컴퓨터보안 실습

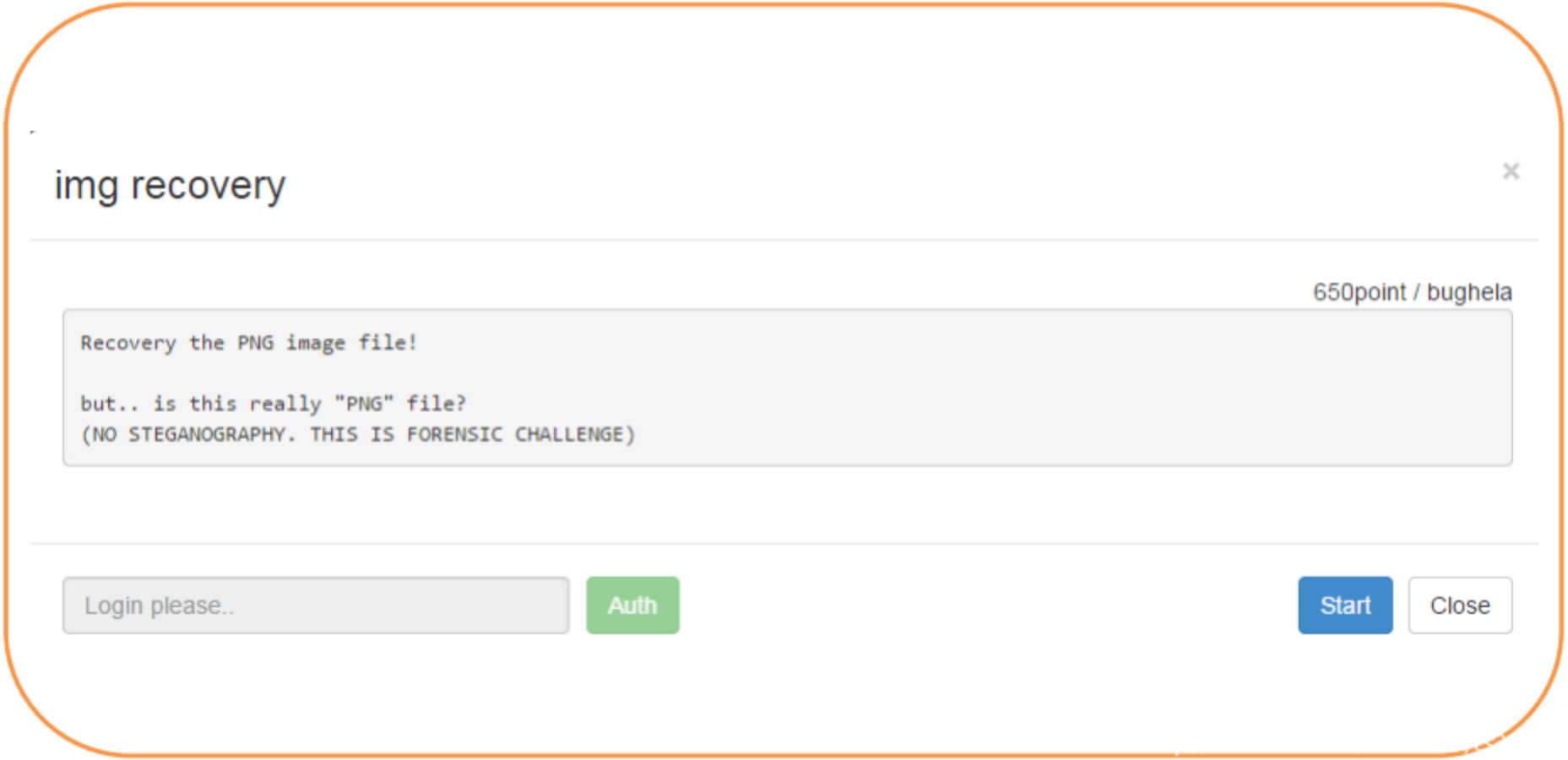
이미지 파일 포렌식 실습

워게임 문제 풀이

이미지 복구

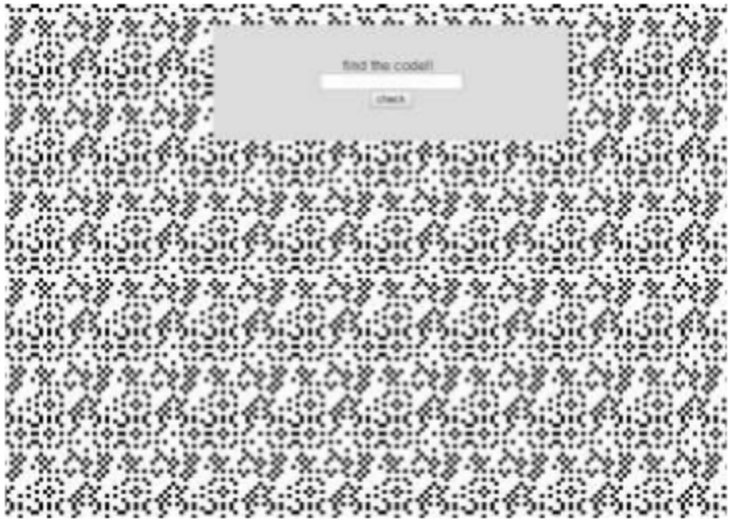
워게임의 일종이자 이미지 파일내에 숨겨진 의미를 파악하는 포렌식 실습

