Introducción al cómputo forense

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
http://homepage.cem.itesm.mx/rogomez

Definición computo forense

- Se refiere al proceso de aplicar técnicas científicas y analíticas a infraestructura de cómputo, para identificar, preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal.
- ¿Que clase de evidencia ?
  - La computadora involucrada de forma directa.
  - La computadora involucrada de forma indirecta.
- Meta: reconstrucción de eventos pasados

¿Qué ofrece el análisis forense?

- El análisis forense informático se aplica una vez que tenemos un incidente y queremos investigar qué fue lo que pasó, quién fue y cómo fue
- Responder a las preguntas W5:
  - ¿Quién?
  - ¿Qué?
  - ¿Cuándo?
  - ¿Dónde?
  - ¿Por qué?
- Reconstrucción de eventos

Lámina 3 Dr. Roberto Gómez Cárdenas

¿Por qué investigar?

- Determinar
  - ¿Cómo entró?
  - ¿Qué daños cometio?
    - Información expuesta
    - Información robada
    - Información borrada
    - Daños a terceros
  - Deslindar responsabilidades
  - Apoyar al ministerio público
  - ¡Saber exactamente qué paso!

Lámina 4 Dr. Roberto Gómez Cárdenas

¿Quién requiere del cómputo forense?

- ¡La víctima!
  - Personas físicas
  - Personas morales
  - Gobierno
- Los cuerpos policíacos
- Las compañías de seguros
- El sistema legal

Lámina 5 Dr. Roberto Gómez Cárdenas

¿A qué se le puede hacer cómputo forense?

- Computadoras
- PDA's
- Cámaras digitales
- Discos duros externos
- Memory sticks
- Impresoras
- Celulares

Lámina 6 Dr. Roberto Gómez Cárdenas

Algunas noticias

Colombia: Interpol asegura autenticidad de las computadoras de "Raúl Reyes"

Infolatam
Bogotá, 15 de mayo 2008

"Nadie puede cuestionar nunca si Colombia manipuló esa evidencia incautada", dijo el secretario general de **Interpol** en rueda de prensa en Bogotá, tras entregar el informe de la organización internacional sobre los computadores.

Noble declaró que estaba convencido de que los equipos que analizó Interpol (tres computadoras) fueron incautados en un campamento de las FARC. "Vinieron de un campamento terrorista de las FARC, así que le pertenecían a la organización y a miembros esa organización", dijo **Noble**, quien enseguida fue contra preguntado por un periodista a qu miembro del grupo delictivo. "Específicamente al señor **"Reyes"**, que está muerto, pero definitivamente eran sus computadores, sus discos, su equipo físico y él es (era) el representante de las FARC y el responsable de su contenido", respondió **Noble.**

El funcionario entregó el informe al director de la Policía colombiana, general **Óscar Naranj** la directora del Departamento Administrativo de Seguridad (DAS, inteligencia estatal), María Pilar Hurtado, y al fiscal general, **Mario Iguarán**, en presencia del canciller, **Fernando Araújo**

En su documentación, y luego ante cerca de 200 periodistas y cámaras, **Noble** insistió en qu 64 expertos, de quince países, trabajaron durante más de cinco mil horas en las ocho "prue documentales decomisadas", compuestas por tres computadoras portátiles, tres unidades memoria USB y dos discos externos.

"Ni muertas" dejan de hablar las computadoras

Mie 12 de Agosto de 2009 a las 09:25 AM

Para cerrar la serie de reportajes sobre seguridad informática que hemos estado publicando esta semana, ahora compartiremos uno de Jorge Chávez Morales, periodista venezolano del diario Últimas Noticias, donde profundiza en la informática forense. Si no sabes qué es eso, te invitamos a leer este interesante trabajo que te explica cómo las computadoras no dejan de hablar "ni muertas"...

En marzo de 2008, la certificación que la Policía Internacional (Interpol) hizo en Colombia de los archivos que contenían las computadoras que presuntamente le fueron decomisadas al asesinado líder de las Fuerzas Armadas Revolucionarias de Colombia (Farc), Raúl Reyes, puso sobre el tapete dos palabras que para muchos eran desconocidas: "Informática Forense".

Lámina 7 Dr. Roberto Gómez Cárdenas

Ejemplos casos (i)

- Agosto 1986.- Caso Iran-Contras
- Tte. Coronel Oliver North escribió unos correos electrónicos que le involucraban en el caso
- Borro los correos de su ordenador
- No se percató que se hacían copias de respaldo de sus mensajes
- Los mensajes se recuperaron de los servidores de respaldo

Lámina 8 Dr. Roberto Gómez Cárdenas

Ejemplos casos (ii)

- 1991.- Caso Guttman
- La esposa de Guttman apareció muerta con una nota de suicidio sin firmar, escrita por ordenador con una impresora matricial
- El ordenador de Guttman NO contenía rastros del documento
- Guttman tenía una amante.
- Se registró la casa de la amante.
- Encontraron un disco flexible de 5 ¼ cortado en pedazos
- Se reconstruyó físicamente el disco y se recuperaron los datos con un programa llamado Anadisk

Lámina 9 Dr. Roberto Gómez Cárdenas

Evidencia

- “Certeza clara, manifiesta, de una cosa”
- Aquellos elementos que nos proporcionan información, que nos permite soportar conclusiones, hallazgos y recomendaciones.
- La evidencia puede ser de varios tipos:
  - Directa
  - Circunstancial
  - Concluyente
  - Pericial
  - ...

