UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE INFORMÁTICA

ENGENHARIA DE COMPUTAÇÃO

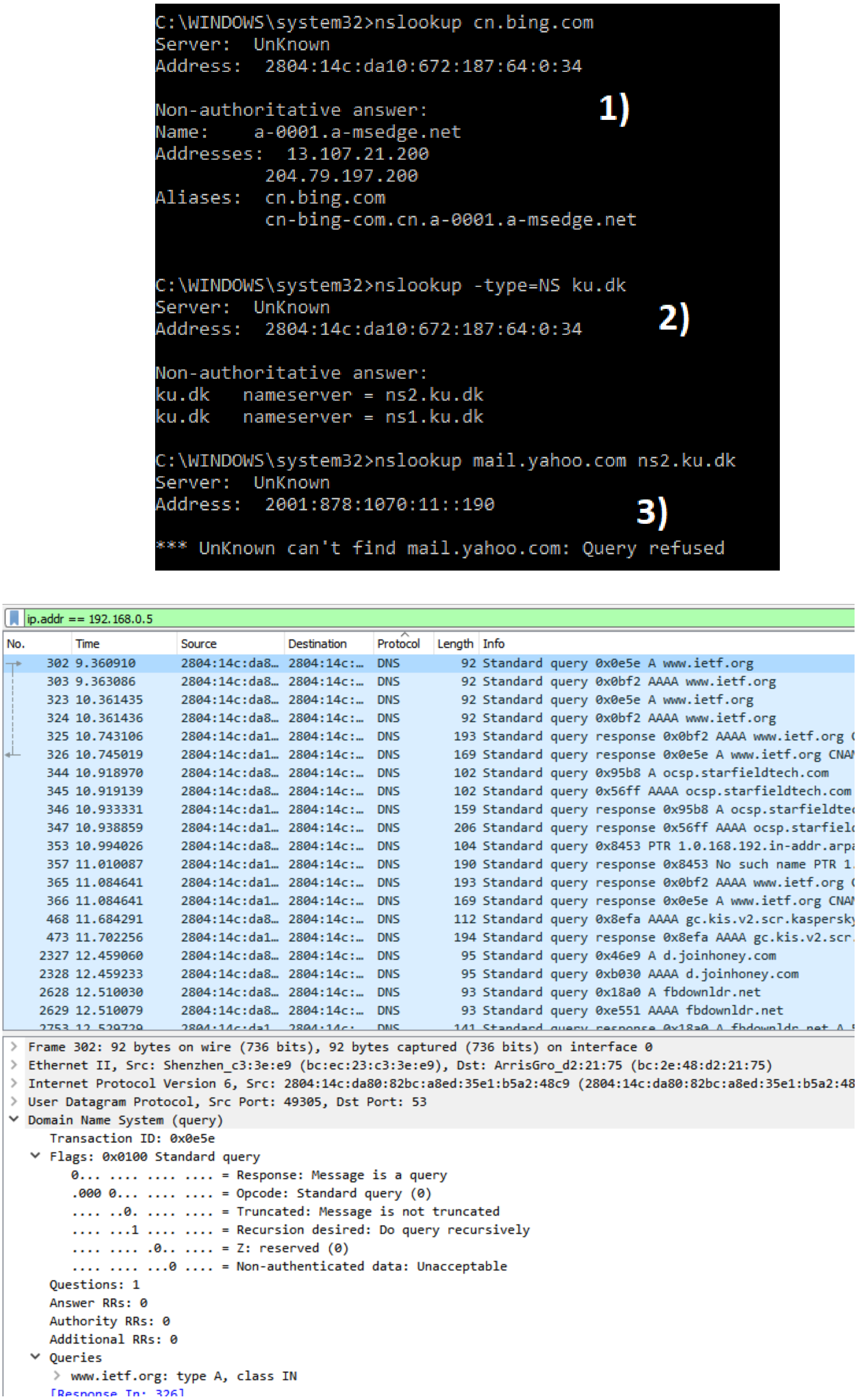
Relatório – Laboratório de Redes
DNS/HTTP

Thiago Gonzaga Gomes - 11504760

Orientador: Profa. Dra. Giorgia de Oliveira Mattos

João Pessoa – 22 de abril de 2019

DNS



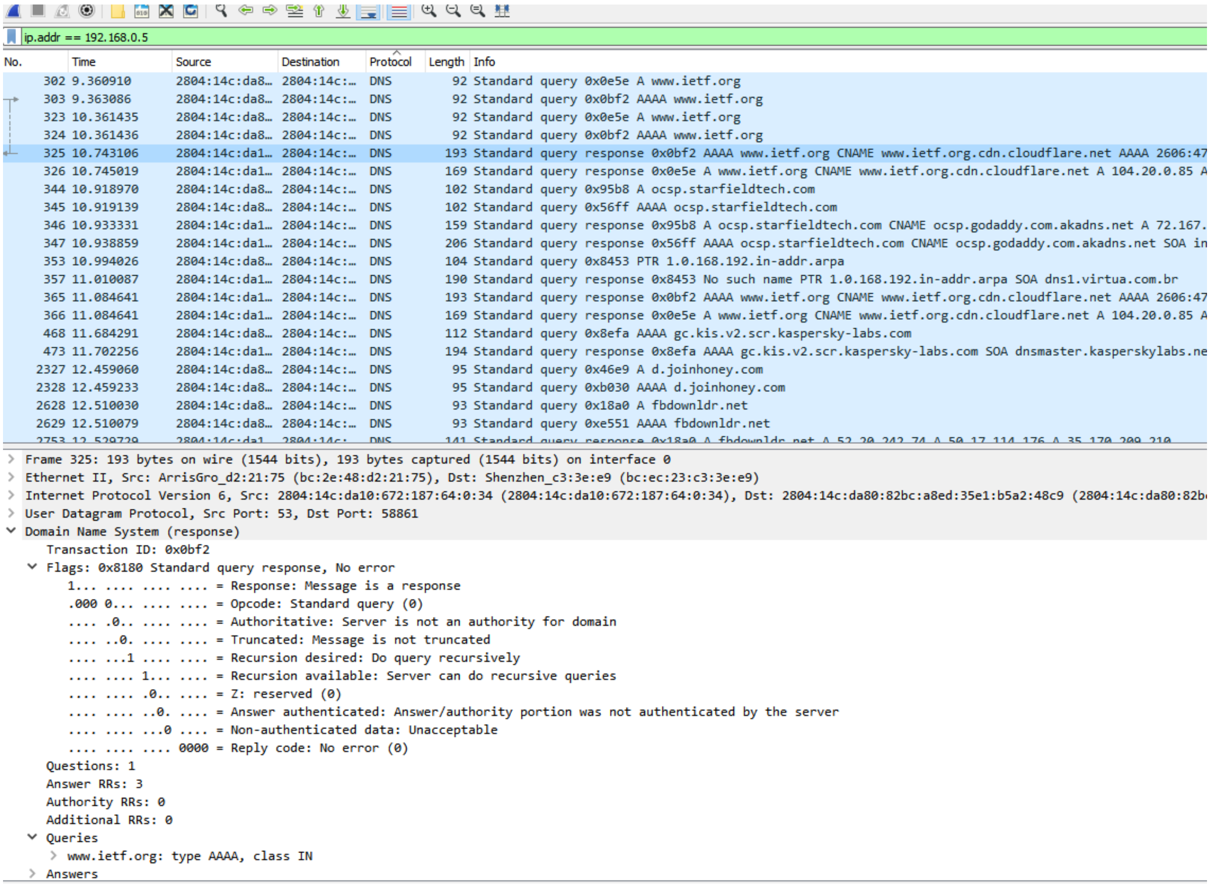
```
C:\WINDOWS\system32>nslookup cn.bing.com
Server:  UnKnown
Address:  2804:14c:da10:672:187:64:0:34

Non-authoritative answer:
Name:    a-0001.a-msedge.net
Addresses:  13.107.21.200
          204.79.197.200
Aliases:  cn.bing.com
          cn-bing-com.cn.a-0001.a-msedge.net


C:\WINDOWS\system32>nslookup -type=NS ku.dk
Server:  UnKnown
Address:  2804:14c:da10:672:187:64:0:34

Non-authoritative answer:
ku.dk   nameserver = ns2.ku.dk
ku.dk   nameserver = ns1.ku.dk

C:\WINDOWS\system32>nslookup mail.yahoo.com ns2.ku.dk
Server:  UnKnown
Address:  2001:878:1070:11::190

*** UnKnown can't find mail.yahoo.com: Query refused
```

