4~7강 핵심 정리

4강\_FTP 패킷 분석

FTP -> File Transfer Protocol.

TCP/IP 프로토콜을 가지고 서버와 클라이언트 사이의 **파일 전송**을 하기 위한 프로토콜임.

(TCP/IP 테이블의) **응용** 계층 프로토콜.

<FTP 통신방식>

FTP => 2개의 포트번호를 사용하는 특징이 있음.

TCP 21, 20을 사용함.

21 : 사용자 인증. 명령어 전달.

20 : 명령 처리 후 결과를 전달.

<FTP 패킷 분석>

1. 어떤 IP에서 어떤 대상으로 접속했는지 전체적으로 파악.

Wireshark 상단의 Statistics에서 Conversation을 선택하면 전체 세션에 대한 정보를 확인할 수 있고, FTP라인을 선택 후 [Apply as Filter], [Selected], [A<->B]를 통해 필터 정책을 수행한다.

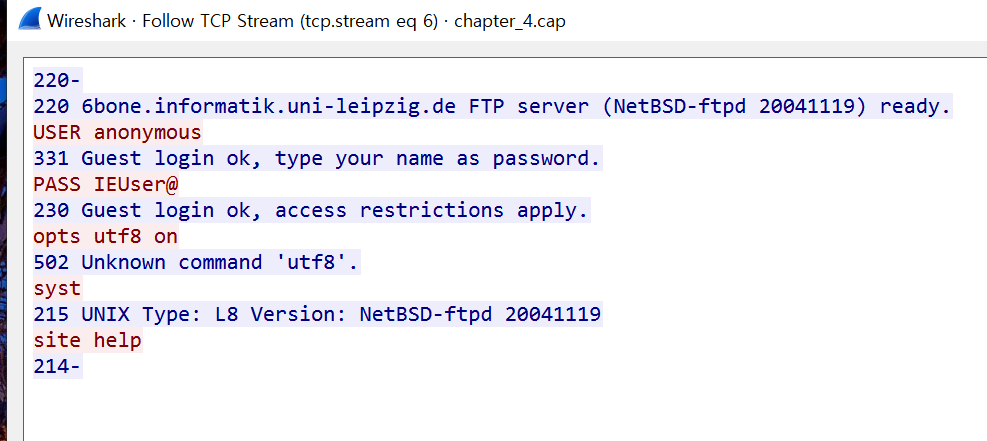
* 해당 세션에 대한 정보만을 제공한다.

그렇게 필터링 된 패킷들 중 하나를 선택하고 오른쪽 마우스 버튼 클릭

-> Follow TCP Stream 명령어 클릭

-> 여러 패킷의 정보를 수집해서 하나와 화면에

FTP인증 사용 정보 및 명령어 들을 보여줌.



이런 식으로 세션별로 필요 정보 수집(Follow Stream).

프로토콜을 상세히 확인.

-계정: anonymous

-암호: IEUser@

-502 Unknown command ‘utf8’ : 그 전에 입력된 명령어 ‘opts utf8 on’이 잘못됨을 알 수 있음.

-\*\* site 명령어 : site 다음의 명령어를 실행함. 여기서는 help를 시행.

5강\_Telnet 패킷 분석

Telnet : Telecommunication Network Protocol

자신이 **사용권한을 가지고 있다는 전제**를 가짐.

원격지에서 **다른 사람의 호스트 컴퓨터에 엑세스** 할 수 있는 기능을 제공함

그를 위한 사용자의 명령들과 TCP/IP 기반의 **어플리케이션** 계층 프로토콜.

<통신 방식>

접속 시 **서버 배너 정보**가 리턴됨.

프롬프트를 따라 계정과 패스워드를 입력하면 접속시간과 함께 프롬프트가 떨어짐.

\*\* 계정을 입력하면 echo현상이 발생함.

