
The (Mis)Education of
macOS Security Internals

~

❯ whoami

```
⌥⌘2                                    ~

~
❯ whoami
  Stuart Ashenbrenner
~
❯ whatdoIdo
```

```
⌥⌘2                                    ~

~
❯ whoami
  Stuart Ashenbrenner
~
❯ whatdoIdo
  Principal Product Researcher, macOS
~
❯ whatelse
```

```
~ ⌥⌘2 ~

~
❯ whoami
  Stuart Ashenbrenner
~
❯ whatdoIdo
  Principal Product Researcher, macOS
~
❯ whatelse
  Alpine, OR → Portland, OR
  Girl Dad
  Basketball Coach
```

Syllabus

Syllabus

THREE LEVELS OF DEFENSE

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

CHECK

BLOCK

REMEDIATE

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

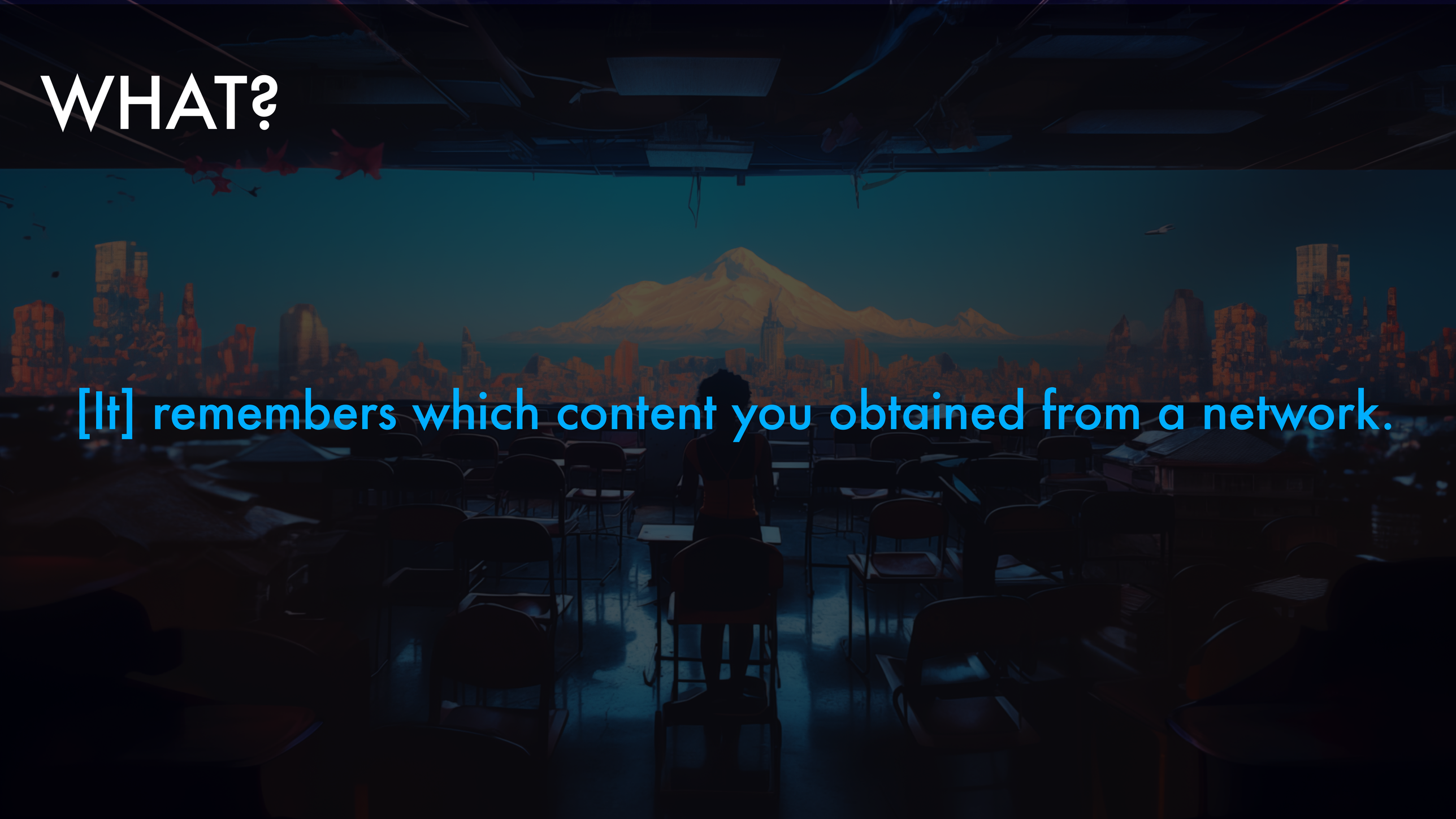
XPROTECT REMEDIATOR


FILE QUARANTINE


WHAT?

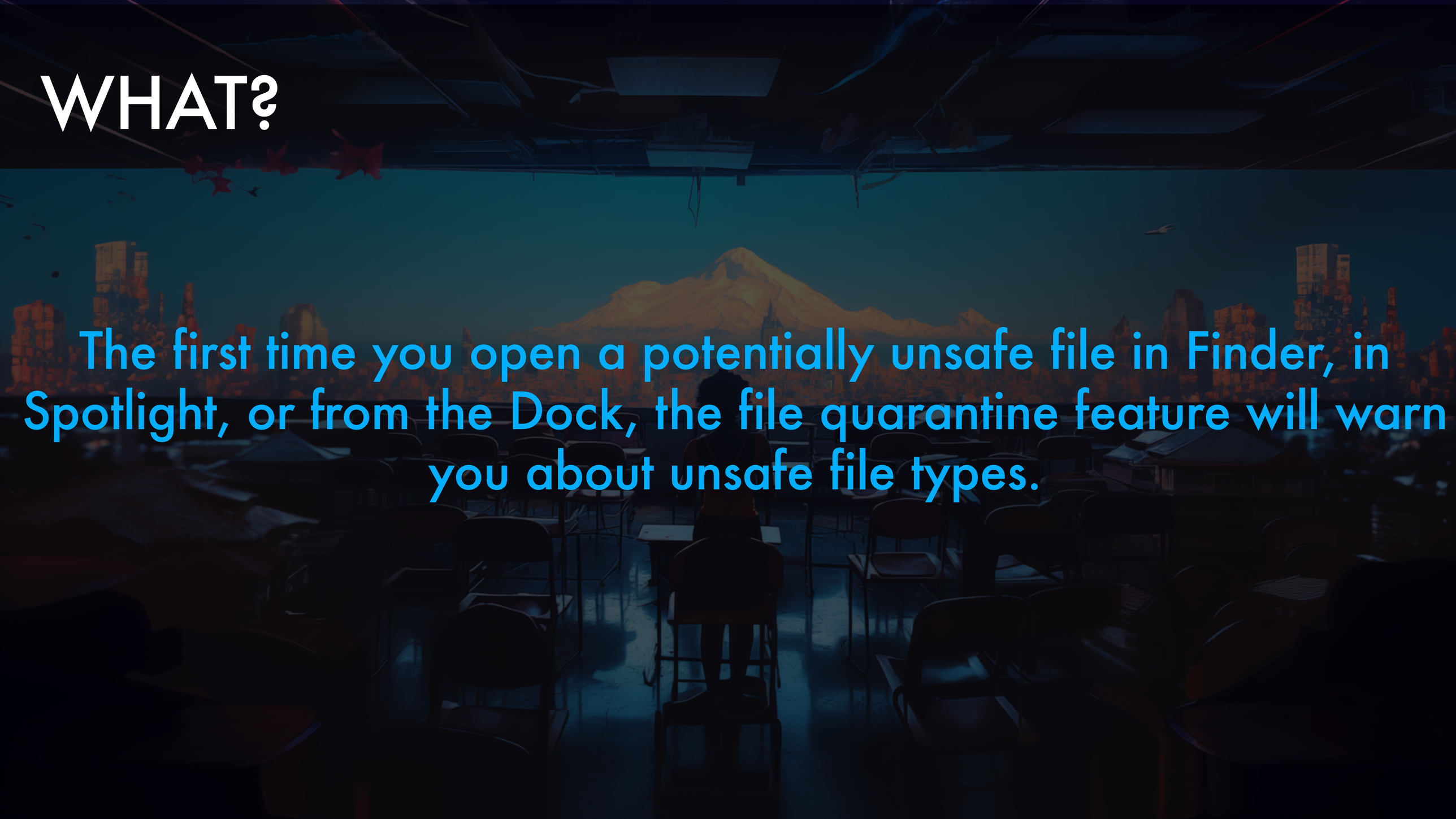
WHAT?

WHAT?



[It] remembers which content you obtained from a network.

WHAT?

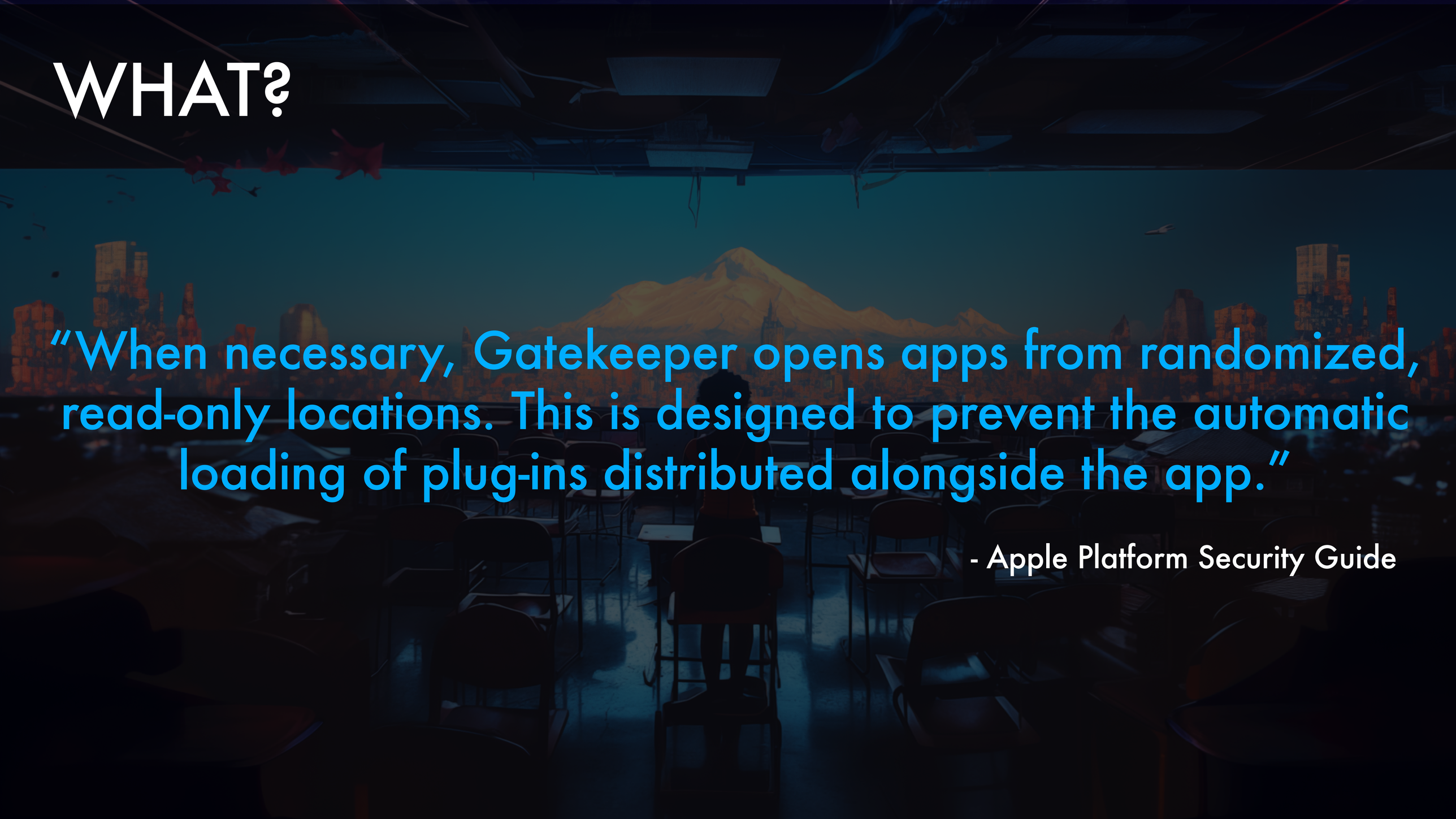


The first time you open a potentially unsafe file in Finder, in Spotlight, or from the Dock, the file quarantine feature will warn you about unsafe file types.


APP TRANSLOCATION


WHAT?

WHAT?



"When necessary, Gatekeeper opens apps from randomized, read-only locations. This is designed to prevent the automatic loading of plug-ins distributed alongside the app."

- Apple Platform Security Guide

WHAT?

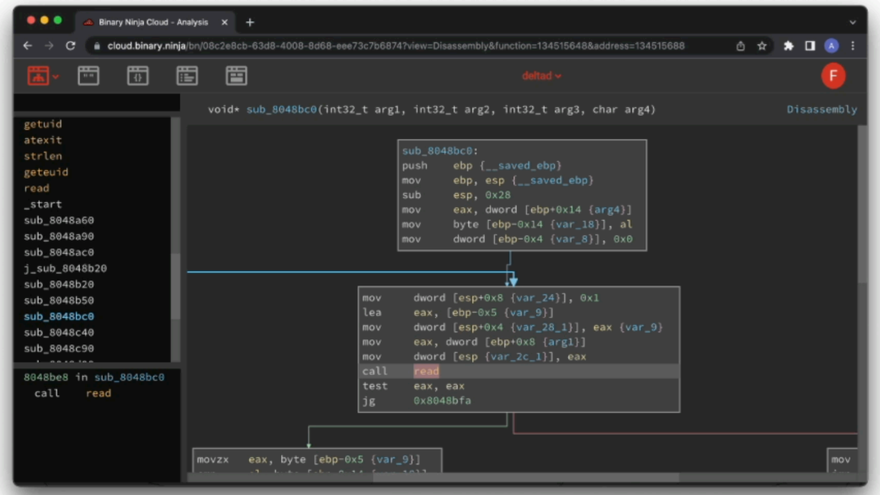
/private/var/folders/<random_characters>/AppTranslocation

binary.ninja

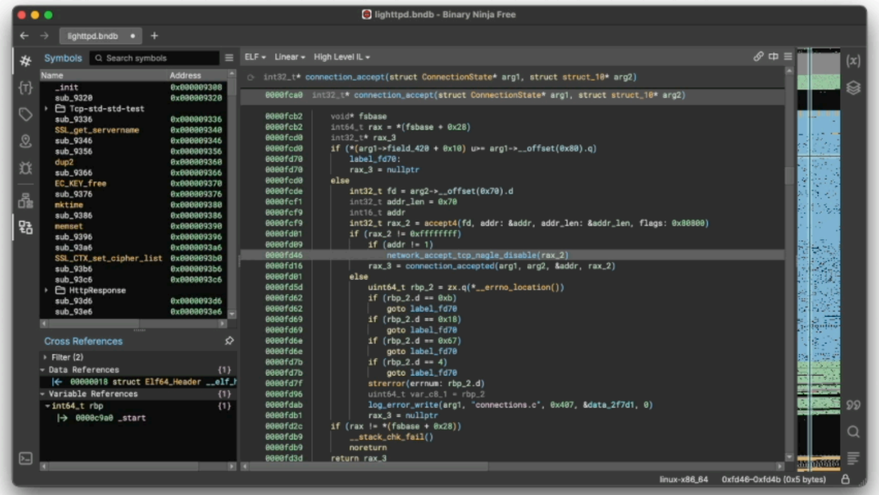
BINARYNINJA Features Enterprise Sidekick Cloud Training Support Blog Gear Free Purchase

There are two ways to try Binary Ninja for free! Binary Ninja Cloud supports all architectures, but requires you to upload your binaries. Binary Ninja Free is a downloadable app that runs locally, but has architecture restrictions. Neither free option supports our powerful API / Plugin ecosystem.

CLOUD



FREE



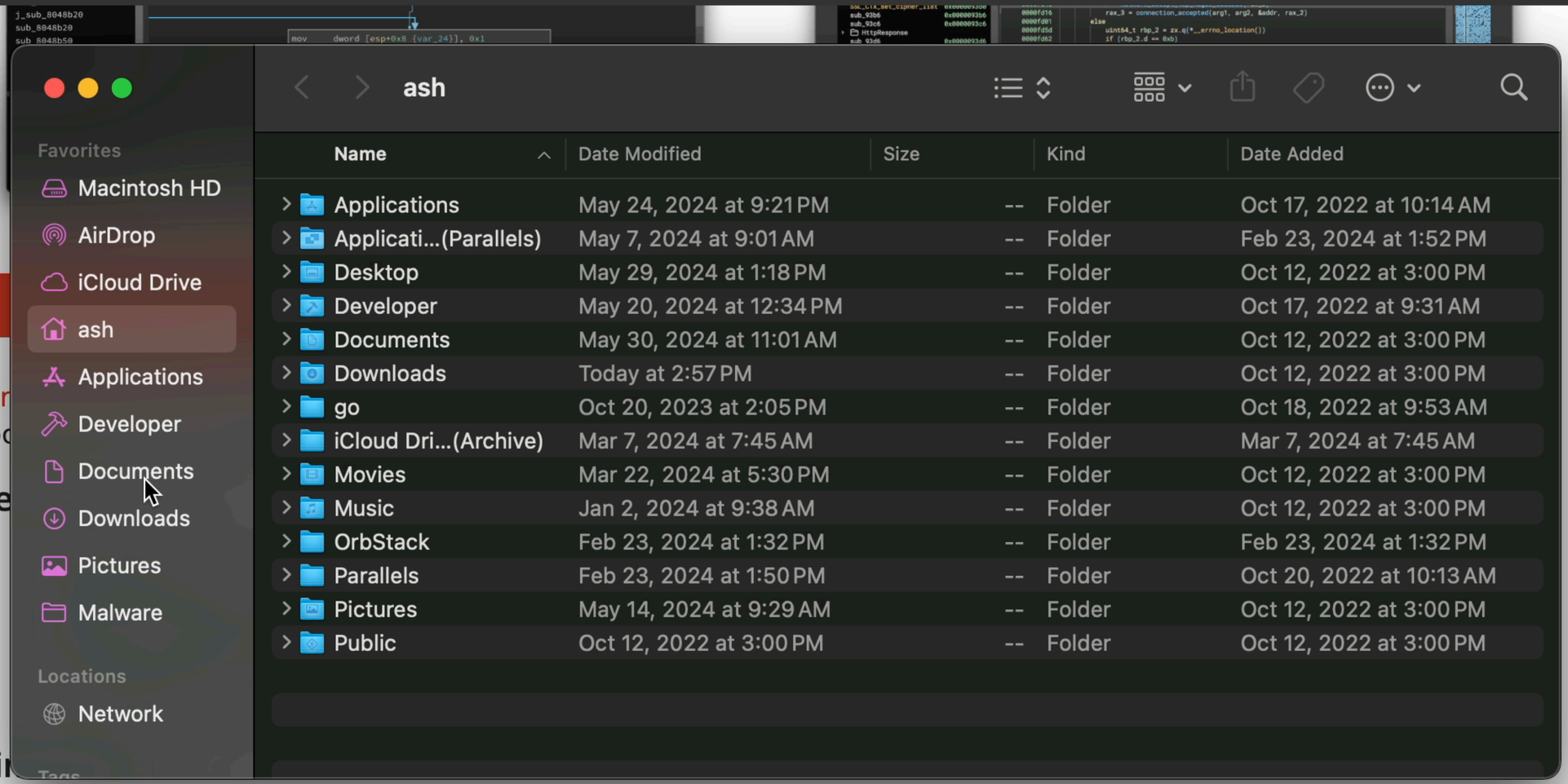
Try Cloud!

Download For Windows

Download For macOS

binary.ninja

BINARYNINJA Features Enterprise Sidekick Cloud Training Support Blog Gear Free Purchase



Bi
to

Fe

Li

It does, however come with some limitations (see the ToS for more info):

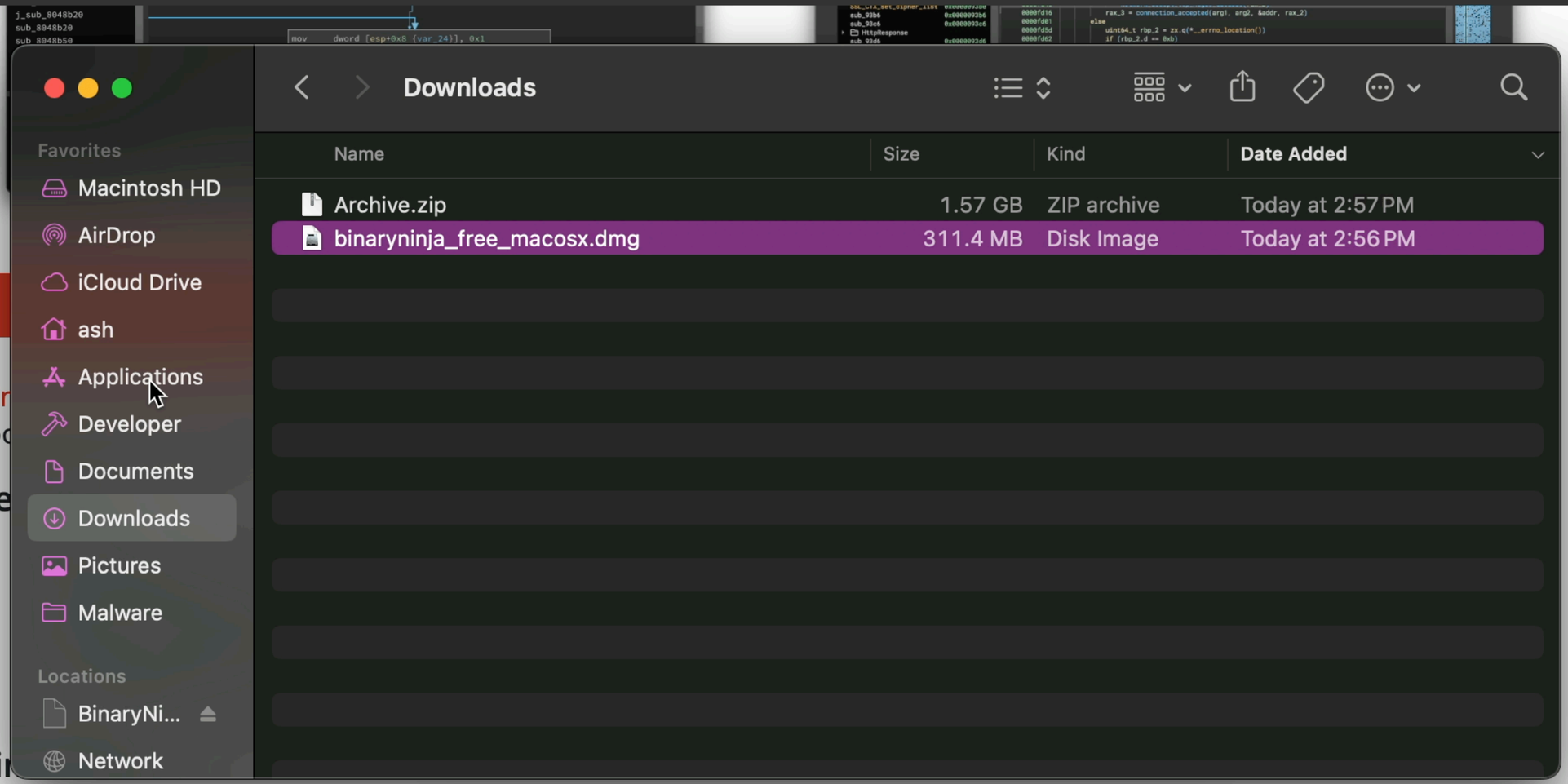
- Not as feature-rich as the native client

Features

- Save/load analysis databases
- Customizable UI
- Integrated Debugger

binary.ninja

BINARYNINJA Features Enterprise Sidekick Cloud Training Support Blog Gear Free Purchase



Bir
too

Fe

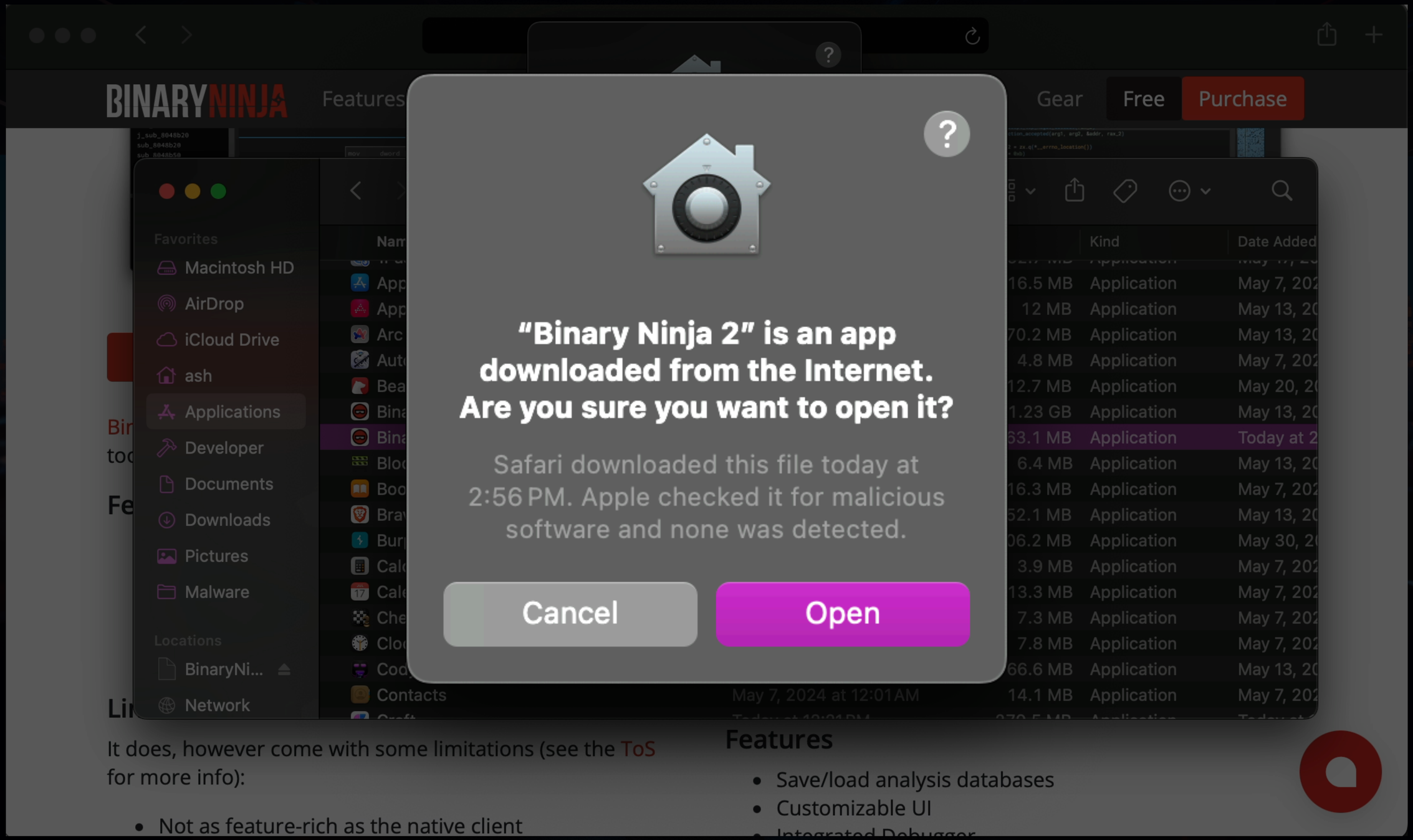
Li

It does, however come with some limitations (see the ToS for more info):

