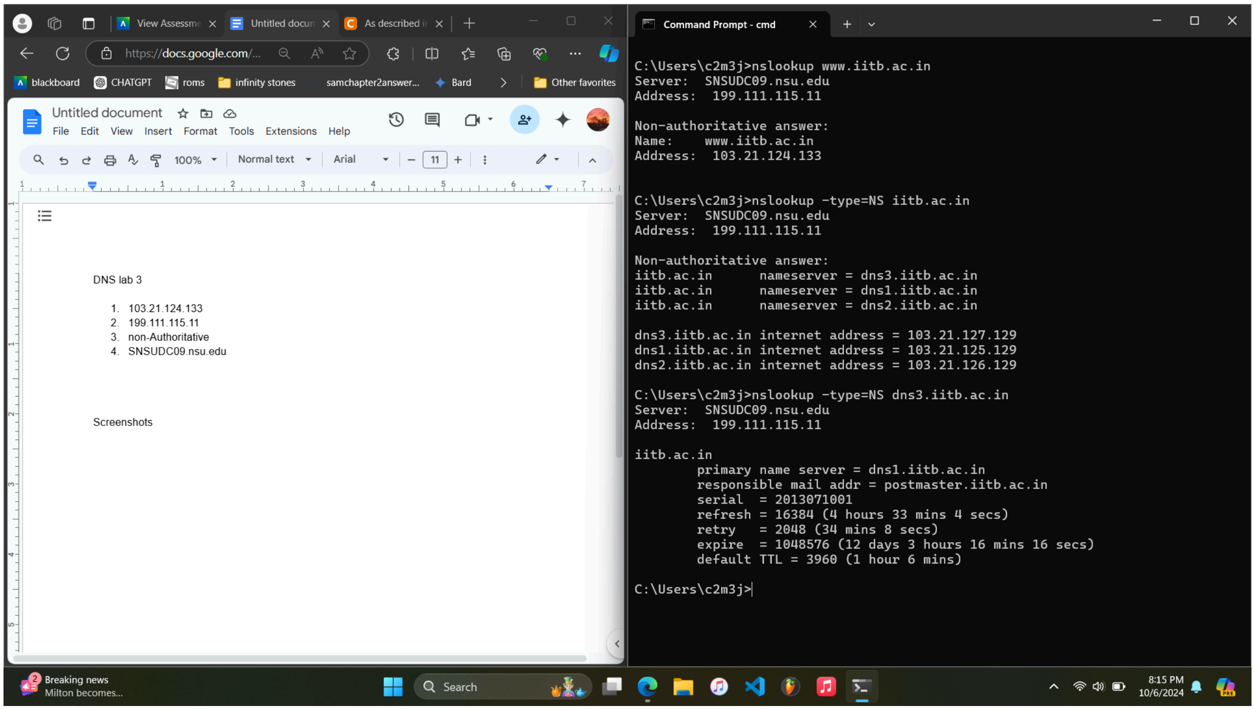
Clay Jones
DNS lab 3

1. 103.21.124.133
2. 199.111.115.11
3. non-Authoritative
4. SNSUDC09.nsu.edu (rest in picture)
5. 45 and UDP
6. 46 and UDP
7. Source port 58435 dest port = 53
8. Destination Address: 199.111.115.11
9. One question and no answer
10. One question and one answer
11. Number for base file: 64, DNS query: 45, 46, graphic book: 132, second query: 46
12. Dest 52488, source 53
13. Destination Address: 199.111.115.11, YES
14. SImple query with no answers
15. One question and one answer
16. 8.8.8.8, yes
17. One question and no answers
18. 3 answers, answers are the authoritative name servers, 2 additional resource records, and those contains the host addresses

Screenshots
1-4



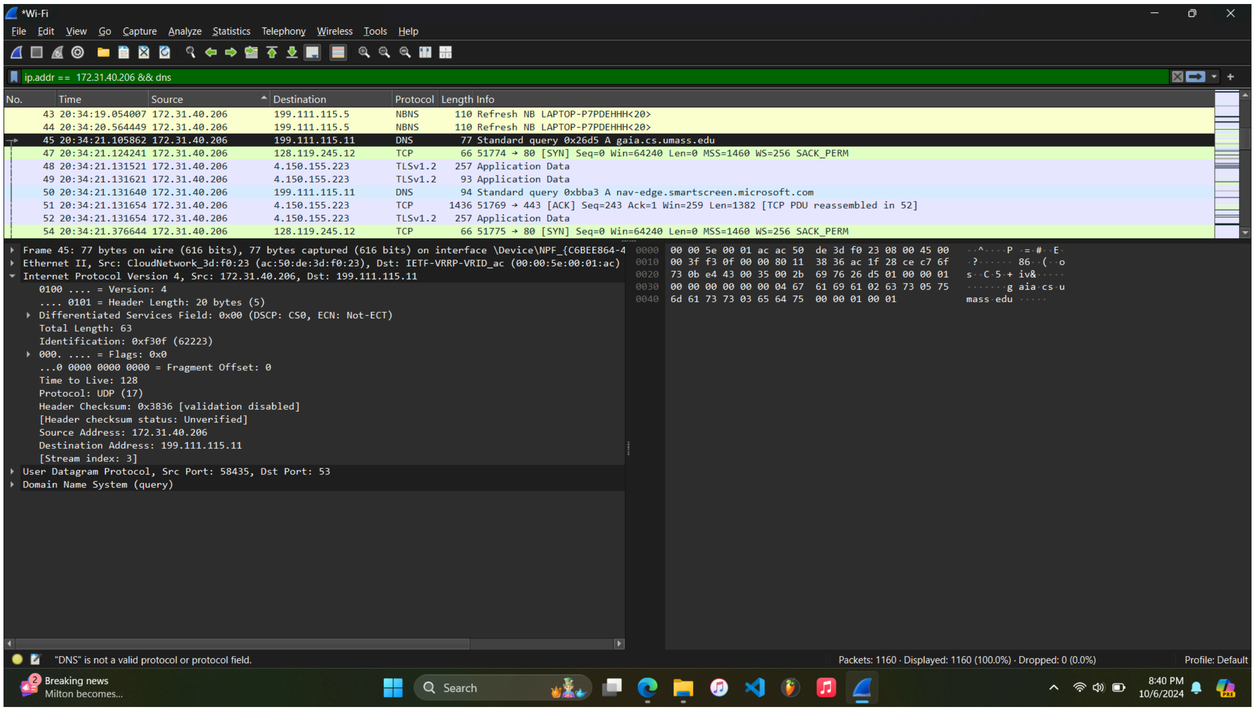
DNS lab 3

1. 103.21.124.133
2. 199.111.115.11
3. non-Authoritative
4. SNSUDC09.nsu.edu

Screenshots

```
C:\Users\c2m3j>nslookup www.iitb.ac.in
Server:  SNSUDC09.nsu.edu
Address:  199.111.115.11

Non-authoritative answer:
Name:    www.iitb.ac.in
Address:  103.21.124.133


C:\Users\c2m3j>nslookup -type=NS iitb.ac.in
Server:  SNSUDC09.nsu.edu
Address:  199.111.115.11

Non-authoritative answer:
iitb.ac.in      nameserver = dns3.iitb.ac.in
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in

dns3.iitb.ac.in internet address = 103.21.127.129
dns1.iitb.ac.in internet address = 103.21.125.129
dns2.iitb.ac.in internet address = 103.21.126.129

C:\Users\c2m3j>nslookup -type=NS dns3.iitb.ac.in
Server:  SNSUDC09.nsu.edu
Address:  199.111.115.11

iitb.ac.in
        primary name server = dns1.iitb.ac.in
        responsible mail addr = postmaster.iitb.ac.in
        serial  = 2013071001
        refresh = 16384 (4 hours 33 mins 4 secs)
        retry   = 2048 (34 mins 8 secs)
        expire  = 1048576 (12 days 3 hours 16 mins 16 secs)
        default TTL = 3960 (1 hour 6 mins)

C:\Users\c2m3j>
```

