2022년 전체 세미나

Cellebrite Inspector

2022-04-29

손지훈
hunjison@korea.ac.kr
Digital Forensic Research Center
Institute of Cyber Security & Privacy, Korea University.

목차

- Macquisition을 이용한 데이터 획득
- Cellebrite Inspector을 이용한 데이터 분석
- 마무리

대상	버전
Mac Air Mid 2012	MacOS X Mojave(10.14.6) MacOS X Catalina(10.15.7)
Macquisition	2020R1
Cellebrite Inspector	10.4
Windows VM	Windows 10 x64 (테스트용 이미지)

Macquisition을 이용한 데이터 획득

Macquisition을 이용한 데이터 획득

Macquisition

- **BlackBag의 Mac 컴퓨터용 자료 획득 도구**
  - 현재 Cellebrite로 인수, Cellbrite Digital Collector로 이름 변경
- **Hardware Acquisition tool + Software write-block 결합**
  - 획득을 위해서 Macquisition 이외의 별도의 도구가 필요하지 않음

Macquisition을 이용한 데이터 획득

Macquisition

- **Boot with Macquisition(오늘 이용할 방법)**
  - Macquisition을 부팅디스크로 이용하는 방법
  - 부팅디스크 연결, 전원 버튼 누르고 Option 키
- **Target Disk Mode**
  - Mac에서 Mac으로 데이터를 전달하는 방법
  - 진입 방법
    - Intel Mac: 종료 후 T 키 + 전원 // 설정 – 시동디스크
    - Apple Silicon: 종료 후 전원버튼 길게 – 디스크 공유
- **(ETC) Live Forensics**
  - Triage
  - Live Acquisition

Macquisition을 이용한 데이터 획득

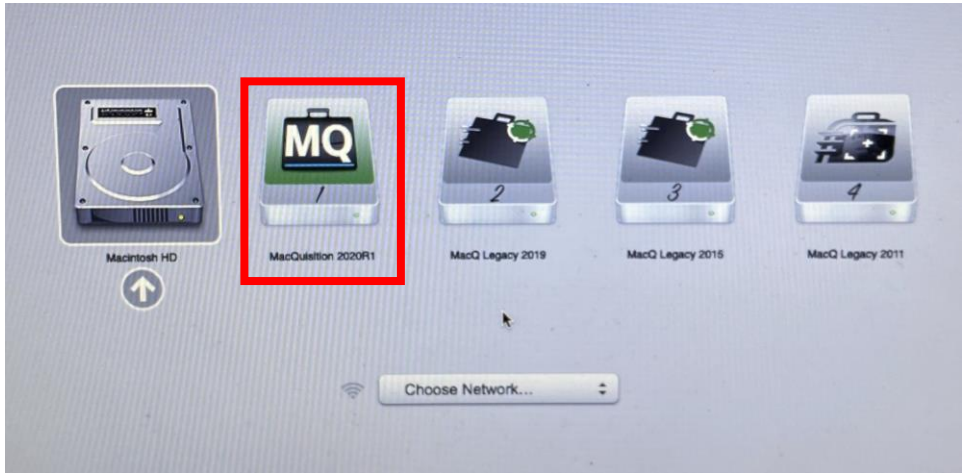
Macquisition

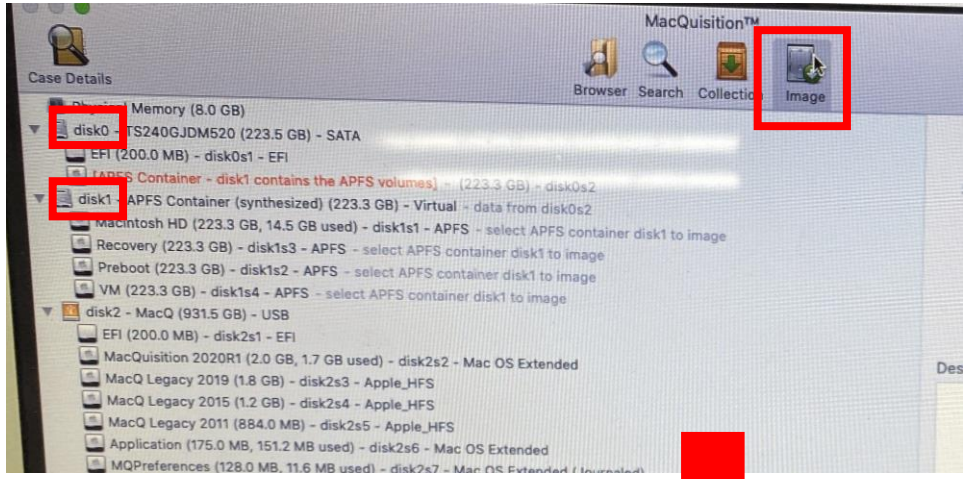
- **배경지식**
  - Firmware password: 부팅 시에 요구되는 패스워드
    - 패스워드 모르면 이미징 불가능 → (다행히) 기본 설정이 아니라 선택사항
    - Apple Silicon 모델에서는 FileVault로 일원화
  - FileVault: 디스크 암호화 패스워드
    - 체크해제하지 않을 경우 기본 설정
    - FileVault만 단독으로 설정될 경우에는 도구에서 암호화 해제 가능
  - T2 chip: 애플의 보안 칩
    - T2 + FileVault가 설정될 경우에는 FileVault 해제 후 획득 절차 진행해야 함
      (해제를 위해서는 iCloud 로그인 or Recovery Key 요구됨)

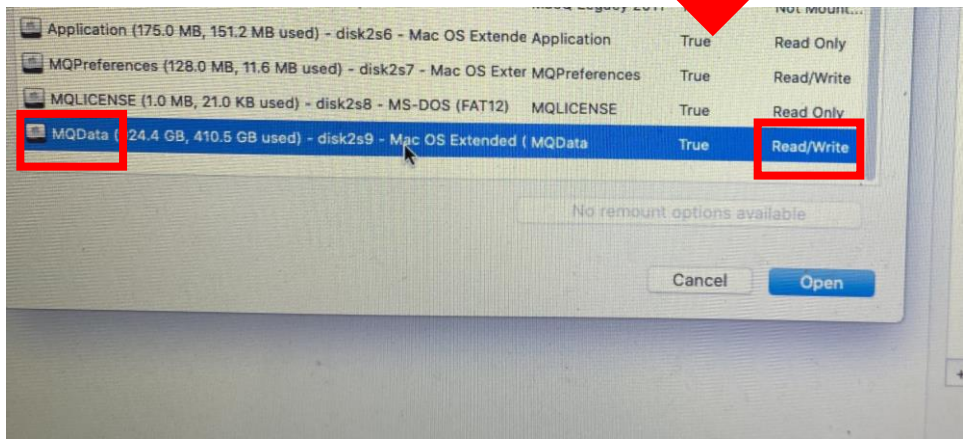
Macquisition을 이용한 데이터 획득

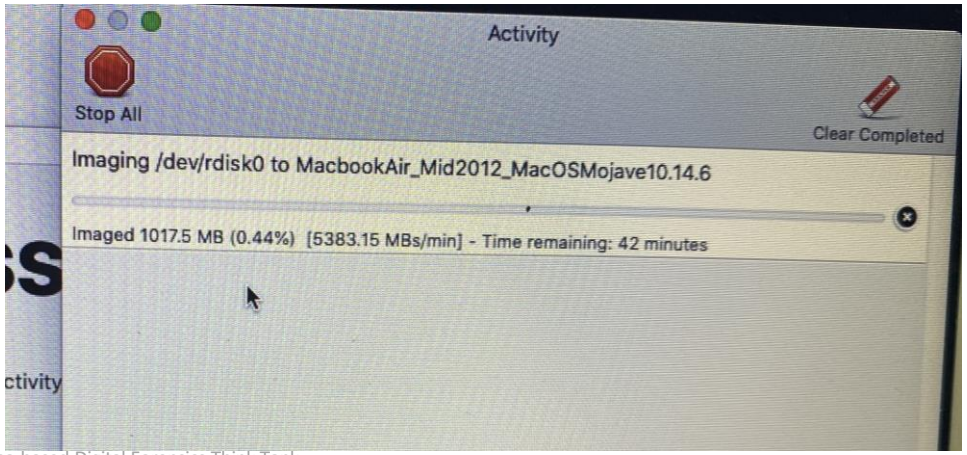
Macquisition

- 획득과정





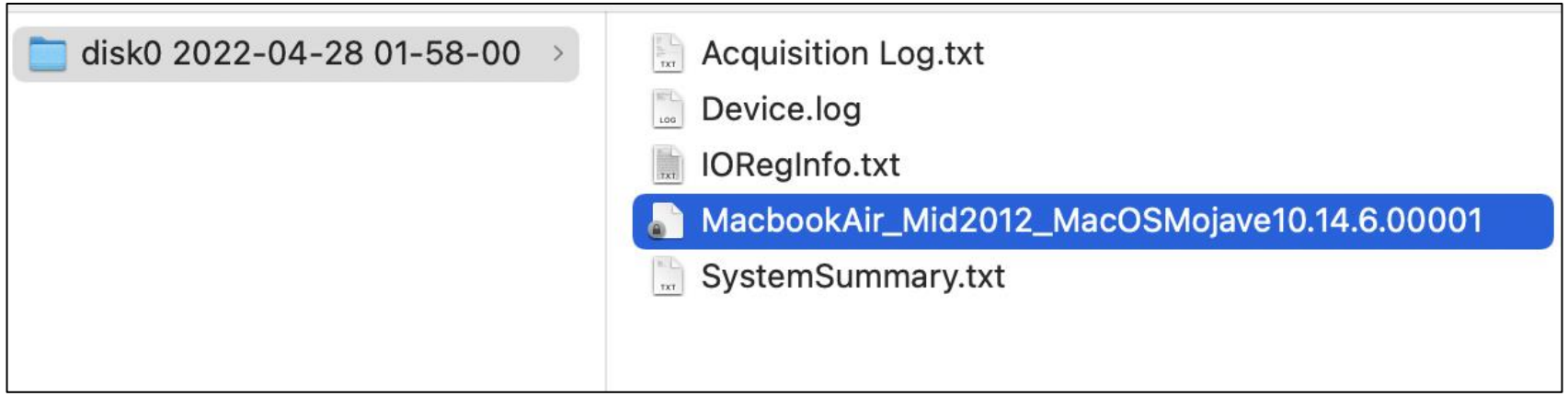




Macquisition을 이용한 데이터 획득

Macquisition

- **획득과정**
  - 획득 완료!



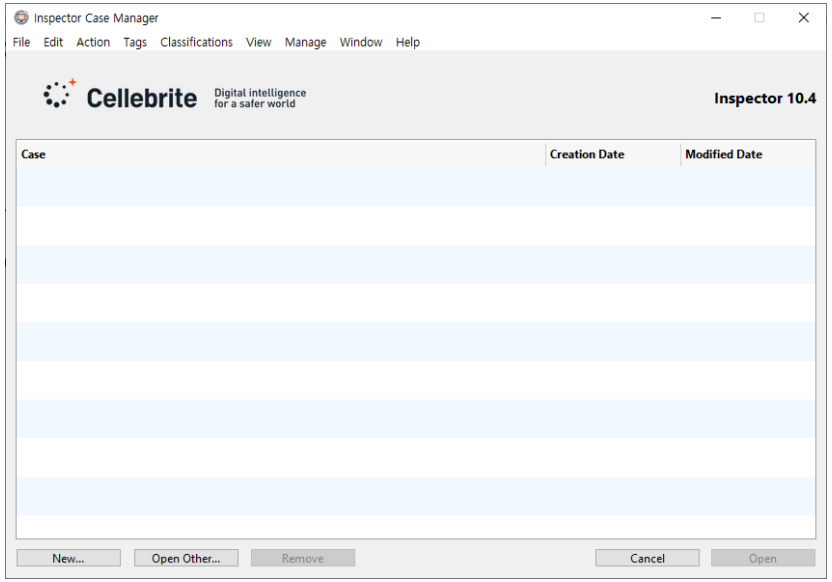
Cellebrite Inspector을 이용한 데이터 분석

Cellebrite Inspector을 이용한 데이터 분석

Cellebrite Inspector

- **Blacklight, BlackBag의 이미지 분석 도구**
  - 현재 Cellebrite로 인수, Cellbrite Inspector로 이름 변경
- **설치 과정**
  - 프로그램 설치 파일을 통해 설치한 후,

