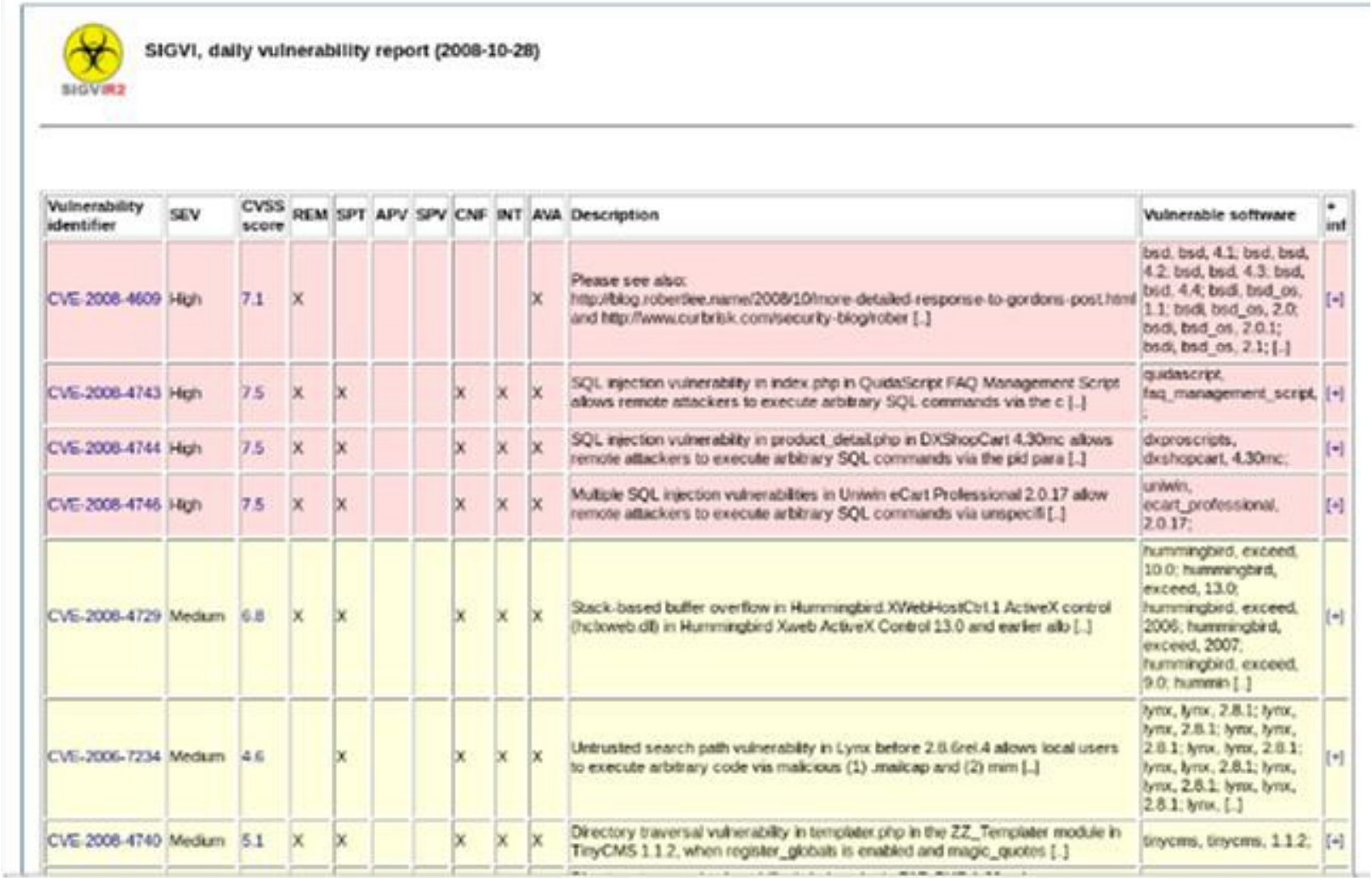
ESTÁNDARES

- CVSS es un conjunto de tres métricas:
  - **Base**: Representa el riesgo intrínseco y características fundamentales de la vulnerabilidad . Es constante en el tiempo.
  - **Temporal**: Representa la evolución del riesgo a medida que va pasando el tiempo.
  - **Entorno**: Representa las características de la vulnerabilidad, en función de un entorno específico para cada usuario.

EJEMPLO. SIGVI

- SIGVI es una aplicación para detectar, notificar y gestionar las vulnerabilidades de los sistemas.
- Funciones:
  - Descarga diariamente las nuevas vulnerabilidades desde recursos definidos como NVD.
  - Buscar en los repositorios de productos para detectar vulnerabilidades en el software instalado.
  - Creación de alertas de seguridad.
  - Finalmente enviar y notificar a cada uno de los administradores

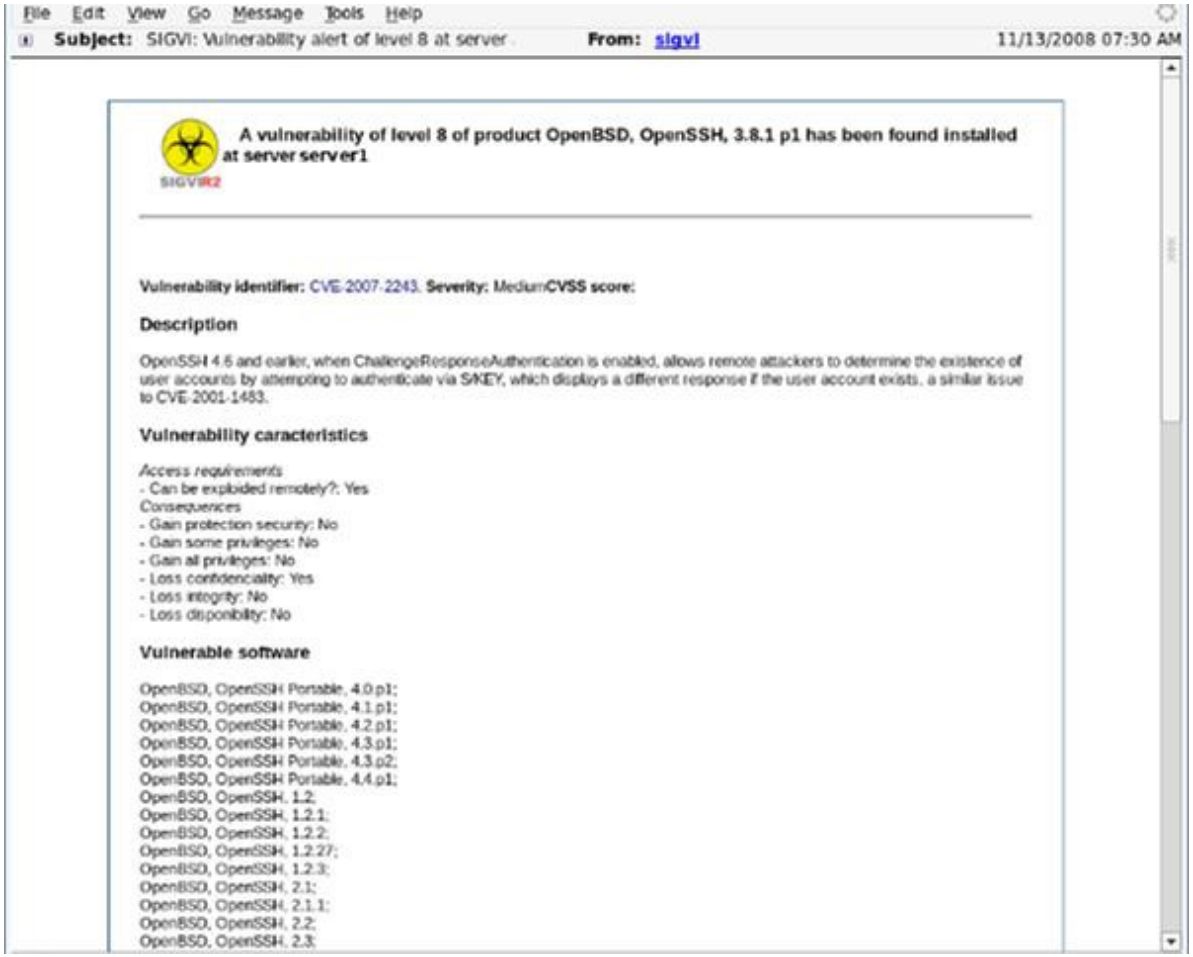
Forensic Readiness
Avisos de vulnerabilidades



SIGVI, daily vulnerability report (2008-10-28)

Vulnerability identifier	SEV	CVSS score	REM	SPT	APV	SPV	CNF	INT	AVA	Description	Vulnerable software	* inf
CVE-2008-4609	High	7.1	X						X	Please see also: http://blog.robertlee.name/2008/10/more-detailed-response-to-gordons-post.html and http://www.curbrisk.com/security-blog/rober [..]	bsd, bsd, 4.1; bsd, bsd, 4.2; bsd, bsd, 4.3; bsd, bsd, 4.4; bsdi, bsd_os, 1.1; bsdi, bsd_os, 2.0; bsdi, bsd_os, 2.0.1; bsdi, bsd_os, 2.1; [..]	[+]
CVE-2008-4743	High	7.5	X	X			X	X	X	SQL injection vulnerability in index.php in QuidaScript FAQ Management Script allows remote attackers to execute arbitrary SQL commands via the c [..]	quidascript, faq_management_script, -	[+]
CVE-2008-4744	High	7.5	X	X			X	X	X	SQL injection vulnerability in product_detail.php in DXShopCart 4.30mc allows remote attackers to execute arbitrary SQL commands via the pid para [..]	dxproscripts, dxshopcart, 4.30mc;	[+]
CVE-2008-4746	High	7.5	X	X			X	X	X	Multiple SQL injection vulnerabilities in Uniwin eCart Professional 2.0.17 allow remote attackers to execute arbitrary SQL commands via unspecifi [..]	uniwin, ecart_professional, 2.0.17;	[+]
CVE-2008-4729	Medium	6.8	X	X			X	X	X	Stack-based buffer overflow in Hummingbird.XWebHostCtrl.1 ActiveX control (hcloweb.dll) in Hummingbird Xweb ActiveX Control 13.0 and earlier allo [..]	hummingbird, exceed, 10.0; hummingbird, exceed, 13.0; hummingbird, exceed, 2006; hummingbird, exceed, 2007; hummingbird, exceed, 9.0; hummin [..]	[+]
CVE-2006-7234	Medium	4.6		X			X	X	X	Untrusted search path vulnerability in Lynx before 2.8.6rel.4 allows local users to execute arbitrary code via malicious (1) .mailcap and (2) mim [..]	lynx, lynx, 2.8.1; lynx, lynx, 2.8.1; lynx, lynx, 2.8.1; lynx, lynx, 2.8.1; lynx, lynx, 2.8.1; lynx, lynx, 2.8.1; lynx, lynx, 2.8.1; lynx, [..]	[+]
CVE-2008-4740	Medium	5.1	X	X			X	X	X	Directory traversal vulnerability in templater.php in the ZZ_Templater module in TinyCMS 1.1.2, when register_globals is enabled and magic_quotes [..]	tinycms, tinycms, 1.1.2;	[+]

