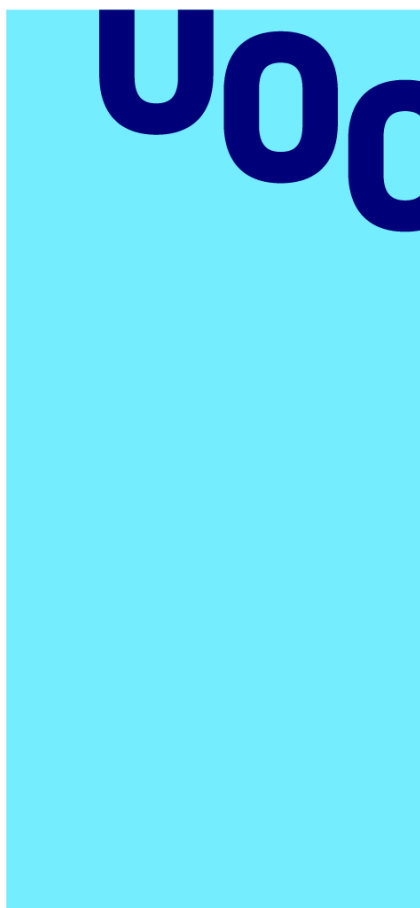


Análisis forense de un ordenador personal



Universitat Oberta
de Catalunya

Alumno:

José Enrique Rodríguez González

Master Universitario de Ciberseguridad y privacidad.

M1.881 - TFM - Análisis forense

Tutora de TFM:

Dña. Elena Botana de Castro

Profesor responsable de la asignatura:

D. Jordi Serra Ruiz

Fecha de Entrega:

Enero de 2024

Agradecimientos

A mi esposa e hija, acompañantes en todo momento de esta aventura académica.

A mis compañeros de trabajo, Juanma, Luisma y Borja, que saben de que estos tres años que llevo realizando este master y han conocido todos los derroteros que me ha llevado este camino.

Índice general

Agradecimientos	I
1. Plan de trabajo	1
1.1. Problema a resolver.	1
1.2. Objetivos.	1
1.3. Descripción del entorno de trabajo.	1
1.4. Listado de tareas.	1
1.5. Planificación temporal de las tareas.	1
1.6. Revisión del estado del arte de la informática forense.	1
2. Extremos del análisis y previsión de pruebas técnicas.	2
2.1. Propuesta de extremos.	2
2.2. Previsión de pruebas técnicas.	2
3. Análisis de la memoria RAM.	3
3.1. Acciones previas al análisis de la memoria RAM.	3
3.2. Datos de interés de la captura de la memoria RAM.	3
3.3. Sistema Operativo de la memoria RAM analizada.	3
3.4. Búsqueda de procesos en funcionamiento de interés para el análisis.	3
3.5. Análisis y extracción de procesos sospechosos.	3
3.6. Listado de conexiones de red y conexiones sospechosas.	3
4. Análisis del disco duro.	4
4.1. Acciones previas al análisis del disco duro.	4
4.2. Datos de interés del disco duro.	4
4.3. Usuarios del sistema.	4
4.4. Análisis de evidencias del disco duro.	4
5. Resumen ejecutivo	5
6. Informe pericial	6
7. Conclusiones	7
8. Referencias bibliográficas	8
9. Anexos	9

Capítulo 1

Plan de trabajo

esto es parte del texto del plan de trabajo

- 1.1. Problema a resolver.
- 1.2. Objetivos.
- 1.3. Descripción del entorno de trabajo.
- 1.4. Listado de tareas.
- 1.5. Planificación temporal de las tareas.
- 1.6. Revisión del estado del arte de la informática forense.

Capítulo 2

Extremos del análisis y previsión de pruebas técnicas.

2.1. Propuesta de extremos.

2.2. Previsión de pruebas técnicas.

Capítulo 3

Análisis de la memoria RAM.

- 3.1. Acciones previas al análisis de la memoria RAM.
- 3.2. Datos de interés de la captura de la memoria RAM.
- 3.3. Sistema Operativo de la memoria RAM analizada.
- 3.4. Búsqueda de procesos en funcionamiento de interés para el análisis.
- 3.5. Análisis y extracción de procesos sospechosos.
- 3.6. Listado de conexiones de red y conexiones sospechosas.

Capítulo 4

Análisis del disco duro.

- 4.1. Acciones previas al análisis del disco duro.
- 4.2. Datos de interés del disco duro.
- 4.3. Usuarios del sistema.
- 4.4. Análisis de evidencias del disco duro.

Capítulo 5

Resumen ejecutivo

Capítulo 6

Informe pericial

Capítulo 7

Conclusiones

Capítulo 8

Referencias bibliográficas

Capítulo 9

Anexos