

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#5 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 1/Diciembre/2020

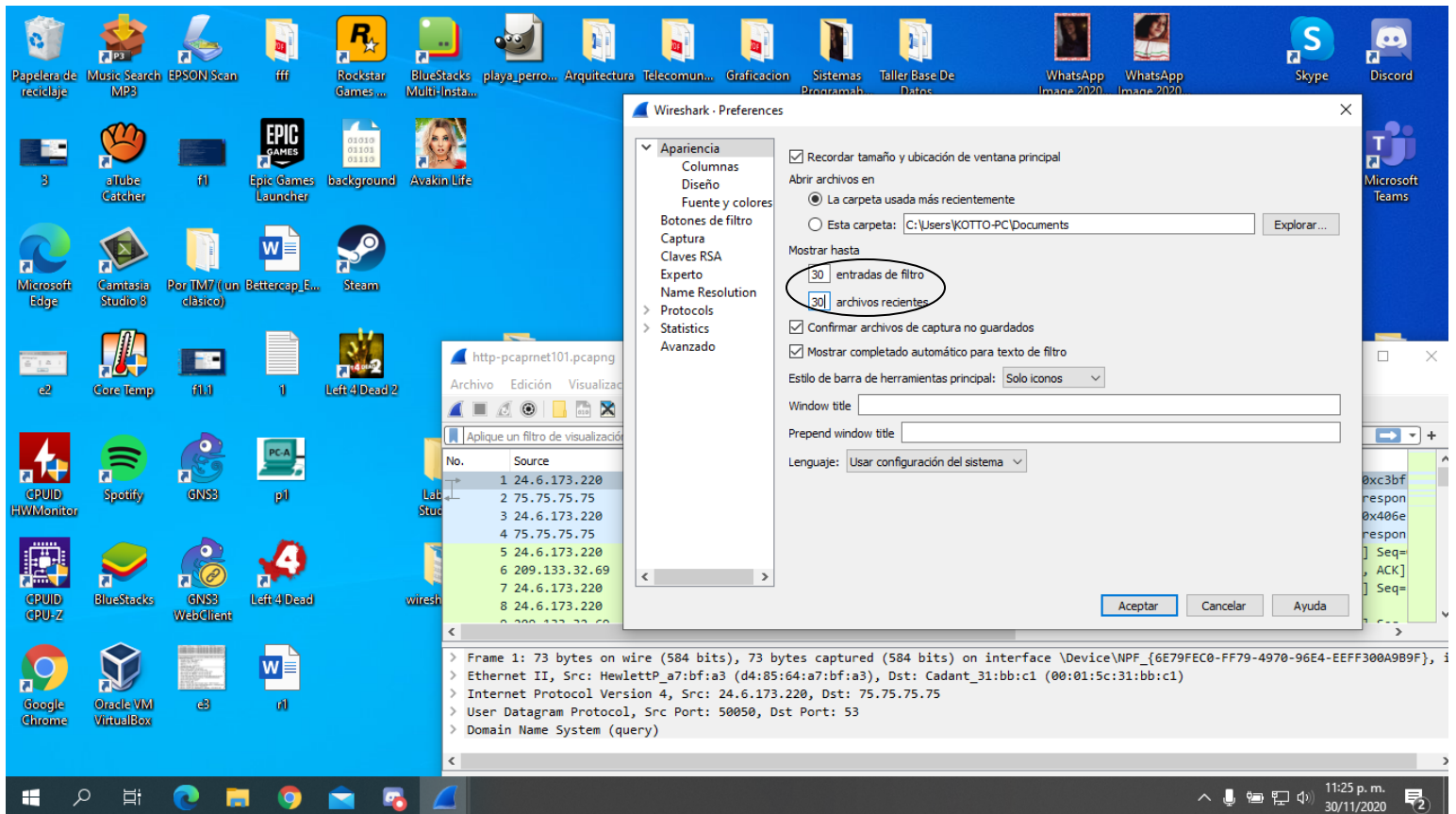
Horario: 5:00 pm – 6:00 pm

Laboratio N#5 – Establecer preferencias de Wireshark (Important Lab)