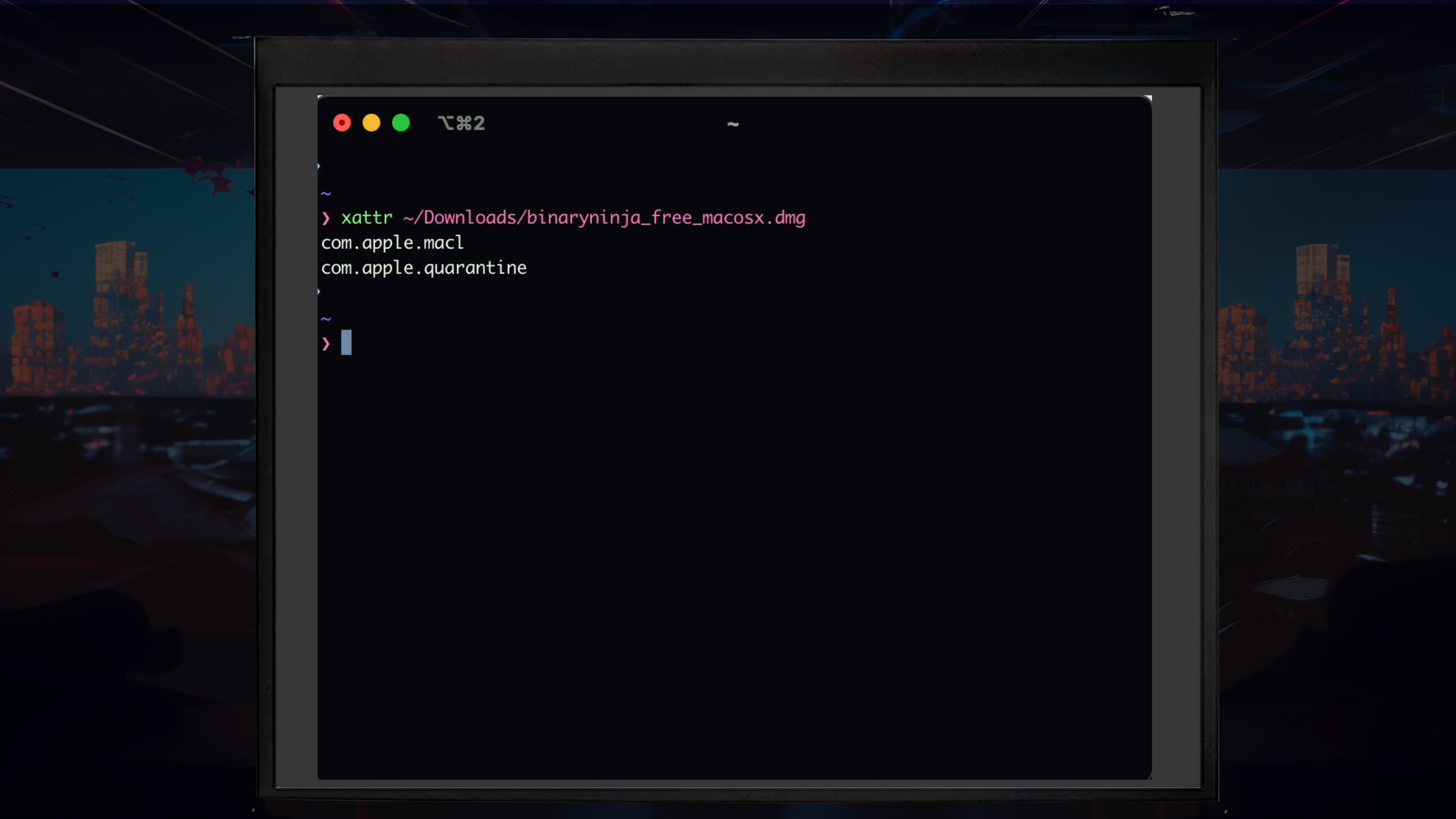
- Not as feature-rich as the native client

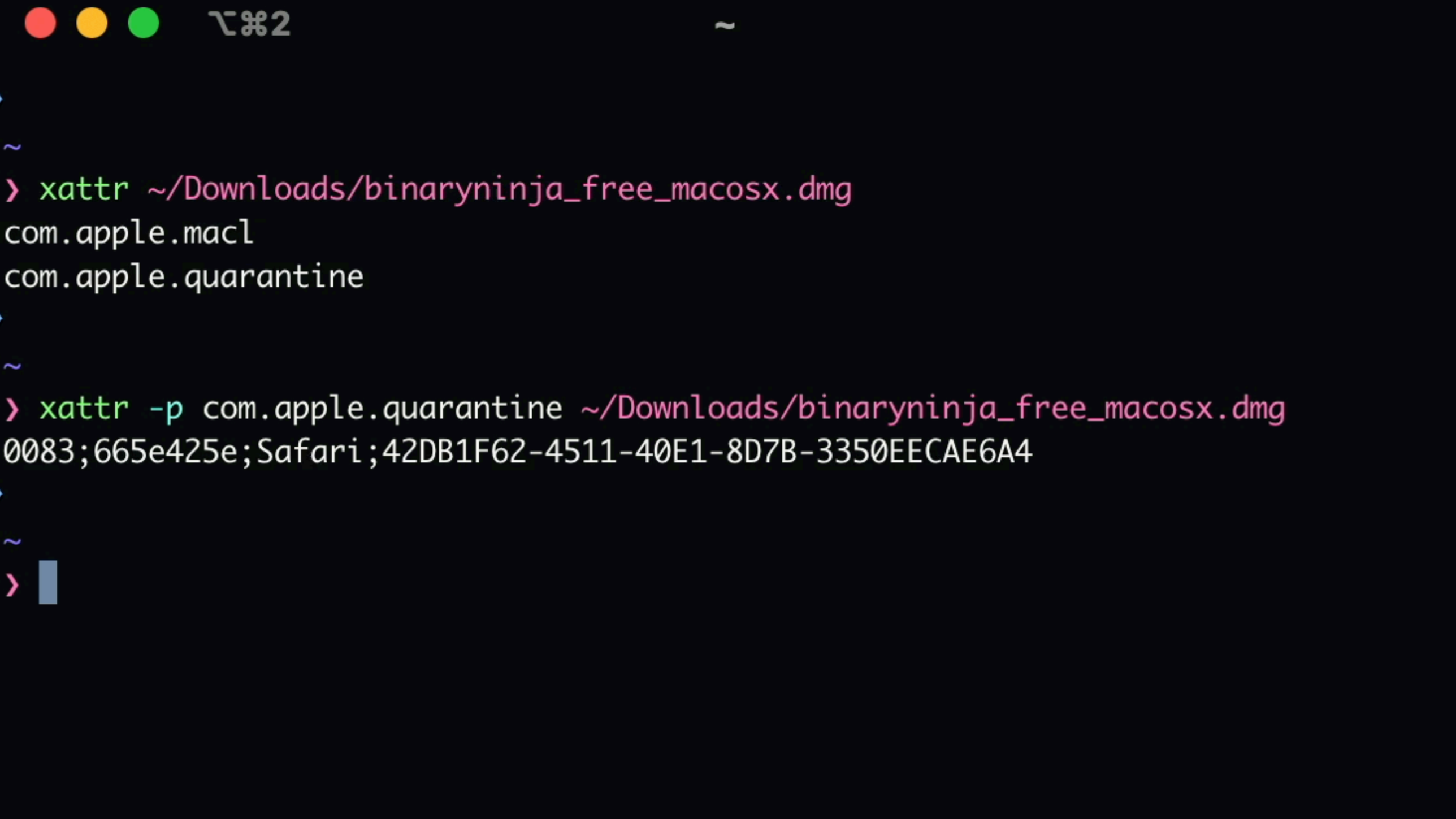
Features

- Save/load analysis databases
- Customizable UI
- Integrated Debugger

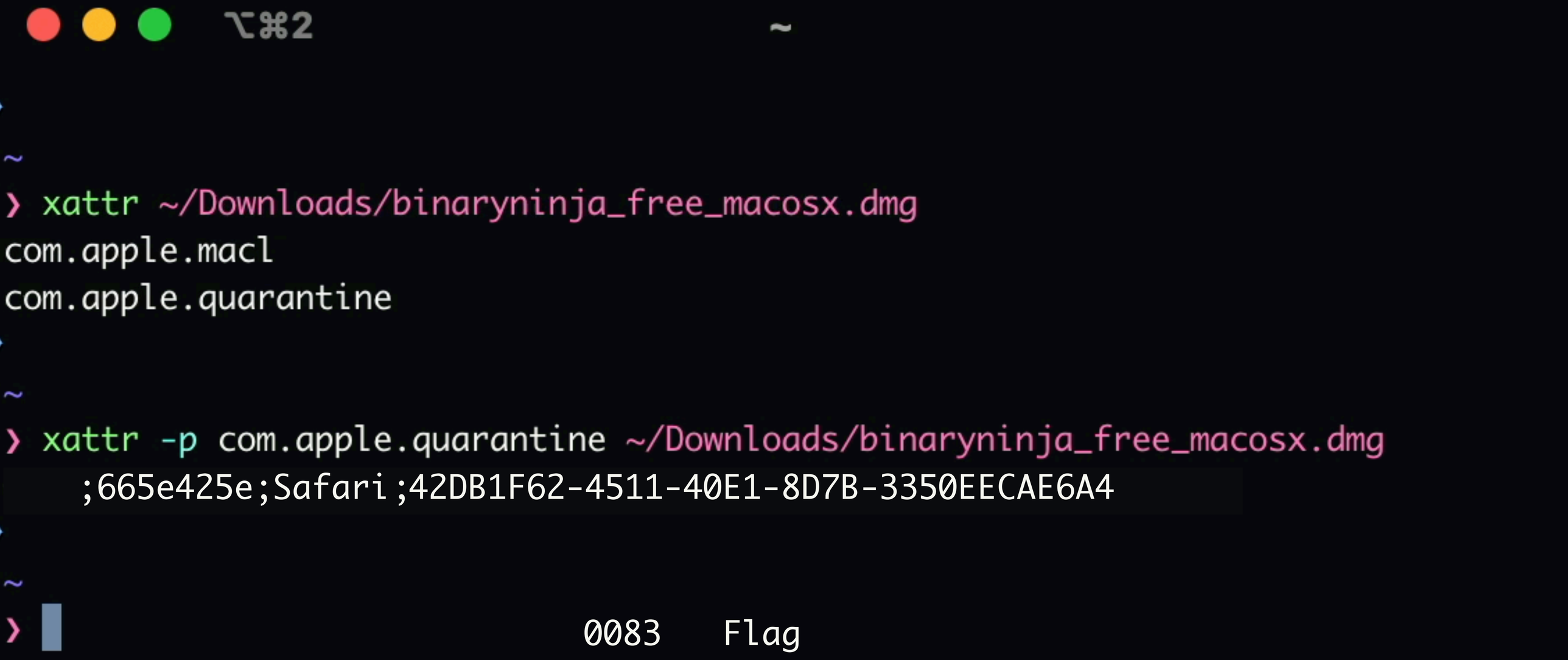

BINARYNINJA
Features
Gear
Free
Purchase
Favorites
Macintosh HD
AirDrop
iCloud Drive
ash
Applications
Developer
Documents
Downloads
Pictures
Malware
Locations
BinaryNi...
Network
Kind
Date Added
"Binary Ninja 2" is an app downloaded from the Internet. Are you sure you want to open it?
Safari downloaded this file today at 2:56 PM. Apple checked it for malicious software and none was detected.
Cancel
Open
It does, however come with some limitations (see the ToS for more info):
Not as feature-rich as the native client
Features
Save/load analysis databases
Customizable UI


⌥⌘2
~
~
❯


⌥⌘2
~
~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine
~
❯

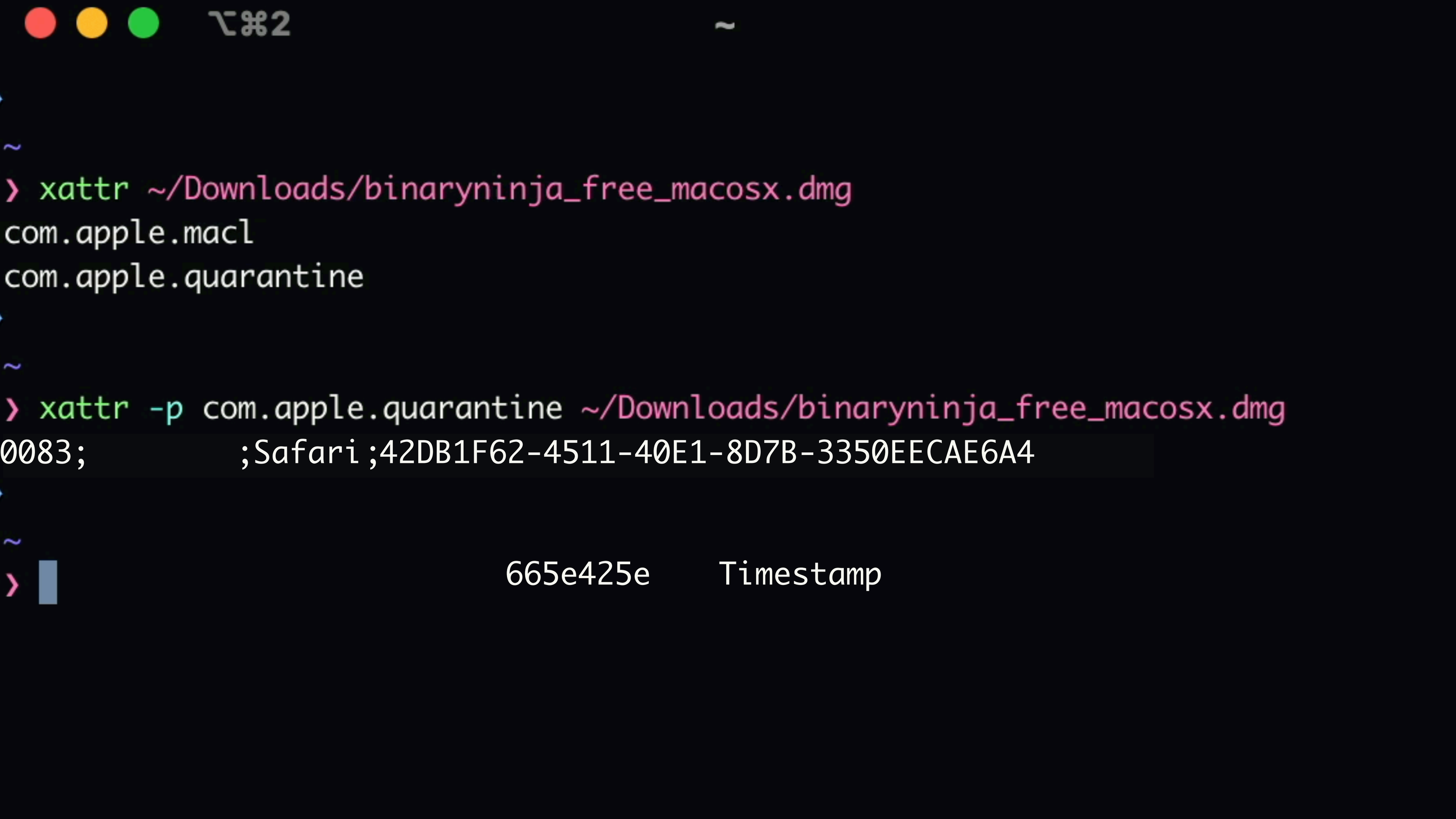

⌥⌘2
~
~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine
~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4
~
❯

```
⌥⌘2                                    ~

~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine

~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4

~
❯
```

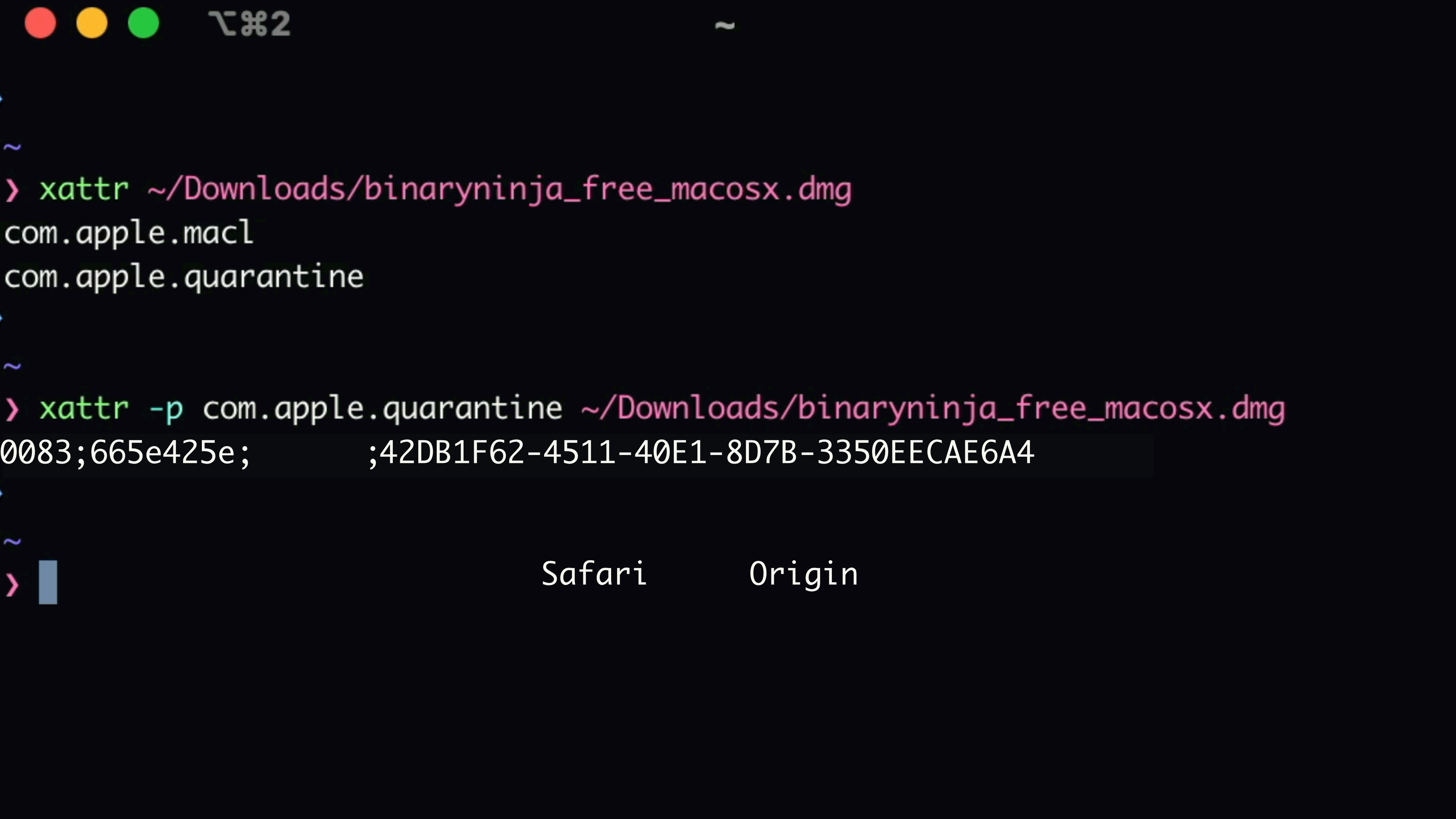

⌥⌘2
~
~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine
~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4
~
❯

0083 Flag

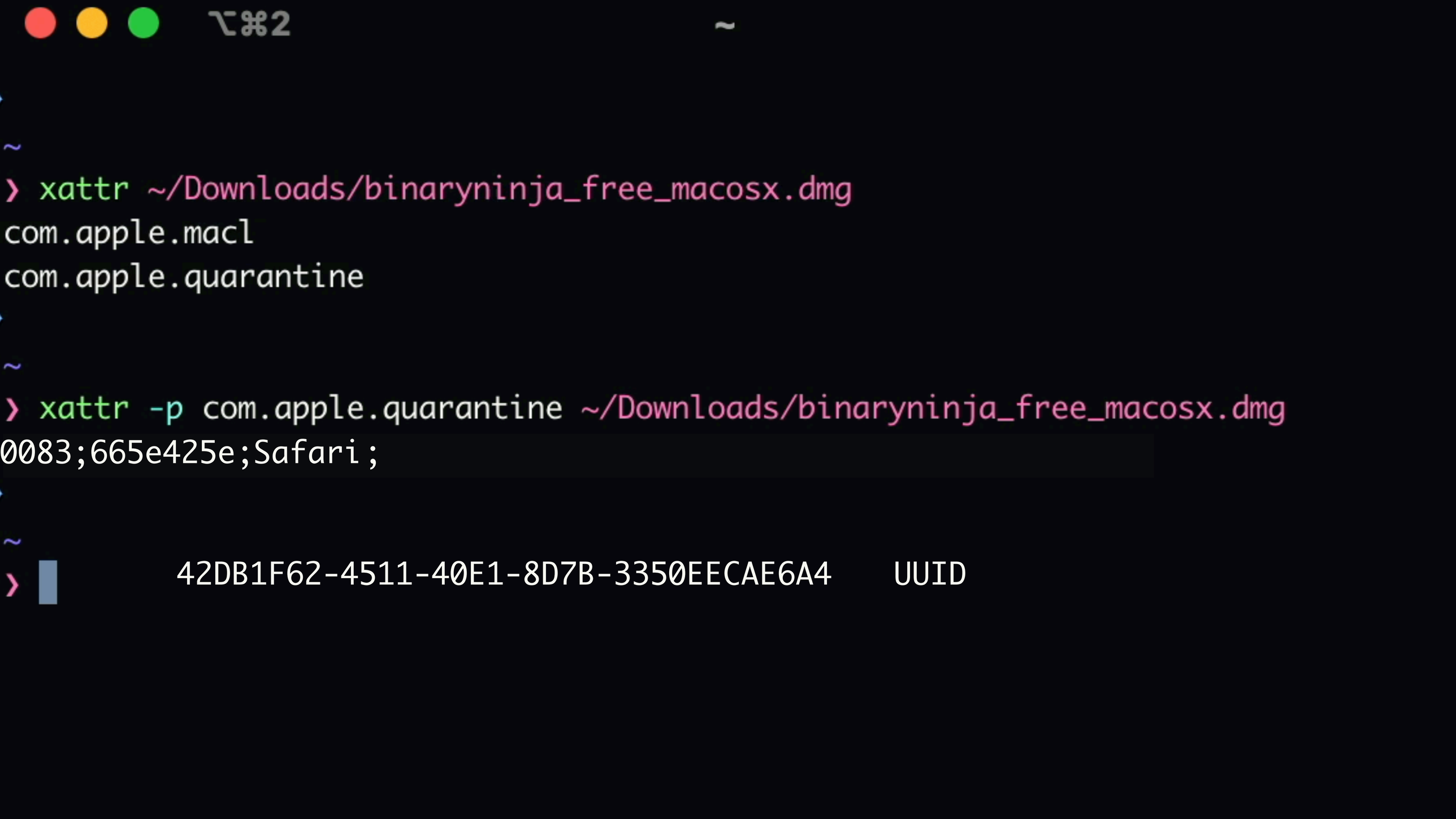
```
⌥⌘2                                    ~

~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine

~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4

~
❯
```


⌥⌘2
~
~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine
~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083; ;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4
~
❯
665e425e Timestamp

```
⌥⌘2                                    ~

~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine

~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4

~
❯
```

