네트워크 포렌식 스터디

CERT-IS

양윤지

19.10.30.수요일

4장 FTP 패킷 분석

Follow Stream(개별 세션별로 필요에 따라 정보를 수집하여 보기)

FTP(File Transfer Protocol): TCP/IP 프로토콜, 서버와 클라이언트 사이의 파일 전송

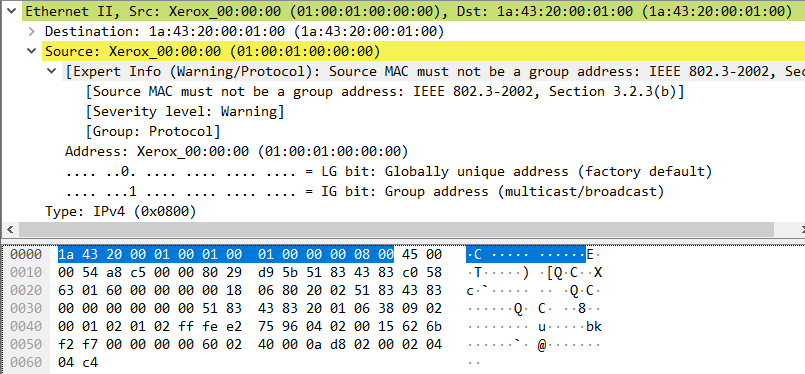
포트: TCP 21(사용자 인증 및 명령어 전달), 20(사용자의 명령 처리, 결과 전달)

\*\*어떤 ip에서 어떤 대상으로 접속했는지,

\*\*데이터에 포함 된 계정 및 암호 등의 정보 확인

0. chapter\_4.cap 분석

1. 이더넷 헤더



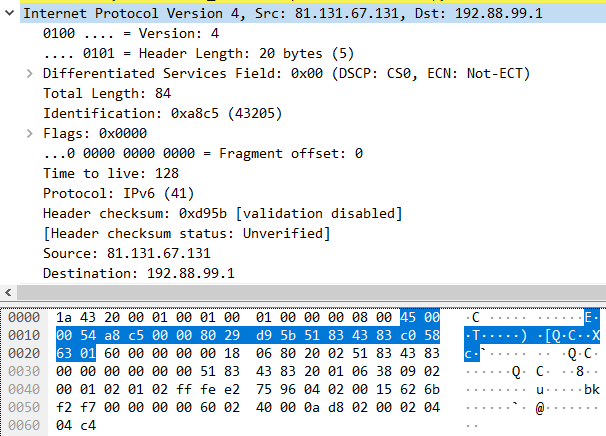
\*필드

-Destination(목적지 MAC 주소) : 1a:43:20:00:01:00

-Source(송신지 MAC 주소) : 01:00:01:00:00:00

-Type(이더넷 헤더 다음 헤더) : 08 00 = IP

2. IPv4 헤더



\*필드

-Version(IP 버전정보) : 4

-Header Length : 5 = 20Byte

-Differentiated Service Field : 0x00 (서비스종류 없음)

--

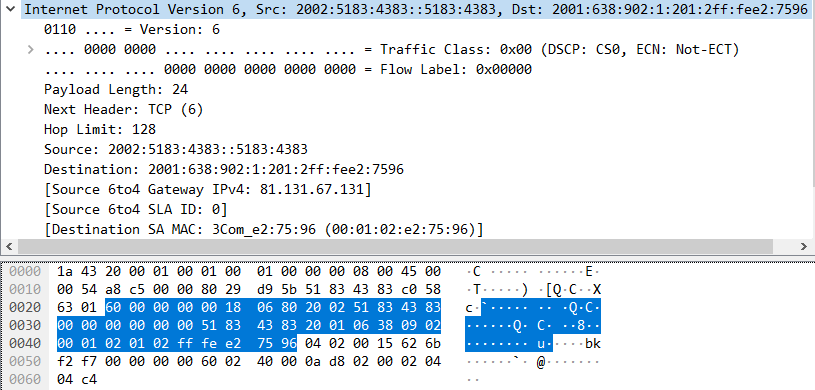
-Protocol(IPv4 다음 프로토콜) : 29 = IPv6

-Source : 51 83 43 83(=81.131.67.131)

-Destination : c0 58 63 01(=192.88.99.1)

3. IPv6 헤더

\*IPv4와 IPv6을 함께 사용하는 네트위크 망 때문에 공존



\*필드

-Version(IP 버전 정보) : 6

--

-Next header : 06(=TCP)

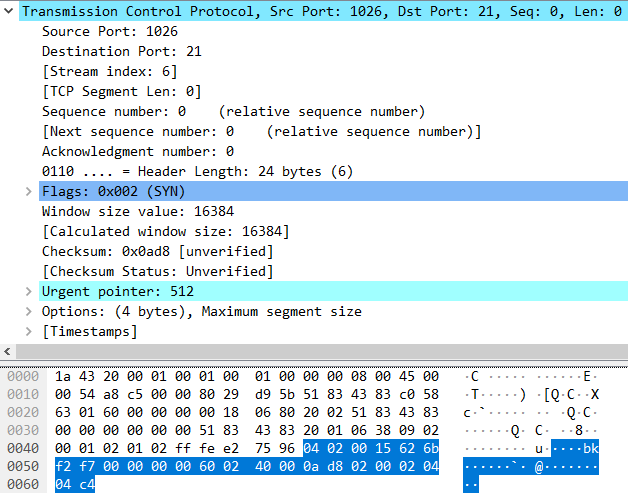
-Source : 20 02 51 83 43 83 00 00 00 00 00 00 51 83 43 83

(=2002:5183:4383::5183:4383)

-Destination : 20 01 06 38 09 02 00 01 02 01 02 ff fe e2

(=2001:683:902:1:201:2ff:fee2:7596)

4. TCP 헤더



\*필드

-Source Port(송신자의 Port) : 04 02(=1026) //얘는 왜 빅앤디언방식인가요?

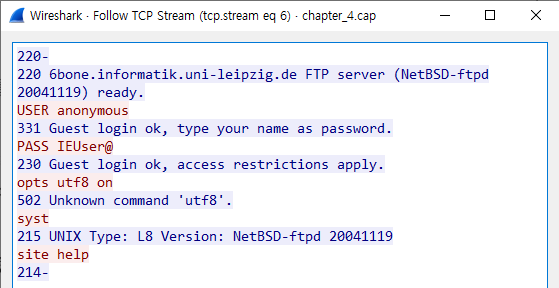
-Destination Port : 00 15(=21)

-Header Length : 60(=24bytes) //16진수 60=24\*8..??

5. FTP 데이터

: FTP 인증 및 데이터 전송 등의 정보 포함

\*\*Follow TCP Stream 명령어 사용



\*명령어

-USER anonymous :Anonymous 계정을 입력함

-PASS IEUser@ :IEUser@ 암호를 입력함 //암호가 230인가요??

-Opts utf8 on :잘못된 명령어 입력한 상태

-Syst :시스템 타입 리턴

-Site help :Site 다음의 명렁어 실행