WINDOWS 8 RECOVERY FORENSICS

Understanding the Three R’s
W. Kenneth Johnson (@patorium)
SANS DFIR SUMMIT 2012
INTRODUCTION

- Who Am I?
  - MS Student at Iowa State University
  - IT Security Analyst with Principal Financial Group
  - Forensic and Malware Researcher

- Why are we here?
  - To understand the forensic impacts of Windows 8 Recovery options
ISSUES

New System Recovery options with new challenges.

1. Availability
2. Data Recovery
3. Additional Artifacts

Today we will cover the following topics:

1. Recovery options Available
2. Forensic Implications
TESTING ENVIRONMENT

- Windows 8 installed in multiple VM instances
  - VMWare Workstation 8
- FTK Imager
- FTK ToolKit

- Impact with Bitlocker enabled not tested
- Solid State Drives not tested
RECOVERY OPTIONS

- System Restore Points
- System Refresh Points
- System Reset
What are they?

SYSTEM RESTORE POINTS
SYSTEM RESTORE POINT

- Relevant Files
- Every 7 Days
- SRSetRestorePoint API
SYSTEM RESTORE – NEW REG KEYS

- HKLM\Software\MS\WindowsNT\CurrentVersion\SystemRestore
  - SystemRestorePointCreationFrequency
  - ScopeSnapshots
SYSTEM RESTORE – ISSUES

- Dual Boot Systems
- Data Retention
What are they?

SYSTEM REFRESH POINTS
SYSTEM REFRESH POINT - PROCESS
SYSTEM REFRESH POINT - DEFAULT

What is Retained

- Wireless Network Connections
- Mobile Broadband Connections
- BitLocker Settings
- BitLocker To GO settings
- Drive Letter Assignments
- Personalization Settings
- Metro Style Application

What is not Retained

- File Type Associations
- Display Settings
- Windows Firewalls
- Desktop Installed Applications
- Volume Shadow Copies
- Restore Points
SYSTEM REFRESH POINT - CUSTOM

- Desktop Applications
- Default Refresh Behavior
- No Volume Shadow Copies
SYSTEM REFRESH POINT

- Default Restore with Install
- Multiple
- One
- Start at Boot Time
SYSTEM REFRESH POINT - CUSTOM

- How is it done?
  - Reclmg.exe
  - ReAgent.exe
System Refresh Point - RecImg

Creates Custom Refresh Image

Image Directory can be on a Local, Removable or Remote Drive.

Set a new current Image

Remove current image and revert back to default

Shows the current image

```
/createimage <directory>
Captures a new custom recovery image in the location specified by <directory>, and sets it as the active recovery image.

/setcurrent <directory>
Sets the active recovery image to the install.wim file in the location specified by <directory>. Windows will use this image when you refresh your PC, even if a recovery image provided by your PC's manufacturer is present.

/deregister
Deregisters the current custom recovery image. If a recovery image provided by your PC's manufacturer is present, Windows will use that image when you refresh your PC. Otherwise, Windows will use your installation media when you refresh your PC.

/showcurrent
Displays the path to the directory in which the current active recovery image is stored.
```
System Refresh Point - ReAgentC

Where the WinRE is located
Configures if machine will start the Recovery process at start up
Sets the location of recovery image

C:\Windows\system32\reagentc

Configures the Windows Recovery Environment (RE) and system reset.

REAGENTC.EXE <command> <arguments>

The following commands can be specified:

/info - Displays Windows RE and system reset configuration information.
/setreimage - Sets the location of the custom Windows RE image.
/enable - Enables Windows RE.
/disable - Disables Windows RE.
/bootories - Configures the system to start Windows RE next time the system starts up.
/setosimage - Sets the location of the recovery image used by system reset.
/setboothelllink - Adds an entry to the Reset and Restore page in the boot menu.

For more information about these commands and their arguments, type REAGENTC.EXE <command> /?.

Examples:
  REAGENTC.EXE /setreimage /?
  REAGENTC.EXE /disable /?

REAGENTC.EXE: Operation Successful.
SYSTEM RESET - PROCESS
SYSTEM RESET – INITIAL COMMANDS

Your PC has more than one drive
Do you want to remove all files from all drives?

- Only the drive where Windows is installed
- All drives

Show me the list of drives that will be affected
How do you want to remove your personal files?

Thoroughly, but this can take several hours
Choose this if you are recycling the PC or giving it away.

