103 - Find the cryptocurrency wallet address

Team Information

Team Name : HSPACE

Team Member : Jinung Lee, Beomjun Park, DoHyeon Kim, Soyoung Cho

Email Address : hspacedigitalforensicslab@gmail.com

Teams must:

- Provide a detailed, step-by-step description of their problem-solving approach to ensure reproducibility by another examiner.
- List all tools used to arrive at their conclusions.

Tools used:

Name:	FTK Imager	Publisher:	AccessData® FTK® Imager
Version:	4.7.3.81		
URL:	https://www.exterro.com/		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com/		

Name:	Magnet Axiom	Publisher:	Magnet Forensics
Version:	9.5.0		
URL:	https://www.magnetforensics.com/		

Name:	VMware Workstation	Publisher:	VMware, Inc,
Version:	17.6.2		
URL:	https://www.vmware.com/		

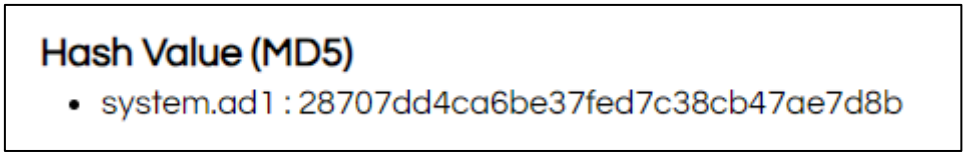
Step-by-step methodology:

Description 경찰은 용의자가 개인 컴퓨터에 지갑 프로그램을 설치하고 암호화폐를 사용했다는 정보를 입수했다. 압수 수색 과정에서 암호화폐 지갑 프로그램은 삭제되어, 지갑 정보를 찾을 수 없었다. 지갑 복구를 위한 정보를 찾으면 지갑을 복구할 수 있다. 숨겨진 정보를 찾아서 지갑을 복구하고, 지갑 주소를 확보하라.

Questions

1. 컴퓨터에서 사용한 암호화폐 지갑 프로그램의 이름은 무엇인가? (10점)
2. 웹 브라우저에서 찾을 수 있는 지갑의 흔적은 무엇인가? (20점)
3. 암호화폐 지갑 복구를 위한 정보가 숨겨진 파일은 무엇인가? (50점)
   - 파일 경로: (20점)
   - 정보: (30점)
4. 암호화폐 비트코인 지갑 주소는 무엇인가? (20점)

문제 풀이에 앞서, dfchallenge.org에 공지된 문제 해시와 다운로드 받은 문제 해시를 비교함으로써 분석 대상이 동일한 파일임을 증명한다.

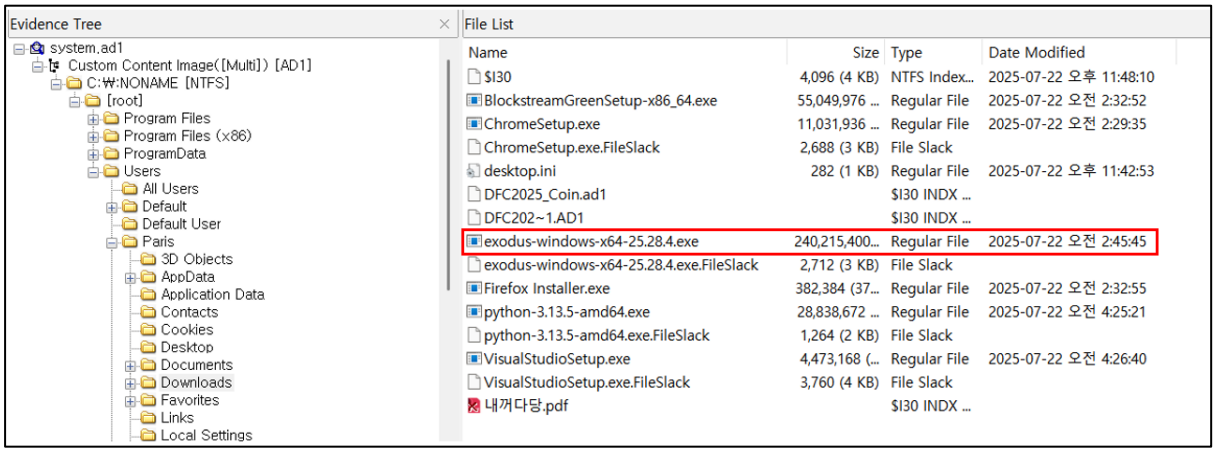


[그림 1] dfchallenge.org에 공지된 문제 해시(MD5) 값.

[그림 2] HashTab을 통해 확인한 문제 해시(MD5) 값.

