

작성자	윤지원
분석 일자	2024.05.16
작성 일자	2024.05.16
분석 대상	evidence01.pcap
문서 버전	3.0
작성자 E-mail	yoonjw0827@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag..... 11

6. 별도 첨부 12

7. Reference 13

1. 문제

URL	https://forensicscontest.com/2009/09/25/puzzle-1-anns-bad-aim
문제 내용	<p>Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company's prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company's secret recipe.</p> <p>Security staff have been monitoring Ann's activity for some time, but haven't found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann's computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.</p> <p>"We have a packet capture of the activity," said security staff, "but we can't figure out what's going on. Can you help?"</p> <p>You are the forensic investigator. Your mission is to figure out who Ann was IM-ing, what she sent, and recover evidence including:</p> <ol style="list-style-type: none"> 1. What is the name of Ann's IM buddy? 2. What was the first comment in the captured IM conversation? 3. What is the name of the file Ann transferred? 4. What is the magic number of the file you want to extract (first four bytes)? 5. What was the MD5sum of the file? 6. What is the secret recipe?
문제 파일	 evidence01.pcap
문제 유형	Network forensics
난이도	2 / 3

2. 분석 도구

도구명	다운로드 링크	Version
Wireshark	Wireshark · Download	3.4.7
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5.0.0

3. 환경

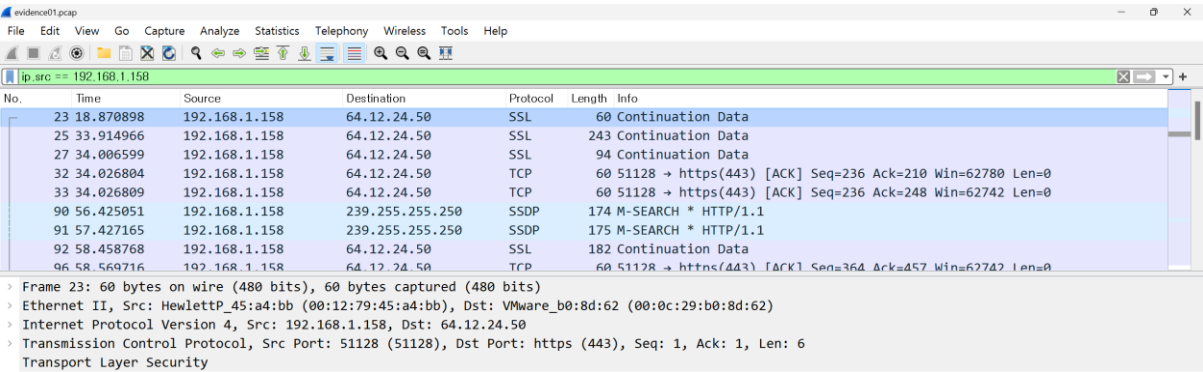
OS
Windows 11 64-bit

4. Write-Up

파일명	evidence01.pcap
용량	69.2KB
SHA256	8b997bb2d221d538174f89796b6434e853d2ed19bd5da5f15bec9bd7bc485650
Timestamp	2024-05-16 3:21:43

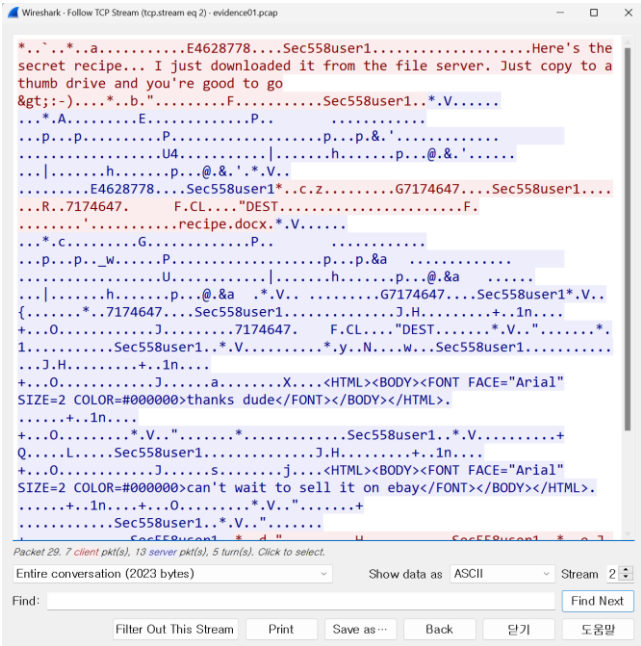
1. What is the name of Ann’s IM buddy?