Lámina 10 Dr. Roberto Gómez Cárdenas

Evidencia

- Para que la evidencia sea admisible, debe ser:
  - Suficiente - ¿existe suficiente evidencia para convencer a una persona "razonable" de la validez de los hallazgos?
  - Relevante - ¿tiene la evidencia una relación sensible y lógica con el hallazgo?
  - Competente - ¿es la evidencia consistente con los hechos? ¿es válida? ¿se genera en el curso normal del negocio?
  - Y por supuesto, legalmente obtenida

Lámina 11 Dr. Roberto Gómez Cárdenas

Evidencia digital

- Evidencia digital o electrónica es MUY frágil.
- Mantener la integridad de la escena del crimen.
- Datos admisibles ante un juez.
- La evidencia volatil es aquella que desaparecerá rápido, como ser conexiones activas de red, procesos en lamemoria, archivos abiertos, etc.
- Lo que se haga, técnicamente va a afectar la evidencia.
  - Ejecutar el comando ps en UNIX sobreescribirá partes de la memoria.
  - Se puede sobreescribir la historia de comandos.
  - Se pueden afectar las fechas de acceso a los archivos.
  - Existe el riesgo de programas "troyanos" y de "rootkits".

Lámina 12 Dr. Roberto Gómez Cárdenas

Principio Heisenberg del análisis del sistema.

- Mundo real: imposible saber tanto el momento como la ubicación; examinando uno afecta al otro
- Computadoras: examinar o recolectar una parte del sistema afectara a otros componentes del sistema. Es imposible capturar el sistema entero en cualquier punto del tiempo.

Lámina 13 Dr. Roberto Gómez Cárdenas

Tipos de análisis forense

- Análisis de intrusión
- Evaluación de daños
- Investigación de sospechosos
- Análisis de herramientas
- Análisis de bitácoras
- Búsqueda de evidencia

Lámina 14 Dr. Roberto Gómez Cárdenas

Análisis de Intrusión

- ¿Quién logró entrar?
- ¿Qué fue lo que hicieron?
- ¿Cuándo ocurrió el evento?
- ¿Adonde más fueron?
- ¿Por qué escogieron el blanco?
- ¿Cómo realizaron esto?

Lámina 15 Dr. Roberto Gómez Cárdenas

Evaluación de Daños

- ¿Qué pudo ver el intruso?
- ¿Qué se llevo?
- ¿Qué fue lo que dejó detrás?
- ¿Adonde se fué?

Lámina 16 Dr. Roberto Gómez Cárdenas

Recuperación de Archivos

- Archivos borrados
- Archivos escondidos
- Slack space
- Bloques dañados
- Esteganografía
- X-Drives

Lámina 17 Dr. Roberto Gómez Cárdenas

Análisis de Herramientas

- ¿Qué herramientas usó el atacante?
- ¿Cómo se utilizaron?
- ¿En que lenguaje están escritas?
- Comparación de la herramienta vs. archivos del sospechoso.

Lámina 18 Dr. Roberto Gómez Cárdenas

Análisis de Bitácoras

- Eventos
  - Monitoreo
  - ¿Qué información se puede obtener?
- ¿FW/Router/Server?
- ¿Tripwire?
- ¿Modem/FTP/Telnet/Ras?

Lámina 19 Dr. Roberto Gómez Cárdenas

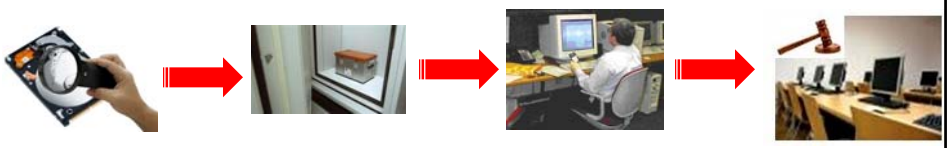
Búsqueda de Evidencia

- Archivos de imágenes
- Software
- Archivos borrados
- Archivos escondidos
- Encriptados
- Particiones escondidas
- Palabras claves
- Herramientas de acceso remoto

Lámina 20 Dr. Roberto Gómez Cárdenas

El proceso forense

- Cuatro pasos



Identificar evidencia

Preservar evidencia

Analizar evidencia

Presentar evidencia

Lámina 21 Dr. Roberto Gómez Cárdenas

Identificar la evidencia

- Los equipos que pueden contener evidencia, reconociendo la frágil naturaleza de los datos digitales
- Identificar la información que se encuentra disponible.
- Determinar la mejor forma de recolectarla.
  - ¿Qué tipo de información está disponible?
  - ¿Cómo la podemos “llevar” de forma segura?.
  - ¿Qué puede formar parte de la evidencia?

