

The (Mis)Education of macOS Security Internals




```
~  
> whoami
```




```
~
> whoami
Stuart Ashenbrenner
~
> whatdoIdo
```



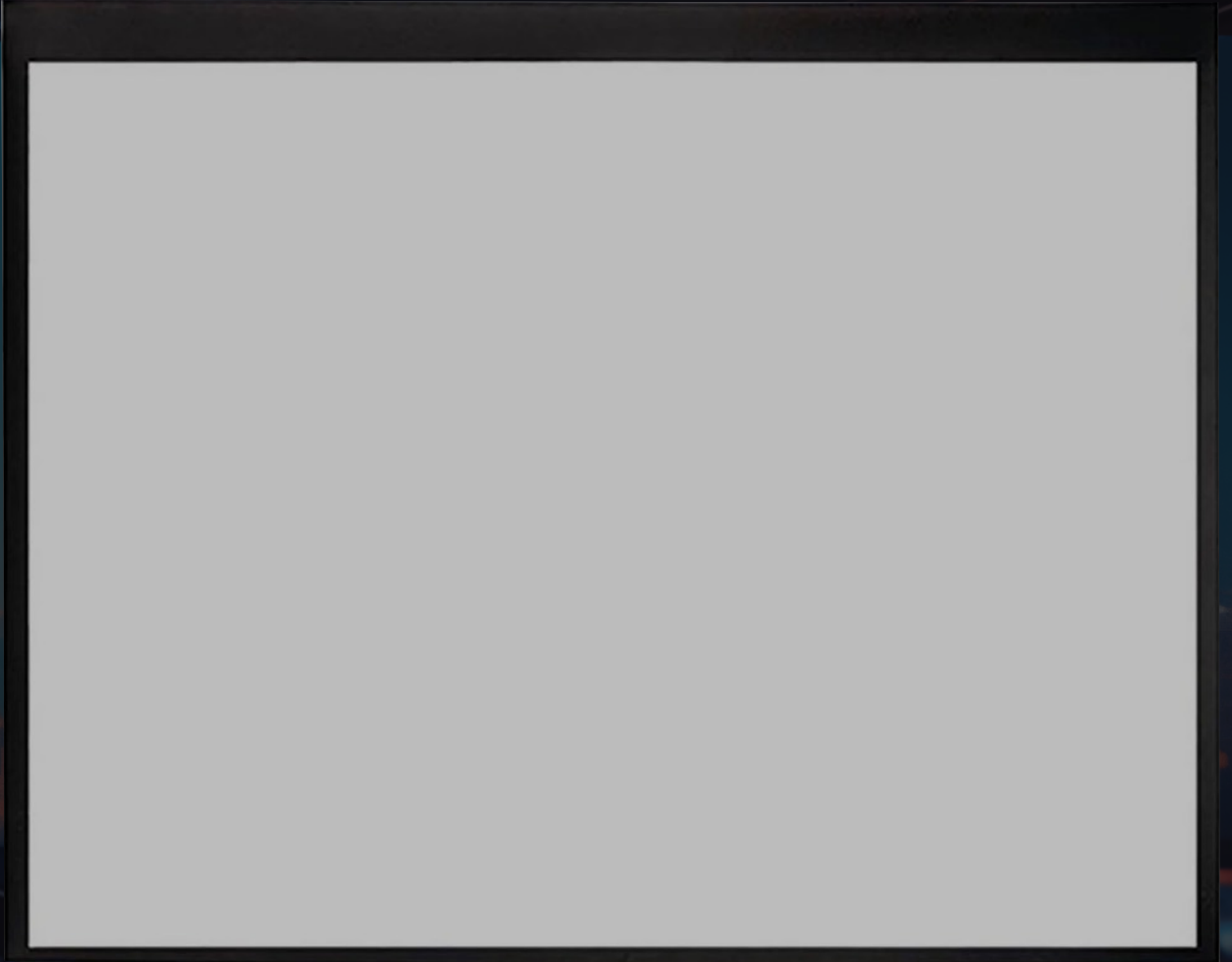

```
~
> whoami
  Stuart Ashenbrenner
~
> whatdoIdo
  Principal Product Researcher, macOS
~
> whatelse
```




