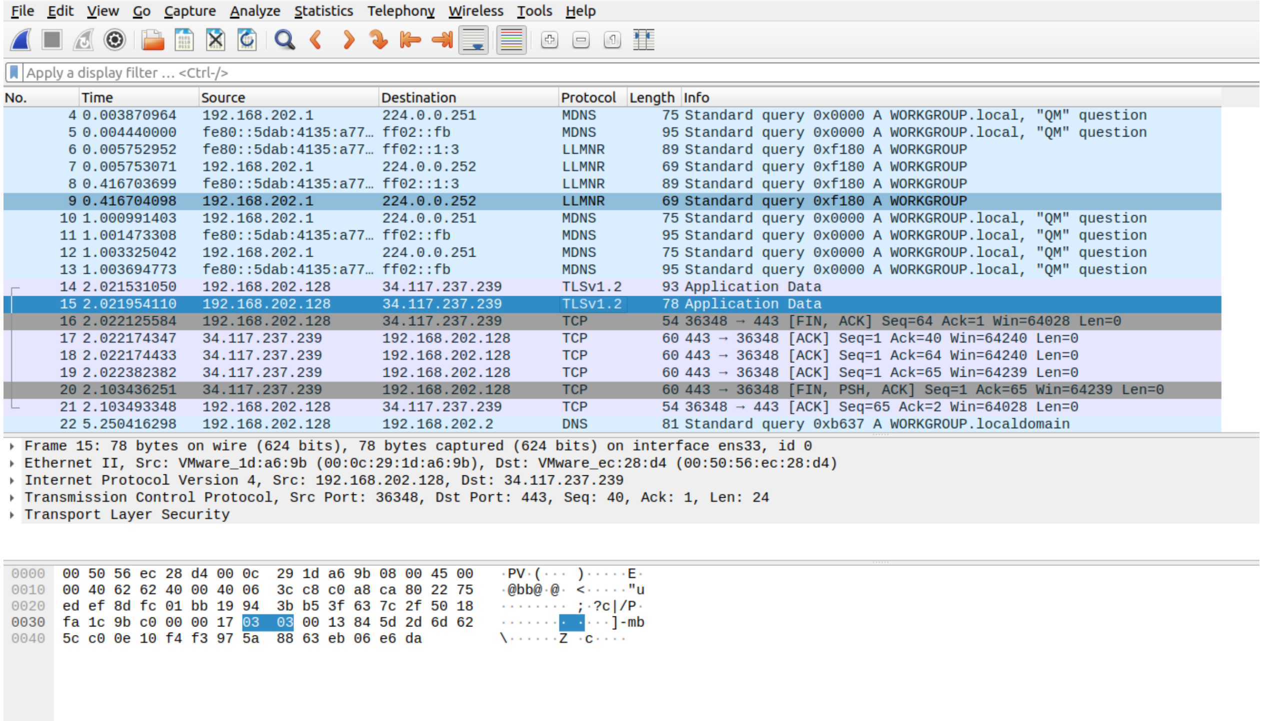
رامتین احسانی - ۹۷۵۲۱۰۱۸ - سوال ۵

- همانطور که در عکس زیر مشخص است application data داده ها encrypt شده و نامفهوم هستند.

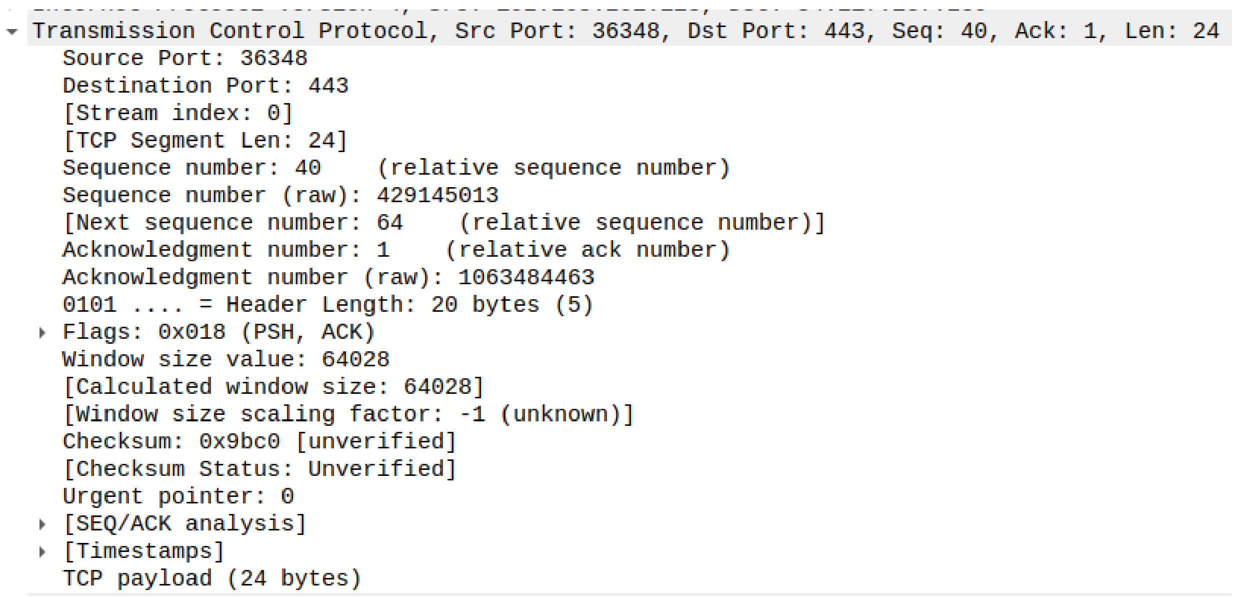


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

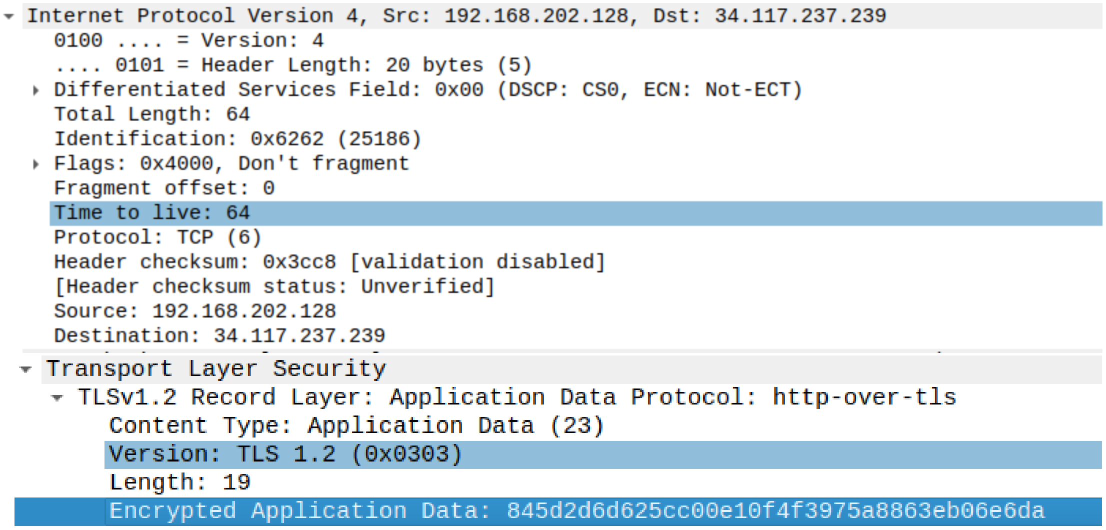
```
No.   Time          Source                   Destination      Protocol  Length Info
    4 0.003870964   192.168.202.1            224.0.0.251      MDNS        75 Standard query 0x0000 A WORKGROUP.local, "QM" question
    5 0.004440000   fe80::5dab:4135:a77…     ff02::fb         MDNS        95 Standard query 0x0000 A WORKGROUP.local, "QM" question
    6 0.005752952   fe80::5dab:4135:a77…     ff02::1:3        LLMNR       89 Standard query 0xf180 A WORKGROUP
    7 0.005753071   192.168.202.1            224.0.0.252      LLMNR       69 Standard query 0xf180 A WORKGROUP
    8 0.416703699   fe80::5dab:4135:a77…     ff02::1:3        LLMNR       89 Standard query 0xf180 A WORKGROUP
    9 0.416704098   192.168.202.1            224.0.0.252      LLMNR       69 Standard query 0xf180 A WORKGROUP
   10 1.000991403   192.168.202.1            224.0.0.251      MDNS        75 Standard query 0x0000 A WORKGROUP.local, "QM" question
   11 1.001473308   fe80::5dab:4135:a77…     ff02::fb         MDNS        95 Standard query 0x0000 A WORKGROUP.local, "QM" question
   12 1.003325042   192.168.202.1            224.0.0.251      MDNS        75 Standard query 0x0000 A WORKGROUP.local, "QM" question
   13 1.003694773   fe80::5dab:4135:a77…     ff02::fb         MDNS        95 Standard query 0x0000 A WORKGROUP.local, "QM" question
   14 2.021531050   192.168.202.128          34.117.237.239   TLSv1.2     93 Application Data
   15 2.021954110   192.168.202.128          34.117.237.239   TLSv1.2     78 Application Data
   16 2.022125584   192.168.202.128          34.117.237.239   TCP         54 36348 → 443 [FIN, ACK] Seq=64 Ack=1 Win=64028 Len=0
   17 2.022174347   34.117.237.239           192.168.202.128  TCP         60 443 → 36348 [ACK] Seq=1 Ack=40 Win=64240 Len=0
   18 2.022174433   34.117.237.239           192.168.202.128  TCP         60 443 → 36348 [ACK] Seq=1 Ack=64 Win=64240 Len=0
   19 2.022382382   34.117.237.239           192.168.202.128  TCP         60 443 → 36348 [ACK] Seq=1 Ack=65 Win=64239 Len=0
   20 2.103436251   34.117.237.239           192.168.202.128  TCP         60 443 → 36348 [FIN, PSH, ACK] Seq=1 Ack=65 Win=64239 Len=0
   21 2.103493348   192.168.202.128          34.117.237.239   TCP         54 36348 → 443 [ACK] Seq=65 Ack=2 Win=64028 Len=0
   22 5.250416298   192.168.202.128          192.168.202.2    DNS         81 Standard query 0xb637 A WORKGROUP.localdomain
```

```
▸ Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_1d:a6:9b (00:0c:29:1d:a6:9b), Dst: VMware_ec:28:d4 (00:50:56:ec:28:d4)
▸ Internet Protocol Version 4, Src: 192.168.202.128, Dst: 34.117.237.239
▸ Transmission Control Protocol, Src Port: 36348, Dst Port: 443, Seq: 40, Ack: 1, Len: 24
▸ Transport Layer Security
```

```
0000  00 50 56 ec 28 d4 00 0c  29 1d a6 9b 08 00 45 00   ·PV·(···)·····E·
0010  00 40 62 62 40 00 40 06  3c c8 c0 a8 ca 80 22 75   ·@bb@·@·<·····"u
0020  ed ef 8d fc 01 bb 19 94  3b b5 3f 63 7c 2f 50 18   ········;·?c|/P·
0030  fa 1c 9b c0 00 00 17 03  03 00 13 84 5d 2d 6d 62   ··········]-mb
0040  5c c0 0e 10 f4 f3 97 5a  88 63 eb 06 e6 da         \······Z·c····
```



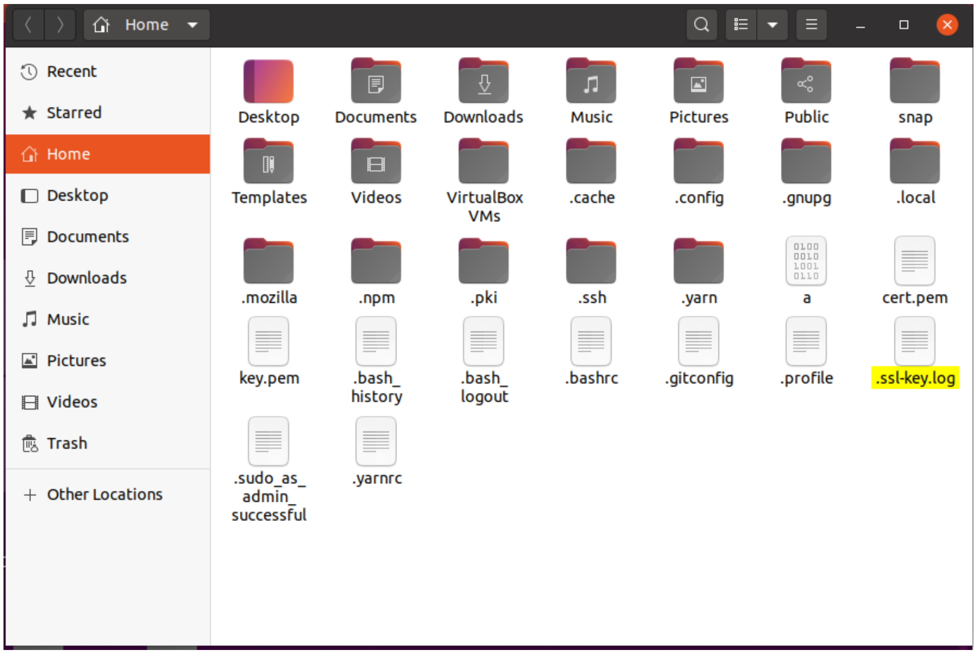
```
▾ Transmission Control Protocol, Src Port: 36348, Dst Port: 443, Seq: 40, Ack: 1, Len: 24
    Source Port: 36348
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 24]
    Sequence number: 40    (relative sequence number)
    Sequence number (raw): 429145013
    [Next sequence number: 64    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1063484463
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 64028
    [Calculated window size: 64028]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x9bc0 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (24 bytes)
```



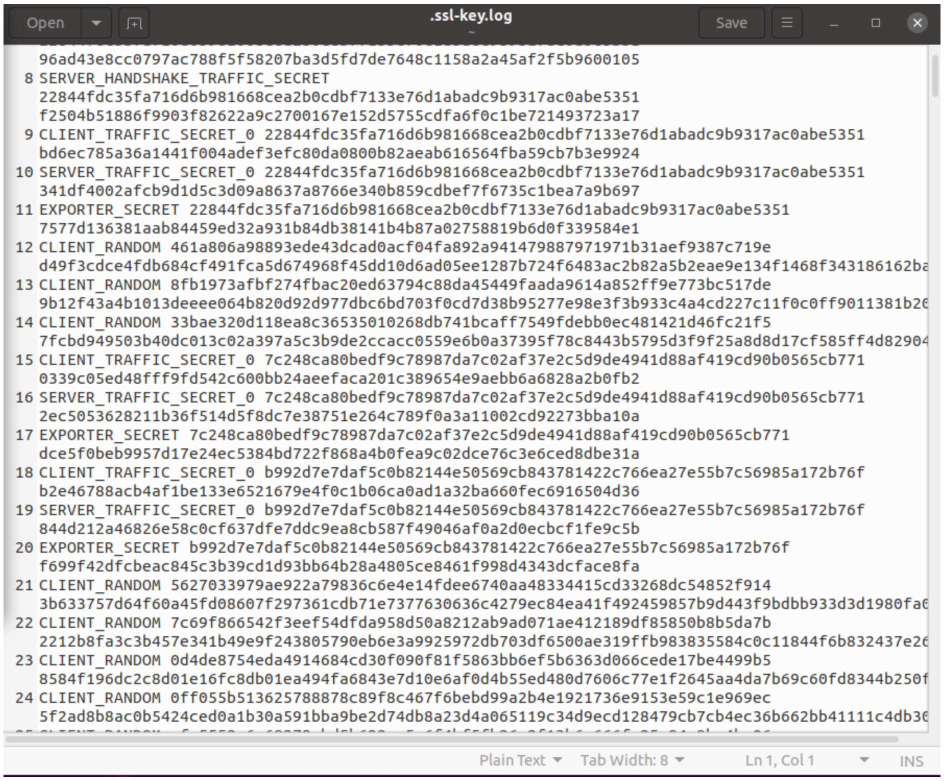
```
▾ Internet Protocol Version 4, Src: 192.168.202.128, Dst: 34.117.237.239
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 64
    Identification: 0x6262 (25186)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x3cc8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.202.128
    Destination: 34.117.237.239
 ▾ Transport Layer Security
   ▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
       Content Type: Application Data (23)
       Version: TLS 1.2 (0x0303)
       Length: 19
       Encrypted Application Data: 845d2d6d625cc00e10f4f3975a8863eb06e6da
```

- ابتدا با دستور زیر در ترمینال، SSL key log را به env اضافه کردم:

- nano ~/.bash_profile
- export SSLKEYLOGFILE=~/.ssl-key.log



بعد از ساختن این فایل، باید با مرورگر سایت های دارای SSL را باز کنیم تا فایل ssl-key.log پر شود.

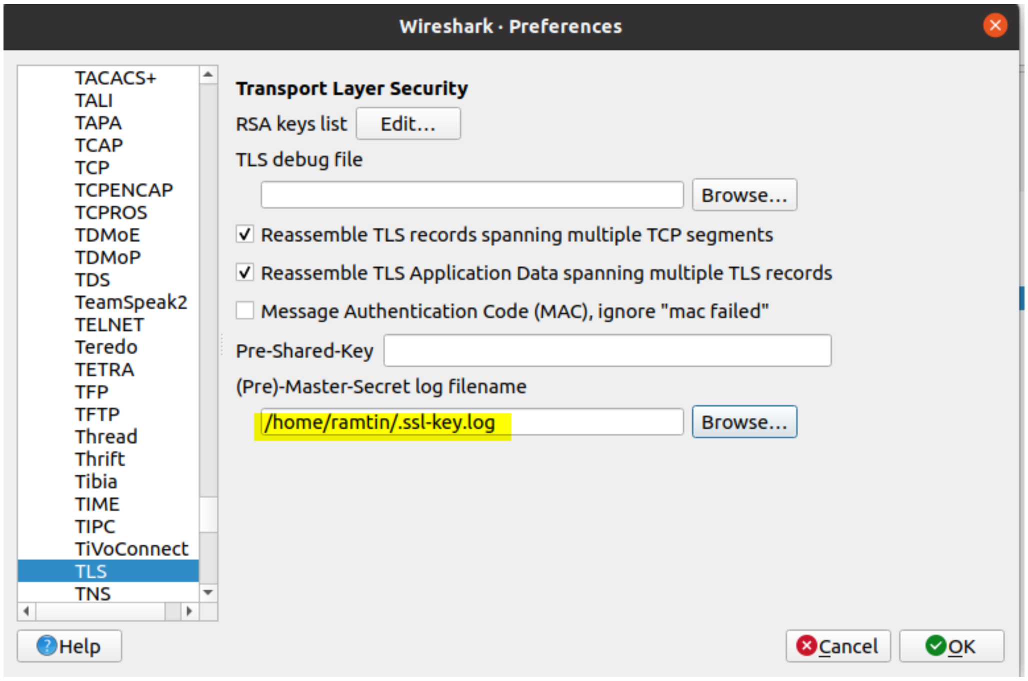


```
96ad43e8cc0797ac788f5f58207ba3d5fd7de7648c1158a2a45af2f5b9600105
SERVER_HANDSHAKE_TRAFFIC_SECRET
22844fdc35fa716d6b981668cea2b0cdbf7133e76d1abadc9b9317ac0abe5351
f2504b51886f9903f82622a9c2700167e152d5755cdfa6f0c1be721493723a17
CLIENT_TRAFFIC_SECRET_0 22844fdc35fa716d6b981668cea2b0cdbf7133e76d1abadc9b9317ac0abe5351
bd6ec785a36a1441f004adef3efc80da0800b82aeab616564fba59cb7b3e9924
SERVER_TRAFFIC_SECRET_0 22844fdc35fa716d6b981668cea2b0cdbf7133e76d1abadc9b9317ac0abe5351
341df4002afcb9d1d5c3d09a8637a8766e340b859cdbef7f6735c1bea7a9b697
EXPORTER_SECRET 22844fdc35fa716d6b981668cea2b0cdbf7133e76d1abadc9b9317ac0abe5351
7577d136381aab84459ed32a931b84db38141b4b87a02758819b6d0f339584e1
CLIENT_RANDOM 461a806a98893ede43dcad0acf04fa892a941479887971971b31aef9387c719e
d49f3cdce4fdb684cf491fca5d674968f45dd10d6ad05ee1287b724f6483ac2b82a5b2eae9e134f1468f343186162ba
CLIENT_RANDOM 8fb1973afbf274fbac20ed63794c88da45449faada9614a852ff9e773bc517de
9b12f43a4b1013deeee064b820d92d977dbc6bd703f0cd7d38b95277e98e3f3b933c4a4cd227c11f0c0ff9011381b20
CLIENT_RANDOM 33bae320d118ea8c36535010268db741bcaff7549fdebb0ec481421d46fc21f5
7fcbd949503b40dc013c02a397a5c3b9de2ccacc0559e6b0a37395f78c8443b5795d3f9f25a8d8d17cf585ff4d82904
CLIENT_TRAFFIC_SECRET_0 7c248ca80bedf9c78987da7c02af37e2c5d9de4941d88af419cd90b0565cb771
0339c05ed48fff9fd542c600bb24aeefaca201c389654e9aebb6a6828a2b0fb2
SERVER_TRAFFIC_SECRET_0 7c248ca80bedf9c78987da7c02af37e2c5d9de4941d88af419cd90b0565cb771
2ec5053628211b36f514d5f8dc7e38751e264c789f0a3a11002cd92273bba10a
EXPORTER_SECRET 7c248ca80bedf9c78987da7c02af37e2c5d9de4941d88af419cd90b0565cb771
dce5f0beb9957d17e24ec5384bd722f868a4b0fea9c02dce76c3e6ced8dbe31a
CLIENT_TRAFFIC_SECRET_0 b992d7e7daf5c0b82144e50569cb843781422c766ea27e55b7c56985a172b76f
b2e46788acb4af1be133e6521679e4f0c1b06ca0ad1a32ba660fec6916504d36
SERVER_TRAFFIC_SECRET_0 b992d7e7daf5c0b82144e50569cb843781422c766ea27e55b7c56985a172b76f
844d212a46826e58c0cf637dfe7ddc9ea8cb587f49046af0a2d0ecbcf1fe9c5b
EXPORTER_SECRET b992d7e7daf5c0b82144e50569cb843781422c766ea27e55b7c56985a172b76f
f699f42dfcbeac845c3b39cd1d93bb64b28a4805ce8461f998d4343dcface8fa
CLIENT_RANDOM 5627033979ae922a79836c6e4e14fdee6740aa48334415cd33268dc54852f914
3b633757d64f60a45fd08607f297361cdb71e7377630636c4279ec84ea41f492459857b9d443f9bdbb933d3d1980fa0
CLIENT_RANDOM 7c69f866542f3eef54dfda958d50a8212ab9ad071ae412189df85850b8b5da7b
2212b8fa3c3b457e341b49e9f243805790eb6e3a9925972db703df6500ae319ffb983835584c0c11844f6b832437e26
CLIENT_RANDOM 0d4de8754eda4914684cd30f090f81f5863bb6ef5b6363d066cede17be4499b5
8584f196dc2c8d01e16fc8db01ea494fa6843e7d10e6af0d4b55ed480d7606c77e1f2645aa4da7b69c60fd8344b250f
CLIENT_RANDOM 0ff055b513625788878c89f8c467f6bebd99a2b4e1921736e9153e59c1e969ec
5f2ad8b8ac0b5424ced0a1b30a591bba9be2d74db8a23d4a065119c34d9ecd128479cb7cb4ec36b662bb41111c4db30
```

سپس در wireshark در قسمت

- edit -> preferences -> protocols -> TLS -> (Pre) Master-log

فایل را وارد کردم.



Transport Layer Security

RSA keys list

TLS debug file

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

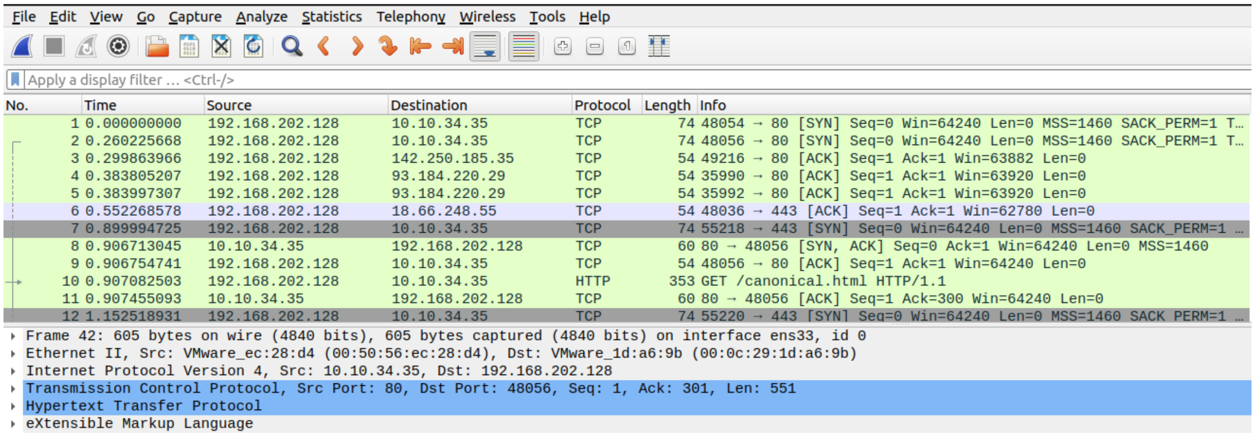
□ Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared-Key

(Pre)-Master-Secret log filename

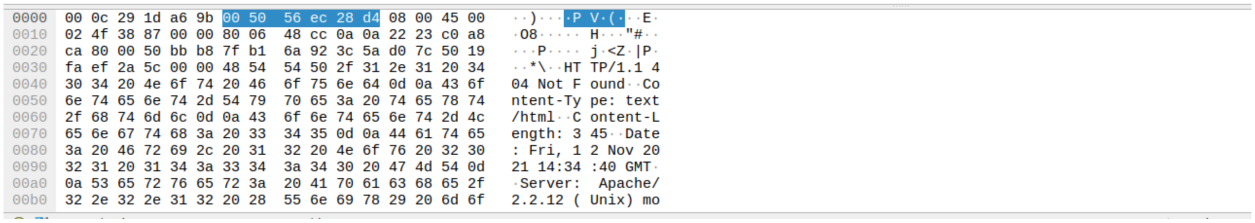
/home/ramtin/.ssl-key.log

بعد از ذخیره کردن فایل log در wireshark برای تنظیمات پروتکل TLS، یک سری از دیتا های HTTP GET نمایان میشوند که decrypt شده و قابل فهم هستند.

