Laboratorio 1, parte 2

Redes

Mauricio Julio Rodrigo Lemus Guzmán – 22461

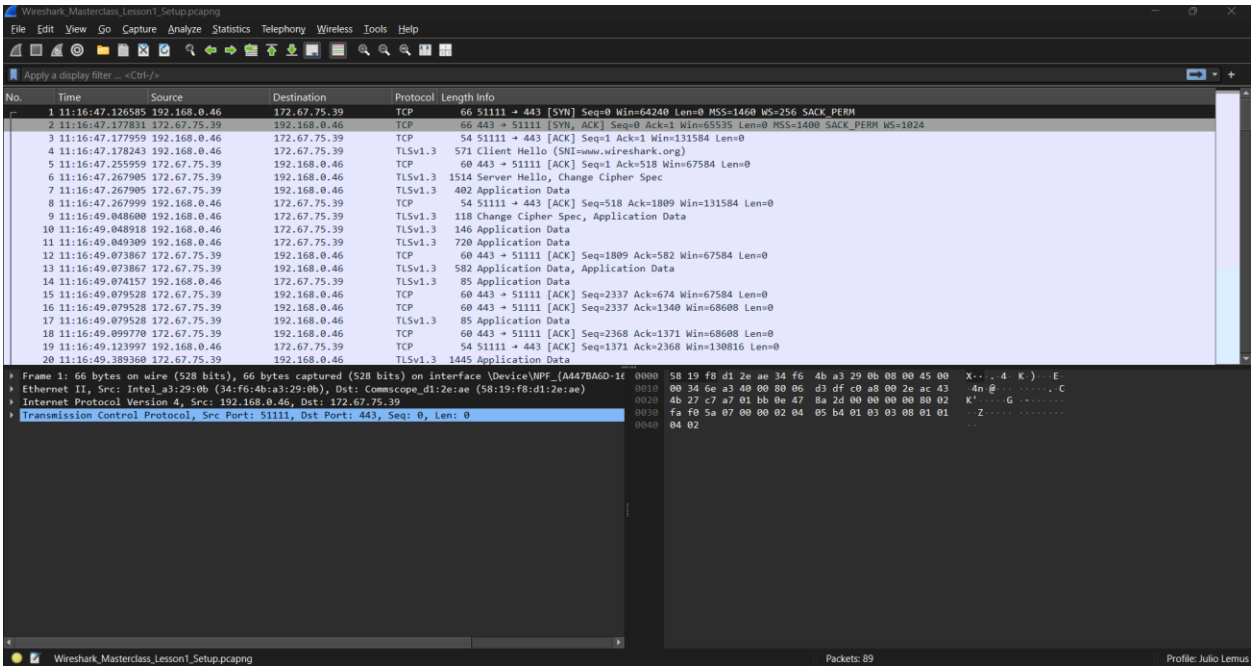
Preguntas

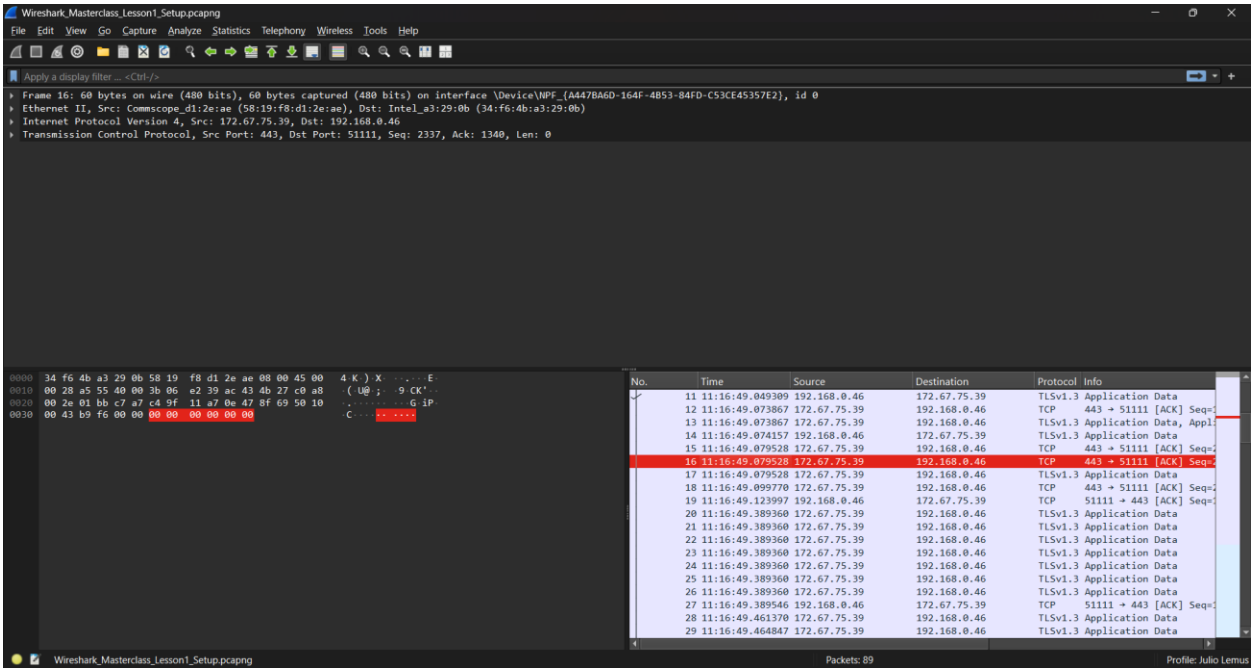
a. ¿Qué versión de HTTP está ejecutando su navegador?
    a. HTTP/1.1
b. ¿Qué versión de HTTP está ejecutando el servidor?
    a. HTTP/1.1
c. ¿Qué lenguajes (si aplica) indica el navegador que acepta a el servidor?
    a. Accept-Language: es-419,es;q=0.9,en;q=0.8
d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
    a. 471
