The world is full of obvious things which nobody by any chance ever observes.
–Sherlock Holmes
Why has the surge worked?
In order to win we are required to have:

- “Firm political will and extreme patience"
- “Considerable expenditure of time and resources"

Successful ... operations require Soldiers to possess the following:

- “A clear appreciation of the essential nature of the conflict.
- “An understanding of the motivation, strengths, and weaknesses of the insurgent“
- “Adaptive, self–aware, and intelligent leaders"
New Threats = Aggressive Tactics

- Understand that the new threats require:
  - Patience and Time
  - Understanding of the Tactics and Strategy of your attackers
  - Resources and Personnel

- Aggressive Incident Response
  - React Faster
  - More Independence
  - Quick Analysis
    - New Indicators
      - Developed in 4 hours
      - Deployed in 24 hours
What?

- 4 hours? Seriously?
- Deployed in an Enterprise in 24 hours?

Why are indicators so important?

- Indicators:
  - Key to being able to detect, react, mitigate attacker
  - Management of indicators crucial to work of responders
    - Network Based Indicators
    - Application/Filesystem Indicators
      - The above is what we will quickly talk about today
  
  - Advantage: You can deploy signatures faster than the attackers are able to code AND deploy new malware
How to do it? Indicator Basics

- **Registry Keys**
  - Default Keys
  - Modified Keys
  - Utilization Keys

- **Default Files**
  - Name
  - Purpose
  - Path
  - MD5 Hash
  - Fuzzy Hash
  - Additional Details
    - Will Anti-Virus Detect

- **Filesystem Timeline Context**
  - Data Modified/Accessed
  - Metadata Modified
  - Volume Birthdate
Application Indicator Tools

- HELIX3 2.0 Bootable CDROM
- VMware Image(s) with snapshots enabled
  - VISTA
  - XP
  - 2000/2003
- Active Registry Monitor
  - Compare two snapshots of a registry to see what has been added/changed
- InCtrl5
  - Application Installer Analyzer
Application Footprinting Tools

- Memory Analysis
  - mdd.exe
  - Volatility

- Timeline Analysis (*fls/*ils/*mactime*)
  - Sleuthkit Version 3.0
  - Monitor file system access while an executable runs/installs
  - Look for recently created/modified files or binaries

- Other Locations for additional indicators
  - Restore Point Data
  - Volume Shadow Copy
What is Active Registry Monitor (ARM)?
What is InCtrl15?

InCtrl15 - Install Control for Windows

Install program details
- Install program: \Documents and Settings\User\Desktop\sp60\setup.exe
- 32-bit Windows Executable
- Parameters:
- Description: sp60setup

Reports
- Report filename: \program files\inctrl15\RPT_0000.HTM

What to track
- Registry...
- Drives...
- INI files...
- Text files...

Pre-install
- Registry
- Files and folders
- INI files
- Text files

Post-install
- Registry
- Files and folders
- INI files
- Text files

Analysis
- Registry
- Files and folders
- INI files
- Text files

Close
Help
About
GO!

HK
KEY_LOCAL_MACHINE\system\controlset001\control\pls\mulanguages\vc\2\ttyres.dll
What is Memory Analysis?

- Snapshot of memory
- Move to analysis system
- Analyze with Volatility

C:\>mdd -o \192.168.2.2\images\appforensics\baseline_memory.img
-> mdd
-> ManTech Physical Memory Dump Utility
Copyright (C) 2008 ManTech Security & Mission Assurance
-> This program comes with ABSOLUTELY NO WARRANTY; for details use option '-w'
This is free software, and you are welcome to redistribute it
under certain conditions; use option '-c' for details.
-> Dumping 255.48 MB of physical memory to file \192.168.2.2\images\appforensics\baseline_memory.img.

65402 map operations succeeded (1.00)
0 map operations failed

took 251 seconds to write
MD5 is: db75142b813a9b2a8a886a5eaaa

C:\>
Timelines of file activity can be easily created using many tools.

The process has two steps:
- Gathering filesystem metadata
- Sorting/Converting metadata into something you can analyze

Benefits:
- Can watch system activity around time of incident
  - Files that were accessed, deleted, and modified
  - Tools that were executed
  - Patterns of activity
MAC Meaning by File System

- The MACB column changes depending on the file system that is being examined.
- NTFS and EXT2/3 Systems identify “C” as the metadata change time.
- File creation time is listed as a ‘B’ for file “Birthdate”.
- FAT does not have a metadata change time.

