CERT-IS 양윤지

1. TCP/IP 개념 정리

-APPLICATION LAYER: FTP, HTTP등.

-TRANSPORT LAYER: TCP, UDP 프로토콜.

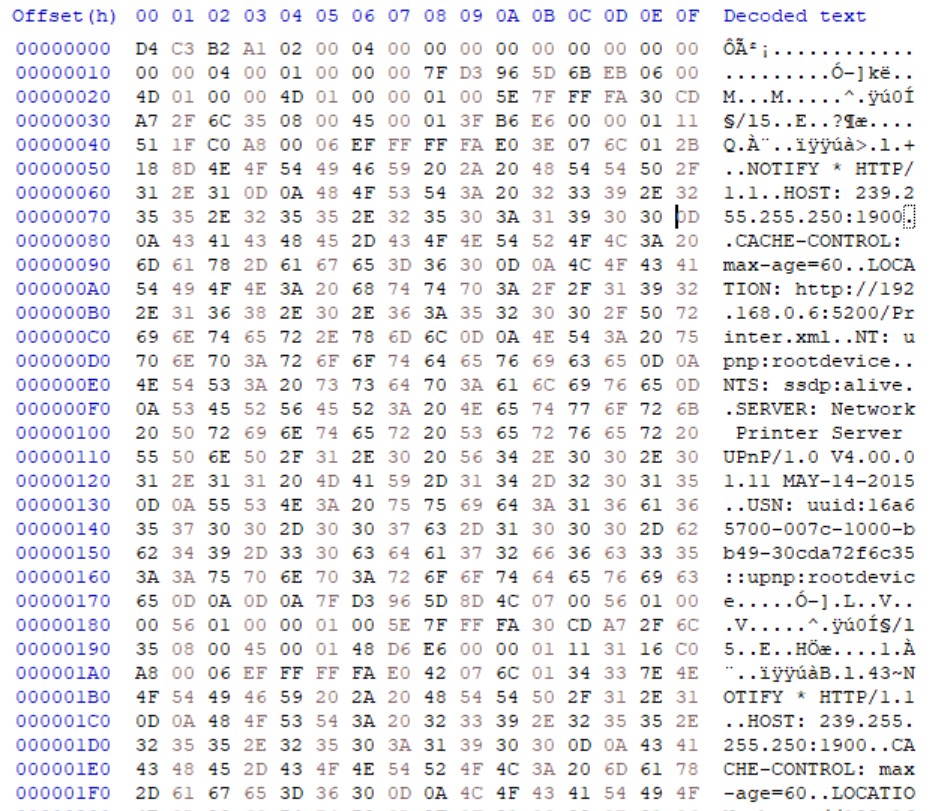
-NETWORK LAYER: IPv4, IPv6, ARP

-DATA LINK LAYER: 오류제어, 흐름제어. MAC ADDRESS

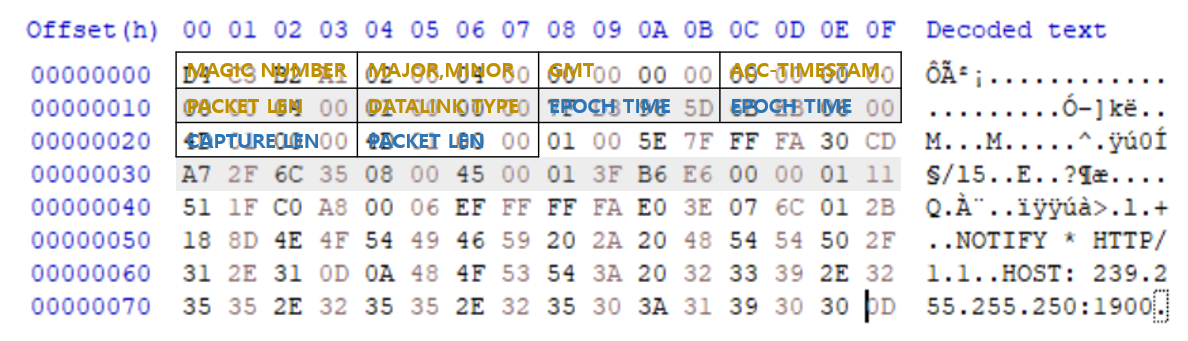
-PHYSICAL LAYER: 전기적 물리적 세부 사항 정의

