#CyberSBC2024

Forense Básico

8 al 18 julio de 2024

León, España

Organizado por:

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

Con la colaboración de:

Canadá

AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León

¿Qué vamos a aprender ?

- Análisis Forense Digital – Conceptos Básicos
- Evidencia Forense Digital
- Nivel de Volatilidad
- Formatos de Evidencia Digital
- Objetivos del análisis de evidencia digital
- Análisis de Evidencia Digital

whoami

Profesional en Ciberseguridad con 20 años de experiencia en el sector, busca compartir conocimiento haciendo uso de su experiencia y conocimiento y en este momento trabaja como CEO de Be Hacker Pro, donde plantea estrategias para el fortalecimiento del capital humano construyendo espacios para desarrollar talentos en ciberseguridad, es cofundador de CSIETE y 7 Way Security, organizador de BSides Colombia, HackLab Bogotá y otros espacios de construcción de conocimiento colectivo.

Conceptos Básicos

Conceptos Básicos

Antes de empezar…

https://github.com/BeHackerPro/INCIBE_forensics

Conceptos Básicos

Recursos

https://csrc.nist.gov/glossary

Conceptos Básicos

Forense Digital

En su connotación más estricta, un proceso de aplicación de la ciencia computacional y procedimientos investigativos que envuelven la evaluación de evidencia digital, siguiendo la autoridad de búsqueda adecuada, cadena de custodia, validación con matemáticas, uso de herramientas validadas, repetibilidad, reportes y posible testimonio experto.

Conceptos Básicos

Forense Digital

La aplicación de ciencia a la identificación, recolección, examen y análisis, de datos mientras se preserva la integridad de la información y se mantiene una estricta cadena de custodia para los datos dentro de un proceso repetible

Conceptos Básicos

Forense Digital

El proceso usado para adquirir, preservar, analizar y documentar sobre evidencia utilizando métodos científicos que sean demostrablemente confiables, precisos y repetibles de modo que puedan usarse en procedimientos judiciales.

Conceptos Básicos

Objetivo del Forense Digital

Usando la evidencia digital determinar quién, qué , dónde, cuándo y cómo se realizó un crimen.

Conceptos Básicos

Uso del Forense Digital

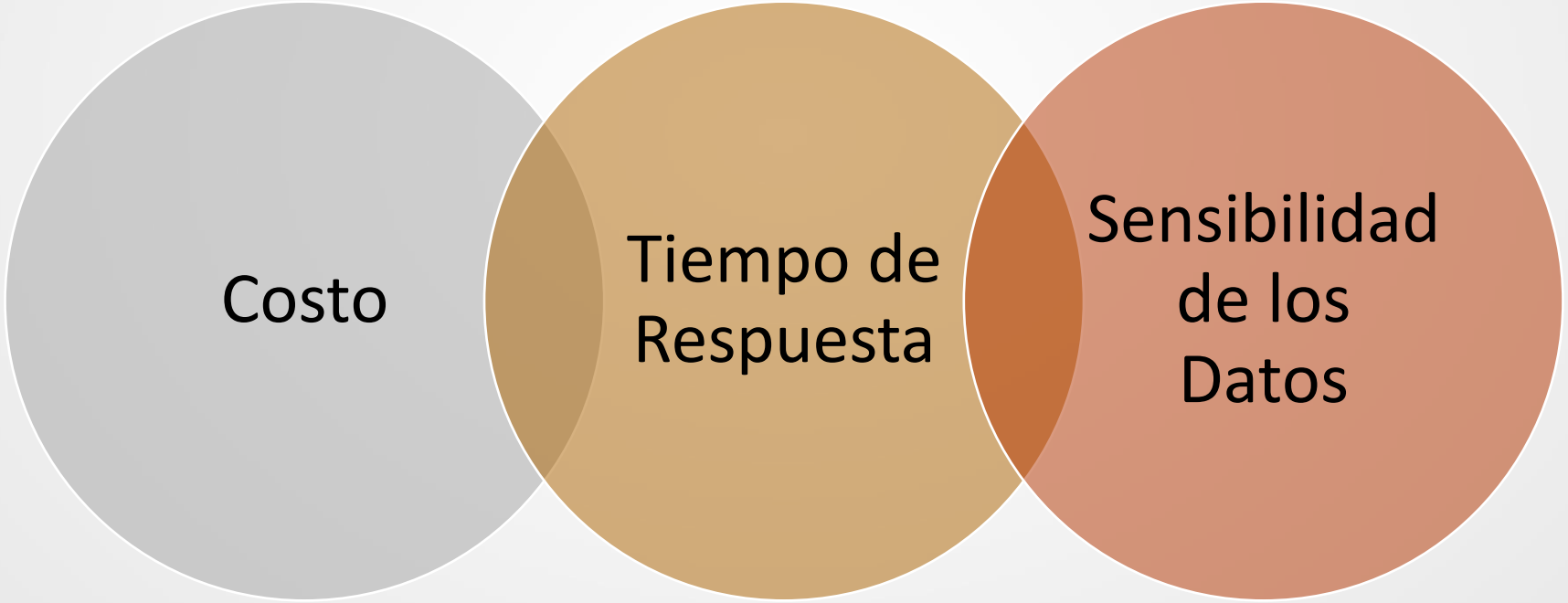
- Solución de problemas operacionales
- Monitoreo de Logs
- Recuperación de Datos
- Adquisición de Datos
- Cumplimiento Regulatorio

