



# SharkFest '18 ASIA



## Wireshark Saves the Day!

A Beginner's Guide to Packet Analysis



Slot1Port0Hostnp1.D.1522808953060.pcap

frame contains "Maher Adib"

Source	Destination	Protocol	Text
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.85	10.10.10.100	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.
10.10.10.100	10.10.10.85	TCP	b. Welcome To Sharkfest'18 Asia!My name is Maher Adib.



# Those Were The Days



What's on your network?

Ethereal-users: [Ethereal-users] monitor and analyze the users

Note: This archive is from the project's previous web site, ethereal.com. This list is no longer active.

- Date Index
- Thread Index
- Other Months
- All Mailing Lists
- Date Prev
- Date Next
- Thread Prev
- Thread Next

From: maher abedib <m2600@xxxxxxxxxxxx>  
Date: Sun, 19 Nov 2000 07:21:36 +0800

Hi everyone,

I start using ethereal since Richard Sharpe give us a talk in LinuxWorld Malaysia a few weeks ago. When I fire up the ethereal ,wow ... I can see my users start to logging/do some their stuff like ftp, telnet and etc.

>From there, I can monitor my users up to.But in order to monitor it, I have to highlight and analyze some packet and use the option "follow tcp stream" and then I can see every keystroke/data that my users type to my Linux server.

If possible,I would like to know, can ethereal continuously monitor the users keystorke,for example,I targeted this user(maher) and see this every single thing that he do.What do I know is the ethereal is a network protocal analyzer.What is the differences between proctol analyzer and keystroke monitoring( monitor users live some sort like capturing the tty users).Can ethereal be functional like that?

Anyway,thank you Richard for highlight/bring up some ethereal development in LinuxWorld Malaysia.

regards,

maher adib

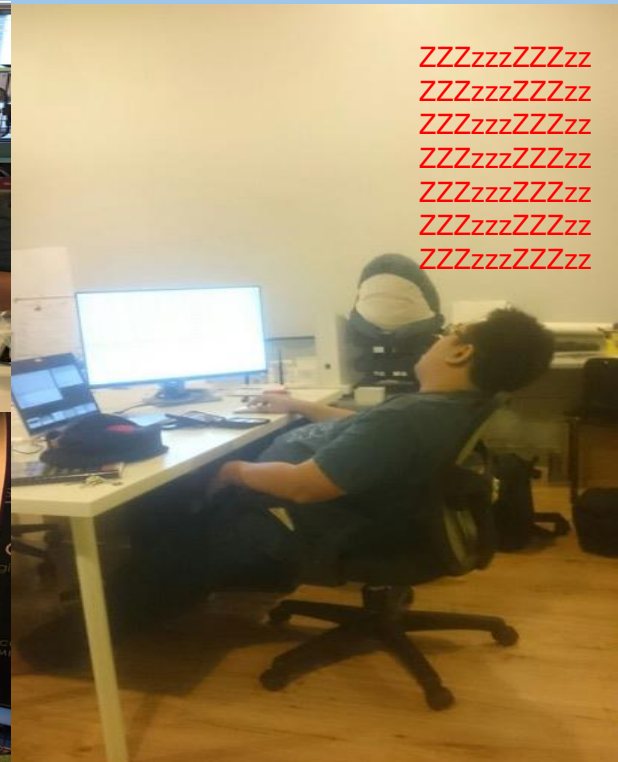
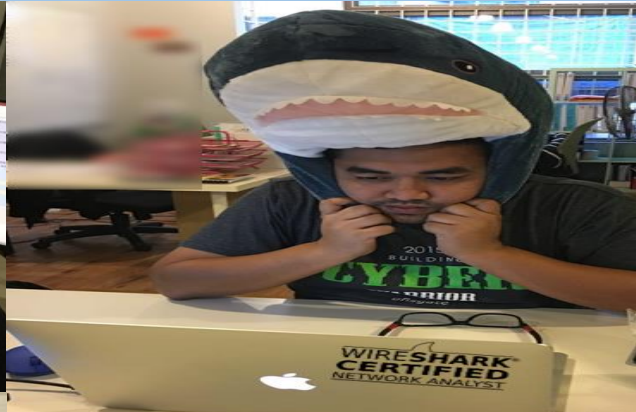
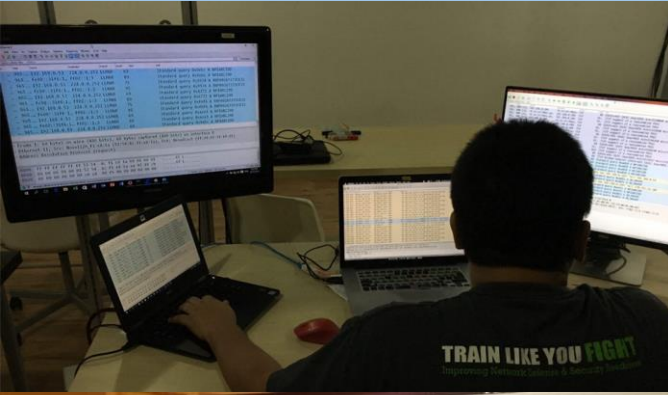


ETHEREAL  
PACKET SNIFFER





# Not an easy job!



What My Company Think I'm Doing

What My Customer see Everyday

This is what I Do Everyday!



# Wireshark To The Rescue!



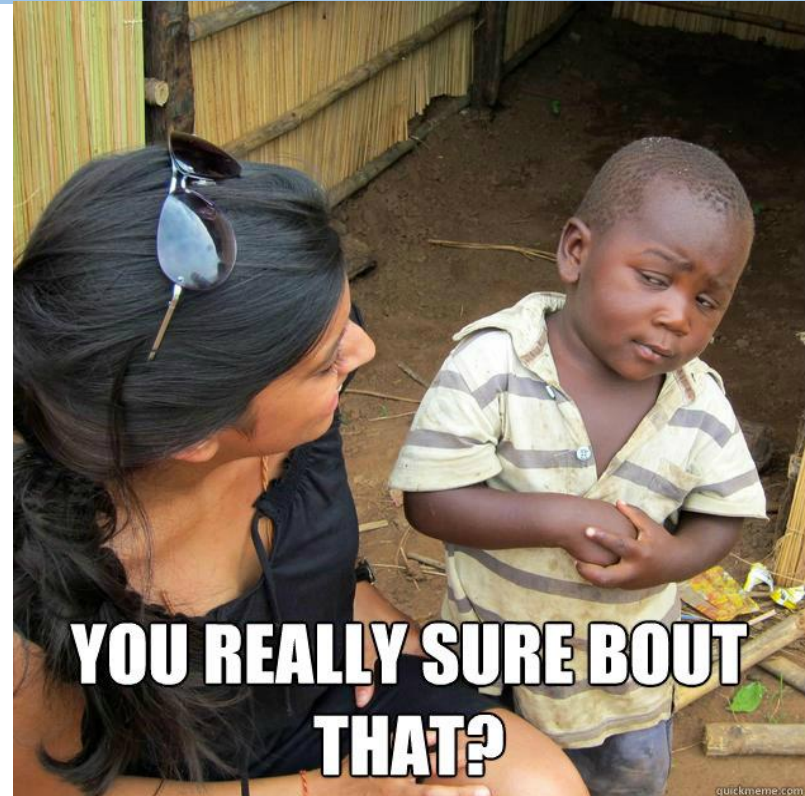


# Trust, But Verify...



Verify what you read. Wireshark is a fantastic educational and verification tool. Wireshark allows us to do that by seeing the actual traffic being sent on the wire, including details such as:

- Protocols
- Port and Protocol numbers
- Header types
- Addresses
- Payloads
- and more, more and more... Thanks Core Dev!





