ma2tl:
macOS Forensic Timeline Generator Using mac_apt Analysis Results

Japan Security Analyst Conference 2022

株式会社インターネットイニシアティブ
小林 稔

Who am I?

小林 稔

- 株式会社インターネットイニシアティブ セキュリティ本部 セキュリティ情報統括室
  技術調査、社内インシデントレスポンス
- 外部活動
  セキュリティキャンプ全国大会講師 2017-2019
  Japan Security Analyst Conference Speaker 2018/2020
  Black Hat USA 2018 Briefing Speaker
- Twitter: @unkn0wnbit

Table of Contents

0 はじめに

はじめに

- 今回の発表内容は全てIntel Macで行った調査や検証に基づいている
- M1 Macでは仕様が異なる点がある可能性がある
- しかし、多くの点において、M1 Macの調査にも流用できるのではないかと思われる

1 モチベーション

フォレンジックにおけるタイムラインの必要性

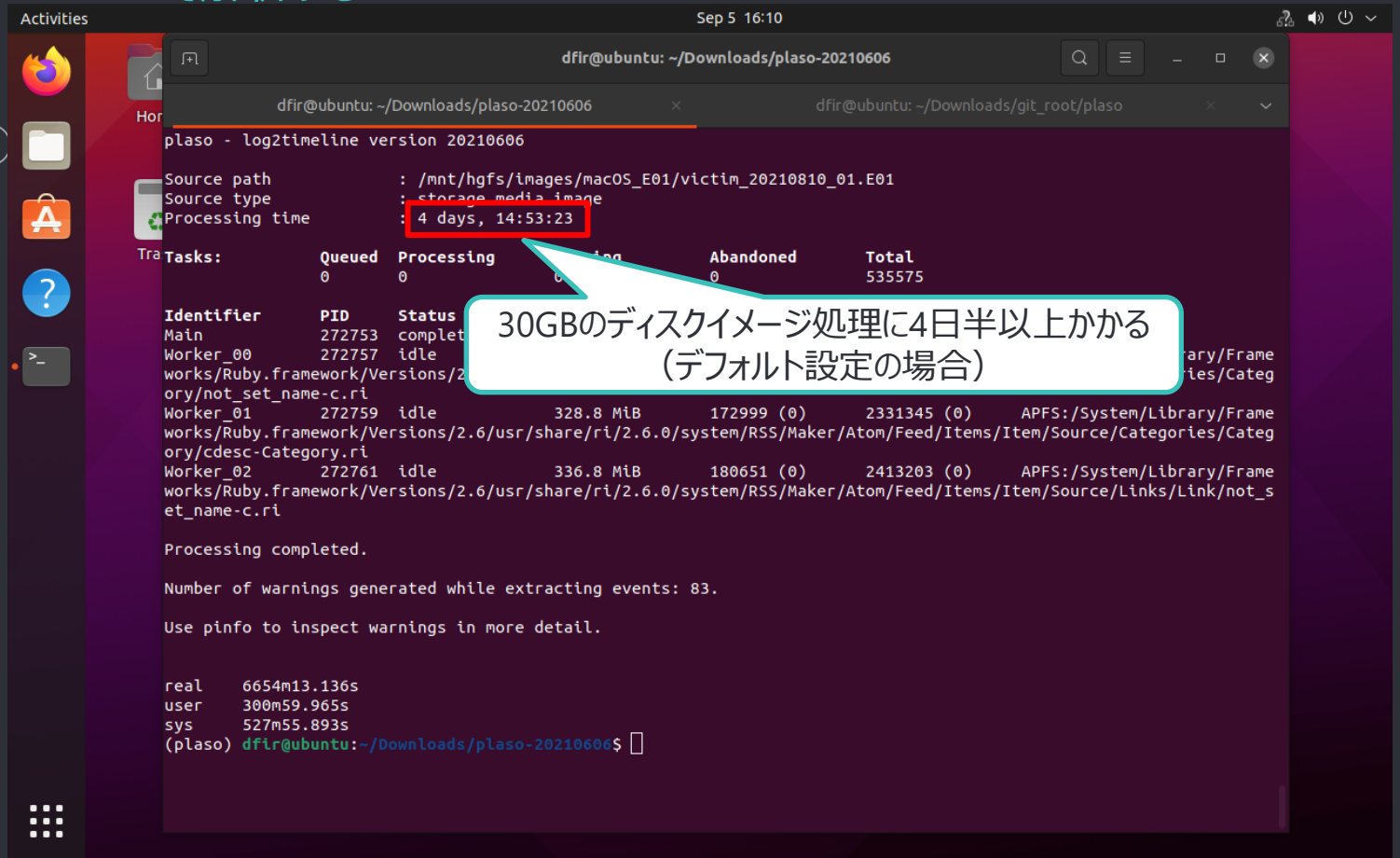
- アーティファクト収集後にやること
  - OSやアプリケーションのアーティファクトをツールで解析し、その結果からタイムラインを作成する
- タイムライン作成の目的
  - 被害端末の状況（疑わしい点）を把握する
  - ユーザーやマルウェア、攻撃者の主だったアクティビティをタイムスタンプを基に整理する
    - プログラム実行、ファイルダウンロード、ボリュームマウント、パーシステンス設定など
  - タイムラインを作成することで、調査を行う上でのバイアスや思考の飛躍、調査対象の漏れを低減することができる

どのツールを選択するか？

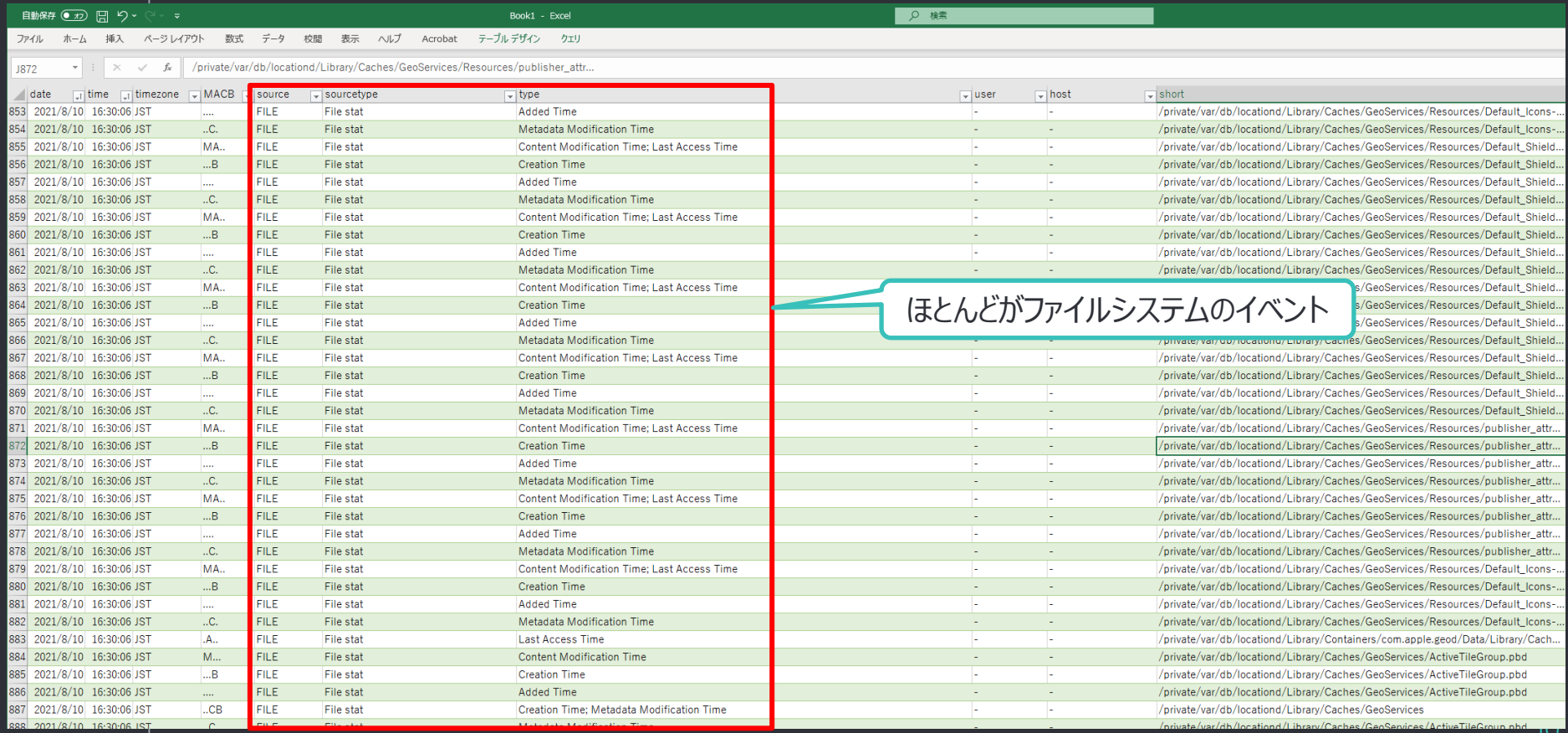
- Plaso
  - https://github.com/log2timeline/plaso
  - スーパータイムラインの自動生成
  - 様々なOSのアーティファクトを解析可能でmacOSにも対応
  - メンテナンスがアクティブ
- Plasoはスーパータイムラインを生成可能😆