e. En el caso que haya un problema de rendimiento mientras se descarga la página, ¿en que elementos de la red convendría "escuchar" los paquetes? ¿Es conveniente instalar Wireshark en el servidor? Justifique.

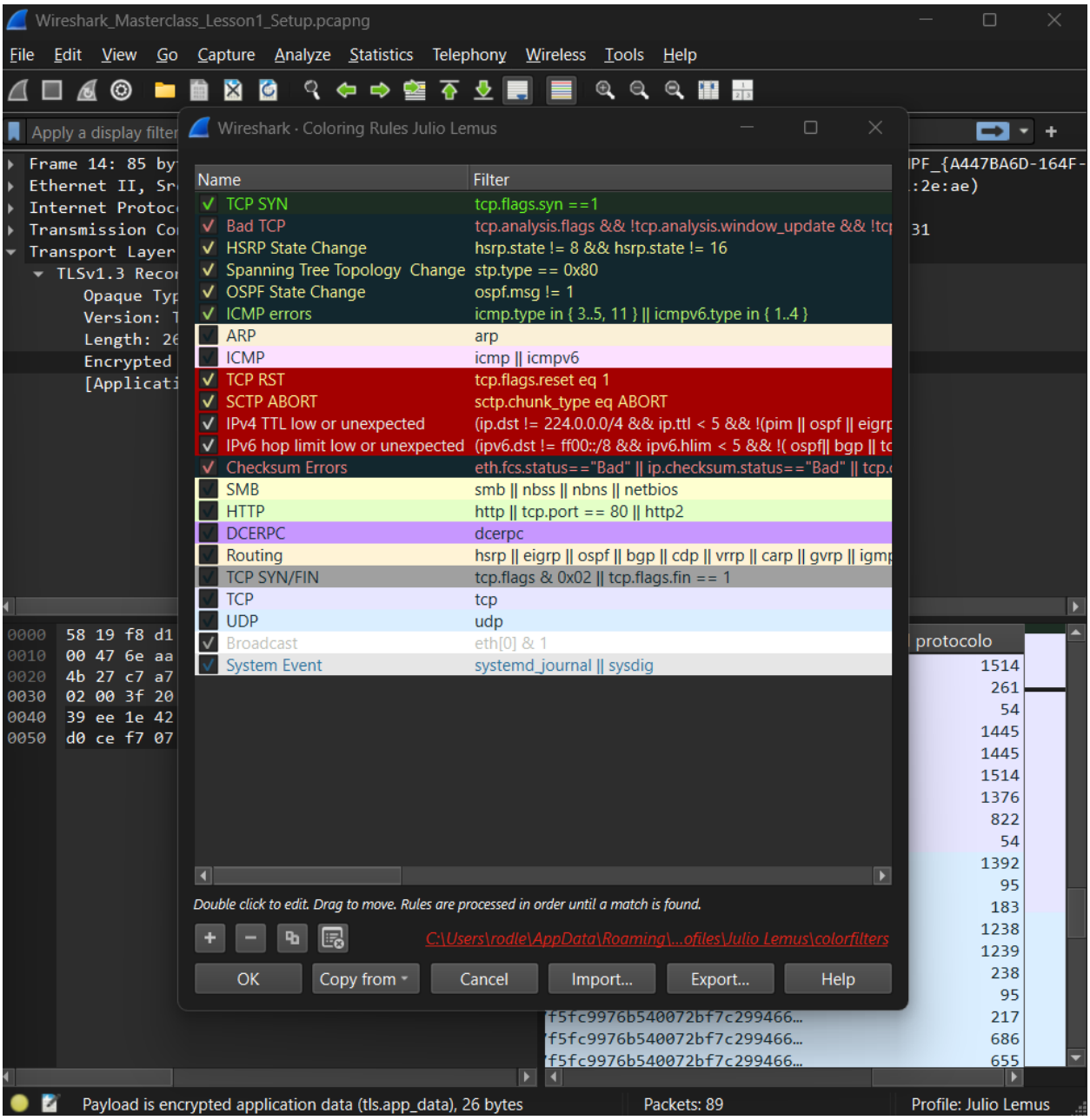
f. En caso de que existan problemas de rendimiento al descargar una página web, lo más recomendable es capturar el tráfico desde el lado del cliente y en puntos intermedios de la red, como switches o routers que actúen como pasarela entre el cliente y el servidor. Esto permite observar el comportamiento de la comunicación en diferentes tramos del recorrido del paquete.

