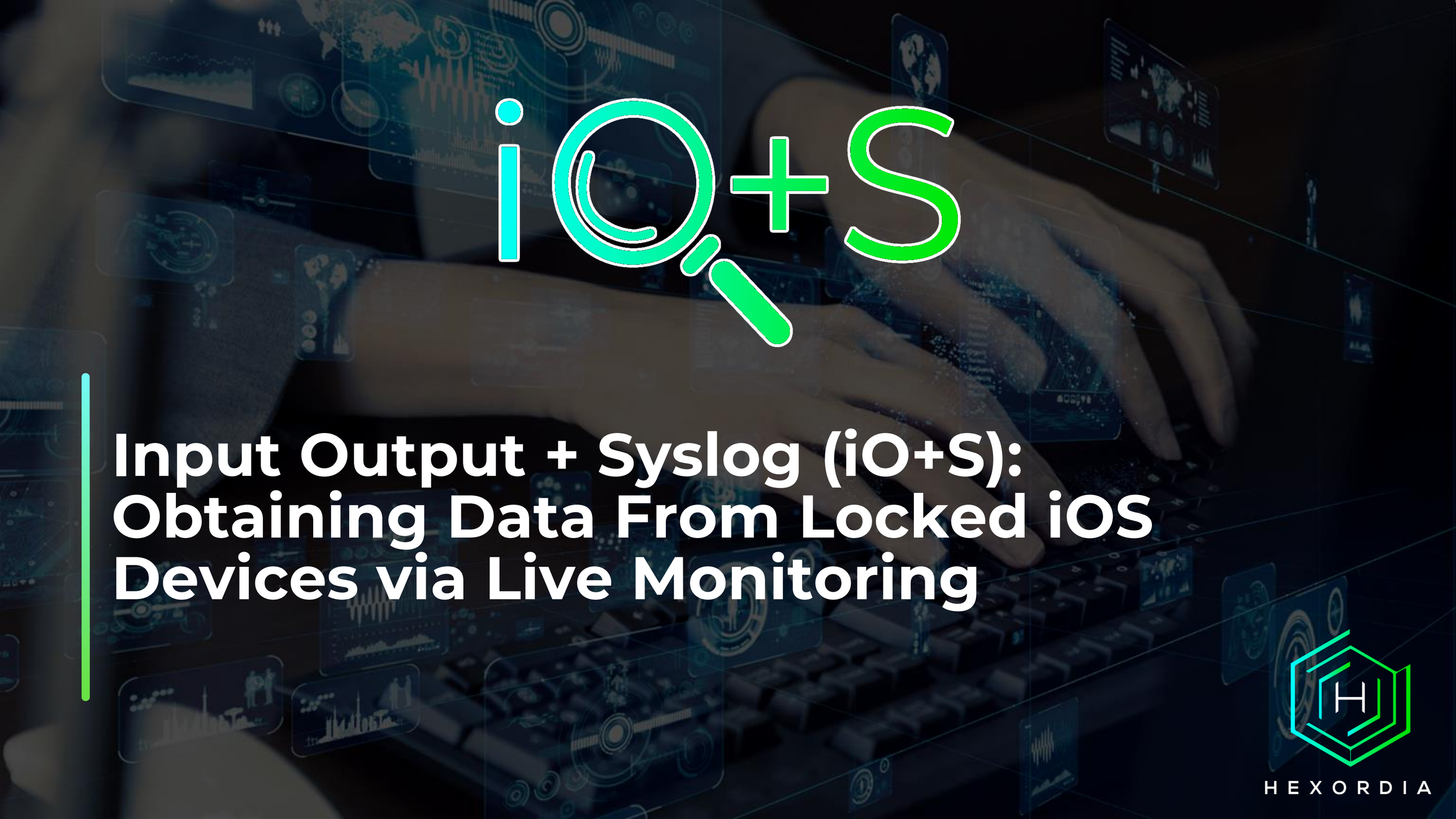


Input Output + Syslog (iO+S): Obtaining Data From Locked iOS Devices via Live Monitoring

HEXORDIA

MEET NICK

DIGITAL FORENSICS SPECIALIST & DEVELOPER, HEXORDIA

- Founder, Dragon Eye Intelligence

Previous:
- Forensics / Malware Research @ Univ. New Haven
- TikTok Research @ Penetrum

DFRWS
National Cyber Crime Conference
High Technology Crime Investigation Association

HEXORDIA

MEET JESSICA

FOUNDER & OWNER, HEXORDIA

- Adjunct Professor, George Mason University

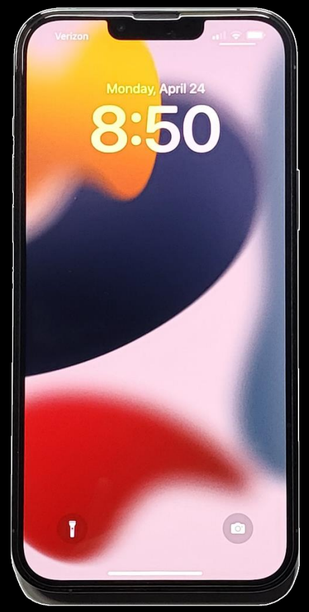
Previous:
- Director Forensics, Magnet Forensics
- Basis Technology
- Ernst and Young
- American Systems

DFIR Review, Chair
FSI: Digital Investigations, Associate Editor
HTCIA IEC, 2nd VP
SWGDE, Member
OSAC, Member

HEXORDIA

iOS Digital Forensics in 2023

HEXORDIA



Exploit
(Obtain Super User Permissions)

FFS Acquisition

No Exploit
(Average User Permissions)

Passcode / Paired PC

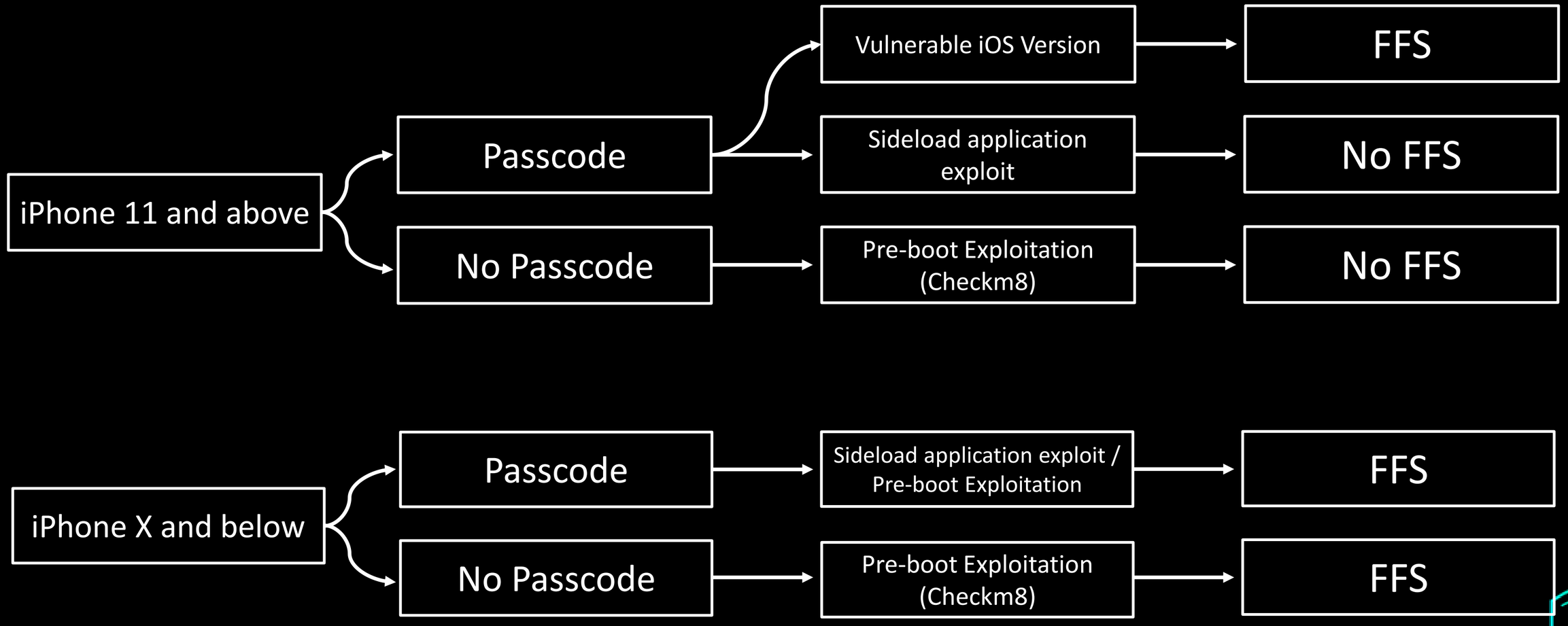
Logical Acquisition

No Passcode / Paired PC

Limited Logical Acquisition

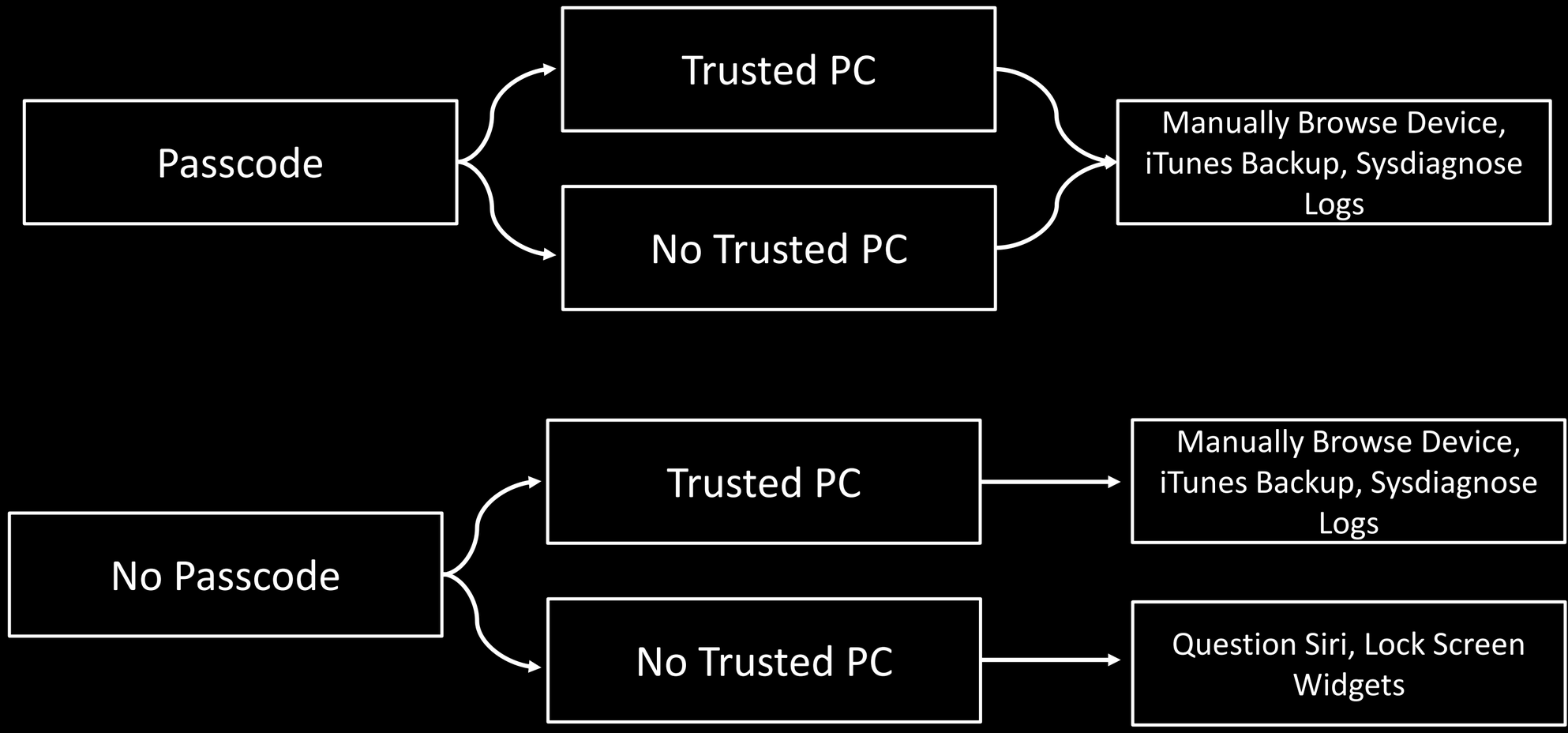
HEXORDIA

Full File System



HEXORDIA

Logical Acquisition



HEXORDIA

Device States

BFU

AFU

DFU

Diagnostics

USB RM

Trusted State

HEXORDIA

BFU (Before First Unlock)

- The state after a device reboots but before it is unlocked for the first time
- Device is protected at a deeper level until it is unlocked for the first time

HEXORDIA

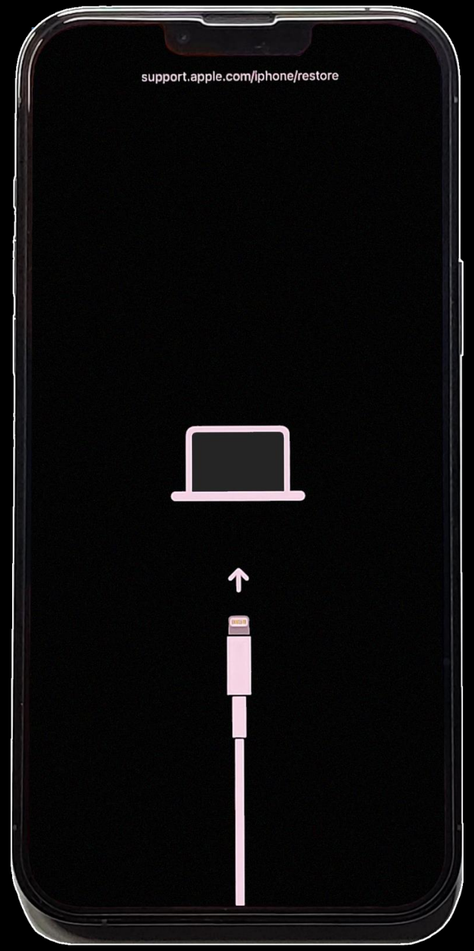
AFU (After First Unlock)

- The state after a device reboots but before it is unlocked for the first time
- Device is less protected than in BFU mode

