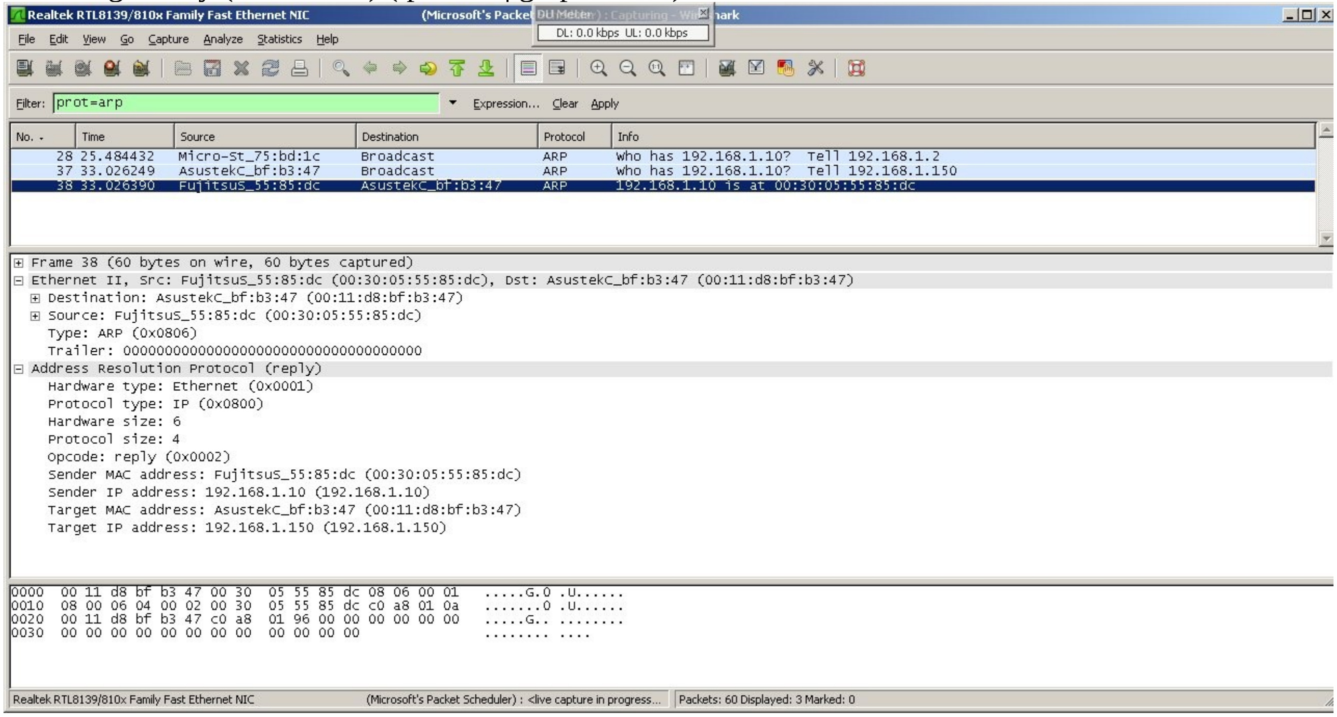
Yamin Mousselli
Cs 8803: Security Operations

How the Internet Works Writeup

Step 1: ARP Process

ARP is a protocol for mapping an IP address to a MAC address on the local network. Unfortunately, my machine was unable to capture ARP packets. I flushed the ARP table, but no dice. It should've communicated with the router and performed ARP on the Default Gateway. There wasn't any ARP traffic when I filtered for 'arp' but here is what it would like if I did find ARP packets in Wireshark:

Default gateway (router's IP) (ip route | grep default): 143.215.204.1


Realtek RTL8139/810x Family Fast Ethernet NIC (Microsoft's Packet DU Meter) : Capturing - Wireshark
DL: 0.0 kbps UL: 0.0 kbps
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: prot=arp

```
No. -  Time         Source               Destination          Protocol  Info
    28 25.484432    Micro-St_75:bd:1c    Broadcast            ARP       Who has 192.168.1.10?  Tell 192.168.1.2
    37 33.026249    AsustekC_bf:b3:47    Broadcast            ARP       Who has 192.168.1.10?  Tell 192.168.1.150
    38 33.026390    FujitsuS_55:85:dc    AsustekC_bf:b3:47    ARP       192.168.1.10 is at 00:30:05:55:85:dc
```

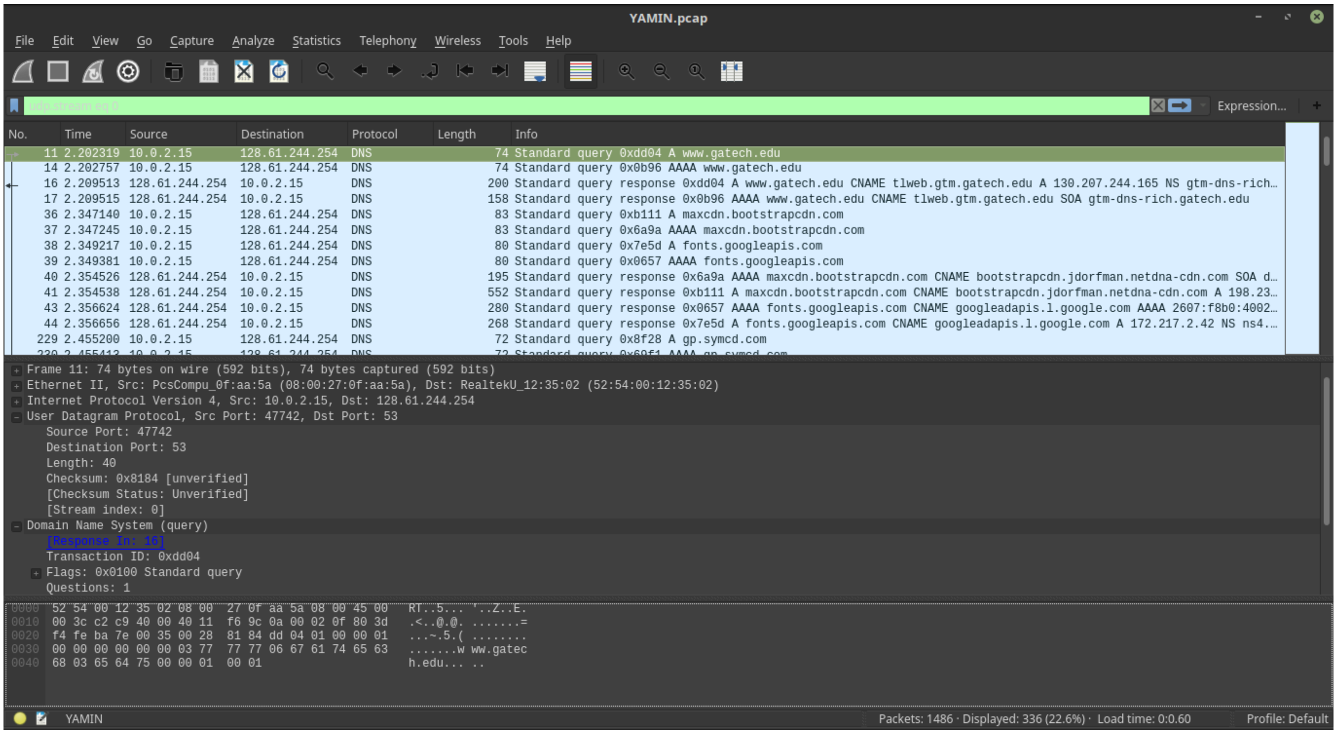
```
⊞ Frame 38 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: FujitsuS_55:85:dc (00:30:05:55:85:dc), Dst: AsustekC_bf:b3:47 (00:11:d8:bf:b3:47)
  ⊞ Destination: AsustekC_bf:b3:47 (00:11:d8:bf:b3:47)
  ⊞ Source: FujitsuS_55:85:dc (00:30:05:55:85:dc)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: FujitsuS_55:85:dc (00:30:05:55:85:dc)
    Sender IP address: 192.168.1.10 (192.168.1.10)
    Target MAC address: AsustekC_bf:b3:47 (00:11:d8:bf:b3:47)
    Target IP address: 192.168.1.150 (192.168.1.150)
```

```
0000  00 11 d8 bf b3 47 00 30  05 55 85 dc 08 06 00 01   .....G.0 .U......
0010  08 00 06 04 00 02 00 30  05 55 85 dc c0 a8 01 0a   .......0 .U......
0020  00 11 d8 bf b3 47 c0 a8  01 96 00 00 00 00 00 00   .....G.. ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Realtek RTL8139/810x Family Fast Ethernet NIC (Microsoft's Packet Scheduler) : <live capture in progress... Packets: 60 Displayed: 3 Marked: 0

Step 2: DNS Process

DNS resolves a host name to an IP address and that mapping is stored in the address record (A-record). The first picture is the DNS request with query id 0xdd04 and the one after it is the DNS response packet.


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

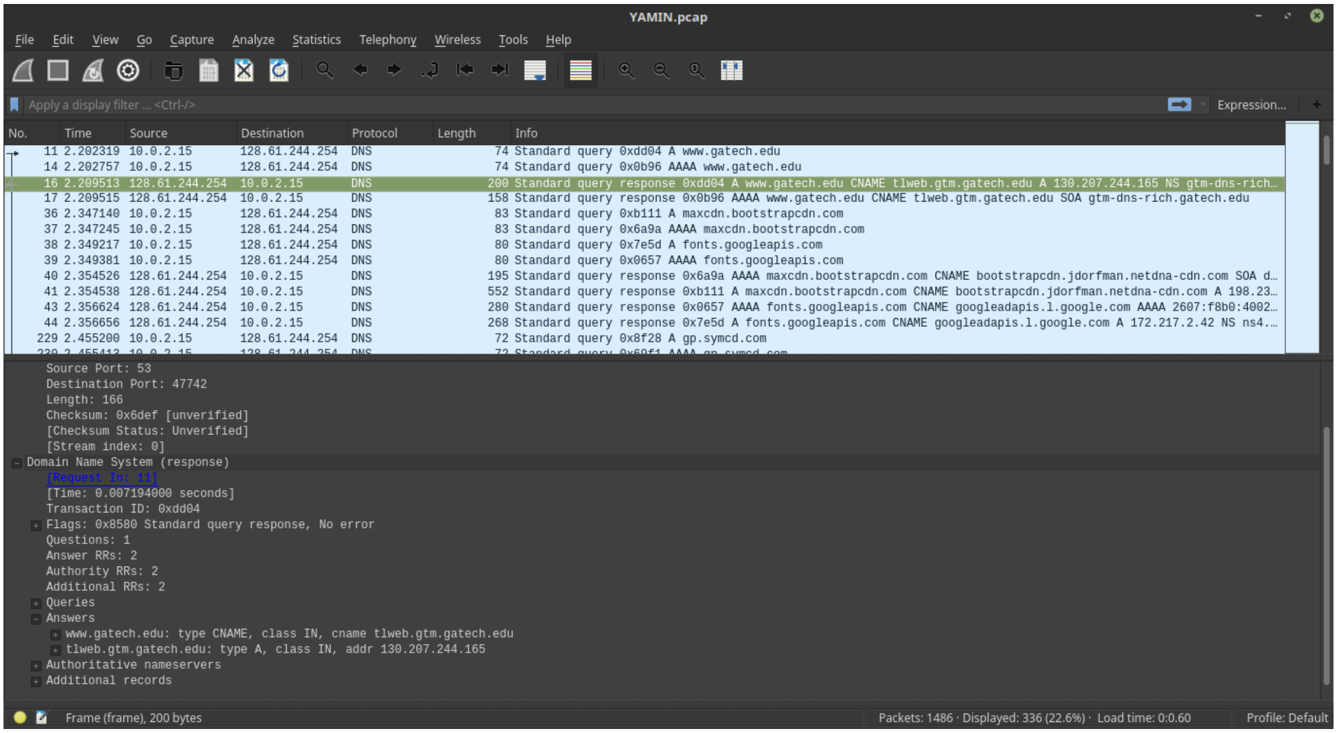
```
udp.stream eq 0
```

```
No.  Time     Source         Destination    Protocol  Length Info
  11 2.202319 10.0.2.15      128.61.244.254 DNS           74 Standard query 0xdd04 A www.gatech.edu
  14 2.202757 10.0.2.15      128.61.244.254 DNS           74 Standard query 0x0b96 AAAA www.gatech.edu
  16 2.209513 128.61.244.254 10.0.2.15      DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
  17 2.209515 128.61.244.254 10.0.2.15      DNS          158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu
  36 2.347140 10.0.2.15      128.61.244.254 DNS           83 Standard query 0xb111 A maxcdn.bootstrapcdn.com
  37 2.347245 10.0.2.15      128.61.244.254 DNS           83 Standard query 0x6a9a AAAA maxcdn.bootstrapcdn.com
  38 2.349217 10.0.2.15      128.61.244.254 DNS           80 Standard query 0x7e5d A fonts.googleapis.com
  39 2.349381 10.0.2.15      128.61.244.254 DNS           80 Standard query 0x0657 AAAA fonts.googleapis.com
  40 2.354526 128.61.244.254 10.0.2.15      DNS          195 Standard query response 0x6a9a AAAA maxcdn.bootstrapcdn.com CNAME bootstrapcdn.jdorfman.netdna-cdn.com SOA d…
  41 2.354538 128.61.244.254 10.0.2.15      DNS          552 Standard query response 0xb111 A maxcdn.bootstrapcdn.com CNAME bootstrapcdn.jdorfman.netdna-cdn.com A 198.23…
  43 2.356624 128.61.244.254 10.0.2.15      DNS          280 Standard query response 0x0657 AAAA fonts.googleapis.com CNAME googleadapis.l.google.com AAAA 2607:f8b0:4002…
  44 2.356656 128.61.244.254 10.0.2.15      DNS          268 Standard query response 0x7e5d A fonts.googleapis.com CNAME googleadapis.l.google.com A 172.217.2.42 NS ns4.…
 229 2.455200 10.0.2.15      128.61.244.254 DNS           72 Standard query 0x8f28 A gp.symcd.com
 230 2.455413 10.0.2.15      128.61.244.254 DNS           72 Standard query 0x69f1 AAAA gp.symcd.com
```

```
+ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
+ Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.61.244.254
- User Datagram Protocol, Src Port: 47742, Dst Port: 53
    Source Port: 47742
    Destination Port: 53
    Length: 40
    Checksum: 0x8184 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
- Domain Name System (query)
    [Response In: 16]
    Transaction ID: 0xdd04
  + Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  00 3c c2 c9 40 00 40 11  f6 9c 0a 00 02 0f 80 3d   .<..@.@. .......=
0020  f4 fe ba 7e 00 35 00 28  81 84 dd 04 01 00 00 01   ...~.5.( ........
0030  00 00 00 00 00 00 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01                     h.edu... ..
```

YAMIN | Packets: 1486 · Displayed: 336 (22.6%) · Load time: 0:0.60 | Profile: Default

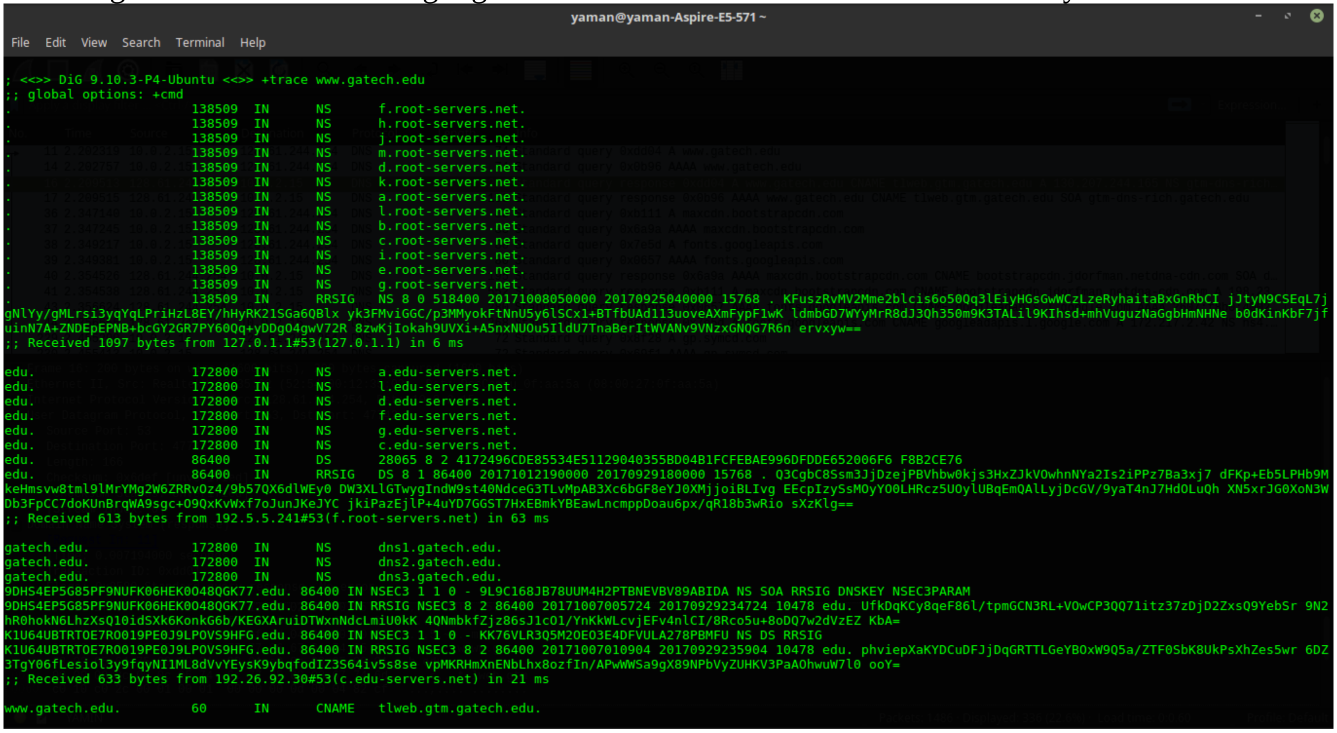

YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time     Source         Destination    Protocol  Length Info
  11 2.202319 10.0.2.15      128.61.244.254 DNS           74 Standard query 0xdd04 A www.gatech.edu
  14 2.202757 10.0.2.15      128.61.244.254 DNS           74 Standard query 0x0b96 AAAA www.gatech.edu
  16 2.209513 128.61.244.254 10.0.2.15      DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
  17 2.209515 128.61.244.254 10.0.2.15      DNS          158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu
  36 2.347140 10.0.2.15      128.61.244.254 DNS           83 Standard query 0xb111 A maxcdn.bootstrapcdn.com
  37 2.347245 10.0.2.15      128.61.244.254 DNS           83 Standard query 0x6a9a AAAA maxcdn.bootstrapcdn.com
  38 2.349217 10.0.2.15      128.61.244.254 DNS           80 Standard query 0x7e5d A fonts.googleapis.com
  39 2.349381 10.0.2.15      128.61.244.254 DNS           80 Standard query 0x0657 AAAA fonts.googleapis.com
  40 2.354526 128.61.244.254 10.0.2.15      DNS          195 Standard query response 0x6a9a AAAA maxcdn.bootstrapcdn.com CNAME bootstrapcdn.jdorfman.netdna-cdn.com SOA d…
  41 2.354538 128.61.244.254 10.0.2.15      DNS          552 Standard query response 0xb111 A maxcdn.bootstrapcdn.com CNAME bootstrapcdn.jdorfman.netdna-cdn.com A 198.23…
  43 2.356624 128.61.244.254 10.0.2.15      DNS          280 Standard query response 0x0657 AAAA fonts.googleapis.com CNAME googleadapis.l.google.com AAAA 2607:f8b0:4002…
  44 2.356656 128.61.244.254 10.0.2.15      DNS          268 Standard query response 0x7e5d A fonts.googleapis.com CNAME googleadapis.l.google.com A 172.217.2.42 NS ns4.…
 229 2.455200 10.0.2.15      128.61.244.254 DNS           72 Standard query 0x8f28 A gp.symcd.com
 230 2.455413 10.0.2.15      128.61.244.254 DNS           72 Standard query 0x69f1 AAAA gp.symcd.com
```

```
    Source Port: 53
    Destination Port: 47742
    Length: 166
    Checksum: 0x6def [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
- Domain Name System (response)
    [Request In: 11]
    [Time: 0.007194000 seconds]
    Transaction ID: 0xdd04
  + Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 2
  + Queries
  - Answers
    + www.gatech.edu: type CNAME, class IN, cname tlweb.gtm.gatech.edu
    + tlweb.gtm.gatech.edu: type A, class IN, addr 130.207.244.165
  + Authoritative nameservers
  + Additional records
```

