306 – Coin Chaser

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun Ha, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.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	CCE5E6ECAF3FF80308384BF226C4E6A6

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)

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

Name:	Exodus	Publisher:	Exodus Movement
Version:	23.8.14		
URL:	https://www.exodus.com/download/		

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

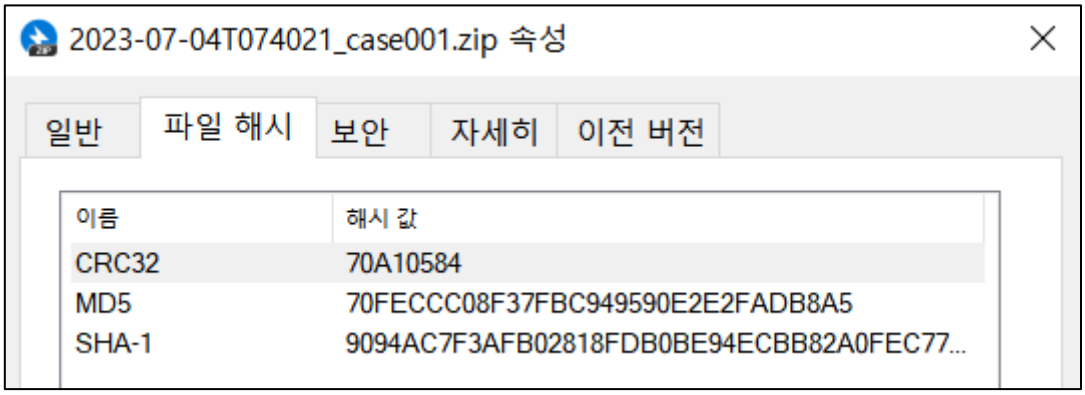
Name:	DB Browser for SQLite	Publisher:	sqlitebrowser
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Name:	Dcode	Publisher:	Digital Detective
Version:	5.5		
URL:	https://www.digital-detective.net/dcode/		

Name:	WinPrefetchView	Publisher:	NirSoft
Version:	1.36		
URL:	https://www.nirsoft.net		

Name:	NTFS Log Tracker	Publisher:	Junghoon Oh
Version:	1.71		
URL:	https://sites.google.com/site/forensicnote/ntfs-log-tracker		

Step-by-step methodology:



[그림 1] 분석 파일의 해시 값 확인 - 1

분석에 앞서, 주어진 2023-07-04T074021_case001.zip 파일에 대한 md5 해시 값이 일치함을 확인하였습니다.

[그림 2] 분석 파일의 해시 값 확인 - 2

또한, memory-001.7z 파일의 해시 값 역시 일치함을 확인하였습니다.

1) When was the crypto wallet program installed? (UTC+0) (20 points)

테이블(T): downloads

	id	guid	current_path
		필터	필터
1	6	2df925f9-1fa1-45c4-a928-9034008da078	C:₩Users₩CryptoManiac₩Downloads₩npp.8.5.4.Installer.x64.exe
2	7	a80e8f80-717b-49cd-b4d5-···	C:₩Users₩CryptoManiac₩Downloads₩sublime_text_build_4143_x64_setup.exe
3	8	e29895b1-1d0d-45ff-b8bd-06ee5fd34120	C:₩Users₩CryptoManiac₩Downloads₩ZoomInstallerFull.exe
4	9	9822bb71-0e6a-4356-aed2-···	C:₩Users₩CryptoManiac₩Downloads₩electrum-4.4.5-setup.exe
5	10	0d11fbf4-23df-4769-bb52-91d1c7fa6328	C:₩Users₩CryptoManiac₩Downloads₩BlockstreamGreen_Windows_x86_64.zip
6	11	e19b4224-4fc2-40fd-9be0-5cde5a554···	C:₩Users₩CryptoManiac₩Downloads₩atomicwallet-2.70.12.exe
7	12	70189542-54bb-4763-9797-773881fff8d2	
8	13	45112af3-63e7-421d-be72-edffa0f3ee64	C:₩Users₩CryptoManiac₩Downloads₩exodus-windows-x64-23.7.3.exe
9	14	aac70ba4-5dd7-418e-8196-···	C:₩Users₩CryptoManiac₩Downloads₩Guarda-Setup-1.0.20.exe
10	16	e5aea787-6c62-45a8-···	C:₩Users₩CryptoManiac₩Downloads₩armory_0.96_win64.exe
11	17	f846cc9e-a8df-4011-9a48-f084fc3250c5	
12	18	a764169e-18d8-4a3c-871a-0cf97bb7a···	C:₩Users₩CryptoManiac₩Downloads₩coinomi-wallet-1.3.0-win64.exe

[그림 3] 용의자가 chrome에서 다운로드 한 파일 정보

먼저, crypto wallet program 관련 다운로드 기록을 확인하기 위해 Chrome history 파일을 db browser for SQLite도구로 확인하였습니다.

EXODUS-WINDOWS-X64-23.7.3.EXE-CCEFE0E1.pf	2023-07-04 오전 11:45:48	2023-07-04 오전 11:45:48	47,467	EXODUS-WINDOWS-X64-...
EXODUS.EXE-AEF31E5D.pf	2023-07-04 오후 1:10:41	2023-07-04 오후 4:22:21	5,175	EXODUS.EXE
EXODUS.EXE-FA238DDE.pf	2023-07-04 오전 11:46:00	2023-07-04 오후 4:22:30	52,338	EXODUS.EXE
EXODUS.EXE-FA238DDF.pf	2023-07-04 오후 1:10:51	2023-07-04 오후 4:22:32	26,077	EXODUS.EXE
EXODUS.EXE-FA238DE0.pf	2023-07-04 오전 11:46:00	2023-07-04 오후 4:24:21	18,502	EXODUS.EXE
EXODUS.EXE-FA238DE6.pf	2023-07-04 오전 11:46:00	2023-07-04 오후 4:23:56	12,319	EXODUS.EXE

[그림 4] 다운로드 된 파일 중 설치 파일을 실행한 기록

또한, prefetch 아티팩트를 통해 실행 기록을 살펴보면 용의자가 다운로드 한 crypto wallet program 중에 exodus-windows-x64-23.7.3.exe 를 실행한 기록을 확인할 수 있습니다.