Conceptos Básicos

Uso de herramientas y técnicas forenses

Conceptos Básicos

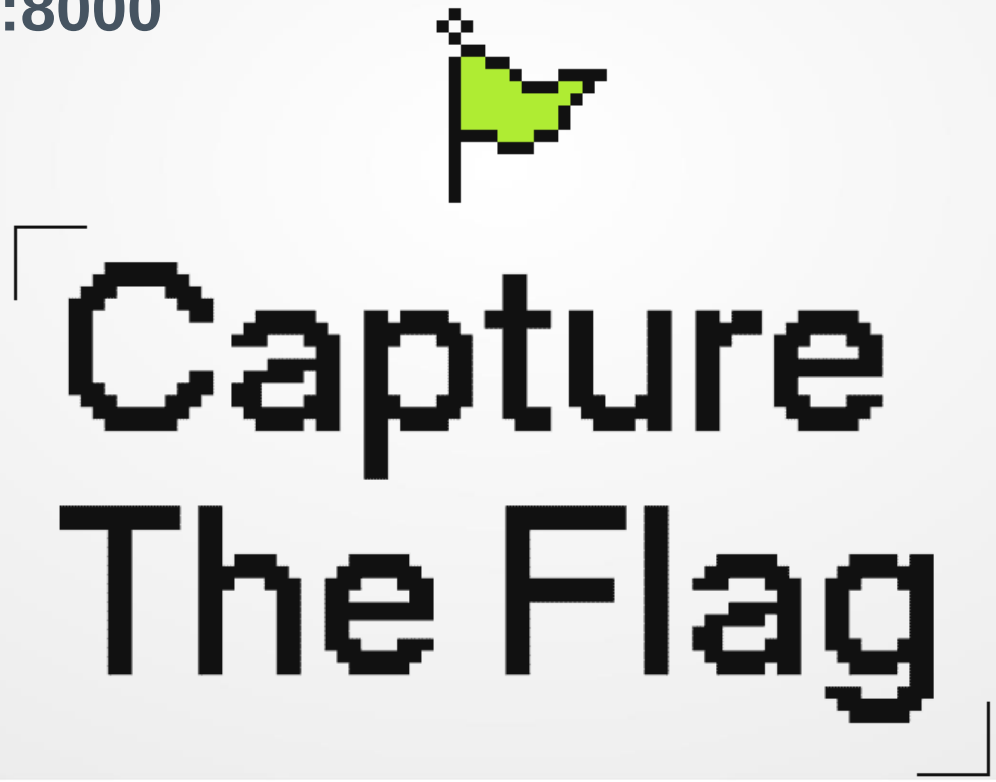
Capacidades Internas o Externas ?