5



ip.addr == 172.31.40.206 && dns

```
No.  Time             Source          Destination      Protocol Length Info
  43 20:34:19.054007 172.31.40.206   199.111.115.5    NBNS      110 Refresh NB LAPTOP-P7PDEHHH<20>
  44 20:34:20.564449 172.31.40.206   199.111.115.5    NBNS      110 Refresh NB LAPTOP-P7PDEHHH<20>
  45 20:34:21.105862 172.31.40.206   199.111.115.11   DNS        77 Standard query 0x26d5 A gaia.cs.umass.edu
  47 20:34:21.124241 172.31.40.206   128.119.245.12   TCP        66 51774 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  48 20:34:21.131521 172.31.40.206   4.150.155.223    TLSv1.2   257 Application Data
  49 20:34:21.131621 172.31.40.206   4.150.155.223    TLSv1.2    93 Application Data
  50 20:34:21.131640 172.31.40.206   199.111.115.11   DNS        94 Standard query 0xbba3 A nav-edge.smartscreen.microsoft.com
  51 20:34:21.131654 172.31.40.206   4.150.155.223    TCP      1436 51769 → 443 [ACK] Seq=243 Ack=1 Win=259 Len=1382 [TCP PDU reassembled in 52]
  52 20:34:21.131654 172.31.40.206   4.150.155.223    TLSv1.2   257 Application Data
  54 20:34:21.376644 172.31.40.206   128.119.245.12   TCP        66 51775 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
Frame 45: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{C6BEE864-4
Ethernet II, Src: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23), Dst: IETF-VRRP-VRID_ac (00:00:5e:00:01:ac)
Internet Protocol Version 4, Src: 172.31.40.206, Dst: 199.111.115.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0xf30f (62223)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x3836 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.31.40.206
    Destination Address: 199.111.115.11
    [Stream index: 3]
User Datagram Protocol, Src Port: 58435, Dst Port: 53
Domain Name System (query)
```

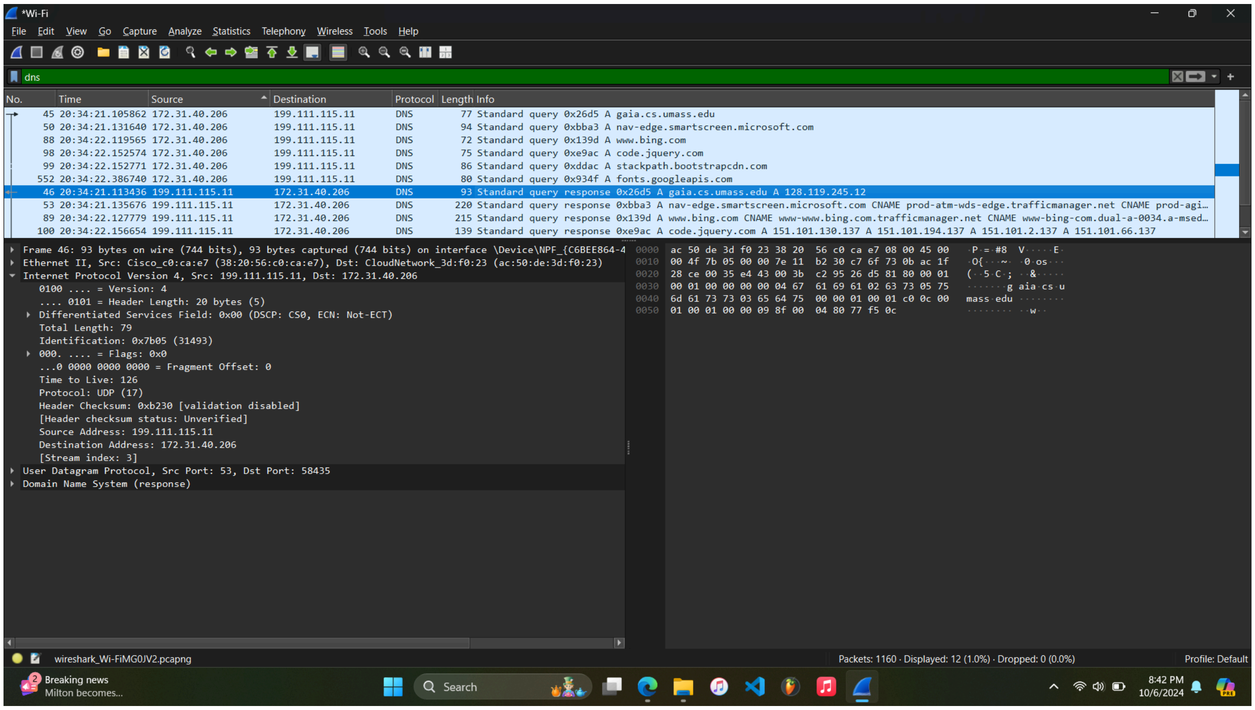
```
0000  00 00 5e 00 01 ac ac 50  de 3d f0 23 08 00 45 00   ··^····P ·=·#··E·
0010  00 3f f3 0f 00 00 80 11  38 36 ac 1f 28 ce c7 6f   ·?······ 86··(··o
0020  73 0b e4 43 00 35 00 2b  69 76 26 d5 01 00 00 01   s··C·5·+ iv&·····
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01           mass·edu ·····
```

"DNS" is not a valid protocol or protocol field.

Packets: 1160 · Displayed: 1160 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

6


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

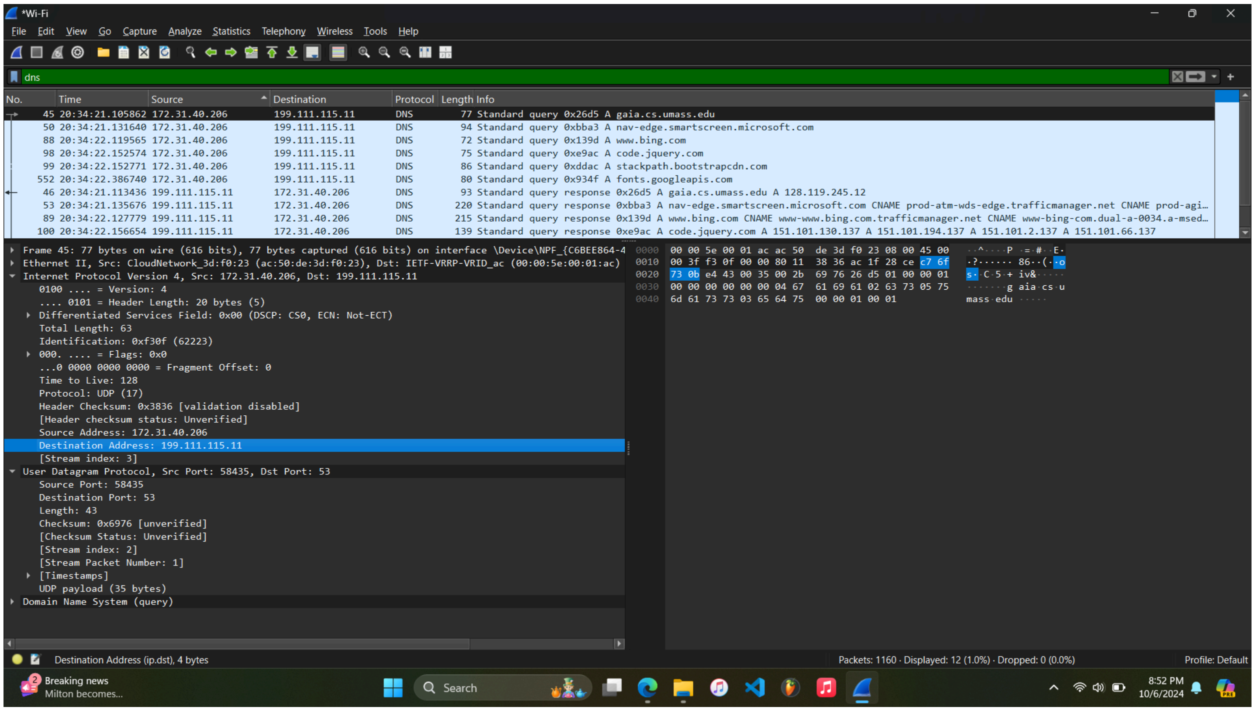
```
No.  Time            Source          Destination     Protocol Length Info
  45 20:34:21.105862 172.31.40.206   199.111.115.11  DNS       77 Standard query 0x26d5 A gaia.cs.umass.edu
  50 20:34:21.131640 172.31.40.206   199.111.115.11  DNS       94 Standard query 0xbba3 A nav-edge.smartscreen.microsoft.com
  88 20:34:22.119565 172.31.40.206   199.111.115.11  DNS       72 Standard query 0x139d A www.bing.com
  98 20:34:22.152574 172.31.40.206   199.111.115.11  DNS       75 Standard query 0xe9ac A code.jquery.com
  99 20:34:22.152771 172.31.40.206   199.111.115.11  DNS       86 Standard query 0xddac A stackpath.bootstrapcdn.com
 552 20:34:22.386740 172.31.40.206   199.111.115.11  DNS       80 Standard query 0x934f A fonts.googleapis.com
  46 20:34:21.113436 199.111.115.11  172.31.40.206   DNS       93 Standard query response 0x26d5 A gaia.cs.umass.edu A 128.119.245.12
  53 20:34:21.135676 199.111.115.11  172.31.40.206   DNS      220 Standard query response 0xbba3 A nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agi…
  89 20:34:22.127779 199.111.115.11  172.31.40.206   DNS      215 Standard query response 0x139d A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www-bing-com.dual-a-0034.a-msed…
 100 20:34:22.156654 199.111.115.11  172.31.40.206   DNS      139 Standard query response 0xe9ac A code.jquery.com A 151.101.130.137 A 151.101.194.137 A 151.101.2.137 A 151.101.66.137
```

```
▸ Frame 46: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{C6BEE864-4
▸ Ethernet II, Src: Cisco_c0:ca:e7 (38:20:56:c0:ca:e7), Dst: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23)
▾ Internet Protocol Version 4, Src: 199.111.115.11, Dst: 172.31.40.206
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0x7b05 (31493)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 126
    Protocol: UDP (17)
    Header Checksum: 0xb230 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 199.111.115.11
    Destination Address: 172.31.40.206
    [Stream index: 3]
▸ User Datagram Protocol, Src Port: 53, Dst Port: 58435
▸ Domain Name System (response)
```

```
0000  ac 50 de 3d f0 23 38 20  56 c0 ca e7 08 00 45 00   ·P·=·#8 V·····E·
0010  00 4f 7b 05 00 00 7e 11  b2 30 c7 6f 73 0b ac 1f   ·O{···~· ·0·os···
0020  28 ce 00 35 e4 43 00 3b  c2 95 26 d5 81 80 00 01   (··5·C·; ··&·····
0030  00 01 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01 c0 0c 00   mass·edu ········
0050  01 00 01 00 00 09 8f 00  04 80 77 f5 0c            ········ ··w··
```

