Wireshark for Beginners: Capture Packets

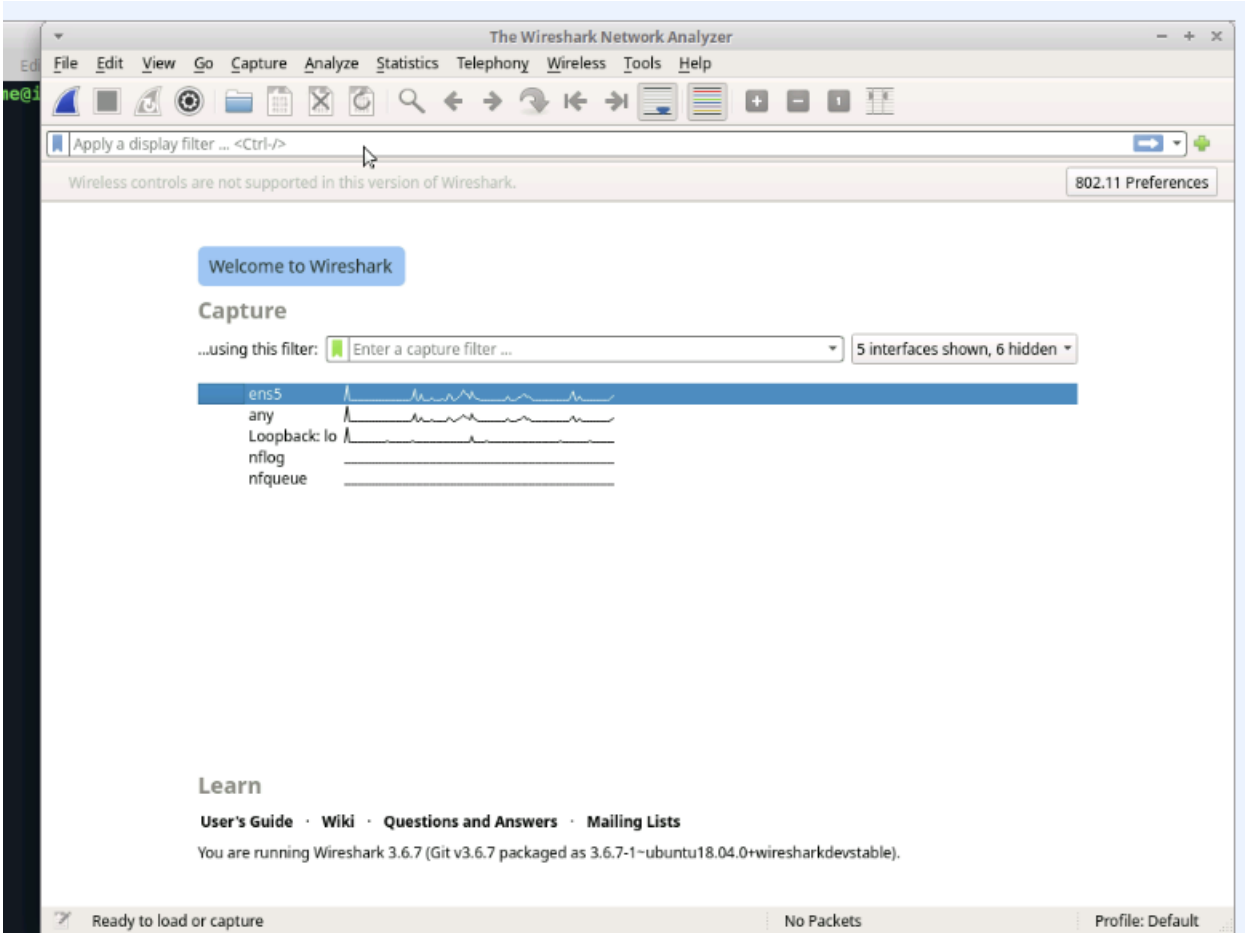
Task 1

Install and set up Wireshark on Ubuntu:

●To get the latest stable version of Wireshark on Ubuntu Linux, use the add-apt-repository command: ***sudo add-apt-repository ppa:wireshark-dev/stable***

●Wireshark should not be run as superuser for security reasons.

●The user can be added to the Wireshark group to add packet capture capabilities: ***sudo usermod -aG wireshark $USER***



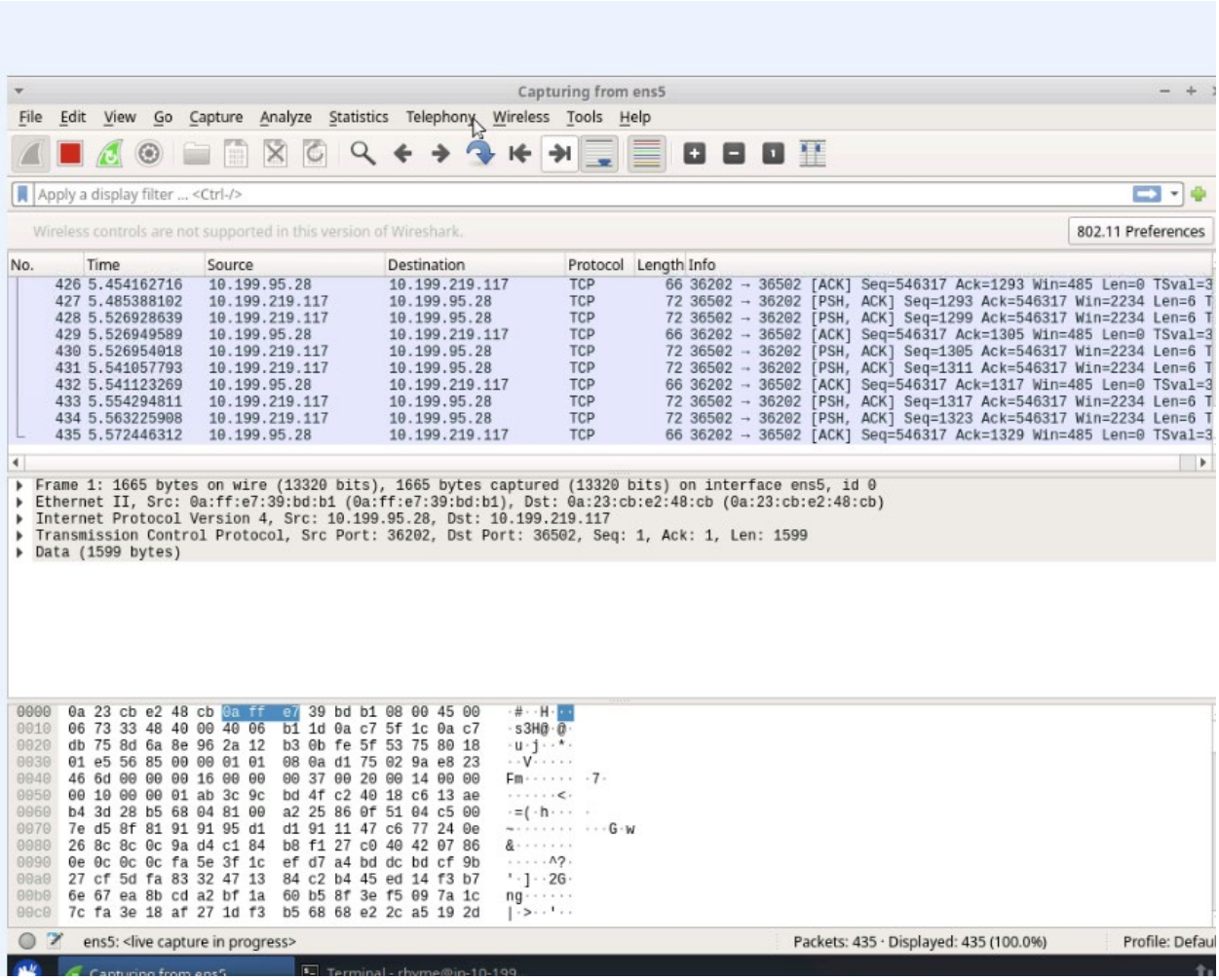
Task 2

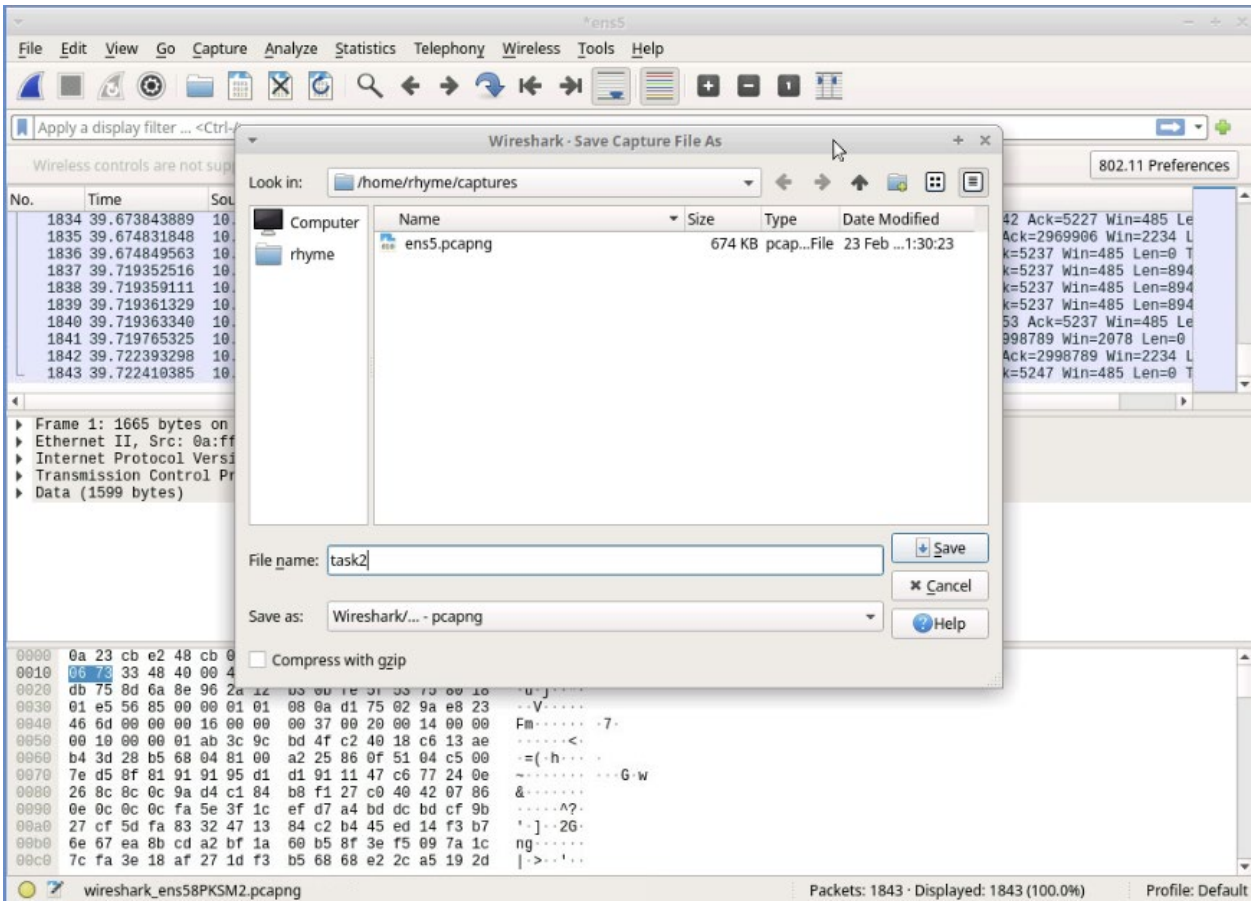
Start a packet capture on an ethernet port and save it to file:

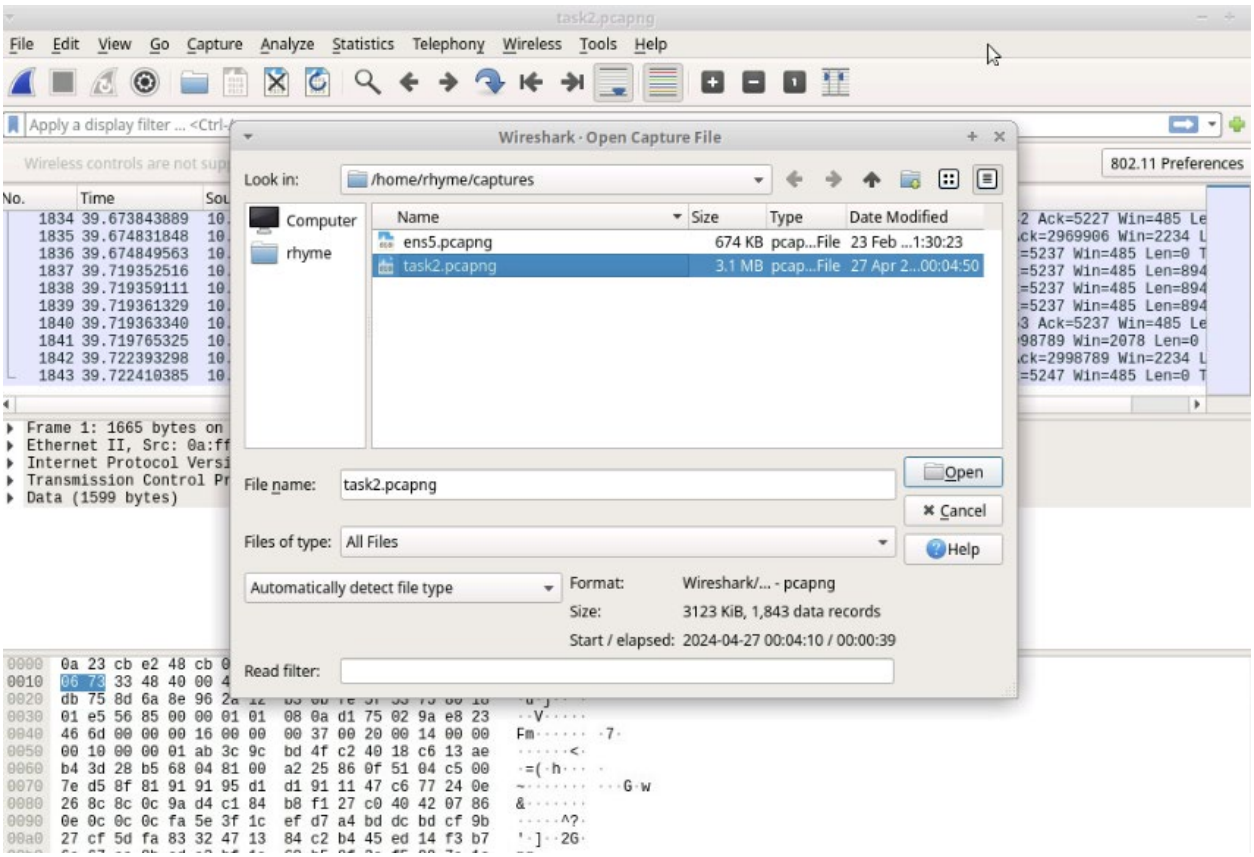
●The wired interface includes the ethernet packet capture, which begins with ‘en’ in Wireshark.

●The Wireshark app includes controls to start packet capture, stop capture, save the packets to a file, and load the capture file.

●A capture can only be saved once the capture has stopped.




*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
802.11 Preferences
No. Time
1834 39.673843889
1835 39.674831848
1836 39.674849563
1837 39.719352516
1838 39.719359111
1839 39.719361329
1840 39.719363340
1841 39.719765325
1842 39.722393298
1843 39.722410385
Frame 1: 1665 bytes on
Ethernet II, Src: 0a:ff
Internet Protocol Versi
Transmission Control Pr
Data (1599 bytes)
Wireshark · Save Capture File As
Look in: /home/rhyme/captures
Computer
rhyme
Name Size Type Date Modified
ens5.pcapng 674 KB pcap...File 23 Feb ...1:30:23
File name: task2
Save as: Wireshark/... - pcapng
Save
Cancel
Help
Compress with gzip
wireshark_ens58PKSM2.pcapng
Packets: 1843 · Displayed: 1843 (100.0%)
Profile: Default

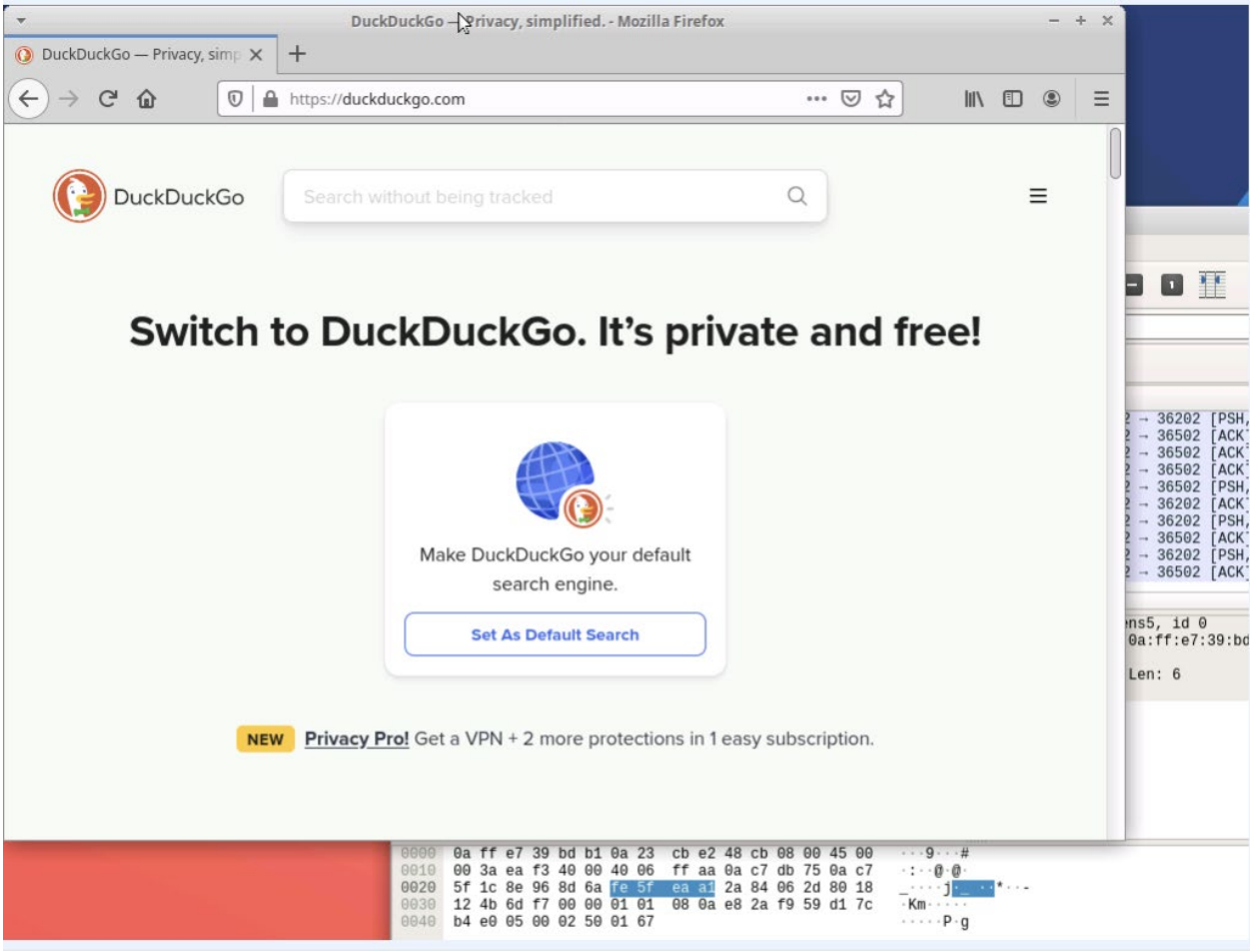


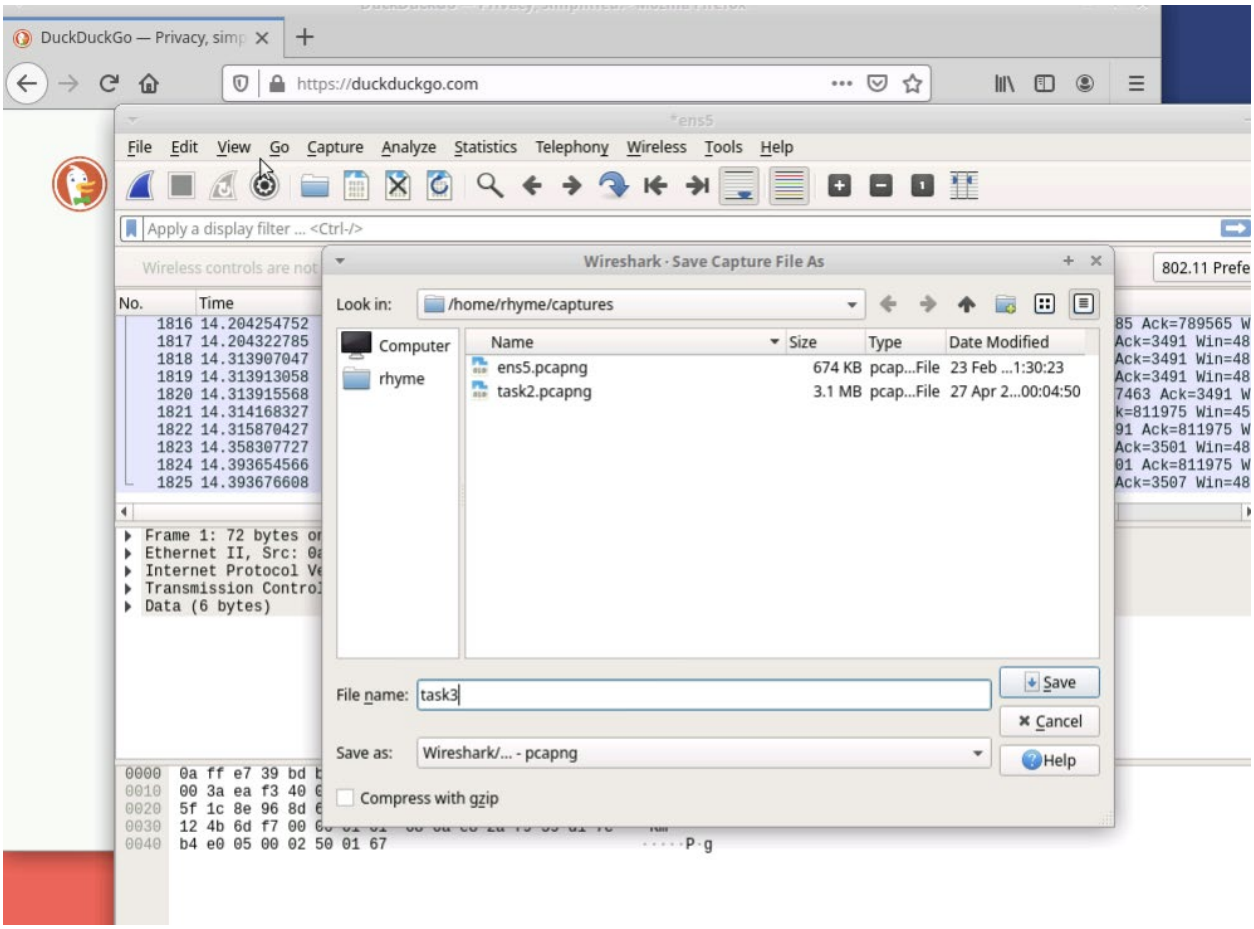
Task 3

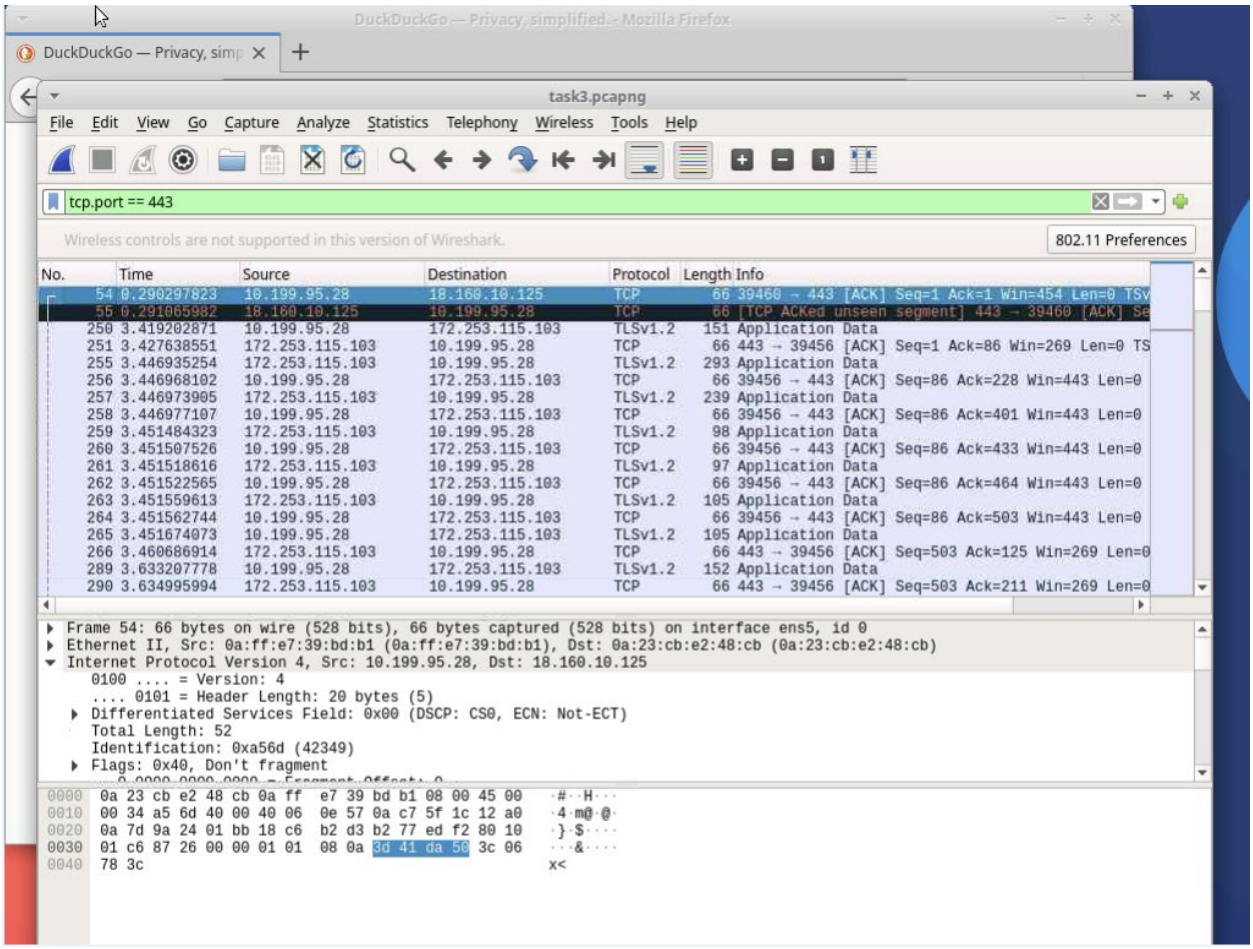
Use a display filter to detect HTTPS packets:

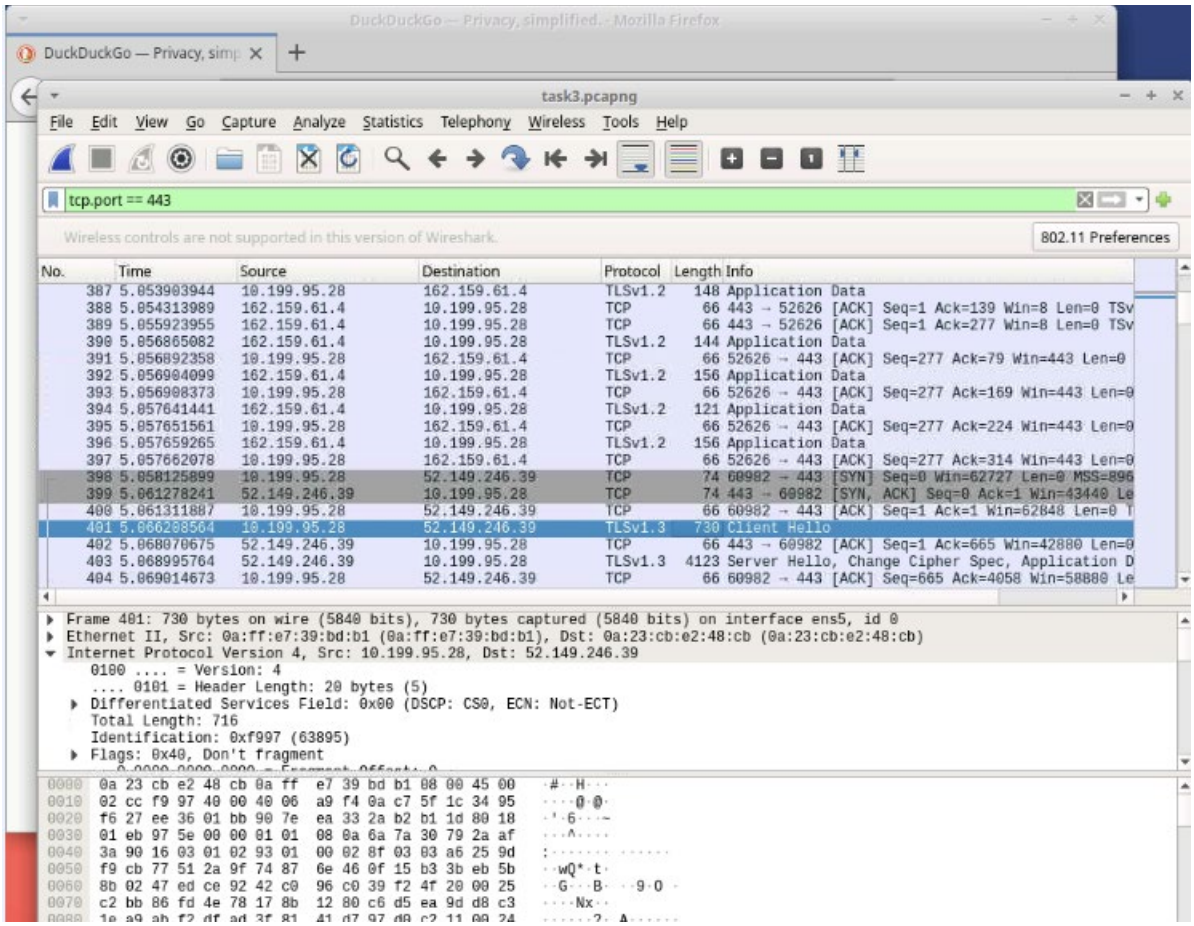
●To display certain packets in an existing packet capture, use a display filter.

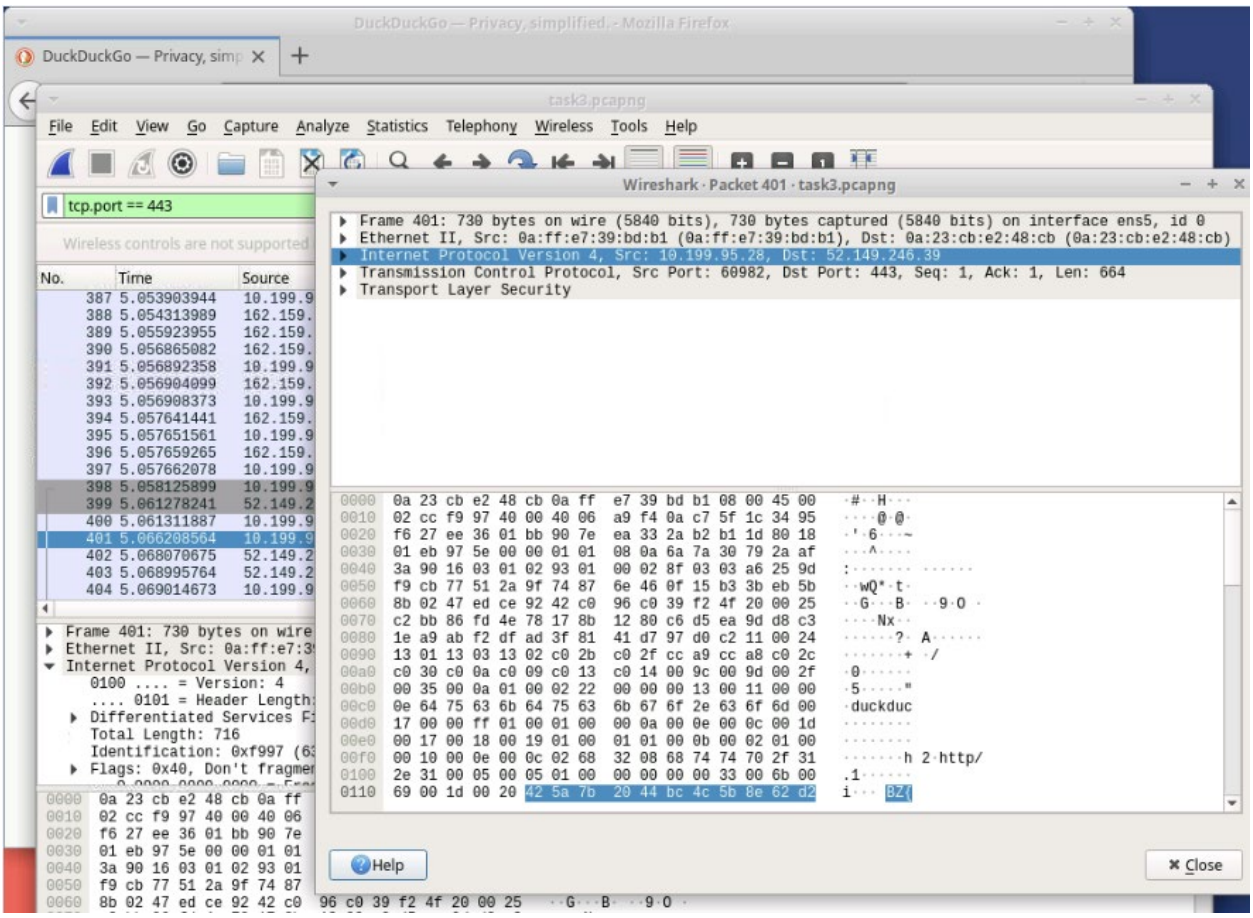
●To display only HTTPS traffic, use a filter on TCP port 443: ***tcp.port == 443***


DuckDuckGo — Privacy, simplified. - Mozilla Firefox
DuckDuckGo — Privacy, simp
https://duckduckgo.com
DuckDuckGo
Search without being tracked
Switch to DuckDuckGo. It's private and free!
Make DuckDuckGo your default search engine.
Set As Default Search
NEW
Privacy Pro!
Get a VPN + 2 more protections in 1 easy subscription.
0000 0a ff e7 39 bd b1 0a 23 cb e2 48 cb 08 00 45 00
0010 00 3a ea f3 40 00 40 06 ff aa 0a c7 db 75 0a c7
0020 5f 1c 8e 96 8d 6a fe 5f ea a1 2a 84 06 2d 80 18
0030 12 4b 6d f7 00 00 01 01 08 0a e8 2a f9 59 d1 7c
0040 b4 e0 05 00 02 50 01 67


DuckDuckGo — Privacy, simp
https://duckduckgo.com
*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireless controls are not
802.11 Prefe
No. Time
1816 14.204254752
1817 14.204322785
1818 14.313907047
1819 14.313913058
1820 14.313915568
1821 14.314168327
1822 14.315870427
1823 14.358307727
1824 14.393654566
1825 14.393676608
Frame 1: 72 bytes or
Ethernet II, Src: 0a
Internet Protocol Ve
Transmission Control
Data (6 bytes)
0000 0a ff e7 39 bd b
0010 00 3a ea f3 40 0
0020 5f 1c 8e 96 8d 6
0030 12 4b 6d f7 00 6
0040 b4 e0 05 00 02 50 01 67
Wireshark · Save Capture File As
Look in: /home/rhyme/captures
Computer
rhyme
Name Size Type Date Modified
ens5.pcapng 674 KB pcap...File 23 Feb ...1:30:23
task2.pcapng 3.1 MB pcap...File 27 Apr 2...00:04:50
File name: task3
Save as: Wireshark/... - pcapng
Compress with gzip
Save
Cancel
Help


DuckDuckGo — Privacy, simplified. - Mozilla Firefox
DuckDuckGo — Privacy, simp
task3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
54 0.290297823 10.199.95.28 18.160.10.125 TCP 66 39460 → 443 [ACK] Seq=1 Ack=1 Win=454 Len=0 TSv
55 0.291065982 18.160.10.125 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 443 → 39460 [ACK] Se
250 3.419202871 10.199.95.28 172.253.115.103 TLSv1.2 151 Application Data
251 3.427638551 172.253.115.103 10.199.95.28 TCP 66 443 → 39456 [ACK] Seq=1 Ack=86 Win=269 Len=0 TS
255 3.446935254 172.253.115.103 10.199.95.28 TLSv1.2 293 Application Data
256 3.446968102 10.199.95.28 172.253.115.103 TCP 66 39456 → 443 [ACK] Seq=86 Ack=228 Win=443 Len=0
257 3.446973905 172.253.115.103 10.199.95.28 TLSv1.2 239 Application Data
258 3.446977107 10.199.95.28 172.253.115.103 TCP 66 39456 → 443 [ACK] Seq=86 Ack=401 Win=443 Len=0
259 3.451484323 172.253.115.103 10.199.95.28 TLSv1.2 98 Application Data
260 3.451507526 10.199.95.28 172.253.115.103 TCP 66 39456 → 443 [ACK] Seq=86 Ack=433 Win=443 Len=0
261 3.451518616 172.253.115.103 10.199.95.28 TLSv1.2 97 Application Data
262 3.451522565 10.199.95.28 172.253.115.103 TCP 66 39456 → 443 [ACK] Seq=86 Ack=464 Win=443 Len=0
263 3.451559613 172.253.115.103 10.199.95.28 TLSv1.2 105 Application Data
264 3.451562744 10.199.95.28 172.253.115.103 TCP 66 39456 → 443 [ACK] Seq=86 Ack=503 Win=443 Len=0
265 3.451674073 10.199.95.28 172.253.115.103 TLSv1.2 105 Application Data
266 3.460686914 172.253.115.103 10.199.95.28 TCP 66 443 → 39456 [ACK] Seq=503 Ack=125 Win=269 Len=0
289 3.633207778 10.199.95.28 172.253.115.103 TLSv1.2 152 Application Data
290 3.634995994 172.253.115.103 10.199.95.28 TCP 66 443 → 39456 [ACK] Seq=503 Ack=211 Win=269 Len=0
Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 18.160.10.125
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xa56d (42349)
Flags: 0x40, Don't fragment
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 00 34 a5 6d 40 00 40 06 0e 57 0a c7 5f 1c 12 a0
0020 0a 7d 9a 24 01 bb 18 c6 b2 d3 b2 77 ed f2 80 10
0030 01 c6 87 26 00 00 01 01 08 0a 3d 41 da 50 3c 06
0040 78 3c


DuckDuckGo — Privacy, simplified. - Mozilla Firefox
DuckDuckGo — Privacy, simp
task3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
387 5.053903944 10.199.95.28 162.159.61.4 TLSv1.2 148 Application Data
388 5.054313989 162.159.61.4 10.199.95.28 TCP 66 443 → 52626 [ACK] Seq=1 Ack=139 Win=8 Len=0 TSv
389 5.055923955 162.159.61.4 10.199.95.28 TCP 66 443 → 52626 [ACK] Seq=1 Ack=277 Win=8 Len=0 TSv
390 5.056865082 162.159.61.4 10.199.95.28 TLSv1.2 144 Application Data
391 5.056892358 10.199.95.28 162.159.61.4 TCP 66 52626 → 443 [ACK] Seq=277 Ack=79 Win=443 Len=0
392 5.056904099 162.159.61.4 10.199.95.28 TLSv1.2 156 Application Data
393 5.056908373 10.199.95.28 162.159.61.4 TCP 66 52626 → 443 [ACK] Seq=277 Ack=169 Win=443 Len=0
394 5.057641441 162.159.61.4 10.199.95.28 TLSv1.2 121 Application Data
395 5.057651561 10.199.95.28 162.159.61.4 TCP 66 52626 → 443 [ACK] Seq=277 Ack=224 Win=443 Len=0
396 5.057659265 162.159.61.4 10.199.95.28 TLSv1.2 156 Application Data
397 5.057662078 10.199.95.28 162.159.61.4 TCP 66 52626 → 443 [ACK] Seq=277 Ack=314 Win=443 Len=0
398 5.058125899 10.199.95.28 52.149.246.39 TCP 74 60982 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
399 5.061278241 52.149.246.39 10.199.95.28 TCP 74 443 → 60982 [SYN, ACK] Seq=0 Ack=1 Win=43440 Le
400 5.061311887 10.199.95.28 52.149.246.39 TCP 66 60982 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 T
401 5.066208564 10.199.95.28 52.149.246.39 TLSv1.3 730 Client Hello
402 5.068070675 52.149.246.39 10.199.95.28 TCP 66 443 → 60982 [ACK] Seq=1 Ack=665 Win=42880 Len=0
403 5.068995764 52.149.246.39 10.199.95.28 TLSv1.3 4123 Server Hello, Change Cipher Spec, Application D
404 5.069014673 10.199.95.28 52.149.246.39 TCP 66 60982 → 443 [ACK] Seq=665 Ack=4058 Win=58880 Le
Frame 401: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 52.149.246.39
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 716
Identification: 0xf997 (63895)
Flags: 0x40, Don't fragment
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 02 cc f9 97 40 00 40 06 a9 f4 0a c7 5f 1c 34 95
0020 f6 27 ee 36 01 bb 90 7e ea 33 2a b2 b1 1d 80 18
0030 01 eb 97 5e 00 00 01 01 08 0a 6a 7a 30 79 2a af
0040 3a 90 16 03 01 02 93 01 00 02 8f 03 03 a6 25 9d
0050 f9 cb 77 51 2a 9f 74 87 6e 46 0f 15 b3 3b eb 5b
0060 8b 02 47 ed ce 92 42 c0 96 c0 39 f2 4f 20 00 25
0070 c2 bb 86 fd 4e 78 17 8b 12 80 c6 d5 ea 9d d8 c3

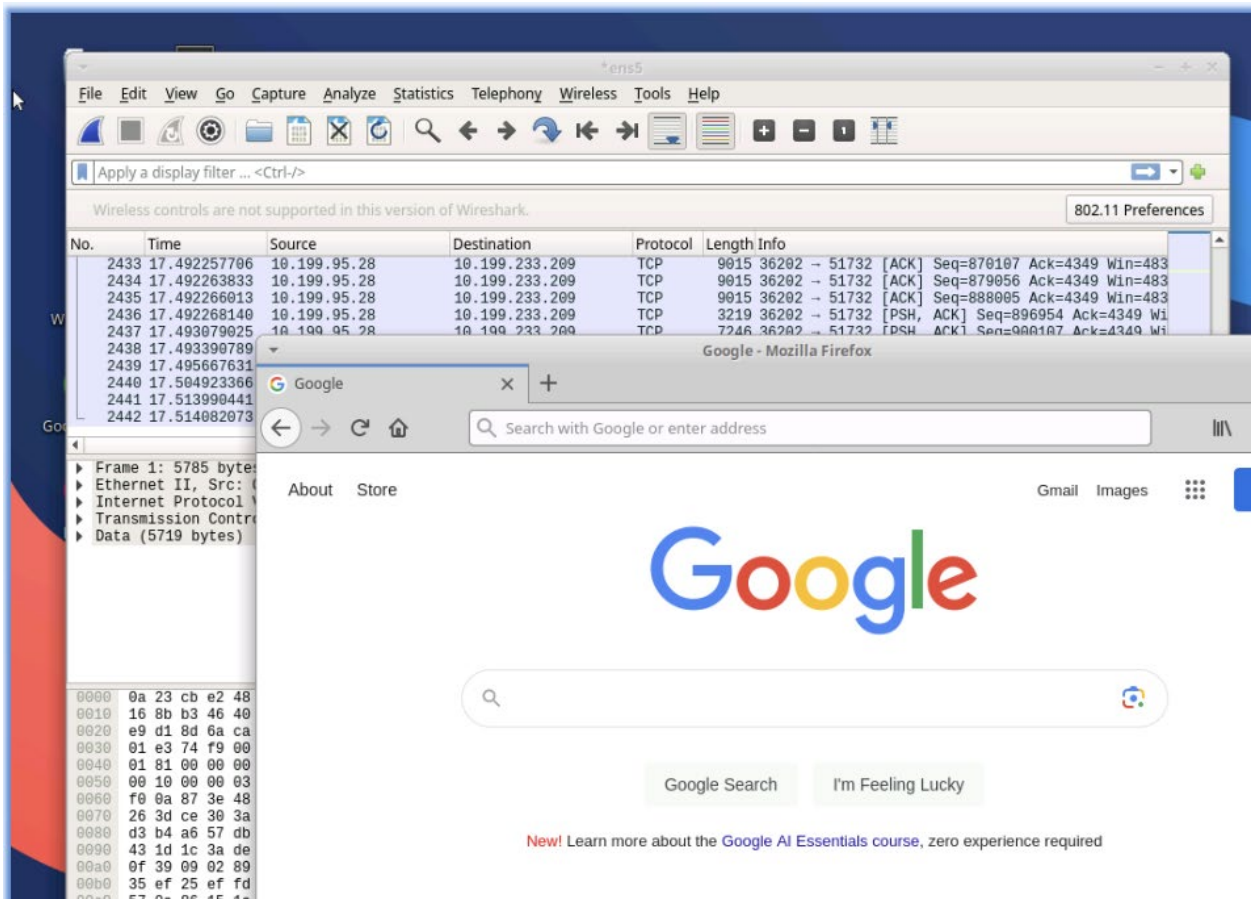


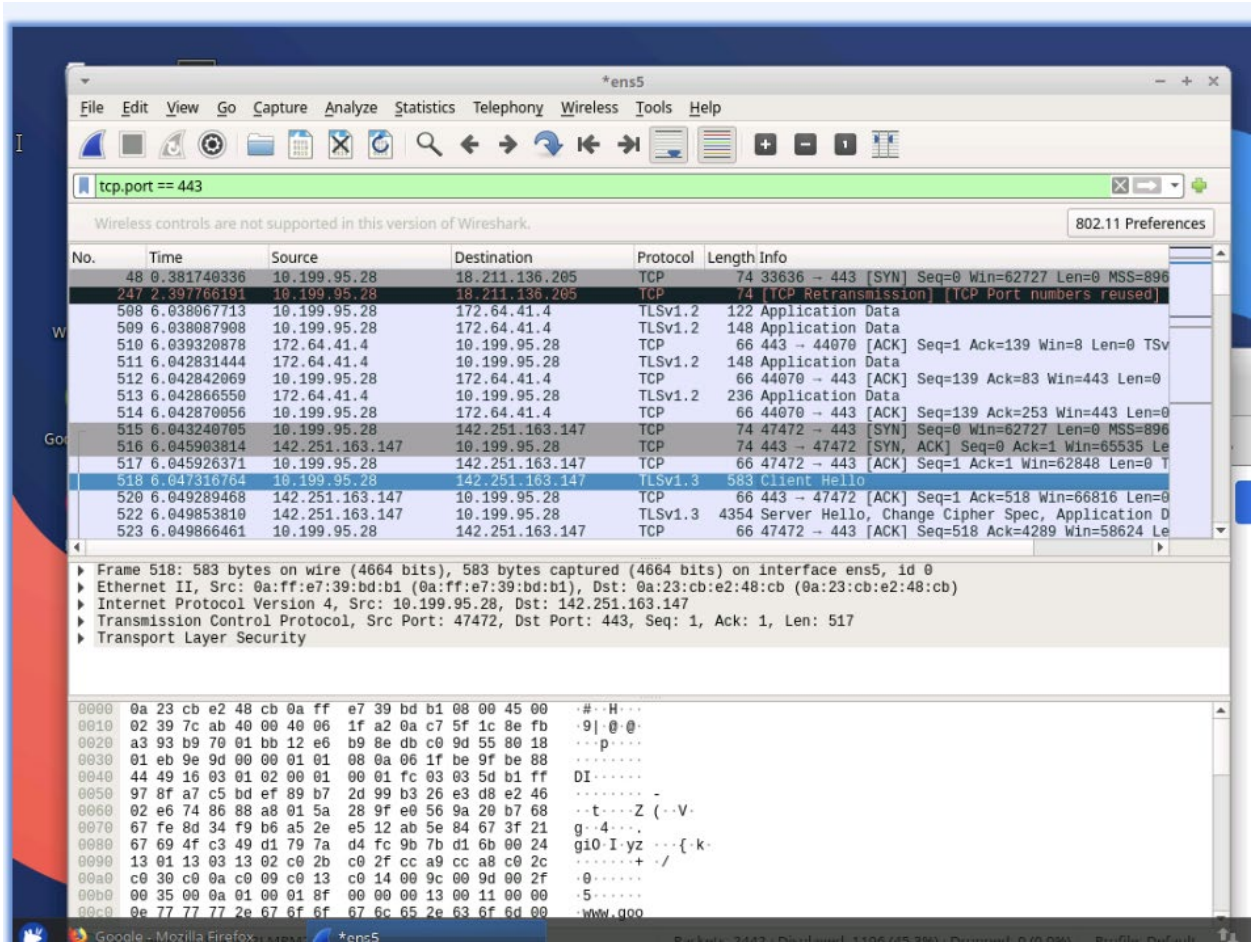
Task 4

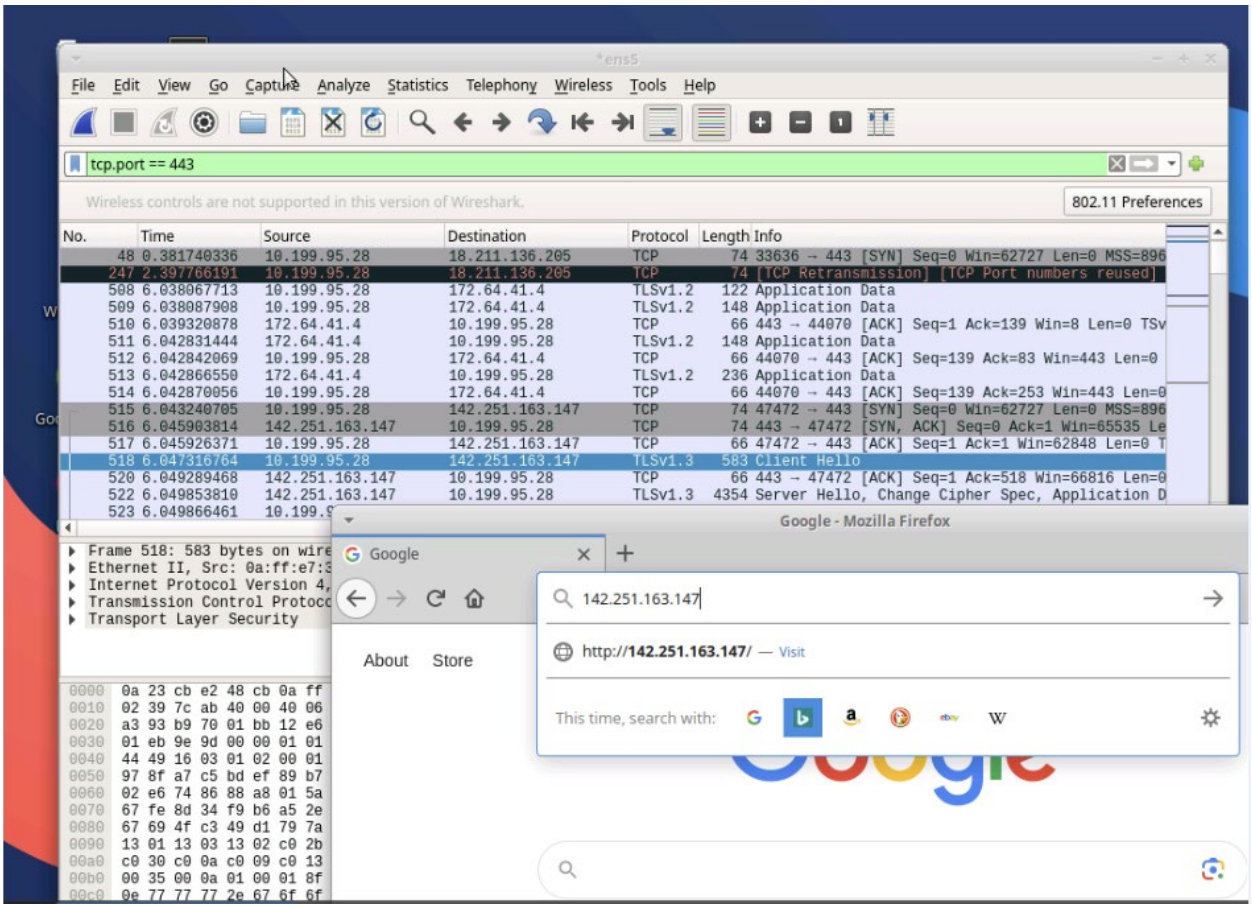
Visit a web page and detect its IP address using a display filter:

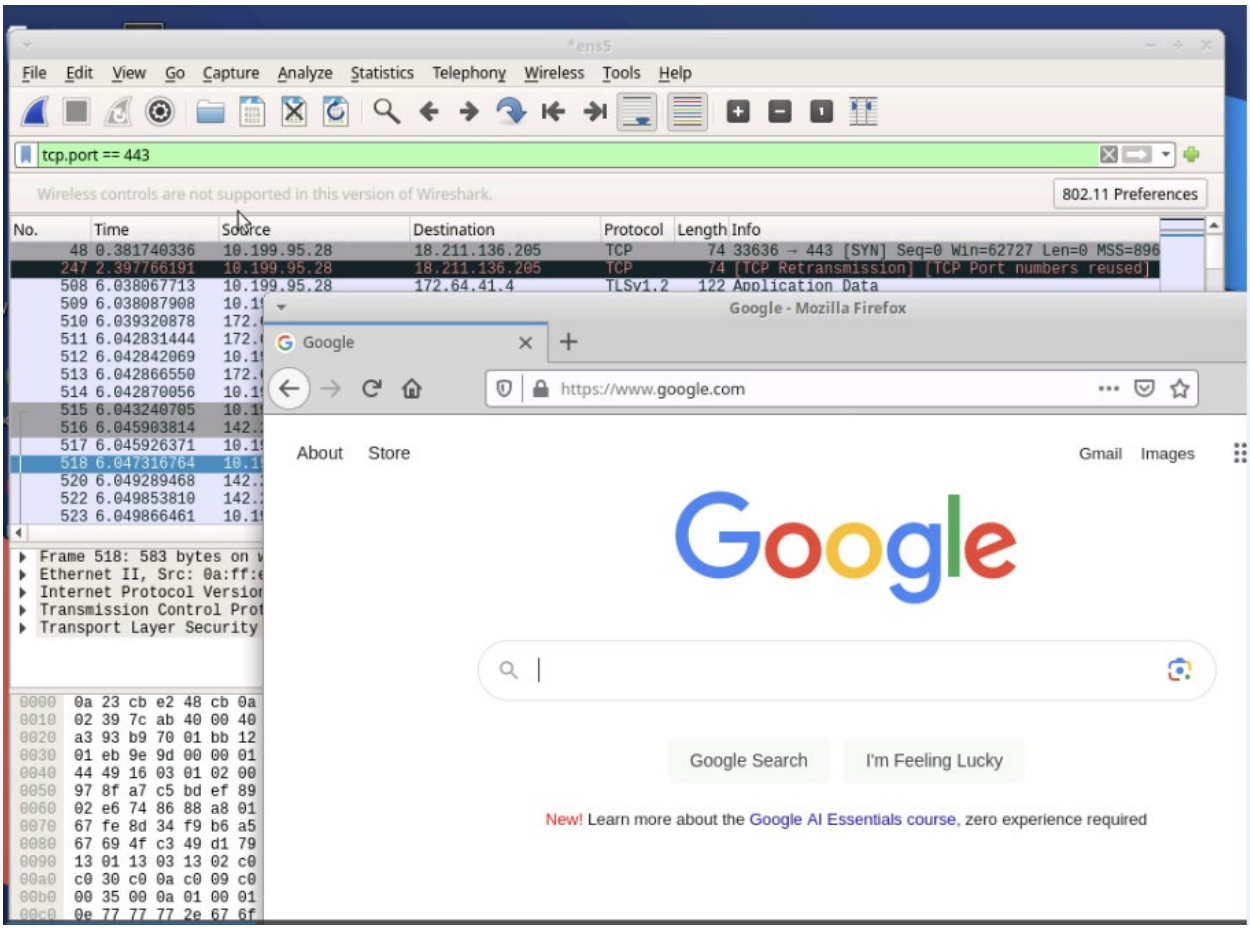
●A TLS handshake display filter may be used to detect a website visit in a packet list: tls.handshake.type ==1

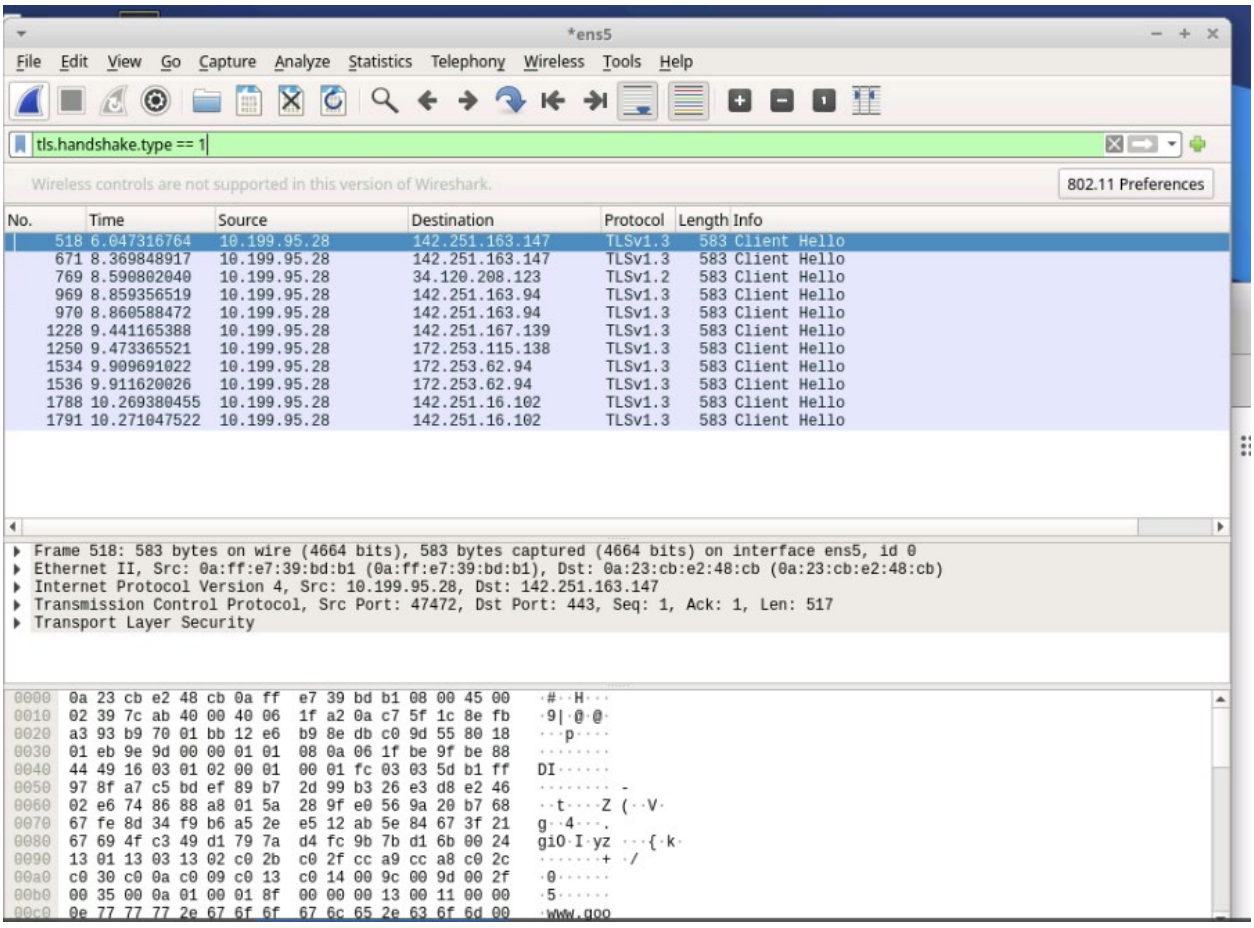
●The IP address is used in a filter to obtain packet information for a particular website: ip.addr == 142.251.163.105

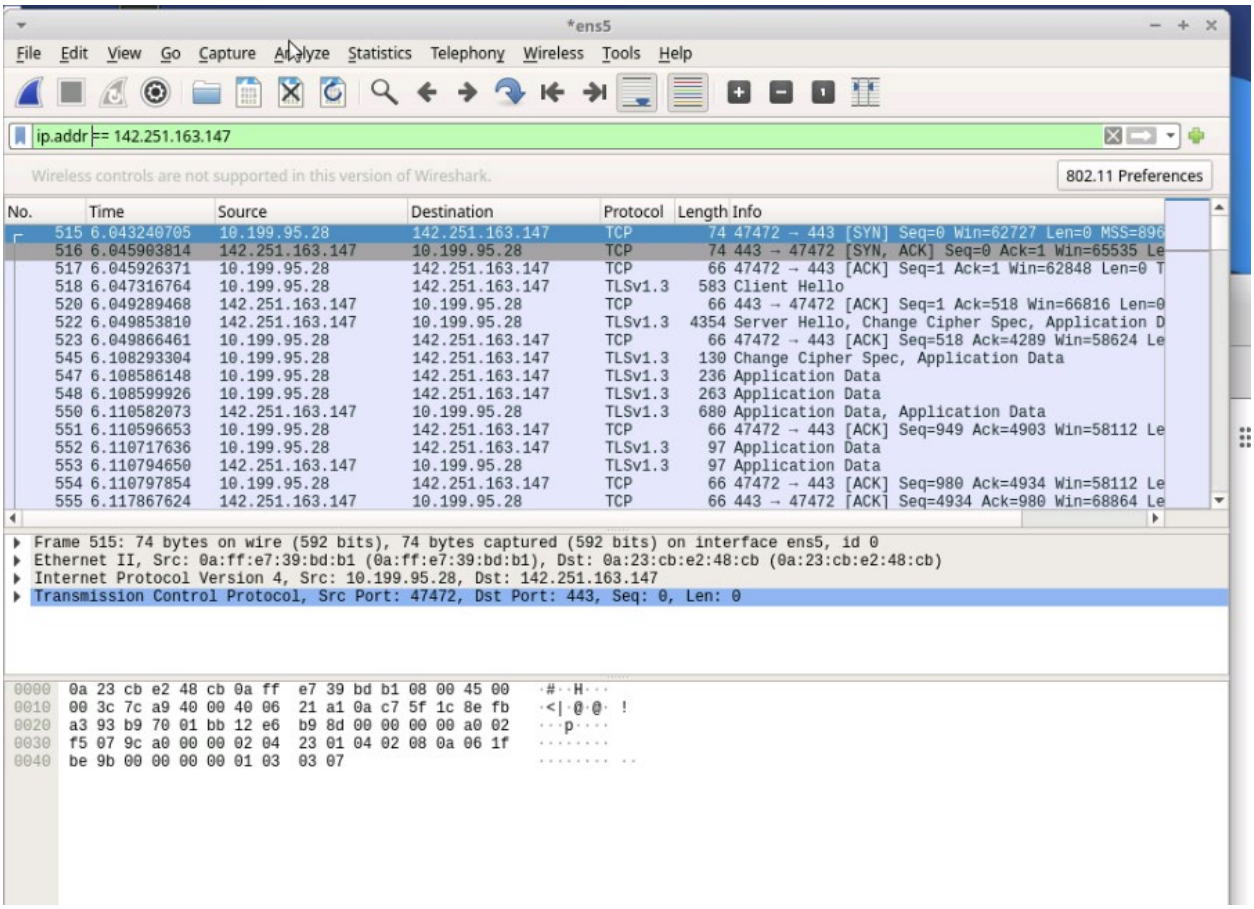

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
2433 17.492257706 10.199.95.28 10.199.233.209 TCP 9015 36202 → 51732 [ACK] Seq=870107 Ack=4349 Win=483
2434 17.492263833 10.199.95.28 10.199.233.209 TCP 9015 36202 → 51732 [ACK] Seq=879056 Ack=4349 Win=483
2435 17.492266013 10.199.95.28 10.199.233.209 TCP 9015 36202 → 51732 [ACK] Seq=888005 Ack=4349 Win=483
2436 17.492268140 10.199.95.28 10.199.233.209 TCP 3219 36202 → 51732 [PSH, ACK] Seq=896954 Ack=4349 Wi
2437 17.493079025
2438 17.493390789
2439 17.495667631
2440 17.504923366
2441 17.513990441
2442 17.514082073
Frame 1: 5785 bytes
Ethernet II, Src:
Internet Protocol
Transmission Contr
Data (5719 bytes)
0000 0a 23 cb e2 48
0010 16 8b b3 46 40
0020 e9 d1 8d 6a ca
0030 01 e3 74 f9 00
0040 01 81 00 00 00
0050 00 10 00 00 03
0060 f0 0a 87 3e 48
0070 26 3d ce 30 3a
0080 d3 b4 a6 57 db
0090 43 1d 1c 3a de
00a0 0f 39 09 02 89
00b0 35 ef 25 ef fd
Google - Mozilla Firefox
Google
Search with Google or enter address
About Store
Gmail Images
Google
Google Search
I'm Feeling Lucky
New! Learn more about the Google AI Essentials course, zero experience required

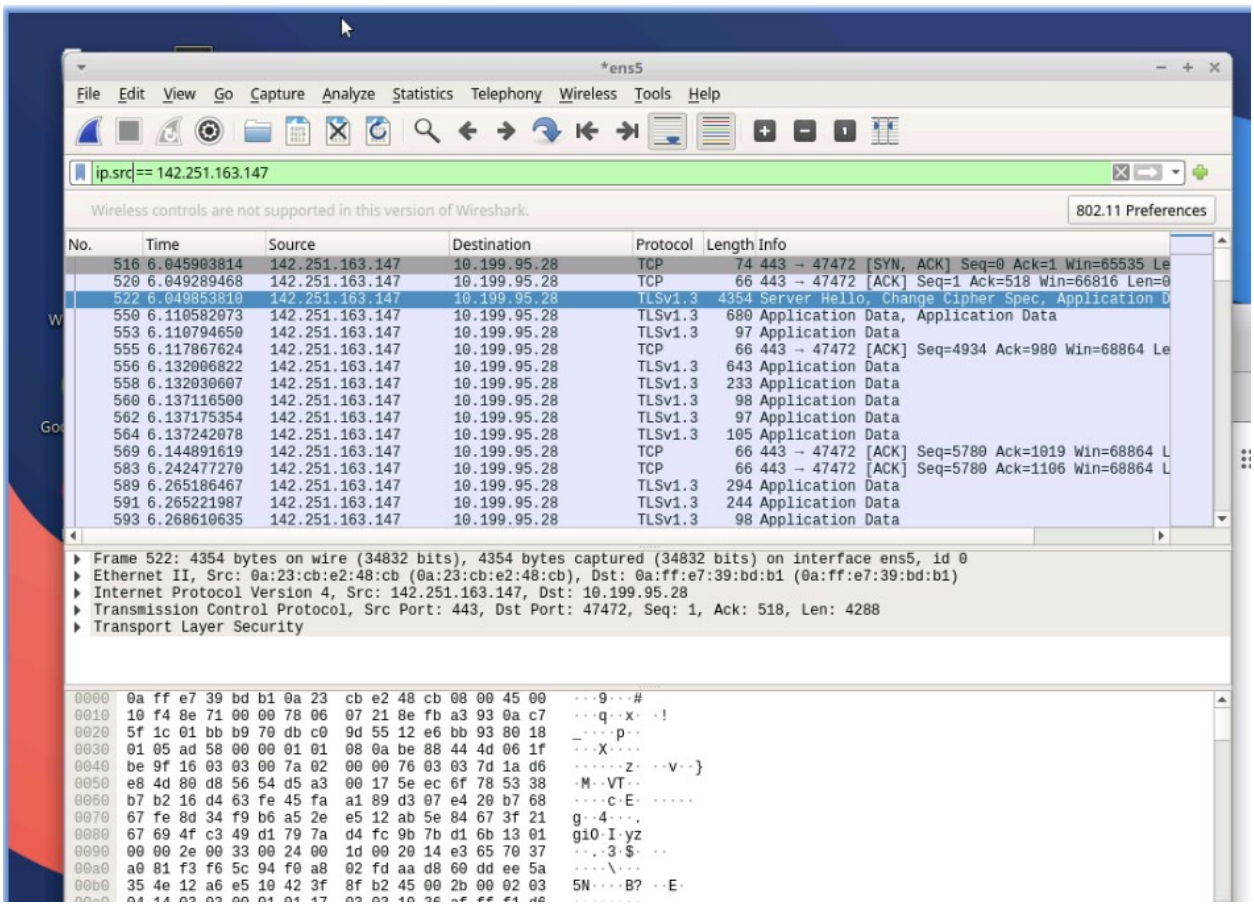

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
48 0.381740336 10.199.95.28 18.211.136.205 TCP 74 33636 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
247 2.397766191 10.199.95.28 18.211.136.205 TCP 74 [TCP Retransmission] [TCP Port numbers reused]
508 6.038067713 10.199.95.28 172.64.41.4 TLSv1.2 122 Application Data
509 6.038087908 10.199.95.28 172.64.41.4 TLSv1.2 148 Application Data
510 6.039320878 172.64.41.4 10.199.95.28 TCP 66 443 → 44070 [ACK] Seq=1 Ack=139 Win=8 Len=0 TSv
511 6.042831444 172.64.41.4 10.199.95.28 TLSv1.2 148 Application Data
512 6.042842069 10.199.95.28 172.64.41.4 TCP 66 44070 → 443 [ACK] Seq=139 Ack=83 Win=443 Len=0
513 6.042866550 172.64.41.4 10.199.95.28 TLSv1.2 236 Application Data
514 6.042870056 10.199.95.28 172.64.41.4 TCP 66 44070 → 443 [ACK] Seq=139 Ack=253 Win=443 Len=0
515 6.043240705 10.199.95.28 142.251.163.147 TCP 74 47472 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
516 6.045903814 142.251.163.147 10.199.95.28 TCP 74 443 → 47472 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
517 6.045926371 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 T
518 6.047316764 10.199.95.28 142.251.163.147 TLSv1.3 583 Client Hello
520 6.049289468 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=1 Ack=518 Win=66816 Len=0
522 6.049853810 142.251.163.147 10.199.95.28 TLSv1.3 4354 Server Hello, Change Cipher Spec, Application D
523 6.049866461 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=518 Ack=4289 Win=58624 Le
Frame 518: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 142.251.163.147
Transmission Control Protocol, Src Port: 47472, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 02 39 7c ab 40 00 40 06 1f a2 0a c7 5f 1c 8e fb
0020 a3 93 b9 70 01 bb 12 e6 b9 8e db c0 9d 55 80 18
0030 01 eb 9e 9d 00 00 01 01 08 0a 06 1f be 9f be 88
0040 44 49 16 03 01 02 00 01 00 01 fc 03 03 5d b1 ff
0050 97 8f a7 c5 bd ef 89 b7 2d 99 b3 26 e3 d8 e2 46
0060 02 e6 74 86 88 a8 01 5a 28 9f e0 56 9a 20 b7 68
0070 67 fe 8d 34 f9 b6 a5 2e e5 12 ab 5e 84 67 3f 21
0080 67 69 4f c3 49 d1 79 7a d4 fc 9b 7b d1 6b 00 24
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c
00a0 c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f
00b0 00 35 00 0a 01 00 01 8f 00 00 00 13 00 11 00 00
00c0 0e 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 00
Google - Mozilla Firefox
*ens5

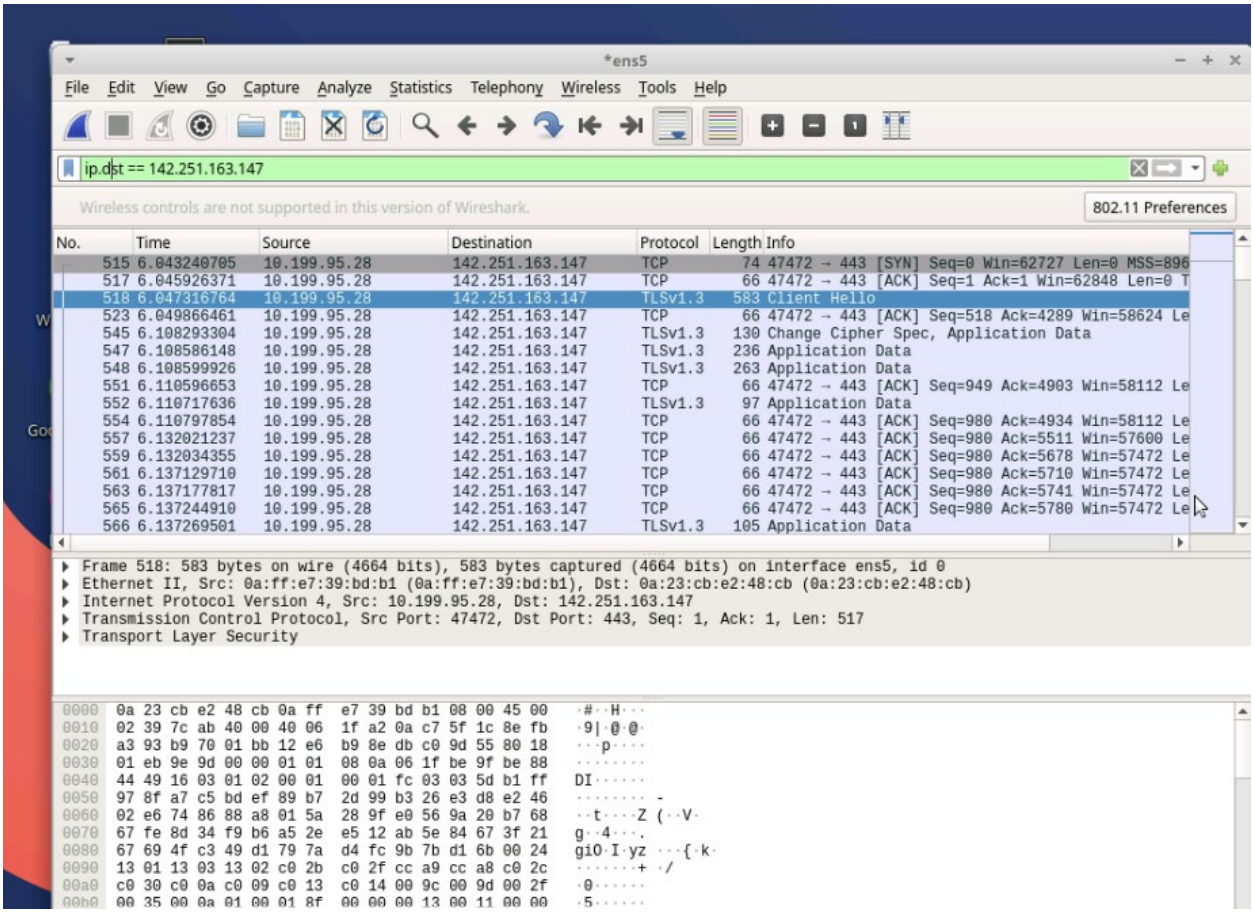

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
48 0.381740336 10.199.95.28 18.211.136.205 TCP 74 33636 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
247 2.397766191 10.199.95.28 18.211.136.205 TCP 74 [TCP Retransmission] [TCP Port numbers reused]
508 6.038067713 10.199.95.28 172.64.41.4 TLSv1.2 122 Application Data
509 6.038087908 10.199.95.28 172.64.41.4 TLSv1.2 148 Application Data
510 6.039320878 172.64.41.4 10.199.95.28 TCP 66 443 → 44070 [ACK] Seq=1 Ack=139 Win=8 Len=0 TSv
511 6.042831444 172.64.41.4 10.199.95.28 TLSv1.2 148 Application Data
512 6.042842069 10.199.95.28 172.64.41.4 TCP 66 44070 → 443 [ACK] Seq=139 Ack=83 Win=443 Len=0
513 6.042866550 172.64.41.4 10.199.95.28 TLSv1.2 236 Application Data
514 6.042870056 10.199.95.28 172.64.41.4 TCP 66 44070 → 443 [ACK] Seq=139 Ack=253 Win=443 Len=0
515 6.043240705 10.199.95.28 142.251.163.147 TCP 74 47472 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
516 6.045903814 142.251.163.147 10.199.95.28 TCP 74 443 → 47472 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
517 6.045926371 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 T
518 6.047316764 10.199.95.28 142.251.163.147 TLSv1.3 583 Client Hello
520 6.049289468 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=1 Ack=518 Win=66816 Len=0
522 6.049853810 142.251.163.147 10.199.95.28 TLSv1.3 4354 Server Hello, Change Cipher Spec, Application D
523 6.049866461
Frame 518: 583 bytes on wire
Ethernet II, Src: 0a:ff:e7:3
Internet Protocol Version 4,
Transmission Control Protocc
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a ff
0010 02 39 7c ab 40 00 40 06
0020 a3 93 b9 70 01 bb 12 e6
0030 01 eb 9e 9d 00 00 01 01
0040 44 49 16 03 01 02 00 01
0050 97 8f a7 c5 bd ef 89 b7
0060 02 e6 74 86 88 a8 01 5a
0070 67 fe 8d 34 f9 b6 a5 2e
0080 67 69 4f c3 49 d1 79 7a
0090 13 01 13 03 13 02 c0 2b
00a0 c0 30 c0 0a c0 09 c0 13
00b0 00 35 00 0a 01 00 01 8f
00c0 0e 77 77 77 2e 67 6f 6f
Google - Mozilla Firefox
Google
142.251.163.147
About Store
http://142.251.163.147/ — Visit
This time, search with:


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
48 0.381740336 10.199.95.28 18.211.136.205 TCP 74 33636 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
247 2.397766191 10.199.95.28 18.211.136.205 TCP 74 [TCP Retransmission] [TCP Port numbers reused]
508 6.038067713 10.199.95.28 172.64.41.4 TLSv1.2 122 Application Data
509 6.038087908
510 6.039320878
511 6.042831444
512 6.042842069
513 6.042866550
514 6.042870056
515 6.043240705
516 6.045903814
517 6.045926371
518 6.047316764
520 6.049289468
522 6.049853810
523 6.049866461
Frame 518: 583 bytes on
Ethernet II, Src: 0a:ff:
Internet Protocol Versio
Transmission Control Pro
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a
0010 02 39 7c ab 40 00 40
0020 a3 93 b9 70 01 bb 12
0030 01 eb 9e 9d 00 00 01
0040 44 49 16 03 01 02 00
0050 97 8f a7 c5 bd ef 89
0060 02 e6 74 86 88 a8 01
0070 67 fe 8d 34 f9 b6 a5
0080 67 69 4f c3 49 d1 79
0090 13 01 13 03 13 02 c0
00a0 c0 30 c0 0a c0 09 c0
00b0 00 35 00 0a 01 00 01
00c0 0e 77 77 77 2e 67 6f
Google - Mozilla Firefox
Google
https://www.google.com
About Store
Gmail Images
Google
Google Search
I'm Feeling Lucky
New! Learn more about the Google AI Essentials course, zero experience required


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls.handshake.type == 1
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
518 6.047316764 10.199.95.28 142.251.163.147 TLSv1.3 583 Client Hello
671 8.369848917 10.199.95.28 142.251.163.147 TLSv1.3 583 Client Hello
769 8.590802040 10.199.95.28 34.120.208.123 TLSv1.2 583 Client Hello
969 8.859356519 10.199.95.28 142.251.163.94 TLSv1.3 583 Client Hello
970 8.860588472 10.199.95.28 142.251.163.94 TLSv1.3 583 Client Hello
1228 9.441165388 10.199.95.28 142.251.167.139 TLSv1.3 583 Client Hello
1250 9.473365521 10.199.95.28 172.253.115.138 TLSv1.3 583 Client Hello
1534 9.909691022 10.199.95.28 172.253.62.94 TLSv1.3 583 Client Hello
1536 9.911620026 10.199.95.28 172.253.62.94 TLSv1.3 583 Client Hello
1788 10.269380455 10.199.95.28 142.251.16.102 TLSv1.3 583 Client Hello
1791 10.271047522 10.199.95.28 142.251.16.102 TLSv1.3 583 Client Hello
Frame 518: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 142.251.163.147
Transmission Control Protocol, Src Port: 47472, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 02 39 7c ab 40 00 40 06 1f a2 0a c7 5f 1c 8e fb
0020 a3 93 b9 70 01 bb 12 e6 b9 8e db c0 9d 55 80 18
0030 01 eb 9e 9d 00 00 01 01 08 0a 06 1f be 9f be 88
0040 44 49 16 03 01 02 00 01 00 01 fc 03 03 5d b1 ff
0050 97 8f a7 c5 bd ef 89 b7 2d 99 b3 26 e3 d8 e2 46
0060 02 e6 74 86 88 a8 01 5a 28 9f e0 56 9a 20 b7 68
0070 67 fe 8d 34 f9 b6 a5 2e e5 12 ab 5e 84 67 3f 21
0080 67 69 4f c3 49 d1 79 7a d4 fc 9b 7b d1 6b 00 24
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c
00a0 c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f
00b0 00 35 00 0a 01 00 01 8f 00 00 00 13 00 11 00 00
00c0 0e 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 00


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 142.251.163.147
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
515 6.043240705 10.199.95.28 142.251.163.147 TCP 74 47472 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
516 6.045903814 142.251.163.147 10.199.95.28 TCP 74 443 → 47472 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
517 6.045926371 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 T
518 6.047316764 10.199.95.28 142.251.163.147 TLSv1.3 583 Client Hello
520 6.049289468 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=1 Ack=518 Win=66816 Len=0
522 6.049853810 142.251.163.147 10.199.95.28 TLSv1.3 4354 Server Hello, Change Cipher Spec, Application D
523 6.049866461 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=518 Ack=4289 Win=58624 Le
545 6.108293304 10.199.95.28 142.251.163.147 TLSv1.3 130 Change Cipher Spec, Application Data
547 6.108586148 10.199.95.28 142.251.163.147 TLSv1.3 236 Application Data
548 6.108599926 10.199.95.28 142.251.163.147 TLSv1.3 263 Application Data
550 6.110582073 142.251.163.147 10.199.95.28 TLSv1.3 680 Application Data, Application Data
551 6.110596653 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=949 Ack=4903 Win=58112 Le
552 6.110717636 10.199.95.28 142.251.163.147 TLSv1.3 97 Application Data
553 6.110794650 142.251.163.147 10.199.95.28 TLSv1.3 97 Application Data
554 6.110797854 10.199.95.28 142.251.163.147 TCP 66 47472 → 443 [ACK] Seq=980 Ack=4934 Win=58112 Le
555 6.117867624 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=4934 Ack=980 Win=68864 Le
Frame 515: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 142.251.163.147
Transmission Control Protocol, Src Port: 47472, Dst Port: 443, Seq: 0, Len: 0
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 00 3c 7c a9 40 00 40 06 21 a1 0a c7 5f 1c 8e fb
0020 a3 93 b9 70 01 bb 12 e6 b9 8d 00 00 00 00 a0 02
0030 f5 07 9c a0 00 00 02 04 23 01 04 02 08 0a 06 1f
0040 be 9b 00 00 00 00 01 03 03 07


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 142.251.163.147
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
516 6.045903814 142.251.163.147 10.199.95.28 TCP 74 443 → 47472 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
520 6.049289468 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=1 Ack=518 Win=66816 Len=0
522 6.049853810 142.251.163.147 10.199.95.28 TLSv1.3 4354 Server Hello, Change Cipher Spec, Application D
550 6.110582073 142.251.163.147 10.199.95.28 TLSv1.3 680 Application Data, Application Data
553 6.110794650 142.251.163.147 10.199.95.28 TLSv1.3 97 Application Data
555 6.117867624 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=4934 Ack=980 Win=68864 Le
556 6.132006822 142.251.163.147 10.199.95.28 TLSv1.3 643 Application Data
558 6.132030607 142.251.163.147 10.199.95.28 TLSv1.3 233 Application Data
560 6.137116500 142.251.163.147 10.199.95.28 TLSv1.3 98 Application Data
562 6.137175354 142.251.163.147 10.199.95.28 TLSv1.3 97 Application Data
564 6.137242078 142.251.163.147 10.199.95.28 TLSv1.3 105 Application Data
569 6.144891619 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=5780 Ack=1019 Win=68864 L
583 6.242477270 142.251.163.147 10.199.95.28 TCP 66 443 → 47472 [ACK] Seq=5780 Ack=1106 Win=68864 L
589 6.265186467 142.251.163.147 10.199.95.28 TLSv1.3 294 Application Data
591 6.265221987 142.251.163.147 10.199.95.28 TLSv1.3 244 Application Data
593 6.268610635 142.251.163.147 10.199.95.28 TLSv1.3 98 Application Data
Frame 522: 4354 bytes on wire (34832 bits), 4354 bytes captured (34832 bits) on interface ens5, id 0
Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb), Dst: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1)
Internet Protocol Version 4, Src: 142.251.163.147, Dst: 10.199.95.28
Transmission Control Protocol, Src Port: 443, Dst Port: 47472, Seq: 1, Ack: 518, Len: 4288
Transport Layer Security
0000 0a ff e7 39 bd b1 0a 23 cb e2 48 cb 08 00 45 00
0010 10 f4 8e 71 00 00 78 06 07 21 8e fb a3 93 0a c7
0020 5f 1c 01 bb b9 70 db c0 9d 55 12 e6 bb 93 80 18
0030 01 05 ad 58 00 00 01 01 08 0a be 88 44 4d 06 1f
0040 be 9f 16 03 03 00 7a 02 00 00 76 03 03 7d 1a d6
0050 e8 4d 80 d8 56 54 d5 a3 00 17 5e ec 6f 78 53 38
0060 b7 b2 16 d4 63 fe 45 fa a1 89 d3 07 e4 20 b7 68
0070 67 fe 8d 34 f9 b6 a5 2e e5 12 ab 5e 84 67 3f 21
0080 67 69 4f c3 49 d1 79 7a d4 fc 9b 7b d1 6b 13 01
0090 00 00 2e 00 33 00 24 00 1d 00 20 14 e3 65 70 37
00a0 a0 81 f3 f6 5c 94 f0 a8 02 fd aa d8 60 dd ee 5a
00b0 35 4e 12 a6 e5 10 42 3f 8f b2 45 00 2b 00 02 03

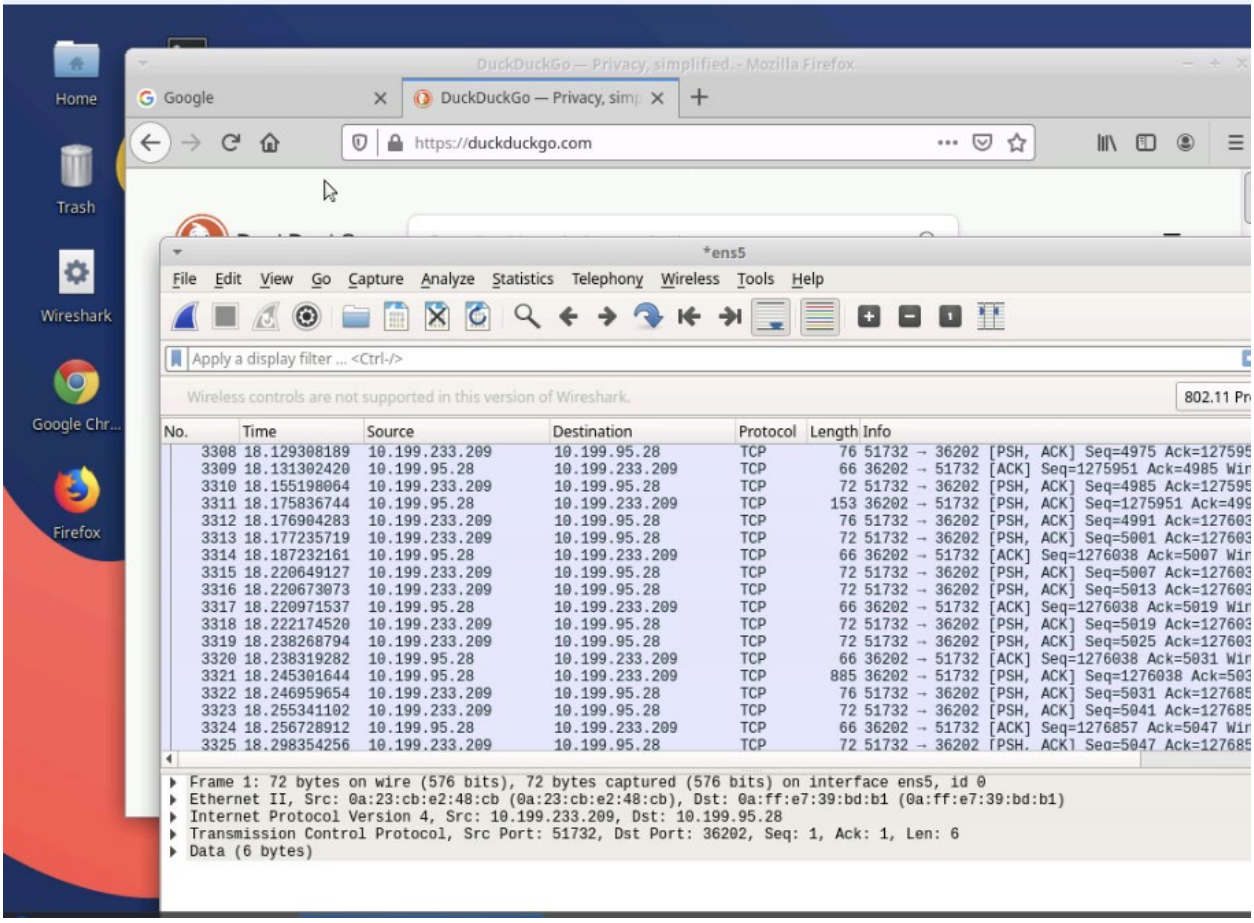


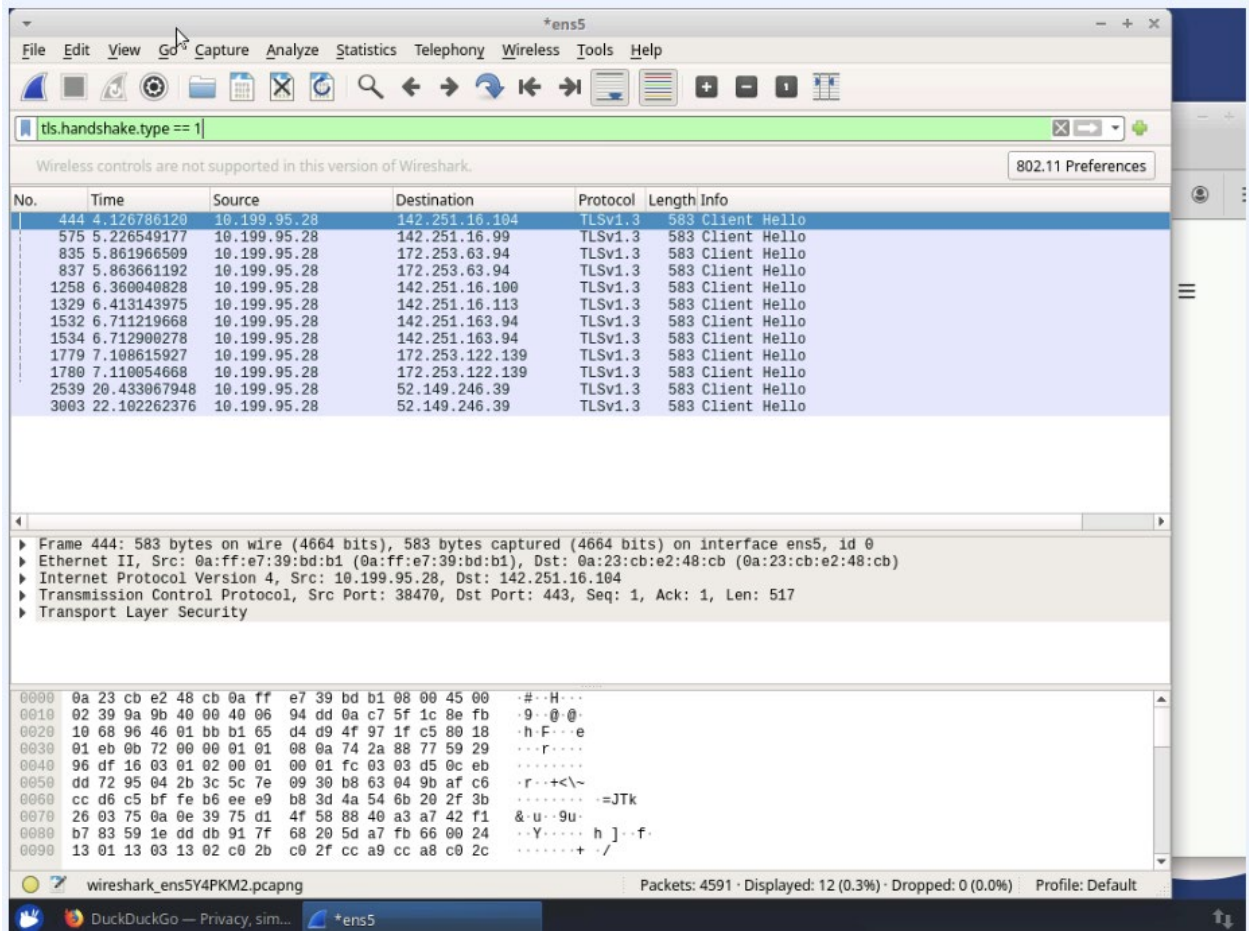
Task 5

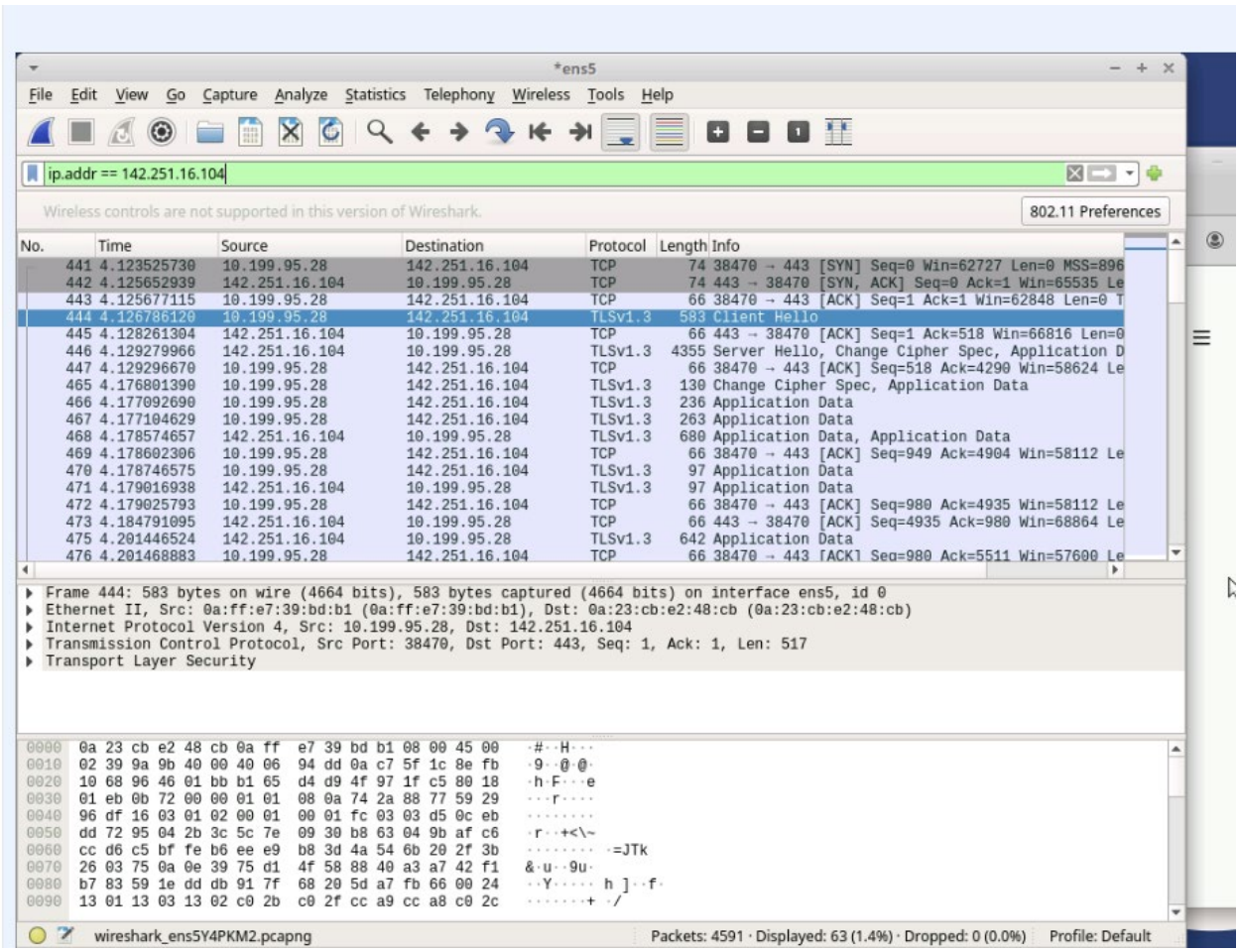
Locate all HTTPS packets from a capture not containing a certain IP address:

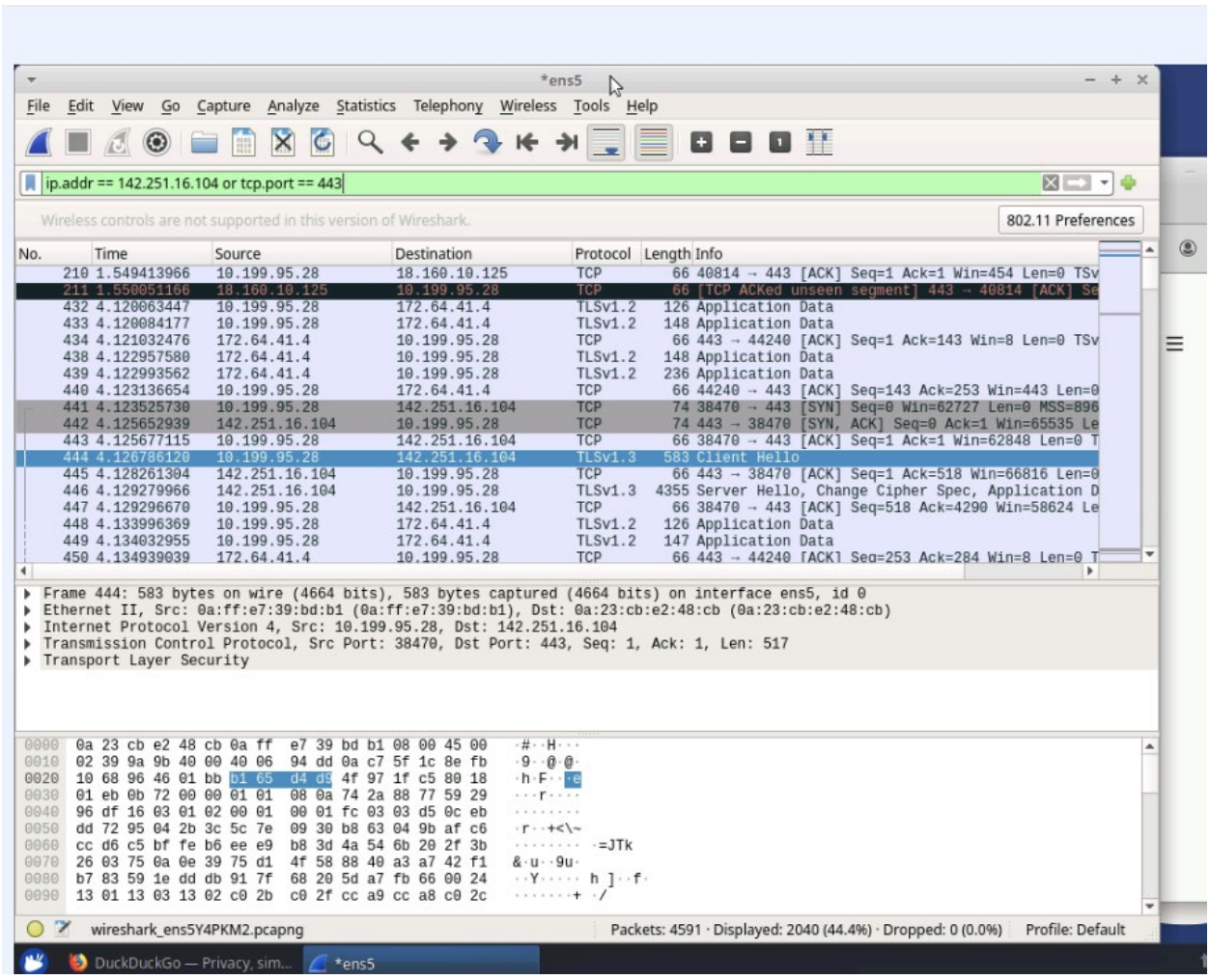
●A Conditional statement may be used to include and eliminate packets from a Wireshark capture: !(ip.addr == 8.43.85.97) and tcp.port == 443

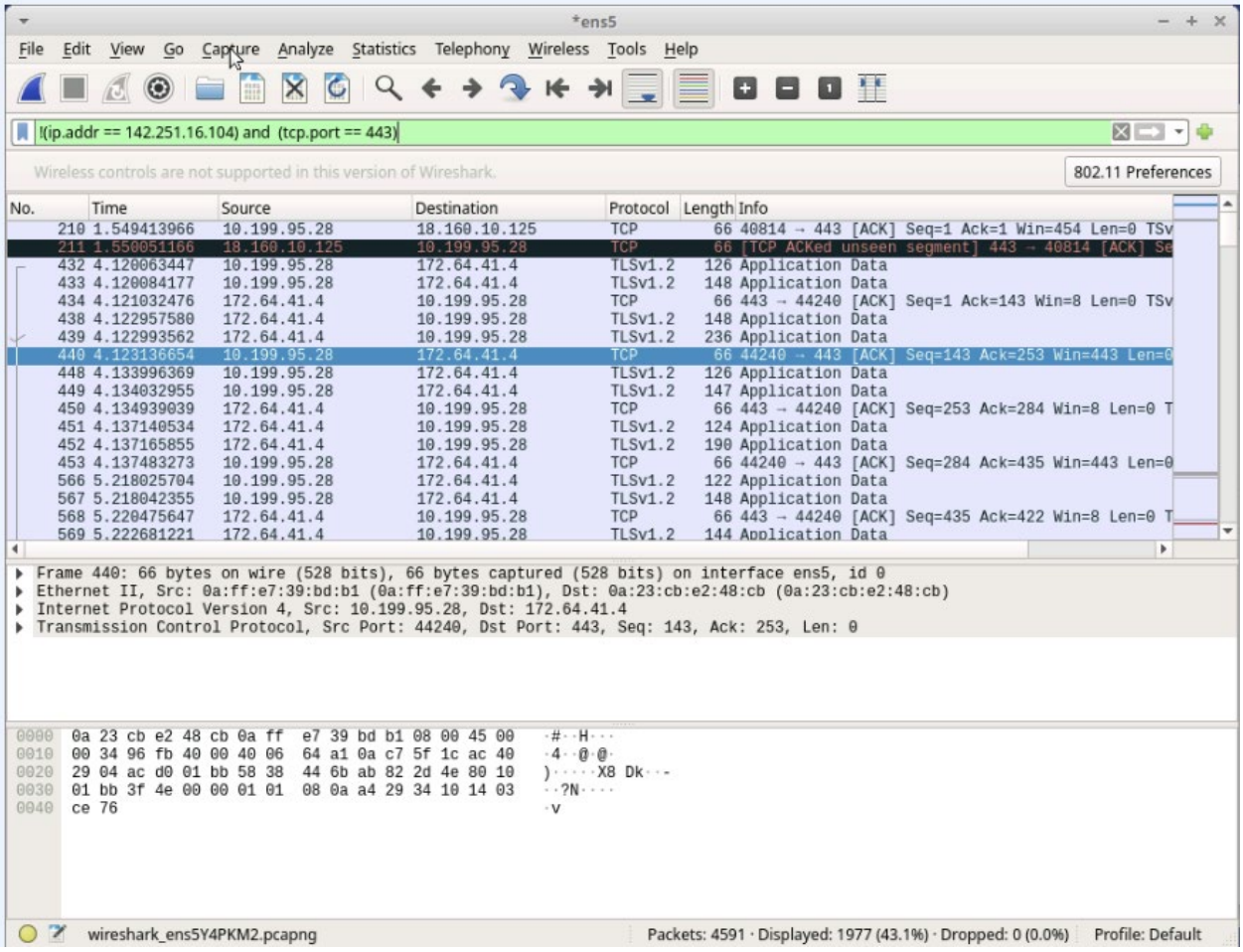
●A compound conditional should include parentheses to avoid order of execution errors: !(ip.addr == 8.43.85.97) and (tcp.port == 80 or tcp.port == 443)

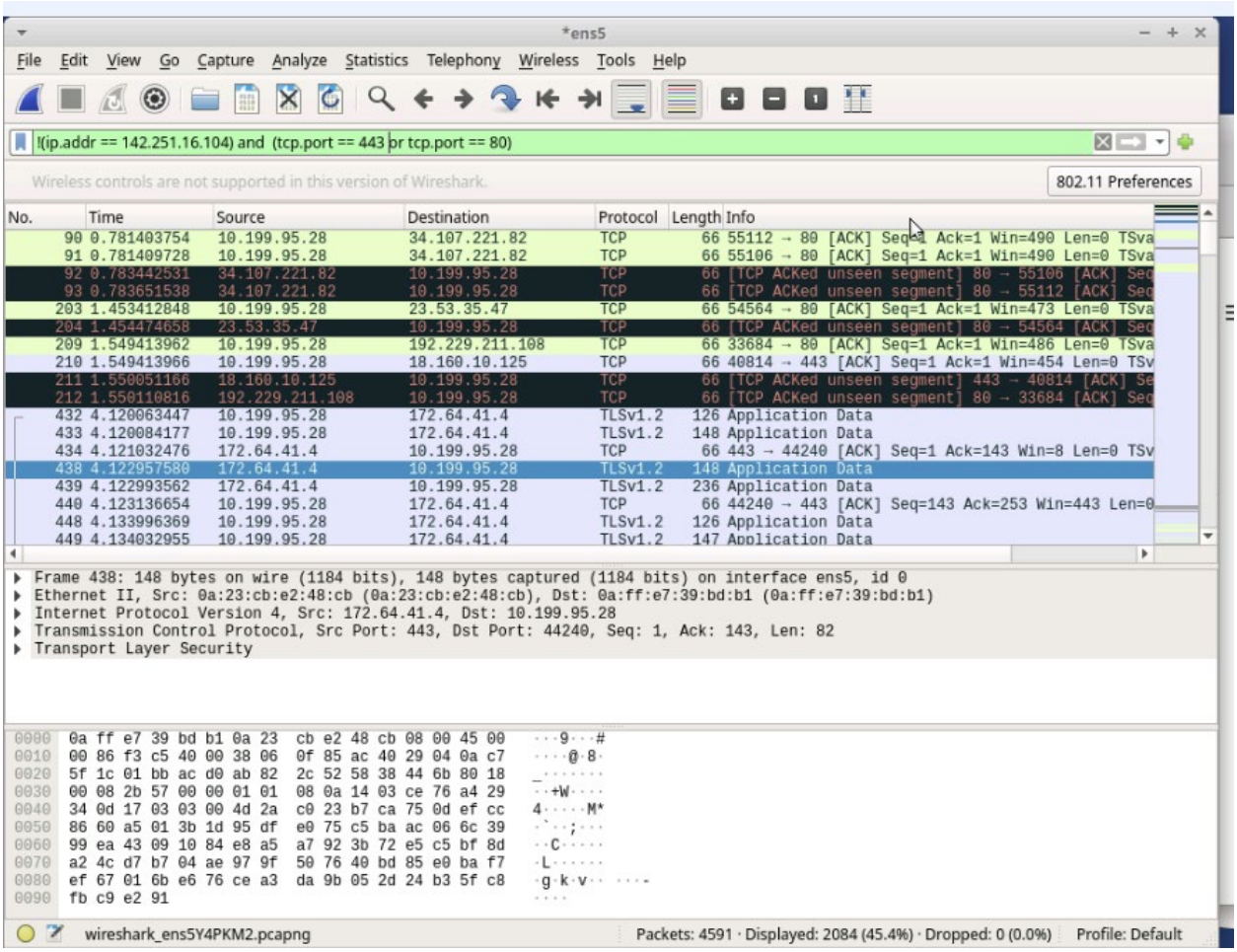

Home
Trash
Wireshark
Google Chr...
Firefox
DuckDuckGo — Privacy, simplified. - Mozilla Firefox
Google
DuckDuckGo — Privacy, simp
https://duckduckgo.com
*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireless controls are not supported in this version of Wireshark.
802.11 Pr
No. Time Source Destination Protocol Length Info
3308 18.129308189 10.199.233.209 10.199.95.28 TCP 76 51732 → 36202 [PSH, ACK] Seq=4975 Ack=127595
3309 18.131302420 10.199.95.28 10.199.233.209 TCP 66 36202 → 51732 [ACK] Seq=1275951 Ack=4985 Wir
3310 18.155198064 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=4985 Ack=127595
3311 18.175836744 10.199.95.28 10.199.233.209 TCP 153 36202 → 51732 [PSH, ACK] Seq=1275951 Ack=499
3312 18.176904283 10.199.233.209 10.199.95.28 TCP 76 51732 → 36202 [PSH, ACK] Seq=4991 Ack=127603
3313 18.177235719 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5001 Ack=127603
3314 18.187232161 10.199.95.28 10.199.233.209 TCP 66 36202 → 51732 [ACK] Seq=1276038 Ack=5007 Wir
3315 18.220649127 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5007 Ack=127603
3316 18.220673073 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5013 Ack=127603
3317 18.220971537 10.199.95.28 10.199.233.209 TCP 66 36202 → 51732 [ACK] Seq=1276038 Ack=5019 Wir
3318 18.222174520 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5019 Ack=127603
3319 18.238268794 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5025 Ack=127603
3320 18.238319282 10.199.95.28 10.199.233.209 TCP 66 36202 → 51732 [ACK] Seq=1276038 Ack=5031 Wir
3321 18.245301644 10.199.95.28 10.199.233.209 TCP 885 36202 → 51732 [PSH, ACK] Seq=1276038 Ack=503
3322 18.246959654 10.199.233.209 10.199.95.28 TCP 76 51732 → 36202 [PSH, ACK] Seq=5031 Ack=127685
3323 18.255341102 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5041 Ack=127685
3324 18.256728912 10.199.95.28 10.199.233.209 TCP 66 36202 → 51732 [ACK] Seq=1276857 Ack=5047 Wir
3325 18.298354256 10.199.233.209 10.199.95.28 TCP 72 51732 → 36202 [PSH, ACK] Seq=5047 Ack=127685
Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface ens5, id 0
Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb), Dst: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1)
Internet Protocol Version 4, Src: 10.199.233.209, Dst: 10.199.95.28
Transmission Control Protocol, Src Port: 51732, Dst Port: 36202, Seq: 1, Ack: 1, Len: 6
Data (6 bytes)


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls.handshake.type == 1
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
444 4.126786120 10.199.95.28 142.251.16.104 TLSv1.3 583 Client Hello
575 5.226549177 10.199.95.28 142.251.16.99 TLSv1.3 583 Client Hello
835 5.861966509 10.199.95.28 172.253.63.94 TLSv1.3 583 Client Hello
837 5.863661192 10.199.95.28 172.253.63.94 TLSv1.3 583 Client Hello
1258 6.360040828 10.199.95.28 142.251.16.100 TLSv1.3 583 Client Hello
1329 6.413143975 10.199.95.28 142.251.16.113 TLSv1.3 583 Client Hello
1532 6.711219668 10.199.95.28 142.251.163.94 TLSv1.3 583 Client Hello
1534 6.712900278 10.199.95.28 142.251.163.94 TLSv1.3 583 Client Hello
1779 7.108615927 10.199.95.28 172.253.122.139 TLSv1.3 583 Client Hello
1780 7.110054668 10.199.95.28 172.253.122.139 TLSv1.3 583 Client Hello
2539 20.433067948 10.199.95.28 52.149.246.39 TLSv1.3 583 Client Hello
3003 22.102262376 10.199.95.28 52.149.246.39 TLSv1.3 583 Client Hello
Frame 444: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 142.251.16.104
Transmission Control Protocol, Src Port: 38470, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 02 39 9a 9b 40 00 40 06 94 dd 0a c7 5f 1c 8e fb
0020 10 68 96 46 01 bb b1 65 d4 d9 4f 97 1f c5 80 18
0030 01 eb 0b 72 00 00 01 01 08 0a 74 2a 88 77 59 29
0040 96 df 16 03 01 02 00 01 00 01 fc 03 03 d5 0c eb
0050 dd 72 95 04 2b 3c 5c 7e 09 30 b8 63 04 9b af c6
0060 cc d6 c5 bf fe b6 ee e9 b8 3d 4a 54 6b 20 2f 3b
0070 26 03 75 0a 0e 39 75 d1 4f 58 88 40 a3 a7 42 f1
0080 b7 83 59 1e dd db 91 7f 68 20 5d a7 fb 66 00 24
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c
wireshark_ens5Y4PKM2.pcapng
Packets: 4591 · Displayed: 12 (0.3%) · Dropped: 0 (0.0%)
Profile: Default
DuckDuckGo — Privacy, sim...
*ens5


*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 142.251.16.104
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
441 4.123525730 10.199.95.28 142.251.16.104 TCP 74 38470 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
442 4.125652939 142.251.16.104 10.199.95.28 TCP 74 443 → 38470 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
443 4.125677115 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 T
444 4.126786120 10.199.95.28 142.251.16.104 TLSv1.3 583 Client Hello
445 4.128261304 142.251.16.104 10.199.95.28 TCP 66 443 → 38470 [ACK] Seq=1 Ack=518 Win=66816 Len=0
446 4.129279966 142.251.16.104 10.199.95.28 TLSv1.3 4355 Server Hello, Change Cipher Spec, Application D
447 4.129296670 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=518 Ack=4290 Win=58624 Le
465 4.176801390 10.199.95.28 142.251.16.104 TLSv1.3 130 Change Cipher Spec, Application Data
466 4.177092690 10.199.95.28 142.251.16.104 TLSv1.3 236 Application Data
467 4.177104629 10.199.95.28 142.251.16.104 TLSv1.3 263 Application Data
468 4.178574657 142.251.16.104 10.199.95.28 TLSv1.3 680 Application Data, Application Data
469 4.178602306 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=949 Ack=4904 Win=58112 Le
470 4.178746575 10.199.95.28 142.251.16.104 TLSv1.3 97 Application Data
471 4.179016938 142.251.16.104 10.199.95.28 TLSv1.3 97 Application Data
472 4.179025793 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=980 Ack=4935 Win=58112 Le
473 4.184791095 142.251.16.104 10.199.95.28 TCP 66 443 → 38470 [ACK] Seq=4935 Ack=980 Win=68864 Le
475 4.201446524 142.251.16.104 10.199.95.28 TLSv1.3 642 Application Data
476 4.201468883 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=980 Ack=5511 Win=57600 Le
Frame 444: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 142.251.16.104
Transmission Control Protocol, Src Port: 38470, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 02 39 9a 9b 40 00 40 06 94 dd 0a c7 5f 1c 8e fb
0020 10 68 96 46 01 bb b1 65 d4 d9 4f 97 1f c5 80 18
0030 01 eb 0b 72 00 00 01 01 08 0a 74 2a 88 77 59 29
0040 96 df 16 03 01 02 00 01 00 01 fc 03 03 d5 0c eb
0050 dd 72 95 04 2b 3c 5c 7e 09 30 b8 63 04 9b af c6
0060 cc d6 c5 bf fe b6 ee e9 b8 3d 4a 54 6b 20 2f 3b
0070 26 03 75 0a 0e 39 75 d1 4f 58 88 40 a3 a7 42 f1
0080 b7 83 59 1e dd db 91 7f 68 20 5d a7 fb 66 00 24
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c
wireshark_ens5Y4PKM2.pcapng
Packets: 4591 · Displayed: 63 (1.4%) · Dropped: 0 (0.0%)
Profile: Default

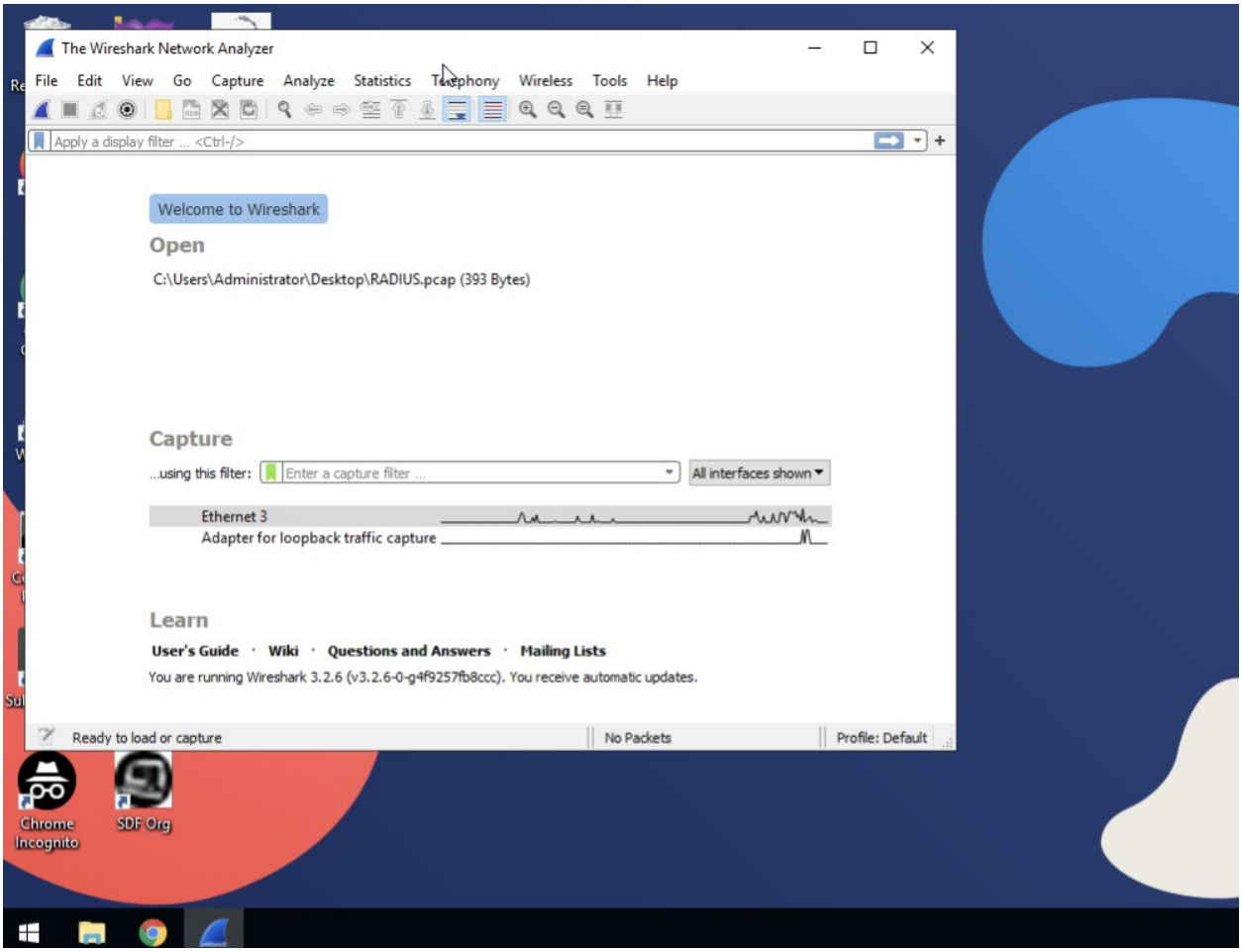

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 142.251.16.104 or tcp.port == 443
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
210 1.549413966 10.199.95.28 18.160.10.125 TCP 66 40814 → 443 [ACK] Seq=1 Ack=1 Win=454 Len=0 TSv
211 1.550051166 18.160.10.125 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 443 → 40814 [ACK] Se
432 4.120063447 10.199.95.28 172.64.41.4 TLSv1.2 126 Application Data
433 4.120084177 10.199.95.28 172.64.41.4 TLSv1.2 148 Application Data
434 4.121032476 172.64.41.4 10.199.95.28 TCP 66 443 → 44240 [ACK] Seq=1 Ack=143 Win=8 Len=0 TSv
438 4.122957580 172.64.41.4 10.199.95.28 TLSv1.2 148 Application Data
439 4.122993562 172.64.41.4 10.199.95.28 TLSv1.2 236 Application Data
440 4.123136654 10.199.95.28 172.64.41.4 TCP 66 44240 → 443 [ACK] Seq=143 Ack=253 Win=443 Len=0
441 4.123525730 10.199.95.28 142.251.16.104 TCP 74 38470 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=896
442 4.125652939 142.251.16.104 10.199.95.28 TCP 74 443 → 38470 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
443 4.125677115 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=1 Ack=1 Win=62848 Len=0 T
444 4.126786120 10.199.95.28 142.251.16.104 TLSv1.3 583 Client Hello
445 4.128261304 142.251.16.104 10.199.95.28 TCP 66 443 → 38470 [ACK] Seq=1 Ack=518 Win=66816 Len=0
446 4.129279966 142.251.16.104 10.199.95.28 TLSv1.3 4355 Server Hello, Change Cipher Spec, Application D
447 4.129296670 10.199.95.28 142.251.16.104 TCP 66 38470 → 443 [ACK] Seq=518 Ack=4290 Win=58624 Le
448 4.133996369 10.199.95.28 172.64.41.4 TLSv1.2 126 Application Data
449 4.134032955 10.199.95.28 172.64.41.4 TLSv1.2 147 Application Data
450 4.134939039 172.64.41.4 10.199.95.28 TCP 66 443 → 44240 [ACK] Seq=253 Ack=284 Win=8 Len=0 T
Frame 444: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 142.251.16.104
Transmission Control Protocol, Src Port: 38470, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 02 39 9a 9b 40 00 40 06 94 dd 0a c7 5f 1c 8e fb
0020 10 68 96 46 01 bb b1 65 d4 d9 4f 97 1f c5 80 18
0030 01 eb 0b 72 00 00 01 01 08 0a 74 2a 88 77 59 29
0040 96 df 16 03 01 02 00 01 00 01 fc 03 03 d5 0c eb
0050 dd 72 95 04 2b 3c 5c 7e 09 30 b8 63 04 9b af c6
0060 cc d6 c5 bf fe b6 ee e9 b8 3d 4a 54 6b 20 2f 3b
0070 26 03 75 0a 0e 39 75 d1 4f 58 88 40 a3 a7 42 f1
0080 b7 83 59 1e dd db 91 7f 68 20 5d a7 fb 66 00 24
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c
wireshark_ens5Y4PKM2.pcapng
Packets: 4591 · Displayed: 2040 (44.4%) · Dropped: 0 (0.0%)
Profile: Default
DuckDuckGo — Privacy, sim...
*ens5

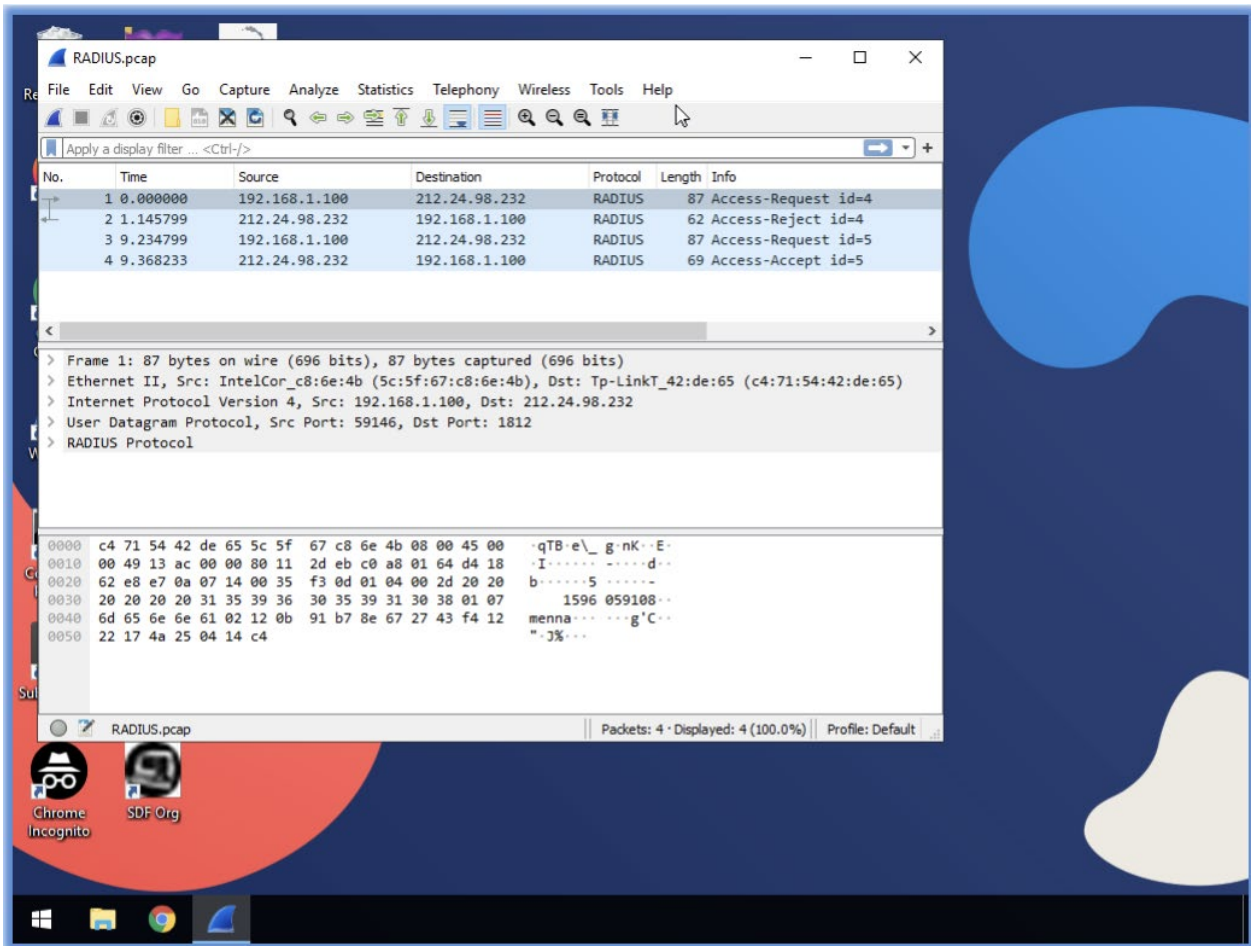

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!(ip.addr == 142.251.16.104) and (tcp.port == 443)
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
210 1.549413966 10.199.95.28 18.160.10.125 TCP 66 40814 → 443 [ACK] Seq=1 Ack=1 Win=454 Len=0 TSv
211 1.550051166 18.160.10.125 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 443 → 40814 [ACK] Se
432 4.120063447 10.199.95.28 172.64.41.4 TLSv1.2 126 Application Data
433 4.120084177 10.199.95.28 172.64.41.4 TLSv1.2 148 Application Data
434 4.121032476 172.64.41.4 10.199.95.28 TCP 66 443 → 44240 [ACK] Seq=1 Ack=143 Win=8 Len=0 TSv
438 4.122957580 172.64.41.4 10.199.95.28 TLSv1.2 148 Application Data
439 4.122993562 172.64.41.4 10.199.95.28 TLSv1.2 236 Application Data
440 4.123136654 10.199.95.28 172.64.41.4 TCP 66 44240 → 443 [ACK] Seq=143 Ack=253 Win=443 Len=0
448 4.133996369 10.199.95.28 172.64.41.4 TLSv1.2 126 Application Data
449 4.134032955 10.199.95.28 172.64.41.4 TLSv1.2 147 Application Data
450 4.134939039 172.64.41.4 10.199.95.28 TCP 66 443 → 44240 [ACK] Seq=253 Ack=284 Win=8 Len=0 T
451 4.137140534 172.64.41.4 10.199.95.28 TLSv1.2 124 Application Data
452 4.137165855 172.64.41.4 10.199.95.28 TLSv1.2 190 Application Data
453 4.137483273 10.199.95.28 172.64.41.4 TCP 66 44240 → 443 [ACK] Seq=284 Ack=435 Win=443 Len=0
566 5.218025704 10.199.95.28 172.64.41.4 TLSv1.2 122 Application Data
567 5.218042355 10.199.95.28 172.64.41.4 TLSv1.2 148 Application Data
568 5.220475647 172.64.41.4 10.199.95.28 TCP 66 443 → 44240 [ACK] Seq=435 Ack=422 Win=8 Len=0 T
569 5.222681221 172.64.41.4 10.199.95.28 TLSv1.2 144 Application Data
Frame 440: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens5, id 0
Ethernet II, Src: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.95.28, Dst: 172.64.41.4
Transmission Control Protocol, Src Port: 44240, Dst Port: 443, Seq: 143, Ack: 253, Len: 0
0000 0a 23 cb e2 48 cb 0a ff e7 39 bd b1 08 00 45 00
0010 00 34 96 fb 40 00 40 06 64 a1 0a c7 5f 1c ac 40
0020 29 04 ac d0 01 bb 58 38 44 6b ab 82 2d 4e 80 10
0030 01 bb 3f 4e 00 00 01 01 08 0a a4 29 34 10 14 03
0040 ce 76
wireshark_ens5Y4PKM2.pcapng
Packets: 4591 · Displayed: 1977 (43.1%) · Dropped: 0 (0.0%)
Profile: Default

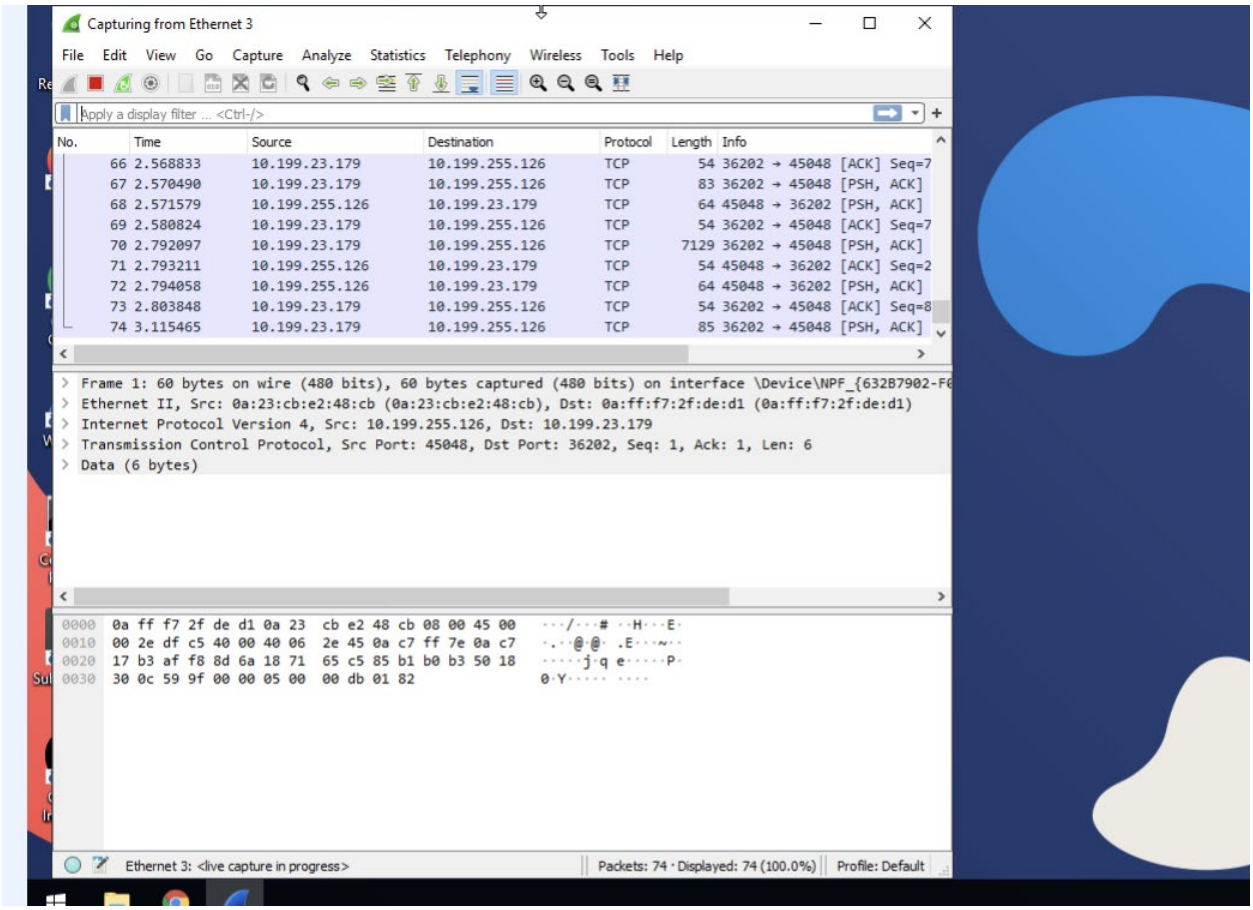

*ens5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!(ip.addr == 142.251.16.104) and (tcp.port == 443 or tcp.port == 80)
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences
No. Time Source Destination Protocol Length Info
90 0.781403754 10.199.95.28 34.107.221.82 TCP 66 55112 → 80 [ACK] Seq=1 Ack=1 Win=490 Len=0 TSva
91 0.781409728 10.199.95.28 34.107.221.82 TCP 66 55106 → 80 [ACK] Seq=1 Ack=1 Win=490 Len=0 TSva
92 0.783442531 34.107.221.82 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 80 → 55106 [ACK] Seq
93 0.783651538 34.107.221.82 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 80 → 55112 [ACK] Seq
203 1.453412848 10.199.95.28 23.53.35.47 TCP 66 54564 → 80 [ACK] Seq=1 Ack=1 Win=473 Len=0 TSva
204 1.454474658 23.53.35.47 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 80 → 54564 [ACK] Seq
209 1.549413962 10.199.95.28 192.229.211.108 TCP 66 33684 → 80 [ACK] Seq=1 Ack=1 Win=486 Len=0 TSva
210 1.549413966 10.199.95.28 18.160.10.125 TCP 66 40814 → 443 [ACK] Seq=1 Ack=1 Win=454 Len=0 TSv
211 1.550051166 18.160.10.125 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 443 → 40814 [ACK] Se
212 1.550110816 192.229.211.108 10.199.95.28 TCP 66 [TCP ACKed unseen segment] 80 → 33684 [ACK] Seq
432 4.120063447 10.199.95.28 172.64.41.4 TLSv1.2 126 Application Data
433 4.120084177 10.199.95.28 172.64.41.4 TLSv1.2 148 Application Data
434 4.121032476 172.64.41.4 10.199.95.28 TCP 66 443 → 44240 [ACK] Seq=1 Ack=143 Win=8 Len=0 TSv
438 4.122957580 172.64.41.4 10.199.95.28 TLSv1.2 148 Application Data
439 4.122993562 172.64.41.4 10.199.95.28 TLSv1.2 236 Application Data
440 4.123136654 10.199.95.28 172.64.41.4 TCP 66 44240 → 443 [ACK] Seq=143 Ack=253 Win=443 Len=0
448 4.133996369 10.199.95.28 172.64.41.4 TLSv1.2 126 Application Data
449 4.134032955 10.199.95.28 172.64.41.4 TLSv1.2 147 Application Data
Frame 438: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface ens5, id 0
Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb), Dst: 0a:ff:e7:39:bd:b1 (0a:ff:e7:39:bd:b1)
Internet Protocol Version 4, Src: 172.64.41.4, Dst: 10.199.95.28
Transmission Control Protocol, Src Port: 443, Dst Port: 44240, Seq: 1, Ack: 143, Len: 82
Transport Layer Security
0000 0a ff e7 39 bd b1 0a 23 cb e2 48 cb 08 00 45 00
0010 00 86 f3 c5 40 00 38 06 0f 85 ac 40 29 04 0a c7
0020 5f 1c 01 bb ac d0 ab 82 2c 52 58 38 44 6b 80 18
0030 00 08 2b 57 00 00 01 01 08 0a 14 03 ce 76 a4 29
0040 34 0d 17 03 03 00 4d 2a c0 23 b7 ca 75 0d ef cc
0050 86 60 a5 01 3b 1d 95 df e0 75 c5 ba ac 06 6c 39
0060 99 ea 43 09 10 84 e8 a5 a7 92 3b 72 e5 c5 bf 8d
0070 a2 4c d7 b7 04 ae 97 9f 50 76 40 bd 85 e0 ba f7
0080 ef 67 01 6b e6 76 ce a3 da 9b 05 2d 24 b3 5f c8
0090 fb c9 e2 91
wireshark_ens5Y4PKM2.pcapng
Packets: 4591 · Displayed: 2084 (45.4%) · Dropped: 0 (0.0%)
Profile: Default

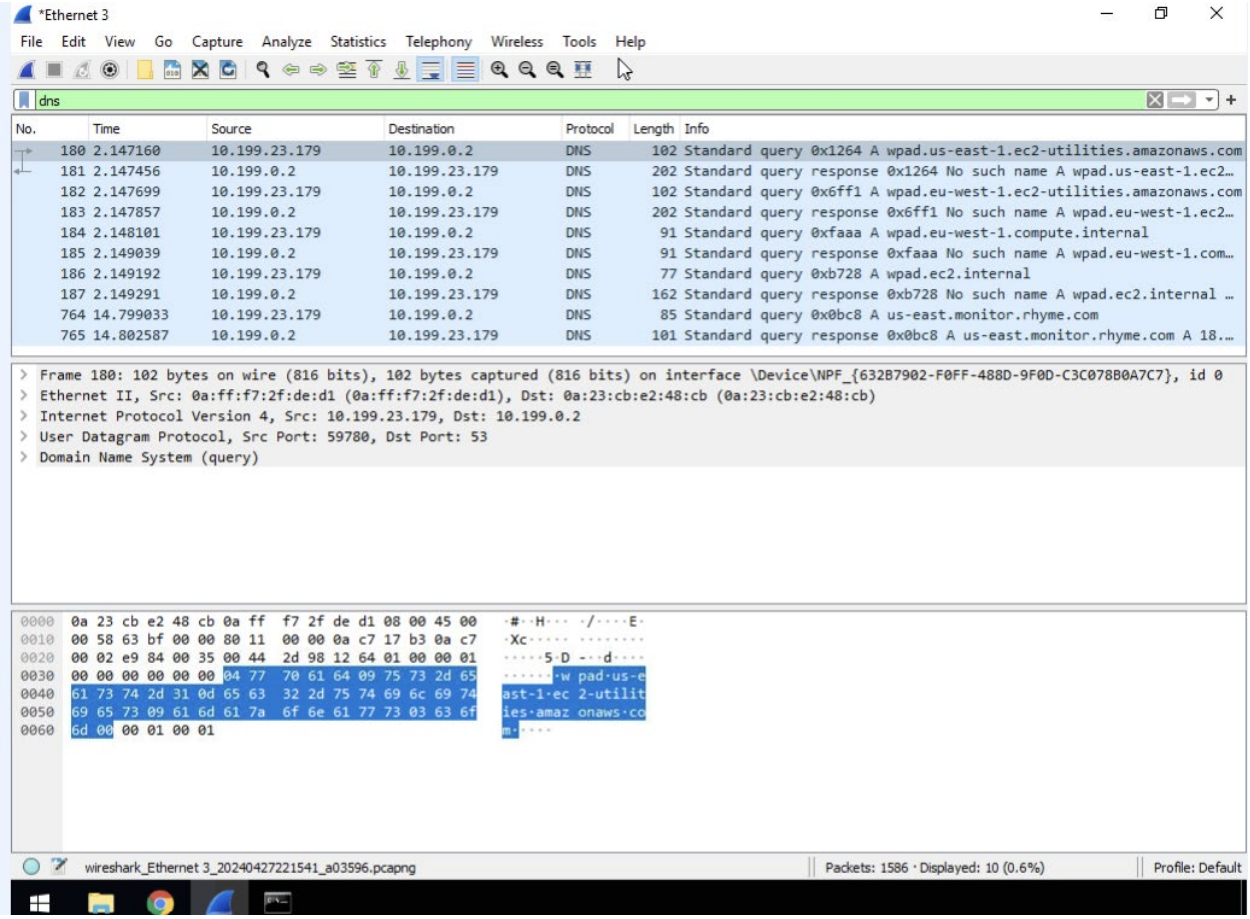
Wireshark for Basic Network Security Analysis

Task 1: Get to know Wireshark and its basic functionalities

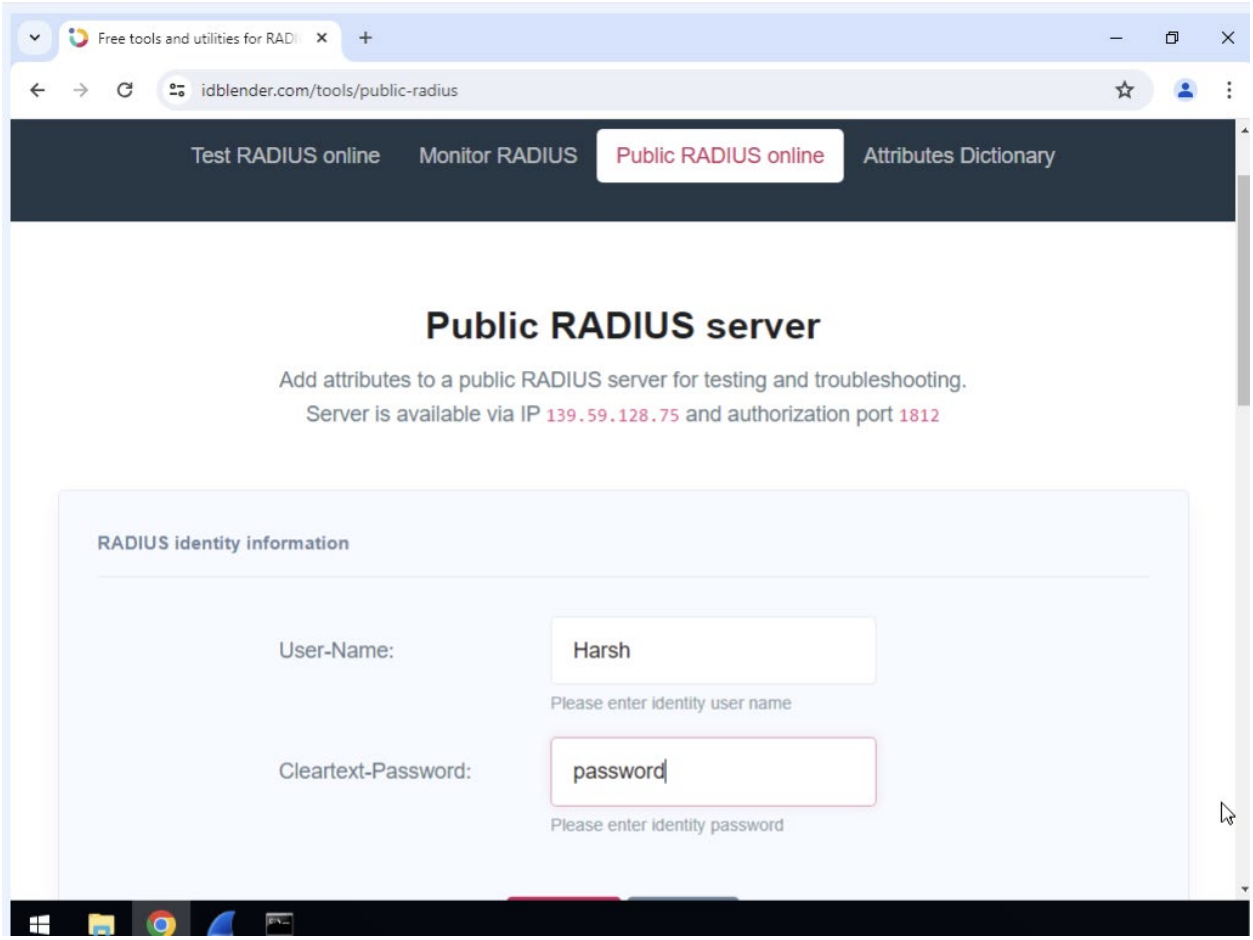


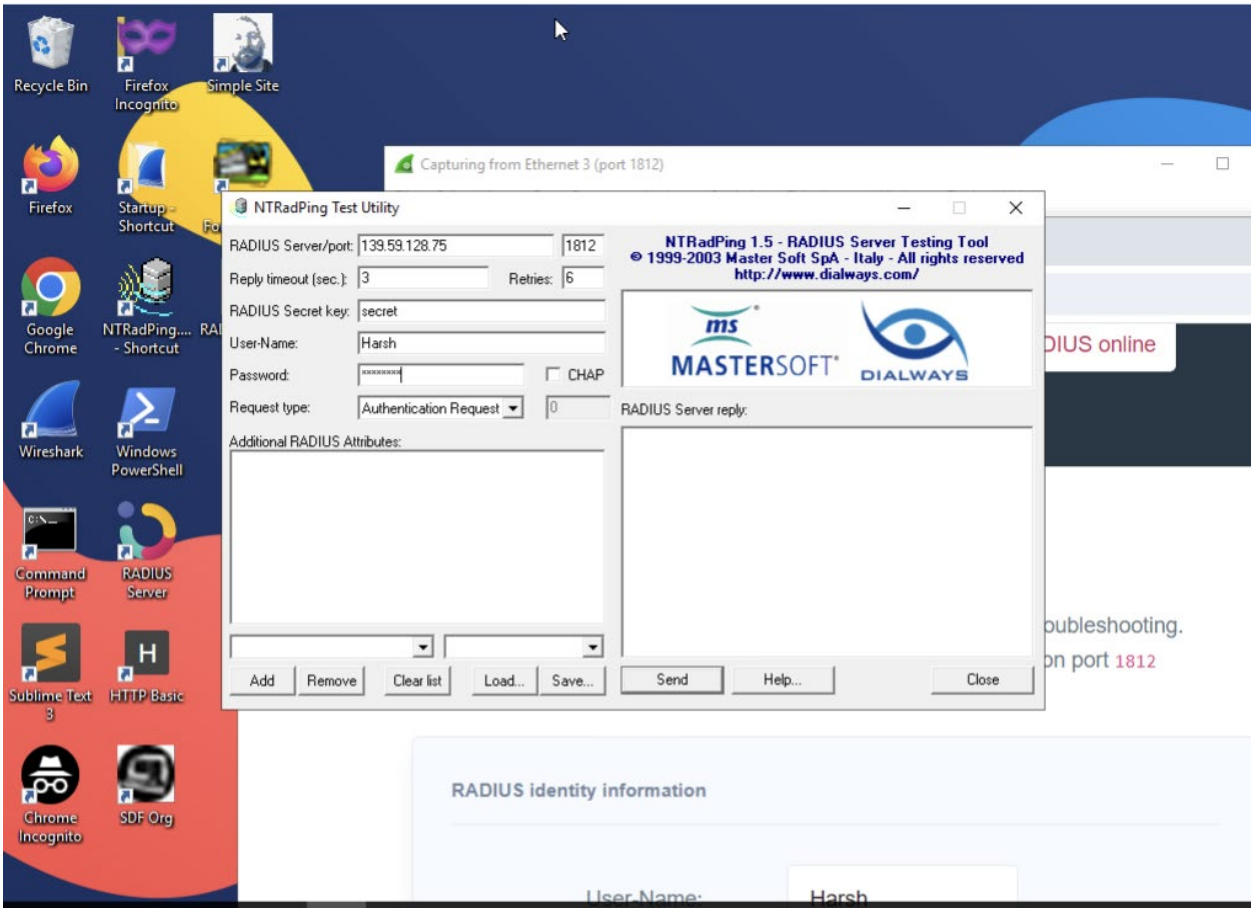

RADIUS.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.100 212.24.98.232 RADIUS 87 Access-Request id=4
2 1.145799 212.24.98.232 192.168.1.100 RADIUS 62 Access-Reject id=4
3 9.234799 192.168.1.100 212.24.98.232 RADIUS 87 Access-Request id=5
4 9.368233 212.24.98.232 192.168.1.100 RADIUS 69 Access-Accept id=5
Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: IntelCor_c8:6e:4b (5c:5f:67:c8:6e:4b), Dst: Tp-LinkT_42:de:65 (c4:71:54:42:de:65)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 212.24.98.232
User Datagram Protocol, Src Port: 59146, Dst Port: 1812
RADIUS Protocol
0000 c4 71 54 42 de 65 5c 5f 67 c8 6e 4b 08 00 45 00
0010 00 49 13 ac 00 00 80 11 2d eb c0 a8 01 64 d4 18
0020 62 e8 e7 0a 07 14 00 35 f3 0d 01 04 00 2d 20 20
0030 20 20 20 20 31 35 39 36 30 35 39 31 30 38 01 07
0040 6d 65 6e 6e 61 02 12 0b 91 b7 8e 67 27 43 f4 12
0050 22 17 4a 25 04 14 c4
RADIUS.pcap
Packets: 4 · Displayed: 4 (100.0%)
Profile: Default
Chrome Incognito
SDF Org

