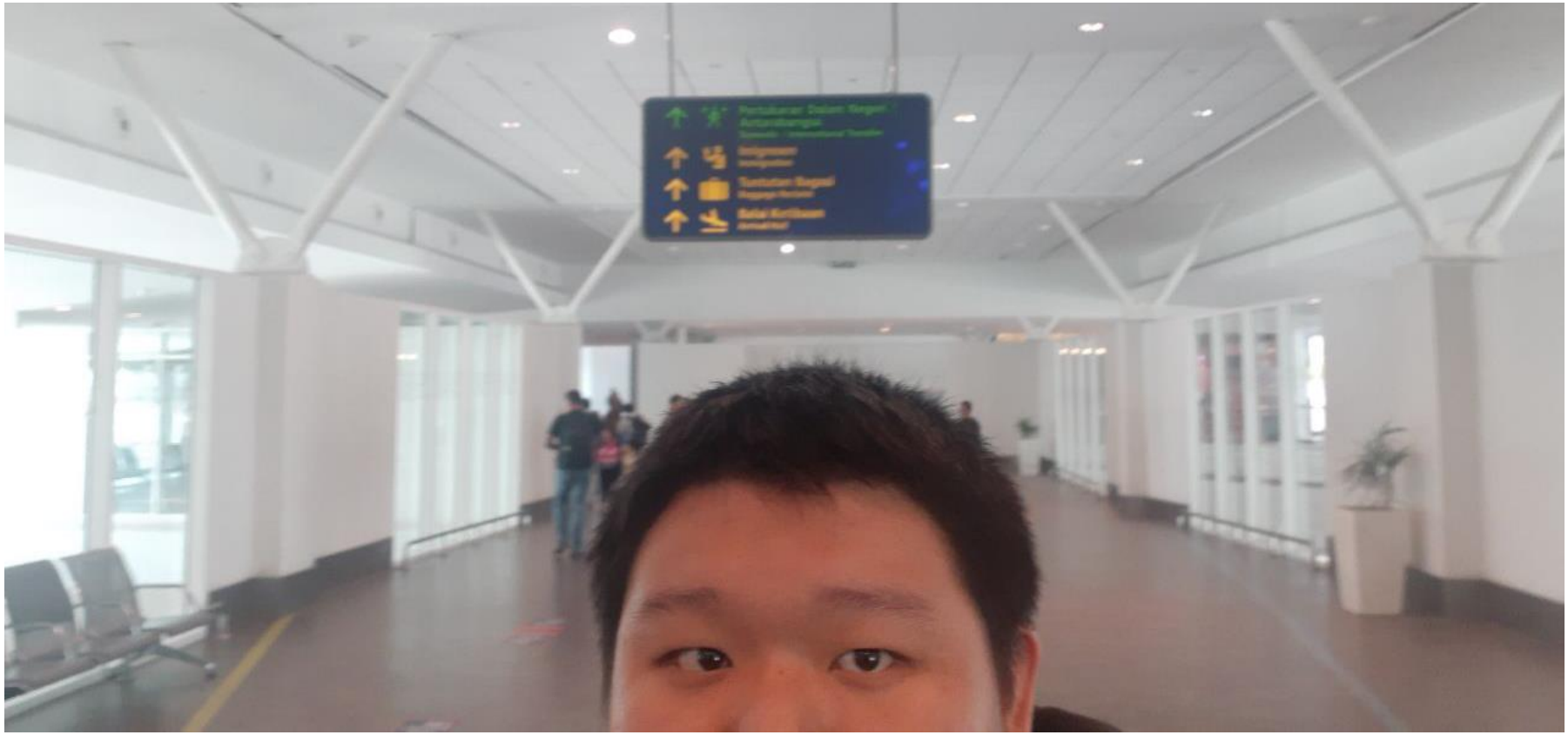
Michael Takeuchi

Practical Packet Analysis for Network Incident Response with MikroTik RouterOS

25 October 2019, Kuta Bali
MikroTik User Meeting Indonesia



Hello, I am **Michael Takeuchi**

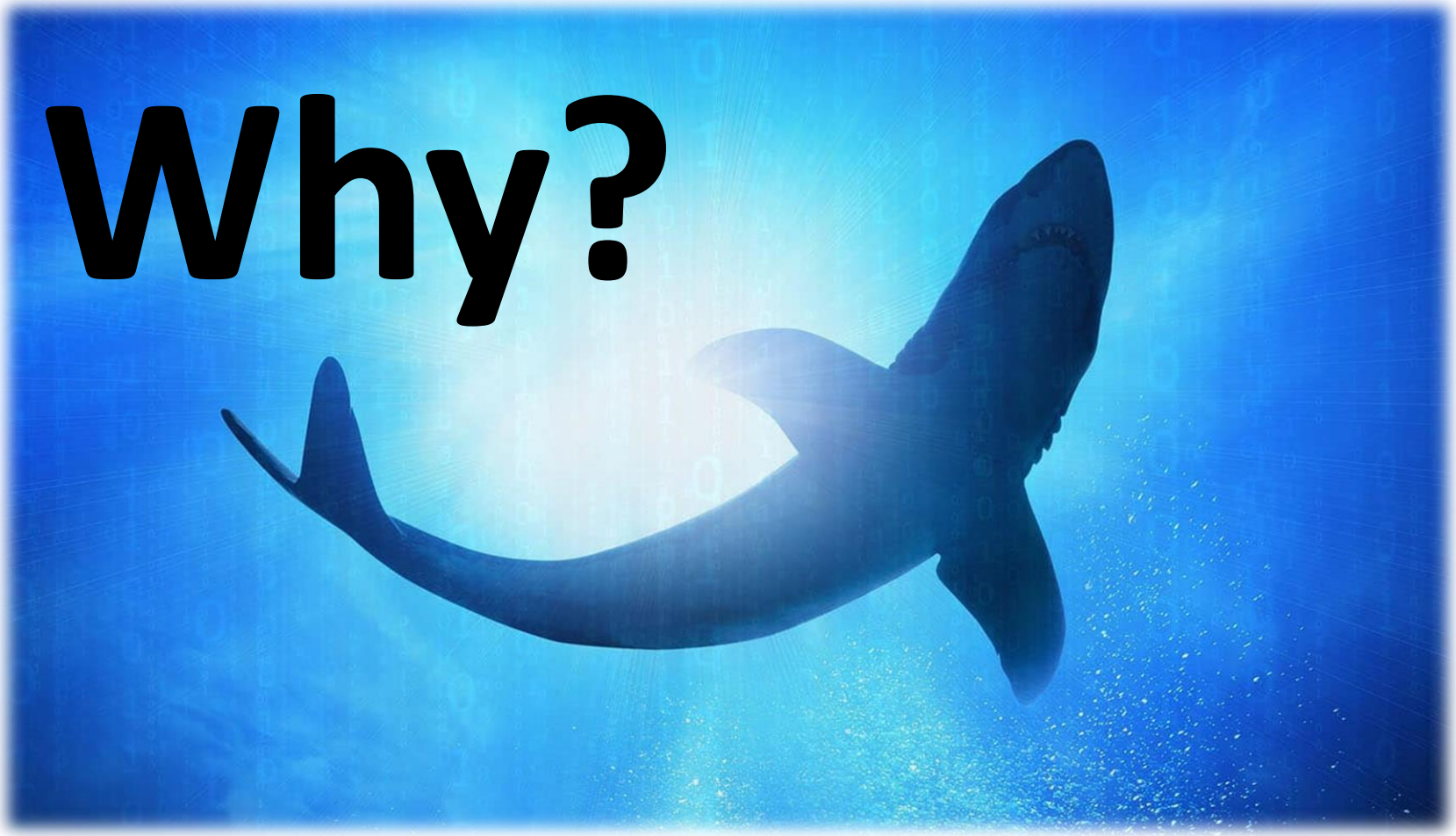
MikroTik Certified Engineer & Consultant from Jakarta, Indonesia

https://www.linkedin.com/in/michael-takeuchi

https://www.facebook.com/mict404

michael@takeuchi.id

Why Packet Analysis?



Why Packet Analysis?

- Information of 5W + 1H
  - **W**hat
    - DDoS? Spam? Flood?
  - **W**ho
    - Router? PC? Server?
  - **W**hen
    - Now? Yesterday?
  - **W**here
    - AS? Network?
  - **W**hy
    - Virus?
  - **H**ow
    - TCP? UDP?
- Action/Decision
  - Fix
  - Stop
  - Deny

Who do Packet Analysis?