Quickly, but your files might be recoverable by someone else
Choose this if you are keeping the PC or giving it to someone you trust.
SYSTEM RESET – DATA WIPE OPTIONS

Quick
- Good if you trust the person you are giving it to.

Thorough
- Good if you are going to give to charity.

Both options are not recommended for cleaning a drive if a multi-pass scrubbing operation is required!
Artifacts and Implications

DIGITAL FORENSICS
RESTORE POINT ARTIFACTS

- Accessible through multiple options
- May contain the following previous versions:
  - Registry Settings
  - Documents and files
  - Applications
  - FileHistory Configuration
  - System Events
RESTORE POINTS - GUI

Current time zone: Pacific Daylight Time

<table>
<thead>
<tr>
<th>Date and Time</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/27/2012 8:00:18 PM</td>
<td>test 4</td>
<td>Manual</td>
</tr>
<tr>
<td>5/27/2012 7:52:35 PM</td>
<td>Test 1</td>
<td>Manual</td>
</tr>
<tr>
<td>5/19/2012 6:05:47 PM</td>
<td>Automatic Restore Point</td>
<td>System</td>
</tr>
</tbody>
</table>
C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001–2005 Microsoft Corp.

Contents of shadow copy set ID: {1f336afa-47da-4f09-add6-a3bd179c807e}
  Contained 1 shadow copies at creation time: 5/19/2012 6:05:59 PM
  Shadow Copy ID: {43cc8e8a-ed3-45ab-8d2c-d0965e835952}
    Original Volume: C:\?\Volume{bbf76cee-6346-11e1-a103-806e6f6e6f63}\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
    Shadow Copy Volume: C:\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
    Originating Machine: sans-64-dfir
    Service Machine: sans-64-dfir
    Provider: 'Microsoft Software Shadow Copy provider 1.0'
    Type: ClientAccessible Writers
    Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered
RESTORE POINT – SYMBOLIC LINK
RESTORE POINT CONCERNS

- Abuse
REFRESH & RESET ARTIFACTS - OVERVIEW

- Similar Artifacts found on the Boot System Volume
- Different Artifacts found on the Operating System Volume
- Different Artifacts based on type of Reset used
REFRESH & RESET ARTIFACTS

Before Refresh/Reset

After Refresh/Reset
# REFRESH & RESET ARTIFACTS

## Before Refresh/Reset

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot.sdi</td>
<td>3,096 KB</td>
<td>Regular File</td>
<td>9/7/2011 8:39:1...</td>
</tr>
<tr>
<td>ReAgent.xml</td>
<td>1 KB</td>
<td>Regular File</td>
<td>3/1/2012 2:39:2...</td>
</tr>
<tr>
<td>Winre.wim</td>
<td>185,398 KB</td>
<td>Regular File</td>
<td>2/18/2012 8:48:...</td>
</tr>
</tbody>
</table>

