

Wireshark

แนะนำ

- 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

Installation

- Download

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

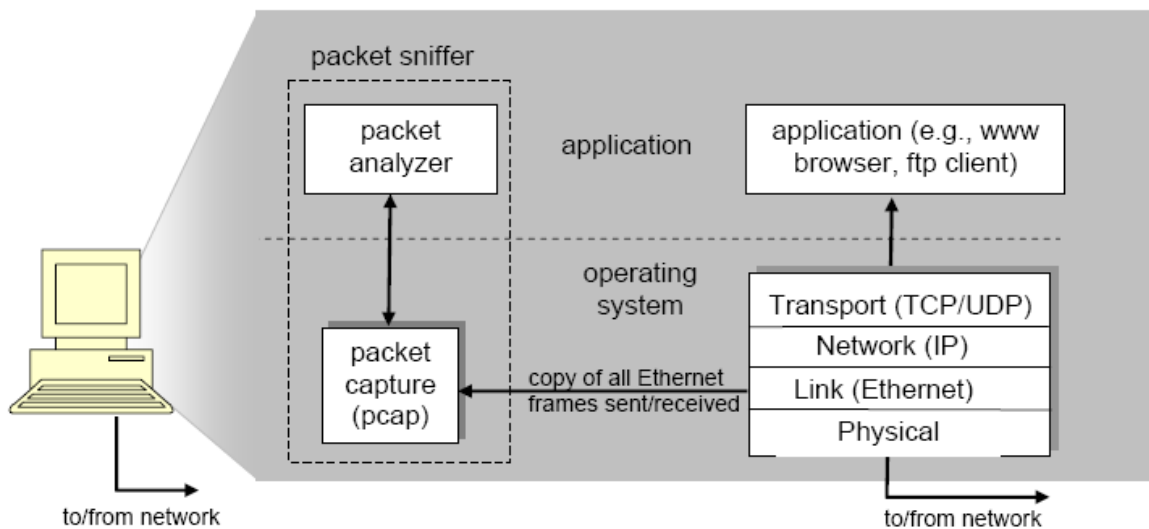
[Wireshark-4.2.7-x64.exe](#)

- Install

+ [Npcap](#)

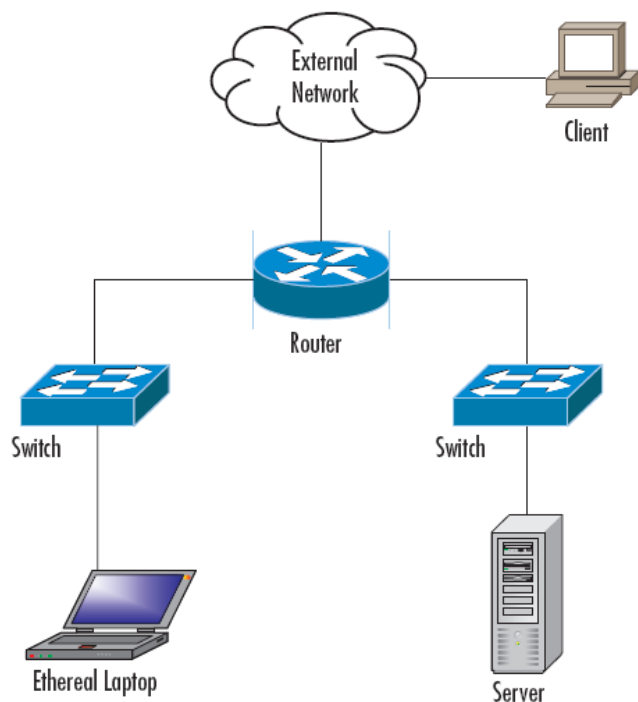
Packet Capture

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

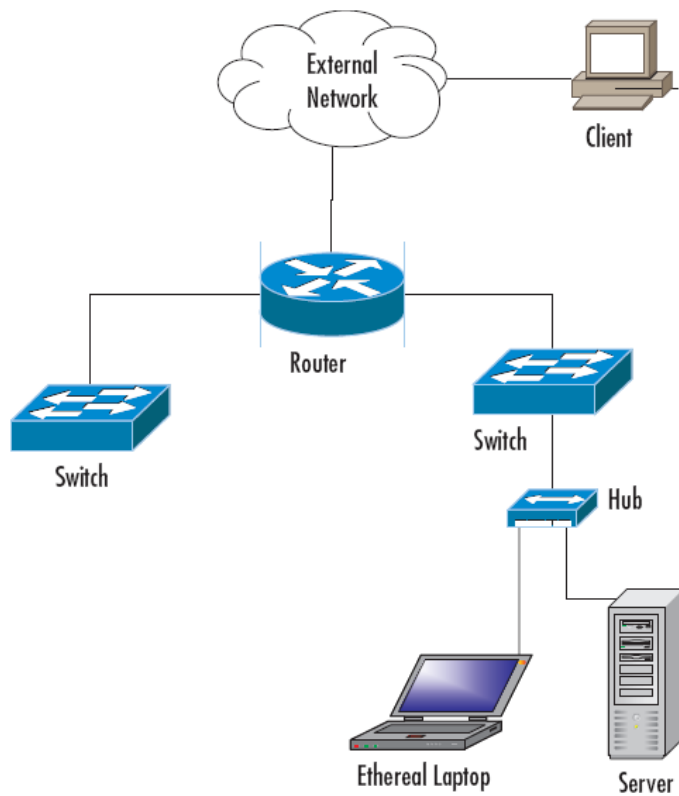


ตำแหน่งสำหรับ Capture packet

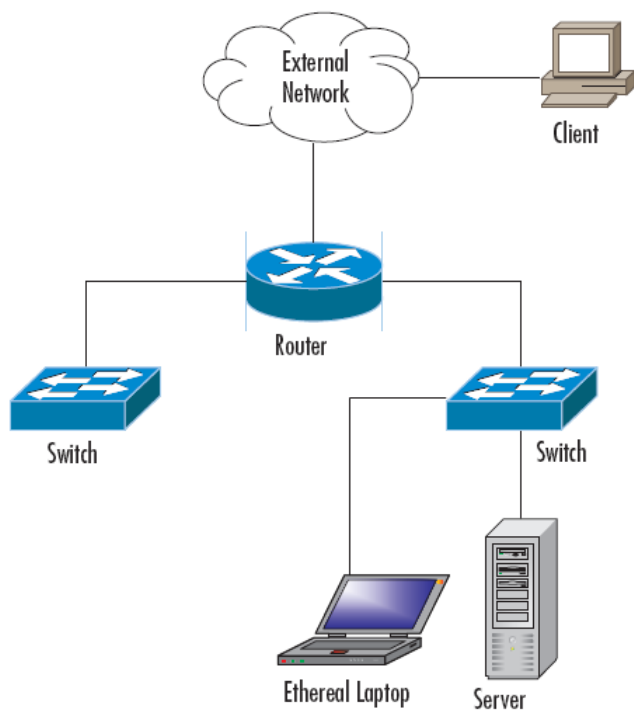
- ไม่สามารถ capture



- สามารถ capture โดยใช้ Hub

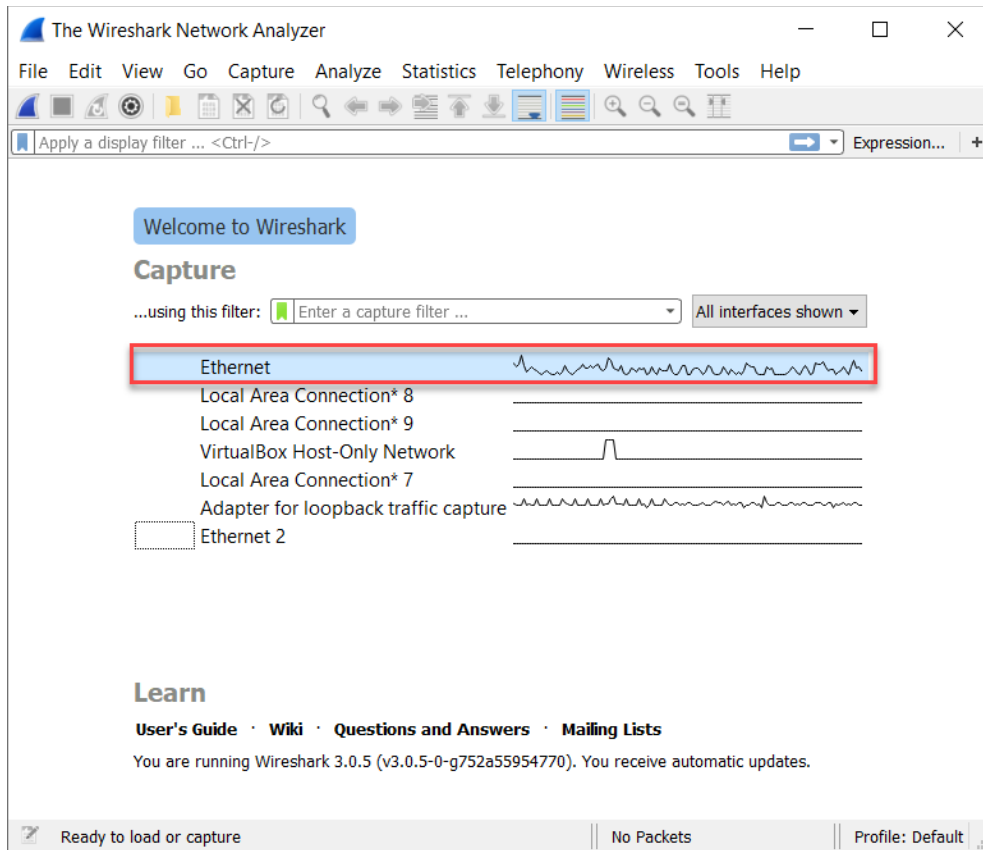


- สามารถ capture โดยใช้ Switch (Port Spanning)



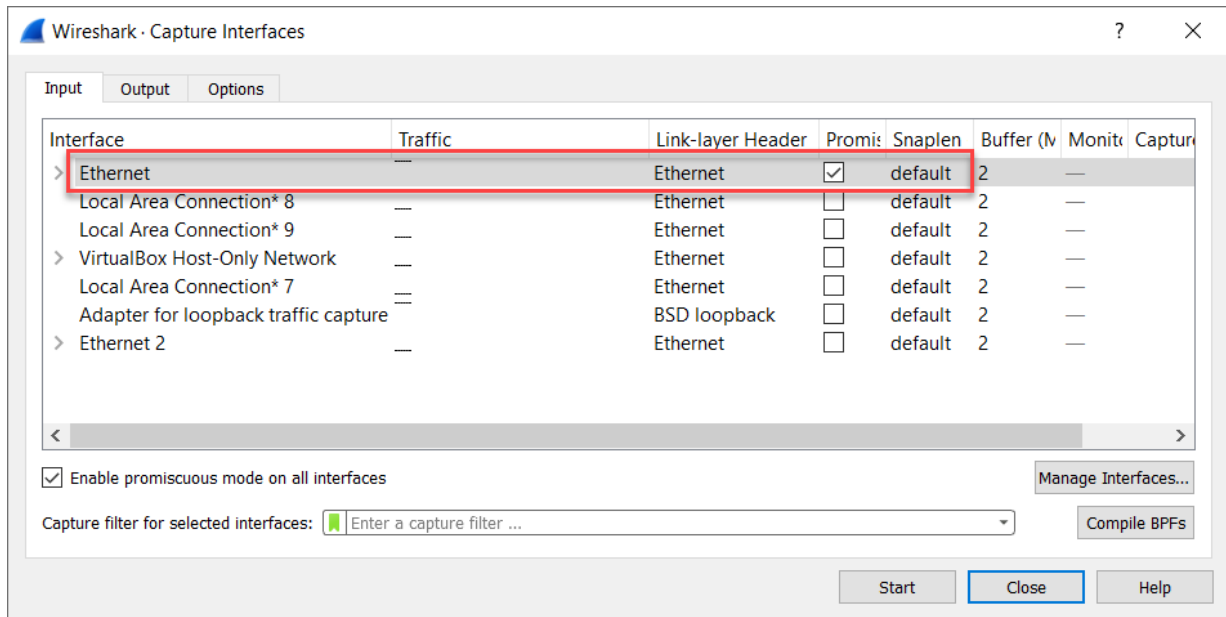
Capture packet

- เริ่ม Wireshark
- Network interface ซึ่งสามารถใช้ดักจับข้อมูล



- Select Network interface

Capture > Options



- เริ่มดักจับ Packet

Capture > Start (Ctrl+E)

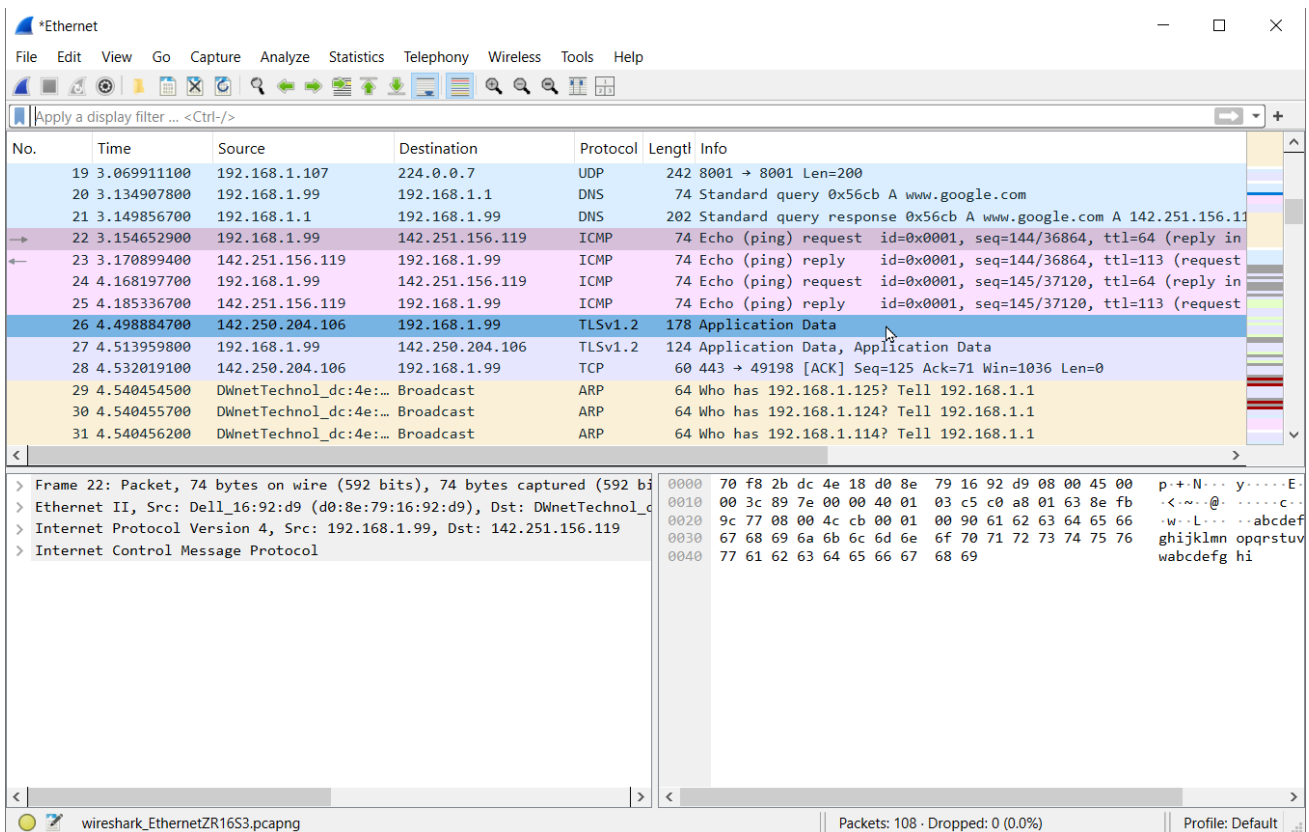
- ทดสอบ ping

ping www.google.com

- หยุดดักจับ Packet

Capture > Stop (Ctrl+E)