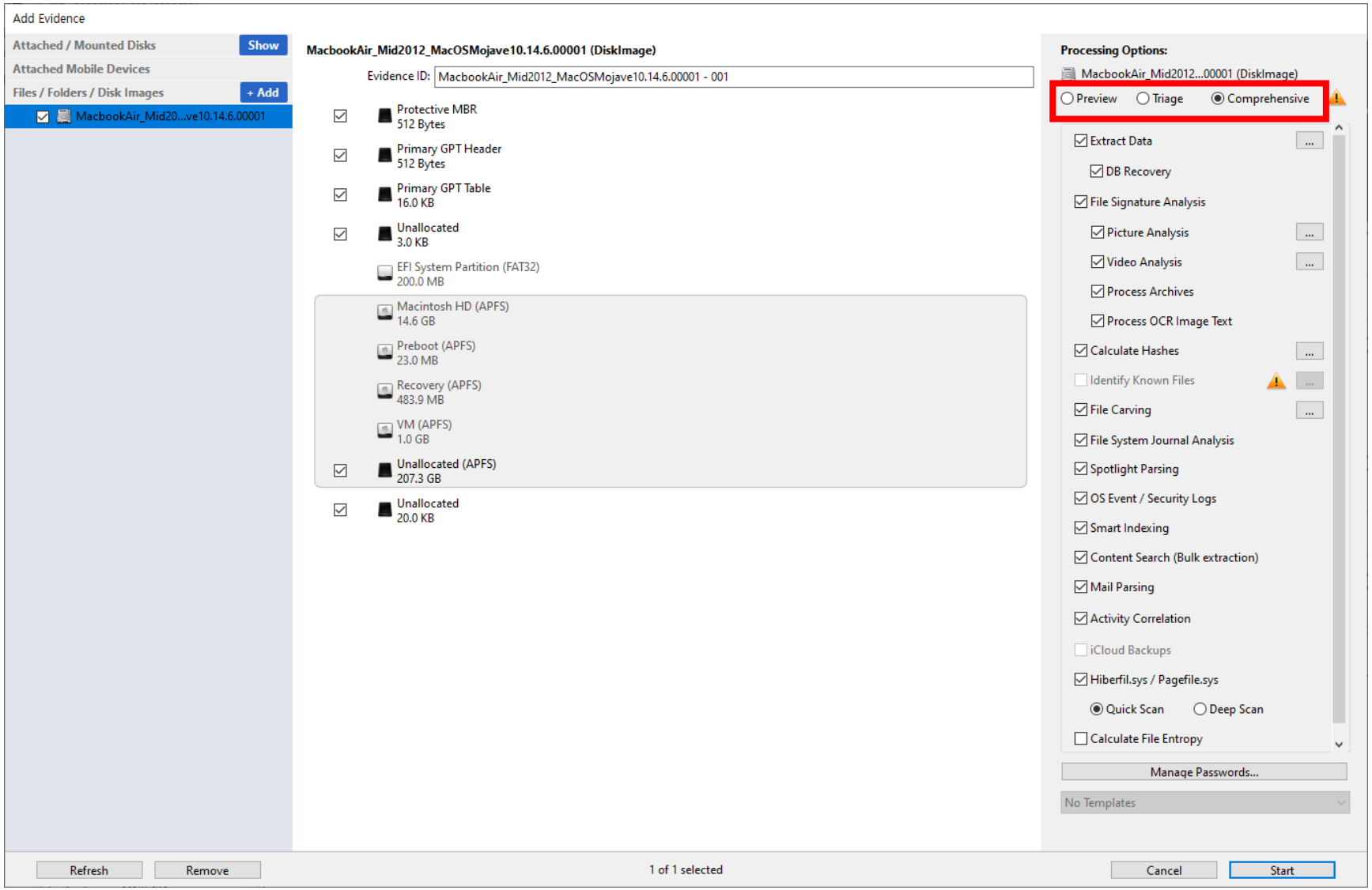
    Cellebrite Licence Loader(X) Manager(O)를 통해 동글 인증
- **설치 완료!**



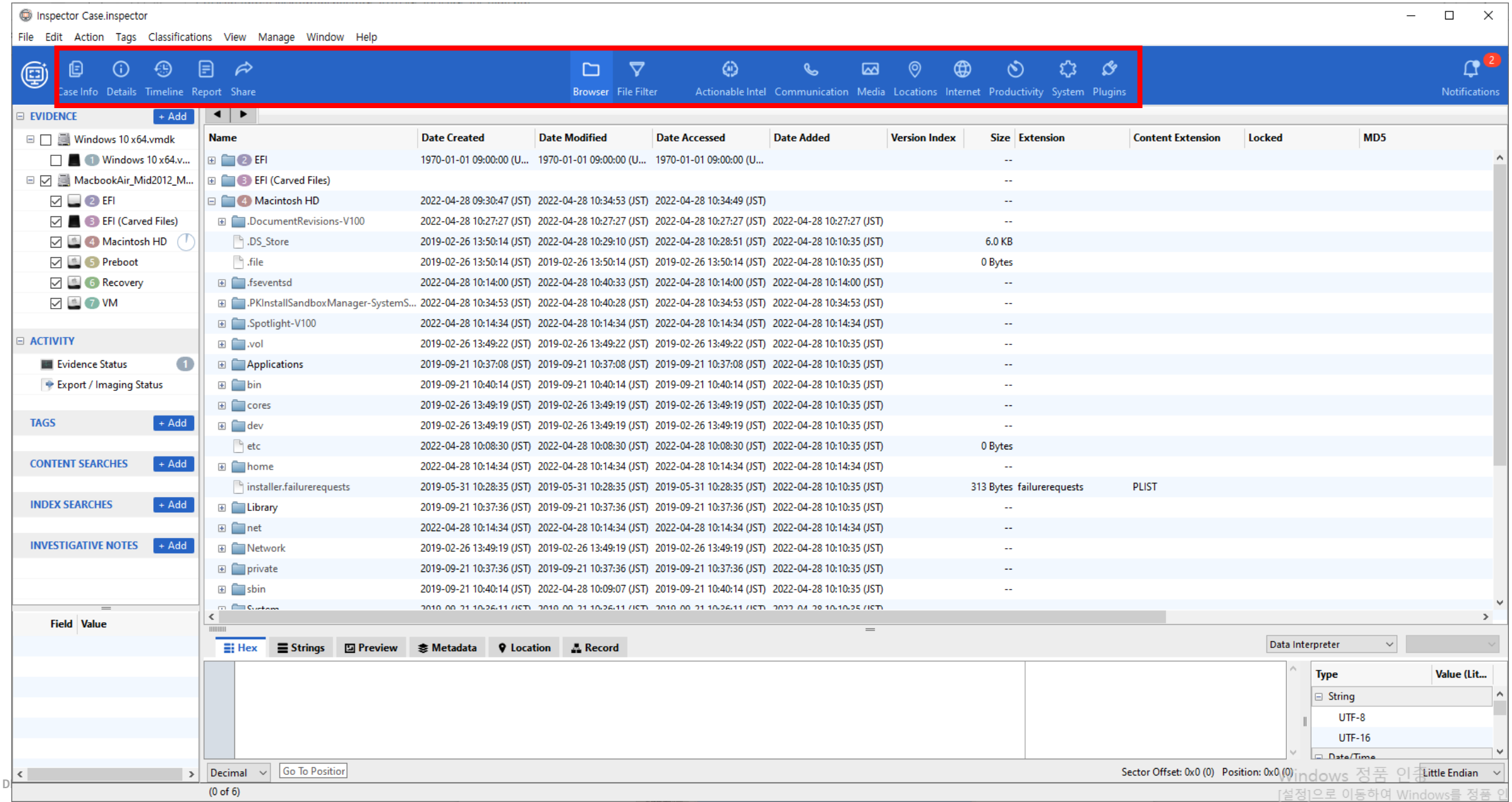
Cellebrite Inspector을 이용한 데이터 분석

Cellebrite Inspector

- **분석 과정**
  - Preview
    - 단순 파일시스템 조회
  - Triage(표준)
    - 사용자 지정 옵션
  - Comprehensive
    - 모든 옵션 사용

