USB Devices and Media Transfer Protocol

Identifying the Existence of Data Exfiltration Artifacts

Nicole Ibrahim

G-C Partners, LLC
Importance

- Increasing adoption of MTP in portable devices
  - Android
  - Windows
  - Blackberry
- It's easy to copy files from a computer to a USB attached MTP device
- Not fully understood in the forensic community
- MTP devices create different Windows artifacts
  - Your analysis may miss that smoking gun if you don't know what to look for
  - Your tools may miss it too
Agenda

- Introduction to USB Device Classes
- USB Device enumeration and driver selection in Windows
- Testing environment used to identify MTP artifacts
  - Devices Tested
  - Testing Procedures
  - Test Results
    - First Time Attached
    - Directory Traversal
    - Opening Files
Introduction to USB Device Classes
USB Device Classes Covered

- Mass Storage Class
- Picture Transfer Protocol
- Media Transfer Protocol
Mass Storage Class

- Well known, researched and documented
- Also referred to as UMS (USB Mass Storage)
- Windows provided native support starting with Windows 2000
- Physical access to the underlying file system
- Can be supported by:
  - Thumb & External Drives
  - MP3 Players
  - Smartphones
  - More..
Mass Storage Class

- Mounts in Windows Explorer as:
  - Hard Disk Drives
  - Devices with Removable Storage
Picture Transfer Protocol

- Developed by International Imaging Industry Association
- Standardize as ISO 15740, communication protocol
- A PTP device in Windows
  - No access to underlying file system
  - Copy media from, not to a connected device
  - Limited, logical view of device contents
  - Only images and video files
- Can be supported by:
  - Cameras & scanners
  - Smartphones & Tablets

Picture Transfer Protocol

- **Windows XP:**
  - Windows Image Acquisition (WIA)
  - Mounts in Explorer as Scanners and Cameras

- **Windows Vista +:**
  - Windows Portable Devices (WPD)
  - Mounts in Explorer as Portable Devices

Media Transfer Protocol

- Developed by Microsoft, standardized by USB Implementers Forum in 2008
- Improvement and extension of PTP
- Can perform automatic transcoding of video and audio files
- An MTP device in Windows
  - No access to underlying file system
  - Access to each storage area on the device (internal and SD card)
  - Copy files from/to connected device or sync files
  - Not so limited, yet logical view of device contents
  - Can be any file type
- Can be supported by:
  - MP3 players, cameras
  - Smartphones & Tablets
  - More..

http://www.usb.org/developers/devclass_docs/MTPv1_1.zip
Media Transfer Protocol

- Windows XP with Windows Media Player 10:
  - Windows Portable Devices (WPD)
  - Mounts in Explorer as Other
- Windows Vista+:
  - Windows Portable Devices (WPD)
  - Mounts in Explorer as Portable Devices

Media Transfer Protocol

- Mobile phone and tablets that support MTP
  - Depends on Phone Provider, OS, and Independent Hardware Vendor

- Mobile OS with MTP support:
  - Android 4.0+ (Ice Cream Sandwich)
  - Windows Phone 8+
  - Blackberry 5+
  - Others?

http://www.blackberry.com/btsc/KB16310
USB Device Enumeration in Windows
USB Enumeration

- USB hub driver, Plug and Play
- Device classes help determine driver
  - Standardized through usb.org [http://www.usb.org/developers/defined_class](http://www.usb.org/developers/defined_class)
- Driver selected handles communication
USB Hub Driver generates Hardware IDs and Compatible IDs.

IDs are communicated to Plug and Play, which relays the IDs to Windows.

Windows searches for matching IDs within INF files or driver packages.

Windows installs drivers and other components, which is stored in the Registry.

PnP assigns resources to the device, drivers communicate with the device.