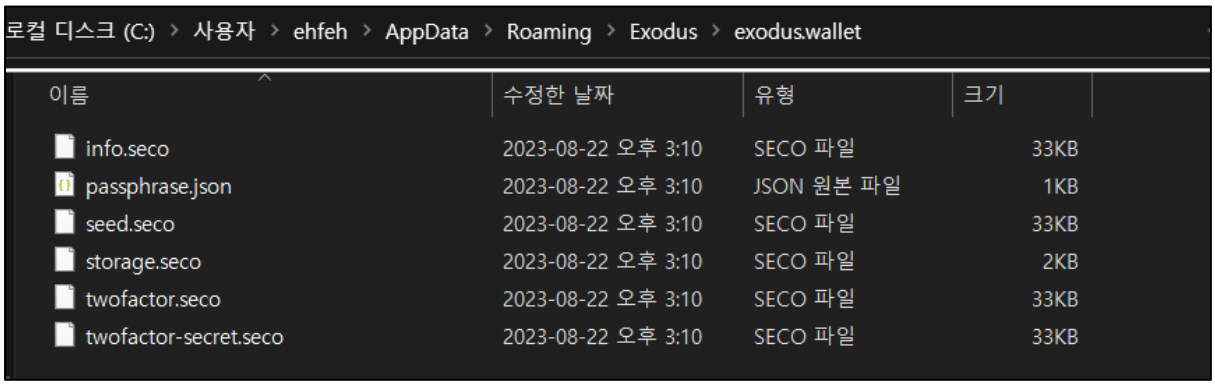
```
Filename        : EXODUS-WINDOWS-X64-23.7.3.EXE-CCEFE0E1.pf
Created Time    : 2023-07-04 오전 11:45:48
Modified Time   : 2023-07-04 오전 11:45:48
File Size       : 47,467
Process EXE     : EXODUS-WINDOWS-X64-23.7.3.EXE
Process Path    : ₩VOLUME{01d9ad6a104f0baa-4e1058a9}₩USERS₩CRYPTO
Run Counter     : 1
Last Run Time   : 2023-07-04 오전 11:45:47
Missing Process : No
```

[그림 5] 설치 시각 확인

이를 통해 해당 프로그램에 대한 정보를 export하여 살펴보았을 때, 용의자가 설치한 crypto wallet program인 exodus의 설치 시각은 **2023-07-04 02:45:47(UTC+0)**임을 확인하였습니다.

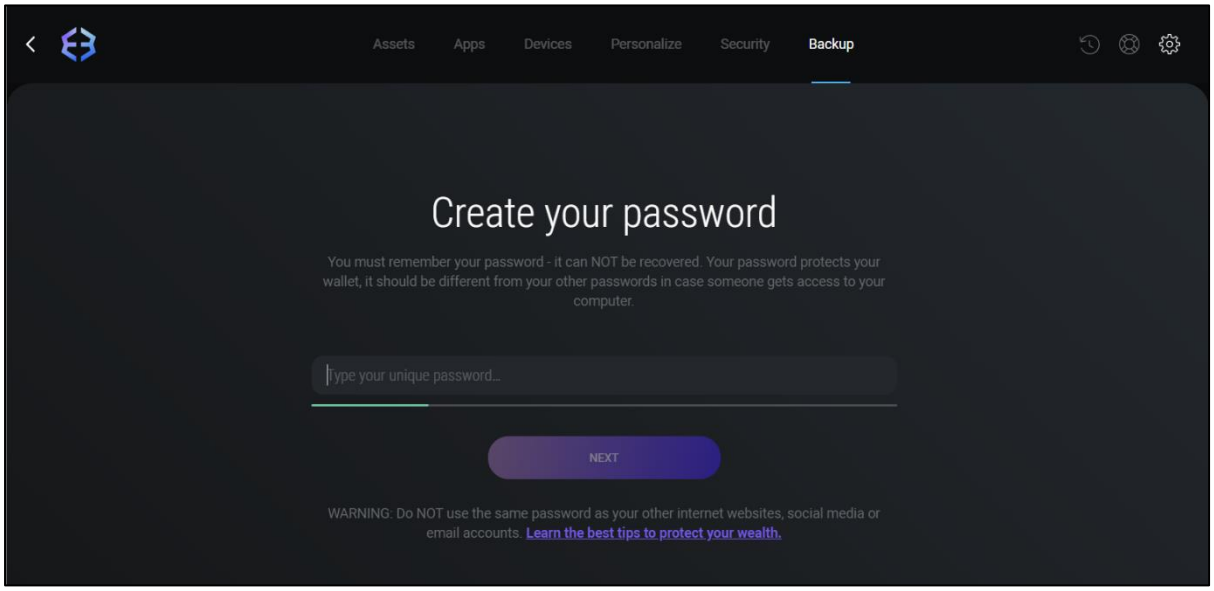
2) What time did the suspect encrypt the wallet? (UTC+0) (100 points)

용의자가 지갑을 암호화한 시각을 파악하기 위해서는 직접 exodus 지갑 프로그램을 설치하여 암호화를 진행해보는 재현의 과정 통해 파일의 변화를 파악하는 부분이 필요하다고 판단하였습니다.