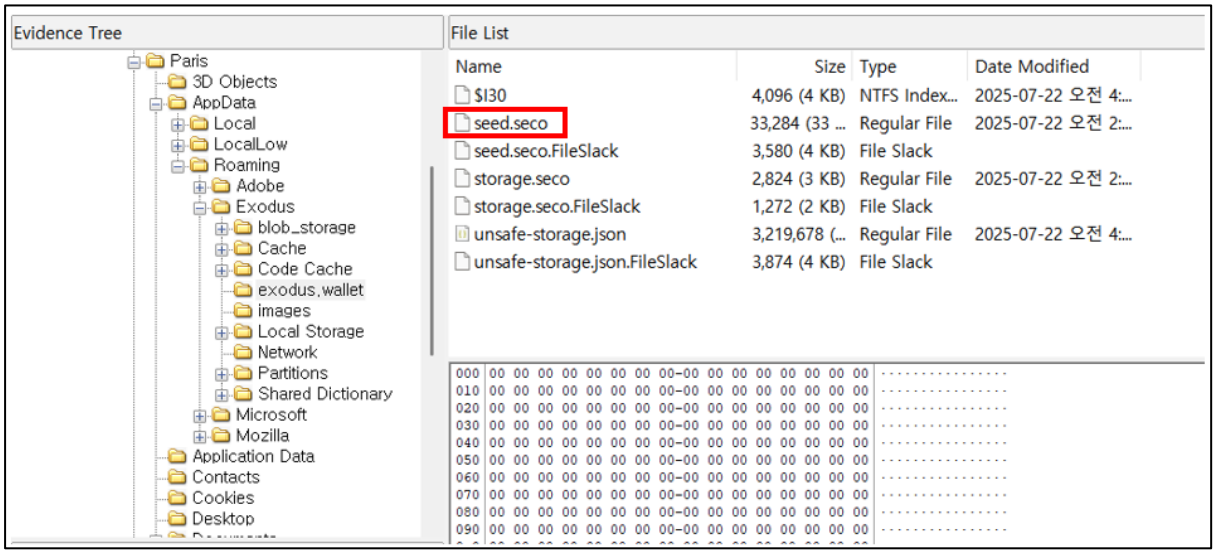
1. 컴퓨터에서 사용한 암호화폐 지갑 프로그램의 이름은 무엇인가?

용의자의 PC Paris 사용자 폴더 하위의 Downloads폴더에서 암호화폐 지갑 프로그램인, exodus의 설치파일(exodus-windows-x64-25.28.4.exe)과 Blockstream Green의 설치파일 (BlockstreamGreenSetup-x86_64.exe)을 확인할 수 있었다.



[그림 3] Downloads 폴더에서 발견된, exodus의 설치 프로그램.

이를 통하여 Users₩Paris₩AppData₩Roaming₩Exodus₩exodus.wallet에 seed.seco로 저장되어 있는 암호화폐 지갑 파일을 발견할 수 있다. 하지만 Blockstream Green에 대한 지갑 및 정보를 확인할 수 없었다.



[그림 4] Paris 사용자의 AppData₩Roaming₩Exodus₩exodus.wallet에서 발견된 암호화폐 지갑.

답: Exodus

2. 웹 브라우저에서 찾을 수 있는 지갑의 흔적은 무엇인가?

2.1 용의자의 구글 검색 정리

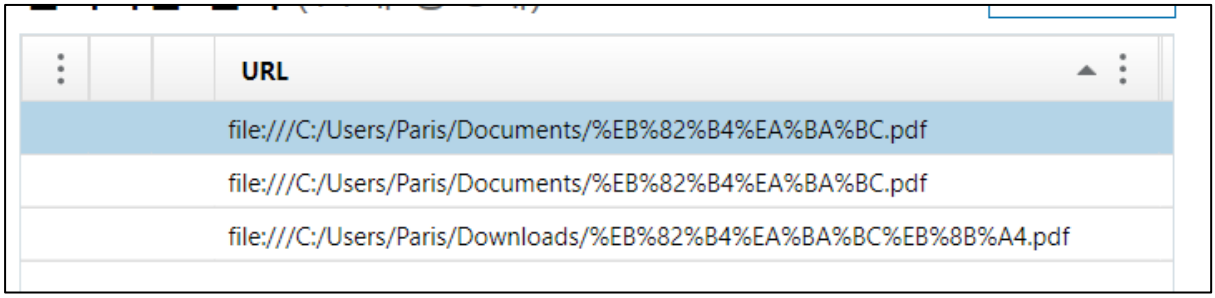
용의자는 Chrome과 Firefox를 이용하여, 비트코인과 니모닉 코드에 대한 내용을 google을 통해 검색했다. 이는 [표 1]과 같이 정리할 수 있으며, 이를 통해 니모닉 코드에 대한 내용을 은닉하고 있음을 시사한다.

검색어	날짜/시간 (UTC+9)	검색 엔진
exodus	2025-07-22 AM 11:31:53.448	Chrome
bitcoin	2025-07-22 AM 11:31:58.531	Chrome
bitcoin wallet	2025-07-22 AM 11:31:59.000	Chrome
니모닉 코드 숨기기	2025-07-22 AM 11:34:27.981	FireFox
니모닉 코드	2025-07-22 AM 11:38:48.435	FireFox
mnemonic code란	2025-07-22 AM 11:39:08.272	FireFox
bip-39	2025-07-22 AM 11:39:39.219	FireFox
Exodus	2025-07-22 AM 11:41:48.272	FireFox
bitcoin window wallet	2025-07-22 AM 11:44:48.641	FireFox
비트코인 은닉	2025-07-22 PM 1:04:22.642	FireFox
비트코인 bip39	2025-07-22 PM 1:04:28.951	FireFox
bip39 word list	2025-07-22 PM 1:04:37.528	FireFox
translate google	2025-07-22 PM 1:18:23.872	FireFox