\*ARP: 송,수신 IP외에 라우터의 주소를 알기 위해 사용하는 프로토콜

2. 패킷 분석



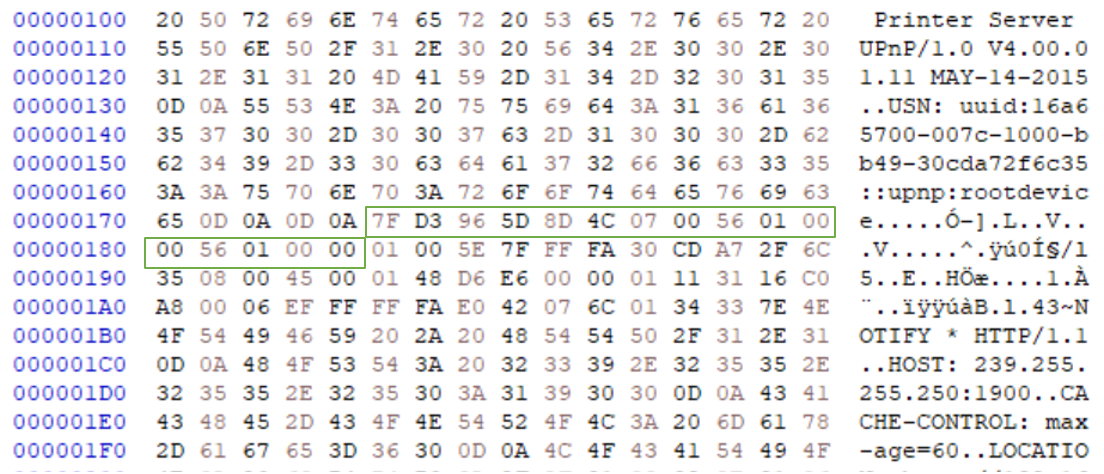
2-1 1ST GLOBAL HEADER & PACKET HEADER



-1ST PACKET LENGTH: 4D 01 00 00 = 333\_(10)

-NEXT PACKET HEADER: 28+14D=175

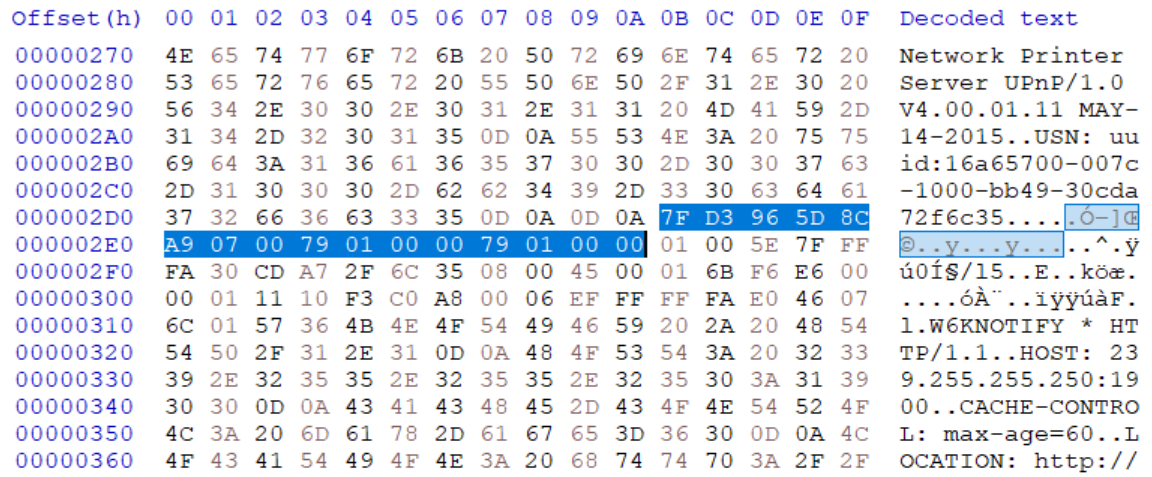
2-2 2ND PACKET HEADER



-2ND PACKET LENGTH: 56 01 00 00 = 342\_(10)