Frame (frame), 200 bytes | Packets: 1486 · Displayed: 336 (22.6%) · Load time: 0:0.60 | Profile: Default

The image below shows me using dig to trace the DNS recursion that occurs locally.


yaman@yaman-Aspire-E5-571 ~
File Edit View Search Terminal Help

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> +trace www.gatech.edu
;; global options: +cmd
.                       138509  IN      NS      f.root-servers.net.
.                       138509  IN      NS      h.root-servers.net.
.                       138509  IN      NS      j.root-servers.net.
.                       138509  IN      NS      m.root-servers.net.
.                       138509  IN      NS      d.root-servers.net.
.                       138509  IN      NS      k.root-servers.net.
.                       138509  IN      NS      a.root-servers.net.
.                       138509  IN      NS      l.root-servers.net.
.                       138509  IN      NS      b.root-servers.net.
.                       138509  IN      NS      c.root-servers.net.
.                       138509  IN      NS      i.root-servers.net.
.                       138509  IN      NS      e.root-servers.net.
.                       138509  IN      NS      g.root-servers.net.
.                       138509  IN      RRSIG   NS 8 0 518400 20171008050000 20170925040000 15768 . KFuszRvMV2Mme2blcis6o50Qq3lEiyHGsGwWCzLzeRyhaitaBxGnRbCI jJtyN9CSEqL7j
gNlYy/gMLrsi3yqYqLPriHzL8EY/hHyRK21SGa6QBlx yk3FMviGGC/p3MMyokFtNnU5y6lSCx1+BTfbUAd113uoveAXmFypF1wK ldmbGD7WYyMrR8dJ3Qh350m9K3TALil9KIhsd+mhVuguzNaGgbHmNHNe b0dKinKbF7jf
uinN7A+ZNDEpEPNB+bcGY2GR7PY60Qq+yDDgO4gwV72R 8zwKjIokah9UVXi+A5nxNUOu5IldU7TnaBerItWVANv9VNzxGNQG7R6n ervxyw==
;; Received 1097 bytes from 127.0.1.1#53(127.0.1.1) in 6 ms

edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    86400   IN      DS      28065 8 2 4172496CDE85534E51129040355BD04B1FCFEBAE996DFDDE652006F6 F8B2CE76
edu.                    86400   IN      RRSIG   DS 8 1 86400 20171012190000 20170929180000 15768 . Q3CgbC8Ssm3JjDzejPBVhbw0kjs3HxZJkVOwhnNYa2Is2iPPz7Ba3xj7 dFKp+Eb5LPHb9M
keHmsvw8tml9lMrYMg2W6ZRRvOz4/9b57QX6dlWEy0 DW3XLlGTwygIndW9st40NdceG3TLvMpAB3Xc6bGF8eYJ0XMjjoiBLIvg EEcpIzySsMOyYO0LHRcz5UOylUBqEmQAlLyjDcGV/9yaT4nJ7HdOLuQh XN5xrJG0XoN3W
Db3FpCC7doKUnBrqWA9sgc+O9QxKvWxf7oJunJKeJYC jkiPazEjlP+4uYD7GGST7HxEBmkYBEawLncmppDoau6px/qR18b3wRio sXzKlg==
;; Received 613 bytes from 192.5.5.241#53(f.root-servers.net) in 63 ms

gatech.edu.             172800  IN      NS      dns1.gatech.edu.
gatech.edu.             172800  IN      NS      dns2.gatech.edu.
gatech.edu.             172800  IN      NS      dns3.gatech.edu.
9DHS4EP5G85PF9NUFK06HEK0O48QGK77.edu. 86400 IN NSEC3 1 1 0 - 9L9C168JB78UUM4H2PTBNEVBV89ABIDA NS SOA RRSIG DNSKEY NSEC3PARAM
9DHS4EP5G85PF9NUFK06HEK0O48QGK77.edu. 86400 IN RRSIG NSEC3 8 2 86400 20171007005724 20170929234724 10478 edu. UfkDqKCy8qeF86l/tpmGCN3RL+VOwCP3QQ71itz37zDjD2ZxsQ9YebSr 9N2
hR0hokN6LhzXsQ10idSXk6KonkG6b/KEGXAruiDTWxnNdcLmiU0kK 4QNmbkfZjz86sJ1cO1/YnKkWLcvjEFv4nlCI/8Rco5u+8oDQ7w2dVzEZ KbA=
K1U64UBTRTOE7RO019PE0J9LPOVS9HFG.edu. 86400 IN NSEC3 1 1 0 - KK76VLR3Q5M2OEO3E4DFVULA278PBMFU NS DS RRSIG
K1U64UBTRTOE7RO019PE0J9LPOVS9HFG.edu. 86400 IN RRSIG NSEC3 8 2 86400 20171007010904 20170929235904 10478 edu. phviepXaKYDCuDFJjDqGRTTLGeYBOxW9Q5a/ZTF0SbK8UkPsXhZes5wr 6DZ
3TgY06fLesiol3y9fqyNI1ML8dVvYEysK9ybqfodIZ3S64iv5s8se vpMKRHmXnENbLhx8ozfIn/APwWWSa9gX89NPbVyZUHKV3PaAOhwuW7l0 ooY=
;; Received 633 bytes from 192.26.92.30#53(c.edu-servers.net) in 21 ms

www.gatech.edu.         60      IN      CNAME   tlweb.gtm.gatech.edu.
```

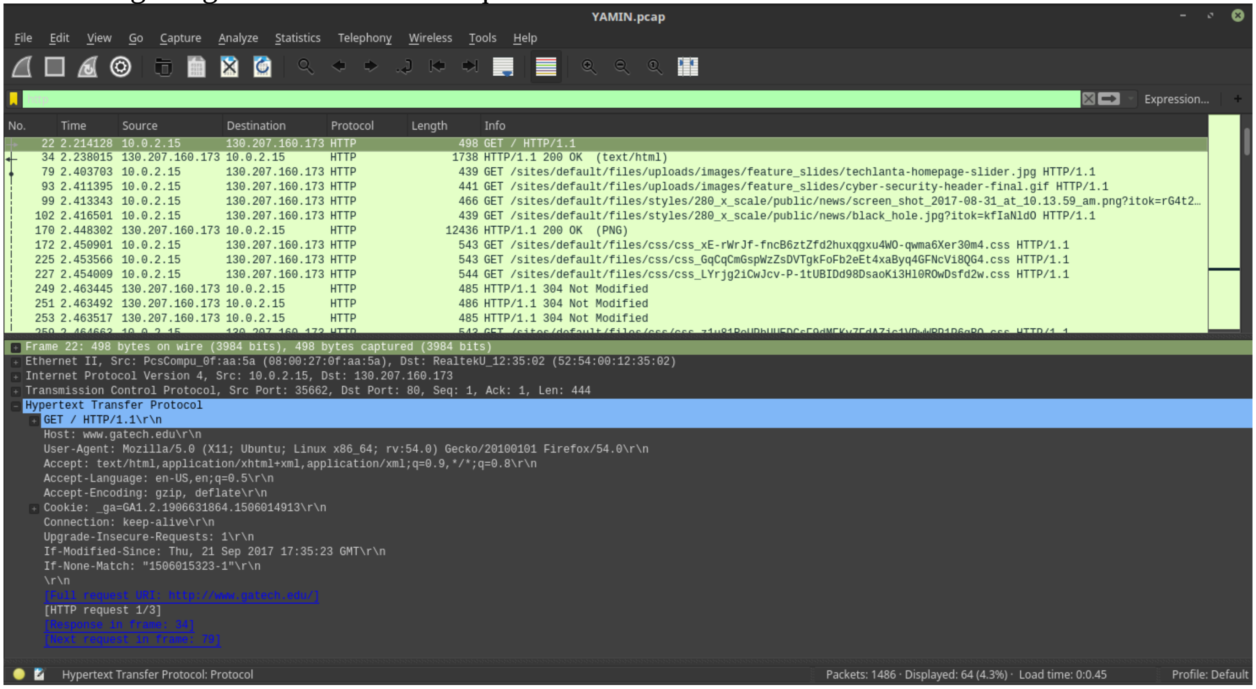
The IP address for www.gatech.edu is 130.204.244.165. www.gatech.edu points to tlweb.gtm.gatech.edu and is modified through the CNAME record.

If I `dig` www.gatech.edu, I might get a different IP address because they load balance (multiple servers and IPs) the top level web.

16 2.209513 128.61.244.254 10.0.2.15 DNS 200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.tgatech.edu A 130.207.244.165 NS gtm-dns-rich.gatech.edu NS gtm-dns-bcdc.gatech.edu A 130.207.160.47 A 130.207.165.192

Step 3: HTTP Request

The following image is a HTTP GET request.

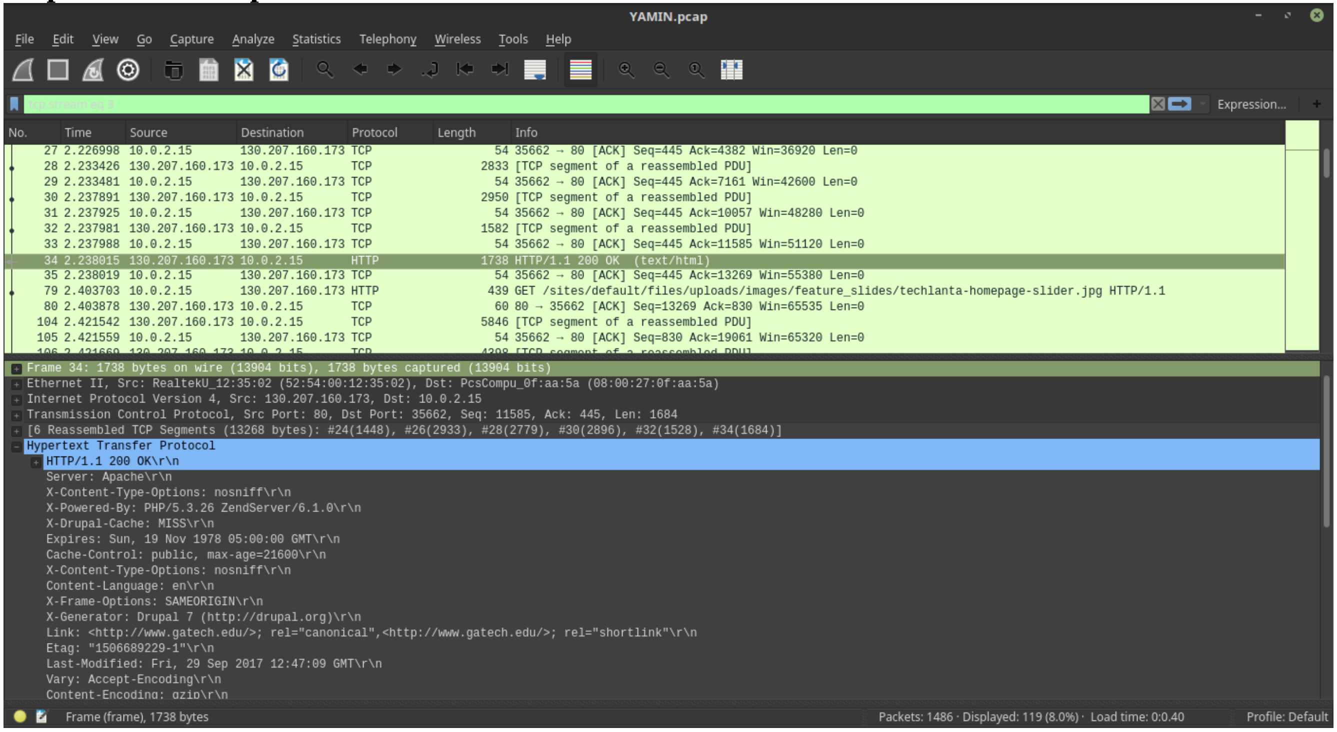

YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.  Time     Source          Destination     Protocol Length Info
  22 2.214128 10.0.2.15       130.207.160.173 HTTP      498 GET / HTTP/1.1
  34 2.238015 130.207.160.173 10.0.2.15       HTTP     1738 HTTP/1.1 200 OK  (text/html)
  79 2.403703 10.0.2.15       130.207.160.173 HTTP      439 GET /sites/default/files/uploads/images/feature_slides/techlanta-homepage-slider.jpg HTTP/1.1
  93 2.411395 10.0.2.15       130.207.160.173 HTTP      441 GET /sites/default/files/uploads/images/feature_slides/cyber-security-header-final.gif HTTP/1.1
  99 2.413343 10.0.2.15       130.207.160.173 HTTP      466 GET /sites/default/files/styles/280_x_scale/public/news/screen_shot_2017-08-31_at_10.13.59_am.png?itok=rG4t2…
 102 2.416501 10.0.2.15       130.207.160.173 HTTP      439 GET /sites/default/files/styles/280_x_scale/public/news/black_hole.jpg?itok=kfIaNldO HTTP/1.1
 170 2.448302 130.207.160.173 10.0.2.15       HTTP    12436 HTTP/1.1 200 OK  (PNG)
 172 2.450901 10.0.2.15       130.207.160.173 HTTP      543 GET /sites/default/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu4WO-qwma6Xer30m4.css HTTP/1.1
 225 2.453566 10.0.2.15       130.207.160.173 HTTP      543 GET /sites/default/files/css/css_GqCqCmGspWzZsDVTgkFoFb2eEt4xaByq4GFNcVi8QG4.css HTTP/1.1
 227 2.454009 10.0.2.15       130.207.160.173 HTTP      544 GET /sites/default/files/css/css_LYrjg2iCwJcv-P-1tUBIDd98DsaoKi3Hl0ROwDsfd2w.css HTTP/1.1
 249 2.463445 130.207.160.173 10.0.2.15       HTTP      485 HTTP/1.1 304 Not Modified
 251 2.463492 130.207.160.173 10.0.2.15       HTTP      486 HTTP/1.1 304 Not Modified
 253 2.463517 130.207.160.173 10.0.2.15       HTTP      485 HTTP/1.1 304 Not Modified
```

```
Frame 22: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits)
Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.207.160.173
Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: www.gatech.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Cookie: _ga=GA1.2.1906631864.1506014913\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  If-Modified-Since: Thu, 21 Sep 2017 17:35:23 GMT\r\n
  If-None-Match: "1506015323-1"\r\n
  \r\n
  [Full request URI: http://www.gatech.edu/]
  [HTTP request 1/3]
  [Response in frame: 34]
  [Next request in frame: 79]
```

```
Hypertext Transfer Protocol: Protocol          Packets: 1486 · Displayed: 64 (4.3%) · Load time: 0:0.45          Profile: Default
```

Step 4: HTTP Response

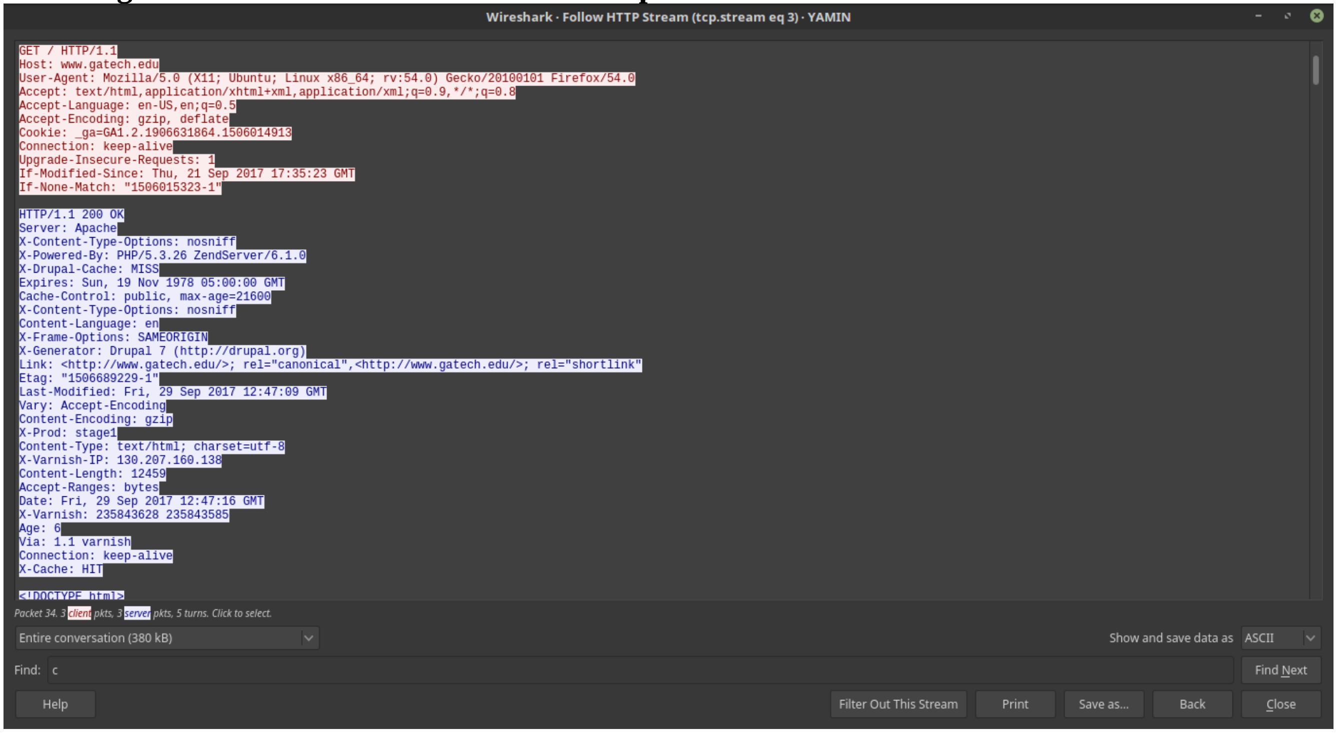

YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 3
Expression...

```
No.  Time     Source          Destination     Protocol Length Info
  27 2.226998 10.0.2.15       130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=445 Ack=4382 Win=36920 Len=0
  28 2.233426 130.207.160.173 10.0.2.15       TCP      2833 [TCP segment of a reassembled PDU]
  29 2.233481 10.0.2.15       130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=445 Ack=7161 Win=42600 Len=0
  30 2.237891 130.207.160.173 10.0.2.15       TCP      2950 [TCP segment of a reassembled PDU]
  31 2.237925 10.0.2.15       130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=445 Ack=10057 Win=48280 Len=0
  32 2.237981 130.207.160.173 10.0.2.15       TCP      1582 [TCP segment of a reassembled PDU]
  33 2.237988 10.0.2.15       130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=445 Ack=11585 Win=51120 Len=0
  34 2.238015 130.207.160.173 10.0.2.15       HTTP     1738 HTTP/1.1 200 OK  (text/html)
  35 2.238019 10.0.2.15       130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=445 Ack=13269 Win=55380 Len=0
  79 2.403703 10.0.2.15       130.207.160.173 HTTP      439 GET /sites/default/files/uploads/images/feature_slides/techlanta-homepage-slider.jpg HTTP/1.1
  80 2.403878 130.207.160.173 10.0.2.15       TCP        60 80 → 35662 [ACK] Seq=13269 Ack=830 Win=65535 Len=0
 104 2.421542 130.207.160.173 10.0.2.15       TCP      5846 [TCP segment of a reassembled PDU]
 105 2.421559 10.0.2.15       130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=830 Ack=19061 Win=65320 Len=0
```

```
Frame 34: 1738 bytes on wire (13904 bits), 1738 bytes captured (13904 bits)
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
Internet Protocol Version 4, Src: 130.207.160.173, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 35662, Seq: 11585, Ack: 445, Len: 1684
[6 Reassembled TCP Segments (13268 bytes): #24(1448), #26(2933), #28(2779), #30(2896), #32(1528), #34(1684)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Server: Apache\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Powered-By: PHP/5.3.26 ZendServer/6.1.0\r\n
  X-Drupal-Cache: MISS\r\n
  Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
  Cache-Control: public, max-age=21600\r\n
  X-Content-Type-Options: nosniff\r\n
  Content-Language: en\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  X-Generator: Drupal 7 (http://drupal.org)\r\n
  Link: <http://www.gatech.edu/>; rel="canonical",<http://www.gatech.edu/>; rel="shortlink"\r\n
  Etag: "1506689229-1"\r\n
  Last-Modified: Fri, 29 Sep 2017 12:47:09 GMT\r\n
  Vary: Accept-Encoding\r\n
  Content-Encoding: gzip\r\n
```

```
Frame (frame), 1738 bytes          Packets: 1486 · Displayed: 119 (8.0%) · Load time: 0:0.40          Profile: Default
```

