Network Forensic:
Exercise

Fakrul Alam (Pappu)
Bangladesh Computer Emergency Response Team

Wireshark?

Wireshark is a network packet/protocol analyzer.

– A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

• Wireshark is perhaps one of the best open source packet analyzers available today for **UNIX** and **Windows**.

About

- Author, Gerald Combs quit Network Integration Services
- Free

• Requirement

- Need to install winpcap
- Latest   , don't worry

  capture

• GUI

- Dramatically improved

Wireshark

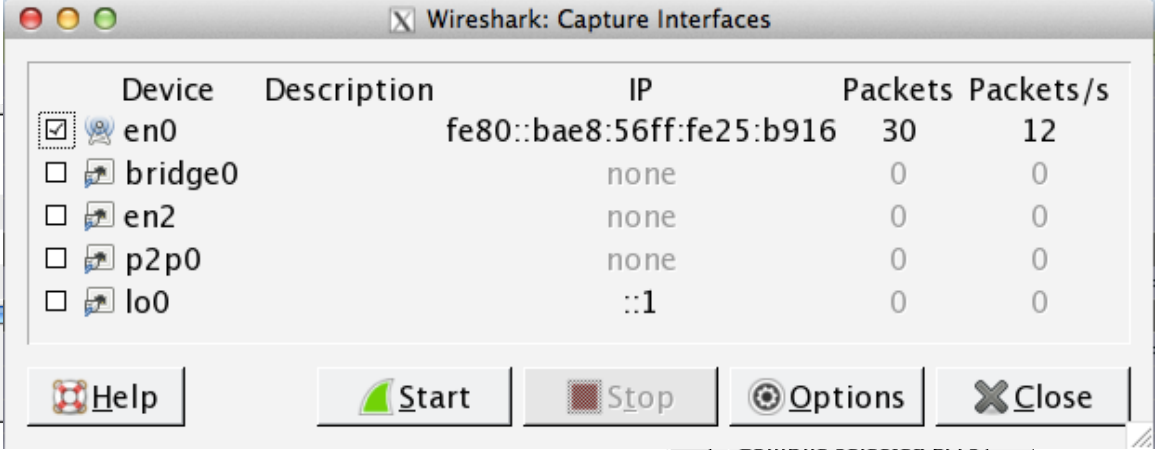- network security engineers use it to **examine security problems**

- developers use it to **debug protocol implementations**

- people use it to **learn network protocol internals**

-

- Wireshark isn't an intrusion detection system.
- Wireshark will not manipulate things on the network, it will only "measure" things from it.

- Very straight forward
- Very straight forward

Capture

Wireshark: Capture Interfaces

	Device	Description	IP	Packets	Packets/s
☑	en0		fe80::bae8:56ff:fe25:b916	30	12
☐	bridge0		none	0	0
☐	en2		none	0	0
☐	p2p0		none	0	0
☐	lo0		::1	0	0

Help   Start   Stop   Options   Close

Wi-Fi: en0	fe80::bae8:56ff:fe25:b916 172.16.1.6	Ethernet
☑		
☐ Thunderbolt Bridge: ...	Ethernet	
☐ Thunderbolt 1: en2	Ethernet	
☐ p2p0	Raw IP	

☐ Capture on all interfaces
☑ Use promiscuous mode on all interfaces
☑ Capture Filter:

Capture Files

File: [   ] Browse...

☐ Use multiple files   ☑ Use pcap-ng format
☑ Next file every   1   megabyte(s)
☐ Next file every   1   minute(s)
☐ Ring buffer with   2   files
☐ Stop capture after 1   file(s)

Stop Capture Automatically After...

☐ 1   packet(s)
☐ 1   megabyte(s)

Display Options

☑ Update list of packets in real time

☑ Automatically scroll during live capture

☑ Hide capture info dialog

Name Resolution

☑ Resolve MAC addresses

☐ Resolve network-layer names

☑ Resolve transport-layer name

☑ Use external network name resolver

Dashboard

Filters

- Capture filter
  - Capture Traffic that match capture filter rule
  - save disk space
  - prevent packet loss
- Display filter
- 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]

Follow TCP Stream

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: [   ] ▼ Expression... Clear Apply Save

