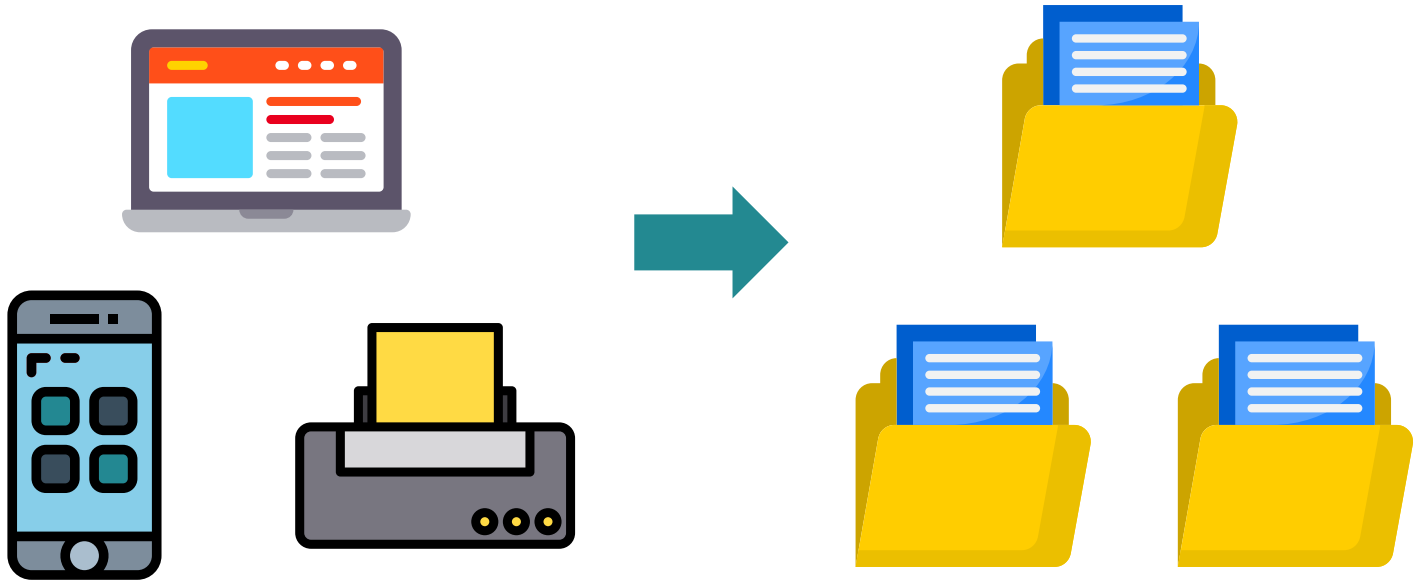
안티 포렌식

- 파일 은닉

SCP 이다영

디지털 포렌식(Digital Forensic)



디지털 포렌식(Digital Forensic)

안티 포렌식(Anti Forensic)

포렌식 기술에 대응하여 자신에게 불리하게 작용할 가능성이 있는
증거물을 차단하려는 일련의 활동

대표적 기술: 데이터 변조, 삭제, 암호화, 은닉

1. 스테가노그래피(Steganography)
2. ADS 내 은닉

파일 은닉 - 스테가노그래피(Steganograpy)

일반적인 파일 안에 텍스트나 파일을 숨기는 기법

파일 은닉 - 스테가노그래피(Steganograpy)

security.jpg

+

in.docx

파일 은닉 - 스테가노그래피(Steganograpy)

```
C:₩Users₩djssl₩Desktop₩steganography>copy /b security.jpg + in.docx security
2.jpg
security.jpg
in.docx
        1개 파일이 복사되었습니다.
```

파일 시그니처(File Signature)

: 각 파일의 형식마다 정해져 있는 특정 바이트

파일 은닉 - 스테가노그래피(Steganograpy)

File Type	Header Signature(Hex)	Footer Signature(Hex)
JPEG	FF D8 FF E0 FF D8 FF E8	FF D9

security.jpg의 Header Signature

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01   ÿØÿà..JFIF......
```

security2.jpg의 Header Signature

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01   ÿØÿà..JFIF......
```

파일 은닉 - 스테가노그래피(Steganograpy)

File Type	Header Signature(Hex)	Footer Signature(Hex)
JPEG	FF D8 FF E0 FF D8 FF E8	FF D9

security.jpg의 Footer Signature

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000087F0   C4 79 47 82 7F FF D9                              ÄyG‚.ÿÙ
```

security2.jpg의 Footer Signature

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00003740   2E 78 6D 6C 50 4B 05 06 00 00 00 00 0D 00 0D 00   .xmlPK..........
00003750   40 03 00 00 04 34 00 00 00 00                     @....4....
```

