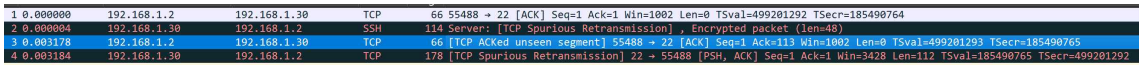


1	0.000000	192.168.1.2	192.168.1.30	TCP	66 55488 → 22 [ACK] Seq=1 Ack=1 Win=1002 Len=0 TSval=499201292 TSecr=185490764
2	0.000004	192.168.1.30	192.168.1.2	SSH	114 Server: [TCP Spurious Retransmission] , Encrypted packet (len=48)
3	0.003178	192.168.1.2	192.168.1.30	TCP	66 [TCP ACKed unseen segment] 55488 → 22 [ACK] Seq=1 Ack=113 Win=1002 Len=0 TSval=499201293 TSecr=185490765
4	0.003184	192.168.1.30	192.168.1.2	TCP	178 [TCP Spurious Retransmission] 22 → 55488 [PSH, ACK] Seq=1 Ack=1 Win=3428 Len=112 TSval=185490765 TSecr=499201292

포트 22로 SSH 연결 시도, 비정상적인 재전송 메시지가 있다. 네트워크 혼잡이나 패킷 손실을 의미한다.

Spurious Retransmission : 패킷이 손실되지 않았음에도 불구하고 재전송이 이루어진 경우

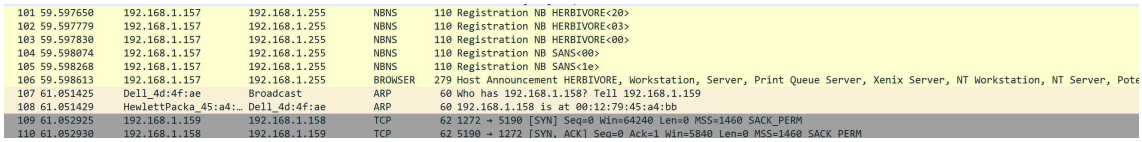
네 번째 패킷에서도 동일한 IP 주소 사이의 TCP 재전송이 있고, 암호화된 패킷으로 표시된다.

(패킷 7~9) NTP 패킷. 192.168.1.1, 192.168.1.10, 192.168.1.255 사이의 시간 동기화 활동을 나타낸다. NTP 버전 4가 사용되고, 클라이언트, 서버, 브로드캐스트로 설정되어 있다.

(패킷 12~19) 192.168.1.2와 192.168.1.157 간의 TCP 연결(포트 80)이 이루어진다. SYN, SYN-ACK, ACK 순서가 있으며, 이후 FIN 패킷을 통해 연결을 종료하는 과정.
포트 80을 사용으로, 간단한 HTTP 연결 시도일 가능성이 있다.

(패킷 21, 22) 192.168.1.30의 MAC 주소를 요청하는 ARP 패킷, 192.168.1.1이 192.168.1.30의 MAC 주소를 조회하고 있으며, 응답을 통해 00:0c:29:69:e6:2b의 MAC 주소를 받는다.

192.168.1.158과 64.12.24.50, 64.12.24.91 사이에 SSL/TLS 통신이 다수 진행되고 있다.
(패킷 23~35) 여러 패킷에 "Continuation Data"가 나타나며, 이는 SSL 데이터가 전송되고 있음을 나타낸다. 92.168.1.158이 64.12.24.50과 64.12.24.91에 걸쳐 TLS 버전 1을 사용하여 데이터를 교환하는 것을 볼 수 있다.



101	59.597650	192.168.1.157	192.168.1.255	NBNS	110 Registration NB HERBIVORE<20>
102	59.597779	192.168.1.157	192.168.1.255	NBNS	110 Registration NB HERBIVORE<03>
103	59.597830	192.168.1.157	192.168.1.255	NBNS	110 Registration NB HERBIVORE<00>
104	59.598074	192.168.1.157	192.168.1.255	NBNS	110 Registration NB SANS<00>
105	59.598268	192.168.1.157	192.168.1.255	NBNS	110 Registration NB SANS<1e>
106	59.598613	192.168.1.157	192.168.1.255	BROWSER	279 Host Announcement HERBIVORE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Pote
107	61.051425	Dell_4d:4f:ae	Broadcast	ARP	60 Who has 192.168.1.158? Tell 192.168.1.159
108	61.051429	HewlettPacka_45:a4:…	Dell_4d:4f:ae	ARP	60 192.168.1.158 is at 00:12:79:45:a4:bb
109	61.052925	192.168.1.159	192.168.1.158	TCP	62 1272 → 5190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
110	61.052930	192.168.1.158	192.168.1.159	TCP	62 5190 → 1272 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