ip.addr == 192.168.0.5

No.	Time	Source	Destination	Protocol	Length	Info
302	9.360910	2804:14c:da8…	2804:14c:…	DNS	92	Standard query 0x0e5e A www.ietf.org
303	9.363086	2804:14c:da8…	2804:14c:…	DNS	92	Standard query 0x0bf2 AAAA www.ietf.org
323	10.361435	2804:14c:da8…	2804:14c:…	DNS	92	Standard query 0x0e5e A www.ietf.org
324	10.361436	2804:14c:da8…	2804:14c:…	DNS	92	Standard query 0x0bf2 AAAA www.ietf.org
325	10.743106	2804:14c:da1…	2804:14c:…	DNS	193	Standard query response 0x0bf2 AAAA www.ietf.org C
326	10.745019	2804:14c:da1…	2804:14c:…	DNS	169	Standard query response 0x0e5e A www.ietf.org CNAM
344	10.918970	2804:14c:da8…	2804:14c:…	DNS	102	Standard query 0x95b8 A ocsp.starfieldtech.com
345	10.919139	2804:14c:da8…	2804:14c:…	DNS	102	Standard query 0x56ff AAAA ocsp.starfieldtech.com
346	10.933331	2804:14c:da1…	2804:14c:…	DNS	159	Standard query response 0x95b8 A ocsp.starfieldtec
347	10.938859	2804:14c:da1…	2804:14c:…	DNS	206	Standard query response 0x56ff AAAA ocsp.starfiel
353	10.994026	2804:14c:da8…	2804:14c:…	DNS	104	Standard query 0x8453 PTR 1.0.168.192.in-addr.arpa
357	11.010087	2804:14c:da1…	2804:14c:…	DNS	190	Standard query response 0x8453 No such name PTR 1.
365	11.084641	2804:14c:da1…	2804:14c:…	DNS	193	Standard query response 0x0bf2 AAAA www.ietf.org C
366	11.084641	2804:14c:da1…	2804:14c:…	DNS	169	Standard query response 0x0e5e A www.ietf.org CNAM
468	11.684291	2804:14c:da8…	2804:14c:…	DNS	112	Standard query 0x8efa AAAA gc.kis.v2.scr.kaspersky
473	11.702256	2804:14c:da1…	2804:14c:…	DNS	194	Standard query response 0x8efa AAAA gc.kis.v2.scr.
2327	12.459060	2804:14c:da8…	2804:14c:…	DNS	95	Standard query 0x46e9 A d.joinhoney.com
2328	12.459233	2804:14c:da8…	2804:14c:…	DNS	95	Standard query 0xb030 AAAA d.joinhoney.com
2628	12.510030	2804:14c:da8…	2804:14c:…	DNS	93	Standard query 0x18a0 A fbdownldr.net
2629	12.510079	2804:14c:da8…	2804:14c:…	DNS	93	Standard query 0xe551 AAAA fbdownldr.net
2753	12.529729	2804:14c:da1…	2804:14c:…	DNS	141	Standard query response 0x18a0 A fbdownldr.net A

```
> Frame 302: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
> Ethernet II, Src: Shenzhen_c3:3e:e9 (bc:ec:23:c3:3e:e9), Dst: ArrisGro_d2:21:75 (bc:2e:48:d2:21:75)
> Internet Protocol Version 6, Src: 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9 (2804:14c:da80:82bc:a8ed:35e1:b5a2:48
> User Datagram Protocol, Src Port: 49305, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0e5e
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 326]
```

Figura 1: Dns Query

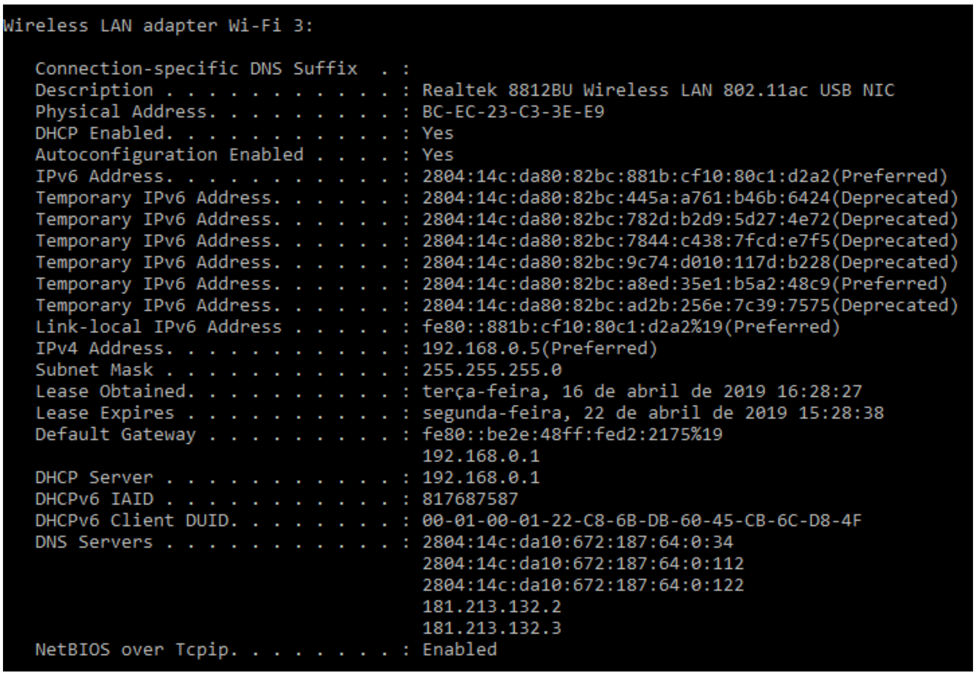


```
ip.addr == 192.168.0.5

No.     Time       Source           Destination   Protocol Length Info
    302 9.360910   2804:14c:da8…    2804:14c:…    DNS       92 Standard query 0x0e5e A www.ietf.org
    303 9.363086   2804:14c:da8…    2804:14c:…    DNS       92 Standard query 0x0bf2 AAAA www.ietf.org
    323 10.361435  2804:14c:da8…    2804:14c:…    DNS       92 Standard query 0x0e5e A www.ietf.org
    324 10.361436  2804:14c:da8…    2804:14c:…    DNS       92 Standard query 0x0bf2 AAAA www.ietf.org
    325 10.743106  2804:14c:da1…    2804:14c:…    DNS      193 Standard query response 0x0bf2 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:47
    326 10.745019  2804:14c:da1…    2804:14c:…    DNS      169 Standard query response 0x0e5e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A
    344 10.918970  2804:14c:da8…    2804:14c:…    DNS      102 Standard query 0x95b8 A ocsp.starfieldtech.com
    345 10.919139  2804:14c:da8…    2804:14c:…    DNS      102 Standard query 0x56ff AAAA ocsp.starfieldtech.com
    346 10.933331  2804:14c:da1…    2804:14c:…    DNS      159 Standard query response 0x95b8 A ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akadns.net A 72.167.
    347 10.938859  2804:14c:da1…    2804:14c:…    DNS      206 Standard query response 0x56ff AAAA ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akadns.net SOA in
    353 10.994026  2804:14c:da8…    2804:14c:…    DNS      104 Standard query 0x8453 PTR 1.0.168.192.in-addr.arpa
    357 11.010087  2804:14c:da1…    2804:14c:…    DNS      190 Standard query response 0x8453 No such name PTR 1.0.168.192.in-addr.arpa SOA dns1.virtua.com.br
    365 11.084641  2804:14c:da1…    2804:14c:…    DNS      193 Standard query response 0x0bf2 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:47
    366 11.084641  2804:14c:da1…    2804:14c:…    DNS      169 Standard query response 0x0e5e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A
    468 11.684291  2804:14c:da8…    2804:14c:…    DNS      112 Standard query 0x8efa AAAA gc.kis.v2.scr.kaspersky-labs.com
    473 11.702256  2804:14c:da1…    2804:14c:…    DNS      194 Standard query response 0x8efa AAAA gc.kis.v2.scr.kaspersky-labs.com SOA dnsmaster.kasperskylabs.ne
   2327 12.459060  2804:14c:da8…    2804:14c:…    DNS       95 Standard query 0x46e9 A d.joinhoney.com
   2328 12.459233  2804:14c:da8…    2804:14c:…    DNS       95 Standard query 0xb030 AAAA d.joinhoney.com
   2628 12.510030  2804:14c:da8…    2804:14c:…    DNS       93 Standard query 0x18a0 A fbdownldr.net
   2629 12.510079  2804:14c:da8…    2804:14c:…    DNS       93 Standard query 0xe551 AAAA fbdownldr.net
   2753 12.529729  2804:14c:da1…    2804:14c:…    DNS      141 Standard query response 0x18a0 A fbdownldr.net A 52.20.242.74 A 50.17.114.176 A 35.170.209.210

> Frame 325: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface 0
> Ethernet II, Src: ArrisGro_d2:21:75 (bc:2e:48:d2:21:75), Dst: Shenzhen_c3:3e:e9 (bc:ec:23:c3:3e:e9)
> Internet Protocol Version 6, Src: 2804:14c:da10:672:187:64:0:34 (2804:14c:da10:672:187:64:0:34), Dst: 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9 (2804:14c:da80:82b
> User Datagram Protocol, Src Port: 53, Dst Port: 58861
v Domain Name System (response)
    Transaction ID: 0x0bf2
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type AAAA, class IN
  > Answers
```

Figura 2: DNS Response

4) Elas são transmitidas via UDP.

