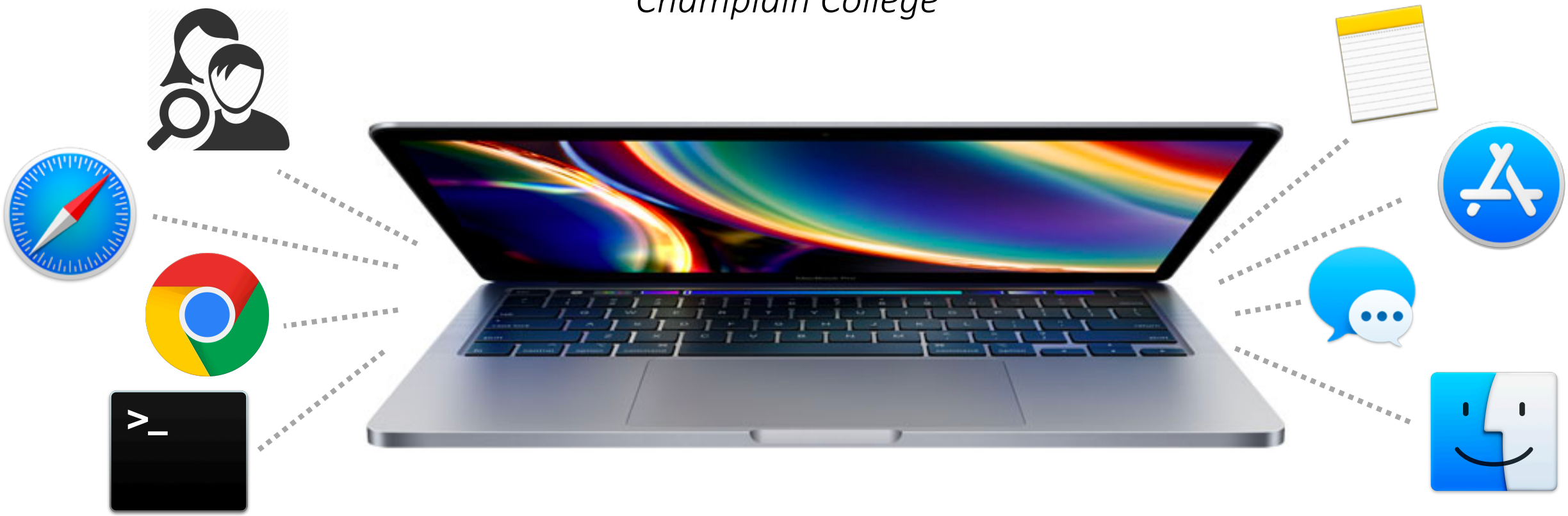
Quick Triage with mac_apt

Yogesh Khatri

Champlain College



About

- Yogesh Khatri
- Champlain College
  - Program Director – Digital Forensics
  - Associate Professor
- *15+ years doing Forensics & IR*
  - *Industry & Academia*
- Author & Maintainer for *mac_apt – Artifact Parsing Tool*