The image below show the GET and HTTP responses in one window. Follow HTTP Stream



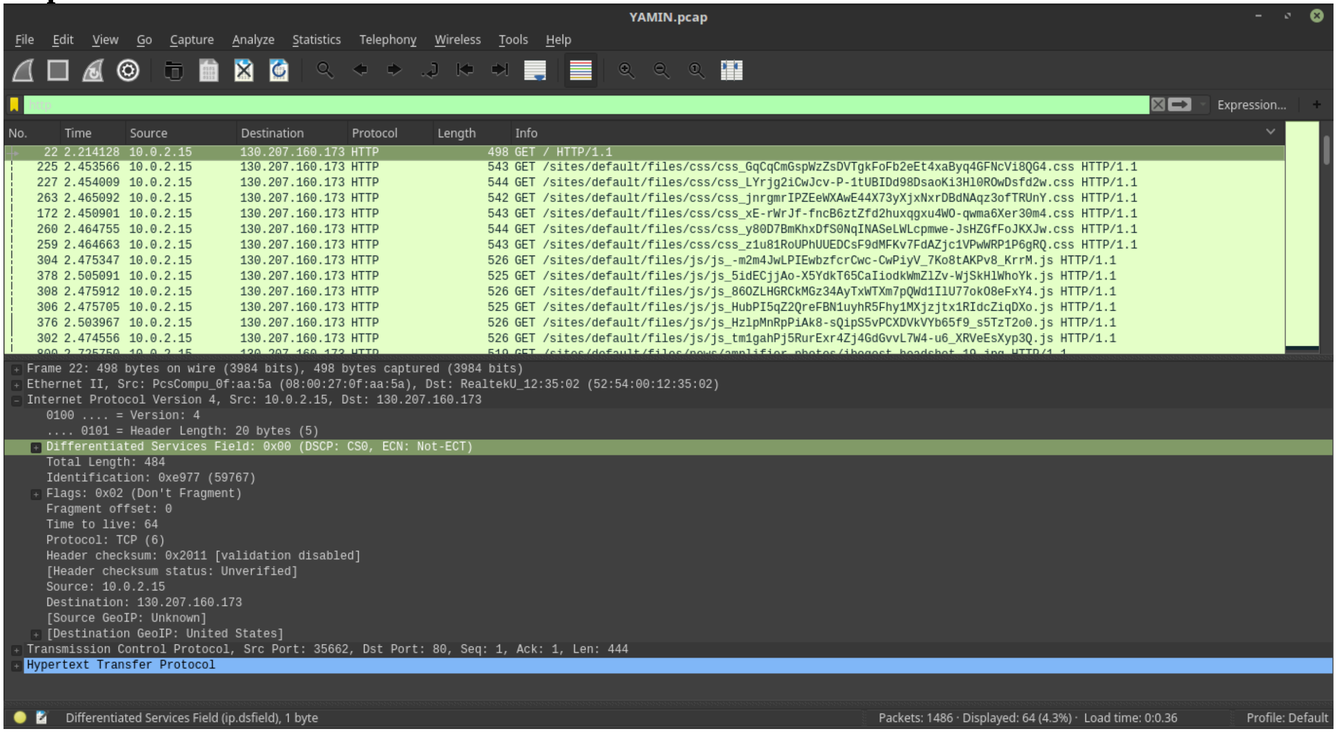
```
GET / HTTP/1.1
Host: www.gatech.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.2.1906631864.1506014913
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 21 Sep 2017 17:35:23 GMT
If-None-Match: "1506015323-1"

HTTP/1.1 200 OK
Server: Apache
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.3.26 ZendServer/6.1.0
X-Drupal-Cache: MISS
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: public, max-age=21600
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-Generator: Drupal 7 (http://drupal.org)
Link: <http://www.gatech.edu/>; rel="canonical",<http://www.gatech.edu/>; rel="shortlink"
Etag: "1506689229-1"
Last-Modified: Fri, 29 Sep 2017 12:47:09 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
X-Prod: stage1
Content-Type: text/html; charset=utf-8
X-Varnish-IP: 130.207.160.138
Content-Length: 12459
Accept-Ranges: bytes
Date: Fri, 29 Sep 2017 12:47:16 GMT
X-Varnish: 235843628 235843585
Age: 6
Via: 1.1 varnish
Connection: keep-alive
X-Cache: HIT

<!DOCTYPE html>
```

Packet 34. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (380 kB)

Find: c

Step 5: IP Packet



Filter: http

```
No.   Time     Source       Destination     Protocol  Length  Info
   22 2.214128 10.0.2.15    130.207.160.173 HTTP      498 GET / HTTP/1.1
  225 2.453566 10.0.2.15    130.207.160.173 HTTP      543 GET /sites/default/files/css/css_GqCqCmGspWzZsDVTgkFoFb2eEt4xaByq4GFNcVi8QG4.css HTTP/1.1
  227 2.454009 10.0.2.15    130.207.160.173 HTTP      544 GET /sites/default/files/css/css_LYrjg2iCwJcv-P-1tUBIDd98DsaoKi3Hl0ROwDsfd2w.css HTTP/1.1
  263 2.465092 10.0.2.15    130.207.160.173 HTTP      542 GET /sites/default/files/css/css_jnrgmrIPZEeWXAwE44X73yXjxNxrDBdNAqz3ofTRUnY.css HTTP/1.1
  172 2.450901 10.0.2.15    130.207.160.173 HTTP      543 GET /sites/default/files/css/css_xE-rWrJf-fncB6ztZfd2huxqgxu4WO-qwma6Xer30m4.css HTTP/1.1
  260 2.464755 10.0.2.15    130.207.160.173 HTTP      544 GET /sites/default/files/css/css_y80D7BmKhxDfS0NqINASeLWLcpmwe-JsHZGfFoJKXJw.css HTTP/1.1
  259 2.464663 10.0.2.15    130.207.160.173 HTTP      543 GET /sites/default/files/css/css_z1u81RoUPhUUEDCsF9dMFKv7FdAZjc1VPwWRP1P6gRQ.css HTTP/1.1
  304 2.475347 10.0.2.15    130.207.160.173 HTTP      526 GET /sites/default/files/js/js_-m2m4JwLPIEwbzfcrCwc-CwPiyV_7Ko8tAKPv8_KrrM.js HTTP/1.1
  378 2.505091 10.0.2.15    130.207.160.173 HTTP      525 GET /sites/default/files/js/js_5idECjjAo-X5YdkT65CaIiodkWmZlZv-WjSkHlWhoYk.js HTTP/1.1
  308 2.475912 10.0.2.15    130.207.160.173 HTTP      526 GET /sites/default/files/js/js_86OZLHGRCkMGz34AyTxWTXm7pQWd1IlU77okO8eFxY4.js HTTP/1.1
  306 2.475705 10.0.2.15    130.207.160.173 HTTP      525 GET /sites/default/files/js/js_HubPI5qZ2QreFBN1uyhR5Fhy1MXjzjtx1RIdcZiqDXo.js HTTP/1.1
  376 2.503967 10.0.2.15    130.207.160.173 HTTP      526 GET /sites/default/files/js/js_HzlpMnRpPiAk8-sQipS5vPCXDVkVYb65f9_s5TzT2o0.js HTTP/1.1
  302 2.474556 10.0.2.15    130.207.160.173 HTTP      526 GET /sites/default/files/js/js_tm1gahPj5RurExr4Zj4GdGvvL7W4-u6_XRVeEsXyp3Q.js HTTP/1.1
  800 2.725750 10.0.2.15    130.207.160.173 HTTP      519 GET /sites/default/files/news/amplifier_photos/ibogost_headshot_10.jpg HTTP/1.1
```

```
+ Frame 22: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits)
+ Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.207.160.173
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  + Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 484
    Identification: 0xe977 (59767)
  + Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x2011 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 130.207.160.173
    [Source GeoIP: Unknown]
  + [Destination GeoIP: United States]
+ Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
+ Hypertext Transfer Protocol
```

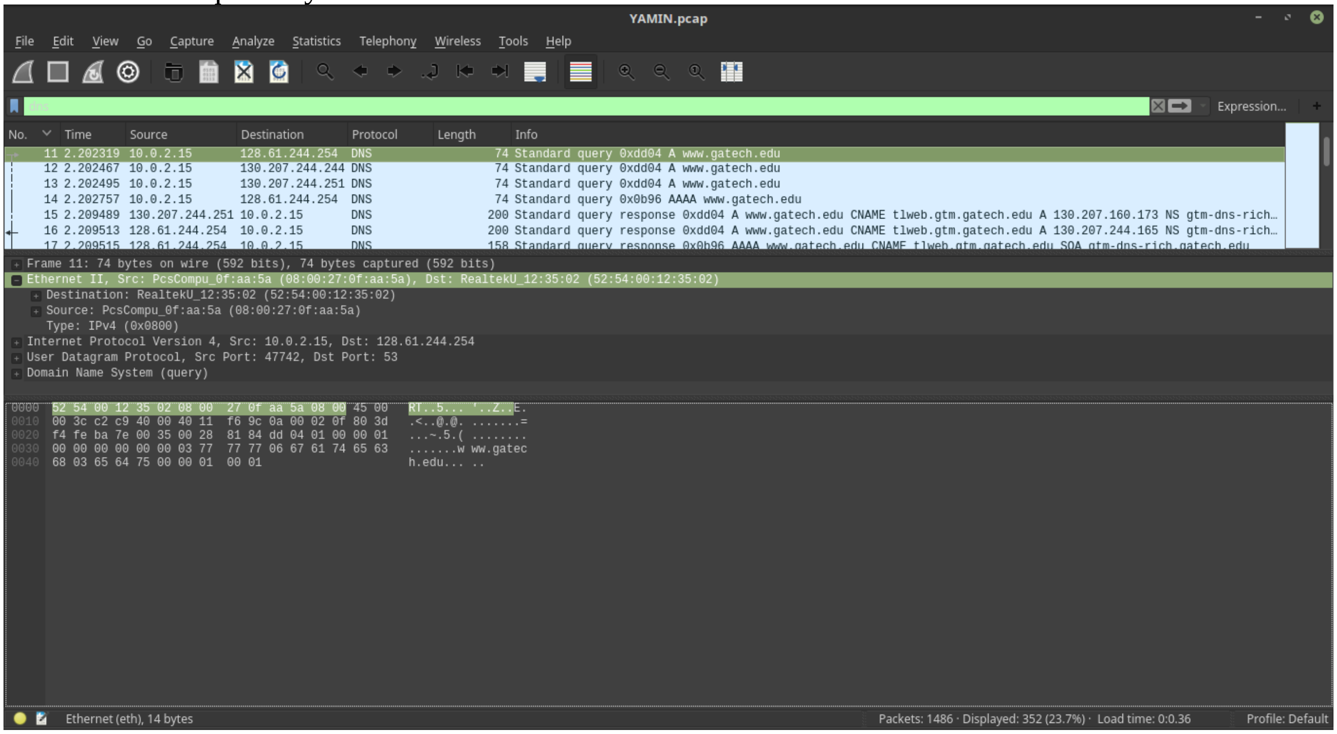
Differentiated Services Field (ip.dsfield), 1 byte

Packets: 1486 · Displayed: 64 (4.3%) · Load time: 0:0.36

Profile: Default

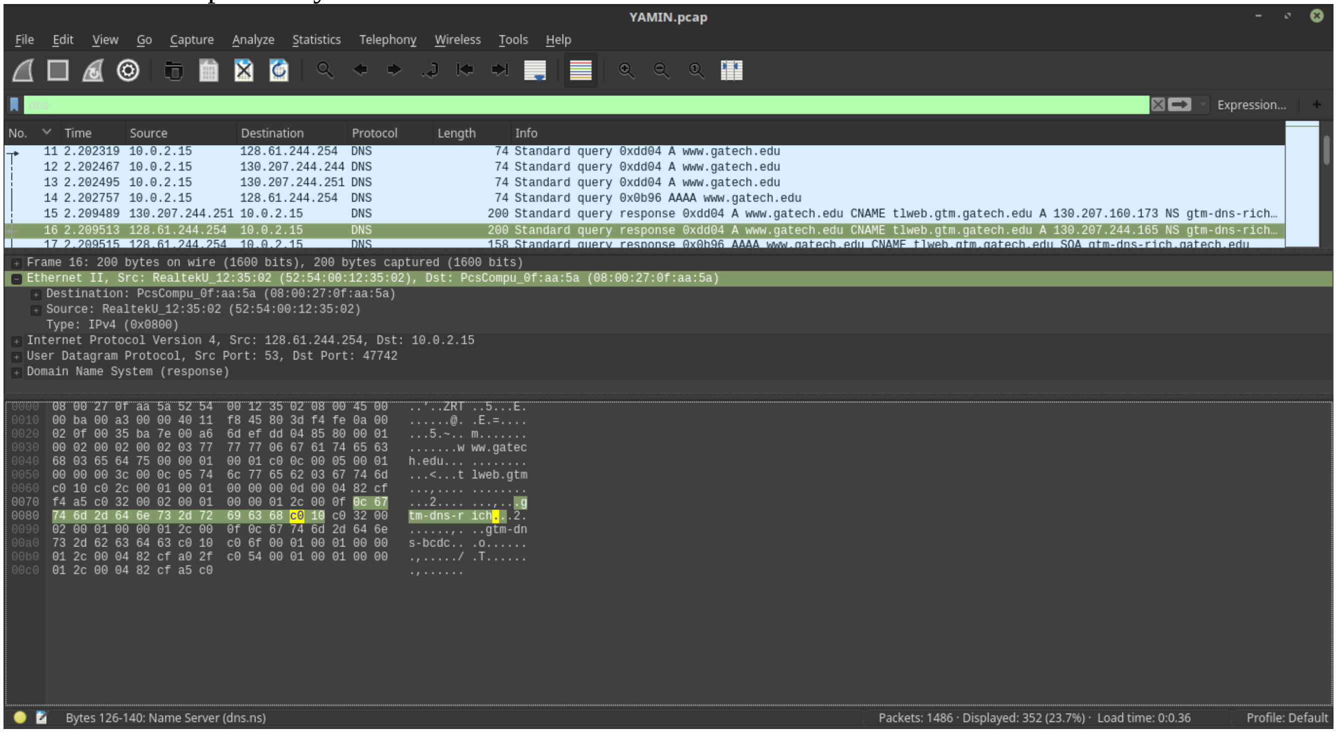
Step 6: Layer 2 up until it leaves the home network

This is DNS Request layer 2


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
Ethernet (eth), 14 bytes
Packets: 1486 · Displayed: 352 (23.7%) · Load time: 0:0.36
Profile: Default

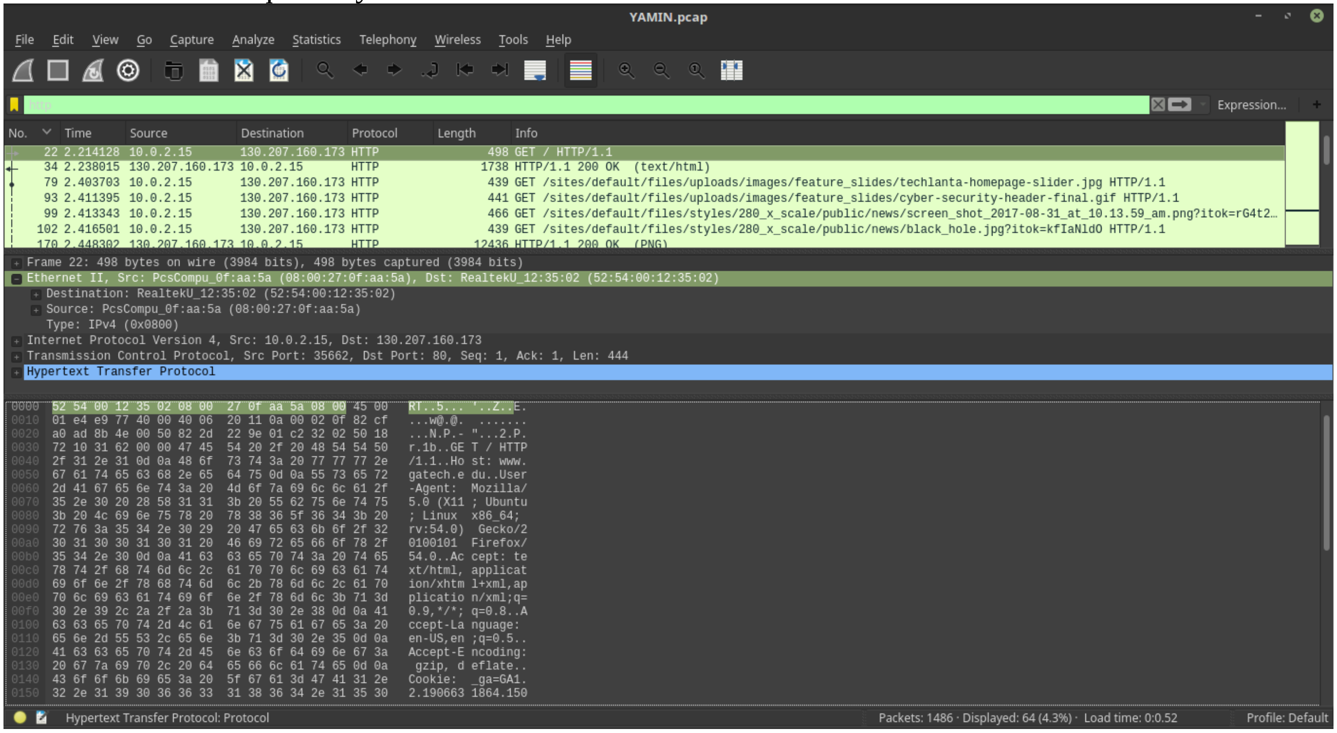
```
No.   Time     Source          Destination     Protocol  Length  Info
   11 2.202319 10.0.2.15       128.61.244.254  DNS           74 Standard query 0xdd04 A www.gatech.edu
   12 2.202467 10.0.2.15       130.207.244.244 DNS           74 Standard query 0xdd04 A www.gatech.edu
   13 2.202495 10.0.2.15       130.207.244.251 DNS           74 Standard query 0xdd04 A www.gatech.edu
   14 2.202757 10.0.2.15       128.61.244.254  DNS           74 Standard query 0x0b96 AAAA www.gatech.edu
   15 2.209489 130.207.244.251 10.0.2.15       DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.160.173 NS gtm-dns-rich…
   16 2.209513 128.61.244.254  10.0.2.15       DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
   17 2.209515 128.61.244.254  10.0.2.15       DNS          158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu

+ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
    + Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
    + Source: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
      Type: IPv4 (0x0800)
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.61.244.254
+ User Datagram Protocol, Src Port: 47742, Dst Port: 53
+ Domain Name System (query)

0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  00 3c c2 c9 40 00 40 11  f6 9c 0a 00 02 0f 80 3d   .<..@.@. .......=
0020  f4 fe ba 7e 00 35 00 28  81 84 dd 04 01 00 00 01   ...~.5.( ........
0030  00 00 00 00 00 00 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01                     h.edu... ..
```

