Lab 7: Network Analysis

ITCS461: Computer and Communication Security

Mahidol University

Table of Contents

1 Preparation

2 Wireshark Basics

3 Network Analysis: TCP Port Scan

4 Network Analysis: Web

5 Network Analysis: HTTPS

Part I

Preparation

Wireshark Program

1. Check if your machine already have Wireshark program
2. If not, download Wireshark from `https://www.wireshark.org/#download`
   Choose “**Windows Installer**” that match with your machine.
3. In the installer it will ask to install “**winpcap**” , install it as well.

Part II

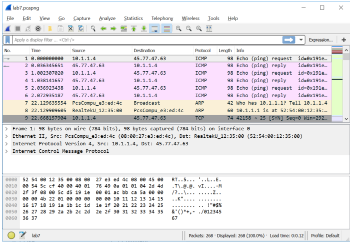
Wireshark Basics

Wireshark Basics

Open a Packet File

Open packet captured file

1. Download “**lab7.pcapng**” from elearning
2. Open Wireshark program –> select menu “**File**” –> “**Open**”
3. Select the file “**lab7.pcapng**” and open it



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.1.1.4	45.77.47.63	ICMP	98	Echo (ping) request id=0x191e…
2	0.036345651	45.77.47.63	10.1.1.4	ICMP	98	Echo (ping) reply id=0x191e…
3	1.002307020	10.1.1.4	45.77.47.63	ICMP	98	Echo (ping) request id=0x191e…
4	1.038141657	45.77.47.63	10.1.1.4	ICMP	98	Echo (ping) reply id=0x191e…
5	2.036923438	10.1.1.4	45.77.47.63	ICMP	98	Echo (ping) request id=0x191e…
6	2.072935187	45.77.47.63	10.1.1.4	ICMP	98	Echo (ping) reply id=0x191e…
7	22.129635554	PcsCompu_e3:ed:4c	Broadcast	ARP	42	Who has 10.1.1.1? Tell 10.1.1.4
8	22.129909605	RealtekU_12:35:00	PcsCompu_e3:ed:4c	ARP	60	10.1.1.1 is at 52:54:00:12:35:…
9	22.668157904	10.1.1.4	45.77.47.63	TCP	74	42158 → 25 [SYN] Seq=0 Win=292…

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: PcsCompu_e3:ed:4c (08:00:27:e3:ed:4c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 45.77.47.63
> Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 e3 ed 4c 08 00 45 00   RT..5... '..L..E.
0010  00 54 5c cf 40 00 40 01  76 49 0a 01 01 04 2d 4d   .T\.@.@. vI....-M
0020  2f 3f 08 00 5c d5 19 1e  00 01 ac bb ca 5a 00 00   /?..\... .....Z..
0030  00 00 4b 22 01 00 00 00  00 00 10 11 12 13 14 15   ..K".... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

lab7 | Packets: 268 · Displayed: 268 (100.0%) · Load time: 0:0.12 | Profile: Default

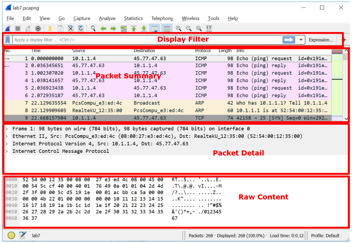
Wireshark Basics

Panels

Wireshark's window has 4 main panels:

- **Display filter:** for enter a statement for filtering the captured packets.
- **Packet Summary:** for listing all the captured packets.

