LAB04 packet analyzing

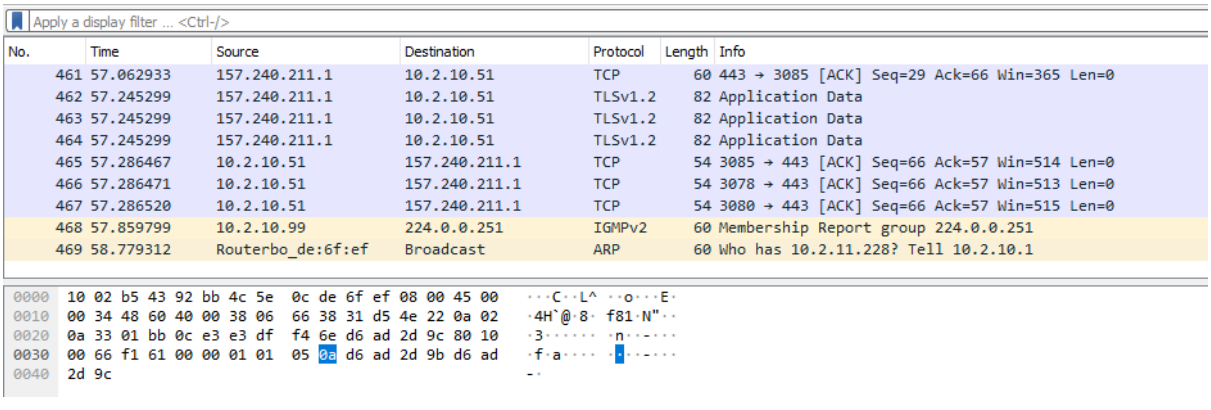
Class	M02
Student ID	B2014926
Name	Tran Dang Khoa
Email address	Khoab2014926@student.ctu.edu.vn
Class	M02
Browser	Safari, Chrome, IE, Firefox

1. Design packet analyzing process under Windows

	scanner	target
OS	Windows Ubuntu	Windows, Linux
IP address	Test - bed host IP	Localhost CTU IP CICT IP Neighboring PC IP VM IP(Ubuntu, Centos)
Analyzing program	Wireshark	
Analyzing types	Filter ARP packet Filter TCP packet	

2. Survey following menu and explain

1 View – packet details



```
C:\Users\PC>ping google.com

Pinging google.com [142.251.220.78] with 32 bytes of data:
Reply from 142.251.220.78: bytes=32 time=84ms TTL=119
Reply from 142.251.220.78: bytes=32 time=32ms TTL=119
Reply from 142.251.220.78: bytes=32 time=33ms TTL=119
Reply from 142.251.220.78: bytes=32 time=50ms TTL=119

Ping statistics for 142.251.220.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 84ms, Average = 49ms
```

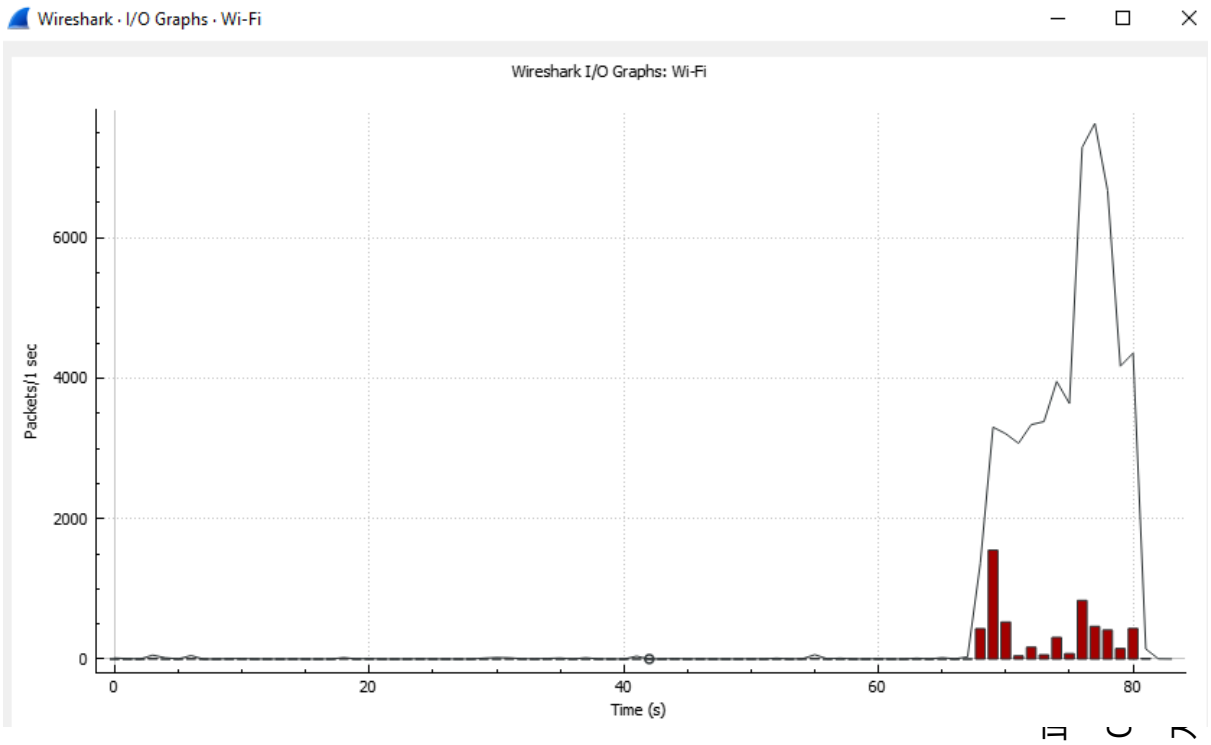
Explan:

2 Statistics - Protocol Hierarchy

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	23	100.0	2796	16 k	0	0	0	23
Ethernet	100.0	23	12.4	346	2023	0	0	0	23
Internet Protocol Version 4	100.0	23	16.5	460	2690	0	0	0	23
User Datagram Protocol	34.8	8	2.3	64	374	0	0	0	8
Mikrotik Neighbor Discovery Protocol	4.3	1	4.9	136	795	1	136	795	1
Data	30.4	7	13.7	382	2234	7	382	2234	7
Transmission Control Protocol	65.2	15	50.4	1408	8235	12	252	1474	15
Transport Layer Security	13.0	3	39.2	1096	6410	3	1096	6410	3

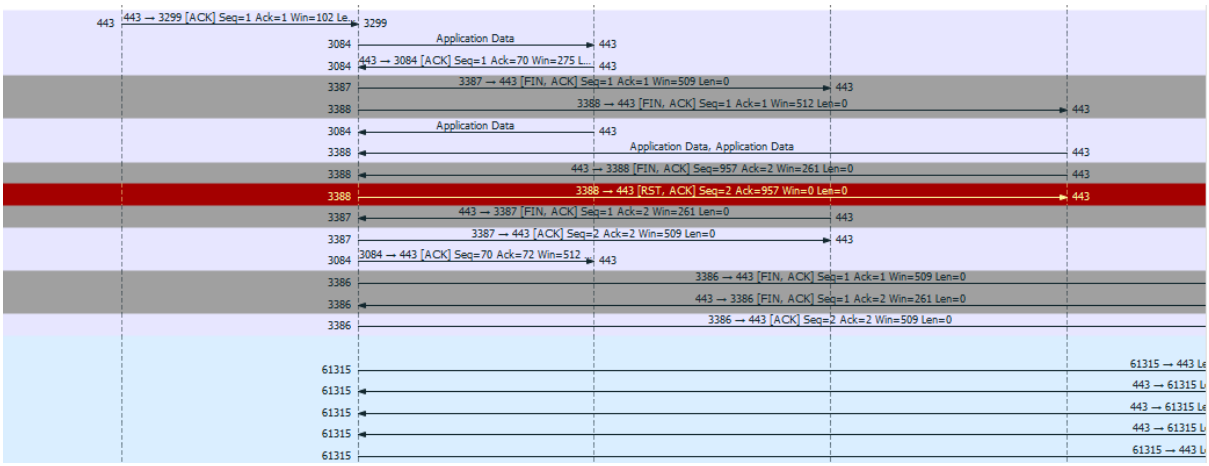
Explan:

3 Statistics - I/O graph -100ms- time of day



Explan:

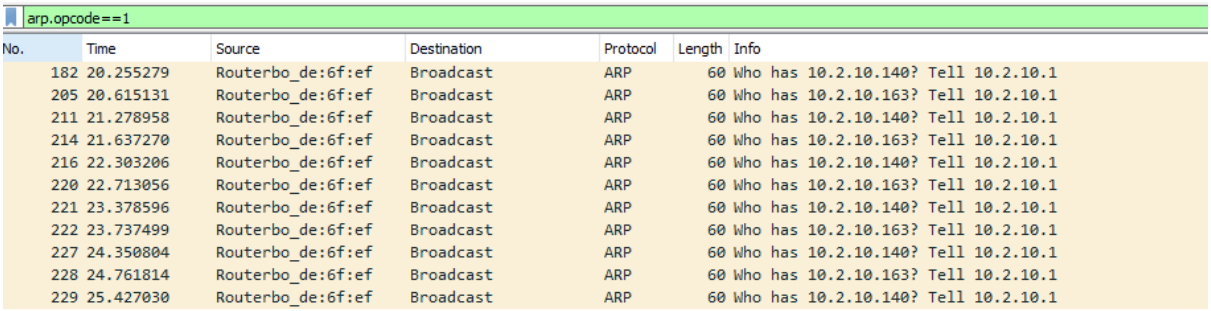
4 Statistics – Flow Graph- Tcp flows[three way hand shake]



Explan:

3. Filter ARP packet

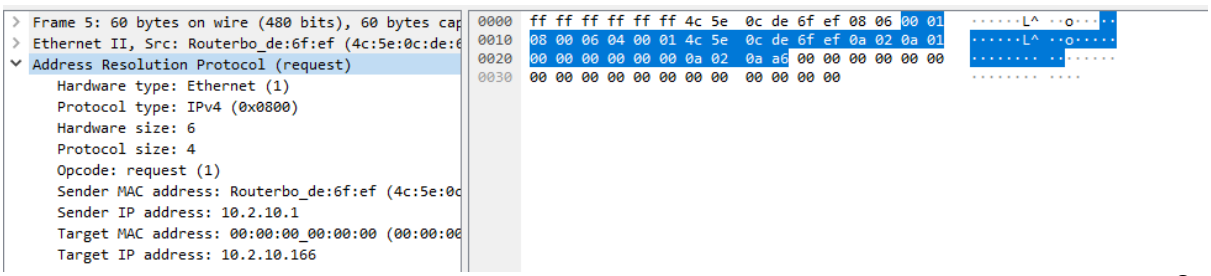
1 Filter ARP request packet : arp.opcode == 1



arp.opcode==1

No.	Time	Source	Destination	Protocol	Length	Info
182	20.255279	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.140? Tell 10.2.10.1
205	20.615131	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.163? Tell 10.2.10.1
211	21.278958	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.140? Tell 10.2.10.1
214	21.637270	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.163? Tell 10.2.10.1
216	22.303206	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.140? Tell 10.2.10.1
220	22.713056	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.163? Tell 10.2.10.1
221	23.378596	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.140? Tell 10.2.10.1
222	23.737499	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.163? Tell 10.2.10.1
227	24.350804	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.140? Tell 10.2.10.1
228	24.761814	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.163? Tell 10.2.10.1
229	25.427030	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.10.140? Tell 10.2.10.1