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

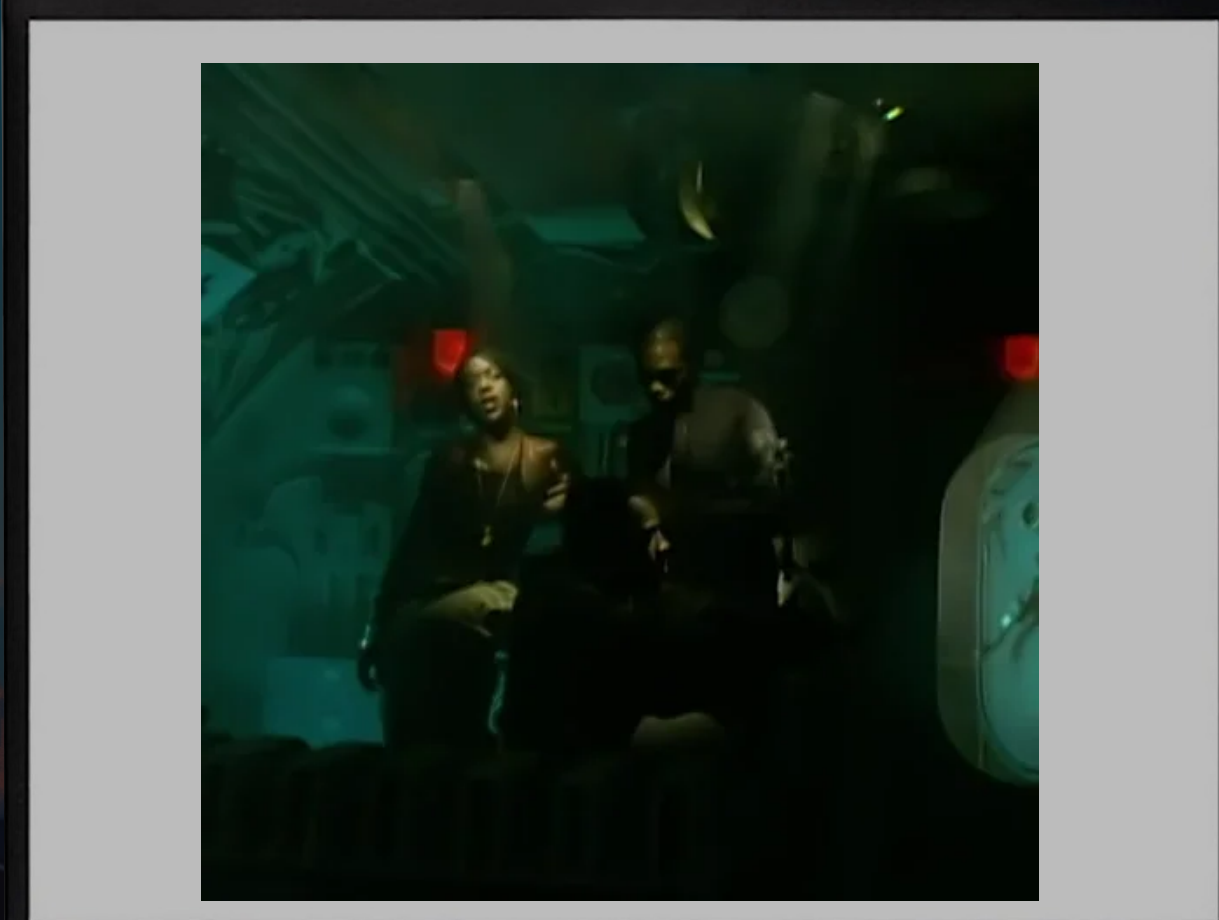


Syllabus



Syllabus

THREE LEVELS OF DEFENSE

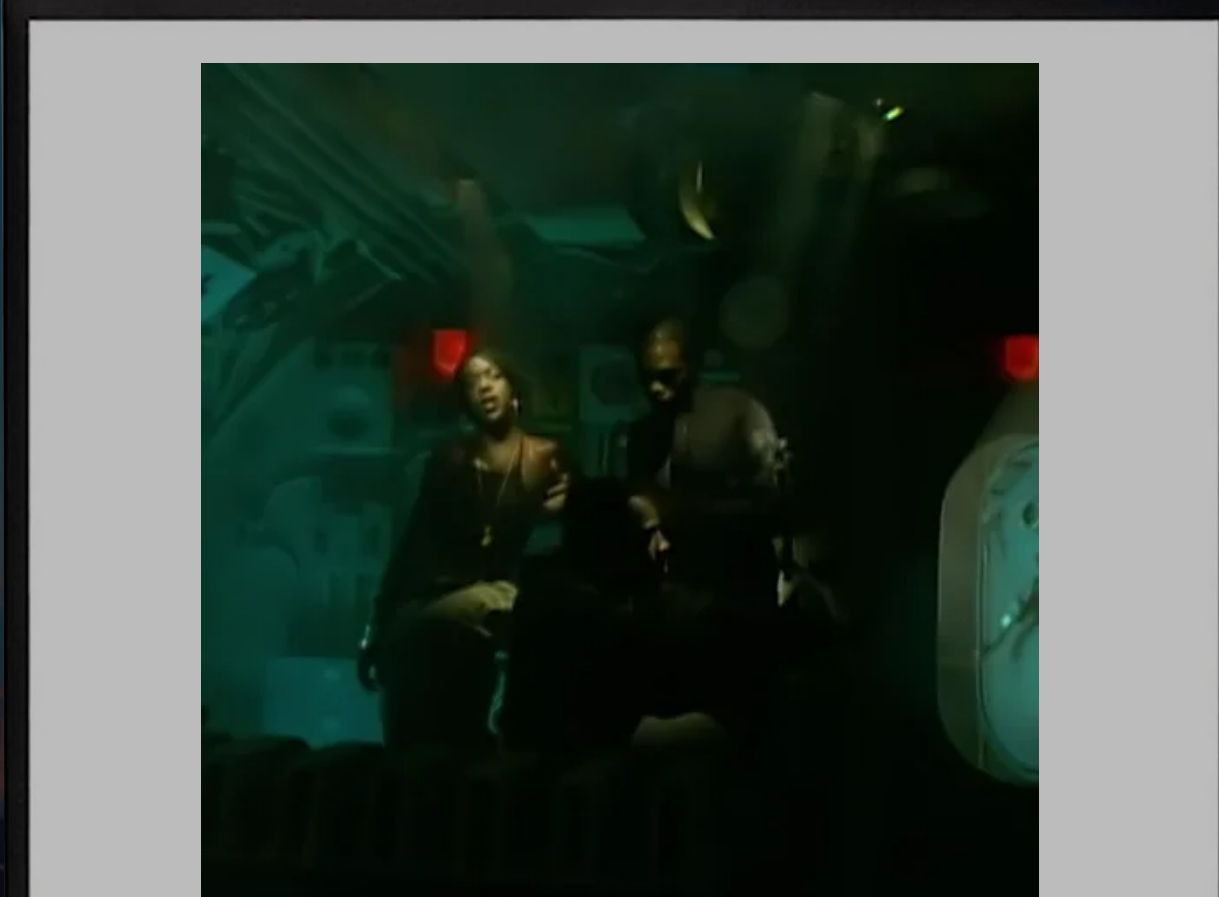


Syllabus

CHECK

BLOCK

REMEDIATE

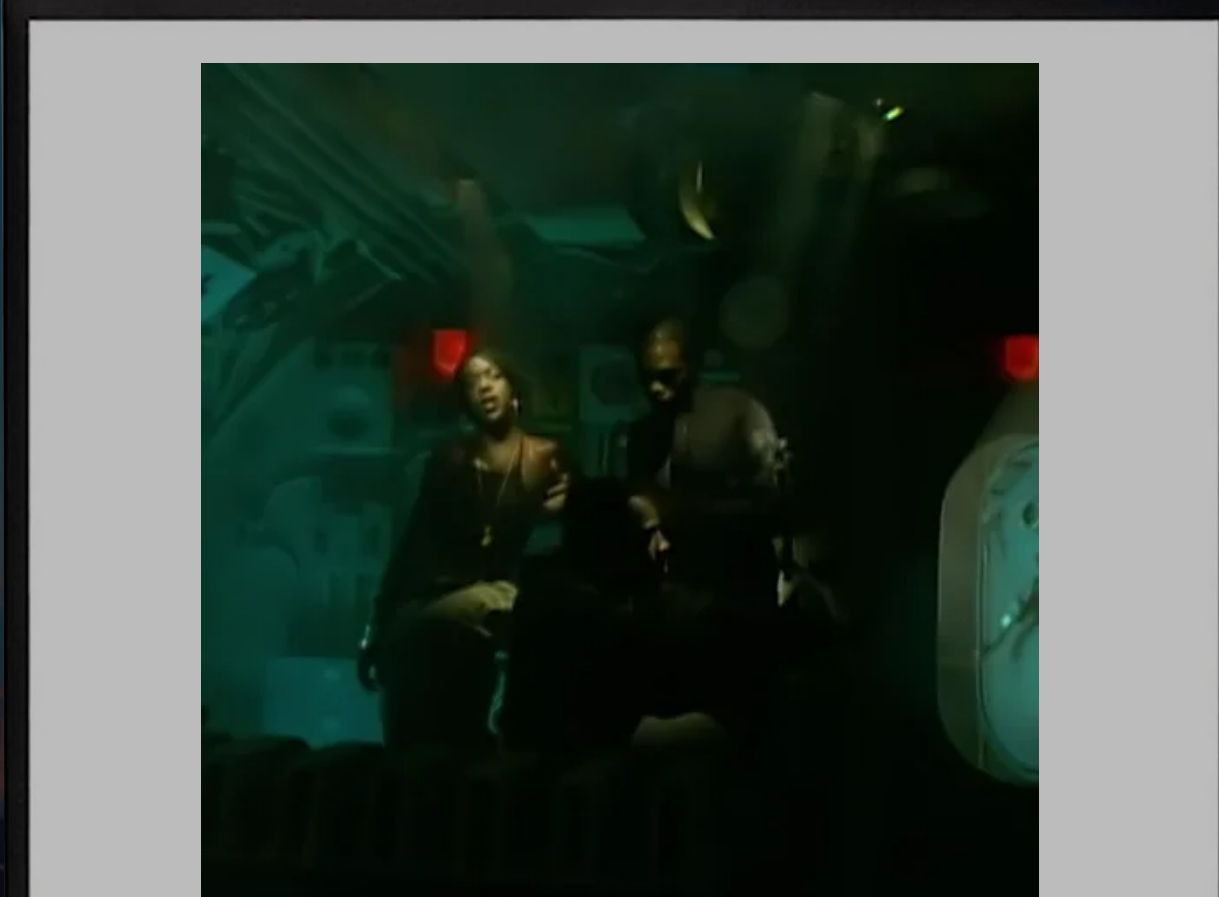


Syllabus

CHECK

BLOCK

REMEDIATE

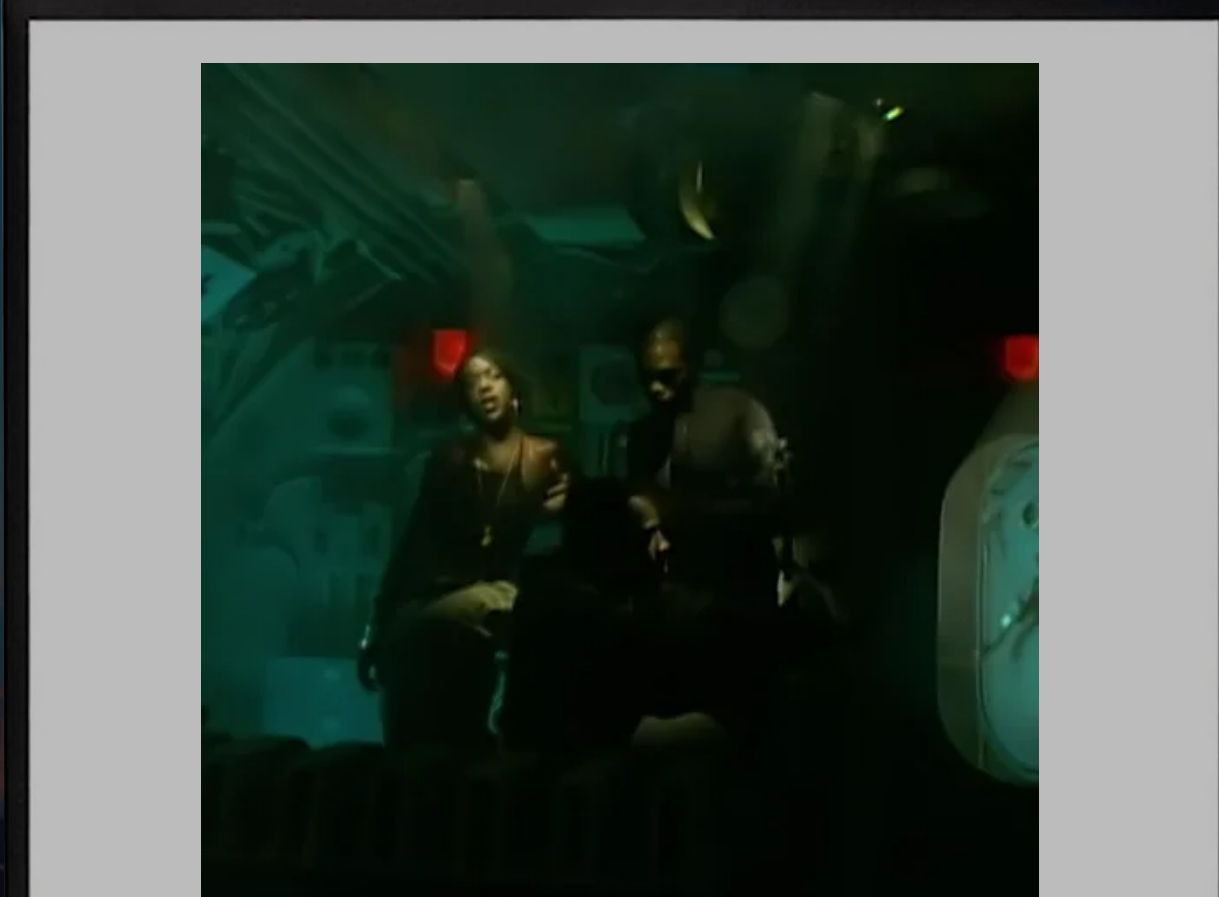


Syllabus

CHECK

BLOCK

REMEDIATE

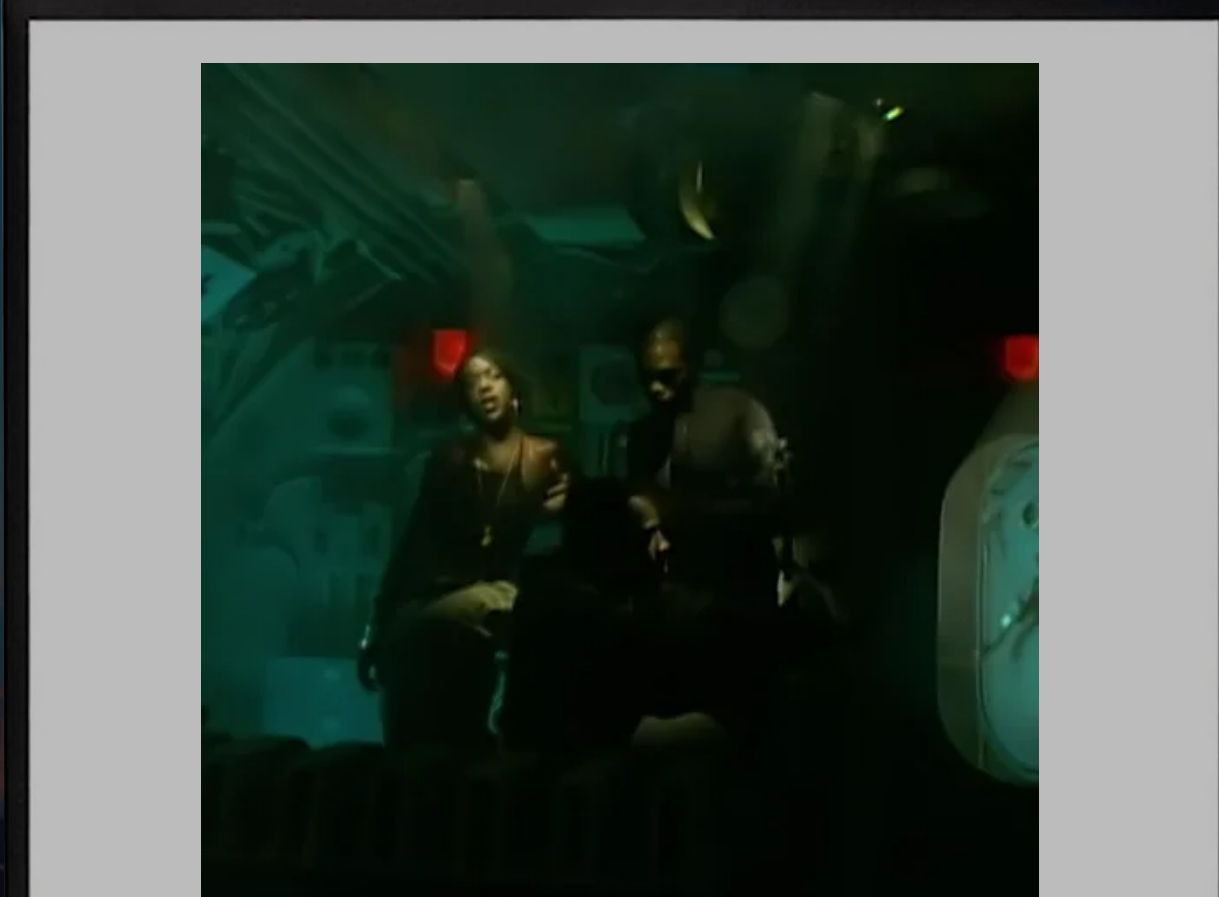


Syllabus

CHECK

BLOCK

REMEDIATE



Syllabus

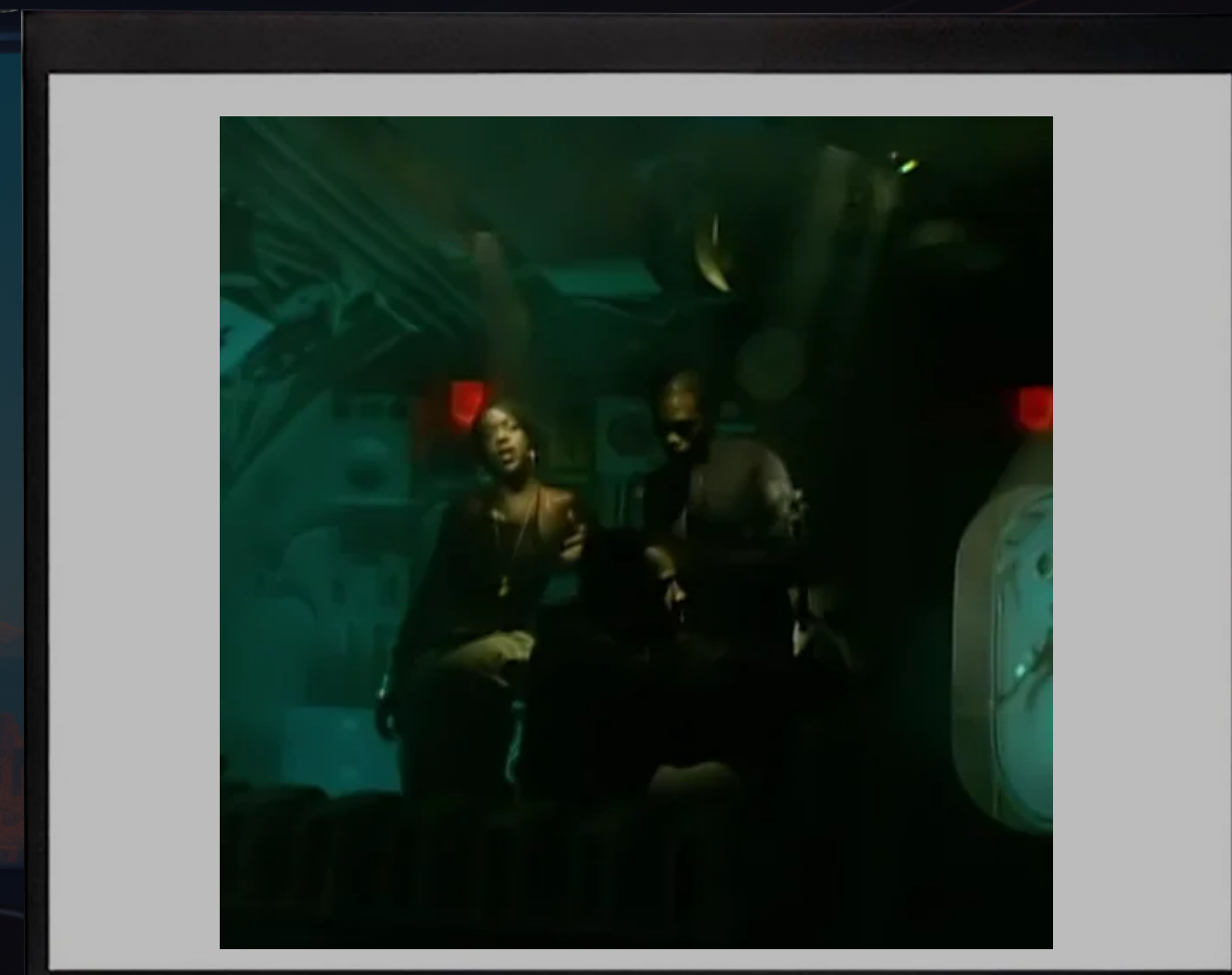
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



Syllabus

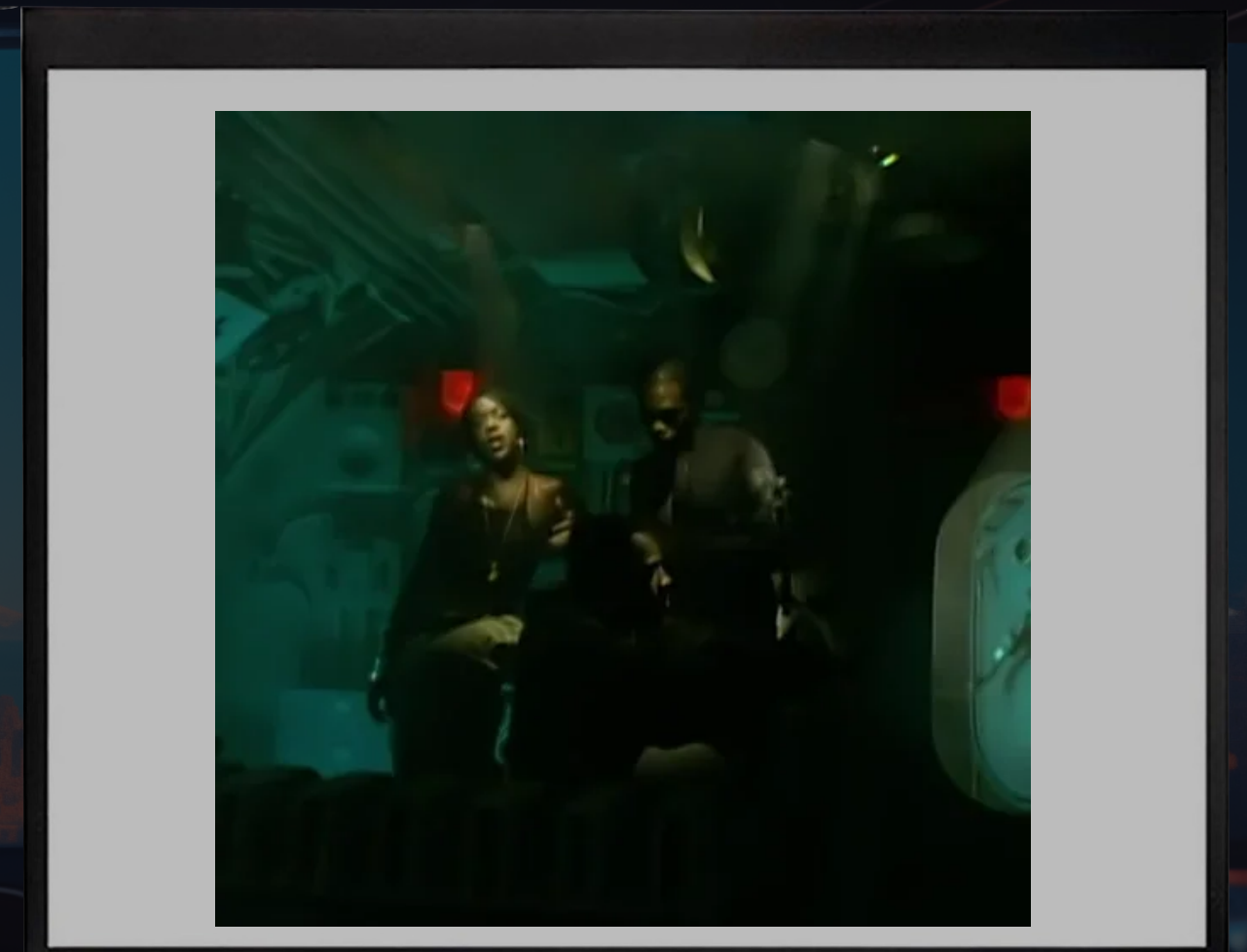
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

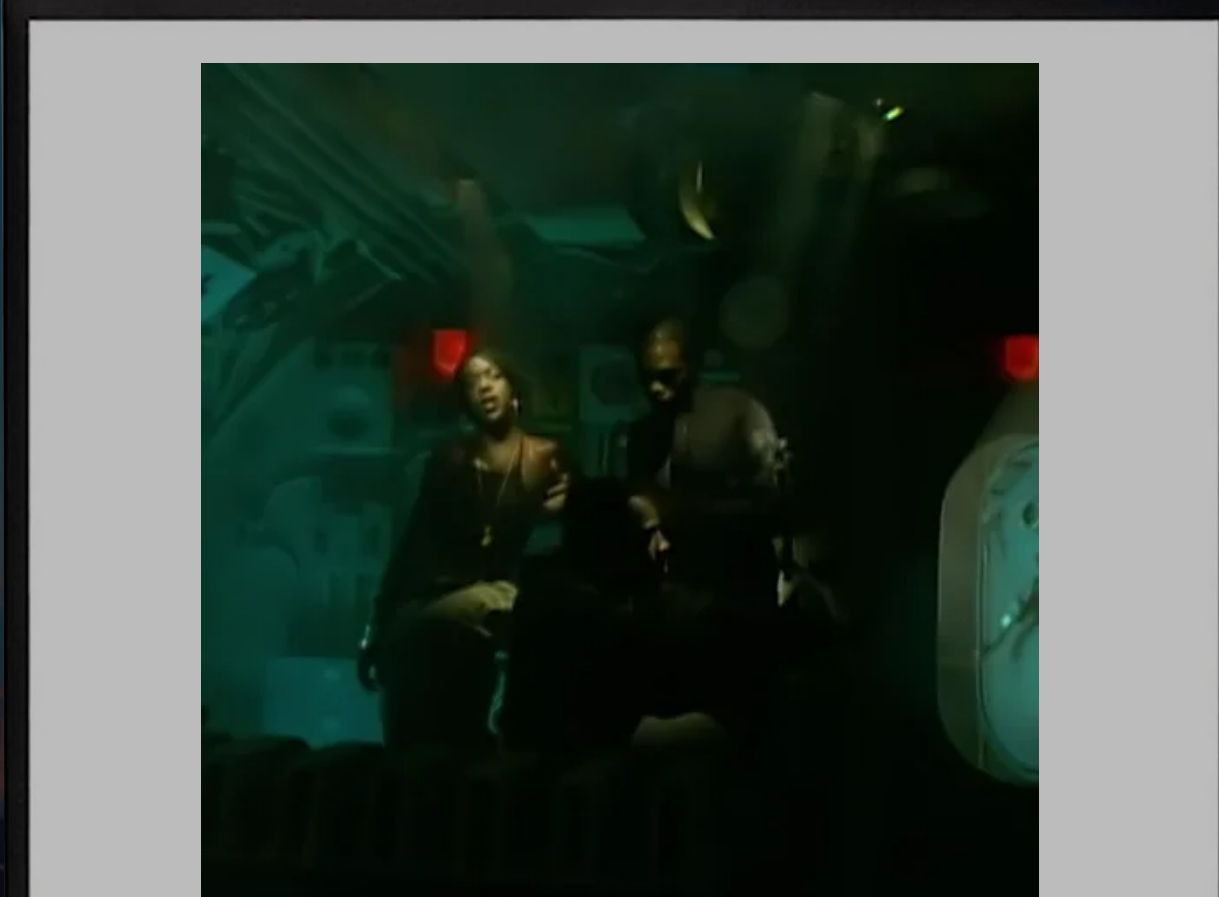


Syllabus

CHECK

BLOCK

REMEDIATE



Syllabus

CHECK

BLOCK

REMEDIATE



Syllabus

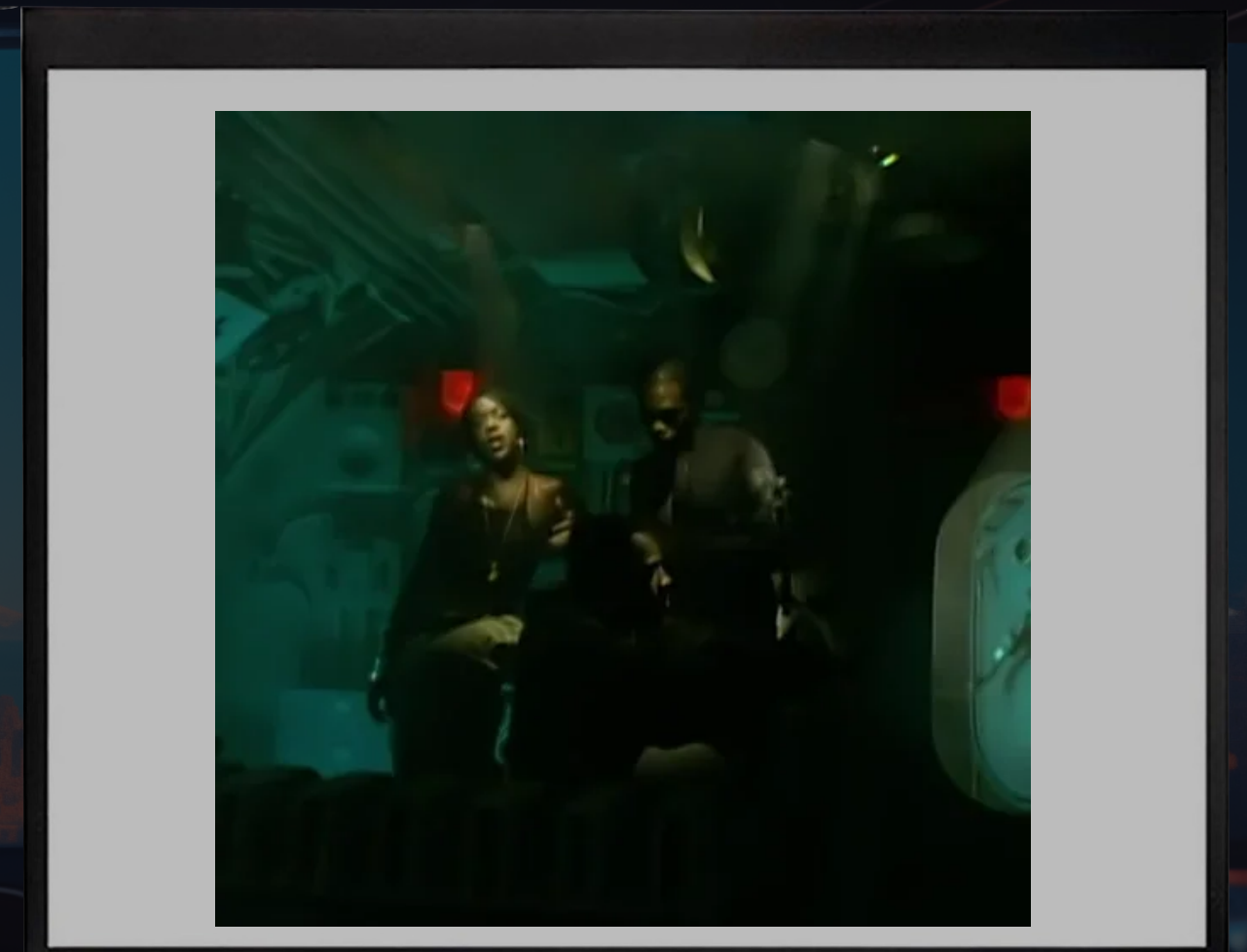
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR

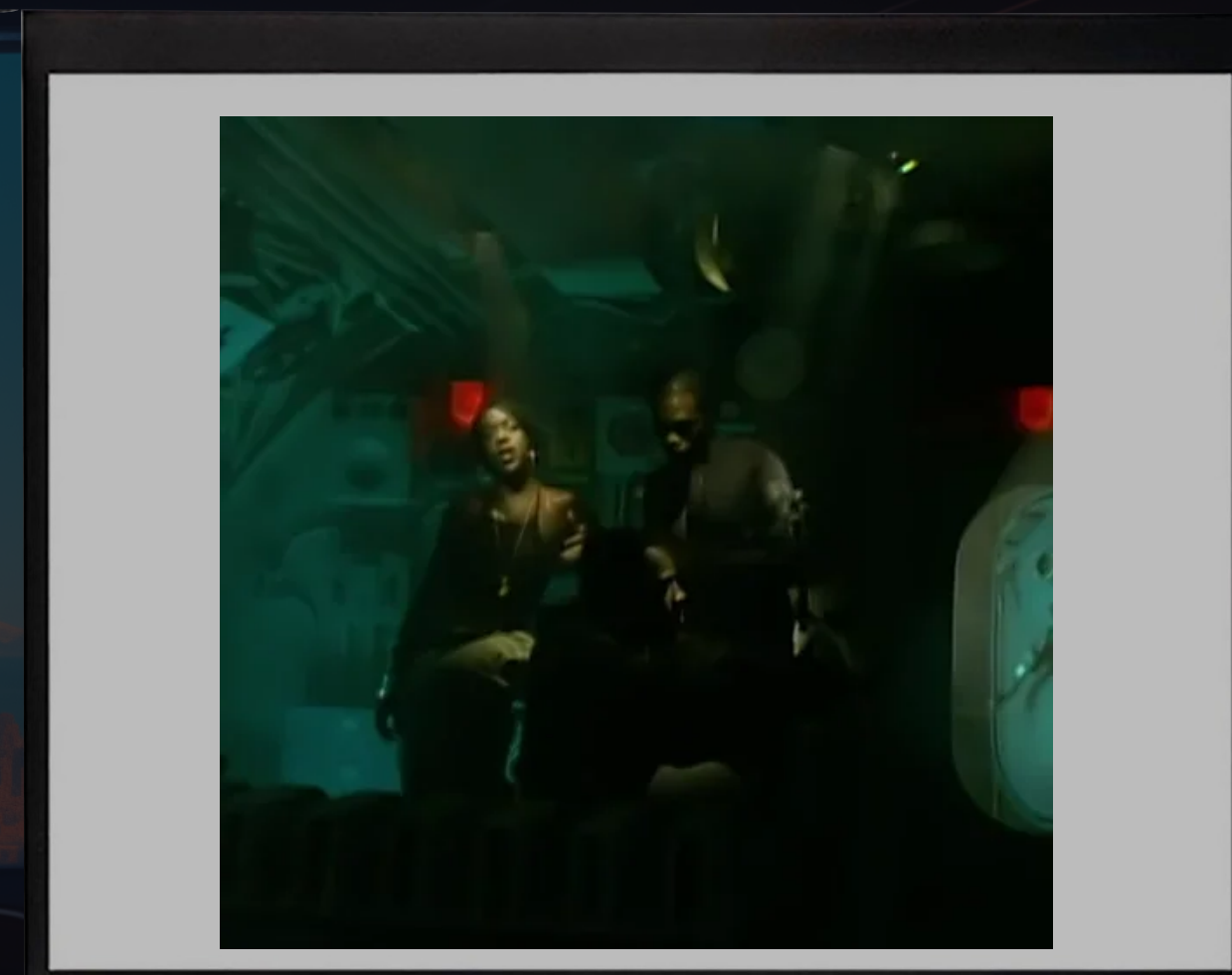


Syllabus

CHECK

BLOCK

REMEDIATE

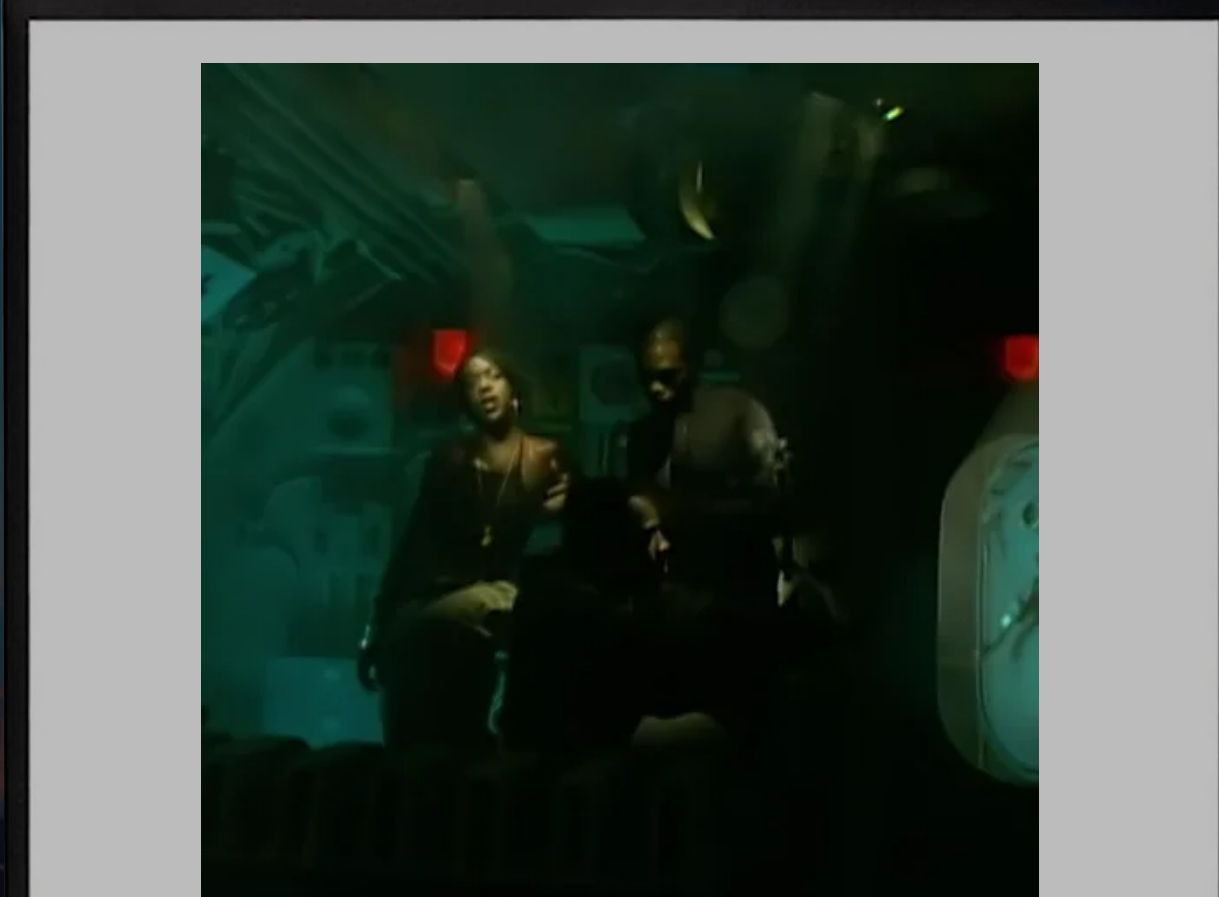


Syllabus

CHECK

BLOCK

REMEDIATE



Syllabus

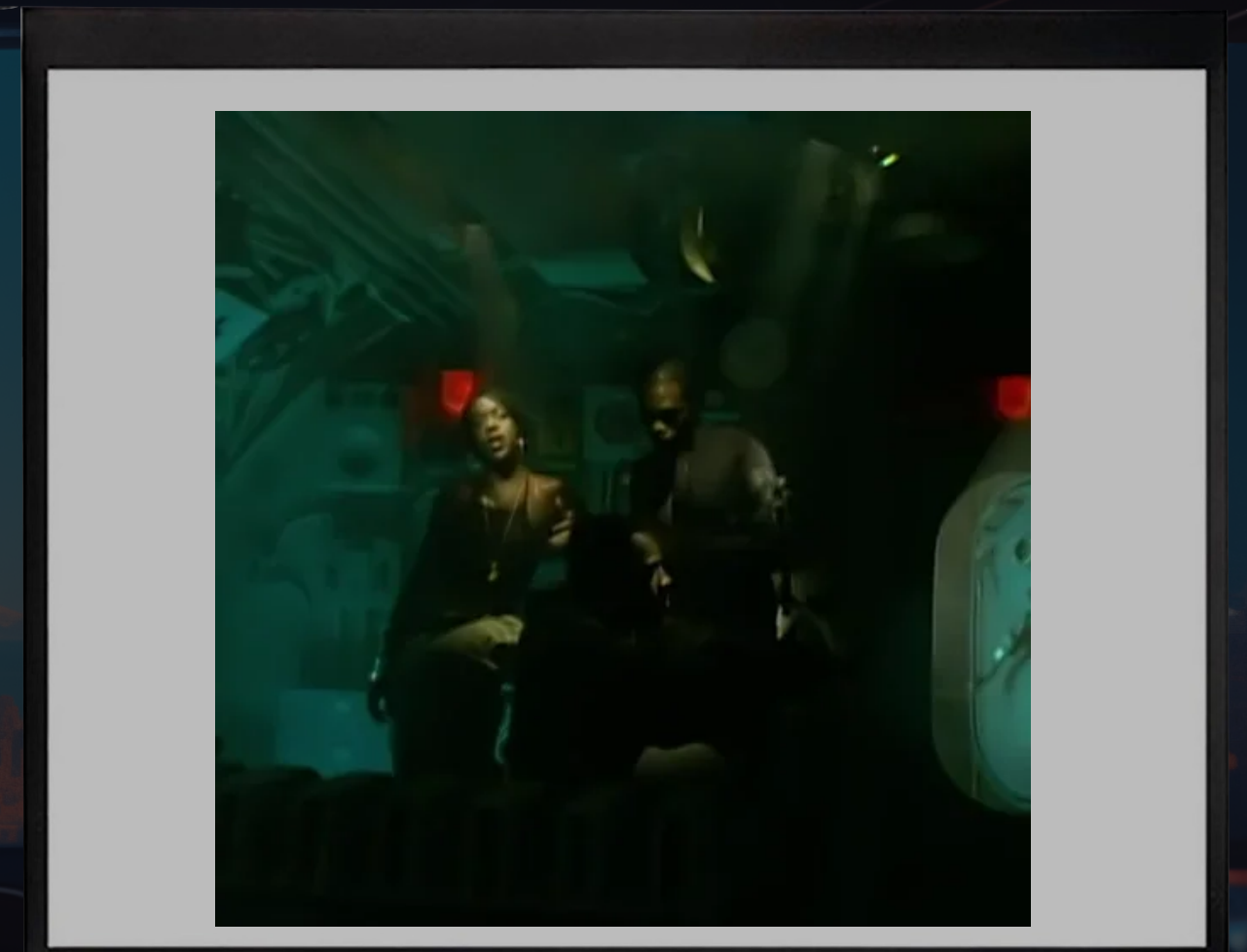
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR



Syllabus

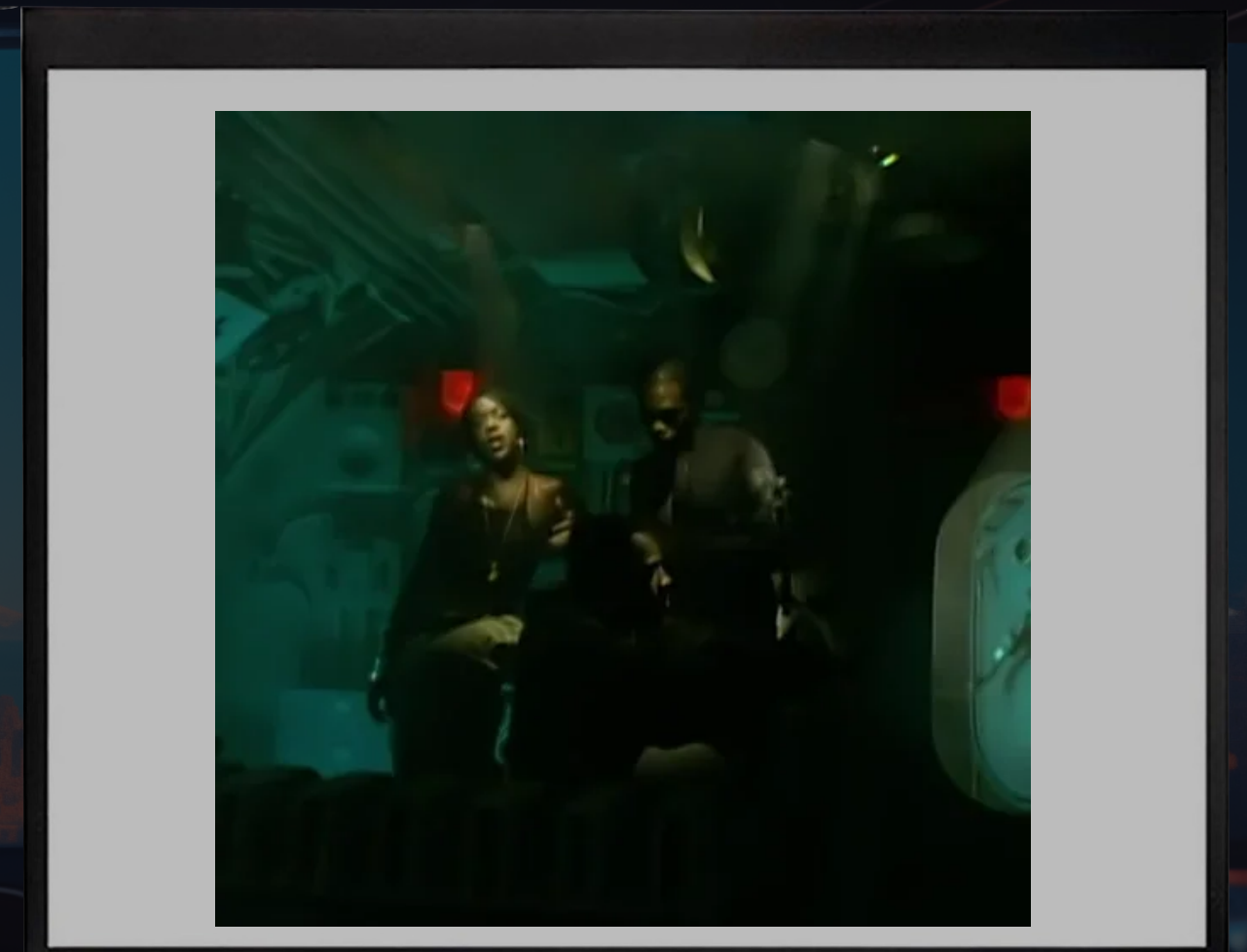
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR



The image depicts a dark, atmospheric scene of a classroom. In the foreground, rows of empty desks and chairs are visible, receding into the distance. The room is dimly lit, with a blue and purple color palette. In the background, a cityscape with various skyscrapers is visible, set against a backdrop of a large, snow-capped volcano. The sky is dark with a few birds flying. The overall mood is somber and desolate.

FILE QUARANTINE

A person is sitting at a desk in the center of a large, empty classroom. The room is filled with rows of desks and chairs, all of which are unoccupied. The background features a panoramic view of a city skyline with various skyscrapers and a large, snow-capped volcano in the distance. The sky is a deep blue, and the overall lighting is dim, creating a somber and contemplative atmosphere. The word "WHAT?" is written in large, white, sans-serif capital letters across the center of the image, partially overlapping the person and the background.

WHAT?

WHAT?

OSX 10.5 Lion

WHAT?

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

A person is sitting at a desk in a classroom, looking out at a cityscape with a large mountain in the background. The scene is dimly lit, with a blue and orange color palette. The person is seen from behind, sitting at a desk in the center of the room. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible, with a large mountain in the distance. The sky is a mix of blue and orange, suggesting a sunset or sunrise. The overall mood is contemplative and somewhat somber.

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.

A person is sitting at a desk in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible under a blue sky, with a large mountain in the distance. The scene is dimly lit, with a blue tint. The text "APP TRANSLOCATION" is overlaid in the center in a bright blue, sans-serif font.

APP TRANSLOCATION

A person is sitting at a desk in the center of a large, empty classroom. The room is filled with rows of desks and chairs, all of which are unoccupied. The background features a panoramic view of a city skyline with various skyscrapers and a large, snow-capped volcano in the distance. The sky is a deep blue, and the overall lighting is dim, creating a somber and contemplative atmosphere. The word "WHAT?" is written in large, bold, white capital letters across the center of the image, partially overlapping the person and the background.

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

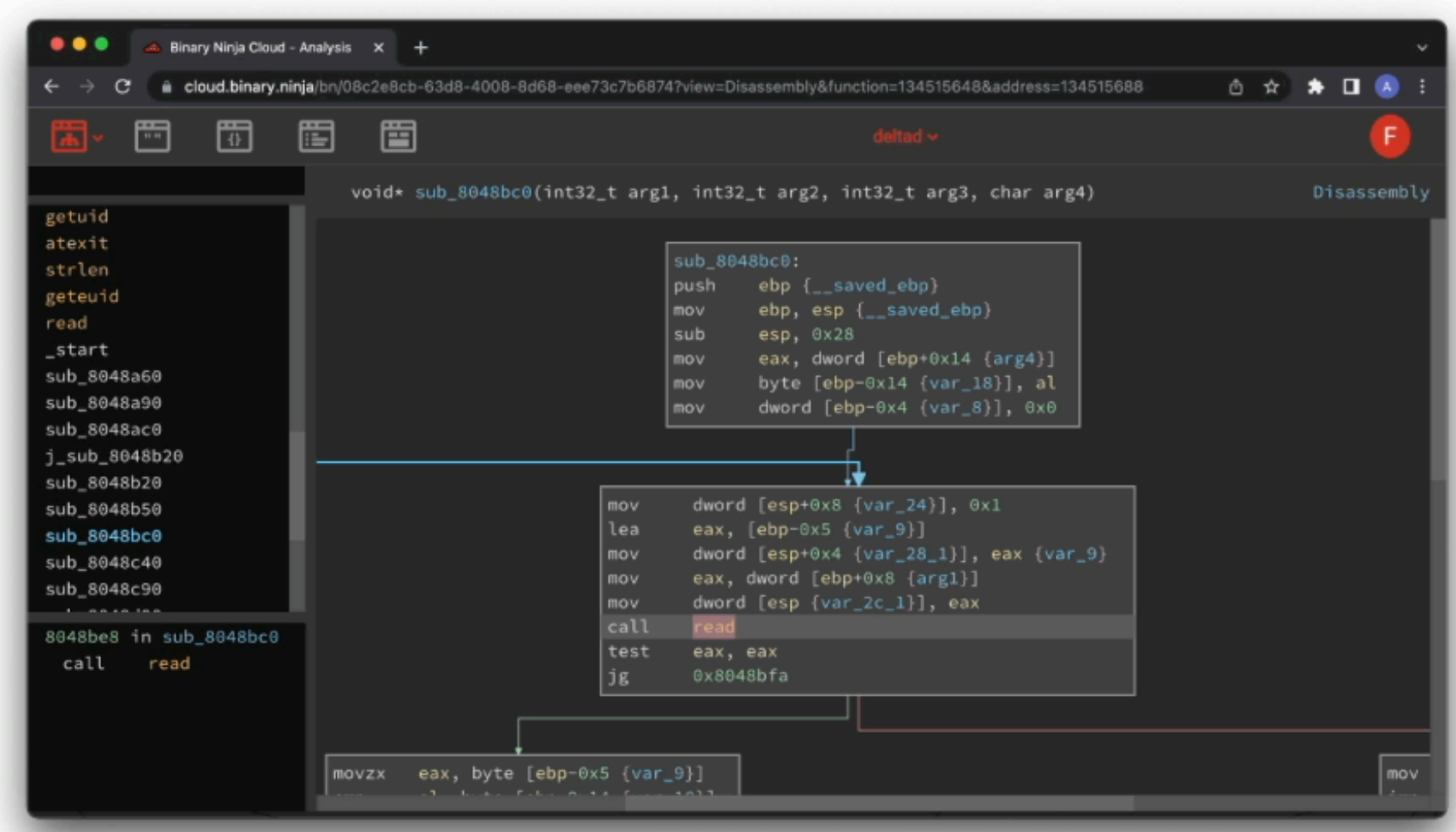
WHAT?

