

## 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:df3:1529:4d9a(Preferred)
Temporary IPv6 Address. . . . . : 2001:fb1:17f:a9d5:89dc:f06e:d64d:159b(Preferred)
Link-local IPv6 Address . . . . . : fe80::89da:df3:1529:4d9a%14(Preferred)
IPv4 Address. . . . . : 192.168.1.38(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 26 สิงหาคม 2565 17:41:56
Lease Expires . . . . . : 27 สิงหาคม 2565 17:41:56
Default Gateway . . . . . : fe80::1%14
                             192.168.1.1
```

2. IP Address ของ [www.thairath.co.th](http://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. อธิบายการใช้ expression ใน Filter toolbar ที่ให้เป็นตัวอย่างในการ Filter แล้วได้ผลลัพธ์อย่างไรออกมา พร้อมทั้งจับภาพหน้าจอ

E.g.1 **ip.src == 192.168.1.38** หมายความว่า เราต้องการหา Packet ที่ส่งไปยัง Source ที่ตำแหน่ง IP ที่เราต้องการ เช่น 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** หมายความว่า เราต้องการหา Packet ที่มีความเกี่ยวข้องกับ IP ที่เราต้องการทั้งหมด ไม่ว่าจะเป็น Source หรือ Destination

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)** หมายความว่า เราจะกรองเอา Packet ที่ไม่ได้เกี่ยวข้องกับ IP Address ที่กรอง/ตั้งไว้

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** หมายความว่า กรองเอาเฉพาะ Packet ที่ส่งมายัง IP address (Destination) ที่เรากรองไว้

ip.dst==192.168.1.38						
No.	Time	Source	Destination	Protocol	Length	Info
391	6.562444	104.19.136.78	192.168.1.38	TCP	66	443 → 50241 [SYN, ACK] Seq=
401	6.594635	104.19.136.78	192.168.1.38	TCP	54	443 → 50241 [ACK] Seq=1 Ac
402	6.597542	104.19.136.78	192.168.1.38	TLSv1.3	1506	Server Hello, Change Cipe
403	6.597542	104.19.136.78	192.168.1.38	TLSv1.3	718	Application Data
428	6.632570	104.19.136.78	192.168.1.38	TCP	54	443 → 50241 [ACK] Seq=2117
429	6.632570	104.19.136.78	192.168.1.38	TCP	54	443 → 50241 [ACK] Seq=2117
430	6.632570	104.19.136.78	192.168.1.38	TLSv1.3	591	Application Data, Applicat
432	6.633987	104.19.136.78	192.168.1.38	TCP	54	443 → 50241 [ACK] Seq=2654
445	6.646937	104.19.136.78	192.168.1.38	TLSv1.3	1445	Application Data
446	6.646937	104.19.136.78	192.168.1.38	TLSv1.3	949	Application Data
447	6.646937	104.19.136.78	192.168.1.38	TLSv1.3	85	Application Data