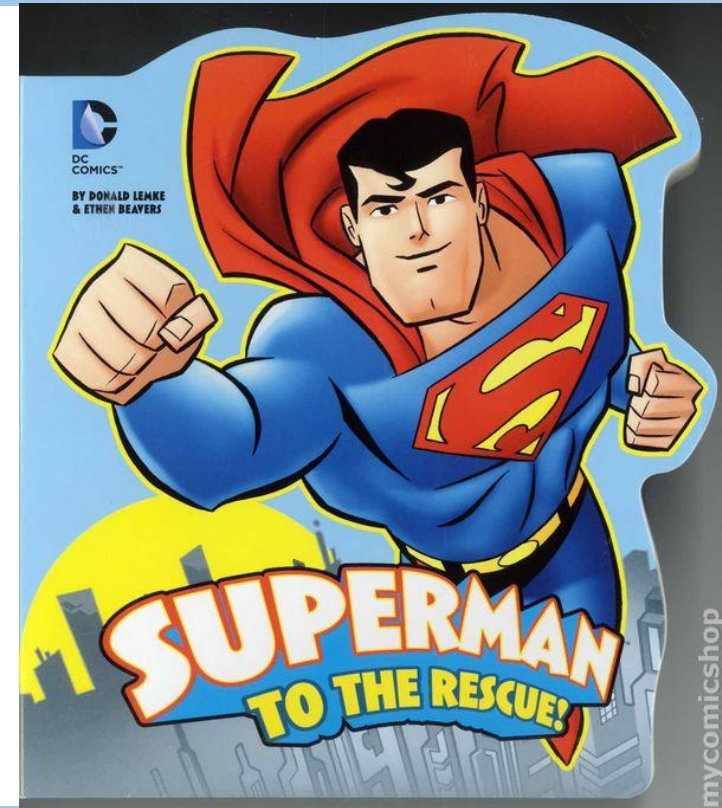


# Be “That” Person!



Many times, a problem can't be solved without going to the packet or frame level to see what is going on.

In that moment, you can be “that person” who has taken the time to learn Wireshark and can now apply the skills to quickly capture and analyze the traffic in question.





# Enjoy The Moments...



It's exciting. Wireshark is one of the most fun network tools out there, when the user of Wireshark has taken some time to learn how to use its features.

Most IT folks still get a thrill out of using Wireshark (and the insight it provides) even after many years of experience in the field.

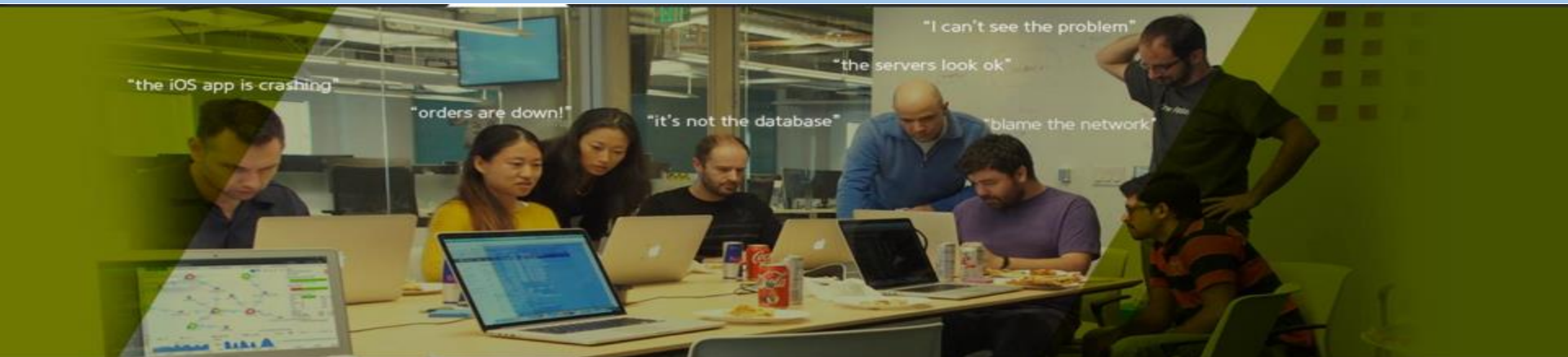
There's always something new to learn from the packets coursing through the veins of a network.







# Sound Familiar?



Solve Problem X



Big Boss

I will do that.



Manager

Solve Problem X



Manager

We will do that.



Project Team

X is not the right problem to solve.



Enterprise Architect

Shut up.

Go away.

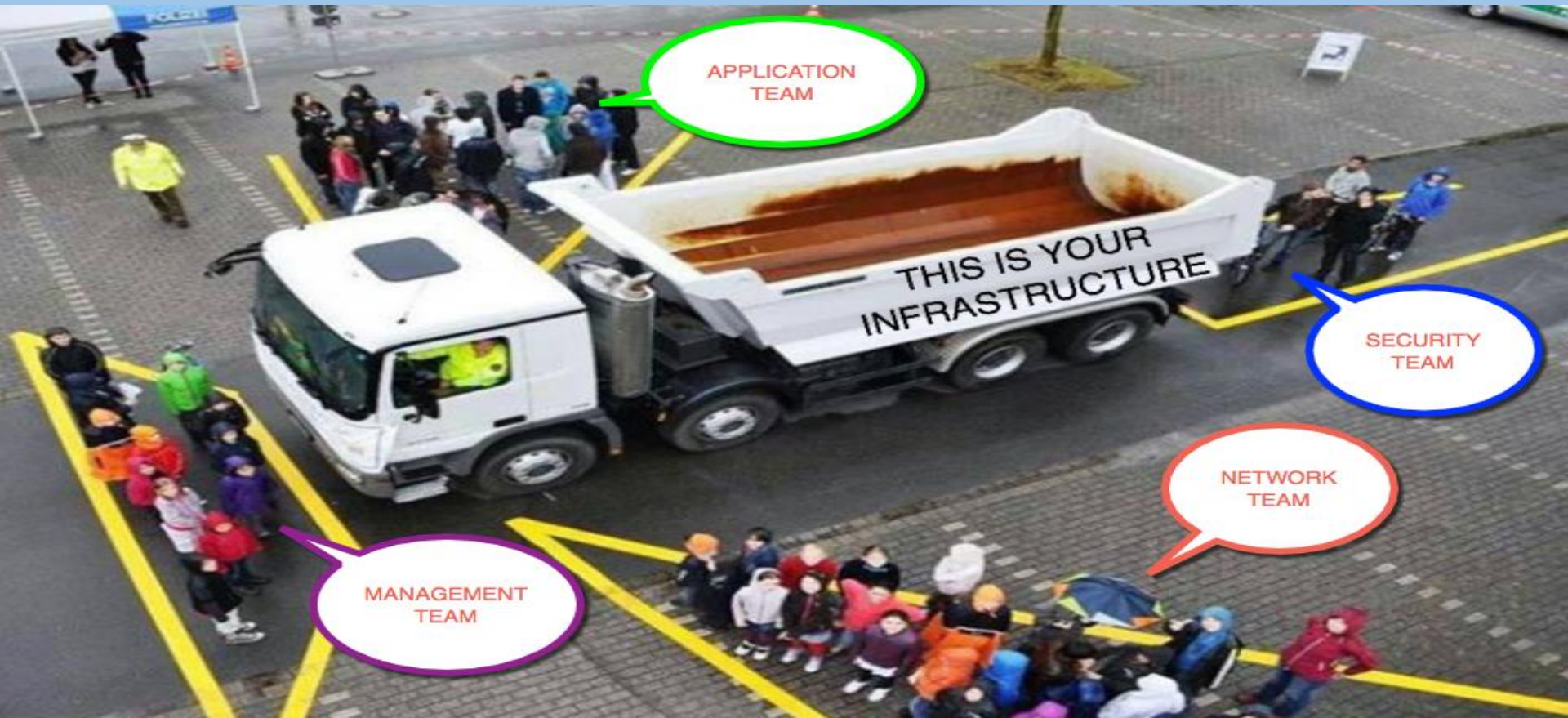
Idiot.



