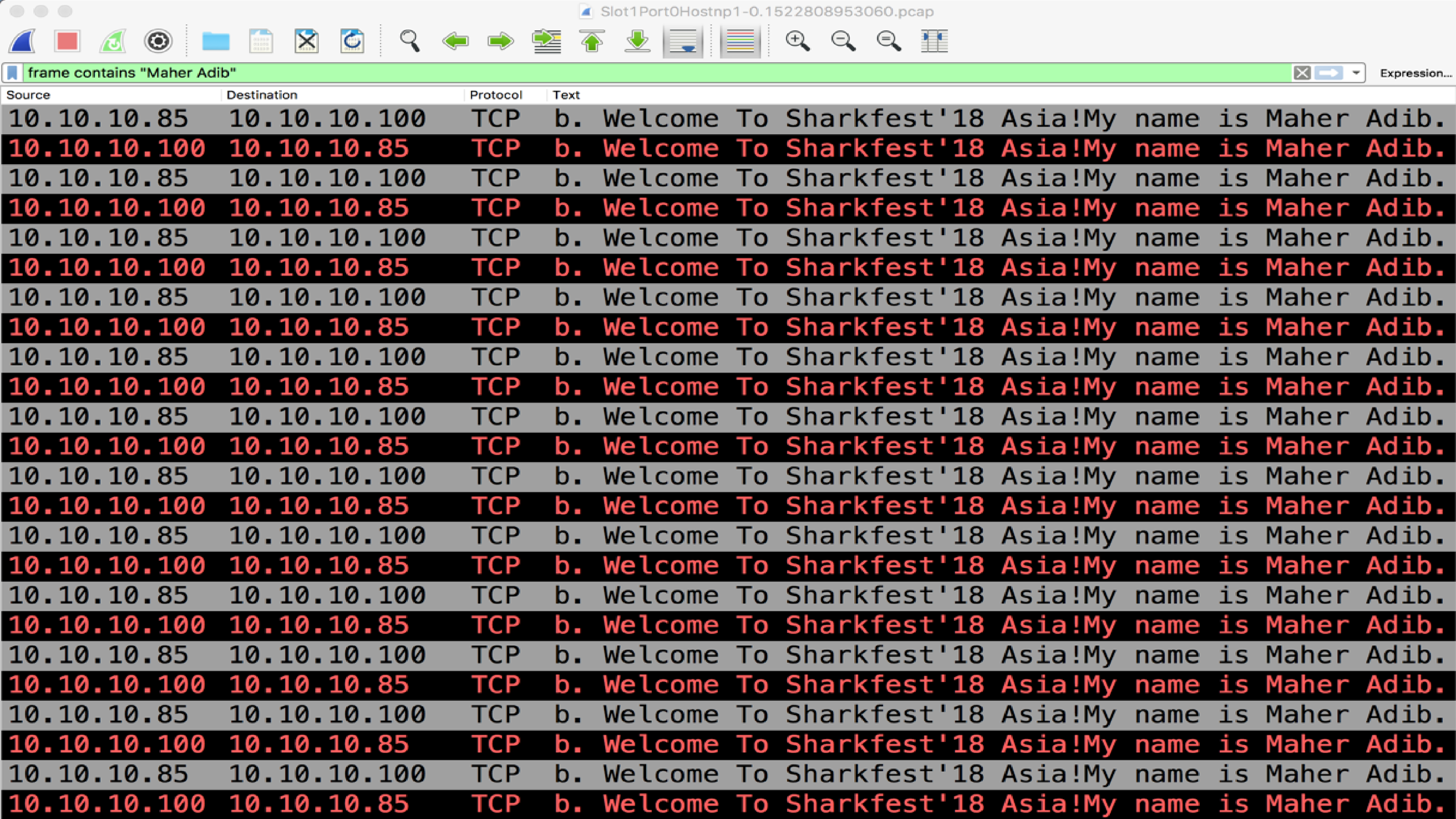
SharkFest ’18 ASIA

Wireshark Saves the Day!

A Beginner’s Guide to Packet Analysis

#sf18asia • NEC, Nanyang Technological University, Singapore • April 9-11



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.
```

Those Were The Days

WIRESHARK Get Acquainted Get Help Develop

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.

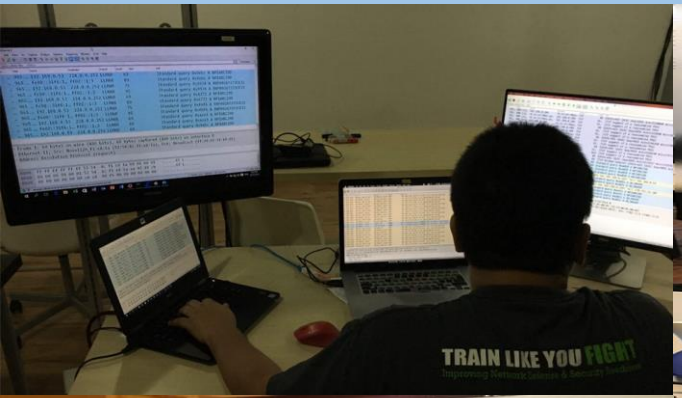
Date Index | Thread Index | Other Months | All Mailing Lists
Date Prev | Date Next | Thread Prev | Thread Next

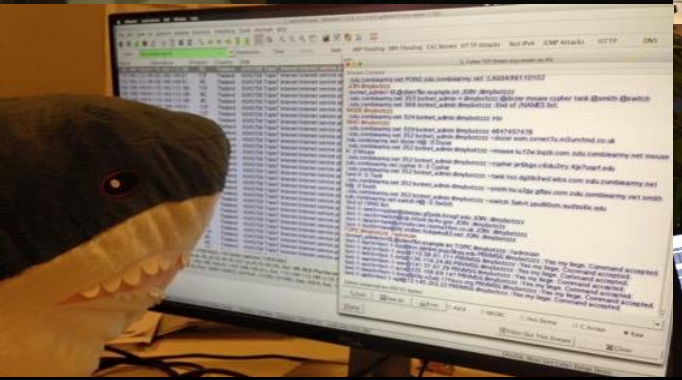
From: maher abedib <m2600@xxxxxxxxxxxx>
Date: Sun, 19 Nov 2000 07:21:36 +0800

```
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 procotol
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
```

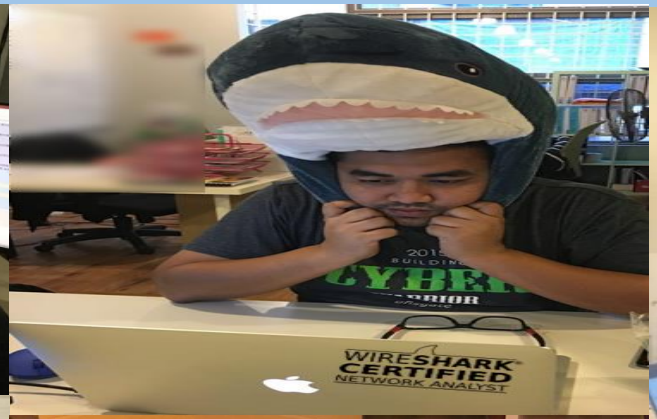
ETHEREAL
PACKET SNIFFER

Not an easy job!

