



[Ann's Deception] Write-Up

작성자	류나연
분석 일자	2024.05.17
작성 일자	2024.05.18
분석 대상	Defcon2011-Contest.tc
문서 버전	1.0
작성자 E-mail	01star01ek@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....9

6. 별도 첨부 10

7. Reference 11

1. 문제

URL	https://forensicscontest.com/2011/08/16/puzzle-9-anns-deception-defcon-2011
문제 내용	The lead chemist of a high-profile pharmaceutical company was involved in a serious accident, leaving him in a coma days before the release of the company's highly publicized "133t pill." The chemist was the only person in possession of the list of ingredients required to produce the wonder drug, and it is not known if he will ever recover. All chemical evidence of the drug has been destroyed, but the company believes that the missing ingredients may have been stored electronically. <u>You have been hired as a forensic investigator, to recover the final ingredient of their 133t pill.</u> Can you find the missing ingredient?
문제 파일	<div>  </div> Defcon2011-Contest.tc
문제 유형	네트워크 포렌식
난이도	? / 5

2. 분석 도구

도구명	다운로드 링크	Version
True Crypt	https://truecrypt.softonic.kr/	V 7.2
WireShark	https://www.wireshark.org/download.html	4.0.10

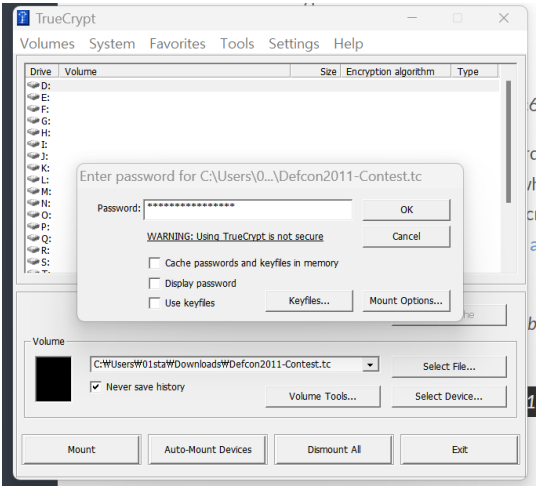
3. 환경

OS
Windows 11 Home, Ubuntu 2204

4. Write-Up

파일명	Defcon2011-Contest.tc
용량	50.0MB
SHA256	6906e4a08bd498c6ff78928b1c8d292a9f89f2ecfac60094528f4497e2254474
Timestamp	2024-05-17 17:38:03

1.tc 파일 확인 및 암호 해제



[사진 1] 암호를 해제하는 모습

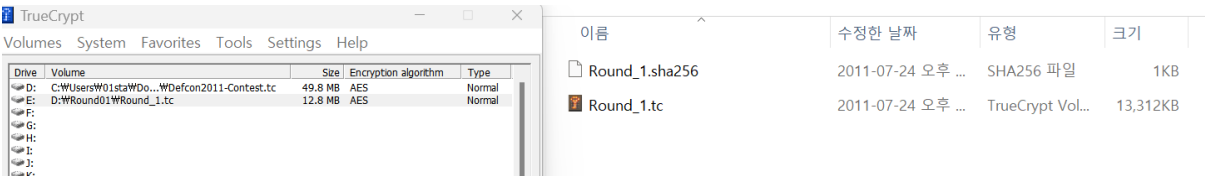
해당 파일의 형식은 tc로 암호화된 가상 디스크이기에 True Cypt 도구를 사용하여 암호화를 해제 해주었다.

이름	수정된 날짜	유형	크기
.Trashes	2011-07-25 오전 ...	파일 폴더	
Round01	2011-07-25 오전 ...	파일 폴더	
Round02	2011-07-25 오전 ...	파일 폴더	
Round03	2011-07-25 오전 ...	파일 폴더	
Round04	2011-07-25 오전 ...	파일 폴더	
Round05	2011-07-25 오전 ...	파일 폴더	
Round06	2011-07-25 오전 ...	파일 폴더	
System Volume Information	2024-05-18 오전 ...	파일 폴더	
휴지통	2024-05-18 오전 ...	파일 폴더	
..Trashes	2011-07-25 오전 ...	TRASHES 파일	4KB

