

# WATCHING THE WATCHERS



Sarah Edwards | @iamevl twin  
mac4n6.com | for518.com



# What & Why?

- Scope
  - *macOS 3<sup>rd</sup> Party Monitoring Software*
    - Objective-See
    - Little Snitch
    - Sophos
    - iStat Menus
- Data Sources
  - Application Logs
  - System Logs (Unified Logs)
- Different Investigative Uses
  - Device Usage & State
  - Processes & Applications Usage
  - Location
  - Network Activity
  - Software Installations
  - Attached Volumes
  - File Downloads
  - Disk Usage
  - Web Browsing



# OBJECTIVE-SEE DO NOT DISTURB



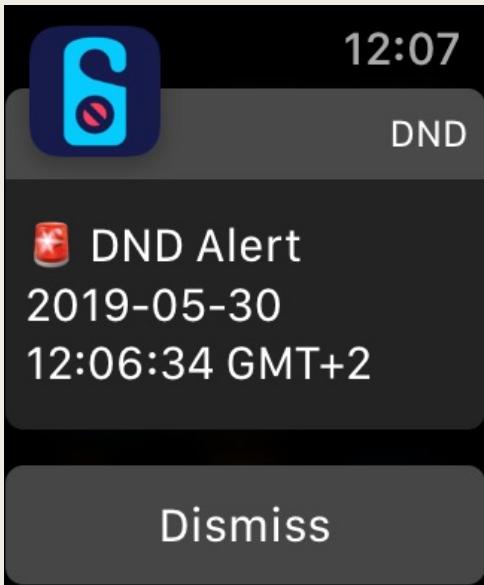
# Objective-See – Do Not Disturb Enable or Disabled – Unified Logs

- log show --info --predicate 'eventMessage contains "DND"'

```
2019-05-24 08:23:16.576467+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: NO
2019-05-24 08:23:16.577401+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: NO
2019-05-24 08:23:20.008294+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: YES
2019-05-24 08:23:20.008888+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: YES
2019-05-24 08:36:28.543931+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: NO
2019-05-24 08:36:28.544513+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: NO
2019-05-24 08:39:22.519578+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: YES
2019-05-24 08:39:22.520254+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: YES
2019-05-24 08:41:28.238207+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: NO
2019-05-24 08:41:28.239125+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: NO
2019-05-24 08:41:28.681095+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: YES
2019-05-24 08:41:28.683372+0200 0xd71 Default 0x0 341 0 identityservicesd: (IMFoundation) [com.apple.IDS:Registration] <private>: DND Enabled: YES
```

# Objective-See - Do Not Disturb Laptop Lid State

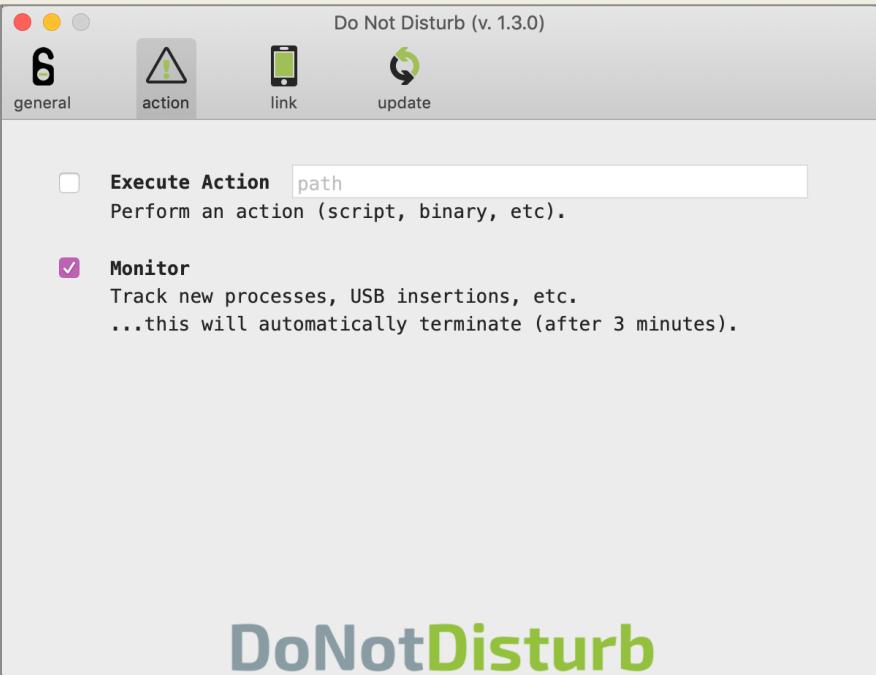
- /Library/Objective-See/DND/DND.log
- Potential Session Usage
- Device Use Frequency



```
2019-05-16 00:05:44 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-16 02:08:40 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 00:39:16 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-17 00:42:31 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 02:49:09 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-17 02:50:42 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 12:37:43 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-17 12:46:22 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 12:57:00 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-17 13:12:20 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 13:12:24 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-17 13:12:48 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 13:18:09 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-17 13:19:35 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-17 14:09:16 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-17 16:18:13 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-18 14:11:15 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-20 06:24:44 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-20 06:33:42 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-20 15:55:19 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-20 16:35:43 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-20 16:40:04 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-20 16:42:47 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-20 16:46:21 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-21 16:13:57 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
2019-05-21 16:15:49 +0000: [NEW EVENT] lid state: open (sleep state: 0)
2019-05-21 17:06:44 +0000: [NEW EVENT] lid state: closed (sleep state: 0)
2019-05-22 06:39:39 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-22 15:24:46 +0000: [NEW EVENT] lid state: closed (sleep state: 0)
2019-05-22 15:41:31 +0000: [NEW EVENT] lid state: open (sleep state: 1)
2019-05-22 16:57:00 +0000: [NEW EVENT] lid state: closed (sleep state: 1)
```

# Objective-See - Do Not Disturb USB & Volumes

- /Library/Objective-See/DND/DND.log
- USB Usage....however not all usage...only the first 3 minutes



DoNotDisturb

```
2019-05-09 04:58:30 +0000: monitor event: usb device inserted
2019-05-09 04:58:30 +0000: usb device name: Nexcopy Device
2019-05-09 04:58:30 +0000: usb device properties: {
    "Built-In" = 0;
    "Bus Power Available" = 450;
    "Device Speed" = 3;
    IOCFPlugInTypes = {
        "9dc7b780-9ec0-11d4-a54f-000a27052861" = "IOUSBFamily.kext/Contents/PlugIns/IOUSBLib.bundle";
    };
    IOClassNameOverride = IOUSBDevice;
    IOGeneralInterest = "IOCommand is not serializable";
    IOPowerManagement = {
        CapabilityFlags = 65536;
        CurrentPowerState = 3;
        DevicePowerState = 0;
        DriverPowerState = 3;
        MaxPowerState = 4;
    };
    IOUserClientClass = IOUSBDeviceUserClientV2;
    PortNum = 2;
    "USB Address" = 1;
    "USB Product Name" = "Nexcopy Device ";
    "USB Serial Number" = "030419-74480";
    "USB Vendor Name" = "Generic ";
    bDeviceClass = 0;
    bDeviceProtocol = 0;
    bDeviceSubClass = 0;
    bMaxPacketSize0 = 9;
    bNumConfigurations = 1;
    bcdDevice = 4352;
    bcdUSB = 768;
    iManufacturer = 1;
    iProduct = 2;
    iSerialNumber = 3;
    idProduct = 4096;
    idVendor = 2316;
    locationID = 2097152;
    "non-removable" = no;
    sessionID = 1245082798918828;
}
2019-05-09 04:58:33 +0000: monitor event: volume mounted: /Volumes/FOR518-A
{
    NSDevicePath = "/Volumes/FOR518-A";
    NSWorkspaceVolumeLocalizedNameKey = "FOR518-A";
    NSWorkspaceVolumeURLKey = "file:///Volumes/FOR518-A/";
}
```

# Objective-See - Do Not Disturb Application Usage & Processes

- /Library/Objective-See/DND/DND.log
- Only the first 3 minutes...

```
2019-05-30 10:08:07 +0000: monitor event: process start: (28336: /Applications/Photos.app/Contents/MacOS/Photos (args: (xpcproxy, "com.apple.Photos.34292")))  
2019-05-30 10:08:10 +0000: monitor event: process start: (28336: /Applications/Photos.app/Contents/MacOS/Photos (args: ("/Applications/Photos.app/Contents/MacOS/Photos")))
```

```
2019-03-31 12:28:33 +0000: monitor event: process start: (65733: /usr/bin/open (args: ()))  
2019-03-31 12:28:34 +0000: monitor event: process start: (65733: /usr/bin/open (args: (open, "com.apple.SoftwareUpdate.plist")))
```

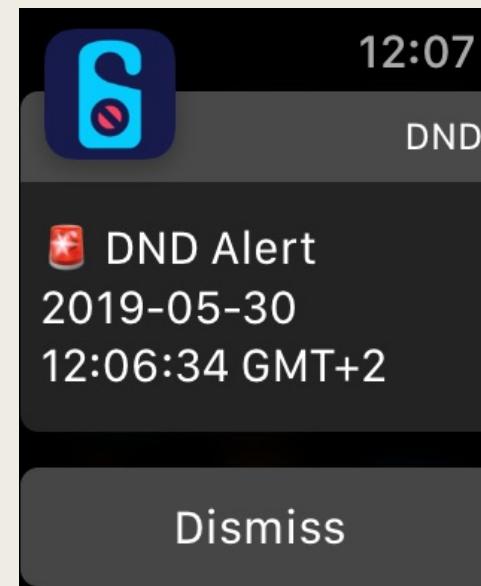
```
2019-03-31 12:29:18 +0000: monitor event: process start: (65739: /usr/bin/find (args: (find, "/Users/oompa", "-ipath", "*softwareupdate*")))
```

# Objective-See - Do Not Disturb User Authentication

- /Library/Objective-See/DND/DND.log

```
2019-05-30 10:06:36 +0000: monitor event: user authentication user auth event
uid: 0 / pid: 302 / text: Touch ID authentication / ret: 0
```

```
2019-05-30 10:06:41 +0000: monitor event: user authentication user auth event
uid: 501 / pid: 368 / text: Verify password for record type Users 'oompa' node '/Local/Default' / ret: 5000
```



