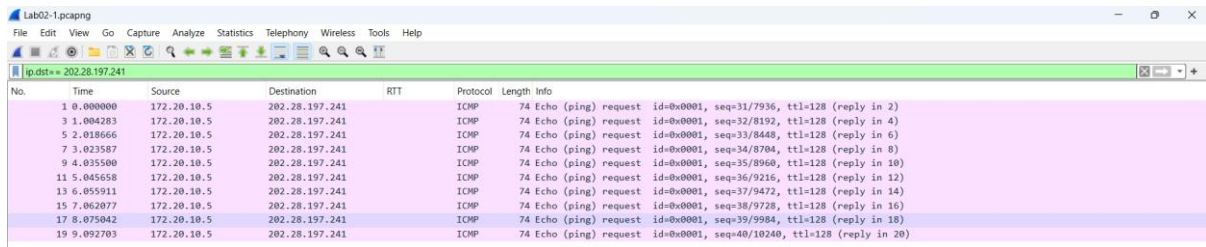


1. Display filter ต่อไปนี้เป็นการกำหนดเงื่อนไขใดในการแสดงผล packets และหากใช้ Display filter ต่อไปนี้กับไฟล์ที่ save เอาไว้ จะเหลือ packets ที่แสดงผลใน Packet List Pane กี่ packets?

Answer : มีจำนวน 10 packets ดังภาพ



Lab02-1.pcapng

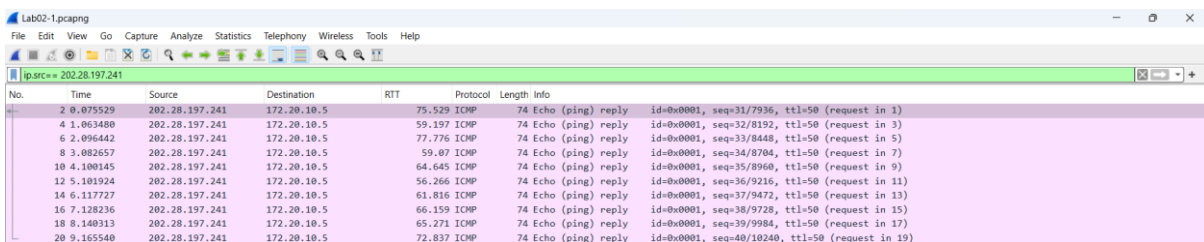
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 202.28.197.241

No.	Time	Source	Destination	RTT	Protocol	Length	Info
1	0.000000	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 2)
3	1.004283	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 4)
5	2.018666	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 6)
7	3.023587	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 8)
9	4.035500	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 10)
11	5.045658	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 12)
13	6.055911	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 14)
15	7.062077	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 16)
17	8.075042	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 18)
19	9.092703	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 20)

2. Display filter ต่อไปนี้เป็นการกำหนดเงื่อนไขใดในการแสดงผล packets และหากใช้ Display filter ต่อไปนี้กับไฟล์ที่ save เอาไว้ จะเหลือ packets ที่แสดงผลใน Packet List Pane กี่ packets?

Answer : มีจำนวน 10 packets ดังภาพ



Lab02-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 202.28.197.241

No.	Time	Source	Destination	RTT	Protocol	Length	Info
2	0.075529	202.28.197.241	172.20.10.5	75.529	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=50 (request in 1)
4	1.063480	202.28.197.241	172.20.10.5	59.197	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=50 (request in 3)
6	2.096442	202.28.197.241	172.20.10.5	77.776	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=50 (request in 5)
8	3.082657	202.28.197.241	172.20.10.5	59.07	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=50 (request in 7)
10	4.100145	202.28.197.241	172.20.10.5	64.645	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=50 (request in 9)
12	5.101924	202.28.197.241	172.20.10.5	56.266	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=50 (request in 11)
14	6.117727	202.28.197.241	172.20.10.5	61.816	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=50 (request in 13)
16	7.128236	202.28.197.241	172.20.10.5	66.159	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=50 (request in 15)
18	8.140313	202.28.197.241	172.20.10.5	65.271	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=50 (request in 17)
20	9.165540	202.28.197.241	172.20.10.5	72.837	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=50 (request in 19)

3. Display filter ต่อไปนี้เป็นการกำหนดเงื่อนไขใดในการแสดงผล packets และหากใช้ Display filter ต่อไปนี้กับไฟล์ที่ save เอาไว้ จะมี packets ที่แสดงผลใน Packet List Pane หรือไม่? เพราะเหตุใด?

