JARINGAN KOMPUTER

TASK 5

Nama : Rufiah

NIM : 09011181419019

Dosen : Deris Stiawan, M.T., PhD

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

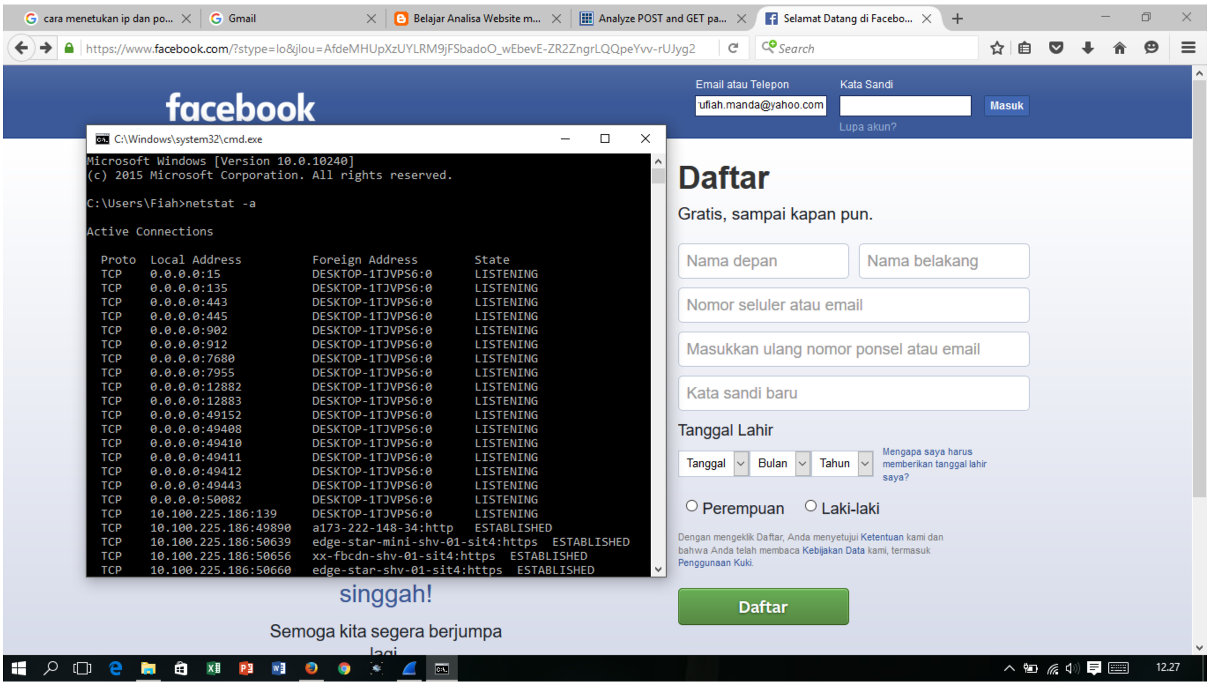
UNIVERSITAS SRIWIJAYA

2016

Ketika Url masuk ke https://www.facebook.com, ketika netstat di command prompt

dengan perintah netstat -a di command prompt

ini adalah tampilan pada command prompt nya



https://www.facebook.com/?stype=lo&jlou=AfdeMHUpXzUYLRM9jFSbadoO_wEbevE-ZR2ZngrLQQpeYvv-rUJyg2

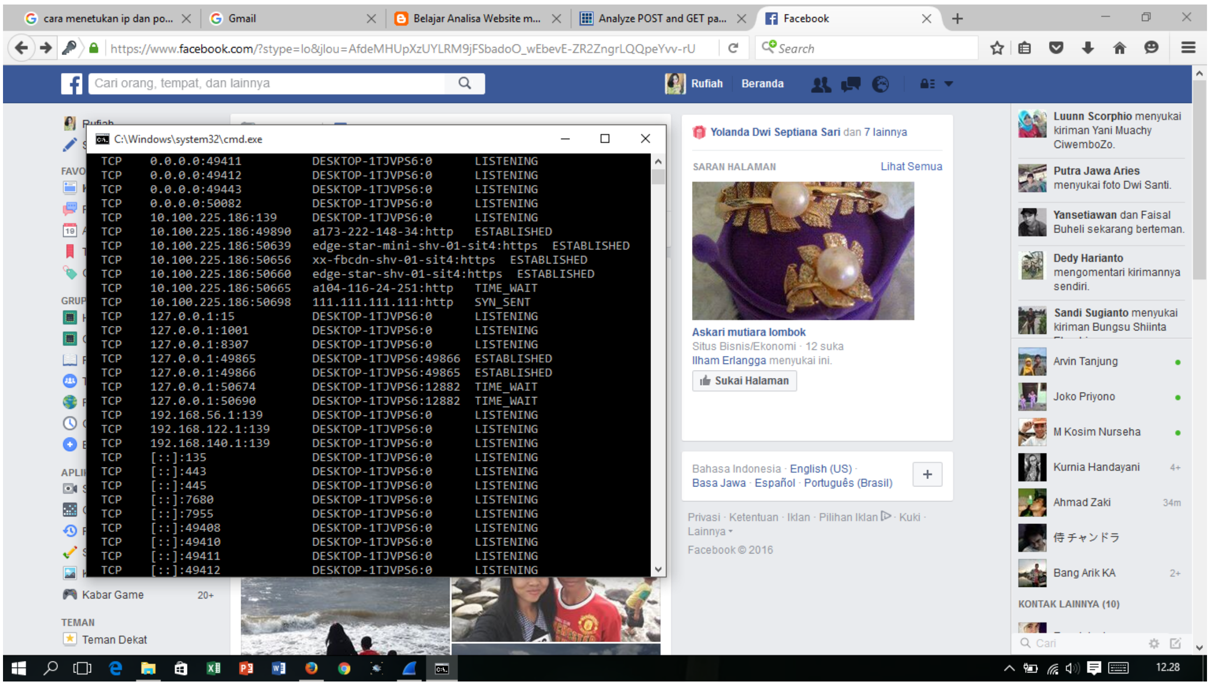
Email atau Telepon: ufiah.manda@yahoo.com

