2022년 전체 세미나

# iOS, MacOS 오픈소스 도구 분석 (APOLLO, iLEAPP)

2022-05-20


손지훈

hunjison@korea.ac.kr

Digital Forensic Research Center

Institute of Cyber Security & Privacy, Korea University.

# 목차

# APOLLO

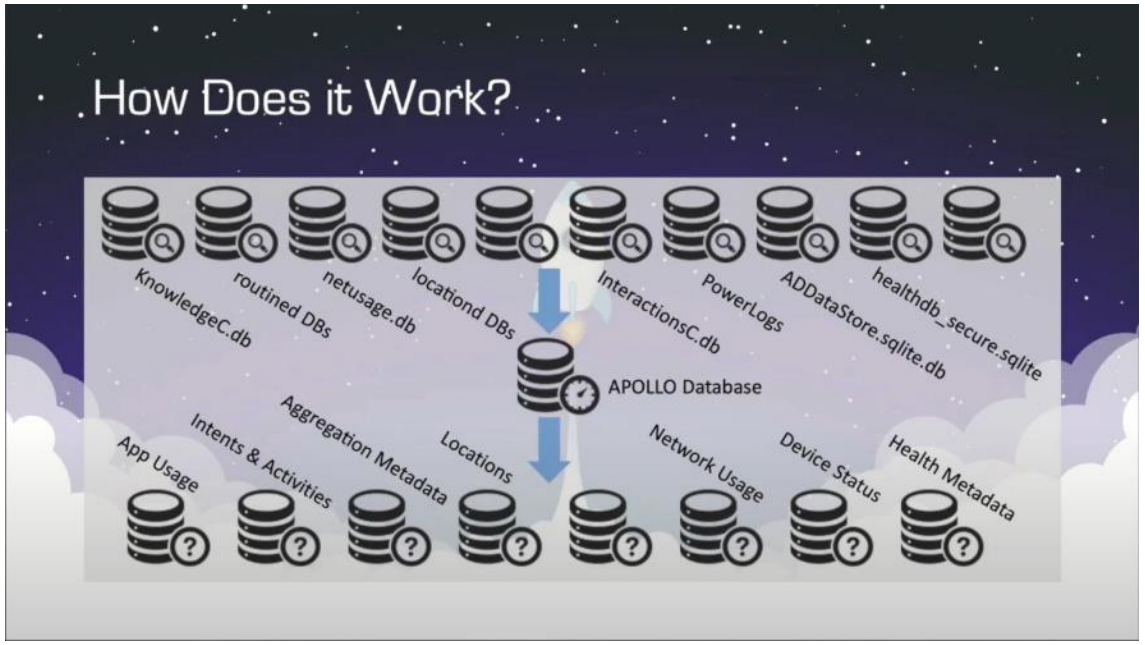
## APOLLO

- **Mac4n6에서 만든 iOS, MacOS 수집 및 분석 도구**
- **지원하는 버전(~ 2020.12)**
  - iOS
    - 8, 9, 10, 11, 12, 13, 14
  - MacOS
    - 10.13, 10.14, 10.15, 10.16(macOS 11)
- **Database 파일 위주의 분석**
  - Database 파일 이름을 기준으로 수집
  - SQL Query를 이용하여 데이터 분석

Apple Pattern of Life Lazy Output'er (APOLLO)

v1.4

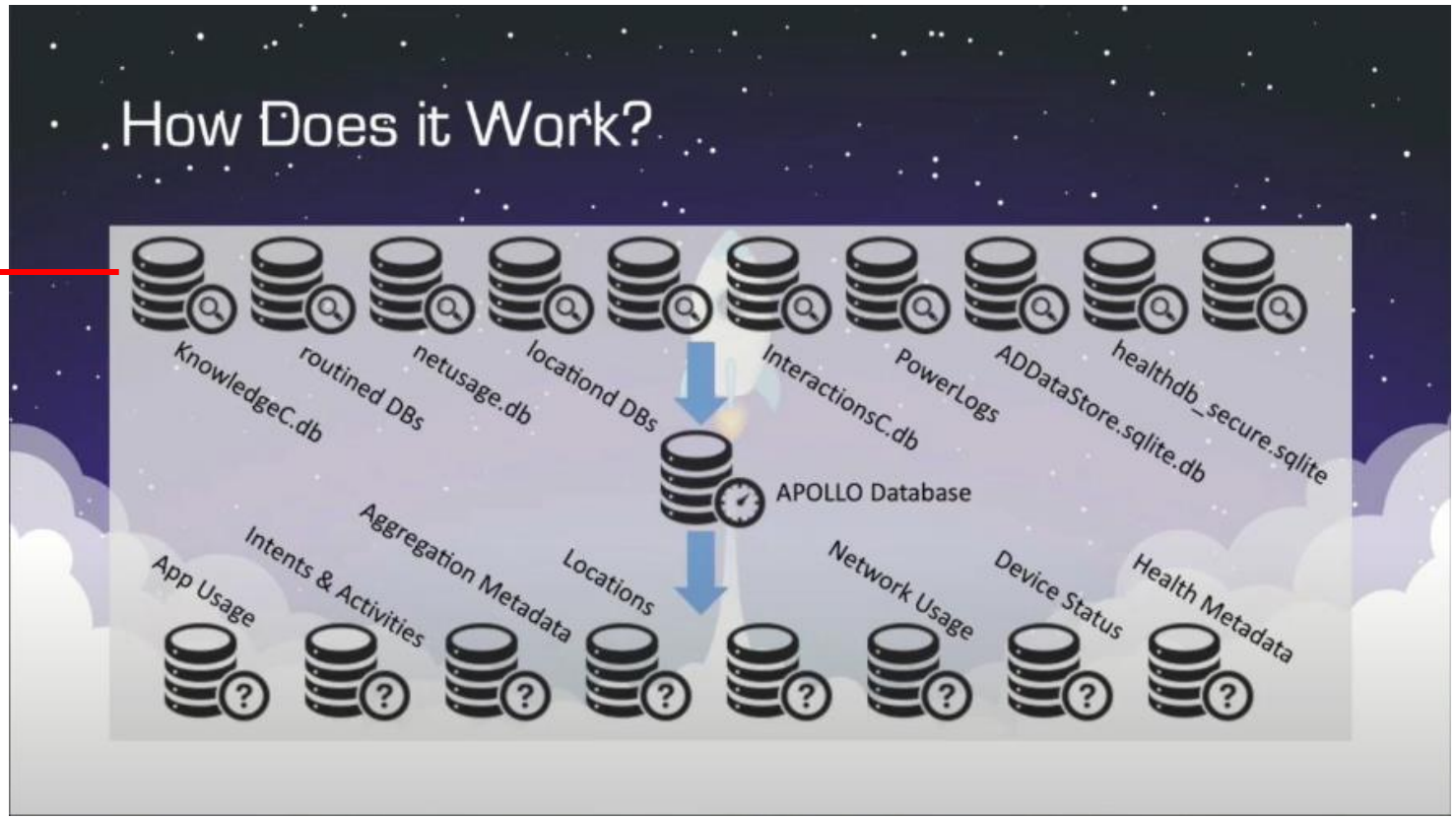
- Gather database files on macOS and jailbroken iOS devices, gather_macos and gather_ios (IP/Port required)
- Ability to ignore certain directories with --ignore
- Improved CSV Output
- JSON Output within SQLite Output



## 동작 원리 - 개요

- **Database들의 목록과 Query를 가지고 있음**

knowledge_app_activity_notes.txt
knowledge_app_activity_passbook.txt
knowledge_app_activity_photos.txt
knowledge_app_activity_safari.txt
knowledge_app_activity_weather.txt



## 동작 원리 - 수집

- **Database들의 목록과 Query를 가지고 있음**

knowledge_app_activity_notes.txt
knowledge_app_activity_passbook.txt
knowledge_app_activity_photos.txt
knowledge_app_activity_safari.txt
knowledge_app_activity_weather.txt