wireshark_Wi-FiMG0JV2.pcapng   Packets: 1160 · Displayed: 12 (1.0%) · Dropped: 0 (0.0%)   Profile: Default

7, 8


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

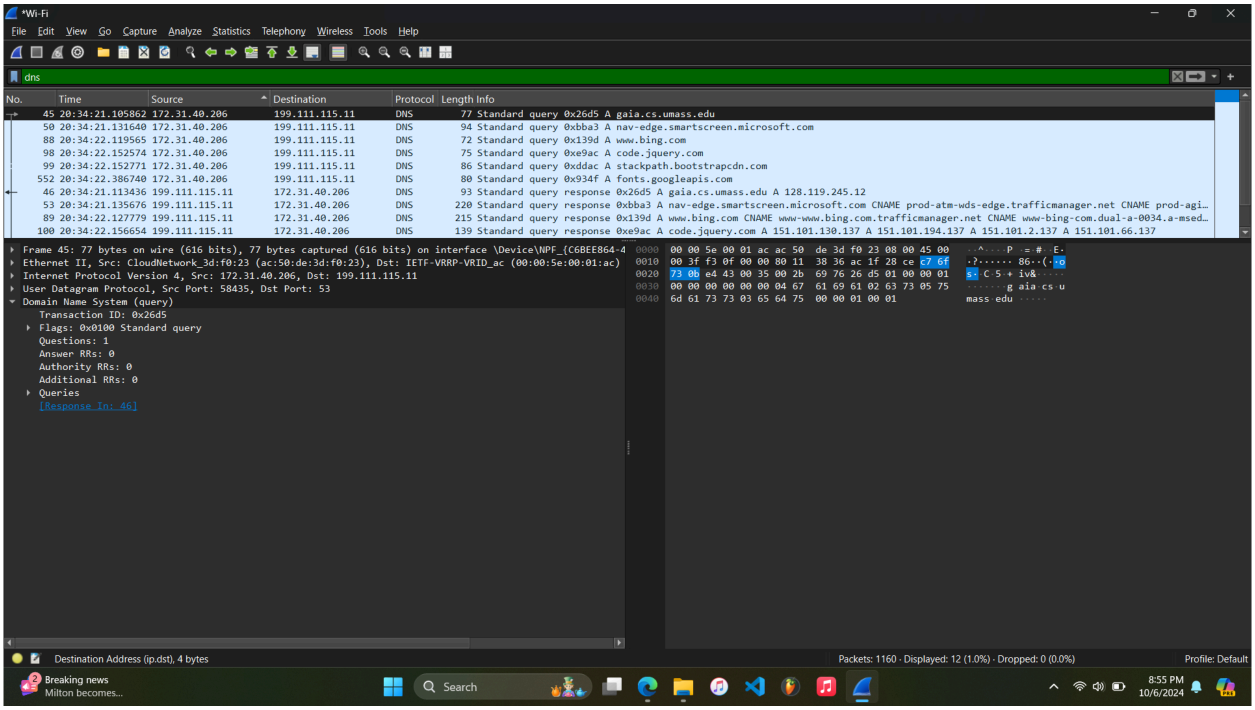
```
No.  Time            Source          Destination     Protocol Length Info
  45 20:34:21.105862 172.31.40.206   199.111.115.11  DNS       77 Standard query 0x26d5 A gaia.cs.umass.edu
  50 20:34:21.131640 172.31.40.206   199.111.115.11  DNS       94 Standard query 0xbba3 A nav-edge.smartscreen.microsoft.com
  88 20:34:22.119565 172.31.40.206   199.111.115.11  DNS       72 Standard query 0x139d A www.bing.com
  98 20:34:22.152574 172.31.40.206   199.111.115.11  DNS       75 Standard query 0xe9ac A code.jquery.com
  99 20:34:22.152771 172.31.40.206   199.111.115.11  DNS       86 Standard query 0xddac A stackpath.bootstrapcdn.com
 552 20:34:22.386740 172.31.40.206   199.111.115.11  DNS       80 Standard query 0x934f A fonts.googleapis.com
  46 20:34:21.113436 199.111.115.11  172.31.40.206   DNS       93 Standard query response 0x26d5 A gaia.cs.umass.edu A 128.119.245.12
  53 20:34:21.135676 199.111.115.11  172.31.40.206   DNS      220 Standard query response 0xbba3 A nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agi…
  89 20:34:22.127779 199.111.115.11  172.31.40.206   DNS      215 Standard query response 0x139d A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www-bing-com.dual-a-0034.a-msed…
 100 20:34:22.156654 199.111.115.11  172.31.40.206   DNS      139 Standard query response 0xe9ac A code.jquery.com A 151.101.130.137 A 151.101.194.137 A 151.101.2.137 A 151.101.66.137
```

```
▸ Frame 45: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{C6BEE864-4
▸ Ethernet II, Src: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23), Dst: IETF-VRRP-VRID_ac (00:00:5e:00:01:ac)
▾ Internet Protocol Version 4, Src: 172.31.40.206, Dst: 199.111.115.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0xf30f (62223)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x3836 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.31.40.206
    Destination Address: 199.111.115.11
    [Stream index: 3]
▾ User Datagram Protocol, Src Port: 58435, Dst Port: 53
    Source Port: 58435
    Destination Port: 53
    Length: 43
    Checksum: 0x6976 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (35 bytes)
▸ Domain Name System (query)
```

```
0000  00 00 5e 00 01 ac ac 50  de 3d f0 23 08 00 45 00   ··^····P ·=·#··E·
0010  00 3f f3 0f 00 00 80 11  38 36 ac 1f 28 ce c7 6f   ·?······ 86··(··o
0020  73 0b e4 43 00 35 00 2b  69 76 26 d5 01 00 00 01   s··C·5·+ iv&·····
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01            mass·edu ·····
```