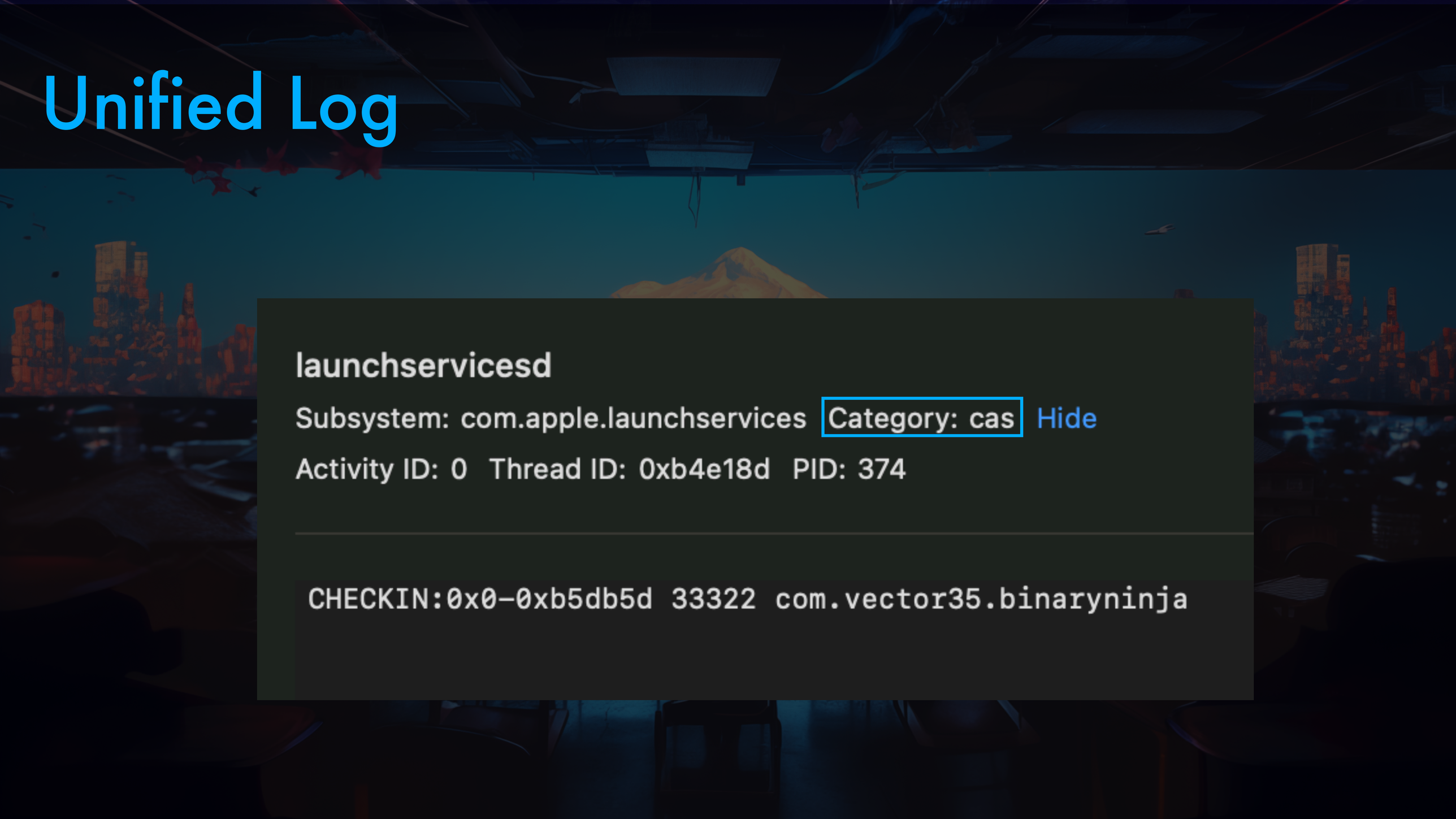

⌥⌘2
~
~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine
~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;   ;42DB1F62-4511-40E1-8D7B-3350EECAE6A4
~
❯
Safari
Origin

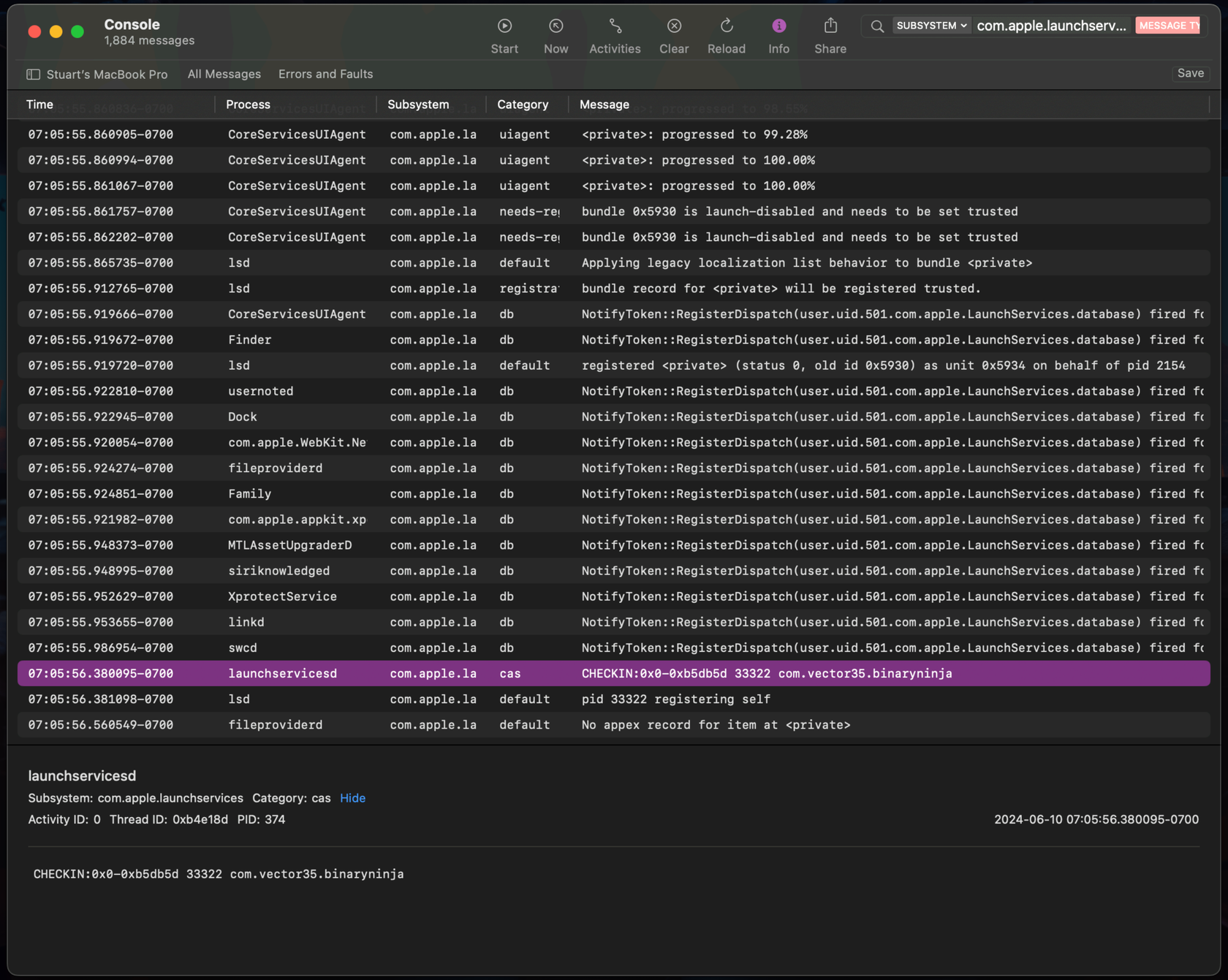
```
⌥⌘2                                    ~

~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine

~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4

~
❯
```


⌥⌘2
~
~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine
~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;
~
❯
42DB1F62-4511-40E1-8D7B-3350EECAE6A4 UUID

```
⌥⌘2                                    ~

~
❯ xattr ~/Downloads/binaryninja_free_macosx.dmg
com.apple.macl
com.apple.quarantine

~
❯ xattr -p com.apple.quarantine ~/Downloads/binaryninja_free_macosx.dmg
0083;665e425e;Safari;42DB1F62-4511-40E1-8D7B-3350EECAE6A4

~
❯
```

Unified Log


launchservicesd
Subsystem: com.apple.launchservices
Category: cas
Hide
Activity ID: 0 Thread ID: 0xb4e18d PID: 374
CHECKIN:0x0-0xb5db5d 33322 com.vector35.binaryninja


Console
1,884 messages
Start
Now
Activities
Clear
Reload
Info
Share
SUBSYSTEM
com.apple.launchserv...
MESSAGE TY
Stuart's MacBook Pro
All Messages
Errors and Faults
Save
Time
Process
Subsystem
Category
Message
07:05:55.860905-0700 CoreServicesUIAgent com.apple.la uiagent <private>: progressed to 99.28%
07:05:55.860994-0700 CoreServicesUIAgent com.apple.la uiagent <private>: progressed to 100.00%
07:05:55.861067-0700 CoreServicesUIAgent com.apple.la uiagent <private>: progressed to 100.00%
07:05:55.861757-0700 CoreServicesUIAgent com.apple.la needs-re bundle 0x5930 is launch-disabled and needs to be set trusted
07:05:55.862202-0700 CoreServicesUIAgent com.apple.la needs-re bundle 0x5930 is launch-disabled and needs to be set trusted
07:05:55.865735-0700 lsd com.apple.la default Applying legacy localization list behavior to bundle <private>
07:05:55.912765-0700 lsd com.apple.la registra bundle record for <private> will be registered trusted.
07:05:55.919666-0700 CoreServicesUIAgent com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.919672-0700 Finder com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.919720-0700 lsd com.apple.la default registered <private> (status 0, old id 0x5930) as unit 0x5934 on behalf of pid 2154
07:05:55.922810-0700 usernoted com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.922945-0700 Dock com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.920054-0700 com.apple.WebKit.Ne com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.924274-0700 fileproviderd com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.924851-0700 Family com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.921982-0700 com.apple.appkit.xp com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.948373-0700 MTLAssetUpgraderD com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.948995-0700 siriknowledged com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.952629-0700 XprotectService com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.953655-0700 linkd com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:55.986954-0700 swcd com.apple.la db NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired fo
07:05:56.380095-0700 launchservicesd com.apple.la cas CHECKIN:0x0-0xb5db5d 33322 com.vector35.binaryninja
07:05:56.381098-0700 lsd com.apple.la default pid 33322 registering self
07:05:56.560549-0700 fileproviderd com.apple.la default No appex record for item at <private>
launchservicesd
Subsystem: com.apple.launchservices Category: cas Hide
Activity ID: 0 Thread ID: 0xb4e18d PID: 374
2024-06-10 07:05:56.380095-0700
CHECKIN:0x0-0xb5db5d 33322 com.vector35.binaryninja

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

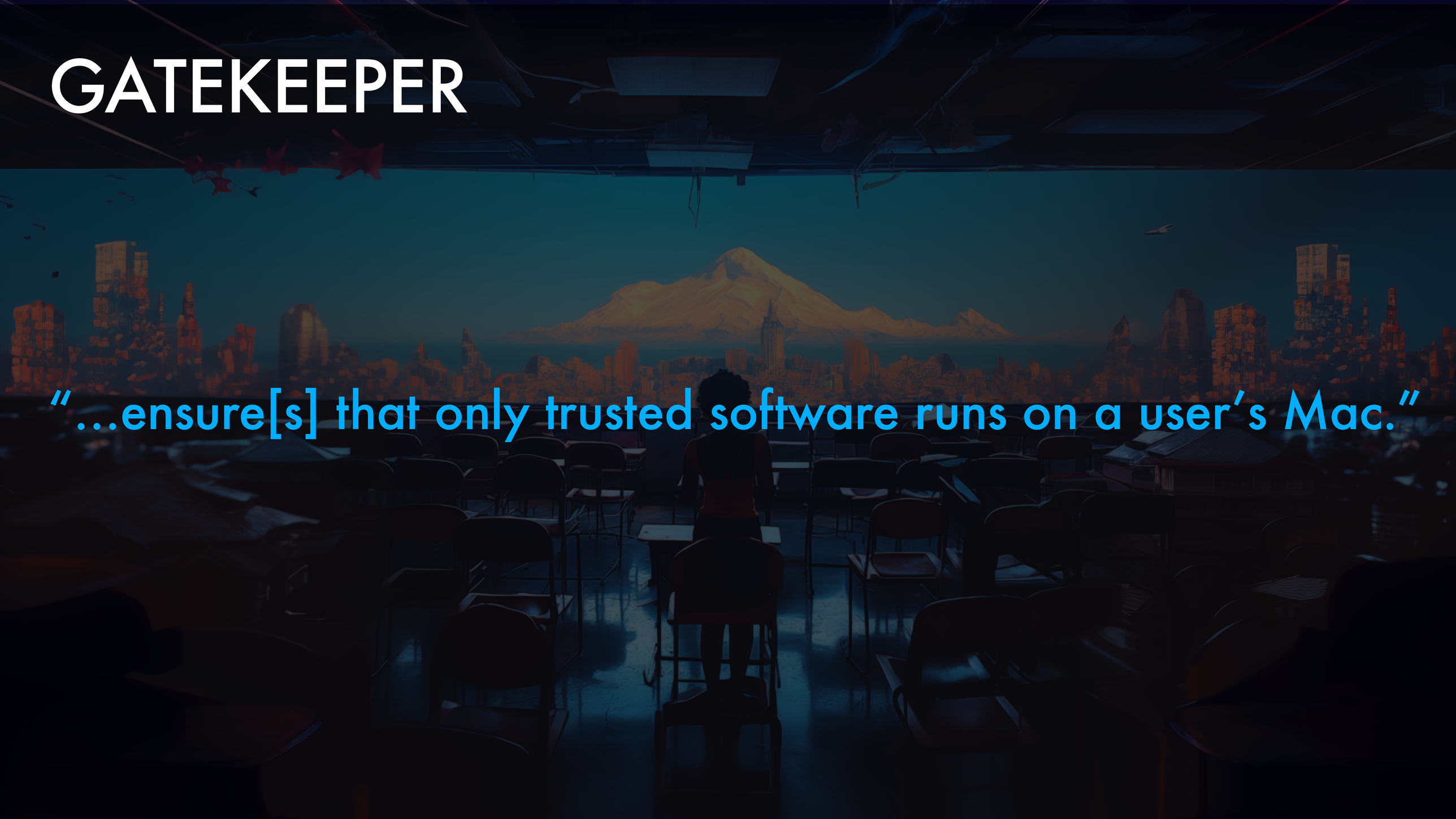
XPR


GATEKEEPER


GATEKEEPER


FILE QUARANTINE
APP TRANSLOCATION
GATEKEEPER

GATEKEEPER



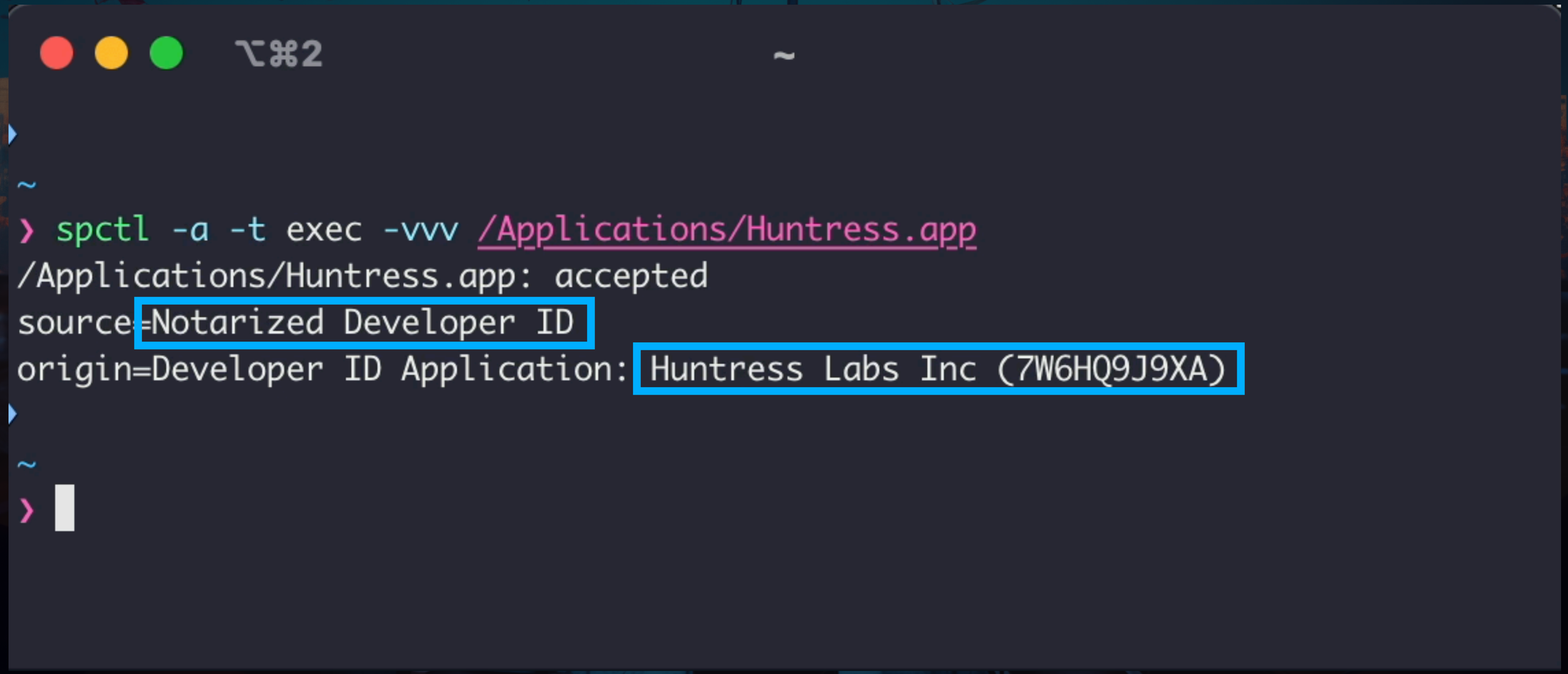
"…ensure[s] that only trusted software runs on a user's Mac."

GATEKEEPER

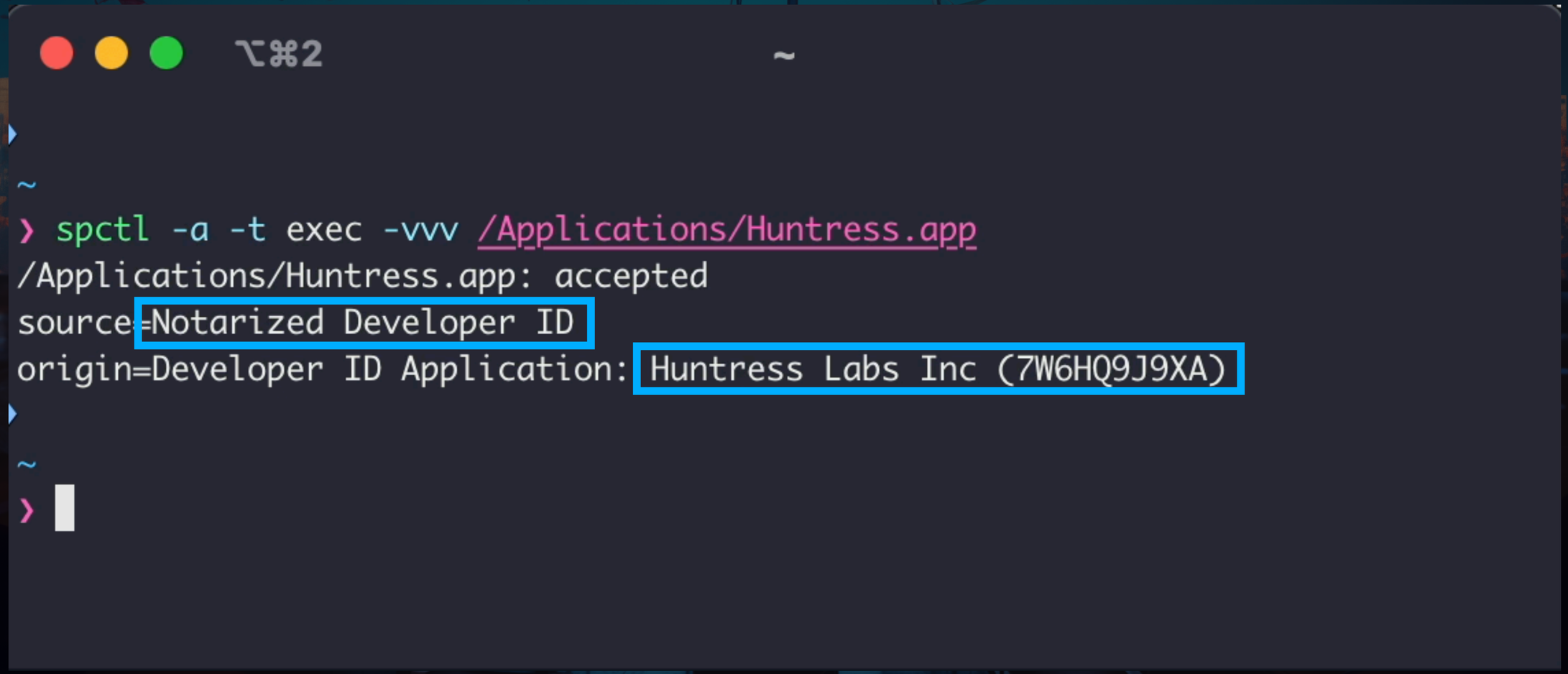
```
/Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources
❱ sqlite3 gk.db
SQLite version 3.43.2 2023-10-10 13:08:14
Enter ".help" for usage hints.
sqlite> .tables
blocked_hashes  blocked_teams   settings
sqlite> select count(*) from blocked_hashes;
578
sqlite> select count(*) from blocked_teams;
132
```

GATEKEEPER

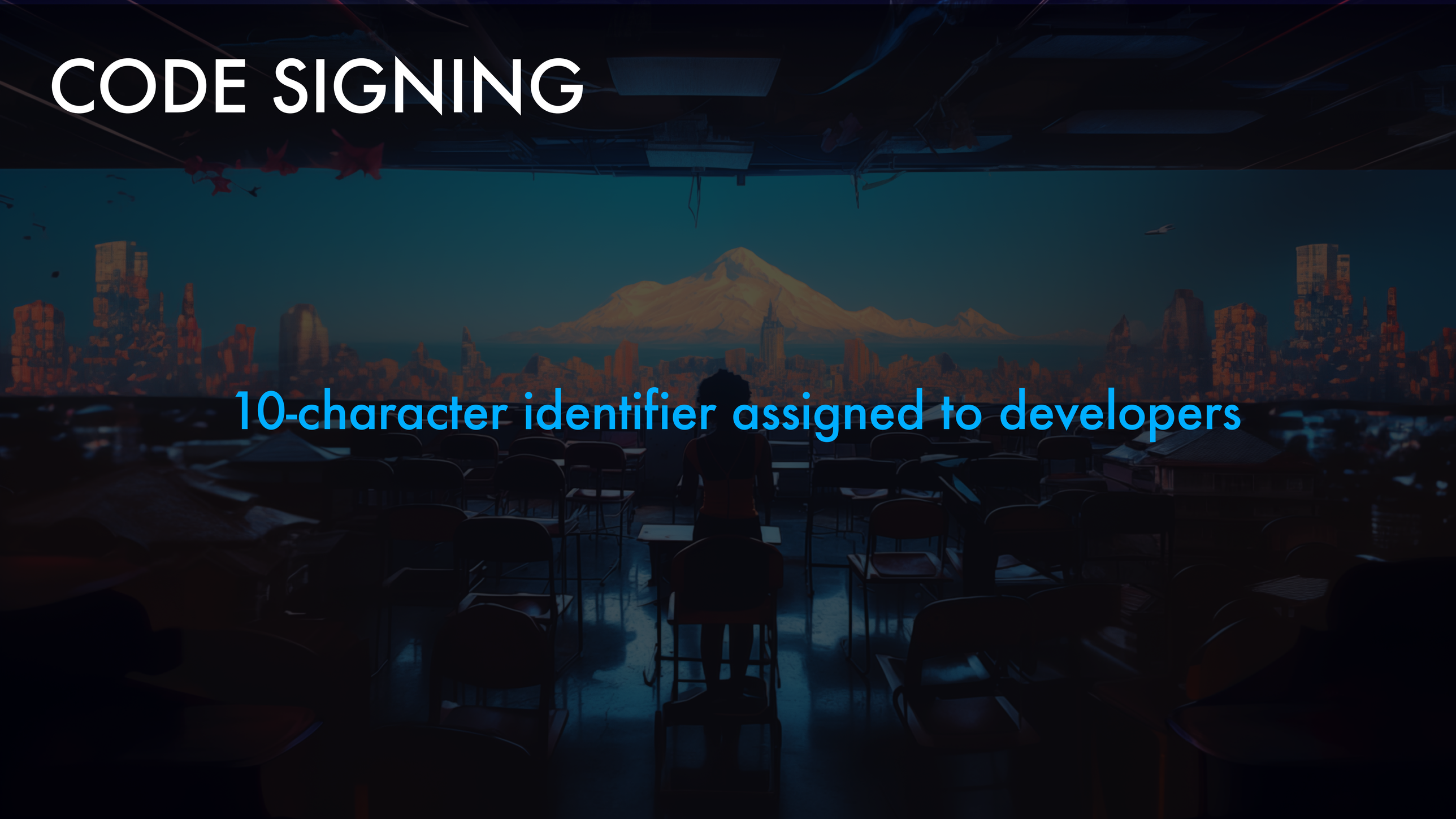
GATEKEEPER


⌥⌘2
~
~
› spctl -a -t exec -vvv /Applications/Huntress.app
/Applications/Huntress.app: accepted
source=Notarized Developer ID
origin=Developer ID Application: Huntress Labs Inc (7W6HQ9J9XA)
~
›

