Report

경성대학교

과목명 : 신기술세미나

학과 : 컴퓨터공학과

학번 : 2016642045

이름 : 강건우

제출일자 : 2019. 12. 16.

목 차

1. 스테가노그래피의 개요

- 스테가노그래피는 그리스어로 “감추어져있다” 라는 뜻인 “stegano“와 그리스어로 “쓰다, 그리다” 라는 뜻인 “graphos“의 합성어로 “감추어쓰다” 라는 의미이다.
  사진, 음악, 동영상 등의 일반적인 파일 안에 데이터를 숨기는 기술을 말한다.

2. 쉘코드의 개요

- Shell Code란 단어는 공격 대상 시스템의 명령어 쉘을 실행시킨다는 의미로 부터 파생되었으며, 주로 소프트웨어 취약점을 통한 공격(Exploitation)이후 실행 될 작은 규모의 프로그램(Payload)으로 사용된다. 쉘코드는 대상에 따라 로컬(Local) 및 원격(Remote) Shell Code로 나눌 수 있으며, 그 자체가 Shell을 실행하지는 않지만 외부의 네트워크로부터 특정 파일을 다운로드하고 실행하는(Download & Execute) 하는 경우도 있다.

1) 로컬 쉘코드(Local Shellcode)
   - 공격자가 대상 시스템에 대한 제한적인(혹은 완전한) 접근 권한을 가지고 있는 경우, 버퍼 오버플로(Buffer Overflow) 등의 취약점이 있는 높은 권한(대부분 root)을 가진 프로세스를 공격하여, 해당 프로세스와 같은 높은 권한을 획득하기 위해 사용된다.

2) 원격 쉘코드(Remote Shellcode)
   - 공격자가 네트워크상의 다른 대상 시스템에 한 취약점이 있는 프로세스를 공격하고자 하는 경우 사용한다. 일반적으로 원격 쉘은 공격자가 대상 시스템의 Shell에 대한 접근을 허용하기 위해 표준 TCP/IP 소켓 연결을 사용하며, 이 때 연결이 어떤 방식으로 이루어졌는가에 따라 다음과 같이 분류될 수 있다.

3) 리버스 쉘코드(Reverse Shellcode)
   - 목표 시스템으로부터 공격자에게 연결을 요청하도록 하기에 커넥트 백(Connect-Back) 쉘코드라고 한다.

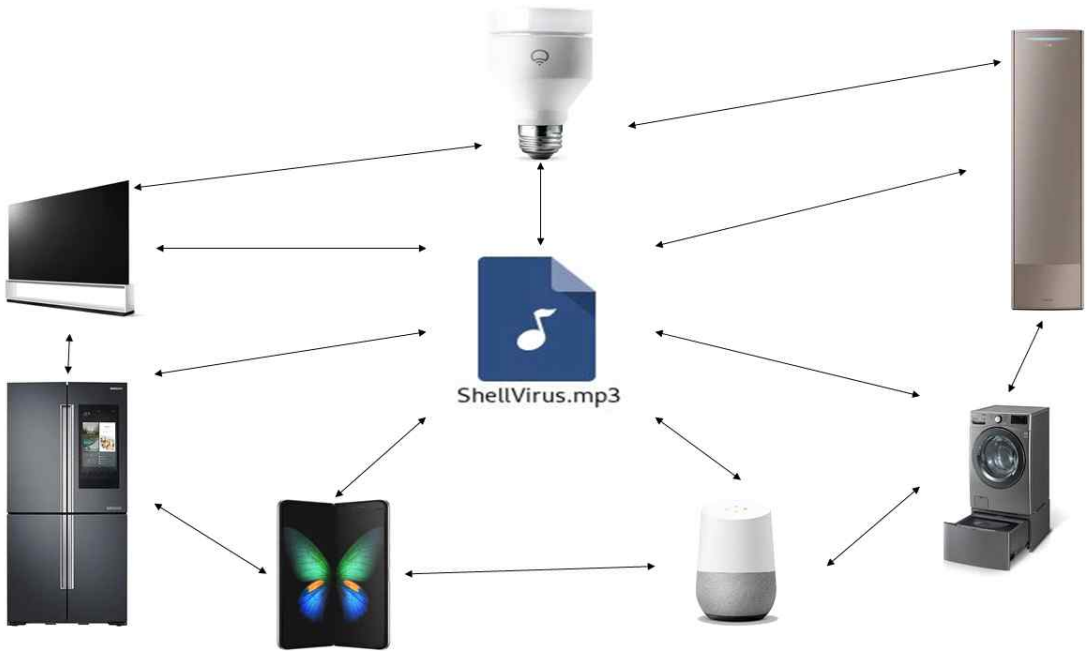
4) 바인드 쉘코드(Bind Shellcode)
   - 목표 시스템의 특정 포트를 바인드하여 공격자가 대상 시스템에 연결 할 수 있도록 한다.

5) 다운로드 및 실행 쉘코드(Download & Execute Shellcode)

- 다운로드 및 실행 쉘코드는 쉘코드가 직접 쉘을 실행하지는 않지만, 주로 외부의 네트워크로부터 Malware(악성코드)를 다운로드하고 실행할 때 주로 사용된다. 특히 요즘에는 대상 시스템이 악성 페이지에 방문하는 것만으로도, 사용자 몰라 악성코드를 내려받아 실행하는 Drive By Download (드라이브 바이 다운로드) 공격에 널리 사용된다.

3. 모의해킹 시나리오

- 공격대상자가 쉘코드 삽입된 mp3파일을 블루투스 해킹을 하여 공격대상의 IoT기기에 직접 다운로드
- 공격자가 쉘코드 삽입된 mp3파일을 타 클라우드 서버에 업로드
- 공격자가 쉘코드 삽입된 mp3파일을 타 사이트에 업로드하여 공격대상자가 mp3파일 다운로드 한 후 IoT기기에 다운로드