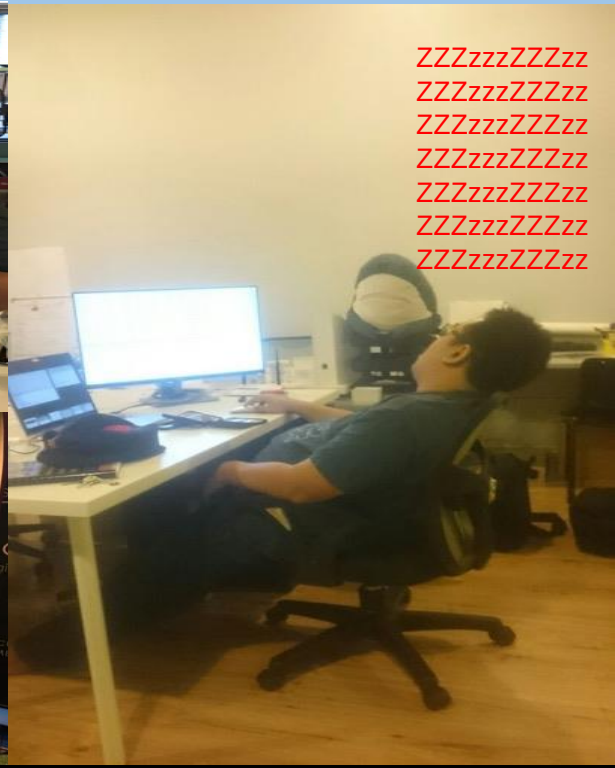




What My Company Think What I'm Doing



What My Customer see Everyday



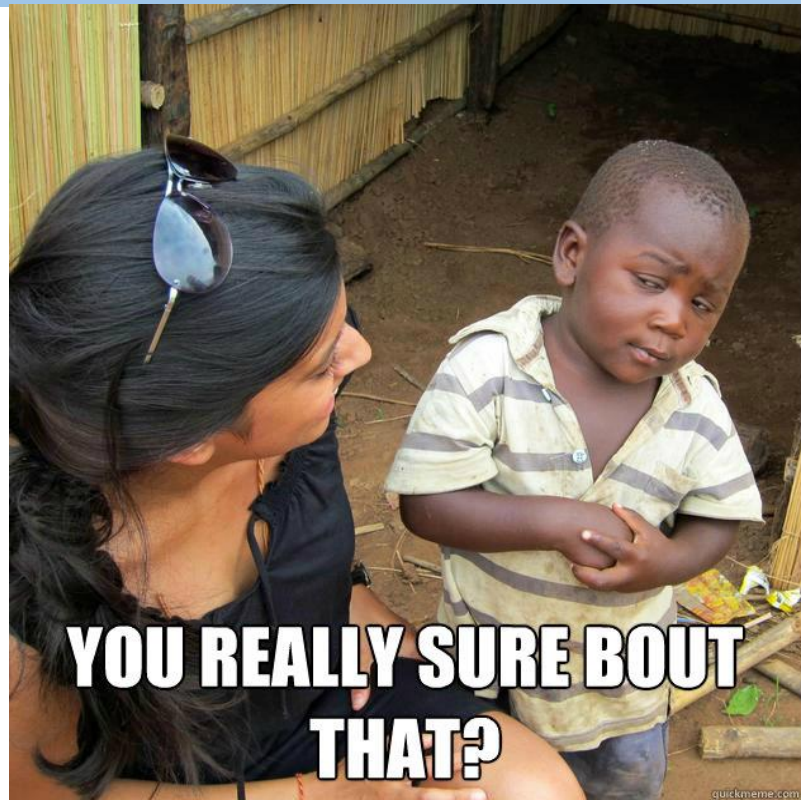
This is what I Do Everyday!

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:

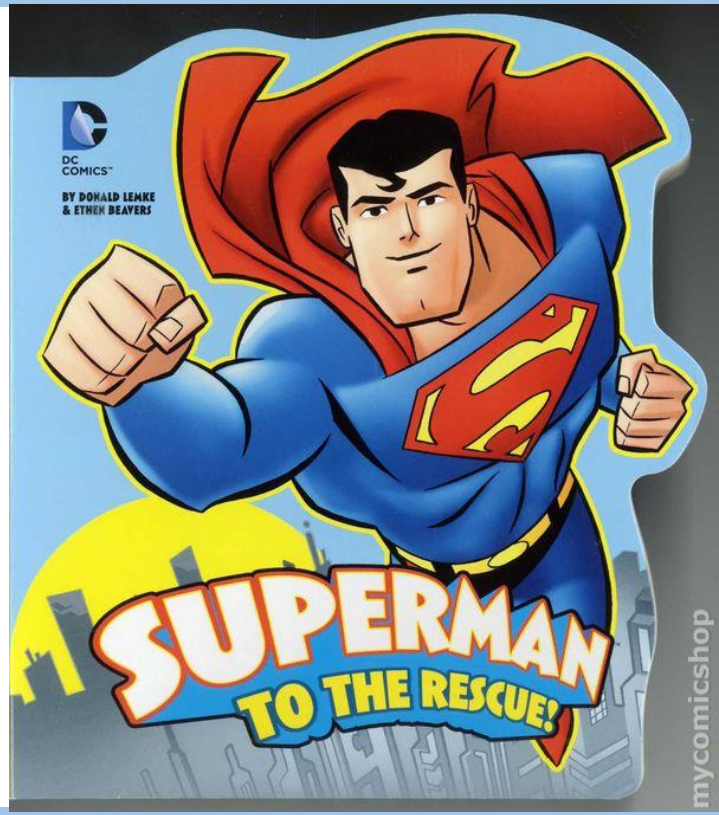
- Protocols
- Port and Protocol numbers
- Header types
- Addresses
- Payloads
- and more, more and more… Thanks Core Dev!



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.



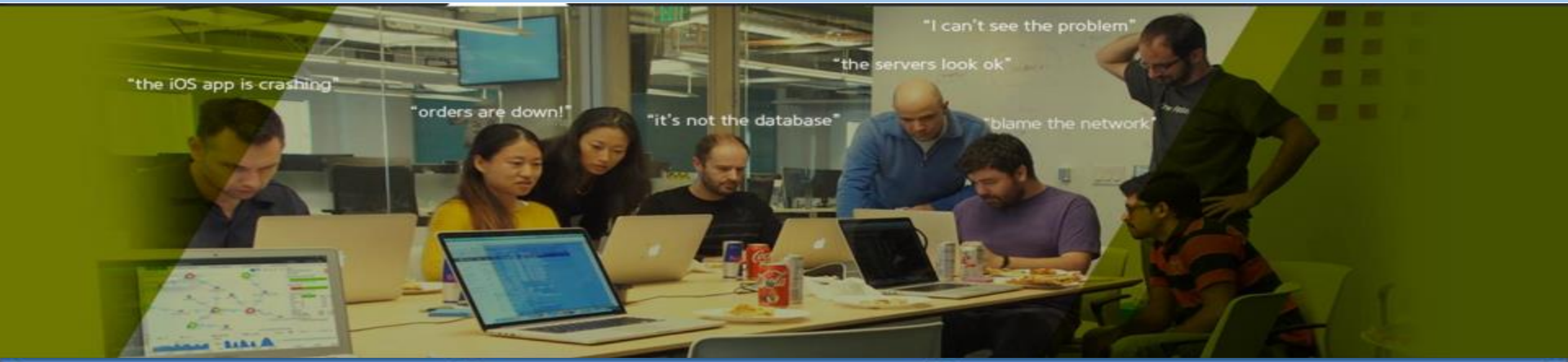
Enjoy The Moments...

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.