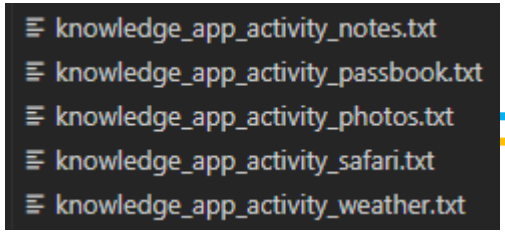
```
63  [Database Metadata]
64  DATABASE=CallHistory.storedata
65  PLATFORM=IOS,MACOS
66  VERSIONS=8,9,10,11,12,13,10.13,10.14,10.15
```

```
63  [Database Metadata]
64  DATABASE=knowledgeC.db
65  PLATFORM=IOS,MACOS
66  VERSIONS=12,13,10.14,10.15,10.16,14
```

```
75  def gathermacos(database_names):
76      tempdir()
77      ignore_dir.append(os.getcwd())
78      print("...Searching for and copying databases into tmp_apollo...")
79      for root, dirs, filenames in os.walk(data_dir, followlinks=False):
80          if not any(ignored in root for ignored in ignore_dir):
81              for f in filenames:
82                  for db in database_names:
83                      if db == "db":
84                          if re.search(rf"^{db}(-shm|-wal|$)", f):
85                              if not os.path.exists(os.getcwd() + "/tmp_apollo" + root):
86                                  os.makedirs(os.getcwd() + "/tmp_apollo" + root)
87                              shutil.copyfile(
88                                  os.path.join(root, f),
89                                  os.getcwd() + "/tmp_apollo" + root + "/" + f,
90                              )
91                      elif re.search(rf"^{db}(-shm|-wal|$)", f):
92                          if not os.path.exists(os.getcwd() + "/tmp_apollo" + root):
93                              os.makedirs(os.getcwd() + "/tmp_apollo" + root)
94                          shutil.copyfile(
95                              os.path.join(root, f),
96                              os.getcwd() + "/tmp_apollo" + root + "/" + f,
97                          )
98      chown_chmod()
```

## 동작 원리 - 분석

- **Database들의 목록과 Query를 가지고 있음**




```
63  [Database Metadata]
64  DATABASE=CallHistory.storedata
65  PLATFORM=IOS,MACOS
66  VERSIONS=8,9,10,11,12,13,10.13,10.14,10.15
```

```
63  [Database Metadata]
64  DATABASE=knowledgeC.db
65  PLATFORM=IOS,MACOS
66  VERSIONS=12,13,10.14,10.15,10.16,14
```

Database

```
73  [SQL Query 12,13,10.14,10.15,10.16,14]
74  QUERY=
75      SELECT
76          DATETIME(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') AS "START",
77          DATETIME(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') AS "END",
78          ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
79          (ZOBJECT.ZENDDATE - ZOBJECT.ZSTARTDATE) AS "USAGE IN SECONDS",
80          (ZOBJECT.ZENDDATE - ZOBJECT.ZSTARTDATE)/60.00 AS "USAGE IN MINUTES",
81          ZSOURCE.ZDEVICEID AS "DEVICE ID (HARDWARE UUID)",
82          ZCUSTOMMETADATA.ZNAME AS "NAME",
83          ZCUSTOMMETADATA.ZDOUBLEVALUE AS "VALUE",
84          CASE ZOBJECT.ZSTARTDAYOFWEEK
85              WHEN "1" THEN "Sunday"
86              WHEN "2" THEN "Monday"
87              WHEN "3" THEN "Tuesday"
88              WHEN "4" THEN "Wednesday"
89              WHEN "5" THEN "Thursday"
90              WHEN "6" THEN "Friday"
91              WHEN "7" THEN "Saturday"
92          END "DAY OF WEEK",
```

SQL Query

## 실행 과정

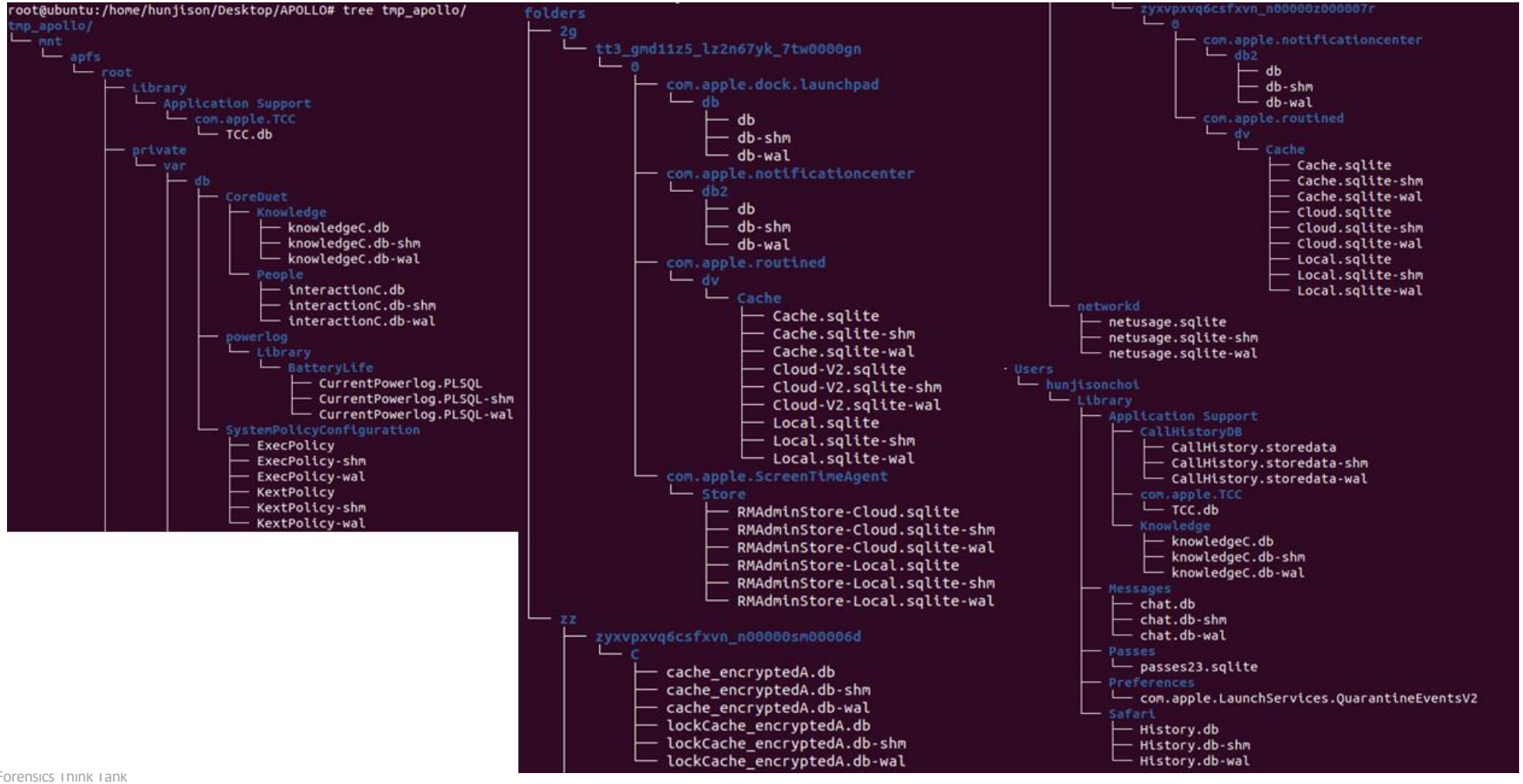
- **수집(Gather)**
  - python3 apollo.py {**gather_macos, gather_ios**} <modules directory> <data directory> --ignore <dir>
  - iOS는 Jailbroken iOS만 지원(ip, port 입력 필요)
- **분석(Extract)**
  - python3 apollo.py extract -o {csv, sql, sql_json} -p {**apple, android, windows, yolo**} -v {**8,9,10,11,12,13,14,10.13,10.14,10.15,10.16,and9,and10,and11,win10_1803,win10_1809,win10_1903, win10_1909,yolo**} -k <modules directory> <data directory>

## 실행 과정

- **Input 데이터, <data directory>**
  - 파일시스템에서 접근 가능한 구조, 마운트된 이미지를 요구함
  - MacOS 분석 시에 별도의 도구(ex. Macquisition)로 이미징 → APFS 이미지 마운트 필요
- **APFS 이미지 마운트**
  - (Windows) WSL2 + APFS for Windows by Paragon Software 시도 → 실패
  - (VM) Linux(Ubuntu) 환경에서 성공
    - ewfmount로 APFS 이미지(E01) 마운트
    - 마운트된 볼륨의 partition layout 파악, mmls(sleuthkit) 명령어 이용
    - losetup 명령어로 명령 루프 디바이스(/dev/loop*)로 등록
    - apfs-fuse로 명령 루프 디바이스를 마운트 성공!

