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`

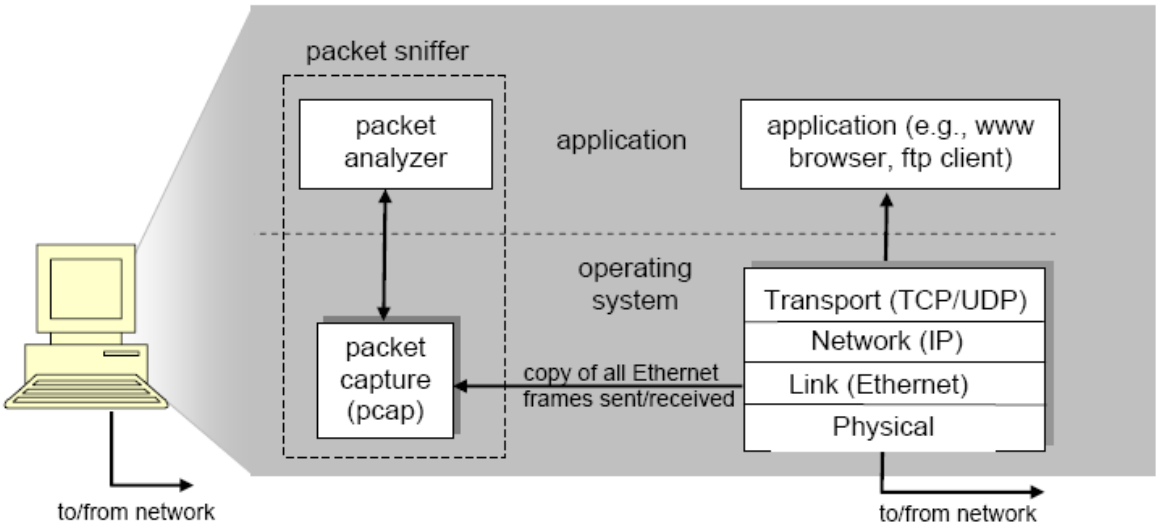
`Wireshark-4.2.7-x64.exe`

- Install

`+ Npcap`

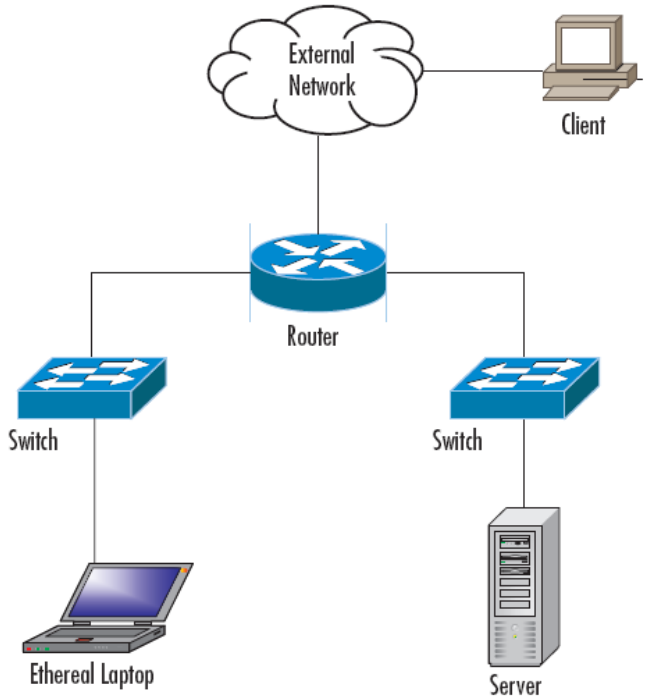
Packet Capture

