



작성자	류나연
분석 일자	2024.05.27-28
작성 일자	2024.05.28
분석 대상	Computer.ad1
문서 버전	3.0
작성자 E-mail	<a href="mailto:01star01ek@gmail.com">01star01ek@gmail.com</a>

0. 목차

1. 문제 .....3

2. 분석 도구 .....3

3. 환경 .....3


4. Write-Up.....4

5. Flag..... 10

6. 별도 첨부 ..... 11

7. Reference ..... 12

### 1. 문제

URL	-
문제 내용	<p>[번역본] (*원본 영문 문제는 별도 첨부에 작성되어 있음)</p> <p>A와 B는 이혼 소송을 진행 중입니다. B는 2022년 5월 초에 구매한 암호화폐도 분할해야 한다고 주장합니다. B의 주장에 따르면 A와 B는 암호화폐를 구매한 후 A의 PC에 설치된 지갑에 보관했습니다. 하지만 A는 암호화폐를 구매하거나 보관한 적이 없다고 주장합니다. B는 A가 사용한 암호화폐 지갑 프로그램과 지갑 파일의 경로, 지갑 주소를 찾기 위해 A의 PC 이미지를 분석해 달라고 요청했습니다. 대상 해시(MD5) Computer.ad1 8fc3335fdd54ddffdbd794f1eaf2ad7</p> <p># UTC+9 시간대를 기준으로 모든 문제를 해결해 주시기 바랍니다.</p> <p>1) 컴퓨터에 설치된 암호화폐 지갑 프로그램의 이름은? (20점)</p> <p>2) 숨겨진 암호화폐 지갑 파일의 전체 경로는? (40점)</p> <p>3) 지갑 주소가 어떻게 되나요? (40점)</p>
문제 파일	 <b>Computer.ad1</b>
문제 유형	디스크 포렌식
난이도	3 / 3

### 2. 분석 도구

도구명	다운로드 링크	Version
FTK imager	<a href="https://go.exterro.com/l/43312/2023-05-03/fc4b78">https://go.exterro.com/l/43312/2023-05-03/fc4b78</a>	4.7.12
INDXParse	<a href="https://github.com/williballenthin/INDXParse">https://github.com/williballenthin/INDXParse</a>	-
HXD	<a href="https://mh-nexus.de/en/hxd/">https://mh-nexus.de/en/hxd/</a>	2.5

### 3. 환경

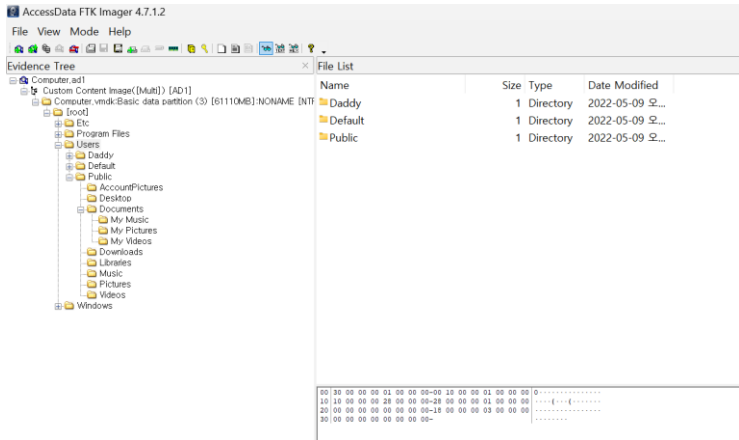
OS
Windows 11 Home

## 4. Write-Up

파일명	Computer.ad1
용량	2.34GB
SHA256	8342633311f5c77023052ccad534eafb8f045991a15fb1b31b9284261c5990b1
Timestamp	2024-05-22 10:02:48

