

컴퓨터보안 실습

네트워크 패킷 분석 및
데이터 추출

패킷 분석

- 간단한 툴을 사용하여 네트워크상에서 오가는 패킷 안의 데이터를 추출
- 패킷 캡처 및 분석 제출
- **kor_moon@naver.com**

패킷 분석

- 기본 파악

- 와이어 샤크 설치 및 사용법

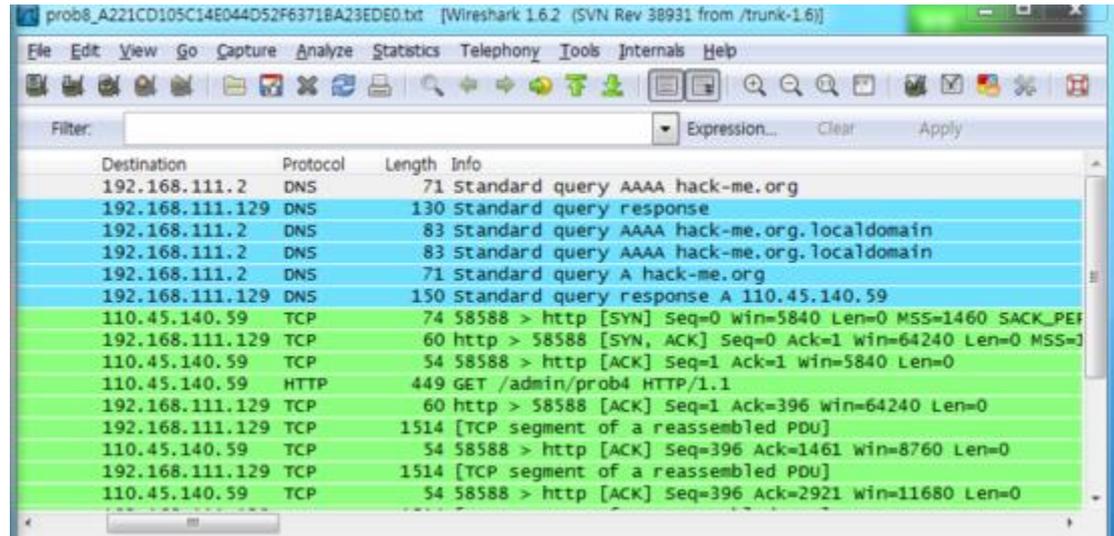
- <http://www.wireshark.org/>

또는 Smart Sniffer 사용

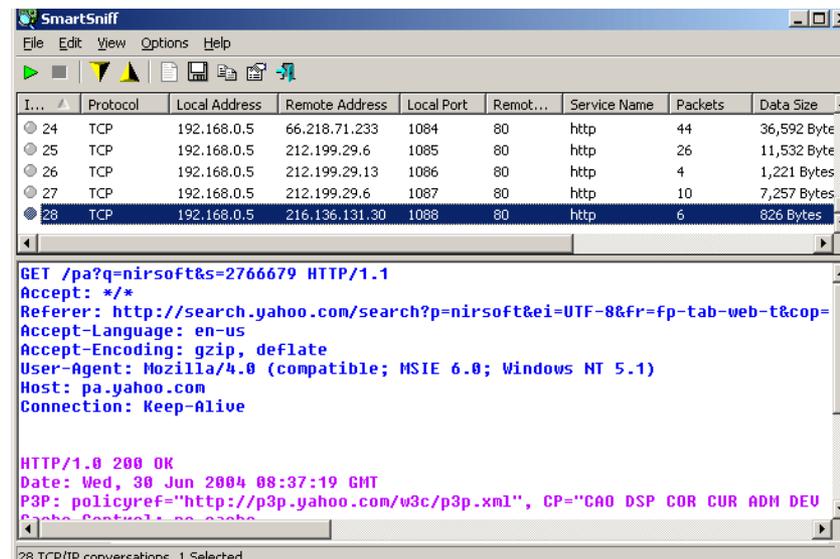
- www.nirsoft.net (networktools 배너 클릭)

패킷 분석

- 와이어 샤크



- Smart Sniffer



패킷 분석

- 의심스러운 파일 파악 – Magic Number
- 메시저는 간단하게 상대방과 채팅을 하거나, 파일 등을 첨부하여 전송할 수 있는 기능을 제공한다.
- 그러나 만약 이러한 내용을 누군가 가로채어 볼 수 있다면 어떨까?
- 네트워크 분석 툴을 통해 메시저 내용을 분석하거나 메시저를 통해 전송된 파일 등을 File Magic Number를 통해 추출하는 방법을 알아보도록 하자.

와이어샷크

- Conversations

The screenshot shows the 'Conversations: chapter_6.pcap' window in Wireshark. The 'TCP: 7' tab is selected, displaying a table of TCP conversations. The 'Name resolution' checkbox at the bottom left is checked and highlighted with a red box. Below the table are buttons for 'Help', 'Copy', 'Follow Stream', 'Graph A→B', 'Graph B→A', and 'Close'.