Setup information is stored in the Registry for future reference.
Testing Environment
Testing Environment

- VMWare Workstation 10 and snapshots
- OS Tested:
  - Windows XP SP3 Professional with Windows Media Player 10
  - Windows 7 SP1 Professional
- Limited Testing:
  - Windows Vista Home Basic
  - Windows 8 Professional
  - Windows 8.1 Professional
- Regshot to identify changes for test performed
- FTK Imager to acquire registry and other files
- 10 MSC devices, 3 PTP devices, 4 MTP devices
- Tests Performed in a Series:
  - USB device first time attached
  - Traversing directories on USB device Windows Explorer
  - Opening files from USB device in Windows Explorer
Testing Procedures

1. Prepared USB device for testing by creating a standard set of folders and files
2. Copied folders and files to USB device
3. Installed Windows OS in VM
4. Downloaded and applied most recent OS patches and updates
5. Installed Regshot and FTK Imager
6. Took a snapshot of VM to use as clean “untested”
7. Ran Regshot to create a baseline of registry and file system (Windows System drive)
8. Performed test
9. Used Regshot to capture changes
10. Used FTK imager to acquire registry files and other files affected from test (as indicated by Regshot’s file added or modified list)
11. Completed next test in series
12. Reverted VM back to clean snapshot for next device
13. Performed procedures above for all other devices
14. Consolidated Regshot reports generated for each device to be analyzed (per test) into spreadsheets
15. Identified files, registry keys and values that were affected across different device types per test
USB Devices Tested

**MSC**
- WD My Passport 500GB USB 2.0
- WD My Passport 1TB USB 3.0
- Toshiba Canvio 1TB USB 3.0
- Toshiba Canvio 1TB USB 2.0
- Seagate Backup Plus 3TB USB 2.0
- SanDisk Cruzer 8GB USB 2.0
- SanDisk Cruzer 16GB USB 2.0
- ADATA S102 8GB USB 3.0
- MP3 Player iPod 5th Gen. 30GB
- Phone HTC Magic Android 2.2.1

**PTP**
- Tablet iPad 1 Model MB293LL OS 4.3.2
- Tablet iPad 2 Model MC979LL OS 4.3.5
- Phone iPhone 4 Model MC676LL OS 4.2.7

**MTP**
- MP3 Player SanDisk Sansa m240 1GB
- Phone Samsung Galaxy SIII Model SCH-I535 Android 4.1.2
- Phone Samsung Galaxy S4 Model SCH-I545 Android 4.3
- Phone Blackberry Storm 9530 OS 4.7.0.148 Platform 4.0.0.181
Test Results: MTP Artifacts in Windows
MTP Artifacts in Windows

- First time attached
  - Registry keys affected
  - A look at Device Stage
- Traversing directories
  - ShellbagMRU
- Open file artifacts
  - LNK Files
  - WPDNSE Folder
First Time Attached: Testing Procedures

1. Used clean VM from snapshot
2. Ran Regshot
3. Attached USB device, selected “Connect to Guest (Disconnect from Host)” in VMWare > VM > Removable Devices
4. Witnessed device installation and mount in Windows Explorer
5. Captured changes with Regshot
6. Acquired registry and other changed files with FTK Imager
7. Continued to next series in tests for device
### First Time Attached: Registry Keys in Windows XP

