La investigación forense

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Rol del investigador forense

- Tomar evidencia para probar que un sospechoso cometió un crimen o violó la política de una organización.
- Colectar evidencia que se pueda presentar en una corte o en una investigación corporativa.
  - Investigar la computadora del sospechoso.
  - Preservar la evidencia en una computadora diferente.

Tipos de incidentes

- Violación de una política de la organización.
  - Puede costarle mucho dinero a la organización.
    - Navegación por internet, enviar correo personales, uso de recursos de la organización
- Despido de un empleado.
  - Abuso de los recursos de la organización.
- Investigaciones abogado-cliente
  - Todos lo que se encontro es confidencial
  - Educar abogados que la evidencia digital se puede ver electrónicamente.

Lámina 3 Dr. Roberto Gómez Cárdenas

Tipos de incidentes

- Fuga de información.
  - Control de información sensitiva puede ser difícil de implementar.
- Espionaje industrial
  - Deben ser tratados como una investigación criminal.

Lámina 4 Dr. Roberto Gómez Cárdenas

Preparando la investigación

- Seguir un procedimiento aceptado para preparar un caso.
- En algunos países existen documentos que explican la adquisición de evidencia electrónica.
- Cuidar la cadena de custodia.
  - La ruta que la evidencia toma desde el momento en que se encontró hasta que el caso es cerrado o se presenta en una corte.

Lámina 5 Dr. Roberto Gómez Cárdenas

Examinando un crimen computacional

- Las computadoras contienen información que ayuda a determinar
  - La cadena de eventos que llevo a un crimen.
  - Evidencia que puede llevar a una convicción.
  - Se debe seguir un procedimiento adecuado cuando se adquiera la evidencia.
  - La evidencia digital puede ser fácilmente alterada
  - La información en discos duros debe estar protegida con una contraseña.

Lámina 6 Dr. Roberto Gómez Cárdenas

Diagrama metodología usada

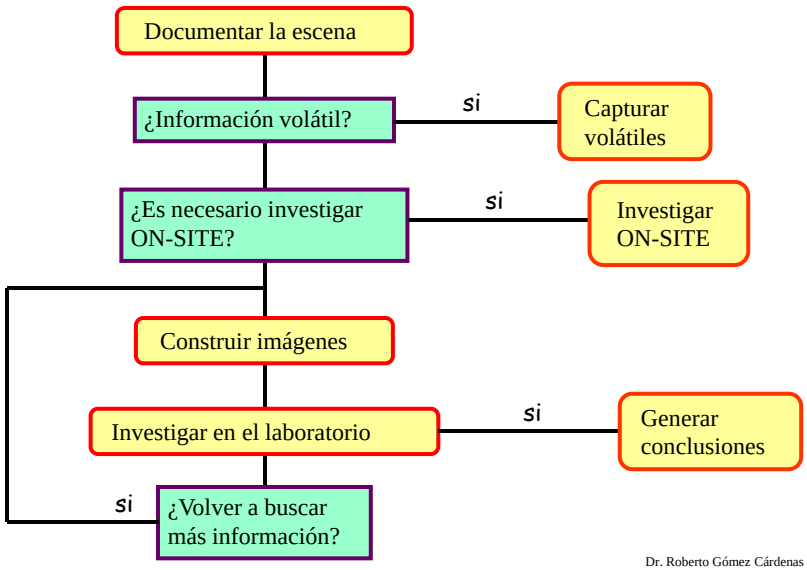


Lámina 7 Dr. Roberto Gómez Cárdenas

Examinando una escena de crimen

Lámina 8 Dr. Roberto Gómez Cárdenas

Forma de custodia de evidencia

- Ayuda a documentar que se ha hecho con la evidencia original y sus copias forenses.
- Dos tipos
  - Forma de evidencia simple.
    - Lista cada pieza de evidencia en una página separada.
  - Forma de multievidencia

Lámina 9 Dr. Roberto Gómez Cárdenas

Forma evidencia simple

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of __

Lámina 10 Dr. Roberto Gómez Cárdenas

Forma multi-evidencia

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence [illegible]		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page ___ of ___

