2023 Digital Forensic Challenge Tech Contest

Advanced Tool Development for Investigating Forensic Artifacts on the latest version of MacOS

MacDonald

Park Woobeen, Kim Minsoo, Park Ah-hyun, Joo Dabin

qkrdnqls30@dgu.ac.kr

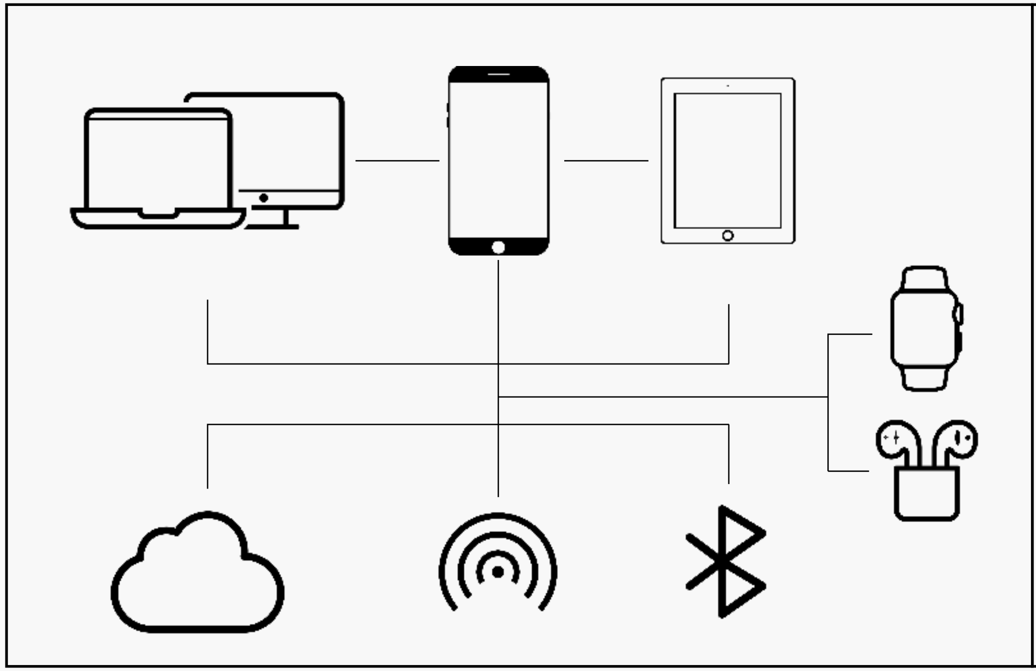
Table of Contents

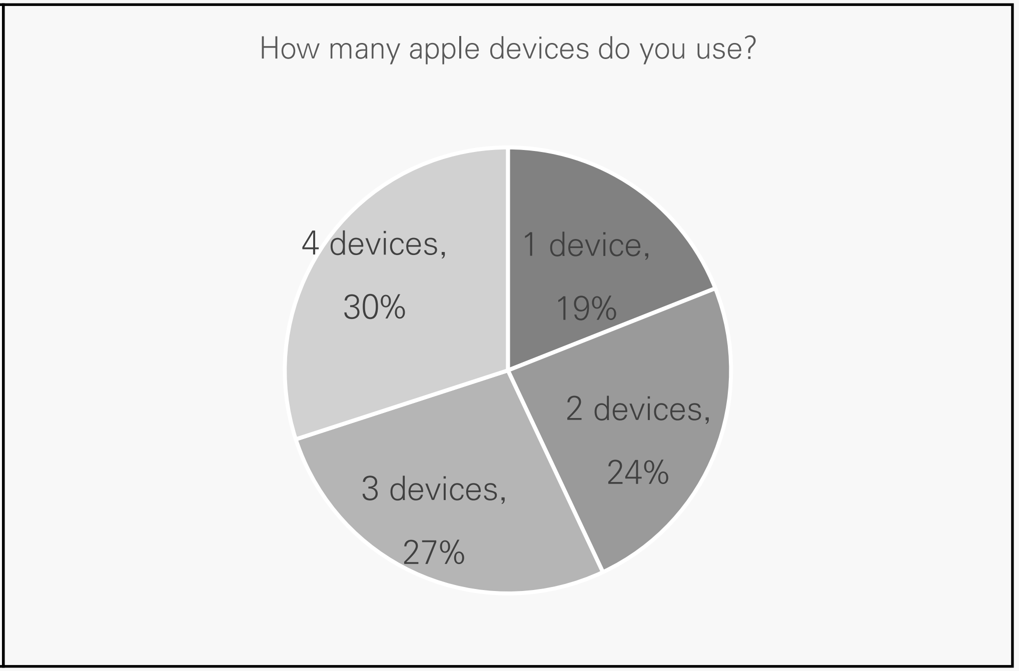
1. Introduction
2. Related Works
3. MacOS Artifacts
4. Tool Explanation
5. Conclusion

1. Introduction

1. Introduction

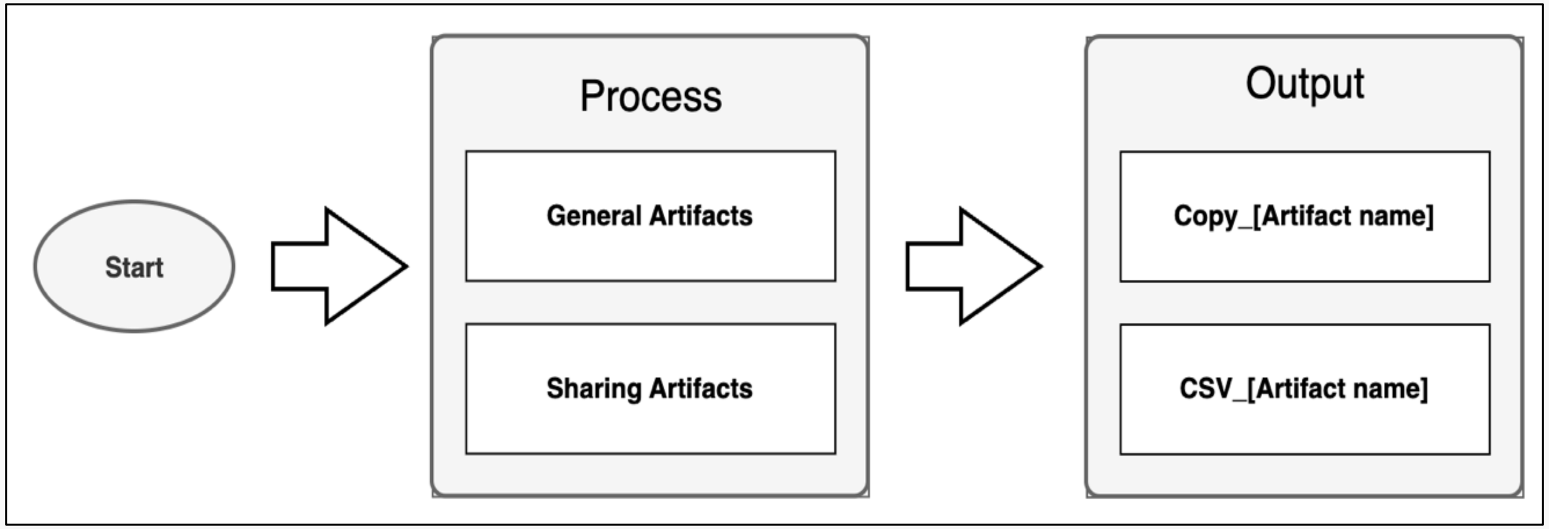
- MacOS has the second-highest OS market share worldwide
- Nearly 60% of Apple customers own 3 to 4 devices (CIRP statistics)
- Marketing focus on 'Apple Ecosystem' and emphasis on device interconnectivity
- Increased file transfer convenience vs. potential for expanded data leakage paths





1. Introduction

- Inadequate data extraction for inter-device connectivity by current forensic tools
- Challenges in collecting active MacOS artifacts and meaningful analysis in MacOS Ventura
  - We focused on investigating the artifacts by active MacOS forensics, particularly on the interconnectivity between Apple devices and the analysis of artifacts related to file sharing.



2. Related Works

① Background

- MacOS
  - Unix-based OS released by Apple
  - APFS2 filesystem
  - Encrypts disk using ‘FileVault’ after MacOS High Sierra(10.13) version
    - ✓ difficult to apply traditional forensic method to image encrypted disk using hardware imaging too
- Two ways to analyze MacOS device
  - Acquiring software image
    - ✓ <u>only possible through commercial software</u>
    - ✓ Test with FTK imager released by Exterro
      - ➢ <u>Impossible to image disk in the latest MacOS version</u>
  - <u>Live forensic</u>

② MacOS Forensic Tools

Tool	Features
Belkasoft X	• A forensic tool from Belkasoft, capable of computer, mobile, and cloud forensics. • Distributed in executable file format: Not usable on active MacOS systems.
Carbon Copy Cloner	• A MacOS-specific backup and disk cloning tool developed by Bombich Software. • Only offers restoration and cloning functions • Closer to a tool for artifact collection than for analysis in terms of artifact forensics.
Recon ITR	• A MacOS-specific imaging and analysis solution developed by SUMURI. • Offers the ability to select the necessary artifacts for analysis. • In the demo version of the tool have confirmed that it fails to extract artifacts properly.

Recon ITR(Contacts)

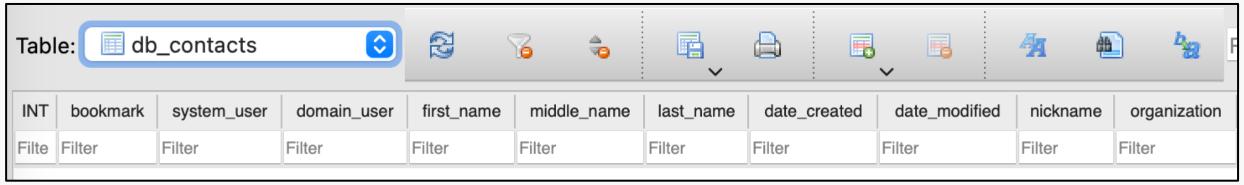
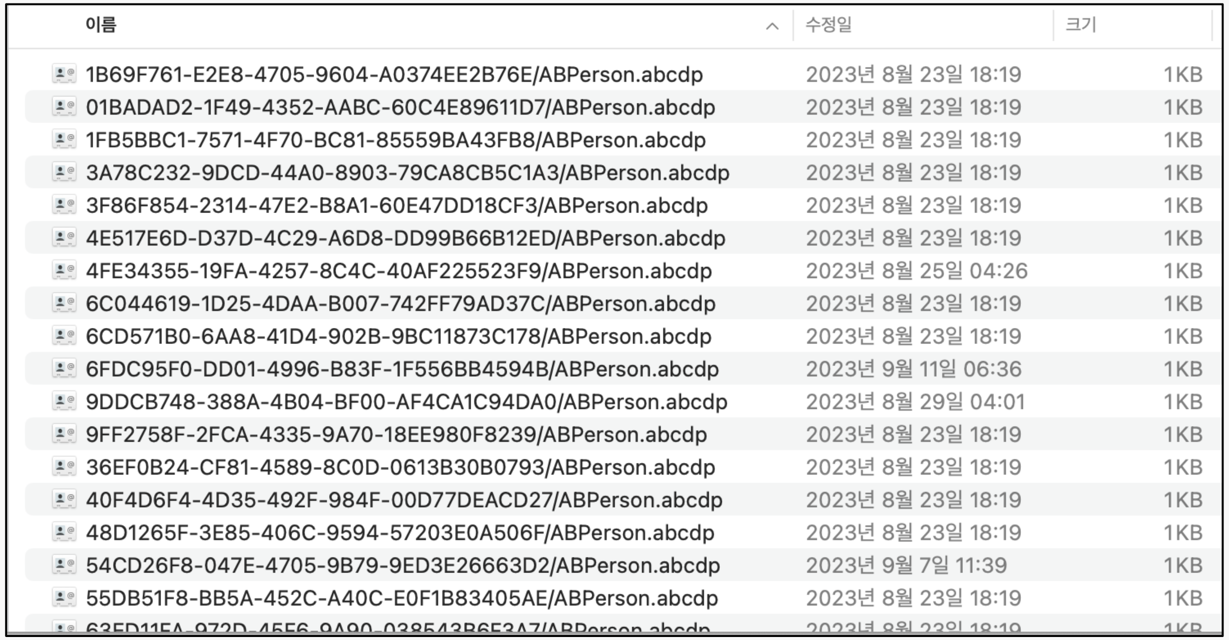


Table: db_contacts

INT	bookmark	system_user	domain_user	first_name	middle_name	last_name	date_created	date_modified	nickname	organization
Filte	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

Tool output file(Contacts) : no records



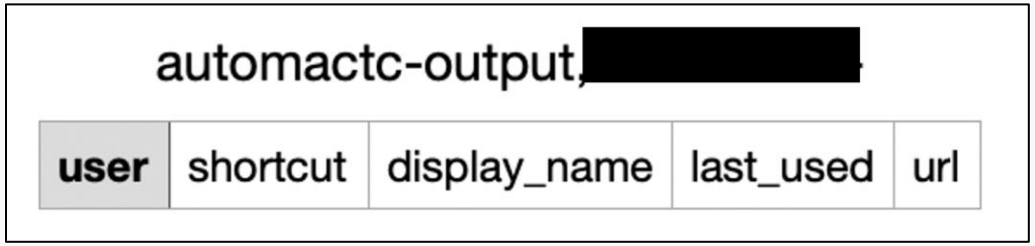
이름	수정일	크기
1B69F761-E2E8-4705-9604-A0374EE2B76E/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
01BADAD2-1F49-4352-AABC-60C4E89611D7/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
1FB5BBC1-7571-4F70-BC81-85559BA43FB8/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
3A78C232-9DCD-44A0-8903-79CA8CB5C1A3/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
3F86F854-2314-47E2-B8A1-60E47DD18CF3/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
4E517E6D-D37D-4C29-A6D8-DD99B66B12ED/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
4FE34355-19FA-4257-8C4C-40AF225523F9/ABPerson.abcdp	2023년 8월 25일 04:26	1KB
6C044619-1D25-4DAA-B007-742FF79AD37C/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
6CD571B0-6AA8-41D4-902B-9BC11873C178/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
6FDC95F0-DD01-4996-B83F-1F556BB4594B/ABPerson.abcdp	2023년 9월 11일 06:36	1KB
9DDCB748-388A-4B04-BF00-AF4CA1C94DA0/ABPerson.abcdp	2023년 8월 29일 04:01	1KB
9FF2758F-2FCA-4335-9A70-18EE980F8239/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
36EF0B24-CF81-4589-8C0D-0613B30B0793/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
40F4D6F4-4D35-492F-984F-00D77DEACD27/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
48D1265F-3E85-406C-9594-57203E0A506F/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
54CD26F8-047E-4705-9B79-9ED3E26663D2/ABPerson.abcdp	2023년 9월 7일 11:39	1KB
55DB51F8-BB5A-452C-A40C-E0F1B83405AE/ABPerson.abcdp	2023년 8월 23일 18:19	1KB
63FD11FA-972D-45E6-9A90-038543B6F3A7/ABPerson.abcdp	2023년 8월 23일 18:19	1KB

Actual contacts folder

② MacOS Forensic Tools

Open source Tool	Features
Autopsy (The SleuthKit)	• A free open-source forensic platform by BasisTech • A Windows-based desktop digital forensic tool. • It also supports Linux and Mac OSX. • It is limited to Mac OSX, no other version of MacOS.
AutoMacTC	• Capable of parsing various artifacts including install history, bash command history, event taps, etc. • Unable to obtain records for Airdrop, Bluetooth, zsh command history, etc. • For terminal state, outputs fewer records than the number of commands entered, questioning the tool's reliability.
Mac_apt	• A new version was released on June 17, 2023, and it handles many artifacts, showing the highest performance among the tested tools. • Permission-related errors occur ("permission denied"), limiting the ability to parse all content properly.