Forensic Readiness
Avisos de vulnerabilidades



File Edit View Go Message Tools Help

Subject: SIGVI: Vulnerability alert of level 8 at server **From:** sigvi 11/13/2008 07:30 AM

A vulnerability of level 8 of product OpenBSD, OpenSSH, 3.8.1 p1 has been found installed at server server1

SIGVIR2

Vulnerability identifier: CVE-2007-2243. **Severity:** Medium**CVSS score:**

Description

OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.

Vulnerability caracteristics

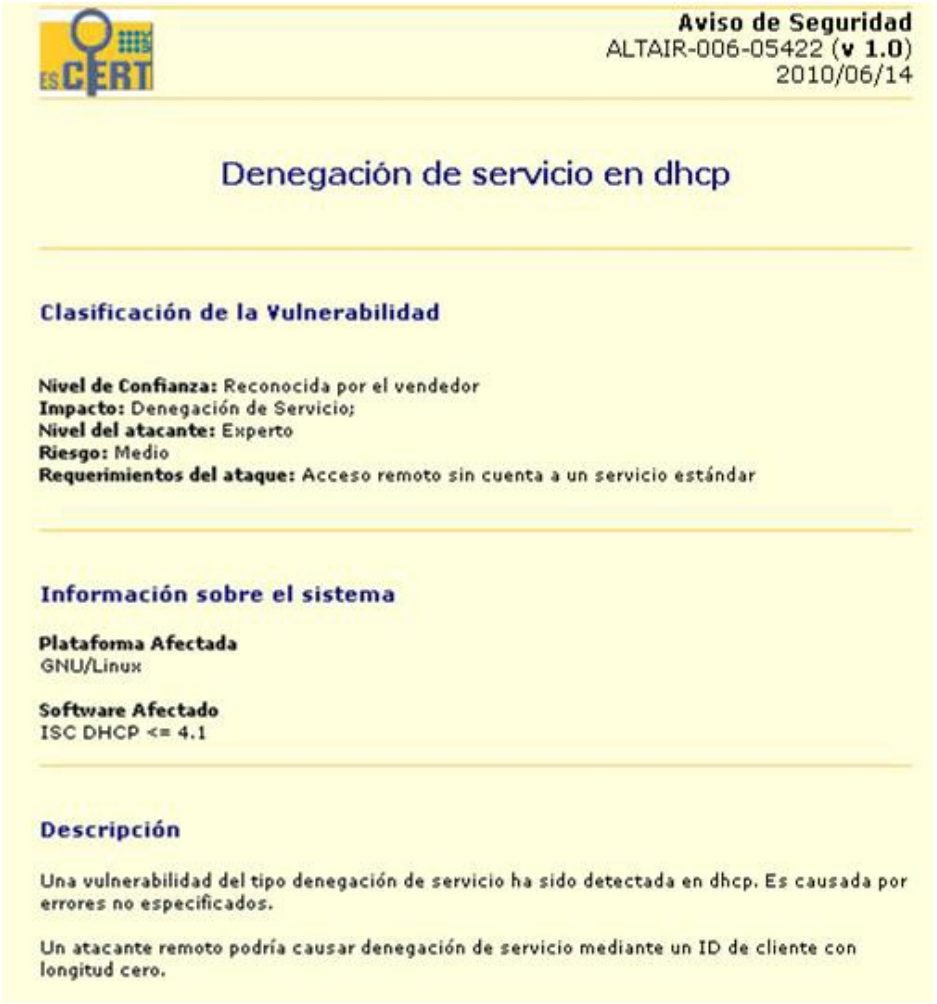
Access requirements
- Can be exploided remotely?: Yes

Consequences
- Gain protection security: No
- Gain some privileges: No
- Gain all privileges: No
- Loss confidenciality: Yes
- Loss integrity: No
- Loss disponibility: No

Vulnerable software

OpenBSD, OpenSSH Portable, 4.0.p1;
OpenBSD, OpenSSH Portable, 4.1.p1;
OpenBSD, OpenSSH Portable, 4.2.p1;
OpenBSD, OpenSSH Portable, 4.3.p1;
OpenBSD, OpenSSH Portable, 4.3.p2;
OpenBSD, OpenSSH Portable, 4.4.p1;
OpenBSD, OpenSSH, 1.2;
OpenBSD, OpenSSH, 1.2.1;
OpenBSD, OpenSSH, 1.2.2;
OpenBSD, OpenSSH, 1.2.27;
OpenBSD, OpenSSH, 1.2.3;
OpenBSD, OpenSSH, 2.1;
OpenBSD, OpenSSH, 2.1.1;
OpenBSD, OpenSSH, 2.2;
OpenBSD, OpenSSH, 2.3;

Forensic Readiness
Avisos de vulnerabilidades



Aviso de Seguridad
ALTAIR-006-05422 (**v 1.0**)
2010/06/14

Denegación de servicio en dhcp

Clasificación de la Vulnerabilidad

Nivel de Confianza: Reconocida por el vendedor
Impacto: Denegación de Servicio;
Nivel del atacante: Experto
Riesgo: Medio
Requerimientos del ataque: Acceso remoto sin cuenta a un servicio estándar

Información sobre el sistema

Plataforma Afectada
GNU/Linux

Software Afectado
ISC DHCP <= 4.1

Descripción

Una vulnerabilidad del tipo denegación de servicio ha sido detectada en dhcp. Es causada por errores no especificados.

Un atacante remoto podría causar denegación de servicio mediante un ID de cliente con longitud cero.

Forensic Readiness
Avisos de vulnerabilidades

Ubuntu 9.10

- mysql-server-5.1 / patch 5.1.37-1ubuntu5.4

Ubuntu 10.04 LTS

- mysql-server-5.1 / patch 5.1.41-3ubuntu12.3

Identificador Estándar

- CVE: CVE-2010-1621

Recursos adicionales

- Mandriva Security Advisory (MDVSA-2010:093)
  - http://www.mandriva.com/security/advisories?name=MDVSA-2010:093
- Ubuntu Security Advisory (USN-950-1)
  - http://www.ubuntu.com/usn/950-1

Histórico de Versiones

Versión	Comentario	Fecha
1.1	Aviso emitido por Ubuntu (USN-950-1)	2010/06/10
1.0	Aviso emitido	2010/05/10

---

esCERT-UPC
C/ Jordi Girona, 1 - 3
Modul D6
08034 Barcelona SPAIN

Website: http://escert.upc.edu
e-mail: altair@escert.upc.edu
Phone: (+34) 934 015 795
Fax: (+34) 934 054 230

Forensic Readiness
Monitorización

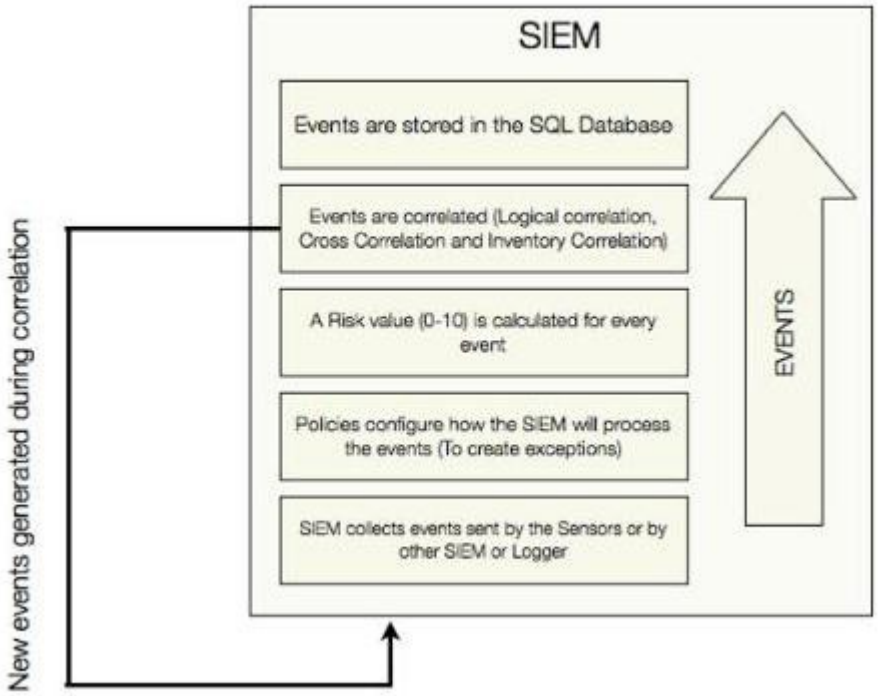
- IDS: Control de firmas
- Honeypots
- ADS: Conocimiento del entorno
- HDS: Tripwire, RKHUNTER
- Logs
- Correlación de eventos:
  - SAWMILL
- All-in-one: SIEM
  - OSSIM
  - Intellitactics