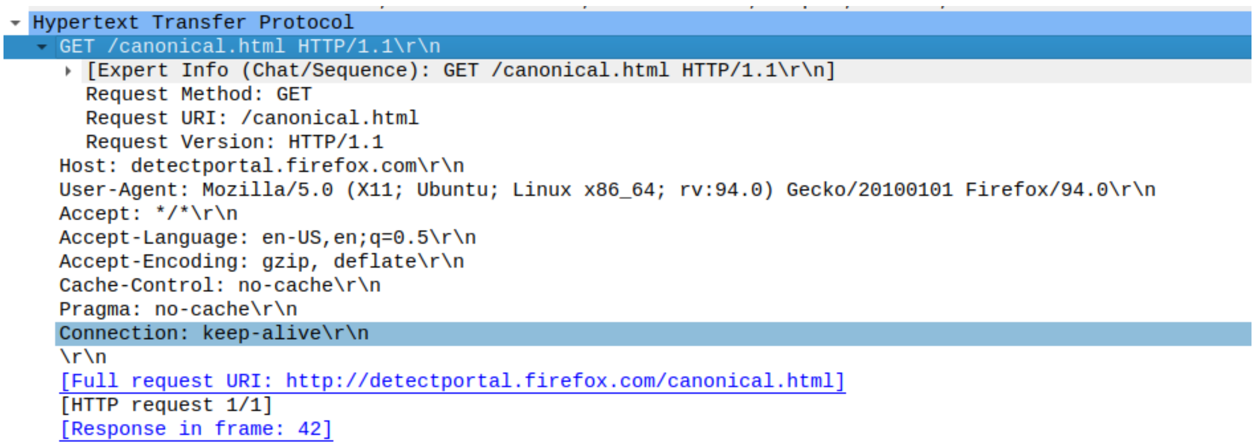

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time         Source           Destination      Protocol Length Info
    1 0.000000000  192.168.202.128  10.10.34.35      TCP        74 48054 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
    2 0.260225668  192.168.202.128  10.10.34.35      TCP        74 48056 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
    3 0.299863966  192.168.202.128  142.250.185.35   TCP        54 49216 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
    4 0.383805207  192.168.202.128  93.184.220.29    TCP        54 35990 → 80 [ACK] Seq=1 Ack=1 Win=63920 Len=0
    5 0.383997307  192.168.202.128  93.184.220.29    TCP        54 35992 → 80 [ACK] Seq=1 Ack=1 Win=63920 Len=0
    6 0.552268578  192.168.202.128  18.66.248.55     TCP        54 48036 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
    7 0.899994725  192.168.202.128  10.10.34.35      TCP        74 55218 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 …
    8 0.906713045  10.10.34.35      192.168.202.128  TCP        60 80 → 48056 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
    9 0.906754741  192.168.202.128  10.10.34.35      TCP        54 48056 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10 0.907082503  192.168.202.128  10.10.34.35      HTTP      353 GET /canonical.html HTTP/1.1
   11 0.907455093  10.10.34.35      192.168.202.128  TCP        60 80 → 48056 [ACK] Seq=1 Ack=300 Win=64240 Len=0
   12 1.152518931  192.168.202.128  10.10.34.35      TCP        74 55220 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 …
```

```
› Frame 42: 605 bytes on wire (4840 bits), 605 bytes captured (4840 bits) on interface ens33, id 0
› Ethernet II, Src: VMware_ec:28:d4 (00:50:56:ec:28:d4), Dst: VMware_1d:a6:9b (00:0c:29:1d:a6:9b)
› Internet Protocol Version 4, Src: 10.10.34.35, Dst: 192.168.202.128
› Transmission Control Protocol, Src Port: 80, Dst Port: 48056, Seq: 1, Ack: 301, Len: 551
› Hypertext Transfer Protocol
› eXtensible Markup Language
```



```
0000  00 0c 29 1d a6 9b 00 50  56 ec 28 d4 08 00 45 00   ··)···P V·(···E·
0010  02 4f 38 87 00 00 80 06  48 cc 0a 0a 22 23 c0 a8   ·O8····· H···"#··
0020  ca 80 00 50 bb b8 7f b1  6a 92 3c 5a d0 7c 50 19   ···P···· j·<Z·|P·
0030  fa ef 2a 5c 00 00 48 54  54 50 2f 31 2e 31 20 34   ··*\··HT TP/1.1 4
0040  30 34 20 4e 6f 74 20 46  6f 75 6e 64 0d 0a 43 6f   04 Not F ound··Co
0050  6e 74 65 6e 74 2d 54 79  70 65 3a 20 74 65 78 74   ntent-Ty pe: text
0060  2f 68 74 6d 6c 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   /html··C ontent-L
0070  65 6e 67 74 68 3a 20 33  34 35 0d 0a 44 61 74 65   ength: 3 45··Date
0080  3a 20 46 72 69 2c 20 31  32 20 4e 6f 76 20 32 30   : Fri, 1 2 Nov 20
0090  32 31 20 31 34 3a 33 34  3a 34 30 20 47 4d 54 0d   21 14:34 :40 GMT·
00a0  0a 53 65 72 76 65 72 3a  20 41 70 61 63 68 65 2f   ·Server:  Apache/
00b0  32 2e 32 2e 31 32 20 28  55 6e 69 78 29 20 6d 6f   2.2.12 ( Unix) mo
```



```
▾ Hypertext Transfer Protocol
  ▾ GET /canonical.html HTTP/1.1\r\n
    › [Expert Info (Chat/Sequence): GET /canonical.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /canonical.html
      Request Version: HTTP/1.1
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:94.0) Gecko/20100101 Firefox/94.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Cache-Control: no-cache\r\n
    Pragma: no-cache\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://detectportal.firefox.com/canonical.html]
    [HTTP request 1/1]
    [Response in frame: 42]
```

- بله بعد از Decrypt شدن قابل فهم است.