ma2tl:
macOS Forensic Timeline Generator Using mac_apt Analysis Results

Japan Security Analyst Conference 2022

Internet Initiative Japan Inc.
Minoru Kobayashi

Who am I?

Minoru Kobayashi

- Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, Internet Initiative Japan Inc.
  Technical research, internal incident response
- External Activities
  Security Camp National Conference Speaker 2017-2019
  Japan Security Analyst Conference Speaker 2018/2020
  Black Hat USA 2018 Briefing Speaker
- Twitter: @unkn0wnbit

Table of Contents

0

Introduction

Introduction

- The contents of this presentation are all based on research and verification conducted on Intel Macs.
- There may be some differences in specifications on M1 Macs.
- However, in many respects, it could be diverted to investigate M1 Macs.

1 Motivation

The Need for Timelines in Forensics

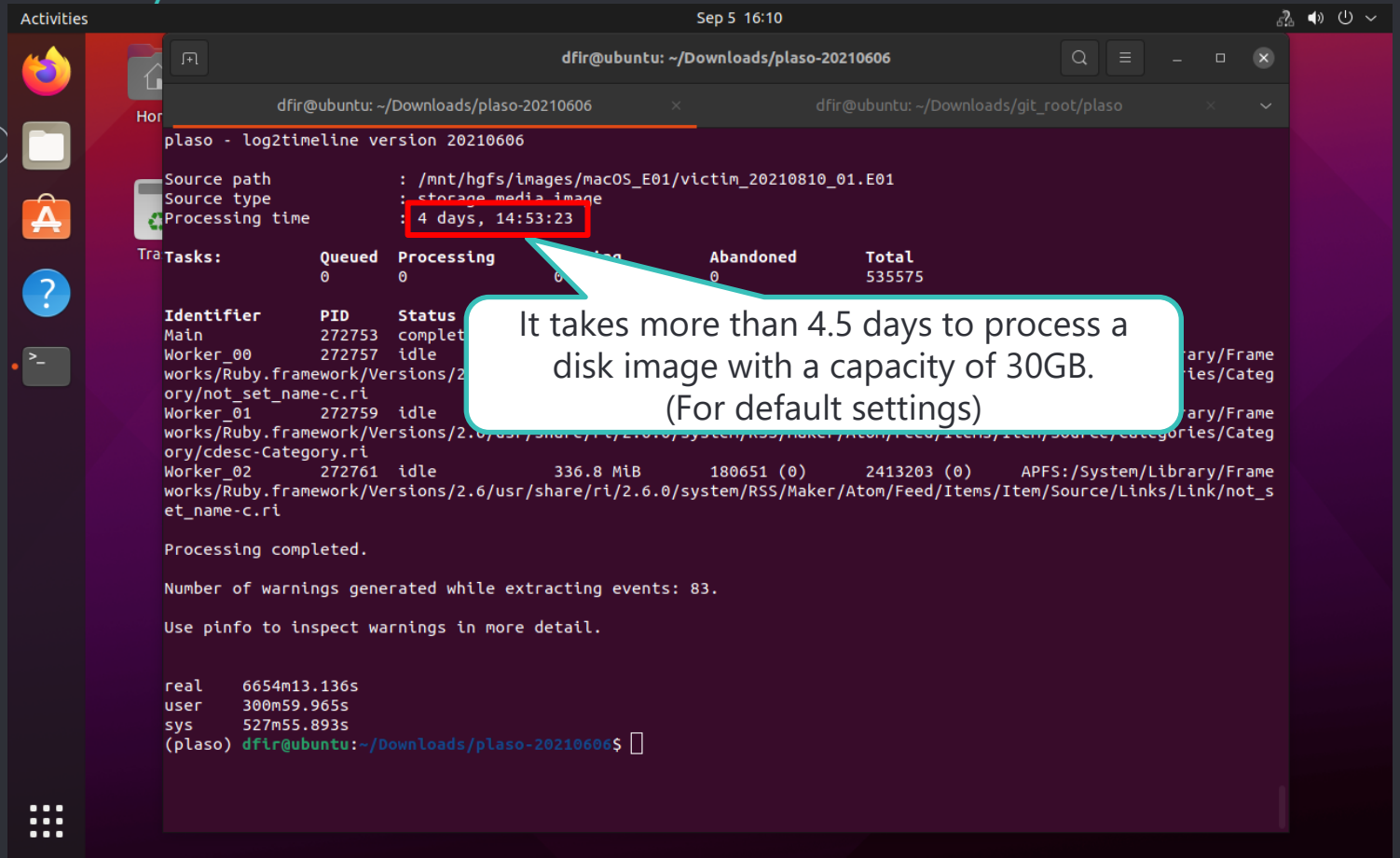
- What to do after collecting artifacts
  - Analyze OS and application artifacts with tools and create a timeline from the results.
- Purpose of creating a timeline
  - Understand the situation (suspicious points) of the affected terminal.
  - Organize the main activities of users, malware, and attackers based on timestamps.
    - Execute programs, download files, mount volumes, set persistence, etc.
  - Creating a timeline can reduce bias, leaps in thinking, and omissions in the research process.

Which tool to choose?

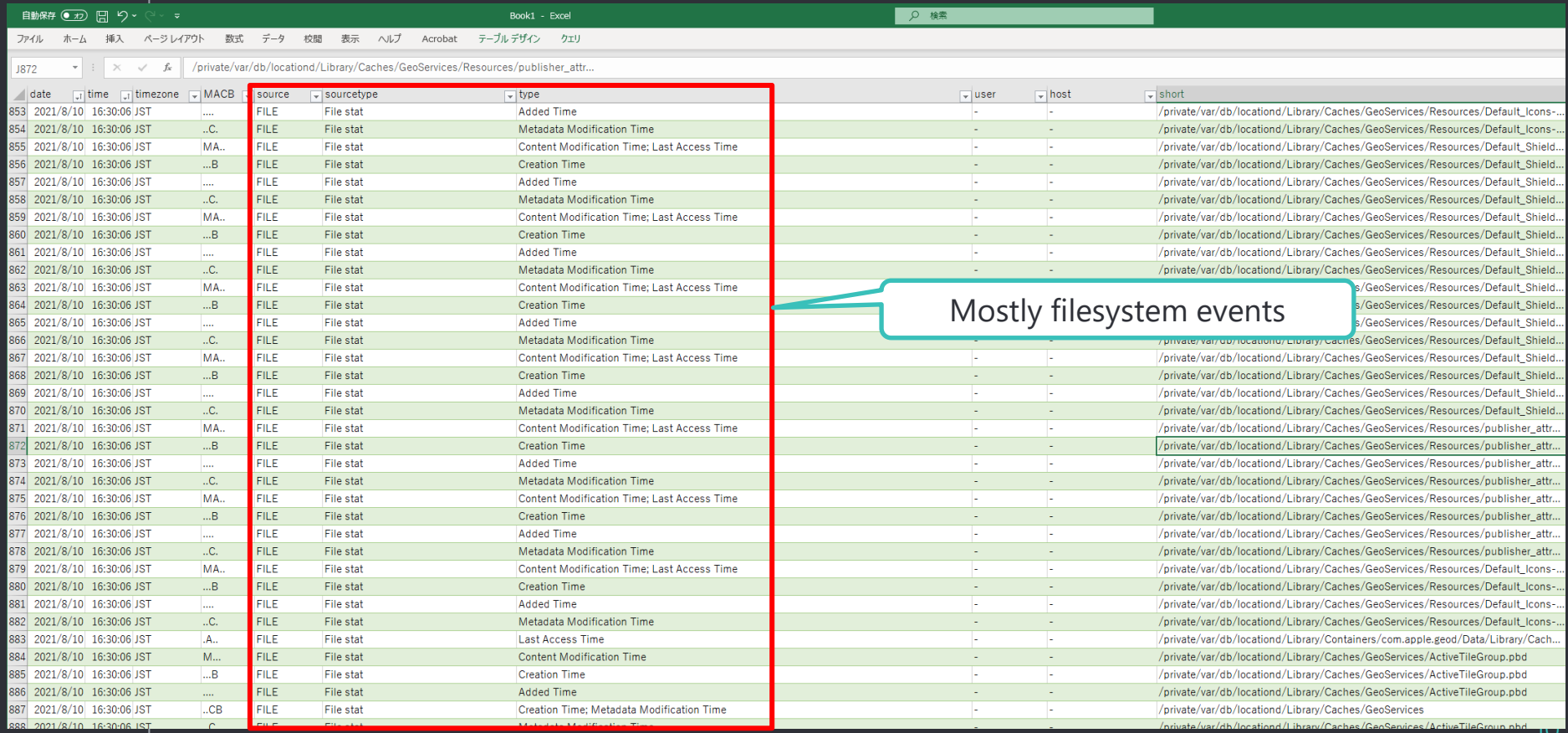
- Plaso
  - https://github.com/log2timeline/plaso
  - Automatic generation of super timelines
  - Capable of analyzing artifacts from various operating systems, including macOS.
  - Maintenance is active
- Plaso can generate super timelines 😃

```
% log2timeline.py --storage-file victim.plaso victim.E01
% psort.py -o l2tcsv -w victime.csv victim.plaso
```

Analyze with Plaso



Super Timeline by Plaso



	date	time	timezone	MACB	source	sourcetype	type	user	host	short
853	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Icons-...
854	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Icons-...
855	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
856	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
857	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
858	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
859	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
860	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
861	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
862	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
863	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
864	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
865	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
866	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
867	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
868	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
869	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
870	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Shield...
871	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
872	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
873	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
874	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
875	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
876	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
877	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
878	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/publisher_attr...
879	2021/8/10	16:30:06	JST	MA..	FILE	File stat	Content Modification Time; Last Access Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Icons-...
880	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Icons-...
881	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Icons-...
882	2021/8/10	16:30:06	JST	..C.	FILE	File stat	Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/Resources/Default_Icons-...
883	2021/8/10	16:30:06	JST	.A..	FILE	File stat	Last Access Time	-	-	/private/var/db/locationd/Library/Containers/com.apple.geod/Data/Library/Cach...
884	2021/8/10	16:30:06	JST	M...	FILE	File stat	Content Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/ActiveTileGroup.pbd
885	2021/8/10	16:30:06	JST	...B	FILE	File stat	Creation Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/ActiveTileGroup.pbd
886	2021/8/10	16:30:06	JST	....	FILE	File stat	Added Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices/ActiveTileGroup.pbd
887	2021/8/10	16:30:06	JST	..CB	FILE	File stat	Creation Time; Metadata Modification Time	-	-	/private/var/db/locationd/Library/Caches/GeoServices

Problems with the super timeline generated by Plaso

- All filesystem metadata is parsed by default.
  - The number of unimportant files in the analysis is much higher.
  - One file metadata is split into four events (MACB).
- The system log is recorded as a line by line event.
  - We want meaningful information about what happened, not just line-by-line events (we don't need just log messages).
  - Unified Logs are not analyzed.
- As a result, most of the super timeline is filled with file system and system log events.
- It takes too long to complete the analysis in the first place.
- This is not the kind of information a forensic analyst wants to see first.

The information the forensic analysts want and the investigation strategy

- For malware infection investigation
  - Persistence setting status
  - Program execution history
  - Volume (USB thumb drives or disk images) mount
  - File Download
- Make this kind of information the most basic timeline.
- Flesh out the timeline by expanding the scope of the investigation or conducting a deeper investigation as needed.

- We need a timeline to use as a basis for the investigation.
- Creating a timeline with only the necessary activities from the analysis results of a tool focused on artifact analysis is more in line with the requirements.

Tools focused on artifact analysis

- There are two candidate analysis tools
  - AutoMacTC
    - https://github.com/CrowdStrike/automactc
    - Maintenance is stagnant.
  - mac_apt
    - https://github.com/ydkhatri/mac_apt
    - Maintenance is active.

Which tool should we use?

- In view of the maintenance status and functionality, I recommend "mac_apt".
- Why is maintenance so important?
  - macOS artifacts often change their file names and paths with version upgrades.
  - Using analysis tools that are not maintained will increase the number of artifacts that cannot be analyzed over time.
- Unified Logs parser is implemented.
  - Unified Logs records a lot of useful information, but only mac_apt has a parser implemented in OSS.

Motivation for creating the tool

- It is currently best to create a timeline that can be used as a template from the results of mac_apt analysis.
- To create a timeline from mac_apt analysis results, we need to refer to various tables.
  - A table will be created for the number of plugins used in the analysis.
  - Spotlight tables are cumbersome with many columns.
- Unified Logs contain useful information, but mac_apt does not analyze them according to the message content.
  - The message may change depending on the OS version upgrade.
  - It is complicated to do a lot of filtering manually.
  - Even with filtering, the output results may be large, and it may be difficult to visually check.
- I need a tool that automatically generates a forensic timeline!

Similar Tools

- In terms of organizing, displaying, and checking the results of mac_apt analysis, the following tools also exist
  - mac_int
    - https://burnhamforensics.com/projects/mac_int/
  - Building a Visualization Tool for mac_apt
    - https://leahycenterblog.champlain.edu/2020/05/01/building-a-visualization-tool-for-mac_apt/
- Different in the following ways
  - The main purpose of these tools is to check the results of mac_apt analysis in GUI, not to generate a timeline.
  - No maintenance is being performed at this time.

