LAB REPORT 1

ECE 455

ODU Honor pledge

“I pledge to support the Honor System of Old Dominion University.

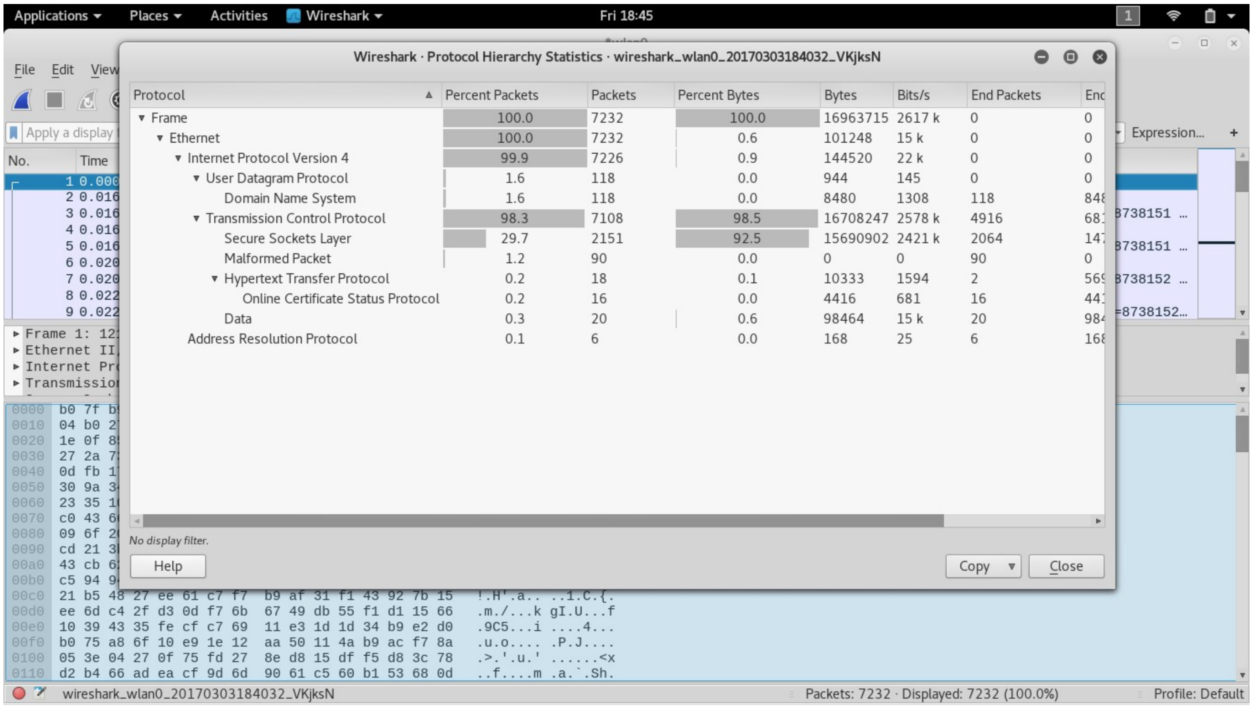
I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violation of the Honor Code. I will report to a hearing if summoned.”

Your name: Bradley McKee

UIN: 00975338

Sign here: BLM (initials represent signature)

In this lab we were instructed to do the networking lab with a program called Wireshark. After reading the lab I decided that it would make it a lot easier on myself if I had a computer than ran Kali Linux. I decided to make a partition on my laptop and install kali linux mainly because it comes with all the software we will be using this semester. Last semester I became familiar with using Wireshark in ECE 355. Attached will be screenshots taken from my laptop as proof that I went through and completed the lab.



