

**INTRODUCCION A LA FORENSIA
DIGITAL**

Año 2023

Carrera/ Plan:

*Licenciatura en Informática Plan 2015/Plan 2012/ Plan 2021
Licenciatura en Sistemas Plan 2015/Plan 2012/ Plan 2021
Analista en Tecnologías de la Información y la Comunicación
Plan 2017/Plan 2021*

Año: 2023

Régimen de Cursada: Semestral

Carácter (Obligatoria/Optativa):

Correlativos: Sistemas Operativos

Profesor/es: Einar Lanfranco

Hs. semanales: 2 hs de teoría y 4 hs de práctica.

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.

COMPETENCIAS

Si bien no es una cátedra donde enfocada ni a al auditoría ni a al peritaje, si se cubren parcialmente las cuestiones prácticas como técnicos informáticos de los siguientes items:

- LI-CE8- Efectuar las tareas de Auditorías de los Sistemas Informáticos. Realizar arbitrajes, peritajes y tasaciones relacionados con los Sistemas Informáticos.
- LS-CE7- Efectuar las tareas de auditoría de los sistemas informáticos. Realizar arbitrajes, pericias y tasaciones relacionados con los sistemas informáticos.

Convocaremos peritos y/o auditores a dictar alguna charla durante el desarrollo de la cursada

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 las 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 currícula vaya avanzando los nuevos talleres estarán relacionados con los talleres prácticos anteriores llegando a completar algún análisis forense completo.

Los talleres prácticos se realizan 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 software 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.

Durante todo el semestre se realizará un evento del tipo CTF (Capture the flag), donde se utilizará la gamificación como opción para organizar el desarrollo de los ejercicios prácticos y así fortalecer el interés de los alumnos en los ejercicios al competir entre ellos por ver quién los resuelve primero. Durante sucesivos años hemos realizado este tipo de organización con gran aceptación por parte del alumnado, tradicionalmente esto se monta en un servidor CTFd donde se publican los retos que los alumnos deben resolver.

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, Docker, Timesketch, Plaso.
- Plataforma de CTF
- 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 más 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

| Clase | Fecha | Contenidos/Actividades |
|-------|-------|--|
| 1 | 6/9 | <ul style="list-style-type: none"> • Presentación de la materia. • Conceptos básicos de Seguridad y Privacidad. • Software Libre, licencias, usos, productos. • Introducción a la Forensia digital • Conceptos relacionados |
| 2 | 13/9 | <ul style="list-style-type: none"> • Metodología y fases de un análisis forense • Proceso forense • Escena del crimen |
| 3 | 20/9 | <ul style="list-style-type: none"> • Evidencia • Valoración de la evidencia |
| 4 | 27/9 | <ul style="list-style-type: none"> • Relevamiento inicial del caso • Adquisición y verificación de evidencias |
| 5 | 4/10 | <ul style="list-style-type: none"> • Adquisición y verificación de evidencias |
| 6 | 11/10 | <ul style="list-style-type: none"> • Conceptos fundamentales: Particiones y Sistemas de archivos • Fase de extracción |
| 7 | 18/10 | <ul style="list-style-type: none"> • Herramientas para extracción |
| 8 | 25/10 | <ul style="list-style-type: none"> • Investigación de la Evidencia • Herramientas de investigación |
| 9 | 1/11 | <ul style="list-style-type: none"> • Evaluación de la evidencia • Aplicando el método científico en la investigación digital • Intrusiones a computadoras • Evidencia digital en los SO |
| 10 | 8/11 | <ul style="list-style-type: none"> • Documentación y Reportes • Comandos y herramientas útiles para la evaluación |
| 11 | 15/11 | <ul style="list-style-type: none"> • Presentación de CTFs y retos Forenses. • Desafíos de forensia en dispositivos no estandard |
| 12 | 22/11 | Charla de peritaje informático en el mundo real |
| 13 | 29/11 | <ul style="list-style-type: none"> • Presentación de trabajo a realizar por los alumnos |
| 14 | 6/12 | |
| 15 | 13/12 | |
| 16 | | |
| 17 | 20/12 | <ul style="list-style-type: none"> • Presentación de las experiencias de los alumnos en el CTF y retos forenses |



| Evaluaciones previstas | Fecha |
|--|-------|
| Evaluación online sobre conceptos básicos | 4/10 |
| Evaluación sobre Evidencia | 1/11 |
| Evaluación etapas de extracción e investigación de evidencia | 29/11 |
| Evaluación final | 3/02 |

Contacto de la cátedra (mail, sitio WEB, plataforma virtual de gestión de cursos):

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/los profesor/es



FRANCISCO EINAR