<table>
<thead>
<tr>
<th>Hive</th>
<th>Key</th>
<th>MSC</th>
<th>PTP</th>
<th>MTP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM</strong></td>
<td>CurrentControlSet\Control\Class{36FC9E60-C465-11CF-8056-444553540000}\</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{4D36E967-E325-11CE-BFC1-08002BE10318}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{71A27CDD-812A-11D0-BEC7-08002BE2092F}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{EEC5AD98-8080-425f-922A-DABF3DE3F69A}</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{14480d3f-7a47-4a75-a9ae-b14f56397153}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f56307-b6bf-11d0-94f2-00a0c91efb8b}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{6ac27878-a6fa-4155-ba85-f98f491d4f33}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{6bd1fc6-810f-11d0-becd7-08002be2092f}</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{a5dcbf10-6530-11d2-901f-00c04fb951ed}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{f33fd04-d1ac-4e8e-9a30-19bbd4b108ae}</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Enum\STORAGE\</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Enum\USB\</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Enum\USBSTOR\</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MountedDevices??\Volume\VolumeGUID\</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MountedDevices\DosDevices\DriveLetter:\</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SOFTWARE</strong></td>
<td>Microsoft\Windows Portable Devices\Devices\</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\DriveLetter:\</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\VolumeGUID\</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NTUSER</strong></td>
<td>CurrentControlSet\Control\Class{36FC9E60-C465-11CF-8056-444553540000}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{4D36E967-E325-11CE-BFC1-08002BE10318}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{71A27CDD-812A-11D0-BEC7-08002BE2092F}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{EEC5AD98-8080-425f-922A-DABF3DE3F69A}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{14480d3f-7a47-4a75-a9ae-b14f56397153}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f56307-b6bf-11d0-94f2-00a0c91efb8b}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{6ac27878-a6fa-4155-ba85-f98f491d4f33}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{6bd1fc6-810f-11d0-becd7-08002be2092f}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{a5dcbf10-6530-11d2-901f-00c04fb951ed}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{f33fd04-d1ac-4e8e-9a30-19bbd4b108ae}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\UsbFlags\vvvvpppprrrr\</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Enum\STORAGE\</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Enum\USB\</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Enum\USBSTOR\</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MountedDevices??\Volume\VolumeGUID\</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MountedDevices\DosDevices\DriveLetter:\</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## First Time Attached: Registry Keys in Windows 7

<table>
<thead>
<tr>
<th>Hive</th>
<th>Key</th>
<th>MSC</th>
<th>PTP</th>
<th>MTP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM</strong></td>
<td>CurrentControlSet\Control\Class{36FC9E60-C465-11CF-8056-444553540000}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{4D36E967-E325-11CE-BFC1-08002BE10318}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{71A27CDD-812A-11D0-BEC7-08002BE2092F}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\Class{EEC5AD98-8080-425f-92A-DABF3DE3F69A}</td>
<td>RM</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{53f56307-b6bf-11d2-901f-00c04fb951ed}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{a5dcbf10-6530-11d2-901f-00c04fb951ed}</td>
<td>RM</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>CurrentControlSet\Control\DeviceClasses{10497b1b-ba51-44e6-8318-a65c837bb600}</td>
<td>RM</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>MountedDevices??\Volume{VolumeGUID}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>MountedDevices\DosDevices\DriveLetter:</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>SOFTWARE</strong></td>
<td>Microsoft\WBEM\WDM\USBSTOR\</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Microsoft\Windows NT\CurrentVersion\EMDMgmt\</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Microsoft\Windows\CurrentVersion\Explorer\MountPoints2{VolumeGUID}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Microsoft\Windows NT\CurrentVersion\DeviceDisplayObjects\KnownDevices</td>
<td>RM</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Microsoft\Windows Portable Devices\Devices\</td>
<td>RM</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>NTUSER</strong></td>
<td>Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2{VolumeGUID}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2{VolumeGUID}</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Software\Microsoft\Windows NT\CurrentVersion\DeviceDisplayObjects\</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
**MTP Devices First Time Attached - XP**

1. **What**: Get Vendor, Product, Version, Serial
   - **Where**: SYSTEM\CurrentControlSet\Enum\USB

2. **Where**: Find Mount Name
   - **When**: Identify first time device was inserted
     - **Who**: Identify who accessed the device
     - **Who**: Search for serial number (Unicode)
     - **Who**: Search for serial number
     - **Who**: Search for serial number
     - **Who**: Search for serial number
     - **Who**: Search for serial number

3. **Where**: Software\Microsoft\Windows\Shell NoRoam\BagMRU

4. **Who**: NTUSER.dat\Software\Microsoft\Windows\Shell NoRoam\BagMRU

5. **Who**: SOFTWARE\Microsoft\Windows Portable Devices\Devices\USB\VID_XXXX&PID_XXXX&SerialNumber FriendlyName: MountName

6. **Who**: \Windows\setupapi.log
MTP Devices First Time Attached - 7

What
1. Get Vendor, Product, Version, Serial

Where
2. Find Mount Name
    Search for serial number

When
3. Identify first time device was inserted
    Search for serial number

Who
4. Identify who accessed the device
    Search for serial number (Unicode)
Microsoft Windows Device Stage