Lámina 11 Dr. Roberto Gómez Cárdenas

Asegurando la evidencia

- Utilizar bolsas para asegurar y catalogar la evidencia.
- Utilizar productos para proteger evidencia digital
  - Bolsas antiestáticas
- Utilizar contenedores bien etiquetados
- Utilizar cinta de evidencia para sellar todos los contenedores.
  - Discos flexibles, CDs, o USBs
  - Cables de fuente de poder

Lámina 12 Dr. Roberto Gómez Cárdenas

Asegurando la evidencia

- Escribir sus iniciales en la cinta para probar que la evidencia no ha sido alterada.
- Considere rangos de temperatura y humedad de los dispositivos computacionales.

Lámina 13 Dr. Roberto Gómez Cárdenas

Entrevista vs interrogatorio

- El convertirse en un entrevistador y/o interrogador puede tomar varios años de experiencia.
- Entrevista
  - Usualmente llevada a cabo para colectar información sobre un sospechoso o víctima
- Interrogación
  - Hacer que un sospechoso confiese

Lámina 14 Dr. Roberto Gómez Cárdenas

Rol del investigador forense en un interrogatorio/entrevista

- Instruir a la persona responsable de conducir la entrevista acerca de las preguntas a realizar.
  - Y las repuestas a esperar
  - Puntos a considerar para una entrevista/interrogatorio
    - Tener paciencia a través de la sesión
    - Repetir o refrasear preguntas a
    - Ser tenaz

Lámina 15 Dr. Roberto Gómez Cárdenas

Entendiendo recuperación datos en estaciones de trabajo y software

- Investigaciones son conducidas en un laboratorio forense computacional (o laboratorio de recuperación de datos).
- Computo forense y recuperación de datos están relacionados pero diferentes.
- Estación de computo forense
  - Computadora personal especialmente configurada
  - Dotada de bahías adicionales y softtware adicional.
- Para evitar
  - Disco/USB de arranque forense
  - Dispositivos bloqueadores de escritura

Lámina 16 Dr. Roberto Gómez Cárdenas

Configurando la computadora para computo forense

- Requerimientos básicos
  - Una estación corriendo Windows, XP, Vista o 7
  - Dispositivo de bloqueador escritura.
  - Herramientas de adquisición de computo forense.
  - Herramientas de análisis de computo forense.
  - Drive específico para recibir los datos de la fuente o disco sospechoso.
  - Puertos Spare PATA SATA
  - Puertos USB

Lámina 17 Dr. Roberto Gómez Cárdenas

Configurando la computadora para computo forense

- Adicionales
  - Tarjeta de red (NIC = Network Interface Card)
  - Puertos USB extra
  - Puertos Fire/Wire 400/800
  - Tarjeta SCSI
  - Software de edición de disco.
  - Editor de textos
  - Programa de visualización de gráficos
  - Otras herramientas de visualización específica.

Lámina 18 Dr. Roberto Gómez Cárdenas

Conduciendo una investigación

- Tomar recursos identificados en el plan de investigación
- Artículos necesitados
  - Medio almacenamiento original.
  - Forma de custodia de la evidencia.
  - Contenedor de la evidencia que se encuentra en el medio de almacenamiento.
  - Herramienta de creación de imágenes.
  - Estación de trabajo forense para copiar y examinar la evidencia.
  - Locker seguro para almacenar evidencia.

Lámina 19 Dr. Roberto Gómez Cárdenas

Obteniendo la evidencia

- Evitar dañar la evidencia.
- Pasos a seguir:
  - Conocer al administrador de TI para entrevistarse con él.
  - Llenar la forma de custodia de evidencia y que la firme el administrador de TI.
  - Depositar la evidencia en un contenedor seguro.
  - Llenar la forma de custodia de evidencia.
  - Llevar la evidencia al laboratorio forense.
  - Crear copias forenses (si es posible).
  - Asegurar la evidencia, asegurando el contenedor con una llave o candado.