CODE SIGNING

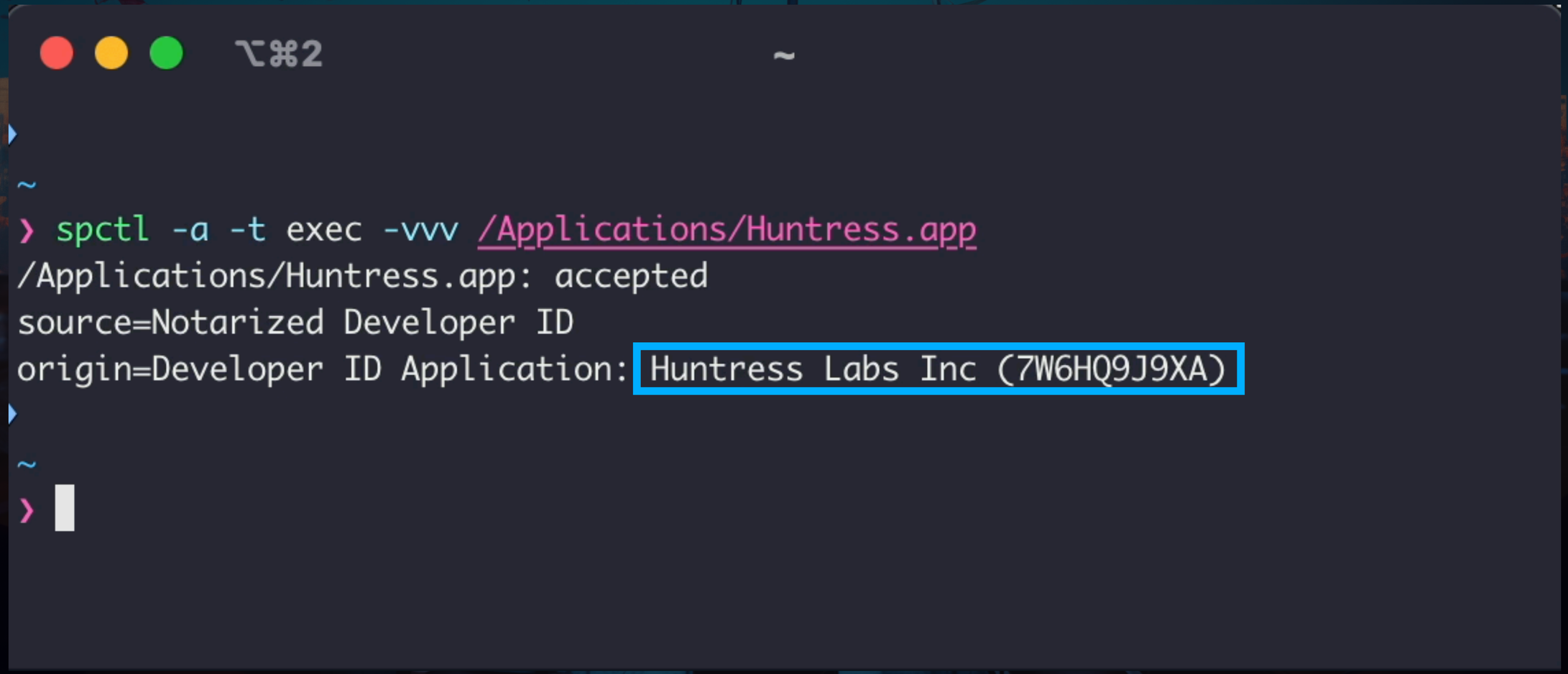


CODE SIGNING

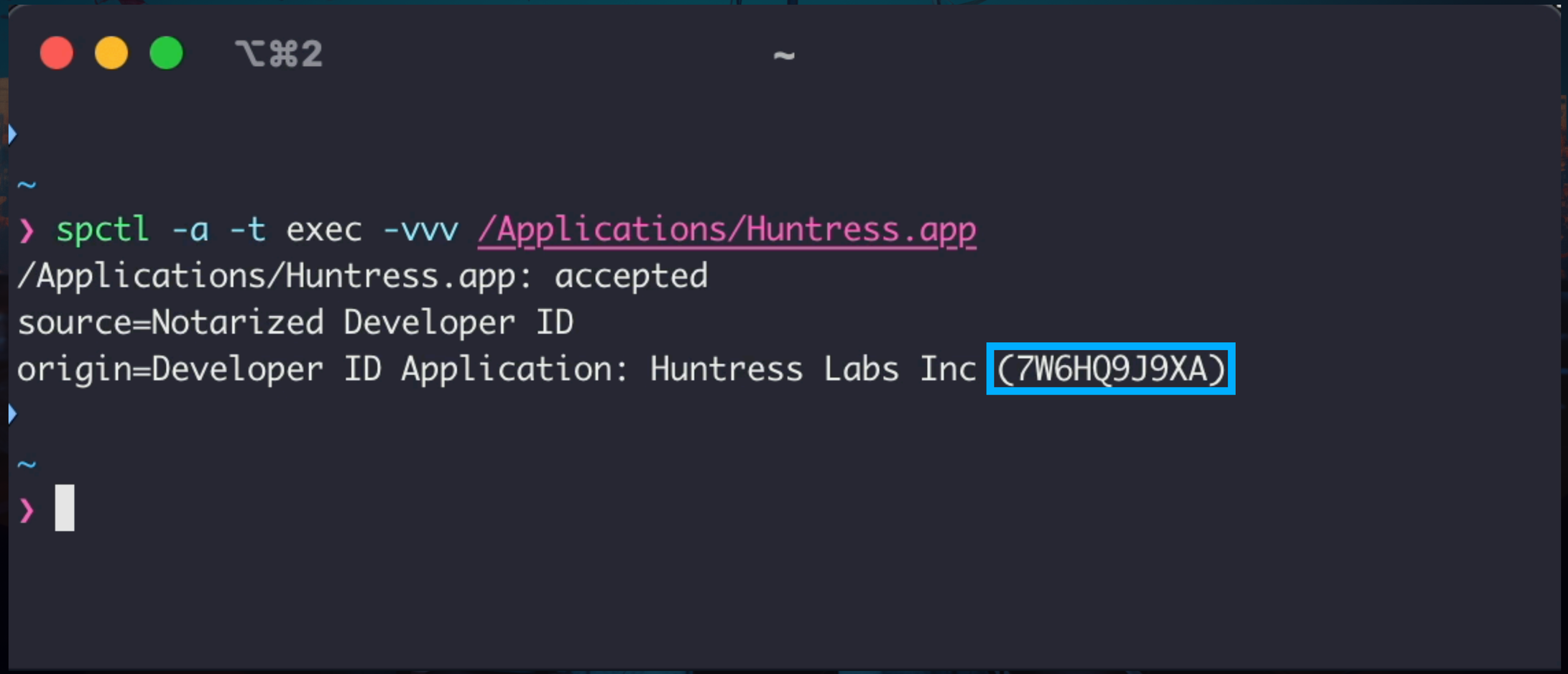


10-character identifier assigned to developers

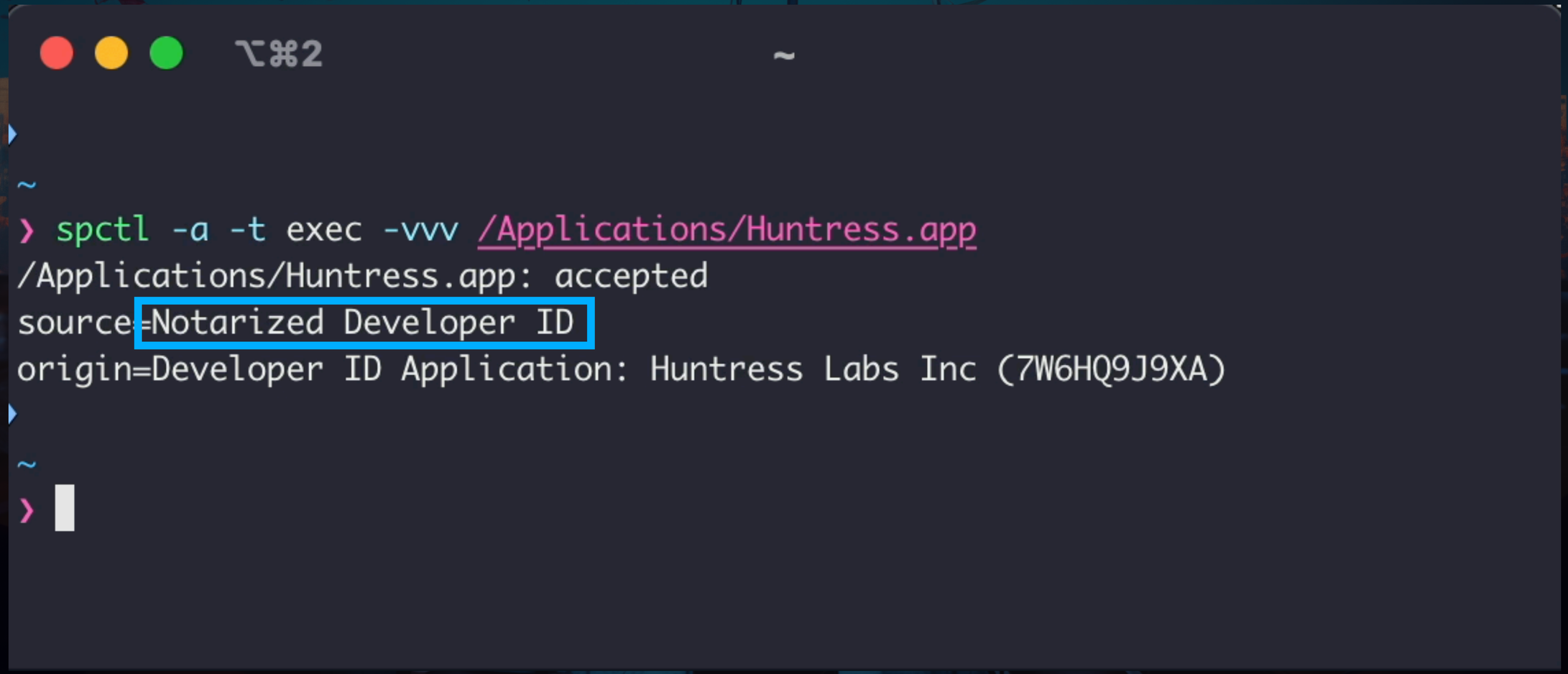
CODE SIGNING



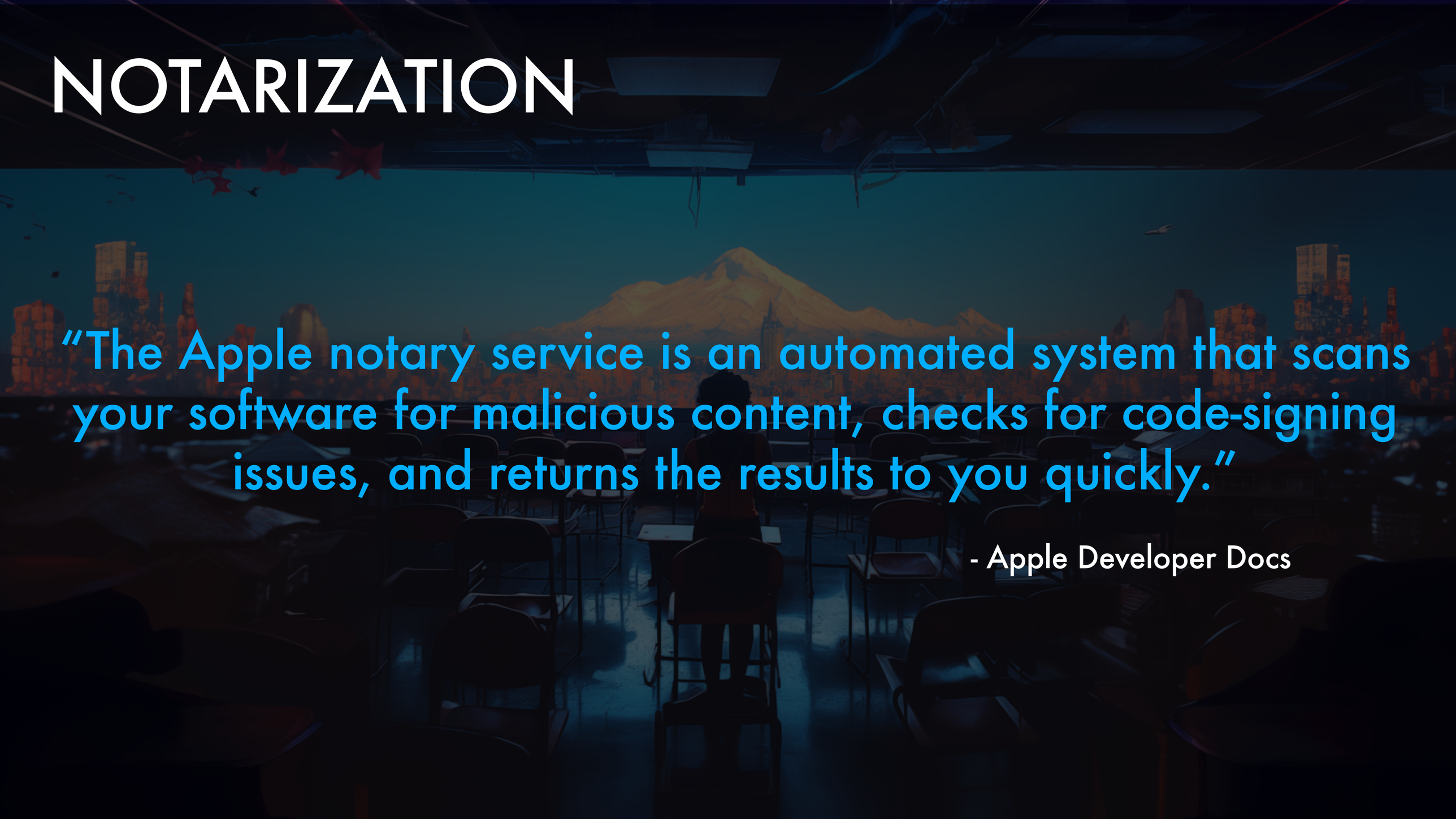
CODE SIGNING



NOTARIZATION



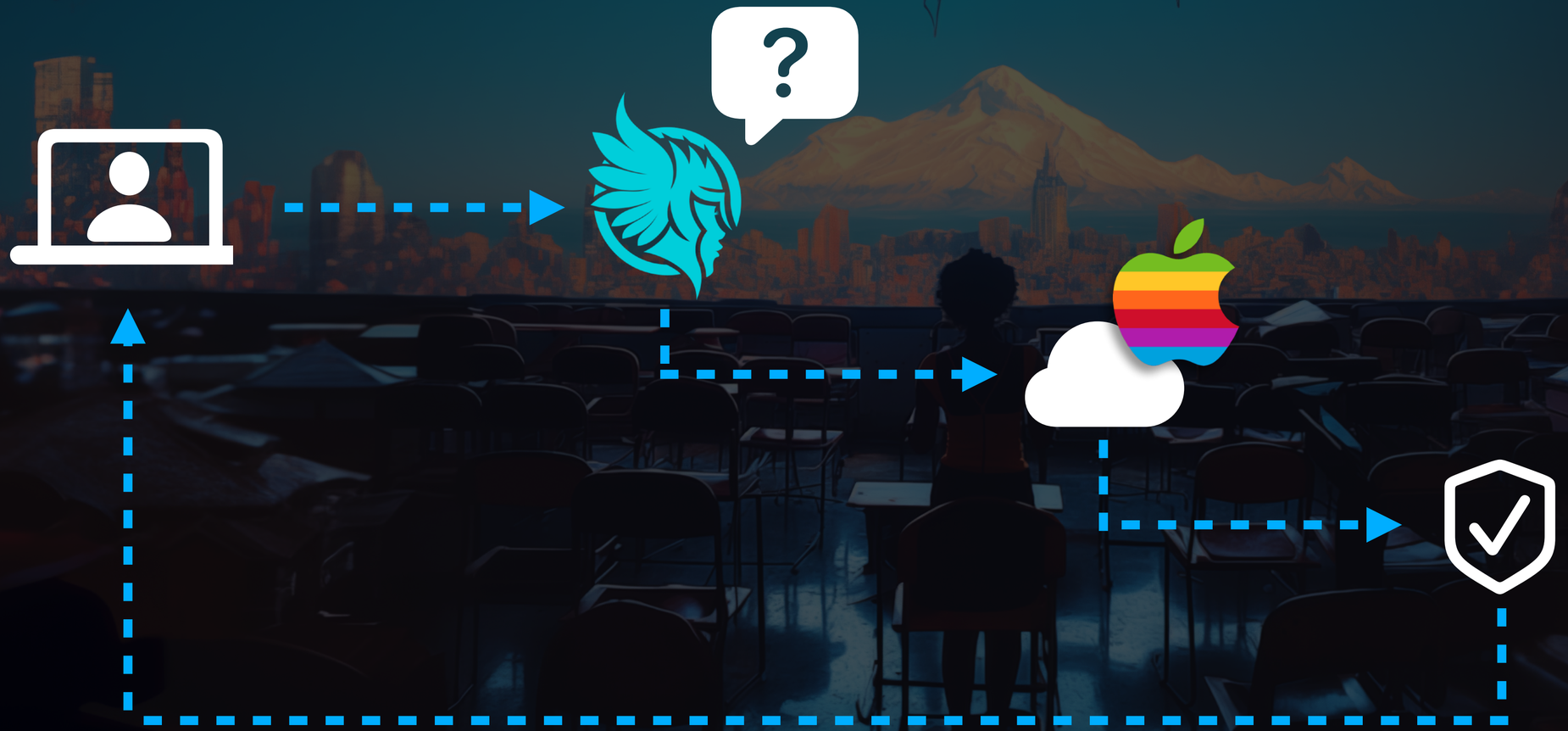
NOTARIZATION



"The Apple notary service is an automated system that scans your software for malicious content, checks for code-signing issues, and returns the results to you quickly."

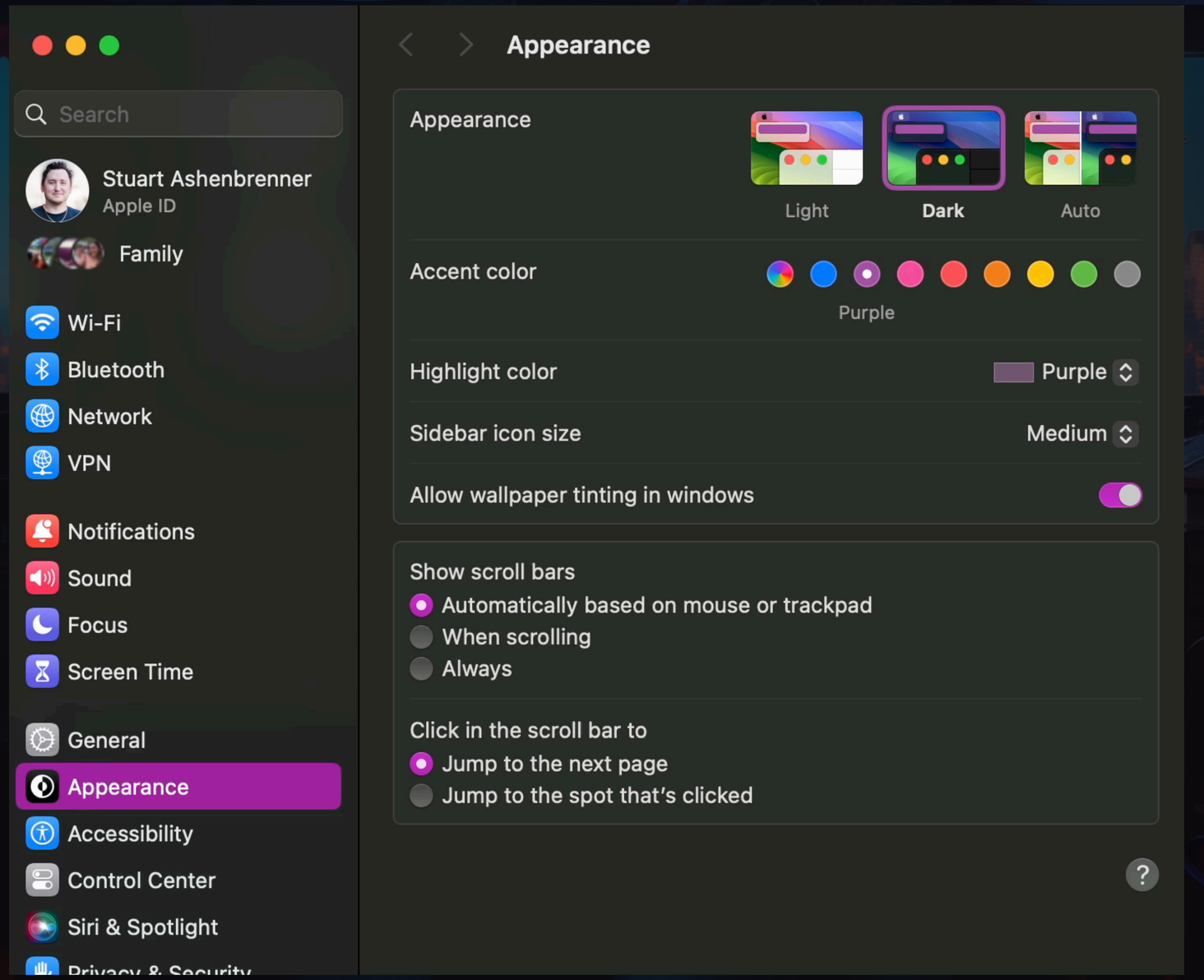
- Apple Developer Docs

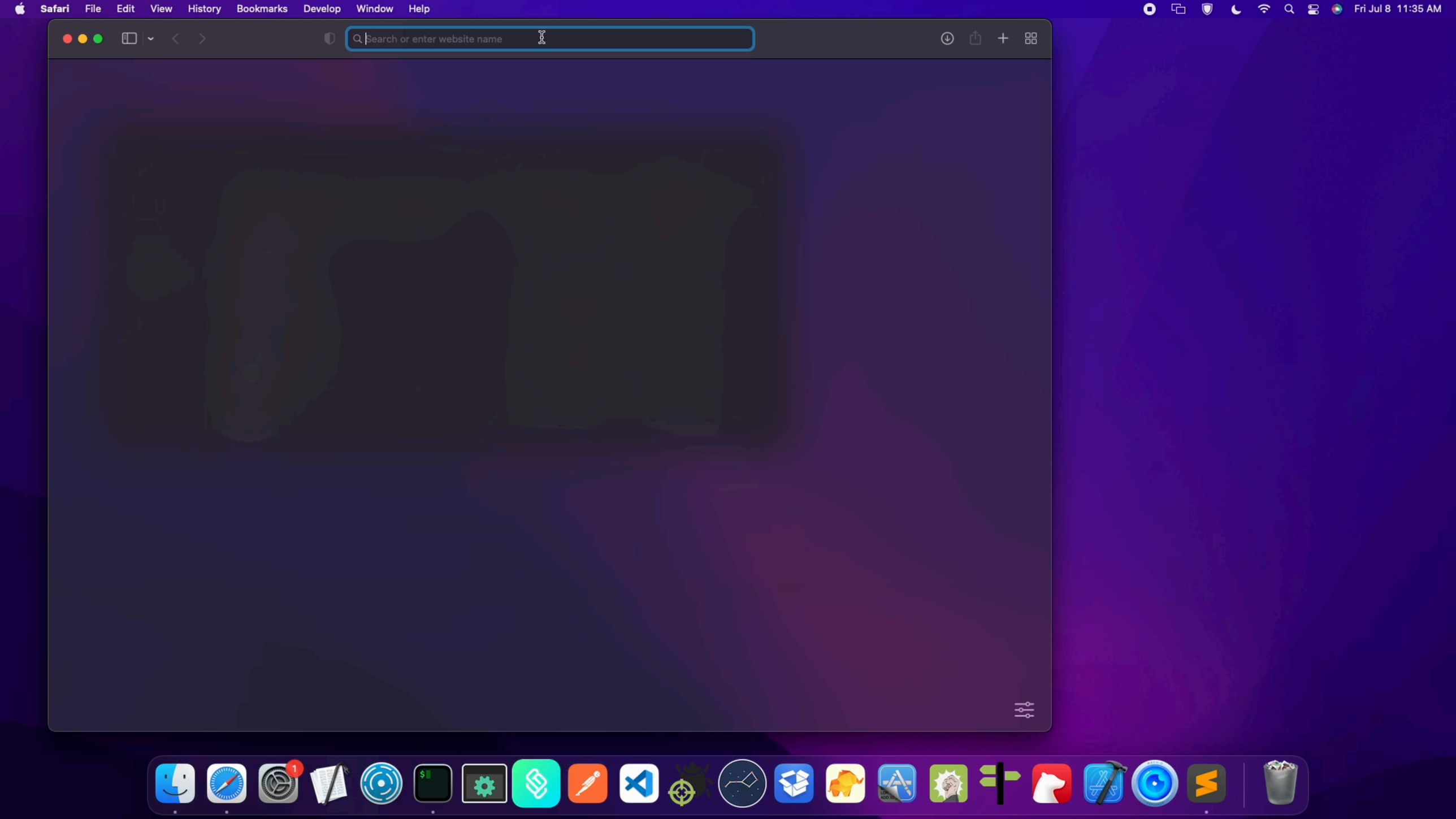
NOTARIZATION



NOTARIZATION

GATEKEEPER OVERRIDE




Safari File Edit View History Bookmarks Develop Window Help
Fri Jul 8 11:35 AM
Search or enter website name

GATEKEEPER


"MachOView" Not Opened
Apple could not verify "MachOView" is free of malware that may harm your Mac or compromise your privacy.
Done
Move to Trash

GATEKEEPER


Search
Stuart Ashenbrenner
Apple Account
Family
Wi-Fi
Bluetooth
Network
VPN
Battery
General
Accessibility
Appearance
Apple Intelligence & Siri
Control Center
Desktop & Dock
Displays
Screen Saver
Spotlight
General
Manage your overall setup and preferences for Mac, such as software updates, device language, AirDrop, and more.
About
Software Update
Storage
AppleCare & Warranty
AirDrop & Handoff
AutoFill & Passwords
Date & Time
Language & Region