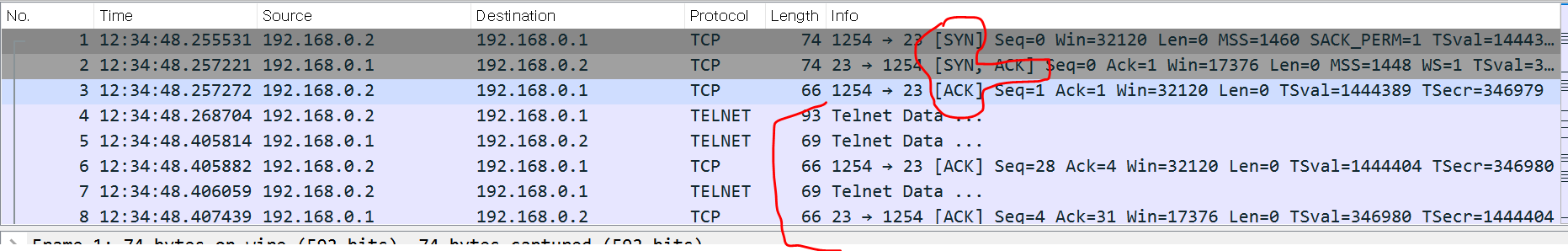
\*\*패스워드는 echo현상 존재 x.

<패킷 분석>

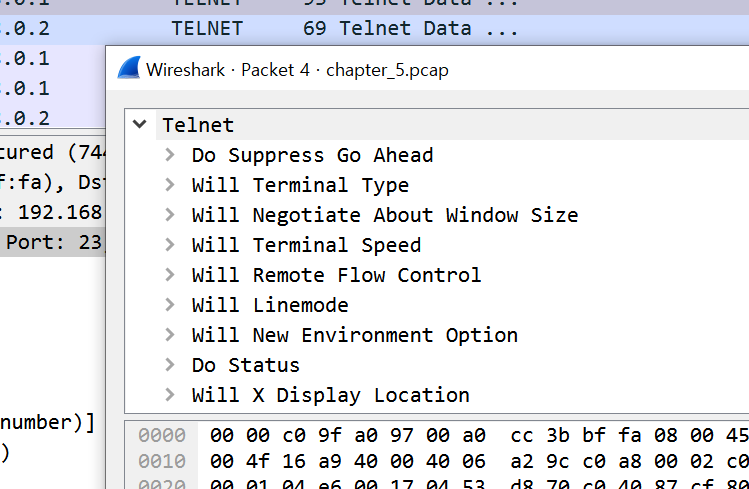
\*Statistics\_Conversations에 들어가면 TCP 탭에 Telnet만 존재함.

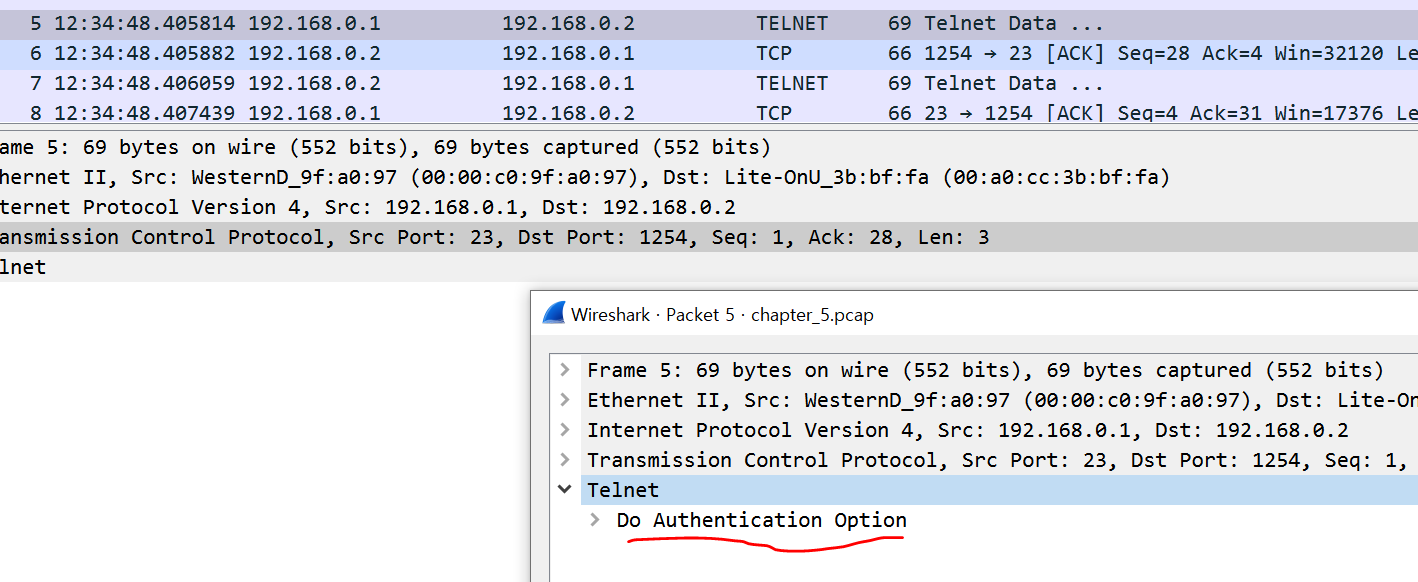
\*프로토콜 구조 : Ethernet, IP, TCP 헤더 + Telnet 데이터.

