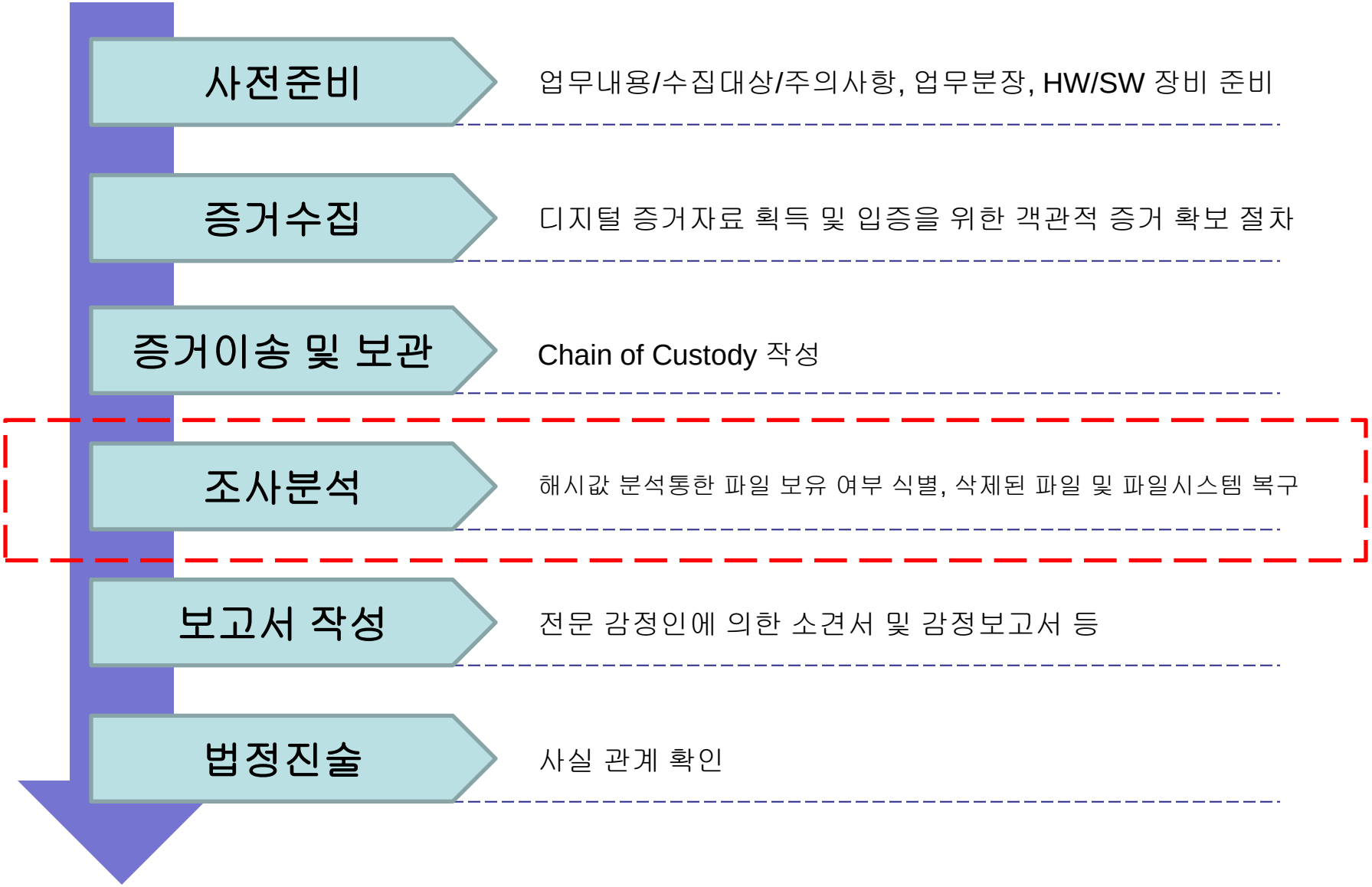
컴퓨터보안 실습

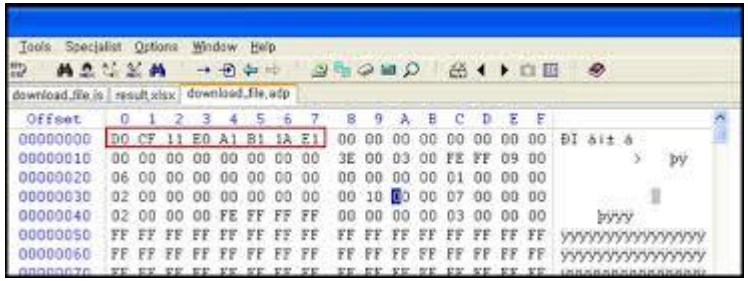
포렌식 실습(실습11)

조사 분석 – 파일 시그니처 분석

디지털포렌식 절차


사전준비
업무내용/수집대상/주의사항, 업무분장, HW/SW 장비 준비
증거수집
디지털 증거자료 획득 및 입증을 위한 객관적 증거 확보 절차
증거이송 및 보관
Chain of Custody 작성