Kata Sandi:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Fiah>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:15             DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:135            DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:443            DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:902            DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:912            DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:7955           DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:12882          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:12883          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49152          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49408          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49410          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49411          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49412          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49443          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:50082          DESKTOP-1TJVPS6:0      LISTENING
  TCP    10.100.225.186:139     DESKTOP-1TJVPS6:0      LISTENING
  TCP    10.100.225.186:49890   a173-222-148-34:http   ESTABLISHED
  TCP    10.100.225.186:50639   edge-star-mini-shv-01-sit4:https  ESTABLISHED
  TCP    10.100.225.186:50656   xx-fbcdn-shv-01-sit4:https  ESTABLISHED
  TCP    10.100.225.186:50660   edge-star-shv-01-sit4:https  ESTABLISHED
```

cara menetukan ip dan po...
Gmail
Belajar Analisa Website m...
Analyze POST and GET pa...
Selamat Datang di Facebo...
Search
facebook
Masuk
Lupa akun?
Daftar
Gratis, sampai kapan pun.
Nama depan
Nama belakang
Nomor seluler atau email
Masukkan ulang nomor ponsel atau email
Kata sandi baru
Tanggal Lahir
Tanggal
Bulan
Tahun
Mengapa saya harus memberikan tanggal lahir saya?
○ Perempuan
○ Laki-laki
Dengan mengeklik Daftar, Anda menyetujui Ketentuan kami dan bahwa Anda telah membaca Kebijakan Data kami, termasuk Penggunaan Kuki.
Daftar
singgah!
Semoga kita segera berjumpa lagi
12.27

Dapat diamati ketika masuk ke facebook.com password yang diketikkan akan dienkripsi. Hal tersebut terekam di port dengan keterangan https. Berarti website ini dilindungi dan menjamin keamanan sistemnya.

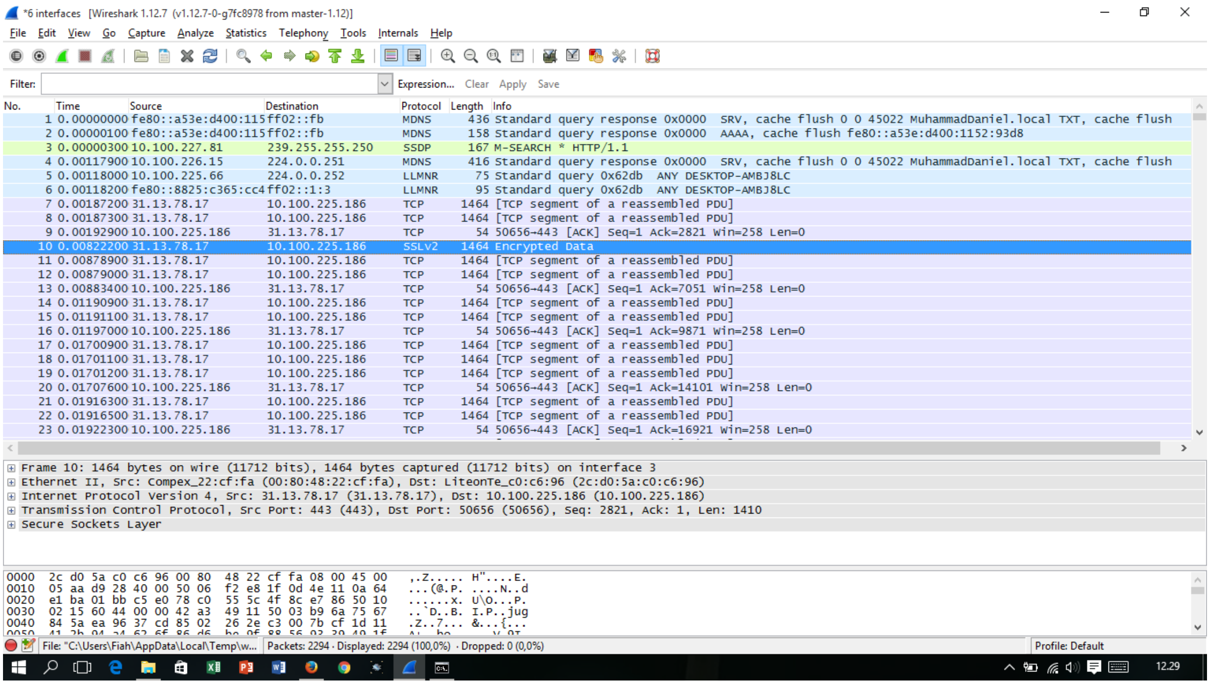


cara menetukan ip dan po...
Gmail
Belajar Analisa Website m...
Analyze POST and GET pa...
Facebook
https://www.facebook.com/?stype=lo&jlou=AfdeMHUpXzUYLRM9jFSbadoO_wEbevE-ZR2ZngrLQQpeYvv-rU
Search
Cari orang, tempat, dan lainnya
Rufiah
Beranda
C:\Windows\system32\cmd.exe
Yolanda Dwi Septiana Sari dan 7 lainnya
SARAN HALAMAN
Lihat Semua
Askari mutiara lombok
Situs Bisnis/Ekonomi · 12 suka
Ilham Erlangga menyukai ini.
Sukai Halaman
Bahasa Indonesia · English (US) · Basa Jawa · Español · Português (Brasil)
Privasi · Ketentuan · Iklan · Pilihan Iklan · Kuki · Lainnya
Facebook © 2016
Kabar Game 20+
TEMAN
Teman Dekat
Luunn Scorphio menyukai kiriman Yani Muachy CiwemboZo.
Putra Jawa Aries menyukai foto Dwi Santi.
Yansetiawan dan Faisal Buheli sekarang berteman.
Dedy Harianto mengomentari kirimannya sendiri.
Sandi Sugianto menyukai kiriman Bungsu Shiinta
Arvin Tanjung
Joko Priyono
M Kosim Nurseha
Kurnia Handayani 4+
Ahmad Zaki 34m
侍 チャンドラ
Bang Arik KA 2+
KONTAK LAINNYA (10)
Cari
12.28