HEXORDIA

Recovery

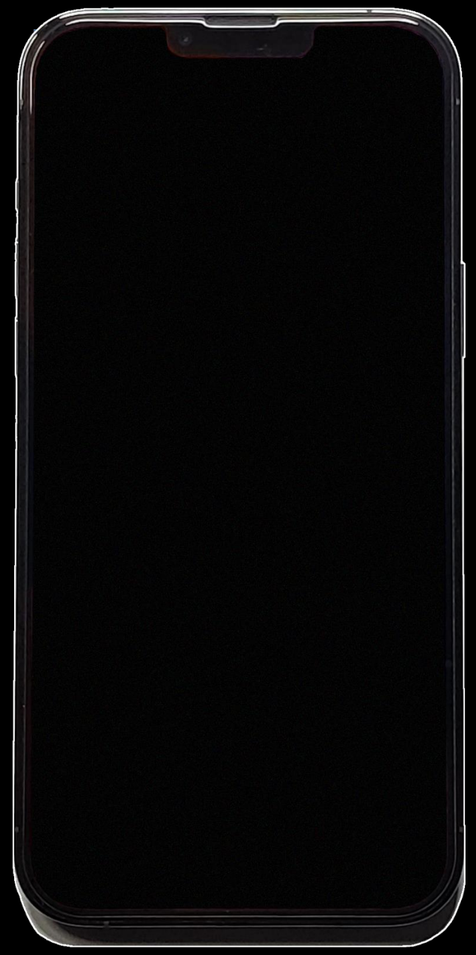
- A diagnostic mode typically used to recover from fatal booting errors
- E.g., Fix boot loops, restore / factory reset devices



HEXORDIA

DFU (Device Firmware Upgrade)

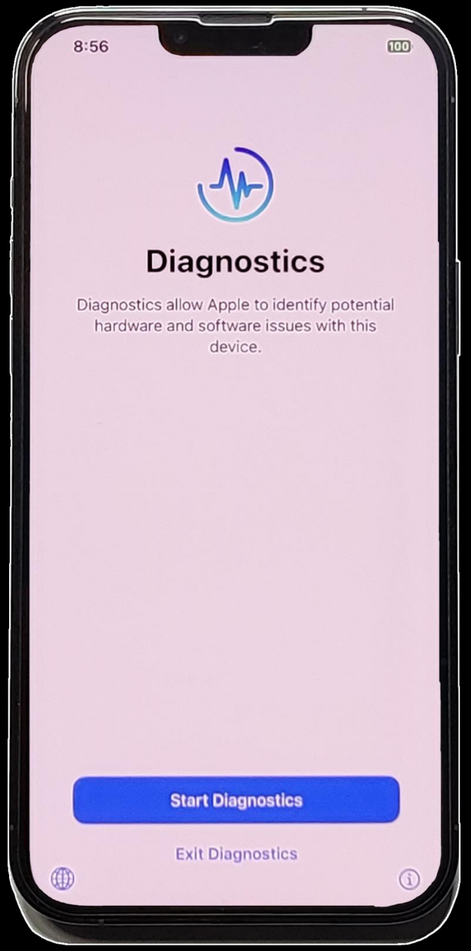
- Low-level bootrom communication tool for developers and device configurations
- Looks like device is powered off



HEXORDIA

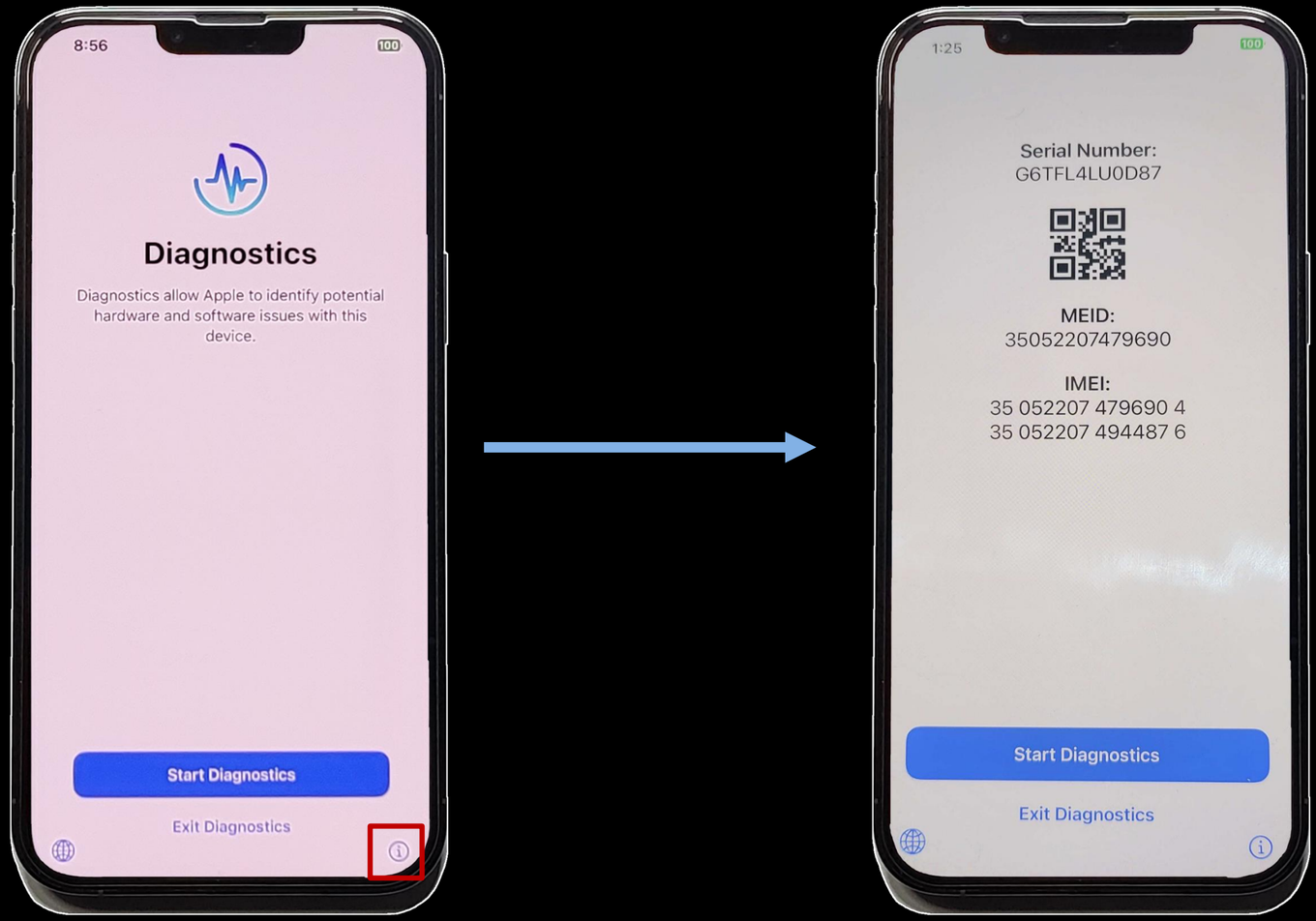
Diagnostics

- Lesser-known mode used for diagnosing hardware issues
- Users will not see anything on this page however if the device is flagged for examination apple support may gather information and view it.



HEXORDIA

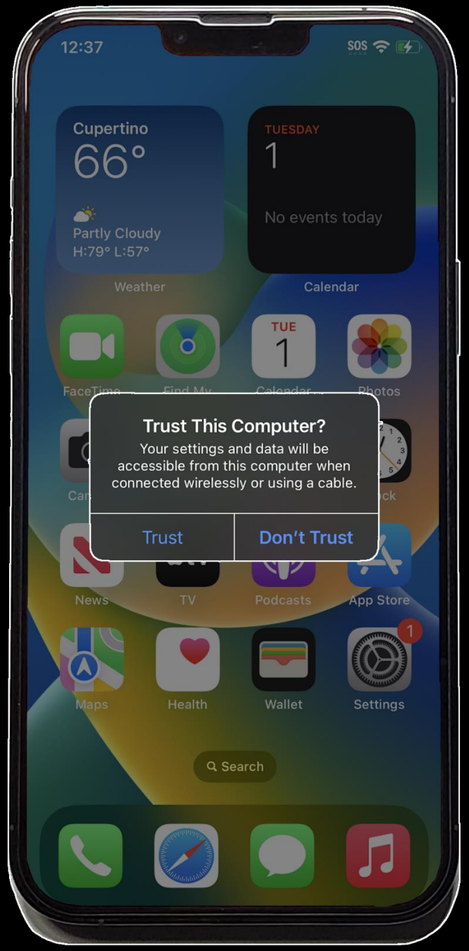
Diagnostics



HEXORDIA

Trusted State

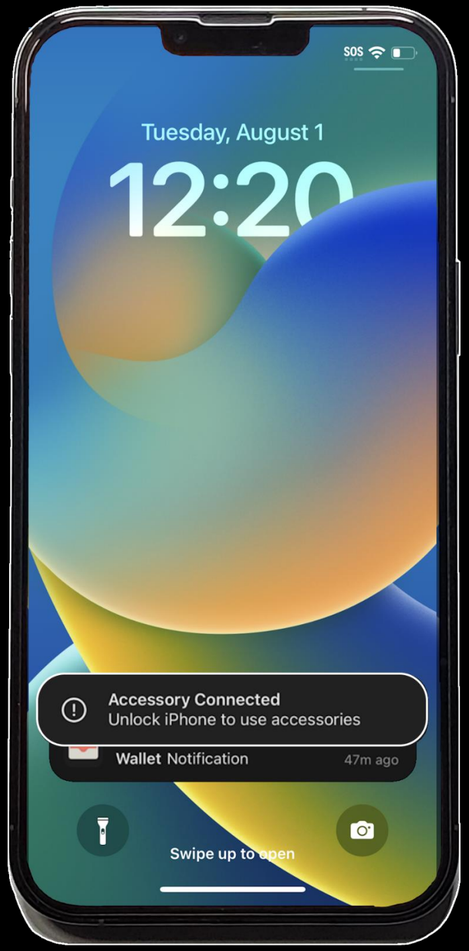
- A state in which after a reboot, SOS mode, or inactive device state the device will refuse to communicate with other devices over USB
- Required for most logical acquisition data



HEXORDIA

USB RM (USB Restricted Mode)

- A state in which after a reboot, SOS mode, or inactive device state the device will refuse to communicate with other devices over USB
- No bueno



HEXORDIA

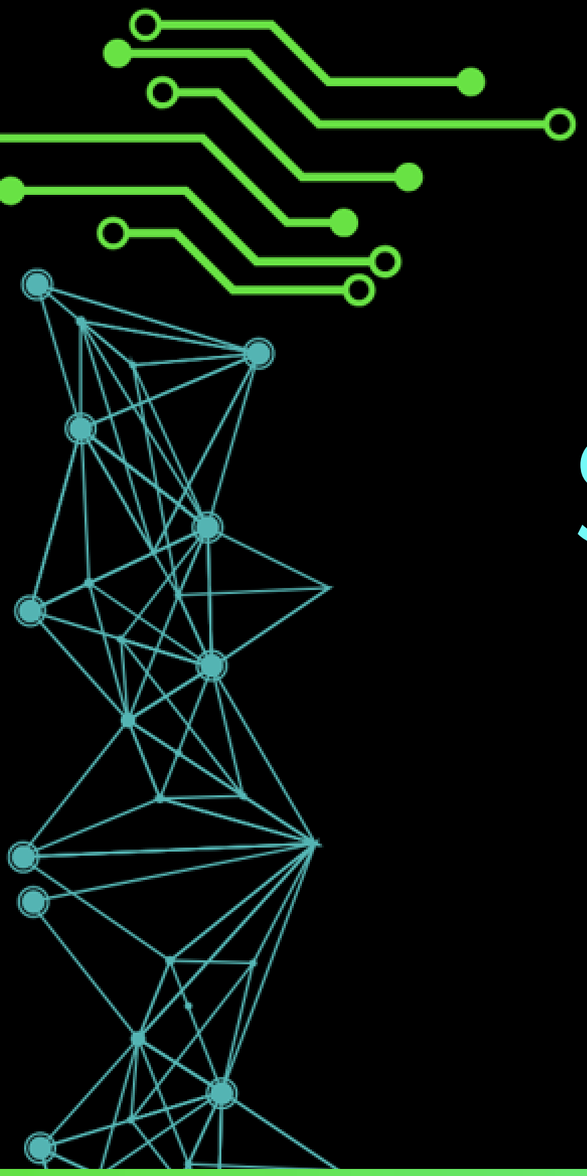
Data Sources

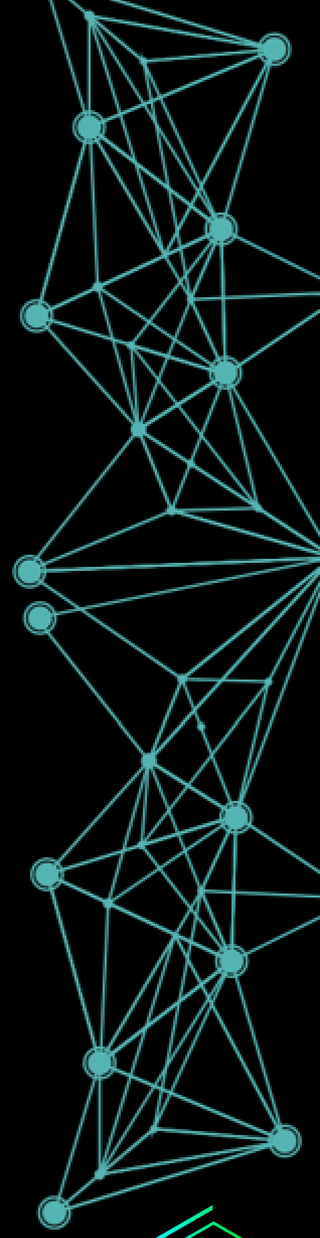
HEXORDIA

Data Source	Can we obtain it?	Is it volatile?
Data through touch UI - As presented to a normal user, many hidden developer features may be accessed through UI	Yes - Amount of data depends on if passcode is known	Somewhat
User Filesystem	Typically, yes	Somewhat
Full Filesystem (FFS)	Typically, with tooling yes - Yet this may change quickly	Somewhat
Raw HDD Data	Too encrypted to understand = useless without decryption keys	Somewhat
Warrant Returns	Yes, if we have the authority	Yes
Call Detail Records (CDR)	Yes, if we have the authority	Yes
API Scraping	Yes	Yes
Random Access Memory (RAM)	Sort of…	Yes
Peripheral Data - On-board devices such as microphone, camera	No, too volatile (With exceptions)	Extremely
Data through wired interface - Live USB / Lightning Interface Data	Yes, but only in real-time (With exceptions)	Extremely
Data through wireless networks - WiFi, Bluetooth, NFC, AirPlay, etc…	Yes, but only in real-time (With exceptions)	Extremely