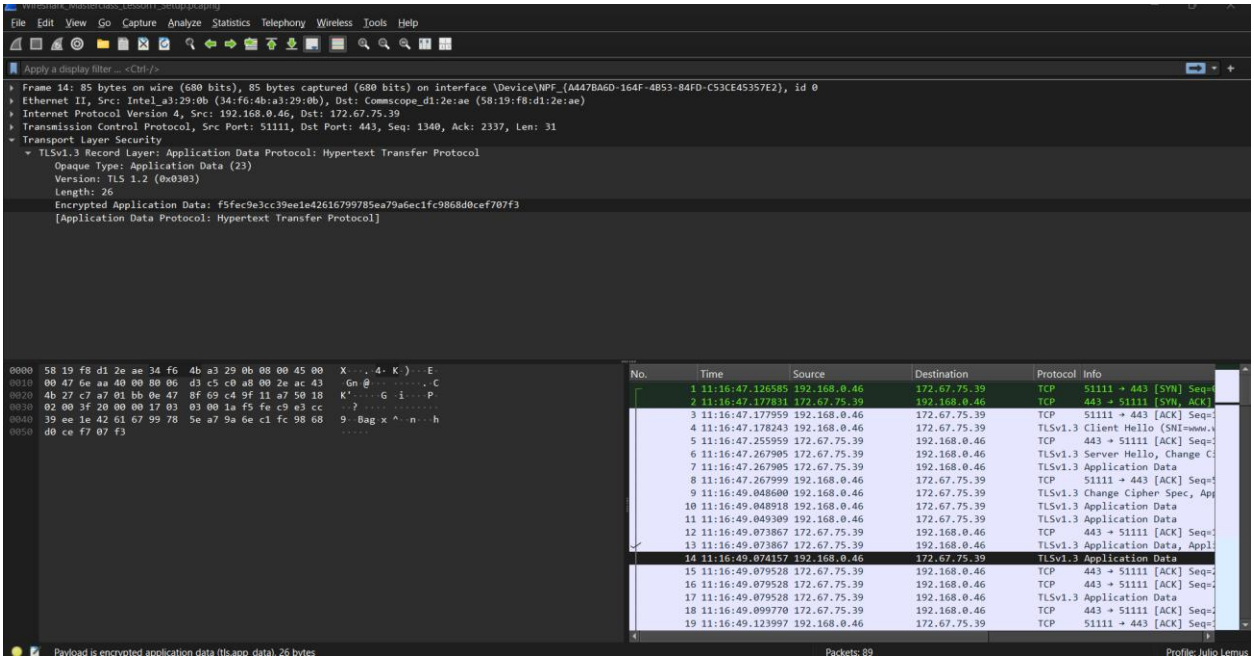
    No es conveniente instalar Wireshark directamente en el servidor, especialmente si este se encuentra en un entorno de producción, ya que puede consumir recursos considerables del sistema y afectar su rendimiento. En lugar de ello, se pueden usar herramientas más ligeras como tcpdump, que permiten realizar capturas puntuales sin comprometer la estabilidad del servidor.