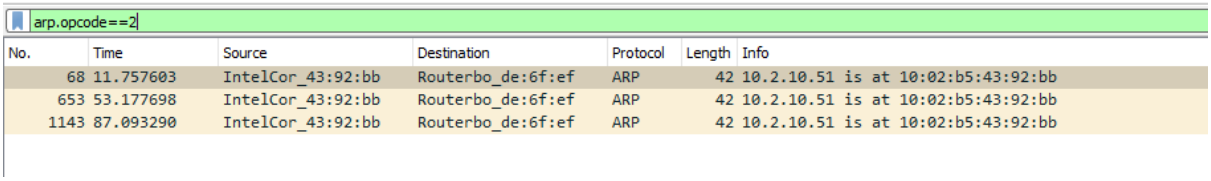
2 Analyze ARP request packet



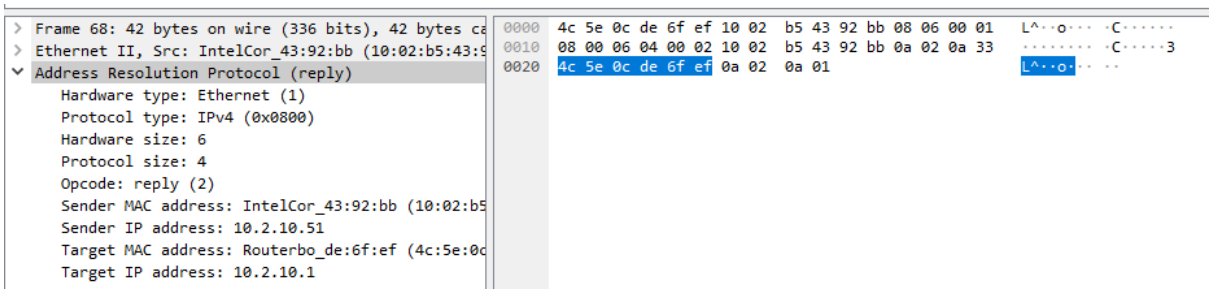
```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes cap
> Ethernet II, Src: Routerbo_de:6f:ef (4c:5e:0c:de:6
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Routerbo_de:6f:ef (4c:5e:0c
    Sender IP address: 10.2.10.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00
    Target IP address: 10.2.10.166
```

```
0000  ff ff ff ff ff ff 4c 5e  0c de 6f ef 08 06 00 01   ......L^ ..o.....
0010  08 00 06 04 00 01 4c 5e  0c de 6f ef 0a 02 0a 01   ......L^ ..o.....
0020  00 00 00 00 00 00 0a 02  0a a6 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

3 Filter ARP reply packet : arp.opcode == 2

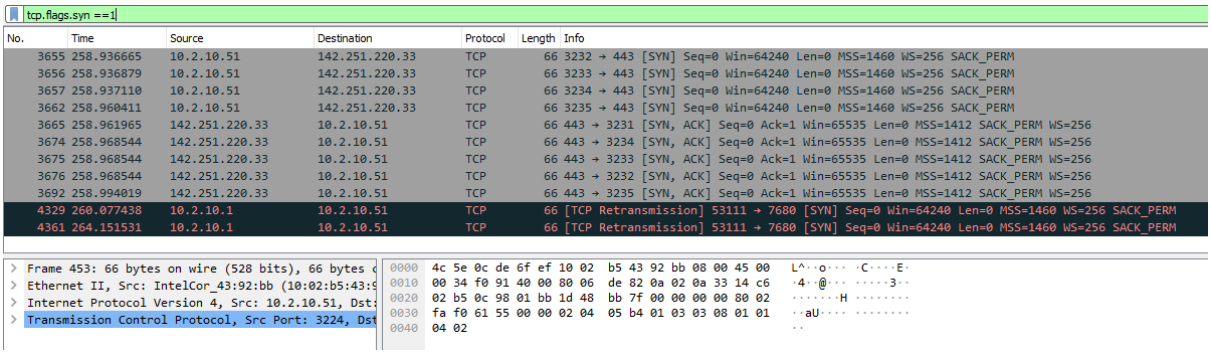


4 Analyze ARP reply packet

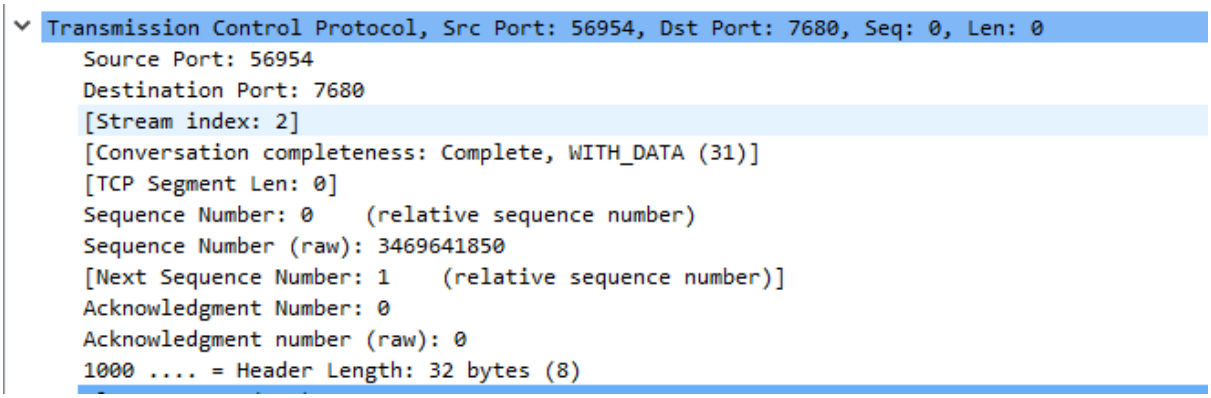


4. Filter SYN packet

1 Filter SYN packet : tcp.flags.syn ==1



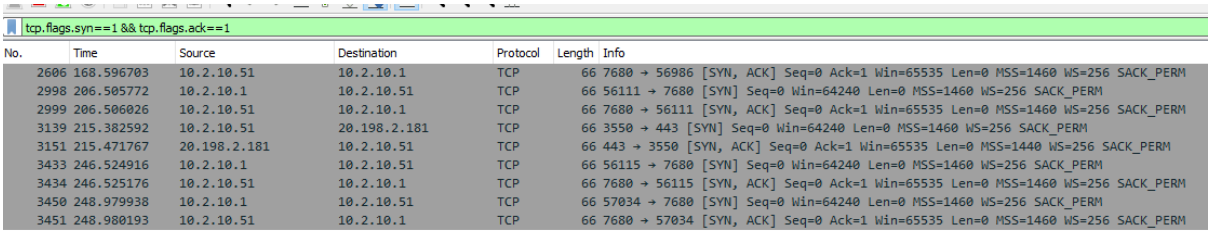
2 Explain seq, ack, leng of SYN packet?