Forensic Readiness
Monitorización

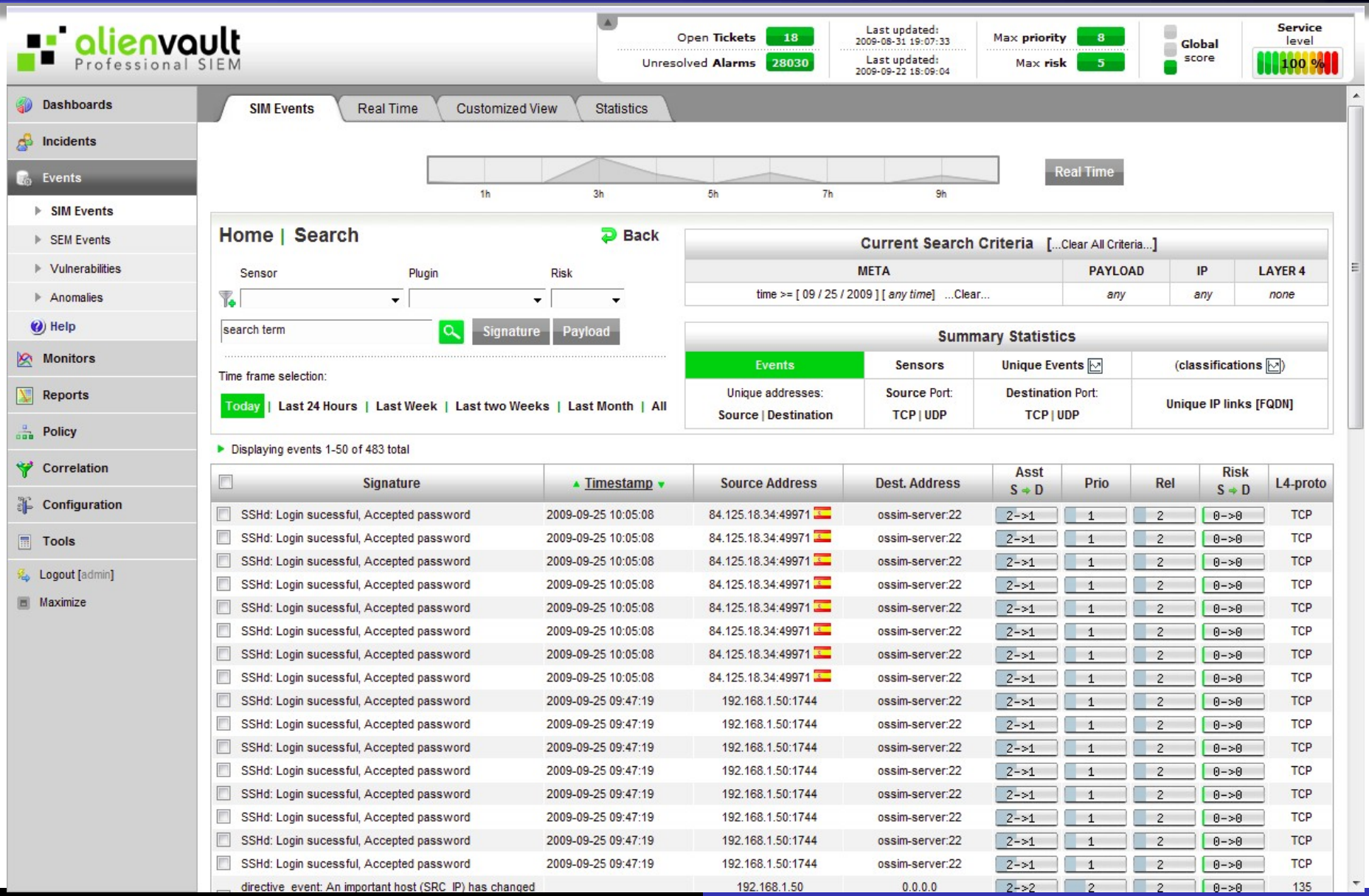
- **SIEM**: Security Information and Event Management
  - Agregación de datos
  - Correlación
  - Alertas
  - Dashboards