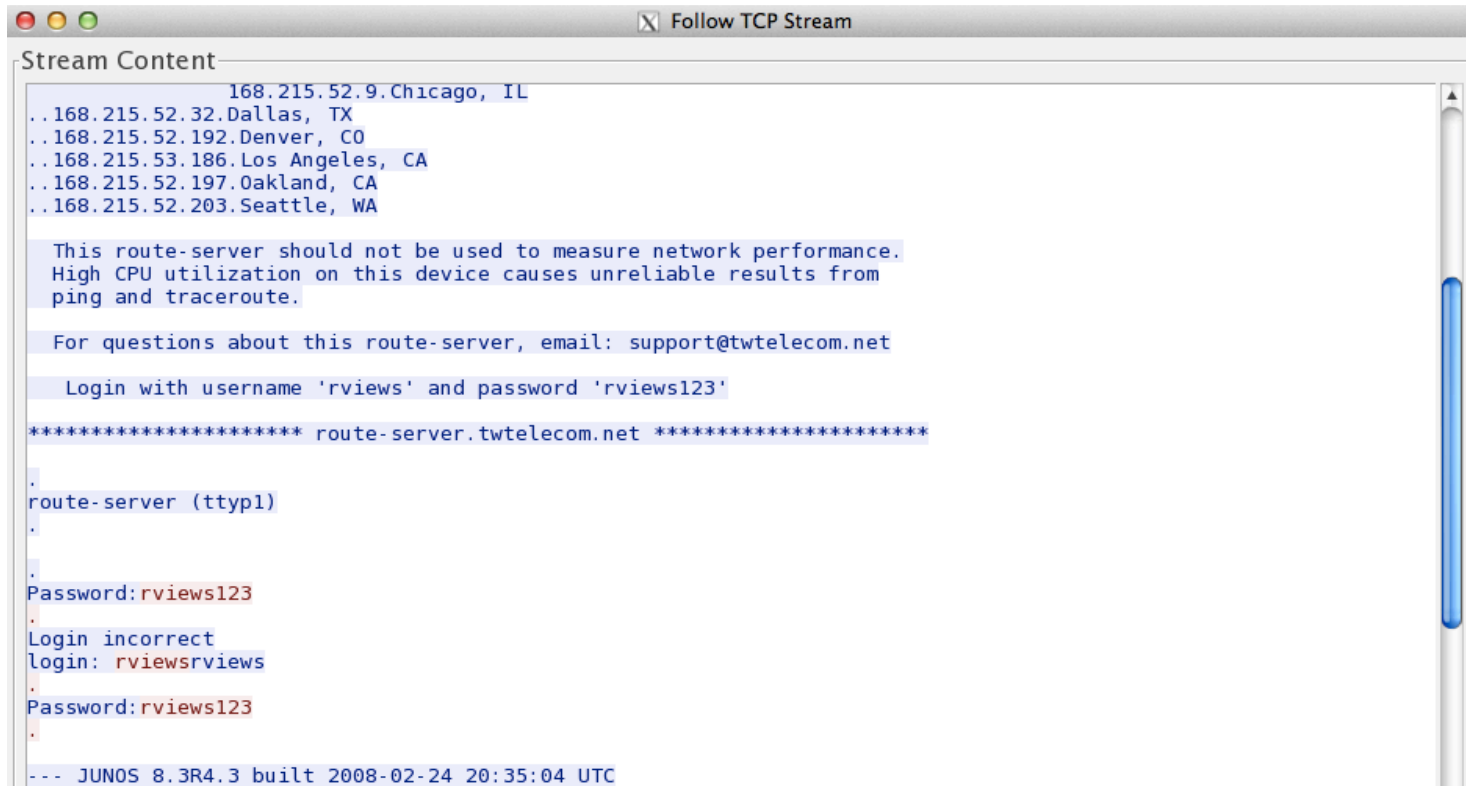| No.	Time	Source	Destination	Protocol	Length	Info
111	14.339156000	172.16.1.3	224.0.0.1	BJNP	58	Scanner Command: Unknown code (2)
112	15.352153000	172.16.1.6	202.4.97.11	SIP	767	Request: PUBLISH sip:09611033085@202.4.97.11;transport=UDP |
113	15.352381000	172.16.1.6	82.129.27.63	CLASSIC-S	70	Message: Binding Request
114	15.352412000	172.16.1.6	202.4.97.11	SIP	996	Request: REGISTER sip:202.4.97.11;transport=UDP |
115	15.352436000	172.16.1.6	202.4.97.11	UDP	46	Source port: 52696 Destination port: sip
116	15.359213000	202.4.97.11	172.16.1.6	SIP	573	Status: 200 OK (1 bindings) |
117	15.773121000	82.129.27.63	172.16.1.6	CLASSIC-S	130	Message: Binding Response
118	16.275298000	172.16.1.6	66.195.95.174	TELNET	72	Telnet Data
119	16.806218000	66.195.95.174	172.16.1.6	TELNET		
120	16.806322000	172.16.1.6	66.195.95.174	TCP		=1277 Win=131056 Len=0 TSval=765842538 TSecr=19497
121	17.112570000	172.16.1.6	66.195.95.174	TELNET		
122	17.616299000	66.195.95.174	172.16.1.6	TELNET		
123	17.616389000	172.16.1.6	66.195.95.174	TCP		=1279 Win=131056 Len=0 TSval=765843345 TSecr=19497
124	18.025688000	66.195.95.174	172.16.1.6	TELNET		
125	18.025773000	172.16.1.6	66.195.95.174	TCP		=1288 Win=131056 Len=0 TSval=765843753 TSecr=19497
126	19.709711000	172.16.1.6	66.195.95.174	TELNET		
127	19.711165000	173.194.38.150	172.16.1.6	TLSv1.2		
128	19.711240000	172.16.1.6	173.194.38.150	TCP		=1486 Win=16380 Len=0
129	20.278535000	66.195.95.174	172.16.1.6	TCP		k=290 Win=57920 Len=0 TSval=1949725785 TSecr=76584

