**Análisis Forense**

# Adquisición de Metodologías de Análisis Forenses

### 

### 

| Objetivo general |
| --- |
| Aprender a realizar capturas de red con diferentes herramientas |
| Resumen de la actividad |
| Aprender a realizar capturas de red tanto con herramientas gráficas como por comandos y  comprobar el resultado |
| Duración prevista |
| 2 horas lectivas. |
| Índice |
| **Portada**1  [Objetivo general](#_4sjnzbnyj3c4) 2  [Resumen de la actividad](#_da5lf25oe9y4) 2  [Duración prevista](#_2l6c9upgfsdg) 2  [Índice](#_z3ju52uh27qp) 2  [Descripción de la Actividad](#_vyo9aggwofcy) 2  [Captura de con Wireshark](#_1u45f4wopl78) 2  [Captura de datos con TCPDump](#_i9odk34g9jfh) 4  [Captura de datos con NetworkMiner](#_xhp0jmmzl6le) 5 |
| Descripción de la Actividad |
| Captura de con Wireshark |
| a) Instalación (ubuntu)  **Sudo apt-get install Wireshark** |
| **Http** |
|  |
|  |
| **Https** |
|  |
| Captura de datos con TCPDump |
| 1. En Kali Linux 6.3.0 viene preinstalado |
| 1. Iniciar captura con la siguiente sintaxis |
| tcp dump -i [inteface] -w [file] |
| 1. Navegar por alguna página web 2. Ctrl+C para detener la captura 3. Abrir el fichero con la captura utilizando Wireshark |
|  |
| Captura de datos con NetworkMiner |
| 1. Descargar NetworkMiner (se trata de un programa portable)    1. https://www.netresec.com/?page=NetworkMiner 2. Abrir el programa como administrador |
|  |
| 1. Seleccionar el interfaz por el que realizar la captura |
|  |
| 4. Iniciar la captura |
|  |
| 5. Navegar por alguna web  6. La información se muestra agrupada por pestañas. |
|  |
| 7. Las capturas se almacenan dentro la carpeta **captures** |
|  |
| 8. Abrir la captura con Wireshark y comprobar que también se puede analizar. |
|  |
|  |

Bibliografia

* <https://contenthub.netacad.com/courses/itn-dl/_common/3.7.9-lab---install-wireshark_es-XL.pdf>