  If any display filter is in-place, this panel will show the filtered packets.
- **Packet Detail:** for displaying analyzed information of the selected packet.
- **Raw Content:** for displaying raw content data of the selected packet.



```
No.  Time          Source              Destination         Protocol  Length  Info
   1 0.000000000   10.1.1.4            45.77.47.63         ICMP        98 Echo (ping) request  id=0x191e…
   2 0.036345651   45.77.47.63         10.1.1.4            ICMP        98 Echo (ping) reply    id=0x191e…
   3 1.002307020   10.1.1.4            45.77.47.63         ICMP        98 Echo (ping) request  id=0x191e…
   4 1.038141657   45.77.47.63         10.1.1.4            ICMP        98 Echo (ping) reply    id=0x191e…
   5 2.036923438   10.1.1.4            45.77.47.63         ICMP        98 Echo (ping) request  id=0x191e…
   6 2.072935187   45.77.47.63         10.1.1.4            ICMP        98 Echo (ping) reply    id=0x191e…
   7 22.129635554  PcsCompu_e3:ed:4c   Broadcast           ARP         42 Who has 10.1.1.1? Tell 10.1.1.4
   8 22.129909605  RealtekU_12:35:00   PcsCompu_e3:ed:4c   ARP         60 10.1.1.1 is at 52:54:00:12:35:…
   9 22.668157904  10.1.1.4            45.77.47.63         TCP         74 42158 → 25 [SYN] Seq=0 Win=292…
```

```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: PcsCompu_e3:ed:4c (08:00:27:e3:ed:4c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 45.77.47.63
> Internet Control Message Protocol
```

```
0000  52 54 00 12 35 00 08 00  27 e3 ed 4c 08 00 45 00   RT..5... '..L..E.
0010  00 54 5c cf 40 00 40 01  76 49 0a 01 01 04 2d 4d   .T\.@.@. vI....-M
0020  2f 3f 08 00 5c d5 19 1e  00 01 ac bb ca 5a 00 00   /?..\... .....Z..
0030  00 00 4b 22 01 00 00 00  00 00 10 11 12 13 14 15   ..K".... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

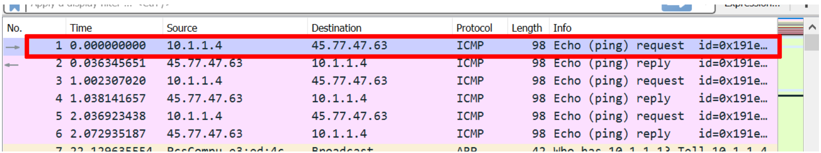
Packets: 268 · Displayed: 268 (100.0%) · Load time: 0:0.12 | Profile: Default

Wireshark Basics

Packet Summary Panel

Select the first packet at the top of the list. In packet summary panel will show you that:

- No. = 1 : first packet in this packet captured file - “lab7.pcapng”
- Time = 0.0000 second : time that this packet was captured, relative to the capturing process was started
- Source = 10.1.1.4 : IP address of the machine sending this packet
- Destination = 45.77.47.63 : IP address of the designed recipient
- Protocol = ICMP : highest level of protocol used in this packet
- Length = 98 byte : size of packet (unit = byte)
- Info = Echo (ping) request : human-readable, short description of this packet



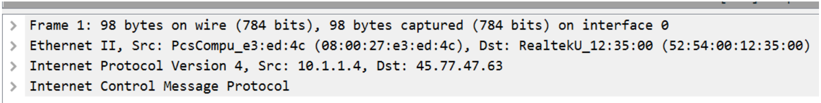
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.1.1.4	45.77.47.63	ICMP	98	Echo (ping) request id=0x191e…
2	0.036345651	45.77.47.63	10.1.1.4	ICMP	98	Echo (ping) reply id=0x191e…
3	1.002307020	10.1.1.4	45.77.47.63	ICMP	98	Echo (ping) request id=0x191e…
4	1.038141657	45.77.47.63	10.1.1.4	ICMP	98	Echo (ping) reply id=0x191e…
5	2.036923438	10.1.1.4	45.77.47.63	ICMP	98	Echo (ping) request id=0x191e…
6	2.072935187	45.77.47.63	10.1.1.4	ICMP	98	Echo (ping) reply id=0x191e…
7	22.129635554	PcsCompu_e3:ed:4c	Broadcast	ARP	42	Who has 10.1.1.1? Tell 10.1.1.4

Wireshark Basics

Packet Detail Panel

In packet detail panel, it will parse the packet and show you that:

- layers of network protocols, starting from layer 1 (Physical Layer) at the first line, layer 2 (Data Link Layer) at line 2, and layer 3 (Network Layer) at line 3-4.
- at Physical Layer: it sends 98 bytes through network interface No. 0
- at Data Link Layer:
  - this packet uses “Ethernet II” protocol
  - it shows 2 physical addresses (MAC), 08:00:27:e3:ed:4c and 52:54:00:12:35:00.
- at Network Layer:
  - first protocol is “Internet Protocol” version 4 (IPv4)
  - sending from IP address 10.1.1.4, to IP address 45.77.47.63
  - second protocol is “Internet Control Message Protocol” (ICMP).
  - ICMP is commonly known as “ping”.



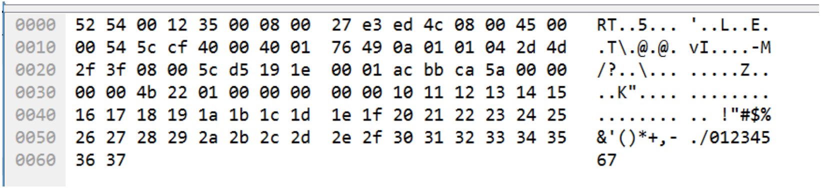
```
> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: PcsCompu_e3:ed:4c (08:00:27:e3:ed:4c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 45.77.47.63
> Internet Control Message Protocol
```

Wireshark Basics

Packet’s Raw Content Panel

In the packet’s raw content panel, you will find the content of the packet in raw format:

- first column: **address** of each byte in the packet (in hexadecimal format)
- second column: value of each byte in the packet (in hexadecimal format)
- third column: value of each byte in the packet (in readable ASCII character format)



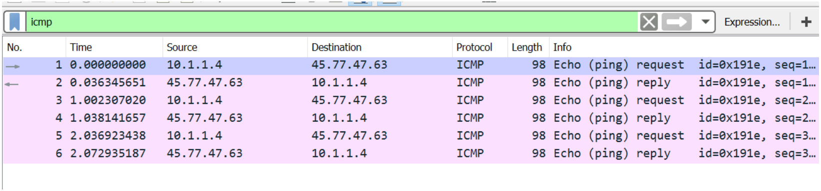
```
0000  52 54 00 12 35 00 08 00  27 e3 ed 4c 08 00 45 00   RT..5... '..L..E.
0010  00 54 5c cf 40 00 40 01  76 49 0a 01 01 04 2d 4d   .T\.@.@. vI....-M
0020  2f 3f 08 00 5c d5 19 1e  00 01 ac bb ca 5a 00 00   /?..\... .....Z..
0030  00 00 4b 22 01 00 00 00  00 00 10 11 12 13 14 15   ..K".... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Wireshark Basics