HEXORDIA

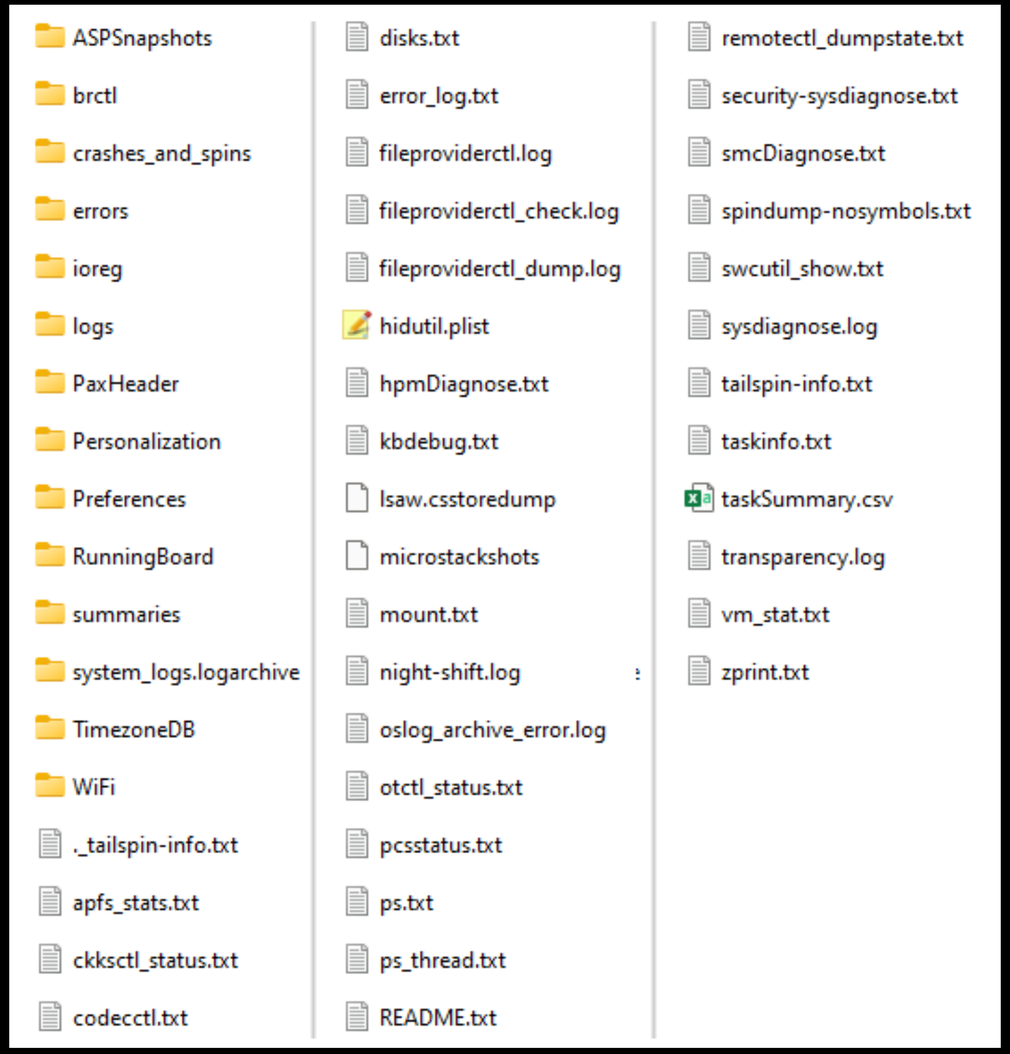
Sysdiagnose Logs





HEXORDIA

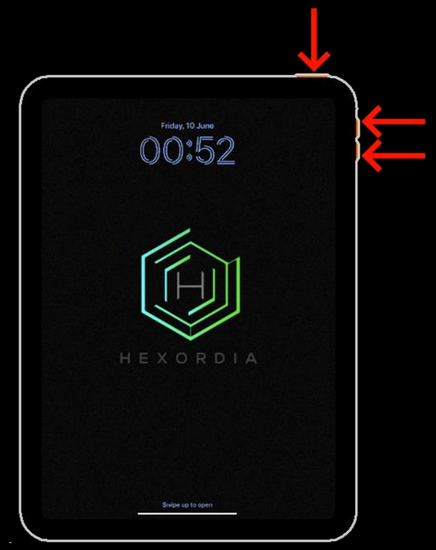
What are Sysdiagnose Logs?



HEXORDIA

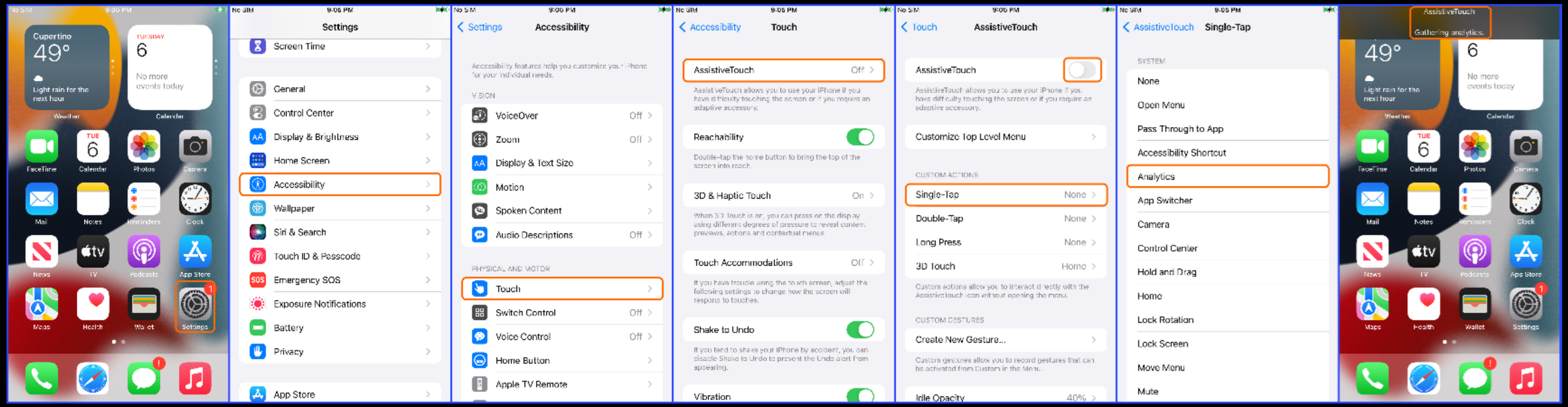
Capturing Sysdiagnose Logs

- For all iPhone / iPad devices: Hold Both Volume buttons for 1.5 seconds
- iPhone will vibrate
- iPad will not vibrate



HEXORDIA

Capturing Sysdiagnose Logs



HEXORDIA

Capturing Sysdiagnose Logs

```
iPhone:~ root# sysdiagnose -h
sysdiagnose version: 3.0 (1133.000000)
USAGE: sysdiagnose [-h] [-f results_directory] [-A archive_name] [-Q] [-b] [-p] [-d] [-X] [process_name | pid]
        -h                      Display this help.
        -v                      Enable verbose mode to display the container information as it executes.
        -f results_directory    Specify the directory where results will be stored.
        -A archive_name         Specify the name of the archive created in the results directory.
        -V volume_path          Specify the root volume for sysdiagnose to run on.
        -n                      Do not tar the resulting sysdiagnose directory.
        -k                      Do not remove the temporary directory.
        -F                      Get feedback data.
        -S                      Disable streaming to tarball.
        -u                      Disable UI feedback.
        -Q                      Skip footprint.
        -b                      Do not show a Finder window upon completion.
        -p                      Collect only time-sensitive data; disregards previous -d or -r flags.
        -P                      Do not collect time-sensitive data.
        -g                      Collect only log Generation data; disregards previous -p or -r flags.
        -G                      Do not run log generation data.
        -d                      Collect only log data; disregards previous -p or -r flags.
        -D                      Do not collect log data.
        -r                      Collect only log archive; disregards previous -p or -d flags.
        -R                      Do not collect log archive.
        [process_name | pid]    If a single process appears to be slowing down the system,
                                passing in the process name or ID as the argument gathers
                                additional process-specific diagnostic data; Specify only ONE process
                                at a time -- specifying multiple processes is not supported.
        -C, --compression type  Specify the compression type. It is an error to use this with the -n flag. Valid options are:
                                yaa: use parallel compression
                                tar: use tar compression
                                no-compression: don't compress the output. Identical to -n
                                default: will use the system default. Currently defaults to tar
```

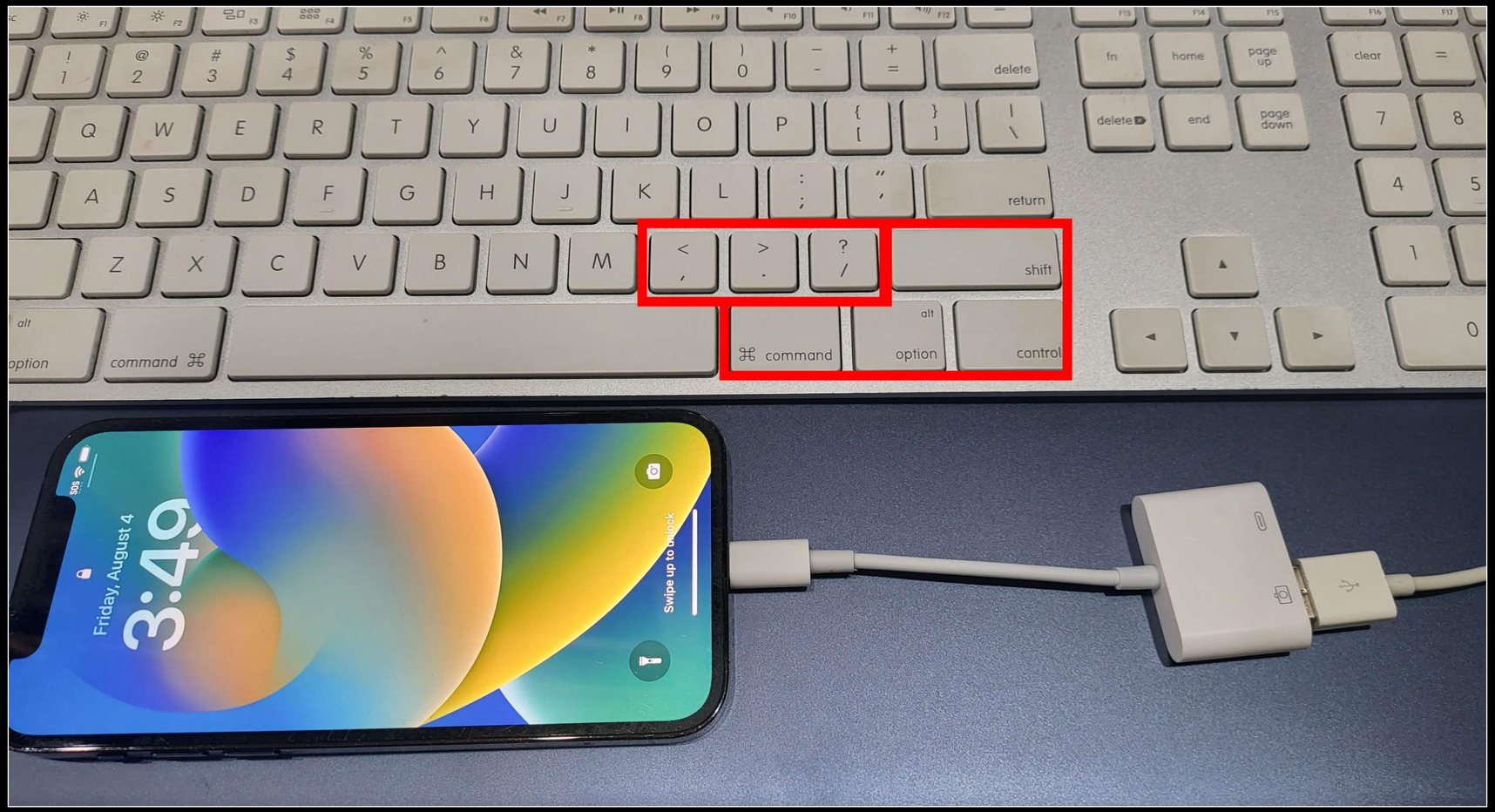
```
iPhone:~ root# sysdiagnose
This tool generates files that allow Apple to investigate issues with your
computer and help improve Apple products. The files might contain personal
information found on your device or associated with your iCloud accounts,
including but not limited to your name, serial numbers of your device,
your device name, your attached peripheral devices, your user name, your
email address and email settings, file paths, file names, Siri suggestions,
your computer's IP addresses, and network connection information.

This information is used by Apple in accordance with its privacy policy
(www.apple.com/privacy) and is not shared with any other company. By using
this tool and sending the results to Apple, you consent to Apple using the
contents of these files to improve Apple products.

Press 'Enter' to continue. Ctrl+\ to cancel.

Progress:
[|||||||||||||||||||||||||||||||||||||100%|||||||||||||||||||||||||||||||||]

Output available at '/private/var/mobile/Library/Logs/CrashReporter/DiagnosticLogs/
sysdiagnose/sysdiagnose_2023.08.02_16-50-41-0400_iPhone-OS_iPhone_20A392.tar.gz'.
```

HEXORDIA

Capturing Sysdiagnose Logs

```
DESCRIPTION:
  sysdiagnose gathers system diagnostic information helpful in investigating system performance issues.
  A great deal of information is harvested, spanning system state and configuration. The data is stored /var/tmp directory.
  sysdiagnose needs to be run as root. To cancel an in-flight sysdiagnose triggered via command line interface, press Ctrl-\.
  sysdiagnose is automatically triggered when the following key chord is pressed: Control-Option-Command-Shift-Period
WHAT sysdiagnose COLLECTS:
  - A spindump of the system
  - Several seconds of fs_usage ouput
  - Several seconds of top output
  - Data about kernel zones
  - Status of loaded kernel extensions
  - Resident memory usage of user processes
  - Recent system logs
  - A System Profiler report
  - Recent crash reports
  - Disk usage information
  - I/O Kit registry information
  - Network status
  - If a specific process is supplied as an argument, will collect:
      - A list of malloc-allocated buffers in the process's heap
      - Data about unreferenced malloc buffers in the process's memory
      - Data about the virtual memory regions allocated in the process
```

