Packet Dump

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

Thanks

- Most contents provided by Fakrul Alam

Packet Dump

- A host sends and receives packets to communicate each others. When you have network related issues, sometimes it's necessary to see the actual packets to troubleshoot.
- And also it helps to understand protocols and devices' behaviors

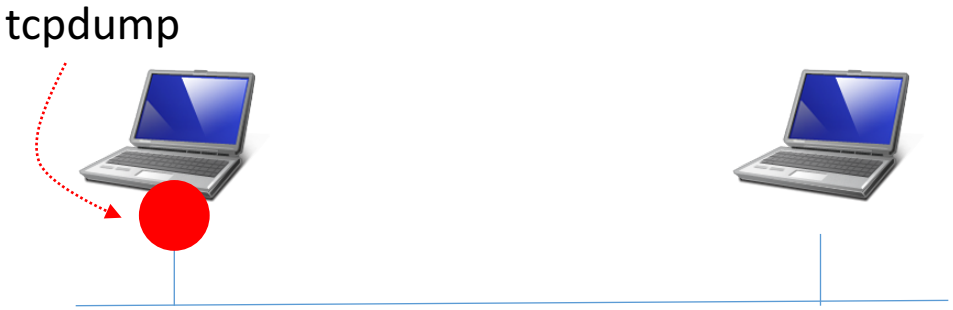
Tcpdump

- Tcpdump is a software to print out a description of the contents of packets on a network interface that match the given option. Details of the packets can be displayed on screen, or they can be saved to a file for later analysis.

- And there are variant of the software
  - Wireshark

What you can see

- Packets arrived on your network interface
  - Packets to/from the host
  - Unicast, Multicast, Broadcast



- You might not see others' communication

Command line

- # tcpdump -ln -i eth0
- # tcpdump -ln -i eth0 tcp and not port 22
- # tcpdump -ln -i eth0 udp and port 53

option	purpose
-n	don‘t resolve numbers to names
-l	make line buffering
-i	interface to watch
port	specifies a port
tcp	tcp packets
udp	udp packets

Host options

- # tcpdump -ln -i eth0 host 10.0.255.1
- # tcpdump -ln -i eth0 tcp and dst port 80
- # tcpdump -ln -i eth0 src host 10.0.255.1 and udp

option	purpose
dst	specifies destination (with host/port)
src	specifies source (with host/port)
host	specifies a host
port	specifies a port

More options

- # tcpdump -ln -i eth0 -c10
- # tcpdump -ln -i eth0 -c10 -s0
- # tcpdump -ln -i eth0 -c10 -s0 -v

option	purpose
-c	# of packets to be captured
-s	packet length to be captured (0=whole)
-v	print a bit more verbose description

Note: Without -c option, tcpdump will continue to capture packets

Saving packets to a file

- # tcpdump -c10 -i eth0 -w <file.pcap>
- # tcpdump -c10 -i eth0 -w <file.pcap> udp

option	purpose
-c	# of packets to be captured
-w	filename to save the captured packets

- Note: .pcap is a common and popular suffix

Opening a saved file

- $ tcpdump -ln -r <file.pcap>
- $ tcpdump -ln -r <file.pcap> tcp and port 21

option	purpose
-r	filename to read the captured packets

Output

04:23:44.648302 IP

(<time>.<subsecond>) (protocol)

10.0.10.75.63260 > 10.0.0.40.22:

(<src ip>.<src port>) > (<dst ip>.<dst port>)

Flags [S],

(Flags [<tcp flags>])

seq 423745570, win 65535,

options [mss 1460,nop,wscale 5,nop,nop,TS val 1187077089 ecr 0,sackOK,eol],

length 0

TCP 3way handshake

04:23:44.648302 IP 10.0.10.75.63260 > 10.0.0.40.22: Flags [S], seq 423745570, win 65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 1187077089 ecr 0,sackOK,eol], length 0

04:23:44.648400 IP 10.0.0.40.22 > 10.0.10.75.63260: Flags [S.], seq 1415462578, ack 423745571, win 28960, options [mss 1460,sackOK,TS val 1374423 ecr 1187077089,nop,wscale 7], length 0

04:23:44.666879 IP 10.0.10.75.63260 > 10.0.0.40.22: Flags [.], ack 1, win 4117, options [nop,nop,TS val 1187077123 ecr 1374423], length 0

04:23:44.668867 IP 10.0.10.75.63260 > 10.0.0.40.22: Flags [P.], seq 1:22, ack 1, win 4117, options [nop,nop,TS val 1187077123 ecr 1374423], length 21