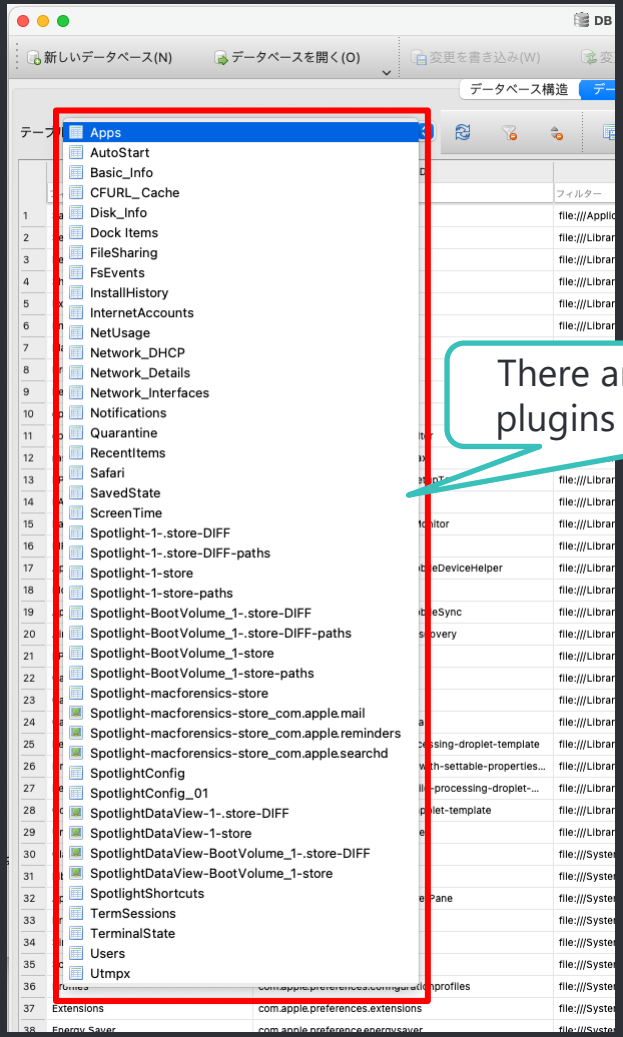
2

How to create a timeline using the analysis results of mac_apt

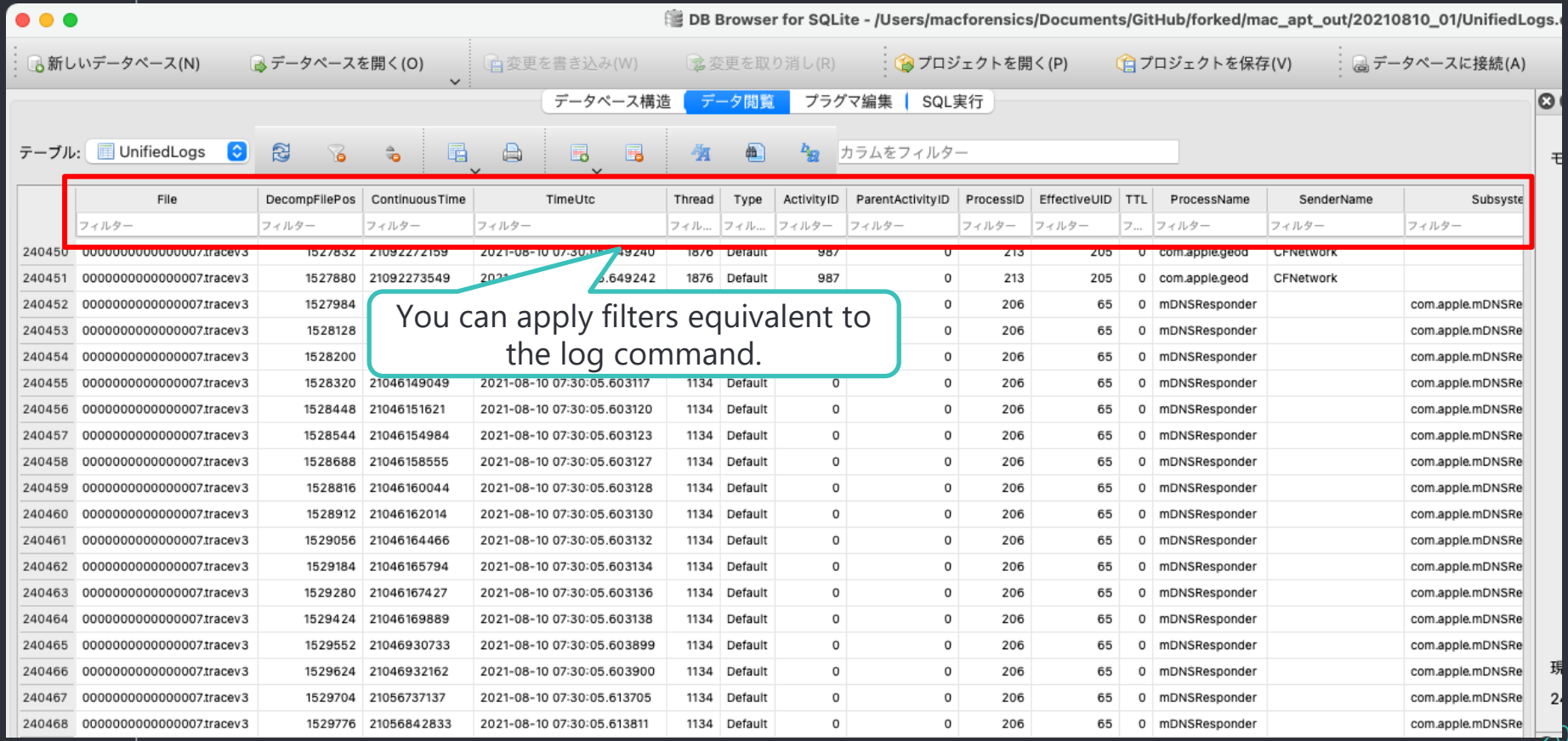
Analysis results of mac_apt

- DB where mac_apt stores the analysis results
  - mac_apt.db : Results of artifact analysis
  - UnifiedLogs.db : Parsed Unified Logs
  - APFS_Volumes_<GUID>.db : Parsed APFS metadata
  - Export and SPOTLIGHT_DATA : Folder where the artifact files exported from the disk image will be saved

mac_apt.db

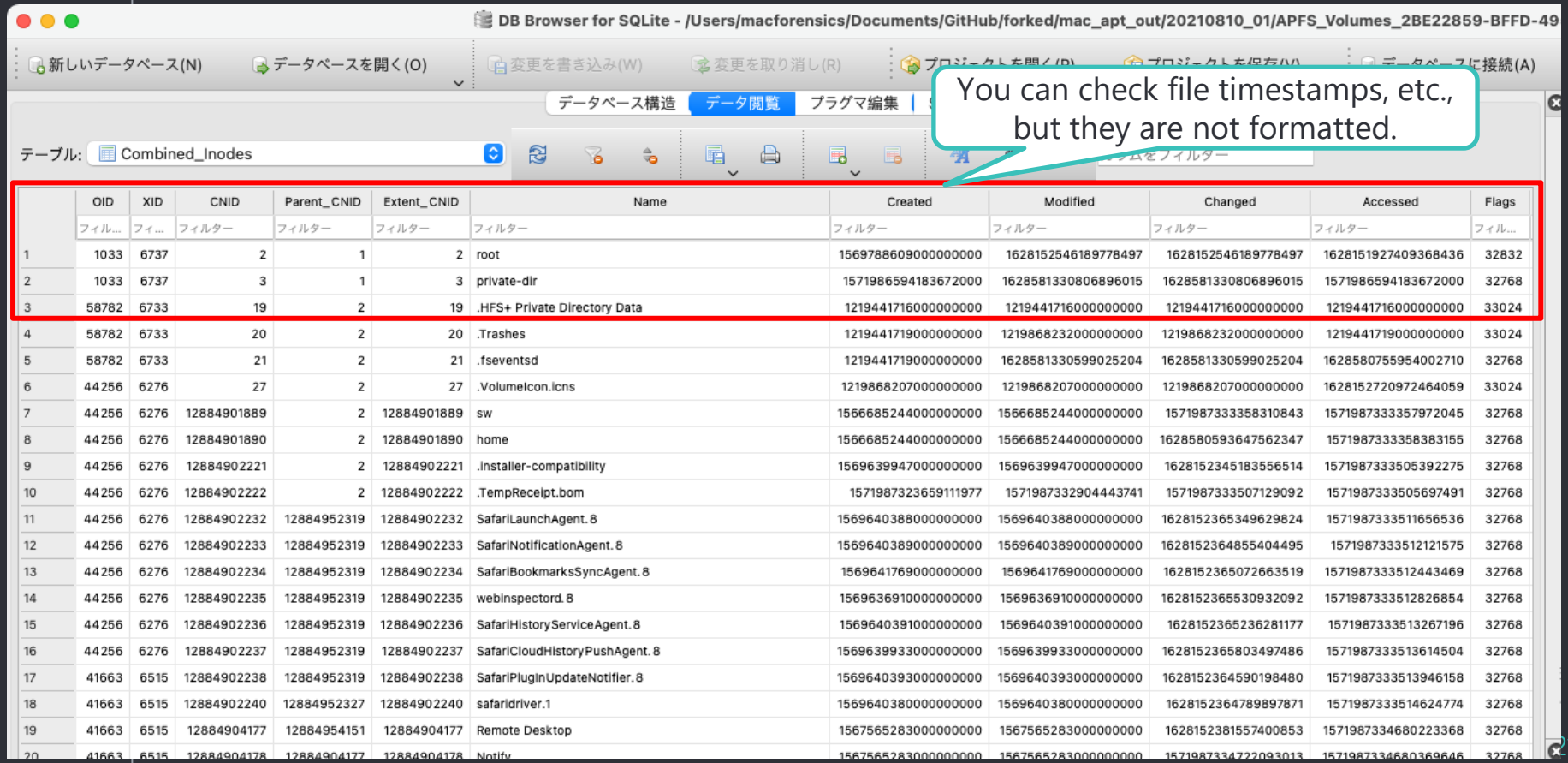

DB
新しいデータベース(N)
データベースを開く(O)
変更を書き込み(W)
データベース構造
Apps
AutoStart
Basic_Info
CFURL_Cache
Disk_Info
Dock Items
FileSharing
FsEvents
InstallHistory
InternetAccounts
NetUsage
Network_DHCP
Network_Details
Network_Interfaces
Notifications
Quarantine
RecentItems
Safari
SavedState
ScreenTime
Spotlight-1-.store-DIFF
Spotlight-1-.store-DIFF-paths
Spotlight-1-store
Spotlight-1-store-paths
Spotlight-BootVolume_1-.store-DIFF
Spotlight-BootVolume_1-.store-DIFF-paths
Spotlight-BootVolume_1-store
Spotlight-BootVolume_1-store-paths
Spotlight-macforensics-store
Spotlight-macforensics-store_com.apple.mail
Spotlight-macforensics-store_com.apple.reminders
Spotlight-macforensics-store_com.apple.searchd
SpotlightConfig
SpotlightConfig_01
SpotlightDataView-1-.store-DIFF
SpotlightDataView-1-store
SpotlightDataView-BootVolume_1-.store-DIFF
SpotlightDataView-BootVolume_1-store
SpotlightShortcuts
TermSessions
TerminalState
Users
Utmpx
There are as many tables as plugins used in the analysis.

UnifiedLogs.db



	File	DecompFilePos	ContinuousTime	TimeUtc	Thread	Type	ActivityID	ParentActivityID	ProcessID	EffectiveUID	TTL	ProcessName	SenderName	Subsyste
	フィルター	フィルター	フィルター	フィルター	フィル...	フィル...	フィルター	フィルター	フィルター	フィルター	フ...	フィルター	フィルター	フィルター
240450	0000000000000007.tracev3	1527832	21092272159	2021-08-10 07:30:0[illegible]9240	1876	Default	987	0	213	205	0	com.apple.geod	CFNetwork	
240451	0000000000000007.tracev3	1527880	21092273549	2021-08-10 07:30:05.649242	1876	Default	987	0	213	205	0	com.apple.geod	CFNetwork	
240452	0000000000000007.tracev3	1527984						0	206	65	0	mDNSResponder		com.apple.mDNSRe
240453	0000000000000007.tracev3	1528128						0	206	65	0	mDNSResponder		com.apple.mDNSRe
240454	0000000000000007.tracev3	1528200						0	206	65	0	mDNSResponder		com.apple.mDNSRe
240455	0000000000000007.tracev3	1528320	21046149049	2021-08-10 07:30:05.603117	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240456	0000000000000007.tracev3	1528448	21046151621	2021-08-10 07:30:05.603120	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240457	0000000000000007.tracev3	1528544	21046154984	2021-08-10 07:30:05.603123	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240458	0000000000000007.tracev3	1528688	21046158555	2021-08-10 07:30:05.603127	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240459	0000000000000007.tracev3	1528816	21046160044	2021-08-10 07:30:05.603128	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240460	0000000000000007.tracev3	1528912	21046162014	2021-08-10 07:30:05.603130	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240461	0000000000000007.tracev3	1529056	21046164466	2021-08-10 07:30:05.603132	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240462	0000000000000007.tracev3	1529184	21046165794	2021-08-10 07:30:05.603134	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240463	0000000000000007.tracev3	1529280	21046167427	2021-08-10 07:30:05.603136	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240464	0000000000000007.tracev3	1529424	21046169889	2021-08-10 07:30:05.603138	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240465	0000000000000007.tracev3	1529552	21046930733	2021-08-10 07:30:05.603899	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240466	0000000000000007.tracev3	1529624	21046932162	2021-08-10 07:30:05.603900	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240467	0000000000000007.tracev3	1529704	21056737137	2021-08-10 07:30:05.613705	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe
240468	0000000000000007.tracev3	1529776	21056842833	2021-08-10 07:30:05.613811	1134	Default	0	0	206	65	0	mDNSResponder		com.apple.mDNSRe

