

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

Apply a display filter ... <Ctrl-/>							
No.	Time	Source	Destination	Protocol	Length	Info	
461	57.062933	157.240.211.1	10.2.10.51	TCP	60	443 → 3085	[ACK] Seq=29 Ack=66 Win=365 Len=0
462	57.245299	157.240.211.1	10.2.10.51	TLSv1.2	82	Application Data	
463	57.245299	157.240.211.1	10.2.10.51	TLSv1.2	82	Application Data	
464	57.245299	157.240.211.1	10.2.10.51	TLSv1.2	82	Application Data	
465	57.286467	10.2.10.51	157.240.211.1	TCP	54	3085 → 443	[ACK] Seq=66 Ack=57 Win=514 Len=0
466	57.286471	10.2.10.51	157.240.211.1	TCP	54	3078 → 443	[ACK] Seq=66 Ack=57 Win=513 Len=0
467	57.286520	10.2.10.51	157.240.211.1	TCP	54	3080 → 443	[ACK] Seq=66 Ack=57 Win=515 Len=0
468	57.859799	10.2.10.99	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251	
469	58.779312	Routerbo_de:6f:ef	Broadcast	ARP	60	Who has 10.2.11.228? Tell 10.2.10.1	

0000	10 02 b5 43 92 bb 4c 5e 0c de 6f ef 08 00 45 00	...C..L^..o...E..
0010	00 34 48 60 40 00 38 06 66 38 31 d5 4e 22 0a 02	..4H'@.8.f81.N"...
0020	0a 33 01 bb 0c e3 e3 df f4 6e d6 ad 2d 9c 80 10	.3.....n.....
0030	00 66 f1 61 00 00 01 01 05 0a d6 ad 2d 9b d6 ad	.f.a....[.....
0040	2d 9c	..

```

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

```

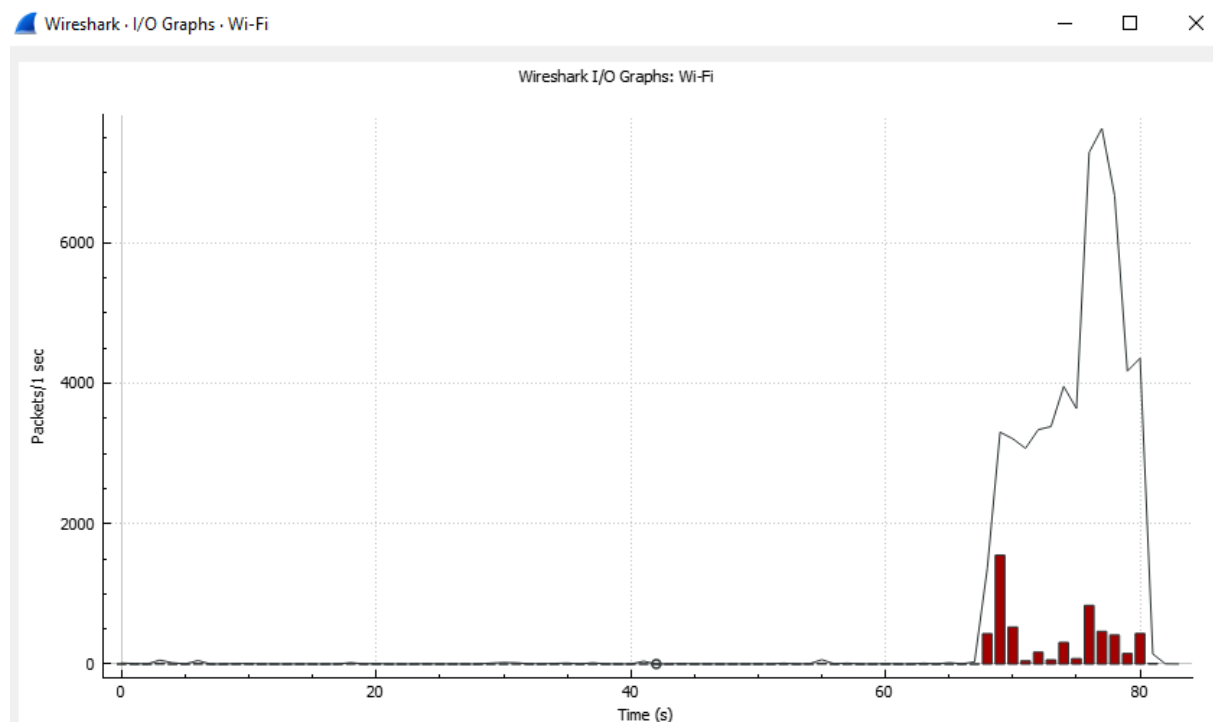
Explan:

