

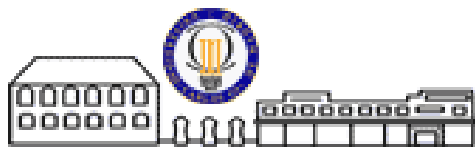
UNIVERSIDAD CARLOS III DE MADRID



Entorno de Recogida de Evidencias Digitales y Análisis

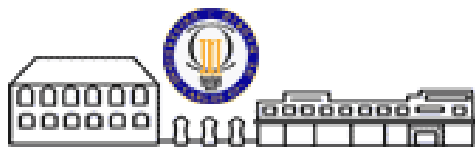
EnREDA

gt 2005
Red IRIS



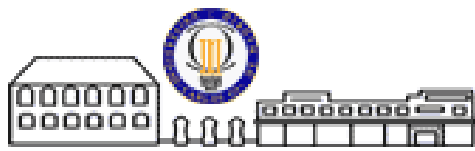
Motivación

- Necesidad de realizar análisis forense
 - Englobado dentro de la respuesta a incidentes
 - Para aprender los métodos/herramientas empleados por los intrusos
- Disponer de una herramienta automatizada
 - Gestionada por la comunidad
 - Adaptada a nuestro entorno
 - “kit de análisis” recomendado
- Análisis de sistemas vivos y muertos



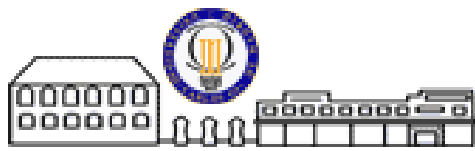
Objetivos

- Análisis de sistemas vivos
 - Windows, Linux, etc
 - Recoger evidencias volátiles (procesos, controladores del S.O., etc)
- Análisis de sistemas muertos
 - CD-Live basado en Linux
- Emplear programas opensource o al menos gratuitos
- Automatizar todo lo posible



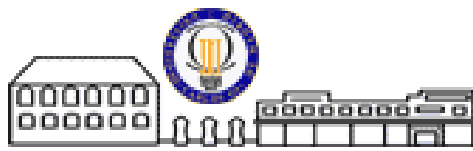
Situación Actual

- Versión 0.0.3a
 - De uso interno. Orientada a Windows
 - Análisis de sistemas Windows en vivo
 - Script .bat para recogida de datos
 - CD-Live basado en GNU/Debian Sarge (kernel 2.6.11)
 - Autopsy, chntpwd y poco más
 - Utiliza bootcdwrite para crear la imagen ISO



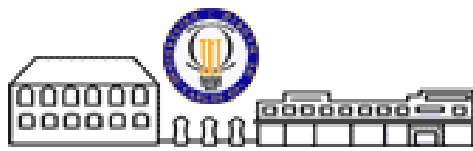
Líneas de investigación

- Imagen ISO
 - Mejorar la creación (usar cloop, etc)
- ¿Otros soportes?
 - ¿Disquete con soporte para USB?
 - ¿Disco USB?
 - ¿256MB, 512MB,...?
- ¿Versiones especializadas?
 - Poca RAM, SMP, etc



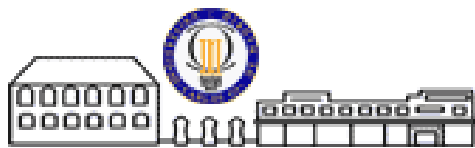
Método de trabajo

- Desarrollo
 - Repositorio CVS para almacenar cambios
 - Pendiente de seleccionar ubicación
 - Lista de correo para desarrolladores
- Gestión de bugs y petición de funcionalidades
 - Portal BSCW (o WiKi) alojado en RedIRIS
- Anuncios y comunicación con usuarios
 - Lista ANAFON e IRIS-CERT(sólo anuncios)



Formas de colaboración

- **Platinum (alias desarrollador):**
 - Scripts de detección de hw
 - Scripts de recogida/análisis de evidencias
 - Creación de la imagen ISO
- **Gold (alias compromisario):**
 - Propuesta/Selección de herramientas a incluir
- **Silver (alias tu mismo)**
 - Beta tester
 - Notificación de fallos
- **Bronce (alias tímido)**
 - No dice que lo usa



Referencias

- Foro de Seguridad de RedIRIS
 - <http://www.rediris.es/cert/doc/reuniones/#fs>
- Revista *Digital Investigation*
 - <http://www.elsevier.com/locate/diin>
- Open source forensics tools
 - http://www.digital-evidence.org/papers/opensrc_legal.pdf
- Custom Live Linux CD
 - <http://souptonuts.sourceforge.net/cdrom.htm>