Command Line:

```
lipo /Applications/Stickies.app/Contents/MacOS/Stickies -info

lsof -i - network connections
lsof -p 1 - open files from process id 1

alias
alias  name_of_alias=command


lsbom -p MUGsf bom file
```

Plists:

Plaintext Format - Json

```
less /Library/Receipts/InstallHistory.plist
plutil -p /Library/Receipts/InstallHistory.plist
```

Apps:

```
cd /Applications/application.app
ls
cd Contents
```

LaunchAgents/Daemons:

```
cd /System/Library/LaunchDaemons/
ls

cd /Library/LaunchDaemons/
ls

cd /System/Library/LaunchAgents/
ls

cd /Library/LaunchAgents/
ls

cd /Users/casper/Library/LaunchAgents
ls
```

/tmp:

```
cd /tmp
```

Browser Extensions:

```
cd /Users/currentuser/Library/Safari/Extensions
cd Library/Application\ Support/Google/Chrome/Default/Extensions/
ls
```

Kernel Extensions:

```
ls /System/Library/Extensions/
kextfind
```

Login Items:

demonstrate on the command line

Logs of interest:

```
less /var/log/install.log
Less /var/log/system.log
```

Quarantined items (from the internet)

```
sqlite3 ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2
select * from LSQuarantineEvent
```

Apple System Logs

```
less private/var/log/asl/
```

```
.bash_history
```

Sysdiagnose:

```
sudo sysdiagnose -f Desktop/ -a DC_Cyber_Meetup
```

Codesign:

```
plutil -p at.obdev.LittleSnitchUIAgent.plist
codesign -dvvvv /Library/Little\ Snitch/Little\ Snitch\ Agent.app/Contents/MacOS/Little\ 
Snitch\ Agent
```

Extended Attributes:

```
cd Downloads
Xattr -l
```

XProtect:

```
cd /System/Library/CoreServices/XProtect.bundle/Contents/Resources
Less XProtect.yara
```

SIP:

```
Cd /usr/bin
rm -f
```

Elevate to root

```
Cd /usr/bin
rm -f
```

MRT:

```
cd /System/Library/CoreServices/MRT.app/Contents/MacOS
strings MRT I less
```