http://wargame.kr/challenge



이미지 다운로드

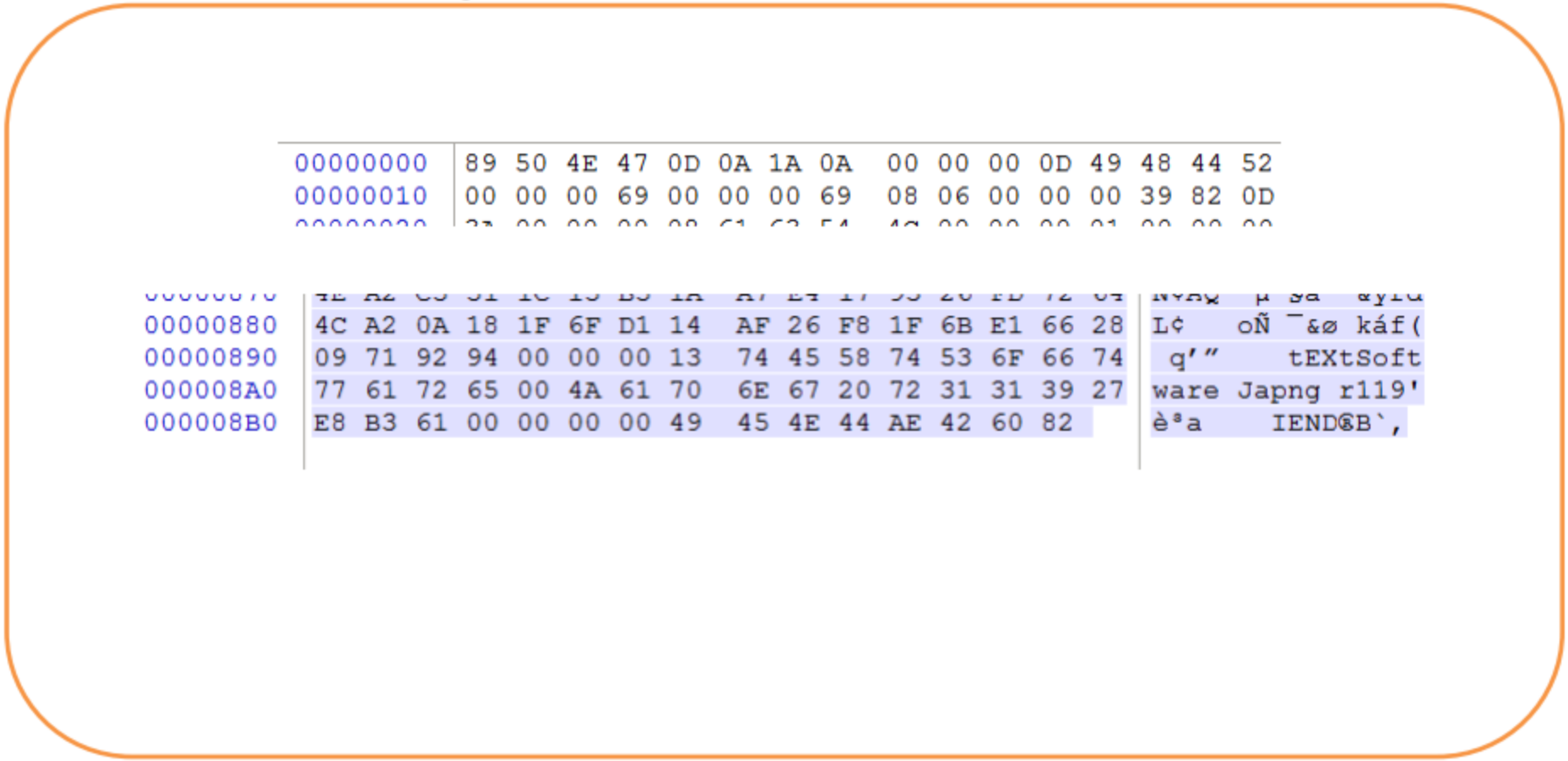
http://wargame.kr:8080/img_recovery/pattern.png
위의 URL로 접속하면
QR코드와 비슷하게 생긴 패턴의 이미지 파일을 찾아낼 수 있다.