2 Statistics - Protocol Hierarchy

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
▼ 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:

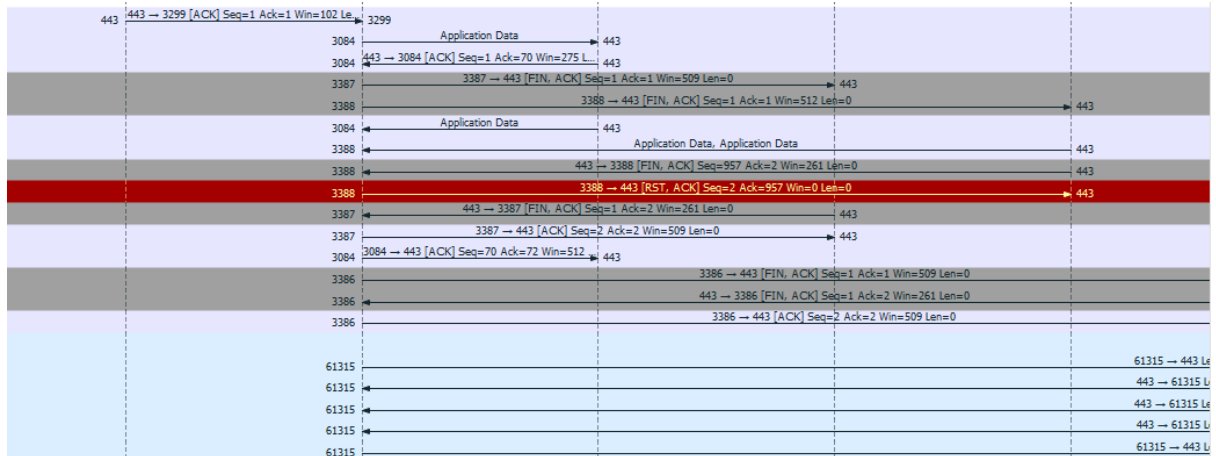
3 Statistics - I/O graph -100ms- time of day



AG
E
M

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 captured		0000	ff ff ff ff ff ff 4c 5e 0c de 6f ef 08 06 00 01L^..o...
> Ethernet II, Src: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef),		0010	08 00 06 04 00 01 4c 5e 0c de 6f ef 0a 02 0a 01L^..o.....
Address Resolution Protocol (request)		0020	00 00 00 00 00 00 0a 02 0a a6 00 00 00 00 00 00:.....
Hardware type: Ethernet (1)		0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Protocol type: IPv4 (0x0800)				
Hardware size: 6				
Protocol size: 4				
Opcode: request (1)				
Sender MAC address: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)				
Sender IP address: 10.2.10.1				
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)				
Target IP address: 10.2.10.166				

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

이제 이 ARP 패킷을 필터링합니다.

arp.opcode==2						
No.	Time	Source	Destination	Protocol	Length	Info
68	11.757603	IntelCor_43:92:bb	Routerbo_de:6f:ef	ARP	42	10.2.10.51 is at 10:02:b5:43:92:bb
653	53.177698	IntelCor_43:92:bb	Routerbo_de:6f:ef	ARP	42	10.2.10.51 is at 10:02:b5:43:92:bb
1143	87.093290	IntelCor_43:92:bb	Routerbo_de:6f:ef	ARP	42	10.2.10.51 is at 10:02:b5:43:92:bb

4 Analyze ARP reply packet

> Frame 68: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0		0000	4c 5e 0c de 6f ef 10 02 b5 43 92 bb 08 06 00 01	L^..o...C.....
> Ethernet II, Src: IntelCor_43:92:bb (10:02:b5:43:92:bb), Dst: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)		0010	08 00 06 04 00 02 10 02 b5 43 92 bb 0a 02 0a 33C.....3
▼ Address Resolution Protocol (reply)		0020	4c 5e 0c de 6f ef 0a 02 0a 01	L^..o... ..
Hardware type: Ethernet (1)				
Protocol type: IPv4 (0x0800)				
Hardware size: 6				
Protocol size: 4				
Opcode: reply (2)				
Sender MAC address: IntelCor_43:92:bb (10:02:b5:43:92:bb)				
Sender IP address: 10.2.10.51				
Target MAC address: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)				
Target IP address: 10.2.10.1				

