Red de Centros de Excelencia de la UIT para la Región de las Américas

INSTITUTO NACIONAL DE INVESTIGACIÓN Y CAPACITACIÓN DE TELECOMUNICACIONES

Curso en línea

ANALISIS FORENSE DIGITAL

INFORMACIÓN GENERAL DEL CURSO

DESCRIPCIÓN DEL CURSO

Título	**ANALISIS FORENSE DIGITAL**
Objetivo	Conocer y familiarizarse con los elementos involucrados en una investigación forense en informática. Explorar técnicas de colección, preservación, análisis y presentación de la evidencia digital.
Duración	40 horas
Costo de formación	**USD 150.00**
Código del curso	**21OI26458AMS-S**

DESCRIPCIÓN DEL CURSO

Este curso está desarrollado considerando los estándares para las mejores prácticas en investigaciones digitales. También está dedicado a aumentar el nivel de conocimiento, comprensión y habilidades en ciberseguridad e investigación. El curso provee las habilidades necesarias para la identificación de huellas digitales y la recopilación de evidencia en caso de persecución penal. La certificación fortifica el nivel de aplicación de conocimientos de quien esté interesado en la integridad de las redes e investigaciones digitales.

RESULTADOS DEL APRENDIZAJE

Al finalizar el curso el estudiante tendrá toda la información pertinente a los aspectos teóricos que enmarcan el mundo de la informática forense, además tiene la oportunidad de explorar algunas técnicas a través de los laboratorios que se realizarán a lo largo del curso.

A QUIÉN VA DIRIGIDO

Profesionales en tecnología de la información, miembros de equipos de respuesta a incidentes, administradores de seguridad de la información, abogados, ingenieros de sistemas, personal policial, ministerio público y cualquier interesado en investigaciones de cómputo forense y seguridad informática.

REQUISITOS DE ADMISIÓN

Se recomienda poseer formación o experiencia en alguna rama de la informática, a nivel técnico o a nivel de gestión.

TUTORES / INSTRUCTORES

Nombre del Tutor / Instructor	Información de Contacto
Juan Carlos Zegarra Vasquez	**jcarlos2411@hotmail.com**
Especialista certificado en Sistemas de Gestión de Seguridad de la Información ISO27001, con cursos de Análisis ISO27001, Análisis y Tratamiento de Riesgos, Implementación de Sistemas de Gestión de Seguridad de la Información, Auditoria de Sistemas de Gestión Seguridad de la Información, Análisis de Legislación y Delitos Informáticos, Planes de Continuidad de Negocios, Técnicas de Defensa y Protección de Infraestructura, Ethical Hacking, Networking. Oficial de Seguridad. 20 años de experiencia en empresas de Telecomunicaciones, Sector Privado y Sector Estatal. Docente en Seguridad de la Información y Analista Forense en INICTEL.	

CONTENIDO DEL CURSO

Tema 1. Informática forense en el mundo de hoy

1.1. La informática forense
1.2 Historia de los delitos informáticos
1.3 Cuáles son los objetivos de la informática forense
1.4 El investigador forense

Tema 2. Proceso de Investigación de Informática Forense

2.1 Identificación del incidente: búsqueda y recopilación de evidencias
2.2 Descubrir las señales del ataque
2.3 Recopilación de evidencias
2.4 Preparación para el análisis
2.5 Reconstrucción de la secuencia temporal del ataque
2.6 Identificación del autor o autores del incidente
2.7 Evaluación del impacto causado al sistema
2.8 Documentación

Tema 3. Entendiendo los discos duros y los sistemas de archivos

3.1 Discos duros
3.2 Estructura lógica
3.3 Estructura física
3.4 Discos IDE, ATA o PATA, SAS, SATA, SCSI
3.5 El Sistema de archivos
3.6 NTFS
3.7. EXT4

Tema 4. Forense del Sistema Operativo (3 horas)

4.1 Identificación y obtención de evidencias volátiles
4.2 Extracción de datos no volátiles
4.3 Creación de la imagen forense
4.4 Información de Sistema
4.5 Logs
4.6 Firewall
4.7 Ejecutables no firmados

Tema 5. Derrotar las técnicas anti-forenses

5.1 Técnicas de borrado o destrucción de la información
5.2 Técnicas de ocultación de la información
5.3 Técnicas de sobreescritura de metadatos
5.4 Técnicas de cifrado de la información
5.5 Otras técnicas.