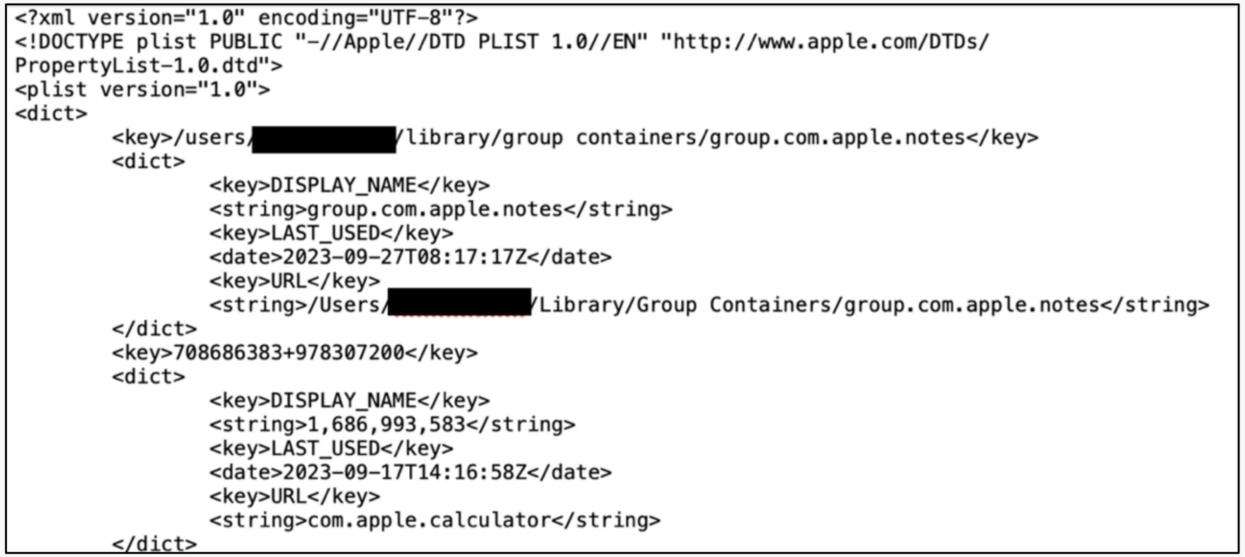
AutoMacTC(Spotlight)



automactc-output[redacted]

user	shortcut	display_name	last_used	url

Tool output file(Spotlight) : no records



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>/users/[redacted]/library/group containers/group.com.apple.notes</key>
        <dict>
                <key>DISPLAY_NAME</key>
                <string>group.com.apple.notes</string>
                <key>LAST_USED</key>
                <date>2023-09-27T08:17:17Z</date>
                <key>URL</key>
                <string>/Users/[redacted]/Library/Group Containers/group.com.apple.notes</string>
        </dict>
        <key>708686383+978307200</key>
        <dict>
                <key>DISPLAY_NAME</key>
                <string>1,686,993,583</string>
                <key>LAST_USED</key>
                <date>2023-09-17T14:16:58Z</date>
                <key>URL</key>
                <string>com.apple.calculator</string>
        </dict>
```

Actual Spotlight file

3. MacOS Artifacts

3. MacOS Artifacts

- In this study, we focused on Apple's device interconnectivity but also considered general artifacts (like web browser history)
- So, We developed a tool by including artifacts as sharing artifacts and general artifacts.
    - Mac Sharing Artifacts
        - ✓ Airdrop, Bluetooth, iCloud, iDevice Backup, Calendar, Call history, …
    - General Artifacts
        - ✓ Login history, Terminal history(bash, zsh), Web browser history, …

3. MacOS Artifacts

Type	Target Artifact	Acquirable data	Update status
Sharing artifacts	Bluetooth	Information from devices connected to your MacBook via Bluetooth.	O
	Calendar	Event information stored in Calendar (date, event name, email and phone number of the person you're sharing with, attachments, etc.)	O
	Call History	Contact times, phone numbers	O
	Contact	Contact information (name, phone number, workplace, etc.)	O
	Download Files	Source of downloaded files (Airdrop, social media, web browser, etc.)	O
	iCloud	user's iCloud account	△
	iDevice Backup	Settings of the backed up iDevice	△
	Notes	Notes content	△
	Photos	Photos stored in Photos (including photos from the linked iDevice)	O
General artifacts	Login window	Account login information for users accessing from a single Mac	O
	Spotlight history	Keywords, times, applications, and more that users have searched for using Spotlight.	X
	Terminal history	Commands entered through the zsh and bash shells.	X
	Web browser	URLs visited or files downloaded through Safari or Chrome.	X

- 'Target Artifact' and 'Acquirable data' which can be analyzed through the developed tool
- 'Updated status' which indicates whether the tool was improved, compared to the existing tools by marking O, △ or X.
  - O: Artifacts which not has been analyzed by existing tools
  - △: Artifacts which has been analyzed by existing tools, but not currently working
  - X: Artifacts which has been analyzed by existing tools and currently working

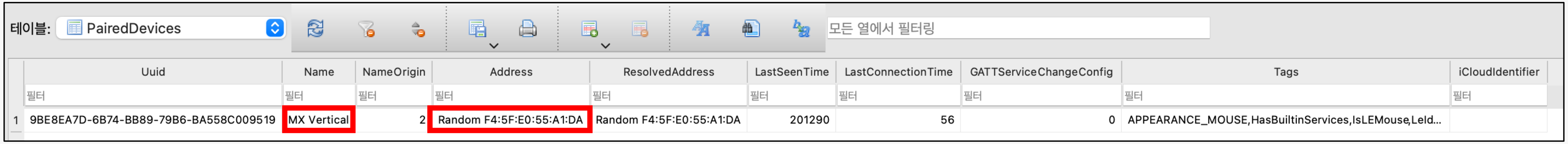
① Target Artifacts Path

Type	Artifact	Path
Sharing Artifacts	Bluetooth	/Library/Bluetooth/com.apple.MobileBluetooth.ledevices.paired.db /Library/Bluetooth/Library/Preferences/com.apple.MobileBluetooth.devices.plist
	Calendar	/Users/[UserName]/Library/Calendars/Calendar.sqlitedb
	Call History	/Users/[UserName]/Library/ApplicationSupport/CallHistoryDB/CallHistory.storedata
	Contact	/Users/[UserName]/Library/Application Support/AddressBook/Sources/〈GUID〉/Metadata/*
	Download Files	/Users/[UserName]/Downloads
	iCloud	/Users/[UserName]/Library/Preferences/MobileMeAccounts.plist
	iDevice Backup	%%users.homedir%%/Library/Application Support/MobileSync/Backup/*/info.plist
	Notes	/Users/UserName/Library/Group Containers/group.com.apple.notes/NoteStore.sqlite
	Photos	/Users/[UserName]/Pictures/Photos Library.photosLibrary/originals/[0~F]/*
General Artifacts	Login window	/Library/Preference/com.apple.loginwindow.plist
	Spotlight history	/Users/[UserName]/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
	Terminal history	/Users/[UserName]/.bash_history /Users/[UserName]/.zsh_history
	Web browser	• Safari /Users/[Username]/Library/Safari/History.db /Users/[Username]/Library/Safari/Download.plist • Chrome /Users/woobeenpark/Library/Application Support/Google/Chrome/Default/History

② Mac Sharing Artifacts

Bluetooth

- Bluetooth with a variety of peripherals and accessories
  - Bluetooth headphones, speaker, wireless keyboards, mouse, trackpad, printer and mobile (Continuity and Handoff)
    - ✓ Continuity and Handoff : function to switch between iOS devices to MacOS devices and performs ongoing tasks, or to use the features of iOS devices such as Facetime and Message via iPhone with MacOS devices
  - History of other devices being Bluetooth-connected in :
    - ✓ /Library/Bluetooth/com.apple.MobileBluetooth.ledevices.paired.db
    - ✓ Existing tool(Mac_apt) do not refer to data on this path

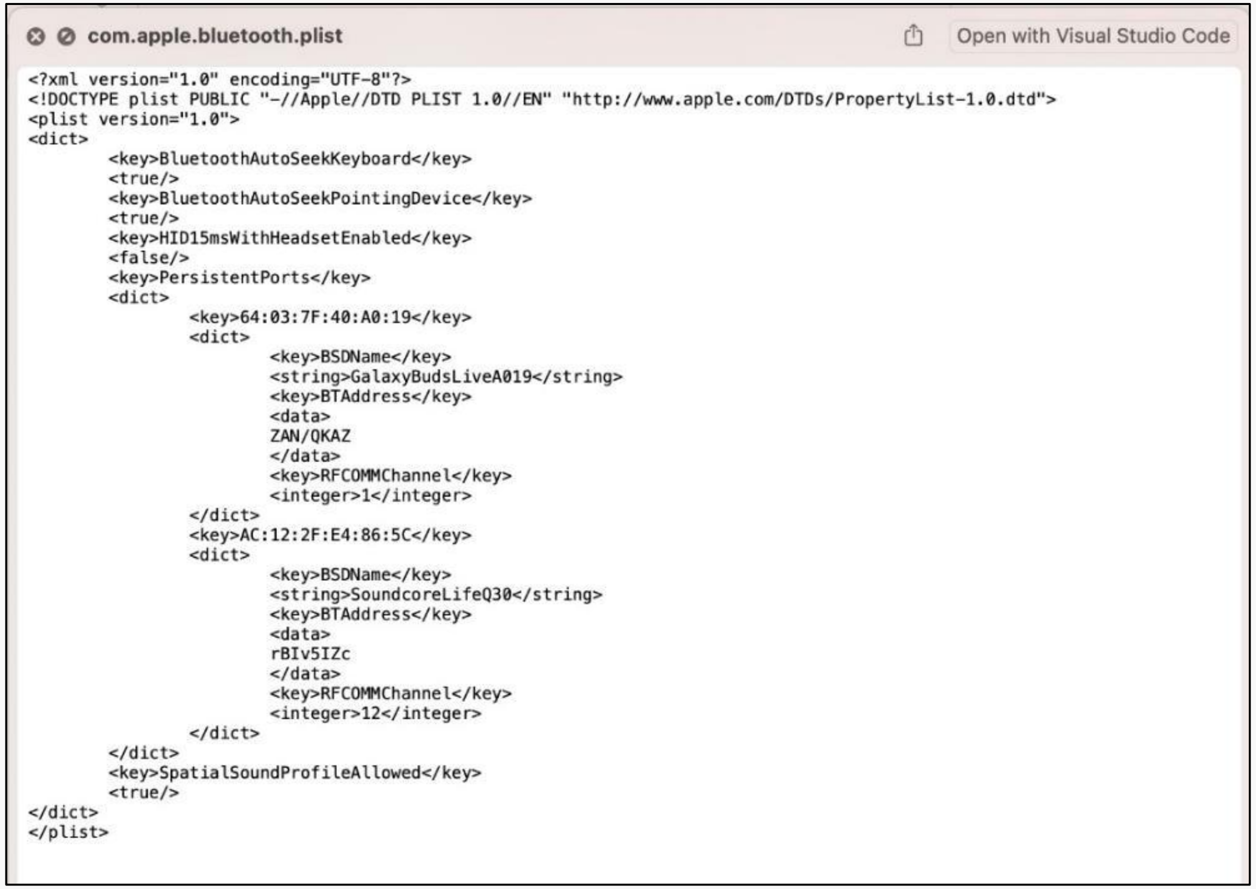


	Uuid	Name	NameOrigin	Address	ResolvedAddress	LastSeenTime	LastConnectionTime	GATTServiceChangeConfig	Tags	iCloudIdentifier
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	9BE8EA7D-6B74-BB89-79B6-BA558C009519	MX Vertical	2	Random F4:5F:E0:55:A1:DA	Random F4:5F:E0:55:A1:DA	201290	56	0	APPEARANCE_MOUSE,HasBuiltinServices,IsLEMouse,LeId...	

② Mac Sharing Artifacts

Bluetooth

- History of other devices being Bluetooth-connected in :
  - /Library/Bluetooth/Library/Preferences/com.apple.MobileBluetooth.devices.plist

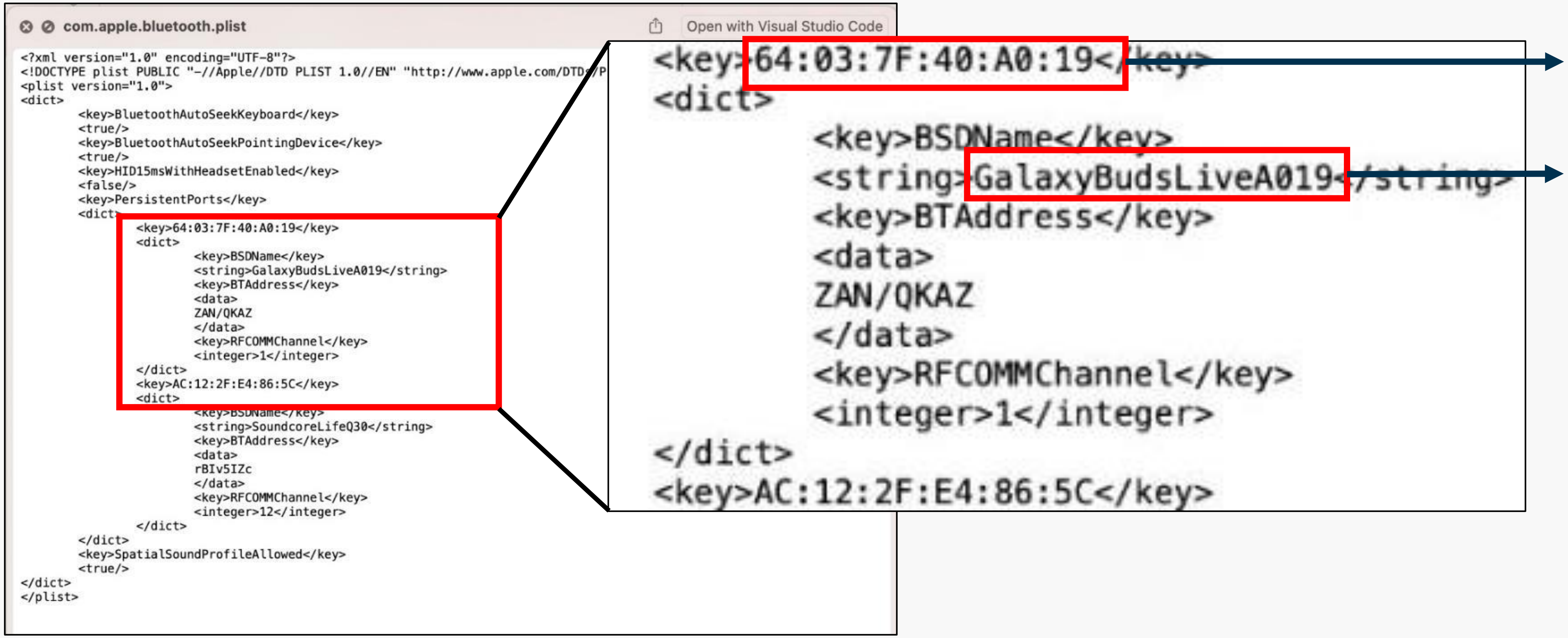


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>BluetoothAutoSeekKeyboard</key>
	<true/>
	<key>BluetoothAutoSeekPointingDevice</key>
	<true/>
	<key>HID15msWithHeadsetEnabled</key>
	<false/>
	<key>PersistentPorts</key>
	<dict>
		<key>64:03:7F:40:A0:19</key>
		<dict>
			<key>BSDName</key>
			<string>GalaxyBudsLiveA019</string>
			<key>BTAddress</key>
			<data>
			ZAN/QKAZ
			</data>
			<key>RFCOMMChannel</key>
			<integer>1</integer>
		</dict>
		<key>AC:12:2F:E4:86:5C</key>
		<dict>
			<key>BSDName</key>
			<string>SoundcoreLifeQ30</string>
			<key>BTAddress</key>
			<data>
			rBIv5IZc
			</data>
			<key>RFCOMMChannel</key>
			<integer>12</integer>
		</dict>
	</dict>
	<key>SpatialSoundProfileAllowed</key>
	<true/>
</dict>
</plist>
```

