Tarea online AFI02.

Título de la tarea: Consideraciones entorno móvil.

Ciclo formativo y módulo: Curso de especialización en ciberseguridad en entornos de las tecnologías de la información - Análisis Forense Informático.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA2.** Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.

Contenidos

1.- Análisis forenses en dispositivos móviles.
- 1.1.- Elementos de un dispositivo móvil.
- 1.2.- Métodos de extracción.
- 1.3.- Herramientas.

1.- Descripción de la tarea.

Caso práctico

Pixabay (Dominio público)

María está trabajando en el laboratorio cuando recibe la tarea de analizar un dispositivo móvil.

Por una parte es un escenario nuevo para ella por lo que esta viendo de qué manera extraer la información. Sabe que es un teléfono móvil Iphone y por tanto es un sistema cerrado que sin los consiguientes accesos será complicado de analizar.

Necesita saber si la actividad del dueño del dispositivo durante las últimas semanas.

¿Qué te pedimos que hagas?

- **Apartado 1: Extracción de la evidencia**

Vamos a trabajar sobre la base de un móvil Iphone, para ello puedes usar tu teléfono o el de algún amigo. Si no tienes estas facilidades puedes disponer de una imagen de teléfono movil en el siguiente enlace: http://downloads.digitalcorpora.org/corpora/mobile/ios_13_4_1/ios_13_4_1.zip

El objetivo de la actividad es entender qué aparte de cómo se realiza una extracción y procesado, qué problemas nos podemos encontrar con el análisis forense de dispositivos móviles en especial de dispositivos basados en iOS.

Necesitas poder extraer la evidencia, para ello tienes dos alternativas:

- Realizar un backup mediante el software de Itunes de Apple.
  - Tienes una guía aquí: Guía Itunes de Apple .
- Extraer las evidencias mediante software forense específico.
  - Tienes el software disponible aquí https://www.magnetforensics.com/resources/magnet-acquire
  - Tienes una guía aquí Guía de software forense (está basado en Android pero el proceso para Iphone es el mismo)

- **Apartado 2: Procesado y Preguntas**
- Utilizaremos el siguiente software para procesar las evidencias:

- https://github.com/abrignoni/iLEAPP
- Tienes una guía del software aquí Guía software de procesado de evidencias
- Te recomendamos que hagas estas dos partes y luego intentes responder a las preguntas. Algunas de las preguntas puede requerir que investigues determinadas características del sistema iOS.

- ¿Qué sucede cuando conectamos el dispositivo móvil al ordenador?
- ¿Qué tipo de extracción es?
- ¿Qué riesgo tenemos? ¿Qué cambios se han producido al hacer este tipo de extracción?
- ¿Qué diferencias tenemos entre este tipo de extracción y una física?
- ¿Qué alternativas tenemos si no conocemos el código de desbloqueo pero tenemos o podemos conseguir el usuario y contraseña de la cuenta de apple?
- ¿Eres capaz de identificar el número de móvil?
- ¿Eres capaz de identificar que apps tienen concedidos permisos a qué recursos? ¿El usuario ha sido consciente de forma explícita de este consentimiento?

NOTA IMPORTANTE

Para todos los apartados es necesario entregar las capturas de pantalla de los principales pasos realizados, explicando el proceso seguido en cada uno de ellos. Las capturas de pantalla realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM
- Conexión a Internet para consultar ejemplos de la Unidad 1.
- Sistemas Operativos Windows 10, Ubuntu 18.04, Ubuntu 20.04
- Navegador web.

Recomendaciones

- Antes de abordar la tarea:
- Lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
- Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- Te recomendamos ver las guías que se han recomendado.
- Te recomendamos tambien investigar los problemas que hay en el forense de dispositivos basados en iOS.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_AFI02_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la segunda unidad del MP de AFI**, debería nombrar esta tarea como...

sanchez_manas_begona_AFI02_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA2

- a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.
- b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.
- c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.
- d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1.a: Se ha conseguido acceder y establecer un sistema de confianza con el ordenador donde se ha extraído la evidencia.	1 punto
Apartado 1.b: Se ha extraer una imagen del sistema o un backup.	1 punto
Apartado 2.a: ¿Qué sucede cuando conectamos el dispositivo móvil al ordenador?	1 punto
Apartado 2.b: ¿Qué tipo de extracción es?	1 punto
Apartado 2.c: ¿Qué riesgo tenemos? ¿Qué cambios se han producido al hacer este tipo de extracción?	1,5 puntos
Apartado 2.d: ¿Qué diferencias tenemos entre este tipo de extracción y el resto?	1 punto
Apartado 2.e:¿Qué alternativas tenemos si no conocemos el código de desbloqueo pero tenemos o podemos conseguir el usuario y contraseña de la cuenta de apple?	2 puntos
Apartado 2.f: ¿Eres capaz de identificar el número de móvil?	0,5 puntos
Apartado 2.g: ¿Eres capaz de identificar que apps tienen concedidos permisos a qué recursos? ¿El usuario ha sido consciente de forma explícita de este consentimiento?	1 punto

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.