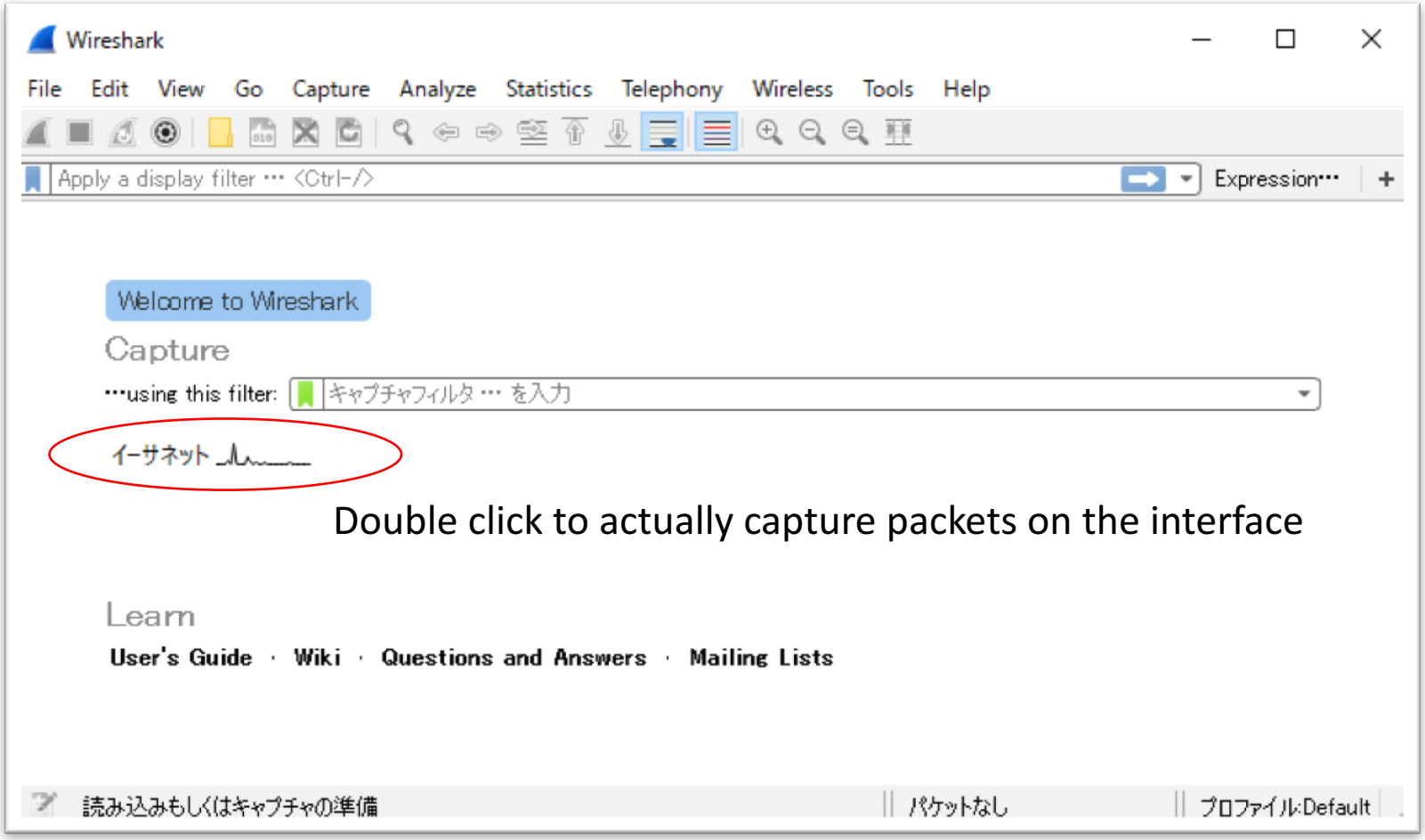
Wireshark

- Yet another packet capturing and analysis software
- GUI
- It can handle the tcpdump file format (pcap)
  - You can analyze packets which is captured on a remote server using tcpdump

How to install

- https://www.wireshark.org/
  - Packages for Windows and MacOS are available
  - Most UNIX system has own package of Wireshark
- Version 2.2.7 is the latest stable version
  - For Windows user: Wireshark needs WinPcap driver to capture packets, and it’s included in the Wireshark package. You are asked to install it during the installation