### 1) 컴퓨터에 설치된 암호화폐 지갑 프로그램의 이름은? (20 점)

#### 1. 파일 확인

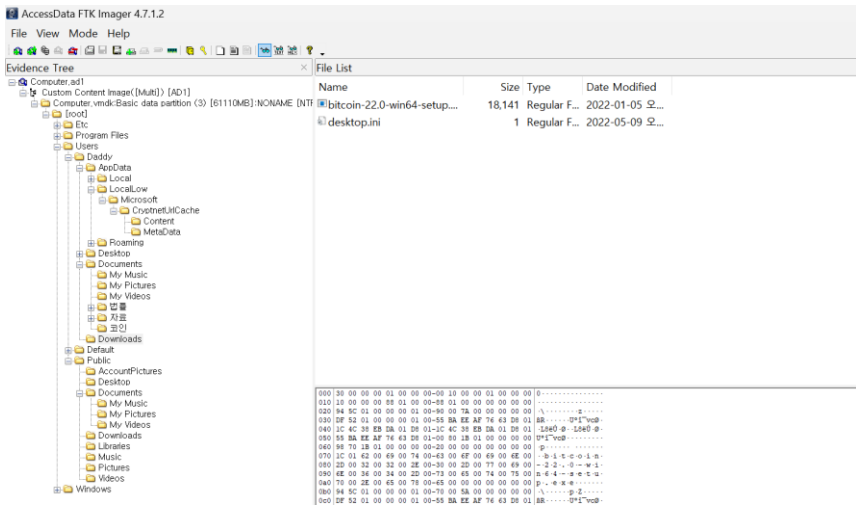


[ 사진 1 ] FTK imager로 열어본 .ad1 파일

먼저 해당 파일을 열기 위해 해당 파일의 확장자를 검색해보았다.

.ad1파일은 디스크 이미지 파일 형식이라고 한다. 따라서 FTK imager를 통해 해당 파일을 열었다.

#### 2. 코인과 관련된 파일, 폴더등의 프로그램 찾기



[ 사진 2 ] bitconin과 관련된 프로그램을 찾은 모습

코인과 관련된 단서를 찾기 위해 여러 폴더들을 이동해가며 찾았다.

Root – program files 에서 딱히 발견할 단서가 없어 Users 에서 각 유저들을 탐색하기 시작했다. 그러던 중 Users – Daddy - Documents 에서 '코인'이라는 폴더명을 발견하였고 이에 따라 Daddy 의 폴더에 집중해 프로그램을 찾게 되었으며 Downloads 안에 bitcoin – 22.0- win64-setup.exe 파일을 발견하게 되었다. 암호화폐 지갑 프로그램이지 발견한 것이다.

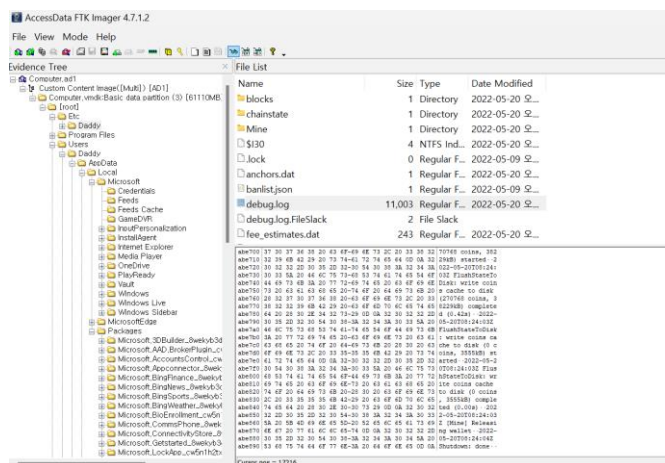
### 3. 프로그램명 정확히 찾기

따라서 프로그램 명은 bitcoin 이라고 생각했는데 답을 확인해보니 틀린 것이다. 이에 따라 다른 writeup 을 참고하였더니 해당 프로그램은 BitCoin Core 라는 프로그램에서 제공하는 설치 프로그램이라고 한다. 구글에 "bitcoin – 22.0"을 검색하면 BitCoin Core 22.0 이 제일 상단에 나온다.

정답은 **BitCoin Core**

## 2) 숨겨진 암호화폐 지갑 파일의 전체 경로는? (40 점)

### 1. 파일 확인



[ 사진 3 ] bitcoin과 관련된 기록을 찾은 모습

해당 프로그램을 사용한 기록을 찾기 위해 탐색하던 중 Users – Daddy 폴더 외에 Etc – Daddy 폴더가 따로 있음을 알게 됐다. 이에 따라 해당 폴더를 탐색하였으며 해당 과정에서 debug.log 파일 내에 coin과 관련된 키워드를 확인하게 되었다. 보기 편하기 위해 해당 파일을 추출하여 메모장을 통해 확인하였다.

