

2025 암호분석경진대회 6번 문제 풀이

2025 암호분석경진대회 6번 문제

한 회사에서 기밀 유출 사건이 발생하여 수사가 시작되었다. 수사를 위해 유력한 용의자 A씨의 PC 데이터 중 사건과 연관된 것으로 추정되는 애플리케이션 데이터가 저장된 ‘%AppData%’ 경로의 파일을 수집하였다. 추가로 데이터 유출 사건이 발생한 기간의 채팅 데이터가 백업된 것으로 보이는 ‘chatBackup.sqlite’ 데이터베이스 파일이 수집되었다. 주어진 데이터를 분석하여 데이터 유출 과정, 유출된 데이터와 접선한 장소를 밝혀내시오. 그리고 분석 과정에서 암호화된 데이터를 활용한 경우 평문 데이터 획득 과정을 상세히 설명하시오.

정보보안암호수학과

20232106 정유진

alice2002@kookmin.ac.kr

20212052 이동훈

dhsama51@kookmin.ac.kr

데이터베이스 내부의 채팅 내역 복호화

chatBackup.sqlite를 DB Browser for SQLite로 분석

테이블(T): ChatRooms

chatid	lastMessageId	lastMessage
필터	필터	필터
123456789012345	2564183412515905536	이제 바꿀때가 된거같네요

테이블(T): ChatLogs

42	2564183412515905536	123456789012345	1	22222	LKuLeuZYyKg3QTYeodAf6ogE7diuGdalw9/...	0	1742637350
----	---------------------	-----------------	---	-------	--	---	------------

암호문 LKuLeuZYyKg3QTYeodAf6ogE7diuGdalw9/zHHYCdzkwjTl=과 평문 "이제 바꿀때가 된거같네요"가 일치함을 볼 수 있다. 암호문은 평문과 키 스트림을 xor 하여 생성되므로, 평문과 암호문을 xor 하면 키 스트림을 얻을 수 있다.

언언엔 키 스트림

c0363f9646c4e84387d5d621213b8a6662b46df845894a4f726f19acefe9f39ddc17a6ee1a6f99e26a61b9acc9ca3baaf2683c814d0d5e4ea96be705aac87901b2a2cf0fa56a222c01cbd7d7a9cff50aa6db1e

복호화된 채팅 기록

1 준비는 잘 되고 있습니까?	15 편의상 구글 드라이브	30 내일 여기서 만나뵙도록 하시죠
2 업체쪽 받아볼 수 있을까요?	16 https://drive.google.com/file/d/	31 너무 인적이 드문 장소 아닐까요?
3 거의다 준비 되었습니다.	17 부분은 생략하고 보냅니다	32 오이러 고려를 잡힐 수도 있을꺼같은데
4 이번주 내로 전달드리겠습니다.	18 17Mq9cPxqchpdacSZvoqOvbjecEaz0E0k	33 그래도 가끔적 사람 없는곳이 좋을 것 같습니다
5 좋습니다.	19 19vcVDYHSmFc6GhJ1j2Zjut_4_EMRh2h_	34 저를 믿으시죠
6 기간 임시 부탁드립니다.	20 혹시몰라 두가지 링크를 드립니다	35 네 그러면 거기서 뵙도록 하죠
7 보수는 약속대로 지급하겠습니다.	21 네 확인했습니다.	36 좋은 거래였습니다.
8 아 그리고 저희가 직접 만나야 할때는	22 자료 확인해보겠습니다.	37 유출 사실이 발각되지 않도록 관리 부탁드립니다.
9 혹시 모르니 저한테 알려드리 방법으로 부탁드립	23 자료 확인해봤는데 압축파일에 암호가 걸려있네	38 네 잘 관리하겠습니다.
니다.	24 ?	39 아 근데 혹시 암호를 다시 알려주실 수 없나요?
10 자료 준비 완료되었습니다.	24 자료 보명은 있어야죠	40 혹시몰라 그날 함께 전달드릴 쪽지에 적어드었습
11 어떻게 전달드릴런 말까요?	25 보수를 확인한 뒤에 알려드리겠습니다.	니다.
12 클라우드 같은데 올리신 뒤 링크를 전달해 주시	26 철저하시군요	41 제가 자주쓰던 비밀번호였는데
면 좋겠습니다.	27 보수는 어떻게 지급받기를 원하십니까?	42 이제 바꿀때가 된거같네요
13 알겠습니다. 내일쯤 전달드리겠습니다.	28 1v17_C3BjDsXfPzKps7e9_StLyuF1pFb5	
14 링크 첨부합니다.	29 1uXmRLy_OA6myj2p5fMIKe52G_J7XSL-X	

