안티 포렌식에 대해 알아보자

2025 WSP 동계 연합 세미나

PRESENTER | Ping! 임승연 EMAIL | lnsndus@gmail.com TEL. | 010-3349-5496

INDEX

1 Intro.

디지털 포렌식 (Digital Forensic)

⇒ "디지털 증거를 수집·보존·분석·현출하는데 적용되는 과학기술 및 절차를 말한다." – 대검찰청 예규

- 시스템 포렌식 — 서버나 PC 등을 대상으로 하는 디지털 포렌식 전반, OS에 따라 차이 ↑
- 네트워크 포렌식 — 통신 디바이스에서 패킷을 수집하여 저장하고 분석
- 모바일 포렌식 — 스마트폰의 등장 이후 성장한 분야, OS에 따라 분석 방법 다름
- 디스크 포렌식 — 저장매체에 관한 포렌식, 무결성, 동일성

- 이메일 포렌식, IoT 포렌식, 멀웨어 포렌식 등 ...

1 Intro.

디지털 포렌식 기본 원칙

- **정당성의 원칙 :** 적법한 절차에 의해 수집되었는지
- **무결성의 원칙 :** 수집 → 이송 → 분석 → 제출 과정에서 위변조 되지 않았는지
- **연계보관성의 원칙 :** 수집 → 이송 → 분석 → 제출 단계에서 관리가 명확했는지
- **신속성의 원칙 :** 모든 과정이 신속하게 진행되었는지
- **재현의 원칙 :** 같은 조건과 상황에서는 항상 같은 결과가 나오는지

2 안티 포렌식 개요

- Anti-Anti Forensic을 소개하기 위한 빌드업

안티 포렌식 (Anti Forensic)이란?

정의

자신에게 불리하게 작용할 가능성이 있는 증거물을 훼손하거나 차단하는 행위

목적

- 탐지를 회피하거나 정보 수집을 방해
- 조사관의 분석 시간 증가
- 도구의 실행을 방해 또는 오류를 발생 시킴
- 증거로서 가치가 없도록 훼손

2 안티 포렌식 개요

안티 포렌식

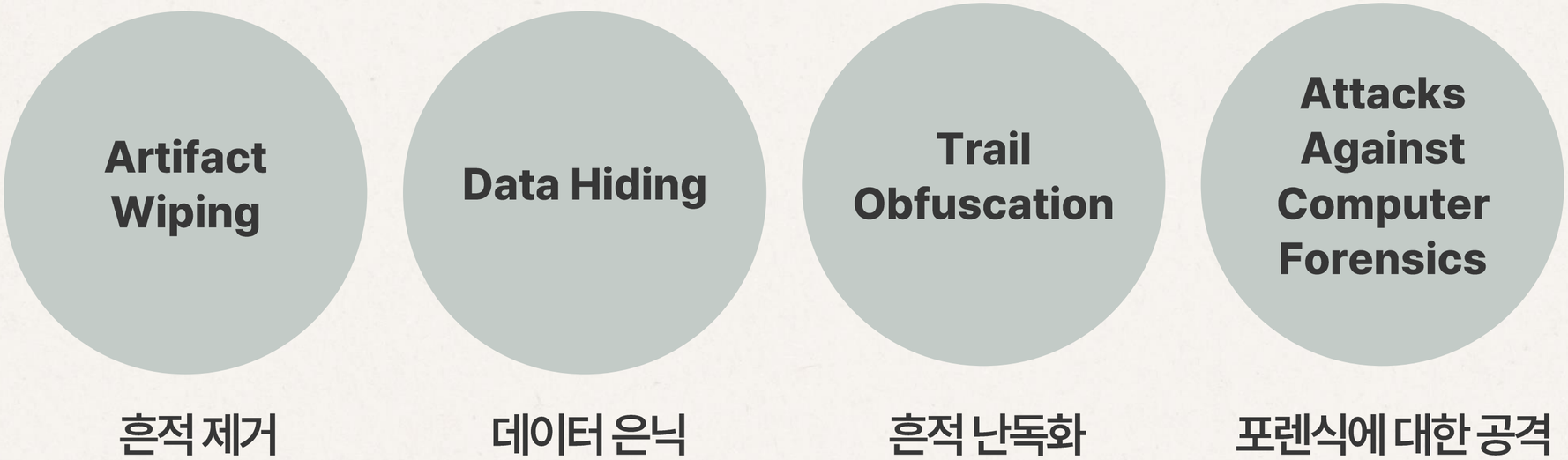
조사를 방해하기 위해 증거를
의도적으로 파괴

정보 보호

사용자 / 기업 입장에서
기밀 데이터 또는 개인정보보호를
위한 파괴

- 같은 기법을 사용하더라도 상황과 의도에 따라 달라질 수 있음

3 안티 포렌식 기법



4가지 기법 분류

3 안티 포렌식 기법(1)