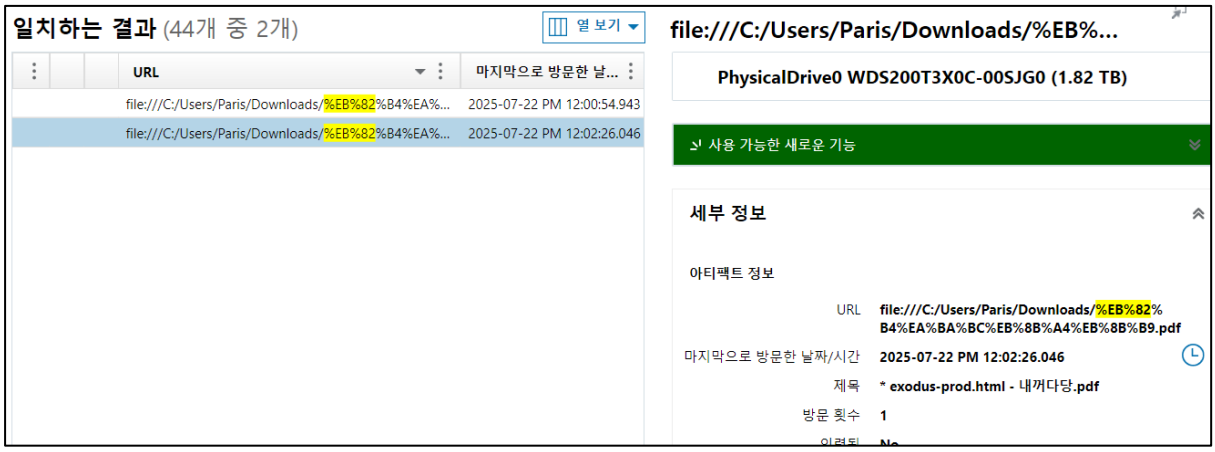
[표 1] FireFox와 Chrome을 이용하여 검색한 주요 내용 정리.

2.2 exodus-prod.html

용의자는 **exodus-prod.html의 제목의 PDF를 "내꺼.pdf", "내꺼다.pdf", "내꺼다당.pdf"의 이름으로 Chrome과 Firefox를 통해 열람했다는 것을 크롬의 최종 탭 세션을 통해 알 수 있었다.**

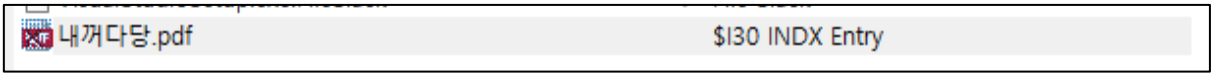


[그림 5] Chrome의 최종 탭 아티팩트에서 확인한, exodus-prod.html의 제목의 PDF 3개.



[그림 6] Firefox의 웹 기록에서 확인된, 내꺼다.pdf와 내꺼다당.pdf.

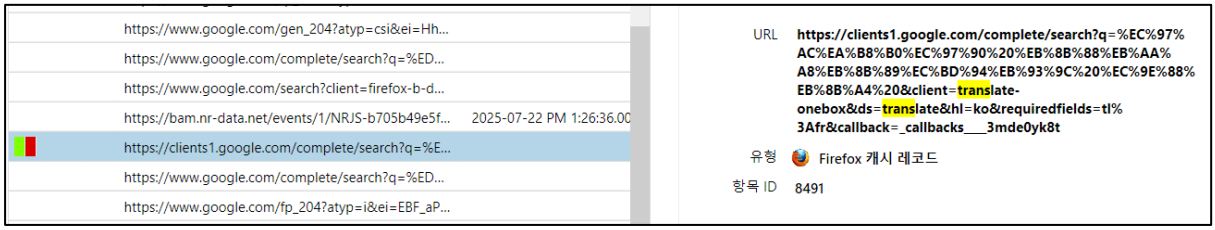
이러한 근거를 통하여, 용의자는 내꺼다.pdf와 내꺼다당.pdf 그리고 내꺼.pdf를 통하여 니모닉 코드를 PC에 저장했음을 시사한다. 추가적으로 다운로드에 저장된 내꺼다당.pdf의 흔적이 저장되어 있다. 이를 복구하기 위해 시도했지만, 복구할 수 없었다.



[그림 7] 다운로드 폴더에서 발견된 내꺼다당.pdf의 흔적.