▷ Frame 118: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
▷ Ethernet II, Src: Apple_25:b9:16 (b8:e8:56:25:b9:16), Dst: Netgear_a5:25:96 (c0:3f:0e:a5
▷ Internet Protocol Version 4, Src: 172.16.1.6 (172.16.1.6), Dst: 66.195.95.174 (66.195.95
▷ Transmission Control Protocol, Src Port: 49447 (49447), Dst Port: telnet (23), Seq: 273,
▷ Telnet

Context menu:
- Mark Packet (toggle)
- Ignore Packet (toggle)
- 🕒 Set Time Reference (toggle)
- 🕒 Time Shift...
- 📝 Packet Comment...
- Manually Resolve Address
- Apply as Filter ▶
- Prepare a Filter ▶
- Conversation Filter ▶
- Colorize Conversation ▶
- SCTP ▶
- **Follow TCP Stream**
- Follow UDP Stream
- Follow SSL Stream
- Copy ▶
- Protocol Preferences ▶
- Decode As...
- Print...
- Show Packet in New Window

```
0000  c0 3f 0e a5 25 96 b8 e8  56 25 b9 16 08 00 45 10   .?..%... V%....E.
0010  00 3a 33 b8 40 00 40 06  b7 6e ac 10 01 06 42 c3   .:3.@.@. .n....B.
0020  5f ae c1 27 00 17 47 46  90 1f 8c 0e 0c 7c 80 18   _..'..GF .....|..
0030  20 00 9d 70 00 00 01 01  08 0a 2d a5 d2 59 74 36    ..p.... ..-..Yt6
0040  71 03 72 76 69 65 77 73                            q.rviews
```

