

Wireshark

Amy Lin

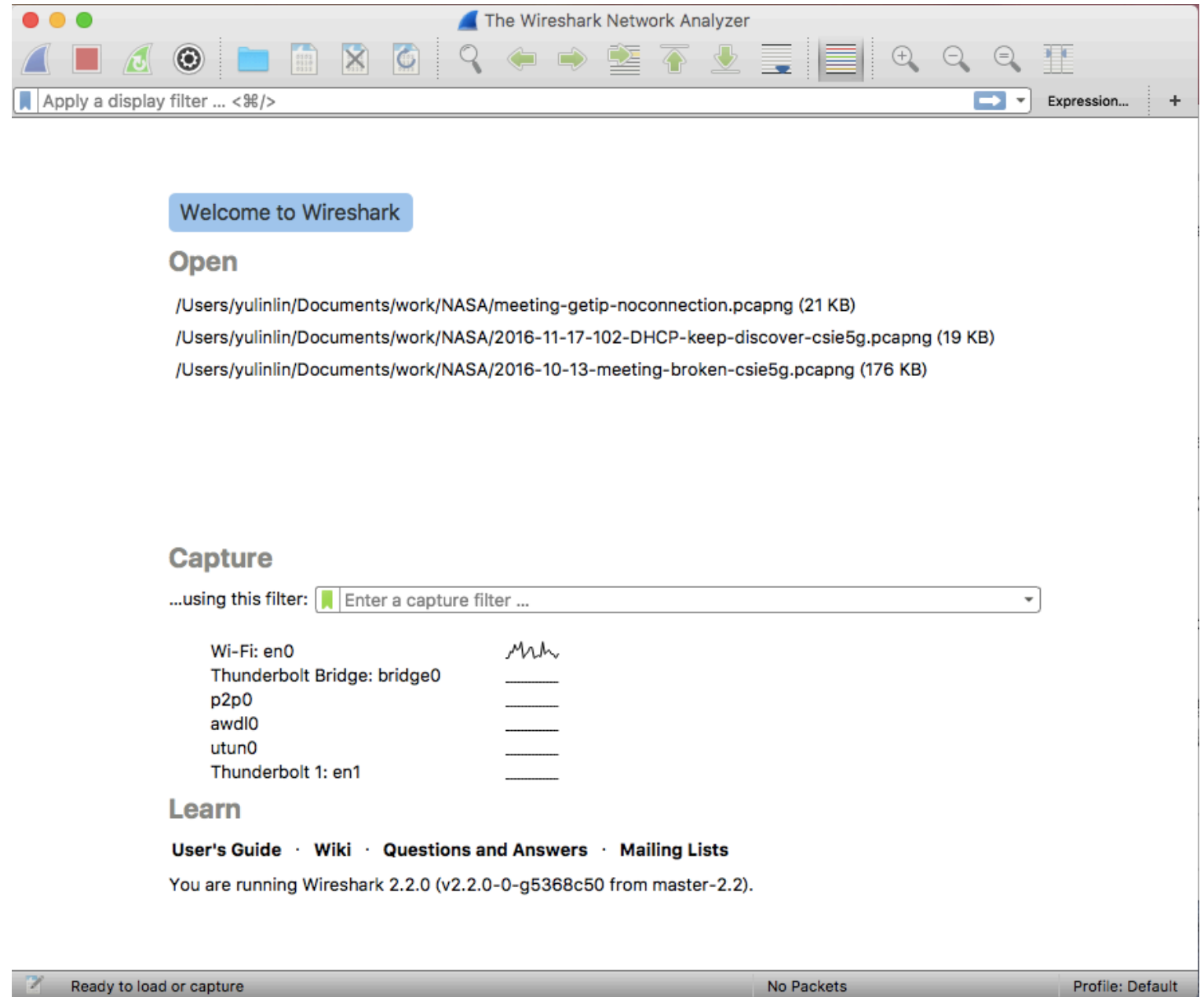
Step 1:

Installation.