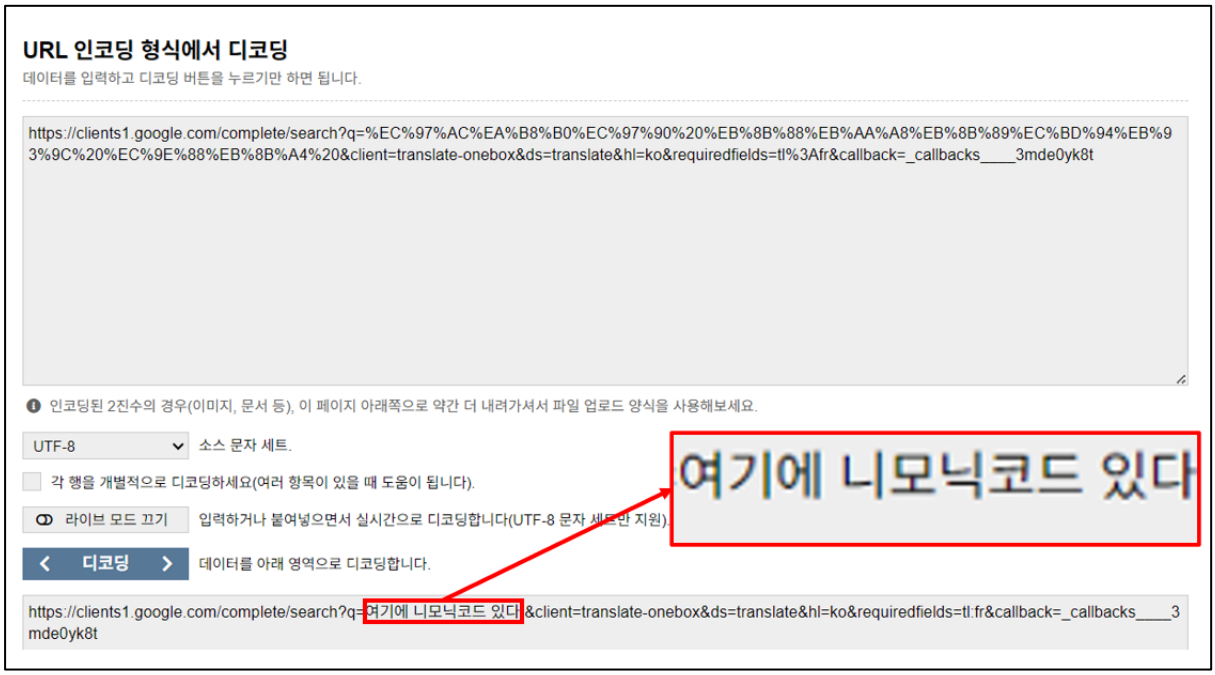
2.3 구글 번역

앞서 [표 1]의 내용을 토대로 용의자는 2025년07월22일 13시 18분에 translate google을 검색한 것을 알 수 있다. Firefox의 캐시 레코드를 확인한다면, [그림 8]과 같이, 구글 번역을 이용한 URL을 얻을 수 있다.



[그림 8] Firefox 캐시 레코드에서 확인한 구글 번역 이용 URL.

해당 내용을 디코딩 하면 [그림 9]와 같이, "여기에 니모닉 코드 있다"는 문자열을 발견할 수 있다.



[그림 9] URL 디코딩 결과.

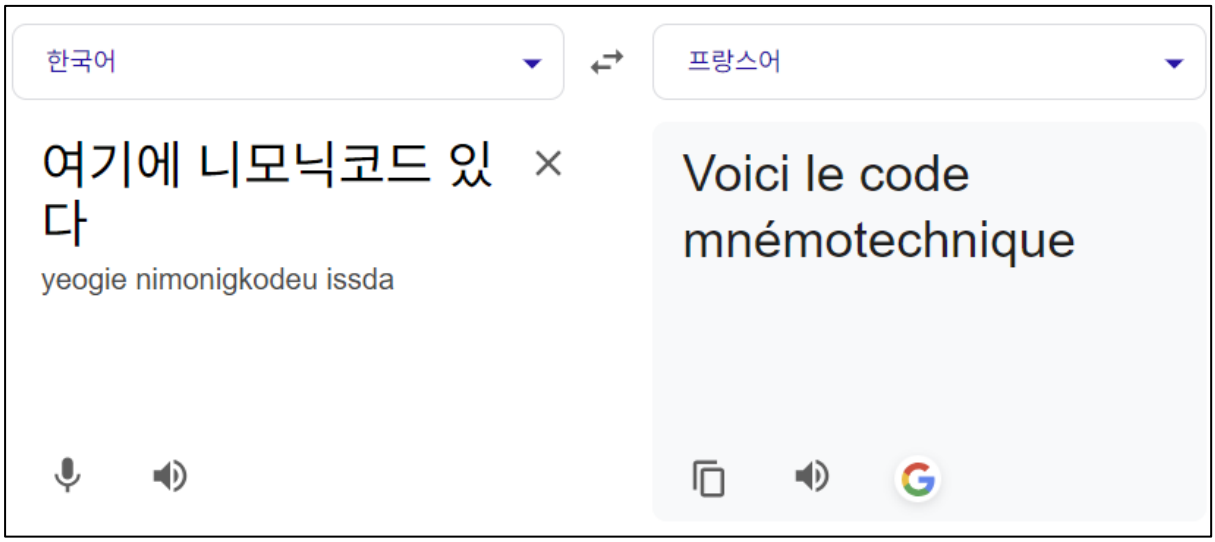
URL을 자세히 분석하면, URL에서 q= 파라미터 부분을 디코딩하면 "여기에 니모닉코드 있다"라는 한국어 텍스트이다. **tl%3Afr** 부분을 보면 **tl:fr**로 디코딩되는데, 이는 **"target language: French"**를 의미한다. 즉, 한국어 "여기에 니모닉코드 있다"를 **프랑스어**로 번역하려고 하는 Google Translate API 요청이다.

2.4 결론

위의 증거는 모두 용의자의 암호화폐 사용 및 지갑에 대한 흔적이라고 볼 수 있다. 사용자의 브라우저 히스토리 및 검색 내역을 확인하여, 용의자가 니모닉 코드를 은닉하였다는 것을 암시하며, 다운로드 폴더에서 발견된 "내꺼다당.pdf"의 흔적을 통해 니모닉 코드가 PC에 존재했다는 사실을 시사한다. 이를 통하여 다음 3. 암호화폐 지갑 복구를 위한 정보가 숨겨진 파일은 무엇인가?를 해결하기 위한 구글 번역 API 요청이기에, 이는 모두 **웹 브라우저에서 찾을 수 있는 지갑의 흔적**이라고 생각된다.