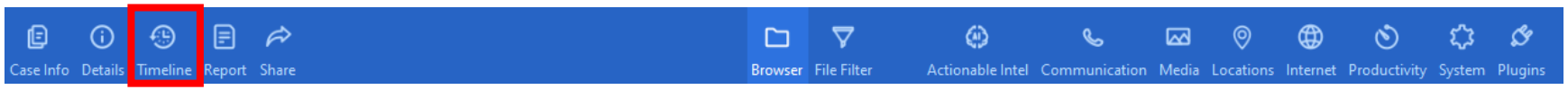


Cellebrite Inspector을 이용한 데이터 분석

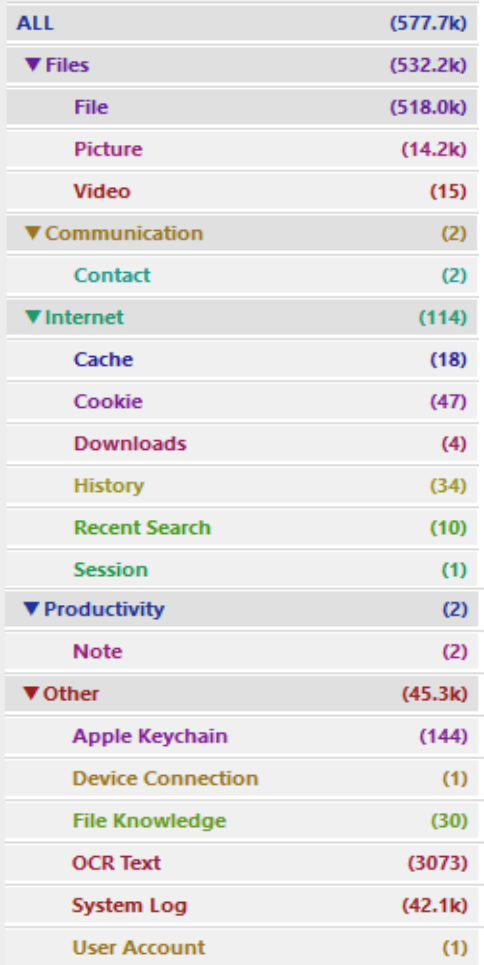


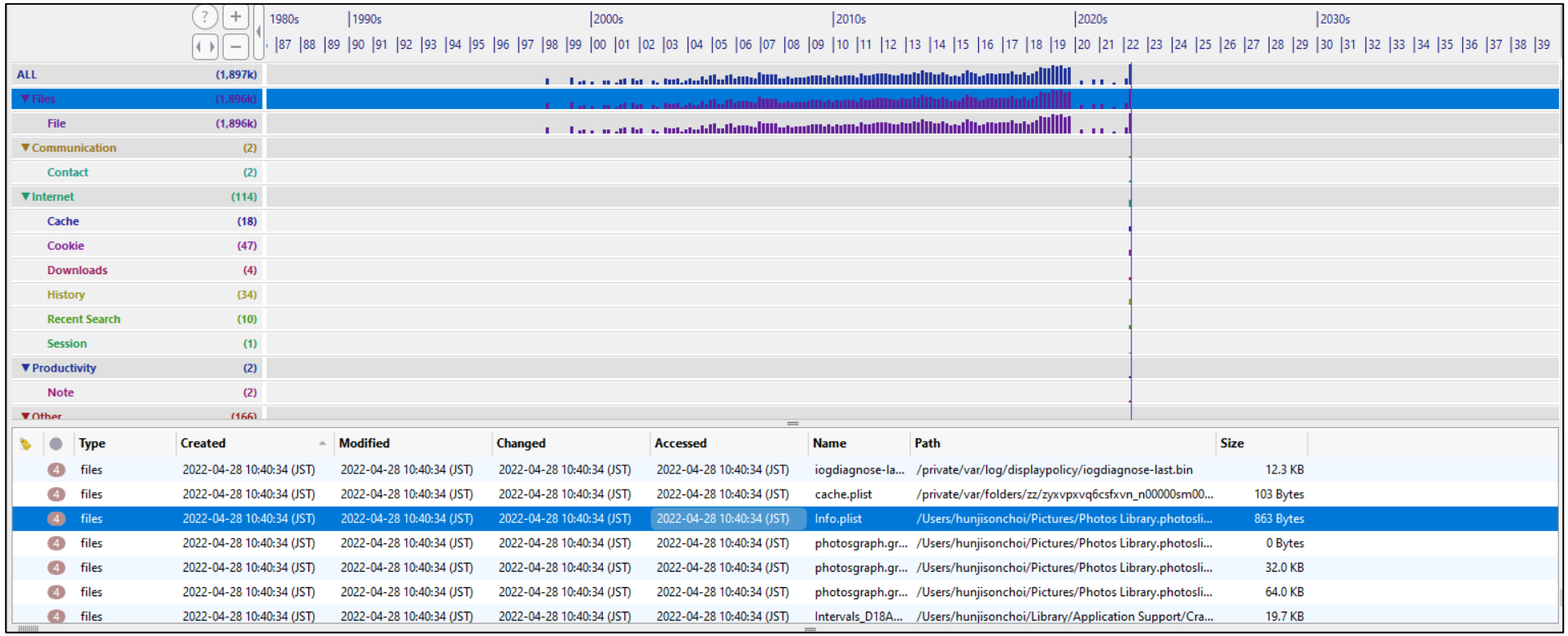
Cellebrite Inspector을 이용한 데이터 분석

Timeline



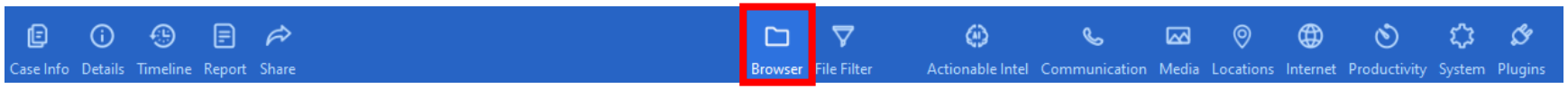
- 타임라인
  - 사용자의 행위를 시간 순서대로 조회할 수 있음





Cellebrite Inspector을 이용한 데이터 분석

Browser

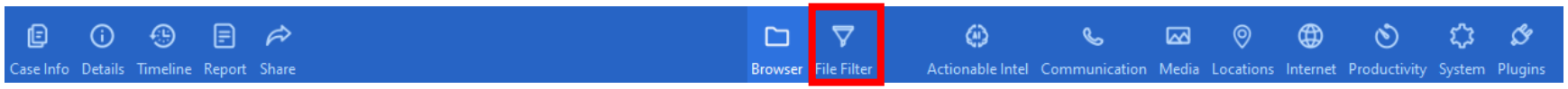


- 브라우저
  - 전체 폴더 구조 조회

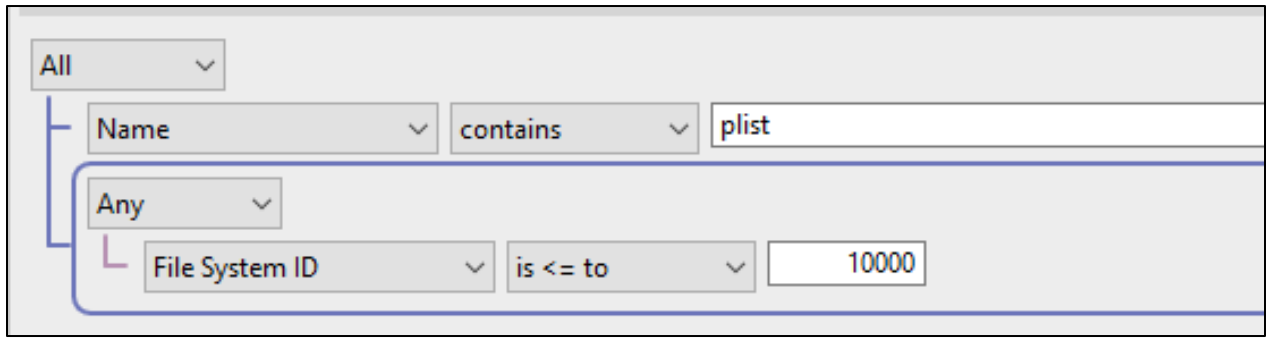
Name	Date Created	Date Modified	Date Accessed	Date Added	Version Index	Size	Extension	Content Extension
2 EFI	1970-01-01 09:00:00 (U...	1970-01-01 09:00:00 (U...	1970-01-01 09:00:00 (U...			--		
3 EFI (Carved Files)						--		
4 Macintosh HD	2022-04-28 09:30:47 (JST)	2022-04-28 10:34:53 (JST)	2022-04-28 10:34:49 (JST)			--		
5 Preboot	2017-11-30 17:30:56 (JST)	2022-04-28 09:55:56 (JST)	2017-11-30 17:30:56 (JST)			--		
6 Recovery	2017-11-30 17:30:57 (JST)	2022-04-28 09:55:56 (JST)	2017-11-30 17:30:57 (JST)			--		
7 VM	2017-11-30 18:02:40 (JST)	2022-04-28 10:35:12 (JST)	2017-11-30 18:02:40 (JST)			--		
1 Windows 10 x64.vmdk (Carved Files)						--		

Cellebrite Inspector을 이용한 데이터 분석

File Filter

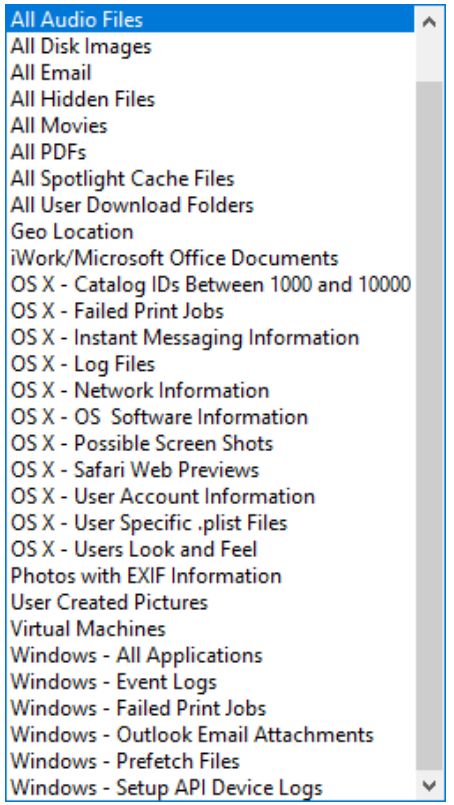


- **파일 필터**
  - 전체 파일 중에 필터에 맞는 파일들 조회 가능



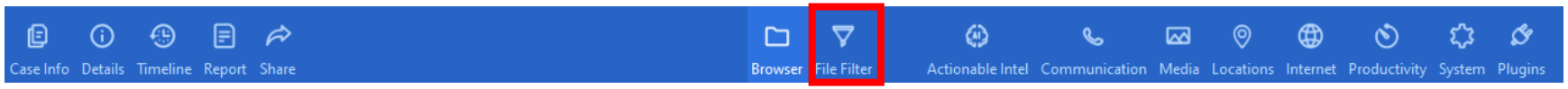
BL ID	FS ID	Name	Size	Date Created	Date Modified
1120924	6385	VersionInfo.plist	2.4 KB	2019-04-19 10:36:22 (JST)	2019-04-19 10:36:22 (JST)
1120991	6361	Info.plist	2.1 KB	2019-04-19 10:36:22 (JST)	2019-04-19 10:36:22 (JST)
1120992	6508	version.plist	503 Bytes	2019-04-19 10:40:55 (JST)	2019-04-19 10:40:55 (JST)
1121278	6866	InfoPlist.strings	42 Bytes	2019-04-19 11:04:31 (JST)	2019-04-19 11:04:31 (JST)
1121280	6886	InfoPlist.strings	42 Bytes	2019-04-19 10:57:15 (JST)	2019-04-19 10:57:15 (JST)

Saved Filters

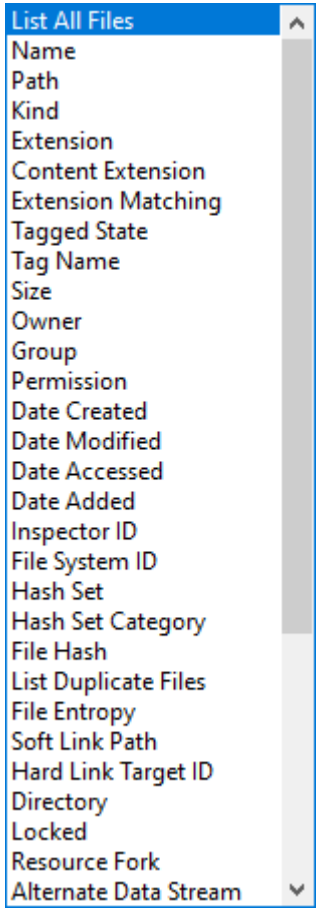


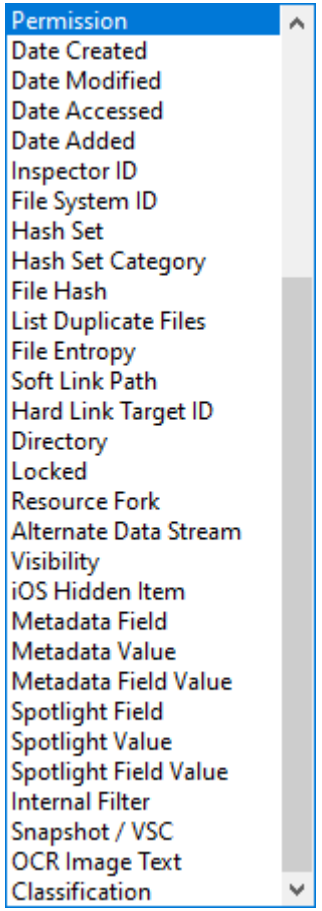
Cellebrite Inspector을 이용한 데이터 분석

File Filter



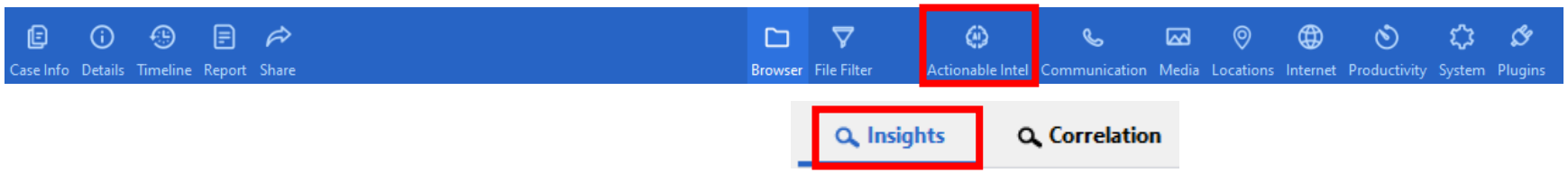
- **파일 필터**
  - 전체 파일 중에 필터에 맞는 파일들 조회 가능
  - 기본 필터
    - Name, Extension, Size, Owner, Permission, MAC time
  - 유용한 필터
    - File Entropy, Spotlight 관련, Locked, OCR Image Text





Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



- **User Action**
  - 유저의 활동과 관련된 아티팩트

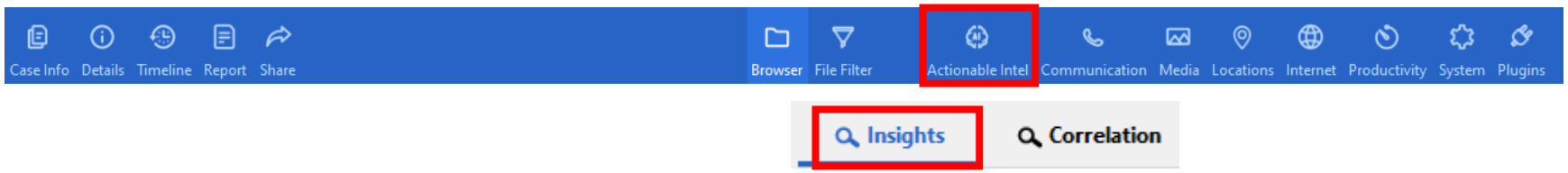
항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Knowledge	Recent Items, Trash Items
Passwords	Apple Keychain
Program Execution	윈도우 전용
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적

Mac

Windows

Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



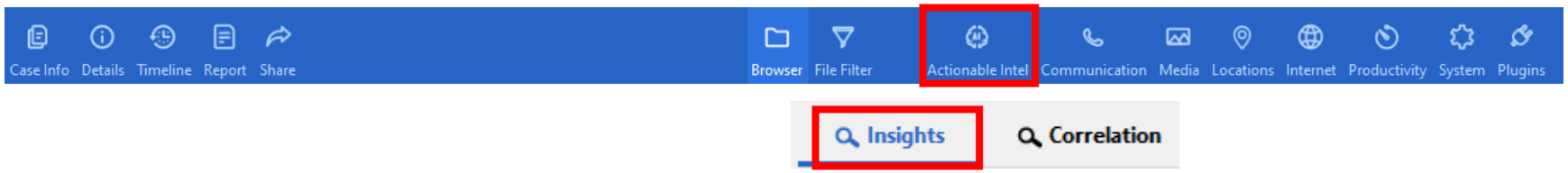
- **User Action**
  - 유저의 활동과 관련된 아티팩트

항목	내용
Device Backups	iOS, iPadOS 백업
Device Connectio	
Account Usage	
Downloads	
File Knowledge	
Passwords	Apple Keychain
Program Execution	윈도우 전용
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적

Name	Model	Phone Number	Last Backup Date	OS Version	Serial Number	UDID	IMEI	Jailbroken
17 hunjison의 iPhone	iPhone 11 Pro	+82 10-8996-7156	2022-05-06 10:22:25 (JST)	15.0.2	DNPZMCU3N6Y9	00008030-000D553E3AC2802E	353833104383358	Unknown

Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



- **User Action**
  - 유저의 활동과 관련된 아티팩트

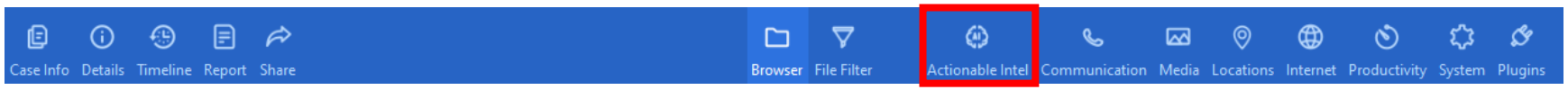
항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파
File Knowledge	Recent Items, Trash Items
Passwords	Apple Keychain
Program Execution	윈도우 전용
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적

Product Name	Serial Number	Last Connected Date	User Name	Vendor
Name: ASM1051E SATA 6Gb/s ...	BBAA000000000003166	2022-05-06 10:35:18 (JST)	Unknown	ASMedia Technology Inc.
Name: ASM1051E SATA 6Gb/s ...	BBAA000000000003166	2022-05-06 10:35:18 (JST)	Unknown	ASMedia Technology Inc.
iPhone	DNPZMCU3N6Y9	2022-05-06 10:17:56 (JST)	hunjisonchoi	Apple, Inc.
Internal Memory Card Reader	000000000310	2022-05-06 08:20:09 (JST)	Unknown	Apple, Inc.