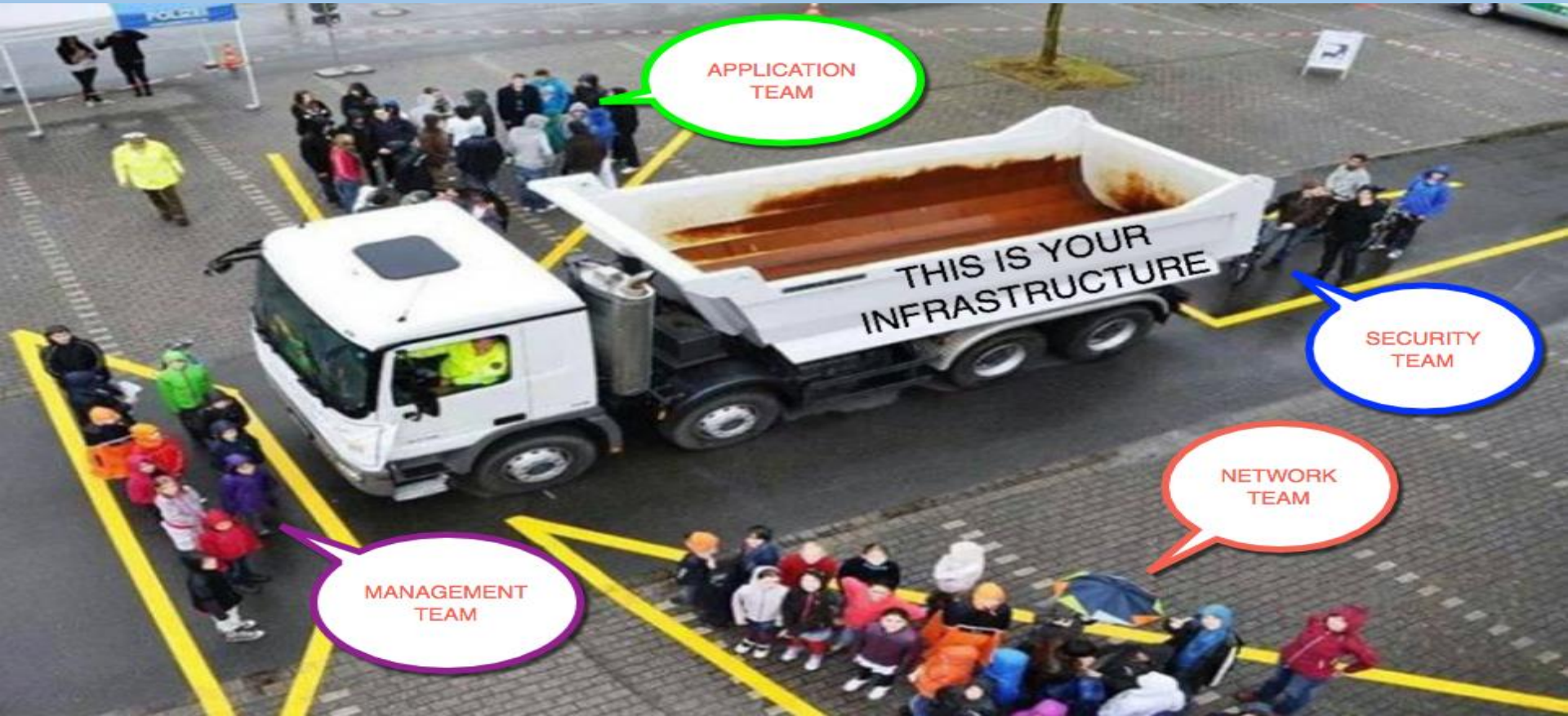
Most IT folks still get a thrill out of using Wireshark (and the insight it provides) even after many years of experience in the field.

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

Sound Familiar?



Different Views



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 confortable 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

WIRESHARK

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 analzyer (Wireshark)**
- **Familiarity with packet structures and typical packet flows**

TCP/IP Communication

Application

Presentation

Session

Transport

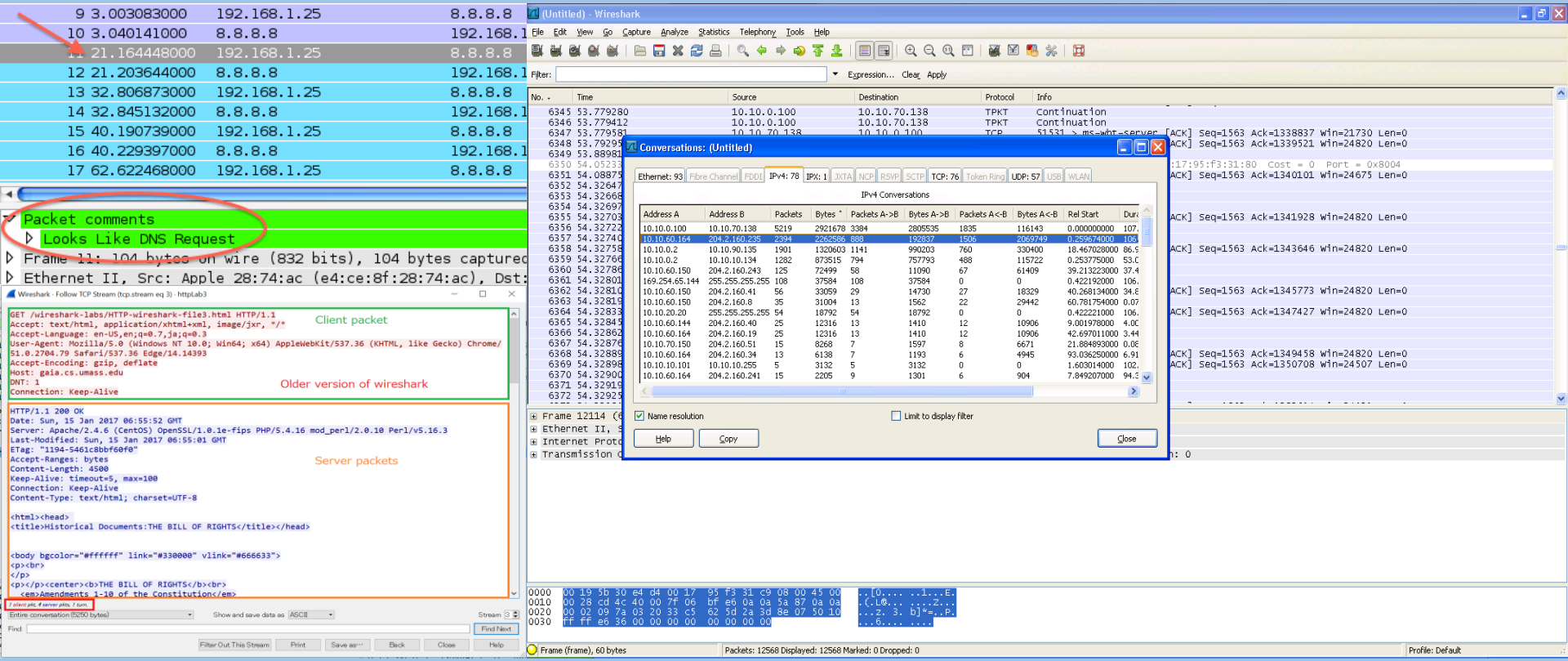
Network

Data Link

Physical

```
▸ Frame 168210: 417 bytes on wire (3336 bits), 417 byte
▸ Ethernet II, Src: Apple_cb:39:45 (68:5b:35:cb:39:45),
▸ Internet Protocol Version 4, Src: 192.168.0.42, Dst:
▸ Transmission Control Protocol, Src Port: 62931, Dst P
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: www.ofisgateacademy.com\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 1
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.ofisgateacademy.com/]
    [HTTP request 1/1]
    [Response in frame: 168228]
```

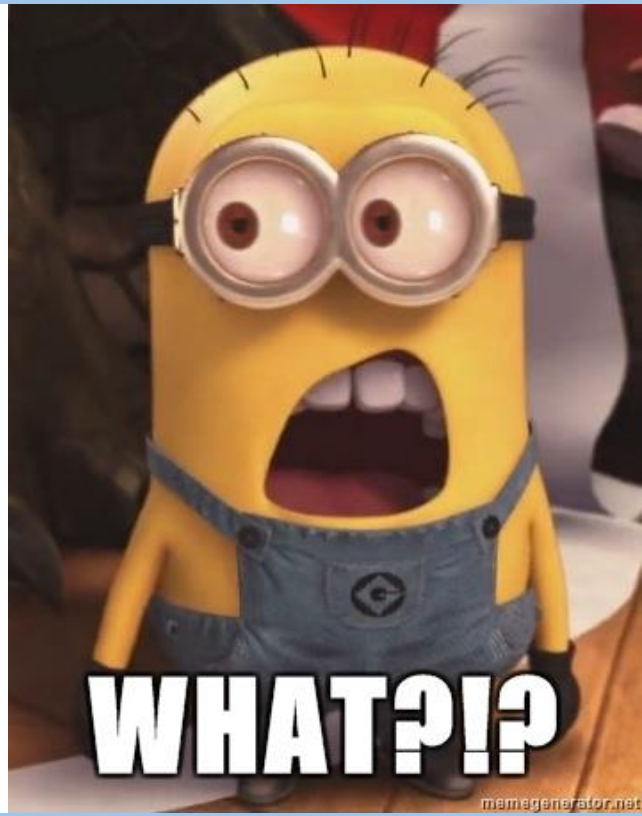
Comfort using any network analzyer (Wireshark)



Familiarity with packet structures and typical packet flows

IP Header			
Version	Header Length	TOS	Total Length
Identification	Flags	Fragment Offset	
Time to Live (TTL)	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			

```
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)
```



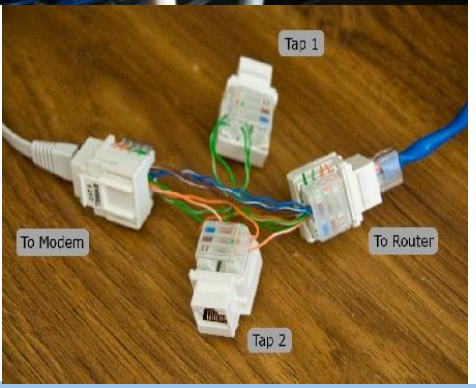
What Is Your Objective?

