UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE SISTEMAS

ASIGNATURA: ELECTIVA INFORMÁTICA FORENSE.
MODALIDAD: PRESENCIAL TEORICO / PRACTICA
INTENSIDAD: 64 HORAS.
PREREQUISITOS:
AREA DE FORMACIÓN: INGENIERIA APLICADA.

OBJETIVO GENERAL

Estudiar los conceptos fundamentales sobre la informática forense y sus aplicaciones en la seguridad de la información, específicamente en los delitos informáticos y sus aspectos legales.

AL FINALIZAR EL CURSO EL ESTUDIANTE DEBE ESTAR EN CAPACIDAD DE:

1. Utilizar las técnicas y los métodos de análisis forense.
2. Analizar los métodos de informática forense y su aplicación en investigaciones sobre delitos informáticos.
3. Analizar y revisar las herramientas de informática forense más utilizadas.

METODOLOGIA

1. El alumno adquirirá los conocimientos básicos a través de clases magistrales.
2. El alumno desarrollará talleres en clase que le ayudarán a llevar a la práctica los conocimientos teóricos adquiridos.
3. El alumno deberá profundizar sus conocimientos con temas complementarios y trabajos de investigación.
4. Utilización de varios programas de apoyo para la parte de aplicaciones forenses.
5. Se presentarán algunos videos relacionados con la informática forense.

CONTENIDO

1. INTRODUCCIÓN AL ANÁLISIS FORENSE (12 horas)
- 1.1. ¿Qué es informática forense?
- 1.2. Objetivos del análisis forense
- 1.3. Etapas del análisis forense
- 1.4. Cadena de custodia de las evidencias digitales

2. SISTEMAS DE ARCHIVOS WINDOWS Y LINUX PARA MANEJO FORENSE(12 horas)
- 2.1. Sistemas de archivos FAT, HPFS, NTFS y EXT
- 2.2. Números mágicos (Cabeceras de tipos de archivos)
- 2.3. Recuperación de los archivos borrados
- 2.4. Esterilización de medios de almacenamiento
- 2.5. Análisis de los metadatos de los archivos

3. ADQUISICIÓN DE EVIDENCIAS (12 horas)
- 3.1. Tipos de evidencias y orden de volatilidad
- 3.2. Acotando la escena del crimen
- 3.3. Adquisición de las evidencias
- 3.4. Preservación de la integridad e identidad de las evidencias

4. ANÁLISIS DE LAS EVIDENCIAS (14 horas)
- 4.1. Esquema de un análisis
- 4.2. Archivos de interés en Windows
- 4.3. Archivos de interés en Linux
- 4.4. Archivos de interés en Mac OS

5. GUIA DE BUENAS PRACTICAS EN INFORMÁTICA FORENSE (14 horas)
- 5.1. Metodologías
- 5.2. Estándares

EVALUACIONES

Se realizarán tres (3) evaluaciones parciales de la siguiente forma:

PARCIAL	%	COMPONENTES	%
Primero	30%	Evaluación Parcial	60%
		Talleres y/o Quices	40%
Segundo	30%	Evaluación Parcial	60%
		Talleres y/o Quices	40%
Tercero	40%	Proyecto de clase	60%
		Talleres y/o Quices	40%

Los trabajos y talleres en grupo serán evaluados individualmente y deben estar debidamente documentados. Todo Proyecto NO sustentado pierde validez. Las sustentaciones serán programadas con anterioridad definiendo fecha y hora para cada alumno.

REFERENCIAS

1. *Pérez Gómez, Elena. (2011). ¿Qué es la informática forense o Forensic?. Recuperado el 14 de febrero de 2013.*
2. *Noblett, M. G. y Pollitt, M. M. (2000). Recovering and Examining Computer Forensic Evidence. Recuperado el 14 de febrero de 2013*.
3. *Kozushko, H. (2003). Digital evidence. Recuperado el 14 de febrero de 2013*.
4. Cano, J. J. (2005). *Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas*. Recuperado el 14 de febrero de 2013.
5. Altheide, C. y Carvey, H. (2011). *Computer forensics with Open Source tools*. Syngress.
6. Brown, C. L. T. (2010). *Computer evidence. Collection and preservation*. Boston:Course Technology PTR.
7. Brezinski, D., y Killalea, T. (2002). *Guidelines for Evidence Collection and Archiving*. Extraído el día 12 de febrero de 2013 desde: http://www.ietf.org/rfc/rfc3227.txt.