# Objective-See - Do Not Disturb Downloaded Files

- /Library/Objective-See/DND/DND.log
- Previously Existing Files, Application Usage, Mail Attachment Opening

```
monitor event: downloaded file: /Users/oompa/Downloads/snagit.dmg
monitor event: downloaded file: /Users/oompa/Downloads/Sublime Text Build 3176.dmg
monitor event: downloaded file: /Users/oompa/Downloads/WhatsApp.dmg
monitor event: downloaded file: /Users/oompa/Downloads/Microsoft_Office_16.19.18110915_Installer.pkg
monitor event: downloaded file: /Users/oompa/Downloads/VMware-Fusion-11.0.2-10952296.dmg
```

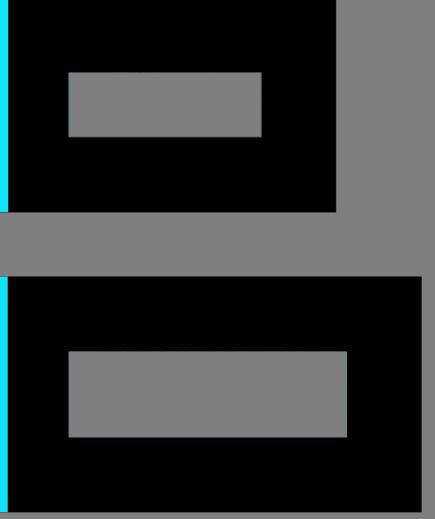
```
2019-05-18 14:13:43 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/470bd6c5-a9f3-3774-b6b9-8c3bd8d4cd55.ics
2019-05-18 14:13:43 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/81f5ec1f-cf4b-3c84-bb11-1f2a20012d3c.ics
2019-05-18 14:13:43 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/628cfb64-f2bb-3448-8a33-dfbdcf7925e9.ics
2019-05-18 14:13:43 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/24ccb28f-892f-3976-b5c0-57d57812eb4f.ics
2019-05-18 14:13:43 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/96/06/EB5FCE20-0D15-4641-BCF5-4FC1F22AAC57/ms-4PecxX.gif
2019-05-18 14:13:43 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/02/02/AC7C9057-FA0C-4524-AF06-407D183B2200/FullSizeRender.jpeg
2019-05-18 14:13:44 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/20/00/D9B19889-7702-47CF-BF22-2DFC752B86A8/IMG_3335.jpeg
2019-05-18 14:13:44 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/20/00/D9B19889-7702-47CF-BF22-2DFC752B86A8/IMG_3335.MOV
2019-05-18 14:13:44 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/d8/08/CEAC53E5-DA3E-4B60-B96E-DE9858702FD9/57981051253__FF7FC393-21F1-4564-A6A1-4E2E39B972B0.jpeg
2019-05-18 14:13:44 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/ee/14/6B518DAB-30DC-4E76-909C-67D00C4D5397/57981044287__5231C098-41A8-4261-8142-3151D074FCC7.jpeg
2019-05-18 14:13:44 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/97/07/070CCD9A-90DD-4633-98E7-45E21DED9F72/IMG_3339.MOV
2019-05-18 14:13:44 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/97/07/070CCD9A-90DD-4633-98E7-45E21DED9F72/IMG_3339.jpeg
2019-05-18 14:14:02 +0000: monitor event: downloaded file: /Users/oompa/Library/Containers/com.apple.mail/Data/Library/Mail/Downloads/62FA9A3F-CA62-432B-859A-B847AEA9F47E/Faculty Friday May 17, 2019.pdf
2019-05-18 14:14:03 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/53/03/C2A578D5-C6E0-4C7D-B339-D462C013AEC7/57981938087__064B5D05-EF24-4D41-A331-B8021EB3EDD3.jpeg
2019-05-18 14:14:03 +0000: monitor event: downloaded file: /Users/oompa/Library/Messages/Attachments/fa/10/FECFB796-F45C-4A9A-B98F-3F046E626AA4/57982167763__43B23A54-ED1F-4AF6-A4E0-5F3E3514A91.jpg.jpeg
2019-05-20 06:33:48 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/3a19ad94-8de7-33bf-8af0-e80e80610d85.ics
2019-05-20 06:33:48 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/3b4ea211-dc06-39cb-b86d-19d17c486b53.ics
2019-05-20 06:33:48 +0000: monitor event: downloaded file: /Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/2243854d-20f4-3691-8876-e46196f3ddd4.ics
```



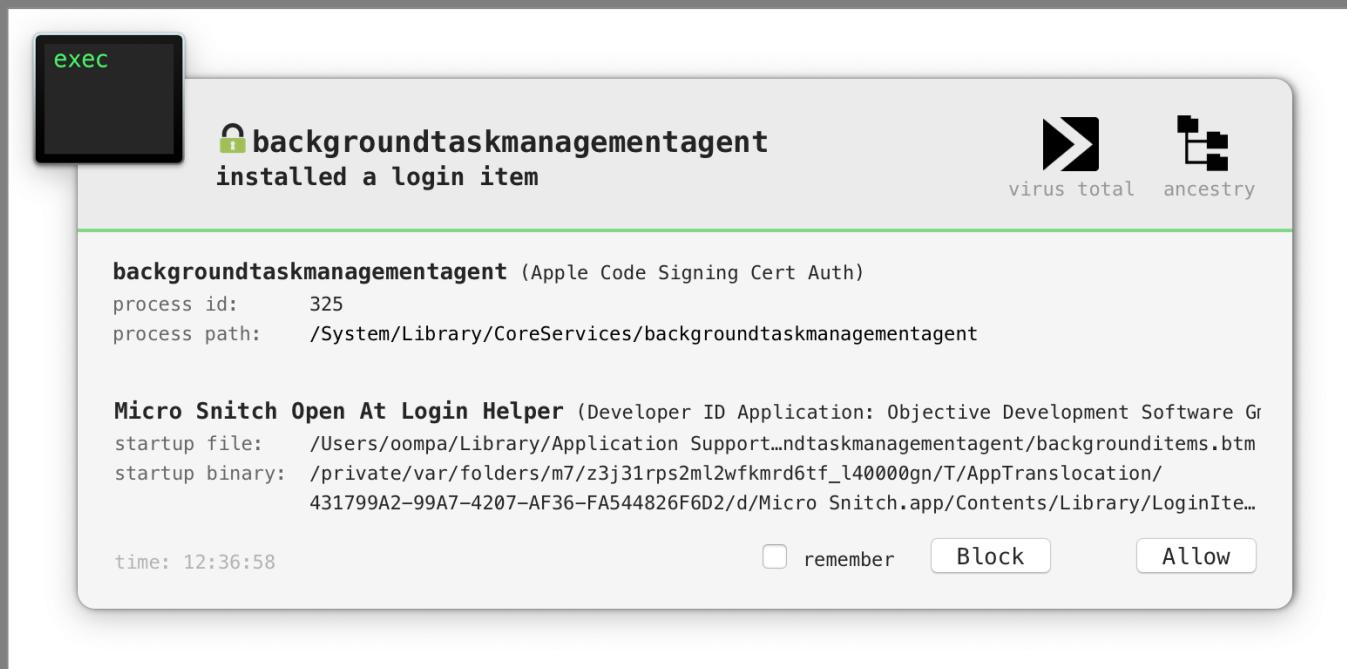
# Objective-See - Do Not Disturb Downloaded Files

- /Library/Objective-See/DND/DND.log
- Previously Existing Files, Application Usage, Mail Attachment Opening

```
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/470bd6c5-a9f3-3774-b6b9-8c3bd8d4cd55.ics
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/81f5ec1f-cf4b-3c04-bb11-1f2a20012d3c.ics
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/628cfb64-f2bb-3448-8a33-dfbdcf7925e9.ics
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/24ccb28f-892f-3976-b5c0-57d57812eb4f.ics
/Users/oompa/Library/Messages/Attachments/96/06/EB5FCE20-0D15-4641-BCF5-4FC1F22AAC57/ms-4PecxX.gif
/Users/oompa/Library/Messages/Attachments/02/02/AC7C9057-FA0C-4524-AF06-407D183B2200/FullSizeRender.jpeg
/Users/oompa/Library/Messages/Attachments/20/00/D9B19889-7702-47CF-BF22-2DFC752B86A8/IMG_3335.jpeg
/Users/oompa/Library/Messages/Attachments/20/00/D9B19889-7702-47CF-BF22-2DFC752B86A8/IMG_3335.MOV
/Users/oompa/Library/Messages/Attachments/d8/08/CEAC53E5-DA3E-4B60-B96E-DE9858702FD9/57981051253__FF7FC393-21F1-4564-A6A1-4E2E39B972B0.jpeg
/Users/oompa/Library/Messages/Attachments/ee/14/6B518DAB-30DC-4E76-909C-67D00C4D5397/57981044287__5231C098-41A8-4261-8142-3151D074FCC7.jpeg
/Users/oompa/Library/Messages/Attachments/97/07/070CCD9A-90DD-4633-98E7-45E21DED9F72/IMG_3339.MOV
/Users/oompa/Library/Messages/Attachments/97/07/070CCD9A-90DD-4633-98E7-45E21DED9F72/IMG_3339.jpeg
/Users/oompa/Library/Containers/com.apple.mail/Data/Library/Mail Downloads/62FA9A3F-CA62-432B-859A-B847AEA9F47E/Faculty Friday May 17, 2019.pdf
/Users/oompa/Library/Messages/Attachments/53/03/C2A578D5-C6E0-4C7D-B339-D462C013AEC7/57981938087__064B5D05-EF24-4D41-A331-B8021EB3EDD3.jpeg
/Users/oompa/Library/Messages/Attachments/fa/10/FECFB796-F45C-4A9A-B98F-3F046E626AA4/57982167763__43B23A54-ED1F-4AF6-A4E0-5F3E3F14A915.JPG.jpeg
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/3a19ad94-8de7-33bf-8af0-e80e80610d85.ics
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/3b4ea211-dc06-39cb-b86d-19d17c486b53.ics
/Users/oompa/Library/Calendars/4D5D9137-6DFC-47B7-81F1-080D731F5728.calendar/Events/2243854d-20f4-3691-8876-e46196f3ddd4.ics
```