This is DNS response layer 2


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
Bytes 126-140: Name Server (dns.ns)
Packets: 1486 · Displayed: 352 (23.7%) · Load time: 0:0.36
Profile: Default

```
No.   Time     Source          Destination     Protocol  Length  Info
   11 2.202319 10.0.2.15       128.61.244.254  DNS           74 Standard query 0xdd04 A www.gatech.edu
   12 2.202467 10.0.2.15       130.207.244.244 DNS           74 Standard query 0xdd04 A www.gatech.edu
   13 2.202495 10.0.2.15       130.207.244.251 DNS           74 Standard query 0xdd04 A www.gatech.edu
   14 2.202757 10.0.2.15       128.61.244.254  DNS           74 Standard query 0x0b96 AAAA www.gatech.edu
   15 2.209489 130.207.244.251 10.0.2.15       DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.160.173 NS gtm-dns-rich…
   16 2.209513 128.61.244.254  10.0.2.15       DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
   17 2.209515 128.61.244.254  10.0.2.15       DNS          158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu

+ Frame 16: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
- Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
    + Destination: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
    + Source: RealtekU_12:35:02 (52:54:00:12:35:02)
      Type: IPv4 (0x0800)
+ Internet Protocol Version 4, Src: 128.61.244.254, Dst: 10.0.2.15
+ User Datagram Protocol, Src Port: 53, Dst Port: 47742
+ Domain Name System (response)

0000  08 00 27 0f aa 5a 52 54  00 12 35 02 08 00 45 00   ..'..ZRT ..5...E.
0010  00 ba 00 a3 00 00 40 11  f8 45 80 3d f4 fe 0a 00   ......@. .E.=....
0020  02 0f 00 35 ba 7e 00 a6  6d ef dd 04 85 80 00 01   ...5.~.. m.......
0030  00 02 00 02 00 02 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01 c0 0c 00 05 00 01   h.edu... ........
0050  00 00 00 3c 00 0c 05 74  6c 77 65 62 03 67 74 6d   ...<...t lweb.gtm
0060  c0 10 c0 2c 00 01 00 01  00 00 00 0d 00 04 82 cf   ...,.... ........
0070  f4 a5 c0 32 00 02 00 01  00 00 01 2c 00 0f 0c 67   ...2.... ...,...g
0080  74 6d 2d 64 6e 73 2d 72  69 63 68 c0 10 c0 32 00   tm-dns-r ich...2.
0090  02 00 01 00 00 01 2c 00  0f 0c 67 74 6d 2d 64 6e   ......,. ..gtm-dn
00a0  73 2d 62 63 64 63 c0 10  c0 6f 00 01 00 01 00 00   s-bcdc.. .o......
00b0  01 2c 00 04 82 cf a0 2f  c0 54 00 01 00 01 00 00   .,...../ .T......
00c0  01 2c 00 04 82 cf a5 c0                            .,......
```

This is the HTTP request layer 2



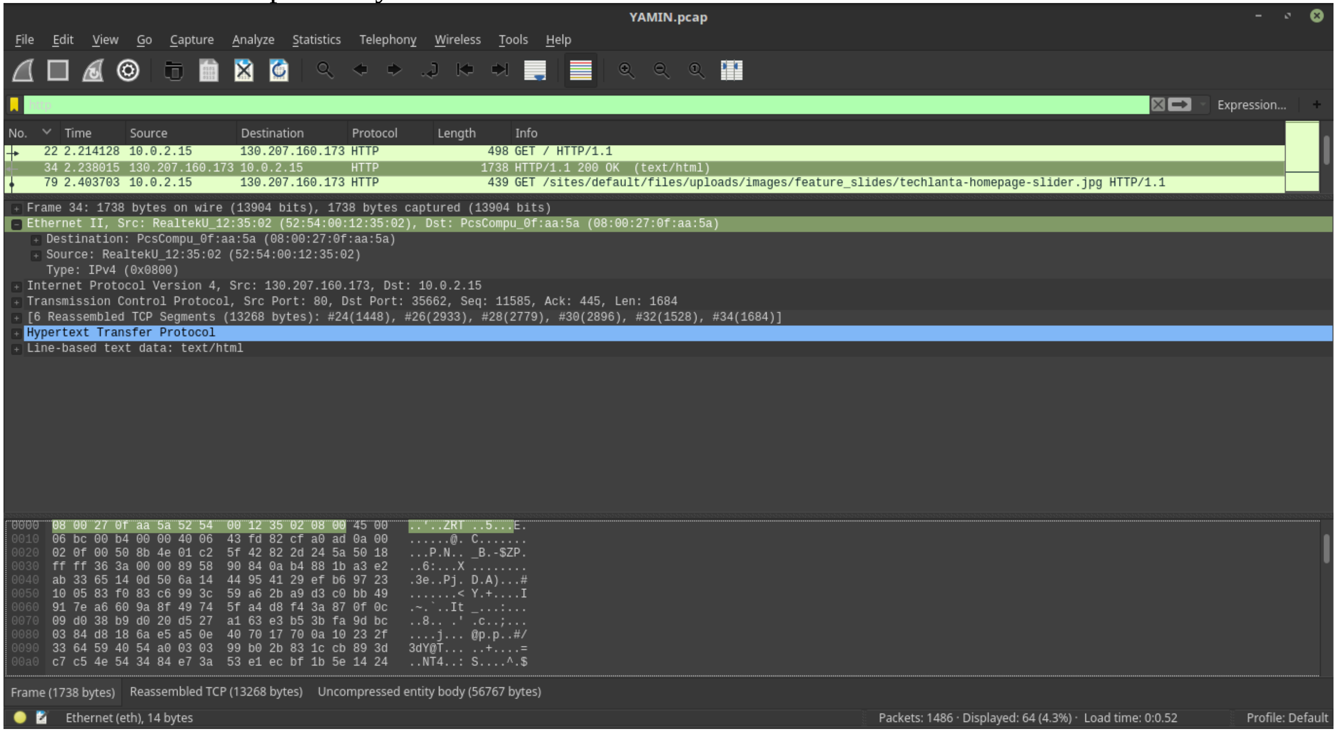
```
No.    Time      Source          Destination     Protocol  Length  Info
 22 2.214128 10.0.2.15       130.207.160.173 HTTP          498 GET / HTTP/1.1
 34 2.238015 130.207.160.173 10.0.2.15       HTTP         1738 HTTP/1.1 200 OK  (text/html)
 79 2.403703 10.0.2.15       130.207.160.173 HTTP          439 GET /sites/default/files/uploads/images/feature_slides/techlanta-homepage-slider.jpg HTTP/1.1
 93 2.411395 10.0.2.15       130.207.160.173 HTTP          441 GET /sites/default/files/uploads/images/feature_slides/cyber-security-header-final.gif HTTP/1.1
 99 2.413343 10.0.2.15       130.207.160.173 HTTP          466 GET /sites/default/files/styles/280_x_scale/public/news/screen_shot_2017-08-31_at_10.13.59_am.png?itok=rG4t2…
102 2.416501 10.0.2.15       130.207.160.173 HTTP          439 GET /sites/default/files/styles/280_x_scale/public/news/black_hole.jpg?itok=kfIaNldO HTTP/1.1
170 2.448302 130.207.160.173 10.0.2.15       HTTP        12436 HTTP/1.1 200 OK  (PNG)
```

```
+ Frame 22: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits)
- Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
    + Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
    + Source: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
      Type: IPv4 (0x0800)
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.207.160.173
+ Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
+ Hypertext Transfer Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  01 e4 e9 77 40 00 40 06  20 11 0a 00 02 0f 82 cf   ...w@.@.  .......
0020  a0 ad 8b 4e 00 50 82 2d  22 9e 01 c2 32 02 50 18   ...N.P.- "...2.P.
0030  72 10 31 62 00 00 47 45  54 20 2f 20 48 54 54 50   r.1b..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 61 74 65 63 68 2e 65  64 75 0d 0a 55 73 65 72   gatech.e du..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X11 ; Ubuntu
0080  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
0090  72 76 3a 35 34 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:54.0)  Gecko/2
00a0  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
00b0  35 34 2e 30 0d 0a 41 63  63 65 70 74 3a 20 74 65   54.0..Ac cept: te
00c0  78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74   xt/html, applicat
00d0  69 6f 6e 2f 78 68 74 6d  6c 2b 78 6d 6c 2c 61 70   ion/xhtm l+xml,ap
00e0  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 3b 71 3d   plicatio n/xml;q=
00f0  30 2e 39 2c 2a 2f 2a 3b  71 3d 30 2e 38 0d 0a 41   0.9,*/*; q=0.8..A
0100  63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20   ccept-La nguage:
0110  65 6e 2d 55 53 2c 65 6e  3b 71 3d 30 2e 35 0d 0a   en-US,en ;q=0.5..
0120  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
0130  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate..
0140  43 6f 6f 6b 69 65 3a 20  5f 67 61 3d 47 41 31 2e   Cookie:  _ga=GA1.
0150  32 2e 31 39 30 36 36 33  31 38 36 34 2e 31 35 30   2.190663 1864.150
```

Hypertext Transfer Protocol: Protocol   Packets: 1486 · Displayed: 64 (4.3%) · Load time: 0:0.52   Profile: Default

This is the HTTP response layer 2



```
No.    Time      Source          Destination     Protocol  Length  Info
 22 2.214128 10.0.2.15       130.207.160.173 HTTP          498 GET / HTTP/1.1
 34 2.238015 130.207.160.173 10.0.2.15       HTTP         1738 HTTP/1.1 200 OK  (text/html)
 79 2.403703 10.0.2.15       130.207.160.173 HTTP          439 GET /sites/default/files/uploads/images/feature_slides/techlanta-homepage-slider.jpg HTTP/1.1
```

```
+ Frame 34: 1738 bytes on wire (13904 bits), 1738 bytes captured (13904 bits)
- Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
    + Destination: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
    + Source: RealtekU_12:35:02 (52:54:00:12:35:02)
      Type: IPv4 (0x0800)
+ Internet Protocol Version 4, Src: 130.207.160.173, Dst: 10.0.2.15
+ Transmission Control Protocol, Src Port: 80, Dst Port: 35662, Seq: 11585, Ack: 445, Len: 1684
+ [6 Reassembled TCP Segments (13268 bytes): #24(1448), #26(2933), #28(2779), #30(2896), #32(1528), #34(1684)]
+ Hypertext Transfer Protocol
+ Line-based text data: text/html
```

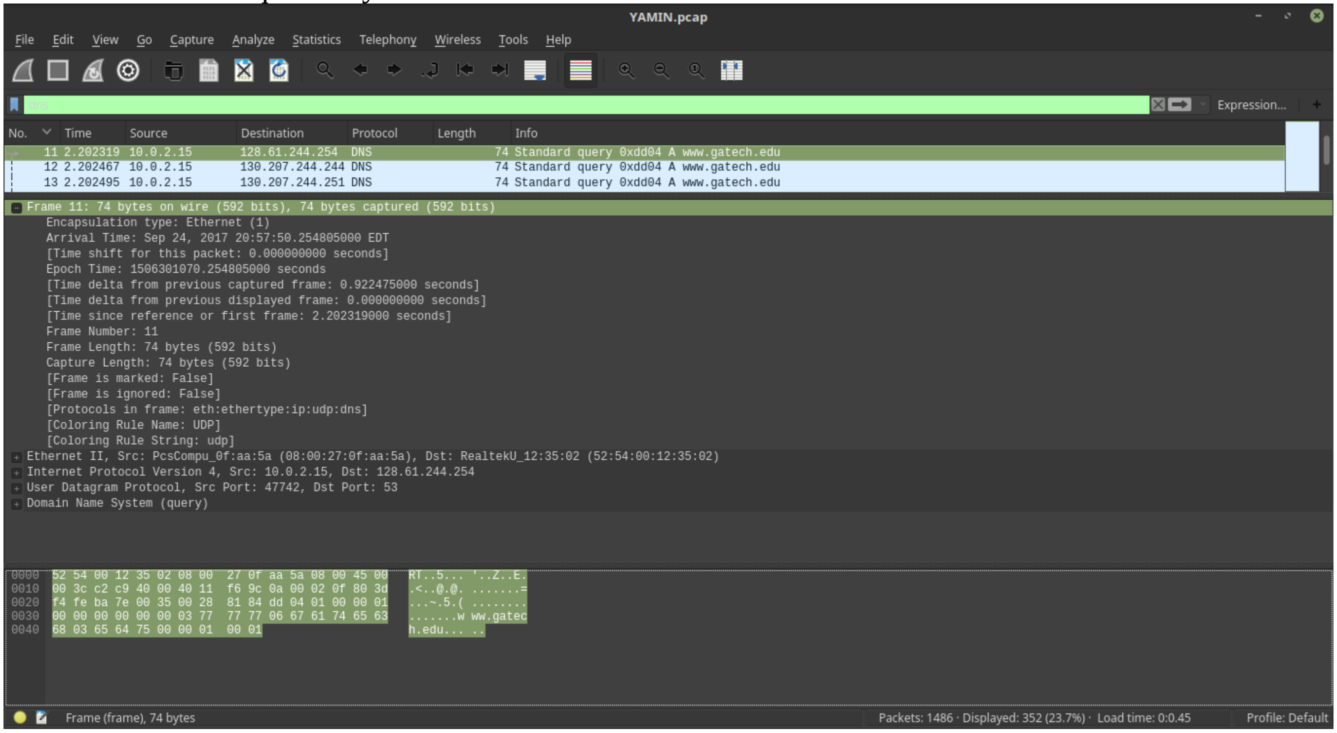
```
0000  08 00 27 0f aa 5a 52 54  00 12 35 02 08 00 45 00   ..'..ZRT ..5...E.
0010  06 bc 00 b4 00 00 40 06  43 fd 82 cf a0 ad 0a 00   ......@. C.......
0020  02 0f 00 50 8b 4e 01 c2  5f 42 82 2d 24 5a 50 18   ...P.N.. _B.-$ZP.
0030  ff ff 36 3a 00 00 89 58  90 84 0a b4 88 1b a3 e2   ..6:...X ........
0040  ab 33 65 14 0d 50 6a 14  44 95 41 29 ef b6 97 23   .3e..Pj. D.A)...#
0050  10 05 83 f0 83 c6 99 3c  59 a6 2b a9 d3 c0 bb 49   .......< Y.+....I
0060  91 7e a6 60 9a 8f 49 74  5f a4 d8 f4 3a 87 0f 0c   .~.`..It _...:...
0070  09 d0 38 b9 d0 20 d5 27  a1 63 e3 b5 3b fa 9d bc   ..8.. .' .c..;...
0080  03 84 d8 18 6a e5 a5 0e  40 70 17 70 0a 10 23 2f   ....j... @p.p..#/
0090  33 64 59 40 54 a0 03 03  99 b0 2b 83 1c cb 89 3d   3dY@T... ..+....=
00a0  c7 c5 4e 54 34 84 e7 3a  53 e1 ec bf 1b 5e 14 24   ..NT4..: S....^.$
```

Frame (1738 bytes)   Reassembled TCP (13268 bytes)   Uncompressed entity body (56767 bytes)

Ethernet (eth), 14 bytes   Packets: 1486 · Displayed: 64 (4.3%) · Load time: 0:0.52   Profile: Default

Step 7: Layer 1 up until it leaves the home network

This is the DNS Request Layer 1


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
+

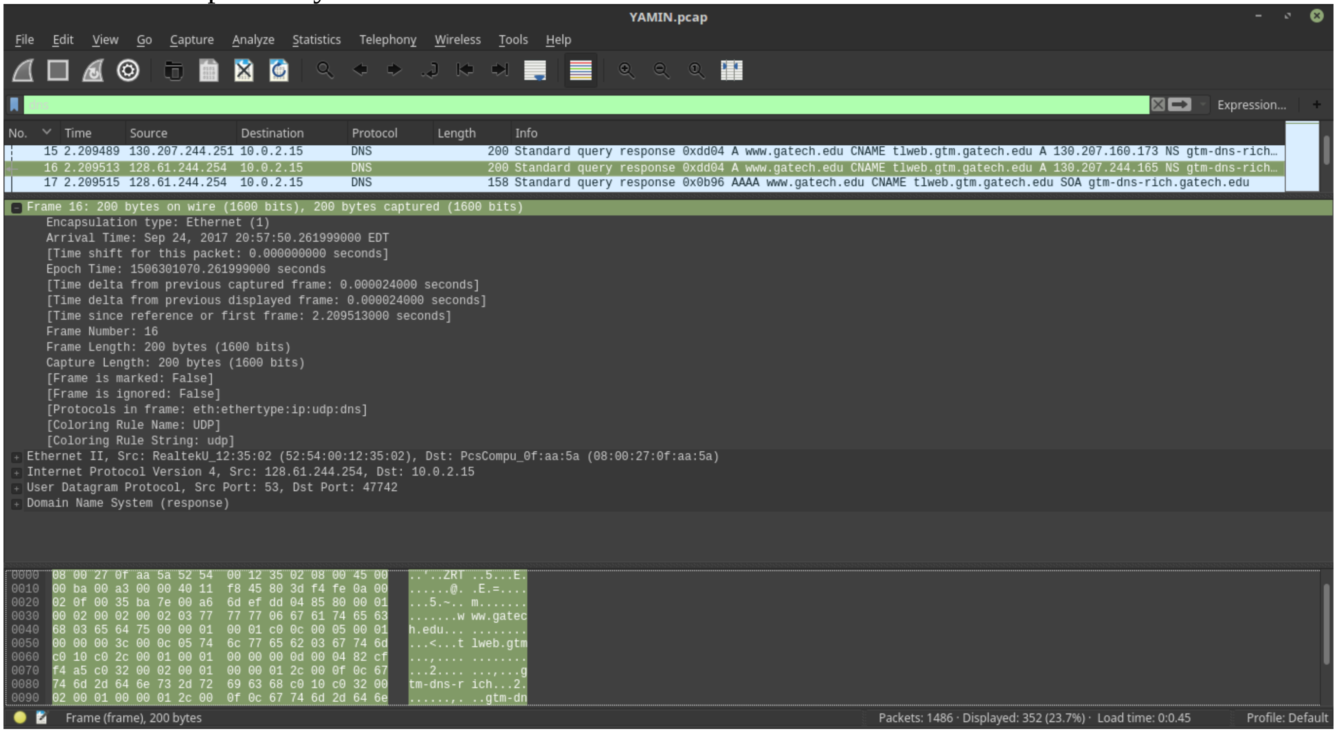
```
No.    Time     Source      Destination     Protocol  Length  Info
    11 2.202319 10.0.2.15   128.61.244.254  DNS          74 Standard query 0xdd04 A www.gatech.edu
    12 2.202467 10.0.2.15   130.207.244.244 DNS          74 Standard query 0xdd04 A www.gatech.edu
    13 2.202495 10.0.2.15   130.207.244.251 DNS          74 Standard query 0xdd04 A www.gatech.edu
```

```
Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 24, 2017 20:57:50.254805000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1506301070.254805000 seconds
    [Time delta from previous captured frame: 0.922475000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.202319000 seconds]
    Frame Number: 11
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.61.244.254
User Datagram Protocol, Src Port: 47742, Dst Port: 53
Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  00 3c c2 c9 40 00 40 11  f6 9c 0a 00 02 0f 80 3d   .<..@.@. .......=
0020  f4 fe ba 7e 00 35 00 28  81 84 dd 04 01 00 00 01   ...~.5.( ........
0030  00 00 00 00 00 00 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01                     h.edu... ..
```