필터링 후를 보면, 제일 먼저 TCP가 세션 연결을 위해 3 way handshaking을 한 것을 볼 수 있고, 그 후 로그인 및 명령어 등을 사용한 내역을 볼 수 있다.



저런 식으로 내용을 주고받으면서 로그인, 명령어 사용의 과정을 거침.

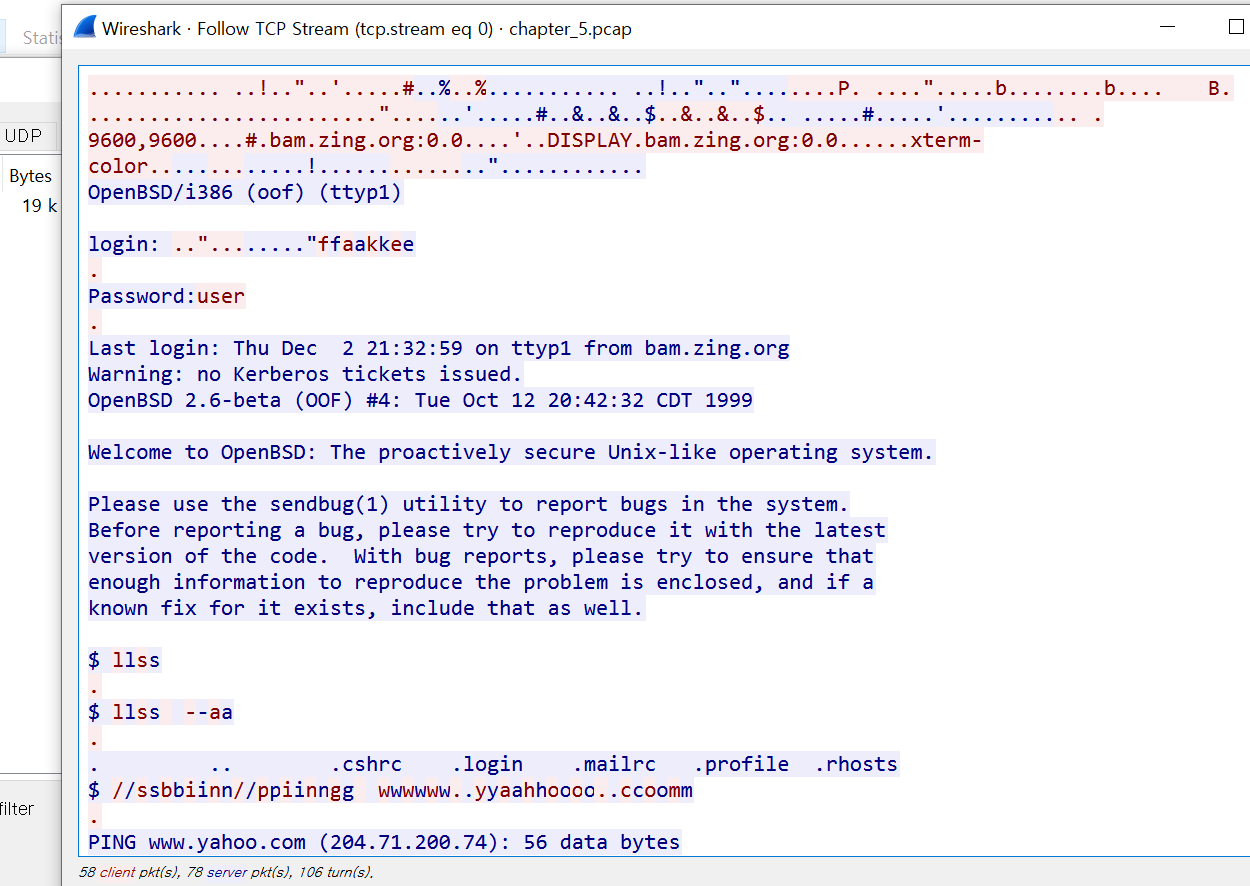


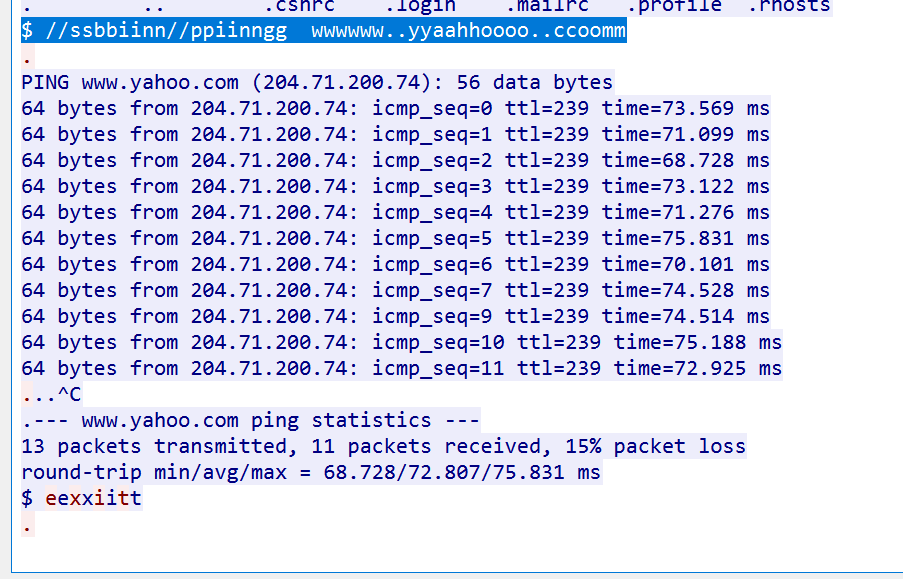


<Follow stream에서 확인할 수 있는 부분>

이러한 패킷들을 조합해서 본 follow stream

->





- 계정 : fake

(프롬프트에서 입력한 부분이 echo로 인해 fake가 ffaakkee와 같이 보이는 것 확인 가능)

- Pass word : user

- 계정 접속 후 Last login : (마지막) 로그인 시각이 21:32:59라는 것 확인 가능.