② Mac Sharing Artifacts

Bluetooth

- History of other devices being Bluetooth-connected in :
  - /Library/Bluetooth/Library/Preferences/com.apple.MobileBluetooth.devices.plist



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/P
<plist version="1.0">
<dict>
        <key>BluetoothAutoSeekKeyboard</key>
        <true/>
        <key>BluetoothAutoSeekPointingDevice</key>
        <true/>
        <key>HID15msWithHeadsetEnabled</key>
        <false/>
        <key>PersistentPorts</key>
        <dict>
                <key>64:03:7F:40:A0:19</key>
                <dict>
                        <key>BSDName</key>
                        <string>GalaxyBudsLiveA019</string>
                        <key>BTAddress</key>
                        <data>
                        ZAN/QKAZ
                        </data>
                        <key>RFCOMMChannel</key>
                        <integer>1</integer>
                </dict>
                <key>AC:12:2F:E4:86:5C</key>
                <dict>
                        <key>BSDName</key>
                        <string>SoundcoreLifeQ30</string>
                        <key>BTAddress</key>
                        <data>
                        rBIv5IZc
                        </data>
                        <key>RFCOMMChannel</key>
                        <integer>12</integer>
                </dict>
        </dict>
        <key>SpatialSoundProfileAllowed</key>
        <true/>
</dict>
</plist>
```

```
<key>64:03:7F:40:A0:19</key>
<dict>
        <key>BSDName</key>
        <string>GalaxyBudsLiveA019</string>
        <key>BTAddress</key>
        <data>
        ZAN/QKAZ
        </data>
        <key>RFCOMMChannel</key>
        <integer>1</integer>
</dict>
<key>AC:12:2F:E4:86:5C</key>
```

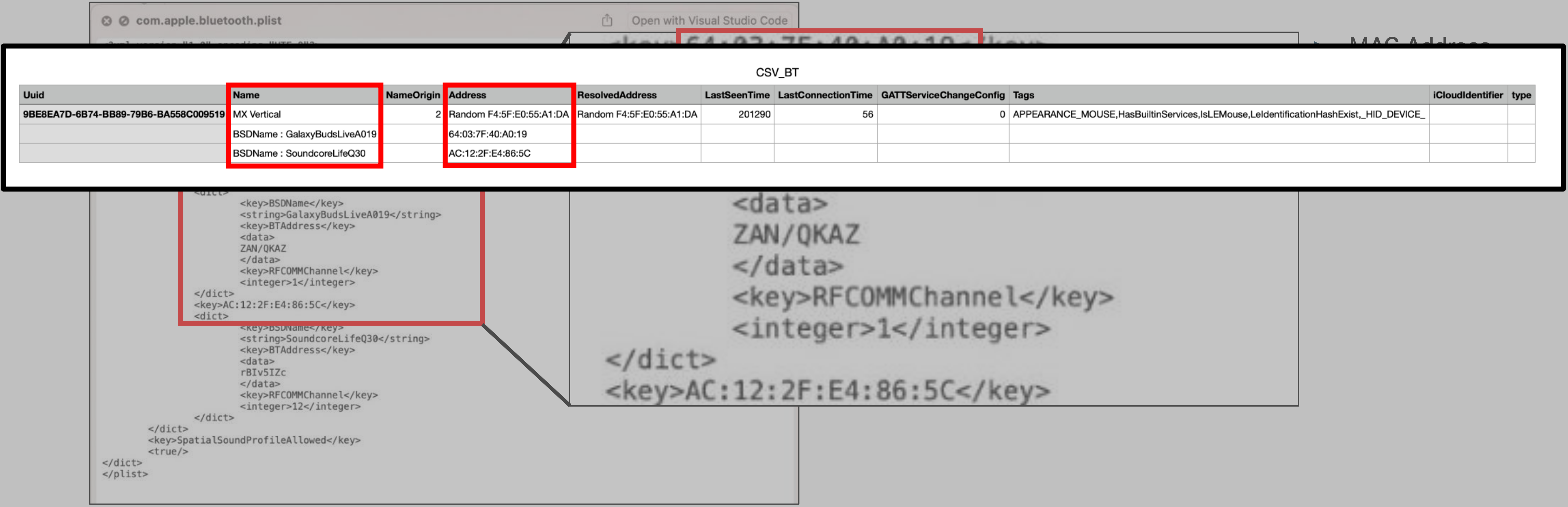
MAC Address

Device Name

② Mac Sharing Artifacts

Bluetooth

- History of other devices being Bluetooth-connected in :
  - /Library/Bluetooth/Library/Preferences/com.apple.MobileBluetooth.devices.plist



CSV_BT

Uuid	Name	NameOrigin	Address	ResolvedAddress	LastSeenTime	LastConnectionTime	GATTServiceChangeConfig	Tags	iCloudIdentifier	type
9BE8EA7D-6B74-BB89-79B6-BA558C009519	MX Vertical	2	Random F4:5F:E0:55:A1:DA	Random F4:5F:E0:55:A1:DA	201290	56	0	APPEARANCE_MOUSE,HasBuiltinServices,IsLEMouse,LeIdentificationHashExist,_HID_DEVICE_		
	BSDName : GalaxyBudsLiveA019		64:03:7F:40:A0:19							
	BSDName : SoundcoreLifeQ30		AC:12:2F:E4:86:5C							

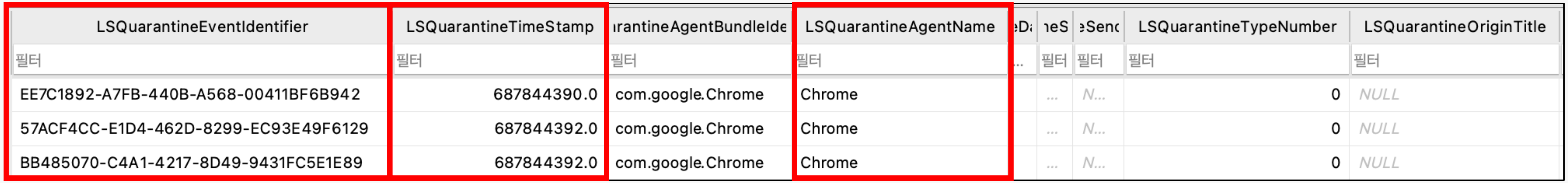
```
<dict>
        <key>BSDName</key>
        <string>GalaxyBudsLiveA019</string>
        <key>BTAddress</key>
        <data>
        ZAN/QKAZ
        </data>
        <key>RFCOMMChannel</key>
        <integer>1</integer>
</dict>
<key>AC:12:2F:E4:86:5C</key>
<dict>
        <key>BSDName</key>
        <string>SoundcoreLifeQ30</string>
        <key>BTAddress</key>
        <data>
        rBIv5IZc
        </data>
        <key>RFCOMMChannel</key>
        <integer>12</integer>
</dict>
    </dict>
    <key>SpatialSoundProfileAllowed</key>
    <true/>
</dict>
</plist>
```

```
        <data>
        ZAN/QKAZ
        </data>
        <key>RFCOMMChannel</key>
        <integer>1</integer>
</dict>
<key>AC:12:2F:E4:86:5C</key>
```

② Mac Sharing Artifacts

Download files (Airdrop, SNS, Web browser, …)

- MacOS devices use a three-pronged security approach to protect against malware
- Files downloaded from unauthorized sources, such as the Internet, are quarantined for check
  - Stores information about these files in 'com.apple.LaunchServices.QuarantineEvents.V2'
  - Existing tools simply extracted the DB file for output -> it is hard to understand the records
    - ✓ 'LSQurantineEventIdentifier' and 'LSQurantineTimeStamp' need to change data to check respectively filename and time.



LSQuarantineEventIdentifier	LSQuarantineTimeStamp	ıırantineAgentBundleIde	LSQuarantineAgentName	eDa	ıeS	eSenc	LSQuarantineTypeNumber	LSQuarantineOriginTitle
필터	필터	필터	필터	...	필터	필터	필터	필터
EE7C1892-A7FB-440B-A568-00411BF6B942	687844390.0	com.google.Chrome	Chrome		...	N...	0	NULL
57ACF4CC-E1D4-462D-8299-EC93E49F6129	687844392.0	com.google.Chrome	Chrome		...	N...	0	NULL
BB485070-C4A1-4217-8D49-9431FC5E1E89	687844392.0	com.google.Chrome	Chrome		...	N...	0	NULL

UUID

Unix Timestamp

Download Agent Name

② Mac Sharing Artifacts

Download files (Airdrop, SNS, Web browser, ···)

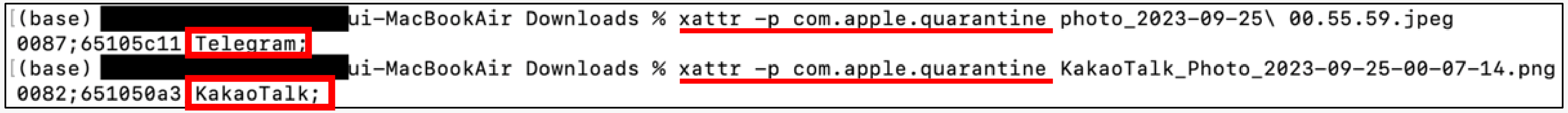
- MacOS devices use a three-pronged security approach to protect against malware
- Files downloaded from unauthorized sources, such as the Internet, are quarantined for check
  - Records are categorized by UUID –> A single record cannot be mapped to the actual filename
  - We found that we can get the values in the database, including the file's UUID from the **data on the downloaded file itself by searching the com.apple.quarantine property.**
    - ✓ Checked the download source in com.apple.quarantine, kMDItemWhereFroms by using 'xattr' command in the download folder

```
'xattr –p [property name] [filename]'
```

② Mac Sharing Artifacts

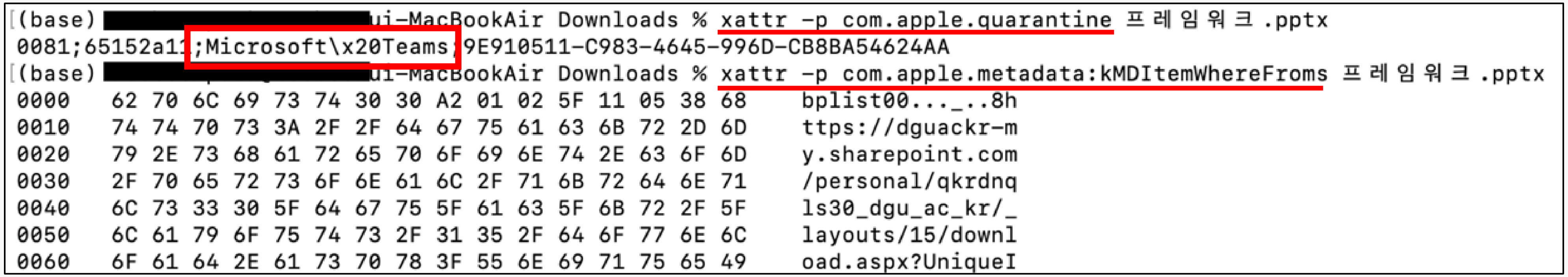
Download files (Airdrop, SNS, Web browser, …)

- For Social Network Service applications (Kakaotalk, Telegram, Teams)
  - In case of Kakaotalk, Telegram, download source can be found in com.apple.quarantine



```
(base) [redacted]ui-MacBookAir Downloads % xattr -p com.apple.quarantine photo_2023-09-25\ 00.55.59.jpeg
0087;65105c11;Telegram;
(base) [redacted]ui-MacBookAir Downloads % xattr -p com.apple.quarantine KakaoTalk_Photo_2023-09-25-00-07-14.png
0082;651050a3;KakaoTalk;
```

  - In case of Teams, source can be found in com.apple.quarantine, and urls, in kMDItemWhereFroms.

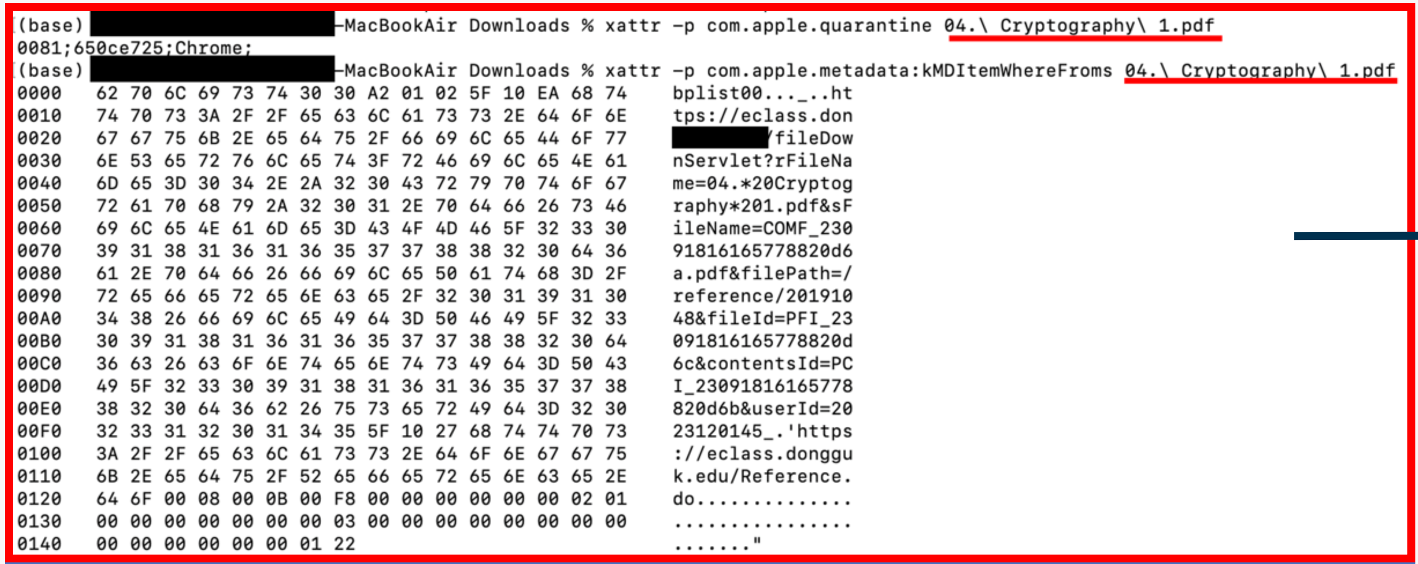


```
(base) [redacted]ui-MacBookAir Downloads % xattr -p com.apple.quarantine 프레임워크.pptx
0081;65152a11;Microsoft\x20Teams;9E910511-C983-4645-996D-CB8BA54624AA
(base) [redacted]ui-MacBookAir Downloads % xattr -p com.apple.metadata:kMDItemWhereFroms 프레임워크.pptx
0000   62 70 6C 69 73 74 30 30 A2 01 02 5F 11 05 38 68    bplist00..._..8h
0010   74 74 70 73 3A 2F 2F 64 67 75 61 63 6B 72 2D 6D    ttps://dguackr-m
0020   79 2E 73 68 61 72 65 70 6F 69 6E 74 2E 63 6F 6D    y.sharepoint.com
0030   2F 70 65 72 73 6F 6E 61 6C 2F 71 6B 72 64 6E 71    /personal/qkrdnq
0040   6C 73 33 30 5F 64 67 75 5F 61 63 5F 6B 72 2F 5F    ls30_dgu_ac_kr/_
0050   6C 61 79 6F 75 74 73 2F 31 35 2F 64 6F 77 6E 6C    layouts/15/downl
0060   6F 61 64 2E 61 73 70 78 3F 55 6E 69 71 75 65 49    oad.aspx?UniqueI
```

② Mac Sharing Artifacts

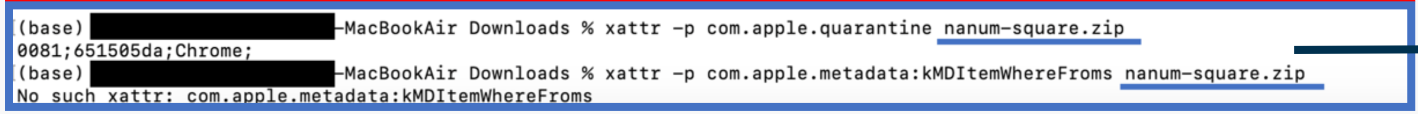
Download files (Airdrop, SNS, Web browser, …)

- For files downloaded from web browser, web browser names are left in the com.apple.quarantine, but in case of kMDItemWhereFroms, some files did not leave the download urls.
    - Found that files downloaded in secret mode of chrome do not leave kMDItemWhereFroms.