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

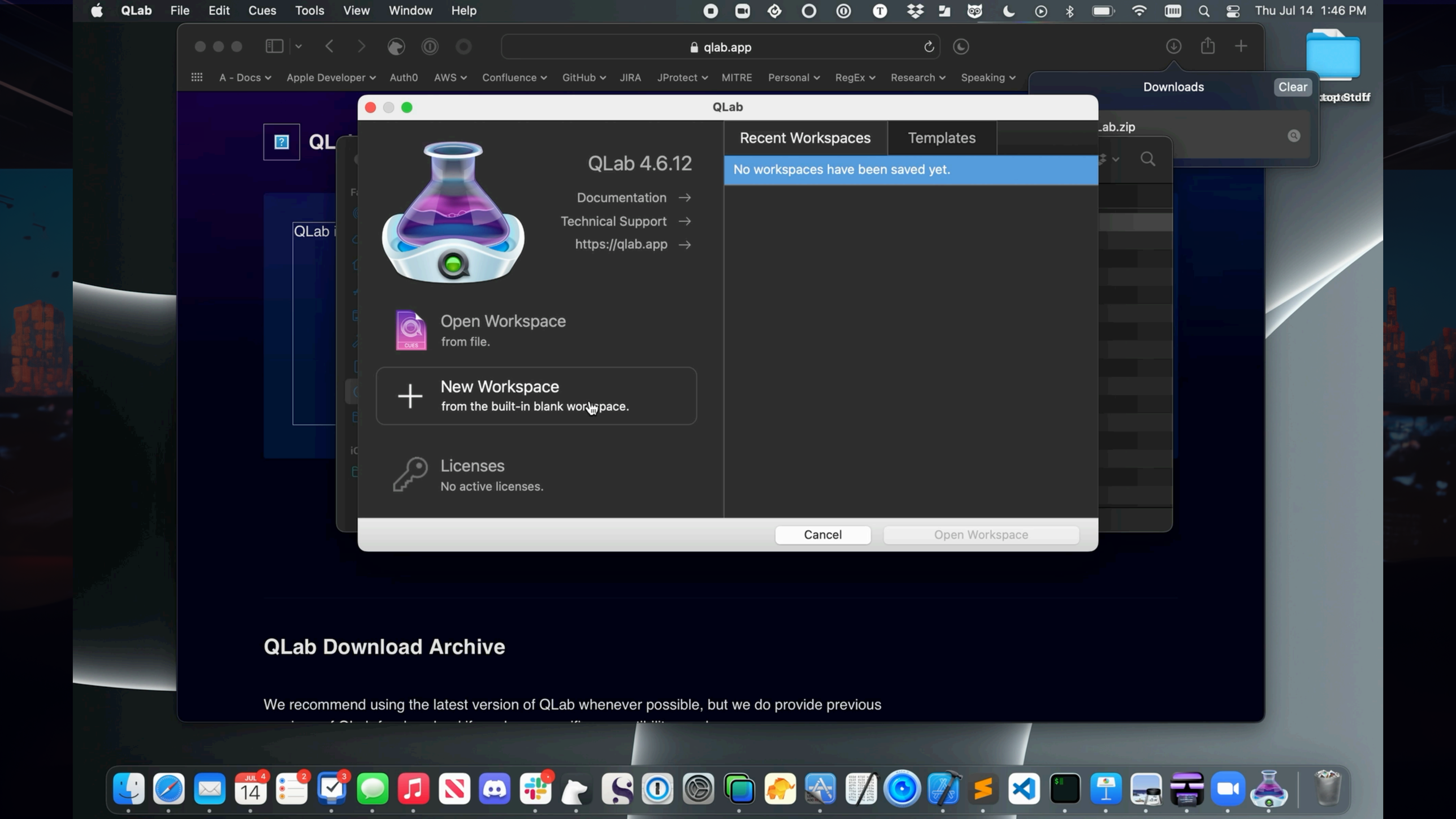
XPR

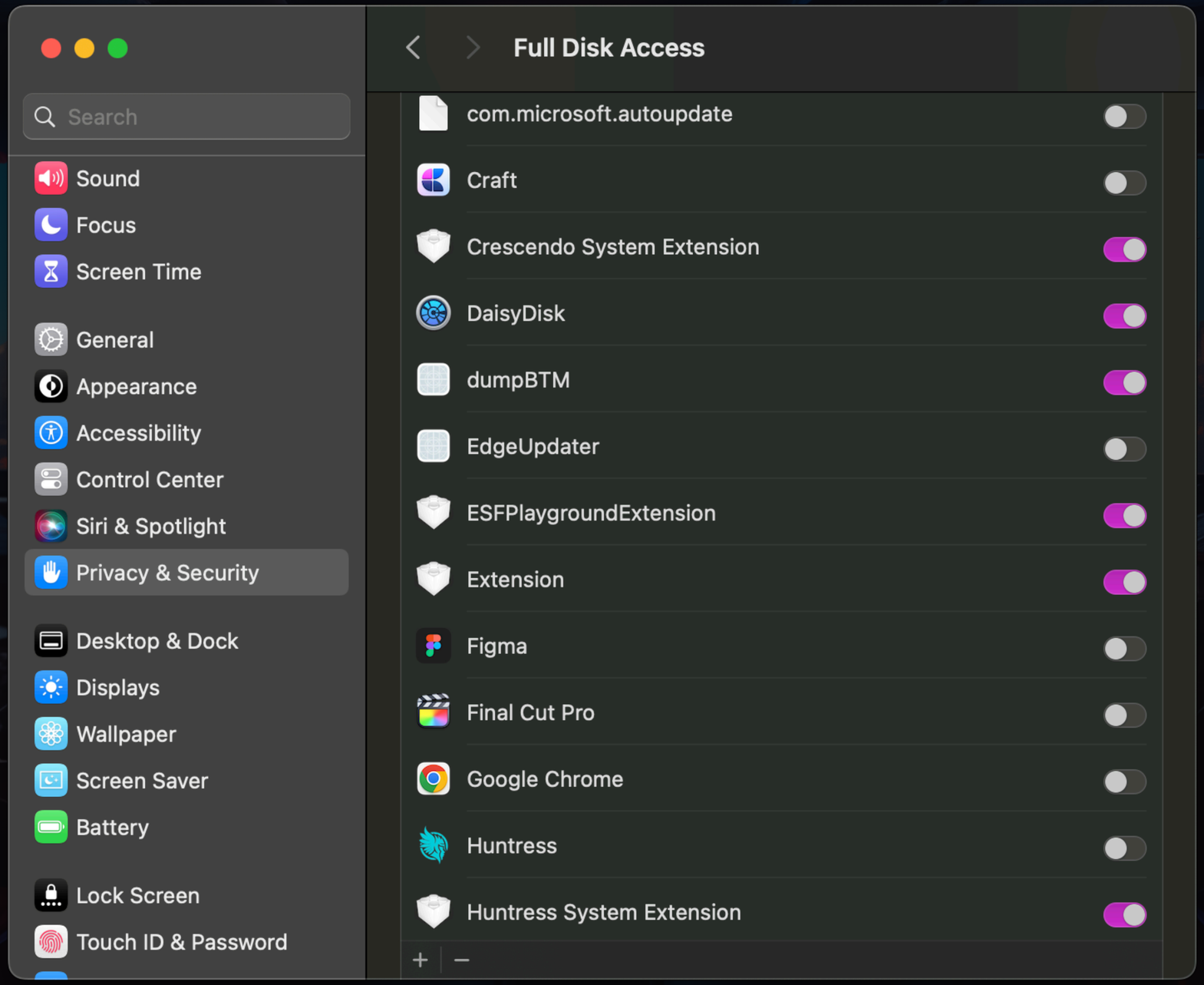

TCC

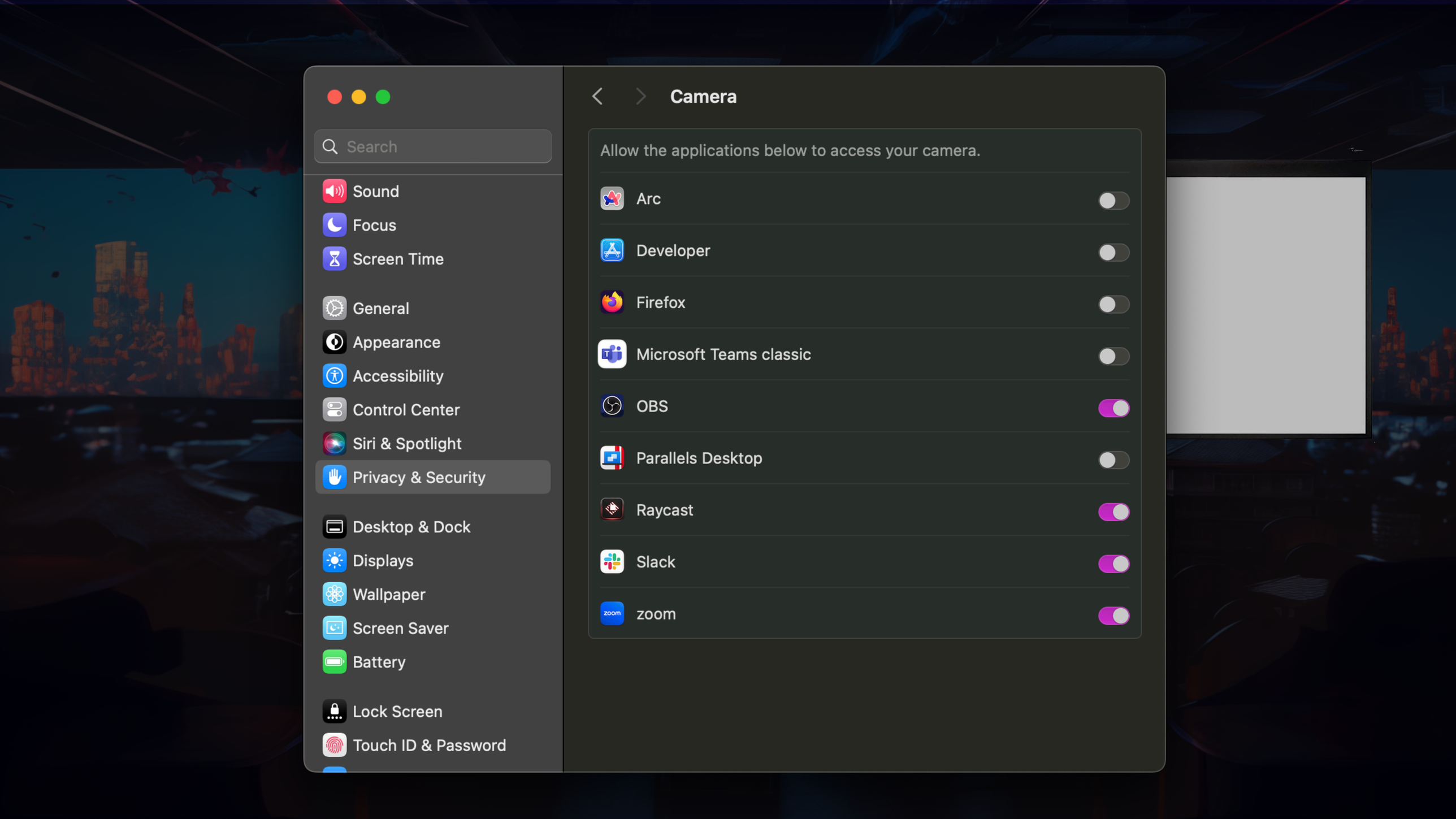

TRANSPARENCY
CONSENT
CONTROL

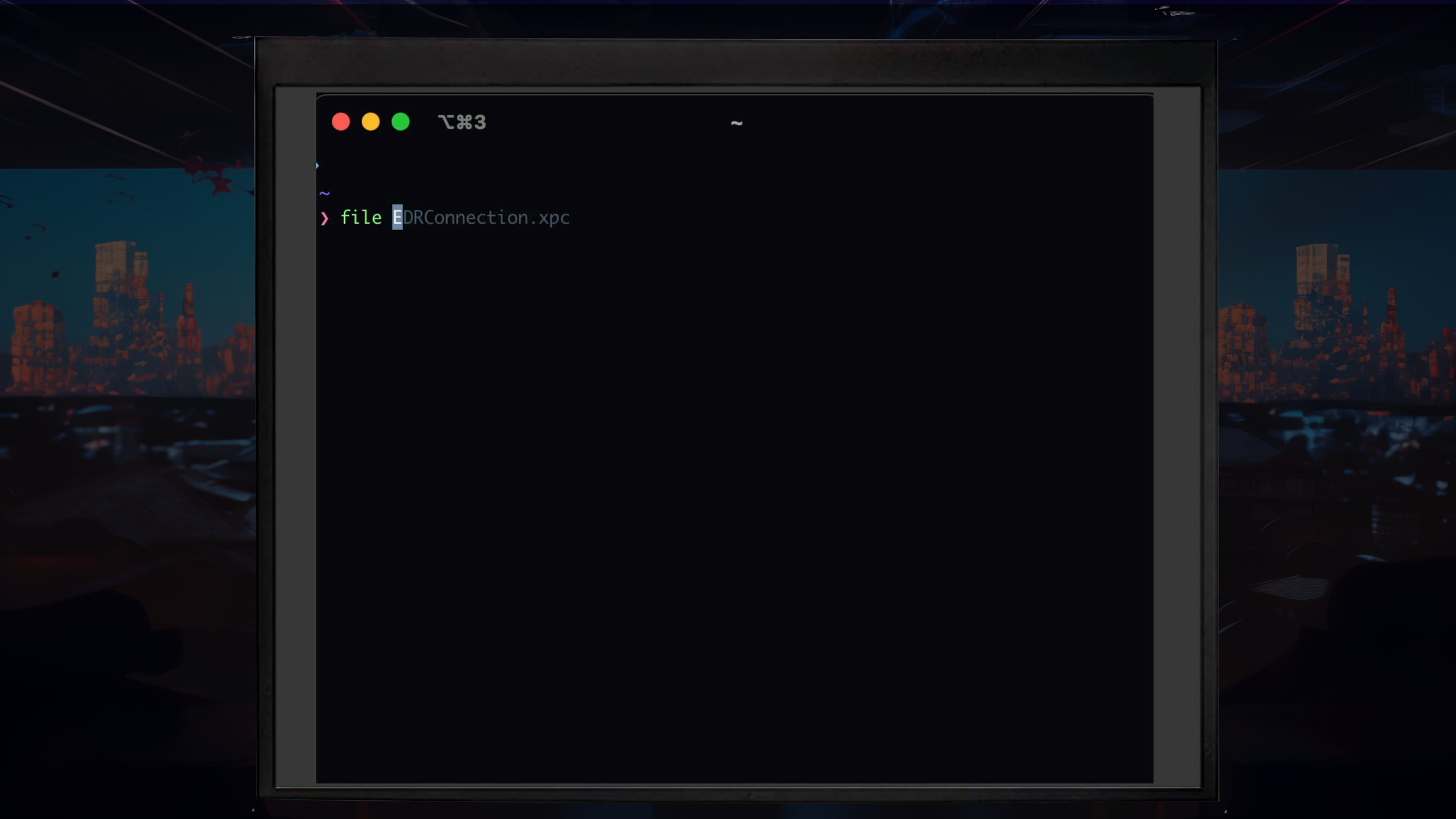
TCC

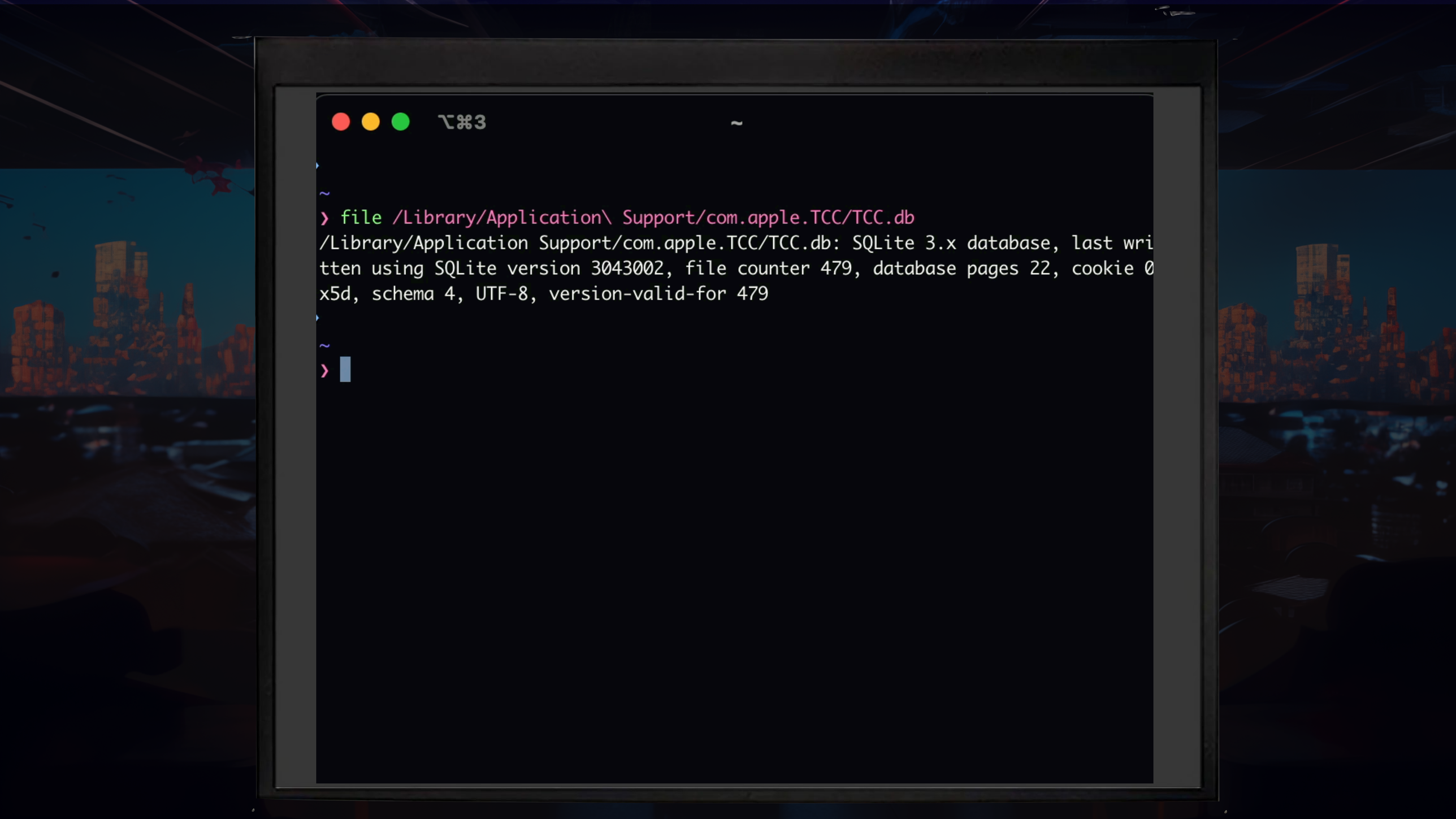
A framework for regulating applications permissions by managing their access to user data

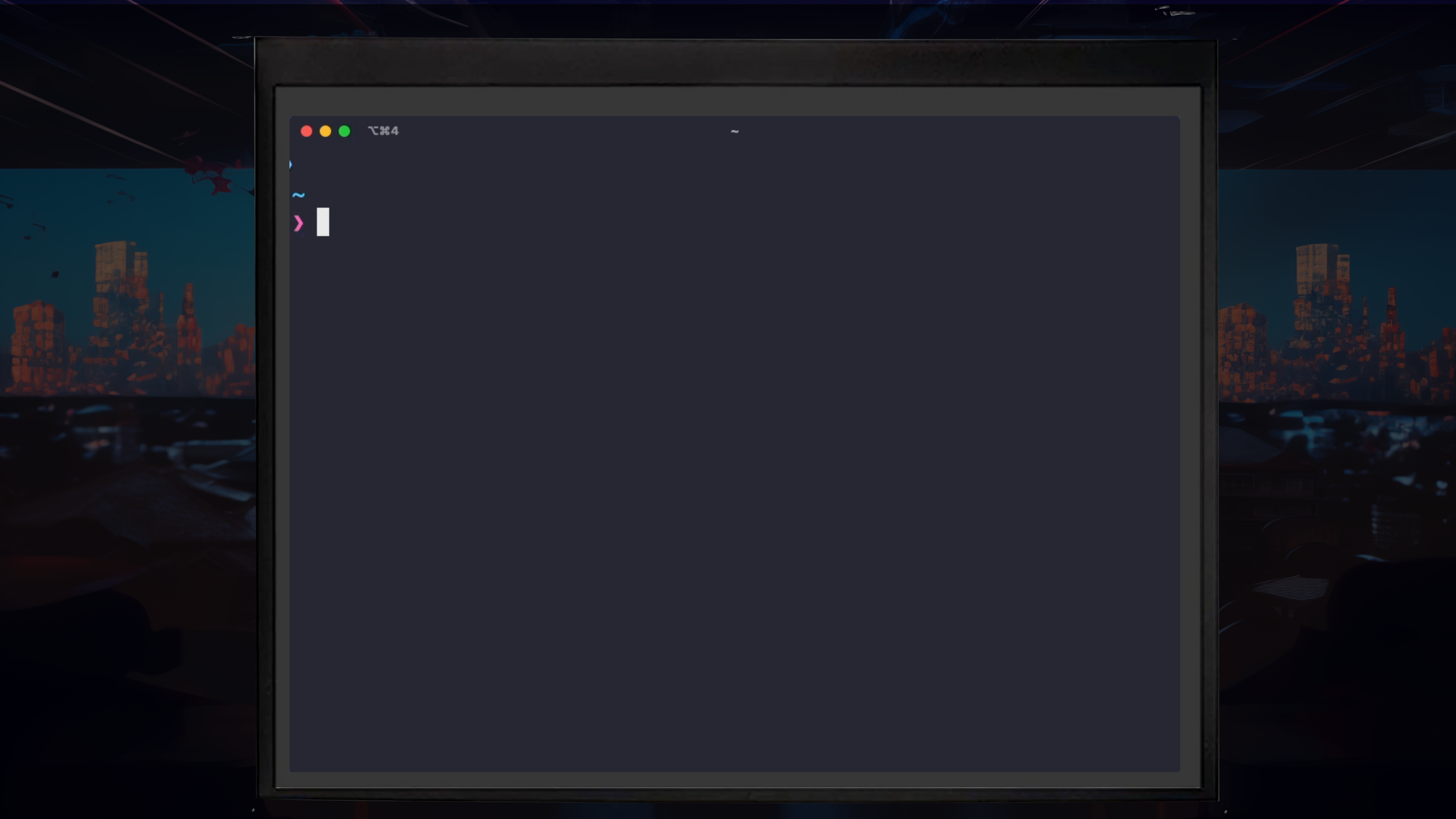

QLab File Edit Cues Tools View Window Help
Thu Jul 14 1:46 PM
qlab.app
A - Docs
Apple Developer
Auth0
AWS
Confluence
GitHub
JIRA
JProtect
MITRE
Personal
RegEx
Research
Speaking
Downloads
Clear
QLab
QLab 4.6.12
Documentation
Technical Support
https://qlab.app
Recent Workspaces
Templates
No workspaces have been saved yet.
Open Workspace
from file.
New Workspace
from the built-in blank workspace.
Licenses
No active licenses.
Cancel
Open Workspace
QLab Download Archive
We recommend using the latest version of QLab whenever possible, but we do provide previous


Search
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Security
Desktop & Dock
Displays
Wallpaper
Screen Saver
Battery
Lock Screen
Touch ID & Password
Full Disk Access
com.microsoft.autoupdate
Craft
Crescendo System Extension
DaisyDisk
dumpBTM
EdgeUpdater
ESFPlaygroundExtension
Extension
Figma
Final Cut Pro
Google Chrome
Huntress
Huntress System Extension


Search
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Security
Desktop & Dock
Displays
Wallpaper
Screen Saver
Battery
Lock Screen
Touch ID & Password
Camera
Allow the applications below to access your camera.
Arc
Developer
Firefox
Microsoft Teams classic
OBS
Parallels Desktop
Raycast
Slack
zoom


⌥⌘3
~
~
❯ file EDRConnection.xpc


⌥⌘3
~
~
❯ file /Library/Application\ Support/com.apple.TCC/TCC.db
/Library/Application Support/com.apple.TCC/TCC.db: SQLite 3.x database, last wri
tten using SQLite version 3043002, file counter 479, database pages 22, cookie 0
x5d, schema 4, UTF-8, version-valid-for 479
~
❯


⌥⌘4
~
~
❯


com.huntresslabs.www|4|2|kTCCServiceSystemPolicyAllFiles

| 4 | 2 | kTCCServiceSystemPolicyAllFiles

```
enum TCCAuthReason: String, CaseIterable {
        case error = "1"
        case userConsent = "2"
        case userSet = "3"
        case systemSet = "4"
        case servicePolicy = "5"
        case mdmPolicy = "6"
        case overridePolicy = "7"
        case missingUsageString = "8"
        case promptTimeout = "9"
        case preflightUnknown = "10"
        case entitled = "11"
        case appTypePolicy = "12"
 }
```

| kTCCServiceSystemPolicyAllFiles

```
enum TCCAuthValue: String, CaseIterable {
        case denied = "0"
        case unknown = "1"
        case allowed = "2"
        case limited = "3"
        case addOnly = "4"
        case singleBootAllowed = "5" // allowed for a unique boot_uuid
}
```

```
enum TCCService: String, CaseIterable {
    // critical
    case location = "kTCCServiceLiverpool"
    case icloud = "kTCCServiceUbiquity"
    case sharing = "kTCCServiceShareKit"
    case fda = "kTCCServiceSystemPolicyAllFiles"

    // common
    case accessibility = "kTCCServiceAccessibility"
    case keystrokes = "kTCCServicePostEvent"
    case inputMonitoring = "kTCCServiceListenEvent"
    case developerTools = "kTCCServiceDeveloperTool"
    case screenCapture = "kTCCServiceScreenCapture"
```