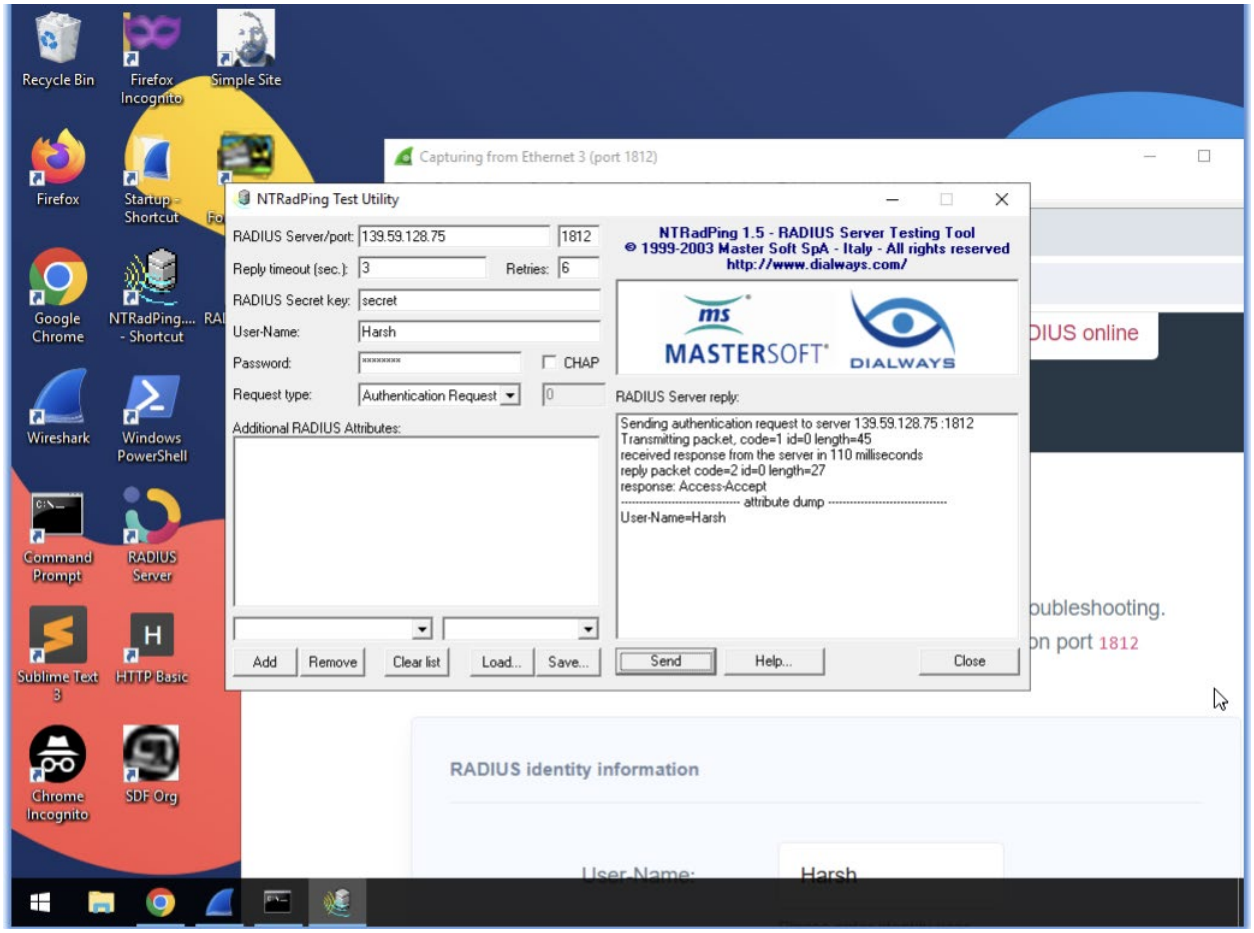

Capturing from Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
66 2.568833 10.199.23.179 10.199.255.126 TCP 54 36202 → 45048 [ACK] Seq=7
67 2.570490 10.199.23.179 10.199.255.126 TCP 83 36202 → 45048 [PSH, ACK]
68 2.571579 10.199.255.126 10.199.23.179 TCP 64 45048 → 36202 [PSH, ACK]
69 2.580824 10.199.23.179 10.199.255.126 TCP 54 36202 → 45048 [ACK] Seq=7
70 2.792097 10.199.23.179 10.199.255.126 TCP 7129 36202 → 45048 [PSH, ACK]
71 2.793211 10.199.255.126 10.199.23.179 TCP 54 45048 → 36202 [ACK] Seq=2
72 2.794058 10.199.255.126 10.199.23.179 TCP 64 45048 → 36202 [PSH, ACK]
73 2.803848 10.199.23.179 10.199.255.126 TCP 54 36202 → 45048 [ACK] Seq=8
74 3.115465 10.199.23.179 10.199.255.126 TCP 85 36202 → 45048 [PSH, ACK]
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{632B7902-F
Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb), Dst: 0a:ff:f7:2f:de:d1 (0a:ff:f7:2f:de:d1)
Internet Protocol Version 4, Src: 10.199.255.126, Dst: 10.199.23.179
Transmission Control Protocol, Src Port: 45048, Dst Port: 36202, Seq: 1, Ack: 1, Len: 6
Data (6 bytes)
0000 0a ff f7 2f de d1 0a 23 cb e2 48 cb 08 00 45 00
0010 00 2e df c5 40 00 40 06 2e 45 0a c7 ff 7e 0a c7
0020 17 b3 af f8 8d 6a 18 71 65 c5 85 b1 b0 b3 50 18
0030 30 0c 59 9f 00 00 05 00 00 db 01 82
Ethernet 3: <live capture in progress>
Packets: 74 · Displayed: 74 (100.0%)
Profile: Default

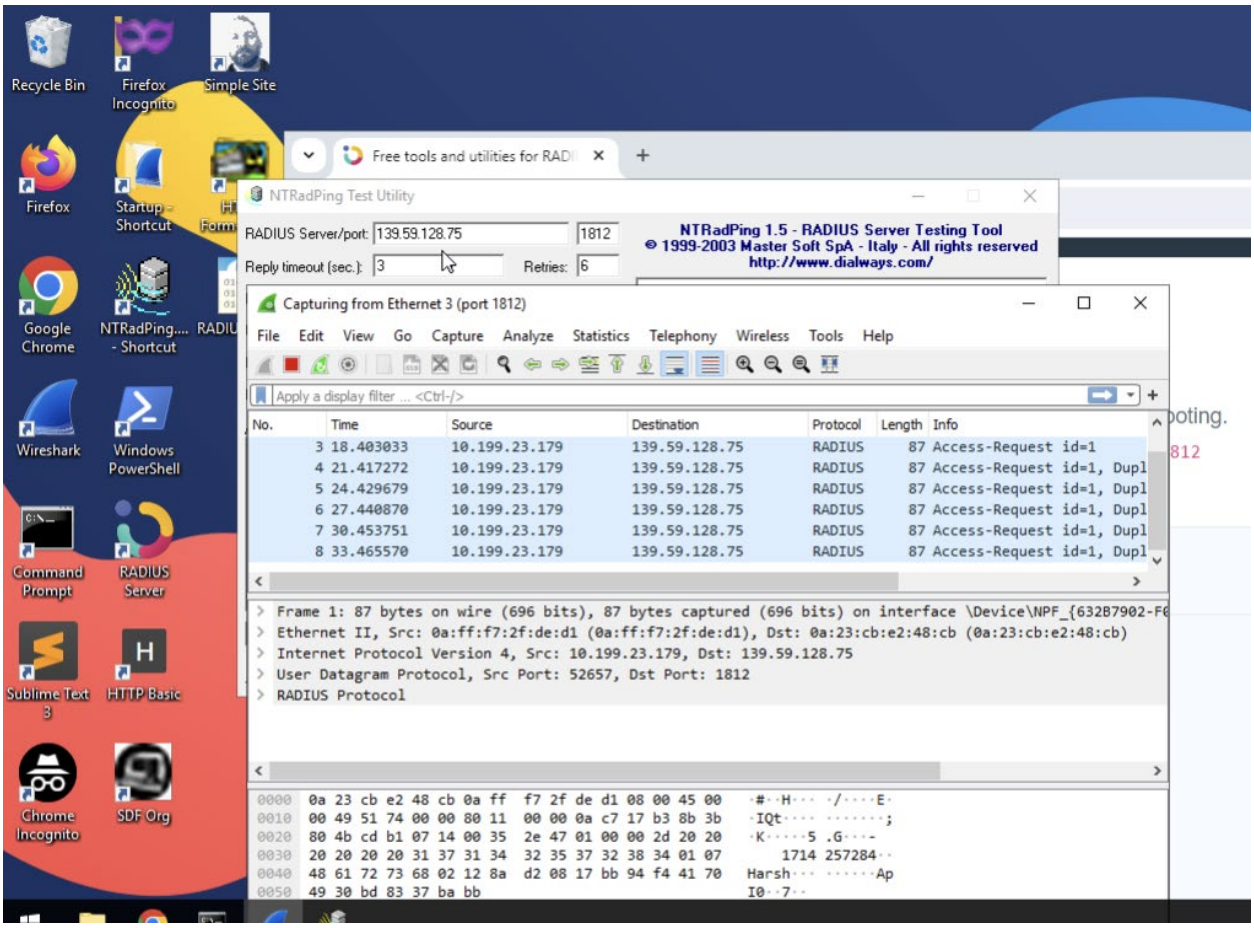


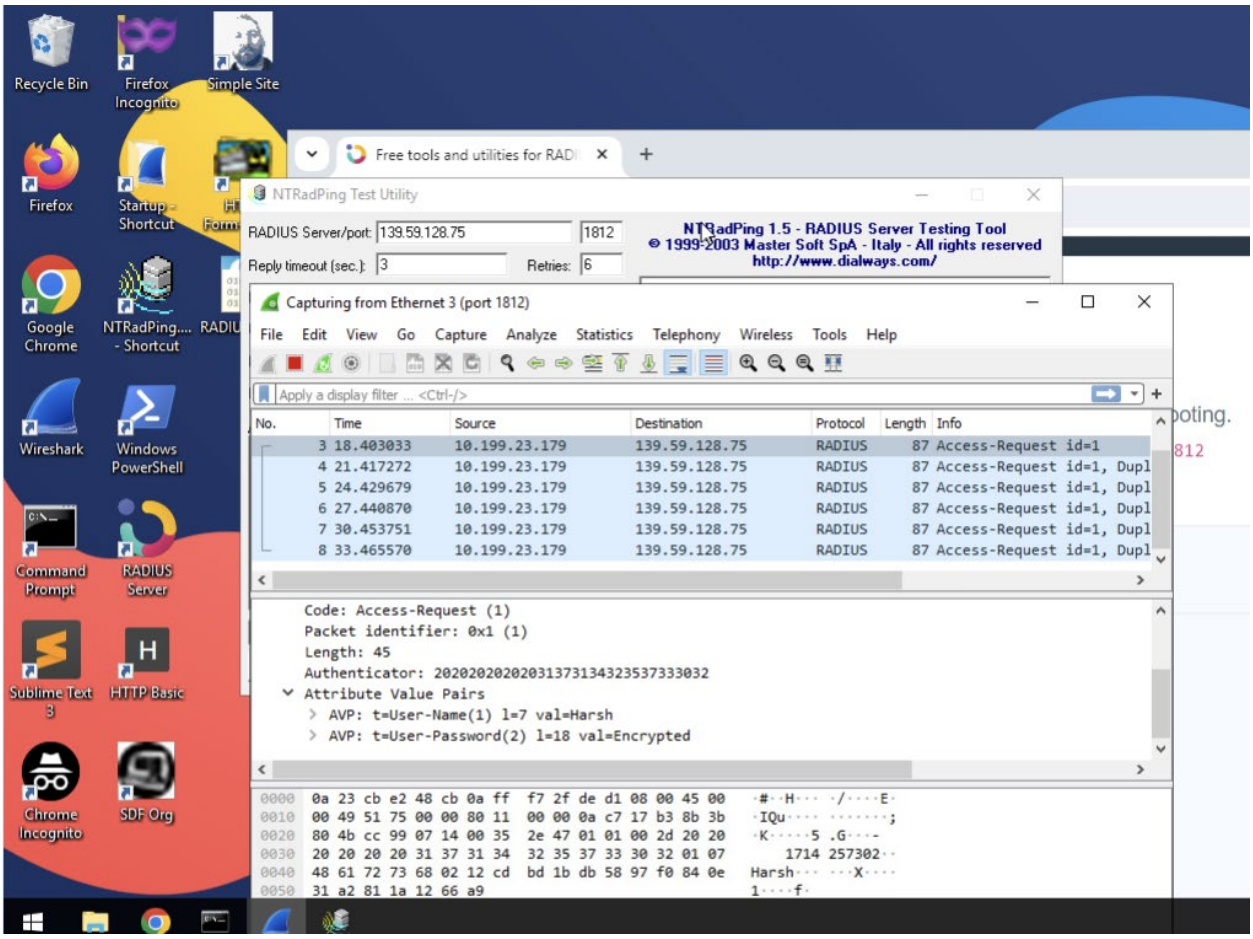
Task 2: Generate and Capture RADIUS Traffic

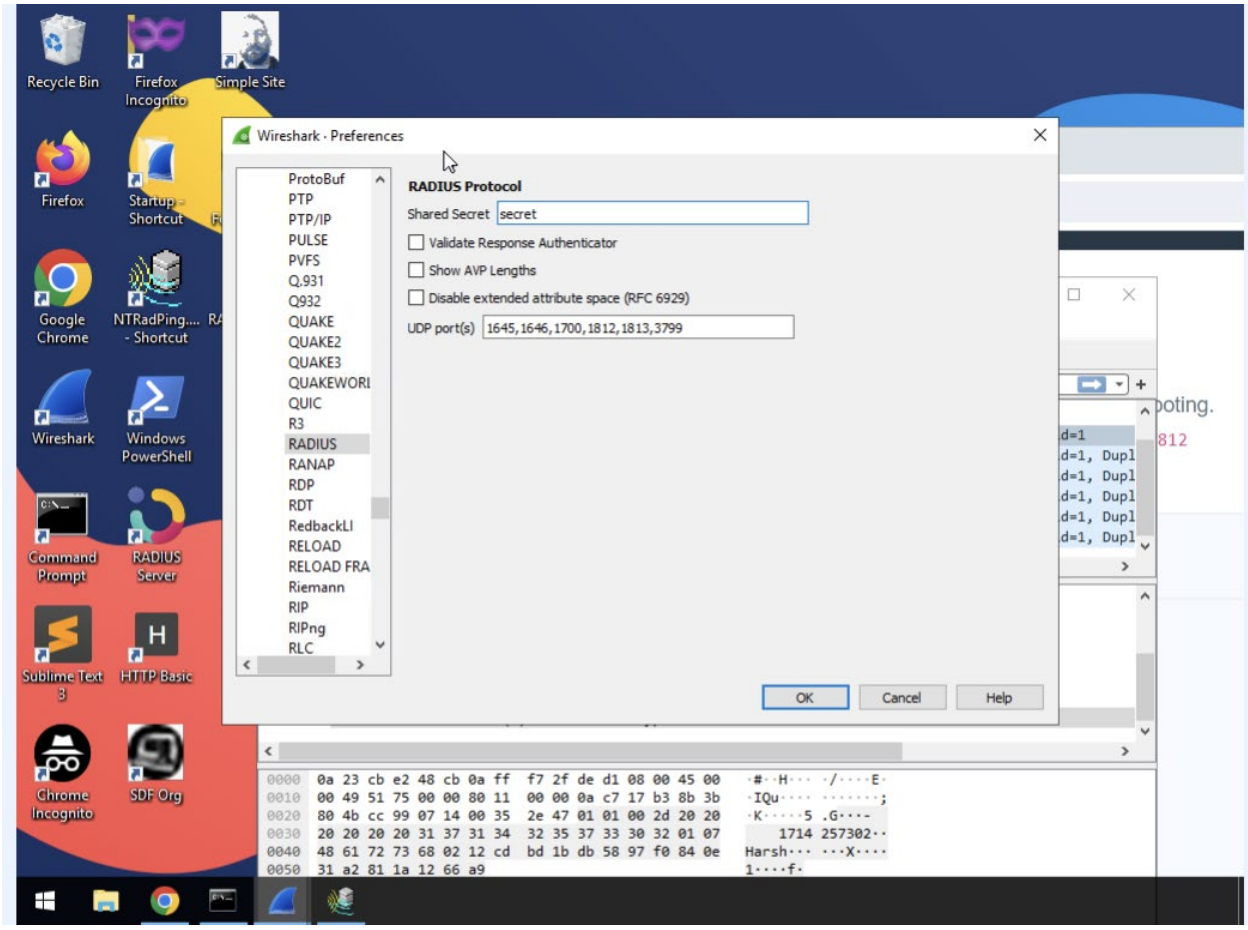

Free tools and utilities for RADI
idblender.com/tools/public-radius
Test RADIUS online
Monitor RADIUS
Public RADIUS online
Attributes Dictionary
Public RADIUS server
Add attributes to a public RADIUS server for testing and troubleshooting.
Server is available via IP 139.59.128.75 and authorization port 1812
RADIUS identity information
User-Name:
Harsh
Please enter identity user name
Cleartext-Password:
password
Please enter identity password

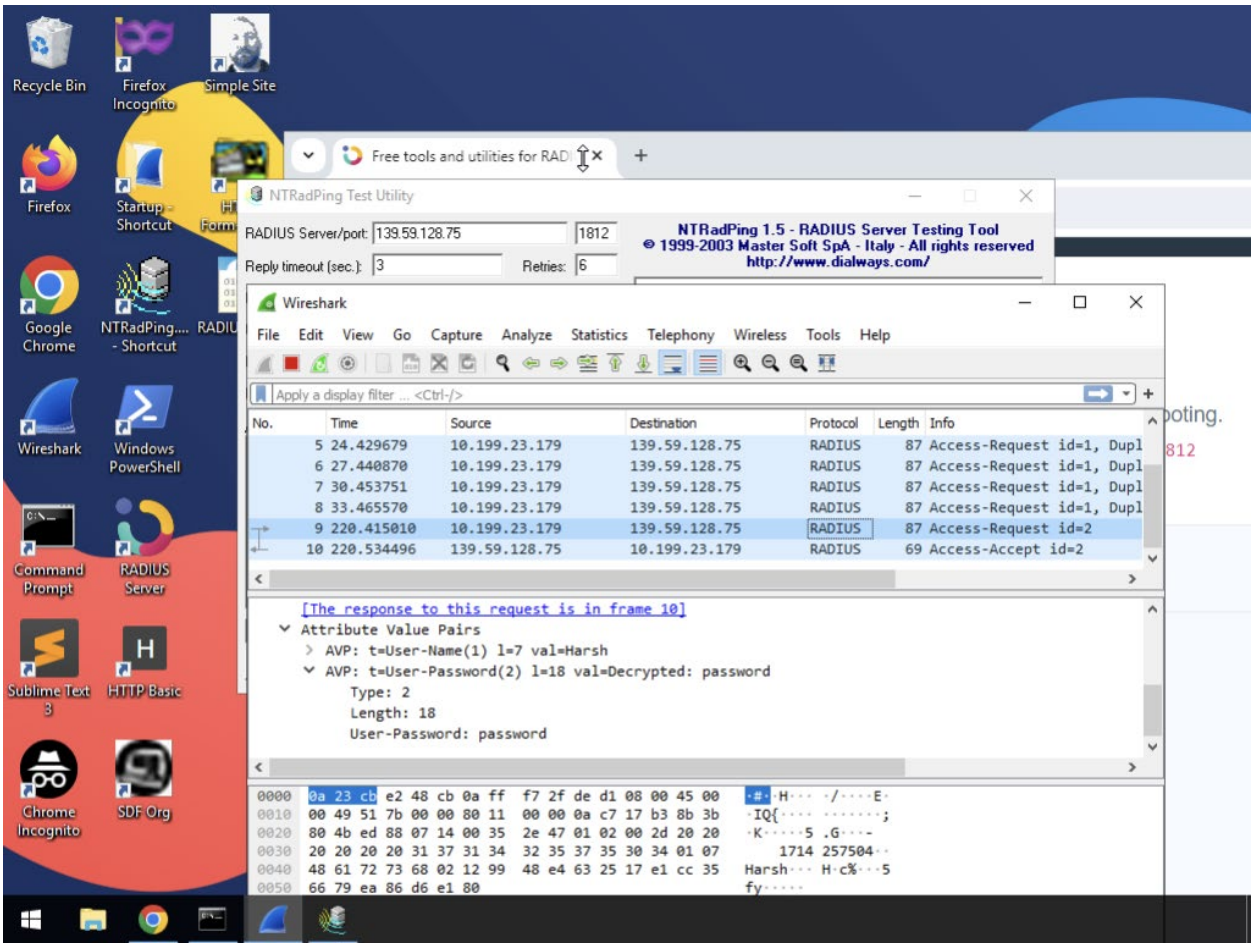

Recycle Bin
Firefox Incognito
Simple Site
Firefox
Startup - Shortcut
Google Chrome
NTRadPing.... - Shortcut
Wireshark
Windows PowerShell
Command Prompt
RADIUS Server
Sublime Text 3
HTTP Basic
Chrome Incognito
SDF Org
Capturing from Ethernet 3 (port 1812)
NTRadPing Test Utility
RADIUS Server/port: 139.59.128.75 1812
Reply timeout (sec.): 3 Retries: 6
RADIUS Secret key: secret
User-Name: Harsh
Password: ********
CHAP
Request type: Authentication Request 0
Additional RADIUS Attributes:
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
MASTERSOFT
DIALWAYS
RADIUS Server reply:
Add
Remove
Clear list
Load...
Save...
Send
Help...
Close
DIUS online
oubleshooting.
on port 1812
RADIUS identity information
User-Name:
Harsh


Recycle Bin
Firefox Incognito
Simple Site
Firefox
Startup - Shortcut
Google Chrome
NTRadPing.... - Shortcut
Wireshark
Windows PowerShell
Command Prompt
RADIUS Server
Sublime Text 3
HTTP Basic
Chrome Incognito
SDF Org
Capturing from Ethernet 3 (port 1812)
NTRadPing Test Utility
RADIUS Server/port: 139.59.128.75 1812
Reply timeout (sec.): 3 Retries: 6
RADIUS Secret key: secret
User-Name: Harsh
Password:
CHAP
Request type: Authentication Request
Additional RADIUS Attributes:
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
MASTERSOFT
DIALWAYS
RADIUS Server reply:
Sending authentication request to server 139.59.128.75 :1812
Transmitting packet, code=1 id=0 length=45
received response from the server in 110 milliseconds
reply packet code=2 id=0 length=27
response: Access-Accept
attribute dump
User-Name=Harsh
Add
Remove
Clear list
Load...
Save...
Send
Help...
Close
DIUS online
ubleshooting.
on port 1812
RADIUS identity information
User-Name:
Harsh

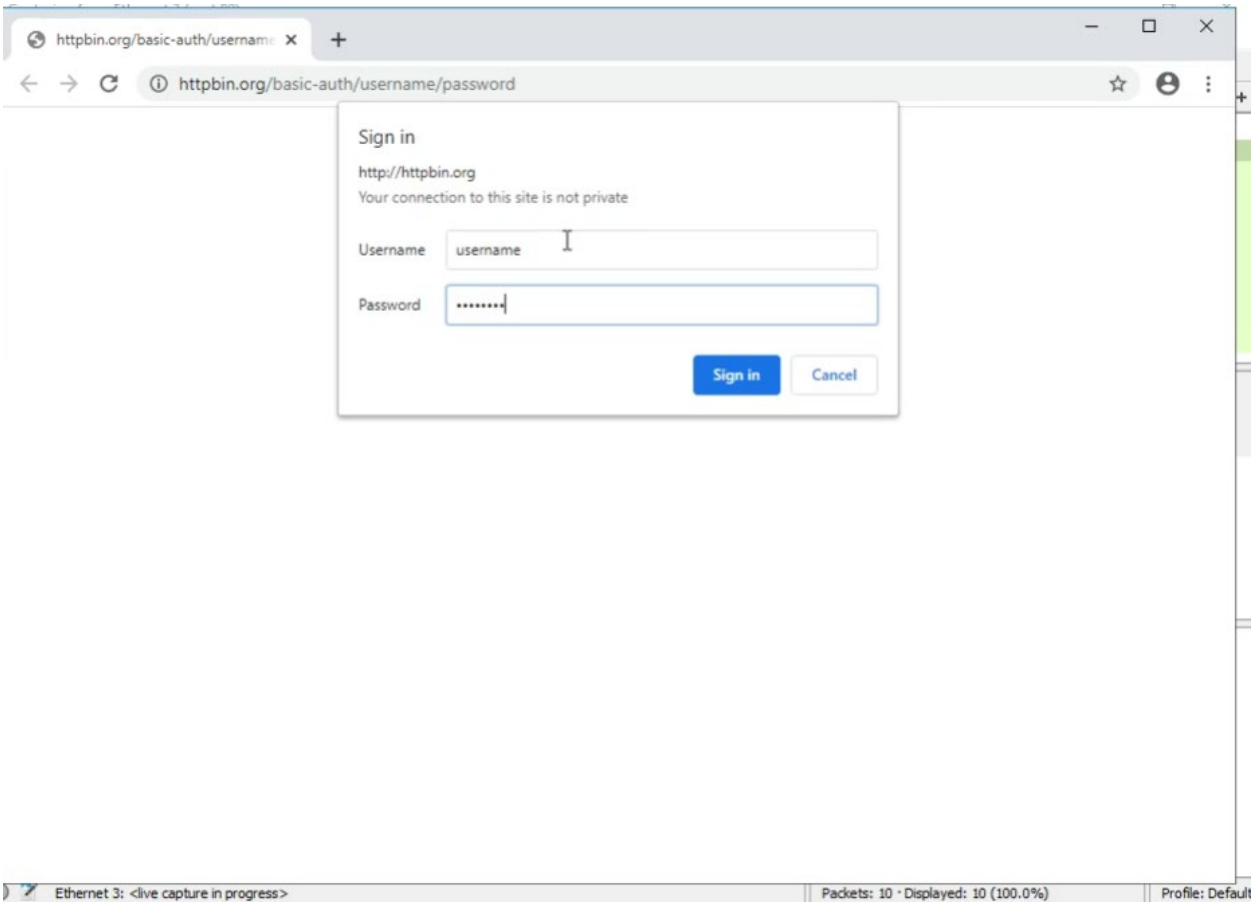

Recycle Bin
Firefox Incognito
Simple Site
Firefox
Startup - Shortcut
Google Chrome
NTRadPing.... - Shortcut
Wireshark
Windows PowerShell
Command Prompt
RADIUS Server
Sublime Text 3
HTTP Basic
Chrome Incognito
SDF Org
Free tools and utilities for RAD
NTRadPing Test Utility
RADIUS Server/port: 139.59.128.75 1812
Reply timeout (sec.): 3 Retries: 6
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
Capturing from Ethernet 3 (port 1812)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3 18.403033 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1
4 21.417272 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
5 24.429679 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
6 27.440870 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
7 30.453751 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
8 33.465570 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{632B7902-F
Ethernet II, Src: 0a:ff:f7:2f:de:d1 (0a:ff:f7:2f:de:d1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.23.179, Dst: 139.59.128.75
User Datagram Protocol, Src Port: 52657, Dst Port: 1812
RADIUS Protocol
0000 0a 23 cb e2 48 cb 0a ff f7 2f de d1 08 00 45 00
0010 00 49 51 74 00 00 80 11 00 00 0a c7 17 b3 8b 3b
0020 80 4b cd b1 07 14 00 35 2e 47 01 00 00 2d 20 20
0030 20 20 20 20 31 37 31 34 32 35 37 32 38 34 01 07
0040 48 61 72 73 68 02 12 8a d2 08 17 bb 94 f4 41 70
0050 49 30 bd 83 37 ba bb
poting.
812

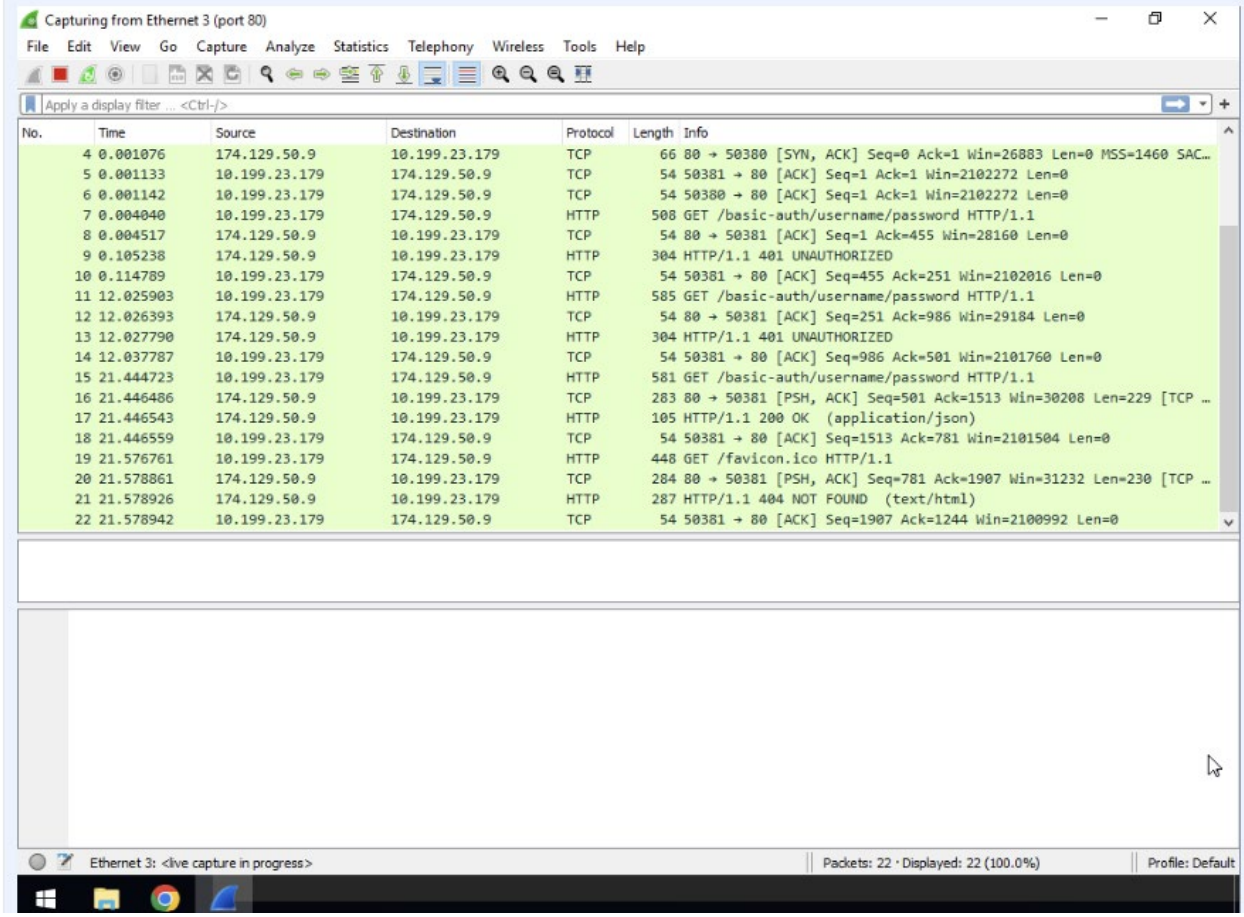

Recycle Bin
Firefox Incognito
Simple Site
Firefox
Startup - Shortcut
Google Chrome
NTRadPing.... - Shortcut
Wireshark
Windows PowerShell
Command Prompt
RADIUS Server
Sublime Text 3
HTTP Basic
Chrome Incognito
SDF Org
Free tools and utilities for RAD
NTRadPing Test Utility
RADIUS Server/port: 139.59.128.75 1812
Reply timeout (sec.): 3 Retries: 6
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
Capturing from Ethernet 3 (port 1812)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3 18.403033 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1
4 21.417272 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
5 24.429679 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
6 27.440870 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
7 30.453751 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
8 33.465570 10.199.23.179 139.59.128.75 RADIUS 87 Access-Request id=1, Dupl
Code: Access-Request (1)
Packet identifier: 0x1 (1)
Length: 45
Authenticator: 20202020202031373134323537333032
Attribute Value Pairs
AVP: t=User-Name(1) l=7 val=Harsh
AVP: t=User-Password(2) l=18 val=Encrypted
0000 0a 23 cb e2 48 cb 0a ff f7 2f de d1 08 00 45 00
0010 00 49 51 75 00 00 80 11 00 00 0a c7 17 b3 8b 3b
0020 80 4b cc 99 07 14 00 35 2e 47 01 01 00 2d 20 20
0030 20 20 20 20 31 37 31 34 32 35 37 33 30 32 01 07
0040 48 61 72 73 68 02 12 cd bd 1b db 58 97 f0 84 0e
0050 31 a2 81 1a 12 66 a9
Harsh
1714 257302
X
1
f

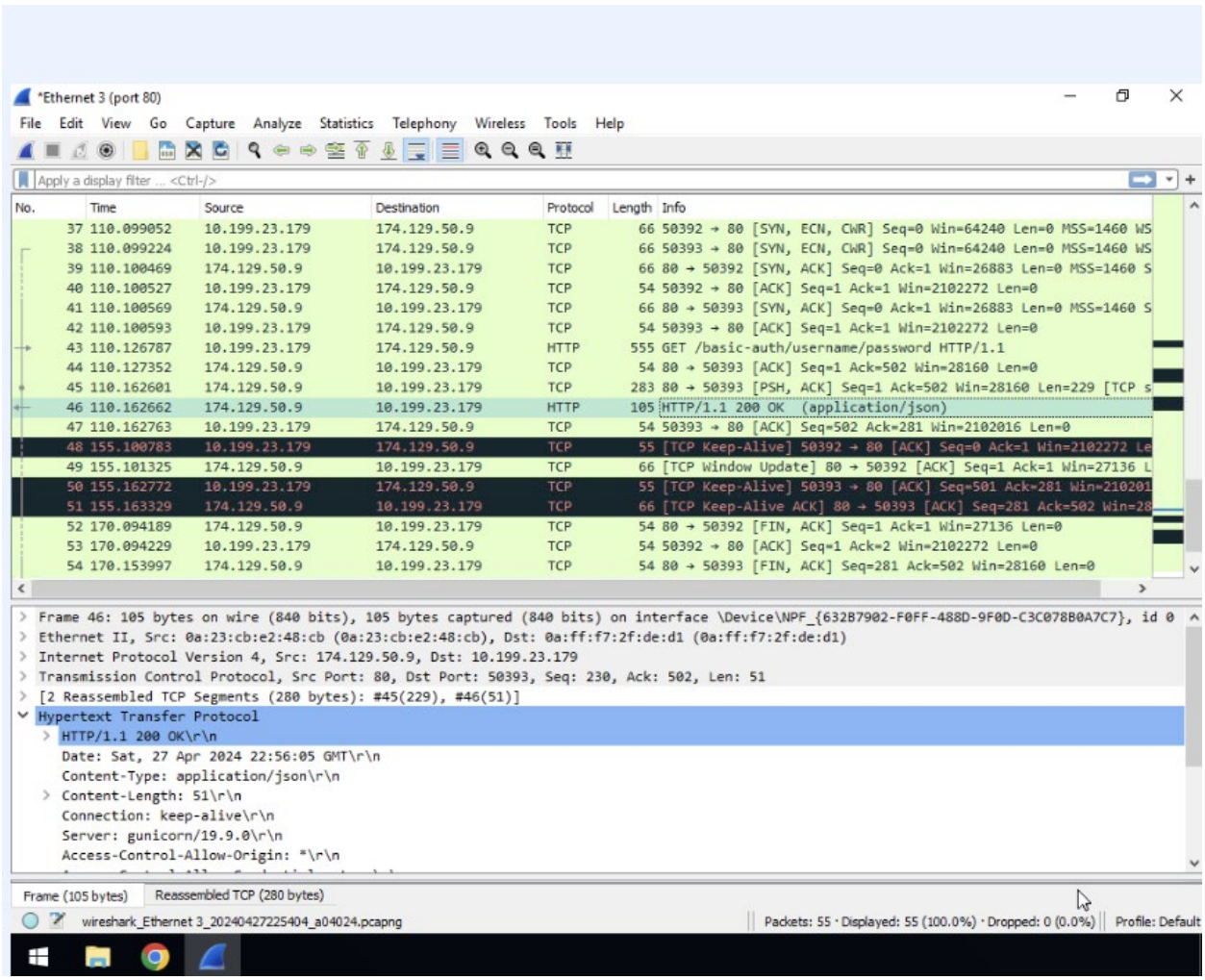

Recycle Bin
Firefox Incognito
Simple Site
Firefox
Startup - Shortcut
Google Chrome
NTRadPing.... - Shortcut
Wireshark
Windows PowerShell
Command Prompt
RADIUS Server
Sublime Text 3
HTTP Basic
Chrome Incognito
SDF Org
Wireshark · Preferences
ProtoBuf
PTP
PTP/IP
PULSE
PVFS
Q.931
Q932
QUAKE
QUAKE2
QUAKE3
QUAKEWORL
QUIC
R3
RADIUS
RANAP
RDP
RDT
RedbackLI
RELOAD
RELOAD FRA
Riemann
RIP
RIPng
RLC
RADIUS Protocol
Shared Secret
secret
Validate Response Authenticator
Show AVP Lengths
Disable extended attribute space (RFC 6929)
UDP port(s)
1645,1646,1700,1812,1813,3799
OK
Cancel
Help
0000 0a 23 cb e2 48 cb 0a ff f7 2f de d1 08 00 45 00
0010 00 49 51 75 00 00 80 11 00 00 0a c7 17 b3 8b 3b
0020 80 4b cc 99 07 14 00 35 2e 47 01 01 00 2d 20 20
0030 20 20 20 20 31 37 31 34 32 35 37 33 30 32 01 07
0040 48 61 72 73 68 02 12 cd bd 1b db 58 97 f0 84 0e
0050 31 a2 81 1a 12 66 a9

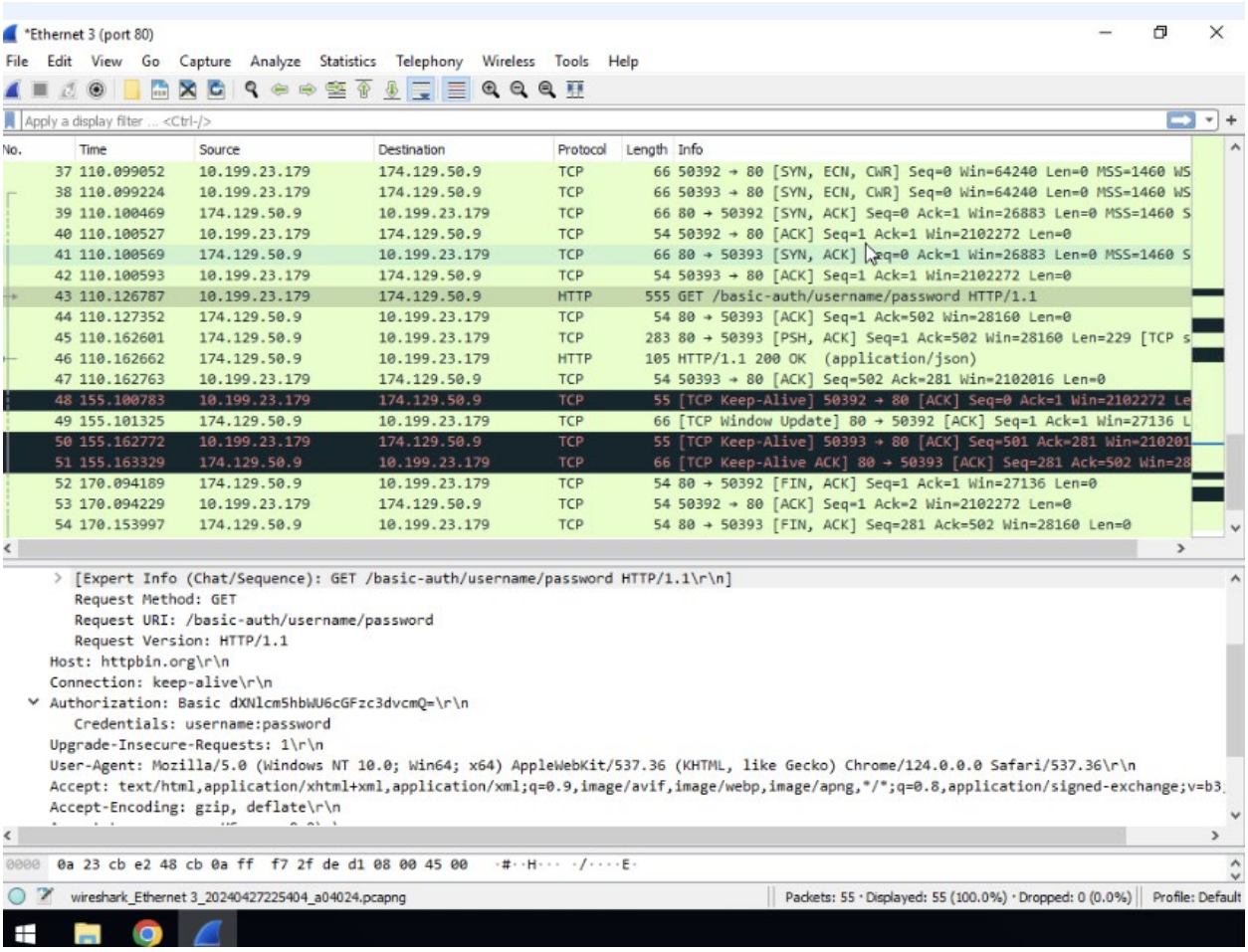


Task 3: Analyze a HTTP Basic Authentication

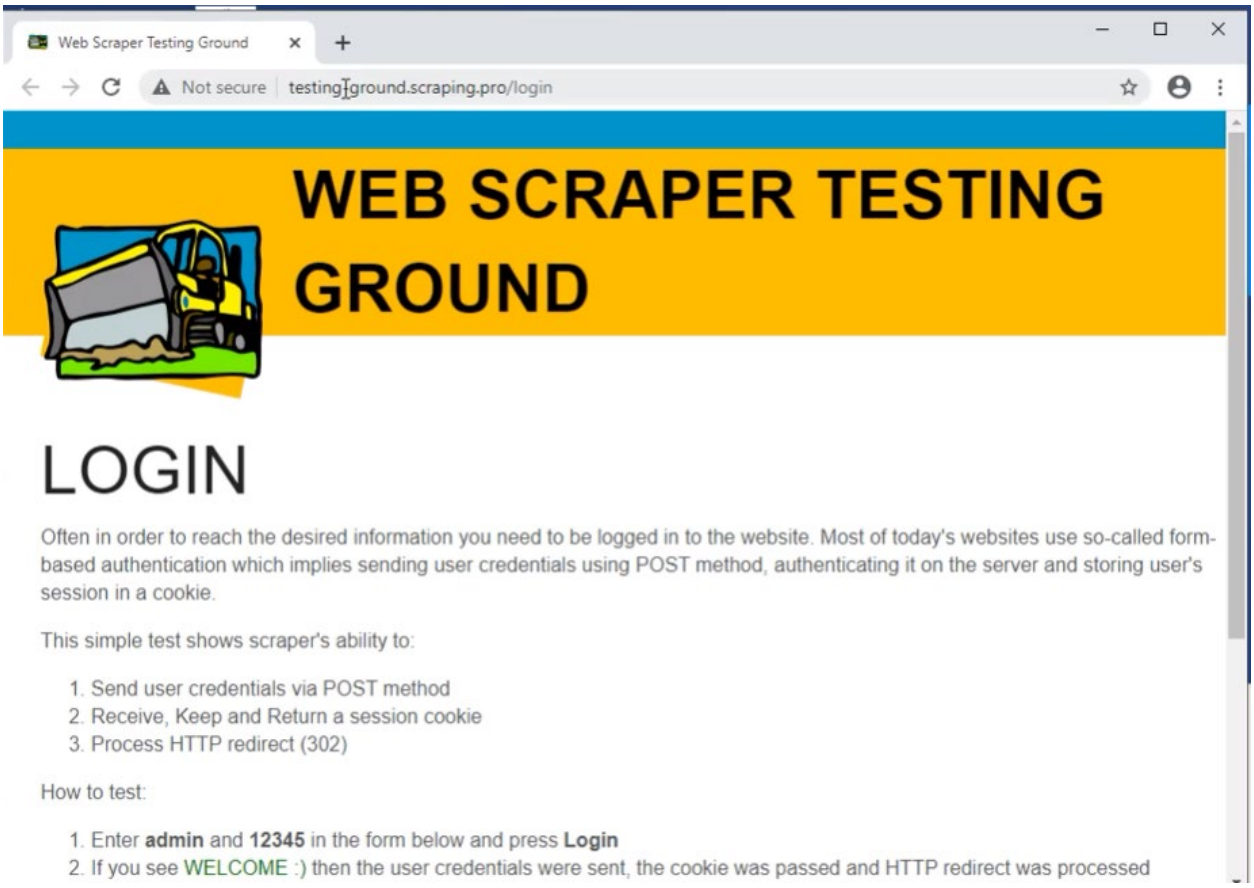

httpbin.org/basic-auth/username/password
Sign in
http://httpbin.org
Your connection to this site is not private
Username
username
Password
Sign in
Cancel
Ethernet 3: <live capture in progress>
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default

