

2022320033 박종혁

이더넷에서 캡처 중

파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전환(Y) 무선(W) 도구(T) 도움말(H)

표시 필터 적용 ... <Ctrl-/>

+

No.	Time	Source	Destination	Protocol	Length	Info
4	2.865106	192.168.219.101	224.0.0.251	MDNS	152	Standard query 0x000c PTR _9f5E7C8F47989526C9BCD95D24084F60827C5ED..._
5	2.868222	192.168.219.21	224.0.0.251	MDNS	447	Standard query response 0x0000 PTR uie4027lgu-2a5450b89035f03286e69235...
6	2.871850	192.168.219.21	224.0.0.251	MDNS	414	Standard query response 0x0000 PTR uie4027lgu-2a5450b89035f03286e69235...
7	2.874465	192.168.219.21	224.0.0.251	MDNS	399	Standard query response 0x0000 PTR uie4027lgu-2a5450b89035f03286e69235...
8	2.949172	121.254.136.90	192.168.219.106	TLSv1.2	78	Application Data
9	2.949268	192.168.219.106	121.254.136.90	TCP	54	63036 → 443 [ACK] Seq=1 Ack=25 Win=2053 Len=0
10	2.949736	121.254.136.90	192.168.219.106	TCP	60	443 → 63036 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
11	2.949803	192.168.219.106	121.254.136.90	TCP	54	63036 → 443 [ACK] Seq=1 Ack=25 Win=2053 Len=0
12	3.850339	192.168.219.106	192.168.219.21	TCP	164	60821 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=1022 Len=110 [TCP segment of a...
13	3.851292	192.168.219.21	192.168.219.106	TCP	164	8009 → 60821 [PSH, ACK] Seq=1 Ack=111 Win=188 Len=110 [TCP segment of a...
14	3.897310	192.168.219.106	192.168.219.21	TCP	54	60821 → 8009 [ACK] Seq=111 Ack=111 Win=1022 Len=0
15	3.900179	GongjinElect_4a:fe::	MicroStarINT_8a:2c::	ARP	60	Who has 192.168.219.106? Tell 192.168.219.1
16	3.900217	MicroStarINT_8a:2c::	GongjinElect_4a:fe::	ARP	42	192.168.219.106 is at 2c:f0:5d:8a:2c:51
17	3.999918	GongjinElect_4a:fe::	Spanning-tree-(for-)	STP	60	Conf. Root = 28672/4095/80:ca:4b:4a:fe:49 Cost = 0 Port = 0x0001
18	4.330083	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x6963f2eb
19	4.920742	20.189.173.6	192.168.219.106	TCP	60	443 → 63054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	6.000343	GongjinElect_4a:fe::	Spanning-tree-(for-)	STP	60	Conf. Root = 28672/4095/80:ca:4b:4a:fe:49 Cost = 0 Port = 0x0001

> Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on in

Ethernet II, Src: GongjinElect_4a:fe:49 (80:ca:4b:4a:fe:49), Dst: MicroSt

> Destination: MicroStarINT_8a:2c:51 (2c:f0:5d:8a:2c:51)

> Source: GongjinElect_4a:fe:49 (80:ca:4b:4a:fe:49)

Type: ARP (0x0806)

Padding: 00

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: GongjinElect_4a:fe:49 (80:ca:4b:4a:fe:49)

Sender IP address: 192.168.219.1

Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.219.106

0000 2c f0 5d 8a 2c 51 80 ca 4b 4a fe 49 08 06 00 01 ,].Q.KJ.I....

0010 08 00 06 04 00 01 80 ca 4b 4a fe 49 c0 a8 db 01KJ.I....

0020 00 00 00 00 00 c0 a8 db 6a 00 00 00 00 00 00j.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00

이더넷 <live capture in progress>

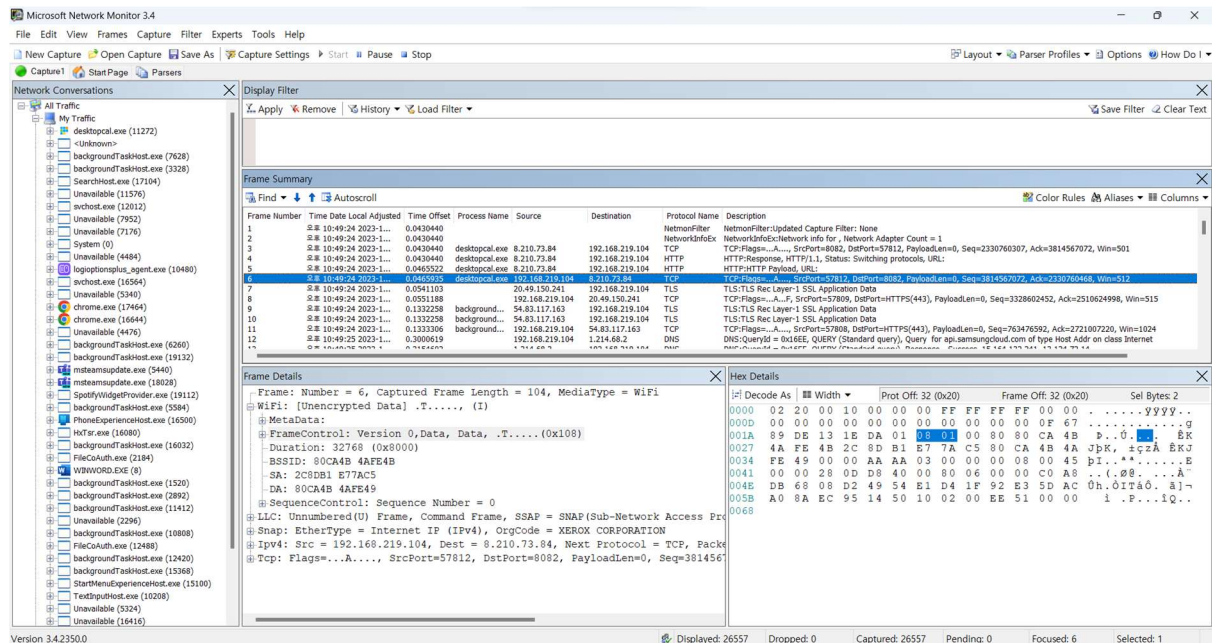
패킷 수: 7965 · 표시됨: 7965(100.0%)

