Ping • Traceroute 메시지 분석

23.10.26

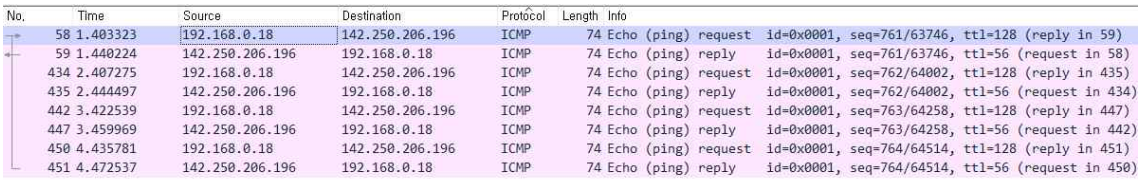
① Ping 메시지 분석

- My IP address : 192.168.0.18

(1) Echo Request / Reply

- 메시지를 보낼 대상 : www.google.com

명령 프롬프트에서 'ping -n 4 www.google.com'을 입력하여 4번(default)의 에코 요청을 보내보았다.



No.	Time	Source	Destination	Protocol	Length	Info
58	1.403323	192.168.0.18	142.250.206.196	ICMP	74	Echo (ping) request id=0x0001, seq=761/63746, ttl=128 (reply in 59)
59	1.440224	142.250.206.196	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=761/63746, ttl=56 (request in 58)
434	2.407275	192.168.0.18	142.250.206.196	ICMP	74	Echo (ping) request id=0x0001, seq=762/64002, ttl=128 (reply in 435)
435	2.444497	142.250.206.196	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=762/64002, ttl=56 (request in 434)
442	3.422539	192.168.0.18	142.250.206.196	ICMP	74	Echo (ping) request id=0x0001, seq=763/64258, ttl=128 (reply in 447)
447	3.459969	142.250.206.196	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=763/64258, ttl=56 (request in 442)
450	4.435781	192.168.0.18	142.250.206.196	ICMP	74	Echo (ping) request id=0x0001, seq=764/64514, ttl=128 (reply in 451)
451	4.472537	142.250.206.196	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=764/64514, ttl=56 (request in 450)

```
> Frame 58: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8F3F2FA1-D467-4B23-A353-0AC0664AF5E1}, id 0