CTF

Vamos a revisar cómo van entendiendo cada concepto…

http://100.24.39.65:8000



Organizado por:

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

Con la colaboración de:

Canadá

AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León

Conceptos Básicos

Recursos

Guide to Integrating Forensic Techniques into Incident NIST SP 900-86

Conceptos Básicos

Fases del Proceso

Conceptos Básicos

Recolección

Identificar, etiquetar, grabar y adquirir datos de posibles fuentes relevantes de datos, mientras se siguen los procedimientos adecuados que aseguren la preservación de la integridad de los datos

Organizado por:

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

Con la colaboración de:

Canadá

AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León

Conceptos Básicos

Examen

Procesamiento forense de los datos recolectados usando una combinación de métodos manuales y automatizados, mientras se validan y extraen datos de interés particular, mientras se preserva la integridad de los datos

Conceptos Básicos

Análisis

Analizar los resultados del examen, usando métodos y técnicas justificables legalmente, para obtener información útil que responda las preguntas precursoras de realizar la recolección y el examen

Conceptos Básicos

Documentación I

Generar un reporte de los resultados del análisis, los cuales deben incluir las acciones usadas, explicaciones de cómo fueron seleccionadas las herramientas y procedimientos

Conceptos Básicos

Documentación II

Determinar que otras acciones debieron se realizadas (examen forense de otras fuentes de datos, aseguramiento de vulnerabilidades identificadas, mejorar controles de seguridad)

Conceptos Básicos

Documentación III

Entregar recomendaciones para la mejora a políticas, procedimientos, herramientas y otros aspectos del proceso forense

Organizado por:
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OEA Más derechos para más gente
Con la colaboración de:
Canadá
AYUNTAMIENTO DE LEÓN
LEÓN CONGRESOS
universidad de León

Conceptos Básicos

Datos

Los datos se refieren a distintas piezas de información digital que han sido formateadas de una manera específica.

Conceptos Básicos

Datos

Debido a la variedad de fuentes de datos, las técnicas forenses digitales se pueden utilizar para muchos propósitos, como investigar delitos y violaciones de políticas internas, reconstruir incidentes de seguridad informática, solucionar problemas operativos y recuperarse de daños accidentales al sistema.

Conceptos Básicos

Recomendaciones

- Las organizaciones deben tener capacidades de realización de tareas forenses para equipos y redes
  - Manejo de evidencia
  - Identificación de eventos

Conceptos Básicos

Recomendaciones

- Quién maneja cada aspecto del proceso forense
  - Capacidades Internas
  - Capacidades Externas

Conceptos Básicos

Recomendaciones

- El equipo de manejo a incidentes debe tener capacidades forenses robustas
  - Más de un solo miembro del equipo
  - Hands - On

Conceptos Básicos

Recomendaciones

- Varios equipos de la organización deben participar en actividades forenses
  - Colaboración
  - Asistencia Adicional
  - TI, Gerencia, Legal, HHRR, auditores, seguridad física

Conceptos Básicos

Recomendaciones

- Consideraciones reflejadas en políticas
  - Autorización del personal para realizar tareas forenses
    - IR / Investigaciones Digitales
  - Roles y Responsabilidades
  - Acciones que se deben y no se deben hacer
  - Forensic Readiness
    - Retención de datos, auditoría de hosts

