



INSIDE THE CORE PODCAST

Show Notes

Episode 9

INTERVIEW OF THE WEEK: JOE DUKE, ACCESSDATA

Joe Duke is retired from the Oakland County Sheriff's Department after serving 28 years with them. He started their Computer Crimes Unit in 1998. He became a contract instructor with AccessData 5 years ago and became a full-time instructor 2 years ago.

- Using FTK 3 to process a Mac using a Windows based tool:
 - FTK 3 allows you to image, analyze, and create a readable HTML report on Mac OSX systems.
 - FTK 3 will:
 - Parse SQLite data bases such as Safari cache
 - Parse URLs and allows examiners to match URLs to cache graphics and file names
 - Parse iPhone back-up files
 - Identify FileVault, but the ability to decrypt within the case is still being worked on
- AccessData offers a 3-day class. For information, go to www.AccessData.com

PLIST OF THE WEEK:

HDD > Library > Preferences > com.apple.loginwindow.plist

- Will indicate that FileVault may be enabled for a particular user
- If FileVault enabled, will show the slices for FV, the FV login account, and the location of the sparse bundle

- Last compression/compaction UNIX date and time
- Last user logged in and user name
- Master password hint and number of attempts before hint is displayed

HDD > Users > username > Library > Preferences > com.apple.loginitems.plist

- Shows if applications that start on login are hidden or not
- Application names and file paths

LOGIN ITEMS AND MAC SECURITY:

- Keeping your system up to date
- Firmware passwords – things you need to know, especially for Mac forensics
- Security Settings
- Firewall Settings
- Accounts tab

MAC HARDENING:

- Key Chains – default and creating new ones
- Secure Notes
- Encrypted .dmg files
- Identifying Keyloggers:
 - HDD > Users > username > Library
 - > LaunchAgents
 - > LaunchDaemons
 - > Startupitems

- HDD > System > Library
 - > LaunchAgents
 - > LaunchDaemons
 - > Startupitems
- HDD > Library
 - > LaunchAgents
 - > LaunchDaemons
 - > Startupitems
- Login Hook
 - (Knowledge Based Document #HT2420, www.support.apple.com)
- Anti-Virus for Macs
 - avast! www.avast.com
 - Symantec www.symantec.com
 - MacAfee www.mcafee.com
 - Kaspersky www.kaspersky.com
 - ClamAV www.clamxav.com
 - VirusBarrier www.intego.com/virusbarrier
 - MacScan (for running virus scan against media) www.macscan.securemac.com
- Useful Websites:
 - www.MacHeist.com (offers free apps for Mac)
 - www.MacShadows.com (Mac security and hacking)
 - www.SecureMac.com (download MacScan, VirusBarrier)
 - www.secsocial.com (Mac security, networks, anti-virus info, Mac OS X Forensics)
 - www.Blog.intego.com (Creators of VirusBarrier, MacScan)
 - www.grc.com/securitynow.htm (Security Now Podcast)