Artifact Wiping

흔적 제거

- **파일 / 폴더 삭제 → 파일 카빙 복구 가능**
- **레코드**(DB, 스마트폰의 채팅, 문자 등) **삭제**
- **사용 흔적 삭제 도구를 이용**

  : Ccleaner, EasyCleaner 등
- **파일 시스템 포맷 → 완전 삭제의 경우 복구 불가**
- **소프트웨어 기반의 완전 삭제**

  : 덮어쓰기
- **하드웨어 기반의 완전 삭제**

  : 디가우징(Degaussing)

  : 물리적 천공 및 파쇄

3 안티 포렌식 기법(2)

Data Hiding

데이터 은닉

- 데이터 구조 이용

  : 파일 헤더 구조체의 사용되지 않는 영역

  → 데이터 구조에 사용되지 않는 필드 검증
- 슬랙 영역 이용

  : 물리적 구조와 논리적 구조의 차이로 발생하는 낭비되는 공간

  → 슬랙 공간 검증
- 스테가노그래피 기법

3 안티 포렌식 기법(3)

Trail Obfuscation

흔적 난독화

- 인코딩

  : 분석 아티팩트에 맞게 다양한 인코딩 방법
- 난독화

  : 프로그래밍 언어로 작성된 코드나 바이너리를 분석하기 어렵게 만듦
- 암호화

  : 알고리즘을 이용해 정보를 확인할 수 없도록 변형

3 안티 포렌식 기법(4)

Attacks Against Computer Forensics

포렌식에 대한 공격

- **데이터 조작**
  : 타임스탬프, 시스템 로그 조작
- **포렌식 도구 취약점 공격**
- **데이터 폭탄 공격**
- **안티포렌식 악성코드**

4 안티 포렌식 예시

스테가노그래피 이용한 문제(워게임)

PDF Analysis

main Back

* 안내 : 본 PDF 파일은 PC에 유해한 작업을 하지 않습니다. 단순 문제 풀이용입니다.

악성코드가 첨부된 PDF를 분석하여 Flag를 찾으세요.

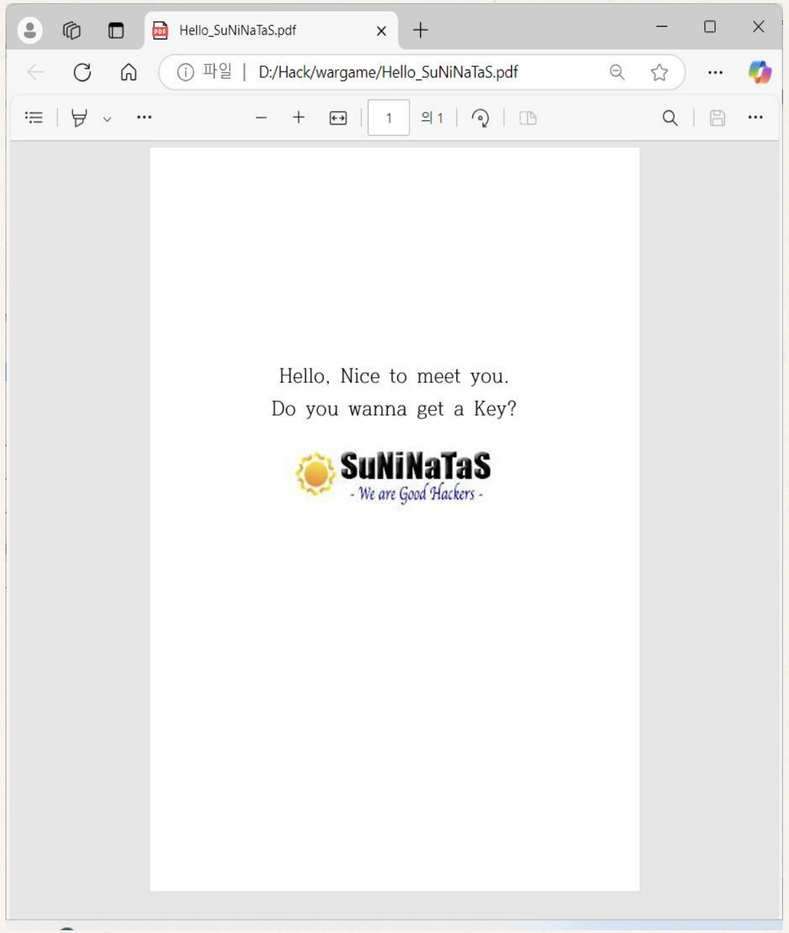
인증키 형식 : lowercase(MD5(Flag))