Capturing Sysdiagnose Logs



HEXORDIA

Sysdiagnose Log Contents

```
iPhone:~ root# while true; do ps -A >> ps.txt; sleep 0.1; done
```

HEXORDIA

Sysdiagnose Log Contents

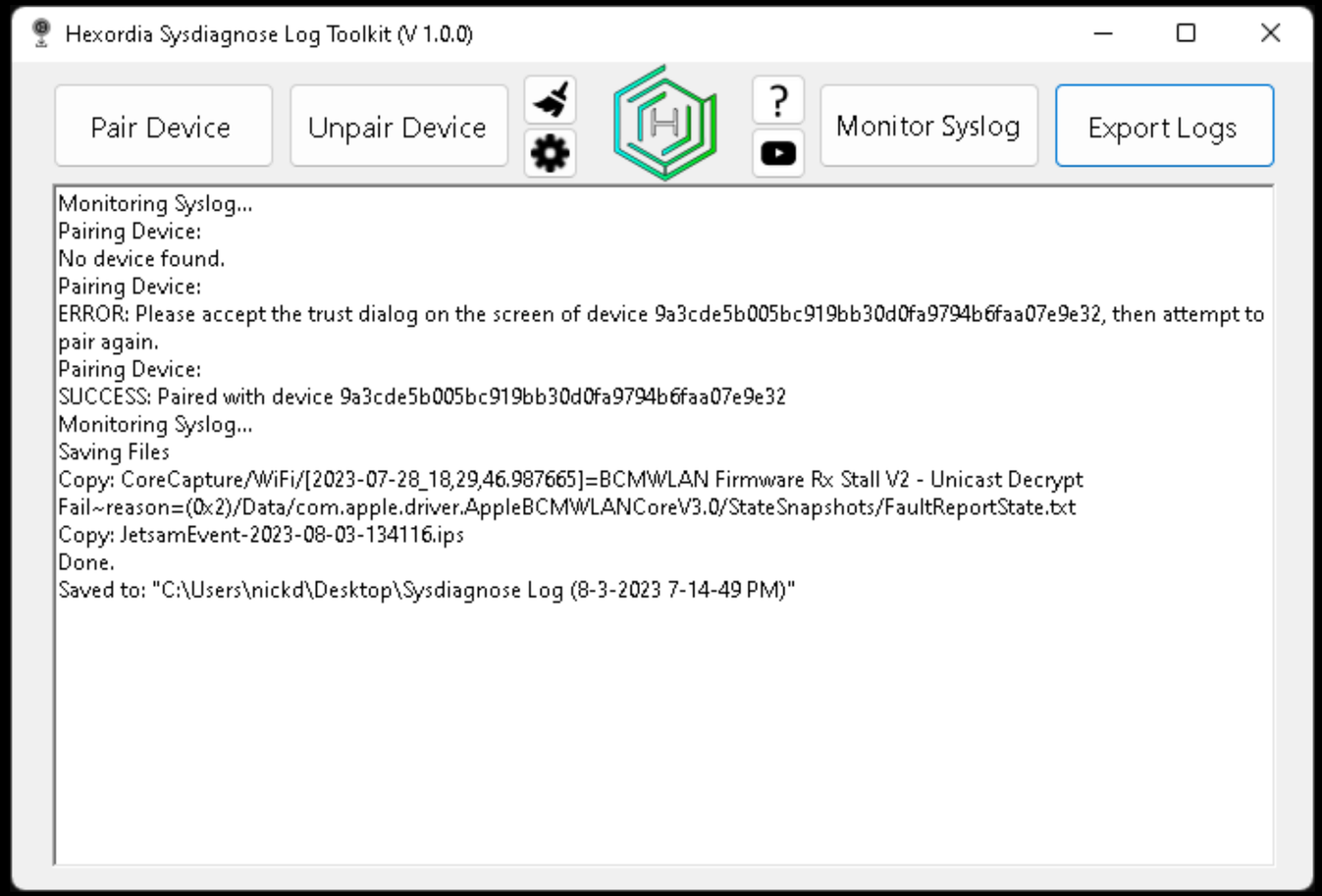
sysdiagnose
/usr/libexec/sysdiagnose_helper
/usr/sbin/spindump -oslog -notarget 2 250 -noProcessingWhileSampling -noSymbolicate -file /private/var/mobile/Library/Logs/CrashReporter/DiagnosticLogs/sysdiagnose/IN_PROGRESS_sysdiagnose_2023.08.02_21-01-23-0400_iPhone-OS_iPhone_20A392.tmp/spindump/spindump-nosymbols.txt
/bin/ps axwww -o user,uid,prsna,pid,ppid,flags,%cpu,%mem,pri,ni,vsz,rss,wchan,tt,stat,start,time,command
/usr/bin/taskinfo --threads --boosts
/usr/bin/vm_stat -c 25 0.2
/sbin/mount
/bin/df -H
/usr/bin/kbdebug
/usr/bin/zprint -t -w
/usr/libexec/smcDiagnose
/usr/local/bin/powermetrics -i 1000 --sample-count 10 --show-all --show-initial-usage --handle-invalid-values
/usr/libexec/remotectl dumpstate
/usr/bin/tbtdiagnose
/usr/bin/hpmdiagnose
/usr/bin/lsdiagnose
/usr/sbin/kextstat
/usr/local/bin/spuctl --sysdiagnose
/usr/libexec/pcsstatus --json capture output
/usr/bin/codecctl -c 1 -a
/usr/libexec/security-sysdiagnose

/usr/bin/hidutil dump
/usr/libexec/securityuploadd
/usr/sbin/ioreg -i -l -p IOService -w 0
/usr/sbin/ioreg -i -l -p IOACPIPlane -w 0
/usr/sbin/ioreg -i -l -p IOPower -w 0
/usr/sbin/ioreg -i -l -p IODeviceTree -w 0
/usr/sbin/ioreg -i -l -p IOUSB -w 0
/usr/sbin/ioreg -i -l -p IOFireWire -w 0
/usr/sbin/ioreg -i -l -p IOPort -w 0
/usr/sbin/ioreg -a -w0 -x 0
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool dbStats
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool filesystemMetadata
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool dbSchema
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool assetVersion
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool RTCGetDictionaryExtractions
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool RTCGetDictionaryInteractions
/System/Library/PrivateFrameworks/CoreSuggestions.framework/Tools/suggest_tool RTCGetDictionaryInteractionsSummary
/usr/libexec/corebrightnessdiag nightshift-internal
/usr/sbin/ckksctl status --json
/usr/sbin/otctl status --json
/System/Library/PrivateFrameworks/ZhuGeSupport.framework/XPCServices/ZhuGeService.xpc/ZhuGeService
/usr/bin/powerlogHelperd

(srsupporttool)
/System/Library/PrivateFrameworks/SharedWebCredentials.framework/Support/swcutil show --verbose
/usr/bin/fileproviderctl dump --limit-dump-size -o /private/var/mobile/Library/Logs/CrashReporter/DiagnosticLogs/sysdiagnose/IN_PROGRESS_sysdiagnose_2023.08.03_13-51-24-0400_iPhone-OS_iPhone_20A392.tmp/task_unnamed_sysdiagnose_temp.iOQyQe/fileproviderctl_dump.log
/usr/bin/brctl diagnose --sysdiagnose /private/var/mobile/Library/Logs/CrashReporter/Cloud/clouddocs_2023.08.03_13-51-40-0400
/usr/bin/brctl diagnose -c --sysdiagnose /private/var/mobile/Library/Logs/CrashReporter/Cloud/clouddocs_2023.08.03_13-51-40-0400
/usr/bin/brctl dump -i
/System/Library/PrivateFrameworks/ABMHelper.framework/Support/abm-helper
/System/Library/PrivateFrameworks/DataMigration.framework/XPCServices/com.apple.datamigrator.xpc/com.apple.datamigrator
/usr/libexec/seputil --daemonize-update-timer

HEXORDIA

Parsing Sysdiagnose – Hexordia iO+S Toolkit

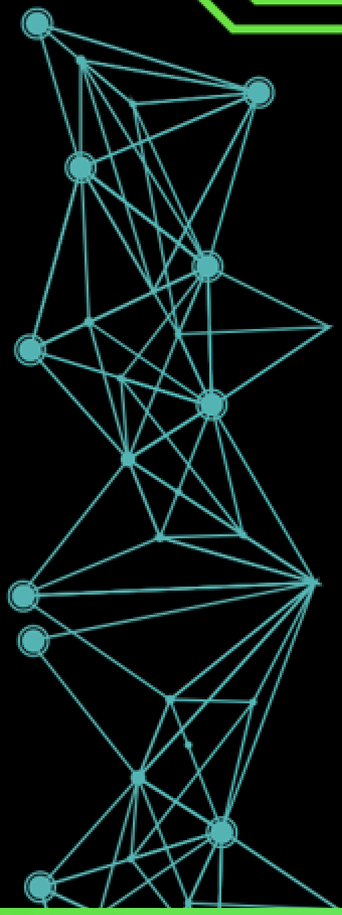


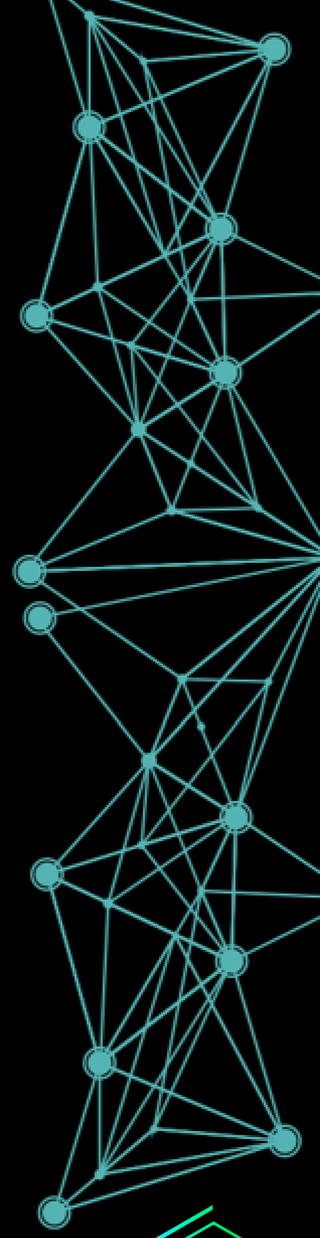
HEXORDIA

Sysdiagnose from Locked USB RM Devices?

HEXORDIA

Syslogs





HEXORDIA

What are Syslogs?

- Realtime Log
- Trust Required

```
Jul 25 14:23:01 suggestd(ProactiveHarvesting)[138] <Notice>: HVQueues: enqueueContent: <private>
Jul 25 14:23:01 suggestd(ProactiveHarvesting)[138] <Notice>: HVQueue<MailContent>: enqueueContent: writing to disk
Jul 25 14:23:01 suggestd(CoreSuggestionsInternals)[138] <Notice>: Decoded 16 of 16 items received from com.apple.mobilemail.
Jul 25 14:23:01 SpringBoard(PosterKit)[32] <Notice>: Significant event timer fired for <LegacyPoster: 0x21d8ed8c8; 63DBDF0F0FAB>
Jul 25 14:23:01 SpringBoard(PaperBoardUI)[32] <Notice>: [lock] Poster Extact update changed 131
Jul 25 14:23:01 SpringBoard(PaperBoardUI)[32] <Notice>: [home] Poster Extact update changed 131
Jul 25 14:23:01 SpringBoard(FrontBoard)[32] <Notice>: [0x2810270c0:PosterKit:45A705BC-8E9D-4DDB-A30E-63DBDF0F0FAB] Scene activity mode did change: support
 (transient).
Jul 25 14:23:01 SpringBoard(FrontBoard)[32] <Notice>: [0x2810270c0:PosterKit:45A705BC-8E9D-4DDB-A30E-63DBDF0F0FAB] Scene assertion state did change: Foreg
roundNonFocal.
Jul 25 14:23:01 SpringBoard(FrontBoard)[32] <Notice>: [xpcservice<com.apple.PaperBoard.LegacyPoster([osservice<com.apple.SpringBoard>:32])>:192] Workspace
 assertion state did change: ForegroundNonFocal (acquireAssertion = YES).
Jul 25 14:23:01 coreduetd(CoreDuet)[129] <Notice>: CDInteractionCache: New recorded interactions
Jul 25 14:23:01 coreduetd(CoreDuet)[129] <Notice>: CDInteractionCache: New recorded interactions
Jul 25 14:23:01 runningboardd(RunningBoard)[31] <Notice>: Acquiring assertion targeting [xpcservice<com.apple.PaperBoard.LegacyPoster([osservice<com.apple
.SpringBoard>:32])>:192] from originator [osservice<com.apple.SpringBoard>:32] with description <RBSAssertionDescriptor| "FBWorkspace (ForegroundNonFocal)
" ID:31-32-545 target:192 attributes:[
        <RBSDomainAttribute| domain:"com.apple.frontboard" name:"Workspace-ForegroundActive" sourceEnvironment:"(null)">,
        <RBSAcquisitionCompletionAttribute| policy:AfterApplication>,
        <RBSDomainAttribute| domain:"com.apple.frontboard" name:"Visibility" sourceEnvironment:"(null)">
        ]>
```

