

Asignatura: **Fundamentos de**

**Ingeniería Telemática**

**Plantilla de Práctica 5 (Sesiones 10 y 11):**

Configuración de Aplicaciones de Red.

Miembro 1 de Grupo

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre1:** | *Escribir aquí el nombre* | **Apellidos1:** | *Escribir aquí los apellidos* |
| **Usuario1:** | *Escribir aquí el usuario ILIAS* | | |

Miembro 2 de Grupo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nombre2:** | *Escribir aquí el nombre* | **Apellidos2:** | *Escribir aquí los apellidos* | |
| **Usuario2:** | *Escribir aquí el usuario ILIAS* | | |

**Instrucciones**

Leer el guion de prácticas y una vez acabadas las dos sesiones de laboratorio correspondientes a la práctica 5 debéis entregar esta plantilla rellena con tus datos y los de tu compañero (sólo debe entregarlo uno de los dos, aunque antes debéis configuraros como equipo).

La entrega se hará mediante el botón "Enviar archivos" de esta tarea (al igual que la configuración de equipo).

En esta plantilla debéis realizar todo lo que se indica rellenándolo en los espacios correspondientes.

***Sesión 10***

1.- Adjunta una captura de pantalla de una trama donde se vean las direcciones IP y MAC origen y destino, así como los puertos origen y destino.

|  |
| --- |
| DIR MAC Origen: no se muestra DIR MAC Dtno: no se muestra  DIR IP Origen: 192.168.15.123 DIR IP Dtno: 192.168.15.123  Puerto Origen: 110 Puerto Dtno: 61597 |

Razona cuál es el equipo servidor y cuál el cliente. ¿Por qué el puerto del cliente es mayor de 1024? Según el puerto usado por el servidor, ¿de qué servicio se trata?

|  |
| --- |
| El cliente y el servidor son el mismo equipo. El puerto del cliente es mayor que 1024 porque se trata de un puerto registrado, usado por el Wireshark. Se trata de un servicio de intercambio de e-mail POP3. |

2.- Adjunta una captura de pantalla de una trama **con la cabecera SMTP** expandida. Identifica el comando capturado del protocolo SMTP.

|  |
| --- |
|  |

3.- Adjunta la captura de pantalla de **tráfico POP3** con la opción “Seguir Flujo TCP” (en formato volcado Hex).

|  |
| --- |
|  |

4. Adjunta la captura de pantalla de tráfico POP3 con la opción **“Gráfica de Flujo -> All flows**”

|  |
| --- |
|  |

5. Adjunta la captura de pantalla de tráfico POP3 con la **opción “Gráfica de Flujos -> TCP Flows”**

|  |
| --- |
|  |

6. Analiza y comenta la diferencia entre las dos modalidades anteriores. Observa como en la modalidad “TCP Flows” los Ack se usan para indicar al otro extremo el próximo byte (Seq) que se espera recibir. **Analiza y comenta un ejemplo de esto último.**

|  |
| --- |
|  |

7. En el gráfico generado por “TCP Flows”, aísla el intercambio de las primeras PDUs donde se establece la conexión TCP (**three-way handshaking**) y pégalas a continuación:

|  |
| --- |
|  |

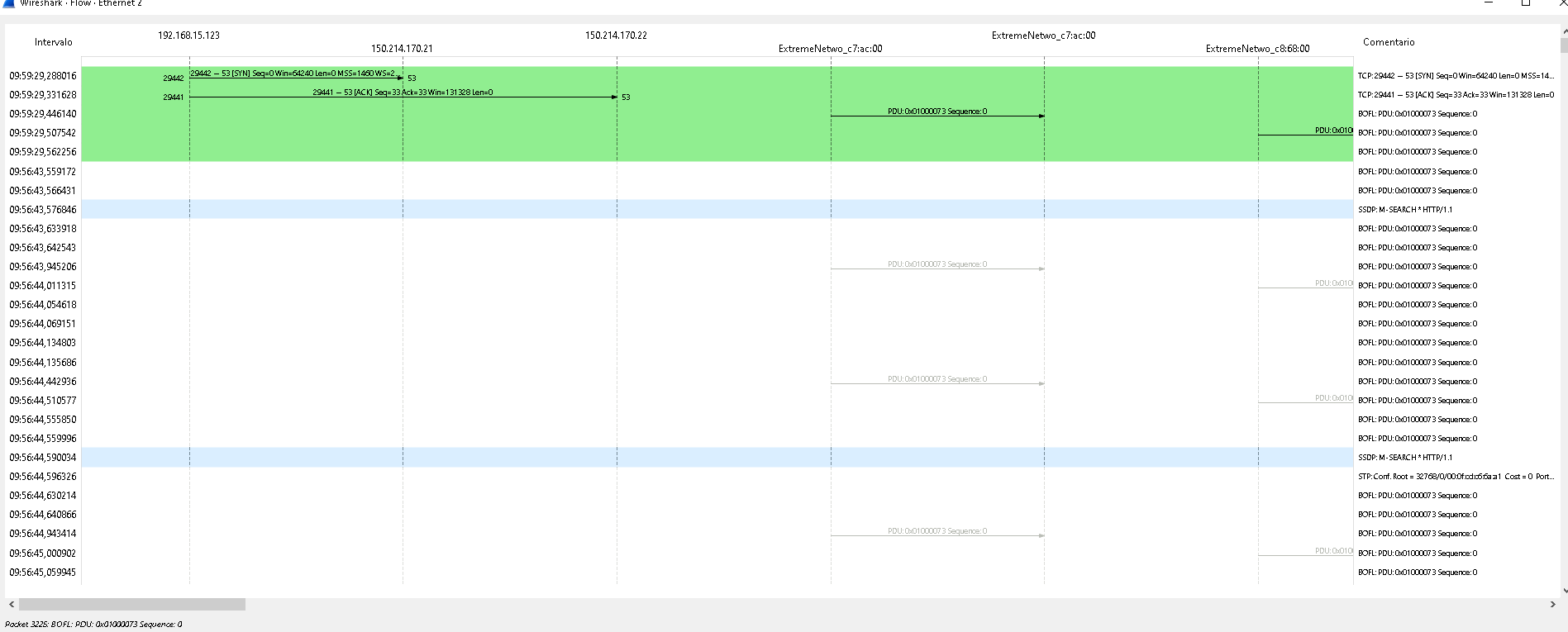
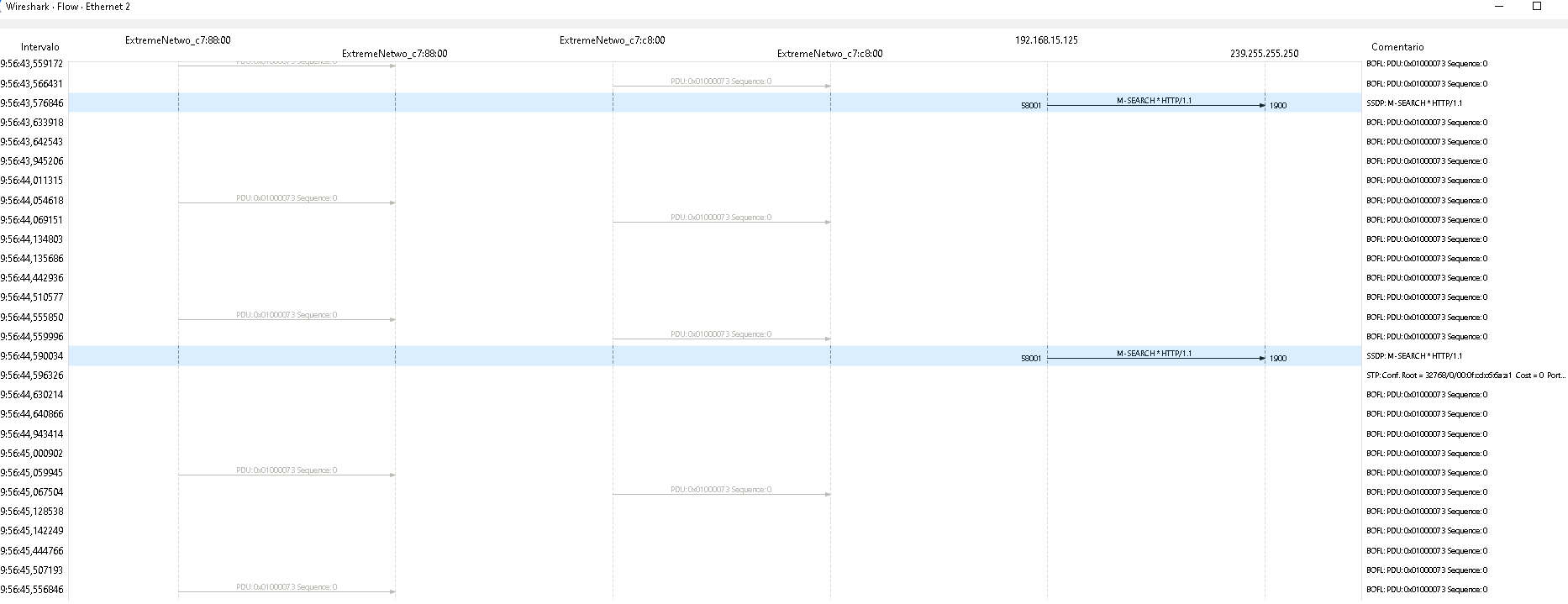
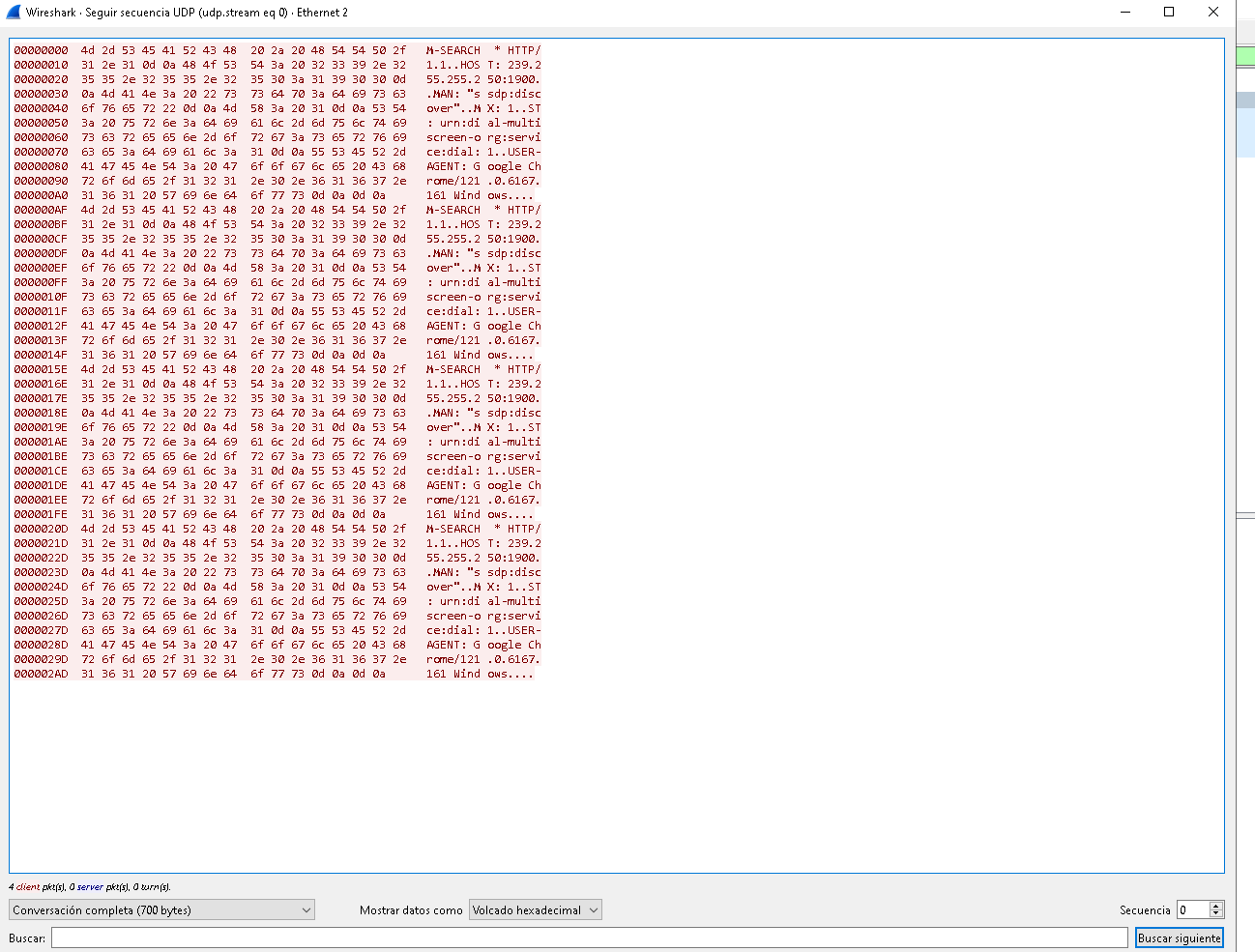
8. Adjunta la captura de pantalla de tráfico SMTP con la opción “Seguir Flujo TCP” (en formato Hex).

