ปฏิบัติการโปรแกรมดักจับข้อมูล ครั้งที่ 2

เรื่อง การคัดเลือกเฉพาะข้อมูลที่สนใจจากโปรแกรม Wireshark

สิ่งที่ควรทราบ

1. IP Address ของเครื่องที่ใช้โปรแกรม Wireshark คือ

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : D4-6D-6D-F4-A5-97
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:fb1:17f:a9d5:89da:dff3:1529:4d9a(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:fb1:17f:a9d5:89dc:f06e:d64d:159b(Preferred)
   Link-local IPv6 Address . . . . . : fe80::89da:dff3:1529:4d9a%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.38(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 26 สิ งหาคม 2565 17:41:56
   Lease Expires . . . . . . . . . . : 27 สิ งหาคม 2565 17:41:56
   Default Gateway . . . . . . . . . : fe80::1%14
                                       192.168.1.1
```

2. IP Address ของ www.thairath.co.th คือ

```
C:\Users\ASAS>nslookup www.thairath.co.th
Server:  dnscon1.v6.trueinternet.co.th
Address:  2001:fb0:100::207:29

Non-authoritative answer:
Name:    thairath-www.cdn.byteark.com
Addresses:  2001:fb0:109f:15::7
          2001:fb0:109f:8011::68
          2001:fb0:109f:15::6
          2001:fb0:109f:8011::67
          2001:fb0:109f:15::8
          2001:fb0:109f:8011::66
          61.91.192.7
          61.91.193.67
          61.91.193.66
          61.91.192.6
          61.91.192.8
          61.91.193.68
Aliases:  www.thairath.co.th

C:\Users\ASAS>
```

สรุปการใช้งานดังต่อไปนี้

1. อธิบายการใช้expression ใน Filter toolbar ที่ให้เป็นตัวอย่างในการ Filter แล้วได้ผลลัพธ์อย่างไรออกมา พร้อมทั้งจับภาพหน้าจอ

E.g.1 *ip.src == 192.168.1.38* ความหมายคือ เราต้องการหา Packet ที่ส่งไปยัง Source ที่ตำแหน่ง IP ที่เราต้องการ เช่น 192.168.1.38