@swiftforensics

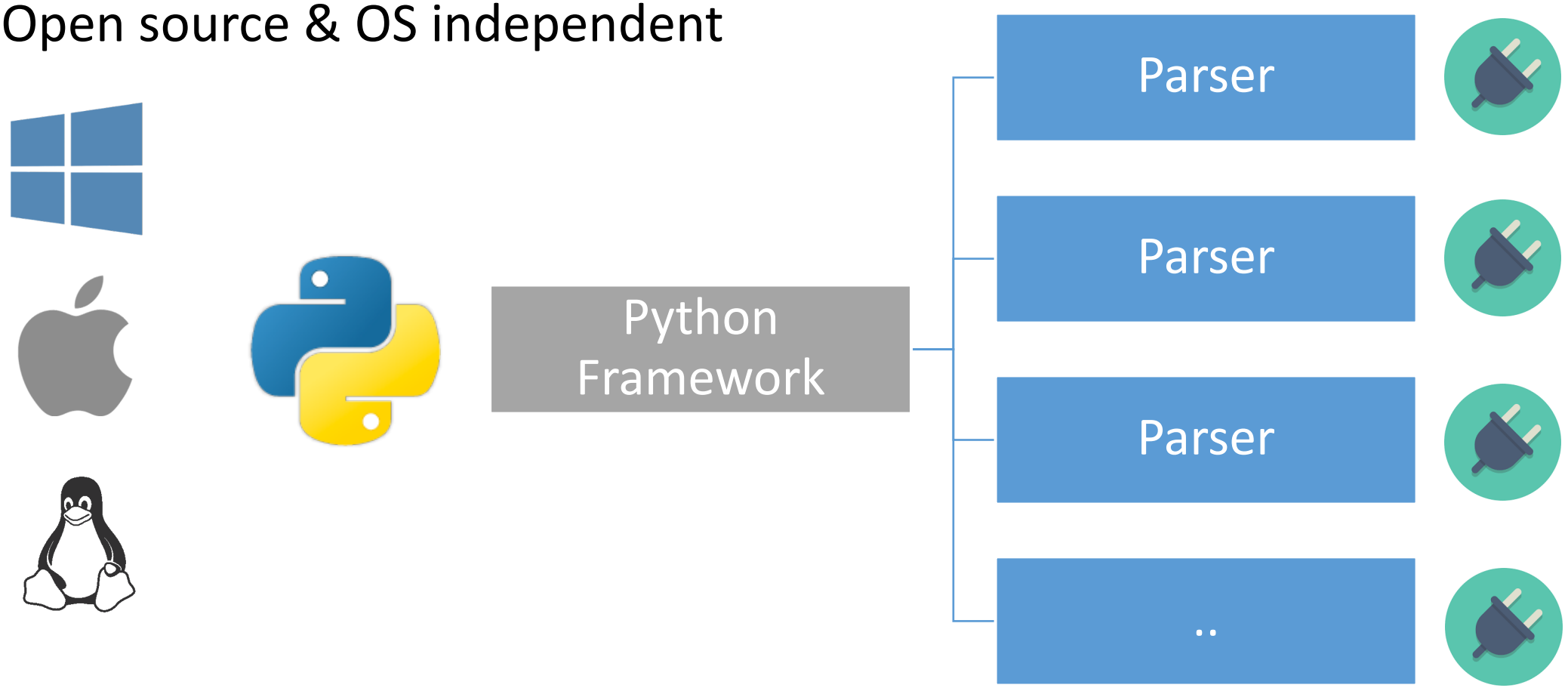
GitHub

https://github.com/ydkhatri

Swiftforensics.com

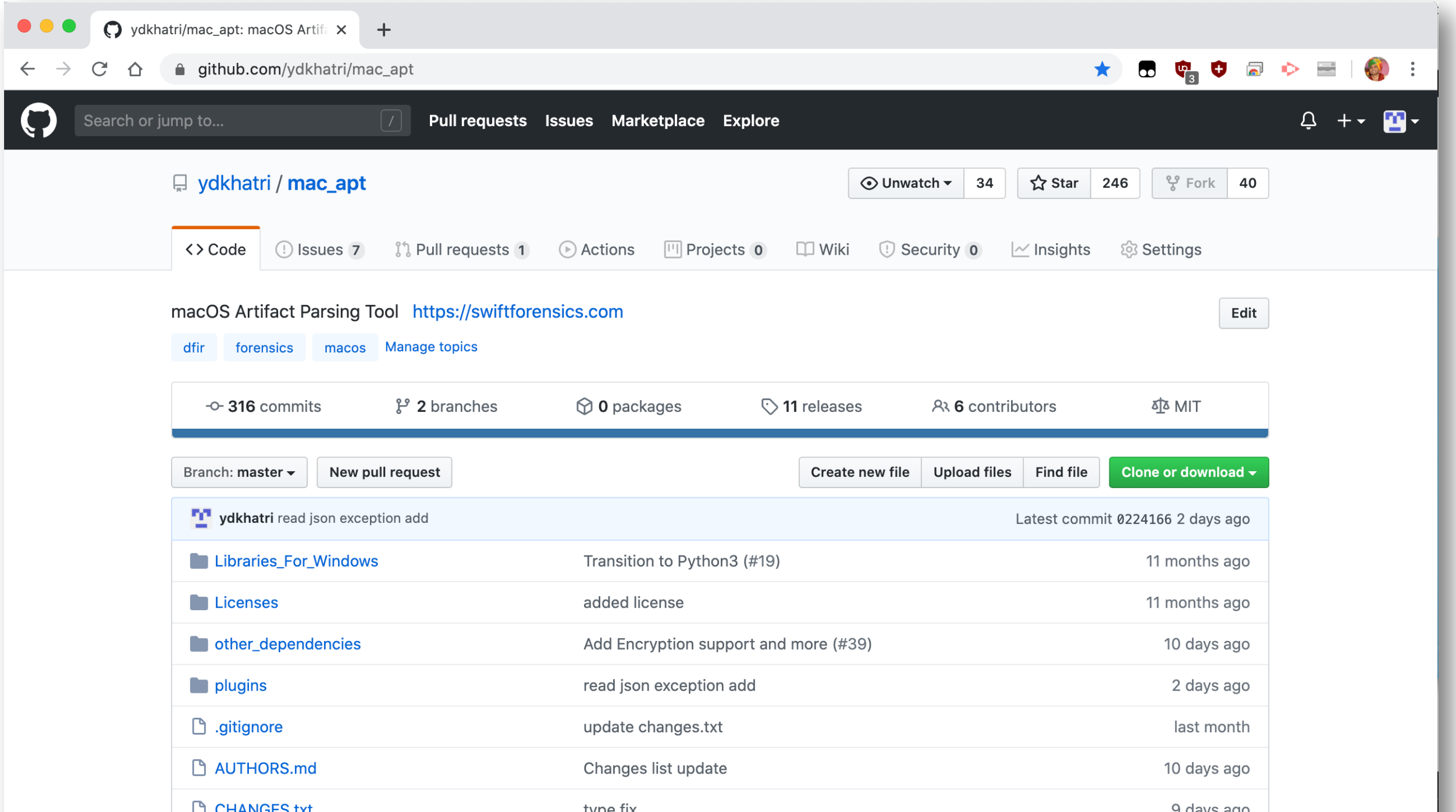
macOS Artifact Parsing Tool – mac_apt

- Open source & OS independent

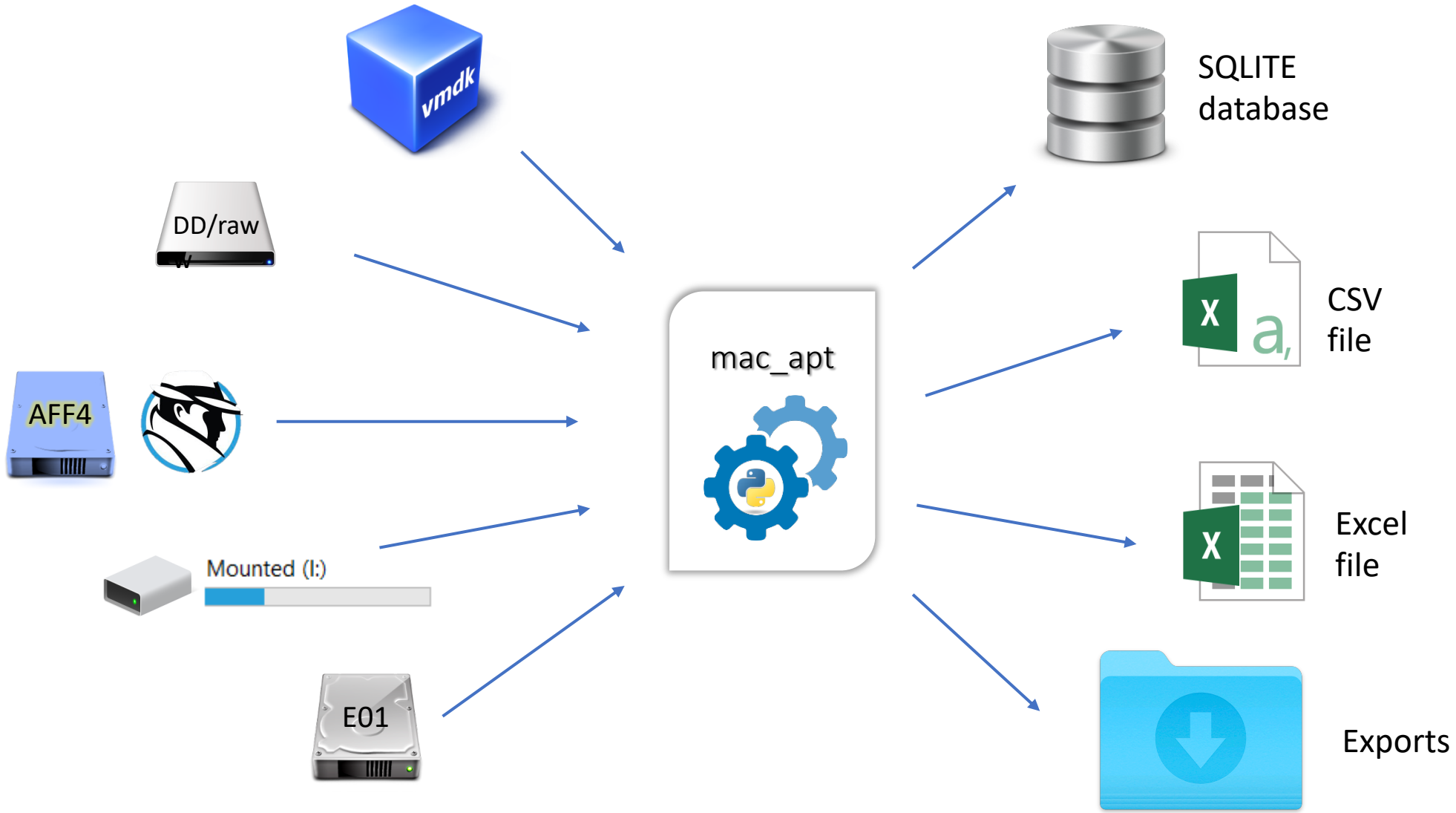


Plugins available (as of version 0.7.dev)

- APPLIST
- ARD
- AUTOSTART
- BASICINFO
- BLUETOOTH
- CHROME
- COOKIES
- DOCKITEMS
- DOMAINS
- FSEVENTS
- IDEVICEBACKUPS
- IDEVICEINFO
- IMESSAGE
- INETACCOUNTS
- INSTALLHISTORY
- MSOFFICE
- NETUSAGE
- NETWORKING
