

## 306 – Coin Chaser

### Team Information

Team Name: kimbabasaksaksak

Team Member: Jaeheon Kim, Donghyun Kim, Soyoung Yoo, Minhee Lee

Email Address: uaaooong@gmail.com

### Instructions

**Description** An investigator was examining a computer in the home of a suspected money launderer and found a cryptocurrency wallet program running. The investigator collected memory dumps and data files from the computer.

Target	Hash (MD5)
2023-07-04T074021_case001.zip	70FECCC08F37FBC949590E2E2FADB8A5
memory.7z	CCE5E6ECA3FF80308384BF226C4E6A6

### Questions

- 1) When was the crypto wallet program installed? (UTC+0) (20 points)
- 2) What time did the suspect encrypt the wallet? (UTC+0) (100 points)
- 3) What was the password for the encrypted wallet? (70 points)
- 4) Who deposited funds to the suspect's wallet address and who transferred funds from the wallet address? (70 points)
- 5) What is the final destination address of the funds transferred from

the suspect's wallet address? (40 points)

**Do not make transactions to cryptocurrency addresses that are checked during the solving question. Any transactions that occurred after the question publication date will not affect question resolution.**

**Tools used:**

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:	Magnet AXIOM	Publisher:	Magnet Forensics
Version:	7.5.0.37231		
URL:	<a href="https://www.magnetforensics.com/">https://www.magnetforensics.com/</a>		

Name:	Everything	Publisher:	voidtools
Version:	1.4.1.1024		
URL:	<a href="https://www.voidtools.com/">https://www.voidtools.com/</a>		

Name:	X-Ways Forensics	Publisher:	X-Ways
Version:	20.0		
URL:	<a href="https://www.x-ways.net/">https://www.x-ways.net/</a>		

Name:	Etherscan	Publisher:	Etherscan
Version:			
URL:	<a href="https://etherscan.io/">https://etherscan.io/</a>		

## Step-by-step methodology:

### Q1. When was the crypto wallet program installed? (UTC+0) (20 points)

Chrome 다운로드 기록을 확인하면, 용의자는 7개의 지갑 프로그램 설치 파일을 다운로드했다.

증거 (12)				
다운로드 소스	파일 이름	시작 시간 날짜/...	종료 시간 날짜/...	
https://github.com/notepad-plus-plus/notepad-plu...	npp.8.5.4.Installer.x64.exe	2023-07-03 AM 8:13:02	2023-07-03 AM 8:13:02	
https://download.sublimetext.com/sublime_text_buil...	sublime_text_build_4143_x64_setup.exe	2023-07-03 AM 8:13:35	2023-07-03 AM 8:13:35	
https://zoom.us/client/5.15.2.18096/ZoomInstallerF...	ZoomInstallerFull.exe	2023-07-03 AM 8:17:38	2023-07-03 AM 8:17:38	
https://download.electrum.org/4.4.5/electrum-4.4.5-...	electrum-4.4.5-setup.exe	2023-07-04 AM 1:24:20	2023-07-04 AM 1:24:20	
https://greenupdate.blockstream.com/desktop/1.2.3-...	BlockstreamGreen_Windows_x86_64.zip	2023-07-04 AM 1:25:05	2023-07-04 AM 1:25:05	
https://get.atomicwallet.io/download/atomicwallet-...	atomicwallet-2.70.12.exe	2023-07-04 AM 1:25:18	2023-07-04 AM 1:25:18	
https://get.atomicwallet.io/download/atomicwallet-...	atomicwallet-2.70.12 (1).exe	2023-07-04 AM 1:25:22	2023-07-04 AM 1:25:22	
https://downloads.exodus.com/releases/exodus-win...	exodus-windows-x64-23.7.3.exe	2023-07-04 AM 1:25:36	2023-07-04 AM 1:25:36	
https://github.com/guardaco/guarda-desktop-relea...	Guarda-Setup-1.0.20.exe	2023-07-04 AM 1:26:58	2023-07-04 AM 1:26:58	
https://objects.githubusercontent.com/github-prod...	armory_0.96_win64.exe	2023-07-04 AM 1:27:41	2023-07-04 AM 1:27:41	
https://objects.githubusercontent.com/github-prod...	armory_0.96_win64 (1).exe	2023-07-04 AM 1:27:44	2023-07-04 AM 1:27:44	
https://storage.coinomi.com/binaries/desktop/coino...	coinomi-wallet-1.3.0-win64.exe	2023-07-04 AM 1:28:12	2023-07-04 AM 1:28:12	

하지만, 그 중에서 용의자는 Exodus 지갑 프로그램만을 사용하였다.