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000000	94.3298	20.86	24
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114000	0.0663	32819.52	24855.1
192.168.1.158	51128	64.12.24.50	443	40	4 303	20	1 681	20	2 622	18.870898000	72.1626	186.36	290.1
192.168.1.159	1221	64.12.25.91	443	40	6 005	16	1 799	24	4 206	34.025532000	57.0382	252.32	589.1
192.168.1.159	1271	205.188.13.12	443	47	31 168	16	1 451	31	29 717	34.211454000	1.2039	9642.08	197473.1
192.168.1.158	5190	192.168.1.159	1272	24	14 142	15	13 100	9	1 042	61.052925000	0.2848	367918.10	29264.1
192.168.1.159	1273	64.236.68.246	80	10	3 509	5	1 964	5	1 545	93.356969000	0.3618	43422.99	34159.1

- 메뉴 [statistics] – [Conversations]를 클릭하고, 포트를 이름으로 보는 대신 번호로 확인하기 위해 하 단의 [Name Resolution]을 체크오프 합니다

와이어샷크

- Conversations

Conversations: chapter_6.pcap

Ethernet: 11 Fibre Channel: FDDI IPv4: 14 IPv6: IPX JXTA NCP RSVP SCTP TCP: 7 Token Ring: UDP: 9 USB WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel Start	Duration	bps A→B	bps B→A
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000000	94.3298	20.86	24
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114000	0.0663	32819.52	24855.1
192.168.1.158	51128	64.12.24.50	443	40	4 303	20	1 681	20	2 622	18.870898000	72.1626	186.36	290.1
192.168.1.159	1221	64.12.25.91	443	40	6 005	16	1 799	24	4 206	34.025532000	57.0382	252.32	589.1
192.168.1.159	1271	205.188.13.12	443	47	31 168	16	1 451	31	29 717	34.211454000	1.2039	9642.08	197473.1
192.168.1.158	5190	192.168.1.159	1272	24	14 142	15	13 100	9	1 042	61.052925000	0.2848	367918.10	29264.1
192.168.1.159	1273	64.236.68.246	80	10	3 509	5	1 964	5	1 545	93.356969000	0.3618	43422.99	34159.1