- Researchers: Access to RAW Data
- Administrator: Debugging Network Problems
- Analyst: Analyze the Traffic
- Incident Responders: Tracing the Incident

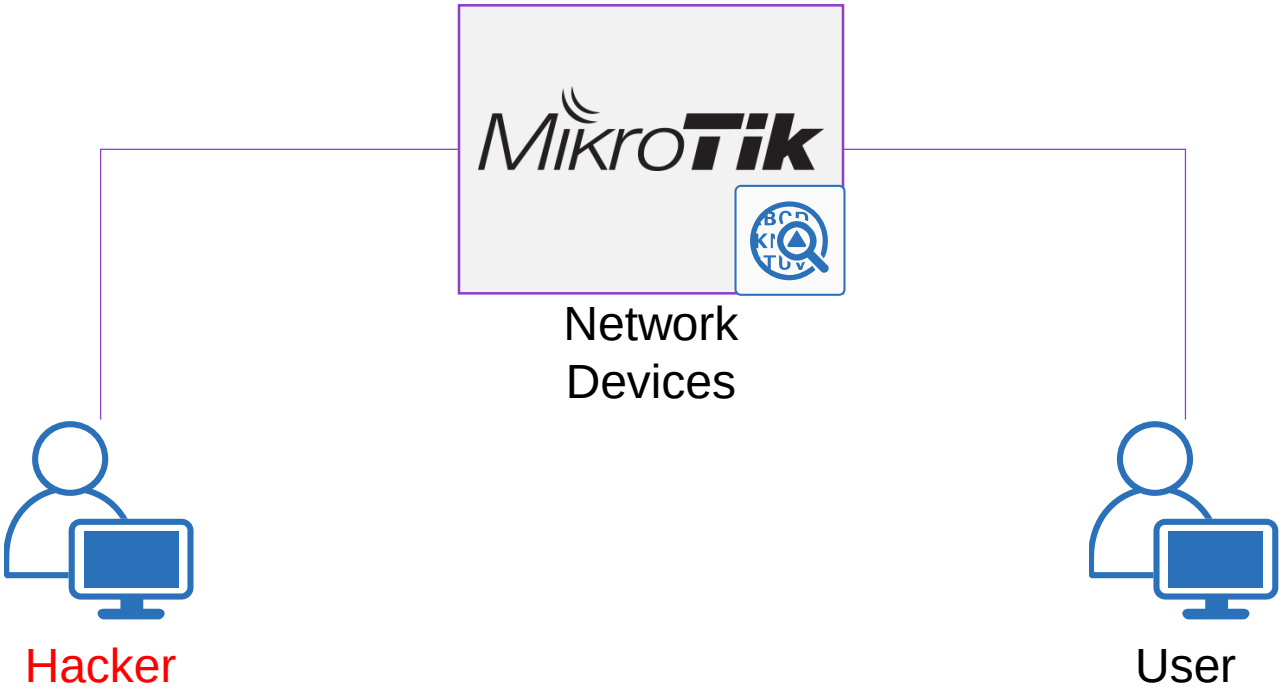
How We Do Packet Analysis?

CAPTURE & ANALYZE

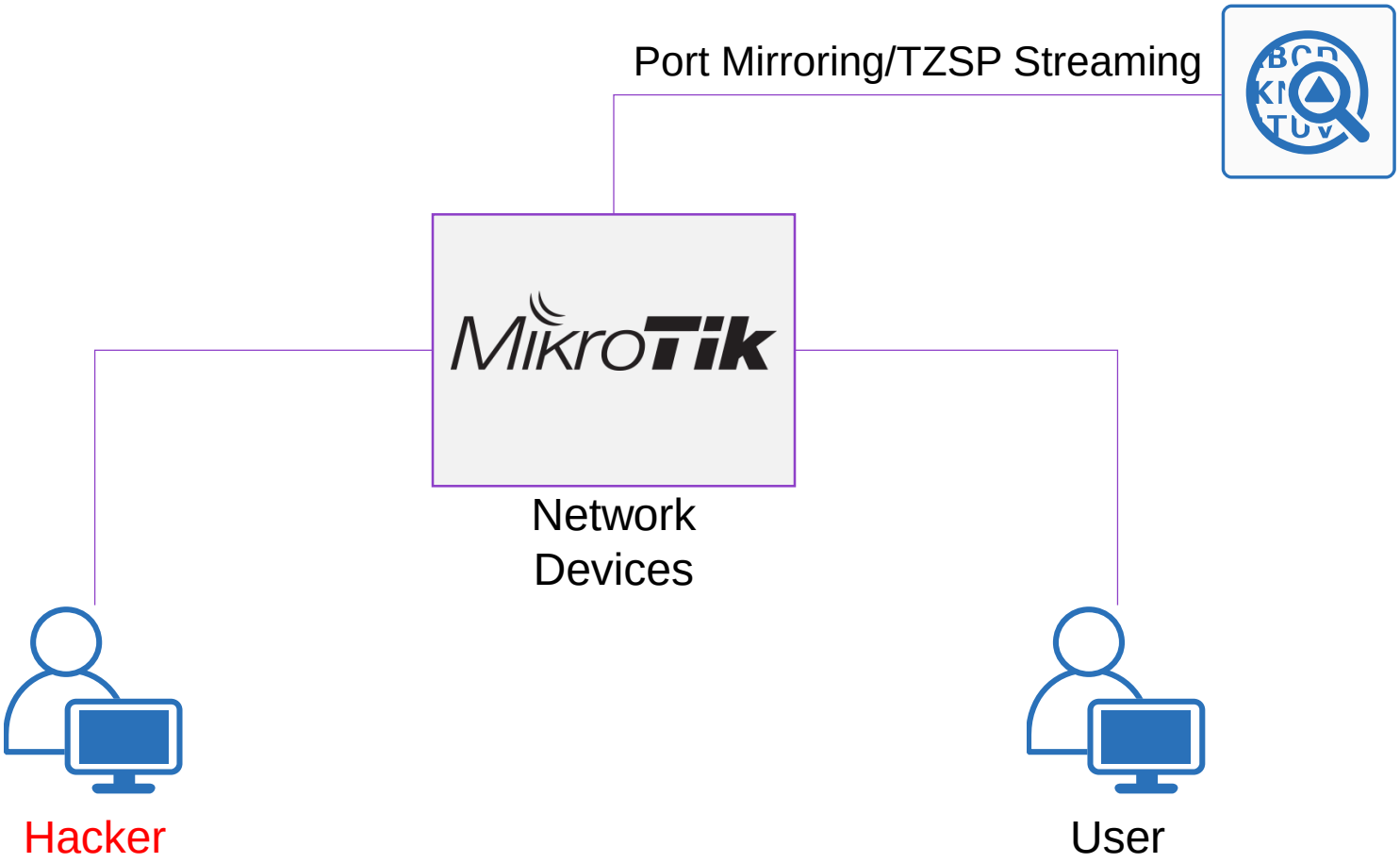
Capturing Packets

- Also known as **SNIFFING**
- PCAP is the common format of **P**acket **Cap**ture
- Perspective is Important
  - In-band
  - Out-band