Lámina 22 Dr. Roberto Gómez Cárdenas

¿Dónde puede residir?

- Discos rígidos.
  - Archivos de SWAP.
  - Archivos temporales.
  - Espacio no asignado en el disco.
  - Espacio File-Slack.
- Memoria y procesos que se encuentran ejecutando.
- Diskettes, CD-ROMS, DVD's, ZIP, Jazz, Tapes.
- Archivos de bitácoras
- Respaldos
- PDA's.
- Memory Stick's.

Lámina 23 Dr. Roberto Gómez Cárdenas

Preservar la evidencia

- Con la menor cantidad de cambios (contaminación).
- El forense debe poder demostrar su responsabilidad en cualquier cambio que tenga la evidencia.
- ¿Cómo demostrar que lo que se tiene como evidencia es exactamente igual a lo que originalmente se recolectó

Lámina 24 Dr. Roberto Gómez Cárdenas

Puntos a considerar

- Se debe tratar de no realizar ningún cambio sobre la misma.
- Se deben registrar y justificar todos los cambios.
- Realizar un by-pass del sistema operativo y crear por “fuera” un backup de toda la evidencia.
- Las copias duplicadas deben ser escritas en otro disco rígido o CD-ROM.
- Se debe realizar una documentación de todo el proceso de la generación de imágenes.
- Se deben autenticar todos los archivos e imágenes utilizadas con obtención de huellas digitales.

Lámina 25 Dr. Roberto Gómez Cárdenas

Orden de volatilidad

Registros	Nanosegundos
Memoria principal	Nanosegundos
Estado red	Milisegundos
Procesos corriendo	Segundos
Disco	Minutos
Floppies, medios de respaldo, etc	Años
CD-ROMS, impresiones	Decenas años

Lámina 26 Dr. Roberto Gómez Cárdenas

Analizar la evidencia

- Extraer, procesar e interpretar.
- La extracción puede obtener solo imágenes binarias, que no son comprendidas por los humanos.
- La evidencia se procesa para poder obtener información que entiendan los investigadores.
- Para interpretar la evidencia se requiere conocimiento profundo para entender como embonan las piezas.
- El análisis efectuado por el forense debe poder ser repetido.

Lámina 27 Dr. Roberto Gómez Cárdenas

Presentar la evidencia

- Abogados, fiscales, jurado, etc.
- La aceptación dependerá de factores como:
  - La forma de presentarla (¿se entiende?, ¿es convincente?)
  - El perfil y credibilidad del expositor.
  - La credibilidad de los procesos usados para preservar y analizar la evidencia.
    - Aumenta si se pueden duplicar el proceso y los resultados.
- Especialmente importante cuando la evidencia se presenta en una corte

Lámina 28 Dr. Roberto Gómez Cárdenas

Requerimientos investigador forense digital

- Conocimiento técnico
- Conocer las implicaciones de sus acciones
- Entender como los datos pueden ser modificados
- Ingenioso, mente abierta
- Etica muy alta
- Educación continua
- Siempre usa fuentes altamente redundantes de datos para obtener sus conclusiones.

Lámina 29 Dr. Roberto Gómez Cárdenas

Certificación y entrenamiento

- International Association of Computer Investigative Specialists (IACIS)
  - Creado por loa oficiales de policía que deseaban formalizar credenciales en investigaciones computacionales.
  - Certified Electronic Evidence Collection Specialist (CEECS)
  - Certified Forensic Computer Examiners (CFCEs)

http://www.iacis.com

Lámina 30 Dr. Roberto Gómez Cárdenas

Certificaciones

- High-Tech Crime Network (HTCN)
  - Certified Computer Crime Investigator, Basic and Advanced Level
  - Certified Computer Forensic Technician, Basic and Advanced Level
- EnCase Certified Examiner (EnCE) Certification
- AccessData Certified Examiner (ACE) Certification
- Otros entrenamientos y certifcaciones
  - High Technology Crime Investigation Association (HTCIA)

Lámina 31 Dr. Roberto Gómez Cárdenas

Otros entrenamientos y certificaciones

- SysAdmin, Audit, Network, Security (SANS) Institute
- Computer Technology Investigators Network (CTIN)
- NewTechnologies, Inc. (NTI)
- Southeast Cybercrime Institute at Kennesaw State University
- Federal Law Enforcement Training Center (FLETC)
- National White Collar Crime Center (NW3C)

Lámina 32 Dr. Roberto Gómez Cárdenas

El laboratorio forense

- La mayor parte de la investigación se lleva a cabo en un laboratorio.
- El laboratorio debe ser seguro, de tal forma que la evidencia no se pierda, corrompa o destruya.
- Proporcionar un ambiente físico seguro.
- Llevar un control de inventario de sus activos.
  - Estar conscientes de cuando ordenar más suministros.

