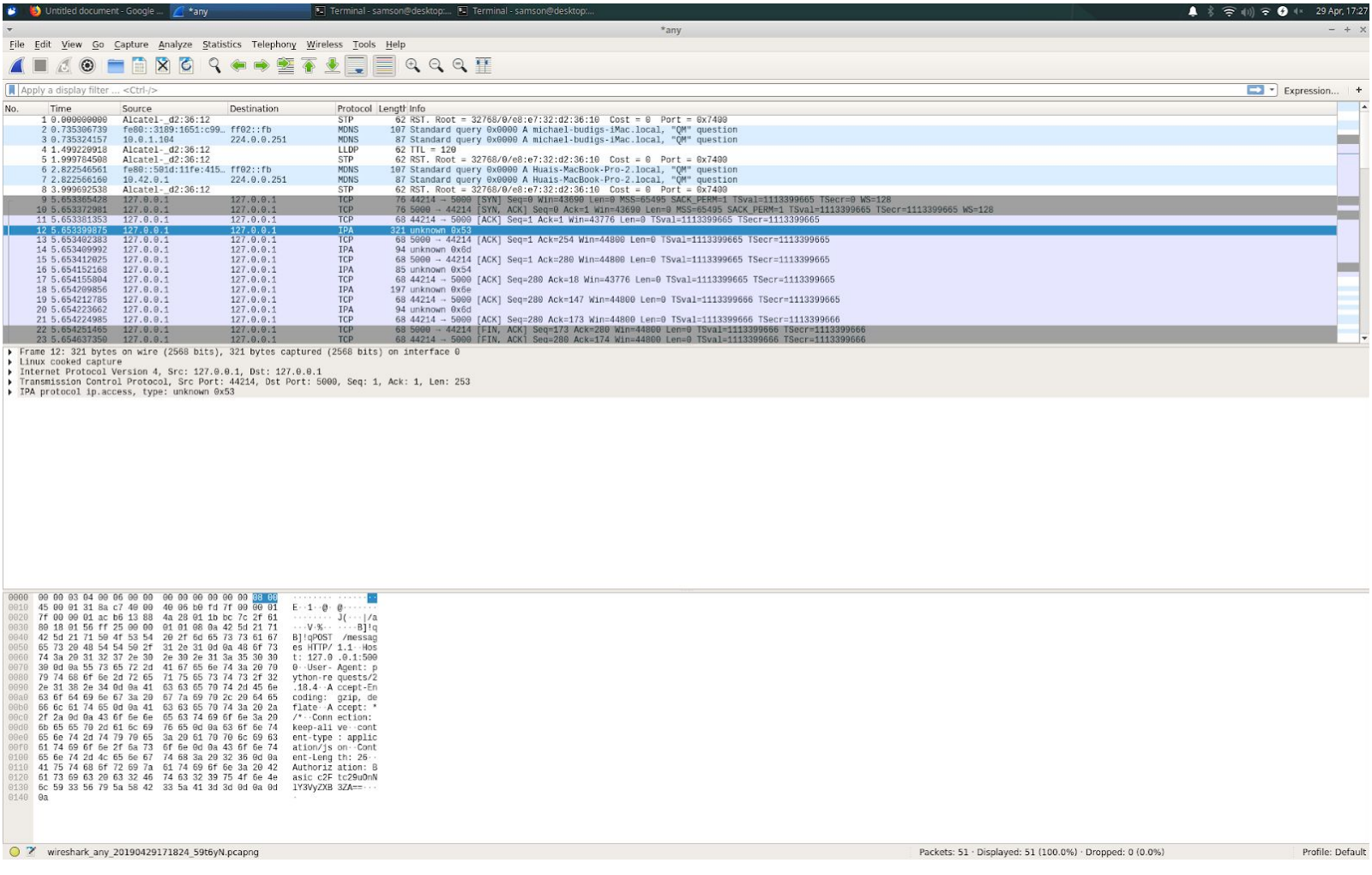
1. Run both the server and client on your machine, and use wireshark to capture the traffic.What information can you obtain by eavesdropping?
I can get the message and the request type and other informations. Screenshots 1 and 2 shows HTTP POST message, 3 and 4 shows HTTP GET message.

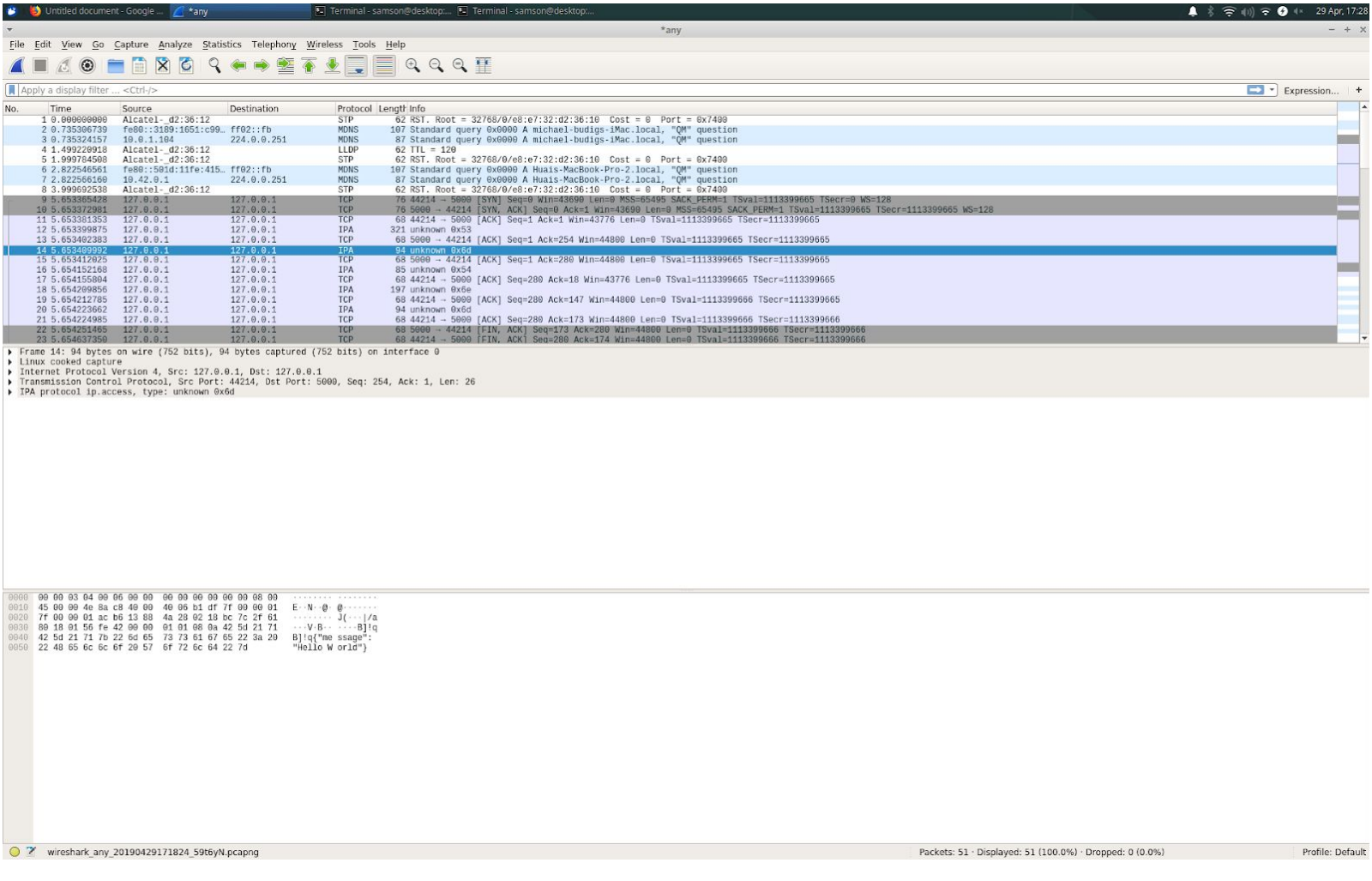
2. What messages are sent out by your machine to perform the attack?
My machine starts to send ARP packets saying “I’m 1.10”.

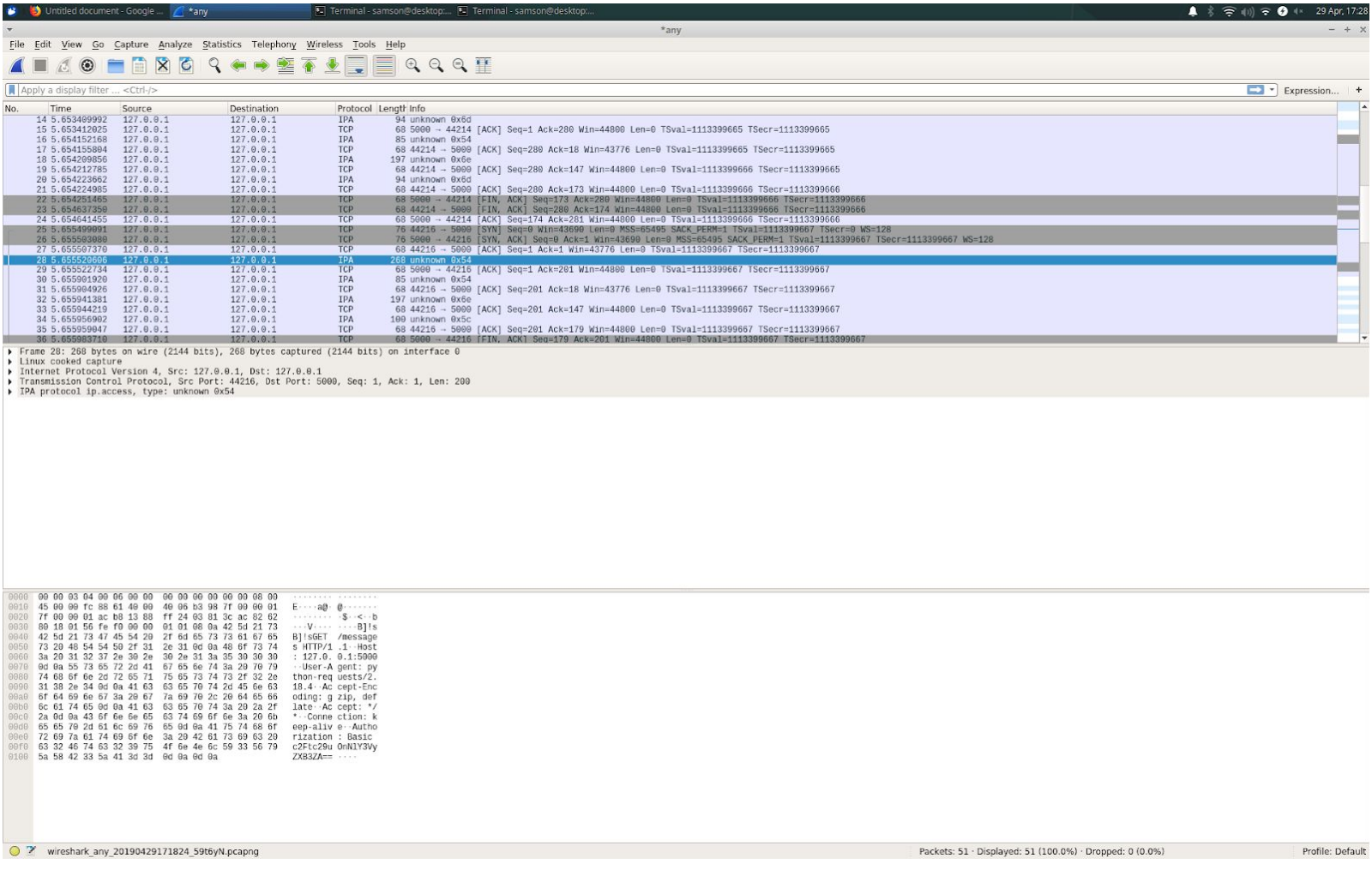
3. Can you see the redirected messages (e.g. using wireshark)? Can you get the HTTP basicauth username and password?
Yes. The username is admin and the password is l4sT_L4b.
Screenshot 5 and 6 shows some of the intercepted messages.
Screenshot 7 and 8 shows where I got the username and password from wireshark and ettercap respectively.

