PCAP 포맷

와이어샤크는 윈도우상에서 Winpcap 라이브러리를 사용해서 패킷을 수집하며, 유닉스계열에서는 Libpcap을 사용하여 패킷을 수집하게 된다. 이때 수집된 데이터 포맷은 PCAP이라는 파일 포맷을 가 지고 있다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Global Header | Packet Header | Packet Data | Packet Header | Packet Data | … |

Global Header 구조체

typedef struct pcap\_hdr\_s {

guint32 magic\_number; /\* magic number \*/

guint16 version\_major; /\* major version number \*/

guint16 version\_minor; /\* minor version number \*/

gint32 thiszone; /\* GMT to local correction \*/

guint32 sigfigs; /\* accuracy of timestamps number \*/

guint32 snaplen; /\* max length of captured packets \*/

guint32 network; /\* data link type \*/

} pcap\_hdr\_t;

Packet Header 구조체

typedef struct pcapec\_hdr\_s {

guint32 ts\_sec; /\* imestamp seconds \*/

guint32 ts\_usec; /\* timestamp microseconds \*/

guint32 incl\_len; /\* number of octets of packet saved in file \*/

guint32 orig\_len; /\* actual length of packet \*/

} pcap\_hdr\_t;

http://wiki.wireshark.org/Development /LibpcapFileFormat