우선 주어진 증거 파일인 evidence01.pcap파일을 wireshark를 통해 열어보았다. Ann의 IP가 주어진 것이 나름의 힌트일 것이라고 생각하여 ip src == 192.168.1.158로 필터링하였다.



[사진 1] Ann의 IP 192.168.1.158로 필터링한 모습

주로 SLL과 TCP 형태의 패킷이 존재하였기에 TCP Stream을 통해 힌트를 얻을 수 있을 것이라고 생각하여 가장 첫번째로 보이는 패킷의 TCP Stream을 살펴보았다.



[사진 2] 23번 패킷의 TCP Stream

[WHS-2] .iso

가장 위의 빨간색 부분에 보이는 문장을 해석해보면 다음과 같다.

‘여기 비법이 있다... 방금 파일 서버에서 다운 받았다. Thumb 드라이브에 복사만 하면 된다.’

내용을 보고 Ann이 buddy에게 보내는 메시지라고 생각했고, 뒤에 존재하는 **Sec558user1**이라는 것이 buddy의 이름이 아닐까 생각했다. 답을 확인해보니 맞았다.

2. What was the first comment in the captured IM conversation?

이 질문은 IM과 한 대화 중 가장 처음으로 한 대화가 무엇인지 물어보는 문제이다. [사진 2]에서 확인할 수 있는 앞서 해석한 문장이 바로 답이 된다.

Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)

3. What is the name of the file Ann transferred?

Ann이 전송한 파일의 이름을 물어보는 문제이다. 이 또한 [사진 2]를 통해 중간에 **recipe.docx**라는 파일명이 존재하는 것을 볼 수 있다.

4. What is the magic number of the file you want to extract(first four bytes)?

Ann이 추출하려는 파일의 매직 넘버(처음 4바이트)를 묻는 문제이다. 매직 넘버가 무엇인지 찾아보니 파일의 시그니처와 같은 뜻이라는 것을 알 수 있었다. 검색을 통해 docx의 파일 시그니처는 **50 4B 03 04**라는 것을 알아냈다.

50 4B 03 04	ZIP,
P K	DOCX, PPTX,

[사진 3] docx의 파일 시그니처

5. What was the MD5sum of the file?

Recipe.docx 파일의 MD5 체크섬을 물어보는 문제이다. 우선 패킷들 중 해당 파일을 포함하고 있는 패킷들을 찾기 위해 tcp contains recipe.docx로 필터링을 진행하였고, [사진 4]와 같이 총 4개의 패킷을 발견했다.



우선적으로 92번 패킷의 TCP Stream을 살펴보았을 때는 앞의 [사진 2]와 같았기 때문에 112번 패킷을 살펴보았다.

