

Comp 2322 Computer Networking

Lab 1: Wireshark Introduction

Student Name: HE YIYANG

Student ID:22100143D

Q1.

The image shows a Wireshark packet capture of network traffic. The packet list on the left shows a sequence of packets including ARP, DNS, and HTTP. The packet details pane on the right shows the structure of an HTTP GET request. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

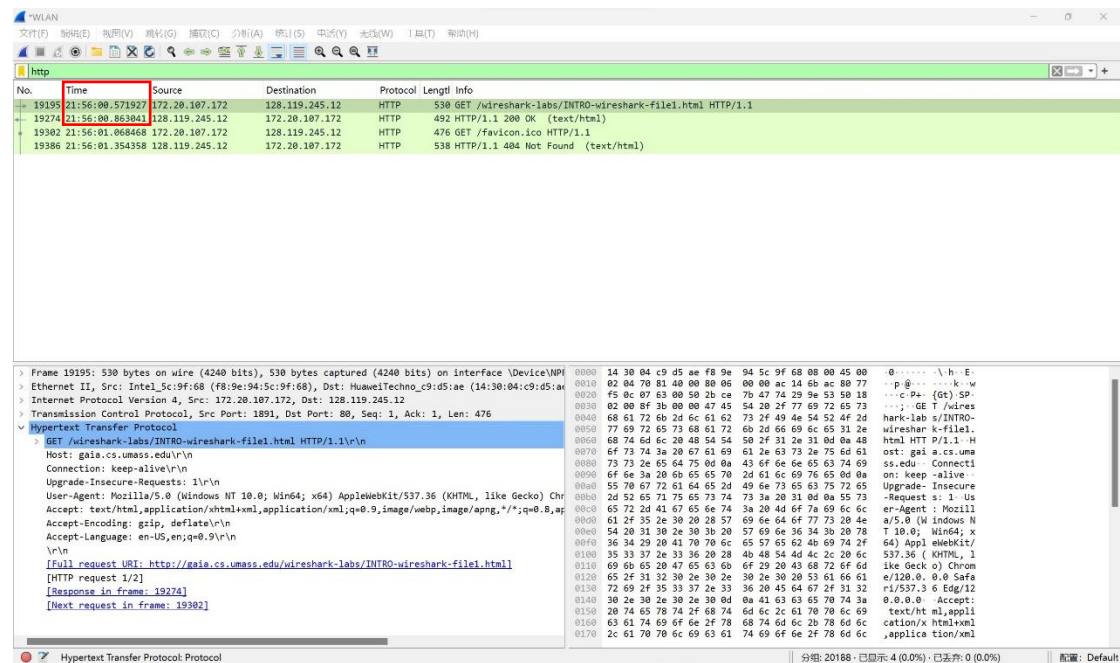
No.	Time	Source	Destination	Protocol	Length	Info
19278	21:56:00.983292	172.20.187.172	128.119.245.12	TCP	54	1891 → 80 [ACK] Seq=477 Ack=439 Win=130560 Len=0
19279	21:56:00.966258	Se:f3:d9:16:10:79	Broadcast	RARP	60	who is ff:ff:ff:ff:ff:ff? Tell Se:f3:d9:16:10:79
19280	21:56:00.966265	172.20.51.102	224.0.0.251	MDNS	109	Standard query 0x0000 TXT Yugeeee 的ipadddd (2)._companion-link_tcp.local, "QM" question
19281	21:56:00.966265	172.20.104.206	172.20.127.255	NBNS	92	Name query NB WPAD<00>
19282	21:56:00.966265	172.20.104.206	224.0.0.252	LUMNR	64	Standard query 0xe7f0 A wpad
19283	21:56:00.966266	172.20.106.7	172.20.127.255	NBNS	92	Name query NB FILE<20>
19284	21:56:00.966266	172.20.73.252	224.0.0.251	MDNS	143	Standard query 0x0000 ANY iPad.local, "QM" question AAAA fe80::1483:f57:cd8d:9b00 A 172.20.73.252 OPT
19285	21:56:00.966266	172.20.74.30	224.0.0.251	MDNS	89	Standard query 0x0000 A Android.local, "QM" question A 172.20.66.42
19286	21:56:00.966267	172.20.107.255	224.0.0.251	MDNS	557	Standard query response 0x0000 TXT PTR 类文的iPad_rdlink_tcp.local PTR 类文的iPad_companion-link_tcp.local TXT, _
19287	21:56:00.966271	172.20.74.101	239.255.255.250	SSDP	456	NOTIFY * HTTP/1.1
19288	21:56:00.966271	172.20.107.53	224.0.0.251	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _airplay_tcp.local PTR Red Hall_iirplay_tcp.local PTR _raop...
19289	21:56:00.966272	172.20.105.253	224.0.0.251	MDNS	579	Standard query response 0x0000 PTR 叶梦翔的 iPad (2)._rdlink_tcp.local TXT PTR 叶梦翔的 iPad (2)._companion-link_t...
19290	21:56:00.966272	172.20.33.121	224.0.0.251	MDNS	885	Standard query response 0x0000 PTR Chong's MacBook Air._airplay_tcp.local PTR Chong's MacBook Air._companion-link...
19291	21:56:00.966273	172.20.108.126	224.0.0.251	MDNS	333	Standard query response 0x0000 PTR hippo的iPad_rdlink_tcp.local TXT, cache flush SRV, cache flush 0 0 49154 h...
19292	21:56:00.966273	172.20.76.70	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19293	21:56:00.966273	172.20.74.248	224.0.0.251	MDNS	88	Standard query response 0x0000 A, cache flush 172.20.74.248
19294	21:56:00.966273	172.20.108.105	224.0.0.251	MDNS	140	Standard query 0x0000 ANY 31:AA:EA:58:BF:06@Blue Hall._raop_tcp.local, "QU" question SRV 0 0 51040 es-31AAEA58BF06...
19295	21:56:00.966274	172.20.75.36	224.0.0.251	MDNS	81	Standard query response 0x0000 PTR _ezcvs_pro_tcp.local, "QM" question
19296	21:56:00.966274	172.20.48.105	224.0.0.251	MDNS	339	Standard query response 0x0000 PTR Pak Yan的iPad_rdlink_tcp.local TXT, cache flush SRV, cache flush 0 0 49153...