Display Filter Panel

In display filter panel, you can use it to filter the captured packets for specific protocol or packet content.

Type in “**icmp**” and press enter. This will filter to display only packets with ICMP protocol.



icmp

```
No.   Time         Source        Destination   Protocol  Length  Info
    1 0.000000000  10.1.1.4      45.77.47.63   ICMP          98  Echo (ping) request  id=0x191e, seq=1…
    2 0.036345651  45.77.47.63   10.1.1.4      ICMP          98  Echo (ping) reply    id=0x191e, seq=1…
    3 1.002307020  10.1.1.4      45.77.47.63   ICMP          98  Echo (ping) request  id=0x191e, seq=2…
    4 1.038141657  45.77.47.63   10.1.1.4      ICMP          98  Echo (ping) reply    id=0x191e, seq=2…
    5 2.036923438  10.1.1.4      45.77.47.63   ICMP          98  Echo (ping) request  id=0x191e, seq=3…
    6 2.072935187  45.77.47.63   10.1.1.4      ICMP          98  Echo (ping) reply    id=0x191e, seq=3…
```

Wireshark Basics

Question

With display filter = “icmp”, answer these questions.

Question 1:

- How many ICMP packets? ________
- If one “**ping**” command consists of 1 request packet and 1 reply packet.

  Then, how many “**ping**” commands has been called? ________

Select one pair of ICMP packets, and inspect each packet in the detail panel.

- Find “**Time to live**” (TTL) value inside Internet Protocol 4.

  What is TTL value for request packet? ________ and reply packet? ________
- What is ICMP Type number for request packet? ________ and for reply packet? ________

  Are they the same number? ________ (Y/N)
- Click on “Data” in ICMP protocol, it will highlight the byte values in raw content panel.

  How long is the ICMP data in request packet? ________ and how long in the reply? ________
- Compare the raw data (in raw content panel) of both request and reply packet.

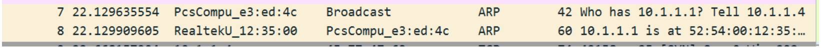
  Are they the same? ________ (Y/N)

Wireshark Basics

Address Resolution Protocol

Next, remove the display filter by deleting words in the text box and press enter.

At packet No. 7-8, they are Address Resolution Protocol (ARP) packets.



```
     7 22.129635554   PcsCompu_e3:ed:4c    Broadcast            ARP        42 Who has 10.1.1.1? Tell 10.1.1.4
     8 22.129909605   RealtekU_12:35:00    PcsCompu_e3:ed:4c    ARP        60 10.1.1.1 is at 52:54:00:12:35:…
```

Question 2:

- What does Address Resolution Protocol do?

  ____

- What is the value of “Hardware type” in packet No.7? ____________(___)
- What is the value of “Protocol type” in packet No.7? ____________(___)
- Using both packet No. 7-8, we can learn the MAC addresses of both sender and receiver.

  IP address: 10.1.1.1 MAC address: __________________

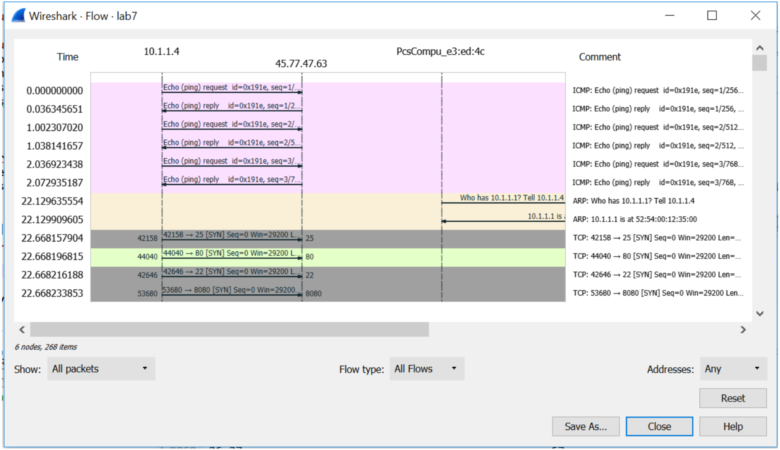
  IP address: 10.1.1.4 MAC address: __________________

Wireshark Basics

Flow Graph

To see the overview of the packet file, we can use Wireshark to display the flow graph.

