

BASIS

TECH

WEEK

4TH ANNUAL

OSDF



2013 Open Source Digital Forensics Conference

Doing More with Less

Willi Ballenthin

Consultant

MANDIANT



- **Professionally**
 - Incident response
 - Malware analysis
 - MANDIANT
- **Personally:**
 - Programming
 - Running
 - NYC, USA
- **Contact:**
 - @williballenthin

Effective enterprise-scale IR must be intelligence-driven

- You cannot keep up with an attacker if you deep-dive everything
 - Closing the door on first introductions probably won't get you anywhere
 - They can tunnel faster than you can image
- Manual review does not scale across an enterprise
 - Codify knowledge
 - Distribute jobs and queries across the environment
 - Go hunting (with a plan)

Funnel the initial analysis results into the intel cycle

- Analysis of a box should yield actionable intelligence
 - It *may* help paint a picture
 - It *must* help you be in a better place tomorrow
 - Understand scope of compromise
 - Know how to find evil elsewhere

Funnel the initial analysis results into the intel cycle

- Questions to answer:
 - Network, host indicators?
 - Infection vector?
 - Compromised accounts?
 - Malware & persistence?
 - Timeframe?
 - Is more analysis needed?

Triage analysis should not take too long

- Prepare for dozens or hundreds of compromised boxes
 - Your time is valuable, and time is of the essence
 - Answer questions and move along
- Upshot: recognize patterns across hosts
 - Bad indicators are verbatim features of a binary (but they're cheap & cost effective)
 - Great indicators describe patterns and generalize well
 - Only humans can do this
- (scripting can help)

Enterprise tools or preparation are required

- Have a remote forensic access route ready
 - Agent-based systems can be a great start
 - Custom solutions work too, just make sure they are be maintained
- Acquire data, analyze, and move along!
 - You don't want to wait for images
 - Respond while attackers are still on the system

Lets brainstorm a balanced set of data to collect for triage

- Desirables:
 - High “bang for the buck”
 - Low resource requirements
 - Bandwidth
 - Storage
 - Worry
 - Pareto principle

Lets brainstorm a balanced set of data to collect for triage

Class	Data	Resources Req'd	Completeness
File System	MFT	50 MB	OK
Configuration	Registry Hives	20 MB	Good
Logs	EVT/EVTX	50 MB?	OK
Memory	???		

```
Git/INDXParse - [master●] » zip MFT.copy0.zip MFT.copy0
  adding: MFT.copy0 (deflated 89%)
Git/INDXParse - [master●] » du -sh MFT.copy0*
93M   MFT.copy0
11M   MFT.copy0.zip
```

```
python-registry/testing - [master●] » zip SYSTEM.zip SYSTEM
  adding: SYSTEM (deflated 80%)
python-registry/testing - [master●] » du -sh SYSTEM*
14M   SYSTEM
2.8M  SYSTEM.zip
```

```
python-evtX/testing-evtXs - [master●] » zip Security.evtX.zip Security.evtX
  adding: Security.evtX (deflated 92%)
python-evtX/testing-evtXs - [master●] » du -sh Security.evtX*
21M   Security.evtX
1.7M  Security.evtX.zip
```

These formats compress very well

In compressed 75MB, you can capture the triage data for a typical workstation

What to do with an MFT file?

- AnalyzeMFT.py
- Sanderson Forensics MFTView (not OSS)
- TZWorks ntfswalk (not OSS)
- MFT tools descending from INDXParse
 - Pure Python
 - Backed by module MFT.py for easy reuse
 - <https://github.com/willballenthin/INDXParse>

list_mft.py

- MFT timelining utility
- Concise code: around 200 lines
- Supports \$SI, multiple \$FN, resident INDX records
- Constant memory usage