```
(base) [redacted]-MacBookAir Downloads % xattr -p com.apple.quarantine 04.\ Cryptography\ 1.pdf
0081;650ce725;Chrome;
(base) [redacted]-MacBookAir Downloads % xattr -p com.apple.metadata:kMDItemWhereFroms 04.\ Cryptography\ 1.pdf
0000   62 70 6C 69 73 74 30 30 A2 01 02 5F 10 EA 68 74    bplist00..._..ht
0010   74 70 73 3A 2F 2F 65 63 6C 61 73 73 2E 64 6F 6E    tps://eclass.don
0020   67 67 75 6B 2E 65 64 75 2F 66 69 6C 65 44 6F 77    [redacted]/fileDow
0030   6E 53 65 72 76 6C 65 74 3F 72 46 69 6C 65 4E 61    nServlet?rFileNa
0040   6D 65 3D 30 34 2E 2A 32 30 43 72 79 70 74 6F 67    me=04.*20Cryptog
0050   72 61 70 68 79 2A 32 30 31 2E 70 64 66 26 73 46    raphy*201.pdf&sF
0060   69 6C 65 4E 61 6D 65 3D 43 4F 4D 46 5F 32 33 30    ileName=COMF_230
0070   39 31 38 31 36 31 36 35 37 37 38 38 32 30 64 36    91816165778820d6
0080   61 2E 70 64 66 26 66 69 6C 65 50 61 74 68 3D 2F    a.pdf&filePath=/
0090   72 65 66 65 72 65 6E 63 65 2F 32 30 31 39 31 30    reference/201910
00A0   34 38 26 66 69 6C 65 49 64 3D 50 46 49 5F 32 33    48&fileId=PFI_23
00B0   30 39 31 38 31 36 31 36 35 37 37 38 38 32 30 64    091816165778820d
00C0   36 63 26 63 6F 6E 74 65 6E 74 73 49 64 3D 50 43    6c&contentsId=PC
00D0   49 5F 32 33 30 39 31 38 31 36 31 36 35 37 37 38    I_23091816165778
00E0   38 32 30 64 36 62 26 75 73 65 72 49 64 3D 32 30    820d6b&userId=20
00F0   32 33 31 32 30 31 34 35 5F 10 27 68 74 74 70 73    23120145_.'https
0100   3A 2F 2F 65 63 6C 61 73 73 2E 64 6F 6E 67 67 75    ://eclass.donggu
0110   6B 2E 65 64 75 2F 52 65 66 65 72 65 6E 63 65 2E    k.edu/Reference.
0120   64 6F 00 08 00 0B 00 F8 00 00 00 00 00 00 02 01    do..............
0130   00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00    ................
0140   00 00 00 00 00 00 01 22                            ......."
```

Chrome download



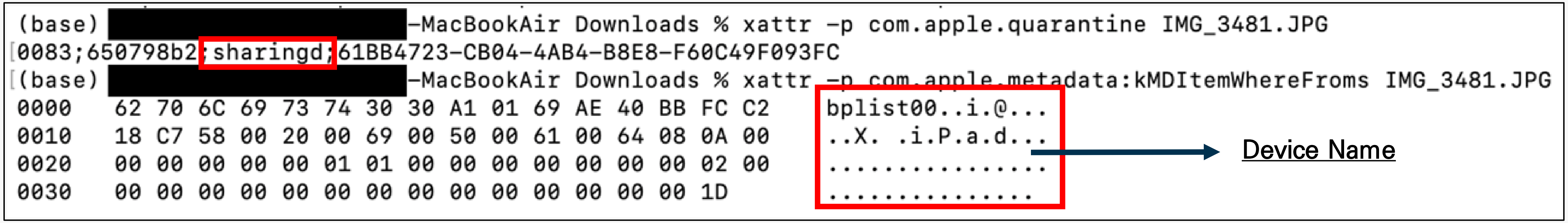
```
(base) [redacted]-MacBookAir Downloads % xattr -p com.apple.quarantine nanum-square.zip
0081;651505da;Chrome;
(base) [redacted]-MacBookAir Downloads % xattr -p com.apple.metadata:kMDItemWhereFroms nanum-square.zip
No such xattr: com.apple.metadata:kMDItemWhereFroms
```

Chrome secret browser download

② Mac Sharing Artifacts

Download files (Airdrop, SNS, Web browser, ···)

- For files downloaded via Airdrop, the ‘download agent data’ of com.apple.quarantine was marked as ‘sharingd’, and the device name was stored as a bplist in kMDItemWhereFroms.



```
(base) [redacted]-MacBookAir Downloads % xattr -p com.apple.quarantine IMG_3481.JPG
[0083;650798b2;sharingd;61BB4723-CB04-4AB4-B8E8-F60C49F093FC
[(base) [redacted]-MacBookAir Downloads % xattr -p com.apple.metadata:kMDItemWhereFroms IMG_3481.JPG
0000   62 70 6C 69 73 74 30 30 A1 01 69 AE 40 BB FC C2   bplist00..i.@...
0010   18 C7 58 00 20 00 69 00 50 00 61 00 64 08 0A 00   ..X. .i.P.a.d...
0020   00 00 00 00 00 01 01 00 00 00 00 00 00 00 02 00   ................
0030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 1D      ...............
```

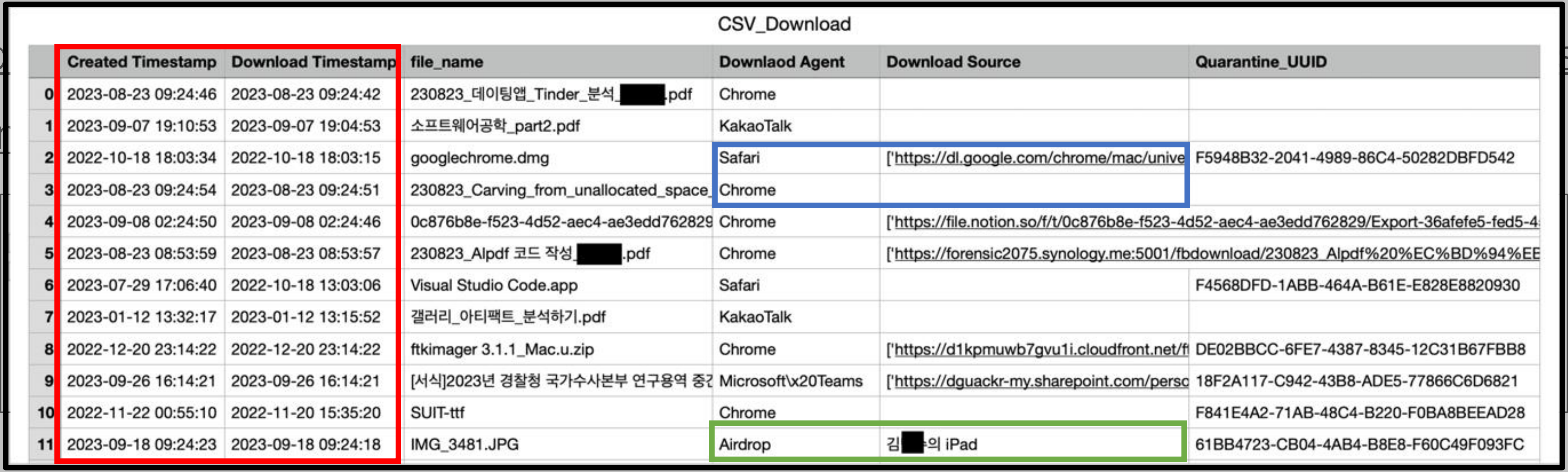
② Mac Sharing Artifacts

Download files (Airdrop, SNS, Web browser, …)

- For files downloaded via Airdrop, the ‘download agent data’ of com.apple.

q st

ir



CSV_Download

	Created Timestamp	Download Timestamp	file_name	Downlaod Agent	Download Source	Quarantine_UUID
0	2023-08-23 09:24:46	2023-08-23 09:24:42	230823_데이팅앱_Tinder_분석_[redacted].pdf	Chrome		
1	2023-09-07 19:10:53	2023-09-07 19:04:53	소프트웨어공학_part2.pdf	KakaoTalk		
2	2022-10-18 18:03:34	2022-10-18 18:03:15	googlechrome.dmg	Safari	['https://dl.google.com/chrome/mac/unive	F5948B32-2041-4989-86C4-50282DBFD542
3	2023-08-23 09:24:54	2023-08-23 09:24:51	230823_Carving_from_unallocated_space_	Chrome		
4	2023-09-08 02:24:50	2023-09-08 02:24:46	0c876b8e-f523-4d52-aec4-ae3edd762829	Chrome	['https://file.notion.so/f/t/0c876b8e-f523-4d52-aec4-ae3edd762829/Export-36afefe5-fed5-4	
5	2023-08-23 08:53:59	2023-08-23 08:53:57	230823_Alpdf 코드 작성_[redacted].pdf	Chrome	['https://forensic2075.synology.me:5001/fbdownload/230823_Alpdf%20%EC%BD%94%EE	
6	2023-07-29 17:06:40	2022-10-18 13:03:06	Visual Studio Code.app	Safari		F4568DFD-1ABB-464A-B61E-E828E8820930
7	2023-01-12 13:32:17	2023-01-12 13:15:52	갤러리_아티팩트_분석하기.pdf	KakaoTalk		
8	2022-12-20 23:14:22	2022-12-20 23:14:22	ftkimager 3.1.1_Mac.u.zip	Chrome	['https://d1kpmuwb7gvu1i.cloudfront.net/f	DE02BBCC-6FE7-4387-8345-12C31B67FBB8
9	2023-09-26 16:14:21	2023-09-26 16:14:21	[서식]2023년 경찰청 국가수사본부 연구용역 중긴	Microsoft\x20Teams	['https://dguackr-my.sharepoint.com/persc	18F2A117-C942-43B8-ADE5-77866C6D6821
10	2022-11-22 00:55:10	2022-11-20 15:35:20	SUIT-ttf	Chrome		F841E4A2-71AB-48C4-B220-F0BA8BEEAD28
11	2023-09-18 09:24:23	2023-09-18 09:24:18	IMG_3481.JPG	Airdrop	김[redacted]의 iPad	61BB4723-CB04-4AB4-B8E8-F60C49F093FC

② Mac Sharing Artifacts

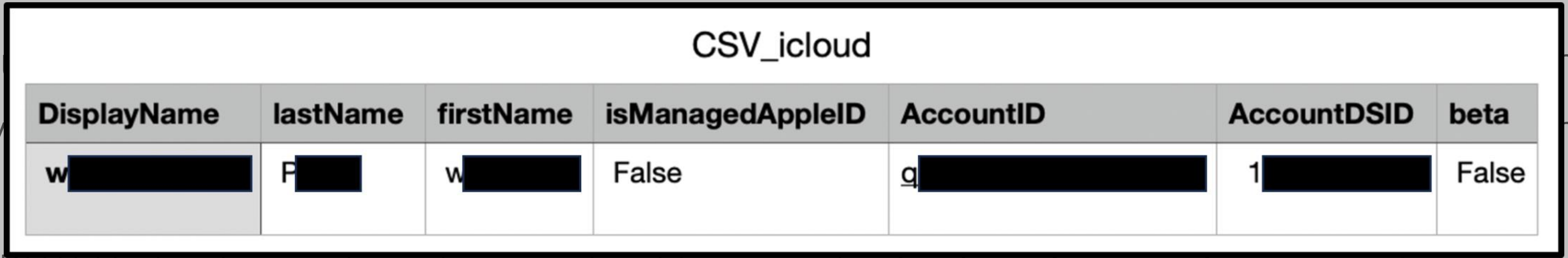
<u>iCloud</u>

- iCloud is a cloud-based service provided by Apple which integrates macOS and other Apple devices
  - Allows users to store and share data between Apple devices and computers
- iCloud is an important part of the Apple ecosystem, providing users with a convenient way to access and manage their data across all their Apple devices, as well as backing up and securing information
  - BUT) Under the conducted current legal framework, <u>cloud services require a separate warrant</u> to search through the account, so we research to <u>obtain account information</u> to issue additional search warrants.
  - iCloud accounts information can be found in ‘Users/[Username]/Library/Preferences/MobileMe Accounts.plist' file.

② Mac Sharing Artifacts

iCloud

- iCloud is a cloud-based service provided by Apple which integrates macOS and other Apple devices
    - Allows users to store and share data between Apple devices and computers
- iClo nt
  way ng up
  and



CSV_icloud

DisplayName	lastName	firstName	isManagedAppleID	AccountID	AccountDSID	beta
w[redacted]	P[redacted]	w[redacted]	False	q[redacted]	1[redacted]	False

    - BUT) Under the conducted current legal framework, cloud services require a separate warrant to search through the account, so we research to obtain account information to issue additional search warrants.
    - iCloud accounts information can be found in 'Users/[Username]/Library/Preferences/MobileMe Accounts.plist' file.

② Mac Sharing Artifacts

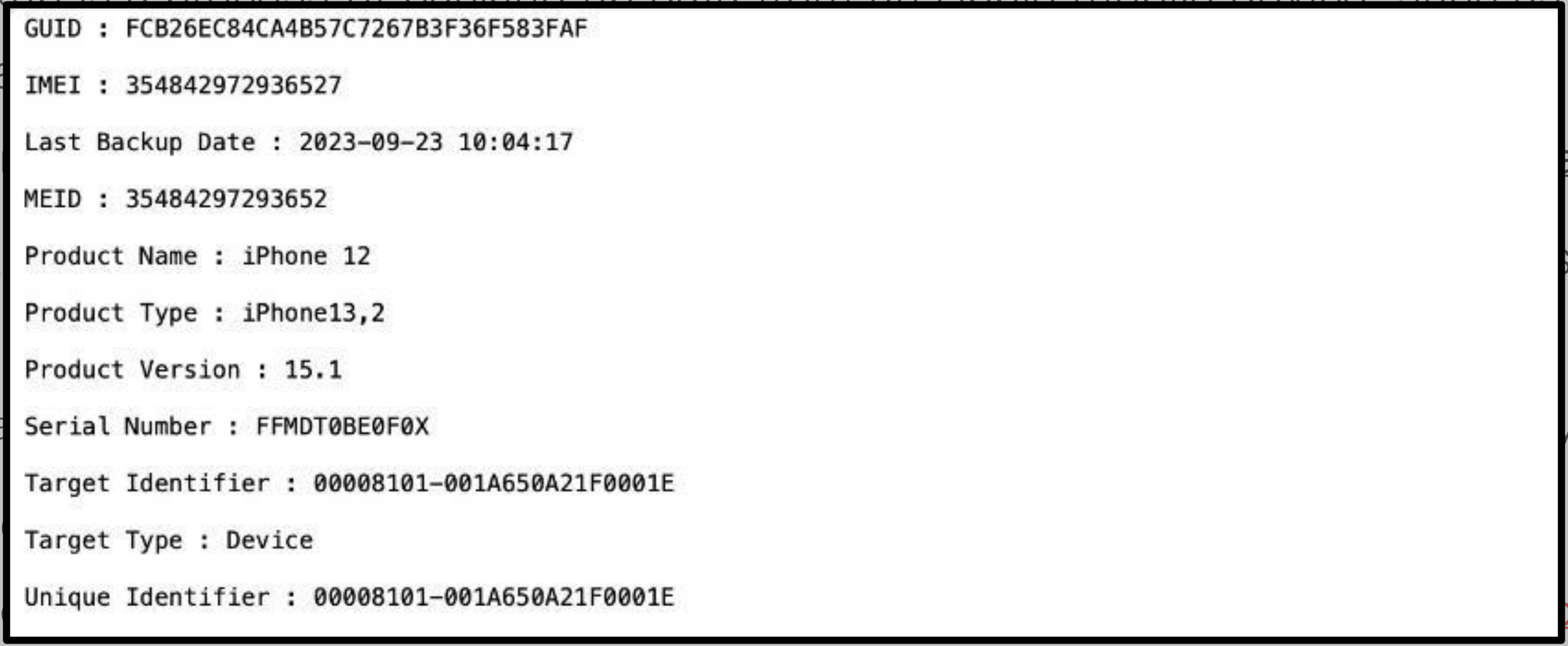
iDevice backup

- iDevice backup is a process of backing up data from an Apple mobile device, such as an iPhone, iPad, to a MacOS PC.
  - Includes information such as app data, device settings, photos, videos, messages, contacts, call logs, etc.
- Since this study is on MacOS PC, we investigated the artifacts left on the PC after using a local backup.
  - The relevant artifacts are stored in '%%users.homedir%%/Library/Application Support/MobileSync/'
- The backup data itself may be **encrypted**, it may not be interpretable
  - So, we tried to provide a full copy of the backup, extracted data to analyse from Info.plist, which can be obtained in plain text even when encrypted.
  - The information in '%%users.homedir%%/Library/Application Support/MobileSync/Info.plist' includes GUID, IMEI, Last Backup Date, etc.

② Mac Sharing Artifacts

iDevice backup

- iDevice backup is a process of backing up data from an Apple mobile device, such as an iPhone, iPad, to a Ma
  - Includes i all logs, etc.
- Since this st sing a local backup.
  - The releva ync/'
- The backup
  - So, we tri ch can be obtained in plain text even when encrypted.
  - The information in '%%users.homedir%%/Library/Application Support/MobileSync/Info.plist' includes GUID, IMEI, Last Backup Date, etc.

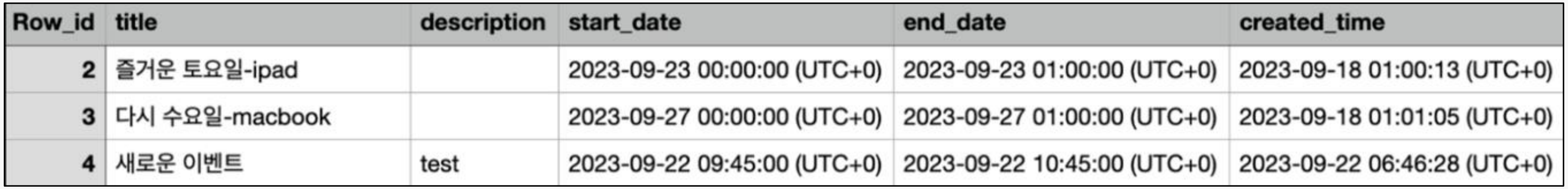