TCC


TCC
MDM


TCC
MDM

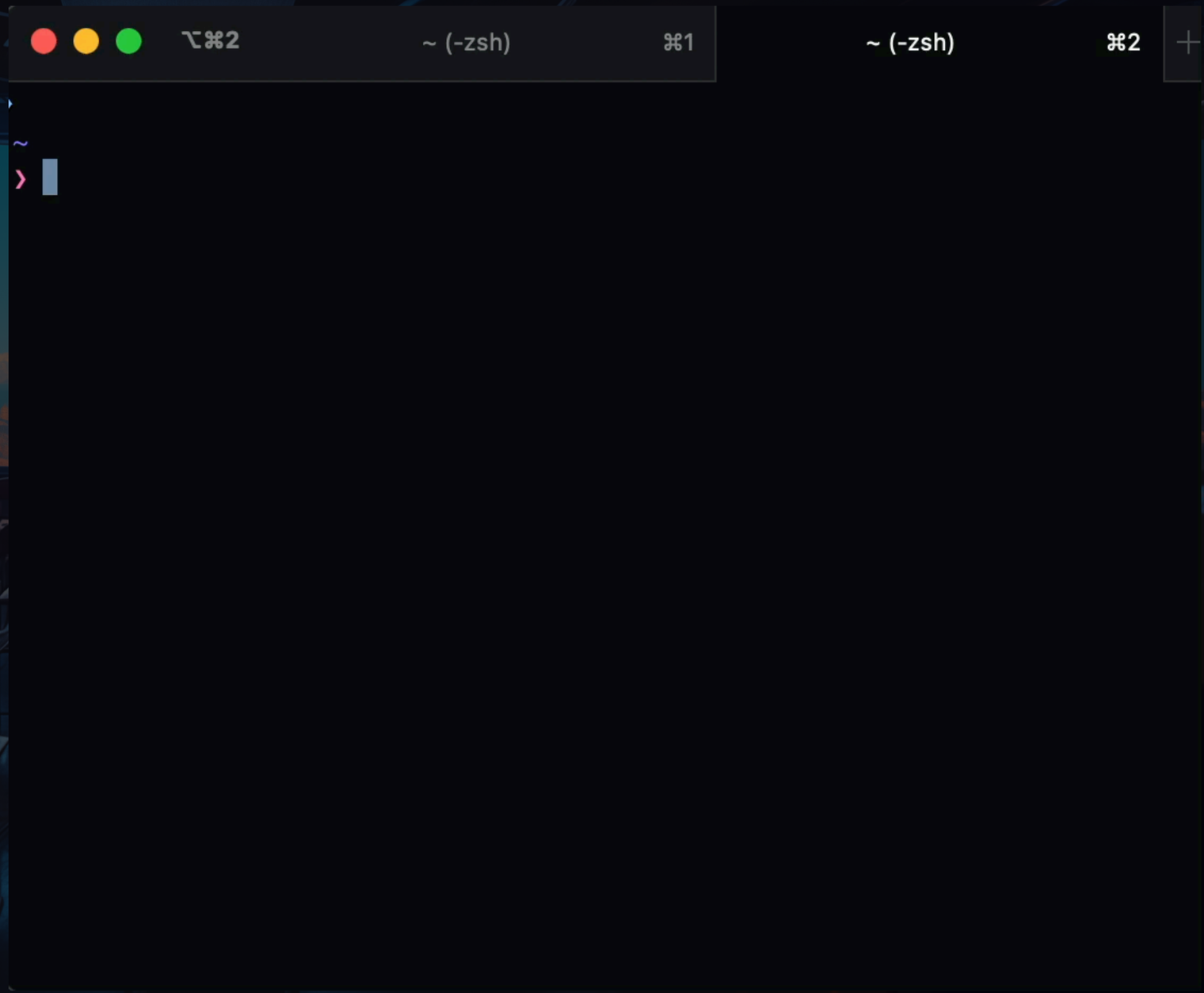

MDM

MDMOverrides

- /Library/Application Support/com.apple.TCC/MDMOverrides.plist

- Not reflected in the System Settings UI

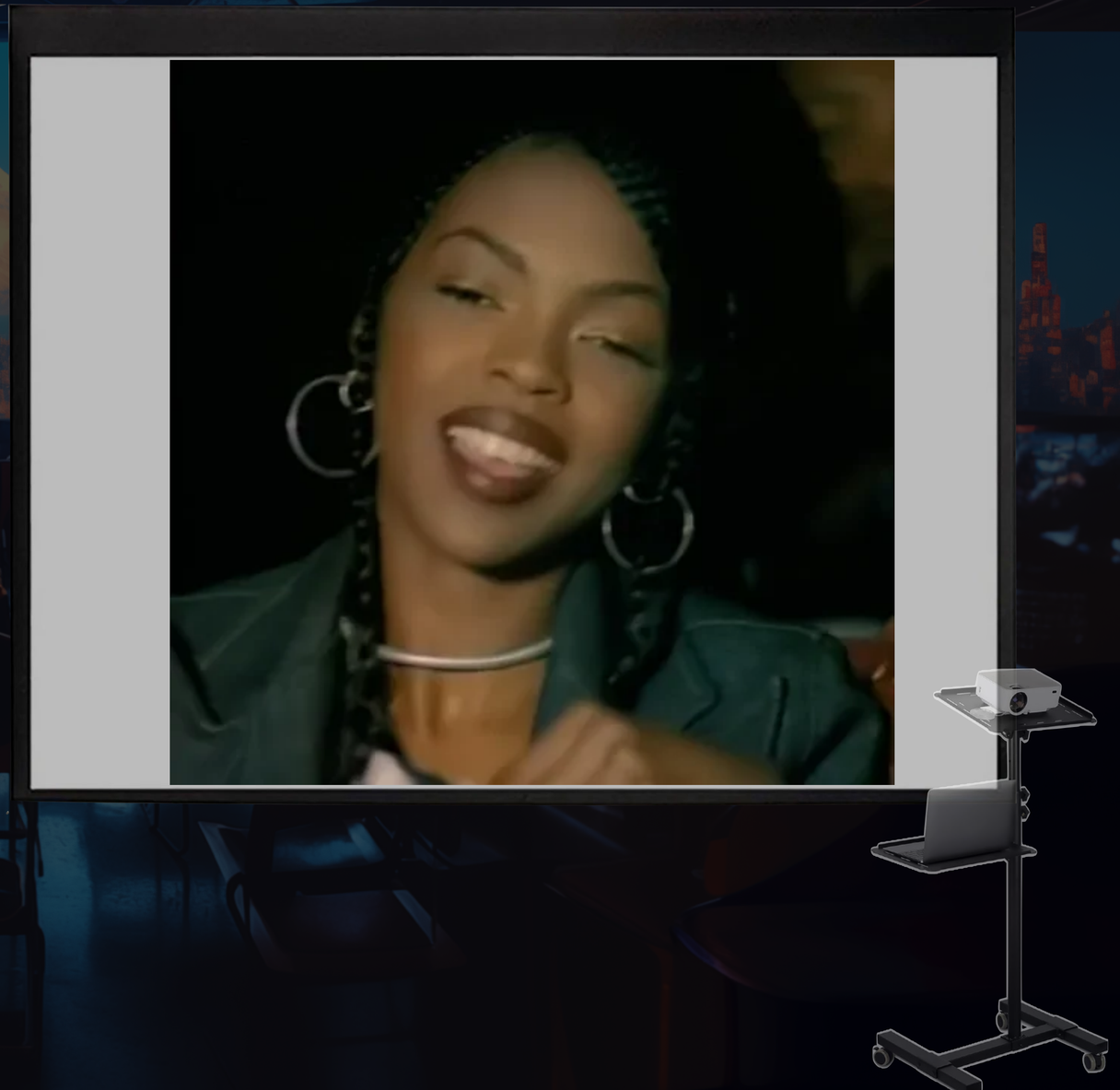
- Not ideal for debugging deployment issues



Headache

- Great for privacy, tough on admin experience

Mac 🤝 Windows



Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

Syllabus

FILE QUARANTINE

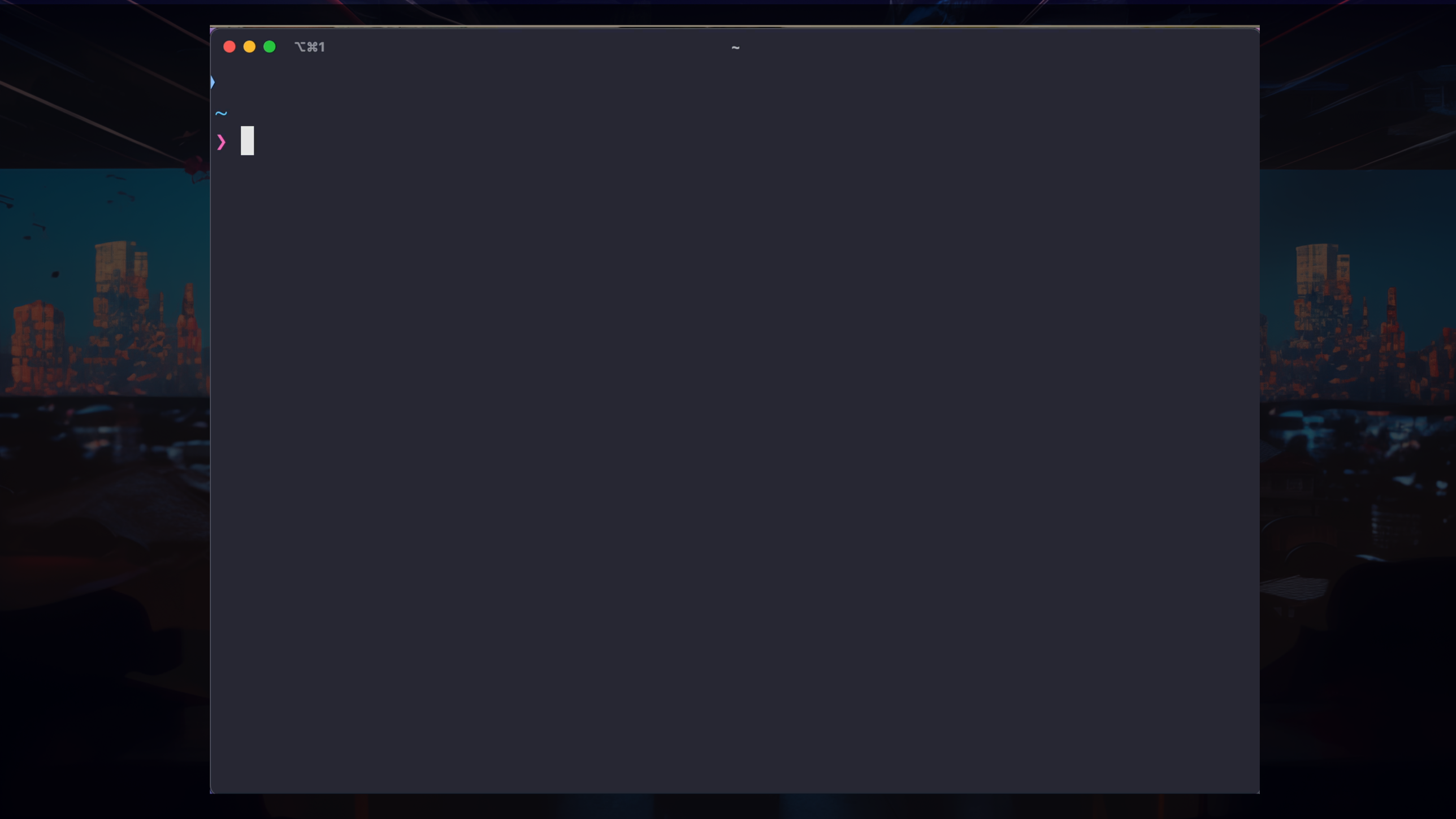
GATEKEEPER

TCC

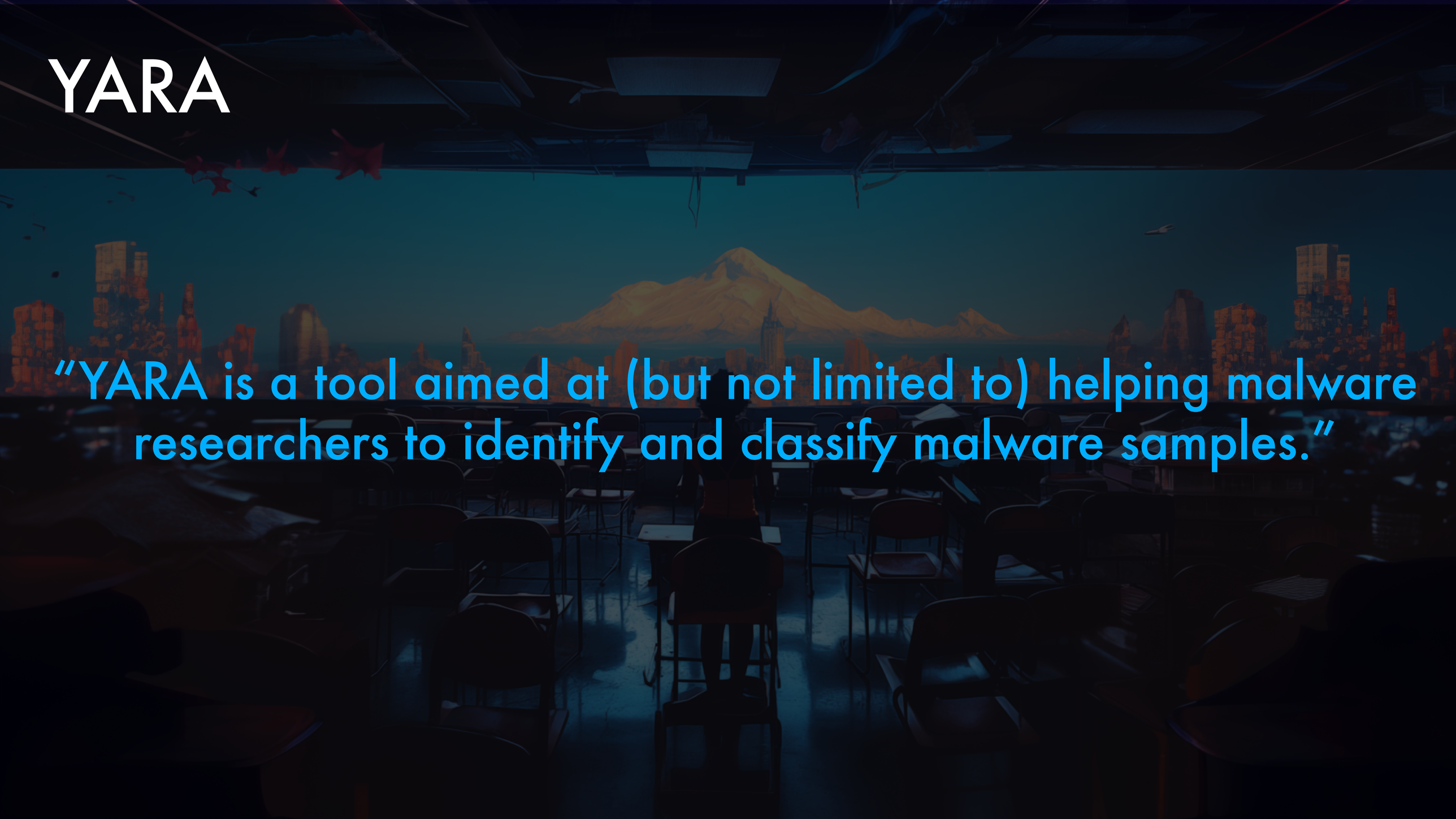
XPROTECT

XPR


XPROTECT

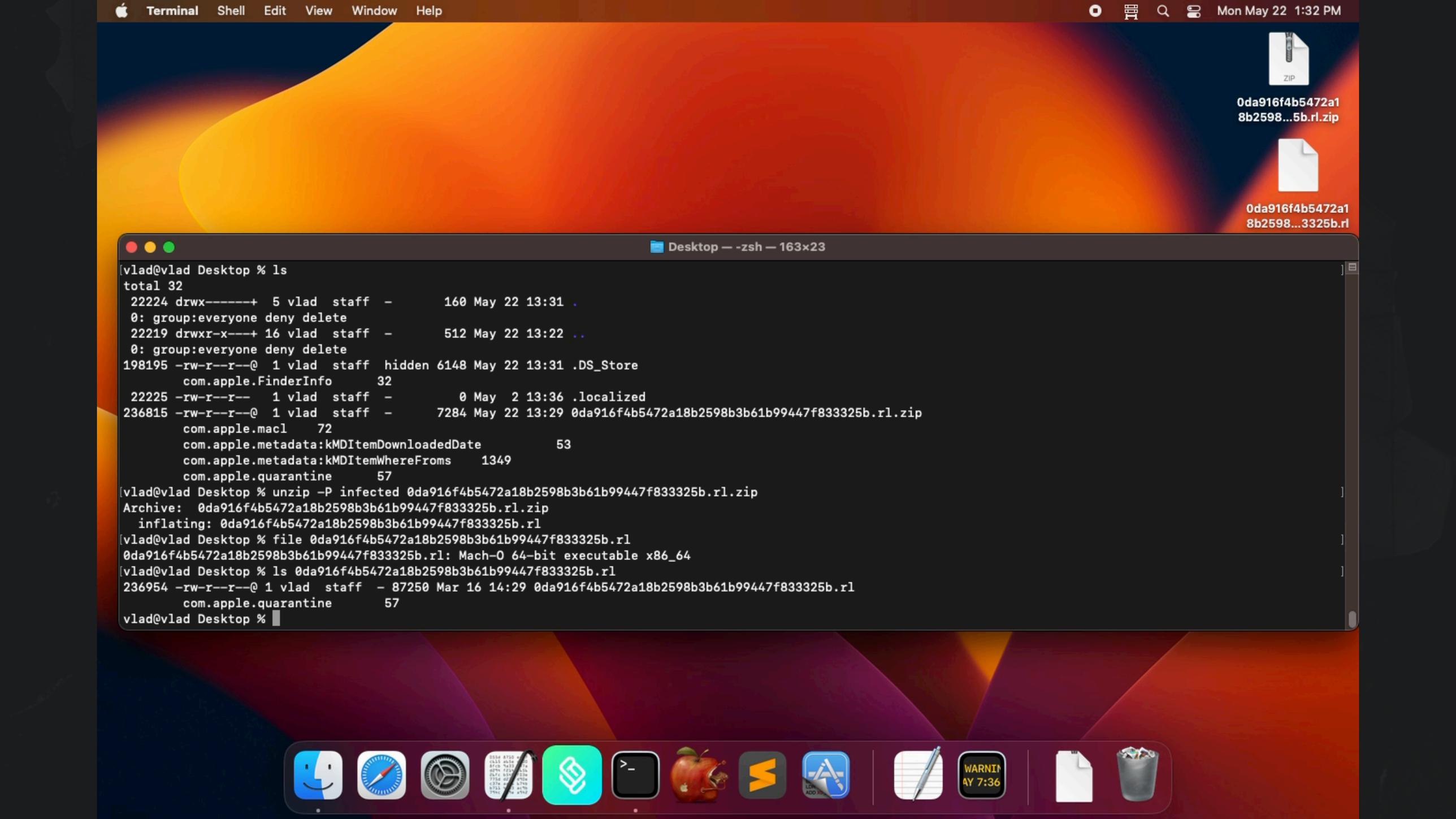

⌥⌘1
~
~
❯

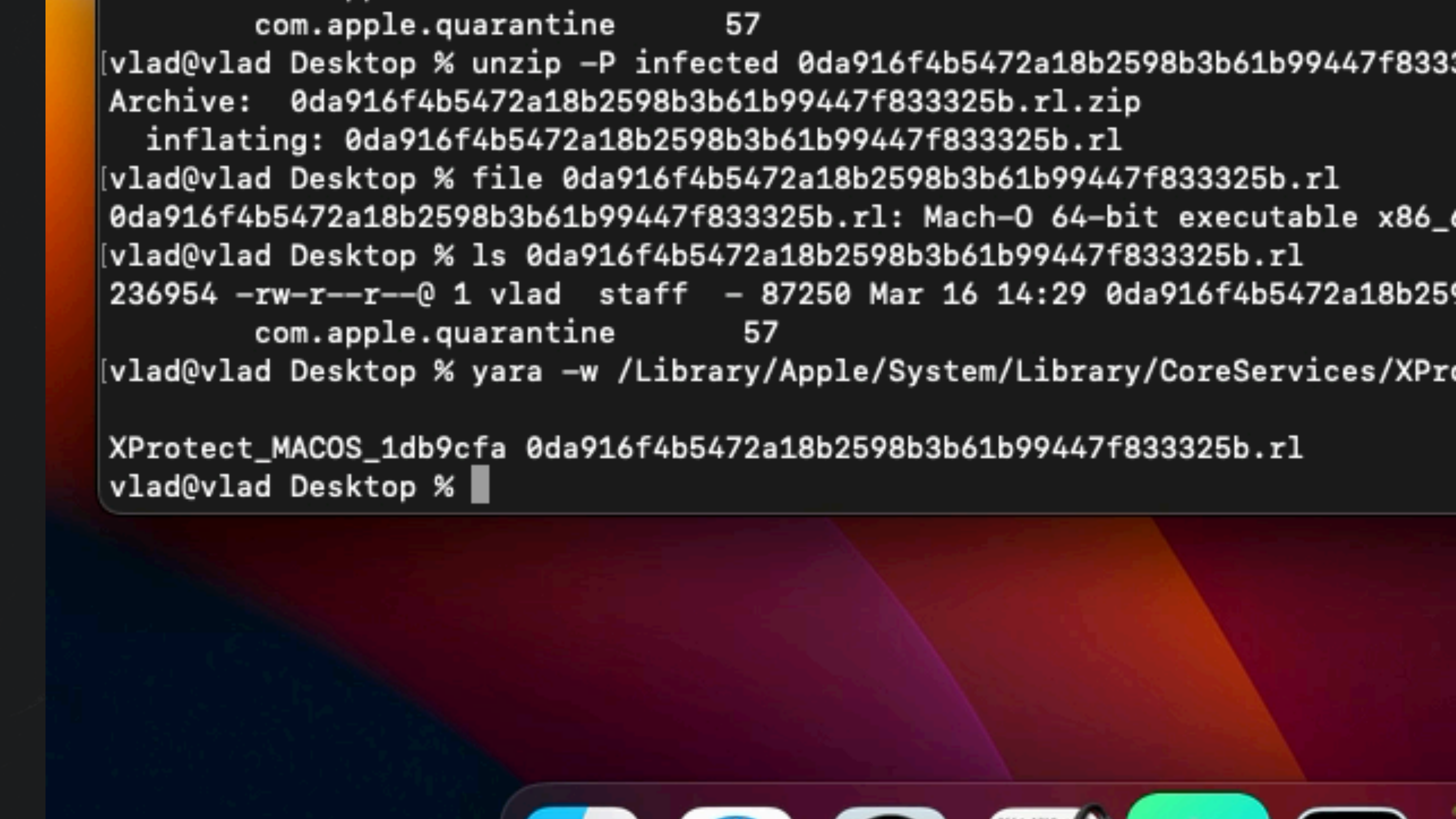
YARA

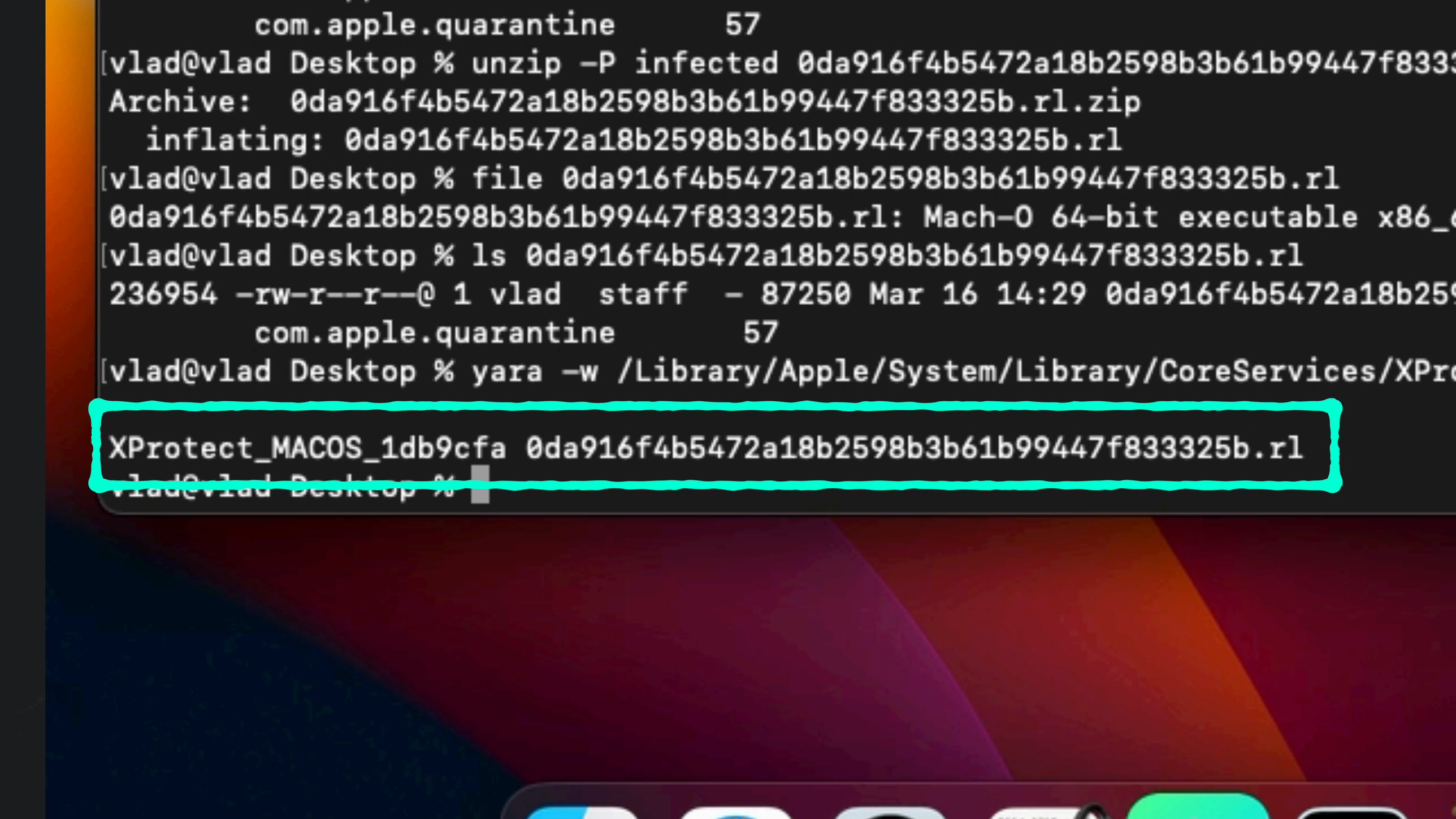


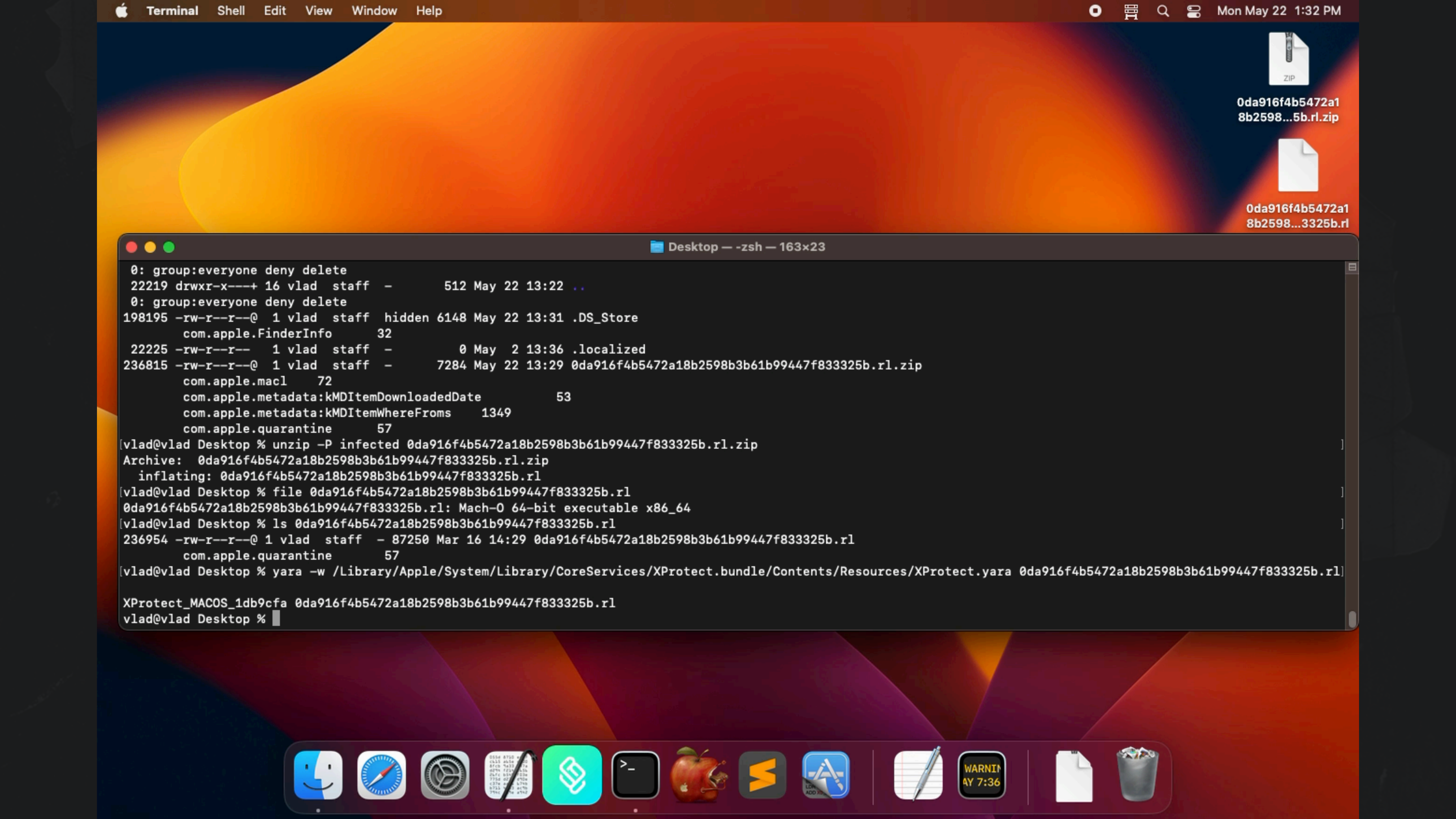
"YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples."