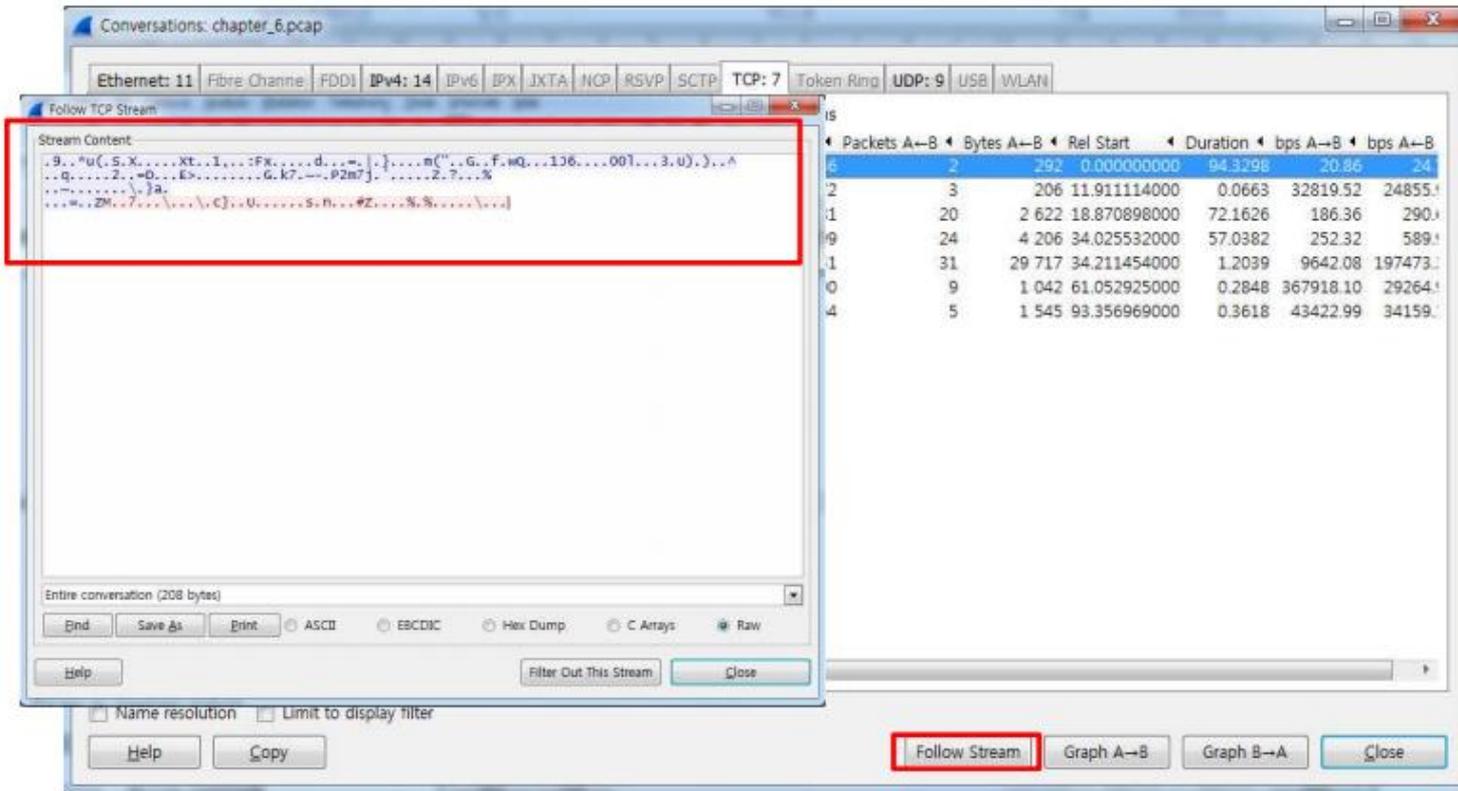
Name resolution Limit to display filter

Help Copy Follow Stream Graph A→B Graph B→A Close

- 첫 번째 세션의 경우, 통신의 방향은 Port A 55488에서 Port 22로 접속한다는 것을 알 수 있는데, TCP 22번은 Telnet 등의 평문데이터를 보호하기 위해 암호화 처리하는 프로토콜이다.

와이어샷크

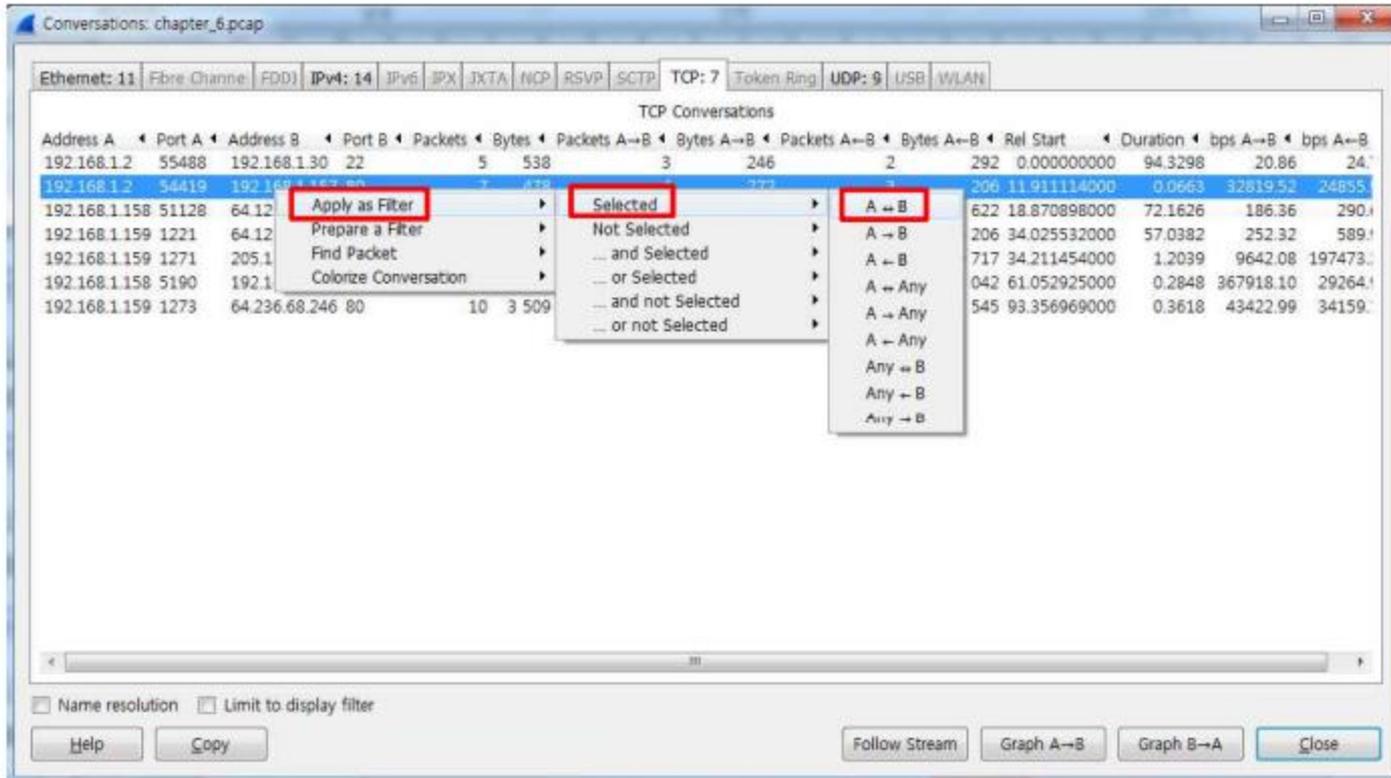
- Follow Stream



- 하단의 [Follow Stream] 클릭을 통해 패킷수집 내용을 확인해보면, 암호화 통신이기 때문에 문자열 확인이 불가능하다..