Lámina 20 Dr. Roberto Gómez Cárdenas

Obtención de evidencia volátil

- Tomar fotografía de lo que se ve en la computadora.
- "Vaciar" el estado de la computadora
  - Puertos abiertos
  - Procesos corriendo
  - Contenido de la RAM
  - Conexiones establecidas.
  - Linux y Unix: Variables de ambiente y directorio /proc
  - Windows: Contenido del registro.
- A notar
  - El ejecutar comandos alterara la RAM del dispositivo.

Lámina 21 Dr. Roberto Gómez Cárdenas

Ejemplo

- Contar con un medio que contenga herramientas básicas
  - El Microsoft Windows Command Prompt
    - cmd.exe
  - Forensic Acquisition Utilities
    - fau-1.3.0.2390a.zip
  - PsTools suite
    - PsTools.zip

Lámina 22 Dr. Roberto Gómez Cárdenas

¿Qué recopilar?

- Fecha y hora de contacto
  - Comandos date y time
- Nombre de la maquina
  - hostname
- Datos de la tarjeta de red
  - ipconfig
- ¿Quién esta conectado?
  - psloggendon.exe (parte de PsTools)
- Procesos ejecutándose
  - pslist (parte de PsTools)

Lámina 23 Dr. Roberto Gómez Cárdenas

Más información

- Sesiones actuales de netbios
  - nbtstat
- Conexiones red
  - netstat
- Aplicaciones asociadas a los puertos abiertos
  - tcpvcon –anc (paquete TCPView)
- Comandos tecleados
  - doskey /h
- Huella digital de todo lo tecleado
  - md5sums
  - sha256sum

Lámina 24 Dr. Roberto Gómez Cárdenas

Imágenes de información en disco

- Objetivo:
  - Obtener una copia exacta (bit a bit) de la información almacenada en un dispositivo de almacenamiento.
- Primer regla del computo forense
  - Preservar la evidencia original
- Llevar a cabo el análisis solo en la copia de los datos.
- Usar herramientas para comenzar a trabajar sobre la evidencia.

Lámina 25 Dr. Roberto Gómez Cárdenas

Copias bit-stream

- Copia bit-stream
  - Copia bit-a-bit del medio de almacenamiento original.
  - Copia exacta del disco original.
  - Diferente de una copia de respaldo.
    - Software de respaldo solo copia archivos conocidos.
    - Software de respaldo no puede copiar archivos borrados, mensajes de correo electrónico o recuperar fragmentos de un archivo.
- Imagen bit-stream
  - Archivo que contiene una copia bit-stream de todos los datos que se encuentran en un disco o partición.
  - También conocida como copia forense.

Lámina 26 Dr. Roberto Gómez Cárdenas

Copias bit-stream

- Copiar el archivo con la imagen a un disco que cuente con las características del disco original (tamaño, modelo)

Disco original Disco imagen Disco de trabajo

Lámina 27 Dr. Roberto Gómez Cárdenas

Formatos de evidencia digital

- Tres formatos
  - Raw
  - Propietario
  - Advanced Forensics Format (AFF)

Lámina 28 Dr. Roberto Gómez Cárdenas

Raw Format

- Hace posible escribir datos de stream de bits a archivos.
- Ventajas
  - Rápida transferencia de datos.
  - Puede ignorar errores menores de adquisición de datos de un drive.
  - La mayor parte de las computadoras pueden leer archivos con este formato.
  - Extensión del archivo: .dd

Lámina 29 Dr. Roberto Gómez Cárdenas

Desventajas formato raw

- Requiere tanto almacenamiento como el disco o dato originales.
- Las herramientas puede no colectar sectores marginales o malos.

Lámina 30 Dr. Roberto Gómez Cárdenas

Datos propietarios

- Características ofrecidas
  - Opción para comprimir o no comprimir archivos de imágenes.
  - Puede dividir una imagen en pequeños archivos segmentados.
  - Puede integrar metadatos en el archivo que contiene la imagen.
- Desventajas
  - No es posible usar la misma imagen con diferentes herramientas.
  - Tamaño de archivo limitado por cada volumen segmentado.