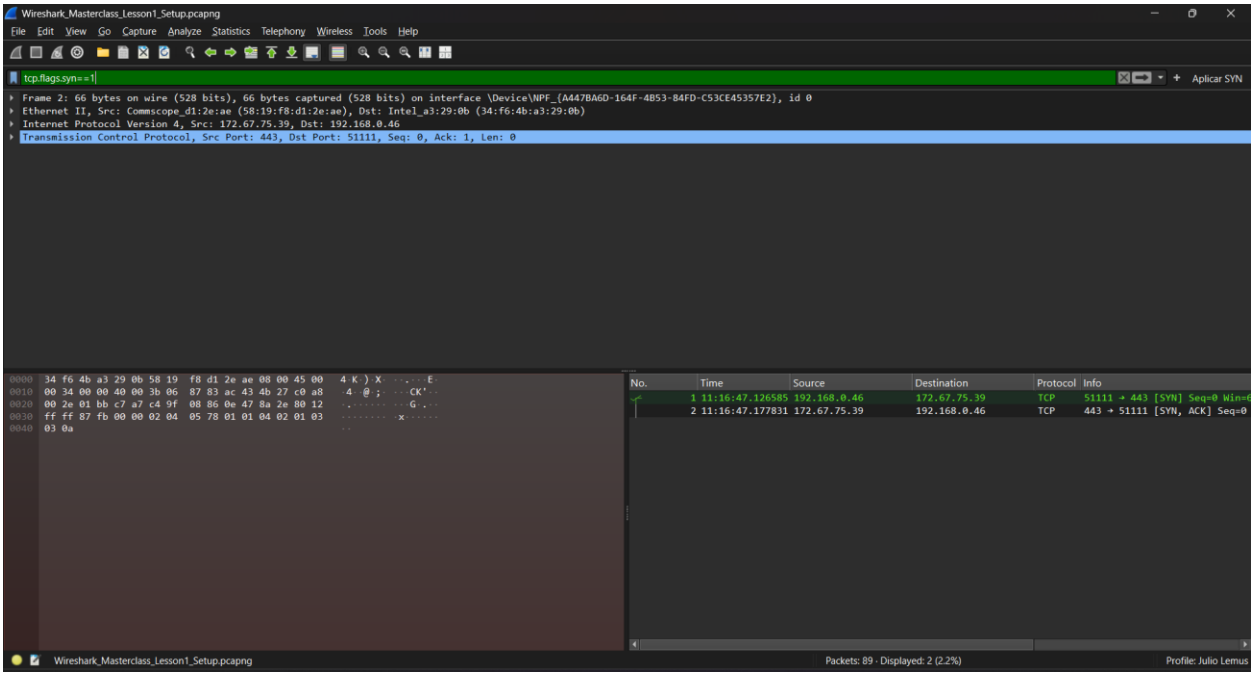
Evidencias

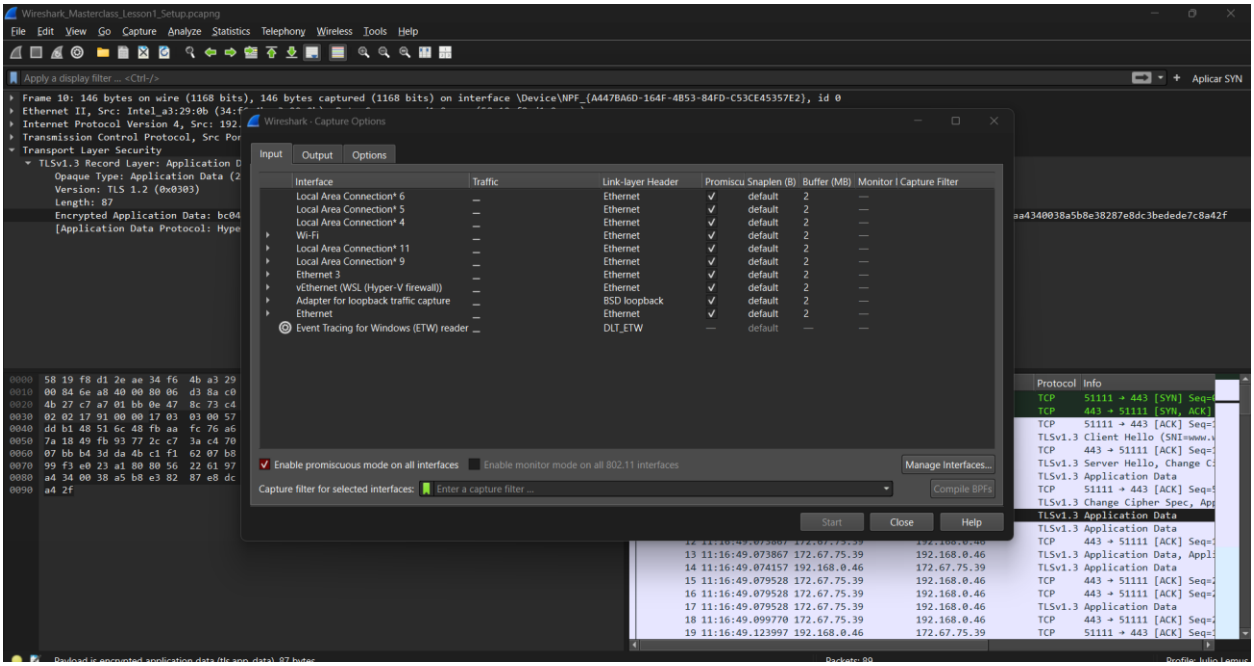

Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 11:16:47.126585 192.168.0.46 172.67.75.39 TCP 66 51111 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2 11:16:47.177831 172.67.75.39 192.168.0.46 TCP 66 443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=1024
3 11:16:47.177959 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
4 11:16:47.178243 192.168.0.46 172.67.75.39 TLSv1.3 571 Client Hello (SNI=www.wireshark.org)
5 11:16:47.255959 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=1 Ack=518 Win=67584 Len=0
6 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 1514 Server Hello, Change Cipher Spec
7 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 402 Application Data
8 11:16:47.267999 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=518 Ack=1809 Win=131584 Len=0
9 11:16:49.048600 192.168.0.46 172.67.75.39 TLSv1.3 118 Change Cipher Spec, Application Data
10 11:16:49.048918 192.168.0.46 172.67.75.39 TLSv1.3 146 Application Data
11 11:16:49.049309 192.168.0.46 172.67.75.39 TLSv1.3 720 Application Data
12 11:16:49.073867 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=1809 Ack=582 Win=67584 Len=0