유출된 데이터 및 접선 장소 획득

아까 채팅 내역 복호화를 통해 총 4개의 구글 드라이브 링크를 얻는다.
<https://drive.google.com/file/d/17Mq9cPxqchpdacSZvoqOvbjecEaz0E0k> - 기밀문서.zip
https://drive.google.com/file/d/19vcVDYHSmFc6GhJ1j2Zjut_4_EMRh2h_ - 기밀문서.zip
https://drive.google.com/file/d/1v17_C3BjDsXfPzKps7e9_StLyuF1pFb5 - staryard_library2.png
https://drive.google.com/file/d/1uXmRLy_OA6myj2p5fMIKe52G_J7XSL-X -staryard_library2.png

기밀문서 zip

압축을 풀기 위해선 암호가 필요하다.
복호화된 채팅을 보면 41번째 대화에 ‘제가 자주쓰던 비밀번호였는데’ 라는 대화가 있다.
AppData.zip을 풀면 나오는 Opera Software 폴더 안 파일들을 분석해서 알아낼 수 있다.

UsersWwlrndjs1WAppDataWRoamingWOpera SoftwareWOpera StableWLocal State
os_crypt":{"audit_enabled":true,"encrypted_key":"Already decrypted 복호화된 값입니다
0xbF A2 38 84 56 55 F6 35 47 29 BA 8B EE A2 2C 49 31 C4 12 F8 0F 14 82 E2 28 F8 54 A5 C8 9A 97 A0 복호화된 값입니다 Already decrypted")

UsersWwlrndjs1WAppDataWRoamingWOpera SoftwareWOpera StableWDefaultWLogin Data

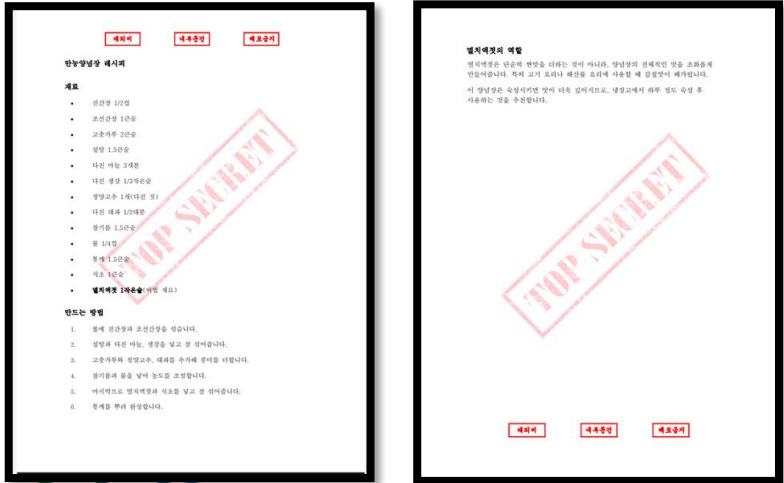
origin_url	action_url	username_element	username_value	password_element	password_value
필터	필터	필터	필터	필터	필터
1 https://signin.aws.amazon.com/			zonxjohn		BLOB
2 https://login.goupang.com/			wlrndjs1@never.com		BLOB
3 https://mail.never.com/			wlrndjs1		BLOB
4 https://test.co.kr/			test		BLOB
5 https://erthergfwer.co2/			fgytnnft		BLOB
6 https://daum.net/			daumiskakao		BLOB

비밀번호 BLOB 복호화

	origin_url	username_value	decrypted_password
0	https://mail.never.com/	wlrndjs1	CrYpT@2025!An@lysis#C0nt3st
1	https://login.goupang.com/	wlrndjs1@never.com	CrYpT@2025!An@lysis#C0nt3st
2	https://test.co.kr/	test	testtest
3	https://signin.aws.amazon.com/	zonxjohn	CrYpT@2025!An@lysis#C0nt3st
4	https://daum.net/	daumiskakao	CrYpT@2025!An@lysis#C0nt3st
5	https://erthergfwer.co2/	fgytnnft	retshdft

PS C:\Users\user\Downloads\code>

CrYpT@2025!An@lysis#BC0nt3st로 기밀 문서 복호화



만능양념장 레시피가 들어있음을 확인 할 수 있다.