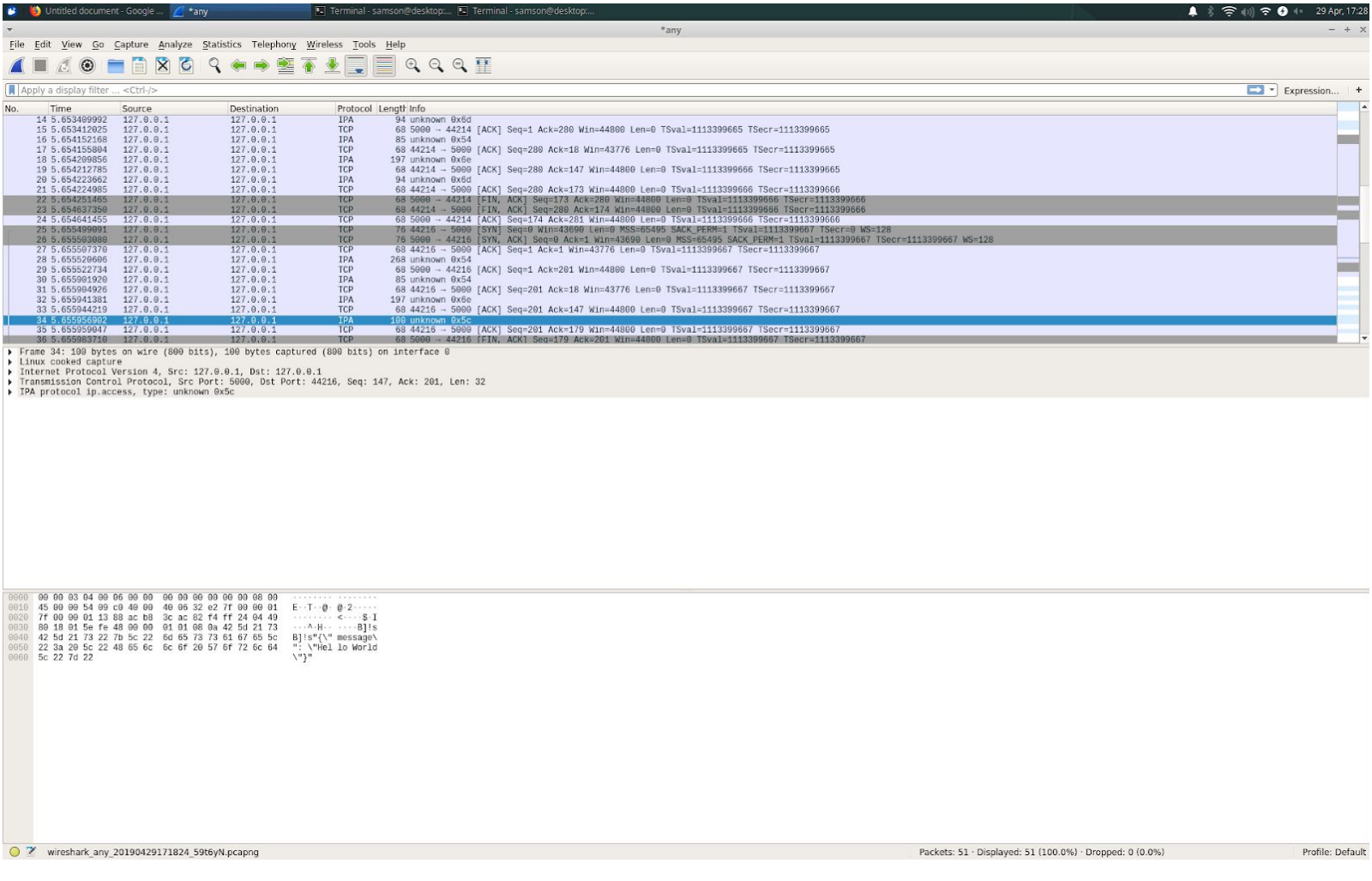
4. TLS and HTTP:
When I first used the default method given in the link, I received the following error:
AttributeError: module 'OpenSSL.SSL' has no attribute 'PROTOCOL_TLSv1_2'
From what I read online, it is depreciated. I therefore removed the 'PROTOCOL_TLSv1_2' and only included my crt and key, which allowed me to run the server code, but the client code still gave me a SSLError: certificate verify failed. This is likely because the certificate is not trusted by the CA.
As a result, I added the line “verify = ‘server.crt’ ” in the client request to use server.crt as CA.
With above changes done, I managed to run the client and server successfully, but only if I run both commands with sudo root privileges. Screenshot 9 shows the two commands and the results.

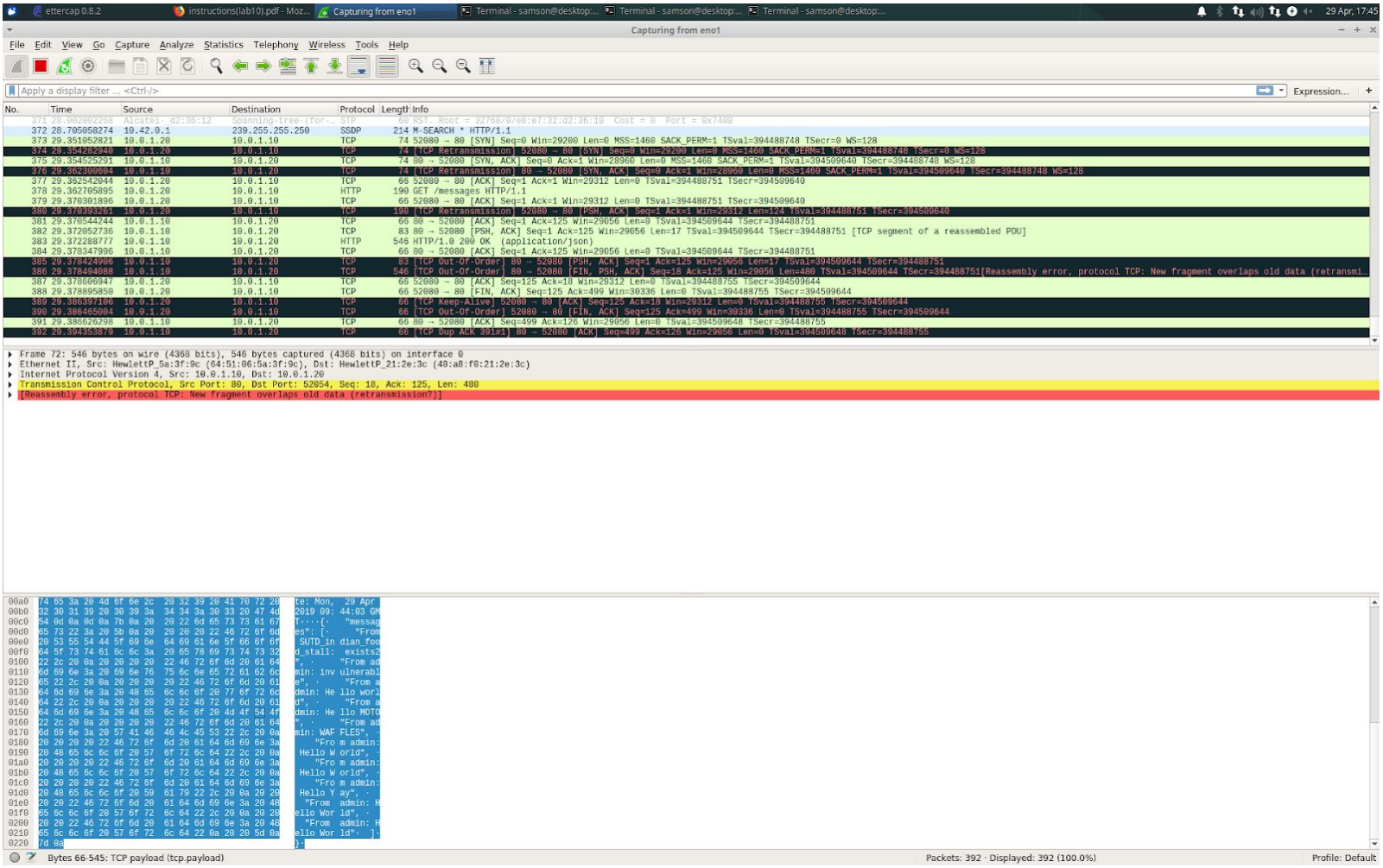
After running the client code to the HTTPS server, Wireshark could no longer read the username, password, or the message, even though it is able to access the certificate information (as it should). Screenshot 10 shows the certificate information captured by Wireshark.

