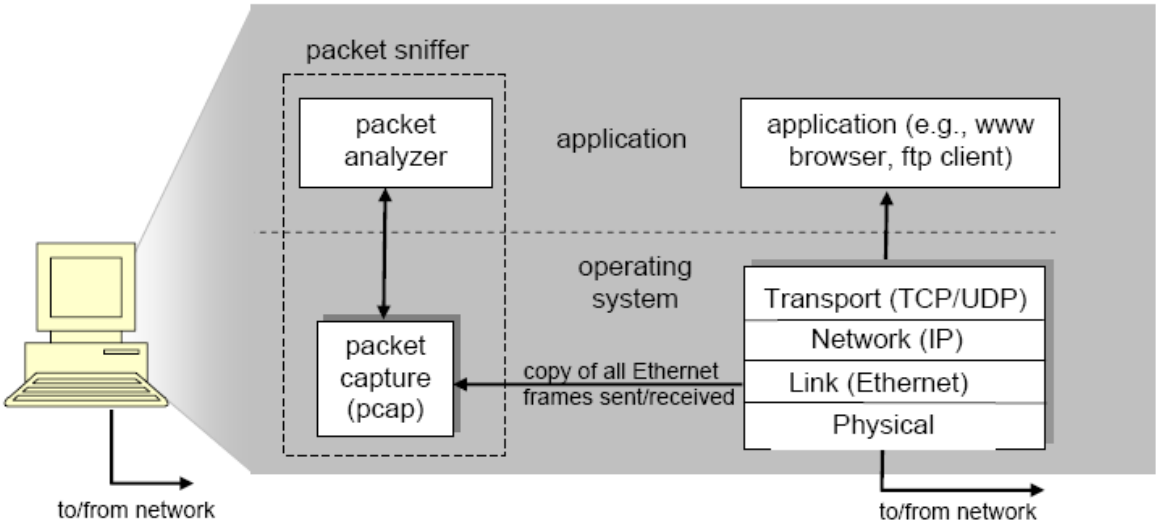
Wireshark

Introduction

- Wireshark โปรแกรมสำหรับใช้ดักจับและวิเคราะห์ข้อมูลบนเครือข่าย (ชื่อเดิม *Etherreal*)
- Wireshark is the world's foremost and widely-used network protocol analyzer
- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis

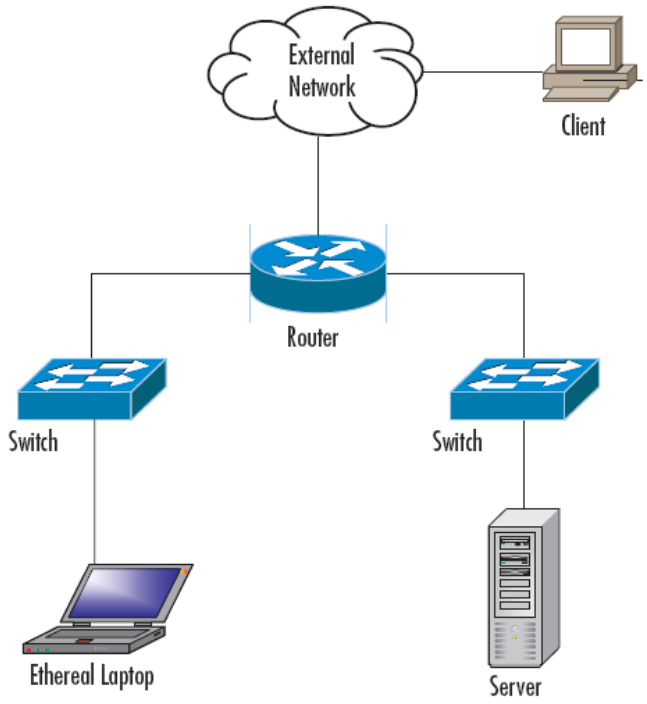
Packet Capture

- *Packet Capture* - การดักจับข้อมูลบนเครือข่าย
- *Packet Analyzer* - การแปลงข้อมูลที่ดักจับได้ให้อยู่ในรูปแบบที่เข้าใจได้ง่าย
- *Packet Sniffer* - โปรแกรมสำหรับใช้ดักจับและแปลงข้อมูลโดยทำงานในแบบ *Promiscuous mode*

