FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

Código	Nombre
CC74C	Informática Forense y Respuesta a Incidentes

Nombre en Inglés
Digital Forensics and Incident Response

SCT	Unidades Docentes	Horas de Cátedra	Horas Docencia Auxiliar	Horas de Trabajo Personal
3	5	1.5	1.5	2.0

Requisitos	Carácter del Curso
Autor sólo Postgrado	Electivo para Magister y Doctorado en Ciencias mención Computación.

Resultados de Aprendizaje

Al termino del curso el estudiante demuestra que:

1. Conoce y aplica los procedimientos apropiados ante ataques computacionales en términos de preservación y análisis de evidencia de los ataques.

2. Descubre, recolecta y analiza evidencia digital de intrusiones y ataques computacionales en dispositivos electrónicos y, en particular, computadores.

3. Aplica herramientas para monitorear ataques computacionales así como para descubrir, recolectar y analizar la evidencia asociada a dichos ataques.

Metodología Docente	Evaluación General
El curso se desarrollará bajo la estrategia activo-participativa, en donde se utilizarán las siguientes: • Clases expositivas. • Aprendizaje basado en ejercicios y tareas semanales, y un proyecto de curso.	Se utilizarán las siguientes instancias de evaluación: • Ejercicios breves semanales en clase. • Tareas semanales y examen. • Proyecto de curso.

Unidades Temáticas

Número	Nombre de la Unidad	Duración en Semanas
1	**Introducción al Análisis Forense Digital**	4

Contenidos	Resultados de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Introducción al análisis forense, respuesta a incidentes y preservación de evidencia digital. 2. El ambiente del análisis forense 3. Mejores prácticas	El estudiante demuestra que: 1. Justifica la importancia del análisis forense para la investigación de ataques. 2. Identifica las tendencias en análisis forense. 3. Identifica las componentes y procedimientos generales.	[G12, cap. 1 y cap. 2]

Número	Nombre de la Unidad	Duración en Semanas
2	**Herramientas de Análisis Forense**	4

Contenidos	Resultados de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Prevención de escritura 2. Imágenes 3. Análisis visual 4. Almacenamiento seguro 5. Otras herramientas: caso dispositivos móviles.	El estudiante demuestra que: 1. Utiliza herramientas de análisis forense, identificando las situaciones adecuadas para cada herramienta. 2. Identifica los beneficios y limitaciones de las herramientas de análisis forense.	[G12, cap. 3]

Número	Nombre de la Unidad	Duración en Semanas
3	**Análisis Forense en Internet**	2

Contenidos	Resultados de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Investigación y análisis forense en entornos de red como Internet. 2. Caso correo electrónico.	El estudiante demuestra que: 1. Detecta y recupera información relevante a un ataque computacional a partir de herramientas y tecnologías de red. 2. Identifica las técnicas posibles de recuperación de información forense y evalúa su efectividad.	[G12, cap. 4, cap. 7]

Número	Nombre de la Unidad	Duración en Semanas
4	**Reportes de Incidentes**	2

Contenidos	Resultados de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Elaboración de reportes 2. Presentación de reportes.	El estudiante demuestra que: 1. Utiliza procedimientos estandarizados y efectivos para la documentación de una investigación forense. 2. Integra buenas prácticas de documentación forense en sus reportes. 3. Comunica efectivamente los resultados de su investigación a sus pares.	[G12, cap. 8]

Número	Nombre de la Unidad	Duración en Semanas
5	**Discusión de Casos y Proyectos**	3

Contenidos	Resultados de Aprendizaje de la Unidad	Referencias a la Bibliografía
3. Presentación y discusión de proyectos.	El estudiante demuestra que: 1. Utiliza los procedimientos y mejores prácticas de informática forense en la investigación de un caso específico. 2. Comunica efectivamente sus resultados. 3. Analiza y evalúa en forma crítica los resultados de investigaciones de sus pares	[G12]

La variante de postgrado del curso considera una reunión extra semanal y las siguientes responsabilidades adicionales:

1) Habrá un análisis forénsico más profundo, incluyendo análisis de teléfonos inteligentes y tablets. Esto incluirá revisión de los desafíos en forénsica móvil, tales como la gran variedad de dispositivos, interfaces y sistemas operativos, tecnologías no soportadas, e implicaciones en la seguridad y privacidad individual.

2) Habrá un proyecto de curso relativo a forénsica en la nube (“cloud forensics”) el cual podrá incluir los desafíos de propiedad de los datos, control, y respuesta a incidentes. Este proyecto no sólo identificará los desafíos para la informática forense en la nube, sino que también deberá sintetizar posibles soluciones y mecanismos de protección.

3) El estudiante de postgrado estará sujeto a una metodología de evaluación que considera casos desde el inicio del incidente pasando por el control físico del equipo (“device seisure”) hasta el procesamiento y preparación del reporte y presentación. El estudiante de pregrado, por otra parte, estará sujeto a una evaluación más focalizada en casos directos y contenidos, así como en investigaciones de carácter más dirigido.

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

Bibliografía General
• [G12] Digital Forensics Explained, Greg Gogolin con Jason Otting, CRC Press, 2012.

Vigencia desde:	Primavera 2013
Elaborado por:	Greg Gogolin
Revisado por:	Alejandro Hevia