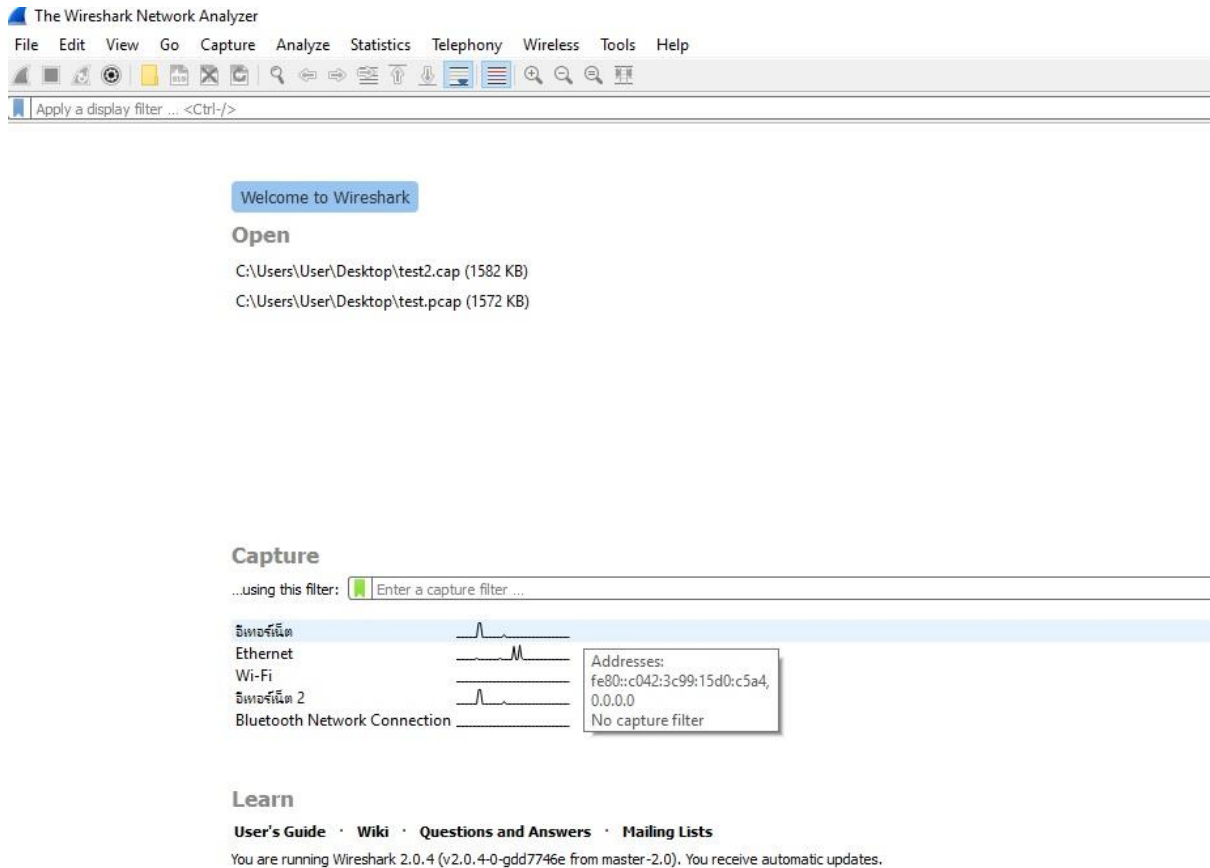


วิธีทำ recvpacket เอง

ก่อนอื่น โหลด wireshark มา <https://www.wireshark.org/download.html>

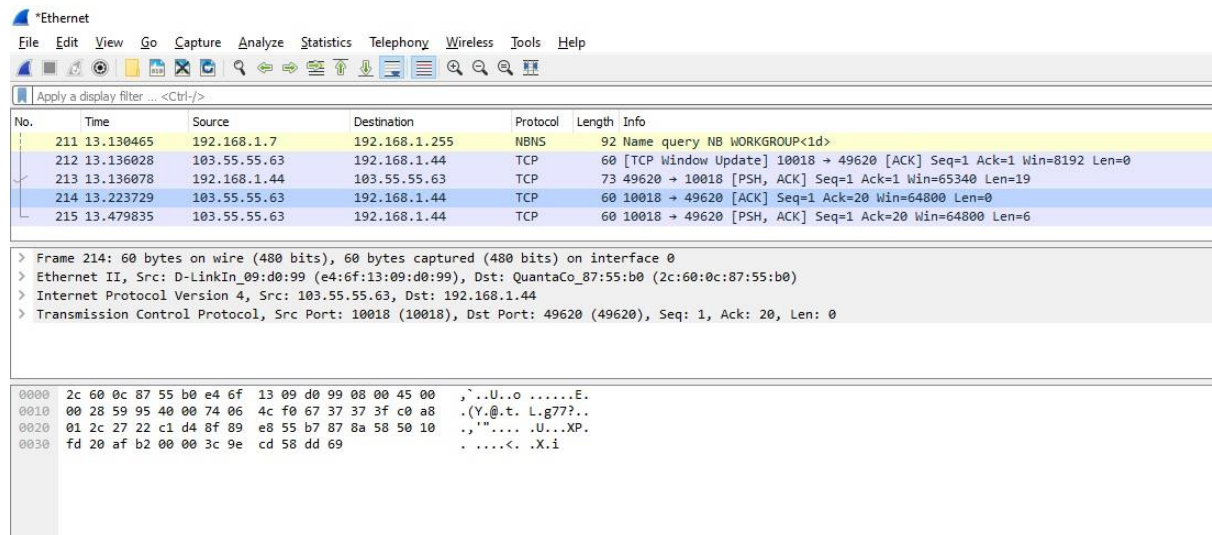
จะ 32 bit หรือ 64 bit ก็โหลดมาตามแต่ OS ของเราที่ลงไว้จนครบแล้วก็ลงให้เรียบร้อยอย่าลืม winpcap ด้วยไม่เช่นนั้น การ์ดแล่นไม่เจอ ต่อมาเปิด wireshark เลือกการ์ดแล่นที่เรามี