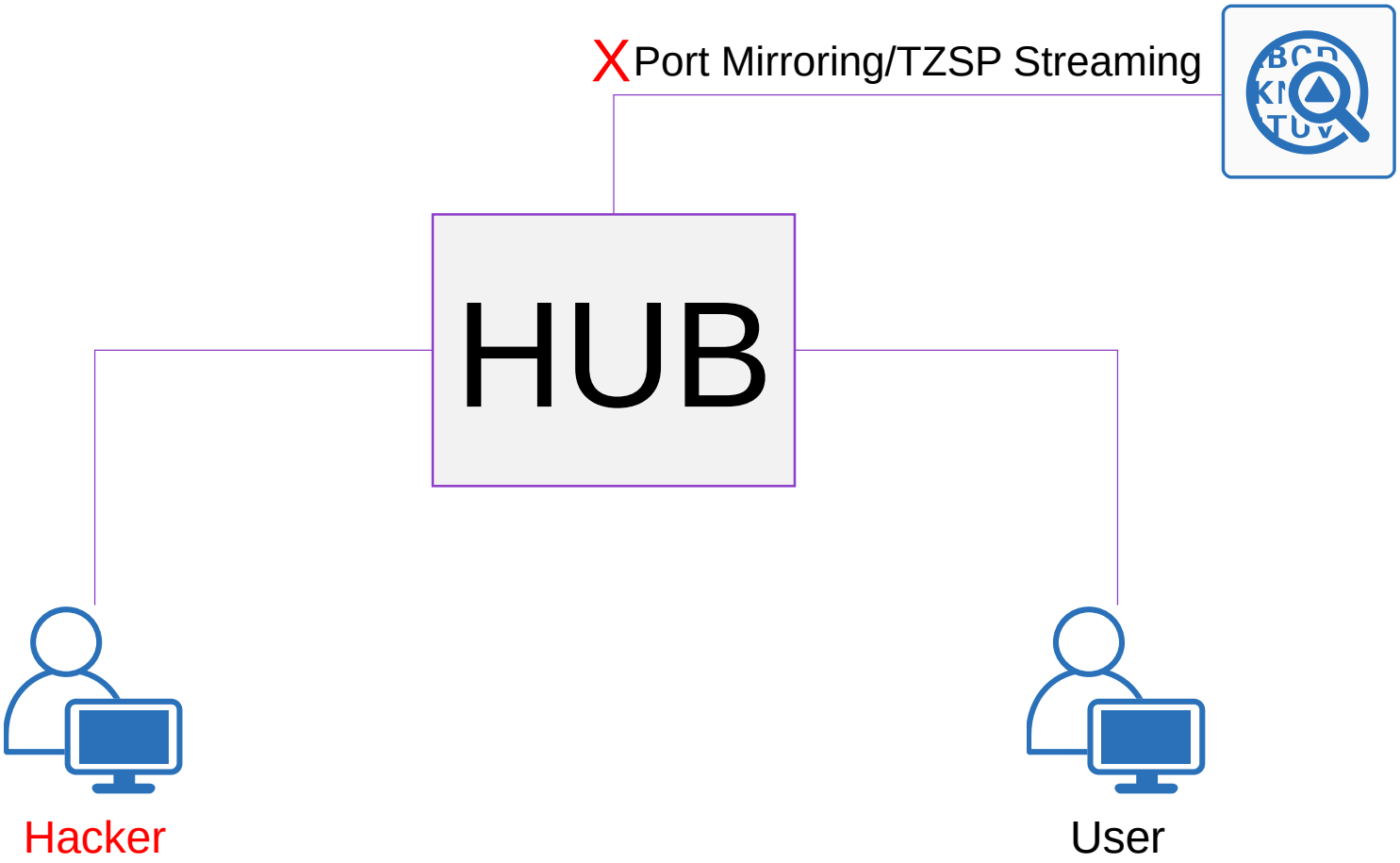
In-Band Capturing Packets/Sniffing



Out-Band Capturing Packets/Sniffing



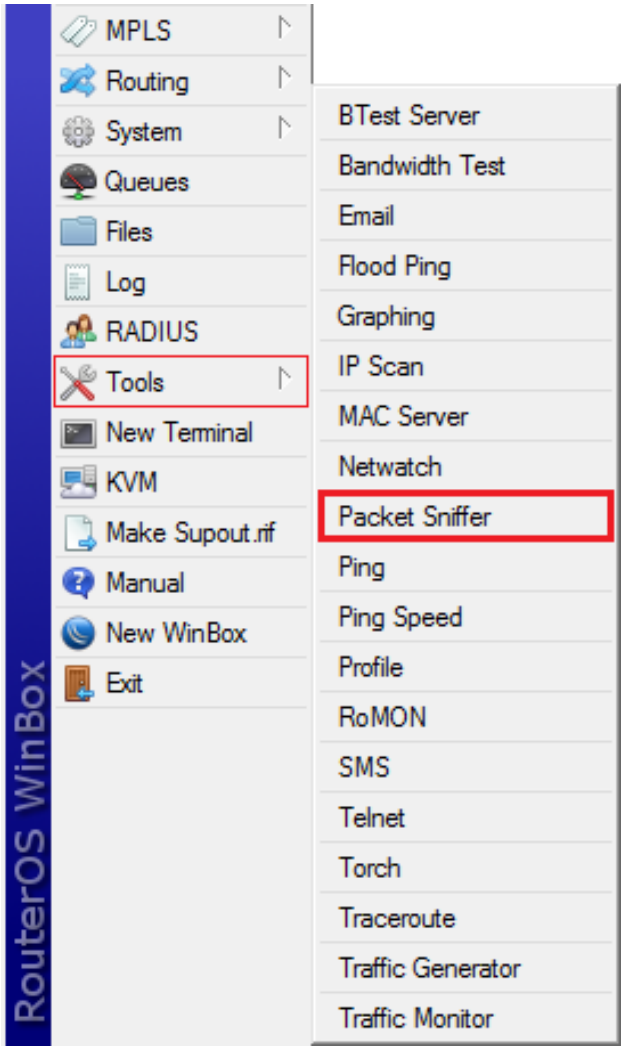
Out-Band Capturing Packets/Sniffing

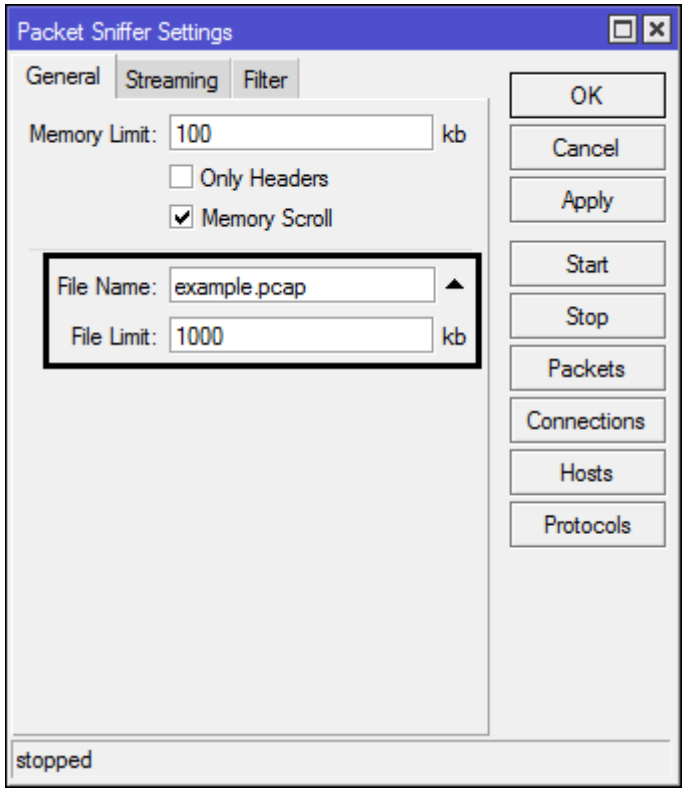


Capturing Packets in MikroTik – HTTP

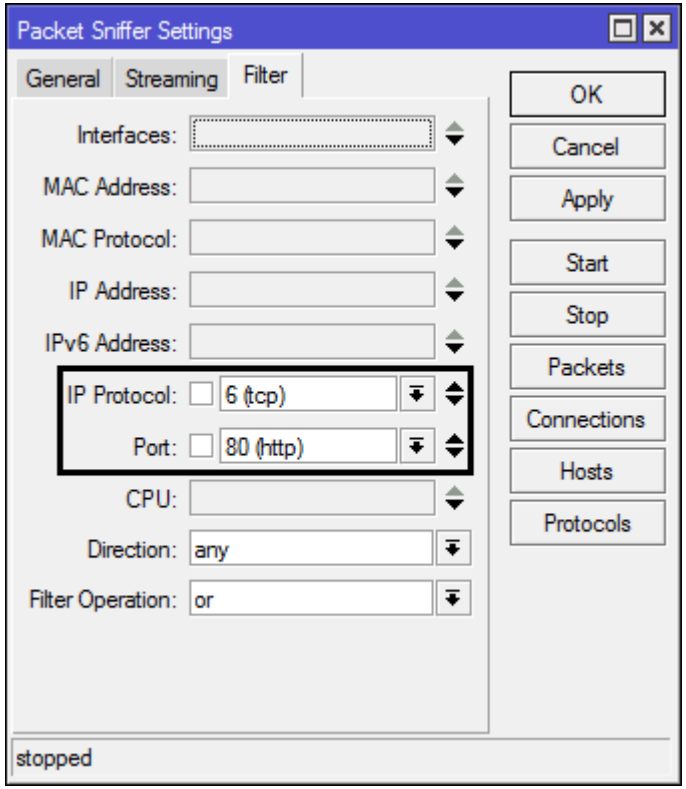
```
/tool sniffer
set file-name="example.pcap"
set file-limit="1000"
set filter-ip-protocol="tcp"
set filter-port="80"
start
/file print where name="example.pcap"
```

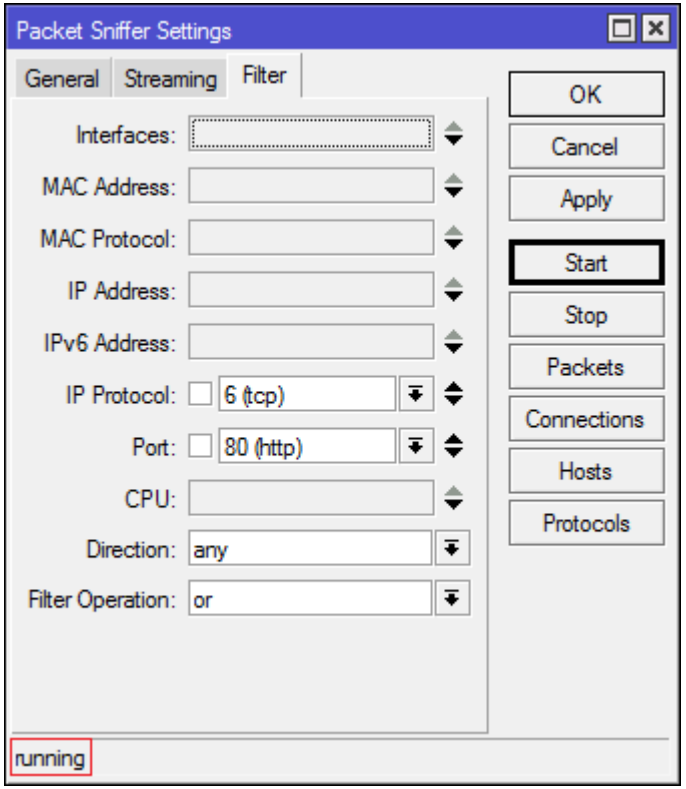
Capturing Packets in MikroTik – HTTP





Capturing Packets in MikroTik – HTTP






```
[takeuchi@MikroTik] > file print where name="example.pcap"
 # NAME                                TYPE                                SIZE
 0 example.pcap                        .pcap file                       1000.2KiB
```

Capturing Packets in MikroTik – Storage Expense

Expense storage quickly!!!