와이어샷크

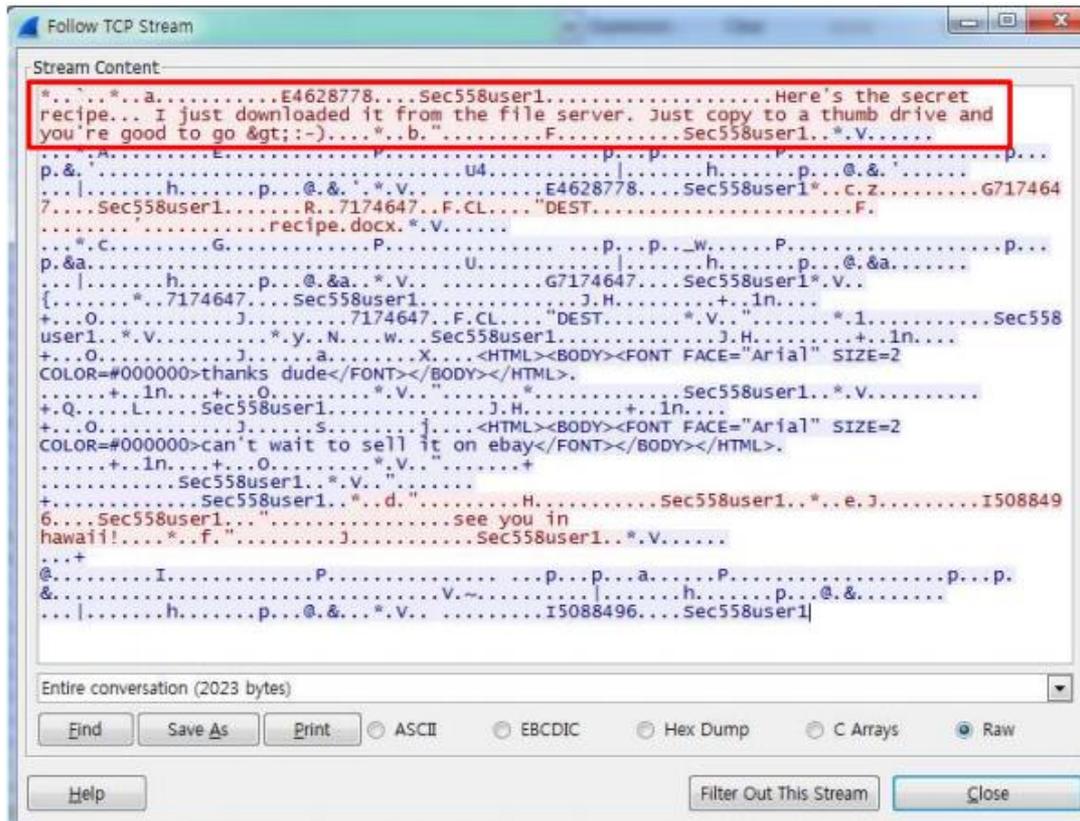
- Follow Stream



- 확인되지 않는 패킷정보는 필터링을 통해 상세분석 할 수있다. 아래 패킷에서 마우스 우클릭, [Apply as Filter]-[Selected]-[A<->B]를 클릭