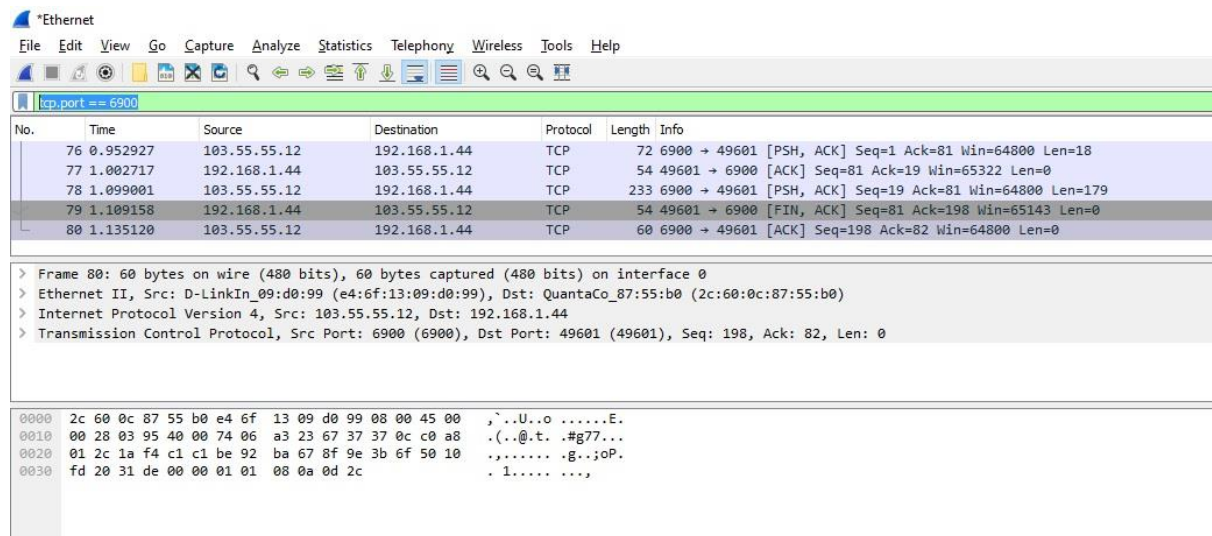
จากนั้น wireshark จะจับ packet ให้เราทันที

เปิด ragnarok แล้ว login ตามปกติ หรือดักจากช่วงไหนก็ได้ที่ต้องการ ลูก นั้ เเดน ยืน อะไรก็ได้

จากนั้นกลับมาที่ wireshark แล้วกดหยุด ปุ่มสี่เหลี่ยมซ้ายบนสีแดงครับ แล้วเราก็จะได้ packet มา