Lámina 31 Dr. Roberto Gómez Cárdenas

Advanced Forensics Format

- Desarrollado por Dr. Simon L. Garfinkel de Basis Technology Corporation.
- Objetivos de diseño
  - Proporcionar archivos de imágenes comprimidos o no comprimidos.
  - No restricción de tamaño para archivos de imágenes de disco.
  - Proporciona espacio en el archivo de imágenes o archivos segmentados para metadatos.
  - Diseño simple con extensión.
  - Open source para múltiples plataformas y Sistemas Operativos.
  - Verificación de consistencia interna para auto-autenticación.

Lámina 32 Dr. Roberto Gómez Cárdenas

Advanced Forensics Format

- Extensiones de archivos incluyen:
  - .afd para archivos de imágenes segmentadas
  - .afm para metadatos AFF
- AFF es open source
- AF4: completo rediseño del formato AFF

Lámina 33 Dr. Roberto Gómez Cárdenas

Formato gfzip

- Generic Forensic Zip file format.
- Pretende proporcionar un formato abierto de archivos para archivos de imágenes de disco comprimidos y firmados.
- Utiliza huellas digitales SHA256 para integridad

Lámina 34 Dr. Roberto Gómez Cárdenas

Formatos específicos a un software

- Encase
- ILookInvestigator IDIF, IRBF e IEIF
- ProDiscover
- PyFlag's sgzip
- Rapid Action Imaging Device (RAID)
- Safeback
- SDi32
- SMART

Lámina 35 Dr. Roberto Gómez Cárdenas

EnCase

- Basado en el formato ASR Data's Expert Witness Compression Format.
- Archivo de evidencia .e01 contiene el stream de bits de un disco, precedido de un encabezado "Case Infro", intercalado con CRCs para cada bloque de 64 sectores y seguido por un hash MD5 de todo el bitstream.
  - En el encabezado se encuentra la fecha y hora de adquisición, el nombre del examinador, notas de la adquisición y opcionalmente una contraseña.
  - El encabezado termina con su propio CRC.

Lámina 36 Dr. Roberto Gómez Cárdenas

ILookInvestigator

- Tres tipos de formatos de imágenes propietarios
  - Comprimido (IDIF)
  - No comprimido (IRBF)
  - Cifrado (IEIF)

Lámina 37 Dr. Roberto Gómez Cárdenas

ProDiscover

- Utilizado por la familia de herramientas de seguridad de Technology Pathways ProDiscover Family
- El archivo consiste de cinco partes
  - Encabezado de archivo de imagen de 16 bytes:
    - Firma, número de versión de la imagen
  - Encabezado de Imagen de 681 bytes
    - Metadatos de la imagen capturados por el usuario.
  - Los datos de la imagen
  - Arreglo de tamaños bloques comprimidos
    - Si los datos de la imagen están comprimidos
  - Bitácoras de errores
    - Describen cualquier problema que se haya presentado durante la creación de la imagen.

Lámina 38 Dr. Roberto Gómez Cárdenas

Determinando el mejor método de adquisición

- Tipo de adquisiciones
  - Adquisiciones estáticas y adquisiciones en vivo
- Cuatro métodos
  - Bit-stream disk a archivo imagen.
  - Bit-stream disco-a-disco.
  - Adquisición disk-to-disk or disk-to-disk data.
  - Copia de datos esparcidos de un archivo o folder.

Lámina 39 Dr. Roberto Gómez Cárdenas

Bit-stream a archivo imagen.

- Método más común.
- Se puede hacer más de una copia
- Las copias son replicas bit-a-bit del drive original.
- Herramientas:
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook

Lámina 40 Dr. Roberto Gómez Cárdenas

Bit-stream disco-a-disco

- Cuando la copia de disco-a-imagen no es posible.
- Considerar la configuración de la geometría del disco.
- Herramientas
  - EnCase
  - SafeBack
  - SnapCopy

Lámina 41 Dr. Roberto Gómez Cárdenas

Adquisición lógica vs esparcida

- Adquisición lógica
  - Solo se capturan archivos específicos relacionados con el caso que se esta investigando.
- Adquisición esparcida
  - Similar a la adquisición lógica pero también recolecta fragmentos de datos no asignados, i.e. datos borrados.