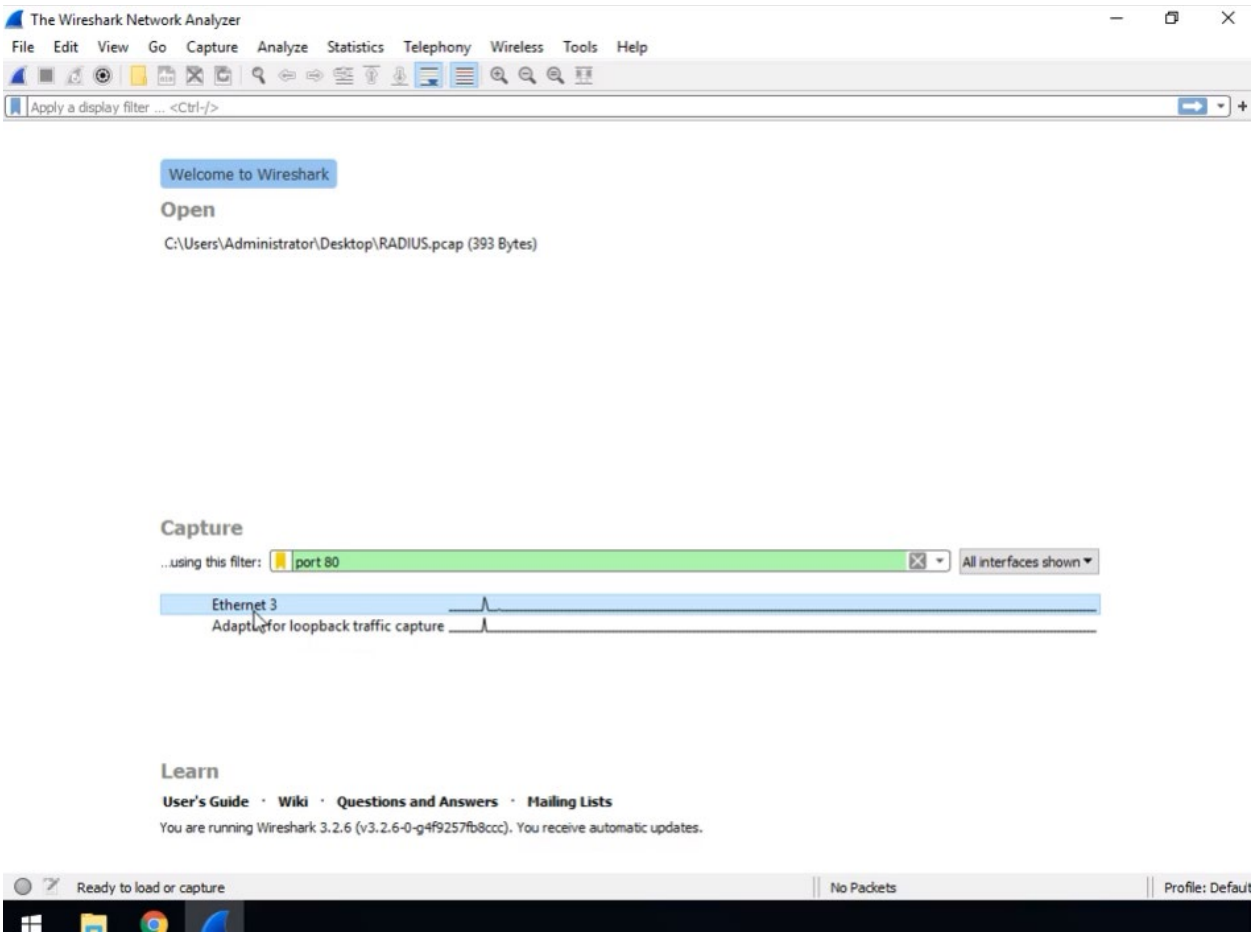

Capturing from Ethernet 3 (port 80)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4 0.001076 174.129.50.9 10.199.23.179 TCP 66 80 → 50380 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SAC…
5 0.001133 10.199.23.179 174.129.50.9 TCP 54 50381 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
6 0.001142 10.199.23.179 174.129.50.9 TCP 54 50380 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
7 0.004040 10.199.23.179 174.129.50.9 HTTP 508 GET /basic-auth/username/password HTTP/1.1
8 0.004517 174.129.50.9 10.199.23.179 TCP 54 80 → 50381 [ACK] Seq=1 Ack=455 Win=28160 Len=0
9 0.105238 174.129.50.9 10.199.23.179 HTTP 304 HTTP/1.1 401 UNAUTHORIZED
10 0.114789 10.199.23.179 174.129.50.9 TCP 54 50381 → 80 [ACK] Seq=455 Ack=251 Win=2102016 Len=0
11 12.025903 10.199.23.179 174.129.50.9 HTTP 585 GET /basic-auth/username/password HTTP/1.1
12 12.026393 174.129.50.9 10.199.23.179 TCP 54 80 → 50381 [ACK] Seq=251 Ack=986 Win=29184 Len=0
13 12.027790 174.129.50.9 10.199.23.179 HTTP 304 HTTP/1.1 401 UNAUTHORIZED
14 12.037787 10.199.23.179 174.129.50.9 TCP 54 50381 → 80 [ACK] Seq=986 Ack=501 Win=2101760 Len=0
15 21.444723 10.199.23.179 174.129.50.9 HTTP 581 GET /basic-auth/username/password HTTP/1.1
16 21.446486 174.129.50.9 10.199.23.179 TCP 283 80 → 50381 [PSH, ACK] Seq=501 Ack=1513 Win=30208 Len=229 [TCP …
17 21.446543 174.129.50.9 10.199.23.179 HTTP 105 HTTP/1.1 200 OK (application/json)
18 21.446559 10.199.23.179 174.129.50.9 TCP 54 50381 → 80 [ACK] Seq=1513 Ack=781 Win=2101504 Len=0
19 21.576761 10.199.23.179 174.129.50.9 HTTP 448 GET /favicon.ico HTTP/1.1
20 21.578861 174.129.50.9 10.199.23.179 TCP 284 80 → 50381 [PSH, ACK] Seq=781 Ack=1907 Win=31232 Len=230 [TCP …
21 21.578926 174.129.50.9 10.199.23.179 HTTP 287 HTTP/1.1 404 NOT FOUND (text/html)
22 21.578942 10.199.23.179 174.129.50.9 TCP 54 50381 → 80 [ACK] Seq=1907 Ack=1244 Win=2100992 Len=0
Ethernet 3: <live capture in progress>
Packets: 22 · Displayed: 22 (100.0%)
Profile: Default

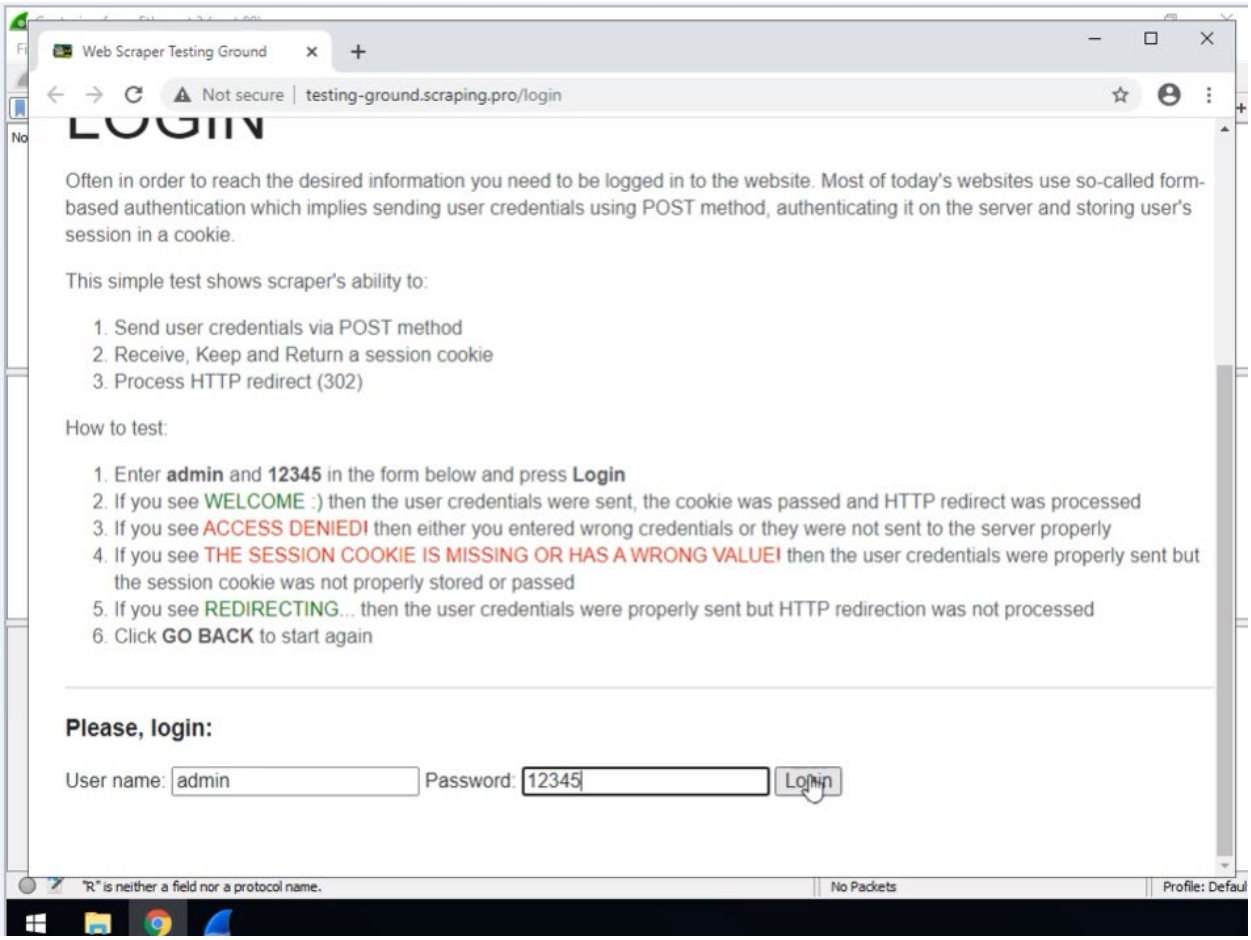

*Ethernet 3 (port 80)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
37 110.099052 10.199.23.179 174.129.50.9 TCP 66 50392 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
38 110.099224 10.199.23.179 174.129.50.9 TCP 66 50393 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
39 110.100469 174.129.50.9 10.199.23.179 TCP 66 80 → 50392 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 S
40 110.100527 10.199.23.179 174.129.50.9 TCP 54 50392 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
41 110.100569 174.129.50.9 10.199.23.179 TCP 66 80 → 50393 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 S
42 110.100593 10.199.23.179 174.129.50.9 TCP 54 50393 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
43 110.126787 10.199.23.179 174.129.50.9 HTTP 555 GET /basic-auth/username/password HTTP/1.1
44 110.127352 174.129.50.9 10.199.23.179 TCP 54 80 → 50393 [ACK] Seq=1 Ack=502 Win=28160 Len=0
45 110.162601 174.129.50.9 10.199.23.179 TCP 283 80 → 50393 [PSH, ACK] Seq=1 Ack=502 Win=28160 Len=229 [TCP s
46 110.162662 174.129.50.9 10.199.23.179 HTTP 105 HTTP/1.1 200 OK (application/json)
47 110.162763 10.199.23.179 174.129.50.9 TCP 54 50393 → 80 [ACK] Seq=502 Ack=281 Win=2102016 Len=0
48 155.100783 10.199.23.179 174.129.50.9 TCP 55 [TCP Keep-Alive] 50392 → 80 [ACK] Seq=0 Ack=1 Win=2102272 Le
49 155.101325 174.129.50.9 10.199.23.179 TCP 66 [TCP Window Update] 80 → 50392 [ACK] Seq=1 Ack=1 Win=27136 L
50 155.162772 10.199.23.179 174.129.50.9 TCP 55 [TCP Keep-Alive] 50393 → 80 [ACK] Seq=501 Ack=281 Win=210201
51 155.163329 174.129.50.9 10.199.23.179 TCP 66 [TCP Keep-Alive ACK] 80 → 50393 [ACK] Seq=281 Ack=502 Win=28
52 170.094189 174.129.50.9 10.199.23.179 TCP 54 80 → 50392 [FIN, ACK] Seq=1 Ack=1 Win=27136 Len=0
53 170.094229 10.199.23.179 174.129.50.9 TCP 54 50392 → 80 [ACK] Seq=1 Ack=2 Win=2102272 Len=0
54 170.153997 174.129.50.9 10.199.23.179 TCP 54 80 → 50393 [FIN, ACK] Seq=281 Ack=502 Win=28160 Len=0
Frame 46: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF_{632B7902-F0FF-488D-9F0D-C3C078B0A7C7}, id 0
Ethernet II, Src: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb), Dst: 0a:ff:f7:2f:de:d1 (0a:ff:f7:2f:de:d1)
Internet Protocol Version 4, Src: 174.129.50.9, Dst: 10.199.23.179
Transmission Control Protocol, Src Port: 80, Dst Port: 50393, Seq: 230, Ack: 502, Len: 51
[2 Reassembled TCP Segments (280 bytes): #45(229), #46(51)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sat, 27 Apr 2024 22:56:05 GMT\r\n
Content-Type: application/json\r\n
Content-Length: 51\r\n
Connection: keep-alive\r\n
Server: gunicorn/19.9.0\r\n
Access-Control-Allow-Origin: *\r\n
Frame (105 bytes)
Reassembled TCP (280 bytes)
wireshark_Ethernet 3_20240427225404_a04024.pcapng
Packets: 55 · Displayed: 55 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

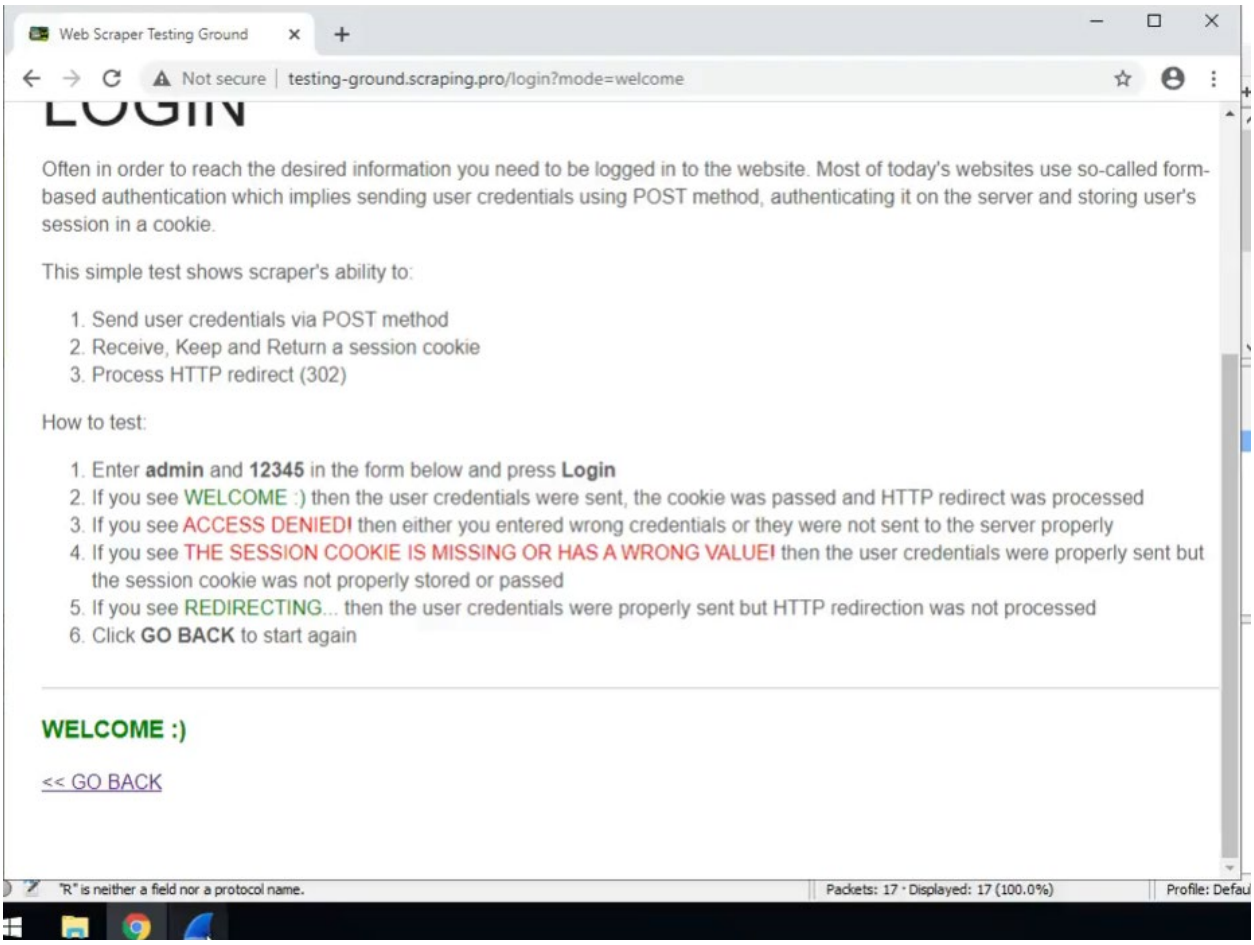


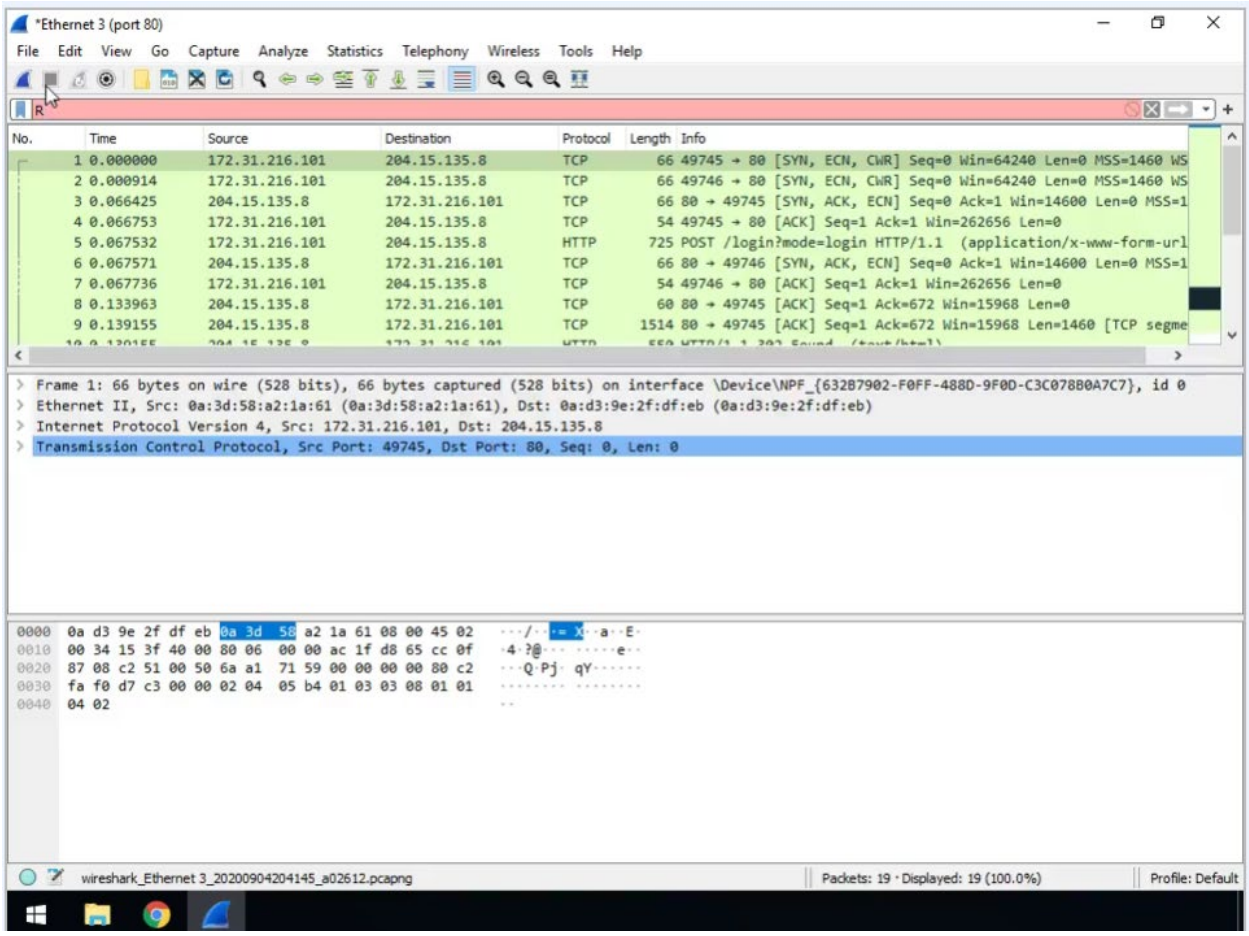
Task 4: HTTP Form-Based Authentication and DNS

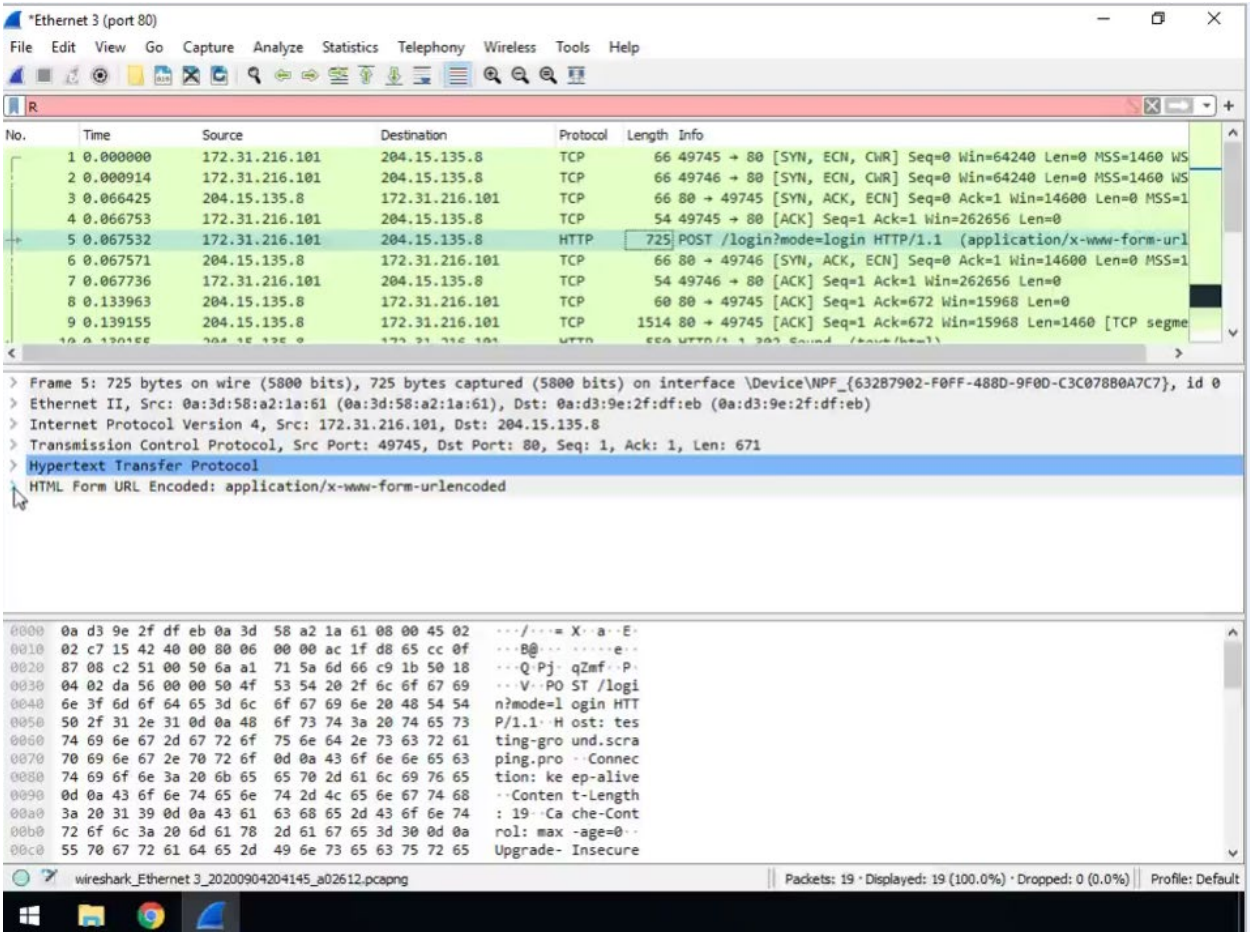

Web Scraper Testing Ground
Not secure
testingground.scraping.pro/login
WEB SCRAPER TESTING GROUND
LOGIN
Often in order to reach the desired information you need to be logged in to the website. Most of today's websites use so-called form-based authentication which implies sending user credentials using POST method, authenticating it on the server and storing user's session in a cookie.
This simple test shows scraper's ability to:
1. Send user credentials via POST method
2. Receive, Keep and Return a session cookie
3. Process HTTP redirect (302)
How to test:
1. Enter admin and 12345 in the form below and press Login
2. If you see WELCOME :) then the user credentials were sent, the cookie was passed and HTTP redirect was processed

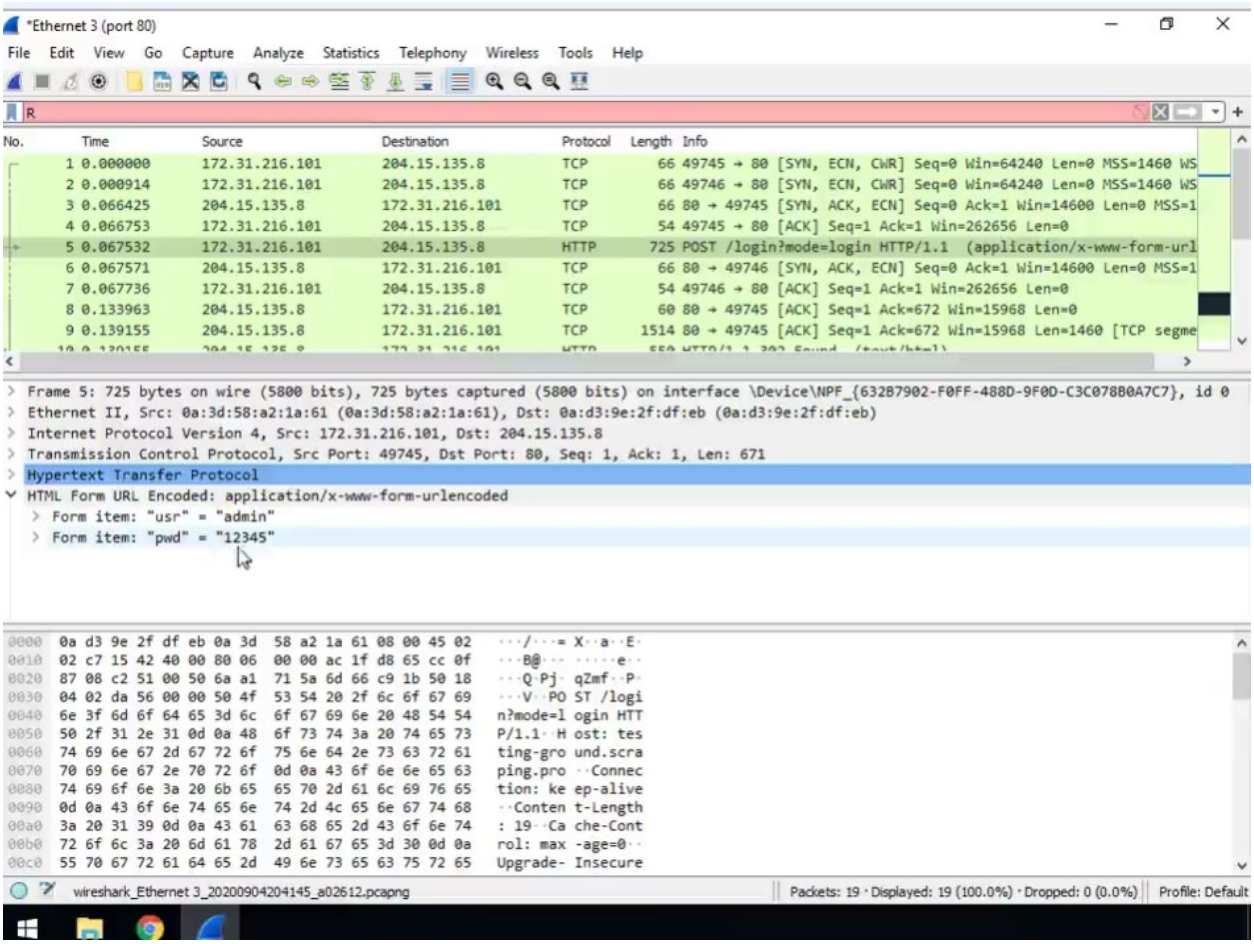

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\Administrator\Desktop\RADIUS.pcap (393 Bytes)
Capture
...using this filter: port 80
All interfaces shown
Ethernet 3
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

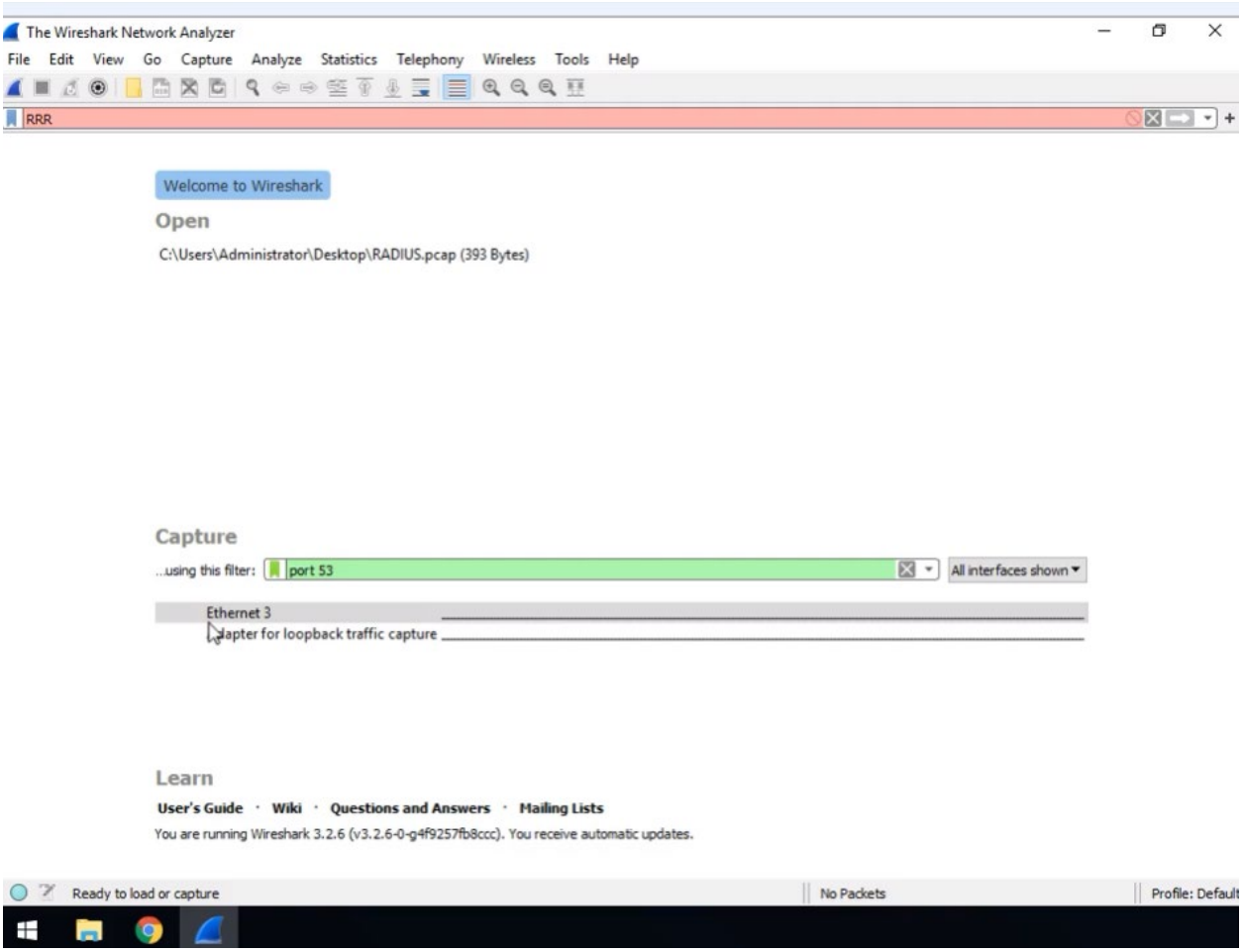

Web Scraper Testing Ground
Not secure | testing-ground.scraping.pro/login
LOGIN
Often in order to reach the desired information you need to be logged in to the website. Most of today's websites use so-called form-based authentication which implies sending user credentials using POST method, authenticating it on the server and storing user's session in a cookie.
This simple test shows scraper's ability to:
1. Send user credentials via POST method
2. Receive, Keep and Return a session cookie
3. Process HTTP redirect (302)
How to test:
1. Enter admin and 12345 in the form below and press Login
2. If you see WELCOME :) then the user credentials were sent, the cookie was passed and HTTP redirect was processed
3. If you see ACCESS DENIED! then either you entered wrong credentials or they were not sent to the server properly
4. If you see THE SESSION COOKIE IS MISSING OR HAS A WRONG VALUE! then the user credentials were properly sent but the session cookie was not properly stored or passed
5. If you see REDIRECTING... then the user credentials were properly sent but HTTP redirection was not processed
6. Click GO BACK to start again
Please, login:
User name: admin
Password: 12345
Login
"R" is neither a field nor a protocol name.
No Packets
Profile: Defaul

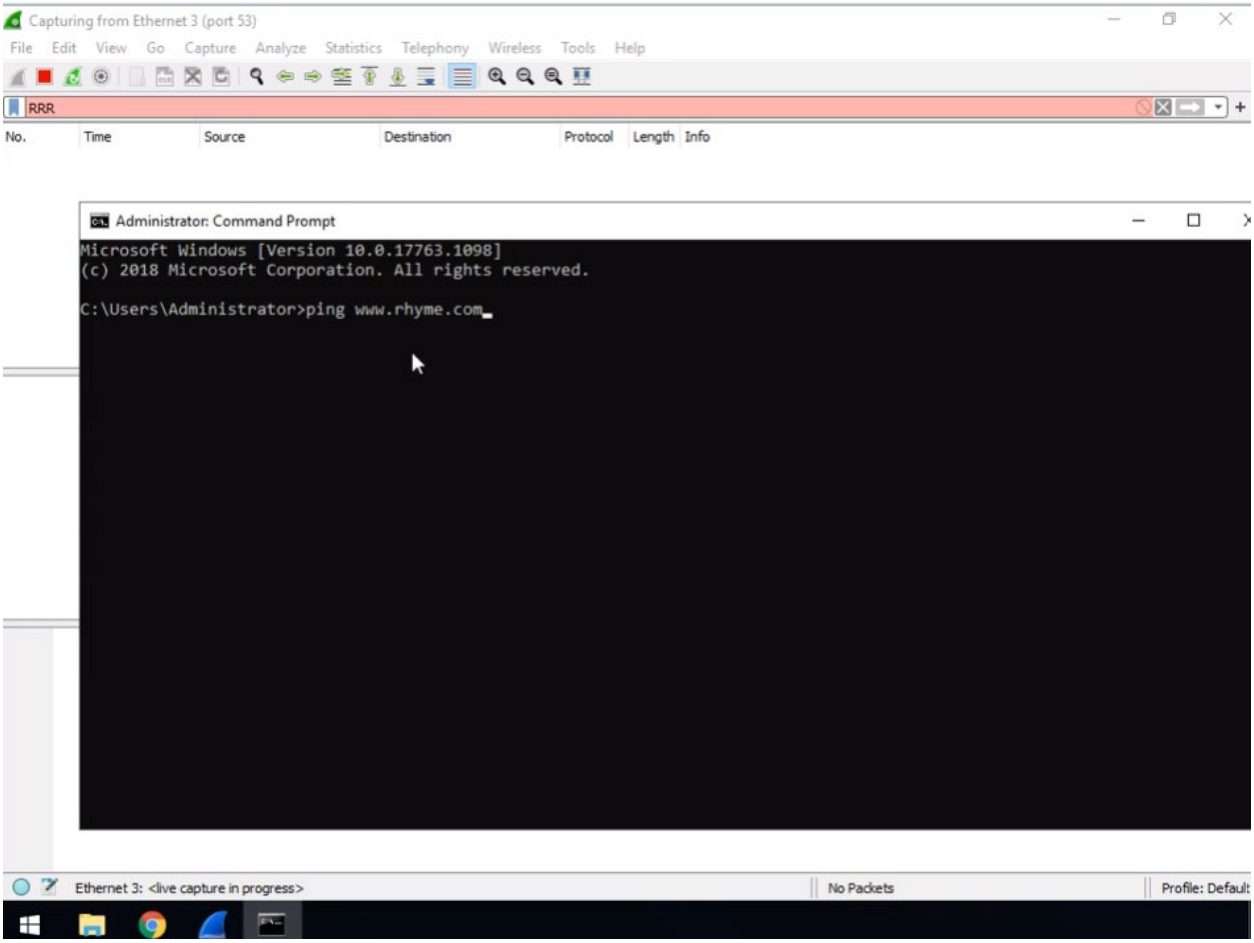

Web Scraper Testing Ground
Not secure | testing-ground.scraping.pro/login?mode=welcome
LOGIN
Often in order to reach the desired information you need to be logged in to the website. Most of today's websites use so-called form-based authentication which implies sending user credentials using POST method, authenticating it on the server and storing user's session in a cookie.
This simple test shows scraper's ability to:
1. Send user credentials via POST method
2. Receive, Keep and Return a session cookie
3. Process HTTP redirect (302)
How to test:
1. Enter admin and 12345 in the form below and press Login
2. If you see WELCOME :) then the user credentials were sent, the cookie was passed and HTTP redirect was processed
3. If you see ACCESS DENIED! then either you entered wrong credentials or they were not sent to the server properly
4. If you see THE SESSION COOKIE IS MISSING OR HAS A WRONG VALUE! then the user credentials were properly sent but the session cookie was not properly stored or passed
5. If you see REDIRECTING... then the user credentials were properly sent but HTTP redirection was not processed
6. Click GO BACK to start again
WELCOME :)
<< GO BACK
"R" is neither a field nor a protocol name.
Packets: 17 · Displayed: 17 (100.0%)
Profile: Defau

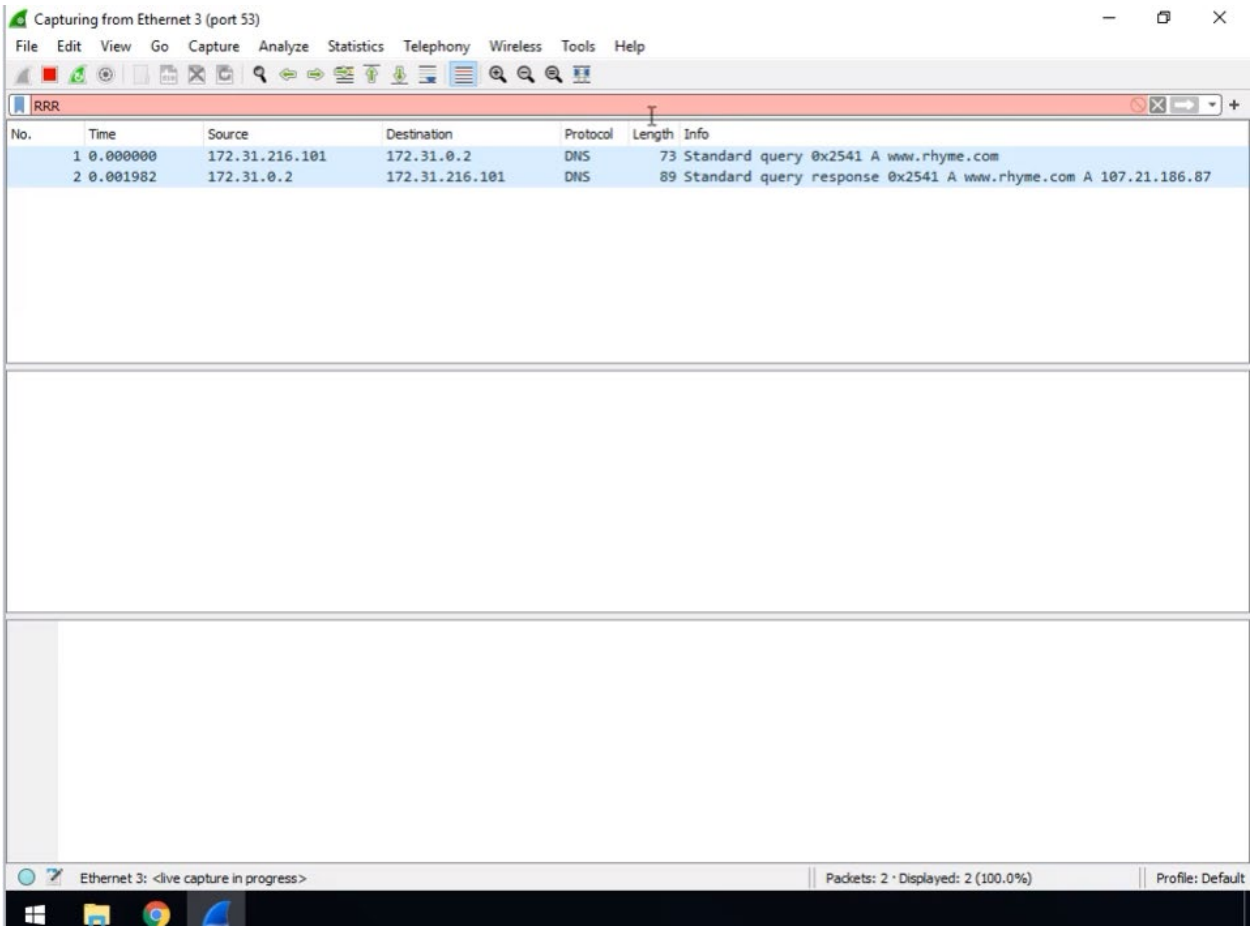

*Ethernet 3 (port 80)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.216.101 204.15.135.8 TCP 66 49745 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
2 0.000914 172.31.216.101 204.15.135.8 TCP 66 49746 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
3 0.066425 204.15.135.8 172.31.216.101 TCP 66 80 → 49745 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
4 0.066753 172.31.216.101 204.15.135.8 TCP 54 49745 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5 0.067532 172.31.216.101 204.15.135.8 HTTP 725 POST /login?mode=login HTTP/1.1 (application/x-www-form-url
6 0.067571 204.15.135.8 172.31.216.101 TCP 66 80 → 49746 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
7 0.067736 172.31.216.101 204.15.135.8 TCP 54 49746 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8 0.133963 204.15.135.8 172.31.216.101 TCP 60 80 → 49745 [ACK] Seq=1 Ack=672 Win=15968 Len=0
9 0.139155 204.15.135.8 172.31.216.101 TCP 1514 80 → 49745 [ACK] Seq=1 Ack=672 Win=15968 Len=1460 [TCP segme
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{632B7902-F0FF-488D-9F0D-C3C078B0A7C7}, id 0
Ethernet II, Src: 0a:3d:58:a2:1a:61 (0a:3d:58:a2:1a:61), Dst: 0a:d3:9e:2f:df:eb (0a:d3:9e:2f:df:eb)
Internet Protocol Version 4, Src: 172.31.216.101, Dst: 204.15.135.8
Transmission Control Protocol, Src Port: 49745, Dst Port: 80, Seq: 0, Len: 0
0000 0a d3 9e 2f df eb 0a 3d 58 a2 1a 61 08 00 45 02
0010 00 34 15 3f 40 00 80 06 00 00 ac 1f d8 65 cc 0f
0020 87 08 c2 51 00 50 6a a1 71 59 00 00 00 00 80 c2
0030 fa f0 d7 c3 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
wireshark_Ethernet 3_20200904204145_a02612.pcapng
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default


*Ethernet 3 (port 80)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.216.101 204.15.135.8 TCP 66 49745 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
2 0.000914 172.31.216.101 204.15.135.8 TCP 66 49746 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
3 0.066425 204.15.135.8 172.31.216.101 TCP 66 80 → 49745 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
4 0.066753 172.31.216.101 204.15.135.8 TCP 54 49745 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5 0.067532 172.31.216.101 204.15.135.8 HTTP 725 POST /login?mode=login HTTP/1.1 (application/x-www-form-url
6 0.067571 204.15.135.8 172.31.216.101 TCP 66 80 → 49746 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
7 0.067736 172.31.216.101 204.15.135.8 TCP 54 49746 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8 0.133963 204.15.135.8 172.31.216.101 TCP 60 80 → 49745 [ACK] Seq=1 Ack=672 Win=15968 Len=0
9 0.139155 204.15.135.8 172.31.216.101 TCP 1514 80 → 49745 [ACK] Seq=1 Ack=672 Win=15968 Len=1460 [TCP segme
Frame 5: 725 bytes on wire (5800 bits), 725 bytes captured (5800 bits) on interface \Device\NPF_{632B7902-F0FF-488D-9F0D-C3C078B0A7C7}, id 0
Ethernet II, Src: 0a:3d:58:a2:1a:61 (0a:3d:58:a2:1a:61), Dst: 0a:d3:9e:2f:df:eb (0a:d3:9e:2f:df:eb)
Internet Protocol Version 4, Src: 172.31.216.101, Dst: 204.15.135.8
Transmission Control Protocol, Src Port: 49745, Dst Port: 80, Seq: 1, Ack: 1, Len: 671
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 0a d3 9e 2f df eb 0a 3d 58 a2 1a 61 08 00 45 02
0010 02 c7 15 42 40 00 80 06 00 00 ac 1f d8 65 cc 0f
0020 87 08 c2 51 00 50 6a a1 71 5a 6d 66 c9 1b 50 18
0030 04 02 da 56 00 00 50 4f 53 54 20 2f 6c 6f 67 69
0040 6e 3f 6d 6f 64 65 3d 6c 6f 67 69 6e 20 48 54 54
0050 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73
0060 74 69 6e 67 2d 67 72 6f 75 6e 64 2e 73 63 72 61
0070 70 69 6e 67 2e 70 72 6f 0d 0a 43 6f 6e 6e 65 63
0080 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65
0090 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68
00a0 3a 20 31 39 0d 0a 43 61 63 68 65 2d 43 6f 6e 74
00b0 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a
00c0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65
wireshark_Ethernet 3_20200904204145_a02612.pcapng
Packets: 19 · Displayed: 19 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


*Ethernet 3 (port 80)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.216.101 204.15.135.8 TCP 66 49745 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
2 0.000914 172.31.216.101 204.15.135.8 TCP 66 49746 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
3 0.066425 204.15.135.8 172.31.216.101 TCP 66 80 → 49745 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
4 0.066753 172.31.216.101 204.15.135.8 TCP 54 49745 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5 0.067532 172.31.216.101 204.15.135.8 HTTP 725 POST /login?mode=login HTTP/1.1 (application/x-www-form-url
6 0.067571 204.15.135.8 172.31.216.101 TCP 66 80 → 49746 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
7 0.067736 172.31.216.101 204.15.135.8 TCP 54 49746 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8 0.133963 204.15.135.8 172.31.216.101 TCP 60 80 → 49745 [ACK] Seq=1 Ack=672 Win=15968 Len=0
9 0.139155 204.15.135.8 172.31.216.101 TCP 1514 80 → 49745 [ACK] Seq=1 Ack=672 Win=15968 Len=1460 [TCP segme
Frame 5: 725 bytes on wire (5800 bits), 725 bytes captured (5800 bits) on interface \Device\NPF_{632B7902-F0FF-488D-9F0D-C3C078B0A7C7}, id 0
Ethernet II, Src: 0a:3d:58:a2:1a:61 (0a:3d:58:a2:1a:61), Dst: 0a:d3:9e:2f:df:eb (0a:d3:9e:2f:df:eb)
Internet Protocol Version 4, Src: 172.31.216.101, Dst: 204.15.135.8
Transmission Control Protocol, Src Port: 49745, Dst Port: 80, Seq: 1, Ack: 1, Len: 671
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "usr" = "admin"
Form item: "pwd" = "12345"
0000 0a d3 9e 2f df eb 0a 3d 58 a2 1a 61 08 00 45 02
0010 02 c7 15 42 40 00 80 06 00 00 ac 1f d8 65 cc 0f
0020 87 08 c2 51 00 50 6a a1 71 5a 6d 66 c9 1b 50 18
0030 04 02 da 56 00 00 50 4f 53 54 20 2f 6c 6f 67 69
0040 6e 3f 6d 6f 64 65 3d 6c 6f 67 69 6e 20 48 54 54
0050 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73
0060 74 69 6e 67 2d 67 72 6f 75 6e 64 2e 73 63 72 61
0070 70 69 6e 67 2e 70 72 6f 0d 0a 43 6f 6e 6e 65 63
0080 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65
0090 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68
00a0 3a 20 31 39 0d 0a 43 61 63 68 65 2d 43 6f 6e 74
00b0 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a
00c0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65
wireshark_Ethernet 3_20200904204145_a02612.pcapng
Packets: 19 · Displayed: 19 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