Magnet AXIOM Examine v7.5.0.37231 - 306

파일(F)

도구

프로세스

도움말(H)

필터

증거

아티팩트

콘텐츠 유형

날짜 및 시간

태그 및 주석

프로필

부분 결과

키워드 목록

스킨톤 분석

exodus

«

🏠

📁 아티팩트

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색

🔍

검색


🔍

검색


🔍

검색

Exodus 설치 프로그램은 <https://downloads.exodus.com/releases/exodus-windows-x64-23.7.3.exe> 에서 다운로드 되어, `\Users\CryptoManiac\Downloads\exodus-windows-x64-23.7.3.exe` 경로에 저장되었다.

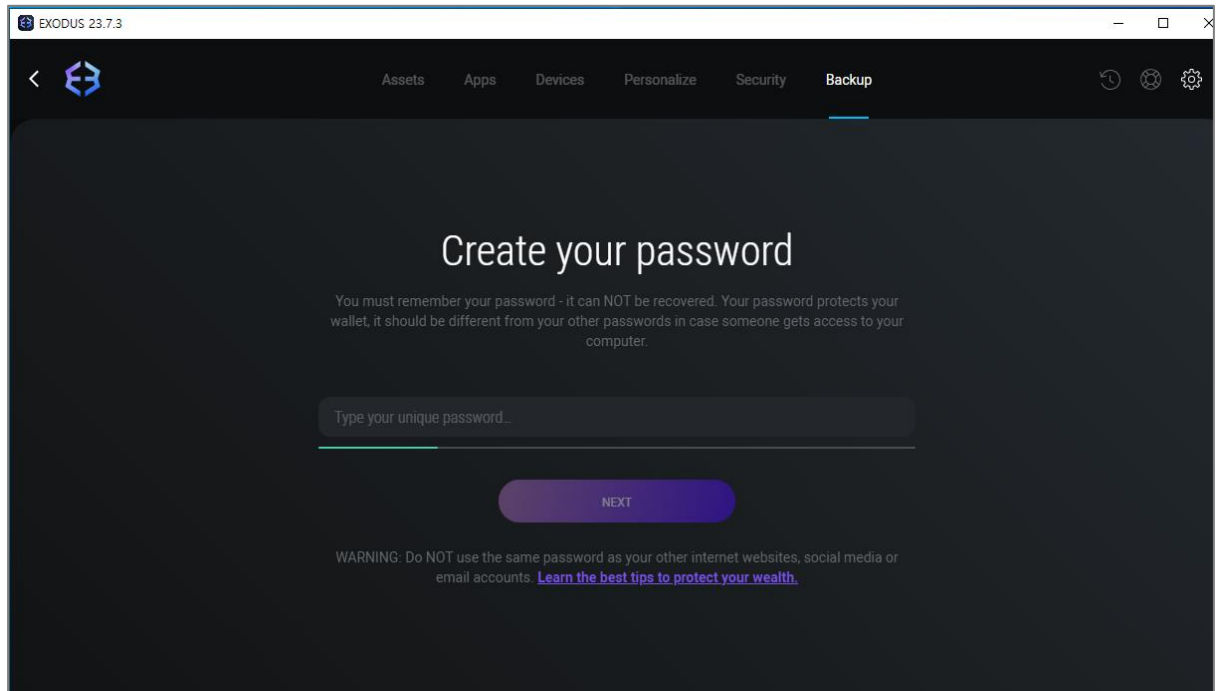
세부 정보		
아티팩트 정보		
다운로드 소스	<a href="https://downloads.exodus.com/releases/exodus-windows-x64-23.7.3.exe">https://downloads.exodus.com/releases/exodus-windows-x64-23.7.3.exe</a>	
파일 이름	<a href="#">exodus-windows-x64-23.7.3.exe</a>	
시작 시간 날짜/시간	2023-07-04 AM 1:25:36	⌚
종료 시간 날짜/시간	2023-07-04 AM 1:25:42	⌚
다음 대상에 저장	C:\Users\CryptoManiac\Downloads\exodus-windows-x64-23.7.3.exe	
상태	Download Complete	
열림	No	
다운로드된 바이트	192709600	
파일 크기(바이트)	192709600	
유형	 Chrome 다운로드	
항목 ID	8998	

Prefetch 기록을 확인하면, 해당 설치 프로그램은 **2023-07-04 02:45:47 (UTC+0)** 에 실행되었다. 즉, 이는 Exodus 지갑 프로그램이 설치된 시각이다.

아티팩트 정보	
응용 프로그램 이름	<a href="#">EXODUS-WINDOWS-X64-23.7.3.EXE</a>
응용 프로그램 경로	<code>\VOLUME{01d9ad6a104f0baa-4e1058a9}\USERS\CRYPTOMANIAC\DOWNLOADS\EXODUS-WINDOWS-X64-23.7.3.EXE</code>
응용 프로그램 실행 횟수	1
파일 생성한 날짜/시간	2023-07-04 AM 2:45:48
마지막 실행 날짜/시간	<a href="#">2023-07-04 AM 2:45:47</a>
파일 해시	CCEFE0E1
볼륨 이름	<code>\VOLUME{01d9ad6a104f0baa-4e1058a9}</code>
볼륨 생성 날짜/시간	2023-07-03 AM 4:51:43
유형	 Windows 8/10 프리패치 파일
항목 ID	2174

## Q2. What time did the suspect encrypt the wallet? (UTC+0) (100 points)

용의자가 설치한 Exodus 지갑 프로그램 23.7.3 버전을 설치하여 확인해보면, Settings > Backup > Create your password 기능을 사용하여 지갑을 암호화할 수 있다.