## 실행 과정

- 실행 결과(수집)


root@ubuntu:/home/hunjison/Desktop/APOLLO# tree tmp_apollo/
tmp_apollo/
mnt
apfs
root
Library
Application Support
com.apple.TCC
TCC.db
private
var
db
CoreDuet
Knowledge
knowledgeC.db
knowledgeC.db-shm
knowledgeC.db-wal
People
interactionC.db
interactionC.db-shm
interactionC.db-wal
powerlog
Library
BatteryLife
CurrentPowerlog.PLSQL
CurrentPowerlog.PLSQL-shm
CurrentPowerlog.PLSQL-wal
SystemPolicyConfiguration
ExecPolicy
ExecPolicy-shm
ExecPolicy-wal
KextPolicy
KextPolicy-shm
KextPolicy-wal
folders
2g
tt3_gmd11z5_lz2n67yk_7tw0000gn
0
com.apple.dock.launchpad
db
db
db-shm
db-wal
com.apple.notificationcenter
db2
db
db-shm
db-wal
com.apple.routined
dv
Cache
Cache.sqlite
Cache.sqlite-shm
Cache.sqlite-wal
Cloud-V2.sqlite
Cloud-V2.sqlite-shm
Cloud-V2.sqlite-wal
Local.sqlite
Local.sqlite-shm
Local.sqlite-wal
com.apple.ScreenTimeAgent
Store
RMAdminStore-Cloud.sqlite
RMAdminStore-Cloud.sqlite-shm
RMAdminStore-Cloud.sqlite-wal
RMAdminStore-Local.sqlite
RMAdminStore-Local.sqlite-shm
RMAdminStore-Local.sqlite-wal
zz
zyxvpxvq6csfxvn_n00000sm00006d
C
cache_encryptedA.db
cache_encryptedA.db-shm
cache_encryptedA.db-wal
lockCache_encryptedA.db
lockCache_encryptedA.db-shm
lockCache_encryptedA.db-wal
zyxvpxvq6csfxvn_n00000z000007r
0
com.apple.notificationcenter
db2
db
db-shm
db-wal
com.apple.routined
dv
Cache
Cache.sqlite
Cache.sqlite-shm
Cache.sqlite-wal
Cloud.sqlite
Cloud.sqlite-shm
Cloud.sqlite-wal
Local.sqlite
Local.sqlite-shm
Local.sqlite-wal
networkd
netusage.sqlite
netusage.sqlite-shm
netusage.sqlite-wal
Users
hunjisonchoi
Library
Application Support
CallHistoryDB
CallHistory.storedata
CallHistory.storedata-shm
CallHistory.storedata-wal
com.apple.TCC
TCC.db
Knowledge
knowledgeC.db
knowledgeC.db-shm
knowledgeC.db-wal
Messages
chat.db
chat.db-shm
chat.db-wal
Passes
passes23.sqlite
Preferences
com.apple.LaunchServices.QuarantineEventsV2
Safari
History.db
History.db-shm
History.db-wal

# 실행 과정

- 실행 결과(분석)

```
modules/powerlog_network_usage.txt on CurrentPowerlog.PLSQL for [SQL Query 10.14,10.15,10.16,13,14]: 1 databases.
        Executing module on: tmp_apollo/mnt/apfs/root/private/var/db/powerlog/Library/BatteryLife/CurrentPowerlog.PLSQL
                Number of Records: 72
```

테이블(T): APOLLO

모든 열에서 필터링

| | Key | Activity | Output | Database | Module |
|---|---|---|---|---|---|
| | 필터 | 필터 | 필터 | 필터 | 필터 |
| 1 | 2022-04-28 01:14:35 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 2 | 2022-04-28 01:14:35 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 3 | 2022-04-28 01:14:35 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 4 | 2022-04-28 01:19:50 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 5 | 2022-04-28 01:19:50 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 6 | 2022-04-28 01:19:50 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 7 | 2022-04-28 01:25:42 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 8 | 2022-04-28 01:25:42 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 9 | 2022-04-28 01:25:42 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 10 | 2022-04-28 01:30:42 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 11 | 2022-04-28 01:30:42 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |
| 12 | 2022-04-28 01:30:42 | Network Usage | [ADJUSTED_TIMESTAMP: 2022-04-28 … | tmp_apollo/mnt/apfs/root/private/var/db/… | modules/powerlog_network_usage.txt#CurrentPowerlog.PLSQL#SQL Query … |

```
modules/knowledge_app_activity_safari.txt on knowledgeC.db for [SQL Query 12,13,10.14,10.15,10.16,14]: 2 databases.
        Executing module on: tmp_apollo/mnt/apfs/root/private/var/db/CoreDuet/Knowledge/knowledgeC.db
                Number of Records: 24
        Executing module on: tmp_apollo/mnt/apfs/root/Users/hunjisonchoi/Library/Application Support/Knowledge/knowledgeC.db
                Number of Records: 0
```

# iLEAPP

## iLEAPP

- **iOS 전용 Log, Event, Plists 파싱 도구**
- **지원하는 버전(현재까지 업데이트 중)**
  - iOS/iPadOS
    - 11, 12, 13, 14
    - 가장 최신 버전인 15는 지원하지 않음
- **주로 plist, database, log 파일에서 데이터를 획득**

## 동작 원리 - 수집

- 아티팩트 목록을 바탕으로 정규표현식을 이용하여 수집

```
126 tosearch = {'lastBuild': ('IOS Build', '*LastBuildInfo.plist'),
127             'accs': ('Accounts', '**/Accounts3.sqlite'),
128             'addressBook': ('Address Book', '**/AddressBook.sqlitedb'),
129             'alarms': ('Alarms', '*private/var/mobile/Library/Preferences/com.apple.mobiletimerd.plist'),
130             'AllTrails': ('AllTrails', '**/Documents/AllTrails.sqlite*'),
131             'appConduit': ('App Conduit', '**/AppConduit.log.*'),
132             'appGrouplisting': ('Installed Apps', ('*/Containers/Shared/AppGroup/*/.com.apple.mobile_container_manager.me
133             'appItunesmeta': ('Installed Apps', ('**/iTunesMetadata.plist', '**/BundleMetadata.plist')),
134             'appleMapsApplication': ('Locations', '**/Data/Application/*/Library/Preferences/com.apple.Maps.plist'),
135             'appleMapsGroup': ('Locations', '**/Shared/AppGroup/*/Library/Preferences/group.com.apple.Maps.plist'),
136             'appleMapsSearchHistory': ('Locations', '*private/var/mobile/Containers/Data/Application/*/Library/Maps/GeoHi
137             'applePodcasts': ('Apple Podcasts', '**/MTLibrary.sqlite*'),
138             'appleWalletCards': ('Apple Wallet', '*/private/var/mobile/Containers/Data/Application/*/Library/Caches/com.a
139             'appleWalletPasses': ('Apple Wallet', ('**/nanopasses.sqlite3*', '**/Cards/*.pkpass/pass.json')),
140             'appleWalletTransactions': ('Apple Wallet', '**/passes23.sqlite'),
141             'appleWifiPlist': ('Wifi Connections', ('**/com.apple.wifi.plist', '**/com.apple.wifi-networks.plist.backup',
142             'applicationSnapshots': ('Installed Apps', ('**/Library/Caches/Snapshots/*', '**/SplashBoard/Snapshots/*')),
143             'applicationstate': ('Installed Apps', '**/applicationState.db'),
144             'airtags': ('Airtags', '*/Caches/com.apple.findmy.fmipcore/Items.data'),
145             'bluetooth': ('Bluetooth', '**/com.apple.MobileBluetooth.*'),
```