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



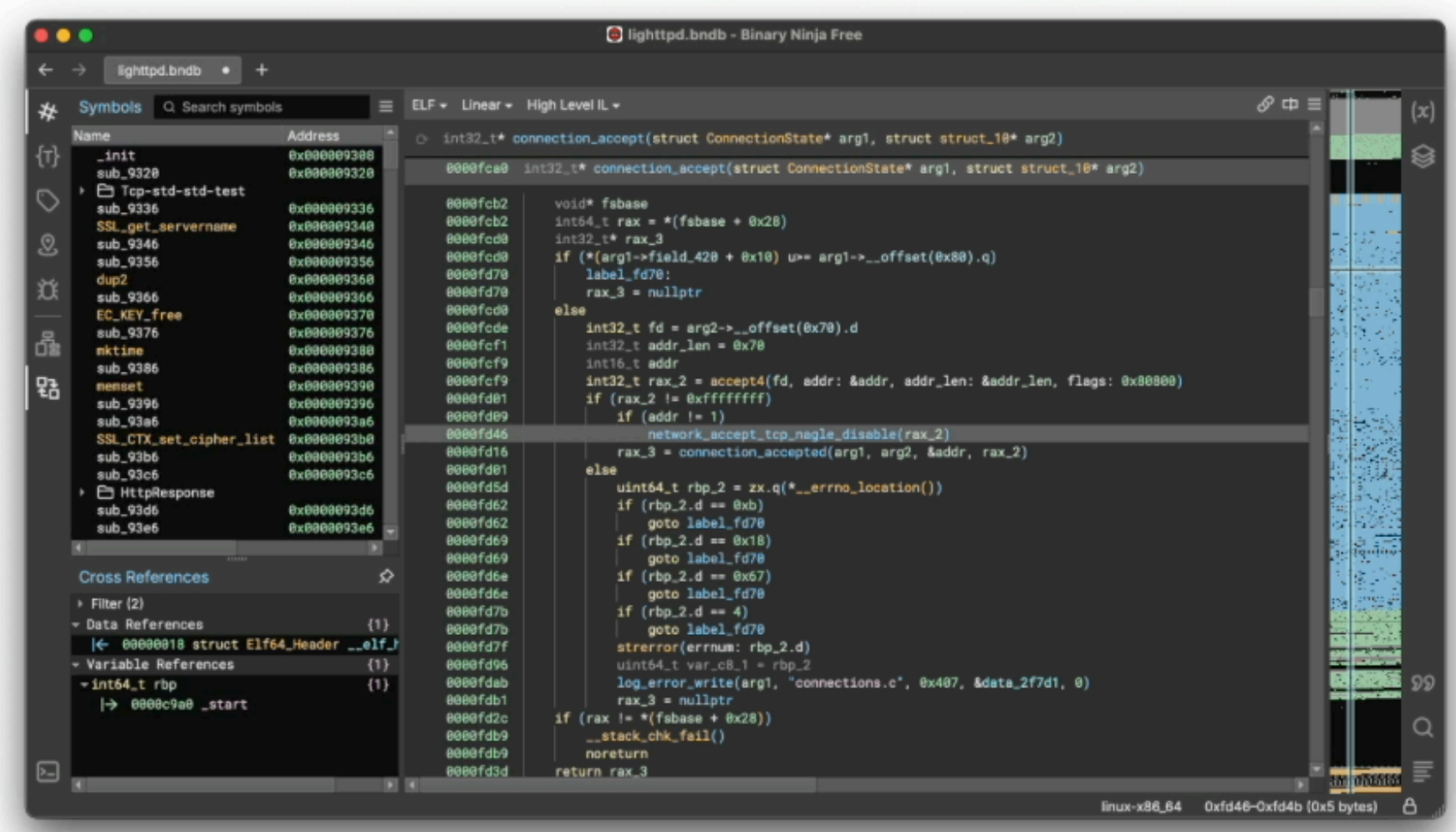
There are two ways to try Binary Ninja for free! Binary Ninja Cloud supports all architectures, but requires you to upload your binaries. Binary Ninja Free is a downloadable app that runs locally, but has architecture restrictions. Neither free option supports our powerful API / Plugin ecosystem.

CLOUD



Try Cloud!

FREE



Download For Windows

Download For macOS



The screenshot shows a macOS file explorer window titled 'ash' overlaid on the binary.ninja website. The file explorer displays a list of folders with the following columns: Name, Date Modified, Size, Kind, and Date Added.

Name	Date Modified	Size	Kind	Date Added
> Applications	May 24, 2024 at 9:21 PM	--	Folder	Oct 17, 2022 at 10:14 AM
> Applicati...(Parallels)	May 7, 2024 at 9:01 AM	--	Folder	Feb 23, 2024 at 1:52 PM
> Desktop	May 29, 2024 at 1:18 PM	--	Folder	Oct 12, 2022 at 3:00 PM
> Developer	May 20, 2024 at 12:34 PM	--	Folder	Oct 17, 2022 at 9:31 AM
> Documents	May 30, 2024 at 11:01 AM	--	Folder	Oct 12, 2022 at 3:00 PM
> Downloads	Today at 2:57 PM	--	Folder	Oct 12, 2022 at 3:00 PM
> go	Oct 20, 2023 at 2:05 PM	--	Folder	Oct 18, 2022 at 9:53 AM
> iCloud Dri...(Archive)	Mar 7, 2024 at 7:45 AM	--	Folder	Mar 7, 2024 at 7:45 AM
> Movies	Mar 22, 2024 at 5:30 PM	--	Folder	Oct 12, 2022 at 3:00 PM
> Music	Jan 2, 2024 at 9:38 AM	--	Folder	Oct 12, 2022 at 3:00 PM
> OrbStack	Feb 23, 2024 at 1:32 PM	--	Folder	Feb 23, 2024 at 1:32 PM
> Parallels	Feb 23, 2024 at 1:50 PM	--	Folder	Oct 20, 2022 at 10:13 AM
> Pictures	May 14, 2024 at 9:29 AM	--	Folder	Oct 12, 2022 at 3:00 PM
> Public	Oct 12, 2022 at 3:00 PM	--	Folder	Oct 12, 2022 at 3:00 PM

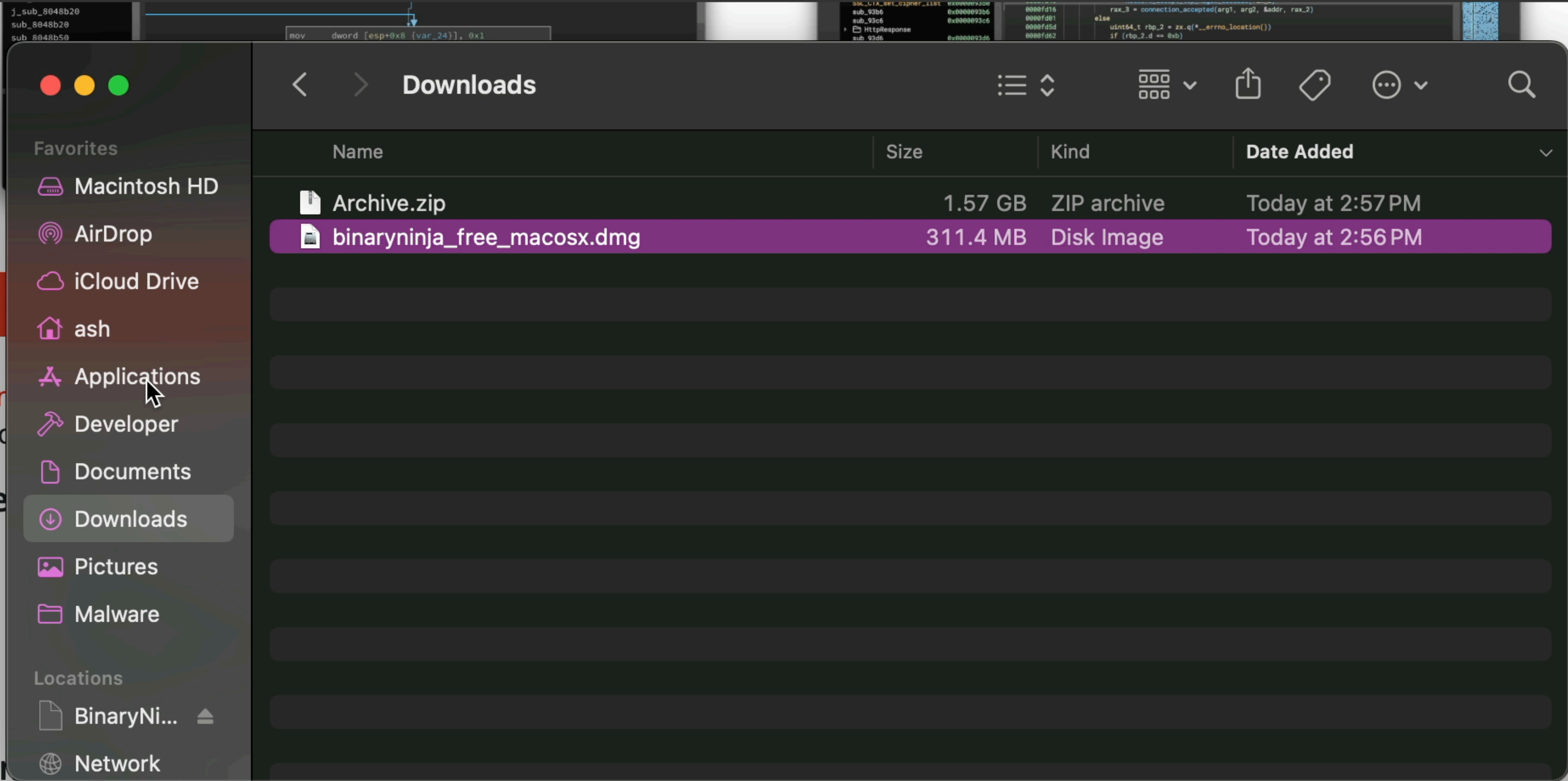
It does, however come with some limitations (see the [ToS](#) for more info):

- Not as feature-rich as the native client

Features

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





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 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):

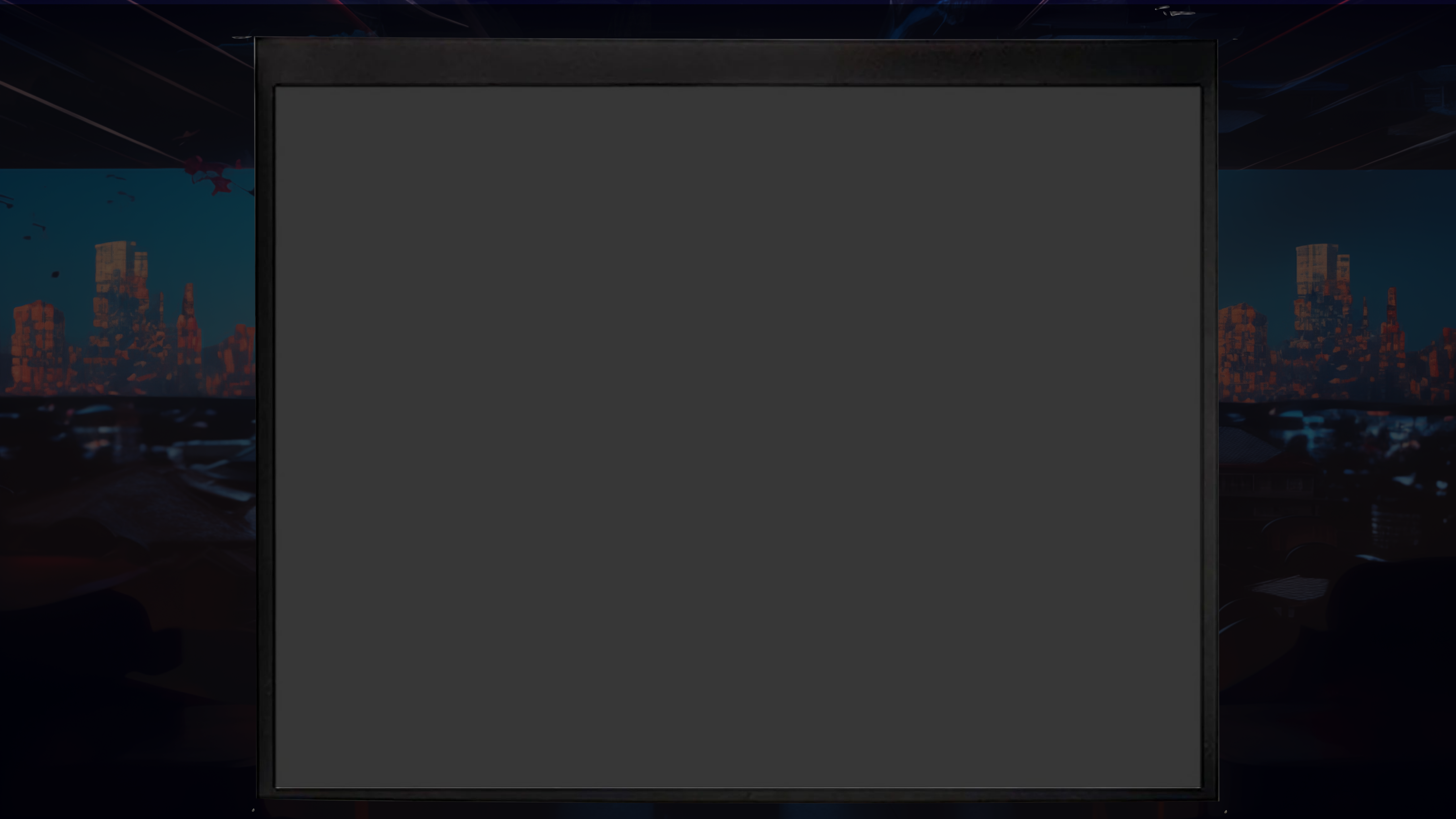
- Not as feature-rich as the native client

Features

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





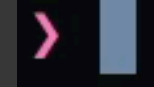




⌘2

~

~



⏏ ⏏ ⏏ ~#2

~

> xattr ~/Downloads/binaryninja_free_macosx.dmg

com.apple.macl

com.apple.quarantine

~

> █

~

> 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

~

> █

~

> 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

~

> █

~

> 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

~

> 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

~

> █

~

> 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

~

> 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

~

> █

~

> 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

~

> 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

~

> █

~

> 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

~

> 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 T

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 f
07:05:55.919672-0700	Finder	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
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 f
07:05:55.922945-0700	Dock	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.920054-0700	com.apple.WebKit.Ne	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.924274-0700	fileproviderd	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.924851-0700	Family	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.921982-0700	com.apple.appkit.xp	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.948373-0700	MTLAssetUpgraderD	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.948995-0700	siriknowledged	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.952629-0700	XprotectService	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.953655-0700	linkd	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
07:05:55.986954-0700	swcd	com.apple.la	db	NotifyToken::RegisterDispatch(user.uid.501.com.apple.LaunchServices.database) fired f
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

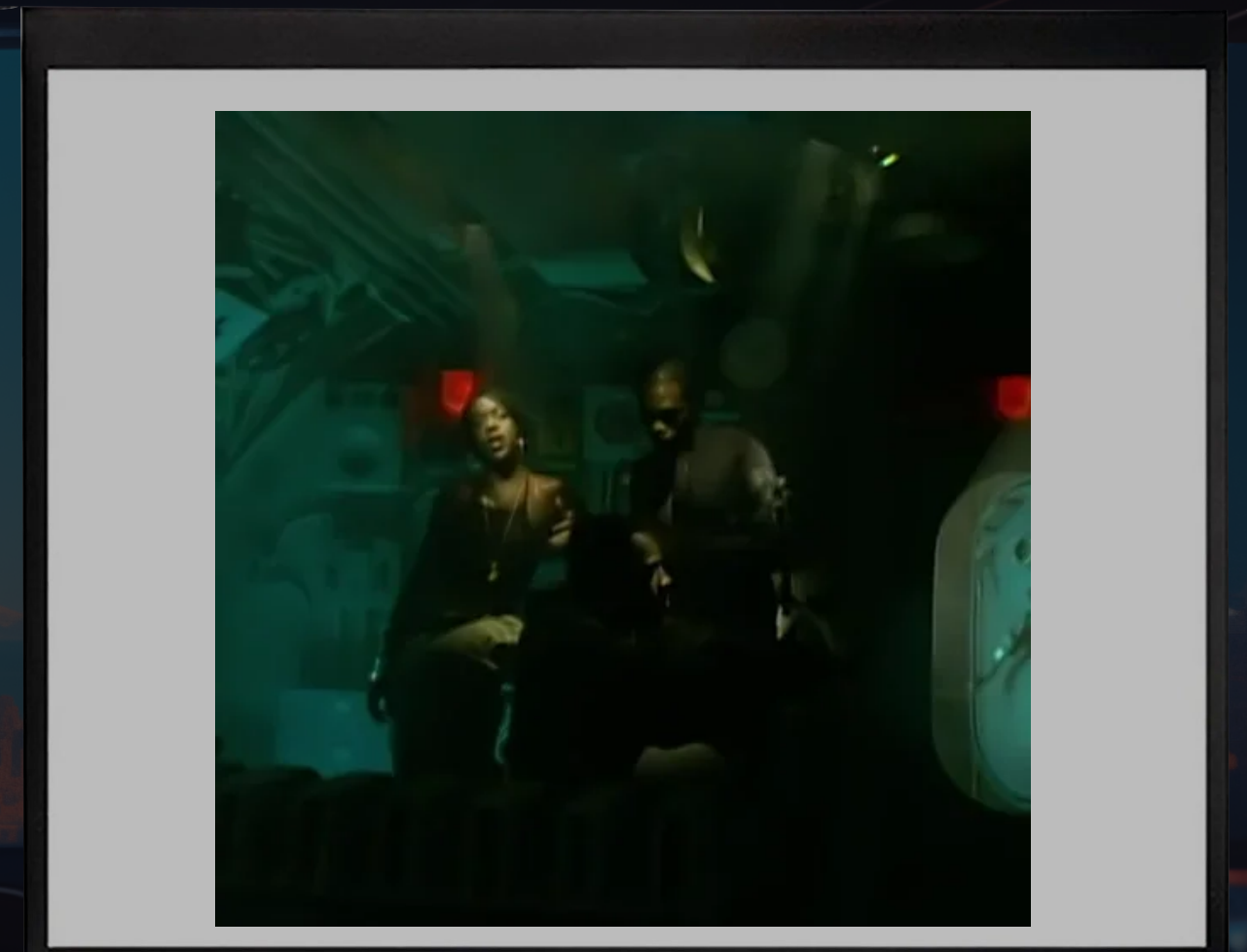
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



Syllabus

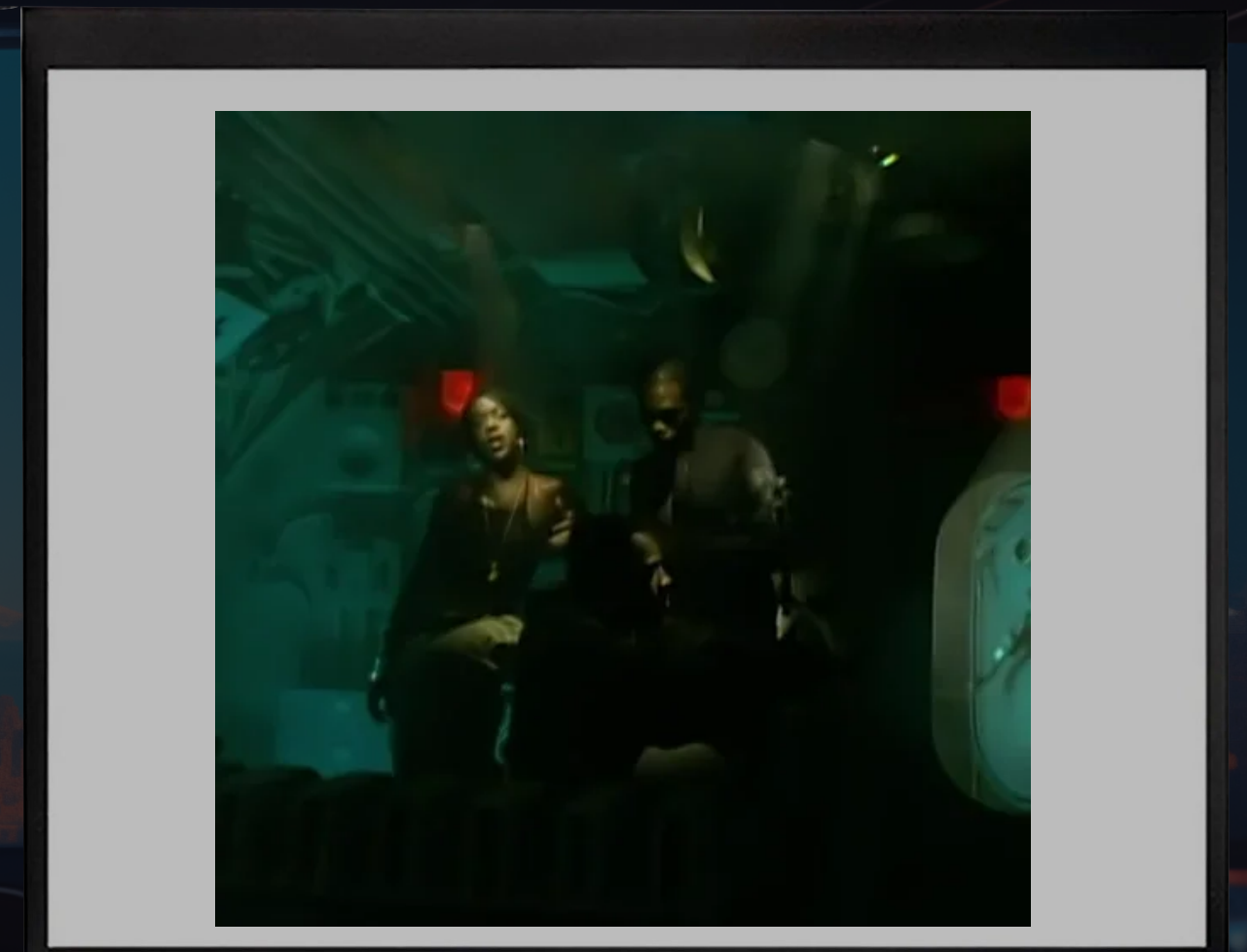
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



A person is sitting at a desk in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible through a large window, with a prominent mountain peak in the distance. The scene is dimly lit, with a blue and orange color palette. The word "GATEKEEPER" is overlaid in the center in a bright blue, sans-serif font.