# OBJECTIVE-SEE BLOCKBLOCK

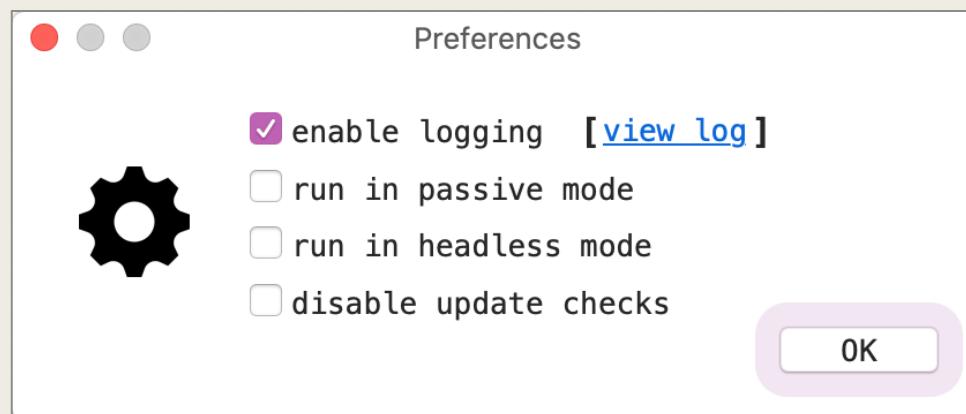


# BlockBlock Alerts & Action

~/Library/Application  
Support/com.objectiveSee.BlockBlock/BlockBlock.log

- ...if logging is enabled

```
2019-05-30 10:31:26 +0000: logging initialized
2019-05-30 10:36:57 +0000: /System/Library/CoreServices/backgroundtaskmanagementagent installed a login item (/Users/omega/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm -> /private/var/folders/m7/z3j31rps2ml2wfkmrd6tf_140000gn/T/AppTranslocation/431799A2-99A7-4207-AF36-FA544826F6D2/d/Micro Snitch.app/Contents/Library/LoginItems/Micro Snitch Open At Login Helper.app)
2019-05-30 10:38:52 +0000: user clicked: Allow
```



# BlockBlock Alerts via Unified Logs

```
[Sarahs-Fridge:Export oompa$ log show --info --predicate 'eventMessage contains[cd] "blockblock" and eventMessage contains[cd] "alert"'  
Filtering the log data using "composedMessage CONTAINS[cd] "blockblock" AND composedMessage CONTAINS[cd] "alert""  
Skipping debug messages, pass --debug to include.  
Timestamp          Thread    Type      Activity        PID    TTL  
2019-05-18 18:13:38.951138+0200 0xc26    Default    0x0           78     0  BlockBlock: BLOCKBLOCK(78) alert: /System/Library/CoreServices/backgroundtaskmanagementagent  
installed a login item (/Users/oompa/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm -> /private/var/folders/m7/z3j31rps2ml2wfkmd6tf_140000g  
n/T/AppTranslocation/623B26EC-2B44-4703-879B-09A330BBB438/d/Micro Snitch.app)  
2019-05-20 08:17:55.932810+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /System/Library/CoreServices/backgroundtaskmanagementagent  
installed a login item (/Users/oompa/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm -> /Users/oompa/Downloads/Micro Snitch.app)  
2019-05-20 08:18:11.785135+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /System/Library/CoreServices/backgroundtaskmanagementagent  
installed a login item (/Users/oompa/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm -> /private/var/folders/m7/z3j31rps2ml2wfkmd6tf_140000g  
n/T/AppTranslocation/C470AFED-428F-4CB3-A4A1-0C33EF86E273/d/Micro Snitch.app/Contents/Library/LoginItems/Micro Snitch Open At Login Helper.app)  
2019-05-20 16:53:54.184008+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /Library/Caches/com.sophos.sau/CID/Sophos Installer.app/Con  
tents/MacOS/tools/InstallationDeployer installed a kernel extension (/Library/Extensions/SophosWebProtection.kext -> /Library/Extensions/SophosWebProtection.kext/Contents/MacOS/Soph  
osSocketFilter)  
2019-05-20 16:53:54.948963+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /Library/Caches/com.sophos.sau/CID/Sophos Installer.app/Con  
tents/MacOS/tools/InstallationDeployer installed a kernel extension (/Library/Extensions/SophosFileMonitor.kext -> /Library/Extensions/SophosFileMonitor.kext/Contents/MacOS/FileMoni  
torKext)  
2019-05-20 16:53:55.739887+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /Library/Caches/com.sophos.sau/CID/Sophos Installer.app/Con  
tents/MacOS/tools/InstallationDeployer installed a kernel extension (/Library/Extensions/SophosFileProtection.kext -> /Library/Extensions/SophosFileProtection.kext/Contents/MacOS/On  
AccessKext)  
2019-05-20 16:53:58.439630+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /Library/Caches/com.sophos.sau/CID/Sophos Installer.app/Con  
tents/MacOS/tools/InstallationDeployer installed a launch daemon or agent (/Library/LaunchAgents/com.sophos.home.ui.plist -> /Applications/Sophos Home.app/Contents/MacOS/Sophos Home  
)  
2019-05-20 16:54:02.111268+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /Library/Caches/com.sophos.sau/CID/Sophos Installer.app/Con  
tents/MacOS/tools/InstallationDeployer installed a launch daemon or agent (/Library/LaunchAgents/com.sophos.agent.plist -> /Library/Sophos Anti-Virus/SophosAgent.app/Contents/MacOS/  
SophosAgent)  
2019-05-20 16:54:03.122212+0200 0xc25    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /Library/Caches/com.sophos.sau/CID/Sophos Installer.app/Con  
tents/MacOS/tools/InstallationDeployer installed a launch daemon or agent (/Library/LaunchDaemons/com.sophos.common.servicemanager.plist -> /Library/Sophos Anti-Virus/SophosServiceM  
anager.bundle/Contents/MacOS/SophosServiceManager)  
2019-05-22 09:53:17.107621+0200 0xc9f    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /bin/cp installed a launch daemon or agent (/Library/Launch  
Daemons/com.microsoft.autoupdate.helper.plist -> /Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper)  
2019-05-30 12:36:55.649277+0200 0xc8b    Default    0x0           85     0  BlockBlock: BLOCKBLOCK(85) alert: /System/Library/CoreServices/backgroundtaskmanagementagent  
installed a login item (/Users/oompa/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm -> /private/var/folders/m7/z3j31rps2ml2wfkmd6tf_140000g  
n/T/AppTranslocation/431799A2-99A7-4207-AF36-FA544826F6D2/d/Micro Snitch.app/Contents/Library/LoginItems/Micro Snitch Open At Login Helper.app)  
  
Log      - Default:      11, Info:          0, Debug:         0, Error:        0, Fault:        0  
Activity - Create:      0, Transition:    0, Actions:       0
```



# OBJECTIVE-SEE LULU FIREWALL

The screenshot shows the Lulu Firewall application window. At the top, there are five tabs: 'all' (selected), 'default', 'apple', '3rd-Party', and 'user'. A search bar labeled 'Search' is located at the top right. Below the tabs is a table titled 'User-specified Programs (manually added, or in response to an alert)'. The table has columns for 'type', 'rule', and a delete button ('x'). The 'rule' column contains checkboxes, all of which are checked ('allow') for the listed programs. The table lists the following programs:

Program Name	Type	Rule
/Library/Objective-See/DND/Do Not Disturb.bundle/Contents/MacOS/Do Not Disturb	user	<input checked="" type="checkbox"/> allow
Do Not Disturb Helper	user	<input checked="" type="checkbox"/> allow
DropboxMacUpdate	user	<input checked="" type="checkbox"/> allow
EgnyteDesktopSync	user	<input checked="" type="checkbox"/> allow
Electron Helper	user	<input checked="" type="checkbox"/> allow
Evernote	user	<input checked="" type="checkbox"/> allow
Excel	user	<input checked="" type="checkbox"/> allow
FrontendAgent	user	<input checked="" type="checkbox"/> allow
G2MUpdate	user	<input checked="" type="checkbox"/> allow
GoogleSoftwareUpdateAgent	user	<input checked="" type="checkbox"/> allow

At the bottom left are two icons: a green upward arrow and a green downward arrow. The word 'LuLu' is centered at the bottom, and an 'add rule' button with a plus sign is located at the bottom right.

# Objective-See – LuLu Firewall

## /Library/Objective-See/LuLu/LuLu.log

- Firewall Status
- Software Installation/Updates by User
- Install Locations
- Associated IP Address/Ports
- Process IDs
- Signing Information
- Entitlements
- Bundle Identifier

```
2019-01-01 20:12:00 +0000: alert reply: {  
    action = 0;  
    args = ( /Applications/Hex Fiend.app/Contents/MacOS/Hex Fiend ,  
             "-psn_0_155686" );  
    hostName = "raw.githubusercontent.com";  
    ipAddr = "151.101.248.133";  
    path = "/Applications/Hex Fiend.app/Contents/MacOS/Hex Fiend";  
    pid = 345;  
    port = 443;  
    protocol = 1;  
    signingInfo = {  
        signatureAuthorities = ( "Developer ID Application: Kevin Wojniak (QK92QP33YN)" ,  
                                 "Developer ID Certification Authority" ,  
                                 "Apple Root CA" );  
        signatureEntitlements = { "com.apple.security.app-sandbox" = 0 ;  
                                 "com.apple.security.get-task-allow" = 1 };  
        signatureIdentifier = "com.ridiculousfish.HexFiend";  
        signatureSigner = 3;  
        signatureStatus = 0; };  
    tempRule = 0;  
    user = 501;  
}
```