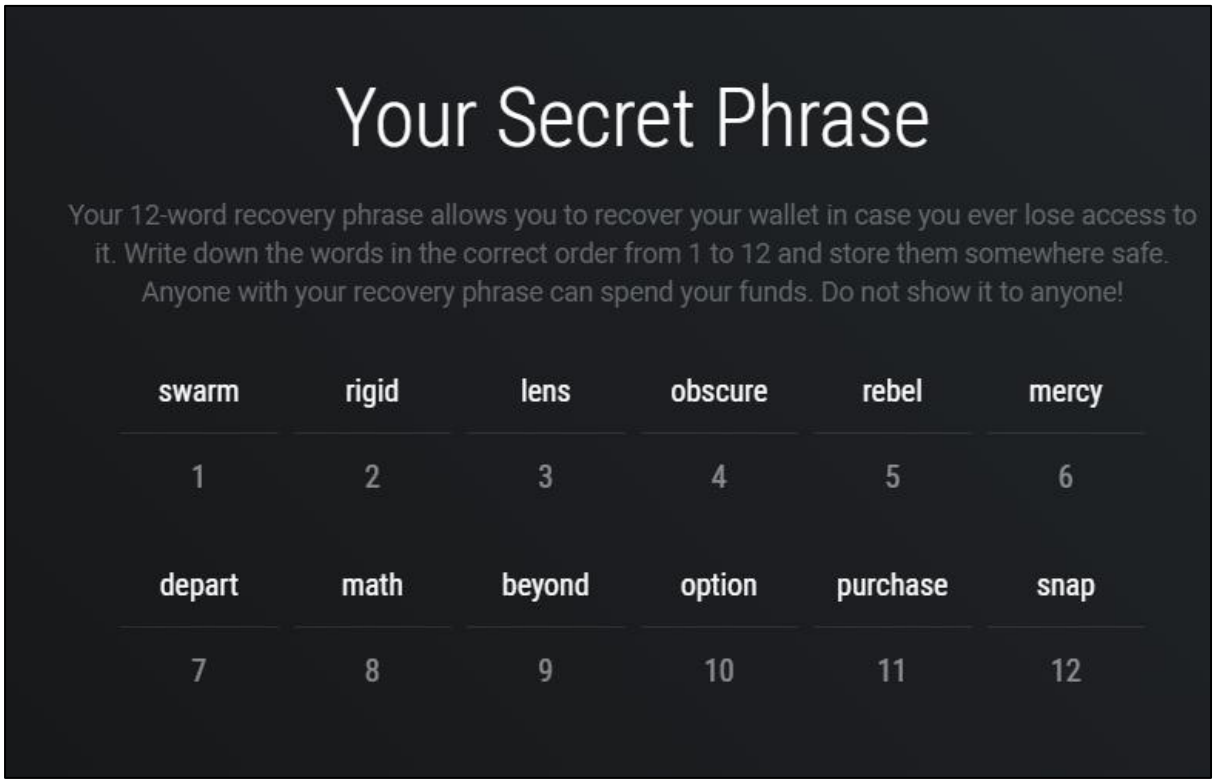
[그림 6] 지갑과 관련된 exodus.wallet 내 초기 파일 구성

먼저 exodus를 설치하고 프로그램을 실행하게 되면 exodus.wallet이라는 폴더와 partitions 폴더가 생성되었습니다. 그 후, exodus.wallet 폴더 내에는 위 그림과 같이 seco파일들과 passphrase.json 파일이 존재하는 것을 확인할 수 있습니다.



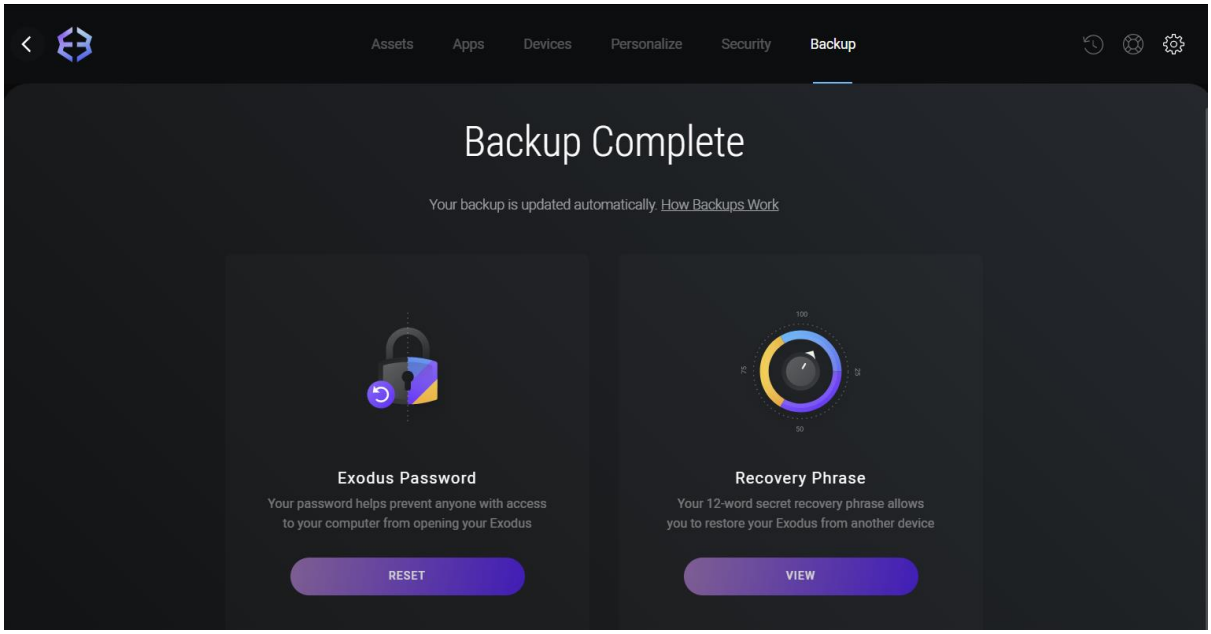
[그림 7] 재현을 위한 암호화 진행 - 1

지갑을 암호화하기 위해 exodus 자체 기능인 backup 설정에서 암호를 입력해주었습니다.