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 582 Application Data, Application Data
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 85 Application Data
15 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=2337 Ack=674 Win=67584 Len=0
16 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=2337 Ack=1340 Win=68608 Len=0
17 11:16:49.079528 172.67.75.39 192.168.0.46 TLSv1.3 85 Application Data
18 11:16:49.099770 172.67.75.39 192.168.0.46 TCP 60 443 → 51111 [ACK] Seq=2368 Ack=1371 Win=68608 Len=0
19 11:16:49.123997 192.168.0.46 172.67.75.39 TCP 54 51111 → 443 [ACK] Seq=1371 Ack=2368 Win=130816 Len=0
20 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 1445 Application Data
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A447BA6D-1E
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b), Dst: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae)
Internet Protocol Version 4, Src: 192.168.0.46, Dst: 172.67.75.39
Transmission Control Protocol, Src Port: 51111, Dst Port: 443, Seq: 0, Len: 0
0000 58 19 f8 d1 2e ae 34 f6 4b a3 29 0b 08 00 45 00
0010 00 34 6e a3 40 00 80 06 d3 df c0 a8 00 2e ac 43
0020 4b 27 c7 a7 01 bb 0e 47 8a 2d 00 00 00 00 80 02
0030 fa f0 5a 07 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Wireshark_Masterclass_Lesson1_Setup.pcapng
Packets: 89
Profile: Julio Lemus