Frame (frame), 74 bytes — Packets: 1486 · Displayed: 352 (23.7%) · Load time: 0:0.45 — Profile: Default

This is DNS response layer 1


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
+

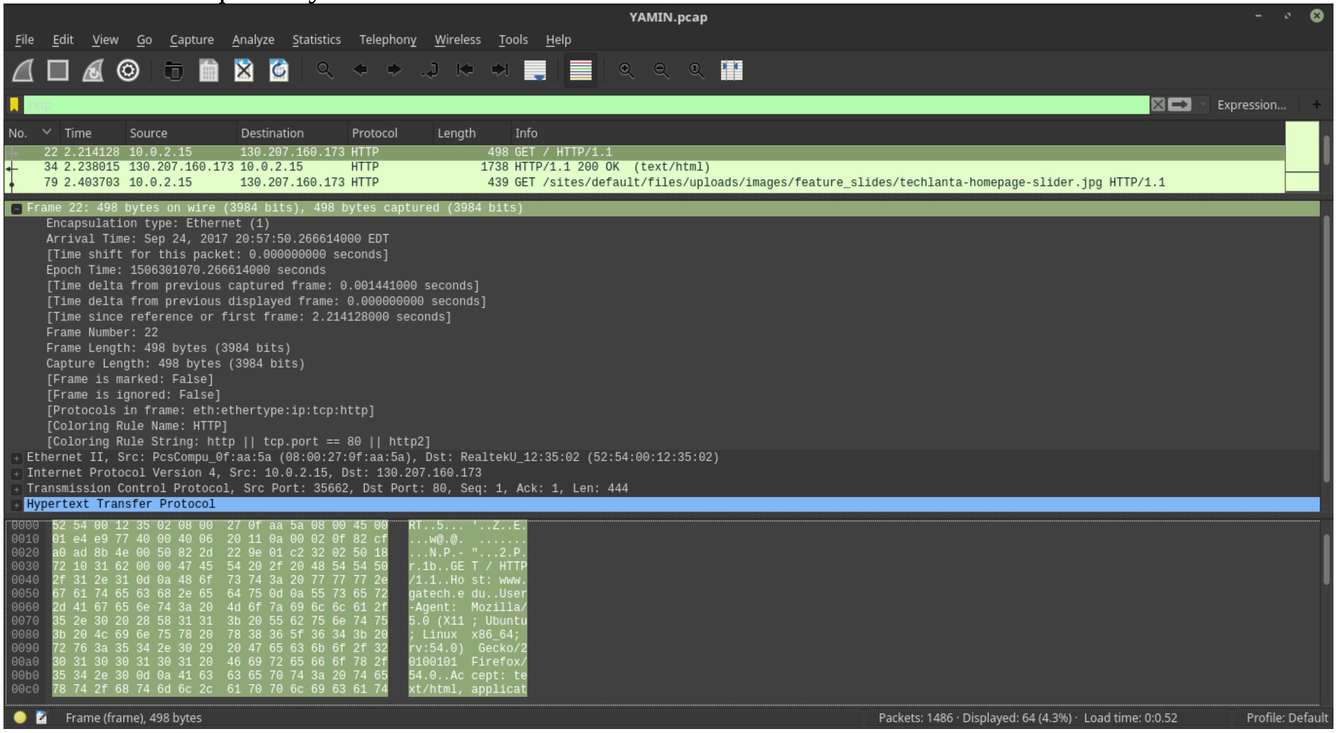
```
No.    Time     Source          Destination  Protocol  Length  Info
    15 2.209489 130.207.244.251 10.0.2.15    DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.160.173 NS gtm-dns-rich…
    16 2.209513 128.61.244.254  10.0.2.15    DNS          200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
    17 2.209515 128.61.244.254  10.0.2.15    DNS          158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu
```

```
Frame 16: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 24, 2017 20:57:50.261999000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1506301070.261999000 seconds
    [Time delta from previous captured frame: 0.000024000 seconds]
    [Time delta from previous displayed frame: 0.000024000 seconds]
    [Time since reference or first frame: 2.209513000 seconds]
    Frame Number: 16
    Frame Length: 200 bytes (1600 bits)
    Capture Length: 200 bytes (1600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
Internet Protocol Version 4, Src: 128.61.244.254, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 47742
Domain Name System (response)
```

```
0000  08 00 27 0f aa 5a 52 54  00 12 35 02 08 00 45 00   ..'..ZRT ..5...E.
0010  00 ba 00 a3 00 00 40 11  f8 45 80 3d f4 fe 0a 00   ......@. .E.=....
0020  02 0f 00 35 ba 7e 00 a6  6d ef dd 04 85 80 00 01   ...5.~.. m.......
0030  00 02 00 02 00 02 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01 c0 0c 00 05 00 01   h.edu... ........
0050  00 00 00 3c 00 0c 05 74  6c 77 65 62 03 67 74 6d   ...<...t lweb.gtm
0060  c0 10 c0 2c 00 01 00 01  00 00 00 0d 00 04 82 cf   ...,.... ........
0070  f4 a5 c0 32 00 02 00 01  00 00 01 2c 00 0f 0c 67   ...2.... ...,...g
0080  74 6d 2d 64 6e 73 2d 72  69 63 68 c0 10 c0 32 00   tm-dns-r ich...2.
0090  02 00 01 00 00 01 2c 00  0f 0c 67 74 6d 2d 64 6e   ......,. ..gtm-dn
```

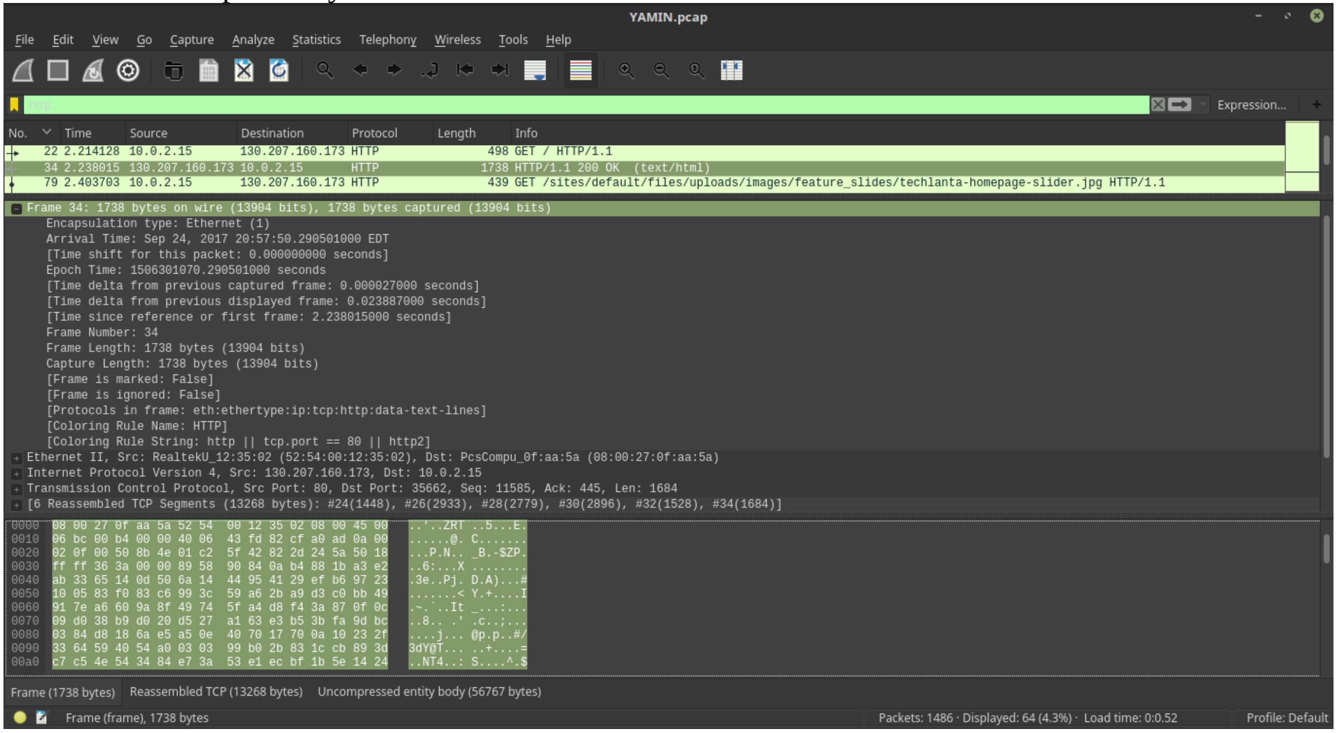
Frame (frame), 200 bytes — Packets: 1486 · Displayed: 352 (23.7%) · Load time: 0:0.45 — Profile: Default

This is HTTP request layer 1


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.    Time     Source          Destination     Protocol  Length  Info
   22 2.214128 10.0.2.15       130.207.160.173 HTTP        498 GET / HTTP/1.1
   34 2.238015 130.207.160.173 10.0.2.15       HTTP       1738 HTTP/1.1 200 OK  (text/html)
   79 2.403703 10.0.2.15       130.207.160.173 HTTP        439 GET /sites/default/files/uploads/images/feature_slides/techlanta-homepage-slider.jpg HTTP/1.1

Frame 22: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 24, 2017 20:57:50.266614000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1506301070.266614000 seconds
    [Time delta from previous captured frame: 0.001441000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.214128000 seconds]
    Frame Number: 22
    Frame Length: 498 bytes (3984 bits)
    Capture Length: 498 bytes (3984 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.207.160.173
Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
Hypertext Transfer Protocol

0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  01 e4 e9 77 40 00 40 06  20 11 0a 00 02 0f 82 cf   ...w@.@.  .......
0020  a0 ad 8b 4e 00 50 82 2d  22 9e 01 c2 32 02 50 18   ...N.P.- "...2.P.
0030  72 10 31 62 00 00 47 45  54 20 2f 20 48 54 54 50   r.1b..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 61 74 65 63 68 2e 65  64 75 0d 0a 55 73 65 72   gatech.e du..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X11 ; Ubuntu
0080  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
0090  72 76 3a 35 34 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:54.0)  Gecko/2
00a0  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
00b0  35 34 2e 30 0d 0a 41 63  63 65 70 74 3a 20 74 65   54.0..Ac cept: te
00c0  78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74   xt/html, applicat

Frame (frame), 498 bytes          Packets: 1486 · Displayed: 64 (4.3%) · Load time: 0:0.52          Profile: Default
```

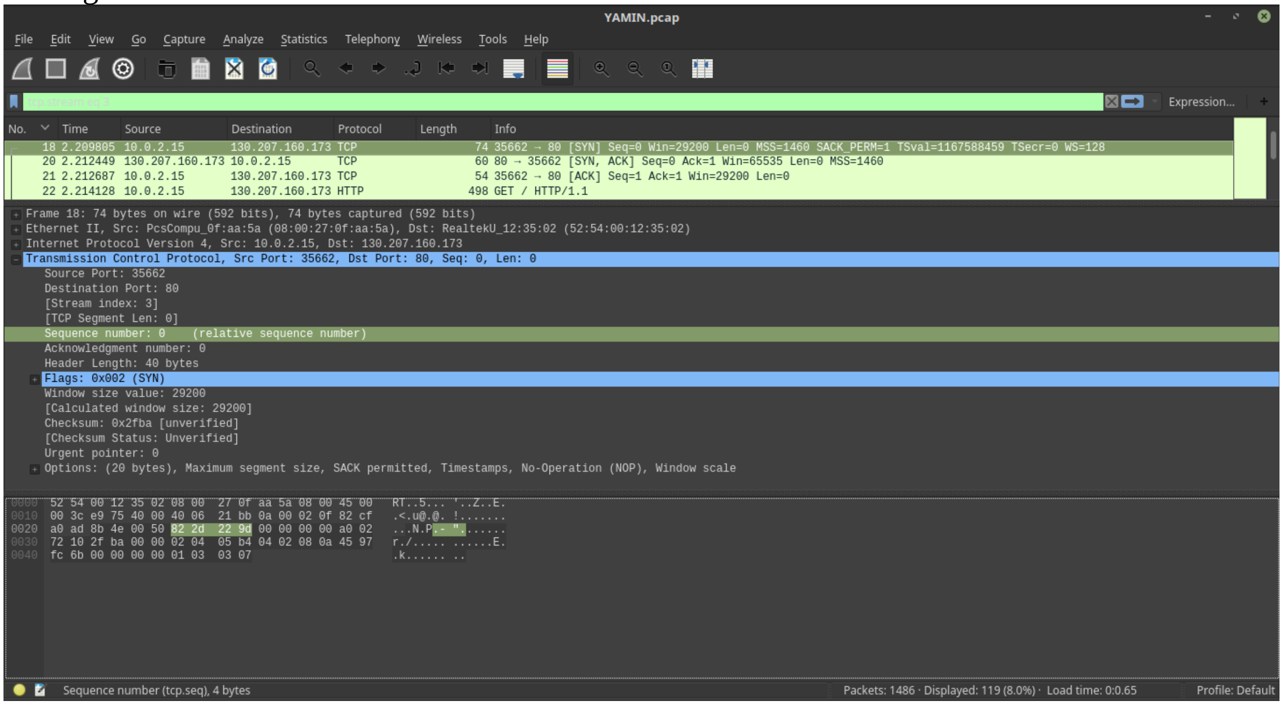
This is HTTP response layer 1


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.    Time     Source          Destination     Protocol  Length  Info
   22 2.214128 10.0.2.15       130.207.160.173 HTTP        498 GET / HTTP/1.1
   34 2.238015 130.207.160.173 10.0.2.15       HTTP       1738 HTTP/1.1 200 OK  (text/html)
   79 2.403703 10.0.2.15       130.207.160.173 HTTP        439 GET /sites/default/files/uploads/images/feature_slides/techlanta-homepage-slider.jpg HTTP/1.1

Frame 34: 1738 bytes on wire (13904 bits), 1738 bytes captured (13904 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 24, 2017 20:57:50.290501000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1506301070.290501000 seconds
    [Time delta from previous captured frame: 0.000027000 seconds]
    [Time delta from previous displayed frame: 0.023887000 seconds]
    [Time since reference or first frame: 2.238015000 seconds]
    Frame Number: 34
    Frame Length: 1738 bytes (13904 bits)
    Capture Length: 1738 bytes (13904 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
Internet Protocol Version 4, Src: 130.207.160.173, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 35662, Seq: 11585, Ack: 445, Len: 1684
[6 Reassembled TCP Segments (13268 bytes): #24(1448), #26(2933), #28(2779), #30(2896), #32(1528), #34(1684)]

0000  08 00 27 0f aa 5a 52 54  00 12 35 02 08 00 45 00   ..'..ZRT ..5...E.
0010  06 bc 00 b4 00 00 40 06  43 fd 82 cf a0 ad 0a 00   ......@. C.......
0020  02 0f 00 50 8b 4e 01 c2  5f 42 82 2d 24 5a 50 18   ...P.N.. _B.-$ZP.
0030  ff ff 36 3a 00 00 89 58  90 84 0a b4 88 1b a3 e2   ..6:...X ........
0040  ab 33 65 14 0d 50 6a 14  44 95 41 29 ef b6 97 23   .3e..Pj. D.A)...#
0050  10 05 83 f0 83 c6 99 3c  59 a6 2b a9 d3 c0 bb 49   .......< Y.+....I
0060  91 7e a6 60 9a 8f 49 74  5f a4 d8 f4 3a 87 0f 0c   .~.`..It _...:...
0070  09 d0 38 b9 d0 20 d5 27  a1 63 e3 b5 3b fa 9d bc   ..8.. .' .c..;...
0080  03 84 d8 18 6a e5 a5 0e  40 70 17 70 0a 10 23 2f   ....j... @p.p..#/
0090  33 64 59 40 54 a0 03 03  99 b0 2b 83 1c cb 89 3d   3dY@T... ..+....=
00a0  c7 c5 4e 54 34 84 e7 3a  53 e1 ec bf 1b 5e 14 24   ..NT4..: S....^.$

Frame (1738 bytes)   Reassembled TCP (13268 bytes)   Uncompressed entity body (56767 bytes)

Frame (frame), 1738 bytes          Packets: 1486 · Displayed: 64 (4.3%) · Load time: 0:0.52          Profile: Default
```

Step 8: TCP process for the HTTP session (multiple packets)

The image below shows the SYN sent from the client.



```
tcp.stream eq 3
```

```
No.  Time     Source         Destination    Protocol  Length  Info
  18 2.209805 10.0.2.15      130.207.160.173 TCP        74 35662 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1167588459 TSecr=0 WS=128
  20 2.212449 130.207.160.173 10.0.2.15      TCP        60 80 → 35662 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  21 2.212687 10.0.2.15      130.207.160.173 TCP        54 35662 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  22 2.214128 10.0.2.15      130.207.160.173 HTTP      498 GET / HTTP/1.1
```

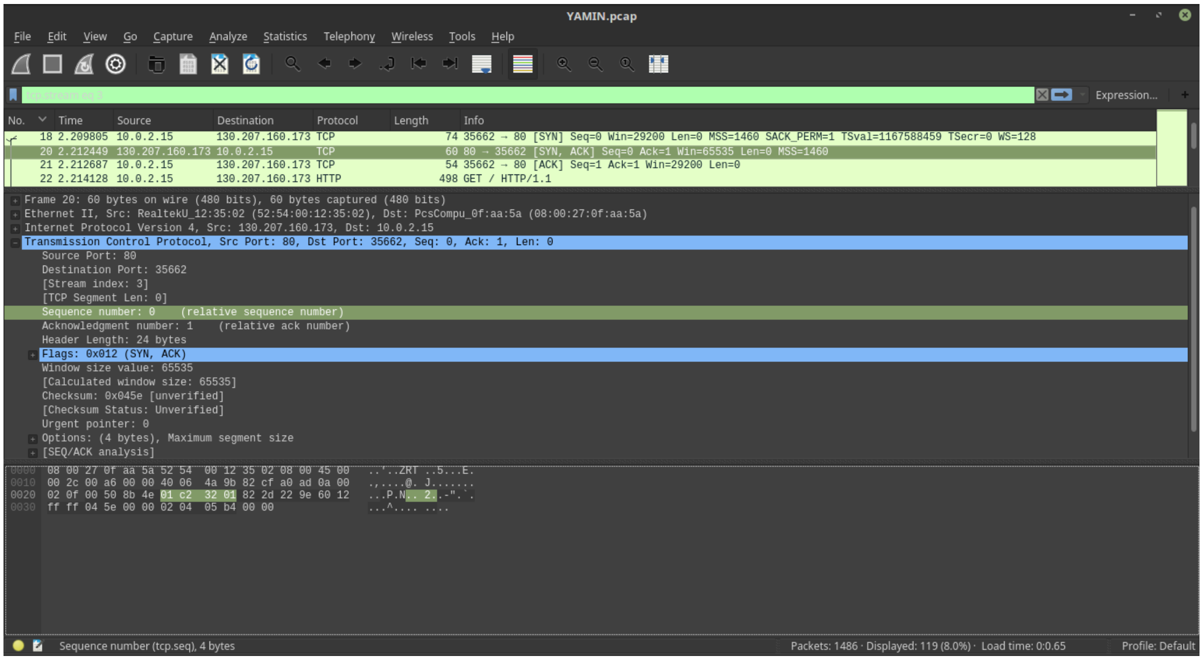
```
+ Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
+ Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.207.160.173
- Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 35662
    Destination Port: 80
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 40 bytes
  + Flags: 0x002 (SYN)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x2fba [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  + Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

```
0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  00 3c e9 75 40 00 40 06  21 bb 0a 00 02 0f 82 cf   .<.u@.@. !.......
0020  a0 ad 8b 4e 00 50 82 2d  22 9d 00 00 00 00 a0 02   ...N.P.- ".......
0030  72 10 2f ba 00 00 02 04  05 b4 04 02 08 0a 45 97   r./..... ......E.
0040  fc 6b 00 00 00 00 01 03  03 07                     .k...... ..
```

```
Sequence number (tcp.seq), 4 bytes        Packets: 1486 · Displayed: 119 (8.0%) · Load time: 0:0.65        Profile: Default
```

I took one screen shot for the TCP stream for the HTTP GET request. The three way handshake occurs with SYN, SYN-ACK, and ACK. The web server listens on the well-known port 80 (defined by the IANA) for the SYN first in which the sequence number is 0. The server acknowledges that the client has sent 1 btye to it and also sends a SYN to the client (thus the server sends SYN-ACK). The client then acknowledges (ACK) the SYN from the server (this SYN is part of the server’s SYN-ACK).

The image below shows the SYN-ACK from the server

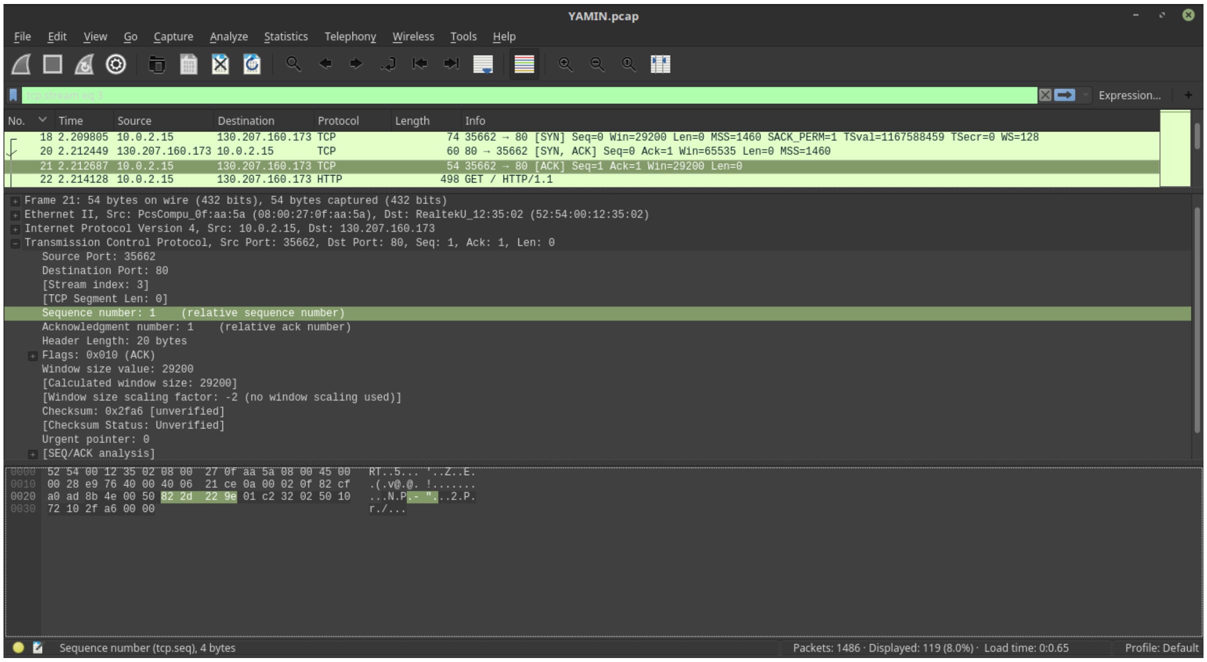

YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 3
Expression...
Sequence number (tcp.seq), 4 bytes
Packets: 1486 · Displayed: 119 (8.0%) · Load time: 0:0.65
Profile: Default

```
No.   Time     Source          Destination     Protocol  Length  Info
   18 2.209805 10.0.2.15       130.207.160.173 TCP           74 35662 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1167588459 TSecr=0 WS=128
   20 2.212449 130.207.160.173 10.0.2.15       TCP           60 80 → 35662 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   21 2.212687 10.0.2.15       130.207.160.173 TCP           54 35662 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
   22 2.214128 10.0.2.15       130.207.160.173 HTTP         498 GET / HTTP/1.1
```

```
+ Frame 20: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
+ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
+ Internet Protocol Version 4, Src: 130.207.160.173, Dst: 10.0.2.15
- Transmission Control Protocol, Src Port: 80, Dst Port: 35662, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 35662
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 24 bytes
  + Flags: 0x012 (SYN, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x045e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  + Options: (4 bytes), Maximum segment size
  + [SEQ/ACK analysis]
```

```
0000  08 00 27 0f aa 5a 52 54  00 12 35 02 08 00 45 00   ..'..ZRT ..5...E.
0010  00 2c 00 a6 00 00 40 06  4a 9b 82 cf a0 ad 0a 00   .,....@. J.......
0020  02 0f 00 50 8b 4e 01 c2  32 01 82 2d 22 9e 60 12   ...P.N.. 2..-".`.
0030  ff ff 04 5e 00 00 02 04  05 b4 00 00               ...^.... ....
```

The image below shows the ACK from the client


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 3
Expression...
Sequence number (tcp.seq), 4 bytes
Packets: 1486 · Displayed: 119 (8.0%) · Load time: 0:0.65
Profile: Default

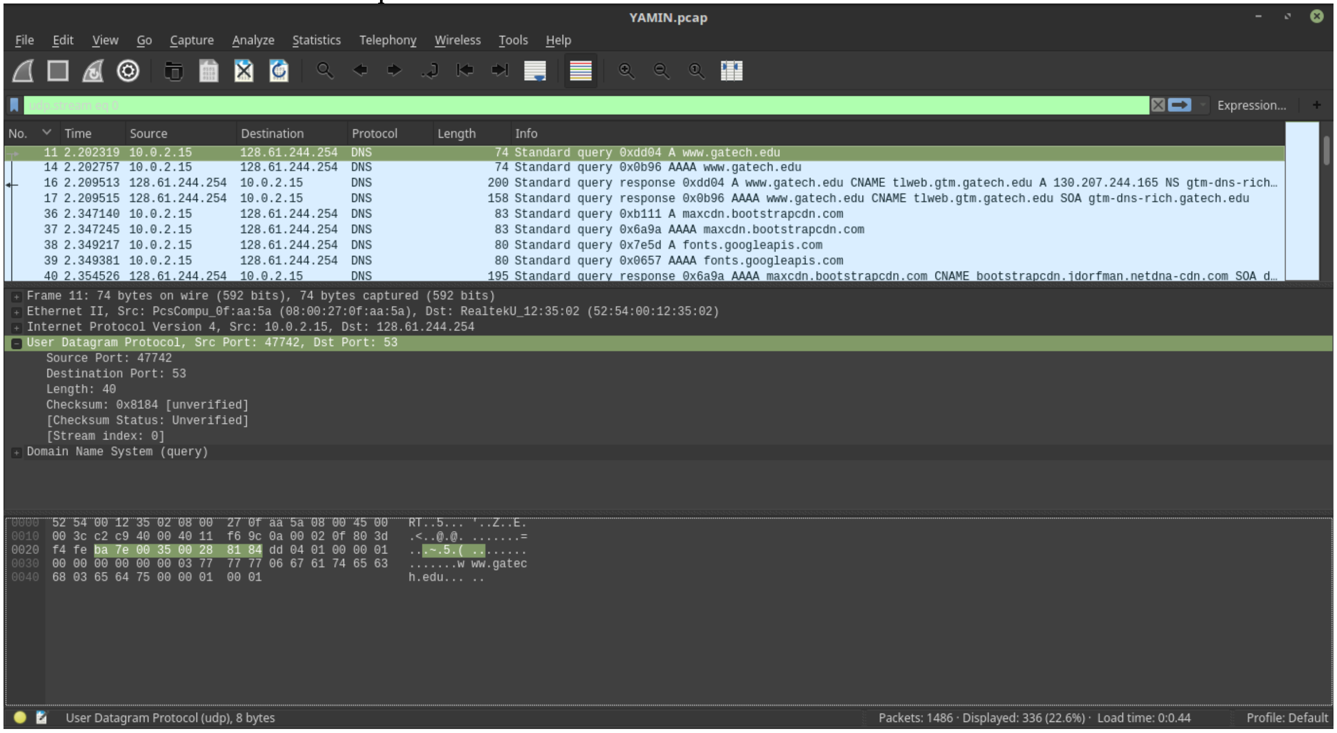
```
No.   Time     Source          Destination     Protocol  Length  Info
   18 2.209805 10.0.2.15       130.207.160.173 TCP           74 35662 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1167588459 TSecr=0 WS=128
   20 2.212449 130.207.160.173 10.0.2.15       TCP           60 80 → 35662 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   21 2.212687 10.0.2.15       130.207.160.173 TCP           54 35662 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
   22 2.214128 10.0.2.15       130.207.160.173 HTTP         498 GET / HTTP/1.1
```

```
+ Frame 21: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
+ Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.207.160.173
- Transmission Control Protocol, Src Port: 35662, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 35662
    Destination Port: 80
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  + Flags: 0x010 (ACK)
    Window size value: 29200
    [Calculated window size: 29200]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x2fa6 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  + [SEQ/ACK analysis]
```

```
0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  00 28 e9 76 40 00 40 06  21 ce 0a 00 02 0f 82 cf   .(.v@.@. !.......
0020  a0 ad 8b 4e 00 50 82 2d  22 9e 01 c2 32 02 50 10   ...N.P.- "...2.P.
0030  72 10 2f a6 00 00                                  r./...
```

Step 9: UDP Process for the DNS query and Response (multiple packets)

This is UDP for the DNS Request


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.stream eq 0

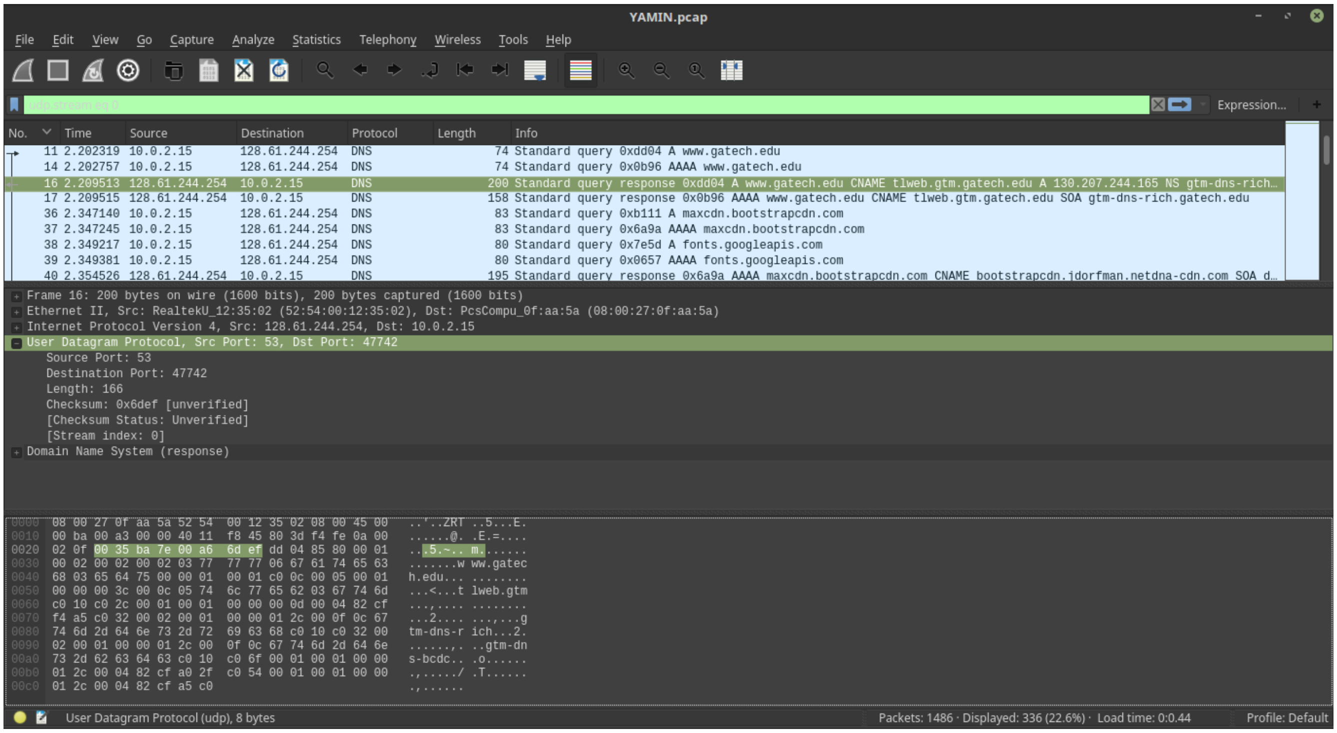
```
No.  Time     Source          Destination     Protocol Length Info
  11 2.202319 10.0.2.15       128.61.244.254  DNS        74 Standard query 0xdd04 A www.gatech.edu
  14 2.202757 10.0.2.15       128.61.244.254  DNS        74 Standard query 0x0b96 AAAA www.gatech.edu
  16 2.209513 128.61.244.254  10.0.2.15       DNS       200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
  17 2.209515 128.61.244.254  10.0.2.15       DNS       158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu
  36 2.347140 10.0.2.15       128.61.244.254  DNS        83 Standard query 0xb111 A maxcdn.bootstrapcdn.com
  37 2.347245 10.0.2.15       128.61.244.254  DNS        83 Standard query 0x6a9a AAAA maxcdn.bootstrapcdn.com
  38 2.349217 10.0.2.15       128.61.244.254  DNS        80 Standard query 0x7e5d A fonts.googleapis.com
  39 2.349381 10.0.2.15       128.61.244.254  DNS        80 Standard query 0x0657 AAAA fonts.googleapis.com
  40 2.354526 128.61.244.254  10.0.2.15       DNS       195 Standard query response 0x6a9a AAAA maxcdn.bootstrapcdn.com CNAME bootstrapcdn.jdorfman.netdna-cdn.com SOA d…
```

```
+ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
+ Ethernet II, Src: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
+ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.61.244.254
- User Datagram Protocol, Src Port: 47742, Dst Port: 53
    Source Port: 47742
    Destination Port: 53
    Length: 40
    Checksum: 0x8184 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
+ Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 0f aa 5a 08 00 45 00   RT..5... '..Z..E.
0010  00 3c c2 c9 40 00 40 11  f6 9c 0a 00 02 0f 80 3d   .<..@.@. .......=
0020  f4 fe ba 7e 00 35 00 28  81 84 dd 04 01 00 00 01   ...~.5.( ........
0030  00 00 00 00 00 00 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01                     h.edu... ..
```

User Datagram Protocol (udp), 8 bytes | Packets: 1486 · Displayed: 336 (22.6%) · Load time: 0:0.44 | Profile: Default

This is UDP for the DNS Response


YAMIN.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

udp.stream eq 0

```
No.  Time     Source          Destination     Protocol Length Info
  11 2.202319 10.0.2.15       128.61.244.254  DNS        74 Standard query 0xdd04 A www.gatech.edu
  14 2.202757 10.0.2.15       128.61.244.254  DNS        74 Standard query 0x0b96 AAAA www.gatech.edu
  16 2.209513 128.61.244.254  10.0.2.15       DNS       200 Standard query response 0xdd04 A www.gatech.edu CNAME tlweb.gtm.gatech.edu A 130.207.244.165 NS gtm-dns-rich…
  17 2.209515 128.61.244.254  10.0.2.15       DNS       158 Standard query response 0x0b96 AAAA www.gatech.edu CNAME tlweb.gtm.gatech.edu SOA gtm-dns-rich.gatech.edu
  36 2.347140 10.0.2.15       128.61.244.254  DNS        83 Standard query 0xb111 A maxcdn.bootstrapcdn.com
  37 2.347245 10.0.2.15       128.61.244.254  DNS        83 Standard query 0x6a9a AAAA maxcdn.bootstrapcdn.com
  38 2.349217 10.0.2.15       128.61.244.254  DNS        80 Standard query 0x7e5d A fonts.googleapis.com
  39 2.349381 10.0.2.15       128.61.244.254  DNS        80 Standard query 0x0657 AAAA fonts.googleapis.com
  40 2.354526 128.61.244.254  10.0.2.15       DNS       195 Standard query response 0x6a9a AAAA maxcdn.bootstrapcdn.com CNAME bootstrapcdn.jdorfman.netdna-cdn.com SOA d…
```

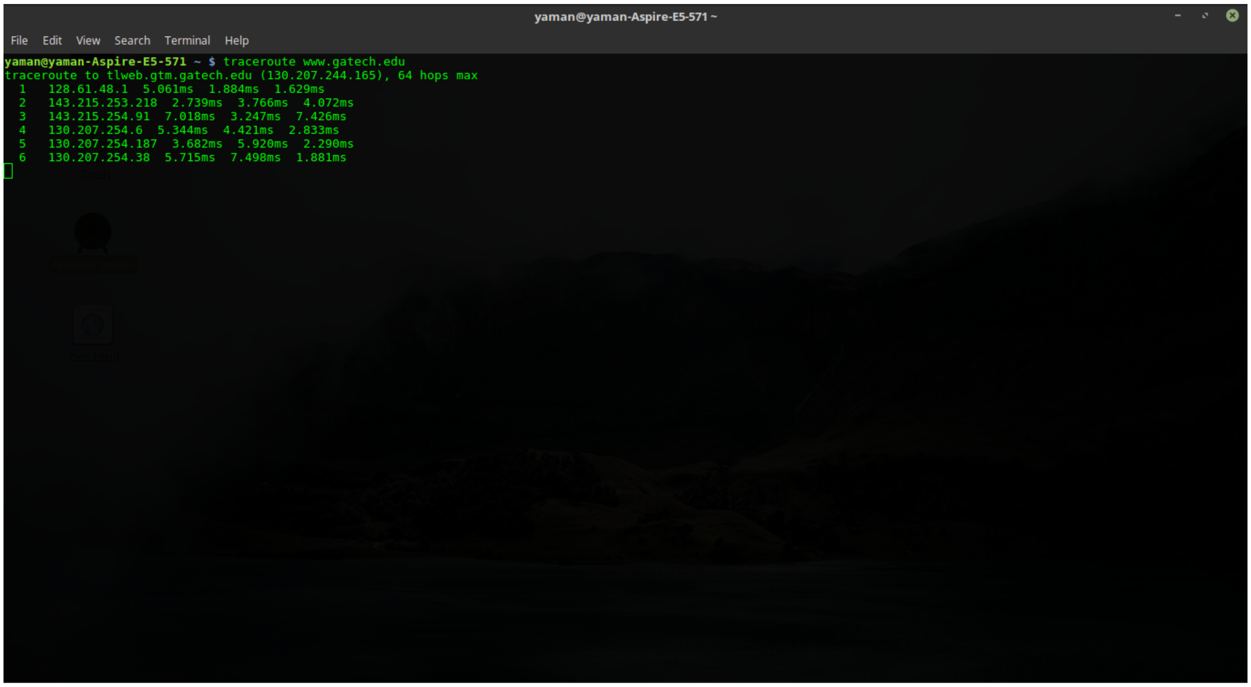
```
+ Frame 16: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
+ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_0f:aa:5a (08:00:27:0f:aa:5a)
+ Internet Protocol Version 4, Src: 128.61.244.254, Dst: 10.0.2.15
- User Datagram Protocol, Src Port: 53, Dst Port: 47742
    Source Port: 53
    Destination Port: 47742
    Length: 166
    Checksum: 0x6def [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
+ Domain Name System (response)
```