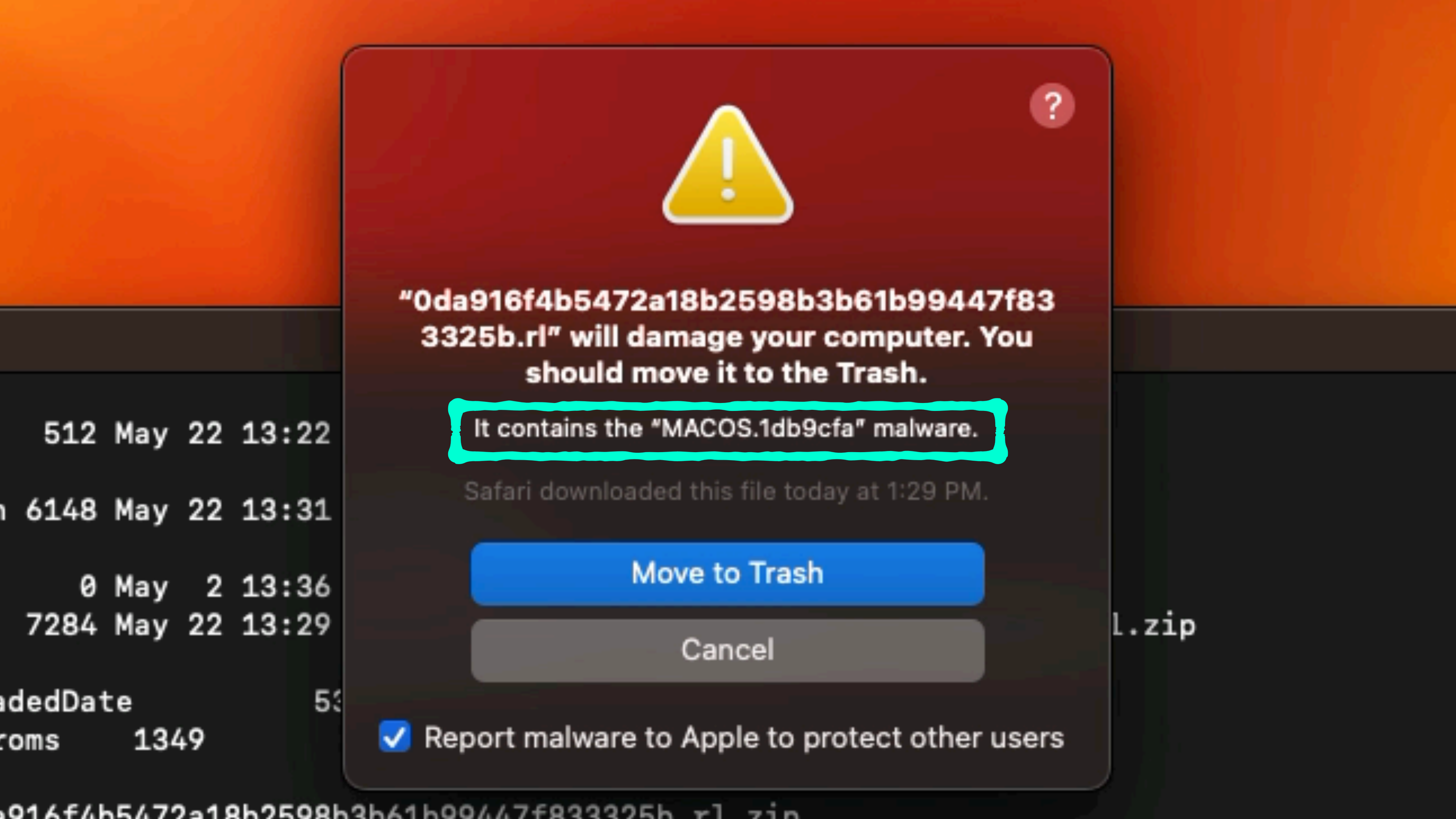

/Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources
❯ cat XProtect.yara | grep -i "rule" | wc -l
379

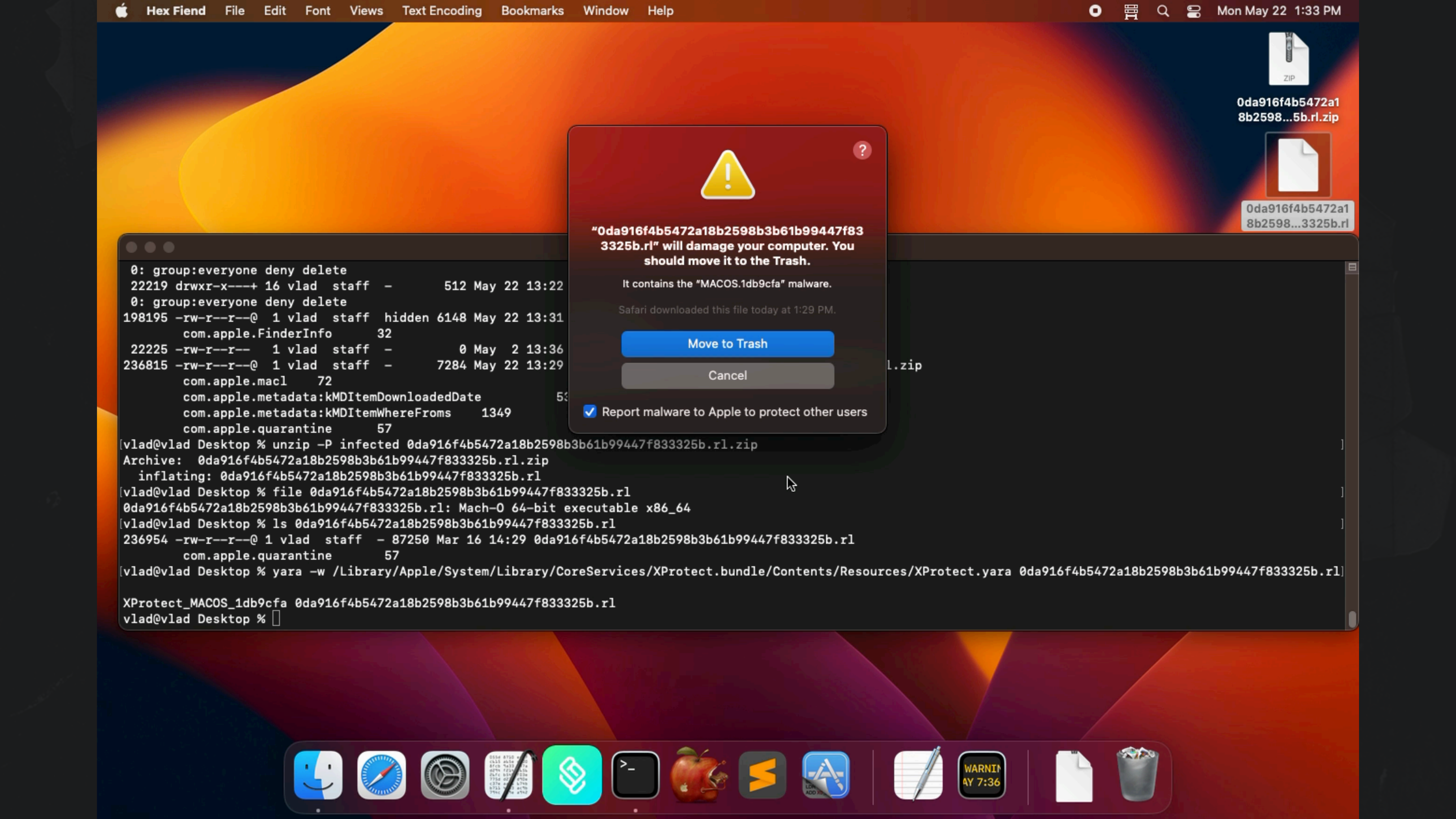

Terminal Shell Edit View Window Help
Mon May 22 1:32 PM
0da916f4b5472a1
8b2598...5b.rl.zip
0da916f4b5472a1
8b2598...3325b.rl
Desktop — -zsh — 163×23
vlad@vlad Desktop % ls
total 32
22224 drwx------+ 5 vlad staff - 160 May 22 13:31 .
0: group:everyone deny delete
22219 drwxr-x---+ 16 vlad staff - 512 May 22 13:22 ..
0: group:everyone deny delete
198195 -rw-r--r--@ 1 vlad staff hidden 6148 May 22 13:31 .DS_Store
com.apple.FinderInfo 32
22225 -rw-r--r-- 1 vlad staff - 0 May 2 13:36 .localized
236815 -rw-r--r--@ 1 vlad staff - 7284 May 22 13:29 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
com.apple.macl 72
com.apple.metadata:kMDItemDownloadedDate 53
com.apple.metadata:kMDItemWhereFroms 1349
com.apple.quarantine 57
vlad@vlad Desktop % unzip -P infected 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
Archive: 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
inflating: 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop % file 0da916f4b5472a18b2598b3b61b99447f833325b.rl
0da916f4b5472a18b2598b3b61b99447f833325b.rl: Mach-O 64-bit executable x86_64
vlad@vlad Desktop % ls 0da916f4b5472a18b2598b3b61b99447f833325b.rl
236954 -rw-r--r--@ 1 vlad staff - 87250 Mar 16 14:29 0da916f4b5472a18b2598b3b61b99447f833325b.rl
com.apple.quarantine 57
vlad@vlad Desktop %

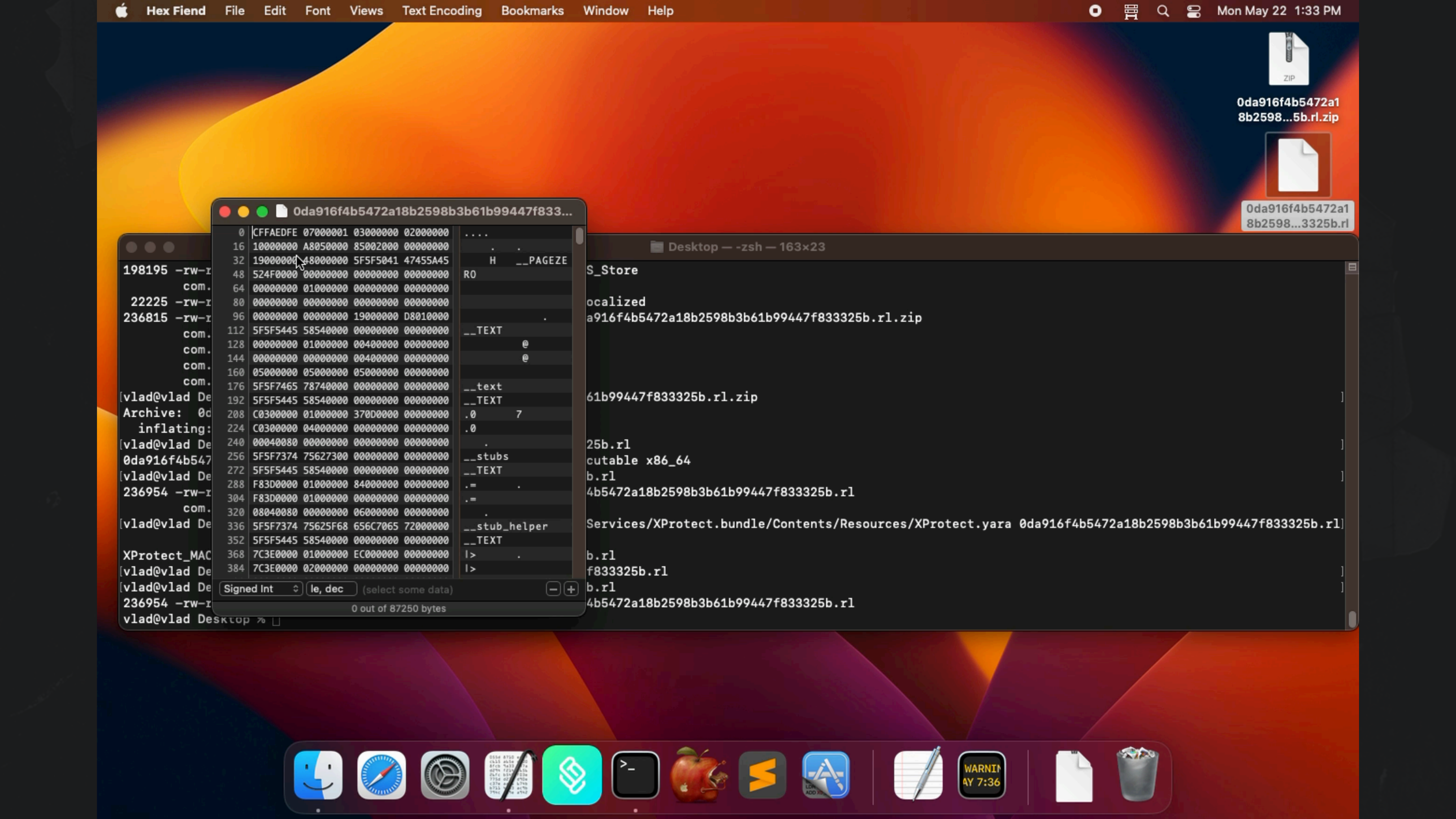

com.apple.quarantine 57
vlad@vlad Desktop % unzip -P infected 0da916f4b5472a18b2598b3b61b99447f833
Archive: 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
inflating: 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop % file 0da916f4b5472a18b2598b3b61b99447f833325b.rl
0da916f4b5472a18b2598b3b61b99447f833325b.rl: Mach-O 64-bit executable x86_
vlad@vlad Desktop % ls 0da916f4b5472a18b2598b3b61b99447f833325b.rl
236954 -rw-r--r--@ 1 vlad staff - 87250 Mar 16 14:29 0da916f4b5472a18b25
com.apple.quarantine 57
vlad@vlad Desktop % yara -w /Library/Apple/System/Library/CoreServices/XPr
XProtect_MACOS_1db9cfa 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop %


com.apple.quarantine 57
vlad@vlad Desktop % unzip -P infected 0da916f4b5472a18b2598b3b61b99447f833
Archive: 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
inflating: 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop % file 0da916f4b5472a18b2598b3b61b99447f833325b.rl
0da916f4b5472a18b2598b3b61b99447f833325b.rl: Mach-O 64-bit executable x86_
vlad@vlad Desktop % ls 0da916f4b5472a18b2598b3b61b99447f833325b.rl
236954 -rw-r--r--@ 1 vlad staff - 87250 Mar 16 14:29 0da916f4b5472a18b25
com.apple.quarantine 57
vlad@vlad Desktop % yara -w /Library/Apple/System/Library/CoreServices/XPr
XProtect_MACOS_1db9cfa 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop %


Terminal Shell Edit View Window Help
Mon May 22 1:32 PM
0da916f4b5472a18b2598...5b.rl.zip
0da916f4b5472a18b2598...3325b.rl
Desktop — -zsh — 163×23
0: group:everyone deny delete
22219 drwxr-x---+ 16 vlad staff - 512 May 22 13:22 ..
0: group:everyone deny delete
198195 -rw-r--r--@ 1 vlad staff hidden 6148 May 22 13:31 .DS_Store
com.apple.FinderInfo 32
22225 -rw-r--r-- 1 vlad staff - 0 May 2 13:36 .localized
236815 -rw-r--r--@ 1 vlad staff - 7284 May 22 13:29 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
com.apple.macl 72
com.apple.metadata:kMDItemDownloadedDate 53
com.apple.metadata:kMDItemWhereFroms 1349
com.apple.quarantine 57
vlad@vlad Desktop % unzip -P infected 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
Archive: 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
inflating: 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop % file 0da916f4b5472a18b2598b3b61b99447f833325b.rl
0da916f4b5472a18b2598b3b61b99447f833325b.rl: Mach-O 64-bit executable x86_64
vlad@vlad Desktop % ls 0da916f4b5472a18b2598b3b61b99447f833325b.rl
236954 -rw-r--r--@ 1 vlad staff - 87250 Mar 16 14:29 0da916f4b5472a18b2598b3b61b99447f833325b.rl
com.apple.quarantine 57
vlad@vlad Desktop % yara -w /Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources/XProtect.yara 0da916f4b5472a18b2598b3b61b99447f833325b.rl
XProtect_MACOS_1db9cfa 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop %


"0da916f4b5472a18b2598b3b61b99447f833325b.rl" will damage your computer. You should move it to the Trash.
It contains the "MACOS.1db9cfa" malware.
Safari downloaded this file today at 1:29 PM.
Move to Trash
Cancel
Report malware to Apple to protect other users
512 May 22 13:22
6148 May 22 13:31
0 May 2 13:36
7284 May 22 13:29
l.zip
adedDate
roms 1349


Hex Fiend File Edit Font Views Text Encoding Bookmarks Window Help
Mon May 22 1:33 PM
0da916f4b5472a18b2598...5b.rl.zip
0da916f4b5472a18b2598...3325b.rl
"0da916f4b5472a18b2598b3b61b99447f833325b.rl" will damage your computer. You should move it to the Trash.
It contains the "MACOS.1db9cfa" malware.
Safari downloaded this file today at 1:29 PM.
Move to Trash
Cancel
Report malware to Apple to protect other users
0: group:everyone deny delete
22219 drwxr-x---+ 16 vlad staff - 512 May 22 13:22
0: group:everyone deny delete
198195 -rw-r--r--@ 1 vlad staff hidden 6148 May 22 13:31
com.apple.FinderInfo 32
22225 -rw-r--r-- 1 vlad staff - 0 May 2 13:36
236815 -rw-r--r--@ 1 vlad staff - 7284 May 22 13:29
com.apple.macl 72
com.apple.metadata:kMDItemDownloadedDate
com.apple.metadata:kMDItemWhereFroms 1349
com.apple.quarantine 57
vlad@vlad Desktop % unzip -P infected 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
Archive: 0da916f4b5472a18b2598b3b61b99447f833325b.rl.zip
inflating: 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop % file 0da916f4b5472a18b2598b3b61b99447f833325b.rl
0da916f4b5472a18b2598b3b61b99447f833325b.rl: Mach-O 64-bit executable x86_64
vlad@vlad Desktop % ls 0da916f4b5472a18b2598b3b61b99447f833325b.rl
236954 -rw-r--r--@ 1 vlad staff - 87250 Mar 16 14:29 0da916f4b5472a18b2598b3b61b99447f833325b.rl
com.apple.quarantine 57
vlad@vlad Desktop % yara -w /Library/Apple/System/Library/CoreServices/XProtect.bundle/Contents/Resources/XProtect.yara 0da916f4b5472a18b2598b3b61b99447f833325b.rl
XProtect_MACOS_1db9cfa 0da916f4b5472a18b2598b3b61b99447f833325b.rl
vlad@vlad Desktop %


Hex Fiend File Edit Font Views Text Encoding Bookmarks Window Help
Mon May 22 1:33 PM
0da916f4b5472a18b2598...5b.rl.zip
0da916f4b5472a18b2598...3325b.rl
0da916f4b5472a18b2598b3b61b99447f833...
0 CFFAEDFE 07000001 03000000 02000000 ....
16 10000000 A8050000 85002000 00000000 . .
32 19000000 48000000 5F5F5041 47455A45 H __PAGEZE
48 524F0000 00000000 00000000 00000000 RO
64 00000000 01000000 00000000 00000000
80 00000000 00000000 00000000 00000000
96 00000000 00000000 19000000 D8010000 .
112 5F5F5445 58540000 00000000 00000000 __TEXT
128 00000000 01000000 00400000 00000000 @
144 00000000 00000000 00400000 00000000 @
160 05000000 05000000 05000000 00000000
176 5F5F7465 78740000 00000000 00000000 __text
192 5F5F5445 58540000 00000000 00000000 __TEXT
208 C0300000 01000000 370D0000 00000000 .0 7
224 C0300000 04000000 00000000 00000000 .0
240 00040080 00000000 00000000 00000000 .
256 5F5F7374 75627300 00000000 00000000 __stubs
272 5F5F5445 58540000 00000000 00000000 __TEXT
288 F83D0000 01000000 84000000 00000000 .= .
304 F83D0000 01000000 00000000 00000000 .=
320 08040080 00000000 06000000 00000000 .
336 5F5F7374 75625F68 656C7065 72000000 __stub_helper
352 5F5F5445 58540000 00000000 00000000 __TEXT
368 7C3E0000 01000000 EC000000 00000000 |> .
384 7C3E0000 02000000 00000000 00000000 |>
Signed Int
le, dec
(select some data)
0 out of 87250 bytes
Desktop — -zsh — 163×23
198195 -rw-r
com.
22225 -rw-r
236815 -rw-r
com.
com.
com.
com.
vlad@vlad De
Archive: 0d
inflating:
vlad@vlad De
0da916f4b547
vlad@vlad De
236954 -rw-r
com.
vlad@vlad De
XProtect_MAC
vlad@vlad De
vlad@vlad De
236954 -rw-r
vlad@vlad Desktop %
S_Store
ocalized
a916f4b5472a18b2598b3b61b99447f833325b.rl.zip
61b99447f833325b.rl.zip
25b.rl
cutable x86_64
b.rl
4b5472a18b2598b3b61b99447f833325b.rl
Services/XProtect.bundle/Contents/Resources/XProtect.yara 0da916f4b5472a18b2598b3b61b99447f833325b.rl
b.rl
f833325b.rl
b.rl
4b5472a18b2598b3b61b99447f833325b.rl


"0da916f4b5472a18b2598b3b61b99447f83
3325b.rl" will damage your computer. You
should move it to the Trash.
This file was downloaded on an unknown date.
Move to Trash
Cancel
Report malware to Apple to protect other users
84 May 22 13:29
l.zip
Date
1349
f4b5472a18b2598
33325b.rl.zip
7f833325b.rl
98b3b61b99447f8
Mach-O 64-bit
b3b61b99447f833325b.rl