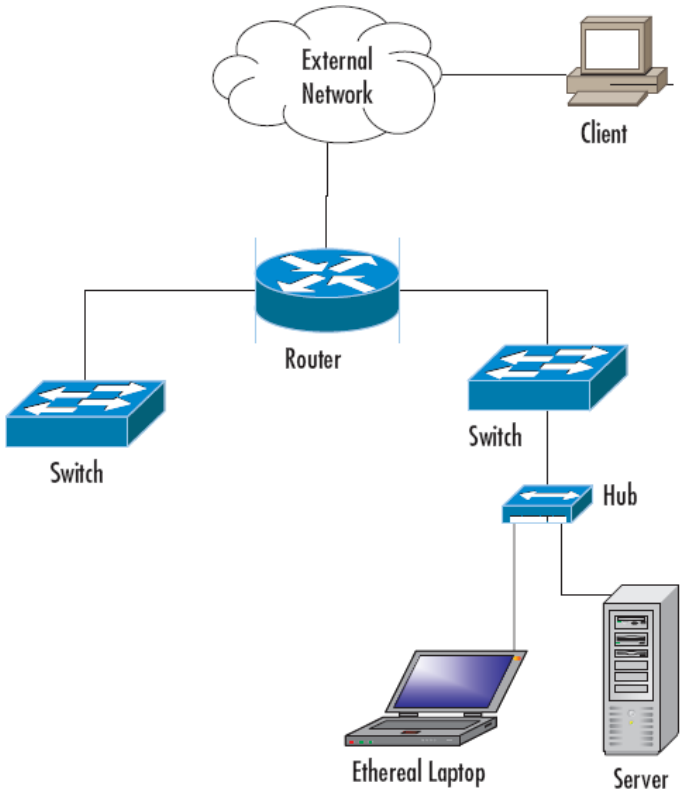


Wireshark Placement

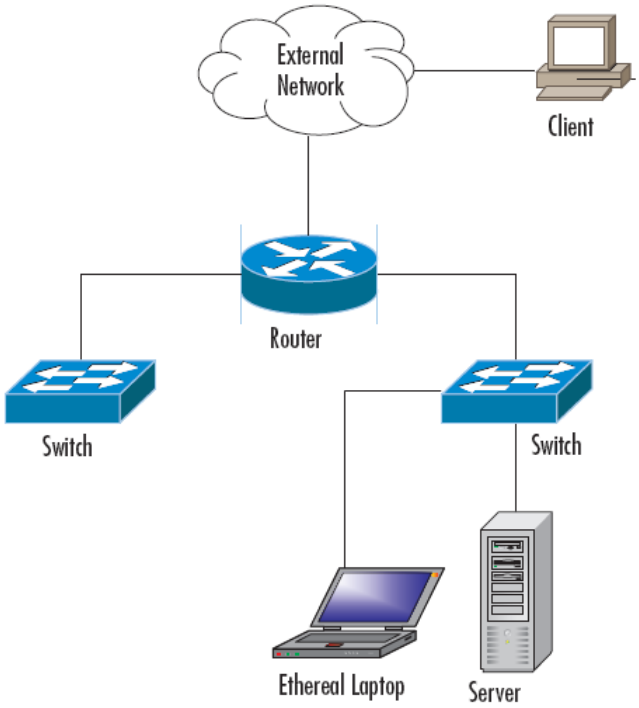
- Incorrect



- Correct - **Hub**



- Correct - **Port Spanning**



Installation

- Download

```
https://www.wireshark.org/download.html
Wireshark-4.2.6-x64.exe
```