Product Name	Device Description	Class	Serial Number	First Connected Date	Last Connected Date
Virtual USB Hub	Generic USB Hub	USB		2022-04-27 10:44:24 (JST)	2022-04-27 10:44:24 (JST)
Virtual USB Hub	Generic USB Hub	USB		2022-04-27 10:44:24 (JST)	2022-04-27 10:44:24 (JST)
Virtual Mouse	USB Input Device	USB		2022-04-26 10:56:14 (JST)	2022-04-26 10:25:50 (JST)
Virtual Mouse	USB Input Device	USB		2022-04-26 10:56:14 (JST)	2022-04-26 10:25:50 (JST)
Virtual Mouse	USB Composite Device	USB		2022-04-26 10:56:14 (JST)	2022-04-26 10:25:50 (JST)

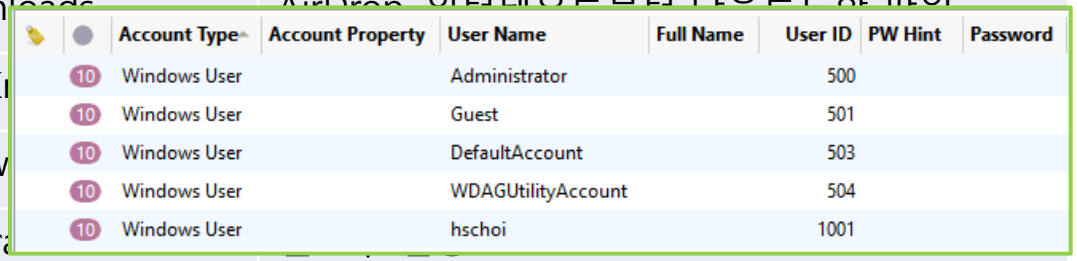
Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel

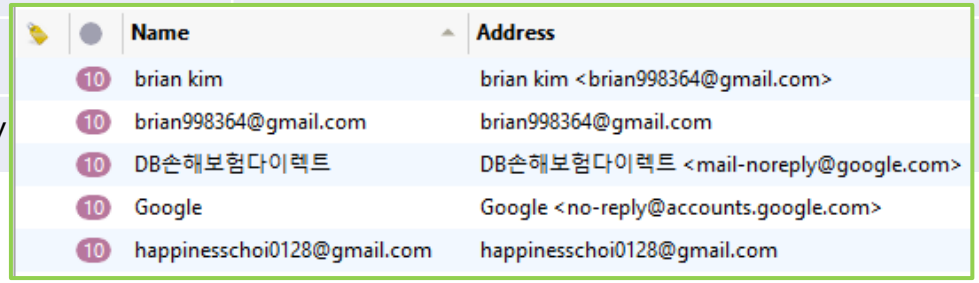


- **User Action**
  - 유저의 활동과 관련된 아티팩트

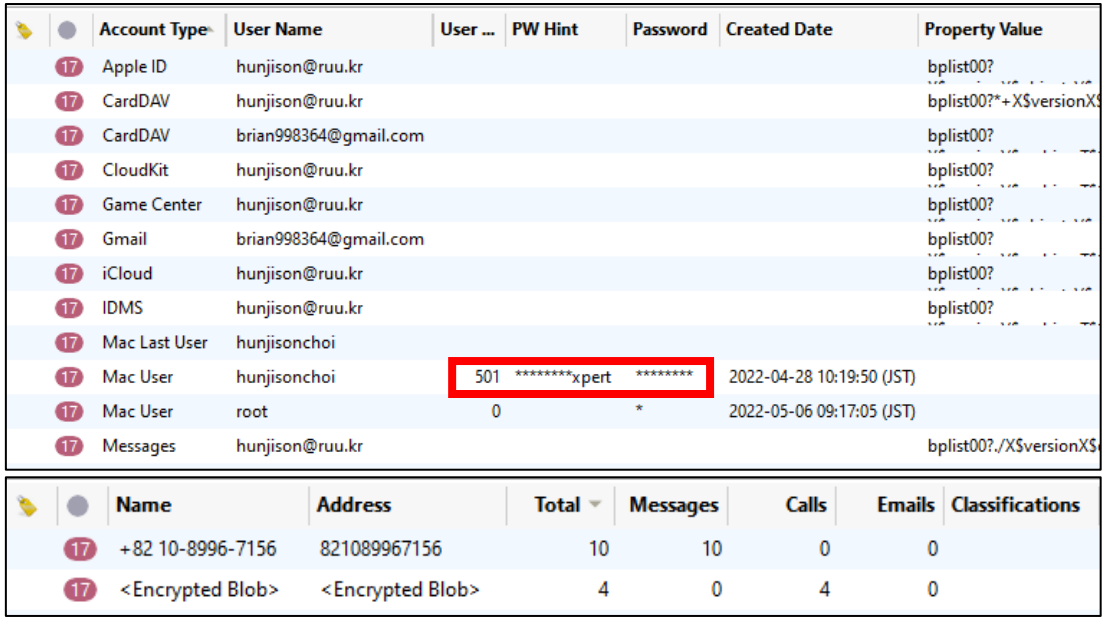
항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보, 연락처 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Ki	
Passw	
Progra	
Search	
Activity	



Account Type	Account Property	User Name	Full Name	User ID	PW Hint	Password
Windows User		Administrator		500		
Windows User		Guest		501		
Windows User		DefaultAccount		503		
Windows User		WDAGUtilityAccount		504		
Windows User		hschoi		1001		



Name	Address
brian kim	brian kim <brian998364@gmail.com>
brian998364@gmail.com	brian998364@gmail.com
DB손해보험다이렉트	DB손해보험다이렉트 <mail-noreply@google.com>
Google	Google <no-reply@accounts.google.com>
happinesschoi0128@gmail.com	happinesschoi0128@gmail.com

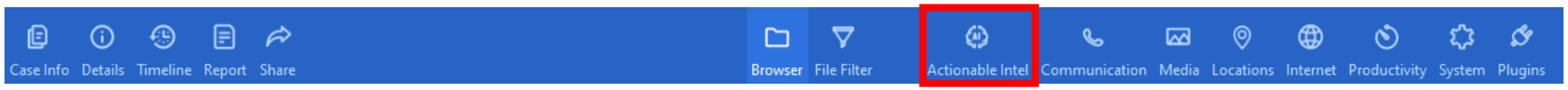


Account Type	User Name	User ...	PW Hint	Password	Created Date	Property Value
Apple ID	hunjison@ruu.kr					bplist00?
CardDAV	hunjison@ruu.kr					bplist00?*+X$versionX$
CardDAV	brian998364@gmail.com					bplist00?
CloudKit	hunjison@ruu.kr					bplist00?
Game Center	hunjison@ruu.kr					bplist00?
Gmail	brian998364@gmail.com					bplist00?
iCloud	hunjison@ruu.kr					bplist00?
IDMS	hunjison@ruu.kr					bplist00?
Mac Last User	hunjisonchoi					
Mac User	hunjisonchoi	501	********xpert	********	2022-04-28 10:19:50 (JST)	
Mac User	root	0		*	2022-05-06 09:17:05 (JST)	
Messages	hunjison@ruu.kr					bplist00?./X$versionX$

Name	Address	Total	Messages	Calls	Emails	Classifications
+82 10-8996-7156	821089967156	10	10	0	0	
<Encrypted Blob>	<Encrypted Blob>	4	0	4	0	

Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



- **User Action**
  - 유저의 활동과 관련된 아티팩트

항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Knowledge	Recent Items, Trash Items
Passwords	Apple Keychain
Program Execution	윈도우 전용
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적

Date	File Name	File Path	Sender Name	Recipients	Type	Direction
17 2022-05-06 08:46:17 (JST)	IMG_2058.HEIC	/Users/hunjis...	hunjison의 iPhone	hunjison c...	Preview.app Document	Inbound
17 2022-05-06 08:46:17 (JST)	IMG_2058.HEIC	/Users/hunjis...	hunjison의 iPhone	hunjison c...	Preview.app Document	Inbound
17 2022-05-06 08:45:40 (JST)	For_ICLOUD.jpg	/Users/hunjis...	hunjison의 iPhone	hunjison c...	JPEG image	Inbound
17 2022-05-06 08:45:40 (JST)	For_ICLOUD.jpg	/Users/hunjis...	hunjison의 iPhone	hunjison c...	JPEG image	Inbound
17 2022-05-06 08:45:03 (JST)	pdf-test.pdf	/Users/hunjis...			PDF document	Outbound

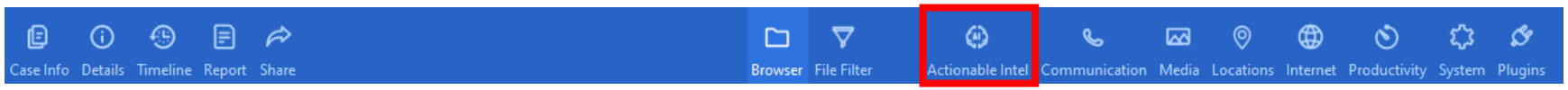
Source	File Name	File Path	Time Stamp	Url	Sender Name
17 Safari			2022-05-06 08:43:44 (JST)	https://www.orimi.com/pdf-test.pdf	
17 sharingd			2022-05-06 08:45:39 (JST)		hunjison의 iPhone
17 sharingd			2022-05-06 08:46:16 (JST)		hunjison의 iPhone

Source	File Name	File Path	Time Stamp	Url
4 Safari	imgres-4.html	/Users/hunji...	2022-04-28 10:29:44 (JST)	https://www.google.com/imgres?
4 Safari	imgres-3.html	/Users/hunji...	2022-04-28 10:29:43 (JST)	https://www.google.com/imgres?
4 Safari	imgres-2.html	/Users/hunji...	2022-04-28 10:29:30 (JST)	https://www.google.com/imgres?
4 Safari	imgres.html	/Users/hunji...	2022-04-28 10:29:27 (JST)	https://www.google.com/imgres?

Source	File Name	File Path	Time Stamp	Url
10 Chrome	ZoomInstaller.exe	C:\Users\hschoi...	2022-04-26 13:34:29 (JST)	https://cdn.zoom.us/prod...

Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



- **User Action**
  - 유저의 활동과 관련된 아티팩트

항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Knowledge	Recent Items, Trash Items
Search	
Activity	

User	Type	Label	Item Name	Path
hunjisonchoi	Shared File List 2	Favorite Items	myDocuments.cannedSearch	file:///System/Library/CoreServices/Finder.app/
hunjisonchoi	Shared File List 2	Favorite Items	Applications	file:///Applications
hunjisonchoi	Shared File List 2	Favorite Items	Desktop	file:///Users/hunjisonchoi/Desktop
hunjisonchoi	Shared File List 2	Favorite Items	Documents	file:///Users/hunjisonchoi/Documents
hunjisonchoi	Shared File List 2	Favorite Items	Downloads	file:///Users/hunjisonchoi/Downloads
hunjisonchoi	Shared File List 2	Recent Applications	Photo Booth	file:///Applications/Photo Booth.app
hunjisonchoi	Shared File List 2	Recent Applications	Mail	file:///Applications/Mail.app
hunjisonchoi	Shared File List 2	Recent Applications	Reminders	file:///Applications/Reminders.app
hunjisonchoi	Shared File List 2	Recent Applications	Maps	file:///Applications/Maps.app
hunjisonchoi	Shared File List 2	Recent Applications	Photos	file:///Applications/Photos.app
hunjisonchoi	Shared File List 2	Recent Applications	Stickies	file:///Applications/Stickies.app
hunjisonchoi	Shared File List 2	Recent Applications	Notes	file:///Applications/Notes.app
hunjisonchoi	Shared File List 2	Recent Applications	Safari	file:///Applications/Safari.app
hunjisonchoi	Shared File List 2	Recent Applications	System Preferences	file:///Applications/System Preferences.app

File Name	Lnk Target	Target Path
ODBC Data Sources (32-bit).lnk	syswow64	%windir%\syswow64
MultiPoint Dashboard.lnk	Windows MultiPoint Server	%ProgramFiles%\Windows MultiPoint Server

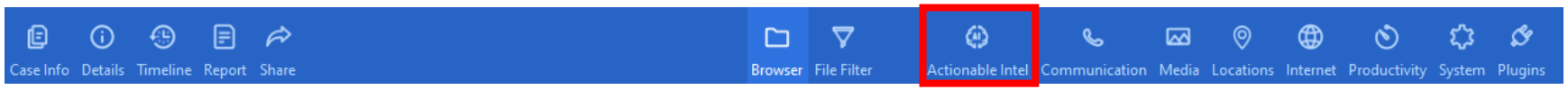
User	Type	Item Name	Path	Date	Index Value
hschoi	Folder	kglcheck/			0
hschoi	Applications	notepad.exe		2022-04-27 10:45:59 (JST)	0
hschoi	Folder	인터넷			1