## After Refresh/Restore

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot.sdi</td>
<td>3,096 KB</td>
<td>Regular File</td>
<td>9/7/2011 8:39:1...</td>
</tr>
<tr>
<td>ReAgent.xml</td>
<td>1 KB</td>
<td>Regular File</td>
<td>4/27/2012 2:40:...</td>
</tr>
<tr>
<td>ReAgent.xml.FileSlack</td>
<td>4 KB</td>
<td>File Slack</td>
<td></td>
</tr>
<tr>
<td>Winre.wim</td>
<td>185,398 KB</td>
<td>Regular File</td>
<td>2/18/2012 8:48:...</td>
</tr>
</tbody>
</table>
**Refresh & Reset Artifacts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI30</td>
<td>4 KB</td>
<td>NTFS Index</td>
<td>6/7/2012 3:44:2...</td>
</tr>
<tr>
<td>BootUX (2).sqml</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/3/2012 8:27:4...</td>
</tr>
<tr>
<td>BootUX (3).sqml</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/3/2012 8:28:3...</td>
</tr>
<tr>
<td>BootUX (4).sqml</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/3/2012 8:40:4...</td>
</tr>
<tr>
<td>BootUX (5).sqml</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/3/2012 8:41:1...</td>
</tr>
<tr>
<td>Reload.xml</td>
<td>2 KB</td>
<td>Regular File</td>
<td>6/7/2012 2:59:2...</td>
</tr>
<tr>
<td>sysreset_exe_BootUX.etl</td>
<td>8 KB</td>
<td>Regular File</td>
<td>6/3/2012 8:41:1...</td>
</tr>
</tbody>
</table>
<xml version="1.0" encoding="utf-8" ?>
  <WindowsRE version="1.0">
    <WinreBCD id="{b1d6602f-6346-11e1-b08c-ff298f72d4a8}" />
    <WinreLocation path="\Recovery\b1d6602f-6346-11e1-b08c-ff298f72d4a8" id="1875952216" offset="1048576" guid="{00000000-0000-0000-0000-000000000000}" />
    <ImageLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" />
    <OsInstallLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" index="0" />
    <CustomImageLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" index="0" />
    <InstallState state="1" />
    <OsInstallAvailable state="0" />
    <CustomImageAvailable state="0" />
    <WinRESTaged state="0" />
    <OperationParam path="" />
    <OsBuildVersion path="8250.0.amd64fre.winmain_win8beta.120217-1520" />
    <OemTool state="0" />
    <BootKey state="0" />
    <IsServer state="0" />
    <ScheduledOperation state="5" />
  </WindowsRE>
</xml>
<?xml version="1.0" encoding="utf-8" ?>
<WindowsRE version="1.0">
  <WinreBCD id="b1d8602f-6346-11e1-b08c-ff298f72d4a8" />
  <WinreLocation path="\Recovery\b1d8602f-6346-11e1-b08c-ff298f72d4a8" id="1875952216"
    offset="1048576" guid="{00000000-0000-0000-0000-000000000000}" />
  <ImageLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" />
  <OsInstallLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" index="0" />
  <CustomImageLocation path="\testrestore" id="0" offset="368050176" guid="{00000000-0000-0000-0000-000000000000}" index="1" />
  <InstallState state="1" />
  <OsInstallAvailable state="0" />
  <CustomImageAvailable state="1" />
  <WinREStaged state="0" />
  <OperationParam path="" />
  <OsBuildVersion path="8250.0.amd64fre.winmain_win8beta.120217-1520" />
  <OemTool state="0" />
  <BootKey state="0" />
  <IsServer state="0" />
  <ScheduledOperation state="5" />
</WindowsRE>
<?xml version="1.0" encoding="utf-8" ?>
<WindowsRE version="1.0">
  <WinreBCD id="{b1d8602f-6346-11e1-b08c-ff298f72d4a8}" />
  <WinreLocation path="\Recovery\b1d8602f-6346-11e1-b08c-ff298f72d4a8" id="1875952216" offset="1048576" guid="{00000000-0000-0000-0000-000000000000}" />
  <ImageLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" />
  <OsInstallLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-000000000000}" index="0" />
  <CustomImageLocation path="\testrestore" id="0" offset="368050176" guid="{00000000-0000-0000-0000-000000000000}" index="1" />
  <InstallState state="1" />
  <OsInstallAvailable state="0" />
  <CustomImageAvailable state="1" />
  <WinREStaged state="0" />
  <OperationParam path="" />
  <OsBuildVersion path="8250.0.amd64fre.winmain_win8beta.120217-1520" />
  <OemTool state="0" />
  <BootKey state="0" />
  <IsServer state="0" />
  <ScheduledOperation state="5" status="1223" />
  <BackupLaunch state="0" status="0" />
  <BackupComplete state="0" status="0" />
  <BackupResult status="0" />
  <MachineGuid id="{00000000-0000-0000-0000-000000000000}" />
  <UserGuid id="{00000000-0000-0000-0000-000000000000}" />
  <OptIn state="0" />
</WindowsRE>
REFRESH ARTIFACTS

Boot System
- Reagent.xml
- Reload.xml
- Logs Directory

OS System
- Unallocated Data
- $SysReset
- Windows.old
- User files will be migrated over
- FileHistory (if enabled)
- Logs of migrated files
- Logs of uninstalled applications
- Logs of Migrated OS Updates
PARTITION 2 ARTIFACTS - REFRESH

Before Refresh, or After Reset

After Refresh Only

[Diagram showing file structures before and after refresh]
REFRESH ARTIFACTS - $SYSRESET
REFRESH ARTIFACTS – USERS DIRECTORY
## Recover Artifacts - Refresh

