Construyendo un Laboratorio Forense Básico en Computación

Agente del Servicio Secreto
Michael S. Morris

Director de Laboratorio - NTRCFL

Temas

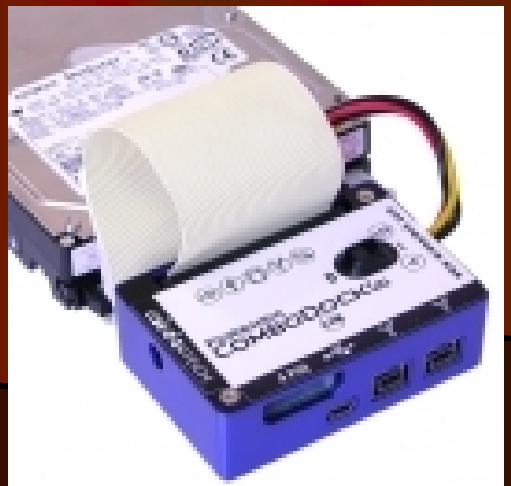
- Espacio del Laboratorio
- Equipos Necesarios
- Software Necesario
- Suministros Necesarios
- Entrenamiento
- Procedimientos

Espacio del Laboratorio

- Seguro
- Electricidad adecuada para los equipos
- Temperatura adecuada, humedad baja para los equipos
- Escritorios/bancos para el análisis forense y para las labores administrativas
- Cuartos para guardar material bajo llave, o contenedores para las pruebas, tanto originales como derivadas
- Conexión a Internet

Equipo – Bloqueador de Escritura (Write Blocker)

- Hardware bloqueador de escritura
  - Funciona con todo tipo de discos duros
  - www.wiebetech.co



	Serial ATA (SATA)	FireWire 400	FireWire 800	USB2	Peak Rate (MB/s)	3.5" IDE Drives	2.5" Notebook Drives	3.5" & 2.5" SATA Drives	1" Drives	1.8" Drives	Bus Powered	Bootable	Chipset
	Host Side					Drive Side							
ComboDock v4 CDKV4			2	1	57	●	●*	●*	●*	●*		●	922
FireWire DriveDock v4 FWDDV4		2		1	34	●	●*	●*	●*	●*		●	911+
Super DriveDock+ SDP			2	1	57	●	●*	●*	●*	●*	●	●	922
Notebook DriveDock v4 NBDV4		2		1	29		●				●	●	911+
SATADock v4 SDKV4			2	1	60			●				●	924
SATADock Bus Power SDK-BP			2	1	60			●			●	●	922
Mini SATADock MSD	1				65			●				●°	—
Mini USBDock MBD				1	30			●					S.I.
Forensic Write-Blocking Docks													
Forensic OfficeDock FOD			2		57	●	●*	●*	●*	●*			922
Forensic ComboDock FCD			2		57	●	●*	●*	●*	●*			922
Forensic ComboDock Bus Power FCD-BP			2		57	●	●*	●*	●*	●*	●		922
Forensic DriveDock+ FODDP		2			34	●							911
Forensic Notebook DriveDock+ FONBP		2			29		●				●		911
Forensic SATADock FSDK			2		60			●					922

* With Combo Adapter
° If supported by host

Equipo – Computadores de Análisis forense

- Usted querrá los computadores más rápidos que pueda comprar, que tengan:
  - RAM – Tanto RAM como el equipo permita, y tanto como usted pueda comprar
  - CPU – Quad, o al menos CPU's Dual Core
  - Una buena tarjeta de video, tarjeta de sonido, parlantes
  - Fire wire 800, 400
  - USB 2
  - Drives DVD/CD-RW y DVD/CD-R
  - Pantalla grande
  - Impresoras

Computadores de Análisis Forense

- Actualmente evaluando el Apple GS5 y el Apple Raid
- Puede iniciarse tres veces (Tri Boot) y correr software de Apple, Windows, y Linux en el mismo equipo