# OBJECTIVE-SEE OVERSIGHT



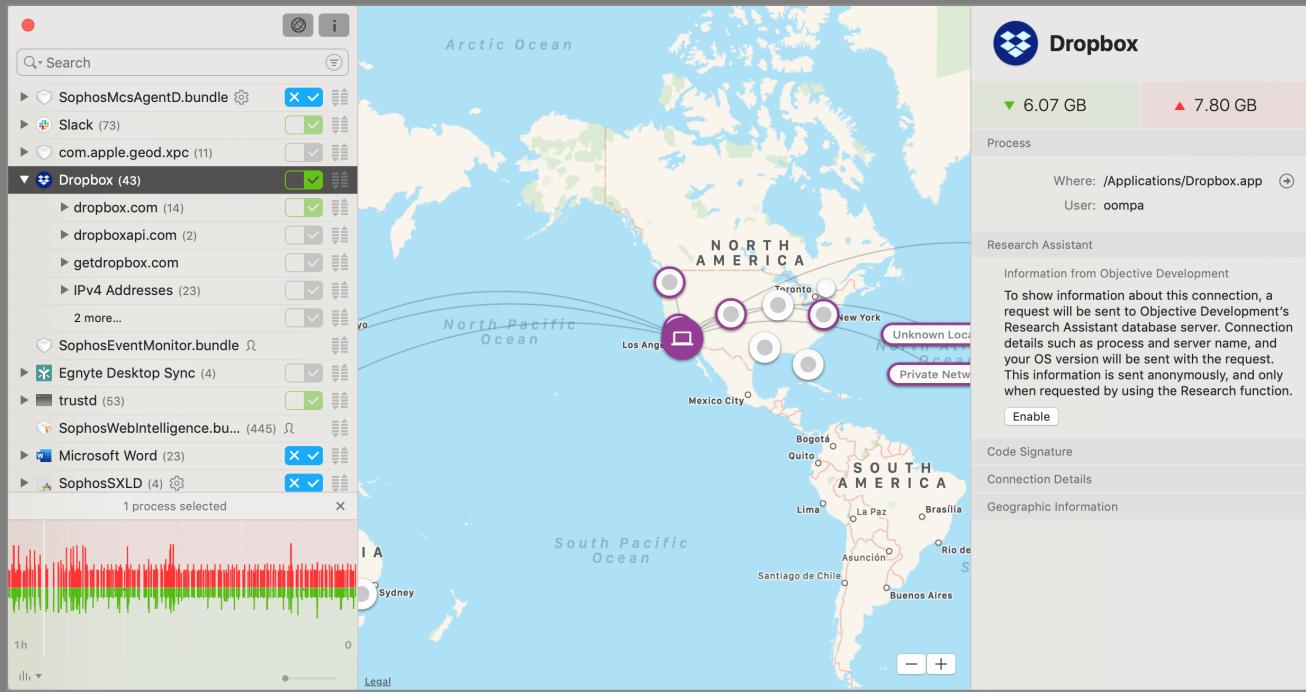
# Objective-See – Oversight

~/Library/Application Support/Objective-See/OverSight/OverSight.log

```
2018-12-15 19:51:39 +0000: Video Device became active (FaceTime HD Camera, process: FaceTime, /Applications/FaceTime.app/Contents/MacOS/FaceTime)
2018-12-15 19:52:05 +0000: Video Device became inactive (FaceTime HD Camera)
2018-12-15 19:52:07 +0000: user clicked 'block' for {
    alertType = 1;
    device = 2;
    processID = 2893;
    processName = FaceTime;
    processPath = "/Applications/FaceTime.app/Contents/MacOS/FaceTime";
}
2018-12-16 21:42:41 +0000: Video Device became active (FaceTime HD Camera, process: FaceTime, /Applications/FaceTime.app/Contents/MacOS/FaceTime)
2018-12-16 21:42:45 +0000: Video Device became inactive (FaceTime HD Camera)
2018-12-16 21:42:47 +0000: user clicked 'block' for {
    alertType = 1;
    device = 2;
    processID = 27370;
    processName = FaceTime;
    processPath = "/Applications/FaceTime.app/Contents/MacOS/FaceTime";
}
2018-12-17 22:57:21 +0000: Video Device became active (FaceTime HD Camera, process: GoToMeeting, /Users/oompa/Applications/GoToMeeting (11282).app/Contents/MacOS/GoToMeeting)
2018-12-17 22:57:50 +0000: user clicked 'allow' for {
    activationType = 4;
    alertType = 1;
    device = 2;
    processID = 64395;
    processName = GoToMeeting;
    processPath = "/Users/oompa/Applications/GoToMeeting (11282).app/Contents/MacOS/GoToMeeting";
}
```



# LITTLE SNITCH NETWORK MONITOR



# Little Snitch - Network Monitor

## ~/Library/Logs/Little Snitch Network Monitor.log

```
2019-01-25 11:17:46.331 Little Snitch Network Monitor[508:6221] Little Snitch Network Monitor version 5210 started.
2019-01-27 09:45:04.522 Little Snitch Network Monitor[508:6221] Freeing 989 physical connections, example connection: LSMPhysicalConnection (0x600001f7f180): Xcode -> miphonex.local:62078
2019-01-27 19:19:50.721 Little Snitch Network Monitor[508:6221] Freeing 768 physical connections, example connection: LSMPhysicalConnection (0x600001f55300): iTunes via ath -> fe80::1c72:23b3:b07e:7752:62078
2019-01-27 19:19:54.719 Little Snitch Network Monitor[508:6221] Freeing 2307 physical connections, example connection: LSMPhysicalConnection (0x600001f66900): iTunes -> client-api.itunes.apple.com:443
2019-02-06 20:14:08.454 Little Snitch Network Monitor[508:6221] Freeing 1287 physical connections, example connection: LSMPhysicalConnection (0x600001c7cd00): Dropbox -> api.dropboxapi.com:443
2019-02-11 08:08:42.077 Little Snitch Network Monitor[508:6221] Freeing 1182 physical connections, example connection: LSMPhysicalConnection (0x600005f54c80): Mail -> mail.csh.rit.edu:143
2019-02-11 08:08:47.077 Little Snitch Network Monitor[508:6221] Freeing 726 physical connections, example connection: LSMPhysicalConnection (0x600001f6f500): Safari -> static1.squarespace.com:443
2019-02-11 08:08:52.077 Little Snitch Network Monitor[508:6221] Freeing 3685 physical connections, example connection: LSMPhysicalConnection (0x600001dd7600): Safari -> bolt.dropbox.com:443
2019-02-11 10:49:52.632 Little Snitch Network Monitor[508:6221] Freeing 2421 physical connections, example connection: LSMPhysicalConnection (0x600005dd0d00): iTunes -> is1-ssl.mzstatic.com:443
2019-02-11 10:51:58.216 Little Snitch Network Monitor[507:6377] Little Snitch Network Monitor version 5210 started.
2019-02-13 14:30:15.694 Little Snitch Network Monitor[507:6377] Freeing 2672 physical connections, example connection: LSMPhysicalConnection (0x60000073b600): iTunes -> ld-5.itunes.apple.com:443
2019-02-14 18:19:50.592 Little Snitch Network Monitor[507:6377] Freeing 475 physical connections, example connection: LSMPhysicalConnection (0x6000007aad80): Microsoft PowerPoint -> nexus.officeapps.live.com:443
2019-02-15 12:50:29.294 Little Snitch Network Monitor[507:6377] Freeing 2650 physical connections, example connection: LSMPhysicalConnection (0x600000431b80): iTunes -> inititunes.apple.com:443
2019-02-16 09:17:43.572 Little Snitch Network Monitor[507:6377] Freeing 1635 physical connections, example connection: LSMPhysicalConnection (0x600000763000): BlackLight via postgres <- localhost:20220
2019-02-23 08:48:34.353 Little Snitch Network Monitor[507:6377] Freeing 2652 physical connections, example connection: LSMPhysicalConnection (0x6000007cbc00): Dropbox -> bolt.dropbox.com:443
2019-02-27 22:56:48.815 Little Snitch Network Monitor[507:6377] Freeing 1865 physical connections, example connection: LSMPhysicalConnection (0x60000c71b900): Mail -> imap.gmail.com:993
2019-03-02 20:29:33.168 Little Snitch Network Monitor[507:6377] Freeing 3596 physical connections, example connection: LSMPhysicalConnection (0x600010787900): iTunes -> is4-ssl.mzstatic.com:443
2019-03-05 17:26:11.695 Little Snitch Network Monitor[507:6377] Freeing 2529 physical connections, example connection: LSMPhysicalConnection (0x60000c693b00): Dropbox -> client.dropbox.com:443
2019-03-09 19:15:48.362 Little Snitch Network Monitor[507:6377] 4.2.4 (5210): lsd died
2019-03-09 19:26:59.515 Little Snitch Network Monitor[570:6891] Little Snitch Network Monitor version 5267 started.
2019-03-31 08:38:58.809 Little Snitch Network Monitor[570:6891] Freeing 299 physical connections, example connection: LSMPhysicalConnection (0x600000bbcbb00): Xcode -> miphonex.local:62078
2019-03-31 08:53:10.985 Little Snitch Network Monitor[451:6870] Little Snitch Network Monitor version 5267 started.
2019-04-01 08:20:11.968 Little Snitch Network Monitor[480:5219] Little Snitch Network Monitor version 5267 started.
2019-04-23 18:49:29.425 Little Snitch Network Monitor[480:5219] Freeing 733 physical connections, example connection: LSMPhysicalConnection (0x600002c8ff00): Xcode -> miphonex.local:49966
2019-05-12 16:46:59.798 Little Snitch Network Monitor[480:5219] 4.3.1 (5267): lsd died
2019-05-12 16:51:31.534 Little Snitch Network Monitor[464:4457] Little Snitch Network Monitor version 5284 started.
2019-05-20 08:17:07.292 Little Snitch Network Monitor[473:4307] Little Snitch Network Monitor version 5284 started.
2019-05-21 08:26:23.785 Little Snitch Network Monitor[375:3715] Little Snitch Network Monitor version 5284 started.
2019-05-23 08:44:44.259 Little Snitch Network Monitor[364:3700] Little Snitch Network Monitor version 5284 started.
2019-05-23 08:46:47.264 Little Snitch Network Monitor[364:3700] Freeing 334 physical connections, example connection: LSMPhysicalConnection (0x600000946c80): Mail -> imap.gmail.com:993
```