- How?
 - Each record has an \$FN attribute with a name. The \$FN attribute has a link to the parent record. Iterate the records and walk up the parent links.

```

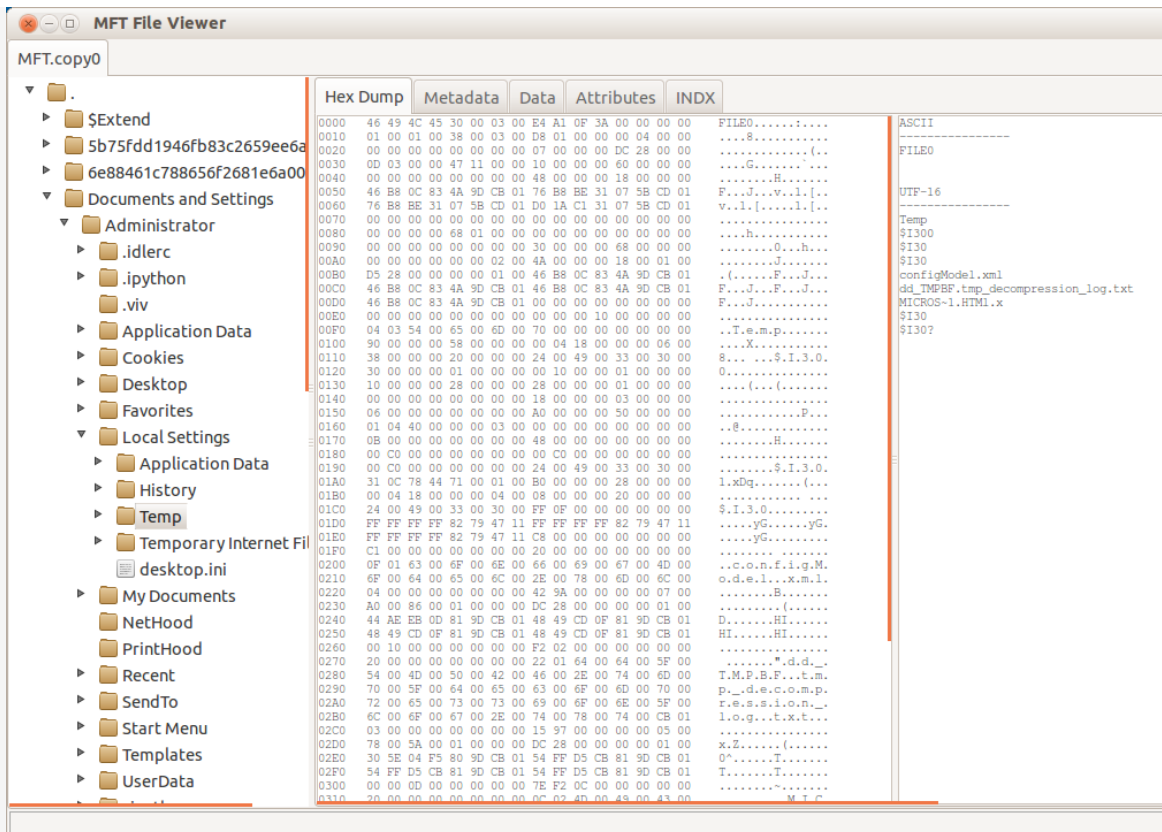
Git/INDXParse - [master] » python list_mft.py MFT.copy0 | tail | mactime -b -
Thu Dec 16 2010 12:56:07      0 ...b 0 368      0      95064      \\.\System Volume Information\_restore{B8A51974-0EE5-4C6F-AC63-
Mon Jul 02 2012 12:31:58      0 mac. 0 368      0      95064      \\.\System Volume Information\_restore{B8A51974-0EE5-4C6F-AC63-
Thu Jul 05 2012 16:52:53      0 macb 0 430      0      95061      \\.\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ngenrootstoreloc
      0 macb 0 430      0      95061      \\.\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ngenrootstoreloc
      16384 macb 0 685      0      95062      \\.\WINDOWS\Temp\Perflib_Perfdata_658.dat (filename, inactive)
      16384 macb 0 685      0      95062      \\.\WINDOWS\Temp\Perflib_Perfdata_658.dat (inactive)
Thu Jul 05 2012 16:52:57      65536 macb 0 279      0      95063      \\.\WINDOWS\SoftwareDistribution\DataStore\Logs\tmp.edb (filena
      65536 macb 0 279      0      95063      \\.\WINDOWS\SoftwareDistribution\DataStore\Logs\tmp.edb (inacti
      0 macb 0 368      0      95064      \\.\System Volume Information\_restore{B8A51974-0EE5-4C6F-AC63-
Thu Jul 05 2012 16:53:04      589824 macb 0 685      0      95060      \\.\WINDOWS\Temp\tmfzggvtv.TMP (filename, inactive)
      589824 macb 0 685      0      95060      \\.\WINDOWS\Temp\tmfzggvtv.TMP (inactive)
python list_mft.py MFT.copy0 266.85s user 0.31s system 99% cpu 4:28.32 total