Wireshark startup



Dashboard

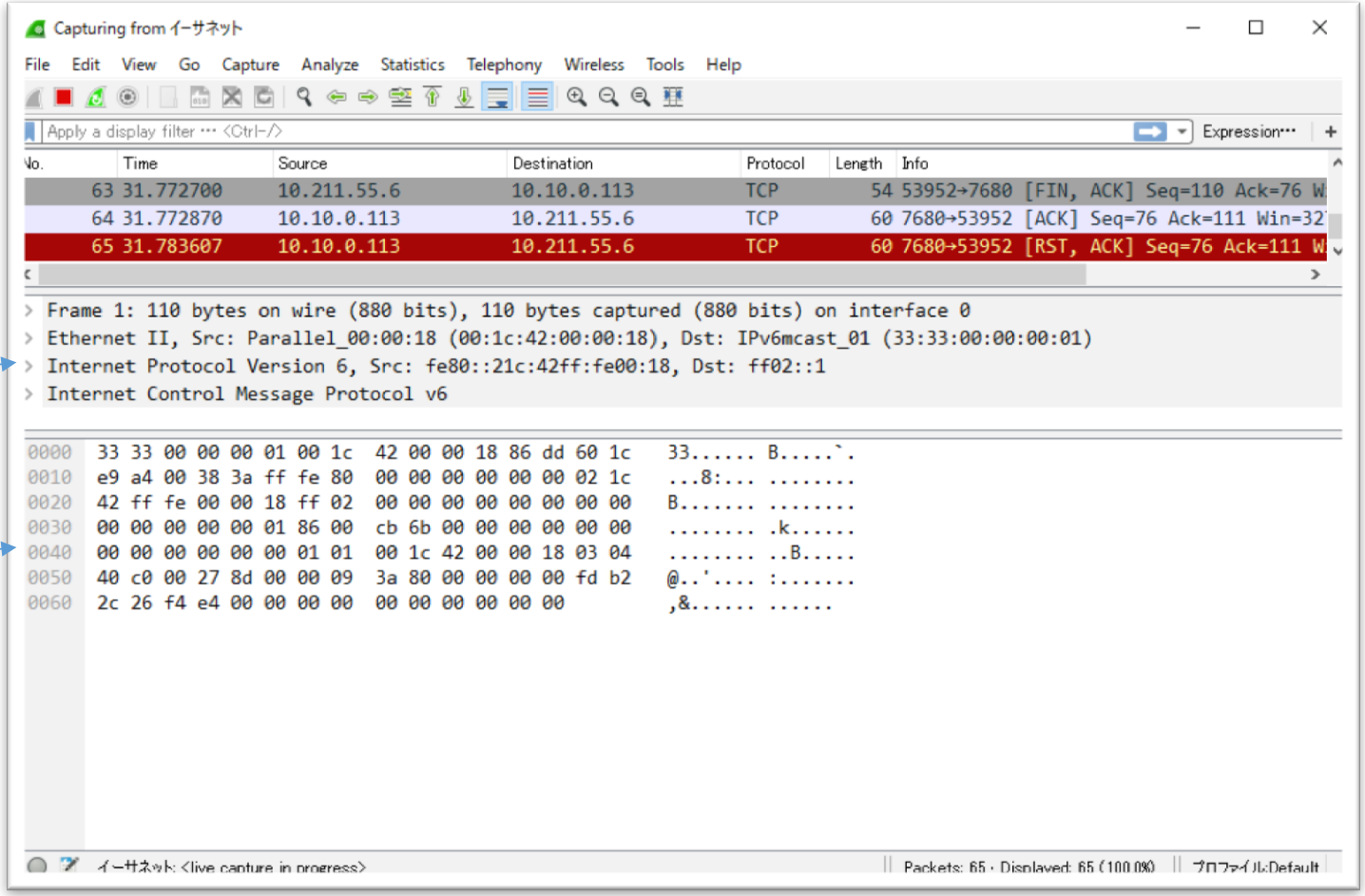
Menu

Filter

Captured data

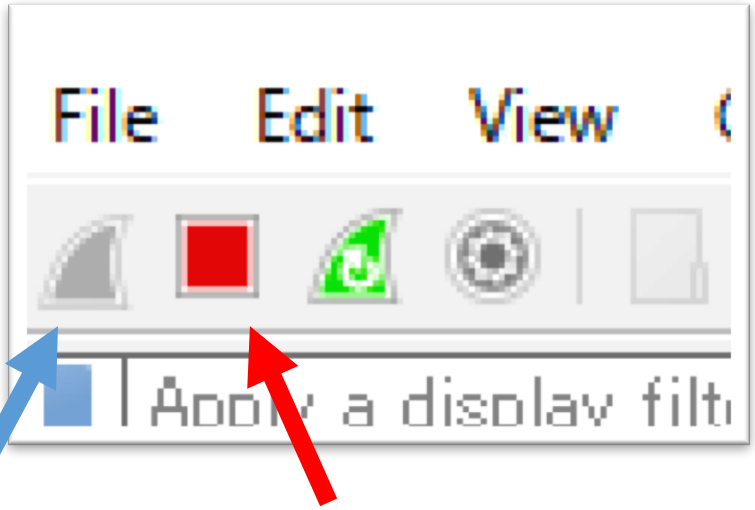
Descriptions of the selected packet

Raw Packet



Stop and start capturing

- As like tcpdump, Wireshark continuously capture packets



Filters

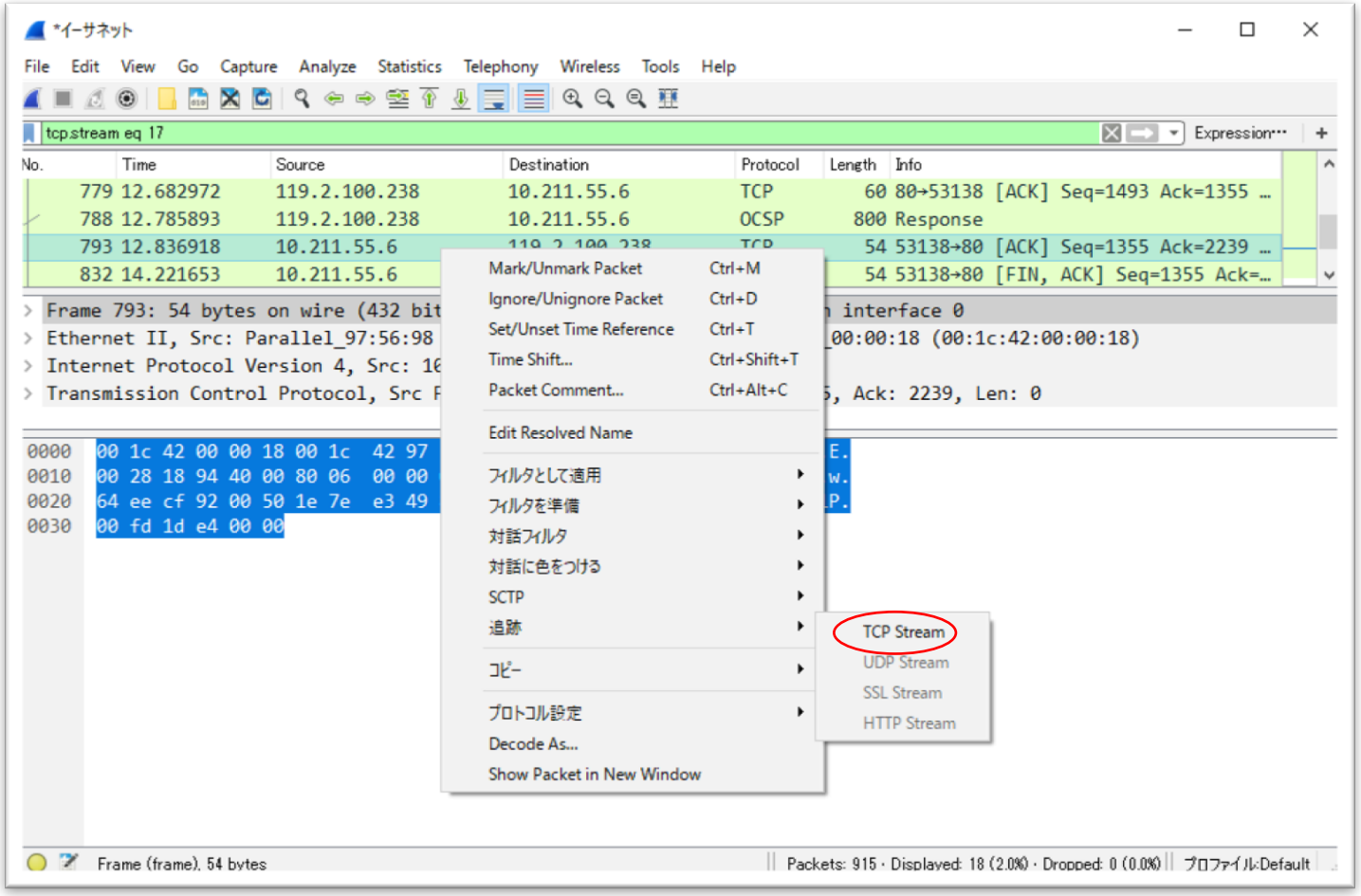
- Capture filter
  - Capture Traffic that match capture filter rule – save disk space
  - prevent packet loss
- Display filter
  - To find particular packets
- Tweak appearance

Apply Filters

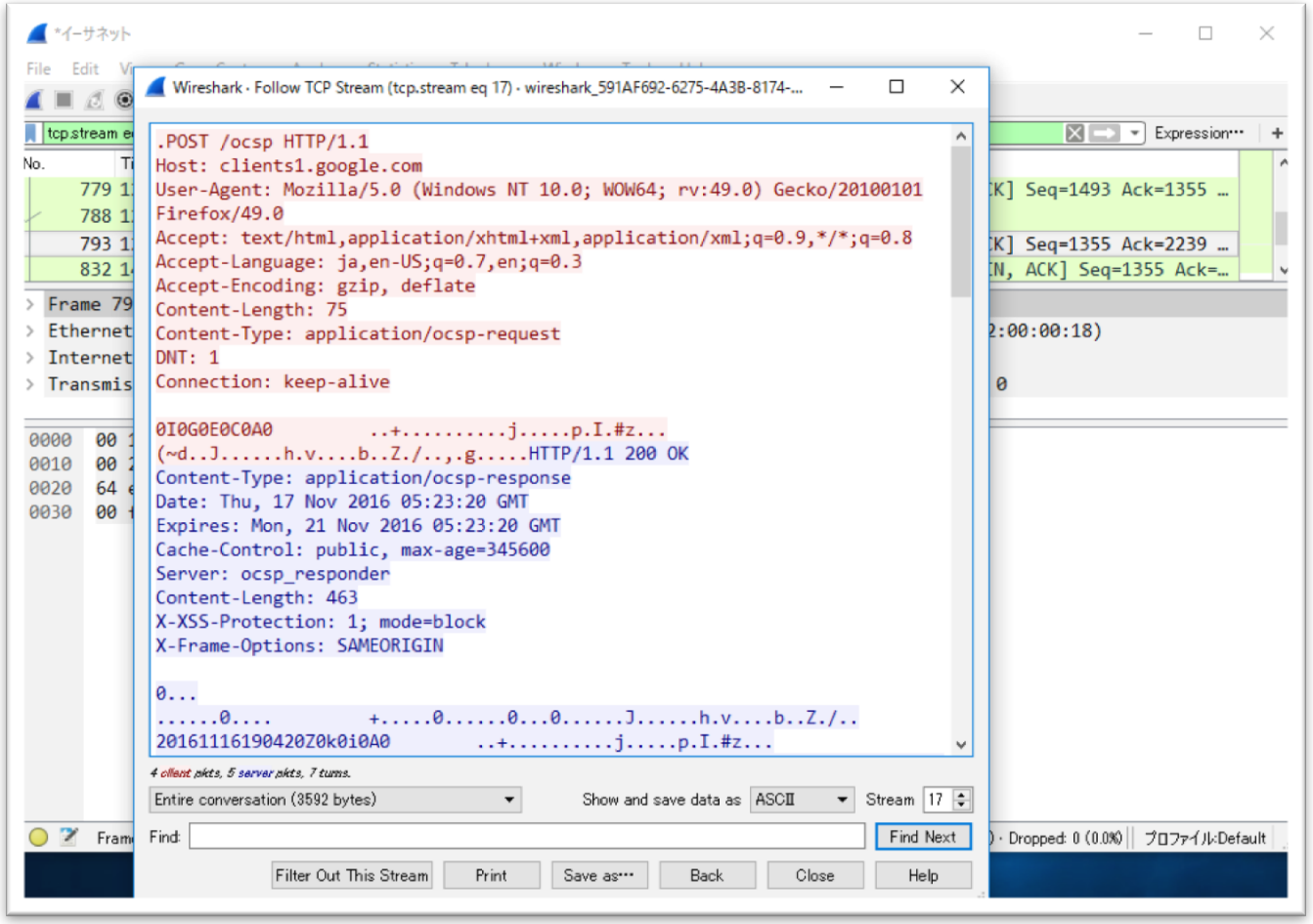
- ip.addr == 10.0.0.1
  - Sets a filter for any packet with 10.0.0.1, as either the source or dest
- ip.addr==10.0.0.1 && ip.addr==10.0.0.2
  - sets a conversation filter between the two defined IP addresses
- http or dns
  - sets a filter to display all http and dns
- tcp.port==4000
  - sets a filter for any TCP packet with 4000 as a source or dest port
- tcp.flags.reset==1
  - displays all TCP resets
- http.request
  - displays all HTTP GET requests
- tcp contains rviews
  - displays all TCP packets that contain the word ‘rviews’. Excellent when searching on a specific string or user ID
- !(arp or icmp or dns)
  - masks out arp, icmp, dns, or whatever other protocols may be background noise. Allowing you to focus on the traffic of interest