Destination Address (ip.dst), 4 bytes   Packets: 1160 · Displayed: 12 (1.0%) · Dropped: 0 (0.0%)   Profile: Default

9


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

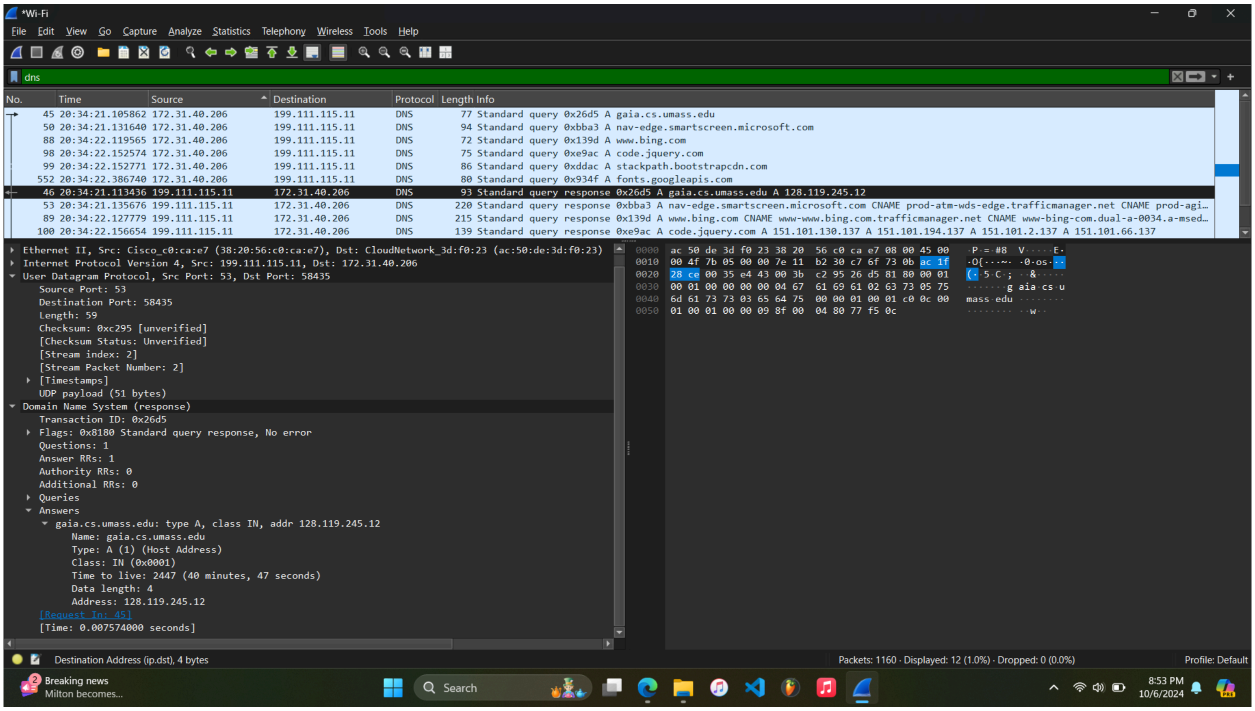
```
No.  Time             Source          Destination     Protocol Length Info
  45 20:34:21.105862 172.31.40.206   199.111.115.11  DNS      77 Standard query 0x26d5 A gaia.cs.umass.edu
  50 20:34:21.131640 172.31.40.206   199.111.115.11  DNS      94 Standard query 0xbba3 A nav-edge.smartscreen.microsoft.com
  88 20:34:22.119565 172.31.40.206   199.111.115.11  DNS      72 Standard query 0x139d A www.bing.com
  98 20:34:22.152574 172.31.40.206   199.111.115.11  DNS      75 Standard query 0xe9ac A code.jquery.com
  99 20:34:22.152771 172.31.40.206   199.111.115.11  DNS      86 Standard query 0xddac A stackpath.bootstrapcdn.com
 552 20:34:22.386740 172.31.40.206   199.111.115.11  DNS      80 Standard query 0x934f A fonts.googleapis.com
  46 20:34:21.113436 199.111.115.11  172.31.40.206   DNS      93 Standard query response 0x26d5 A gaia.cs.umass.edu A 128.119.245.12
  53 20:34:21.135676 199.111.115.11  172.31.40.206   DNS     220 Standard query response 0xbba3 A nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agi…
  89 20:34:22.127779 199.111.115.11  172.31.40.206   DNS     215 Standard query response 0x139d A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www-bing-com.dual-a-0034.a-msed…
 100 20:34:22.156654 199.111.115.11  172.31.40.206   DNS     139 Standard query response 0xe9ac A code.jquery.com A 151.101.130.137 A 151.101.194.137 A 151.101.2.137 A 151.101.66.137
```

```
> Frame 45: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{C6BEE864-4
> Ethernet II, Src: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23), Dst: IETF-VRRP-VRID_ac (00:00:5e:00:01:ac)
> Internet Protocol Version 4, Src: 172.31.40.206, Dst: 199.111.115.11
> User Datagram Protocol, Src Port: 58435, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x26d5
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 46]
```

```
0000  00 00 5e 00 01 ac ac 50  de 3d f0 23 08 00 45 00   ··^····P ·=·#··E·
0010  00 3f f3 0f 00 00 80 11  38 36 ac 1f 28 ce c7 6f   ·?······ 86··(··o
0020  73 0b e4 43 00 35 00 2b  69 76 26 d5 01 00 00 01   s··C·5·+ iv&·····
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01            mass·edu ·····
```

Destination Address (ip.dst), 4 bytes Packets: 1160 · Displayed: 12 (1.0%) · Dropped: 0 (0.0%) Profile: Default

