

## 101 – Where is his money?

### Team Information

Team Name : ISEGYE\_IDOL

Team Member : Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address : dfc-isegyeidol@googlegroups.com

### Instructions

**Description** 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	8fc3335fdd54ddffdbd794f1eaf2ad7

### 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).

#### Tools used:

Name:	FTK Imager	Publisher:	AccessData® FTK® Imager
Version:	4.7.1.2		
URL:	<a href="https://accessdata.com/product-download/ftk-imager-version-4-5">https://accessdata.com/product-download/ftk-imager-version-4-5</a>		

Name:	REGA	Publisher:	DFRC, Korea Univ
Version:	1.5.3.0		
URL:	<a href="http://forensic.korea.ac.kr/tools.html">http://forensic.korea.ac.kr/tools.html</a>		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0 (x86-64)		
URL:	<a href="https://mh-nexus.de/en/hxd/">https://mh-nexus.de/en/hxd/</a>		

Name:	JumpListView	Publisher:	Nirsoft
Version:	1.16		
URL:	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>		

#### Analysis PC used:

OS:	Windows 11 Pro	Version:	10.0.22000 build 2000
-----	----------------	----------	-----------------------

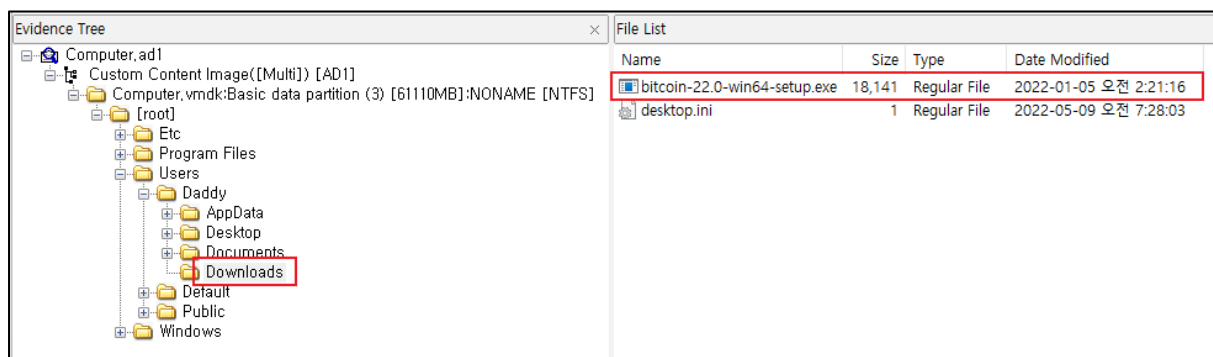
System  
Name:

DESKTOP-RN5F5V6

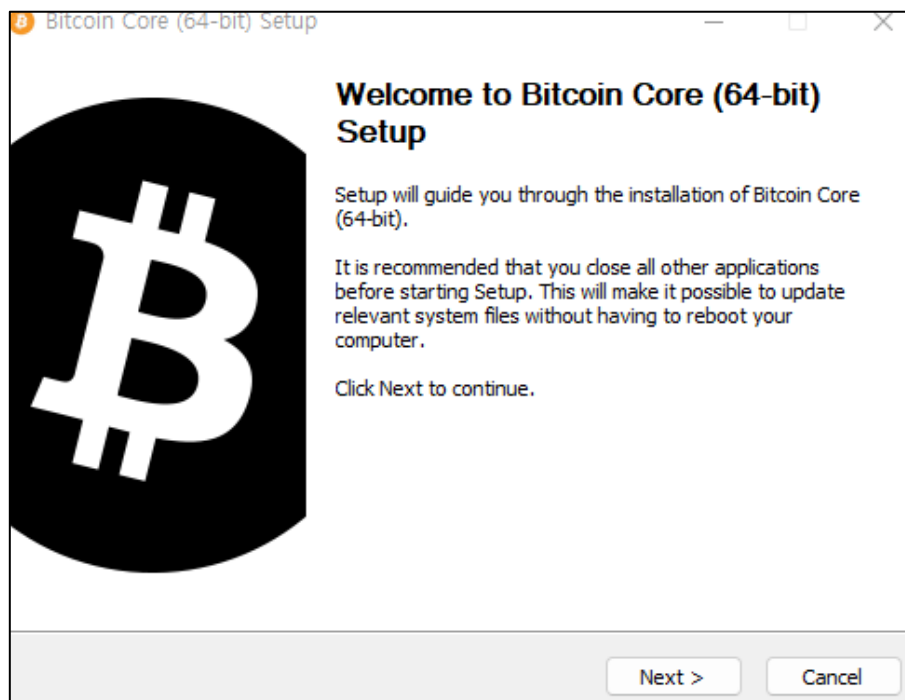
## Step-by-step methodology:

- 1) What is the name of the cryptocurrency wallet program installed on the computer?

Daddy User 폴더 하위 다운로드 폴더에 bitcoin-22.0-win64-setup.exe가 존재한다. 분석 PC에서 위 파일을 실행해보니 Bitcoin Core (64bit) 지갑의 설치 프로그램이다.



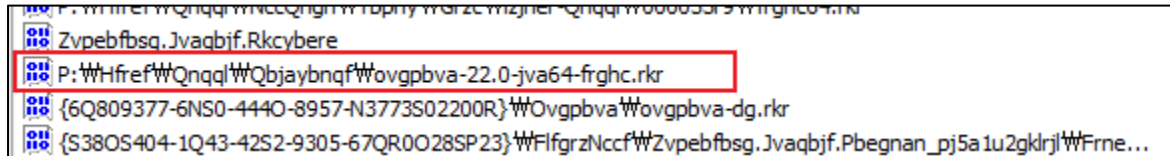
[그림 1] Daddy User의 다운로드 폴더 내 비트코인 코어 설치 파일 (FTK Imager)



[그림 2] Bitcoin-Core (64-bit) 설치 프로그램

- 설치 흔적 (UserAssist)

대상자 PC에서 지갑 설치 프로그램의 실행 여부를 확인하기 위해, UserAssist<sup>1</sup>를 분석하여 최근 실행한 응용 프로그램의 정보(파일명, 실행 횟수, 마지막 실행 시간)을 확인하였다. UserAssist의 Rot13 인코딩 방식을 해석한 결과, 다운로드 폴더에 존재하던 Bitcoin Core (64bit) 설치 프로그램의 파일명이 키 값으로 존재함을 확인하였다.

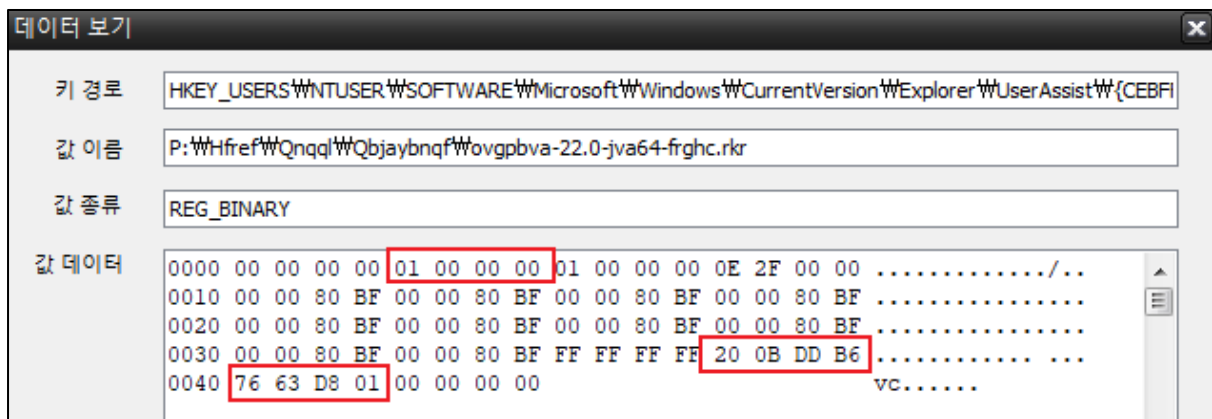


[그림 3] NTUSER 하위 UserAssist 키 값에 존재하는 Bitcoin Core 설치 프로그램 (REGA)