User	File ...	Trash Name	Original Path	Deleted Date	Size
hschoi	ㅇ.txt	$RPC9UNH.txt	C:\Users\hschoi\Desktop\ㅇ.txt	2022-05-04 13:40:27 (JST)	646

User	File Name	Trash Name	Original Path	Deleted Date	Size	Classifications
EFI	501		/.Trashes/501		512	
EFI	._501		/.Trashes/._501		4096	
Preboot	501		/.Trashes/501		0	
Recovery	501		/.Trashes/501		0	

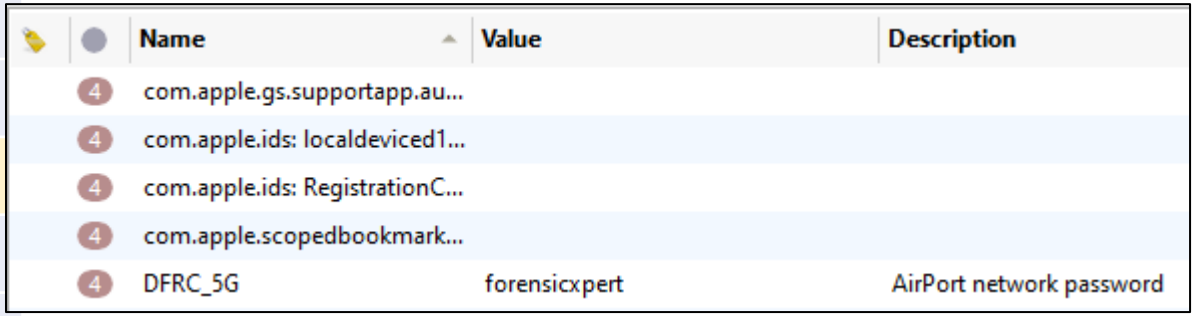
Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



- **User Action**
  - 유저의 활동과 관련된 아티팩트

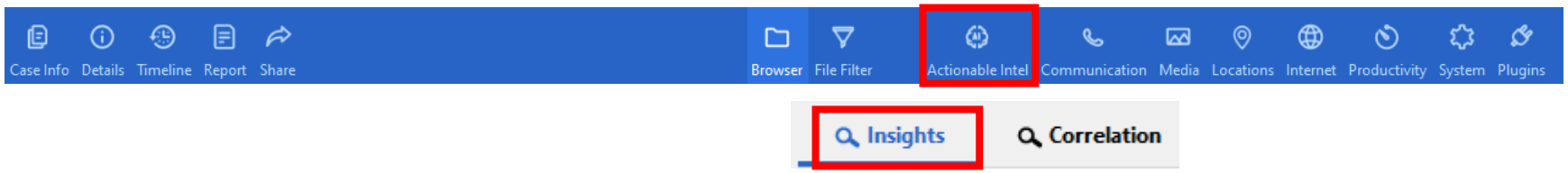
항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Knowledge	Recent Items, Trash Items
Passwords	Apple Keychain
Program Execution	윈도우 전용
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적



Name	Value	Description
com.apple.gs.supportapp.au...		
com.apple.ids: localdeviced1...		
com.apple.ids: RegistrationC...		
com.apple.scopedbookmark...		
DFRC_5G	forensicxpert	AirPort network password

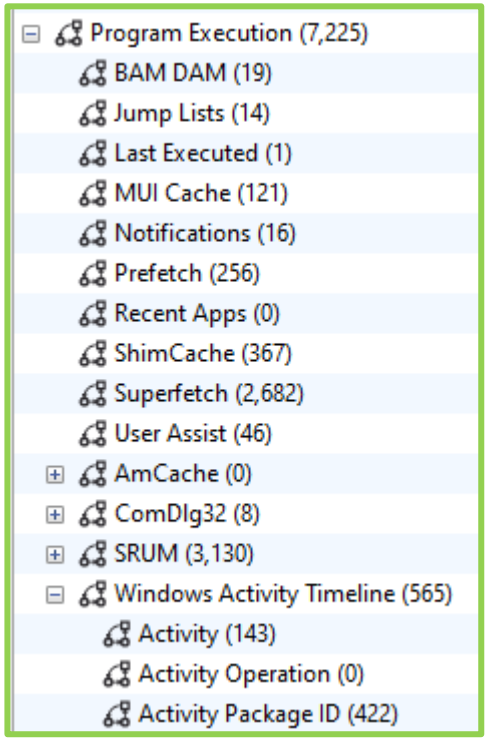
Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



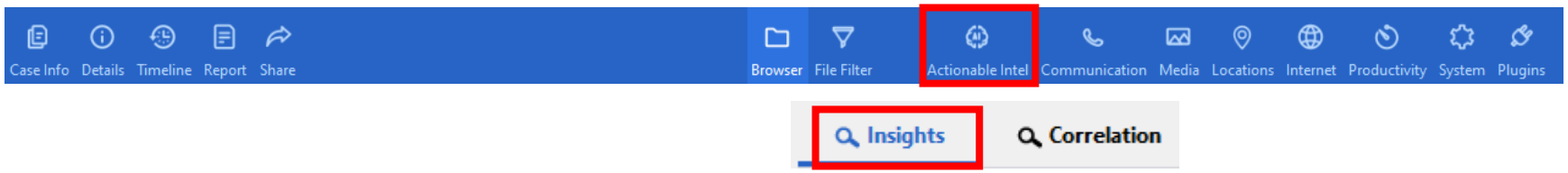
- **User Action**
  - 유저의 활동과 관련된 아티팩트

항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Knowledge	Recent Items, Trash Items
Passwords	Apple Keychain
Program Execution	응용프로그램 실행 흔적
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적



Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel



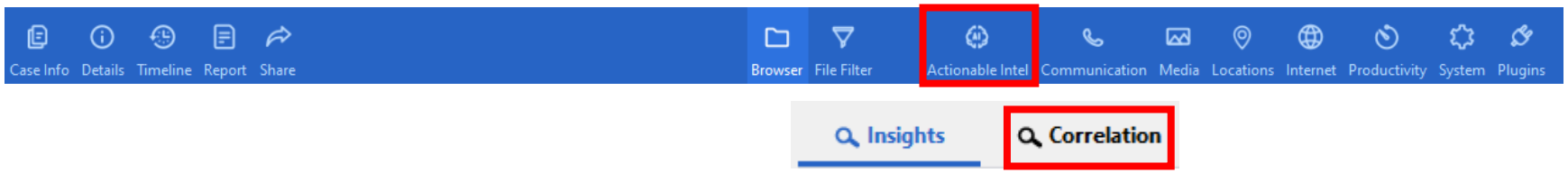
- **User Action**
  - 유저의 활동과 관련된 아티팩트

항목	내용
Device Backups	iOS, iPadOS 백업
Device Connections	iPhone, SD Card 등 연결된 디바이스
Account Usage	유저 계정 정보
Downloads	AirDrop, 인터넷으로부터 다운로드한 파일
File Knowledge	Recent Items, Trash Items
Passwords	Apple Keychain
Program Execution	윈도우 전용
Search	Spotlight Shortcuts
Activity Correlation	사용자 행위 추적

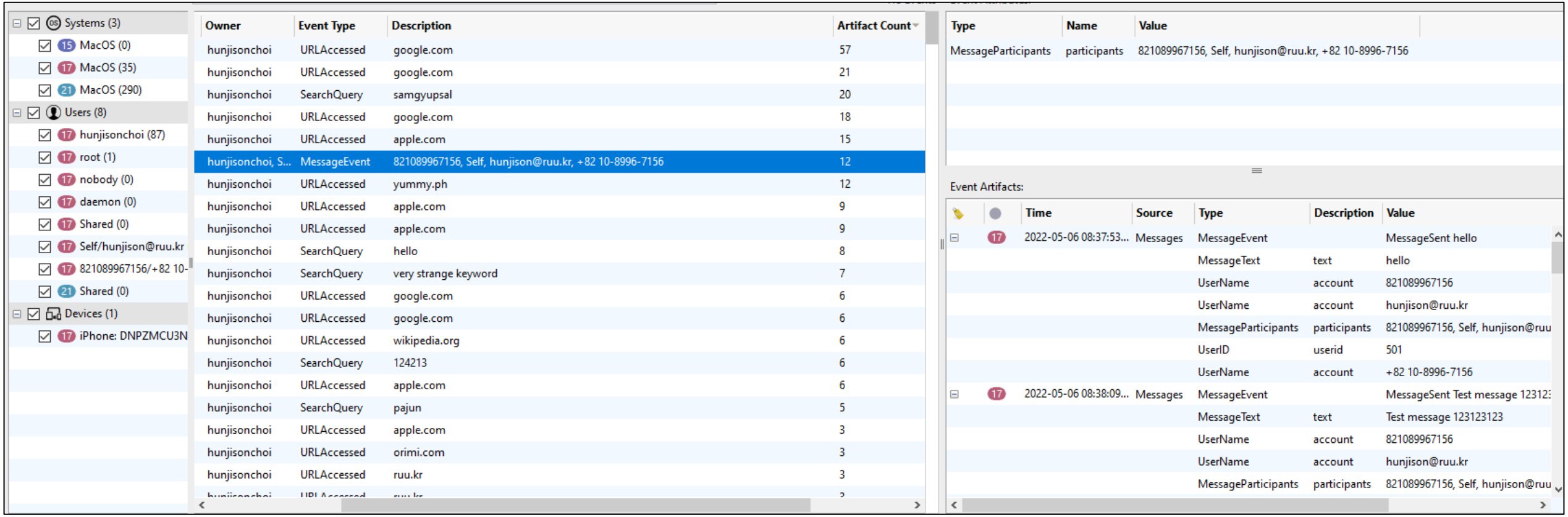
User	Typed	Display Name	Last Used	URL
hunjisonchoi	aird	AirDrop	2022-05-06 08:45:14 (JST)	/System/Library/CoreServices/Finder.ap
hunjisonchoi	iclo	iCloud Drive	2022-05-06 08:42:59 (JST)	/System/Library/CoreServices/Finder.ap
hunjisonchoi	icl	iTunes	2022-05-06 08:42:47 (JST)	file:///Applications/iTunes.app/
hunjisonchoi	apps	App Store	2022-05-06 08:21:17 (JST)	/System/Applications/App Store.app

Cellebrite Inspector을 이용한 데이터 분석

Actionable Intel

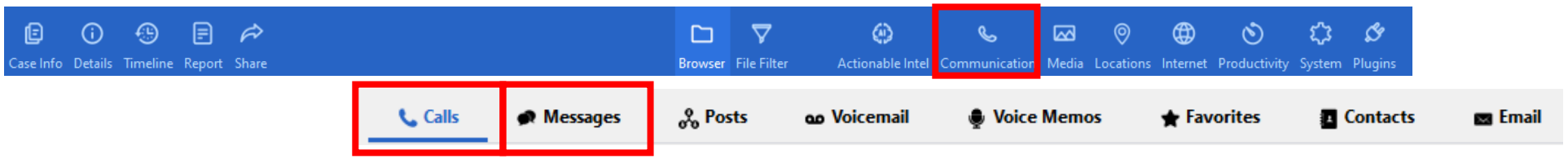


- **User Action**
  - 유저의 활동과 관련된 아티팩트



Cellebrite Inspector을 이용한 데이터 분석

Communication



- **Communication**
  - 다른 사용자와의 전화, 문자 등 대화 내역

전화

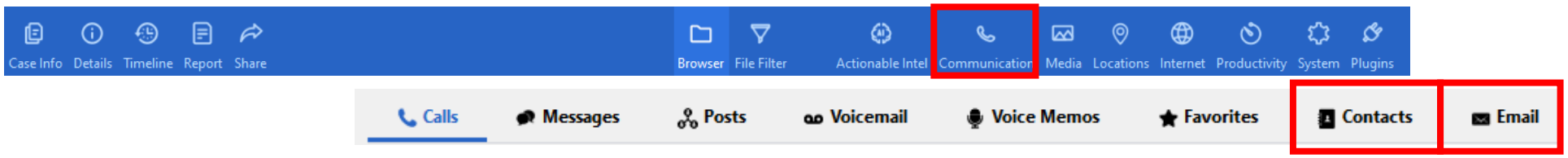
Service	Direction	Type	Date	Contacts	Duration (HH:MM:SS)
FaceTime	Outgoing	Audio	2022-05-06 08:39:36 (JST)	<Encrypted Blob>, <Encrypted Blob>	00:00:09
FaceTime	Outgoing	Video	2022-05-06 08:39:54 (JST)	<Encrypted Blob>, <Encrypted Blob>	00:00:08