\* $ : 명령어 프롬프트.

- $IIss와 $IIss --aa : Is와 Is -a 명령어 사용. 명령어도 (서버에서 응답수신한)에코 발생.

- $ //ssbbiinn//ppiinngg wwwwww.yyaahhoooo..ccoomm

실제 명령어 : /sbin/ping [www.yahoo.com](http://www.yahoo.com)

yahoo페이지에 ping을 전송하라는 내용.

- $ exit => exit 명령어를 입력했음을 알 수 있음.

6강\_파일 Magic Number

File Magic Number를 통해서 **메신저 속 전송된 파일**을 분석할 수 있음.

와이어샤크를 통해 **메신저 분석** 가능.

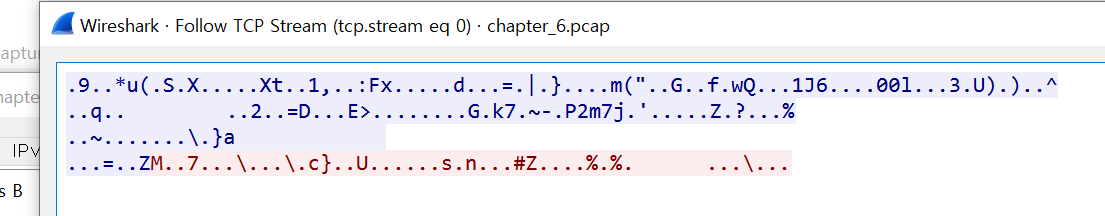
(Conversations를 통해 전체 내용을 파악하고, Follow Stream을 통해 통신내용 분석.