APFS_Volumes_<GUID>. db



	OID	XID	CNID	Parent_CNID	Extent_CNID	Name	Created	Modified	Changed	Accessed	Flags
1	1033	6737	2	1	2	root	1569788609000000000	1628152546189778497	1628152546189778497	1628151927409368436	32832
2	1033	6737	3	1	3	private-dir	1571986594183672000	1628581330806896015	1628581330806896015	1571986594183672000	32768
3	58782	6733	19	2	19	.HFS+ Private Directory Data	1219441716000000000	1219441716000000000	1219441716000000000	1219441716000000000	33024
4	58782	6733	20	2	20	.Trashes	1219441719000000000	1219868232000000000	1219868232000000000	1219441719000000000	33024
5	58782	6733	21	2	21	.fseventsd	1219441719000000000	1628581330599025204	1628581330599025204	1628580755954002710	32768
6	44256	6276	27	2	27	.VolumeIcon.icns	1219868207000000000	1219868207000000000	1219868207000000000	1628152720972464059	33024
7	44256	6276	12884901889	2	12884901889	sw	1566685244000000000	1566685244000000000	1571987333358310843	1571987333357972045	32768
8	44256	6276	12884901890	2	12884901890	home	1566685244000000000	1566685244000000000	1628580593647562347	1571987333358383155	32768
9	44256	6276	12884902221	2	12884902221	.installer-compatibility	1569639947000000000	1569639947000000000	1628152345183556514	1571987333505392275	32768
10	44256	6276	12884902222	2	12884902222	.TempReceipt.bom	1571987323659111977	1571987332904443741	1571987333507129092	1571987333505697491	32768
11	44256	6276	12884902232	12884952319	12884902232	SafariLaunchAgent.8	1569640388000000000	1569640388000000000	1628152365349629824	1571987333511656536	32768
12	44256	6276	12884902233	12884952319	12884902233	SafariNotificationAgent.8	1569640389000000000	1569640389000000000	1628152364855404495	1571987333512121575	32768
13	44256	6276	12884902234	12884952319	12884902234	SafariBookmarksSyncAgent.8	1569641769000000000	1569641769000000000	1628152365072663519	1571987333512443469	32768
14	44256	6276	12884902235	12884952319	12884902235	webinspectord.8	1569636910000000000	1569636910000000000	1628152365530932092	1571987333512826854	32768
15	44256	6276	12884902236	12884952319	12884902236	SafariHistoryServiceAgent.8	1569640391000000000	1569640391000000000	1628152365236281177	1571987333513267196	32768
16	44256	6276	12884902237	12884952319	12884902237	SafariCloudHistoryPushAgent.8	1569639933000000000	1569639933000000000	1628152365803497486	1571987333513614504	32768
17	41663	6515	12884902238	12884952319	12884902238	SafariPluginUpdateNotifier.8	1569640393000000000	1569640393000000000	1628152364590198480	1571987333513946158	32768
18	41663	6515	12884902240	12884952327	12884902240	safaridriver.1	1569640380000000000	1569640380000000000	1628152364789897871	1571987333514624774	32768
19	41663	6515	12884904177	12884954151	12884904177	Remote Desktop	1567565283000000000	1567565283000000000	1628152381557400853	1571987334680223368	32768
20	41663	6515	12884904178	12884904177	12884904178	Notify	1567565283000000000	1567565283000000000	1571987334722093013	1571987334680369646	32768

Timeline Creation Policy

- Focus the investigation on analysis results with time stamps.
  - If timestamp is missing, refer to other tables or APFS_Volumes_xxxx.db
- Create a timeline for the following activities
  - Persistence setting status
  - Program execution history
  - Volume mount
  - File Download

Persistence Analysis (1/3)

- mac_apt.db : AutoStart
  - First, check the general user settings.
  - No timestamp was recorded.

テーブル: AutoStart

カラムをフィルター

	Type	Name	User	StartupType	Disabled	AppPath	Source
	フィルター	フィルター	macforensics	フィルター	フィルター	フィルター	フィルター
1	Background ...	BlockBlock Helper	macforensics	Run at Login		/Applications/BlockBlock Helper.app	/Users/macforensics/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm
2	Background ...	KeepingYouAwake Launcher.app	macforensics	Run at Login		/Applications/KeepingYouAwake.app/Contents/Library/...	/Users/macforensics/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm
3	Background ...	MountyHelper	macforensics	Run at Login		/Applications/Mounty.app/Contents/Library/LoginItems/...	/Users/macforensics/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm
4	Background ...	LuLu	macforensics	Run at Login		/Applications/LuLu.app	/Users/macforensics/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm
5	Background ...	LaunchAtLoginHelper.app	macforensics	Run at Login		/Applications/LaunchAtLogin.app/Contents/Library/LoginItems/...	/Users/macforensics/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm
6	Apps To ...	com.apple.finder	macforensics	Run at Login		/System/Library/CoreServices/Finder.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist
7	Apps To ...	com.apple.terminal	macforensics	Run at Login		/System/Applications/Utilities/Terminal.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist
8	Apps To ...	net.sourceforge.sqlitebrowser	macforensics	Run at Login		/Applications/DB Browser for SQLite.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist
9	Apps To ...	com.vmware.fusion	macforensics	Run at Login		/Applications/VMware Fusion.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist
10	Apps To ...	com.microsoft.vscode	macforensics	Run at Login		/Applications/Visual Studio Code.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist
11	Apps To ...	com.evernote.evernote	macforensics	Run at Login		/Applications/Evernote.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist
12	Apps To ...	org.mozilla.firefox	macforensics	Run at Login		/Applications/Firefox.app	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.C10D872E-0A37-54FA-8ABB-6788CD3453EA.plist

Autorun program

Autorun configuration file

Persistence Analysis (2/3)

- Check the timestamp of the auto-run configuration file and the executable in APFS_Volumes_xxxx.db

```
SELECT * FROM Combined_Paths LEFT JOIN Combined_Inodes ON Combined_Paths.CNID = Combined_Inodes.CNID WHERE
Combined_Paths.Path = "/path/to/file" LIMIT 1;
```

	CNID	Path	OID	XID	CNID	Parent_CNID	Extent_CNID	Name	Created	Modified	Changed	Accessed
1	25694948	/Users/macforensics/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm	961668	1223	25694948	1097909	25694948	backgrounditems.btm	1632886716865390428	1632886716865601893	1632886716866972041	1633103847655622647

	CNID	Path	OID	XID	CNID	Parent_CNID	Extent_CNID	Name	Created	Modified	Changed	Accessed
1	21400048	/Applications/KeepingYouAwake.app/Contents/Library/...	875376	851	21400048	21400047	21400048	KeepingYouAwake Launcher.app	1627112080000000000	1627112080000000000	1627137248003391691	1627137247993534000

File creation timestamp

Persistence Analysis (3/3)

- Many autorun programs can be found in the folders listed on the right.
- Since macOS 10.15, the system volume and data volume have been split.
  - The system volume is mounted as read-only, so the risk of tampering is lower than before.
  - Starting with macOS 11, the system volume is also signed.
- Therefore, programs on the system volume can be excluded from the investigation at first

Excerpt from the source code of ma2tl

```
26  std_apppath_system_vol = (
27      '/System/Applications/',
28      '/System/Library/CoreServices/',
29      '/System/Library/Extensions/',
30      '/System/Library/Frameworks/',
31      '/System/Library/PrivateFrameworks/',
32      '/System/Library/CryptoTokenKit/',
33      '/System/Library/Filesystems/',
34      '/System/Library/Image Capture/',
35      '/System/Library/Input Methods/',
36      '/System/Library/PreferencePanes/',
37      '/System/Library/Services/',
38      '/System/iOSSupport/',
39      '/System/Installation/',
40      '/usr/libexec/',
41      '/usr/bin/',
42      '/usr/sbin/',
43      '/bin/',
44      '/sbin/'
45  )
46
47  std_persistence_system_vol = (
48      '/System/Library/LaunchDaemons/',
49      '/System/Library/LaunchAgents/'
50  )
51
52  std_apppath_data_vol = (
53      '/Applications/',
54      '/Library/Apple/',
55      '/Library/Application Support/',
56      '/Library/Extensions/'
57  )
```

Since macOS 10.15, it is mounted as read-only, so there is little risk of tampering.

System volume

Data volume

Program execution history analysis

- mac_apt.db : SpotlightShortcuts
  - Applications executed via Spotlight will be recorded.

The string entered in Spotlight

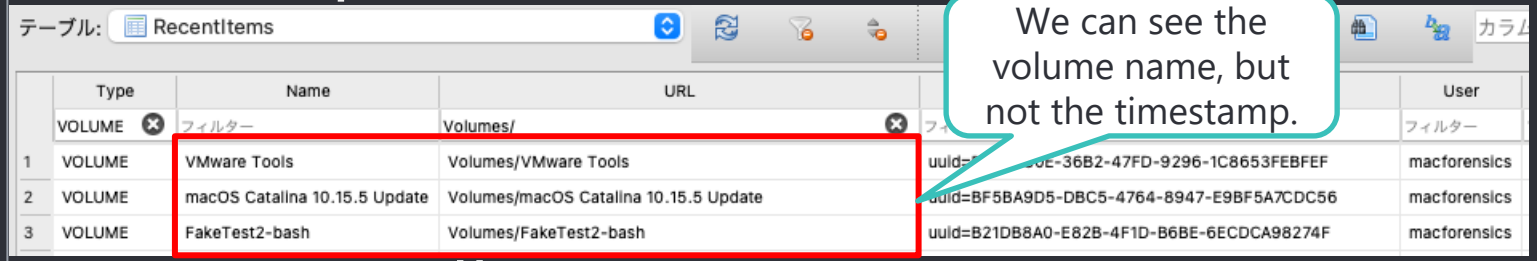
Timestamp
(Only the date and time of the last execution.)

Application path

Application name

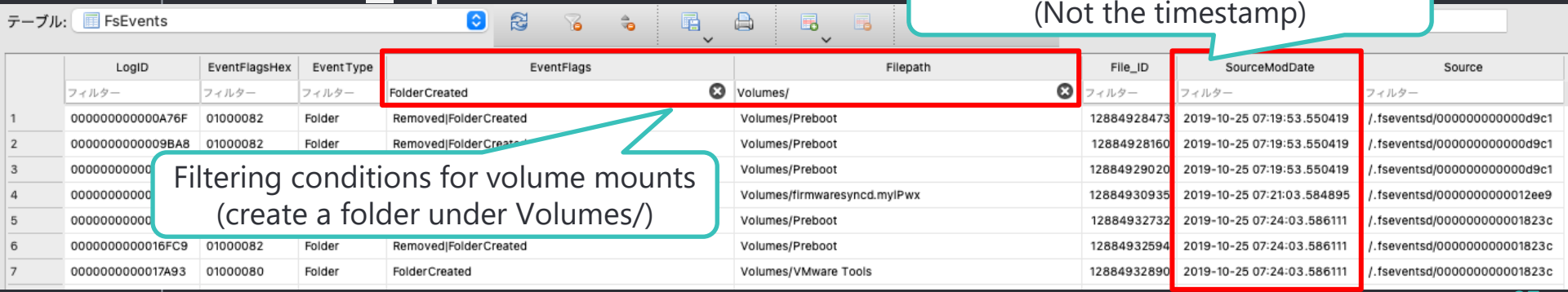
	User	UserTyped	DisplayName	LastUsed	URL	Source
	フィルター	フィルター	フィルター	フィルター	フィルター	
1	macforensics	activi	アクティビティモニタ	2	/System/Applications/Utilities/Activity Monitor.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
2	macforensics	applesc	スクリプトエディタ	2021-09-27 08:28:31	/System/Applications/Utilities/Script Editor.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
3	macforensics	applescri	スクリプトエディタ	2019-09-25 01:46:04	/System/Applications/Utilities/Script Editor.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
4	macforensics	atom	Atom	2019-10-10 05:37:02	/Applications/Atom.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
5	macforensics	auto	Automator	2021-09-27 08:03:54	/System/Applications/Automator.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
6	macforensics	blackl	BlackLight	2019-07-31 02:19:55	/Applications/BlackLight/BlackLight 2019 Release 1.1/...	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
7	macforensics	bre	Brewlet	2021-09-28 00:20:59	/Applications/Brewlet.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
8	macforensics	brew	Brewlet	2021-09-09 06:40:28	/Applications/Brewlet.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
9	macforensics	cal	計算機	2021-10-01 09:15:52	/System/Applications/Calculator.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
10	macforensics	calc	計算機	2021-09-13 02:11:07	/System/Applications/Calculator.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
11	macforensics	ch	Google Chrome	2021-09-13 02:10:43	/Applications/Google Chrome.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
12	macforensics	chro	Google Chrome	2021-09-29 04:18:17	/Applications/Google Chrome.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
13	macforensics	chrome	Google Chrome	2021-09-27 05:31:26	/Applications/Google Chrome.app	/Users/macforensics/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3

