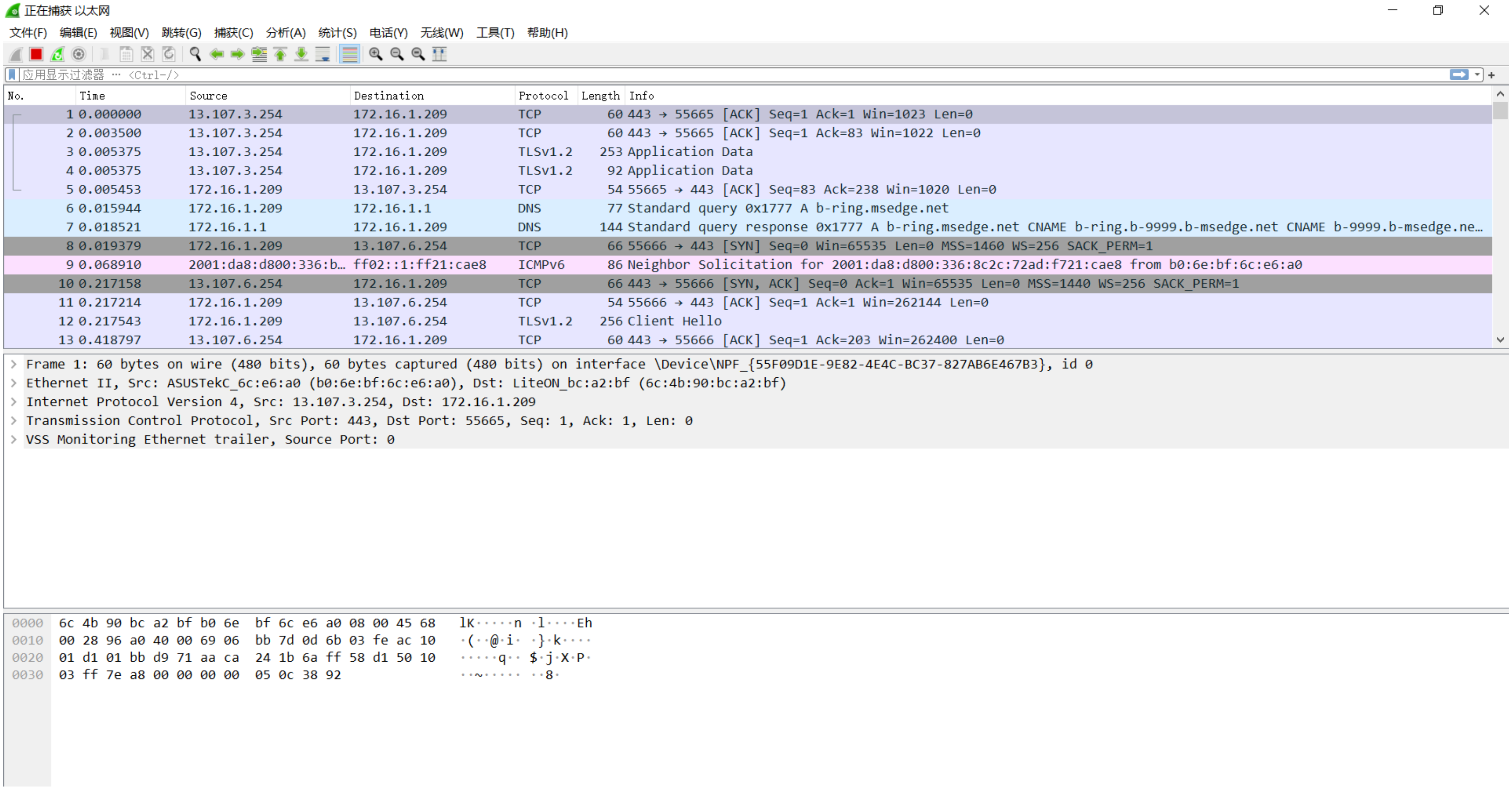
Packet Capture with Pingplotter

Preparation

- Install Wireshark
  - Freeware from https://www.wireshark.org/
- Install Pingplotter
  - Download a copy from www.bb.ustc.edu.cn
    - 14 days trial
  - You can use it to perform traceroute, and configure things like packet size, transfer interval, etc.
  - Graphic output for network metrics