Primero debemos de abrir el archivo http-pccapnet101.pcapg

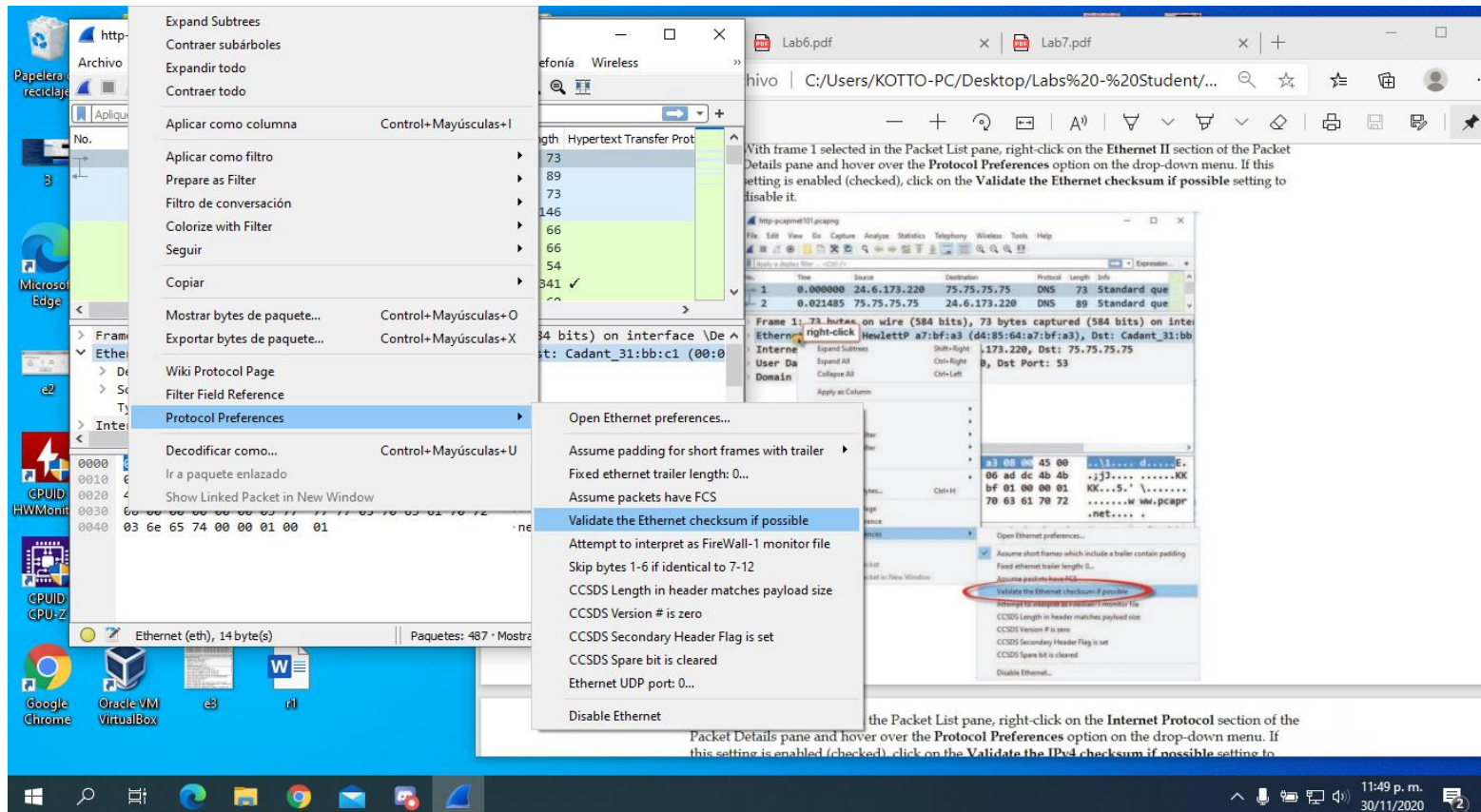
Le damos a la opcion de editar | preferencias en el menu.