- Introduced in Windows 7
- Interact with eligible devices
- Applies to Printers & Scanners, Portable Devices and Smart Cards

Directory Traversal: Testing Procedures

1. Continued from last test in series for the device (First Time Attached)
2. Ran Regshot and captured baseline
3. Traversed directories on device in Windows Explorer
4. Captured changes with Regshot
5. Acquired registry and other changed files with FTK Imager
6. Continued to next series in tests
Directory Traversal Scenario Windows 7: Android Galaxy S3

Computer\SCH-I535\  Computer\SCH-I535\Card\  Computer\SCH-I535\Card\Android
Directory Traversal Scenario: Computer\SCH-I535\ UsrClass.DAT
Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0:
Directory Traversal Scenario: Computer\SCH-I535\Card

UsrClass.DAT
Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0:
Directory Traversal Scenario: Computer\SCH-I535\Card\Android

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000h</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>DC</td>
<td>02</td>
<td>06</td>
<td>20</td>
<td>19</td>
<td>07</td>
<td>F8</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0010h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>CE</td>
<td>01</td>
<td>00</td>
<td>74</td>
<td>94</td>
<td>38</td>
<td>2F</td>
<td>79</td>
<td>CE</td>
<td>01</td>
<td>92</td>
<td>E3</td>
<td>27</td>
</tr>
<tr>
<td>0020h</td>
<td>ED</td>
<td>48</td>
<td>A8</td>
<td>0C</td>
<td>E1</td>
<td>77</td>
<td>05</td>
<td>A0</td>
<td>5F</td>
<td>85</td>
<td>2B</td>
<td>07</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0030h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>27</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0040h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0050h</td>
<td>27</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0060h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0070h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0080h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0090h</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>

UsrClass.DAT
Local Settings\Software\Microsoft\Windows\Shell\BagMRU\7\0\0\0:
MTP Considerations

- Last folder visited may not be added to the registry
- Some tools may not account for MTP ShellbagMRU structure
- Traversing directories creates LNK files
Opening Files: Testing Procedures

1. Continued from last test in series for device (Traversing Directories)
2. Ran Regshot and captured baseline
3. Opened files
4. Captured changes with Regshot
5. Acquired registry and other changed files with FTK Imager
6. Reverted VM back to clean snapshot for next device
Opening Files Scenario Windows 7: Android Galaxy S3
Opening Files Scenario Windows 7: Android Galaxy S3

- Folders created in WPDNSE folder
Opening Files Scenario Windows 7: Android Galaxy S3

- Linking ShellbagMRU to folder in WPDNSE
Opening Files Scenario Windows 7: Android Galaxy S3

- Contents of WPDNSE folders
  - All files present except for JPGs
Opening Files Scenario Windows 7: Android Galaxy S3

- Recent folder contains LNK files created after opening JPG files
  - LNK files point to directory where JPG files are located
  - Why?
MTP Considerations

- Files on a MTP device cannot be directly viewed or altered.
  - They must first be copied to the host computer first.
  - Exceptions may exist. JPG files? Device’s supported features?
- Files opened are copied to the WPDNSE folder
  - Windows 7: C:\Users\<UserName>\AppData\Local\Temp\WPDNSE\{FolderGUID}
  - Windows XP: C:\Documents and Settings\<UserName>\AppData\Local\Temp\WPDNSE\{FolderName}
  - WPDNSE is in a temp directory, contents do not survive reboot
  - File contents can be recovered from unallocated space
- LNK files do not generally get created for files opened
  - Exceptions exist
    - May involve file type or application used to open file
  - LNK files may also point back to WPDNSE folders
Further Research

- PTP and MTP devices in Unix based OSs
- Larger variety of devices to test
- Windows 8 phones
- Scenarios where LNK files are created
- Syncing software and Device Stage
- Last insert date
- More testing in Windows 8 and 8.1
Questions?

Email: Nicole.Ibrahim08@yahoo.com
Blog: www.nicoleibrahim.com