Wireshark


正在捕获 以太网
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)
应用显示过滤器 … <Ctrl-/>

```
No.     Time        Source                 Destination          Protocol  Length Info
      1 0.000000    13.107.3.254           172.16.1.209         TCP          60 443 → 55665 [ACK] Seq=1 Ack=1 Win=1023 Len=0
      2 0.003500    13.107.3.254           172.16.1.209         TCP          60 443 → 55665 [ACK] Seq=1 Ack=83 Win=1022 Len=0
      3 0.005375    13.107.3.254           172.16.1.209         TLSv1.2     253 Application Data
      4 0.005375    13.107.3.254           172.16.1.209         TLSv1.2      92 Application Data
      5 0.005453    172.16.1.209           13.107.3.254         TCP          54 55665 → 443 [ACK] Seq=83 Ack=238 Win=1020 Len=0
      6 0.015944    172.16.1.209           172.16.1.1           DNS          77 Standard query 0x1777 A b-ring.msedge.net
      7 0.018521    172.16.1.1             172.16.1.209         DNS         144 Standard query response 0x1777 A b-ring.msedge.net CNAME b-ring.b-9999.b-msedge.net CNAME b-9999.b-msedge.ne…
      8 0.019379    172.16.1.209           13.107.6.254         TCP          66 55666 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
      9 0.068910    2001:da8:d800:336:b…   ff02::1:ff21:cae8    ICMPv6       86 Neighbor Solicitation for 2001:da8:d800:336:8c2c:72ad:f721:cae8 from b0:6e:bf:6c:e6:a0
     10 0.217158    13.107.6.254           172.16.1.209         TCP          66 443 → 55666 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
     11 0.217214    172.16.1.209           13.107.6.254         TCP          54 55666 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
     12 0.217543    172.16.1.209           13.107.6.254         TLSv1.2     256 Client Hello
     13 0.418797    13.107.6.254           172.16.1.209         TCP          60 443 → 55666 [ACK] Seq=1 Ack=203 Win=262400 Len=0
```