- **OSSIM**:Open Source Security Information Management

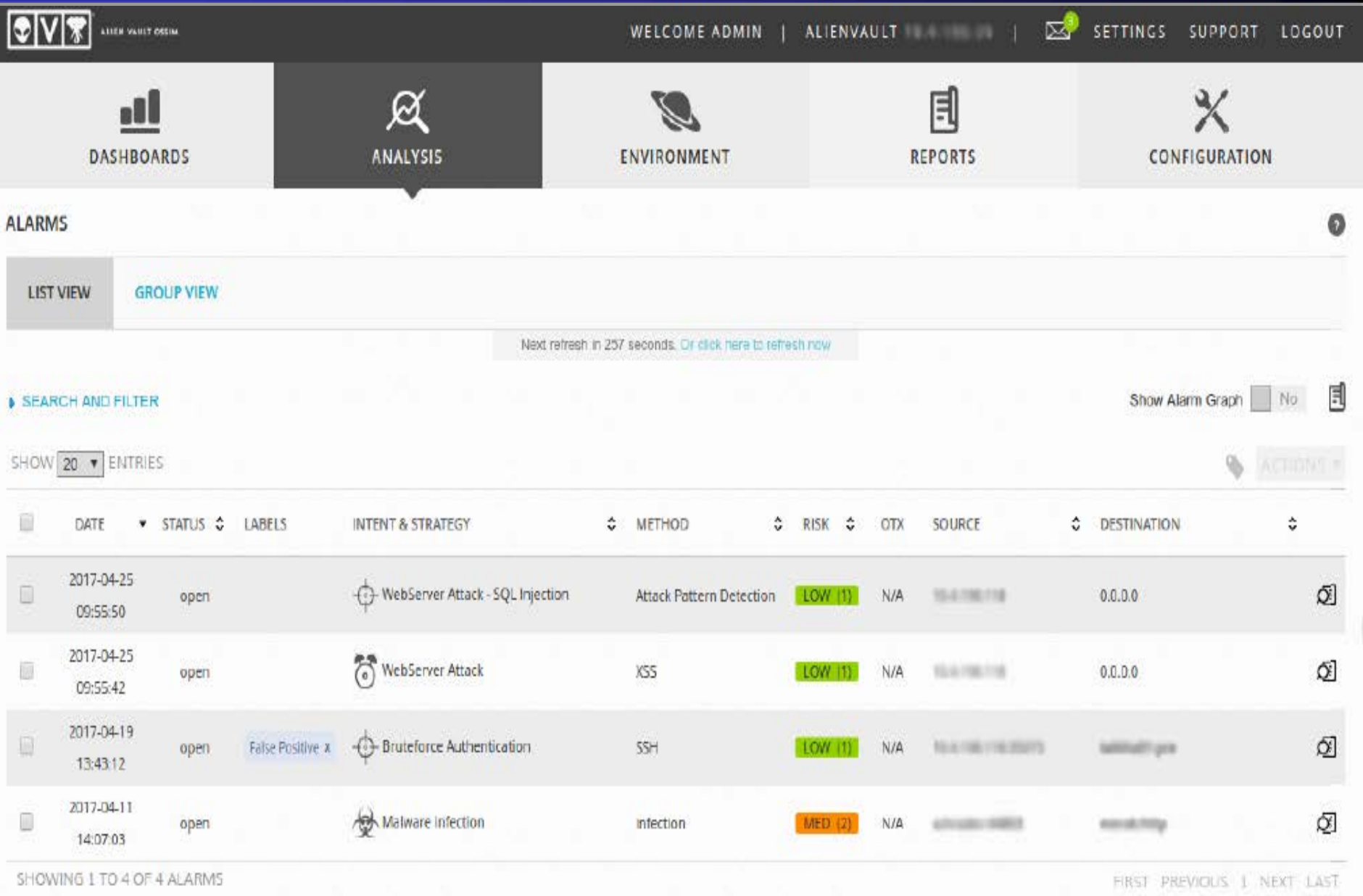
Forensic Readiness
Monitorización



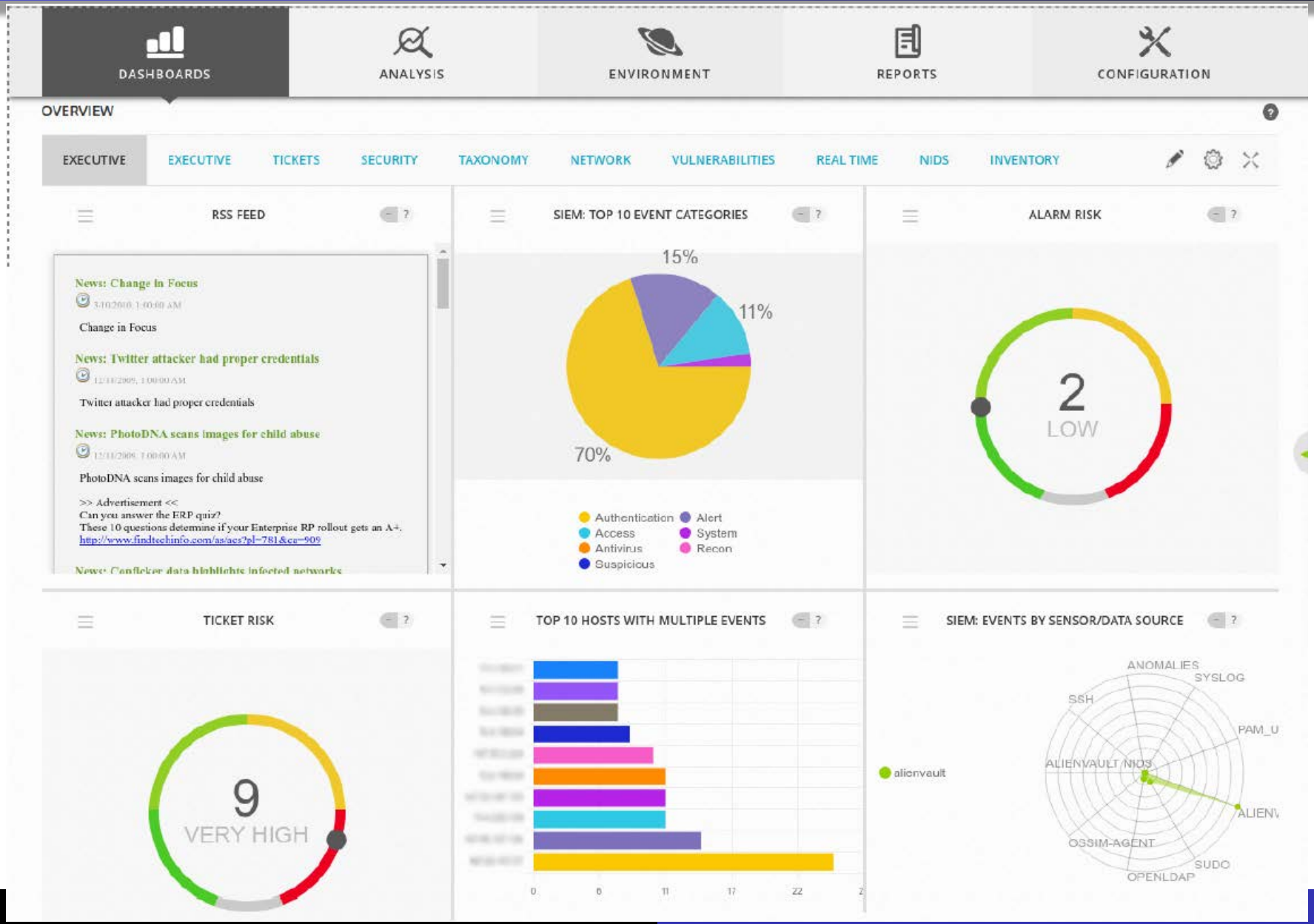
Forensic Readiness
Monitorización



Forensic Readiness
Monitorización: Alarmas



Forensic Readiness
Monitorización: dashboard



OSSIM…problema: Los eventos se almacenan en SQL

Solución:

-Almacenar logs en local

-OSSIM unified

"The Logger component stores events in raw format in the file system. Events are digitally signed and stored en masse, ensuring their admissibility as evidence in a court of law.

The logger component allows storage of an unlimited number of events for forensic. Logger addresses security, legal and compliances needs through:

- Digital Signatures ensures data integrity
- Encrypted Transport ensures Chain-of-Custody
- 10:1 Compression saves valuable space
- SAN/NAS Interoperability allows for limitless scalability"

Unified Version: https://cloud.alienvault.com/signintest/

Forensic Readiness
Gestión de incidentes

From: paramount@copyright-compliance.com

To: abuse@upc.edu

Subject: XXXXXXX Notice of Unauthorized Use of Paramount Pictures Corporation Property

Dear Sir or Madam:

Irdeto USA, Inc. (hereinafter referred to as "Irdeto") swears under penalty of perjury that **Paramount Pictures** Corporation ("Paramount") has authorized Irdeto to act as its non-exclusive agent for **copyright infringement notification**. Irdeto's search of the protocol listed below has detected infringements of Paramount's copyright interests on your IP addresses as detailed in the below report.

Irdeto has reasonable good faith belief that use of the material in the manner complained of in the below report is not authorized by Paramount, its agents, or the law. **The information provided herein is accurate to the best of our knowledge**. Therefore, this letter is an official notification to effect **removal of the detected infringement** listed in the below report. The Berne Convention for the Protection of Literary and Artistic Works, the Universal Copyright Convention, as well as bilateral treaties with other countries allow for protection of client's copyrighted work even beyond U.S. borders. The below documentation specifies the exact location of the infringement.

We hereby **request that you immediately remove or block access to the infringing material**, as specified in the copyright laws, and insure the user refrains from using or sharing with others unauthorized Paramount's materials in the future.

Further, we believe that the entire Internet community benefits when these matters are resolved cooperatively. We urge you to take immediate action to stop this infringing activity and inform us of the results of your actions. We appreciate your efforts toward this common goal.

Please send us a prompt response indicating the actions you have taken to resolve this matter, making sure to reference the Notice ID number above in your response.

If you do not wish to reply by email, please use our Web Interface by clicking on the following link:
http://webreply.copyright-compliance.com/WebReply?webreplyhash=7b62d0e313489b26e43a149e4dd41fac

Nothing in this letter shall serve as a waiver of any rights or remedies of Paramount with respect to the alleged infringement, all of which are expressly reserved.
Should you need to contact me, I may be reached at the below address.

Forensic Readiness
Gestión de incidentes

Andrew Beck Irdeto
USA, Inc.
3255-3 Scott Blvd. Suite 101 Santa Clara, CA 95054
Phone: 408-492-8500 fax: 408-727-6743
paramount@copyright-compliance.com

*pgp public key is available on the key server at http://pgp.mit.edu

This infringement notice contains an XML tag that can be used to automate the processing of this data. If you would like more information on how to use this tag please contact Irdeto.

Evidentiary Information:

Notice ID: xxxxxxxxxxxxx

Initial Infringement Timestamp: 20 May 2014 11:06:19 GMT
Recent Infringement Timestamp: 20 May 2014 11:06:19 GMT
Infringers IP Address: 147.83.x.x
Protocol: **BitTorrent**
Infringed Work: **The Wolf of Wall Street**
Infringing File Name: The.Wolf.of.Wall.Street.2013.DVDSCR.XviD-BiDA
Infringing File Size: 1491708060
Bay ID: ce9fbdaa734cfbc160e8ef9d29072646c09958dd|1491708060
Port ID: 49504
Infringer's User Name:

Forensic Readiness
Gestión de incidentes

- **Necesidad de recibir, filtrar y priorizar incidentes.**
- **Ejemplos:**
  - OTRS
  - E-TICKET
  - Uqueue
  - RTIR

Open-source Ticket Request System (OTRS)

- Sistema abierto de solicitud y gestión de tickets.
- Asigna identificadores únicos llamados ticket a solicitudes de servicio o de información.
- Facilita el seguimiento y manejo de dichas solicitudes así como cualquier otra interacción con sus clientes o usuarios.
- OTRS es distribuido bajo los términos de "GPL General Public License“

FORENSICS

Adquisición de datos

Adquisición

- **Acta notarial**
  - **Manifestaciones**:
    - El perito manifiesta que ha realizado una acción.
  - **De requerimiento y presencia (diligencias.pdf):**
    - Las actas de presencia acreditan la realidad o verdad del hecho que motiva su autorización; en consecuencia, es muy posible que “la prueba esté servida” :
    - Se hace constar en un documento ya preexistente una actuación posterior en el tiempo.
    - Esta actuación se refleja en el acta por medio de unas diligencias con la firma del notario.
- **Depósito**
  - Notaría
  - Dependencias judiciales

Adquisición
Formatos

- dd
- Encase (EWF)
- Advance Forensics format (AFF)
  - Permite almacenar metadatos junto con las imágenes
  - Consume menos espacio que formatos propietarios

Adquisición
dd & hash

- Local
  - dd if=/dev/hdaX of=/media/disk/hdaX.dd conv=notrunc,noerror,sync
- Remoto
  - dd if=/dev/had bs=512 | gzip -c | nc -v -<image server ip> 3333
  - nc -v -w 120 -p 3333 -l > image.gz

- No trunc= se sobreescribe el destino, no se borra
- No error= continuar aunque haya un error
- Sync= Rellena cada bloque leido con ceros si hay un problema

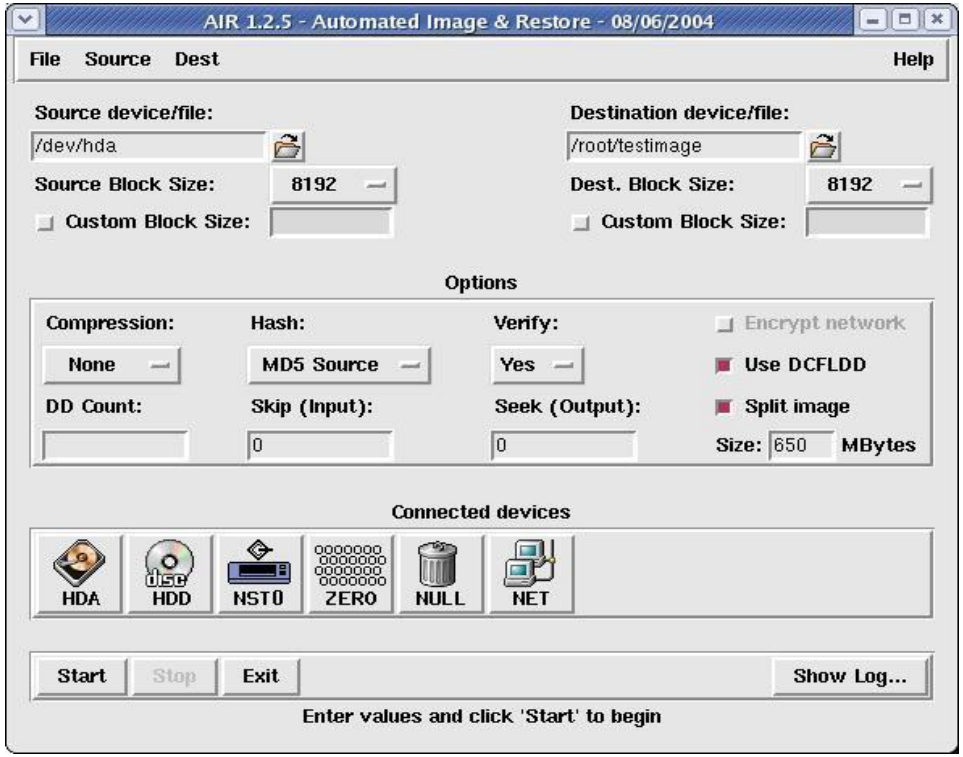
Adquisición
dd & hash

```
$> md5sum /dev/hda1.ddOrig
50d30762425e3a86f6bab0196dea63a9
```