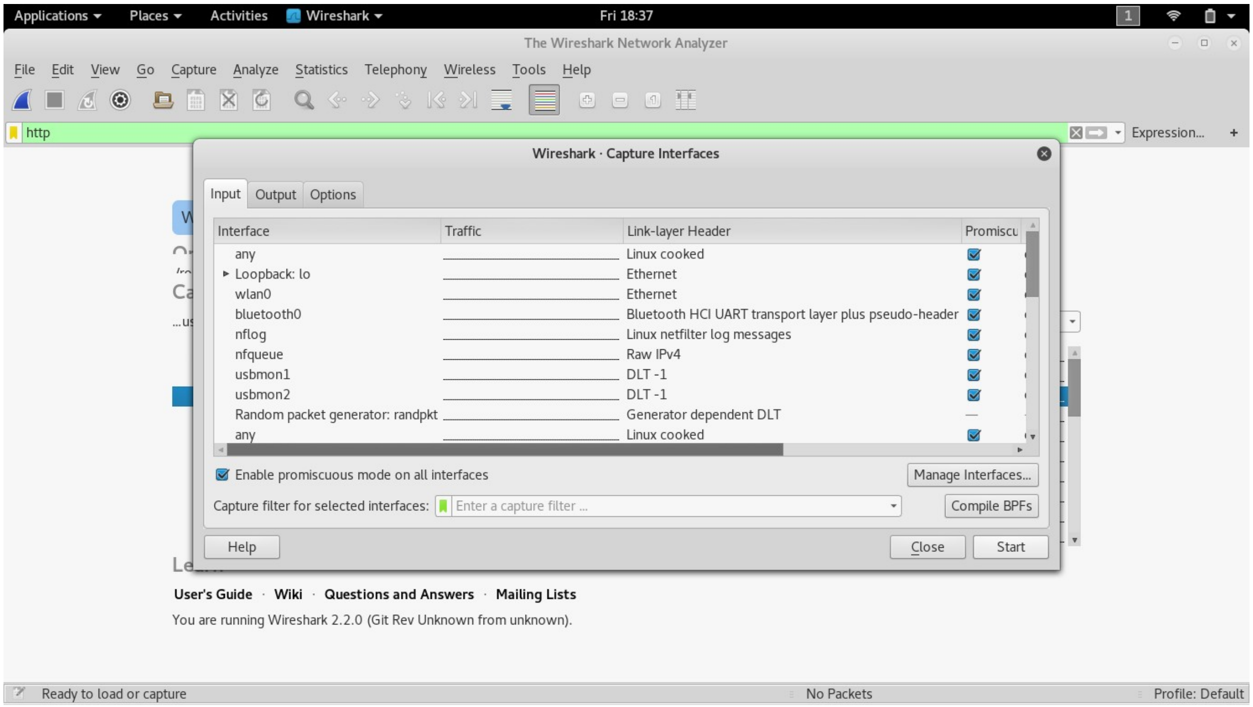
Wireshark · Protocol Hierarchy Statistics · wireshark_wlan0_20170303184032_VKjksN

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	Enc
▾ Frame	100.0	7232	100.0	16963715	2617 k	0	0
▾ Ethernet	100.0	7232	0.6	101248	15 k	0	0
▾ Internet Protocol Version 4	99.9	7226	0.9	144520	22 k	0	0
▾ User Datagram Protocol	1.6	118	0.0	944	145	0	0
Domain Name System	1.6	118	0.0	8480	1308	118	848
▾ Transmission Control Protocol	98.3	7108	98.5	16708247	2578 k	4916	681
Secure Sockets Layer	29.7	2151	92.5	15690902	2421 k	2064	147
Malformed Packet	1.2	90	0.0	0	0	90	0
▾ Hypertext Transfer Protocol	0.2	18	0.1	10333	1594	2	569
Online Certificate Status Protocol	0.2	16	0.0	4416	681	16	441
Data	0.3	20	0.6	98464	15 k	20	984
Address Resolution Protocol	0.1	6	0.0	168	25	6	168

No display filter.

```
No.   Time
  1 0.000
  2 0.016
  3 0.016                8738151 ...
  4 0.016
  5 0.016                8738151 ...
  6 0.020
  7 0.020                8738152 ...
  8 0.022
  9 0.022                =8738152...
▸ Frame 1: 12
▸ Ethernet II,
▸ Internet Pr
▸ Transmissior
0000  b0 7f b
0010  04 b0 2
0020  1e 0f 8
0030  27 2a 7
0040  0d fb 1
0050  30 9a 3
0060  23 35 1
0070  c0 43 6
0080  09 6f 2
0090  cd 21 3
00a0  43 cb 6
00b0  c5 94 9
00c0  21 b5 48 27 ee 61 c7 f7  b9 af 31 f1 43 92 7b 15   !.H'.a.. ..1.C.{.
00d0  ee 6d c4 2f d3 0d f7 6b  67 49 db 55 f1 d1 15 66   .m./...k gI.U...f
00e0  10 39 43 35 fe cf c7 69  11 e3 1d 1d 34 b9 e2 d0   .9C5...i ....4...
00f0  b0 75 a8 6f 10 e9 1e 12  aa 50 11 4a b9 ac f7 8a   .u.o.... .P.J....
0100  05 3e 04 27 0f 75 fd 27  8e d8 15 df f5 d8 3c 78   .>.'.u.' ......<x
0110  d2 b4 66 ad ea cf 9d 6d  90 61 c5 60 b1 53 68 0d   ..f....m .a.`.Sh.
```

wireshark_wlan0_20170303184032_VKjksN   Packets: 7232 · Displayed: 7232 (100.0%)   Profile: Default



http

Wireshark · Capture Interfaces

Interface	Traffic	Link-layer Header	Promiscu
any		Linux cooked	☑
▸ Loopback: lo		Ethernet	☑
wlan0		Ethernet	☑
bluetooth0		Bluetooth HCI UART transport layer plus pseudo-header	☑
nflog		Linux netfilter log messages	☑
nfqueue		Raw IPv4	☑
usbmon1		DLT -1	☑
usbmon2		DLT -1	☑
Random packet generator: randpkt		Generator dependent DLT	—
any		Linux cooked	☑