497	6.679433	171.102.241.95	192.168.1.38	TCP	66	443 → 50245 [SYN, ACK] Seq=

## 2. การแตกต่างระหว่าง Filter display และ Capture filter อย่างไร และสามารถนำไปใช้งานได้

อย่างไร ในแต่ละแบบ

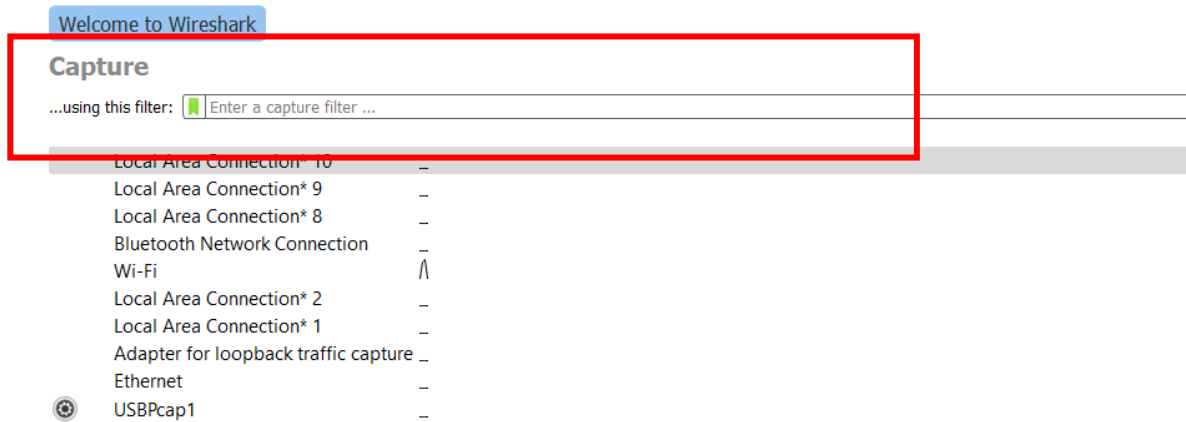
- **Filter Display** -> จะแสดงอยู่ในหน้าการตรวจจับ packet เราสามารถกรองสิ่งที่เราต้องการได้โดยพิมพ์ที่ช่องว่างดังที่แสดง

Capturing from Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2001:fb1:17f:a9d5:c...	2404:6800:4003:c04:...	TCP	75	55834 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment o
2	0.034168	2404:6800:4003:c04:...	2001:fb1:17f:a9d5:c...	TCP	86	443 → 55834 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
3	0.062376	2001:fb1:17f:a9d5:c...	2404:6800:4001:803:...	UDP	95	52647 → 443 Len=33
4	0.096751	2404:6800:4001:803:...	2001:fb1:17f:a9d5:c...	UDP	88	443 → 52647 Len=26
5	0.136497	162.159.135.234	192.168.1.38	TLSv1.2	101	Application Data
6	0.188576	192.168.1.38	162.159.135.234	TCP	54	64060 → 443 [ACK] Seq=1 Ack=48 Win=500 Len=0

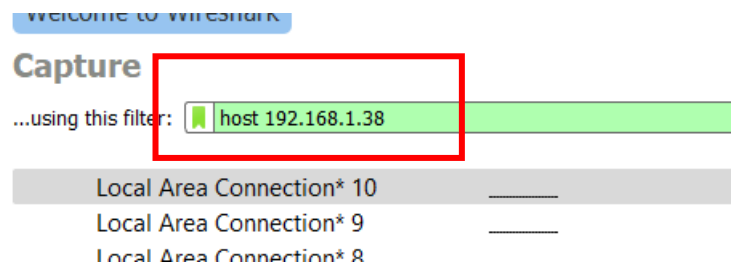
ทั้งนี้หน้า Capture หรือ หน้าจะตรวจจับจะแสดงทุกอย่างที่เราได้กระทำ ทุก Packet ที่ได้รับหรือส่ง ทุก Protocols ไม่ได้แสดงเฉพาะ เหมือนกับ Capture filter ซึ่งเราสามารถเลือกได้ว่าต้องการกรองอะไร หรือ กรองเฉพาะอะไรได้ ไม่เหมือนกับ Capture filter ที่จะแสดงเฉพาะสิ่งที่เราต้องการเท่านั้น หากเราต้องการ กรองอย่างอื่นต้องเริ่มทำการตรวจจับใหม่นั้นเอง

ip.dst==192.168.1.38						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.001810	192.168.1.1	192.168.1.38	ICMP	138	Destination unreachable (Port unreachable)
7	1.504208	192.168.1.1	192.168.1.38	ICMP	138	Destination unreachable (Port unreachable)
12	4.366785	162.159.135.234	192.168.1.38	TLSv1.2	275	Application Data
25	6.632280	20.25.241.18	192.168.1.38	TLSv1.2	229	Application Data
63	21.576314	122.155.167.45	192.168.1.38	TCP	66	443 → 55844 [ACK] Seq=1 Ack=2 Win=248 Len=0 SLE=1 SR
74	28.735063	162.159.135.234	192.168.1.38	TCP	54	443 → 64060 [ACK] Seq=222 Ack=52 Win=5 Len=0
75	28.971481	162.159.135.234	192.168.1.38	TLSv1.2	87	Application Data

- **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

No.	Time	Source	Destination	Protocol	Length	Info
7	10.316706	162.159.135.234	192.168.1.38	TLSv1.2	103	Application Data