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

Plasoで解析する


Activities
Sep 5 16:10
dfir@ubuntu: ~/Downloads/plaso-20210606
dfir@ubuntu: ~/Downloads/plaso-20210606
dfir@ubuntu: ~/Downloads/git_root/plaso
plaso - log2timeline version 20210606
Source path : /mnt/hgfs/images/macOS_E01/victim_20210810_01.E01
Source type : storage media image
Processing time : 4 days, 14:53:23
Tasks: Queued Processing Abandoned Total
0 0 0 535575
Identifier PID Status
Main 272753 complet
Worker_00 272757 idle
works/Ruby.framework/Versions/2
ory/not_set_name-c.ri
Worker_01 272759 idle 328.8 MiB 172999 (0) 2331345 (0) APFS:/System/Library/Frame
works/Ruby.framework/Versions/2.6/usr/share/ri/2.6.0/system/RSS/Maker/Atom/Feed/Items/Item/Source/Categories/Categ
ory/cdesc-Category.ri
Worker_02 272761 idle 336.8 MiB 180651 (0) 2413203 (0) APFS:/System/Library/Frame
works/Ruby.framework/Versions/2.6/usr/share/ri/2.6.0/system/RSS/Maker/Atom/Feed/Items/Item/Source/Links/Link/not_s
et_name-c.ri
Processing completed.
Number of warnings generated while extracting events: 83.
Use pinfo to inspect warnings in more detail.
real 6654m13.136s
user 300m59.965s
sys 527m55.893s
(plaso) dfir@ubuntu:~/Downloads/plaso-20210606$
30GBのディスクイメージ処理に4日半以上かかる
（デフォルト設定の場合）

Plasoによるスーパータイムライン



	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

ほとんどがファイルシステムのイベント

Plasoが生成するスーパータイムラインの問題点

- デフォルトでファイルシステムの全てのメタデータが解析される
  - 調査上、重要でないファイル数の方が圧倒的に多い
  - 1つのファイルメタデータが4つのイベント(MACB)に分割される
- システムログは行単位でイベントとして記録される
  - 単なる行単位のイベントではなく、何が起こったのか意味のある情報が欲しい（単なるログメッセージは必要ない）
  - Unified Logsは解析対象外
- 結果として、スーパータイムラインのほとんどはファイルシステムとシステムログのイベントで埋まってしまう
- そもそも、解析完了まで時間がかかりすぎる
- フォレンジック解析者が最初に確認したい情報は、このような情報ではない

フォレンジック解析者が欲しい情報と調査方針

- マルウェア感染調査の場合
  - パーシステンスの設定状況
  - プログラムの実行履歴
  - ボリューム（USBメモリやディスクイメージ）マウント
  - ファイルダウンロード
- このような情報を最も基本的なタイムラインとする
- 必要に応じて調査の範囲を広げたり、より深く調査を行って、タイムラインを肉付けする

- 調査のたたき台となるタイムラインが欲しい
- アーティファクト解析にフォーカスしたツールの解析結果から、必要なアクティビティだけでタイムラインを作成する方が要望に合致する

アーティファクト解析にフォーカスしたツール

- 候補となる解析ツールは2つ
  - AutoMacTC
    - https://github.com/CrowdStrike/automactc
    - メンテナンスは停滞気味
  - mac_apt
    - https://github.com/ydkhatri/mac_apt
    - メンテナンスがアクティブ

どちらのツールを使うべきか？

- メンテナンス状況および機能から鑑みて、薦められるのは「mac_apt」
- なぜ、メンテナンスが重要なのか
  - macOSのアーティファクトはバージョンアップによって、ファイル名やパスが変わることが多い
  - メンテナンスが行われていない解析ツールを使うと、時間とともに解析できないアーティファクトが増えていく
- Unified Logsパーサーが実装されている
  - Unified Logsには有益な情報が多く記録されているが、OSSでパーサーが実装されているのはmac_aptのみ

ツール作成のモチベーション

- mac_aptの解析結果からたたき台となるタイムラインを作成するのが現状ではベスト
- mac_aptの解析結果からタイムラインを作成するには、様々なテーブルを参照する必要がある
  - 解析に使用したプラグインの数だけテーブルが作られる
  - Spotlightのテーブルはカラム数が多く煩雑
- Unified Logsには有益な情報が含まれているが、mac_aptでは解析されない（パースはされる）
  - OSのバージョンアップによってメッセージが変わることがある
  - 手動で多くのフィルタリングを行うのは煩雑
  - フィルタリングを行っても出力結果が大量になる場合があり、目視で漏れなく確認するのは困難な場合がある
- 自動的にフォレンジックタイムラインを生成するツールが欲しい！

類似ツール

- mac_aptの解析結果を整理して表示および確認するという観点では以下のようなツールも存在する
  - 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/
- 以下の点で異なる
  - mac_aptの解析結果をGUIで確認するのが主目的で、タイムラインを生成するツールではない
  - 現在はメンテナンスが行われていない