\*\* 그래도 확인되지 않는 정보 -> 필터링\*을 통해 상세히 분석.)

Cf) ▣ 마다 다른 세션 얘기임.

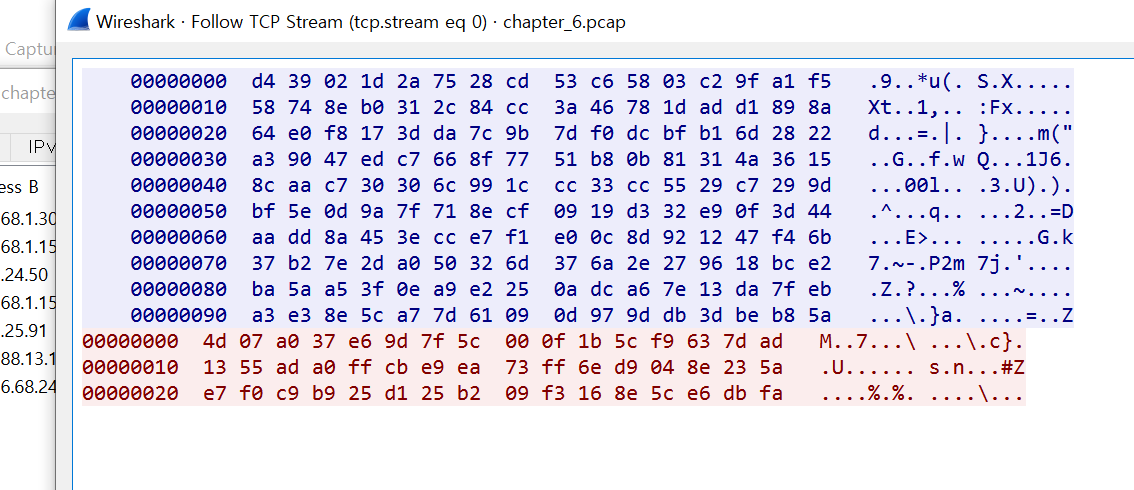
▣ TCP 22번 -> Telnet 등의 평문 데이터를 보호하기 위한 **암호화**를 처리하는 프로토콜임.

그래서 Follow Stream으로 수집 내용을 확인해도 **확인 불가능한 문자열**이 뜸.



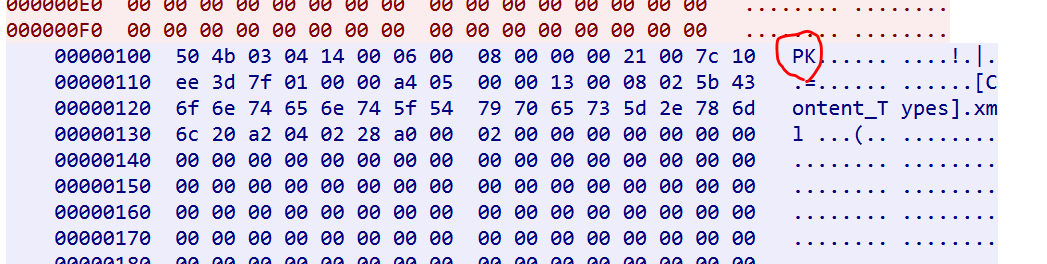
▣ Follow Stream의 구조를 다른 포맷으로 확인해서 정보 조합을 확인해보면, (ex. Hex dump)

Magic Number를 얻을 수 있다.



- 파일 포맷마다 고유한 Magic Number를 가지고 있음.

- 파일 종류를 확인, 추출 가능. (파일 종류마다 Magic number 다름) ex) PCAP : D4C3B2A1



=> 이 경우 Magic Number : PK.

ZIP코드 및 OFFICE 등 파일의 Magic Number임.

