天津大学

Wireshark Lab: Getting Started 实验报告

学院： 智能与计算学部

专业： 计算机科学与技术

姓名： 陈秋澄

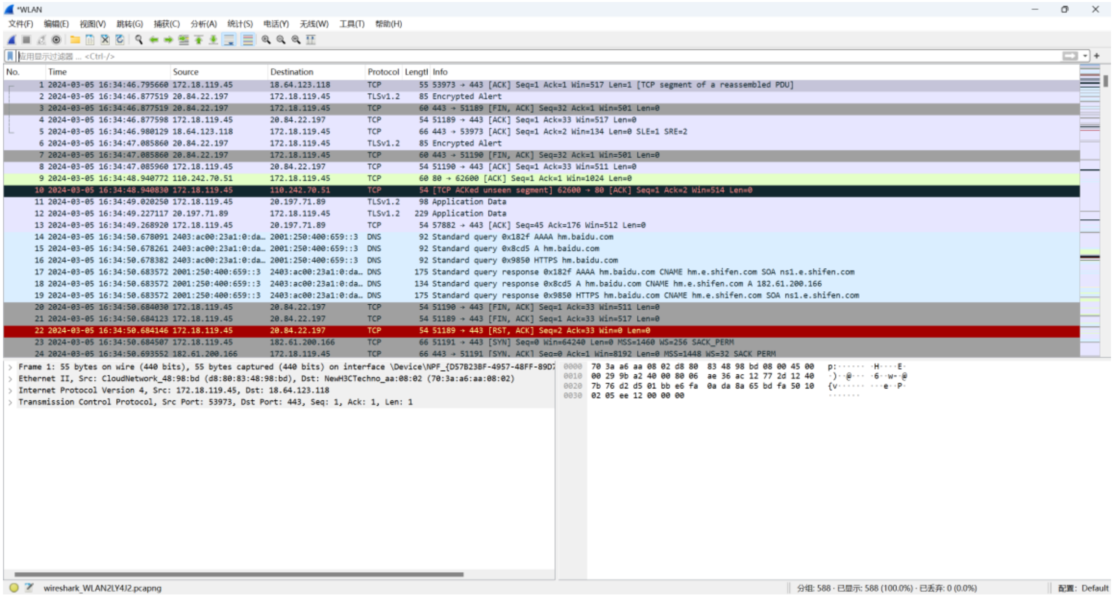
学号： 3022244290

2024 年 3 月 5 日

下面，我将根据自己的 Wireshark 实验回答以下四个问题：

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

Answer 1: 从图 1 的 Protocol 协议列中可以找到三个不同的协议，即：DNS、TCP、TLSV1.2。



```
No.  Time                       Source             Destination        Protocol Lengtl Info
   1 2024-03-05 16:34:46.795660 172.18.119.45      18.64.123.118      TCP       55 53973 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
   2 2024-03-05 16:34:46.877519 20.84.22.197       172.18.119.45      TLSv1.2   85 Encrypted Alert
   3 2024-03-05 16:34:46.877519 20.84.22.197       172.18.119.45      TCP       60 443 → 51189 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0
   4 2024-03-05 16:34:46.877598 172.18.119.45      20.84.22.197       TCP       54 51189 → 443 [ACK] Seq=1 Ack=33 Win=517 Len=0
   5 2024-03-05 16:34:46.980129 18.64.123.118      172.18.119.45      TCP       66 443 → 53973 [ACK] Seq=1 Ack=2 Win=134 Len=0 SLE=1 SRE=2
   6 2024-03-05 16:34:47.085860 20.84.22.197       172.18.119.45      TLSv1.2   85 Encrypted Alert
   7 2024-03-05 16:34:47.085860 20.84.22.197       172.18.119.45      TCP       60 443 → 51190 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0
   8 2024-03-05 16:34:47.085960 172.18.119.45      20.84.22.197       TCP       54 51190 → 443 [ACK] Seq=1 Ack=33 Win=511 Len=0
   9 2024-03-05 16:34:48.940772 110.242.70.51      172.18.119.45      TCP       60 80 → 62600 [ACK] Seq=1 Ack=1 Win=1024 Len=0
  10 2024-03-05 16:34:48.940830 172.18.119.45      110.242.70.51      TCP       54 [TCP ACKed unseen segment] 62600 → 80 [ACK] Seq=1 Ack=2 Win=514 Len=0
  11 2024-03-05 16:34:49.020250 172.18.119.45      20.197.71.89       TLSv1.2   98 Application Data
  12 2024-03-05 16:34:49.227117 20.197.71.89       172.18.119.45      TLSv1.2  229 Application Data
  13 2024-03-05 16:34:49.268920 172.18.119.45      20.197.71.89       TCP       54 57882 → 443 [ACK] Seq=45 Ack=176 Win=512 Len=0
  14 2024-03-05 16:34:50.678091 2403:ac00:23a1:0:da… 2001:250:400:659::3 DNS     92 Standard query 0x182f AAAA hm.baidu.com
  15 2024-03-05 16:34:50.678261 2403:ac00:23a1:0:da… 2001:250:400:659::3 DNS     92 Standard query 0x8cd5 A hm.baidu.com