와이어샷크

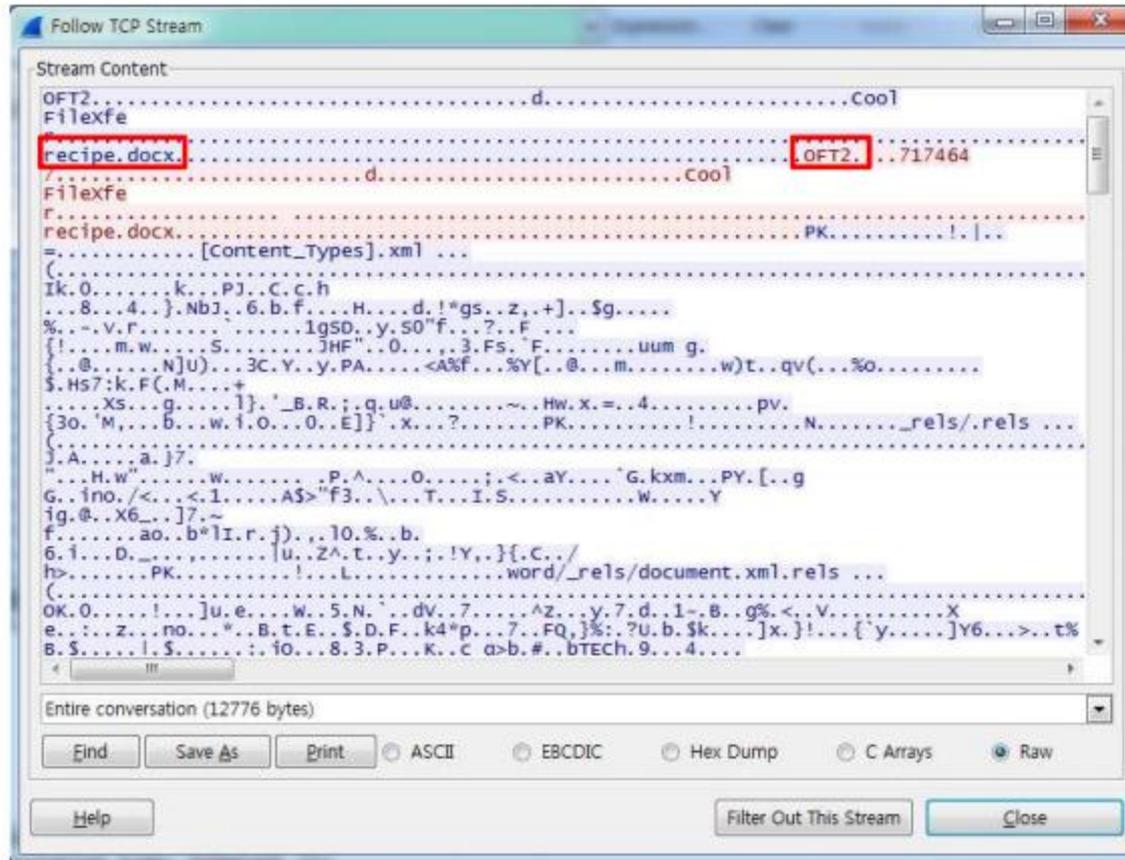
- Follow Stream



- 일부패킷은 [Follow stream]으로 확인해보면 HTTPS 통신임에도 불구하고, 일부 확인할 수 있는 문자열 등이 보인다.

와이어샷크

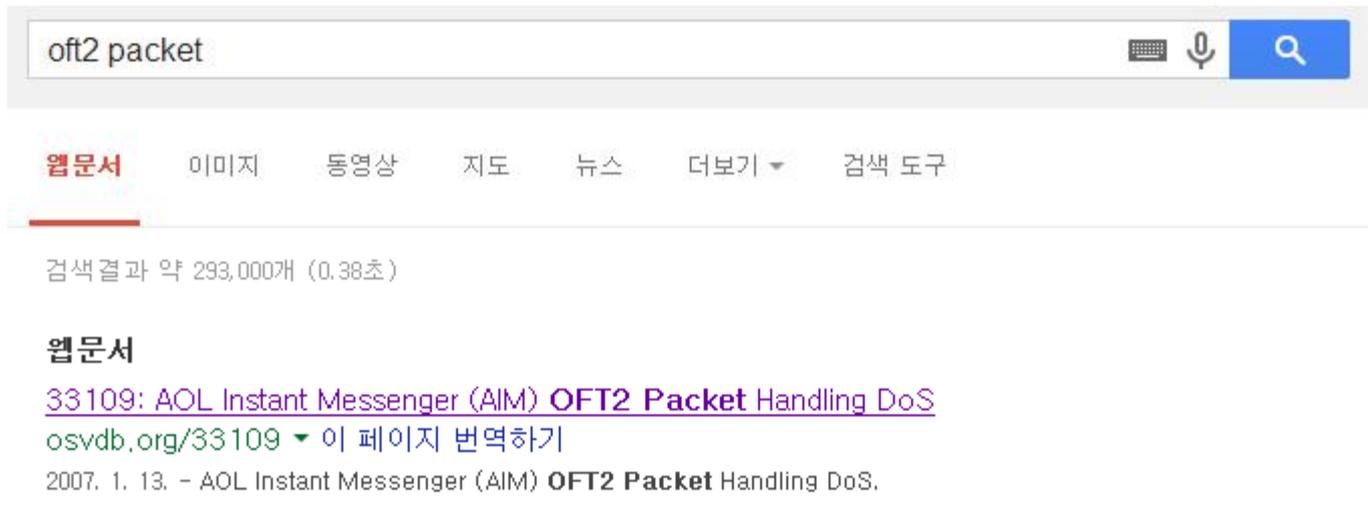
- 분석을 통한 파일 추출



[Follow Stream]을 통해 확인해 보면 OFT2 및 recipe.docx 등의 정보가 보이는 것을 알 수 있다.