Rot13 디코딩 전	P:WHfrefWQnqqlWQbjaybnqfWovgpbva-22.0-jva64-frghc.rkr
Rot13 디코딩 후	C:\Users\Daddy\Downloads\bitcoin-22.0-win64-setup.exe

[표 1] UserAssist 키 값의 Rot13 디코딩 전후 비교

UserAssist 키의 [C:\Users\Daddy\Downloads\bitcoin-22.0-win64-setup.exe] 데이터에서 응용 프로그램 실행 횟수(Offset 0x04 ~ 0x07)는 **1번**이며, 마지막 실행 시간(Offset 0x60 ~ 0x67)은 **2022-05-09 오후 4:30:53 (KST)**이다.



[그림 4] UserAssist 키의 Bitcoin core 설치 프로그램의 데이터 (REGA)

<sup>1</sup> HKEY\_USERS\NTUSER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}

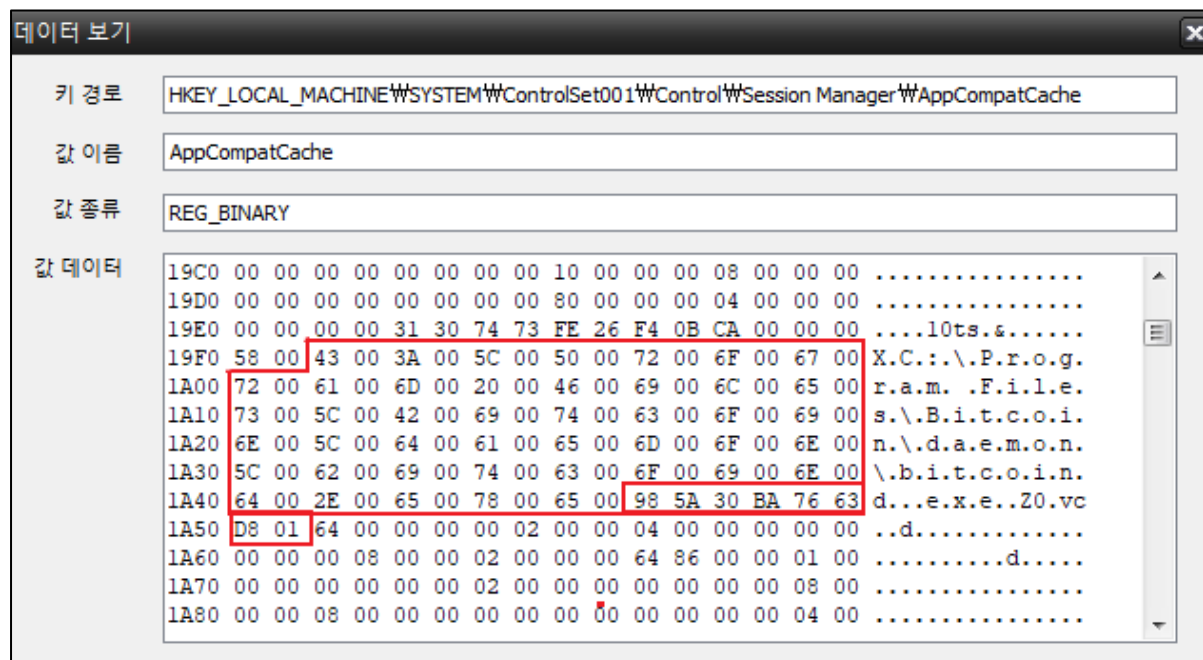
- 설치 흔적(Shim Cache)

응용 프로그램을 설치하면 일반적으로 설치되는 표준 경로인 [Program Files] 디렉터리에 Bitcoin Core 지갑 프로그램 흔적을 Shim Cache에서 발견하였다. Shim Cache<sup>2</sup> 내부에 “Bitcoin” 키워드 검색이 6건 확인(Keyword Hit)되었으며, 모든 결과는 [C:\Program Files\Bitcoin\] 하위 파일임을 확인하였다.

