206 – Secret message

Team Information

Team Name : DogeCoin

Team Member : Dongbin Oh, Donghyun Kim, Donghyun Kim, Yeongwoong Kim

Email Address : dfc-dogecoin@naver.com

Instructions

Description. An investigator found a suspicious file.

Target	Hash (MD5)
Monthly Report.docx	208a9911b6ff922fe228812b0bf61dce

Questions

Find a hidden message in 'Monthly Report.docx' and then complete the following sentence.

"Get (something) **from** (name) **at** (location) **at** (date & time)**."**

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

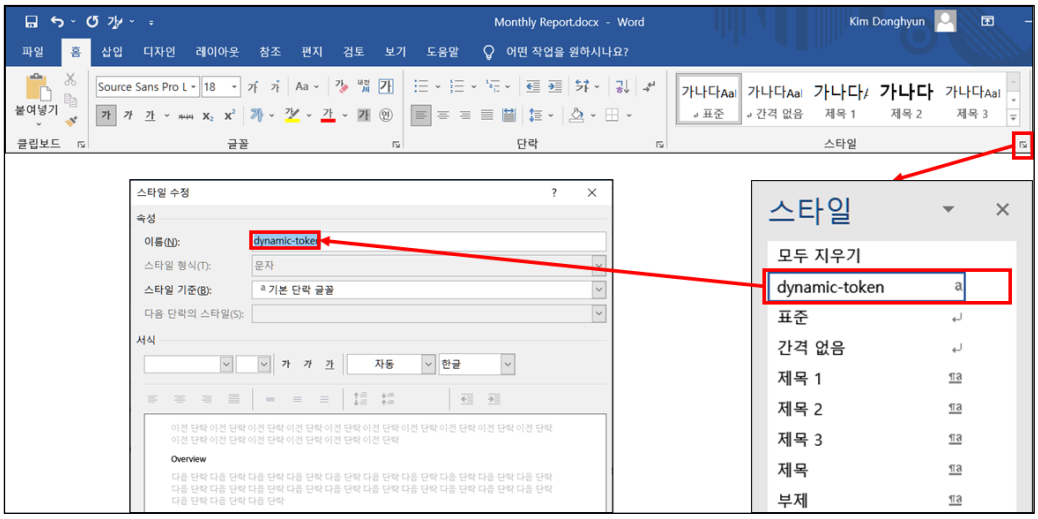
Name:	Word Microsoft 365	Publisher:	Mircosoft
Version:	16.0.14228.20200		
URL:	https://www.microsoft.com/ko-kr/microsoft-365/buy/compare-all-microsoft-365-products?ocid=oo_support_mix_marvel_ups_support_smcuhfbnpromo&rtc=1#		

Name:	Python	Publisher:	Python Software Foundation
Version:	3.8.6		
URL:	https://www.python.org/downloads/release/python-386/		

Step-by-step methodology:

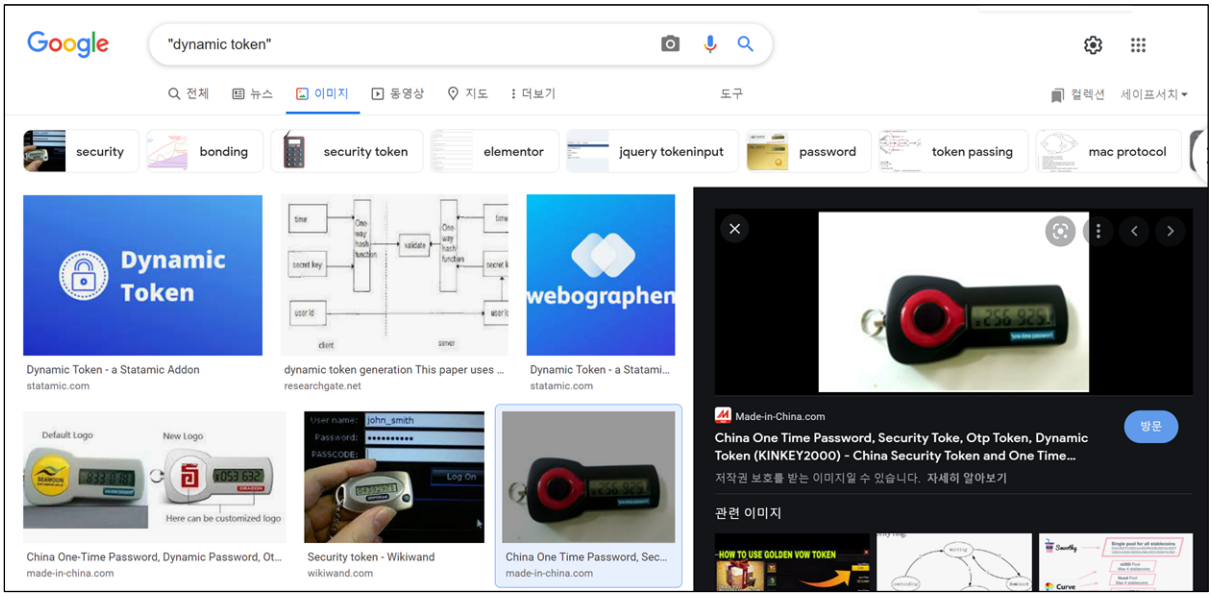
1. How to find “Something”.