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

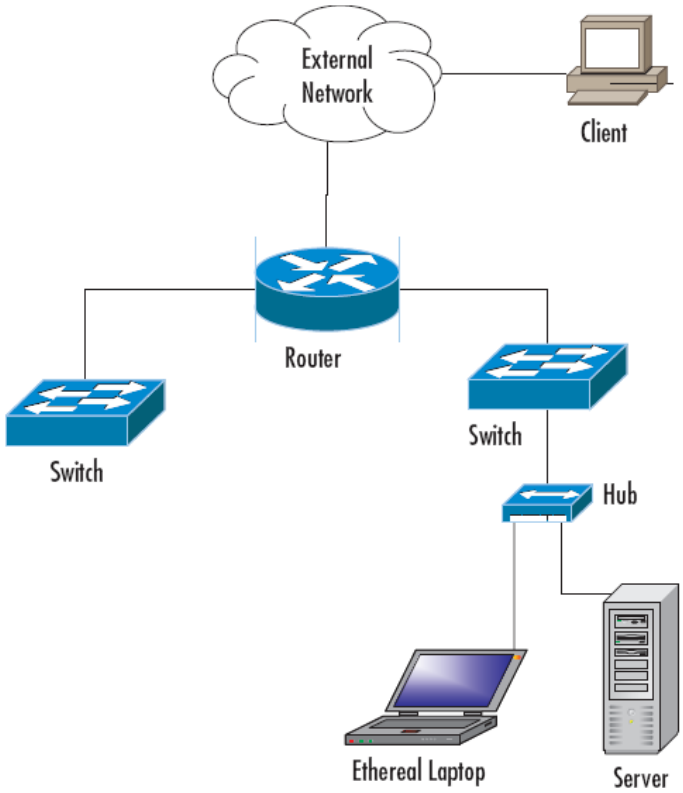


ตำแหน่งสำหรับ Capture packet

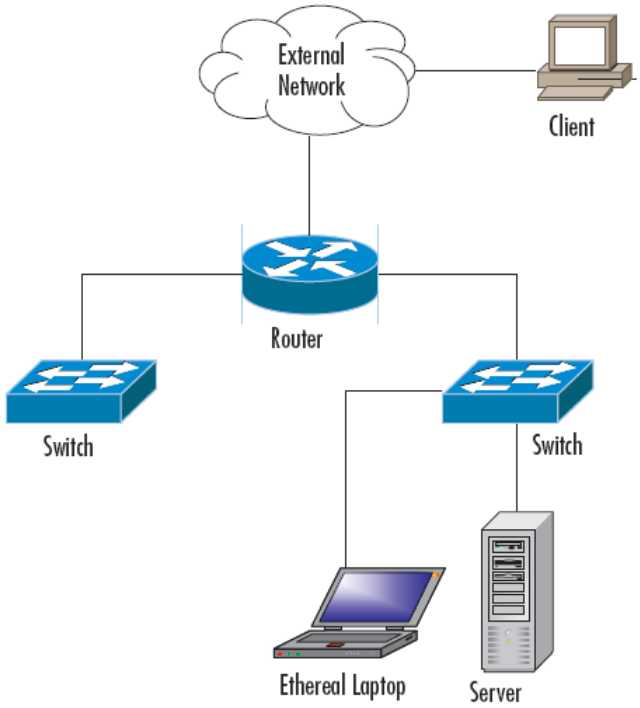
- ไม่สามารถ capture



- สามารถ capture โดยใช้ **Hub**