와이어샷크

- 분석을 통한 파일 추출



The screenshot shows a search engine interface with the search term "oft2 packet" entered in the search bar. Below the search bar, there are navigation tabs for "웹문서" (Web Documents), "이미지" (Images), "동영상" (Videos), "지도" (Maps), "뉴스" (News), "더보기" (More), and "검색 도구" (Search Tools). The search results indicate approximately 293,000 results found in 0.38 seconds. The first result is a document titled "33109: AOL Instant Messenger (AIM) OFT2 Packet Handling DoS" from osvdb.org, dated 2007. 1. 13.

oft2 packet

웹문서 이미지 동영상 지도 뉴스 더보기 검색 도구

검색결과 약 293,000개 (0.38초)

웹문서

[33109: AOL Instant Messenger \(AIM\) OFT2 Packet Handling DoS](#)
[osvdb.org/33109](#) 이 페이지 번역하기

2007. 1. 13. - AOL Instant Messenger (AIM) OFT2 Packet Handling DoS.

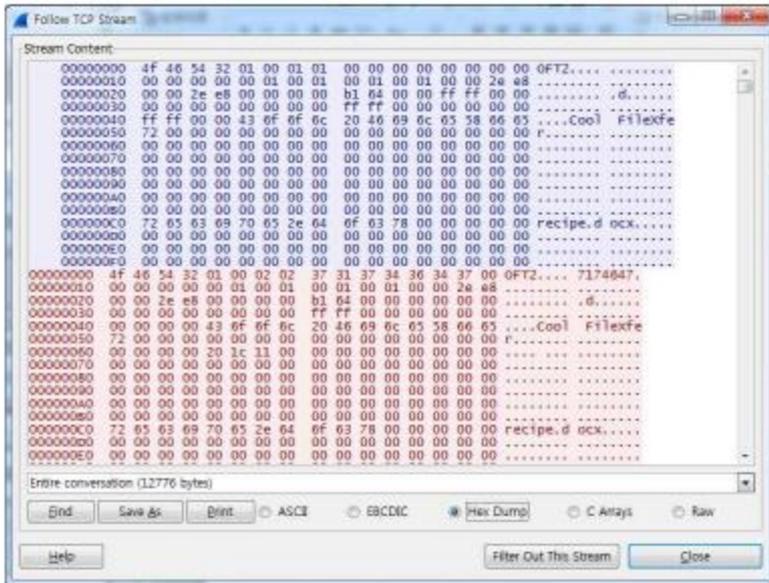
“OFT2 packet”으로 검색을 해보면 “AOL Instant Messenger”라는 정보를 제공하는데, 이를 통해 메신저 프로그램을 이용한 통신임을 가정해 볼 수 있다.

와이어샤크

- 분석을 통한 파일 추출



해당 [Follow Stream] 구조를 다른 포맷으로 확인하여, 어떤 정보들의 조합인지를 쉽게 확인해 볼 수 있는데, 대표적인 것이 Hex Dump라는 것이다.



Hex Dump를 체크하고 보면 색상이 다르게 구분된 것이 총 4개라는 것을 볼 수 있다.

와이어샷크

- 분석을 통한 파일 추출



OFT2는 메신저 통신내용으로 4개 중 3개를 차지하고 있는데, OFT2 블록마다 recipe.docx라는 문자열이 보인다. 여기서 세 번째 블록에 보이는 "PK"라는 문자열은 Magic Number 라는 값이다.

와이어샷크

- 분석을 통한 파일 추출

```
00000100 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 7c 10 PK. .... !. |.  
00000110 ee 3d 7f 01 00 00 a4 05 00 00 13 00 08 02 5b 43 ..[C  
00000120 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d ontent_T ypes].xm  
00000130 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 1 ... (.  
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

PCAP 포맷의 구조체에서 언급한 Magic Number라고 언급했었다. 파일포맷마다 고유의 Magic Number를 가지고 있어, 이를 통해 패킷 내에 포함된 파일종류를 확인하고, 추출해낼 수가 있다.

http://www.garykessler.net/library/file_sigs.html

위의 URL에서 파일포맷의 종류를 검색해 볼 수 있다.

와이어샷크

- 분석을 통한 파일 추출

```
00000100 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 7c 10 PK. .... !. |.  
00000110 ee 3d 7f 01 00 00 a4 05 00 00 13 00 08 02 5b 43 ..... [C  
00000120 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d ontent_T ypes].xm  
00000130 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 1 ... (. . . . .  
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... . . . . .
```

검색페이지에서 PK의 16진수 값 뒤에 함께 오는 값을 검색해 보면, OFFICE 계열의 포맷이라는 것을 확인할 수가 있다.