## 2. 메모장으로 확인하는 debug.log

```

2022-05-20T08:22:40Z GUI: "registerShutdownBlockReason: Successfully registered: Bitcoin Core가 아직 안전천개 종료되지 않았습니..."
2022-05-20T08:22:40Z Default data directory C:\Users\Daddy\AppData\Roaming\Bitcoin
2022-05-20T08:22:40Z Using data directory C:\Etc\WDaddy
2022-05-20T08:22:40Z Config file: C:\Etc\WDaddy\Bitcoin.conf (not found, skipping)
2022-05-20T08:22:40Z Setting file arg: wallet = ["mine"]
2022-05-20T08:22:40Z Using at most 125 automatic connections (2048 file descriptors available)
2022-05-20T08:22:40Z Using 16 MiB out of 32/2 requested for signature cache, able to store 524288 elements
2022-05-20T08:22:40Z Using 16 MiB out of 32/2 requested for script execution cache, able to store 524288 elements
2022-05-20T08:22:40Z Script verification uses 1 additional threads
2022-05-20T08:22:40Z scheduler thread start
2022-05-20T08:22:40Z Using wallet directory C:\Etc\WDaddy
2022-05-20T08:22:40Z init message: 지갑(들) 검증 중...
2022-05-20T08:22:40Z Using BerkeleyDB version Berkeley DB 4.8.30: (April 9, 2010)
2022-05-20T08:22:40Z Using wallet C:\Etc\WDaddy\Mine\wallet.dat
2022-05-20T08:22:40Z BerkeleyEnvironment::Open: LogDir=C:\Etc\WDaddy\Mine\database ErrorFile=C:\Etc\WDaddy\Mine\debug.log
2022-05-20T08:22:41Z init message: Loading banlist...
2022-05-20T08:22:41Z SetNetworkActive: true
2022-05-20T08:22:41Z Using /16 prefix for IP bucketing
2022-05-20T08:22:41Z Cache configuration:
2022-05-20T08:22:41Z * Using 2.0 MiB for block index database
2022-05-20T08:22:41Z * Using 8.0 MiB for chain state database
2022-05-20T08:22:41Z * Using 440.0 MiB for in-memory UTXO set (plus up to 286.1 MiB of unused mempool space)
2022-05-20T08:22:41Z init message: Loading block index...
2022-05-20T08:22:41Z Switching active chainstate to Chainstate [ibid] @ height -1 (null)
2022-05-20T08:22:41Z Opening LevelDB in C:\Etc\WDaddy\Blocks\index
2022-05-20T08:22:41Z Opened LevelDB successfully
2022-05-20T08:22:41Z Using obfuscation key for C:\Etc\WDaddy\Blocks\index: 0000000000000000
2022-05-20T08:22:45Z LoadBlockIndexDB: last block file = 22
2022-05-20T08:22:45Z LoadBlockIndexDB: last block file info: CBlockFileInfo(blocks=186, size=16678541, heights=196731..197979, time=2012-09-01..2012-09-09)
2022-05-20T08:22:45Z Checking all blk files are present...
2022-05-20T08:22:45Z LoadBlockIndexDB0: Block files have previously been pruned

