



Título: Análisis Forense Digital en entornos Windows, iOS y Android

Fecha: Jueves, 30 de octubre – 9:30 a 20:00h

Formador: Juan Antonio Calles



Juan Antonio Calles es socio fundador de la compañía Zink Security S.L. Ingeniero en Informática de Sistemas, Postgrado en Tecnologías de la Información y Sistemas Informáticos y Postgrado en Ingeniería de Sistemas de Decisión, actualmente realizando un Doctorado en Informática sobre Seguridad de la Información. Certified Hacking Forensic Investigator (CHFI v8) por Ec-Council, CISA por la ISACA, ITIL v3 por EXIN, Dlink Certified y FTSAI. Es miembro de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE). Es ponente habitual en diversos foros y congresos de seguridad entre los que destacan No cON Name y RootedCon, las Jornadas Nacionales de Prevención y Seguridad en Internet, las Jornadas de Seguridad de la Información y Defensa, el IEE Region 8 SB & Gold Congress, o el Salón Internacional de Tecnologías de Seguridad y Defensa, y otros cursos y formaciones como el Curso de Perito Telemático Forense de la Universidad a Distancia de Madrid y el Curso de Perito Informático Forense de la Universitat Rovira i Virgili, así como otras publicaciones científicas para ACM. Completa su bagaje con la organización de las Jornadas X1RedMasSegura.

Descripción y objetivos:

La ciencia forense consiste en la aplicación de técnicas científicas y analíticas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

A lo largo del taller sobre Análisis Forense Digital podrás aprender los conceptos base que todo analista forense debe conocer antes de enfrentarse a un análisis pericial. Durante el taller se analizarán distintos entornos ante los que un perito podría encontrarse, poniendo foco en los dispositivos y sistemas operativos más extendidos entre la sociedad.



Contenidos:

- ¿Qué es el análisis forense digital?
- Escenarios forenses.
- Procedimientos para el análisis forense.

Evidencia digital (1 hora)

- La obtención de evidencias. Herramientas HW y SW.
- Metodología para la adquisición de evidencias.
- RFC 3227.
- Firmado de evidencias.
- La cadena de custodia.

Análisis de datos (1 hora)

- Tratamiento de evidencias.
- El principio de Locard.
- La línea temporal.

- Buscando información a través de aplicaciones forense.

Correo electrónico (30 minutos)

- Análisis forense de correo electrónico

Forense de aplicativos (1:30 horas)

- Forense en redes de datos.
- Forense de memoria RAM.
- Análisis de malware.

Forense de dispositivos móviles iOS y Android (3 horas)

- Introducción a la seguridad en dispositivos móviles
 - Arquitectura del sistema iOS
 - Seguridad en sistemas iOS
 - Arquitectura del sistema Android
 - Seguridad en sistemas Android
- Vulnerabilidades y exploits
- Reversing de aplicaciones móviles
- Análisis Forense



- Preservación de evidencias
- Obtención de información del dispositivo
- Obtención de datos de la tarjeta SD
- Volcado de memoria RAM
- Adquisición de imagen física de la memoria interna
- Live Forensics
- Adquisición de información de la tarjeta SIM
- Informe

Elaboración del informe pericial (30 minutos)

- Objetivo y elaboración del informe.
- Puntos clave.

Duración: 8h

Público objetivo: Administradores de Sistemas, Administradores de red, profesional de la seguridad informática, analistas forenses.

Conocimientos previos: Conocimientos básicos en Windows, iOS y Android.

Requisitos tecnológicos: PC portátil para tomar notas y realización de demos.

**Cualquier pregunta dirigirse directamente en el formulario de contacto de la web:
sección: FORMACIONES**

Precio: 200€ (impuestos incluidos). Incluye desayuno y bufet libre.

La inscripción y pago de todas las formaciones incluyen la entrada gratuita al Congreso No cON Name edición 2014. Todas las formaciones tienen un mínimo de 7 alumnos. En caso de no realizarse se devolvería el importe íntegro.

Para efectuar el pago los solicitantes deben hacer su inscripción a través de la web: <http://www.noconname.org/inscripcion/>