แล้วไปที่ช่อง filter ข้างล่างปุ่มหยุด ช่องที่เขียนว่า apply a display filter แล้วใส่คำว่า tcp.port == 6900 แล้วกด enter (กรณีนี้คือผมทำแค่ login นะครับ ส่วน map ต้อง apply เอาเอง)



เราจะได้ packet ทุกการเชื่อมต่อมาจากนั้นกดเลือกที่ packet ที่เราต้องการจะดูในที่นี่ผมขอเลือก packet ที่จะเลือก server นะครับ

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 6900

No.	Time	Source	Destination	Protocol	Length	Info
76	0.952927	103.55.55.12	192.168.1.44	TCP	72	6900 → 49601 [PSH, ACK] Seq=1 Ack=81 Win=64800 L
77	1.002717	192.168.1.44	103.55.55.12	TCP	54	49601 → 6900 [ACK] Seq=81 Ack=19 Win=65322 Len=0
78	1.099001	103.55.55.12	192.168.1.44	TCP	233	6900 → 49601 [PSH, ACK] Seq=19 Ack=81 Win=64800
79	1.109158	192.168.1.44	103.55.55.12	TCP	54	49601 → 6900 [FIN, ACK] Seq=81 Ack=198 Win=65143
80	1.135120	103.55.55.12	192.168.1.44	TCP	60	6900 → 49601 [ACK] Seq=198 Ack=82 Win=64800 Len=

> Frame 78: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface 0
 > Ethernet II, Src: D-LinkIn_09:d0:99 (e4:6f:13:09:d0:99), Dst: QuantaCo_87:55:b0 (2c:60:0c:87:55:b0)
 > Internet Protocol Version 4, Src: 103.55.55.12, Dst: 192.168.1.44
 > Transmission Control Protocol, Src Port: 6900 (6900), Dst Port: 49601 (49601), Seq: 19, Ack: 81, Len: 179
 > Data (179 bytes)

```

0000 2c 60 0c 87 55 b0 e4 6f 13 09 d0 99 08 00 45 00 ,..U..o .....E.
0010 00 db 03 93 40 00 74 06 a2 72 67 37 37 0c c0 a8 ....@.t. .rg77...
0020 01 2c 1a f4 c1 c1 be 92 b9 b4 8f 9e 3b 6e 50 18 ,..... ;nP.
0030 fd 20 09 be 00 00 76 02 b3 00 7d 1f 00 00 92 a2 . ....v. ..}.....
0040 06 00 01 00 00 00 00 00 00 00 1b 16 42 00 cf f7 ..... ..B...
0050 4b 29 38 f9 30 00 c8 92 2f 00 38 f9 30 00 c8 92 K)8.0... /.8.0...
0060 2f 00 00 00 00 64 00 00 00 67 37 37 3d 94 11 43 /....d.. .g77=..C
0070 68 61 6f 73 28 4e 65 77 29 00 00 00 00 00 00 00 haos(New ).....
0080 00 00 00 89 20 00 00 00 00 67 37 37 33 94 11 4f .... . .g773..0
0090 64 69 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 din.....
00a0 00 00 00 68 25 00 00 00 00 67 37 37 29 94 11 4c ...h%... .g77)..L
00b0 6f 6b 69 00 00 00 00 00 00 00 00 00 00 00 00 00 oki.....
00c0 00 00 00 95 39 00 00 00 00 67 37 37 1f 94 11 54 ....9... .g77...T
00d0 68 6f 72 00 00 00 00 00 00 00 00 00 00 00 00 00 hor.....
00e0 00 00 00 3d 3d 00 00 00 00 00 00 00 00 00 00 00 ...==...
  
```

สังเกตที่ช่องกลาง คำว่า data มันเขียนว่า Data (179 bytes)

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 6900

No.	Time	Source	Destination	Protocol	Length	Info
76	0.952927	103.55.55.12	192.168.1.44	TCP	72	6900 → 49601 [PSH, ACK] Seq=1 Ack=81 W
77	1.002717	192.168.1.44	103.55.55.12	TCP	54	49601 → 6900 [ACK] Seq=81 Ack=19 Win=6
78	1.099001	103.55.55.12	192.168.1.44	TCP	233	6900 → 49601 [PSH, ACK] Seq=19 Ack=81
79	1.109158	192.168.1.44	103.55.55.12	TCP	54	49601 → 6900 [FIN, ACK] Seq=81 Ack=198
80	1.135120	103.55.55.12	192.168.1.44	TCP	60	6900 → 49601 [ACK] Seq=198 Ack=82 Win=