TCP stream

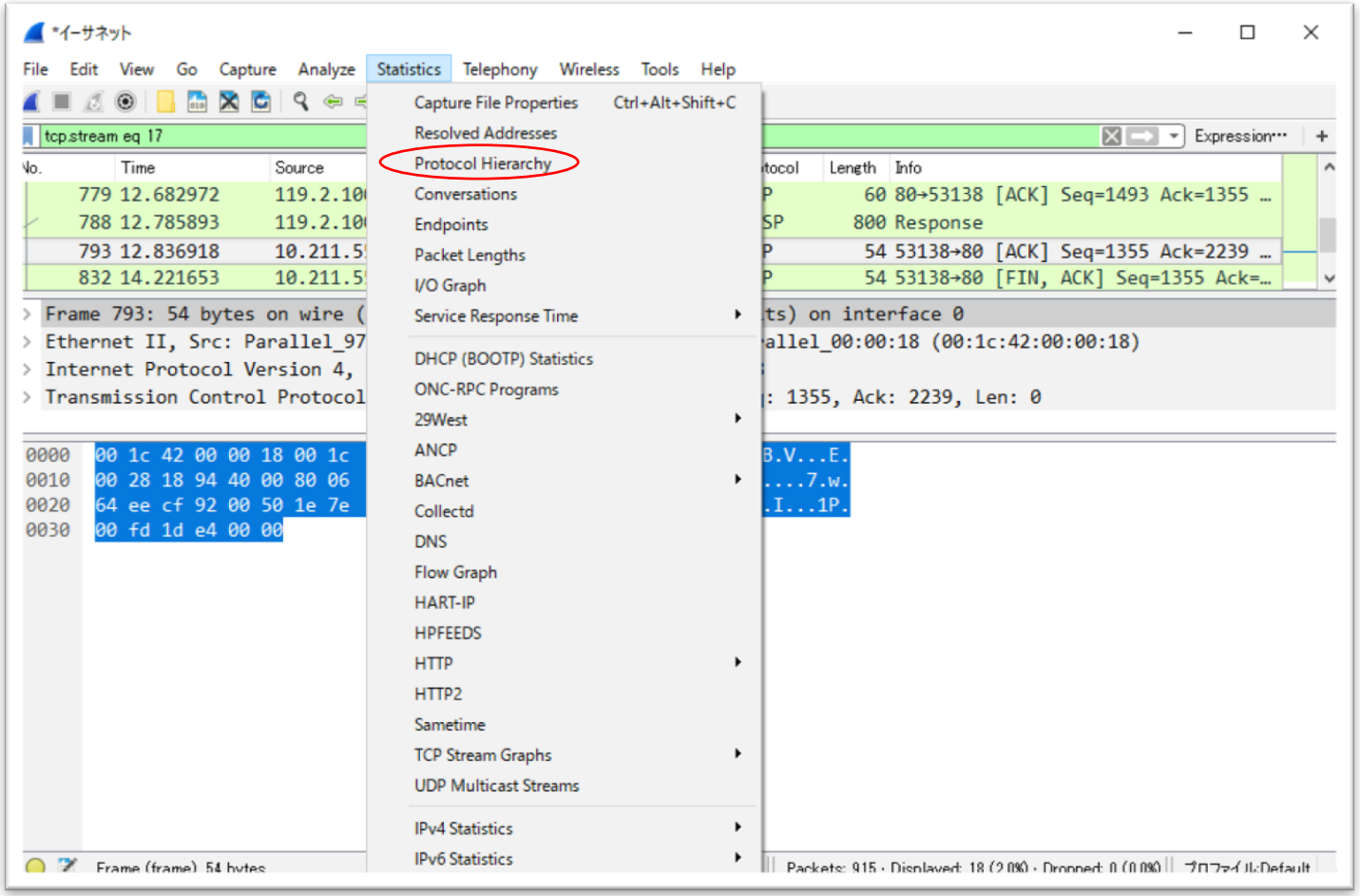
Right click a tcp packet and select ”TCP Stream”