- Volume mount analysis
  - mac_apt.db : RecentItems



	Type	Name	URL	User
	VOLUME	フィルター	Volumes/	フィルター
1	VOLUME	VMware Tools	Volumes/VMware Tools	macforensics
2	VOLUME	macOS Catalina 10.15.5 Update	Volumes/macOS Catalina 10.15.5 Update	macforensics
3	VOLUME	FakeTest2-bash	Volumes/FakeTest2-bash	macforensics

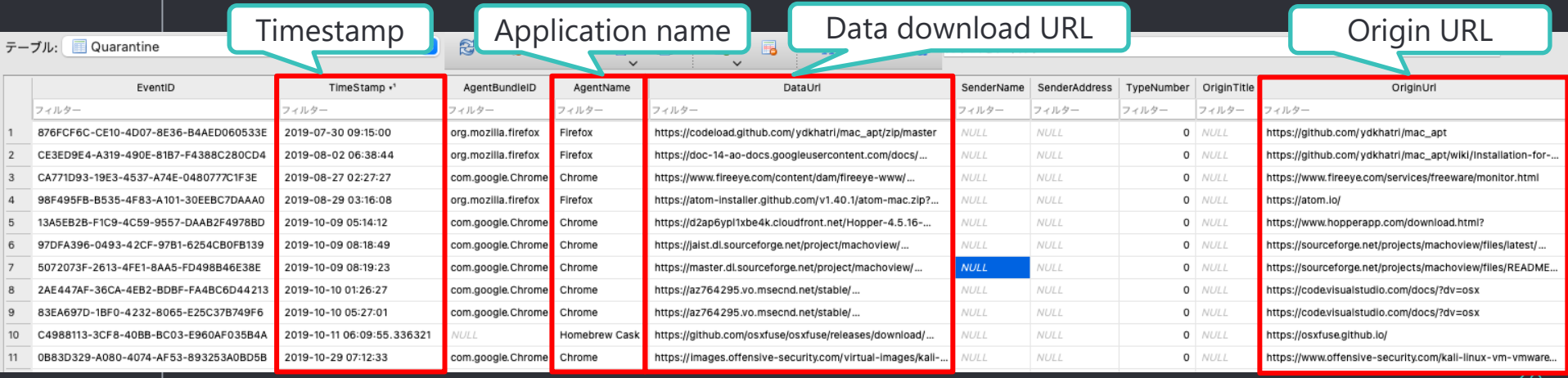
  - mac_apt.db : FsEvents



	LogID	EventFlagsHex	EventType	EventFlags	Filepath	File_ID	SourceModDate	Source
	フィルター	フィルター	フィルター	FolderCreated	Volumes/	フィルター	フィルター	フィルター
1	000000000000A76F	01000082	Folder	Removed|FolderCreated	Volumes/Preboot	12884928473	2019-10-25 07:19:53.550419	/.fseventsd/000000000000d9c1
2	0000000000009BA8	01000082	Folder	Removed|FolderCreated	Volumes/Preboot	12884928160	2019-10-25 07:19:53.550419	/.fseventsd/000000000000d9c1
3	0000000000				Volumes/Preboot	12884929020	2019-10-25 07:19:53.550419	/.fseventsd/000000000000d9c1
4	0000000000				Volumes/firmwaresyncd.myIPwx	12884930935	2019-10-25 07:21:03.584895	/.fseventsd/0000000000012ee9
5	0000000000				Volumes/Preboot	12884932732	2019-10-25 07:24:03.586111	/.fseventsd/000000000001823c
6	0000000000016FC9	01000082	Folder	Removed|FolderCreated	Volumes/Preboot	12884932594	2019-10-25 07:24:03.586111	/.fseventsd/000000000001823c
7	0000000000017A93	01000080	Folder	FolderCreated	Volumes/VMware Tools	12884932890	2019-10-25 07:24:03.586111	/.fseventsd/000000000001823c

File download analysis (1/5)

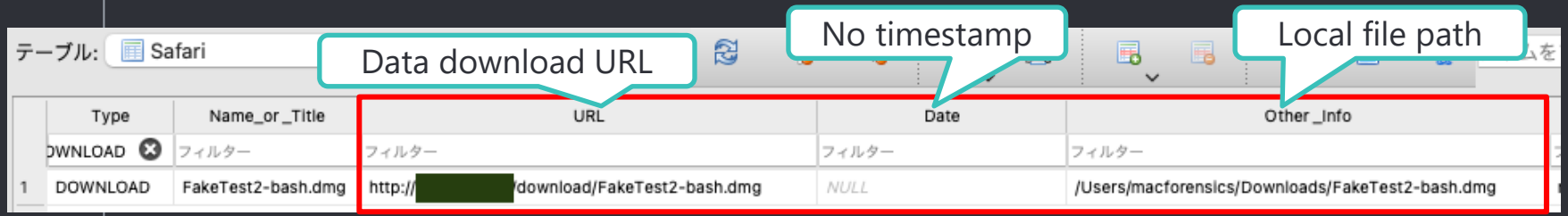
- mac_apt.db : Quarantine
  - DB analysis results that store the same content as the com.apple.quarantine extended attribute that is assigned to files downloaded by web browsers, etc.



	EventID	TimeStamp	AgentBundleID	AgentName	DataUrl	SenderName	SenderAddress	TypeNumber	OriginTitle	OriginUrl
	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター
1	876FCF6C-CE10-4D07-8E36-B4AED060533E	2019-07-30 09:15:00	org.mozilla.firefox	Firefox	https://codeload.github.com/ydkhatri/mac_apt/zip/master	NULL	NULL	0	NULL	https://github.com/ydkhatri/mac_apt
2	CE3ED9E4-A319-490E-81B7-F4388C280CD4	2019-08-02 06:38:44	org.mozilla.firefox	Firefox	https://doc-14-ao-docs.googleusercontent.com/docs/...	NULL	NULL	0	NULL	https://github.com/ydkhatri/mac_apt/wiki/Installation-for-...
3	CA771D93-19E3-4537-A74E-0480777C1F3E	2019-08-27 02:27:27	com.google.Chrome	Chrome	https://www.fireeye.com/content/dam/fireeye-www/...	NULL	NULL	0	NULL	https://www.fireeye.com/services/freeware/monitor.html
4	98F495FB-B535-4F83-A101-30EEBC7DAAA0	2019-08-29 03:16:08	org.mozilla.firefox	Firefox	https://atom-installer.github.com/v1.40.1/atom-mac.zip?...	NULL	NULL	0	NULL	https://atom.io/
5	13A5EB2B-F1C9-4C59-9557-DAAB2F4978BD	2019-10-09 05:14:12	com.google.Chrome	Chrome	https://d2ap6ypl1xbe4k.cloudfront.net/Hopper-4.5.16-...	NULL	NULL	0	NULL	https://www.hopperapp.com/download.html?
6	97DFA396-0493-42CF-97B1-6254CB0FB139	2019-10-09 08:18:49	com.google.Chrome	Chrome	https://jaist.dl.sourceforge.net/project/machoview/...	NULL	NULL	0	NULL	https://sourceforge.net/projects/machoview/files/latest/...
7	5072073F-2613-4FE1-8AA5-FD498B46E38E	2019-10-09 08:19:23	com.google.Chrome	Chrome	https://master.dl.sourceforge.net/project/machoview/...	NULL	NULL	0	NULL	https://sourceforge.net/projects/machoview/files/README...
8	2AE447AF-36CA-4EB2-BDBF-FA4BC6D44213	2019-10-10 01:26:27	com.google.Chrome	Chrome	https://az764295.vo.msecnd.net/stable/...	NULL	NULL	0	NULL	https://code.visualstudio.com/docs/?dv=osx
9	83EA697D-1BF0-4232-8065-E25C37B749F6	2019-10-10 05:27:01	com.google.Chrome	Chrome	https://az764295.vo.msecnd.net/stable/...	NULL	NULL	0	NULL	https://code.visualstudio.com/docs/?dv=osx
10	C4988113-3CF8-40BB-BC03-E960AF035B4A	2019-10-11 06:09:55.336321	NULL	Homebrew Cask	https://github.com/osxfuse/osxfuse/releases/download/...	NULL	NULL	0	NULL	https://osxfuse.github.io/
11	0B83D329-A080-4074-AF53-893253A0BD5B	2019-10-29 07:12:33	com.google.Chrome	Chrome	https://images.offensive-security.com/virtual-images/kali-...	NULL	NULL	0	NULL	https://www.offensive-security.com/kali-linux-vm-vmware...

File download analysis (2/5)

- mac_apt.db : Safari
  - The destination of the file will be recorded.
  - Since there is no timestamp, the timestamp is inferred by linking the URL to the DataUrl in the Quarantine table.
  - Safari's download history is deleted after a day by default.



File download analysis (3/5)

- mac_apt.db : Chrome

テーブル: Chrome

カラムをフィルター

	Type	Name_or_Title	URL	Date ▾¹	End Date	Local Path	Referrer or Previous Page	Other_Info
	WNLOAD	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター	フィルター
1	DOWNLOAD	sdl-monitor.zip	https://www.fireeye.com/content/dam/fireeye-www/...	2019-08-27 02:27:27.464501	2019-08-27 02:27:29.604466	/Users/macforensics/Downloads/sdl-monitor.zip	https://www.fireeye.com/services/freeware/monitor.html	Received Bytes = 7692341/7692341
2	DOWNLOAD	Hopper-4.5.16-demo.dmg	https://d2ap6ypl1xbe4k.cloudfront.net/Hopper-4.5.16-...	2019-10-09 05:14:12.480311	2019-10-09 05:14:26.798347	/Users/macforensics/Downloads/Hopper-4.5.16-demo.dmg	https://www.hopperapp.com/download.html?	Received Bytes = 33689651/33689651
3	DOWNLOAD	MachOView-2.4.9200.dmg	https://sourceforge.net/projects/machoview/files/latest/...	2019-10-09 08:18:49.483219	2019-10-09 08:18:50.915335	/Users/macforensics/Downloads/...	https://sourceforge.net/projects/machoview/files/latest/...	Received Bytes = 8809952/8809952
4	DOWNLOAD	README	https://sourceforge.net/projects/machoview/files/README...	2019-10-09 08:19:23.285423	2019-10-09 08:19:23.486107	/Users/macforensics/Downloads/README	https://sourceforge.net/projects/machoview/files/README...	Received Bytes = 3161/3161
5	DOWNLOAD	VSCode-darwin-stable.zip	https://code.visualstudio.com/docs/?dv=osx	2019-10-10 01:26:27.983309	2019-10-10 01:26:35.131621	/Users/macforensics/Downloads/VSCode-darwin-stable.zip	https://code.visualstudio.com/docs/?dv=osx	Received Bytes = 79314517/79314517
6	DOWNLOAD	VSCode-darwin-stable (1).zip	https://code.visualstudio.com/docs/?dv=osx	2019-10-10 05:27:01.509979	2019-10-10 05:27:08.834005	/Users/macforensics/Downloads/VSCode-darwin-stable ...	https://code.visualstudio.com/docs/?dv=osx	Received Bytes = 79314517/79314517
7	DOWNLOAD	kali-linux-2019.3-vmware-amd64.7z	https://www.offensive-security.com/kali-linux-vm-vmware...	2019-10-29 07:12:33.813455	2019-10-29 07:15:58.915961	/Users/macforensics/Downloads/kali-linux-2019.3-...	https://www.offensive-security.com/kali-linux-vm-vmware...	Received Bytes = 2287213608/2287213608
8	DOWNLOAD	Dummy.zip	https://objective-see.com/downloads/malware/Dummy.zip	2019-12-23 10:11:51.649643	2019-12-23 10:11:55.658081	/Users/macforensics/Downloads/Dummy.zip		Received Bytes = 10336168/10336168

Data download URL

Download start timestamp

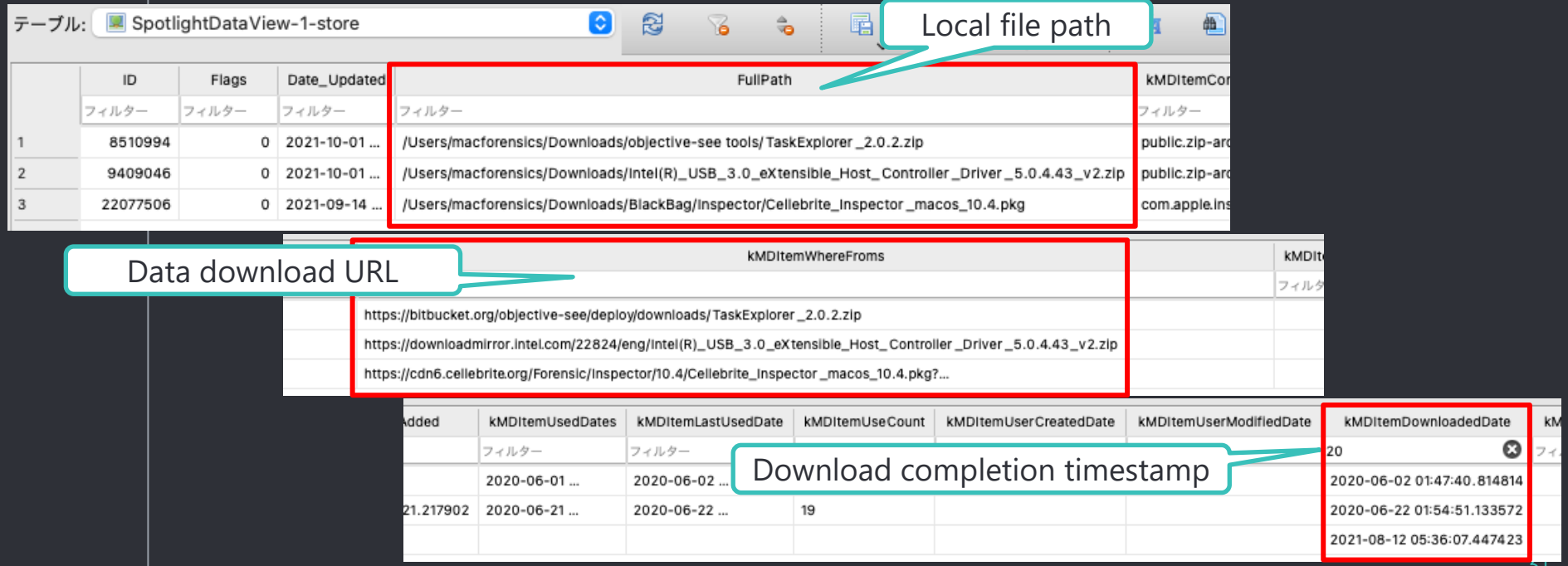
Download completion timestamp

Local file path

Origin URL

File download analysis (4/5)

mac_apt.db : SpotlightDataView



File download analysis (5/5)

- No artifacts are left behind when files are downloaded with the macOS standard command "curl".
  - It leaves traces of the curl execution itself, but does not tell us where it was accessed.
- In such cases, other investigations such as malware analysis are also necessary.