Computadores de Análisis - Almacenamiento

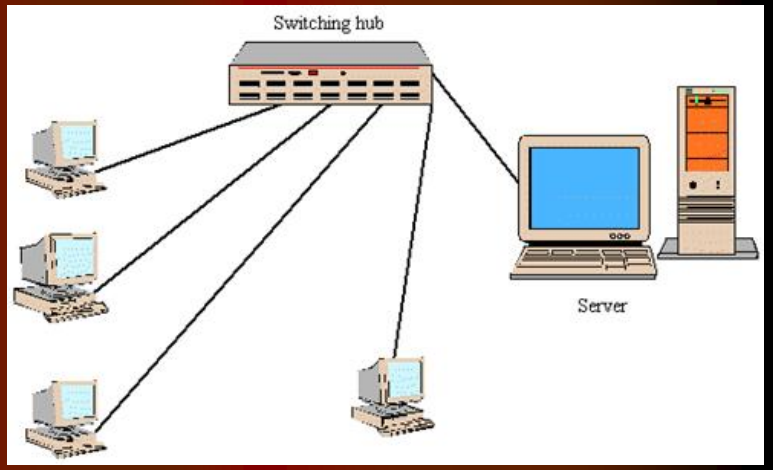
- Los discos duro de 1 Terabyte ya están disponibles. ¿Cuánto es eso?
  - 1 millón de fotos
  - 16 días de video en calidad DVD
  - 1 millón de minutos de música

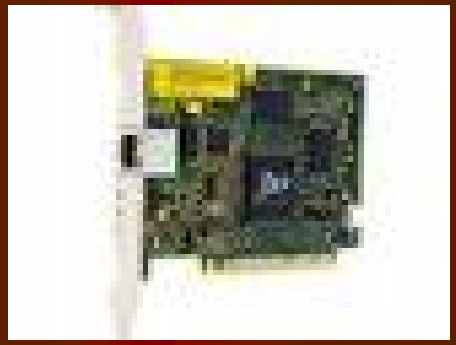
Computadores de Examen - Almacenamiento

- Es necesario medir el almacenamiento con base en lo que estén usando los sujetos.
- Con los discos duros de 1 TB ahora a la venta, conseguiría por lo menos 10 a 20 TB, o tantos como el presupuesto lo permita.
- Si hay más de un analista forense, recomiendo comprar algún tipo de almacenamiento en red (NAS, SAN); también se pueden usar discos duros
  - Posibles vendedores (hay muchos otros en el mercado)
    - Apple xraid
    - Raid Inc. falcon
    - Compellent SAN

Equipo de Red

- Interruptor (*switch*) de red, cableado, tarjetas de red para trabajo forense
- Otro juego completo para Internet y un firewall, se pueden combinar firewall/router/switch



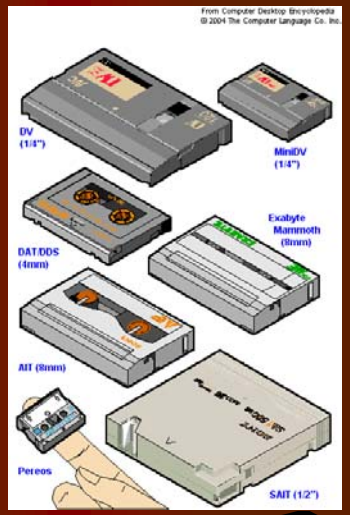


Equipo – Teléfonos celulares / PDAs

- Cada teléfono y PDA usa conectores de datos diferentes, al igual que cargadores eléctricos diferentes.
- Puede pensar en itips para las necesidades eléctricas.
- Cables de soporte para los cables de datos telefónicos.
- También necesitará algún tipo de cubrimiento para bloquear señales al realizar análisis de teléfonos celulares: Faraday Bag.