해당 기능을 사용하여 지갑을 암호화하면, 동시에 **\AppData\Roaming\Exodus\exodus.wallet** **\seed.seco** 파일과 **\AppData\Roaming\Exodus\exodus.wallet\twofactor-secret.seco** 파일이 수정된다.

이름	경로	크기	수정된 날짜
<input type="checkbox"/> twofactor-secret.seco	C:\Users\mal4e\AppData\Roaming\Exodus\exodus.wallet\twofactor-secret.seco	33 KB	2023-09-23 오후 3:49
<input type="checkbox"/> seed.seco	C:\Users\mal4e\AppData\Roaming\Exodus\exodus.wallet\seed.seco	33 KB	2023-09-23 오후 3:49
<input type="checkbox"/> TransportSecurity	C:\Users\mal4e\AppData\Roaming\Exodus\exodus.wallet\TransportSecurity	2 KB	2023-09-23 오후 3:49
<input type="checkbox"/> f_00000e	C:\Users\mal4e\AppData\Roaming\Exodus\exodus.wallet\f_00000e	2,635 KB	2023-09-23 오후 3:49
<input type="checkbox"/> lastalive0.dat	C:\Windows\ServiceState\EventLog\Data	2 KB	2023-09-23 오후 3:48
<input type="checkbox"/> storage.seco	C:\Users\mal4e\AppData\Roaming\Exodus\exodus.wallet\storage.seco	3 KB	2023-09-23 오후 3:48
<input type="checkbox"/> EVERYTHING.EXE-BC6730CA.pf	C:\Windows\Prefetch	15 KB	2023-09-23 오후 3:47
<input type="checkbox"/> ActivitiesCache.db-wal	C:\Users\mal4e\AppData\Local\Connecticut\ActivitiesCache.db-wal	1,924 KB	2023-09-23 오후 3:47
<input type="checkbox"/> RecoveryStore.{35EA8F3D-B629-4A92-A981-8C136C7474D5}.dat	C:\Users\mal4e\AppData\Local\PackageRecoveryStore.dat	7 KB	2023-09-23 오후 3:47
<input type="checkbox"/> mpenginedb.db-wal	C:\ProgramData\Microsoft\Windows Defender\mpenginedb.db-wal	2,861 KB	2023-09-23 오후 3:47
<input type="checkbox"/> SvcEngine-2023-09-23.0607.11744.1.aodl	C:\Users\mal4e\AppData\Local\Microsoft\SvcEngine-2023-09-23.0607.11744.1.aodl	419 KB	2023-09-23 오후 3:46

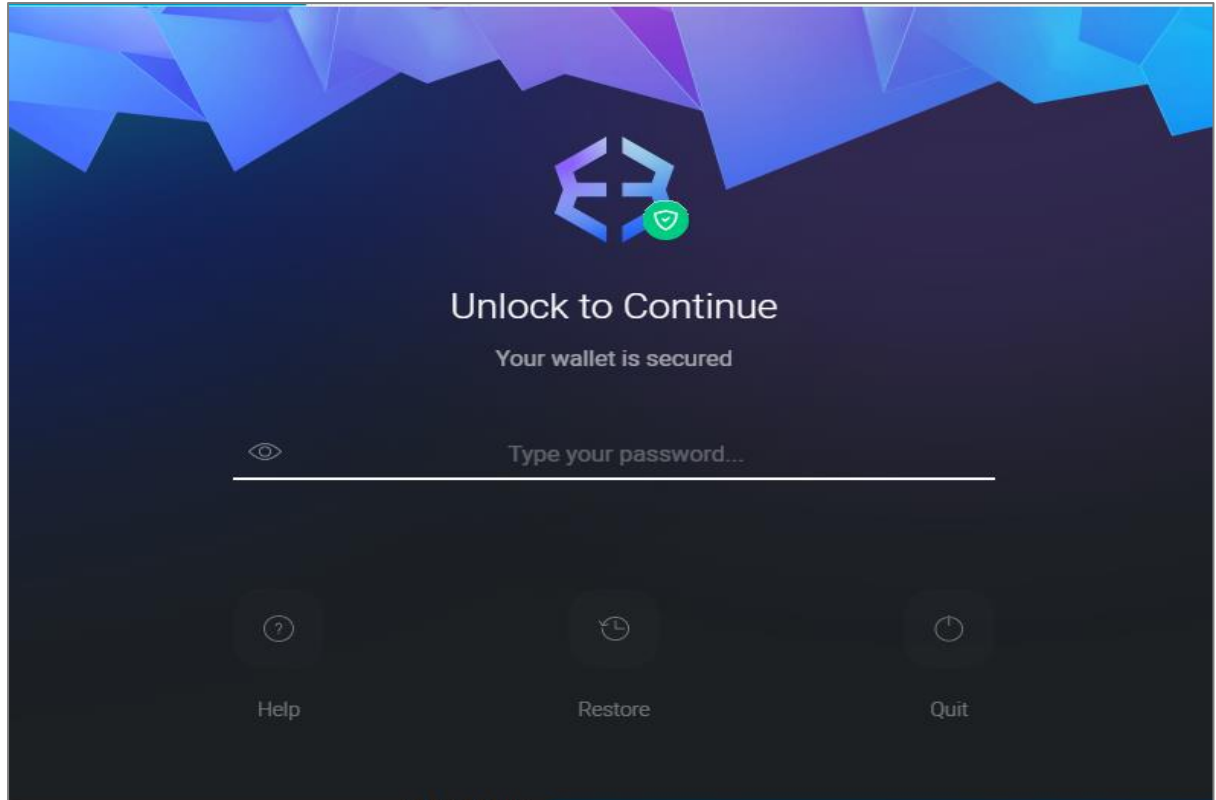
이미지 파일에서 두 파일이 수정된 시각을 확인하면, **2023-07-04 06:54:26 (UTC+0)** 시각에 수정되었다. 즉, 이는 용의자가 지갑을 암호화한 시각이다.