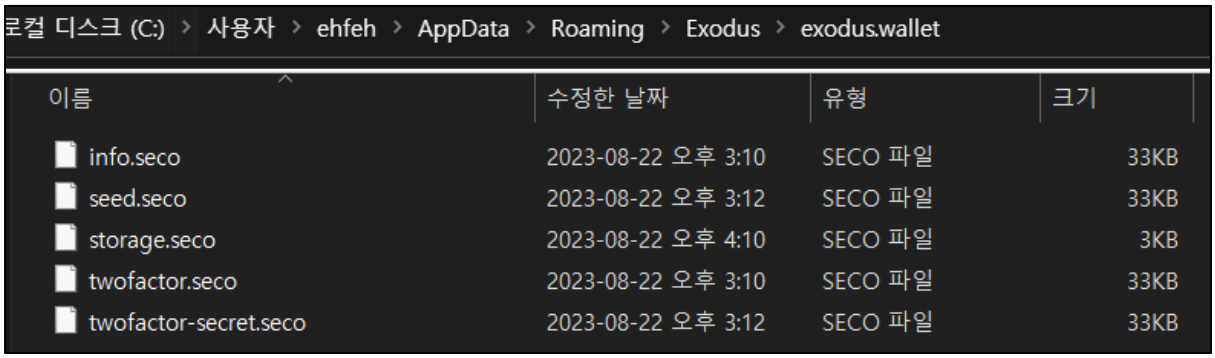
[그림 8] 재현을 위한 암호화 진행 - 2

그 후, 암호를 입력하고 12개의 secret phrase를 확인한 다음, 검증을 위해 질문에서 요구하는 phrase를 하나 선택하게 됩니다.



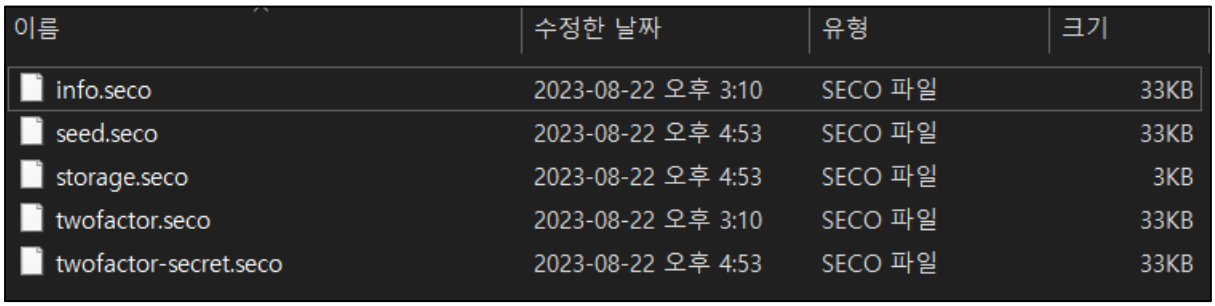
[그림 9] 재현을 위한 암호화 진행 - 3

입력 과정이 끝나면 암호화가 정상적으로 완료되고, 위 그림과 같은 화면을 확인할 수 있습니다.



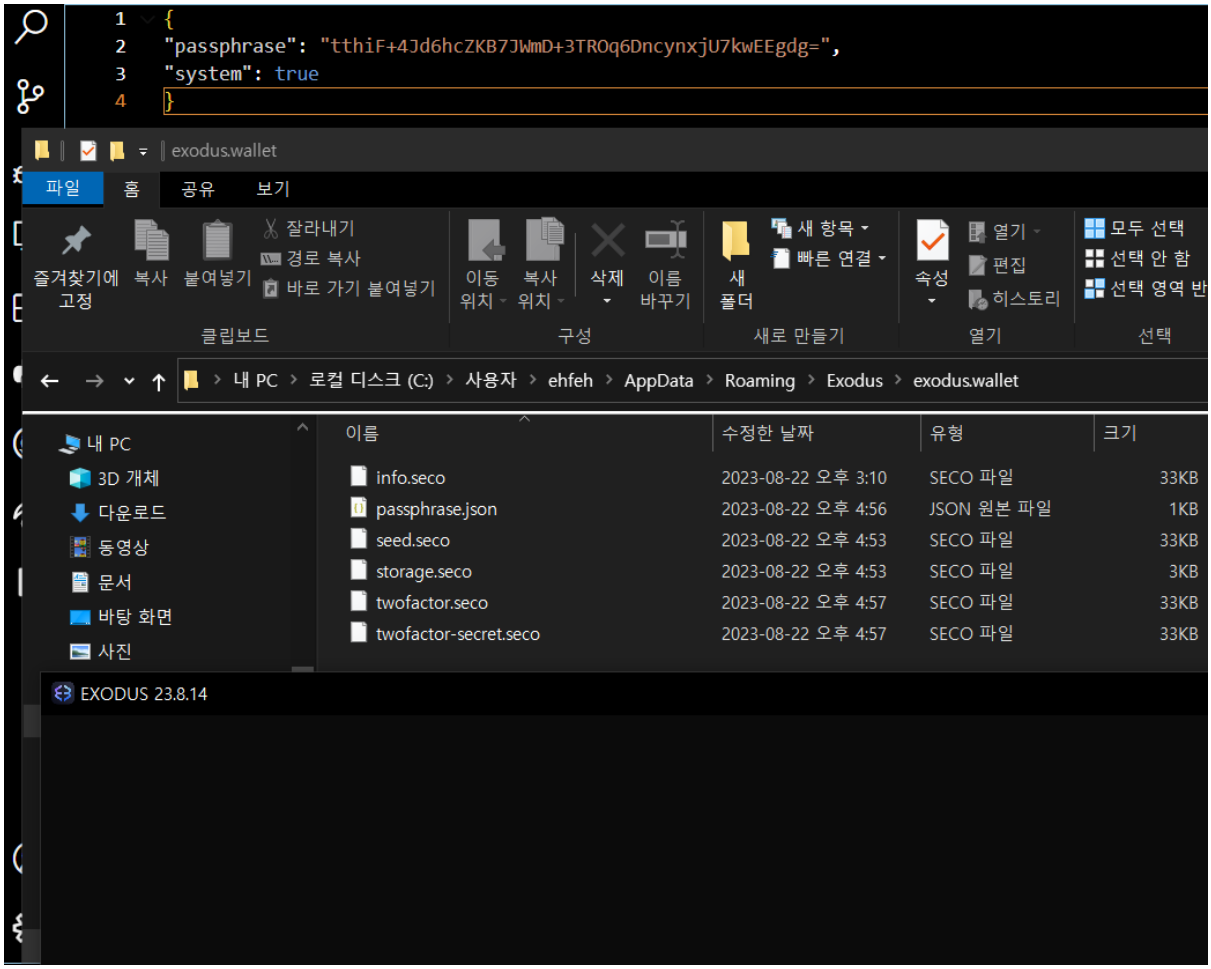
[그림 10] 암호화 이후 exodus.wallet 내 파일 구성 상태

암호화를 진행하고 나면, 위 그림의 경로에서 passphrase.json파일이 삭제되고, seed.seco 파일과 twofactor-secret.seco, 그리고 storage.seco 파일의 시각이 변경되는 것을 확인하였습니다. 하지만, storage.seco는 암호화가 아닌 다른 기능을 이용해도 수시로 갱신되기 때문에 수정날짜가 계속 최신화되는 것도 확인이 가능했습니다.