<table>
<thead>
<tr>
<th>File System</th>
<th>M</th>
<th>A</th>
<th>C</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ext2/3</td>
<td>Modified</td>
<td>Accessed</td>
<td>Inode Changed</td>
<td></td>
</tr>
<tr>
<td>FAT</td>
<td>Modified</td>
<td>Accessed Date</td>
<td></td>
<td>Created</td>
</tr>
<tr>
<td>NTFS</td>
<td>Modified</td>
<td>Accessed</td>
<td>MFT Modified</td>
<td>Created</td>
</tr>
</tbody>
</table>
The timeline has many columns:
- Time: All entries with the same time are grouped
- Size of file
- m, a c, or b: each is set depending on metadata file system type
- Permissions and mode
- User and Group
- Metadata Address
- File Name
  - Deleted files have “(deleted)” at the end
  - Unallocated inodes are: <image_device_name-dead-2043>

<table>
<thead>
<tr>
<th>TIME</th>
<th>FILESIZE</th>
<th>MACB time</th>
<th>Permissions</th>
<th>UID/GID</th>
<th>INODE #</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 03 2006 16:20:37</td>
<td>20452</td>
<td>m.c.</td>
<td>-rwxr-xr-x</td>
<td>root</td>
<td>80932</td>
<td>C:\rob.doc</td>
</tr>
</tbody>
</table>
Example of timeline output collected from a Windows Machine

```
Sat Aug 18 2007 10:48:54 22016 n... -/rrrxrxxwx 0 0 60 <ipcase_ntfs.img-PS.doc-dead-60>
Sat Aug 18 2007 10:50:07 22016 n... -/rrrxrxxwx 0 0 63 <ipcase_ntfs.img-PPS.doc-dead-63>
Sat Aug 18 2007 16:47:59 26348294 .a.b -/rrrxrxxwx 0 0 48 <ipcase_ntfs.img-SNL - Celebrity Jeopardy - Robin Wi
Zet4db.avi-dead-48>
Sat Aug 18 2007 17:05:33 22016 .a.b -/rrrxrxxwx 0 0 60 <ipcase_ntfs.img-PS.doc-dead-60>
Sat Aug 18 2007 17:06:46 22016 .a.b -/rrrxrxxwx 0 0 63 <ipcase_ntfs.img-PPS.doc-dead-63>
Sat Aug 18 2007 17:35:08 435904 ...b -/rrrxrxxwx 0 0 71 <ipcase_ntfs.img-$858D311.jpg-dead-71>
Sat Aug 18 2007 17:45:04 435904 .a... -/rrrxrxxwx 0 0 71 <ipcase_ntfs.img-$858D311.jpg-dead-71>
Sat Aug 18 2007 17:45:06 435904 n... -/rrrxrxxwx 0 0 71 <ipcase_ntfs.img-$858D311.jpg-dead-71>
Sat Aug 18 2007 17:47:27 0 nach -/rr-rr-rr-rr-0 0 0 78 <ipcase_ntfs.img-PA150105.JPG-FF3a00b448-thp-dead-78>
Sat Aug 18 2007 18:41:51 22016 ..c -/rrrxrxxwx 0 0 60 <ipcase_ntfs.img-PS.doc-dead-60>
Sat Aug 18 2007 18:41:52 22016 ..c -/rrrxrxxwx 0 0 63 <ipcase_ntfs.img-PPS.doc-dead-63>
Sat Aug 18 2007 19:07:36 544 nach -/rrrxrxxwx 0 0 58 <ipcase_ntfs.img-$188D311.jpg-dead-58>
Sat Aug 18 2007 19:08:21 26348294 ..c. -/rrrxrxxwx 0 0 71 <ipcase_ntfs.img-$858D311.jpg-dead-71>
Zet4db.avi-dead-48>
Tue Jun 26 2001 12:48:34 26348294 n... -/rrrxrxxwx 0 0 48 <ipcase_ntfs.img-SNL - Celebrity Jeopardy - Robin Wi
Zet4db.avi-dead-48>
```
How do I Create a Timeline?