Num	Offset	Path Value	Last Modified Time
1	0x1956	C:\Program Files\Bitcoin\daemon\bitcoin-cli.exe	2022-05-09 PM 4:30:59 (KST)
2	0x1A32	C:\Program Files\Bitcoin\daemon\bitcoind.exe	2022-05-09 PM 4:30:58 (KST)
3	0x1B08	C:\Program Files\Bitcoin\daemon\bitcoin-wallet.exe	2022-05-09 PM 4:30:59 (KST)
4	0x1BEA	C:\Program Files\Bitcoin\daemon\bitcoin-tx.exe	2022-05-09 PM 4:30:59 (KST)
5	0x3BB4	C:\Program Files\Bitcoin\bitcoin-qt.exe	2022-05-09 PM 4:30:58 (KST)
6	0x4EE4	C:\Users\Daddy\Downloads\bitcoin-22.0-win64-setup.exe	2022-01-05 AM 11:21:16 (KST)

[표 2] Shim Cache 중 Bitcoin 키워드 검색 결과 정리

Shim Cache인 AppCompatCache 키 데이터 중 “Bitcoin” 키워드 검색 결과 예시는 [그림 5]와 같다. 파일 경로(Offset 0x19F2 ~ 0x1A49)는 [C:\Program Files\Bitcoin\daemon\bitcoind.exe]이며, 마지막 수정 시간(Offset 0x1A4A ~ 0x1A51)은 **2022-05-09 오후 4:30:58 (KST)**이다.



<sup>2</sup> HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache

[그림 5] Shim Cache(AppCompatCache) 내부 (REGA)

따라서 대상자는 **2022-05-09 오후 4:30:53 (KST)**에 다운로드 폴더에 존재하는 **Bitcoin Core (64bit) 지갑** 설치 프로그램을 실행하였으며, UsrAssist와 Shim Cache 아티팩트로부터 Bitcoin Core 지갑 프로그램이 설치되었음을 확인하였다.

2) What is the full path of the hidden cryptocurrency wallet file? (40 points)

C 드라이브 하위 [Etc] 디렉터리에 Bitcoin Core 지갑의 흔적이 존재한다. 그 중 Debug.log은 Bitcoin core 지갑 프로그램의 디버깅 로그로서, 대상자의 프로그램 활동 이력을 기록하는 파일이다. Debug.log 파일 내 마지막으로 기록된 로그는 프로그램 종료(Shutdown: done)이며, 활동 시간은 **2022-05-20 오후 5:24:04 (KST)**이다.

```
2022-05-20T08:24:03Z Writing 0 unbroadcast transactions to disk.
2022-05-20T08:24:03Z Dumped mempool: 0s to copy, 0s to dump
2022-05-20T08:24:03Z FlushStateToDisk: write coins cache to disk (270768 coins, 38229kB) started
2022-05-20T08:24:03Z FlushStateToDisk: write coins cache to disk (270768 coins, 38229kB) completed (0.42s)
2022-05-20T08:24:03Z FlushStateToDisk: write coins cache to disk (0 coins, 3555kB) started
2022-05-20T08:24:03Z FlushStateToDisk: write coins cache to disk (0 coins, 3555kB) completed (0.00s)
2022-05-20T08:24:03Z [Mine] Releasing wallet
2022-05-20T08:24:04Z Shutdown: done
```

[그림 6] [etc] 디렉터리 하위 Debug.log 파일

지갑 프로그램을 종료하고 40초 뒤인 **2022-05-20 오후 5:24:47 (KST)**에 대상자는 [System32] 하위 [My] 디렉터리에 접근한 것을 Jumplist에서 확인하였다. Jumplist는 대상자가 최근에 접근한 폴더를 파악할 수 있는데, [System32]는 윈도우 32bit용 시스템 파일을 보관하는 용도로서 일반 사용자가 접근하기 쉽지 않으며, 동시에 접근 시간대가 지갑 프로그램을 종료한 시점과 유사한 것으로 보아 [My] 디렉터리를 살펴볼 필요성이 있다.

