Programa del curso

Semestre 2021-10

Nombre del curso:	Computación Forense: Delitos informáticos, Aspectos Legales y Evidencia Digital
Créditos:	4
Profesores	Ing. Juan Diego Jiménez (jujimene@uniandes.edu.co)
Versión PDF	Ver

Descripción

En este curso se conocerán los elementos involucrados en una investigación forense digital, teniendo en cuenta la importancia que toma cada vez más el uso de dispositivos móviles, y el uso de la nube. Se explorarán algunas técnicas de recolección, preservación, análisis y presentación de la evidencia digital. Se expondrán conceptos referentes a la importancia de los datos que se recuperan y como estos pueden ser interpretados como información y/o evidencia, acercándolos lo mejor posible a la escena del evento ocurrido. Fundamentos de preservación de la evidencia digital, la cual es frágil por su misma naturaleza. Además, tendrán la oportunidad de conocer y manejar todo el contexto Nacional e internacional, de los aspectos legales que se involucran y de conformidad poder, dirigir, tomar y presentar evidencias digitales y en general pruebas técnicas, con toda la legalidad que estas requieren.

Objetivos

Al final del curso el estudiante podrá:

- Entender los conceptos, principios y elementos que involucran en la computación forense y su uso en los diferentes casos de seguridad de la información.
- Adquirir conceptos básicos de las diferentes tecnologías que se trabajan en el día de hoy y su relación con la computación forense.
- Elaborar un levantamiento post-mortem basado en un incidente y generar una imagen forense.
- Identificar y realizar una correcta preservación de la evidencia y el manejo de la cadena de custodia
- Realizar el respectivo análisis sobre imágenes forenses presentadas como evidencias digitales.
- Entender los conceptos y elementos legales que se involucran en la computación forense y el entorno de un marco jurídico colombiano.

Contenido

Semana	Fecha	Tema	Profesor
1	* Introducción. *Definiciones y elementos fundamentales en la computación forense. *Gestión de Incidentes y la Computación Forense	Enero 21	Juan Diego Jiménez
2	*Forensic Laboratory Sizing *Sistemas de Archivos	Enero 28	Juan Diego Jiménez
3	*Sistemas Operativos	Febrero 4	Juan Diego Jiménez
4	*Proceso de Investigación *ISOS *Identificación y Planeación	Febrero 11	Juan Diego Jiménez
5	**Primer Parcial** *Preservación de la escena	Febrero 18	Juan Diego Jiménez
6	*Recomendaciones y acciones en un ámbito Judicial	Febrero 25	Coronel Freddy Bautista
7	*Análisis Forense	Marzo 3	Juan Diego Jiménez
8	*Perfilamiento *Adquisición de la evidencia	Marzo 10	Juan Diego Jiménez
9	**Semana Receso**	Marzo 17	**Semana Receso**
10	*Judicialización Delitos Informáticos	Marzo 24	Coronel Freddy Bautista
11	*Herramientas y técnicas utilizadas por la policía judicial	Marzo 31	Coronel Freddy Bautista
12	**Semana santa**	Marzo 17	**Semana santa**
13	**Segundo Parcial** *Técnicas Anti forenses	Abril 14	Juan Diego Jiménez
14	*Delitos Informáticos y sus Aspectos Legales en la Computación Forense.	Abril 21	Ricardo Posada (Facultad de Derecho)
15	*Delitos Informáticos y sus Aspectos Legales en la Computación Forense.	Abril 28	Ricardo Posada (Facultad de Derecho)

16	*Delitos Informáticos y sus Aspectos Legales en la Computación Forense.	Mayo 5	Ricardo Posada (Facultad de Derecho)
17	Presentación de Informe y Evidencia	Mayo 12	Juan Diego Jiménez
18	Análisis de caso practico	Mayo 19	Juan Diego Jiménez

Metodología

El desarrollo del curso se efectuará por medio de explicaciones dadas por el profesor en el aspecto teórico y reforzado con los talleres y proyectos en temas específicos. También se estimulará la participación activa del estudiante mediante trabajos de investigación con la debida sustentación ante el profesor y el curso.