- Creation of a timeline is a three step process:
  - Create an intermediate data file
    - The resulting file is often called the BODY file
    - Two tools that can create a BODY file:
      1. ils (live system or against an image file)
      2. fls (live system or against an image file)
  - Sort the data to create a timeline
    3. mactime (sort bodyfile using the mactime tool)
Timeline Creation: Steps One/Two

- A *BODY* file is first generated with data on all files in the images.
- Data can be collected for:
  - Allocated files (*fls*)
  - Deleted file names (*fls*)
  - Unallocated inodes (*ils*)
The `fls` tool in The Sleuth Kit can be used to collect timeline information from the filename layer.

- `--m <mount>` flag forces the tool to output data in the mactime format, including data on deleted files.
- The `--m` flag also requires the mounting point of the image for cosmetic reasons.
- Remember to give the `--r` flag for recursive.

Usage:

```
# fls --r --m <mountpoint> <image/device>
```

- `--r`: Recurse on directories
- `--s <seconds>`: timeskew of system in seconds
- `--m <mountpoint>`: Prepend output with appropriate mount point (e.g. C:, /bin, or even just a “/”)
Bodyfile
Step #2: ils -m

- The *f1s* tool gave us timeline data for allocated and deleted files from the filename layer, but there is more to see.
- Some deleted files will not have a deleted filename, but the metadata structure still contains valuable information.
- We have to parse the metadata layer using *ils*.

Usage:

```
# ils -m <image/device>
-m: mactime format
-s <seconds>: timeskew of system in seconds
```
The third step is to make a timeline with a subset of the *BODY* file

- Human-Readable
- In order from earliest timestamp to latest timestamp
Create Timeline
Step #3 mactime

- The mactime tool is a perl script that takes the data files as input (from mac-robber)
- It can be given a date range to restrict itself or it can cover the entire time range.

USAGE:

# mactime <options> -b bodyfile <date-range>

Options:
- -b: Body file location (data file) (STDIN is default)
- -y: Dates use the year first
- -m: Months use a number instead of the month name
- -z: Specify the time zone
- -d: Comma delimited format (can be imported into a database)
  Optional: Date Range
  - Example 01/01/2002–02/01/2002
What is: Fuzzy Hashing?

- Identify Similar Files
  - Altered Documents
  - Partial Files
- Hashes and compares similarities between files based on hash values
  - Called Piecewise Hashing
- Typical hash algorithms take whole file
- Fuzzy hashing slice up file and examine smaller pieces
ssdeep

# ssdeep -m file_of_hashes [OPTIONS] FILES

Options:
- `-m file_of_hashes`: Load file of hashes for matching
- `-r`: Enable recursive mode
- `-p`: Pretty matching mode
- `-d`: Enable directory mode
- `-b`: Strips leading directory information
- `-l`: Displays relative file path

Website: http://ssdeep.sourceforge.net/
GUI front-end: http://forensicszone.com/SSDeepFE/SSDeepFE.htm
ssdeep File Matching

Example 1: Comparing two similar files using ssdeep

C:\>ssdeep ESSAY_DRAFT.doc
ssdeep 1.0--blocksize:hash:hash.filename
1536:pyZWX5Q+30JmFKSG+xDg/h+xD+xD+xD+xIWFxIWY+xD+xEwrpGvpGc+xD+xDn:Iz5Q0,"C:\ESSAY_DRAFT.doc"

C:\>ssdeep ESSAY_FINAL.doc
ssdeep 1.0--blocksize:hash:hash.filename
1536:xfgcSKWtiy53Bza73sKSG+xDg/h+xD+xD+xIWFxIWY+xD+xEwk+xD+xIWHAPuMx1:xSKo53B1s
"C:\ESSAY_FINAL.doc"

C:\>ssdeep -b ESSAY_DRAFT.doc > hashes.txt

C:\>ssdeep -bm hashes.txt ESSAY_FINAL.doc
ESSAY_FINAL.doc matches ESSAY_DRAFT.doc (61)
Application Forensics Methodology

We have the tools.. Here is one way to apply them.
Application Footprinting Step-By-Step

- Create a baseline image and take a snapshot of that image.
Registry Snapshot Baseline