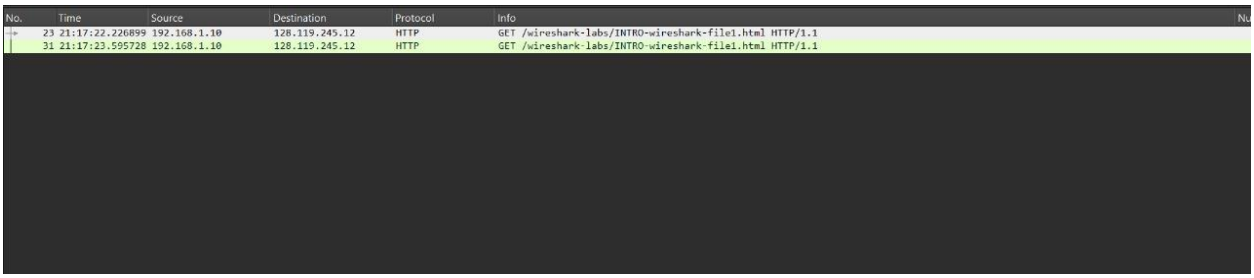

Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A447BA6D-164F-4B53-84FD-C53CE45357E2}, id 0
Ethernet II, Src: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae), Dst: Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Internet Protocol Version 4, Src: 172.67.75.39, Dst: 192.168.0.46
Transmission Control Protocol, Src Port: 443, Dst Port: 51111, Seq: 2337, Ack: 1340, Len: 0
0000 34 f6 4b a3 29 0b 58 19 f8 d1 2e ae 08 00 45 00
0010 00 28 a5 55 40 00 3b 06 e2 39 ac 43 4b 27 c0 a8
0020 00 2e 01 bb c7 a7 c4 9f 11 a7 0e 47 8f 69 50 10
0030 00 43 b9 f6 00 00 00 00 00 00 00 00
No. Time Source Destination Protocol Info
11 11:16:49.049309 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
12 11:16:49.073867 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 Application Data, Appl
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
15 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
16 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
17 11:16:49.079528 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
18 11:16:49.099770 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
19 11:16:49.123997 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=
20 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
21 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
22 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
23 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
24 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
25 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
26 11:16:49.389360 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
27 11:16:49.389546 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=
28 11:16:49.461370 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
29 11:16:49.464847 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
Wireshark_Masterclass_Lesson1_Setup.pcapng
Packets: 89
Profile: Julio Lemus

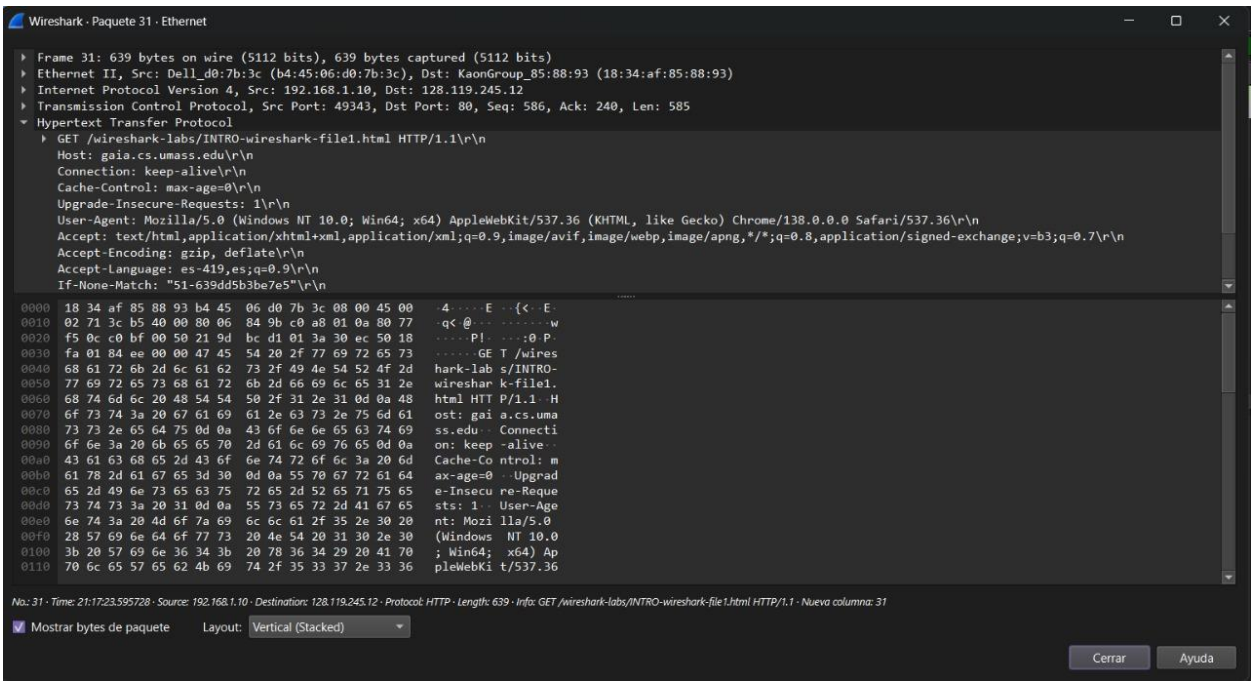

Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter
Wireshark · Coloring Rules Julio Lemus
Name
Filter
TCP SYN
tcp.flags.syn ==1
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update && !tcp
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
IPv4 TTL low or unexpected
(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp
IPv6 hop limit low or unexpected
(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tc
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.
SMB
smb || nbss || nbns || netbios
HTTP
http || tcp.port == 80 || http2
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
System Event
systemd_journal || sysdig
Double click to edit. Drag to move. Rules are processed in order until a match is found.
C:\Users\rodle\AppData\Roaming\...ofiles\Julio Lemus\colorfilters
OK
Copy from
Cancel
Import...
Export...
Help
protocolo
Payload is encrypted application data (tls.app_data), 26 bytes
Packets: 89
Profile: Julio Lemus