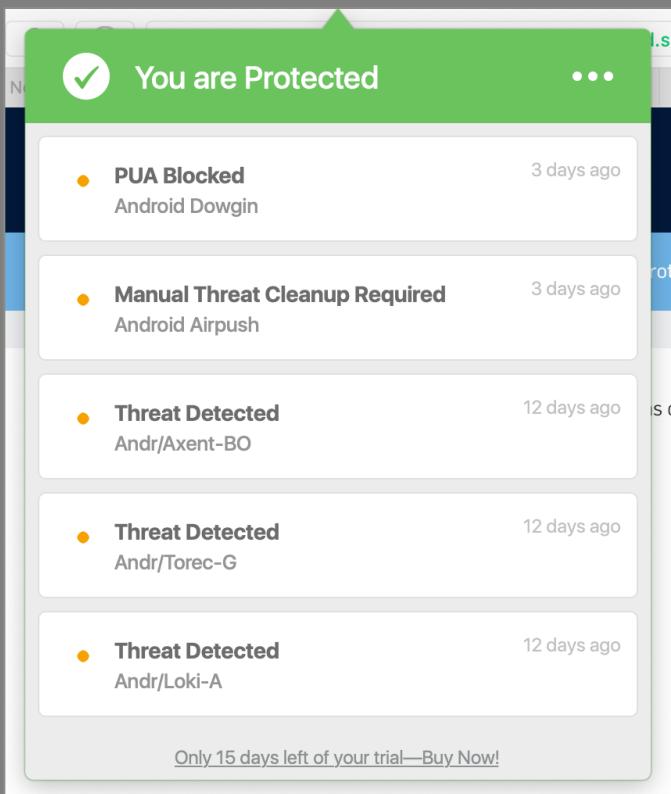


# Little Snitch - Network Monitor

## ~/Library/Logs/Little Snitch Network Monitor.log

```
Little Snitch Network Monitor version 5210 started.
Freeing 989 physical connections, example connection: LSMPhysicalConnection (0x600001f7f180): Xcode -> miphonex.local:62078
Freeing 768 physical connections, example connection: LSMPhysicalConnection (0x600001f55300): iTunes via ath -> fe80::1c72:23b3:b07e:7752:62078
Freeing 2307 physical connections, example connection: LSMPhysicalConnection (0x600001f66900): iTunes -> client-api.itunes.apple.com:443
Freeing 1287 physical connections, example connection: LSMPhysicalConnection (0x600001c7cd00): Dropbox -> api.dropboxapi.com:443
Freeing 1182 physical connections, example connection: LSMPhysicalConnection (0x600005f54c80): Mail -> mail.csh.rit.edu:143
Freeing 726 physical connections, example connection: LSMPhysicalConnection (0x600001f6f500): Safari -> static1.squarespace.com:443
Freeing 3685 physical connections, example connection: LSMPhysicalConnection (0x600001dd7600): Safari -> bolt.dropbox.com:443
Freeing 2421 physical connections, example connection: LSMPhysicalConnection (0x600005dd0d00): iTunes -> is1-ssl.mzstatic.com:443
Little Snitch Network Monitor version 5210 started.
Freeing 2672 physical connections, example connection: LSMPhysicalConnection (0x60000073b600): iTunes -> ld-5.itunes.apple.com:443
Freeing 475 physical connections, example connection: LSMPhysicalConnection (0x6000007aad80): Microsoft PowerPoint -> nexus.officeapps.live.com:443
Freeing 2650 physical connections, example connection: LSMPhysicalConnection (0x600000431b80): iTunes -> init.itunes.apple.com:443
Freeing 1635 physical connections, example connection: LSMPhysicalConnection (0x600000763000): BlackLight via postgres <- localhost:20220
Freeing 2652 physical connections, example connection: LSMPhysicalConnection (0x6000007cbc00): Dropbox -> bolt.dropbox.com:443
Freeing 1865 physical connections, example connection: LSMPhysicalConnection (0x60000c71b900): Mail -> imap.gmail.com:993
Freeing 3596 physical connections, example connection: LSMPhysicalConnection (0x600010787900): iTunes -> is4-ssl.mzstatic.com:443
Freeing 2529 physical connections, example connection: LSMPhysicalConnection (0x60000c693b00): Dropbox -> client.dropbox.com:443
4.2.4 (5210): lsd died
Little Snitch Network Monitor version 5267 started.
Freeing 299 physical connections, example connection: LSMPhysicalConnection (0x600000bbcb00): Xcode -> miphonex.local:62078
Little Snitch Network Monitor version 5267 started.
Little Snitch Network Monitor version 5267 started.
Freeing 733 physical connections, example connection: LSMPhysicalConnection (0x600002c8ff00): Xcode -> miphonex.local:49966
4.3.1 (5267): lsd died
Little Snitch Network Monitor version 5284 started.
Freeing 334 physical connections, example connection: LSMPhysicalConnection (0x600000946c80): Mail -> imap.gmail.com:993
```

# SOPHOS ANTIVIRUS



# Sophos - Files & Volumes

## /Library/Sophos Anti-Virus/events.db

```
1 select
2     datetime(zdetectiondate+978307200,'unixepoch') as DETECTION_DATE,
3     zdetectionpath,
4     zdetectionuser,
5     zthreatlongname
6     from ZTHREATLOCATION
7     left join ZEVENT on zevent.Z_PK = ZTHREATLOCATION.ZTHREATEVENT
```

	DETECTION_DATE	ZDETECTIONPATH	ZDETECTIONUSER	ZTHREATLONGNAME
1	2019-05-19 05:55:32	/Users/oompa/Downloads/Lazarus/CelasTradePro-Installer.dmg	oompa	OSX/Lazarus-D
2	2019-05-18 21:55:30	/Users/oompa/Downloads/Lazarus/Updater	oompa	OSX/Lazarus-D
3	2019-05-18 21:55:42	/Users/oompa/Downloads/Lazarus/Updater	oompa	OSX/Lazarus-D
4	2019-05-19 01:32:02	/Users/oompa/Library/Mail/V6/49285778-1207-4AB3-8F55-EE3A063B6743/[Gmail].mbox/All Mail.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/...	oompa	OSX/Imuler-B
5	2019-05-19 01:24:11	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/INBOX.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/1/6/Attachme...	oompa	Mal/DrodZp-A
6	2019-05-19 01:24:16	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/INBOX.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/1/6/Attachme...	oompa	Mal/DrodZp-A
7	2019-05-19 01:26:10	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/INBOX.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/5/6/Attachme...	oompa	Mal/DrodZp-A
8	2019-05-19 01:26:14	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/INBOX.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/5/6/Attachme...	oompa	Mal/DrodZp-A
9	2019-05-19 01:18:18	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/INBOX.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/9/9/Attachme...	oompa	Mal/DrodZp-A
10	2019-05-19 01:18:19	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/INBOX.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/9/9/Attachme...	oompa	Mal/DrodZp-A
11	2019-05-19 01:28:09	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/Sent Messages.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/7/9/A...	oompa	OSX/Imuler-B
12	2019-05-19 01:30:04	/Users/oompa/Library/Mail/V6/F37CEC82-FE8E-46B6-B236-CBF1D57D5D85/Sent Messages.mbox/57323BCC-F4E8-4B36-916F-8FA70C262EB0/Data/7/9/A...	oompa	OSX/Imuler-B
13	2019-05-21 12:13:30	/Volumes/DFIRNETWARS/SANS DFIR NETWARS KEY TOOLS/Windows Forensics/SysinternalsSuite/PsExec.exe	oompa	PsExec
14	2019-05-21 12:13:08	/Volumes/DFIRNETWARS/SANS DFIR NETWARS KEY TOOLS/Windows Forensics/SysinternalsSuite/pskill.exe	oompa	PsKill
15	2019-05-21 12:13:25	/Volumes/DFIRNETWARS/SANS DFIR NETWARS KEY TOOLS/Windows Forensics/command line tools/PsExec.exe	oompa	PsExec
16	2019-05-21 12:13:08	/Volumes/DFIRNETWARS/SANS DFIR NETWARS KEY TOOLS/Windows Forensics/command line tools/pskill.exe	oompa	PsKill

# Sophos – Network Connections

## /Library/Logs/SophosDiagnostics\*.gz

```
2019-05-25 09:46:07.358 [SophosWebIntelligence 265:2740 webengine] Closing connection 0x7fa6c1f03710 for 'https://oasc17.247realmedia.com': request=517b, response=0b, lifetime=99ms, businessLogicDelay=10ms, timeInCache=1ms
2019-05-25 09:46:07.515 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2f8a220 for 'https://events.airoav.com': request=517b, response=0b, lifetime=8ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:08.377 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2cb1650 for 'https://www.united.com': request=517b, response=0b, lifetime=33ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:10.604 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb591f7d0 for 'https://oasc17.247realmedia.com': request=517b, response=0b, lifetime=16ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:13.188 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2d7c930 for 'https://www.united.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:13.194 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2e23430 for 'https://www.united.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:13.227 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2dd9420 for 'https://cdn.optimizely.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:14.493 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2d7c930 for 'https://media.united.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:14.650 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2f8a220 for 'https://snowflake.bjango.com': request=517b, response=0b, lifetime=152ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:15.390 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2c323a0 for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=148ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:15.397 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2d56f70 for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=149ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:15.401 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2e74eb0 for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=157ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:15.410 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb5841600 for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=164ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:18.026 [SophosEventMonitor 267:2877 webengine] Request url 'https://7fadb2fd0740 for 'https://gateway.icloud.com': request=517b, response=0b, lifetime=14ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:37.186 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2e2f5e0 for 'https://dci.sophosupd.com': request=517b, response=0b, lifetime=12ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:39.538 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2c12e30 for 'https://dci.sophosupd.net': request=517b, response=0b, lifetime=5ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:41.916 [SophosWebIntelligence 265:2740 webengine] Closing connection 0x7fa6c1c155e0 for 'https://oasc17.247realmedia.com': request=1754b, response=29422b, lifetime=31327ms, firstResponse=200ms, businessLogicDelay=2ms, in=200ms, out=1012ms, l.eos=31326ms
2019-05-25 09:46:42.705 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2f946a0 for 'https://dzc-mcs-amzn-us-east-1-h0m3.up.e.p.hmr.sophos.com': request=517b, response=0b, lifetime=93ms, businessLogicDelay=0ms
2019-05-25 09:46:42.775 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2ca5af0 for 'https://play.itunes.apple.com': request=181b, response=0b, lifetime=17ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:43.206 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb2da8770 for 'https://aod.itunes.apple.com': request=180b, response=0b, lifetime=5ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:50.093 [SophosEventMonitor 267:2877 webengine] Closing connection 0x7fadb5813c30 for 'https://www.viator.com': request=517b, response=0b, lifetime=1ms, businessLogicDelay=0ms, timeInCache=0ms
2019-05-25 09:46:53.319 [SophosWebIntelligence 265:2740 webengine] Closing connection 0x7fa6c1c10fa0 for 'https://cdn.optimizely.com': request=1050b, response=3902b, lifetime=40085ms, firstResponse=23ms, businessLogicDelay=1ms, in=23ms, out=40084ms, r.eos=40084ms
```



# Sophos – Network Connections

## /Library/Logs/SophosDiagnostics\*.gz

```
?10 for 'https://oasc17.247realmedia.com': request=517b, response=0b, lifetime=99ms, businessLogicDelay=10ms, timeInCache=1ms
for 'https://eventsairoav.com': request=517b, response=0b, lifetime=8ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://www.united.com': request=517b, response=0b, lifetime=33ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://oasc17.247realmedia.com': request=517b, response=0b, lifetime=16ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://www.united.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://www.united.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://cdn.optimizely.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://media.united.com': request=517b, response=0b, lifetime=0ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://snowflake.bjango.com': request=517b, response=0b, lifetime=152ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=148ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=149ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=157ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://snowflake2.bjango.com': request=517b, response=0b, lifetime=164ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://gateway.icloud.com': request=517b, response=0b, lifetime=14ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://dci.sophosupd.com': request=517b, response=0b, lifetime=12ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://dci.sophosupd.net': request=517b, response=0b, lifetime=5ms, businessLogicDelay=0ms, timeInCache=0ms
5e0 for 'https://oasc17.247realmedia.com': request=1754b, response=29422b, lifetime=31327ms, firstResponse=200ms, businessLogicDelay=10ms
for 'https://dzc-mcs-amzn-us-east-1-h0m3.up.e.p.hmr.sophos.com': request=517b, response=0b, lifetime=93ms, businessLogicDelay=0ms
for 'https://play.itunes.apple.com': request=181b, response=0b, lifetime=17ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://aod.itunes.apple.com': request=180b, response=0b, lifetime=5ms, businessLogicDelay=0ms, timeInCache=0ms
for 'https://www.viator.com': request=517b, response=0b, lifetime=1ms, businessLogicDelay=0ms, timeInCache=0ms
fa0 for 'https://cdn.optimizely.com': request=1050b, response=3902b, lifetime=40085ms, firstResponse=23ms, businessLogicDelay=0ms
```