|  |
| --- |
|  |

9. Adjunta la captura de pantalla correspondiente a la trama de respuesta del DNS donde se vean los campos **“Queries” y “Answers” del protocolo DNS**. Según la captura de la trama, ¿qué protocolo de transporte se usa y cuáles son los puertos usados (del servidor y del cliente)?

|  |
| --- |
|  |

10. Tras introducir como filtro de captura de solo UDP, incorpore alguna captura donde se muestre el resultado de Gráfica de Flujo “All Flows” y compárelo con el obtenido sin el filtro de captura.



***Sesión 11***

11. Adjunta la captura de pantalla correspondiente donde se vean solamente las tramas de POP3 con las claves de correo electrónico.

|  |
| --- |
|  |

12. Especifique un posible filtro de visualización que permita:

a) Visualizar solo paquetes del protocolo SMTP

|  |
| --- |
|  |

b) Visualizar solo paquetes con dirección IP destino 192.168.15.247 y de tipo UDP:

|  |
| --- |
|  |

c) Visualizar paquetes TCP dirigidos al puerto 80:

|  |
| --- |
|  |

d) Visualizar paquetes con un tamaño de trama de más de 100 bytes:

|  |
| --- |
|  |

13. Responda cómo capturaría tráfico que vaya siempre dirigido a la misma máquina.

|  |
| --- |
| Se puede añadir un filtro de captura donde el Host se especifica una Ip, así solo muestreará tráficos que vaya siempre a la misma maquina |

14. Adjunta la captura de pantalla correspondiente a tráfico capturado en una red inalámbrica, en el que se vea la diferencia entre conectar a <https://www.ujaen.es> y a http://www.labtelema.ujaen.es

|  |
| --- |
|  |

15. Describa qué es una RFC y diga cuál de ellas describe al protocolo SMTP. Dibuje un intercambio de primitivas de este protocolo indicando los comandos usados y especificados en la RFC.

|  |
| --- |
|  |