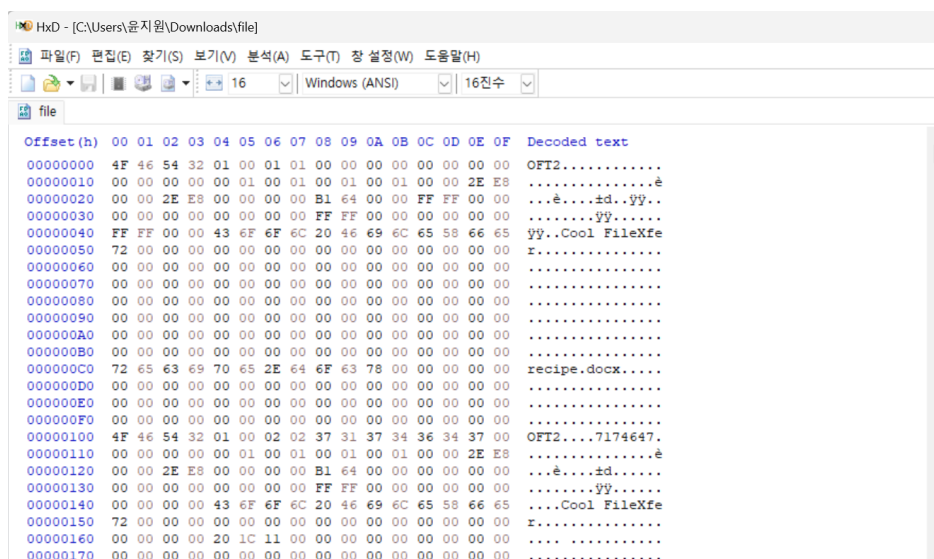


6



[사진 6] 112번 패킷을 raw 형태로 변환한 모습

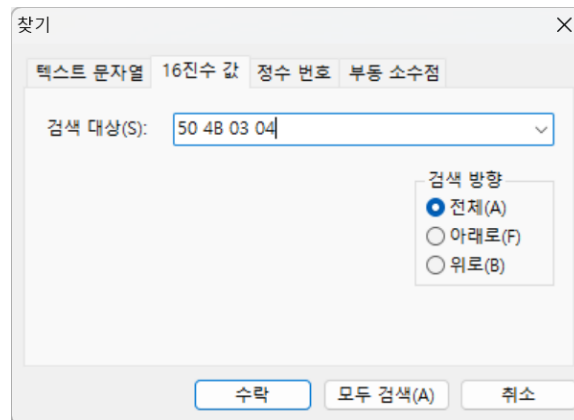
[사진 6]에 표시한 부분을 보면 504b0304를 발견할 수 있다. 이것은 docx의 파일 시그니처이다. 따라서 이를 통해 우리가 찾던 recipe.docx 파일이 들어있다는 것을 확실히 알 수 있다. 이 상태로 Save as... 를 이용하여 file이라는 이름으로 저장해주었다. 이렇게 추출한 파일을 HxD를 이용하여 열어주었다.



[사진 7] file을 HxD에 넣은 모습

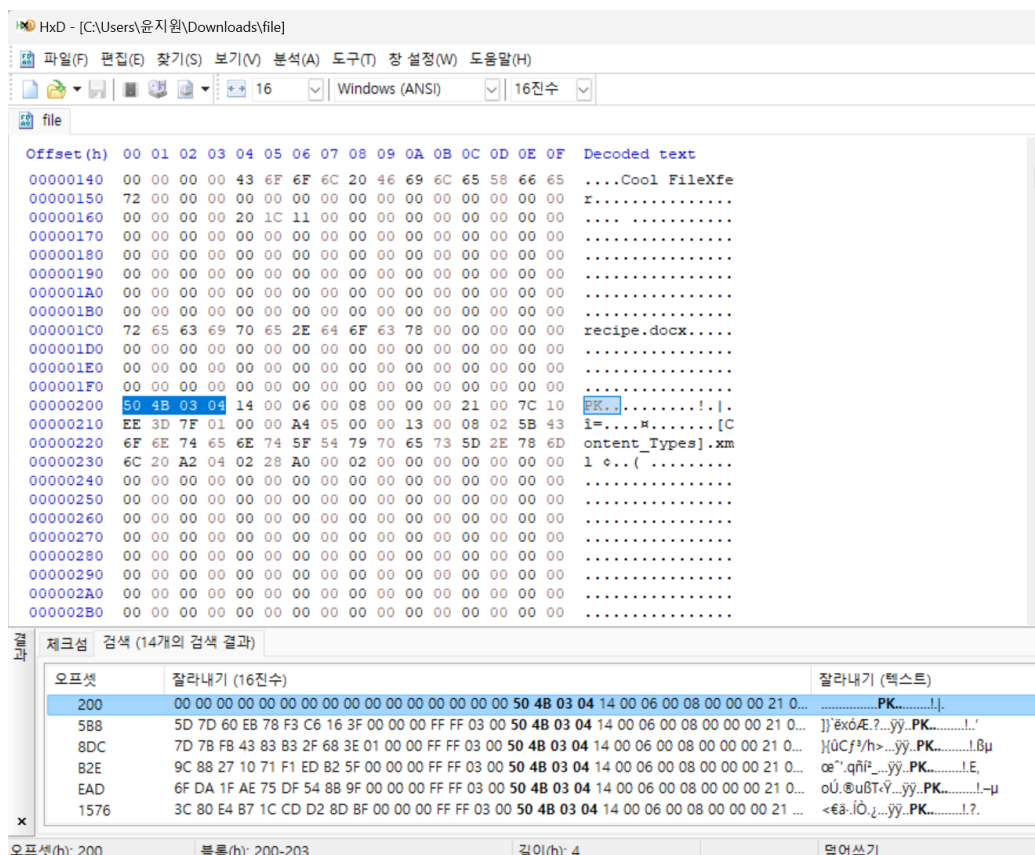
[WHS-2] .iso

여기서 recipe.docx 파일을 추출하기 위해 우선적으로 파일 시그니처인 50 4B 03 04를 검색해주었다.