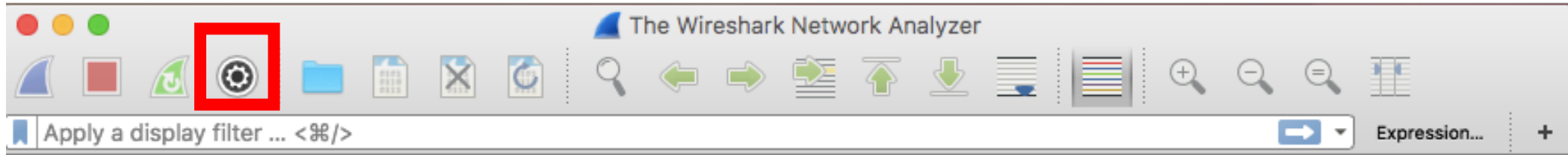
<https://www.wireshark.org/download.html>

Step 2:

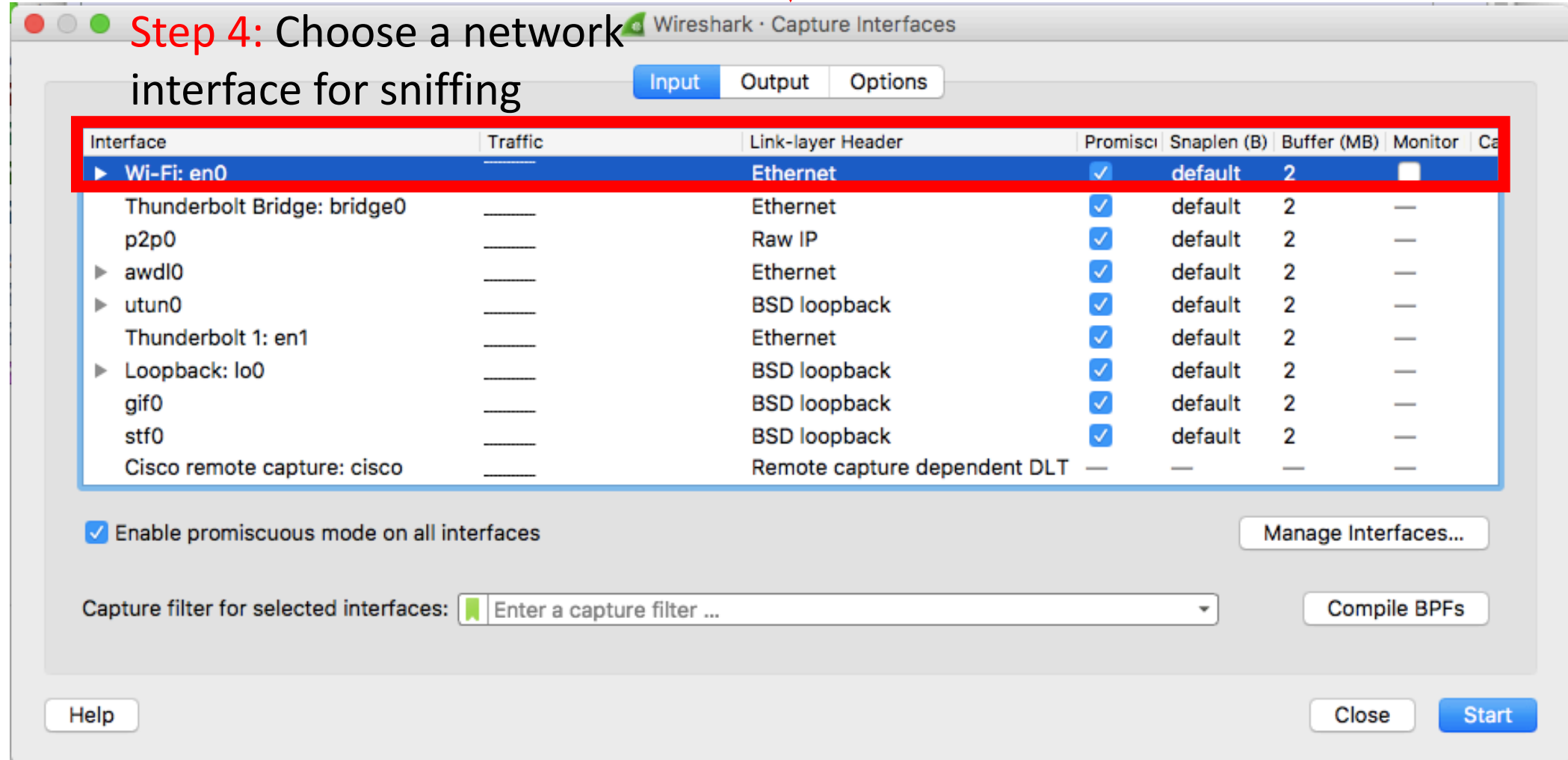
Open wireshark. Here comes the welcome page of wireshark.