Lámina 33 Dr. Roberto Gómez Cárdenas

El laboratorio forense

- Laboratorio de computo forense
  - Donde se va a llevar a cabo su investigación.
  - Almacenar evidencia.
  - Donde se quedará el equipo, hardware y software
- La American Society of Crime Laboratory Directors (ASCLD) , ofrece guías sobre
  - Administración de un laboratorio.
  - Adquirir una certificación oficial.
  - Auditar funciones y procedimientos del laboratorio.

Lámina 34 Dr. Roberto Gómez Cárdenas

Requerimientos seguridad del laboratorio

- Facilidades seguridad.
  - Debe preservar la integridad de la evidencia.
- Requerimientos mínimos.
  - Pequeño cuarto con paredes de piso a techo.
  - Acceso a través de una puerta con mecanismo de bloqueo.
  - Contenedores seguros.
  - Bitácora de visitantes.
- Gente trabajando juntas debe contar con el mismo nivel de acceso.
- Informar al staff acerca de las políticas de seguridad.

Lámina 35 Dr. Roberto Gómez Cárdenas

Conduciendo investigaciones de alto riesgo

- Investigaciones de alto riesgo requieren más seguridad que los requerimientos mínimos de un laboratorio.
  - Instalaciones TEMPEST
    - A prueba de radiación electromagnetica, (EMR).
  - Las instalaciones TEMPEST son caras
    - Posible usar estaciones de baja emanación.

Lámina 36 Dr. Roberto Gómez Cárdenas

Contenedores de evidencia

- Conocidos como lockers de evidencia.
  - Deben ser lo suficientemente seguros para que personas no autorizadas puede acceder a la evidencia.
- Recomendaciones para asegurar contenedores de almacenamiento.
  - Ubicarlos en un área restringida.
  - Número limitado de personas autorizadas a acceder los contenedores.
  - Mantener registros de quien esta autorizado a acceder que lockers.
  - Contenedores deben permanecer bloqueados/cerrados cuando no se estén usando.

Lámina 37 Dr. Roberto Gómez Cárdenas

Políticas cerrojos contenedores

- Sistema de combinación.
  - Proporcionar el mismo nivel de seguridad para las combinaciones que para el contenido de los contenedores.
  - Destruir las combinaciones después de configurar una nueva combinación.
  - Solo personal autorizado puede cambiar la combinación.
  - Cambiar la combinación cada seis meses o cuando se requiera.
- Sistema en base a llaves.
  - Designar un guardia de la llave.
  - Escribir números secuenciales en cada duplicado de llave.
  - Registro de que llave se le ha asignado a que persona.
  - Cambiar cerrojos y llaves cada año.

