UNIVERSIDAD DEL SAGRADO CORAZÓN
DECANATO ASOCIADO DE ESTUDIOS GRADUADOS

PRONTUARIO

TÍTULO: Investigación forense

CODIFICACIÓN: ASI 730

PRERREQUISITOS: ASI 650 (o GSI 650 o CON 710) & GSI 731

CRÉDITOS: Tres (3) créditos, tres (3) horas semanales, una (1) sesión
Componente en línea: participar en una (1) sesión de una (1) hora semanal de discusión en línea.

DESCRIPCIÓN

Estudio de los principios fundamentales en la investigación forense de sistemas informáticos, incluyendo metodologías, procedimientos y herramientas disponibles para el análisis de dichos sistemas. El curso, dirigido a estudiantes graduados, cubre aspectos legales en adquisición, protección, custodia, y preservación de recursos informáticos, con énfasis en los aspectos técnicos asociados con la adquisición, investigación y análisis forense de evidencia y la preparación de reportes sumativos y técnicos de los hallazgos. Este curso contiene actividades y discusiones en línea.

JUSTIFICACIÓN

El aumento en ataques cibernéticos a sistemas informáticos, aunados a nuevas leyes y reglamentaciones para la protección de información, han hecho que los profesionales en recursos informáticos, tales como oficiales de seguridad y gerentes y auditores de sistema de información, deben tener conocimiento de los principios fundamentales en investigaciones forenses. De esta manera podrán conducir investigaciones de incidentes de seguridad e interpretar los resultados del los análisis forenses para identificar posibles vulnerabilidades, delinear responsabilidades, o tomar las medidas apropiadas para proteger los recursos informáticos.

OBJETIVOS

Al finalizar el curso el estudiante estará capacitado para:

1. Conocer y aplicar la metodología y proceso de la investigación forense de incidentes de seguridad

2. Utilizar los principios fundamentales en la adquisición, custodia, preservación y análisis de evidencia
3. Distinguir las funciones del investigador forense incluyendo las leyes pertinentes al análisis forense digital.
4. Conocer y utilizar el proceso de investigación forense de sistemas informáticos
5. Evaluar y utilizar herramientas disponibles para la investigación y análisis de diferentes sistemas informáticos
6. Redactar reportes sumativos y técnicos de investigación y análisis forenses de incidentes de seguridad.

CONTENIDO

I. Principios fundamentales
   - A. Respuesta a incidentes de seguridad e informática forense
   - B. El proceso de investigación de incidentes de seguridad
   - C. Proceso de escenas de crimen e incidentes de seguridad
   - D. Control de evidencia
     1. Aspectos legales y técnicos
   - A. Investigación digital
     1. El proceso forense
        a. Estudio preliminar
        b. Adquisición de datos
        c. Análisis forense
     2. Informe de investigación y hallazgos

II. Técnicas de investigación forense
   - A. Conceptos básicos de informática para investigadores digitales
   - B. Herramientas para investigaciones forenses
   - C. Examen forense de sistemas Windows
   - D. Examen forense de sistemas Unix
   - E. Examen forense de redes
   - F. Examen forense de dispositivos portátiles

III. Evidencia digital en el proceso judicial
     1. Custodia y Admisibilidad

2. Reportes y testimonio experto

ESTRATEGIAS INSTRUCCIONALES

Conferencias y lecturas
Discusiones, ejercicios e investigaciones forenses
Redacción de reportes y hallazgos
Actividades didácticas a través de la Internet

EVALUACIÓN

Examen parcial	20%
Ejercicios y Asignaciones	15%
Participación en clase, discusiones en línea	10%
Informes de análisis forenses	35%
Proyecto de Investigación (evaluación final)	20%
Total	**100%**

TEXTO

Nelson B., Phillips A., Enfinger F., and Steuart C. (2007). *Guide to Computer Forensics and Investigations*. Thomson Course Technology.

BIBLIOGRAFÍA

Carrier B. (2005) *File System Forensic Analysis.* Addison-Wesley Professional

Casey, E. (2004). *Digital evidence and computer crime: Forensic Science,Computers and the Internet* (2nd ed.). London ; San Diego, Calif.: Academic Press.

Davis C., Philipp A., and Cowen D. (2004). *Hacking Exposed: Computer Forensics Secrets and Solutions.* McGraw Hill Osborne. (ISBN 0072256753).

Farmer D., & Venema W. (2005). *Forensic Discover.* Addison-Wesley Professional Computing Series.

Prosise, C., Mandia, K., & NetLibrary, I. (2003). *Incident Response & Computer Forensics* (2nd ed.). New York: McGraw-Hill/Osborne. (ISBN: 007222696X).

Rankin K. (2007). Knoppix Hacks: Tips and Tools for Using the Linux Live CD to Hack, Repair, and Enjoy Your PC by. The O'Reilly Hacks Series.

Volonino L., Anzaldua R., & Godwin J. (2006). *Computer Forensics: Principles and*

Practices. Prentice Hall (ISBN 0131547275).

Las bases de datos electrónicas a las cuales la Biblioteca Madre María Teresa Guevara está suscrita directamente y a través del Consorcio COBIMET, incluyen, documentos, artículos de revistas y periódicos y otros recursos de información relacionados con los temas del curso. Al utilizarlas siga los siguientes pasos:

Para **acceder desde cualquier lugar en la Universidad**

- escriba la dirección http://biblioteca.sagrado.edu/,
- seleccione **Biblioteca Virtual** y aparecerá la página en donde podrá acceder a las bases de datos, por disciplina o en orden alfabético.

Para **acceder fuera de la Universidad**

- escriba la dirección http://biblioteca.sagrado.edu/,
- seleccione **Biblioteca Virtual** y aparecerá la página en donde podrá acceder a las bases de datos, por disciplina o en orden alfabético.
- escriba el nombre del usuario y la contraseña (El nombre de usuario y la contraseña, los solicita personalmente en la Biblioteca)

INTERNET

The International Association of Investigative Specialist (IACIS), (2007). Recuperado el 13 de febrero de 2008 de http://www.cops.org.

The International Association of Investigative Specialist (IACIS), (2007). *Forensic Procedures.* Recuperado el 13 de febrero de 2008 de http://www.cops.org/forensicprocedures.

United States Department of Justice (2007). *Computer Crime and Intellectual Property Section (CCIPS)* Recuperado el 13 de febrero de 2007 de http://www.cybercrime.gov.

US Department of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*. Recuperado el 13 de febrero de 2008 de http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

US Department of Justice. *National Crime Justice Reference Service*. Recuperado el 13 de febrero de 2008 de http://www.ncjrs.gov/.

Cualquier estudiante que necesite acomodo razonable deberá solicitarlo al Decano Asociado de Asuntos Estudiantiles.

diciembre 2008