Cambiamos las entradas de los filtros que se muestran a continuacion a 30.



Le damos clic en aceptar. Esto se guardara automaticamente en la configuracion.

Ahora pasamos al paso siguiente en el cual debemos de deshabilitar la validacion de Ethernet. Seleccionamos el frame 1 en la lista de paquetes y hacemos clic derecho y luego a Protocol Preferences y lo tenemos que desactivar com se muestra en la captura.



Ya con el frame 1 seleccionado le damos clic a protocolo de internet del panel de detalles de los paquetes y hacemos el mismo proceso que en anterior solo que ahora debemos de comprobar la validacion de la suma de comprobacion de ipv4 y desactivarlo.

The screenshot shows the Wireshark interface with the 'Protocol Preferences' menu open for the Internet Protocol Version 4 (IPv4) protocol. The menu is located in the 'Packet Details' pane, under the 'Protocol' section. The 'Validate the IPv4 checksum if possible' option is highlighted. The background shows the Wireshark packet list and packet details pane.

Step 8: Select frame 5 in the Packet List pane. Right-click the Transmission Control Protocol section of the Packet Details pane and, under Protocol Preferences, disable the Validate the TCP checksum if possible setting if it is currently enabled.

Step 9: Since Wireshark closes the TCP protocol settings menu after you select an option, you must right-click the Transmission Control Protocol section of the Packet Details pane and, under Protocol Preferences, disable the Validate the TCP checksum if possible setting if it is currently enabled.

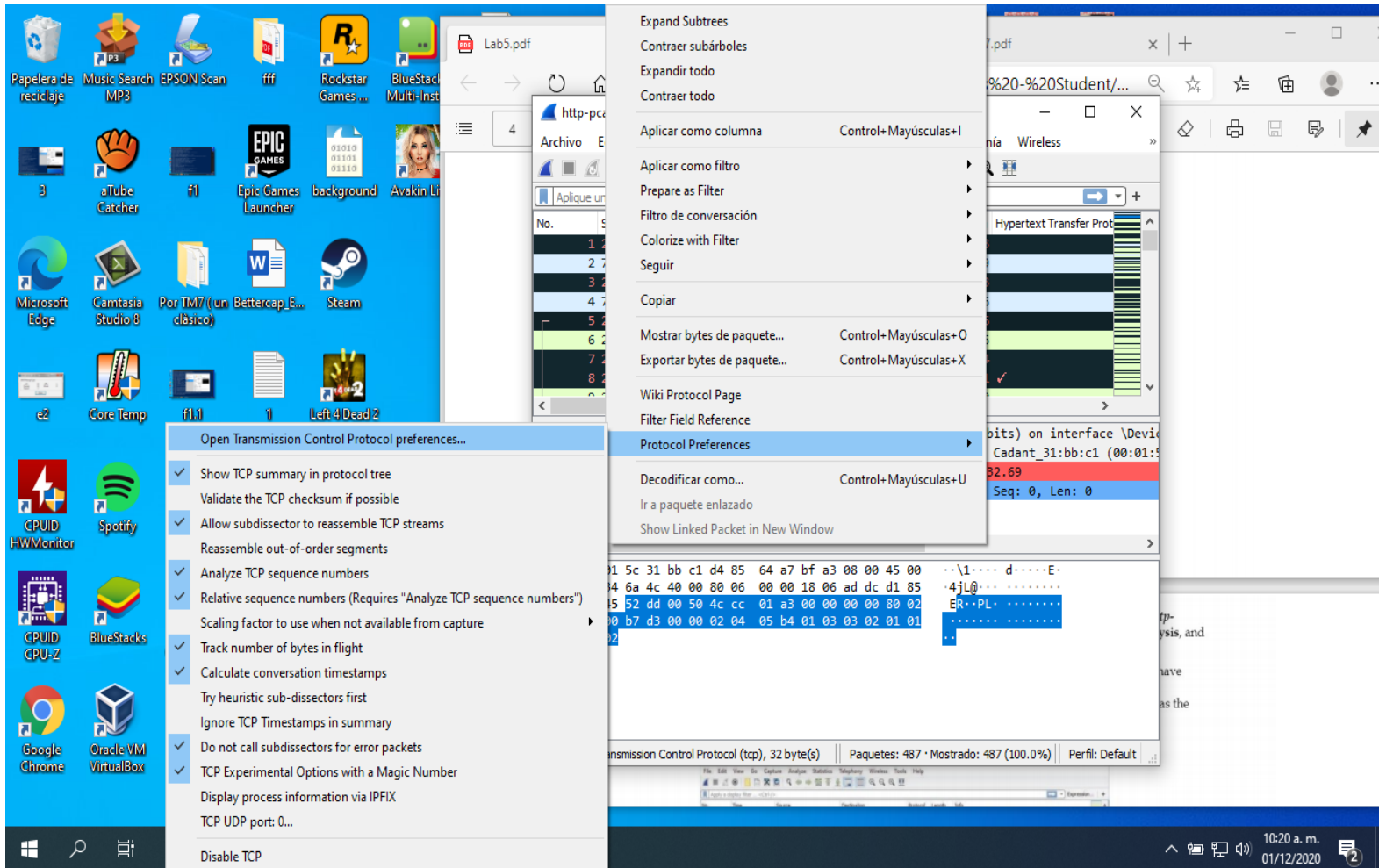
En esta ocasión vamos a seleccionar el frame 5 en el panel de la lista de paquetes y con clic derecho en las preferencias de protocolo debemos de deshabilitar la validacion de la suma de comprobacion TCP.