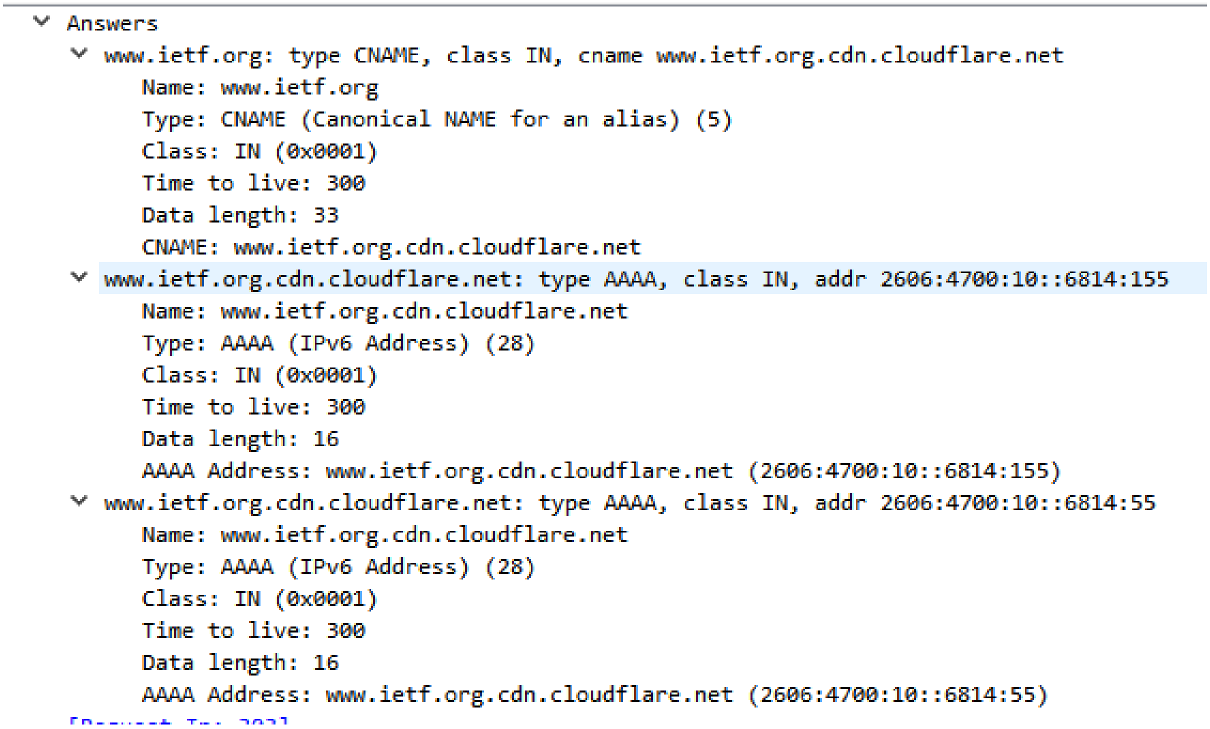
5) Porta 53 para o destino e para a origem.



```
Wireless LAN adapter Wi-Fi 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8812BU Wireless LAN 802.11ac USB NIC
   Physical Address. . . . . . . . . : BC-EC-23-C3-3E-E9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2804:14c:da80:82bc:881b:cf10:80c1:d2a2(Preferred)
   Temporary IPv6 Address. . . . . . : 2804:14c:da80:82bc:445a:a761:b46b:6424(Deprecated)
   Temporary IPv6 Address. . . . . . : 2804:14c:da80:82bc:782d:b2d9:5d27:4e72(Deprecated)
   Temporary IPv6 Address. . . . . . : 2804:14c:da80:82bc:7844:c438:7fcd:e7f5(Deprecated)
   Temporary IPv6 Address. . . . . . : 2804:14c:da80:82bc:9c74:d010:117d:b228(Deprecated)
   Temporary IPv6 Address. . . . . . : 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9(Preferred)
   Temporary IPv6 Address. . . . . . : 2804:14c:da80:82bc:ad2b:256e:7c39:7575(Deprecated)
   Link-local IPv6 Address . . . . . : fe80::881b:cf10:80c1:d2a2%19(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : terça-feira, 16 de abril de 2019 16:28:27
   Lease Expires . . . . . . . . . . : segunda-feira, 22 de abril de 2019 15:28:38
   Default Gateway . . . . . . . . . : fe80::be2e:48ff:fed2:2175%19
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 817687587
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-22-C8-6B-DB-60-45-CB-6C-D8-4F
   DNS Servers . . . . . . . . . . . : 2804:14c:da10:672:187:64:0:34
                                       2804:14c:da10:672:187:64:0:112
                                       2804:14c:da10:672:187:64:0:122
                                       181.213.132.2
                                       181.213.132.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figura 3: ipconfig -all

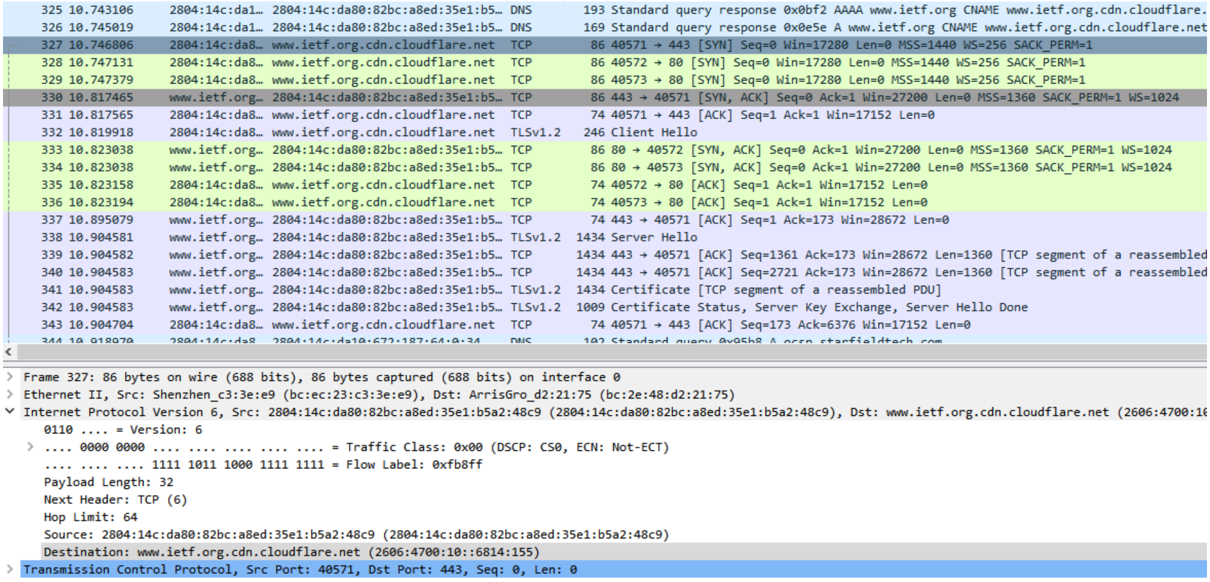
6) É enviado para 2804:14c:da10:672:187:64:0:34, que é um dos meus servidores DNS.
7) É uma query padrão do tipo A (host address) e ela não contém nenhuma resposta.



```
  Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
        Name: www.ietf.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 300
        Data length: 33
        CNAME: www.ietf.org.cdn.cloudflare.net
    www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:155
        Name: www.ietf.org.cdn.cloudflare.net
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 300
        Data length: 16
        AAAA Address: www.ietf.org.cdn.cloudflare.net (2606:4700:10::6814:155)
    www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:55
        Name: www.ietf.org.cdn.cloudflare.net
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 300
        Data length: 16
        AAAA Address: www.ietf.org.cdn.cloudflare.net (2606:4700:10::6814:55)
    [Request In: 303]
```

Figura 4: answers da response query

8) Existem 3 respostas, que contém o nome do host, o tipo de endereço, classe, TTL, tamanho do datagrama e o endereço.

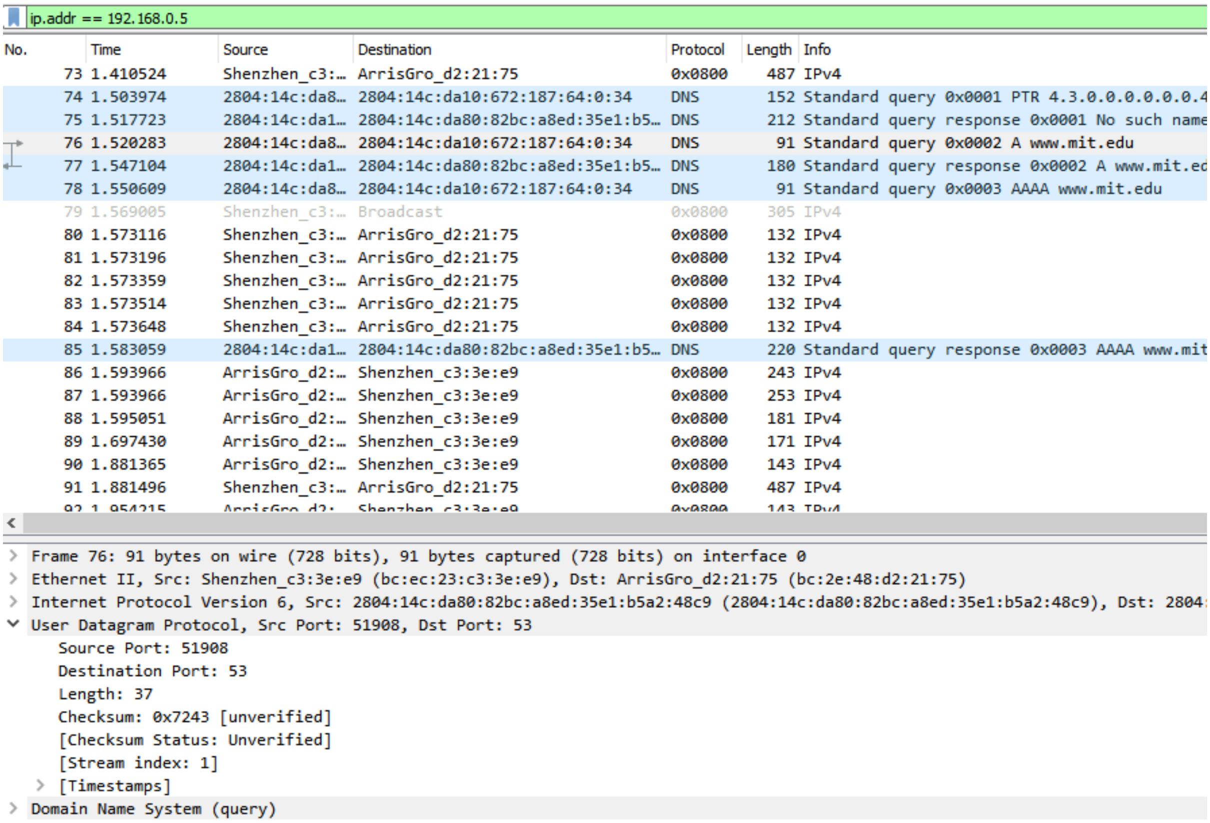