Lámina 42 Dr. Roberto Gómez Cárdenas

Consideraciones

- Cuando se lleva a cabo una copia hay que considerar:
  - Tamaño del disco fuente
    - Comprensión sin perdida (lossless compression) puede ser útil.
    - Utilizar firmas digitales para verificación
  - Cuando se trabaja con drives muy grandes, una alternativa es usar sistemas de respaldos basados en cinta.
  - Se debe conservar el disco original.

Lámina 43 Dr. Roberto Gómez Cárdenas

Contingencia para adquisición de imágenes

- Crear un duplicado del archivo que almacena la imagen de la evidencia.
- Crear con al menos dos imágenes de la evidencia digital.
  - Utilizar diferentes herramientas o técnicas.
- También copiar la parte protegida del disco
- Estar preparados para enfrentarse a dispositivos cifrados.
  - Windows 7 y Vista cuentan con la posibilidad de cifrar todo el disco.

Lámina 44 Dr. Roberto Gómez Cárdenas

Herramientas de adquisión

- USBs
- Linux Boot CD
- Herramientas
  - ProDiscover
  - FTK
  - EnCase

Lámina 45 Dr. Roberto Gómez Cárdenas

Validación adquisición datos

- Aspecto critico computo forense
- Requiere usar un algoritmo hash
- Técnicas válidas
  - CRC-32, MD5, and SHA-1 to SHA-512

Lámina 46 Dr. Roberto Gómez Cárdenas

Adquisición remota

- Se puede conectar vía remota a una computadora sospechosa y copiar datos de ella.
- Herramientas varían en configuraciones y capacidades.
  - Ejemplo: netcat
- Desventajas
  - Velocidades de transferencia
  - Conflictos tabal de rutero
  - Permisos necesarios para acceder a redes/subredes aseguradas.
  - Tráfico pesado puede causar problemas.

Lámina 47 Dr. Roberto Gómez Cárdenas

Analizando la evidencia digital

- El objetivo es recuperar información de
  - Archivos borrados
  - Fragmentos de archivos
  - Archivos completos
- Archivos borrados permanecen en el disco hasta que nuevos datos son almacenados en la misma ubicación física.

Lámina 48 Dr. Roberto Gómez Cárdenas

Adquisición datos en RAID

- El tamaño es el principal problema
  - Muchos sistemas RAID alamcenan terabytes de datos.

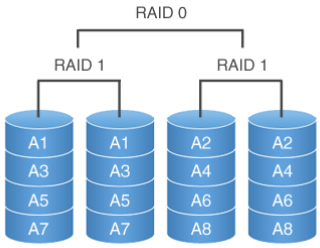


Lámina 49 Dr. Roberto Gómez Cárdenas

Entendiendo sistemas RAID

- Redundant Array of Independent (Inexpensive) Disk
- Sistema de almacenamiento que usa múltiples discos duros o SSD entre los que distribuye o replica los datos
- Originalmente desarrollado como una medida de redundancia de datos.
- Combina varios discos duros en una sola unidad lógica.
  - Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo.

Lámina 50 Dr. Roberto Gómez Cárdenas

Niveles raid

- Son las distintas configuraciones que soporta.
- La elección de los diferentes niveles de RAID va a depender de las necesidades del usuario en lo que respecta a factores como seguridad, velocidad, capacidad, coste, etc.
- Cada nivel de RAID ofrece una combinación específica de tolerancia a fallos (redundancia), rendimiento y coste, diseñadas para satisfacer las diferentes necesidades de almacenamiento.
- La mayoría de los niveles sólo pueden satisfacer 1 o 2 de estos aspectos.

Lámina 51 Dr. Roberto Gómez Cárdenas

Raid 0 o “striping”

- Los datos se rompen en grupos y se escriben en los discos que forman parte del conjunto.
- No proporciona redundancia o tolerancia al fallo.
- Aumenta el riesgo de fallo pero rendimiento es muy bueno, muy alta tasa de transferencia.
- Mínimo de dos unidades.

