2024. 10. 16. (수)
김 역

2024학년도 2학기
디지털포렌식 과제-①

세종사이버대학교
정보보호학과

I Exercise 1

문제설명 : 학습 자료실에서 제공된 링크의 이미지 파일을 다운받아 문제를 순서대로 풀어가면 됩니다. (1)에서 이미지를 복원하고, 복원한 이미지로 (2),(3),(4),(5) 문제를 해결해서 답안을 작성합니다. 작성한 내용은 pdf 파일 형식으로 제출합니다.

(1) 학습자료실의 링크를 이용해서 homework_2.001 파일을 다운로드해서 이미지를 복원하세요.

a) HxD를 이용해서 다운로드한 이미지의 SHA-256 해시값을 구하세요.

- 과제 제출 내용 : ① 해시값 ② HxD에서 SHA-256으로 해시값 구한 화면 캡쳐
- 게시판에 명시된 이미지 해시값과 비교해서 해시값이 다른 경우에는 다운로드 작업을 다시 해서 확인해야 함(다운로드시 파일이 손상되었을 수 있음)
- 다운로드한 이미지 무결성 값은 아래와 동일해야 함
- SHA-256 :
  0x09B03AC95C156B13FFF28ADF92D659B29135F4DB4D427ECE64A829BBBBE92655

b) 이미지 파일의 파일 시스템이 손상되어 있습니다. 이를 복원하세요.

- 과제 제출 내용 :

① 손상된 이미지를 FTK Imager에서 읽어와서 Evidence Tree 창 캡쳐

② 이미지 복원 과정 설명

③ 복원한 이미지를 FTK Imager에서 읽어와서 Evidence Tree 창 캡쳐

- 이미지 복원은 HxD를 이용해서 수행함

(2) SHA1의 해시값이 "6826890df368ede2eafe9277e68b2f2e209c1d15" 인 파일을 찾고 파일명, 파일 크기, 시간 정보를 구해주세요.

a) FTK Imager에서 폴더 내에 있는 파일들의 해시값 목록을 구하세요.

b) 무결성 값이 동일한 파일을 찾아 Properties를 확인하세요.

- 과제 제출 내용 : ① 해시값 목록 파일 캡쳐 ② 찾고자 하는 파일의 속성 창 캡쳐

(3) major_curriculmn.xlsx 파일 내용을 확인하려면 파일의 암호를 알아야 합니다. 이미지 내에 암호가 명시되어 있으니 확인해서 파일을 열어 확인하세요.

a) 암호 파일은 이미지 내에 있으니 해당 파일을 찾아 확인해 보세요.

- 과제 제출 내용 : ① 암호 찾는 과정 설명 ② major_curriculmn.xlsx 파일 내용 캡쳐

(4) 이미지에서 FAT1의 위치 주소와 크기를 계산하고, 루트 디렉토리에 위치한 sample.txt 파일 내용이 있는 클러스터에 해당되는 FAT1의 FAT entry를 확인해서 캡쳐하고 관련 내용을 설명해 주세요.

a) 예약 영역 정보를 이용해서 FAT1 주소와 크기를 계산합니다.

- 과제 제출 내용 : ① 관련된 자료가 있는 예약 영역 위치와 해당 화면 캡쳐
- ② ①에서 확인한 정보를 이용해서 FAT1의 주소와 크기 계산 절차와 결과 값

b) sample.txt가 저장된 클러스터와 주소를 계산해서 해당 내용에 sample.txt 내용이 있는지 확인합니다.

- 과제 제출 내용 : ① sample.txt 파일에 대한 directory entry를 찾아 클러스터 값을 계산하는 절차와 결과값
- ② ①에서 확인한 정보를 이용해서 sample.txt 파일이 있는 화면을 주소가 보이도록 화면 캡쳐

c) FAT1에서 sample.txt 파일에 해당되는 FAT entry를 찾아 봅니다.

- 과제 제출 내용 : ① FAT1에서 sample.txt 파일에 대한 FAT entry 표시한 화면 캡쳐