```

[ 사진 4 ] bitcoin과 관련된 log

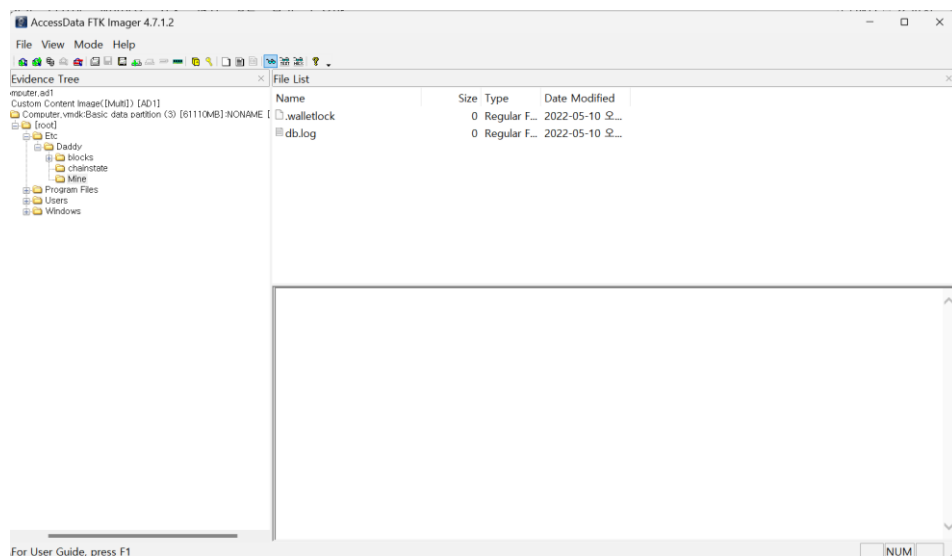
Debug.log 파일을 추출하여 확인하며 bitcoin과 관련된 log들도 확인하게 되었다.

해당 log들 중 2022-05-20T08:22:40Z Setting file arg: wallet = ["Mine"]

2022-05-20T08:22:40Z Using wallet C:\Etc\W\Daddy\W\Mine\wallet.dat를 통해

Mine이 지갑의 이름이며 Mine 폴더 내 wallet.dat 데이터에 기록되고 있음을 확인했다.

### 3. 존재하지 않는 지갑 관련 데이터



[ 사진 5 ] ftk imager로 확인한 Mine 폴더 내의 모습

따라서 해당 경로의 파일들을 확인하였으나 해당 이름의 파일이 존재하지 않음을 알 수 있었다.

## [WHS-2] .iso

즉 파일을 다른 경로에 옮기거나 삭제 했을 거라고 생각하여 관련 정보를 찾아보았다.