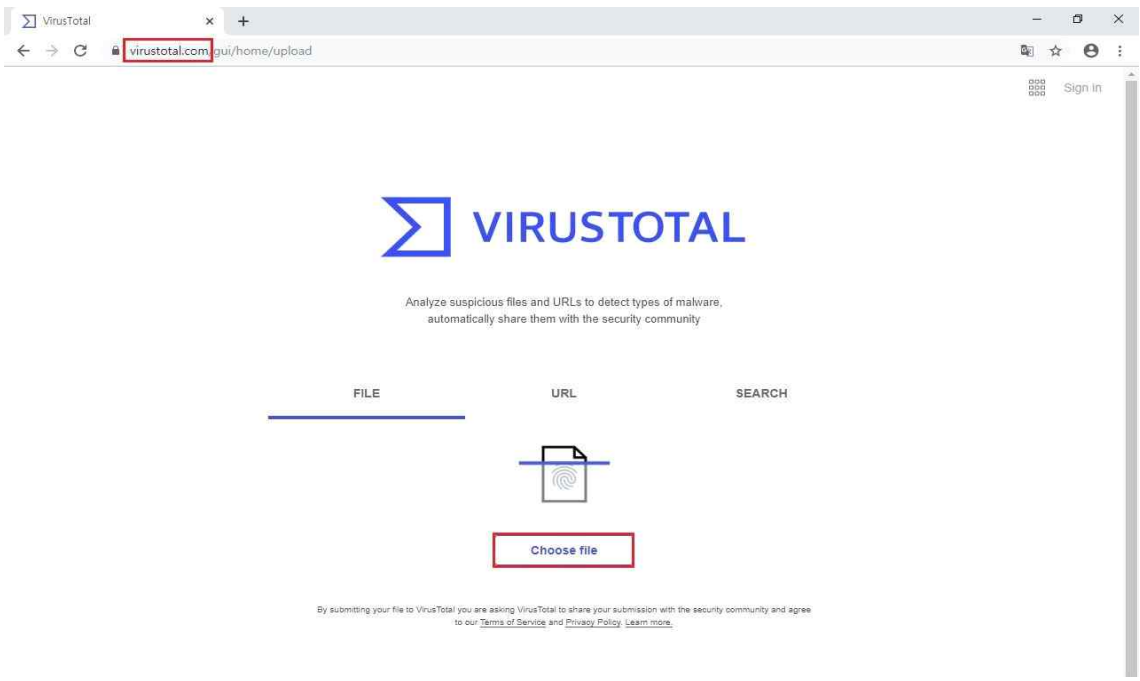


4. 모의해킹 실습

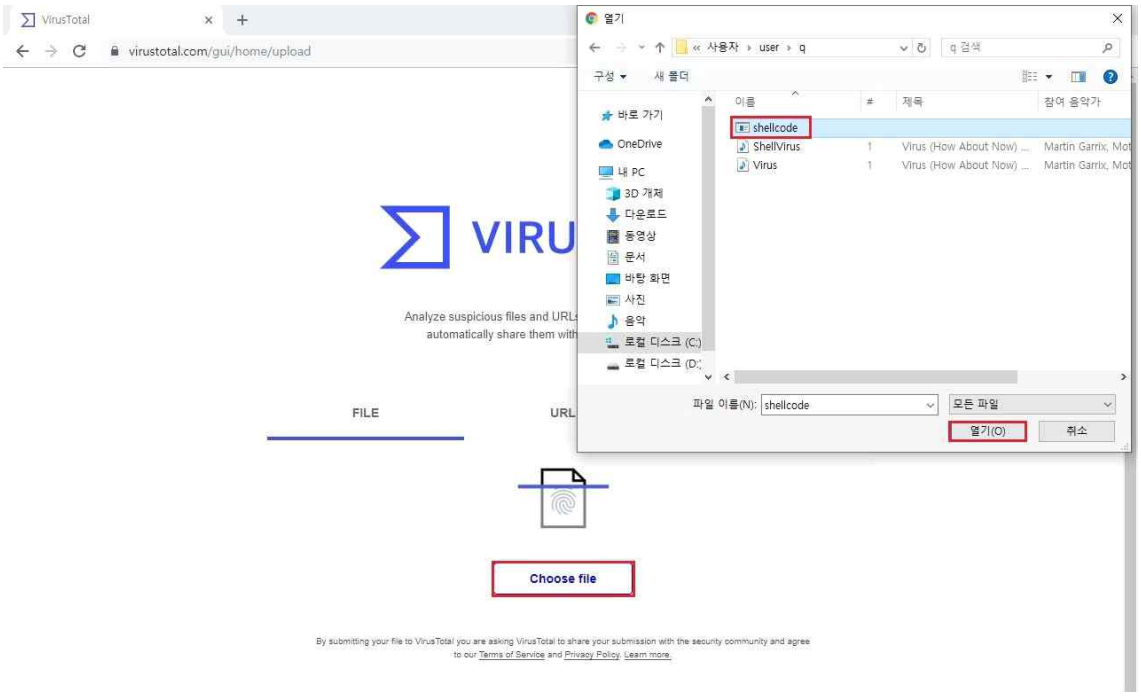
* 본 실습은 exe파일확장자라서 스마트폰이나 스마트밴드(웨어러블 기기)에서는 쉘코드가 작동하지 않았으며 복호화가 되지 않았음(복호화 과정 생략)

1) 실습을 위해 mp3파일과 쉘코드가 삽입된 exe파일을 준비

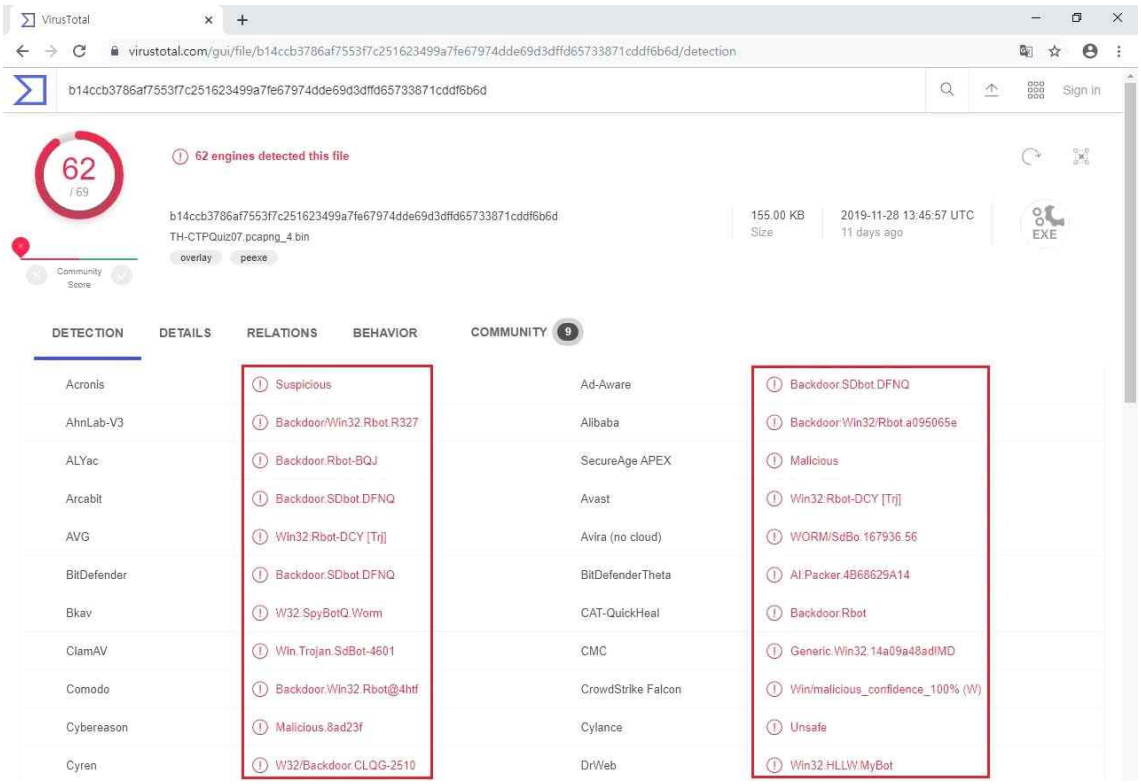
2) shellcode.exe 파일 바이러스의 여부를 위해
www.virustotal.com 홈페이지 접속