JumpListsView		
File Edit View Options Help		
Filename	Full Path	Record Time
My	C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\SystemCertificates\My	2022-05-20 오후 5:24:47
법률	C:\Users\Daddy\Documents\법률	2022-05-16 오후 8:12:47
합의이혼	C:\Users\Daddy\Documents\법률\합의이혼	2022-05-16 오후 8:12:47
자료	C:\Users\Daddy\Documents\자료	2022-05-16 오후 8:12:26
최종	C:\Users\Daddy\Documents\자료\최종	2022-05-16 오후 8:12:28

[그림 7] Jumplist 목록 (JumpListsView)

[C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\SystemCertificates\My] 경로에 가면, [그림 8]과 같이 [AppContainerUserCerRead] 파일명을 지닌 파일이 2개가 존재한다.

Name	Size	Type	Date Modified
Certificates	1	Directory	2022-05-09 오전 7:28:55
CRLs	1	Directory	2022-05-09 오전 7:28:55
CTLs	1	Directory	2022-05-09 오전 7:28:55
\$I30	4	NTFS Index...	2022-05-20 오전 8:25:03
AppContainerUserCertRead	0	Regular File	2022-05-09 오전 7:28:55
AppContainerUserCertRead.sys	904	Regular File	2022-05-20 오전 8:24:03

[그림 8] 2개의 AppContainerUserCerRead 파일

“sys” 확장자가 붙은 AppContainerUserRead의 데이터를 분석한 결과, Bitcoin Core 지갑임을 확인하였다. 실제로 분석 PC의 지갑과 비교 분석하여 AppContainerUserRead.sys 파일은 Bitcoin core 지갑 파일(이하 wallet.dat)의 헤더 시그니처와 동일하였다.

AppContainerUserCertRead.sys		904	Regular File	2022-05-20 오전 8:24:03
00000	00 00 00 00 01 00 00 00-00 00 00 00 62 31 05 00	.....b1..		
00010	09 00 00 00 00 00 20 00 00-00 09 00 00 00 00 00	.....		
00020	70 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	p.....		
00030	20 00 00 00 00 6C 62 00 00-00 00 33 00 77 CC 84 E0	...lb...3-wI-à		
00040	00 00 00 00 00 00 00 00 00-00 00 00 00 02 00 00	.....		
00050	00 00 00 00 00 20 00 00 00-01 00 00 00 00 00 00	.....		

[그림 9] AppContainerUserCerRead.sys (FTK Imager)




Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	00	00	00	00	01	00	00	00	00	00	00	00	62	31	05	00	.....b1..
00000010	09	00	00	00	00	20	00	00	00	09	00	00	00	00	00	00	.....
00000020	70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	p.....
00000030	20	00	00	00	6C	62	00	00	00	00	33	00	77	CC	84	E0	...lb....3.wl,,à
00000040	00	00	00	00	00	00	00	00	00	00	00	00	02	00	00	00	.....
00000050	00	00	00	00	20	00	00	00	01	00	00	00	00	00	00	00	....

[그림 10] 분석 PC에서의 Bitcoin core의 wallet.dat (HxD)

따라서 대상자는  
 [C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\SystemCertificates\My\AppContainerUserCerRead.sys] 경로에 Bitcoin Core 지갑을 숨겨두었다.

