대 본(어미는 나중에 통일을 시키면 될 듯)

– 인삿말
안녕하세요, 이번 '장군님 암호문 쓰신다 - 스테가노그래피 해석' 에 오신 여러분을 환영합니다. 저희는 발표를 맡은 진용훈, 신재훈입니다.
순서는 다음과 같습니다.
시작하기에 앞서,
여러분들이 활동을 할 때 필요한 기본적인 지식들과 툴 사용법, 이론들을 10분가량 설명드릴 거고요, 제일 빠르게 활동을 끝낸 3명에게는 한성 과학고가 각인되어있는 주문제작 샤프가 준비되어 있으니 잘 듣고 받아가시길 바라겠습니다

– 목차소개
빠르게 목차 소개 하겠습니다. 보안의 중요성부터 시저 암호, 헥스 코드와 포렌식, 스테가노그래피까지 이론 설명을, 기초적인 툴 설명과 분석으로 실습에 관련된 설명을 드릴 겁니다.

– 최근 사건 소개, 보안 중요성 설명
먼저 보안의 중요성입니다. 최근에 큰 사건이 두개 연달아 터졌죠? 하나는 sk 유심 칩 사태로 여기 계신 분들 중 몇몇도 아마 칩을 바꾸거나 통신사를 바꾸려고 생각 중일 거예요. 또한, sk가 해킹당하기 전에 오라클이라는 미국 소프트웨어 회사의 DB가 털렸었어요. '–로그인' 같은 기능 한번쯤은 보셨을 거에요. 이런 기능들을 Auth라 하는데, 이번에 오라클이 털리며, 이런 로그인 데이터들이 전부 유출되어서 여러 사용자들이 피해를 입었어요. 저희야 뭐 개인정보가 공공재라고 자조어린 소리를 하긴 하지만, 이런 부분에서 민감한 서양쪽은 민감한 이야기이기도 하고, 오라클이 동네 중소기업이 아니라 세계적인 빅테크 기업이기 때문에 보안의 중요성이 다시 화제에 오르는 사건이였죠. 이런 사례들로 볼 수 있듯이 한 번 성공하는 순간 막대한 재산피해를 유발할 수 있는 게 해킹이기 때문에 이를 방지하는 보안이 중요한 거고요.

– 스테가노그래피 설명
본격적인 설명에 들어가기 전에, 스테가노그래피에 대하여 설명하겠습니다. 어원은 그리스어, 숨겨진이라는 의미의 steganos 와 쓰다 라는 의미의 graphein이 합쳐진 단어에요. 이름에서 유추할 수 있는 것처럼 스테가노그래피는 이미지, 텍스트나 오디오 등 자료에 데이터를 숨겨 놓는 방식을 통칭하는 용어에요. 스테가노그래피는 우리가 생각하는 디지털 스테가노그래피 뿐만 아니라 어떠한 물체를 이용하기도 했어요. 고대 그리스에서는 맨머리에 메시지를 새긴 후 자란 머리카락으로 메시지를 가리거나 나무판에 메시지를 새기고 왁스로 덮어 숨기는 방식을 이용했어요. 중세에서는 잉크 기술이 발전했기에 보이지 않는 잉크가 개발되었고 우유, 레몬즙, 식초 등을 이용해 글을 적고 열을 가해 글자가 나타나는 방식도 이용하였습니다. 전근대 시대에서는 스테가노그래피에 대한 문서가 출판되었고 매체에 메시지를 숨기거나 언어를 활용하여 암호화시켰습니다. 현재에 이르러 우리가 이용하는 디지털 스테가노그래피는 비트 단위로 데이터를 기술로 은닉하며 LSB 기법을 이용해 이미지 파일의 마지막 비트에 정보를 숨기는 등 탐지하기 어려운 기술이 발전하게 되었습니다.

– HEX 코드랑 HxD(헥스 에디터) 설명
실습에 관련된 개념이나 툴 사용법들을 알려드리겠습니다. 이번 활동에서는 파일을 16진수 - Hex 코드르 보여주는 헥스 에디터라는 프로그램을 사용할 거에요. 16진수는 말 그대로 자릿수 하나마다 0에서 f까지, 16개의 숫자를 사용하는 수 체계이고요, 왜 하필 16진수를

사용하냐 하면, 컴퓨터가 기본적으로 처리하는 2진수와, 사람들이 알아들을 수 있는 문자 사이에서 찾은 합의점이기 때문이에요. 16진수 정도면 2진수에서 변환하기에도, 사람들이 이를 표와 데이터를 이용해 문자로 바꿔 보기에도 별 어려움이 없다는 거에요.
헥스 에디터는 이진수로 되어있는 파일들을 각각 16진수와, 이를 변환하여 문자열로 나타낸 걸 보여주는 툴이에요. 이를 통해서 확장자를 지칭하는 헤더나 이번에 자주 보게 될 숨겨진 문자열을 찾는 등 여러 방면으로 사용할 수 있어요.

```
증거 자료 파일(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?
```