

wireshark filter

Syn and Syn-Ack

`tcp.flags.syn==1`

No.	Time	Source	Destination	Protocol	Length	Info
17	27.282700261	192.168.195.174	172.25.8.201	TCP	74	48244 → 80 [SYN] Seq=0 Win=29200 Len=0
18	27.283416058	172.25.8.201	192.168.195.174	TCP	74	80 → 48244 [SYN, ACK] Seq=0 Ack=1 Win=1
36	37.939183991	192.168.195.174	172.25.8.201	TCP	74	48246 → 80 [SYN] Seq=0 Win=29200 Len=0
37	37.940977858	172.25.8.201	192.168.195.174	TCP	74	80 → 48246 [SYN, ACK] Seq=0 Ack=1 Win=1

Ack after Syn-Ack

`tcp.flags.ack==1 && tcp.seq==1 && tcp.len==0 && tcp.ack==1`

No.	Time	Source	Destination	Protocol	Length	Info
19	27.283481605	192.168.195.174	172.25.8.201	TCP	66	48244 → 80 [ACK] Seq=1
38	37.941772765	192.168.195.174	172.25.8.201	TCP	66	48246 → 80 [ACK] Seq=1

Only specific packet number

`frame.number==20`

No.	Time	Source	Destination	Protocol	Length	Info
20	27.283532750	172.25.8.181	192.168.195.174	DNS	137	Standard query query

Filter by protocol

`http`

No.	Time	Source	Destination	Protocol	Length	Info
22	27.283714565	192.168.195.174	172.25.8.201	HTTP	387	GET / HTTP/1.1
24	27.284868356	172.25.8.201	192.168.195.174	HTTP	422	HTTP/1.1 200 OK (text/html)
26	29.977617112	192.168.195.174	172.25.8.201	HTTP	434	GET /student HTTP/1.1
27	29.979726685	172.25.8.201	192.168.195.174	HTTP	584	HTTP/1.1 301 Moved Permanently
29	30.001599779	192.168.195.174	172.25.8.201	HTTP	435	GET /student/ HTTP/1.1
31	30.002321391	172.25.8.201	192.168.195.174	HTTP	421	HTTP/1.1 200 OK (text/html)
39	37.942206033	192.168.195.174	172.25.8.201	HTTP	536	POST /student/index.py HTTP/1.1
41	38.051321261	172.25.8.201	192.168.195.174	HTTP	445	HTTP/1.1 200 OK (text/html)

Right click and follow http stream

`http`

No.	Time	Source	Destination	Protocol	Length	Info
22	27.283714565	192.168.195.174	172.25.8.201	HTTP	387	GET / HTTP/1.1

```
GET / HTTP/1.1
Host: server201.example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

3 packet in sequence

`frame.number >= 17 && frame.number <= 19`

No.	Time	Source	Destination	Protocol	Length	Info
17	27.282700261	192.168.195.174	172.25.8.201	TCP	74	48244 → 80 [SYN] Seq=0
18	27.283416058	172.25.8.201	192.168.195.174	TCP	74	80 → 48244 [SYN, ACK]
19	27.283481605	192.168.195.174	172.25.8.201	TCP	66	48244 → 80 [ACK] Seq=1