2

mac_aptの解析結果を用いたタイムライン作成方法

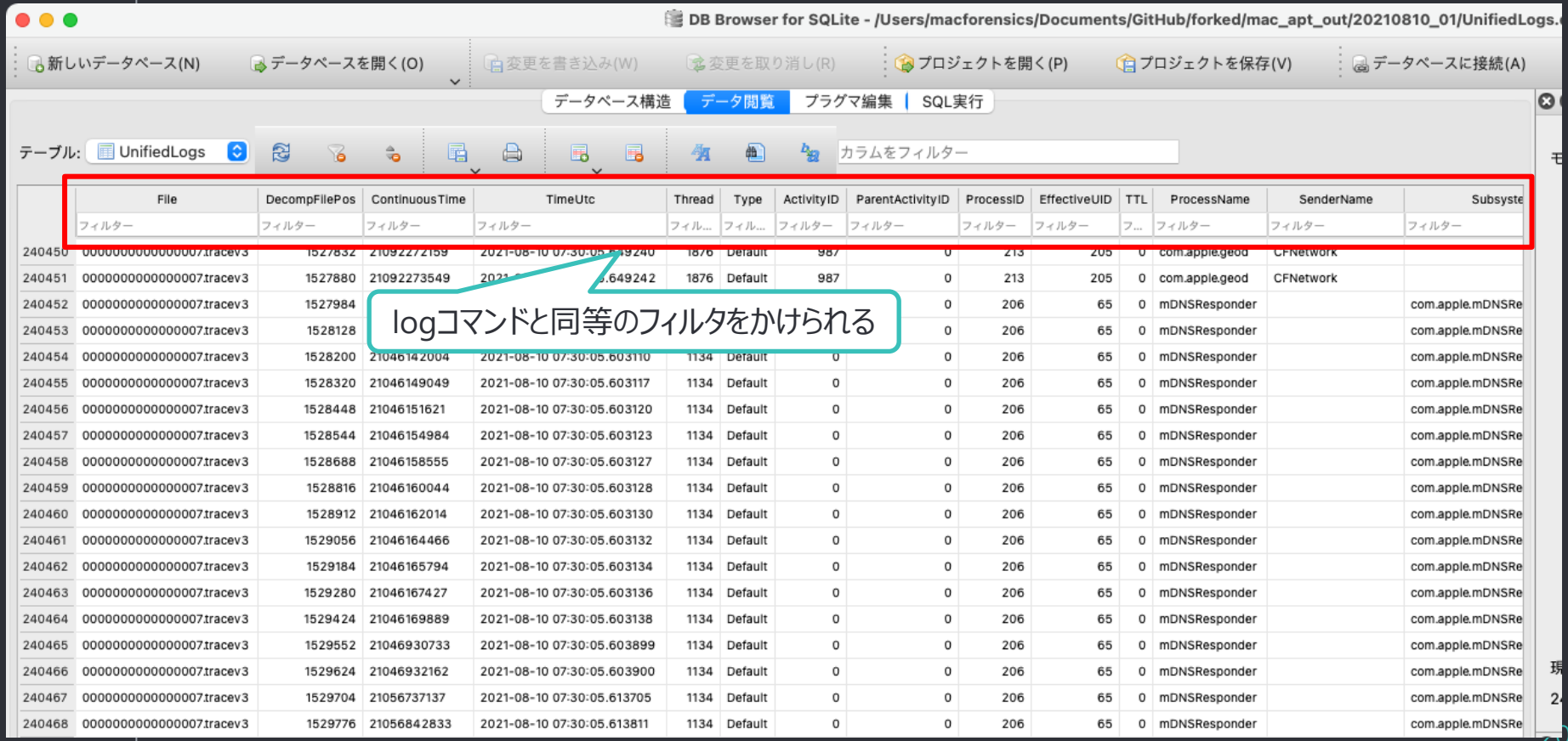
mac_aptの解析結果

- mac_aptが解析結果を保存するDB
  - mac_apt.db : アーティファクトの解析結果
  - UnifiedLogs.db : パースされたUnified Logs
  - APFS_Volumes_<GUID>.db : パースされたAPFSメタデータ
  - ExportおよびSPOTLIGHT_DATA : ディスクイメージからエクスポートされたアーティファクトファイルが保存されるフォルダ

mac_apt.db

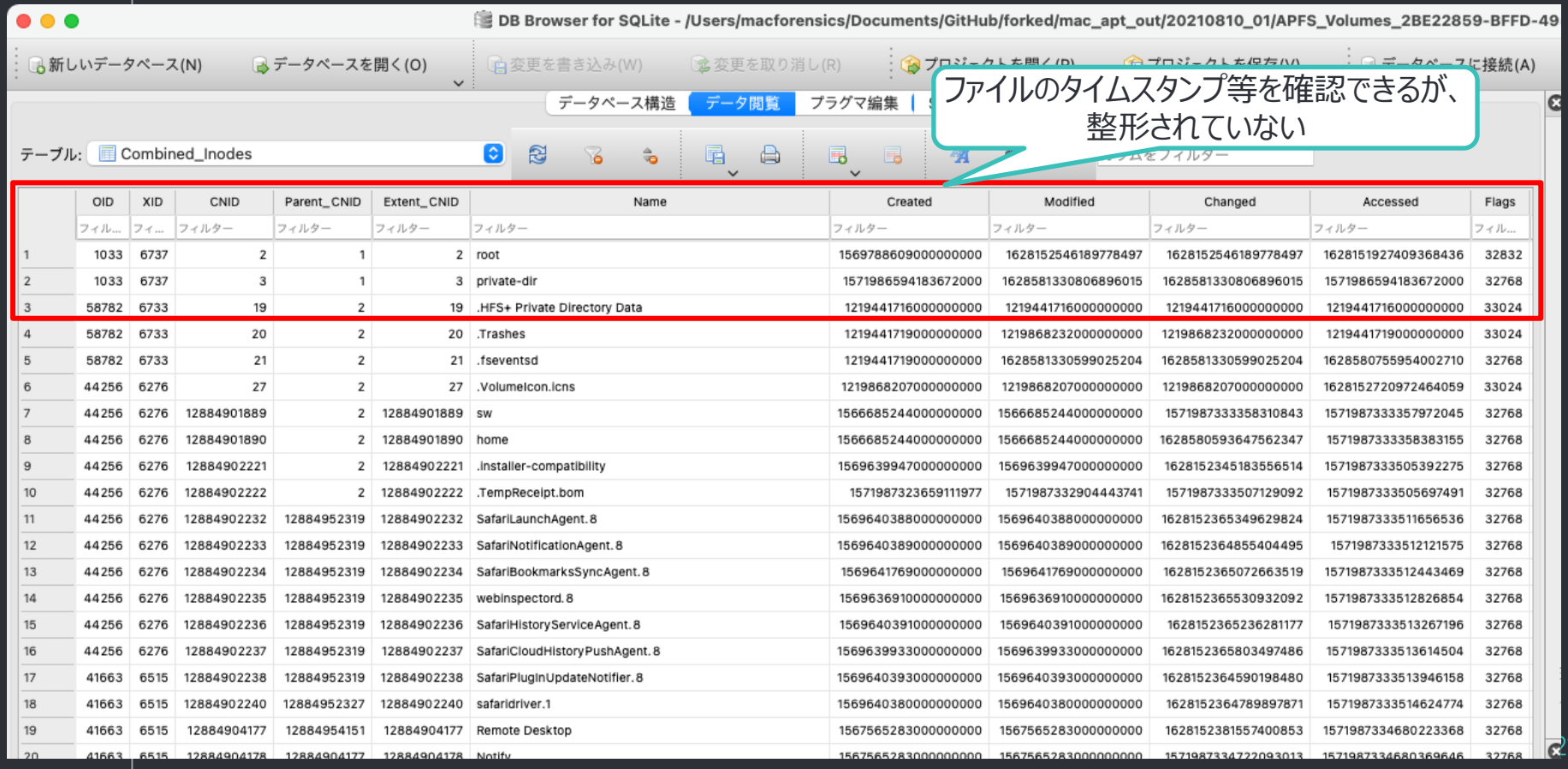

DB
新しいデータベース(N)
データベースを開く(O)
変更を書き込み(W)
データベース構造
Apps
AutoStart
Basic_Info
CFURL_Cache
Disk_Info
Dock Items
FileSharing
FsEvents
InstallHistory
InternetAccounts
NetUsage
Network_DHCP
Network_Details
Network_Interfaces
Notifications
Quarantine
RecentItems
Safari
SavedState
ScreenTime
Spotlight-1-.store-DIFF
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
Extensions
com.apple.preferences.extensions
解析に使われたプラグインの数だけ
テーブルが作られる

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 07:30:05.649240	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	21046142004	2021-08-10 07:30:05.603110	1134	Default	0	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

タイムラインの作成方針

- タイムスタンプを持つ解析結果を中心に調査を行う
  - タイムスタンプがない場合、他のテーブルやAPFS_Volumes_xxxx.dbを参照する
- 以下のアクティビティのタイムラインを作成する
  - パーシステンスの設定状況
  - プログラムの実行履歴
  - ボリューム（USBメモリやディスクイメージ）マウント
  - ファイルダウンロード

パーシステンスの調査 (1/3)

- mac_apt.db : AutoStart
  - 最初は一般ユーザーの設定を確認する
  - タイムスタンプは記録されていない

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/Utilities/LaunchAtLoginHelper.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