조사분석
해시값 분석통한 파일 보유 여부 식별, 삭제된 파일 및 파일시스템 복구
보고서 작성
전문 감정인에 의한 소견서 및 감정보고서 등
법정진술
사실 관계 확인

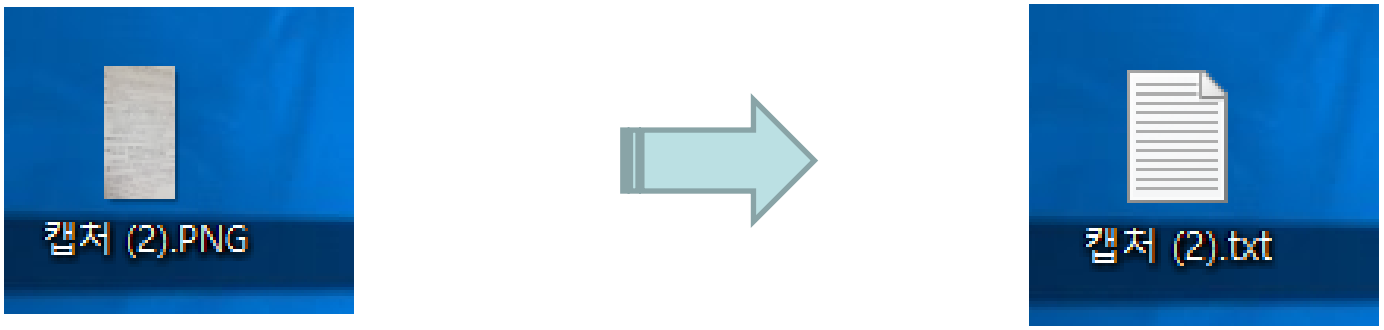
파일 확장자



[파일 시그니처]

- 소프트웨어가 데이터를 해석할 수 있도록 가지는 특정한 파일 형식
- 소프트웨어들은 자신만의 고유한 파일 포맷을 사용함
- EX) JPEG, GIF, DOC, PPT