GATEKEEPER

A person is sitting at a desk in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible through a large window, with a prominent mountain peak in the distance. The scene is dimly lit, with a blue and orange color palette. The word "GATEKEEPER" is overlaid in the center in a bright blue, sans-serif font.

GATEKEEPER

FILE QUARANTINE



APP TRANSLOCATION



GATEKEEPER

GATEKEEPER

A person is sitting at a desk in a classroom, looking out at a cityscape with a large mountain in the background. The scene is dimly lit, with a blue and orange color palette. The person is seen from behind, sitting at a desk with a laptop. The classroom has many other desks and chairs, all empty. The cityscape in the background features various buildings and a large, prominent mountain.

“...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

```
~  
> 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

```
~  
> 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

A person is sitting at a desk in a classroom, looking out at a city skyline with a large mountain in the background. The scene is dimly lit, with a blue and orange color palette. The person is in the center, facing away from the camera. The city skyline is visible through the windows, and the mountain is the central focus of the background.

10-character identifier assigned to developers

CODE SIGNING

```
~  
> 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

```
~  
> spctl -a -t exec -vvv /Applications/Huntress.app  
/Applications/Huntress.app: accepted  
source=Notarized Developer ID  
origin=Developer ID Application: Huntress Labs Inc (7W6HQ9J9XA)  
~  
> █
```


NOTARIZATION

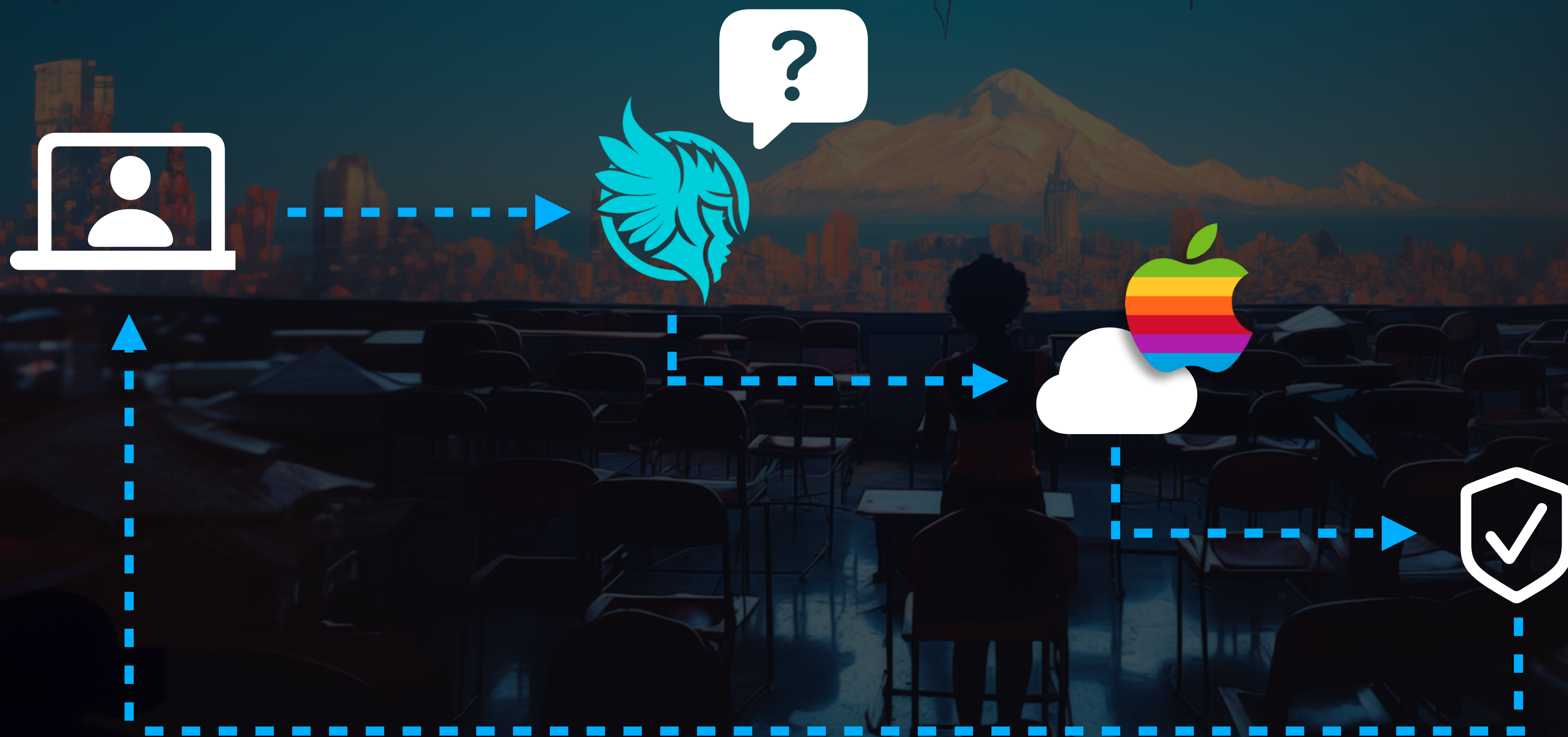
```
~  
> spctl -a -t exec -vvv /Applications/Huntress.app  
/Applications/Huntress.app: accepted  
source=Notarized Developer ID  
origin=Developer ID Application: Huntress Labs Inc (7W6HQ9J9XA)  
~  
> |
```


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

The image shows a macOS System Preferences window with the 'Appearance' panel selected. The left sidebar lists various settings, with 'Appearance' highlighted in purple. The main panel shows options for appearance, accent color, highlight color, sidebar icon size, and scroll bar settings. The 'Appearance' section has three options: 'Light', 'Dark', and 'Auto'. The 'Dark' option is selected and highlighted with a purple border. The 'Accent color' section shows a row of color swatches, with 'Purple' selected. The 'Highlight color' section shows a purple color swatch. The 'Sidebar icon size' section shows 'Medium' selected. The 'Allow wallpaper tinting in windows' toggle is turned on. The 'Show scroll bars' section has three options: 'Automatically based on mouse or trackpad' (selected), 'When scrolling', and 'Always'. The 'Click in the scroll bar to' section has two options: 'Jump to the next page' (selected) and 'Jump to the spot that's clicked'. A question mark icon is visible in the bottom right corner of the panel.

Appearance

Appearance

Light Dark Auto

Accent color

Purple

Highlight color

Purple

Sidebar icon size

Medium

Allow wallpaper tinting in windows

Show scroll bars

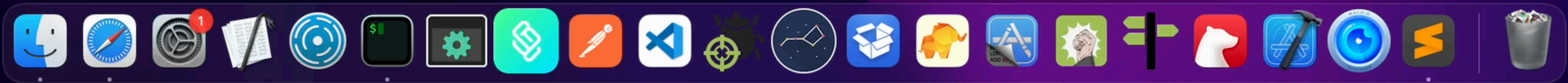
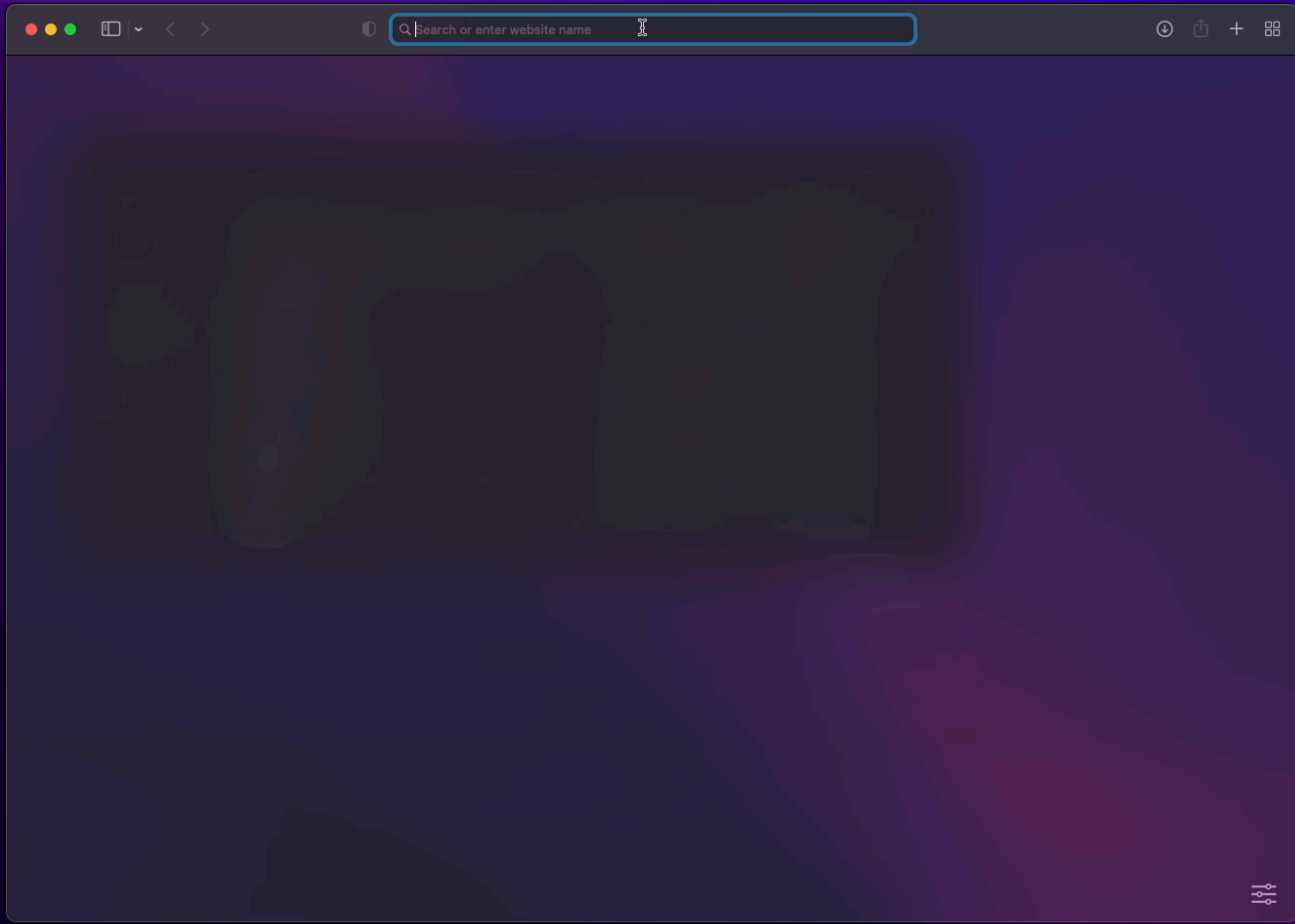
- Automatically based on mouse or trackpad
- When scrolling
- Always

Click in the scroll bar to

- Jump to the next page
- Jump to the spot that's clicked

?

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

The image shows a macOS System Preferences window with a dark theme. The left sidebar contains a search bar and a list of settings categories. The 'General' category is selected and highlighted in purple. The main content area displays the 'General' settings page, which includes a gear icon, the title 'General', a descriptive paragraph, and a list of sub-settings with right-pointing chevrons.

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

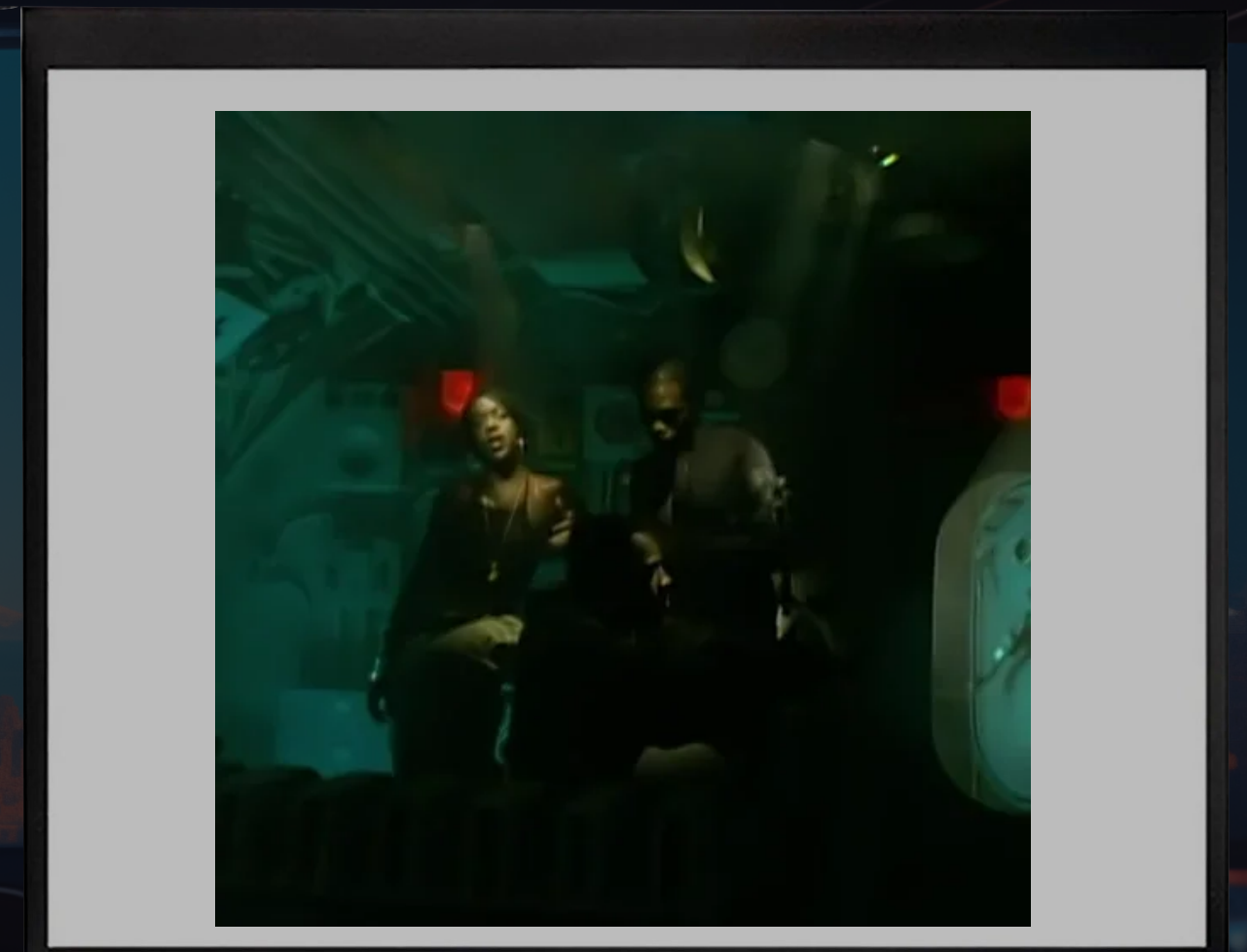
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



Syllabus

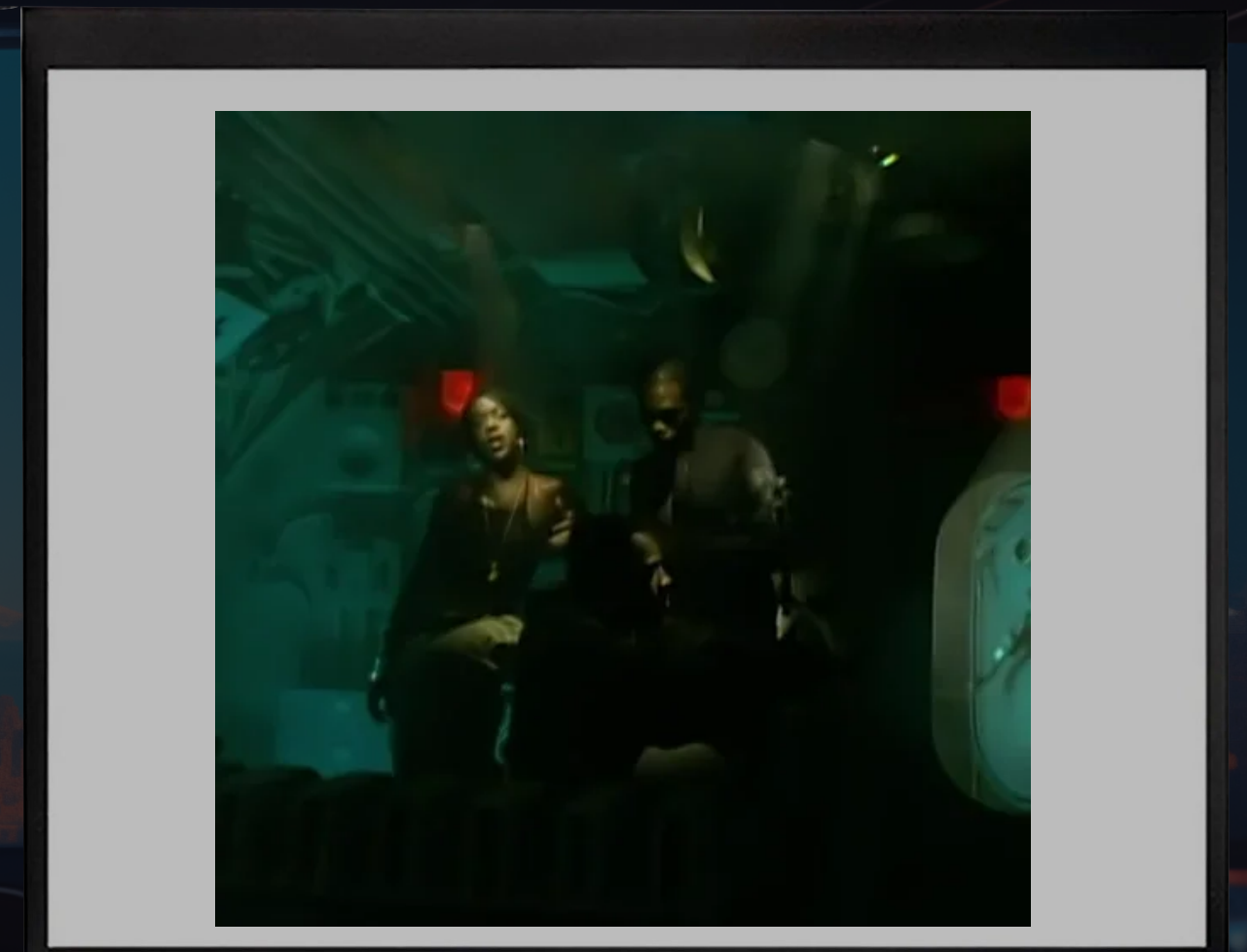
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



A person is sitting at a desk in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible under a blue sky, with a large mountain in the distance. The scene is dimly lit, with a blue color cast. The text 'TCC' is overlaid in the center of the image.

TCC

A person is sitting in the center of an empty classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible through a large window, with a prominent mountain range in the distance. The scene is dimly lit, with a blue and orange color palette. The text 'TRANSPARENCY', 'CONSENT', and 'CONTROL' is overlaid on the left side of the image in a bright blue, sans-serif font.

TRANSPARENCY


CONSENT

CONTROL

TCC


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

QLab




QLab 4.6.12

Documentation →
 Technical Support →
<https://qlab.app> →

 Open Workspace from file.

+ New Workspace
 from the built-in blank workspace.

 Licenses
 No active licenses.

Recent Workspaces: No workspaces have been saved yet.
 Templates:

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 | <input type="checkbox"/> |
|  Craft | <input type="checkbox"/> |
|  Crescendo System Extension | <input checked="" type="checkbox"/> |
|  DaisyDisk | <input checked="" type="checkbox"/> |
|  dumpBTM | <input checked="" type="checkbox"/> |
|  EdgeUpdater | <input type="checkbox"/> |
|  ESFPlaygroundExtension | <input checked="" type="checkbox"/> |
|  Extension | <input checked="" type="checkbox"/> |
|  Figma | <input type="checkbox"/> |
|  Final Cut Pro | <input type="checkbox"/> |
|  Google Chrome | <input type="checkbox"/> |
|  Huntress | <input type="checkbox"/> |
|  Huntress System Extension | <input checked="" type="checkbox"/> |

+ -

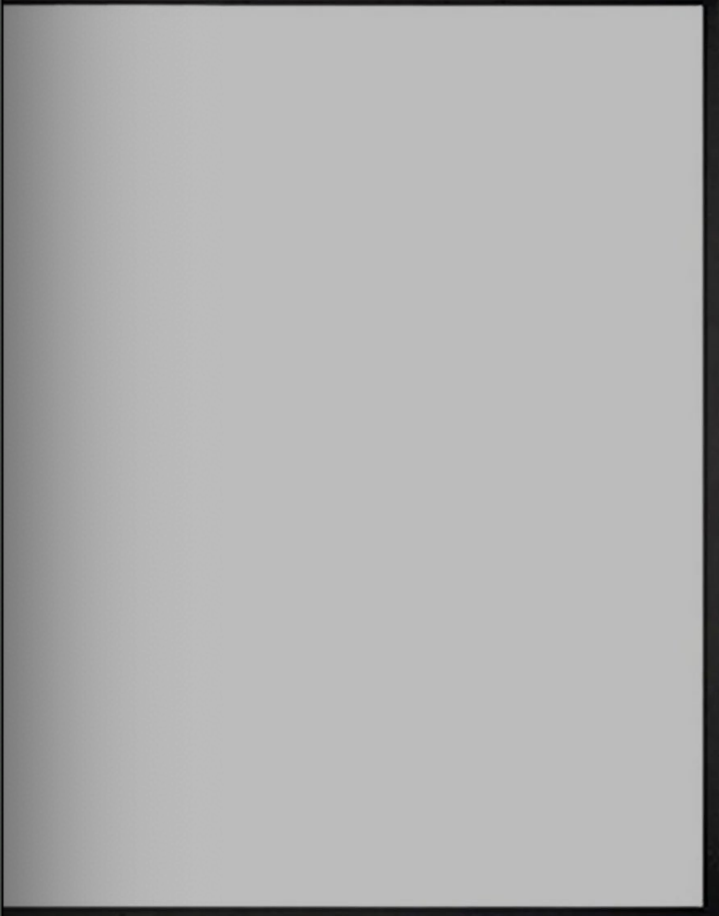
System Settings sidebar with search bar and various categories.

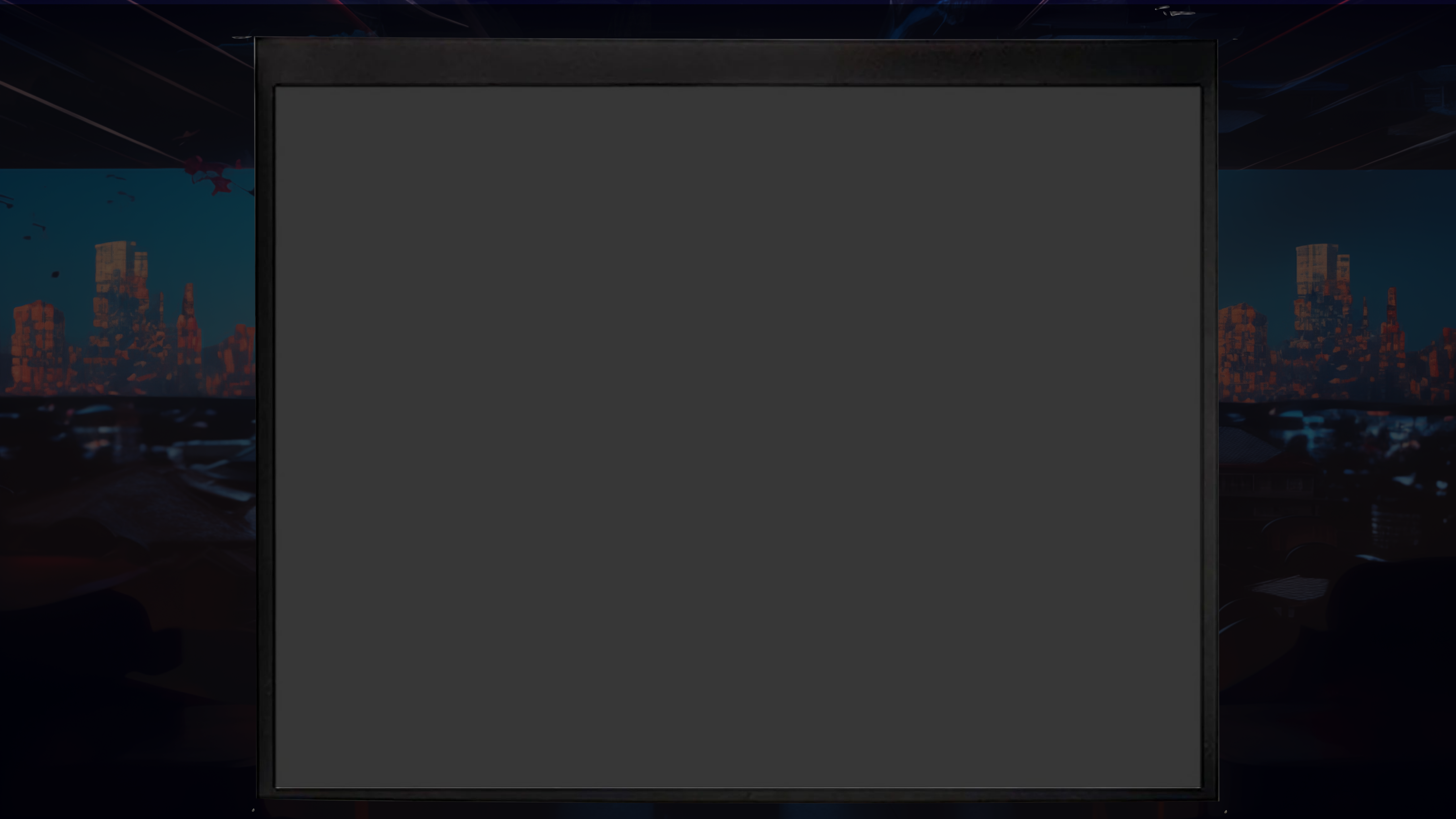
- Search
- Sound
- Focus
- Screen Time
- General
- Appearance
- Accessibility
- Control Center
- Siri & Spotlight
- Privacy & Security
- Desktop & Dock
- Displays
- Wallpaper
- Screen Saver
- Battery
- Lock Screen
- Touch ID & Password

Camera

Allow the applications below to access your camera.

Application	Camera Access
Arc	Off
Developer	Off
Firefox	Off
Microsoft Teams classic	Off
OBS	On
Parallels Desktop	Off
Raycast	On
Slack	On
zoom	On





⏏ ⏏ ⏏ ƒ3

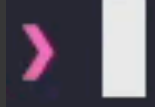
~
> file EDRConnection.xpc

⏏ ⏏ ⏏ ~#3

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