Pattern.png

이미지 분석

WinHex 프로그램을 통해 헥사 데이터를 확인한다.
파일의 끝에 Software Japng 를 확인할 수 있다.



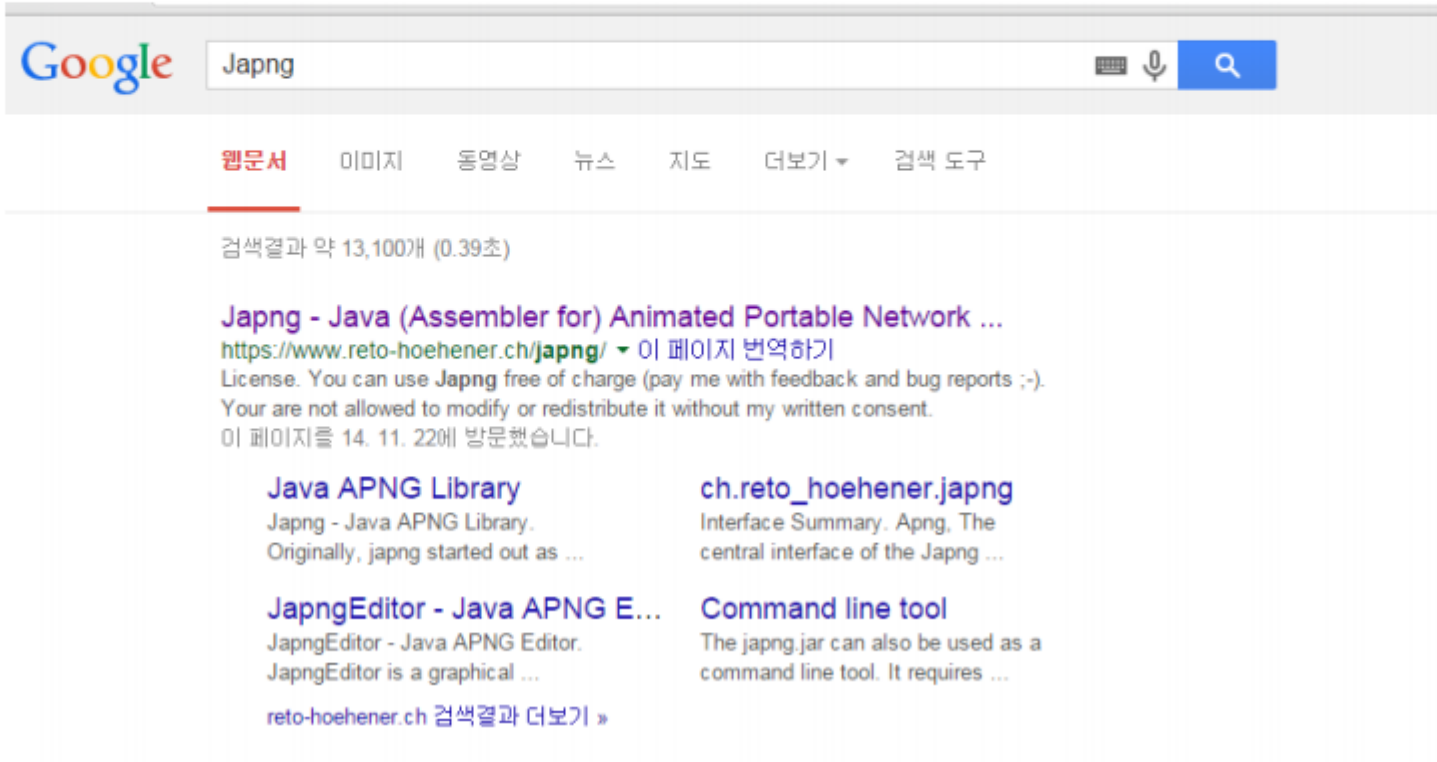
```
00000000  89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52
00000010  00 00 00 69 00 00 00 69  08 06 00 00 00 39 82 0D
```

```
00000880  4C A2 0A 18 1F 6F D1 14  AF 26 F8 1F 6B E1 66 28   L¢   oÑ ¯&ø káf(
00000890  09 71 92 94 00 00 00 13  74 45 58 74 53 6F 66 74    q'"    tEXtSoft
000008A0  77 61 72 65 00 4A 61 70  6E 67 20 72 31 31 39 27   ware Japng r119'
000008B0  E8 B3 61 00 00 00 00 49  45 4E 44 AE 42 60 82      è³a    IEND®B`,
```

