1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia

ANALISIS FORENSE DIGITAL

Clave de la materia:	Horas de teoría:	Horas de práctica:	Total de Horas:	Valor en créditos:
IC464	40	40	80	8

Tipo de curso: (Marque con una X)											
C= Curso		P= Práctica		CT = Curso–Taller	x	M=Módulo		C= Clínica		S= Seminario	

Nivel en que ubica: (Marque con una X)			
L=Licenciatura	x	P=Posgrado	

Prerrequisitos formales (Materias previas establecidas en el Plan de Estudios)	Prerrequisitos recomendados (Materias sugeridas en la ruta académica aprobada)

Departamento:	Ciencias Exactas y Tecnología	
Carrera:	Licenciatura en Tecnologías de la **Información**	
Área de formación:	Especializante Selectiva	
Historial de revisiones:	Fecha:	Responsable:
Elaboración	13 de Marzo del 2018	**Mtro. Victor Becerra Cordoba**

Academia: Cómputo	
Aval de la Academia:	

2. OBJETIVO GENERAL

Formar en el alumno el conocimiento de las bases y requisitos para llevar a cabo el análisis forense digital, con un enfoque teórico-práctico, aplicando algunas de las técnicas de computo forense, abarcando las áreas legales e informáticas.

3. CONTENIDO

Temas y Subtemas
Unidad I.- METODOLOGÍA JURÍDICA DE LA INVESTIGACIÓN 1.1. Introducción al cómputo forense 1.2. Conceptos básicos 1.3. Proceso de análisis forense 1.4. Cadena de custodia 1.5. Análisis del cumplimiento de la cadena de custodia 1.6. Dictamen pericial Unidad II. – TÉCNICAS DE LOS PRINCIPALES DELITOS INFORMÁTICOS 2.1. Introducción 2.2. Conductas y patrones de comportamiento de ciber criminales 2.3. Pishing y análisis forense de dominios 2.4. Análisis del funcionamiento de tarjetas de bancarias 2.5. Análisis e interpretación de metadatos de archivos y sus propiedades de usuario, sistema, EXIF para geolocalización.

2.6. Navegación en internet de forma oculta con navegadores o sistemas especiales.
2.7. Metodología de la informática forense

Unidad III.- REDES INORMÁTICAS Y HERRAMIENTAS FORENSES
3.1 Introducción a las redes informáticas
3.2 Tipos de herramientas para análisis forense y su aplicación
3.3 Herramientas para detectar vulnerabilidades en redes.
3.4 Uso de sniffer y minería de paquetes para análisis de red
3.5 Interpretación de datos de tráfico de red
3.6 Equipos de infraestructura de red contemplados dentro del análisis forense digital
3.7 Herramientas generales y de propósito específico para análisis forense digital

Unidad IV.- EVIDENCIA FÍSICA
4.1. Introducción
4.2. Clasificación de dispositivos contemplados como evidencia física
4.3. Características de dispositivos de evidencia física
4.4. Estructura de dispositivos de almacenamiento
4.5. Herramientas para análisis de evidencia física

Unidad V.- EVIDENCIA DIGITAL
5.1. Introducción
5.2. Análisis de caso de estudio para toma de decisiones con evidencia digital
5.3. Memoria volátil
5.4. Proceso para creación de imágenes de discos
5.5. Proceso para creación de volcado de memoria RAM
5.6. Proceso para preservar la evidencia
5.7. Herramientas para análisis de evidencia digital

Unidad VI. SISTEMAS VIRTUALES
6.1. Introducción
6.2. Análisis de imágenes de discos duros
6.3. Análisis de volcado de memoria RAM
6.4. Análisis y proceso de sistemas virtuales
6.5. Herramientas para análisis de sistemas virtuales

Unidad VII.- SISTEMAS DE ARCHIVOS
7.1. Introducción
7.2. Tipos de sistemas de archivos
7.3. Estructura de los sistemas de archivos
7.4. Funcionamiento de los sistemas de archivos
7.5. Herramientas para análisis de sistemas de archivos

Unidad VIII.- ANALISIS FORENSE A SISTEMAS OPERATIVOS WINDOWS
8.1. Introducción
8.2. Gestión de registro de Windows
8.3. Gestión de la papelera de reciclaje
8.4. Sesiones en Windows
8.5. Herramientas para análisis a sistema operativo Windows

Unidad IX.- ANALISIS FORENSE A SISTEMAS OPERATIVOS LINUX
9.1. Introducción
9.2. Gestión de kernel
9.3. Sesiones en Linux
9.4. Gestión de procesos
9.5. Herramientas para análisis a sistema operativo Windows

Unidad X.- Análisis Forense en Dispositivos Móviles
10.1. Introducción
10.2. Características de dispositivos IOS
10.3. Características de dispositivos Android
10.4. Aspectos básicos para análisis forense en dispositivos IOS
10.5. Aspectos básicos para análisis forense en dispositivos Android
10.6. Herramientas para análisis a dispositivos

4. BIBLIOGRAFÍA BÁSICA (Preferentemente ediciones recientes, 5 años)

Libro: Análisis forense de sistemas informáticos. Helena Rifà Pous (coordinadora), Jordi Serra Ruiz (coordinador), José Luis Rivas López (2009). ISBN: 978-84-692-3343-6

Libro / Revista: Computer Forensics – Evidence Collection & Preservation. ISBN-13: 978-1-4354-8349-1

Libro: Practical Digital Forensics. Richard Boddington.Editorial Packt Publishing. ISBN 978-1-78588-710-9

Libros / Revistas Libro: Windows Forensic Analysis toolkit. Advances analysis techniques for Windows 8.
Harlan Carvey (2014) Elsevier No. Ed 4

ISBN: ISBN: 978-0-12-417157-2

Libro: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.
Michael Hale Ligh, Andrew Case (2014) Wiley No. Ed 1

ISBN: ISBN: 1118825098

Libro: Digital Forensics with Open Source Tools.
Cory Altheide y Harlan Carvey, (2011) Syngress No. Ed 1

ISBN: ISBN: 1597495867

Libro: Cybersecurity and Cyberwar: What Everyone Needs to Know
P.W. Singer y Allan Friedman (2014) Oxford University Press No. Ed 1

ISBN: ISBN 978-0-19-991811

Libro: Android Malware and Analysis.
Ken Dunham (2014) CRC Press No. Ed 1

ISBN: ISBN-13: 978-1482252194