ip.src==192.168.1.38

No.	Time	Source	Destination	Protocol	Length	Info
588	6.712506	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=72254 Win=132096
591	6.717328	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=75158 Win=132096
595	6.717697	192.168.1.38	171.102.241.95	TCP	66	50245 → 443 [ACK] Seq=3141 Ack=78062 Win=132096
596	6.717713	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=88226 Win=132096
605	6.718588	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=95486 Win=132096
607	6.719501	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=108554 Win=13209
609	6.720182	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=111458 Win=13209
612	6.720524	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=121622 Win=13209
614	6.721143	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=124526 Win=13209
617	6.721406	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=135281 Win=13209
619	6.721885	192.168.1.38	171.102.241.95	TCP	54	50245 → 443 [ACK] Seq=3141 Ack=136718 Win=13056
622	6.722785	192.168.1.38	104.19.135.78	TCP	54	50244 → 443 [ACK] Seq=518 Ack=2116 Win=131584 L
624	6.726310	192.168.1.38	104.19.135.78	TLSv1.3	118	Change Cipher Spec, Application Data
630	6.743501	192.168.1.38	104.19.136.78	QUIC	87	Protected Payload (KP0), DCID=01fc0a5292a78e694
631	6.743573	192.168.1.38	104.19.136.78	QUIC	89	Protected Payload (KP0), DCID=01fc0a5292a78e694

E.g.2 *ip.addr == 192.168.1.38* ความหมายคือ เราต้องการหา Packet ที่มีความเกี่ยวข้องกับ IP ที่เราต้องการทั้งหมด ไม่ว่าจะเป็น Source หรือ Destination

ip.addr==192.168.1.38

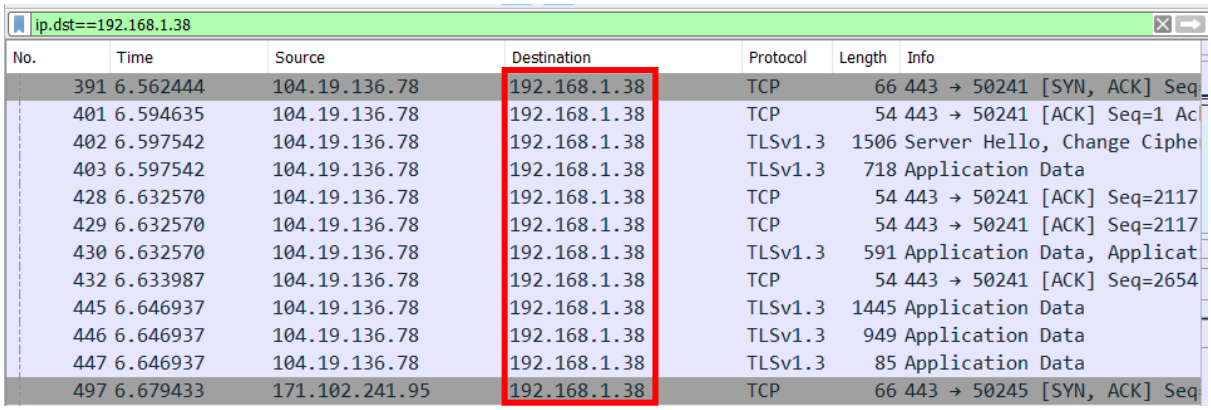
No.	Time	Source	Destination	Protocol	Length	Info
57	2.333519	192.168.1.38	185.184.10.30	TCP	55	50015 → 443 [ACK] Seq=1 Ack=1 Win
58	2.575217	185.184.10.30	192.168.1.38	TCP	54	443 → 50015 [ACK] Seq=1 Ack=2 Win
145	6.317343	192.168.1.38	18.140.108.173	TLSv1.2	1257	Application Data
146	6.317421	192.168.1.38	18.140.108.173	TLSv1.2	100	Application Data
174	6.341022	192.168.1.38	18.140.108.173	TLSv1.2	917	Application Data
183	6.352608	18.140.108.173	192.168.1.38	TCP	54	443 → 50220 [ACK] Seq=1 Ack=1250
184	6.352608	18.140.108.173	192.168.1.38	TLSv1.2	100	Application Data
186	6.355359	18.140.108.173	192.168.1.38	TLSv1.2	670	Application Data
187	6.355359	18.140.108.173	192.168.1.38	TLSv1.2	92	Application Data
188	6.355393	192.168.1.38	18.140.108.173	TCP	54	50220 → 443 [ACK] Seq=2113 Ack=70
189	6.355878	192.168.1.38	18.140.108.173	TLSv1.2	96	Application Data
223	6.386640	18.140.108.173	192.168.1.38	TCP	54	443 → 50220 [ACK] Seq=701 Ack=215
230	6.398247	18.140.108.173	192.168.1.38	TLSv1.2	670	Application Data
231	6.398247	18.140.108.173	192.168.1.38	TLSv1.2	92	Application Data
232	6.398264	192.168.1.38	18.140.108.173	TCP	54	50220 → 443 [ACK] Seq=2155 Ack=13

E.g.3 *!(ip.addr==192.168.1.38)* ความหมายคือ เราจะกรองเอา Packet ที่ไม่ได้เกี่ยวข้องกับ IP Address ที่กรอง/ตั้งไว้

!(ip.addr==192.168.1.38)

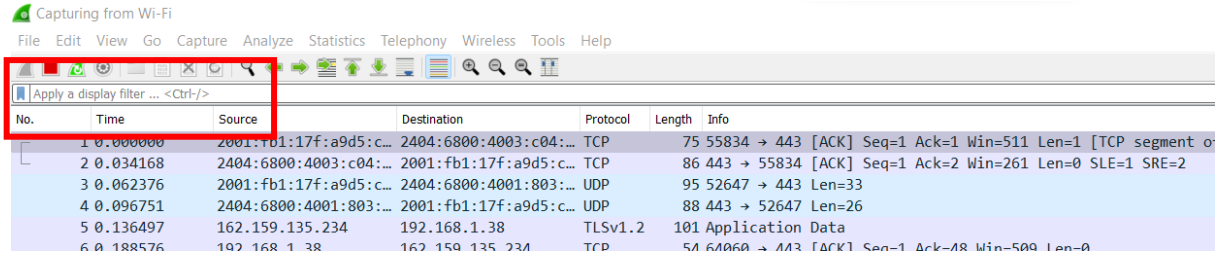
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a02:6ea0:d100::12	2001:fb1:17f:a9d5:c…	TLSv1.2	113	Application Data
2	0.000000	2a02:6ea0:d100::12	2001:fb1:17f:a9d5:c…	TLSv1.2	98	Application Data
3	0.000000	2a02:6ea0:d100::12	2001:fb1:17f:a9d5:c…	TCP	74	443 → 50187 [FIN, ACK] Seq=64
4	0.000060	2001:fb1:17f:a9d5:c…	2a02:6ea0:d100::12	TCP	74	50187 → 443 [ACK] Seq=1 Ack=65
5	0.607401	2001:fb1:17f:a9d5:c…	2001:fb0:109f:8011:…	TLSv1.2	334	Application Data
6	0.613793	2001:fb0:109f:8011:…	2001:fb1:17f:a9d5:c…	TCP	74	443 → 50175 [ACK] Seq=1 Ack=26
7	0.614291	2001:fb0:109f:8011:…	2001:fb1:17f:a9d5:c…	TCP	2938	443 → 50175 [ACK] Seq=1 Ack=26
8	0.614314	2001:fb1:17f:a9d5:c…	2001:fb0:109f:8011:…	TCP	74	50175 → 443 [ACK] Seq=261 Ack=
9	0.614849	2001:fb0:109f:8011:…	2001:fb1:17f:a9d5:c…	TCP	2938	443 → 50175 [ACK] Seq=2865 Ack
10	0.614868	2001:fb1:17f:a9d5:c…	2001:fb0:109f:8011:…	TCP	74	50175 → 443 [ACK] Seq=261 Ack=

E.g.4 *ip.dst==192.168.1.38* ความหมายคือ กรองเอาเฉพาะ Packet ที่ส่งมายัง IP address (Destination) ที่เรากรองไว้

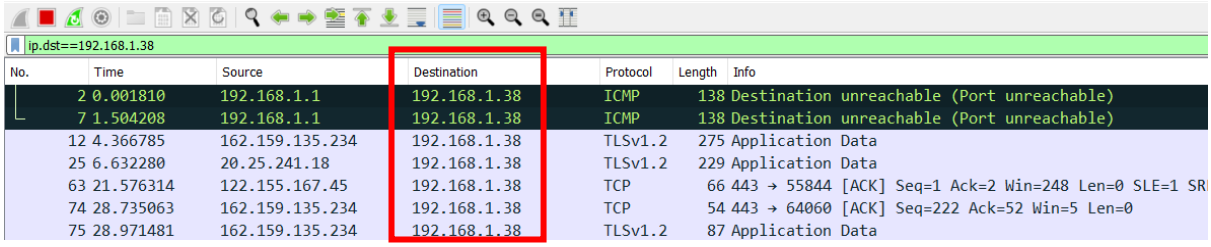


2. การแตกต่างระหว่าง Filter display และ Capture filter อย่างไร และสามารถนำไปใช้งานได้อย่างไร ในแต่ละแบบ

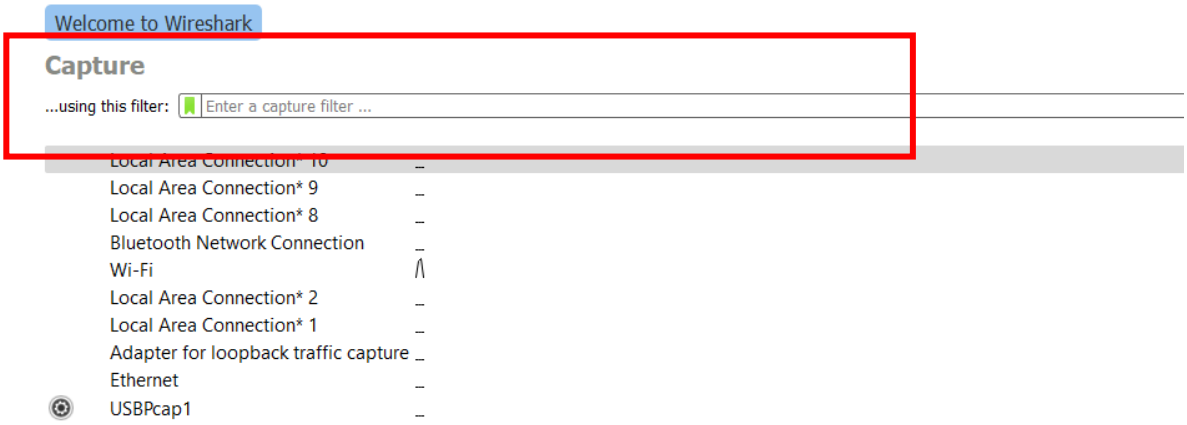
- *Filter Display* -> จะแสดงอยู่ในหน้าการตรวจจับ packet เราสามารถกรองสิ่งที่เราต้องการได้โดยพิมพ์ที่ช่องว่างดังที่แสดง



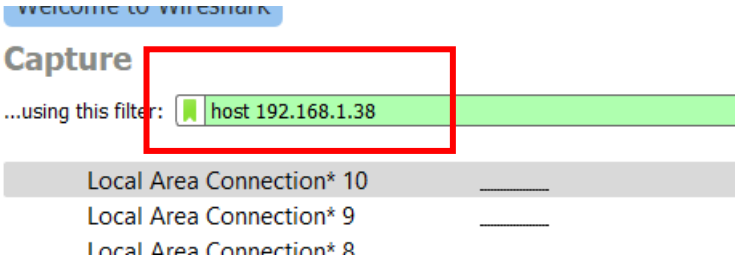
ทั้งนี้หน้า Capture หรือ หน้าจะตรวจจับจะแสดงทุกอย่างที่เราได้กระทำ ทุก Packet ที่ได้รับหรือส่ง ทุก Protocols ไม่ได้แสดงเฉพาะ เหมือนกับ Capture filter ซึ่งเราสามารถเลือกได้ว่าต้องการกรองอะไร หรือกรองเฉพาะอะไรได้ ไม่เหมือนกับ Capture filter ที่จะแสดงเฉพาะสิ่งเราต้องการเท่านั้น หากเราต้องการกรองอย่างอื่นต้องเริ่มทำการตรวจจับใหม่นั่นเอง



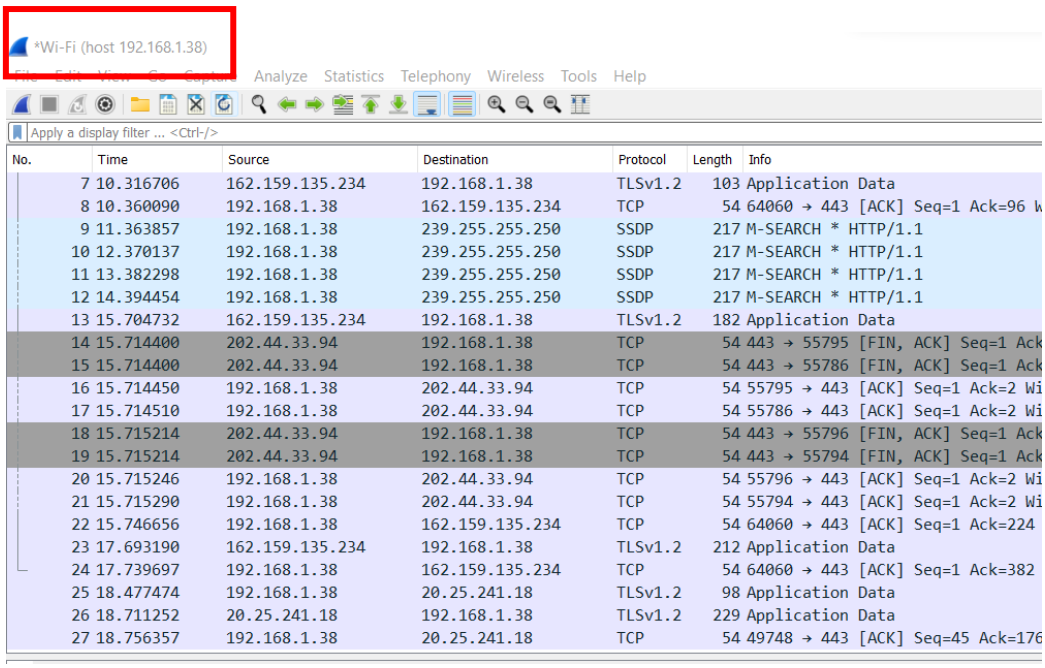
- *Capture filter* -> จะกรองเฉพาะสิ่งที่เรากำหนดไว้ตั้งแต่ต้นที่เริ่มโปรแกรม โดยตัว Capture filter จะอยู่ที่หน้าโปรแกรมตั้งแต่เปิด ดังที่แสดง