-NEXT PACKET HEADER: 185+156=2DB

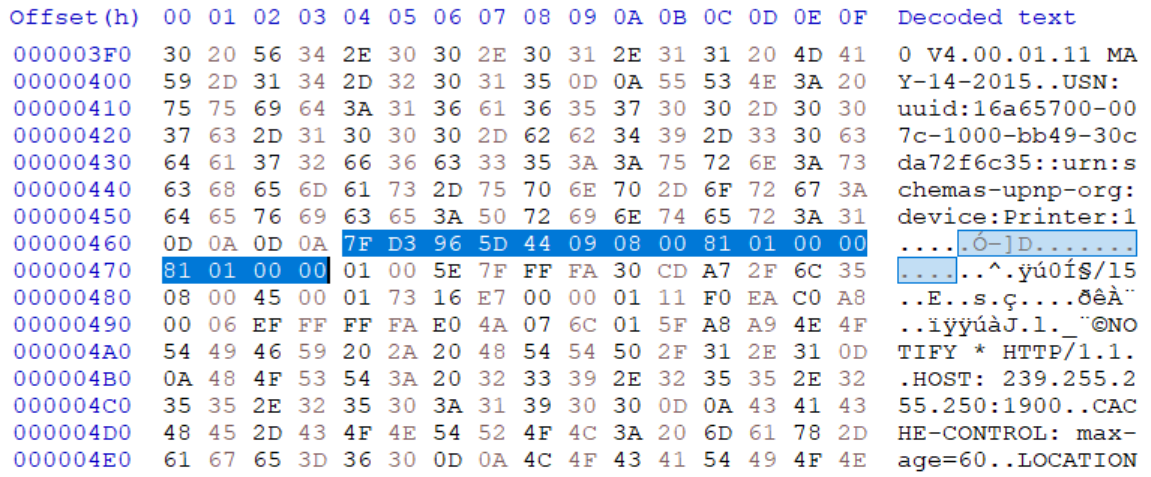
2-3 3RD PACKET HEADER



-3RD PACKET LENGTH: 79 01 00 00 = 377\_(10)

-NEXT PACKET HEADER: 179+2EB=464

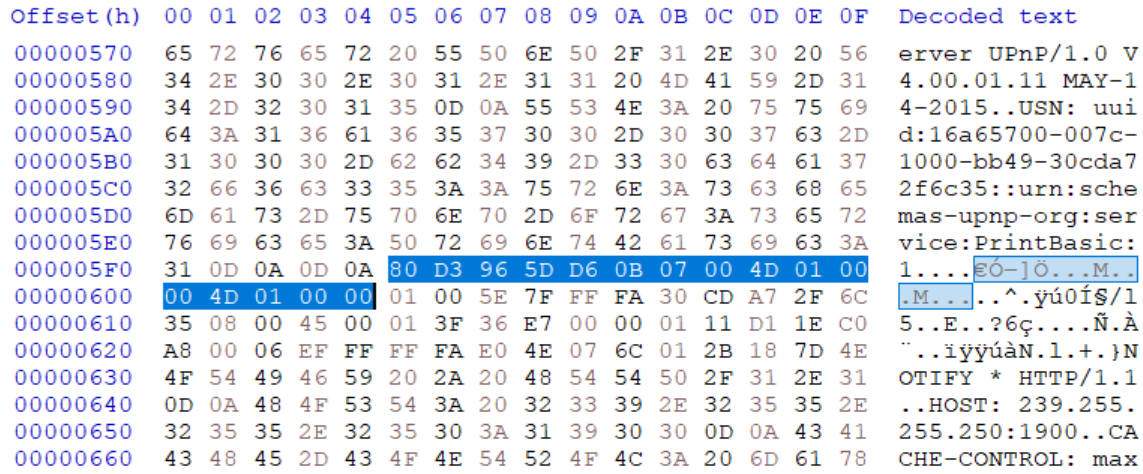
2-4 4TH PACKET HEADER



-4TH PACKET LENGTH:81 01 00 00 = 385\_(10)

-NEXT PACKET HEADER: 181+474=5F5

2-5 5TH PACKET HEADER



-5TH PACKET LENGTH:4D 01 00 00 = 333\_(10)

-NEXT PACKET HEADER: 14D+605=752

-5TH PACKET

