Computer Forensics

Mac & Linux Forensics

Mac Forensics

Artifact Locations

User Folders

- Desktop
- Downloads
- Documents
- Pictures
- Movies

System Folders

- /Volumes
- /Application
- /Network
- /etc
- /Users/{username}/Library/Preferences/
- /Users/{username}/.Trash/

Mac Forensics

Mac Forensic Techniques

Obtaining date & time:

Start computer in single-user mode → hold down [Command] + [S] during power on

Type ”date” in the Terminal window

*NOTE This may not work on some computers due to user setting

Alternative acquisition of SSD/HDD (Difficult to physically access or inaccessible)

Connect forensic Mac computer to target Mac computer

Start computer in Target Mode → hold down [T] during power on

Run dd command or other imaging software from forensic Mac

Mac Forensics

Artifacts

System Information

- User/owner info
  /private/var/db/.AppleSetupDone
- OS version
  /System/Library/CoreServices/SystemVersion.plist
- OS Installation date
  /private/var/log/install.log
- Software Installation and OS update dates
  /Library/Receipts/InstallHistory.plist
- Login window info
  /Library/Preferences/com.apple.loginwindow.plist

Mac Forensics

Internet Artifacts

- Firefox

  ~/Library/Application/Support/Firefox/Profiles/*{alpha-numeric name}*/places.sqlite

  Other files: formhistory.sqlite, cookies.sqlite, login data

- Chrome

  ~/Library/Application/Support/Google/Chrome/Default/History

  Other files: Bookmarks, cookies, top sites

- Safari

  ~/Library/Safari/History.db

  Other files: Bookmarks.plist, downloads.plist, topsites.plist

Linux Forensics

Artifact Locations

Directories

- /root
- /bin
- /sbin
- / etc
- /dev
- /mnt
- /usr
- /var/log
- /home/{username}

Linux Forensics

Internet Artifacts

- Firefox

  ~/.mozilla/firefox firefox/*.default

- Chrome

  ~/.config/chromium/Default