自動実行プログラム

自動実行設定ファイル

パーシステンスの調査 (2/3)

- 自動実行の設定ファイルと実行ファイルのタイムスタンプをAPFS_Volumes_xxxx.dbで確認する

```
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

ファイル作成日時

パーシステンスの調査 (3/3)

- 多くの自動実行プログラムは、右記のフォルダ以下に存在する
- macOS 10.15以降、システムボリュームとデータボリュームが分割された
  - システムボリュームはread-onlyでマウントされており、改ざんされる危険性は以前よりも低い
  - macOS 11以降はシステムボリュームに署名もされる
- したがって、システムボリューム上のプログラムは、最初は調査対象から外しても良いと考えられる

ma2tlのソースコードより抜粋

```
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  )
```

macOS 10.15以降、リードオンリーでマウントされるため、改ざんされる危険性は低い

システムボリューム

データボリューム

プログラム実行履歴の調査

- mac_apt.db : SpotlightShortcuts
  - Spotlight経由で実行したアプリケーションが記録される

Spotlightに入力した文字列

タイムスタンプ（最後に実行した日時のみ）

アプリケーション名

アプリケーションパス

	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

ボリュームマウントの調査

- mac_apt.db : RecentItems

テーブル: RecentItems

ボリューム名は分かるが、タイムスタンプはない

	Type	Name	URL		User
	VOLUME	フィルター	Volumes/	フィルター	フィルター
1	VOLUME	VMware Tools	Volumes/VMware Tools	uuid=DF9C7C0E-36B2-47FD-9296-1C8653FEBFEF	macforensics
2	VOLUME	macOS Catalina 10.15.5 Update	Volumes/macOS Catalina 10.15.5 Update	uuid=BF5BA9D5-DBC5-4764-8947-E9BF5A7CDC56	macforensics
3	VOLUME	FakeTest2-bash	Volumes/FakeTest2-bash	uuid=B21DB8A0-E82B-4F1D-B6BE-6ECDCA98274F	macforensics

- mac_apt.db : FsEvents

アーティファクトファイルの修正日時（マウントしたタイムスタンプではない）

テーブル: 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|Folder	Volumes/Preboot	12884928160	2019-10-25 07:19:53.550419	/.fseventsd/000000000000d9c1
3	00000000000				Volumes/Preboot	12884929020	2019-10-25 07:19:53.550419	/.fseventsd/000000000000d9c1
4	00000000000				Volumes/firmwaresyncd.myIPwx	12884930935	2019-10-25 07:21:03.584895	/.fseventsd/0000000000012ee9
5	00000000000				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

ボリュームマウントのフィルタリング条件（Volumes/以下にフォルダを作成）

ファイルダウンロードの調査 (1/5)

- mac_apt.db : Quarantine
  - Webブラウザ等でダウンロードしたファイルに付与されるcom.apple.quarantine拡張属性と同じ内容が保存されるDBの解析結果