Information confirmed from mac_apt analysis results (1/2)

- Persistence setting status
  - We know the autorun configuration file and the program to be autorun.
  - We can also see the timestamps of the above files.
- Program execution history
  - We know which applications were executed via Spotlight.
  - We know when it was last executed.
  - There is no other execution history with timestamps.
- Volume mount
  - We know the name of the volume you mounted.
  - The exact date and time of the mount is unknown.
- File Download
  - We know the date and time of the download, the URL from which it was downloaded, and the file path to which it was saved.

Not enough information.

Information confirmed from mac_apt analysis results (2/2)

- The information in mac_apt.db alone is clearly not enough to create a timeline
- Any other data we should investigate?

"UnifiedLogs.db"

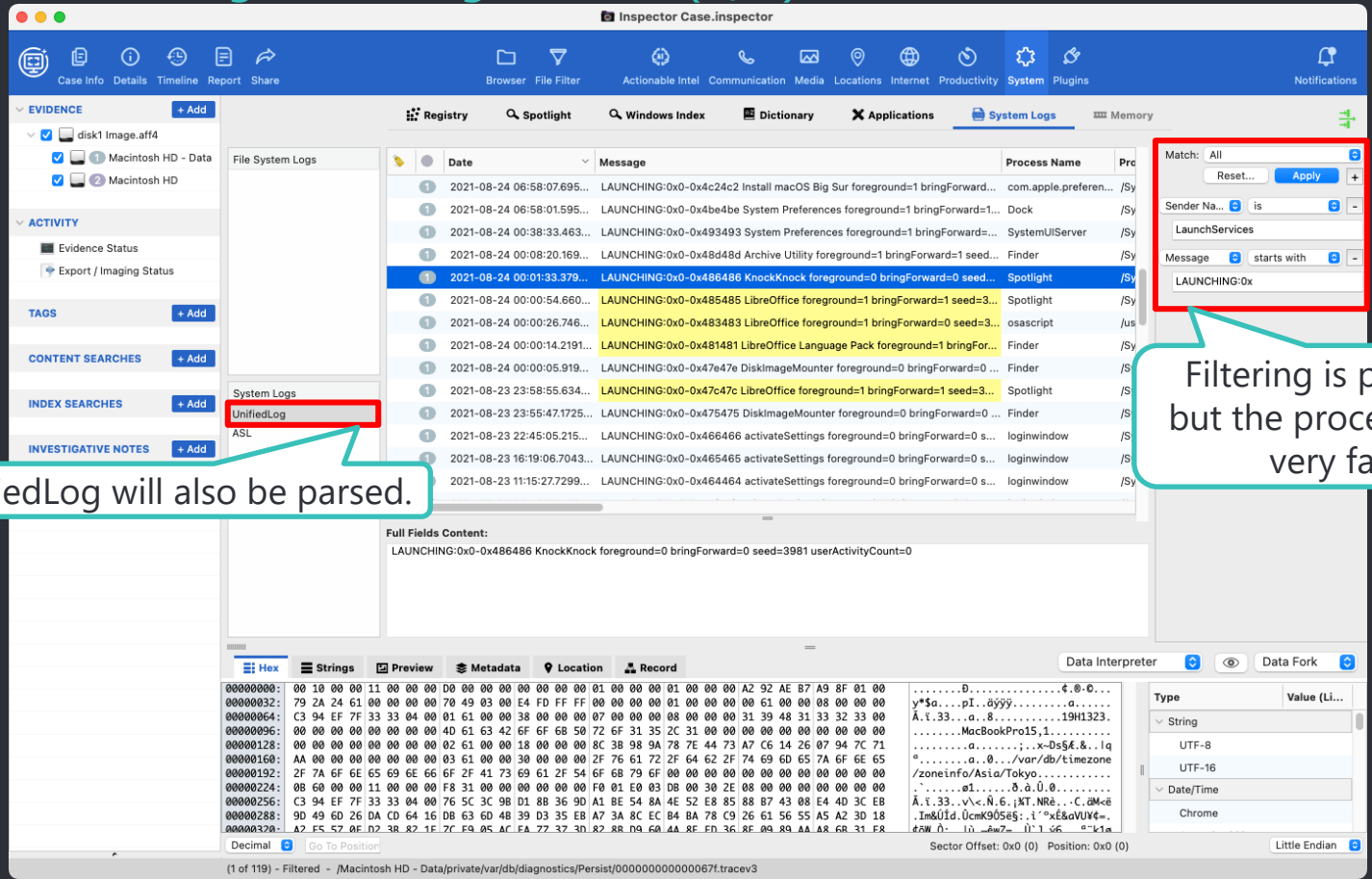
UnifiedLogs.db is a goldmine (1/5)

- Unified Logs contains information necessary to create a timeline, such as program execution history and volume mount history, which are not left in other artifacts.
- A veritable gold mine for macOS forensics
- But for some reason, I almost never see articles or blogs that explain this kind of information.

UnifiedLogs.db is a goldmine (2/5)

- Even commercial products parse Unified Logs, but do not perform analysis based on message content.
- Database load time, filtering time, etc. are also slower than processing UnifiedLogs.db.

UnifiedLogs.db is a goldmine (3/5)



UnifiedLog will also be parsed.

Filtering is possible, but the process is not very fast.

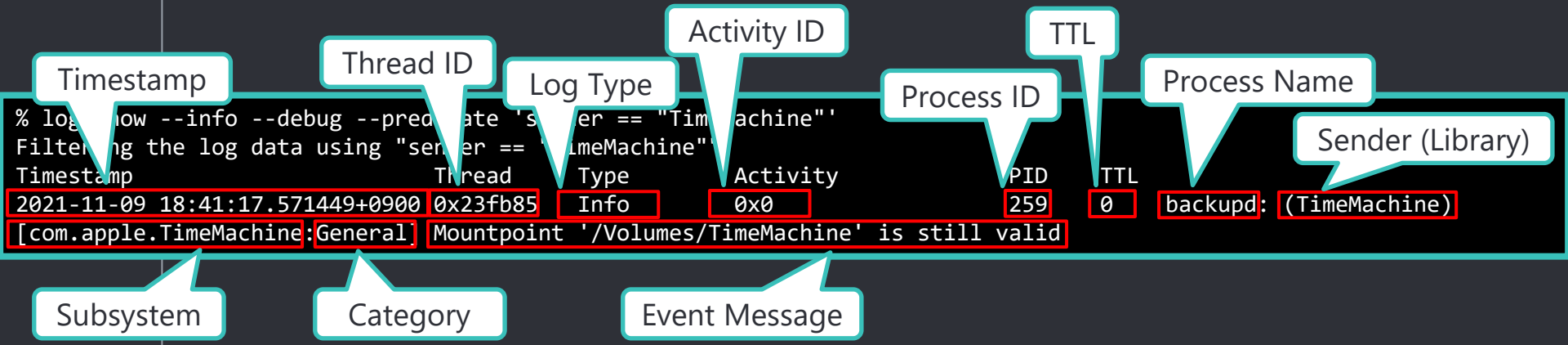
- UnifiedLogs.db is a goldmine (4/5)
  - log command

```
% log show --predicate 'FILTERING CONDITION' --start 'YYYY-MM-DD hh:mm:ss' --end 'YYYY-MM-DD hh:mm:ss'
```

  - Filtering Keywords

```
eventType           The type of event: activityCreateEvent, activityTransitionEvent, logEvent, signpostEvent, stateEvent,
timesyncEvent, traceEvent and userActionEvent.
eventMessage        The pattern within the message text, or activity name of a log/trace entry.
messageType         For logEvent and traceEvent, the type of the message itself: default, info, debug, error or fault.
process             The name of the process the originated the event.
processImagePath    The full path of the process that originated the event.
sender              The name of the library, framework, kernel extension, or mach-o image, that originated the event.
senderImagePath     The full path of the library, framework, kernel extension, or mach-o image, that originated the event.
subsystem           The subsystem used to log an event.  Only works with log messages generated with os_log(3) APIs.
category            The category used to log an event.  Only works with log messages generated with os_log(3) APIs.  When
category is used, the subsystem filter should also be provided.
```

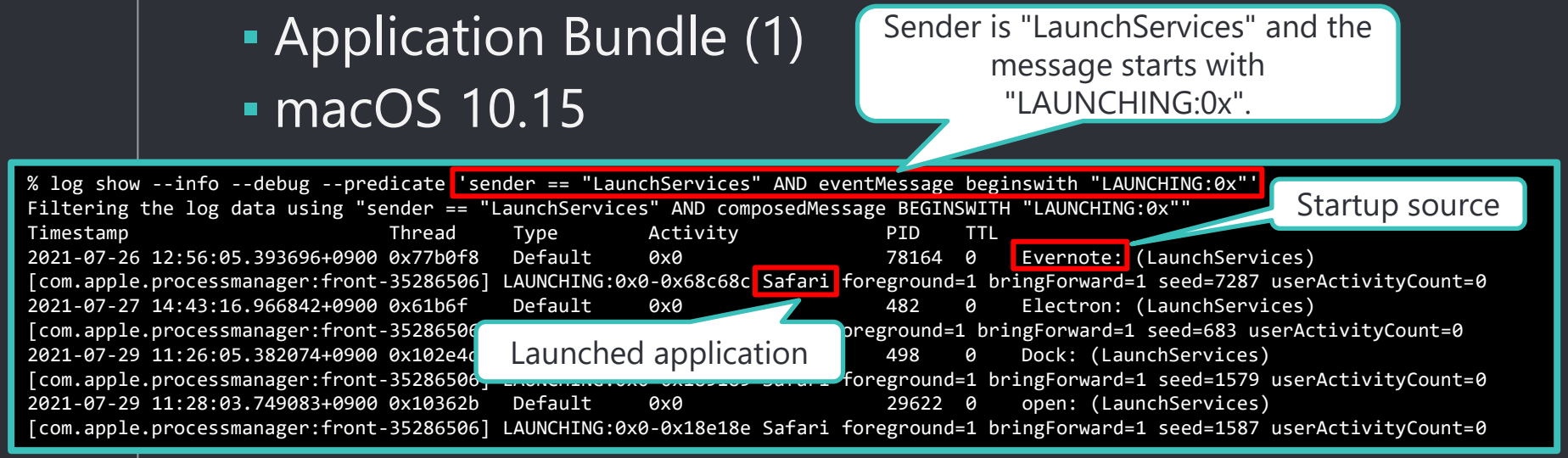
- UnifiedLogs.db is a goldmine (5/5)
  - Unified Logs format



    - In fact, it is displayed as a single line.

