Guía de Implementación de un Laboratorio de Informática Forense

Computer Forensics Lab – Hardware and Software Guidelines

Autor: Leopoldo Sebastián Gómez - Argentina

1) Servidor del Laboratorio

Requerimientos mínimos: Este servidor actuará funcionalmente equiparado a un NAS para el almacenamiento de evidencia digital, casuística y reportes técnicos. Asimismo, se utilizará para la ejecución de máquinas virtuales y para operaciones que demanden tiempo de cómputo intensivo. Deberá tener un espacio de almacenamiento de 4,5 Tb en discos SAS, los que se dividirán en dos zonas (grupos lógicos). La primera zona se implementará como un RAID-1E de 1,5 Tb (o sea que ya utilizó 3 de los 4,5). Este repositorio se utilizará para almacenar información de los casos trabajados (ej. informes técnicos, dictámenes) y selectivamente alguna evidencia digital que sea conveniente resguardar porque puede ser objeto de un peritaje posterior. La segunda zona tendrá un RAID-0 de 750 Gb (o sea 1,5 Tb que quedaban de los 4,5) y se utilizará principalmente como repositorio de trabajo temporal, para actividades forenses específicas: ej. carving e indexados.

Recomendaciones

a) Se estima que $s 20.000 son suficientes para un Laboratorio de Informática Forense que comienza sus actividades. Puede adquirirse un Servidor Blade, ej. IBM Blade Center "S", con una o dos hojas Blade como máximo. Estos equipos son escalables.
b) El servidor deberá tener preferentemente un S.O. que brinde servicios de Terminal Server para inicio de sesiones remotas. Se recomienda Windows Server 2008.
c) Se requieren UPS acordes al Servidor del Laboratorio. Si se utiliza un Blade Center "S", podrán utilizarse UPS estándares del mercado, que son de costo moderado. Ej. marca APC.

2) Red interna de laboratorio de tipo Gigabit Ethernet

Requerimientos Mínimos: Red local aislada y de uso exclusivo del Laboratorio, Gigabit Ethernet.

Recomendaciones: Se estima en función de los puestos de trabajo se requieren pero no supone mayores costos. (Rack + Switch + Placas de Red para cada puesto + Cableado Estructurado + Red eléctrica separada para conexión de para equipos informáticos).

3) Protectores contra escritura (Write Blockers) & Duplicadores

Requerimientos Mínimos

- Tableau T8 (U$s 269,15 por unidad)
- Tableau TD1 (U$s 1314 por unidad)
- Disk Jockey Pro Forensic Kit (U$s 657,85 por unidad)

Recomendaciones: Se debe estimar U$s 5000 en este rubro para una suite de productos de trabajo típicos.

4) Telefonía celular

Requerimientos Mínimos

- Caja de Faraday para el Laboratorio (U$s 1495 por unidad)
- Bolsas de Faraday (U$s 30 por unidad)
- Device Seizure Toolbox (U$s 750 por unidad)
- Lector de memorias + Cargador externo (U$s 50)
- CSI Stick (U$s 299 por unidad)

Recomendaciones

a) Se debe estimar U$s 4000 en este rubro para una suite de productos de trabajo típicos.
b) Existen Forensic Kits de Hardware + Software que disminuyen sensiblemente los costos de adquisición. Ej. Device Seizure Field Kit de Paraben (U$s 3495).

5) Equipo Informático Forense Móvil

Requerimientos mínimos: Se debe prever una notebook, una impresora portátil y otros materiales típicos para el trabajo de campo (ej. allanamientos), al que se sumará eventualmente parte del equipo forense del punto 3 y 4.

Recomendaciones

a) Se debe estimar U$s 3000 por notebook que requiera para procedimientos judiciales, U$s 300 por impresora portátil, y U$s 500 para otros elementos operativos (caja de herramientas, pinzas, destornilladores, cables de datos, etc.). No se debe gastar más dinero en este ítem porque la mayor parte del trabajo se realiza en el Laboratorio.
b) En caso de realizar un procedimiento judicial se debe planificar el trabajo de campo ya que es probable que se requieran elementos de almacenamiento de evidencia digital adicionales.

6) Equipo Informático Forense para Laboratorio (Forensic Workstation)

Requerimientos mínimos: Memoria RAM de 4 Gb o superior, Monitor LCD 22", RAID-0 de 750 Gb o superior, placa de red Ethernet Gigabit, Sistema Operativo Windows Vista Ultimate.

Recomendaciones

a) Se debe estimar U$s 3.500 por puesto de trabajo.
b) Los equipos deben tener las interfaces para conexión de dispositivos externos, ej. USB, P-ATA, S-ATA, FIREWIRE, etc.
c) También se debe contemplar que en gran parte de los casos la evidencia digital se almacena temporariamente en el RAID-0 del Laboratorio que actúa como repositorio compartido. Puede aprovecharse la potencia de cómputo de las hojas Blade del Servidor del Laboratorio, estableciendo una sesión remota mediante Terminal Services.

7) Periféricos del Laboratorio

Requerimientos mínimos: Impresora laser con conexión a red de buen rendimiento en Blanco y Negro, y una impresora color de un costo que no sea elevado ya que tendrá menor uso. Cámara digital de costo moderado.

Recomendaciones: Se debe estimar U$s 6.000 para estos periféricos.

8) Software Forense

Requerimientos mínimos: puede utilizarse software gratuito como Helix, Liveview!, FTK Imager, etc.

Recomendaciones

a) EnCase: 1 Licencia por puesto de trabajo U$s 3000 + PLSP por 3 años U$s 3000
b) Device Seizure: depende del número de casos que deban trabajarse (como mínimo 1 Licencia, U$s 1095 + Suscripcion por 1 año U$s 220)
c) Mount Image Pro: depende del número de casos que deban trabajarse (como mínimo 1 licencia, U$s 299).
d) VMware Workstation: 1 Licencia por puesto de trabajo U$s 189

9) Entrenamiento Forense

Recomendaciones

Capacitación In Company: El instructor viaja a la institución e imparte un curso especializado con un programa predefinido. Se resuelven casos prácticos y se exponen dictámenes de peritajes informáticos. *El personal del laboratorio local queda capacitado en todos los aspectos esenciales sobre metodología de trabajo forense, técnicas de investigación de delitos con tecnología informática, y uso de hardware y software forense*. Duración: 5 días. Lenguaje: Español. Cantidad de asistentes: máximo 10 personas por curso.

Ventajas: Reduce los costos operativos cuando se debe capacitar a varias personas. Es posible armar el programa de entrenamiento a medida, según los temas que más interesen y los que requieran mayor atención, descartando todos aquellos que aún no tienen uso.

Instructor: Leopoldo Sebastián Gómez. Abogado (UCaSal-Argentina), Lic. En Ciencias de la Computación (UNS-Argentina), Magister en Ingeniería del Software (ITBA-Argentina), Posgraduado en Gestión y Calidad del Software (UPC-España), Master en Ingeniería del Software (UPM-España). Perito Informático Oficial – Poder Judicial – Argentina. Contacto: http://sebastiangomez.sytes.net

Los cursos se dictan durante el mes de Enero o Julio, a convenir.

Posibilidades de continuar el entrenamiento online mediante clases asincrónicas con videos, tutoriales, examen multiple choice, biblioteca digital forense y foros de consulta. Website: www.informaticapericial.com.ar