Conceptos Básicos

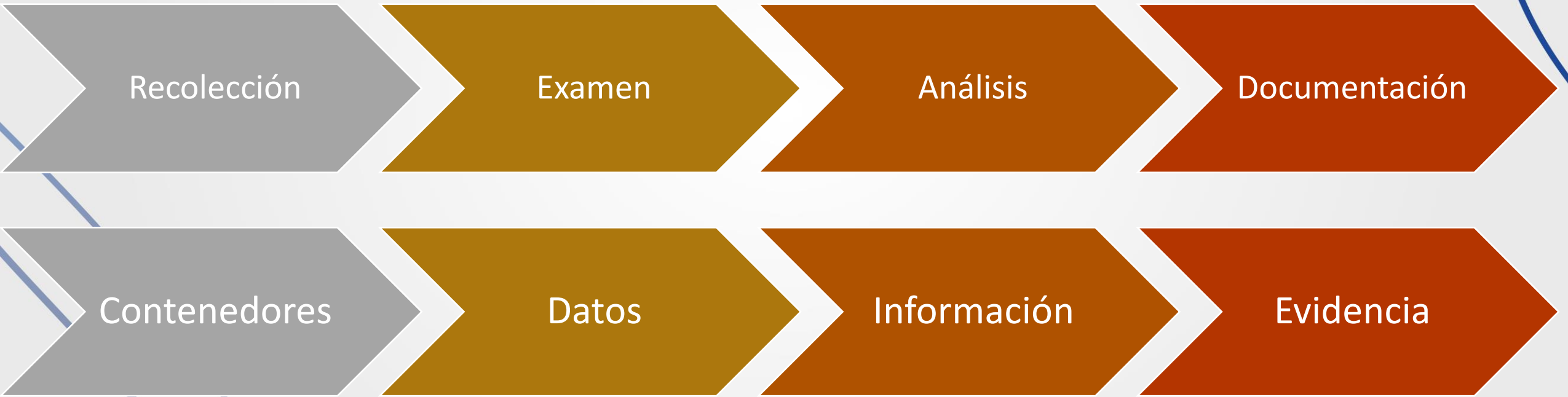
Recomendaciones

- Guías y procedimientos para la ejecución de tareas forenses
  - Procedimientos paso a paso
  - Metodologías generales de investigación de un incidente haciendo uso de técnicas forenses

Evidencia Forense Digital

Evidencia Forense Digital

Fases del Proceso



Evidencia Forense Digital

Fuentes

Fuentes potenciales de evidencia y cómo adquirir datos de cada una de ellas…

Evidencia Forense Digital

Fuentes

- Equipos de escritorio
- Servidores
- Dispositivos de almacenamiento de red
- Portátiles

Evidencia Forense Digital

Fuentes

- CDs y DVDs
- Puertos
  - USB
  - PCMCIA
  - Firewire

Evidencia Forense Digital

Fuentes

- Almacenamiento
  - Memorias y tarjetas flash
  - Thumb Drive
  - Dispositivos Ópticos

Evidencia Forense Digital

Fuentes

- Datos volátiles

Evidencia Forense Digital

Fuentes

- PDAs
- Móviles
- Cámaras
- Grabadoras
- Reproductores de Audio

Evidencia Forense Digital

Fuentes

- Logs del ISP ?
- Logs de una red social ?
- Auth en un servicio de nube ?

Evidencia Forense Digital

Fuentes

- Casa de un colaborador en modelo de teletrabajo ?

Evidencia Forense Digital

Adquisición de Datos

- Desarrollar un plan de trabajo de adquisición
  - Posible Valor
  - Volatilidad
  - Esfuerzo Requerido

Evidencia Forense Digital

Adquisición de Datos

- Recolección de Datos
  - Volátil
  - No Volátil
  - Medios no volátiles
- Verificación de la Integridad de los Datos

CADENA DE CUSTODIA

Organizado por:

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

Con la colaboración de:

Canadá

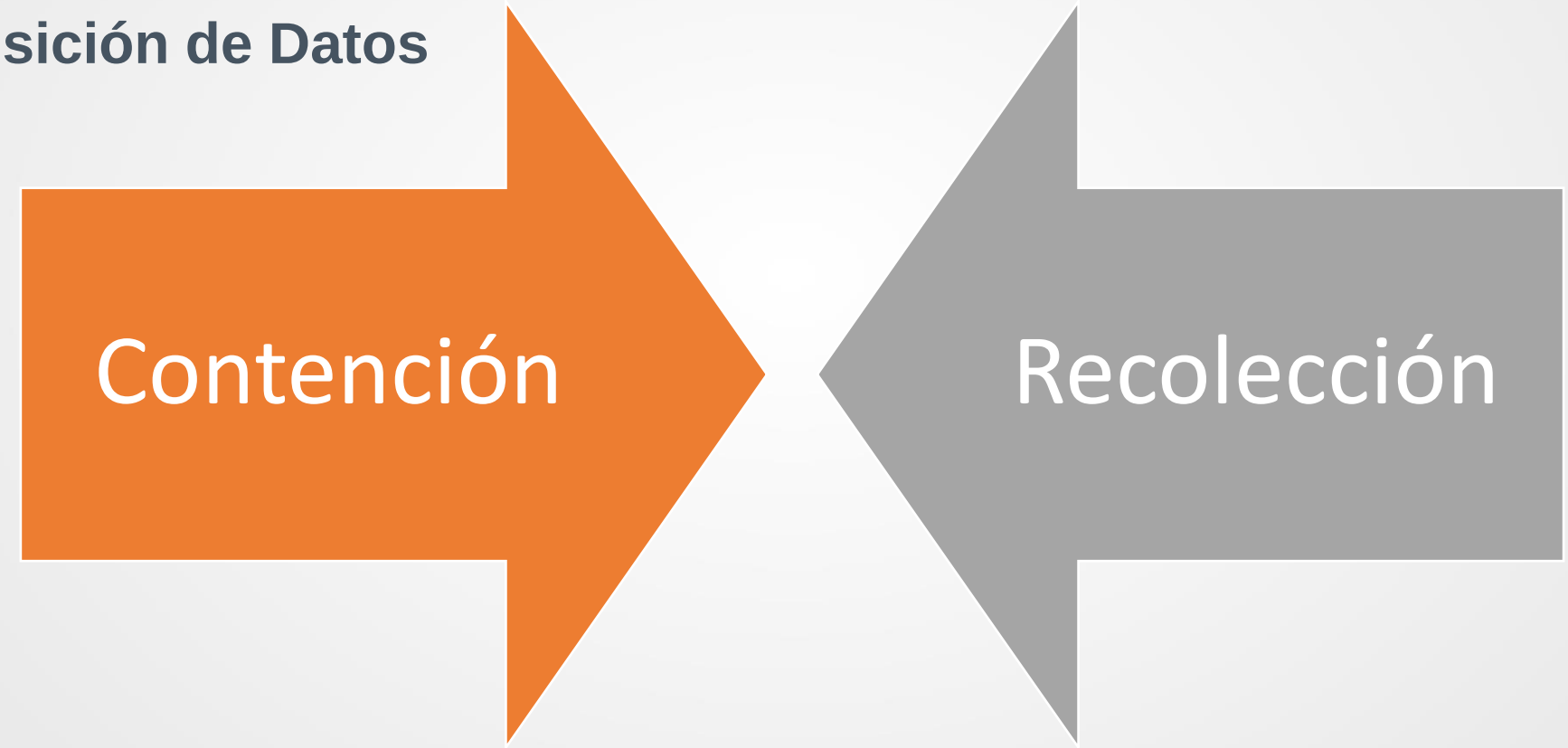
AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León

Evidencia Forense Digital

Adquisición de Datos



Evidencia Forense Digital

Examen

- Evaluar y extraer piezas de datos relevantes de los contenedores adquiridos

Evidencia Forense Digital

Examen

- Un log de millones de conexiones de un firewall…
- Solo 5 datos son relevantes para nuestra investigación

Evidencia Forense Digital

Examen

- Patrones de texto
- Archivos conocidos
- Tipos de Archivos
- Cifrado

Evidencia Forense Digital

Análisis

- Correlación entre elementos
  - Log del equipo
  - IDS
  - Antivirus
- Conclusiones

Evidencia Forense Digital

Documentación - Reporte

- Explicaciones alternativas
  - Información Incompleta
  - 2 o más explicaciones posibles

