



“Secretaría De La Educación Superior”  
“Instituto Tecnológico de Cancún”

## **Ingeniería en Sistemas Computacionales**

**Materia:** Fundamentos de Telecomunicaciones

**Tema:** Laboratorio N#28 Wireshark

**Alumno:** Vargas Rodríguez Javier Jesús

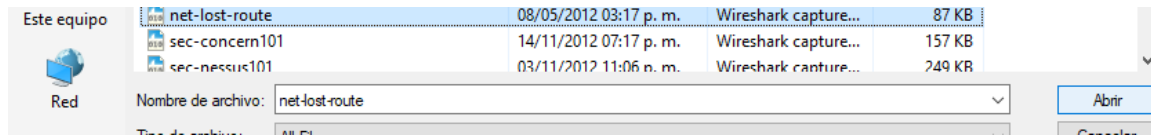
**Maestro:** Ismael Jiménez Sánchez

***Fecha De Entrega: 5/Diciembre/2020***

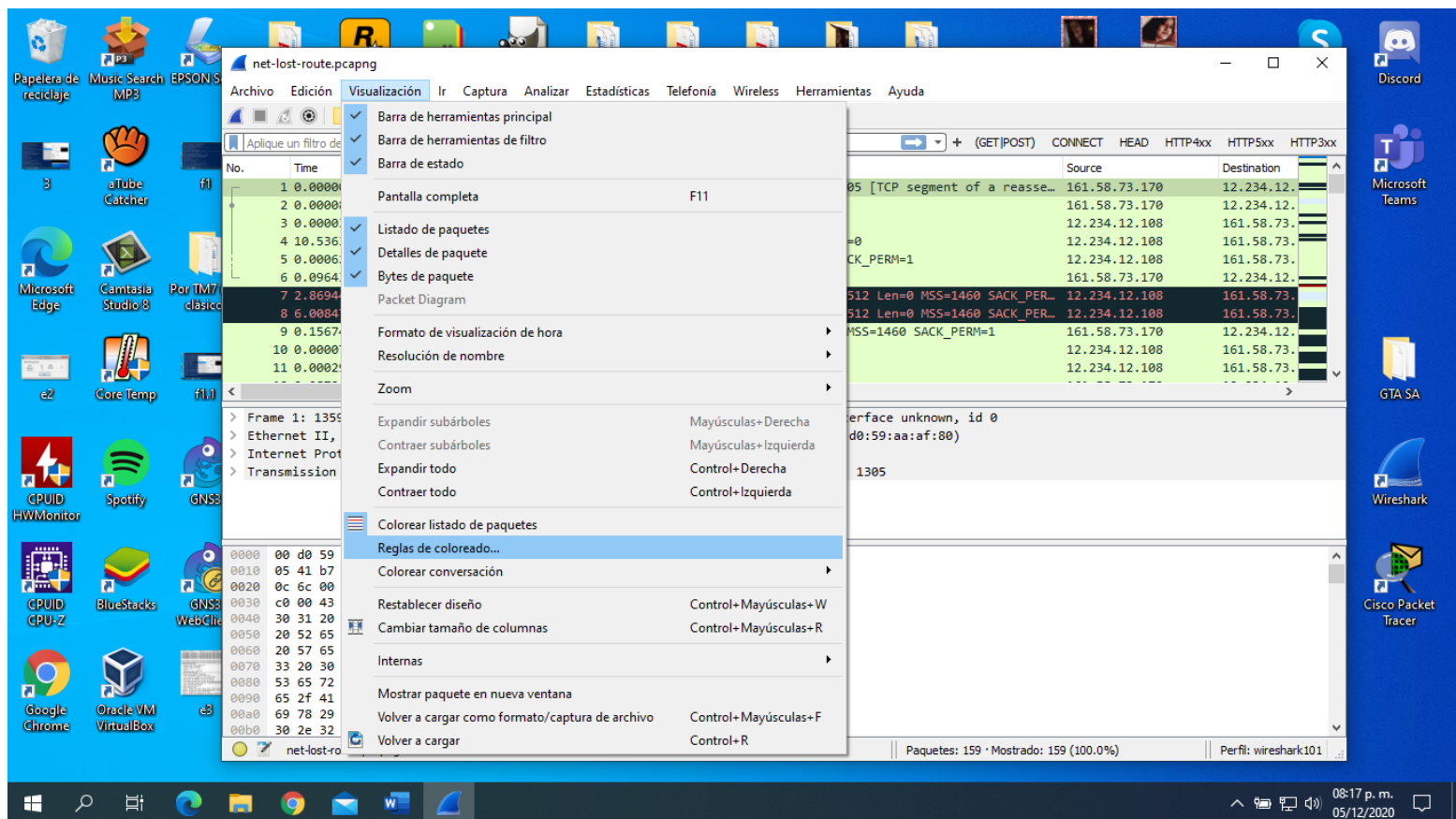
Horario: 5:00 pm – 6:00 pm

## ***Laboratio N#28 – Utilize la barra de desplazamiento inteligente para encontrar los problemas rapidamente.***

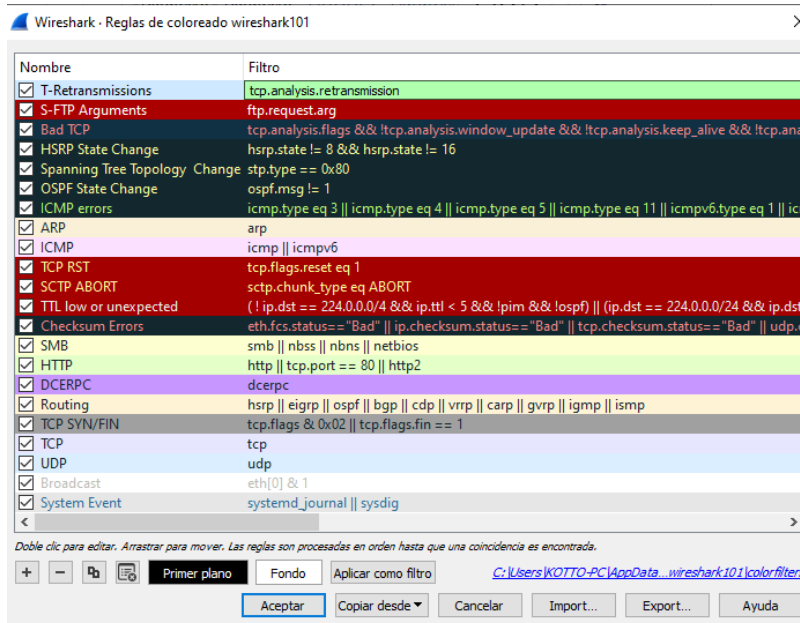
Paso 1 – Abrimos el archivo nes-lost-route.pcapng.



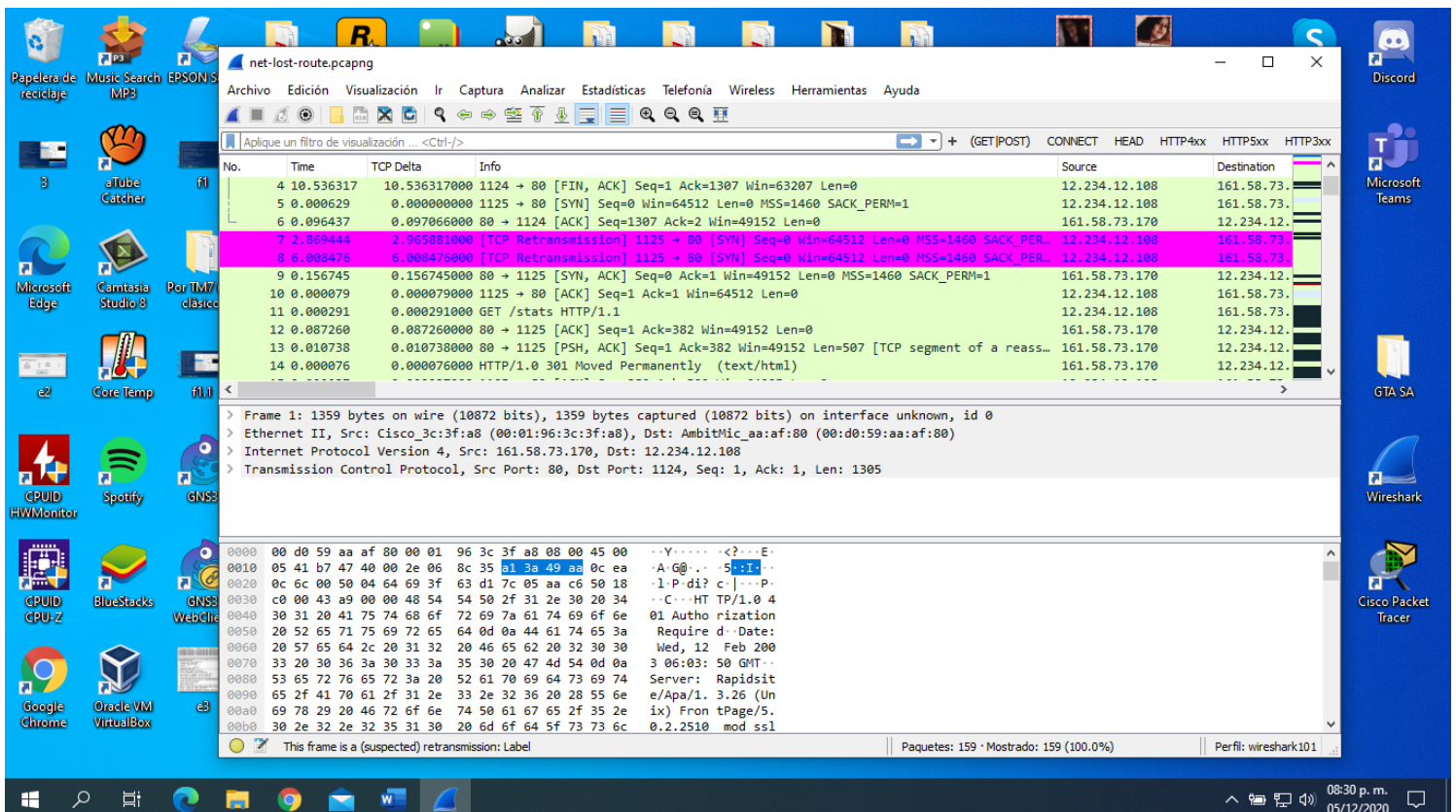
Paso 2 – Ahora vamos a crear una nueva regla de color para diferenciar las retransmisiones del resto de tráfico. Seleccionamos Ver | Reglas para colorear para abrir la ventana de reglas.



Paso 3 – Hacemos clic en el botón agregar. Nombramos la nueva regla de coloración T-Retransmissions. En el filtro debemos de poner tcp.analysis.retransmission.



Paso 4 – Con la nueva regla de coloración Seleccionada, hacemos clic en el fondo y seleccionamos un color vibrante. Hacemos clic en aceptar para seleccionar el color para cerrar las reglas de coloración.



## Paso 5 – Seleccionamos Vista | Reglas para colorear y deshabilitar todas sus reglas de coloración personalizada en este punto.

The screenshot displays the Wireshark application window. The main window shows a packet capture list on the left, a details pane in the middle, and a packet bytes pane at the bottom. A dialog box titled 'Wireshark - Reglas de coloreado wireshark101' is open in the foreground. The dialog has two columns: 'Nombre' (Name) and 'Filtro' (Filter). The 'Nombre' column is circled. The 'Filtro' column contains various network protocol filters. The dialog also includes a search bar, a list of rules, and buttons for 'Aceptar', 'Copiar desde', 'Cancelar', 'Import...', 'Export...', and 'Ayuda'.

No.	Time	TCP Delta	Info
4	10.536317	10.536317000	1124 → 80 [FIN, ...]
5	0.000629	0.000000000	1125 → 80 [SYN, ...]
6	0.096437	0.097066000	80 → 1124 [ACK, ...]
7	2.869444	2.965881000	[TCP Retransmission]
8	6.008476	6.008476000	[TCP Retransmission]
9	0.156745	0.156745000	80 → 1125 [SYN, ...]
10	0.000079	0.000079000	1125 → 80 [ACK, ...]
11	0.000291	0.000291000	GET /stats HTTP/1.1
12	0.087260	0.087260000	80 → 1125 [ACK, ...]
13	0.010738	0.010738000	80 → 1125 [PSH, ...]
14	0.000076	0.000076000	HTTP/1.0 301 Moved

Nombre	Filtro
<input type="checkbox"/> T-Retransmissions	tcp.analysis.retransmission
<input checked="" type="checkbox"/> S-FTP Arguments	ftp.request.arg
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis...
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3    icmp.type eq 4    icmp.type eq 5    icmp.type eq 11    icmpv6.type eq 1    icr...
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp    icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !ipm && !ospf )    ( ip.dst == 224.0.0.0/24 && ip.dst...
<input checked="" type="checkbox"/> Checksum Errors	eth.fcs.status == "Bad"    ip.checksum.status == "Bad"    tcp.checksum.status == "Bad"    udp.c...
<input checked="" type="checkbox"/> SMB	smb    nbss    nbns    netbios
<input checked="" type="checkbox"/> HTTP	http    tcp.port == 80    http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp    eigrp    ospf    bgp    cdp    vrrp    carp    gvrp    igmp    ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02    tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal    sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

<C:\Users\KOTTO-PC\AppData\Roaming\Wireshark\profiles\wireshark101\colorfilters>

Acceptar Copiar desde Cancelar Import... Export... Ayuda

This frame is a (suspected) retransmission: Label Paquetes: 159 - Mostrado: 159 (100.0%) Perfil: wireshark101