> Ethernet II, Src: IntelCor_0c:51:39 (b0:60:88:0c:51:39), Dst: EFMNetwo_ca:68:70 (70:5d:cc:ca:68:70)
> Internet Protocol Version 4, Src: 192.168.0.18, Dst: 142.250.206.196
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4a62 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 761 (0x02f9)
    Sequence Number (LE): 63746 (0xf902)
    [Response frame: 59]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

위에서부터 두 묶음씩이 하나의 Echo Request/Reply이다. 오른쪽의 Info를 통해 메시지를 분석할 수 있다.

No	Time	Request/reply	id	seq	TTL
58	1.403323	Request	0x0001	761	128
59	1.440224	Reply	0x0001	761	56
434	2.407275	Request	0x0001	762	128
435	2.444497	Reply	0x0001	762	56
442	3.425239	Request	0x0001	763	128
447	3.459969	Reply	0x0001	763	56
450	4.435781	Request	0x0001	764	128
451	4.472537	Reply	0x0001	764	56

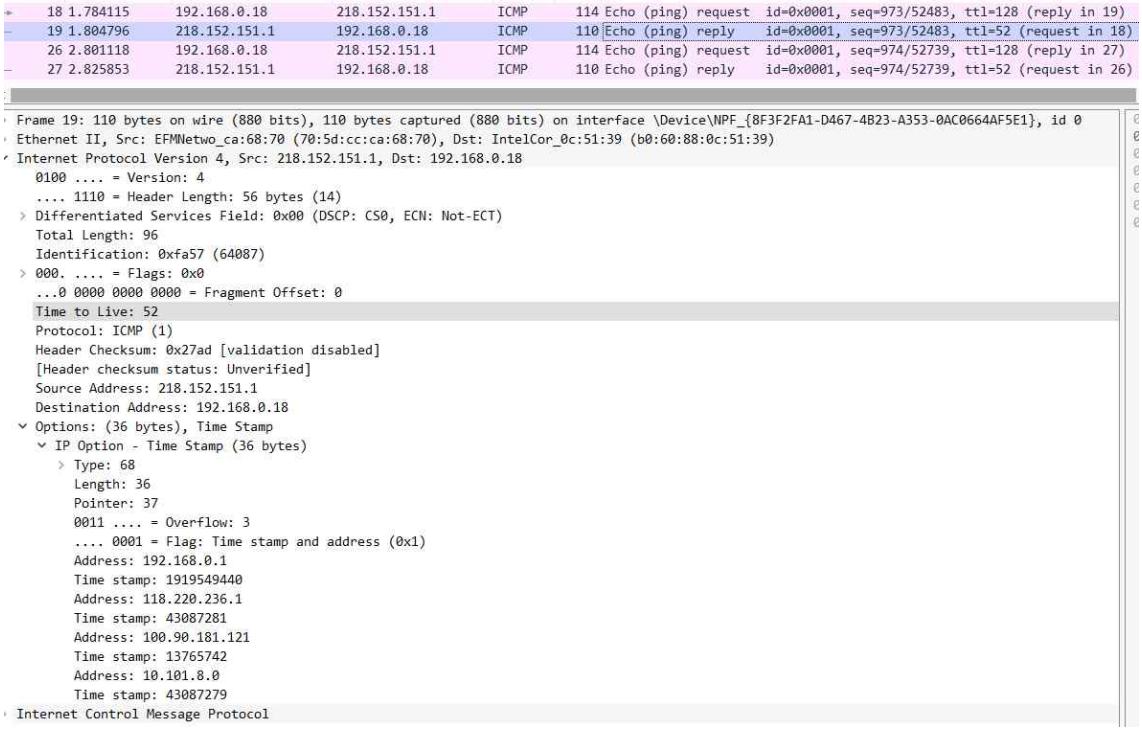
(Reply time - Request time)을 구함으로 Response time을 계산할 수 있다.

(2) Timestamp 사용

제대로 된 결과를 도출하기 위해 공용 IP 주소를 사용하였다.

- Ping을 보낼 대상 : 218.152.151.1
- 명령어: 'ping -s 4 -n 2 218.152.151.1 (두 번만 보낸다.)

다음은 wireshark로 캡처한 결과이다. IP packet: 옵션부에 Time stamp 결과가 들어있다.



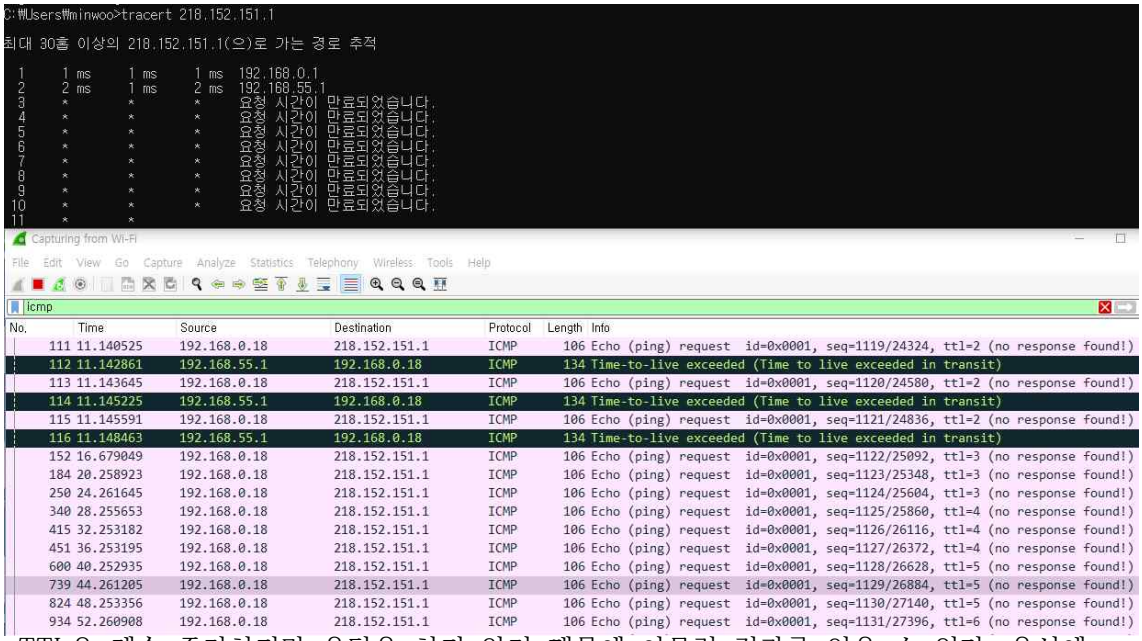
최초 4개의 router 주소와, 지나간 Time stamp가 찍혀 있는 모습을 볼 수 있다.

비교하기 위해 프롬프트에서 캡처한 결과를 보인다.

위와는 경로가 다르다. 상황에 따라 경로는 계속 변할 수 있음을 알려준다.

② Traceroute 메시지 분석

국내에서는 ICMP 요청을 거부하는 사이트가 많아 제대로 된 분석을 하기 어렵다. 예를 들어 위의 IP 주소로 경로추적을 하면 다음과 같이 된다.