HEXORDIA

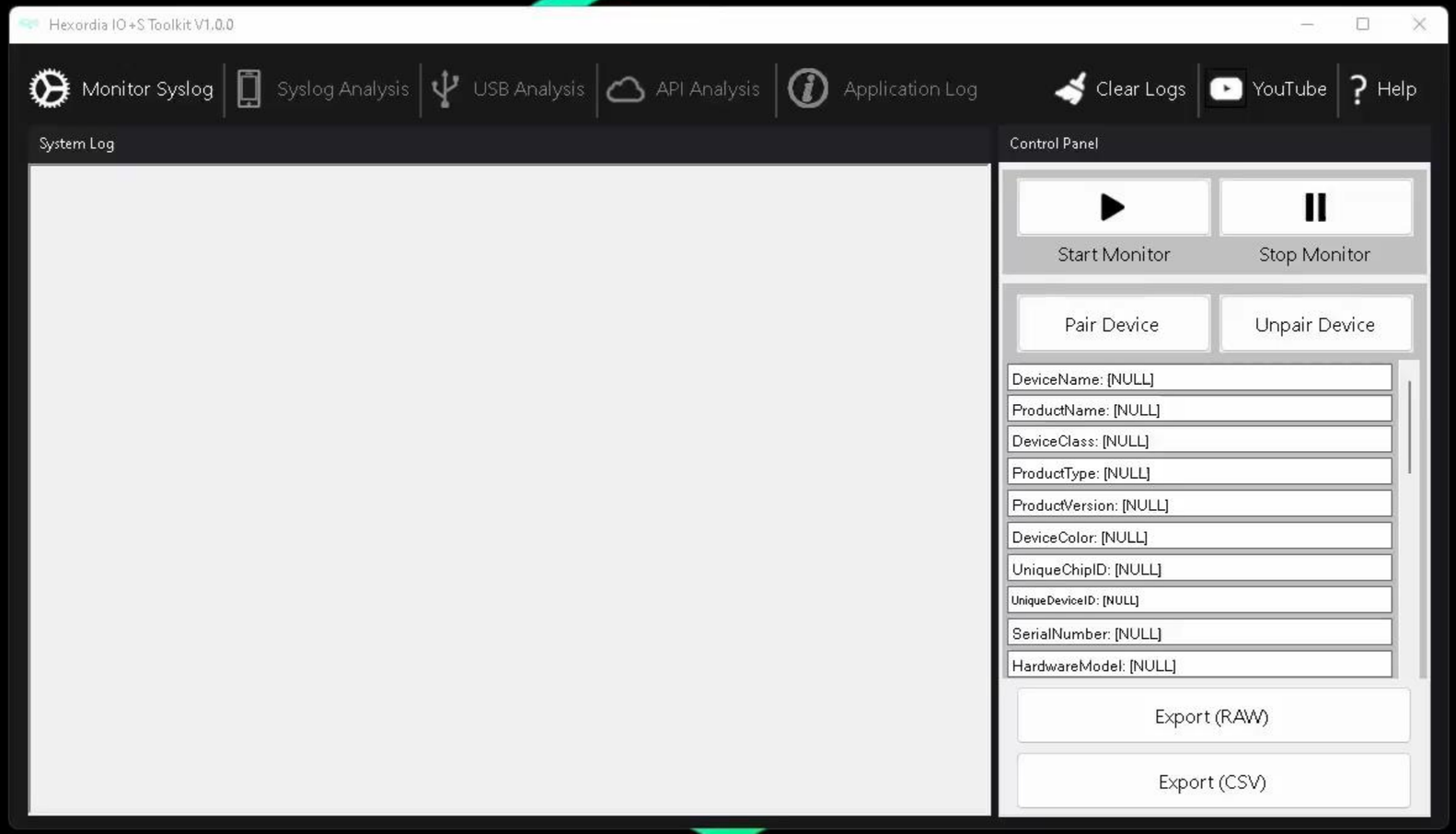
Capturing Syslogs - Libimobiledevice

- Official Source Code:
  https://github.com/libimobiledevice/libimobiledevice
- Precompiled Windows Binaries:
  https://github.com/iFred09/libimobiledevice-windows

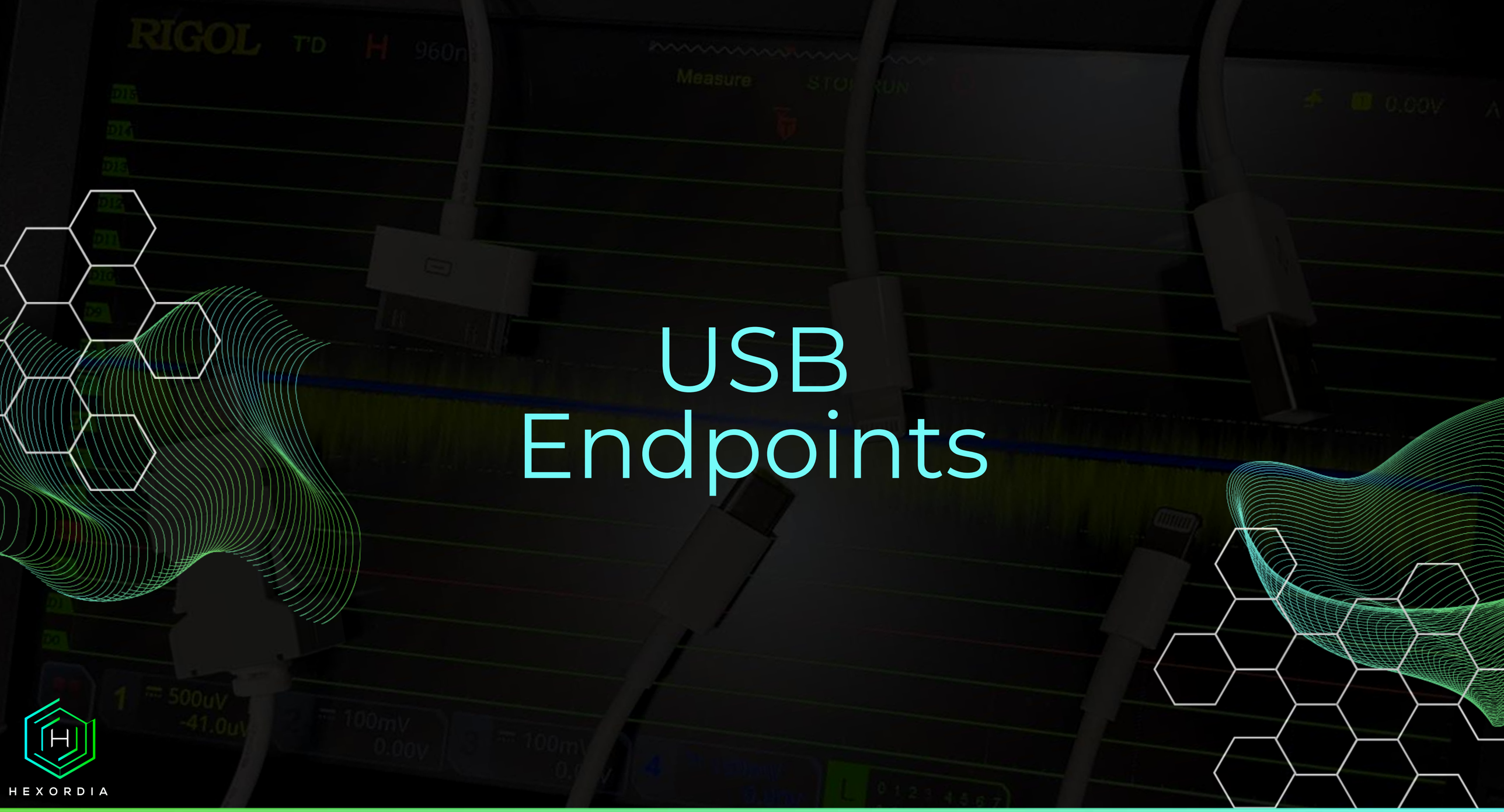
```
PS C:\Users\nickd\Desktop\libimobile> .\idevicesyslog.exe
[connected:9a3cde5b005bc919bb30d0fa9794b6faa07e9e32]
Jul 25 14:26:01 SpringBoard(CoreMotion)[32] <Notice>: [CLIoHidInterface] Property for usage pair {65280, 9}: {GyroProperties = {
    GyroFactoryMode = 0;
    GyroMeasurementRange = 2000;
    GyroXAxisOffset = 0;
    GyroYAxisOffset = 0;
    GyroZAxisOffset = 0;
}} was set successfully
Jul 25 14:26:01 backboardd(IOKit)[63] <Notice>: 0x100000536: set report interval:5000 client:801B1C8A-C6F3-4E26-A273-94A92229F97E
Jul 25 14:26:01 SpringBoard(CoreMotion)[32] <Notice>: [CLIoHidInterface] Property for usage pair {65280, 9}: {ReportInterval = 5000} was set successfully
Jul 25 14:26:01 SpringBoard(CoreMotion)[32] <Notice>: [CLIoHidInterface] Property for usage pair {65280, 9}: {GyroExtLevelTriggerSync = 0} was set success
fully
Jul 25 14:26:01 SpringBoard(CoreMotion)[32] <Notice>: [CLIoHidInterface] Property for usage pair {65280, 9}: {BatchInterval = 15000} was set successfully
Jul 25 14:26:01 SpringBoard(CoreMotion)[32] <Notice>: {"msg":"CLGyroBiasEstimatorClientRemote::registerWithGyroBiasEstimatorPrivate", "event":"activity",
"isBuildingGYTT":0, "client":"0x282c60a40", "info":"0x90ae205a8"}
Jul 25 14:26:01 backboardd(IOKit)[63] <Notice>: 0x100000536: set batch interval:15000 client:801B1C8A-C6F3-4E26-A273-94A92229F97E
Jul 25 14:26:01 SpringBoard(LocationSupport)[32] <Notice>: {"msg":"Sending cached messages to daemon", "event":"activity"}
```

Capture & Parse Syslog IO+S Toolkit

HEXORDIA


Hexordia IO+S Toolkit V1.0.0
Monitor Syslog
Syslog Analysis
USB Analysis
API Analysis
Application Log
Clear Logs
YouTube
Help
System Log
Control Panel
Start Monitor
Stop Monitor
Pair Device
Unpair Device
DeviceName: [NULL]
ProductName: [NULL]
DeviceClass: [NULL]
ProductType: [NULL]
ProductVersion: [NULL]
DeviceColor: [NULL]
UniqueChipID: [NULL]
UniqueDeviceID: [NULL]
SerialNumber: [NULL]
HardwareModel: [NULL]
Export (RAW)
Export (CSV)

USB Endpoints

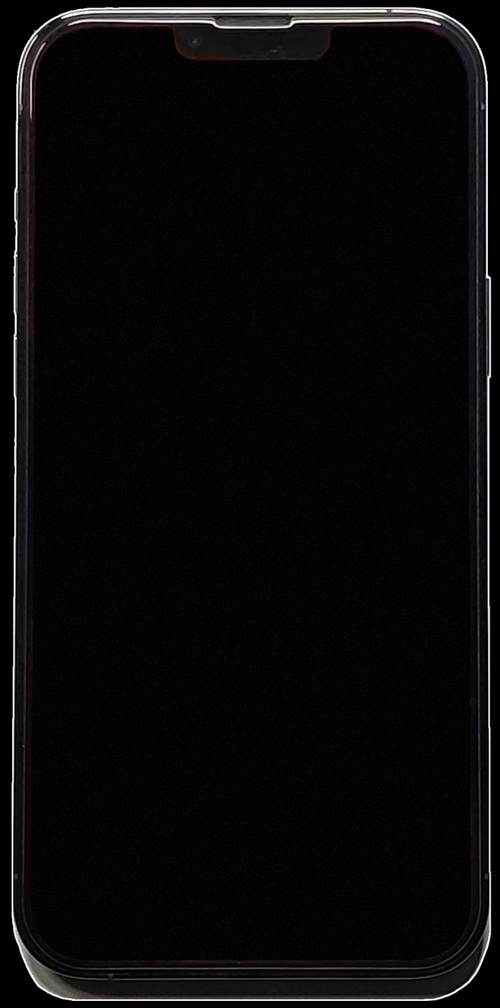


HEXORDIA

USB Endpoints

iPhone X

iOS 16.0.3 (20A392)