Use the menu “**Statistics**” –> “**Flow Graph**”.



Wireshark · Flow · lab7

Time	10.1.1.4		45.77.47.63	PcsCompu_e3:ed:4c		Comment
0.000000000		Echo (ping) request id=0x191e, seq=1/... →				ICMP: Echo (ping) request id=0x191e, seq=1/256...
0.036345651		← Echo (ping) reply id=0x191e, seq=1/2...				ICMP: Echo (ping) reply id=0x191e, seq=1/256, ...
1.002307020		Echo (ping) request id=0x191e, seq=2/... →				ICMP: Echo (ping) request id=0x191e, seq=2/512...
1.038141657		← Echo (ping) reply id=0x191e, seq=2/5...				ICMP: Echo (ping) reply id=0x191e, seq=2/512, ...
2.036923438		Echo (ping) request id=0x191e, seq=3/... →				ICMP: Echo (ping) request id=0x191e, seq=3/768...
2.072935187		← Echo (ping) reply id=0x191e, seq=3/7...				ICMP: Echo (ping) reply id=0x191e, seq=3/768, ...
22.129635554					Who has 10.1.1.1? Tell 10.1.1.4	ARP: Who has 10.1.1.1? Tell 10.1.1.4
22.129909605					← 10.1.1.1 is	ARP: 10.1.1.1 is at 52:54:00:12:35:00
22.668157904	42158	42158 → 25 [SYN] Seq=0 Win=29200 L... →	25			TCP: 42158 → 25 [SYN] Seq=0 Win=29200 Len=...
22.668196815	44040	44040 → 80 [SYN] Seq=0 Win=29200 L... →	80			TCP: 44040 → 80 [SYN] Seq=0 Win=29200 Len=...
22.668216188	42646	42646 → 22 [SYN] Seq=0 Win=29200 L... →	22			TCP: 42646 → 22 [SYN] Seq=0 Win=29200 Len=...
22.668233853	53680	53680 → 8080 [SYN] Seq=0 Win=29200... →	8080			TCP: 53680 → 8080 [SYN] Seq=0 Win=29200 Len...

6 nodes, 268 items

Show: All packets

Flow type: All Flows

Addresses: Any

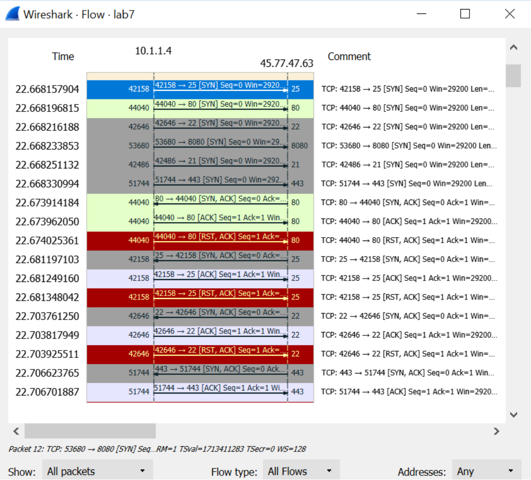
Part III

Network Analysis: TCP Port Scan

Network Analysis

TCP Port Scan

Packet No. 9 - 29, they are an attack of port scanning using TCP protocol.