[사진 2] 해당 디스크 안에 들어있는 내용

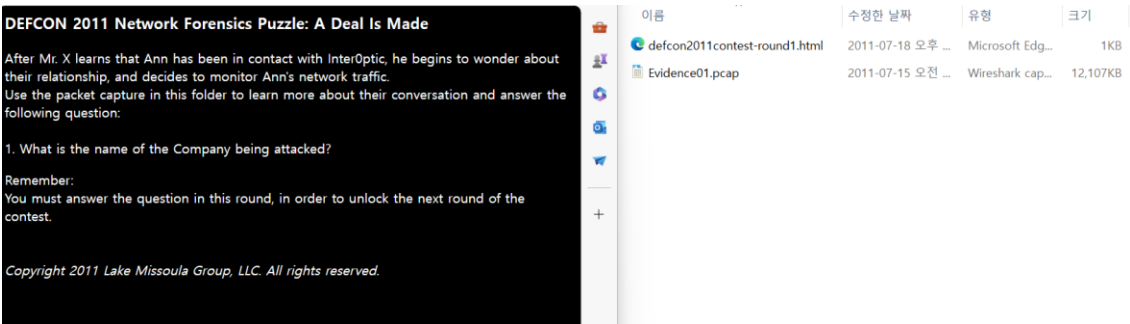
암호가 해제된 가상 디스크에는 총 6라운드의 문제가 들어있었다. 이에 따라 각 라운드를 해결하고자 하였다.

2-1. Round01 암호 파일 해제 및 문제 확인



[사진 3] Round01.tc 파일 암호 해제

첫 라운드의 폴더를 들어가보니 암호화된 가상 디스크를 발견할 수 있었다. 이에 따라 이전과 동일한 방법으로 암호를 해제해주었다.



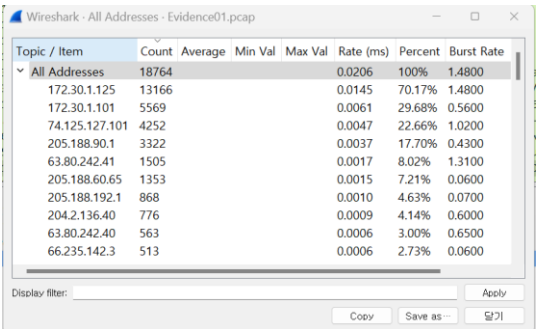
[사진 4] Round1 문제 확인

암호를 확인해보니 해당 디스크안에는 html 파일과 pcap 파일이 들어있었다.

문제는 1. What is the name of the Company being attacked? 이다.

따라서 해당 문제의 답을 찾으려고 노력하였다.

2-2. PCAP 구조 파악

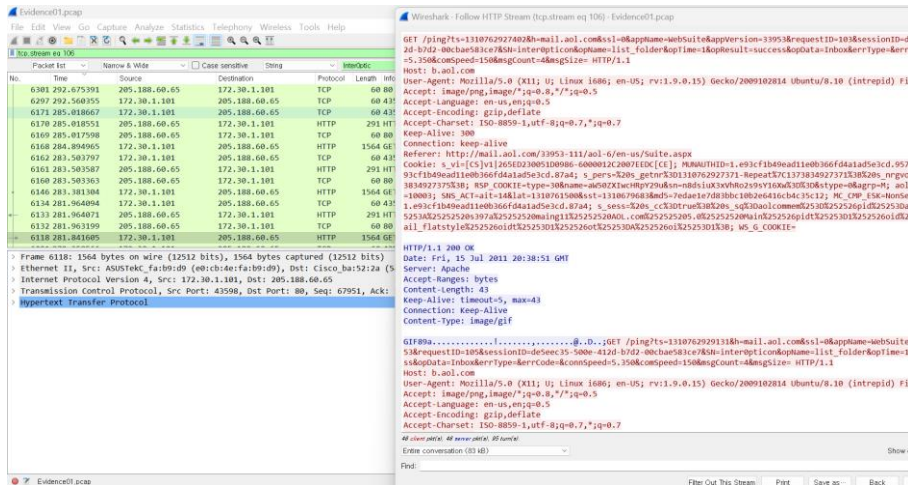


[사진 5] 와이어샤크를 통해 도출한 통신한 ip4 주소

[WHS-2] .iso

와이어샤크를 통해 기본적으로 한 번 훑으며 특이사항을 파악하였다. mail관련 키워드가 많아 이에 주목했으며 와이어샤크의 통계 기능을 활용하여 어떠한 ip들과 가장 많이 통신했는지 확인하였다.

2-3. 분석



The image shows a Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows several packets, with packet 6118 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The HTTP section shows a GET request to a mail.aol.com URL.