Tema 6. Adquisición y duplicación de datos

6.1 Obtención de la información dinámica o en procesamiento
6.2 Generación de imagen forense
6.3 Análisis de imagen forense

Tema 7. Forense de la Red de comunicaciones
7.1 Conceptos básicos de TCP/IP
7.2 Network Miner. Ejecutándolo por primera vez
7.3 Análisis de los archivos capturados
7.4 WinPcap

Tema 8. Investigando los ataques web
8.1 Los registros (logs)
8.2 mod_log_forensics
8.3 Vinculación con los logs de acceso regulares

Tema 9. Forense de la Base de datos
9.1 Características de las bases de datos
9.2 Auditoria de bases de datos
9.3 Registros logs

CRONOGRAMA DEL CURSO

Semana / Sesión	Tema	Ejercicios e interacciones
Semana 1	Informática forense en el mundo de hoy Proceso de Investigación de Informática Forense	Practica del Proceso de Investigación de Informática Forense
Semana 2	Entendiendo los discos duros y los sistemas de archivos Forense del Sistema Operativo	Laboratorio Forense del Sistema Operativo
Semana 3	Derrotar las técnicas anti-forenses Adquisición y duplicación de dato Ataques WEB	Laboratorio Derrotar las técnicas anti-forenses Laboratorio Adquisición y duplicación de dato
Semana 4	Forense de la Red de comunicaciones Forense de la Base de datos	Laboratorio de Forense de la Red de comunicaciones Laboratorio de Forense de la Base de datos

METODOLOGIA

El presente curso es en línea/asincrónico. La metodología que orienta este curso será eminentemente participativa. La estrategia metodológica utilizada para el desarrollo de curso propone al participante una diversidad de actividades.

Se espera que cada estudiante participe mediante la lectura del material que estará disponible desde el inicio del curso, aportes escritos a los debates, foros, actividades, ejercicios de refuerzo y exámenes que

serán definidos y los cuales serán realizadas en forma asincrónica. Esta técnica asegurará la flexibilidad de tiempo necesaria para que cada participante pueda organizarse de la manera que mejor le convenga.

Los participantes aprobados en el curso según los criterios de evaluación que sean indicados por los tutores y todos aquellos que sean aprobados recibirán un Certificado que será emitido por vía electrónica

EVALUACIÓN Y CALIFICACIÓN

El curso propone un sistema de evaluación combinado el cual se compone de: foros de debate, actividades y evaluaciones. Las fechas de cada uno de estos ítems están definidas en el cronograma. El sistema de calificación de este curso se explica a continuación junto con los porcentajes de peso de cada una de las actividades a evaluar.

Pesos de evaluación

- Foro de debate (20%): Tendrán un peso del 20% sobre la calificación final. Se realizará 1u 2 foros de debate en el curso. Cada estudiante deberá participar un mínimo de dos veces en el foro con aportes de valor para obtener el 100% del porcentaje semanalmente. En caso de participar una vez obtendrá en 50% y en caso de no participar será un 0%.
- Actividades (60%): también denominados retos, actividades, laboratorios u trabajos individuales tendrán un peso total del 60% y estarán compuestas de algunas de estas opciones: desarrollo de trabajos individuales, retos trabajos grupales, actividades con entrega en la plataforma.
- Evaluaciones (20%): Las evaluaciones del presente curso tendrán un peso total del 20% y podrán efectuarse mediante dos exámenes en línea, El esquema para este curso está indicado en el cronograma de actividades.
- Aprobación: Para aprobar este curso se debe completar un acumulado de mínimo 60%.