# Sophos – Web Visits

## /Library/Logs/SophosDiagnostics\*.gz

```
2019-05-25 09:03:32.213 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.213175, URL : http://marriottinternational.demdex.net/event?d_cid=64650%0117B72965362B70102859951904871947B.01%010&d_event=imp&c_mailingname=2019_03_12_OBOP_Prod_PreachArrival, pid : 14513}
2019-05-25 09:03:32.231 [SophosEventMonitor 267:4365481 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.231278, URL : http://epidm.edgesuite.net/CMS/Coding/Marriott/RTM/2017/dot.gif, pid : 14513}
2019-05-25 09:03:32.232 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.232048, URL : http://epidm.edgesuite.net/CMS/Coding/Marriott/RTM/2017/24_11172017_confirmation-template-final-black.png, pid : 14513}
2019-05-25 09:03:32.308 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.307705, URL : http://www.marriott.com/Images/email/apm/APMV2/Hertz1.jpg, pid : 14513}
2019-05-25 09:03:32.308 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.308482, URL : http://www.marriott.com/Images/email/apm/APMV2/LM_avecamour_pattern1.jpg, pid : 14513}
2019-05-25 09:03:32.310 [SophosEventMonitor 267:4365479 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.309620, URL : http://www.marriott.com/Images/email/apm/APMV2/PlacePass.jpg, pid : 14513}
2019-05-25 09:03:32.359 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 443, isBrowser : 1, timestamp : 1558767812.359156, URL : https://www.marriott.com, pid : 14513}
2019-05-25 09:03:32.389 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 443, isBrowser : 1, timestamp : 1558767812.388893, URL : https://cache.marriott.com, pid : 14513}
2019-05-25 09:03:32.389 [SophosEventMonitor 267:4365046 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.389136, URL : http://cache.marriott.com/aka-fonts/proxima-nova-regular.woff, pid : 14513}
2019-05-25 09:03:32.390 [SophosEventMonitor 267:4365481 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 80, isBrowser : 1, timestamp : 1558767812.389707, URL : http://cache.marriott.com/aka-fonts/LeMeridien/GriffithGothic-Light.woff, pid : 14513}
2019-05-25 09:03:32.700 [SophosEventMonitor 267:4365479 EventRecord exclude] [SMEEEventRecord.m:104] Browser connection is ignored. Event: {isProxy : 0, ipVersion : 4, eventType : SMEEEventNetworkKextConnection, destPort : 443, isBrowser : 1, timestamp : 1558767812.699769, URL : https://res-marriott.com, pid : 14513}
```

# Sophos – Processes

## /Library/Logs/SophosDiagnostics\*.gz

```
2019-05-30 13:51:49.529 [SophosCryptoGuard 263:2761 context signature] Process: /Applications/Utilities/Terminal.app/Contents/MacOS/Terminal (29292) is Apple signed
2019-05-30 13:51:49.529 [SophosCryptoGuard 263:2761 context signature] Process: /Applications/Utilities/Terminal.app/Contents/MacOS/Terminal (29292) Signature Identifier: com.apple.Terminal and TeamID: (null)
2019-05-30 13:51:49.576 [SophosCryptoGuard 263:2761 context signature] Process: /usr/bin/login (29292) is Apple signed
2019-05-30 13:51:49.576 [SophosCryptoGuard 263:2761 context signature] Process: /usr/bin/login (29292) Signature Identifier: com.apple.login and TeamID: (null)
2019-05-30 13:51:49.925 [SophosCryptoGuard 263:2761 context signature] Process: /usr/bin/login (29293) is Apple signed
2019-05-30 13:51:49.925 [SophosCryptoGuard 263:2761 context signature] Process: /usr/bin/login (29293) Signature Identifier: com.apple.login and TeamID: (null)
2019-05-30 13:51:49.970 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29293) is Apple signed
2019-05-30 13:51:49.970 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29293) Signature Identifier: com.apple.bash and TeamID: (null)
2019-05-30 13:51:50.020 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29293) is Apple signed
2019-05-30 13:51:50.020 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29293) Signature Identifier: com.apple.bash and TeamID: (null)
2019-05-30 13:51:50.034 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29294) is Apple signed
2019-05-30 13:51:50.034 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29294) Signature Identifier: com.apple.bash and TeamID: (null)
2019-05-30 13:51:50.081 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29295) is Apple signed
2019-05-30 13:51:50.081 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29295) Signature Identifier: com.apple.bash and TeamID: (null)
2019-05-30 13:51:50.117 [SophosCryptoGuard 263:2761 context signature] Process: /usr/libexec/path_helper (29295) is Apple signed
2019-05-30 13:51:50.117 [SophosCryptoGuard 263:2761 context signature] Process: /usr/libexec/path_helper (29295) Signature Identifier: com.apple.path_helper and TeamID: (null)
2019-05-30 13:51:50.131 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29296) is Apple signed
2019-05-30 13:51:50.131 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29296) Signature Identifier: com.apple.bash and TeamID: (null)
2019-05-30 13:51:50.161 [SophosCryptoGuard 263:2761 context signature] Process: /bin/mkdir (29296) is Apple signed
2019-05-30 13:51:50.161 [SophosCryptoGuard 263:2761 context signature] Process: /bin/mkdir (29296) Signature Identifier: com.apple.mkdir and TeamID: (null)
2019-05-30 13:51:50.210 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29297) is Apple signed
2019-05-30 13:51:50.210 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29297) Signature Identifier: com.apple.bash and TeamID: (null)
2019-05-30 13:51:50.220 [SophosCryptoGuard 263:2761 context signature] Process: /Users/oompa/anaconda3/bin/python3.7 (29298) is unsigned
2019-05-30 13:51:50.225 [SophosCryptoGuard 263:2761 context signature] Process: /Users/oompa/anaconda3/bin/conda (29298) is unsigned
2019-05-30 13:51:50.230 [SophosCryptoGuard 263:2761 context signature] Process: /Users/oompa/anaconda3/bin/python3.7 (29298) is unsigned
2019-05-30 13:51:52.675 [SophosCryptoGuard 263:2761 context signature] Process: /Users/oompa/anaconda3/bin/python3.7 (29299) is unsigned
2019-05-30 13:51:52.730 [SophosCryptoGuard 263:2761 context signature] Process: /bin/sh (29299) is Apple signed
2019-05-30 13:51:52.730 [SophosCryptoGuard 263:2761 context signature] Process: /bin/sh (29299) Signature Identifier: com.apple.sh and TeamID: (null)
2019-05-30 13:51:52.772 [SophosCryptoGuard 263:2761 context signature] Process: /bin/sh (29300) is Apple signed
2019-05-30 13:51:52.772 [SophosCryptoGuard 263:2761 context signature] Process: /bin/sh (29300) Signature Identifier: com.apple.sh and TeamID: (null)
2019-05-30 13:51:52.782 [SophosCryptoGuard 263:2761 context signature] Process: /usr/bin/uname (29300) is Apple signed
2019-05-30 13:51:52.782 [SophosCryptoGuard 263:2761 context signature] Process: /usr/bin/uname (29300) Signature Identifier: com.apple.uname and TeamID: (null)
2019-05-30 13:51:54.173 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29301) is Apple signed
2019-05-30 13:51:54.174 [SophosCryptoGuard 263:2761 context signature] Process: /bin/bash (29301) Signature Identifier: com.apple.bash and TeamID: (null)
```



