Volume Shadow Copy and Registry Forensics

Eric Rowe
eric.rowe@rcmp-grc.gc.ca
Technological Crime Learning Institute

High tech crime investigations are growing globally, and the Canadian Police College (CPC) is the only organization in Canada that offers a comprehensive cybercrime training program. A national approach to technological crime investigations is critical in maintaining optimal response capability in terms of common knowledge, skills and abilities. The Technological Crime Learning Institute’s (TCLI) centralized training approach, relatively unique internationally, prevents bad case law and ensures consistent, high-quality standards in Canadian high-tech crime investigations.

The TCLI offers advanced and specialized workshops and courses ranging from computer forensic analysis to Internet investigative techniques to computer network intrusion investigations. The top-notch staff and instructors/facilitators consist of officers from various police services, civilian specialists and public service employees, and also include law-enforcement and private-sector subject-matter experts.

To offer the very best training, the TCLI team is continually alert, staying on top of new trends, keeping up to speed with new technology and staying connected to the global community through diverse communities of practice.
What am I going to cover

• Volume Shadow Copy Basics
• Shadow Copies on a Live Machine
• Some Command Line
• Shadow Explorer
• Working with Disk Images
• Some Registry Keys
Why look at old versions of the Registry?

- **Overwritten data**: Values and data in keys such as *typedURLs* may be over-written from one session to another.

- **Registry Related Timeline Analysis**: You may be able to determine user activity during a more extended time frame.

- **Anti-Anti-Forensics**: Technologically sophisticated users may attempt to “clean” their Registry.
Why look at old versions of the Registry?

- **Deleted users**: Deleted users’ NTUSER.DAT files will show up in the Shadow Copies.

- **Malware Analysis**: Changes can help you determine when malware was installed.
SHADOW COPY BASICS
Volume Shadow Service (VSS)

“The Volume Shadow Copy Service (VSS) is a built-in Windows mechanism that enables the creation of consistent point-in-time copies of data, known as shadow copies or snapshots.”

- Introduced with Windows XP/2003
- XP used it to back up critical system files only
Volume Shadow Copy (VSC)

- Introduced with Windows 2003 Server and Vista
- **Block level incremental snapshots** are taken of any thing modified on the system
- **2003 Server** - Users can recover older versions of documents from their network shares
- **Vista** – Users can recover older versions of files
VSC Availability

**Vista**: Business, Enterprise, and Ultimate

**VSS** runs on all platforms of Vista however.

**Windows 7**: All editions
Block-level differential copy

Whenever a change is made to live data, the *block of data being modified* is *copied* to a “differences area” associated with the shadow copy before the change is written to the live data block.

Overlaying the modified data on the live data creates a view of the live data at the point in time when the shadow copy was created.
Volume Shadow Copy

- Shadow Copy data is stored in the `<Volume>\System Volume Information` folder
Volume Shadow Copy

- **Does not snapshot:**
  - Unallocated space
  - Slack space
  - Page file
  - Hibernation file
Shadow Copy Maximum

- Maximum number of snapshots: 64
- Number of snapshots may also be limited by the maximum size of snapshots - set in the configuration settings
- Old shadow copies are purged (i.e. over-written)
Q: How Often are Shadow Copies Made?
A: It varies....

- When **new software** is installed
- When **new drivers** are installed
- **Every 24 hours** on some systems
- **7am and 12am** (Mon-Fri) on **servers**
- Whenever a **user decides** to make one

- You may find **several shadow copies** taken on the **same day**
Question

Q: Is a **securely deleted** (i.e. **overwritten**) file recoverable from a volume shadow copy?

A: **Yes**, because a block-level copy of the overwritten file is made.
Q: Are the **date and time stamps** on files found in shadow copies accurate?

A: They should be. However you need to adjust your **time zone settings** make sure the UTC times are properly dealt with.
Question

Q: Can I delete or modify a file found inside a shadow copy?
A: No. Windows will not allow you to.
Questions

Q: Can I *create* a file inside a shadow copy?
A: **No.** Windows will not allow you to.