```

list_mft.py

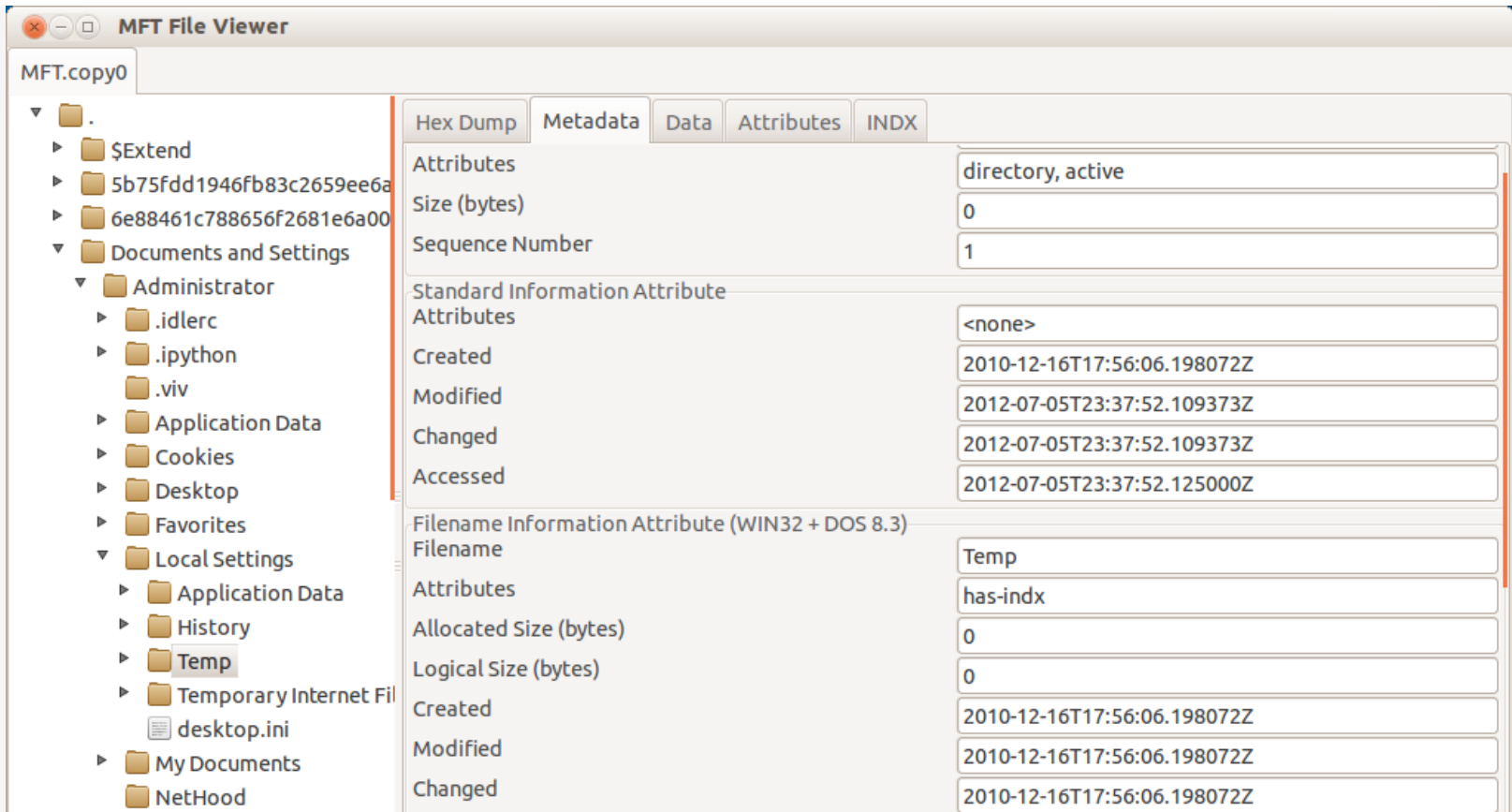
MFTView.py

- Unoriginal name, sorry.
- Pure Python
- Interactive inspection of a file system using only an MFT
- Some features
 - Integrated INDX record parsing
 - Strings, hex view
 - Data extraction and cluster run calculations



MFTView.py

Explore a NTFS file system from just the MFT



MFTView.py Metadata

MFTView.py

- ▼ .
 - ▶ \$Extend
 - ▶ 5b75fdd1946fb83c2659ee6a
 - ▶ 6e88461c788656f2681e6a00
 - ▼ Documents and Settings
 - ▼ Administrator
 - ▶ .idlerc
 - ▶ .ipython
 - ▶ .viv
 - ▶ Application Data
 - ▶ Cookies
 - ▶ Desktop
 - ▶ Favorites
 - ▼ Local Settings
 - ▶ Application Data
 - ▶ History
 - ▶ Temp

Hex Dump	Metadata	Data	Attributes	INDX
0000	5B 2E 53 68 65 6C 6C 43 6C 61 73 73 49 6E 66 6F			[.ShellClassInfo
0010	5D 0D 0A 4C 6F 63 61 6C 69 7A 65 64 52 65 73 6F]..LocalizedReso
0020	75 72 63 65 4E 61 6D 65 3D 40 73 68 65 6C 6C 33			urceName=@shell3
0030	32 2E 64 6C 6C 2C 2D 32 31 37 37 34 0D 0A			2.dll,-21774..