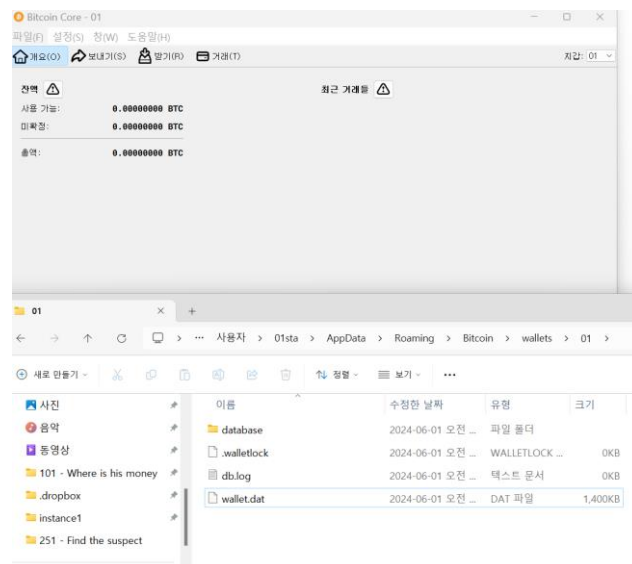
### 4. 사라진 지갑 관련 정보 찾기

```
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ explorer.exe . /
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ explorer.exe .
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ python INDXParse.py -c $130
usage: INDXParse.py [-h] [-c | -b] [-d] [-v] [-t [dir,sh,sql]] filename
INDXParse.py: error: the following arguments are required: filename
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ explorer.exe .
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ python INDXParse.py -c $130
usage: INDXParse.py [-h] [-c | -b] [-d] [-v] [-t [dir,sh,sql]] filename
INDXParse.py: error: the following arguments are required: filename
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ explorer.exe
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$ python INDXParse.py -c 130
FILENAME, PHYSICAL SIZE, LOGICAL SIZE, MODIFIED TIME, ACCESSED TIME, CHANGED TIME, CREATED TIME
/home/dorothy@helix/INDXParse/indxparse/INDXParse.py: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a
future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.fromtimestamp(timestamp, datetime.UTC).
return datetime.datetime.fromtimestamp(float(word) * 1e-7 - 11644473600)
locks, 0, 0, 2022-05-09 07:31:27.575613, 2022-05-09 07:31:27.575613, 2022-05-09 07:31:27.575613, 2022-05-09 07:31:27.575613
anchors.dat, 80, 75, 2022-05-20 08:24:03.319736, 2022-05-20 08:24:03.319736, 2022-05-20 08:24:03.335533, 2022-05-20 08:24:03.319736
banlist.json, 40, 38, 2022-05-09 07:31:27.606607, 2022-05-09 07:31:27.606607, 2022-05-09 07:31:27.606607, 2022-05-09 07:31:27.606607
banlist.json, 40, 38, 2022-05-09 07:31:27.606607, 2022-05-09 07:31:27.606607, 2022-05-09 07:31:27.606607, 2022-05-09 07:31:27.606607
blocks, 0, 0, 2022-05-20 08:23:48.729111, 2022-05-20 08:23:48.729111, 2022-05-20 08:23:48.729111, 2022-05-09 07:31:27.566723
chainstate, 0, 0, 2022-05-20 08:24:03.802013, 2022-05-20 08:24:03.802013, 2022-05-20 08:24:03.802013, 2022-05-09 07:31:27.619629
chainstate, 0, 0, 2022-05-20 08:24:03.802013, 2022-05-20 08:24:03.802013, 2022-05-20 08:24:03.802013, 2022-05-09 07:31:27.619629
debug.log, 11268996, 11268996, 2022-05-20 08:24:05.095819, 2022-05-09 07:31:27.581568, 2022-05-20 08:24:05.095819, 2022-05-09 07:31:27.581568
fee_estimates.dat, 249856, 249856, 2022-05-20 08:24:03.335533, 2022-05-09 07:31:37.418798, 2022-05-20 08:24:03.335533, 2022-05-09 07:31:37.418798
fee_estimates.dat, 249856, 249856, 2022-05-20 08:24:03.335533, 2022-05-09 07:31:37.418798, 2022-05-20 08:24:03.335533, 2022-05-09 07:31:37.418798
LOCK=1, 0, 0, 2022-05-09 07:31:27.575613, 2022-05-09 07:31:27.575613, 2022-05-09 07:31:27.575613, 2022-05-09 07:31:27.575613
mempool.dat, 24, 18, 2022-05-20 08:24:03.335533, 2022-05-20 08:24:03.335533, 2022-05-20 08:24:03.335533, 2022-05-20 08:24:03.335533
mine, 0, 0, 2022-05-20 08:24:07.425885, 2022-05-20 08:24:07.425885, 2022-05-20 08:24:07.425885, 2022-05-18 00:04:13.354080
peers.dat, 692112, 691542, 2022-05-20 08:24:02.787886, 2022-05-20 08:24:02.768301, 2022-05-20 08:24:03.319736, 2022-05-20 08:24:02.768301
settings.json, 48, 46, 2022-05-20 08:22:36.317812, 2022-05-20 08:22:36.317812, 2022-05-20 08:22:36.317812, 2022-05-20 08:22:36.317812
SETTINGS=1, 48, 46, 2022-05-20 08:22:36.317812, 2022-05-20 08:22:36.317812, 2022-05-20 08:22:36.317812, 2022-05-20 08:22:36.317812
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$
(base) dorothy@helixlocalhost:~/INDXParse/indxparse$
```