Follow TCP Stream

- Build TCP Stream
  - Select TCP Packet -> Follow TCP Stream


```
                    168.215.52.9.Chicago, IL
..168.215.52.32.Dallas, TX
..168.215.52.192.Denver, CO
..168.215.53.186.Los Angeles, CA
..168.215.52.197.Oakland, CA
..168.215.52.203.Seattle, WA

 This route-server should not be used to measure network performance.
 High CPU utilization on this device causes unreliable results from
 ping and traceroute.

 For questions about this route-server, email: support@twtelecom.net

  Login with username 'rviews' and password 'rviews123'

********************* route-server.twtelecom.net *********************

.
route-server (ttyp1)
.

.
Password:rviews123
.
Login incorrect
login: rviewsrviews
.
Password:rviews123
.

--- JUNOS 8.3R4.3 built 2008-02-24 20:35:04 UTC
```
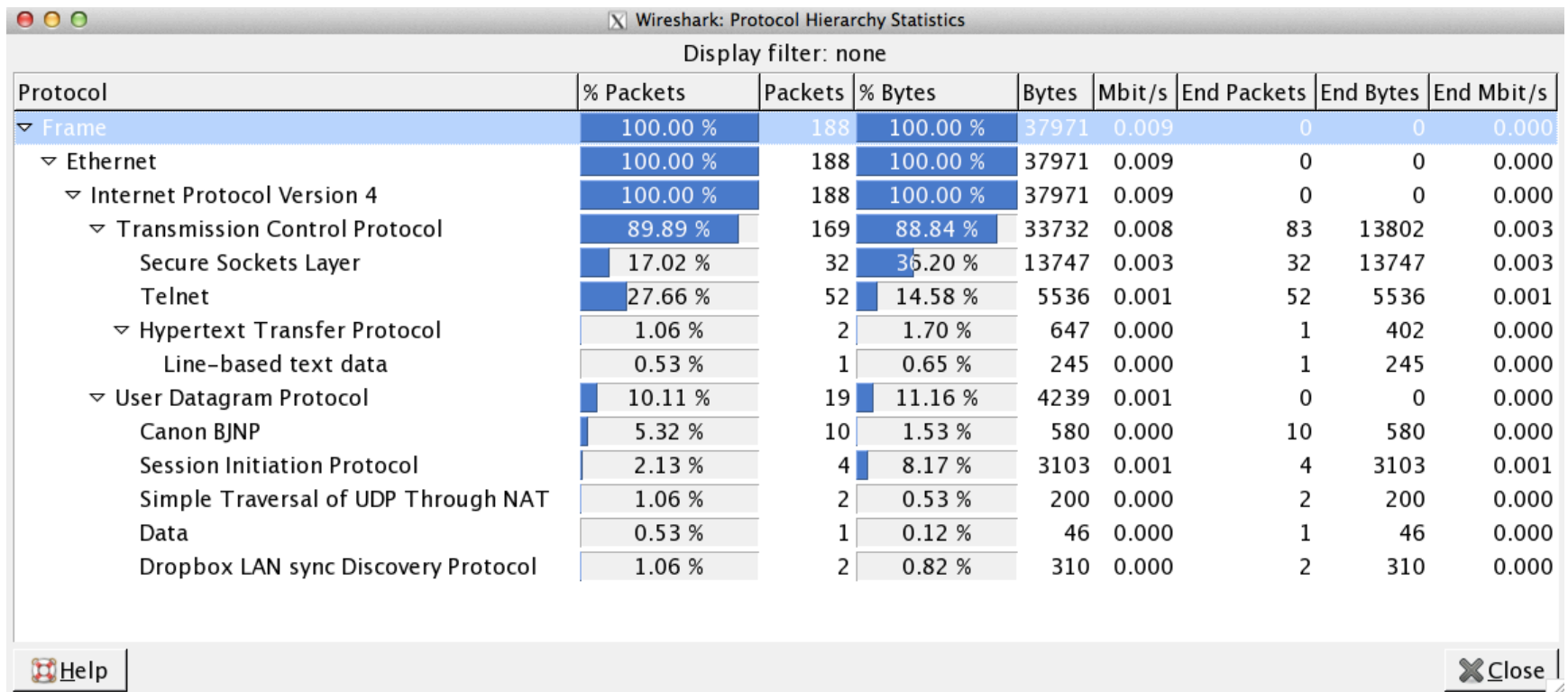
Use "Statistics"

