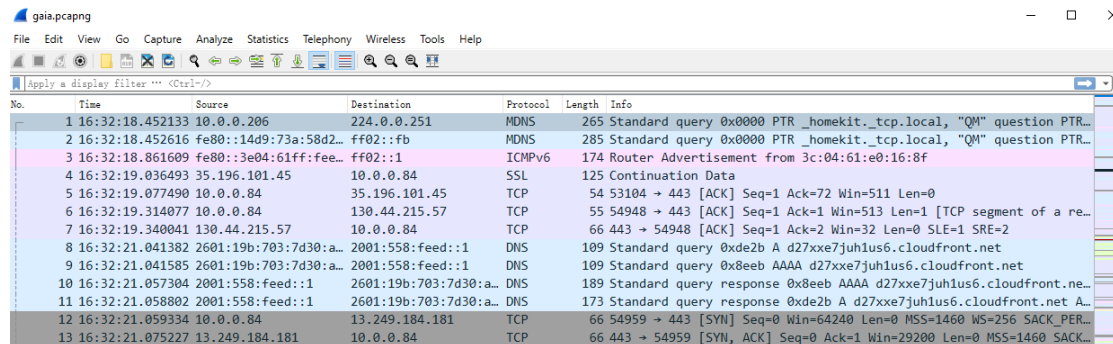


CS 655 Computer Network -- Lab1 Introduction to Wireshark

Ziqi Tan U 88387934

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

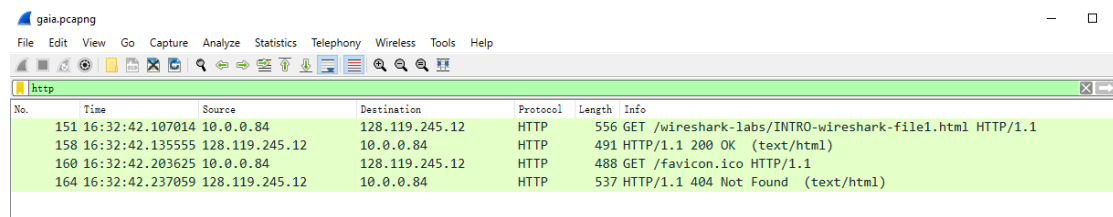


The screenshot shows the Wireshark interface with the 'packet-listing' pane selected. The display filter is empty. The table lists 13 captured packets with their respective protocols: MDNS, ICMPv6, SSL, TCP, and DNS.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|------------------------|------------------------|----------|--------|---|
| 1 | 16:32:18.452133 | 10.0.0.206 | 224.0.0.251 | MDNS | 265 | Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR... |
| 2 | 16:32:18.452616 | fe80::14d9:73a:58d2... | ff02::fb | MDNS | 285 | Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR... |
| 3 | 16:32:18.861609 | fe80::3e04:61ff:fee... | ff02::1 | ICMPv6 | 174 | Router Advertisement from 3c:04:61:e0:16:8f |
| 4 | 16:32:19.036493 | 35.196.101.45 | 10.0.0.84 | SSL | 125 | Continuation Data |
| 5 | 16:32:19.077490 | 10.0.0.84 | 35.196.101.45 | TCP | 54 | 53104 → 443 [ACK] Seq=1 Ack=72 Win=511 Len=0 |
| 6 | 16:32:19.314077 | 10.0.0.84 | 130.44.215.57 | TCP | 55 | 54948 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a re... |
| 7 | 16:32:19.340041 | 130.44.215.57 | 10.0.0.84 | TCP | 66 | 443 → 54948 [ACK] Seq=1 Ack=2 Win=32 Len=0 SLE=1 SRE=2 |
| 8 | 16:32:21.041382 | 2601:19b:703:7d30:a... | 2001:558:feed::1 | DNS | 109 | Standard query 0xde2b A d27xxe7juh1us6.cloudfront.net |
| 9 | 16:32:21.041585 | 2601:19b:703:7d30:a... | 2001:558:feed::1 | DNS | 109 | Standard query 0x8eeb AAAA d27xxe7juh1us6.cloudfront.net |
| 10 | 16:32:21.057304 | 2001:558:feed::1 | 2601:19b:703:7d30:a... | DNS | 189 | Standard query response 0x8eeb AAAA d27xxe7juh1us6.cloudfront.net |
| 11 | 16:32:21.058802 | 2001:558:feed::1 | 2601:19b:703:7d30:a... | DNS | 173 | Standard query response 0xde2b A d27xxe7juh1us6.cloudfront.net A... |
| 12 | 16:32:21.059334 | 10.0.0.84 | 13.249.184.181 | TCP | 66 | 54959 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER... |
| 13 | 16:32:21.075227 | 13.249.184.181 | 10.0.0.84 | TCP | 66 | 443 → 54959 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK... |

As we can see, MDNS, ICMP, SSL, TCP, DNS and TCP are shown in the screenshot.

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?



The screenshot shows the Wireshark interface with the 'packet-listing' pane selected. The display filter is set to 'http'. The table lists 4 HTTP packets: a GET request, an OK response, another GET request, and a Not Found response.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|----------------|----------------|----------|--------|---|
| 151 | 16:32:42.107014 | 10.0.0.84 | 128.119.245.12 | HTTP | 556 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 158 | 16:32:42.135555 | 128.119.245.12 | 10.0.0.84 | HTTP | 491 | HTTP/1.1 200 OK (text/html) |
| 160 | 16:32:42.203625 | 10.0.0.84 | 128.119.245.12 | HTTP | 488 | GET /favicon.ico HTTP/1.1 |
| 164 | 16:32:42.237059 | 128.119.245.12 | 10.0.0.84 | HTTP | 537 | HTTP/1.1 404 Not Found (text/html) |

It takes 0.028541 second.

3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?

gaia.cs.umass.edu: 128.119.245.12

My computer: 10.0.0.84

4. Print the two HTTP messages (GET and OK) referred to in question 2 above.

```
No.      Time      Source      Destination      Protocol Length Info
 151 16:32:42.107014 10.0.0.84      128.119.245.12      HTTP      556      GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 151: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-
B549-CE934C3E04AA}, id 0
Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: ARRISGro_e0:16:8f (3c:04:61:e0:16:8f)
Internet Protocol Version 4, Src: 10.0.0.84, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54961, Dst Port: 80, Seq: 1, Ack: 1, Len: 502
Hypertext Transfer Protocol
```

```
No.      Time      Source      Destination      Protocol Length Info
 158 16:32:42.135555 128.119.245.12 10.0.0.84      HTTP      491      HTTP/1.1 200 OK (text/html)
Frame 158: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-
B549-CE934C3E04AA}, id 0
Ethernet II, Src: ARRISGro_e0:16:8f (3c:04:61:e0:16:8f), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.84
Transmission Control Protocol, Src Port: 80, Dst Port: 54961, Seq: 1, Ack: 503, Len: 437
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```