- NOTES
- NOTIFICATIONS
- PRINTJOBS
- QUARANTINE
- QUICKLOOK
- RECENTITEMS
- SAFARI
- SAVEDSTATE
- SCREENTIME
- SPOTLIGHT
- SPOTLIGHTSHORTCUTS
- TERMINALSTATE
- TERMSESSIONS
- UNIFIEDLOGS
- USERS
- WIFI


ydkhatri/mac_apt: macOS Artif
github.com/ydkhatri/mac_apt
Search or jump to...
Pull requests
Issues
Marketplace
Explore
ydkhatri / mac_apt
Unwatch 34
Star 246
Fork 40
Code
Issues 7
Pull requests 1
Actions
Projects 0
Wiki
Security 0
Insights
Settings
macOS Artifact Parsing Tool https://swiftforensics.com
Edit
dfir
forensics
macos
Manage topics
316 commits
2 branches
0 packages
11 releases
6 contributors
MIT
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
ydkhatri read json exception add
Latest commit 0224166 2 days ago
Libraries_For_Windows
Transition to Python3 (#19)
11 months ago
Licenses
added license
11 months ago
other_dependencies
Add Encryption support and more (#39)
10 days ago
plugins
read json exception add
2 days ago
.gitignore
update changes.txt
last month
AUTHORS.md
Changes list update
10 days ago