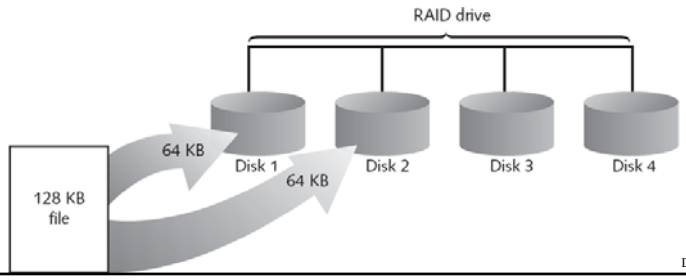


Lámina 52 Dr. Roberto Gómez Cárdenas

Raid 1 o disco espejo

- Escribe datos idénticos en cada uno de los discos.
- Simple y alto nivel de transferencia E/S.
- Mejora el rendimiento aplicaciones de lectura intensa.
- En caso de fallo se sigue trabajando con los discos no dañados sin detener el sistema.
- Bueno para servidores de archivos pequeños.
- Mínimo de dos unidades.

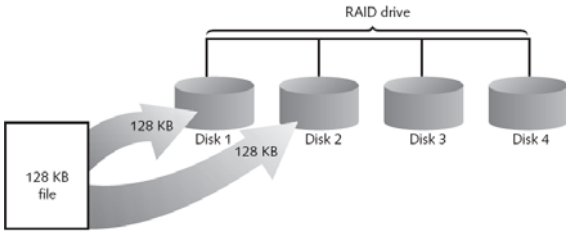


Lámina 53 Dr. Roberto Gómez Cárdenas

Raid 2

- Divide los datos a nivel de bits en lugar de a nivel de bloques
- Acceso paralelo con discos especializados.
- Código de Hamming para correción y detección de errores.
- Ventajas
  - Mejorar la demanda y la velocidad de transferencia
  - Podemos recuperar los datos gracias a los discos de código de error.

Lámina 54 Dr. Roberto Gómez Cárdenas

Raid 2

- Desventajas
  - Caro puesto que se necesitan muchos discos para guardar los códigos de error.
  - Tiempos de escritura lentos.

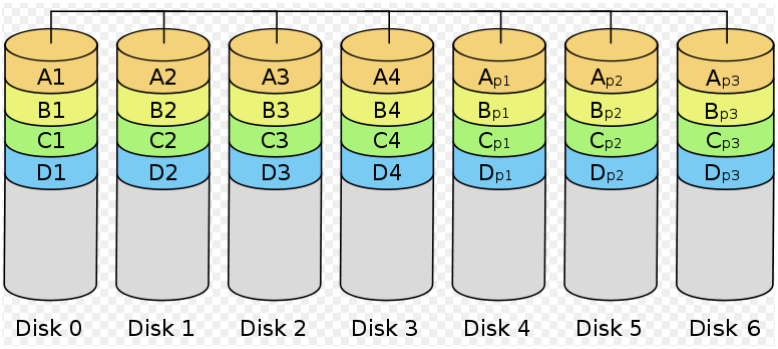


Lámina 55 Dr. Roberto Gómez Cárdenas

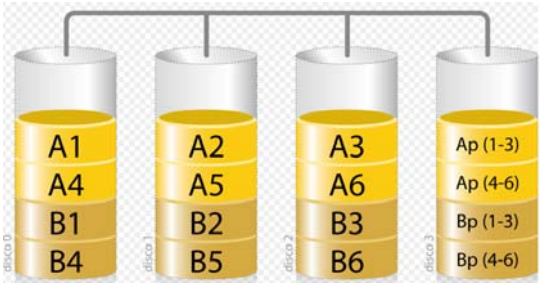
RAID 3

- Usa división a nivel de bytes con un disco de paridad dedicado.
- Acceso síncrono con un disco dedicado a paridad
- Ofrece altas tasas de transferencia, alta fiabilidad y alta disponibilidad.
- Mínimo de tres unidades.
- Ventajas
  - Alto rendimiento para aplicaciones de transferencia alta.
  - Recuperación de datos gracias al disco de paridad.