HEXORDIA

USB Endpoints (Normal Device State)

```
INTERFACE 0: Image ===================================
  bLength         : 0x9 (9 bytes)
  bDescriptorType : 0x4 Interface
  bInterfaceNumber : 0x0
  bAlternateSetting : 0x0
  bNumEndpoints   : 0x3
  bInterfaceClass : 0x6 Image
  bInterfaceSubClass : 0x1
  bInterfaceProtocol : 0x1
  iInterface      : 0xe PTP
   ENDPOINT 0x2: Bulk OUT ==============================
    bLength         : 0x7 (7 bytes)
    bDescriptorType : 0x5 Endpoint
    bEndpointAddress : 0x2 OUT
    bmAttributes    : 0x2 Bulk
    wMaxPacketSize  : 0x200 (512 bytes)
    bInterval       : 0x0
   ENDPOINT 0x81: Bulk IN ==============================
    bLength         : 0x7 (7 bytes)
    bDescriptorType : 0x5 Endpoint
    bEndpointAddress : 0x81 IN
    bmAttributes    : 0x2 Bulk
    wMaxPacketSize  : 0x200 (512 bytes)
    bInterval       : 0x0
   ENDPOINT 0x83: Interrupt IN ==========================
    bLength         : 0x7 (7 bytes)
    bDescriptorType : 0x5 Endpoint
    bEndpointAddress : 0x83 IN
    bmAttributes    : 0x3 Interrupt
    wMaxPacketSize  : 0x40 (64 bytes)
    bInterval       : 0xa
CONFIGURATION 2: 500 mA ==================================
  bLength         : 0x9 (9 bytes)
  bDescriptorType : 0x2 Configuration
  wTotalLength    : 0x95 (149 bytes)
  bNumInterfaces  : 0x3
  bConfigurationValue : 0x2
  iConfiguration  : 0x6 iPod USB Interface
  bmAttributes    : 0xc0 Self Powered
  bMaxPower       : 0xfa (500 mA)
   INTERFACE 0: Audio ==================================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x0
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x0
    bInterfaceClass : 0x1 Audio
    bInterfaceSubClass : 0x1
    bInterfaceProtocol : 0x0
    iInterface      : 0x0
   INTERFACE 1: Audio ===================================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x1
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x0
    bInterfaceClass : 0x1 Audio
    bInterfaceSubClass : 0x2
    bInterfaceProtocol : 0x0
    iInterface      : 0x0
   INTERFACE 1, 1: Audio ================================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x1
    bAlternateSetting : 0x1
    bNumEndpoints   : 0x1
    bInterfaceClass : 0x1 Audio
    bInterfaceSubClass : 0x2
    bInterfaceProtocol : 0x0
    iInterface      : 0x0
     ENDPOINT 0x81: Isochronous IN =======================
      bLength         : 0x9 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x81 IN
      bmAttributes    : 0x1 Isochronous
      wMaxPacketSize  : 0xc0 (192 bytes)
      bInterval       : 0x4
   INTERFACE 2: Human Interface Device ==================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x2
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x1
    bInterfaceClass : 0x3 Human Interface Device
    bInterfaceSubClass : 0x0
    bInterfaceProtocol : 0x0
    iInterface      : 0x0
     ENDPOINT 0x83: Interrupt IN =========================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x83 IN
      bmAttributes    : 0x3 Interrupt
      wMaxPacketSize  : 0x40 (64 bytes)
      bInterval       : 0x1
CONFIGURATION 3: 500 mA ==================================
  bLength         : 0x9 (9 bytes)
  bDescriptorType : 0x2 Configuration
  wTotalLength    : 0x3e (62 bytes)
  bNumInterfaces  : 0x2
  bConfigurationValue : 0x3
  iConfiguration  : 0x7 PTP + Apple Mobile Device
  bmAttributes    : 0xc0 Self Powered
  bMaxPower       : 0xfa (500 mA)
   INTERFACE 0: Image ==================================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x0
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x3
    bInterfaceClass : 0x6 Image
    bInterfaceSubClass : 0x1
    bInterfaceProtocol : 0x1
    iInterface      : 0xe PTP
     ENDPOINT 0x2: Bulk OUT ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x2 OUT
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x81: Bulk IN ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x81 IN
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x83: Interrupt IN ==========================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x83 IN
      bmAttributes    : 0x3 Interrupt
      wMaxPacketSize  : 0x40 (64 bytes)
      bInterval       : 0xa
   INTERFACE 1: Vendor Specific =========================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x1
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x2
    bInterfaceClass : 0xff Vendor Specific
    bInterfaceSubClass : 0xfe
    bInterfaceProtocol : 0x2
    iInterface      : 0xf Apple USB Multiplexor
     ENDPOINT 0x4: Bulk OUT ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x4 OUT
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x85: Bulk IN ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x85 IN
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
CONFIGURATION 4: 500 mA ==================================
  bLength         : 0x9 (9 bytes)
  bDescriptorType : 0x2 Configuration
  wTotalLength    : 0x75 (117 bytes)
  bNumInterfaces  : 0x3
  bConfigurationValue : 0x4
  iConfiguration  : 0x8 PTP + Apple Mobile Device + Apple USB Ethernet
  bmAttributes    : 0xc0 Self Powered
  bMaxPower       : 0xfa (500 mA)
   INTERFACE 0: Image ==================================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x0
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x3
    bInterfaceClass : 0x6 Image
    bInterfaceSubClass : 0x1
    bInterfaceProtocol : 0x1
    iInterface      : 0xe PTP
     ENDPOINT 0x2: Bulk OUT ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x2 OUT
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x81: Bulk IN ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x81 IN
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x83: Interrupt IN ==========================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x83 IN
      bmAttributes    : 0x3 Interrupt
      wMaxPacketSize  : 0x40 (64 bytes)
      bInterval       : 0xa
   INTERFACE 1: Vendor Specific =========================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x1
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x2
    bInterfaceClass : 0xff Vendor Specific
    bInterfaceSubClass : 0xfe
    bInterfaceProtocol : 0x2
    iInterface      : 0xf Apple USB Multiplexor
     ENDPOINT 0x4: Bulk OUT ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x4 OUT
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x85: Bulk IN ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x85 IN
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
   INTERFACE 2: Vendor Specific =========================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x2
    bAlternateSetting : 0x0
    bNumEndpoints   : 0x0
    bInterfaceClass : 0xff Vendor Specific
    bInterfaceSubClass : 0xfd
    bInterfaceProtocol : 0x1
    iInterface      : 0x11 AppleUSBEthernet
   INTERFACE 2, 1: Vendor Specific ======================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x2
    bAlternateSetting : 0x1
    bNumEndpoints   : 0x2
    bInterfaceClass : 0xff Vendor Specific
    bInterfaceSubClass : 0xfd
    bInterfaceProtocol : 0x1
    iInterface      : 0x11 AppleUSBEthernet
     ENDPOINT 0x86: Bulk IN ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x86 IN
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x5: Bulk OUT ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x5 OUT
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
   INTERFACE 2, 2: Vendor Specific ======================
    bLength         : 0x9 (9 bytes)
    bDescriptorType : 0x4 Interface
    bInterfaceNumber : 0x2
    bAlternateSetting : 0x2
    bNumEndpoints   : 0x2
    bInterfaceClass : 0xff Vendor Specific
    bInterfaceSubClass : 0xfd
    bInterfaceProtocol : 0x1
    iInterface      : 0x11 AppleUSBEthernet
     ENDPOINT 0x86: Bulk IN ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x86 IN
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
     ENDPOINT 0x5: Bulk OUT ==============================
      bLength         : 0x7 (7 bytes)
      bDescriptorType : 0x5 Endpoint
      bEndpointAddress : 0x5 OUT
      bmAttributes    : 0x2 Bulk
      wMaxPacketSize  : 0x200 (512 bytes)
      bInterval       : 0x0
======================================================
```

HEXORDIA

USB Endpoints (Recovery Mode)

```
============================================================
Configuration Value: 1
Interface Number: 0,Alternate Setting: 0
Endpoint Address: 4
Interface Number: 1,Alternate Setting: 0
Interface Number: 1,Alternate Setting: 1
Endpoint Address: 129
Endpoint Address: 2
============================================================


============================================================
DEVICE ID 05ac:1281 on Bus 001 Address 003 =================
 bLength             :  0x12 (18 bytes)
 bDescriptorType     :  0x1 Device
 bcdUSB              : 0x200 USB 2.0
 bDeviceClass        :  0x0 Specified at interface
 bDeviceSubClass     :  0x0
 bDeviceProtocol     :  0x0
 bMaxPacketSize0     :  0x40 (64 bytes)
 idVendor            : 0x05ac
 idProduct           : 0x1281
 bcdDevice           :  0x0 Device 0.0
 iManufacturer       :  0x2 Apple Inc.
 iProduct            :  0x3 Apple Mobile Device (Recovery Mode)
 iSerialNumber       :  0x4 SDOM:01 CPID:8015 CPRV:11 CPFM:03 SCEP:01
 BDID:0E ECID:000C2C680044E02E IBFL:3D SRNM:[FK1WT6BPJCLH]
 bNumConfigurations  :  0x1
  CONFIGURATION 1: 500 mA ==================================
   bLength           :  0x9 (9 bytes)
   bDescriptorType   :  0x2 Configuration
   wTotalLength      :  0x39 (57 bytes)
   bNumInterfaces    :  0x2
   bConfigurationValue :  0x1
   iConfiguration    :  0x5 Apple Mobile Device (Recovery Mode)
   bmAttributes      :  0x80 Bus Powered
   bMaxPower         :  0xfa (500 mA)
    INTERFACE 0: Application Specific =======================
     bLength         :  0x9 (9 bytes)
     bDescriptorType :  0x4 Interface
     bInterfaceNumber :  0x0
     bAlternateSetting :  0x0
     bNumEndpoints   :  0x1
     bInterfaceClass :  0xfe Application Specific
     bInterfaceSubClass :  0x1
     bInterfaceProtocol :  0x2
     iInterface      :  0x0
      ENDPOINT 0x4: Bulk OUT ================================
       bLength       :  0x7 (7 bytes)
       bDescriptorType :  0x5 Endpoint
       bEndpointAddress :  0x4 OUT
       bmAttributes  :  0x2 Bulk
       wMaxPacketSize :  0x200 (512 bytes)
       bInterval     :  0x0
    INTERFACE 1: Vendor Specific ============================
     bLength         :  0x9 (9 bytes)
     bDescriptorType :  0x4 Interface
     bInterfaceNumber :  0x1
     bAlternateSetting :  0x0
     bNumEndpoints   :  0x0
     bInterfaceClass :  0xff Vendor Specific
     bInterfaceSubClass :  0xff
     bInterfaceProtocol :  0x51
     iInterface      :  0x0
    INTERFACE 1, 1: Vendor Specific =========================
     bLength         :  0x9 (9 bytes)
     bDescriptorType :  0x4 Interface
     bInterfaceNumber :  0x1
     bAlternateSetting :  0x1
     bNumEndpoints   :  0x2
     bInterfaceClass :  0xff Vendor Specific
     bInterfaceSubClass :  0xff
     bInterfaceProtocol :  0x51
     iInterface      :  0x6 Apple USB Serial Interface
      ENDPOINT 0x81: Bulk IN ================================
       bLength       :  0x7 (7 bytes)
       bDescriptorType :  0x5 Endpoint
       bEndpointAddress :  0x81 IN
       bmAttributes  :  0x2 Bulk
       wMaxPacketSize :  0x200 (512 bytes)
       bInterval     :  0x0
      ENDPOINT 0x2: Bulk OUT =================================
       bLength       :  0x7 (7 bytes)
       bDescriptorType :  0x5 Endpoint
       bEndpointAddress :  0x2 OUT
       bmAttributes  :  0x2 Bulk
       wMaxPacketSize :  0x200 (512 bytes)
       bInterval     :  0x0
============================================================
```

HEXORDIA

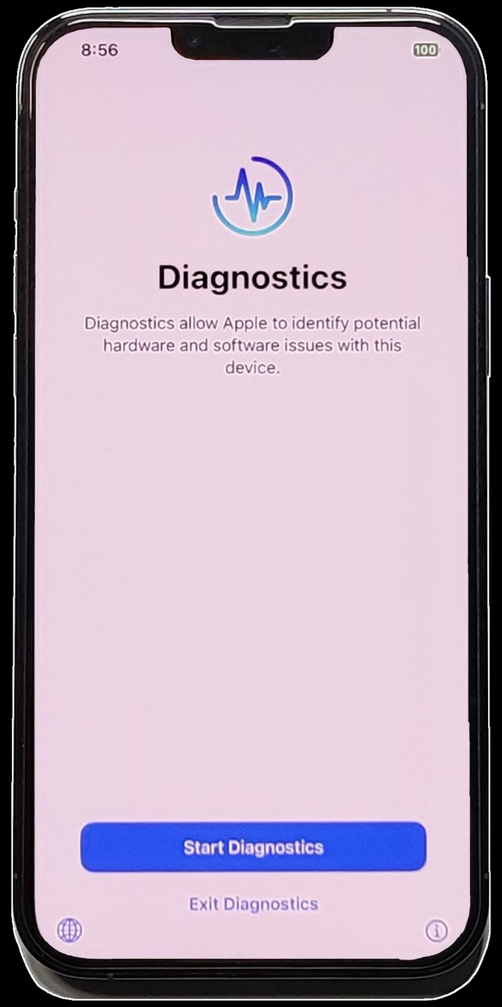
USB Endpoints (DFU Mode)

```
============================================================
Configuration Value: 1
Interface Number: 0,Alternate Setting: 0
============================================================


============================================================
DEVICE ID 05ac:1227 on Bus 001 Address 009 ==================
 bLength             :  0x12 (18 bytes)
 bDescriptorType     :  0x1 Device
 bcdUSB              : 0x200 USB 2.0
 bDeviceClass        :  0x0 Specified at interface
 bDeviceSubClass     :  0x0
 bDeviceProtocol     :  0x0
 bMaxPacketSize0     :  0x40 (64 bytes)
 idVendor            : 0x05ac
 idProduct           : 0x1227
 bcdDevice           :  0x0 Device 0.0
 iManufacturer       :  0x2 Apple Inc.
 iProduct            :  0x3 Apple Mobile Device (DFU Mode)
 iSerialNumber       :  0x4 CPID:8015 CPRV:11 CPFM:03 SCEP:01
BDID:0E ECID:000C2C680044E02E IBFL:3C SRTG:[iBoot-3332.0.0.1.23]
 bNumConfigurations  :  0x1
  CONFIGURATION 1: 500 mA ==================================
   bLength           :  0x9 (9 bytes)
   bDescriptorType   :  0x2 Configuration
   wTotalLength      : 0x19 (25 bytes)
   bNumInterfaces    :  0x1
   bConfigurationValue :  0x1
   iConfiguration    :  0x5 Apple Mobile Device (DFU Mode)
   bmAttributes      : 0x80 Bus Powered
   bMaxPower         :  0xfa (500 mA)
    INTERFACE 0: Application Specific =======================
     bLength         :  0x9 (9 bytes)
     bDescriptorType :  0x4 Interface
     bInterfaceNumber :  0x0
     bAlternateSetting :  0x0
     bNumEndpoints   :  0x0
     bInterfaceClass :  0xfe Application Specific
     bInterfaceSubClass :  0x1
     bInterfaceProtocol :  0x0
     iInterface      :  0x0
============================================================
```

HEXORDIA

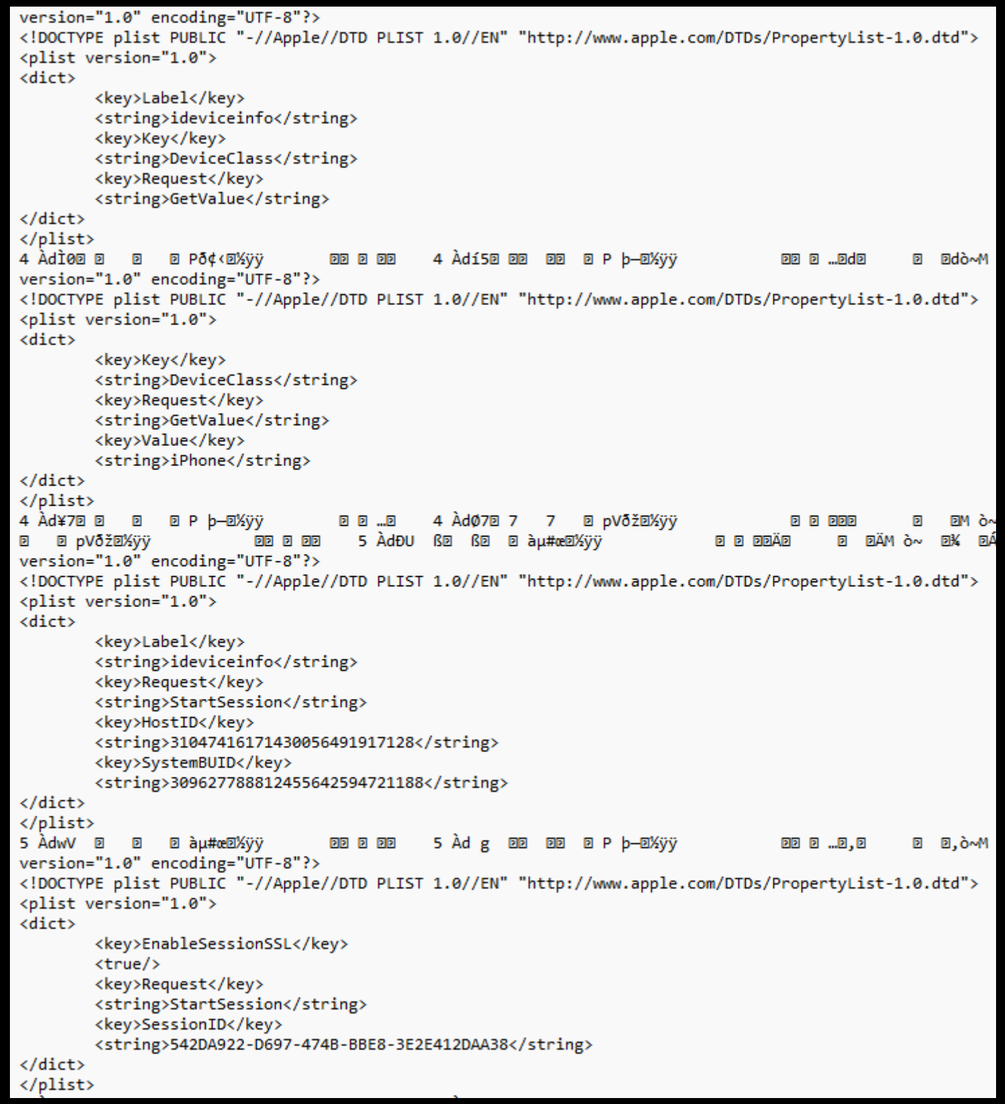
USB Endpoints (Diagnostics Mode)