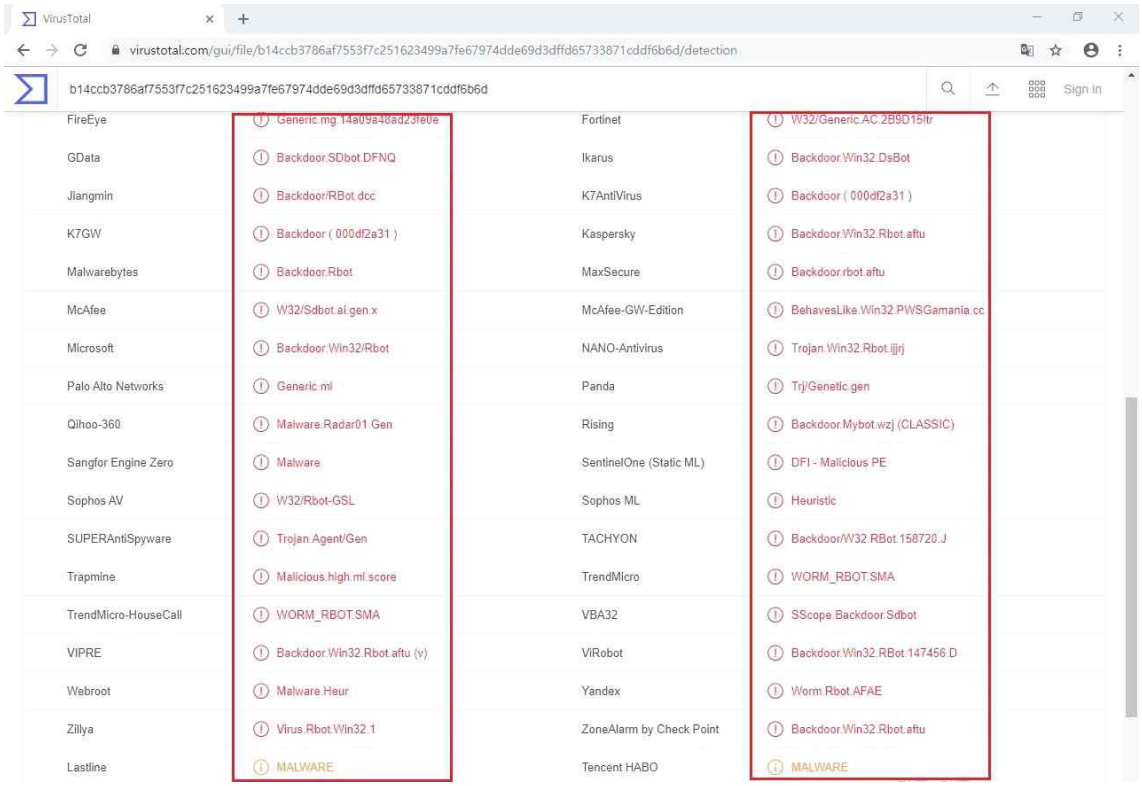


3) Choose file을 눌러 shellcode.exe 파일을 선택



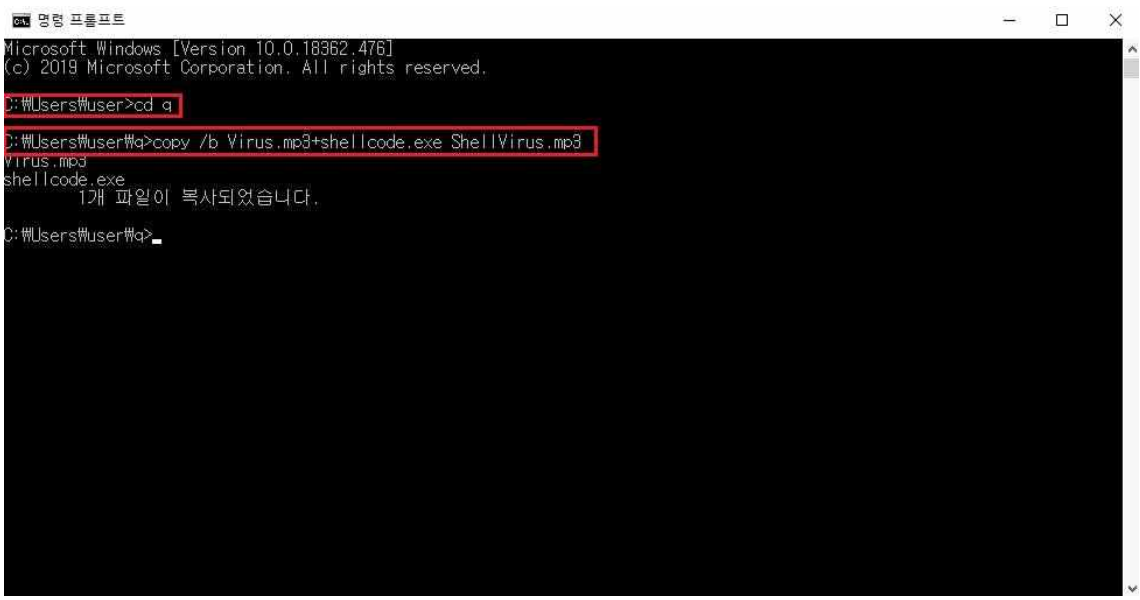
4) shellcode.exe 파일에 있는 여러 가지 바이러스들을 확인할 수 있음





