

# Internet Traffic Analysis using Wireshark

Tan Wei Xuan (49003140)

tanweixuan@postech.ac.kr

April 25, 2019

## 1 Project Overview

*Wireshark 3.0.1* is used to analyze the network traffic captured over a specified period of time.

## 2 Capturing Packets using Wireshark

## 3 Traffic Analysis using Wireshark

Analysis is done on the captured network traffic within the provided tracefile. Network Traffic is captured for a period of **59.088** seconds.

### 3.1 Total Number of Packets and Bytes

#### Statistics

Measurement	Captured	Displayed	Marked
Packets	4137680	4137680 (100.0%)	—
Time span, s	59.088	59.088	—
Average pps	70026.3	70026.3	—
Average packet size, B	754	754	—
Bytes	3120951509	3120951509 (100.0%)	0
Average bytes/s	52 M	52 M	—
Average bits/s	422 M	422 M	—

Figure 1: *Capture Statistics (Statistics → Capture File Properties)*

The total number of packets being captured between a **59 second period** is **4137680**. The total number of Bytes between captured is **3120951509**. This information can be obtained thorough *Stastics → Capture File Properties*.

### 3.2 Time Difference between First and Last Packet

frame.number == 1    frame.number == 4137680				
No.	Time	Source	Destination	Protocol
1	0.000000	141.223.170.141	112.162.88.78	TCP
4137680	59.087530	95.39.36.34	141.223.60.4	SIP

We know that the total number of packets being captured is **4137680**. As such, the first frame be captured will be **1** and the last frame being captured will be **4137680**. We can filter out these two frames by applying the filter, **(frame.number == 1) || (frame.number == 4137680)**. From the filtered results, we can see that the first packet is being transmitted at **0.0** seconds while the last packet is being transmitted at **59.087530** seconds. As such, the **time difference** between the **first** and **last** packet is **59.087530** seconds

### 3.3 The number of packet and total bytes of TCP, UDP and ICMP traffic

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
▼ Frame				
▼ Ethernet				
▼ Internet Protocol Version 4				
> User Datagram Protocol	61.2	2533291	0.6	20266328
> Transmission Control Protocol	37.9	1568769	1.4	43878139
> Internet Protocol Version 6	0.1	3870	0.0	112314
> Internet Control Message Protocol	0.8	31256	0.0	978571

Figure 2: *TCP,UDP and ICMP Proticool Hierarchy (Statistics → Protocol Hierarchy)*

The entirety of the network traffic is being transmitted through **IPv4** as it takes up **100%** of the total packets. The total number of packet and total bytes of IPv4 TCP, UDP and Internet Control Message Protocol (ICMP) traffic are as follow:

#### 1. TCP

The total number of packets being transmitted using TCP is **1568769** and the total number of bytes being transmitted is **43878139**. TCP takes up **37.9%** of total network traffic.

#### 2. UDP

The total number of packets being transmitted using UDP is **2533291** and the total number of bytes being transmitted is **20266328**. UDP takes up **61.2%** of total network traffic.

#### 3. ICMP

The total number of packets being transmitted using ICMP is **31256** and the total number of bytes being transmitted is **978571**. ICMP takes up **0.8%** of total network traffic.

For this captured network traffic, IPv4 TCP and UDP take the majority of the percent of total packets, with **UDP taking up most of the traffic (61%)**. Most of the traffic is probably allocated for UDP services such as Media Streaming, VoIP, etc. This information can be obtained thorough *Statistics → Protocol Hierarchy*.

### 3.4 Total Number of Packets and Bytes of each end host

### 3.5 The number of packet and total bytes of FTP, SSH, DNS, and HTTP

In order to identify the total number of packets and bytes trasmitted using File Transfer Protocol (FTP), Secure Shell (SSH), Domain Name System (DNS) and Hypertext Transfer Protocol

(HTTP), we have to know the reserved port numbers that are being allocated to these services. The ports allocated for each of these services are as shown in the diagram below:

Port	Usage
20	FTP - Data
21	FTP - Control
22	SSH
23	Telnet
25	SMTP
37	TIME
49	TACACS
53	DNS
67	DHCP Server (UDP)
68	DHCP Client (UDP)
69	TFTP (UDP)
79	Finger
80	HTTP
110	POP3
111	RPC (UDP)
119	NNTP
123	NTP
137-139	NetBIOS
161	SNMP
162	Trap (UDP)

Figure 3: *Well-Known Ports* (<https://networking.ringofsaturn.com/Protocols/wellknownports.php>)

## 1. FTP

The port numbers that are being reserved for FTP is **20** and **21**. FTP uses two TCP connections for communication. Port 20 to pass control information and Port 21 to send the data files between the client and the server. The connection has to be established before the files can actually be sent across. As FTP is a TCP connection and thus in order to analyze only the traffic on ports 21 and 22, we apply a display filter to the entire captured traffic (`tcp.port == 20 || tcp.port == 21`)

(tcp.port==21    tcp.port==20)					
No.	Time	Source	Destination	Protocol	Length
509072	7.066944	121.180.215.243	141.223.49.78	FTP	90
1183616	16.735828	195.2.240.180	141.223.30.53	TCP	62
1183617	16.735835	195.2.240.180	141.223.30.53	TCP	62
1183628	16.735947	195.2.240.180	141.223.30.53	TCP	62
1183629	16.735954	195.2.240.180	141.223.30.53	TCP	62
1183641	16.736030	195.2.240.180	141.223.30.53	TCP	62
1183642	16.736036	195.2.240.180	141.223.30.53	TCP	62
1183647	16.736104	195.2.240.180	141.223.30.53	TCP	62

Figure 4: *Filter By FTP Port Numbers*

Statistics		
Measurement	Captured	Displayed
Packets	4137680	127 (0.0%)
Time span, s	59.088	47.645
Average pps	70026.3	2.7
Average packet size, B	754	63
Bytes	3120951509	7946 (0.0%)
Average bytes/s	52 M	166
Average bits/s	422 M	1334

Figure 5: *FTP Capture Statistics (Statistics → Capture File Properties)*

From the capture statistics, we can tell that the total number of packets being captured for FTP is **127** and the total number of Bytes being captured is **7946**. FTP takes up close to **0%** of the entire network traffic. From Figure 4, we can tell that there are two Source Destination, **121.180.215** and **195.2.240.180** and two destination addresses, **141.223.49.78** and **141.223.30.53**. This sequence of captured traffic is probably the exchange of files (63.568kb) between POSTECH webpages and a client's computer as the IP prefix for POSTECH is *141.223.xx.xx*.

## 2. SSH

The port number that is being reserved for SSH is **22**. As SSH is a TCP connection and thus in order to analyze only the traffic on port 22, we apply a display filter to the entire captured traffic (*tcp.port == 22*)

(tcp.port == 22)					
No.	Time	Source	Destination	Protocol	Length
3843	0.053993	141.223.175.232	222.122.81.122	TCP	114
4476	0.062046	222.122.81.122	141.223.175.232	TCP	66
9437	0.126503	141.223.175.232	222.122.81.122	TCP	114
10007	0.133305	222.122.81.122	141.223.175.232	TCP	66
15535	0.205917	141.223.175.232	222.122.81.122	TCP	114
16123	0.213105	222.122.81.122	141.223.175.232	TCP	66
20789	0.268580	141.223.200.153	1.97.49.96	TCP	78
26633	0.345960	141.223.175.232	222.122.81.122	TCP	114
27053	0.352743	222.122.81.122	141.223.175.232	TCP	66

Figure 6: *Filter By SSH Port Numbers*

Statistics		
Measurement	Captured	Displayed
Packets	4137680	799 (0.0%)
Time span, s	59.088	58.909
Average pps	70026.3	13.6
Average packet size, B	754	166
Bytes	3120951509	132704 (0.0%)
Average bytes/s	52 M	2252
Average bits/s	422 M	18 k

Figure 7: *SSH Capture Statistics (Statistics → Capture File Properties)*

From the capture statistics, we can tell that the total number of packets being captured for SSH is **799** and the total number of Bytes being captured is **132704**. SSH takes up close to **0%** of the entire network traffic. SSH is typically used to log into a remote machine and execute commands and can be used to transfer files using the associated SSH

file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model.