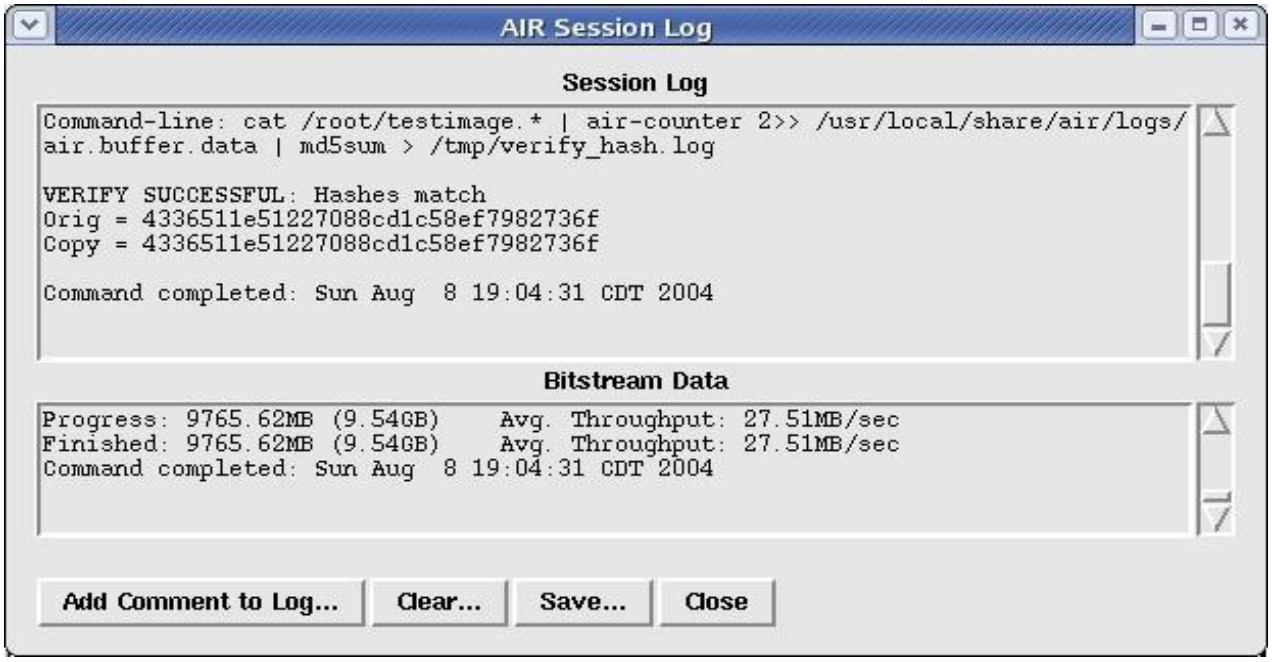
```
$> md5sum /mnt/hda1.ddCopy
50d30762425e3a86f6bab0196dea63a9
```

Adquisición
Air imager

- Utiliza **dc3dd**
- Compresión automática de imagenes
- Generación de hash “on the fly

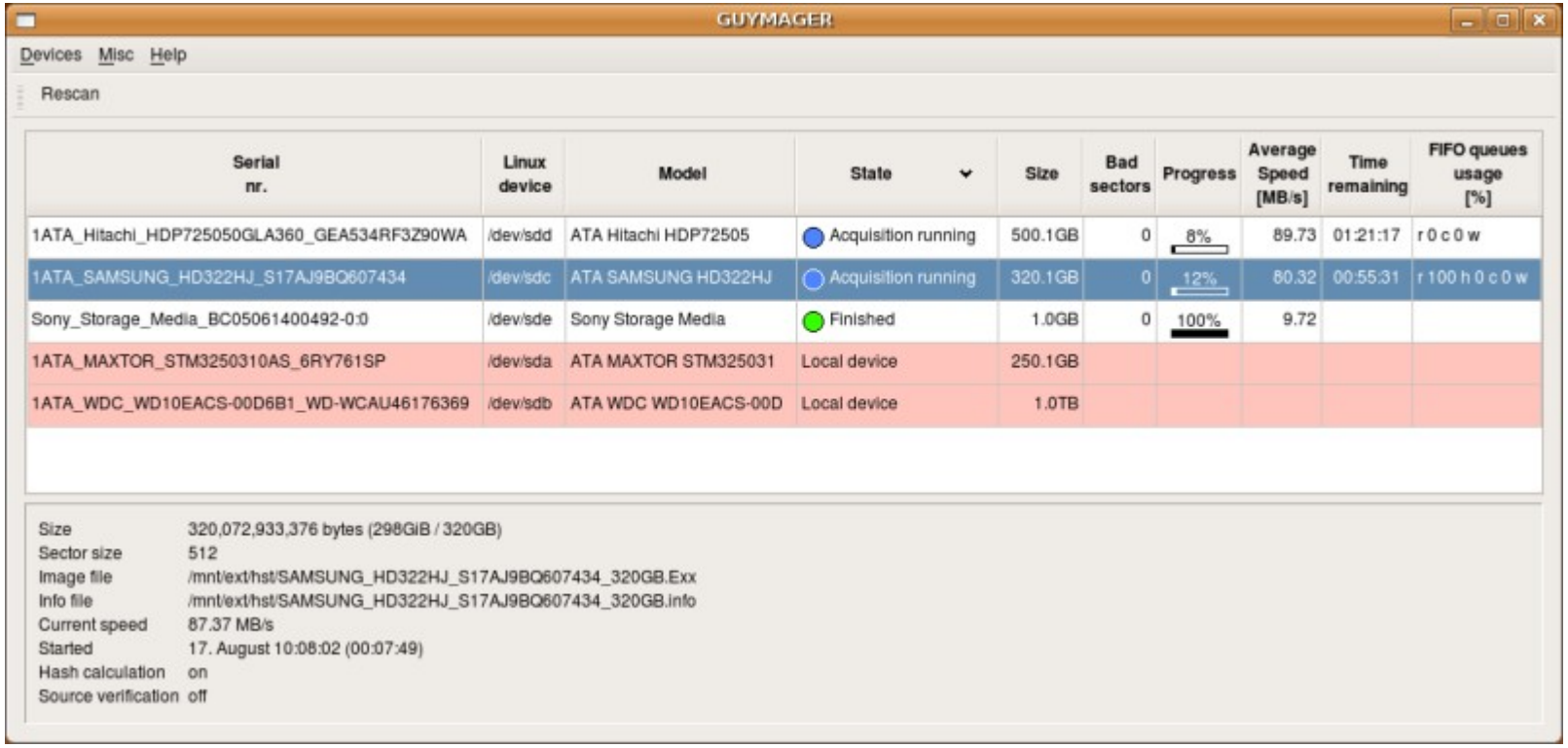


Adquisición
Air imager



Adquisición
Guymager

- Más sencillo de instalar que air
- Más fácil de utilizar



Forensics

Análisis post mortem

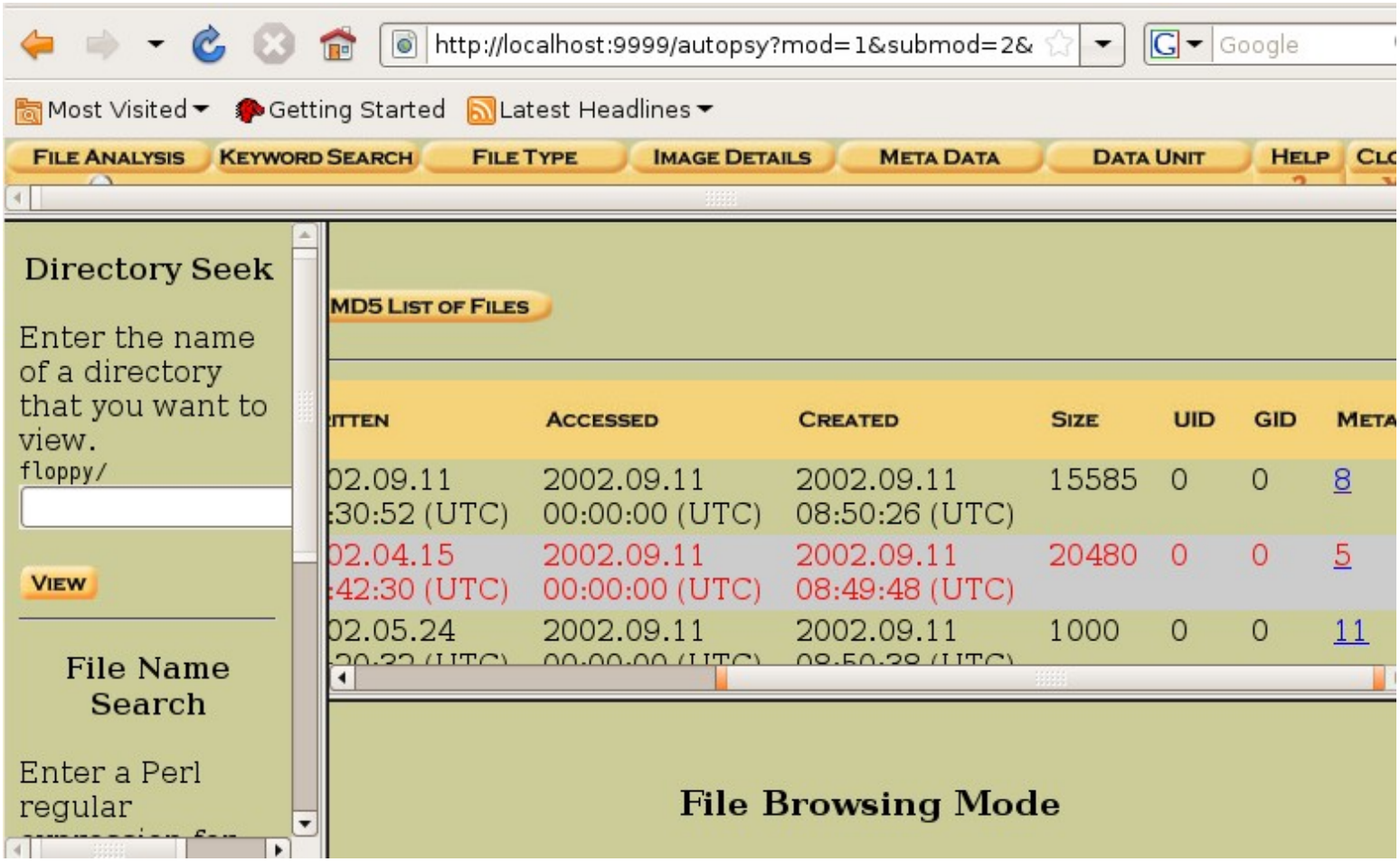
Análisis Postmortem
¿Qué es un sistema de archivo?

