

1. Global Header 구조체

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÖÃ=;.....
00000010	00	00	04	00	01	00	00	00	4E	F6	9A	5D	32	B8	06	00Nöš]2...
00000020	41	00	00	00	41	00	00	00	88	36	6C	1B	D3	00	F8	A2	A...A...^6l.Ö.ø¢
00000030	D6	57	DE	F5	08	00	45	00	00	33	46	1D	40	00	80	11	ÖWpö...E...3F.€.€.

- ① D4 C3 B2 A1
: Magic Number (해당 값을 통해 PCAP 파일포맷임을 알 수 있음)
- ②, ③ 02 00 04 00
: Major/Minor (현재 버전이 2.4임을 표시)
- ④ 00 00 00 00
: GMT (기본 값으로 0 값 세팅)
- ⑤ 00 00 00 00
: accuracy of timestamps필드 (0 값 세팅)
- ⑥ 00 00 04 00
: 실제 수집된 패킷길이
- ⑦ 01 00 00 00
: data link type (Ethernet은 1 값이 세팅됨)

2. Packet Header 구조체

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÖÃ=;.....
00000010	00	00	04	00	01	00	00	00	4E	F6	9A	5D	32	B8	06	00Nöš]2...
00000020	41	00	00	00	41	00	00	00	88	36	6C	1B	D3	00	F8	A2	A...A...^6l.Ö.ø¢
00000030	D6	57	DE	F5	08	00	45	00	00	33	46	1D	40	00	80	11	ÖWpö...E...3F.€.€.

- ① 4E F6 9A 5D
: timestamp seconds (와이어샤크 부분에서 Epoch Time 부분의 앞쪽의 10진수_1570436686)
- ② 32 B8 06 00
: timestamp microseconds (Epoch Time의 두 번째 자리부분_440370000)
- ③ 41 00 00 00
: number of octets of packet saved in file (Capture Length 부분_65 bytes (=520 bits))
- ④ 41 00 00 00
: actual length of packet (Frame Length 부분_65 bytes (=520 bits))

$$28+41 = 69$$

2주차 - 패킷캡처.pcap																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÔÃ°j;.....
00000010	00	00	04	00	01	00	00	00	4E	F6	9A	5D	32	B8	06	00Nöš]2,..
00000020	41	00	00	00	41	00	00	00	88	36	6C	1B	D3	00	F8	A2	A...A...^61.Ö.øø
00000030	D6	57	DE	F5	08	00	45	00	00	33	46	1D	40	00	80	11	ÖWpö..E..3F.Ö.€.
00000040	2D	C7	C0	A8	00	06	AC	D9	19	4E	FA	69	01	BB	00	1F	-ÇÀ`...-Û.Núi.»..
00000050	65	B9	40	0C	6F	80	34	7D	70	ED	21	05	C9	A2	14	F7	e¹@.øø4}pi!..Éø.÷
00000060	78	F1	C0	42	92	22	82	0E	75	4E	F6	9A	5D	FD	C3	07	xñÄB' ",.uNöš]ýÃ.
00000070	00	3E	00	00	00	3E	00	00	00	F8	A2	D6	57	DE	F5	88	.>...>...øøÖWpö^
00000080	36	6C	1B	D3	00	08	00	45	00	00	30	00	00	40	00	37	61.Ö...E..0..@.7

$$79+3E = B7$$

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000090	11	BC	E7	AC	D9	19	4E	C0	A8	00	06	01	BB	FA	69	00	.¼ç-Û.NÄ`...»úi.
000000A0	1C	37	95	40	06	96	D6	60	AB	D7	A8	02	FD	CD	9D	64	.7*@.-Ö`«*`.ýí.d
000000B0	4A	64	98	B1	19	EB	5D	5C	F6	9A	5D	E6	6F	07	00	2E	Jd`±.ë]öš]æø...
000000C0	00	00	00	2E	00	00	00	F8	A2	D6	57	DE	F5	88	36	6CøøÖWpö^61
000000D0	1B	D3	00	08	00	46	00	00	20	EF	72	40	00	01	02	54	.Ö...F.. ír@...T

$$C7+2E = F5$$

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000000C0	00	00	00	2E	00	00	00	F8	A2	D6	57	DE	F5	88	36	6CøøÖWpö^61
000000D0	1B	D3	00	08	00	46	00	00	20	EF	72	40	00	01	02	54	.Ö...F.. ír@...T
000000E0	BA	C0	A8	00	01	E0	00	00	01	94	04	00	00	11	01	EE	°Ä`...ä...`.....î
000000F0	FE	00	00	00	00	5C	F6	9A	5D	0E	60	0D	00	2E	00	00	p....öš].....
00000100	00	2E	00	00	00	01	00	5E	7F	FF	FA	F8	A2	D6	57	DE^..ýúøøÖWpö
00000110	F5	08	00	46	00	00	20	46	00	00	00	01	02	2E	2F	C0	ö...F.. F...../Ä

$$105+2E = 133$$

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000120	A8	00	06	EF	FF	FF	FA	94	04	00	00	16	00	FA	04	EF	`..îýýú".....ú.î
00000130	FF	FF	FA	5C	F6	9A	5D	8B	61	0D	00	2E	00	00	00	2E	ýýúöš]<a.....
00000140	00	00	00	01	00	5E	00	00	FC	F8	A2	D6	57	DE	F5	08	...^..ûøøÖWpö.
00000150	00	46	00	00	20	24	69	00	00	01	02	5E	C4	C0	A8	00	.F.. \$i....^ÄÄ`.

$$143+2E = 171$$

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000150	00	46	00	00	20	24	69	00	00	01	02	5E	C4	C0	A8	00	.F.. \$i....^ÄÄ`.
00000160	06	E0	00	00	FC	94	04	00	00	16	00	09	03	E0	00	00	.ä..ü".....ä..
00000170	FC	5C	F6	9A	5D	22	62	0D	00	2E	00	00	00	2E	00	00	üöš]"b.....
00000180	00	01	00	5E	00	00	FB	F8	A2	D6	57	DE	F5	08	00	46	ü...^..ûøøÖWpö..F