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR

Syllabus

FILE QUARANTINE

GATEKEEPER

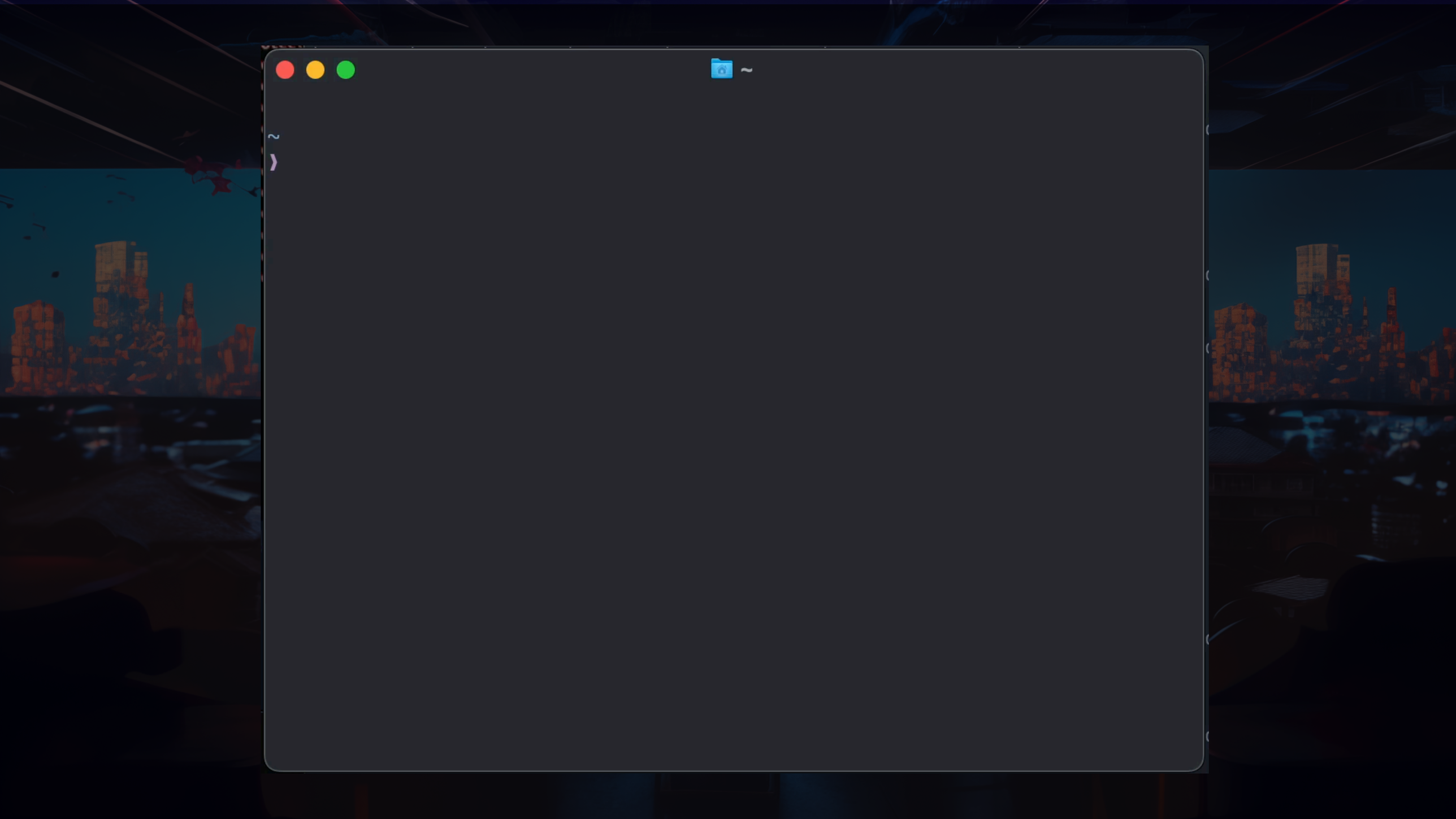
TCC

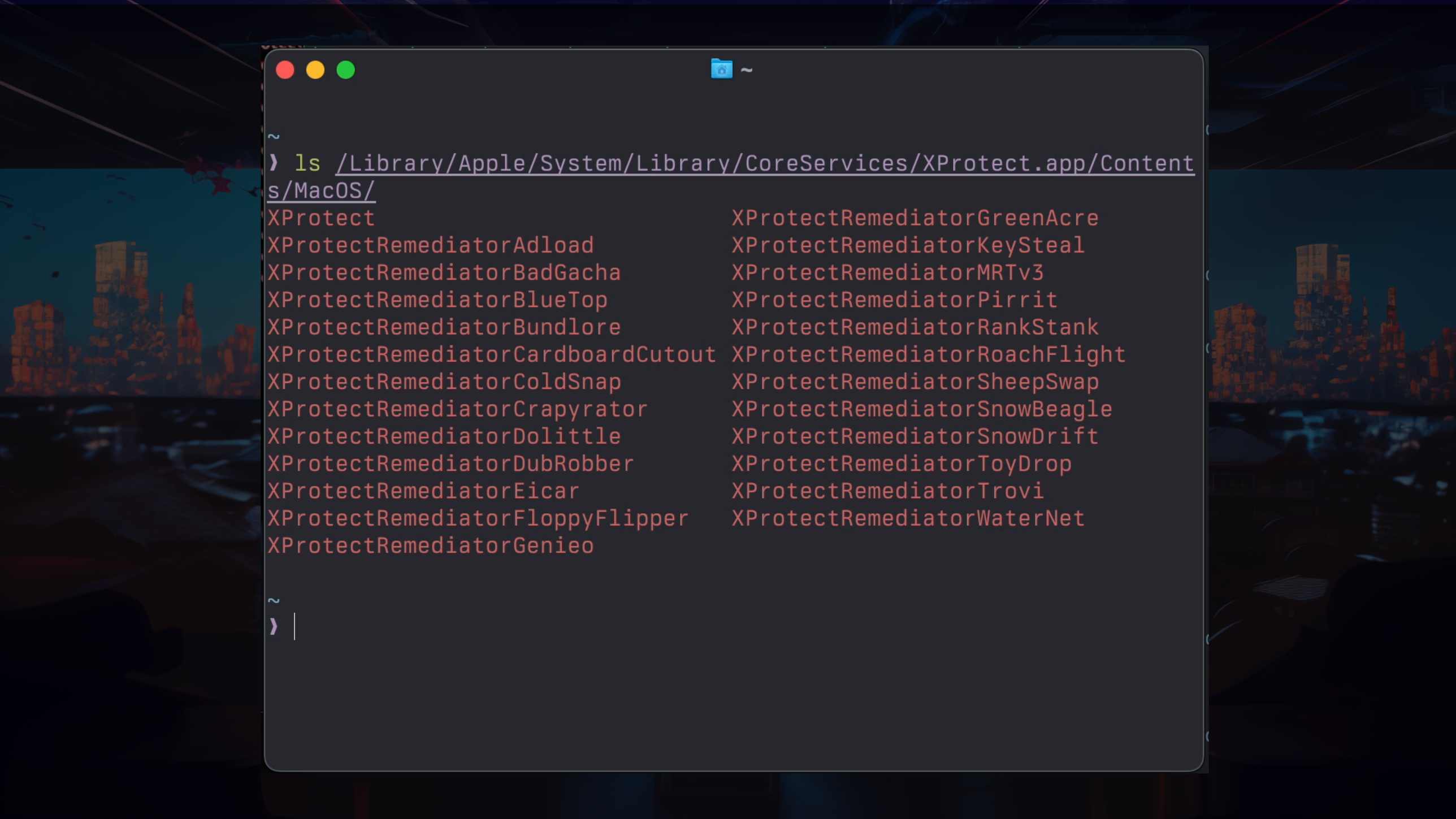
XPROTECT

XPROTECT REMEDIATOR


XPROTECT REMEDIATOR


BASTION




~
❯ ls /Library/Apple/System/Library/CoreServices/XProtect.app/Contents/MacOS/
XProtect
XProtectRemediatorAdload
XProtectRemediatorBadGacha
XProtectRemediatorBlueTop
XProtectRemediatorBundlore
XProtectRemediatorCardboardCutout
XProtectRemediatorColdSnap
XProtectRemediatorCrapyrator
XProtectRemediatorDolittle
XProtectRemediatorDubRobber
XProtectRemediatorEicar
XProtectRemediatorFloppyFlipper
XProtectRemediatorGenieo
XProtectRemediatorGreenAcre
XProtectRemediatorKeySteal
XProtectRemediatorMRTv3
XProtectRemediatorPirrit
XProtectRemediatorRankStank
XProtectRemediatorRoachFlight
XProtectRemediatorSheepSwap
XProtectRemediatorSnowBeagle
XProtectRemediatorSnowDrift
XProtectRemediatorToyDrop
XProtectRemediatorTrovi
XProtectRemediatorWaterNet
~
❯

mod_init_func()

```
1000040a8  void* mod_init_func_0()

1000040ad      void* rax
1000040ad      void* var_18 = rax
1000040ae      rax.b = obj_guard
1000040b6      if (rax.b == 0)
100004115          rax = ___cxa_guard_acquire(&obj_guard)
10000411c          if (rax.d != 0)
10000411e              data_100118ff5 = 1
10000413b              _memcpy(&local_thread_var, &encrypted_str, 0x11f25)
100004151              ___cxa_atexit(func: func, arg: &local_thread_var, dso_handle: &__macho_header)
10000415d              rax = ___cxa_guard_release(&obj_guard)
1000040bf      if (data_100118ff5 != 0)
1000040c1          rax = &local_thread_var
1000040c8          int64_t i = 0
1000040f0          do
1000040df              *rax = *rax ^ (0x383a34303a343600 u>> (i.b & 0x38)).b
1000040e2              i = i + 8
1000040e6              rax = rax + 1
1000040f0          while (i != 0x8f928)
1000040f2          data_100118ff5 = 0
100004100      data_100106c80 = &local_thread_var
10000410d      return rax
```

mod_init_func()

```
rule macos_rankstank
{
    strings:
        $injected_func = "_run_avcodec"
        $xor_decrypt = { 80 b4 04 ?? ?? 00 00 7a }
        $stringA = "%s/.main_storage"
        $stringB = ".session-lock"
        $stringC = "%s/UpdateAgent"
    condition:
        2 of them
}
```

BEHAVIORAL DETECTIONS

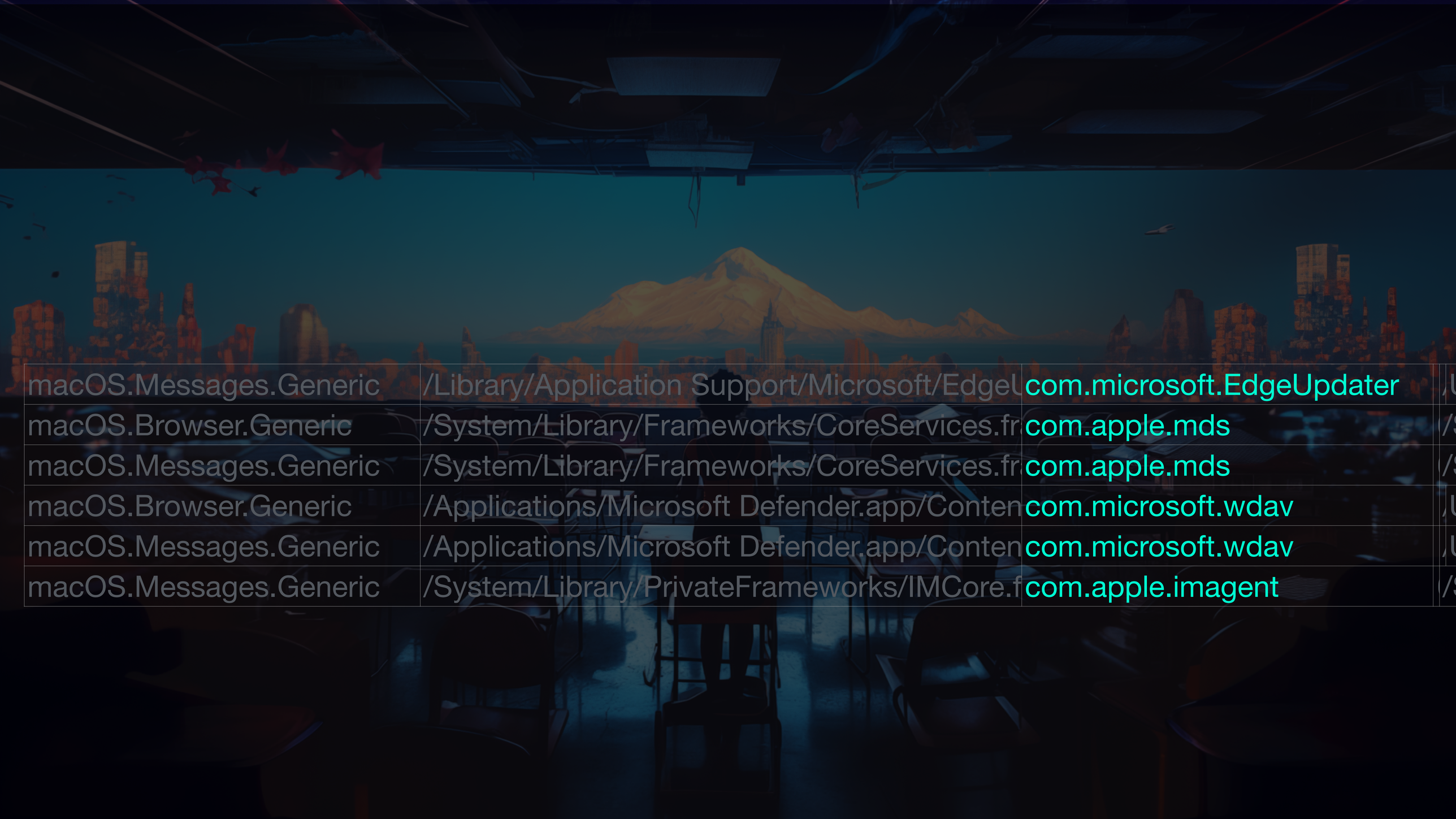
```
/var/protected/xprotect
❯  sudo sqlite3 -header -csv /var/protected/xprotect/XPdb "select * from events;
" > /Users/Shared/XPE.csv
```

BEHAVIO(U)RAL DETECTIONS

macOS.Messages.Generic	/Library/Applic	com.micros	1	/Library/Application Support/Microsoft/EdgeUpd
macOS.Browser.Generic	/System/Librar	com.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Messages.Generic	/System/Librar	com.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Browser.Generic	/Applications/M	com.micros	1	/Applications/Microsoft Defender.app/Contents/M
macOS.Messages.Generic	/Applications/M	com.micros	1	/Applications/Microsoft Defender.app/Contents/M
macOS.Messages.Generic	/System/Librar	com.apple.	0	/System/Library/PrivateFrameworks/IMCore.fram

macOS.Messages.Generic	/Library/Applic	com.micros	1	/Library/Application Support/Microsoft/EdgeUpd
macOS.Browser.Generic	/System/Librar	com.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Messages.Generic	/System/Librar	com.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Browser.Generic	/Applications/M	com.micros	1	/Applications/Microsoft Defender.app/Contents/M
macOS.Messages.Generic	/Applications/M	com.micros	1	/Applications/Microsoft Defender.app/Contents/M
macOS.Messages.Generic	/System/Librar	com.apple.	0	/System/Library/PrivateFrameworks/IMCore.fram

macOS.Messages.Generic	/Library/Application Support/Microsoft/EdgeUpdater/118.0.2088.86/EdgeUp
macOS.Browser.Generic	/System/Library/Frameworks/CoreServices.framework/Versions/A/Framewo
macOS.Messages.Generic	/System/Library/Frameworks/CoreServices.framework/Versions/A/Framewo
macOS.Browser.Generic	/Applications/Microsoft Defender.app/Contents/MacOS/wdavdaemon
macOS.Messages.Generic	/Applications/Microsoft Defender.app/Contents/MacOS/wdavdaemon
macOS.Messages.Generic	/System/Library/PrivateFrameworks/IMCore.framework/imagent.app/Conter



macOS.Messages.Generic	/Library/Application Support/Microsoft/EdgeU	com.microsoft.EdgeUpdater
macOS.Browser.Generic	/System/Library/Frameworks/CoreServices.fr	com.apple.mds
macOS.Messages.Generic	/System/Library/Frameworks/CoreServices.fr	com.apple.mds
macOS.Browser.Generic	/Applications/Microsoft Defender.app/Conten	com.microsoft.wdav
macOS.Messages.Generic	/Applications/Microsoft Defender.app/Conten	com.microsoft.wdav
macOS.Messages.Generic	/System/Library/PrivateFrameworks/IMCore.f	com.apple.imagent

Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR

Syllabus

FILE QUARANTINE

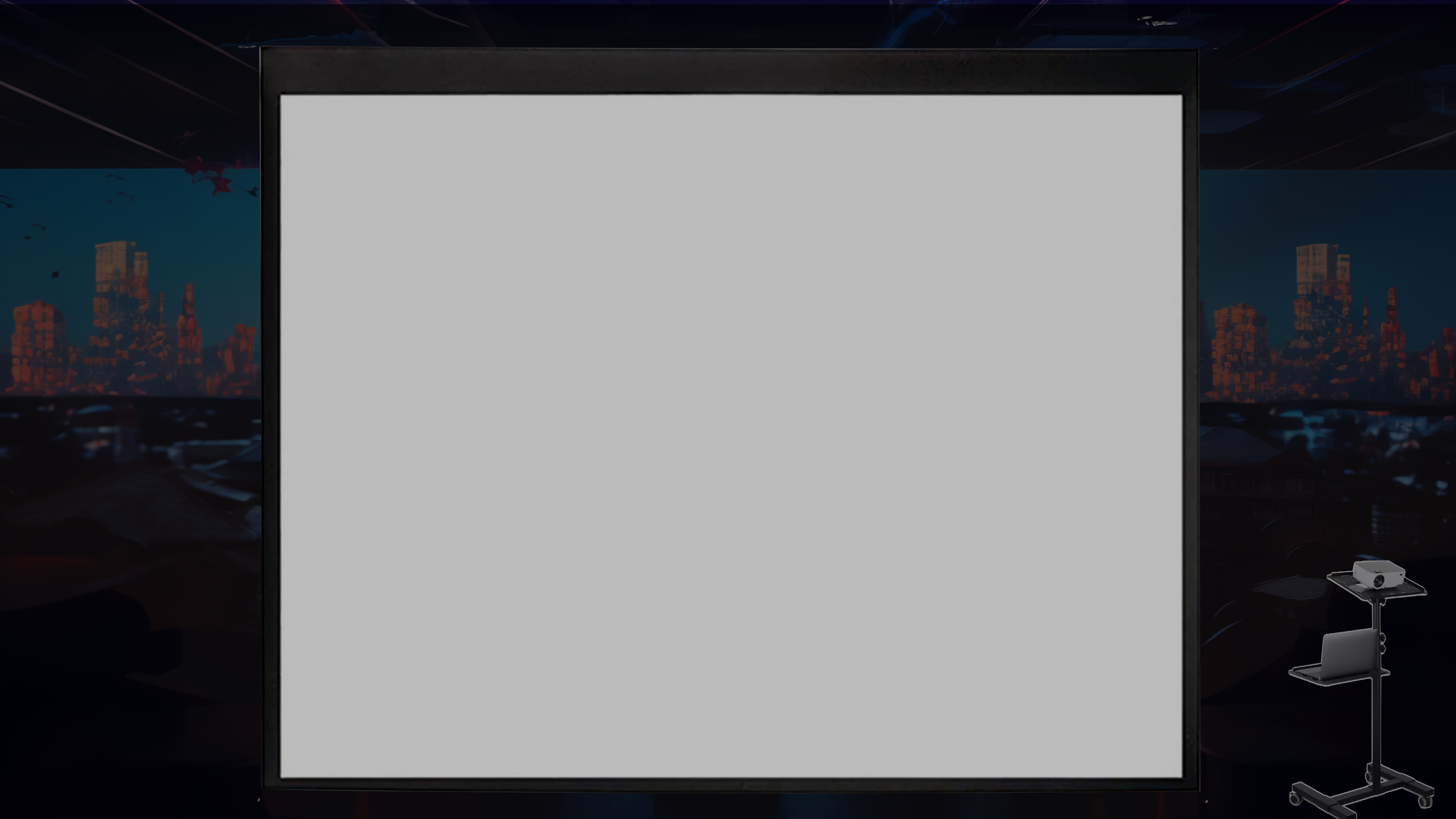
GATEKEEPER

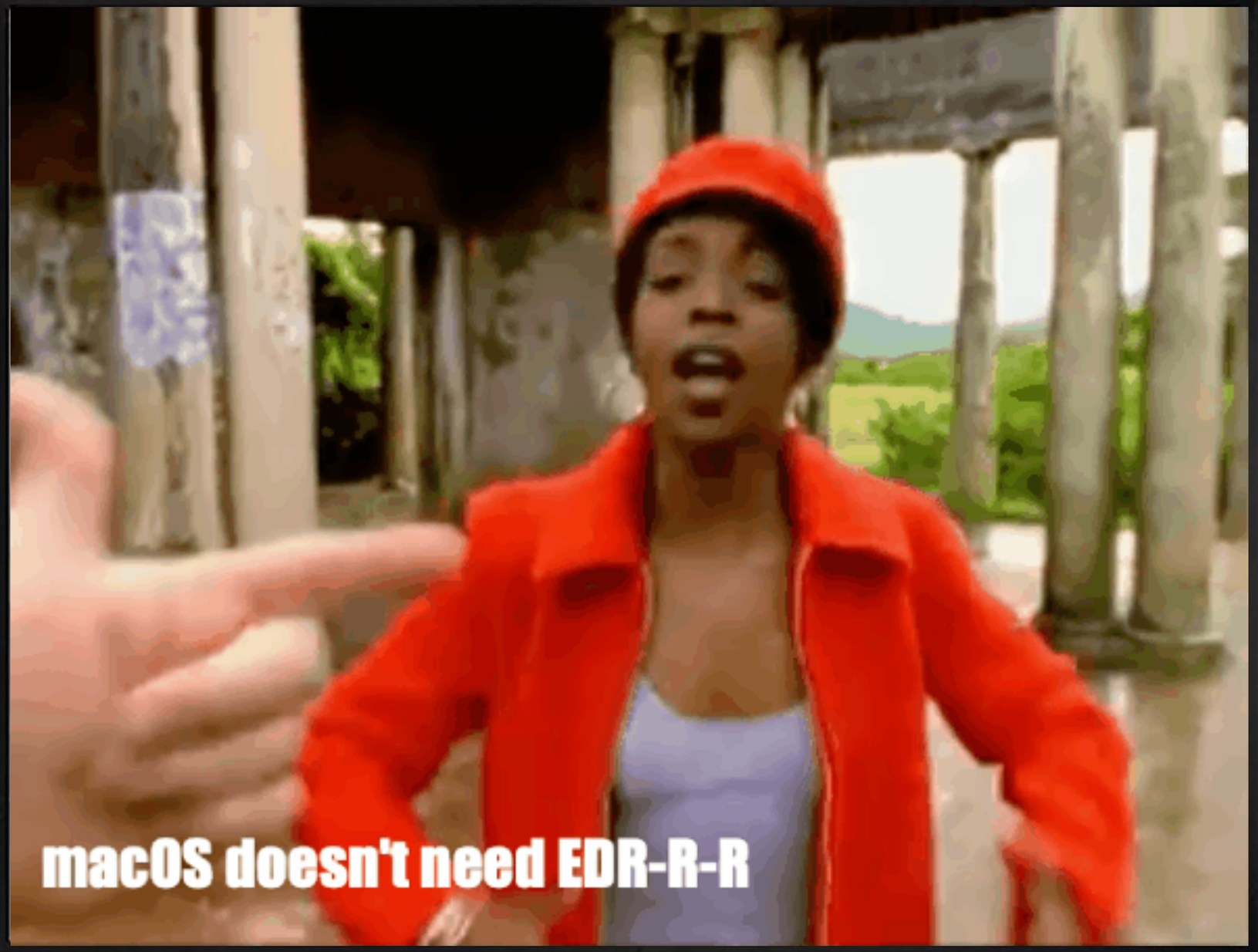
TCC

XPROTECT

XPROTECT REMEDIATOR

WHAT ABOUT YOU




macOS doesn't need EDR-R-R

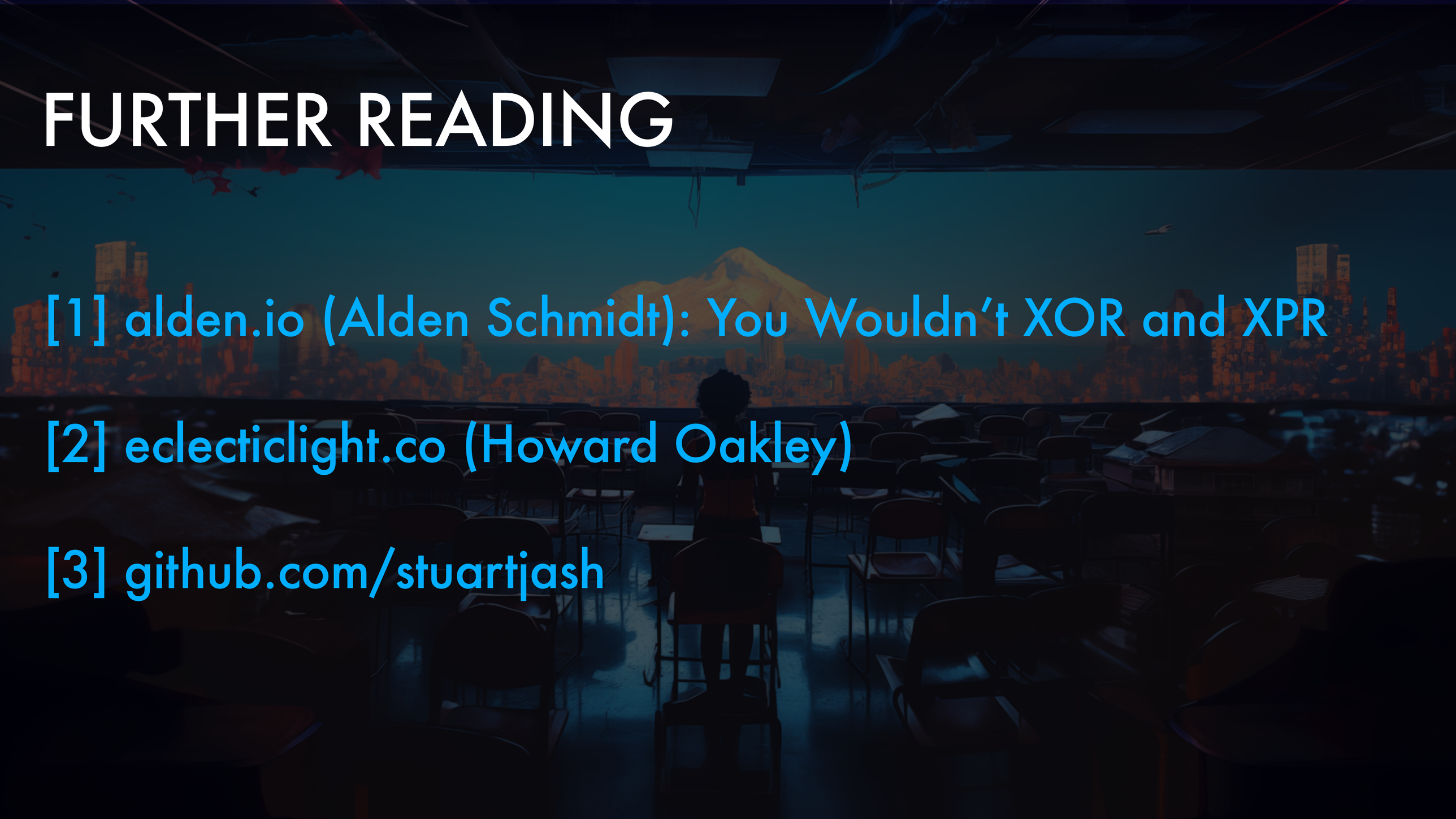

REACTIVE
HUNTRESS
PROACTIVE

REFERENCES

[1] alden.io (Alden Schmidt): You Wouldn't XOR and XPR

[2] eclecticlight.co (Howard Oakley)

[3] huntress.com/authors/stuart-ashenbrenner



FURTHER READING

[1] alden.io (Alden Schmidt): You Wouldn’t XOR and XPR

[2] eclecticlight.co (Howard Oakley)

[3] github.com/stuartjash

Q&A