mac_apt - Input & output types

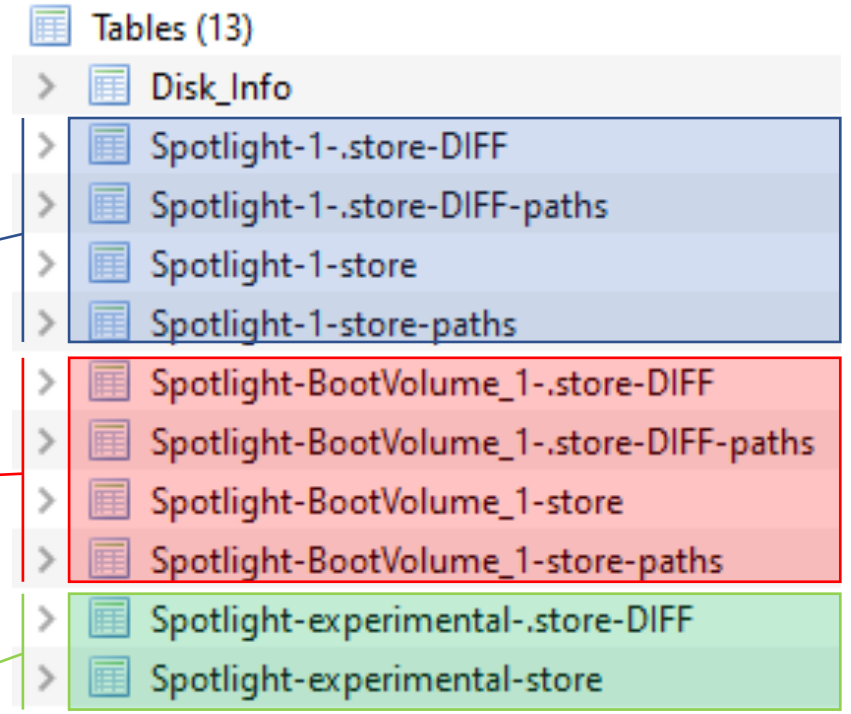


mac_apt demo

Desired Items/Activity (to search for)	Plugins
User accounts on system	USERS
User accounts (cloud)	INETACCOUNTS
Communication & Internet	IMESSAGE, SAFARI, CHROME, COOKIES
App/Program List	APPLIST, INSTALLHISTORY, DOCKITEMS, AUTOSTART
App/Program usage	TERMINALSTATE, TERMSESSIONS, SAVEDSTATE, ARD, SCREENTIME, SPOTLIGHTSHORTCUTS
Data Usage	NETUSAGE
Printing	PRINTJOBS
Accessed Files, Folders, Volumes, Disks, Servers	RECENTITEMS, MSOFFICE, SPOTLIGHT, QUARANTINE
Network & Connected devices	WIFI, NETWORKING, BLUETOOTH, IDEVICEINFO, IDEVICEBACKUPS
Notifications	NOTIFICATIONS
File, Note, Email usage (last used/viewed, num times, ..)	SPOTLIGHT
User stored notes	NOTES, SPOTLIGHT
OS (system) & Disk info	BASICINFO, DOMAINS
Filesystem activity	FSEVENTS

Understanding SPOTLIGHT output

- Multiple spotlight databases exist on macOS Catalina
  - Volume databases
    - One for DATA volume
    - One for SYSTEM volume (under BootVolume folder)
  - Per-user databases
    - One per user (stores records from Apps that user interacts with)



mac_apt.db

NOTE: -.store-DIFF tables only contain data not saved in the -store tables to avoid duplication

Useful queries for SPOTLIGHT tables

- Email

```
SELECT _kMDItemExternalID, kMDItemContentCreationDate, kMDItemSubject, com_apple_mail_read,
com_apple_mail_dateLastViewed, kMDItemUseCount, _kMDItemSnippet, kMDItemAuthorEmailAddresses, kMDItemAuthors,
kMDItemPrimaryRecipientEmailAddresses
FROM "Spotlight-YOURUSER-store"
WHERE kMDItemKind LIKE "email message"
```

- Application usage (DATA volume)

```
SELECT kMDItemDisplayName, _kMDItemFileName, kMDItemUseCount, kMDItemUsedDates, kMDItemLastUsedDate
FROM "Spotlight-1-store"
WHERE kMDItemKind LIKE "Application" and kMDItemUseCount not like ""
ORDER BY kMDItemUseCount DESC
```

- Application usage (SYSTEM volume)

```
SELECT kMDItemDisplayName, _kMDItemFileName, kMDItemUseCount, kMDItemUsedDates, kMDItemLastUsedDate
FROM "Spotlight-BootVolume_1-store"
WHERE kMDItemKind LIKE "Application" and kMDItemUseCount not like ""
ORDER BY kMDItemUseCount DESC
```

Thanks for watching!

Any Questions?

https://github.com/ydkhatri/mac_apt

@swiftforensics

Yogesh@swiftforensics.com