<b>Name</b>	seed.seco
<b>Path</b>	WUsers\WCryptoManiac\WAppData\WRoaming\WExodus\Wexodus.wallet
<b>Full path</b>	WUsers\WCryptoManiac\WAppData\WRoaming\WExodus\Wexodus.wallet\seed.seco
<b>Existent</b>	✓
<b>Description</b>	existing
<b>Ext.</b>	seco
<b>Type</b>	seco
<b>Type status</b>	not verified
<b>Type descr.</b>	seco
<b>Category</b>	Other/unknown type
<b>Evidence object</b>	C
<b>Parent name</b>	exodus.wallet
<b>Size</b>	32.5 KB (33,284)
<b>Created</b>	2023/07/04d04:10:45 +0
<b>Modified</b>	2023/07/04d06:54:26 +0
<b>Accessed</b>	2023/07/04d06:54:26 +0
<b>Attr.</b>	A
<b>ID</b>	5684

<b>Name</b>	twofactor-secret.seco
<b>Path</b>	WUsers\WCryptoManiac\WAppData\WRoaming\WExodus\Wexodus.wallet
<b>Full path</b>	WUsers\WCryptoManiac\WAppData\WRoaming\WExodus\Wexodus.wallet\Wtwofactor-secret.seco
<b>Existent</b>	✓
<b>Description</b>	existing
<b>Ext.</b>	seco
<b>Type</b>	seco
<b>Type status</b>	not verified
<b>Type descr.</b>	seco
<b>Category</b>	Other/unknown type
<b>Evidence object</b>	C
<b>Parent name</b>	exodus.wallet
<b>Size</b>	32.5 KB (33,284)
<b>Created</b>	2023/07/04d04:10:46 +0
<b>Modified</b>	2023/07/04d06:54:26 +0
<b>Accessed</b>	2023/07/04d06:54:26 +0
<b>Attr.</b>	A
<b>ID</b>	5686

### Q3. What was the password for the encrypted wallet? (70 points)

지갑을 암호화하고 지갑 프로그램을 다시 실행하면, 다음과 같이 패스워드를 입력해야 한다.



패스워드를 입력하고 해당 Exodus 프로그램의 메모리를 덤프하여 확인해보면, 패스워드가 평문으로 남아있다.