4. Filter SYN packet

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

tcp.flags.syn == 1						
No.	Time	Source	Destination	Protocol	Length	Info
3655	258.936665	10.2.10.51	142.251.220.33	TCP	66	3232 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3656	258.936879	10.2.10.51	142.251.220.33	TCP	66	3233 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3657	258.937110	10.2.10.51	142.251.220.33	TCP	66	3234 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3662	258.960411	10.2.10.51	142.251.220.33	TCP	66	3235 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3665	258.961965	142.251.220.33	10.2.10.51	TCP	66	443 → 3231 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
3674	258.968544	142.251.220.33	10.2.10.51	TCP	66	443 → 3234 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
3675	258.968544	142.251.220.33	10.2.10.51	TCP	66	443 → 3233 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
3676	258.968544	142.251.220.33	10.2.10.51	TCP	66	443 → 3232 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
3692	258.994019	142.251.220.33	10.2.10.51	TCP	66	443 → 3235 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
4329	260.077438	10.2.10.1	10.2.10.51	TCP	66	[TCP Retransmission] 53111 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4361	264.151531	10.2.10.1	10.2.10.51	TCP	66	[TCP Retransmission] 53111 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

> Frame 453: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0		0000	4c 5e 0c de 6f ef 10 02 b5 43 92 bb 08 00 45 00	L^..o...C.....E
> Ethernet II, Src: IntelCor_43:92:bb (10:02:b5:43:92:bb), Dst: Routerbo_de:6f:ef (4c:5e:0c:de:6f:ef)		0010	00 34 f0 91 40 00 00 06 de 82 0a 02 0a 33 14 c6	..4..@... ..3..
> Internet Protocol Version 4, Src: 10.2.10.51, Dst: 10.2.10.1		0020	02 b5 0c 98 01 bb 1d 48 bb 7f 00 00 00 00 00 02H.....
> Transmission Control Protocol, Src Port: 3224, Dst Port: 7680		0030	fa f0 61 55 00 00 02 04 05 b4 01 03 03 08 01 01	..aU.....
		0040	04 02	..

2 Explain seq, ack, leng of SYN packet?

▼ Transmission Control Protocol, Src Port: 56954, Dst Port: 7680, Seq: 0, Len: 0	
Source Port: 56954	
Destination Port: 7680	
[Stream index: 2]	
[Conversation completeness: Complete, WITH_DATA (31)]	
[TCP Segment Len: 0]	
Sequence Number: 0 (relative sequence number)	
Sequence Number (raw): 3469641850	
[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

```

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)`

tcp.flags.syn == 1 or tcp.flags.ack == 1 or (tcp.flags.syn == 1 and tcp.flags.ack == 1)						
No.	Time	Source	Destination	Protocol	Length	Info
4564	373.672073	49.213.78.34	10.2.10.51	TLSv1.2	404	Application Data
4565	373.679928	10.2.10.51	49.213.78.34	TCP	590	3471 → 443 [ACK] Seq=6559 Ack=2451 Win=517 Len=536 [TCP segment of a reassembled PDU]
4566	373.679928	10.2.10.51	49.213.78.34	TCP	590	3471 → 443 [ACK] Seq=7095 Ack=2451 Win=517 Len=536 [TCP segment of a reassembled PDU]
4567	373.679928	10.2.10.51	49.213.78.34	TLSv1.2	75	Application Data
4568	373.687083	49.213.78.34	10.2.10.51	TCP	66	[TCP Window Update] 443 → 3471 [ACK] Seq=2451 Ack=6559 Win=156 Len=0 SLE=7631 SRE=7652
4569	373.687302	49.213.78.34	10.2.10.51	TCP	66	443 → 3471 [ACK] Seq=2451 Ack=7095 Win=158 Len=0 SLE=7631 SRE=7652
4570	373.690768	49.213.78.34	10.2.10.51	TCP	60	443 → 3471 [ACK] Seq=2451 Ack=7652 Win=161 Len=0
4584	377.935781	10.2.10.51	173.194.174.188	TCP	55	[TCP Keep-Alive] 2887 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
4585	377.985160	173.194.174.188	10.2.10.51	TCP	66	[TCP Keep-Alive ACK] 5228 → 2887 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2

```
tcp.flags.syn == 1 or tcp.flags.ack == 1 or (tcp.flags.syn == 1 and tcp.flags.ack == 1)
```

- 2 Analyze [ACK] packet