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Frame 14: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{A447BA6D-164F-4B53-84FD-C53CE45357E2}, id 0
Ethernet II, Src: Intel_a3:29:0b (34:f6:4b:a3:29:0b), Dst: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae)
Internet Protocol Version 4, Src: 192.168.0.46, Dst: 172.67.75.39
Transmission Control Protocol, Src Port: 51111, Dst Port: 443, Seq: 1340, Ack: 2337, Len: 31
Transport Layer Security
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 26
Encrypted Application Data: f5fec9e3cc39ee1e42616799785ea79a6ec1fc9868d0cef707f3
[Application Data Protocol: Hypertext Transfer Protocol]
0000 58 19 f8 d1 2e ae 34 f6 4b a3 29 0b 08 00 45 00
0010 00 47 6e aa 40 00 80 06 d3 c5 c0 a8 00 2e ac 43
0020 4b 27 c7 a7 01 bb 0e 47 8f 69 c4 9f 11 a7 50 18
0030 02 00 3f 20 00 00 17 03 03 00 1a f5 fe c9 e3 cc
0040 39 ee 1e 42 61 67 99 78 5e a7 9a 6e c1 fc 98 68
0050 d0 ce f7 07 f3
No. Time Source Destination Protocol Info
1 11:16:47.126585 192.168.0.46 172.67.75.39 TCP 51111 → 443 [SYN] Seq=0
2 11:16:47.177831 172.67.75.39 192.168.0.46 TCP 443 → 51111 [SYN, ACK]
3 11:16:47.177959 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=1
4 11:16:47.178243 192.168.0.46 172.67.75.39 TLSv1.3 Client Hello (SNI=www.
5 11:16:47.255959 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=1
6 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 Server Hello, Change C
7 11:16:47.267905 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
8 11:16:47.267999 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=1
9 11:16:49.048600 192.168.0.46 172.67.75.39 TLSv1.3 Change Cipher Spec, Ap
10 11:16:49.048918 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
11 11:16:49.049309 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
12 11:16:49.073867 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=1
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 Application Data, Appl
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
15 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=2
16 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=2
17 11:16:49.079528 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
18 11:16:49.099770 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=2
19 11:16:49.123997 172.67.75.39 192.168.0.46 TCP 51111 → 443 [ACK] Seq=1
Payload is encrypted application data (tls.app_data), 26 bytes
Packets: 89
Profile: Julio Lemus


Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn==1
Aplicar SYN
Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A447BA6D-164F-4B53-84FD-C53CE45357E2}, id 0
Ethernet II, Src: Commscope_d1:2e:ae (58:19:f8:d1:2e:ae), Dst: Intel_a3:29:0b (34:f6:4b:a3:29:0b)
Internet Protocol Version 4, Src: 172.67.75.39, Dst: 192.168.0.46
Transmission Control Protocol, Src Port: 443, Dst Port: 51111, Seq: 0, Ack: 1, Len: 0
0000 34 f6 4b a3 29 0b 58 19 f8 d1 2e ae 08 00 45 00
0010 00 34 00 00 40 00 3b 06 87 83 ac 43 4b 27 c0 a8
0020 00 2e 01 bb c7 a7 c4 9f 08 86 0e 47 8a 2e 80 12
0030 ff ff 87 fb 00 00 02 04 05 78 01 01 04 02 01 03
0040 03 0a
No. Time Source Destination Protocol Info
1 11:16:47.126585 192.168.0.46 172.67.75.39 TCP 51111 → 443 [SYN] Seq=0 Win=6
2 11:16:47.177831 172.67.75.39 192.168.0.46 TCP 443 → 51111 [SYN, ACK] Seq=0
Wireshark_Masterclass_Lesson1_Setup.pcapng
Packets: 89 · Displayed: 2 (2.2%)
Profile: Julio Lemus