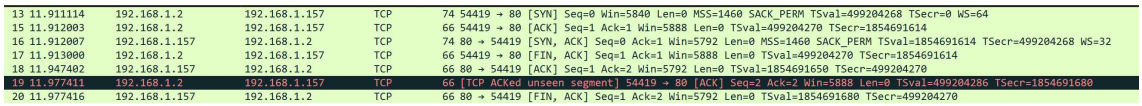
(패킷 101~106) NBNS는 네트워크에서 NetBIOS 이름을 IP 주소로 변환하는 데 사용된다. 여러 개의 "Registration NB" 메시지가 보이는데 192.168.1.157이 특정 이름을 등록하기 위해 NBNS 서버에 요청하고 있다는 것을 나타낸다. 각 패킷의 목적지는 192.168.1.255 브로드캐스트 주소로, 네트워크 내 모든 장치에 전송하는 것을 의미한다.

(패킷 107~110) ARP로 MAC 주소 요청하고 패킷 109~110은 SYN 요청하고, 그에 대한 ACK 응답 보내어 연결이 성공적으로 설정된다.

(패킷 170~173) 192.168.1.159에서 64.12.25.91로의 SYN 요청한 후 ACK 패킷과 함께 데이터 전송한다. 패킷 173은 TCP 재전송 패킷으로, 데이터가 손실되었거나 ACK가 수신되지 않아 재전송된 경우이다.

TCP 통해서 통신하는
(포트 22번) telnet 원격 접속할 때 사용하는 프로토콜, 평문 통신하니까 보안적으로 문제 있어서 ssh 통해서 대칭키와 비대칭키 사용해서 확인할 수 있다.
암호화해서 확인하기 어렵다

(포트 80번)



13 11.911114	192.168.1.2	192.168.1.157	TCP	74 54419 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=499204268 TSecr=0 WS=64
15 11.912003	192.168.1.2	192.168.1.157	TCP	66 54419 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=499204270 TSecr=1854691614
16 11.912007	192.168.1.157	192.168.1.2	TCP	74 80 → 54419 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1854691614 TSecr=499204268 WS=32
17 11.913000	192.168.1.2	192.168.1.157	TCP	66 54419 → 80 [FIN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=499204270 TSecr=1854691614
18 11.947402	192.168.1.157	192.168.1.2	TCP	66 80 → 54419 [ACK] Seq=1 Ack=2 Win=5792 Len=0 TSval=1854691650 TSecr=499204270
19 11.977411	192.168.1.2	192.168.1.157	TCP	66 [TCP ACKed unseen segment] 54419 → 80 [ACK] Seq=2 Ack=2 Win=5888 Len=0 TSval=499204286 TSecr=1854691680
20 11.977416	192.168.1.157	192.168.1.2	TCP	66 80 → 54419 [FIN, ACK] Seq=1 Ack=2 Win=5792 Len=0 TSval=1854691680 TSecr=499204270

접속 하고나서 바로 끊었다 라는 것만 확인할 수 있다. (=연결 가능한지만 확인함 (스캐닝 같은 느낌))

```
GET /adiframe/3.0/5113.1/221794/0/-1/size=120x90;noperf=1;alias=93245558;cfp=1;noaddonpl=y;artexc=all;artinc=art_image%2Cart_img
1x1%2Cart_3pimg%2Cart_text%2Cart_imgtrack;kvmn=93245558;target=_blank;aduho=360;grp=143115875;misc=143115875 HTTP/1.1
Accept: */*
Referer: http://www.aim.com/redirects/inclient/AIM_UAC_v2.adp?magic=93245558&width=120&height=90&sn=Sec558user1
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: at.atwola.com
Connection: Keep-Alive
Cookie: JEB2=4A839DDB6E65181C45921CB2F00016D8; ATTACID=a3Z0aWQ9MTU4NzdpYTAwYTh2Ymk=; ATTAC=a3ZzZWc9OTk5OTk6NTAyODA=; badsrfi=V0d
710994e8ccb8db64a83a07939b2; atdemo=a3ZhZz1hbTM6dWEzOTtrdnVnPTE7; AxData=; atdses=0
```

GET : 페이지 요청
http://www.aim.com/ 이 페이지를 보여달라
Host: at.atwola.com : 해당되는 페이지 보여달라

443 /
https - 암호화하는 것, 우리가 알 수 있는 것은 거의 없다. 문자열들 정도만 확인 가능하다.