# 동작 원리 - 분석

- **아티팩트 파싱**
  - plist

```
purchasedate = plist.get('com.apple.iTunesStore.downloadInfo', {}).get('purchaseDate', '')
bundleid = plist.get('softwareVersionBundleId', '')
itemname = plist.get('itemName', '')
artistname = plist.get('artistName', '')
versionnum = plist.get('bundleShortVersionString', '')
downloadedby = plist.get('com.apple.iTunesStore.downloadInfo', {}) .get('accountInfo', {}).get('AppleID', '')
genre = plist.get('genre', '')
```

  - SQL query

```
7   def get_addressBook(files_found, report_folder, seeker):
8       file_found = str(files_found[0])
9       db = open_sqlite_db_readonly(file_found)
10      cursor = db.cursor()
11      cursor.execute('''
12      SELECT
13      ABPerson.ROWID,
14      c16Phone,
15      FIRST,
16      MIDDLE,
17      LAST,
18      c17Email,
19      DATETIME(CREATIONDATE+978307200,'UNIXEPOCH'),
20      DATETIME(MODIFICATIONDATE+978307200,'UNIXEPOCH'),
21      NAME
22      FROM ABPerson
23      LEFT OUTER JOIN ABStore ON ABPerson.STOREID = ABStore.ROWID
```

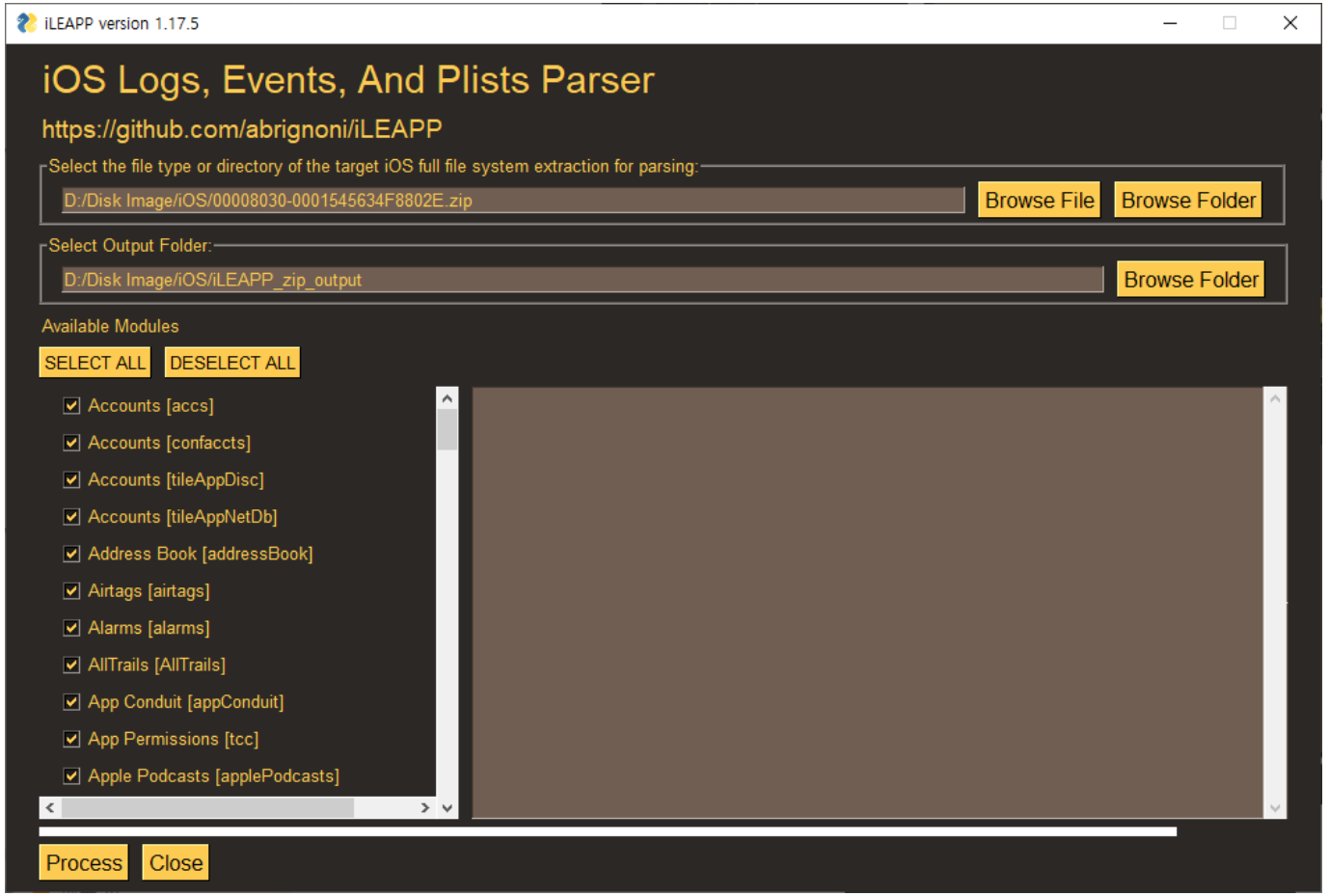
## 동작 원리 - 분석

- **보고서 생성**

```
27      all_rows = cursor.fetchall()
28      usageentries = len(all_rows)
29      if usageentries > 0:
30          data_list = []
31          for row in all_rows:
32              if row[1] is not None:
33                  numbers = row[1].split(" +")
34                  number = numbers[1].split(" ")
35                  phone_number = "+{}".format(number[0])
36              else:
37                  phone_number = ''
38
39              data_list.append((row[0], phone_number, row[2], row[3], row[4], row[5], row[6], row[7], row[8]))
40
41          report = ArtifactHtmlReport('Address Book Contacts')
42          report.start_artifact_report(report_folder, 'Address Book Contacts')
43          report.add_script()
44          data_headers = ('Contact ID', 'Contact Number', 'First Name', 'Middle Name', 'Last Name', 'Email Address', 'Creation Date'
45          report.write_artifact_data_table(data_headers, data_list, file_found)
46          report.end_artifact_report()
47
48          tsvname = 'Address Book'
49          tsv(report_folder, data_headers, data_list, tsvname)
50
51          tlactivity = 'Address Book'
52          timeline(report_folder, tlactivity, data_list, data_headers)
```

## 실행 과정

- **GUI 지원**
  - Input 파일
    - 압축파일(.tar, .zip)
    - 압축 해제된 디렉토리
    - iTunes Backup 폴더
      - Manifest.db 기준으로 해석
      - 암호화 Backup 지원하지 않음
- **Process 버튼**
  - 수집 및 분석 한 번에



## 실행 과정

- **수집 과정**

```
Files for **/Accounts3.sqlite located at D:\tmp\iOS_folderExtract\2_dfrc의 iPhone\mobile\Library\Accounts\Accounts3.sqlite

Files for **/Accounts3.sqlite located at D:\tmp\iOS_folderExtract\2_dfrc의 iPhone\mobile\Library\Accounts\VerifiedBackup\Accounts3.sqlite

Files for **/com.apple.accounts.exists.plist located at D:\tmp\iOS_folderExtract\2_dfrc의 iPhone\preferences\SystemConfiguration\com.apple.accounts.exists.plist

No files found for tileAppDisc -> */private/var/mobile/Containers/Shared/AppGroup/*/com.thetileapp.tile-DiscoveredTileDB.sqlite*

No files found for tileAppNetDb -> */private/var/mobile/Containers/Shared/AppGroup/*/com.thetileapp.tile-TileNetworkDB.sqlite*
```