Evaluación

El desarrollo del curso es estrictamente presencial. Se dispondrá de 2 exámenes, una serie de laboratorios, un proyecto y un examen final. Los porcentajes serán los siguientes:

Evaluación	%	Fecha
1er Parcial	20	18 de Febrero
2do Parcial	20	14 de Abril
Laboratorios y Quices	20	Cada uno tiene fecha
Proyecto CASO ESTUDIIO	20	Por definir
Final	20	Por definir

Calificación final:

En este curso las calificaciones definitivas no tendrán aproximaciones, la nota final es la suma de todas las evaluaciones.

Generalidades

- Clases: 3 horas semanales, de asistencia obligatoria. Durante las clases el profesor llevará una bitácora de presencia de los estudiantes como registro de asistencia. El estudiante que no asista al menos al 80% de las clases y sesiones de trabajo supervisado no podrá aprobar el curso.
- La grabación por cualquier medio, de este curso NO está autorizada. En caso de requerirla realice una solicitud por escrito dirigida al profesor del curso justificando las razones.

- Los canales oficiales de comunicación del curso son el correo electrónico de uniandes, la lista de correo del curso y SICUA+, http://sicuaplus.uniandes.edu.co.

Disposiciones del Curso

  - Los exámenes, quizzes, tareas y proyectos se deben realizar individualmente a menos que el profesor indique lo contrario explícitamente. Cualquier incumplimiento de esta norma se considera copia.
  - Las tareas y los proyectos se deben entregar en la fecha que se indique al enunciarlas (se entregan, no se recogen). Los trabajos que no se entreguen o lleguen a entregarse por fuera de horario y fecha acordada, se calificarán con cero.
  - Si se presenta algún inconveniente para presentar o entregar un parcial o trabajo en la fecha indicada, se debe avisar al profesor con anterioridad a la misma.
  - Los trabajos en grupo son en grupo; es decir, todo el grupo responde solidariamente por el contenido de todo el trabajo, y lo elabora conjuntamente (no es trabajo en grupo repartirse puntos o trabajos diferentes).
  - Para los trabajos en grupo, se puede solicitar una sustentación a cualquier miembro del grupo sobre cualquier parte del trabajo. El resultado de la sustentación afectará la nota de todos los miembros del grupo.
  - En caso de que se realice algún reporte, tenga en cuenta lo siguiente:
    - Exprese las ideas en sus propios términos, y, si no son originales suyos, haga referencia al autor.
    - Si transcribe información textualmente, póngala entre comillas, indique este hecho explícitamente, así como quién es el autor y de dónde se obtuvo la información. Evite poner mucho texto, o textos muy largos, entre comillas (¡mucho texto entre comillas indica que no hubo mayor aporte suyo!). Exprese su propia comprensión del tema.
    - Incluya bibliografía (en el caso de Internet, URL, y, de ser posible, autor y/o corporación).
  - Recuerde que el plagio es una forma de fraude académico

- Si un estudiante falta a la presentación de una evaluación debidamente programada, podrá ser calificado con cero (0,0). Sin embargo, el estudiante podrá justificar su ausencia ante el profesor dentro de un término no superior a (8) días hábiles siguientes a la realización de la prueba. Justificada la inasistencia el profesor deberá indicarle al estudiante la nueva fecha y hora en que le realizará el examen, dentro de las dos (2) semanas siguientes a la aceptación de la justificación presentada.

Bibliografía

[1] Brian Carrier. File System Forensic Analysis. 1st Edition : TSO, 2005 [2] Keith J. Jones, Richard Bejtlich, Curtis W. Rose. Real Digital Forensics. 1st Edition : TSO, 2005 [3] Andrew Hoog. Android Forensics: Investigation, Analysis and Mobile Security for Google Android. 1st Edition : TSO 2011 [4] Cory Altheide. Digital Forensics with Open Source Tools. 1st Edition TSO 2011 [5] ISO/IEC 27000-1:2013, Estándar de un sistema de gestión de la seguridad de la información. [6] Harlan Carvey. Widows Forensic Analysis Toolkit. 4th Edition TSO [7] Chris Pogue. Unix and Linux Forensic Analysis. 1st Edition TSO 2008