[사진 8] docx 파일의 시그니처를 검색한 모습

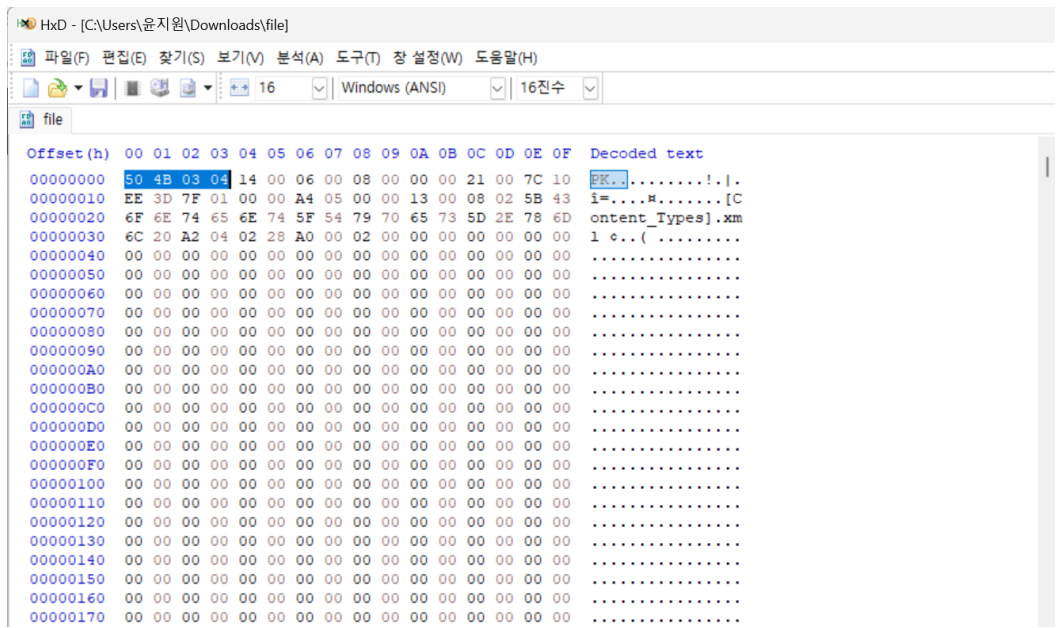
파일 시그니처를 검색해보니 다음과 같이 총 14개가 검색되었는데, 그 중에서 가장 처음으로 검색된 오프셋 200으로 이동해보았다.



[사진 9] 파일 시그니처가 가장 처음 검색된 부분으로 이동한 모습

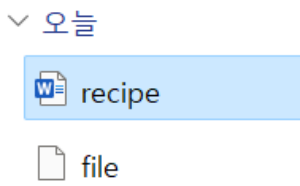
아무래도 이곳부터 recipe.docx 파일이 시작된 것 같아서 이 앞부분을 모두 지워주었다.

[WHS-2] .iso



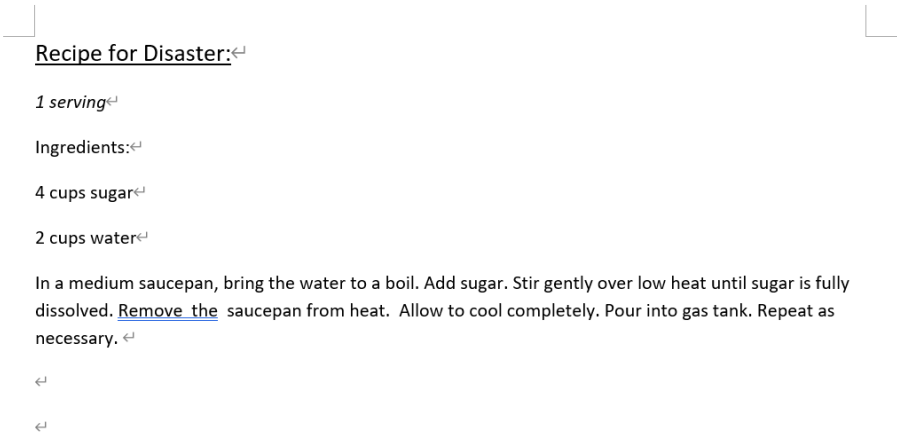
[사진 10] 파일 시그니처가 오프셋 0으로 온 모습

이 상태에서 다른 이름으로 저장을 이용하여 recipe.docx라는 이름으로 파일 추출에 성공하였다.