Frame 19195: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on Interface \Device\NPF...
Ethernet II, Src: Intel_5c:9f:68 (f8:9e:94:5c:9f:68), Dst: HuaweiTechno_c9:d5:ae (14:30:04:c9:d5:ae)
Internet Protocol Version 4, Src: 172.20.107.172, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1891, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html 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/100.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 19274]
[Next request in frame: 19302]

1. TCP 2. RARP 3. MDNS

Q2.

Method1:



Timestamp of HTTP GET is 21:56:00.571927

Timestamp of HTTP OK is 21:56:00.863041

Time Taken = 21:56:00.863041 – 21:56:00.571927 = 0.291114s

Method2:

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.291114000 seconds]

[Request in frame: 19195]

[Next request in frame: 19302]

[Next response in frame: 19386]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Time request is shown in the Hypertext Transfer Protocol of HTTP OK

Q3.

The image shows a Wireshark capture of network traffic on the 'http' filter. The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
19195	21:56:00.571927	172.20.107.172	128.119.245.12	HTTP	530	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
19274	21:56:00.863041	128.119.245.12	172.20.107.172	HTTP	492	HTTP/1.1 200 OK (text/html)
19302	21:56:01.068468	172.20.107.172	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
19386	21:56:01.354358	128.119.245.12	172.20.107.172	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for the selected packet (No. 19195) shows the following structure:

- Frame 19195: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF...
- Ethernet II, Src: Intel_5c:9f:68 (f8:9e:94:5c:9f:68), Dst: HuaweiTechno_c9:d5:ae (14:30:04:c9:d5:ae)
- Internet Protocol Version 4, Src: 172.20.107.172, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 1891, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
- Hypertext Transfer Protocol
 - GET /wireshark-labs/INTRO-wireshark-file1.html 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/120.0.0.0 Safari/537.36 Edg/120.0.0.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
 - [HTTP request 1/2]
 - [Response in frame: 19274]
 - [Next request in frame: 19302]

The packet bytes pane shows the raw data in hexadecimal and ASCII.

The Internet address of the gaia.cs.umass.edu is the Destination of HTTP GET, which is 128.119.245.12

The Internet address of my computer is the Source of HTTP OK, which is 172.20.107.172

Q4.

The last printed trace file shows the two HTTP messages

```
No.      Time                Source                Destination            Protocol Length Info
19195 21:56:00.571927    172.20.107.172        128.119.245.12        HTTP 530 GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 19195: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{438E97CA-A6FF-4D1D-B0ED-
A35C8A4C4FF}, id 0
Ethernet II, Src: Intel_5c:9f:68 (f8:9e:94:5c:9f:68), Dst: HuaweiTechno_c9:d5:ae (14:30:04:c9:d5:ae)
Internet Protocol Version 4, Src: 172.20.107.172, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1891, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html 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/120.0.0.0 Safari/537.36 Edg/
120.0.0.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  [HTTP request 1/2]
  [Response in frame: 19274]
  [Next request in frame: 19302]
No.      Time                Source                Destination            Protocol Length Info
19274 21:56:00.863041    128.119.245.12        172.20.107.172        HTTP 492 HTTP/1.1 200 OK (text/html)
Frame 19274: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{438E97CA-A6FF-4D1D-B0ED-
A35C8A4C4FF}, id 0
Ethernet II, Src: HuaweiTechno_c9:d5:ae (14:30:04:c9:d5:ae), Dst: Intel_5c:9f:68 (f8:9e:94:5c:9f:68)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.107.172
Transmission Control Protocol, Src Port: 80, Dst Port: 1891, Seq: 1, Ack: 477, Len: 438
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 26 Jan 2024 13:56:01 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Fri, 26 Jan 2024 06:59:01 GMT\r\n
  ETag: "51-60fd3d4b71aab"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 81\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.291114000 seconds]
  [Request in frame: 19195]
  [Next request in frame: 19302]
  [Next response in frame: 19386]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
Line-based text data: text/html (3 lines)
```