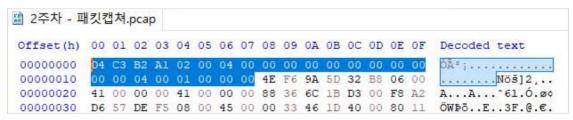
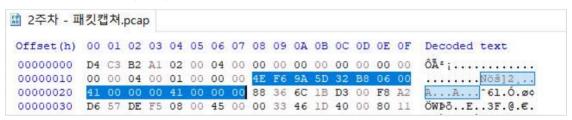
## 1. Global Header 구조체



- 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)
- @ 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



- 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))

```
關 2주차 - 패킷캡쳐.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 0Ã:.....
 00000010 00 00 04 00 01 00 00 00 4E F6 9A 5D 32 B8 06 00
                                                          .......Nöš]2,..
00000020 41 00 00 00 41 00 00 00 88 36 6C 1B D3 00 F8 A2
                                                          A...A...^61.Ó.ø¢
00000030 D6 57 DE F5 08 00 45 00 00 33 46 1D 40 00 80 11
                                                          ÖWÞő..E..3F.@.€.
00000040 2D C7 C0 A8 00 06 AC D9 19 4E FA 69 01 BB 00 1F
                                                          -ÇÀ"..¬Ù.Núi.»..
00000050 65 B9 40 0C 6F 80 34 7D 70 ED 21 05 C9 A2 14 F7
                                                          e¹@.o€4}pí!.É¢.÷
                                                          xñÀB'", .uNöš]ýÃ.
          78 F1 C0 42 92 22 82 0E 75 4E F6 9A 5D FD C3 07
00000060
          00 3E 00 00 00 3E 00 00 00 F8 A2 D6 57 DE F5 88
                                                          .>...>...ø¢ÖWÞő^
00000070
                                                          61.Ó...E..O..@.7
00000080 36 6C 1B D3 00 08 00 45 00 00 30 00 00 40 00 37
```

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 .4cp\\(\tilde{\text}\).N\(\text{A}^*\)...\(\text{wii}\).

0000000A0 1C 37 95 40 06 96 D6 60 AB D7 A8 02 FD CD 9D 64 .7\(\text{e}\).-\(\text{O}^*\)«\(\tilde{\text{w}}\).'\(\text{i}\).\(\text{d}\)

000000B0 4A 64 98 B1 19 EB 5D 5C F6 9A 5D E6 6F 07 00 2E ....\(\text{g}\).\(\text{d}\)

000000C0 00 00 00 2E 00 00 00 F8 A2 D6 57 DE F5 88 36 6C ....\(\text{g}\).\(\text{c}\)\(\text{O}\)*\(\text{b}\)\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\(\text{o}\)*\
```

C7+2F = F5

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 "..ïyyú"...ú.ï

00000130 FF FF FA 5C F6 9A 5D 8B 61 0D 00 2E 00 00 00 2E yyú(ōš]<a.....

00000140 00 00 00 01 00 5E 00 00 FC F8 A2 D6 57 DE F5 08 ....^..üz°ÖWÞő.

00000150 00 46 00 00 20 24 69 00 00 01 02 5E C4 C0 A8 00 .F.. $i...^ÄÄ".
```

143+2E = 171