```
  TCP    0.0.0.0:49411          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49412          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:49443          DESKTOP-1TJVPS6:0      LISTENING
  TCP    0.0.0.0:50082          DESKTOP-1TJVPS6:0      LISTENING
  TCP    10.100.225.186:139     DESKTOP-1TJVPS6:0      LISTENING
  TCP    10.100.225.186:49890   a173-222-148-34:http   ESTABLISHED
  TCP    10.100.225.186:50639   edge-star-mini-shv-01-sit4:https  ESTABLISHED
  TCP    10.100.225.186:50656   xx-fbcdn-shv-01-sit4:https  ESTABLISHED
  TCP    10.100.225.186:50660   edge-star-shv-01-sit4:https  ESTABLISHED
  TCP    10.100.225.186:50665   a104-116-24-251:http   TIME_WAIT
  TCP    10.100.225.186:50698   111.111.111.111:http   SYN_SENT
  TCP    127.0.0.1:15           DESKTOP-1TJVPS6:0      LISTENING
  TCP    127.0.0.1:1001         DESKTOP-1TJVPS6:0      LISTENING
  TCP    127.0.0.1:8307         DESKTOP-1TJVPS6:0      LISTENING
  TCP    127.0.0.1:49865        DESKTOP-1TJVPS6:49866  ESTABLISHED
  TCP    127.0.0.1:49866        DESKTOP-1TJVPS6:49865  ESTABLISHED
  TCP    127.0.0.1:50674        DESKTOP-1TJVPS6:12882  TIME_WAIT
  TCP    127.0.0.1:50690        DESKTOP-1TJVPS6:12882  TIME_WAIT
  TCP    192.168.56.1:139       DESKTOP-1TJVPS6:0      LISTENING
  TCP    192.168.122.1:139      DESKTOP-1TJVPS6:0      LISTENING
  TCP    192.168.140.1:139      DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:135               DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:443               DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:445               DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:7680              DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:7955              DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:49408             DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:49410             DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:49411             DESKTOP-1TJVPS6:0      LISTENING
  TCP    [::]:49412             DESKTOP-1TJVPS6:0      LISTENING
```

Percobaan menggunakan wireshark

Ke facebook.com



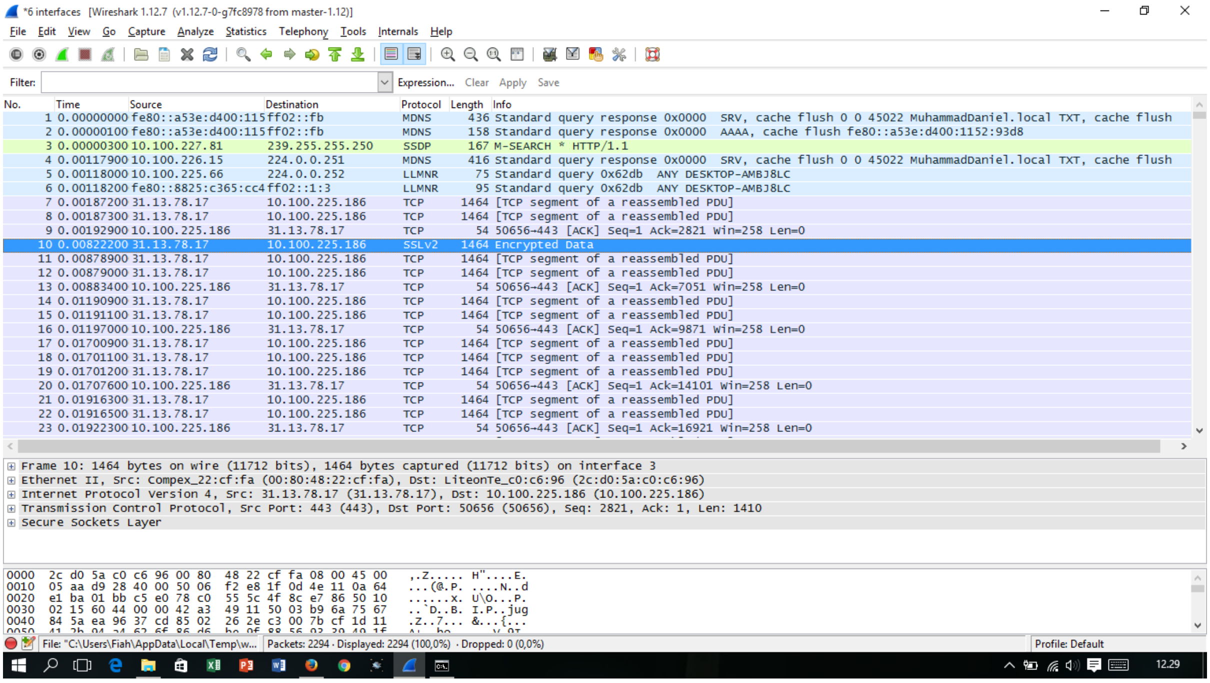
*6 interfaces [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default
12.29

```
No.  Time        Source               Destination      Protocol Length Info
   1 0.00000000 fe80::a53e:d400:115 ff02::fb          MDNS      436 Standard query response 0x0000  SRV, cache flush 0 0 45022 MuhammadDaniel.local TXT, cache flush
   2 0.00000100 fe80::a53e:d400:115 ff02::fb          MDNS      158 Standard query response 0x0000  AAAA, cache flush fe80::a53e:d400:1152:93d8
   3 0.00000300 10.100.227.81       239.255.255.250   SSDP      167 M-SEARCH * HTTP/1.1
   4 0.00117900 10.100.226.15       224.0.0.251       MDNS      416 Standard query response 0x0000  SRV, cache flush 0 0 45022 MuhammadDaniel.local TXT, cache flush
   5 0.00118000 10.100.225.66       224.0.0.252       LLMNR      75 Standard query 0x62db  ANY DESKTOP-AMBJ8LC
   6 0.00118200 fe80::8825:c365:cc4 ff02::1:3         LLMNR      95 Standard query 0x62db  ANY DESKTOP-AMBJ8LC
   7 0.00187200 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
   8 0.00187300 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
   9 0.00192900 10.100.225.186      31.13.78.17       TCP        54 50656→443 [ACK] Seq=1 Ack=2821 Win=258 Len=0
  10 0.00822200 31.13.78.17         10.100.225.186    SSLv2    1464 Encrypted Data
  11 0.00878900 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  12 0.00879000 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  13 0.00883400 10.100.225.186      31.13.78.17       TCP        54 50656→443 [ACK] Seq=1 Ack=7051 Win=258 Len=0
  14 0.01190900 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  15 0.01191100 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  16 0.01197000 10.100.225.186      31.13.78.17       TCP        54 50656→443 [ACK] Seq=1 Ack=9871 Win=258 Len=0
  17 0.01700900 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  18 0.01701100 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  19 0.01701200 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  20 0.01707600 10.100.225.186      31.13.78.17       TCP        54 50656→443 [ACK] Seq=1 Ack=14101 Win=258 Len=0
  21 0.01916300 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  22 0.01916500 31.13.78.17         10.100.225.186    TCP      1464 [TCP segment of a reassembled PDU]
  23 0.01922300 10.100.225.186      31.13.78.17       TCP        54 50656→443 [ACK] Seq=1 Ack=16921 Win=258 Len=0
```

