

303 – Recovery and Restoration

Team Information

Team Name: ISEGYE_IDOL

Team Member: Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address: dfc-isegyeidol@googlegroups.com

Instructions

Description Some of the data that the suspects were transmitting was collected.

Target	Hash (MD5)
Data.bin	13af52d1f91bb13491f890dd35514e78

Questions

1. Recover the given data in its original file format and present the result. (40 points)
2. Figure out the URL that can be obtained by restoring the result of question #1. (200 points)
3. Present the text (numbers) extracted from the downloaded file in the result of question #2. (60 points)

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:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Name:	QRazyBox	Publisher:	Merricx
Version:			
URL:	https://merricx.github.io/qrazybox/		

Name:	PIXLR	Publisher:	PIXLR
Version:			
URL:	https://pixlr.com/kr/editor/		

Name:	Dynamsoft Barcode Reader	Publisher:	Dynamsoft
Version:			
URL:	https://demo.dynamsoft.com/barcode-reader/		

Step-by-step methodology:

1. Recover the given data in its original file format and present the result.

주어진 data.bin을 HxD로 열어보면 JPG파일의 APP0 JFIF Maker 값 일부를 확인할 수 있다.

data.bin																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	10	4A	46	49	46	00	01	01	01	00	60	00	60	00	00	FF	.JFIF.....`...ÿ
00000010	DB	00	43	00	02	01	01	02	01	01	02	02	02	02	02	02	Û.C.....
00000020	02	02	03	05	03	03	03	03	03	06	04	04	03	05	07	06
00000030	07	07	07	06	07	07	08	09	0B	09	08	08	0A	08	07	07
00000040	0A	0D	0A	0A	0B	0C	0C	0C	0C	07	09	0E	0F	0D	0C	0E
00000050	0B	0C	0C	0C	FF	DB	00	43	01	02	02	02	03	03	03	06ÿÛ.C.....
00000060	03	03	06	0C	08	07	08	0C	0C	0C	0C	0C	0C	0C	0C	0C
00000070	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C
00000080	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C
00000090	0C	0C	0C	0C	0C	0C	0C	0C	0C	FF	C0	00	11	08	02	30ÿA....0

[그림 1] data.bin의 APP0 JFIF Maker 일부

따라서 해당 파일은 JPG 파일이었던 것으로 판단되어 손실된 헤더 값 일부를 아래 그림2와 같이 복

원하고 파일명을 data.jpg로 변경하여 윈도우 기본 이미지 뷰어로 열어보았다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	ÿøÿà..JFIF.....`
00000010	00	60	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02	.`...ÿÛ.C.....
00000020	02	02	02	02	02	02	02	03	05	03	03	03	03	03	06	04
00000030	04	03	05	07	06	07	07	07	06	07	07	08	09	0B	09	08
00000040	08	0A	08	07	07	0A	0D	0A	0A	0B	0C	0C	0C	0C	07	09
00000050	0E	0F	0D	0C	0E	0B	0C	0C	0C	FF	DB	00	43	01	02	02ÿÛ.C...
00000060	02	03	03	03	06	03	03	06	0C	08	07	08	0C	0C	0C	0C
00000070	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C
00000080	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C
00000090	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	FF	C0ÿÀ

[그림 2] JPG 헤더 복원



[그림 3] 복원된 이미지

2. Figure out the URL that can be obtained by restoring the result of question #1.

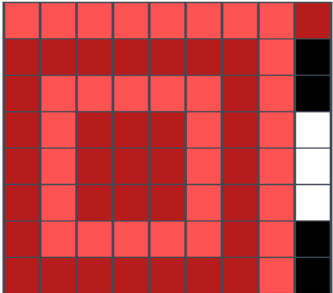
복원된 그림 3의 이미지를 보면 이미지 하단 일부가 회색으로 덮여 QR 코드의 일부가 손상되어 있어서 QR 코드를 정상적으로 인식할 수 없는 상태임을 알 수 있다.

해당 QR코드를 복구하기 위해 QRazyBox를 사용했다.

우리는 왼쪽 아래 Format Info Pattern에서 상단 2칸은 검정색이고 그 아래 3칸은 하얀색임을 알 수 있는데, 이를 만족하는 패턴은 가능한 모든 패턴들 중에서 Error Correction Level이 L이고 Mask Pattern이 5인 패턴밖에 존재하지 않는다. 따라서 해당 Format Info Pattern을 아래와 같이 복구하였다.