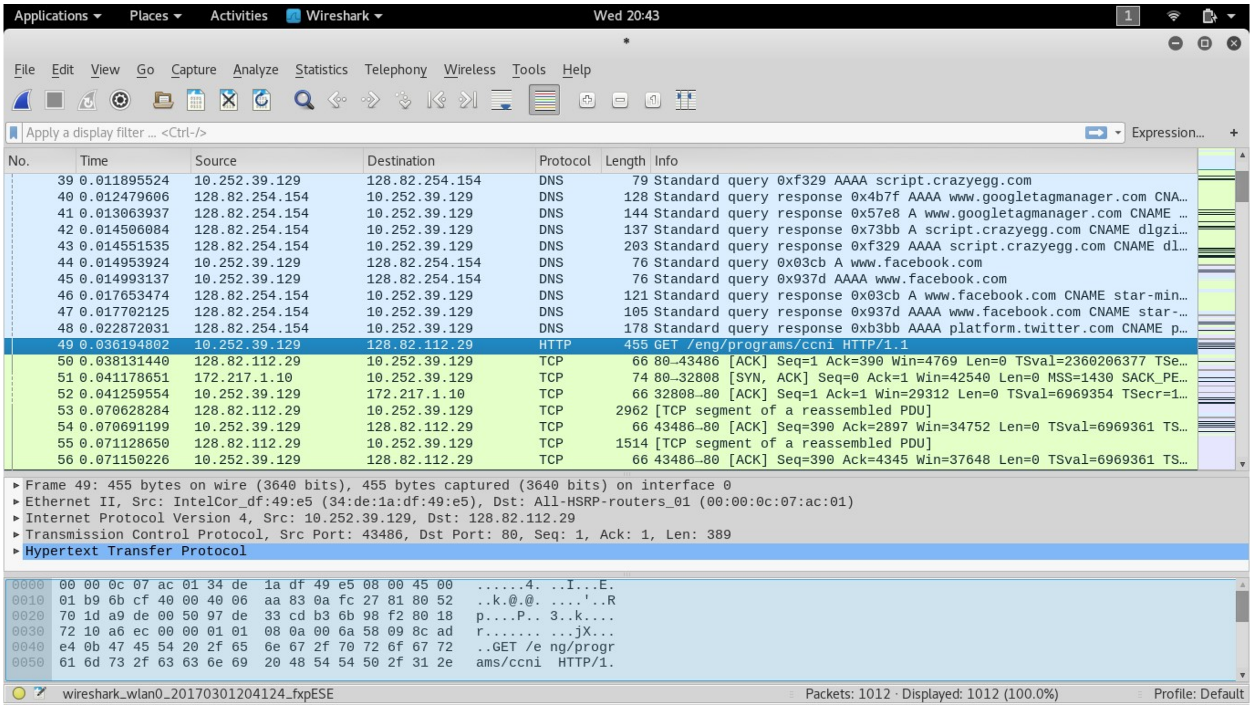
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.2.0 (Git Rev Unknown from unknown).