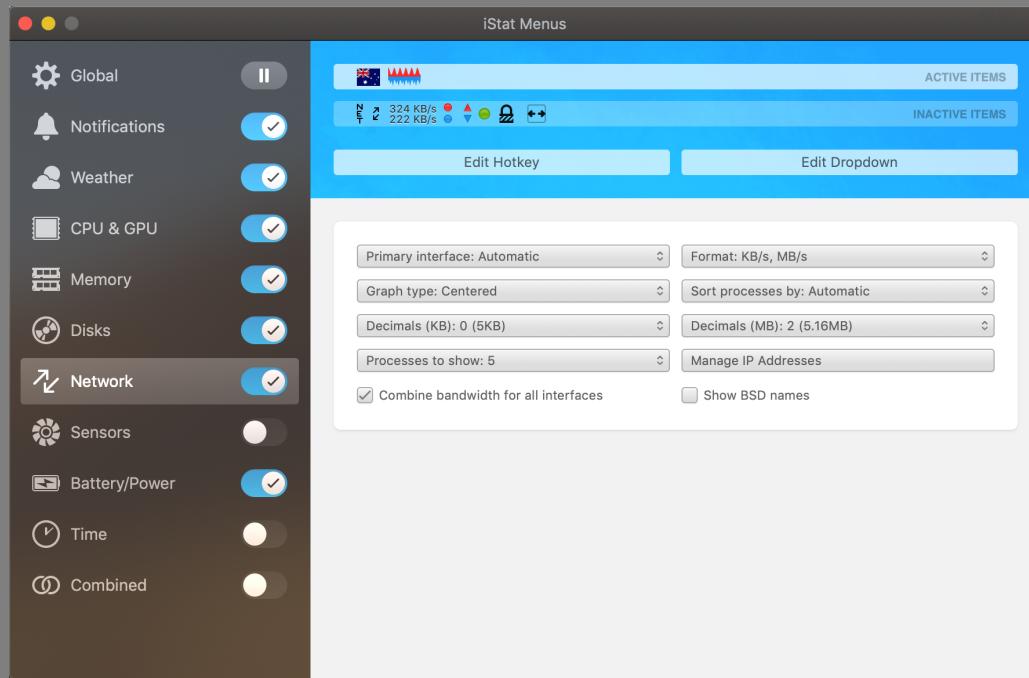
# Sophos – Processes

## /Library/Logs/SophosDiagnostics\*.gz

```
Process: /Applications/Utilities/Terminal.app/Contents/MacOS/Terminal (29292) is Apple signed
Process: /Applications/Utilities/Terminal.app/Contents/MacOS/Terminal (29292) Signature Identifier: com.apple.Terminal and TeamID: (null)
Process: /usr/bin/login (29292) is Apple signed
Process: /usr/bin/login (29292) Signature Identifier: com.apple.login and TeamID: (null)
Process: /usr/bin/login (29293) is Apple signed
Process: /usr/bin/login (29293) Signature Identifier: com.apple.login and TeamID: (null)
Process: /bin/bash (29293) is Apple signed
Process: /bin/bash (29293) Signature Identifier: com.apple.bash and TeamID: (null)
Process: /bin/bash (29293) is Apple signed
Process: /bin/bash (29293) Signature Identifier: com.apple.bash and TeamID: (null)
Process: /bin/bash (29294) is Apple signed
Process: /bin/bash (29294) Signature Identifier: com.apple.bash and TeamID: (null)
Process: /bin/bash (29295) is Apple signed
Process: /bin/bash (29295) Signature Identifier: com.apple.bash and TeamID: (null)
Process: /usr/libexec/path_helper (29295) is Apple signed
Process: /usr/libexec/path_helper (29295) Signature Identifier: com.apple.path_helper and TeamID: (null)
Process: /bin/bash (29296) is Apple signed
Process: /bin/bash (29296) Signature Identifier: com.apple.bash and TeamID: (null)
Process: /bin/mkdir (29296) is Apple signed
Process: /bin/mkdir (29296) Signature Identifier: com.apple.mkdir and TeamID: (null)
Process: /bin/bash (29297) is Apple signed
Process: /bin/bash (29297) Signature Identifier: com.apple.bash and TeamID: (null)
Process: /Users/oompa/anaconda3/bin/python3.7 (29298) is unsigned
Process: /Users/oompa/anaconda3/bin/conda (29298) is unsigned
Process: /Users/oompa/anaconda3/bin/python3.7 (29298) is unsigned
Process: /Users/oompa/anaconda3/bin/python3.7 (29299) is unsigned
Process: /bin/sh (29299) is Apple signed
Process: /bin/sh (29299) Signature Identifier: com.apple.sh and TeamID: (null)
Process: /bin/sh (29300) is Apple signed
Process: /bin/sh (29300) Signature Identifier: com.apple.sh and TeamID: (null)
Process: /usr/bin/uname (29300) is Apple signed
Process: /usr/bin/uname (29300) Signature Identifier: com.apple.uname and TeamID: (null)
Process: /bin/bash (29301) is Apple signed
Process: /bin/bash (29301) Signature Identifier: com.apple.bash and TeamID: (null)
```



# ISTAT MENUS SYSTEM MONITOR



# iStat Menus – Sleep & Showdown Status

## /Library/Application Support/iStat Menus 6/uptime.db

```
1 select
2 datetime(start,'unixepoch') as START,
3 datetime(end,'unixepoch') as END,
4 (END - START) as "TOTAL SLEEPTIME (Seconds)"
5 from sleep
```

	START	END	TOTAL SLEEPTIME (Seconds)
582	2019-05-23 15:54:22	2019-05-23 16:01:14	411.863147974014
583	2019-05-23 19:30:23	2019-05-24 06:23:17	39173.9351830482
584	2019-05-24 06:23:38	2019-05-24 06:36:29	771.645309925079
585	2019-05-24 15:58:46	2019-05-24 16:02:49	243.306120872498
586	2019-05-24 19:50:49	2019-05-25 06:44:49	39240.5683829784
587	2019-05-25 06:44:54	2019-05-25 06:44:56	1.63985085487366
588	2019-05-25 12:02:11	2019-05-25 12:18:15	963.722643136978
589	2019-05-25 12:18:31	2019-05-25 12:44:33	1561.35718083382
590	2019-05-25 13:00:11	2019-05-25 13:00:47	36.0671730041504
591	2019-05-25 13:26:25	2019-05-26 08:06:04	67178.7833242416
592	2019-05-26 09:19:49	2019-05-26 09:30:19	630.411379098892

```
1 select
2 datetime(boot,'unixepoch') as BOOT,
3 case shutdown
4 when "0" then 0
5 else datetime(shutdown,'unixepoch')
6 end SHUTDOWN
7 from uptime
```

	BOOT	SHUTDOWN
5	2018-12-15 16:40:31	2018-12-28 00:38:34
6	2018-12-28 00:39:49	2018-12-29 18:16:48
7	2018-12-28 00:39:53	2019-01-01 03:03:07
8	2019-01-01 03:05:42	2019-01-25 16:15:31
9	2019-01-25 16:16:19	2019-02-11 10:50:06
10	2019-02-11 10:50:36	2019-02-16 14:43:36
11	2019-02-11 10:50:51	2019-03-10 03:19:34
12	2019-03-10 03:25:37	2019-03-31 12:42:24
13	2019-03-31 12:51:32	2019-04-01 12:18:26

# iStat Menus – Network Usage

/Library/Application Support/iStat Menus 6/bandwidth.db

```
1 select
2 sample,
3 datetime(start,'unixepoch') as START,
4 datetime(end,'unixepoch') as END,
5 bandwidth_interface_map.interface,
6 bandwidth_wifi_map.name,
7 bandwidth_wifi_map.bssid,
8 upload,
9 download
10 from bandwidth_samples
11 left join bandwidth_interface_map on bandwidth_interface_map.identifier = bandwidth_samples.interface
12 left join bandwidth_wifi_map on bandwidth_wifi_map.identifier = bandwidth_samples.network
```

	sample	START	END	interface	name	bssid	upload	download
11626	11626	2019-05-26 09:30:19	2019-05-26 09:30:55	en0	ZurichAirport	78:72:5d:b8:bd:00	701440.0	763904.0
11627	11627	2019-05-26 09:30:55	2019-05-26 09:40:00	en0	ZurichAirport	78:0c:f0:12:e3:0f	875520.0	553984.0
11628	11628	2019-05-26 09:40:00	2019-05-26 09:50:00	en0	ZurichAirport	78:0c:f0:12:e3:0f	5902336.0	1134592.0
11629	11629	2019-05-26 09:50:00	2019-05-26 10:00:00	en0	ZurichAirport	78:0c:f0:12:e3:0f	1338368.0	596992.0
11630	11630	2019-05-26 10:00:00	2019-05-26 10:10:00	en0	ZurichAirport	78:0c:f0:12:e3:0f	2446336.0	3884032.0
11631	11631	2019-05-26 10:10:00	2019-05-26 10:18:29	en0	ZurichAirport	78:0c:f0:12:e3:0f	3245056.0	31963136.0
11632	11632	2019-05-26 10:18:29	2019-05-26 10:20:00	en0	ZurichAirport	78:0c:f0:12:e3:0f	108544.0	75776.0
11633	11633	2019-05-26 10:26:25	2019-05-26 10:30:00	en0	ZurichAirport	a0:23:9f:d9:56:a0	214016.0	196608.0
11634	11634	2019-05-27 19:27:54	2019-05-27 19:28:24	en0	ACCORHOTELS-GUESTS	40:18:b1:82:48:54	148480.0	1589248.0
11635	11635	2019-05-27 19:28:24	2019-05-27 19:30:00	en0	ACCORHOTELS-GUESTS	40:18:b1:81:e7:68	574464.0	603136.0

# iStat Menus - Sleep & Wake

## /Library/Logs/ iStat Menus /Daemon/ iStatMenuDaemon\*.log

```
[Sarahs-Fridge:Daemon oompa$ pwd  
/Library/Logs/iStat Menus/Daemon  
[Sarahs-Fridge:Daemon oompa$ ls -la  
total 176  
drwxr-xr-x 8 root wheel 256 May 13 01:50 .  
drwxr-xr-x 3 root wheel 96 Nov 30 02:04 ..  
-rw-r--r-- 1 root wheel 7402 May 30 13:02 daemon.log  
-rw-r--r--@ 1 root wheel 8511 Dec 29 20:05 iStatMenusDaemon 2018-11-30 01-04.log  
-rw-r--r--@ 1 root wheel 8594 Feb 11 09:07 iStatMenusDaemon 2018-12-30 04-12.log  
-rw-r--r--@ 1 root wheel 9989 Mar 22 02:54 iStatMenusDaemon 2019-02-11 10-50.log  
-rw-r--r--@ 1 root wheel 14026 May 13 01:49 iStatMenusDaemon 2019-03-23 13-48.log  
-rw-r--r-- 1 root wheel 24974 May 30 15:24 iStatMenusDaemon 2019-05-12 23-50.log
```

2019/05/23 08:43:37:383	Preparing smc
2019/05/23 08:43:37:383	Preparing network
2019/05/23 08:43:56:567	Preparing smart
2019/05/23 08:43:56:567	Preparing processes
2019/05/23 08:43:56:569	Preparing battery
2019/05/23 08:43:56:573	Preparing power notifier
2019/05/23 08:43:56:573	Preparing bandwidth
2019/05/23 08:43:56:665	Starting network
2019/05/23 08:43:56:666	Starting processes
2019/05/23 08:43:56:666	Daemon started
2019/05/23 17:54:22:557	sleep
2019/05/23 18:01:14:420	wake
2019/05/23 18:01:14:420	411.86
2019/05/23 21:30:23:072	sleep
2019/05/24 08:23:17:007	wake
2019/05/24 08:23:17:007	39173.94
2019/05/24 08:23:38:180	sleep
2019/05/24 08:36:29:826	wake
2019/05/24 08:36:29:826	771.65
2019/05/24 17:58:46:316	sleep
2019/05/24 18:02:49:622	wake
2019/05/24 18:02:49:622	243.31
2019/05/24 21:50:49:307	sleep
2019/05/25 08:44:49:875	wake
2019/05/25 08:44:49:875	39240.57
2019/05/25 08:44:54:564	sleep
2019/05/25 08:44:56:205	wake
2019/05/25 08:44:56:205	1.64
2019/05/25 14:02:11:505	sleep
2019/05/25 14:18:15:228	wake
2019/05/25 14:18:15:228	963.72
2019/05/25 14:18:31:848	sleep

# iStat Menus Power Status

- ~/Library/Application Support/iStat Menus/databases/iStatMenusStatus.db
- Also:
  - *Battery Percentage by*
    - Hour
    - Day
    - Week
    - Month