Info	
59320 → 22 [PSH, ACK] Seq=1 Ack=1 Win=1002 Len=48 TSval=13844...	1
22 → 59320 [ACK] Seq=1 Ack=49 Win=379 Len=0 TSval=2084580922 ...	
59320 → 22 [PSH, ACK] Seq=49 Ack=1 Win=1002 Len=48 TSval=1384...	
22 → 59320 [ACK] Seq=1 Ack=97 Win=379 Len=0 TSval=2084580993 ...	
59320 → 22 [PSH, ACK] Seq=97 Ack=1 Win=1002 Len=48 TSval=1384...	

Figure 8: *SSH Traffic Info*

From Figure 8, the [ACK] indicates that a host is acknowledging having received some data, and the [PSH,ACK] indicates the host is acknowledging receipt of some previous data and also transmitting some more data. This sequence of captured data is thus probably the transfers of files between a Postech Server (Identifiable by IP Address Prefix) and a Client's Computer.

### 3. DNS

A DNS server listens for requests on port **53 (both UDP and TCP)**. In order to analyze both TCP and UDP traffic on port 53, we apply a display filter to the entire captured traffic (*tcp.port == 53 || udp.port == 53*)

(tcp.port == 53    udp.port == 53)					
No.	Time	Source	Destination	Protocol	Length
98292	1.325406	141.223.82.102	168.126.63.2	DNS	72
98632	1.329624	141.223.1.33	192.112.36.4	DNS	87
98675	1.330268	141.223.1.33	192.112.36.4	DNS	87
98676	1.330301	141.223.1.33	192.112.36.4	DNS	88
98684	1.330425	141.223.1.33	192.112.36.4	DNS	88
98752	1.331466	141.223.1.34	192.43.172.30	DNS	90
98766	1.331598	141.223.1.34	192.43.172.30	DNS	90
98792	1.331966	141.223.1.34	119.205.216.45	DNS	91
98847	1.332616	141.223.1.34	119.205.216.45	DNS	84

Figure 9: *Filter By DNS Port Numbers*

#### Statistics

##### Measurement

Packets  
Time span, s  
Average pps  
Average packet size, B  
Bytes  
Average bytes/s  
Average bits/s

##### Captured

4137680  
59.088  
70026.3  
754  
3120951509  
52 M  
422 M

##### Displayed

31076 (0.8%)  
59.081  
526.0  
124  
3850567 (0.1%)  
65 k  
521 k

Figure 10: *DNS Capture Statistics (Statistics → Capture File Properties)*

From the capture statistics, we can tell that the total number of packets being captured for DNS is **31076** and the total number of Bytes being captured is **3850567**. DNS takes up about **0.8%** of the entire network traffic.

**Statistics**

Measurement	Captured
Packets	4137680
Time span, s	59.088
Average pps	70026.3
Average packet size, B	754
Bytes	3120951509
Average bytes/s	52 M
Average bits/s	422 M

Displayed
27129 (0.7%)
59.081
459.2
131
3560143 (0.1%)
60 k
482 k

Figure 11: *DNS (UDP) Capture Statistics***Statistics**

Measurement	Captured
Packets	4137680
Time span, s	59.088
Average pps	70026.3
Average packet size, B	754
Bytes	3120951509
Average bytes/s	52 M
Average bits/s	422 M

Displayed
3947 (0.1%)
58.848
67.1
74
290424 (0.0%)
4935
39 k

Figure 12: *DNS (TCP) Capture Statistics*

DNS realizes UDP as its main transport layer protocol as it is much faster than TCP, which requires a 3 way handshake. TCP is generally used for transmitted large amount of information (> 512 bytes). Comparing Figure 11 and 12, this is true for the captured network traffic as **more UDP packets (27129)** are being sent over the network as compared to TCP packets (3947).

**4. HTTP**

The port number that is being reserved for HTTP is **80**.

- 3.6** Select two applications other than the aforementioned applications, and print out the number of packets and the bytes of the traffic which allocates well-known port number (TCP/UDP 1 - 1024)
- 3.7** Enumerate the average packet size, average packet inter-arrival time