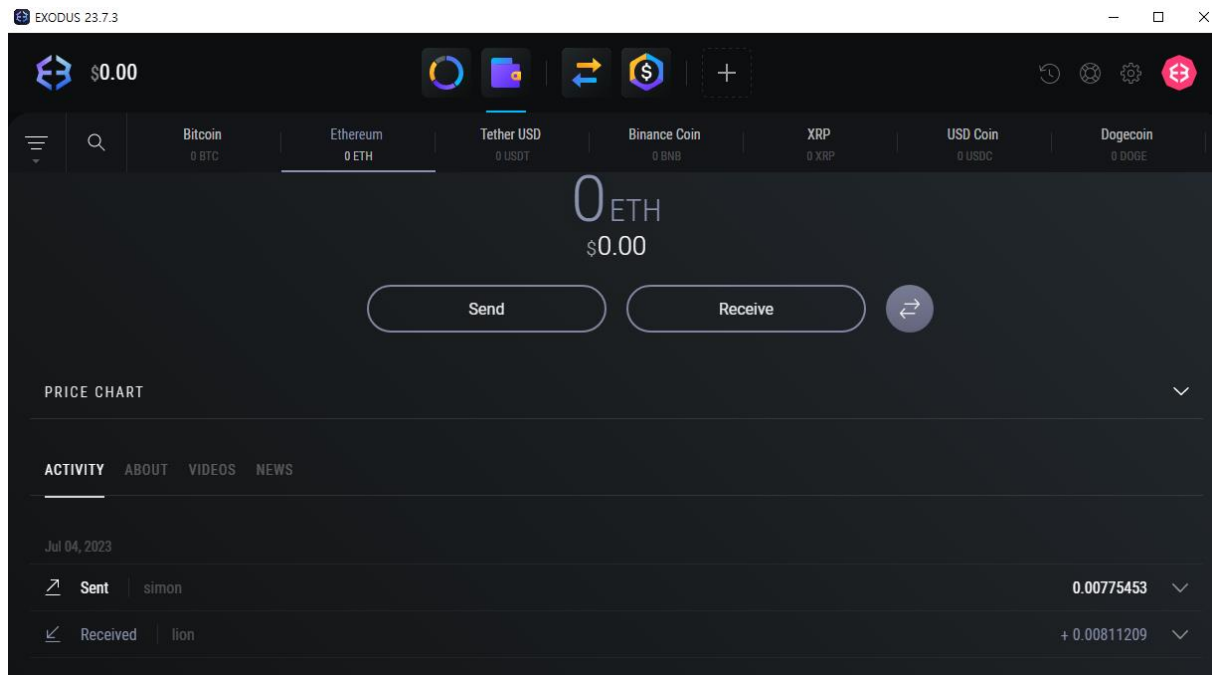
```
0050:2A70 0A 00 00 00 00 00 00 00 00 00 CD 0C 00 00 03 .....i....
0050:2A80 00 00 00 F9 00 00 00 66 69 6C 65 3A 2F 2F 2F 43 ...ù...file:///C
0050:2A90 3A 2F 55 73 65 72 73 2F 6D 61 6C 34 65 2F 41 70 :/Users/mal4e/Ap
0050:2AA0 70 44 61 74 61 2F 4C 6F 63 61 6C 2F 65 78 6F 64 pData/Local/exod
0050:2AB0 75 73 2F 61 70 70 2D 32 33 2E 37 2E 33 2F 72 65 us/app-23.7.3/re
0050:2AC0 73 6F 75 72 63 65 73 2F 61 70 70 2E 61 73 61 72 sources/app.asar
0050:2AD0 2F 73 72 63 2F 73 74 61 74 69 63 2F 77 61 6C 6C /src/static/wall
0050:2AE0 65 74 2E 68 74 6D 6C 23 25 37 42 25 32 32 77 61 et.html#%7B%22wa
0050:2AF0 6C 6C 65 74 44 69 72 25 32 32 25 33 41 25 32 32 lletDir%22%3A%22
0050:2B00 43 25 33 41 25 35 43 25 35 43 55 73 65 72 73 25 C%3A%5C%5CUsers%
0050:2B10 35 43 25 35 43 6D 61 6C 34 65 25 35 43 25 35 43 5C%5Cmal4e%5C%5C
0050:2B20 41 70 70 44 61 74 61 25 35 43 25 35 43 52 6F 61 AppData%5C%5CRoa
0050:2B30 6D 69 6E 67 25 35 43 25 35 43 45 78 6F 64 75 73 ming%5C%5CExodus
0050:2B40 25 35 43 25 35 43 65 78 6F 64 75 73 2E 77 61 6C %5C%5Cexodus.wal
0050:2B50 6C 65 74 25 32 32 25 32 43 25 32 32 70 61 73 73 let%22%2C%22pass
0050:2B60 70 68 72 61 73 65 25 32 32 25 33 41 25 32 32 64 phrase%22%3A%22d
0050:2B70 66 63 31 71 32 77 33 65 34 72 25 32 32 25 37 44 fc1q2w3e4r%22%7D
0050:2B80 00 00 00 05 11 00 00 06 00 00 00 55 6B 8D 00 E5 .....Uk..â
0050:2B90 38 82 00 01 02 00 00 31 F9 5C 00 C9 01 00 00 C9 8,...1ù\..É...É
0050:2BA0 01 00 00 A1 38 82 00 D1 38 82 00 05 11 00 00 0C ...j8,..N8,...
0050:2BB0 00 00 00 11 1E 00 00 11 1E 00 00 11 1E 00 00 4D .....M
0050:2BC0 BB 7B 00 91 38 82 00 01 02 00 00 2D 9A 8A 00 C9 »{.'8,...-šš.É
0050:2BD0 01 00 00 C9 01 00 00 19 3A 82 00 A5 EF 5C 00 C9 ...É.....:..¥i\..É
0050:2BE0 01 00 00 C9 01 00 00 00 07 00 00 09 39 82 00 0D ...É.....9...
0050:2BF0 33 00 00 0D 33 00 00 21 39 82 00 E5 01 00 00 35 3...3...!9,..â...5
```