- Organización del espacio de almacenamiento
  - Espacio de almacenamiento: secuencia de unidades mínimas de transferencia (sectores)
  - Partición: unidad de uso mínima de un disco

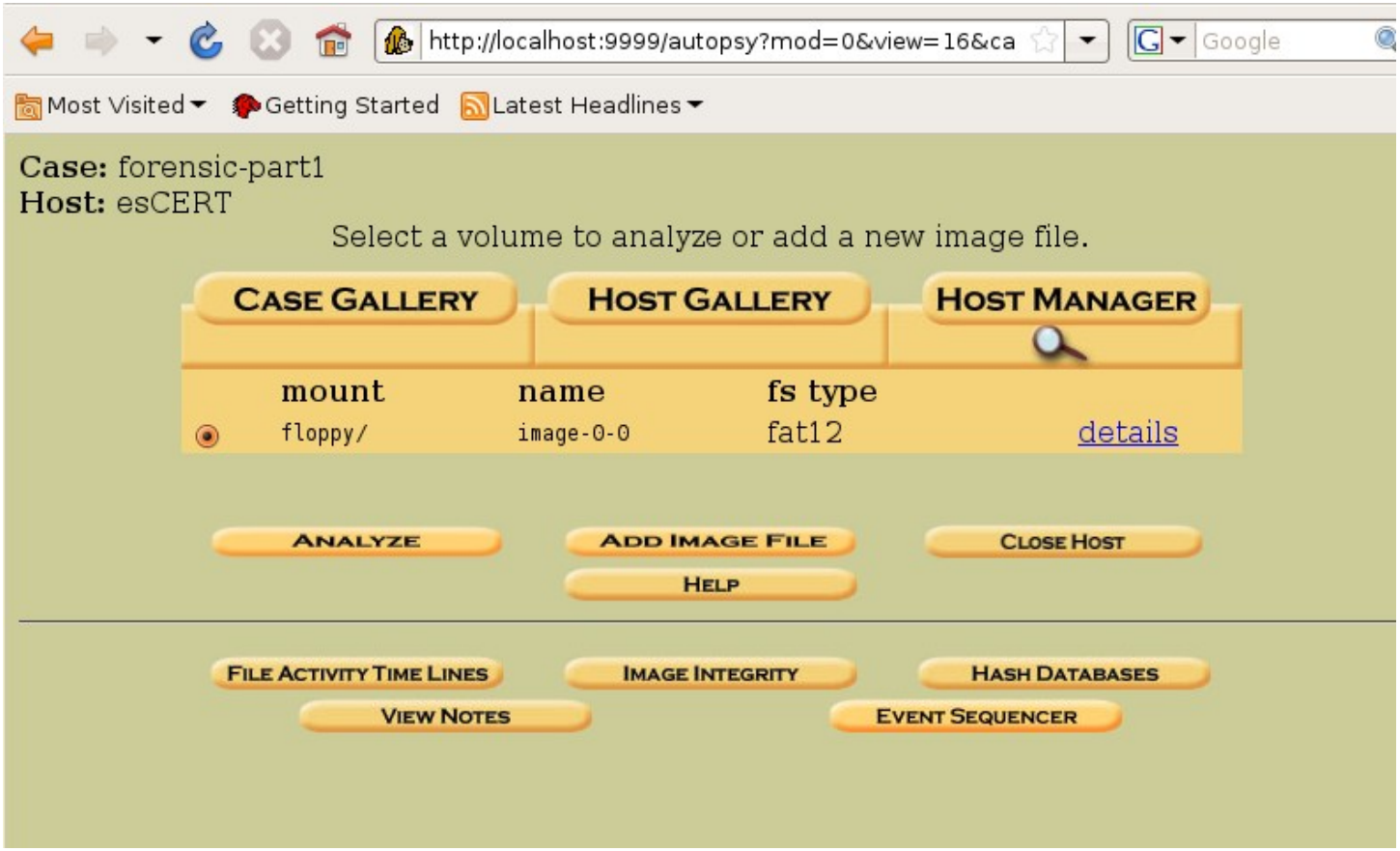
Análisis Postmortem
Herramientas

- Sleuthkit (Open Source). Basado en Coroner's Toolkit (TCT)
- Autopsy (Open Source)
- Encase (Comercial)
  - Estandar de Adquisición
- Forensic Toolkit (FTK) (Comercial)
  - Inluye herramientas para aciones concretas: mail, navegadores, passwords, etc.
  - Incluye una herramienta de adquisición (FTK imager)

Análisis Postmortem
Herramientas. Autopsy

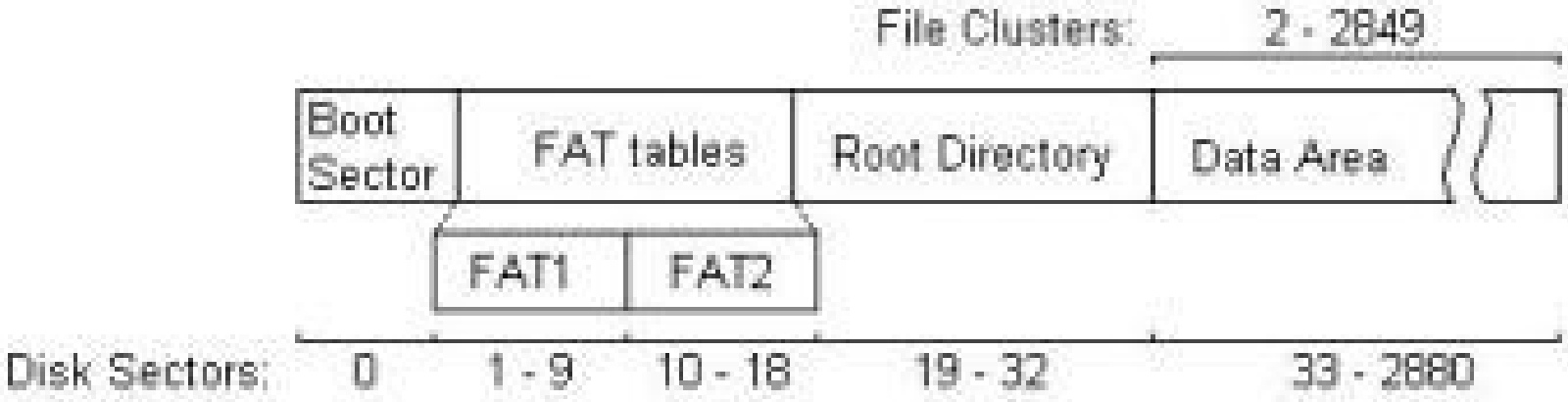


Análisis Postmortem
Herramientas. Autopsy



Análisis Postmortem
FAT

- 1 cluster= 1 sector = 512 bytes (puede cambiar)



Análisis Postmortem
FAT

- MBR da el control a Boot Record
- FAT. Representación de los clusters. Posibles valores:
  - 0x000 (Free Cluster)
  - 0x001 (Reserved Cluster)
  - 0x002 - 0xFEF (Used cluster; value points to next cluster)
  - 0xFF0 - 0xFF6 (Reserved values)
  - 0xFF7 (Bad cluster)
  - 0xFF8 - 0xFFF (Last cluster in file)
- Root directory
  - Nombre
  - Primer cluster
  - Tamaño

Laboratorio. FAT12

Laboratorio. Estaganografía

Análisis Postmortem
Esteganografía

- del griego *στεγανος* (*steganos*):cubierto u oculto, y *γραφος* (*graphos*): escritura
- Necesitamos un portador
- Problema del prisionero
  - Dos prisioneros quieren fugarse y solo pueden pasarse mensajes a través del guardian (portador)
  - Si el guardian detecta algún tipo de cifrado dejara de enviar mesajes
- Diferente a la criptografía pero pueden complementarla

Análisis Postmortem
NTFS

- Sucesor de FAT[]
- Soporta tamaños de partición mayores
- Incorpora mecanismos de protección a nivel de archivo
- Mejora la eficiencia de acceso a los archivos
- Un archivo de log permite la recuperación del sistema retrocediendo en la secuencia de acciones.
- Incorpora funciones especiales: compresión, encriptación, tratamiento optimizado de archivos “escasos”…
- Soporta el tratamiento de archivos enlazados (archivos con múltiples nombres)
- …

Análisis Postmortem
NTFS

- ¿Qué debemos conocer?
  - Estrucura del sistema de archivos: BS, BPB, MFT
  - Borrado de archivos
  - Data Streams
  - LNKs

Análisis Postmortem
NTFS . Estructura: Punto de entrada

- BS: primer sector de la partición
- Contiene información básica (técnica y específica) sobre el sistema de archivos

Análisis Postmortem
NTFS . Estructura: BS

Byte Offset	Field Length	Field Name
0x00	3 bytes	Jump instruction
0x03	8 bytes	OEM ID
0x0B	25 bytes	BPB
0x24	48 bytes	Extended BPB
0x54	426 bytes	Bootstrap code
0x01FE	2 bytes	End of sector marker

El código de arranque del MBR selecciona la partición “activa” y continúa la ejecución por esta instrucción de salto

La instrucción de salto es el punto de entrada al BootStrap code.

Análisis Postmortem
NTFS . Estructura: BS

Byte Offset	Field Length	Field Name
		Jump instruction
		OEM ID
0x0B	25 bytes	BPB
0x24	48 bytes	Extended BPB
0x54	426 bytes	Bootstrap code
0x01FE	2 bytes	End of sector marker

Identificación del S.O. que formateó.

BPB – BPB extendido: información básica del FS. En particular localización de la MFT

Análisis Postmortem
NTFS. Estructura: BPB

- Logical Cluster Number for the File $MFT”
  - Apunta al comienzo de la tabla de archivos
- Logical Cluster Number for the File $MFTMirr
  - Apunta a una copia de la tabla de archivos
- Clusters Per Index Buffer
  - (tamaño de un nodo relacionado con la estructura de directorio)

Análisis Postmortem
NTFS. Estructura: MFT

- MFT: tabla de archivos.
  - Combina las funciones de la FAT de directorio y tabla FAT
- Cada entrada a la tabla (Record) implica un “archivo”
  - “Archivo” es todo elemento almacenado en el disco. Esta propia tabla es considerada un archivo.
- Cada entrada está compuesta de Atributos
  - “Atributo” es cualquier característica asociada al archivo, desde su nombre hasta sus propios datos.

