ENGINEERING. SCIENCE. COMPUTING.	# 수학과학체험전	중학교: 이름:

HEX 코드와 HxD

#HEX코드란 데이터를 [16진수]로 표현한 값을 의미한다.

-8bit 단위로 만들어진 Hash 값을 문자로 표기할 때

-RGB를 문자로 표기할 때

대부분의 경우, 컴퓨터 내부 데이터(0과 1의 조합)를 사람이 **간단하고 알아보기 좋게** 표시하기 위해 사용한다.

예) 10진수 : 255 = 2진수 : 1111111 = 16진수 : FF

(2진수를 16진수로 변환할 때 4자리씩 끊어서 분석하면 편리하다)

#HxD(HEX editor)란 파일, 디스크, 메모리, 덤프를 16진수 형식으로 보여주고,
[분석] 및 [수정]할 수 있는 도구이다.

-분석: 파일의 헤더 정보, 바이너리 데이터, ASCII 값

-이용 분야: 디지털 포렌식, 리버스 엔지니어링, 데이터 복구, 코드 분석

#용어 정리

Hash 값: 어떤 데이터(문자, 파일 등)를 암호처럼 바꾼 고정된 길이의 숫자. 예) SHA-256, MD5

덤프(dump): RAM이 같은 내부기억장치의 내용을 프린터와 같은 외장하드 등 외부기억장치에 복사하는 것

파일 헤더 정보: 파일 맨 앞부분에 있는 파일의 종류와 구조를 설명하는 정보.
예) PNG 파일은 항상 '.PNG'로 시작함

바이너리 데이터: 사람이 읽기 어려운 0과 1로 구성된 데이터, 모든 프로그램, 이미지, 영상은 결국 이 형태로 저장됨.

ASCII 값: 문자(A, B, 1, ! 등)를 숫자로 표현하는 국제 표준.
예) 문자 A의 ASCII 값은 65, 16진수로는 41

디지털 포렌식: 디지털 장치에서 증거를 찾는 작업

리버스 엔지니어링: 완성된 프로그램(또는 기계)을 거꾸로 분석해서 어떻게 만들어졌는지 알아내는 작업
예) 실행 파일을 Hex Editor로 열어서 내부 코드를 분석하는 것

숨겨진 데이터 찾기 (비밀 메시지 찾기!)

1. HxD 파일 열기
2. 헤더 분석
3. 비정상적인 데이터 탐색 (의미 없는 텍스트나 알 수 없는 HEX 값)
4. 스테가노그래피의 탐색 (이미지 파일의 끝에 추가된 HEX 값 파악)

수학과학체험전

중학교:
이름:

시놉시스:

한성과학고 ESC 동아리는 매년 화려한 게임 기반 체험관으로 수학과학체험전의 하이라이트를 장식해왔다. 올해도 마찬가지로 행사를 준비하던 중, 충격적인 사건이 발생한다. 모든 파일이 완벽하게 삭제되었다. 내부 서버, 클라우드, 백업까지 모두 흔적도 없이 이미지 파일로 암호화 된 것.

복구 과정에서 클라우드 루트 디렉터리에 단 두 개의 파일만이 남겨진 것을 발견한다. 의문의 이미지와 수수께끼 같은 텍스트 파일이다. 더 충격적인 것은 모든 로그가 정상이라는 점. 침입 흔적이 전혀 없다. 이 공격자는 시스템 내부 구조를 완벽히 파악하고 있었다. ESC 부원이 아니면 불가능한 일이었다.

의혹의 그림자가 내부자로 점점 짙게 드리워지는 가운데, ESC는 체험전 운영을 단념하고 복구에 총력을 기울인다. 그리고 지금, 이 프로그램을 풀 수 있는 유일한 존재인 당신에게 SOS가 도착했다.

당신이 직면한 것은 단순한 활동이 아니다.

숨겨진 진실을 밝혀내고, 누구도 열지 못했던 비밀을 마주해야만 한다.

목표:

ESC의 파일을 모두 삭제한 범인을 확인하고, 범인이 숨기고 간 비밀번호를 통해 파일을 복구한다.

참고 자료:

JPG 파일:

이미지를 손실 압축할 수 있는 파일로서, 파일의 용량을 줄여 저장하는 이미지 파일이다. 통상적인 JPG 파일의 크기는 수십 MB 정도이다.