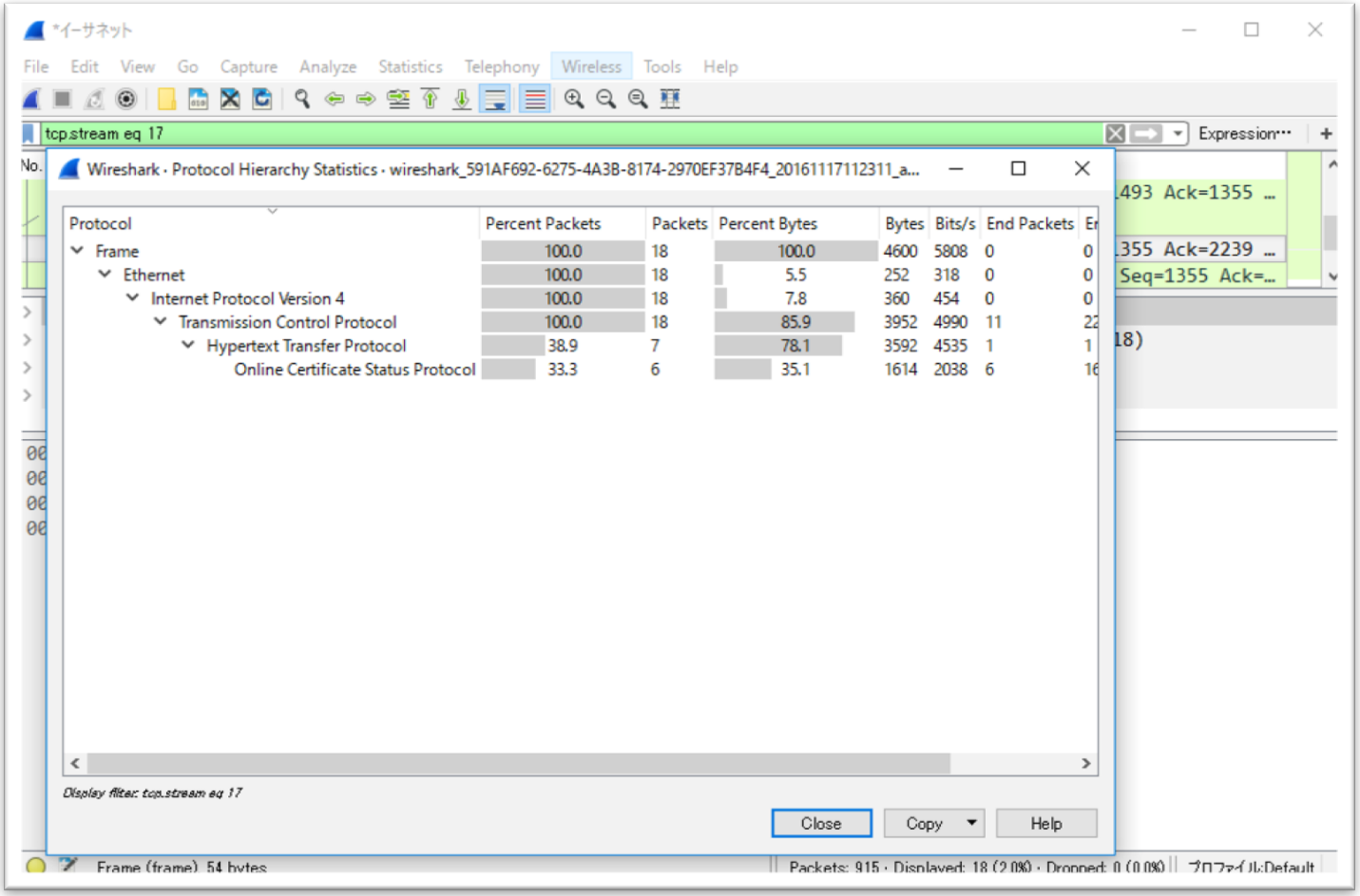
Follow TCP steam



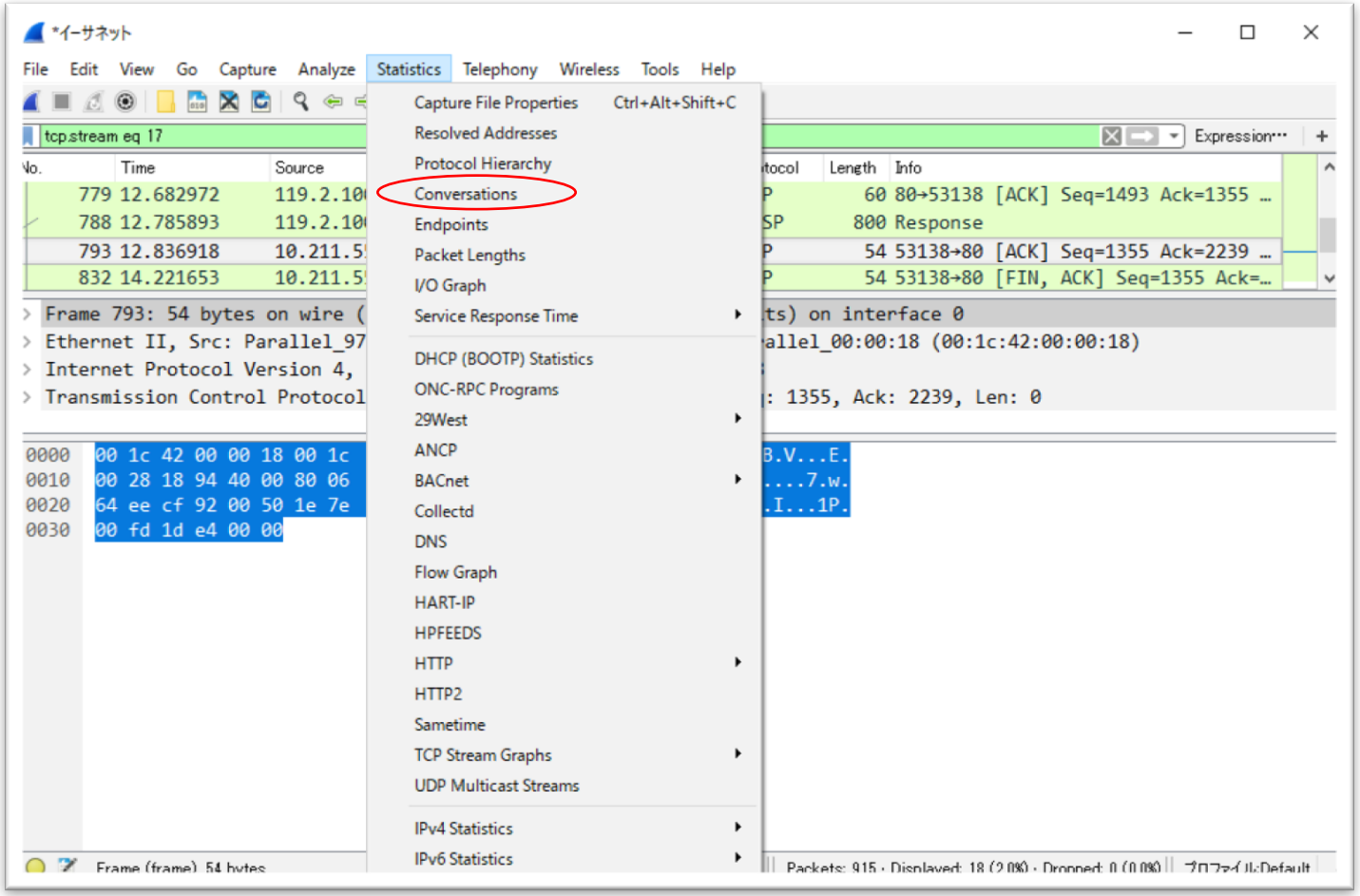
Statistics - Protocol Hierarchy



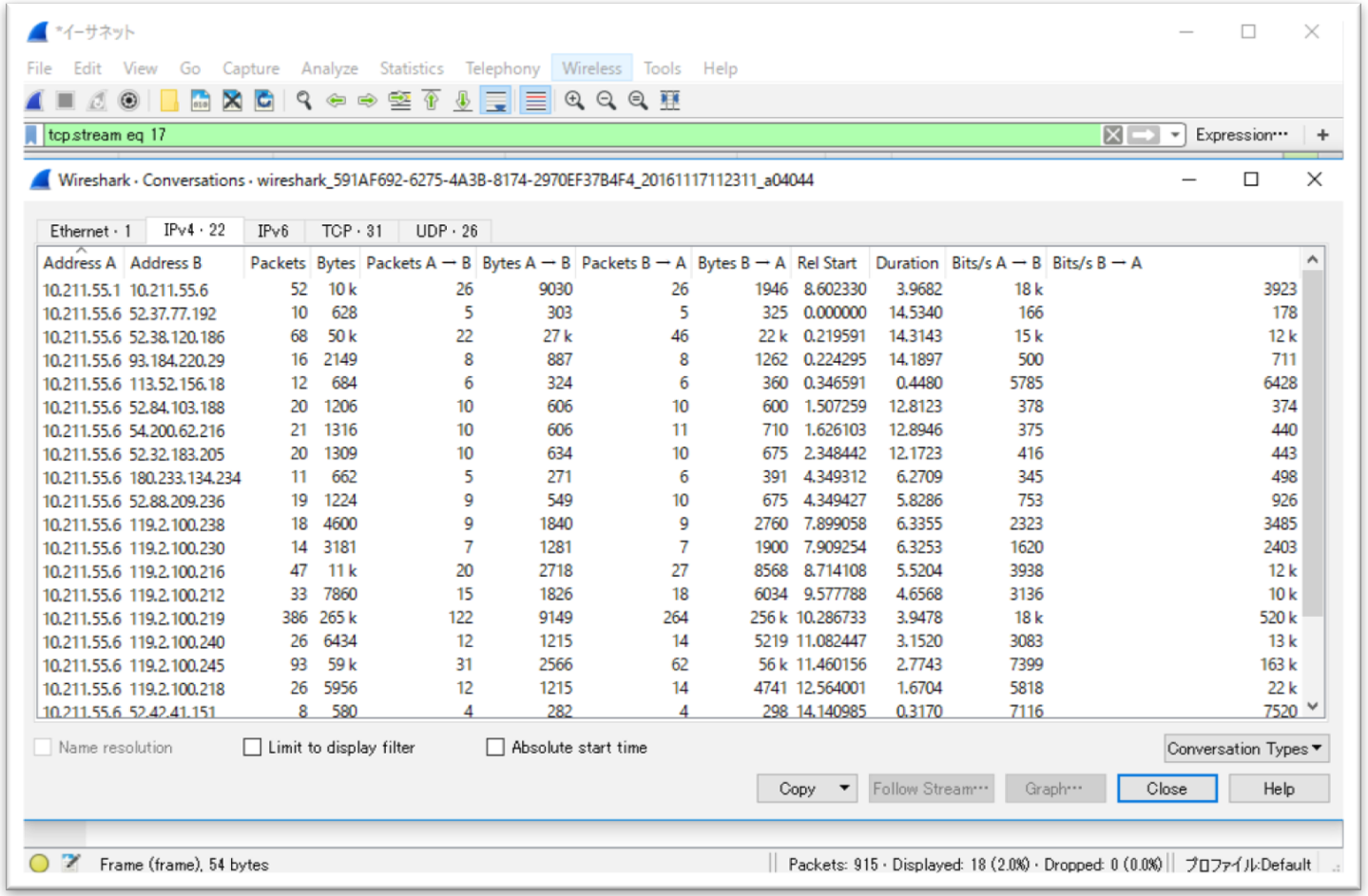
Protocol Hierarchy



Statistics - Conversations



Conversations



Exercise Setup

- Install Wireshark
- Or, you can use VM (tcpdump)
  - $ ssh workshop@10.0.0.x
    - Note: x is your group#
    - Note: password is iij/2497

- Download “packetdump-data.zip” from the workshop web

Exercise 1: Telnet

- File
  - 01telnet.pcap
- Question
  - Reconstruct the telnet session.
- Q1: Who logged into 192.168.0.1
  - Username _____, Password _____ .
- Q2: After logged in what did the user do?
- Tip
  - telnet traffic is not secure

Exercise 2: TCP SYN

- File
  - 02massivesyn1.pcap and 02massivesyn2.pcap
- Question
  - Point the difference with them.
- Q1: 02massivesyn1.pcap is a _____ attempt.
