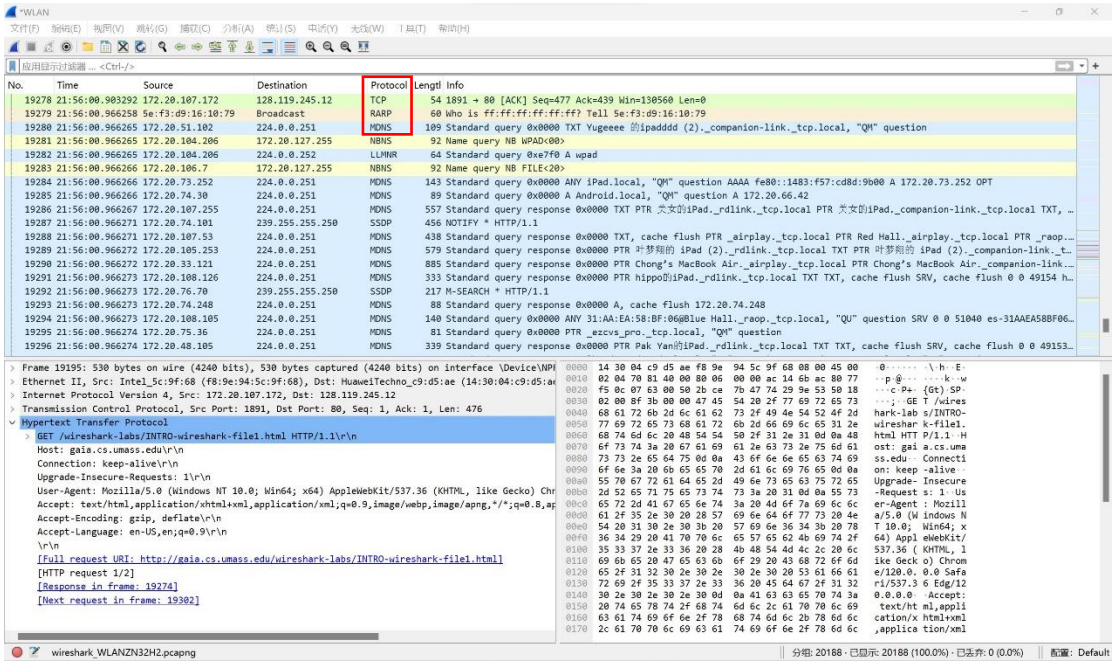
Comp 2322 Computer Networking

Lab 1: Wireshark Introduction

Student Name: HE YIYANG

Student ID:22100143D

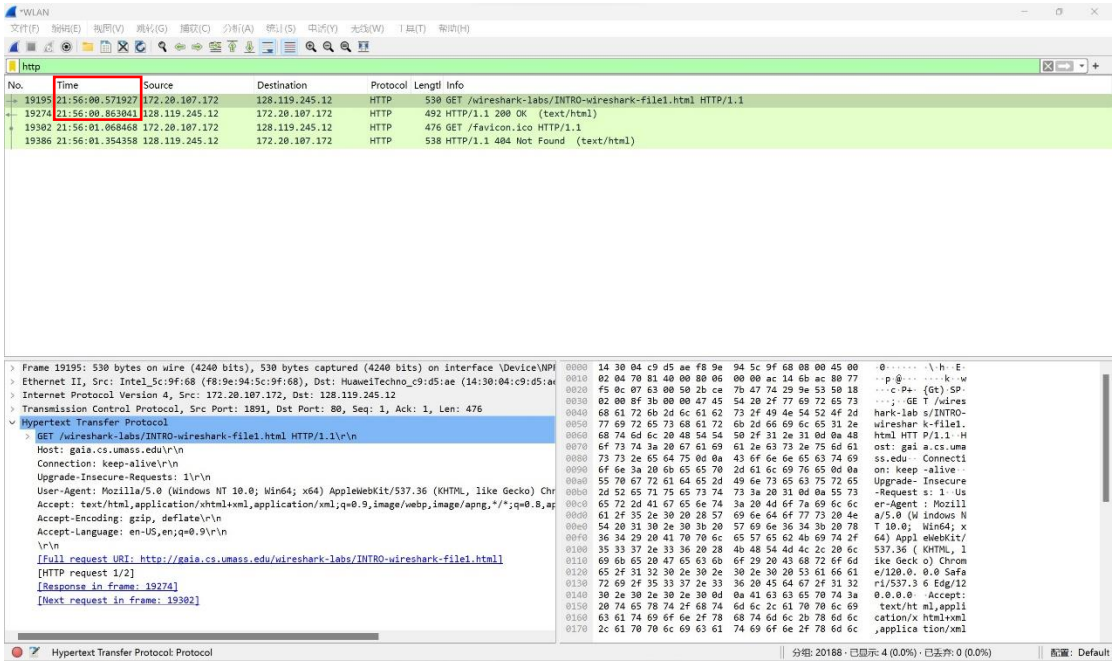
Q1.



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

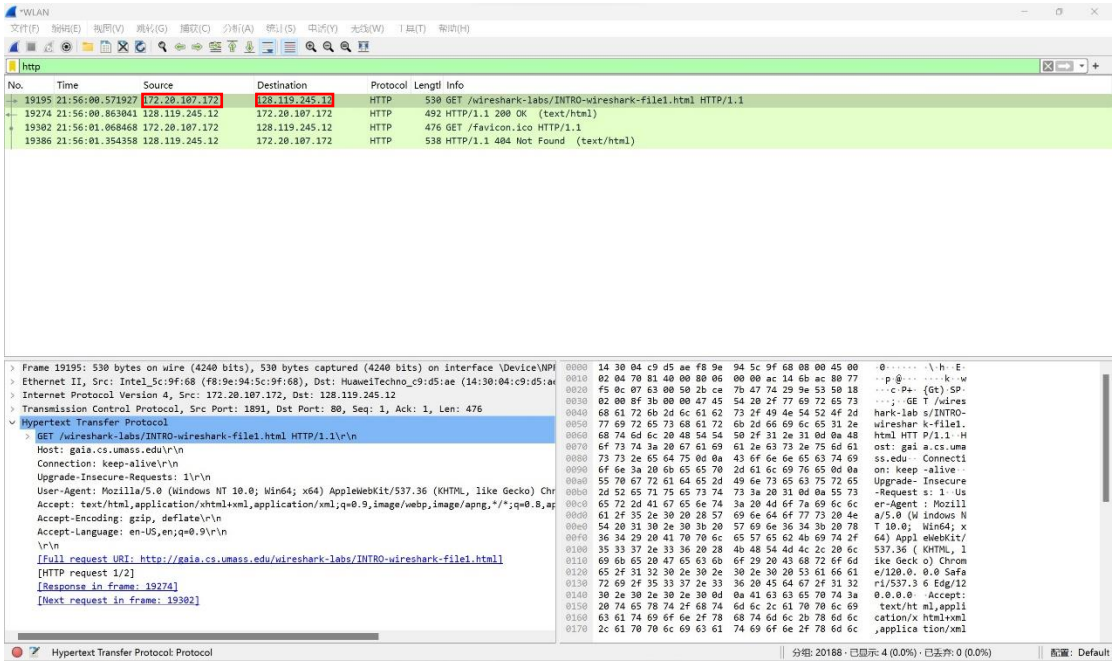
Time Taken = 21:56:00.863041 – 21:56:00.571927 = 0.291114s

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 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-
A35CA8A4C4FF}, 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-
A35CA8A4C4FF}, 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)
```