Project Team



# Different Views



APPLICATION  
TEAM

THIS IS YOUR  
INFRASTRUCTURE

SECURITY  
TEAM

NETWORK  
TEAM

MANAGEMENT  
TEAM



# What is your skills level with Wireshark?



- A. I know how to spell it
- B. I know how to scroll and see the packet
- C. I am comfortable capturing and analyzing most traffic
- D. I use it daily. I eat packet for breakfast ( Not Me! )



Beginner - Intermediate





<https://www.wireshark.org/download.html>



NEWS Get Acquainted ▾ Get Help ▾ Develop ▾ Our Sponsor [SharkFest](#)

## Download Wireshark

The current stable release of Wireshark is 2.4.6. It supersedes all previous releases. You can also download the latest development release (2.5.1) and documentation.

- Stable Release (2.4.6)** ←
- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.6 and later Intel 64-bit .dmg
- Source Code
- Old Stable Release (2.2.14)
- Development Release (2.5.1)
- Documentation

Having Problems?

Explore our [download area](#) or look in our [third party package list](#) below.

Installation Notes

### Downloads

Clear

- wireshark-2.4.6.tar.xz  
28.9 MB
- Wireshark 2.4.6 Intel 64.dmg  
27.7 MB of 42.5 MB — 35 seconds remaining
- WiresharkPortable\_2.4.6.paf.exe  
28.8 MB of 45.4 MB — 39 seconds remaining
- Wireshark-win32-2.4.6.exe  
30.9 MB of 52.7 MB — 49 seconds remaining
- Wireshark-win64-2.4.6.exe  
38.3 MB of 57.9 MB — 36 seconds remaining



# What Is Packet Analysis?



Anyone can analyze network communications. You do, however, need to acquire three basic skills to be a top notch packet analyst who can spot the cause of performance problems, evidence of breached hosts, misbehaving applications or the impending overload of the network.

- A solid understanding of TCP/IP communications**
- Comfort using any network analyzer (Wireshark)**
- Familiarity with packet structures and typical packet flows**



# TCP/IP Communication



Application

[Response in frame: 168228]

Presentation

[Full request URI: http://www.ofisgateacademy.com/]  
[HTTP request 1/1]

Session

\r\n  
Connection: keep-alive\r\n  
Accept-Encoding: gzip, deflate\r\n  
Accept-Language: en-us\r\n

Transport

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_6\_8; rv:1.9.2.15) Gecko/20111201 Firefox/3.6.15  
Accept: text/html,application/xhtml+xml,application/javascript;q=0.9,\*/\*;q=0.8  
Upgrade-Insecure-Requests: 1\r\n  
Host: www.ofisgateacademy.com\r\n

Network

GET / HTTP/1.1\r\n  
Hypertext Transfer Protocol

Data Link

Transmission Control Protocol, Src Port: 62931, Dst Port: 80  
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 192.168.0.1  
Ethernet II, Src: Apple\_cb:39:45 (68:5b:35:cb:39:45), Dst: Realtek\_8c:85:3e:12:12:12 (08:00:27:8c:85:3e:12:12:12), Length: 1440

Physical

Frame 168210: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface 0





# Comfort using any network analyzer (Wireshark)



**Packet comments**

- Looks Like DNS Request

Frame 11: 104 bytes on wire (832 bits), 104 bytes captured on interface eth0

Ethernet II, Src: Apple 28:74:ac (e4:ce:8f:28:74:ac), Dst: 08:00:27:00:00:00

Client packet

Older version of wireshark

Server packets

HTTP/1.1 200 OK  
Date: Sun, 15 Jan 2017 06:55:52 GMT  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod\_perl/2.0.10 Perl/v5.16.3  
Last-Modified: Sun, 15 Jan 2017 06:55:01 GMT  
ETag: "1194-5461c8b9f0f0"  
Accept-Ranges: bytes  
Content-Length: 4500  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

html<head>  
<title>Historical Documents:THE BILL OF RIGHTS</title></head>  
<body bgcolor="#ffffff" link="#330000" vlink="#666633">  
<p><br>  
</p>  
<p></p><center><b>THE BILL OF RIGHTS</b></center>  
<em>Amendments 1-10 of the Constitution</em>

Stream 3: Entire conversation (8200 bytes)

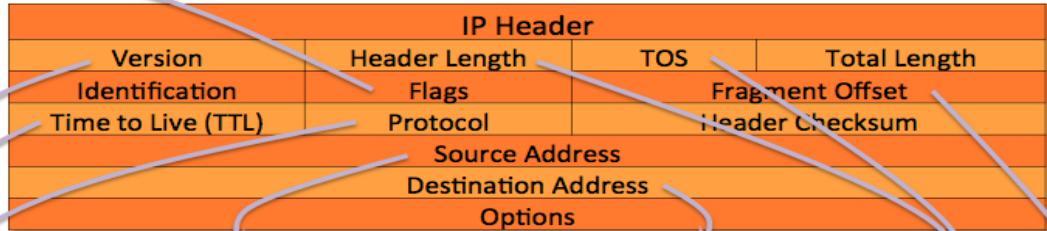
Find

Filter Out This Stream: Print Save as... Back Close Help

Frame (frame), 60 bytes      Packets: 12568 Displayed: 12568 Marked: 0 Dropped: 0      Profile: Default



# Familiarity with packet structures and typical packet flows



Internet Protocol Version 4, Src: 10.100.16.200 (10.100.16.200), Dst: 10.100.185.66 (10.100.185.66)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
0000 00.. = Differentiated Services Codepoint: Default (0x00)  
.... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)

Total Length: 1420

Identification: 0x126d (4717)

Flags: 0x02 (Don't Fragment)  
0... .... = Reserved bit: Not set  
.1.. .... = Don't fragment: Set  
..0. .... = More fragments: Not set

Fragment offset: 0

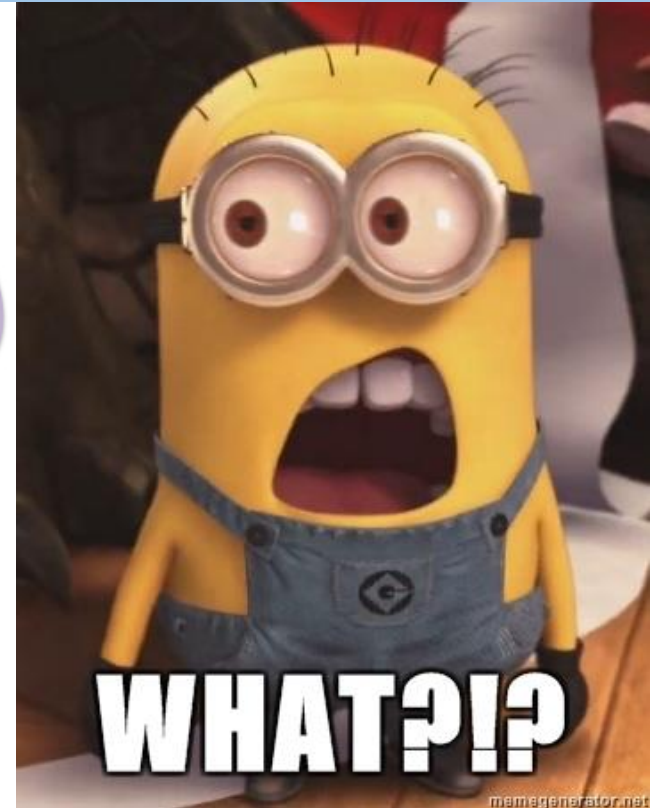
Time to live: 255

Protocol: TCP (6)

Header checksum: 0x98ad [correct]  
[Good: True]  
[Bad: False]

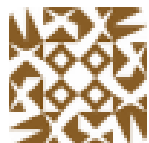
Source: 10.100.16.200 (10.100.16.200)

Destination: 10.100.185.66 (10.100.185.66)





# What Is Your Objective?



**Peter Wu**

@Lekensteyn

This happens way too often:

"help, need to learn wireshark"

"What is your goal?"

"hacking web password like gmail facebook"

...





