INTRODUCCIÓN A LA FORENSIA DIGITAL	**Carrera/ Plan:** *Licenciatura en Sistemas* Plan 2003-07 / Plan 2012 /Plan 2015 *Licenciatura en Informática* Plan 2003-07 / Plan 2012 /Plan 2015
Año 2017	**Año:** 2017 **Régimen de Cursada:** *Semestral* **Carácter:** *Optativa* **Correlativas**: *Sistemas Operativos* **Profesor/es:** *Einar Lanfranco*
	Hs. semanales: 6 horas

FUNDAMENTACIÓN

La Informática Forense trata sobre la aplicación de técnicas científicas y analíticas en el ámbito de las TICs para identificar, preservar, analizar y presentar datos que sirvan a los fines de una investigación, la cual muchas veces se da dentro de un proceso legal. Para poder llevar a cabo esta tarea no sólo se utilizan tecnologías de punta para procesar información resguardando su integridad, sino que es imprescindible contar con un perfil con un grado de especialización maduro que pueda sostener esta actividad sobre cualquier dispositivo electrónico involucrado o infraestructura tecnológica afectada. Este conocimiento incluye software, hardware, redes, seguridad, hacking, cracking, recuperación de información.

La asignatura “Introducción a la forensia digital” aporta a los alumnos de una visión de los procedimientos y técnicas que se utilizan en este tipo de investigaciones.

El público objetivo son los Interesados en dar los primeros pasos en la forensia digital. Se utilizarán diversos productos de software libre y manejo de máquinas virtuales para los laboratorios, por los que conocimientos previos básicos sobre el uso de GNU/Linux y utilización de software de virtualización son recomendables.

OBJETIVOS GENERALES

- *Introducir a los alumnos en el análisis digital Forense*
- *Consolidar la formación experimental con actividades prácticas sobre todos los temas abordados.*
- *Volcar los conocimientos en actividades prácticas integradoras entre los alumnos y la Cátedra en las que se resuelvan problemas forenses tanto ejercicios simulados, como en el contexto de algún evento internacional de seguridad o con casos reales ante sistemas comprometidos que se puedan conseguir.*

CONTENIDOS MINIMOS (de acuerdo al Plan de Estudios)

- *Cuidado de la evidencia: cadena de custodia*
- *Etapas del análisis forenses*
- *Extracción de evidencias*

- *Filesystems más comunes y su estructura*
- *Recuperación de filesystem*
- *Recuperación de archivos*
- *Reconstrucción de archivos*

PROGRAMA ANALÍTICO

Unidad 1:

- Introducción a la Forensia digital
- Conceptos relacionados
- Metodología y fases de un análisis forense
- Proceso forense
- Escena del crimen

Unidad 2:

- Valoración de la evidencia
- Relevamiento inicial del caso
- Adquisición y verificación de evidencias

Unidad 3:

- Conceptos fundamentales: Particiones y Sistemas de archivos
- Fase de extracción
    - Herramientas
- Investigación de la Evidencia
    - Herramientas

Unidad 4:

- Evaluación de la evidencia
- Aplicando el método científico en la investigación digital
- Intrusiones a computadoras
- Evidencia digital en los SO

Unidad 5:

- Documentación y Reportes
- Comandos y herramientas útiles para la evaluación

BIBLIOGRAFÍA

- Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. U.S. Autor: Department of Justice Office of Justice Programs
- Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. Autor: Eoghan Casey cmdLabs, Baltimore, Maryland, USA. With contributions from: Susan W. Brenner, Bert-Jaap Koops, Tessa Robinson, Bradley Schatz, Brent E. Turvey, Terrance Maguire, Monique Ferraro, Michael McGrath, Christopher Daywalt, Benjamin Turnbull
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Autor: U.S. Department of Justice Office of Justice Programs
- Best Practices For Seizing Electronic Evidence v.3. A Pocket Guide for First Responders. Autor: U.S. Department of Homeland Security United States Secret Service
- File System Forensic Analysis. Brian Carrier . Publisher: Addison Wesley

METODOLOGÍA DE ENSEÑANZA

El alumno recibirá clases teóricas sobre los distintas etapas de un estudio de forensia digital para comprender todas las etapas del mismo. Cada tema dará lugar a un taller práctico sobre el mismo, a la vez que el desarrollo de la curricula vaya avanzando los nuevos talleres estarán relacionados con los talleres prácticos anteriores llegando a completar algún análisis forense completo.
Los talleres prácticos se realizarán utilizando herramientas de software libre de virtualización, las cuales facilitan a cada alumno el montaje de los laboratorios necesarios para la realización de las prácticas.
Todo el soft a utilizar en las prácticas es libre, y por ende su uso legal y de aplicación inmediata por el alumno en el mundo real.

Se utilizará la plataforma de e-learning Moodle (https:/catedras.info.unlp.edu.ar) para:

- *Publicar las clases teóricas.*
- *Publicar los enunciados de los talleres prácticos.*
- *Realizar las entregas de los talleres prácticos.*
- *Realizar las consultas en los foros.*
- *Realizar las comunicaciones de la Cátedra a los alumnos.*

Las soluciones implementadas por los distintos alumnos, serán retroalimentadas a sus compañeros de clase en forma de exposición en clase.

Se trabajará principalmente con los siguiente recursos:

- *Guías, diapositivas, videos, libros, tutoriales y configuraciones a utilizar.*
- *Cañón, PCs, demostraciones de usos de herramientas con ejemplos en vivo.*
- *Herramientas: Sleuthkit, Volatility, Linux, VirtualBox, Autopsy.*
- *Plataforma de e-learning.*

EVALUACIÓN

Algunos prácticos incluirán ejercicios de entrega obligatoria o evaluación online por medio de la plataforma virtual. Las entregas formarán parte del trabajo final para la aprobación de la cursada.

Al finalizar la cursada se toma una evaluación integradora con sus correspondientes recuperatorios.

*La **aprobación de la materia** estará dada por la aprobación de los trabajos prácticos, las evaluaciones online y el resultado de un trabajo integrador formado por todas las entregas parciales necesarias para la aprobación de la cursada mas una extensión del mismo. La asistencia a las clases teóricas aportará a la calificación final.*

La nota promedio de todos los ítems descriptos será la nota final de la materia

CRONOGRAMA DE CLASES Y EVALUACIONES

CRONOGRAMA DE CLASES Y EVALUACIONES

Clase	Fecha	Contenidos/Actividades
1	30/3	• Presentación de la materia. • Conceptos básicos de Seguridad y Privacidad. • Software Libre, licencias, usos, productos. • Introducción a la Forensia digital • Conceptos relacionados
2	6/4	• Metodología y fases de un análisis forense • Proceso forense • Escena del crimen
3	20/4	• Evidencia • Valoración de la evidencia
4	27/4	• Relevamiento inicial del caso • Adquisición y verificación de evidencias
5	4/5	• Adquisición y verificación de evidencias
6	11/5	• Conceptos fundamentales: Particiones y Sistemas de archivos • Fase de extracción
7	18/5	• Herramientas para extracción
8	1/6	• Investigación de la Evidencia • Herramientas de investigación
9	8/6	• Evaluación de la evidencia

		• Aplicando el método científico en la investigación digital • Intrusiones a computadoras • Evidencia digital en los SO
10	15/6	• Documentación y Reportes • Comandos y herramientas útiles para la evaluación
11	22/6	• Presentación de CTFs y retos Forenses. • Desafíos de forensia en dispositivos no estandard
12	29/6	• Presentación de trabajo a realizar por los alumnos
13	6/7	
14	13/7	
15	3/8	
16	10/8	• Presentación de las experiencias de los alumnos en el CTF y retos forenses

Evaluaciones previstas	Fecha
Evaluación online sobre conceptos básicos	13/4
Evaluación sobre Evidencia	11/5
Evaluación etapas de extracción e investigación de evidencia	1/6
Evaluación sobre evaluación de la evidencia	22/6

Para contactar a la cátedra:

- **Mail: einar@info.unlp.edu.ar**
- **Plataforma virtual de gestión de cursos:** https://catedras.info.unlp.edu.ar

Firma del profesor

Einar Lanfranco