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searches</td>
<td>1 KB</td>
<td>Directory</td>
<td>6/19/2012 3:00:21 AM</td>
</tr>
<tr>
<td>SendTo</td>
<td>1 KB</td>
<td>Reparse Point</td>
<td>6/19/2012 2:33:29 AM</td>
</tr>
<tr>
<td>Start Menu</td>
<td>1 KB</td>
<td>Reparse Point</td>
<td>6/19/2012 2:33:29 AM</td>
</tr>
<tr>
<td>Templates</td>
<td>1 KB</td>
<td>Reparse Point</td>
<td>6/19/2012 2:33:29 AM</td>
</tr>
<tr>
<td>$I30</td>
<td>12 KB</td>
<td>NTFS Index All...</td>
<td>6/19/2012 11:37:56 AM</td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>512 KB</td>
<td>Regular File</td>
<td>6/19/2012 5:45:55 AM</td>
</tr>
<tr>
<td>ntuser.dat.LOG1</td>
<td>8 KB</td>
<td>Regular File</td>
<td>6/19/2012 2:33:29 AM</td>
</tr>
<tr>
<td>ntuser.dat.LOG2</td>
<td>0 KB</td>
<td>Regular File</td>
<td>6/19/2012 2:33:29 AM</td>
</tr>
<tr>
<td>NTUSER.DAT{9faa23b...}</td>
<td>64 KB</td>
<td>Regular File</td>
<td>6/19/2012 5:45:55 AM</td>
</tr>
<tr>
<td>NTUSER.DAT{9faa23b...}</td>
<td>512 KB</td>
<td>Regular File</td>
<td>6/19/2012 5:45:55 AM</td>
</tr>
<tr>
<td>NTUSER.DAT{9faa23b...}</td>
<td>512 KB</td>
<td>Regular File</td>
<td>6/19/2012 2:33:33 AM</td>
</tr>
<tr>
<td>ntuser.ini</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/19/2012 2:57:02 AM</td>
</tr>
<tr>
<td>File</td>
<td>Size</td>
<td>Type</td>
<td>Date/Time</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------</td>
<td>---------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Templates</td>
<td>1 KB</td>
<td>Reparse Point</td>
<td>6/10/2012 2:03 AM</td>
</tr>
<tr>
<td>$I30</td>
<td>8 KB</td>
<td>NTFS Index All...</td>
<td>6/19/2012 12:3 AM</td>
</tr>
<tr>
<td>$TXF_DATA</td>
<td>1 KB</td>
<td>NTFS Logged...</td>
<td>6/19/2012 12:3 AM</td>
</tr>
<tr>
<td>NTUSER.DAT</td>
<td>512 KB</td>
<td>Regular File</td>
<td>6/19/2012 1:38 AM</td>
</tr>
<tr>
<td>ntuser.dat.LOG1</td>
<td>8 KB</td>
<td>Regular File</td>
<td>6/10/2012 2:03 AM</td>
</tr>
<tr>
<td>ntuser.dat.LOG2</td>
<td>0 KB</td>
<td>Regular File</td>
<td>6/10/2012 2:03 AM</td>
</tr>
<tr>
<td>NTUSER.DAT{f498d4f8...}</td>
<td>64 KB</td>
<td>Regular File</td>
<td>6/19/2012 1:33 AM</td>
</tr>
<tr>
<td>NTUSER.DAT{f498d4f8...}</td>
<td>512 KB</td>
<td>Regular File</td>
<td>6/19/2012 1:33 AM</td>
</tr>
<tr>
<td>NTUSER.DAT{f498d4f8...}</td>
<td>512 KB</td>
<td>Regular File</td>
<td>6/19/2012 1:33 AM</td>
</tr>
<tr>
<td>ntuser.ini</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/10/2012 2:03 AM</td>
</tr>
</tbody>
</table>
RECOVERY ARTIFACTS - REFRESH
RECOVERY ARTIFACTS – REFRESH FILEHISTORY
RECOVERY ARTIFACTS – REFRESH FILEHISTORY
## Recovery Artifacts – Refresh FileHistory