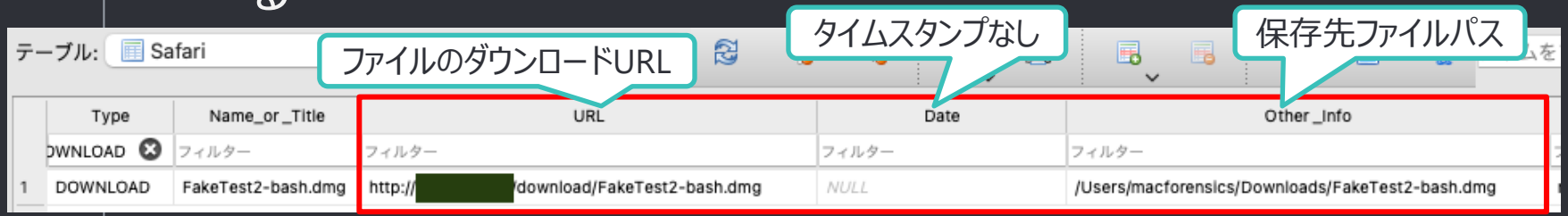
タイムスタンプ　アプリケーション名　ファイルのダウンロードURL　ダウンロード元URL

テーブル: Quarantine

	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...

ファイルダウンロードの調査 (2/5)

- mac_apt.db : Safari
  - ファイルの保存先が記録される
  - タイムスタンプがないため、Quarantineテーブルの DataUrlと紐づけて、タイムスタンプを推測する
  - Safariのダウンロード履歴はデフォルト1日で削除される



ファイルダウンロードの調査 (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	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

ファイルのダウンロードURL

ダウンロード開始日時

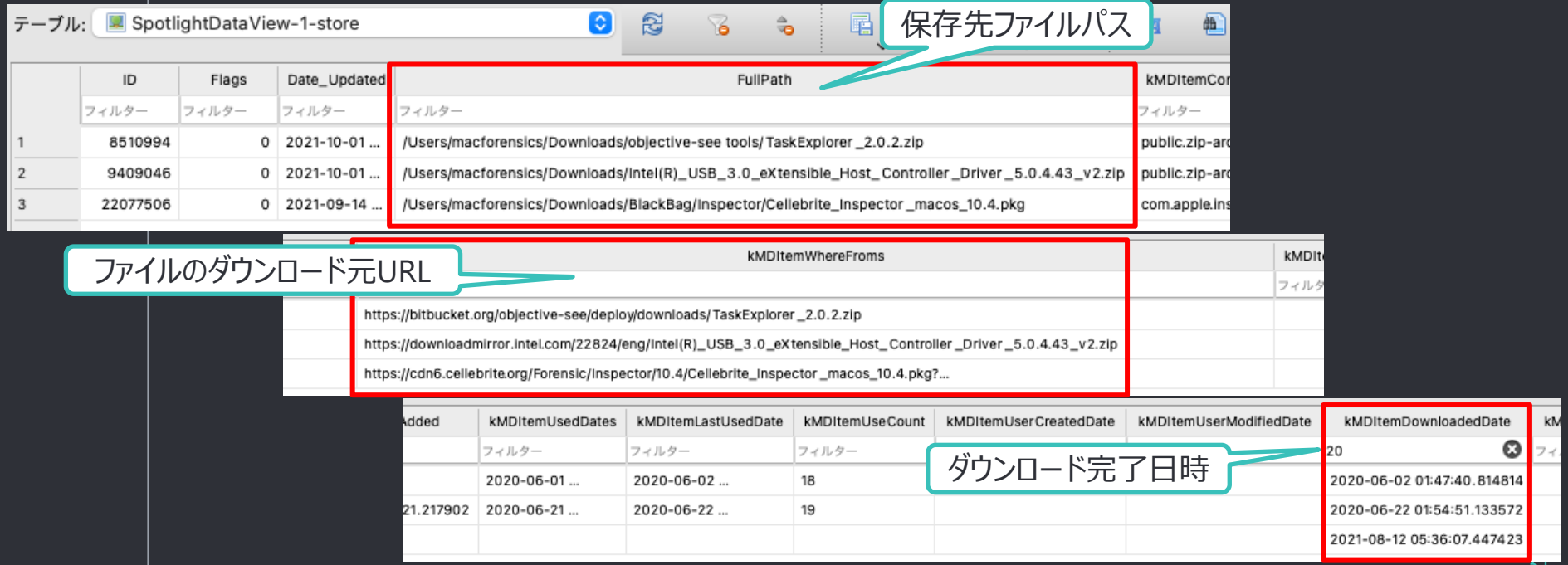
ダウンロード完了日時

保存先ファイルパス

ダウンロード元URL

ファイルダウンロードの調査 (4/5)

mac_apt.db : SpotlightDataView



ファイルダウンロードの調査 (5/5)

- macOS標準コマンドのcurlでファイルをダウンロードされるとアーティファクトが残らない
  - curlが実行されたこと自体の痕跡は残るが、アクセス先は分からない
- このような場合、マルウェア解析など他の調査も必要

mac_aptの解析結果から確認できた情報 (1/2)

- パーシステンスの設定状況
  - 自動実行の設定ファイルおよび自動実行されるプログラムは分かる
  - 上記のファイルのタイムスタンプも分かる
- プログラムの実行履歴
  - Spotlight経由で実行されたアプリケーションは分かる
  - 最後に実行された日時は分かる
  - 他にタイムスタンプを伴う実行履歴はない
- ボリュームマウント
  - マウントしたボリューム名は分かる
  - マウントした正確な日時は不明
- ファイルダウンロード
  - ダウンロード日時、ダウンロード元URL、保存先のファイルパスが分かる

情報が足りない

mac_aptの解析結果から確認できた情報 (2/2)

- mac_apt.dbの情報だけでは、タイムラインを作成するための情報が明らかに足りない
- 他に調査すべきデータは？

“UnifiedLogs.db”

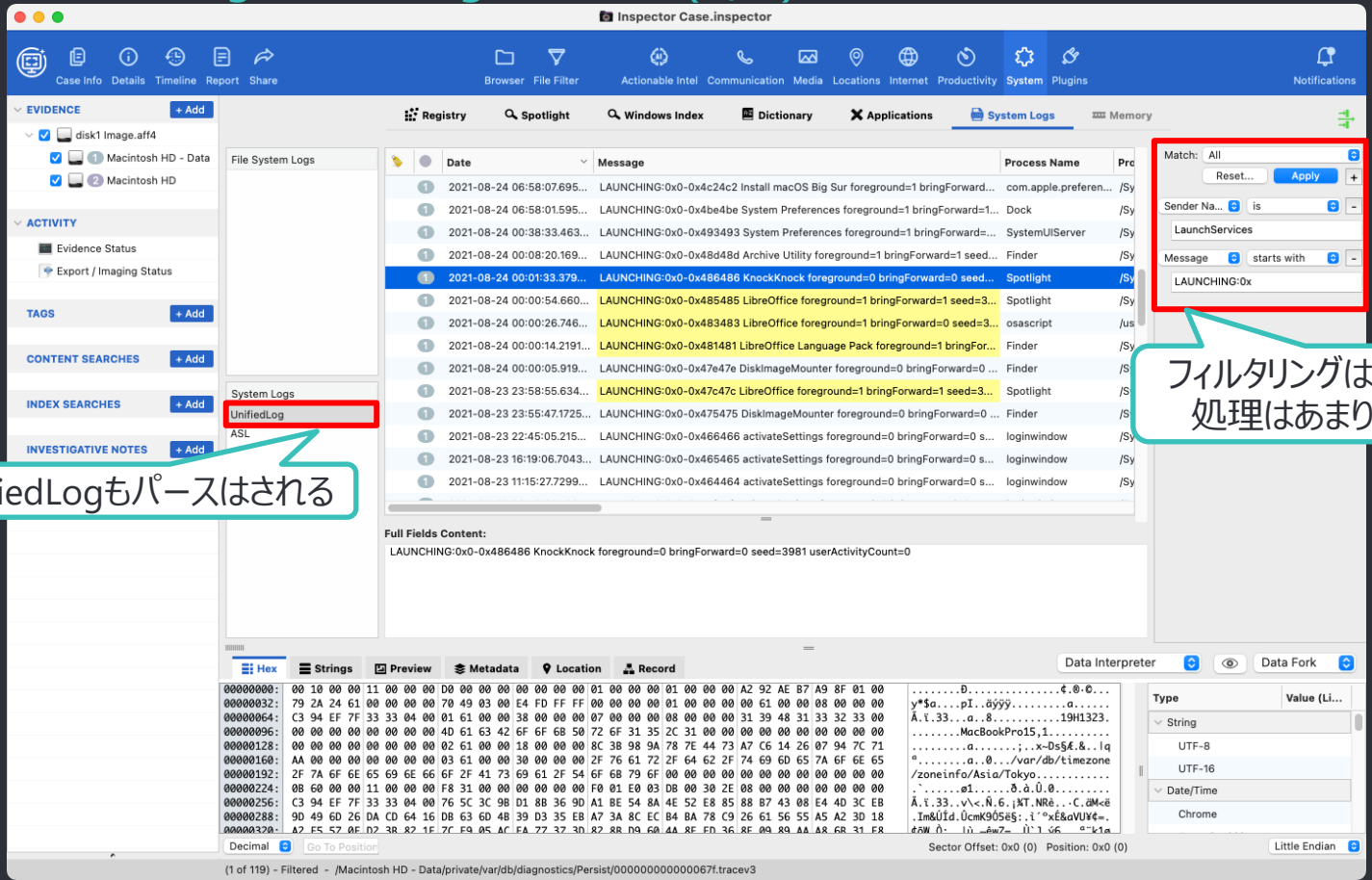
UnifiedLogs.db is a goldmine (1/5)

- Unified Logsには、他のアーティファクトに残らないプログラムの実行履歴やボリュームマウント履歴など、タイムライン作成に必要な情報が記録されている
- macOSフォレンジックにとって、まさに金鉱
- しかし、このような情報を解説する記事やブログは、何故かほぼ見かけない

UnifiedLogs.db is a goldmine (2/5)

- 商用製品であってもUnified Logsのパースは行うが、メッセージの内容に基づく解析は行わない
- データベースのロード時間やフィルタリング等の処理時間もUnifiedLogs.dbを処理するより遅い

UnifiedLogs.db is a goldmine (3/5)



UnifiedLogもパースはされる

フィルタリングはできるが、
処理はあまり速くない

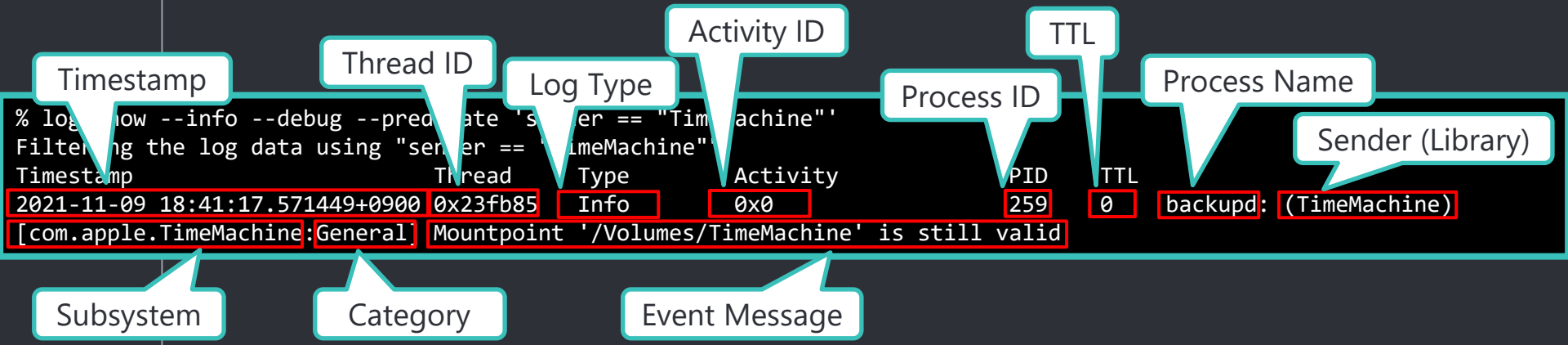
- UnifiedLogs.db is a goldmine (4/5)
  - logコマンド

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

  - フィルタリングキーワード

```
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フォーマット



    - 実際は1行

Unified Logsの調査 (1/13)