```
325 10.743106   2804:14c:da1…  2804:14c:da80:82bc:a8ed:35e1:b5… DNS      193 Standard query response 0x0bf2 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.
326 10.745019   2804:14c:da1…  2804:14c:da80:82bc:a8ed:35e1:b5… DNS      169 Standard query response 0x0e5e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net
327 10.746806   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       86 40571 → 443 [SYN] Seq=0 Win=17280 Len=0 MSS=1440 WS=256 SACK_PERM=1
328 10.747131   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       86 40572 → 80 [SYN] Seq=0 Win=17280 Len=0 MSS=1440 WS=256 SACK_PERM=1
329 10.747379   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       86 40573 → 80 [SYN] Seq=0 Win=17280 Len=0 MSS=1440 WS=256 SACK_PERM=1
330 10.817465   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TCP       86 443 → 40571 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS=1024
331 10.817565   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       74 40571 → 443 [ACK] Seq=1 Ack=1 Win=17152 Len=0
332 10.819918   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TLSv1.2  246 Client Hello
333 10.823038   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TCP       86 80 → 40572 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS=1024
334 10.823038   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TCP       86 80 → 40573 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS=1024
335 10.823158   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       74 40572 → 80 [ACK] Seq=1 Ack=1 Win=17152 Len=0
336 10.823194   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       74 40573 → 80 [ACK] Seq=1 Ack=1 Win=17152 Len=0
337 10.895079   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TCP       74 443 → 40571 [ACK] Seq=1 Ack=173 Win=28672 Len=0
338 10.904581   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TLSv1.2 1434 Server Hello
339 10.904582   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TCP     1434 443 → 40571 [ACK] Seq=1361 Ack=173 Win=28672 Len=1360 [TCP segment of a reassembled
340 10.904583   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TCP     1434 443 → 40571 [ACK] Seq=2721 Ack=173 Win=28672 Len=1360 [TCP segment of a reassembled
341 10.904583   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TLSv1.2 1434 Certificate [TCP segment of a reassembled PDU]
342 10.904583   www.ietf.org…  2804:14c:da80:82bc:a8ed:35e1:b5… TLSv1.2 1009 Certificate Status, Server Key Exchange, Server Hello Done
343 10.904704   2804:14c:da8…  www.ietf.org.cdn.cloudflare.net  TCP       74 40571 → 443 [ACK] Seq=173 Ack=6376 Win=17152 Len=0
344 10.918970   2804:14c:da8…  2804:14c:da10:672:187:64:0:34    DNS      102 Standard query 0x95b8 A ocsp.starfieldtech.com

> Frame 327: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: Shenzhen_c3:3e:e9 (bc:ec:23:c3:3e:e9), Dst: ArrisGro_d2:21:75 (bc:2e:48:d2:21:75)
v Internet Protocol Version 6, Src: 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9 (2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9), Dst: www.ietf.org.cdn.cloudflare.net (2606:4700:10
     0110 .... = Version: 6
   > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
     .... .... .... 1111 1011 1000 1111 1111 = Flow Label: 0xfb8ff
     Payload Length: 32
     Next Header: TCP (6)
     Hop Limit: 64
     Source: 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9 (2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9)
     Destination: www.ietf.org.cdn.cloudflare.net (2606:4700:10::6814:155)
> Transmission Control Protocol, Src Port: 40571, Dst Port: 443, Seq: 0, Len: 0
```

Figura 5: pacote SYN

9) O pacote SYN foi enviado para 2606:4700:10::6814:55, que corresponde ao endereço IP da segunda resposta do DNS.

10) Não. Existe cache DNS da query anterior.



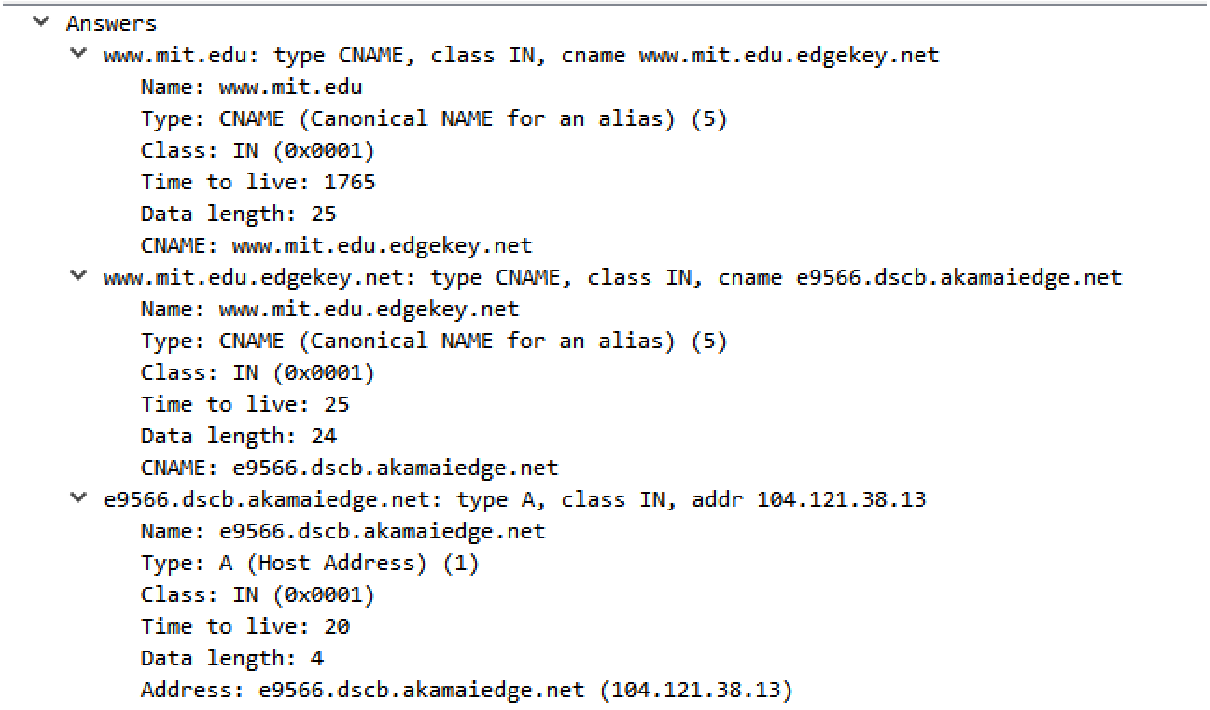
```
ip.addr == 192.168.0.5
No.    Time      Source           Destination                        Protocol Length Info
    73 1.410524  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    487 IPv4
    74 1.503974  2804:14c:da8…    2804:14c:da10:672:187:64:0:34      DNS       152 Standard query 0x0001 PTR 4.3.0.0.0.0.0.4
    75 1.517723  2804:14c:da1…    2804:14c:da80:82bc:a8ed:35e1:b5…   DNS       212 Standard query response 0x0001 No such name
    76 1.520283  2804:14c:da8…    2804:14c:da10:672:187:64:0:34      DNS        91 Standard query 0x0002 A www.mit.edu
    77 1.547104  2804:14c:da1…    2804:14c:da80:82bc:a8ed:35e1:b5…   DNS       180 Standard query response 0x0002 A www.mit.ed
    78 1.550609  2804:14c:da8…    2804:14c:da10:672:187:64:0:34      DNS        91 Standard query 0x0003 AAAA www.mit.edu
    79 1.569005  Shenzhen_c3:…    Broadcast                          0x0800    305 IPv4
    80 1.573116  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    132 IPv4
    81 1.573196  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    132 IPv4
    82 1.573359  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    132 IPv4
    83 1.573514  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    132 IPv4
    84 1.573648  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    132 IPv4
    85 1.583059  2804:14c:da1…    2804:14c:da80:82bc:a8ed:35e1:b5…   DNS       220 Standard query response 0x0003 AAAA www.mit
    86 1.593966  ArrisGro_d2:…    Shenzhen_c3:3e:e9                  0x0800    243 IPv4
    87 1.593966  ArrisGro_d2:…    Shenzhen_c3:3e:e9                  0x0800    253 IPv4
    88 1.595051  ArrisGro_d2:…    Shenzhen_c3:3e:e9                  0x0800    181 IPv4
    89 1.697430  ArrisGro_d2:…    Shenzhen_c3:3e:e9                  0x0800    171 IPv4
    90 1.881365  ArrisGro_d2:…    Shenzhen_c3:3e:e9                  0x0800    143 IPv4
    91 1.881496  Shenzhen_c3:…    ArrisGro_d2:21:75                  0x0800    487 IPv4
    92 1.954215  ArrisGro_d2:…    Shenzhen_c3:3e:e9                  0x0800    143 IPv4