[사진 11] recipe.docx 파일 추출에 성공한 모습

해당 파일을 열면 다음과 같은 내용을 성공적으로 볼 수 있다.



[사진 12] recipe.docx 내용

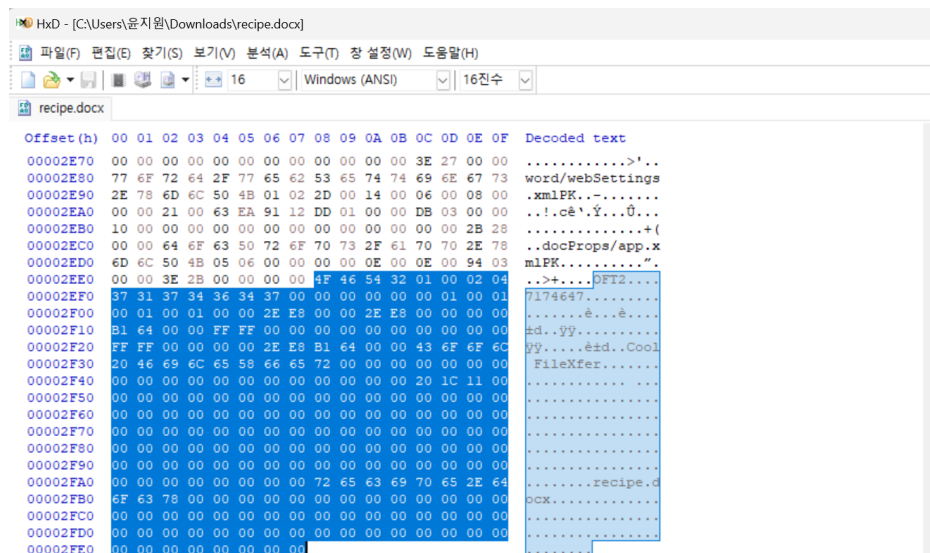
[WHS-2] .iso

이 recipe.docx의 파일을 다시 HxD에 넣은 다음, [분석] - [체크섬] - [체크섬 생성]을 통해 MD5로 체크섬을 생성해보면 다음과 같이 체크섬이 성공적으로 나온다.

결과 체크섬 검색 (14개의 검색 결과)		
C:\Users\윤지원\Downloads\recipe.docx		
알고리즘	체크섬	사용방법
MD-5	10893FD7CFF66DCA193F658CA9438D15	

[사진 13] recipe.docx의 MD5 체크섬

그러나 공식적인 답과 다른 체크섬 값이 나왔다. 그래서 추가적으로 HxD를 통해 파일 뒤에 불필요한 부분이 있다는 것을 알 수 있었다. 앞에서 삭제한 부분과 유사하게 OFT2~로 시작하였기에 쉽게 알 수 있었다. 따라서 이 부분도 지우고 파일을 저장한 다음, 다시 체크섬을 생성해보니 공식적인 답과 같은 값인 **8350582774E1D4DBE1D61D64C89E0EA1**이 나오는 것을 확인할 수 있었다.



[사진 14] 파일 뒤에 불필요한 부분을 발견한 모습

결과 체크섬 검색 (1개의 검색 결과)		
C:\Users\윤지원\Downloads\recipe.docx		
알고리즘	체크섬	사용방법
MD-5	8350582774E1D4DBE1D61D64C89E0EA1	

[사진 15] recipe.docx의 최종 MD5 체크섬

6. What is the secret recipe?

이 문제는 recipe.docx에 있던 비밀 레시피를 물어보는 것이므로, [사진 12]에서 확인할 수 있는 파일 내용이 바로 답이다



5. Flag

1번 : Sec558user1

2번 : Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)

3번 : recipe.docx

4번 : 0x504B0304

5번 : 8350582774E1D4DBE1D61D64C89E0EA1

6번 :

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

6. 별도 첨부

7. Reference

- <http://forensic-proof.com/archives/300>