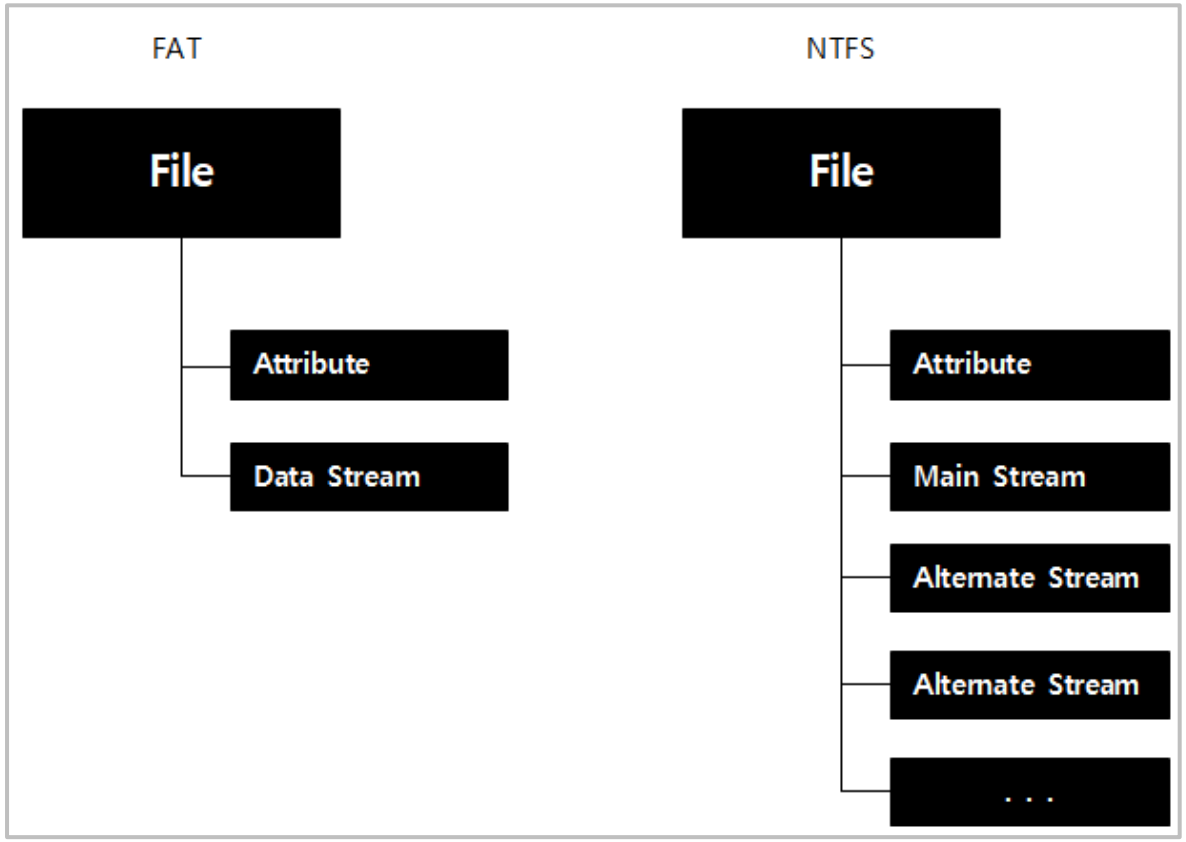
docx 파일의 Footer Signature

파일 은닉 – ADS 내 은닉

파일 시스템: 파일 저장 규칙

- NTFS, FAT

파일 은닉 – ADS 내 은닉



Alternate Data Stream

ADS 영역을 이용한 행위

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위
2. ADS 영역에 은닉된 실행 파일 실행 행위
3. 인터넷에서 파일을 다운로드를 했을 시에 Host URL과 Reference URL을 확인하는 행위

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>dir
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 09:47    <DIR>          .
2021-05-02  오후 09:47    <DIR>          ..
2021-05-02  오후 09:47                 5 test.txt
               1개 파일                   5 바이트
               2개 디렉터리  16,713,428,992 바이트 남음

C:₩Users₩djssl₩Desktop₩ADS>more < test.txt
Hello
```

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>dir
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 09:47    <DIR>          .
2021-05-02  오후 09:47    <DIR>          ..
2021-05-02  오후 09:47                 5 test.txt
               1개 파일                   5 바이트
               2개 디렉터리  16,713,428,992 바이트 남음

C:₩Users₩djssl₩Desktop₩ADS>more < test.txt
Hello
```

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>echo "ADS Data!!!" > test.txt:ads_data
```

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>dir
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 09:47    <DIR>          .
2021-05-02  오후 09:47    <DIR>          ..
2021-05-02  오후 10:01                 5 test.txt
               1개 파일                   5 바이트
               2개 디렉터리  16,702,230,528 바이트 남음
```