문자

Service	Direction	Date	Content	Subject	Sender
iMessage	Outgoing	2022-05-06 08:37:53 (JST)	hello		Self (e:hunjison@ruu.kr)
iMessage	Outgoing	2022-05-06 08:37:53 (JST)	hello		Self (hunjison@ruu.kr)
iMessage	Outgoing	2022-05-06 08:38:09 (JST)	Test message 123123123		Self (e:hunjison@ruu.kr)
iMessage	Outgoing	2022-05-06 08:38:09 (JST)	Test message 123123123		Self (hunjison@ruu.kr)
iMessage	Outgoing	2022-05-06 08:38:27 (JST)			Self (e:hunjison@ruu.kr)
iMessage	Outgoing	2022-05-06 08:38:27 (JST)			Self (hunjison@ruu.kr)
iMessage	Outgoing	2022-05-06 08:38:27 (JST)	<Attachment - image/png - Messages Image(3919061813).png>		Self (hunjison@ruu.kr)
iMessage	Incoming	2022-05-06 08:38:38 (JST)	omg what up		+82 10-8996-7156 (821089967156)
iMessage	Incoming	2022-05-06 08:38:38 (JST)	omg what up		+82 10-8996-7156 (821089967156)

Cellebrite Inspector을 이용한 데이터 분석

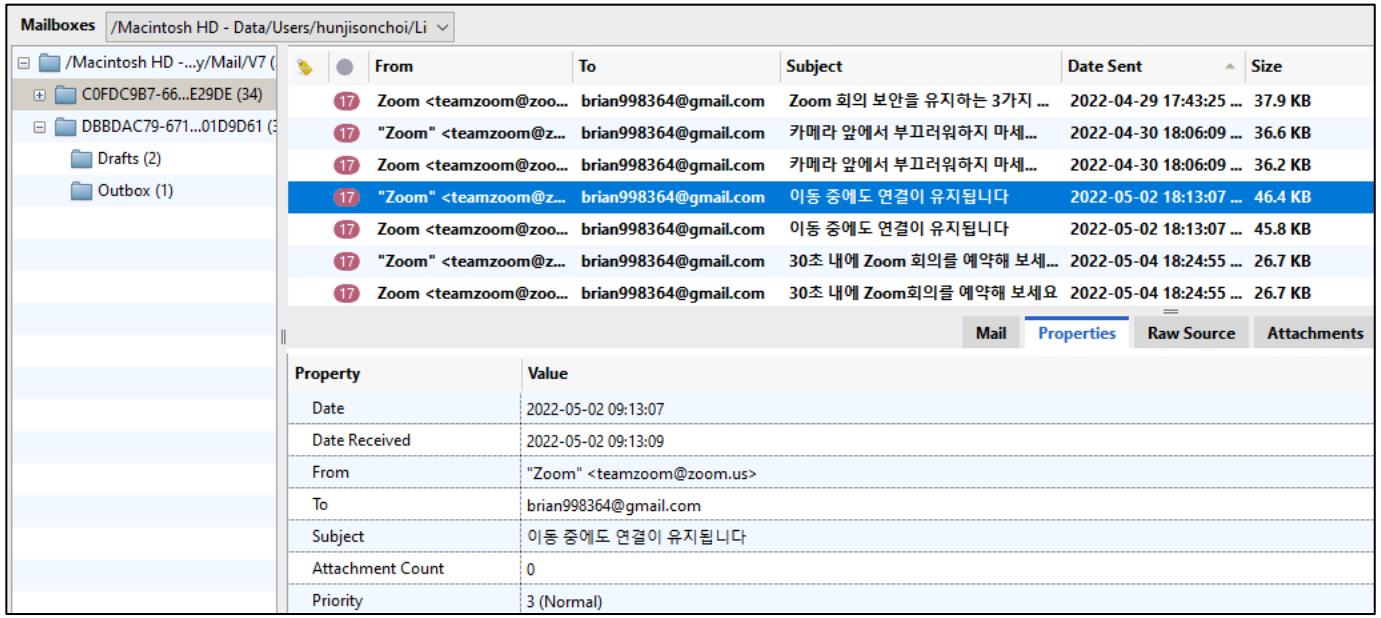
Communication



- **Communication**
  - 다른 사용자와의 전화, 문자 등 대화 내역

First	Last	Organization	Service
		애플코리아 (유...	Mac AddressBook
			Mac AddressBook
		Korea University ...	Mac AddressBook
821089967156			Recents
<Encrypted Blob>			FaceTime
Cellebrite	INSPECTOR	DFRC	Mac AddressBook
esby97@naver.com			Recents
For	Inspector		Mac AddressBook
hunjison	choi		Mac AddressBook
hunjison	choi		iChat
+82	10-8996-7156		iChat

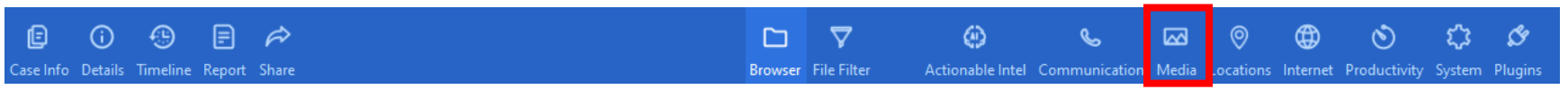
연락처



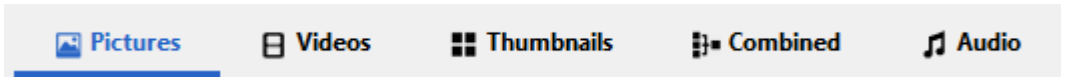
이메일

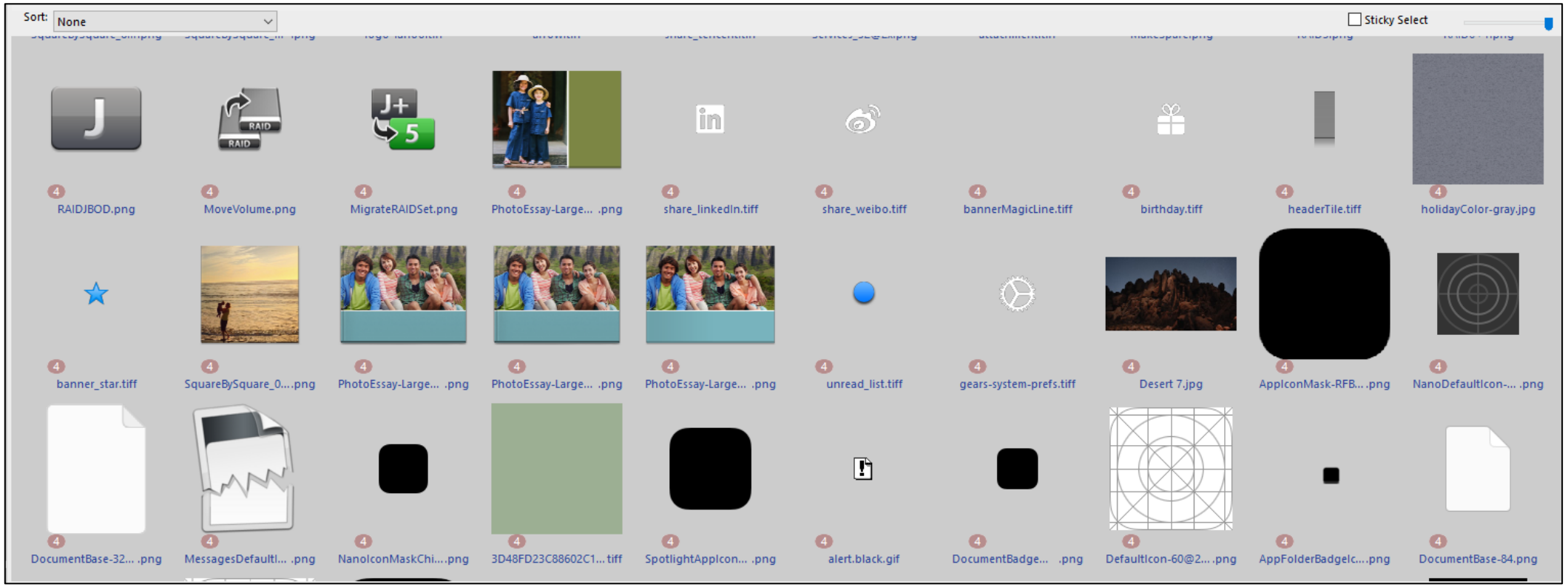
Cellebrite Inspector을 이용한 데이터 분석

Media



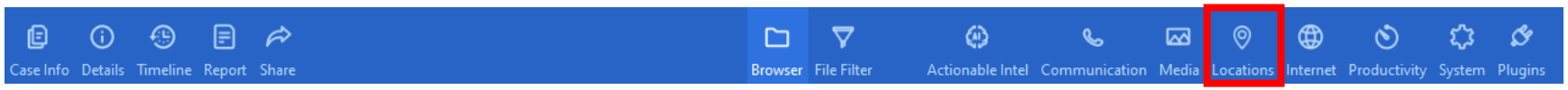
- **Media Files**
  - 사진, 비디오, 썸네일, 오디오 등 지원

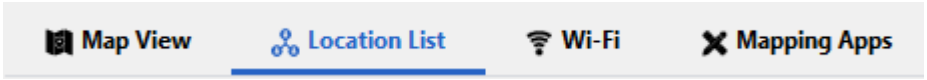




Cellebrite Inspector을 이용한 데이터 분석

Locations



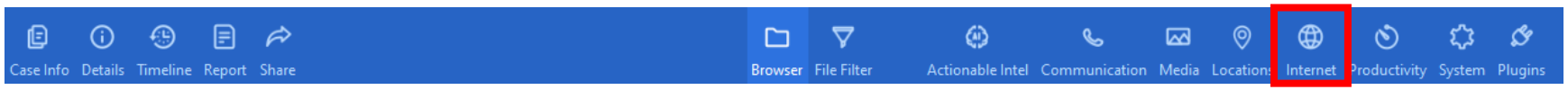


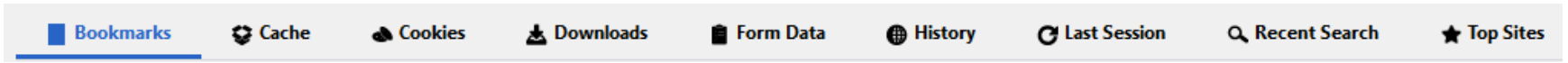
- **위치 정보**
  - Map View
    - 다양한 아티팩트에서 나오는 위치 정보를 Google Maps에 연동하여 보여줌
    - 동작하지 않음
  - Location List
    - GPS(위도, 경도) 목록
    - 동작하지 않음
  - Wi-Fi
    - 연결된 와이파이 목록

	SSID	BSSID	Strength	Security	Last Joined
4	DFRC_5G		0%	WPA2 Personal	2022-04-28 10:15:44 (JST)

Cellebrite Inspector을 이용한 데이터 분석

Internet



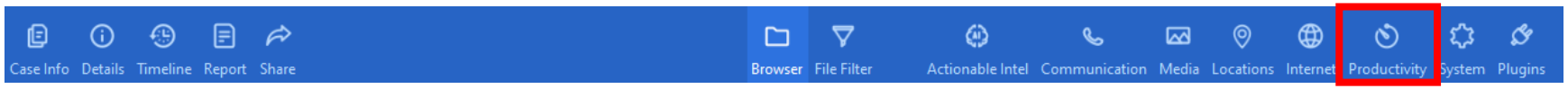


- **인터넷**
  - URL 관련
    - Bookmarks, Download, History, Last Session, Top Sites
  - 접속 정보
    - Cache, Cookies, Form Data
  - Recent Search

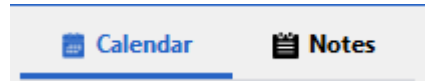
Browser	Search String	Search Engine	Date Last Visited	Visit Count	User Profile	Classifications
Safari	pajun	Google	2022-04-28 10:29:21 (JST)	2	hunjisonchoi	
Safari	very strange keyword	Google	2022-04-28 10:29:20 (JST)	2	hunjisonchoi	
Safari	pajun	Google	2022-04-28 10:29:40 (JST)	1	hunjisonchoi	
Safari	hello	Google	2022-04-28 10:29:59 (JST)	2	hunjisonchoi	
Safari	hello	Google	2022-04-28 10:29:58 (JST)	2	hunjisonchoi	
Safari	samgyupsal	Google	2022-04-28 10:37:20 (JST)	2	hunjisonchoi	
Safari	samgyupsal	Google	2022-04-28 10:37:18 (JST)	2	hunjisonchoi	
Safari	samgyupsal	Google	2022-04-28 10:37:20 (JST)	1	hunjisonchoi	
Safari	samgyupsal	Google	2022-04-28 10:37:29 (JST)	1	hunjisonchoi	
Safari	samgyupsal	Google	2022-04-28 10:37:31 (JST)	1	hunjisonchoi	

Cellebrite Inspector을 이용한 데이터 분석

Productivity



- **생산성 도구(기본 앱)**



  - Calender
    - 달력 기본 앱

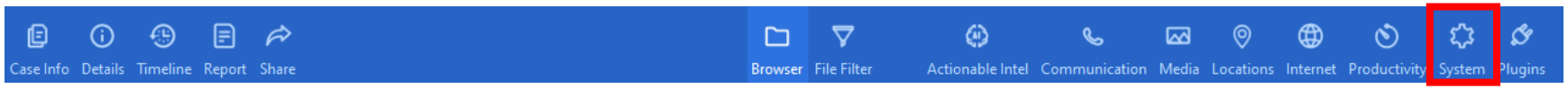
Date	Duration	Summary	Location	Time Zone	Calendar
2022-05-07 00:30:00 (JST)	1 hour	DFRC seminar on		Asia/Seoul	
2022-05-07 23:00:00 (JST)	1 hour	family meeting on		Asia/Seoul	