> Frame 76: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
> Ethernet II, Src: Shenzhen_c3:3e:e9 (bc:ec:23:c3:3e:e9), Dst: ArrisGro_d2:21:75 (bc:2e:48:d2:21:75)
> Internet Protocol Version 6, Src: 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9 (2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9), Dst: 2804:
v User Datagram Protocol, Src Port: 51908, Dst Port: 53
    Source Port: 51908
    Destination Port: 53
    Length: 37
    Checksum: 0x7243 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
> Domain Name System (query)
```

Figura 6: lookup mit.edu

11) A porta da resposta e do request é 53.

12) É enviado para 2804:14c:da10:672:187:64:0:34, que é um dos meus servidores DNS.

13) É uma query padrão do tipo A (host address) e ela não contém nenhuma resposta.



```
v Answers
  v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1765
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 25
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 104.121.38.13
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: e9566.dscb.akamaiedge.net (104.121.38.13)
```

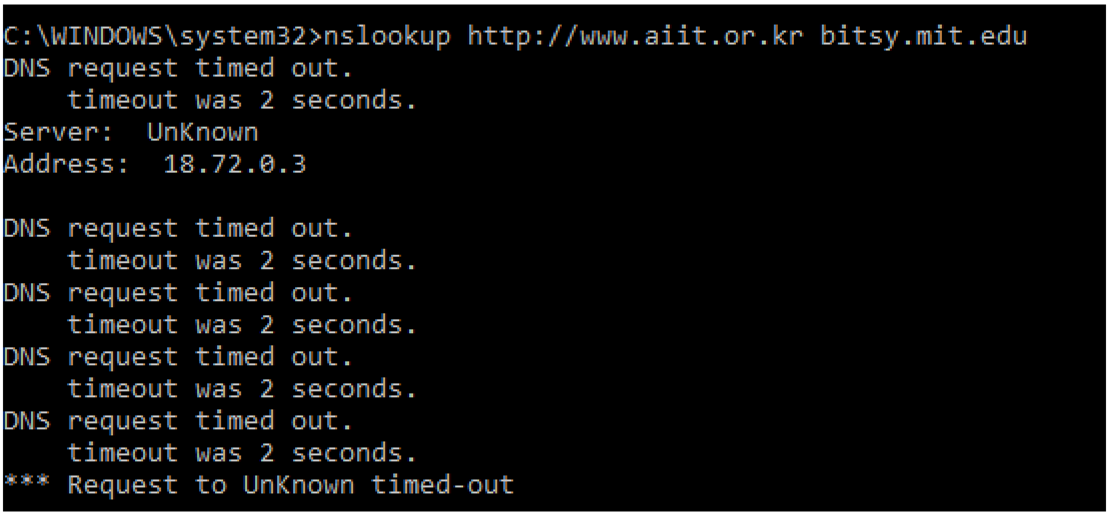
Figura 7: Response DNS lookup mit.edu

14) Existem 3 respostas, que contém o nome do host, o tipo de endereço, classe, TTL, tamanho do datagrama e o endereço.

16) É enviado para 2804:14c:da10:672:187:64:0:34.

17) É uma query padrão do tipo NS e não contém nenhuma resposta.

18) A reposta não contém nenhum nameserver.

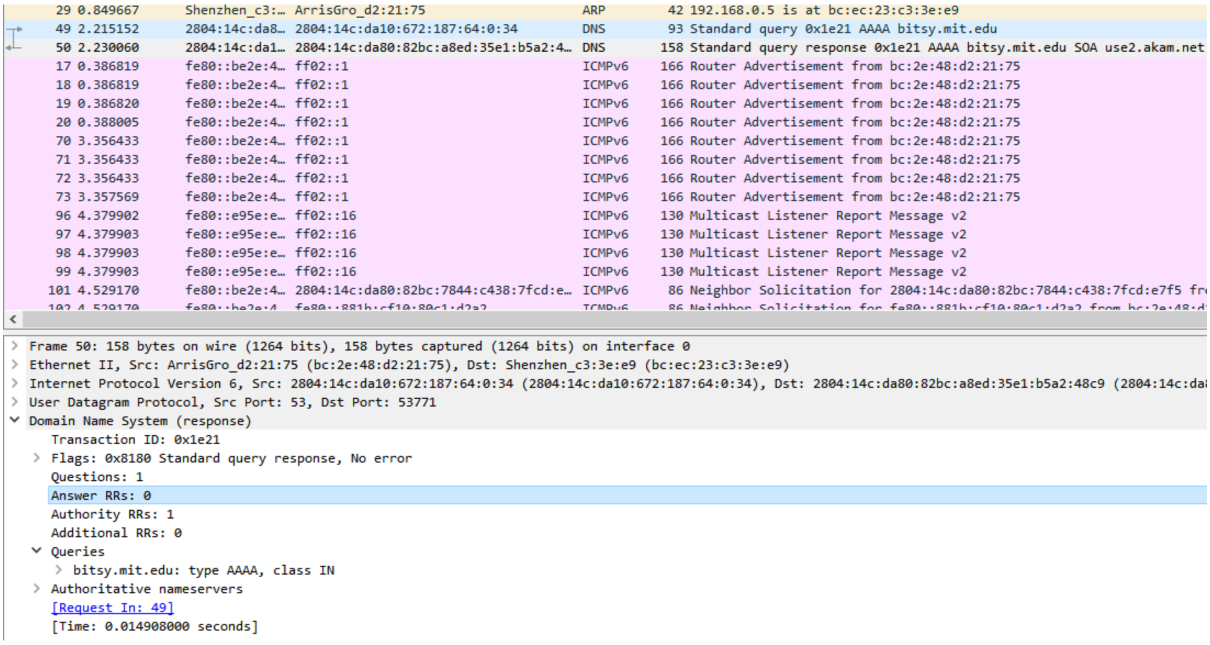


```
C:\WINDOWS\system32>nslookup http://www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.72.0.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

Percebe-se timeout em 4 tentativas.

19) O endereço IP do destino é 18.72.0.3, que é o ip do servidor do bitsy.mit.edu.