```
C:₩Users₩minwoo>tracert 218.152.151.1

최대 30홉 이상의 218.152.151.1(으)로 가는 경로 추적

  1    1 ms    1 ms    1 ms  192.168.0.1
  2    2 ms    1 ms    2 ms  192.168.55.1
  3     *       *       *     요청 시간이 만료되었습니다.
  4     *       *       *     요청 시간이 만료되었습니다.
  5     *       *       *     요청 시간이 만료되었습니다.
  6     *       *       *     요청 시간이 만료되었습니다.
  7     *       *       *     요청 시간이 만료되었습니다.
  8     *       *       *     요청 시간이 만료되었습니다.
  9     *       *       *     요청 시간이 만료되었습니다.
 10     *       *       *     요청 시간이 만료되었습니다.
 11     *       *
```

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
111	11.140525	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1119/24324, ttl=2 (no response found!)
112	11.142861	192.168.55.1	192.168.0.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
113	11.143645	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1120/24580, ttl=2 (no response found!)
114	11.145225	192.168.55.1	192.168.0.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
115	11.145591	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1121/24836, ttl=2 (no response found!)
116	11.148463	192.168.55.1	192.168.0.18	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
152	16.679049	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1122/25092, ttl=3 (no response found!)
184	20.258923	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1123/25348, ttl=3 (no response found!)
250	24.261645	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1124/25604, ttl=3 (no response found!)
340	28.255653	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1125/25860, ttl=4 (no response found!)
415	32.253182	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1126/26116, ttl=4 (no response found!)
451	36.253195	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1127/26372, ttl=4 (no response found!)
600	40.252935	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1128/26628, ttl=5 (no response found!)
739	44.261205	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1129/26884, ttl=5 (no response found!)
824	48.253356	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1130/27140, ttl=5 (no response found!)
934	52.260908	192.168.0.18	218.152.151.1	ICMP	106	Echo (ping) request id=0x0001, seq=1131/27396, ttl=6 (no response found!)

TTL은 계속 증가하지만 응답을 하지 않기 때문에 아무런 결과를 얻을 수 없다. 옵션에 -w 8000으로 대기시간을 늘렸지만 마찬가지였다.

하지만 초반 라우터에서는 time-exceeded를 통해 경로를 전달했음을 알 수 있다.

233	5.891000	192.168.0.1	192.168.0.18	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
234	5.891372	192.168.0.18	218.152.151.1	ICMP	106 Echo (ping) request id=0x0001, seq=1266/61956, ttl=1 (no response found!)
235	5.892158	192.168.0.1	192.168.0.18	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
237	5.892469	192.168.0.18	218.152.151.1	ICMP	106 Echo (ping) request id=0x0001, seq=1267/62212, ttl=1 (no response found!)
238	5.893840	192.168.0.1	192.168.0.18	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
244	5.901245	192.168.0.1	192.168.0.18	ICMP	120 Destination unreachable (Port unreachable)
297	7.403146	192.168.0.1	192.168.0.18	ICMP	120 Destination unreachable (Port unreachable)
363	8.914235	192.168.0.1	192.168.0.18	ICMP	120 Destination unreachable (Port unreachable)
487	11.427083	192.168.0.18	218.152.151.1	ICMP	106 Echo (ping) request id=0x0001, seq=1268/62468, ttl=2 (no response found!)
488	11.429569	192.168.55.1	192.168.0.18	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
489	11.429929	192.168.0.18	218.152.151.1	ICMP	106 Echo (ping) request id=0x0001, seq=1269/62724, ttl=2 (no response found!)
490	11.431495	192.168.55.1	192.168.0.18	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
491	11.431843	192.168.0.18	218.152.151.1	ICMP	106 Echo (ping) request id=0x0001, seq=1270/62980, ttl=2 (no response found!)
495	11.433467	192.168.55.1	192.168.0.18	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
951	16.951128	192.168.0.18	218.152.151.1	ICMP	106 Echo (ping) request id=0x0001, seq=1271/63236, ttl=3 (no response found!)

```
ternet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 192.168.0.18, Dst: 218.152.151.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 92
  Identification: 0x3177 (12663)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x55d6 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.18
  Destination Address: 218.152.151.1
```

0000
0010
0020
0030
0040
0050
0060
0070
0080