메모리에 패스워드가  
평문으로 남아있음



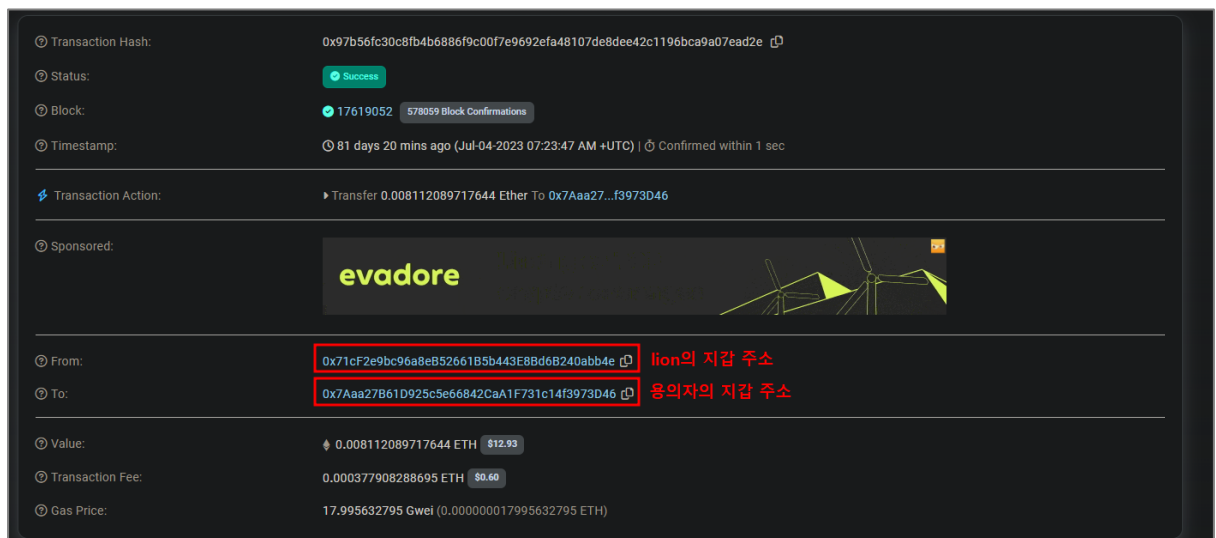
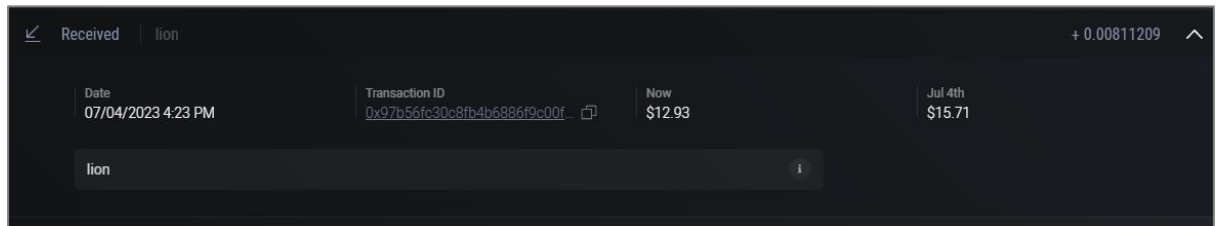


지갑 프로그램을 실행하여 **dkagghghkvP#** 패스워드를 입력하면, 정상적으로 지갑이 복호화되며 용의자의 지갑 데이터를 확인할 수 있다.

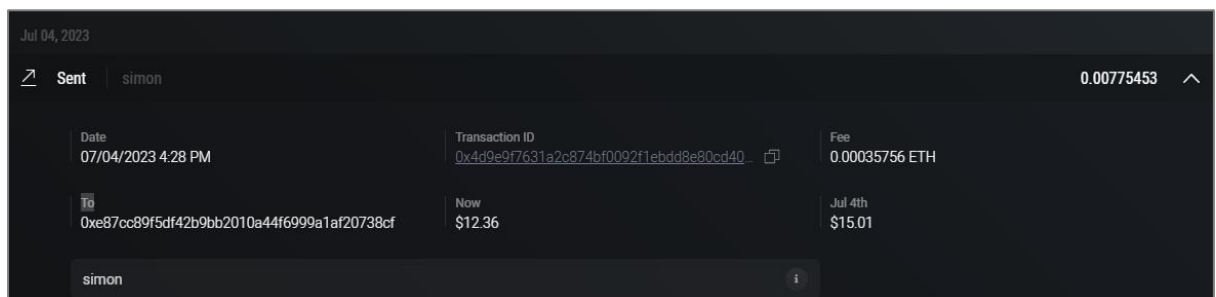


**Q4.** Who deposited funds to the suspect's wallet address and who transferred funds from the wallet address? (70 points)

용의자의 지갑을 확인하면, Ethereum의 Activity만 존재한다. 용의자의 지갑으로 자금을 입금한 사람은 **lion** 이며, 해당 Transaction의 ID는 **0x97b56fc30c8fb4b6886f9c00f7e9692efa48107de8dee42c1196bca9a07ead2e** 이다. Etherscan을 사용하여 해당 Transaction 기록을 확인하면, lion의 지갑 주소는 **0x71cF2e9bc96a8eB52661B5b443E8Bd6B240abb4e** 인 것을 알 수 있다.