- ผลลัพธ์



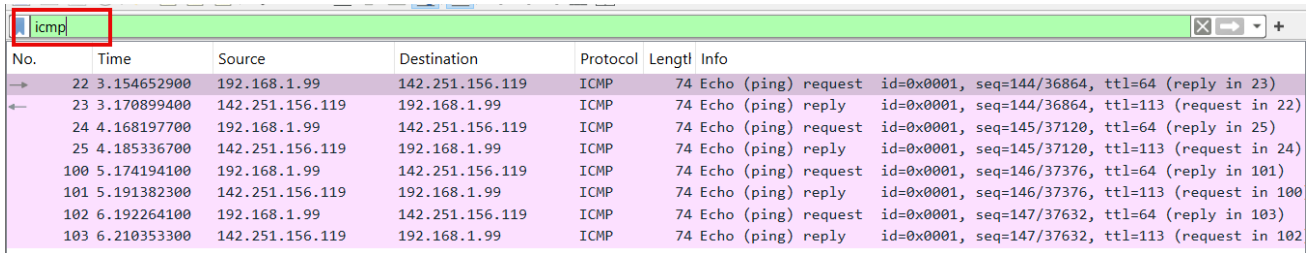
- บันทึก

- 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

Display Filter

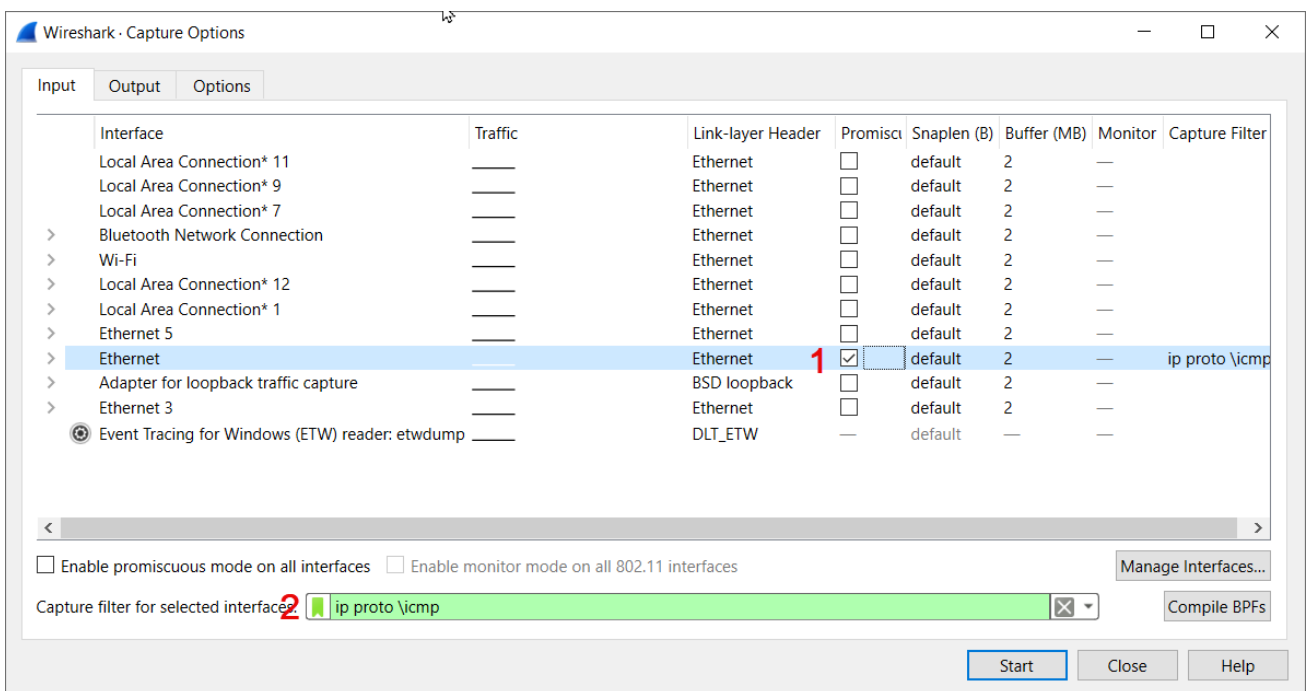
- แสดงเฉพาะ icmp



No.	Time	Source	Destination	Protocol	Length	Info
22	3.154652900	192.168.1.99	142.251.156.119	ICMP	74	Echo (ping) request id=0x0001, seq=144/36864, ttl=64 (reply in 23)
23	3.170899400	142.251.156.119	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=144/36864, ttl=113 (request in 22)
24	4.168197700	192.168.1.99	142.251.156.119	ICMP	74	Echo (ping) request id=0x0001, seq=145/37120, ttl=64 (reply in 25)
25	4.185336700	142.251.156.119	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=145/37120, ttl=113 (request in 24)
100	5.174194100	192.168.1.99	142.251.156.119	ICMP	74	Echo (ping) request id=0x0001, seq=146/37376, ttl=64 (reply in 101)
101	5.191382300	142.251.156.119	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=146/37376, ttl=113 (request in 100)
102	6.192264100	192.168.1.99	142.251.156.119	ICMP	74	Echo (ping) request id=0x0001, seq=147/37632, ttl=64 (reply in 103)
103	6.210353300	142.251.156.119	192.168.1.99	ICMP	74	Echo (ping) reply id=0x0001, seq=147/37632, ttl=113 (request in 102)

Capture Filter

- ดักจับเฉพาะ icmp



ตัวอย่าง Capture Filter

- 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
```