  - Notes
    - 메모 기본 앱

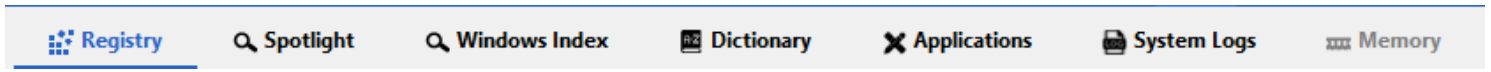
Date Created	Date Modified	Title	Summary	Account	Source/Folder	Classifications
2022-04-28 10:27:22 (JST)	2022-04-28 10:27:53 (JST)	It is very secret	My privacy note	1_iCloud	Notes	
2022-05-06 08:41:50 (JST)	2022-05-06 08:41:54 (JST)		very simple			

Cellebrite Inspector을 이용한 데이터 분석

System



- **System Artifacts**



  - Spotlight

Date Updated	File Name	Display Name	Kind
2022-04-28 10:38:35 (JST)	UNADJUSTEDNONRAW_mini_3.jpg	UNADJUSTEDNONRAW_mini_3.jpg	JPEG image
2022-04-28 10:38:35 (JST)	UNADJUSTEDNONRAW_thumb_3.jpg	UNADJUSTEDNONRAW_thumb_3.jpg	JPEG image
2022-04-28 10:38:35 (JST)	20220428-013829	20220428-013829	Folder

  - Applications
    - 설치된 모든 앱

Application
Terminal
TextEdit
ThermalTrap
Ticket Viewer
Time Machine

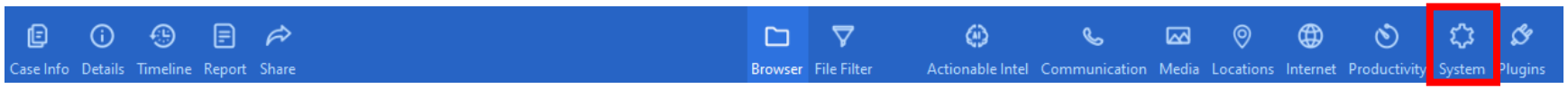
Name	Date Created	Date Modified
Terminal.app	2019-04-16 11:05:00 (JST)	2019-04-16 11:05:00 (JST)
Contents	2019-04-16 11:19:28 (JST)	2019-04-16 11:19:28 (JST)
_CodeSignature	2019-04-16 11:05:00 (JST)	2019-04-16 11:05:00 (JST)
Info.plist	2019-04-16 11:03:38 (JST)	2019-04-16 11:03:38 (JST)
MacOS	2019-09-21 10:42:12 (JST)	2019-09-21 10:42:12 (JST)

Application
Bandizip
Common Files
Google

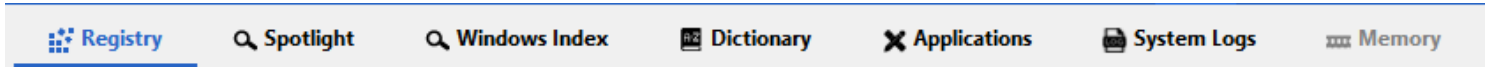
Name	Date Created	Date Modified	Date Accessed
Bandizip	2022-04-26 13:19:24 (JST)	2022-04-26 13:19:25 (JST)	2022-05-04 14:08:40 (JST)
ark.x64.dll	2022-04-26 13:19:24 (JST)	2022-04-13 14:08:24 (JST)	2022-04-27 10:46:04 (JST)
ark.x64.lgpl.dll	2022-04-26 13:19:24 (JST)	2022-04-13 11:22:34 (JST)	2022-04-26 13:19:26 (JST)

Cellebrite Inspector을 이용한 데이터 분석

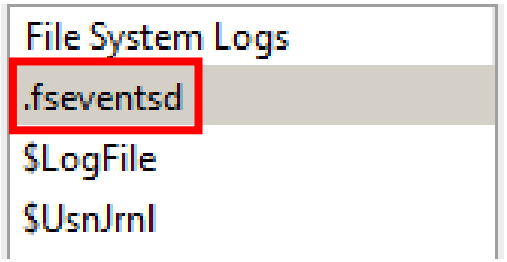
System

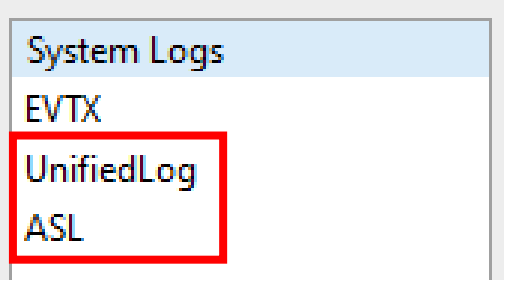


- **System Artifacts**



  - System Logs





Identifier	S...	Inode	Name	Path	Flags	Offset
236858	20...	465	.DS_Store	.DS_Store	InodeMetaMod, Modified, IsF...	12
63882	20...		Preboot	/Volumes/Preboot	Removed, CreateDirectory, Is...	12
430700	20...		sl-compat	.fseventsd/sl-compat	IsDirectory	12
165694	20...	741210	.OSInstallerMessages	.OSInstallerMessages	Removed, IsFile	12
108733	20...		Preboot	/Volumes/Preboot	Mounted, Unmounted	12

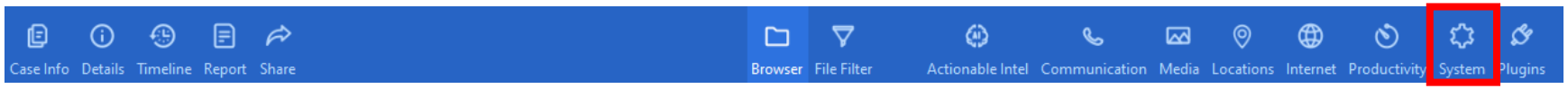
Source File	Date	Fields	Flags	UID	PID	GID	Level
2022.04.28.asl	2022-04-28 10:40:30 (JST)	message: None	2	501	702	20	5
2022.04.28.asl	2022-04-28 10:40:30 (JST)	message: None	2	501	702	20	5
2022.04.28.asl	2022-04-28 10:40:30 (JST)	message: None	2	501	702	20	5

Full Fields Content:

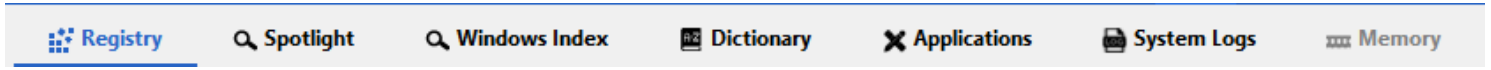
```
message: None
SenderMachUUID: 14FBFAF2-268F-3DA9-8ACF-CCC13AC8AF12
com.apple.message.__source__: SPI
com.apple.message.domain: com.apple.usage.app_activetime
com.apple.message.result: NO
com.apple.message.signature2: com.apple.CoreLocationAgent ||| 1486.12 (1486.12)
com.apple.message.signature: CoreLocationAgent
```

Cellebrite Inspector을 이용한 데이터 분석

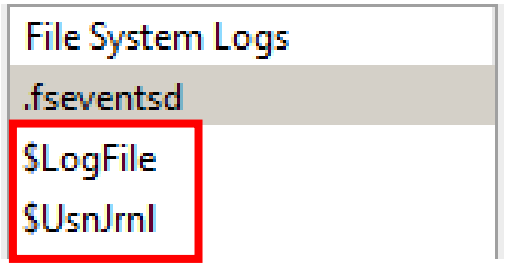
System

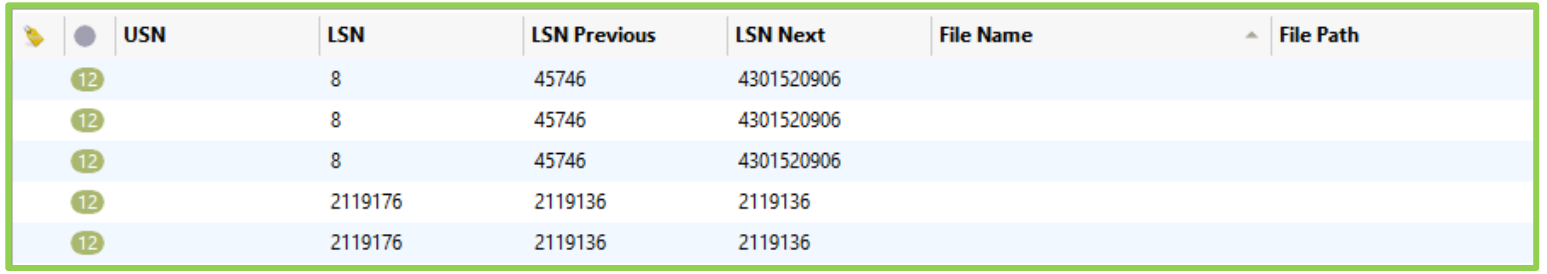


- **System Artifacts**

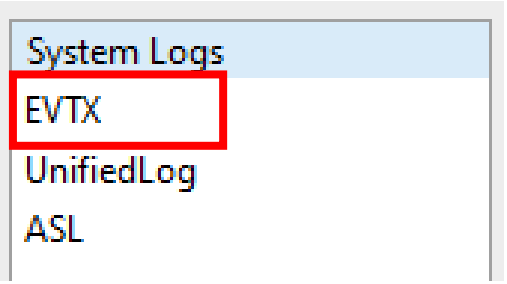


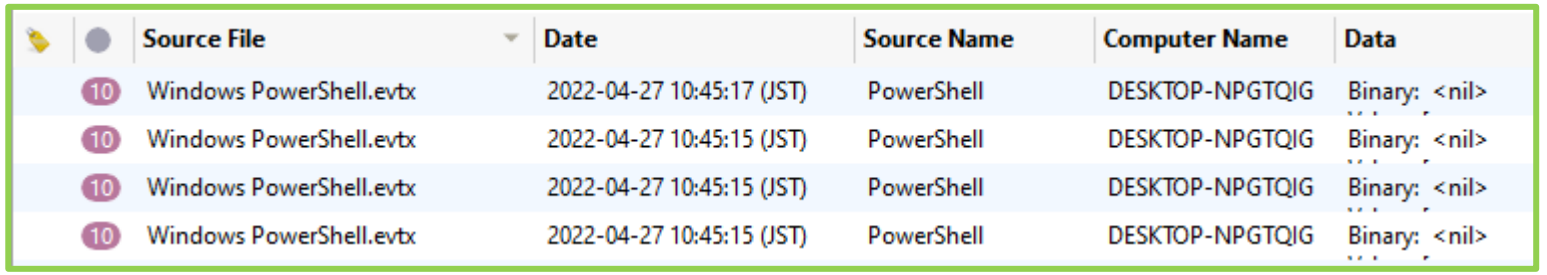
  - System Logs





	USN	LSN	LSN Previous	LSN Next	File Name	File Path
12		8	45746	4301520906		
12		8	45746	4301520906		
12		8	45746	4301520906		
12		2119176	2119136	2119136		
12		2119176	2119136	2119136		

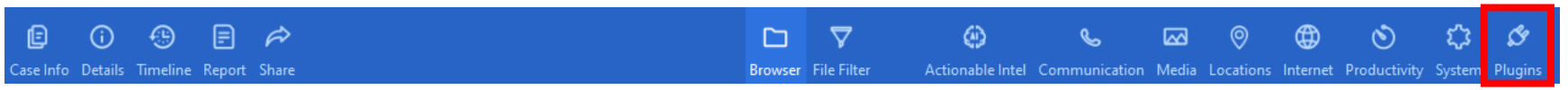




	Source File	Date	Source Name	Computer Name	Data
10	Windows PowerShell.evtx	2022-04-27 10:45:17 (JST)	PowerShell	DESKTOP-NPGTQIG	Binary: <nil>
10	Windows PowerShell.evtx	2022-04-27 10:45:15 (JST)	PowerShell	DESKTOP-NPGTQIG	Binary: <nil>
10	Windows PowerShell.evtx	2022-04-27 10:45:15 (JST)	PowerShell	DESKTOP-NPGTQIG	Binary: <nil>
10	Windows PowerShell.evtx	2022-04-27 10:45:15 (JST)	PowerShell	DESKTOP-NPGTQIG	Binary: <nil>