- 10Mbps * 3600 (second) * 24 (hours) = 864000Mb
- 864000Mb / 8 = 108000 Megabyte for 1 Day

10Mbps Bandwidth need 100+ Gigabyte storage for 1 Day

Double for full-duplex (200+ Gigabyte)

How big is your storage?

Solution? Use Out-Band Capturing Packets/Sniffing method with Port Mirroring, TZSP Streaming or use HUB

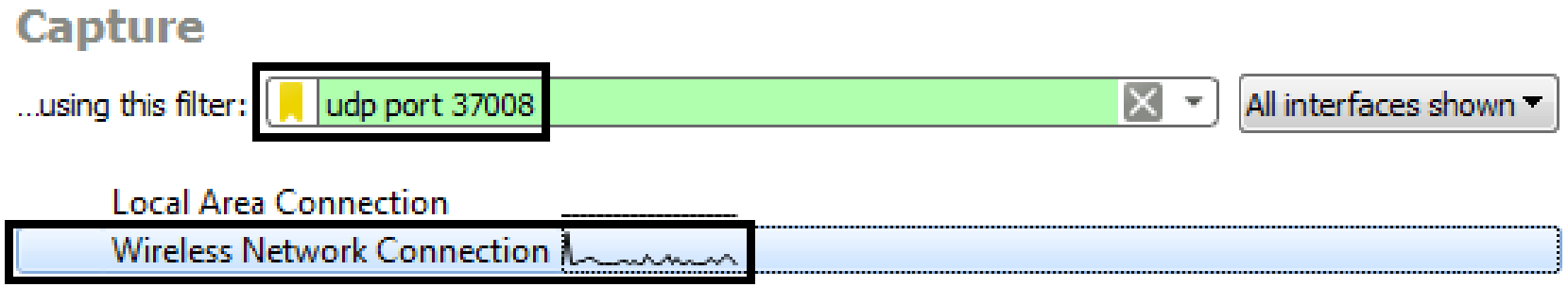
Capturing Packets in MikroTik – Port Mirroring

- Port Mirroring is Switch Chip Feature
- MikroTik devices without switch chip can’t do Port Mirroring

```
/interface ethernet switch
set switch1 mirror-source=ether2
set switch1 mirror-target=ether3
```

Capturing Packets in MikroTik – TZSP Configuration

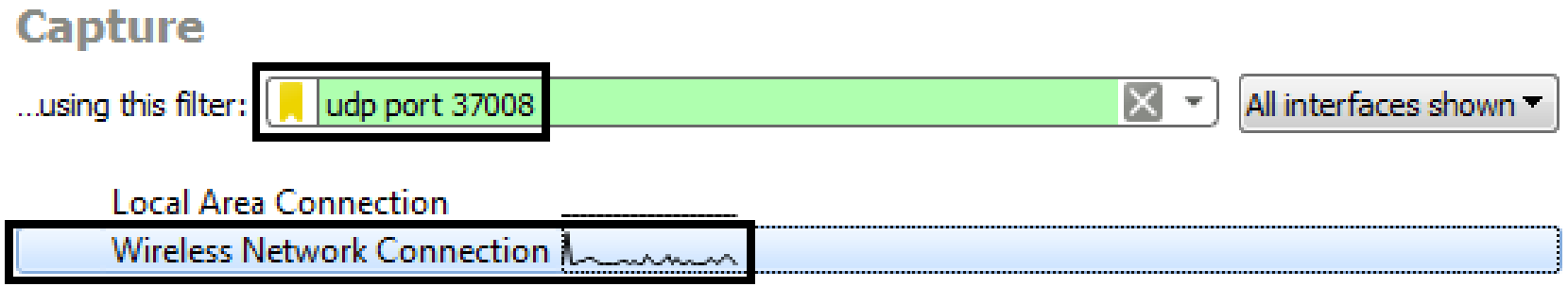
```
/tool sniffer
streaming-server=ip.of.wireshark.box
set streaming-enabled=yes
start
```



TZSP is run on UDP/37008, you can listen on UDP/37008 with your sniffing tools like **wireshark** (will introduced more in analyze step)

Capturing Packets in MikroTik – TZSP Configuration (Alt.)

```
/ip firewall mangle
add action=sniff-tzsp chain=prerouting
sniff-target=ip.of.wireshark.box
sniff-target-port=port.of.wireshark.box
```



By default TZSP is run on UDP/37008, so you can listen on UDP/37008 with your sniffing tools like **wireshark**
(will introduce wireshark more in analyze step)

Capturing Packets in MikroTik – Done

Are you done?

Let’s continue to analyze the PCAP!

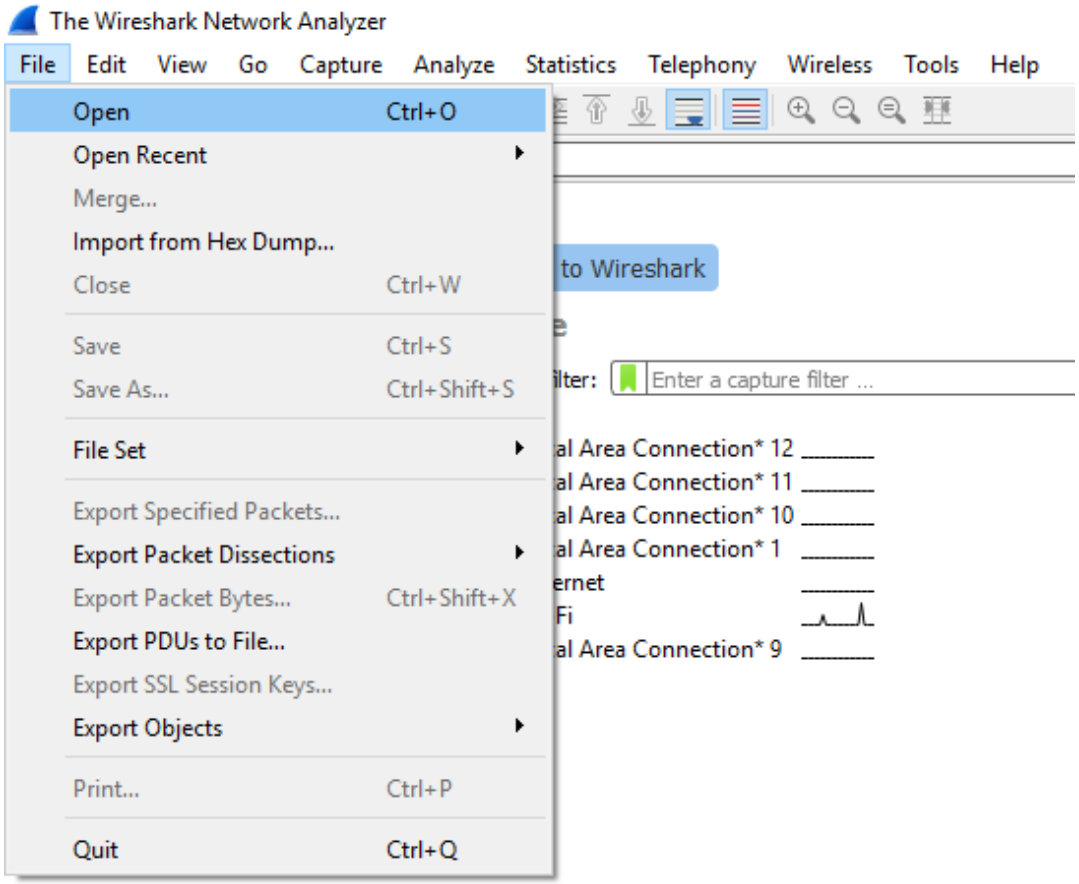
Analyzing Packets – Fire On The Tools

Fire on your tools:

- **Wireshark**
  - Open Source (GNU Public License)
  - Multi-Platform (Windows, Linux, *BSD & MacOS)
  - Advanced Filtering & Analyzing
  - Used for Live Sniffing & Packet Analysis
- Some people use **Wireshark** for:
  - Network Administrators: troubleshoot network problems
  - Network Security Engineers: examine security problems
  - Developers: debug protocol implementations
  - Peoples: learn network protocol internals

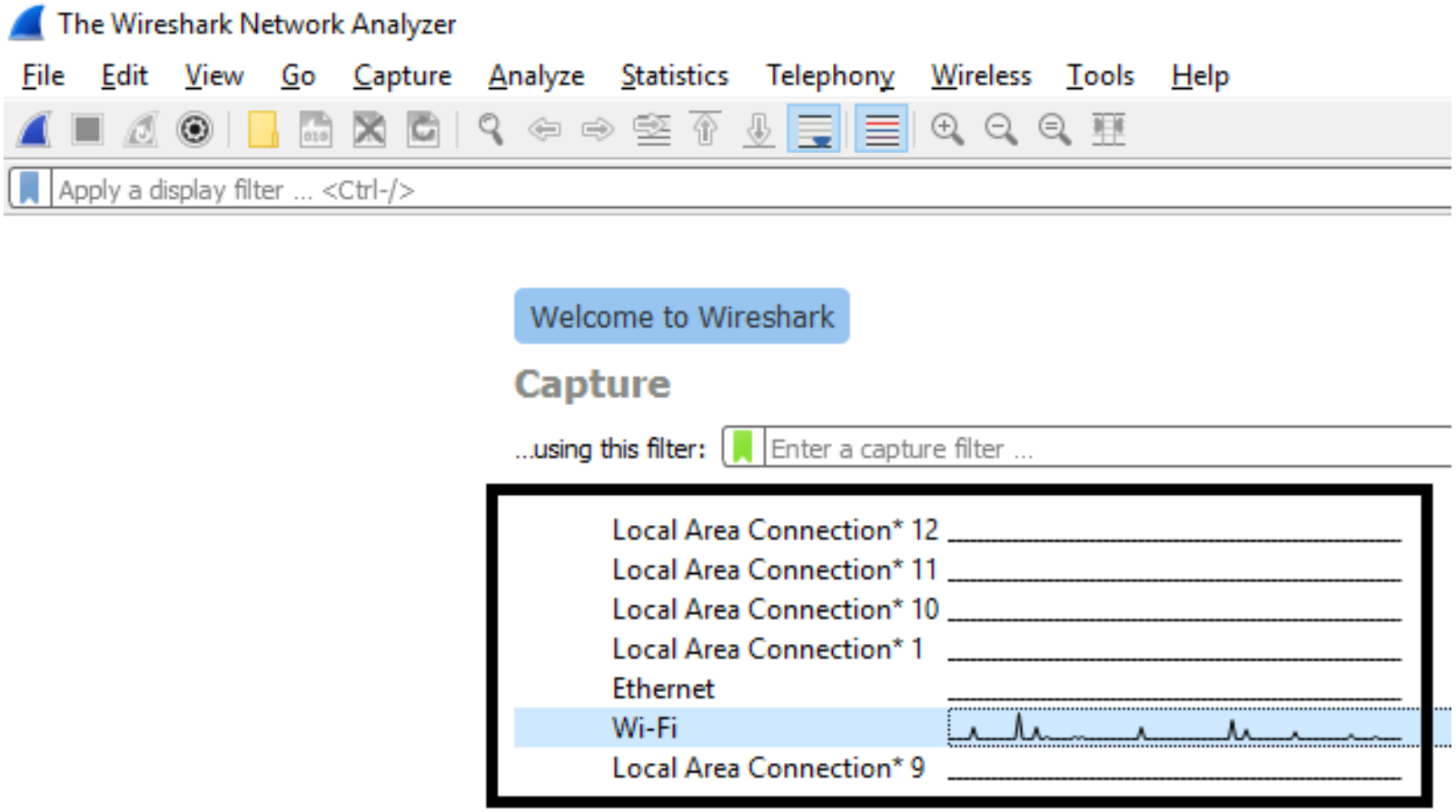
Analyzing Packets – Getting Started with Wireshark

- To getting started with wireshark you can open the pcap file that you have from capturing packets