5) shellcode.exe 파일을 은닉하기 위해 명령프롬프트(cmd)를 실행하여 해당 경로로 들어가 명령을 입력

- copy /b Virus.mp3+shellcode.exe ShellVirus.mp3

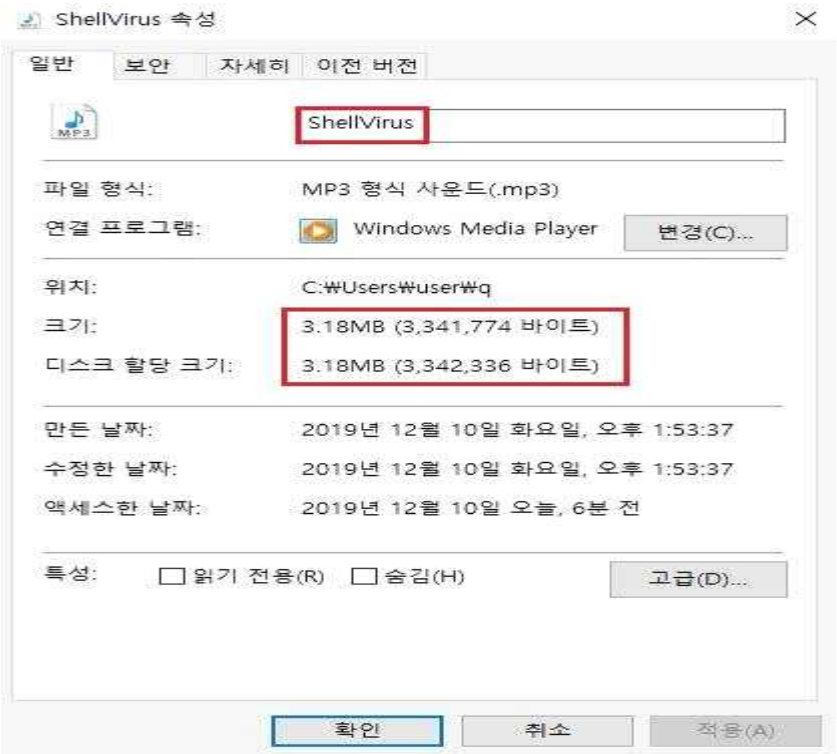


6) 해당 경로에 ShellVirus.mp3가 생성된 것을 확인할 수 있음

7) 원본 파일(Virus.mp3)의 크기 확인

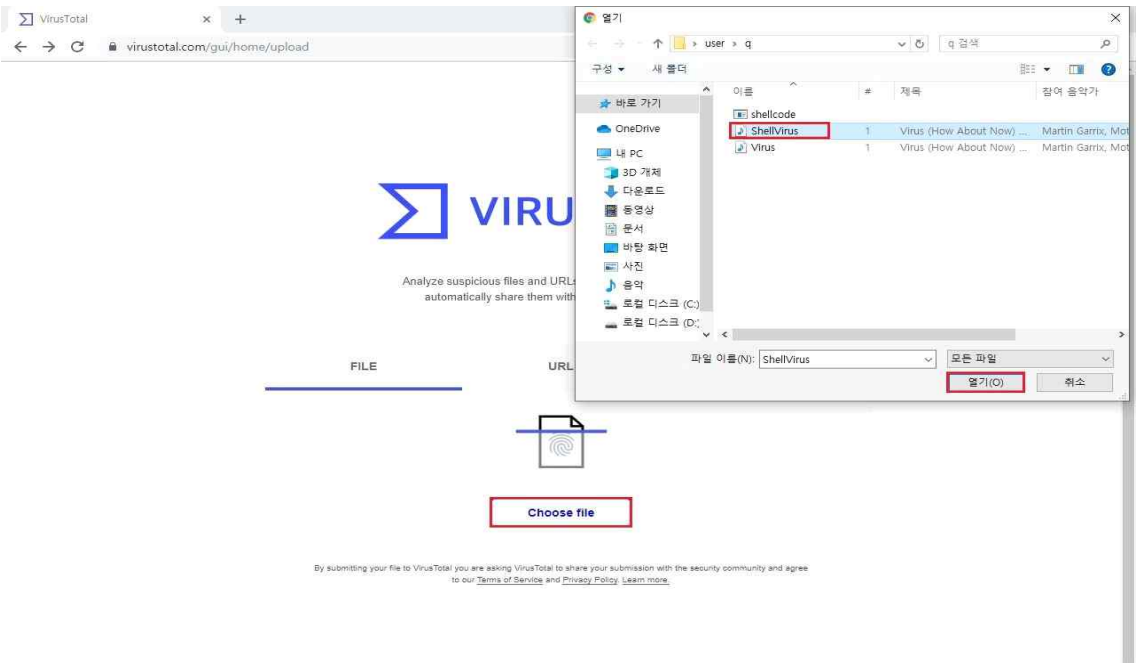
8) 쉘코드 실행파일이 은닉된 파일(ShellVirus.mp3)의 크기 확인