Lámina 38 Dr. Roberto Gómez Cárdenas

Laboratorio pequeño o casero

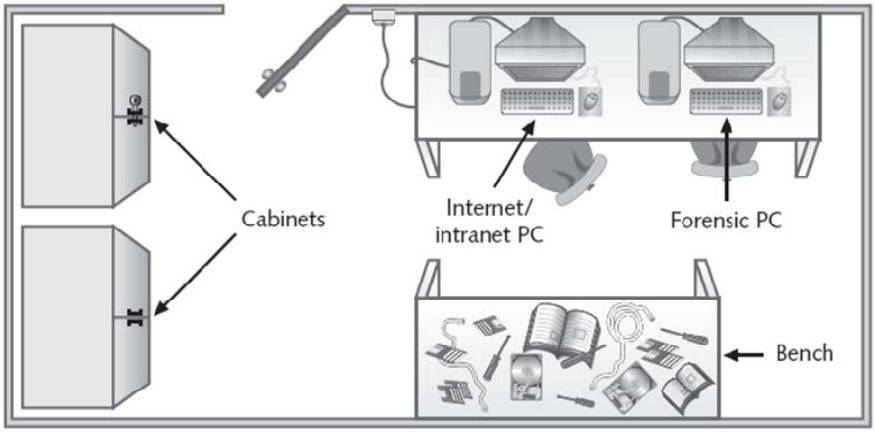


Lámina 39 Dr. Roberto Gómez Cárdenas

Laboratorio mediano

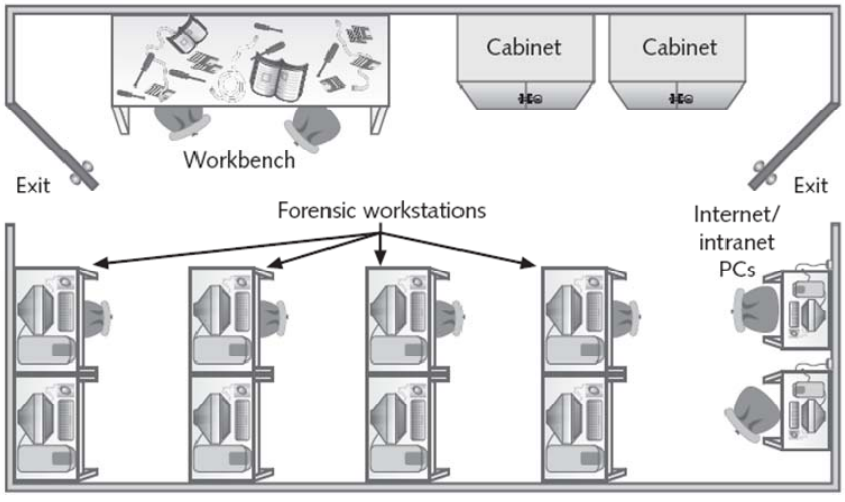


Lámina 40 Dr. Roberto Gómez Cárdenas

Laboratorio regional

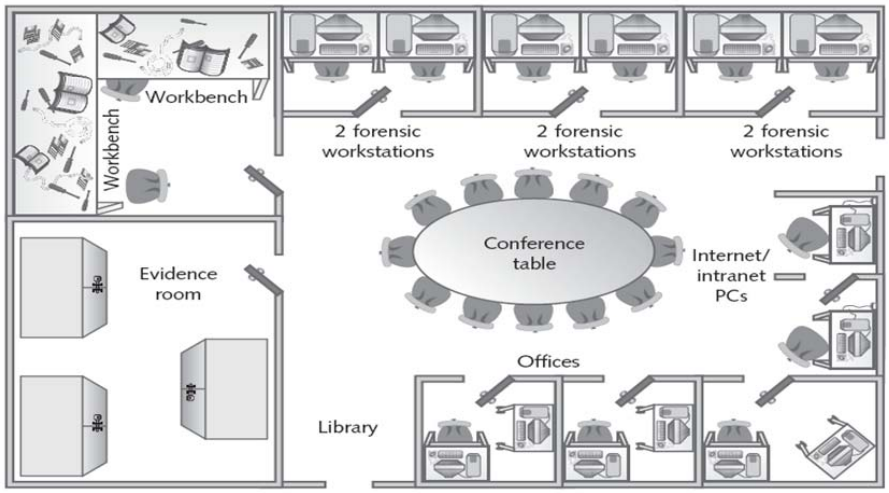


Lámina 41 Dr. Roberto Gómez Cárdenas

Imagenes de un laboratorio forense

Lámina 42 Dr. Roberto Gómez Cárdenas

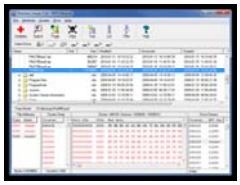
Software necesario

- Contar con licencias de softtware como
  - Microsoft Officce 2007, 2010, XP, 2003, 2000, 97 y 95.
  - Quicken
  - Lenguajes de programación
  - Visualizadores especializados
  - Corel Office Suite
  - StarOffice/OpenOffice
  - Aplicaciones de contabilidad de Peachtree

Lámina 43 Dr. Roberto Gómez Cárdenas

Mas software

- Directory Snoop (FAT, NTFS)
  - http://www.briggsoft.com
- ThumbsPlus (Imagenes)
  - http://www.cerious.com
- WinHex y X-Ways
  - http://www.winhex.com
- Mount Image
  - http://www.mountimage.com
- LiveView
  - http://liveview.sourceforge.net/
- Autopsy Forensic Browser
  - http://www.sleuthkit.org/autopsy/



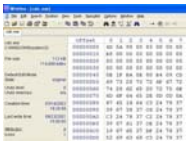
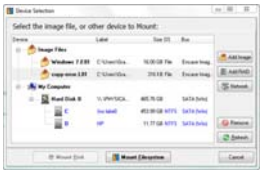
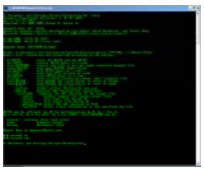
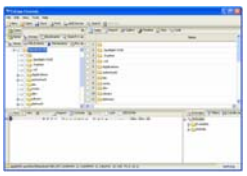



Lámina 44 Dr. Roberto Gómez Cárdenas

Aún más software

- Forensic Acquisition Utilities
  - http://gmgsystemsinc.com/fau/
- Encase
  - http://www.guidancesoftware.com/
- FTK
  - http://www.accessdata.com/
- ProDiscover Forensics
  - http://www.techpathways.com/prodiscoverdft.htm
- Net Witness
  - www.netwitness.com/
- Xplico
  - http://www.xplico.org/

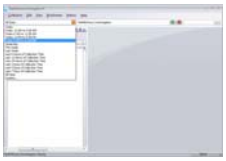




Lámina 45 Dr. Roberto Gómez Cárdenas

Pequeña recomendación

¡No usar software pirata!