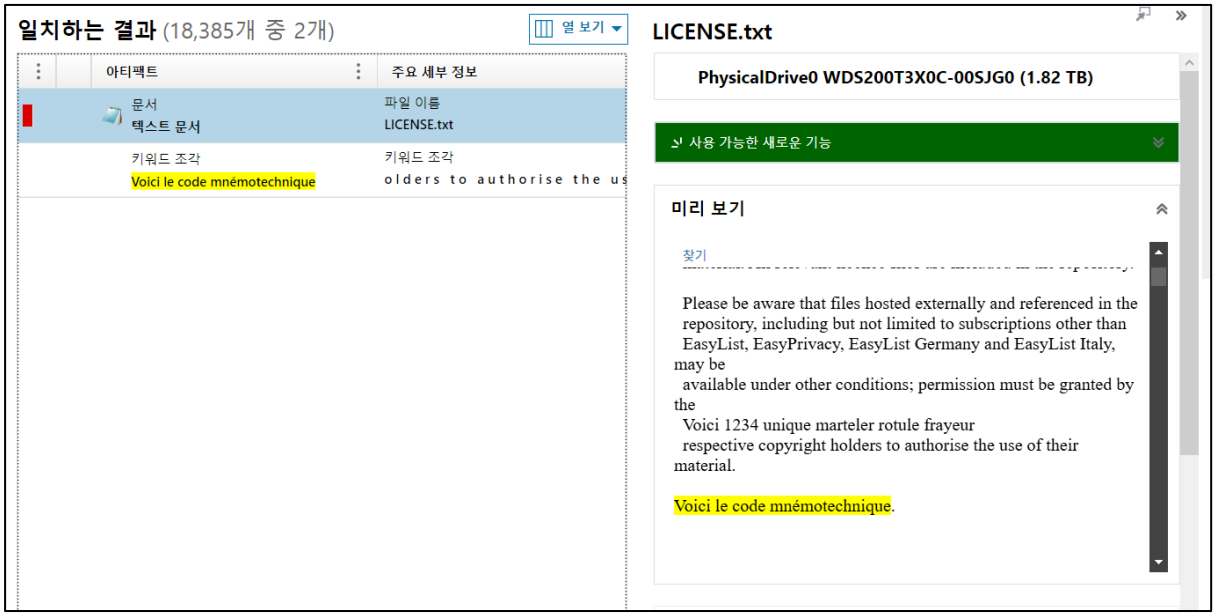
3. 암호화폐 지갑 복구를 위한 정보가 숨겨진 파일은 무엇인가?

앞서 발견된 프랑스어로 번역된 "여기에 니모닉코드 있다"의 문자열을 용의자와 동일하게 번역하여 용의자가 획득한 문자열을 확인했다.



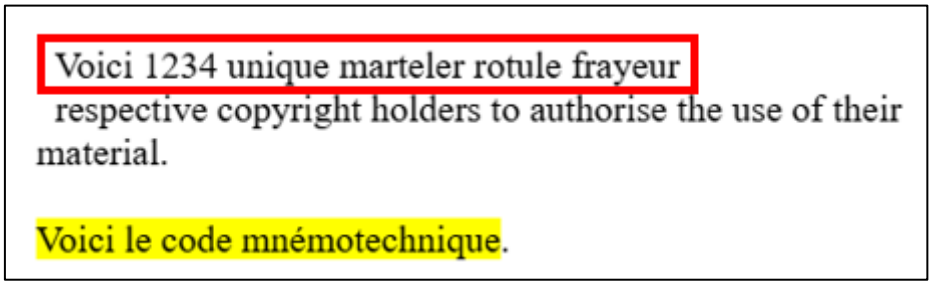
[그림 10] 구글 번역을 통하여 확인한 "여기에 니모닉코드 있다"의 번역.

이를 이용하여 색인하면, [그림 11]과 같이 ₩Users₩Paris₩AppData₩Local₩₩Google₩Chrome ₩User Data₩Subresource Filter₩Unindexed Rules₩9.56.0₩LICENSE.txt안에 있는 Voici le code mnémotechnique를 확인할 수 있다.



[그림 11] Voici le code mnémotechnique로 색인한 결과.

또한, [그림 12]와 같이 Voici le code mnémotechnique 바로 위에 Voici라는 문자열을 확인할 수 있다. 이를 번역하면 "여기는"라는 뜻으로 4개의 니모닉 코드가 해당 문자열에 있다는 것을 알 수 있다.



[그림 12] Voici le code mnémotechnique위에서 발견된 니모닉 코드의 일부.

이와 같이 프랑스어로 번역된 12개의 모든 단어를 찾을 수 있었으며, 결과는 [표 2]와 같다.

라인	내용
16	Voici 1234 unique marteler rotule frayeur
87	Voici 9101112 lampe récolter citerne cerner
135	Voici 5678 dégager ozone limer Lunaire

[표 2] 프랑스어로 번역된 니모닉 코드가 포함된 라인 정리.

[표 2]의 내용을 프랑스어에서 영어로 번역하며 니모닉 코드의 2048개의 단어를 고려하면 [표 3]과 같이 정리할 수 있다.

1	2	3	4	5	6
unique	hammer	ball	scare	clean	Ozone
7	**8**	**9**	**10**	**11**	**12**
file	lunar	lamp	harvest	tank	invest

[표 3] 용의자의 니모닉 코드 정리.

