Metodología para la admisibilidad de las evidencias Digitales

VII Jornada Nacional de Seguridad Informática

COMPUTACIÓN FORENSE: RASTREANDO LA INSEGURIDAD INFORMÁTICA

JUNIO 20, 21 Y 22 DE 2007

Biblioteca Luis Ángel Arango
Calle 11 No 4-14
Bogotá D.C., Colombia.

Conferencista:
José Ebert Bonilla
Corporación Universitaria Unitec
jbonilla@unitec.edu.co

ACIS

Agenda

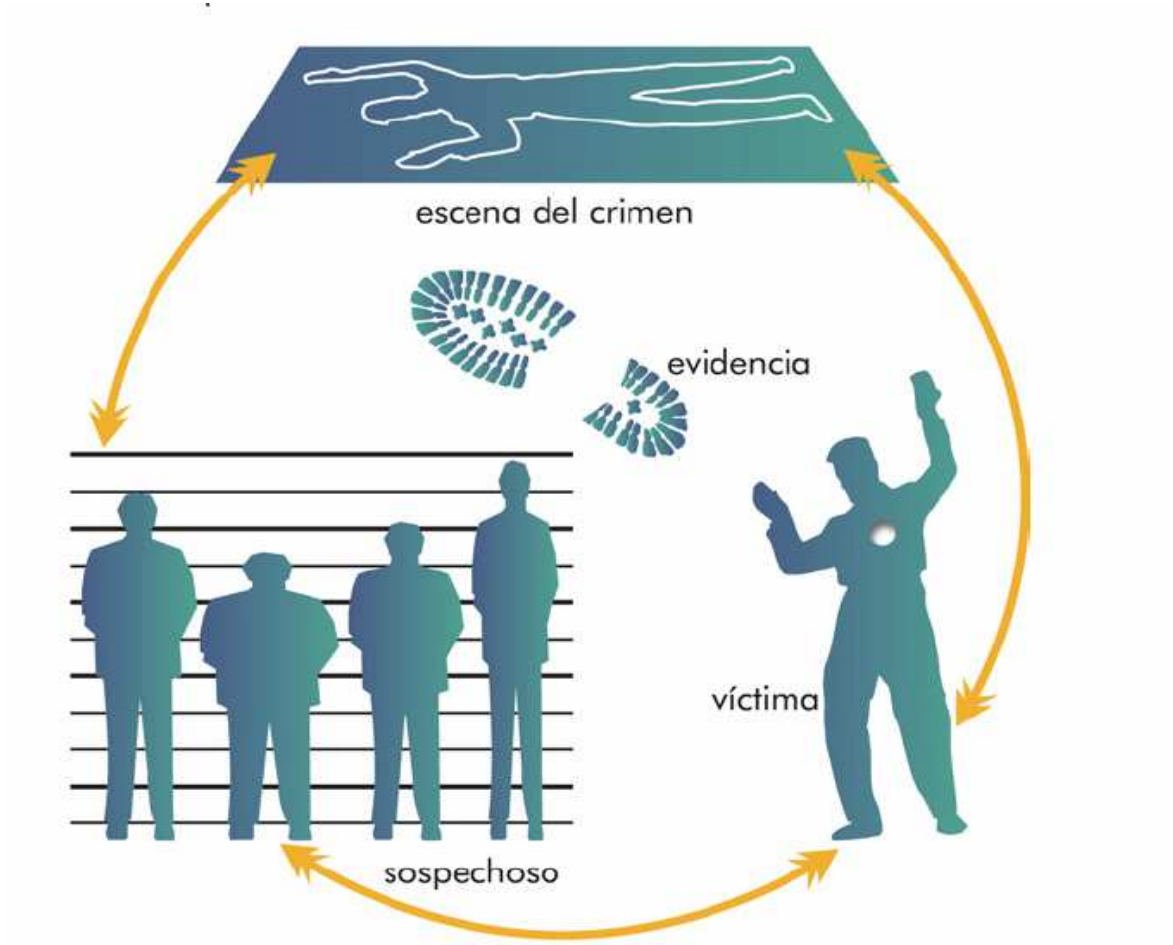
- Definición de computación forense
- Principio de Locard
- Evidencia Digital
- Problemática abordada
  - Técnico
  - Jurídico
- Metodología Propuesta
- Preguntas

Definición de Computación Forense

El proceso de identificación, preservación, análisis y presentación de evidencia digital de tal forma que sea legalmente aceptable.

McKemmish

Principio de Locard



GARCIA M, Antonio Javier. La formación de un equipote respuesta a Incidentes Forenses. SIC. No. 59. Abril del 2004.