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileHistory</td>
<td>1 KB</td>
<td>Directory</td>
<td>6/19/2012 5:24:04 AM</td>
</tr>
<tr>
<td>Ken Hives</td>
<td>1 KB</td>
<td>Directory</td>
<td>6/19/2012 5:23:29 AM</td>
</tr>
<tr>
<td>RegRipper</td>
<td>1 KB</td>
<td>Directory</td>
<td>6/19/2012 5:23:01 AM</td>
</tr>
<tr>
<td>$130</td>
<td>4 KB</td>
<td>NTFS Index All</td>
<td>6/19/2012 5:23:01 AM</td>
</tr>
<tr>
<td>FileHistory Services (2...)</td>
<td>282 KB</td>
<td>Regular File</td>
<td>6/9/2012 3:22:10 AM</td>
</tr>
<tr>
<td>FileHistory Services (2...)</td>
<td>3 KB</td>
<td>File Slack</td>
<td>6/8/2012 3:26:56 PM</td>
</tr>
<tr>
<td>ft12 (2012_05_24 12_12...)</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/8/2012 3:26:56 PM</td>
</tr>
<tr>
<td>ft12 (2012_05_24 12_12...)</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/8/2012 3:26:56 PM</td>
</tr>
<tr>
<td>fttt6 (2012_05_24 12_12...)</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/8/2012 3:28:30 PM</td>
</tr>
<tr>
<td>fttt6 (2012_05_24 12_12...)</td>
<td>4 KB</td>
<td>File Slack</td>
<td>6/8/2012 3:28:30 PM</td>
</tr>
<tr>
<td>fttt6 (2012_05_24 12_12...)</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/8/2012 3:28:30 PM</td>
</tr>
<tr>
<td>fttt7 (2012_05_24 12_12...)</td>
<td>1 KB</td>
<td>Regular File</td>
<td>6/8/2012 3:30:14 PM</td>
</tr>
</tbody>
</table>
QUICK RESET ARTIFACTS

Boot System
- Reagent.xml
- Reload.xml
- Logs Directory

OS System
- Unallocated Data
- Must be Carved
RECOVERY ARTIFACTS

Test Data

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTW7CND1141K9R_20120511 - 092555746...</td>
<td>5/11/2012 9:26 AM</td>
<td>7Z File</td>
<td>5,153 KB</td>
</tr>
<tr>
<td>PracticalMalwareAnalysis-Labs</td>
<td>5/11/2012 8:15 AM</td>
<td>7Z File</td>
<td>908 KB</td>
</tr>
<tr>
<td>Standardizing Collection and Analysis</td>
<td>5/11/2012 8:04 AM</td>
<td>Microsoft PowerP...</td>
<td>188 KB</td>
</tr>
</tbody>
</table>
RECOVER ARTIFACTS – QUICK RESET
### RECOVER ARTIFACTS – QUICK RESET

<table>
<thead>
<tr>
<th>17 Hits in 6 Files - QUERY: (PracticalMalwareAnalysis)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Hits - [03004550_4] C:\Users\Rasp\Desktop\DFIR Summit Talk\QuickResetUnallocated[unallocated space]\03004550_4</td>
</tr>
<tr>
<td>5 Hits - [03004550_3] C:\Users\Rasp\Desktop\DFIR Summit Talk\QuickResetUnallocated[unallocated space]\03004550_3</td>
</tr>
<tr>
<td>3 Hits - [03081350_1] C:\Users\Rasp\Desktop\DFIR Summit Talk\QuickResetUnallocated[unallocated space]\03081350_1</td>
</tr>
<tr>
<td>1 Hit - [02978950_1] C:\Users\Rasp\Desktop\DFIR Summit Talk\QuickResetUnallocated[unallocated space]\02978950_1</td>
</tr>
<tr>
<td>1 Hit - [02953350_4] C:\Users\Rasp\Desktop\DFIR Summit Talk\QuickResetUnallocated[unallocated space]\02953350_4</td>
</tr>
<tr>
<td>1 Hit - [00805376_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\QuickResetUnallocated[unallocated space]\00805376_2</td>
</tr>
</tbody>
</table>
RECOVER ARTIFACTS – QUICK RESET
RECOVER ARTIFACTS – QUICK RESET
RECOVER ARTIFACTS – QUICK RESET

```xml
<DPFrequency>600</DPFrequency>
<DPStatus>ENABLED</DPStatus>
<Target>
  <TargetName>Removable Disk</TargetName>
  <TargetUrl>E:\</TargetUrl>
  <TargetVolumePath>\\Volume{e9a6af5d-a594-11e1-a105-000c29bdff6a6}</TargetVolumePath>
  <TargetDriveType>REMOVABLE</TargetDriveType>
  <TargetConfigPath1>Ken\SANS-64-DFIR\Configuration\Config1.xml</TargetConfigPath1>
  <TargetConfigPath2>Ken\SANS-64-DFIR\Configuration\Config2.xml</TargetConfigPath2>
  <TargetCatalogPath1>Ken\SANS-64-DFIR\Configuration\Catalog1.edb</TargetCatalogPath1>
  <TargetCatalogPath2>Ken\SANS-64-DFIR\Configuration\Catalog2.edb</TargetCatalogPath2>
  <TargetBackupStorePath>Ken\SANS-64-DFIR\Data</TargetBackupStorePath>
  <TargetWarningThreshold>98</TargetWarningThreshold>
</Target>
</DataProtectionUserConfig>
```
RECOVER ARTIFACTS – QUICK RESET
RECOVER ARTIFACTS – QUICK RESET