Answer : ไม่มี packets แสดงดังภาพด้านล่าง เพราะ ใน packet ทั้งหมดที่ทำการดักจับและใช้ capture filter เป็น protocol เป็น ICMP ไม่มี packet ใดที่ทั้ง source ip และ destination ip เป็น address เดียวกัน (202.28.197.241)



Lab02-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 202.28.197.241 and ip.src == 202.28.197.241

No.	Time	Source	Destination	RTT	Protocol	Length	Info
-----	------	--------	-------------	-----	----------	--------	------

4. Display filter ต่อไปนี้เป็นการกำหนดเงื่อนไขใดในการแสดงผล packets และหากใช้ Display filter ต่อไปนี้กับไฟล์ที่ save เอาไว้ จะเหลือ packets ที่แสดงผลใน Packet List Pane กี่ packets?

Answer : มีจำนวน 20 packets ดังภาพ

No.	Time	Source	Destination	RTT	Protocol	Length	Info
4	1.063480	202.28.197.241	172.20.10.5	59.197	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=50 (request in 3)
5	2.018666	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 6)
6	2.096442	202.28.197.241	172.20.10.5	77.776	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=50 (request in 5)
7	3.023587	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 8)
8	3.082657	202.28.197.241	172.20.10.5	59.07	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=50 (request in 7)
9	4.035500	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 10)
10	4.100145	202.28.197.241	172.20.10.5	64.645	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=50 (request in 9)
11	5.045658	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 12)
12	5.101924	202.28.197.241	172.20.10.5	56.266	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=50 (request in 11)
13	6.055911	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 14)
14	6.117727	202.28.197.241	172.20.10.5	61.816	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=50 (request in 13)
15	7.062077	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 16)
16	7.128236	202.28.197.241	172.20.10.5	66.159	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=50 (request in 15)
17	8.075042	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 18)
18	8.140313	202.28.197.241	172.20.10.5	65.271	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=50 (request in 17)
19	9.092703	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 20)
20	9.165540	202.28.197.241	172.20.10.5	72.837	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=50 (request in 19)

5.Displayfilter ต่อไปนี้เป็นกรกำหนดเงื่อนไขใดในการแสดงผล packets และหากใช้ Display filter ต่อไปนี้กับไฟล์ที่ save เอาไว้ จะเหลือ packets ที่แสดงผลใน Packet List Pane กี่ packets?ต่างกับข้อที่แล้วหรือไม่?

Answer : ไม่แตกต่างจากข้อที่4ที่ผ่านมา เพราะ ip.addr จะmatchทั้ง ip source และ ip destination ของ ip header

No.	Time	Source	Destination	RTT	Protocol	Length	Info
4	1.063480	202.28.197.241	172.20.10.5	59.197	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=50 (request in 3)
5	2.018666	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 6)
6	2.096442	202.28.197.241	172.20.10.5	77.776	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=50 (request in 5)
7	3.023587	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 8)
8	3.082657	202.28.197.241	172.20.10.5	59.07	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=50 (request in 7)
9	4.035500	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 10)
10	4.100145	202.28.197.241	172.20.10.5	64.645	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=50 (request in 9)
11	5.045658	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 12)
12	5.101924	202.28.197.241	172.20.10.5	56.266	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=50 (request in 11)
13	6.055911	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 14)
14	6.117727	202.28.197.241	172.20.10.5	61.816	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=50 (request in 13)
15	7.062077	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 16)
16	7.128236	202.28.197.241	172.20.10.5	66.159	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=50 (request in 15)
17	8.075042	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 18)
18	8.140313	202.28.197.241	172.20.10.5	65.271	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=50 (request in 17)
19	9.092703	172.20.10.5	202.28.197.241		ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 20)
20	9.165540	202.28.197.241	172.20.10.5	72.837	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=50 (request in 19)