Format Info Pattern

Bottom Left ▾



Error Correction Level:

L M Q H

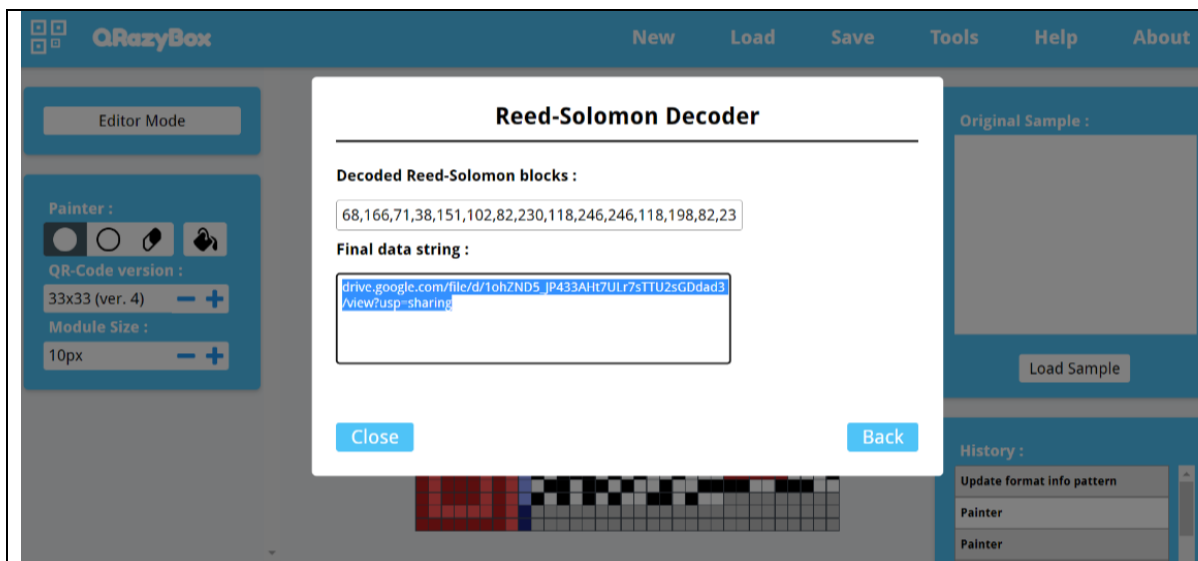
Mask Pattern :

0 1 2 3 4 5 6 7

Save Cancel

[그림 4] 복구한 Bottom Left의 Format Info Pattern

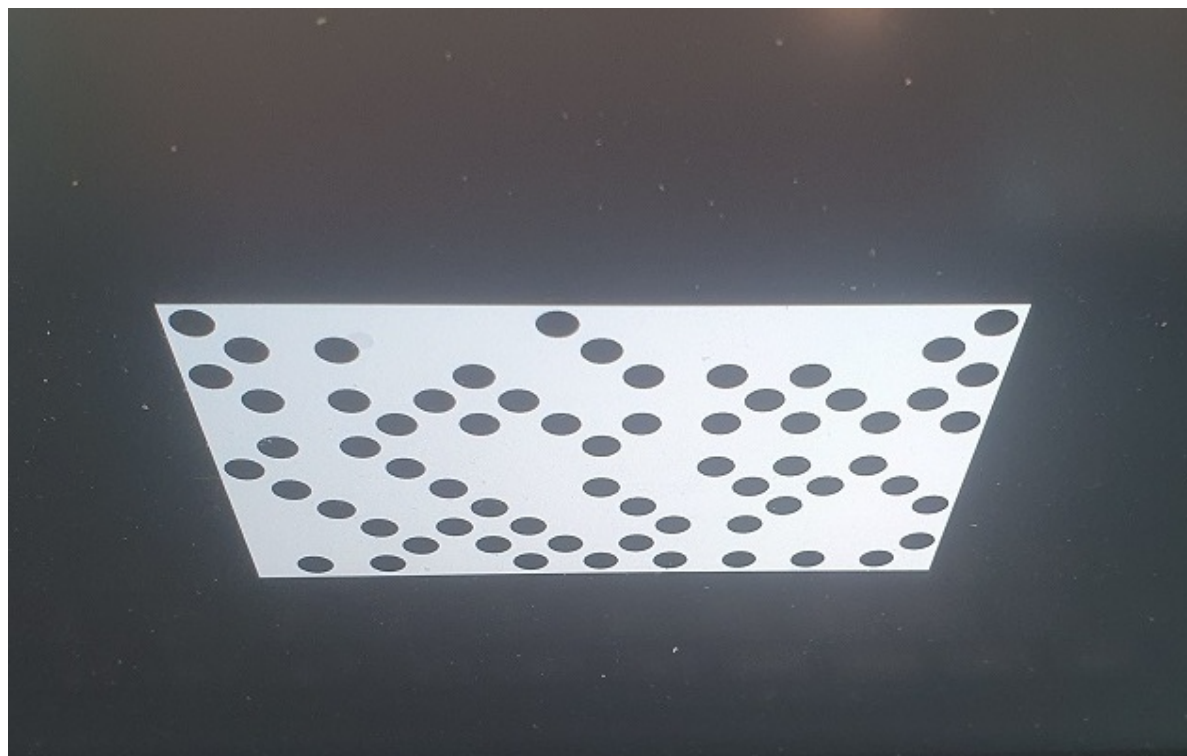
이후 일부 데이터가 손상되었을 때 사용할 수 있는 오류 정정 코드인 Reed-Solomon Decoder를 사용하여 QR Code의 데이터를 디코딩하는 데에 성공하였다.