Wireshark · Flow · lab7

Time	10.1.1.4		45.77.47.63	Comment
22.668157904	42158	42158 → 25 [SYN] Seq=0 Win=2920...	25	TCP: 42158 → 25 [SYN] Seq=0 Win=29200 Len=...
22.668196815	44040	44040 → 80 [SYN] Seq=0 Win=2920...	80	TCP: 44040 → 80 [SYN] Seq=0 Win=29200 Len=...
22.668216188	42646	42646 → 22 [SYN] Seq=0 Win=2920...	22	TCP: 42646 → 22 [SYN] Seq=0 Win=29200 Len=...
22.668233853	53680	53680 → 8080 [SYN] Seq=0 Win=29...	8080	TCP: 53680 → 8080 [SYN] Seq=0 Win=29200 Len...
22.668251132	42486	42486 → 21 [SYN] Seq=0 Win=2920...	21	TCP: 42486 → 21 [SYN] Seq=0 Win=29200 Len=...
22.668330994	51744	51744 → 443 [SYN] Seq=0 Win=292...	443	TCP: 51744 → 443 [SYN] Seq=0 Win=29200 Len...
22.673914184	44040	80 → 44040 [SYN, ACK] Seq=0 Ack=...	80	TCP: 80 → 44040 [SYN, ACK] Seq=0 Ack=1 Win=...
22.673962050	44040	44040 → 80 [ACK] Seq=1 Ack=1 Win...	80	TCP: 44040 → 80 [ACK] Seq=1 Ack=1 Win=29200...
22.674025361	44040	44040 → 80 [RST, ACK] Seq=1 Ack=...	80	TCP: 44040 → 80 [RST, ACK] Seq=1 Ack=1 Win=...
22.681197103	42158	25 → 42158 [SYN, ACK] Seq=0 Ack=...	25	TCP: 25 → 42158 [SYN, ACK] Seq=0 Ack=1 Win=...
22.681249160	42158	42158 → 25 [ACK] Seq=1 Ack=1 Win...	25	TCP: 42158 → 25 [ACK] Seq=1 Ack=1 Win=29200...
22.681348042	42158	42158 → 25 [RST, ACK] Seq=1 Ack=...	25	TCP: 42158 → 25 [RST, ACK] Seq=1 Ack=1 Win=...
22.703761250	42646	22 → 42646 [SYN, ACK] Seq=0 Ack=...	22	TCP: 22 → 42646 [SYN, ACK] Seq=0 Ack=1 Win=...
22.703817949	42646	42646 → 22 [ACK] Seq=1 Ack=1 Win...	22	TCP: 42646 → 22 [ACK] Seq=1 Ack=1 Win=29200...
22.703925511	42646	42646 → 22 [RST, ACK] Seq=1 Ack=...	22	TCP: 42646 → 22 [RST, ACK] Seq=1 Ack=1 Win=...
22.706623765	51744	443 → 51744 [SYN, ACK] Seq=0 Ack...	443	TCP: 443 → 51744 [SYN, ACK] Seq=0 Ack=1 Win...
22.706701887	51744	51744 → 443 [ACK] Seq=1 Ack=1 Wi...	443	TCP: 51744 → 443 [ACK] Seq=1 Ack=1 Win=2920...

Packet 12: TCP: 53680 → 8080 [SYN] Seq...RM=1 TSval=1713411283 TSecr=0 WS=128

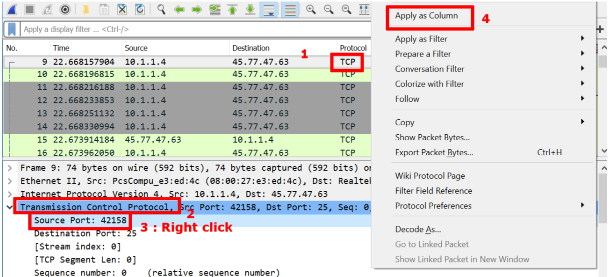
Show: All packets Flow type: All Flows Addresses: Any

Network Analysis

TCP Port Scan

In the standard packet summary panel, it does not show port number. Let’s add two columns for “source port” and “destination port”.

1. select any TCP packet
2. in detail panel, browse into “**Transmission Control Protocol**”
3. right click at “**Source Port**”
4. select “**Apply as Column**”
5. also repeat step 3-4 for “**Destination Port**” as well.



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol
9	22.668157904	10.1.1.4	45.77.47.63	TCP
10	22.668196815	10.1.1.4	45.77.47.63	TCP
11	22.668216188	10.1.1.4	45.77.47.63	TCP
12	22.668233853	10.1.1.4	45.77.47.63	TCP
13	22.668251132	10.1.1.4	45.77.47.63	TCP
14	22.668330994	10.1.1.4	45.77.47.63	TCP
15	22.673914184	45.77.47.63	10.1.1.4	TCP
16	22.673962050	10.1.1.4	45.77.47.63	TCP

```
> Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) or
> Ethernet II, Src: PcsCompu_e3:ed:4c (08:00:27:e3:ed:4c), Dst: Realtel
> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 45.77.47.63
v Transmission Control Protocol, Src Port: 42158, Dst Port: 25, Seq: 0,
    Source Port: 42158
    Destination Port: 25
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
```

Network Analysis

TCP Port Scan

With packet No. 9 - 29 answer these question.

Question 3:

- Can you find what IP address is the target? (hint: public IP is likely to be a server) ____________________________
- What is IP address of the attacker? ____________________________
- What are the ports that being scanned? (hint: known ports are low numbers)

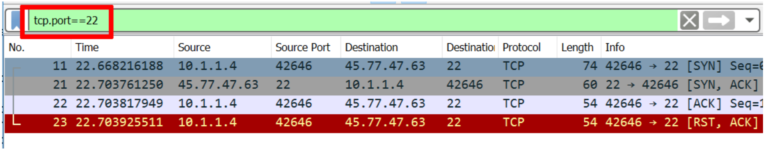
  ____

Network Analysis

TCP Port Scan

You can filter to select only specific port number, by using **tcp.port**. For example:

- tcp.port==22 : filter for transmission on port 22, either source port or destination port
- tcp.srcport==42646 : filter for packets that sent from port 52094
- tcp.dstport==80 : filter for packets that sent to port 80



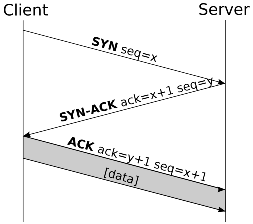
tcp.port==22

No.	Time	Source	Source Port	Destination	Destinatio	Protocol	Length	Info
11	22.668216188	10.1.1.4	42646	45.77.47.63	22	TCP	74	42646 → 22 [SYN] Seq=6
21	22.703761250	45.77.47.63	22	10.1.1.4	42646	TCP	60	22 → 42646 [SYN, ACK]
22	22.703817949	10.1.1.4	42646	45.77.47.63	22	TCP	54	42646 → 22 [ACK] Seq=1
23	22.703925511	10.1.1.4	42646	45.77.47.63	22	TCP	54	42646 → 22 [RST, ACK]

Network Analysis

TCP Port Scan

Normally if a TCP port is opened, it will follow TCP handshake protocol like this.



Question 4: Within packet No. 9-29:

- What ports are following these TCP handshake? (It also means that the ports are opened for connection.) ____

- Pick one of the opening port from above question, check if the number is following this diagram.

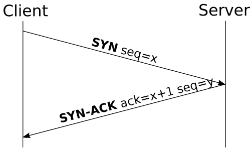
  Port = ________, sequence number (x) = ________, sequence number (y) = ________

  Do the acknowledgement numbers according to diagram above? ________ (Y/N)

Network Analysis

TCP Port Scan: SYN Scan

However, if the attacker just want to know which ports are opened, he/she does not need to complete the TCP handshake. Only 2 packets, SYN and SYN-ACK, are enough.



Packet No. 32 - 47 are a TCP port scanning attempt using only SYN packet.

Question 5: Within packet No. 32 - 47:

- What ports are in this scanning pattern? ______________________________
- What ports are opened? (hint: ports that respond with SYN-ACK) _______________

Part IV

Network Analysis: Web

Network Analysis

DNS

When a URL is entered, it needs to translate it to an IP address first. This is done using DNS protocol.

Question 6: Filter the packets with “dns”

- What is the domain name that used in DNS query? ______________________________
- What is the IP address response? (only IPv4 address) __________________________
- Does DNS operate on-top of TCP? ________ (Y/N)
- What port is used by DNS? ________

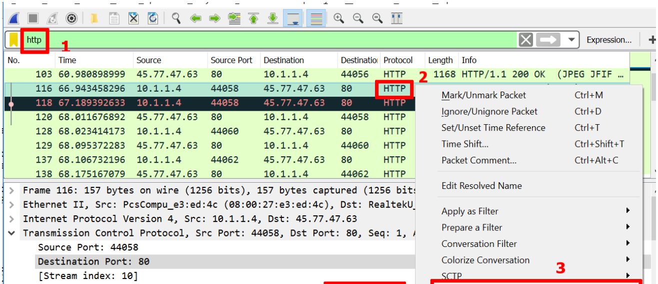
Network Analysis

HTTP

Web is run using HTTP. Because HTTP is plain-text and human readable, we can read the content directly after stitching related packet it together, as a stream.

View HTTP packets as stream:

1. filter using "**http**"
2. right click at any packet
3. select "**Follow**"
4. select "**TCP Stream**"



```
No.   Time          Source       Source Port  Destination  Destinatio Protocol  Length  Info
  103 60.980898999  45.77.47.63  80           10.1.1.4     44056      HTTP      1168    HTTP/1.1 200 OK  (JPEG JFIF …
  116 66.943458296  10.1.1.4     44058        45.77.47.63  80         HTTP
  118 67.189392633  10.1.1.4     44058        45.77.47.63  80         HTTP
  120 68.011676892  45.77.47.63  80           10.1.1.4     44058      HTTP
  128 68.023414173  10.1.1.4     44060        45.77.47.63  80         HTTP
  129 68.095372283  45.77.47.63  80           10.1.1.4     44060      HTTP
  137 68.106732196  10.1.1.4     44062        45.77.47.63  80         HTTP
  138 68.175167079  45.77.47.63  80           10.1.1.4     44062      HTTP
```