[ 사진 6 ] INDXParse를 이용해 확인해본 \$130 파일

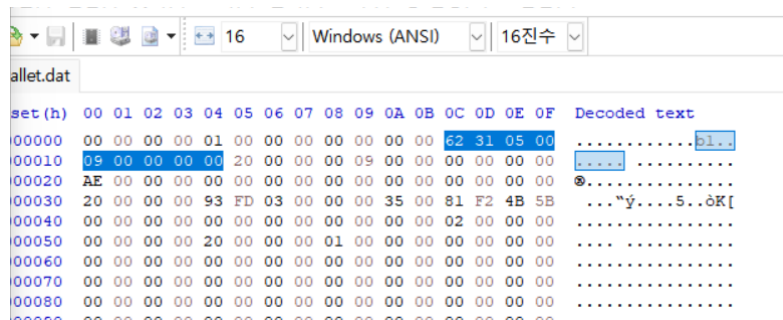
사라진 지갑 관련 데이터를 찾기 위해 \$130 파일을 파싱해서 확인해보거나 여러 개의 .dat 파일을 확인해보는 등 다양한 방법으로 시도해보았다. 그러나 해당 과정에서 유의미한 결과를 찾지 못하였다. 따라서 차라리 bitcoin.core를 직접 깔아보고 이에 대해 파악한 후 답을 찾아야 겠다 싶어 bitcoin.core 앱에 대해 이해하는 시간을 가졌다.

### 5. BitCoin Core 설치 및 실행



[ 사진 7 ] 직접 설치해본 bitCoin Core

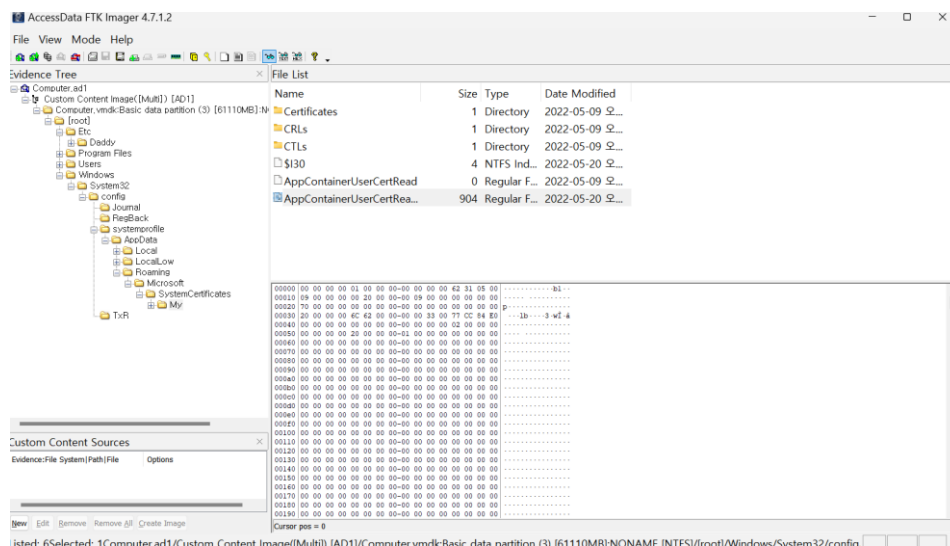
동일한 버전의 프로그램을 찾아 설치해보았다.



**[ 사진 8 ] Wallet.dat 파일 메타데이터 확인**

이를 통해 wallet.dat 파일을 확인할 수 있었으며 HXD를 통해 메타데이터를 확인하였다. 해당 유형의 파일은 62 31 05 00 09 00 00 00 00 00 를 형식으로 가졌다. 이를 통해 해당 유형의 파일을 파악했다.