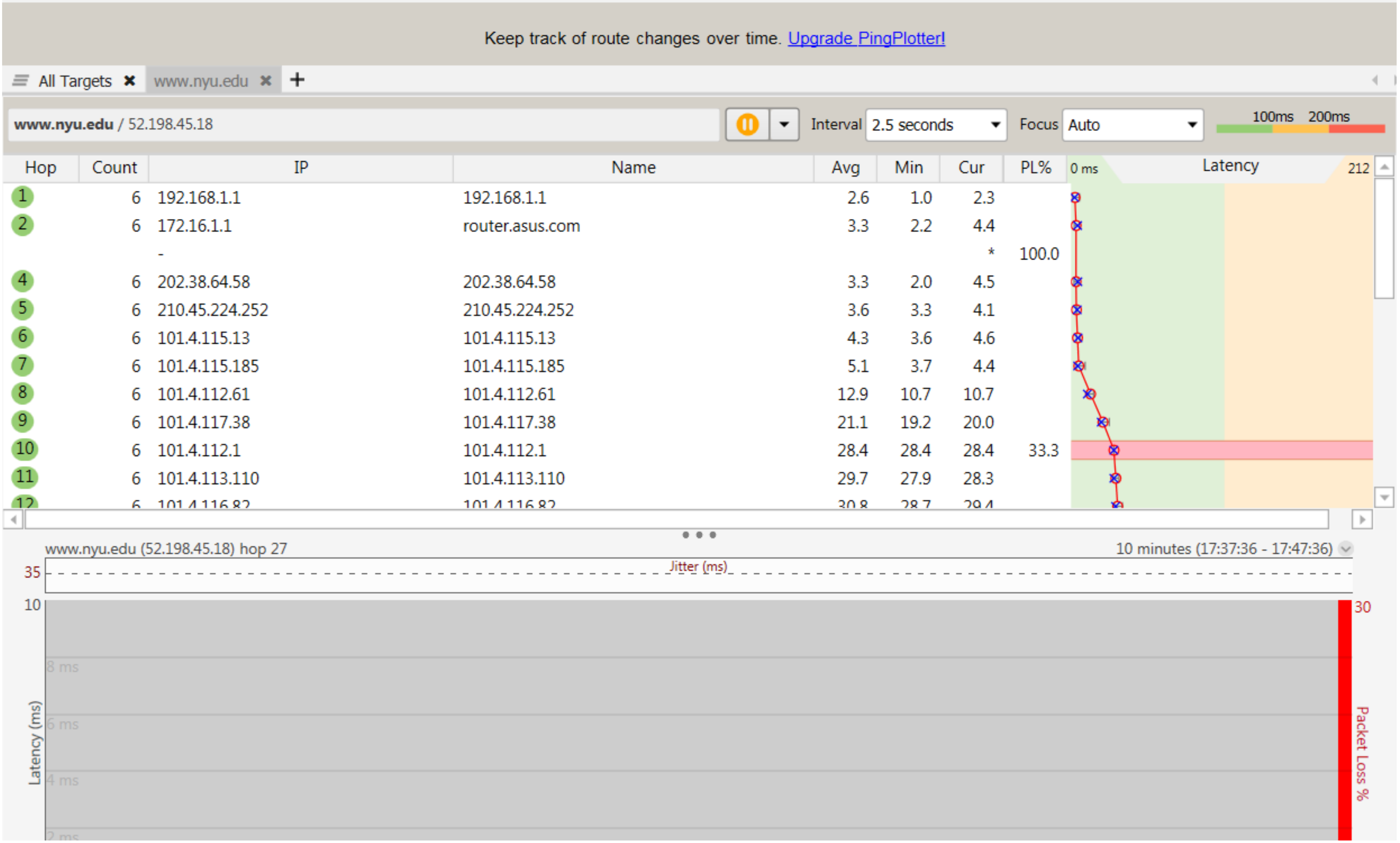
```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{55F09D1E-9E82-4E4C-BC37-827AB6E467B3}, id 0
> Ethernet II, Src: ASUSTekC_6c:e6:a0 (b0:6e:bf:6c:e6:a0), Dst: LiteON_bc:a2:bf (6c:4b:90:bc:a2:bf)
> Internet Protocol Version 4, Src: 13.107.3.254, Dst: 172.16.1.209
> Transmission Control Protocol, Src Port: 443, Dst Port: 55665, Seq: 1, Ack: 1, Len: 0
> VSS Monitoring Ethernet trailer, Source Port: 0
```

```
0000  6c 4b 90 bc a2 bf b0 6e  bf 6c e6 a0 08 00 45 68   lK·····n ·l····Eh
0010  00 28 96 a0 40 00 69 06  bb 7d 0d 6b 03 fe ac 10   ·(··@·i· ·}·k····
0020  01 d1 01 bb d9 71 aa ca  24 1b 6a ff 58 d1 50 10   ·····q·· $·j·X·P·
0030  03 ff 7e a8 00 00 00 00  05 0c 38 92               ··~····· ··8·
```

Wireshark

- Learning material
  - wireshark_lecture.pdf from www.bb.ustc.edu.cn
  - https://wiki.wireshark.org/CaptureFilters#Useful_Filters
  - https://www.wireshark.org/docs/man-pages/pcap-filter.html

PingPlotter



Keep track of route changes over time. Upgrade PingPlotter!