  16 2024-03-05 16:34:50.678382 2403:ac00:23a1:0:da… 2001:250:400:659::3 DNS     92 Standard query 0x9850 HTTPS hm.baidu.com
  17 2024-03-05 16:34:50.683572 2001:250:400:659::3 2403:ac00:23a1:0:da… DNS    175 Standard query response 0x182f AAAA hm.baidu.com CNAME hm.e.shifen.com SOA ns1.e.shifen.com
  18 2024-03-05 16:34:50.683572 2001:250:400:659::3 2403:ac00:23a1:0:da… DNS    134 Standard query response 0x8cd5 A hm.baidu.com CNAME hm.e.shifen.com A 182.61.200.166
  19 2024-03-05 16:34:50.683572 2001:250:400:659::3 2403:ac00:23a1:0:da… DNS    175 Standard query response 0x9850 HTTPS hm.baidu.com CNAME hm.e.shifen.com SOA ns1.e.shifen.com
  20 2024-03-05 16:34:50.684030 172.18.119.45      20.84.22.197       TCP       54 51190 → 443 [FIN, ACK] Seq=1 Ack=33 Win=511 Len=0
  21 2024-03-05 16:34:50.684123 172.18.119.45      20.84.22.197       TCP       54 51189 → 443 [FIN, ACK] Seq=1 Ack=33 Win=517 Len=0
  22 2024-03-05 16:34:50.684146 172.18.119.45      20.84.22.197       TCP       54 51189 → 443 [RST, ACK] Seq=2 Ack=33 Win=0 Len=0
  23 2024-03-05 16:34:50.684507 172.18.119.45      182.61.200.166     TCP       66 51191 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  24 2024-03-05 16:34:50.693552 182.61.200.166     172.18.119.45      TCP       66 443 → 51191 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1448 WS=32 SACK_PERM
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{D57B23BF-4957-48FF-89D7
> Ethernet II, Src: CloudNetwork_48:98:bd (d8:80:83:48:98:bd), Dst: NewH3CTechno_aa:08:02 (70:3a:a6:aa:08:02)
> Internet Protocol Version 4, Src: 172.18.119.45, Dst: 18.64.123.118
> Transmission Control Protocol, Src Port: 53973, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

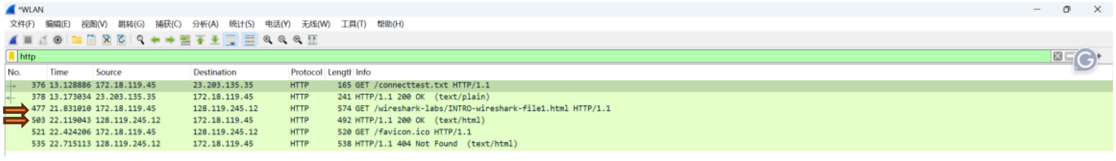
```
0000  70 3a a6 aa 08 02 d8 80  83 48 98 bd 08 00 45 00   p:······ ·H····E·
0010  00 29 9b a2 40 00 80 06  ae 36 ac 12 77 2d 12 40   ·)··@··· ·6··w-·@
0020  7b 76 d2 d5 01 bb e6 fa  0a da 8a 65 bd fa 50 10   {v······ ···e··P·
0030  02 05 ee 12 00 00 00                               ·······
```

wireshark_WLAN2LY4J2.pcapng
分组: 588 · 已显示: 588 (100.0%) · 已丢弃: 0 (0.0%)
配置: Default

图 1 Question 1 佐证

Question 2: How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

Answer 2:



```
No.  Time      Source          Destination     Protocol Lengtl Info
 376 13.128886 172.18.119.45   23.203.135.35   HTTP     165 GET /connecttest.txt HTTP/1.1
 378 13.173034 23.203.135.35   172.18.119.45   HTTP     241 HTTP/1.1 200 OK  (text/plain)
 477 21.831010 172.18.119.45   128.119.245.12  HTTP     574 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 503 22.119043 128.119.245.12  172.18.119.45   HTTP     492 HTTP/1.1 200 OK  (text/html)
 521 22.424206 172.18.119.45   128.119.245.12  HTTP     520 GET /favicon.ico HTTP/1.1
 535 22.715113 128.119.245.12  172.18.119.45   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

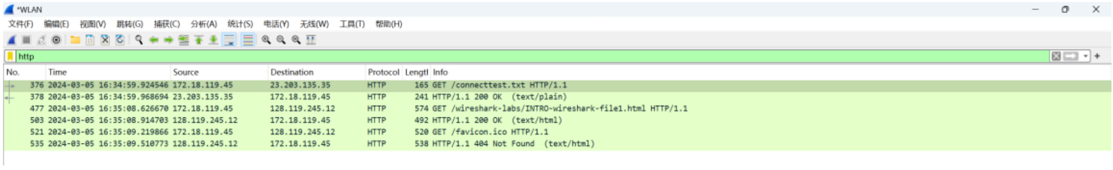
图 2 Question 2 佐证 a

我们选取 Source 和 Destination 交叉对应一致且 Info 为题中要求的两组。从图 2 中箭头指向的两行，可以看出:

HTTP GET message 被发送的相对时间是：21.831010s；HTTP OK message 被接收时间的相对时间是：22.119043s。

所以从 HTTP GET message 被发送到 HTTP OK message 被接受的时间为：22.119043-21.831010=0.288033s。

另附展示绝对时间的图 3，进一步加以说明。


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http

No.	Time	Source	Destination	Protocol	Lengtl	Info
376	2024-03-05 16:34:59.924546	172.18.119.45	23.203.135.35	HTTP	165	GET /connecttest.txt HTTP/1.1
378	2024-03-05 16:34:59.968694	23.203.135.35	172.18.119.45	HTTP	241	HTTP/1.1 200 OK (text/plain)
477	2024-03-05 16:35:08.626670	172.18.119.45	128.119.245.12	HTTP	574	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
503	2024-03-05 16:35:08.914703	128.119.245.12	172.18.119.45	HTTP	492	HTTP/1.1 200 OK (text/html)
521	2024-03-05 16:35:09.219866	172.18.119.45	128.119.245.12	HTTP	520	GET /favicon.ico HTTP/1.1
535	2024-03-05 16:35:09.510773	128.119.245.12	172.18.119.45	HTTP	538	HTTP/1.1 404 Not Found (text/html)

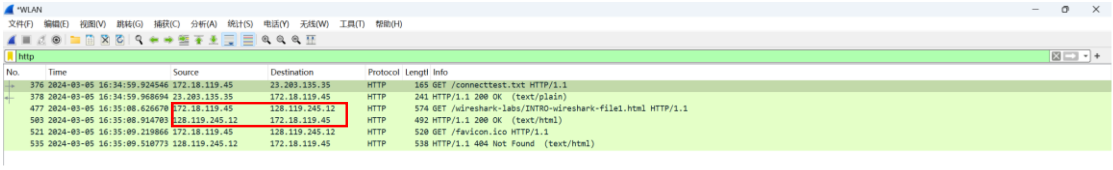
图 3　Question 2 佐证 b（绝对时间的展示）

Question 3: What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

Answer 3:

我们选取 Source 和 Destination 交叉对应一致且 Info 为题中要求的两组。根据图 4 红框中内容，gaia.cs.umass.edu 的网络地址为：128.119.245.12；

我的电脑的网络地址为：172.18.119.45。

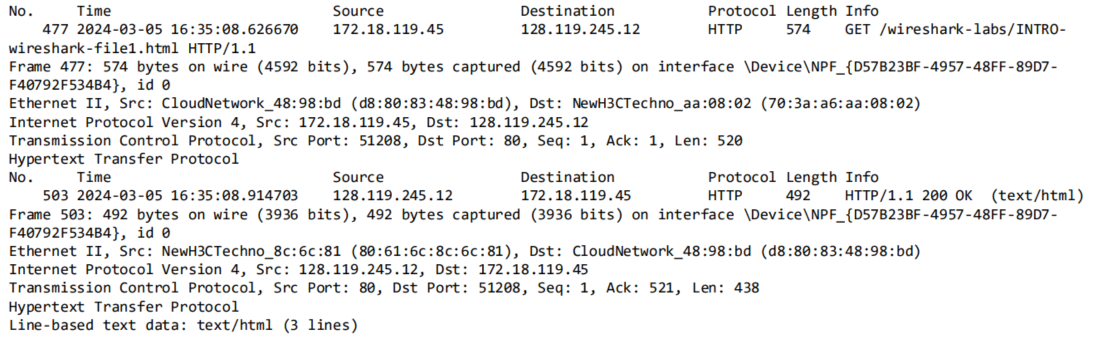

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http

No.	Time	Source	Destination	Protocol	Lengtl	Info
376	2024-03-05 16:34:59.924546	172.18.119.45	23.203.135.35	HTTP	165	GET /connecttest.txt HTTP/1.1
378	2024-03-05 16:34:59.968694	23.203.135.35	172.18.119.45	HTTP	241	HTTP/1.1 200 OK (text/plain)
477	2024-03-05 16:35:08.626670	172.18.119.45	128.119.245.12	HTTP	574	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
503	2024-03-05 16:35:08.914703	128.119.245.12	172.18.119.45	HTTP	492	HTTP/1.1 200 OK (text/html)
521	2024-03-05 16:35:09.219866	172.18.119.45	128.119.245.12	HTTP	520	GET /favicon.ico HTTP/1.1
535	2024-03-05 16:35:09.510773	128.119.245.12	172.18.119.45	HTTP	538	HTTP/1.1 404 Not Found (text/html)

图 4　Question 3 佐证

Question 4: Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

Answer 4: 根据题目要求打印所选分组并输出为 PDF，截图如下：



```
No.     Time                          Source                Destination           Protocol Length Info
    477 2024-03-05 16:35:08.626670    172.18.119.45         128.119.245.12        HTTP     574    GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 477: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface \Device\NPF_{D57B23BF-4957-48FF-89D7-
F40792F534B4}, id 0
Ethernet II, Src: CloudNetwork_48:98:bd (d8:80:83:48:98:bd), Dst: NewH3CTechno_aa:08:02 (70:3a:a6:aa:08:02)
Internet Protocol Version 4, Src: 172.18.119.45, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51208, Dst Port: 80, Seq: 1, Ack: 1, Len: 520
Hypertext Transfer Protocol
No.     Time                          Source                Destination           Protocol Length Info
    503 2024-03-05 16:35:08.914703    128.119.245.12        172.18.119.45         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 503: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{D57B23BF-4957-48FF-89D7-
F40792F534B4}, id 0
Ethernet II, Src: NewH3CTechno_8c:6c:81 (80:61:6c:8c:6c:81), Dst: CloudNetwork_48:98:bd (d8:80:83:48:98:bd)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.119.45
Transmission Control Protocol, Src Port: 80, Dst Port: 51208, Seq: 1, Ack: 521, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

图 5　Question 4 佐证