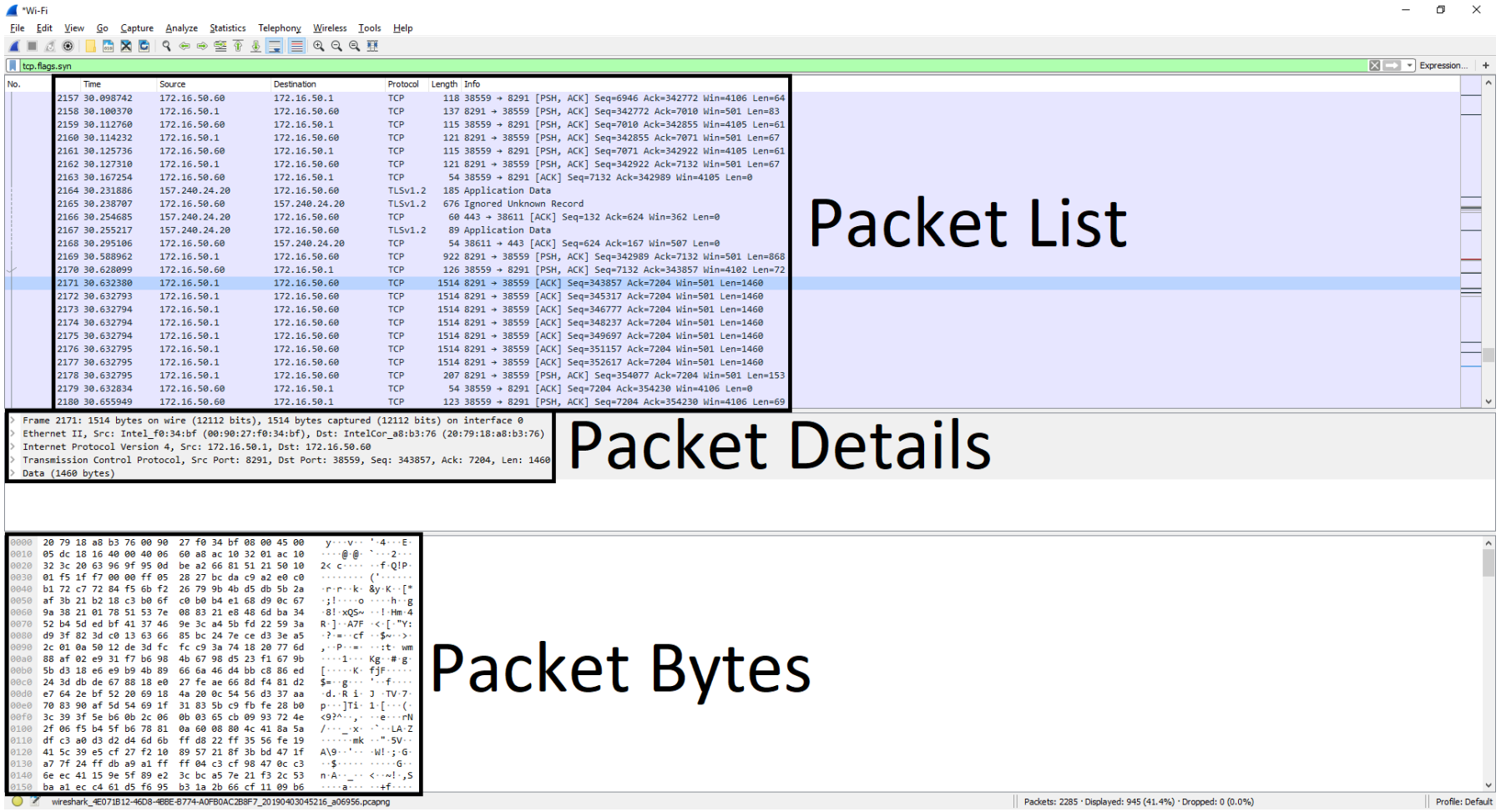


Analyzing Packets – Getting Started with Wireshark

- Or you can capture the new packets ☺

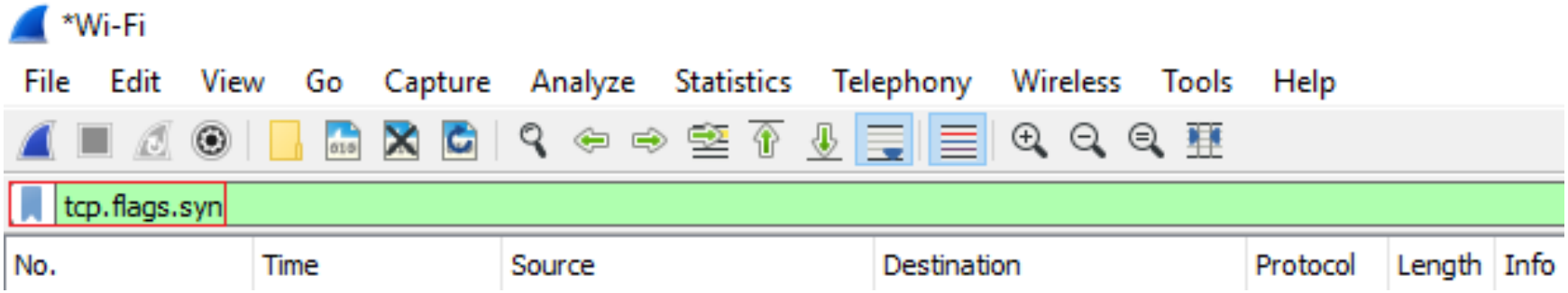


Analyzing Packets – Wireshark Interfaces



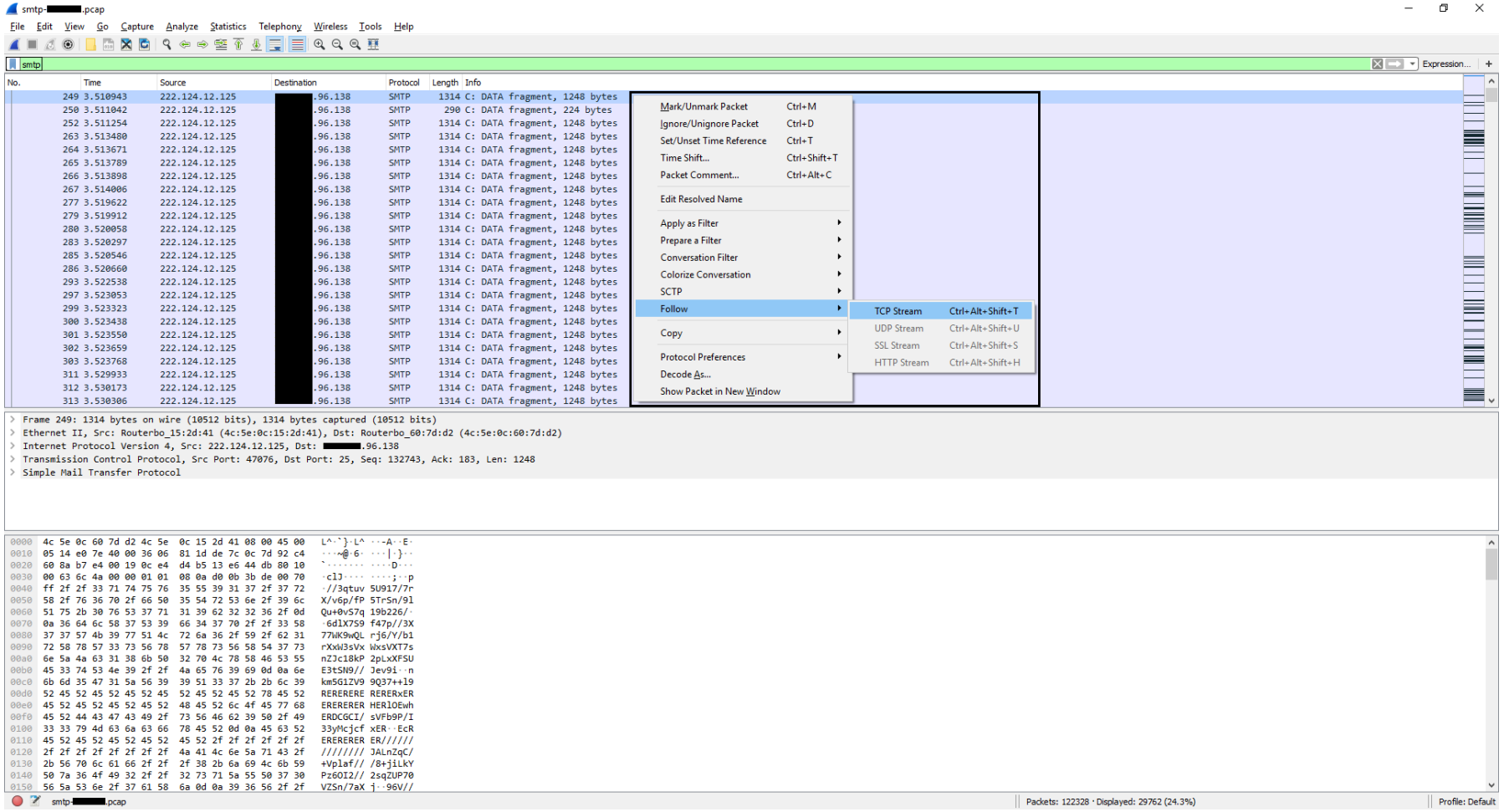
Analyzing Packets – Packet Filtering

- We can filter specific packet type in wireshark

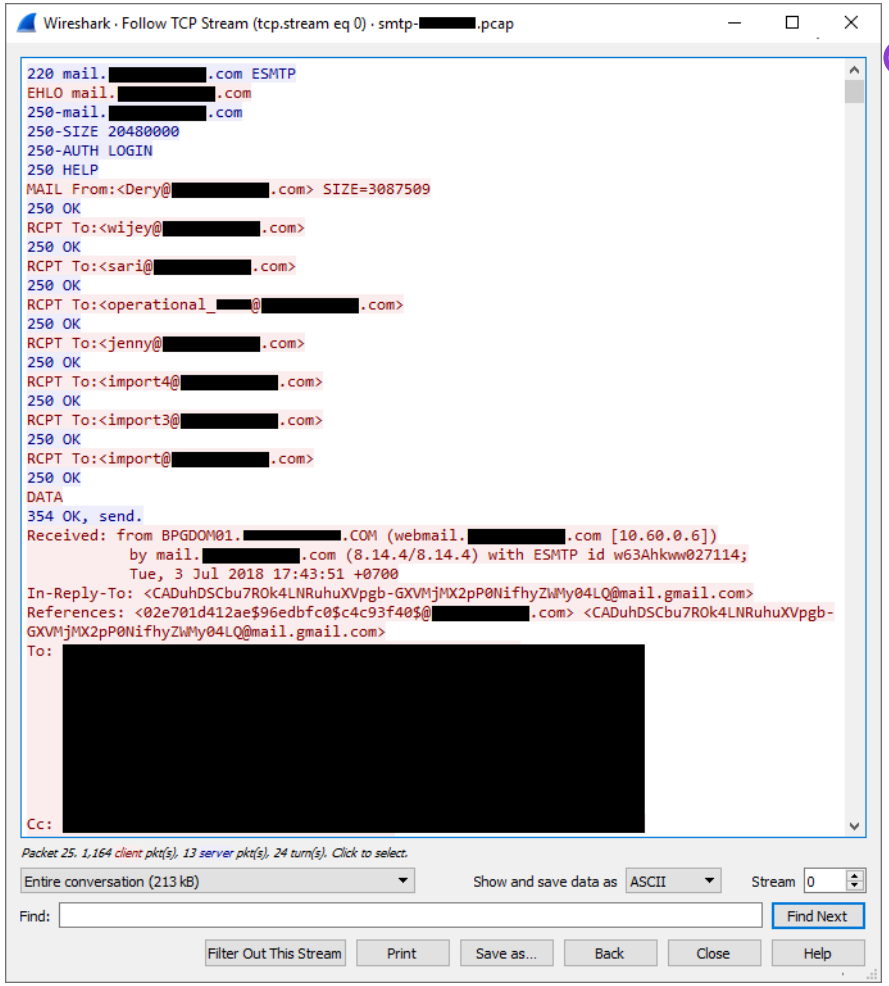


- You can check the cheat sheet on
  http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

Analyzing Packets – Fetching a Messages

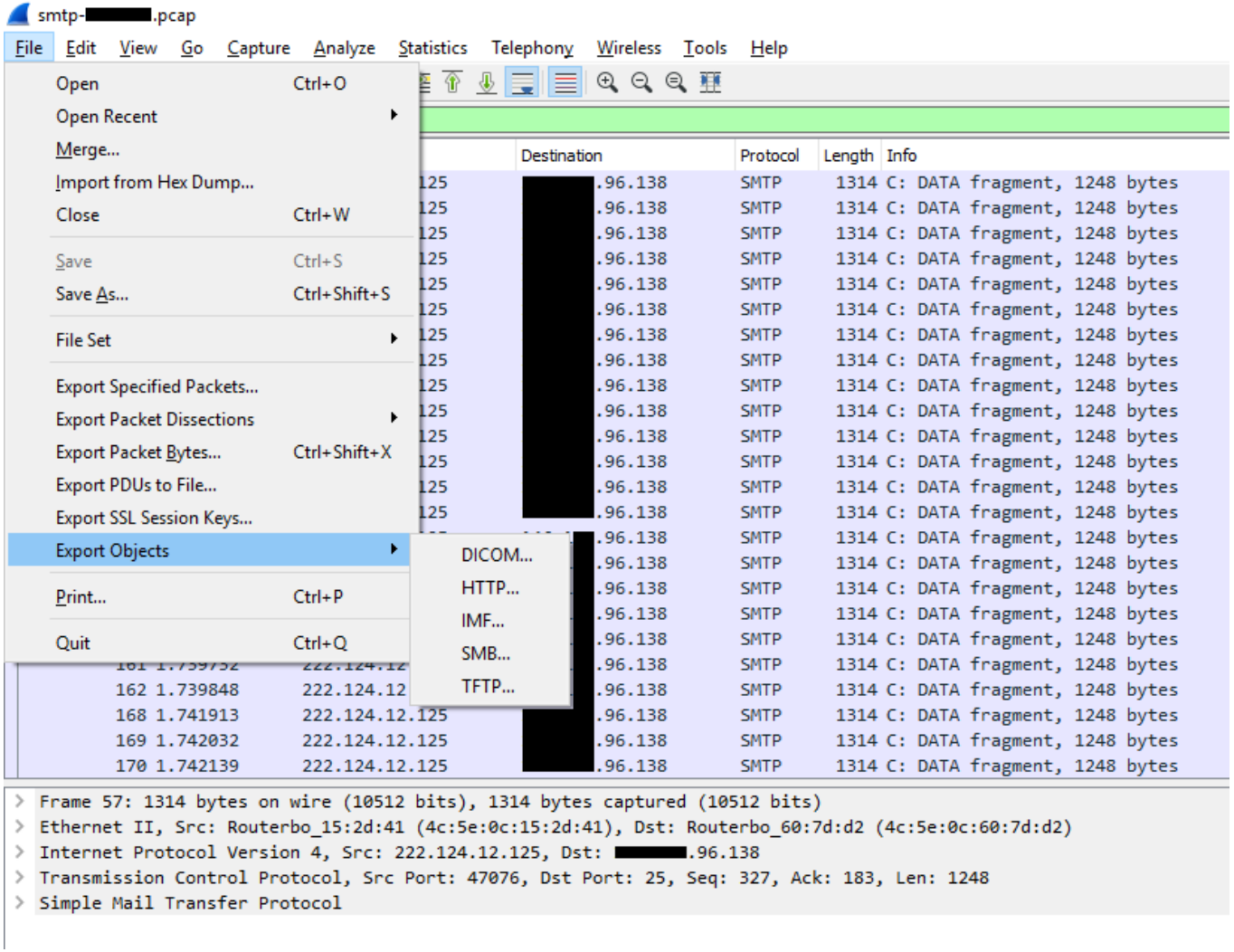


Analyzing Packets – Fetching a Messages



- Now we got a messages from email ☺ and now we can analyze the email

Analyzing Packets – Exporting Object (PDF, JPG, PNG, etc.)