- **분석 과정**

```
No files found for bumble -> **/Library/Caches/Chat.sqlite*

No files found for bumble -> **/Documents/yap-database.sqlite*

Calendar [calendarAll] artifact executing
No data available for Calendar Identity
Calendar [calendarAll] artifact completed in time 0.0 seconds

Call History [callHistory] artifact executing
Call History [callHistory] artifact completed in time 0.015625 seconds
```

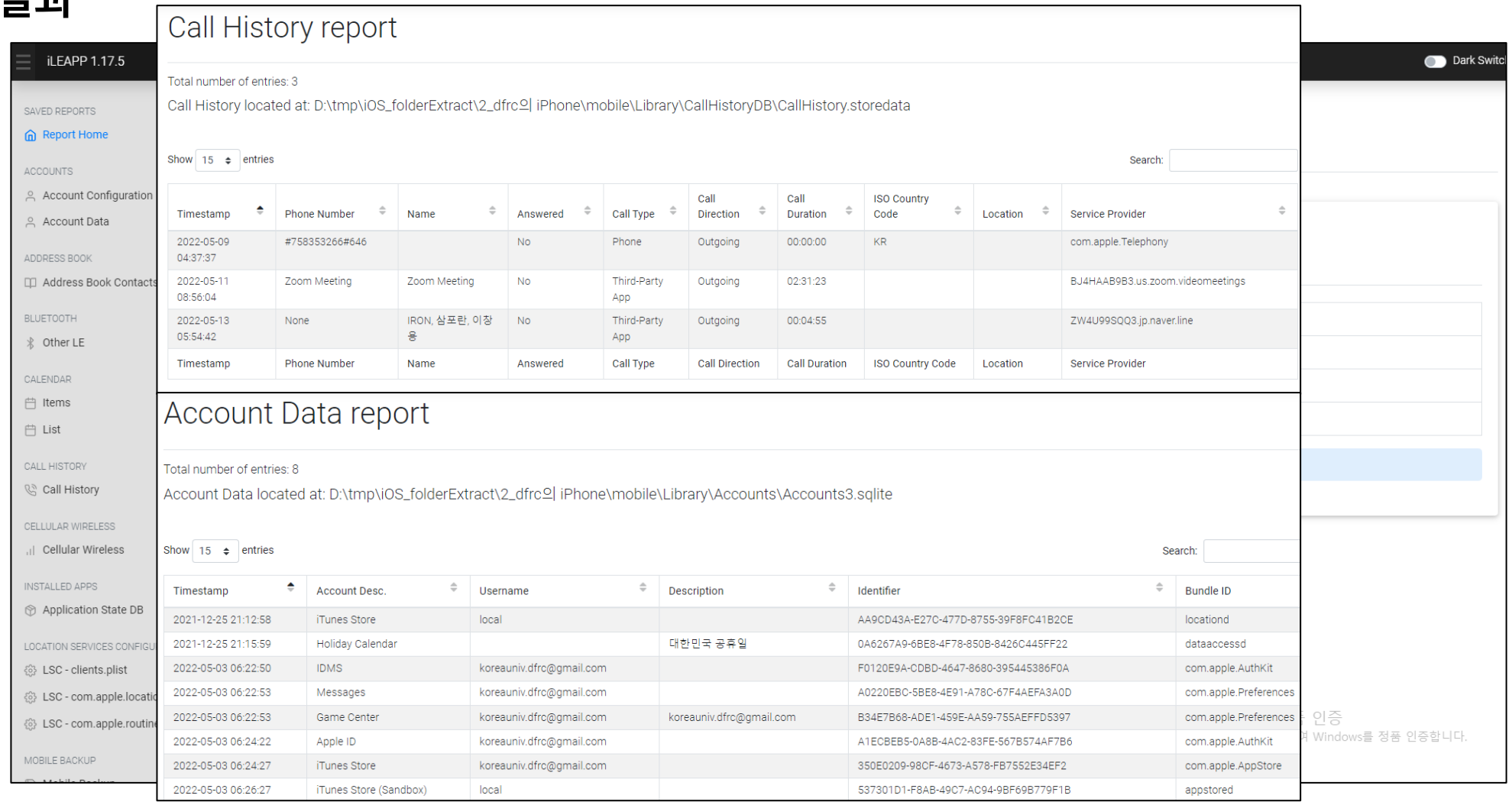
수집 실패

분석 실패(데이터없음 or 구조 다름)

분석 성공

# 실행 과정

- 실행 결과




## Call History report

Total number of entries: 3

Call History located at: D:\tmp\iOS_folderExtract\2_dfrc의 iPhone\mobile\Library\CallHistoryDB\CallHistory.storedata

Show 15 entries Search:

| Timestamp | Phone Number | Name | Answered | Call Type | Call Direction | Call Duration | ISO Country Code | Location | Service Provider |
|---|---|---|---|---|---|---|---|---|---|
| 2022-05-09 04:37:37 | #758353266#646 | | No | Phone | Outgoing | 00:00:00 | KR | | com.apple.Telephony |
| 2022-05-11 08:56:04 | Zoom Meeting | Zoom Meeting | No | Third-Party App | Outgoing | 02:31:23 | | | BJ4HAAB9B3.us.zoom.videomeetings |
| 2022-05-13 05:54:42 | None | IRON, 삼포란, 이장용 | No | Third-Party App | Outgoing | 00:04:55 | | | ZW4U99SQQ3.jp.naver.line |
| Timestamp | Phone Number | Name | Answered | Call Type | Call Direction | Call Duration | ISO Country Code | Location | Service Provider |

## Account Data report

Total number of entries: 8

Account Data located at: D:\tmp\iOS_folderExtract\2_dfrc의 iPhone\mobile\Library\Accounts\Accounts3.sqlite

Show 15 entries Search:

| Timestamp | Account Desc. | Username | Description | Identifier | Bundle ID |
|---|---|---|---|---|---|
| 2021-12-25 21:12:58 | iTunes Store | local | | AA9CD43A-E27C-477D-8755-39F8FC41B2CE | locationd |
| 2021-12-25 21:15:59 | Holiday Calendar | | 대한민국 공휴일 | 0A6267A9-6BE8-4F78-850B-8426C445FF22 | dataaccessd |
| 2022-05-03 06:22:50 | IDMS | koreauniv.dfrc@gmail.com | | F0120E9A-CDBD-4647-8680-395445386F0A | com.apple.AuthKit |
| 2022-05-03 06:22:53 | Messages | koreauniv.dfrc@gmail.com | | A0220EBC-5BE8-4E91-A78C-67F4AEFA3A0D | com.apple.Preferences |
| 2022-05-03 06:22:53 | Game Center | koreauniv.dfrc@gmail.com | koreauniv.dfrc@gmail.com | B34E7B68-ADE1-459E-AA59-755AEFFD5397 | com.apple.Preferences |
| 2022-05-03 06:24:22 | Apple ID | koreauniv.dfrc@gmail.com | | A1ECBEB5-0A8B-4AC2-83FE-567B574AF7B6 | com.apple.AuthKit |
| 2022-05-03 06:24:27 | iTunes Store | koreauniv.dfrc@gmail.com | | 350E0209-98CF-4673-A578-FB7552E34EF2 | com.apple.AppStore |
| 2022-05-03 06:26:27 | iTunes Store (Sandbox) | local | | 537301D1-F8AB-49C7-AC94-9BF69B779F1B | appstored |

# 도구 비교

# 도구 비교

## 비교 방법

- **소스코드 분석**
  - 소스코드에 포함된 아티팩트 종류 분석
- **실행 결과 비교**
  - iLEAPP
    - iPhone 6S (iOS 13.3.1)
  - APOLLO
    - Mac Air Mid 2012 (MacOS 10.15.7)
- **도구 비교 정리**