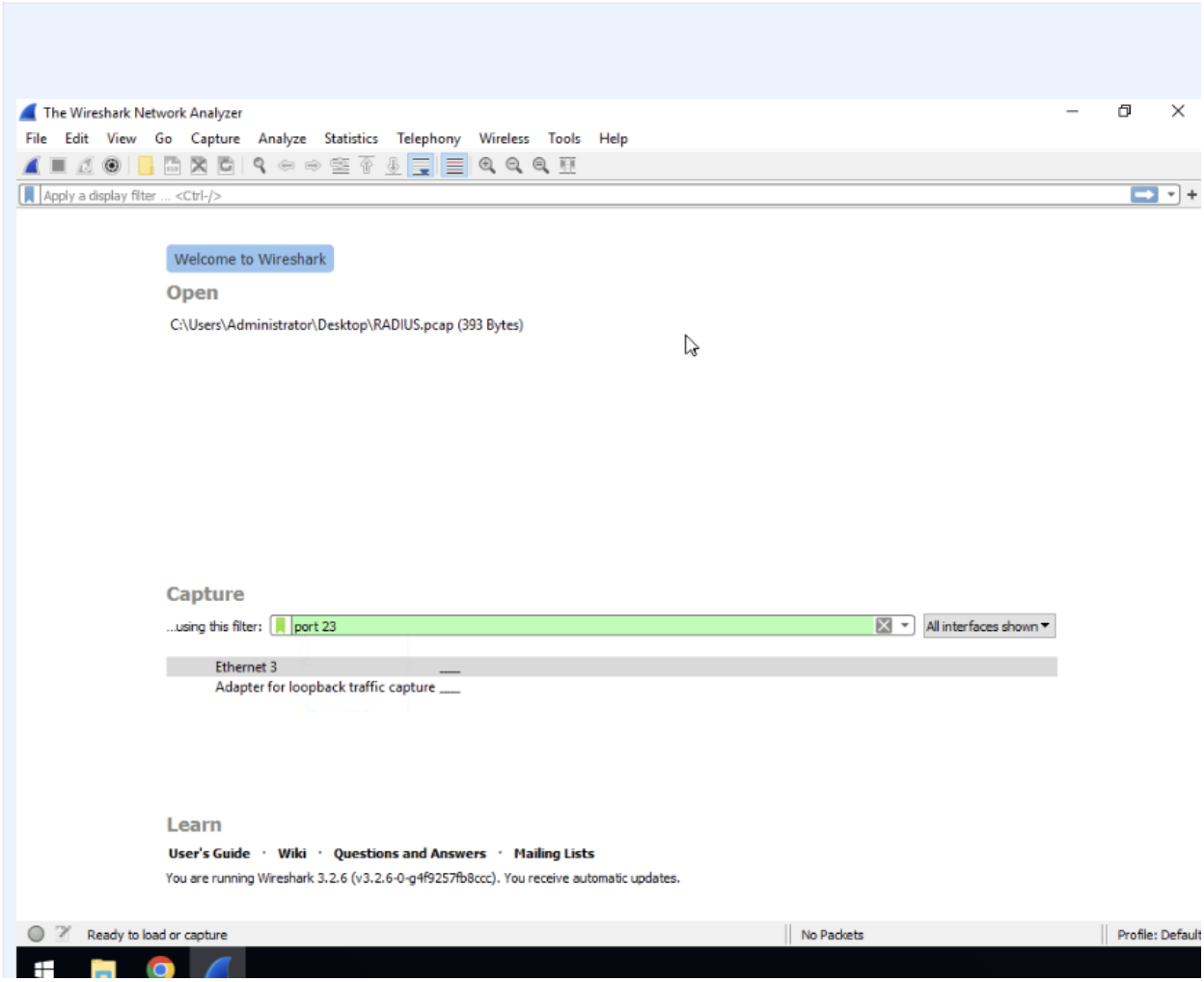

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
RRR
Welcome to Wireshark
Open
C:\Users\Administrator\Desktop\RADIUS.pcap (393 Bytes)
Capture
...using this filter:
port 53
All interfaces shown
Ethernet 3
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

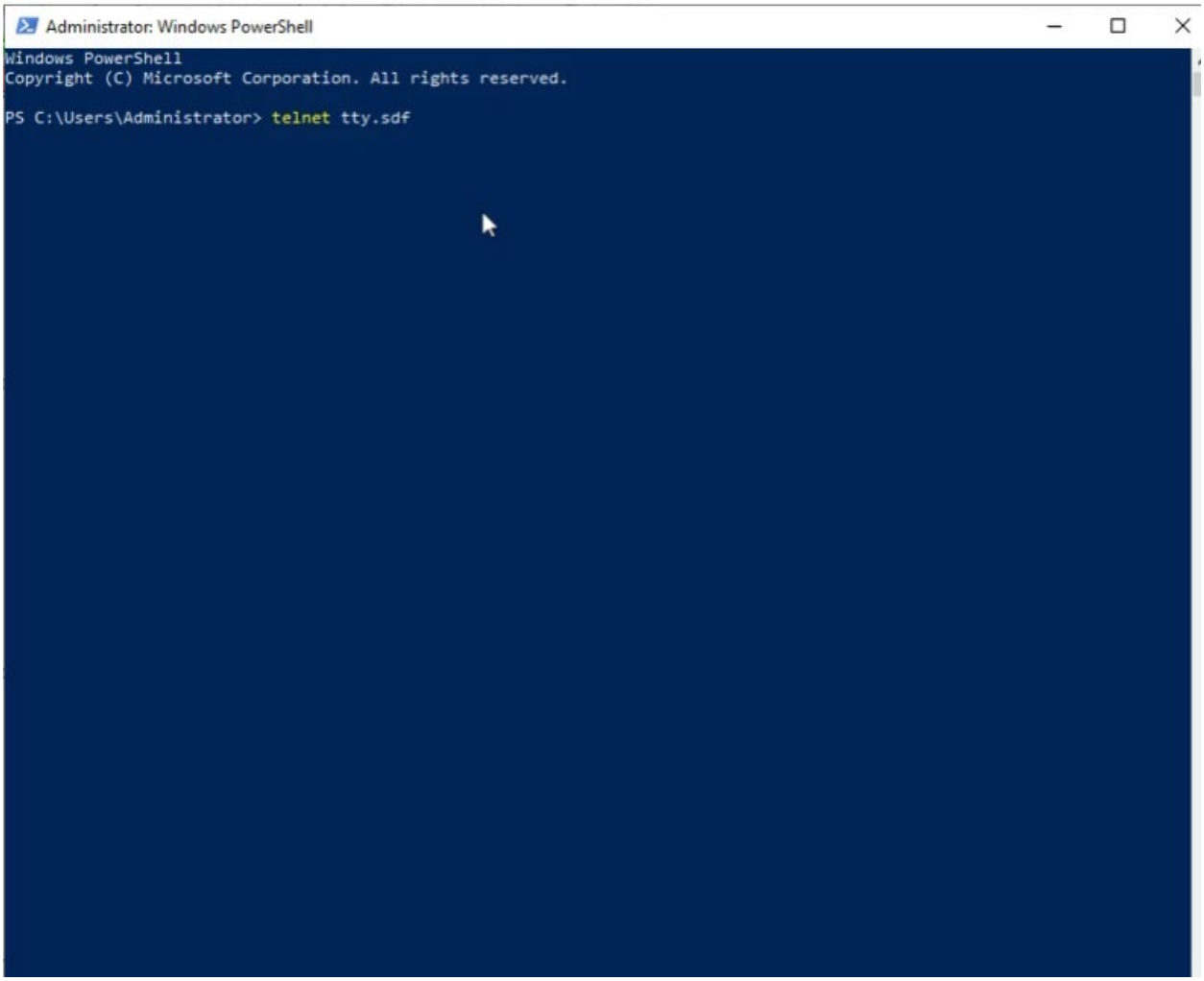

Capturing from Ethernet 3 (port 53)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
RRR
No. Time Source Destination Protocol Length Info
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping www.rhyme.com
Ethernet 3: <live capture in progress>
No Packets
Profile: Default

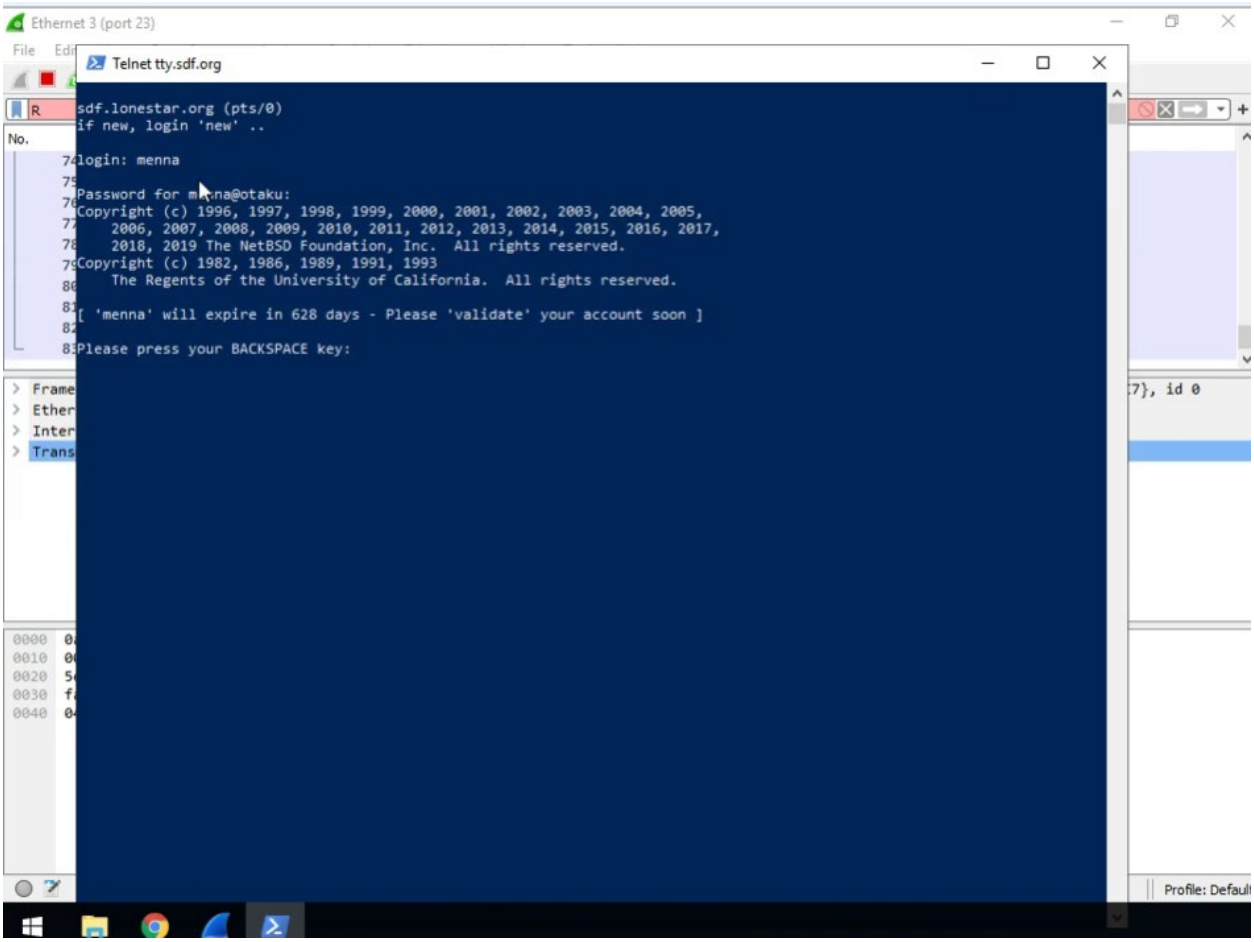


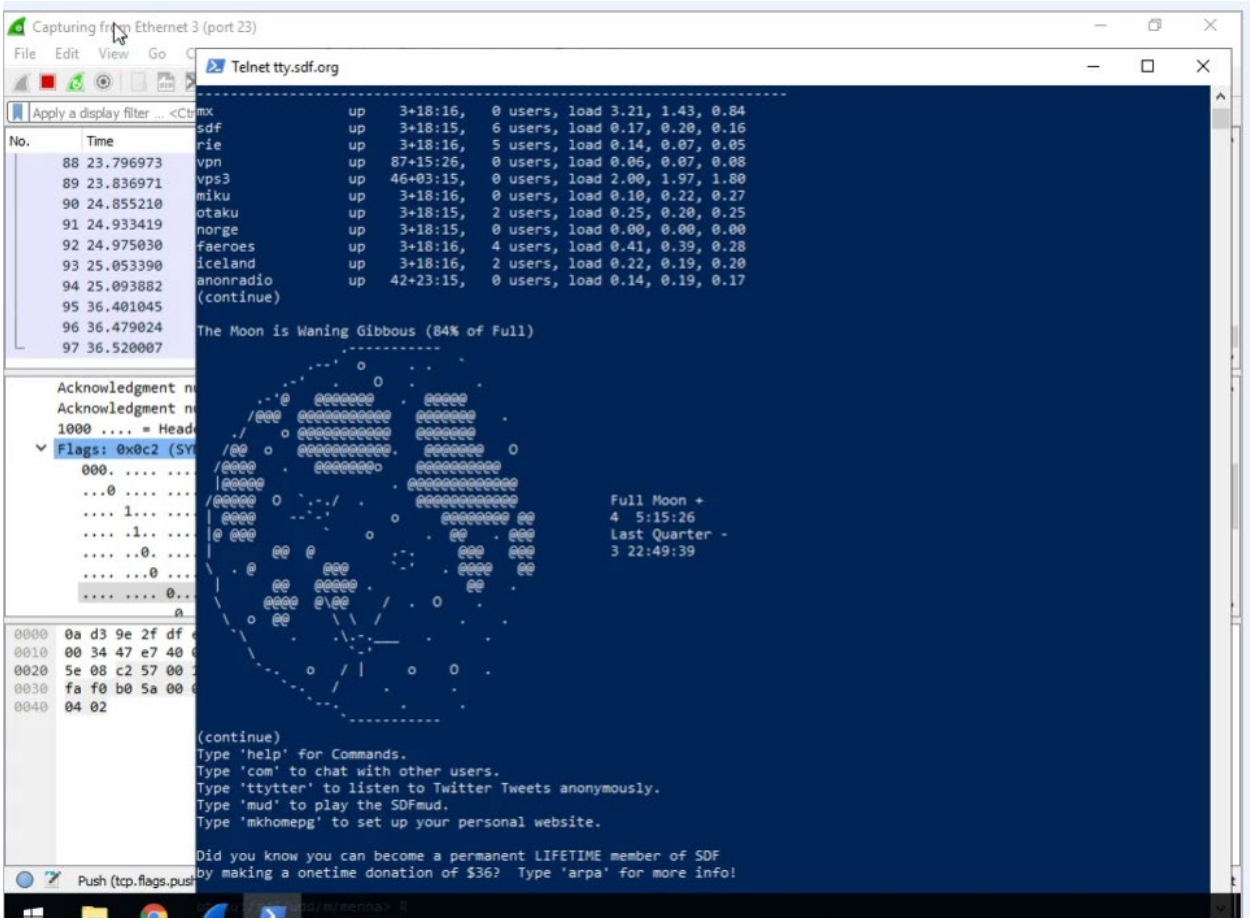
Task 5: Initiate, Capture and Analyze Telnet Sessions

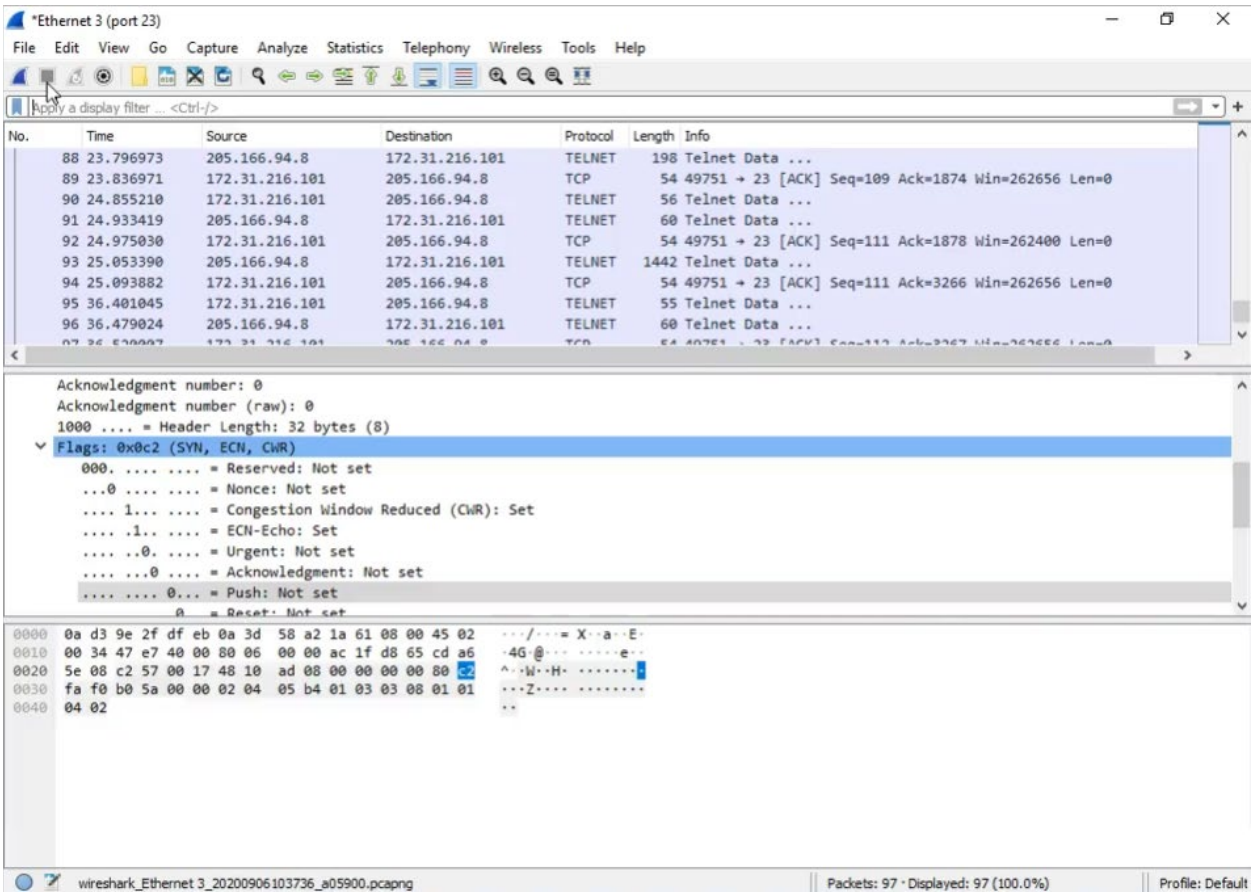

SDF Public Access UNIX System
Not secure
tty.sdf.org
[SDF Public Access UNIX System .. Est. 1987]
join welcome faq status members projects store tour gopher abuse dialup minecraft social
tilde nihongo europa webmail gallery usermap irc tutorials telnet git ssh
-=- a community platform for inspiring, facilitating and implementing new ideas -=-
Create a Free UNIX Shell Account
Your E-Mail:
Preferred Login:
Confirm
Alternative methods
MacOS X users, click here: ssh://new@sdf.org
Web Browser users may use our HTML5 SSH client: https://ssh.sdf.org
Linux/UNIX users can type 'ssh new@sdf.org' at their shell prompts.
For Microsoft Windows we highly recommend the free SSH client putty.exe.
If you have any questions or cannot figure out how to use SSH, live help
is available on IRC via irc.sdf.org in the #helpdesk channel.
Make a Donation
Please be sure fill in the description
with your login and membership option.
©1987-2065 SDF Public Access UNIX System, Inc. 501(c)(7)
(this page was generated using ksh, sed and awk)

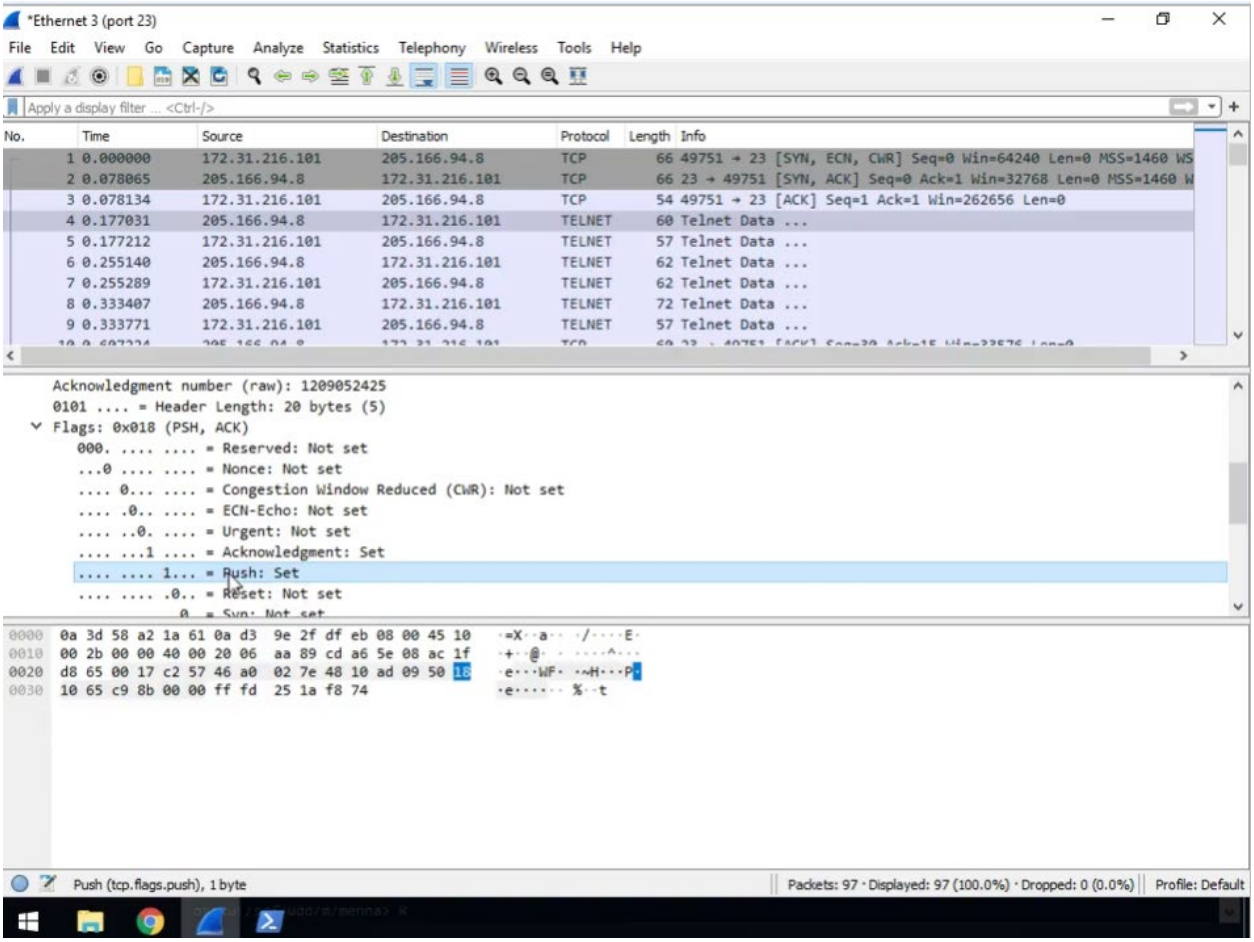

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\Administrator\Desktop\RADIUS.pcap (393 Bytes)
Capture
...using this filter: port 23
All interfaces shown
Ethernet 3
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

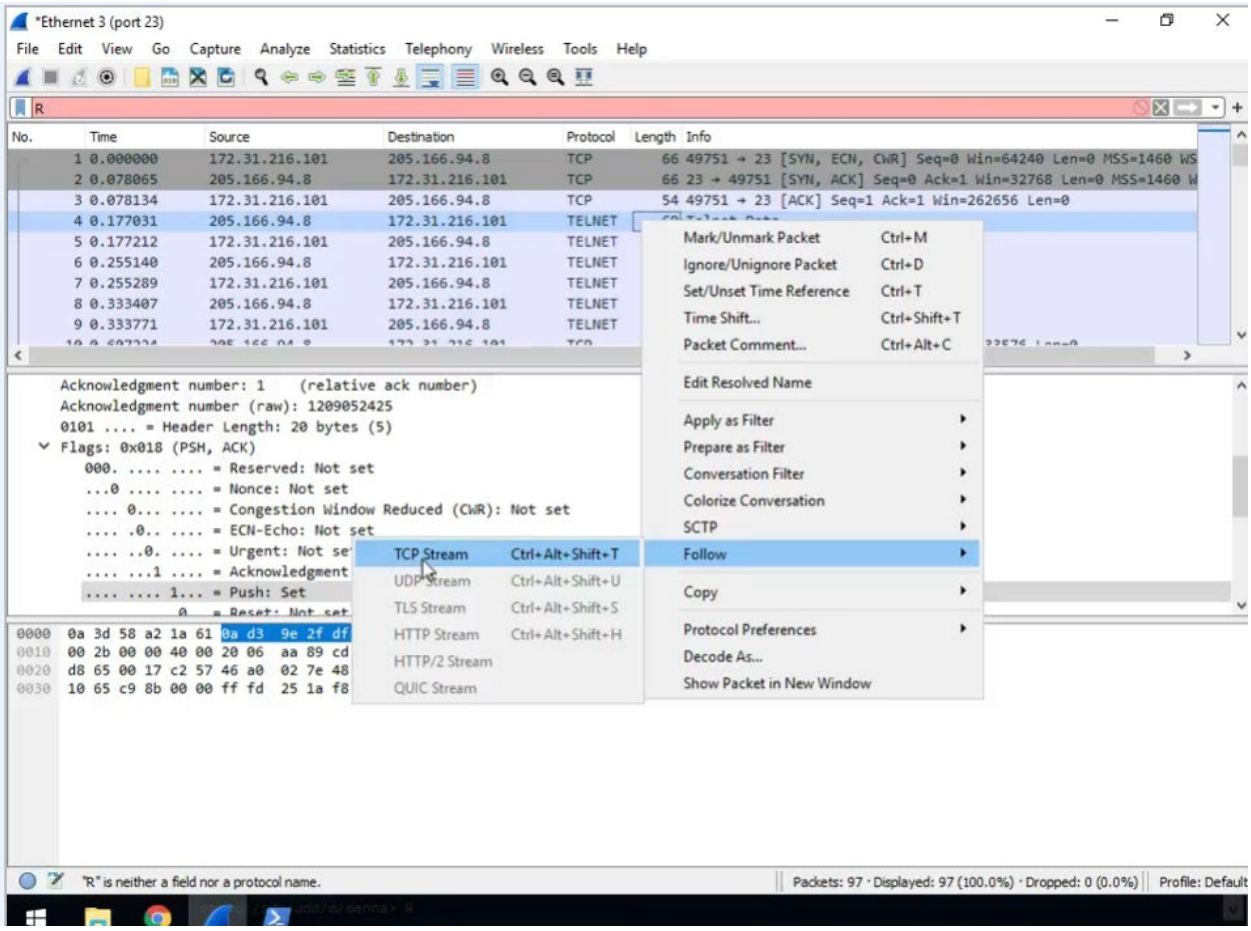

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> telnet tty.sdf

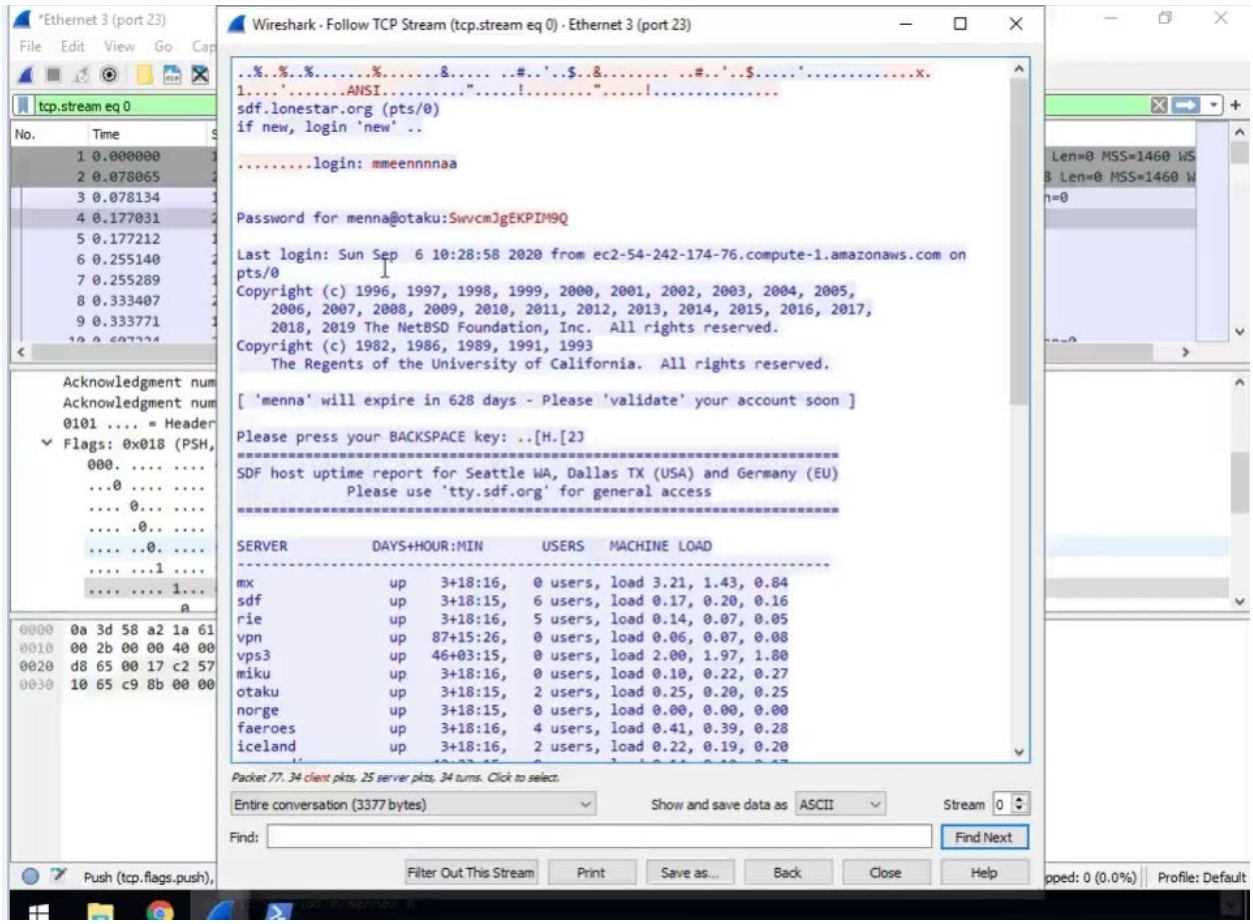

Ethernet 3 (port 23)
File
Telnet tty.sdf.org
sdf.lonestar.org (pts/0)
if new, login 'new' ..
login: menna
Password for menna@otaku:
Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005,
2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017,
2018, 2019 The NetBSD Foundation, Inc. All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
The Regents of the University of California. All rights reserved.
['menna' will expire in 628 days - Please 'validate' your account soon]
Please press your BACKSPACE key:
No.
Profile: Default

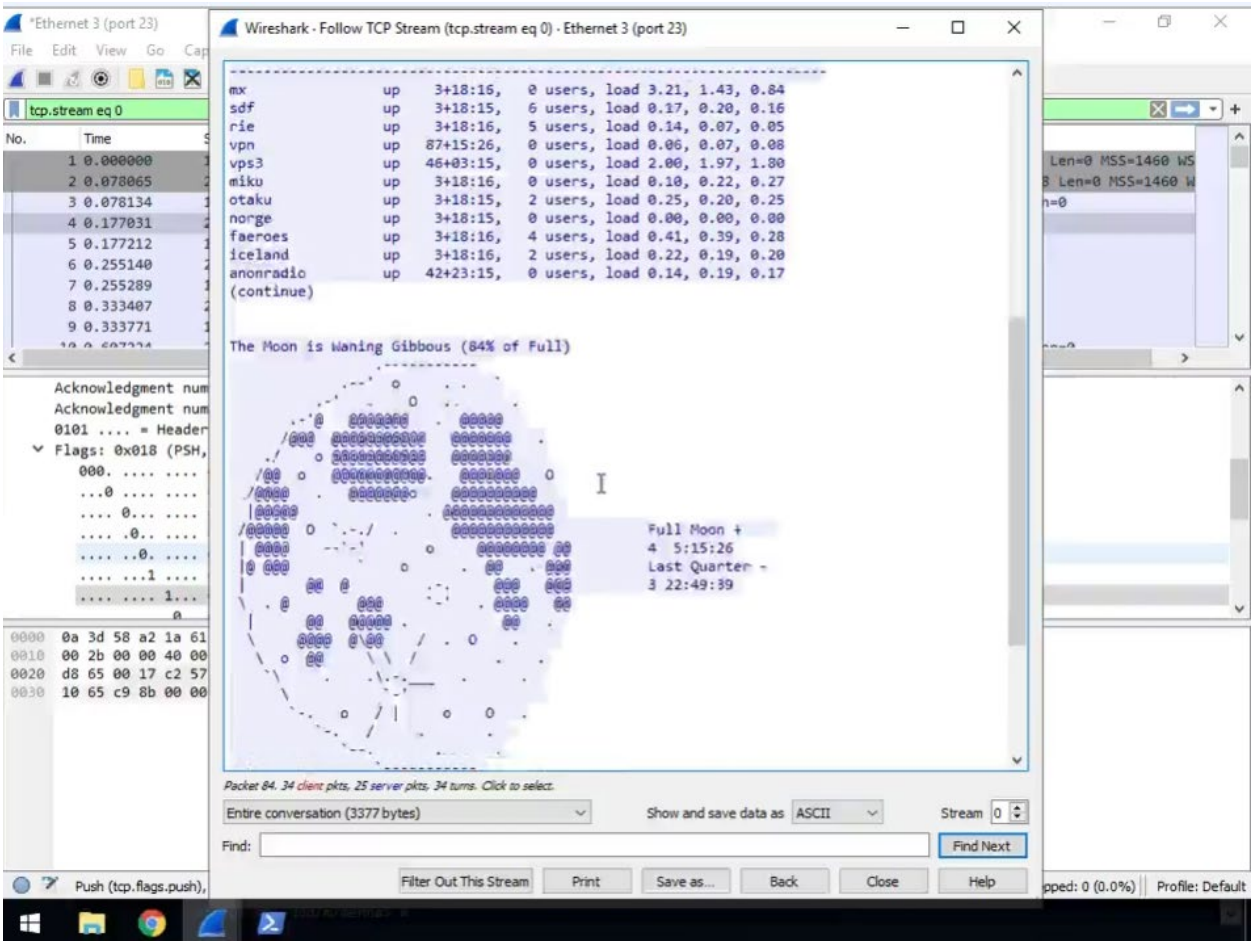

Capturing from Ethernet 3 (port 23)
File Edit View Go
Apply a display filter ... <Ctl
No. Time
88 23.796973
89 23.836971
90 24.855210
91 24.933419
92 24.975030
93 25.053390
94 25.093882
95 36.401045
96 36.479024
97 36.520007
Acknowledgment nu
Acknowledgment nu
1000 .... = Head
Flags: 0x0c2 (SY
000. ....
...0 ....
.... 1... ....
.... .1.. ....
.... ..0. ....
....0 ....
.... 0..
0000 0a d3 9e 2f df
0010 00 34 47 e7 40
0020 5e 08 c2 57 00
0030 fa f0 b0 5a 00
0040 04 02
Push (tcp.flags.push
Telnet tty.sdf.org
mx up 3+18:16, 0 users, load 3.21, 1.43, 0.84
sdf up 3+18:15, 6 users, load 0.17, 0.20, 0.16
rie up 3+18:16, 5 users, load 0.14, 0.07, 0.05
vpn up 87+15:26, 0 users, load 0.06, 0.07, 0.08
vps3 up 46+03:15, 0 users, load 2.00, 1.97, 1.80
miku up 3+18:16, 0 users, load 0.10, 0.22, 0.27
otaku up 3+18:15, 2 users, load 0.25, 0.20, 0.25
norge up 3+18:15, 0 users, load 0.00, 0.00, 0.00
faeroes up 3+18:16, 4 users, load 0.41, 0.39, 0.28
iceland up 3+18:16, 2 users, load 0.22, 0.19, 0.20
anonradio up 42+23:15, 0 users, load 0.14, 0.19, 0.17
(continue)
The Moon is Waning Gibbous (84% of Full)
Full Moon +
4 5:15:26
Last Quarter -
3 22:49:39
(continue)
Type 'help' for Commands.
Type 'com' to chat with other users.
Type 'ttytter' to listen to Twitter Tweets anonymously.
Type 'mud' to play the SDFmud.
Type 'mkhomepg' to set up your personal website.
Did you know you can become a permanent LIFETIME member of SDF
by making a onetime donation of $36? Type 'arpa' for more info!


*Ethernet 3 (port 23)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
88 23.796973 205.166.94.8 172.31.216.101 TELNET 198 Telnet Data ...
89 23.836971 172.31.216.101 205.166.94.8 TCP 54 49751 → 23 [ACK] Seq=109 Ack=1874 Win=262656 Len=0
90 24.855210 172.31.216.101 205.166.94.8 TELNET 56 Telnet Data ...
91 24.933419 205.166.94.8 172.31.216.101 TELNET 60 Telnet Data ...
92 24.975030 172.31.216.101 205.166.94.8 TCP 54 49751 → 23 [ACK] Seq=111 Ack=1878 Win=262400 Len=0
93 25.053390 205.166.94.8 172.31.216.101 TELNET 1442 Telnet Data ...
94 25.093882 172.31.216.101 205.166.94.8 TCP 54 49751 → 23 [ACK] Seq=111 Ack=3266 Win=262656 Len=0
95 36.401045 172.31.216.101 205.166.94.8 TELNET 55 Telnet Data ...
96 36.479024 205.166.94.8 172.31.216.101 TELNET 60 Telnet Data ...
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x0c2 (SYN, ECN, CWR)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 1... .... = Congestion Window Reduced (CWR): Set
.... .1.. .... = ECN-Echo: Set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
0000 0a d3 9e 2f df eb 0a 3d 58 a2 1a 61 08 00 45 02
0010 00 34 47 e7 40 00 80 06 00 00 ac 1f d8 65 cd a6
0020 5e 08 c2 57 00 17 48 10 ad 08 00 00 00 00 80 c2
0030 fa f0 b0 5a 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
wireshark_Ethernet 3_20200906103736_a05900.pcapng
Packets: 97 · Displayed: 97 (100.0%)
Profile: Default

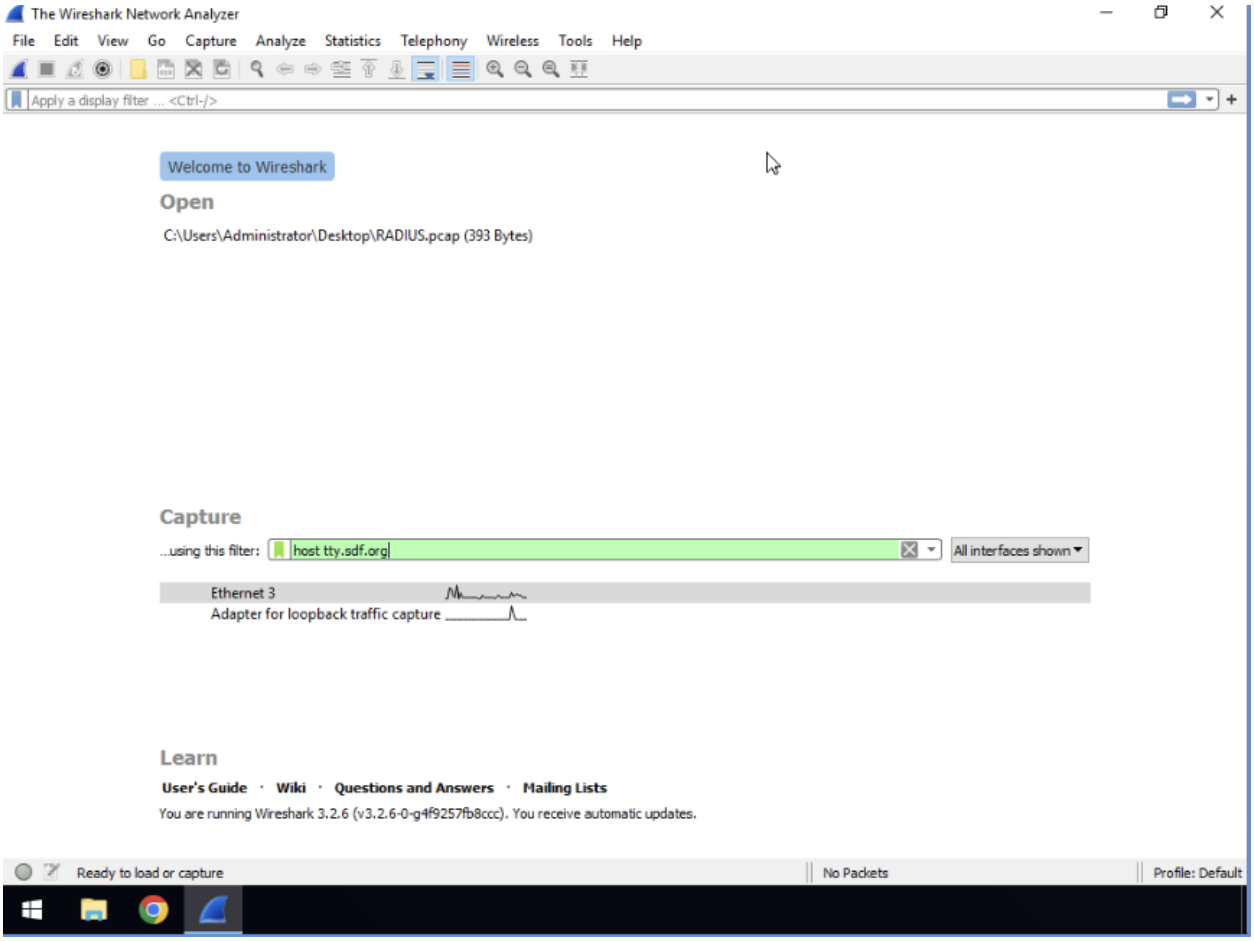

*Ethernet 3 (port 23)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.216.101 205.166.94.8 TCP 66 49751 → 23 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
2 0.078065 205.166.94.8 172.31.216.101 TCP 66 23 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 W
3 0.078134 172.31.216.101 205.166.94.8 TCP 54 49751 → 23 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4 0.177031 205.166.94.8 172.31.216.101 TELNET 60 Telnet Data ...
5 0.177212 172.31.216.101 205.166.94.8 TELNET 57 Telnet Data ...
6 0.255140 205.166.94.8 172.31.216.101 TELNET 62 Telnet Data ...
7 0.255289 172.31.216.101 205.166.94.8 TELNET 62 Telnet Data ...
8 0.333407 205.166.94.8 172.31.216.101 TELNET 72 Telnet Data ...
9 0.333771 172.31.216.101 205.166.94.8 TELNET 57 Telnet Data ...
Acknowledgment number (raw): 1209052425
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
0000 0a 3d 58 a2 1a 61 0a d3 9e 2f df eb 08 00 45 10
0010 00 2b 00 00 40 00 20 06 aa 89 cd a6 5e 08 ac 1f
0020 d8 65 00 17 c2 57 46 a0 02 7e 48 10 ad 09 50 18
0030 10 65 c9 8b 00 00 ff fd 25 1a f8 74
Push (tcp.flags.push), 1 byte
Packets: 97 · Displayed: 97 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

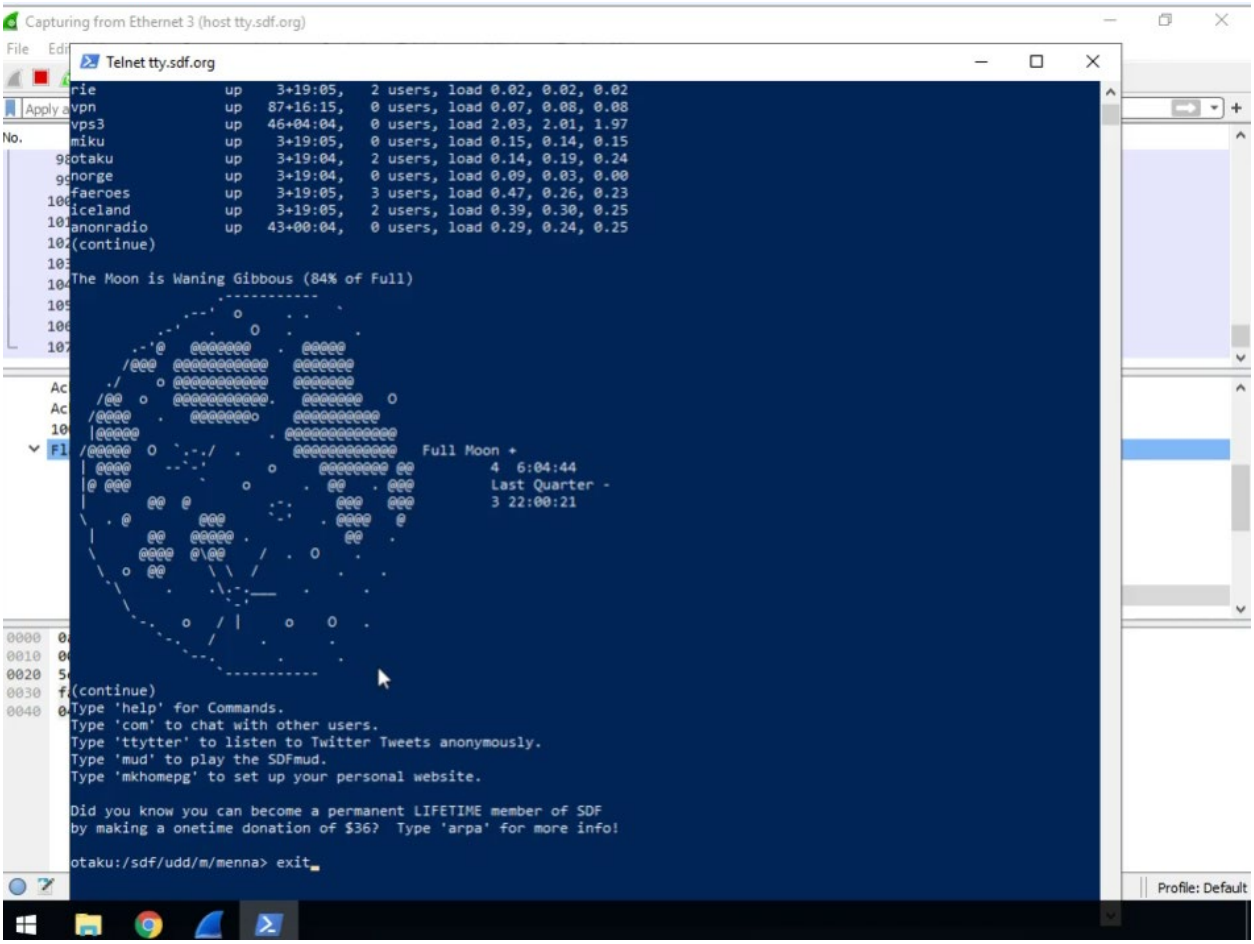

*Ethernet 3 (port 23)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.216.101 205.166.94.8 TCP 66 49751 → 23 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS
2 0.078065 205.166.94.8 172.31.216.101 TCP 66 23 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 W
3 0.078134 172.31.216.101 205.166.94.8 TCP 54 49751 → 23 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4 0.177031 205.166.94.8 172.31.216.101 TELNET
5 0.177212 172.31.216.101 205.166.94.8 TELNET
6 0.255140 205.166.94.8 172.31.216.101 TELNET
7 0.255289 172.31.216.101 205.166.94.8 TELNET
8 0.333407 205.166.94.8 172.31.216.101 TELNET
9 0.333771 172.31.216.101 205.166.94.8 TELNET
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1209052425
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment
.... 1... = Push: Set
0 = Reset: Not set
0000 0a 3d 58 a2 1a 61 0a d3 9e 2f df
0010 00 2b 00 00 40 00 20 06 aa 89 cd
0020 d8 65 00 17 c2 57 46 a0 02 7e 48
0030 10 65 c9 8b 00 00 ff fd 25 1a f8
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
"R" is neither a field nor a protocol name.
Packets: 97 · Displayed: 97 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