## 6. 탐색을 통한 같은 메타데이터 파일 찾기



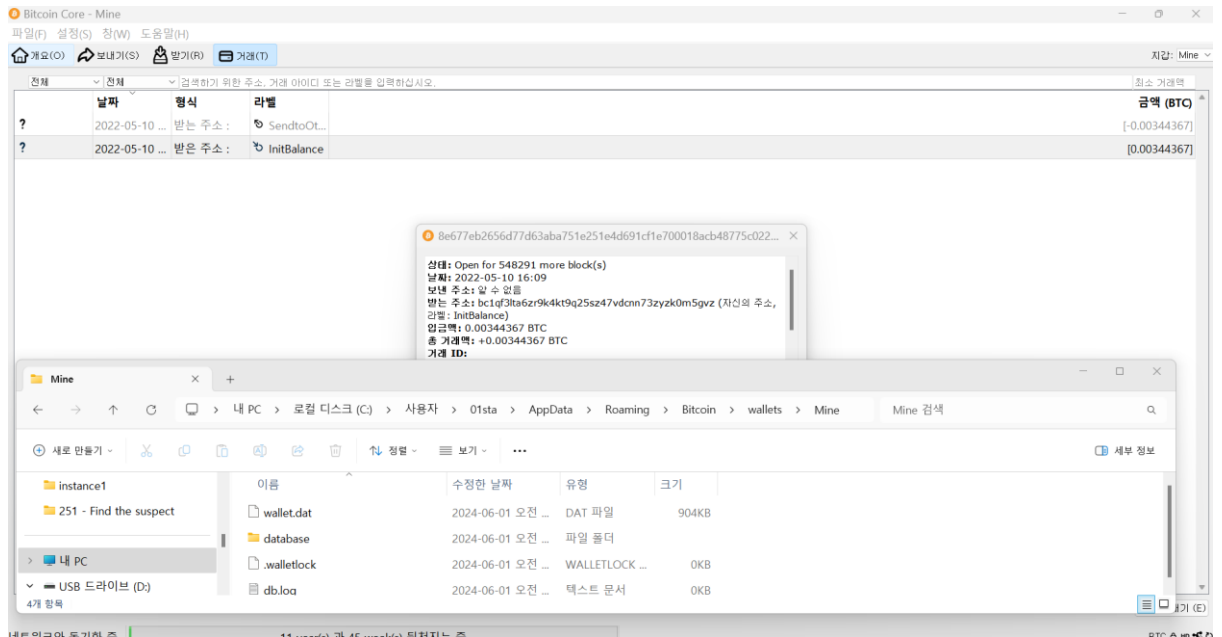
[ 사진 9 ] 찾은 wlllet.dat과 같은 메타데이터를 가지고 있는 파일

추후 다른분들의 writeup을 확인해보니 autospy나 다른 툴들을 이용하거나 다른 코드를 확인하여 해당 경로에 특이점이 있음을 알아내어 이 파일을 식별했다고 한다. 필자의 경우에는 하나하나 메타데이터의 파일들을 확인하며 이를 찾아내었다. (굉장히 비효율적인 것 같다.)

## 7. 해당 파일 실행해보기



## [WHS-2] .iso



### [ 사진 10 ] 해당 파일을 wllet.dat으로 변경후 bitCoinCore를 통해 실행해보기

해당 파일을 ftk imager를 통해 추출하고 이를 wallet.dat으로 변경해준 뒤 정해진 형식에 맞춰 Mine 폴더를 새로 만들어 안에 넣어주었다. 이를 Bitcoin Core 지갑 열기로 열 수 있었으며 이는 문제에서 요구한 wallet.dat 이 맞아보였다. 따라서 정답은

**Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\SystemCertificate\My\MyAppContainerUserCertRead.sys**

### 3) 지갑 주소가 어떻게 되나요? (40점)

거래 확인을 통해 내 지갑의 주소를 볼 수 있었다.

**bc1qf3lta6zr9k4kt9q25sz47vdcnn73zyzk0m5gvz (자신의 주소, 라벨: InitBalance)**

## 5. Flag

- 1. BitCoin Core
- 2.

Windows\WSystem32\Wconfig\systemprofile\AppData\Roaming\Microsoft\SystemCertificates\My\AppDataContainerUser\CertRead.sys

- 3. bc1qf3lta6zr9k4kt9q25sz47vdcnn73zyzk0m5gvz

## 6. 별도 첨부

- 원본 영문 문제

A and B are in the process of filing for divorce. B argues that the cryptocurrencies purchased in early May 2022 must also be divided. According to B's claim, A and B bought cryptocurrencies and then stored them in a wallet installed on A's PC. However, A claims that he has never purchased or stored cryptocurrency. B asked you to analyze A's PC image to find the cryptocurrency wallet program used by A, the path of the wallet file, and the wallet address.

Target	Hash (MD5)
Computer.ad1	8fc3335fdd54ddfffd794f1eaf2ad7

### Questions

# Please solve all problems based on UTC+9 time zone.

- 1) What is the name of the cryptocurrency wallet program installed on the computer? (20 points)
- 2) What is the full path of the hidden cryptocurrency wallet file? (40 points)
- 3) What is the 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).
-

## 7. Reference

- BitCoin Core  
<https://bitcoin.org/en/bitcoin-core/>