Cellebrite Inspector을 이용한 데이터 분석

Plugins

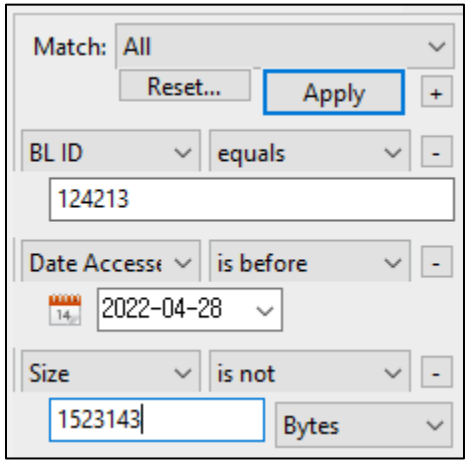


- **Apollo-master**
  - mac4n6에서 개발한 플러그인
  - Powerlog
    - Timezone, Process, Network usage, Battery Level,
  - Netusage
    - Wifi, Zliveusage(프로세스별 네트워크 이용량)
  - Knowledge
    - App별 사용 시간, App Infocus, App별 활동
  - Dock
    - 설치된 앱

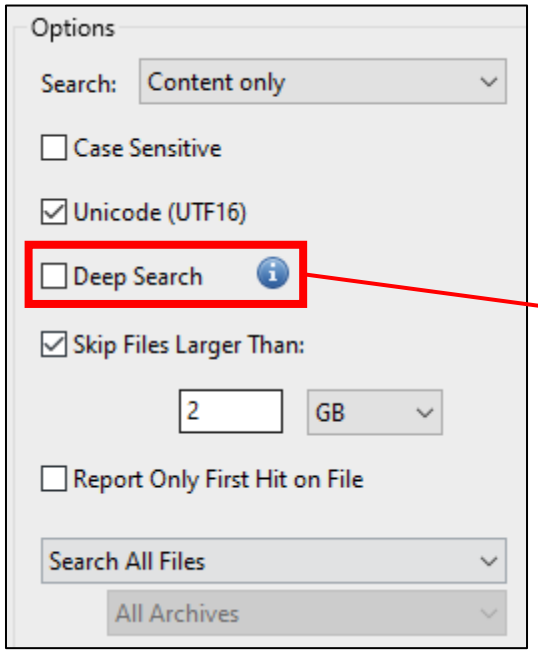
Cellebrite Inspector을 이용한 데이터 분석

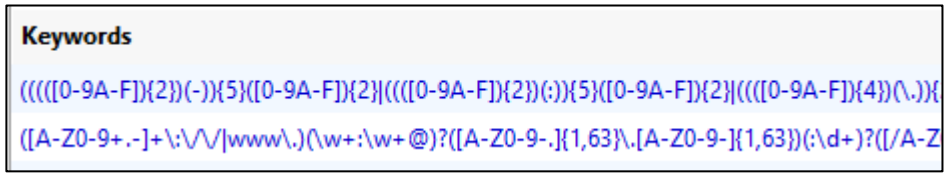
Search

- **검색 기능**
  - Index Searches
    - 여러 조건들 결합 가능



  - Content Searches
    - 파일의 Content 검색
    - 정규표현식 기반



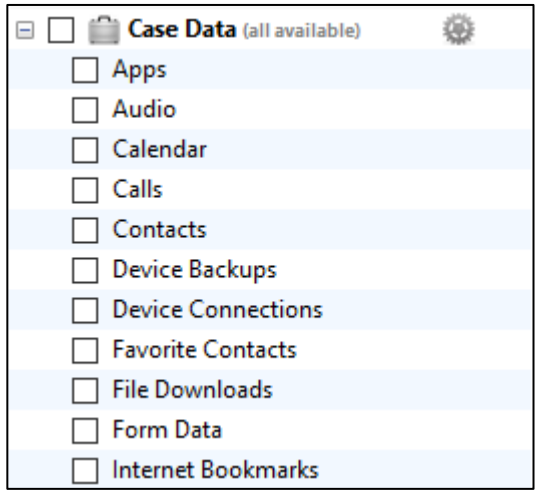


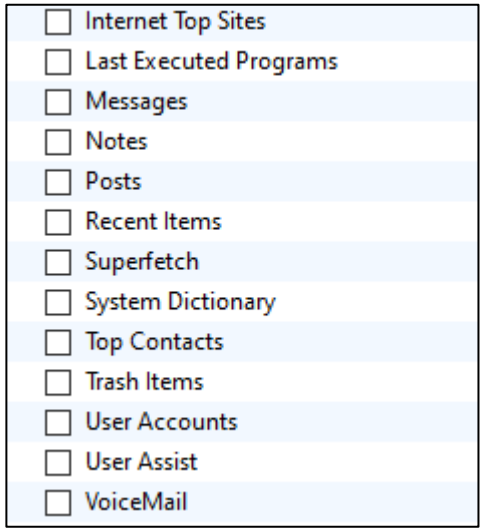
container, archive, database, multimedia 전부 검색할지 여부

Cellebrite Inspector을 이용한 데이터 분석

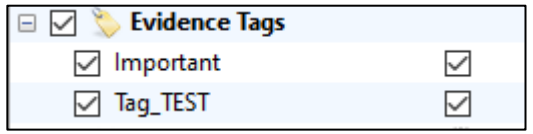
Report

- **보고서 생성**
  - 기본 제공
    - 기본 정보, 디스크, 볼륨 등
    - 자동으로 분류된
      카테고리별 데이터





  - 유저 설정
    - 태그



- **출력 방식**
  - HTML, Docx, PDF, Text, CSV

마무리

분석을 마치며,,

분류	내용	MacOS	Windows
Actionable Intel	Device Backups	O	Not tested
	Device Connections	O	O
	Account Usage	O	O
	Downloads	O(AirDrop 지원)	O
	File Knowledge	O	O(LNK 포함)
	Passwords(Apple KeyChain)	O	X
	Program Execution	X	O
	Search(Spotlight)	O	X
	Activity Correlation	O	O
Communication	Contacts, Email	O	O
	Call, Messages	O	Not tested
	Voicemail, Voice Memos, Favorites	Not tested	Not tested
Media	전체	O	O
Location	Wifi	O	Not tested
	Wifi 제외(Map View, Location List, Mapping Apps)	X	X
Internet	전체	O	O
Productivity	전체(캘린더, 노트)	O	X
System	Registry, Windows Index	X	O
	Spotlight, Dictonary	O	X
	Application, System Logs	O	O
Plugins	APPOLLO-master	O	X

마무리

분석을 마치며,,

- 최적화가 나쁘다

  분석 시간, 실행 속도 ... 😫

- 하나의 프로그램이 Windows, MacOS, iOS, Android 모두를 다루다 보니 중구난방인 느낌

  특히 MacOS에서 지원되지 않는 것들을 식별하기 어려웠다

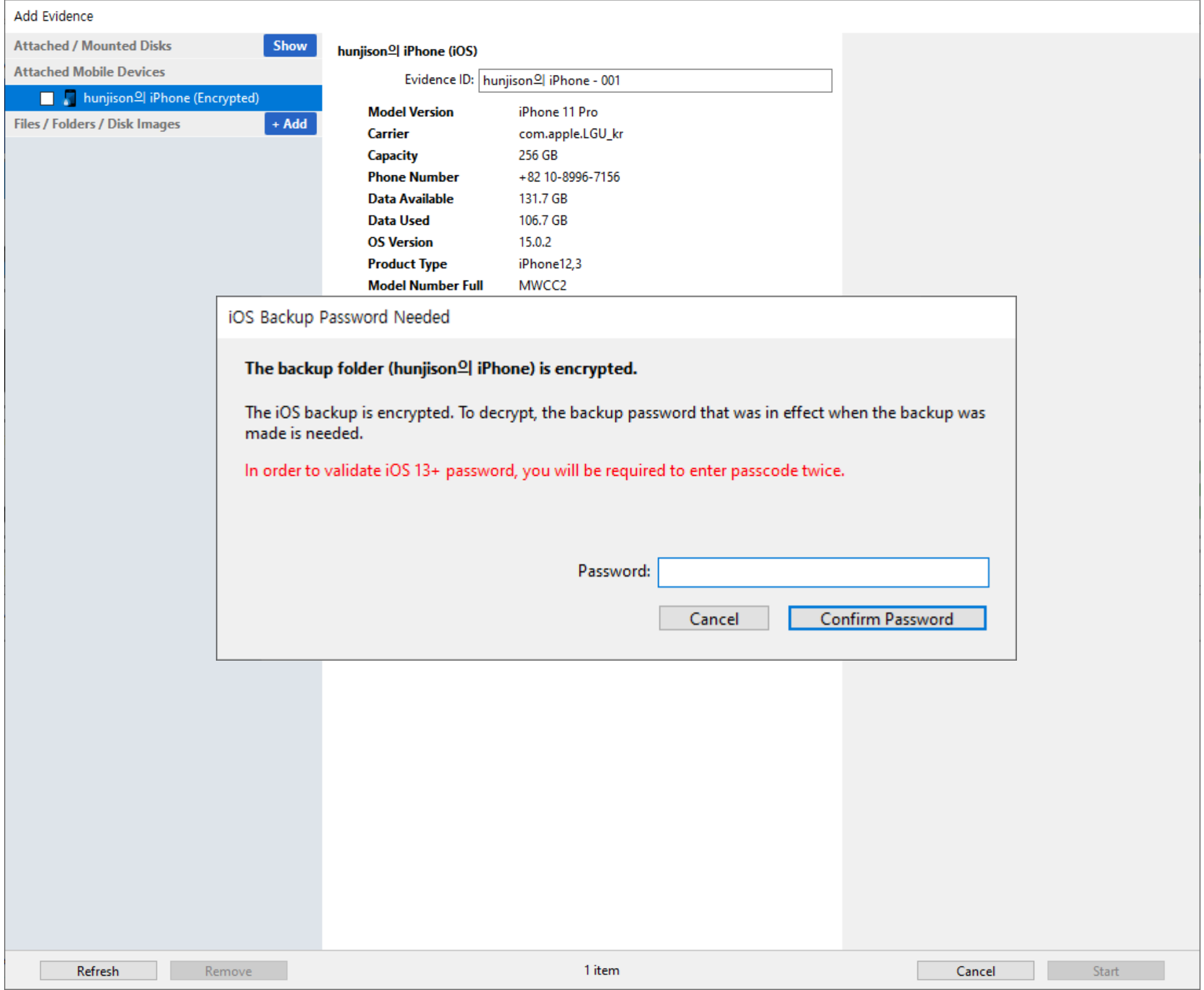
THANK YOU
for Listening!

Digital Forensic Research Center

Graduate School of Information Security, Korea Univ.

forensic.korea.ac.kr

Questions?


Add Evidence
Attached / Mounted Disks
Show
Attached Mobile Devices
hunjison의 iPhone (Encrypted)
Files / Folders / Disk Images
+ Add
hunjison의 iPhone (iOS)
Evidence ID:
hunjison의 iPhone - 001
Model Version
iPhone 11 Pro
Carrier
com.apple.LGU_kr
Capacity
256 GB
Phone Number
+82 10-8996-7156
Data Available
131.7 GB
Data Used
106.7 GB
OS Version
15.0.2
Product Type
iPhone12,3
Model Number Full
MWCC2
iOS Backup Password Needed
The backup folder (hunjison의 iPhone) is encrypted.
The iOS backup is encrypted. To decrypt, the backup password that was in effect when the backup was made is needed.
In order to validate iOS 13+ password, you will be required to enter passcode twice.
Password:
Cancel
Confirm Password
Refresh
Remove
1 item
Cancel
Start

Add Evidence

Attached / Mounted Disks [Show]

Attached Mobile Devices

☑ hunjison의 iPhone

Files / Folders / Disk Images [+ Add]

hunjison의 iPhone (iOS)

Evidence ID: hunjison의 iPhone - 001

Model Version	iPhone 11 Pro
Carrier	com.apple.LGU_kr
Capacity	256 GB
Phone Number	+82 10-8996-7156
Data Available	131.7 GB
Data Used	106.7 GB
OS Version	15.0.2
Product Type	iPhone12,3
Model Number Full	MWCC2
Firmware Version	iBoot-7429.12.15
Serial Number	DNPZMCU3N6Y9
UDID	00008030-000D553E3AC2802E
IMEI	353833104383358
IMSI	450061089967156
ICCID	8982067590404097389
WiFi Address	74:42:8b:ed:b0:5c
Bluetoo...ddress	74:42:8b:e8:ea:55
Time Zone	Asia/Seoul
Password	1234

Processing Options:

hunjison의 iPhone (iOS)

○ Preview ○ Triage ◉ Comprehensive ⚠

- ☑ Extract Data ...
  - ☑ DB Recovery
- ☑ File Signature Analysis
  - ☑ Picture Analysis ...
  - ☑ Video Analysis ...
  - ☑ Process Archives
  - ☑ Process OCR Image Text
- ☑ Calculate Hashes ...
- ☐ Identify Known Files ⚠ ...
- ☐ File Carving ...
- ☐ File System Journal Analysis
- ☐ Spotlight Parsing
- ☐ OS Event / Security Logs
- ☑ Smart Indexing
- ☐ Content Search (Bulk extraction)
- ☑ Mail Parsing
- ☑ Activity Correlation
- ☐ iCloud Backups
- ☐ Hiberfil.sys / Pagefile.sys
  - ◉ Quick Scan ○ Deep Scan
- ☐ Calculate File Entropy

[Manage Passwords...]

No Templates

[Refresh] [Remove] 1 of 1 selected [Cancel] [Start]