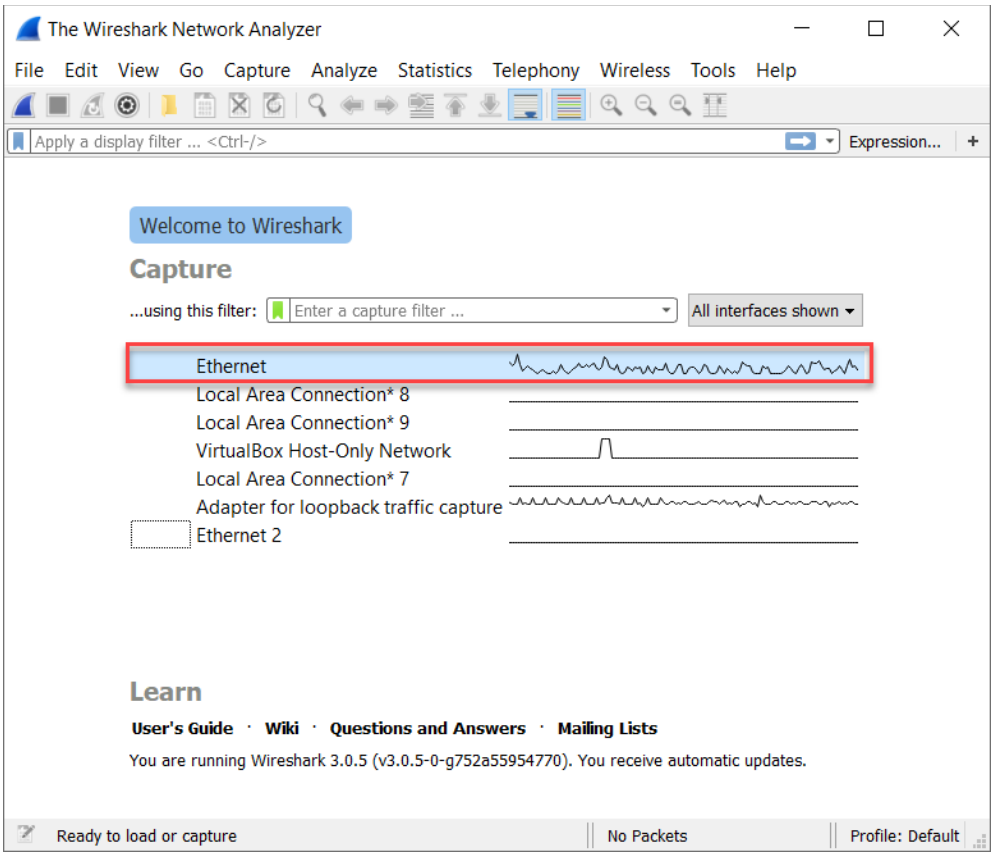


- สามารถ capture โดยใช้ **Swith (Port Spanning)**



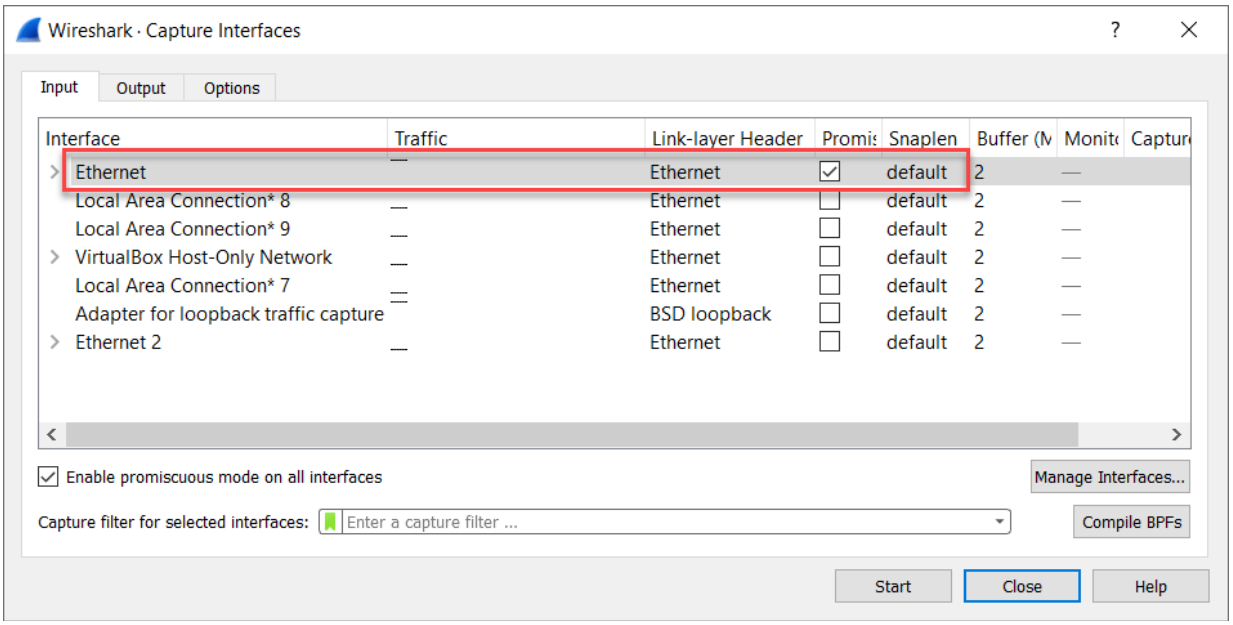
Capture packet

- เริ่ม Wireshark
- Network interface ซึ่งสามารถใช้ดักจับข้อมูล