Equipo – Drive de Cinta (Tape Drive)

- Las cintas vienen en todos los tipos y tamaños
  - DLT/SDLT
  - DDS/DAT
  - LTO
- Se usan para leer las cintas de los sujetos, y para archivar productos del trabajo



Software Forense

- Protección contra virus
  - Symantec
  - McAfee
- Paquetes forenses
  - Encase
  - FTK
    - FTK
    - PRTK
    - Registry Viewer
  - Ilook
  - Black Bag – Apple
- Teléfonos celulares
  - Data pilot
  - Mobil edit – forensic
  - Simmus
  - bkforensics
  - Software suministrado por el fabricante del teléfono
- Software de Sistema Fantasma
  - Symantec – Ghost
- Herramientas forenses gratuitas - www.acesle.org

Suministros

- Administrativos – papel, lapiceros, etc.
- Forense
  - Cables para los equipos
  - CD-Rs, DVD-Rs, y estuches para ellos
  - Cintas
  - Discos duros
  - Paquete de herramientas
  - Linterna
  - Bolsas estáticas de plástico, y envolturas de burbujas
  - Etiquetas – CD/DVD y ordinarias
  - Cartuchos para las impresoras

Entrenamiento - Mínimo

- Hardware de computador / Redes
  - A+; Net+
- Conocimiento básico de herramientas forenses informáticas
  - Asociación Internacional de Especialistas en Investigación por Computador (IACIS)
  - NW3C – BDRA, ADRA (Recuperación de Datos Básica/Avanzada)
- Entrenamiento para herramientas específicas
  - Encase
  - FTK
  - Ilook
- Entrenamiento jurídico – Órdenes de registro, testigos, problemas informáticos y normas sobre delitos informáticos en su país.
- El campo forense informático requiere aprendizaje diario; la tecnología cambia todos los días
- Evaluación – Cada analista forense, antes de realizar análisis, debe tomar y pasar un examen de competencia, para demostrar que entiende tanto los principios forenses como el uso de las herramientas.

Políticas de Laboratorio

- Un laboratorio debe establecer y seguir un conjunto de políticas y procedimientos sobre el manejo del laboratorio y sobre la manera de realizar análisis en general.
- Bases
  - Cadena de custodia y protección de las pruebas
    - Pruebas originales
    - Pruebas derivadas
    - Todas las pruebas con las que trabaje el analista deben llevar sus iniciales, la fecha, y el nombre del caso escrito con tinta indeleble sobre la prueba.
    - Cadena de custodia (quién, qué, cuándo, dónde, por qué)
  - Apuntes de análisis
  - Reportes de análisis
  - Resumen del trabajo hecho en el laboratorio
    - Revisión técnica de los apuntes de análisis
    - Revisión administrativa del reporte de análisis

Apoyo en el Laboratorio

- Grupo Científico de Trabajo sobre Pruebas Digitales (SWGDE) http://ncfs.org/swgde
- **Sociedad Americana de Directores de Laboratorios sobre Delitos / Comité de Acreditación de Laboratorios – Internacional** http://www.ascld-lab.org/

Procedimientos en el Laboratorio – Análisis

- Los análisis no deben realizarse sobre las pruebas originales; un bloqueador de escritura debe incorporarse al disco duro y una imagen verificada (MD5; SHA1) debe hacerse (DD, E01, etc.), con software de almacenamiento (Encase, FTK Imager, DD, etc.).
- La computadora de análisis usado para el análisis debe ser recargado (Symatec Ghost) entre exámenes, con una carga base y software anti-virus actualizado (Symantec, McAfee)
- Los hallazgos (archivos de interés) deben grabarse en un CD-R, o un DVD-R, y los discos deben ser finalizados (de tal manera que nada más pueda grabarse al disco)
- Después del análisis, el archivo de imagen usado para el examen debe ser re-validado para demostrar que el análisis no lo corrompió
- Todas las actuaciones del analista deben ser registradas en sus apuntes. Los apuntes deben llevar sus iniciales en cada página, las páginas deben ser numeradas “1 de ____”, y deben mostrar el número del caso.

¿¿ Preguntas ??

Agente del Servicio Secreto Michael S. Morris
Michael.morris@ic.fbi.gov