Ready to load or capture   No Packets   Profile: Default

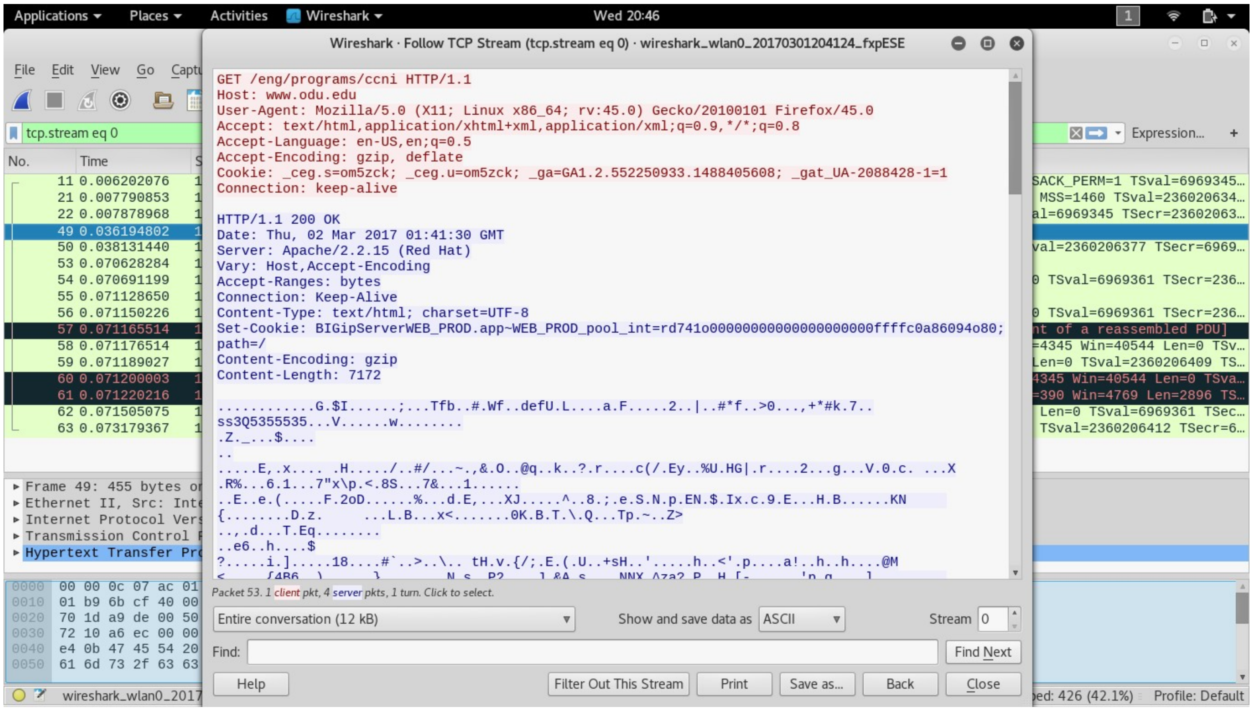


```
No.  Time         Source          Destination     Protocol Length Info
  39 0.011895524  10.252.39.129   128.82.254.154  DNS        79 Standard query 0xf329 AAAA script.crazyegg.com
  40 0.012479606  128.82.254.154  10.252.39.129   DNS       128 Standard query response 0x4b7f AAAA www.googletagmanager.com CNA…
  41 0.013063937  128.82.254.154  10.252.39.129   DNS       144 Standard query response 0x57e8 A www.googletagmanager.com CNAME …
  42 0.014506084  128.82.254.154  10.252.39.129   DNS       137 Standard query response 0x73bb A script.crazyegg.com CNAME dlgzi…
  43 0.014551535  128.82.254.154  10.252.39.129   DNS       203 Standard query response 0xf329 AAAA script.crazyegg.com CNAME dl…
  44 0.014953924  10.252.39.129   128.82.254.154  DNS        76 Standard query 0x03cb A www.facebook.com
  45 0.014993137  10.252.39.129   128.82.254.154  DNS        76 Standard query 0x937d AAAA www.facebook.com
  46 0.017653474  128.82.254.154  10.252.39.129   DNS       121 Standard query response 0x03cb A www.facebook.com CNAME star-min…
  47 0.017702125  128.82.254.154  10.252.39.129   DNS       105 Standard query response 0x937d AAAA www.facebook.com CNAME star-…
  48 0.022872031  128.82.254.154  10.252.39.129   DNS       178 Standard query response 0xb3bb AAAA platform.twitter.com CNAME p…
  49 0.036194802  10.252.39.129   128.82.112.29   HTTP      455 GET /eng/programs/ccni HTTP/1.1
  50 0.038131440  128.82.112.29   10.252.39.129   TCP        66 80→43486 [ACK] Seq=1 Ack=390 Win=4769 Len=0 TSval=2360206377 TSe…
  51 0.041178651  172.217.1.10    10.252.39.129   TCP        74 80→32808 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1430 SACK_PE…
  52 0.041259554  10.252.39.129   172.217.1.10    TCP        66 32808→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=6969354 TSecr=1…
  53 0.070628284  128.82.112.29   10.252.39.129   TCP      2962 [TCP segment of a reassembled PDU]
  54 0.070691199  10.252.39.129   128.82.112.29   TCP        66 43486→80 [ACK] Seq=390 Ack=2897 Win=34752 Len=0 TSval=6969361 TS…
  55 0.071128650  128.82.112.29   10.252.39.129   TCP      1514 [TCP segment of a reassembled PDU]
  56 0.071150226  10.252.39.129   128.82.112.29   TCP        66 43486→80 [ACK] Seq=390 Ack=4345 Win=37648 Len=0 TSval=6969361 TS…

▸ Frame 49: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 0
▸ Ethernet II, Src: IntelCor_df:49:e5 (34:de:1a:df:49:e5), Dst: All-HSRP-routers_01 (00:00:0c:07:ac:01)
▸ Internet Protocol Version 4, Src: 10.252.39.129, Dst: 128.82.112.29
▸ Transmission Control Protocol, Src Port: 43486, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
▸ Hypertext Transfer Protocol

0000  00 00 0c 07 ac 01 34 de  1a df 49 e5 08 00 45 00   ......4. ..I...E.
0010  01 b9 6b cf 40 00 40 06  aa 83 0a fc 27 81 80 52   ..k.@.@. ....'..R
0020  70 1d a9 de 00 50 97 de  33 cd b3 6b 98 f2 80 18   p....P.. 3..k....
0030  72 10 a6 ec 00 00 01 01  08 0a 00 6a 58 09 8c ad   r....... ...jX...
0040  e4 0b 47 45 54 20 2f 65  6e 67 2f 70 72 6f 67 72   ..GET /e ng/progr
0050  61 6d 73 2f 63 63 6e 69  20 48 54 54 50 2f 31 2e   ams/ccni  HTTP/1.
```

wireshark_wlan0_20170301204124_fxpESE   Packets: 1012 · Displayed: 1012 (100.0%)   Profile: Default