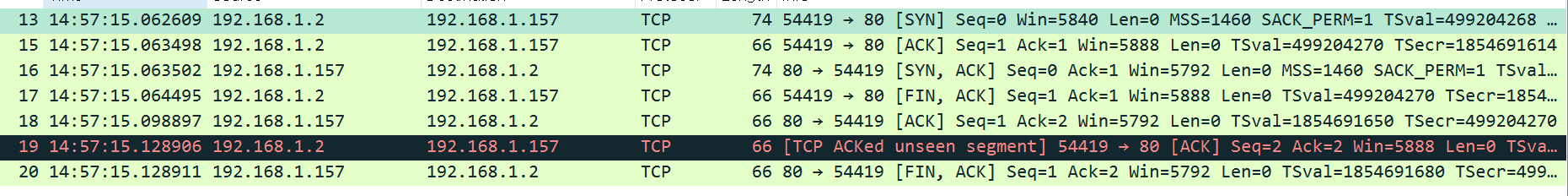
16진수 값 : 50 4b 03 04 14 00 06 00 => 검색 => office계열임(여기선 아마 docx?)

패킷에서 파일을 추출하려면(여기서는 docx를 추출해 볼 것) **불필요한 블록을 제거**해야 하는데, Hex Editor로 이 작업을 수행한다.

* OFT2 블록 다 제거하고 PK만 남기면 receipe.docx파일 추출됨.

▣ 주고 받은 데이터가 없는 경우도 있음.

* 단지 포트오픈여부를 확인한 경우.



(SYN, ACK, FIN, ACK 뿐)

▣ Follow Stream에서 어느 사이트에 어디를 경유해서 접속했는지 바로 알 수 있는 경우도 있음.



Refere가 경유지, Host가 목적지

7강\_HTTP 컨텐츠 분석

주제 : HTTP 패킷 내에 포함된 그림파일을 추출하는 방법.

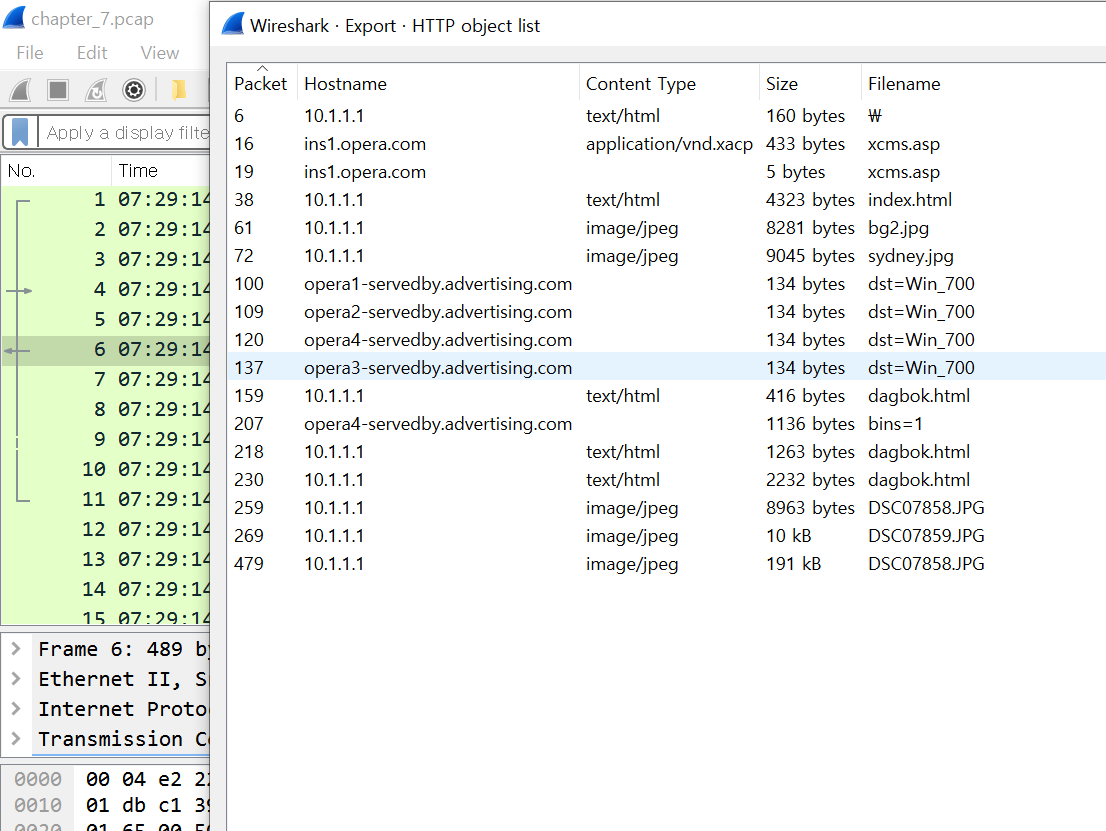
(와이어샤크의 기본 기능과 NetworkMiner라는 툴을 사용해 가능.)