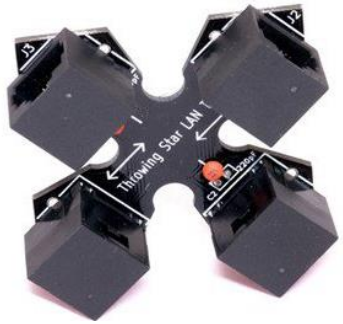
Peter Wu
@Lekensteyn

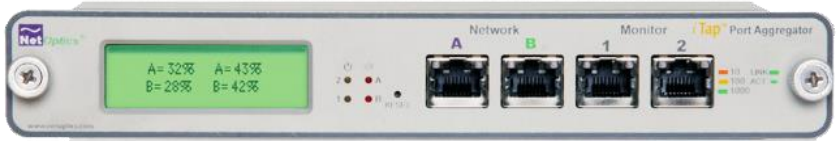
This happens way too often:
"help, need to learn wireshark"
"What is your goal?"
"hacking web password like gmail facebook"
...

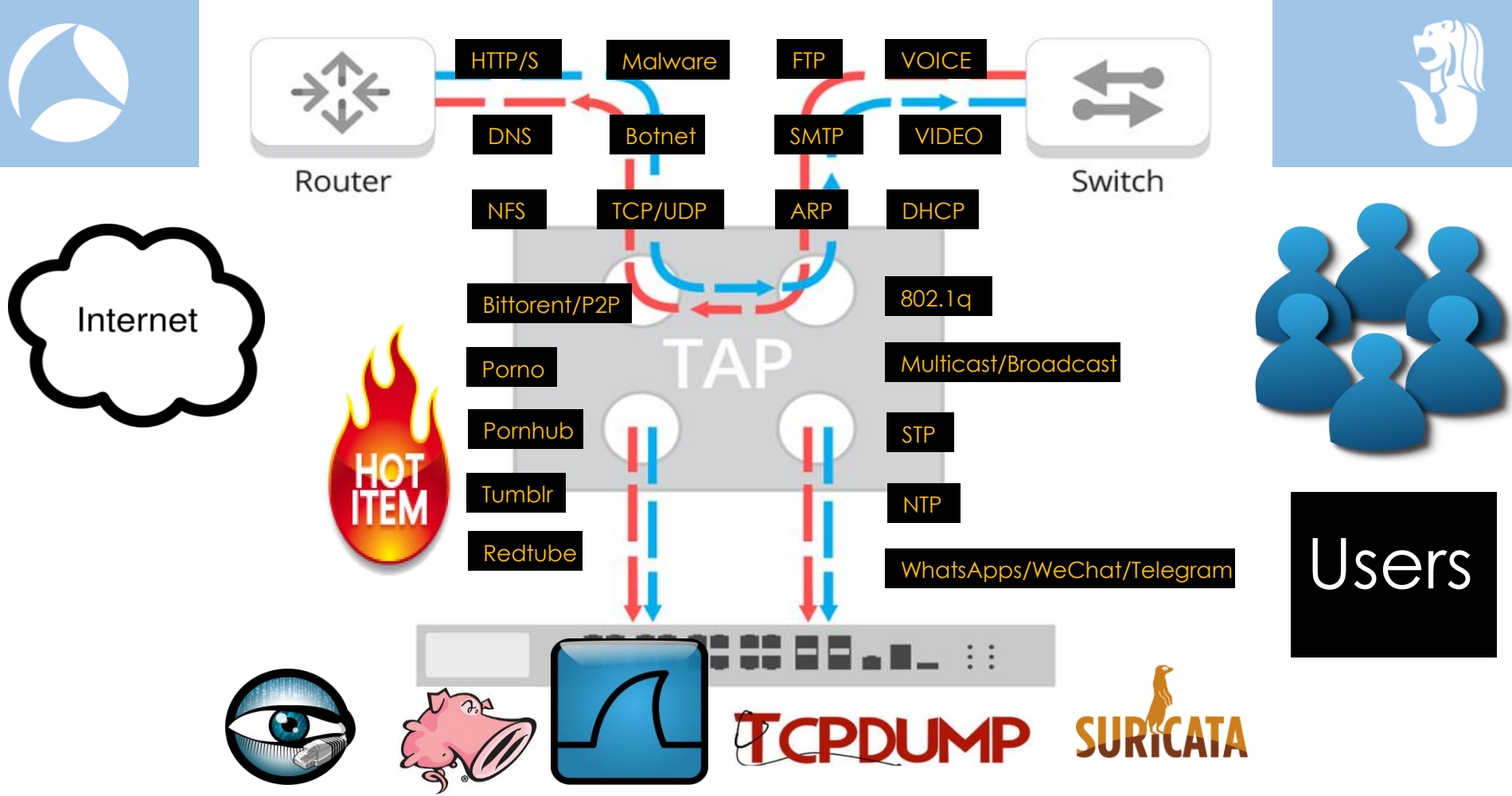
Know Your Enviroment

Intercept The Communication








Router
Switch
HTTP/S
Malware
FTP
VOICE
DNS
Botnet
SMTP
VIDEO
NFS
TCP/UDP
ARP
DHCP
Internet
TAP
Bittorent/P2P
802.1q
Porno
Multicast/Broadcast
Pornhub
STP
Tumblr
NTP
Redtube
WhatsApps/WeChat/Telegram
HOT ITEM
Users
TCPDUMP
SURICATA

SPAN/Mirroring

ProCurve Networking

- Home
  - Setup Network
- ▶ Status