- Select Network interface

```
Capture > Options
```



- เริ่มดักจับ Packet

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

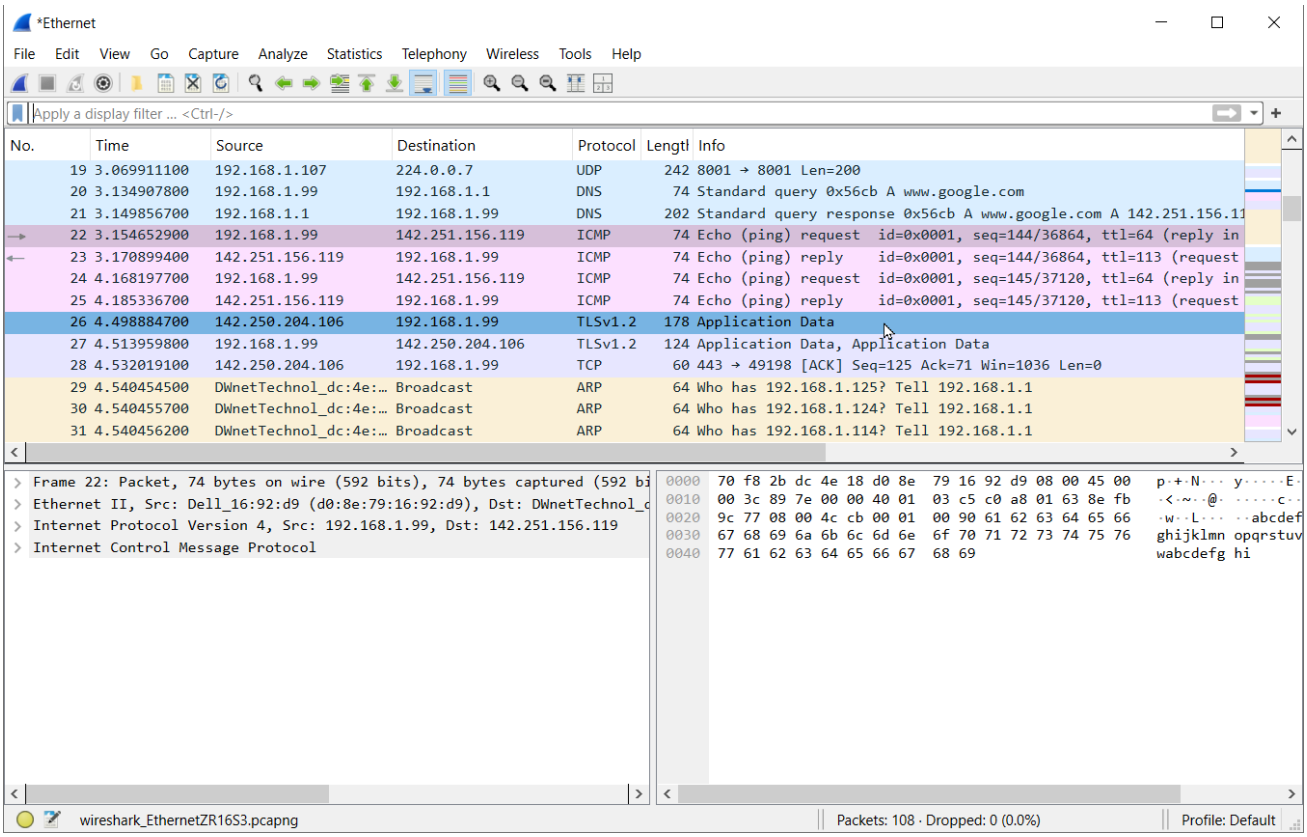
- ทดสอบ ping

```
ping www.google.com
```