[사진 6] 와이어샤크를 통한 패킷 분석

이에 따라 다양한 방법으로 분석을 시도하였다. 해본 방법은

1. InterOptic 키워드 검색을 통한 관련 stream 확인
2. 가장 많은 통신이 있던 ip 172.30.1.125 추적 (ip.addr == 172.30.1.125)
3. Company, Firm 등의 회사 관련 키워드 검색
4. Mail 관련 http stream 확인 -> webmail 중 aol.com 추적
5. Tcp dup ack 가 다량으로 발생한 지점 조사
6. http 통신 조사

해당 과정에서 배운 새로운 사실은 gzip 으로 압축된 데이터를 볼 때에는 HTTP 스트림을 보는 것이 가장 일반적인 방법이라는 것이다.

결국 정답을 찾은 방법은

strings [파일명] | grep company 명령어를 사용한 것으로

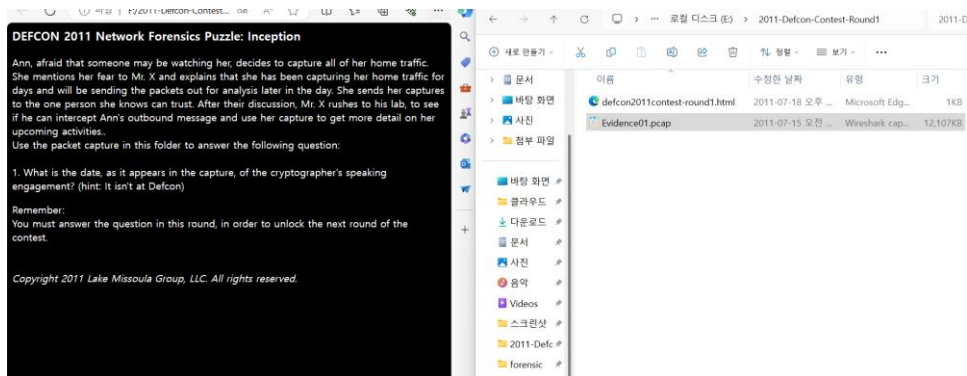
[WHS-2] .iso



[사진 7] strings 명령어로 정답을 찾은 사진

해당 명령어의 결과로 나온 무수한 글자들 사이에서 답을 발견할 수 있었다.

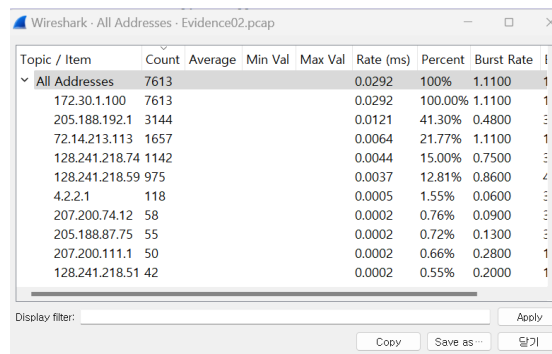
3-1. Round02 암호 파일 해제 및 문제 확인



[사진 8] Round02 문제 확인

Round01의 정답 확인을 통해 동일한 답을 확인한 뒤 알려진 암호키를 통해 다음 단계의 문제 또한 암호를 해제하여 확인하였다. 이번 문제는 **1. What is the date, as it appears in the capture, of the cryptographer's speaking engagement? (hint: It isn't at Defcon)** 이었다.

3-2. PCAP 구조 파악



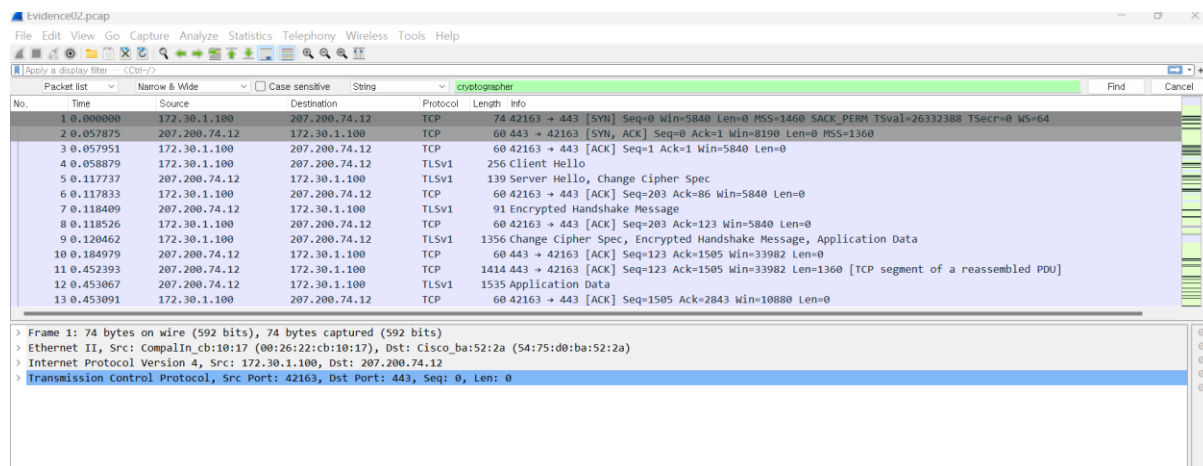
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate
All Addresses	7613				0.0292	100%	1.1100
172.30.1.100	7613				0.0292	100.00%	1.1100
205.188.192.1	3144				0.0121	41.30%	0.4800
72.14.213.113	1657				0.0064	21.77%	1.1100
128.241.218.74	1142				0.0044	15.00%	0.7500
128.241.218.59	975				0.0037	12.81%	0.8600
4.2.2.1	118				0.0005	1.55%	0.0600
207.200.74.12	58				0.0002	0.76%	0.0900
205.188.87.75	55				0.0002	0.72%	0.1300
207.200.111.1	50				0.0002	0.66%	0.2800
128.241.218.51	42				0.0002	0.55%	0.2000

