Facultad de Ingeniería
Comisión Académica de Posgrado

Formulario de Aprobación Curso de Actualización 2014

Asignatura: Metodologías para el análisis forense informático

Profesor de la asignatura :
Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación

Profesor Responsable Local:
(título, nombre, grado, Instituto)

Otros docentes de la Facultad:
Ing. Marcelo Rodríguez, Asistente, Instituto de Computación

Docentes fuera de Facultad:
(título, nombre, cargo, Institución, país)

Instituto ó Unidad: Computación
Departamento ó Área: Programación, Grupo de Seguridad Informática

Fecha de inicio y finalización: 1 de julio al 1 de agosto
Horario y Salón: Jueves y Viernes de 18 a 21 hs. Salón Rojo

Horas Presenciales: 38
(se deberán discriminar las mismas en el ítem Metodología de enseñanza)

Arancel: $ 10.000
(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem metodología de la enseñanza)

Público objetivo y Cupos:
Profesionales y estudiantes interesados en Seguridad Informática, y en particular, profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información para el aseguramiento de las organizaciones.
Sin cupo.

(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción en el Depto. de Posgrado, hasta completar el cupo asignado)

Objetivos:

El objetivo de este curso es introducir al estudiante en los conceptos básicos del análisis forense informático. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas. Al finalizar el curso el alumno habrá adquirido los conceptos técnicos básicos necesarios en lo que respecta a las metodologías de análisis y el tratamiento y/o adquisición de la evidencia digital.

Conocimientos previos exigidos: Profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información

Conocimientos previos recomendados: Redes de computadores, seguridad en redes, sistemas y aplicaciones

Metodología de enseñanza:
El curso consiste de un 75% de exposiciones teóricas (24hs) y el otro 25% (8hs) de trabajos prácticos en grupos, que son realizados usando la infraestructura del LaSI (Laboratorio de Seguridad Informática).

El cuso se dictará en 8 clases teóricas de 3 horas, 2 clase por semana, durante 4 semanas y 2 sesiones de laboratorio de 4 horas.

- Horas clase (teórico):24
- Horas clase (práctico):0
- Horas clase (laboratorio):8
- Horas consulta:3
- Horas evaluación:3
  - Subtotal horas presenciales: 38
- Horas estudio: 37
- Horas resolución ejercicios/prácticos:
- Horas proyecto final/monografía:
  - Total de horas de dedicación del estudiante: 75

Forma de evaluación:
Se evaluarán los trabajos de laboratorio y un examen final. La realización de las prácticas de laboratorio es obligatoria.

Temario:

1. Bases y Motivación
   a) Introducción.
   b) Motivación, definiciones y objetivos del análisis forense informático
   c) Principios de análisis forense
   d) Usos del análisis informático forense

2. Evidencia digital
   a) Tipos de evidencia
      i. Volátil
      ii. Persistente
      iii. Física
      iv. Lógica
   b) Propiedades (Admisible, autentica, completa, confiable, creíble)
   c) Fuentes de obtención de evidencias
   d) Cadena de custodia

3. Tipos de análisis forense
   a) Análisis post-mortem
   b) Live análisis
   c) Análisis On-Site
   d) Análisis en el laboratorio

4. Metodologías para el análisis forense
   a) Identificación
   b) Preservación

c) Análisis
d) Presentación

5. Herramientas de soporte a la metodología
   a) Herramientas de identificación
   b) Herramientas de preservación
   c) Herramientas de análisis
   d) Herramientas de presentación

6. Anti-forense
   a) Problemáticas y desafíos del análisis forense informático
   b) Técnicas anti-forenses
   c) Clasificación de métodos anti-forenses
      i. Destrucción de la evidencia
      ii. Ocultar la evidencia
      iii. Eliminación de las fuentes de la evidencia.
      iv. Falsificación de la evidencia
   d) Herramientas anti-forenses

Bibliografía:

Libros

The Basics of Digital Forensics.The Primer for Getting Started in Digital Forensics. Autor: John Sammons, Publisher: Syngress, ISBN-10: 1597496618.

File System Forensic Analysis, Autor: Brian Carrier, Publisher: Addison-Wesley Professional, ISBN-10: 0-321-26817-2.

Handbook of Digital Forensics and Investigation, Autor: Eoghan Casey, Publisher: Academic Press, ISBN-10: 0123742676.

Digital Evidence And Computer Crime, Autor: Eoghan Casey, Publisher: Academic Press, ISBN-10: 0-12-163104-4.

Computación Forense. Descubriendo los rastros informáticos, Autor: Jeimy Cano, Editorial: Alfaomega, ISBN: 978-958-682-767-6.

Artículos

Manual de Peritaje Informático, Autor: Maricarmen Pascale (Coordinadora), Fundación de Cultura Universitaria, 2007.