```
~  
> █
```


⏏ 4





| 4 | 2 | kTCCServiceSystemPolicyAllFiles

com.huntresslabs.www

client




```
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"  
}
```

com

4

Client

Reason


```
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"
```


A person is sitting at a desk in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible under a blue sky, with a large mountain in the distance. The scene is dimly lit, with a blue color cast. The text 'TCC' is overlaid in the center of the image.

TCC

A person is sitting in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape with tall buildings and a large mountain range is visible under a blue sky. A vertical white line runs down the center of the image, separating the text 'TCC' on the left and 'MDM' on the right.

TCC

MDM



TCC

MDM

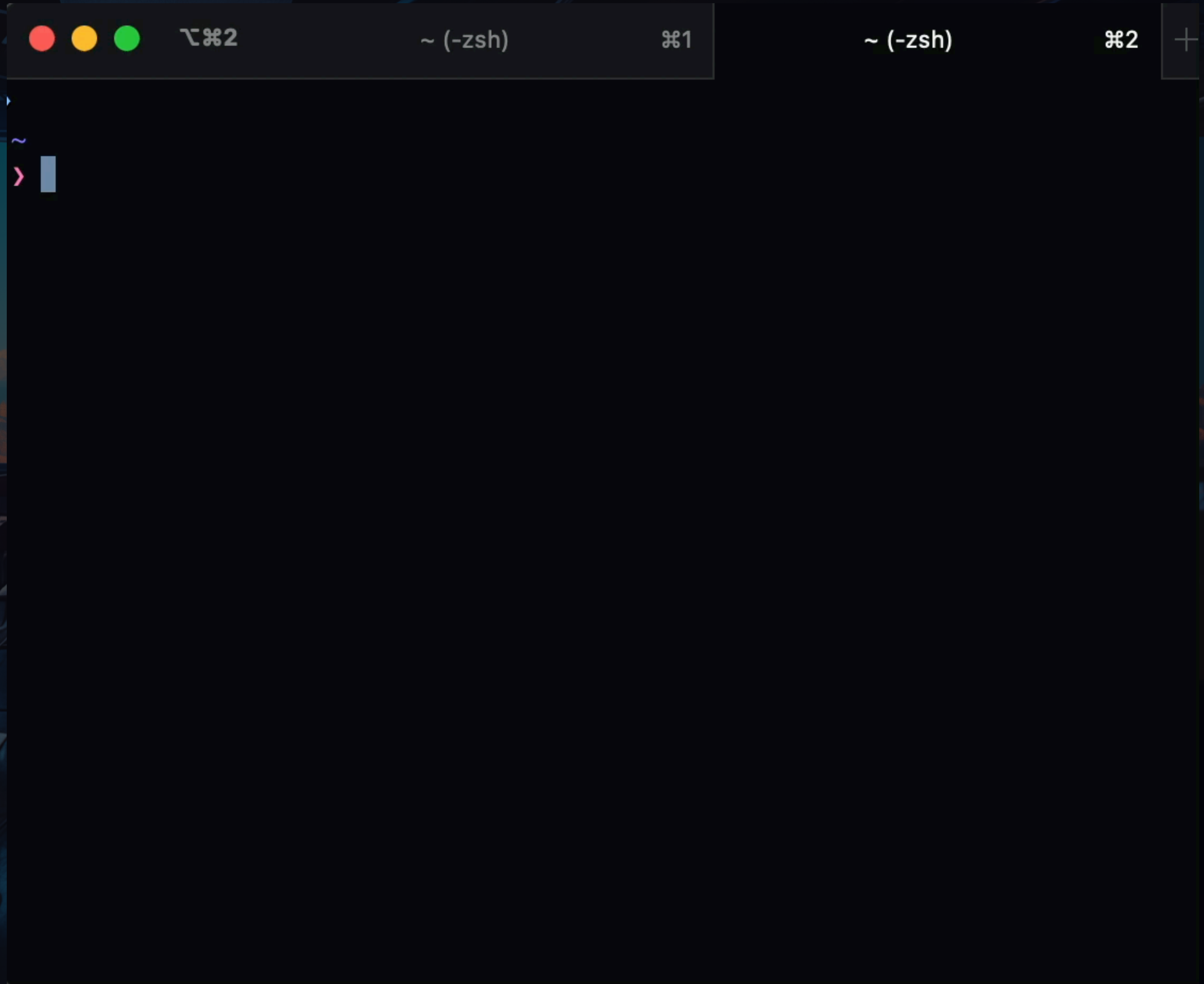
A person is sitting in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a large window shows a cityscape with a prominent mountain range under a blue sky. The scene is dimly lit, with a blue and purple color palette. A vertical white line runs down the center of the image, passing through the person's head.

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

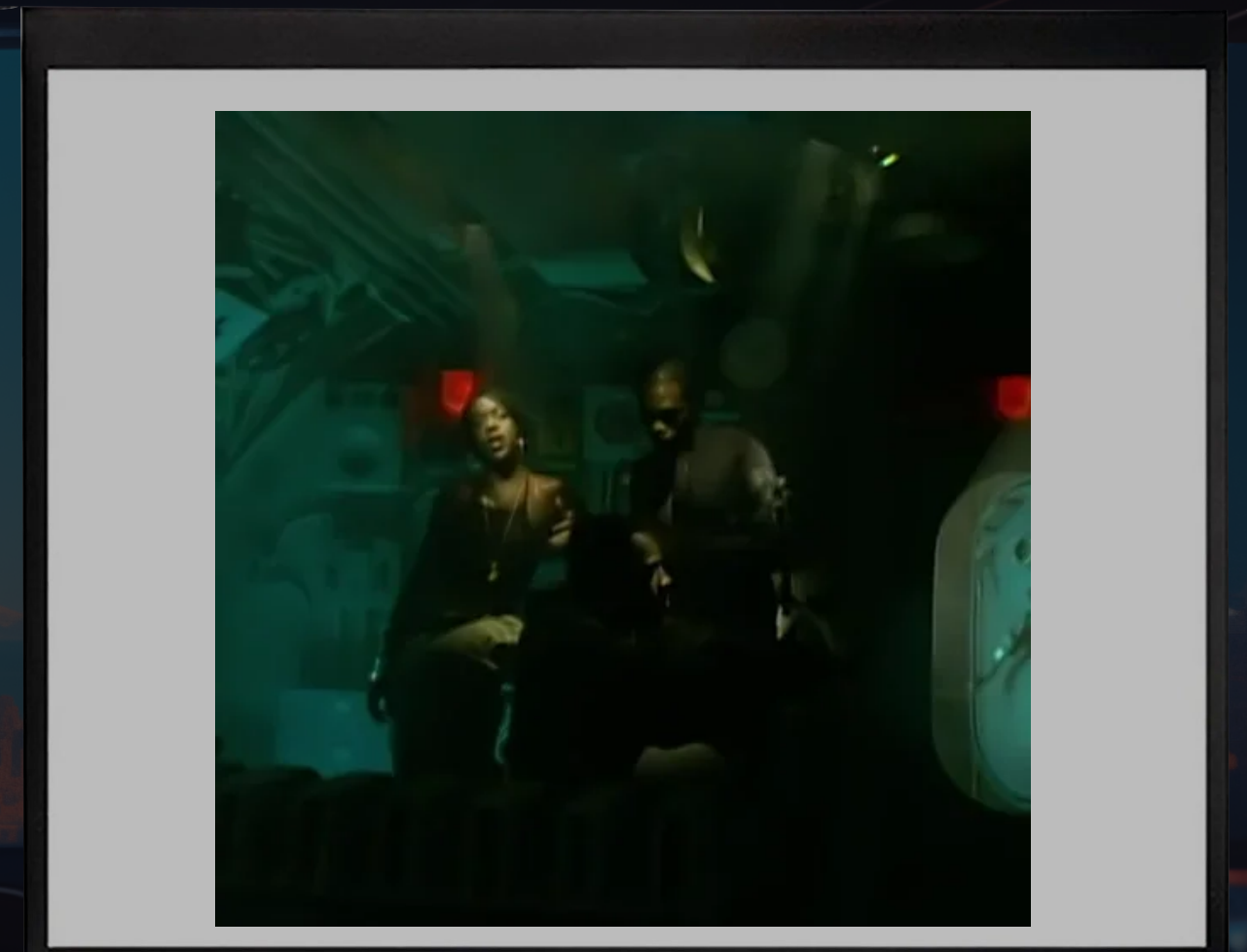
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPR



Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

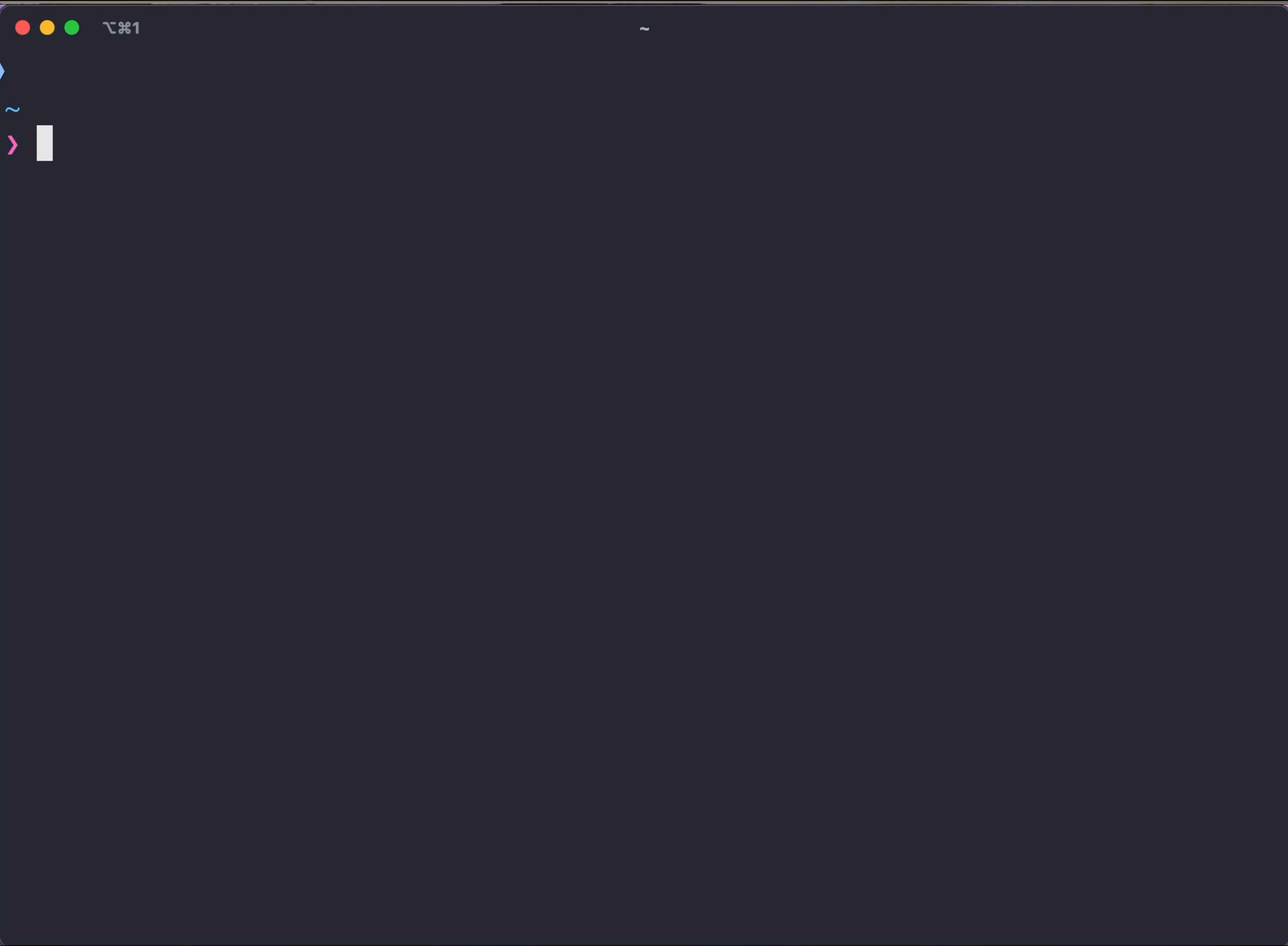
XPROTECT

XPR



A person is sitting at a desk in a classroom, viewed from behind. The classroom is filled with rows of desks and chairs. In the background, a cityscape is visible, with a large volcano in the distance. The scene is dimly lit, with a blue and orange color palette. The text 'XPROTECT' is overlaid in the center of the image.

XPROTECT

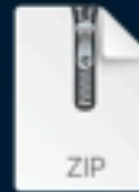


YARA

“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
```