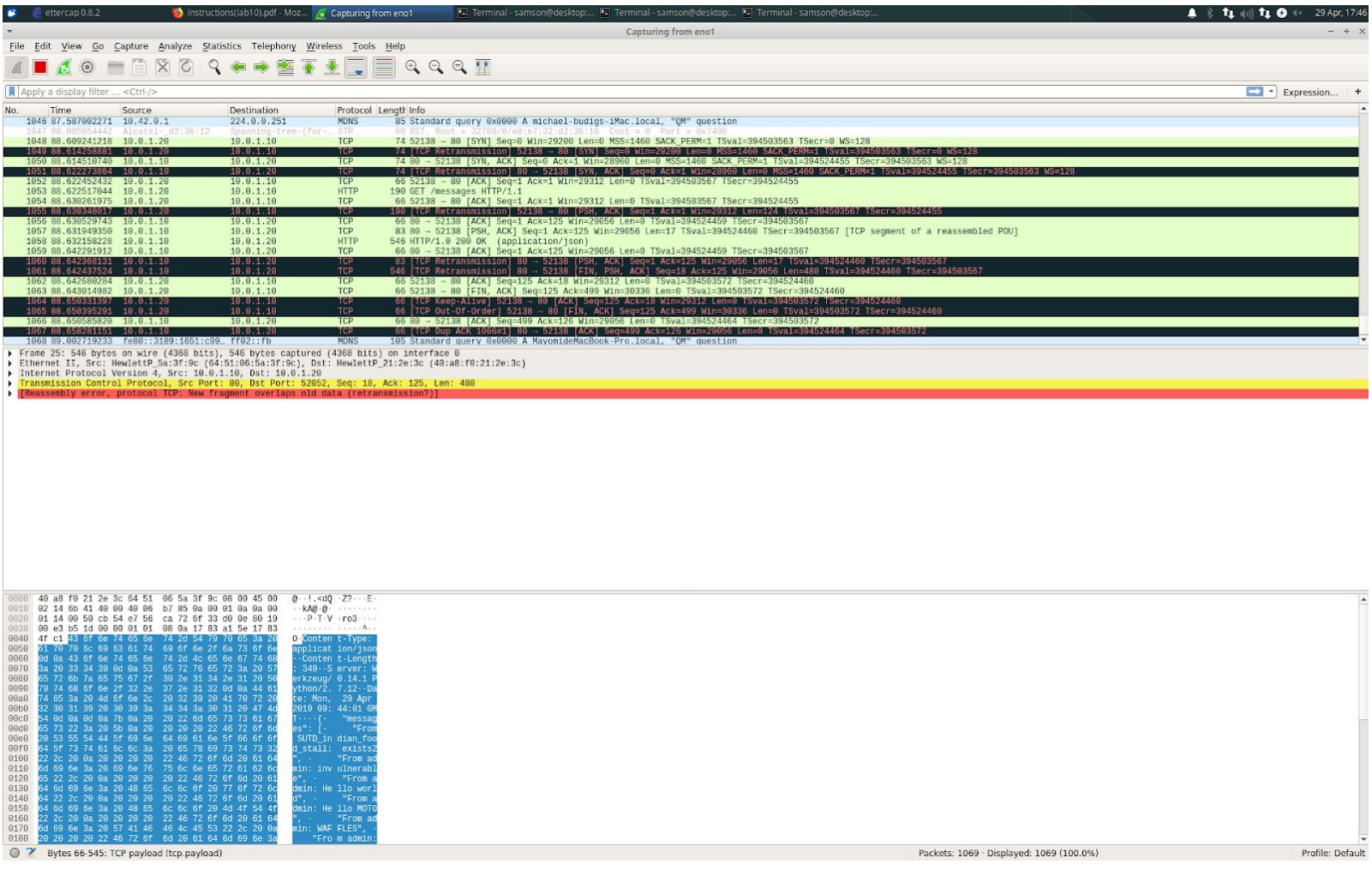

Untitled document - Google ...
*any
Terminal - samson@desktop:...
Terminal - samson@desktop:...
29 Apr, 17:27
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
2 0.735306739 fe80::3189:1651:c99... ff02::fb MDNS 107 Standard query 0x0000 A michael-budigs-iMac.local, "QM" question
3 0.735324157 10.0.1.104 224.0.0.251 MDNS 87 Standard query 0x0000 A michael-budigs-iMac.local, "QM" question
4 1.499220918 Alcatel-_d2:36:12 LLDP 62 TTL = 120
5 1.999784508 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
6 2.822546561 fe80::501d:11fe:415... ff02::fb MDNS 107 Standard query 0x0000 A Huais-MacBook-Pro-2.local, "QM" question
7 2.822566160 10.42.0.1 224.0.0.251 MDNS 87 Standard query 0x0000 A Huais-MacBook-Pro-2.local, "QM" question
8 3.999692538 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
9 5.653365428 127.0.0.1 127.0.0.1 TCP 76 44214 → 5000 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399665 TSecr=0 WS=128
10 5.653372981 127.0.0.1 127.0.0.1 TCP 76 5000 → 44214 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399665 TSecr=1113399665 WS=128
11 5.653381353 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=1113399665 TSecr=1113399665
12 5.653399875 127.0.0.1 127.0.0.1 IPA 321 unknown 0x53
13 5.653402383 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=1 Ack=254 Win=44800 Len=0 TSval=1113399665 TSecr=1113399665
14 5.653409992 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
15 5.653412025 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=1 Ack=280 Win=44800 Len=0 TSval=1113399665 TSecr=1113399665
16 5.654152168 127.0.0.1 127.0.0.1 IPA 85 unknown 0x54
17 5.654155804 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=18 Win=43776 Len=0 TSval=1113399665 TSecr=1113399665
18 5.654209856 127.0.0.1 127.0.0.1 IPA 197 unknown 0x6e
19 5.654212785 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=147 Win=44800 Len=0 TSval=1113399666 TSecr=1113399665
20 5.654223662 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
21 5.654224985 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=173 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
22 5.654251465 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [FIN, ACK] Seq=173 Ack=280 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
23 5.654637350 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [FIN, ACK] Seq=280 Ack=174 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
Frame 12: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 44214, Dst Port: 5000, Seq: 1, Ack: 1, Len: 253
IPA protocol ip.access, type: unknown 0x53
0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00 ....
0010 45 00 01 31 8a c7 40 00 40 06 b0 fd 7f 00 00 01 E··1··@· @·......
0020 7f 00 00 01 ac b6 13 88 4a 28 01 1b bc 7c 2f 61 .... J(···|/a
0030 80 18 01 56 ff 25 00 00 01 01 08 0a 42 5d 21 71 ···V·%·· ····B]!q
0040 42 5d 21 71 50 4f 53 54 20 2f 6d 65 73 73 61 67 B]!qPOST /messag
0050 65 73 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 es HTTP/ 1.1··Hos
0060 74 3a 20 31 32 37 2e 30 2e 30 2e 31 3a 35 30 30 t: 127.0 .0.1:500
0070 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 70 0··User- Agent: p
0080 79 74 68 6f 6e 2d 72 65 71 75 65 73 74 73 2f 32 ython-re quests/2
0090 2e 31 38 2e 34 0d 0a 41 63 63 65 70 74 2d 45 6e .18.4··A ccept-En
00a0 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de
00b0 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 3a 20 2a flate··A ccept: *
00c0 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 /*··Conn ection:
00d0 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 63 6f 6e 74 keep-ali ve··cont
00e0 65 6e 74 2d 74 79 70 65 3a 20 61 70 70 6c 69 63 ent-type : applic
00f0 61 74 69 6f 6e 2f 6a 73 6f 6e 0d 0a 43 6f 6e 74 ation/js on··Cont
0100 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 38 0d 0a ent-Leng th: 28··
0110 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 Authoriz ation: B
0120 61 73 69 63 20 63 32 46 74 63 32 39 75 4f 6e 4e asic c2F tc29uOnN
0130 6c 59 33 56 79 5a 58 42 33 5a 41 3d 3d 0d 0a 0d lY3VyZXB 3ZA==···
0140 0a ·
wireshark_any_20190429171824_59t6yN.pcapng
Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