- ▶ Network Setup
- ▼ Switching
  - Port Configuration
  - Jumbo Frames
  - Port Mirroring
  - Flow Control
  - Green Features
  - Loop Protection
- ▶ Security
- ▶ Trunks

Switching ► Port Mirroring

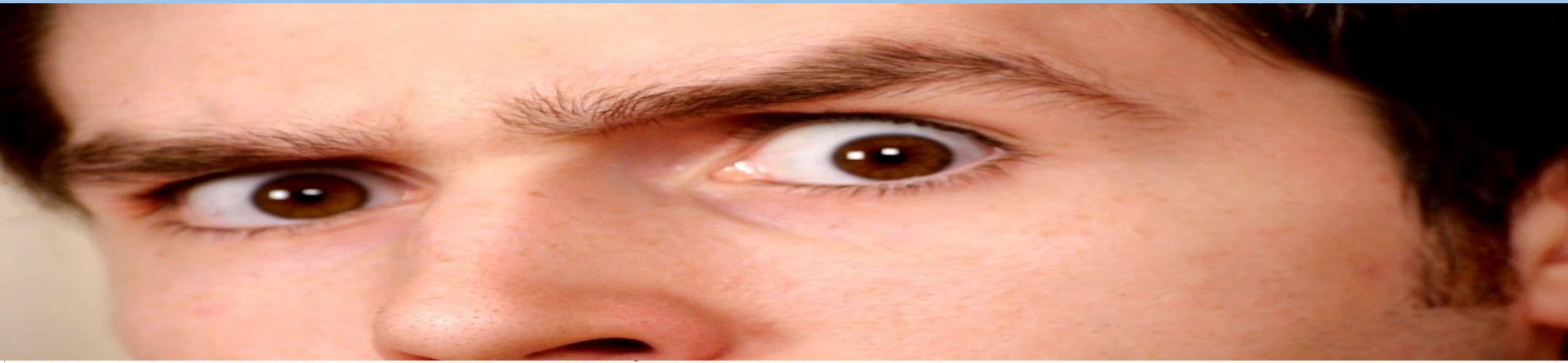
Port Mirroring Configuration

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 Enviroment

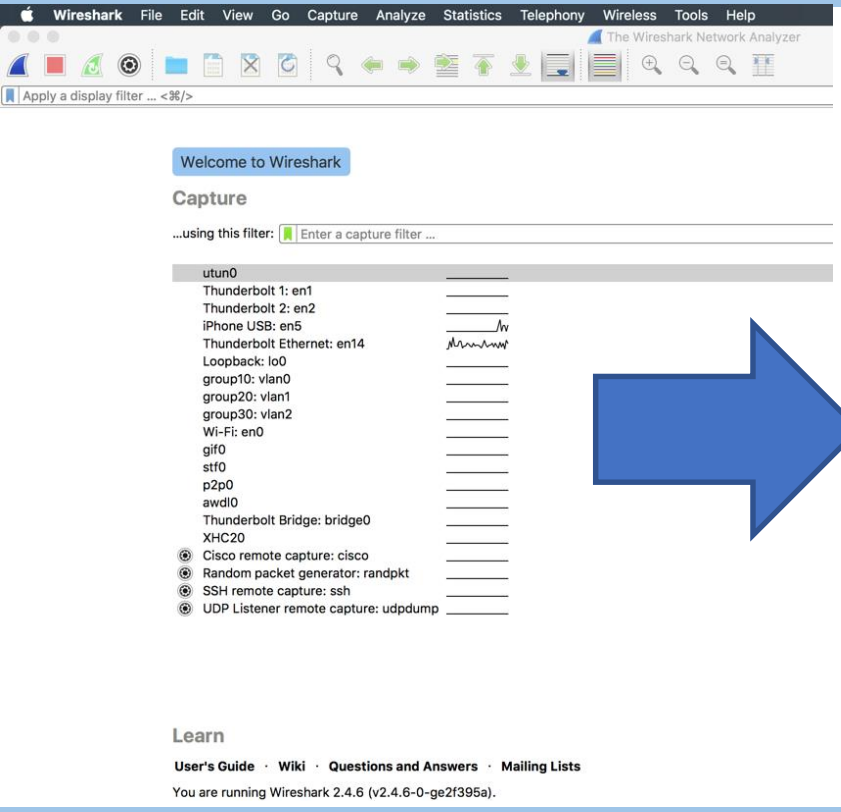
nslookup www.maybank2u.com.my
Server:1.1.1.1
Address:1.1.1.1#53

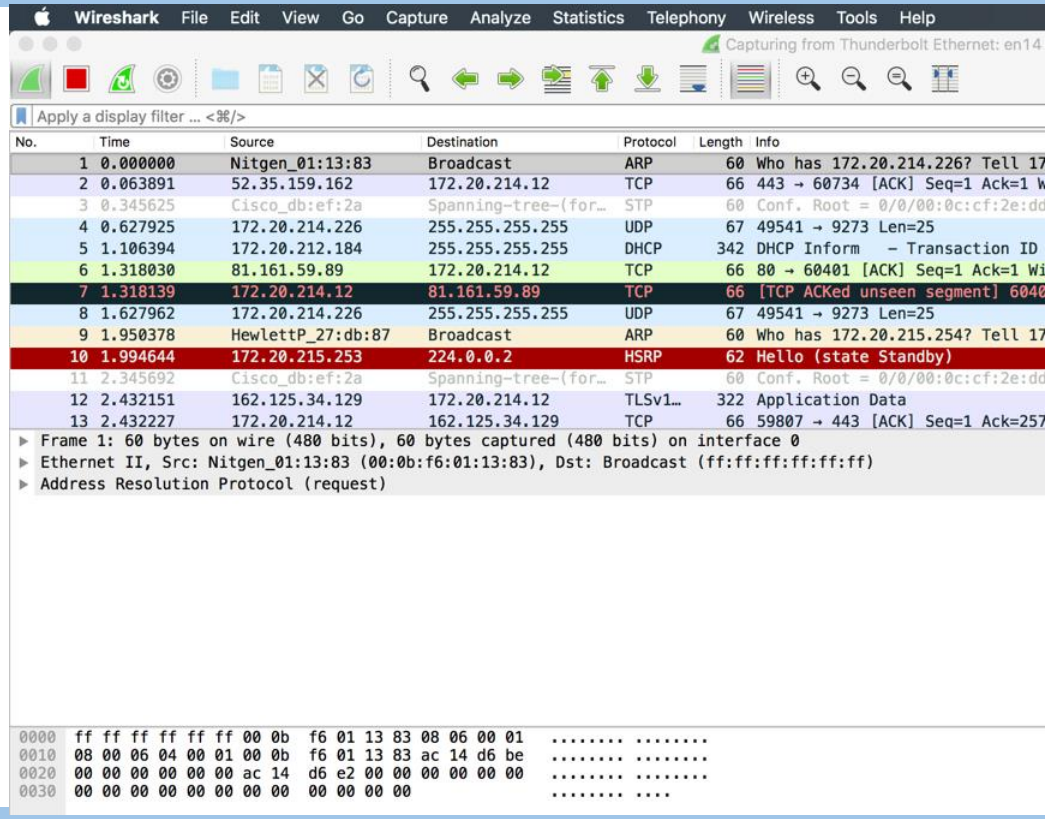
Non-authoritative answer:
www.maybank2u.com.mycanonical name = www.maybank2u.com.my.edgekey.net.
www.maybank2u.com.my.edgekey.netcanonical name = e7160.x.akamaiedge.net.