10


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

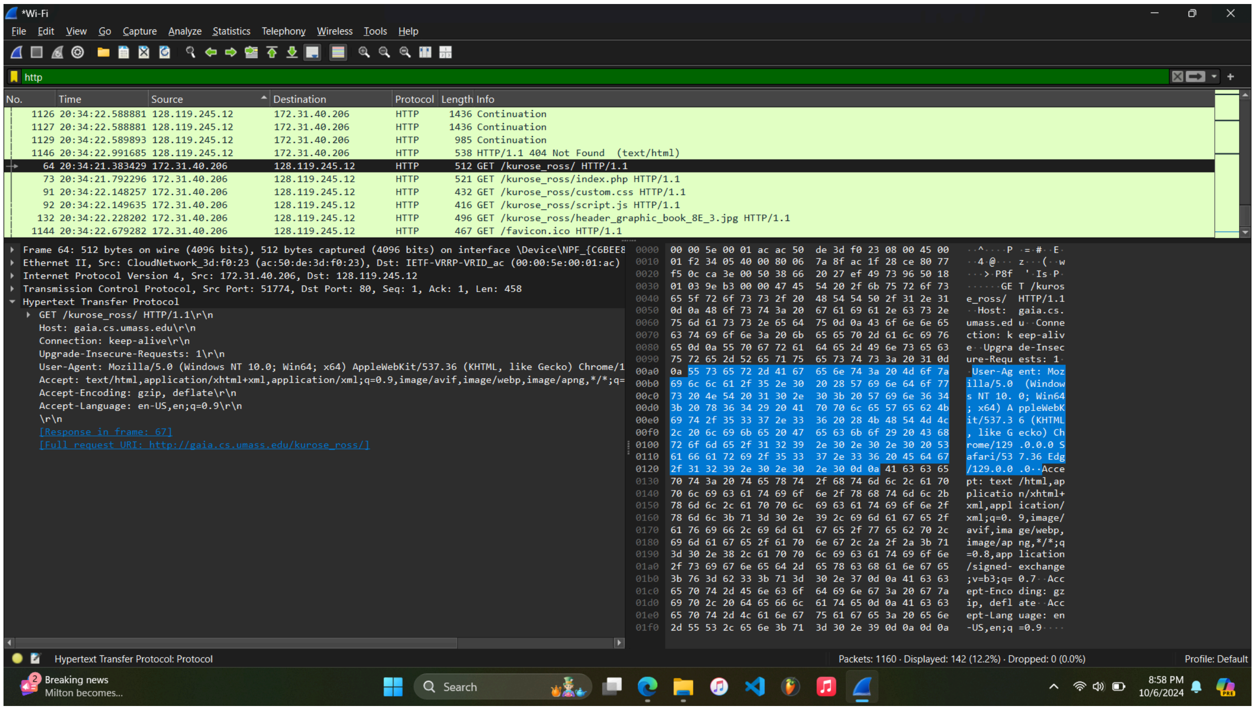
```
No.  Time             Source          Destination     Protocol Length Info
  45 20:34:21.105862 172.31.40.206   199.111.115.11  DNS      77 Standard query 0x26d5 A gaia.cs.umass.edu
  50 20:34:21.131640 172.31.40.206   199.111.115.11  DNS      94 Standard query 0xbba3 A nav-edge.smartscreen.microsoft.com
  88 20:34:22.119565 172.31.40.206   199.111.115.11  DNS      72 Standard query 0x139d A www.bing.com
  98 20:34:22.152574 172.31.40.206   199.111.115.11  DNS      75 Standard query 0xe9ac A code.jquery.com
  99 20:34:22.152771 172.31.40.206   199.111.115.11  DNS      86 Standard query 0xddac A stackpath.bootstrapcdn.com
 552 20:34:22.386740 172.31.40.206   199.111.115.11  DNS      80 Standard query 0x934f A fonts.googleapis.com
  46 20:34:21.113436 199.111.115.11  172.31.40.206   DNS      93 Standard query response 0x26d5 A gaia.cs.umass.edu A 128.119.245.12
  53 20:34:21.135676 199.111.115.11  172.31.40.206   DNS     220 Standard query response 0xbba3 A nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agi…
  89 20:34:22.127779 199.111.115.11  172.31.40.206   DNS     215 Standard query response 0x139d A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www-bing-com.dual-a-0034.a-msed…
 100 20:34:22.156654 199.111.115.11  172.31.40.206   DNS     139 Standard query response 0xe9ac A code.jquery.com A 151.101.130.137 A 151.101.194.137 A 151.101.2.137 A 151.101.66.137
```

```
> Ethernet II, Src: Cisco_c0:ca:e7 (38:20:56:c0:ca:e7), Dst: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23)
> Internet Protocol Version 4, Src: 199.111.115.11, Dst: 172.31.40.206
v User Datagram Protocol, Src Port: 53, Dst Port: 58435
    Source Port: 53
    Destination Port: 58435
    Length: 59
    Checksum: 0xc295 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 2]
  > [Timestamps]
    UDP payload (51 bytes)
v Domain Name System (response)
    Transaction ID: 0x26d5
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v gaia.cs.umass.edu: type A, class IN, addr 128.119.245.12
        Name: gaia.cs.umass.edu
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 2447 (40 minutes, 47 seconds)
        Data length: 4
        Address: 128.119.245.12
    [Request In: 45]
    [Time: 0.007574000 seconds]
```

```
0000  ac 50 de 3d f0 23 38 20  56 c0 ca e7 08 00 45 00   ·P·=·#8  V·····E·
0010  00 4f 7b 05 00 00 7e 11  b2 30 c7 6f 73 0b ac 1f   ·O{···~· ·0·os···
0020  28 ce 00 35 e4 43 00 3b  c2 95 26 d5 81 80 00 01   (··5·C·; ··&·····
0030  00 01 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01 c0 0c 00   mass·edu ········
0050  01 00 01 00 00 09 8f 00  04 80 77 f5 0c            ········ ··w··
```

Destination Address (ip.dst), 4 bytes Packets: 1160 · Displayed: 12 (1.0%) · Dropped: 0 (0.0%) Profile: Default

11


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Breaking news
Milton becomes...
Search
8:58 PM
10/6/2024

http

```
No.  Time            Source          Destination     Protocol Length Info
1126 20:34:22.588881 128.119.245.12  172.31.40.206   HTTP     1436 Continuation
1127 20:34:22.588881 128.119.245.12  172.31.40.206   HTTP     1436 Continuation
1129 20:34:22.589893 128.119.245.12  172.31.40.206   HTTP      985 Continuation
1146 20:34:22.991685 128.119.245.12  172.31.40.206   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  64 20:34:21.383429 172.31.40.206   128.119.245.12  HTTP      512 GET /kurose_ross/ HTTP/1.1
  73 20:34:21.792296 172.31.40.206   128.119.245.12  HTTP      521 GET /kurose_ross/index.php HTTP/1.1
  91 20:34:22.148257 172.31.40.206   128.119.245.12  HTTP      432 GET /kurose_ross/custom.css HTTP/1.1
  92 20:34:22.149635 172.31.40.206   128.119.245.12  HTTP      416 GET /kurose_ross/script.js HTTP/1.1
 132 20:34:22.228202 172.31.40.206   128.119.245.12  HTTP      496 GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1
1144 20:34:22.679282 172.31.40.206   128.119.245.12  HTTP      467 GET /favicon.ico HTTP/1.1
```

```
> Frame 64: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface \Device\NPF_{C6BEE8
> Ethernet II, Src: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23), Dst: IETF-VRRP-VRID_ac (00:00:5e:00:01:ac)
> Internet Protocol Version 4, Src: 172.31.40.206, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51774, Dst Port: 80, Seq: 1, Ack: 1, Len: 458
v Hypertext Transfer Protocol
  > GET /kurose_ross/ HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Response in frame: 67]
    [Full request URI: http://gaia.cs.umass.edu/kurose_ross/]
```

