1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos del Análisis Forense
Clave de la asignatura:	CSD-2105
SATCA[1]:	2 – 3 – 5
Carrera:	Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del egresado los conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario.

También aplica normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información. Así como también realizar actividades de auditoría y consultoría relacionadas con la función informática.

Esta asignatura comprende las diferentes técnicas y herramientas de hardware y software que se utilizan para realizar un trabajo pericial, como lo es el analizar sistemas informáticos en busca de evidencia que ayude a efectuar una causa judicial y detectar intrusiones que hayan tenido lugar en sistemas informáticos. También toma curso la investigación en sistemas de información para poder detectar cualquier clase de evidencia de vulnerabilidad que puedan tener y establecer una solución rápida cuando dichas vulnerabilidades ya se han producido.

Intención didáctica

La asignatura se encuentra organizada en cinco temas.

El primer tema es introductorio, se estudian los conceptos del análisis forense. Se ve por dónde empezar a analizar, qué analizar y cómo hacerlo.

En el tema dos se estudian las cookies del sistema, su exploración, la exploración del historial de navegación y favoritos.

El tercer tema trata como un SO usa las bases de datos miniatura, se explora y examinan los hashes de contraseñas. También se trata el cómo develar los hashes de contraseñas y comandos escritos por intrusión.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

El tema cuatro y cinco se propone y estudia una metodología para realizar un análisis forense satisfactorio como: verificar accesos no deseados, comprobar cambios en niveles de ejecución, auditar el modo promiscuo de las tarjetas de red, ubicar software sospechoso y pesado, asegurar conexiones, así como la manera de hacerlo.

Los contenidos se abordarán de manera secuencial como los marca el programa, buscando la aplicación del conocimiento en el mundo real con un enfoque basado en actividades que promuevan en el estudiante el desarrollo de sus habilidades para trabajar de manera práctica.

La extensión y profundidad de los temas es suficiente para garantizar que el estudiante logre las competencias señaladas oportunamente. Por otro lado, el estudiante deberá comprometerse a trabajar permanentemente en el análisis y resolución de ejercicios y problemas a fin de que logre dichas competencias antes de concluir la materia.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Revisión del 26 al 30 de abril del 2021 por parte del Tecnológico Nacional de México Campus Lerdo.	Representantes de los Institutos Tecnológicos Superiores de: Instituto Tecnológico Superior de Lerdo.	Reunión para el Análisis y Diseño por competencias de la Especialidad de "*Ciberseguridad*".

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
● Comprende los conceptos necesarios de informática forense. ● Evalúa quién ha invadido (hackeado) un sistema informático con Windows, Unix o GNU Linux. ● Valora cómo un atacante ha logrado realizar un ingreso no deseado. ● Comprueba cuándo un Hacker ha tenido una intrusión en un sistema informático.

5. Competencias previas

- Se recomiendan las competencias desarrolladas y adquiridas en la materia de Gestión de amenazas.
- Habilidades de gestión de información, en la búsqueda y análisis de información de diferentes fuentes.
- Habilidades cognitivas de abstracción, análisis, síntesis y reflexión.
- Capacidad de pensamiento lógico, analítico y crítico.

6. **Temario**

No.	Temas	Subtemas
1	Introducción	1.1. Flujo de datos alternos, ocultación típica. 1.2. Visualización de datos ocultos descubiertos. 1.3. Datos EXIF. 1.4. Tablas de cuantización de la evidencia. 1.5. Minado de datos. 1.6. Metadatos.
2	Análisis de Cookies.	2.1. Concepto y definición. 2.2. Tipos de cookies. 2.3. Datos del intruso. 2.4. Desencriptando cookies. 2.5. Historial de navegación. 2.6. Aplicaciones ejecutadas por un intruso. 2.7. Recursos de versión y caché MUI (Interfaz de usuario multilenguaje)
3	Base de datos de miniatura en el SO y objetos fuera de lo normal.	3.1. Extracción de nombres de aplicación. 3.2. Hashes de contraseña. 3.3. Detección de objetos sin permisos de lectura. 3.4. Develar comandos escritos por intrusión. 3.5. Detección de directorios sin permiso de lectura.
4	Metodología forense Parte 1	4.1. Verificar Hash del Kernel. 4.2. Verificar proceso de inicialización. 4.3. Verificar accesos no deseados. 4.4. Comprobación de cambios en los niveles de ejecución. 4.5. Auditoría en el modo promiscuo de las NIC's. 4.6. Encontrar intentos de elevación de privilegios.
5	Metodología forense Parte 2 (Datos ocultos)	5.1. Cambios en los paquetes de software. 5.2. Ubicación de software pesado. 5.3. Verificación de procesos en ejecución. 5.4. Aseguramiento de conexiones permitidas en los nodos. 5.5. Comprobar la especificación de privilegios. 5.6. Técnica antiforense en metadatos. 5.7. Construcción de un medio-forensis encriptado.

		5.8. Extracción de evidencia en accesos protegidos.

7. Actividades de aprendizaje de los temas

Introducción	
Competencias	Actividades de aprendizaje
Específica(s): ● Conoce y comprende la importancia de la informática forense. ● Infiere dónde empezar a analizar, qué analizar y cómo hacerlo. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Realizar un esquema con la importancia de la informática forense. ● Elaborar una infografía acerca de dónde empezar a analizar, qué analizar y cómo hacerlo. ● Investigar ¿Qué son los datos EXIF? ● Investigar ¿Qué son los metadatos de una imagen descubierta? ● Realizar un minado de datos.
Análisis de Cookies y base de datos miniatura	
Competencias	Actividades de aprendizaje
Específica(s): ● Explora y analiza las cookies del sistema, su historial y favoritos. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Explorar las cookies, historiales y favoritos y hacer un reporte. ● Hurgar entre los datos del intruso. ● Investigar ¿Qué es la caché MUI? ● Realizar las prácticas del tema.
Base de datos de miniatura en el SO y objetos fuera de lo normal	
Competencias	Actividades de aprendizaje
Específica(s): ● Explora y analiza las bases de datos miniatura del SO.	● Investigar cómo ubicar las bases de datos miniatura del SO.