- Setup

```
Install
+ Npcap
```

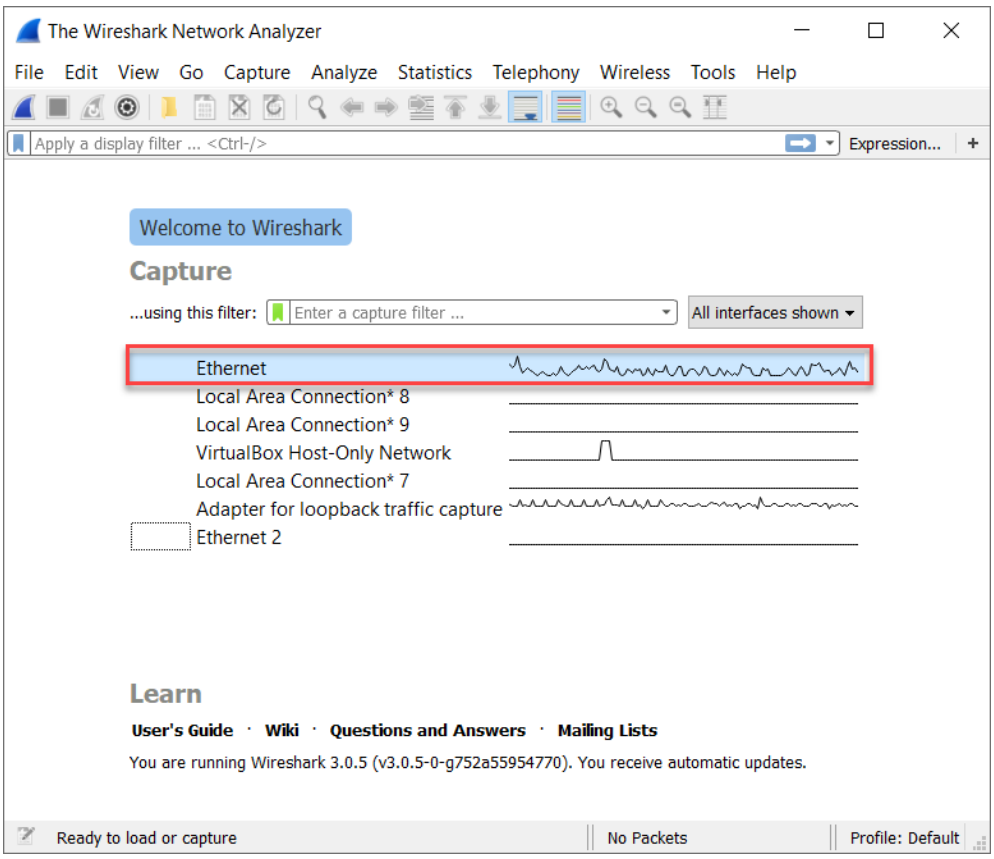
Capture packet

- ตรวจสอบ Network card และ IP

```
ipconfig /all
```

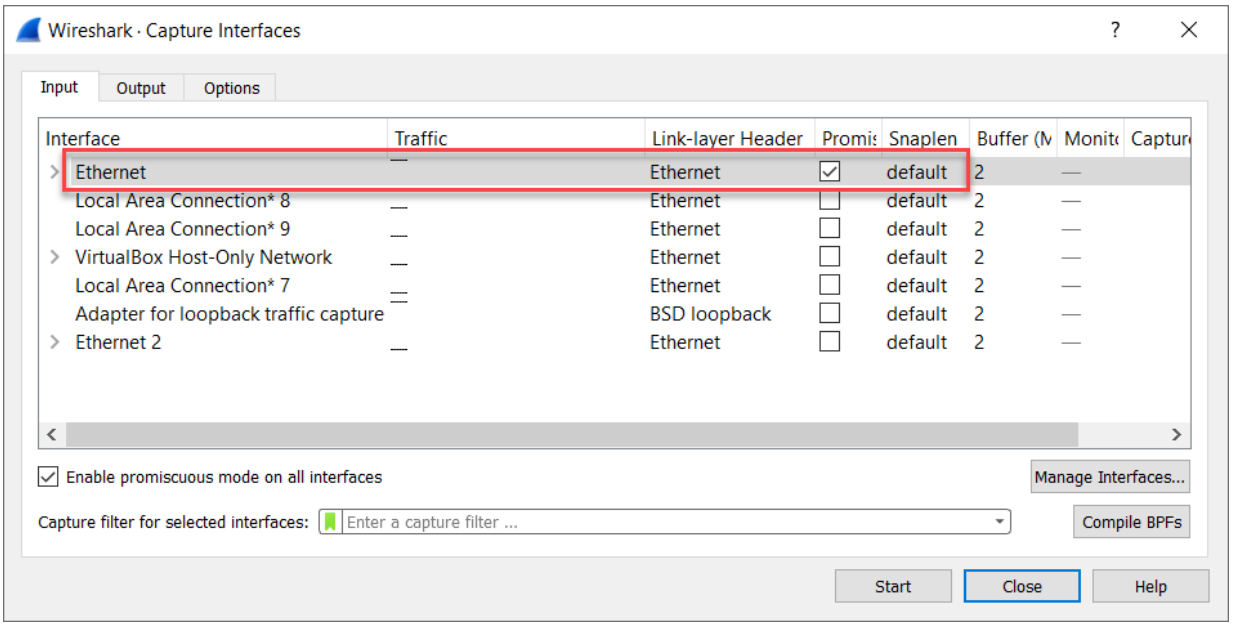
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (14) I219-LM
   Physical Address. . . . . . . . . : 46-E5-17-4B-76-A2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.117(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 17 กรกฎาคม 2566 13:34:07
   Lease Expires . . . . . . . . . . : 18 กรกฎาคม 2566 13:34:04
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- เริ่มต้น Wireshark
- Network interface ซึ่งสามารถใช้ดักจับข้อมูล



- Select Network interface

`Capture > Options`



- เริ่มดักจับ Packet

`Capture > Start (Ctrl+E)`

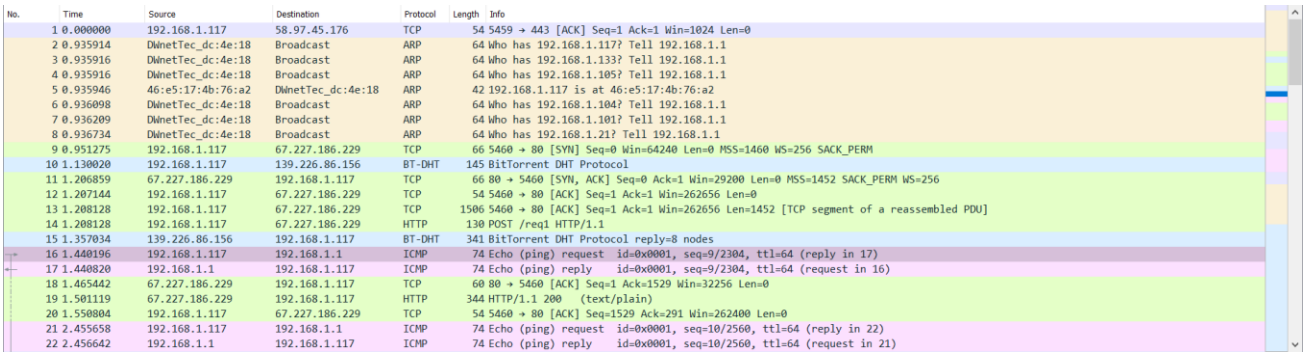
- เปลี่ยนเป็นเครื่อง Teacher

`ping ?`

- หยุดดักจับ Packet

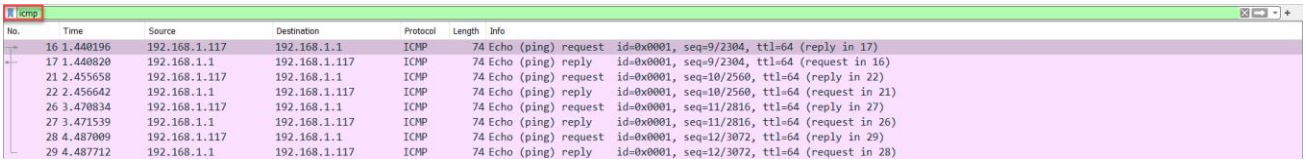
`Capture > Stop (Ctrl+E)`

- Result
  - ต้องการเฉพาะ ICMP สีชมพู



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.117	58.97.45.176	TCP	54	5459 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
2	0.935914	DWnetTec_dc:4e:18	Broadcast	ARP	64	Who has 192.168.1.117? Tell 192.168.1.1
3	0.935916	DWnetTec_dc:4e:18	Broadcast	ARP	64	Who has 192.168.1.133? Tell 192.168.1.1
4	0.935916	DWnetTec_dc:4e:18	Broadcast	ARP	64	Who has 192.168.1.105? Tell 192.168.1.1
5	0.935946	46:e5:17:4b:76:a2	DWnetTec_dc:4e:18	ARP	42	192.168.1.117 is at 46:e5:17:4b:76:a2
6	0.936098	DWnetTec_dc:4e:18	Broadcast	ARP	64	Who has 192.168.1.104? Tell 192.168.1.1
7	0.936209	DWnetTec_dc:4e:18	Broadcast	ARP	64	Who has 192.168.1.101? Tell 192.168.1.1
8	0.936734	DWnetTec_dc:4e:18	Broadcast	ARP	64	Who has 192.168.1.21? Tell 192.168.1.1
9	0.951275	192.168.1.117	67.227.186.229	TCP	66	5460 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	1.130020	192.168.1.117	139.226.86.156	BT-DHT	145	BitTorrent DHT Protocol
11	1.206859	67.227.186.229	192.168.1.117	TCP	66	80 → 5460 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=256
12	1.207144	192.168.1.117	67.227.186.229	TCP	54	5460 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
13	1.208128	192.168.1.117	67.227.186.229	TCP	1506	5460 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=1452 [TCP segment of a reassembled PDU]
14	1.208128	192.168.1.117	67.227.186.229	HTTP	130	POST /req1 HTTP/1.1
15	1.357034	139.226.86.156	192.168.1.117	BT-DHT	341	BitTorrent DHT Protocol reply=8 nodes
16	1.440196	192.168.1.117	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 17)
17	1.440820	192.168.1.1	192.168.1.117	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 16)
18	1.465442	67.227.186.229	192.168.1.117	TCP	60	80 → 5460 [ACK] Seq=1 Ack=1529 Win=32256 Len=0
19	1.501119	67.227.186.229	192.168.1.117	HTTP	344	HTTP/1.1 200 (text/plain)
20	1.550804	192.168.1.117	67.227.186.229	TCP	54	5460 → 80 [ACK] Seq=1529 Ack=291 Win=262400 Len=0
21	2.455658	192.168.1.117	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 22)
22	2.456642	192.168.1.1	192.168.1.117	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 21)

- **Display Filter** - icmp



- ความหมายของข้อมูล

Column	Description
No.	The frame number within the capture
Time	- Time from the beginning of the capture to the time when the packet was captured (seconds) - สามารถเปลี่ยนได้จาก View -> Time DIsplay Format
Source	Source address
Destination	Destination address
Protocol	Network Protocol
Info	Summary for this packet

- Save

Capture packet โดยใช้ Filter

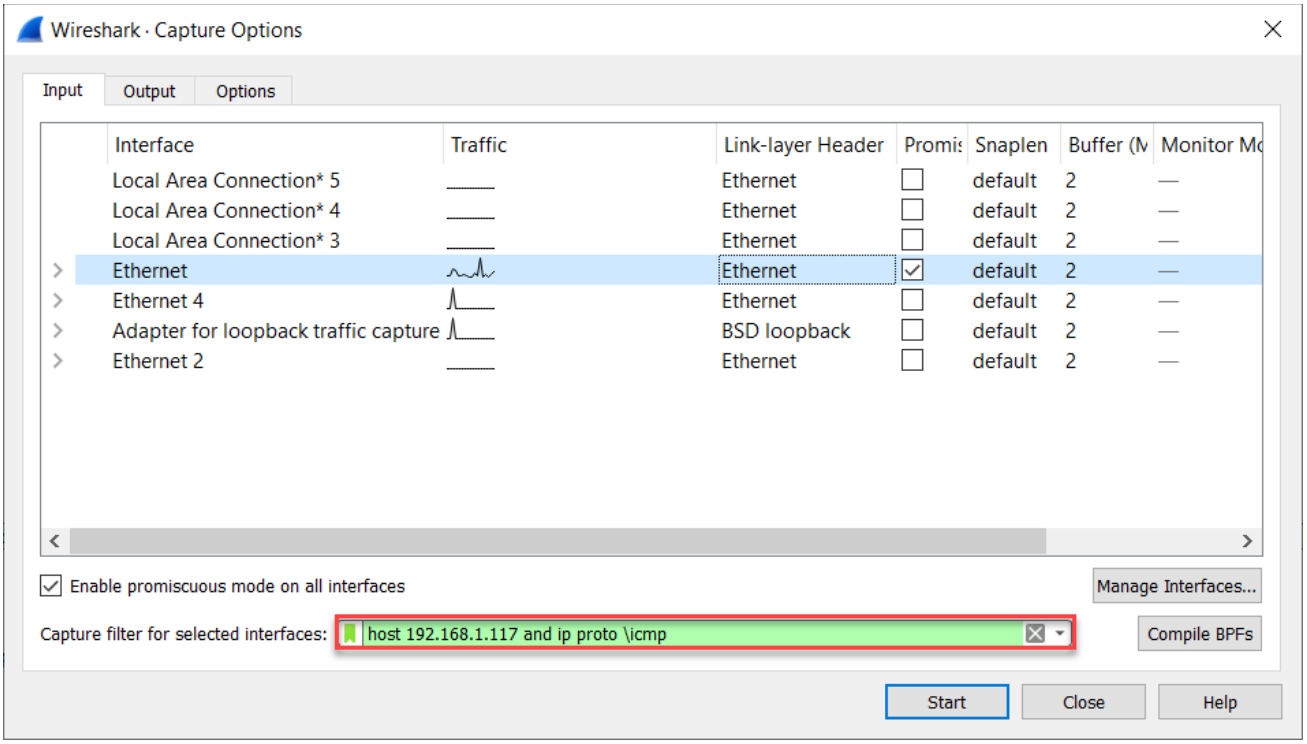
- Packet Filter

```
Capture > Options
```

- เปลี่ยน 192.168.1.117 เป็น ip ของ นศ

```
host 192.168.1.117 and ip proto \icmp
```

- สีพื้นหลังต้องเป็นสีเขียว



- เริ่มดักจับ Packet

```
Capture > Start (Ctrl+E)
```

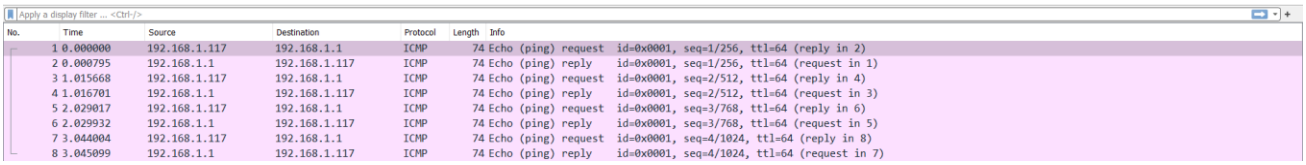
- เปลี่ยนเป็นเครื่อง Teacher

```
ping ?
```

- หยุดดักจับ Packet

```
Capture > Stop (Ctrl+E)
```

- Result



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.117	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 2)
2	0.000795	192.168.1.1	192.168.1.117	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1)
3	1.015668	192.168.1.117	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 4)
4	1.016701	192.168.1.1	192.168.1.117	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 3)
5	2.029017	192.168.1.117	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 6)
6	2.029932	192.168.1.1	192.168.1.117	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 5)
7	3.044004	192.168.1.117	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 8)
8	3.045099	192.168.1.1	192.168.1.117	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 7)

Filter options

- กรอง MAC address

```
ether [ src | dst ] host MAC
ether host 00:08:15:00:08:15
```

- กรอง Ethernet data type

```
ether proto [ \ip | \arp ]
ether proto \arp
```

- กรอง IP address

```
[ src | dst ] host IP
host 192.168.0.1
```

- กรอง TCP/IP protocol

```
ip proto [ \icmp | \tcp | \udp ]
ip proto \icmp
```

- กรอง Port

```
[ tcp | udp ] [ src | dst ] PORT
tcp port 80
```

- กรองโดยใช้ and, or, not

```
host 192.168.1.2 and (port 25 or port 110)
host 192.168.1.2 and not port 80
```