* Info : This PDF file don't attack your PC. Just using for study.

Analyze this PDF and Find a Flag.

Auth Key = lowercase(MD5(Flag))

down



- 악성코드가 첨부된 PDF
- 인증키 형식 → Flag 형식

4 안티 포렌식 예시

```
┌──(kali㉿kali)-[~/Downloads/peepdf]
└─$ python2 peepdf.py -i /home/kali/Downloads/Hello_SuNiNaTaS.pdf
Warning: PyV8 is not installed!!
Warning: pylibemu is not installed!!
Warning: Python Imaging Library (PIL) is not installed!!

File: Hello_SuNiNaTaS.pdf
MD5: 2a7a558ca100a0d9b9cf8973a0ad8424
SHA1: 8ed5e1da7f1021860ae56008788dd5892ce5b58c
SHA256: d1d3fd81952ffab1d52509a0d6dd7bcd27017e082ec99d4b0c4a0004577c4fdf
Size: 25232 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 1
Objects: 40
Streams: 11
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 2
        Info: 4
        Objects (29): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
        Streams (8): [14, 13, 6, 18, 19, 20, 22, 23]
                Encoded (6): [14, 13, 6, 19, 20, 22]
                Decoding errors (1): [13]

Version 1:
        Catalog: 2
        Info: 4
        Objects (11): [2, 4, 23, 30, 31, 35, 36, 37, 38, 39, 40]
        Streams (3): [23, 37, 39]
                Encoded (1): [39]
        Objects with JS code (1): [37]
        Suspicious elements:
                /OpenAction (1): [39]
                /Names (3): [2, 31, 38]
                /JavaScript (3): [30, 36, 39]
                /JS (2): [35, 39]
                /EmbeddedFiles: [30]
```

```
Catalog: 2
Info: 4
Objects (11): [2, 4, 23, 30, 31, 35, 36, 37, 38, 39, 40]
Streams (3): [23, 37, 39]
        Encoded (1): [39]
Objects with JS code (1): [37]
Suspicious elements:
        /OpenAction (1): [39]
        /Names (3): [2, 31, 38]
        /JavaScript (3): [30, 36, 39]
        /JS (2): [35, 39]
        /EmbeddedFiles: [30]
```

- peepdf : pdf 분석 도구
- 수상한 object 37, 39

4 안티 포렌식 예시

```
PPDF> stream 39

%PDF-1.7
%◆◆◆◆◆◆
1 0 obj
<< /Type /Catalog
/Pages 2 0 R
/OpenAction 4 0 R >>
endobj

2 0 obj
<< /Kids [ 3 0 R ]
/Type /Pages
/Count 1 >>
endobj

3 0 obj
<< /Parent 2 0 R
/Type /Page
/Resources << >>
/MediaBox [ 0 0 600 800 ] >>
endobj

4 0 obj
<< /Type /Action
/S /JavaScript
/JS 5 0 R >>
endobj

5 0 obj
<< /Length 45
/Filter /FlateDecode >>
stream
◆◆4◆◆◆◆lB◆◆◆◆◆◆"]◆^w
c◆◆◆◆◆Q◆◆k◆◆◆É◆◆

endstream
endobj
```

```
4 0 obj
<< /Type /Action
/S /JavaScript
/JS 5 0 R >>
endobj

5 0 obj
<< /Length 45
/Filter /FlateDecode >>
stream
◆◆4◆◆◆◆lB◆◆◆◆◆◆"]◆^w
c◆◆◆◆◆Q◆◆k◆◆◆É◆◆

endstream
endobj

xref
0 6
0000000000 65535 f
0000000017 00000 n
0000000085 00000 n
0000000145 00000 n
0000000236 00000 n
0000000297 00000 n
trailer
<< /Size 6
/Root 1 0 R
/ID [ (1d31cbadbd55f4859fcc1dcbd1b1a79e) (1d31cbadbd55f4859fcc1dcbd1b1a79e) ]
/Encrypt << /O (6Eu;|◆,\(◆fZ◆◆5?◆4◆Sh◆◆◆◆\\W◆)
/Filter /Standard
/Length 128
/V 2
/U (◆8◆/◆◆◆◆◆1□#◆\rs◆◆8~r◆ksl□;◆◆◆)
/R 3
/P 1073741823 >> >>
startxref
414
%%EOF
```

```
PPDF> stream 39 > obj39_stream.pdf
PPDF>
```

- stream 39 → 수상함
- obj 39의 데이터 정보

  %PDF-1.7

  → 파일 시그니처

  → 전체 PDF의 버전은 1.4
- 추출

4 안티 포렌식 예시

```
┌──(kali㉿kali)-[~/Downloads/peepdf]
└─$ python2 peepdf.py -i /home/kali/Downloads/peepdf/obj39_stream.pdf
File: obj39_stream.pdf
MD5: cba38ac7200a2a463b2177afcbf33490
SHA1: fbb4a23ea3b6769ae77c6656f7bee4e5c453b4ad
SHA256: 875712f32153cbfaf0b7d48a69ed17d6ce2725a89e8cecb9e23a37e5c8c59b08
Size: 823 bytes
Version: 1.7
Binary: True
Linearized: False
Encrypted: True (RC4 128 bits)
Updates: 0
Objects: 5
Streams: 1
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: No
        Objects (5): [1, 2, 3, 4, 5]
        Streams (1): [5]
                Encoded (1): [5]
        Objects with JS code (1): [5]
        Suspicious elements:
                /OpenAction (1): [1]
                /JS (1): [4]
                /JavaScript (1): [4]
```

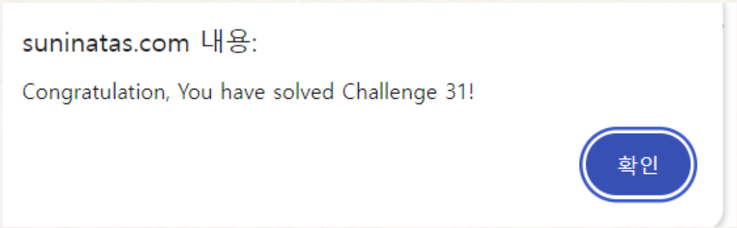
```
Streams (1): [5]
        Encoded (1): [5]
Objects with JS code (1): [5]
```

```
PPDF> stream 5

"HERE IS FLAGS SunINatAsGOodWeLL!@#$"
```

- Obj 5가 수상함
- Obj 의 데이터 정보

  → Flag 값?!
- 인증키 형식으로 입력



5 Anti-Anti Forensic

정의

- 안티 포렌식 기법에 대응하기 위한 기법

기법

- 데이터 복구
- 은닉된 데이터 탐지
- 조작된 증거 식별
- 아티팩트에 대한 연구 및 통합 분석

감사합니다.

Thank You

REFERENCE

- http://kcfpa.or.kr/bbs/board.php?bo_table=forensicnews&wr_id=6&sca=주요법률&sst=wr_datetime&sod=asc&sop=and&page=1
- http://forensic-proof.com/archives/4689
- https://github.com/proneer/Slides/blob/master/Advanced/(FP) 안티안티 포렌식 (Anti-Anti Forensics).pdf
- https://shalomlaw.co.kr/archives/1474
- A. Yaacoub, Jp & Noura, Hassan & Salman, Ola & Chehab, Ali. (2021). Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. 10.48550/arXiv.2103.17028.
- https://rohit12.medium.com/executed-anti-forensic-lab-using-steganography-e-mail-forensic-and-exif-metadata-techniques-all-d7b1bad61a32
- 한현동, 조영준, 조재연, 김세온, 한완섭, 최용준, 이정훈, 김민수. "안티 포렌식 동향 분석 및 대응 방안 연구." 융합보안논문지 23, no.1 (2023): 97-107.
- https://asec.ahnlab.com/ko/82150/
- 워게임 : Suninatas – Forensic 31번
- Chat GPT ...