```
50 4B 03 04 14 00 06 00
```

DOCX, PPTX, XLSX

PK.....

Microsoft Office Open XML Format (OOXML) Document

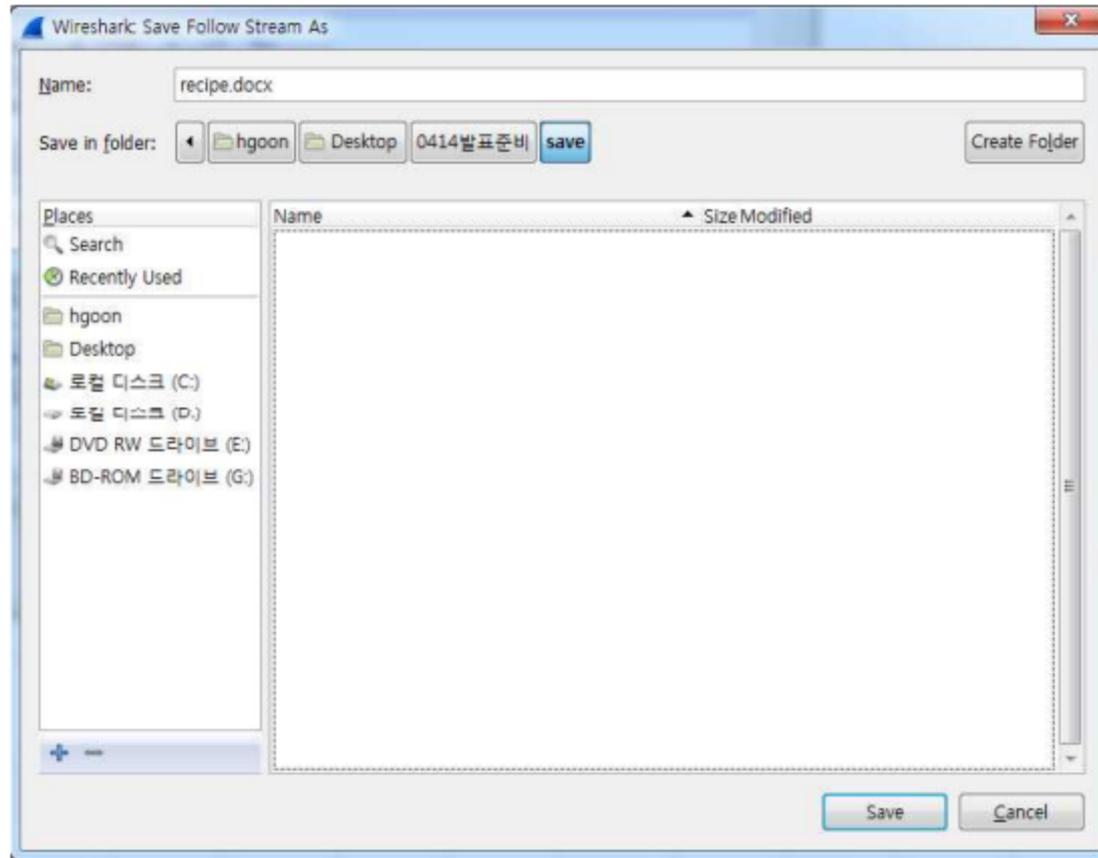
NOTE: There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively.

Trailer: Look for 50 4B 05 06 (PK..) followed by 18 additional bytes at the end of the file.

이로써 해당 블록이 OFT2 블록에서 보였던 recipe.docx라고 가정하고 접근해 볼 수 있다.

와이어샤크

- 분석을 통한 파일 추출



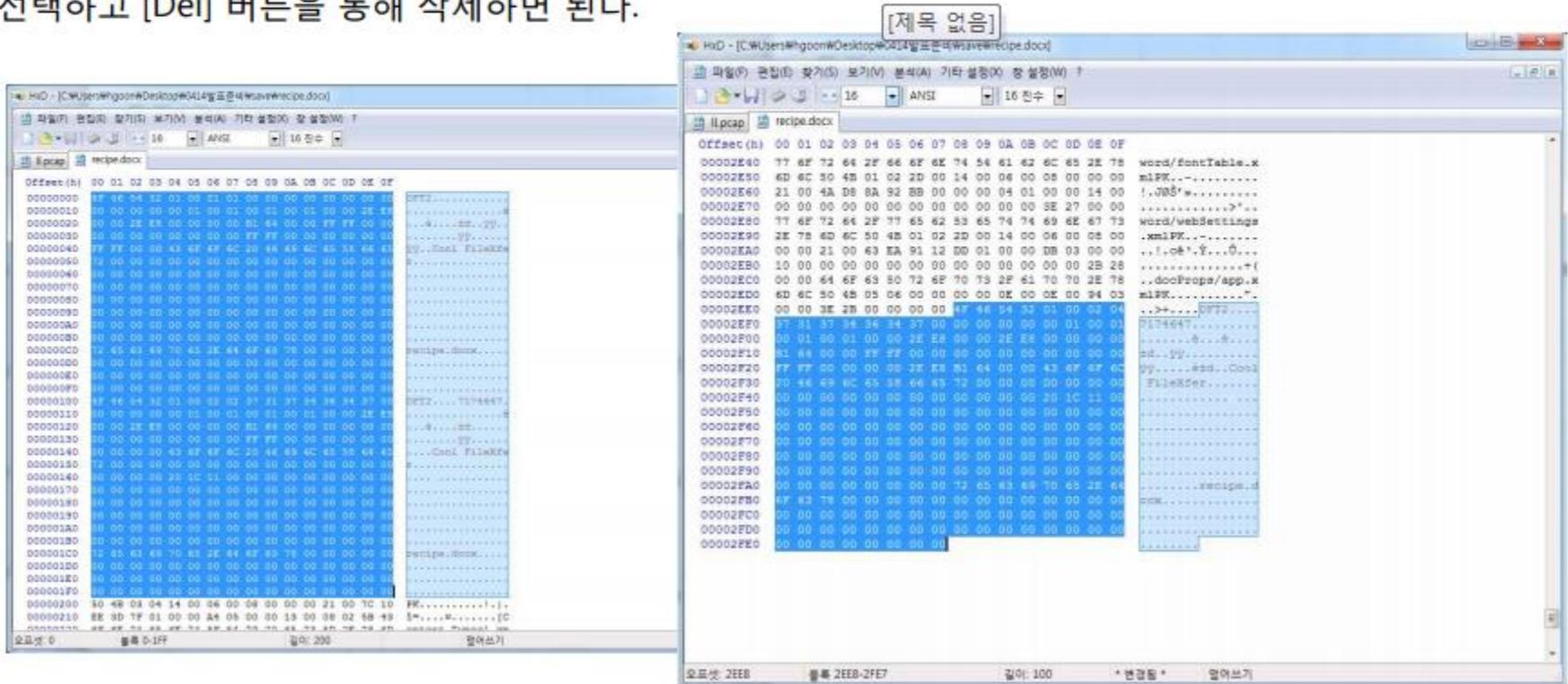