Debemos de volverle a dar clic derecho y abrir de nuevo las preferencias del protocolo para revisar las siguientes configuraciones esten de esta manera.

Disabled: Allow subdissector to resamble tcp streams.

Enabled: Track number of bytes in flight.

Enabled: Calculate conversation timestamps.



Ahora debemos de comprobar que wireshark no esta validando la suma de comprobacion TCP y los bytes de datos que esta enviando como muestra la captura de pantalla.

The screenshot shows a Windows desktop with various icons on the taskbar and desktop. A Wireshark window is open, displaying a packet capture of an HTTP GET request. The packet list shows the following details:

No.	Source	Destination	Protocol	Length	Info
1	24.6.173.220	75.75.75.75	DNS	73	Standard
2	75.75.75.75	24.6.173.220	DNS	89	Standard
3	24.6.173.220	75.75.75.75	DNS	73	Standard
4	75.75.75.75	24.6.173.220	DNS	146	Standard
5	24.6.173.220	209.133.32.69	TCP	66	21213 → 21213
6	209.133.32.69	24.6.173.220	TCP	66	80 → 21213
7	24.6.173.220	209.133.32.69	TCP	54	21213 → 80
8	24.6.173.220	209.133.32.69	HTTP	341	GET / HTTP
9	209.133.32.69	24.6.173.220	TCP	60	80 → 21213

The packet details pane shows the following information:

- Checksum: 0xb8e6 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (287 bytes)

The raw data pane shows the following hex and ASCII representation:

```
0020 20 45 52 dd 00 50 4c cc 01 a4 04 ea 62 2d 50 18 ER...P...b-P-
0030 40 29 b8 e6 00 00 47 45 54 20 2f 20 48 54 54 50 @)...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 72 2e /1.1..Ho st: www.
0050 70 63 61 70 72 2e 6e 65 74 0d 0a 55 73 65 72 2d pcapr.ne t..User-
0060 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5
0070 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 .0 (Wind ows NT 6
0080 2e 31 3b 20 57 4f 57 36 34 3b 20 72 76 3a 31 36 .1; WOW6 4; rv:16
0090 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 .0) Gecko o/201001
00a0 30 31 20 46 69 72 65 66 6f 78 2f 31 36 2e 30 0d 01 Firef ox/16.0
00b0 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 .Accept: text/ht
00c0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x
```

The status bar at the bottom of the Wireshark window shows: Transmission Control Protocol (tcp), 20 byte(s) | Paquetes: 487 · Mostrado: 487 (100.0%) | Perfil: Default