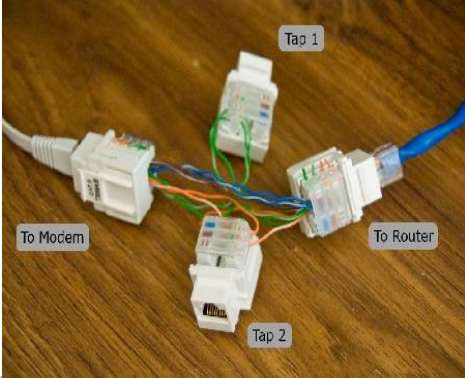
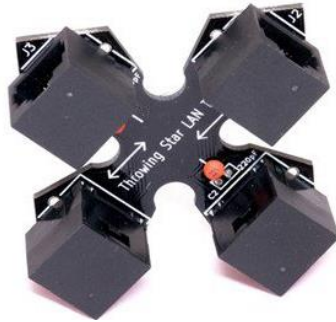


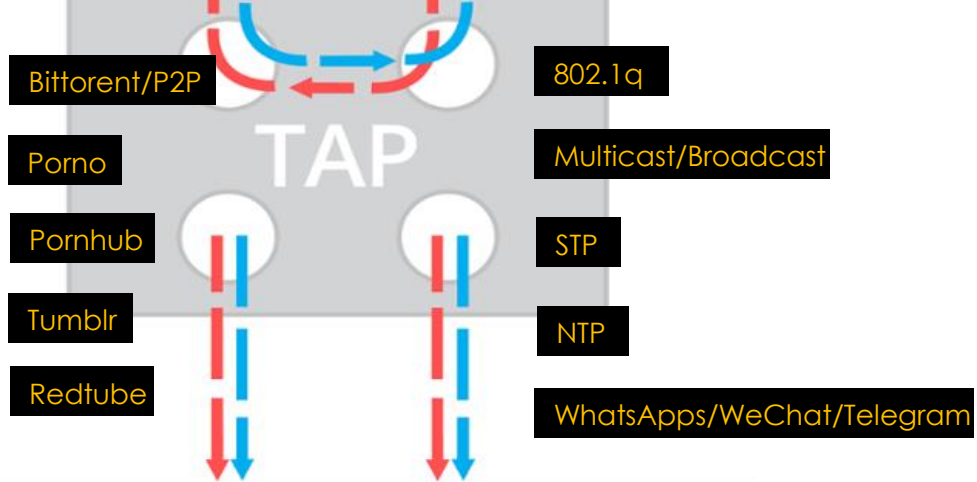
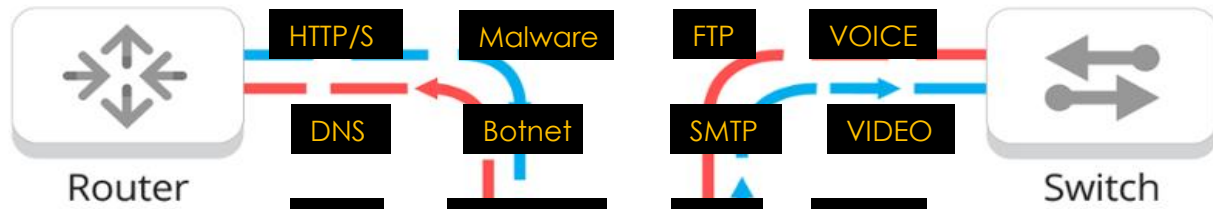
# Know Your Environment





# Intercept The Communication





Users



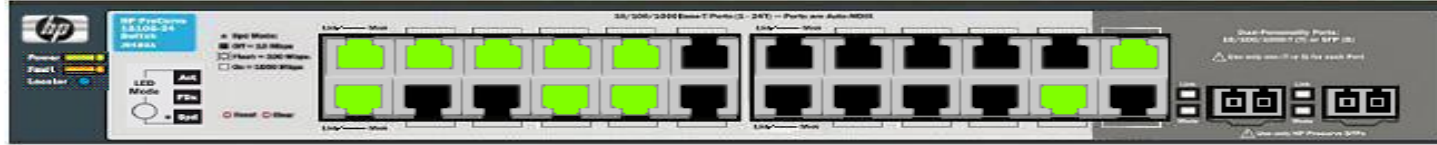
TCPDUMP

SURICATA





# SPAN/Mirroring



## Home

Setup Network

## Status

## Network Setup

## Switching

Port Configuration

Jumbo Frames

Port Mirroring

Flow Control

Green Features

Loop Protection

## Security

## Trunks

## Switching ► Port Mirroring

### Port Mirroring Configuration

Enable Mirroring

Destination Port



24

Source Port	Direction
3	None
4	None
5	None
6	None
7	Tx and Rx
8	None

```
Switch(config)#monitor session 1 source interface gigabitEthernet 1/7 both  
Switch(config)#monitor session 1 destination interface gigabitEthernet 1/24
```



# Don't Just Look at Wireshark??!!!



88804	0.160334	172.20.215.253	224.0.0.2	HSRP	62	Hello (state Standby)
88805	0.011761	172.20.212.179	172.20.2...	NBNS	92	Name query NB PMBIPRCIM03<00>
88806	0.029309	172.20.212.176	172.20.2...	NBNS	92	Name query NB WPAD<00>
88807	0.031753	172.20.214.226	255.255...	UDP	67	49541 → 9273 Len=25
88808	0.085212	423-qbusjdl15.l...	Broadcast	ARP	60	Who has 172.20.215.213? Tell 172.20.214.189
88809	0.047256	NPI27DB87.local	Broadcast	ARP	60	Who has 172.20.215.254? Tell 172.20.214.4
88810	0.031008	172.20.212.179	224.0.0...	LLM...	71	Standard query 0xe843 AAAA PMBIPRCIM03
88811	0.000002	172.20.212.179	224.0.0...	LLM...	71	Standard query 0xd0a5 A PMBIPRCIM03
88812	0.228457	fe80::401c:47d7...	ff02::1:3	LLM...	94	Standard query 0x1bd7 A zeocybskgsipox
88813	0.000158	172.20.212.176	224.0.0...	LLM...	74	Standard query 0x1bd7 A zeocybskgsipox
88814	0.003079	fe80::401c:47d7...	ff02::1:3	LLM...	95	Standard query 0x25b8 A tqfydkveyepackl
88815	0.000130	172.20.212.176	224.0.0...	LLM...	75	Standard query 0x25b8 A tqfydkveyepackl
88816	0.004524	fe80::401c:47d7...	ff02::1:3	LLM...	87	Standard query 0x883c A borgghn
88817	0.000009	172.20.212.176	224.0.0...	LLM...	67	Standard query 0x883c A borgghn



# Listen To Conversation



No.	Source	Destination	Protocol	Length	Info
144226	172.20.212.176	224.0.0.252	LLMNR	64	Standard query 0x1ee9 A wpad
144227	172.20.212.176	172.20.215...	NBNS	92	Name query NB WPAD<00>
144228	Cisco_db:ef:2a	Spanning-t...	STP	60	Conf. Root = 0/0/00:0c:cf:2e:dd:c2 Cost = 6008 Port = 0x802a
144229	172.20.215.252	224.0.0.5	OSPF	98	Hello Packet
144230	fe80::401c:47d7:8a...	ff02::1:3	LLMNR	84	Standard query 0x1ee9 A wpad
144231	172.20.212.176	224.0.0.252	LLMNR	64	Standard query 0x1ee9 A wpad
144232	172.20.212.176	172.20.215...	NBNS	92	Name query NB WPAD<00>
144233	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.215.230? Tell 172.20.215.252
144234	155.69.5.151	172.20.212...	TCP	60	[TCP Keep-Alive] 135 → 62813 [ACK] Seq=1 Ack=1 Win=256 Len=1
144235	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.214.176? Tell 172.20.215.252
144236	172.20.215.252	224.0.0.2	HSRP	62	Hello (state Active)
144237	172.20.214.226	255.255.25...	UDP	67	49541 → 9273 Len=25
144238	Cisco_db:ef:2a	CDP/VTP/DT...	CDP	398	Device ID: NEC-05-E04_STD2.ntu.edu.sg Port ID: FastEthernet0/42
144239	172.20.212.176	172.20.215...	NBNS	92	Name query NB WPAD<00>
144240	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.215.214? Tell 172.20.215.252
144241	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.212.5? Tell 172.20.215.252
144242	155.69.5.151	172.20.212...	TCP	60	[TCP Keep-Alive] 135 → 62813 [ACK] Seq=1 Ack=1 Win=256 Len=1
144243	172.20.214.226	255.255.25...	UDP	67	49541 → 9273 Len=25
144244	Cisco_db:ef:2a	Spanning-t...	STP	60	Conf. Root = 0/0/00:0c:cf:2e:dd:c2 Cost = 6008 Port = 0x802a
144245	155.69.5.177	172.20.214...	TCP	60	135 → 51130 [ACK] Seq=1 Ack=1 Win=256 Len=1
144246	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.212.224? Tell 172.20.215.252
144247	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.215.211? Tell 172.20.215.252
144248	155.69.5.151	172.20.212...	TCP	60	[TCP Keep-Alive] 135 → 62813 [ACK] Seq=1 Ack=1 Win=256 Len=1
144249	172.20.214.226	255.255.25...	UDP	67	49541 → 9273 Len=25