스타일 설정 (단축키: Ctrl + Alt + Shift + S) 창을 통해서 “dynamic-token” 이름으로 숨겨진 스타일을 발견할 수 있었다.



[그림 1] 숨겨진 스타일

dynamic-token이 실제로 존재하는 물건인지 확인하기 위해 구글에 검색하였다. dynamic-token은 OTP (One Time Password), Security token과 같이 일회용 비밀번호 장치를 나타내는 용어 중에 하나였다. 따라서, dynamic-token은 문제에서 요구하는 **“Something”**에 부합한다.

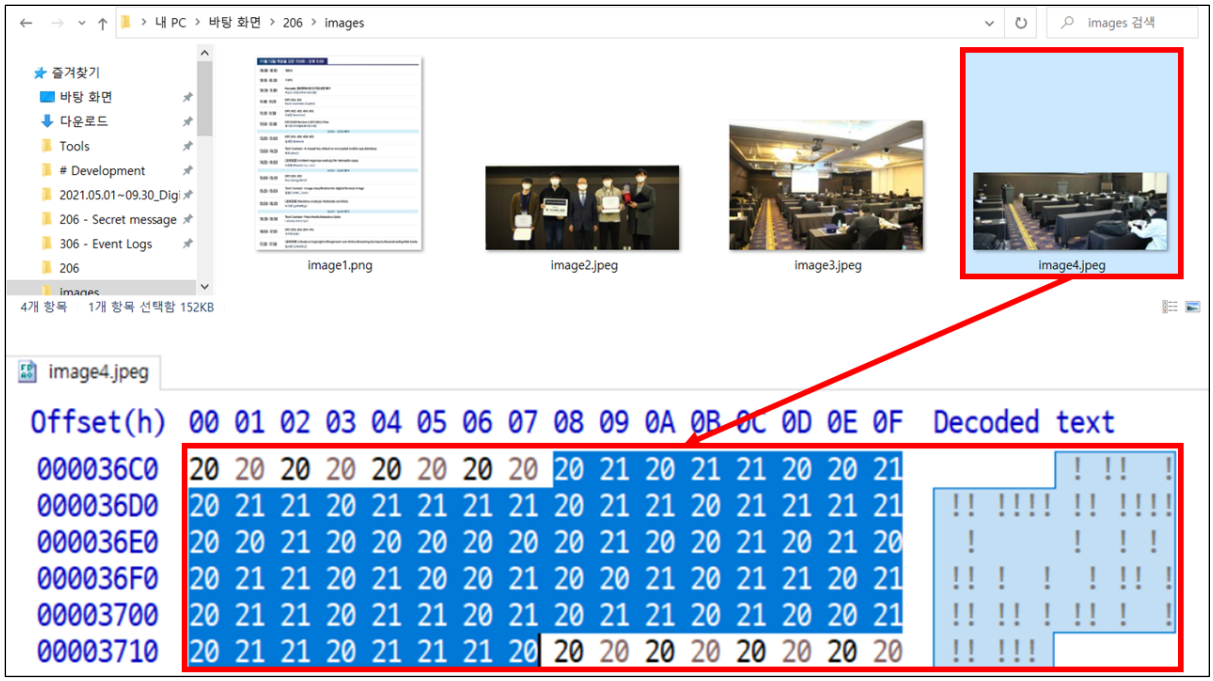


[그림 2] dynamic-token 검색 결과

답: dynamic-token

2. How to find “name”.

주어진 문서에 삽입된 이미지는 총 4개이다. 문서를 압축 해제하여, 각 이미지의 원본을 확인하면 4번째 이미지에서 의심되는 문자열을 확인할 수 있다.



[그림 1] 의심되는 문자열을 포함하는 이미지 (Image4.jpg)

다음과 같은 Python 소스코드로 “ “ (스페이스 공백)은 0으로, “!” (느낌표)는 1으로 변환하여 디코딩한 결과, 이름을 확인할 수 있었다.