The same endpoints as Normal Device State; endpoints do not work the same



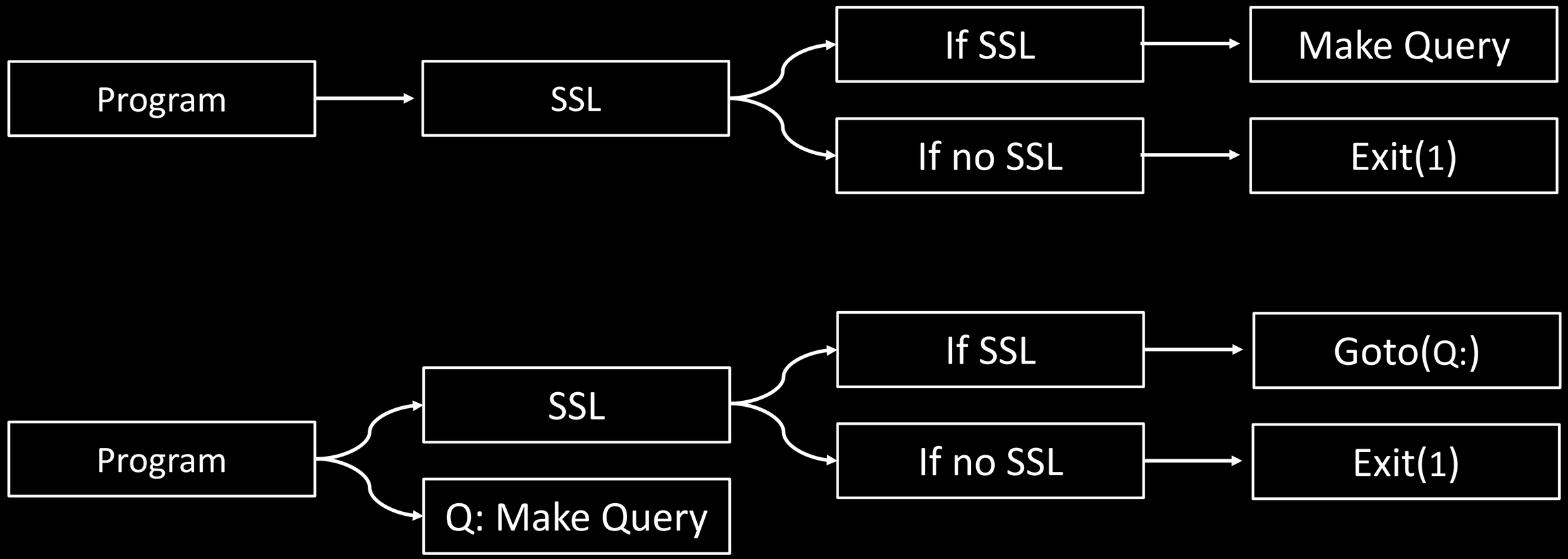
HEXORDIA

usbmuxd & SSL



HEXORDIA

Some Programs…



HEXORDIA

Working with USB Endpoints

1. Capture and Examine Raw USB Traffic

2. Send Custom Raw HID / USB Packets

HEXORDIA

Capturing USB Traffic

https://desowin.org/usbpcap/

HEXORDIA

Capturing USB Traffic

HEXORDIA

Identifying iOS USB Traffic

HEXORDIA

Identifying iOS USB Traffic

- No data sent in USB RM
- Tokens and Certificates seen while in locked and unlocked state
- Setup Phase and Deactivated devices are automatically trusted

Contents will vary depending on:

- Device Boot State (Normal, DFU, Etc…)
- Device Lock State (BFU, AFU)
- Trust or No Trust
- PC Software

HEXORDIA

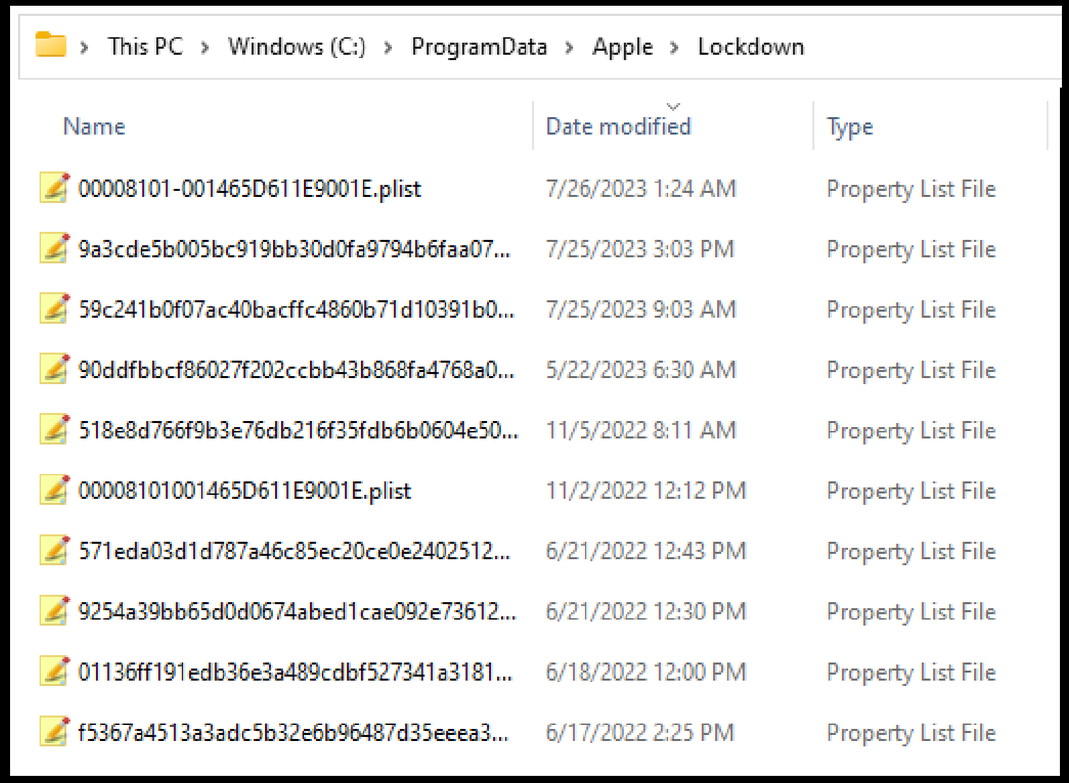
USB RM Ruins it

HEXORDIA

Pairing Records

Windows: C:\ProgramData\Apple\Lockdown

MacOS: /var/db/lockdown

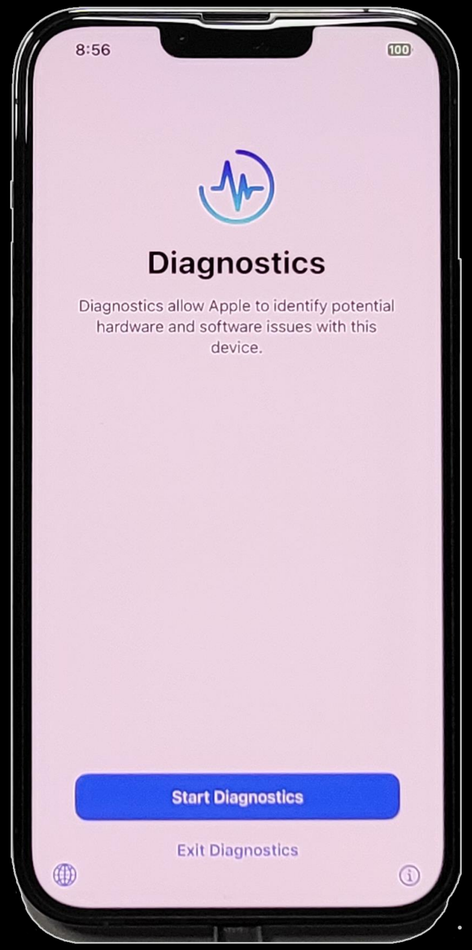


HEXORDIA

USB RM Bypass… Kinda

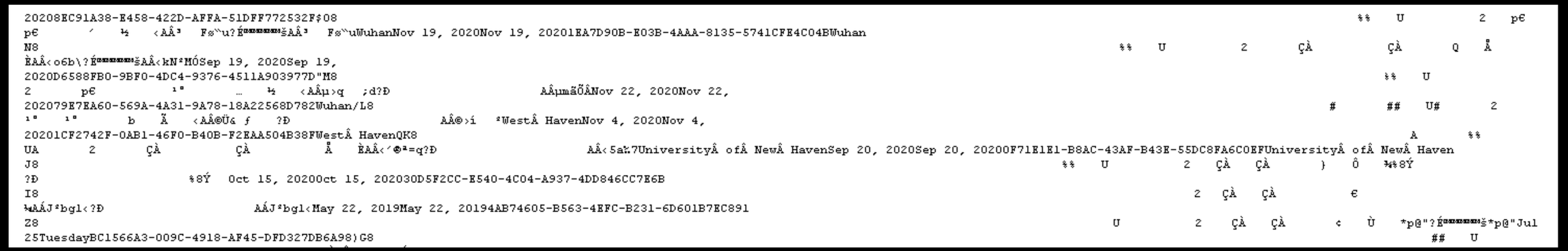
A device in Diagnostics Mode has no USB RM:

- Device endpoints are limited however most identifiers can be recovered
- Lockdownd will not establish a complete connection as the device is in a “passcode protected” state
- May send custom commands which can work in a passcode protected state