Evidencia Digital

Es un tipo de evidencia física. Está constituida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales

C. Eoghan. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Second Edition. Great Britain.: Elsevier – Academia Press

Problemática

- Técnico
  - Experiencia del Investigador
  - No alteración de la escena
  - Recolección
  - Autenticidad
  - Sincronización
- Jurídico
  - Información como un bien
  - Cadena de custodia
  - Delitos Informáticos
  - Admisibilidad de la evidencia

Metodología Propuesta

- Basada en:
  - Legislación colombiana
  - Cadena de Custodia
  - Documentación
- Por etapas
  - Autorización,
  - preparación,
  - recopilación de pruebas,
  - análisis de información y
  - documentación

Etapas

- Autorización
- Preparación
  - Asegurar el área
  - Levantamiento de acta
  - Tomar fotografías del lugar
  - Identificación de las fuentes de evidencias
  - Sanetización de medios
- Recopilación de pruebas
  - Ataque en proceso?
  - Toma de evidencia volátiles
  - Toma de firma digitales
  - Toma de imágenes
  - Toma de firma de imágenes
  - Guardar original y copias en lugares seguros

Etapas …

- Análisis de Información
  - Caracterización de medios
    - Identificación de particiones
    - Identificación de sistemas de archivos
    - Identificación de archivos existentes
    - Caracterización individual y por grupos
    - Evaluación de fuentes
  - Recuperación de Archivos
    - Archivos borrados
    - Recuperación de información escondida
  - Análisis de Información
    - Información de log's
    - Revisión de archivos de contraseñas y permisos
    - Análisis de evidencias volátiles
  - Filtrado Información y reducción de información
  - Reconstrucción de los hechos
    - Análisis Relacional
    - Análisis Temporal
    - Información y archivos comprometidos en el caso

Etapas …

  - Línea del Tiempo
- Documentación
  - Hacer el informes de hallazgos
  - Entregar documentación total de la investigación

Preguntas

http://www.firebirds.com.ar/circulofyh/photogallery/pregunta.jpg

Bibliografía

- Garfinkel, S.L. AFF: New format for storing hard drive images. Communications of the ACM. Vol.49, No. 2 (February 2006), pp 85-87. http://www.acm.org
- M. Rodney. What is forensic computing?. Australian Institute of Criminology. Trends & Issues in crime and criminal justicie. No. 118. Junio de 1999. Tomado de http://www.aic.gov.au/publications/tandi/ti118.pdf
- C. Eoghan. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Second Edition. Great Britain.: Elsevier – Academia Press. 2004, p. 8.
- R. James. Corporate management of computer forensic evidence. InfosecCD Conference'06 September 22-23 2005. Copyright 2006 ACM.
- R. Román. El principio de Intercambio V 2.0. Chase The Sun. Septiembre de 2004. Este documento fue tomado de la página Web www.chasethesun.es.
- B. Rahul. State and local law enforcement is not ready for a cyber Katrina. Communications of the ACM. February 2006 vol 49 No. 2
- L. Ryan; K. Axel. A Formalization of digital forensic. International Journal of digital evidence. Fall 2004, vol 3 issue 2
- Computer evidence defined. New Technologies Inc. www.forensics-intl.com/def3.html
- C. Jeimy. Computación Forense. Un reto técnico – legal para el próximo milenio. Conferencia presentada en el marco del I congreso Internacional de Ingeniería de Sistemas y Ciencias de la Computación. Universidad Industrial de Santander. Bucaramanga. Colombia. Nov. 2000. http://www.criptored.upm.es/paginas/docencia.htm
- L. Ryan; K. Axel. A Formalization of digital forensic. International Journal of digital evidence. Fall 2004, vol 3 issue 2

Bibliografía

- F. R., Hilma Ximena. Constitución Nacional Actualizada y comentada. Fondo Educativo Panamericano. 2005. Pág. 23
- M. E. Carlos Pablo. El delito informático. La información y la comunicación en la esfera penal. Conforme con el nuevo código penal. Editorial Leyer. 2002. Págs. 23- 73
- Código Penal. Temis. Artículo 9. Pág. 13
- Código Civil. Artículos 666 y siguientes.
- M. E. Carlos Pablo, op. cit. Pág. 101.
- www.forensics-intl.com/evidguid.html
- H., Mathew. To revisit: What is forensic computing?. University of South Australia. 2004. http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf
- U.S Department of Justice. Office of justice program. National Institute of justice. Electronic crime scene investigation. A guide for first responder. NCJ 187736. July 2001. http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
- C. Eoghan. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Op. Cit.
- C. Brian. File System Forensic Analysis. United States: Pearson Education, Inc. 2005, pp 5–13.
- L. Ryan; K. Axel. A Formalization of digital forensic. Op. Cit
- Garfinkel, S.L. AFF: New format for storing hard drive images. Op. Cit.
- Marcella, A.J. y Greenfield, R.S. Caber Forensics. A field manual for collecting, examining, and preserving evidence of computer crimes. United States of America: CRC press LLC. 2002. pp 19 –77
- www.cert.org/stats/cert_stats.html
- A. Michael R. Computer Evidence Processing. Good documentation is essential. New Technologies Inc. www.forensics-intl.com.art10.html

Muchas Gracias!!!