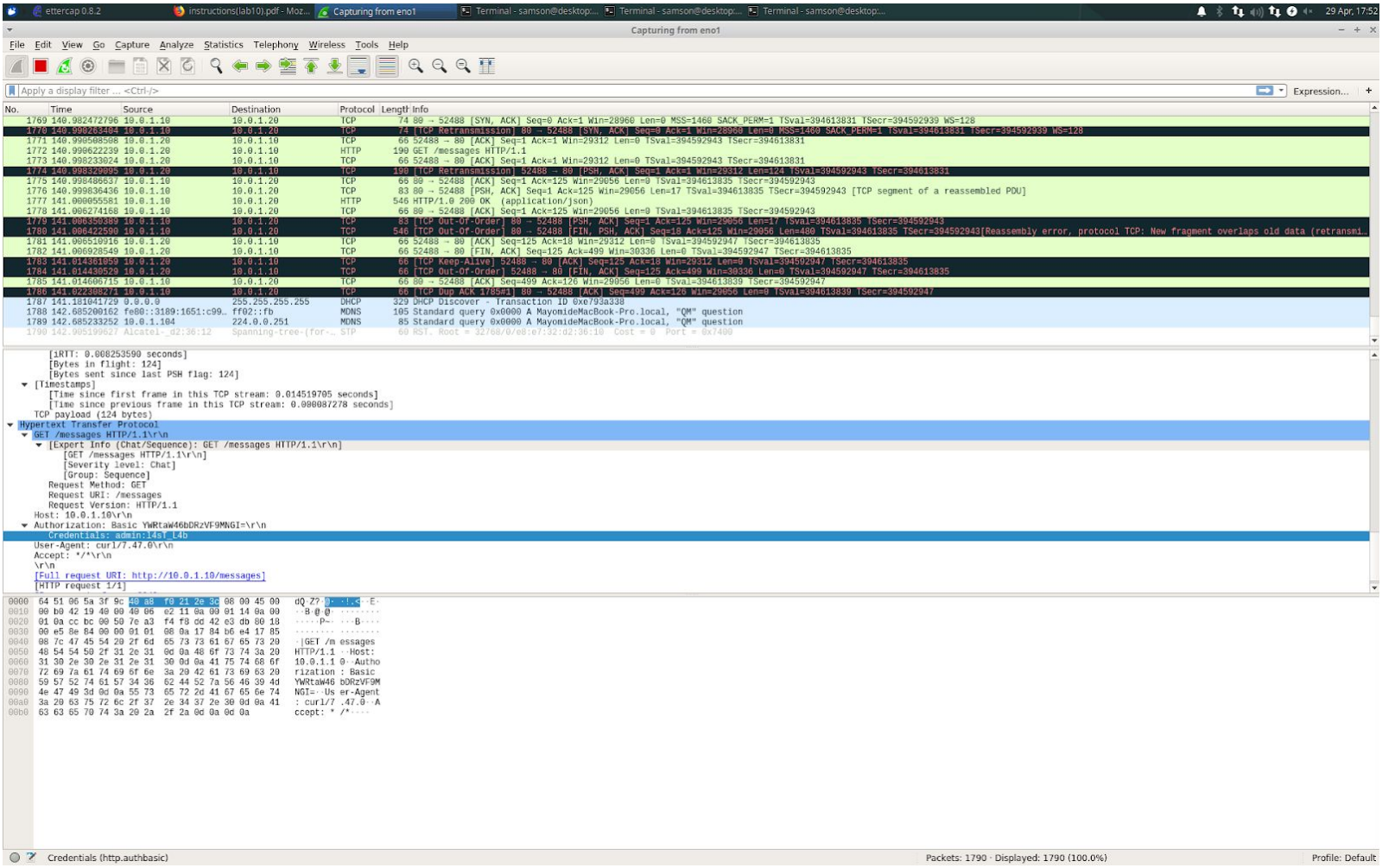

Untitled document - Google ...
*any
Terminal - samson@desktop:...
Terminal - samson@desktop:...
29 Apr, 17:28
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
2 0.735306739 fe80::3189:1651:c99... ff02::fb MDNS 107 Standard query 0x0000 A michael-budigs-iMac.local, "QM" question
3 0.735324157 10.0.1.104 224.0.0.251 MDNS 87 Standard query 0x0000 A michael-budigs-iMac.local, "QM" question
4 1.499220918 Alcatel-_d2:36:12 LLDP 62 TTL = 120
5 1.999784508 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
6 2.822546561 fe80::501d:11fe:415... ff02::fb MDNS 107 Standard query 0x0000 A Huais-MacBook-Pro-2.local, "QM" question
7 2.822566160 10.42.0.1 224.0.0.251 MDNS 87 Standard query 0x0000 A Huais-MacBook-Pro-2.local, "QM" question
8 3.999692538 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
9 5.653365428 127.0.0.1 127.0.0.1 TCP 76 44214 → 5000 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399665 TSecr=0 WS=128
10 5.653372981 127.0.0.1 127.0.0.1 TCP 76 5000 → 44214 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399665 TSecr=1113399665 WS=128
11 5.653381353 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=1113399665 TSecr=1113399665
12 5.653399875 127.0.0.1 127.0.0.1 IPA 321 unknown 0x53
13 5.653402383 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=1 Ack=254 Win=44800 Len=0 TSval=1113399665 TSecr=1113399665
14 5.653409992 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
15 5.653412025 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=1 Ack=280 Win=44800 Len=0 TSval=1113399665 TSecr=1113399665
16 5.654152168 127.0.0.1 127.0.0.1 IPA 85 unknown 0x54
17 5.654155804 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=18 Win=43776 Len=0 TSval=1113399665 TSecr=1113399665
18 5.654209856 127.0.0.1 127.0.0.1 IPA 197 unknown 0x6e
19 5.654212785 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=147 Win=44800 Len=0 TSval=1113399666 TSecr=1113399665
20 5.654223662 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
21 5.654224985 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=173 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
22 5.654251465 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [FIN, ACK] Seq=173 Ack=280 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
23 5.654637350 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [FIN, ACK] Seq=280 Ack=174 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
Frame 14: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 44214, Dst Port: 5000, Seq: 254, Ack: 1, Len: 26
IPA protocol ip.access, type: unknown 0x6d
0000 00 00 03 04 00 06 00 00 00 00 00 00 08 00 ....
0010 45 00 00 4e 8a c8 40 00 40 06 b1 df 7f 00 00 01 E··N··@· @·......
0020 7f 00 00 01 ac b6 13 88 4a 29 02 18 bc 7c 2f 61 .... J(···|/a
0030 80 18 01 56 fe 42 00 00 01 01 08 0a 42 5d 21 71 ···V·B·· ····B]!q
0040 42 5d 21 71 7b 22 6d 65 73 73 61 67 65 22 3a 20 B]!q{"me ssage":
0050 22 48 65 6c 6c 6f 20 57 6f 72 6c 64 22 7d "Hello W orld"}
wireshark_any_20190429171824_59t6yN.pcapng
Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

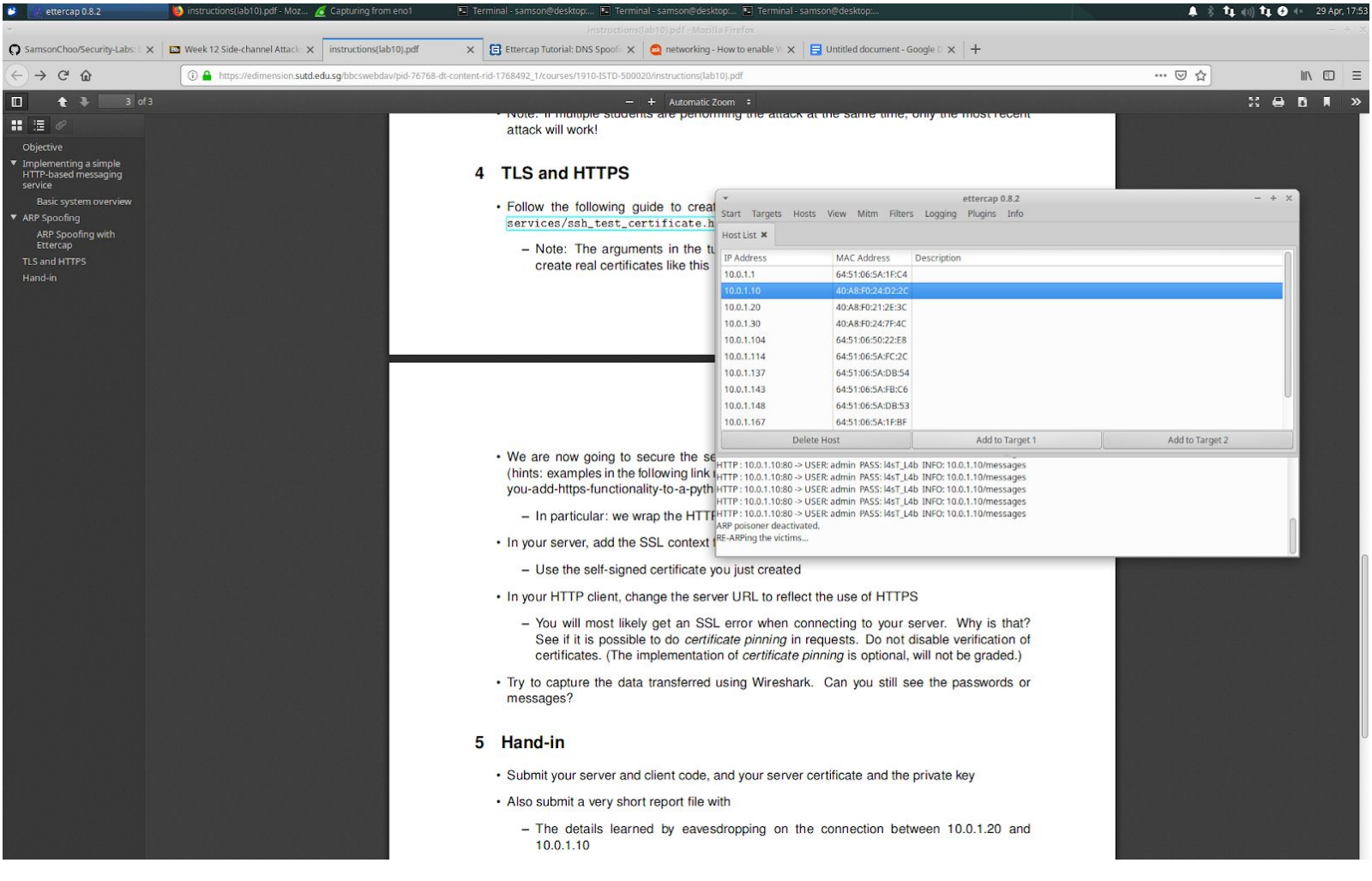

Untitled document - Google ...
*any
Terminal - samson@desktop:...
Terminal - samson@desktop:...
29 Apr, 17:28
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14 5.653409992 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
15 5.653412025 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=1 Ack=280 Win=44800 Len=0 TSval=1113399665 TSecr=1113399665
16 5.654152168 127.0.0.1 127.0.0.1 IPA 85 unknown 0x54
17 5.654155804 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=18 Win=43776 Len=0 TSval=1113399665 TSecr=1113399665
18 5.654209856 127.0.0.1 127.0.0.1 IPA 197 unknown 0x6e
19 5.654212785 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=147 Win=44800 Len=0 TSval=1113399666 TSecr=1113399665
20 5.654223662 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
21 5.654224985 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=173 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
22 5.654251465 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [FIN, ACK] Seq=173 Ack=280 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
23 5.654637350 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [FIN, ACK] Seq=280 Ack=174 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
24 5.654641455 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=174 Ack=281 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
25 5.655499091 127.0.0.1 127.0.0.1 TCP 76 44216 → 5000 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399667 TSecr=0 WS=128
26 5.655503080 127.0.0.1 127.0.0.1 TCP 76 5000 → 44216 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399667 TSecr=1113399667 WS=128
27 5.655507370 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=1113399667 TSecr=1113399667
28 5.655520606 127.0.0.1 127.0.0.1 IPA 268 unknown 0x54
29 5.655522734 127.0.0.1 127.0.0.1 TCP 68 5000 → 44216 [ACK] Seq=1 Ack=201 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
30 5.655901920 127.0.0.1 127.0.0.1 IPA 85 unknown 0x54
31 5.655904926 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=201 Ack=18 Win=43776 Len=0 TSval=1113399667 TSecr=1113399667
32 5.655941381 127.0.0.1 127.0.0.1 IPA 197 unknown 0x6e
33 5.655944219 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=201 Ack=147 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
34 5.655956902 127.0.0.1 127.0.0.1 IPA 100 unknown 0x5c
35 5.655959047 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=201 Ack=179 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
36 5.655983710 127.0.0.1 127.0.0.1 TCP 68 5000 → 44216 [FIN, ACK] Seq=179 Ack=201 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
Frame 28: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 44216, Dst Port: 5000, Seq: 1, Ack: 1, Len: 200
IPA protocol ip.access, type: unknown 0x54
0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00 ....
0010 45 00 00 fc 88 61 40 00 40 06 b3 98 7f 00 00 01 E....a@. @.......
0020 7f 00 00 01 ac b8 13 88 ff 24 03 81 3c ac 82 62 ....$..<..b
0030 80 18 01 56 fe f0 00 00 01 01 08 0a 42 5d 21 73 ...V.... ....B]!s
0040 42 5d 21 73 47 45 54 20 2f 6d 65 73 73 61 67 65 B]!sGET /message
0050 73 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 s HTTP/1 .1..Host
0060 3a 20 31 32 37 2e 30 2e 30 2e 31 3a 35 30 30 30 : 127.0. 0.1:5000
0070 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 70 79 ..User-A gent: py
0080 74 68 6f 6e 2d 72 65 71 75 65 73 74 73 2f 32 2e thon-req uests/2.
0090 31 38 2e 34 0d 0a 41 63 63 65 70 74 2d 45 6e 63 18.4..Ac cept-Enc
00a0 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 oding: g zip, def
00b0 6c 61 74 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f late..Ac cept: */
00c0 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b *..Conne ction: k
00d0 65 65 70 2d 61 6c 69 76 65 0d 0a 41 75 74 68 6f eep-aliv e..Autho
00e0 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 rization : Basic
00f0 63 32 46 74 63 32 39 75 4f 6e 4e 6c 59 33 56 79 c2Ftc29u OnNlY3Vy
0100 5a 58 42 33 5a 41 3d 3d 0d 0a 0d 0a ZXB3ZA== ....
wireshark_any_20190429171824_59t6yN.pcapng
Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