- プログラム実行履歴 (1)
  - アプリケーションバンドル (1)
  - macOS 10.15

Senderが「LaunchServices」かつ
メッセージが「LAUNCHING:0x」で始まる

起動元アプリケーション

起動されたアプリケーション

```
% log show --info --debug --predicate 'sender == "LaunchServices" AND eventMessage beginswith "LAUNCHING:0x"'
Filtering the log data using "sender == "LaunchServices" AND composedMessage BEGINSWITH "LAUNCHING:0x""
Timestamp                       Thread     Type        Activity             PID    TTL
2021-07-26 12:56:05.393696+0900 0x77b0f8   Default     0x0                  78164  0    Evernote: (LaunchServices)
[com.apple.processmanager:front-35286506] LAUNCHING:0x0-0x68c68c Safari foreground=1 bringForward=1 seed=7287 userActivityCount=0
2021-07-27 14:43:16.966842+0900 0x61b6f    Default     0x0                  482    0    Electron: (LaunchServices)
[com.apple.processmanager:front-35286506                                oreground=1 bringForward=1 seed=683 userActivityCount=0
2021-07-29 11:26:05.382074+0900 0x102e4c                                498    0    Dock: (LaunchServices)
[com.apple.processmanager:front-35286506                                foreground=1 bringForward=1 seed=1579 userActivityCount=0
2021-07-29 11:28:03.749083+0900 0x10362b   Default     0x0                  29622  0    open: (LaunchServices)
[com.apple.processmanager:front-35286506] LAUNCHING:0x0-0x18e18e Safari foreground=1 bringForward=1 seed=1587 userActivityCount=0
```

Unified Logsの調査 (2/13)

- 起動元アプリケーション例
  - Finder
  - Dock
  - Spotlight
  - loginwindow
    - ログアウト時のダイアログで「再ログイン時にウィンドウを再度開く」をチェックし、再ログインした際に実行されたアプリケーション
    - 「ユーザとグループ」の「ログイン項目」で指定されたアプリケーション
  - open
    - openコマンドでアプリケーションを実行した場合

Unified Logsの調査 (3/13)

- プログラム実行履歴 (2)
  - アプリケーションバンドル (2)
  - macOS 11.0.1 – 12.0.1

メッセージが「LAUNCH: 0x」に変わる

起動元アプリケーション

起動されたアプリケーション
（アプリケーションバンドルID）

```
% 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                                  3e 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.
```

Unified Logsの調査 (4/13)

- macOS 11以降の挙動 (1)
  - openコマンドで実行されたアプリケーションは記録されない
  - macOS 11.6のバグ（？）
    - 起動元が「loginwindow」、「SystemUIServer」、「SoftwareUpdateNotificationManager」以外はログが記録されない
    - macOS 11.6.1以降は11.5.2までと同じ仕様に戻った
    - macOS 11.6.xのリリースノートは公開されていないため詳細は不明
      - https://developer.apple.com/documentation/macos-release-notes

Unified Logsの調査 (5/13)

- macOS 11以降の挙動 (2)
  - 起動元が「loginwindow」の場合
    - 「再ログイン時にウィンドウを再度開く」の対象になったアプリケーションは、記録されるログが「Type = Info」となり、メモリ上にのみ記録される
      - メッセージに「launchInStoppedState=true」が含まれる
    - 「ユーザとグループ」の「ログイン項目」で指定されたアプリケーションは、ログが「Type = Default」であるため、再起動後もログが残る

「再ログイン時にウィンドウを再度開く」で実行されたアプリケーションのログ

```
% log show --info --debug --predicate 'sender == "LaunchServices" and eventMess
Filtering the log data using "sender == "LaunchServices" AND composedMessage BE
Timestamp                       Thread     Type        Activity             PID    T
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.
```

Unified Logsの調査 (6/13)

- macOS 11以降の挙動 (3)
  - インターネットからダウンロードしたアプリケーションの初回実行時、Gakekeeperのチェックが行われる
  - その際のログは「Type = Info」で記録される（メモリ上にのみ記録される）
  - メッセージに「launchInQuarantine == true」が含まれる

```
% 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 == "LaunchServices" AND composedMessage BEGINSWITH "LAUNCH: 0x""
Timestamp                       Thread     Type        Activity             PID    TTL
2022-01-14 13:17:44.405335+0900 0x4786     De                                                [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 wit                .aunchInQuarantine == 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.
```

ダウンロードしたアプリケーションを実行（1回目）

ダウンロードしたアプリケーションを実行（2回目）

Unified Logsの調査 (7/13)

プログラム実行履歴 (3)

アプリケーションバンドルIDがない場合 (1)

- アプリケーションバンドルIDが「(null)」で記録される
- macOS 11以降

```
% 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.
```

Unified Logsの調査 (8/13)

- プログラム実行履歴 (4)
  - アプリケーションバンドルがない場合 (2
    - (null)で記録されたアプリケーションの特定

プロセス名「lsd」、メッセージ「Non-fatal error enumerating」、(null)が記録される直前の時刻でフィルタリング

```
% log show --predicate 'process == "lsd" and eventMessage beginswith "Non-fatal error enumerating"' --start '2022-01-12 03:57:24' --
end '2022-01-12 03:57:26'
Filtering the log data using "process == "lsd" AND composedMessage BEGINSWITH "Non-fatal error enumerating""
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       Thread     Type        Activity             PID    TTL
2022-01-12 03:57:25.2459                   0x0                              357    2    lsd: (LaunchServices)
[com.apple.launchservice                   erating at <private>, continuing: Error Domain=NSCocoaErrorDomain Code=260
"The file “PlugIns” coul                   no such file." UserInfo={NSURL=PlugIns/ --
file:///Volumes/FakeTest/Fak               pp/Contents/, NSFilePath=/Volumes/FakeTest/FakeApp.app/Contents/PlugIns,
NSUnderlyingError=0x7fc1edc2d550 {Error Domain=NSPOSIXErrorDomain Code=2 "No such file or directory"}}
2022-01-12 03:57:25.255719+0900 0x18fd     Default     0x0                  357    2    lsd: (LaunchServices)
[com.apple.launchservices:default] Non-fatal error enumerating at <private>, continuing: Error Domain=NSCocoaErrorDomain Code=260
"The file “PlugIns” couldn’t be opened because there is no such file." UserInfo={NSURL=PlugIns/ --
file:///Volumes/FakeTest/FakeApp.app/Contents/, NSFilePath=/Volumes/FakeTest/FakeApp.app/Contents/PlugIns,
NSUnderlyingError=0x7fc1edc2d550 {Error Domain=NSPOSIXErrorDomain Code=2 "No such file or directory"}}
```

(null)が記録される直前（0.1秒程度以内？）

アプリケーションパス

Unified Logsの調査 (9/13)

- プログラム実行履歴 (5)
  - Gatekeeperに実行許可された未署名プログラム
  - 未署名DMGのマウント時のログも残る
  - 初回実行時にのみログが残る
  - 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
```

実行許可されたプログラム
またはマウントしたDMG

Unified Logsの調査 (10/13)

- プログラム実行履歴 (6)
  - adhoc署名されたプログラム
  - 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             PID    TTL
2022-01-19 16:06:09.001258+0900 0x3753     Default     0x0                  0      0    kernel: (AppleMobileFileIntegrity) 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
```

実行されたプログラムと
adhoc署名である旨を示すログ

実行されたプログラムと
署名が無効である旨を示すログ

Unified Logsの調査 (11/13)