Step 3: click here to start capturing



Step 4: Choose a network interface for sniffing



Step 5:
Set display filter

PS. 172.217.24.14 is
one of Google main
webpage server's IP

The image shows a Wireshark network traffic capture. At the top, a display filter is set to `ip.dst == 172.217.24.14`. The main pane shows a list of captured packets. Packet 271 is selected, and its details pane is expanded to show the Hypertext Transfer Protocol (HTTP) data. The HTTP data includes the request line `GET / HTTP/1.1`, host `google.com`, and various headers like `Connection: keep-alive`, `User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/5...`, and `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8`.

No.	Time	Source	Destination	Protocol	Length	Info
254	10.954918	192.168.1.102	172.217.24.14	TCP	78	58999->80 [SYN] Seq=0 Win=65535 .
255	10.955033	192.168.1.102	172.217.24.14	TCP	78	59000->80 [SYN, ECN, CWR] Seq=0 .
260	10.995474	192.168.1.102	172.217.24.14	TCP	66	59000->80 [ACK] Seq=1 Ack=1 Win=.
261	10.995625	192.168.1.102	172.217.24.14	TCP	66	58999->80 [ACK] Seq=1 Ack=1 Win=.
271	11.330486	192.168.1.102	172.217.24.14	HTTP	1103	GET / HTTP/1.1
275	11.346319	192.168.1.102	172.217.24.14	TCP	66	59000->80 [ACK] Seq=1038 Ack=480.
818	17.188013	192.168.1.102	172.217.24.14	QUIC	1392	Client Hello, PKN: 1, CID: 1245.
819	17.188631	192.168.1.102	172.217.24.14	QUIC	1392	Payload (Encrypted), PKN: 2, CI.
820	17.188632	192.168.1.102	172.217.24.14	QUIC	1261	Payload (Encrypted), PKN: 3, CI.
824	17.226409	192.168.1.102	172.217.24.14	QUIC	83	Payload (Encrypted), PKN: 4, CI.
830	17.589131	192.168.1.102	172.217.24.14	QUIC	83	Payload (Encrypted), PKN: 5, CI.
831	17.589197	192.168.1.102	172.217.24.14	QUIC	80	Payload (Encrypted), PKN: 6, CI.
833	17.885058	192.168.1.102	172.217.24.14	QUIC	1392	Payload (Encrypted), PKN: 7, CI.
834	17.885133	192.168.1.102	172.217.24.14	QUIC	282	Payload (Encrypted), PKN: 8, CI.
839	18.154849	192.168.1.102	172.217.24.14	QUIC	83	Payload (Encrypted), PKN: 9, CI.
040	22.180002	192.168.1.102	172.217.24.14	QUIC	65	Payload (Encrypted), PKN: 10, C

```
▶ Frame 271: 1103 bytes on wire (8824 bits), 1103 bytes captured (8824 bits) on interface 0
▶ Ethernet II, Src: Apple_4e:b4:a0 (84:38:35:4e:b4:a0), Dst: Tp-LinkT_d7:ca:7a (b0:48:7a:d7:ca:7a)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 172.217.24.14
▶ Transmission Control Protocol, Src Port: 59000, Dst Port: 80, Seq: 1, Ack: 1, Len: 1037
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: google.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/5...
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
```

HTTP data

Layer Information
of selected packet