[그림 5] Reed-Solomon Decoder

drive.google.com/file/d/1ohZND5_JP433AHt7ULr7sTTU2sGDdad3/view?usp=sharing

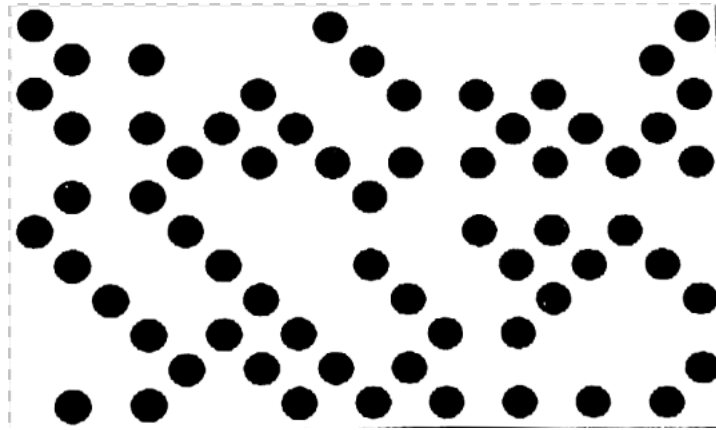
3. Present the text (numbers) extracted from the downloaded file in the result of question #2.



[그림 6] #2에서 획득한 이미지

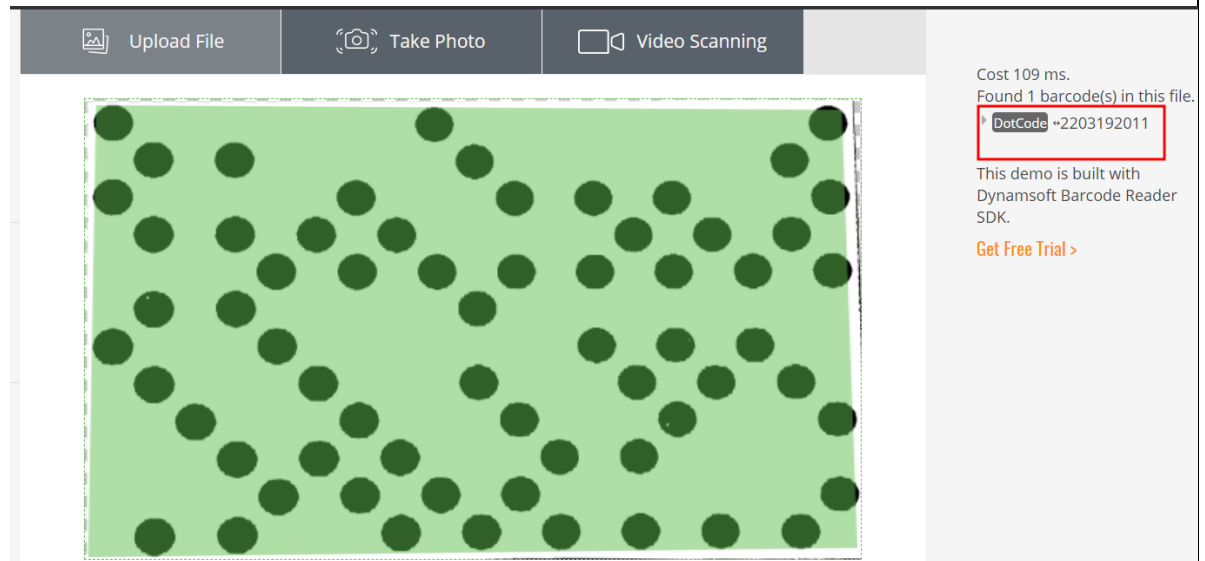
#2에서 획득한 이미지인 그림 5를 보면 dotcode 이미지를 기울여 놓은 것을 알 수 있다.

온라인 이미지 편집도구인 을 사용하여 주어진 이미지에서 dotcode 이미지 부분만 자른 뒤 직사각형 형태로 변형시켰다.



[그림 7] 직사각형 형태로 변형된 dotcode 이미지

이후 직사각형 형태로 변형된 이미지를 Dynamsoft Barcode Reader로 인식하였다.



[그림 8] Dynamsoft Barcode Reader 인식 결과

그 결과, 2203192011 라는 값이 나왔다.