- 원본 파일과 생성된 파일의 크기가 서로 다른 것을 확인할 수 있음

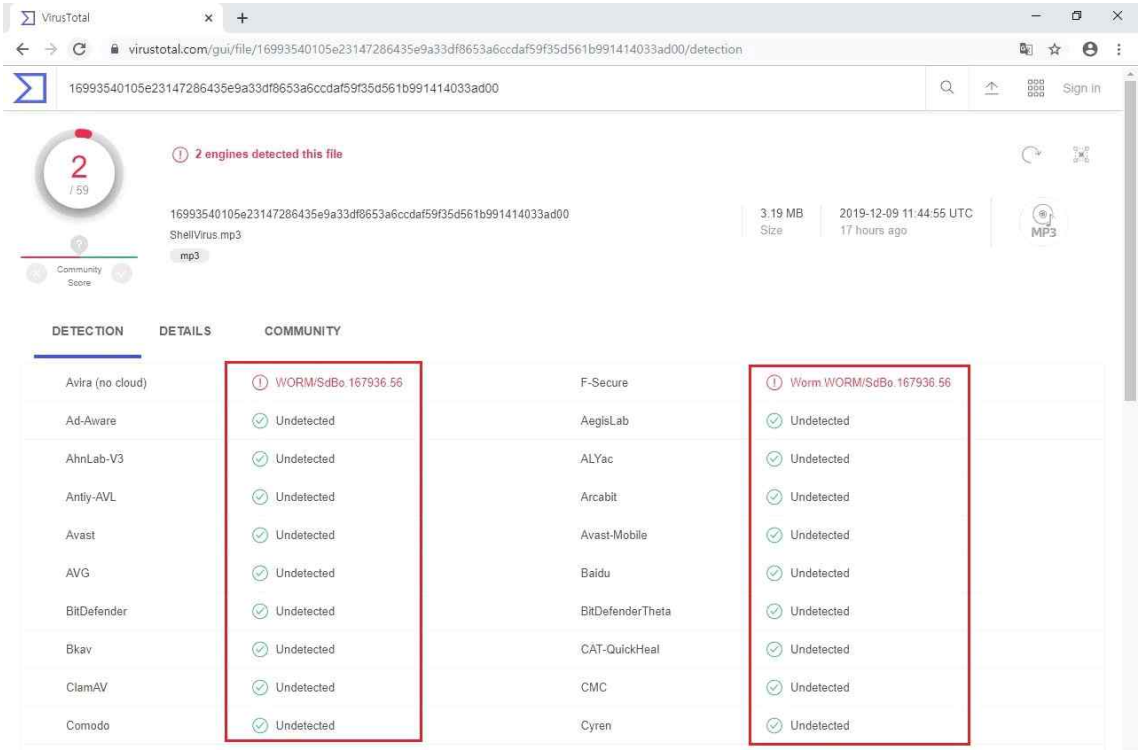


9) ShellVirus.mp3 파일의 바이러스 여부를 위해

www.virustotal.com 홈페이지에서 ShellVirus.mp3 파일을 선택



10) 웜바이러스만 발견되고 나머지 바이러스들은 은닉되어 짐



5. 모의해킹 결과의 문제점 및 느낀점

1) 윈도우의 확장자가 아닌 스마트폰이나 IoT기기에서도 실행되는 쉘코드 실행확장자를 구축하고 싶었으나 뜻대로 되지 않았습니다.
2) 블루투스를 이용한 모의해킹, 클라우드 서버를 이용한 모의해킹도 구상하였지만 가지고 있는 IoT기기가 스마트밴드 밖에 없고 삼성의 보안을 뚫기에는 법적으로 문제가 되기 때문에 다소 무리가 있었습니다.
3) 윈도우 보안이 철저해서 쉘코드가 계속 지워지는 문제가 있었습니다.
4) 실습과 자료를 찾아보면서 IoT보안에 대해서 많은 것을 알게 되었고 취약점을 이용하여 해킹이 가능하다는 것을 알게 되었습니다.
5) 이미지파일(png, jpg)이나 압축파일(zip, rar)로 스테가노그래피 실습 해본 경험이 있지만 음악파일은 처음이라 암호화, 복호화 과정이 잘 되지 않은 부분이 있어서 아쉬웠습니다.