- Take initial registry snapshot using ARM
- Save to disk
Memory Image Baseline

- Snapshot of memory
- Move to analysis system
Boot into HELIX
Run `fls` and `ils` into a bodyfile and copy the bodyfile off the system

```
[root (bin)]# fdisk -l /dev/sda

Disk /dev/sda: 17.1 GB, 17179869184 bytes
255 heads, 63 sectors/track, 2088 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot Start  End   Blocks  Id  System
/dev/sda1   * 1 2089 16775168   7  HPFS/NTFS
[root (bin)]# ./fls -r -m C: /dev/sda1 > ~/BODYFILE BEFORE_TEST

[root (bin)]# ./ils -m /dev/sda1 >> ~/BODYFILE BEFORE_TEST

[root (bin)]# scp /root/BODYFILE BEFORE TEST root@192.168.2.2:/images/windowsforensics
[root@linuxforensics windowsforensics]# cd /images/windowsforensics/
[root@linuxforensics windowsforensics]# mactime -b BODYFILE BEFORE_TEST > timeline1.txt
[root@linuxforensics windowsforensics]#
```
Start Activity

- Once you have baselined your system take your initial action or install of the device.
- Take another snapshot as soon as the device or application has been recognized by the system.
- Continue to take snapshots periodically as well as boot into Helix to see how the filesystem has been affected.
Install/Run Program

Spector Pro Setup V6.0 Build 1288

- Progress
  - Installing Spector Pro 6.0
  - Initializing Configuration

- Spector Pro Setup
  - Would you like to remove the Spector installation file?
    - It is recommended that you say Yes for optimal stealth performance.
      - Yes
      - No
Registry Comparison

- Take another Registry Snapshot and use the “Compare Here” option
  - Examine New Keys (Added)
  - Examine Modified Keys (Distinction in Data)
Memory Analysis Program Running

C:\Documents and Settings\User>cd ..
C:\Documents and Settings>cd ..
C:\>mdd -o \\192.168.2.2\images\appforensics\afterinstall_memory.img

- ManTech Physical Memory Dump Utility
  Copyright (C) 2008 ManTech Security & Mission Assurance

- This program comes with ABSOLUTELY NO WARRANTY; for details use option `-w`
  This is free software, and you are welcome to redistribute it
  under certain conditions; use option `-c` for details.

- Dumping 255.48 MB of physical memory to file \\192.168.2.2\images\appforensics\afterinstall_memory.img.

65402 map operations succeeded (1.00)
0 map operations failed

took 190 seconds to write
MD5 is: 5b3a732c8b40d821986e349012f4482

C:\>

[root@SIFTWorkstation Volatility-1.3_Beta]# python volatility files -f /images/appforensics\afterinstall_memory.img

******************************************************************************
Pid: 4
File \WINDOWS\system32\config\SECURITY.LOG
File \pagefile.sys
File \Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat.LOG
File \WINDOWS\system32\config\SECURITY
File \WINDOWS\system32\config\default
File \WINDOWS\system32\config\default.LOG
File \Documents and Settings\NetworkService\ntuser.dat.LOG
File \WINDOWS\system32\config\SAM.LOG
### Timeline Analysis

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User</th>
<th>Command/Path</th>
<th>Action</th>
<th>Arguments</th>
<th>Permissions</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun Oct 12 2008 14:31:11</td>
<td>4412912</td>
<td>.b</td>
<td>r/rrwxrwxrwx</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/Documents and Settings/User/Desktop/</td>
</tr>
<tr>
<td>Sun Oct 12 2008 14:31:12</td>
<td>4412912</td>
<td>.ac</td>
<td>r/rrwxrwxrwx</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/Documents and Settings/User/Desktop/</td>
</tr>
<tr>
<td>Wed Aug 04 2004 03:56:42</td>
<td>10369</td>
<td>r/rr-xr-xr-x</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/basenser/DE337C952D298F3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rr-xr-xr-x</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/basenser/PP7A32F42F1D076</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/Documents and Settings/User/Local Setting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/diripimg32.dll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>r/rrwxrwxrwx</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
<td>067-128-4 C:/WINDOWS/system32/ftp.exe (deleted-realloc</td>
</tr>
</tbody>
</table>

---

08471114DCF1D14645PE7D1DFP.KWE
InCtrl5 Examination
Formal Catalog Of Indicators

- Registry Keys
  - Default Keys
  - Modified Keys
  - Utilization Keys

- Default Files
  - Name
  - Purpose
  - Path
  - MD5 Hash
  - Fuzzy Hash
  - Additional Details
    - Will Anti-Virus Detect

- Filesystem Timeline Context
  - Data Modified/Accessed
  - Metadata Modified
  - File Birthdate
IR and Forensic Counter Insurgency Manual

- Patience
- Aggressive IR
- Know your network and react accordingly
- Catalog of indicators is vital to your success in large enterprise incidents

- Rob Lee
  - rob.lee@mandiant.com
  - forensics.sans.org