```
GUID : FCB26EC84CA4B57C7267B3F36F583FAF

IMEI : 354842972936527

Last Backup Date : 2023-09-23 10:04:17

MEID : 35484297293652

Product Name : iPhone 12

Product Type : iPhone13,2

Product Version : 15.1

Serial Number : FFMDT0BE0F0X

Target Identifier : 00008101-001A650A21F0001E

Target Type : Device

Unique Identifier : 00008101-001A650A21F0001E
```

② Mac Sharing Artifacts

Calendar

- Handoff: Synchronizing data between Mac, iPhone, iPad, iPod touch, Apple Watch when user logs in with identical profile.
  - Includes information such as Note, Calendar, Call History, Contact, Photo, etc.
- Calendar is the application to note and share the schedule
  - User can include Location Information, email and phone number to share, attachment, etc.
  - Timestamps are encoded by Mac TimeStamp (CFAbsolute Time)

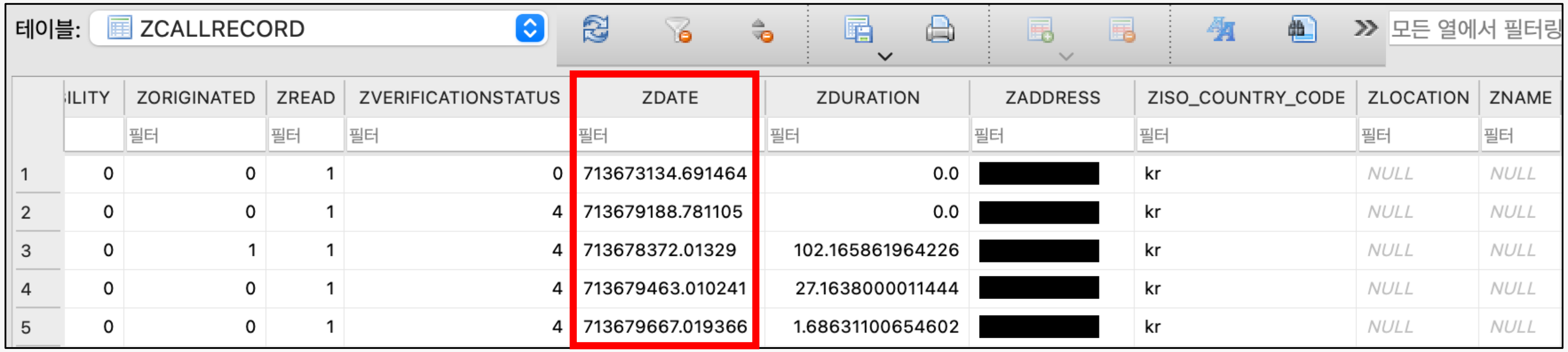


Row_id	title	description	start_date	end_date	created_time
2	즐거운 토요일-ipad		2023-09-23 00:00:00 (UTC+0)	2023-09-23 01:00:00 (UTC+0)	2023-09-18 01:00:13 (UTC+0)
3	다시 수요일-macbook		2023-09-27 00:00:00 (UTC+0)	2023-09-27 01:00:00 (UTC+0)	2023-09-18 01:01:05 (UTC+0)
4	새로운 이벤트	test	2023-09-22 09:45:00 (UTC+0)	2023-09-22 10:45:00 (UTC+0)	2023-09-22 06:46:28 (UTC+0)

② Mac Sharing Artifacts

Call History

- Call History stores information of voice and video calls when iOS, MacOS are synchronized
  - ‘/User/[Username]/Library/Application Support/CallHistoryDB/CallHistory.storesdata
  - ZCALLRECORD Table includes **call duration**(ZDURATION), **call date**(ZDATE), **phone address**(ZADDRESS), **country code**(ZISO_COUNTRY_CODE), etc.
    - ✓ ZDATE refers to call date, which are encoded by Mac Timestamp (CFAbsolute Time)



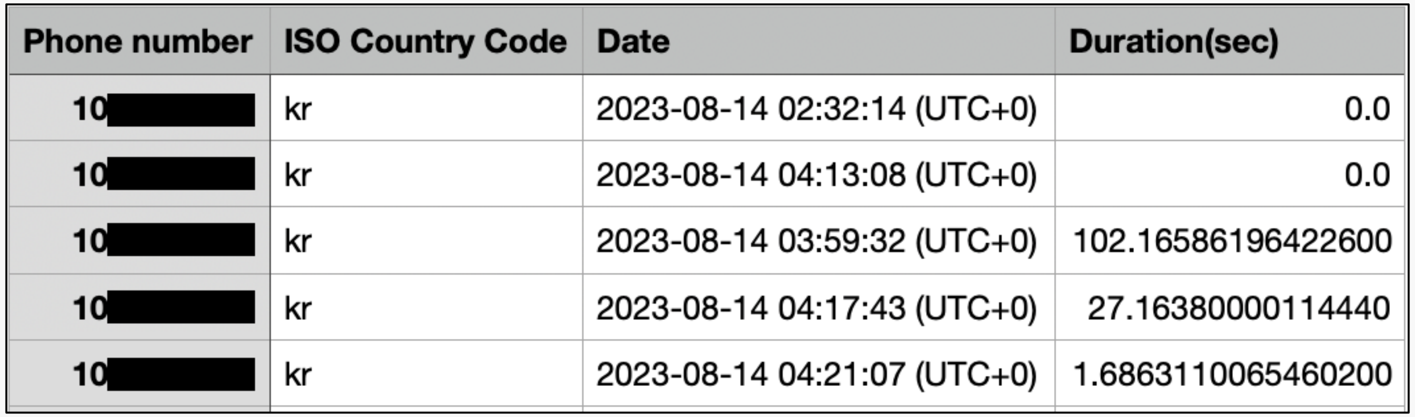
테이블: ZCALLRECORD

	ILITY	ZORIGINATED	ZREAD	ZVERIFICATIONSTATUS	ZDATE	ZDURATION	ZADDRESS	ZISO_COUNTRY_CODE	ZLOCATION	ZNAME
		필터	필터	필터	필터	필터	필터	필터	필터	필터
1	0	0	1	0	713673134.691464	0.0	[redacted]	kr	NULL	NULL
2	0	0	1	4	713679188.781105	0.0	[redacted]	kr	NULL	NULL
3	0	1	1	4	713678372.01329	102.165861964226	[redacted]	kr	NULL	NULL
4	0	0	1	4	713679463.010241	27.1638000011444	[redacted]	kr	NULL	NULL
5	0	0	1	4	713679667.019366	1.68631100654602	[redacted]	kr	NULL	NULL

② Mac Sharing Artifacts

Contacts

- Contacts stores the phone addresses which are stored in iOS devices
  - Contacts stores contact data in the folder named '/Users/[Username]/Library/Application Support/AddressBook/ Sources/〈GUID〉/Metadata'
  - Each contact data is stored in the file named '〈UUID〉/ABPerson.abcdp'
  - Every device has different GUID
- Each phone address file stores last name, first name, workplace, phone address.

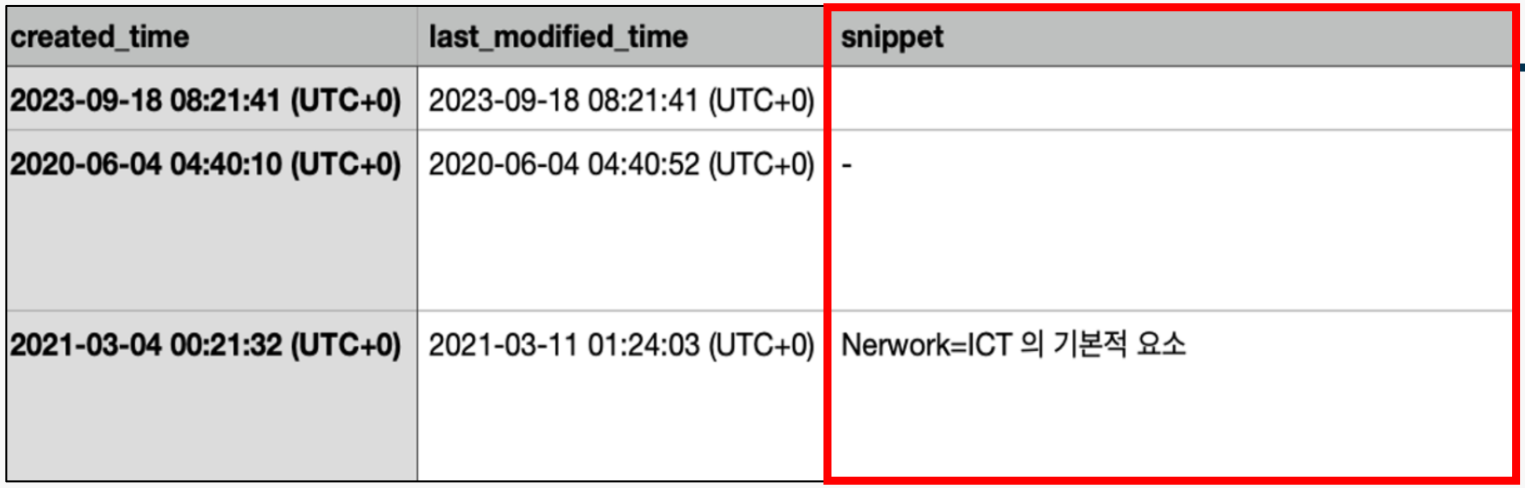


Phone number	ISO Country Code	Date	Duration(sec)
10[redacted]	kr	2023-08-14 02:32:14 (UTC+0)	0.0
10[redacted]	kr	2023-08-14 04:13:08 (UTC+0)	0.0
10[redacted]	kr	2023-08-14 03:59:32 (UTC+0)	102.16586196422600
10[redacted]	kr	2023-08-14 04:17:43 (UTC+0)	27.16380000114440
10[redacted]	kr	2023-08-14 04:21:07 (UTC+0)	1.6863110065460200

② Mac Sharing Artifacts

Notes

- Notes is the application to write, and attach checklist, image, web link, scanned document, etc.
  - Synchronized by the identical profile logged in the iCloud
- Part of the data stored in the DB is compressed by gzip format
  - Time information is encoded by Mac Timestamp (CFAbsolute Time)



created_time	last_modified_time	snippet
2023-09-18 08:21:41 (UTC+0)	2023-09-18 08:21:41 (UTC+0)	