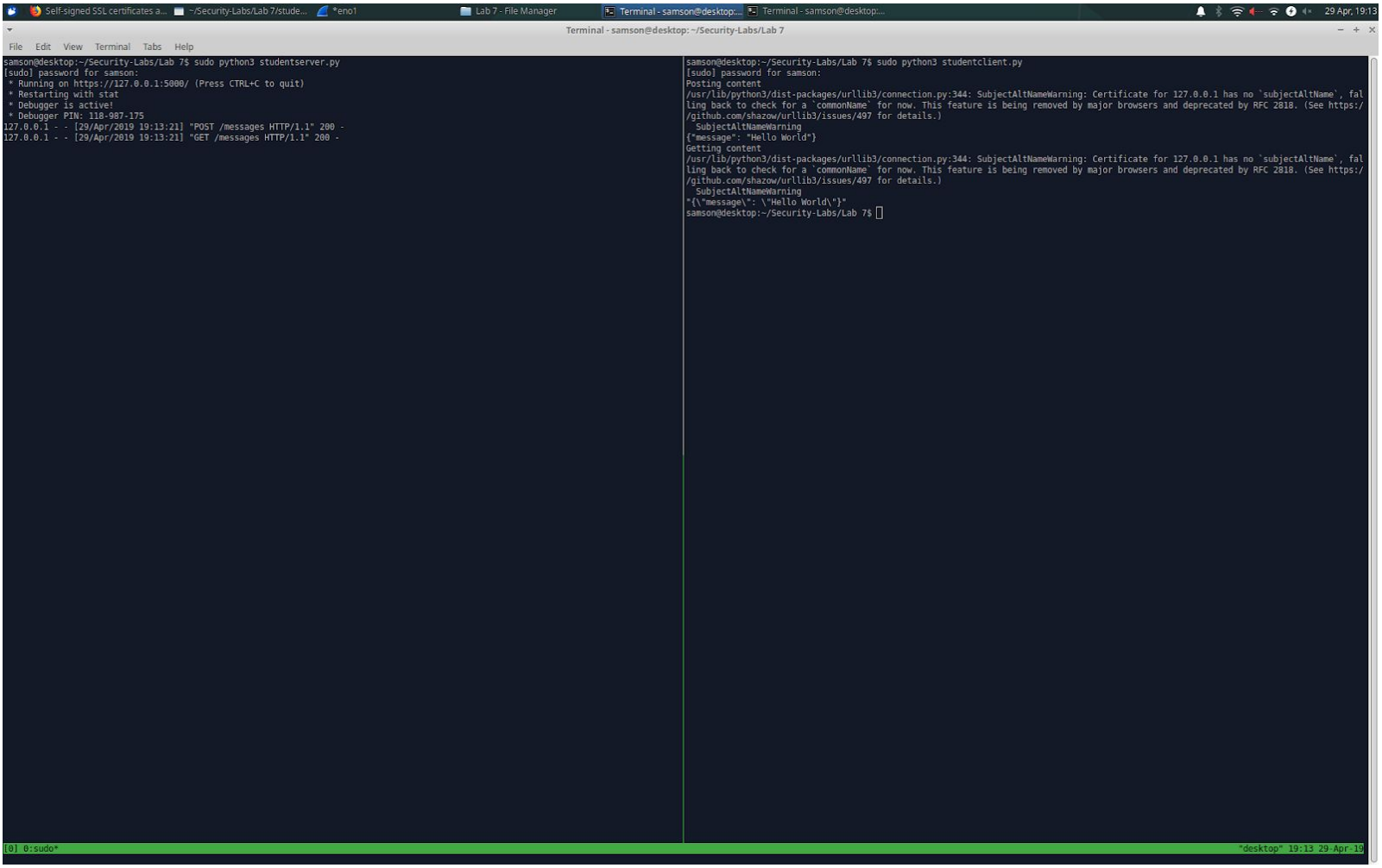

Untitled document - Google ...
*any
Terminal - samson@desktop:...
Terminal - samson@desktop:...
29 Apr, 17:28
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14 5.653409992 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
15 5.653412025 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=1 Ack=280 Win=44800 Len=0 TSval=1113399665 TSecr=1113399665
16 5.654152168 127.0.0.1 127.0.0.1 IPA 85 unknown 0x54
17 5.654155804 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=18 Win=43776 Len=0 TSval=1113399665 TSecr=1113399665
18 5.654209856 127.0.0.1 127.0.0.1 IPA 197 unknown 0x6e
19 5.654212785 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=147 Win=44800 Len=0 TSval=1113399666 TSecr=1113399665
20 5.654223662 127.0.0.1 127.0.0.1 IPA 94 unknown 0x6d
21 5.654224985 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [ACK] Seq=280 Ack=173 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
22 5.654251465 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [FIN, ACK] Seq=173 Ack=280 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
23 5.654637350 127.0.0.1 127.0.0.1 TCP 68 44214 → 5000 [FIN, ACK] Seq=280 Ack=174 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
24 5.654641455 127.0.0.1 127.0.0.1 TCP 68 5000 → 44214 [ACK] Seq=174 Ack=281 Win=44800 Len=0 TSval=1113399666 TSecr=1113399666
25 5.655499091 127.0.0.1 127.0.0.1 TCP 76 44216 → 5000 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399667 TSecr=0 WS=128
26 5.655503080 127.0.0.1 127.0.0.1 TCP 76 5000 → 44216 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1113399667 TSecr=1113399667 WS=128
27 5.655507370 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=1113399667 TSecr=1113399667
28 5.655520606 127.0.0.1 127.0.0.1 IPA 268 unknown 0x54
29 5.655522734 127.0.0.1 127.0.0.1 TCP 68 5000 → 44216 [ACK] Seq=1 Ack=201 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
30 5.655901920 127.0.0.1 127.0.0.1 IPA 85 unknown 0x54
31 5.655904926 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=201 Ack=18 Win=43776 Len=0 TSval=1113399667 TSecr=1113399667
32 5.655941381 127.0.0.1 127.0.0.1 IPA 197 unknown 0x6e
33 5.655944219 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=201 Ack=147 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
34 5.655956902 127.0.0.1 127.0.0.1 IPA 100 unknown 0x5c
35 5.655959047 127.0.0.1 127.0.0.1 TCP 68 44216 → 5000 [ACK] Seq=201 Ack=179 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
36 5.655983710 127.0.0.1 127.0.0.1 TCP 68 5000 → 44216 [FIN, ACK] Seq=179 Ack=201 Win=44800 Len=0 TSval=1113399667 TSecr=1113399667
Frame 34: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 5000, Dst Port: 44216, Seq: 147, Ack: 201, Len: 32
IPA protocol ip.access, type: unknown 0x5c
0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00 ....
0010 45 00 00 54 09 c0 40 00 40 06 32 e2 7f 00 00 01 E..T..@. @.2.....
0020 7f 00 00 01 13 88 ac b8 3c ac 82 f4 ff 24 04 49 .... <....$.I
0030 80 18 01 5e fe 48 00 00 01 01 08 0a 42 5d 21 73 ...^.H.. ....B]!s
0040 42 5d 21 73 22 7b 5c 22 6d 65 73 73 61 67 65 5c B]!s"{\" message\
0050 22 3a 20 5c 22 48 65 6c 6c 6f 20 57 6f 72 6c 64 ": \"Hel lo World
0060 5c 22 7d 22 \"}"
wireshark_any_20190429171824_59t6yN.pcapng
Packets: 51 · Displayed: 51 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