Name:e7160.x.akamaiedge.net
Address: 184.51.97.173

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



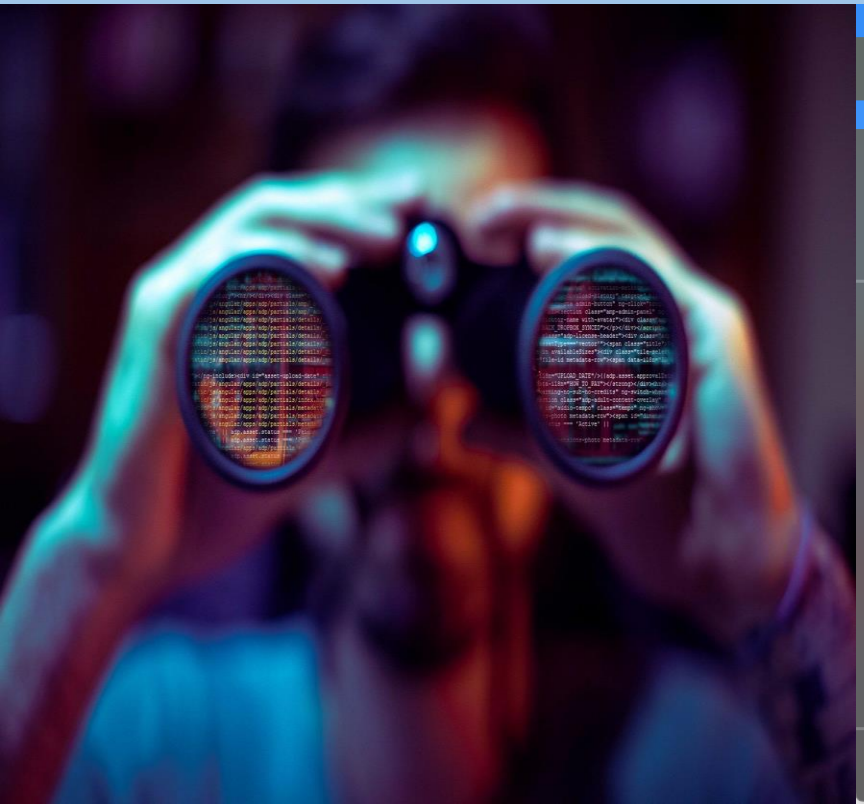


Customize Your Views

NETWORK | APPLICATION | SECURITY | TROUBLESHOOTING | ETC

MyProfile | MyWiFe | MyDad | MyMom | MyBOSS | IHateThisGuy

Overview Traffics



Statistics | Telephony | Wireless

- Capture File Properties ⌥⇧⌘C
- Resolved Addresses
- Protocol Hierarchy
- 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 capt
▶ Ethernet II, Src: Cisco_42:dd:7c (00:0c:cf:42:dd:7c)                    :00:02)
▶ Internet Protocol Version 4, Src: 172.20.215.253 (17                    mcast.net (224.0.0.2)
▶ User Datagram Protocol, Src Port: 1985, Dst Port: 19
▼ 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 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.9.2.5.6.0.0.0.0.0.0.0.0.0.
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!

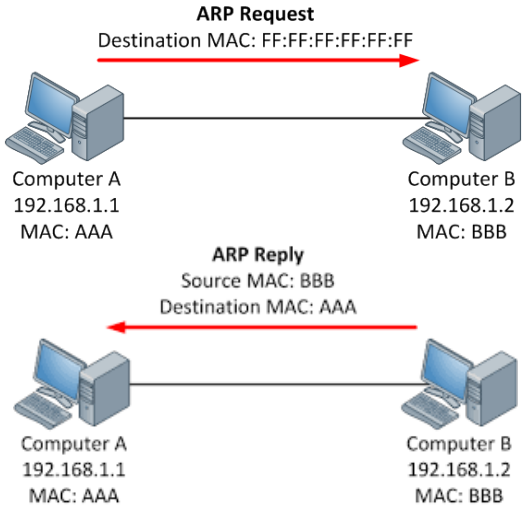
Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq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