# Baseline Your Environment



nslookup www.maybank2u.com.my

Server:1.1.1.1

Address:1.1.1.1#53

Non-authoritative answer:

www.maybank2u.com.mycanonical name = www.maybank2u.com.my.edgekey.net.

www.maybank2u.com.my.edgekey.netcanonical name = e7160.x.akamaiedge.net.

Name:e7160.x.akamaiedge.net

Address: 184.51.97.173



nslookup www.maybank2u.com.my

Server:155.69.3.9

Address:155.69.3.9#53

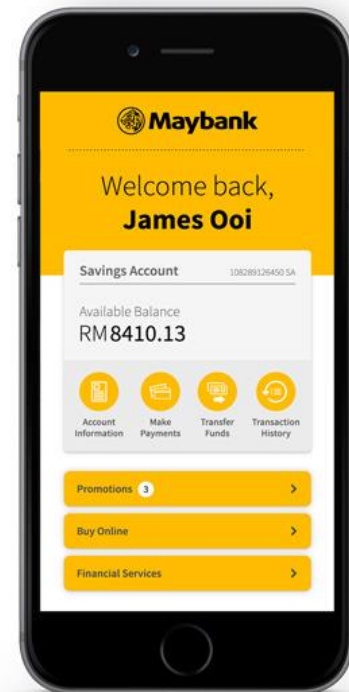
Non-authoritative answer:

www.maybank2u.com.mycanonical name = www.maybank2u.com.my.edgekey.net.

www.maybank2u.com.my.edgekey.netcanonical name = e7160.x.akamaiedge.net.

Name:e7160.x.akamaiedge.net

Address: 23.49.30.121







# The Navigation



**Wireshark** File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

The Wireshark Network Analyzer

Apply a display filter ... <:\*/>

Welcome to Wireshark

**Capture**

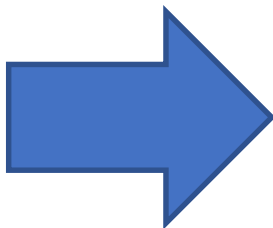
...using this filter:

- utun0
- Thunderbolt 1: en1
- Thunderbolt 2: en2
- iPhone USB: en5
- Thunderbolt Ethernet: en14
- Loopback: lo0
- group10: vlan0
- group20: vlan1
- group30: vlan2
- Wi-Fi: en0
- gif0
- stf0
- p2p0
- awdl0
- Thunderbolt Bridge: bridge0
- XHC20
- Cisco remote capture: cisco
- Random packet generator: randpkt
- SSH remote capture: ssh
- UDP Listener remote capture: udpdump

**Learn**

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395a).



**Wireshark** File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capturing from Thunderbolt Ethernet: en14

Apply a display filter ... <:\*/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Nitgen_01:13:83	Broadcast	ARP	60	Who has 172.20.214.226? Tell 17
2	0.063891	52.35.159.162	172.20.214.12	TCP	66	443 → 60734 [ACK] Seq=1 Ack=1 W
3	0.345625	Cisco_db:ef:2a	Spanning-tree-(for...	STP	60	Conf. Root = 0/0/00:0c:cf:2e:dd
4	0.627925	172.20.214.226	255.255.255.255	UDP	67	49541 → 9273 Len=25
5	1.106394	172.20.212.184	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID
6	1.318030	81.161.59.89	172.20.214.12	TCP	66	80 → 60401 [ACK] Seq=1 Ack=1 Wi
7	1.318139	172.20.214.12	81.161.59.89	TCP	66	[TCP ACKed unseen segment] 6040
8	1.627962	172.20.214.226	255.255.255.255	UDP	67	49541 → 9273 Len=25
9	1.950378	HewlettP_27:db:87	Broadcast	ARP	60	Who has 172.20.215.254? Tell 17
10	1.994644	172.20.215.253	224.0.0.2	HSRP	62	Hello (state Standby)
11	2.345692	Cisco_db:ef:2a	Spanning-tree-(for...	STP	60	Conf. Root = 0/0/00:0c:cf:2e:dd
12	2.432151	162.125.34.129	172.20.214.12	TLSv1...	322	Application Data
13	2.432227	172.20.214.12	162.125.34.129	TCP	66	59807 → 443 [ACK] Seq=1 Ack=257

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▶ Ethernet II, Src: Nitgen\_01:13:83 (00:0b:f6:01:13:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▶ Address Resolution Protocol (request)

```

0000 ff ff ff ff ff ff 00 0b f6 01 13 83 08 06 00 01 .....
0010 08 00 06 04 00 01 00 0b f6 01 13 83 ac 14 d6 be .....
0020 00 00 00 00 00 00 ac 14 d6 e2 00 00 00 00 00 00 .....
0030 00 00 00 00 00 00 00 00 00 00 00 00 .....

```



# Customize Your Views

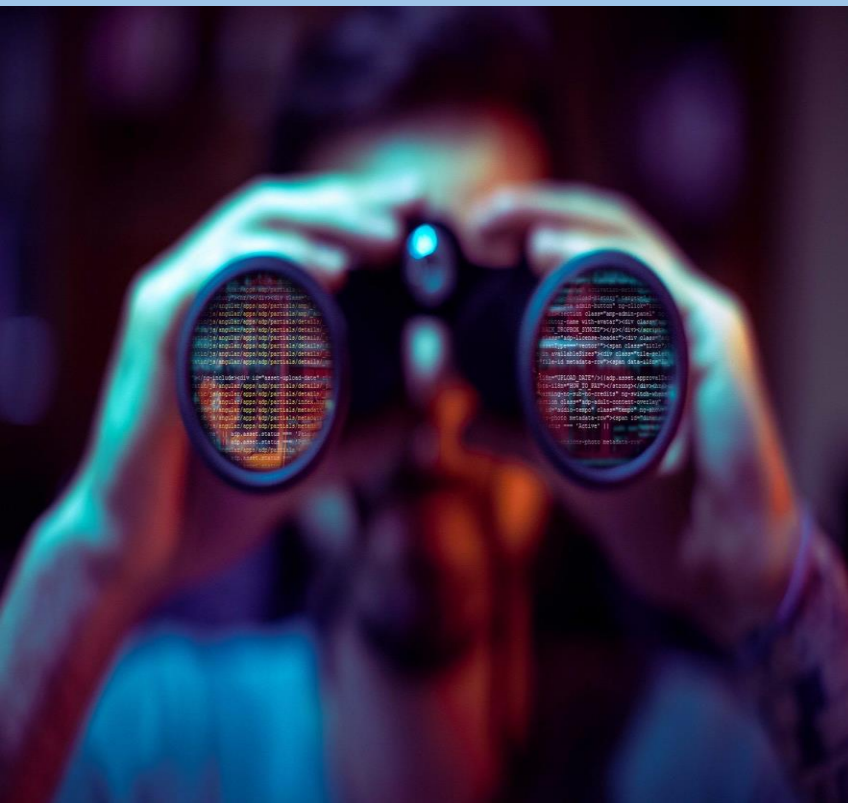


NETWORK | APPLICATION | SECURITY | TROUBLESHOOTING | ETC

MyProfile | MyWiFe | MyDad | MyMom | MyBOSS | IHateThisGuy



# Overview Traffics



Statistics	Telephony	Wireless
Capture File Properties		↗ ↕ ⌂ C
Resolved Addresses		
<b>Protocol Hierarchy</b>		
Conversations		
Endpoints		
Packet Lengths		
I/O Graph		
Service Response Time		▶
DHCP (BOOTP) Statistics		
ONC-RPC Programs		
29West		▶
ANCP		
BACnet		▶
Collectd		
DNS		
Flow Graph		
HART-IP		
HPFEEDS		
HTTP		▶
HTTP2		
Sametime		
TCP Stream Graphs		▶
UDP Multicast Streams		
IPv4 Statistics		▶
IPv6 Statistics		▶