```
⊞ Frame 10: 1464 bytes on wire (11712 bits), 1464 bytes captured (11712 bits) on interface 3
⊞ Ethernet II, Src: Compex_22:cf:fa (00:80:48:22:cf:fa), Dst: LiteonTe_c0:c6:96 (2c:d0:5a:c0:c6:96)
⊞ Internet Protocol Version 4, Src: 31.13.78.17 (31.13.78.17), Dst: 10.100.225.186 (10.100.225.186)
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 50656 (50656), Seq: 2821, Ack: 1, Len: 1410
⊞ Secure Sockets Layer
```

```
0000  2c d0 5a c0 c6 96 00 80  48 22 cf fa 08 00 45 00   ,.Z..... H"....E.
0010  05 aa d9 28 40 00 50 06  f2 e8 1f 0d 4e 11 0a 64   ...(@.P. ....N..d
0020  e1 ba 01 bb c5 e0 78 c0  55 5c 4f 8c e7 86 50 10   ......x. U\O...P.
0030  02 15 60 44 00 00 42 a3  49 11 50 03 b9 6a 75 67   ..`D..B. I.P..jug
0040  84 5a ea 96 37 cd 85 02  26 2e c3 00 7b cf 1d 11   .Z..7... &...{...
```

File: "C:\Users\Fiah\AppData\Local\Temp\w... Packets: 2294 · Displayed: 2294 (100,0%) · Dropped: 0 (0,0%)


*6 interfaces [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

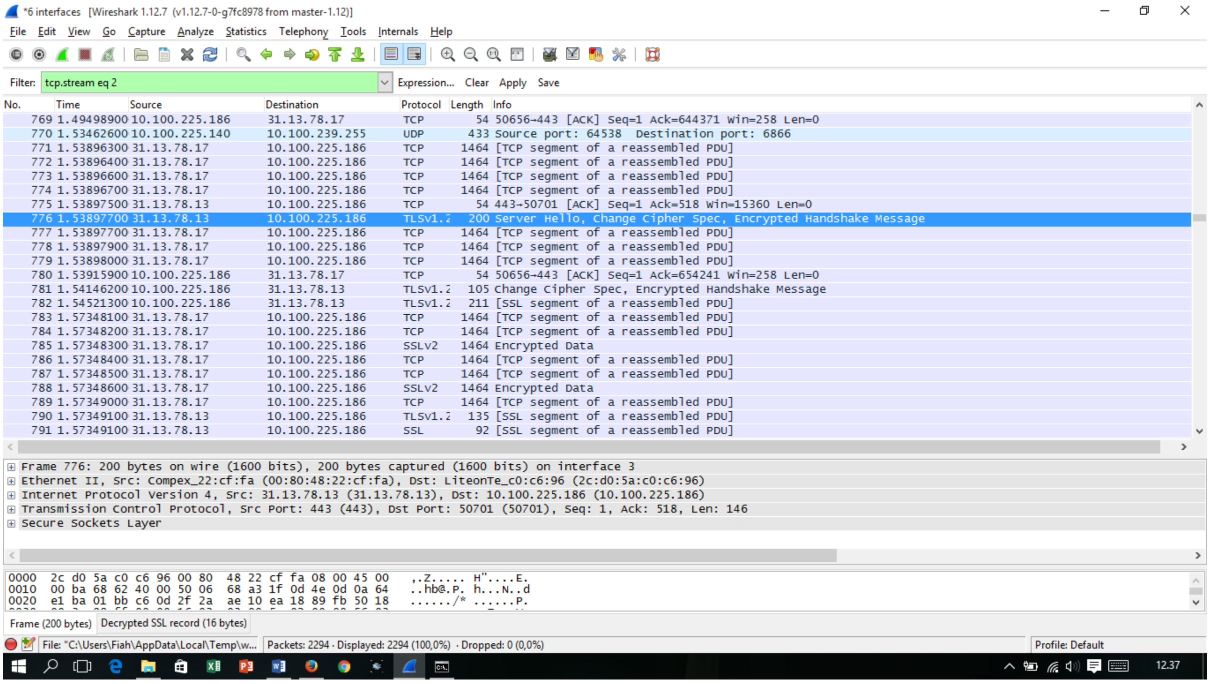
```
No.  Time       Source                Destination      Protocol Length Info
   1 0.00000000 fe80::a53e:d400:115ff02::fb           MDNS      436 Standard query response 0x0000  SRV, cache flush 0 0 45022 MuhammadDaniel.local TXT, cache flush
   2 0.00000100 fe80::a53e:d400:115ff02::fb           MDNS      158 Standard query response 0x0000  AAAA, cache flush fe80::a53e:d400:1152:93d8
   3 0.00000300 10.100.227.81         239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
   4 0.00117900 10.100.226.15         224.0.0.251      MDNS      416 Standard query response 0x0000  SRV, cache flush 0 0 45022 MuhammadDaniel.local TXT, cache flush
   5 0.00118000 10.100.225.66         224.0.0.252      LLMNR      75 Standard query 0x62db  ANY DESKTOP-AMBJ8LC
   6 0.00118200 fe80::8825:c365:cc4ff02::1:3          LLMNR      95 Standard query 0x62db  ANY DESKTOP-AMBJ8LC
   7 0.00187200 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
   8 0.00187300 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
   9 0.00192900 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=2821 Win=258 Len=0
  10 0.00822200 31.13.78.17           10.100.225.186   SSLv2    1464 Encrypted Data
  11 0.00878900 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  12 0.00879000 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  13 0.00883400 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=7051 Win=258 Len=0
  14 0.01190900 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  15 0.01191100 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  16 0.01197000 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=9871 Win=258 Len=0
  17 0.01700900 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  18 0.01701100 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  19 0.01701200 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  20 0.01707600 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=14101 Win=258 Len=0
  21 0.01916300 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  22 0.01916500 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
  23 0.01922300 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=16921 Win=258 Len=0
```