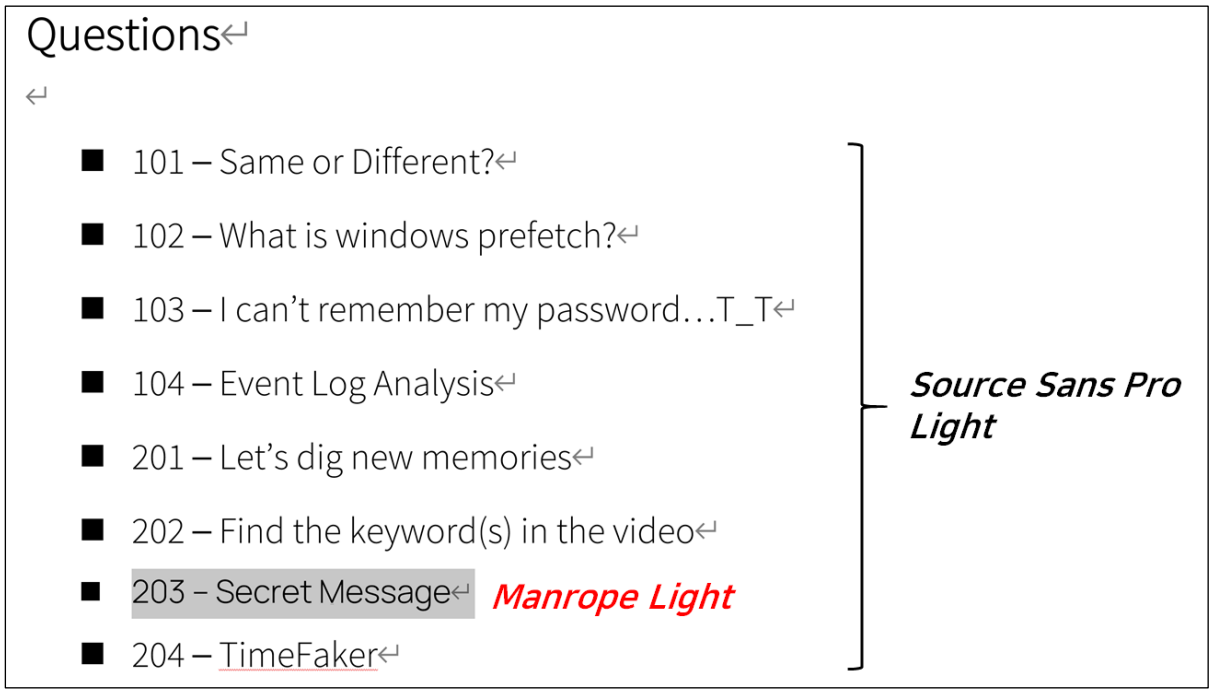
```
enc_message = "20 21 20 21 21 20 20 21 20 21 21 20 21 21 21 21 20 21 21 20 21 21 21 21
20 20 21 20 20 20 20 20 20 21 20 20 21 20 21 20 20 21 21 20 21 20 20 21 20 20 21 20 21
21 20 21 20 21 21 20 21 21 20 21 20 21 21 20 21 20 20 21 20 21 21 20 21 21 21 20"
bins = enc_message.replace("20", "0").replace("21", "1").replace(" ", "")

result = ""
for x in range(0, len(bins), 8):
    result += chr(int(bins[x:x + 8], 2))
print(result)           # Yoo Ji-min
```

[그림 2] 의심되는 문자열 변환 소스코드

답: Yoo Ji-min

3. How to find “location”.

기본적으로 주어진 문서에는 Source Sans Pro Light라는 폰트가 사용되었다. 하지만, **[그림 3]**과 같이 DFC 2020에 출제된 문제 목록을 나열한 Question에서 “203 - Secret Message” 항목만 폰트가 Manrope Light로 다른 것을 확인하였다.



[그림 3] Question 부분에서 폰트가 다른 항목

해당 항목을 글꼴 및 화면 확대를 통해서 확인하면, 문자 “M”에서 숨겨진 위치를 확인할 수 있었다.

[그림 4] 문자 “M”을 확대하여 발견한 위치(Location)

답: 51, Jong-ro, Jongno-gu, Seoul

4. How to find “date & time”.

다음의 정보는 바닥글에서 발견할 수 있었다. 흰색으로 은닉된 글자를 검은색으로 변경하여 날짜를 확인하였다. 은닉된 날짜는 두번째 페이지부터 바닥글에서 확인할 수 있다.

[그림 5] 바닥글에 흰색으로 은닉된 날짜 발견

[그림 6] 바닥글에 흰색으로 은닉된 날짜 확인 (검은색 변경)

답: 2 p.m. on June 30

5. Conclusion

지금까지 찾은 4 개 정보를 종합하면 **6월 30일 오후 2시 (2 p.m. on June 30), 서울특별시 종로구 종로2가 6 종로타워 (51, Jong-ro, Jongno-gu, Seoul)**에서 **유지민 (Yoo Ji-min)** 에게 **“dynamic-token”**을 받으라는 메시지를 확인할 수 있다.

> **“Get** dynamic-token **from** Yoo Ji-min **at** 51, Jong-ro, Jongno-gu, Seoul **at** 2 p.m. on June 30**.”**

[그림 7] 획득한 정보를 기반으로 조합한 은닉 메시지