이미지 분석

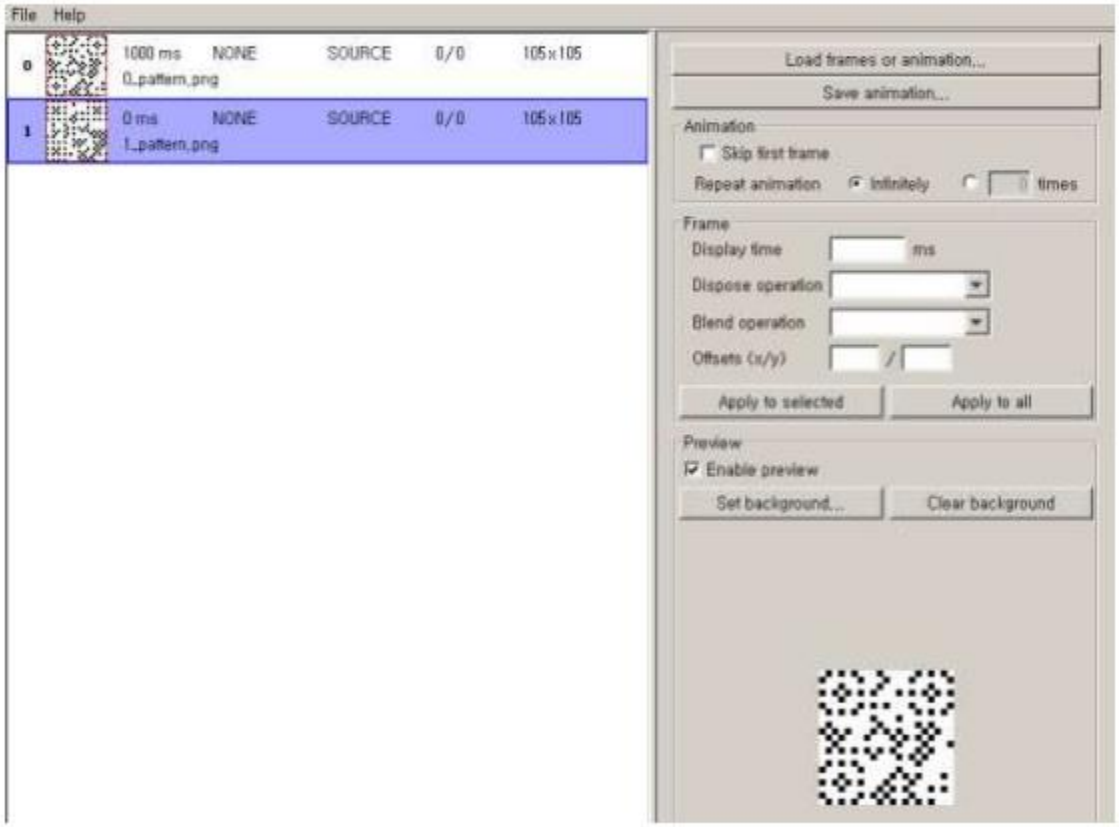
Japng 은 APNG포맷의 이미지를 생성하기 위한 소프트웨어임.

APNG(Animated Portable Network Graphics)는 PNG를 확장한 이미지 파일 포맷으로 GIF와 비슷한 방법으로 애니메이션을 구현하면서 기존 PNG 파일과의 하위 호환성을 유지했기 때문에 GIF보다 더 높은 품질을 보여 준다.



이미지 복구

다음과같이 두개의 파일로 이루어져 있는 것을 확인할 수 있음.



이미지 복구 최종

그림의 모습으로 미루어보아 QR코드임을 확인할 수 있음.

기존의 바코드는 기본적으로 가로 배열에 최대 20여 자의 숫자 정보만 넣을 수 있는 1차원적 구성이지만, QR코드는 가로, 세로를 활용하여 숫자는 최대 7,089자, 문자는 최대 4,296자, 한자도 최대 1,817자 정도를 기록할 수 있는 2차원적 구성이다. 때문에 바코드는 기껏해야 특정 상품명이나 제조사 등의 정보만 기록할 수 있었지만, QR코드에는 긴 문장의 인터넷 주소(URL)나 사진 및 동영상 정보, 지도 정보, 명함 정보 등을 모두 담을 수 있다. 최근에는 QR코드가 기업의 중요한 홍보/마케팅 수단으로 통용되면서 온/오프라인을 걸쳐 폭넓게 활용되고 있다.

Q & A