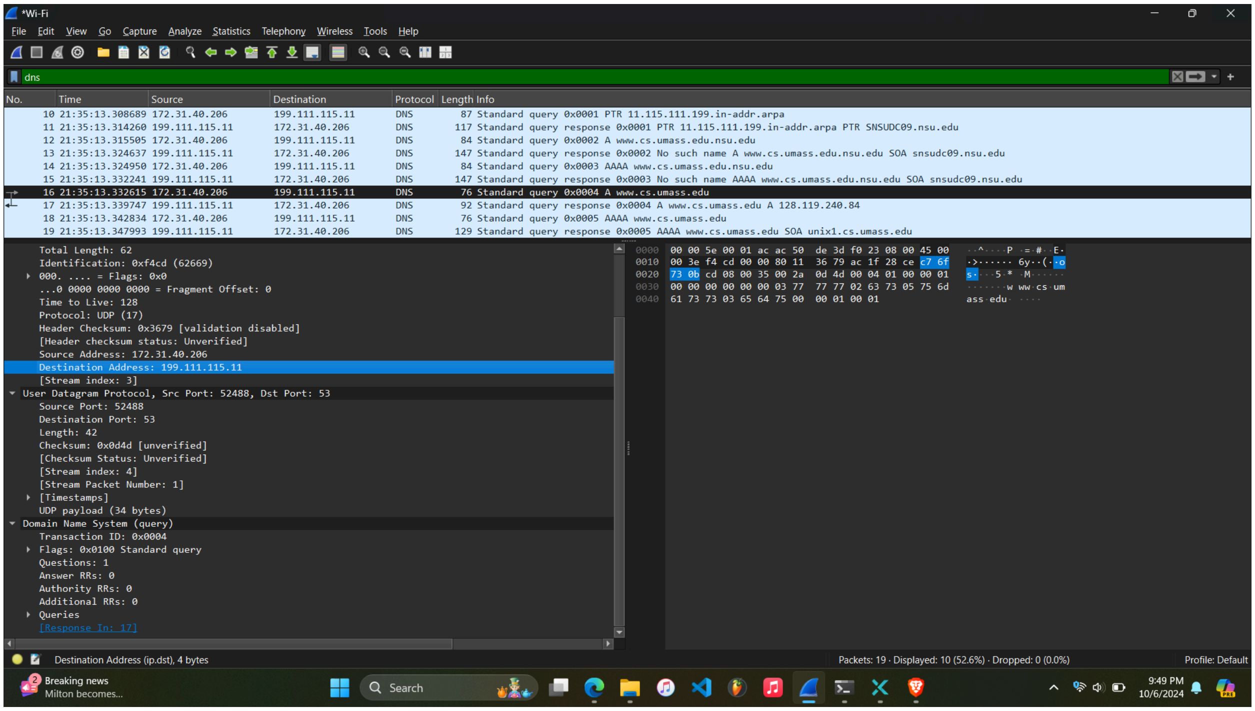
```
0000  00 00 5e 00 01 ac ac 50  de 3d f0 23 08 00 45 00   ··^····P ·=·#··E·
0010  01 f2 34 05 40 00 80 06  7a 8f ac 1f 28 ce 80 77   ··4·@··· z···(··w
0020  f5 0c ca 3e 00 50 38 66  20 27 ef 49 73 96 50 18   ···>·P8f  '·Is·P·
0030  01 03 9e b3 00 00 47 45  54 20 2f 6b 75 72 6f 73   ······GE T /kuros
0040  65 5f 72 6f 73 73 2f 20  48 54 54 50 2f 31 2e 31   e_ross/  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0060  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
0070  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
0080  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
0090  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
00a0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00b0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
00c0  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
00d0  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
00e0  69 74 2f 35 33 37 2e 33  36 20 28 4b 48 54 4d 4c   it/537.3 6 (KHTML
00f0  2c 20 6c 69 6b 65 20 47  65 63 6b 6f 29 20 43 68   , like G ecko) Ch
0100  72 6f 6d 65 2f 31 32 39  2e 30 2e 30 2e 30 20 53   rome/129 .0.0.0 S
0110  61 66 61 72 69 2f 35 33  37 2e 33 36 20 45 64 67   afari/53 7.36 Edg
0120  2f 31 32 39 2e 30 2e 30  2e 30 0d 0a 41 63 63 65   /129.0.0 .0··Acce
0130  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 61 70   pt: text /html,ap
0140  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d 6c 2b   plicatio n/xhtml+
0150  78 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   xml,appl ication/
0160  78 6d 6c 3b 71 3d 30 2e  39 2c 69 6d 61 67 65 2f   xml;q=0. 9,image/
0170  61 76 69 66 2c 69 6d 61  67 65 2f 77 65 62 70 2c   avif,ima ge/webp,
0180  69 6d 61 67 65 2f 61 70  6e 67 2c 2a 2f 2a 3b 71   image/ap ng,*/*;q
0190  3d 30 2e 38 2c 61 70 70  6c 69 63 61 74 69 6f 6e   =0.8,app lication
01a0  2f 73 69 67 6e 65 64 2d  65 78 63 68 61 6e 67 65   /signed- exchange
01b0  3b 76 3d 62 33 3b 71 3d  30 2e 37 0d 0a 41 63 63   ;v=b3;q= 0.7··Acc
01c0  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 67 7a   ept-Enco ding: gz
01d0  69 70 2c 20 64 65 66 6c  61 74 65 0d 0a 41 63 63   ip, defl ate··Acc
01e0  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
01f0  2d 55 53 2c 65 6e 3b 71  3d 30 2e 39 0d 0a 0d 0a   -US,en;q =0.9····
```

Hypertext Transfer Protocol: Protocol

Packets: 1160 · Displayed: 142 (12.2%) · Dropped: 0 (0.0%)

Profile: Default

12-14


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Breaking news
Milton becomes...
Search
9:49 PM
10/6/2024

dns

```
No. Time            Source          Destination     Protocol Length Info
 10 21:35:13.308689 172.31.40.206   199.111.115.11  DNS       87 Standard query 0x0001 PTR 11.115.111.199.in-addr.arpa
 11 21:35:13.314260 199.111.115.11  172.31.40.206   DNS      117 Standard query response 0x0001 PTR 11.115.111.199.in-addr.arpa PTR SNSUDC09.nsu.edu
 12 21:35:13.315505 172.31.40.206   199.111.115.11  DNS       84 Standard query 0x0002 A www.cs.umass.edu.nsu.edu
 13 21:35:13.324637 199.111.115.11  172.31.40.206   DNS      147 Standard query response 0x0002 No such name A www.cs.umass.edu.nsu.edu SOA snsudc09.nsu.edu
 14 21:35:13.324950 172.31.40.206   199.111.115.11  DNS       84 Standard query 0x0003 AAAA www.cs.umass.edu.nsu.edu
 15 21:35:13.332241 199.111.115.11  172.31.40.206   DNS      147 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.nsu.edu SOA snsudc09.nsu.edu
 16 21:35:13.332615 172.31.40.206   199.111.115.11  DNS       76 Standard query 0x0004 A www.cs.umass.edu
 17 21:35:13.339747 199.111.115.11  172.31.40.206   DNS       92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
 18 21:35:13.342834 172.31.40.206   199.111.115.11  DNS       76 Standard query 0x0005 AAAA www.cs.umass.edu
 19 21:35:13.347993 199.111.115.11  172.31.40.206   DNS      129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
```

```
    Total Length: 62
    Identification: 0xf4cd (62669)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x3679 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.31.40.206
    Destination Address: 199.111.115.11
    [Stream index: 3]
v User Datagram Protocol, Src Port: 52488, Dst Port: 53
    Source Port: 52488
    Destination Port: 53
    Length: 42
    Checksum: 0x0d4d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (34 bytes)
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 17]
```

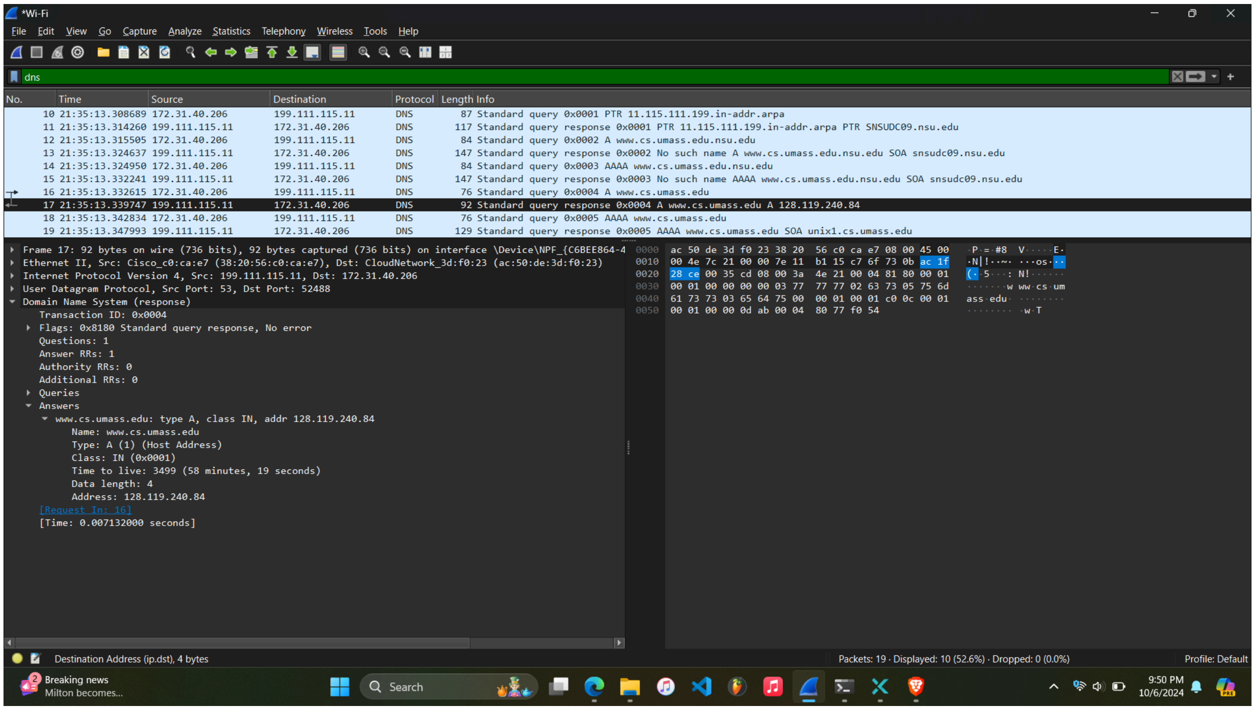
```
0000  00 00 5e 00 01 ac ac 50  de 3d f0 23 08 00 45 00   ··^····P ·=·#··E·
0010  00 3e f4 cd 00 00 80 11  36 79 ac 1f 28 ce c7 6f   ·>······ 6y··(··o
0020  73 0b cd 08 00 35 00 2a  0d 4d 00 04 01 00 00 01   s····5·* ·M······
0030  00 00 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01               ass·edu· ····
```