- プログラム実行履歴 (7)
  - セキュリティポリシーによる実行拒否
  - 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
```

メッセージに「Security policy would not allow process」が含まれる

実行が拒否されたプログラム

  - macOS 11.0.1 – 12.0.1

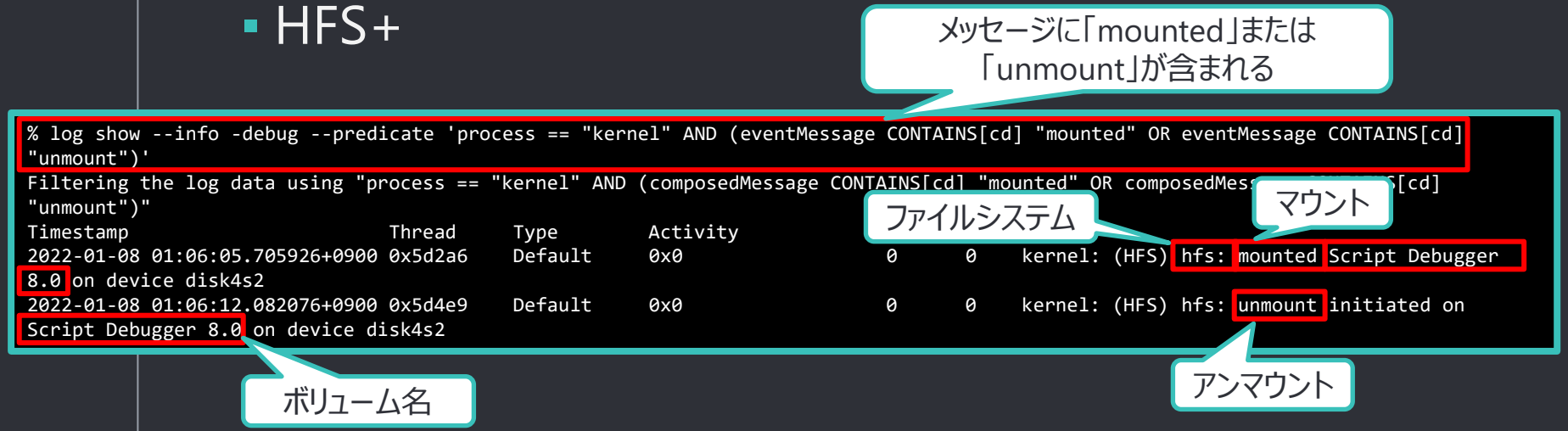
```
% log show --info --debug --predicate 'eventMessage contains "Security policy would not allow process"'
Filtering the log data using "composedMessage CONTAINS "Security policy would not allow process""
Timestamp                       Thread     Type        Activity             PID    TTL
2021-08-20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

macOS 10.15と同じ条件で検索できるが、メッセージのフォーマットが少し変わる

macOS 11以降追加された

Unified Logsの調査 (12/13)

- ボリュームマウント (1)
  - macOS 10.15 – 12.0.1
  - HFS+



Unified Logsの調査 (13/13)

- ボリュームマウント (2)
  - macOS 10.15 – 12.0.1
  - APFS（HFS+と同じフィルタリング条件）

```
% 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 01:07:39.919784+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
```

ローカルスナップショットは無視できる

マウント or アンマウント

ボリューム名

ファイルシステム

3 ma2tlの実装

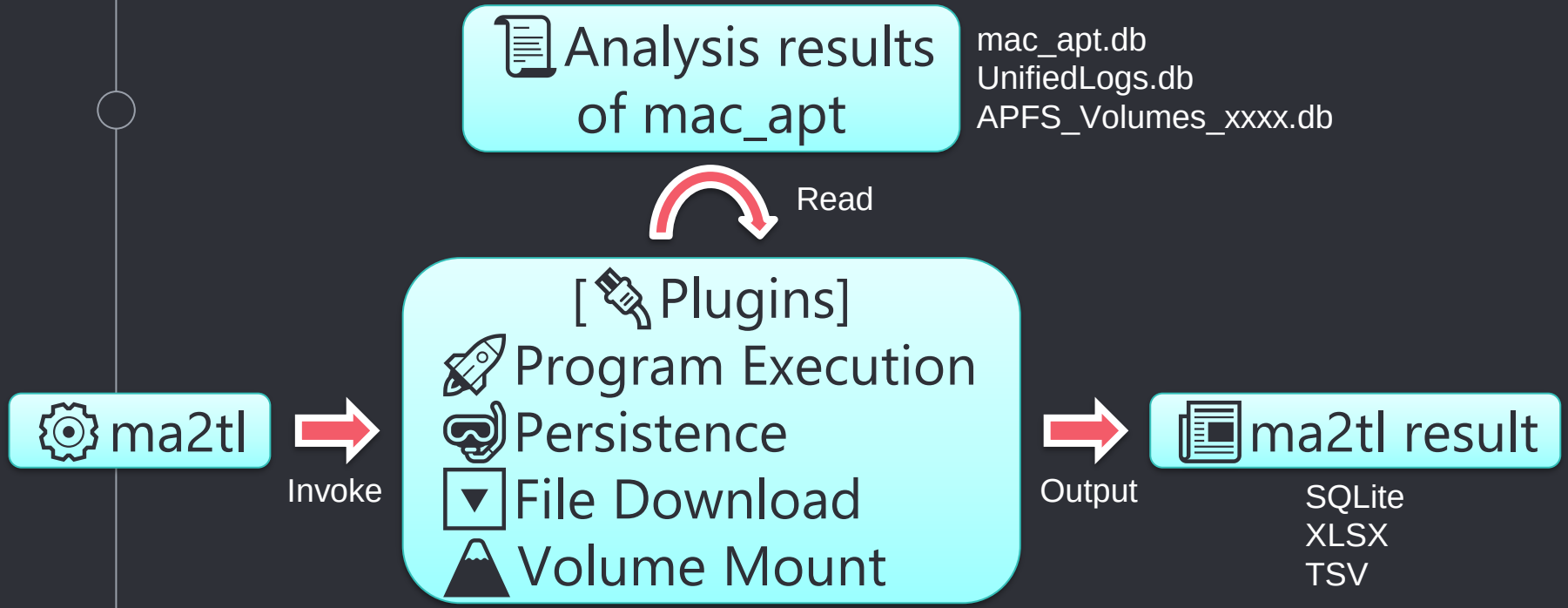
ma2tl実装方針 (1/2)

- mac_apt to timeline → ma2tl
- macOS 10.15以降をサポート
- 前出した各アクティビティの確認手順を自動化
  - タイムスタンプを持つ解析結果は主要なデータからイベントを作る
    - mac_apt.db : SpotlightShortcuts
  - タイムスタンプがない解析結果は関連するテーブルとイベントを作る
    - mac_apt.db : AutoStart + APFS_Volumes_xxxx.db
    - mac_apt.db : Safari + Quarantine
  - UnifiedLogs.dbにフィルタリングを行い、メッセージから必要な情報を抽出する

ma2tl実装方針 (2/2)

- アクティビティの種類毎に解析プラグインを実装
  - アクティビティの記録は複数の解析結果にまたがって記録されている場合があり、タイムラインとして出力するには情報の統合が必要
  - 新しいアクティビティが必要な場合、新しいプラグインを追加すればよい
- Unified Logsのイベントメッセージは、意味を理解しやすい内容に置き換える
- タイムラインのタイムレンジは手動で指定
  - スーパータイムラインではなく、調査のたたき台になる必要最低限のタイムラインが欲しい
  - フォレンジック解析者が気になる日時の範囲を指定する

ma2tlの構成


Analysis results of mac_apt
mac_apt.db
UnifiedLogs.db
APFS_Volumes_xxxx.db
Read
[Plugins]
Program Execution
Persistence
File Download
Volume Mount
ma2tl
Invoke
Output
ma2tl result
SQLite
XLSX
TSV

プラグイン実装例：ファイルダウンロード

	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
```

①mac_apt.dbのSafariテーブルとQuarantineテーブルから、ファイルダウンロードのイベントに必要な情報を構成する

②データを抽出

③重複判定

④タイムラインに追加

プラグイン実装例：ボリュームマウント

	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ボリュームマウントのログをフィルタリング

無視するボリューム名

ボリュームをマウントした際のメッセージの正規表現

②正規表現でメッセージからボリューム名を抽出する

- 実行例

mac_aptの解析結果が保存されているパス

ma2tlの出力先

生成するタイムラインのタイムレンジ