● Descubre los hashes de contraseñas y comandos escritos por intrusión. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Poblar en una tabla el resultado de la extracción de los hashes de contraseña. ● Elabora un esquema de cómo detectar objetos sin permiso general de lectura. ● Elabora un esquema de cómo develar los comandos escritos por el intruso. ● Elabora un esquema de cómo detectar directorios sin permiso general de lectura.
Metodología forense Parte 1	
Competencias	Actividades de aprendizaje
Específica(s): ● Organiza una metodología para realizar un análisis forense satisfactorio. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Realiza una reseña de cómo Verificar el Hash del Kernel. ● Realiza una descripción de cómo verificar el proceso de inicialización. ● Elabora un diagrama de cómo verificar accesos no deseados. ● Explicar cómo comprobar cambios en los niveles de ejecución. ● Exponer cómo encontrar intentos de elevación de privilegios.
Metodología forense Parte 2 (Datos ocultos)	
Competencias	Actividades de aprendizaje
Específica(s): ● Organiza una metodología para realizar un análisis forense satisfactorio. ● Descubre datos ocultos. ● Crea una herramienta en algún medio de almacenamiento de manera encriptada para utilizarlo en un contexto forense. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita.	● Crea una infografía de cómo auditar el modo promiscuo en las NICs. ● Ilustrar cómo asegurar las conexiones permitidas en los nodos. ● Realiza un informe de cómo ubicar software “pesado”. ● Exponer un ejemplo de técnica anti-Forense en metadatos. ● Investigar cómo extraer evidencias en accesos protegidos por Windows.

● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	

8. Práctica(s)

- Encontrar los datos ocultos por el intruso.
- Investigando el disco duro, puentear el SO.
- Visualizar los datos ocultos descubiertos.
- Encontrar datos EXIF
- Compilar una herramienta de detección.
- Analizar y elaborar “Tablas de Cuantización” de la evidencia.
- Realizar minado de datos a la página de la víctima.
- Analizar los Metadatos de una imagen descubierta.
- Desencriptar Cookies del intruso.
- Ahondar en los “Recursos de versión y la caché MUI”.
- Explorar cookies, historiales y favoritos.
- Ubicar las bases de datos de miniaturas en el sistema víctima.
- Ubicando hashes de contraseñas en el archivo descubierto.
- Detectar objetos sin permiso general de lectura.
- Descubrir los comandos escritos por el intruso.
- Detectar directorios sin permiso general de lectura.
- Verificar el Hash del Kernel.
- Verificar el proceso de inicialización.
- Verificar accesos no deseados.
- Comprobar cambios en los niveles de ejecución.
- Auditar el modo promiscuo en las NICs.
- Encontrar intentos de elevación de privilegios.
- Auditar cambios en los paquetes de software.
- Ubicar software “pesado”.
- Verificar los procesos en ejecución.
- Asegurar las conexiones permitidas en los nodos
- Comprobar la especificación de privilegios.

9. Proyecto de asignatura

- Planificar y ejecutar un proyecto / trabajo Forense donde se detecten las intrusiones que hayan tenido lugar en algún sistema informático.
- Diseñar un plan metodológico forense de detección de singularidades o anormalidades. (por ejemplo, verificar el kernel, el proceso de inicialización del sistema, accesos y cambios de niveles de ejecución, NICs promiscuas, intentos de elevar privilegios, cambios en el software, procesos anormales, escaneos, etc.)

10. Evaluación por competencias

La evaluación debe ser continua, formativa y sumativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Evaluación diagnóstica.
- Investigación en diversas fuentes de información.
- Desarrollo de actividad(es) y reporte de prácticas.
- Exposición de temas específicos.
- Exámenes teóricos - prácticos que demuestre parte del conocimiento adquirido durante la asignatura.

11. Fuentes de información

Helmer Muñoz, J. D. (15 de 10 de 2020). Informática forense y auditoría forense: Nuevas perspectivas en tiempos de COVID-19. *Espacios*, pág. 13.

Lorenzo, J. A. (18 de 08 de 2020). *Mejores herramientas gratuitas de informática forense*. Obtenido de redeszone.net: https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

Martha Irene Romero Castro, E. A. (2020). *LA INFORMÁTICA FORENSE DESDE UN ENFOQUE PRÁCTICO.* Manabí, Ecuador: Editorial Área de Innovación y Desarrollo,S.L.

Mikhaylov, I. (2017). *Mobile Forensics Cookbook, Data acquisition, extraction, recovery techniques, and investigations using modern forensic tools.* Birmingham, UK: Packt Publishing Ltd.

Parasram, S. V. (2017). *Digital Forensics with Kali Linux.* Birmingham, UK: Packt Publishing Ltd.

Parasram, S. V. (2020). *Digital Forensics with Kali Linux, Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux.* Birmingham, UK: Packt Publishing Ltd.

Preston Miller, C. B. (2019). *Learning Python for Forensics, Leverage the power of Python in forensic investigations.* Birmingham, UK: Packt Publishing Ltd.

Tapia, M. E. (05 de 2021). *Foro de Seguridad*. Obtenido de forodeseguridad.com: http://www.forodeseguridad.com/artic/discipl/4166.htm