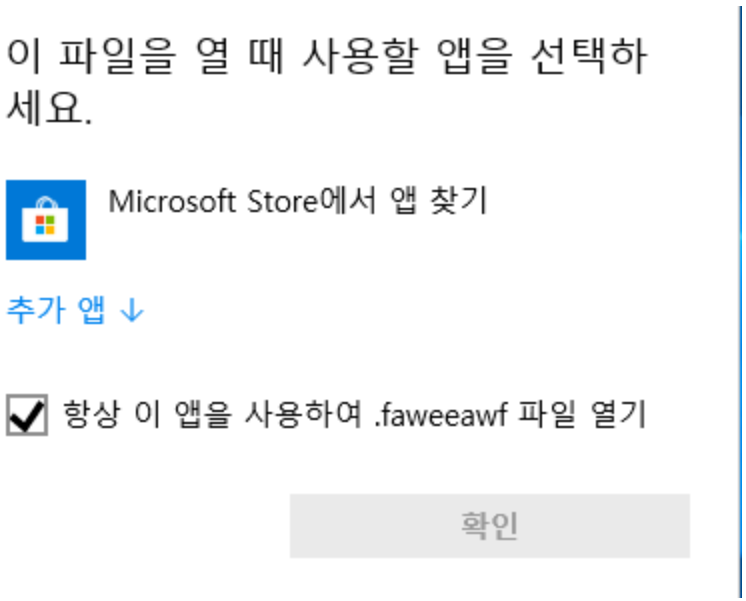
파일 확장자

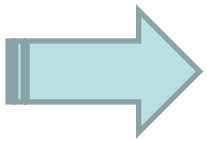


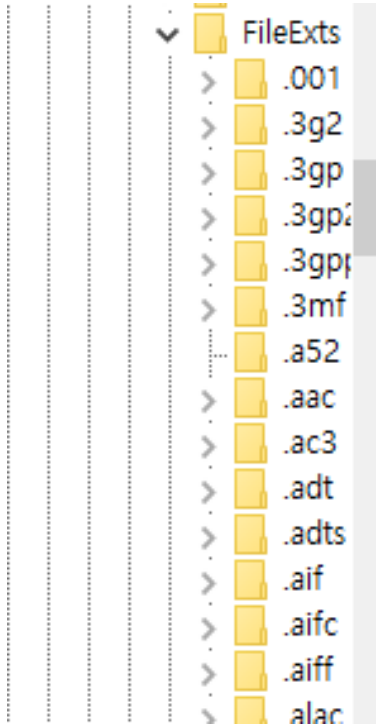
[파일 확장자 변경]

- 사용자는 확장자 변경으로 파일을 의도적으로 숨길 수 있음
- 또한 확장자에 따라 연결되는 어플리케이션이 달라짐

파일 확장자 분류

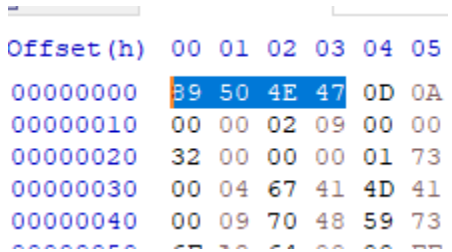






- 윈도우는 기본적으로 확장자 기반의 애플리케이션 바인딩 사용
- 파일의 이름 바꾸는 것 만으로 다른 소프트웨어에서 실행됨
- 애플리케이션 바인딩 정보는 레지스트리(HKEY_CURRENT_USER)에 저장
- HKEY_CURRENT_USER\Software\Micros oft\Windows\CurrentVersion\Explorer \FileExts

파일 시그니처 분석



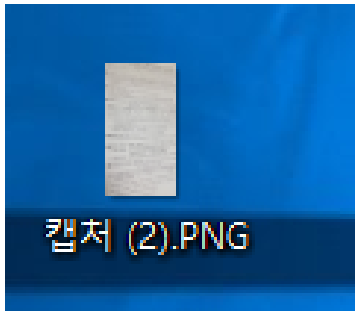
Offset(h)	00	01	02	03	04	05
00000000	89	50	4E	47	0D	0A
00000010	00	00	02	09	00	00
00000020	32	00	00	00	01	73
00000030	00	04	67	41	4D	41
00000040	00	09	70	48	59	73

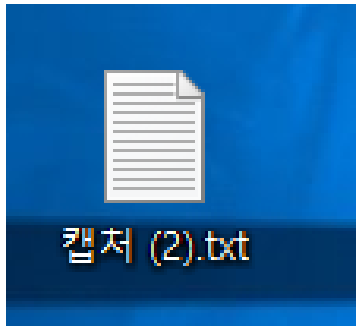
파일 포맷	시작 값(헤더)	마지막 값(푸터)
JPEG	FF D8 FF E0 00 FF D8 FF E1 00 ..	FF D9
GIF	47 49 46 38 37 61 or 47 49 46 38 39 61	00 3B
PDF	25 50 44 46 2D 31 2E	25 25 45 4F 46