![Error message](Unable to create file)

 Syndrome error (65535).
Q: Can I create / delete / modify a Registry Key, value, or data inside a shadow copy?
A: No. Windows will not allow you to.
**Q:** Do users have access to the System Volume Information folder?

**A:** No. You can change your access rights however...

```
C:\>cacls "C:\System Volume Information" /P
user:F

Are you sure (Y/N)? y
```

processed dir: C:\System Volume Information
SHADOW COPIES ON A LIVE MACHINE
Is VSC turned on?

- Automatically on for the **drive** that Windows is installed on.
- Can only be turned on for drives that are formatted using the **NTFS file system**.
SOME COMMAND LINE...
Command Shell

- Commands should be run from within an administrative command shell
Display the Shadow Copy Storage

- `vssadmin list shadowstorage`
- `vssadmin list shadowstorage /on=c:`

![Screenshot showing the output of `vssadmin list shadowstorage` command with details for volumes C: and E:]

- **Volume C:**
  - Shadow Copy Storage association
  - Used Shadow Copy Storage space: 8.906 GB (3%)
  - Allocated Shadow Copy Storage space: 9.353 GB (3%)
  - Maximum Shadow Copy Storage space: 10 GB (3%)

- **Volume E:**
  - Shadow Copy Storage association
  - Used Shadow Copy Storage space: 366.016 MB (0%)
  - Allocated Shadow Copy Storage space: 642.891 MB (0%)
  - Maximum Shadow Copy Storage space: 1.821 GB (0%)
List all the volume shadow copies

- vssadmin list shadows

```
C:\sandbox> 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: \{8167c355-5a3f-4fbe-bef2-a21e23a83134\}
  Contained 1 shadow copies at creation time: 13/03/2012 7:07:21 AM
  Shadow Copy ID: \{d4b94ee3-6619-45b7-9b6f-ba29a8a5636\}
    Original Volume: \?\Volume\{ab7f9be2-4b71-11e1-8313-806e6f6e6963\}\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
    Originating Machine: user-PC
    Service Machine: user-PC
    Provider: 'Microsoft Software Shadow Copy provider 1.0'
    Type: ClientAccessible
    Attributes: Persistent, Client-accessible, No auto release, Differentiable, Auto recovered

Contents of shadow copy set ID: \{51a5c02-6d8e-4d45-bd18-fd67ea720117\}
  Contained 1 shadow copies at creation time: 14/03/2012 3:25:33 PM
  Shadow Copy ID: \{964cb613-15f9-4fca-8ee1-cd6264f81135\}
    Original Volume: \?\Volume\{ab7f9be2-4b71-11e1-8313-806e6f6e6963\}\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
    Originating Machine: user-PC
    Service Machine: user-PC
    Provider: 'Microsoft Software Shadow Copy provider 1.0'
```
Creation Time and Shadow Copy Volume Number

NOTE: creation time is saved in UTC, however it is displayed adjusted for the displaying computer’s time zone settings.
Original Volume and Machine

Contents of shadow copy set ID: \{afbef1ad-ac86-411d-b9e1-09e6191d7e74\}
  Contained 2 shadow copies at creation time: 19/03/2012 9:37:14 AM
  Shadow Copy ID: \{1ac6b03e-867c-4949-afc0-f05cbec41f98\}
  Original Volume: \(\text{C:}\)\\\%\Volume\{ab7fbbe2-4b71-11e1-8313-806e6f6e6963\}\GLOBALROOT\Device\HarddiskVolumeShadowCopy17
  Originating Machine: user-PC
  Service Machine: user-PC
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered

  Shadow Copy ID: \{2c062ad3-ecf4-4d2e-a4d9-ba42ae1c779c\}
  Original Volume: \(\text{E:}\)\\\%\Volume\{3bfe23de-5657-11e1-8ff3-806e6f6e6963\}\GLOBALROOT\Device\HarddiskVolumeShadowCopy16
  Originating Machine: user-PC
  Service Machine: user-PC
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered
List the volume shadow copies for a specific volume