2020-06-04 04:40:10 (UTC+0)	2020-06-04 04:40:52 (UTC+0)	-
2021-03-04 00:21:32 (UTC+0)	2021-03-11 01:24:03 (UTC+0)	Nerwork=ICT 의 기본적 요소

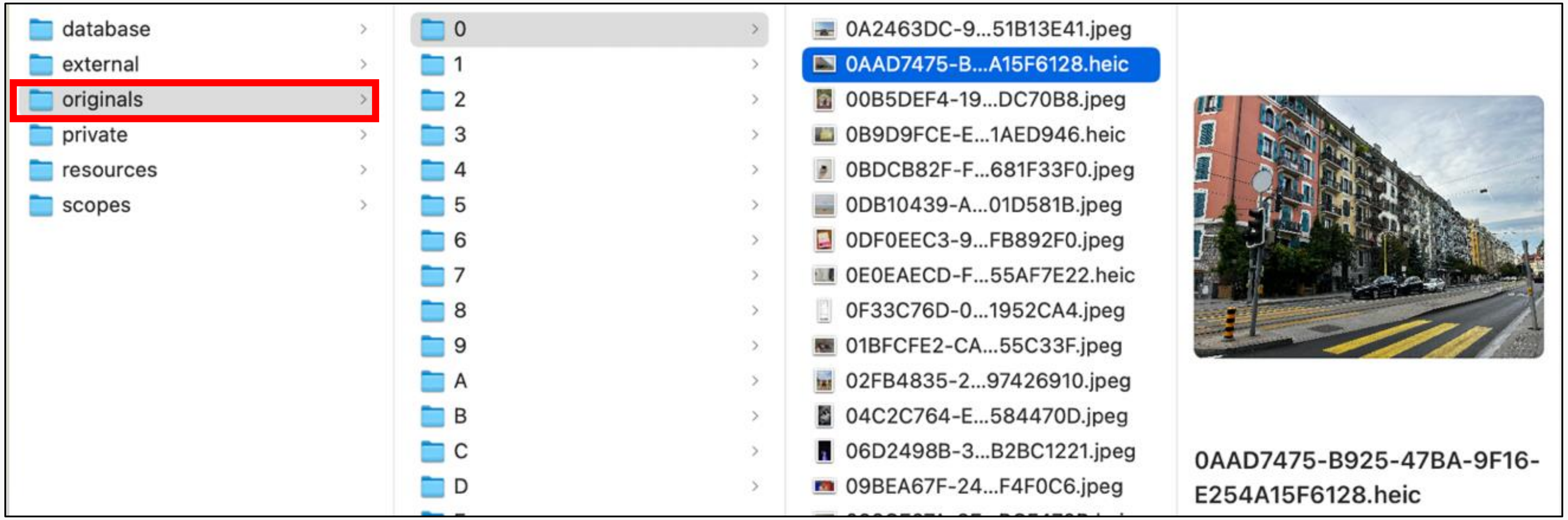
Note Preview

② Mac Sharing Artifacts

Photos

- Photos saves images or videos inside the album of synchronized iOS devices
  - '/Users/[Username]/Pictures/Photos Library.photosLibrary'

- For '**originals**' in Photos Library.photosLibrary, all images & videos are stored in the folder '0' to 'F'



database
external
originals
private
resources
scopes

0
1
2
3
4
5
6
7
8
9
A
B
C
D

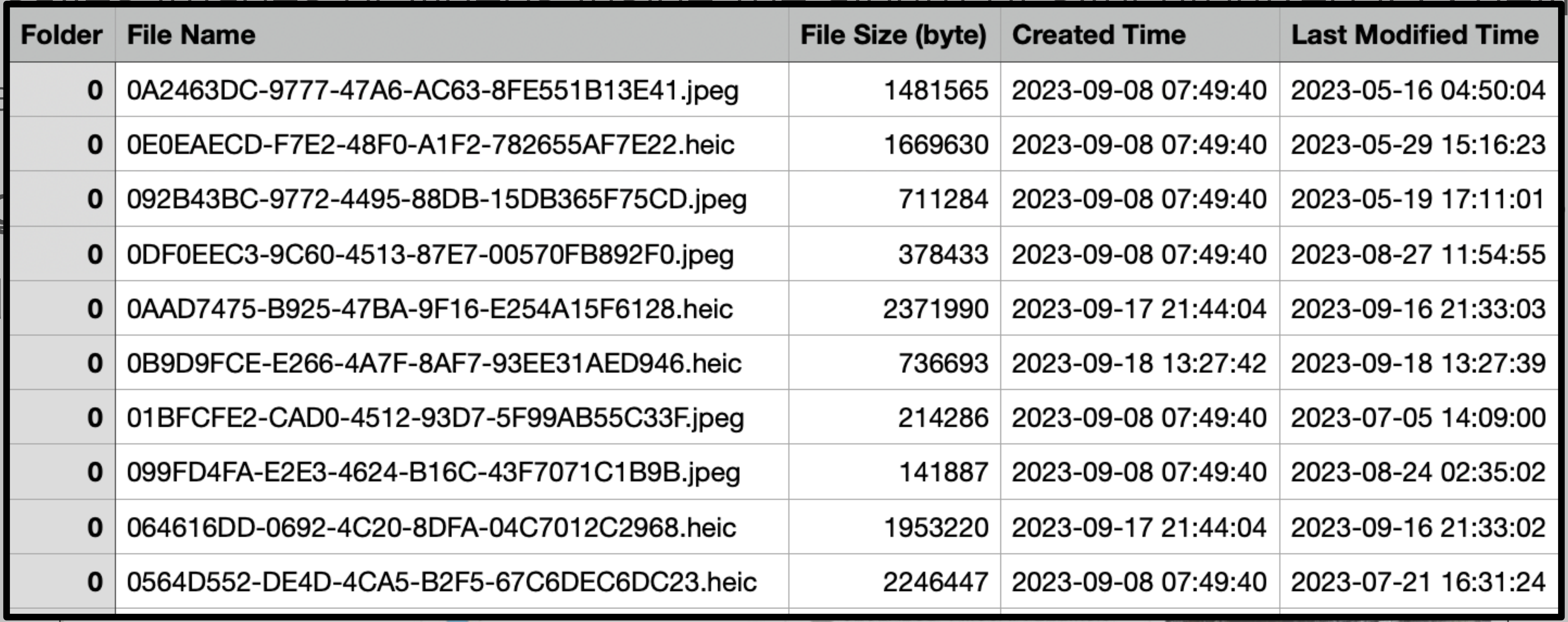
0A2463DC-9...51B13E41.jpeg
0AAD7475-B...A15F6128.heic
00B5DEF4-19...DC70B8.jpeg
0B9D9FCE-E...1AED946.heic
0BDCB82F-F...681F33F0.jpeg
0DB10439-A...01D581B.jpeg
0DF0EEC3-9...FB892F0.jpeg
0E0EAECD-F...55AF7E22.heic
0F33C76D-0...1952CA4.jpeg
01BFCFE2-CA...55C33F.jpeg
02FB4835-2...97426910.jpeg
04C2C764-E...584470D.jpeg
06D2498B-3...B2BC1221.jpeg
09BEA67F-24...F4F0C6.jpeg

0AAD7475-B925-47BA-9F16-E254A15F6128.heic

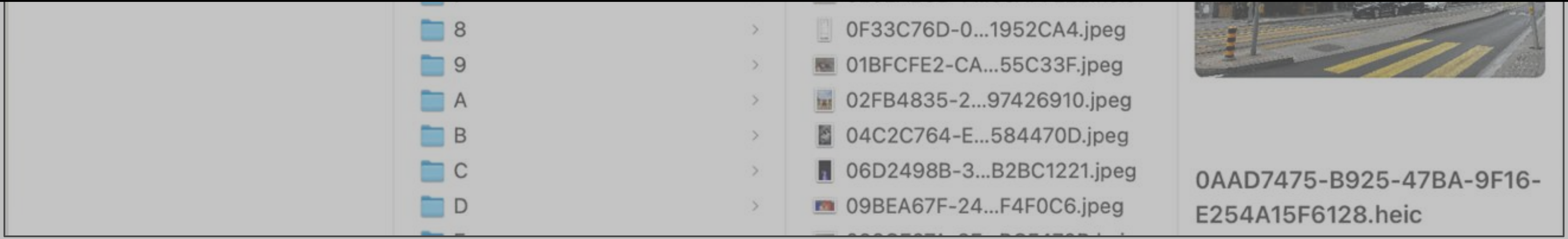
② Mac Sharing Artifacts

Photos

- Photos saves images or videos inside the album of synchronized iOS devices
  - '/Use
- For 'orig red in the fold



Folder	File Name	File Size (byte)	Created Time	Last Modified Time
0	0A2463DC-9777-47A6-AC63-8FE551B13E41.jpeg	1481565	2023-09-08 07:49:40	2023-05-16 04:50:04
0	0E0EAECD-F7E2-48F0-A1F2-782655AF7E22.heic	1669630	2023-09-08 07:49:40	2023-05-29 15:16:23
0	092B43BC-9772-4495-88DB-15DB365F75CD.jpeg	711284	2023-09-08 07:49:40	2023-05-19 17:11:01
0	0DF0EEC3-9C60-4513-87E7-00570FB892F0.jpeg	378433	2023-09-08 07:49:40	2023-08-27 11:54:55
0	0AAD7475-B925-47BA-9F16-E254A15F6128.heic	2371990	2023-09-17 21:44:04	2023-09-16 21:33:03
0	0B9D9FCE-E266-4A7F-8AF7-93EE31AED946.heic	736693	2023-09-18 13:27:42	2023-09-18 13:27:39
0	01BFCFE2-CAD0-4512-93D7-5F99AB55C33F.jpeg	214286	2023-09-08 07:49:40	2023-07-05 14:09:00
0	099FD4FA-E2E3-4624-B16C-43F7071C1B9B.jpeg	141887	2023-09-08 07:49:40	2023-08-24 02:35:02
0	064616DD-0692-4C20-8DFA-04C7012C2968.heic	1953220	2023-09-17 21:44:04	2023-09-16 21:33:02
0	0564D552-DE4D-4CA5-B2F5-67C6DEC6DC23.heic	2246447	2023-09-08 07:49:40	2023-07-21 16:31:24

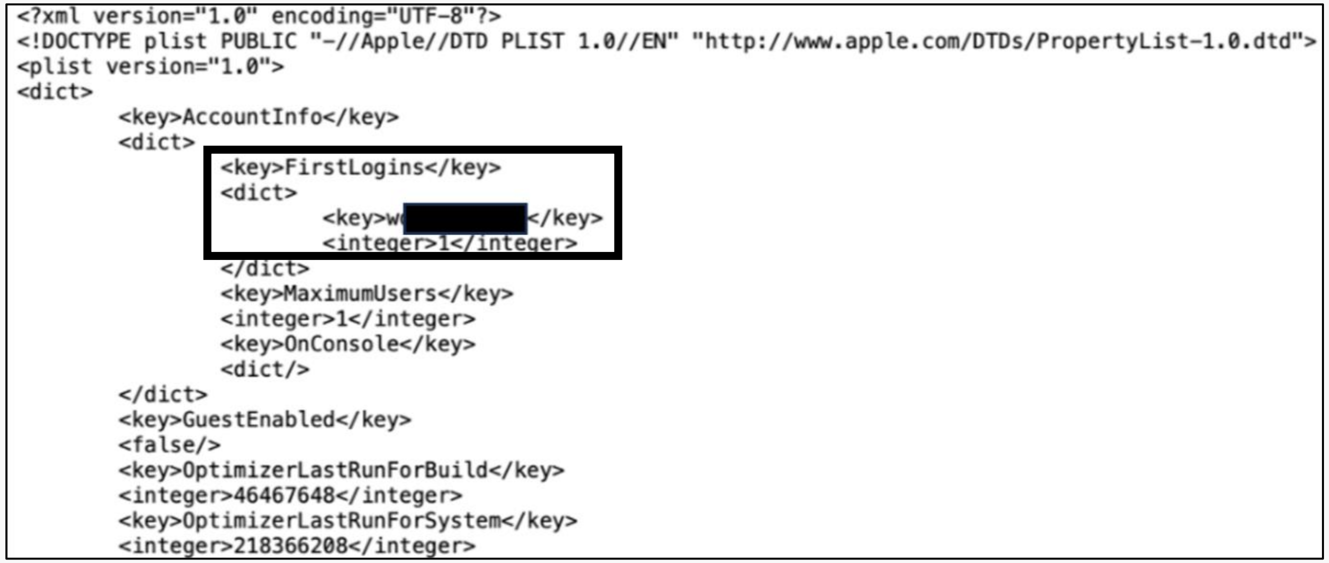

8
9
A
B
C
D
0F33C76D-0...1952CA4.jpeg
01BFCFE2-CA...55C33F.jpeg
02FB4835-2...97426910.jpeg
04C2C764-E...584470D.jpeg
06D2498B-3...B2BC1221.jpeg
09BEA67F-24...F4F0C6.jpeg
0AAD7475-B925-47BA-9F16-E254A15F6128.heic

③ General Artifacts

Login Window

- Login Window stores the users' profile login information
  - Includes the last login user profile, last login user's state (login/logout), auto-login profile, auto-login user's screenlock, etc.

- Updated by the Login Window
  - Login Window is the first service which user can check when the Mac is on

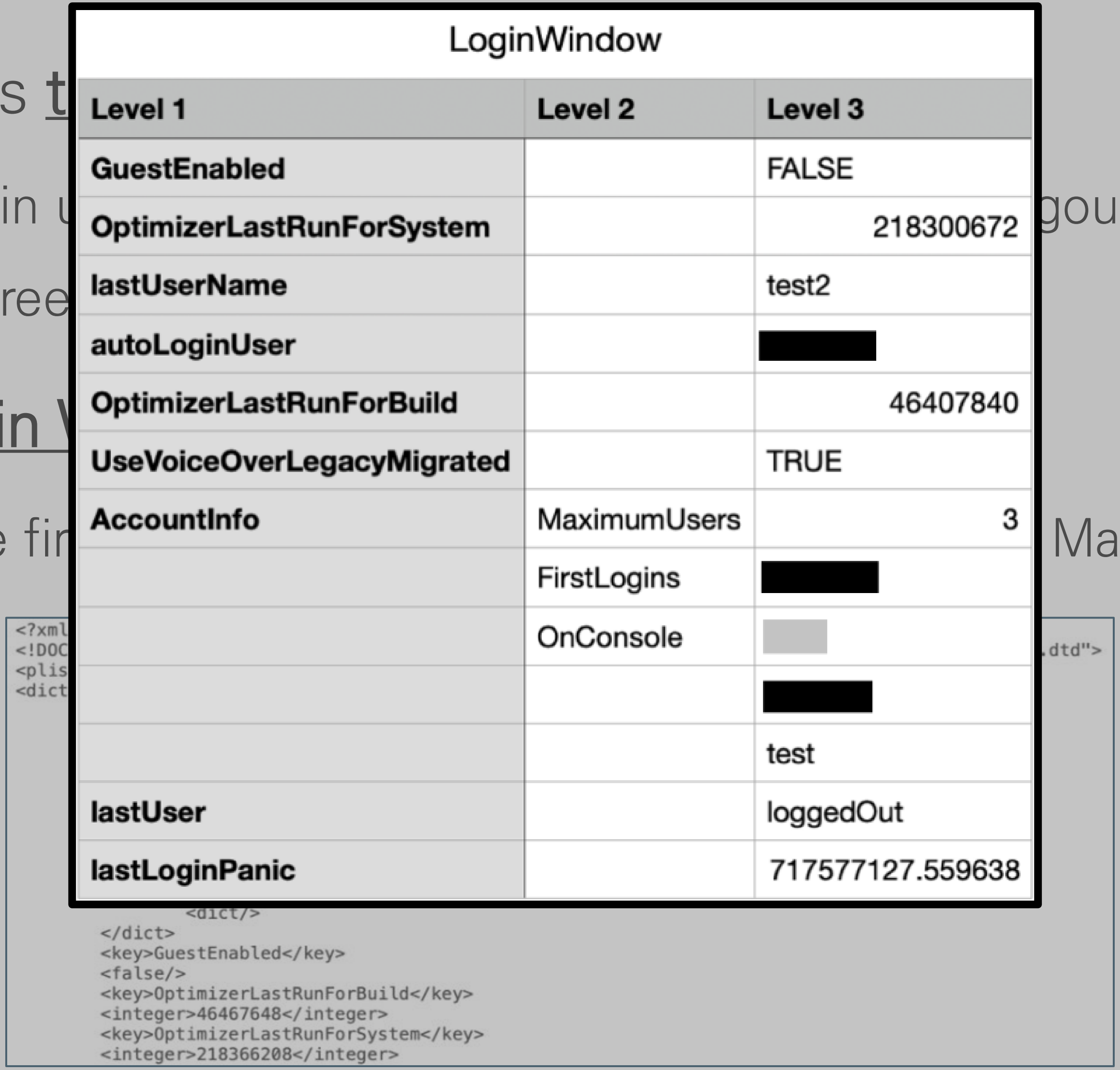


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>AccountInfo</key>
        <dict>
                <key>FirstLogins</key>
                <dict>
                        <key>[redacted]</key>
                        <integer>1</integer>
                </dict>
                <key>MaximumUsers</key>
                <integer>1</integer>
                <key>OnConsole</key>
                <dict/>
        </dict>
        <key>GuestEnabled</key>
        <false/>
        <key>OptimizerLastRunForBuild</key>
        <integer>46467648</integer>
        <key>OptimizerLastRunForSystem</key>
        <integer>218366208</integer>
```