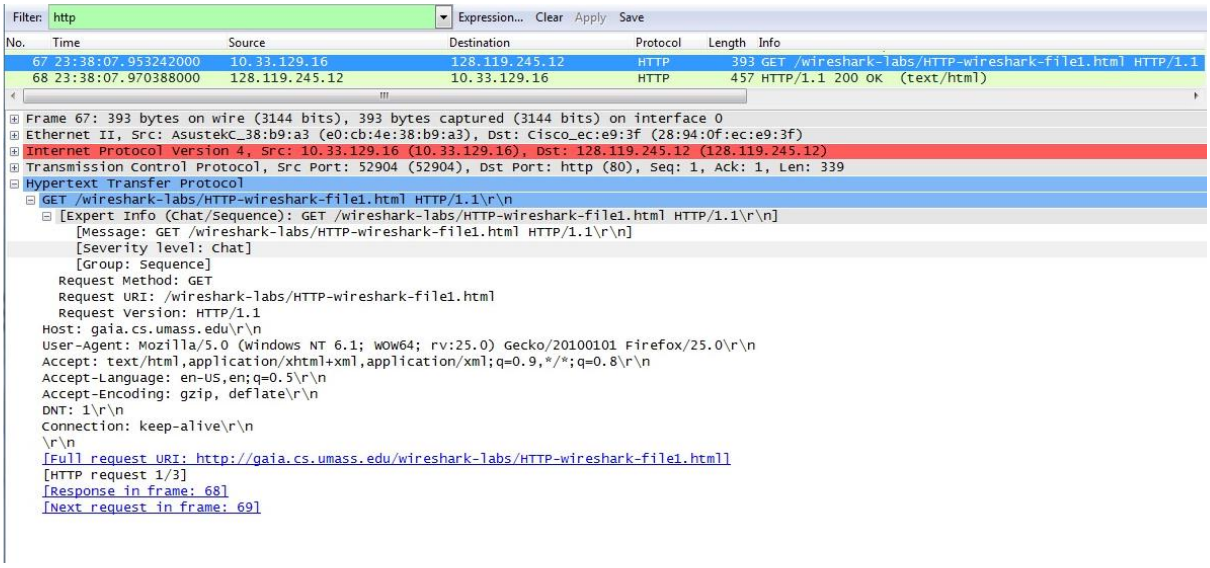
20) É do tipo A, sem respostas.



```
 29 0.849667    Shenzhen_c3:…  ArrisGro_d2:21:75                            ARP      42 192.168.0.5 is at bc:ec:23:c3:3e:e9
 49 2.215152    2804:14c:da8…  2804:14c:da10:672:187:64:0:34                DNS      93 Standard query 0x1e21 AAAA bitsy.mit.edu
 50 2.230060    2804:14c:da1…  2804:14c:da80:82bc:a8ed:35e1:b5a2:4…         DNS     158 Standard query response 0x1e21 AAAA bitsy.mit.edu SOA use2.akam.net
 17 0.386819    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 18 0.386819    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 19 0.386820    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 20 0.388005    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 70 3.356433    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 71 3.356433    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 72 3.356433    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 73 3.357569    fe80::be2e:4…  ff02::1                                      ICMPv6  166 Router Advertisement from bc:2e:48:d2:21:75
 96 4.379902    fe80::e95e:e…  ff02::16                                     ICMPv6  130 Multicast Listener Report Message v2
 97 4.379903    fe80::e95e:e…  ff02::16                                     ICMPv6  130 Multicast Listener Report Message v2
 98 4.379903    fe80::e95e:e…  ff02::16                                     ICMPv6  130 Multicast Listener Report Message v2
 99 4.379903    fe80::e95e:e…  ff02::16                                     ICMPv6  130 Multicast Listener Report Message v2
101 4.529170    fe80::be2e:4…  2804:14c:da80:82bc:7844:c438:7fcd:e…         ICMPv6   86 Neighbor Solicitation for 2804:14c:da80:82bc:7844:c438:7fcd:e7f5 fr
102 4.529170    fe80::be2e:4…  fe80::881b:cf10:80c1:d2a2                    ICMPv6   86 Neighbor Solicitation for fe80::881b:cf10:80c1:d2a2 from bc:2e:48:d

> Frame 50: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
> Ethernet II, Src: ArrisGro_d2:21:75 (bc:2e:48:d2:21:75), Dst: Shenzhen_c3:3e:e9 (bc:ec:23:c3:3e:e9)
> Internet Protocol Version 6, Src: 2804:14c:da10:672:187:64:0:34 (2804:14c:da10:672:187:64:0:34), Dst: 2804:14c:da80:82bc:a8ed:35e1:b5a2:48c9 (2804:14c:da
> User Datagram Protocol, Src Port: 53, Dst Port: 53771
v Domain Name System (response)
    Transaction ID: 0x1e21
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    > bitsy.mit.edu: type AAAA, class IN
  > Authoritative nameservers
    [Request In: 49]
    [Time: 0.014908000 seconds]
```

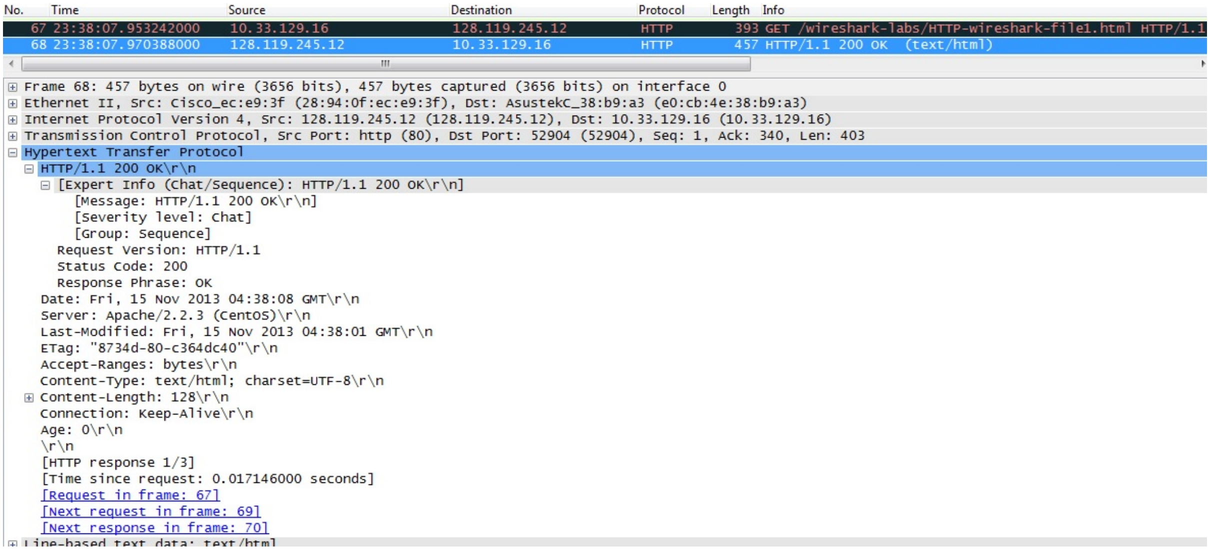
21) Não existem respostas.

HTTP



```
No.   Time                 Source          Destination      Protocol  Length  Info
  67 23:38:07.953242000    10.33.129.16    128.119.245.12   HTTP      393 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  68 23:38:07.970388000    128.119.245.12  10.33.129.16     HTTP      457 HTTP/1.1 200 OK  (text/html)

⊞ Frame 67: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3), Dst: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f)
⊞ Internet Protocol Version 4, Src: 10.33.129.16 (10.33.129.16), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 52904 (52904), Dst Port: http (80), Seq: 1, Ack: 1, Len: 339
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Message: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0\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
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/3]
    [Response in frame: 68]
    [Next request in frame: 69]
```

Figura 8: GET



```
No.   Time                 Source          Destination      Protocol  Length  Info
  67 23:38:07.953242000    10.33.129.16    128.119.245.12   HTTP      393 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  68 23:38:07.970388000    128.119.245.12  10.33.129.16     HTTP      457 HTTP/1.1 200 OK  (text/html)

⊞ Frame 68: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0
⊞ Ethernet II, Src: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f), Dst: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3)
⊞ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.33.129.16 (10.33.129.16)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 52904 (52904), Seq: 1, Ack: 340, Len: 403
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 15 Nov 2013 04:38:08 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Fri, 15 Nov 2013 04:38:01 GMT\r\n
    ETag: "8734d-80-c364dc40"\r\n
    Accept-Ranges: bytes\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  ⊞ Content-Length: 128\r\n
    Connection: Keep-Alive\r\n
    Age: 0\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.017146000 seconds]
    [Request in frame: 67]
    [Next request in frame: 69]
    [Next response in frame: 70]
⊞ Line-based text data: text/html
```

Figura 9: Resposta

1) HTTP/1.1

2) en-US

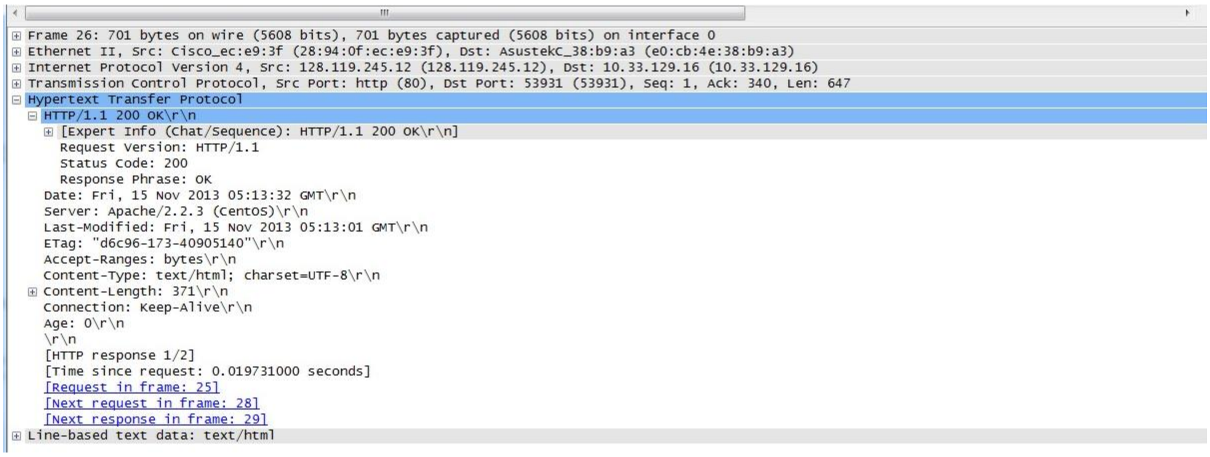
3) O endereço do servidor é 128.119.245.12.

4) O servidor enviou o código 200 (OK).