```
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
```

5. Filter SYN, ACK packet

1 Filter SYN, ACK packet : tcp.flags.syn ==1 && tcp.flags.ack ==1



tcp.flags.syn==1 && tcp.flags.ack==1

No.	Time	Source	Destination	Protocol	Length	Info
2606	168.596703	10.2.10.51	10.2.10.1	TCP	66	7680 → 56986 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2998	206.505772	10.2.10.1	10.2.10.51	TCP	66	56111 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2999	206.506026	10.2.10.51	10.2.10.1	TCP	66	7680 → 56111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3139	215.382592	10.2.10.51	20.198.2.181	TCP	66	3550 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3151	215.471767	20.198.2.181	10.2.10.51	TCP	66	443 → 3550 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
3433	246.524916	10.2.10.1	10.2.10.51	TCP	66	56115 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3434	246.525176	10.2.10.51	10.2.10.1	TCP	66	7680 → 56115 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3450	248.979938	10.2.10.1	10.2.10.51	TCP	66	57034 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3451	248.980193	10.2.10.51	10.2.10.1	TCP	66	7680 → 57034 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

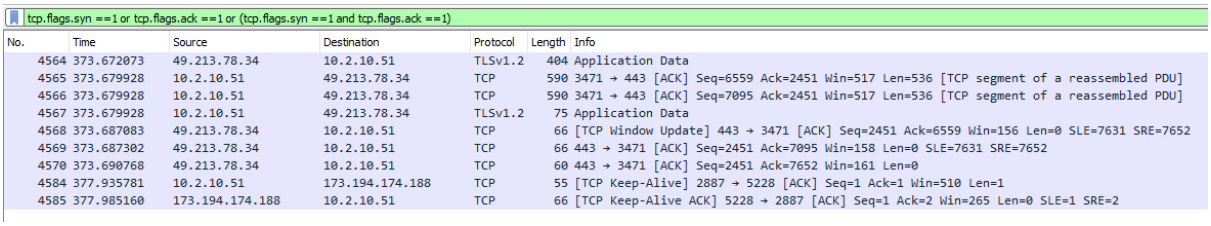
2 Analyze [SYN, ACK] packet

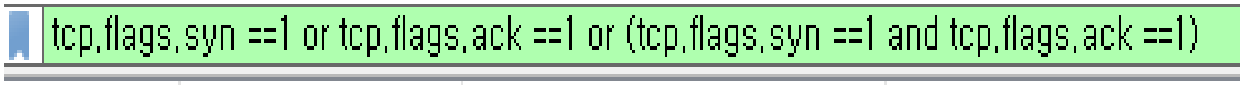
```
Transmission Control Protocol, Src Port: 56079, Dst Port: 7680, Seq: 0, Len: 0
    Source Port: 56079
    Destination Port: 7680
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2337278566
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
```

```
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
```

6. Filter ACK packet

1 Filter ACK packet: tcp.flags.syn ==1 or tcp.flags.ack ==1 or (tcp.flags.syn ==1 and tcp.flags.ack ==1)





2 Analyze [ACK] packet