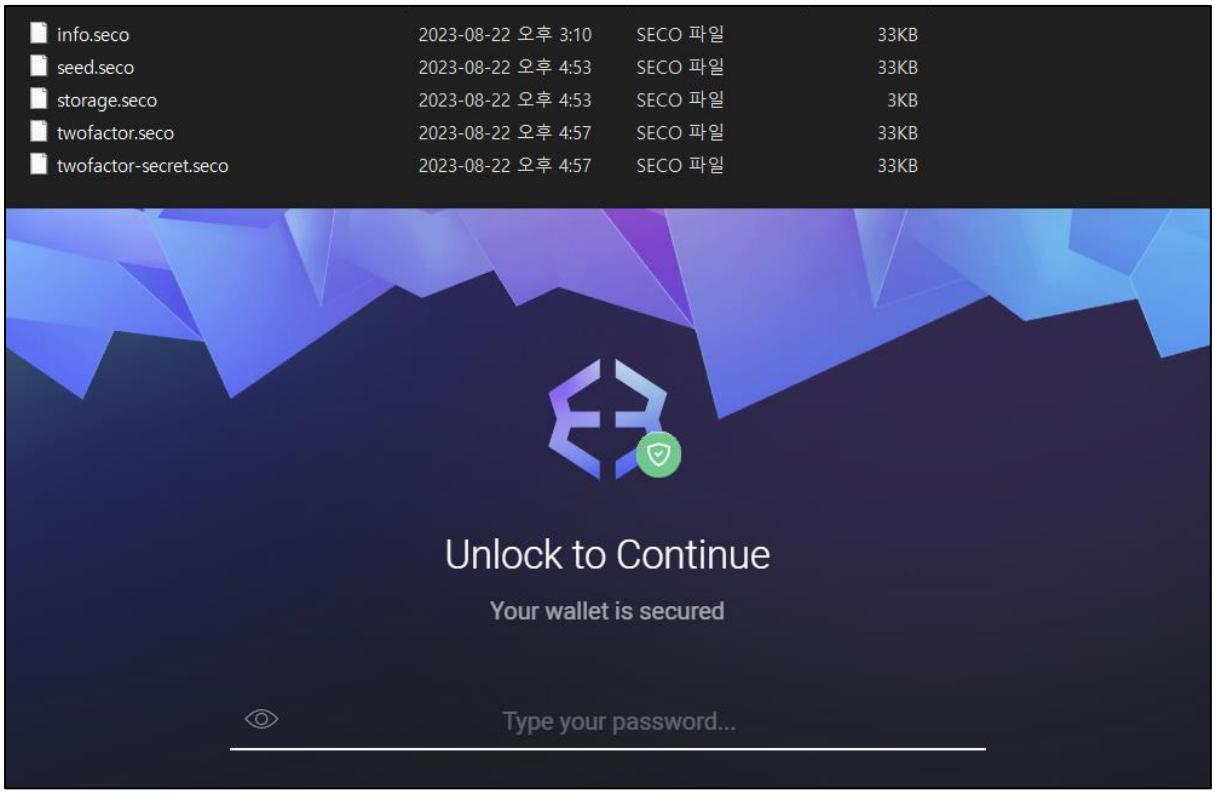
[그림 11] reset 후 재암호화 시 변경 시각 정보

여러 번의 재현 과정을 통해 재암호화 시 마찬가지로 seed.seco, storage.seco, twofactor-secret.seco 파일의 변경 상태를 확인하였으며, 이때는 암호화 직후로 세 파일의 시각이 동일함을 확인하였습니다.



[그림 12] 초기 passphrase.json 파일을 재생성 후 실행 시도

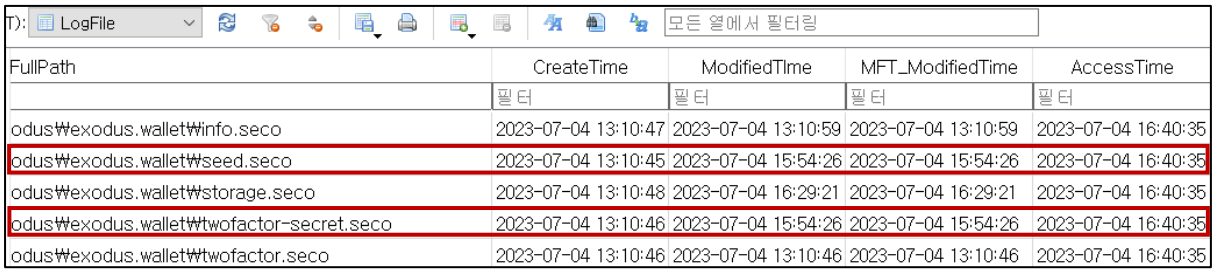
이번에는, exodus password reset 기능을 이용하여 password를 reset 한 후에 초기에 삭제되었던 passphrase.json을 다시 exodus.wallet 폴더에 생성한 후, 프로그램을 실행시키면 정상적으로 동작하지 않는 것을 확인하였습니다.



[그림 13] password reset 후 다시 실행

또한, password를 reset하였음에도 wallet은 이미 암호화가 진행되어 다시 프로그램을 실행하면 다음과 같은 화면이 나타나는 것을 확인할 수 있습니다.

따라서, 용의자가 지갑 암호화를 수행했던 시각은 여러 번의 재현 과정을 통해 passphrase.json이 삭제된 시각과 seed.seco 및 twofactor-secret.seco 파일 변경 시각과 관련이 있을 것으로 판단하였습니다.