0da916f4b5472a1
8b2598...5b.rl.zip



0da916f4b5472a1
8b2598...3325b.rl

Desktop — -zsh — 163x23

```
[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 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
```

```
XProtect_MACOS_1db9cfa 0da916f4b5472a18b2598b3b61b99447f833325b.rl
```

```
vlad@vlad Desktop % █
```



```
com.apple.quarantine 57
```

```
[vlad@vlad Desktop % unzip -P infected 0da916f4b5472a18b2598b3b61b99447f8333
```

```
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
```

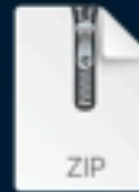
```
236954 -rw-r--r--@ 1 vlad  staff  - 87250 Mar 16 14:29 0da916f4b5472a18b2598b3b61b99447f833325b.rl
```

```
com.apple.quarantine 57
```

```
[vlad@vlad Desktop % yara -w /Library/Apple/System/Library/CoreServices/XProtect
```

```
XProtect_MACOS_1db9cfa 0da916f4b5472a18b2598b3b61b99447f833325b.rl
```

```
vlad@vlad Desktop % █
```

0da916f4b5472a1
8b2598...5b.rl.zip



0da916f4b5472a1
8b2598...3325b.rl

Desktop — -zsh — 163x23

```
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
adedDate 53
oms 1349

.zip

0da916f4b5472a18b2598b3b61b99447f833325b_rl.zip


```

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 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

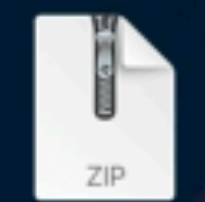
Report malware to Apple to protect other users

ZIP

0da916f4b5472a18b2598...5b.rl.zip

0da916f4b5472a18b2598...3325b.rl





Oda916f4b5472a18b2598...5b.rl.zip



Oda916f4b5472a18b2598...3325b.rl

```

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 l>
384 7C3E0000 02000000 00000000 00000000 l>

```

Signed Int | le, dec (select some data) [-] [+]

0 out of 87250 bytes

```

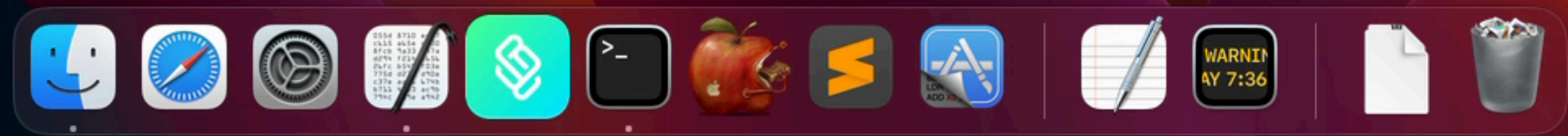
198195 -rw-r--r--
com.
22225 -rw-r--r--
236815 -rw-r--r--
com.
com.
com.
com.
vlad@vlad De
Archive: 0c
inflating:
vlad@vlad De
0da916f4b547
vlad@vlad De
236954 -rw-r--r--
com.
vlad@vlad De
XProtect_MAC
vlad@vlad De
vlad@vlad De
236954 -rw-r--r--
vlad@vlad Desktop %

```

```

Desktop -- -zsh -- 163x23
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

```





"0da916f4b5472a18b2598b3b61b99447f833325b.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

Syllabus

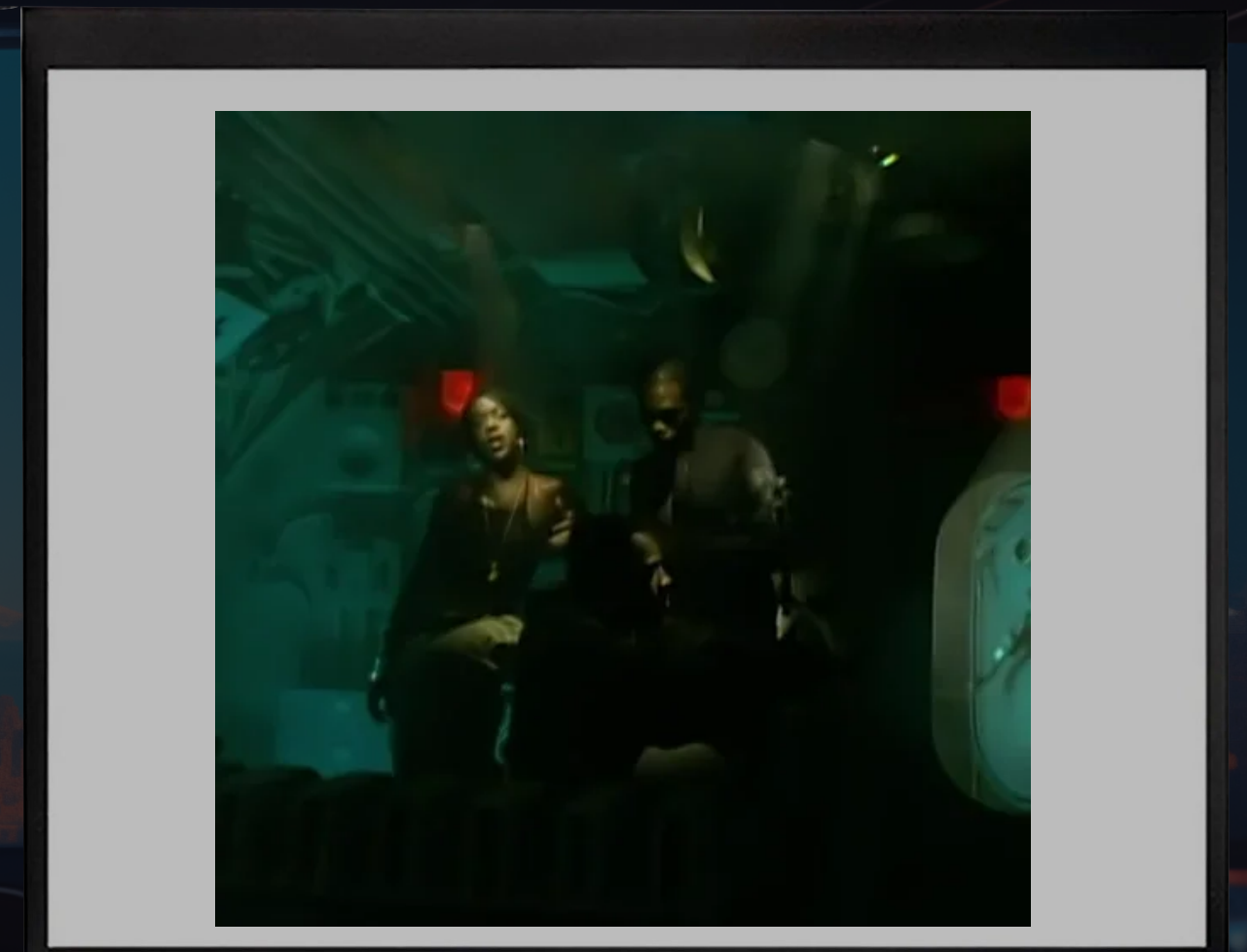
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR



Syllabus

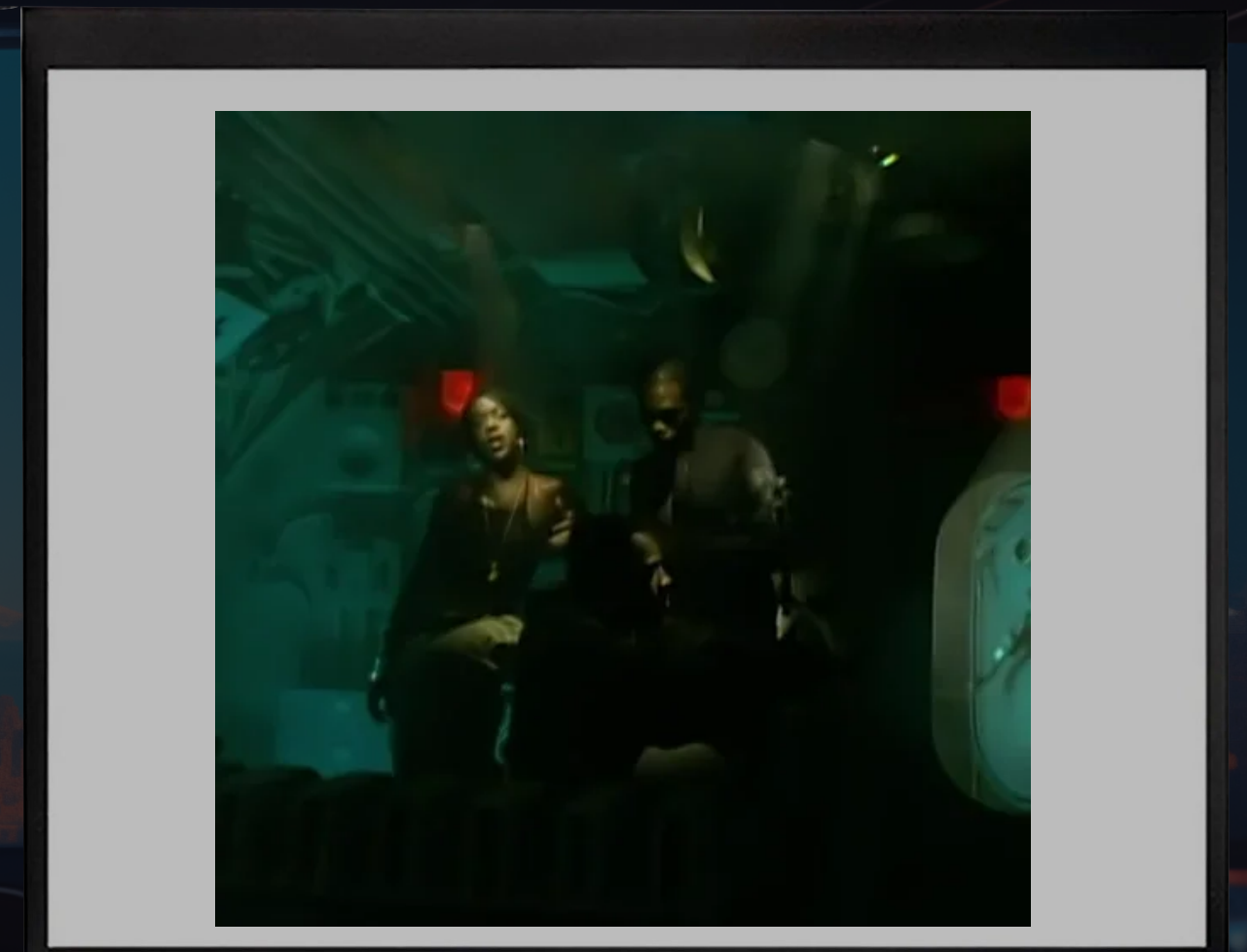
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR



Syllabus

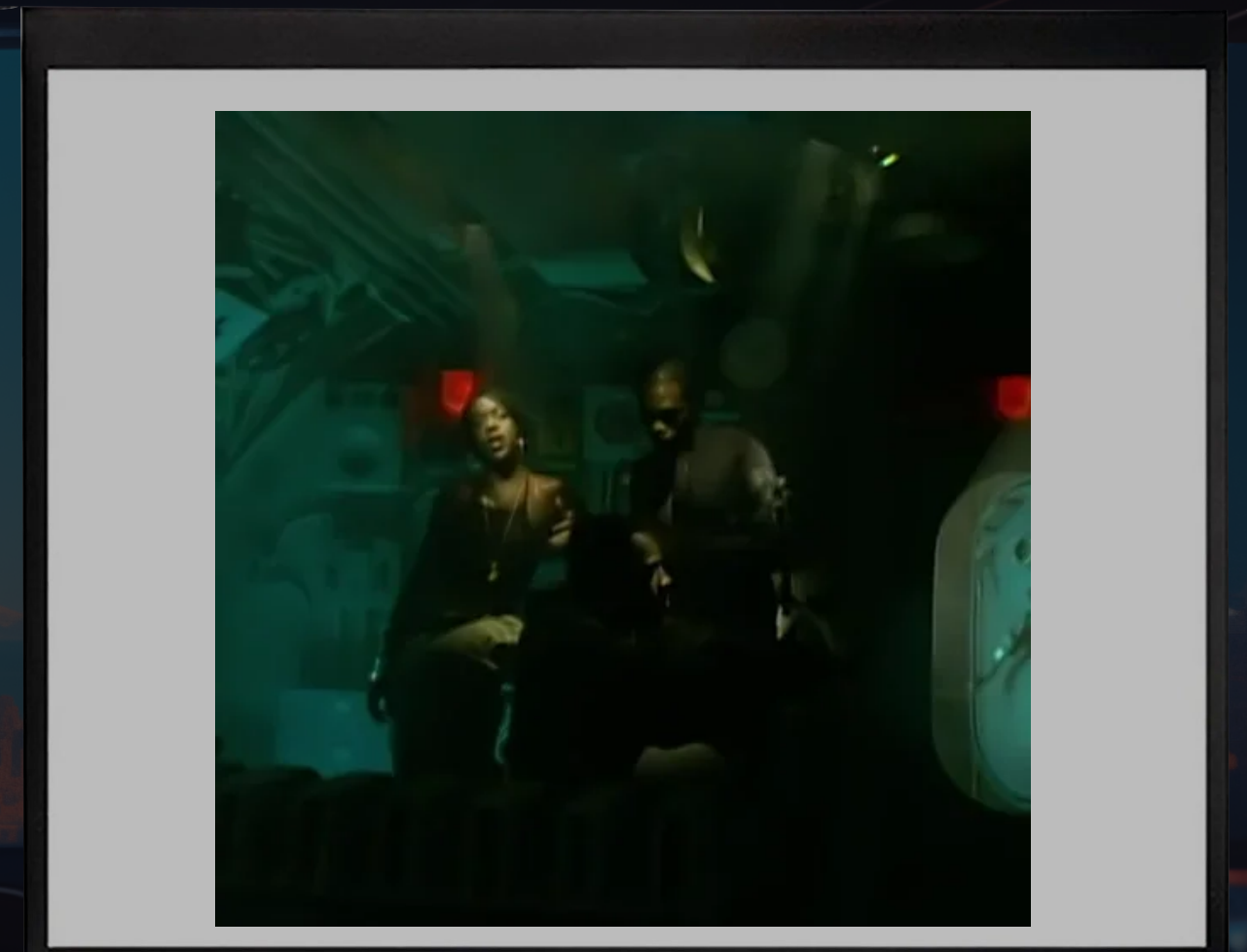
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR

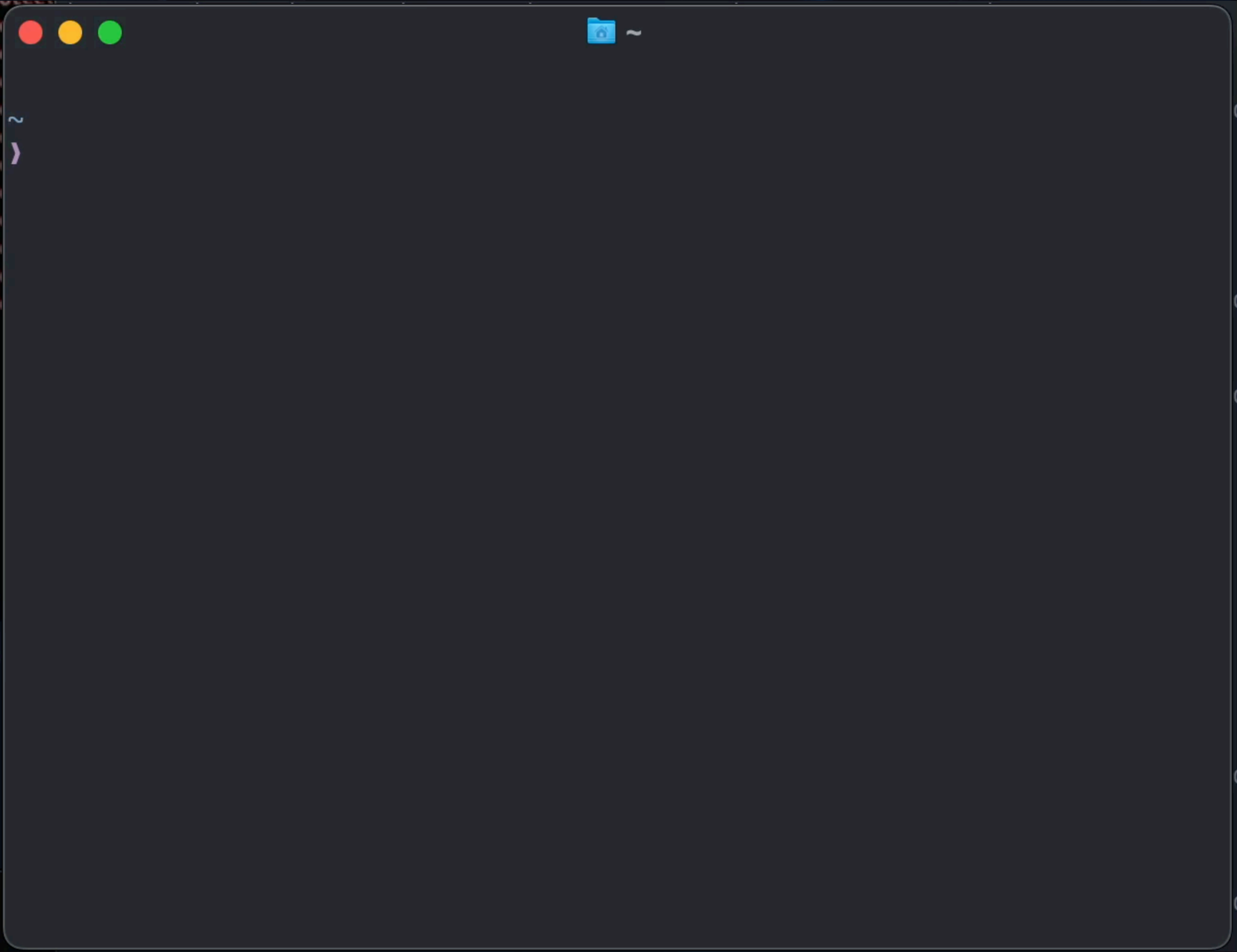




XPROTECT REMEDIATOR

A person is sitting at a desk in a classroom, looking out at a cityscape with a large mountain in the background. The scene is dimly lit, with a blue and orange color palette. The word "BASTION" is overlaid in the center in a bright blue font.