### 3) What is the wallet address? (40 points)

분석 PC의 Bitcoin core 프로그램에 [AppContainerUserCerRead.sys]를 [wallet.dat]로 파일명을 변경하여 지갑 복구를 시도해보니 정상적으로 프로그램에서 열렸다. 최근 거래 내역에 2개의 거래가 발견되었으며, **2022-05-11 오전 01:09 (KST)**에 초기 자본(InitBalance)을 받고, **2022-05-11 오전 06:14 (KST)**에 다른 주소로 BTC를 보냈다.

최근 거래들 		
	2022-05-10 21:14 SendtoOther	<span style="color: red;">[-0.00344367 BTC]</span>
	2022-05-10 16:09 InitBalance	<span style="color: green;">[+0.00344367 BTC]</span>

[그림 11] AppContainerUserCerRead.sys의 최근 거래 내역

#### ● 첫번째 거래 (First Transaction)

대상자 PC 내 지갑 주소는 [bc1qf3lta6zr9k4kt9q25sz47vdcnn73zyzk0m5gvz]로서, 초기 자본으로 **0.00344367 BTC**를 받았으며, 2022-05-11 오전 01:09 (KST)에 거래가 이루어졌다.

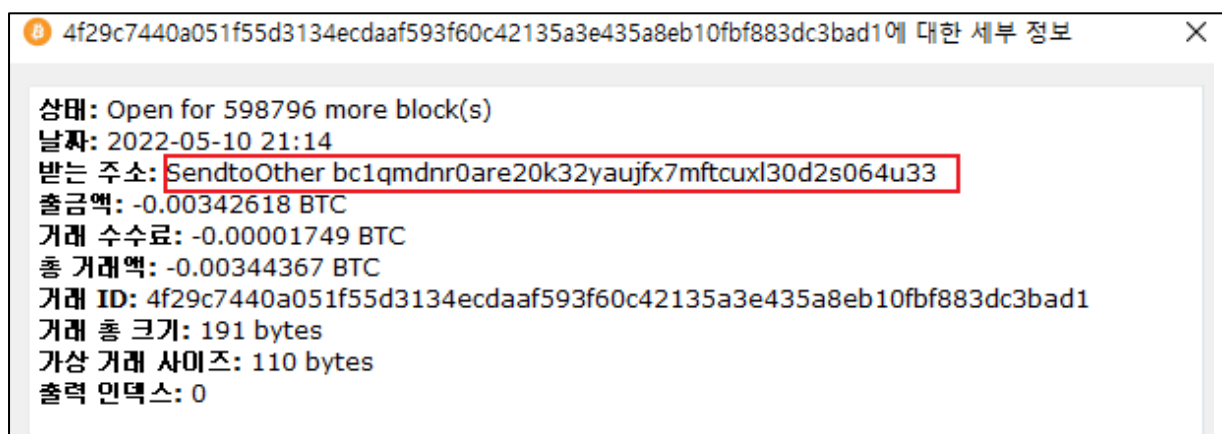




[그림 12] AppContainerUserCerRead.sys의 첫번째 거래 세부 정보

- 두번째 거래 (Second Transaction)

첫번째 거래에서 받았던 대상자 PC 내 지갑 초기 자본에서 **0.00342618 BTC**를 다른 지갑 주소 **[bc1qmdnr0are20k32yaujfx7mftcuxl30d2s064u33]**로 보냈다. 해당 거래는 2022-05-11 오전 06:14 (KST)에 이루어졌다.



[그림 13] AppContainerUserCerRead.sys의 두번째 거래 세부 정보

따라서 대상자 PC 내 지갑을 분석 PC의 Bitcoin Core 프로그램에서 복구해낸 결과, 지갑에서 두 번의 거래를 확인하였고, 사용된 주소를 정리한 표는 다음과 같다.

Num	Address
1	bc1qf3lta6zr9k4kt9q25sz47vdcnn73zyzk0m5gvz (대상자 지갑)
2	bc1qmdnr0are20k32yaujfx7mftcuxl30d2s064u33 (다른 지갑)

[표 3] 지갑 내 Transaction에 사용된 Address 정리