tcp.stream eq 0

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_wlan0_20170301204124_fxpESE

```
GET /eng/programs/ccni HTTP/1.1
Host: www.odu.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ceg.s=om5zck; _ceg.u=om5zck; _ga=GA1.2.552250933.1488405608; _gat_UA-2088428-1=1
Connection: keep-alive

HTTP/1.1 200 OK
Date: Thu, 02 Mar 2017 01:41:30 GMT
Server: Apache/2.2.15 (Red Hat)
Vary: Host,Accept-Encoding
Accept-Ranges: bytes
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: BIGipServerWEB_PROD.app~WEB_PROD_pool_int=rd741o00000000000000000000ffffc0a86094o80;
path=/
Content-Encoding: gzip
Content-Length: 7172

............G.$I......;...Tfb..#.Wf..defU.L....a.F.....2..|..#*f..>0...,+*#k.7..
ss3Q5355535...V......w........
.Z._...$....
..
.....E,.x.... .H...../..#/...~.,&.O..@q..k..?.r....c(/.Ey..%U.HG|.r....2...g...V.0.c. ...X
.R%...6.1...7"x\p.<.8S...7&...1......
..E..e.(.....F.2oD......%...d.E,...XJ.....^..8.;.e.S.N.p.EN.$.Ix.c.9.E...H.B......KN
{........D.z.     ...L.B...x<.......0K.B.T.\.Q...Tp.~..Z>
..,.d...T.Eq........
..e6..h....$
?.....i.].....18....#`..>..\.. tH.v.{/;.E.(.U..+sH..'.....h..<'.p....a!..h..h....@M
```

Packet 53. 1 client pkt, 4 server pkts, 1 turn. Click to select.

Entire conversation (12 kB)   Show and save data as ASCII   Stream 0

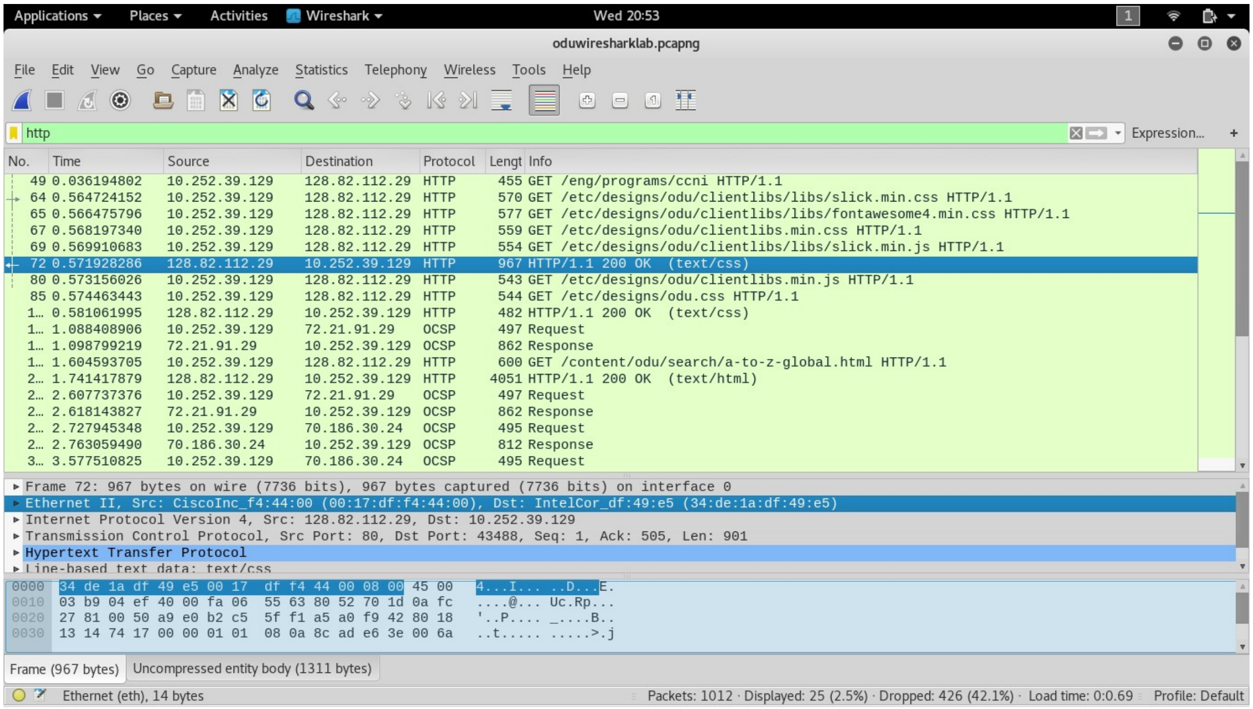
Find:

```
No.  Time
  11 0.006202076    SACK_PERM=1 TSval=6969345…
  21 0.007790853    MSS=1460 TSval=236020634…
  22 0.007878968    al=6969345 TSecr=23602063…
  49 0.036194802
  50 0.038131440    val=2360206377 TSecr=6969…
  53 0.070628284
  54 0.070691199    0 TSval=6969361 TSecr=236…
  55 0.071128650
  56 0.071150226    0 TSval=6969361 TSecr=236…
  57 0.071165514    nt of a reassembled PDU]
  58 0.071176514    =4345 Win=40544 Len=0 TSv…
  59 0.071189027    Len=0 TSval=2360206409 TS…
  60 0.071200003    4345 Win=40544 Len=0 TSva…
  61 0.071220216    =390 Win=4769 Len=2896 TS…
  62 0.071505075    Len=0 TSval=6969361 TSec…
  63 0.073179367    TSval=2360206412 TSecr=6…

▸ Frame 49: 455 bytes or
▸ Ethernet II, Src: Inte
▸ Internet Protocol Vers
▸ Transmission Control P
▸ Hypertext Transfer Pro

0000  00 00 0c 07 ac 01
0010  01 b9 6b cf 40 00
0020  70 1d a9 de 00 50
0030  72 10 a6 ec 00 00
0040  e4 0b 47 45 54 20
0050  61 6d 73 2f 63 63
```