# 도구 비교

## 소스코드 분석

- **데이터 정리**
  - 내부 데이터를 한 눈에 볼 수 있도록 스크립트 작성

```
                        sql_query = parser.items(section, "QUERY")
                        if "SQL Query" in section:
                            for item in sql_query[0]:
                                query = item
                                uniquekey = mod_def + "#" + db + "#" + section

                                if activity in data.keys():
                                    data[activity][section] = [query_name, db]
                                else:
                                    data[activity] = {}
                                    data[activity][section] = [query_name, db]
    import pprint

    with open(r"C:\Users\dfrc\Desktop\APOLLO.txt", "w") as f:
        f.write(pprint.pformat(data))
```

```
'Airplane Mode': {'SQL Query 13,14': ['knowledge_system_airplane_mode',
                                      'knowledgeC.db'],
                  'SQL Query 8,9': ['coreduetd_device_airplane_state',
                                    'coreduetd.db']},
'Airplay Prediction': {'SQL Query 13,14': ['knowledge_airplay_prediction',
                                           'knowledgeC.db']},
'App Audio Routing': {'SQL Query 9,10,11,12,13,14': ['powerlog_app_audio',
                                                     'CurrentPowerlog.PLSQL']},
'App Deletion': {'SQL Query 10': ['powerlog_app_deletion',
                                  'CurrentPowerlog.PLSQL'],
                 'SQL Query 11,12,13,14': ['powerlog_app_deletion',
                                           'CurrentPowerlog.PLSQL'],
                 'SQL Query 9': ['powerlog_app_deletion',
                                 'CurrentPowerlog.PLSQL']},
```

**APOLLO**

```
new = {}
for key, value in tosearch.items():
    if value[0] in new.keys():
        new[value[0]].append([key, value[1]])
    else:
        new[value[0]] = [[key, value[1]]]

import pprint

with open(r"C:\Users\dfrc\Desktop\iLEAPP.txt", "w") as f:
    f.write(pprint.pformat(new))
```

```
'Files App': [['filesAppsclient',
               '*private/var/mobile/Library/Application '
               'Support/CloudDocs/session/db/client.db*'],
              ['filesAppsdb',
               '*private/var/mobile/Library/Application '
               'Support/CloudDocs/session/db/server.db*'],
              ['filesAppsm',
               '*private/var/mobile/Containers/Shared/AppGroup/*/
'Geolocation': [['geodApplications', '**/AP.db'],
                ['geodMapTiles', '**/MapTiles.sqlitedb'],
                ['geodPDPlaceCache', '**/PDPlaceCache.db'],
                ['mapsSync', '*/MapsSync_0.0.1*']],
```

**iLEAPP**

# 도구 비교

## 소스코드 분석

- **APOLLO**
  - 버전 별로 아티팩트를 다르게 수집하고 있음

```
'Cellular Location': {'cache_encryptedA.db#SQL Query 10': ['locationd_cacheencryptedAB_celllocationharvest',
                                                           'cache_encryptedA.db'],
                      'cache_encryptedA.db#SQL Query 8': ['locationd_cacheencryptedAB_ltecelllocationharvest',
                                                          'cache_encryptedA.db'],
                      'cache_encryptedA.db#SQL Query 8,9,10,11,12,13,14': ['locationd_cacheencryptedAB_ltecelllocationlocal',
                                                                           'cache_encryptedA.db'],
                      'cache_encryptedA.db#SQL Query 9': ['locationd_cacheencryptedAB_celllocationharvest',
                                                          'cache_encryptedA.db'],
                      'cache_encryptedA.db#SQL Query 9,10': ['locationd_cacheencryptedAB_ltecelllocationharvest',
                                                             'cache_encryptedA.db'],
                      'cache_encryptedA.db#SQL Query 9,10,11,12,13,14': ['locationd_cacheencryptedAB_scdmacelllocation',
                                                                         'cache_encryptedA.db'],
                      'cache_encryptedB.db#SQL Query 10': ['locationd_cacheencryptedAB_celllocationharvest',
                                                           'cache_encryptedB.db'],
                      'cache_encryptedB.db#SQL Query 8': ['locationd_cacheencryptedAB_ltecelllocationharvest',
                                                          'cache_encryptedB.db'],
                      'cache_encryptedB.db#SQL Query 8,9,10,11,12,13,14': ['locationd_cacheencryptedAB_ltecelllocationlocal',
                                                                           'cache_encryptedB.db'],
                      'cache_encryptedB.db#SQL Query 9': ['locationd_cacheencryptedAB_celllocationharvest',
                                                          'cache_encryptedB.db'],
                      'cache_encryptedB.db#SQL Query 9,10': ['locationd_cacheencryptedAB_ltecelllocationharvest',
                                                             'cache_encryptedB.db'],
                      'cache_encryptedB.db#SQL Query 9,10,11,12,13,14': ['locationd_cacheencryptedAB_scdmacelllocation',
                                                                         'cache_encryptedB.db'],
                      'lockCache_encryptedA.db#SQL Query 8,9,10,11,12,13,14': ['locationd_cacheencryptedAB_ltecelllocationlocal',
                                                                               'lockCache_encryptedA.db'],
                      'lockCache_encryptedA.db#SQL Query 9,10,11,12,13,14': ['locationd_cacheencryptedAB_scdmacelllocation',
                                                                             'lockCache_encryptedA.db']},
```

# 도구 비교

## 소스코드 분석

- **APOLLO**
  - 몇몇 db에서 대부분의 결과를 끌어내고 있음
  - 특히 **KnowledgeC.db, CurrentPowerlog.PLSQL**, healthdb_secure.sqlite, cache_encrypted*.db 등

```
collect = {'ADDataStore.sqlitedb',
 'Cache.sqlite',
 'CallHistory.storedata',
 'Cloud-V2.sqlite',
 'Cloud.sqlite',
 'CoreRoutine.sqlite',
 'CurrentPowerlog.PLSQL',
 'DataUsage-watch.sqlite',
 'DataUsage.sqlite',
 'ExecPolicy',
 'History.db',
 'KextPolicy',
 'Local.sqlite',
 'RMAdminStore-Cloud.sqlite',
 'RMAdminStore-Local.sqlite',
 'TCC.db',
 'cache_encryptedA.db',
 'cache_encryptedB.db',
 'cache_encryptedC.db',
 'chat.db',
 'com.apple.LaunchServices.QuarantineEventsV2',
 'coreduetd.db',
 'coreduetdClassD.db',
 'db',
 'healthdb_secure.sqlite',
 'interactionC.db',
 'knowledgeC.db',
 'lockCache_encryptedA.db',
 'netusage.sqlite',
 'passes23.sqlite',
 'query_predictions.db',
 'sms.db'}
```

# 도구 비교

## 소스코드 분석

- **iLEAPP**
  - 버전 구별 없이 아티팩트를 수집하고 있음

```
'Locations': [['appleMapsApplication',
               '**/Data/Application/*/Library/Preferences/com.apple.Maps.plist'],
              ['appleMapsGroup',
               '**/Shared/AppGroup/*/Library/Preferences/group.com.apple.Maps.plist'],
              ['appleMapsSearchHistory',
               '*private/var/mobile/Containers/Data/Application/*/Library/Maps/GeoHistory.mapsdata'],
              ['cacheRoutesGmap',
               '**/Library/Application Support/CachedRoutes/*.plist'],
              ['tileApp',
               '*private/var/mobile/Containers/Data/Application/*/Library/log/com.thetileapp.tile*'],
              ['tileAppDb',
               '*private/var/mobile/Containers/Shared/AppGroup/*/com.thetileapp.tile-TileNetworkDB.sqlite*'],
              ['weatherAppLocations',
               '*/private/var/mobile/Containers/Shared/AppGroup/*/Library/Preferences/group.com.apple.weather.plist']],
```