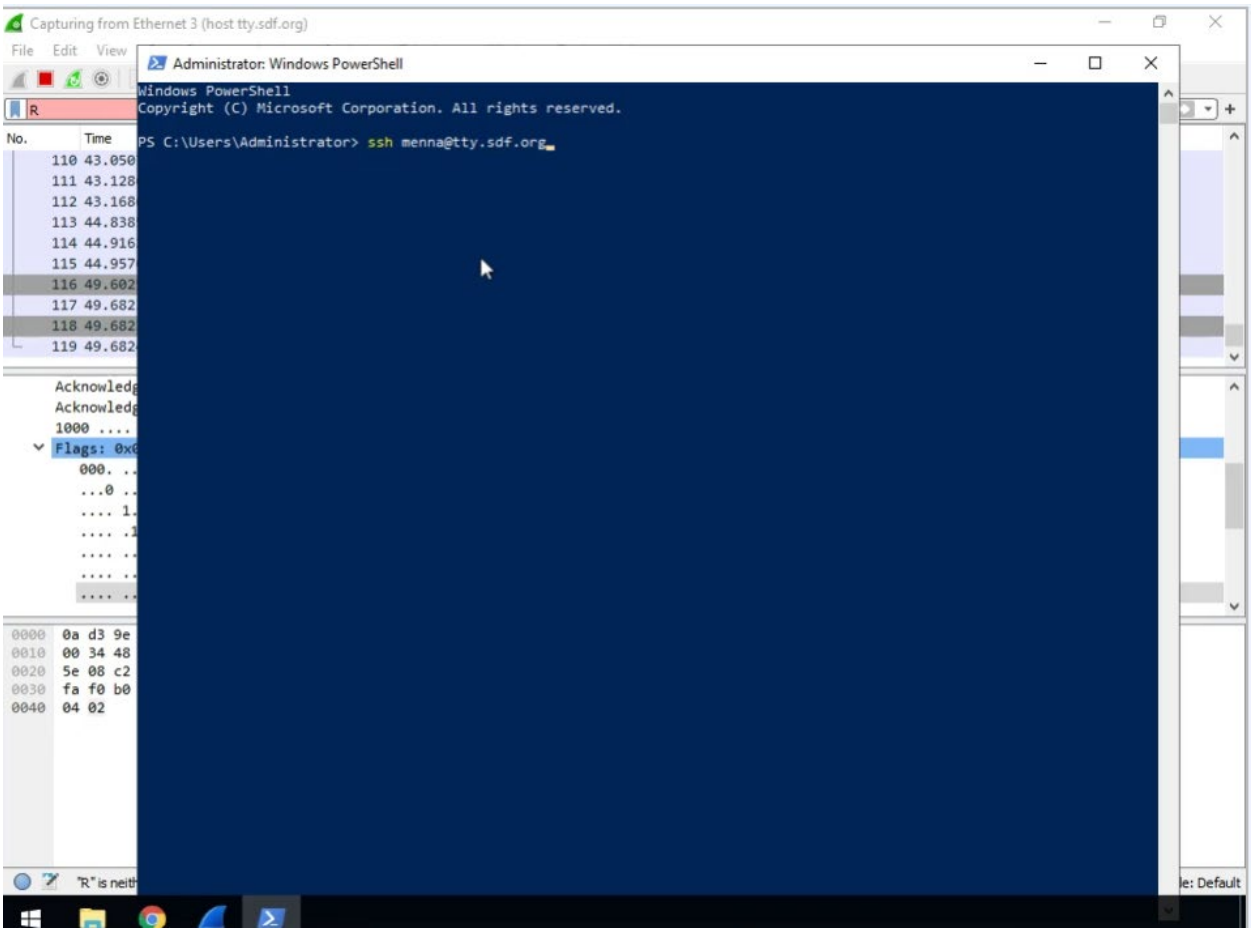

*Ethernet 3 (port 23)
File Edit View Go Cap
tcp.stream eq 0
No. Time
1 0.000000
2 0.078065
3 0.078134
4 0.177031
5 0.177212
6 0.255140
7 0.255289
8 0.333407
9 0.333771
Acknowledgment num
Acknowledgment num
0101 .... = Header
Flags: 0x018 (PSH,
000. ....
...0 ....
.... 0... ....
.... .0.. ....
.... ..0. ....
....1 ....
.... 1...
0000 0a 3d 58 a2 1a 61
0010 00 2b 00 00 40 00
0020 d8 65 00 17 c2 57
0030 10 65 c9 8b 00 00
Push (tcp.flags.push),
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet 3 (port 23)
..%..%..%.....%.....&..... ..#..'..$..&..... ..#..'..$.....'.....x.
1....'.....ANSI.....".....!....."....."....!.....
sdf.lonestar.org (pts/0)
if new, login 'new' ..
.....login: mmeennnnaa
Password for menna@otaku:SwvcmJgEKPIM9Q
Last login: Sun Sep 6 10:28:58 2020 from ec2-54-242-174-76.compute-1.amazonaws.com on
pts/0
Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005,
2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017,
2018, 2019 The NetBSD Foundation, Inc. All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
The Regents of the University of California. All rights reserved.
['menna' will expire in 628 days - Please 'validate' your account soon]
Please press your BACKSPACE key: ..[H.[2J
SDF host uptime report for Seattle WA, Dallas TX (USA) and Germany (EU)
Please use 'tty.sdf.org' for general access
SERVER DAYS+HOUR:MIN USERS MACHINE LOAD
mx up 3+18:16, 0 users, load 3.21, 1.43, 0.84
sdf up 3+18:15, 6 users, load 0.17, 0.20, 0.16
rie up 3+18:16, 5 users, load 0.14, 0.07, 0.05
vpn up 87+15:26, 0 users, load 0.06, 0.07, 0.08
vps3 up 46+03:15, 0 users, load 2.00, 1.97, 1.80
miku up 3+18:16, 0 users, load 0.10, 0.22, 0.27
otaku up 3+18:15, 2 users, load 0.25, 0.20, 0.25
norge up 3+18:15, 0 users, load 0.00, 0.00, 0.00
faeroes up 3+18:16, 4 users, load 0.41, 0.39, 0.28
iceland up 3+18:16, 2 users, load 0.22, 0.19, 0.20
Packet 77. 34 client pkts, 25 server pkts, 34 turns. Click to select.
Entire conversation (3377 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Len=0 MSS=1460 WS
Len=0 MSS=1460 W
Profile: Default

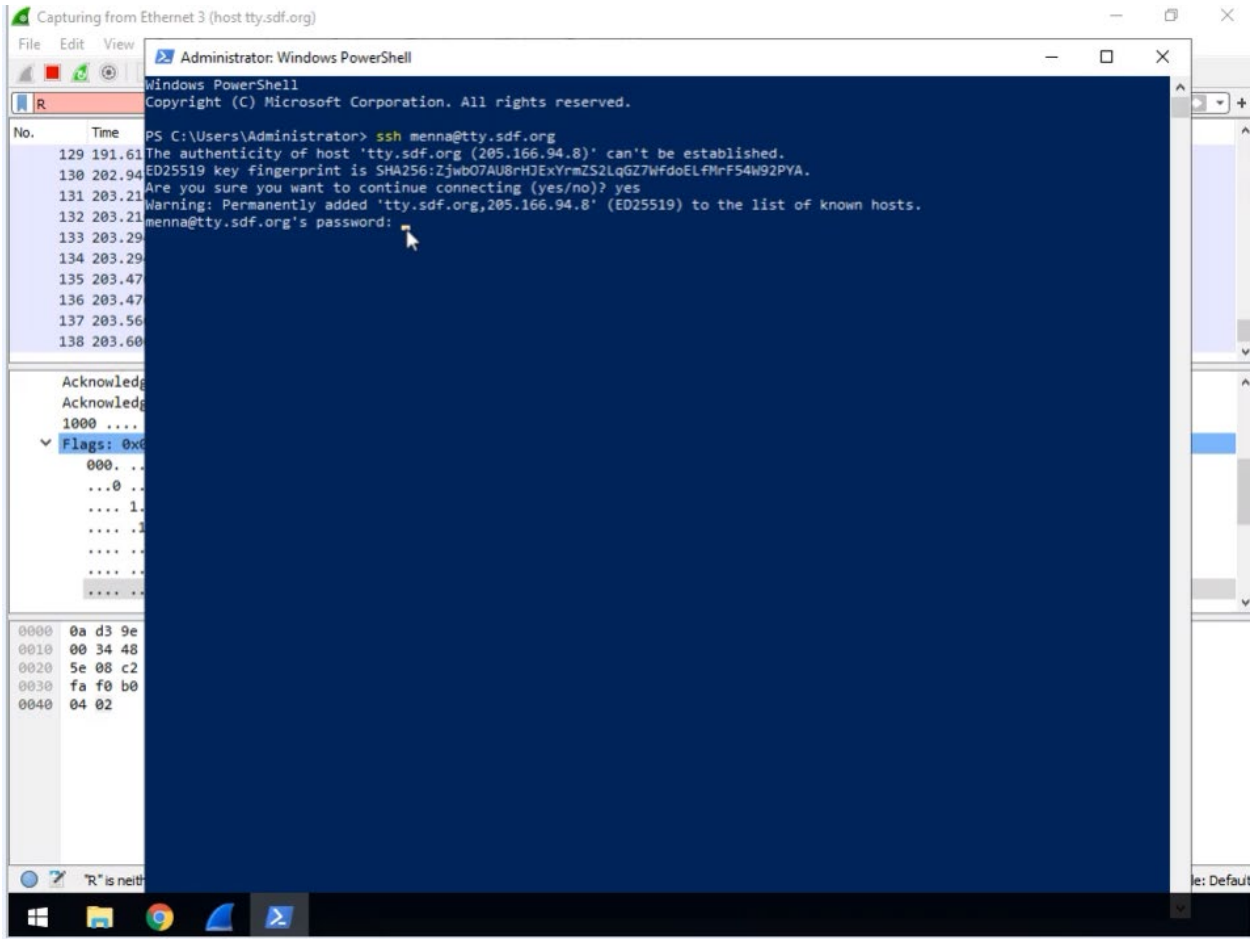


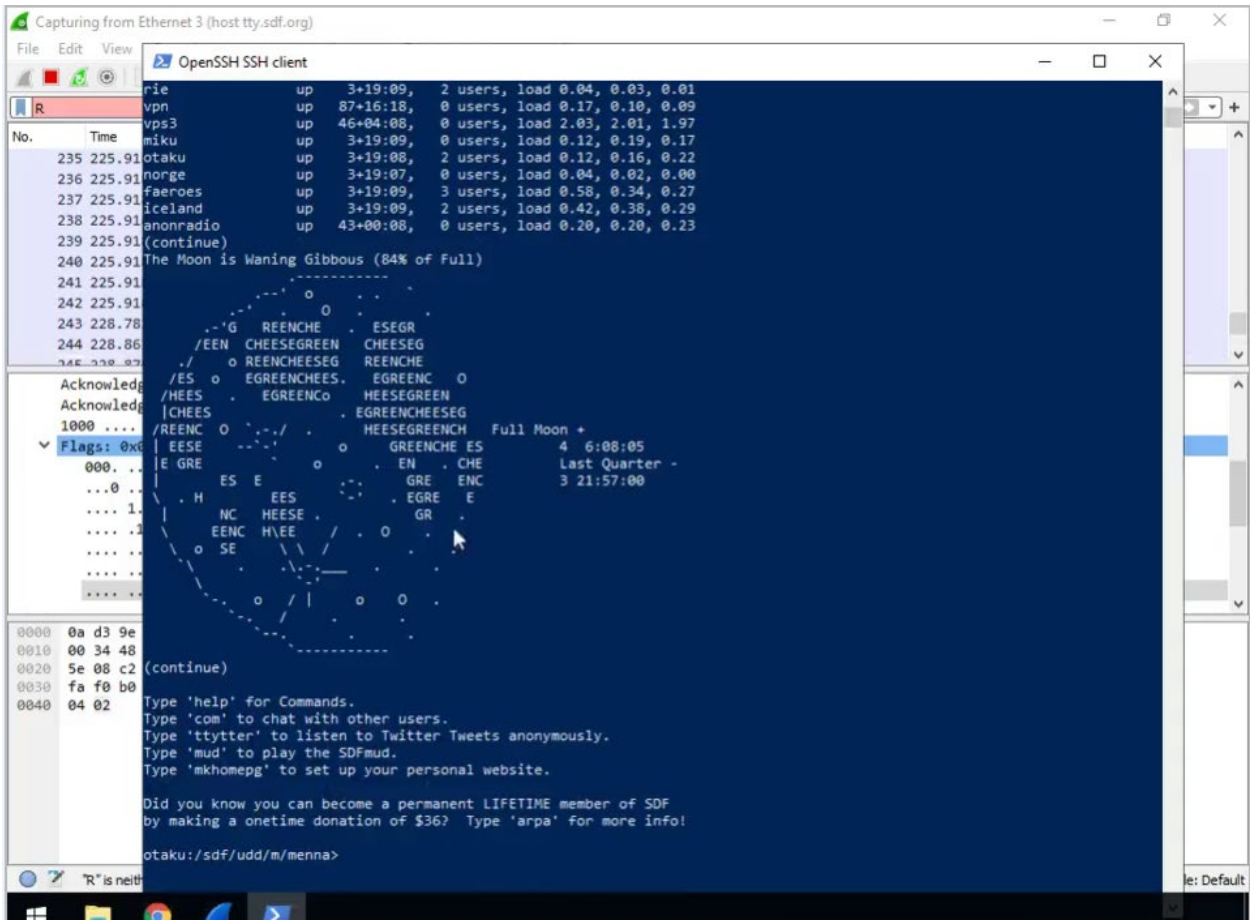
Task 6: Capturing and Analyzing SSH Sessions

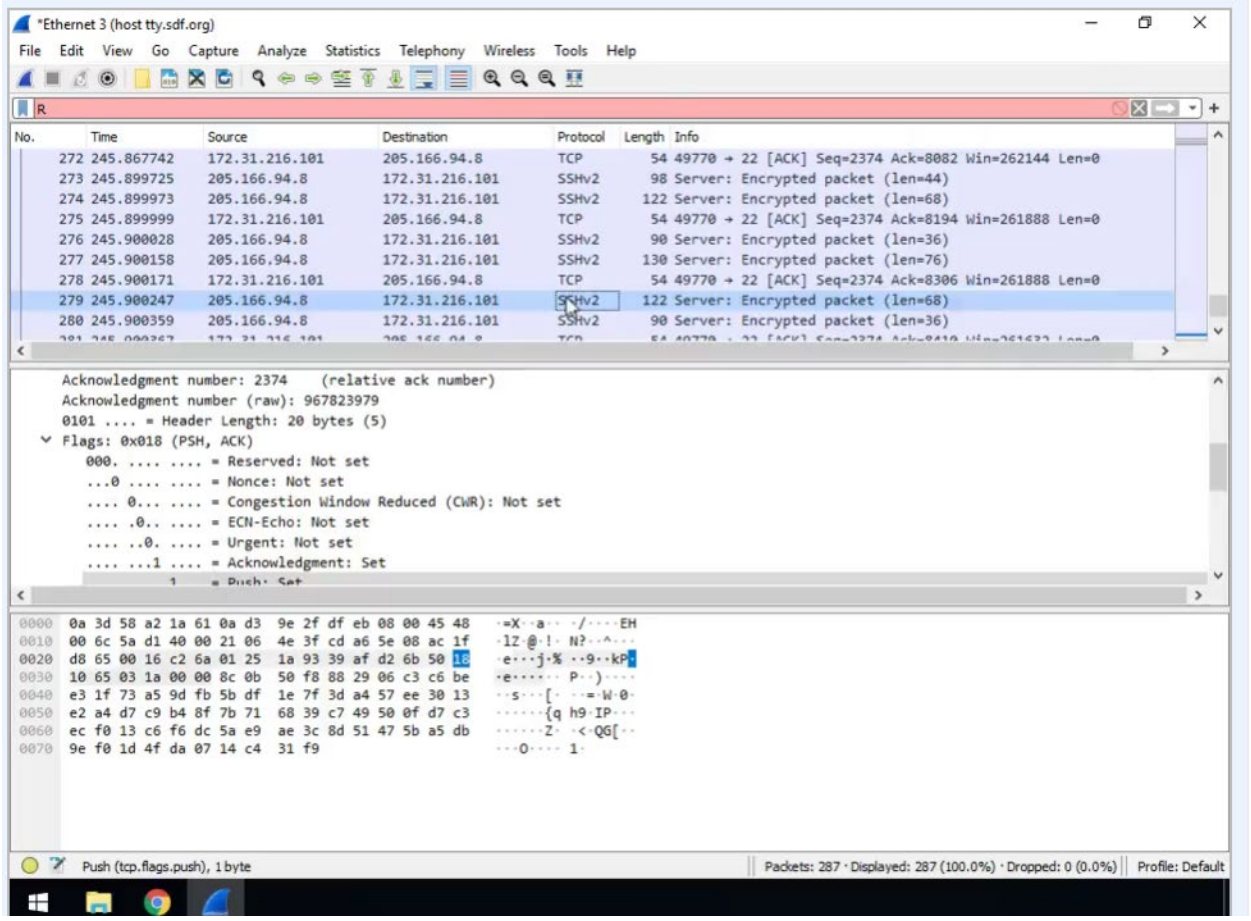

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\Administrator\Desktop\RADIUS.pcap (393 Bytes)
Capture
...using this filter: host tty.sdf.org
All interfaces shown
Ethernet 3
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

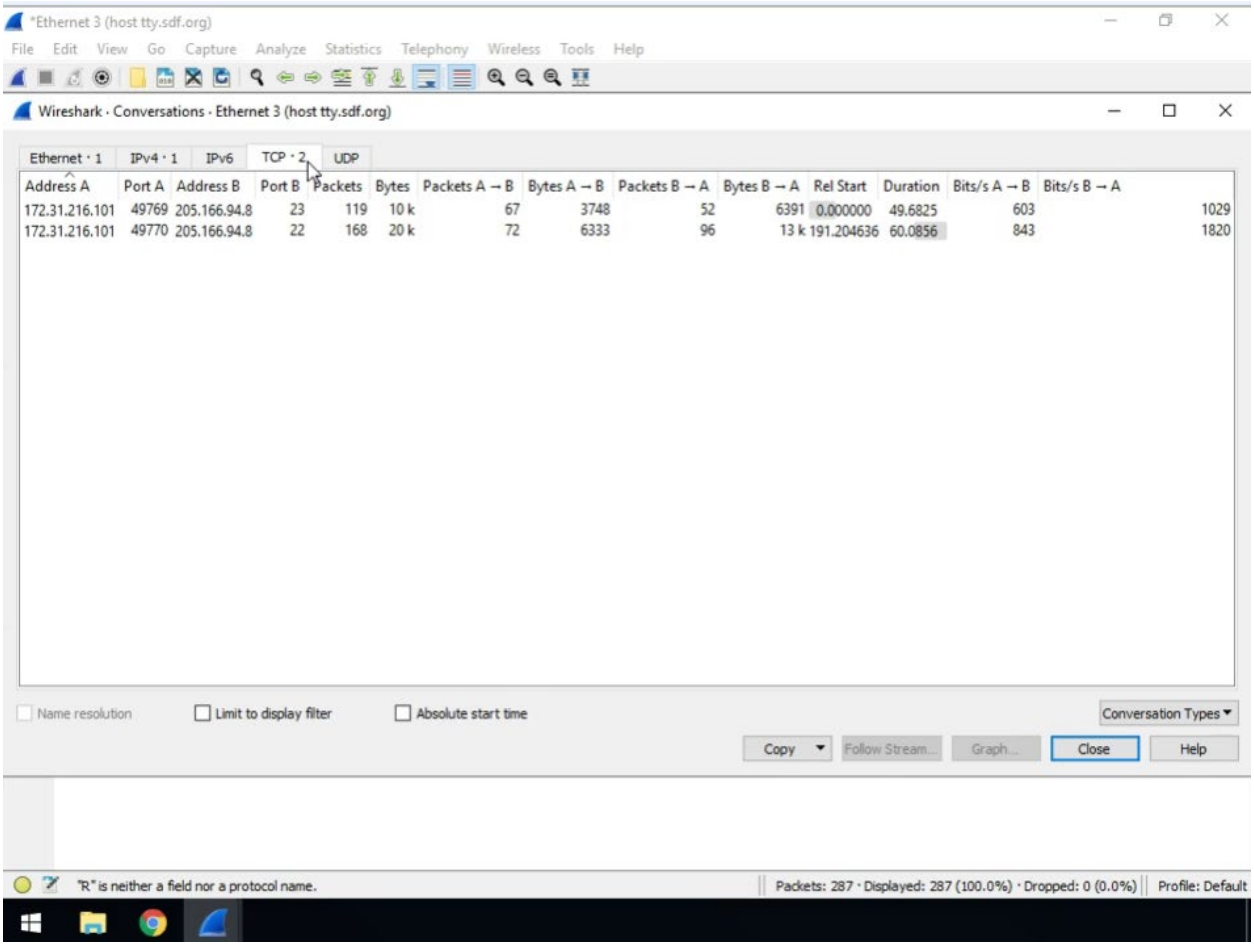

Capturing from Ethernet 3 (host tty.sdf.org)
Telnet tty.sdf.org
rie up 3+19:05, 2 users, load 0.02, 0.02, 0.02
vpn up 87+16:15, 0 users, load 0.07, 0.08, 0.08
vps3 up 46+04:04, 0 users, load 2.03, 2.01, 1.97
miku up 3+19:05, 0 users, load 0.15, 0.14, 0.15
otaku up 3+19:04, 2 users, load 0.14, 0.19, 0.24
norge up 3+19:04, 0 users, load 0.09, 0.03, 0.00
faeroes up 3+19:05, 3 users, load 0.47, 0.26, 0.23
iceland up 3+19:05, 2 users, load 0.39, 0.30, 0.25
anonradio up 43+00:04, 0 users, load 0.29, 0.24, 0.25
(continue)
The Moon is Waning Gibbous (84% of Full)
Full Moon + 4 6:04:44
Last Quarter - 3 22:00:21
(continue)
Type 'help' for Commands.
Type 'com' to chat with other users.
Type 'ttytter' to listen to Twitter Tweets anonymously.
Type 'mud' to play the SDFmud.
Type 'mkhomepg' to set up your personal website.
Did you know you can become a permanent LIFETIME member of SDF
by making a onetime donation of $36? Type 'arpa' for more info!
otaku:/sdf/udd/m/menna> exit
Profile: Default

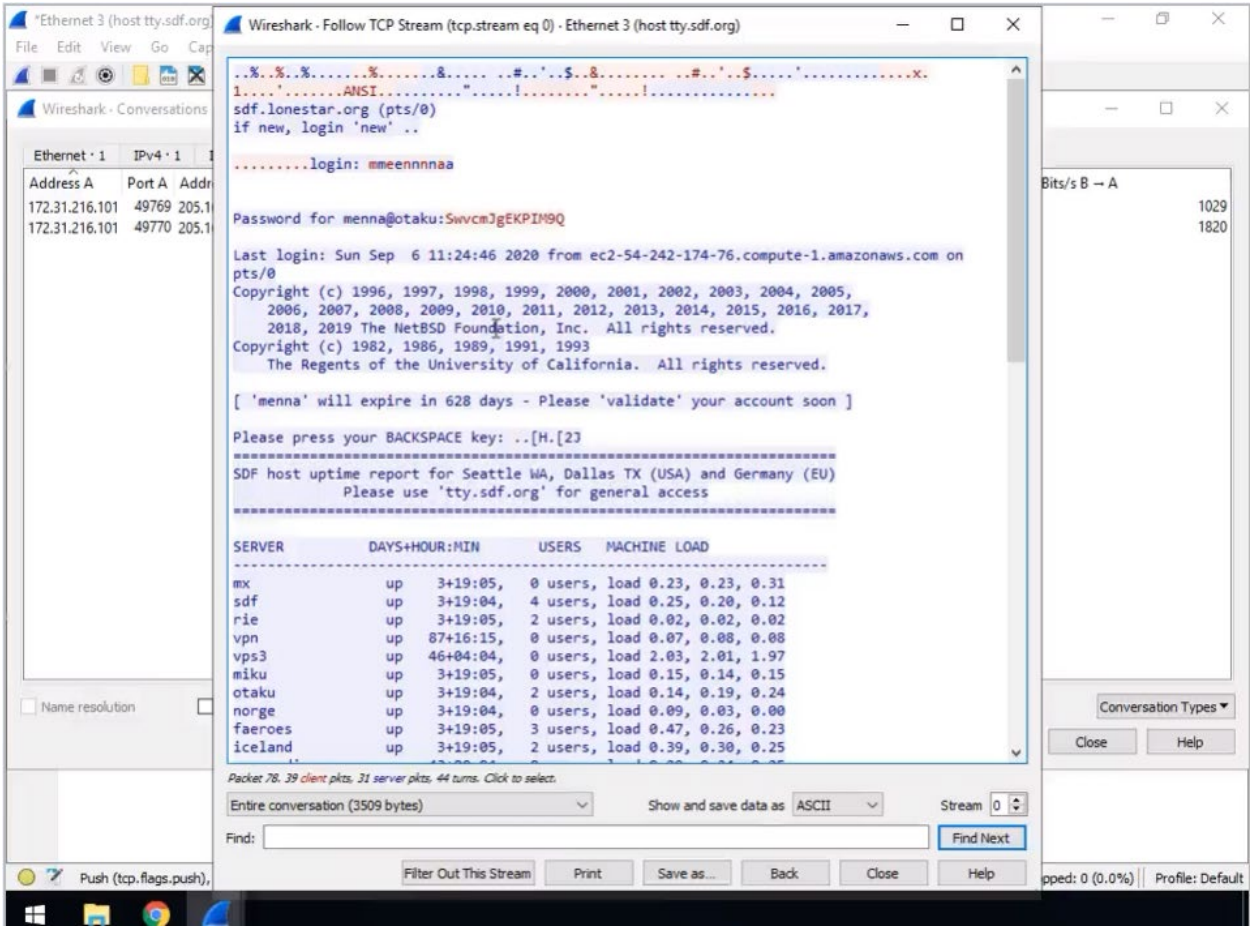

Capturing from Ethernet 3 (host tty.sdf.org)
File Edit View
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> ssh menna@tty.sdf.org

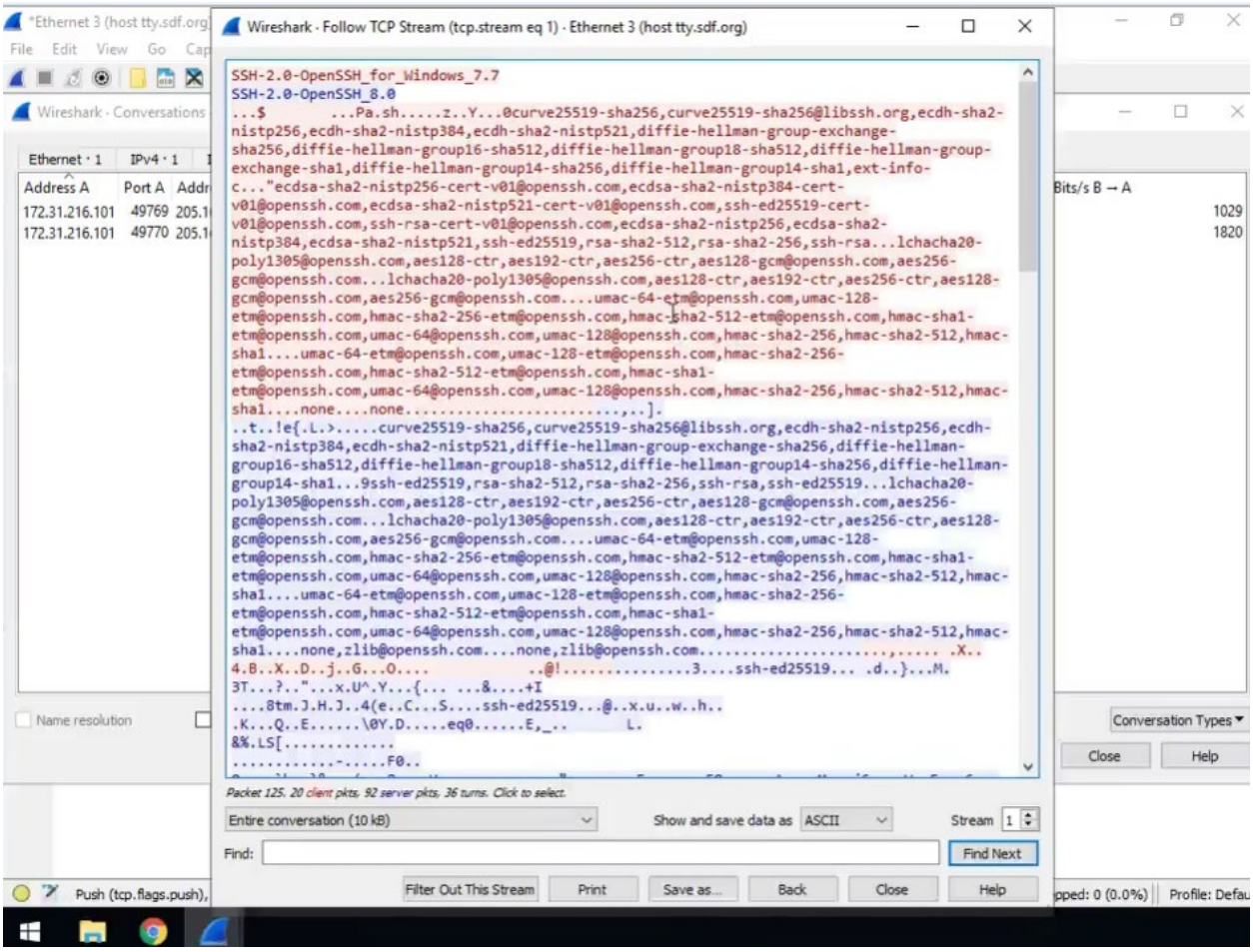

Capturing from Ethernet 3 (host tty.sdf.org)
File Edit View
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> ssh menna@tty.sdf.org
The authenticity of host 'tty.sdf.org (205.166.94.8)' can't be established.
ED25519 key fingerprint is SHA256:ZjwbO7AU8rHJExYrmZS2LqGZ7WfdoELfMrF54W92PYA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'tty.sdf.org,205.166.94.8' (ED25519) to the list of known hosts.
menna@tty.sdf.org's password:


Capturing from Ethernet 3 (host tty.sdf.org)
File Edit View
OpenSSH SSH client
rie up 3+19:09, 2 users, load 0.04, 0.03, 0.01
vpn up 87+16:18, 0 users, load 0.17, 0.10, 0.09
vps3 up 46+04:08, 0 users, load 2.03, 2.01, 1.97
miku up 3+19:09, 0 users, load 0.12, 0.19, 0.17
otaku up 3+19:08, 2 users, load 0.12, 0.16, 0.22
norge up 3+19:07, 0 users, load 0.04, 0.02, 0.00
faeroes up 3+19:09, 3 users, load 0.58, 0.34, 0.27
iceland up 3+19:09, 2 users, load 0.42, 0.38, 0.29
anonradio up 43+00:08, 0 users, load 0.20, 0.20, 0.23
(continue)
The Moon is Waning Gibbous (84% of Full)
Full Moon +
4 6:08:05
Last Quarter -
3 21:57:00
(continue)
Type 'help' for Commands.
Type 'com' to chat with other users.
Type 'ttytter' to listen to Twitter Tweets anonymously.
Type 'mud' to play the SDFmud.
Type 'mkhomepg' to set up your personal website.
Did you know you can become a permanent LIFETIME member of SDF
by making a onetime donation of $36? Type 'arpa' for more info!
otaku:/sdf/udd/m/menna>

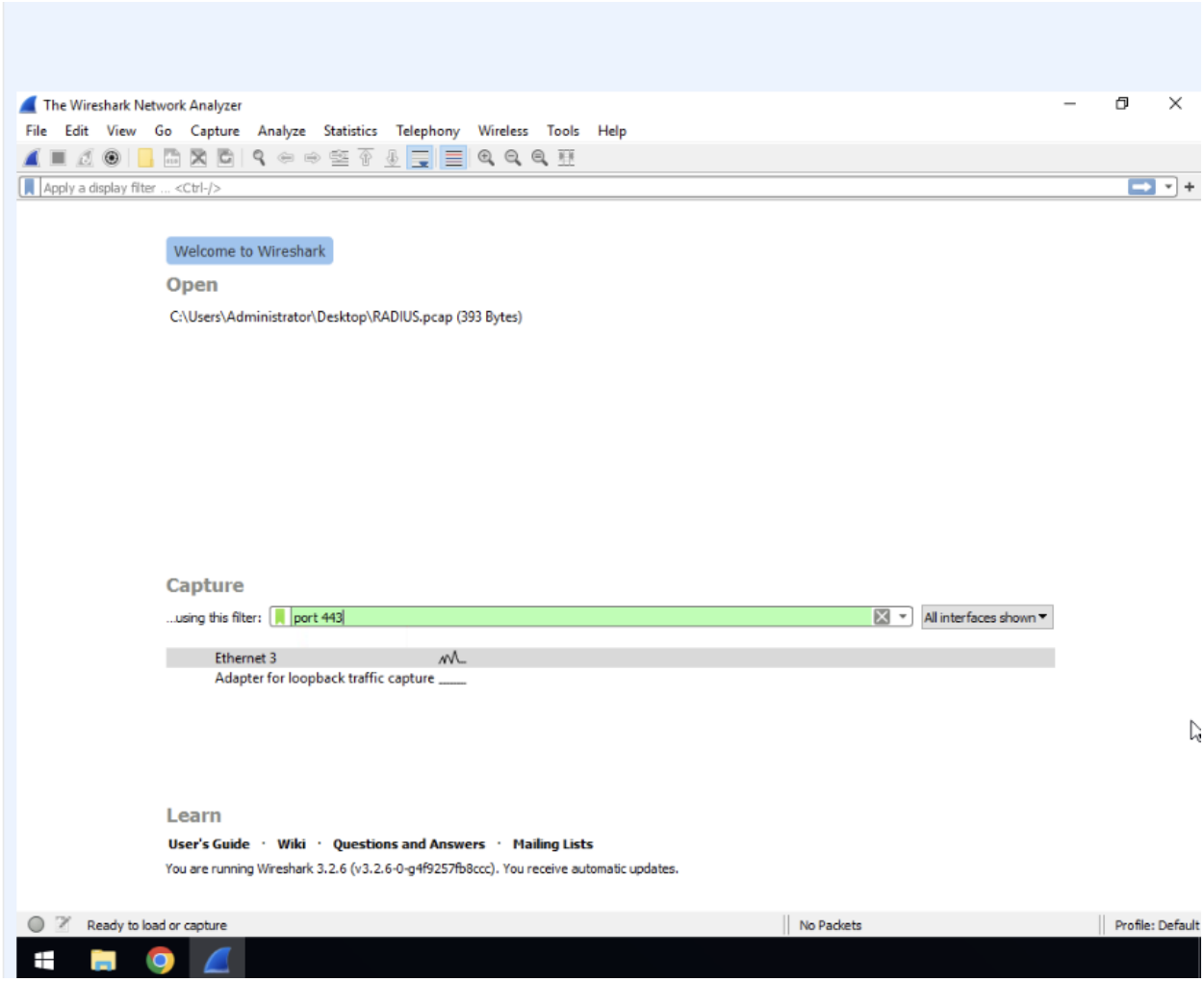

*Ethernet 3 (host tty.sdf.org)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
272 245.867742 172.31.216.101 205.166.94.8 TCP 54 49770 → 22 [ACK] Seq=2374 Ack=8082 Win=262144 Len=0
273 245.899725 205.166.94.8 172.31.216.101 SSHv2 98 Server: Encrypted packet (len=44)
274 245.899973 205.166.94.8 172.31.216.101 SSHv2 122 Server: Encrypted packet (len=68)
275 245.899999 172.31.216.101 205.166.94.8 TCP 54 49770 → 22 [ACK] Seq=2374 Ack=8194 Win=261888 Len=0
276 245.900028 205.166.94.8 172.31.216.101 SSHv2 90 Server: Encrypted packet (len=36)
277 245.900158 205.166.94.8 172.31.216.101 SSHv2 130 Server: Encrypted packet (len=76)
278 245.900171 172.31.216.101 205.166.94.8 TCP 54 49770 → 22 [ACK] Seq=2374 Ack=8306 Win=261888 Len=0
279 245.900247 205.166.94.8 172.31.216.101 SSHv2 122 Server: Encrypted packet (len=68)
280 245.900359 205.166.94.8 172.31.216.101 SSHv2 90 Server: Encrypted packet (len=36)
Acknowledgment number: 2374 (relative ack number)
Acknowledgment number (raw): 967823979
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
0000 0a 3d 58 a2 1a 61 0a d3 9e 2f df eb 08 00 45 48
0010 00 6c 5a d1 40 00 21 06 4e 3f cd a6 5e 08 ac 1f
0020 d8 65 00 16 c2 6a 01 25 1a 93 39 af d2 6b 50 18
0030 10 65 03 1a 00 00 8c 0b 50 f8 88 29 06 c3 c6 be
0040 e3 1f 73 a5 9d fb 5b df 1e 7f 3d a4 57 ee 30 13
0050 e2 a4 d7 c9 b4 8f 7b 71 68 39 c7 49 50 0f d7 c3
0060 ec f0 13 c6 f6 dc 5a e9 ae 3c 8d 51 47 5b a5 db
0070 9e f0 1d 4f da 07 14 c4 31 f9
Push (tcp.flags.push), 1 byte
Packets: 287 · Displayed: 287 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

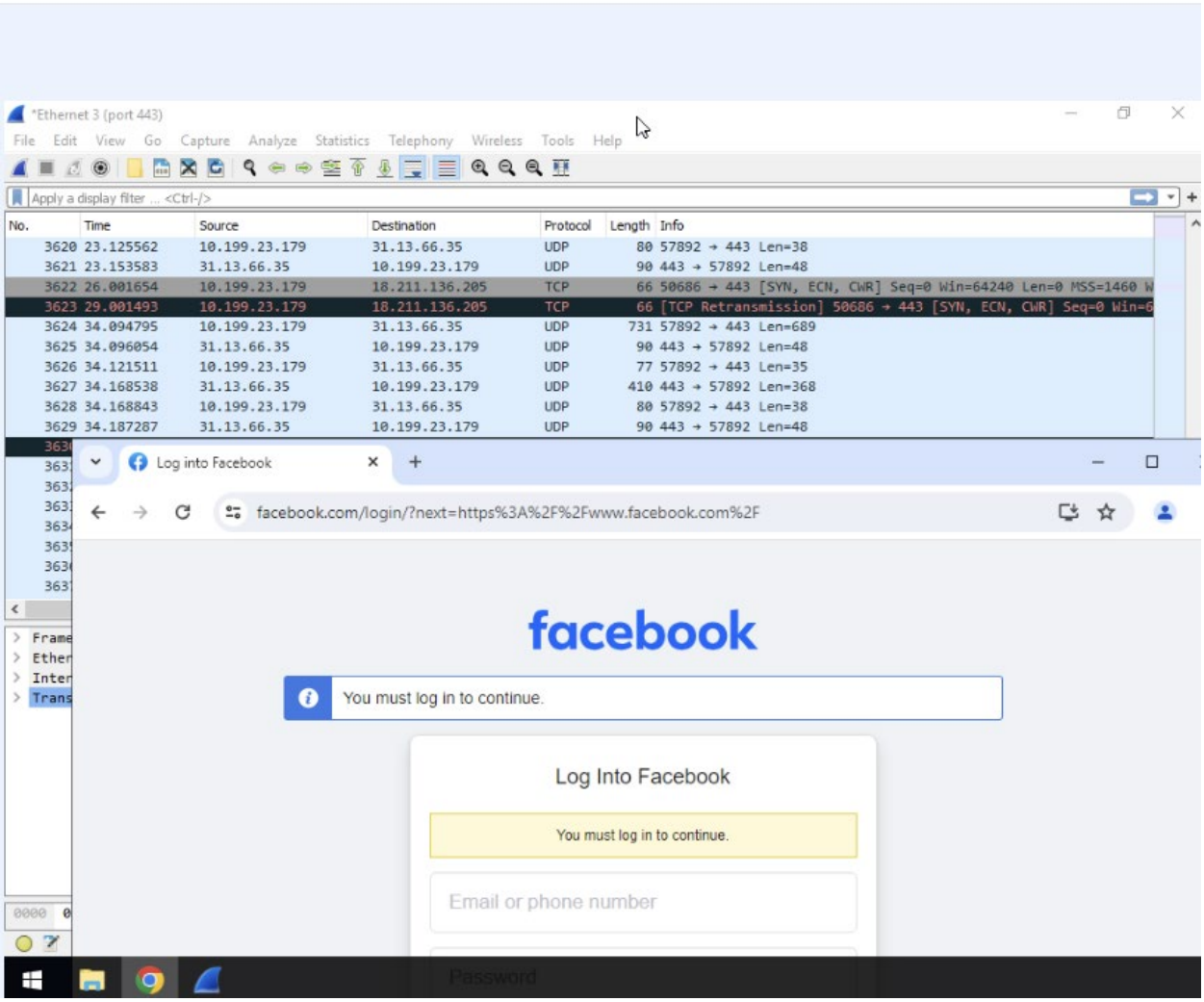

*Ethernet 3 (host tty.sdf.org)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · Ethernet 3 (host tty.sdf.org)
Ethernet · 1
IPv4 · 1
IPv6
TCP · 2
UDP
Address A Port A Address B Port B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A
172.31.216.101 49769 205.166.94.8 23 119 10 k 67 3748 52 6391 0.000000 49.6825 603 1029
172.31.216.101 49770 205.166.94.8 22 168 20 k 72 6333 96 13 k 191.204636 60.0856 843 1820
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help
"R" is neither a field nor a protocol name.
Packets: 287 · Displayed: 287 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

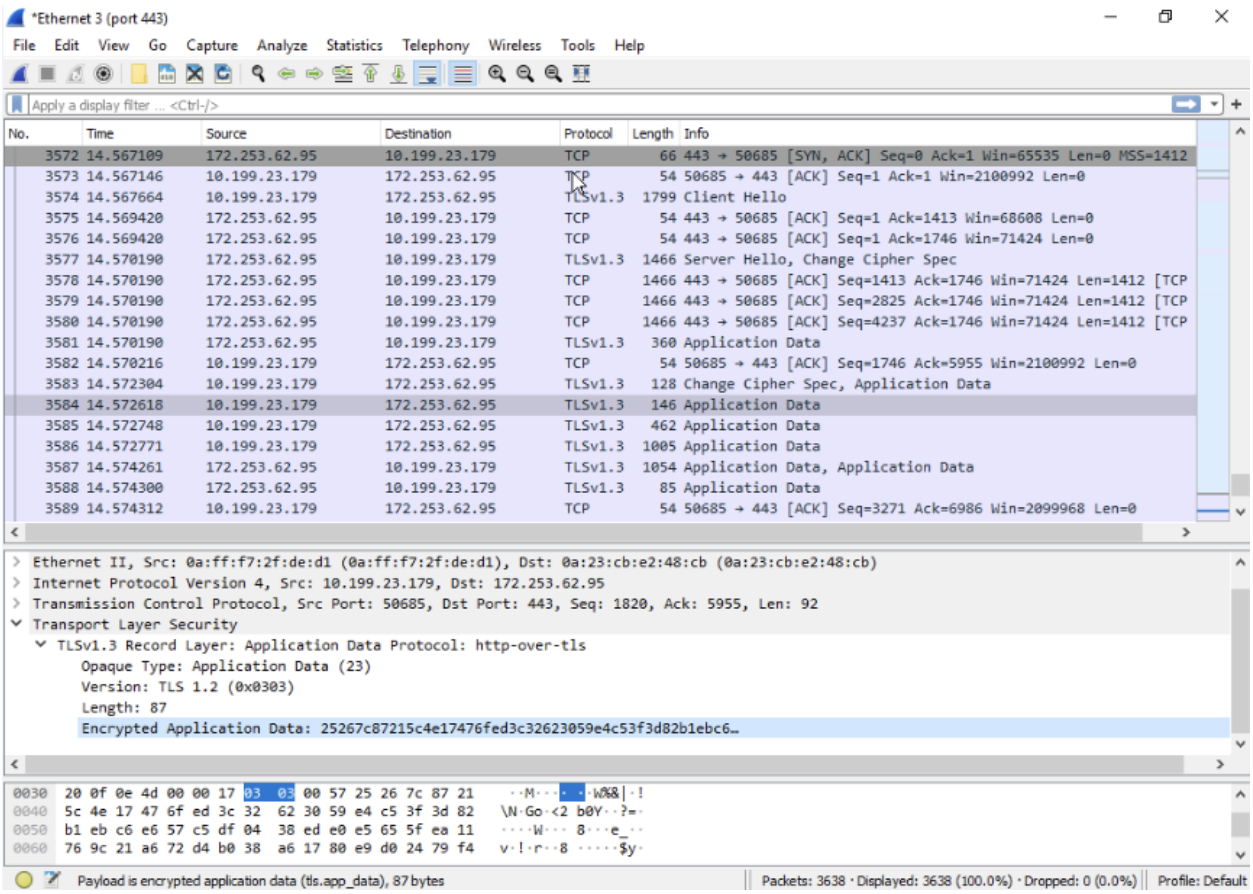

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet 3 (host tty.sdf.org)
..%..%..%.....%.....&..... ..#..'..$..&..... ..#..'..$.....'.....x.
1...'.....ANSI.....".....!.....".....!.....
sdf.lonestar.org (pts/0)
if new, login 'new' ..
.....login: mmeennnnaa
Password for menna@otaku:SwvcmJgEKPIM9Q
Last login: Sun Sep 6 11:24:46 2020 from ec2-54-242-174-76.compute-1.amazonaws.com on
pts/0
Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005,
2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017,
2018, 2019 The NetBSD Foundation, Inc. All rights reserved.
Copyright (c) 1982, 1986, 1989, 1991, 1993
The Regents of the University of California. All rights reserved.
['menna' will expire in 628 days - Please 'validate' your account soon]
Please press your BACKSPACE key: ..[H.[2J
SDF host uptime report for Seattle WA, Dallas TX (USA) and Germany (EU)
Please use 'tty.sdf.org' for general access
SERVER DAYS+HOUR:MIN USERS MACHINE LOAD
mx up 3+19:05, 0 users, load 0.23, 0.23, 0.31
sdf up 3+19:04, 4 users, load 0.25, 0.20, 0.12
rie up 3+19:05, 2 users, load 0.02, 0.02, 0.02
vpn up 87+16:15, 0 users, load 0.07, 0.08, 0.08
vps3 up 46+04:04, 0 users, load 2.03, 2.01, 1.97
miku up 3+19:05, 0 users, load 0.15, 0.14, 0.15
otaku up 3+19:04, 2 users, load 0.14, 0.19, 0.24
norge up 3+19:04, 0 users, load 0.09, 0.03, 0.00
faeroes up 3+19:05, 3 users, load 0.47, 0.26, 0.23
iceland up 3+19:05, 2 users, load 0.39, 0.30, 0.25
Packet 78. 39 client pkts, 31 server pkts, 44 turns. Click to select.
Entire conversation (3509 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Wireshark · Conversations
Ethernet · 1
IPv4 · 1
Address A
Port A
172.31.216.101 49769
172.31.216.101 49770
Bits/s B → A
1029
1820
Name resolution
Conversation Types
Close
Help
Push (tcp.flags.push),
Profile: Default

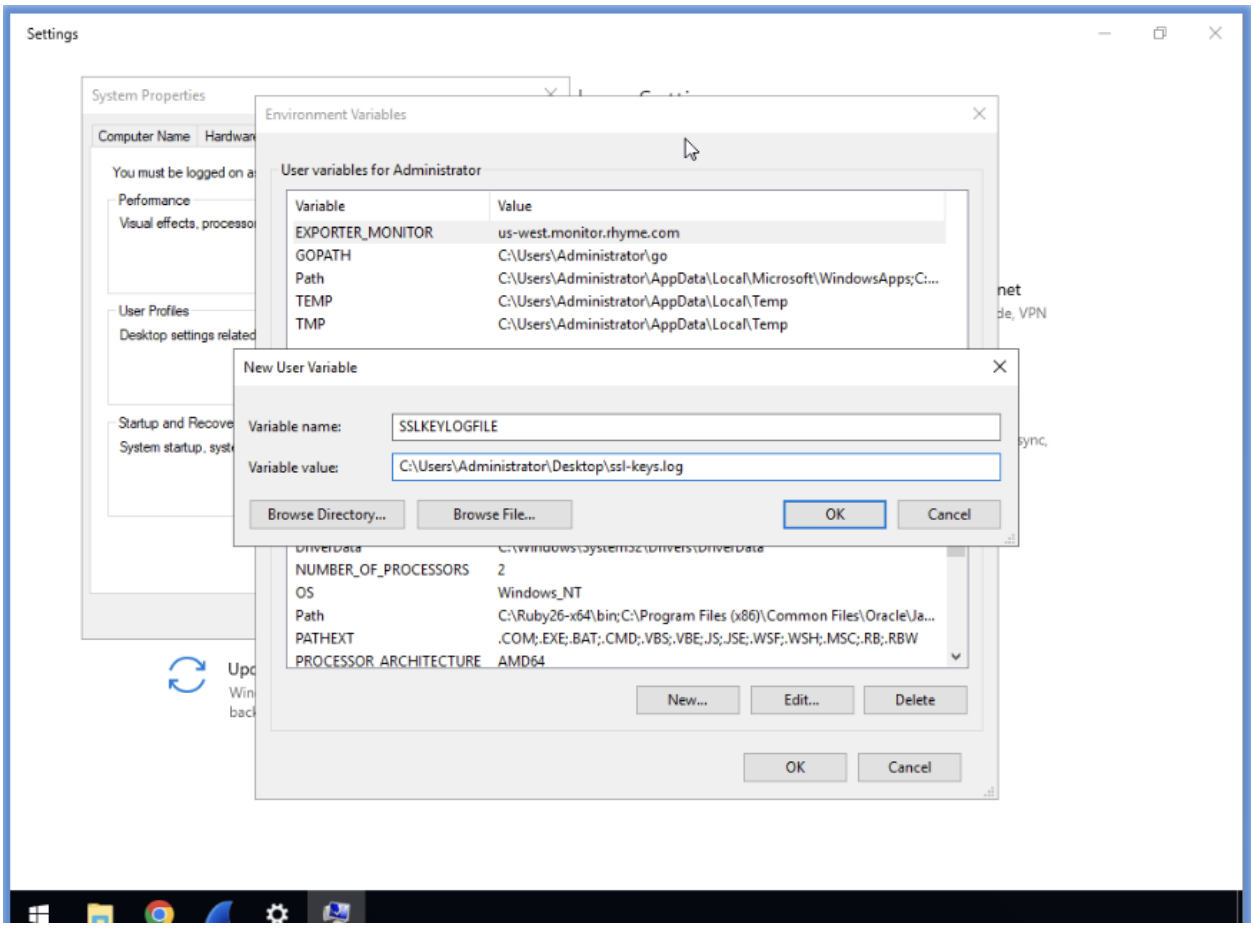


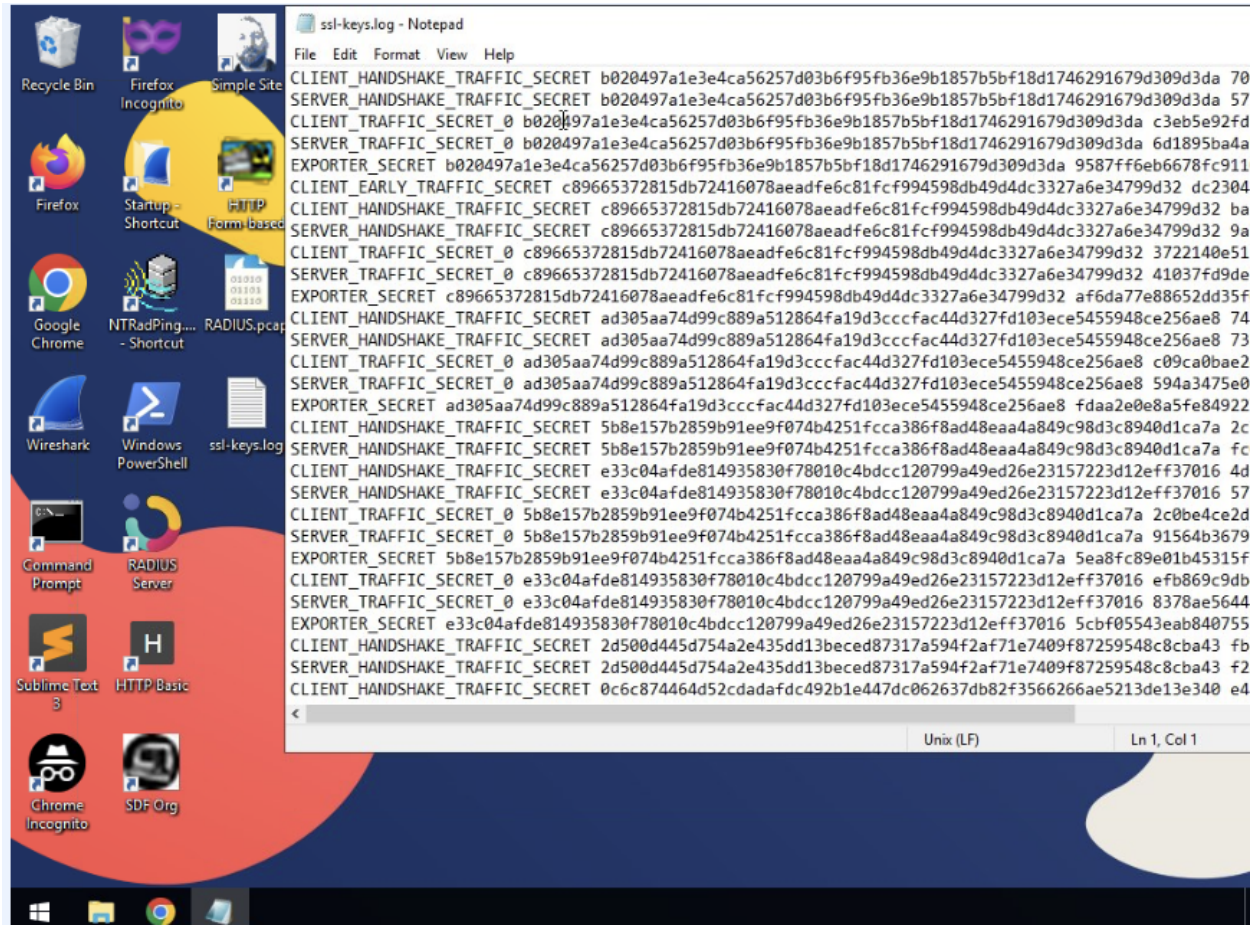
Task 7: Generate, Capture, Analyze then Decrypt HTTPS Traffic