6. 모의해킹 환경

1) 사용한 기기

- 삼성 노트북, 삼성 갤럭시노트9, 삼성 기어핏2

2) 운영체제

- Windows10, Kali Linux

3) 사용한 프로그램 종류

- 명령 프롬프트(CMD)
- VirusTotal
- WireShark
- OpenStego

7. 연구 분담 및 기여도

1) 연구 분담

- 강건우 : 자료조사, 쉘코드 추출, 모의해킹, 발표자료 및 결과보고서 작성
- 오준혁 : 발표

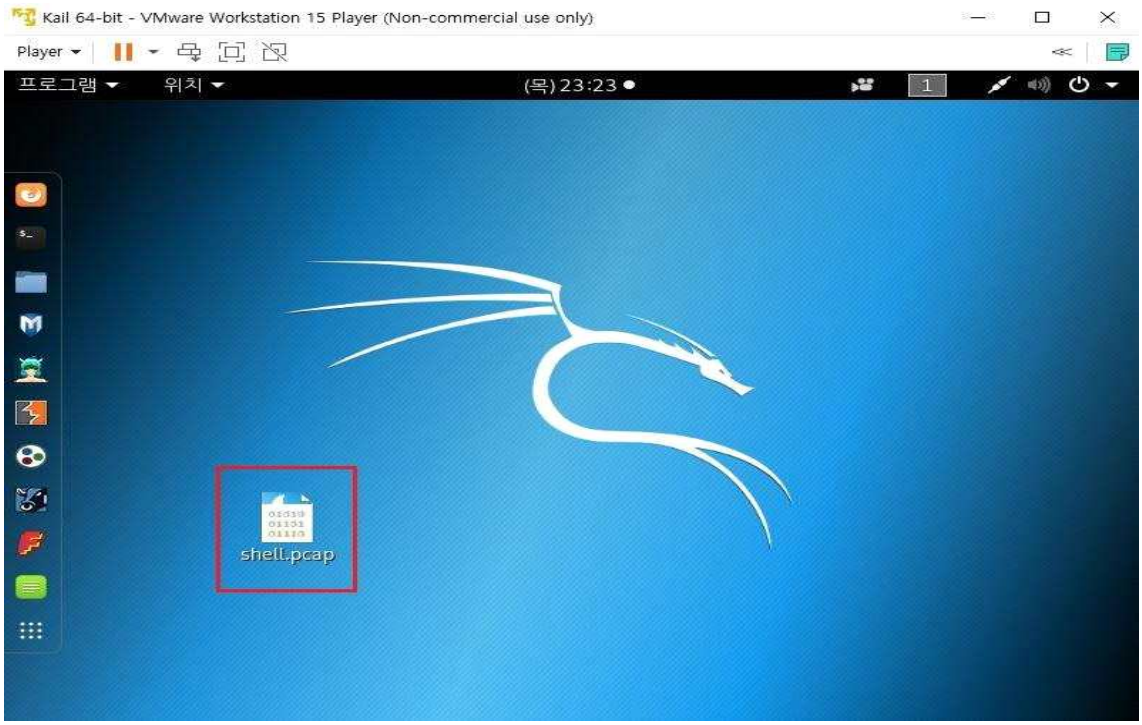
2) 기여도

- 강건우 : 90%
- 오준혁 : 10%

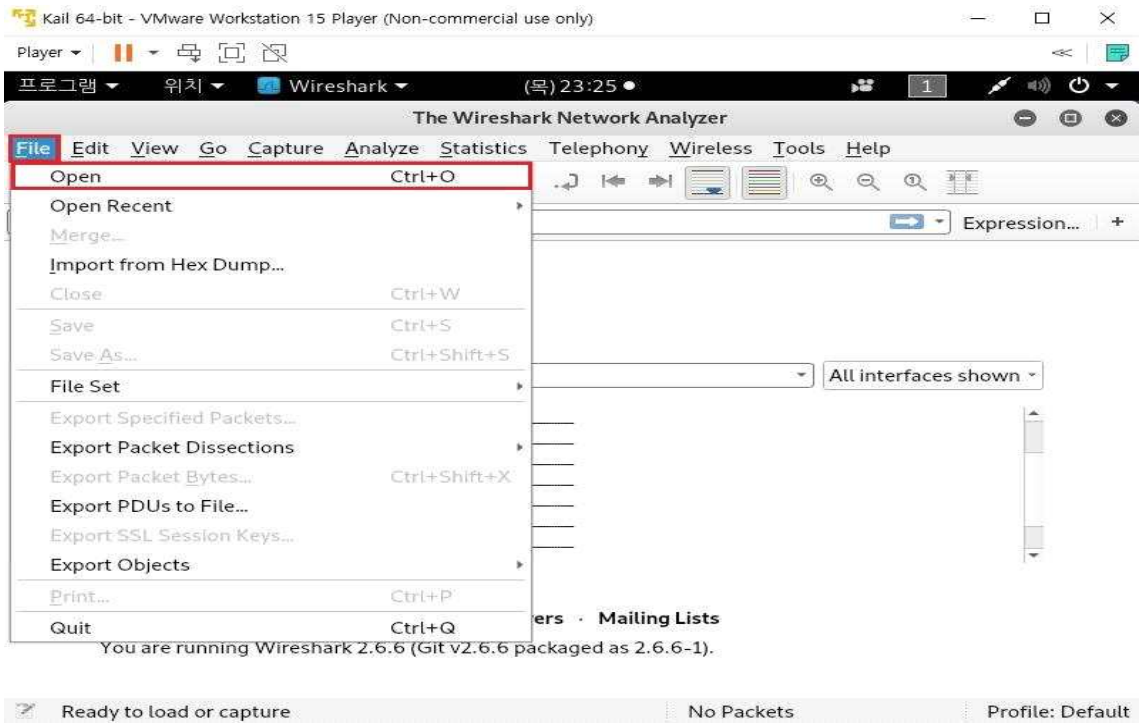