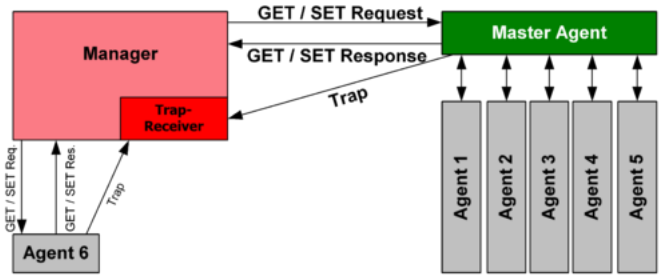
Double click to edit. Drag to move. Rules are processed in order until a match is found.

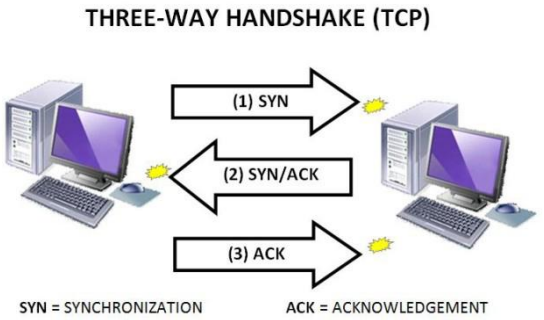
+ −

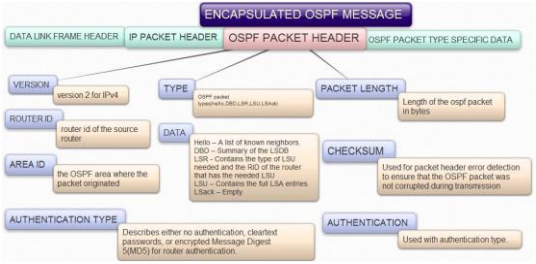
Help Import... Export... Cancel OK

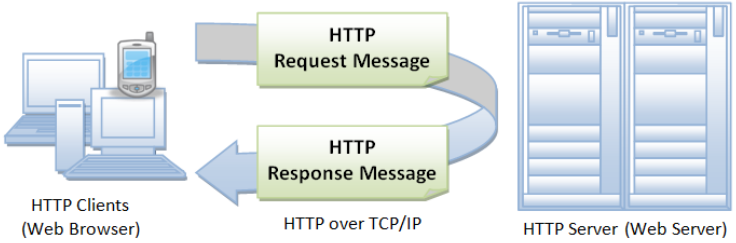
Protocol Behaviors











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

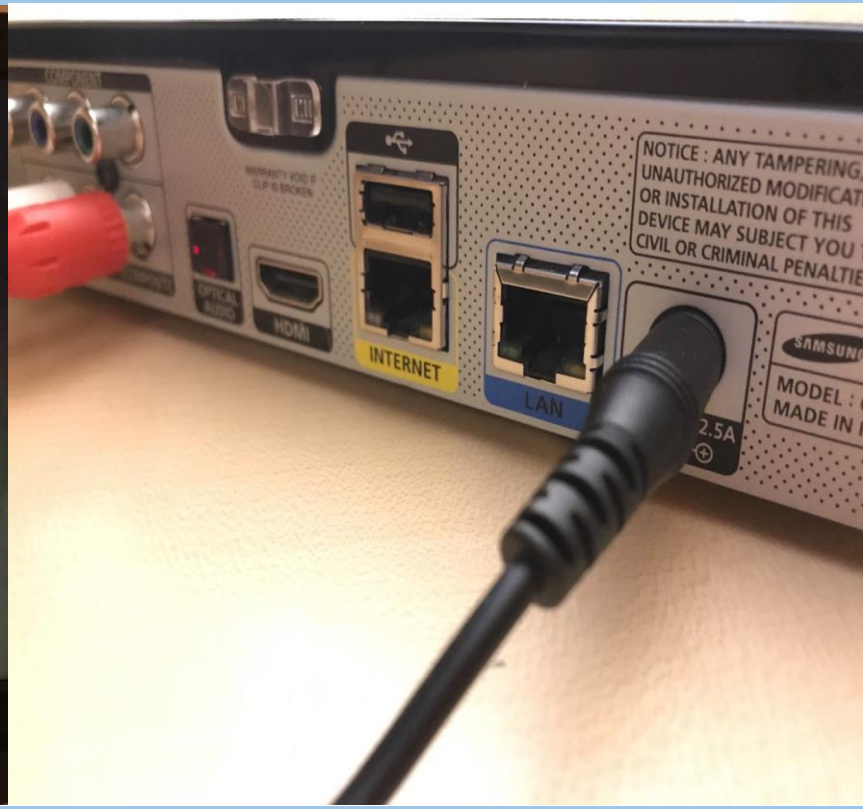
StarHub

STB INFORMATION

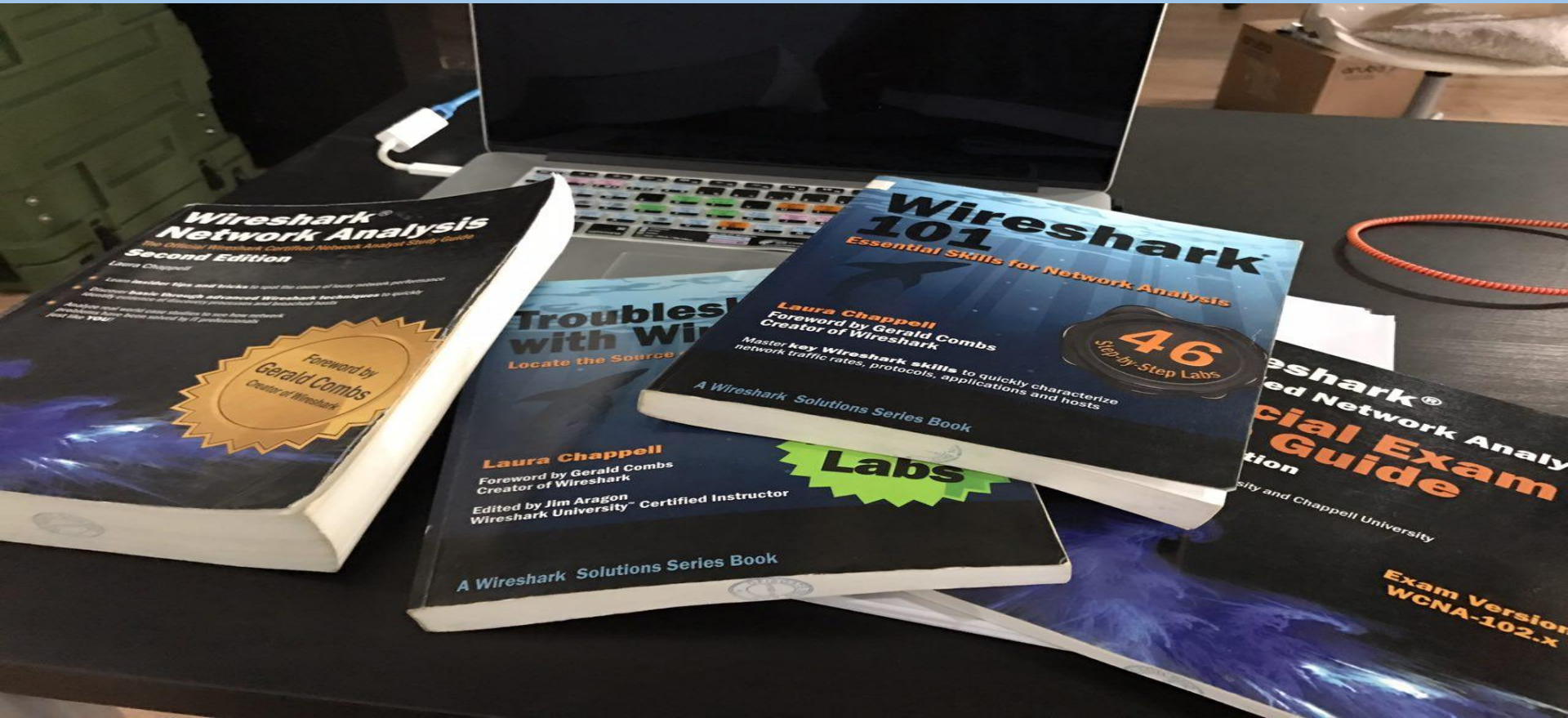
DECODER INFO >

STB Model	:	Samsung GX-SH530CF
Firmware Version	:	OTV5.1.2_BLD18.42e_080317_V2_0
CM Firmware	:	S-SH530CFDEAG-0122
UI Version	:	1.8.49Pr1
Bootloader Version	:	8.0.9.5.4
MAC Address	:	20:D5:BF:D7:1F:B7
IP Address	:	10.27.30.167
Gateway	:	10.27.0.1

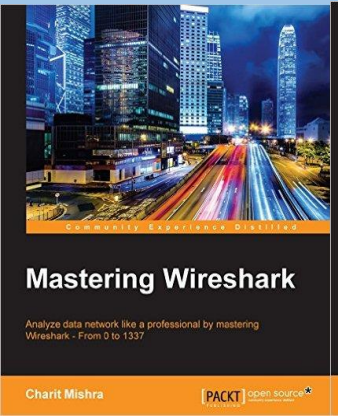
TOSHIBA

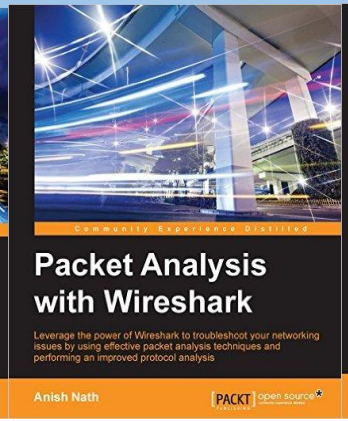


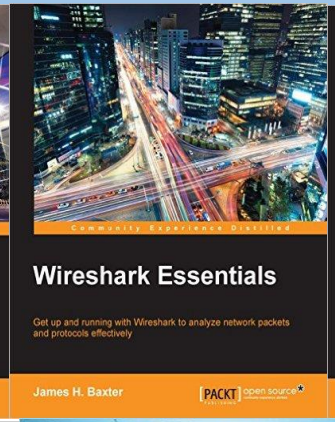
Buy All Books From Laura!

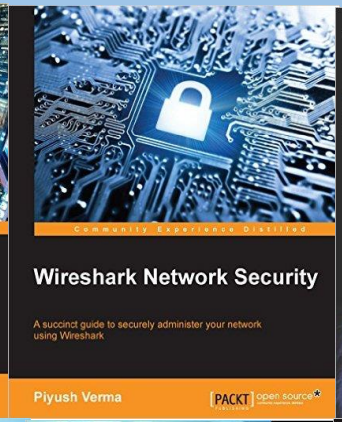


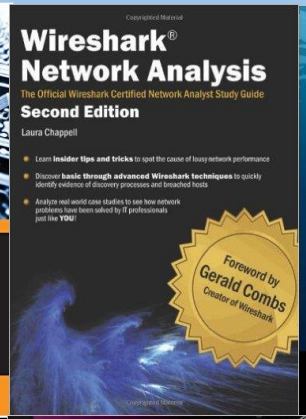
Buy All Books About Wireshark!