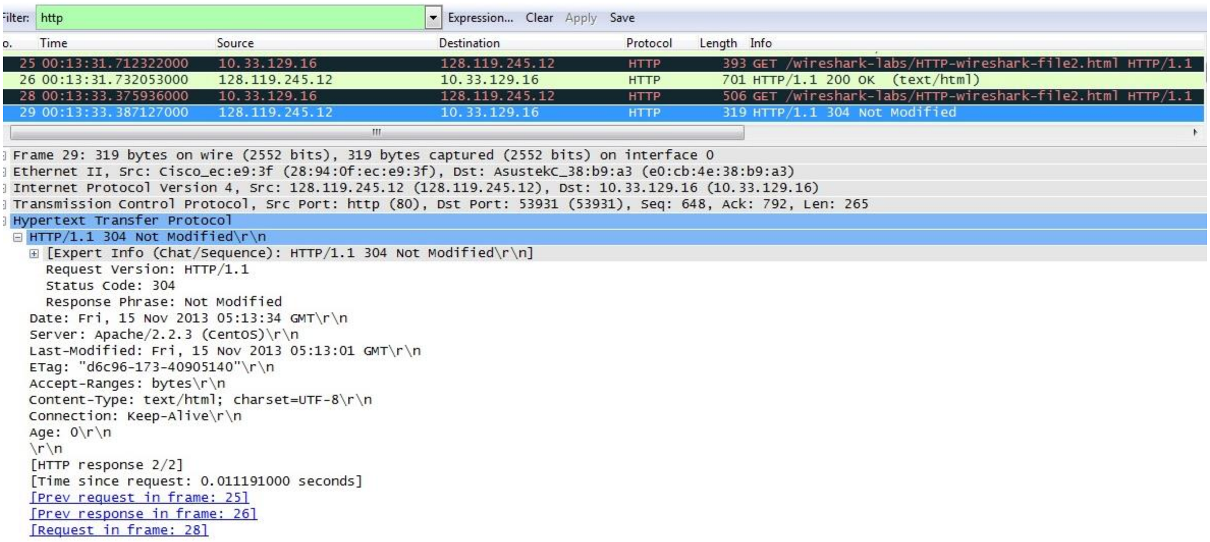
5) Fri, 15 Nov 2013 04:38:01 GMT

6) 128 bytes.

7) Não.



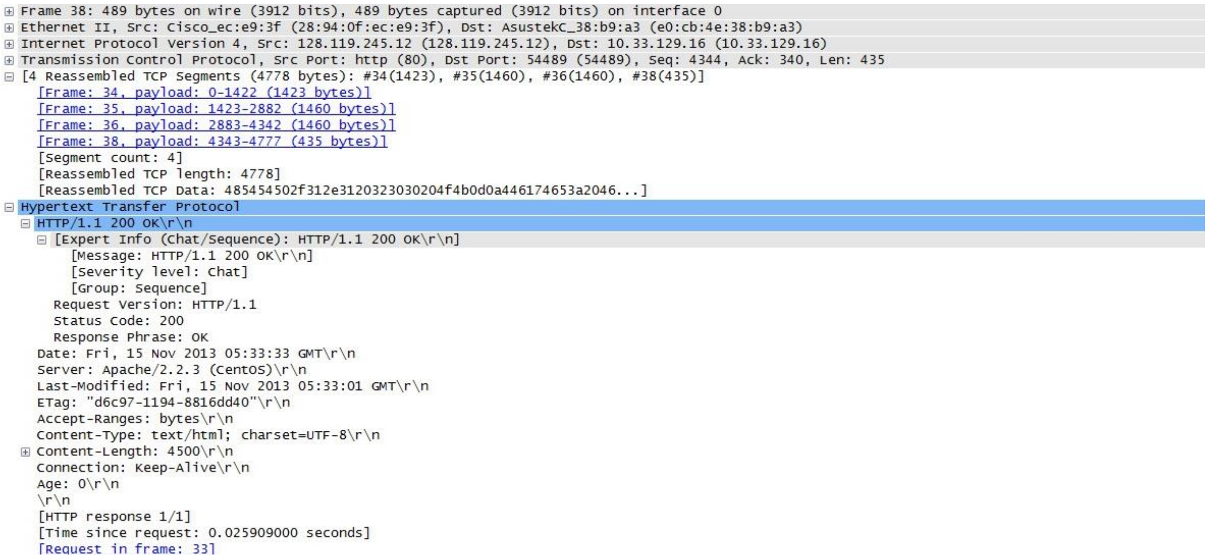
```
⊞ Frame 26: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bits) on interface 0
⊞ Ethernet II, Src: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f), Dst: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3)
⊞ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.33.129.16 (10.33.129.16)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 53931 (53931), Seq: 1, Ack: 340, Len: 647
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 15 Nov 2013 05:13:32 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Fri, 15 Nov 2013 05:13:01 GMT\r\n
    ETag: "d6c96-173-40905140"\r\n
    Accept-Ranges: bytes\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  ⊞ Content-Length: 371\r\n
    Connection: Keep-Alive\r\n
    Age: 0\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.019731000 seconds]
    [Request in frame: 25]
    [Next request in frame: 28]
    [Next response in frame: 29]
⊞ Line-based text data: text/html
```



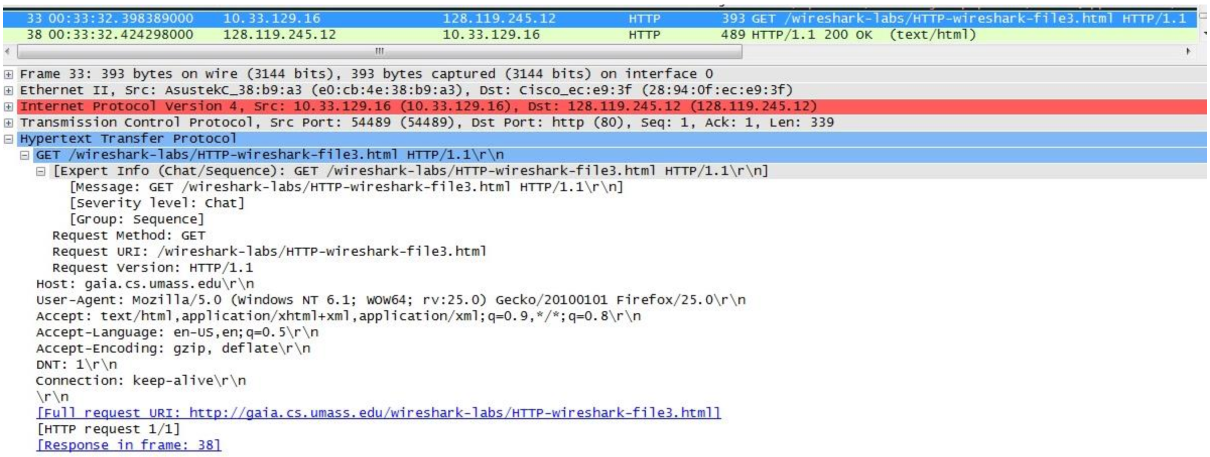
```
o.  Time                Source           Destination      Protocol  Length  Info
 25 00:13:31.712322000  10.33.129.16     128.119.245.12   HTTP         393  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 26 00:13:31.732053000  128.119.245.12   10.33.129.16     HTTP         701  HTTP/1.1 200 OK  (text/html)
 28 00:13:33.375936000  10.33.129.16     128.119.245.12   HTTP         506  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 29 00:13:33.387127000  128.119.245.12   10.33.129.16     HTTP         319  HTTP/1.1 304 Not Modified
```

```
Frame 29: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits) on interface 0
Ethernet II, Src: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f), Dst: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.33.129.16 (10.33.129.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 53931 (53931), Seq: 648, Ack: 792, Len: 265
Hypertext Transfer Protocol
⊟ HTTP/1.1 304 Not Modified\r\n
  ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    Request Version: HTTP/1.1
    Status Code: 304
    Response Phrase: Not Modified
  Date: Fri, 15 Nov 2013 05:13:34 GMT\r\n
  Server: Apache/2.2.3 (CentOS)\r\n
  Last-Modified: Fri, 15 Nov 2013 05:13:01 GMT\r\n
  ETag: "d6c96-173-40905140"\r\n
  Accept-Ranges: bytes\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Connection: Keep-Alive\r\n
  Age: 0\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.011191000 seconds]
  [Prev request in frame: 25]
  [Prev response in frame: 26]
  [Request in frame: 28]
```

8) Não. Só mostraria caso o site houvesse sido visitado anteriormente.
9) Sim, enviou o código 200 (OK), afirmando que não houve nada de errado, e enviou 371 bytes.
10) Sim, o IF_MODIFIED_SINCE aparece pois o site foi visitado anteriormente. If-Modified-Since: Fri, 15 Nov 2013 05:13:01 GMT
11) O código é 304 (Not modified). Como o conteúdo já está no cache, o servidor não retorna o conteúdo mais uma vez.



```
⊞ Frame 38: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0
⊞ Ethernet II, Src: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f), Dst: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3)
⊞ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.33.129.16 (10.33.129.16)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 54489 (54489), Seq: 4344, Ack: 340, Len: 435
⊟ [4 Reassembled TCP Segments (4778 bytes): #34(1423), #35(1460), #36(1460), #38(435)]
    [Frame: 34, payload: 0-1422 (1423 bytes)]
    [Frame: 35, payload: 1423-2882 (1460 bytes)]
    [Frame: 36, payload: 2883-4342 (1460 bytes)]
    [Frame: 38, payload: 4343-4777 (435 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4778]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2046...]
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊟ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 15 Nov 2013 05:33:33 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Fri, 15 Nov 2013 05:33:01 GMT\r\n
    ETag: "d6c97-1194-8816dd40"\r\n
    Accept-Ranges: bytes\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  ⊞ Content-Length: 4500\r\n
    Connection: Keep-Alive\r\n
    Age: 0\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.025909000 seconds]
    [Request in frame: 33]
```