Other Data Recoverable
THOROUGH RESET ARTIFACTS

**Boot System**
- Reagent.xml
- Reload.xml
- Logs Directory

**OS System**
- Unallocated Data
- Difficult to be carved
RECOVERY ARTIFACTS – THOROUGH RESET

- 7 Hits in 7 Files - QUERY: (ltw7)
  - 1 Hit - [12824923_1] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\12824923_1
    ...
  - 1 Hit - [11416923_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\11416923_2
    ...
  - 1 Hit - [10520923_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\10520923_2
  - 1 Hit - [05938523_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\05938523_2
  - 1 Hit - [05349723_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\05349723_2
  - 1 Hit - [05042523_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\05042523_2
RECOVERY ARTIFACTS – THOROUGH RESET

- 5 Hits in 2 Files - QUERY: (malware)
  - 4 Hits - [01944923_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\01944923_2
    - .0 6.2.8250.0 amd64_security-<<malware>>-windows-defender_31bf3856ad364e35_none_df06fcba70152883 6.2.8250.0 6.2.8250.0 amd64_security-<<malware>>-windows-filehashcode_31bf3856ad364e35_none_d611e9b4b9fbb4533 6.2.8250.0 6.2.8250.0 amd64
    - 50.0 4.0.8250.0 x86_security-<<malware>>-windows-filehashcode_31bf3856ad364e35_none_79f34e31019dd3fd k6.2.8250.0 6.2.8250.0 x86

  - 1 Hit - [01944923_1] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\01944923_1
    - 06( Description Help prevent <<malware>> from accessing your computer. 1200(2300 2301(1201_2302 1206 1207 Icon( winet.dll#00

  - 06( Description Help prevent <<malware>> from accessing your computer. 1200(2300 2301(1201_2302 1206 1207 Icon( winet.dll
RECOVERY ARTIFACTS – THOROUGH RESET

- 261 Hits in 3 Files - QUERY: (standard)
  - 205 Hits - [01944923_2] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\01944923_2
  - 55 Hits - [01944923_1] C:\Users\Rasp\Desktop\DFIR Summit Talk\ThroughResetUnallocated\[unallocated space]\01944923_1

-28DB04C10000} WDM Streaming <<Standard>> Interface Handler InprocServer32 C:\Windows\System32\ksproxy.ax ThreadingModel Both {
  -B703EF0} Microsoft WBEM (non) <<Standard>> Marshaling for IEnumWbemClassObject InprocServer32 %systemroot%\system32\wbem\fastpro
  cor\WebDVD Device Segment to <<Standard>> Video Renderer Device Segment C:\Windows\System32\mpvidctl.dll ThreadingModel Apartma
RECOVERY ARTIFACTS – THOROUGH RESET
SUMMARY

- Each Recovery option will leave unique Artifacts behind
- System Restore Points are accessible using current technology
- Refresh and Reset will leave similar artifacts in the Boot System
- Refresh and Reset will destroy all System Restore Points on machine
- Users Settings will persist over Refresh and Restore Point
- Refresh will have a copy of the Registry file prior to refresh in Windows.old
- The thorough reset option does the best job of destroying the evidence
Questions?

WINDOWS 8 FORENSICS
WINDOWS 8 RESEARCH

- Amanda C.F. Thomson
  - [http://propellerheadforensics.com/](http://propellerheadforensics.com/)
- Ethan Fleisher
  - [http://computerforensics.champlain.edu/blog/windows-8-forensics-part-2](http://computerforensics.champlain.edu/blog/windows-8-forensics-part-2)
- My Research
  - [http://randomthoughtsofforensics.blogspot.com/](http://randomthoughtsofforensics.blogspot.com/)
WINDOWS 8 RESOURCES

MICROSOFT TECHNET ARTICLES

- System Restore

- System Refresh and Reset