# 도구 비교

## 소스코드 분석

- **iLEAPP**
  - 단순 정규표현식 기반의 파일 수집
  - KnowledgeC.db, CurrentPowerlog.PLSQL 등

    **존재하지 않음**
  - 비교적 다양한 경로에서 데이터 수집

    db, plist, json, webp, txt 등

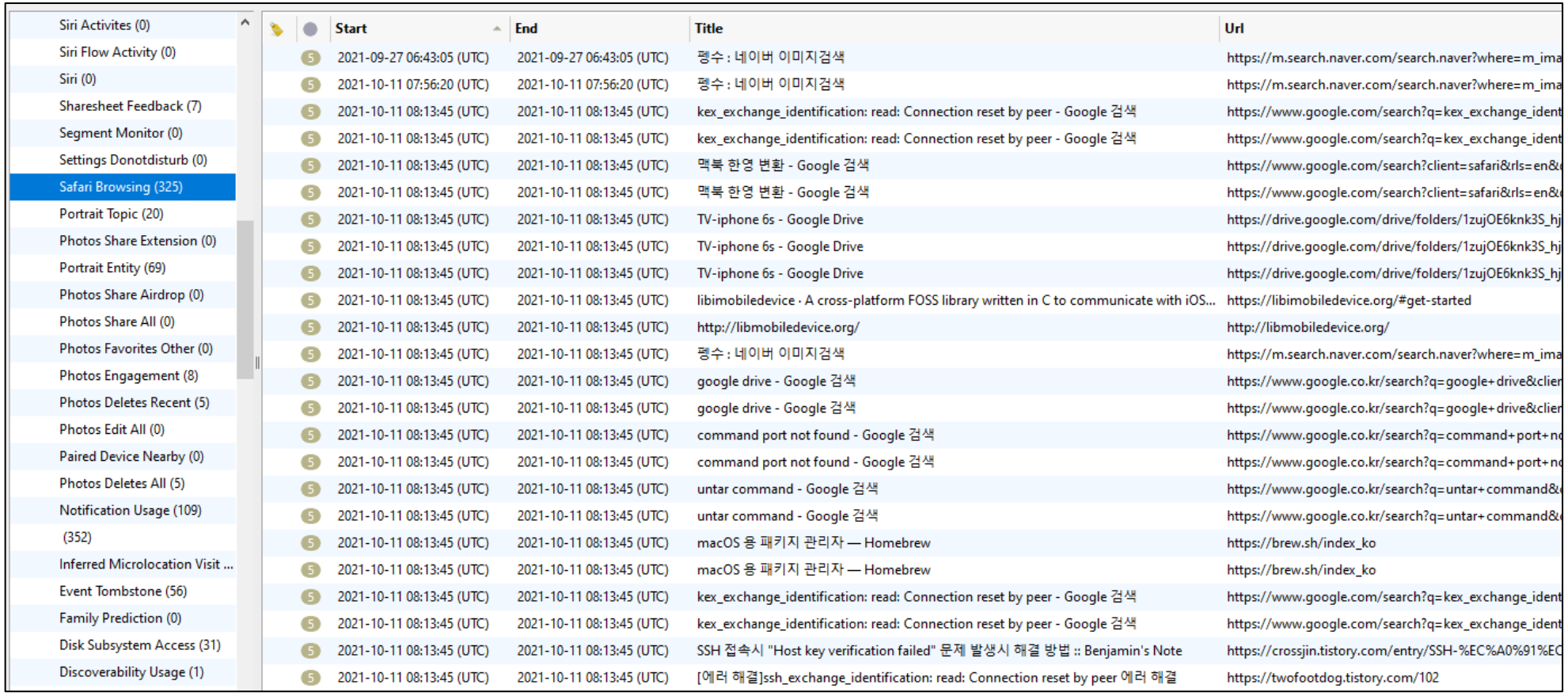
```
collect = {'**/AP.db',
 '**/Accounts3.sqlite',
 '**/AddressBook.sqlitedb',
 '**/AppConduit.log.*',
 '**/Calendar.sqlitedb',
 '**/CallHistory.storedata*',
 '**/Data/Application/*/Library/Preferences/com.apple.M
 '**/Documents/AllTrails.sqlite*',
 '**/Library/Application Support/CachedRoutes/*.plist',
 '**/Library/Preferences/com.apple.mobilesafari.plist',
 '**/MTLibrary.sqlite*',
 '**/MapTiles.sqlitedb',
 '**/Medialibrary.sqlitedb',
 '**/PDPlaceCache.db',
 '**/Photos.sqlite',
 '**/Reminders/Container_v1/Stores/*.sqlite*',
 '**/Safari/Bookmarks.db',
 '**/Safari/BrowserState.db',
 '**/Safari/History.db',
```

```
 ('*/Library/Preferences/com.apple.locationd.plist',
  '*/Library/Caches/locationd/clients.plist',
  '*/Library/Preferences/com.apple.routined.plist'),
 ('*/group.ch.protonmail.protonmail.plist',
  '*/ProtonMail.sqlite*',
  '*/Containers/Data/Application/*/tmp/*'),
 ('*/mobile/Containers/Shared/AppGroup/*/cores/private/
  '*/mobile/Containers/Shared/AppGroup/*/cores/private/
 ('*/var/mobile/Containers/Shared/AppGroup/*/ChatStorag
  '*/var/mobile/Containers/Shared/AppGroup/*/Message/Me
 ('*/var/mobile/Containers/Shared/AppGroup/*/SkypeSpace
  '*/var/mobile/Containers/Shared/AppGroup/*/SkypeSpace
 ('*PrivateFeed', '*PublicFeed', '*FriendsFeed')}
```

# 도구 비교

## 실행 결과 비교

- **APOLLO**
  - Cellebrite Inspector 내부의 UI를 이용



| | Start | End | Title | Url |
|---|---|---|---|---|
| Siri Activites (0) | 2021-09-27 06:43:05 (UTC) | 2021-09-27 06:43:05 (UTC) | 펭수 : 네이버 이미지검색 | https://m.search.naver.com/search.naver?where=m_ima |
| Siri Flow Activity (0) | 2021-10-11 07:56:20 (UTC) | 2021-10-11 07:56:20 (UTC) | 펭수 : 네이버 이미지검색 | https://m.search.naver.com/search.naver?where=m_ima |
| Siri (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | kex_exchange_identification: read: Connection reset by peer - Google 검색 | https://www.google.com/search?q=kex_exchange_ident |
| Sharesheet Feedback (7) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | kex_exchange_identification: read: Connection reset by peer - Google 검색 | https://www.google.com/search?q=kex_exchange_ident |
| Segment Monitor (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | 맥북 한영 변환 - Google 검색 | https://www.google.com/search?client=safari&rls=en& |
| Settings Donotdisturb (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | 맥북 한영 변환 - Google 검색 | https://www.google.com/search?client=safari&rls=en& |
| Safari Browsing (325) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | TV-iphone 6s - Google Drive | https://drive.google.com/drive/folders/1zujOE6knk3S_hj |
| Portrait Topic (20) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | TV-iphone 6s - Google Drive | https://drive.google.com/drive/folders/1zujOE6knk3S_hj |
| Photos Share Extension (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | TV-iphone 6s - Google Drive | https://drive.google.com/drive/folders/1zujOE6knk3S_hj |
| Portrait Entity (69) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | libimobiledevice · A cross-platform FOSS library written in C to communicate with iOS... | https://libimobiledevice.org/#get-started |
| Photos Share Airdrop (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | http://libmobiledevice.org/ | http://libmobiledevice.org/ |
| Photos Share All (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | 펭수 : 네이버 이미지검색 | https://m.search.naver.com/search.naver?where=m_ima |
| Photos Favorites Other (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | google drive - Google 검색 | https://www.google.co.kr/search?q=google+drive&clier |
| Photos Engagement (8) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | google drive - Google 검색 | https://www.google.co.kr/search?q=google+drive&clier |
| Photos Deletes Recent (5) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | command port not found - Google 검색 | https://www.google.co.kr/search?q=command+port+n |
| Photos Edit All (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | command port not found - Google 검색 | https://www.google.co.kr/search?q=command+port+n |
| Paired Device Nearby (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | untar command - Google 검색 | https://www.google.co.kr/search?q=untar+command& |
| Photos Deletes All (5) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | untar command - Google 검색 | https://www.google.co.kr/search?q=untar+command& |
| Notification Usage (109) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | macOS 용 패키지 관리자 — Homebrew | https://brew.sh/index_ko |
| (352) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | macOS 용 패키지 관리자 — Homebrew | https://brew.sh/index_ko |
| Inferred Microlocation Visit ... | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | kex_exchange_identification: read: Connection reset by peer - Google 검색 | https://www.google.com/search?q=kex_exchange_ident |
| Event Tombstone (56) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | kex_exchange_identification: read: Connection reset by peer - Google 검색 | https://www.google.com/search?q=kex_exchange_ident |
| Family Prediction (0) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | SSH 접속시 "Host key verification failed" 문제 발생시 해결 방법 :: Benjamin's Note | https://crossjin.tistory.com/entry/SSH-%EC%A0%91%EC |
| Disk Subsystem Access (31) | 2021-10-11 08:13:45 (UTC) | 2021-10-11 08:13:45 (UTC) | [에러 해결]ssh_exchange_identification: read: Connection reset by peer 에러 해결 | https://twofootdog.tistory.com/102 |
| Discoverability Usage (1) | | | | |