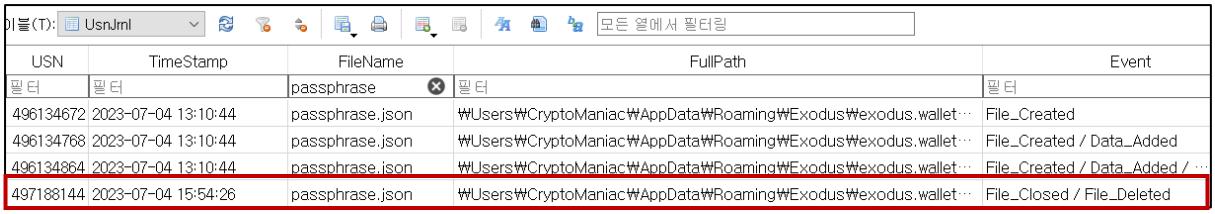


T): LogFile 모든 열에서 필터링

FullPath	CreateTime	ModifiedTIme	MFT_ModifiedTime	AccessTime
	필터	필터	필터	필터
odus₩exodus.wallet₩info.seco	2023-07-04 13:10:47	2023-07-04 13:10:59	2023-07-04 13:10:59	2023-07-04 16:40:35
odus₩exodus.wallet₩seed.seco	2023-07-04 13:10:45	2023-07-04 15:54:26	2023-07-04 15:54:26	2023-07-04 16:40:35
odus₩exodus.wallet₩storage.seco	2023-07-04 13:10:48	2023-07-04 16:29:21	2023-07-04 16:29:21	2023-07-04 16:40:35
odus₩exodus.wallet₩twofactor-secret.seco	2023-07-04 13:10:46	2023-07-04 15:54:26	2023-07-04 15:54:26	2023-07-04 16:40:35
odus₩exodus.wallet₩twofactor.seco	2023-07-04 13:10:46	2023-07-04 13:10:46	2023-07-04 13:10:46	2023-07-04 16:40:35

[그림 14] $Logfile 내 seed.seco 파일과 twofactor-secret.seco 파일 변경 시각 확인

주어진 증거파일 내 존재하던 $Logfile, $MFT, $UsnJrnl 을 ntfs log tracker를 통해 파싱한 후, 파일 변경 시각을 살펴보았을 때, $Logfile에서 seed.seco와 twofactor-secret.seco의 modifiedTime이 2023-07-04 15:54:26(UTC+9)임을 확인할 수 있었습니다.



)이블(T): UsnJrnl 모든 열에서 필터링

USN	TimeStamp	FileName	FullPath	Event
필터	필터	passphrase	필터	필터
496134672	2023-07-04 13:10:44	passphrase.json	₩Users₩CryptoManiac₩AppData₩Roaming₩Exodus₩exodus.wallet···	File_Created
496134768	2023-07-04 13:10:44	passphrase.json	₩Users₩CryptoManiac₩AppData₩Roaming₩Exodus₩exodus.wallet···	File_Created / Data_Added
496134864	2023-07-04 13:10:44	passphrase.json	₩Users₩CryptoManiac₩AppData₩Roaming₩Exodus₩exodus.wallet···	File_Created / Data_Added / ···
497188144	2023-07-04 15:54:26	passphrase.json	₩Users₩CryptoManiac₩AppData₩Roaming₩Exodus₩exodus.wallet···	File_Closed / File_Deleted

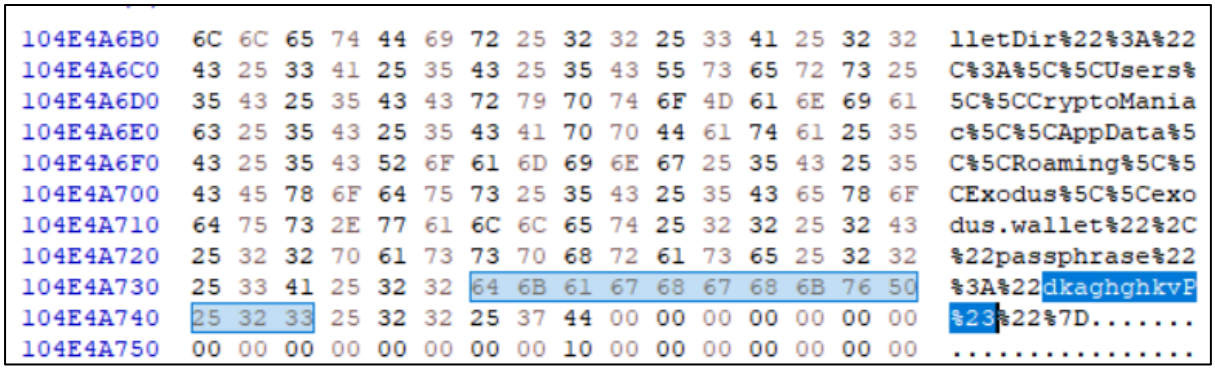
[그림 15] passphrase.json 파일의 삭제 시각 확인

또한, $UsnJrnl에서는 passphrase.json 파일의 삭제 시각이 2023-07-24 15:54:26(UTC+9)로 이는 seed.seco와 twofactor-secret.seco 파일의 변경시각과 일치했습니다.

따라서, 용의자가 지갑을 암호화 한 시각은 **2023-07-24 06:54:26(UTC+0)**으로 확인하였습니다.

3) What was the password for the encrypted wallet? (70 points)

암호화된 지갑에 대한 패스워드 정보는 주어진 메모리 덤프 파일에서 확인할 수 있었습니다.