[사진 9] 와이어샤크를 통해 도출한 통신한 ip4 주소

와이어샤크를 통해 기본적으로 한 번 훑으며 특이사항을 파악하였다. 모든 통신이 172.30.1.100

을 바탕으로 진행됨을 알 수 있었다.

3-3. 분석



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.1.100	207.200.74.12	TCP	74	42163 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=26332308 TSecr=0 WS=64
2	0.057875	207.200.74.12	172.30.1.100	TCP	60	443 → 42163 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360
3	0.057951	172.30.1.100	207.200.74.12	TCP	60	42163 → 443 [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	0.058879	172.30.1.100	207.200.74.12	TLSv1	256	client Hello
5	0.117737	207.200.74.12	172.30.1.100	TLSv1	139	Server Hello, Change Cipher Spec
6	0.117833	172.30.1.100	207.200.74.12	TCP	60	42163 → 443 [ACK] Seq=203 Ack=86 Win=5840 Len=0
7	0.118409	207.200.74.12	172.30.1.100	TLSv1	91	Encrypted Handshake Message
8	0.118526	172.30.1.100	207.200.74.12	TCP	60	42163 → 443 [ACK] Seq=203 Ack=123 Win=5840 Len=0
9	0.120462	172.30.1.100	207.200.74.12	TLSv1	1356	Change Cipher Spec, Encrypted Handshake Message, Application Data
10	0.184979	207.200.74.12	172.30.1.100	TCP	60	443 → 42163 [ACK] Seq=123 Ack=1505 Win=33982 Len=0
11	0.452393	207.200.74.12	172.30.1.100	TCP	1414	443 → 42163 [ACK] Seq=123 Ack=1505 Win=33982 Len=1360 [TCP segment of a reassembled PDU]
12	0.453067	207.200.74.12	172.30.1.100	TLSv1	1535	Application Data
13	0.453091	172.30.1.100	207.200.74.12	TCP	60	42163 → 443 [ACK] Seq=1505 Ack=2843 Win=10880 Len=0

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 > Ethernet II, Src: CompalIn_cb:10:17 (00:26:22:cb:10:17), Dst: Cisco_ba:52:2a (54:75:d0:ba:52:2a)
 > Internet Protocol Version 4, Src: 172.30.1.100, Dst: 207.200.74.12
 > Transmission Control Protocol, Src Port: 42163, Dst Port: 443, Seq: 0, Len: 0

[사진 10] 와이어샤크를 통한 패킷 분석

이에 따라 다양한 방법으로 시도해 보았으나 관련 정답을 찾지 못했다.

시도해본 방법은

1. strings를 통한 cryptographer 검색
2. 키워드 검색을 통한 cryptographer 검색
3. Mail 관련 http stream 추적
4. 두번째로 가장 많은 통신이 있던 ip 추적

➔ 결론적으로 해당 단계에서 막혀 이후 단계를 진행할 수가 없어 이 문제를 풀이 완료하지 못하였다. 해당 과정과 관련하여 풀이를 찾아보았는데 이와 관련하여 마땅히 참고할 자료가 없었다. 처음으로 PCAP 문제를 풀어본 것이다 보니 문제 난이도도 있긴 하겠지만 개인 지식의 한계가 있어 풀이 완료하지 못한 것 같다. 추후 학습을 통해 이에 대한 지식을 쌓고 차후에 해결해 보겠다.

5. Flag

1. Factory-Made-Winning-Pharmaceuticals

6. 별도 첨부

7. Reference

- [URL]