- `vssadmin list shadows /for=E:`
Create a link to a specific shadow copy

mklink /d C:\vsc
<ShadowCopyVolume>\

mklink /d C:\vsc
\\GLOBALROOT\Device\HarddiskVolumeShadowCopy13\
Create a link to a specific set of shadow copies – batch file

- The following command creates links to Volume Shadow Copies 4-6
- They will be placed under the C:\vsc\ folder
- The C:\vsc folder must be created before you run the command

```
for /l %%i in (4,1,6) do mklink /d C:\vsc\vsc%%i\\?\GLOBALROOT\DEVICE\HarddiskVolumeShadowCopy%%i
```
c:\sandbox> createlinks.bat

c:\sandbox> for /L %i in (4 1 6) do mklink /d C:\vsc\vsc%i \%GLOBALROOT\Device\HarddiskVolumeShadowCopy%i

c:\sandbox> mklink /d C:\vsc\vsc4 \%GLOBALROOT\Device\HarddiskVolumeShadowCopy4\symbolic link created for C:\vsc\vsc4

c:\sandbox> mklink /d C:\vsc\vsc5 \%GLOBALROOT\Device\HarddiskVolumeShadowCopy5\symbolic link created for C:\vsc\vsc5

c:\sandbox> mklink /d C:\vsc\vsc6 \%GLOBALROOT\Device\HarddiskVolumeShadowCopy6\symbolic link created for C:\vsc\vsc6
Create a link to a every shadow copy on the system

```powershell
for /f "tokens=4" %f in ('vssadmin list shadows ^|findstr GLOBALROOT') do @for /f "tokens=4 delims=\" %g in ("%f") do @mklink /d %SYSTEMDRIVE%\vsc\%g %f
```

Scripted for command shell – not for a batch file
Create a link to a every shadow copy on the system

- This will create links to every VSC on every volume currently connected to the computer
- You will need to run vssadmin in order to know the details (e.g. creation times) of each VSC
Write Blocked Drives

- You should be able to use all these commands on write-blocked drives that are connected to your investigator PC.
- You can create symbolic links on your investigator’s HD from a write-blocked HD.
Acquiring older versions of the Registry from links

1. List the shadow copies
2. Create symbolic links to the VSCs
3. Use FTK imager to logically acquire the shadow copies
4. You can export the Registry files

C:\Windows\System32\config
C:\Users\<username>\NTUSER.DAT
NTUSER.DAT – FTK Imager
(Export the NTUSER.DAT file)
SHADOW EXPLORER
Shadow Explorer

• Shadow Explorer can be run on write-blocked drives connected to your Investigator PC
• Shadow Explorer can be run in VMs
Shadow Explorer

- You can connect to a **write-protected hard drive** and use Shadow Explorer to view and export files from snapshots.
WORKING WITH DISK IMAGES
Working with Disk Images

- **LiveView**: Create a virtual hard drive from the image file, then add it to an existing VM with VSC turned off for analysis.

- **EnCase**: Mount the image with the Physical Disk Emulator module (PDE) then analyze.

- **ProDiscover**: Add the image and mount the shadow copies or use VM method.
Working with Disk Images

See Chapter 3 – Volume Shadow Copies:

• Forensic Tool
• Allows you to mount and view shadow copies
• Allows you to export Registry files
• You can then use the tool of your choice to analyze the Registry files
ProDiscover Forensics - VSC Test 002

File  Action  View  Tools  Help

- Capture Image...
- Add
- Create Search Index
- Search
- Stop Search

Capture & Add Image...
- Image File...
- Disk...

All supported files (*.eve;*.cmp;*.pdg;*.pds;*.dd;*.e01;*.lfc;*.vhd;*.vmdk;*.000;*.Ex01)
Right-click on the volume and select Mount Shadow Volume
Select the Shadow Copy Volume that you want. Then select the drive letter you want to give it.
The volume that you seized from the suspect HD will appear as the first drive in the list.