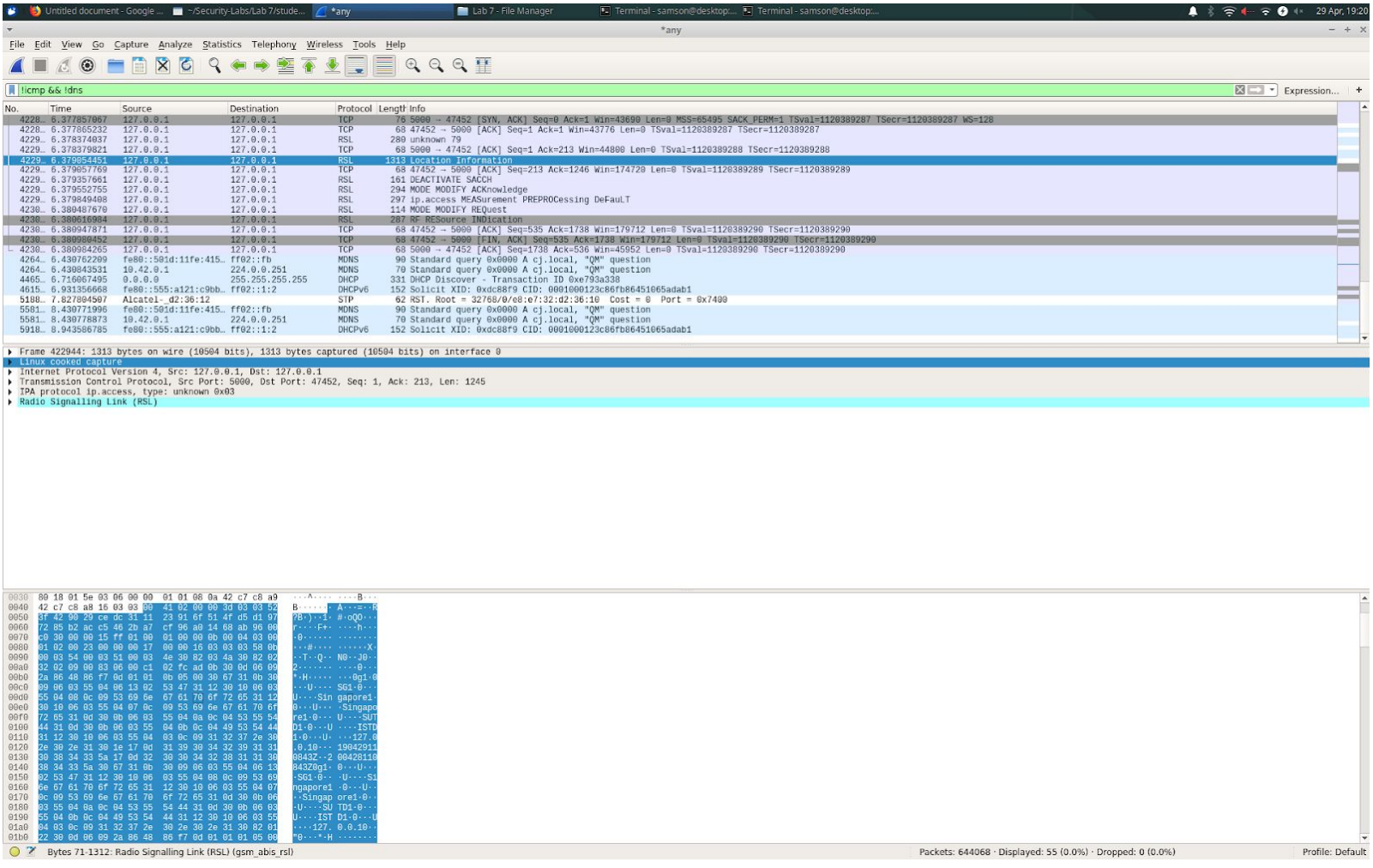

ettercap 0.8.2
instructions(lab10).pdf - Moz...
Capturing from eno1
Terminal - samson@desktop:...
Terminal - samson@desktop:...
Terminal - samson@desktop:...
29 Apr, 17:45
Capturing from eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
371 28.002002268 Alcatel-_d2:36:12 Spanning-tree-(for-... STP 60 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
372 28.705058274 10.42.0.1 239.255.255.250 SSDP 214 M-SEARCH * HTTP/1.1
373 29.351052821 10.0.1.20 10.0.1.10 TCP 74 52080 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=394488748 TSecr=0 WS=128
374 29.354282940 10.0.1.20 10.0.1.10 TCP 74 [TCP Retransmission] 52080 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=394488748 TSecr=0 WS=128
375 29.354525291 10.0.1.10 10.0.1.20 TCP 74 80 → 52080 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=394509640 TSecr=394488748 WS=128
376 29.362309684 10.0.1.10 10.0.1.20 TCP 74 [TCP Retransmission] 80 → 52080 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=394509640 TSecr=394488748 WS=128
377 29.362542044 10.0.1.20 10.0.1.10 TCP 66 52080 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=394488751 TSecr=394509640
378 29.362705895 10.0.1.20 10.0.1.10 HTTP 190 GET /messages HTTP/1.1
379 29.370301896 10.0.1.10 10.0.1.20 TCP 66 52080 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=394488751 TSecr=394509640
380 29.370393261 10.0.1.20 10.0.1.10 TCP 190 [TCP Retransmission] 52080 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=124 TSval=394488751 TSecr=394509640
381 29.370544244 10.0.1.10 10.0.1.20 TCP 66 80 → 52080 [ACK] Seq=1 Ack=125 Win=29056 Len=0 TSval=394509644 TSecr=394488751
382 29.372052736 10.0.1.10 10.0.1.20 TCP 83 80 → 52080 [PSH, ACK] Seq=1 Ack=125 Win=29056 Len=17 TSval=394509644 TSecr=394488751 [TCP segment of a reassembled PDU]
383 29.372308777 10.0.1.10 10.0.1.20 HTTP 546 HTTP/1.0 200 OK (application/json)
384 29.378347996 10.0.1.10 10.0.1.20 TCP 66 80 → 52080 [ACK] Seq=1 Ack=125 Win=29056 Len=0 TSval=394509644 TSecr=394488751
385 29.378424906 10.0.1.10 10.0.1.20 TCP 83 [TCP Out-Of-Order] 80 → 52080 [PSH, ACK] Seq=1 Ack=125 Win=29056 Len=17 TSval=394509644 TSecr=394488751
386 29.378494088 10.0.1.10 10.0.1.20 TCP 546 [TCP Out-Of-Order] 80 → 52080 [FIN, PSH, ACK] Seq=18 Ack=125 Win=29056 Len=480 TSval=394509644 TSecr=394488751[Reassembly error, protocol TCP: New fragment overlaps old data (retransmi...
387 29.378606947 10.0.1.10 10.0.1.20 TCP 66 52080 → 80 [ACK] Seq=125 Ack=18 Win=29312 Len=0 TSval=394488755 TSecr=394509644
388 29.378895850 10.0.1.20 10.0.1.10 TCP 66 52080 → 80 [FIN, ACK] Seq=125 Ack=499 Win=30336 Len=0 TSval=394488755 TSecr=394509644
389 29.386397106 10.0.1.20 10.0.1.10 TCP 66 [TCP Keep-Alive] 52080 → 80 [ACK] Seq=125 Ack=18 Win=29312 Len=0 TSval=394488755 TSecr=394509644
390 29.386465004 10.0.1.20 10.0.1.10 TCP 66 [TCP Out-Of-Order] 52080 → 80 [FIN, ACK] Seq=125 Ack=499 Win=30336 Len=0 TSval=394488755 TSecr=394509644
391 29.386626298 10.0.1.10 10.0.1.20 TCP 66 80 → 52080 [ACK] Seq=499 Ack=126 Win=29056 Len=0 TSval=394509648 TSecr=394488755
392 29.394353879 10.0.1.10 10.0.1.20 TCP 66 [TCP Dup ACK 391#1] 80 → 52080 [ACK] Seq=499 Ack=126 Win=29056 Len=0 TSval=394509648 TSecr=394488755
Frame 72: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface 0
Ethernet II, Src: HewlettP_5a:3f:9c (64:51:06:5a:3f:9c), Dst: HewlettP_21:2e:3c (40:a8:f0:21:2e:3c)
Internet Protocol Version 4, Src: 10.0.1.10, Dst: 10.0.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 52054, Seq: 18, Ack: 125, Len: 480
[Reassembly error, protocol TCP: New fragment overlaps old data (retransmission?)]
00a0 74 65 3a 20 4d 6f 6e 2c 20 32 39 20 41 70 72 20 te: Mon, 29 Apr
00b0 32 30 31 39 20 30 39 3a 34 34 3a 30 33 20 47 4d 2019 09: 44:03 GM
00c0 54 0d 0a 0d 0a 7b 0a 20 20 22 6d 65 73 73 61 67 T····{· "messag
00d0 65 73 22 3a 20 5b 0a 20 20 20 20 22 46 72 6f 6d es": [· "From
00e0 20 53 55 54 44 5f 69 6e 20 64 69 61 6e 5f 66 6f SUTD_in dian_fo
00f0 64 5f 73 74 61 6c 6c 3a 20 65 78 69 73 74 73 32 d_stall: exists2
0100 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 64 ", · "From ad
0110 6d 69 6e 3a 20 69 6e 76 75 6c 6e 65 72 61 62 6c min: inv ulnerabl
0120 65 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 e", · "From a
0130 64 6d 69 6e 3a 20 48 65 6c 6c 6f 20 77 6f 72 6c dmin: He llo worl
0140 64 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 d", · "From a
0150 64 6d 69 6e 3a 20 48 65 6c 6c 6f 20 4d 4f 54 4f dmin: He llo MOTO
0160 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 64 ", · "From ad
0170 6d 69 6e 3a 20 57 41 46 46 4c 45 53 22 2c 20 0a min: WAF FLES", ·
0180 20 20 20 20 22 46 72 6f 6d 20 61 64 6d 69 6e 3a "Fro m admin:
0190 20 48 65 6c 6c 6f 20 57 6f 72 6c 64 22 2c 20 0a Hello W orld", ·
01a0 20 20 20 20 22 46 72 6f 6d 20 61 64 6d 69 6e 3a "Fro m admin:
01b0 20 48 65 6c 6c 6f 20 57 6f 72 6c 64 22 2c 20 0a Hello W orld", ·
01c0 20 20 20 20 22 46 72 6f 6d 20 61 64 6d 69 6e 3a "Fro m admin:
01d0 20 48 65 6c 6c 6f 20 59 61 79 22 2c 20 0a 20 20 Hello Y ay", ·
01e0 20 20 22 46 72 6f 6d 20 61 64 6d 69 6e 3a 20 48 "From admin: H
01f0 65 6c 6c 6f 20 57 6f 72 6c 64 22 2c 20 0a 20 20 ello Wor ld", ·
0200 20 20 22 46 72 6f 6d 20 61 64 6d 69 6e 3a 20 48 "From admin: H
0210 65 6c 6c 6f 20 57 6f 72 6c 64 22 0a 20 20 5d 0a ello Wor ld".]·
0220 7d 0a }·
Bytes 66-545: TCP payload (tcp.payload)
Packets: 392 · Displayed: 392 (100.0%)
Profile: Default