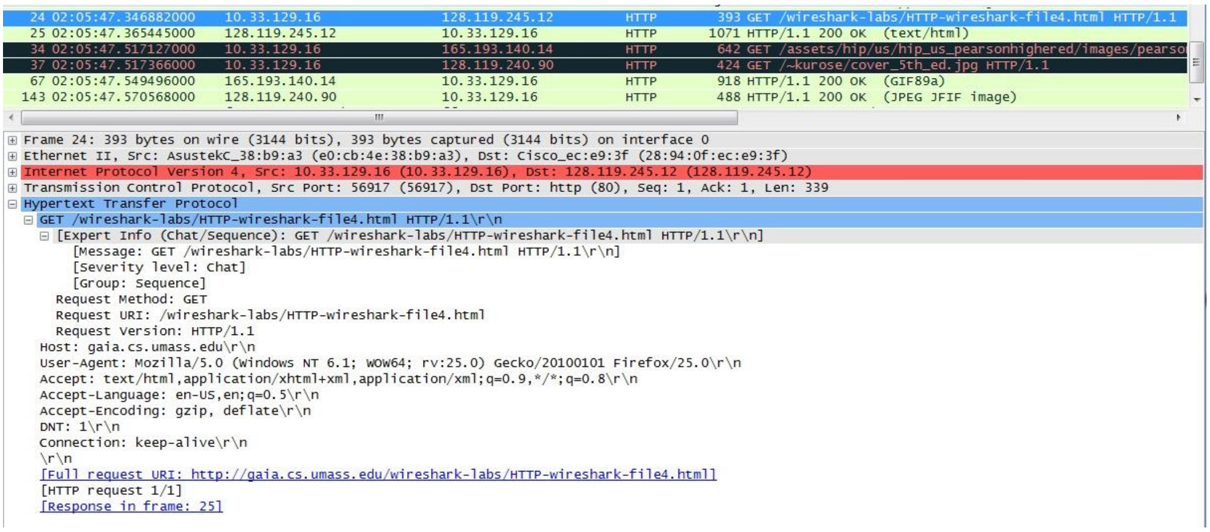
```
 33 00:33:32.398389000   10.33.129.16      128.119.245.12     HTTP     393 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 38 00:33:32.424298000   128.119.245.12    10.33.129.16       HTTP     489 HTTP/1.1 200 OK  (text/html)

⊞ Frame 33: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3), Dst: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f)
⊞ Internet Protocol Version 4, Src: 10.33.129.16 (10.33.129.16), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 54489 (54489), Dst Port: http (80), Seq: 1, Ack: 1, Len: 339
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [Message: GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0\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
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 38]
```

12) O browser enviou apenas um GET request. Só há um pacote.

13) 4 segmentos TCP pra carregar a página.

14) 200 (OK).

15) Não.

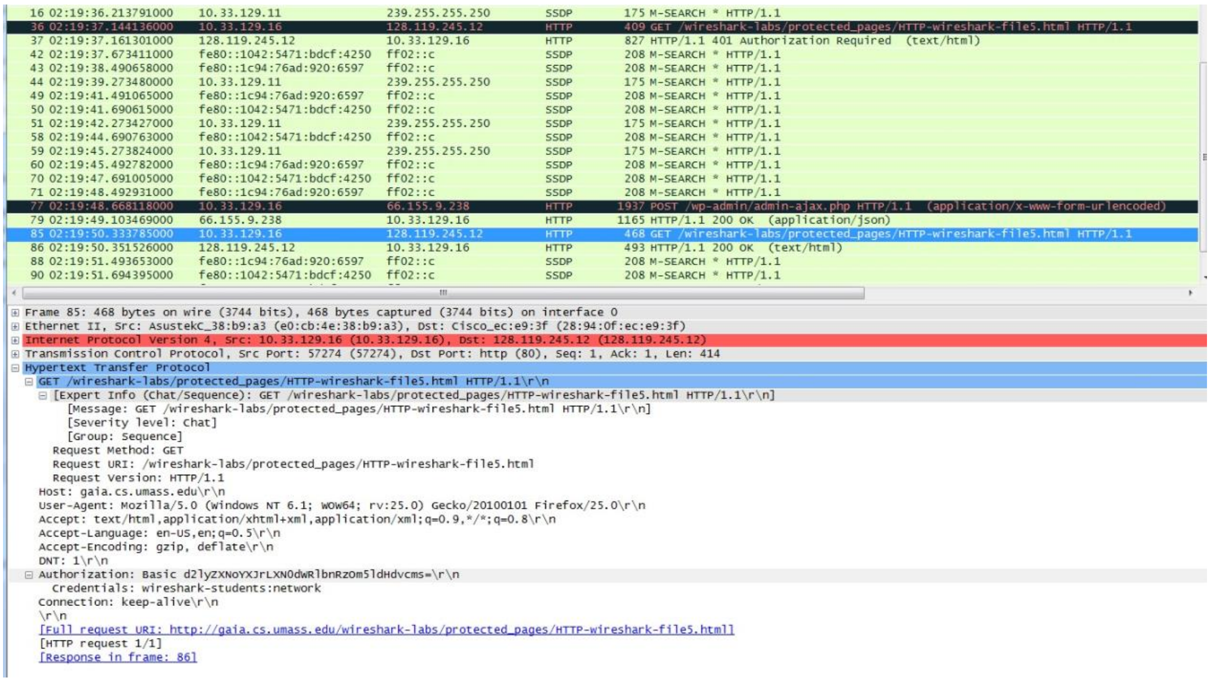


```
 24 02:05:47.346882000   10.33.129.16      128.119.245.12    HTTP    393 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 25 02:05:47.365445000   128.119.245.12    10.33.129.16      HTTP   1071 HTTP/1.1 200 OK  (text/html)
 34 02:05:47.517127000   10.33.129.16      165.193.140.14    HTTP    642 GET /assets/hip/us/hip_us_pearsonhighered/images/pearso
 37 02:05:47.517366000   10.33.129.16      128.119.240.90    HTTP    424 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 67 02:05:47.549496000   165.193.140.14    10.33.129.16      HTTP    918 HTTP/1.1 200 OK  (GIF89a)
143 02:05:47.570568000   128.119.240.90    10.33.129.16      HTTP    488 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
⊞ Frame 24: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3), Dst: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f)
⊞ Internet Protocol Version 4, Src: 10.33.129.16 (10.33.129.16), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 56917 (56917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 339
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
        [Message: GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file4.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0\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
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/1]
    [Response in frame: 25]
```

16) O browser enviou 3 GET requests. Para: 128.119.245.12, 165.193.140.14 e 128.119.240.90.

17) Cada imagem foi transmitida em uma conexão TCP diferente, são baixadas em série.



```
16 02:19:36.213791000  10.33.129.11               239.255.255.250  SSDP    175 M-SEARCH * HTTP/1.1
36 02:19:37.144136000  10.33.129.16               128.119.245.12   HTTP    409 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
37 02:19:37.161301000  128.119.245.12             10.33.129.16     HTTP    827 HTTP/1.1 401 Authorization Required  (text/html)
42 02:19:37.673411000  fe80::1042:5471:bdcf:4250  ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
43 02:19:38.490658000  fe80::1c94:76ad:920:6597   ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
44 02:19:39.273480000  10.33.129.11               239.255.255.250  SSDP    175 M-SEARCH * HTTP/1.1
49 02:19:41.491065000  fe80::1c94:76ad:920:6597   ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
50 02:19:41.690615000  fe80::1042:5471:bdcf:4250  ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
51 02:19:42.273427000  10.33.129.11               239.255.255.250  SSDP    175 M-SEARCH * HTTP/1.1
58 02:19:44.690763000  fe80::1042:5471:bdcf:4250  ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
59 02:19:45.273824000  10.33.129.11               239.255.255.250  SSDP    175 M-SEARCH * HTTP/1.1
60 02:19:45.492782000  fe80::1c94:76ad:920:6597   ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
70 02:19:47.691005000  fe80::1042:5471:bdcf:4250  ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
71 02:19:48.492931000  fe80::1c94:76ad:920:6597   ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
77 02:19:48.668118000  10.33.129.16               66.155.9.238     HTTP   1937 POST /wp-admin/admin-ajax.php HTTP/1.1  (application/x-www-form-urlencoded)
79 02:19:49.103469000  66.155.9.238               10.33.129.16     HTTP   1165 HTTP/1.1 200 OK  (application/json)
85 02:19:50.333785000  10.33.129.16               128.119.245.12   HTTP    468 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
86 02:19:50.351526000  128.119.245.12             10.33.129.16     HTTP    493 HTTP/1.1 200 OK  (text/html)
88 02:19:51.493653000  fe80::1c94:76ad:920:6597   ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
90 02:19:51.694395000  fe80::1042:5471:bdcf:4250  ff02::c          SSDP    208 M-SEARCH * HTTP/1.1
```

```
⊞ Frame 85: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_38:b9:a3 (e0:cb:4e:38:b9:a3), Dst: Cisco_ec:e9:3f (28:94:0f:ec:e9:3f)
⊞ Internet Protocol Version 4, Src: 10.33.129.16 (10.33.129.16), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 57274 (57274), Dst Port: http (80), Seq: 1, Ack: 1, Len: 414
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [Message: GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0\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
    DNT: 1\r\n
  ⊟ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 86]
```

18) 401 (Auth required).

19) Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Credentials: wireshark-students:network