Investigating Unified Logs (1/13)

- Program execution history (1)
  - Application Bundle (1)
  - macOS 10.15

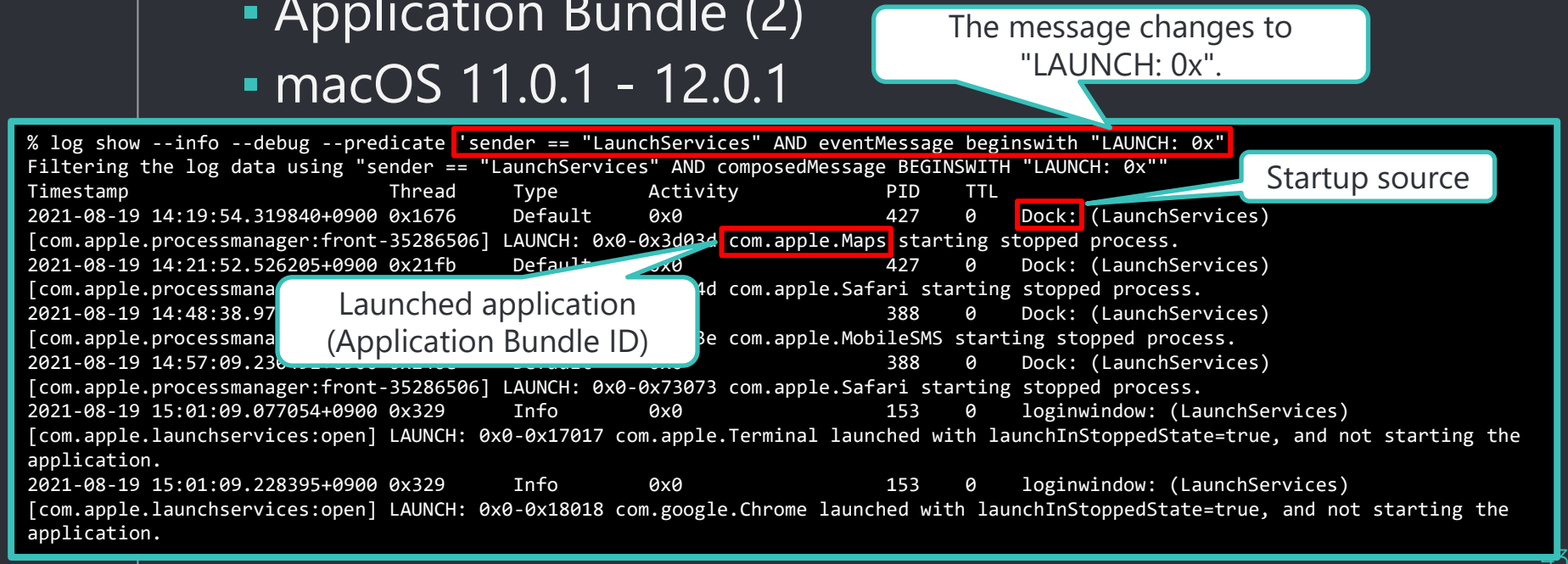


Investigating Unified Logs (2/13)

- Examples of startup source
  - Finder
  - Dock
  - Spotlight
  - loginwindow
    - Applications that were executed when the "Reopen windows when logging back in" checkbox was checked in the logout dialog box and the user logged in again.
    - The application specified in "Login Items" under "Users & Groups".
  - open
    - If you run the application with the open command

Investigating Unified Logs (3/13)

- Program Execution History (2)
  - Application Bundle (2)
  - macOS 11.0.1 - 12.0.1




```
% log show --info --debug --predicate 'sender == "LaunchServices" AND eventMessage beginswith "LAUNCH: 0x"
Filtering the log data using "sender == "LaunchServices" AND composedMessage BEGINSWITH "LAUNCH: 0x""
Timestamp                       Thread     Type        Activity            PID    TTL
2021-08-19 14:19:54.319840+0900 0x1676     Default     0x0                 427    0    Dock: (LaunchServices)
[com.apple.processmanager:front-35286506] LAUNCH: 0x0-0x3d03d com.apple.Maps starting stopped process.
2021-08-19 14:21:52.526205+0900 0x21fb     Default     0x0                 427    0    Dock: (LaunchServices)
[com.apple.processmana                                  4d com.apple.Safari starting stopped process.
2021-08-19 14:48:38.97                                  388    0    Dock: (LaunchServices)
[com.apple.processmana                                  e com.apple.MobileSMS starting stopped process.
2021-08-19 14:57:09.23                                  388    0    Dock: (LaunchServices)
[com.apple.processmanager:front-35286506] LAUNCH: 0x0-0x73073 com.apple.Safari starting stopped process.
2021-08-19 15:01:09.077054+0900 0x329      Info        0x0                 153    0    loginwindow: (LaunchServices)
[com.apple.launchservices:open] LAUNCH: 0x0-0x17017 com.apple.Terminal launched with launchInStoppedState=true, and not starting the
application.
2021-08-19 15:01:09.228395+0900 0x329      Info        0x0                 153    0    loginwindow: (LaunchServices)
[com.apple.launchservices:open] LAUNCH: 0x0-0x18018 com.google.Chrome launched with launchInStoppedState=true, and not starting the
application.
```

Investigating Unified Logs (4/13)

- Behavior in macOS 11 and later (1)
  - Applications executed with the open command will not be recorded.
  - Bugs in macOS 11.6 (?)
    - Logging does not occur unless the startup source is "loginwindow", "SystemUIServer", or "SoftwareUpdateNotificationManager".
    - macOS 11.6.1 and later are back to the same specifications as 11.5.2 before.
    - Release notes for macOS 11.6.x have not been released, so details are unknown.
      - https://developer.apple.com/documentation/macos-release-notes

Investigating Unified Logs (5/13)

- Behavior in macOS 11 and later (2)
  - When the startup source is "loginwindow".
    - Applications that are subject to "Reopen windows when logging back in" will be logged as "Type = Info" and will only be logged in memory.
      - The message contains "launchInStoppedState=true"
    - Applications specified in the "Login Items" section of "Users & Groups" are logged as "Type = Default" and will remain logged even after reboot.

```
% log show --info --debug --predicate 'sender == "LaunchServices" and eventMessage beginswith
Filtering the log data using "sender == "LaunchServices" AND composedMessage BEGINSWITH "LAUNC
Timestamp                       Thread     Type        Activity             PID    TTL
2022-01-14 08:21:21.918761+0900 0x21efb    Info        0x0                  4067   0    loginwindow: (LaunchServices) [com.apple.launchservices:open]
LAUNCH: 0x0-0x9ee9ee com.apple.Terminal launched with launchInStoppedState=true, and not starting the application.
```

Log of application executed with "Reopen windows when logging back in".

Investigating Unified Logs (6/13)

- Behavior in macOS 11 and later (3)
  - The first time you run an application downloaded from the Internet, Gakekeeper will be checked.
  - The log will be recorded with "Type = Info" (recorded in memory only).
  - The message contains "launchInQuarantine == true".

```
% log show --info --debug --predicate 'sender == "LaunchServices" and eventMessage beginswith "LAUNCH: 0x"' --start '2022-01-14 13:00:00'
Filtering the log data using "sender == "Laun                                    : 0x""
Timestamp                       Thread     Ty
2022-01-14 13:17:44.405335+0900 0x4786     De                                    aunchServices) [com.apple.processmanager:front-35286506]
LAUNCH: 0x0-0xd80d8 com.apple.Safari starting
2022-01-14 13:18:44.148002+0900 0x50ea     Info                                  1124   0    Dock: (LaunchServices) [com.apple.launchservices:open] LAUNCH:
0x0-0xeb0eb com.apple.DiskImageMounter launched with launchInQuarantine == true, so not starting the application.
2022-01-14 13:19:19.907199+0900 0x523c     Info         0x0                      1127   0    Finder: (LaunchServices) [com.apple.launchservices:open] LAUNCH:
0x0-0xf10f1 com.ridiculousfish.HexFiend launched with launchInQuarantine == true, so not starting the application.
2022-01-14 13:21:21.389996+0900 0x5472     Default      0x0                      1127   0    Finder: (LaunchServices) [com.apple.processmanager:front-
35286506] LAUNCH: 0x0-0x100100 com.ridiculousfish.HexFiend starting stopped process.
```

Run the downloaded application (the first time).

Run the downloaded application (the second time).

Investigating Unified Logs (7/13)

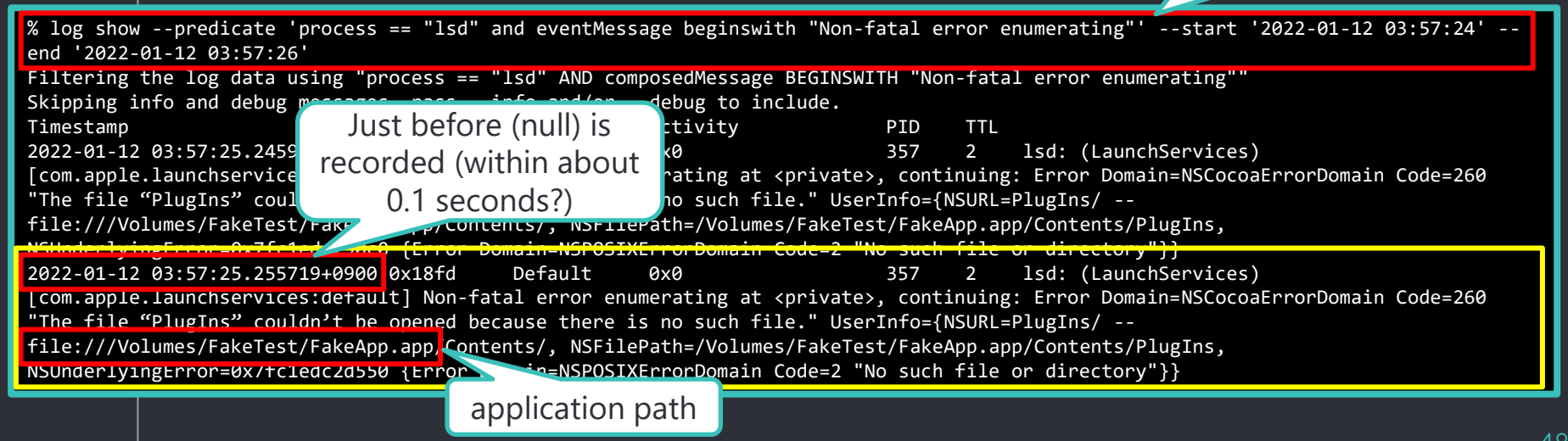
Program Execution History (3)

- If there is no application bundle ID (1)
  - The application bundle ID is recorded as "(null)".
  - macOS 11 or later

```
% log show --predicate 'eventMessage beginswith "LAUNCH: 0x"' --start '2022-01-12'
Filtering the log data using "composedMessage BEGINSWITH "LAUNCH: 0x""
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       Thread     Type        Activity             PID    TTL
2022-01-12 03:57:14.516187+0900 0x1693     Default     0x0                  358    0    Finder: (LaunchServices)
[com.apple.processmanager:front-35286506] LAUNCH: 0x0-0x4d04d com.apple.DiskImageMounter starting stopped process.
2022-01-12 03:57:25.281130+0900 0x1d25     Default     0x0                  358    0    Finder: (LaunchServices)
[com.apple.processmanager:front-35286506] LAUNCH: 0x0-0x50050 (null) starting stopped process.
```

Investigating Unified Logs (8/13)

- Program Execution History (4)
  - No application bundle (2)
    - Identify applications recorded as (null)



Investigating Unified Logs (9/13)

- Program Execution History (5)
  - Unsigned programs allowed to run by Gatekeeper
  - It also logs the mounting of unsigned DMGs.
  - Logged only on first run.
  - macOS 10.15 - 12.0.1

```
% log show --info --debug --predicate 'category == "gk" and eventMessage BEGINSWITH "temporarySigning"'
Filtering the log data using "category == "gk" AND composedMessage BEGINSWITH "temporarySigning""
Timestamp                       Thread     Type        Activity             PID    TTL
2021-08-10 16:41:11.730226+0900 0x1dc9     Default     0x0                  212    0    syspolicyd: (Security)
[com.apple.securityd:gk] temporarySigning type=3 matchFlags=0x0 path=/Users/macforensics/Downloads/FakeTest2-bash.dmg
2021-08-10 16:41:26.286794+0900 0x206c     Default     0x0                  212    0    syspolicyd: (Security)
[com.apple.securityd:gk] temporarySigning type=1 matchFlags=0x0 path=/Volumes/FakeTest2-bash/FakeApp.app/Contents/MacOS/FakeApp
```

Programs with execute permission or mounted DMGs

Investigating Unified Logs (10/13)

- Program Execution History (6)
  - adhoc signed program
  - macOS 10.15 - 12.0.1

```
% log show --predicate '(process == "kernel" and eventMessage beginswith "AMFI: " and eventMessage contains " adhoc ") or (process == "amfid" and eventMessage contains "signature")'
Filtering the log data using "(process == "kernel" AND composedMessage BEGINSWITH "AMFI: " AND composedMessage CONTAINS " adhoc ") OR (process == "amfid" AND composedMessage CONTAINS "signature")"
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       Thread     Type        Activity             P
2022-01-19 16:06:09.001258+0900 0x3753     Default     0x0                                egrity) AMFI:
'/Users/macforensics/Downloads/SysJoker/types-config.ts' is adhoc signed.
2022-01-19 16:06:09.002729+0900 0x1c8c     Default     0x0                  215    0    amfid:
/Users/macforensics/Downloads/SysJoker/types-config.ts signature not valid: -67050
```

The executed program has an adhoc signature.

The executed program has an invalid signature.

