A Forensic First Look

Presented By:
Josh Brunty
Assistant Professor of Digital Forensics
Marshall University

Access this Presentation Online At:
http://goo.gl/Hqydt
What we'll cover...

- Operating System Overview
- Metro Interface
- How OS Interacts with External Accounts
- File Structure within FTK
- Forensic Artifacts
- Immersive Browser Artifacts
- Registry Artifacts
- Discussion of ReFS
Windows 8 Overview

- Windows 8 is newest Operating System
- Set to release in late 2012
- Features a new Metro-style interface that was designed for touchscreen, mouse, keyboard, and pen input
Metro Interface
Local Folder

%Root%\Users\%User%\AppData\Local\

**there are many items forensic interest in the Local folder**
Metro Apps

• Metro Apps that are displayed on the Metro Desktop will have a link file associated with them that will display who created the app and the app’s location. This data will be available in plain text.
• Each Immersive App as it’s own registry file
Metro App Artifacts

A majority of apps in Windows 8 connected to the Internet with a Windows Live (Microsoft) Account and each app is considered to be what Windows calls an “immersive” environment. This means that from within each app, you can access other apps, so in a sense, that app becomes the operating system. Because of this immersive concept, each app will have its own Internet artifacts.
Metro App Artifacts

- Metro App Cache
  %Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetCache
  Contains web cache specific to Metro App.

- Metro App Cookies
  %Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetCookies
  Contains cookie files specific to Metro App. Data is contained in a text file. Metro App Web History

- Metro App History
  %Root%\Users\%User%\AppData\Local\Packages\%MetroAppName%\AC\INetHistory
  Contains Internet history files specific to Metro App and the format of the data is consistent with previous versions.
Internet Explorer 10 Artifacts

- IE 10 Websites Visited (Immersive)
  %Root%\Users\%User%\AppData\Local\Microsoft\InternetExplorer\ Recovery\Immersive\Active

- IE 10 Websites Visited (Desktop IE)
  %Root%\Users\%User%\AppData\Local\Microsoft\InternetExplorer\ Recovery\Active

Websites user visited while browsing with IE10.

- User-Pinned Favorite Tiles
  %Root%\Users\%User%\AppData\Local\Microsoft\Windows\RoamingTiles
  Contains tiles that user has pinned as favorite

**It's important for the examiner to keep in mind that there are essentially 2 separate versions of IE built into Windows 8 (Immersive & Desktop)**
Communication App

The Communications App includes the user’s e-mail, chat clients, Facebook, and other social networking sites (e.g. Twitter). Anything that can allow the user to interact with another person appears to fall under “Communications Apps”.
Don't believe a word of Josh Brunty's Windows 8 presentation at the Techno Security Conference. He is full of crap and must be defeated

About a minute ago via Twitter
Communication App Artifacts

- Communication App Web Cache
  `%Root%\Users\%User%\AppData\Local\Packages\microsoft.windows.communicatisapps_8wekyb3d8bbwe\AC\INetCache`

- Communication App Cookies
  `%Root%\Users\%User%\AppData\Local\Packages\microsoft.windows.communicatisapps_8wekyb3d8bbwe\AC\INetCookies`
Communication App Artifacts (User Contacts)

- User’s Contacts from Communications Apps
  %Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\%User’s WindowsLiveEmail Address%\%App-CurrentVersion%\DBStore\LogFiles\edb####.log
Communication App Artifacts (User Contacts)

- User Tile Associated with Contact

%Root%\Users\%User%\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\LiveComm\%User’sWindowsLiveEmail Address\%AppCurrentVersion\DBStore\UserTiles
Windows 8 Registry

Additional Registry Files Are Still Present

SAM

SYSTEM
Windows 8 Registry

- Traditional Registry Files Are Still Present
  - SAM
  - SYSTEM
  - SOFTWARE
  - SECURITY
  - NTUSER.DAT (Multiple for each user)
Windows 8 Registry

- New Registry Files to Windows 8
  - ELAM (Early Launch Anti-Malware)
  - BBI (Browser-Based Interface)
  - SETTINGS.DAT (User Profile)
New NTUSER.DAT Artifacts

- TypedURLsTime

%SystemRoot%\Users\%User%\NTUSER.DAT\Software\Microsoft\Microsoft\InternetExplorer\TypedURLsTime
New SOFTWARE Artifacts

- Metro Apps Installed on System
  Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Applications

- User Account Installed Metro Apps
  Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\%SID%
New SAM Artifacts

- Internet User Name
  %SystemRoot%\Windows\System32\Config\SAM\Domains\Account\Users\Internet User Name
  InternetUserName

- User's Tile
  %SystemRoot%\Windows\System32\Config\SAM\Domains\Account\Users\UserTile
Other Unique Artifacts

- 2 Swapfiles (pagefile.sys, swapfile.sys)
- ISO Automount
- Resilient File System (set to release with Server 2013)
  - File History (replacement of volume shadow copy)
  - Storage Pools (Resilient Storage Area)
Questions??

Josh Brunty
Marshall University Department of Integrated Science & Technology
Email: josh.brunty@marshall.edu
Phone: 304-696-5602
Web: www.marshall.edu/isat