Wireshark_Masterclass_Lesson1_Setup.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Aplicar SYN
Frame 10: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{A447BA6D-164F-4B53-84FD-C53CE45357E2}, id 0
Ethernet II, Src: Intel_a3:29:0b (34:f
Internet Protocol Version 4, Src: 192.
Transmission Control Protocol, Src Por
Transport Layer Security
TLSv1.3 Record Layer: Application D
Opaque Type: Application Data (2
Version: TLS 1.2 (0x0303)
Length: 87
Encrypted Application Data: bc04
[Application Data Protocol: Hype
aa4340038a5b8e38287e8dc3bedede7c8a42f
Wireshark · Capture Options
Input Output Options
Interface Traffic Link-layer Header Promiscu Snaplen (B) Buffer (MB) Monitor I Capture Filter
Local Area Connection* 6 Ethernet default 2
Local Area Connection* 5 Ethernet default 2
Local Area Connection* 4 Ethernet default 2
Wi-Fi Ethernet default 2
Local Area Connection* 11 Ethernet default 2
Local Area Connection* 9 Ethernet default 2
Ethernet 3 Ethernet default 2
vEthernet (WSL (Hyper-V firewall)) Ethernet default 2
Adapter for loopback traffic capture BSD loopback default 2
Ethernet Ethernet default 2
Event Tracing for Windows (ETW) reader DLT_ETW default
Enable promiscuous mode on all interfaces
Enable monitor mode on all 802.11 interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start Close Help
Protocol Info
TCP 51111 → 443 [SYN] Seq=
TCP 443 → 51111 [SYN, ACK]
TCP 51111 → 443 [ACK] Seq=
TLSv1.3 Client Hello (SNI=www.v
TCP 443 → 51111 [ACK] Seq=
TLSv1.3 Server Hello, Change C
TLSv1.3 Application Data
TCP 51111 → 443 [ACK] Seq=
TLSv1.3 Change Cipher Spec, Ap
TLSv1.3 Application Data
TLSv1.3 Application Data
TCP 443 → 51111 [ACK] Seq=
13 11:16:49.073867 172.67.75.39 192.168.0.46 TLSv1.3 Application Data, Appli
14 11:16:49.074157 192.168.0.46 172.67.75.39 TLSv1.3 Application Data
15 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
16 11:16:49.079528 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
17 11:16:49.079528 172.67.75.39 192.168.0.46 TLSv1.3 Application Data
18 11:16:49.099770 172.67.75.39 192.168.0.46 TCP 443 → 51111 [ACK] Seq=
19 11:16:49.123997 192.168.0.46 172.67.75.39 TCP 51111 → 443 [ACK] Seq=


No. Time Source Destination Protocol Info
23 21:17:22.226899 192.168.1.10 128.119.245.12 HTTP GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
31 21:17:23.595728 192.168.1.10 128.119.245.12 HTTP GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1


Wireshark · Paquete 31 · Ethernet
Frame 31: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits)
Ethernet II, Src: Dell_d0:7b:3c (b4:45:06:d0:7b:3c), Dst: KaonGroup_85:88:93 (18:34:af:85:88:93)
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49343, Dst Port: 80, Seq: 586, Ack: 240, Len: 585
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: es-419,es;q=0.9\r\n
If-None-Match: "51-639dd5b3be7e5"\r\n
0000 18 34 af 85 88 93 b4 45 06 d0 7b 3c 08 00 45 00 ·4·····E ··{<··E·
0010 02 71 3c b5 40 00 80 06 84 9b c0 a8 01 0a 80 77 ·q<·@··· ·······w
0020 f5 0c c0 bf 00 50 21 9d bc d1 01 3a 30 ec 50 18 ·····P!· ···:0·P·
0030 fa 01 84 ee 00 00 47 45 54 20 2f 77 69 72 65 73 ·····GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1··H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu·· Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive··
00a0 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d Cache-Co ntrol: m
00b0 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 ax-age=0 ··Upgrad
00c0 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 e-Insecu re-Reque
00d0 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 sts: 1·· User-Age
00e0 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0
00f0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 (Windows NT 10.0
0100 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 ; Win64; x64) Ap
0110 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 pleWebKi t/537.36
No.: 31 · Time: 21:17:23.595728 · Source: 192.168.1.10 · Destination: 128.119.245.12 · Protocol: HTTP · Length: 639 · Info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 · Nueva columna: 31
Mostrar bytes de paquete
Layout: Vertical (Stacked)
Cerrar
Ayuda

Referencias

University of Massachusetts Amherst. (n.d.). *INTRO-wireshark-file1.html*. Wireshark Labs. https://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html