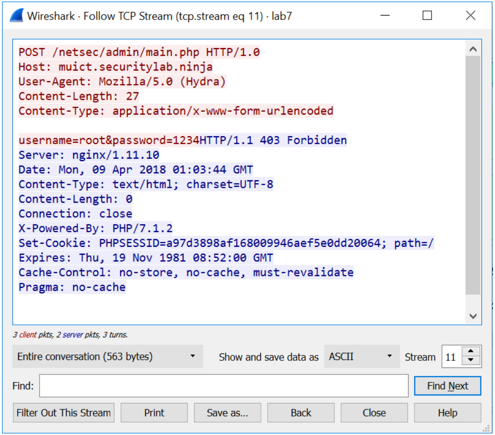
```
> Frame 116: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bit:
> Ethernet II, Src: PcsCompu_e3:ed:4c (08:00:27:e3:ed:4c), Dst: RealtekU_
> Internet Protocol Version 4, Src: 10.1.1.4, Dst: 45.77.47.63
v Transmission Control Protocol, Src Port: 44058, Dst Port: 80, Seq: 1,
    Source Port: 44058
    Destination Port: 80
    [Stream index: 10]
```

http
1
Expression...
2
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
3

Network Analysis

HTTP

Example of HTTP request and response in one stream



Wireshark · Follow TCP Stream (tcp.stream eq 11) · lab7

```
POST /netsec/admin/main.php HTTP/1.0
Host: muict.securitylab.ninja
User-Agent: Mozilla/5.0 (Hydra)
Content-Length: 27
Content-Type: application/x-www-form-urlencoded

username=root&password=1234HTTP/1.1 403 Forbidden
Server: nginx/1.11.10
Date: Mon, 09 Apr 2018 01:03:44 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: close
X-Powered-By: PHP/7.1.2
Set-Cookie: PHPSESSID=a97d3898af168009946aef5e0dd20064; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

3 client pkts, 2 server pkts, 3 turns.

Entire conversation (563 bytes) · Show and save data as: ASCII · Stream: 11

Find:

You can view other stream's content by increasing/decreasing the "**Stream**" number on the right bottom.

Network Analysis

HTTP

There are attempts of brute-forcing for username and password on a web login page. Can you see them? **Question 7:**

- What is the URL of the login page? ______________________
- What is version of PHP the server is running? ______________________
- What is the final username and password that got the attacker to login? (hint: it returns "HTTP/1.1 200 OK") ______________________
- Try login to the website using username & password and fill the form there.

Part V

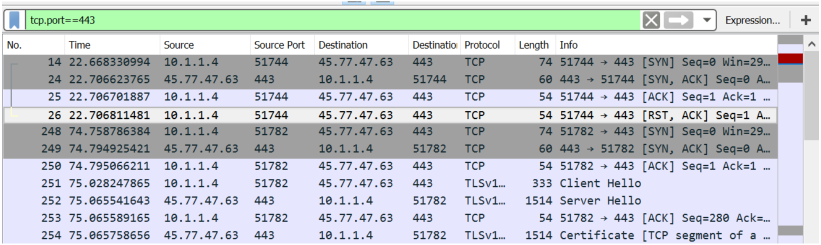
Network Analysis: HTTPS

Network Analysis

HTTPS

HTTP Secure / HTTP over SSL (HTTPS) is a protocol that encrypts HTTP messages so that they are unreadable if intercepted, and checks if the website visiting is able to trust. HTTPS normally uses TCP port 443.

Let’s start by applying filter “tcp.port==443”.



tcp.port==443

No.	Time	Source	Source Port	Destination	Destinatio	Protocol	Length	Info
14	22.668330994	10.1.1.4	51744	45.77.47.63	443	TCP	74	51744 → 443 [SYN] Seq=0 Win=29…
24	22.706623765	45.77.47.63	443	10.1.1.4	51744	TCP	60	443 → 51744 [SYN, ACK] Seq=0 A…
25	22.706701887	10.1.1.4	51744	45.77.47.63	443	TCP	54	51744 → 443 [ACK] Seq=1 Ack=1 …
26	22.706811481	10.1.1.4	51744	45.77.47.63	443	TCP	54	51744 → 443 [RST, ACK] Seq=1 A…
248	74.758786384	10.1.1.4	51782	45.77.47.63	443	TCP	74	51782 → 443 [SYN] Seq=0 Win=29…
249	74.794925421	45.77.47.63	443	10.1.1.4	51782	TCP	60	443 → 51782 [SYN, ACK] Seq=0 A…
250	74.795066211	10.1.1.4	51782	45.77.47.63	443	TCP	54	51782 → 443 [ACK] Seq=1 Ack=1 …
251	75.028247865	10.1.1.4	51782	45.77.47.63	443	TLSv1…	333	Client Hello
252	75.065541643	45.77.47.63	443	10.1.1.4	51782	TLSv1…	1514	Server Hello
253	75.065589165	10.1.1.4	51782	45.77.47.63	443	TCP	54	51782 → 443 [ACK] Seq=280 Ack=…
254	75.065758656	45.77.47.63	443	10.1.1.4	51782	TLSv1…	1514	Certificate [TCP segment of a …

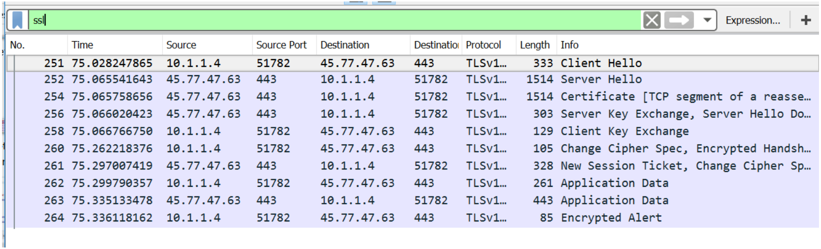
Because HTTPS is on-top of TCP protocol, you can see the TCP handshake here again.

Network Analysis

HTTPS

You might notice that there are TCP handshake packets still present in the list, which is unwanted for analyzing just only HTTPS protocol.

We want to see only HTTPS, we can change the filter to **“ssl”**[1] which is the base protocol for HTTPS.



ssl

No.	Time	Source	Source Port	Destination	Destinatio	Protocol	Length	Info
251	75.028247865	10.1.1.4	51782	45.77.47.63	443	TLSv1…	333	Client Hello
252	75.065541643	45.77.47.63	443	10.1.1.4	51782	TLSv1…	1514	Server Hello
254	75.065758656	45.77.47.63	443	10.1.1.4	51782	TLSv1…	1514	Certificate [TCP segment of a reasse…
256	75.066020423	45.77.47.63	443	10.1.1.4	51782	TLSv1…	303	Server Key Exchange, Server Hello Do…
258	75.066766750	10.1.1.4	51782	45.77.47.63	443	TLSv1…	129	Client Key Exchange
260	75.262218376	10.1.1.4	51782	45.77.47.63	443	TLSv1…	105	Change Cipher Spec, Encrypted Handsh…
261	75.297007419	45.77.47.63	443	10.1.1.4	51782	TLSv1…	328	New Session Ticket, Change Cipher Sp…
262	75.299790357	10.1.1.4	51782	45.77.47.63	443	TLSv1…	261	Application Data
263	75.335133478	45.77.47.63	443	10.1.1.4	51782	TLSv1…	443	Application Data
264	75.336118162	10.1.1.4	51782	45.77.47.63	443	TLSv1…	85	Encrypted Alert

[1] SSL protocol has been deprecated. Currently, TLS protocol (SSL predecessor) is used instead.

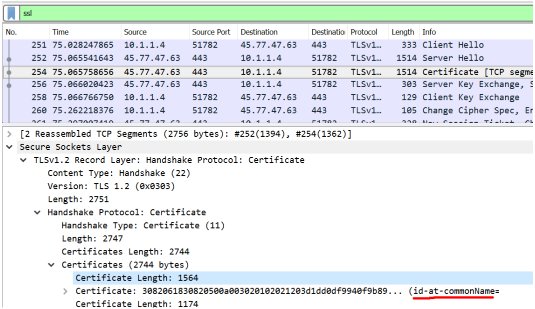
Network Analysis

HTTPS

To verify if the website is a real website, the server will provide a certificate to client to check.

Inspect detail of packet starts with the word **"Certificate…"**.

Browse in the packet detail panel: **Secure Socket Layers –> TLS…: Certificate –> Handshake Protocol: Certificate –> Certificates**