wireshark_wlan0_2017   ed: 426 (42.1%)   Profile: Default



```
http
```

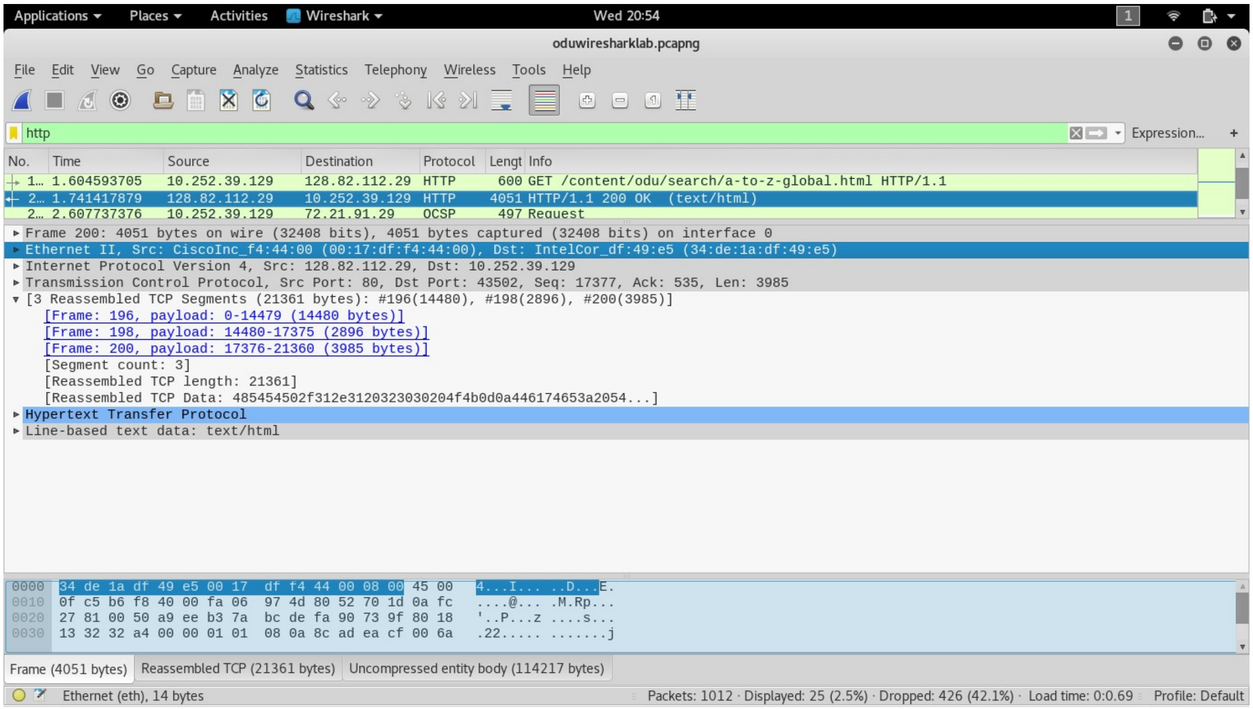
```
No.  Time         Source          Destination     Protocol Lengt Info
  49 0.036194802  10.252.39.129   128.82.112.29   HTTP      455 GET /eng/programs/ccni HTTP/1.1
  64 0.564724152  10.252.39.129   128.82.112.29   HTTP      570 GET /etc/designs/odu/clientlibs/libs/slick.min.css HTTP/1.1
  65 0.566475796  10.252.39.129   128.82.112.29   HTTP      577 GET /etc/designs/odu/clientlibs/libs/fontawesome4.min.css HTTP/1.1
  67 0.568197340  10.252.39.129   128.82.112.29   HTTP      559 GET /etc/designs/odu/clientlibs.min.css HTTP/1.1
  69 0.569910683  10.252.39.129   128.82.112.29   HTTP      554 GET /etc/designs/odu/clientlibs/libs/slick.min.js HTTP/1.1
  72 0.571928286  128.82.112.29   10.252.39.129   HTTP      967 HTTP/1.1 200 OK  (text/css)
  80 0.573156026  10.252.39.129   128.82.112.29   HTTP      543 GET /etc/designs/odu/clientlibs.min.js HTTP/1.1
  85 0.574463443  10.252.39.129   128.82.112.29   HTTP      544 GET /etc/designs/odu.css HTTP/1.1
  1… 0.581061995  128.82.112.29   10.252.39.129   HTTP      482 HTTP/1.1 200 OK  (text/css)
  1… 1.088408906  10.252.39.129   72.21.91.29     OCSP      497 Request
  1… 1.098799219  72.21.91.29     10.252.39.129   OCSP      862 Response
  1… 1.604593705  10.252.39.129   128.82.112.29   HTTP      600 GET /content/odu/search/a-to-z-global.html HTTP/1.1
  2… 1.741417879  128.82.112.29   10.252.39.129   HTTP     4051 HTTP/1.1 200 OK  (text/html)
  2… 2.607737376  10.252.39.129   72.21.91.29     OCSP      497 Request
  2… 2.618143827  72.21.91.29     10.252.39.129   OCSP      862 Response
  2… 2.727945348  10.252.39.129   70.186.30.24    OCSP      495 Request
  2… 2.763059490  70.186.30.24    10.252.39.129   OCSP      812 Response
  3… 3.577510825  10.252.39.129   70.186.30.24    OCSP      495 Request
```

```
▸ Frame 72: 967 bytes on wire (7736 bits), 967 bytes captured (7736 bits) on interface 0
▸ Ethernet II, Src: CiscoInc_f4:44:00 (00:17:df:f4:44:00), Dst: IntelCor_df:49:e5 (34:de:1a:df:49:e5)
▸ Internet Protocol Version 4, Src: 128.82.112.29, Dst: 10.252.39.129
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 43488, Seq: 1, Ack: 505, Len: 901
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/css
```

```
0000  34 de 1a df 49 e5 00 17  df f4 44 00 08 00 45 00   4...I... ..D...E.
0010  03 b9 04 ef 40 00 fa 06  55 63 80 52 70 1d 0a fc   ....@... Uc.Rp...
0020  27 81 00 50 a9 e0 b2 c5  5f f1 a5 a0 f9 42 80 18   '..P.... _....B..
0030  13 14 74 17 00 00 01 01  08 0a 8c ad e6 3e 00 6a   ..t..... .....>.j
```