유출된 데이터 및 접선 장소 획득

UsersWwlrndjs1WAppDataWRoamingWOpera SoftwareWOpera StableWDefaultWHistory

테이블(T): urls

title
필터
1 암호분석 경진대회 - Google 검색
2 암호분석 경진대회 - Google 검색
3 2025년 제 11회 암호분석경진 대회
4 2025년 제 11회 암호분석경진 대회
5 2024 암호분석경진대회 후기 Jinpyo Kim
6 sol3.pdf
7 스테가노그래피 - Google 검색
8 TTA정보통신용어사전
9 TTA정보통신용어사전
10 TTA정보통신용어사전
11 TTA정보통신용어사전
12 LSB 은닉 - Google 검색
13 [Forensic] 2bpp LSB Steganography : ...
14 [Forensic] 2bpp LSB Steganography : ...
15 LSB 은닉 - Google 검색
16 4교시2 LSB를 이용한 정보은닉, 스테가노그래...

테이블(T): urls

17 4교시2 LSB를 이용한 정보은닉, 스테가노그래...
18 이미지에 데이터 은닉하는 방법 - Google 검색
19 이미지에 텍스트 또는 파일 은닉 및 ...
20 이미지에 텍스트 또는 파일 은닉 및 ...
21 텍스트 qr코드 변환 - Google 검색
22 텍스트 QR Code 만들기 - mQR
23 텍스트 QR Code 만들기 - mQR
24 텍스트 QR Code 만들기 - mQR
25 텍스트 QR Code 만들기 - mQR
26 위치 공유하는법 - Google 검색
27 Google 지도에서 내 실시간 위치를 다른 ...
28 Google 지도에서 내 실시간 위치를 다른 ...
29 별마당 도서관 - Google 검색
30 별마당 도서관 - Google 검색
31 Staryard library - Imgur
32 NAVER

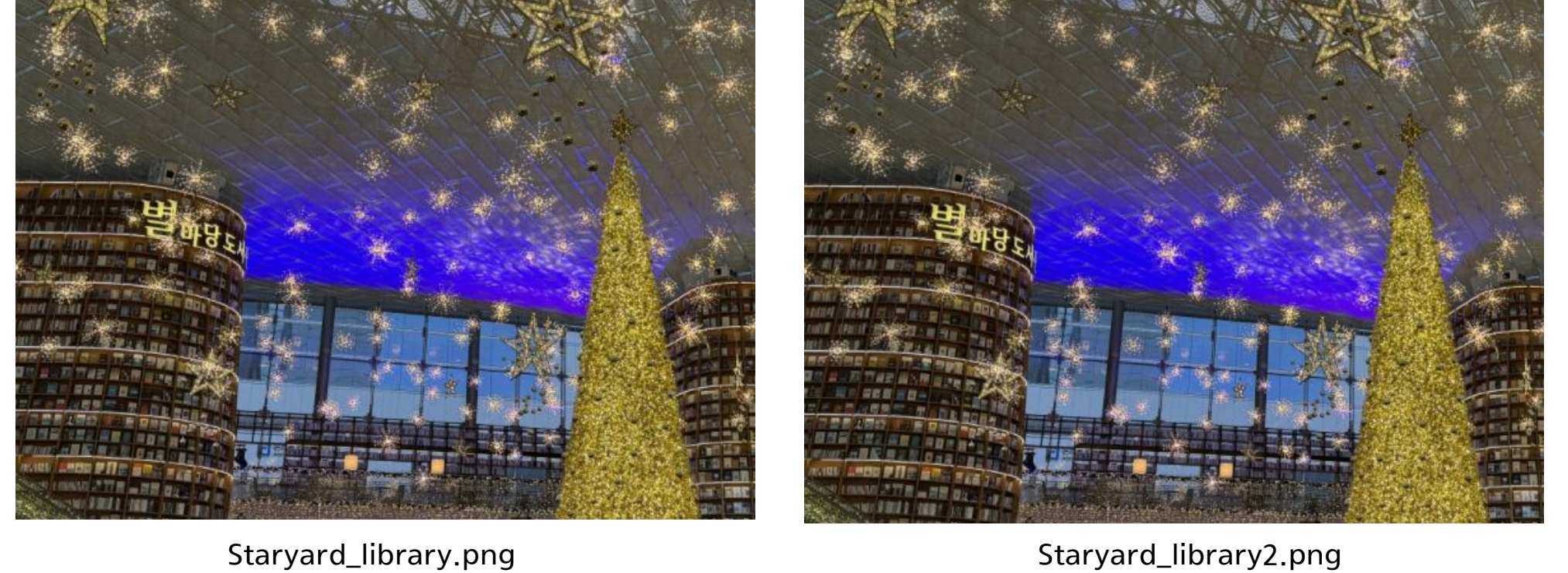
어떤 위치 주소를 QR 코드로 변환하고, 그 이미지를 2bpp LSB Steganography로 은닉했음을 추정해 볼 수 있다.