Analyzing Packets – Flood Example (DNS)

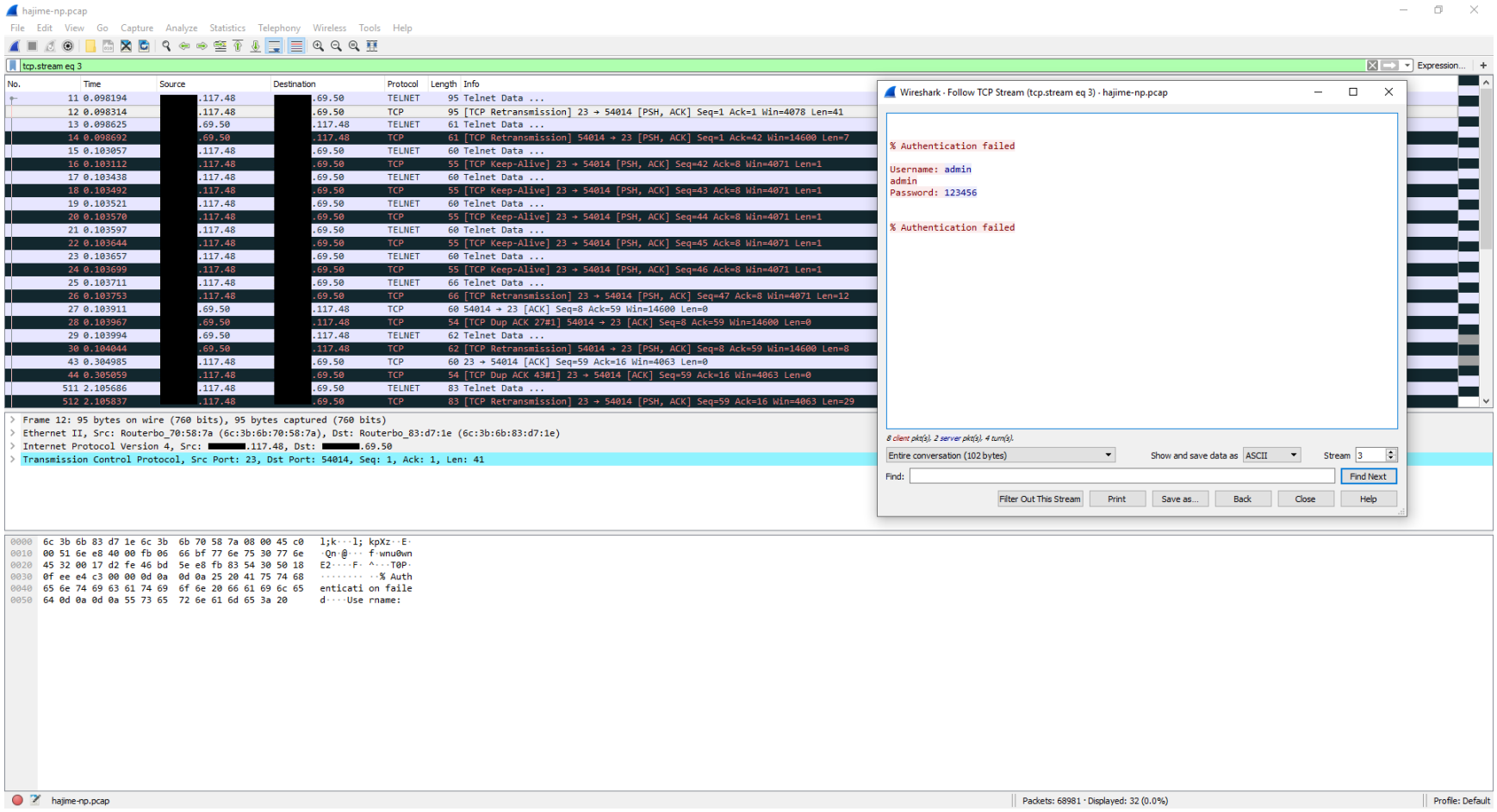
udp53.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

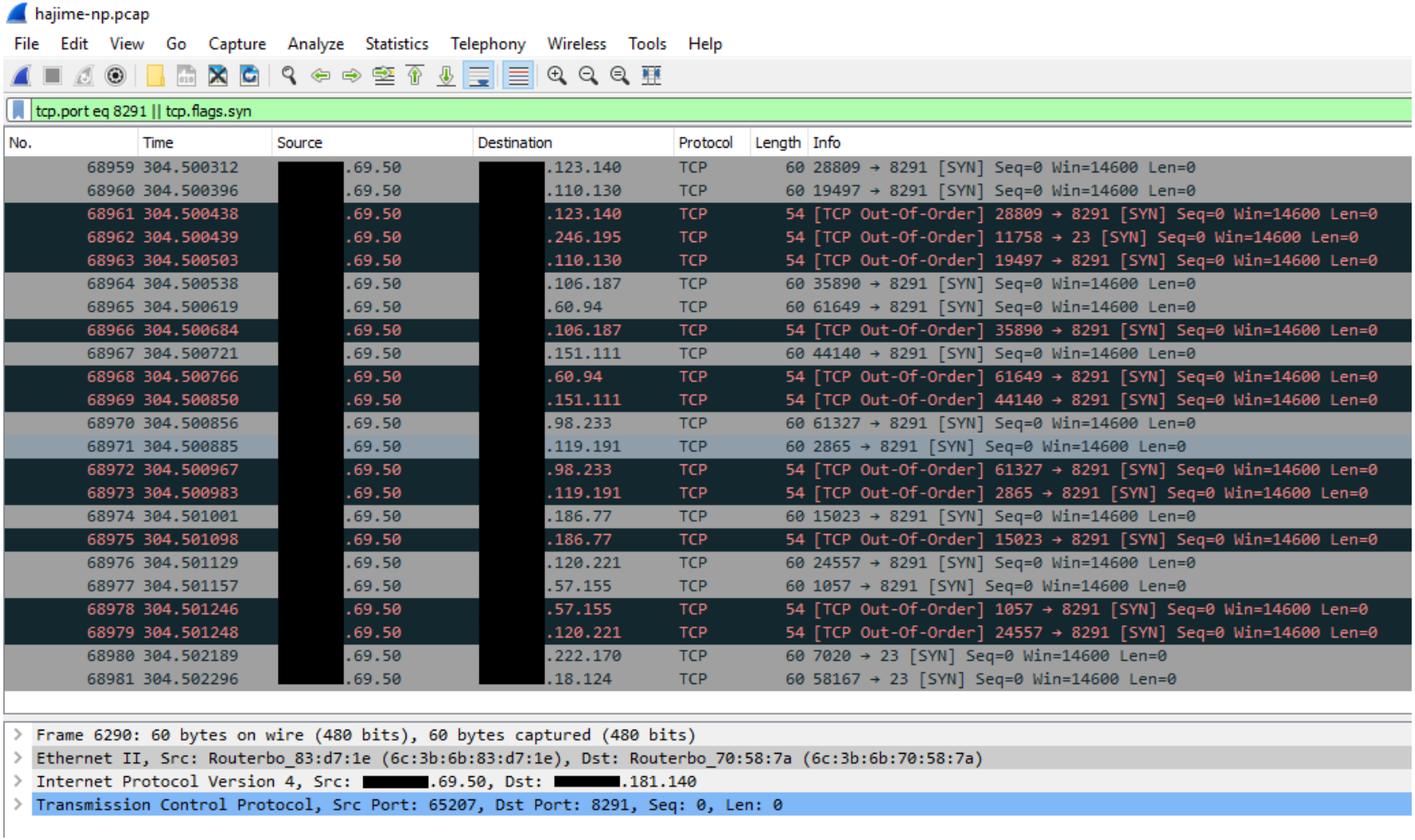
dns

No.	Time	Source	Destination	Protocol	Length	Info
6321	32.997895	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb6d3 A m9.tthbbre.com
2336	9.379658	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb6d3 A m6.rszxbjn.com
2335	9.379443	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb6d3 A m6.rszxbjn.com
856	3.542306	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb676 A m36.qjbyfio.com
855	3.542067	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb676 A m36.qjbyfio.com
2827	11.392291	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb669 A m10.qjwhpfe.net
2826	11.392077	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb669 A m10.qjwhpfe.net
3397	13.700797	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb607 A m28.pgxgxmo.com
3396	13.700657	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb607 A m28.pgxgxmo.com
3173	13.030748	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb603 A m38.ddjctyf.biz
3172	13.030574	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb603 A m38.ddjctyf.biz
662	2.620854	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb5c0 A m31.swwgocu.net
661	2.620628	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb5c0 A m31.swwgocu.net
4996	26.914537	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb5be A m7.brmgkod.com
4995	26.914357	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb5be A m7.brmgkod.com
7936	40.211405	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb596 A m9.bnwqcxl.com
7935	40.211193	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb596 A m9.bnwqcxl.com
6961	35.918350	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb588 A m30.atoifmo.com
6960	35.918120	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb588 A m30.atoifmo.com
7059	36.405497	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb54d A m16.plswhql.cc
7058	36.405310	[redacted].68.170	8.8.4.4	DNS	74	Standard query 0xb54d A m16.plswhql.cc
134	0.488968	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb51b A m30.shbqnoe.net
133	0.488805	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb51b A m30.shbqnoe.net
1256	5.029502	[redacted].68.170	8.8.4.4	DNS	75	Standard query 0xb51a A m31.gumqkle.net