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>dir /r
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 09:47    <DIR>          .
2021-05-02  오후 09:47    <DIR>          ..
2021-05-02  오후 10:01                 5 test.txt
                                      16 test.txt:ads_data:$DATA
               1개 파일                   5 바이트
               2개 디렉터리  16,705,179,648 바이트 남음

C:₩Users₩djssl₩Desktop₩ADS>more < test.txt:ads_data
"ADS Data!!!"
```

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>echo "ADS_DATA in Directory!!!" > :ads_data

C:₩Users₩djssl₩Desktop₩ADS>dir /r
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 10:10    <DIR>          .
                                        29 .:ads_data:$DATA
2021-05-02  오후 10:10    <DIR>          ..
2021-05-02  오후 10:01                 5 test.txt
                                        16 test.txt:ads_data:$DATA
               1개 파일                   5 바이트
               2개 디렉터리  16,704,524,288 바이트 남음
```

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

```
C:₩Users₩djssl₩Desktop₩ADS>echo "ADS_DATA in Directory!!!" > :ads_data

C:₩Users₩djssl₩Desktop₩ADS>dir /r
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 10:10    <DIR>          .
                                        29 .:ads_data:$DATA
2021-05-02  오후 10:10    <DIR>          ..
2021-05-02  오후 10:01                 5 test.txt
                                       16 test.txt:ads_data:$DATA
               1개 파일                   5 바이트
               2개 디렉터리  16,704,524,288 바이트 남음
```

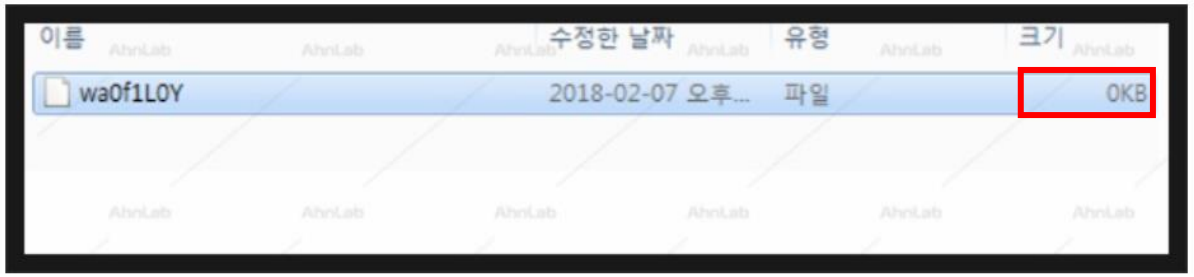
1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

Magniber 랜섬웨어 파일 생성방식의 변화 (파일은폐)

멀버타이징(Malvertising)을 통해 유포되는 Magniber 랜섬웨어의 최근 유포방식에서 사용자 시스템에 랜섬웨어 파일을 생성할때 Alternate Data Stream(ADS)를 활용한 파일 은폐 기법이 사용되었다. 멀버타이징(Malvertising)은 광고 서비스의 정상적인 네트워크를 이용하여 악성코드를 유포 및 감염 시키는 방법이다.

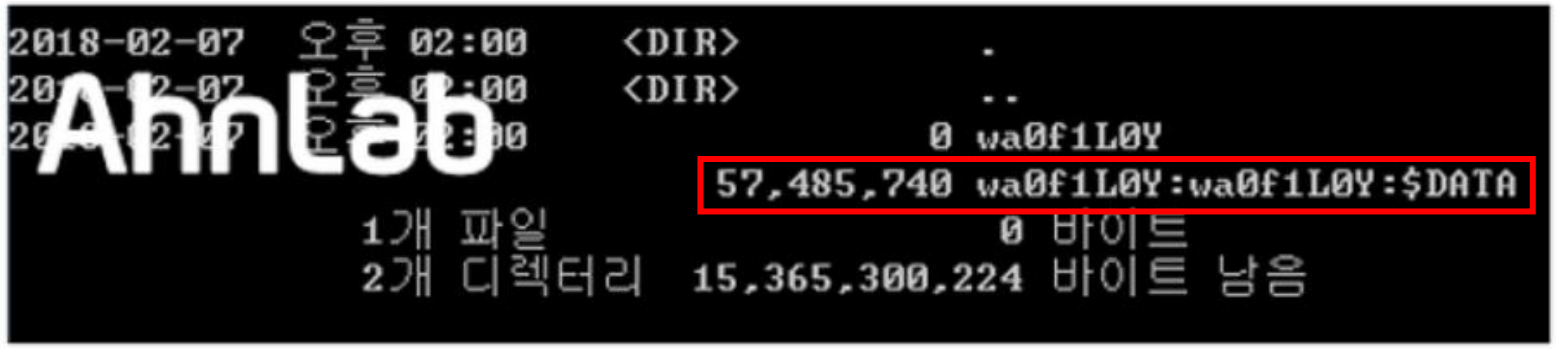
1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위

해당 기법을 통해 로컬에 저장된 파일은 디렉터리에서 확인하면 [그림 3]과 같이 파일의 크기가 0byte 로 보여진다. 하지만 [그림 4]와 같이 커맨드 명령(dir /r)을 통해 해당 경로를 확인해 보면 “wa0flL0Y: wa0flL0Y” 라는 이름의 Alternate Data Stream(ADS)에 실제 랜섬웨어 파일이 쓰여진다.



[그림 3] temp 폴더에 생성된 파일

1. 파일 및 디렉터리의 ADS 영역에 문자열 은닉 행위



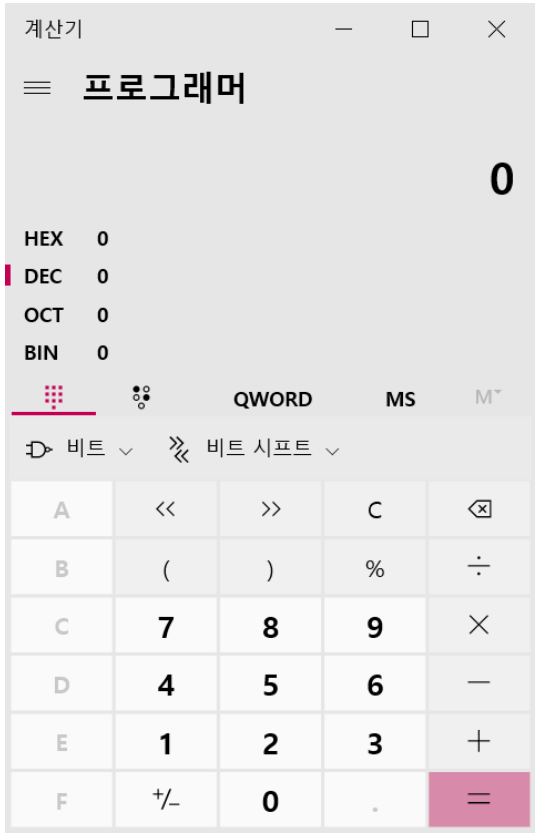
[그림 4] 커맨드 명령을 통해 확인한 실제 폴더구조

2. ADS 영역에 은닉된 실행 파일 실행 행위

```
C:₩Users₩djssl₩Desktop₩ADS>type C:₩Windows₩System32₩calc.exe > C:₩Users₩djss
l₩Desktop₩ADS₩data.txt:calc.exe
```

2. ADS 영역에 은닉된 실행 파일 실행 행위

```
C:₩Users₩djssl₩Desktop₩ADS>WMIC process call create C:₩Users₩djssl₩Desktop₩A
DS₩data.txt:calc.exe
(Win32_Process)->Create() 실행 중
메서드를 실행했습니다.
Out 매개 변수:
instance of __PARAMETERS
{
        ProcessId = 1464;
        ReturnValue = 0;
};
```



3. 파일 다운로드 경로 확인 행위

```
C:₩Users₩djssl₩Desktop₩ADS>dir /R
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 10:50    <DIR>          .
                                29 .:ads_data:$DATA
2021-05-02  오후 10:50    <DIR>          ..
2021-05-02  오후 10:47           277,786 test.pdf
                               137 test.pdf:Zone.Identifier:$DATA
               1개 파일             277,786 바이트
               2개 디렉터리  16,690,327,552 바이트 남음
```

3. 파일 다운로드 경로 확인 행위

```
C:₩Users₩djssl₩Desktop₩ADS>dir /R
 C 드라이브의 볼륨: 로컬 디스크
 볼륨 일련 번호: 74F3-F503

 C:₩Users₩djssl₩Desktop₩ADS 디렉터리

2021-05-02  오후 10:50    <DIR>          .
                                29 .:ads_data:$DATA
2021-05-02  오후 10:50    <DIR>          ..
2021-05-02  오후 10:47           277,786 test.pdf
                                137 test.pdf:Zone.Identifier:$DATA
               1개 파일             277,786 바이트
               2개 디렉터리  16,690,327,552 바이트 남음
```

3. 파일 다운로드 경로 확인 행위

```
C:₩Users₩djssl₩Desktop₩ADS>more < test.pdf:Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.google.com/
HostUrl=https://t1.daumcdn.net/cfile/tistory/1810F4314CE9CB4202?download
```

ReferrerUrl: 해당 파일을 다운로드 받은 경로

HostUrl: 해당 파일을 다운로드 받을 때 사용한 Url

감사합니다 ☺