443 /
16진수로 봐도 알 수 있는 내용은 없다.

1221 /
크게 확인할 것 없다.

1271 -> 1590

```
PK.........!.|..=............[Content_Types].xml ...(.....................................................................
.....................................................................................................................
.....................................................................................................................
.....................................................................................................................
.....................................................Ik.0.......k...PJ..C.c.h
...8...4..}.NbJ..6.b.f....H....d.!*gs..z,.+]..$g.....%..-.v.r.......`......1gSD..y.S0"f...?..F ...{!....m.w.....S........JHF"..
...,.3.Fs.`F........uum g.{..@......N]U)     ..3C.Y..y.PA.....<A%f...%Y[..@...m........w)t..qv(...%o.........$.Hs7:k.F(.M....+
.....Xs...g.....l}.'_B.R.;.q.u@........~..Hw.x.=..4.........pv.{3o.'M,...b...w.i.O...0..E]}`.x...?.......PK.........!.........
......._rels/.rels ...(.....................................................................................
.....................................................................................................................
.....................................................................................................................
.....................................................................................................................
.............................J.A.....a.}7.
"...H.w".....w.......  .P.^....O.....;.<..aY....`G.kxm...PY.[..g
G..ino./<...<.1.....A$>"f3..\...T...I        S...........W.....Y
ig.@..X6_..]7.~
```

1, 2, 4번째 블록이 OFT2(메신저 통신)로 시작하고 세번째 블록은 PK로 시작하는 것을 볼 수 있음. PK는 magic number로, pcap의 경우 파일 포맷마다 고유의 magic number를 가지고 있어 이를 통해 패킷 내에 포함된 파일 종류를 확인하고 추출할 수 있음.

▾ 16진수 형식으로 확인

```
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   l ...(.. ........
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

50 4b 03 04 14 00 06 00(magic number)을 구글링해보면, 파일 시그니처임을 알 수 있고, DOCX, PPTX, XLSX과 같은 microsoft office xml 포맷의 도큐먼트임을 알 수 있음.
→ 그러고 나서 다시 ascii로 확인하면 실제로 recipe.docx를 볼 수 있으므로 word 파일임을 알 수 있음.
(MZ: 실행 파일, PK: 어떠한 파일인지- 어떤 파일인지 확인하려면 안의 magic number를 봐야 함. , OFT2: 메신저)

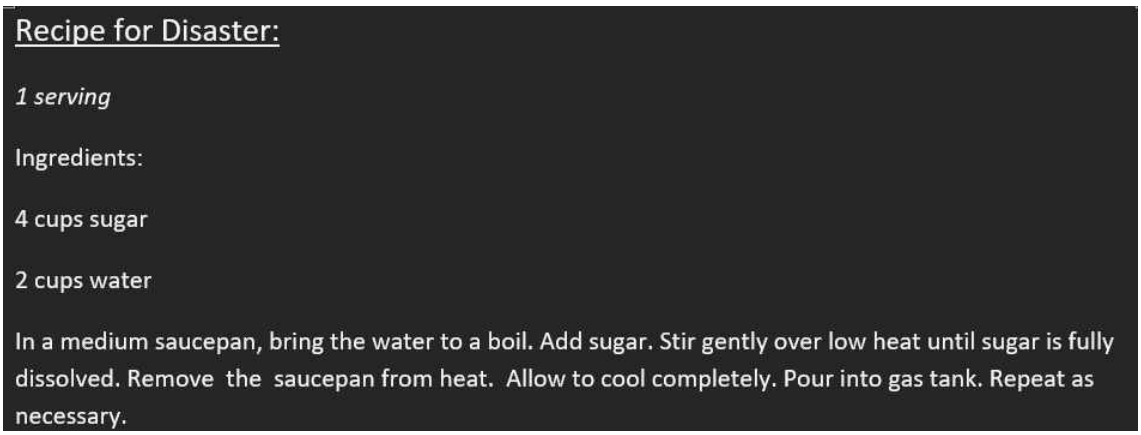
▾ HxD 통해 워드 파일 추출

c6 5

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   50 4B 03 04 14 00 06 00 08 00 00 00 21 00 7C 10  PK.........!.|.
00000010   EE 3D 7F 01 00 00 A4 05 00 00 13 00 08 02 5B 43  i=....¤.......[C
00000020   6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
00000030   6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l ¢..( .........
00000040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

세 개의 OFT2 블록을 삭제하고 PK 블록만 남긴 후 저장하여 docx 파일 추출.

해당 파일을 열어보면



위와 같은 내용을 확인할 수 있음.