테이블(T): downloads

ta	tab_url
필터	
1	https://imgur.com/gallery/staryard-...

복호화된 채팅 내역의 구글 드라이브: staryard_library2.png
downloads: staryard_library.png
staryard_library.png에 무언가를 2bpp LSB Steganography로 은닉해서 staryard_library2.png를 만들었음을 추정할 수 있다.
두 이미지는 육안으로 구별하기가 거의 불가능하다.

<https://imgur.com/gallery/staryard-library-Bay2Hhr>



2bpp Steganography

2bpp Steganography를 사용.

- 두 이미지의 차이 계산 (2bpp LSB 추출을 위한 XOR 방식)
- diff = (arr1 ^ arr2) & 0b11 (하위 2비트만 추출)

차이 데이터를 흑백 이미지로 시각화 (값이 있을수록 밝게)

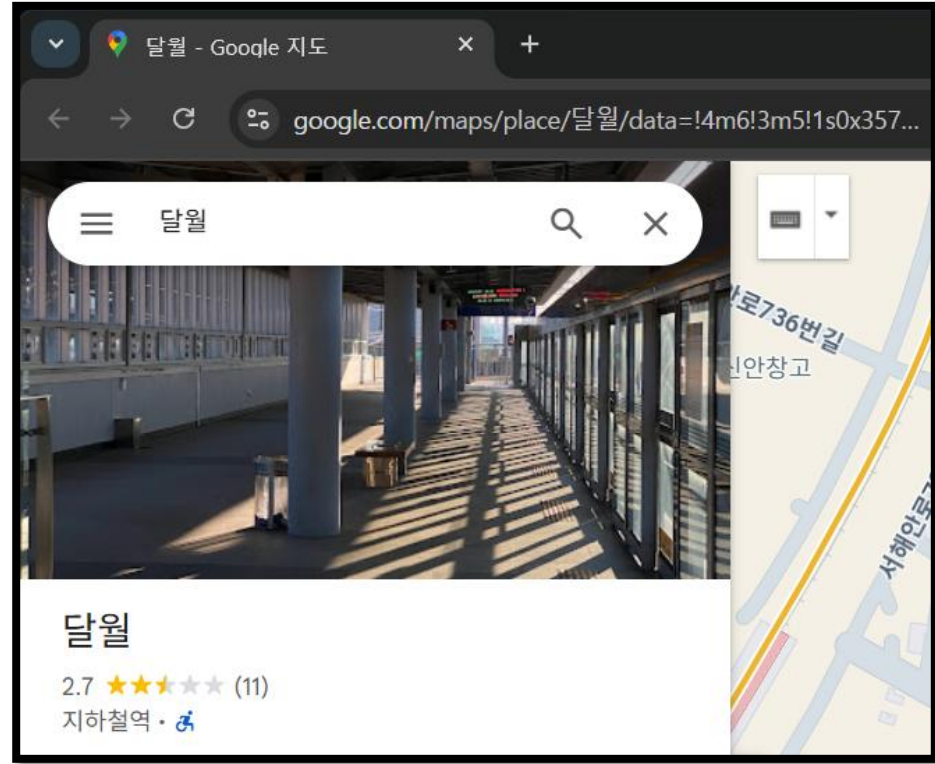
- diff_gray = np.sum(diff, axis=2) * 85 (각 픽셀 RGB 합산 후 확장 (0~3)*85 => 0~255)

stegano_result.png 파일을 추출



QR 코드를 핸드폰 카메라로 스캔하면 구글 지도 링크가 나온다.
https://www.google.com/maps/place/%EB%8B%AC%EC%9B%94/data=!4m6!3m5!1s0x357b7079205e20ad:0xe2ae06812f1a76c2!8m2!3d37.380008!4d126.745449!16s%2Fg%2F121p7q0x?entry=ttu&g_ep=EgoyMDI1MDcyMi4wIjKXMDSoASAFQAw%3D%3D

접선 장소



접선 장소가 달월역임을 확인할 수 있다.