The Shadow Copy Volume will show up as the drive letter you have given it.
You can export Registry files from the original volume as well as from any of the shadow copy volumes.
You can now examine the exported Registry files.
ProDiscover VMWare Method

• You can also create a **virtual hard disk** with **ProDiscover** and add it to an **existing virtual machine**.

• You should then be able to **examine** and **export** the shadow copies from inside the virtual machine using the tools of your choice. (e.g. Vssadmin, Shadow Explorer, etc.)
ProDiscover Image Conversion Tools

- Secure Wipe...
- Copy Disk...
- Copy Evidence of Interest
- Filter By Hash Set
- Batch Calculate Hashing...
- Signature Matching...
- Scan HPA...
- Image Conversion Tools
- VMWare Support for "DD" Images...
- Convert ProDiscover Image to "DD"...
- Convert ProDiscover Image to "ISO"...
- Convert "DD" Image to "ISO"...
- Convert Expert Witness Image to "DD"...
Open VMWare and add the HD to an existing virtual machine.
1. Mount the E01 file with FTK imager
2. Use LiveView to create the VM
3. VMWare will start the VM
4. Create symbolic links to Shadow Copies
5. Export Registry files to your analysis computer
Mount the E01 file with FTK imager.

- Select "Image Mounting..." from the menu.
- Choose the E01 file and set the mount type to "Physical Only".
- Set the mount method to "Block Device / Writable".
- Click "Mount" to mount the file.

Disk image is now mounted.
Use LiveView to create the VM
VMware will start the VM
You will need VMWare Tools
Create symbolic links to the Shadow Copies
Export the Registry files and run your analysis tools.
VOLUME SHADOW COPY AND THE REGISTRY
Tools and Techniques

Method #1: Registry Decoder

Method #2: RegRipper & WinMerge
Registry Decoder

Dr. Lodovico Marziale - Digital Forensics Solutions

- Allows you to extract all the shadow copy versions of Registry files from mounted disks

- Allows you to run RegRipper type scripts on extracted individual Registry files

- Allows you to run RegRipper type scripts on extracted pairs of Registry files
Registry Decoder

- Registry files from current machine as well as shadow copies must be collected from a live machine using RegDecoderLive.
- You will need to mount the image.
- You will need the user’s password.
- You may need to extract the Registry files from the image and then crack the password.
Ripping & Differencing
Differencing

Results from the search or plug-in that are only in the first file chosen are **RED**, results that are common between both files are **BLACK**, and results that are only in the second file are **BLUE**.
<table>
<thead>
<tr>
<th>Device Name</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 \DosDevices\D:</td>
<td>??\IDE#CdRomNECVMMWar_VMware\IDE\CDR10__________1.00</td>
<td></td>
</tr>
<tr>
<td>2 \DosDevices\E:</td>
<td>??\STORAGE\RemovableMedia\8&amp;\a6d4ec4\0\RM{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
<tr>
<td>3 ??\Volume{61e2385b-bbde-11e1-8efc-000c290bab6f}</td>
<td>??\STORAGE\RemovableMedia\8&amp;\a6d4ec4\0\RM{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
<tr>
<td>4 ??\Volume{096a8cf5-39fd-11e1-91c8-806d6172696f}</td>
<td>??\IDE#CdRomNECVMMWar_VMware\IDE\CDR10__________1.00</td>
<td></td>
</tr>
<tr>
<td>5 \DosDevices\A:</td>
<td>??\FDC\GENERIC_FLOPPY_DRIVE{6&amp;\1435b2e2&amp;\0&amp;\0{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
<tr>
<td>6 ??\Volume{096a8cf7-39fd-11e1-91c8-806d6172696f}</td>
<td></td>
<td>북북북</td>
</tr>
<tr>
<td>7 \DosDevices\C:</td>
<td></td>
<td>북북북</td>
</tr>
<tr>
<td>8 ??\Volume{aa8c2eb6-3ae4-11e1-8ef7-806d6172696f}</td>
<td>??\IDE#CdRomOptiarc\DVD_RW_AD-7580S__________F820__________F820___</td>
<td></td>
</tr>
<tr>
<td>9 ??\Volume{aa8c2ebf-3ae4-11e1-8ef7-000c298bea7c}</td>
<td>??\STORAGE\RemovableMedia\8&amp;\236c8015\0\RM{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
<tr>
<td>10 ??\Volume{aa8c2e0-3ae4-11e1-8ef7-000c298bea7c}</td>
<td>??\STORAGE\RemovableMedia\8&amp;\9acc928\0\RM{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
<tr>
<td>11 ??\Volume{096a8cf4-39fd-11e1-91c8-806d6172696f}</td>
<td>??\FDC\GENERIC_FLOPPY_DRIVE{6&amp;\1435b2e2&amp;\0&amp;\0{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
<tr>
<td>12 \DosDevices\D:</td>
<td>??\IDE#CdRomOptiarc\DVD_RW_AD-7580S__________F820__________F820___</td>
<td></td>
</tr>
<tr>
<td>13 \DosDevices\E:</td>
<td>??\STORAGE\RemovableMedia\8&amp;\9acc928\0\RM{53f5630d-b6bf-4f5d-96d2-50c000a2f1d2}</td>
<td></td>
</tr>
</tbody>
</table>
Timelining