- Las primeras 16 entradas están reservadas para archivos de sistema
  - Las dos primeras hacen referencia a **la propia MFT y su copia**
  - **LogFile** contiene la secuencia de últimas acciones realizadas (+ ó -)
  - **Cluster BitMap** indica los clusteres libres y ocupados

Análisis Postmortem
NTFS. Estructura: MFT y Clusteres

- El cluster es la unidad mínima de asignación
  - Se define su tamaño (en términos de sectores en BPB)
- Todo sistema de archivos debe tener un medio de mecanismo de control de clusters en uso
  - FAT: tabla FAT
  - NTFS: $BitMap record

MFTZone es el espacio reservado para la MFT.

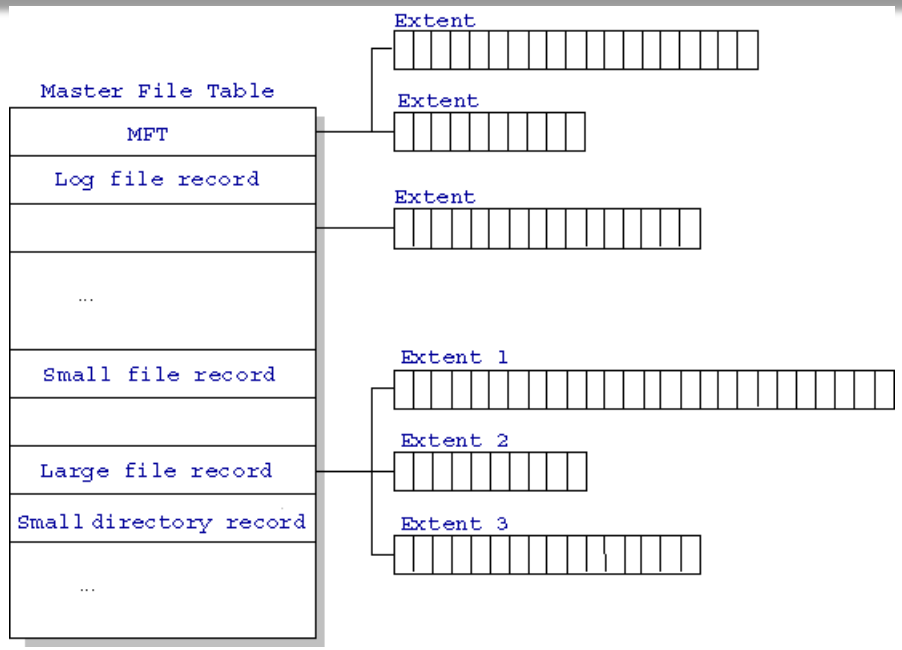
El resto del espacio de la partición lo ocupan los clústeres libres.
(excluyendo el sector de arranque y la copia de la MFT)
La copia de la MFT no es completa (primeros cuatro records)

Es reconfigurable

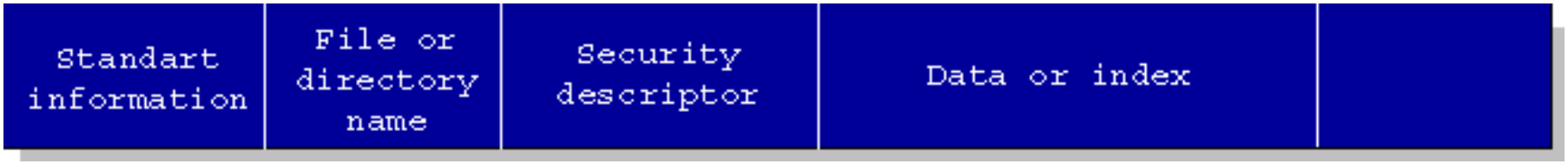
- Si muchos archivos de pequeño tamaño (900 bytes) => MFTZone grande
- Si muchos archivos de gran tamaño => MFTZone pequeña

Análisis Postmortem
NTFS. Estructura: MFT

- Cada entrada un archivo completo
  - Incluido datos
- Los archivos se describen en términos de atributos
- Si los datos no caben en el espacio reservado (1Kbyte) un atributo extiende el espacio



El acceso a los archivos se realiza de manera directa, sin indirecciones (en los archivos pequeños)



Análisis Postmortem
NTFS. Estructura: MFT

- Resident vs Extended Records
- Lo directorios pequeños se almacenan en la MFT
- Los grandes directorios se almacenan en estructuras de b-trees

Análisis Postmortem
NTFS. Borrado de datos

- Cuando un archivo se borra en NTFS se marca como borrado en la MFT
  - Archivo activo “01 00” bytes 22 y 23
  - Archivo borrado “00 00” bytes 22 y 23
- En el BitMap se marcan los clusters corerspondientes al archivo como libres

- https://www.youtube.com/watch?v=TmDkktcm-Ls#t=193

Análisis Postmortem
NTFS. Alternate Data streams

- NTFS file support multiple $DATA attributes, each of which is referred to as an alternate data stream (ADS).
- ADS allows Windows programs to store additional information in the form of a separate stream.
- The data contained in the alternate stream would not be displayed by non-ADS aware applications.
- The directory listing would only show the primary file name; even the file size displayed is only the size for the primary stream as well.

Análisis Postmortem
NTFS. Alternate Data streams

```
C:\Test>echo This is a Test File > innocuous.txt

C:\Test>type innocuous.txt
This is a Test File

C:\Test>dir
Volume in drive C has no label.
Volume Serial Number is 00A8-1CDC

Directory of C:\Test

09/20/2004 12:39 PM <DIR> .
09/20/2004 12:39 PM <DIR> ..
09/20/2004 12:39 PM 22 innocuous.txt
1 File(s) 22 bytes
2 Dir(s) 3,003,953,152 bytes free
```

Análisis Postmortem
NTFS. Alternate Data streams

C:\Test>echo Here is a second file > innocuous.txt:secret

C:\Test>dir
Volume in drive C has no label.
Volume Serial Number is 00A8-1CDC

Directory of C:\Test

09/20/2004 12:39 PM <DIR> .
09/20/2004 12:39 PM <DIR> ..
09/20/2004 12:39 PM 22 innocuous.txt
1 File(s) 22 bytes
2 Dir(s) 3,003,953,152 bytes free

C:\Test>type innocuous.txt
This is a Test File

C:\Test>type innocuous.txt:secret
The filename, directory name, or volume label syntax is incorrect.

C:\Test>more < innocuous.txt:secret
Here is a second file

Análisis Postmortem
NTFS. Alternate Data streams

Sysinternals Tool: Streams

- http://technet.microsoft.com/en-us/sysinternals/bb897440

```
C:\Test>streams *

Streams v1.5 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2003 Mark Russinovich
Sysinternals - www.sysinternals.com
```

NTFS. Otras características

- Compresión
  - Permite la manipulación habitual de un archivo comprimido sin necesidad de realizar de forma explícita las operaciones de compresión y descompresión.
- Encriptación
  - Se realiza a nivel de usuario. Otro usuario no podría acceder al archivo, ni tampoco en otro S.O. Permite también la manipulación sin requerir desencriptación explícita.
- Archivos escasos
  - Un tipo especial de compresión para archivos con información redundante.

JOURNALING

- Se logea todos los cambios
  - Creación, modificación, camio de nombre, editar guardar.
- Si algo se daña es más facil recuperarlo

SPARSE FILES

Si un archivo tiene una zona con “0” se elimina

Discos más eficientes!

Análisis Postmortem
NTFS. LNKs

- “Soft-link”
- • “Acceso directo”
- • Un fichero que apunta a otro fichero
- • Uso habitual en sistemas windows…?

Análisis Postmortem
NTFS. LNKs

- Creados automáticamente al hacer doble-click sobre un fichero (“recientes” de windows)
- Listado de “recientes” en varias aplicaciones
- Se guarda un gran número de ellos, aunque en la lista se muestren pocos
- Son muy pequeños (<1024 bytes normalmente,
- <4096 bytes prácticamente siempre)
- Se borran al ser muy antiguos y alcanzar un gran espacio utilizado (o sea, casi nunca)

Análisis Postmortem
NTFS. LNKs

- Contiene información sobre la ubicación del fichero al que apunta
- Contiene información sobre el fichero al que apunta
- Es un buen indicador de la actividad llevada a cabo en un equipo

Análisis Postmortem
NTFS. LNKs

- Tamaño inferior a un cluster
- Fácil de hacer carving
  - O no sale nada (primeros bytes de la cabecera sobreescritos al reusar el cluster)
  - O sale completo (siempre suele ocupar menos de un cluster)
- No hay que tratar con elementos corruptos

Análisis Postmortem
NTFS. LNKs

- Contiene información acerca del fichero al que apunta, no solamente el nombre:
  - Fecha de creación
  - Fecha de modificación
  - Fecha de acceso
  - Flags del fichero
  - Tamaño del fichero

- Puede contener información sobre el
- volumen donde se encuentra el fichero:
  - Tipo de volumen
  - Número de serie del volumen
  - Etiqueta de volumen
  - Nombre de recurso de red (en caso de ser un recurso compartido)

Análisis Postmortem
EXT

- “fácil” recuperar información de FAT y NTFS
- Muy complicado en ext. Porqué?
  - Información basica se elimina duarnte el proceso de borrado.
- Normalmente tenemos sectores de 512 bytes
- Los sectores se agrupan en bloques de 1024 a 4096 bytes
- Los **bloques** se almacenan en **grupos de bloques.**
- Cada archivo se almacena en:
  - bloques
  - i-nodos
  - Entradas de directorios (directory entries)

i-nodos

- Los i-nodos se almacenan en al principio de cada grupo de bloques.
- almacenan los metadatos: MAC, tamaño, user id, direcciones de los nodos correspondientes, etc.
- **Las direcciones de los primeros 12 bloques se almacenan en el i-nodo**
- El resto de direcciones se almacenan en bloques indirectos (indirect blocks). Dobles, triples, etc.