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
XProtectRemediatorTrove
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
```

100004109

return rax

100004108

data_100106c80 = &local_thread_var

mod_init_func()

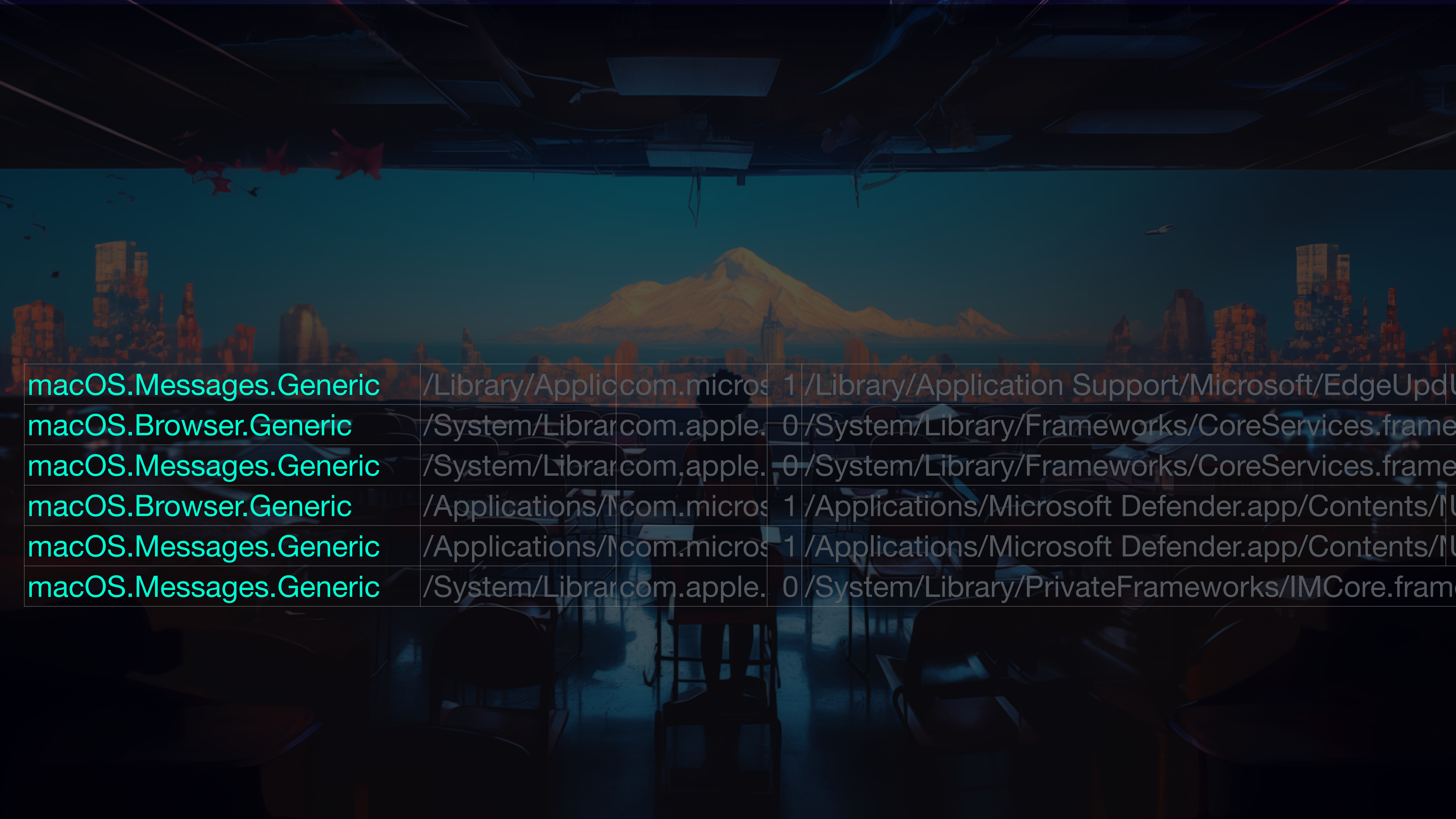
```
1 rule macos_rankstank
2 {
3     strings:
4         $injected_func = "_run_avcodec"
5         $xor_decrypt = { 80 b4 04 ?? ?? 00 00 7a }
6         $stringA = "%s/.main_storage"
7         $stringB = ".session-lock"
8         $stringC = "%s/UpdateAgent"
9     condition:
10        2 of them
11 }
```


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/Applicom.micros	1	/Library/Application Support/Microsoft/EdgeUpdU
macOS.Browser.Generic	/System/Librarcom.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Messages.Generic	/System/Librarcom.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Browser.Generic	/Applications/Mcom.micros	1	/Applications/Microsoft Defender.app/Contents/MU
macOS.Messages.Generic	/Applications/Mcom.micros	1	/Applications/Microsoft Defender.app/Contents/MU
macOS.Messages.Generic	/System/Librarcom.apple.	0	/System/Library/PrivateFrameworks/IMCore.frame



macOS.Messages.Generic	/Library/Applicom.micros	1	/Library/Application Support/Microsoft/EdgeUpdU
macOS.Browser.Generic	/System/Librarcom.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Messages.Generic	/System/Librarcom.apple.	0	/System/Library/Frameworks/CoreServices.frame
macOS.Browser.Generic	/Applications/Mcom.micros	1	/Applications/Microsoft Defender.app/Contents/MU
macOS.Messages.Generic	/Applications/Mcom.micros	1	/Applications/Microsoft Defender.app/Contents/MU
macOS.Messages.Generic	/System/Librarcom.apple.	0	/System/Library/PrivateFrameworks/IMCore.fram

macOS.Messages.Generic	/Library/Application Support/Microsoft/EdgeUpdater/118.0.2088.86/EdgeUpd
macOS.Browser.Generic	/System/Library/Frameworks/CoreServices.framework/Versions/A/Framework
macOS.Messages.Generic	/System/Library/Frameworks/CoreServices.framework/Versions/A/Framework
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	/U
macOS.Browser.Generic	/System/Library/Frameworks/CoreServices.fr	com.apple.mds	/S
macOS.Messages.Generic	/System/Library/Frameworks/CoreServices.fr	com.apple.mds	/S
macOS.Browser.Generic	/Applications/Microsoft Defender.app/Conten	com.microsoft.wdav	/U
macOS.Messages.Generic	/Applications/Microsoft Defender.app/Conten	com.microsoft.wdav	/U
macOS.Messages.Generic	/System/Library/PrivateFrameworks/IMCore.f	com.apple.imagent	/S

Syllabus

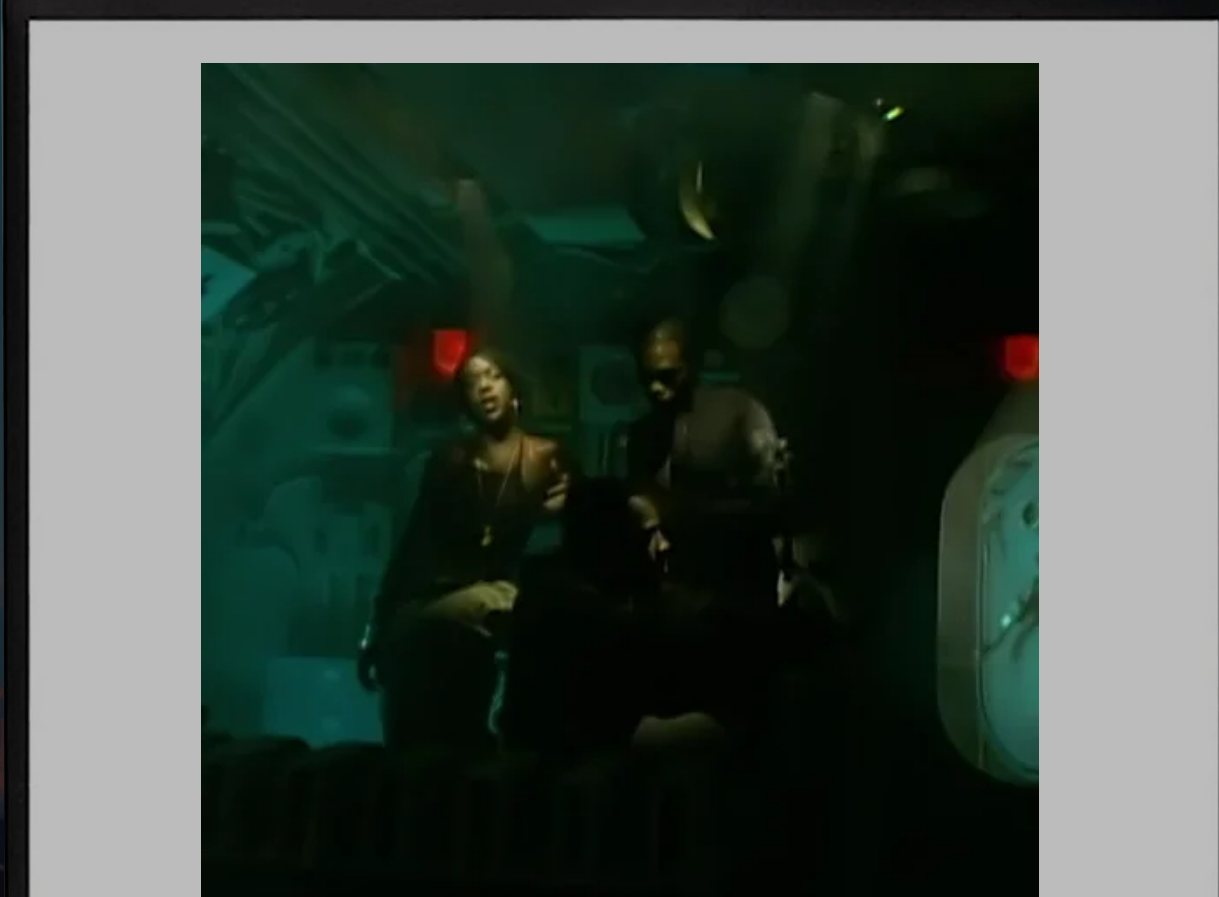
FILE QUARANTINE

GATEKEEPER

TCC

XPROTECT

XPROTECT REMEDIATOR



Syllabus

FILE QUARANTINE

GATEKEEPER

TCC

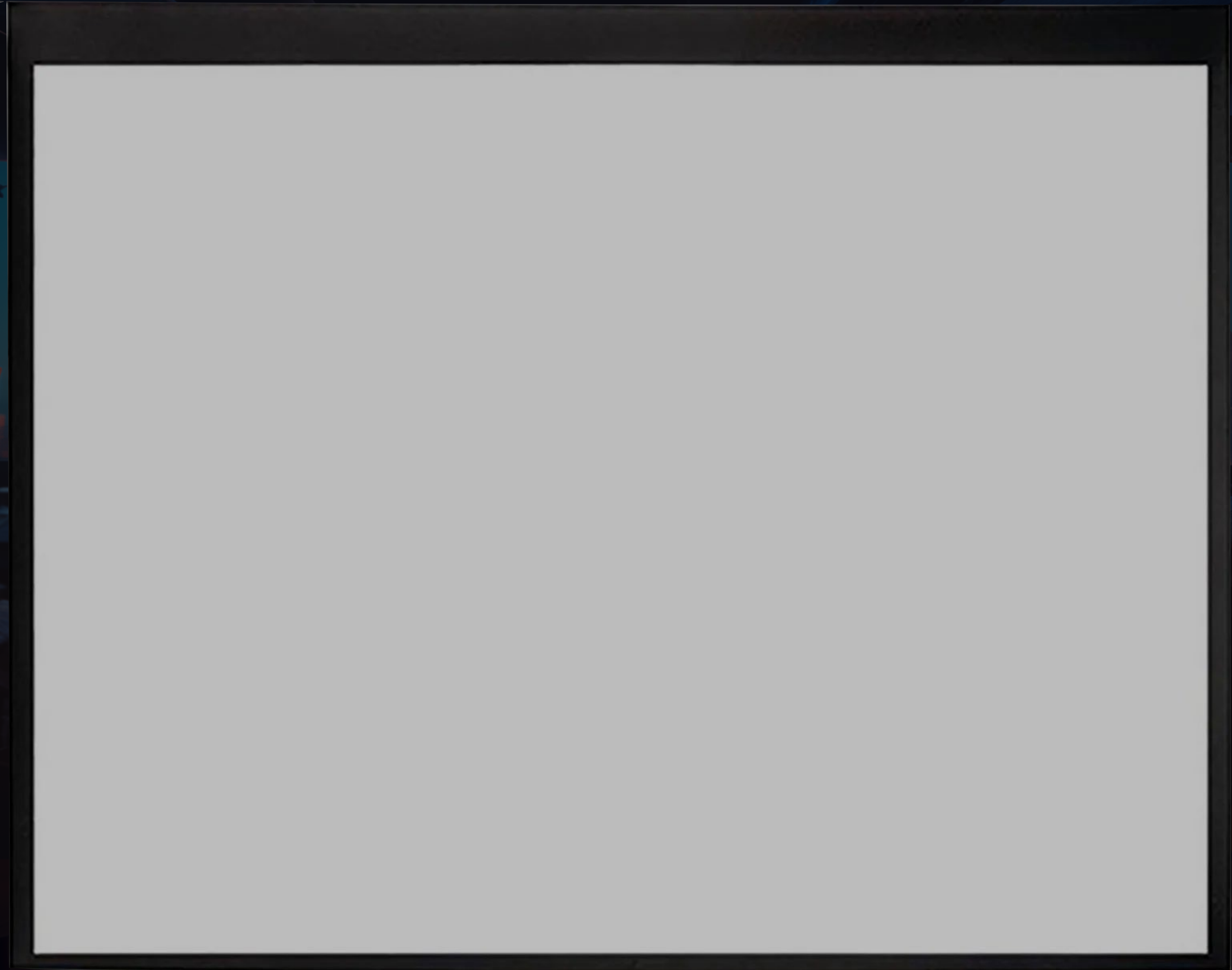
XPROTECT

XPROTECT REMEDIATOR

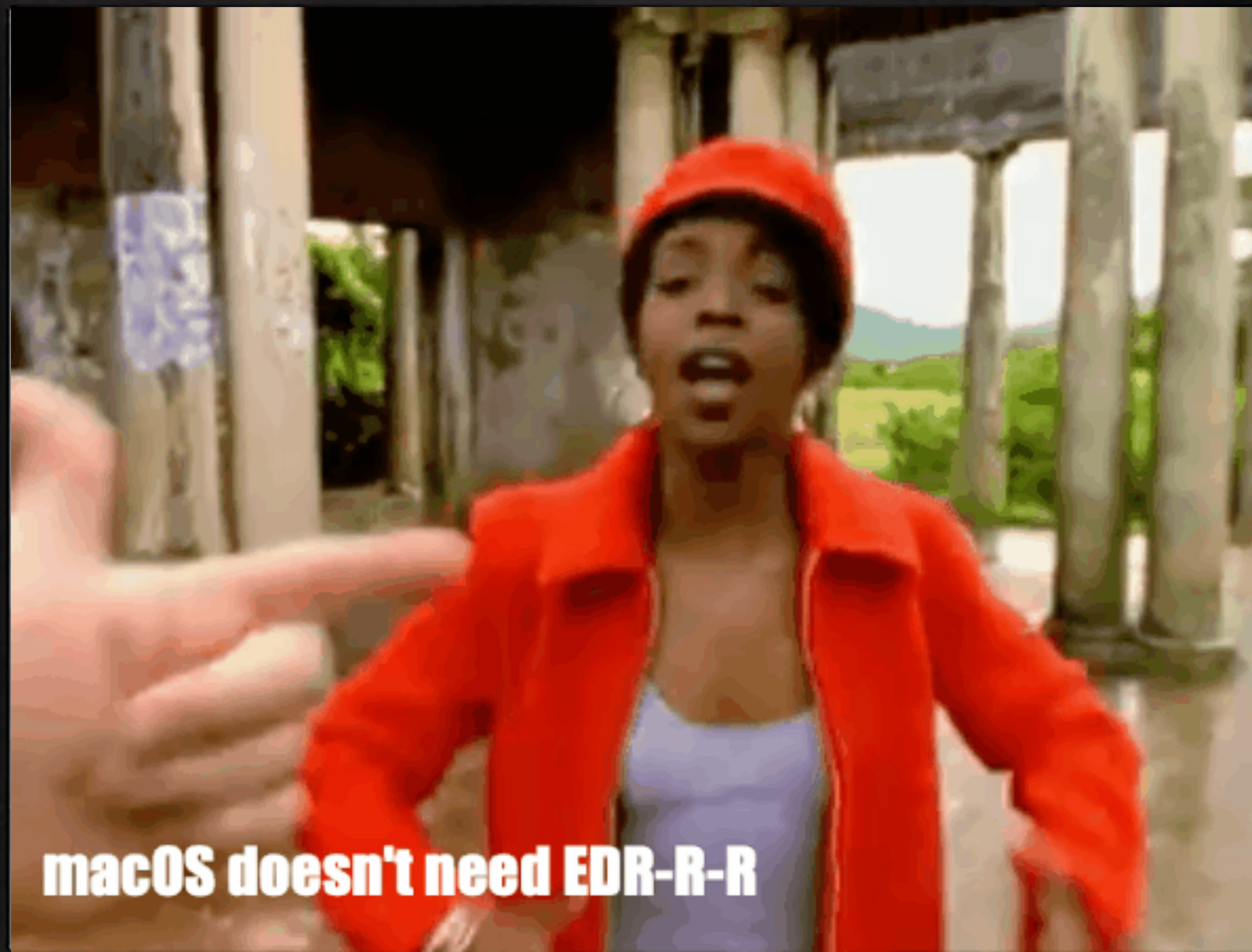


WHAT ABOUT YOU









macOS doesn't need EDR-R-R





REACTIVE



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