- What protocol is used in your network
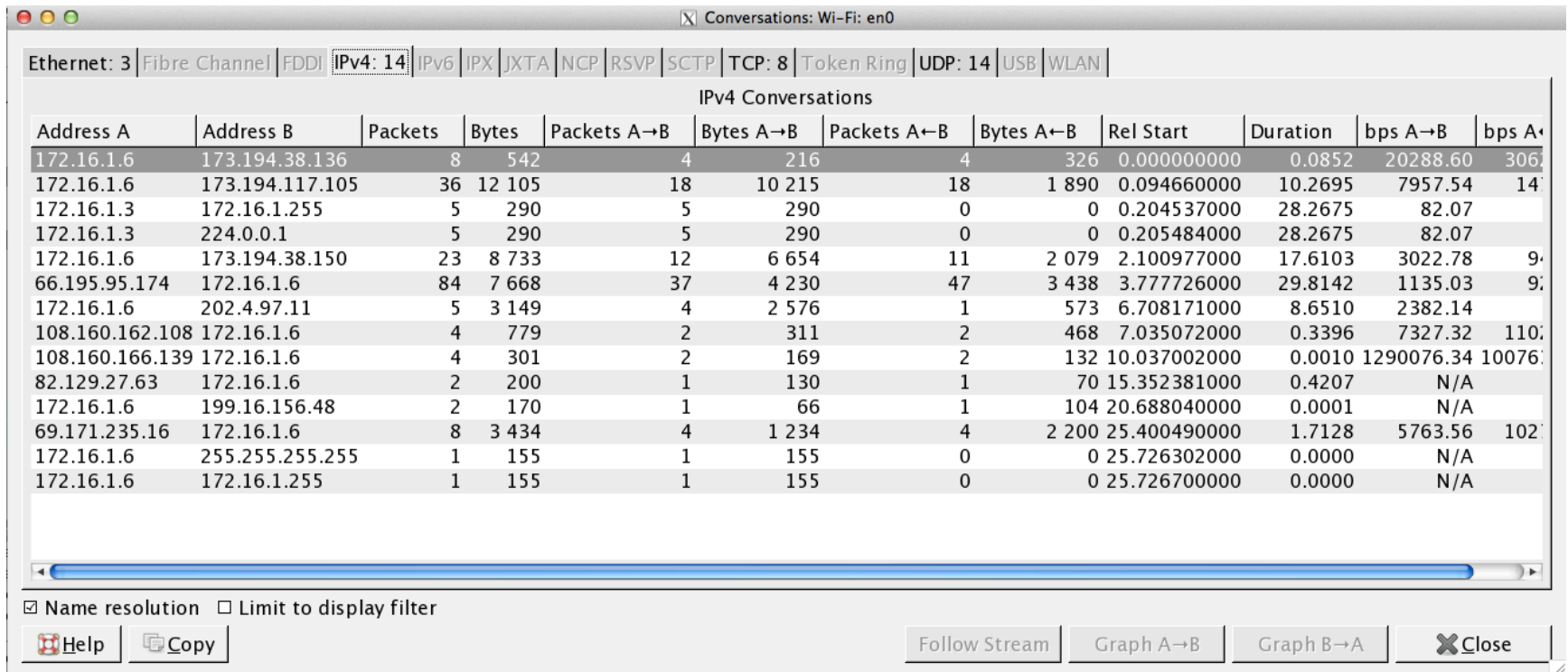 - Statistics -> Protocol Hierarchy

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▽ Frame	100.00 %	188	100.00 %	37971	0.009	0	0	0.000
▽ Ethernet	100.00 %	188	100.00 %	37971	0.009	0	0	0.000
▽ Internet Protocol Version 4	100.00 %	188	100.00 %	37971	0.009	0	0	0.000
▽ Transmission Control Protocol	89.89 %	169	88.84 %	33732	0.008	83	13802	0.003
Secure Sockets Layer	17.02 %	32	36.20 %	13747	0.003	32	13747	0.003
Telnet	27.66 %	52	14.58 %	5536	0.001	52	5536	0.001
▽ Hypertext Transfer Protocol	1.06 %	2	1.70 %	647	0.000	1	402	0.000
Line-based text data	0.53 %	1	0.65 %	245	0.000	1	245	0.000
▽ User Datagram Protocol	10.11 %	19	11.16 %	4239	0.001	0	0	0.000
Canon BJNP	5.32 %	10	1.53 %	580	0.000	10	580	0.000
Session Initiation Protocol	2.13 %	4	8.17 %	3103	0.001	4	3103	0.001
Simple Traversal of UDP Through NAT	1.06 %	2	0.53 %	200	0.000	2	200	0.000
Data	0.53 %	1	0.12 %	46	0.000	1	46	0.000
Dropbox LAN sync Discovery Protocol	1.06 %	2	0.82 %	310	0.000	2	310	0.000

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Help — Close

Use "Statistics"

- Which host most chatty
  - Statistics -> Conversations

Use "Statistics"