```
ssl
```

No.	Time	Source	Source Port	Destination	Destinatio	Protocol	Length	Info
251	75.028247865	10.1.1.4	51782	45.77.47.63	443	TLSv1…	333	Client Hello
252	75.065541643	45.77.47.63	443	10.1.1.4	51782	TLSv1…	1514	Server Hello
254	75.065758656	45.77.47.63	443	10.1.1.4	51782	TLSv1…	1514	Certificate [TCP segme
256	75.066020423	45.77.47.63	443	10.1.1.4	51782	TLSv1…	303	Server Key Exchange, S
258	75.066766750	10.1.1.4	51782	45.77.47.63	443	TLSv1…	129	Client Key Exchange
260	75.262218376	10.1.1.4	51782	45.77.47.63	443	TLSv1…	105	Change Cipher Spec, Er

```
> [2 Reassembled TCP Segments (2756 bytes): #252(1394), #254(1362)]
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 2751
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 2747
        Certificates Length: 2744
      v Certificates (2744 bytes)
          Certificate Length: 1564
        > Certificate: 3082061830820500a003020102021203d1dd0df9940f9b89... (id-at-commonName=
          Certificate Length: 1174
```

Network Analysis

HTTPS

Question 8:

- There are 2 certificates sent in this packet. Can you find what are their subject and issuer? (answer only field "id-at-commonName")
  - certificiate 1:

    subject = ____

    issuer = ____
  - certificiate 2:

    subject = ____

    issuer = ____
- What is version of Secure Sockets Layer used in this traffic? ________________
- After SSL Handshake, the data should be encrypted. In packet labeled "Application Data", is the data still human-readable? ________ (Y/N)