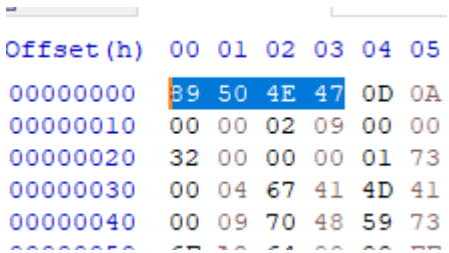
- HxD로 분석할 경우 처음에 존재하는 부분을 시그니처의 헤더, 마지막 값은 푸터라고 함
- 파일 시그니처는 파일 포맷 분석, 악성코드 분석, 복구 등에 중요하게 사용됨

- 시그니처 모음 : https://www.garykessler.net/library/file_sigs.html

(실습)파일 시그니처 분석





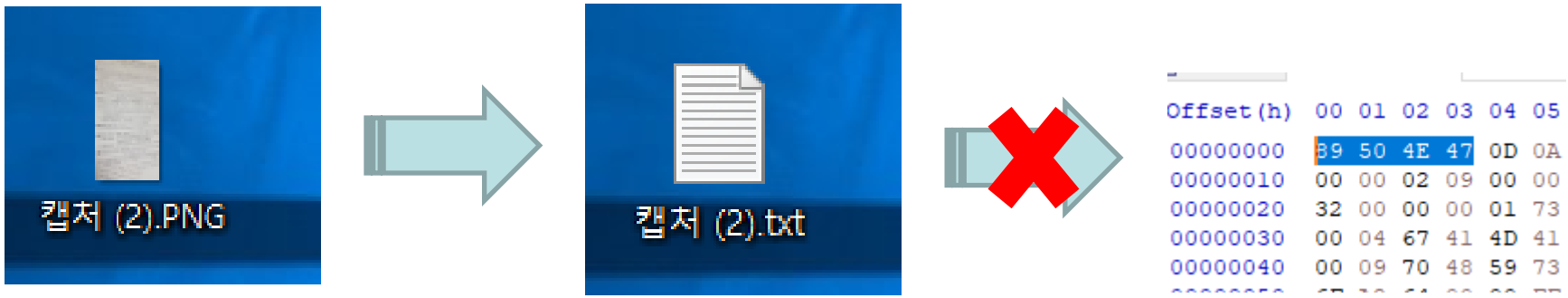


[파일 확장자 변경]

[HxD로 시그니처 분석]

1. 파일 임의 생성
2. HxD로 시그니처 분석 및 메모
3. 파일 확장자 임의 변경(JPG, PPT, EXE등등)
4. 다시 HxD로 분석하여 시그니처 변경여부 확인

(실습)파일 시그니처 분석



[파일 확장자 변경]

- 포렌식 툴로 쉽게 찾아지는 이유는 파일의 '시그니처 ' 가 있기 때문

파일 시그니처 활용

- 멀웨어(로키봇) https://www.malware-traffic-analysis.net/2019/03/15/index2.html

- .zipx → .PNG 로 시그니처까지 완벽 변조
→ 이는 보안 탐지 기술을 피하기 위함

- 사용자는 정상파일로 착각, 실행

- PNG 어플리케이션의 취약점 : IEND(이미지 끝부분 표시) 뒤 데이터에 악성 코드 삽입

- 어플리케이션의 취약점 + 시그니처 변조를 이용한 멀웨어

[Loki-Bot 변종]

참고문헌

- 정보 보안 개론[개정3판], 양대일 저, 한빛미디어, 2018, 1.
- 디지털 포렌식 개론(2판), 이상진 저, 이룬 출판사, 2015. 5.
- 컴퓨터보안, William Stalling 저, 한티미디어, 2016. 8
- 정보보안과 사이버 해킹의 기초, 김경신 저, 2016. 8
- RFC 3227, Guidelines for Evidence Collection and Archiving
- NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response
- https://www.boannews.com/media/view.asp?idx=78503

Q & A