ettercap 0.8.2
instructions(lab10).pdf - Moz...
Capturing from eno1
Terminal - samson@desktop:...
Terminal - samson@desktop:...
Terminal - samson@desktop:...
29 Apr, 17:46
Capturing from eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1046 87.587002271 10.42.0.1 224.0.0.251 MDNS 85 Standard query 0x0000 A michael-budigs-iMac.local, "QM" question
1047 88.005954442 Alcatel-_d2:36:12 Spanning-tree-(for-... STP 60 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
1048 88.609241218 10.0.1.20 10.0.1.10 TCP 74 52138 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=394503563 TSecr=0 WS=128
1049 88.614235881 10.0.1.20 10.0.1.10 TCP 74 [TCP Retransmission] 52138 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=394503563 TSecr=0 WS=128
1050 88.614510740 10.0.1.10 10.0.1.20 TCP 74 80 → 52138 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=394524455 TSecr=394503563 WS=128
1051 88.622273864 10.0.1.10 10.0.1.20 TCP 74 [TCP Retransmission] 80 → 52138 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=394524455 TSecr=394503563 WS=128
1052 88.622452432 10.0.1.20 10.0.1.10 TCP 66 52138 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=394503567 TSecr=394524455
1053 88.622517044 10.0.1.20 10.0.1.10 HTTP 190 GET /messages HTTP/1.1
1054 88.630261975 10.0.1.20 10.0.1.10 TCP 66 52138 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=394503567 TSecr=394524455
1055 88.630348917 10.0.1.20 10.0.1.10 TCP 190 [TCP Retransmission] 52138 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=124 TSval=394503567 TSecr=394524455
1056 88.630529743 10.0.1.10 10.0.1.20 TCP 66 80 → 52138 [ACK] Seq=1 Ack=125 Win=29056 Len=0 TSval=394524459 TSecr=394503567
1057 88.631949350 10.0.1.10 10.0.1.20 TCP 83 80 → 52138 [PSH, ACK] Seq=1 Ack=125 Win=29056 Len=17 TSval=394524460 TSecr=394503567 [TCP segment of a reassembled PDU]
1058 88.632158228 10.0.1.10 10.0.1.20 HTTP 546 HTTP/1.0 200 OK (application/json)
1059 88.642291912 10.0.1.10 10.0.1.20 TCP 66 80 → 52138 [ACK] Seq=1 Ack=125 Win=29056 Len=0 TSval=394524459 TSecr=394503567
1060 88.642368131 10.0.1.10 10.0.1.20 TCP 83 [TCP Retransmission] 80 → 52138 [PSH, ACK] Seq=1 Ack=125 Win=29056 Len=17 TSval=394524460 TSecr=394503567
1061 88.642437524 10.0.1.10 10.0.1.20 TCP 546 [TCP Retransmission] 80 → 52138 [FIN, PSH, ACK] Seq=18 Ack=125 Win=29056 Len=480 TSval=394524460 TSecr=394503567
1062 88.642680284 10.0.1.20 10.0.1.10 TCP 66 52138 → 80 [ACK] Seq=125 Ack=18 Win=29312 Len=0 TSval=394503572 TSecr=394524460
1063 88.643014982 10.0.1.10 10.0.1.20 TCP 66 52138 → 80 [FIN, ACK] Seq=125 Ack=499 Win=30336 Len=0 TSval=394503572 TSecr=394524460
1064 88.650331397 10.0.1.20 10.0.1.10 TCP 66 [TCP Keep-Alive] 52138 → 80 [ACK] Seq=125 Ack=18 Win=29312 Len=0 TSval=394503572 TSecr=394524460
1065 88.650395291 10.0.1.20 10.0.1.10 TCP 66 [TCP Out-Of-Order] 52138 → 80 [FIN, ACK] Seq=125 Ack=499 Win=30336 Len=0 TSval=394503572 TSecr=394524460
1066 88.650585820 10.0.1.10 10.0.1.20 TCP 66 80 → 52138 [ACK] Seq=499 Ack=126 Win=29056 Len=0 TSval=394524464 TSecr=394503572
1067 88.650831151 10.0.1.10 10.0.1.20 TCP 66 [TCP Dup ACK 1066#1] 80 → 52138 [ACK] Seq=499 Ack=126 Win=29056 Len=0 TSval=394524464 TSecr=394503572
1068 89.090219231 fe80::3189:1651:c99… ff02::fb MDNS 105 Standard query 0x0000 A MayomideMacBook-Pro.local, "QM" question
Frame 25: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface 0
Ethernet II, Src: HewlettP_5a:3f:9c (64:51:06:5a:3f:9c), Dst: HewlettP_21:2e:3c (40:a8:f0:21:2e:3c)
Internet Protocol Version 4, Src: 10.0.1.10, Dst: 10.0.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 52052, Seq: 18, Ack: 125, Len: 480
[Reassembly error, protocol TCP: New fragment overlaps old data (retransmission?)]
0000 40 a8 f0 21 2e 3c 64 51 06 5a 3f 9c 08 00 45 00 @··!.<dQ ·Z?···E·
0010 02 14 6b 41 40 00 40 06 b7 85 0a 00 01 0a 0a 00 ··kA@·@· ········
0020 01 14 00 50 cb 54 e7 56 ca 72 6f 33 c0 0e 80 19 ···P·T·V ·ro3····
0030 00 e3 b5 1d 00 00 01 01 08 0a 17 83 a1 5e 17 83 ········ ·····^··
0040 4f c1 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 O·Conten t-Type:
0050 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e applicat ion/json
0060 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 ··Conten t-Length
0070 3a 20 33 34 39 0d 0a 53 65 72 76 65 72 3a 20 57 : 349··S erver: W
0080 65 72 6b 7a 65 75 67 2f 30 2e 31 34 2e 31 20 50 erkzeug/ 0.14.1 P
0090 79 74 68 6f 6e 2f 32 2e 37 2e 31 32 0d 0a 44 61 ython/2. 7.12··Da
00a0 74 65 3a 20 4d 6f 6e 2c 20 32 39 20 41 70 72 20 te: Mon, 29 Apr
00b0 32 30 31 39 20 30 39 3a 34 34 3a 30 31 20 47 4d 2019 09: 44:01 GM
00c0 54 0d 0a 0d 0a 7b 0a 20 20 22 6d 65 73 73 61 67 T····{· "messag
00d0 65 73 22 3a 20 5b 0a 20 20 20 20 22 46 72 6f 6d es": [· "From
00e0 20 53 55 54 44 5f 69 6e 20 64 69 61 6e 5f 66 6f SUTD_in dian_fo
00f0 64 5f 73 74 61 6c 6c 3a 20 65 78 69 73 74 73 32 d_stall: exists2
0100 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 64 ", · "From ad
0110 6d 69 6e 3a 20 69 6e 76 75 6c 6e 65 72 61 62 6c min: inv ulnerabl
0120 65 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 e", · "From a
0130 64 6d 69 6e 3a 20 48 65 6c 6c 6f 20 77 6f 72 6c dmin: He llo worl
0140 64 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 d", · "From a
0150 64 6d 69 6e 3a 20 48 65 6c 6c 6f 20 4d 4f 54 4f dmin: He llo MOTO
0160 22 2c 20 0a 20 20 20 20 22 46 72 6f 6d 20 61 64 ", · "From ad
0170 6d 69 6e 3a 20 57 41 46 46 4c 45 53 22 2c 20 0a min: WAF FLES", ·
0180 20 20 20 20 22 46 72 6f 6d 20 61 64 6d 69 6e 3a "Fro m admin:
Bytes 66-545: TCP payload (tcp.payload)
Packets: 1069 · Displayed: 1069 (100.0%)
Profile: Default


Capturing from eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1769 140.982472796 10.0.1.10 10.0.1.20 TCP 74 80 → 52488 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=394613831 TSecr=394592939 WS=128
1770 140.990263484 10.0.1.10 10.0.1.20 TCP 74 [TCP Retransmission] 80 → 52488 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=394613831 TSecr=394592939 WS=128
1771 140.990508508 10.0.1.20 10.0.1.10 TCP 66 52488 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=394592943 TSecr=394613831
1772 140.990622239 10.0.1.20 10.0.1.10 HTTP 190 GET /messages HTTP/1.1
1773 140.998233024 10.0.1.10 10.0.1.20 TCP 66 52488 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=394592943 TSecr=394613831
1774 140.998329095 10.0.1.20 10.0.1.10 TCP 190 [TCP Retransmission] 52488 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=124 TSval=394592943 TSecr=394613831
1775 140.998486663 10.0.1.10 10.0.1.20 TCP 66 80 → 52488 [ACK] Seq=1 Ack=125 Win=29056 Len=0 TSval=394613835 TSecr=394592943
1776 140.999836436 10.0.1.10 10.0.1.20 TCP 83 80 → 52488 [PSH, ACK] Seq=1 Ack=125 Win=29056 Len=17 TSval=394613835 TSecr=394592943 [TCP segment of a reassembled PDU]
1777 141.000055581 10.0.1.10 10.0.1.20 HTTP 546 HTTP/1.0 200 OK (application/json)
1778 141.006274168 10.0.1.10 10.0.1.20 TCP 66 80 → 52488 [ACK] Seq=1 Ack=125 Win=29056 Len=0 TSval=394613835 TSecr=394592943
1779 141.006350389 10.0.1.10 10.0.1.20 TCP 83 [TCP Out-Of-Order] 80 → 52488 [PSH, ACK] Seq=1 Ack=125 Win=29056 Len=17 TSval=394613835 TSecr=394592943
1780 141.006422590 10.0.1.10 10.0.1.20 TCP 546 [TCP Out-Of-Order] 80 → 52488 [FIN, PSH, ACK] Seq=18 Ack=125 Win=29056 Len=480 TSval=394613835 TSecr=394592943[Reassembly error, protocol TCP: New fragment overlaps old data (retransmi…
1781 141.006510916 10.0.1.20 10.0.1.10 TCP 66 52488 → 80 [ACK] Seq=125 Ack=18 Win=29312 Len=0 TSval=394592947 TSecr=394613835
1782 141.006928549 10.0.1.20 10.0.1.10 TCP 66 52488 → 80 [FIN, ACK] Seq=125 Ack=499 Win=30336 Len=0 TSval=394592947 TSecr=394613835
1783 141.014361059 10.0.1.10 10.0.1.20 TCP 66 [TCP Keep-Alive] 52488 → 80 [ACK] Seq=125 Ack=18 Win=29312 Len=0 TSval=394592947 TSecr=394613835
1784 141.014430529 10.0.1.20 10.0.1.10 TCP 66 [TCP Out-Of-Order] 52488 → 80 [FIN, ACK] Seq=125 Ack=499 Win=30336 Len=0 TSval=394592947 TSecr=394613835
1785 141.014606715 10.0.1.10 10.0.1.20 TCP 66 80 → 52488 [ACK] Seq=499 Ack=126 Win=29056 Len=0 TSval=394613839 TSecr=394592947
1786 141.022398271 10.0.1.10 10.0.1.20 TCP 66 [TCP Dup ACK 1785#1] 80 → 52488 [ACK] Seq=499 Ack=126 Win=29056 Len=0 TSval=394613839 TSecr=394592947
1787 141.181041729 0.0.0.0 255.255.255.255 DHCP 329 DHCP Discover - Transaction ID 0xe793a338
1788 142.685200162 fe80::3189:1651:c99… ff02::fb MDNS 105 Standard query 0x0000 A MayomideMacBook-Pro.local, "QM" question
1789 142.685233252 10.0.1.104 224.0.0.251 MDNS 85 Standard query 0x0000 A MayomideMacBook-Pro.local, "QM" question
1790 142.995199627 Alcatel-_d2:36:12 Spanning-tree-(for-… STP 60 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
[iRTT: 0.008253590 seconds]
[Bytes in flight: 124]
[Bytes sent since last PSH flag: 124]
[Timestamps]
[Time since first frame in this TCP stream: 0.014519705 seconds]
[Time since previous frame in this TCP stream: 0.000087278 seconds]
TCP payload (124 bytes)
Hypertext Transfer Protocol
GET /messages HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /messages HTTP/1.1\r\n]
[GET /messages HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /messages
Request Version: HTTP/1.1
Host: 10.0.1.10\r\n
Authorization: Basic YWRtaW46bDRzVF9MNGI=\r\n
Credentials: admin:l4sT_L4b
User-Agent: curl/7.47.0\r\n
Accept: */*\r\n
\r\n
[Full request URI: http://10.0.1.10/messages]
[HTTP request 1/1]
0000 64 51 06 5a 3f 9c 40 a8 f0 21 2e 3c 08 00 45 00 dQ·Z?·@· ·!.<··E·
0010 00 b0 42 19 40 00 40 06 e2 11 0a 00 01 14 0a 00 ··B·@·@· ········
0020 01 0a cc bc 00 50 7e a3 f4 f8 dd 42 e3 db 80 18 ·····P~· ···B····
0030 00 e5 8e 84 00 00 01 01 08 0a 17 84 b6 e4 17 85 ···· ···· ········
0040 08 7c 47 45 54 20 2f 6d 65 73 73 61 67 65 73 20 ·|GET /m essages
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
0060 31 30 2e 30 2e 31 2e 31 30 0d 0a 41 75 74 68 6f 10.0.1.1 0··Autho
0070 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 rization : Basic
0080 59 57 52 74 61 57 34 36 62 44 52 7a 56 46 39 4d YWRtaW46 bDRzVF9M
0090 4e 47 49 3d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 NGI=··Us er-Agent
00a0 3a 20 63 75 72 6c 2f 37 2e 34 37 2e 30 0d 0a 41 : curl/7 .47.0··A
00b0 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a ccept: * /*····
Credentials (http.authbasic)
Packets: 1790 · Displayed: 1790 (100.0%)
Profile: Default