```
% python ./ma2tl.py -i ~/Documents/test -o ../ma2tl_output/test -s '2022-01-13 11:00:00' -e '2022-
01-13 11:59:59' ALL
Output path: /Users/ma                                    tHub/ma2tl_output/test
MA2TL-INFO-Command line                                   /macforensics/Documents/test -o ../ma2tl_output/test -s
2022-01-13 11:00:00 -e                                    L
MA2TL-INFO-Input path : /Users/macforensics/Documents/GitHub/forked/mac_apt_out/test
MA2TL-INFO--------------------------------------------------
MA2TL-INFO-Running plugin FILE_DOWNLOAD
MA2TL.PLUGINS.FILE_DOWNLOAD-INFO-Detected 1 events.
MA2TL-INFO--------------------------------------------------
MA2TL-INFO-Running plugin PERSISTENCE
MA2TL.PLUGINS.PERSISTENCE-INFO-Detected 8 events.
MA2TL-INFO--------------------------------------------------
MA2TL-INFO-Running plugin PROG_EXEC
MA2TL.PLUGINS.PROG_EXEC-INFO-Detected 2 events.
MA2TL-INFO--------------------------------------------------
MA2TL-INFO-Running plugin VOLUME_MOUNT
MA2TL.PLUGINS.VOLUME_MOUNT-INFO-Detected 2 events.
```

使用するプラグイン
ALL: すべてのプラグイン

プラグインの出力

解析結果の例

- macOS 11.5.2でSafariを使って、Script Debuggerをダウンロードおよびインストール後、実行した際のタイムライン

タイムスタンプ（ユーザー指定タイムゾーン）
デフォルト：システムローカル

タイムスタンプ(UTC)

アクティビティタイプ

アクティビティの説明

プラグイン名

	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	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		tence App Creation	/System/Library/CoreServices/Finder.app	PERSISTENCE
3	2020-01-01 08:00:00.000000		tence App Creation	/Applications/Safari.app	PERSISTENCE
4	2020-01-01 08:00:00.000000	2020-01-01 17:00:00.000000	Persistence App Creation	/System/Applications/Utilities/ Terminal.app	PERSISTENCE
5	20	13882	Program Execution	com.apple.Safari (Launched from /System/Library/CoreServices/Dock.app/Contents/MacOS/Dock)	PROG_EXEC
6	20	384641	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	20	74674	Volume Mount	Script Debugger 8.0.3 (hfs)	VOLUME_MOUNT
8	20		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			stence File Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /System/Library/CoreServices/Finder.app)	PERSISTENCE
12			rsistence File Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /Applications/Safari.app)	PERSISTENCE
13			rsistence File Creation	/Users/macforensics/Library/Preferences/ByHost/com.apple.loginwindow.564DA379-E347-051F-7B91-8B0A4CE11DA5.plist (AppPath: /System/Applications/Utilities/ Terminal.app)	PERSISTENCE

Safariを起動

DMGをダウンロード

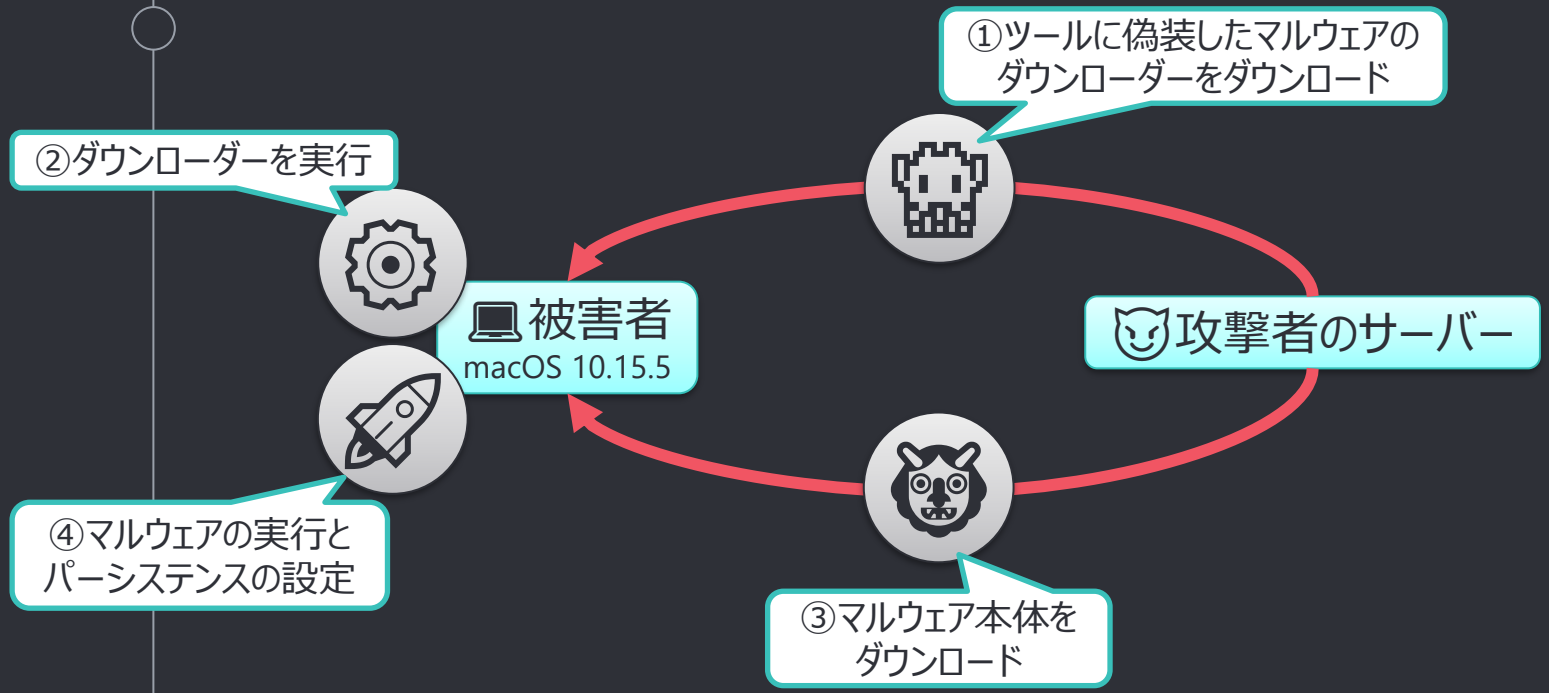
ボリュームマウント

Script Debuggerから
システム環境設定を起動

macOS 11なので初回の
Script Debuggerの起動は
残っていない

ma2tl demo

ma2tl demo scenario



ma2tl demo timeline

③マルウェア本体のダウンロードはcurlが使われたので、ma2tlが生成するタイムラインには含まれない

	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/macforensics/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	(Launched 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			fs)	VOLUME_MOUNT
20	2022-01-19 04:17:10.885914			Library/Preferences/ByHost/com.apple.loginwindow.564DEC83-30EE-2106-4E98-889A4115F061.plist (AppPath: /Applications/Safari.app)	PERSISTENCE

① ② ④

adhoc署名されている

自動実行されるプログラムのパスが標準的なフォルダではない

4 Future work

Future work

- より多くのmac_apt解析結果のサポート
  - タイムスタンプがある解析結果
  - APFS_Volumes_xxxx.dbと組み合わせてタイムスタンプがわかる解析結果
- 継続的なUnified Logsの調査
  - アプリケーション実行
  - システムに実行拒否されたプログラム
  - exFAT, NTFS, SMBボリュームマウント
- タイムラインの最適化
  - 重複イベントの排除
  - 注意を促すメッセージを入れるイベントの対象を拡大
- メンテナンス
  - 新しいバージョンのmacOSでもma2tlが認識できるログメッセージが記録されるか

5 まとめ

まとめ

- mac_aptの解析結果とUnified Logsからタイムラインを作成するハウハウを共有した
- ma2tlの実装と機能を紹介した
  - mac_aptの解析結果とUnified Logsからタイムラインを自動生成する
  - プラグインでサポートするアクティビティを増やせる
- 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