```
⊞ Frame 10: 1464 bytes on wire (11712 bits), 1464 bytes captured (11712 bits) on interface 3
⊞ Ethernet II, Src: Compex_22:cf:fa (00:80:48:22:cf:fa), Dst: LiteonTe_c0:c6:96 (2c:d0:5a:c0:c6:96)
⊞ Internet Protocol Version 4, Src: 31.13.78.17 (31.13.78.17), Dst: 10.100.225.186 (10.100.225.186)
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 50656 (50656), Seq: 2821, Ack: 1, Len: 1410
⊞ Secure Sockets Layer
```

```
0000  2c d0 5a c0 c6 96 00 80  48 22 cf fa 08 00 45 00   ,.Z..... H"....E.
0010  05 aa d9 28 40 00 50 06  f2 e8 1f 0d 4e 11 0a 64   ...(@.P. ....N..d
0020  e1 ba 01 bb c5 e0 78 c0  55 5c 4f 8c e7 86 50 10   ......x. U\O...P.
0030  02 15 60 44 00 00 42 a3  49 11 50 03 b9 6a 75 67   ..`D..B. I.P..jug
0040  84 5a ea 96 37 cd 85 02  26 2e c3 00 7b cf 1d 11   .Z..7... &...{...
```

File: "C:\Users\Fiah\AppData\Local\Temp\w... Packets: 2294 · Displayed: 2294 (100,0%) · Dropped: 0 (0,0%) Profile: Default

12.29


*6 interfaces [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: tcp.stream eq 2

```
No.  Time       Source                Destination      Protocol Length Info
 769 1.49498900 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=644371 Win=258 Len=0
 770 1.53462600 10.100.225.140        10.100.239.255   UDP       433 Source port: 64538  Destination port: 6866
 771 1.53896300 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 772 1.53896400 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 773 1.53896600 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 774 1.53896700 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 775 1.53897500 31.13.78.13           10.100.225.186   TCP        54 443→50701 [ACK] Seq=1 Ack=518 Win=15360 Len=0
 776 1.53897700 31.13.78.13           10.100.225.186   TLSv1.2   200 Server Hello, Change Cipher Spec, Encrypted Handshake Message
 777 1.53897700 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 778 1.53897900 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 779 1.53898000 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 780 1.53915900 10.100.225.186        31.13.78.17      TCP        54 50656→443 [ACK] Seq=1 Ack=654241 Win=258 Len=0
 781 1.54146200 10.100.225.186        31.13.78.13      TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
 782 1.54521300 10.100.225.186        31.13.78.13      TLSv1.2   211 [SSL segment of a reassembled PDU]
 783 1.57348100 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 784 1.57348200 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 785 1.57348300 31.13.78.17           10.100.225.186   SSLv2    1464 Encrypted Data
 786 1.57348400 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 787 1.57348500 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 788 1.57348600 31.13.78.17           10.100.225.186   SSLv2    1464 Encrypted Data
 789 1.57349000 31.13.78.17           10.100.225.186   TCP      1464 [TCP segment of a reassembled PDU]
 790 1.57349100 31.13.78.13           10.100.225.186   TLSv1.2   135 [SSL segment of a reassembled PDU]
 791 1.57349100 31.13.78.13           10.100.225.186   SSL        92 [SSL segment of a reassembled PDU]
```

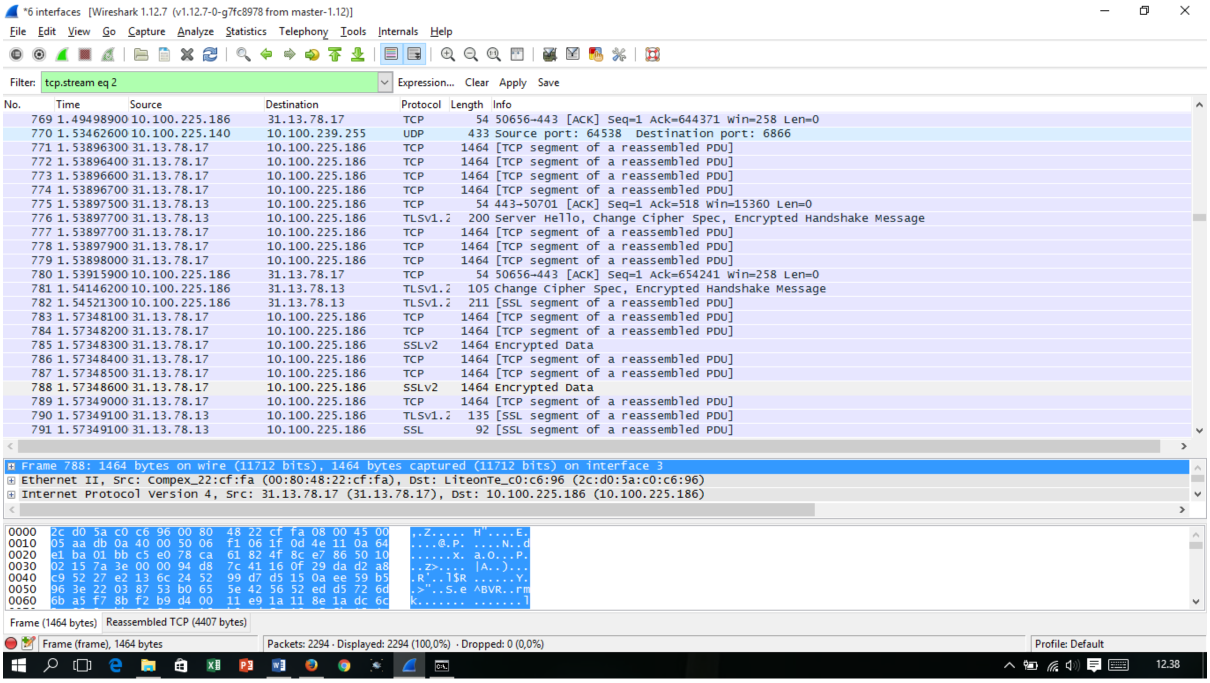
```
⊞ Frame 776: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface 3
⊞ Ethernet II, Src: Compex_22:cf:fa (00:80:48:22:cf:fa), Dst: LiteonTe_c0:c6:96 (2c:d0:5a:c0:c6:96)
⊞ Internet Protocol Version 4, Src: 31.13.78.13 (31.13.78.13), Dst: 10.100.225.186 (10.100.225.186)
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 50701 (50701), Seq: 1, Ack: 518, Len: 146
⊞ Secure Sockets Layer
```