- You can create Registry Key timelines and export them.
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSDTC\MTxOCI</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSDTC\SECURITY</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSDTC\SECURITY\XAKkey</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSDTC\Setup</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSDTC\XADLL</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSLicensing</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSLicensing\HardwareID</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSLicensing\Store</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSMQ</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSMQ\Parameters</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSMQ\Parameters\LOCMsetup</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSMQ\Parameters\Setup</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSMQ\Setup</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSNInstaller</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSXML60</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MSXML60\Setup</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MULTIMEDIA</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MULTIMEDIA\audio</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MULTIMEDIA\audio\VolumeControl</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MULTIMEDIA\DirectXMedia</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MULTIMEDIA\MediaPlayer2</td>
</tr>
<tr>
<td>08/01/12</td>
<td>restore[0ABC30C1-22A7-4F03-8BD5-291E]</td>
<td>CORE from Z:\vmshared 2\coord-exfil-1</td>
<td>$PROTOCOL.HIV\Microsoft\MULTIMEDIA\MediaPlayer2\Devices</td>
</tr>
</tbody>
</table>
Searching

- You can search the current Registry as well as the shadow copies.
- You can do comparative searches between two Registry files in order to highlight differences.
<table>
<thead>
<tr>
<th>Rank</th>
<th>Last Write Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2012/01/08 14:41:57</td>
<td>$SPROTON.HIV\Microsoft\Windows NT\CurrentVersion\Terminal Server\In</td>
</tr>
<tr>
<td>2</td>
<td>2012/01/08 14:50:50</td>
<td>$SPROTON.HIV\Microsoft</td>
</tr>
<tr>
<td>3</td>
<td>2012/01/08 14:43:07</td>
<td>$SPROTON.HIV\Policies\Microsoft</td>
</tr>
<tr>
<td>4</td>
<td>2012/02/02 11:22:39</td>
<td>$SPROTON.HIV\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft</td>
</tr>
<tr>
<td>5</td>
<td>2012/01/08 08:37:00</td>
<td>$SPROTON.HIV\Classes\CLSID{6FDDC324-4E03-4BFE-B185-3D77768DC92F}</td>
</tr>
<tr>
<td>6</td>
<td>2012/01/08 08:37:00</td>
<td>$SPROTON.HIV\Classes\CLSID{6FDDC324-4E03-4BFE-B185-3D77768DC93D}</td>
</tr>
<tr>
<td>7</td>
<td>2012/01/08 08:37:00</td>
<td>$SPROTON.HIV\Classes\CLSID{6FDDC324-4E03-4BFE-B185-3D77768DC92E}</td>
</tr>
<tr>
<td>8</td>
<td>2012/01/08 08:37:00</td>
<td>$SPROTON.HIV\Classes\CLSID{B54ED509-4E03-4BFE-B185-3D77768DC908}</td>
</tr>
<tr>
<td>9</td>
<td>2012/01/08 08:37:00</td>
<td>$SPROTON.HIV\Classes\CLSID{114F5598-0B22-40A0-86A1-C83EA495ADB}</td>
</tr>
<tr>
<td>10</td>
<td>2012/01/08 08:37:01</td>
<td>$SPROTON.HIV\Classes\CLSID{6FDDC324-4E03-4BFE-B185-3D77768DC37}</td>
</tr>
<tr>
<td>11</td>
<td>2012/01/08 08:37:00</td>
<td>$SPROTON.HIV\Classes\CLSID{6FDDC324-4E03-4BFE-B185-3D77768DC932}</td>
</tr>
</tbody>
</table>
REGRIPPER AND WINMERGE
RegRipper and WinMerge