# 도구 비교

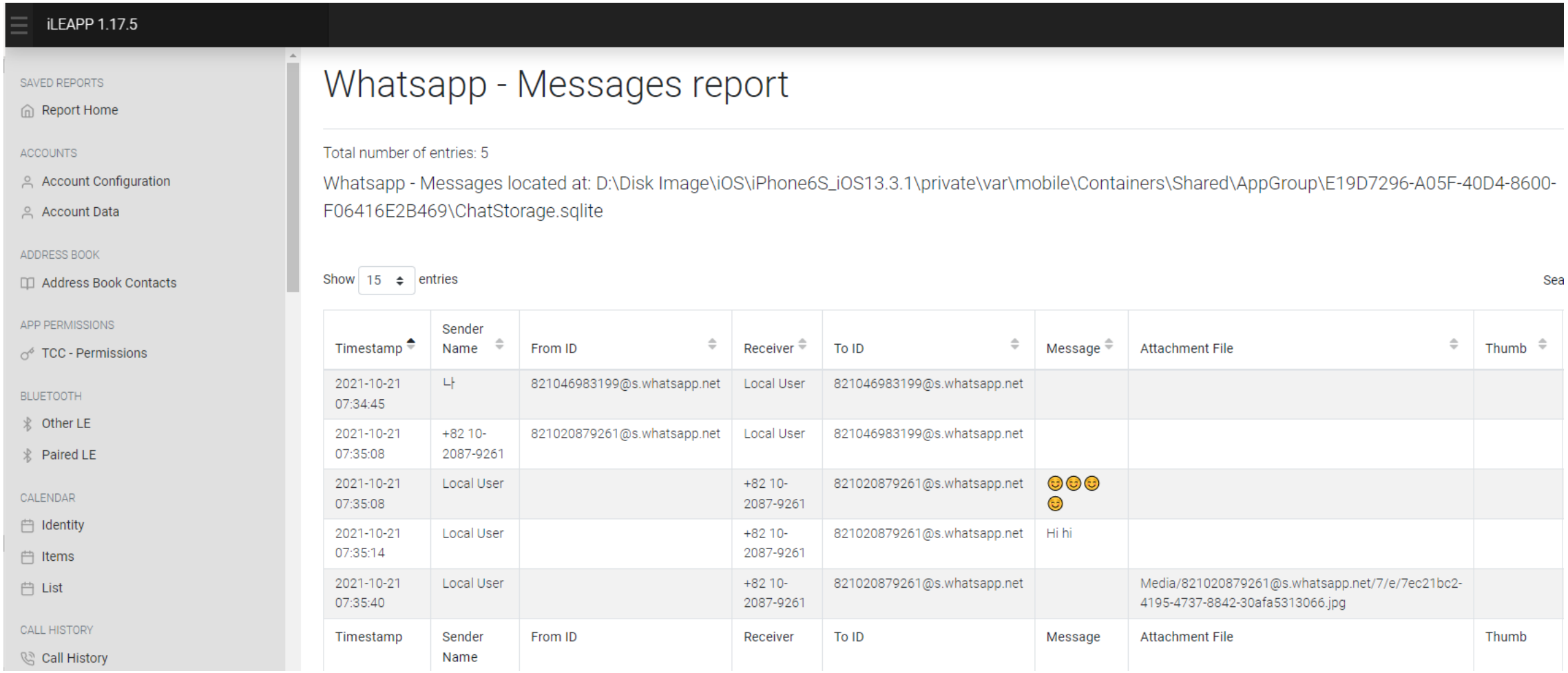
## 실행 결과 비교

- **APOLLO**
  - App/Application
    - Info, Install/Deletion, Location, Usage, Permission 등
  - I/O & Communication
    - SMS, Telephony
    - Audio, Bluetooth, Airdrop, Paired Device, Siri, Wifi, Wallet
  - System Log
    - Device(Battery, Lock, Plugin), Notification, Screen Time, System Policy Configuration, Calender
  - Health
    - Workout, Location, Temperature, Time,
  - Routined Location
    - Entry, Learned Location, Map Item, Vehicle, Visit

# 도구 비교

## 실행 결과 비교

- **iLEAPP**



# 도구 비교

## 실행 결과 비교

- **iLEAPP**
  - App/Application
    - Install, Permission, Conduit
  - I/O & Communication
    - Address Book, Call History, SMS/iMessage
    - CarPlay, Safari, Voice-Recording, iCloud, iOS Mail,
  - System Log
    - Cellular Wireless, Keyboard, Mobile Backup, Software Update, Wifi Connections
  - **Messenger & SNS**
    - Facebook Messenger, Google Duo, IMO HD Chat, Instagram, Microsoft Teams, Slack, TikTok, Viber, Whatsapp, Discord
  - ETC
    - Notes, Photos

# 도구 비교

## 도구 비교 정리

| | APOLLO | iLEAPP |
|---|---|---|
| Support | iOS: 8, 9, 10, 11, 12, 13, 14<br>MacOS: 10.13, 10.14, 10.15, 10.16(macOS 11)<br>마지막 업데이트: 2020년 12월 | iOS/iPadOS: 11, 12, 13, 14<br>마지막 업데이트: 현재까지 계속 지원 |
| 사용 편의 | CLI<br>Input: 디렉토리<br>**Output: apollo.db** | GUI<br>Input: 압축파일, 디렉토리, iTunes Backup<br>**Output: HTML 형태의 보고서** |
| 수집 및 분석 방법 | 수집: 버전, 파일이름 기반으로 탐색<br>분석: SQL Query를 포함하고 있음 | 수집: 정규표현식 기반으로 탐색<br>분석: SQL, Plist 등 구조에 맞는 분석 코드 포함 |
| 수집 아티팩트 개수<br>(중복 제거) | 32개<br>(KnowledgeC.db, CurrentPowerlog.PLSQL 등 몇몇 DB를 아주 자세히 분석함) | 130개 이상<br>(다양한 아티팩트를 포함) |
| 장점 | Application의 동작(In Focus, Network Usage), System의 동작(Wifi, Battery) 등 중요 데이터의 분석이 자세함<br>Cellebrite Inspector UI와 같이 쓰면 쓸만하다(?) | 전반적으로 균형잡힌 분석을 지원함<br>(시스템 기본 앱, Bluetooth 등 연결 기기 등등)<br>다양한 종류의 Messenger 분석을 지원 |

THANK YOU
for Listening!

**Digital Forensic Research Center**

Graduate School of Information Security, Korea Univ.

forensic.korea.ac.kr

Questions?