- หยุดดักจับ Packet

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

- ผลลัพธ์



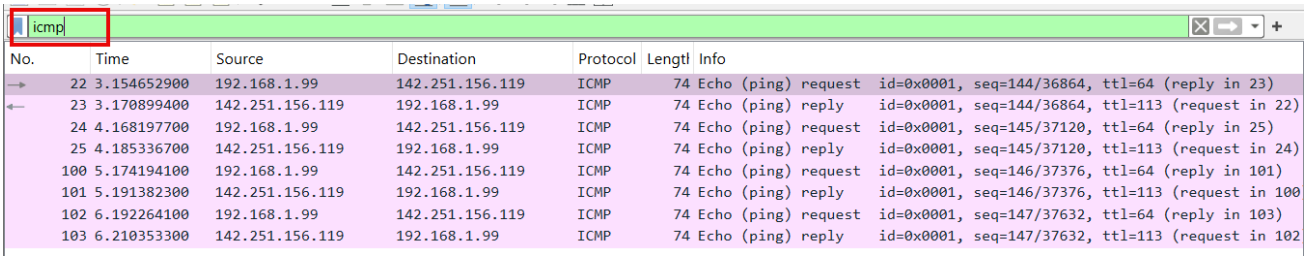
- บันทึก

- 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

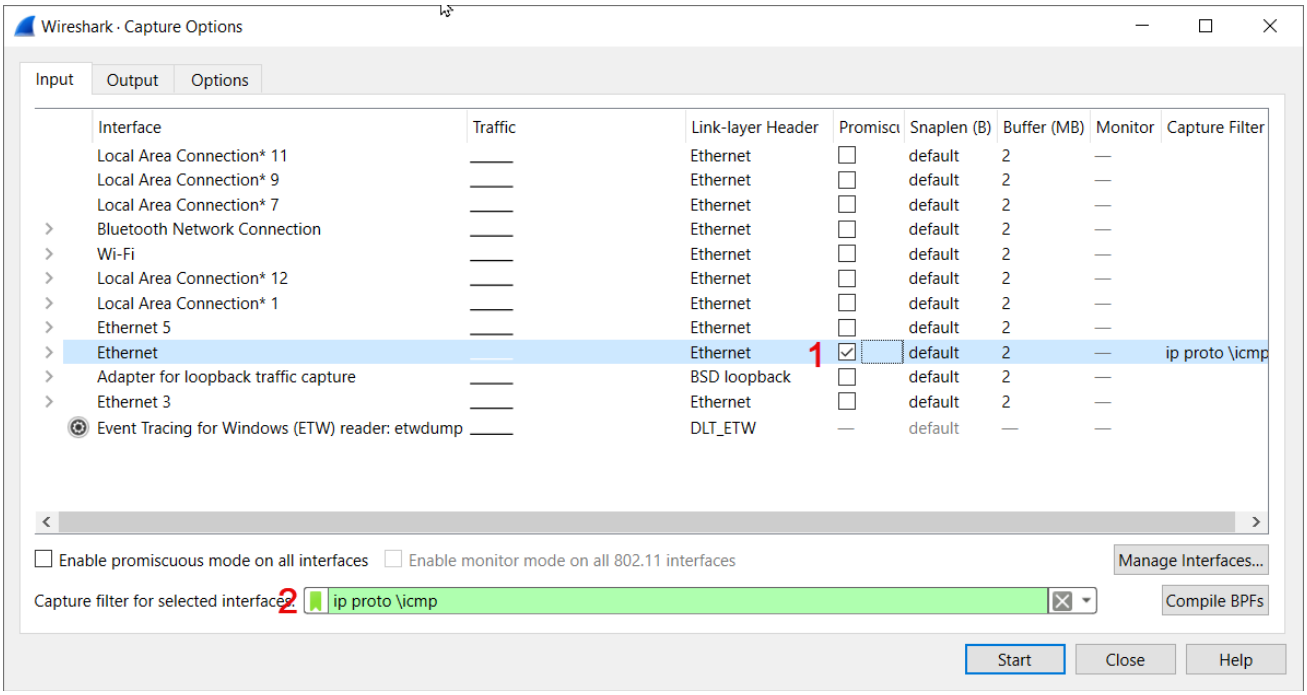
Display Filter

- แสดงเฉพาะ icmp



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
```