Step #1: Mount Image

Step #2: Create links to shadow copies

Step #3: Export Registry files

Step #4: Run Registry Ripper on the files

Step #5: Use WinMerge to compare them
RegRipper

• Harlan Carvey
• Free Tool - You can also write your own Perl scripts for it

“RegRipper is NOT intended for use with live hive files. Hive files need to be extracted from a case (or from a live system using FTK Imager…), or accessible via a tool such as Mount Image Pro or F-Response.”
Registry Ripper

Registry Ripper, v.2.02

- **Hive File:** C:\Users\user\Desktop\ProDiscoverRegistry\Volur
- **Report File:** C:\sandbox\Volume2.txt
- **Plugin File:** ntuser

- **winlogon_u... Done.**
- **policies_u... Done.**
- **wallpaper... Done.**
- **vista_bitbucket... Done.**
- **shellfolders... Done.**
- **arpcache... Done.**
- **clampitm... Done.**
- **unreadmail... Done.**

0 plugins completed with errors.

- **Rip It** 
- **Close**
Registry Ripper

- Registry Ripper output is a text file
WinMerge

• WinMerge is a free Open Source differencing and merging tool for Windows.

• WinMerge can compare both folders and files, presenting differences in a visual text format that is easy to understand and handle.

• It can be used to compare RegRipper output files
Choose the two ripped files you want to compare.
WinMerge

Difference locations

Differences show up as coloured lines

Identical data is not coloured
Reporting

- WinMerge can create HTML reports of the differences between compared files
SOME EXAMPLES OF REGISTRY KEYS WORTH LOOKING AT...
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