Destination Address (ip.dst), 4 bytes

Packets: 19 · Displayed: 10 (52.6%) · Dropped: 0 (0.0%)

Profile: Default

15


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Breaking news
Milton becomes...
Search
9:50 PM
10/6/2024

```
No.  Time             Source           Destination      Protocol Length Info
  10 21:35:13.308689 172.31.40.206    199.111.115.11   DNS       87 Standard query 0x0001 PTR 11.115.111.199.in-addr.arpa
  11 21:35:13.314260 199.111.115.11   172.31.40.206    DNS      117 Standard query response 0x0001 PTR 11.115.111.199.in-addr.arpa PTR SNSUDC09.nsu.edu
  12 21:35:13.315505 172.31.40.206    199.111.115.11   DNS       84 Standard query 0x0002 A www.cs.umass.edu.nsu.edu
  13 21:35:13.324637 199.111.115.11   172.31.40.206    DNS      147 Standard query response 0x0002 No such name A www.cs.umass.edu.nsu.edu SOA snsudc09.nsu.edu
  14 21:35:13.324950 172.31.40.206    199.111.115.11   DNS       84 Standard query 0x0003 AAAA www.cs.umass.edu.nsu.edu
  15 21:35:13.332241 199.111.115.11   172.31.40.206    DNS      147 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.nsu.edu SOA snsudc09.nsu.edu
  16 21:35:13.332615 172.31.40.206    199.111.115.11   DNS       76 Standard query 0x0004 A www.cs.umass.edu
  17 21:35:13.339747 199.111.115.11   172.31.40.206    DNS       92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
  18 21:35:13.342834 172.31.40.206    199.111.115.11   DNS       76 Standard query 0x0005 AAAA www.cs.umass.edu
  19 21:35:13.347993 199.111.115.11   172.31.40.206    DNS      129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
```

```
Frame 17: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{C6BEE864-4
Ethernet II, Src: Cisco_c0:ca:e7 (38:20:56:c0:ca:e7), Dst: CloudNetwork_3d:f0:23 (ac:50:de:3d:f0:23)
Internet Protocol Version 4, Src: 199.111.115.11, Dst: 172.31.40.206
User Datagram Protocol, Src Port: 53, Dst Port: 52488
Domain Name System (response)
  Transaction ID: 0x0004
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
    www.cs.umass.edu: type A, class IN, addr 128.119.240.84
      Name: www.cs.umass.edu
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 3499 (58 minutes, 19 seconds)
      Data length: 4
      Address: 128.119.240.84
  [Request In: 16]
  [Time: 0.007132000 seconds]
```

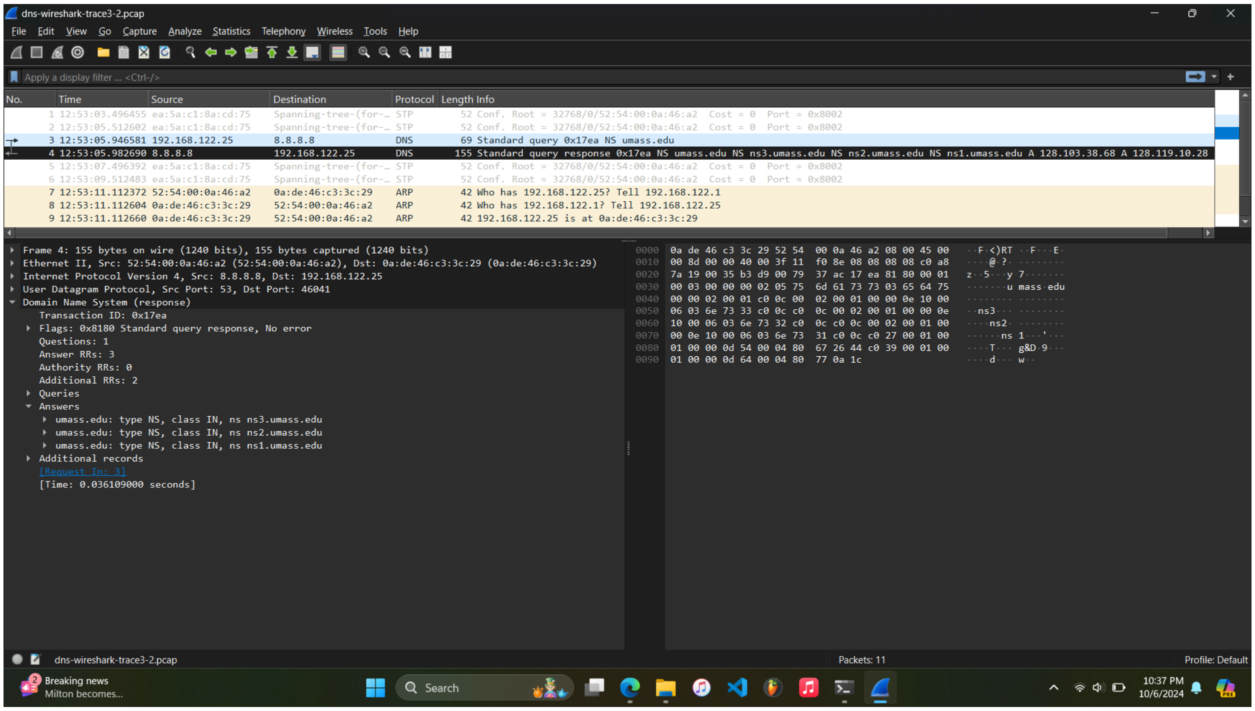
```
0000  ac 50 de 3d f0 23 38 20  56 c0 ca e7 08 00 45 00   ·P·=·#8 V·····E·
0010  00 4e 7c 21 00 00 7e 11  b1 15 c7 6f 73 0b ac 1f   ·N|!··~· ···os···
0020  28 ce 00 35 cd 08 00 3a  4e 21 00 04 81 80 00 01   (··5···: N!······
0030  00 01 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01 c0 0c 00 01   ass·edu· ········
0050  00 01 00 00 0d ab 00 04  80 77 f0 54               ········ ·w·T
```

Destination Address (ip.dst), 4 bytes

Packets: 19 · Displayed: 10 (52.6%) · Dropped: 0 (0.0%)

Profile: Default

16, 17,18


dns-wireshark-trace3-2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Breaking news
Milton becomes...
Search
10:37 PM
10/6/2024

```
No.  Time            Source             Destination          Protocol Length Info
   1 12:53:03.496455 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   2 12:53:05.512602 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   3 12:53:05.946581 192.168.122.25     8.8.8.8              DNS       69 Standard query 0x17ea NS umass.edu
   4 12:53:05.982690 8.8.8.8            192.168.122.25       DNS      155 Standard query response 0x17ea NS umass.edu NS ns3.umass.edu NS ns2.umass.edu NS ns1.umass.edu A 128.103.38.68 A 128.119.10.28
   5 12:53:07.496392 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   6 12:53:09.512483 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   7 12:53:11.112372 52:54:00:0a:46:a2  0a:de:46:c3:3c:29    ARP       42 Who has 192.168.122.25? Tell 192.168.122.1
   8 12:53:11.112604 0a:de:46:c3:3c:29  52:54:00:0a:46:a2    ARP       42 Who has 192.168.122.1? Tell 192.168.122.25
   9 12:53:11.112660 0a:de:46:c3:3c:29  52:54:00:0a:46:a2    ARP       42 192.168.122.25 is at 0a:de:46:c3:3c:29
```

```
Frame 4: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
Ethernet II, Src: 52:54:00:0a:46:a2 (52:54:00:0a:46:a2), Dst: 0a:de:46:c3:3c:29 (0a:de:46:c3:3c:29)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.122.25
User Datagram Protocol, Src Port: 53, Dst Port: 46041
Domain Name System (response)
  Transaction ID: 0x17ea
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 2
  Queries
  Answers
    umass.edu: type NS, class IN, ns ns3.umass.edu
    umass.edu: type NS, class IN, ns ns2.umass.edu
    umass.edu: type NS, class IN, ns ns1.umass.edu
  Additional records
  [Request In: 3]
  [Time: 0.036109000 seconds]
```