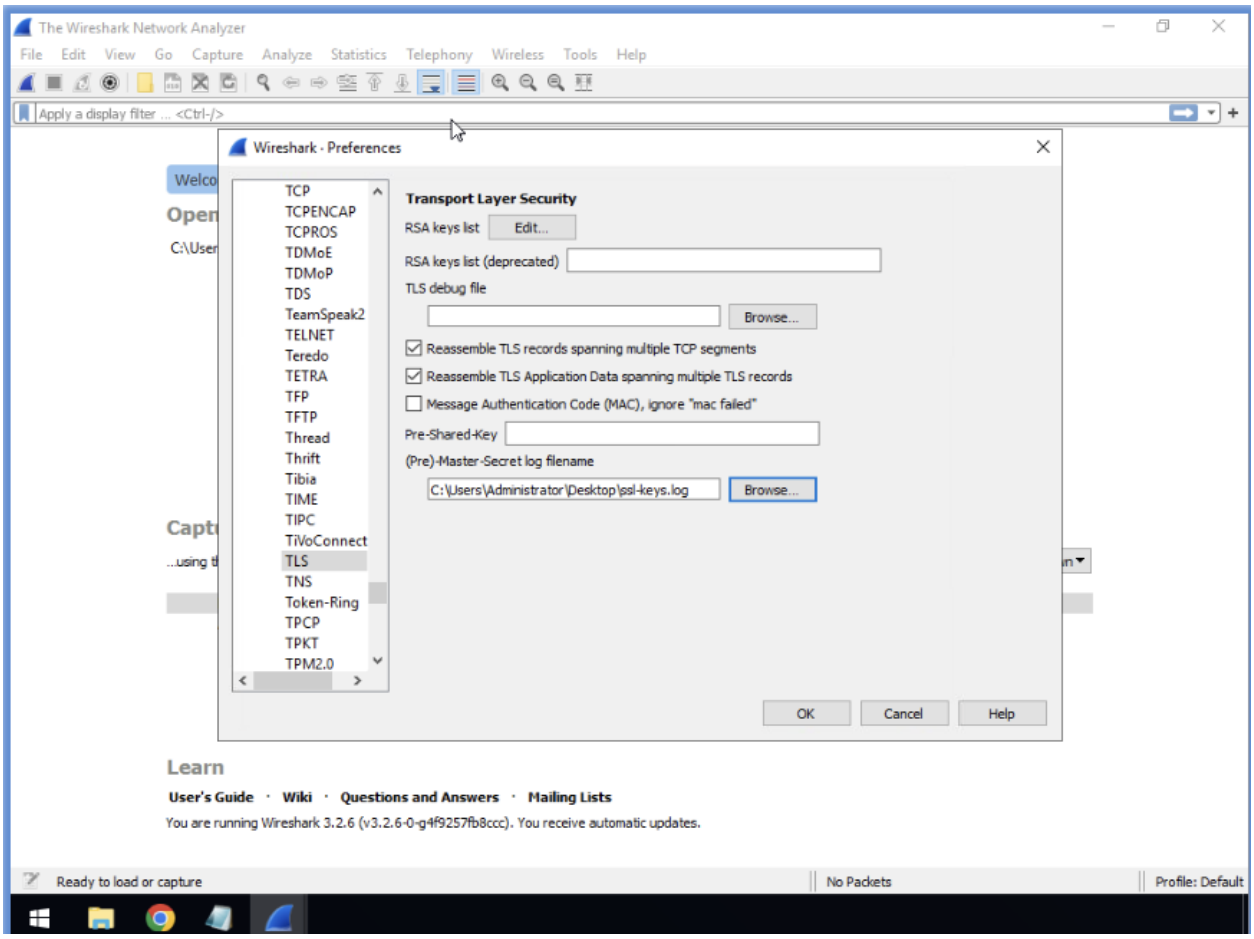

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\Administrator\Desktop\RADIUS.pcap (393 Bytes)
Capture
...using this filter: port 443
All interfaces shown
Ethernet 3
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

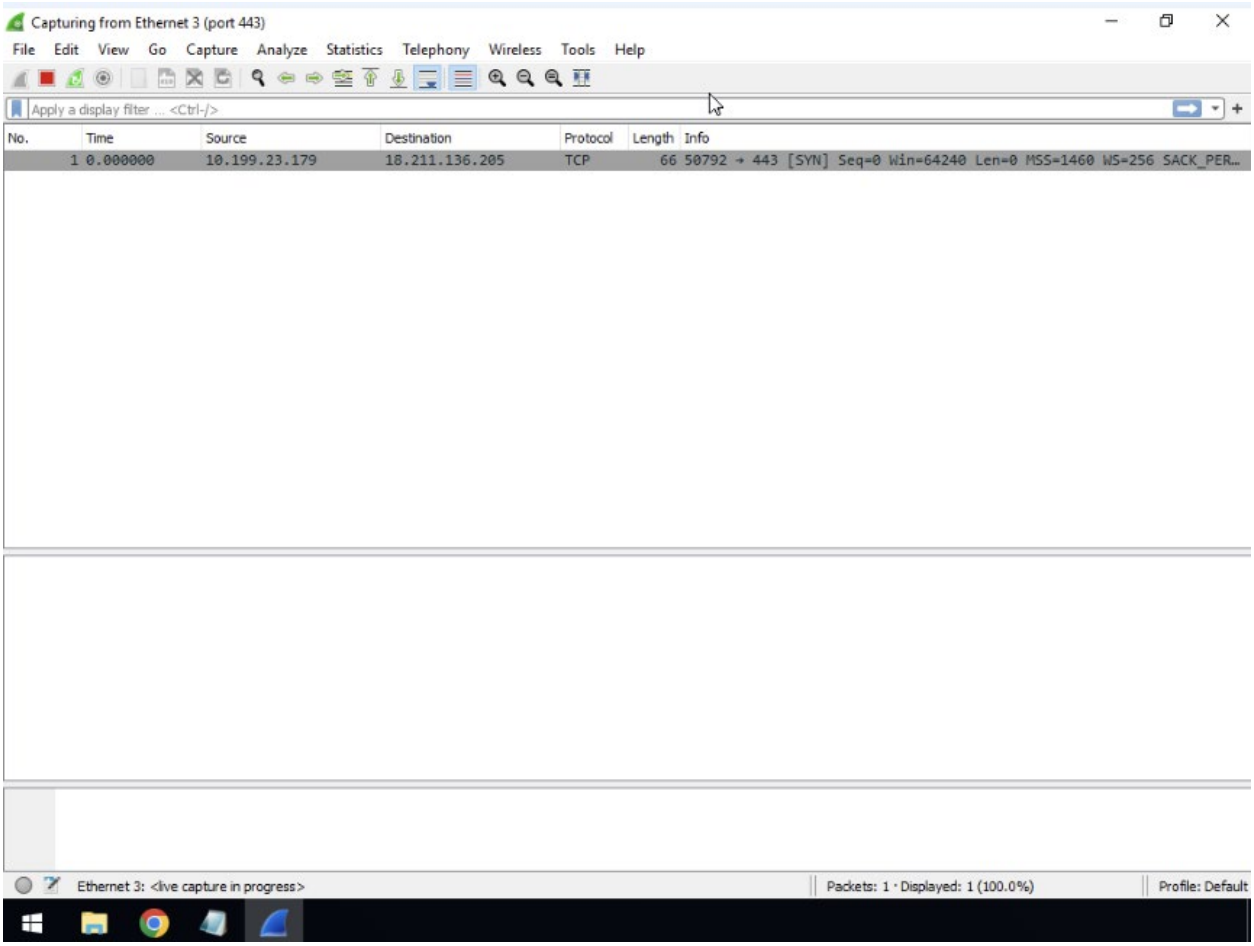

*Ethernet 3 (port 443)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3620 23.125562 10.199.23.179 31.13.66.35 UDP 80 57892 → 443 Len=38
3621 23.153583 31.13.66.35 10.199.23.179 UDP 90 443 → 57892 Len=48
3622 26.001654 10.199.23.179 18.211.136.205 TCP 66 50686 → 443 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 W
3623 29.001493 10.199.23.179 18.211.136.205 TCP 66 [TCP Retransmission] 50686 → 443 [SYN, ECN, CWR] Seq=0 Win=6
3624 34.094795 10.199.23.179 31.13.66.35 UDP 731 57892 → 443 Len=689
3625 34.096054 31.13.66.35 10.199.23.179 UDP 90 443 → 57892 Len=48
3626 34.121511 10.199.23.179 31.13.66.35 UDP 77 57892 → 443 Len=35
3627 34.168538 31.13.66.35 10.199.23.179 UDP 410 443 → 57892 Len=368
3628 34.168843 10.199.23.179 31.13.66.35 UDP 80 57892 → 443 Len=38
3629 34.187287 31.13.66.35 10.199.23.179 UDP 90 443 → 57892 Len=48
Log into Facebook
facebook.com/login/?next=https%3A%2F%2Fwww.facebook.com%2F
facebook
You must log in to continue.
Log Into Facebook
You must log in to continue.
Email or phone number
Password

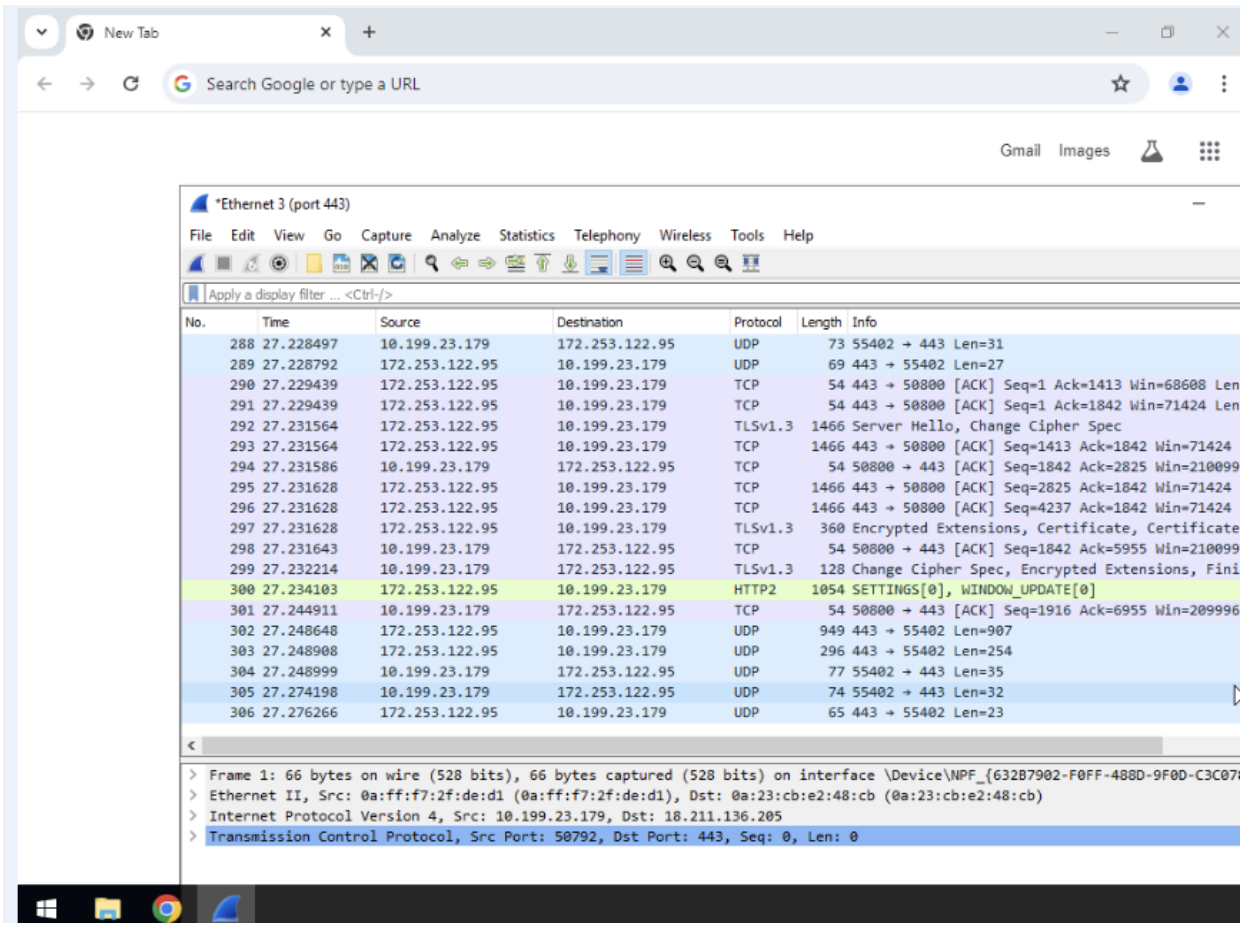

*Ethernet 3 (port 443)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3572 14.567109 172.253.62.95 10.199.23.179 TCP 66 443 → 50685 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412
3573 14.567146 10.199.23.179 172.253.62.95 TCP 54 50685 → 443 [ACK] Seq=1 Ack=1 Win=2100992 Len=0
3574 14.567664 10.199.23.179 172.253.62.95 TLSv1.3 1799 Client Hello
3575 14.569420 172.253.62.95 10.199.23.179 TCP 54 443 → 50685 [ACK] Seq=1 Ack=1413 Win=68608 Len=0
3576 14.569420 172.253.62.95 10.199.23.179 TCP 54 443 → 50685 [ACK] Seq=1 Ack=1746 Win=71424 Len=0
3577 14.570190 172.253.62.95 10.199.23.179 TLSv1.3 1466 Server Hello, Change Cipher Spec
3578 14.570190 172.253.62.95 10.199.23.179 TCP 1466 443 → 50685 [ACK] Seq=1413 Ack=1746 Win=71424 Len=1412 [TCP
3579 14.570190 172.253.62.95 10.199.23.179 TCP 1466 443 → 50685 [ACK] Seq=2825 Ack=1746 Win=71424 Len=1412 [TCP
3580 14.570190 172.253.62.95 10.199.23.179 TCP 1466 443 → 50685 [ACK] Seq=4237 Ack=1746 Win=71424 Len=1412 [TCP
3581 14.570190 172.253.62.95 10.199.23.179 TLSv1.3 360 Application Data
3582 14.570216 10.199.23.179 172.253.62.95 TCP 54 50685 → 443 [ACK] Seq=1746 Ack=5955 Win=2100992 Len=0
3583 14.572304 10.199.23.179 172.253.62.95 TLSv1.3 128 Change Cipher Spec, Application Data
3584 14.572618 10.199.23.179 172.253.62.95 TLSv1.3 146 Application Data
3585 14.572748 10.199.23.179 172.253.62.95 TLSv1.3 462 Application Data
3586 14.572771 10.199.23.179 172.253.62.95 TLSv1.3 1005 Application Data
3587 14.574261 172.253.62.95 10.199.23.179 TLSv1.3 1054 Application Data, Application Data
3588 14.574300 172.253.62.95 10.199.23.179 TLSv1.3 85 Application Data
3589 14.574312 10.199.23.179 172.253.62.95 TCP 54 50685 → 443 [ACK] Seq=3271 Ack=6986 Win=2099968 Len=0
Ethernet II, Src: 0a:ff:f7:2f:de:d1 (0a:ff:f7:2f:de:d1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.23.179, Dst: 172.253.62.95
Transmission Control Protocol, Src Port: 50685, Dst Port: 443, Seq: 1820, Ack: 5955, Len: 92
Transport Layer Security
TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 87
Encrypted Application Data: 25267c87215c4e17476fed3c32623059e4c53f3d82b1ebc6…
0030 20 0f 0e 4d 00 00 17 03 03 00 57 25 26 7c 87 21
0040 5c 4e 17 47 6f ed 3c 32 62 30 59 e4 c5 3f 3d 82
0050 b1 eb c6 e6 57 c5 df 04 38 ed e0 e5 65 5f ea 11
0060 76 9c 21 a6 72 d4 b0 38 a6 17 80 e9 d0 24 79 f4
Payload is encrypted application data (tls.app_data), 87 bytes
Packets: 3638 · Displayed: 3638 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

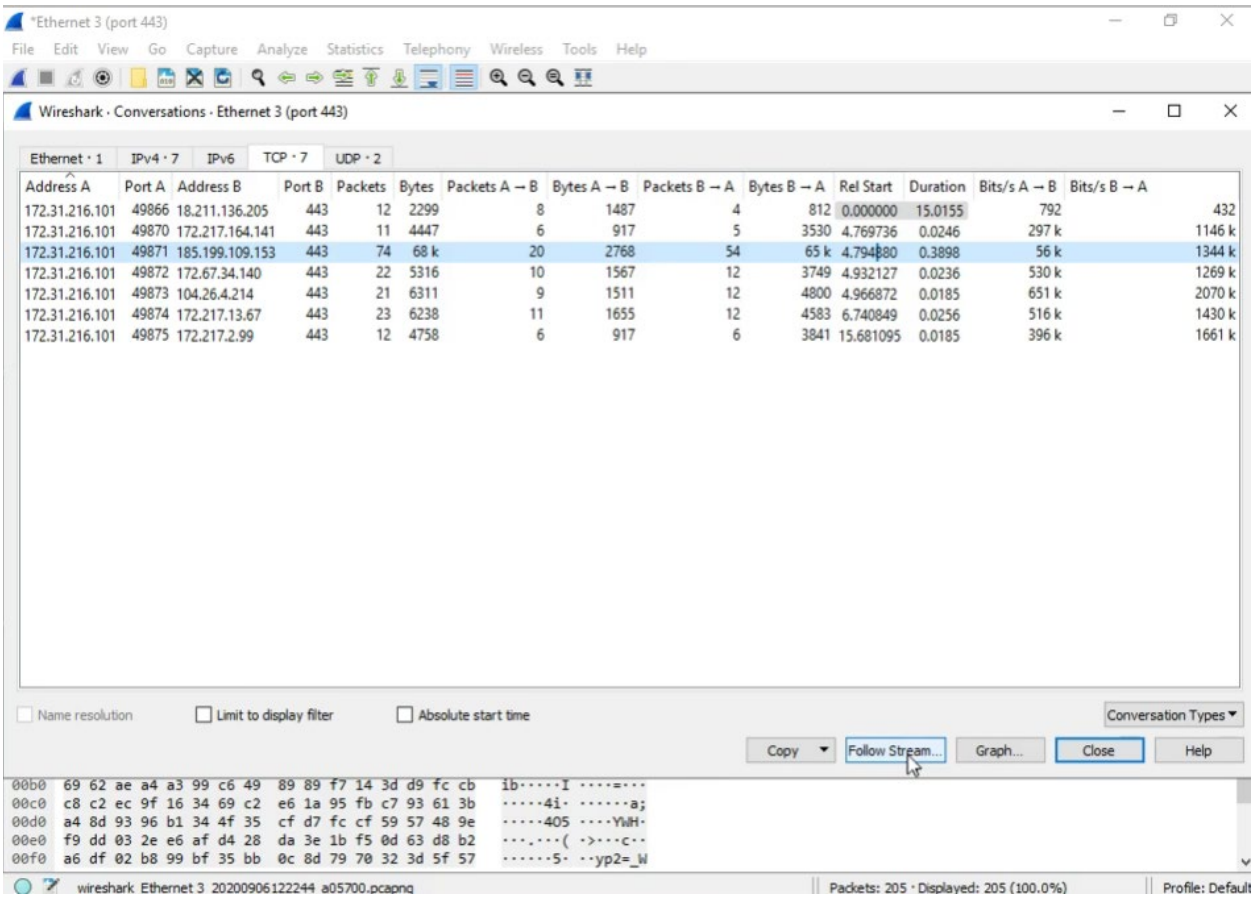

Settings
System Properties
Computer Name
Hardware
You must be logged on a
Performance
Visual effects, processo
User Profiles
Desktop settings related
Startup and Recove
System startup, syst
Environment Variables
User variables for Administrator
Variable
Value
EXPORTER_MONITOR
us-west.monitor.rhyme.com
GOPATH
C:\Users\Administrator\go
Path
C:\Users\Administrator\AppData\Local\Microsoft\WindowsApps;C:...
TEMP
C:\Users\Administrator\AppData\Local\Temp
TMP
C:\Users\Administrator\AppData\Local\Temp
New User Variable
Variable name:
SSLKEYLOGFILE
Variable value:
C:\Users\Administrator\Desktop\ssl-keys.log
Browse Directory...
Browse File...
OK
Cancel
NUMBER_OF_PROCESSORS
2
OS
Windows_NT
Path
C:\Ruby26-x64\bin;C:\Program Files (x86)\Common Files\Oracle\Ja...
PATHEXT
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.RB;.RBW
PROCESSOR_ARCHITECTURE
AMD64
New...
Edit...
Delete
OK
Cancel

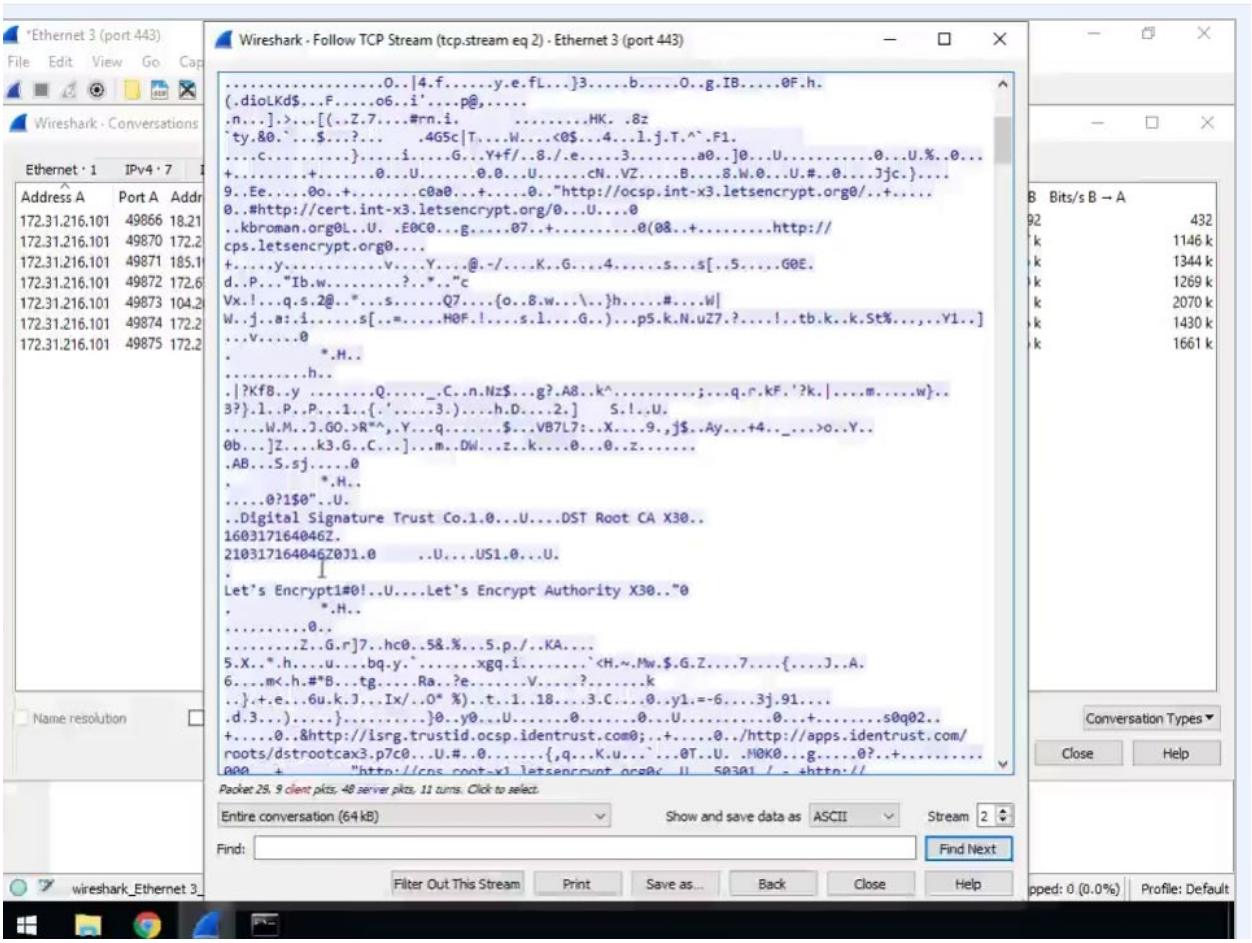

Recycle Bin
Firefox Incognito
Simple Site
Firefox
Startup - Shortcut
HTTP Form-based
Google Chrome
NTRadPing.... - Shortcut
RADIUS.pcap
Wireshark
Windows PowerShell
ssl-keys.log
Command Prompt
RADIUS Server
Sublime Text 3
HTTP Basic
Chrome Incognito
SDF Org
ssl-keys.log - Notepad
File Edit Format View Help
CLIENT_HANDSHAKE_TRAFFIC_SECRET b020497a1e3e4ca56257d03b6f95fb36e9b1857b5bf18d1746291679d309d3da 70
SERVER_HANDSHAKE_TRAFFIC_SECRET b020497a1e3e4ca56257d03b6f95fb36e9b1857b5bf18d1746291679d309d3da 57
CLIENT_TRAFFIC_SECRET_0 b020497a1e3e4ca56257d03b6f95fb36e9b1857b5bf18d1746291679d309d3da c3eb5e92fd
SERVER_TRAFFIC_SECRET_0 b020497a1e3e4ca56257d03b6f95fb36e9b1857b5bf18d1746291679d309d3da 6d1895ba4a
EXPORTER_SECRET b020497a1e3e4ca56257d03b6f95fb36e9b1857b5bf18d1746291679d309d3da 9587ff6eb6678fc911
CLIENT_EARLY_TRAFFIC_SECRET c89665372815db72416078aeadfe6c81fcf994598db49d4dc3327a6e34799d32 dc2304
CLIENT_HANDSHAKE_TRAFFIC_SECRET c89665372815db72416078aeadfe6c81fcf994598db49d4dc3327a6e34799d32 ba
SERVER_HANDSHAKE_TRAFFIC_SECRET c89665372815db72416078aeadfe6c81fcf994598db49d4dc3327a6e34799d32 9a
CLIENT_TRAFFIC_SECRET_0 c89665372815db72416078aeadfe6c81fcf994598db49d4dc3327a6e34799d32 3722140e51
SERVER_TRAFFIC_SECRET_0 c89665372815db72416078aeadfe6c81fcf994598db49d4dc3327a6e34799d32 41037fd9de
EXPORTER_SECRET c89665372815db72416078aeadfe6c81fcf994598db49d4dc3327a6e34799d32 af6da77e88652dd35f
CLIENT_HANDSHAKE_TRAFFIC_SECRET ad305aa74d99c889a512864fa19d3cccfac44d327fd103ece5455948ce256ae8 74
SERVER_HANDSHAKE_TRAFFIC_SECRET ad305aa74d99c889a512864fa19d3cccfac44d327fd103ece5455948ce256ae8 73
CLIENT_TRAFFIC_SECRET_0 ad305aa74d99c889a512864fa19d3cccfac44d327fd103ece5455948ce256ae8 c09ca0bae2
SERVER_TRAFFIC_SECRET_0 ad305aa74d99c889a512864fa19d3cccfac44d327fd103ece5455948ce256ae8 594a3475e0
EXPORTER_SECRET ad305aa74d99c889a512864fa19d3cccfac44d327fd103ece5455948ce256ae8 fdaa2e0e8a5fe84922
CLIENT_HANDSHAKE_TRAFFIC_SECRET 5b8e157b2859b91ee9f074b4251fcca386f8ad48eaa4a849c98d3c8940d1ca7a 2c
SERVER_HANDSHAKE_TRAFFIC_SECRET 5b8e157b2859b91ee9f074b4251fcca386f8ad48eaa4a849c98d3c8940d1ca7a fc
CLIENT_HANDSHAKE_TRAFFIC_SECRET e33c04afde814935830f78010c4bdcc120799a49ed26e23157223d12eff37016 4d
SERVER_HANDSHAKE_TRAFFIC_SECRET e33c04afde814935830f78010c4bdcc120799a49ed26e23157223d12eff37016 57
CLIENT_TRAFFIC_SECRET_0 5b8e157b2859b91ee9f074b4251fcca386f8ad48eaa4a849c98d3c8940d1ca7a 2c0be4ce2d
SERVER_TRAFFIC_SECRET_0 5b8e157b2859b91ee9f074b4251fcca386f8ad48eaa4a849c98d3c8940d1ca7a 91564b3679
EXPORTER_SECRET 5b8e157b2859b91ee9f074b4251fcca386f8ad48eaa4a849c98d3c8940d1ca7a 5ea8fc89e01b45315f
CLIENT_TRAFFIC_SECRET_0 e33c04afde814935830f78010c4bdcc120799a49ed26e23157223d12eff37016 efb869c9db
SERVER_TRAFFIC_SECRET_0 e33c04afde814935830f78010c4bdcc120799a49ed26e23157223d12eff37016 8378ae5644
EXPORTER_SECRET e33c04afde814935830f78010c4bdcc120799a49ed26e23157223d12eff37016 5cbf05543eab840755
CLIENT_HANDSHAKE_TRAFFIC_SECRET 2d500d445d754a2e435dd13beced87317a594f2af71e7409f87259548c8cba43 fb
SERVER_HANDSHAKE_TRAFFIC_SECRET 2d500d445d754a2e435dd13beced87317a594f2af71e7409f87259548c8cba43 f2
CLIENT_HANDSHAKE_TRAFFIC_SECRET 0c6c874464d52cdadafdc492b1e447dc062637db82f3566266ae5213de13e340 e4
Unix (LF)
Ln 1, Col 1

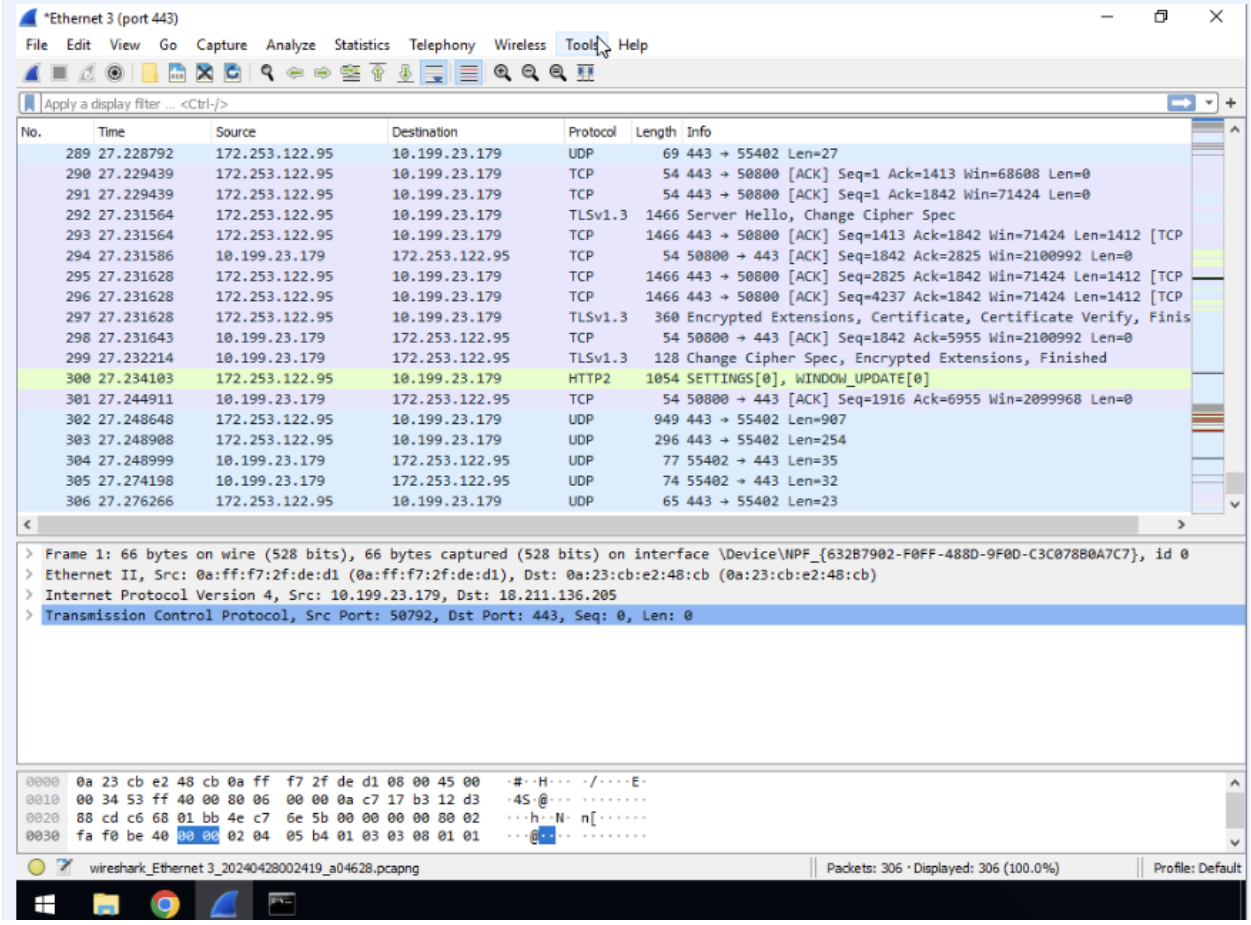

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Preferences
TCP
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
TeamSpeak2
TELNET
Teredo
TETRA
TFP
TFTP
Thread
Thrift
Tibia
TIME
TIPC
TiVoConnect
TLS
TNS
Token-Ring
TPCP
TPKT
TPM2.0
Transport Layer Security
RSA keys list
Edit...
RSA keys list (deprecated)
TLS debug file
Browse...
Reassemble TLS records spanning multiple TCP segments
Reassemble TLS Application Data spanning multiple TLS records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared-Key
(Pre)-Master-Secret log filename
C:\Users\Administrator\Desktop\ssl-keys.log
Browse...
OK
Cancel
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.6 (v3.2.6-0-g4f9257fb8ccc). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default


Capturing from Ethernet 3 (port 443)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.199.23.179 18.211.136.205 TCP 66 50792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER…
Ethernet 3: <live capture in progress>
Packets: 1 · Displayed: 1 (100.0%)
Profile: Default


New Tab
Search Google or type a URL
Gmail
Images
*Ethernet 3 (port 443)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
288 27.228497 10.199.23.179 172.253.122.95 UDP 73 55402 → 443 Len=31
289 27.228792 172.253.122.95 10.199.23.179 UDP 69 443 → 55402 Len=27
290 27.229439 172.253.122.95 10.199.23.179 TCP 54 443 → 50800 [ACK] Seq=1 Ack=1413 Win=68608 Len
291 27.229439 172.253.122.95 10.199.23.179 TCP 54 443 → 50800 [ACK] Seq=1 Ack=1842 Win=71424 Len
292 27.231564 172.253.122.95 10.199.23.179 TLSv1.3 1466 Server Hello, Change Cipher Spec
293 27.231564 172.253.122.95 10.199.23.179 TCP 1466 443 → 50800 [ACK] Seq=1413 Ack=1842 Win=71424
294 27.231586 10.199.23.179 172.253.122.95 TCP 54 50800 → 443 [ACK] Seq=1842 Ack=2825 Win=210099
295 27.231628 172.253.122.95 10.199.23.179 TCP 1466 443 → 50800 [ACK] Seq=2825 Ack=1842 Win=71424
296 27.231628 172.253.122.95 10.199.23.179 TCP 1466 443 → 50800 [ACK] Seq=4237 Ack=1842 Win=71424
297 27.231628 172.253.122.95 10.199.23.179 TLSv1.3 360 Encrypted Extensions, Certificate, Certificate
298 27.231643 10.199.23.179 172.253.122.95 TCP 54 50800 → 443 [ACK] Seq=1842 Ack=5955 Win=210099
299 27.232214 10.199.23.179 172.253.122.95 TLSv1.3 128 Change Cipher Spec, Encrypted Extensions, Fini
300 27.234103 172.253.122.95 10.199.23.179 HTTP2 1054 SETTINGS[0], WINDOW_UPDATE[0]
301 27.244911 10.199.23.179 172.253.122.95 TCP 54 50800 → 443 [ACK] Seq=1916 Ack=6955 Win=209996
302 27.248648 172.253.122.95 10.199.23.179 UDP 949 443 → 55402 Len=907
303 27.248908 172.253.122.95 10.199.23.179 UDP 296 443 → 55402 Len=254
304 27.248999 10.199.23.179 172.253.122.95 UDP 77 55402 → 443 Len=35
305 27.274198 10.199.23.179 172.253.122.95 UDP 74 55402 → 443 Len=32
306 27.276266 172.253.122.95 10.199.23.179 UDP 65 443 → 55402 Len=23
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{632B7902-F0FF-488D-9F0D-C3C07
Ethernet II, Src: 0a:ff:f7:2f:de:d1 (0a:ff:f7:2f:de:d1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.23.179, Dst: 18.211.136.205
Transmission Control Protocol, Src Port: 50792, Dst Port: 443, Seq: 0, Len: 0


*Ethernet 3 (port 443)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · Ethernet 3 (port 443)
Ethernet · 1
IPv4 · 7
IPv6
TCP · 7
UDP · 2
Address A Port A Address B Port B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A
172.31.216.101 49866 18.211.136.205 443 12 2299 8 1487 4 812 0.000000 15.0155 792 432
172.31.216.101 49870 172.217.164.141 443 11 4447 6 917 5 3530 4.769736 0.0246 297 k 1146 k
172.31.216.101 49871 185.199.109.153 443 74 68 k 20 2768 54 65 k 4.794380 0.3898 56 k 1344 k
172.31.216.101 49872 172.67.34.140 443 22 5316 10 1567 12 3749 4.932127 0.0236 530 k 1269 k
172.31.216.101 49873 104.26.4.214 443 21 6311 9 1511 12 4800 4.966872 0.0185 651 k 2070 k
172.31.216.101 49874 172.217.13.67 443 23 6238 11 1655 12 4583 6.740849 0.0256 516 k 1430 k
172.31.216.101 49875 172.217.2.99 443 12 4758 6 917 6 3841 15.681095 0.0185 396 k 1661 k
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help
00b0 69 62 ae a4 a3 99 c6 49 89 89 f7 14 3d d9 fc cb ib·····I ····=···
00c0 c8 c2 ec 9f 16 34 69 c2 e6 1a 95 fb c7 93 61 3b ·····4i· ·····a;
00d0 a4 8d 93 96 b1 34 4f 35 cf d7 fc cf 59 57 48 9e ·····4O5 ····YWH·
00e0 f9 dd 03 2e e6 af d4 28 da 3e 1b f5 0d 63 d8 b2 ···.···(·>···c··
00f0 a6 df 02 b8 99 bf 35 bb 0c 8d 79 70 32 3d 5f 57 ·····5· ··yp2=_W
wireshark_Ethernet 3_20200906122244_a05700.pcapng
Packets: 205 · Displayed: 205 (100.0%)
Profile: Default


*Ethernet 3 (port 443)
File Edit View Go Cap
Wireshark · Conversations
Ethernet · 1
IPv4 · 7
Address A
Port A
Addr
172.31.216.101 49866 18.21
172.31.216.101 49870 172.2
172.31.216.101 49871 185.1
172.31.216.101 49872 172.6
172.31.216.101 49873 104.2
172.31.216.101 49874 172.2
172.31.216.101 49875 172.2
Name resolution
wireshark_Ethernet 3_
Wireshark - Follow TCP Stream (tcp.stream eq 2) - Ethernet 3 (port 443)
.....O..|4.f.....y.e.fL...}3.....b.....O..g.IB.....0F.h.
(.dioLKd$...F.....o6..i'....p@,.....
.n...].>...[(..Z.7....#rn.i. .....HK. .8z
`ty.&0.`...$...?... .4G5c|T....W....<0$...4...l.j.T.^`.F1.
....c.........}.....i.....G...Y+f/..8./.e.....3.....a0..]0...U.....0...U.%..0...
+.....+.....0...U.....0.0...U.....cN..VZ.....B....8.W.0...U.#..0....Jjc.}....
9..Ee.....0o..+.....c0a0...+.....0.."http://ocsp.int-x3.letsencrypt.org0/..+.....
0..#http://cert.int-x3.letsencrypt.org/0...U....0
..kbroman.org0L..U. .E0C0...g.....07..+.....0(0&..+.....http://
cps.letsencrypt.org0....
+.....y.....v....Y....@.-/....K..G....4.....s...s[..5.....G0E.
d..P..."Ib.w.....?..*..^c
Vx.!...q.s.2@..*...s.....Q7....{o..8.w...\..}h.....#....W|
W..j..a:.i.....s[..=.....H0F.!....s.l....G..)...p5.k.N.uZ7.?....!..tb.k..k.St%...,..Y1..]
...v.....0
. *.H..
.....h..
.|?Kf8..y .....Q....._.C..n.Nz$...g?.A8..k^.....;...q.r.kF.'?k.|....m.....w}..
3?}.l..P..P...1..{.'....3.)....h.D....2.] S.!..U.
.....W.M..J.GO.>R"^,.Y...q.....$...VB7L7:..X....9.,j$..Ay...+4.._...>o..Y..
0b...]Z....k3.G..C...]...m..DW...z..k....0...0..z.....
.AB...S.sj.....0
. *.H..
.....0?1$0"..U.
..Digital Signature Trust Co.1.0...U....DST Root CA X30..
160317164046Z.
210317164046Z0J1.0 ..U....US1.0...U.
.
Let's Encrypt1#0!..U....Let's Encrypt Authority X30.."0
. *.H..
.....0..
.....Z..G.r]7..hc0..5&.%...5.p./..KA....
5.X..*.h....u....bq.y.`.....xgq.i.....`<H.~.Mw.$.G.Z....7....{....J..A.
6....m<.h.#*B...tg.....Ra..?e.....V.....?.....k
..}.+.e...6u.k.J...Ix/..O* %)..t..1..18....3.C....0..y1.=-6....3j.91....
.d.3...).....}.....}0..y0...U.....0.....0...U.....0...+.....s0q02..
+.....0..&http://isrg.trustid.ocsp.identrust.com0;..+.....0../http://apps.identrust.com/
roots/dstrootcax3.p7c0...U.#..0.....{,q...K.u...`...0T..U. .M0K0...g.....0?..+.....
Packet 29. 9 client pkts, 48 server pkts, 11 turns. Click to select.
Entire conversation (64 kB)
Show and save data as ASCII
Stream 2
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Conversation Types
Close
Help
Profile: Default


*Ethernet 3 (port 443)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
289 27.228792 172.253.122.95 10.199.23.179 UDP 69 443 → 55402 Len=27
290 27.229439 172.253.122.95 10.199.23.179 TCP 54 443 → 50800 [ACK] Seq=1 Ack=1413 Win=68608 Len=0
291 27.229439 172.253.122.95 10.199.23.179 TCP 54 443 → 50800 [ACK] Seq=1 Ack=1842 Win=71424 Len=0
292 27.231564 172.253.122.95 10.199.23.179 TLSv1.3 1466 Server Hello, Change Cipher Spec
293 27.231564 172.253.122.95 10.199.23.179 TCP 1466 443 → 50800 [ACK] Seq=1413 Ack=1842 Win=71424 Len=1412 [TCP
294 27.231586 10.199.23.179 172.253.122.95 TCP 54 50800 → 443 [ACK] Seq=1842 Ack=2825 Win=2100992 Len=0
295 27.231628 172.253.122.95 10.199.23.179 TCP 1466 443 → 50800 [ACK] Seq=2825 Ack=1842 Win=71424 Len=1412 [TCP
296 27.231628 172.253.122.95 10.199.23.179 TCP 1466 443 → 50800 [ACK] Seq=4237 Ack=1842 Win=71424 Len=1412 [TCP
297 27.231628 172.253.122.95 10.199.23.179 TLSv1.3 360 Encrypted Extensions, Certificate, Certificate Verify, Finis
298 27.231643 10.199.23.179 172.253.122.95 TCP 54 50800 → 443 [ACK] Seq=1842 Ack=5955 Win=2100992 Len=0
299 27.232214 10.199.23.179 172.253.122.95 TLSv1.3 128 Change Cipher Spec, Encrypted Extensions, Finished
300 27.234103 172.253.122.95 10.199.23.179 HTTP2 1054 SETTINGS[0], WINDOW_UPDATE[0]
301 27.244911 10.199.23.179 172.253.122.95 TCP 54 50800 → 443 [ACK] Seq=1916 Ack=6955 Win=2099968 Len=0
302 27.248648 172.253.122.95 10.199.23.179 UDP 949 443 → 55402 Len=907
303 27.248908 172.253.122.95 10.199.23.179 UDP 296 443 → 55402 Len=254
304 27.248999 10.199.23.179 172.253.122.95 UDP 77 55402 → 443 Len=35
305 27.274198 10.199.23.179 172.253.122.95 UDP 74 55402 → 443 Len=32
306 27.276266 172.253.122.95 10.199.23.179 UDP 65 443 → 55402 Len=23
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{632B7902-F0FF-488D-9F0D-C3C078B0A7C7}, id 0
Ethernet II, Src: 0a:ff:f7:2f:de:d1 (0a:ff:f7:2f:de:d1), Dst: 0a:23:cb:e2:48:cb (0a:23:cb:e2:48:cb)
Internet Protocol Version 4, Src: 10.199.23.179, Dst: 18.211.136.205
Transmission Control Protocol, Src Port: 50792, Dst Port: 443, Seq: 0, Len: 0
0000 0a 23 cb e2 48 cb 0a ff f7 2f de d1 08 00 45 00
0010 00 34 53 ff 40 00 80 06 00 00 0a c7 17 b3 12 d3
0020 88 cd c6 68 01 bb 4e c7 6e 5b 00 00 00 00 80 02
0030 fa f0 be 40 00 00 02 04 05 b4 01 03 03 08 01 01
wireshark_Ethernet 3_20240428002419_a04628.pcapng
Packets: 306 · Displayed: 306 (100.0%)
Profile: Default