- Gives you a better idea of the time frame during which each URL was visited
- Finding a TypedURL in several different shadow copies speaks to the frequency with which the URL may have been visited
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>url1</td>
<td>REG_SZ</td>
<td><a href="http://www.theweathernetwork.com/weather/maps/caouno">http://www.theweathernetwork.com/weather/maps/caouno</a></td>
</tr>
<tr>
<td>url10</td>
<td>REG_SZ</td>
<td><a href="http://www.cnn.com/">http://www.cnn.com/</a></td>
</tr>
<tr>
<td>url11</td>
<td>REG_SZ</td>
<td><a href="http://cbc.ca/">http://cbc.ca/</a></td>
</tr>
<tr>
<td>url12</td>
<td>REG_SZ</td>
<td><a href="http://centralops.net/">http://centralops.net/</a></td>
</tr>
<tr>
<td>url13</td>
<td>REG_SZ</td>
<td><a href="http://www.whatismyip.com/">http://www.whatismyip.com/</a></td>
</tr>
<tr>
<td>url14</td>
<td>REG_SZ</td>
<td><a href="http://keepvid.com/">http://keepvid.com/</a></td>
</tr>
<tr>
<td>url15</td>
<td>REG_SZ</td>
<td><a href="http://zythom.blogspot.com/">http://zythom.blogspot.com/</a></td>
</tr>
<tr>
<td>url16</td>
<td>REG_SZ</td>
<td><a href="http://blog.crimenumerique.fr/">http://blog.crimenumerique.fr/</a></td>
</tr>
<tr>
<td>url17</td>
<td>REG_SZ</td>
<td><a href="http://192.168.6.107/">http://192.168.6.107/</a></td>
</tr>
<tr>
<td>url19</td>
<td>REG_SZ</td>
<td><a href="http://htciawcc.webex.com/">http://htciawcc.webex.com/</a></td>
</tr>
<tr>
<td>url2</td>
<td>REG_SZ</td>
<td><a href="http://www.bbc.co.uk/news/health-18770328">http://www.bbc.co.uk/news/health-18770328</a></td>
</tr>
<tr>
<td>url20</td>
<td>REG_SZ</td>
<td><a href="https://htciawcc.webex.com/mw0306ld/mywebex/default">https://htciawcc.webex.com/mw0306ld/mywebex/default</a></td>
</tr>
<tr>
<td>url21</td>
<td>REG_SZ</td>
<td><a href="http://www.dmares.com/pub/nt_32/vss.exe">http://www.dmares.com/pub/nt_32/vss.exe</a></td>
</tr>
<tr>
<td>url22</td>
<td>REG_SZ</td>
<td><a href="http://www.francopol.org/comites-techniques/cybercrime">http://www.francopol.org/comites-techniques/cybercrime</a></td>
</tr>
<tr>
<td>url23</td>
<td>REG_SZ</td>
<td><a href="http://www.francopol.org/file:///C:/Program%20Files%20(x86)/VMware/VMware%20Player/VMwarePlayer/VMwarePlayer.exe">http://www.francopol.org/file:///C:/Program%20Files%20(x86)/VMware/VMware%20Player/VMwarePlayer/VMwarePlayer.exe</a></td>
</tr>
<tr>
<td>url25</td>
<td>REG_SZ</td>
<td><a href="http://ninjacloak.com/">http://ninjacloak.com/</a></td>
</tr>
<tr>
<td>url3</td>
<td>REG_SZ</td>
<td><a href="http://www.slavasoftware.com/hashcalc/">http://www.slavasoftware.com/hashcalc/</a></td>
</tr>
<tr>
<td>url4</td>
<td>REG_SZ</td>
<td></td>
</tr>
</tbody>
</table>
\System\ControlSet#\Services\TCPIP\Parameters Interfaces

- May give you an **IP address & configuration history**
- May, in conjunction with \WZCSVC\Parameters\Interfaces\CLSID, show you **multiple dates and times** that a user **connected to a WAP**
Software\Microsoft\WZCSVC\Parameters\Interfaces

- Can allow you to determine if a WAP’s settings were changed recently (encryption, authentication, SSID, etc.)
Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

- Can allow you to determine multiple last connected dates and times
<table>
<thead>
<tr>
<th>Name</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProfileName</td>
<td>Network 2</td>
</tr>
<tr>
<td>Description</td>
<td>Network</td>
</tr>
<tr>
<td>Managed</td>
<td>0x0000000000 (0)</td>
</tr>
<tr>
<td>Category</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>Date Created</td>
<td>DB 07 0B 00 02 00 16 00 0D 00 08 00 3B 00 19 00</td>
</tr>
<tr>
<td>Name Type</td>
<td>0x00000006 (6)</td>
</tr>
<tr>
<td>Date Last Connected</td>
<td>DB 07 0B 00 02 00 16 00 0D 00 0B 00 1C 00 BD 03</td>
</tr>
</tbody>
</table>

- **Category 0 = Public Network Configuration**
- **Network Information, Stored by GUID**
- **Date Created:** 2011-11-Tue-22 22:13:08:59
- **Name Type:** 6 = Wired
- **Date Last Connected:** 2011-11-Tue-22 13:11:28

**Key Properties**

- **Last Written Time:** 11/22/2011 18:11:28 UTC

software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{994C3340-A060-43CC-964D-D7A2F3B121CE}
Autorun Keys

- Registry autoruns are still the most frequently used mechanisms for malware persistence
- May show you when malware was first installed on the computer
- May help you confirm how long malware has been on the system
MRUs

- May allow you to determine a time frame during which docs were opened
- May show docs that were opened from removable (or networked) storage media
Deleted or altered Keys/Values/Data

- May allow you to **identify and recover** deleted or altered Keys, Values, or Data