반면에, 용의자가 자금을 송금한 대상자는 **simon** 이며, 해당 Transaction의 ID는 **0x4d9e9f7631a2c874bf0092f1ebdd8e80cd40d75fd18fabcd229ced126b8a2d6d**이다. Etherscan을 사용하여 해당 Transaction 기록을 확인하면, simon의 지갑 주소는 **0xe87Cc89F5dF42B9BB2010a44f6999a1af20738cF** 인 것을 알 수 있다.



Transaction Hash:

0x4d9e9f7631a2c874bf0092f1ebdd8e80cd40d75fd18fab0229ced126b8a2d6d

Status:

Success

Block:

17619078578066 Block Confirmations

Timestamp:

81 days 22 mins ago (Jul-04-2023 07:28:59 AM +UTC) | Confirmed within 10 secs

Transaction Action:

Transfer 0.007754533164073 Ether To 0xe87Cc8...f20738cF

Sponsored:

b

Blockscan Chat

Wallet-to-wallet instant messaging platform.

Start Chat

From:

0x7Aaa27B61D925c5e66842CaA1F731c14f3973D46

용의자의 지갑 주소

To:

0xe87Cc89F5dF42B9BB2010a44F6999a1af20738cF

simon의 지갑 주소

Value:

0.007754533164073 ETH\$12.36

Transaction Fee:

0.000357556553571 ETH\$0.57

Gas Price:

17.026502551 Gwei (0.000000017026502551 ETH)

More Details:

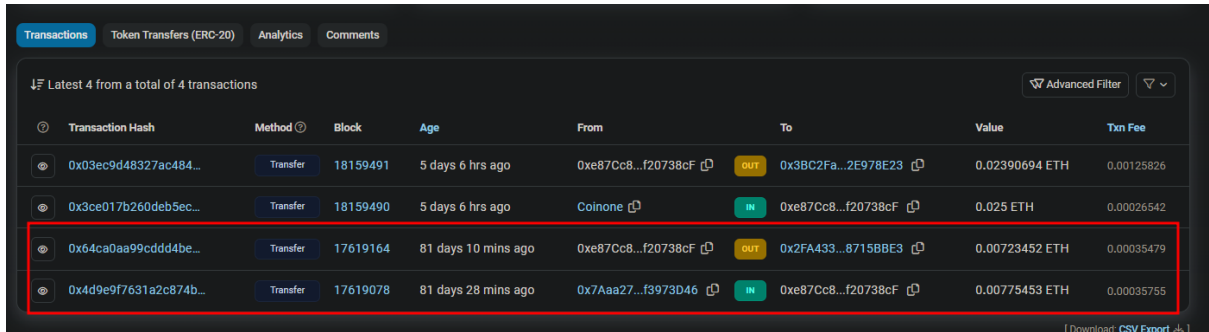
+ Click to show more

Private Note:

To access the Private Note feature, you must be Logged In

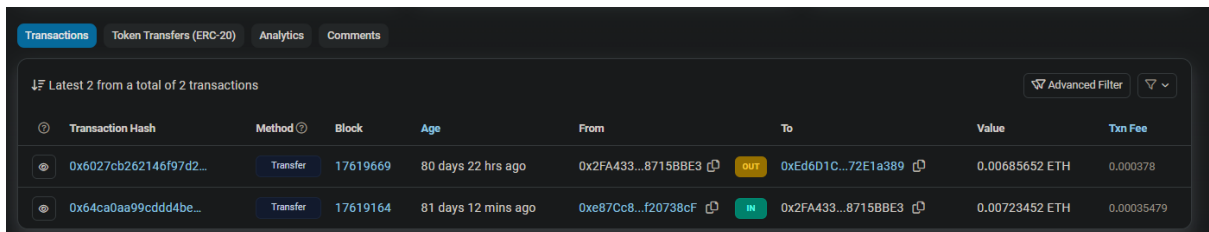
## Q5. What is the final destination address of the funds transferred from the suspect's wallet address? (40 points)

simon의 transaction 기록을 확인하면, 용의자에게 받은 자금을 0x2FA433c7A349CE4737c32578Ac5d5be28715BBE3 주소로 전달하였다.



