E&S Engineering & Services	Curso Metodológico	Universidad El Bosque – Escuela 4Ri
GUIA DE ACTIVIDADES		

CURSO	Informatica Forense
DESCRIPCIÓN	Guía de actividades
COMPETENCIAS A DESARROLLAR	El estudiante afianza los conceptos básicos, adquiere habilidades teórico-práctico, para la realización de informes forenses, al finalizar el curso tendrá juicio suficiente para realizar una investigación, entendiendo desde la visión de ciberseguridad y desde el rol del atacante.

Bienvenidos al curso de Informática forense

Este curso tiene la intención de llegar a personas que quieran obtener conocimientos sobre la informática forense, así no esté dentro de sus actividades diarias. Dirigido a personas que buscan un mayor conocimiento acerca de los principales fundamentos sobre los que trabajan las principales herramientas de informática forense.

El curso de informática forense está constituido por 3 módulos, 50 temas, incluyendo temas de apoyo que serán indispensables en el desarrollo del curso, enfocados en la implementación actual de la informática forense.

CURSO INFORMATICA FORENSE

Módulo 1:

1.1 Introducción a la informática / auditoria forense

- Definición: qué es exactamente la informática forense.
- Finalidad de un análisis forense.
- Principales razones que desencadenan un análisis forense.
- La cadena de custodia.

1.2 Vertientes de un análisis forense

1.2.1 Dispositivos de almacenamiento

- Identificación de objetivos
- Preservación de evidencias
    - Metodología de trabajo

  - Procedimiento de clonado
  - Revisión del checksum
  - Herramienta

- Recuperación y análisis
  - Recuperación de datos borrados / perdidos
  - Aplicación de técnicas de análisis sobre los datos adquiridos
- Presentación de resultados y objetivos del proceso de análisis forense
  - Importancia de la documentación durante el proceso
  - Herramientas y técnicas de análisis forense.

Módulo 2

Análisis práctico de los fundamentos y las posibles dificultades de un análisis informático forense

2.1 Analizando los fundamentos forenses

- Estructura física de un disco duro
- Estructura lógica de un disco duro
- FAT
- NTFS
- EXT2, EXT3, EXT4
- HFS+
- APFS

Borrado de datos

- Qué es realmente el borrado
- Borrado seguro
- Recuperación de datos borrados

2.2 Posibles dificultades en un análisis forense

- Sectores defectuosos
- Condiciones de trabajo adversas
- Discos duros dañados
- Sistemas RAID

- Encriptación
- Antiforénsica

Módulo 3

Realización práctica del proceso de recopilación de evidencias y análisis de las mismas. Los asistentes se familiarizan con el proceso y con las herramientas más comúnmente utilizadas en el Análisis Informático Forense.

3.1 Recopilación de evidencias

- Metodología de trabajo
- Diferentes herramientas para clonado de discos duros y teléfonos móviles

3.2 Análisis de datos y reconstrucción de evidencias

3.2.1 Análisis informático con distintas herramientas software de investigación

Utilización de herramientas:

- EnCase
- WinHex

Para el desarrollo de las actividades:

- Visualice todos los videos
- Desarrolle las prácticas propuestas
- Desarrolle las evaluaciones

  Como evidencia elabore un documento cumpliendo normas APA donde agregue toda la información pertinente a las actividades.

Temáticas a desarrollar:

Unidad 1 – Introducción a la informática / auditoria forense

Unidad 2 – Análisis práctico de los fundamentos y las posibles dificultades de un análisis informático forense

Unidad 3 –Análisis de evidencia y entendimiento desde el punto de vista del atacante

	Curso Metodológico	
GUIA DE ACTIVIDADES		

DESARROLLO DE LAS ACTIVIDADES DEL CURSO

1) Al iniciar el curso realizará una actividad de pre-saberes, que tiene como finalidad conocer cuáles son sus bases frente al tema de Informática forense utilizando una herramienta informática llamada educaplay, test de 8 preguntas. En el siguiente enlace:

:https://es.educaplay.com/recursos-educativos/8562610-presaberes_curso_inf_forense.html

2) Una vez desarrolle la actividad individual, es necesario que la socialice con sus compañeros dentro del foro, esto con el fin de que estos aportes se conviertan en la base para las siguientes fases de la estrategia de aprendizaje.

3) Finalizando EL módulo 2, se realizará el laboratorio y una evaluación que dará el 25 % de la nota el curso un análisis de caso de la eps "vida sana "ubicado en el carpeta de actividades delito por fraude, también realizará el análisis y la actividad práctica ubicada en la carpeta de actividades mediante el cual realizará un cuadro comparativo teniendo en cuenta los delitos mencionados en este análisis, de la siguiente manera , delito, tipo de delito y pena o multa, con un mínimo de 10 ejemplos
4) Al finalizar el curso el estudiante presentará la evaluación final que tiene un valor del 30 %, y un laboratorio denominado "Adquisición de datos ", donde se aplicará los conocimientos adquiridos, el laboratorio se encuentra dentro de la carpeta módulo 3, una vez realizado y aplicando cada una de las ilustraciones del video donde está el laboratorio, el estudiante realizará el entregable, con las normas APA, y mostrará la evidencia de la aplicación del Laboratorio.
5) Dentro de la carpeta de actividades el estudiante podrá ver otro estudio del caso, para su respectivo análisis y socialización en el foro.

Uso de referencias, Normas APA

Políticas de plagio: Se considera como faltas que atentan contra el orden académico: "El plagio, es decir, presentar como de su propia autoría la totalidad o parte de una obra, trabajo, documento o invención realizado por otra persona. Implica también el uso de citas o referencias falsas, o proponer citar donde no haya coincidencia entre ella y la referencia", "El reproducir, o copiar con fines de lucro, materiales educativos o resultados de productos de investigación, que cuentan con derechos intelectuales reservados.

E&S Engineering & Services Training, Consulting and Engineering Services	Curso Metodológico	UNIVERSIDAD EL BOSQUE ESCUELA 4Ri FACULTAD DE INGENIERÍA
GUIA DE ACTIVIDADES		