헤더와 푸터:

헤더와 푸터는 파을의 고유 형식을 알 수 있는 앞 뒤 주요한 HEX 코드를 의미한다. 이 코드를 통해 해당 파일 기록의 시작과 종료를 확인할 수 있으며, 만약 헤더와 푸터가 일치하지 않는다면 다음과 같은 결론 중 하나를 도출할 수 있다.

1. 파일이 손상되었다.
2. 뒤에 숨겨진 파일이 추가되었다.

한편, 앞 헤더와 뒤의 헤더가 일치하는 경우에도 안심할 수 없다. 같은 파일이 두 개 이상 겹쳐 있을 수도 있기 때문이다. 이를 확인하기 위해서는 동일한 헤더와 푸터가 한 번씩만 나오는지 확인하는 작업이 필수이다.

파일 형식	확장자	헤더 (Header, HEX)	푸터 (Footer, HEX)
JPEG	.jpg	FF D8 FF	FF D9
PNG	.png	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
GIF	.gif	47 49 46 38 37 61 또는 47 49 46 38 39 61	00 3B
PDF	.pdf	25 50 44 46	25 25 45 4F 46 또는 0A 25 25 45 4F 46
ZIP	.zip	50 4B 03 04	50 4B 05 06 또는 50 4B 06 06
RAR (v1.5)	.rar	52 61 72 21 1A 07 00	없음 (또는 구조상 EOF 없음)
7z	.7z	37 7A BC AF 27 1C	없음 (구조상 내부 존재)
HWP(한글)	.hwp	48 57 50 20 00 00 00 00	없음 (구조상 내부 구조 다름)

FLAG:

FLAG란 해당 어떤 암호문에 숨겨져 있는 키를 뜻한다. FLAG는 주로 FLAG{(내용)}으로 표기하며, 이를 이용하여 결정적 단서를 찾거나 암호를 해석하는 데 도움을 받을 수 있다.

기타 단축키:

ctrl + F : 파일에서 찾기 / ctrl + N : 새 파일 / ctrl + S : 저장하기 / ctrl + O : 파일 열기 /
클릭 → shift + 클릭 : 전 클릭 지점부터 후 클릭 지점까지 복사하기

ENGINEERING. SCIENCE. COMPUTING.	# 수학과학체험전	중학교: 이름:

튜토리얼:

증거 자료(evidence.jpg)에 수상한 흔적이 있는지 확인해보자.

1. evidence.jpg 파일을 이미지 뷰어로 열어보자.
   1.1. 어떠한 모습의 이미지인가(간단히)?
   1.2. 이미지에서 발견할 수 있는 단서는 무엇인가? 단서는 모니터 안에 있다.

2. evidence.jpg 파일을 HxD 에디터로 열어보자.
   2.1. 해당 파일의 헤더(시작하는 두 개의 마디)는 무엇인가?
   2.2. 해당 파일의 푸터(끝나는 두 개의 마디)는 무엇인가?
   2.3. .jpg 파일의 헤더와 푸터는 무엇인가?
   2.4. 해당 파일에 사용된 기법은 무엇인가?
   2.5. 해당 파일 안에는 어떠한 파일이 숨겨져 있는가?
   2.6. 해당 파일 안에는 어떠한 비밀 메세지(FLAG)가 숨겨져 있는가?

결과적으로, 해당 파일을 통해 알아낸 결정적 결론은 무엇인가?

활동 체크:

1. 해당 사건의 범인은 어떠한 이유로 사건을 일으켰는가?

2. 해당 사건의 용의자는 누구인가(3명)?

3. 해당 사건의 범인은 누구인가?

4. 숨겨진 폴더에는 무엇이 들어있었는가(관계자한테 보여주세요).

ENGINEERING. SCIENCE. COMPUTING.	# 수학과학체험전	중학교: 이름:

연습 용지:

설문조사(시작하라고 말할 때 해 주세요):

본 설문은 ESC에서 자체 평가 및 방향성을 수립하기 위해 진행하는 것으로, 학교 측과는 무관합니다.
설문의 익명성은 보장됩니다. 설문은 ESC 자체 평가를 위한 자료로, 외부에 전달 및 유출되지 않습니다.

아래 링크에 접속해주세요:
https://forms.gle/8k8MMJuHpX2Vp3Gj8

수학과학체험전에 참여해주셔서 대단히 감사합니다.
앞으로의 미래를 응원합니다.