Frame (967 bytes) | Uncompressed entity body (1311 bytes)

Ethernet (eth), 14 bytes   Packets: 1012 · Displayed: 25 (2.5%) · Dropped: 426 (42.1%) · Load time: 0:0.69   Profile: Default



```
http
```

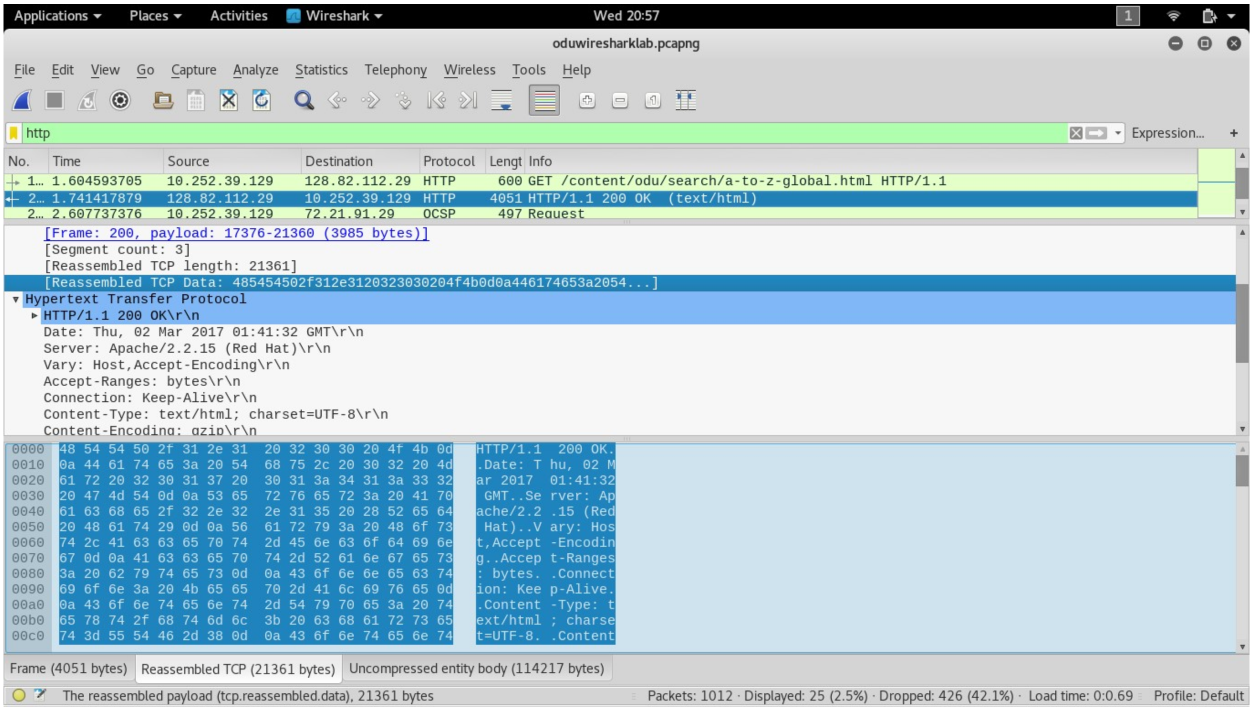
```
No.  Time         Source          Destination     Protocol Lengt Info
  1… 1.604593705  10.252.39.129   128.82.112.29   HTTP      600 GET /content/odu/search/a-to-z-global.html HTTP/1.1
  2… 1.741417879  128.82.112.29   10.252.39.129   HTTP     4051 HTTP/1.1 200 OK  (text/html)
  2… 2.607737376  10.252.39.129   72.21.91.29     OCSP      497 Request
```

```
▸ Frame 200: 4051 bytes on wire (32408 bits), 4051 bytes captured (32408 bits) on interface 0
▸ Ethernet II, Src: CiscoInc_f4:44:00 (00:17:df:f4:44:00), Dst: IntelCor_df:49:e5 (34:de:1a:df:49:e5)
▸ Internet Protocol Version 4, Src: 128.82.112.29, Dst: 10.252.39.129
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 43502, Seq: 17377, Ack: 535, Len: 3985
▾ [3 Reassembled TCP Segments (21361 bytes): #196(14480), #198(2896), #200(3985)]
    [Frame: 196, payload: 0-14479 (14480 bytes)]
    [Frame: 198, payload: 14480-17375 (2896 bytes)]
    [Frame: 200, payload: 17376-21360 (3985 bytes)]
    [Segment count: 3]
    [Reassembled TCP length: 21361]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054...]
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html
```

```
0000  34 de 1a df 49 e5 00 17  df f4 44 00 08 00 45 00   4...I... ..D...E.
0010  0f c5 b6 f8 40 00 fa 06  97 4d 80 52 70 1d 0a fc   ....@... .M.Rp...
0020  27 81 00 50 a9 ee b3 7a  bc de fa 90 73 9f 80 18   '..P...z ....s...
0030  13 32 32 a4 00 00 01 01  08 0a 8c ad ea cf 00 6a   .22..... .......j
```