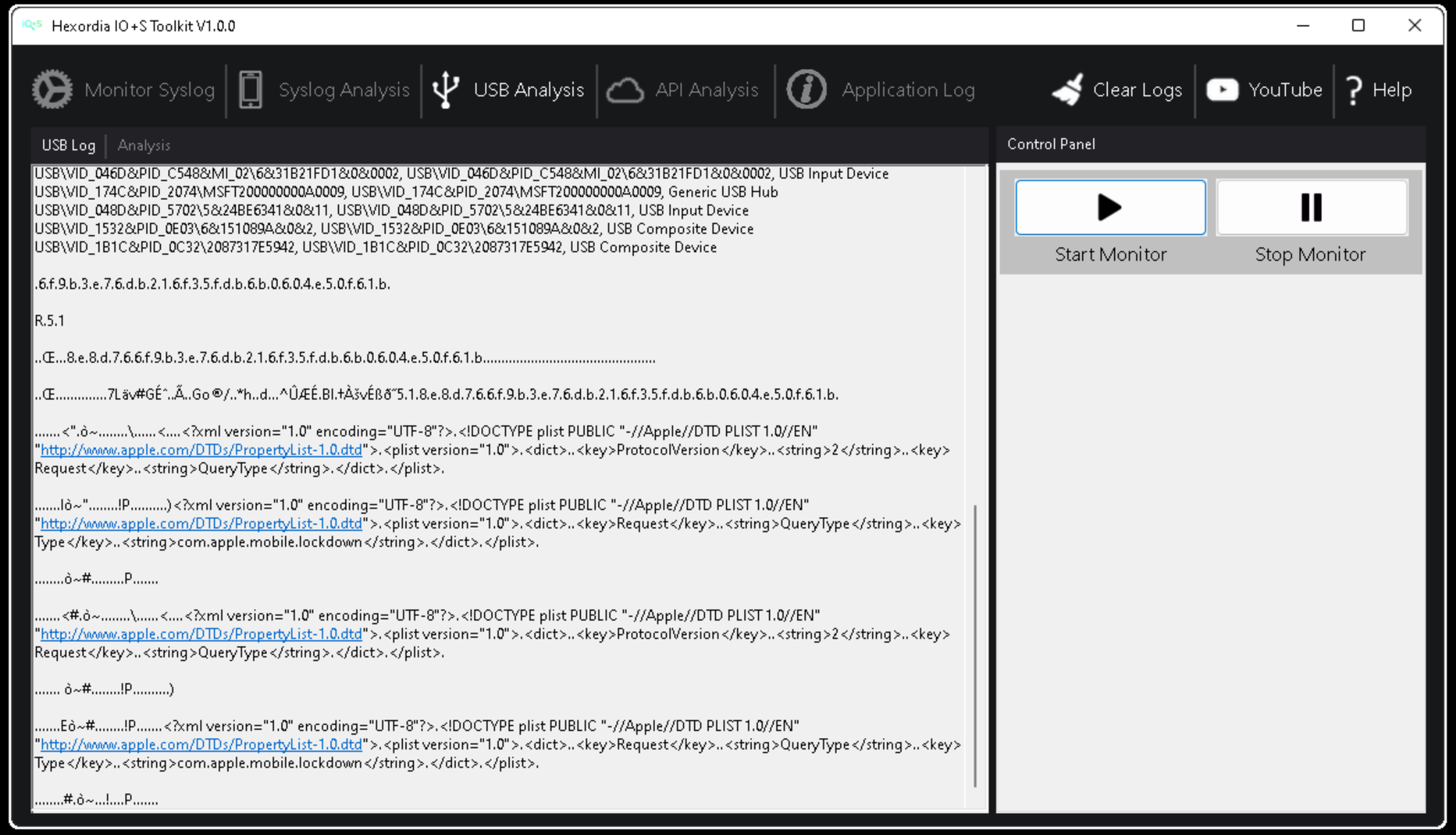
HEXORDIA

USB RM Bypass… Kinda



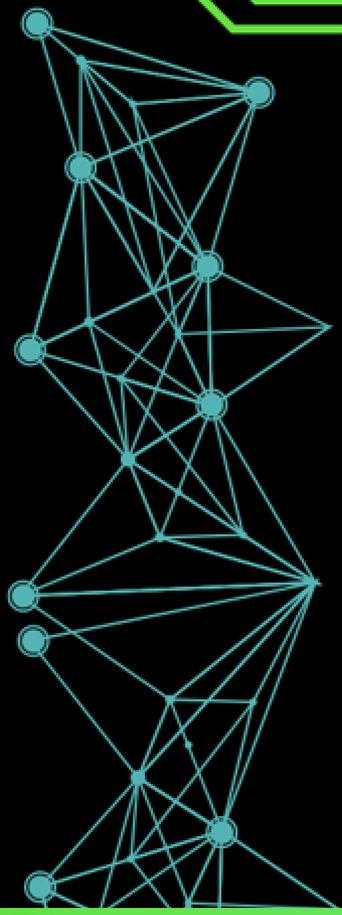
HEXORDIA

Parsing USB Traffic – Hexordia iO+S Toolkit



HEXORDIA

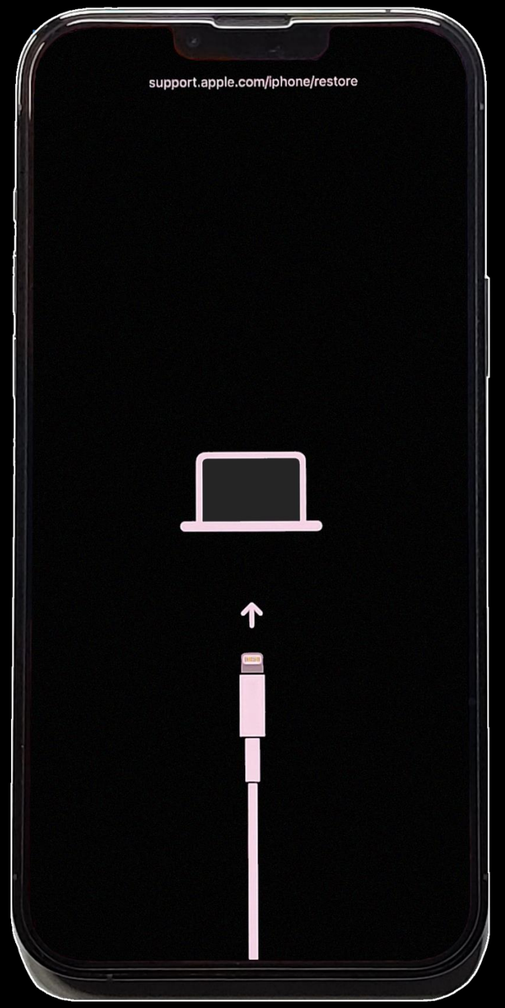
Query Recovery Mode



HEXORDIA

idevicerecovery - getenv

Command	Example
getenv build-version	iBoot-6723.80.19
getenv auto-boot	true
getenv bootdelay	0
getenv backlight-level	1505
getenv boot-command	fsboot
getenv image-version	0x4
getenv secure-boot	0x1
getenv ?	0x0
getenv boot-partition	0
getenv boot-path	/System/Library/Caches/com.apple.kernelcaches/kernelcache
getenv dt-path	/usr/standalone/firmware/devicetree.img4
getenv build-style	RELEASE
getenv config_board	d201
getenv board-rev	0xf
getenv loadaddr	0x801000000
getenv ramdisk-size	0x20000000
getenv idle-off	true
getenv boot-device	nvme_nand0
getenv display-color-space	ARGB8101010
getenv fm-activation-locked	
getenv restore-outcome	
getenv fm-account-masked	do********@ic****.***
getenv fm-spstatus	
getenv obliteration	handle_message: Obliteration Complete
getenv backlight-nits	0x00ac7a3f
getenv usbcfwflasherResult	No errors
getenv fm-spkeys	
nonce-seeds	



HEXORDIA

Fuzzing Recovery Mode

```
import os
import subprocess
import time
import signal

os.chdir("C:/Users/nickd/Desktop/Reverse Engineering Syslog/Raw Data/libimobiledevice_32")

f = open("C:/Users/nickd/Desktop/fuzzme.txt", "r", encoding="utf8", errors="ignore")
out = open("C:/Users/nickd/Desktop/getrecovery.txt", "w", errors="ignore")
out2 = open("C:/Users/nickd/Desktop/runrecovery.txt", "w", errors="ignore")
Lines = f.read().splitlines()
#subprocess.Popen('irecovery.exe -c & ping -n 30 127.0.0.1 &', shell=False, stderr=f, stdout=f)
#time.sleep(10)

get = 1
set = 0
run = 0

if(get==1):
    for line in Lines:
        str='/c echo getenv ' + line + ' | irecovery.exe -s'
        out.write("\n\n")
        out.flush()
        print(str)
        proc = subprocess.Popen(["cmd",str], stderr=out,stdout=out)
        time.sleep(0.4)
        try:
            os.kill(proc.pid, signal.SIGINT)
        except: pass

if(set==1):
    for line in Lines:
        str='/c echo setenv ' + line + ' false | irecovery.exe -s'
        out.write("\n\n")
        out.flush()
        print(str)
        proc = subprocess.Popen(["cmd",str], stderr=out,stdout=out)
        time.sleep(0.2)
        try:
            os.kill(proc.pid, signal.SIGINT)
        except: pass
    str='/c echo saveenv' + ' | irecovery.exe -s'
    proc = subprocess.Popen(["cmd", str], stderr=out, stdout=out)
    os.kill(proc.pid, signal.SIGINT)

if(run==1):
    for line in Lines:
        str='/c echo ' + line + ' | irecovery.exe -s'
        out2.write("\n\n")
        out2.flush()
        print(str)
        proc = subprocess.Popen(["cmd",str], stderr=out2,stdout=out2)
        time.sleep(0.2)
        try:
            os.kill(proc.pid, signal.SIGINT)
        except: pass
```

HEXORDIA

What Can we Recover From Locked Devices?

Paired Locked Device

- Sysdiagnose Logs
- Live Syslogs
- iTunes Backups
- Siri
- Lockscreen Widgets & Info
- RAW USB Traffic Data
- Recovery Mode Data
- DFU Mode Data
- Diagnostics Mode Data

HEXORDIA

Unpaired Locked Device

Siri

Lockscreen Widgets & Info

RAW USB Traffic Data

Recovery Mode Data

DFU Mode Data

Diagnostics Mode Data

Remote Sysdiagnose Logs

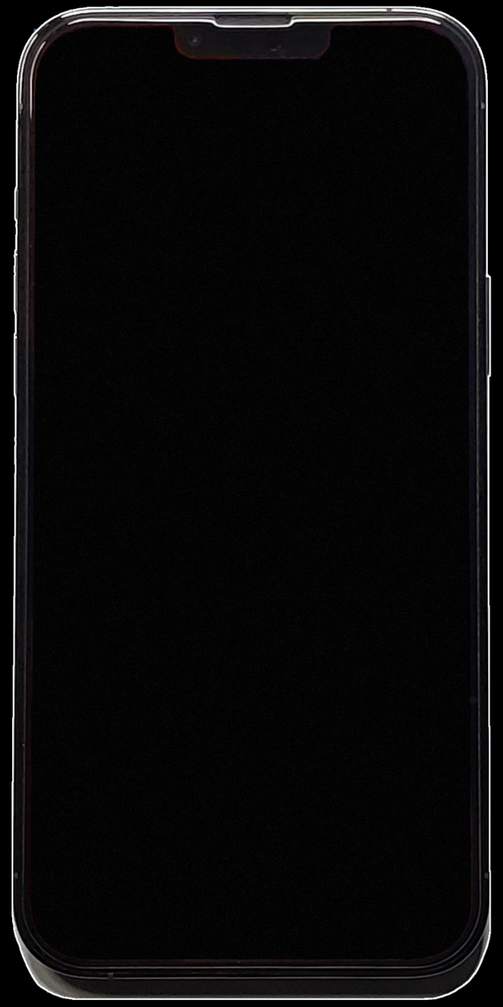
HEXORDIA

Case Study

iPhone 12 Pro

USB RM, Untrusted, AFU

iOS 16.2



HEXORDIA

APIs

- iTunes Account Email Address
- First and Last Name
- Additional Generic iTunes Account Info

Recovery Mode

- Device Model
- Unique Device Identifier, Current IMEI & Generic Device Info
- Partial iCloud Email Address
- Device is iCloud Locked

HEXORDIA

Diagnostics Mode

- Serial No.
- MEID
- IMEI
- Unique Device Identifier, WiFi MAC, Additional Hardware Info.
- iOS Version
- Baseband Info.
- Names of Photos
- Photo Metadata (Datetime & Location)

HEXORDIA

Sysdiagnose Log – Device Info

- Device Name, iOS Version + OS Info., UUID,
- Languages, Timezones, Keyboards
- Power on Times, Application Run Times, Screenshot Taken Times
- Connected USB Devices, Device Trust Datetime Logs, Bat. %, Device Orientation, Charging, Screen Status, Brightness, Motion

Sysdiagnose Log – Application Info

- Installed Applications, Application Versions,Appliaction permissions
- Currently Running Applications / Processes, Application Run Times

HEXORDIA

Sysdiagnose Log – WiFi & Bluetooth

- HW MAC Address, Private MACs
- Connected SSID, BSSID, Country Code, IP Address, Router IP Address, DNS
- WiFi Scaned Networks, First Joined Times, Last Joined Times
- Paired / Connected Bluetooth Devices
- Networks lat., long. location
- External IP Addresses & Domains

Sysdiagnose Log – User & Cloud Info

- Full Name
- iCloud Email, Unique Username Identifiers
- Cloud Sync Timestamps, API Keys, Keychain Info., Cloud Container Info.

HEXORDIA

Sysdiagnose Log – “Logs”

- Transparency, Consent, and Control (TCC) Database, Device Settings and Preferences
- Powerlog
- Application Usage Logs, Application Battery Consumption
- Mobile Installation Logs (Installation Logs Including Deleted Apps)
- Calandar Email Addr. & Contents
- Installed Device Profiles, Profile Configuration
- Mobile Activation Logs
- Lockdownd Logs
- Update, User, & Restore Logs
- SiriAnalytics (Siri Activation Times)

HEXORDIA

Sysdiagnose Log – logarchive

- A LOT of Hardware info
- Full Name, Email Addresses, Mail Tokens, Account Phone Number
- Safari History
- Installed Applications
- Paired / Connected Bluetooth Devices, BLE Scans
- Device Orientation, Maps Locations, Location (Long./Lat.)
- AirDrop Logs + Phone Numbers/Email
- AirTag Logs (#Durian)
- Contact Information (Names + Email + Phone Number)

HEXORDIA

Key Takeaways For Researchers

Find More Endpoints

Use FFS to Find Endpoints

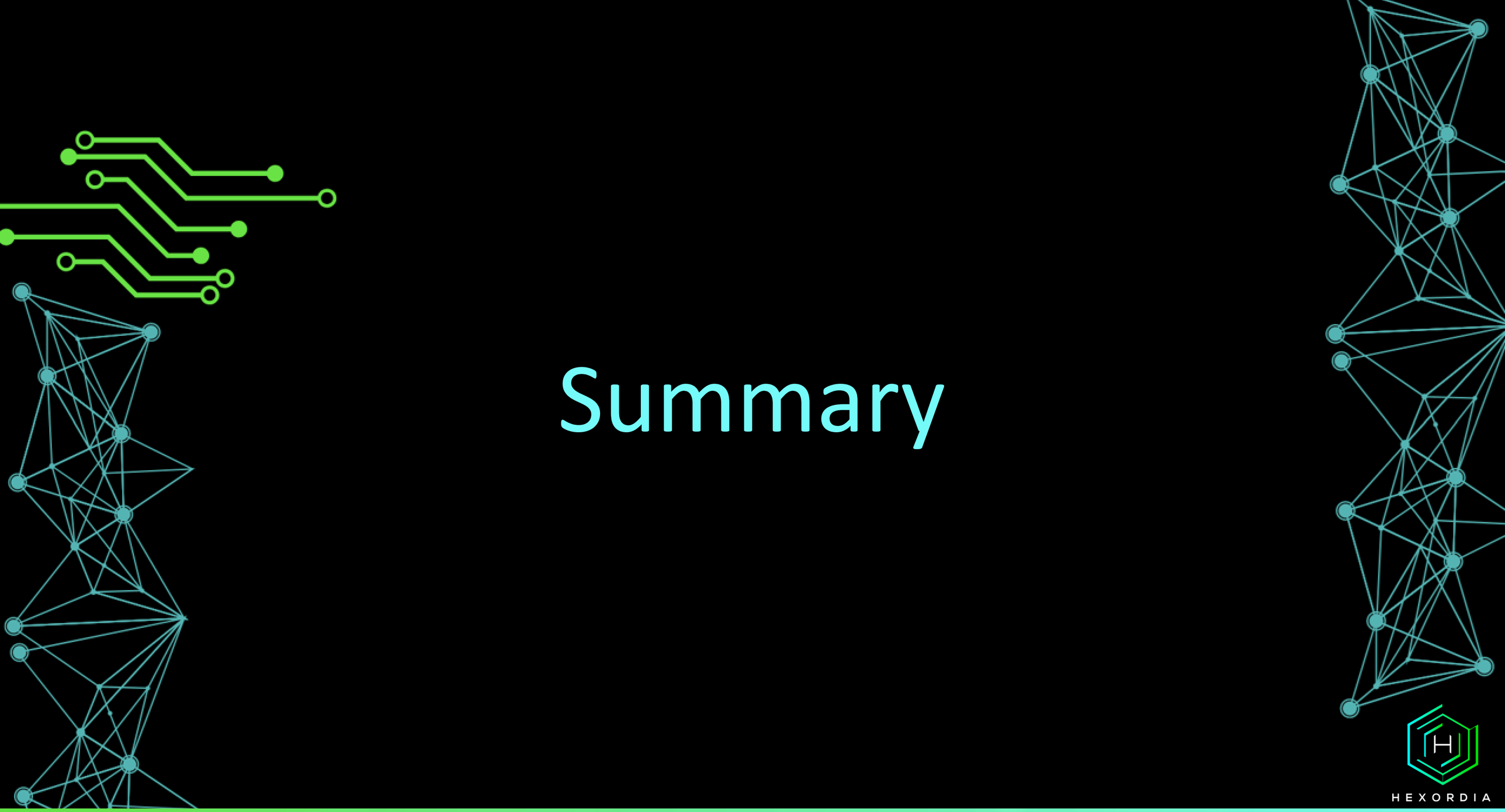
Diagnostics Mode

HEXORDIA

Future Work

- Fuzzing DFU Mode More
- Examine diagnostics mode API
- Fuzzing recovery commands more

Summary



QUESTIONS?

Nicholas Dubois
@noot4n6

Jessica Hyde
@b1n2h3x

HEXORDIA