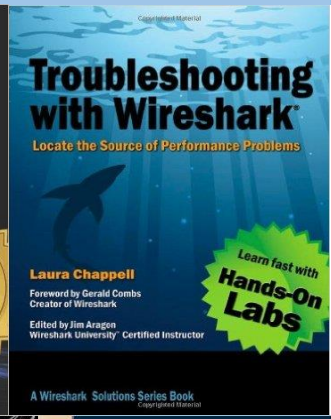


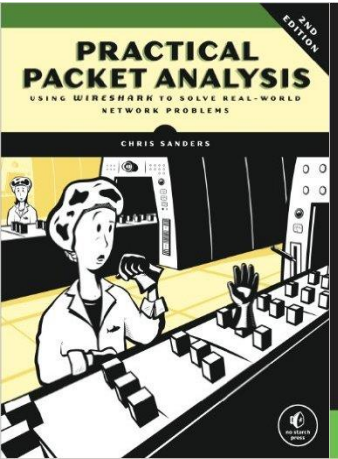


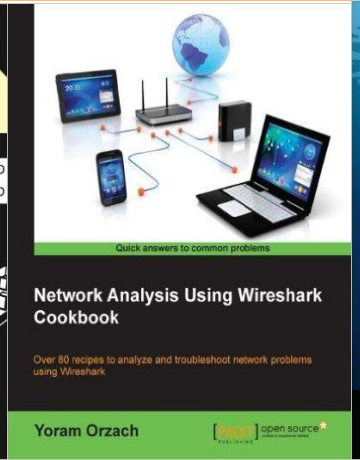


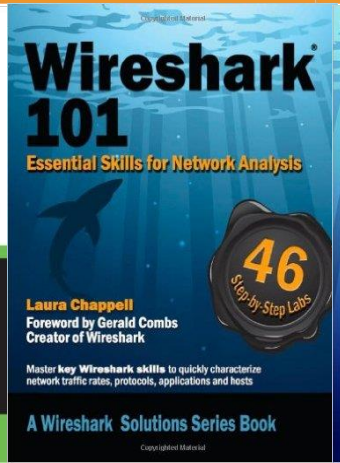


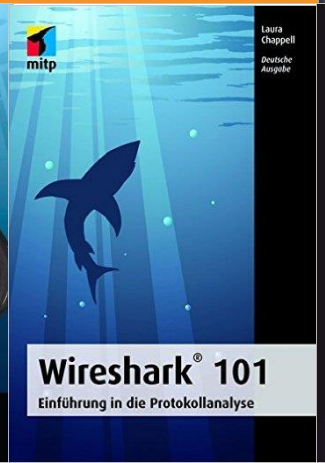


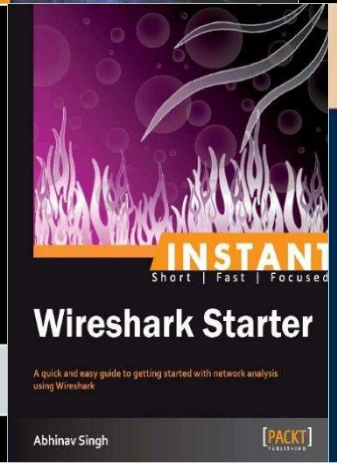


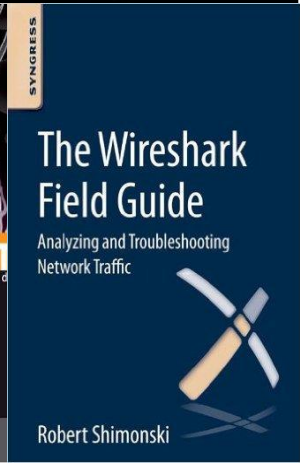




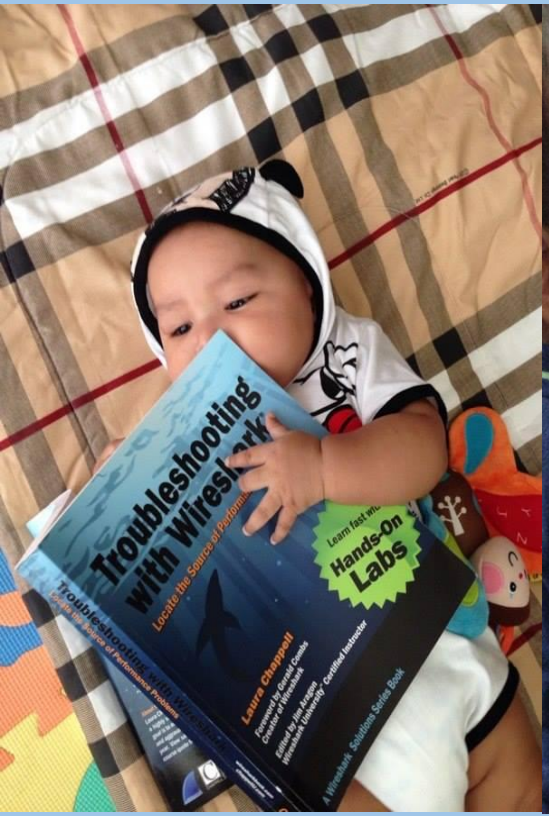


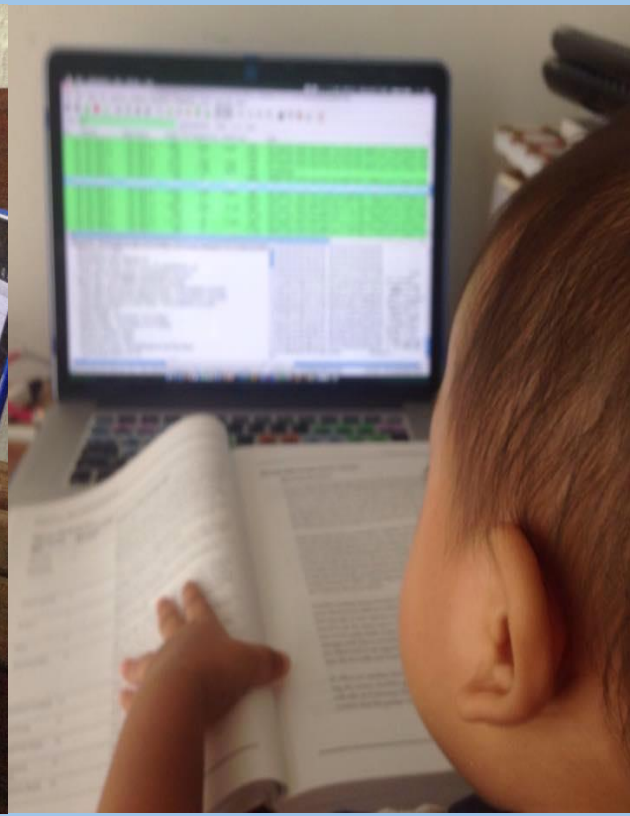






It’s never too late. Start now!

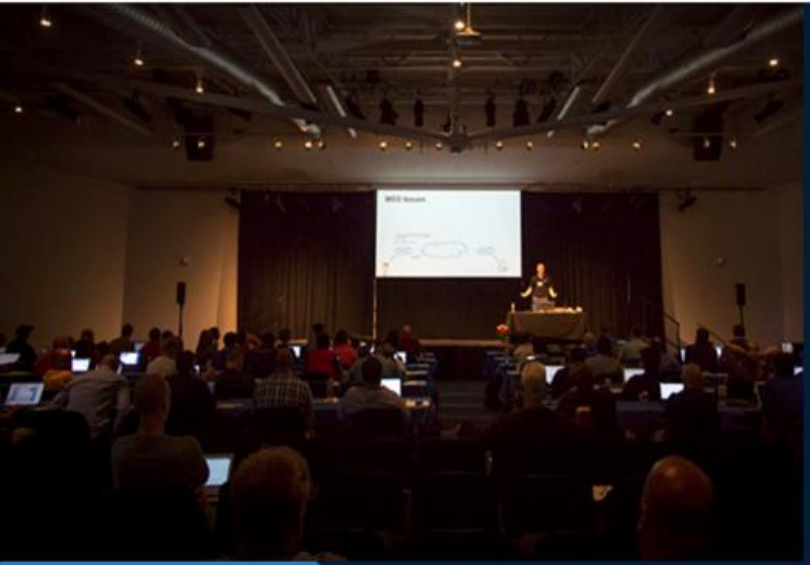




See Ya In SharkFest'18 US

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	Day 02	Day 03	Day 04	Day 05	Day 06
6.23.2018	6.24.2018	6.25.2018	6.26.2018	6.27.2018	6.28.2018

Thank you & Enjoy Packet Analysis