ตัวอย่าง เช่น เราต้องการให้แสดงเฉพาะ Packet ที่เกี่ยวข้องกับ Host IP เท่านั้น



หลังจากเราเข้ามาที่หน้า capture แล้วจะเห็นว่า ทุกๆ Packet จะเกี่ยวข้องกับ IP Address 192.168.1.38 ไม่ว่าจะเป็น Source หรือ Destination



3. ข้อดี ข้อเสียในแต่ละแบบของการ Filter display และ Capture filter

Filter display

ข้อดี

- เราสามารถกรอง Packet ใหม่ได้โดยไม่ต้องทำการ Capture Packets ใหม่ (ปิด-เปิดใหม่) เนื่องจากเราไม่ได้ทำการกรองให้แสดงเฉพาะตั้งแต่ต้น ทำให้หน้าแสดง Packet เต็มไปด้วย Packet มากมาย หลากหลาย

- เราสามารถระบุข้อมูลมากกว่า 1 ได้เพื่อกรองเอาเฉพาะ Packet ได้ ถ้าให้กล่าวเข้าใจง่ายๆคือ เราสามารถบอกกับแม่ค้าขายข้าวได้ว่า ต้องการกินผัดกะเพรา ที่ใส่ กะเพราเยอะๆ ใส่กระเทียมเยอะๆ ไม่เผ็ดมาก ก็คือการเพิ่มข้อมูลสิ่งที่เราต้องการตรวจจับให้กับโปรแกรมที่ทำการกรอง เพื่อเพิ่มรายละเอียดในการค้นหามากขึ้น

ข้อเสีย

- การค้นหาเฉพาะ Packet ยากมาก เพราะ หน้าแสดง Packet มา Packet มากมาย หลายหลายตามที่อธิบายไว้ข้างต้น ทำให้เราต้องเพิ่มรายละเอียดในการค้นหาเข้าไปอีกขั้นหนึ่ง สำหรับมือใหม่ที่ต้องการหา Packet หนึ่งๆ เป็นไปได้ยากมาก เช่น เราต้องการหา กะเพรา บางทีเรากรองไป เราอาจจะเจอ กะเพราหมูกรอบ กะเพราไก่ กระเพราเนื้อ หรือ ใบกระเพรา ก็ได้ เราต้องเพิ่มรายละเอียดมากขึ้น

Capture filter

ข้อดี

- เราสามารถตั้งค่าให้แสดงเฉพาะรายะเอียดที่เราต้องการเฉพาะได้ โดยจะไม่มีนอกเหนือสิ่งที่เราต้องการเลยในหน้าแสดงPacket

- การแสดงผลในการตรวจจับไว เนื่องจากเราได้กรองเฉพาะ Packet ที่เราสนใจไว้แล้วนั่นเอง

ข้อเสีย

- เนื่องจากเราได้กำหนดค่าที่ต้องการให้แสดงเฉพาะไว้ตั้งแต่หน้าแรกของโปรแกรมแล้ว หากเราต้องการเปลี่ยนค่าที่ต้องการตรวจจับ Packet หรือเปลี่ยน Packet ที่เราต้องการ จำเป็นต้องไปตั้งค่าใหม่ที่หน้าแรกของโปรแกรม หรือ ปิด-เปิดโปรแกรมใหม่นั่นเอง