```
0000  2c d0 5a c0 c6 96 00 80  48 22 cf fa 08 00 45 00   ,.Z..... H"....E.
0010  00 ba 68 62 40 00 50 06  68 a3 1f 0d 4e 0d 0a 64   ..hb@.P. h...N..d
0020  e1 ba 01 bb c6 0d 2f 2a  ae 10 ea 18 89 fb 50 18   ....../* ......P.
```

Frame (200 bytes) Decrypted SSL record (16 bytes)

File: "C:\Users\Fiah\AppData\Local\Temp\w... Packets: 2294 · Displayed: 2294 (100,0%) · Dropped: 0 (0,0%) Profile: Default

12.37



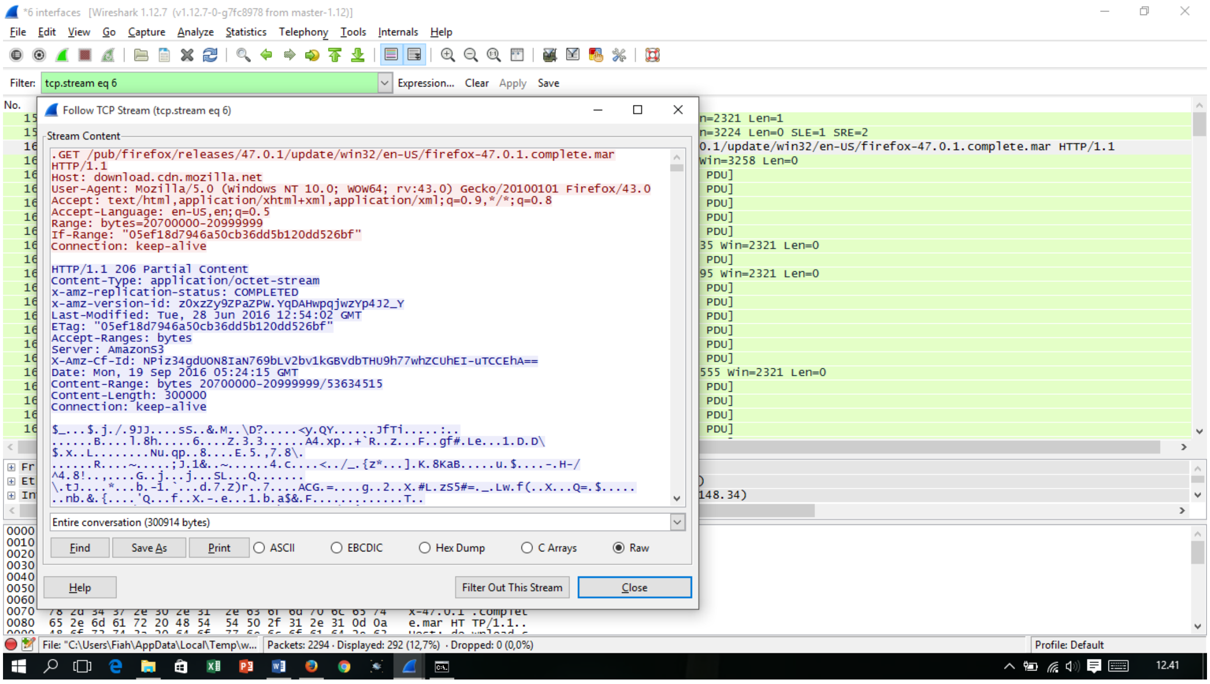
*6 interfaces [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp.stream eq 2

```
No.  Time       Source         Destination     Protocol Length Info
 769 1.49498900 10.100.225.186 31.13.78.17     TCP        54 50656→443 [ACK] Seq=1 Ack=644371 Win=258 Len=0
 770 1.53462600 10.100.225.140 10.100.239.255  UDP       433 Source port: 64538  Destination port: 6866
 771 1.53896300 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 772 1.53896400 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 773 1.53896600 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 774 1.53896700 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 775 1.53897500 31.13.78.13    10.100.225.186  TCP        54 443→50701 [ACK] Seq=1 Ack=518 Win=15360 Len=0
 776 1.53897700 31.13.78.13    10.100.225.186  TLSv1.2   200 Server Hello, Change Cipher Spec, Encrypted Handshake Message
 777 1.53897700 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 778 1.53897900 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 779 1.53898000 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 780 1.53915900 10.100.225.186 31.13.78.17     TCP        54 50656→443 [ACK] Seq=1 Ack=654241 Win=258 Len=0
 781 1.54146200 10.100.225.186 31.13.78.13     TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
 782 1.54521300 10.100.225.186 31.13.78.13     TLSv1.2   211 [SSL segment of a reassembled PDU]
 783 1.57348100 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 784 1.57348200 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 785 1.57348300 31.13.78.17    10.100.225.186  SSLv2    1464 Encrypted Data
 786 1.57348400 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 787 1.57348500 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 788 1.57348600 31.13.78.17    10.100.225.186  SSLv2    1464 Encrypted Data
 789 1.57349000 31.13.78.17    10.100.225.186  TCP      1464 [TCP segment of a reassembled PDU]
 790 1.57349100 31.13.78.13    10.100.225.186  TLSv1.2   135 [SSL segment of a reassembled PDU]
 791 1.57349100 31.13.78.13    10.100.225.186  SSL        92 [SSL segment of a reassembled PDU]