③ General Artifacts

Login Window

- Login Window stores t
  - Includes the last login u gout), auto–login profile, auto–login user's scree
- Updated by the Login W
  - Login Window is the fir Mac is on



LoginWindow

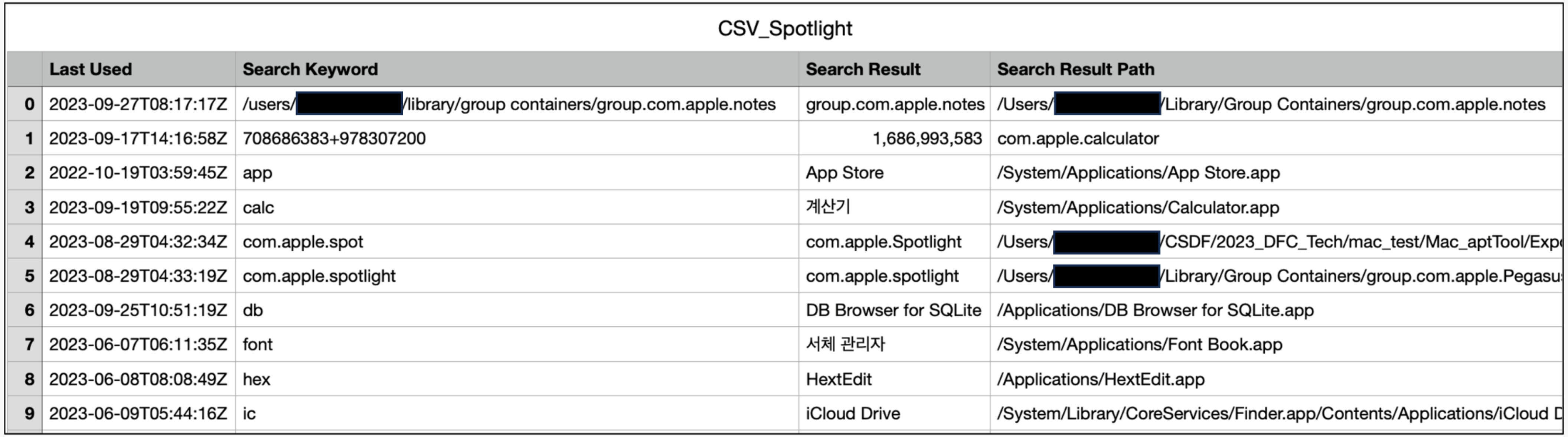
Level 1	Level 2	Level 3
GuestEnabled		FALSE
OptimizerLastRunForSystem		218300672
lastUserName		test2
autoLoginUser		[redacted]
OptimizerLastRunForBuild		46407840
UseVoiceOverLegacyMigrated		TRUE
AccountInfo	MaximumUsers	3
	FirstLogins	[redacted]
	OnConsole	
		[redacted]
		test
lastUser		loggedOut
lastLoginPanic		717577127.559638

```
<?xml
<!DOC                                                                    .dtd">
<plis
<dict
            <dict/>
        </dict>
        <key>GuestEnabled</key>
        <false/>
        <key>OptimizerLastRunForBuild</key>
        <integer>46467648</integer>
        <key>OptimizerLastRunForSystem</key>
        <integer>218366208</integer>
```

③ General Artifacts

Spotlight

- Spotlight is the search utility provided by Mac
  - User can search about application, document, browser, etc.
  - /Users/[UserName]/Library/ApplicationSupport/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3



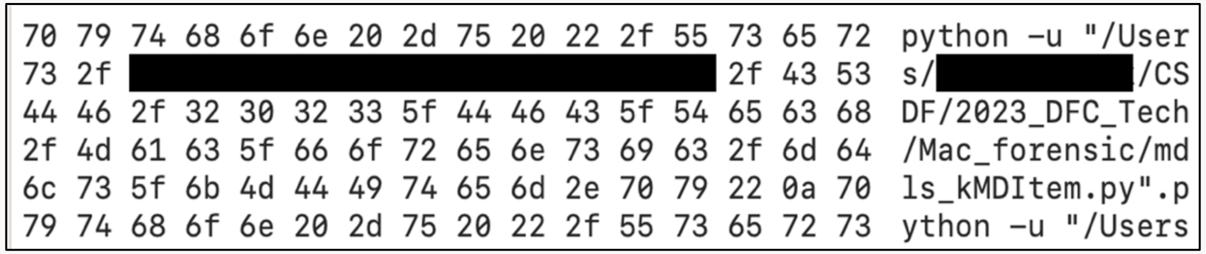
CSV_Spotlight

	Last Used	Search Keyword	Search Result	Search Result Path
0	2023-09-27T08:17:17Z	/users/[redacted]/library/group containers/group.com.apple.notes	group.com.apple.notes	/Users/[redacted]/Library/Group Containers/group.com.apple.notes
1	2023-09-17T14:16:58Z	708686383+978307200	1,686,993,583	com.apple.calculator
2	2022-10-19T03:59:45Z	app	App Store	/System/Applications/App Store.app
3	2023-09-19T09:55:22Z	calc	계산기	/System/Applications/Calculator.app
4	2023-08-29T04:32:34Z	com.apple.spot	com.apple.Spotlight	/Users/[redacted]/CSDF/2023_DFC_Tech/mac_test/Mac_aptTool/Exp
5	2023-08-29T04:33:19Z	com.apple.spotlight	com.apple.spotlight	/Users/[redacted]/Library/Group Containers/group.com.apple.Pegasu
6	2023-09-25T10:51:19Z	db	DB Browser for SQLite	/Applications/DB Browser for SQLite.app
7	2023-06-07T06:11:35Z	font	서체 관리자	/System/Applications/Font Book.app
8	2023-06-08T08:08:49Z	hex	HextEdit	/Applications/HextEdit.app
9	2023-06-09T05:44:16Z	ic	iCloud Drive	/System/Library/CoreServices/Finder.app/Contents/Applications/iCloud D

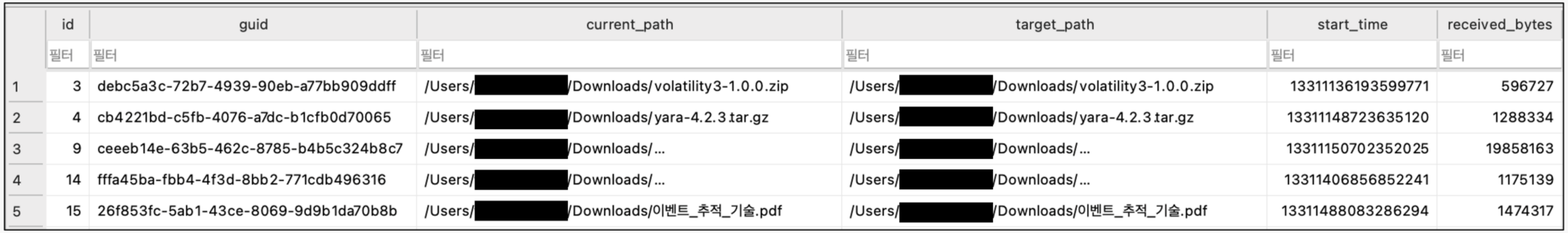
③ General Artifacts

Terminal History

- The Default shell type of terminal differs through MacOS version.
  - Under 10.15 : bash shell
    - ✓ Bash: '/Users/[Username]/.bash_history'
  - Over 10.15 : zsh shell
    - ✓ Zsh: '/Users/[Username]/.zsh_history'



```
70 79 74 68 6f 6e 20 2d 75 20 22 2f 55 73 65 72  python -u "/User
73 2f [redacted] 2f 43 53  s/[redacted]/CS
44 46 2f 32 30 32 33 5f 44 46 43 5f 54 65 63 68  DF/2023_DFC_Tech
2f 4d 61 63 5f 66 6f 72 65 6e 73 69 63 2f 6d 64  /Mac_forensic/md
6c 73 5f 6b 4d 44 49 74 65 6d 2e 70 79 22 0a 70  ls_kMDItem.py".p
79 74 68 6f 6e 20 2d 75 20 22 2f 55 73 65 72 73  ython -u "/Users
```

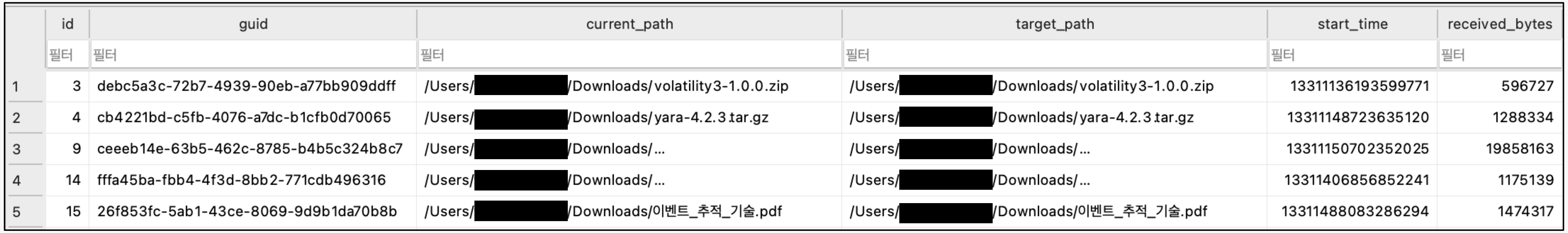


	id	guid	current_path	target_path	start_time	received_bytes
	필터	필터	필터	필터	필터	필터
1	3	debc5a3c-72b7-4939-90eb-a77bb909ddff	/Users/[redacted]/Downloads/volatility3-1.0.0.zip	/Users/[redacted]/Downloads/volatility3-1.0.0.zip	13311136193599771	596727
2	4	cb4221bd-c5fb-4076-a7dc-b1cfb0d70065	/Users/[redacted]/Downloads/yara-4.2.3.tar.gz	/Users/[redacted]/Downloads/yara-4.2.3.tar.gz	13311148723635120	1288334
3	9	ceeeb14e-63b5-462c-8785-b4b5c324b8c7	/Users/[redacted]/Downloads/...	/Users/[redacted]/Downloads/...	13311150702352025	19858163
4	14	fffa45ba-fbb4-4f3d-8bb2-771cdb496316	/Users/[redacted]/Downloads/...	/Users/[redacted]/Downloads/...	13311406856852241	1175139
5	15	26f853fc-5ab1-43ce-8069-9d9b1da70b8b	/Users/[redacted]/Downloads/이벤트_추적_기술.pdf	/Users/[redacted]/Downloads/이벤트_추적_기술.pdf	13311488083286294	1474317

③ General Artifacts

Web browser history(Safari, Chrome)

- Traces of the browser installation are stored '~/Library folder name'
  - Safari: '~/Library/Safari/'
    - ✓ Stored in History.db(visit history) and Downloads.plist(download history)
  - Chrome: '~/Library/ Application Support/Google/Chrome/Default/History'
    - ✓ Downloads table stores the download path, download start time, received data size, etc.
    - ✓ Url table stores **visited url, title of the visited web site, last visited time, etc.**



	id	guid	current_path	target_path	start_time	received_bytes
	필터	필터	필터	필터	필터	필터
1	3	debc5a3c-72b7-4939-90eb-a77bb909ddff	/Users/[redacted]/Downloads/volatility3-1.0.0.zip	/Users/[redacted]/Downloads/volatility3-1.0.0.zip	13311136193599771	596727
2	4	cb4221bd-c5fb-4076-a7dc-b1cfb0d70065	/Users/[redacted]/Downloads/yara-4.2.3.tar.gz	/Users/[redacted]/Downloads/yara-4.2.3.tar.gz	13311148723635120	1288334
3	9	ceeeb14e-63b5-462c-8785-b4b5c324b8c7	/Users/[redacted]/Downloads/...	/Users/[redacted]/Downloads/...	13311150702352025	19858163
4	14	fffa45ba-fbb4-4f3d-8bb2-771cdb496316	/Users/[redacted]/Downloads/...	/Users/[redacted]/Downloads/...	13311406856852241	1175139
5	15	26f853fc-5ab1-43ce-8069-9d9b1da70b8b	/Users/[redacted]/Downloads/이벤트_추적_기술.pdf	/Users/[redacted]/Downloads/이벤트_추적_기술.pdf	13311488083286294	1474317

4. Code implementation

Pseudocode

```
input artifact_file

Function artifact_function()
    if artifact_file is True:
        Copy_file(artifact_path, copy_path)
        analyze_artifact(copy_path)
        make_CsvFile(script_path)

if parameter is not “” :
    artifact_function(parameter)
```

- The tool was developed using Python3 and tested on four MacOS devices(Macbook Air and MacBook Pro, OS: 13.4.*).
- The reason for copying and analyzing artifact-related files is down below:

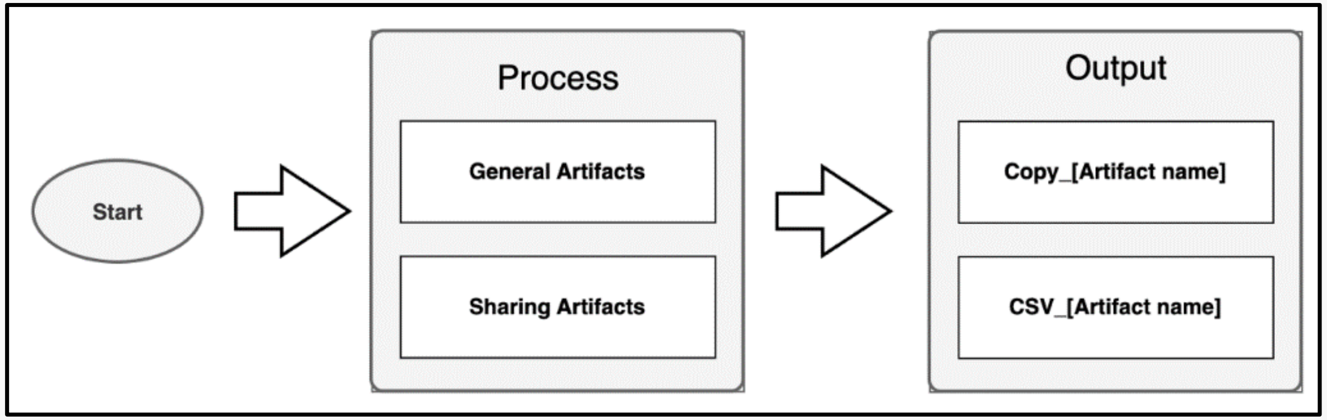
  1) Collect artifacts
  2) Create a folder in the path where the script files are located to access them

     ✓ Since in certain folders, it’s impossible to analyse the files directly.