All Targets ✖ www.nyu.edu ✖ +

www.nyu.edu / 52.198.45.18

Interval 2.5 seconds

Focus Auto

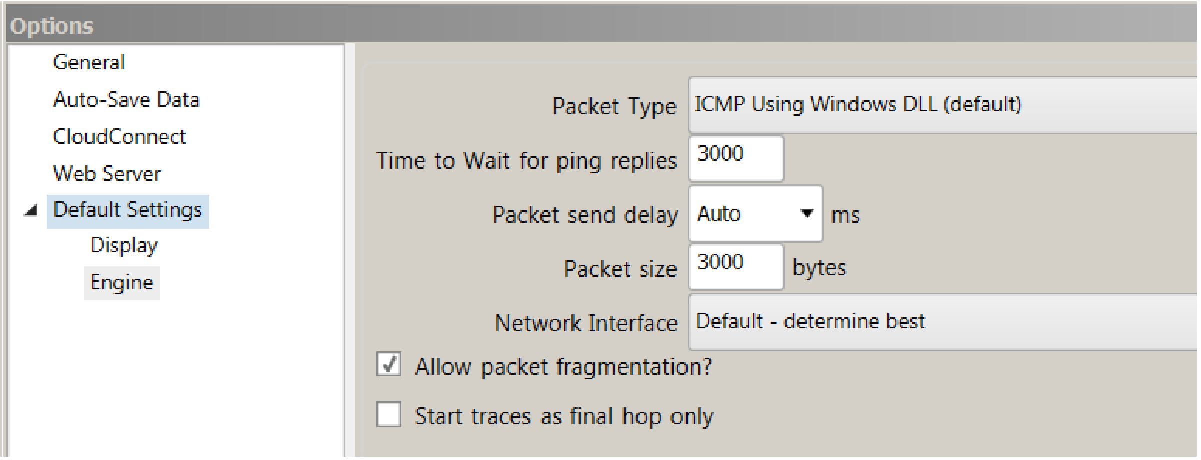
Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	6	192.168.1.1	192.168.1.1	2.6	1.0	2.3	
2	6	172.16.1.1	router.asus.com	3.3	2.2	4.4	
	-					*	100.0
4	6	202.38.64.58	202.38.64.58	3.3	2.0	4.5	
5	6	210.45.224.252	210.45.224.252	3.6	3.3	4.1	
6	6	101.4.115.13	101.4.115.13	4.3	3.6	4.6	
7	6	101.4.115.185	101.4.115.185	5.1	3.7	4.4	
8	6	101.4.112.61	101.4.112.61	12.9	10.7	10.7	
9	6	101.4.117.38	101.4.117.38	21.1	19.2	20.0	
10	6	101.4.112.1	101.4.112.1	28.4	28.4	28.4	33.3
11	6	101.4.113.110	101.4.113.110	29.7	27.9	28.3	
12	6	101.4.116.82	101.4.116.82	30.8	28.7	29.4	

www.nyu.edu (52.198.45.18) hop 27

10 minutes (17:37:36 - 17:47:36)

Packet Capture

- Set packet size as 3000 bytes
  - Menu→edit→options
- Keep “Allow packet fragmentation” checked



Options

Packet Type: ICMP Using Windows DLL (default)

Time to Wait for ping replies: 3000

Packet send delay: Auto ms

Packet size: 3000 bytes

Network Interface: Default - determine best

☑ Allow packet fragmentation?

□ Start traces as final hop only

Packet Capture

- Traceroute to gaia.cs.umass.edu, stop when the count is 3 or 4.
- Meanwhile, capture the packets with wireshark

Questions

1. Display the rules to filter the IP and ICMP packets between source host and destination host. Are there any other Application-layer protocols when you traceroute gaia.cs.umass.edu?[15%]
2. Find the first ICMP Echo Request packet that has TTL=1, is this packet fragmented? If yes, how many fragments, and why is the packet fragmented? [25%]
3. How the packets are fragmented and resembled? For each fragment, how to know if it is the last fragment, and how many bytes are contained in each fragment? Print the packets and answer by highlighting the relevant fields. [20%]

Questions

4. What packet is returned from the router when TTL expires? What is contained in the payload of the packet? [20%]
5. Which link crosses the Pacific, give the router addresses at the two ends of the link. Explained your reason. [10%]
6. How long is the trans-Pacific link? (given that a bit transmits 2*10^8 m/s in fiber). [10%]

Submission

- Submit to bb.ustc.edu.cn
  1. A pdf file named “id + name + traceroute.pdf”
  2. The packet trace you have captured.
  3. Your answers to the questions
  4. For Q1, you need to give the screenshot of the result after performing filter rules and packet with the application-layer protocol.
  5. For Q2- Q6, you need to give the corresponding screenshot and explanation.
  6. deadline: 2021/11/30