8. 부록

8-1) 쉘코드 추출 과정

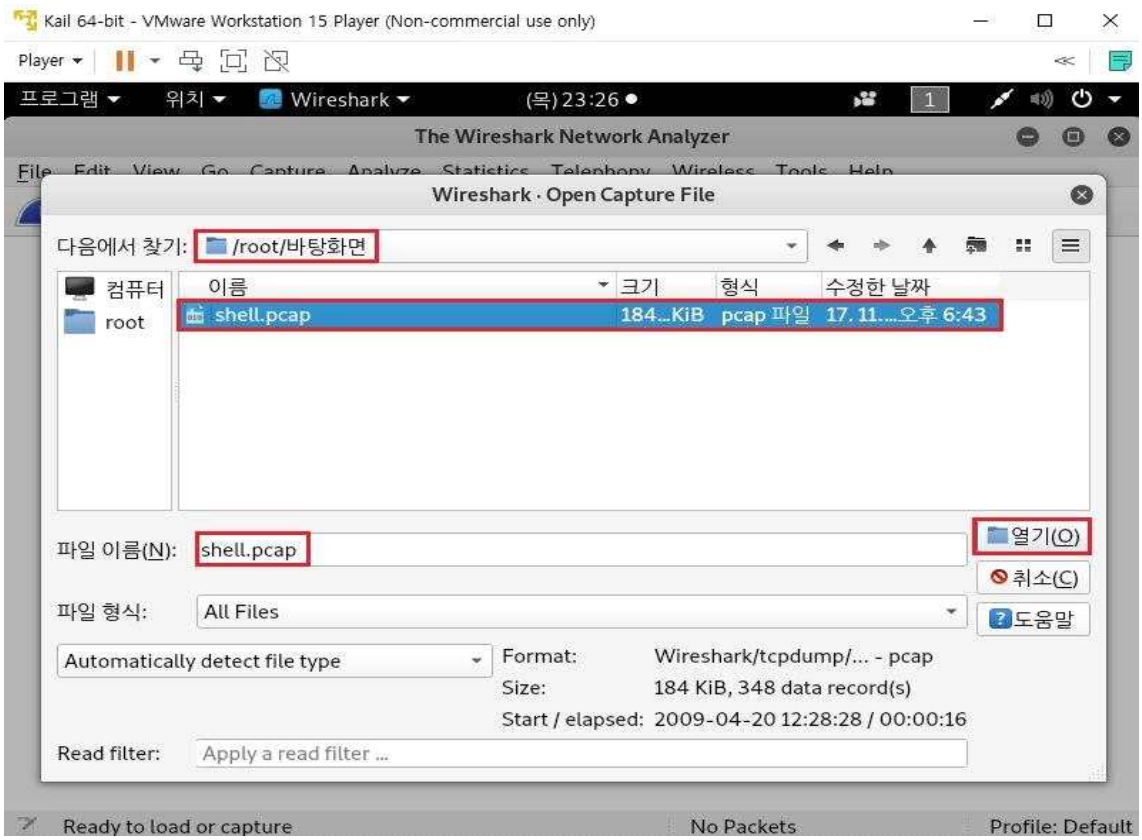
- 쉘코드를 추출하기 위해 샘플 패킷을 준비



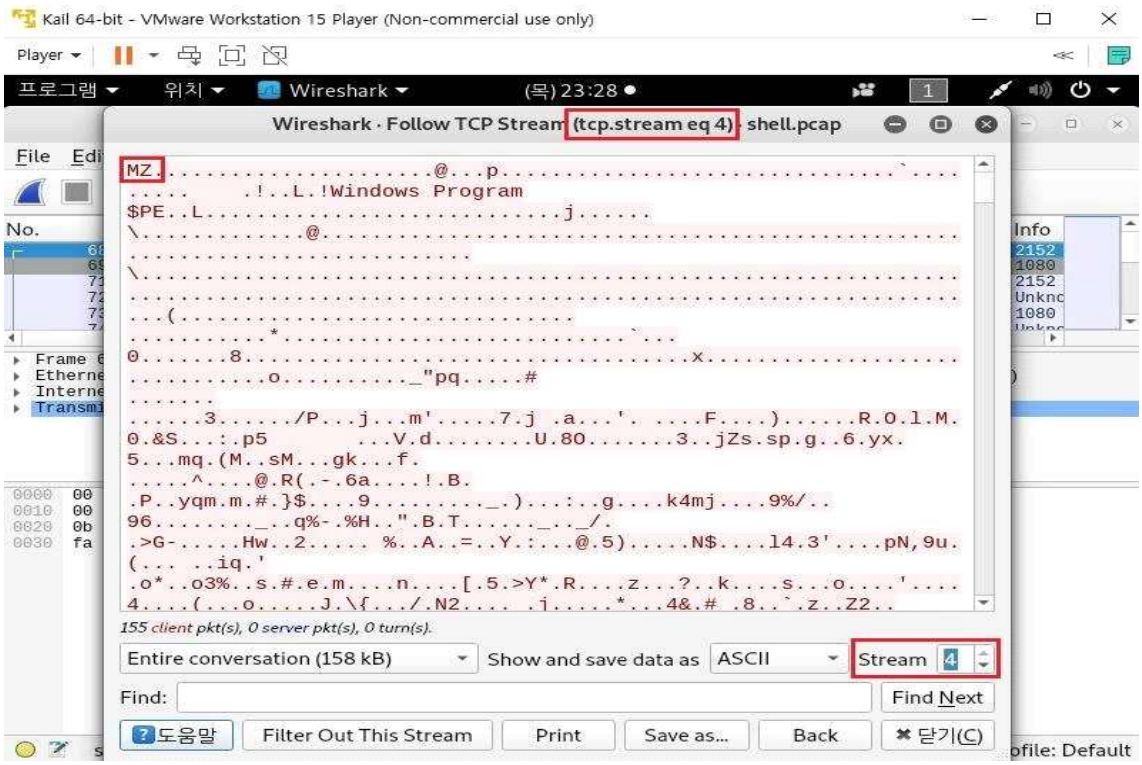
- WireShark를 실행하여 메뉴 -> Open을 선택



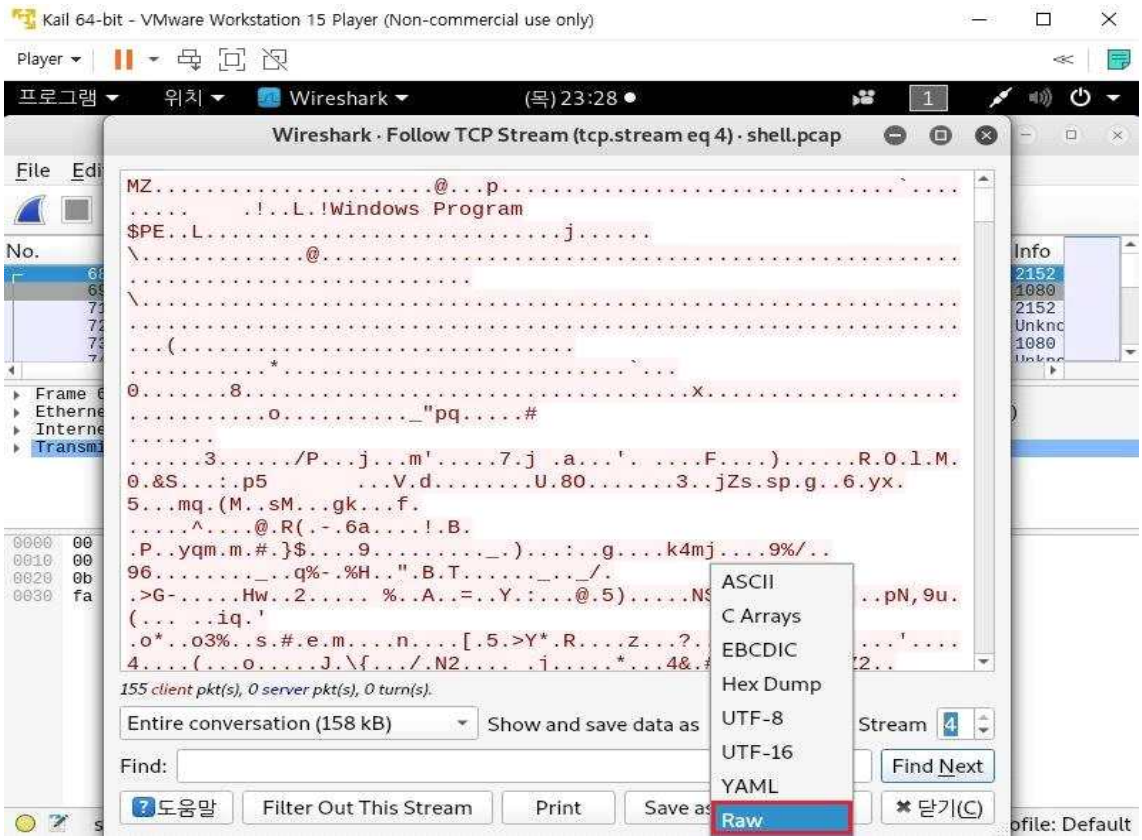
- 준비한 샘플 패킷을 선택



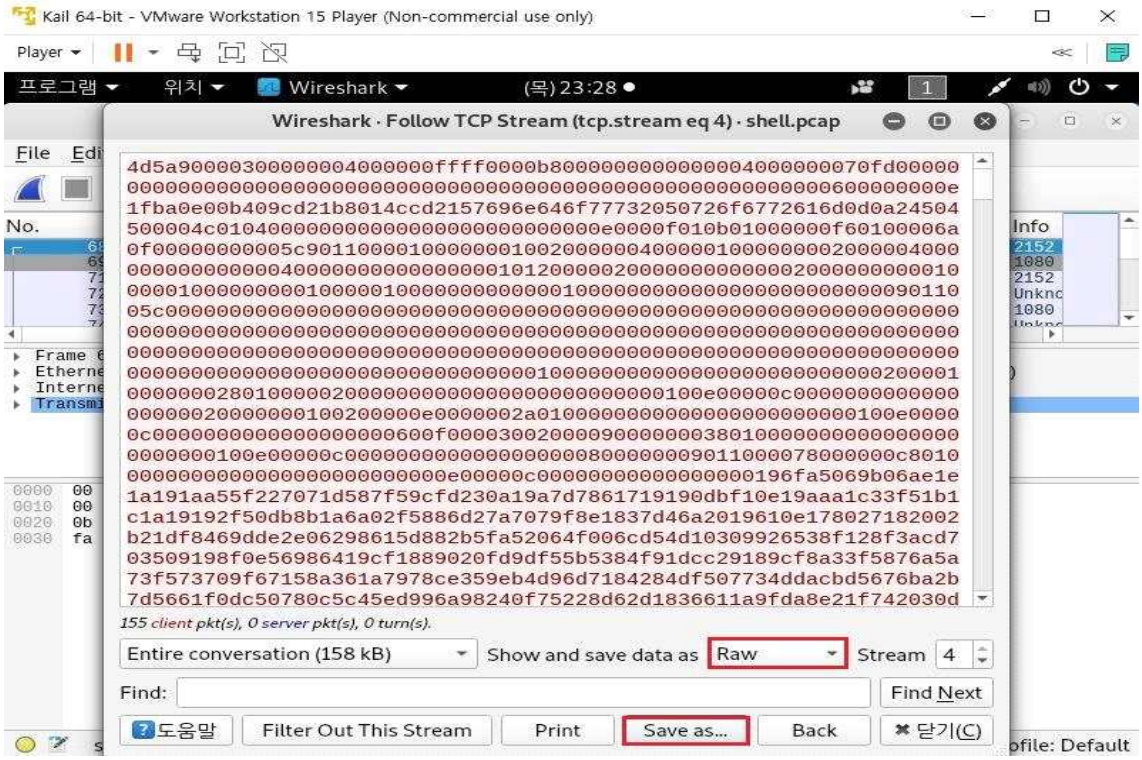
- TCP Stream4를 선택하여 MZ 확인(.exe 파일 시그니처 -> MZ)