Lámina 46 Dr. Roberto Gómez Cárdenas

Hardware necesario

- Cualquier laboratorio debe tener
  - Cables IDE
  - Cables Ribbon
  - Tarjetas SCSI
  - Tarjetas gráficas, de tipo PCI y AGP
  - Cables de electricidad.
  - Discos duros
  - Al menos dos adaptadores IDE/ATA o SATA para discos duros de Notebook.
  - Herramientas



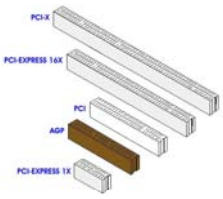




Lámina 47 Dr. Roberto Gómez Cárdenas

Bloque escritura hardware

- Dispositivo que se conecta a un sistema computacional con el propósito primario de interceptar y prevenir (o bloquear) cualquier comando de modificación del dispositivo de almacenamiento.
- Físicamente, el dispositivo es conectado entre la computadora y el dispositivo de almacenamiento.
- Algunas de sus funciones abarcan monitoreo y filtrado de cualquier actividad que es transmitida o recibida entre su interfaz de conexión y la computadora y el dispositivo de almacenamiento.

Lámina 48 Dr. Roberto Gómez Cárdenas

Ejemplo bloqueadores

- Forensic SATA Bridge
- Forensic IDE Pocket Bridge

Lámina 49 Dr. Roberto Gómez Cárdenas

Disco de booteo (live) de forensia

- Usado para arrancar sistemas sospechoso de forma segura
- Contiene un sistema de archivos y utilidades ligadas estáticamente, (p.e. ls, fdisk, ps, nc, dd, ifconfig, etc.)
- Reconoce particiones largas (+2Gb o +8Gb)
- Deja el medio en un estado de bloqueado o de solo lectura
- No hace ningún swap de datos al medio sospechoso.

Lámina 50 Dr. Roberto Gómez Cárdenas

Ejemplos CD Live

- Helix
  - http://www.e-fense.com/helix/
  - Creado a partir de Knoppix
- Trinux
  - http://trinux.sourceforge.net/
- BartPE
  - http://www.nu2.nu/pebuilder/
- FIRE
  - http://fire.dmzs.com/
- DEFT
  - http://www.deftlinux.net/
- CAINE
  - http://www.caine-live.net/

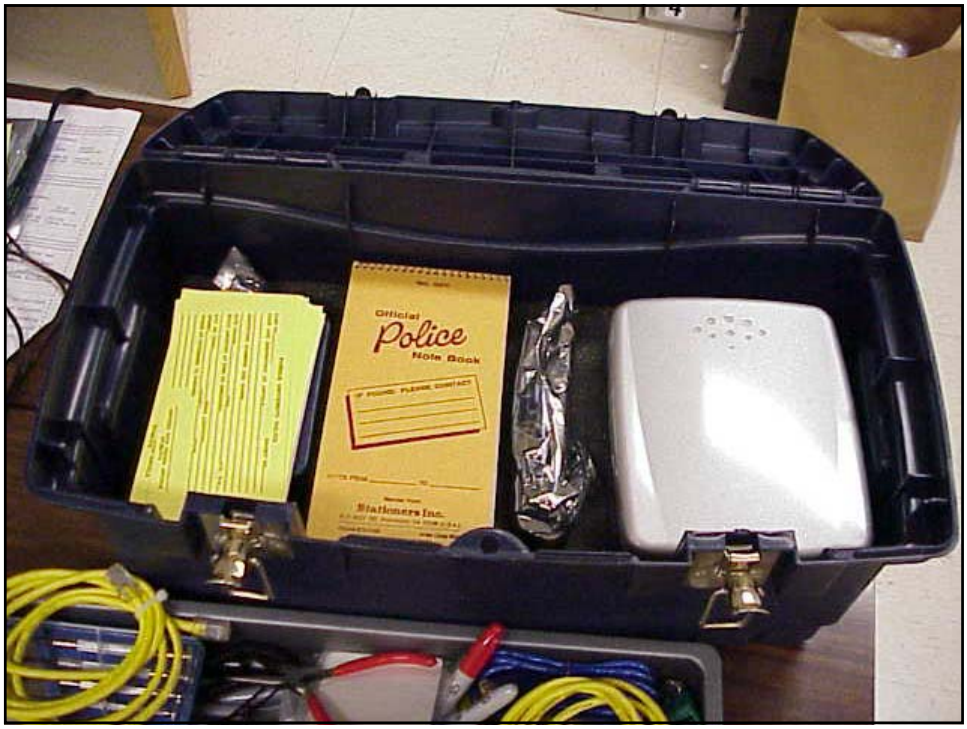
Lámina 51 Dr. Roberto Gómez Cárdenas

Forensics toolkit

- Herramientas de documentación
  - Etiquetas cables
  - Marcadores permanentes
  - Etiquetas stick-on
- Herramientas de desemblaje y de borrado
  - Desarmadores de todo tipo y variedad
  - Cortadores de cables
  - Correas antiestáticas
  - Pequeñas cintas

Lámina 52 Dr. Roberto Gómez Cárdenas


3
2
4


Official
Police
Note Book
Stationers Inc.