[그림 16] memory.dump 내 식별된 password 정보

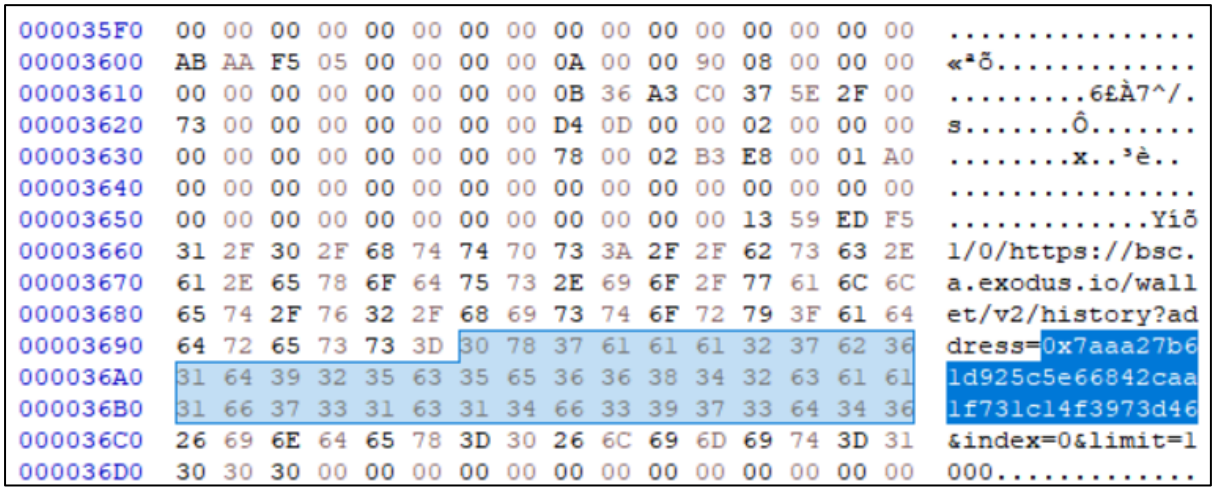
참고자료[1]를 통해 암호화된 지갑에 대한 password 정보가 메모리 덤프를 진행했기 때문에 해당 파일 내에 평문으로 존재할 것이라고 생각했고, "exodus.wallet%22%2C%22passphrase"라는 문자열을 HxD상에서 검색하여 다량의 method call 정보 내 들어있는 특정 password 문자열을 확인하였습니다. 이로써, 용의자가 지갑 암호화에 사용한 비밀번호는 **dkaghghkvP#** 로 확인하였습니다.

[1] https://www.upsightsecurity.com/post/hot-wallets-during-crypto-winter

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

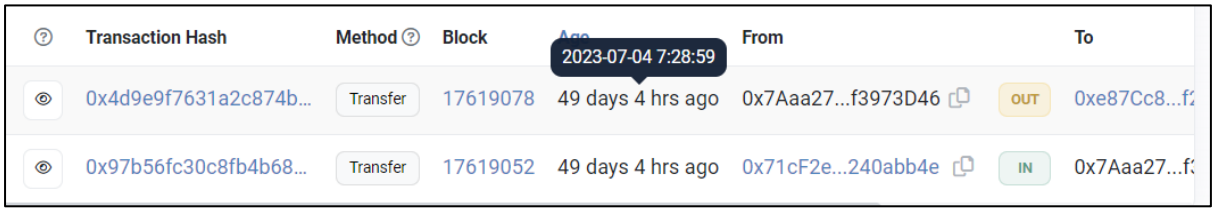
용의자의 지갑 주소 정보는 다음과 같은 파일에서 발견할 수 있었습니다.

- C:\Users\CryptoManiac\AppData\Roaming\Exodus\Partitions\main\Cache\Cache_Data\data_1



[그림 17] data_1 파일에서 발견된 용의자의 지갑 주소

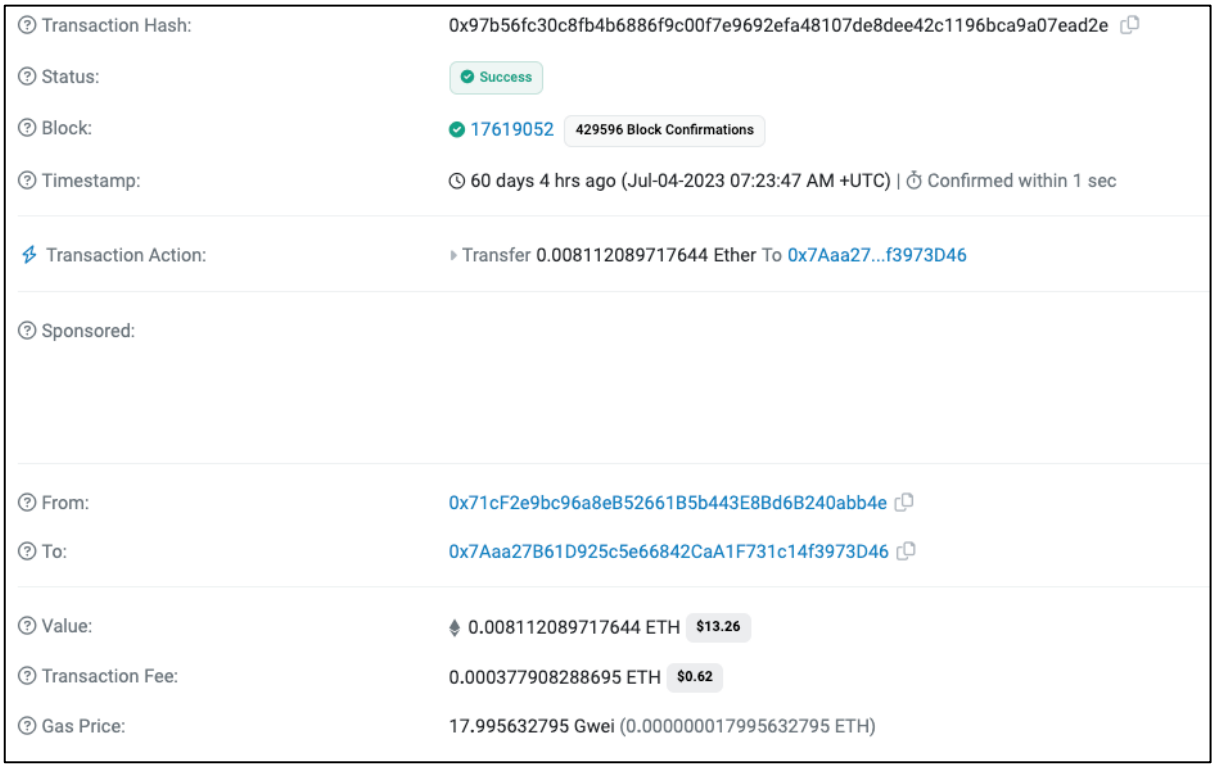
Cache_data 폴더 내 data_1 파일에는 캐시 정보가 남아있었고, HxD를 통해 탐색을 진행한 결과 위 그림과 같이 0x7aaa27b61d925c5e66842caa1f731c14f3973d46 라는 주소를 발견할 수 있었습니다.