답안	
파일 경로	[root]₩Users₩Paris₩AppData₩Local₩Google₩Chrome₩User Data₩Subresource Filter₩Unindexed Rules₩9.56.0₩LICENSE.txt
정보	Voici le code mnémotechnique Voici 1234 unique marteler rotule frayeur Voici 9101112 lampe récolter citerne cerner Voici 5678 dégager ozone limer lunaire

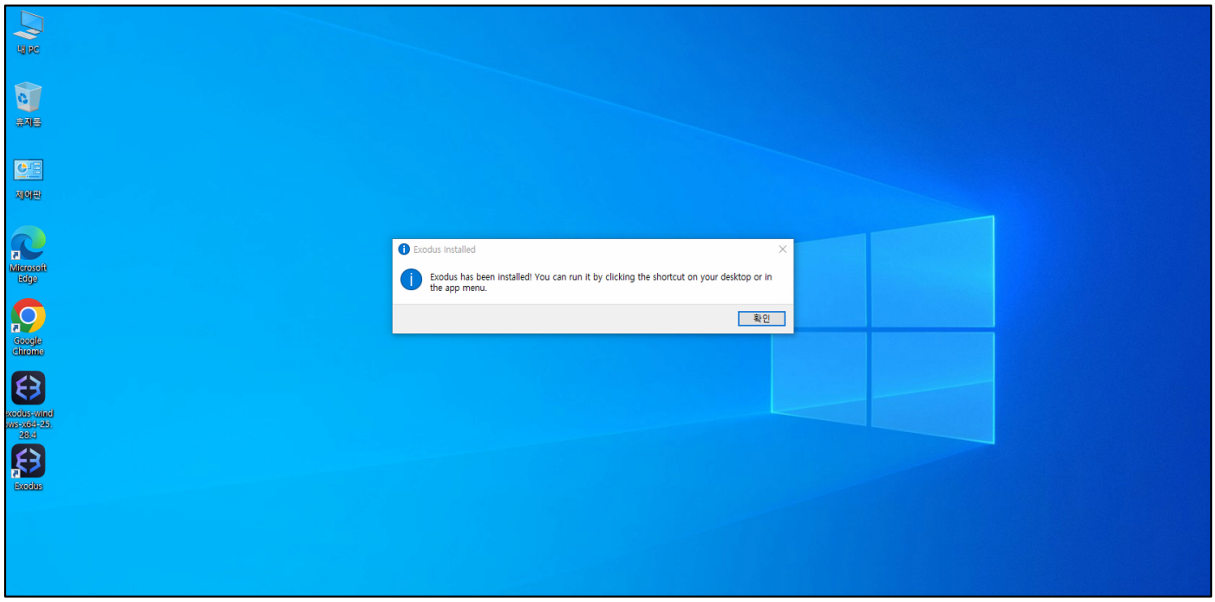
[표 4] 질문 3의 답안.

4. 암호화폐 비트코인 지갑 주소는 무엇인가?

이를 해결하기 위하여 VMware를 이용하여 가상머신을 생성하고, 해당 지갑프로그램과 용의자의 exodus 폴더를 덮어쓰기하여 최대한 동일한 환경에서 검증하였다. 해당 환경에서 사용한 OS 정보는 [표 5]와 같다.

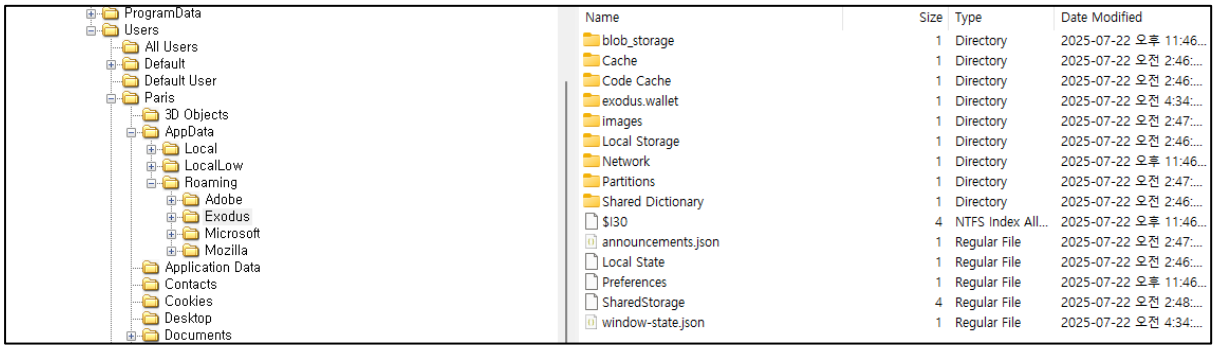
OS	Windows 10
버전	2004
릴리즈	19041.1

[표 5] 가상환경 생성에 사용된 OS 정보 정리.



[그림 13] 가상 머신에서 Exodus설치를 완료한 모습.

동일한 환경구성을 위하여 [그림 14]와 같이, FTK Imager를 이용하여 용의자의 Exodus를 추출하였으며, 이를 압축파일로 변환하였다. 또한 해당 압축파일의 정보는 [표 6]과 같다.