- Make graph
  - Statistics -> IO Graph
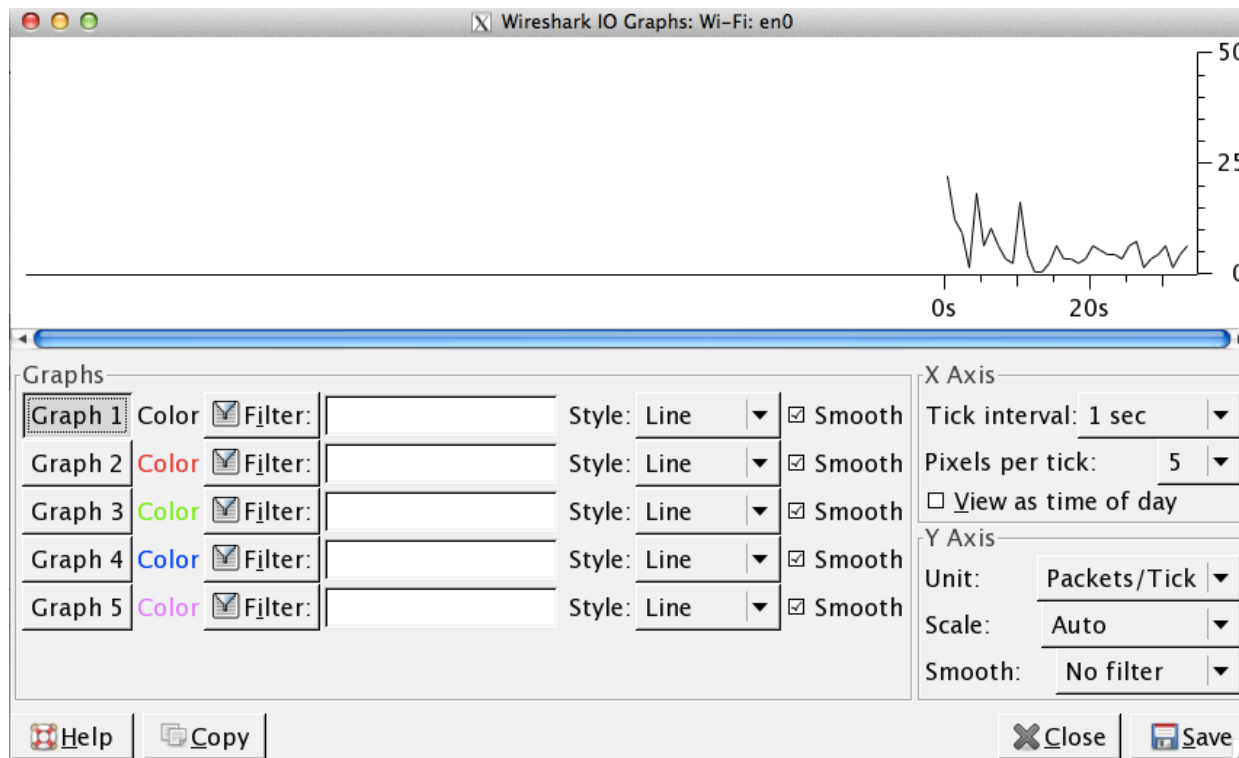
Need CUI?

- If you stick to character based interface, try tshark.exe
- C:\program files\wireshark\tshark.exe

Tcpdump & Wireshark

- tcpdump -i <interface> -s 65535 -w <some-file>

Exercise

- Install Wireshark into your PC
- Run wireshark and Capture inbound/outbound traffic
- Download capture files from
  - Follow the instructor's guide.

Exercise1: Good Old Telnet

- File
  - telnet.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: Massive TCP SYN

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

Exercise 3: Compare the traffic

- Scenario
- You're an IT admin of company X. You had a report that Jim (a new employee) can not browse or mail with his laptop. After researching you found that Risa, sitting next to Jim, can brose without any problem.
- File
  - Risa.pcap, jim.pcap
- Question
- Compare the capture file from both machines and find out why Jim's machine is not online.
  - Jim must _____ .
- Tip
  - Pay attention to the first arp packet.

Exercise 4: Chatty Employees

- File
  - chat.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 5: Suspicious FTP activity

- File
  - ftp1.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 6: Unidentified Traffic

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

Exercise 7: Covert channel

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