[그림 18] 최종 거래 날짜 확인

Etherscan을 통해 해당 주소를 검색한 결과 거래 날짜가 용의자가 exodus를 설치하고 암호화를 한 날짜와 일치했으며, HxD 탐색 상 to와 from wallet address 정보와 및 block hash 정보 확인되는 지갑 주소는 0x7aaa27b61d925c5e66842caa1f731c14f3973d46가 유일했기 때문에 용의자의 지갑 주소라고 판단하였습니다.

위 검색결과를 바탕으로 ehtereum이 송금된 트랜잭션 0x97b56fc30c8fb4b6886f9c00f7e9692efa48107de8dee42c1196bca9a07ead2e을 확인할 수 있었습니다.



[그림 19] Ethereum이 입금된 트랜잭션

위 트랜잭션의 정보를 통해 From(0x71cF2e9bc96a8eB52661B5b443E8Bd6B240abb4e)의 주소가 0.008112089717644 ETH를 용의자의 지갑으로 송금한 것을 확인하였습니다.

[그림 20] Etherscan 검색결과

0x71cF2e9bc96a8eB52661B5b443E8Bd6B240abb4e 또한 트랜잭션 0x7d2085d2bf4870c11241b8e8428f84fb97d3960cb50b15cb04c13e1b79dc4396을 통해 0x0628A01D1a3232FB0E77202647790B01540894c1로부터 0.008489998006339 ETH를 송금 받은 것을 확인할 수 있습니다.

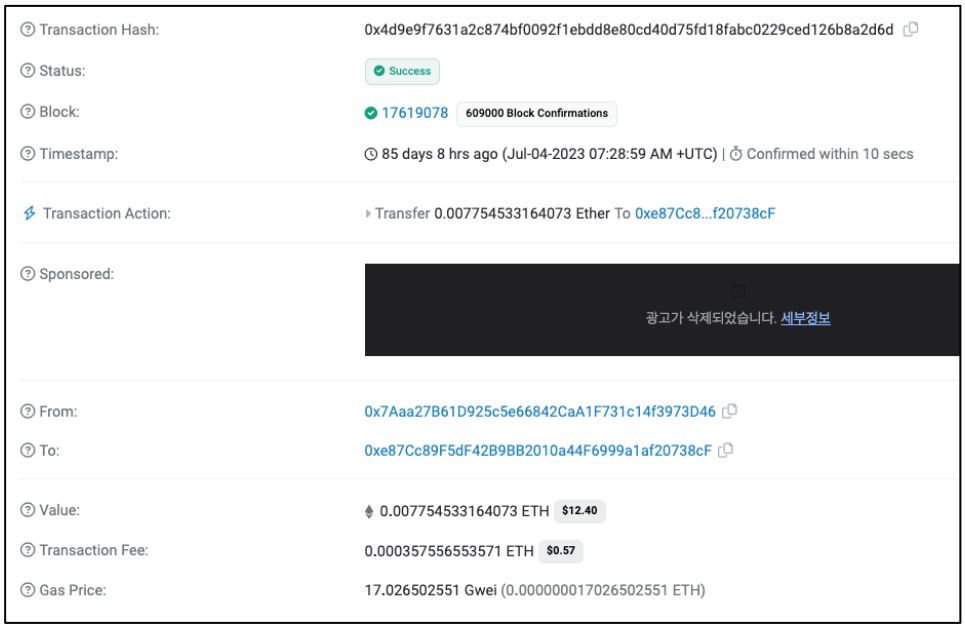
[그림 21] 자금 출처 도식

같은 방식으로 추적을 진행하다 보면 위와 같은 결과를 확인할 수 있었으며 최종적으로 0x4862e147504d9f20fa5f410c4661f91e36b123dc에서 자금을 송금한 것을 알 수 있었습니다. 해당 주소는 Ethermine(0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8)으로 부터 Ethereum을 받았는데, 이는 채굴 커뮤니티로 채굴과 관련된 주소임을 확인할 수 있었습니다.

추가로 7월 31일경 국내 거래소 코인원으로부터 0.0084 ETH를 입금 받은 주소가 추적 대상 지갑에 입금한 0x71cF2e9bc96a8eB52661B5b443E8Bd6B240abb4e에 입금한 기록을 찾을 수 있었으며 이는 동일 인물의 작업으로 유추할 수 있습니다.

따라서, 용의자의 지갑 주소로 자금을 직전에 입금한 사람은 트랜잭션 분석을 통해

0x71cF2e9bc96a8eB52661B5b443E8Bd6B240abb4e임을 알 수 있습니다.



[그림 22] Ethereum이 출금된 트랜잭션

또한, 대상 지갑으로부터 자금을 출금한 주소는 위 그림 상에서 트랜잭션 0x4d9e9f7631a2c874bf0092f1ebdd8e80cd40d75fd18fabc0229ced126b8a2d6d을 통해 0xe87Cc89F5dF42B9BB2010a44F6999a1af20738cF임을 알 수 있었고 0.007754533164073 ETH를 출금하였음을 알 수 있습니다.

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

4번과 같은 방식으로 Etherscan을 이용하여 추적을 진행하였습니다.

그림 23 자금 흐름 분석 결과

추적 대상 지갑인 0x7Aaa27B61D925c5e66842CaA1F731c14f3973D46에서 트랜잭션의 흐름을 타고 분석한 결과 0x8E510474bA2F602f2D27BDdd68C02A85cBbd753c에서 0.005746417068157 ETH를 수령 후 트랜잭션이 더이상 발생하지 않음을 확인할 수 있었습니다.

따라서, final destination은 0x8E510474bA2F602f2D27BDdd68C02A85cBbd753c임을 알 수 있습니다.