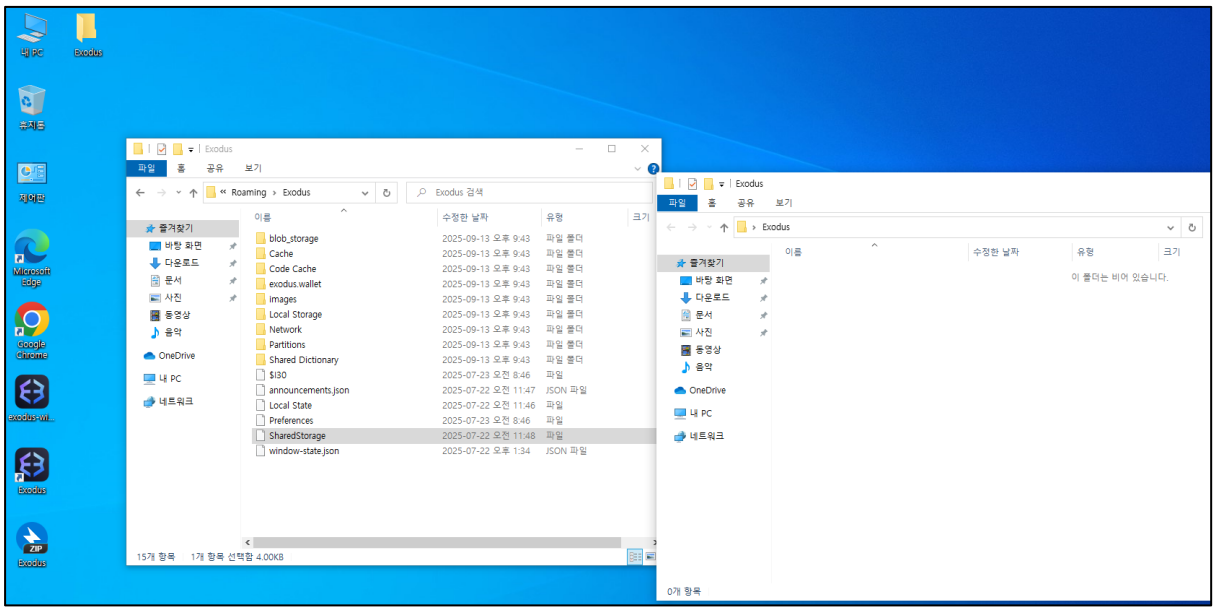


[그림 14] FTK imager를 이용한 용의자 PC의 Exodus.

파일이름	Exodus.zip	CRC32	E39B1B8B
크기	10.7MB (11,234,585 바이트)		
SHA1	4D7D3F8193427419EDD107A9A9A91EA3EFCCB0F1		

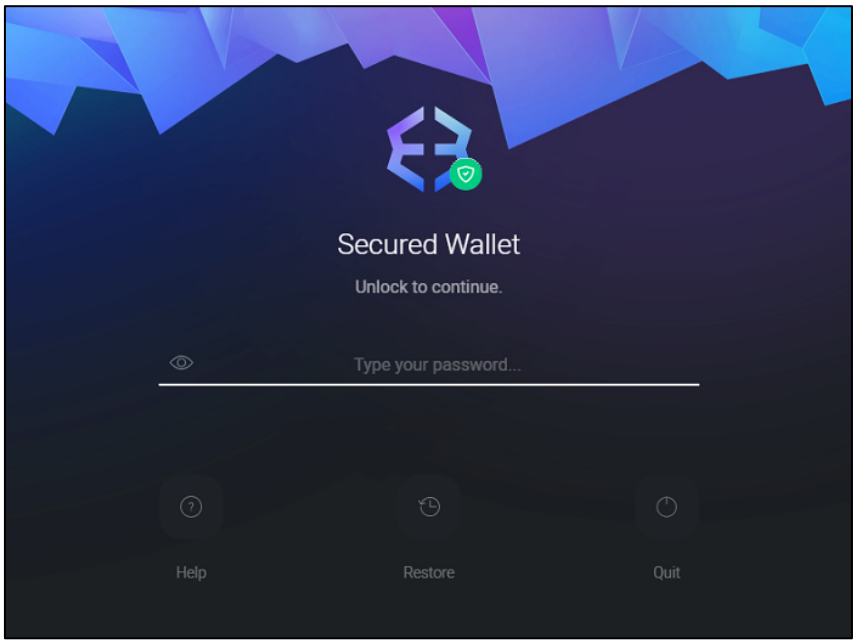
[표 6] 압축파일의 체크섬 및 정보 정리.

[그림 15]와 같이, 해당 압축파일을 가상환경에 옮긴 후, 이를 설치한 Exodus 폴더로 옮겼다.



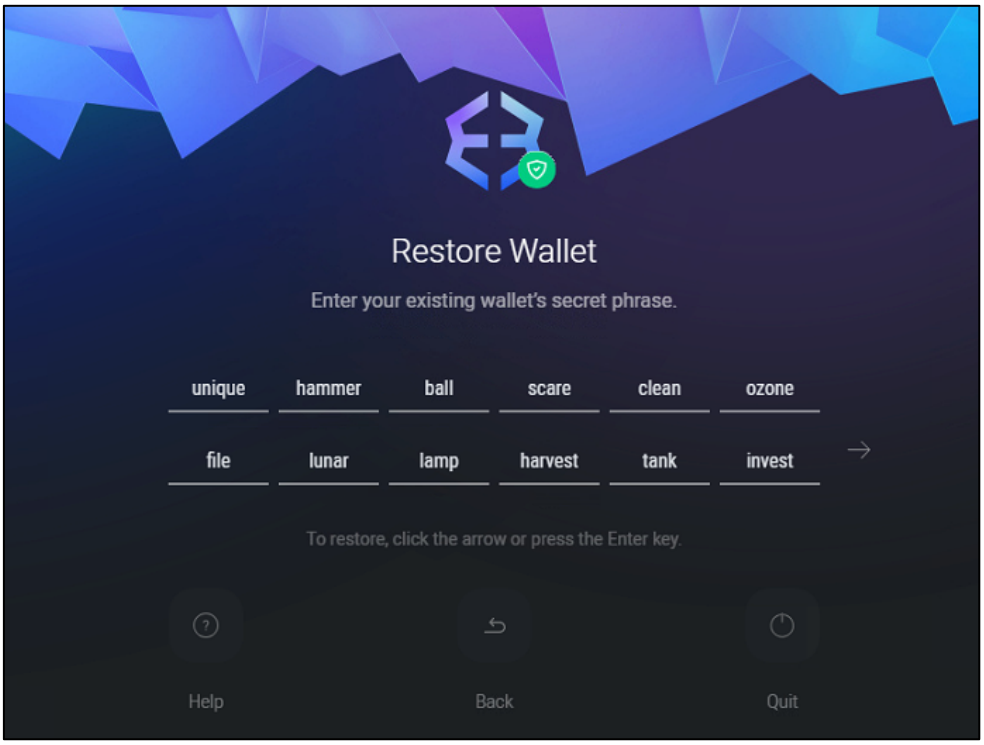
[그림 15] 설정을 모두 붙여넣은 모습.