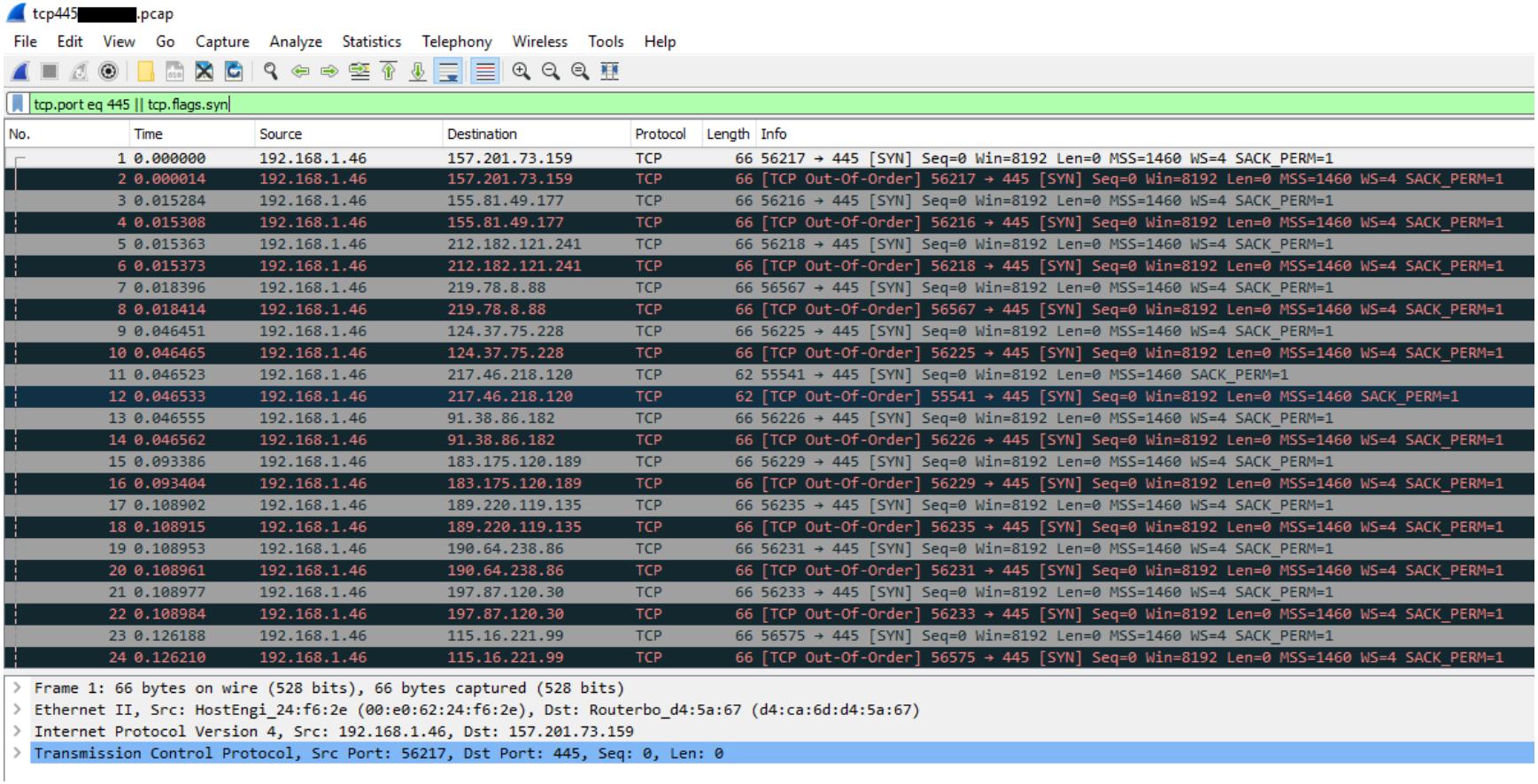
Analyzing Packets – Flood Example (TELNET)



Analyzing Packets – Flood Example (WINBOX)



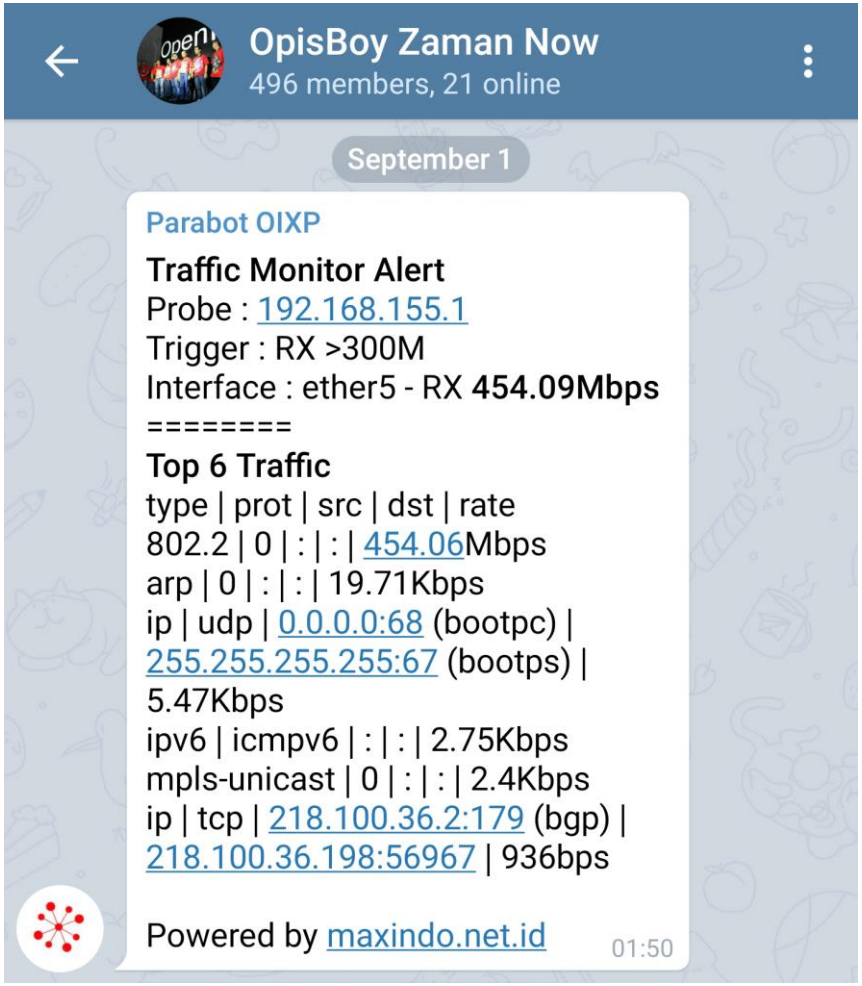
Analyzing Packets – Flood Example (SMB)



Analyzing Packets – Wireshark Reference

- Wireshark Website
  http://www.wireshark.org
- Wireshark Documentation
  http://www.wireshark.org/docs/
- Wireshark Wiki
  http://wiki.wireshark.org
- Network analysis Using Wireshark Cookbook
  http://www.amazon.com/Network-Analysis-Using-WiresharkCookbook/dp/1849517649

Study Case – Parabot OpenIXP



- **OpenIXP** is one of the biggest Internet Exchange in Indonesia
- and **Parabot**, a Bot in Telegram that brewed by **@ericksetiawan** and the Infrastructure was provided by **@mtakeuchi** using MikroTik RouterOS as a Probe & BGP router in OpenIXP, also Powered by **Maxindo** Networks
- Parabot help to notify us when the router **receiving** broadcast or flood on OpenIXP interface
- Parabot will do Torch and start **Packet Sniffer** on your Router

Conclusion

Secure ≠ Easy

Feel so hard to analyze?

Let me help you!

michael@takeuchi.id

https://www.facebook.com/mict404

https://www.linkedin.com/in/michael-takeuchi/

Question & Answer

Slide is available in my GitHub repository
https://github.com/mict404/slide/