```
0000  08 00 27 0f aa 5a 52 54  00 12 35 02 08 00 45 00   ..'..ZRT ..5...E.
0010  00 ba 00 a3 00 00 40 11  f8 45 80 3d f4 fe 0a 00   ......@. .E.=....
0020  02 0f 00 35 ba 7e 00 a6  6d ef dd 04 85 80 00 01   ...5.~.. m.......
0030  00 02 00 02 00 02 03 77  77 77 06 67 61 74 65 63   .......w ww.gatec
0040  68 03 65 64 75 00 00 01  00 01 c0 0c 00 05 00 01   h.edu... ........
0050  00 00 00 3c 00 0c 05 74  6c 77 65 62 03 67 74 6d   ...<...t lweb.gtm
0060  c0 10 c0 2c 00 01 00 01  00 00 00 0d 00 04 82 cf   ...,.... ........
0070  f4 a5 c0 32 00 02 00 01  00 00 01 2c 00 0f 0c 67   ...2.... ...,...g
0080  74 6d 2d 64 6e 73 2d 72  69 63 68 c0 10 c0 32 00   tm-dns-r ich...2.
0090  02 00 01 00 00 01 2c 00  0f 0c 67 74 6d 2d 64 6e   ......,. ..gtm-dn
00a0  73 2d 62 63 64 63 c0 10  c0 6f 00 01 00 01 00 00   s-bcdc.. .o......
00b0  01 2c 00 04 82 cf a0 2f  c0 54 00 01 00 01 00 00   .,...../ .T......
00c0  01 2c 00 04 82 cf a5 c0                            .,......
```

User Datagram Protocol (udp), 8 bytes | Packets: 1486 · Displayed: 336 (22.6%) · Load time: 0:0.44 | Profile: Default

Step 10: How routers and switches are involved in the entire process

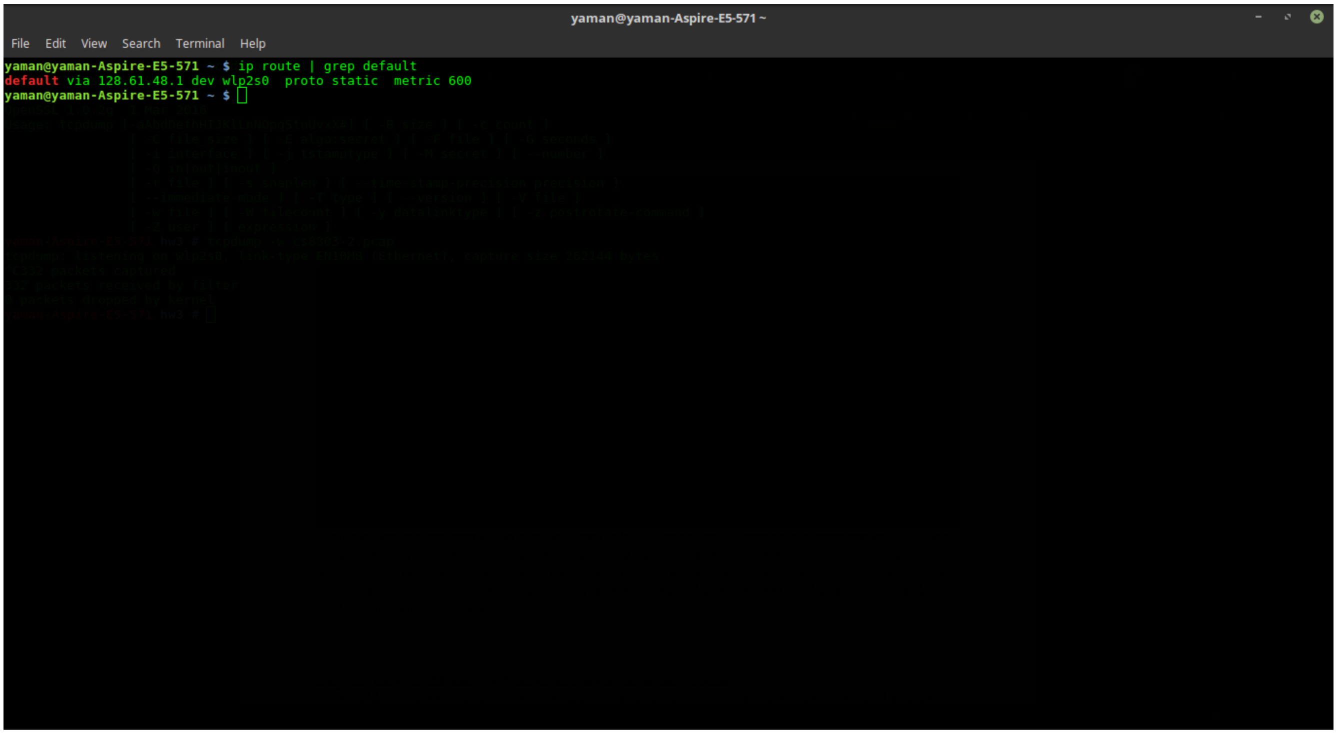
Routers are typically layer 3 (IP layer). We will assume you are on a local network, your router is configured with DHCP, and your device is assigned an IP address and default gateway. ARP then performs on the default gateway that you are assigned, and converts that to a MAC address. You are now able to connect to your router. Next, you perform DNS on the host name that you want to go to via the router. The router resolves the host name to an IP address. Your device then forms the HTTP packet with the source IP and destination IP and sends it to your router. I ran tracerroute to show how my router (default gateway) bounces off nodes when routing to www.gatech.edu (Uses Djiktras when routing). On a side note, stars represent a firewall blocking the tracerroute protocol.


yaman@yaman-Aspire-E5-571 ~
File Edit View Search Terminal Help

```
yaman@yaman-Aspire-E5-571 ~ $ traceroute www.gatech.edu
traceroute to tlweb.gtm.gatech.edu (130.207.244.165), 64 hops max
  1   128.61.48.1  5.061ms  1.884ms  1.629ms
  2   143.215.253.218  2.739ms  3.766ms  4.072ms
  3   143.215.254.91  7.018ms  3.247ms  7.426ms
  4   130.207.254.6  5.344ms  4.421ms  2.833ms
  5   130.207.254.187  3.682ms  5.920ms  2.290ms
  6   130.207.254.38  5.715ms  7.498ms  1.881ms
```

Multiple devices can connect to a switch (multiple Ethernets) and it connects to your router. Switches do not perform any routing (assuming we're only talking about layer 2 switches and not layer 3 or 4 switches, aka multilayer switches). Switches connect local devices only and if you're trying to connect to a server or device outside your subnet, then you'll have to use your router's default gateway. Switches use ARP to resolve MAC addresses on your subnet; that's how you're able to connect to local devices without using a router.

The image below shows my default gateway:



yaman@yaman-Aspire-E5-571 ~
File Edit View Search Terminal Help

```
yaman@yaman-Aspire-E5-571 ~ $ ip route | grep default
default via 128.61.48.1 dev wlp2s0  proto static  metric 600
yaman@yaman-Aspire-E5-571 ~ $ 
```

Step 11: How CAM and ARP tables are involved in the process

The CAM table resides on the switch and it maps a device’s MAC address to a particular port on the switch. You need to know this because when you’re trying to connect to a device and send it stuff (assuming both of you are connected to the switch), you need to know which port it’s connected to.

An ARP table stores IP address to MAC address mappings. ARP is a caching mechanism as well because when you resolve the device once, the mapping will be stored in the ARP cache for much faster fetching. ARP commands are operating system agnostic (e.g., arp -a).

You can run `arp -a` to view your ARP cache.

You can run `ifconfig -a` to view your IP address and MAC address for whatever interface you’re on.

Terminology: MAC address, physical address, hardware address, and burndown address are synonymous. It’s a quasi-unique identifier for your machine on a particular network interface.

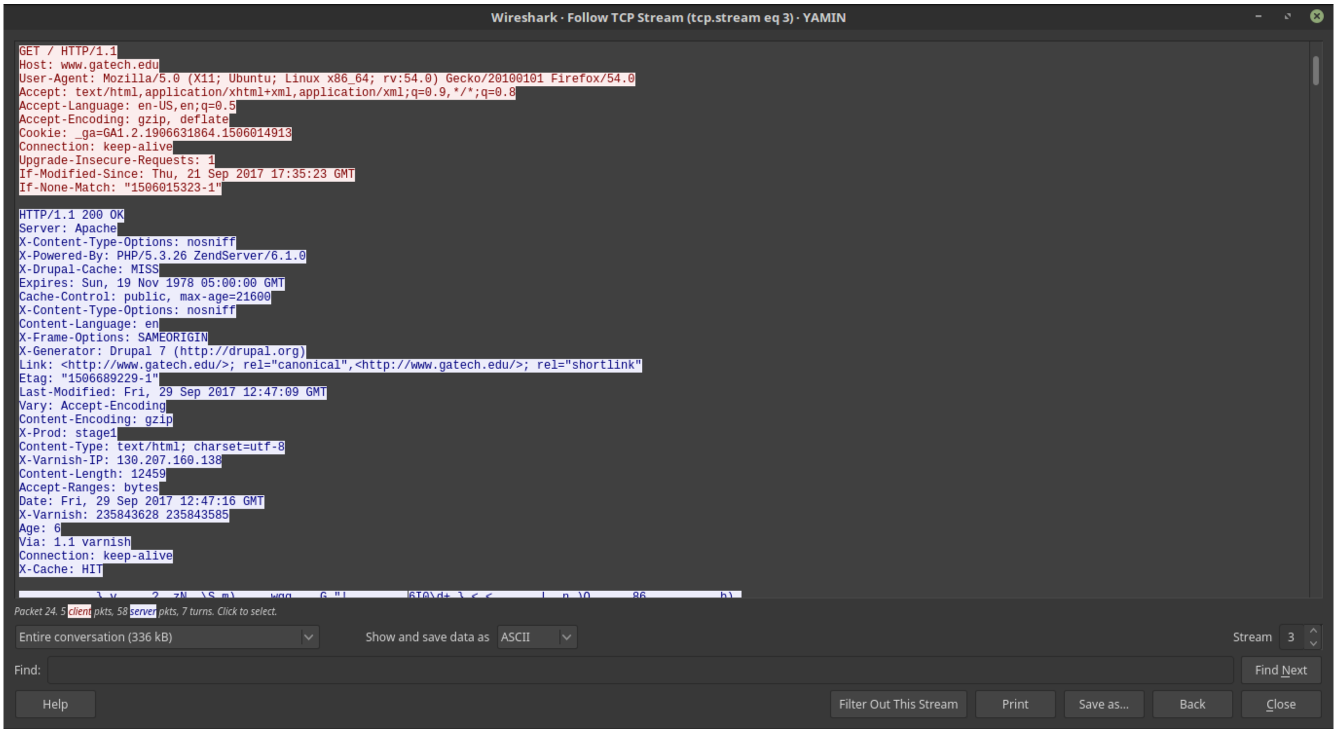
Step 12: DNS caching

First, your primary DNS queries the root servers and the root servers return a list of .edu top-level domain servers. Next, your primary server will then query the .edu top-level domain server(s) and the top-level domain server(s) will return the gatech.edu name server. The .edu top-level domain servers at this point are cached so you will not have to fetch them again. Finally, you query the gatech.edu name server and you receive the IP address for www.gatech.edu.

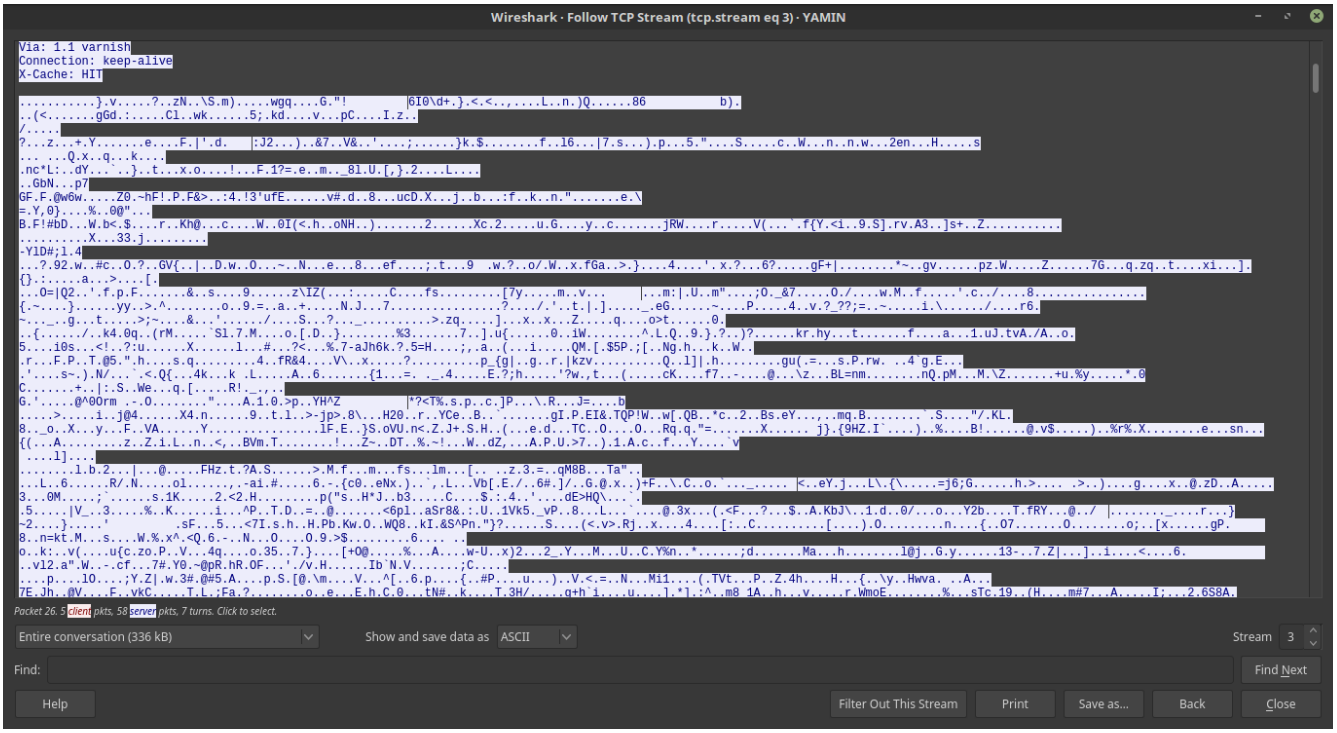
Say you want to visit www.ny.edu after visiting www.gatech.edu, then your primary server can go straight to the .edu top-level domain servers and continue the process. It doesn't have to query the root servers because the .edu top-level domain servers have been cached from the previous request.

Step 13: What happens at Layer 6 (encoding for the HTTP response)

The two images below show the g-zip encoding of the HTTP GET Request.

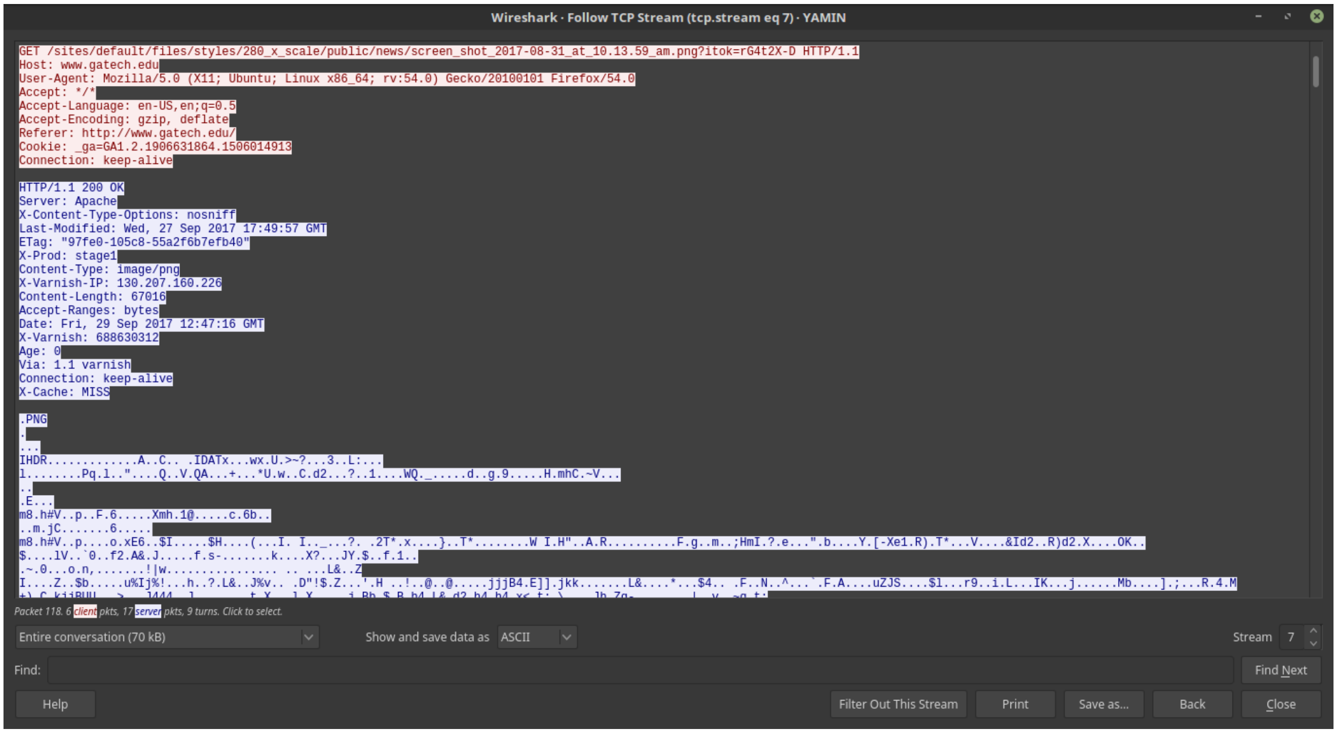

Wireshark · Follow TCP Stream (tcp.stream eq 3) · YAMIN
Packet 24. 5 client pkts, 58 server pkts, 7 turns. Click to select.
Entire conversation (336 kB)
Show and save data as
ASCII
Stream
3
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

```
GET / HTTP/1.1
Host: www.gatech.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
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: _ga=GA1.2.1906631864.1506014913
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 21 Sep 2017 17:35:23 GMT
If-None-Match: "1506015323-1"