Objective
Implementing a simple HTTP-based messaging service
Basic system overview
ARP Spoofing
ARP Spoofing with Ettercap
TLS and HTTPS
Hand-in
attack will work!
4 TLS and HTTPS
• Follow the following guide to creat
services/ssh_test_certificate.h
– Note: The arguments in the t
create real certificates like this
ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
10.0.1.1 64:51:06:5A:1F:C4
10.0.1.10 40:A8:F0:24:D2:2C
10.0.1.20 40:A8:F0:21:2E:3C
10.0.1.30 40:A8:F0:24:7F:4C
10.0.1.104 64:51:06:50:22:E8
10.0.1.114 64:51:06:5A:FC:2C
10.0.1.137 64:51:06:5A:DB:54
10.0.1.143 64:51:06:5A:FB:C6
10.0.1.148 64:51:06:5A:DB:53
10.0.1.167 64:51:06:5A:1F:BF
Delete Host Add to Target 1 Add to Target 2
HTTP : 10.0.1.10:80 -> USER: admin PASS: l4sT_L4b INFO: 10.0.1.10/messages
HTTP : 10.0.1.10:80 -> USER: admin PASS: l4sT_L4b INFO: 10.0.1.10/messages
HTTP : 10.0.1.10:80 -> USER: admin PASS: l4sT_L4b INFO: 10.0.1.10/messages
HTTP : 10.0.1.10:80 -> USER: admin PASS: l4sT_L4b INFO: 10.0.1.10/messages
HTTP : 10.0.1.10:80 -> USER: admin PASS: l4sT_L4b INFO: 10.0.1.10/messages
ARP poisoner deactivated.
RE-ARPing the victims...
• We are now going to secure the se
(hints: examples in the following link
you-add-https-functionality-to-a-pyth
– In particular: we wrap the HTT
• In your server, add the SSL context
– Use the self-signed certificate you just created
• In your HTTP client, change the server URL to reflect the use of HTTPS
– You will most likely get an SSL error when connecting to your server. Why is that? See if it is possible to do certificate pinning in requests. Do not disable verification of certificates. (The implementation of certificate pinning is optional, will not be graded.)
• Try to capture the data transferred using Wireshark. Can you still see the passwords or messages?
5 Hand-in
• Submit your server and client code, and your server certificate and the private key
• Also submit a very short report file with
– The details learned by eavesdropping on the connection between 10.0.1.20 and 10.0.1.10


Terminal - samson@desktop: ~/Security-Labs/Lab 7
File Edit View Terminal Tabs Help
samson@desktop:~/Security-Labs/Lab 7$ sudo python3 studentserver.py
[sudo] password for samson:
* Running on https://127.0.0.1:5000/ (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 118-987-175
127.0.0.1 - - [29/Apr/2019 19:13:21] "POST /messages HTTP/1.1" 200 -
127.0.0.1 - - [29/Apr/2019 19:13:21] "GET /messages HTTP/1.1" 200 -
samson@desktop:~/Security-Labs/Lab 7$ sudo python3 studentclient.py
[sudo] password for samson:
Posting content
/usr/lib/python3/dist-packages/urllib3/connection.py:344: SubjectAltNameWarning: Certificate for 127.0.0.1 has no `subjectAltName`, falling back to check for a `commonName` for now. This feature is being removed by major browsers and deprecated by RFC 2818. (See https://github.com/shazow/urllib3/issues/497 for details.)
SubjectAltNameWarning
{"message": "Hello World"}
Getting content
/usr/lib/python3/dist-packages/urllib3/connection.py:344: SubjectAltNameWarning: Certificate for 127.0.0.1 has no `subjectAltName`, falling back to check for a `commonName` for now. This feature is being removed by major browsers and deprecated by RFC 2818. (See https://github.com/shazow/urllib3/issues/497 for details.)
SubjectAltNameWarning
"{\"message\": \"Hello World\"}"
samson@desktop:~/Security-Labs/Lab 7$
[0] 0:sudo*
"desktop" 19:13 29-Apr-19


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!icmp && !dns
No. Time Source Destination Protocol Length Info
4228… 6.377857067 127.0.0.1 127.0.0.1 TCP 76 5000 → 47452 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=1120389287 TSecr=1120389287 WS=128
4228… 6.377865232 127.0.0.1 127.0.0.1 TCP 68 47452 → 5000 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=1120389287 TSecr=1120389287
4229… 6.378374037 127.0.0.1 127.0.0.1 RSL 280 unknown 79
4229… 6.378379821 127.0.0.1 127.0.0.1 TCP 68 5000 → 47452 [ACK] Seq=1 Ack=213 Win=44800 Len=0 TSval=1120389288 TSecr=1120389288
4229… 6.379054151 127.0.0.1 127.0.0.1 RSL 1313 Location Information
4229… 6.379057769 127.0.0.1 127.0.0.1 TCP 68 47452 → 5000 [ACK] Seq=213 Ack=1246 Win=174720 Len=0 TSval=1120389289 TSecr=1120389289
4229… 6.379357661 127.0.0.1 127.0.0.1 RSL 161 DEACTIVATE SACCH
4229… 6.379552755 127.0.0.1 127.0.0.1 RSL 294 MODE MODIFY ACKnowledge
4229… 6.379849408 127.0.0.1 127.0.0.1 RSL 297 ip.access MEASurement PREPROCessing DeFauLT
4230… 6.380487670 127.0.0.1 127.0.0.1 RSL 114 MODE MODIFY REQuest
4230… 6.380916984 127.0.0.1 127.0.0.1 RSL 287 RF ResOurce INDication
4230… 6.380947871 127.0.0.1 127.0.0.1 TCP 68 47452 → 5000 [ACK] Seq=535 Ack=1738 Win=179712 Len=0 TSval=1120389290 TSecr=1120389290
4230… 6.380980452 127.0.0.1 127.0.0.1 TCP 68 47452 → 5000 [FIN, ACK] Seq=535 Ack=1738 Win=179712 Len=0 TSval=1120389290 TSecr=1120389290
4230… 6.380984265 127.0.0.1 127.0.0.1 TCP 68 5000 → 47452 [ACK] Seq=1738 Ack=536 Win=45952 Len=0 TSval=1120389290 TSecr=1120389290
4264… 6.430762209 fe80::501d:11fe:415… ff02::fb MDNS 90 Standard query 0x0000 A cj.local, "QM" question
4264… 6.430843531 10.42.0.1 224.0.0.251 MDNS 70 Standard query 0x0000 A cj.local, "QM" question
4465… 6.711667495 0.0.0.0 255.255.255.255 DHCP 331 DHCP Discover - Transaction ID 0xe793a338
4615… 6.931356668 fe80::555:a121:c9bb… ff02::1:2 DHCPv6 152 Solicit XID: 0xdc88f9 CID: 0001000123c86fb86451065adab1
5188… 7.827804507 Alcatel-_d2:36:12 STP 62 RST. Root = 32768/0/e8:e7:32:d2:36:10 Cost = 0 Port = 0x7400
5581… 8.430771996 fe80::501d:11fe:415… ff02::fb MDNS 90 Standard query 0x0000 A cj.local, "QM" question
5581… 8.430778873 10.42.0.1 224.0.0.251 MDNS 70 Standard query 0x0000 A cj.local, "QM" question
5918… 8.943586785 fe80::555:a121:c9bb… ff02::1:2 DHCPv6 152 Solicit XID: 0xdc88f9 CID: 0001000123cb86fb86451065adab1
Frame 422944: 1313 bytes on wire (10504 bits), 1313 bytes captured (10504 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 5000, Dst Port: 47452, Seq: 1, Ack: 213, Len: 1245
IPA protocol ip.access, type: unknown 0x03
Radio Signalling Link (RSL)
Bytes 71-1312: Radio Signalling Link (RSL) (gsm_abis_rsl)
Packets: 644068 · Displayed: 55 (0.0%) · Dropped: 0 (0.0%)
Profile: Default