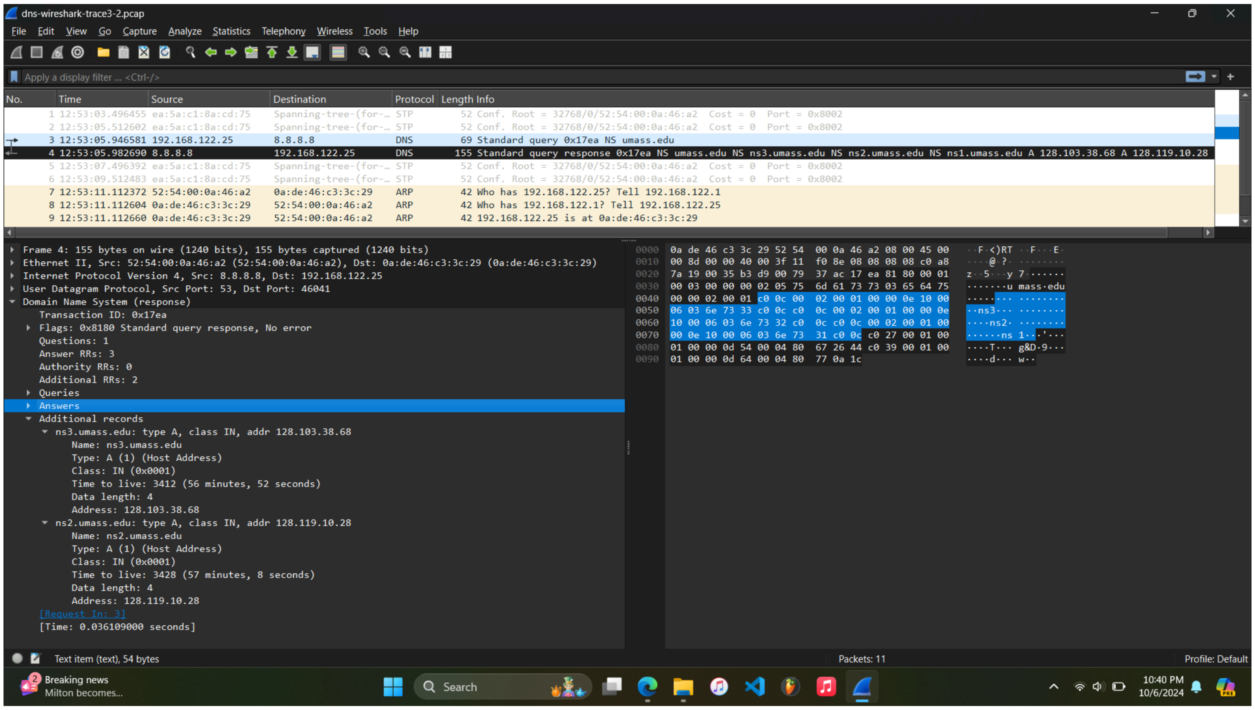
```
0000  0a de 46 c3 3c 29 52 54  00 0a 46 a2 08 00 45 00   ··F·<)RT ··F···E·
0010  00 8d 00 00 40 00 3f 11  f0 8e 08 08 08 08 c0 a8   ····@·?· ········
0020  7a 19 00 35 b3 d9 00 79  37 ac 17 ea 81 80 00 01   z··5···y 7·······
0030  00 03 00 00 00 02 05 75  6d 61 73 73 03 65 64 75   ·······u mass·edu
0040  00 00 02 00 01 c0 0c 00  02 00 01 00 00 0e 10 00   ········ ········
0050  06 03 6e 73 33 c0 0c c0  0c 00 02 00 01 00 00 0e   ··ns3··· ········
0060  10 00 06 03 6e 73 32 c0  0c c0 0c 00 02 00 01 00   ····ns2· ········
0070  00 0e 10 00 06 03 6e 73  31 c0 0c c0 27 00 01 00   ······ns 1···'···
0080  01 00 00 0d 54 00 04 80  67 26 44 c0 39 00 01 00   ····T··· g&D·9···
0090  01 00 00 0d 64 00 04 80  77 0a 1c                  ····d··· w··
```

dns-wireshark-trace3-2.pcap

Packets: 11

Profile: Default

18



```
No.  Time            Source             Destination           Protocol Length Info
   1 12:53:03.496455 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   2 12:53:05.512602 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   3 12:53:05.946581 192.168.122.25     8.8.8.8              DNS       69 Standard query 0x17ea NS umass.edu
   4 12:53:05.982690 8.8.8.8            192.168.122.25       DNS      155 Standard query response 0x17ea NS umass.edu NS ns3.umass.edu NS ns2.umass.edu NS ns1.umass.edu A 128.103.38.68 A 128.119.10.28
   5 12:53:07.496392 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   6 12:53:09.512483 ea:5a:c1:8a:cd:75  Spanning-tree-(for-… STP       52 Conf. Root = 32768/0/52:54:00:0a:46:a2  Cost = 0  Port = 0x8002
   7 12:53:11.112372 52:54:00:0a:46:a2  0a:de:46:c3:3c:29    ARP       42 Who has 192.168.122.25? Tell 192.168.122.1
   8 12:53:11.112604 0a:de:46:c3:3c:29  52:54:00:0a:46:a2    ARP       42 Who has 192.168.122.1? Tell 192.168.122.25
   9 12:53:11.112660 0a:de:46:c3:3c:29  52:54:00:0a:46:a2    ARP       42 192.168.122.25 is at 0a:de:46:c3:3c:29
```

```
> Frame 4: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
> Ethernet II, Src: 52:54:00:0a:46:a2 (52:54:00:0a:46:a2), Dst: 0a:de:46:c3:3c:29 (0a:de:46:c3:3c:29)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.122.25
> User Datagram Protocol, Src Port: 53, Dst Port: 46041
v Domain Name System (response)
    Transaction ID: 0x17ea
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 2
  > Queries
  > Answers
  v Additional records
    v ns3.umass.edu: type A, class IN, addr 128.103.38.68
          Name: ns3.umass.edu
          Type: A (1) (Host Address)
          Class: IN (0x0001)
          Time to live: 3412 (56 minutes, 52 seconds)
          Data length: 4
          Address: 128.103.38.68
    v ns2.umass.edu: type A, class IN, addr 128.119.10.28
          Name: ns2.umass.edu
          Type: A (1) (Host Address)
          Class: IN (0x0001)
          Time to live: 3428 (57 minutes, 8 seconds)
          Data length: 4
          Address: 128.119.10.28
    [Request In: 3]
    [Time: 0.036109000 seconds]
```

```
0000  0a de 46 c3 3c 29 52 54  00 0a 46 a2 08 00 45 00   ··F·<)RT ··F···E·
0010  00 8d 00 00 40 00 3f 11  f0 8e 08 08 08 08 c0 a8   ····@·?· ········
0020  7a 19 00 35 b3 d9 00 79  37 ac 17 ea 81 80 00 01   z··5···y 7·······
0030  00 03 00 00 00 02 05 75  6d 61 73 73 03 65 64 75   ·······u mass·edu
0040  00 00 02 00 01 c0 0c 00  02 00 01 00 00 0e 10 00   ········ ········
0050  06 03 6e 73 33 c0 0c c0  0c 00 02 00 01 00 00 0e   ··ns3··· ········
0060  10 00 06 03 6e 73 32 c0  0c c0 0c 00 02 00 01 00   ····ns2· ········
0070  00 0e 10 00 06 03 6e 73  31 c0 0c c0 27 00 01 00   ······ns 1···'···
0080  01 00 00 0d 54 00 04 80  67 26 44 c0 39 00 01 00   ····T··· g&D·9···
0090  01 00 00 0d 64 00 04 80  77 0a 1c                  ····d··· w··
```

Text item (text), 54 bytes   Packets: 11   Profile: Default