Suplementos de empaquetamiento y transporte

- Bolsas antiestáticas
- Cables para atar
- Bolsas de evidencia
- Cinta para empacar
- Cinta de evidencia
- Cajas resistentes de varios tamaños
- Cinta de embalaje

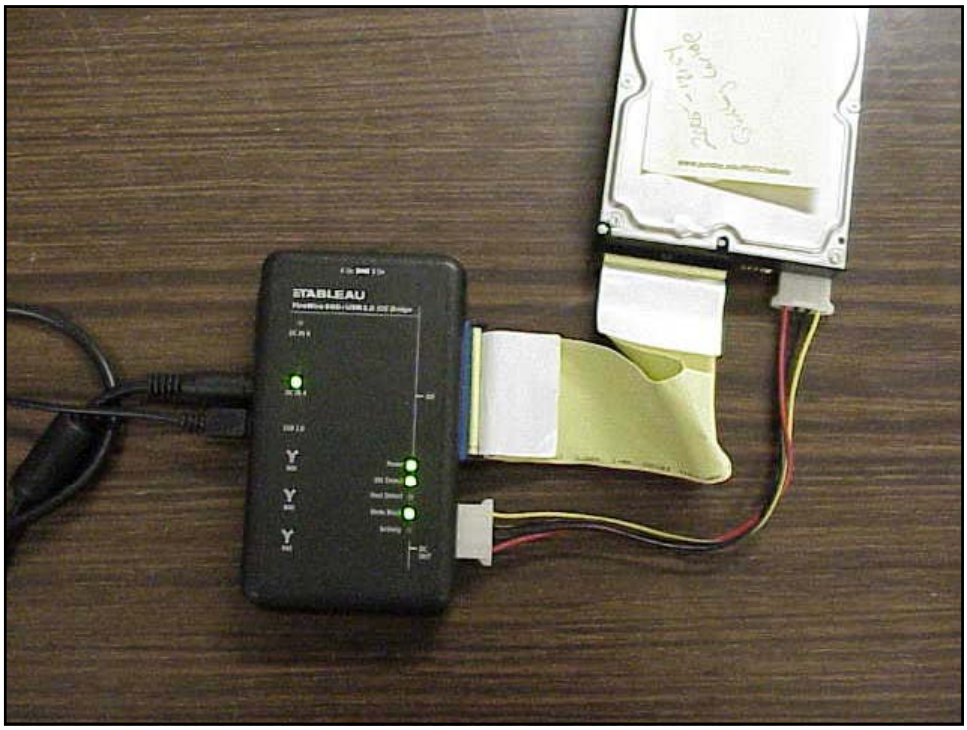
Lámina 59 59 Dr. Roberto Gómez Cárdenas

Otros

- Guantes de goma
- Lista de teléfonos de contactos para asistencia
- Ligas grandes
- Lupa
- Papel para imprimir
- Lámpara pequeña
- Medios de almacenamiento removibles (CD, DVD, etc)
- Discos duros en blanco

Lámina 60 60 Dr. Roberto Gómez Cárdenas


Digital Intelligence
UltraKit



TABLEAU


DC IN A
USB 2.0
800
800
400
IDE
Power
IDE Detect
Host Detect
Write Block
Activity
DC
OUT


Digital Intelligence
www.digitalintel.com
UltraBlock - SATA
FireWire800+USB2.0 Serial ATA Bridge
DC INPUT: +5V 2.0A +12V 2.0A
DC OUTPUT (max): +5V 1.0A +12V 1.0A
+12V +5V
GND
GND
GND
+12V
+5V
CAUTION:
Do not plug/unplug the DC Out connector while the "Power" LED is illuminated.
Powered by:
TABLEAU


Digital Intelligence
www.digitalintel.com
UltraBlock - SCSI
FireWire800+USB2.0 SCSI Bridge
DC INPUT: +5V 2.0A +12V 2.0A
DC OUTPUT (max): +5V 1.0A +12V 1.0A
+12V +5V
GND
GND
GND
+12V
+5V
CAUTION:
Do not plug/unplug the DC Out connector while the "Power" LED is illuminated.
Powered by:
TABLEAU
Tableau, LLC
www.tableau.com