프로필: Default

Comparison:

- 1) 이더넷 헤더 프레임의 첫 6바이트는 destination address로, 목적지 MAC 주소를 나타낸다. 따라서 위 패킷의 목적지 MAC 주소는 '2c f0 5d 8a 2c 51'이다.
- 2) 그 다음 6바이트는 source address로, 출발지 MAC 주소를 나타낸다. 따라서 위 패킷의 출발지 MAC 주소는 '80 ca 4b 4a fe 49'에 해당한다.
- 3) 그 다음 2바이트는 EtherType 필드이다. 위 패킷의 해당 필드 값은 '08 06'으로, ARP(Address Resolution Protocol) 타입의 프레임을 의미한다. 여기까지가 이더넷 헤더에 속한다.
- 4) EtherType 필드 이후부터 끝까지는 데이터 필드이며, EtherType이 ARP이므로 ARP패킷의 데이터가 들어있는 것을 알 수 있다. 또한 데이터 필드의 최소 바이트 수는 46이지만 ARP패킷은 총 28바이트이므로 나머지 18바이트는 Padding으로 채우고 있다.

2. 802.11 Frame Header



Comparison:



- 1) 802.11 프레임 헤더의 첫 2 바이트는 Frame Control 필드이다. 총 16 비트로 이루어져 있으며, 비트 단위로 정보를 담고 있다. 특히 3~4 번째 비트는 프레임 타입을 의미하는데, 위 패킷의 경우 해당 비트가 '10'이므로 데이터 프레임에 해당한다.
- 2) 그 다음 2 바이트는 Duration/ID 필드로, 위 패킷에서는 NAV 값을 나타낸다. 해당 필드의 값이 대기 시간의 최댓값인 '32768'로 설정되어 있는 것으로 보아, contention-free 방식을 사용한다고 추측할 수 있다.
- 3) 그 다음 18 바이트는 각 6 바이트로 이루어진 3 개의 주소 값 필드로 구성되어 있다. 각 주소의 의미는 Frame Control 필드의 값에 따라 조금씩 다른데, 분석 결과 위 패킷의 address1, 2, 3 의 값은 각각 BSSID, SA, DA 를 의미하며 그 값은 '80CA4B 4AFE4B', '2C8DB1 E77AC5', '80CA4B 4AFE49'이다.
- 4) 그 다음 2 바이트는 Sequence Control 필드이다. 제어 프레임에서는 사용되지 않지만, 위 패킷은 데이터 프레임이므로 Sequence Control 필드를 사용한다. 16 비트 중 4 비트는 FragmentNumber, 나머지 12 비트는 SequenceNumber 값을 의미한다. 분석 결과 위 패킷에서는 '00 00'으로, 두 값 모두 0 임을 확인할 수 있다.

- 5) 프레임 타입과 서브타입에 따라 헤더에 Address4, QoS Control, HT Control 등의 필드가 추가로 포함되기도 하지만, 위 패킷에서는 Sequence Control 필드 이후 곧바로 Frame Body(LLC Frame)가 등장하고 있다.
- 6) LLC Frame 에서, 첫 3 개의 바이트는 각각 DSAP, SSAP, Control 필드이다. 이때, 위 패킷은 DSAP 과 SSAP 의 값이 모두 0xAA 이므로 SNAP 을 사용할 것임을 알 수 있다. Control 필드의 0x03 은 UI frame 을 의미한다.
- 7) DSAP 과 SSAP 에서 SNAP 을 추가로 사용할 것임을 명시했으므로, 다음 5 바이트는 SNAP 부분이다. 앞 3 바이트는 OUI, 뒤 2 바이트는 EtherType 필드로, 위 패킷에서는 그 값이 각각 0x0000, 0x0800 이다. 이는 IEEE 표준에 따르면 XEROX CORPORATION 에서 제조, IPv4 프로토콜을 사용함을 의미한다.