8	10.360090	192.168.1.38	162.159.135.234	TCP	54	64060 → 443 [ACK] Seq=1 Ack=96 W
9	11.363857	192.168.1.38	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10	12.370137	192.168.1.38	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
11	13.382298	192.168.1.38	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	14.394454	192.168.1.38	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13	15.704732	162.159.135.234	192.168.1.38	TLSv1.2	182	Application Data
14	15.714400	202.44.33.94	192.168.1.38	TCP	54	443 → 55795 [FIN, ACK] Seq=1 Ack
15	15.714400	202.44.33.94	192.168.1.38	TCP	54	443 → 55786 [FIN, ACK] Seq=1 Ack
16	15.714450	192.168.1.38	202.44.33.94	TCP	54	55795 → 443 [ACK] Seq=1 Ack=2 Wi
17	15.714510	192.168.1.38	202.44.33.94	TCP	54	55786 → 443 [ACK] Seq=1 Ack=2 Wi
18	15.715214	202.44.33.94	192.168.1.38	TCP	54	443 → 55796 [FIN, ACK] Seq=1 Ack
19	15.715214	202.44.33.94	192.168.1.38	TCP	54	443 → 55794 [FIN, ACK] Seq=1 Ack
20	15.715246	192.168.1.38	202.44.33.94	TCP	54	55796 → 443 [ACK] Seq=1 Ack=2 Wi
21	15.715290	192.168.1.38	202.44.33.94	TCP	54	55794 → 443 [ACK] Seq=1 Ack=2 Wi
22	15.746656	192.168.1.38	162.159.135.234	TCP	54	64060 → 443 [ACK] Seq=1 Ack=224
23	17.693190	162.159.135.234	192.168.1.38	TLSv1.2	212	Application Data
24	17.739697	192.168.1.38	162.159.135.234	TCP	54	64060 → 443 [ACK] Seq=1 Ack=382
25	18.477474	192.168.1.38	20.25.241.18	TLSv1.2	98	Application Data
26	18.711252	20.25.241.18	192.168.1.38	TLSv1.2	229	Application Data
27	18.756357	192.168.1.38	20.25.241.18	TCP	54	49748 → 443 [ACK] Seq=45 Ack=176

### 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 หลากหลายตามที่อธิบายไว้ข้างต้น ทำให้เราต้องเพิ่มรายละเอียดในการค้นหาเข้าไปอีกขั้นหนึ่ง สำหรับมือใหม่ที่ต้องการหา Packet หนึ่งๆ เป็นไปได้ยากมาก เช่น เราต้องการหา กะเพรา บางที่เรากรองไป เราอาจจะเจอ กะเพราหมูกรอบ กะเพราไก่ กระเพราเนื้อ หรือ ใบกระเพรา ก็ได้ เราต้องเพิ่มรายละเอียดมากขึ้น

#### Capture filter

##### ข้อดี

- เราสามารถตั้งค่าให้แสดงเฉพาะรายละเอียดที่เราต้องการเฉพาะได้ โดยจะไม่มีนอกเหนือสิ่งที่เราต้องการเลยในหน้าแสดงPacket
- การแสดงผลในการตรวจจับไว้ เนื่องจากเราได้กรองเฉพาะ Packet ที่เราสนใจไว้แล้วนั่นเอง

##### ข้อเสีย

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