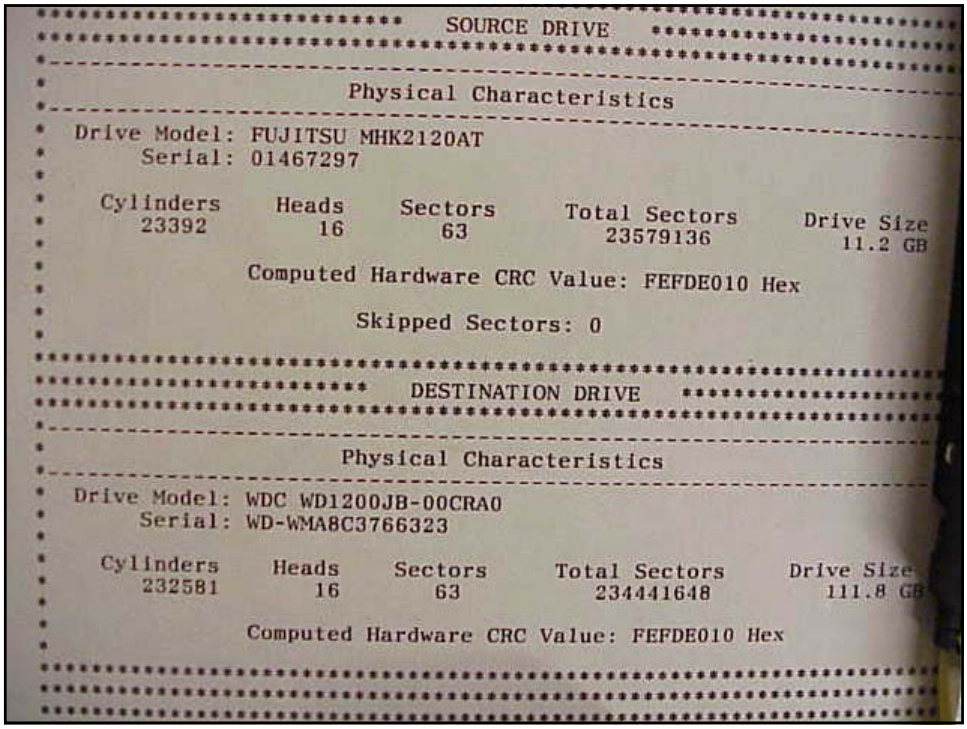

UltraBlock
Digital Intelligence
READ ONLY

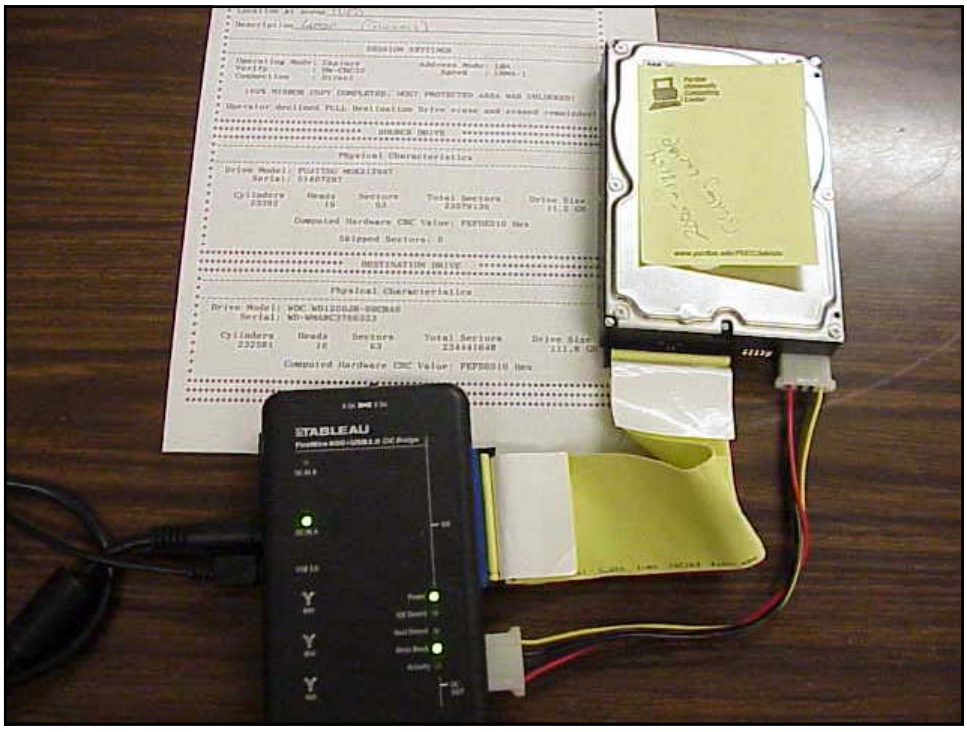

TABLEAU
Forensic USB Bridge
DC IN
Host Detect
Power
Write Block
Activity
Menu
Enter
Device Detect
ON
OFF
USB 2.0


4


Canon
BJC-85


Logicube SF-5000
LOGICUBE FORENSICS HARD DRIVE CAPTURE SYSTEM
BACK
ERROR STATUS POWER
SELECT
HELP
START
STOP
SET


SOURCE DRIVE
Physical Characteristics
Drive Model: FUJITSU MHK2120AT
Serial: 01467297
Cylinders 23392
Heads 16
Sectors 63
Total Sectors 23579136
Drive Size 11.2 GB
Computed Hardware CRC Value: FEFDE010 Hex
Skipped Sectors: 0
DESTINATION DRIVE
Physical Characteristics
Drive Model: WDC WD1200JB-00CRA0
Serial: WD-WMA8C3766323
Cylinders 232581
Heads 16
Sectors 63
Total Sectors 234441648
Drive Size 111.8 GB
Computed Hardware CRC Value: FEFDE010 Hex



TABLEAU


Introducción al computo forense
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
http://homepage.cem.itesm.mx/rogomez
Lámina 77
Dr. Roberto Gómez Cárdenas