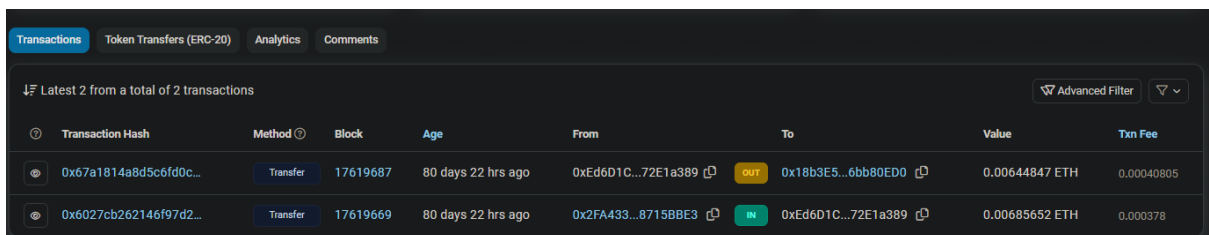
Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x03ec9d48327ac484...	Transfer	18159491	5 days 6 hrs ago	0xe87Cc8...f20738cF	0x3BC2Fa...2E978E23	0.02390694 ETH	0.00125826
0x3ce017b260deb5ec...	Transfer	18159490	5 days 6 hrs ago	Coinone	0xe87Cc8...f20738cF	0.025 ETH	0.00026542
0x64ca0aa99cddd4be...	Transfer	17619164	81 days 10 mins ago	0xe87Cc8...f20738cF	0x2FA433...8715BBE3	0.00723452 ETH	0.00035479
0x4d9e9f7631a2c874b...	Transfer	17619078	81 days 28 mins ago	0x7Aaa27...f3973D46	0xe87Cc8...f20738cF	0.00775453 ETH	0.00035755

해당 지갑의 transaction 기록을 확인하면, 수신한 자금을 0xEd6D1C4B8d55a2562799a933a93910A572E1a389 주소로 전달하였다.



Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x6027cb262146f97d2...	Transfer	17619669	80 days 22 hrs ago	0x2FA433...8715BBE3	0xEd6D1C...72E1a389	0.00685652 ETH	0.000378
0x64ca0aa99cddd4be...	Transfer	17619164	81 days 12 mins ago	0xe87Cc8...f20738cF	0x2FA433...8715BBE3	0.00723452 ETH	0.00035479

해당 지갑의 transaction 기록을 확인하면, 수신한 자금을 0x18b3E50152679c313A8d4eCBDB93eF5f6bb80ED0 주소로 전달하였다.



Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x67a1814a8d5c6fd0c...	Transfer	17619687	80 days 22 hrs ago	0xEd6D1C...72E1a389	0x18b3E5...6bb80ED0	0.00644847 ETH	0.00040805
0x6027cb262146f97d2...	Transfer	17619669	80 days 22 hrs ago	0x2FA433...8715BBE3	0xEd6D1C...72E1a389	0.00685652 ETH	0.000378

해당 지갑의 transaction 기록을 확인하면, 수신한 자금을 0xe435a736aD93F0Ea614F2a753a5f44116b21F1BD 주소로 전달하였다.

Transactions								
Token Transfers (ERC-20)								
Analytics								
Comments								
Latest 2 from a total of 2 transactions								
Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee	
0xc0260f644c0c552e5...	Transfer	17619690	80 days 22 hrs ago	0x18b3E5...6bb80ED0	OUT 0xe435a7...6b21F1BD	0.00604041 ETH	0.00040805	
0x67a1814a8d5c6fd0c...	Transfer	17619687	80 days 22 hrs ago	0xE6d6D1C...72E1a389	IN 0x18b3E5...6bb80ED0	0.00644847 ETH	0.00040805	

해당 지갑의 transaction 기록을 확인하면, 수신한 자금을 0x8E510474bA2F602f2D27BDd68C02A85cBbd753c 주소로 전달하였다.

Transactions								
Token Transfers (ERC-20)								
Analytics								
Comments								
Latest 2 from a total of 2 transactions								
Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee	
0xe949f7f10eac6fd34...	Transfer	17619704	80 days 22 hrs ago	0xe435a7...6b21F1BD	OUT 0x8E5104...cBbd753c	0.00574641 ETH	0.000294	
0xc0260f644c0c552e5...	Transfer	17619690	80 days 22 hrs ago	0x18b3E5...6bb80ED0	IN 0xe435a7...6b21F1BD	0.00604041 ETH	0.00040805	

해당 지갑의 transaction 기록을 확인하면, 수신한 자금을 더 이상 송신하지 않고 보관하고 있다. 즉, 0x8E510474bA2F602f2D27BDd68C02A85cBbd753c 가 최종 도착 주소이다.

Transactions								
Token Transfers (ERC-20)								
Analytics								
Comments								
Latest 1 from a total of 1 transactions								
Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee	
0xe949f7f10eac6fd34...	Transfer	17619704	80 days 22 hrs ago	0xe435a7...6b21F1BD	IN 0x8E5104...cBbd753c	0.00574641 ETH	0.000294	