6.จากhost ปลายทางในตารางต่อไปนี้จงหาหมายเลข IP address และRound-trip time (RTT) ระหว่างเครื่องผู้เรียน และปลายทางโดยหา RTT ต่ำสุด สูงสุด และเฉลี่ย จากการส่งICMP packets ไม่น้อยกว่า 10 packets

Answer :

Destination Host	IPv4	Min RTT(ms)	Max RTT(ms)	Average RTT(ms)
<a href="http://www.aarnet.edu.au">www.aarnet.edu.au</a>	202.158.207.3	141	174	151
<a href="http://www.apan.net">www.apan.net</a>	104.21.39.91	23	47	34
Internet2.edu	165.227.252.59	275	391	295
<a href="http://www.geant.org">www.geant.org</a>	83.97.93.30	281	2017	505
<a href="http://www.singaren.net.sg">www.singaren.net.sg</a>	203.30.39.25	50	88	58
<a href="http://www.surf.nl">www.surf.nl</a>	145.100.190.243	203	266	224
<a href="http://www.switch.ch">www.switch.ch</a>	13.107.213.59	25	52	36
www.uni.net.th	202.28.197.241	60	163	82

7.จากข้อ6ผู้เรียนสามารถอนุมานได้หรือไม่ว่าแต่host ปลายทางเหล่านั้นอยู่ในประเทศอะไร?โปรดสืบค้นข้อมูลเพิ่มเติมจากอินเทอร์เน็ตในการตอบคำถามนี้

Answe :

Destination Host	Country
<a href="http://www.aarnet.edu.au">www.aarnet.edu.au</a>	Australia
<a href="http://www.apan.net">www.apan.net</a>	United States
Internet2.edu	United States
<a href="http://www.geant.org">www.geant.org</a>	United Kingdom
<a href="http://www.singaren.net.sg">www.singaren.net.sg</a>	Singapore
<a href="http://www.surf.nl">www.surf.nl</a>	Netherlands
<a href="http://www.switch.ch">www.switch.ch</a>	United States
<a href="http://www.uni.net.th">www.uni.net.th</a>	Thailand

8. จากข้อ 6 และ ข้อ 7 จาก host ปลายทางทั้งหมดในตาราง ปลายทางใดมีค่า RTT เจลี่ยน้อยที่สุด? host ปลายทางดังกล่าว อยู่ในประเทศใด?

Answer : host ที่มีค่า RTT เจลี่ยน้อยที่สุดคือ [www.aarnet.edu.au](http://www.aarnet.edu.au) อยู่ในประเทศ Australia

9. เข้าไปที่หน้าต่าง Capture File Properties ในหมวด Statistics ที่อยู่ด้านล่าง โปรดอธิบายว่าแต่ละค่าหมายถึงอะไรบ้าง และที่มีการแบ่งเป็น 3 คอลัมน์ แต่ละคอลัมน์ต่างกันอย่างไร

Answer : ค่าทั้ง 3 คอลัมน์มีชื่อดังนี้ตามลำดับ Captured, Displayed, Marked

โดย Captured จะแสดงค่าของ packet ทั้งหมดที่อยู่ใน saved capture file

Displayed จะแสดงค่าของ packet ที่ทำการ set display filter ไว้ (หาก set)

Marked จะแสดงค่าของ packet ที่ทำการ Marked เอาไว้

Reference :

ข้อ 7 <https://www.iplocation.net/ip-lookup>

ข้อ 5 <https://wiki.wireshark.org/DisplayFilters>

ข้อ 9 [https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChStatSummary.html](https://www.wireshark.org/docs/wsug_html_chunked/ChStatSummary.html)