

빨간 박스 – Global Header 구조체

* Magic Number : 해당 값을 통해 PCAP 파일포맷임을 알 수 있다.

D4 C3 B2 A1

* Major/Minor 버전 정보 : 현재 2.4버전

02 00 04 00

* GMT : 기본 기본 값으로 0 값이 세팅

00 00 00 00

* Accuracy of timestamps : 0 값이 세팅

00 00 00 00

* 실제 수집된 패킷 길이

00 00 04 00

* Data link type : Ethernet 은 1값이 세팅

01 00 00 00

파란 박스 – Packet Header 구조체

* Timestamp seconds : 와이어샤크 부분에 Epoch Time 부분의 앞쪽 10진수 (1570083523)

C3 92 95 5D

* Timestamp microseconds : Epoch Time의 두 번째 자리부분의 10진수 (392914000)

D2 FE 05 00

* Number of octets of packet saved in file : Capture Length 부분 (366 byte)

6E 01 00 00

* Actual length of packet : Frame Length 부분 (366 byte)

6E 01 00 00