Frame (4051 bytes) | Reassembled TCP (21361 bytes) | Uncompressed entity body (114217 bytes)

Ethernet (eth), 14 bytes   Packets: 1012 · Displayed: 25 (2.5%) · Dropped: 426 (42.1%) · Load time: 0:0.69   Profile: Default



```
http
```

```
No.   Time          Source          Destination     Protocol  Lengt Info
1…  1.604593705   10.252.39.129   128.82.112.29   HTTP       600 GET /content/odu/search/a-to-z-global.html HTTP/1.1
2…  1.741417879   128.82.112.29   10.252.39.129   HTTP      4051 HTTP/1.1 200 OK  (text/html)
2…  2.607737376   10.252.39.129   72.21.91.29     OCSP       497 Request
```

```
    [Frame: 200, payload: 17376-21360 (3985 bytes)]
    [Segment count: 3]
    [Reassembled TCP length: 21361]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054...]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Thu, 02 Mar 2017 01:41:32 GMT\r\n
    Server: Apache/2.2.15 (Red Hat)\r\n
    Vary: Host,Accept-Encoding\r\n
    Accept-Ranges: bytes\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Content-Encoding: gzip\r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 54  68 75 2c 20 30 32 20 4d   .Date: T hu, 02 M
0020  61 72 20 32 30 31 37 20  30 31 3a 34 31 3a 33 32   ar 2017  01:41:32
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0040  61 63 68 65 2f 32 2e 32  2e 31 35 20 28 52 65 64   ache/2.2 .15 (Red
0050  20 48 61 74 29 0d 0a 56  61 72 79 3a 20 48 6f 73    Hat)..V ary: Hos
0060  74 2c 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   t,Accept -Encodin
0070  67 0d 0a 41 63 63 65 70  74 2d 52 61 6e 67 65 73   g..Accep t-Ranges
0080  3a 20 62 79 74 65 73 0d  0a 43 6f 6e 6e 65 63 74   : bytes. .Connect
0090  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive.
00a0  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   .Content -Type: t
00b0  65 78 74 2f 68 74 6d 6c  3b 20 63 68 61 72 73 65   ext/html ; charse
00c0  74 3d 55 54 46 2d 38 0d  0a 43 6f 6e 74 65 6e 74   t=UTF-8. .Content
```

Frame (4051 bytes) | Reassembled TCP (21361 bytes) | Uncompressed entity body (114217 bytes)

The reassembled payload (tcp.reassembled.data), 21361 bytes · Packets: 1012 · Displayed: 25 (2.5%) · Dropped: 426 (42.1%) · Load time: 0:0.69 · Profile: Default

We can only see the HTTP request and response in plain text, but the data part is completely scrambled, Why?

I suspect that the data part is scrambled because the way that it is encrypted when it is being sent. From my understanding is that when they send packets of data it is compressed and then decompressed once the whole segment is transmitted. I think it decompresses the data transfer after all the segments have been received and then it converts it to readable plaintext at the end.