HTTP/1.1 200 OK
Server: Apache
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.3.26 ZendServer/6.1.0
X-Drupal-Cache: MISS
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: public, max-age=21600
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-Generator: Drupal 7 (http://drupal.org)
Link: <http://www.gatech.edu/>; rel="canonical",<http://www.gatech.edu/>; rel="shortlink"
Etag: "1506689229-1"
Last-Modified: Fri, 29 Sep 2017 12:47:09 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
X-Prod: stage1
Content-Type: text/html; charset=utf-8
X-Varnish-IP: 130.207.160.138
Content-Length: 12459
Accept-Ranges: bytes
Date: Fri, 29 Sep 2017 12:47:16 GMT
X-Varnish: 235843628 235843585
Age: 6
Via: 1.1 varnish
Connection: keep-alive
X-Cache: HIT
```


Wireshark · Follow TCP Stream (tcp.stream eq 3) · YAMIN
Packet 26. 5 client pkts, 58 server pkts, 7 turns. Click to select.
Entire conversation (336 kB)
Show and save data as
ASCII
Stream
3
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

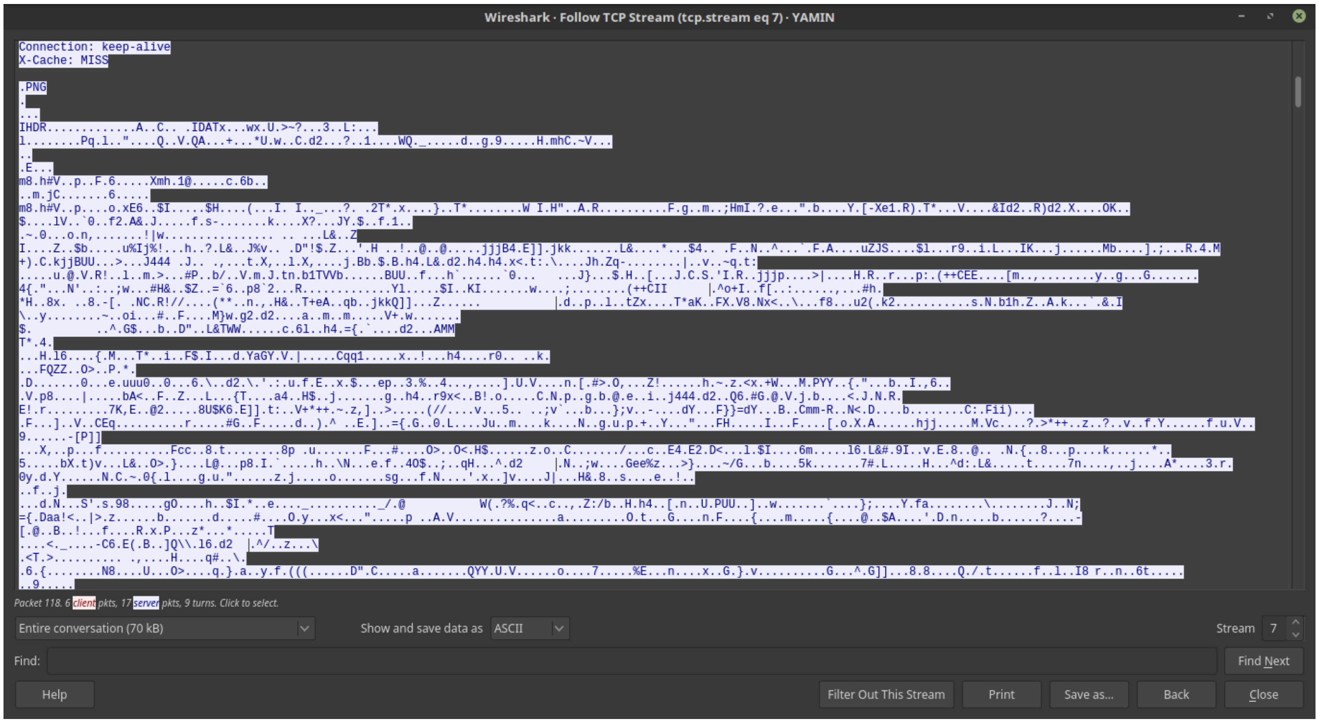
```
Via: 1.1 varnish
Connection: keep-alive
X-Cache: HIT

...........}.v.....?..zN..\S.m).....wgq....G."!          6I0\d+.}.<.<..,....L..n.)Q......86          b).
..(<.......gGd.:.....Cl..wk......5;.kd....v...pC....I.z..
/.....
?...z...+.Y.......e....F.|'.d.    :J2...)..&7..V&..'....;......}k.$........f..l6...|7.s...).p...5."....S.....c..W...n..n.w...2en...H.....s
... ...Q.x..q...k....
.nc*L:..dY...`..}..t...x.o....!...F.1?=.e..m.._8l.U.[,}.2....L....
..GbN...p7
GF.F.@w6w.....Z0.~hF!.P.F&>..:4.!3'ufE......v#.d..8...ucD.X...j..b...:f..k..n."........e.\
=.Y,0}....%..0@"...
B.F!#bD...W.b<.$....r..Kh@...c....W..0I(<.h..oNH..).......2......Xc.2.....u.G....y..c.......jRW....r.....V(...`.f{Y.<i..9.S].rv.A3..]s+..Z..........
..........X...33.j.........
-YlD#;l.4
...?.92.w..#c..O.?..GV{..|..D.w..O...~..N...e...8...ef....;.t...9  .w.?..o/.W..x.fGa..>.}....4....'.x.?...6?.....gF+|........*~..gv......pz.W.....Z......7G...q.zq..t....xi...].
{}.:.....a...>....[.
...O=|Q2..'.f.p.F.......&..s....9......z\IZ(...:.....C....fs.........[7y.....m..v...     ...m:|.U..m"....;O._&7.....O./....w.M..f.....'.c../....8................
{.~....}......yy..>.^........o..9.=..a..+.....N.J...7.................?..../.'..t.|.]....._.eG......~....P.....4..v.?_??;=..~.....i.\....../....r6.
~..._..g...t.....>;~....&...'....../....S...?..._..........>.zq.....]...x..x...Z.....q....o>t......0.
..{....../..k4.0q..(rM.....`Sl.7.M....o.[.D..}........%3.......7..].u{......0..iW........^.L.Q..9.}.?..)?......kr.hy...t.......f....a...1.uJ.tvA./A..o.
5....i0s...<!..?:u......X......l...#...?<...%.7-aJh6k.?.5=H....;,.a..(...i.....QM.[.$5P.;[..Ng.h...k..W..
.r...F.P..T.@5.".h....s.q.........4..fR&4....V\..x.....?..........p_{g|..g..r.|kzv..........Q..l]|.h.........gu(.=...s.P.rw. ..4`g.E...
.'....s~.).N/...`.<.Q{...4k...k .L.....A..6.......{1...=. ._.4.....E.?;h.....'?w.,t...(.....cK....f7..-....@...\z...BL=nm........nQ.pM...M.\Z.......+u.%y.....*.0
C.......+..|:.S..We...q.[.....R!._.,..
G.'.....@^0Orm .-.O........"....A.1.0.>p..YH^Z           *?<T%.s.p..c.]P...\.R...J=....b
.....>.....i..j@4......X4.n......9..t.l..>-jp>.8\...H20..r..YCe..B..`.......gI.P.EI&.TQP!W..w[.QB..*c..2..Bs.eY...,..mq.B........`.S...."/.KL.
8.._o..X...y...F..VA......Y.................lF.E..}S.oVU.n<.Z.J+.S.H..(...e.d...TC..O....O...Rq.q."=.......X...... j}.{9HZ.I`....)..%....B!......@.v$.....)..%r%.X.........e...sn...
{(...A..........z..Z.i.L..n..<,..BVm.T........!...Z~..DT..%.~!...W..dZ,...A.P.U.>7..).1.A.c..f...Y....`v
 ....l]....
........l.b.2...|...@.....FHz.t.?A.S......>.M.f...m...fs...lm...[..  ..z.3.=..qM8B...Ta"..
...L..6......R/.N.....ol......,-ai.#.....6.-.{c0..eNx.)..`,.L...Vb[.E./..6#.]/..G.@.x..)+F..\.C..o.`..._.....  <..eY.j...L\.{\.....=j6;G......h.>....  .>..)....g....x..@.zD..A.....
3...0M.....;`......s.1K.....2.<2.H.........p("s..H*J..b3.....C....$.:.4..'....dE>HQ\...`.
.5.....|V_..3.....%..K......i...^P..T.D..=..@.......<6pl..aSr8&.:.U..1Vk5._vP..8...L...`....@.3x...(.<F...?...$..A.KbJ\..1.d..0/...o...Y2b....T.fRY...@../  ........_....r...}
~2....}.....'           .sF...5...<7I.s.h..H.Pb.Kw.O..WQ8..kI.&S^Pn."}?......S....(<.v>.Rj..x....4....[:..C..........[....).O.........n....{..O7.......O.........o;..[x......gP.
8..n=kt.M...s....W.%.x^.<Q.6.-..N...O....O.9.>$.........6.... ..
o..k:..v(....u{c.zo.P..V...4q....o.35..7.}....[+O@.....%...A....w-U..x)2...2_.Y...M...U..C.Y%n..*......;d.......Ma...h........l@j..G.y......13-..7.Z|...]..i....<....6.
..vl2.a".W..-.cf...7#.Y0.~@pR.hR.OF...'./v.H......Ib`N.V.......;C.....
....p....lO....;Y.Z|.w.3#.@#5.A....p.S.[@.\m....V...^[..6.p....{..#P.....u...)..V.<.=..N...Mi1....(.TVt...P..Z.4h....H...{..\y..Hwva.  ..A...
7E.Jh..@V....F..vkC.....T.L.;Fa.?........o..e...E.h.C.0...tN#..k....T.3H/.....g+h`i....u....].*].:^..m8 1A..h...v.....r.WmoE........%...sTc.19..(H....m#7...A.....I;...2.6S8A.
```

The images below (2 images for the same follow) are a combination of the HTTP GET requests and HTTP RESPONSE requests for an image that was rendered on the web page. The default encoding for something that does not have the content-encoding header is US-ASCII.



```
GET /sites/default/files/styles/280_x_scale/public/news/screen_shot_2017-08-31_at_10.13.59_am.png?itok=rG4t2X-D HTTP/1.1
Host: www.gatech.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.gatech.edu/
Cookie: _ga=GA1.2.1906631864.1506014913
Connection: keep-alive

HTTP/1.1 200 OK
Server: Apache
X-Content-Type-Options: nosniff
Last-Modified: Wed, 27 Sep 2017 17:49:57 GMT
ETag: "97fe0-105c8-55a2f6b7efb40"
X-Prod: stage1
Content-Type: image/png
X-Varnish-IP: 130.207.160.226
Content-Length: 67016
Accept-Ranges: bytes
Date: Fri, 29 Sep 2017 12:47:16 GMT
X-Varnish: 688630312
Age: 0
Via: 1.1 varnish
Connection: keep-alive
X-Cache: MISS

.PNG
.
...
IHDR.............A..C.. .IDATx...wx.U.>~?...3..L:...
l........Pq.l.."....Q..V.QA...+...*U.w..C.d2...?..1....WQ._.....d..g.9.....H.mhC.~V...
..
.E...
m8.h#V..p..F.6.....Xmh.1@.....c.6b..
..m.jC.......6.....
m8.h#V..p....o.xE6..$I.....$H....(...I. I.._...?. .2T*.x....}..T*........W I.H"..A.R..........F.g..m..;HmI.?.e...".b....Y.[-Xe1.R).T*...V....&Id2..R)d2.X....OK..
$....lV..`0..f2.A&.J.....f.s-.......k....X?...JY.$..f.1..
.~.0...o.n,.......!|w............... .. ...L&..Z
I....Z..$b.....u%Ij%!...h..?.L&..J%v.. .D"!$.Z...'.H ..!..@..@.....jjjB4.E]].jkk.......L&....*...$4.. .F..N..^...`.F.A....uZJS....$l...r9..i.L...IK...j......Mb....].;...R.4.M
+).C.kjjBUU...>...J444 .J.. .,...t.X,..l.X,....j.Bb.$.B.h4.L&.d2.h4.h4.x<.t:.\....Jh.Zq-........|..v..~q.t:
```

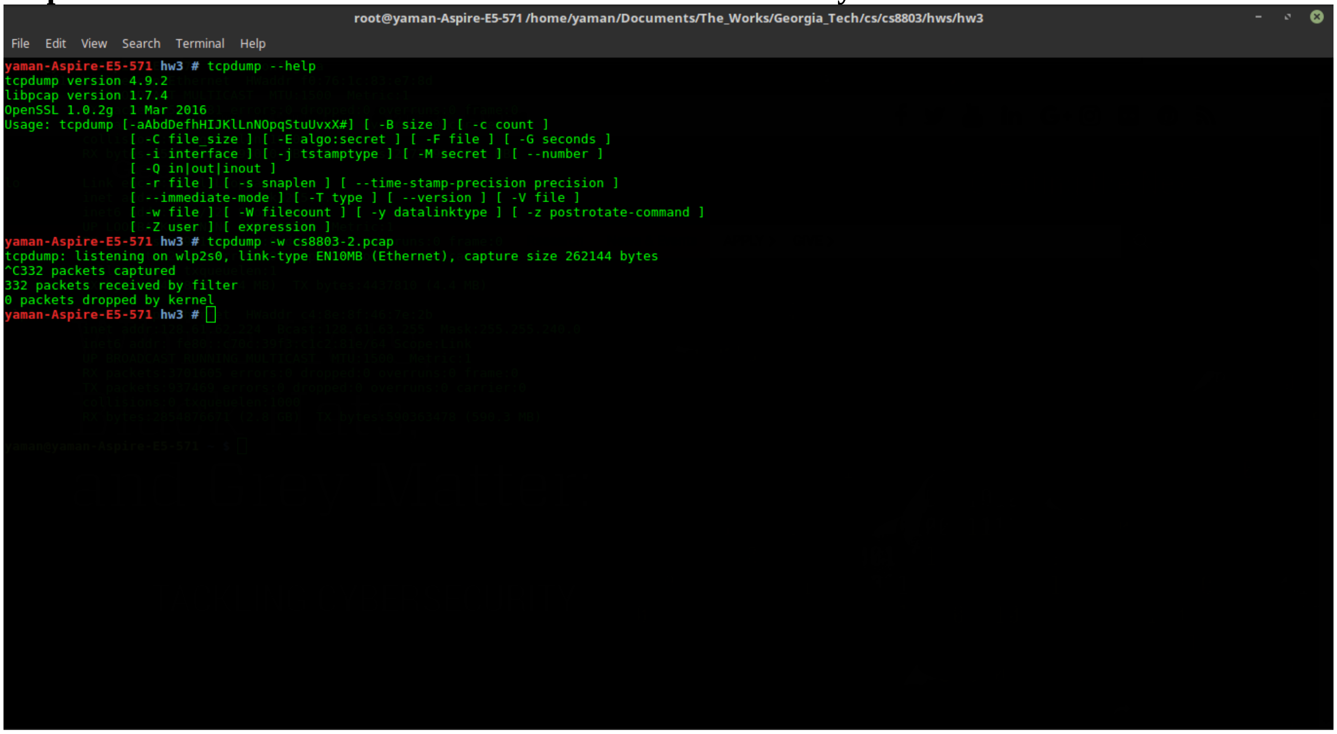
Packet 118. 6 client pkts, 17 server pkts, 9 turns. Click to select.



```
Connection: keep-alive
X-Cache: MISS

.PNG
.
...
IHDR.............A..C.. .IDATx...wx.U.>~?...3..L:...
l........Pq.l.."....Q..V.QA...+...*U.w..C.d2...?..1....WQ._.....d..g.9.....H.mhC.~V...
..
.E...
m8.h#V..p..F.6.....Xmh.1@.....c.6b..
..m.jC.......6.....
m8.h#V..p....o.xE6..$I.....$H....(...I. I.._...?. .2T*.x....}..T*........W I.H"..A.R..........F.g..m..;HmI.?.e...".b....Y.[-Xe1.R).T*...V....&Id2..R)d2.X....OK..
$....lV..`0..f2.A&.J.....f.s-.......k....X?...JY.$..f.1..
.~.0...o.n,.......!|w............... .. ...L&..Z
I....Z..$b.....u%Ij%!...h..?.L&..J%v.. .D"!$.Z...'.H ..!..@..@.....jjjB4.E]].jkk.......L&....*...$4.. .F..N..^...`.F.A....uZJS....$l...r9..i.L...IK...j......Mb....].;...R.4.M
+).C.kjjBUU...>...J444 .J.. .,...t.X,..l.X,....j.Bb.$.B.h4.L&.d2.h4.h4.x<.t:.\....Jh.Zq-........|..v..~q.t:
.....u.@.V.R!..l..m.>...#P..b/..V.m.J.tn.b1TVVb......BUU..f...h`......`0...    ...J}...$.H..[...J.C.S.'I.R..jjjp....>|....H.R..r...p:.(++CEE....[m..,........y..g...G......
4{."...N'..:..;w...#H&..$Z..=`6..p8`2...R............Yl.....$I..KI.......w....;........(++CII       |.^o+I..f[..:......,...#h.
*H..8x. ..8.-[. .NC.R!//....(**..n.,.H&..T+eA..qb..jkkQ]]...Z......          |.d..p..l..tZx....T*aK..FX.V8.Nx<..\...f8...u2(.k2...........s.N.b1h.Z..A.k...`.&.I
\..y........~..oi...#..F....M}w.g2.d2....a..m..m.....V+.w.......
$.          ..^.G$...b..D"..L&TWW......c.6l..h4.={.`....d2...AMM
T*.4.
...H.l6....{.M...T*..i..F$.I...d.YaGY.V.|.....Cqq1.....x..!...h4....r0.. ..k.
...FQZZ..O>..P.*.
.D.......0...e.uuu0..0...6.\..d2.\.'.:.u.f.E..x.$...ep..3.%..4...,....].U.V....n.[.#>.O,...Z!......h.~.z.<x.+W...M.PYY..{."...b..I.,6..
.V.p8....|.....bA<..F..Z...L...{T....a4..H$..j.......g..h4..r9x<..B!.o.....C.N.p..g.b.@.e..i..j444.d2..Q6.#G.@.V.j.b....<.J.N.R.
E!.r.........7K,E..@2.....8U$K6.E]].t:..V+*++.~.z,]..>.....(//....v...5.. ..;v`...b...};v..-....dY...F}}=dY...B..Cmm-R..N<.D....b........C:.Fii)...
.F...]..V..CEq..........r.....#G..F.....d..).^ ..E.]..={.G..0.L....Ju..m....k....N..g.u.p.+..Y..."...FH.....I...F....[.o.X.A......hjj.....M.Vc....?.>*++..z..?..v..f.Y......f.u.V..
9......-[P]]
...X,..p...f.........Fcc..8.t........8p .u.......F...#....O>..O<.H$......z.o..C......./...c..E4.E2.D<...l.$I....6m.....l6.L&#.9I..v.E.8..@.. .N.{..8...p....k......*..
5.....bX.t)v...L&..O>.}....L@...p8.I.`.....h..\N...e.f..4O$..;..qH...^.d2      |.N..;w....Gee%z...>}....~/G...b....5k.......7#.L.....H...^d:.L&.....t.....7n...,..j....A*....3.r.
0y.d.Y......N.C.~.0{.l....g.u."......z.j.....o.......sg...f.N....'.x..]v....J|...H&.8..s....e..!..
..f..j.
...d.N...S'.s.98.....gO....h..$I.*..e..._.........._/.@           W(.?%.q<..c..,.Z:/b..H.h4..[.n..U.PUU..]..w.......`....};....Y.fa........\........J..N;
={.Daa!<..|>.z......b.......d.....#....O.y...x<..."....p ..A.V...............a.........O.t...G....n.F....{....m.....{....@..$A....'.D.n.....b......?....-
[.@..B..!...f....R.x.P...z*...*.....T
....<._....-C6.E(.B..]Q\\.l6.d2  |.^/..z...\
.<T.>......... .,....H....q#..\.
.6.{........N8....U...O>....q.}.a..y.f.(((......D".C.....a.......QYY.U.V......o....7.....%E...n....x..G.}.v..........G...^.G]]...8.8....Q./.t......f..l..I8 r..n..6t.....
..9.....
```

Packet 118. 6 client pkts, 17 server pkts, 9 turns. Click to select.

Step 14: Evidence via screenshot that a PCAP was successfully created


root@yaman-Aspire-E5-571 /home/yaman/Documents/The_Works/Georgia_Tech/cs/cs8803/hws/hw3
File Edit View Search Terminal Help

```
yaman-Aspire-E5-571 hw3 # tcpdump --help
tcpdump version 4.9.2
libpcap version 1.7.4
OpenSSL 1.0.2g  1 Mar 2016
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
yaman-Aspire-E5-571 hw3 # tcpdump -w cs8803-2.pcap
tcpdump: listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C332 packets captured
332 packets received by filter
0 packets dropped by kernel
yaman-Aspire-E5-571 hw3 #
```

Step 15 (extra credit): Use DIG to show DNS recursive process

I’ve attached this image to step 2 (DNS). Thank you.