How the tool works and results

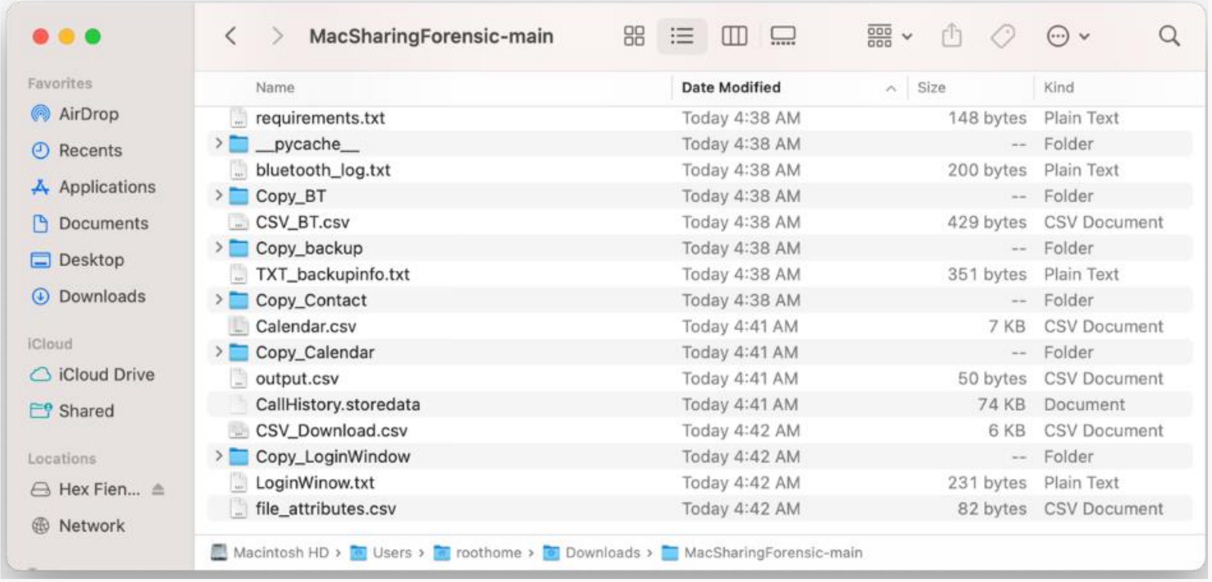
- Tool can be used on the active system with root privilege.
- By running the tool on the target PC (MacOS Ventura) collects the artifacts and produces folder by each artifact
  - Copy all the artifact files and create an analysis result file.

  1) −all command: run collection and analysis on all artifacts
  2) Arguments: run tools on each artifact.

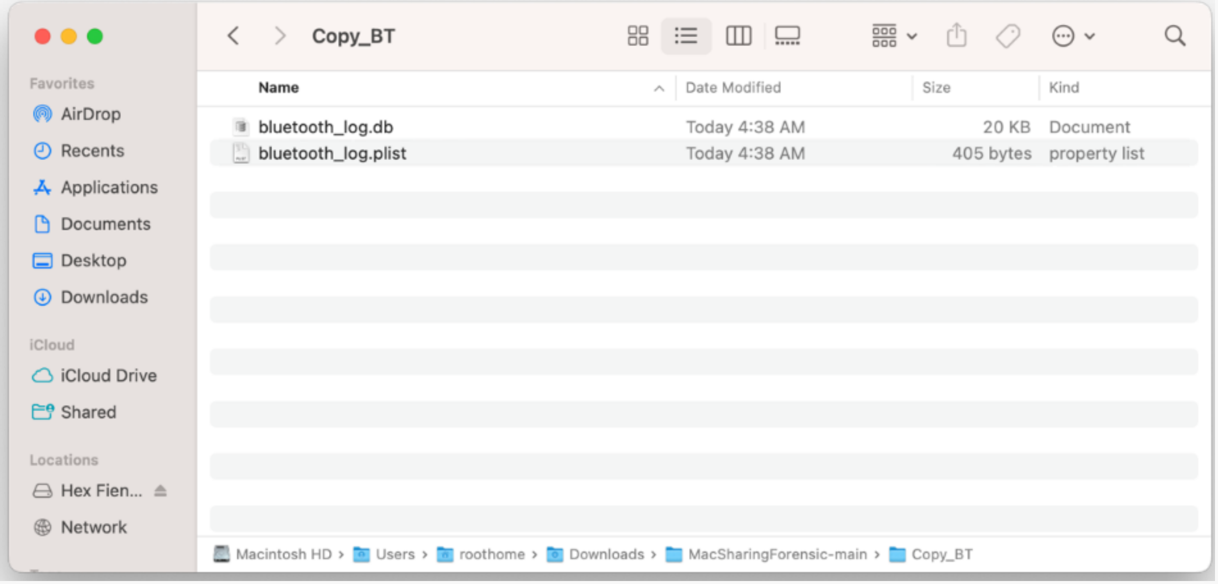


Type	Artifacts(Arguments)		
General Artifact	login window (−l)	Spotlight (−s)	Terminal History (−cont)
Mac Sharing Artifact	Bluetooth (−bt)	Calendar(−cale)	Call history (−call)
	Contact (−cont)	Download Files (−d)	icloud account (−ic)
	iDevice Backup (−id)	notes(−n)	Photos (−p)

How the tool works and results



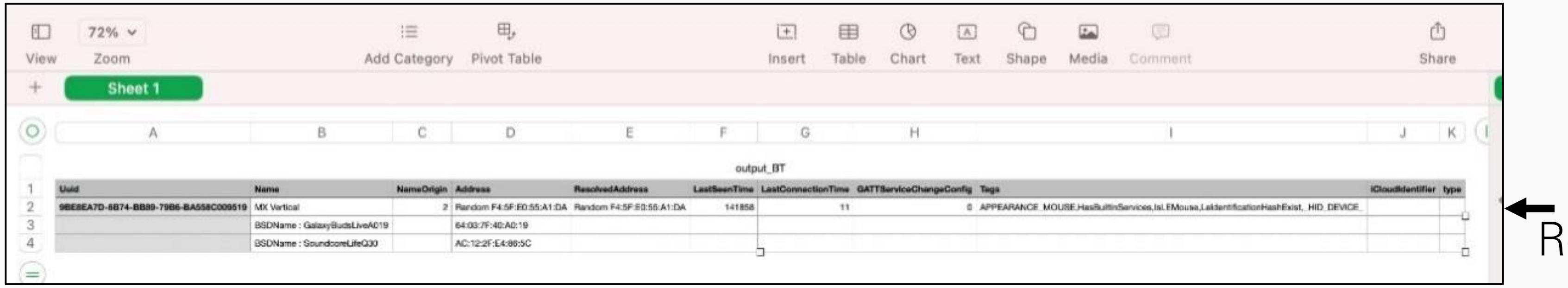
Name	Date Modified	Size	Kind
requirements.txt	Today 4:38 AM	148 bytes	Plain Text
__pycache__	Today 4:38 AM	--	Folder
bluetooth_log.txt	Today 4:38 AM	200 bytes	Plain Text
Copy_BT	Today 4:38 AM	--	Folder
CSV_BT.csv	Today 4:38 AM	429 bytes	CSV Document
Copy_backup	Today 4:38 AM	--	Folder
TXT_backupinfo.txt	Today 4:38 AM	351 bytes	Plain Text
Copy_Contact	Today 4:38 AM	--	Folder
Calendar.csv	Today 4:41 AM	7 KB	CSV Document
Copy_Calendar	Today 4:41 AM	--	Folder
output.csv	Today 4:41 AM	50 bytes	CSV Document
CallHistory.storedata	Today 4:41 AM	74 KB	Document
CSV_Download.csv	Today 4:42 AM	6 KB	CSV Document
Copy_LoginWindow	Today 4:42 AM	--	Folder
LoginWinow.txt	Today 4:42 AM	231 bytes	Plain Text
file_attributes.csv	Today 4:42 AM	82 bytes	CSV Document



Name	Date Modified	Size	Kind
bluetooth_log.db	Today 4:38 AM	20 KB	Document
bluetooth_log.plist	Today 4:38 AM	405 bytes	property list

↑Result of using the –all command

↑Result folder of Bluetooth analysis

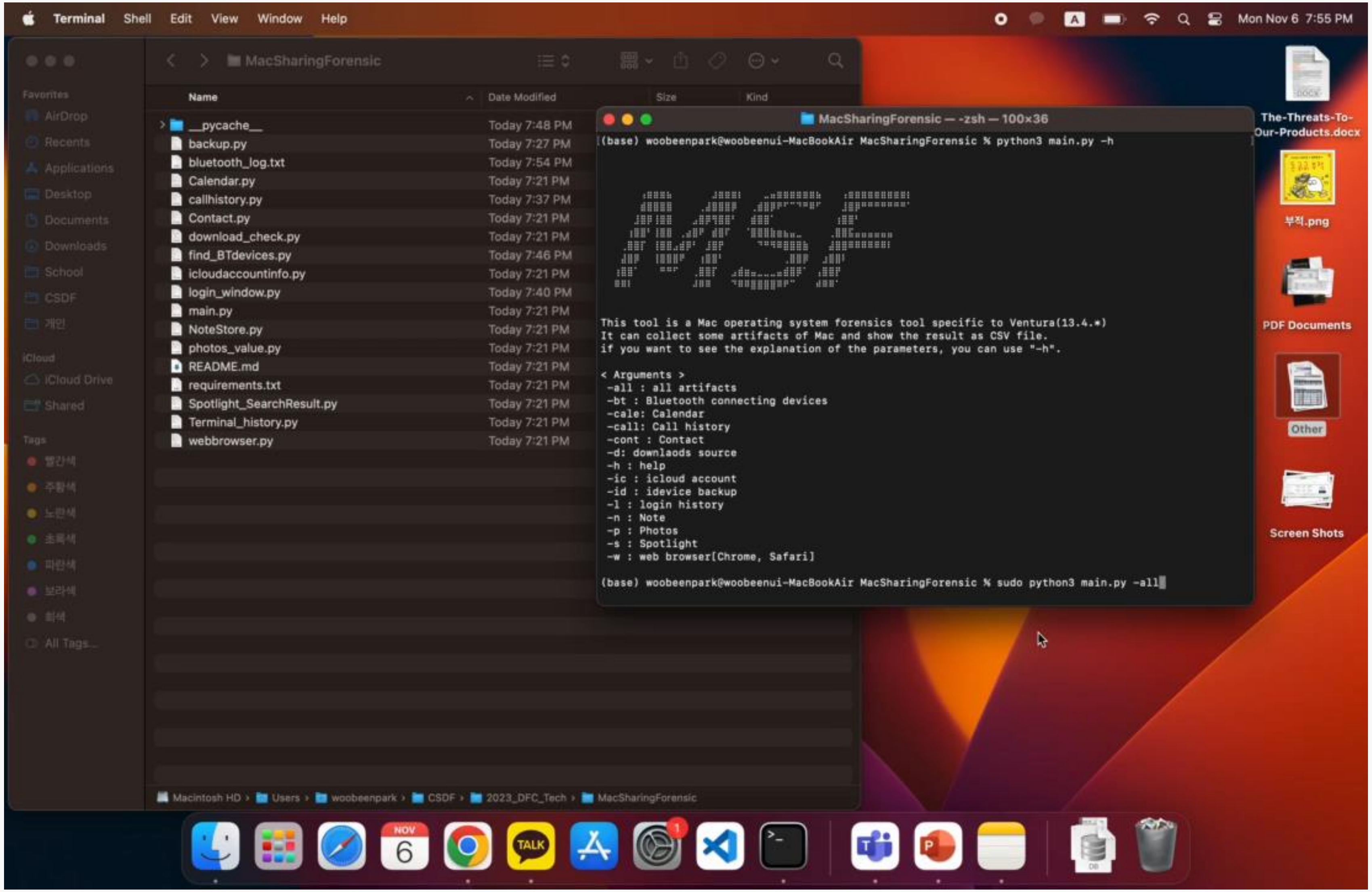


output_BT

Uuid	Name	NameOrigin	Address	ResolvedAddress	LastSeenTime	LastConnectionTime	GATTServiceChangeConfig	Tags	iCloudIdentifier	type
9BE8EA7D-6B74-BB89-79B6-BA558C009519	MX Vertical	2	Random F4:5F:E0:55:A1:DA	Random F4:5F:E0:55:A1:DA	141858	11	0	APPEARANCE_MOUSE,HasBuiltinServices,IsLEMouse,LeIdentificationHashExist,_HID_DEVICE_		
	BSDName : GalaxyBudsLiveA019		64:03:7F:40:A0:19							
	BSDName : SoundcoreLifeQ30		AC:12:2F:E4:86:5C							

←Result csv file example of Bluetooth

Example of code operation



Name	Date Modified	Size	Kind
__pycache__	Today 7:48 PM		
backup.py	Today 7:27 PM		
bluetooth_log.txt	Today 7:54 PM		
Calendar.py	Today 7:21 PM		
callhistory.py	Today 7:37 PM		
Contact.py	Today 7:21 PM		
download_check.py	Today 7:21 PM		
find_BTdevices.py	Today 7:46 PM		
icloudaccountinfo.py	Today 7:21 PM		
login_window.py	Today 7:40 PM		
main.py	Today 7:21 PM		
NoteStore.py	Today 7:21 PM		
photos_value.py	Today 7:21 PM		
README.md	Today 7:21 PM		
requirements.txt	Today 7:21 PM		
Spotlight_SearchResult.py	Today 7:21 PM		
Terminal_history.py	Today 7:21 PM		
webbrowser.py	Today 7:21 PM		

MacSharingForensic — -zsh — 100×36

```
(base) woobeenpark@woobeenui-MacBookAir MacSharingForensic % python3 main.py -h

This tool is a Mac operating system forensics tool specific to Ventura(13.4.*)
It can collect some artifacts of Mac and show the result as CSV file.
if you want to see the explanation of the parameters, you can use "-h".

< Arguments >
 -all : all artifacts
 -bt : Bluetooth connecting devices
 -cale: Calendar
 -call: Call history
 -cont : Contact
 -d: downlaods source
 -h : help
 -ic : icloud account
 -id : idevice backup
 -l : login history
 -n : Note
 -p : Photos
 -s : Spotlight
 -w : web browser[Chrome, Safari]

(base) woobeenpark@woobeenui-MacBookAir MacSharingForensic % sudo python3 main.py -all
```

5. Conclusion

Conclusion

Contribution

- Modernized the MacOS forensic tools which can analyze the interconnectivity
  - Tool development based on latest Mac version Ventura (MacOS version 13.4)
  - Tool targeted artifacts related to interconnectivity
- Addressed the limitations of the range of analyzable artifacts, and the user–unfriendliness of tool outputs.
  - Developed tool using 13 artifacts including 7 unanalyzed artifacts and 3 not working artifacts on existing tool

Future Study

- Tool for track and explain the trace of file sharing

Thank you.

https://github.com/MacD0nald/MacSharingForensic