Investigating Unified Logs (11/13)

Program Execution History (7)

- Deny execution by security policy
- macOS 10.15

```
% log show --predicate 'eventMessage contains "Security policy would not allow process"'
Filtering the log data using "composedMessage CONTAINS "Security policy would not allow process""
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       Thread     Type        Activity            PID    TTL
2022-01-12 02:35:12.569186+0900 0xa980     Default     0x0                 0      0    kernel: (AppleSystemPolicy) Security policy
would not allow process: 822, /Users/macforensics/Downloads/floss
```

Message contains "Security policy would not allow process

Program refused to run

- macOS 11.0.1 - 12.0.1

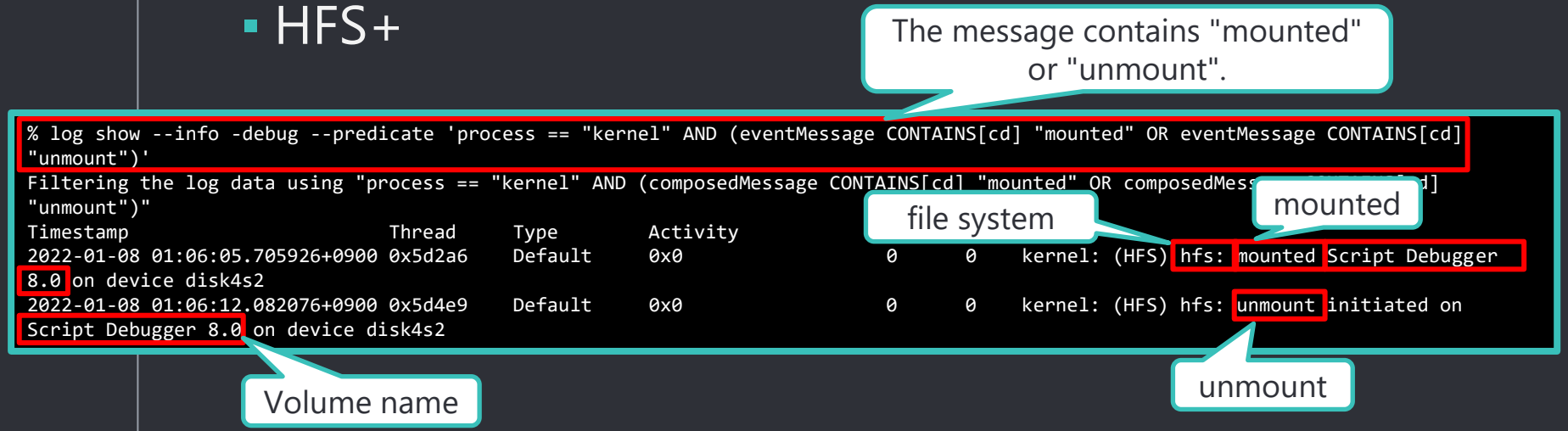
```
% log show --info --debug --predicate 'eventMessage contains "Security policy would not allow process"'
Filtering the log data using "composedMessage CONTAINS "Security policy would not allow process""
Timestamp                       Thread     Type        Activity            PID    TTL
2021-08-20 17:26:24.667681+0900 0x1b6ba    Default     0x0                 0      0    kernel: (AppleSystemPolicy) ASP: Security
policy would not allow process: 2954, /Users/macforensics/Downloads/floss
```

You can search using the same criteria as macOS 10.15, but the message formatting will be slightly different.

Added since macOS 11.

Investigating Unified Logs (12/13)

- Volume Mount (1)
  - macOS 10.15 - 12.0.1
  - HFS+



Investigating Unified Logs (13/13)

- Volume Mount (2)
  - macOS 10.15 - 12.0.1
  - APFS (same filtering conditions as HFS+)

```
% log show --info -debug --predicate 'process == "kernel" AND (eventMessage CONTAINS[cd] "mounted" OR eventMessage CONTAINS[cd]
"unmount")'
Filtering the log data using "process == "kernel" AND (composedMe                    composedMessage CONTAINS[cd]
"unmount")"
Timestamp                       Thread     Type        Activity
2022-01-08 01:04:48.911752+0900 0x5cfc7    Default     0x0                  0      0    kernel: (apfs) apfs_vfsop_unmount:2441:
disk1: unmounting volume  com.apple.TimeMachine.2022-01-08-000409.local
2022-01-08 01:04:48.911778+0900 0x5cfc7    Default     0x0                  0      0    kernel: (apfs) apfs_vfsop_unmount:2733:
snapshot deletion completed on the livefs
2022-01-08 01:04:48.911782+0900 0x5cfc7    Default     0x0                  0      0    kernel: (apfs) apfs_vfsop_unmount:2798:
                                900 0x5cfc7    D                        0      0    kernel: (apfs) apfs_vfsop_unmount:2807: all
done.           home.  (numMountedAPFSVolumes 44
2022-01-08  1:07:39.919784+0900 0x5d869    Default     0x0                  0      0    kernel: (apfs)  apfs_vfsop_mount:2234:
disk5s1:  mounted  volume:  FakeTest2-bash
2022-01-08 01:07:45.865955+0900 0x5d9f4    Default     0x0                  0      0    kernel: (apfs) apfs_vfsop_unmount:2441:
disk5:  unmounting  volume  FakeTest2-bash
```

Local snapshots can be ignored.

Mount or unmount

Volume name

file system

3 Implementation of ma2tl

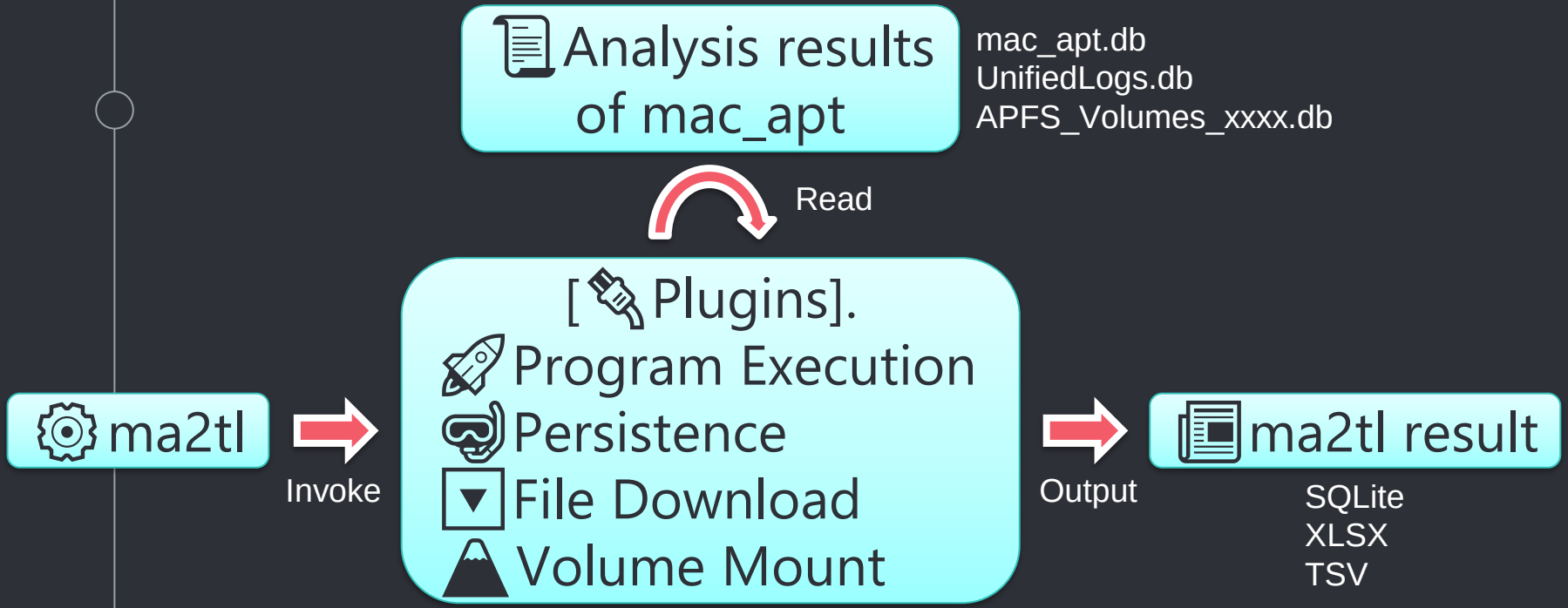
ma2tl implementation policy (1/2)

- mac_apt to timeline → ma2tl
- Support for macOS 10.15 or later
- Automate the verification procedure for each of the activities mentioned above.
  - If the analysis result has timestamps, create events from the main data.
    - mac_apt.db : SpotlightShortcuts
  - If the analysis result does not have timestamps, create events by associating it with a table of relevance.
    - mac_apt.db : AutoStart + APFS_Volumes_xxxx.db
    - mac_apt.db : Safari + Quarantine
  - Filtering UnifiedLogs.db to extract necessary information from messages

ma2tl implementation policy (2/2)

- Implement analysis plugins for each type of activity.
  - Activities may be recorded across multiple analysis results, and information needs to be integrated to be output as a timeline.
  - If you need a new activity, just add a new plugin
- Replace Unified Logs event messages with content whose meaning is easy to understand.
- Specify the timeline time range manually.
  - I don't want a super timeline, but a minimum timeline that can be used as a starting point for investigation.
  - Specify the range of dates and times that the forensic analysts are interested in.

Configuration of ma2tl



Plugin implementation example: File download

	TimeStamp	AgentName	DataUrl	OriginUrl	Other_Info
1	2022-01-13 02:48:41.884641	Safari	https://s3.amazonaws.com/latenightsw.com/ScriptDebugger8.0.3-8A49.dmg?	NULL	/Users/macforensics/Downloads/ScriptDebugger8.0.3-8A49.dmg

```
def extract_safari_quarantine_file_download(basic_info, filedownload_events):
    run_query = basic_info.mac_apt_dbs.run_query
    start_ts, end_ts = basic_info.get_between_dates_utc()
    sql = 'SELECT Quarantine.TimeStamp, Quarantine.AgentName, Quarantine.DataUrl, Quarantine.OriginUrl, Safari.Other_Info FROM Quarantine \
           INNER JOIN Safari ON Safari.Type = "DOWNLOAD" AND Quarantine.DataUrl = Safari.URL \
           WHERE Quarantine.TimeStamp BETWEEN "{}" AND "{}" AND \
           Quarantine.AgentName = "Safari" \
           ORDER BY TimeStamp;'.format(start_ts, end_ts)

    for row in run_query(MacAptDBType.MACAPT_DB, sql):
        skip_flag = False
        ts = row['TimeStamp']
        data_url = row['DataUrl']
        origin_url = row['OriginUrl']
        local_path = row['Other_Info']
        agent = row['AgentName']

        for event in filedownload_events:
            if event.data_url == data_url and event.local_path == local_path and get_timedelta(event.ts, ts) <= datetime.timedelta(seconds=1):
                skip_flag = True
                break

        if not skip_flag:
            filedownload_events.append(FileDownloadEvent(ts, data_url, origin_url, local_path, agent))

    return True
```

1) Configure the information required for the file download events from the Safari and Quarantine tables in mac_apt.db.

2) Extract the data.

3) Determine the duplication.

4) Add to timeline.

Plugin implementation example: Volume mount

	File	DecompFilePos	ContinuousTime	TimeUtc	Thread	Type	ActivityID	ParentActivityID	ProcessID	EffectiveUID	TTL	ProcessName
1	0000000000000005.tracev3	15461784	486064043460	2022-01-13 02:49:06.174674	9597	Default						
2	0000000000000005.tracev3	16047632	537063942698	2022-01-13 02:49:57.174574	10171	Default						

ProcessImagePath	Message
ontents/MacOS/HFS	/kernel	hfs: mounted Script Debugger 8.0.3 on device disk2s2...
ontents/MacOS/HFS	/kernel	hfs: unmount initiated on Script Debugger 8.0.3 on device disk2...

```
24  def extract_volume_mount_hfs_apfs(basic_info, timeline_events):
25      run_query = basic_info.mac_apt_dbs.run_query
26      start_ts, end_ts = basic_info.get_between_dates_utc()
27      sql = 'SELECT * FROM UnifiedLogs WHERE TimeUtc BETWEEN "{}" AND "{}" AND \
28          (ProcessName = "kernel" AND (Message like "%mounted%" OR Message like "%unmount%")) \
29          ORDER BY TimeUtc;'.format(start_ts, end_ts)
30
31      ignore_volumes = ('Preboot', 'Recovery', 'Boot OS X', 'macOS Base System', 'com.apple.TimeMachine.')
32
33      regex_dic = {
34          'mount_hfs': r'hfs: mounted (.+) on device (.+)',
35          'unmount_hfs': r'hfs: unmount initiated on (.+) on device (.+)',
36          'mount_apfs': r'apfs_vfsop_mount:\d+: mounted volume: (.+)',
37          'unmount_apfs': r'apfs_vfsop_unmount:\d+: .+: unmounting volume \'(.+)\'
38      }
39
40      for row in run_query(MacAptDBType.UNIFIED_LOGS, sql):
41          for reg_type, regex in regex_dic.items():
42              result = re.match(regex, row['Message'])
43              if result:
44                  volume = result.group(1)
```