⊞ Frame 788: 1464 bytes on wire (11712 bits), 1464 bytes captured (11712 bits) on interface 3
⊞ Ethernet II, Src: Compex_22:cf:fa (00:80:48:22:cf:fa), Dst: LiteonTe_c0:c6:96 (2c:d0:5a:c0:c6:96)
⊞ Internet Protocol Version 4, Src: 31.13.78.17 (31.13.78.17), Dst: 10.100.225.186 (10.100.225.186)

0000  2c d0 5a c0 c6 96 00 80  48 22 cf fa 08 00 45 00   ,.Z..... H"....E.
0010  05 aa db 0a 40 00 50 06  f1 06 1f 0d 4e 11 0a 64   ....@.P. ....N..d
0020  e1 ba 01 bb c5 e0 78 ca  61 82 4f 8c e7 86 50 10   ......x. a.O...P.
0030  02 15 7a 3e 00 00 94 d8  7c 41 16 0f 29 da d2 a8   ..z>.... |A..)...
0040  c9 52 27 e2 13 6c 24 52  99 d7 d5 15 0a ee 59 b5   .R'..l$R ......Y.
0050  96 3e 22 03 87 53 b0 65  5e 42 56 52 ed d5 72 6d   .>"..S.e ^BVR..rm
0060  6b a5 f7 8b f2 b9 d4 00  11 e9 1a 11 8e 1a dc 6c   k....... .......l
```

Frame (1464 bytes) | Reassembled TCP (4407 bytes)

Frame (frame), 1464 bytes | Packets: 2294 · Displayed: 2294 (100,0%) · Dropped: 0 (0,0%) | Profile: Default



*6 interfaces [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp.stream eq 6

Follow TCP Stream (tcp.stream eq 6)

Stream Content

```
.GET /pub/firefox/releases/47.0.1/update/win32/en-US/firefox-47.0.1.complete.mar
HTTP/1.1
Host: download.cdn.mozilla.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Range: bytes=20700000-20999999
If-Range: "05ef18d7946a50cb36dd5b120dd526bf"
Connection: keep-alive

HTTP/1.1 206 Partial Content
Content-Type: application/octet-stream
x-amz-replication-status: COMPLETED
x-amz-version-id: z0xzZy9ZPaZPW.YqDAHwpqjwzYp4J2_Y
Last-Modified: Tue, 28 Jun 2016 12:54:02 GMT
ETag: "05ef18d7946a50cb36dd5b120dd526bf"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Id: NPiz34gdUON8IaN769bLV2bv1kGBVdbTHU9h77whZCUhEI-uTCCEhA==
Date: Mon, 19 Sep 2016 05:24:15 GMT
Content-Range: bytes 20700000-20999999/53634515
Content-Length: 300000
Connection: keep-alive

$_...$.j./.9JJ....sS..&.M..\D?.....<y.QY......JfTi.....:..
......B....l.8h.....6....Z.3.3......A4.xp..+`R..z...F..gf#.Le...1.D.D\
$.x..L........Nu.qp..8....E.5.,7.8\.
......R....~.....;J.1&..~......4.c....<../_.{z*...].K.8KaB.....u.$....-.H-/
^4.8!..,....G..j...j...SL...Q.......
\.tJ....*...b.-1.`...d.7.Z)r..7....ACG.=....g..2..X.#L.zS5#=._.Lw.f(..X...Q=.$.....
..nb.&.{....'Q...f..X.-.e...1.b.a$&.F.............T..
```

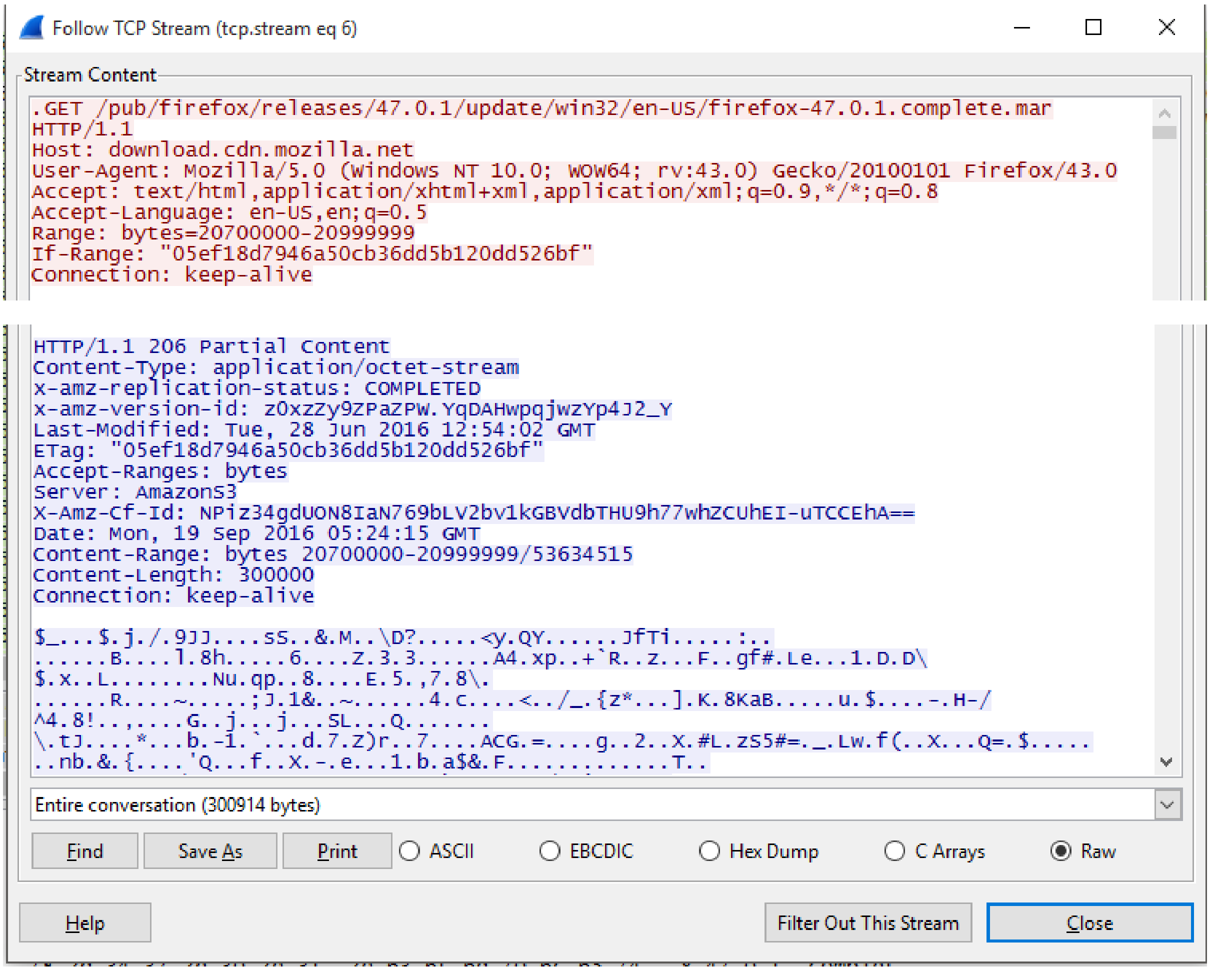
Entire conversation (300914 bytes)

Find | Save As | Print | ○ ASCII | ○ EBCDIC | ○ Hex Dump | ○ C Arrays | ● Raw

Help | Filter Out This Stream | Close

```
n=2321 Len=1
n=3224 Len=0 SLE=1 SRE=2
0.1/update/win32/en-US/firefox-47.0.1.complete.mar HTTP/1.1
Win=3258 Len=0
35 Win=2321 Len=0
95 Win=2321 Len=0
555 Win=2321 Len=0
148.34)

0070  78 2d 34 37 2e 30 2e 31  2e 63 6f 6d 70 6c 65 74   x-47.0.1 .complet
0080  65 2e 6d 61 72 20 48 54  54 50 2f 31 2e 31 0d 0a   e.mar HT TP/1.1..
```

File: "C:\Users\Fiah\AppData\Local\Temp\w... | Packets: 2294 · Displayed: 292 (12,7%) · Dropped: 0 (0,0%) | Profile: Default



```
.GET /pub/firefox/releases/47.0.1/update/win32/en-US/firefox-47.0.1.complete.mar
HTTP/1.1
Host: download.cdn.mozilla.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Range: bytes=20700000-20999999
If-Range: "05ef18d7946a50cb36dd5b120dd526bf"
Connection: keep-alive

HTTP/1.1 206 Partial Content
Content-Type: application/octet-stream
x-amz-replication-status: COMPLETED
x-amz-version-id: z0xzZy9ZPaZPW.YqDAHwpqjwzYp4J2_Y
Last-Modified: Tue, 28 Jun 2016 12:54:02 GMT
ETag: "05ef18d7946a50cb36dd5b120dd526bf"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Id: NPiz34gdUON8IaN769bLV2bv1kGBVdbTHU9h77whZCUhEI-uTCCEhA==
Date: Mon, 19 Sep 2016 05:24:15 GMT
Content-Range: bytes 20700000-20999999/53634515
Content-Length: 300000
Connection: keep-alive

$_...$.j./.9JJ....sS..&.M..\D?.....<y.QY......JfTi.....:..
......B....l.8h.....6....Z.3.3......A4.xp..+`R..z...F..gf#.Le...1.D.D\
$.x..L........Nu.qp..8....E.5.,7.8\.
......R....~.....;J.1&..~......4.c....<../_.{z*...].K.8KaB.....u.$....-.H-/
^4.8!..,....G..j...j...SL...Q.......
\.tJ....*...b.-1.`...d.7.Z)r..7....ACG.=....g..2..X.#L.zS5#=._.Lw.f(..X...Q=.$.....
..nb.&.{....'Q...f..X.-.e...1.b.a$&.F.............T..
```

Entire conversation (300914 bytes)

Analisis :

Wireshark digunakan untuk menganalisis paket inbound dan outbound dari sistem kita. kita gunakan untuk memantau permintaan GET dan POST yang sedang dikirim dari mesin kita. Ini membantu kita menganalisis data yang tepat yang sedang dikirim ke situs web tertentu. paket mulai dapat ditangkap dan kita dapat melihat mereka di jendela Wireshark. Amati protokol paket, wireshark memberitahu kita apa protokol yang digunakan untuk mentransfer paket. Ini membantu kita menyaring mana paket yang kita butuhkan dan meninggalkan sisanya. Sekarang kita menemukan GET dan POST paket (yang mengikuti protokol HTTP) kita perlu mengatur filter yang sesuai. Perhatikan kotak filter teks. Kita ketik **http.request.method == GET atau http.request.method == POST** dan tekan enter. kita dapat menyimpannya untuk penggunaan selanjutnya juga, sehingga kita tidak perlu mengingat setiap kali kita ingin menyaring paket.

Klik kanan pada paket yang kita ingin menganalisis dan klik pada Follow TCP Stream. Sebuah jendela baru akan terbuka dengan semua rincian data yang dikirim dan diterima. Untuk lebih akurat, permintaan yang dikirim dan respon diterima. Yang kita pilih mungkin sekali berbeda tetapi dasar-dasar tetap sama.

GET menunjukkan metode yang digunakan (GET atau POST) URL menunjukkan URL yang permintaan sedang dikirim.

Protokol dalam hal ini jelas akan HTTP. Hal ini juga menunjukkan yaitu Jika diubah adalah salah satu pesan header, ini menunjukkan bahwa permintaan ini hanya untuk memeriksa apakah URL tersebut dimodifikasi sejak waktu yang ditentukan.

Seperti yang kita lihat dalam pesan Response semua kita kembali adalah Not Modified User Agent berisi informasi tentang browser yang digunakan. Referer menunjukkan URL dari mana permintaan itu disebut. Terima-Encoding juga merupakan salah satu dari header pesan yang menunjukkan metode encoding yang berbeda yang dapat diterjemahkan oleh browser dari mana permintaan sedang dikirim. Cookie berisi data yang disimpan dalam cookie browser kita saat ini. Kita dapat membaca respon dengan cara yang sama HTTP menunjukkan protokol versi yang digunakan. 304 adalah kode status Not Modified. Anda dapat menemukan semua kode status HTTP Tanggal menunjukkan waktu selama respon yang dihasilkan. Jadi sekarang kita tahu bagaimana menganalisis paket menggunakan Wireshark.