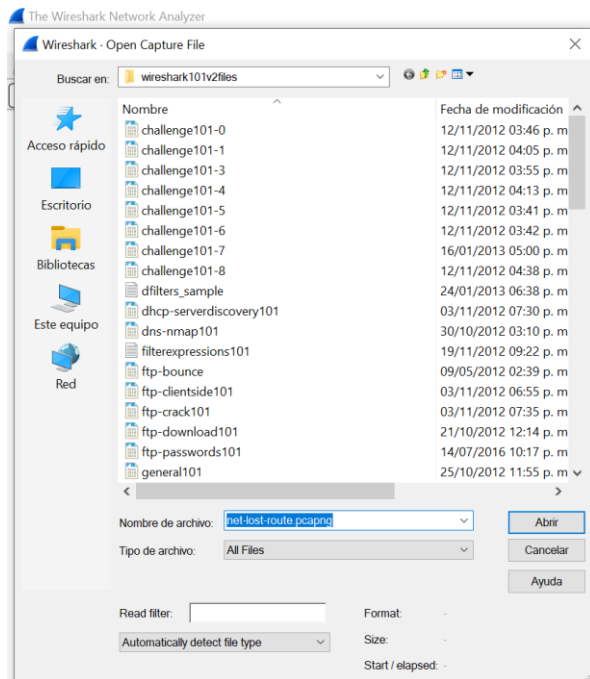
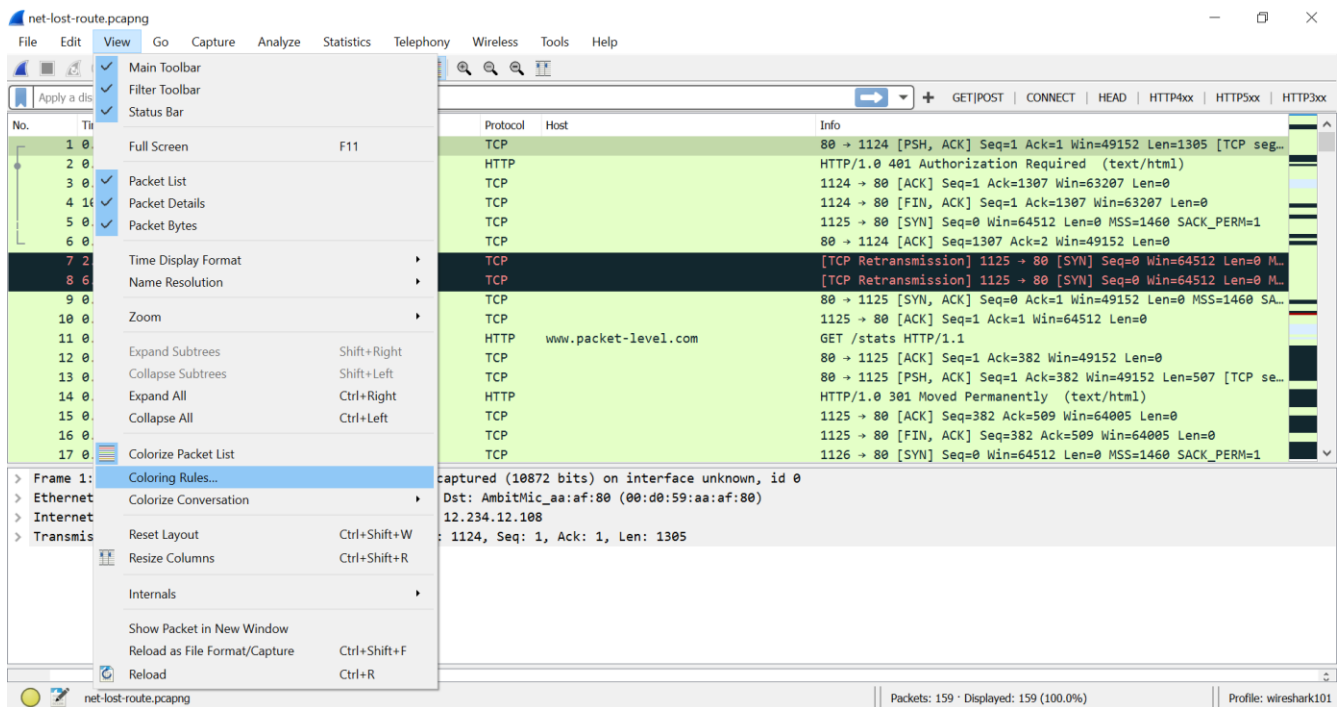


Lab 28

Abriremos el siguiente archivo



En la pestaña de view y coloring rules



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is titled 'Wireshark - Coloring Rules wireshark101'. It features a table with two columns: 'Name' and 'Filter'. The table lists various network events and their corresponding filters, such as 'T-Retransmissions' with filter 'tcp.analysis.retransmission' and 'S-FTP Arguments' with filter 'ftp.request.arg'. The main packet list on the left shows a sequence of packets from 1 to 17, with packet 7 highlighted in pink. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

Name	Filter
<input checked="" 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
<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 icmp.v6.type eq 1 icmp.v6.type eq 2 icmp.v6.type eq 3
<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 == 224.0.0.4 && ip.ttl < 5 && ip.m && !ospf) (ip.dst == 224.0.0.251 && ip.ttl < 5 && !ospf)
<input checked="" type="checkbox"/> Checksum Errors	eth.fc.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad" udp.checksum.status == "Bad"
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCE/RPC	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.dst == ff:ff:ff:ff:ff:ff

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

Buttons: +, -, Copy, Paste, Foreground, Background, Apply as filter, OK, Copy from, Cancel, Import..., Export..., Help

URL: C:\Users\jgael\AppData\Roaming\Wireshark\profiles\wireshark101\colorfilters

Packet list (left):

No.	Time	Source
1	0.000000	161.58.73.170
2	0.000083	161.58.73.170
3	0.00038	12.234.12.108
4	10.536317	12.234.12.108
5	0.000629	12.234.12.108
6	0.096437	161.58.73.170
7	2.869444	12.234.12.108
8	6.008476	12.234.12.108
9	0.156745	161.58.73.170
10	0.000079	12.234.12.108
11	0.000291	12.234.12.108
12	0.087260	161.58.73.170
13	0.010738	161.58.73.170
14	0.000076	161.58.73.170
15	0.000037	12.234.12.108
16	0.000253	12.234.12.108
17	0.158637	12.234.12.108

Packet details (right):

- Frame 1: 1359 bytes on wire (10872 bit)
- Ethernet II, Src: Cisco_3c:3f:a8 (00:0c:29:3c:3f:a8), Dst: 12.234.12.108 (02:00:14:00:00:00)
- Internet Protocol Version 4, Src: 161.58.73.170, Dst: 12.234.12.108
- Transmission Control Protocol, Src Port: 80, Dst Port: 80

net-lost-route.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

GET|POST | CONNECT | HEAD | HTTP4xx | HTTP5xx | HTTP3xx

No.	Time	Source	Destination	Protocol	Host	Info
15	0.000037	12.234.12.108	161.58.73.170	TCP		1125 → 80 [ACK] Seq=382 Ack=509 Win=64005 Len=0
16	0.000253	12.234.12.108	161.58.73.170	TCP		1125 → 80 [FIN, ACK] Seq=382 Ack=509 Win=64005 Len=0
17	0.158637	12.234.12.108	161.58.73.170	TCP		1126 → 80 [SYN] Seq=0 Win=64512 Len=0 MSS=1460 SACK_PERM=1
18	0.081801	161.58.73.170	12.234.12.108	TCP		80 → 1126 [SYN, ACK] Seq=0 Ack=1 Win=49152 Len=0 MSS=1460 SA...
19	0.000051	12.234.12.108	161.58.73.170	TCP		1126 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0
20	0.000436	12.234.12.108	161.58.73.170	HTTP	www.packet-level.com	GET /stats/ HTTP/1.1
21	0.158091	161.58.73.170	12.234.12.108	TCP		[TCP Spurious Retransmission] 80 → 1125 [FIN, PSH, ACK] Seq=...
22	0.000080	12.234.12.108	161.58.73.170	TCP		[TCP Dup ACK 15#1] 1125 → 80 [ACK] Seq=383 Ack=509 Win=64005...
23	1.949341	12.234.12.108	161.58.73.170	TCP		[TCP Retransmission] 1125 → 80 [FIN, ACK] Seq=382 Ack=509 Wi...
24	0.079541	161.58.73.170	12.234.12.108	TCP		80 → 1125 [ACK] Seq=509 Ack=383 Win=49152 Len=0
25	0.721616	12.234.12.108	161.58.73.170	TCP		[TCP Retransmission] 1126 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64...
26	0.079445	161.58.73.170	12.234.12.108	TCP		80 → 1126 [ACK] Seq=1 Ack=383 Win=49152 Len=0
27	8.995030	161.58.73.170	12.234.12.108	TCP		80 → 1126 [PSH, ACK] Seq=1 Ack=383 Win=49152 Len=188 [TCP se...
28	0.138774	12.234.12.108	161.58.73.170	TCP		1126 → 80 [ACK] Seq=383 Ack=189 Win=64324 Len=0
29	0.308542	161.58.73.170	12.234.12.108	TCP		80 → 1126 [ACK] Seq=189 Ack=383 Win=49152 Len=1460 [TCP segm...
30	0.001233	161.58.73.170	12.234.12.108	TCP		80 → 1126 [ACK] Seq=1649 Ack=383 Win=49152 Len=1460 [TCP seg...
31	0.000067	12.234.12.108	161.58.73.170	TCP		1126 → 80 [ACK] Seq=383 Ack=3109 Win=64512 Len=0

> Frame 1: 1359 bytes on wire (10872 bits), 1359 bytes captured (10872 bits) on interface unknown, id 0

> Ethernet II, Src: Cisco_3c:3f:a8 (00:01:96:3c:3f:a8), Dst: AmbitMic_aa:af:80 (00:00:59:aa:af:80)

> Internet Protocol Version 4, Src: 161.58.73.170, Dst: 12.234.12.108

> Transmission Control Protocol, Src Port: 80, Dst Port: 1124, Seq: 1, Ack: 1, Len: 1305

net-lost-route.pcapng

Packets: 159 · Displayed: 159 (100.0%)

Profile: wireshark10