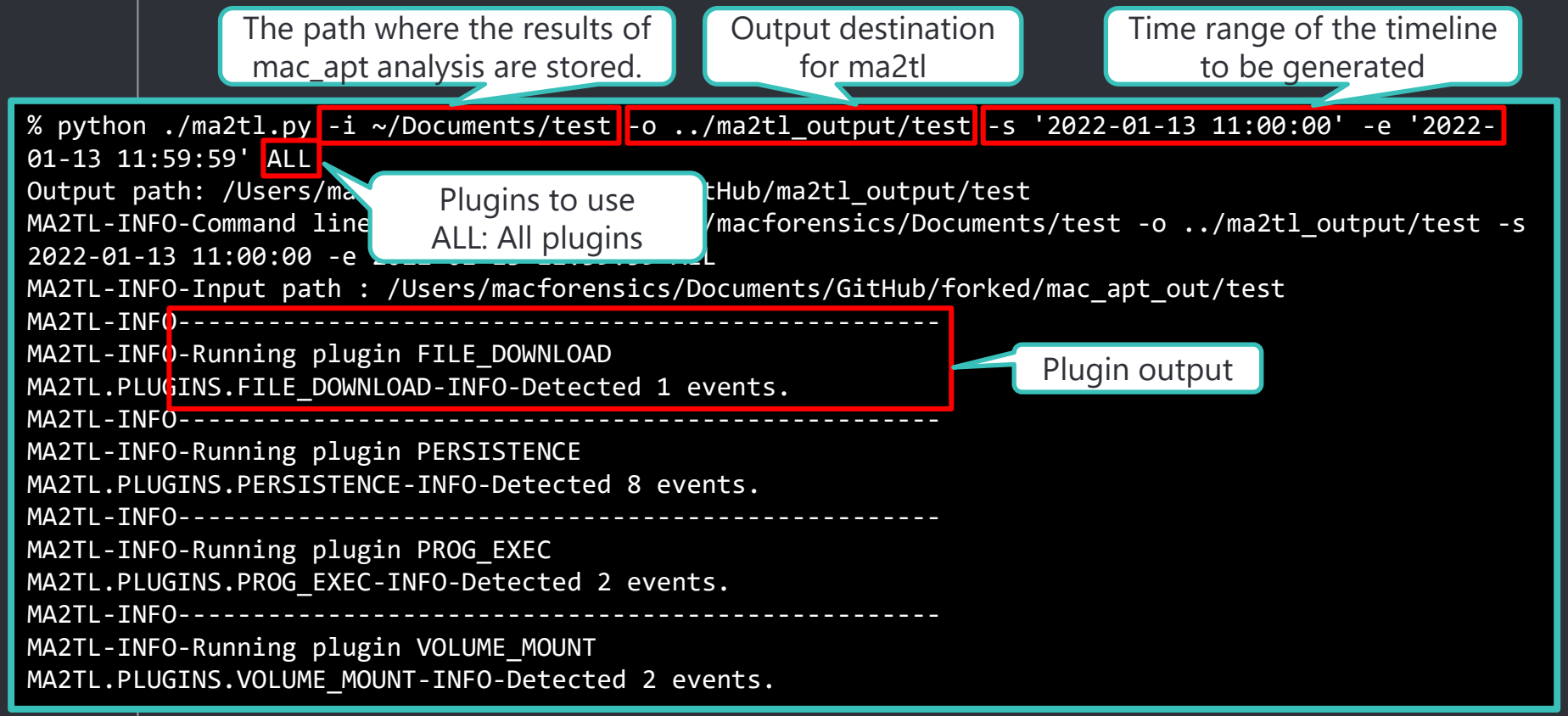
1) Filter the logs of volume mounts.

Volume names to ignore

Regular expressions of the message when the volume is mounted

2) Extracting volume name from messages using regular expressions

Execution example



Example of analysis results

- Timeline of Script Debugger downloaded, installed, and run on macOS 11.5.2.

Timestamp (user-specified time zone)
Default: system local

Timestamp (UTC)

Activity Type

Activity Description

Plugin name

	Timestamp (UTC)	Timestamp (Asia/Tokyo)	ActivityType	Message	PluginName
1	2020-01-01 08:00:00.000000	2020-01-01 17:00:00.000000	Persistence App Creation	/System/Applications/System Preferences.app	PERSISTENCE
2	2020-01-01 08:00:00.000000		ce App Creation	/System/Library/CoreServices/Finder.app	PERSISTENCE
3	2020-01-01 08:00:00.000000		ce App Creation	/Applications/Safari.app	PERSISTENCE
4			sistence App Creation	/System/Applications/Utilities/ Terminal.app	PERSISTENCE
5			Program Execution	com.apple.Safari (Launched from /System/Library/CoreServices/Dock.app/Contents/MacOS/Dock)	PROG_EXEC
6			File Download	/Users/macforensics/Downloads/ScriptDebugger8.0.3-8A49.dmg (From https://s3.amazonaws.com/latenightsw.com/ScriptDebugger8.0.3-8A49.dmg? ,Agent: Safari)	FILE_DOWNLOAD
7			Volume Mount	Script Debugger 8.0.3 (hfs)	VOLUME_MOUNT
8			Volume Unmount	Script Debugger 8.0.3 (hfs)	VOLUME_MOUNT
9	2022-01-13 02:50:18.099821	2022-01-13 11:50:18.099821	Program Execution	com.apple.systempreferences (Launched from /Applications/Script Debugger.app/Contents/MacOS/Script Debugger)	PROG_EXEC
10			File Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /System/Applications/System Preferences.app)	PERSISTENCE
11			Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /System/Library/CoreServices/Finder.app)	PERSISTENCE
12			ile Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /Applications/Safari.app)	PERSISTENCE
13			ile Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /System/Applications/Utilities/ Terminal.app)	PERSISTENCE

Launch Safari

Download a DMG

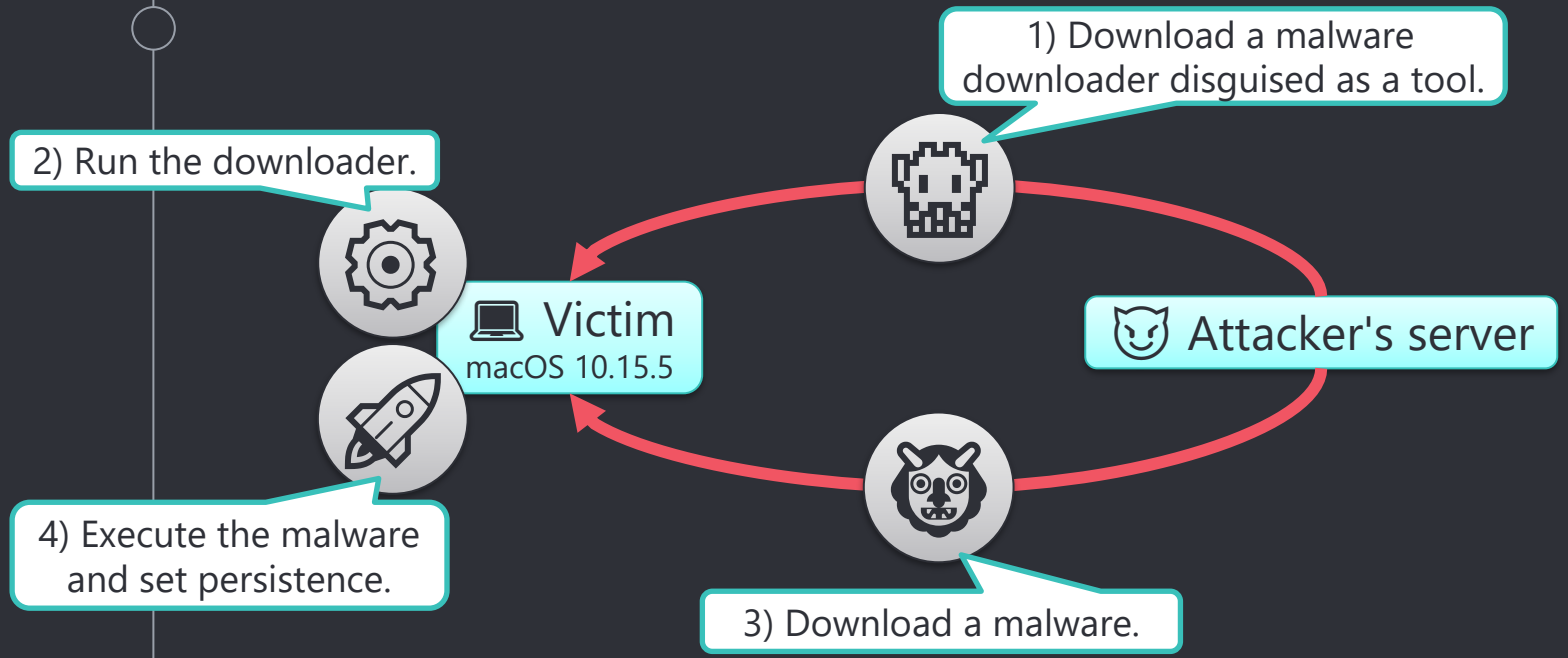
Volume mount

Launch System Preferences from Script Debugger

Since it is macOS 11, the Script Debugger first-time startup artifacts are not left behind.

ma2tl demo

ma2tl demo scenario



ma2tl demo timeline

3) The malware was downloaded using curl, so it is not included in the timeline generated by ma2tl.

	Timestamp (UTC)	Timestamp (Asia/Tokyo)	ActivityType	Message	PlugInName
	フィルター	フィルター	フィルター	フィルター	フィルター
1	2019-09-28 03:14:32.000000	2019-09-28 12:14:32.000000	Persistence App Creation	/Applications/Safari.app	PERSISTENCE
2	2022-01-19 04:12:06.451319	2022-01-19 13:12:06.451319	Program Execution	Safari (Launched from /System/Library/CoreServices/Dock.app/Contents/MacOS/Dock)	PROG_EXEC
3	2022-01-19 04:12:06.473788	2022-01-19 13:12:06.473788	Program Execution	Safari,PID=489	PROG_EXEC
4	2022-01-1	2022-01-19 13:15:37.694711	File Download	/Users/macforensics/Downloads/SysJoker Installer.dmg (From http://www.evil.test/download/SysJoker%20Installer.dmg ,Origin: N/A ,Agent: Safari)	FILE_DOWNLOAD
5	2022-01-19 04:15:48.786814	2022-01-19 13:15:48.786814	Program Execution	DiskImageMounter (Launched from /System/Library/CoreServices/Finder.app/Contents/MacOS/Finder)	PROG_EXEC
6	2022-01-19 04:15:48.799587	2022-01-19 13:15:48.799587	Program Execution	DiskImageMounter,PID=556	PROG_EXEC
7	2022-01-19 04:15:48.900227	2022-01-19 13:15:48.900227	Program Execution	/Users/macforensics/Downloads/SysJoker Installer.dmg	PROG_EXEC
8	2022-01-19 04:15:49.336667	2022-01-19 13:15:49.336667	Program Execution	DiskImages UI Agent,PID=561	PROG_EXEC
9	2022-01-1	2022-01-19 13:15:56.568206	Volume Mount	SysJoker Installer (apfs)	VOLUME_MOUNT
10	2022-01-19 04:16:07.742841	2022-01-19 13:16:07.742841	Program Execution	SJ_Installer (Launched from /System/Library/CoreServices/Finder.app/Contents/MacOS/Finder)	PROG_EXEC
11	2022-01-19 04:16:07.761348	2022-01-19 13:16:07.761348	Program Execution	bash,PID=575	PROG_EXEC
12	2022-01-19 04:16:08.011109	2022-01-19 13:16:08.011109	Program Execution	/Volumes/SysJoker Installer/SJ_Installer.app/Contents/MacOS/SJ_Installer	PROG_EXEC
13	2022-01-1	2022-01-19 13:16:08.069812	Program Execution	/Users/macforensics/.ts_setup/types-config.ts (adhoc signed.signature not valid.)	PROG_EXEC
14	2022-01-19 04:16:08.359620	2022-01-19 13:16:08.359620	Persistence File Creation	[Non-standard AppPath] /Users/macforensics/Library/LaunchAgents/com.apple.update.plist (AppPath: /Users/macforensics/Library/MacOsServices/updateMacOs)	PERSISTENCE
15	2022-01-19 04:16:08.366018	2022-01-19 13:16:08.366018	Persistence App Creation	[Non-standard AppPath] /Users/macforensics/Library/MacOsServices/updateMacOs	PERSISTENCE
16	2022-01-19 04:16:08.379932	2022-01-19 13:16:08.379932	Program Execution	/Users/m…sics/Library/MacOsServices/updateMacOs (adhoc signed.signature not valid.)	PROG_EXEC
17	2022-01-19 04:16:20.601321	2022-01-19 13:16:20.601321	Program Execution	…ched from /System/Library/CoreServices/Dock.app/Contents/MacOS/Dock)	PROG_EXEC
18	2022-01-19 04:16:20.612856				PROG_EXEC
19	2022-01-19 04:16:58.724747				VOLUME_MOUNT
20	2022-01-19 04:17:10.885914			…/Preferences/ByHost/com.apple.loginwindow.564DEC83-30EE-2106-4E98-889A4115F061.plist (AppPath: /Applications/Safari.app)	PERSISTENCE

1)

2)

4)

adhoc signed

The path of the autorun program is not a standard folder.

4 Future work

Future work

- Support for more mac_apt analysis results
  - Analysis results with timestamp
  - Analysis results showing timestamps in combination with APFS_Volumes_xxxx.db
- Ongoing investigation of Unified Logs
  - Application Execution
  - Program refused to be executed by the system
  - exFAT, NTFS, SMB volume mount
- Optimize the timeline to be generated
  - Eliminate duplicate events
  - Expand the scope of events to include cautionary messages.
- Maintenance
  - Will newer versions of macOS still record log messages that ma2tl can recognize?

5 Summary

Summary

- Shared how to create a timeline from mac_apt analysis results and Unified Logs.
- Introduced the implementation and function of ma2tl.
  - Automatic generation of timeline from mac_apt analysis results and Unified Logs
  - More activities can be supported by plugins.
- ma2tl GitHub repository
  - https://github.com/mnrkbys/ma2tl

Thank you for listening!

Any questions?

CREDITS for this presentation template and Icons

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival