Terremark WorldWide

Harlan Carvey

Vice President, Secure Information Services

BEYOND AVAILABILITY

Registry and Timeline Analysis

SANS Forensic Summit 2010

Today’s Workshop – Registry/Timeline Analysis

- What is “Registry Analysis”?
- Who needs timelines?
- How do I get mine?

Registry Analysis

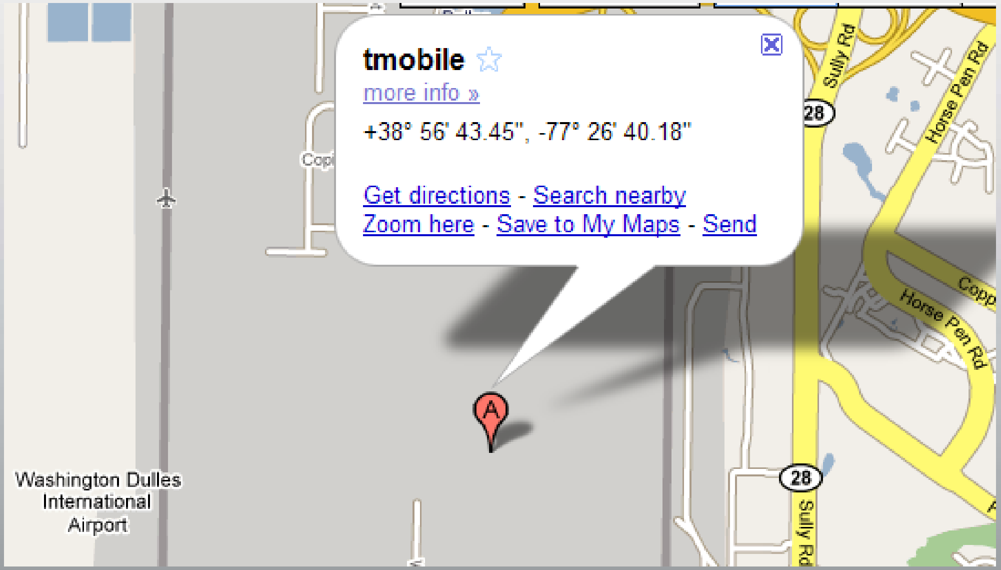
- Registry has a lot of data!
- Registry == logfile
- Binary format of Registry remains the same across versions of Windows (2000 -> Win7), although the artifacts themselves change

What is the Registry?

- Hierarchal binary database structure
- Maintains configuration information about the system, as well as information about the user “e***XP***erience”
- Open Solitaire, change game settings, resize window, close; after rebooting, the settings remain…*how’d that happen?*
- Information like:
  - WAPs connected to (geolocation)
  - IP addresses assigned
  - Devices connected to the system (USB, TrueCrypt volumes, etc.)
  - File accessed or saved by the user
  - Media files viewed by the user (application MRUs)
  - Applications launched by the user

What is the Registry?

- Information like:
  - WAPs connected to (WiFi geolocation)
  - IP addresses assigned
  - Devices connected to the system (USB, TrueCrypt volumes, etc.)
  - File accessed or saved by the user
  - Media files viewed by the user (application MRUs)
  - Applications launched by the user



tmobile

+38° 56' 43.45", -77° 26' 40.18"

more info »
Get directions - Search nearby
Zoom here - Save to My Maps - Send
A
Washington Dulles International Airport
Sully Rd
28
Horse Pen Rd
Copp
Cop

What can we find in the Registry?

```
UserAssist (Active Desktop)
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\…
LastWrite Time Fri Jan 18 00:53:33 2008 (UTC)
Fri Jan 18 00:52:42 2008 (UTC)
    UEME_RUNPATH:C:\WINDOWS\System32\cmd.exe (2)
Fri Jan 18 00:52:34 2008 (UTC)
    UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe (2)
    UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} (2)
```

**GUID refers to an Explorer shell extension*

```
Fri Jan 18 00:52:24 2008 (UTC)
    UEME_RUNCPL:timedate.cpl (4)
Fri Jun 18 23:49:49 2004 (UTC)
    UEME_RUNPATH:C:\System Volume Information\_restore{…}\
            RP2\snapshot\Repository\FS\sms.exe (1)
Fri Jun 18 19:17:05 2004 (UTC)
    UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE (1)
Fri Jun 18 19:16:36 2004 (UTC)
    UEME_RUNPATH:D:\setup.exe (1)
```

What can we find in the Registry?

More examples from the NTUSER.DAT

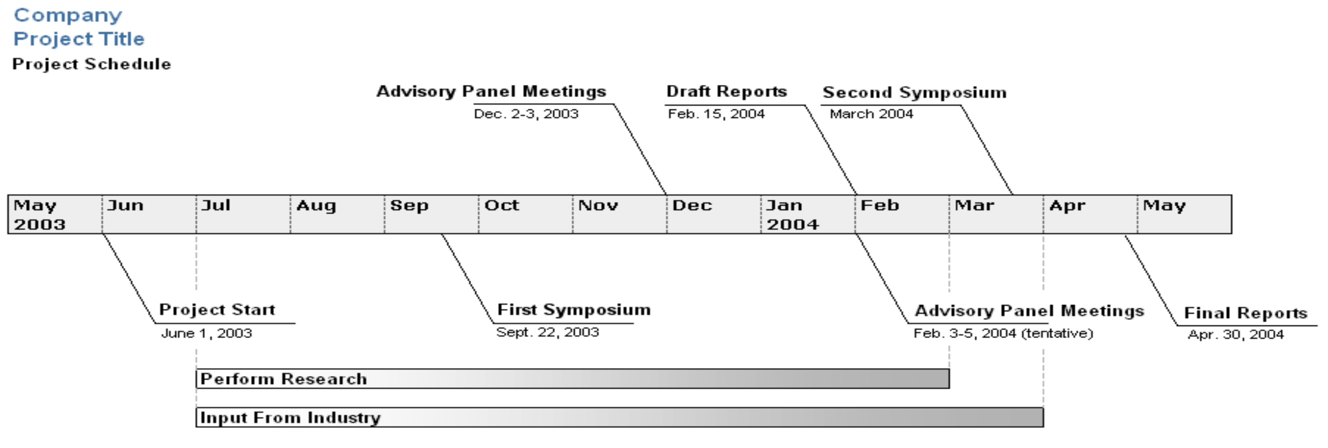
```
Software\Microsoft\Windows\CurrentVersion\Run
LastWrite Time Fri Jun 18 23:49:49 2004 (UTC)
     RPC Drivers -> C:\WINDOWS\System32\inetsrv\rpcall.exe
```

```
RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Fri Jun 18 23:48:17 2004 (UTC)
  MRUList = a
  a   cmd\1
```

What else?

Timelines

Use multiple data sources to provide ***context***, as well as increase ***relative confidence*** of the data



You can also optimize/parallelize analysis but providing a limited data set to another analyst; this is great for scoping, as well as getting answers to the customer.

Data Sources

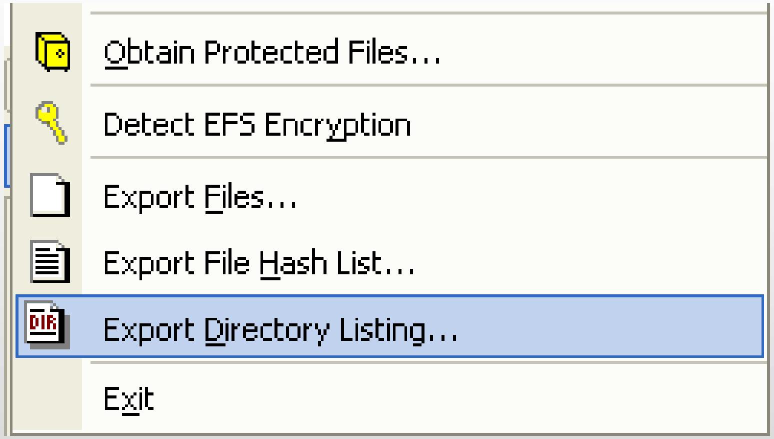
- Time-based data sources on Windows systems – there are a ***LOT*** of them!
  - Different time formats
- Depending upon your analysis goals, you may not need all of them.
- Approach 1: Build your “onion” a layer at a time
- Approach 2: Build your “onion”, peel back the layers

Time Formats

- String: “02/19/2009”
- Unix time: 32-bit
- FILETIME: 64-bit; 100-nanosec increments since midnight, 1 Jan 1601
- SYSTEMTIME: 128-bit (YYYY/MM/DD, HH:MM:SS:msec packed in a structure)
- OLE time: floating point value, days since 30 Dec 1899 (min/sec represented in fraction)

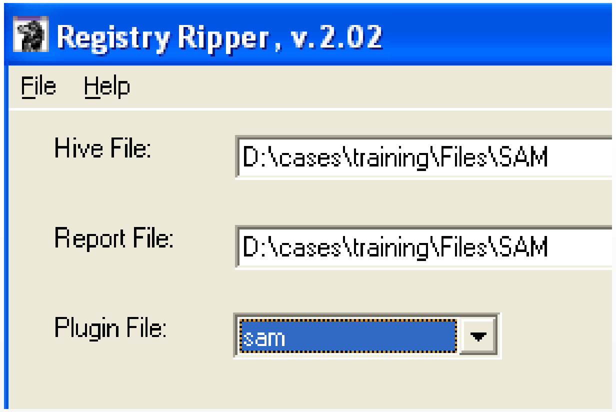
Data Sources

- File system
  - Fls – Directly from image
  - Perl – FTK Imager directory listing
  - MFT/$FILE_NAME attribute
- Prefetch files
- INFO2
- EVT/EVTX
  - Evt – Evtrpt.pl/Evtparse.pl
  - Andreas Schuster’s tools
  - LogParser + Perl
- Windows shortcut/*.lnk files



Data Sources

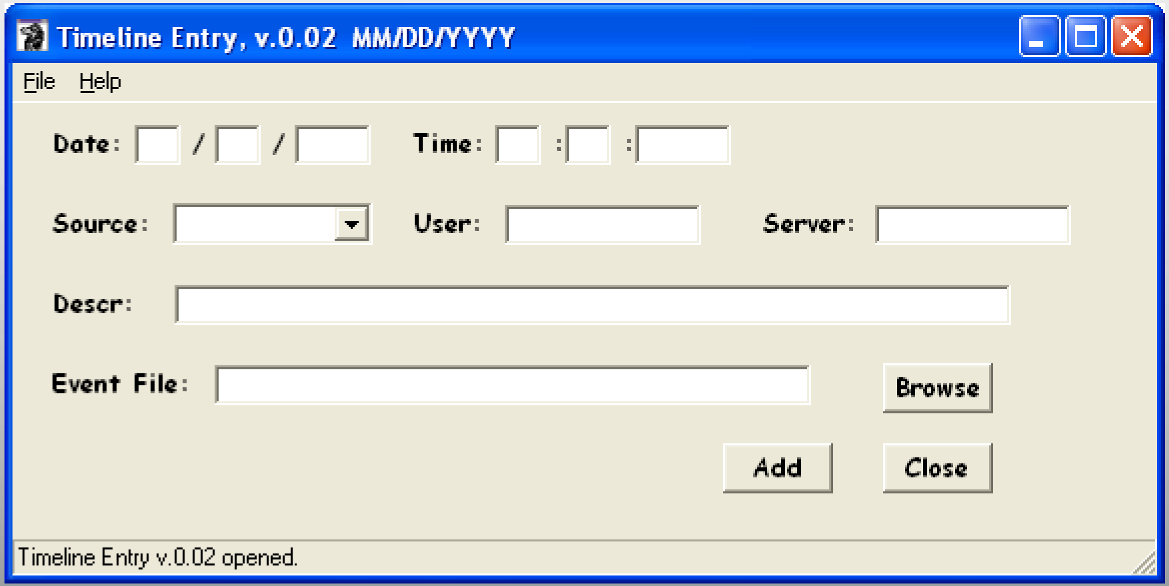
- Registry - RegRipper



Hive File: D:\cases\training\Files\SAM

Report File: D:\cases\training\Files\SAM

Plugin File: sam



Timeline Entry v.0.02 opened.

Data Sources

- XP Restore Points/rp.log
  - RipXP (Registry hives)
- Data within Volume Shadow Copies (Registry hives)
- Document metadata
- Scheduled Task – SchedLgu.txt, *.job files
- Mrt.log, AV logs
- IIS web server logs
- Other application logs
- Index Alloc/$I30 files (contain $FILE_NAME attr)
- Etc, etc…

Timeline Event Format

- Five Field Format
- ***Time*** – Normalized to GMT/UTC
- ***Source*** – What is the source of the data (and there are many, each with their own context)
- ***System/Host*** – Which system is this from? Working with multiple systems?
- ***User***
- ***Description***
- Separator – Pipe, comma, whatever

Ex: time|source|server|user|event description

Creating Timelines

- Sample Image

http://www.forensickb.com/2008/01/forensic-practical.html

- Hakin9 article #2
- Article provides a complete walk-through of tools and commands used
- Let’s look at an example…

Example 1

```
Fri Jun 18 23:49:59 2004 Z
  FILE     System1   - MA.E C:/WINDOWS/Prefetch/RPCALL.EXE-394030D7.pf

Fri Jun 18 23:49:53 2004 Z
  FILE     System1   - MA.E C:/Documents and Settings/vmware/Local Settings/Temp
  FILE     System1   - MACE C:/WINDOWS/Prefetch/PING.EXE-31216D26.pf

Fri Jun 18 23:49:49 2004 Z
  PREF     System1   - PING.EXE-31216D26.pf last run
  PREF     System1   - RPCALL.EXE-394030D7.pf last run
  PREF     System1   - SMS.EXE-01DC4541.pf last run
  FILE     System1   - ...E C:/Documents and Settings/vmware/NTUSER.DAT
  FILE     System1   - MACE C:/WINDOWS/Prefetch/SMS.EXE-01DC4541.pf
  FILE     System1   - ..C. C:/WINDOWS/Prefetch/RPCALL.EXE-394030D7.pf
  FILE     System1   - M..E C:/WINDOWS/system32/inetsrv
  FILE     System1   - .A.. C:/WINDOWS/system32/ping.exe
  REG      System1  vmware - UserAssist: UEME_RUNPATH:C:\System Volume
     Information\_restore{..}\RP2\snapshot\Repository\FS\sms.exe
  REG      System1  vmware - HKCU\..\Run: RPC Drivers -> C:\WINDOWS\System32\inetsrv\rpcall.exe
```

Other Examples

- Parsed Internet.evt file with Perl script and found Security Event Log entries (file initialization); added records to file system metadata, had a complete picture/window of compromise.
- SQL Injection – parsed IIS logs for relevant entries, added those to file system metadata, had what amounted to a .bash_history with time stamps!
- Okay, so now Registry data was used in these examples, but where would you use it?
- User account was used to view images/videos (including dates); sort of obviates the “Trojan Defense”

Tools

- FOSS tools (TSK – mmls/fls, even blkls)
- Pasco – IE index.dat files
- Perl (glue)
- LOTS of customized programming; required, given the sources
- Commercial tools do not provide any of this capability
- SANS SIFT v2.0/log2timeline – uses approach #2 (build the “onion”)

Tools

- Advantages
  - Powerful and flexible
  - Greater coverage for new data formats
- Disadvantages
  - Command line; difficult for some to use
  - No common “standards”

Factors that influence timelines…

- Temporal proximity (close to incident == better data)
- Understanding what you’re looking for (goals, baby!)
- Understanding the system (applications, data sources, etc.)
- JUST DO IT!

Questions?

Harlan Carvey

VP, SIS, Terremark

hcarvey@terremark.com