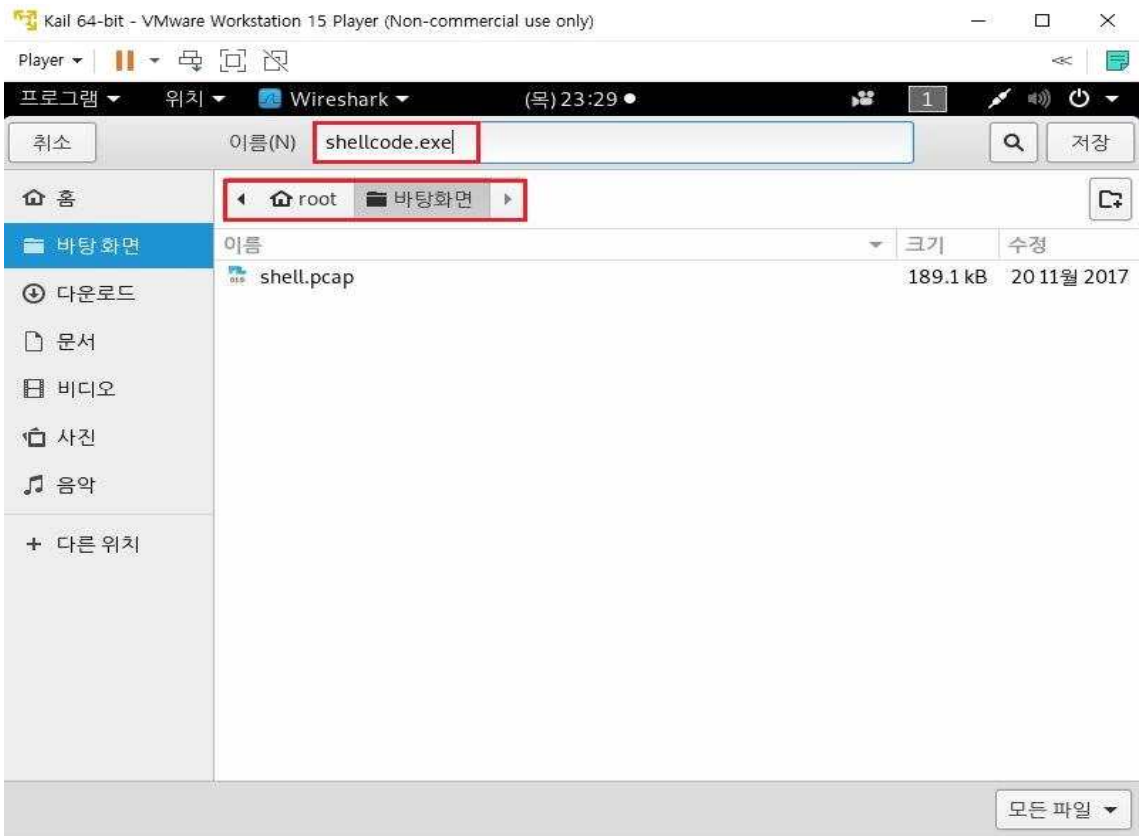
- exe 파일로 추출하기 위해 데이터 값을 Raw로 변경



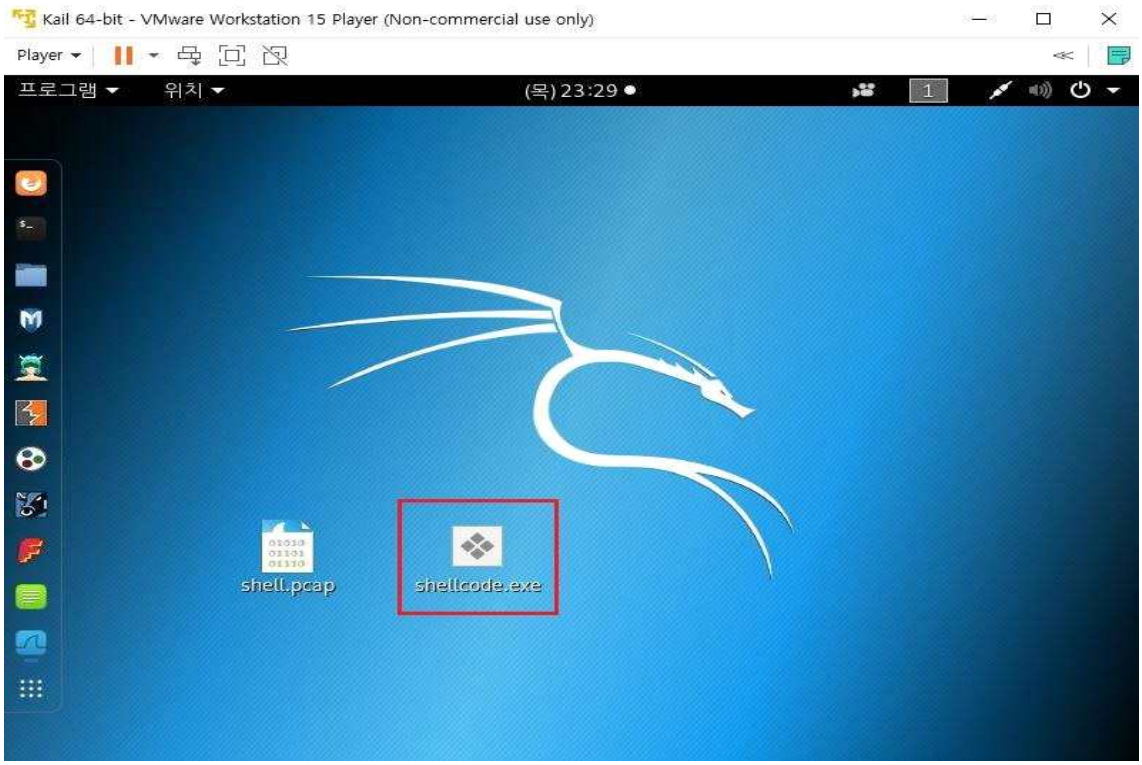
- Save as 선택



- 해당 경로에 shellcode.exe 이름의 파일로 저장



- shellcode.exe 파일(쉘코드 실행파일)이 정상적으로 추출되었음을 확인



8-2) 참고 자료

- http://www.itworld.co.kr/news/115083
- http://www.ciokorea.com/news/38809
- https://blog.alyac.co.kr/1556
- https://www.hankyung.com/it/article/201903290219g
- http://www.donga.com/news/article/all/20190731/96765493/1
- https://blog.lgcns.com/1462
- 네트워크 패킷 포렌식 책 / SECU BOOK
- 디지털 포렌식 개론 책 / 이룬
- 리눅스 커맨드라인 쉘스크립트 바이블 책 / 스포트라잇북