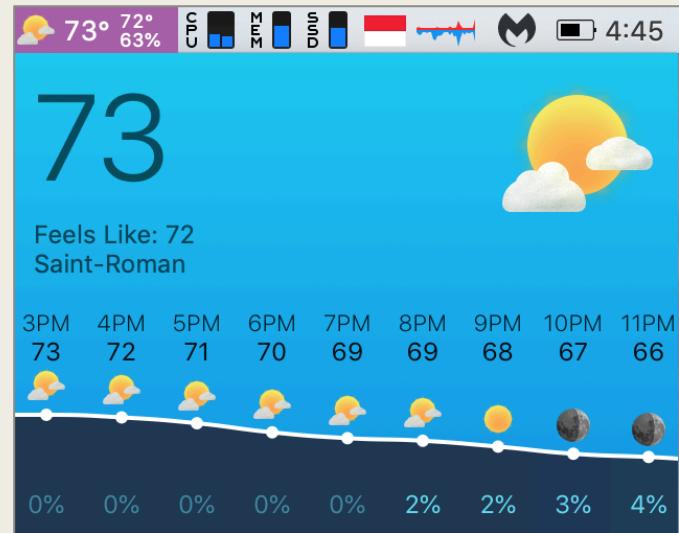
		uuid	source	TIMESTAMP
278	F5D84	F5D84	Unplugged	2019-04-21 14:42:47
279	F5D84		Plugged In	2019-04-21 17:01:03
280	F5D84		Unplugged	2019-04-21 23:53:49
281	F5D84		Plugged In	2019-04-22 00:30:57
282	F5D84		Unplugged	2019-04-24 00:32:16
283	F5D84		Plugged In	2019-04-24 01:46:56
284	F5D84		Unplugged	2019-05-02 04:07:04
285	F5D84		Plugged In	2019-05-03 14:25:22
286	F5D84		Unplugged	2019-05-05 02:31:22
287	F5D84		Plugged In	2019-05-05 06:37:00

# iStat Menus – Disk Status

~/Library/Application Support/iStat Menus/databases/iStatMenusStatus.db

## ■ By Hour, Day, Week, & Month

	1	select	2	datetime(time,'unixepoch','localtime') as TIMESTAMP,	3	uuid,	4	used,	5	size,	6	free	7	from day_diskhistory
76		2019-05-29 22:38:22		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952607940073.739		1500518756352.0		547910816278.261				
77		2019-05-29 22:40:46		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952611367980.522		1500518756352.0		547907388371.478				
78		2019-05-29 22:43:10		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952608684714.667		1500518756352.0		547910071637.333				
79		2019-05-29 22:43:10		D4F4D282-D342-30B7-B991-3B6375ABBA3A		42633134080.0		62911283200.0		20278149120.0				
80		2019-05-29 22:45:34		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		951558048871.884		1500518756352.0		548960707480.116				
81		2019-05-29 22:45:34		89B6ABB2-C7BA-355C-99C8-AD7E5285D2F2		45551294873.6		62911283200.0		17359988326.4				
82		2019-05-29 22:47:58		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952607327781.101		1500518756352.0		547911428570.898				
83		2019-05-29 22:50:22		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952611957181.217		1500518756352.0		547906799170.783				
84		2019-05-29 22:52:46		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952845288759.652		1500518756352.0		547673467592.348				
85		2019-05-29 22:55:10		B14200B0-B7E2-4F40-8CA0-9A313061BDF9		952805932966.957		1500518756352.0		547712823385.043				



# iStat Menus – Location

~/Library/Logs/iStat Menus/iStat Menus Status/status.log & Unified Logs

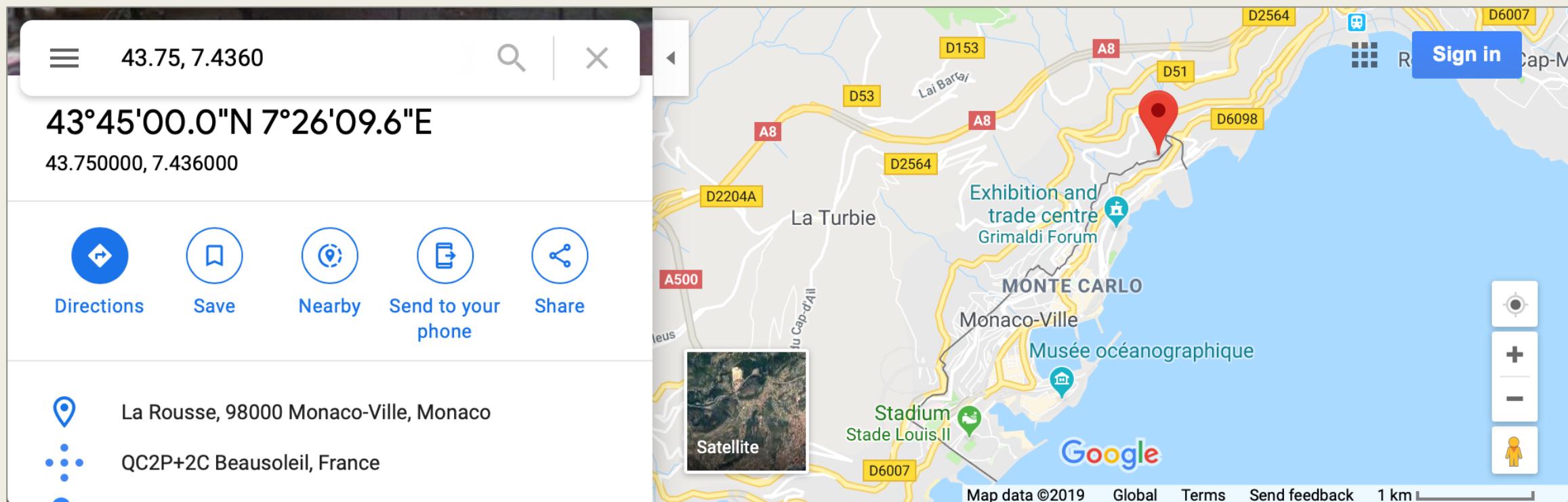
- Longitude, Latitude

```
2019-05-30 13:19:57.838 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4358, 43.75
2019-05-30 13:34:59.714 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 900.57
2019-05-30 13:35:01.367 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4358, 43.75
2019-05-30 13:50:03.156 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 900.75
2019-05-30 13:50:04.908 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 14:05:06.188 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 900.17
2019-05-30 14:05:07.891 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 14:20:10.403 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 901.51
2019-05-30 14:20:12.067 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 14:35:13.581 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 900.57
2019-05-30 14:35:15.347 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 14:57:30.333 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 1333.70
2019-05-30 14:57:31.024 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 15:25:18.320 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 1666.59
2019-05-30 15:25:18.357 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 15:40:20.834 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 901.49
2019-05-30 15:40:21.896 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
2019-05-30 15:55:23.567 iStat Menus Status[644:7980] need to fetch. seconds since last fetch 900.72
2019-05-30 15:55:25.081 iStat Menus Status[644:7980] Fetching weather for lcoation 7.4360, 43.75
```

# iStat Menus – Location

~/Library/Logs/iStat Menus/iStat Menus Status/status.log  
& Unified Logs

- Stored as Longitude, Latitude

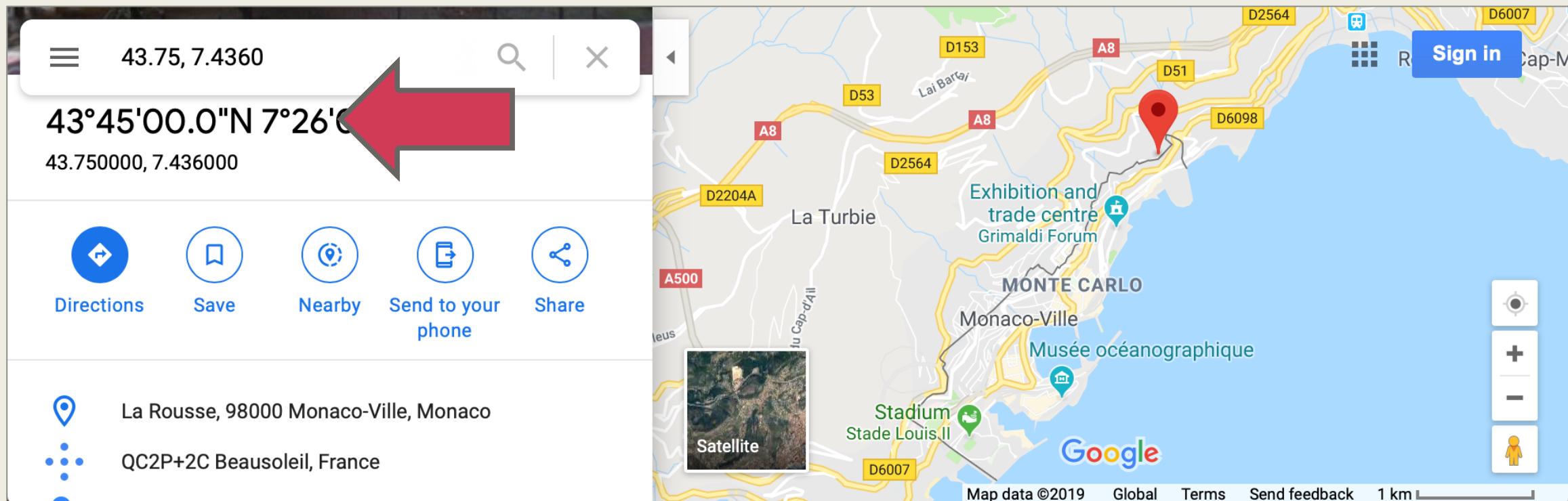


Detailed weather data in NSKeyedArchiver Plist: ~/Library/Caches/iStat Menus/Weather/-7/data.cache

# iStat Menus – Location

~/Library/Logs/iStat Menus/iStat Menus Status/status.log  
& Unified Logs

- Stored as Longitude, Latitude



Detailed weather data in NSKeyedArchiver Plist: ~/Library/Caches/iStat Menus/Weather/-7/data.cache

# Merci!

- Different applications log different data – some better than others.
- Your (sometimes sensitive) data are my investigative pivot points.
  - *How were you using your system?*
  - *When were you using your system?*
  - *Did you download anything, was it malicious, did you install it anyway?*
  - *What volumes did you have access to?*
  - *Where were you?*
- Twitter: @iamevlwin
- Blog & Presentations - [mac4n6.com](http://mac4n6.com)
- Take a class! Mac and iOS Forensic Analysis & Incident Response
  - [for518.com](http://for518.com)