이제 패킷에서 파일(recipe.docx)을 추출하기 위해 하단의 파일포맷을 (Raw)을 선택하고, [Save as] 하여, recipe.docx라는 이름으로 저장한다.

와이어샤크

- 분석을 통한 파일 추출

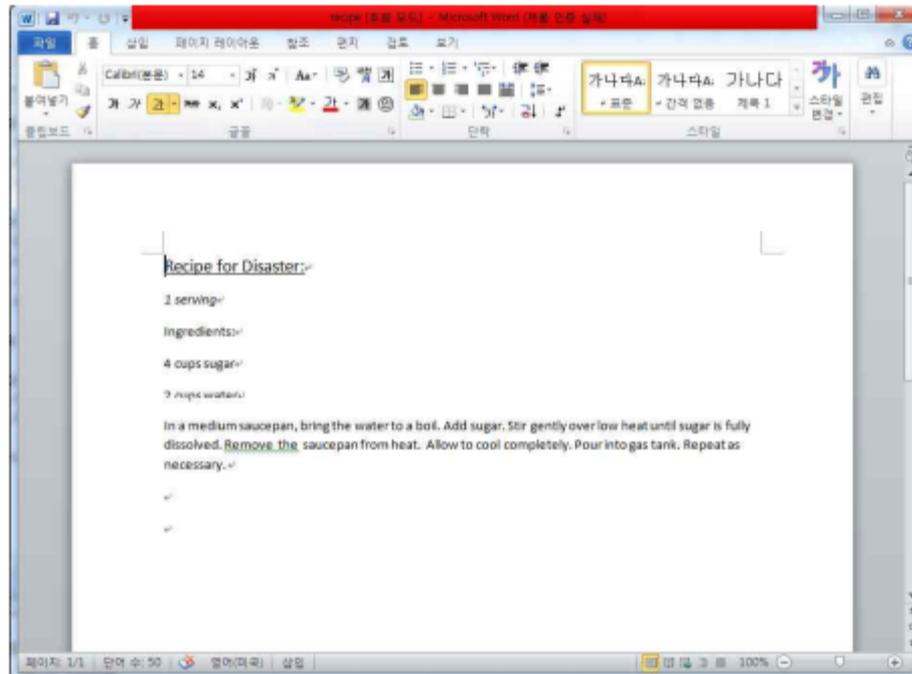
이 작업만으로 파일이 추출된 것은 아니며, 불필요한 부분인 OFT2블럭을 제거해야만 본래의 recipe.docx를 얻을 수 있다.

헥사 에디터에서 보이는 OFT2블럭을 삭제하기 위해 PK 값이 보이는 위쪽 부분을 마우스로 드래그하여 선택하고 [Del] 버튼을 통해 삭제하면 된다.



와이어샷크

- 분석을 통한 파일 추출



블록을 삭제하고 저장한뒤 recipe.docx 파일을 열면 위의 그림과 같이 "Recipe for Disaster" 라는 제목으로 시작하는 워드문서를 확인할 수 있다.

Q & A