COORDINACION DEL CURSO

Coordinación Académica	Coordinador UIT
Iris Pretel Trejo INICTEL-UNI ipretel@inictel-uni.edu.pe	Rodrigo Robles Oficina Regional de la UIT para las Américas rodrigo.robles@itu.int

REGISTRO Y PAGO

Creación de la cuenta en ITU Academy

El proceso de inscripción y el pago deben ser realizados en línea a través del Portal ITU Academy. Para registrarse en el curso es **NECESARIO**, primero, crear una cuenta en la plataforma en el siguiente enlace.

Inscripción en el curso

Una vez creada la cuenta nueva, ya se puede realizar la inscripción para el curso en línea en el siguiente enlace https://academy.itu.int/index.php/training-courses/full-catalogue/analisis-forense-digital

También es posible registrarse en el curso deseado por medio de nuestro catálogo de cursos.

Inscripción en el curso

1. **Pago en línea**
   Se aplica una tarifa de formación de **USD 150** por participante para este curso. El pago debe ser realizado a través del sistema en línea utilizando el enlace mencionado anteriormente para la

inscripción en: https://academy.itu.int/index.php/training-courses/full-catalogue/analisis-forense-digital

2. Transferencia bancaria internacional

Cuando no sea posible realizar el pago a través del sistema en línea, es posible seleccionar la opción de *offline payment* para generar una factura a través del miso enlace del curso. Descargue la factura para realizar una transferencia bancaria a la cuenta de la UIT que se indica a continuación, y remita el comprobante de la transferencia y la copia de la factura a hcbmail@itu.int, con copia para el Coordinador de Curso en UIT. **Todas las tarifas sobre transacciones bancarias deben ser sufragadas por el participante.**

En el caso de que los documentos referentes al pago no sean enviados, la inscripción en el curso no será confirmada.

3. Pago en grupo

Si desea pagar por más de un participante mediante transferencia bancaria y necesita una factura para todos ellos, cree una cuenta como **Contacto institucional**. Los contactos institucionales son usuarios que representan una organización. Cualquier estudiante puede solicitar ser un contacto institucional o pertenecer a cualquier organización existente.

Para hacer esto, diríjase a su página de perfil haciendo clic en el botón **"Mi cuenta"** en el menú del usuario. Al final de esta página debería ver dos botones:

a. Si desea **convertirse en un contacto institucional**, haga clic en el **botón "Solicitar ser un contacto institucional"**. Esto lo redirigirá a un pequeño formulario que le pedirá el nombre de la organización. Después de completar el nombre de la organización que desea representar, haga clic en **"continuar"** y se creará una solicitud. Un administrador de la Academia de la UIT revisará manualmente esta solicitud y la aceptará o denegará en consecuencia.

b. Si desea **pertenecer a una organización existente**, haga clic en el botón **"Solicitar pertenecer a un contacto institucional"**. Esto lo redireccionará a un pequeño formulario que le pedirá que seleccione la organización a la que desea unirse de una lista de organizaciones. Después de seleccionar la organización correcta, haga clic en **"continuar"**, se creará una solicitud. El contacto institucional que representa a esa organización aceptará o denegará manualmente su solicitud para unirse a la organización.

ITU BANK ACCOUNT DETAILS:	
Name and Address of Bank:	UBS Switzerland AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiary:	Union Internationale des Télécommunications
Account number:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Amount:	USD 150
Payment Reference:	CoE-AMS 26458 - P.40591.1.02

4. Otros métodos de pago

En caso de que las regulaciones nacionales restrinjan la posibilidad de completar el pago mediante las opciones informadas, le solicitamos contactar al Coordinador de la UIT para mayor asistencia.