Análisis Postmortem
EXT

- Un directorio es parecido a un archivo
  - Contiene una lista de entradas, cada una de las cuales es un archivo y los inodos con los metadatos (ls -i)
  - Cada entrada almacena:
    - Nombre del archivo
    - Inodo
    - Tamaño
    - Tipo
    - ….
- Creación de archivos:
  - El sistema alocata bloques de datos e inodos en un mismo grupo de bloques que el directorio donde se almacena.
  - Los archivos de un directorios están cerca.

Análisis Postmortem
EXT

- Borrado de archivos
  - El sistema operativo marca marca los bloques, inodos y directory entry como disponibles.
  - Si el inodo existe -> Se pueden ver los bloques!
  - Pero….
  - En ext3 y ext4 al borrar un archivo la informacion dentro del inodo se borra.

Análisis Postmortem
EXT

- Recuperacion de archivos:
  - Tipo de archivo
  - Journal
- debugfs (The sleuth kit)
- ds –d->Vemos en qué inodo se almacena la info de un archivo
- El journal contiene copias de inodos, por lo que podemos ver varias versiones del un mismo inodo.
  - Logdump –i <inodo>

- Más info: http://linux.sys-con.com/node/117909

FORENSICS

LIVE FORENSICS

Live Windows

- Archivos interesantes:
  - **pagefile.sys**->swap. 1.5 veces mas grande que la memoria RAM
    - Eliminar: **Sin archivo de paginación**
  - **hiberfil.sys**-> Hibernación de discos
    - Eliminar: Opciones de energia->Habilitar hibernación
  - **index.dat**->Internet explorer. Últimas urls visitadas
  - C:\ Documents and Settings\ username\ Application Data\ Mozilla\ Firefox\\profiles\ xxxxxx\ **Cache-**>Firefox

Index.dat

- Windows XP
  - \Documents and Settings\<Username>\Cookies\index.dat
  - \Documents and Settings\<Username>\Local Settings\History\History.IE5\index.dat
  - \Documents and Settings\<Username>\Local Settings\History\History.IE5\MSHist012001123120020101\index.dat
  - \Documents and Settings\<Username>\Local Settings\History\History.IE5\MSHist012002010720020114\index.dat
  - \Documents and Settings\<Username>\Local Internet Files\Content.IE5\index.dat

Index.dat

- Windows 7
  - \Users\<Username>\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  - \Users\<Username>\AppData\Roaming\Microsoft\Windows\Cookies\low\index.dat
  - \Users\<Username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
  - C:\Users\<UserName>\AppData\Local\Microsoft\Windows\History\Content.IE5\index.dat

Live Windows

- Pslist: Process List
  - http://technet.microsoft.com/en-us/sysinternals/bb896682
- fport: Ports list
  - http://www.mcafee.com/us/downloads/free-tools/fport.aspx
- Pmdump
  - http://ntsecurity.nu/toolbox/pmdump/
- Sysinternals

Live
Windows. Memory

Memory dump: mdd

- http://www.forensicswiki.org/wiki/Tools:Memory_Imaging
- http://sourceforge.net/projects/mdd/files/mdd/mdd-1.3/mdd_1.3.exe/download
- $ mmd –o memdump

Image analysis: Volatility

- https://www.volatilesystems.com/VolatileWeb/volatility.gsp
- http://code.google.com/p/volatility/wiki/CommandReference

$ volatility pslist -f memdump

Name	Pid	PPid	Thds	Hnds	Time
System	4	0	55	259	Thu Jan 01 00:00:00 1970
smss.exe	532	4	3	19	Mon Nov 10 17:50:51 2008
csrss.exe	596	532	11	350	Mon Nov 10 17:50:53 2008
winlogon.exe	620	532	17	441	Mon Nov 10 17:50:53 2008
services.exe	664	620	15	244	Mon Nov 10 17:50:54 2008
lsass.exe	676	620	22	348	Mon Nov 10 17:50:54 2008

Live
Windows. Memory

Volatility

connections	Print list of open connections
connscan	Scan for connection objects
connscan2	Scan for connection objects (New)
datetime	Get date/time information for image
dlllist	Print list of loaded dlls for each process
psscan	Scan for EPROCESS objects
psscan2	Scan for process objects (New)
raw2dmp	Convert a raw dump to a crash dump
regobjkeys	Print list of open regkeys for each process
sockets	Print list of open sockets
files	Print list of open files for each process
hibinfo	Convert hibernation file to linear raw image
memdmp	Dump the addressable memory for a process

HELIX

Initialize Client:

- export safe="/mnt/cdrom"
- export nc="/mnt/cdrom/ -w 3 192.168.1.253 65534"
- $safe/bash # trusted shell
- export PATH=$safe # clear path

Initialise Server (for each command):

- nc -l -p 65534 >> forensics.data.txt

Files and Network Connections

- $safe/lsof -nDr | $nc # open files
- $safe/netstat -nap | $nc # network connections
- $safe/netstat -nr | $nc # routes
- $safe/ils -o /dev/hdaN |$nc #deleted & open files

Live Linux

Processes

- $safe/ps -leaf | $nc # solaris: suspect processes
- $safe/ps -auxl | $nc # linux: suspect processes

Users

- $safe/who -Hl | $nc # active users
- $safe/tar cf - /proc | $nc # system info

Swap space (already have /proc/kcore)

- $safe/dd if=/dev/SWAPdev bs=2k | $nc # swap space

MBR

- dd if=/dev/hda of=/media/disk/mbr.dd bs=512 count=1

Temporary partition

- $safe/dd if=/dev/TMPdev bs=2k | $nc # temp partition

File access times

- $safe/ls -alRu / | $nc # access times
- $safe/ls -alRc / | $nc # modification times
- $safe/ls -alR / | $nc # creation times

Is possible do this process with any automated form?

Linux-ir (Linux)

Forensics

ÁNALISIS DE MALWARE

Análisis de Malware

- Objetivo: Entender las funcionalidades de un malware
- El número de especímenes crece rápidamente
  - ¿Porqué analizarlos? Conseguir información sobre:
  - ¿Cuál es el objetivo?
  - ¿Cómo?
  - ¿Quién?
  - ¿Como se puede borrar?
  - ¿Qué se ha borrado?
  - ¿Cómo se propaga?

Análisis de Malware

- Análisis de comportamiento/entorno
  - Ejecución de malware en un entorno aislado
  - Uso de sensores

- Análisis de código
  - El código puede o no ejecutarse
  - Se estudia todo
  - En muchas ocasiones hay que desensamblar
  - Hay que tener encuenta técnicas como ofuscación o packing

Análisis de Malware

- Análisis estático
  - Examinar el malware sin ser ejecutado
- Análisis dinámico
  - Ejecución del malware en entornos controlados

Análisis de Malware

- Herramientas
- Process Explore
- Process Monitor
- Registry Monitor/Regshot
- TCPview
- Capturebat/wireshark
- Servidores Fake

Análisis de Malware
Packers

- Los binarios que contienen pocas palabras suelen presentarse con un packer.
- UPX es un compresor de código muy utilizado como packer.
- Un ejecutable “packeado” tiene dos componentes:
  - Una rutina para packear
  - El código original packeado
- Las secciones .text, .data, .idata pasan a UPX1
- La rutina tambien se almacena en UPX1
- UPX está vacía
- UPX contiene tablas de importación y datos
- PEid es una buena herramienta para detectar packers

Análisis de Malware

- ¿Qué es un entry point (OEP)?
- Lugar donde el progrma empieza su ejecución
- En el caso de programas packeados el OEP es el inicio del unpacking. Una vez finaliza la rutina se salta al código original
  - JMP, SEH, CALL, RET

Análisis de Malware.
Behavioral analysis

1. Fingerprint: md5sum
2. Antivirus: www.virustotal.com
3. Registry changes: Regmon
4. System info: Process Monitor
5. Capture traffic: CaptureBat/wireshark
6. Simulate servers: Mailpor, Fake DNS

- " A disassembler will take a binary and break it down into human readable assembly."(static analysis)
- With a debugger we can step through, break and edit the assembly while it is executing (dynamic analysis).

Análisis de Malware.
Behavioral analysis

Interesting tools for preliminar forensic analysis:

http://download.sysinternals.com/Files/SysinternalsSuite.zip

Filemon.exe: Allows us to "strace -eopen,read,write..."

Regmon.exe: Monitors windows registry accesses
Tcpview.exe: "netstat -tunl" equivalent, can kill connections
Procexp.exe: Allows us to attach to a process using windbg
WinObj.exe: Displays NT objects.

Análisis de Malware.
Code analysis

- Windows Live Messenger
  - Compiled windows executables
  - No source code
- Getting ready:
  - Have a prepared Lab
  - Support for snapshots
  - Mitigate the risk of malware attempting to escape

Análisis de Malware.
Code analysis

1. Fingerprint: md5sum
2. Antivirus: www.virustotal.com
3. Details about the PE: PEiD.
    1. Is it Packed?
4. Readable code: strings
5. More Details about the PE: PEview
    1. Imports
    2. Exports
    3. Metadata
    4. Resources
6. Disassembly

Análisis de Malware.
Code analysis

- http://zeltser.com/reverse-malware/reverse-malware-cheat-sheet.html

  Es una especie de intérprete de código de aplicación

- Each OS has its own system calls.
- An assembler program cannot be ported.

Análisis de Malware.
Code analysis

- **Olly Debug (dynamic code abalysis)**
- Search for->All referenced text strings
- Test vs Hello
- Look for strings and find the code that uses them:
  - “Hello” is not found
- Run
- Goal: Set a break point
  - Locate in memory- Alt-M ->Memory map
    - Binary search-Crtl+B, Crtl+L (Next) (Go back to the memory window)
    - Breakpoint->Memory on access

Análisis de Malware.
Code analysis

- **Olly Debug (dynamic code analysis)**

- Execute just one instruction
  - Debug->Step into
  - CMP->Compares data(‘t’ vs ‘g’)->test vs name
  - CL is part of ECX
  - BL is part of EBX

Manuel García-Cervigón