> Frame 78: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface 0
 > Ethernet II, Src: D-LinkIn_09:d0:99 (e4:6f:13:09:d0:99), Dst: QuantaCo_87:55:b0 (2c:60:0c:87:55:b0)
 > Internet Protocol Version 4, Src: 103.55.55.12, Dst: 192.168.1.44
 > Transmission Control Protocol, Src Port: 6900 (6900), Dst Port: 49601 (49601), Seq: 19, Ack: 81, Len: 179
 > Data (179 bytes)

```

0000 2c 60 0c 87 55 b0 e4 6f 13 09 d0 99 08 00 45 00 ,..U..o .....E.
0010 00 db 03 93 40 00 74 06 a2 72 67 37 37 0c c0 a8 ....@.t. .rg77...
0020 01 2c 1a f4 c1 c1 be 92 b9 b4 8f 9e 3b 6e 50 18 ,..... ;nP.
0030 fd 20 09 be 00 00 76 02 b3 00 7d 1f 00 00 92 a2 . ....v. ..}.....
0040 06 00 01 00 00 00 00 00 00 00 1b 16 42 00 cf f7 ..... ..B...
0050 4b 29 38 f9 30 00 c8 92 2f 00 38 f9 30 00 c8 92 K)8.0... /.8.0...
0060 2f 00 00 00 00 64 00 00 00 67 37 37 3d 94 11 43 /....d.. .g77=..C
0070 68 61 6f 73 28 4e 65 77 29 00 00 00 00 00 00 00 haos(New ).....
0080 00 00 00 89 20 00 00 00 00 67 37 37 33 94 11 4f .... . .g773..0
0090 64 69 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 din.....
00a0 00 00 00 68 25 00 00 00 00 67 37 37 29 94 11 4c ...h%... .g77)..L
00b0 6f 6b 69 00 00 00 00 00 00 00 00 00 00 00 00 00 oki.....
00c0 00 00 00 95 39 00 00 00 00 67 37 37 1f 94 11 54 ....9... .g77...T
00d0 68 6f 72 00 00 00 00 00 00 00 00 00 00 00 00 00 hor.....
00e0 00 00 00 3d 3d 00 00 00 00 00 00 00 00 00 00 00 ...==...
  
```

นั่นแหละครับ ขนาด packet หรือ packet length เราก็เอาไปใส่ใน recvpacket ได้เลย ส่วนหัว packet ให้เราใส่ 2 บิตแรกหรือ 4 ตัวอักษรแรกเท่านั้น hilight ไว้ เช่นตัวนี้ 7602 แต่เวลาใส่จริงจะเป็น 0276 179

ป.ล. เสริมอีกนิดนึง ตัวอย่าง packet นี้

```
76 02 b3 00 7d 1f 00 00 92 a2 06 00 01 00 00 00
00 00 00 00 1b 16 42 00 cf f7 4b 29 38 f9 30 00
c8 92 2f 00 38 f9 30 00 c8 92 2f 00 00 00 00
```

IP = 67 37 37 3d

Port = 94 11

Server name = 43 68 61 6f 73 28 4e 65 77 29 00 00 00 00 00 00 00 00 00 00

User in game = 89 20 00 00 00 00

ตัวเลขทั้งหมดนี้สามารถเอาไปแปลงใน calculator ใน windows ได้เลยนะครับ เช่น Port 94 11 ตัวนี้ต้องกลับบิตด้วยนะครับจะกลายเป็น 4500

หรือ IP ตัวนี้แปลงตรงๆเลยครับเช่น 67 = 100 37 = 55 37 = 55 3d = 61 รวมกันก็จะกลายเป็น Chaos IP 103.55.55.61 port 4500



```
67 37 37 33 94 11 4f 64 69 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 68 25 00 00 00 00
67 37 37 29 94 11 4c 6f 6b 69 00 00 00 00 00 00 00 00 00 00 00 00 00 95 39 00 00 00 00
67 37 37 1f 94 11 54 68 6f 72 00 00 00 00 00 00 00 00 00 00 00 00 00 3d 3d 00 00 00 00
```

ชุดที่เหลือลองฝึกแปลงกันดูนะครับ