모든 환경 설정을 완료한 후, Exodus를 실행하면, [그림 16]과 같이, 비밀번호를 입력하기 위한 화면을 확인할 수 있다. 또한 Restore을 통하여 니모닉 코드를 입력하는 창으로 이동할 수 있다.



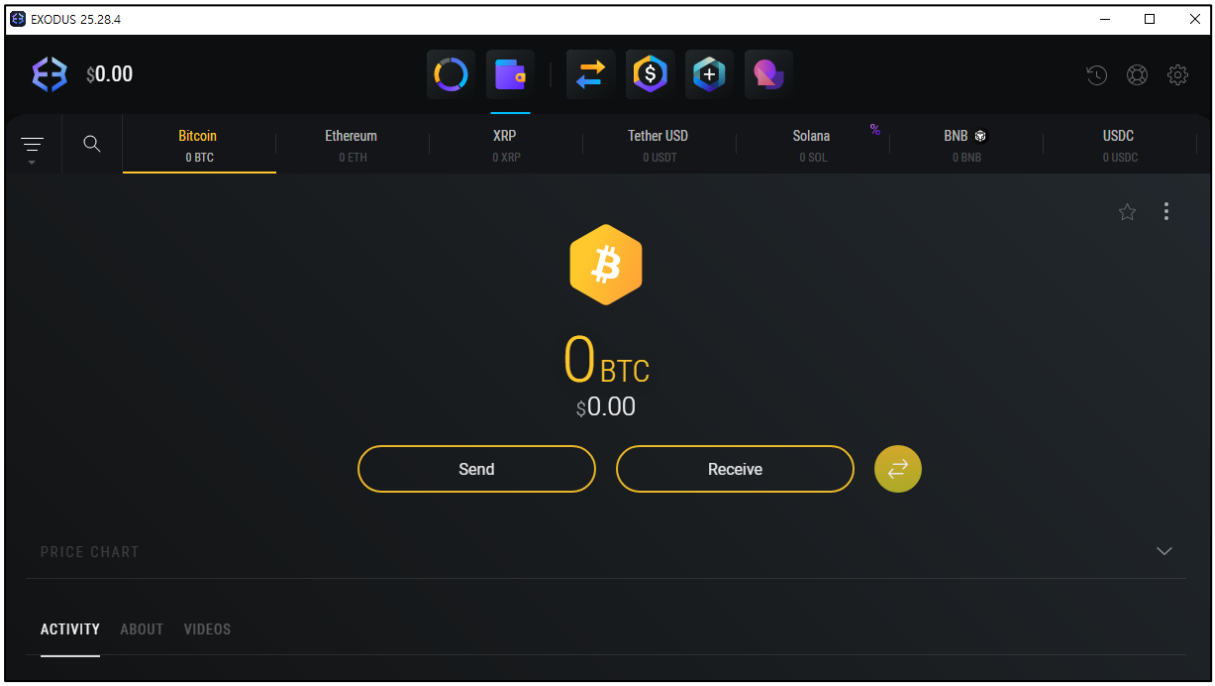
[그림 16] Exodus를 실행한 모습.

문제 2번에서 발견된 니모닉 코드를 [그림 17]과 같이 입력한 후 다음 버튼을 눌러 복구를 시도할 수 있다.



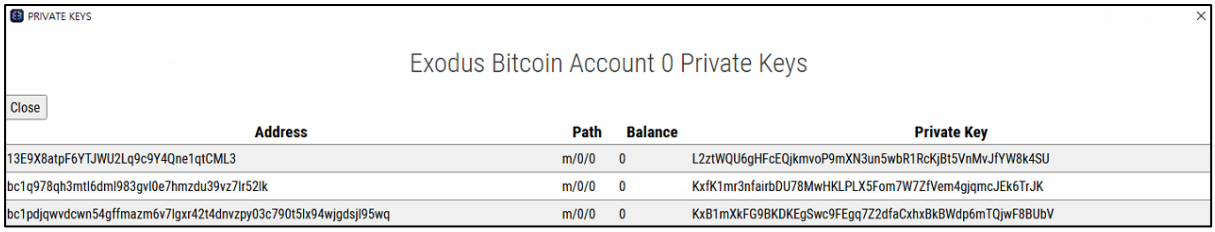
[그림 17] 니모닉 코드를 통한 복구 화면과 입력한 모습.

이를 통하여 정상적으로 용의자의 Exodus에 접속할 수 있었다.



[그림 18] 용의자의 Exodus 접속 모습.

이를 통하여 [그림 19]와 같이, 용의자의 비트코인 지갑 주소와 비밀 키를 획득할 수 있었다.



[그림 19] 용의자의 비트코인 지갑 주소와 비밀키.

비트코인 지갑 주소의 경우 "bc1"으로 시작되는 특성을 고려해 [표 7]과 같이 답안을 작성할 수 있다.

지갑 주소
bc1q978qh3mtl6dml983gvl0e7hmzdu39vz7lr52lk
bc1pdjqwvdcwn54gffmazm6v7lgxr42t4dnvzpy03c790t5lx94wjgdsjl95wq

[표 7] 용의자의 비트코인 지갑 주소.