- Q2: 02massivesyn2.pcap is a _____ attempt.
- Tip
  - Pay attention to Src IP

Exercise 3: Chatty Employees

- File
  - 03chat.dmp
- Question
- Q1: What kind protocol is used? _____
- Q2: This is conversation between _____@hotmail.com and _____@hotmail.com
- Q3: What do they say about you(sysadmin)?
- Tip
  - Your chat can be monitored by network admin.

Exercise 4: Suspicious FTP activity

- File
  - 04ftp1.pcap
- Question
- Q1: 10.121.70.151 is FTP _____ .
- Q2: 10.234.125.254 is FTP _____ .
- Q3: FTP Err Code 530 means _____ .
- Q4: 10.234.125.254 attempt _____.
- Tip
  - How many login error occur within a minute?

Exercise 5: Unidentified Traffic

- File
  - 05foobar.pcap
- Question
- Q1: see what's going on
  - Wireshark: Statistics -> Conversation List -> TCP (*)
- Q2: Which application use TCP/6346? Check the web.

Exercise 6: Covert channel

- File
  - 06covertinfo.pcap
- Question
- Q1: What kind of tool do they use? Check the web.
- Q2: Name other application which tunneling user traffic.
- Tip
  - Take a closer look! This is not a typical ICMP Echo/Reply...

Exercise 7: Analyze Malware

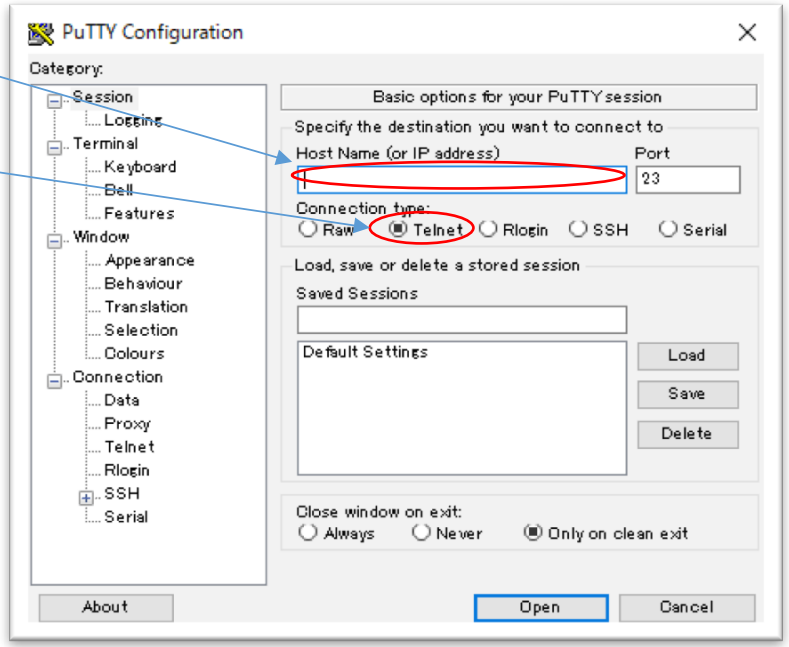
- File
  - 07malware.pcap
- Question
- Q1: Find the bad HTTP traffic
- Q2: Is there any malware in the HTTP traffic?
- Tip
  - Filter with **http contains "in DOS mode”**

Exercise 8: SIP

- File
  - 08sip_chat.pcap
- Question
- Q1: Can we listen to SIP voice?

Exercise 9: Your telnet

- Capture your telnet session to VM
  - PuTTY can telnet
  - Host Name: 10.0.0.x
  - Select Telnet
- Login: workshop
- Password: iij/2497
- Look at the captured data



Exercise 10: Your ssh

- Capture your ssh session to VM
  - $ ssh workshop@10.0.0.x
  - password is iij/2497

- Look at the captured data