<HTTP 컨텐츠 분석>

Magic number를 이용할 수도, NetworkMiner를 이용할 수도 있음

<Wireshark 이용>

File에서 HTTP objects들을 다 구하면(export objects)

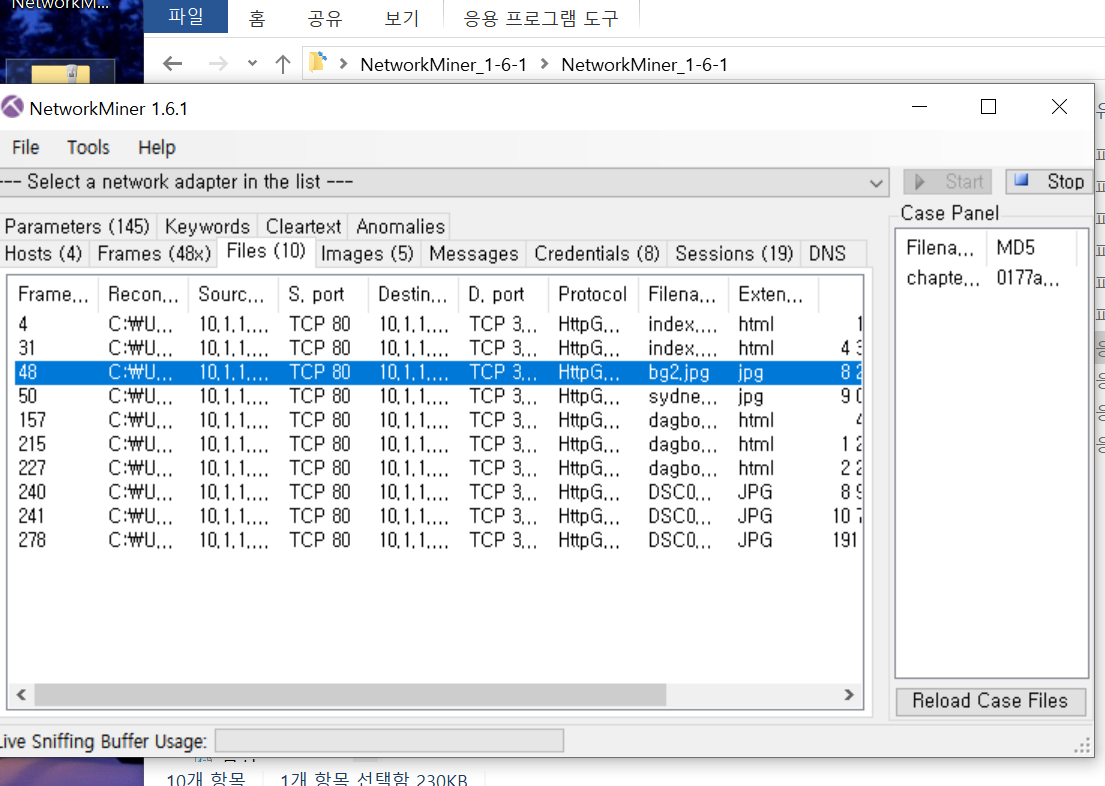


Content type에서, 패킷 내에 그림파일도 포함돼 있다는 걸 알수있음. 여기서 바로 [저장]으로 추출 가능

추출한 그림:



<Network Miner 사용>



Pcap파일 열어서 files 탭 선택

추출하려는 파일이 있는 라인을 선택

마우스 오른쪽 버튼 클릭

Open folder 메뉴 선택으로 그림파일 요청

=> images 탭에서 요청한 그림 확인 가능