Protocol	Percent Packets
▼ Frame	100.0
▼ Ethernet	100.0
▼ Internet Protocol Version 4	50.4
▼ User Datagram Protocol	37.2
Data	19.7
Cisco Hot Standby Router Protocol	8.3
Simple Network Management Protocol	3.2
NetBIOS Name Service	2.1
Link-local Multicast Name Resolution	1.8
Bootstrap Protocol	0.8
Dropbox LAN sync Discovery Protocol	0.6
▼ NetBIOS Datagram Service	0.6
▶ SMB (Server Message Block Protocol)	0.6
Multicast Domain Name System	0.2
▶ Transmission Control Protocol	7.0
Open Shortest Path First	4.4
Protocol Independent Multicast	1.3
Internet Group Management Protocol	0.3
Host Identity Protocol	0.1
Address Resolution Protocol	22.1
▶ Internet Protocol Version 6	12.2
▶ Logical-Link Control	11.7
▶ Configuration Test Protocol (loopback)	2.0
▶ Internetwork Packet eXchange	1.6
Data	0.1



# The Power Of The Right Click!



No.	Source	Destination	Protocol	Length	Info
25	172.20.214.226	255.255.255.2...	UDP	67	49541 → 9273 Len=25
26	Toshiba_88:c2:76	Broadcast	ARP	60	Who has 172.20.215.230? Tell 172.20.213.220
27	172.20.215.252	224.0.0.2	HSRP	62	Hello (state Active)
28	Cisco_bc:fd:9c	Broadcast	ARP	60	Who has 172.20.214.176? Tell 172.20.215.252
29	Cisco_db:ef:2a	Spanning-tree...	STP	60	Conf. Root = 0/0/00:0c:cf:2e:dd:c2 Cost = 6008 Port = 0x802a
30	hbsu-PC.local	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
31	172.20.214.226	255.255.255.2...	UDP	67	49541 → 9273 Len=25
32	Toshiba_88:c2:76	Broadcast	ARP	60	Who has 172.20.215.230? Tell 172.20.213.220
33	172.20.215.253	224.0.0.2	HSRP	62	Hello (state Standby)
34	172.20.214.226	255.255.255.2...	UDP	67	49541 → 9273 Len=25

Frame 33: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0:00:02

Ethernet II, Src: Cisco\_42:dd:7c (00:0c:cf:42:dd:7c), Dst: Broadcast (ff:ff:ff:ff:ff:ff), Length: 62, Protocol: Internet Protocol Version 4

Internet Protocol Version 4, Src: 172.20.215.253 (172.20.215.253), Dst: 224.0.0.2 (224.0.0.2), Protocol: User Datagram Protocol, Src Port: 1985, Dst Port: 1985

Cisco Hot Standby Router Protocol

Version: 0

Op Code: Hello (0)

State: Standby (8)

Hellotime: Non-Default (5)

Holdtime: Non-Default (15)

Priority: 100

Group: 3

Reserved: 0

Authentication Data: Default (cisco)

Virtual IP Address: 172.20.215.254 (172.20.215.254)

- Expand Subtrees
- Expand All
- Collapse All
- Apply as Column
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Show Packet Bytes...
- Export Packet Bytes... ⌘H
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As...
- Go to Linked Packet
- Show Linked Packet in New Window

```
0000  01 00 5e 00 00 02 00 0c  cf 42 dd 7c 08 00 45 c0  ..^.... .B.|..E.
0010  00 30 00 00 00 02 11  53 e9 ac 14 d7 fd e0 00  .0..... S.....
0020  00 02 07 c1 07 c1 00 1c  a7 d5 00 00 08 05 0f 64  .....d.....
0030  03 00 63 69 73 63 6f 00  00 00 ac 14 d7 fe  ..Cisco. ....
```







# Look For The Sign!



No.	Time	Source	Destination	Protocol	Length	Info
1767	0.558362	172.20.214.12	1.1.1.1	DNS	86	Standard query 0xfa5f A assets.cloud.techsmith.com
1771	0.999979	172.20.214.12	1.1.1.1	DNS	86	Standard query 0xfa5f A assets.cloud.techsmith.com
1780	2.004717	172.20.214.12	1.1.1.1	DNS	86	Standard query 0xfa5f A assets.cloud.techsmith.com
1784	1.213630	172.20.214.12	1.1.1.1	DNS	76	Standard query 0x4e2f A osx.telegram.org
1785	0.078221	172.20.214.12	1.1.1.1	DNS	92	Standard query 0xb7bb A 0-courier.sandbox.push.apple.com
1790	1.004962	172.20.214.12	1.1.1.1	DNS	92	Standard query 0xb7bb A 0-courier.sandbox.push.apple.com
1799	2.004598	172.20.214.12	1.1.1.1	DNS	92	Standard query 0xb7bb A 0-courier.sandbox.push.apple.com
1804	1.403431	172.20.214.12	1.1.1.1	DNS	85	Standard query 0x25fc A nexus.officeapps.live.com
1805	0.000064	172.20.214.12	1.1.1.1	DNS	81	Standard query 0x0325 A config.edge.skype.com
1806	0.000042	172.20.214.12	1.1.1.1	DNS	91	Standard query 0x605a A client-office365-tas.msedge.net
1816	0.483327	172.20.214.12	1.1.1.1	DNS	75	Standard query 0x40fb A www.outlook.com
1830	2.113753	172.20.214.12	1.1.1.1	DNS	92	Standard query 0xb7bb A 0-courier.sandbox.push.apple.com
1843	1.172684	172.20.214.12	1.1.1.1	DNS	84	Standard query 0x10ad A 5-edge-chat.facebook.com
1844	0.000041	172.20.214.12	1.1.1.1	DNS	84	Standard query 0x6866 A 6-edge-chat.facebook.com
1857	1.950417	172.20.214.12	1.1.1.1	DNS	85	Standard query 0xf424 A 23-courier.push.apple.com
1861	1.005220	172.20.214.12	1.1.1.1	DNS	85	Standard query 0xf424 A 23-courier.push.apple.com
1875	2.001699	172.20.214.12	1.1.1.1	DNS	85	Standard query 0xf424 A 23-courier.push.apple.com
1890	1.147561	172.20.214.12	1.1.1.1	DNS	132	Standard query 0x2eb3 PTR d.1.b.a.0.0.7.6.7.2.1.d.9.2.5.6.0.0.0.0.0.0.
1901	0.727052	172.20.214.12	1.1.1.1	DNS	92	Standard query 0xb7bb A 0-courier.sandbox.push.apple.com
1923	2.125736	172.20.214.12	1.1.1.1	DNS	85	Standard query 0xf424 A 23-courier.push.apple.com
1935	1.146600	172.20.214.12	1.1.1.1	DNS	132	Standard query 0x2eb3 PTR d.1.b.a.0.0.7.6.7.2.1.d.9.2.5.6.0.0.0.0.0.0.
1972	5.777781	172.20.214.12	1.1.1.1	DNS	84	Standard query 0xaf42 A 2-edge-chat.facebook.com
1978	1.005271	172.20.214.12	1.1.1.1	DNS	84	Standard query 0xaf42 A 2-edge-chat.facebook.com
1979	0.075314	172.20.214.12	1.1.1.1	DNS	85	Standard query 0xf424 A 23-courier.push.apple.com
1989	1.929310	172.20.214.12	1.1.1.1	DNS	84	Standard query 0xaf42 A 2-edge-chat.facebook.com
1991	0.213171	172.20.214.12	1.1.1.1	DNS	132	Standard query 0x2eb3 PTR d.1.b.a.0.0.7.6.7.2.1.d.9.2.5.6.0.0.0.0.0.0.0.0.
2017	2.711211	172.20.214.12	1.1.1.1	DNS	93	Standard query 0x79ad A 10-courier.sandbox.push.apple.com
2021	1.001116	172.20.214.12	1.1.1.1	DNS	93	Standard query 0x79ad A 10-courier.sandbox.push.apple.com
2022	0.079133	172.20.214.12	1.1.1.1	DNS	84	Standard query 0xaf42 A 2-edge-chat.facebook.com
2033	1.921191	172.20.214.12	1.1.1.1	DNS	93	Standard query 0x79ad A 10-courier.sandbox.push.apple.com