Lámina 56 Dr. Roberto Gómez Cárdenas

RAID 3

- Desventajas
  - Si perdemos el disco de paridad perdemos la redundancia.
  - Tiempo de escritura bastante lento.



Cada número representa un byte de datos; cada columna, un disco

Lámina 57 Dr. Roberto Gómez Cárdenas

RAID 4

- Usa división a nivel de bloques con un disco de paridad dedicado.
- Necesita un mínimo de 3 discos físicos.
- El RAID 4 es parecido al RAID 3 excepto porque divide a nivel de bloques en lugar de a nivel de bytes
- Se puede reconstruir en tiempo real.
- Indicado para almacenamiento de ficheros de gran tamaño, aplicaciones gráficas.

Lámina 58 Dr. Roberto Gómez Cárdenas

RAID 4

- Cada miembro del conjunto funciona independientemente cuando se solicita un único bloque.
- Si la controladora de disco lo permite, un conjunto RAID 4 puede servir varias peticiones de lectura simultáneamente.

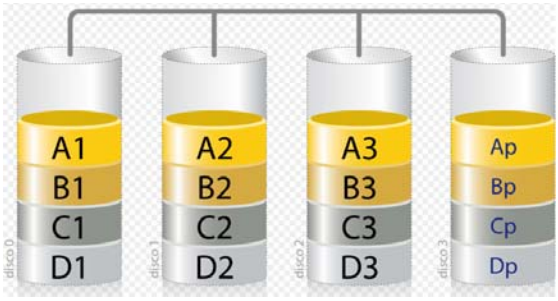


Lámina 59 *Cada número representa un bloque de datos; cada columna, un disco* Dr. Roberto Gómez Cárdenas

RAID 5

- Usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto.
- La información se almacena por bloques y de forma alternativa en todos ellos.
- El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia.

Lámina 60 Dr. Roberto Gómez Cárdenas

Ejemplo RAID 5

- El RAID 5 requiere al menos tres unidades de disco para ser implementado.
- El fallo de un segundo disco provoca la pérdida completa de los datos.
- El número máximo de discos en un grupo de redundancia RAID 5 es teóricamente ilimitado.

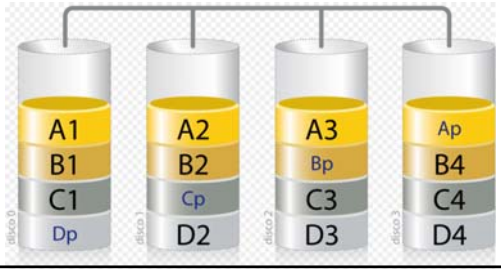


Lámina 61 Dr. Roberto Gómez Cárdenas

Adquiriendo discos RAID

- ¿Preocupaciones?
  - ¿Cuánto información es necesaria?
  - ¿Qué tipo de RAID es usado?
  - ¿Se cuenta con la herramienta de adquisición adecuada?
  - ¿La herramienta puede leer una imagen forense de la imagen RAID?
- Hardware-firmware RAID viejo puede ser un reto cuando se esta construyendo la imagen.

Lámina 62 Dr. Roberto Gómez Cárdenas

Adquiriendo discos RAID

- Vendedores ofrecen funciones de adquisición
  - Technologies Pathways ProDiscover
  - Guidance Software EnCase
  - X-Ways Forensics
  - Runtime Software
  - R-Tools Technologies
- Ocasionalmente, un sistema RAID es muy grande
  - Obtener solamente los datos relevantes a la investigación.

Lámina 63 Dr. Roberto Gómez Cárdenas

Completando el caso

- Es necesario producir un reporte final.
  - Establecer que se hizo y que se encontrón.
- Incluir reportes generados por la herramienta utilizada.
  - Esto es un complemento, no es el reporte
- Descubrimientos repetidos
  - Repetir los pasos y producir el mismo resultado.
- Si se requiere usar un formato de reporte.
- El reporte debe mostrar evidencia concluyente.
  - El sospechoso llevo a cabo, o no, un crimen o violo una política de la organización

Lámina 64 Dr. Roberto Gómez Cárdenas


La investigación forense
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
Lámina 65
Dr. Roberto Gómez Cárdenas