Evidencia Forense Digital

Documentación - Reporte

- Consideración de la audiencia
- Información accionable

Niveles de Volatilidad

Niveles de Volatilidad

Concepto

Un dato volátil es considerado como cualquier evento que solo puede ser recolectado de un sistema encendido y que no ha sido reiniciado desde que el evento sucedió

Niveles de Volatilidad

Concepto

Cualquier acción realizada en un sistema bien sea por personas o el sistema operativo puede afectar la integridad de un dato vólatil

Niveles de Volatilidad

Concepto

Decision

Niveles de Volatilidad

Volatilidad en Sistemas Operativos

- Conexiones de Red
- Sesiones Conectadas
- Procesos en Ejecución

Niveles de Volatilidad

Volatilidad en Sistemas Operativos

- Archivos abiertos
- Configuración de Red
- Tiempo en el sistema operativo

Niveles de Volatilidad

Volatilidad en Sistemas Operativos

- Memoria
  - Slack Space
  - Free Space

Formatos de Evidencia Digital

Formatos de Evidencia Digital

Archivo de Datos

Una colección de información agrupada de manera lógica dentro de una única entidad y referenciada por un único nombre

Formatos de Evidencia Digital

Medios de Almacenamiento

CD-ROM, DVD-ROM, Disco Duro, Backup Tape, Magneto Optical Disk, Advanced Technology Attachment (ATA) flash card, Flash, Compact Flash, SD, Smart Media, Nube

Formatos de Evidencia Digital

Sistemas de Archivos

FAT12, FAT16, FAT32, NTFS, High Performance File System HPFS, Second Extended Filesystem (ext2fs), ext3fs, ext4fs, ReiserFS, Hierarchical File System (HFS), HFS+, Unix File System (UFS), Compact Disk File System (CDFS), ISO 9660 y Joilet, Universal Disk Format (UDF)

Formatos de Evidencia Digital

Otros Datos

- Archivos Borrados
- Slack Space
- Espacio Libre
- Alternate Data Streams

Formatos de Evidencia Digital

Tipo de Adquisición

- Lógico
- Bit Stream - Físico

Formatos de Evidencia Digital

Firmas de Archivos

https://www.garykessler.net/library/file_sigs.html

Formatos de Evidencia Digital

Recomendación

- No se hace una recolección física de un sistema en ejecución ya que por los cambios que se pueden presentar no se puede comprobar al finalizar el proceso

Formatos de Evidencia Digital

Recomendación

- Si hay backups disponibles es mejor no hacer una copia lógica para no modificar los datos dentro de los archivos

Formatos de Evidencia Digital

Calculo y protección de Integridad

- Comparación con contenedores originales
- Uso de bloqueadores de escritura
  - Hardware o Software

Formatos de Evidencia Digital

Desafíos

- Borrado Seguro o Degaussing
- ADS en NTFS
- Host Protected Area (HPA)
- RAID-0 o RAID-5
- Steg

Formatos de Evidencia Digital

Formatos Forenses

- E01 – Encase Evidence Image
- Raw
- DMG – Disk Image File
- LEF – Encase Logical Evidence File

Análisis de Evidencia Digital

Análisis de Evidencia Digital

Herramientas Forenses

- Visores de Archivos
- Descomprimir Archivos
- Interfaz gráfica para ver la estructura de archivos

Análisis de Evidencia Digital

Herramientas Forenses

- Identificación de archivos conocidos
  - National Software Refence Library
- Búquedas de strings y patrones
- Acceso a los metadatos de archivos

Análisis de Evidencia Digital

Herramientas Forenses

Computer Forensics Tool Testing Program (CFTT)

Organizado por:
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OEA Más derechos para más gente
Con la colaboración de:
Canadá
AYUNTAMIENTO DE LEÓN
LEÓN CONGRESOS
universidad de León

Cybersecurity Summer Bootcamp

LEÓN - 2024

8 al 18 julio de 2024

León, España

#CyberSBC2024

incibe.es/eventos/summer-bootcamp

Organizado por:

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

Con la colaboración de:

Canadá

AYUNTAMIENTO DE LEÓN

LEÓN CONGRESOS

universidad de León