# Spot with Color!



Name	Filter
<input type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
<input type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input type="checkbox"/> OSPF State Change	ospf.msg != 1
<input type="checkbox"/> ICMP errors	icmp.type eq 3    icmp.type eq 4    icmp.type eq 5    icmp.type eq 11    icmpv6.type eq 1
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp    icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf)    (ip.dst == 224.0.0.0/24 && ip.ds
<input type="checkbox"/> Checksum Errors	eth.fcs.status=="Bad"    ip.checksum.status=="Bad"    tcp.checksum.status=="Bad"    ud
<input checked="" type="checkbox"/> SMB	smb    nbss    nbns    nbipx    ipxsap    netbios
<input checked="" type="checkbox"/> HTTP	http    tcp.port == 80    http2
<input checked="" type="checkbox"/> IPX	ipx    spx
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp    eigrp    ospf    bgp    cdp    vrrp    carp    gvrp    igmp    ismp
<input type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02    tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1

Double click to edit. Drag to move. Rules are processed in order until a match is found.

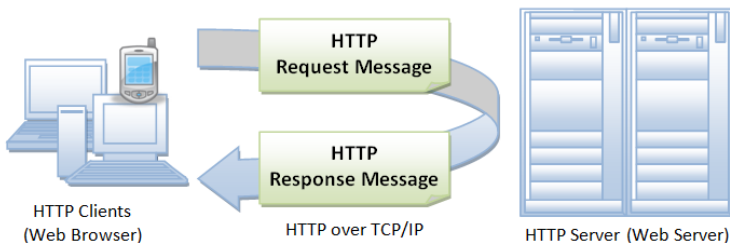
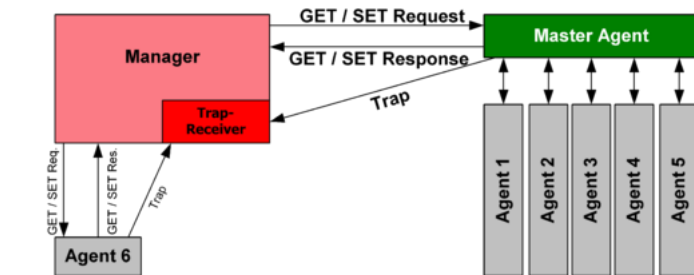
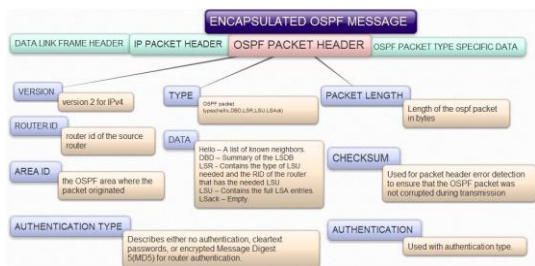
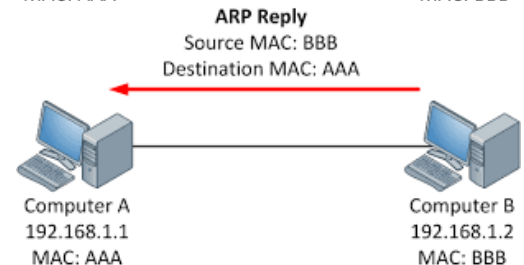
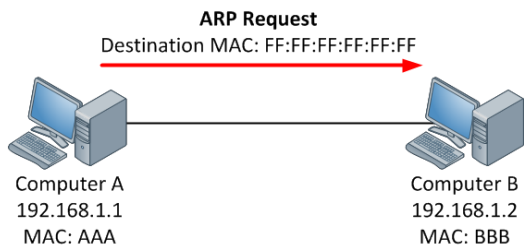
+ - [Refresh]

Help Import... Export... Cancel OK

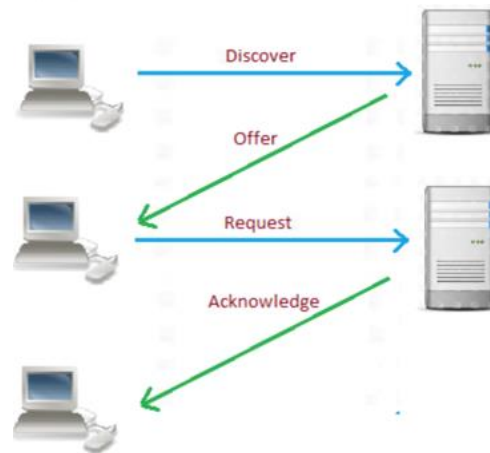
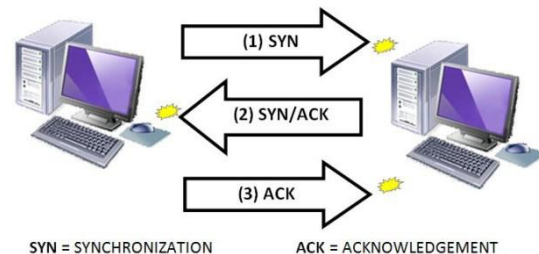




# Protocol Behaviors



## THREE-WAY HANDSHAKE (TCP)







# Why Curiosity is Important



1. Keep an open mind
2. Don't take things as granted
3. Ask questions relentlessly
4. Don't label something as boring
5. See learning as something fun
6. Read diverse kinds of reading

\*lifehacks.org





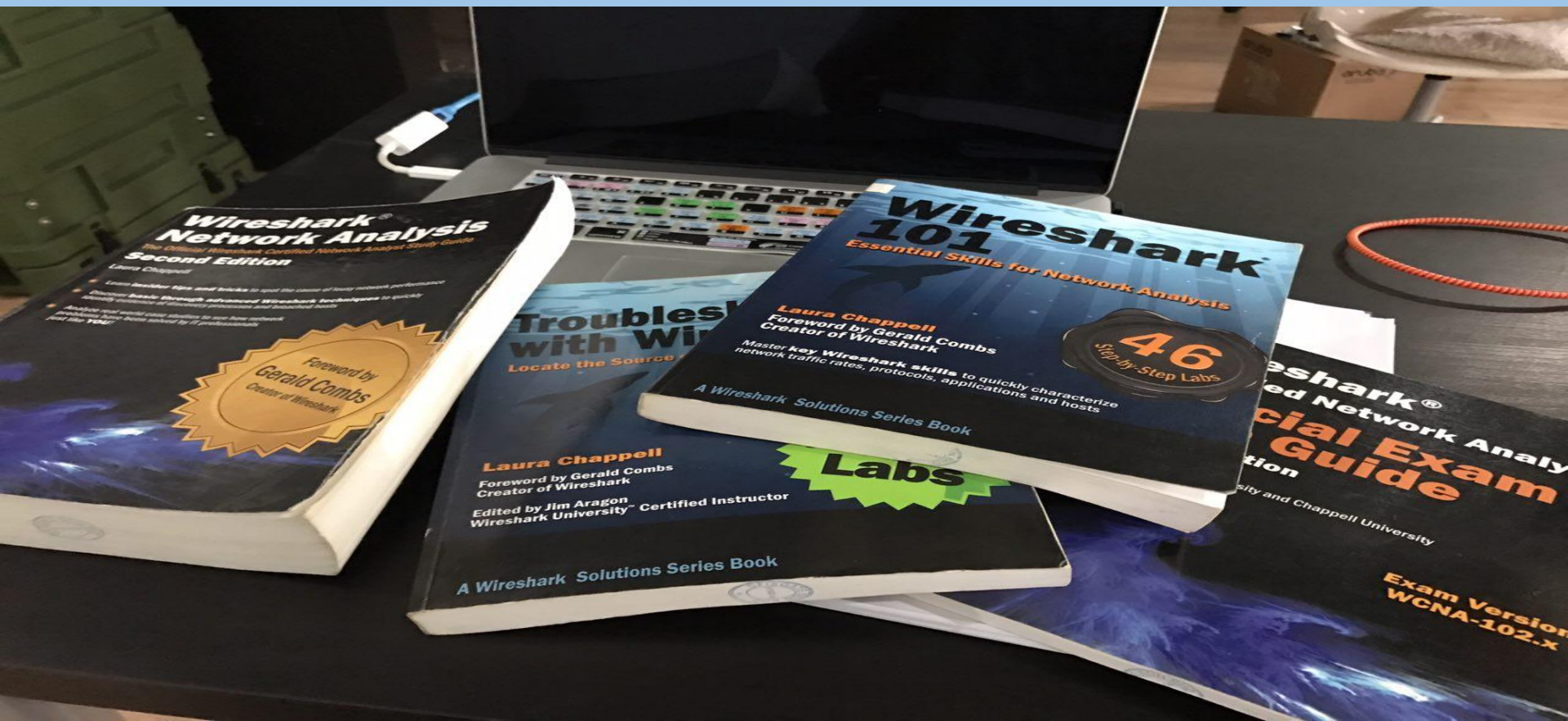


# When there is Ethernet Port – there must be Packets





# Buy All Books From Laura!







# Buy All Books About Wireshark!



Community Experience Distilled

## Mastering Wireshark

Analyze data network like a professional by mastering Wireshark - From 0 to 137

Charit Mishra

**PACKT** open source\*

Community Experience Distilled

## Packet Analysis with Wireshark

Leverage the power of Wireshark to troubleshoot your networking issues by using effective packet analysis techniques and performing an improved protocol analysis

Anish Nath

**PACKT** open source\*

Community Experience Distilled

## Wireshark Essentials

Get up and running with Wireshark to analyze network packets and protocols effectively

James H. Baxter

**PACKT** open source\*

Community Experience Distilled

## Wireshark Network Security

A succinct guide to securely administer your network using Wireshark

Piyush Verma

**PACKT** open source\*

Copyrighted Material

## Wireshark® Network Analysis

The Official Wireshark Certified Network Analyst Study Guide  
Second Edition

Laura Chappell

- Learn **insider tips and tricks** to spot the cause of lousy network performance
- Discover **basics through advanced Wireshark techniques** to quickly identify evidence of discovery processes and breached hosts
- Analyze **real world case studies** to see how network problems have been solved by IT professionals and the YD!

Foreword by Gerald Combs  
Creator of Wireshark

Copyrighted Material

Copyrighted Material

## Troubleshooting with Wireshark®

Locate the Source of Performance Problems

Laura Chappell

Foreword by Gerald Combs  
Creator of Wireshark

Edited by Jim Aragon  
Wireshark University - Certified Instructor

Learn fast with **Hands-On Labs**

A Wireshark Solutions Series Book  
Copyrighted Material

2ND EDITION

## PRACTICAL PACKET ANALYSIS

USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS

CHRIS SANDERS

Over 80 recipes to analyze and troubleshoot network problems using Wireshark

Copyrighted Material

Quick answers to common problems

## Network Analysis Using Wireshark Cookbook

Over 80 recipes to analyze and troubleshoot network problems using Wireshark

Yoram Orzach

**PACKT** open source\*

Copyrighted Material

## Wireshark® 101

Essential Skills for Network Analysis

46 Step-by-Step Labs

Laura Chappell  
Foreword by Gerald Combs  
Creator of Wireshark

Master **key Wireshark skills** to quickly characterize network traffic rates, protocols, applications and hosts

A Wireshark Solutions Series Book  
Copyrighted Material

mitp

Laura Chappell  
Deutsche Ausgabe

## Wireshark® 101

Einführung in die Protokollanalyse

Copyrighted Material

## Wireshark Starter

A quick and easy guide to getting started with network analysis using Wireshark

Ahnav Singh

**PACKT** Publishing

SYNGRESS

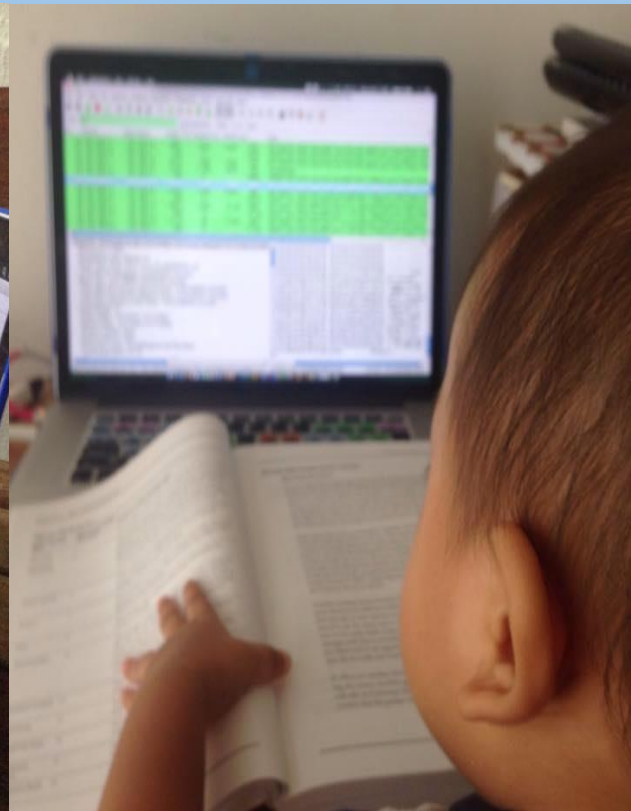
## The Wireshark Field Guide

Analyzing and Troubleshooting Network Traffic

Robert Shimonski



# It's never too late. Start now!







# See Ya In SharkFest'18 US



**SharkFest'18 US**  
June 25 - 28 • Computer History Museum

[About](#) [Agenda](#) [Registration](#) [Lodging](#) [Shuttle](#) [Sponsors](#) [Retrospective](#)



## SharkFest Conference Daily Schedule

Full Agenda with Bios & Abstracts

Day 01  
6.23.2018

Day 02  
6.24.2018

Day 03  
6.25.2018

Day 04  
6.26.2018

Day 05  
6.27.2018

Day 06  
6.28.2018



# Thank you & Enjoy Packet Analysis




Singtel 11:30 PM 100%

< 04: Wireshark Saves the Day! A Be... 11:15 AM-12:30 PM

doing packet analysis with Wireshark so that when your network or application is not performing as expected, you'll feel confident in firing up Wireshark and looking for an answer! This Hands-On Lab will guide the Wireshark beginner through the Wireshark UI and explore basic features and functionality like the navigation button, capture filters, display filters, column configuration, and how to create a shortcut button to make your packet analysis exercises easy. You'll learn to identify the correct fields in packet contents and look for clues to quickly and accurately diagnose networking issues.

SPEAKERS

 **Maher Adib**  
Principal Consultant, Ofisgate Sdn Bhd >

FORMS

**SharkFest'18 Asia Feedback** >  
Fill out this form to leave your feedback for SharkF...

Added to my schedule Remove >