MFTView.py Resident Data

MFT.copy0

- Desktop
 - Favorites
 - Local Settings
 - Application Data
 - History
 - Temp
 - Temporary Internet Files
 - desktop.ini
 - My Documents
 - NetHood
 - PrintHood
 - Recent
 - SendTo
 - Start Menu
 - Templates
 - UserData
 - _python
 - .Visisect_history
 - NTUSER.DAT

Hex Dump Metadata **Data** Attributes INDX

NOTE: Check Disk Geometry

These byte offsets assume the following disk geometry.
Please double check the geometry and update it here.

Volume Offset (bytes)	32256	Cluster Size (bytes)	4096
-----------------------	-------	----------------------	------

Cluster Run	
Offset (clusters)	7307340
Length (clusters)	384
Offset (bytes)	29930896896
Length (bytes)	1572864

Cluster Run	
Offset (clusters)	4953998
Length (clusters)	64
Offset (bytes)	20291608064
Length (bytes)	262144

MFTView.py Non-Resident Data

Desktop

- ▶ Favorites
- ▼ Local Settings
 - ▶ Application Data
 - ▶ History
 - ▶ Temp
 - ▶ Temporary Internet Files
 - desktop.ini
- ▶ My Documents
- ▶ NetHood
- ▶ PrintHood
- ▶ **Recent**
- ▶ SendTo
- ▶ Start Menu
- ▶ Templates
- ▶ UserData
- ▶ _ipython
- .Vivisect_history
- .NTUSER.DAT
- .ntuser.dat.LOG
- .ntuser.dat

Hex Dump Metadata Data Attributes **INDX**

NOTE: Check Disk Geometry

These byte offsets assume the following disk geometry.
Please double check the geometry and update it here.

Volume Offset (bytes) 32256 Cluster Size (bytes) 4096

INDX Record Information

Filename	CWINDO~1.LNK
Size (bytes)	587
Created	2011-08-10T17:30:11.728249Z
Modified	2011-08-10T17:30:11.728249Z
Changed	2011-08-10T17:30:11.728249Z
Accessed	2011-08-10T17:30:11.728249Z

INDX Record Information

Filename	GETTEX~1.LNK
Size (bytes)	693
Created	2011-08-11T15:23:26.862000Z
Modified	2011-08-11T15:23:26.862000Z

MFTView.py INDX Records

Hex Dump	Metadata	Data	Attributes	INDX
0000	46 49 4C 45 30 00 03 00 13 60 0D 3A 00 00 00 00	FILE0....`.:....		ASCII
0010	01 00 01 00 38 00 03 00 D8 01 00 00 00 04 00 00	...8.....		-----
0020	00 00 00 00 00 00 00 00 07 00 00 00 48 00 00 00H...		FILE0
0030	28 01 47 11 00 00 00 00 10 00 00 00 60 00 00 00	(.G.....`...		
0040	00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00H.....		
0050	88 83 2A 30 16 9D CB 01 28 99 76 66 05 5B CD 01	..*0....(.vf.[..		UTF-16
0060	28 99 76 66 05 5B CD 01 28 99 76 66 05 5B CD 01	(.vf.[..(.vf.[..		-----
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		Temp
0080	00 00 00 00 AE 02 00 00 00 00 00 00 00 00 00 00		\$I300
0090	00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 000...h...		\$I30
00A0	00 00 00 00 00 00 02 00 4A 00 00 00 18 00 01 00J.....		\$I30
00B0	1C 00 00 00 00 00 01 00 88 83 2A 30 16 9D CB 01*0....		37.tmp
00C0	88 83 2A 30 16 9D CB 01 88 83 2A 30 16 9D CB 01	..*0.....*0....		MPC4B.tmp
00D0	88 83 2A 30 16 9D CB 01 00 00 00 00 00 00 00 00	..*0.....		MPC5F.tmp
00E0	00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00		\$I30
00F0	04 03 54 00 65 00 6D 00 70 00 00 00 00 00 00 00	..T.e.m.p.....		\$I30?
0100	90 00 00 00 58 00 00 00 00 04 18 00 00 00 06 00	...X.....		~DFF2A7.tmp
0110	38 00 00 00 20 00 00 00 24 00 49 00 33 00 30 00	8... ..\$.I.3.0.		
0120	30 00 00 00 01 00 00 00 00 10 00 00 01 00 00 00	0.....		
0130	10 00 00 00 28 00 00 00 28 00 00 00 01 00 00 00	...{...{.....		
0140	00 00 00 00 00 00 00 00 18 00 00 00 03 00 00 00		
0150	06 00 00 00 00 00 00 00 A0 00 00 00 50 00 00 00P...		
0160	01 04 40 00 00 00 03 00 00 00 00 00 00 00 00 00	..e.....		
0170	0A 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00H.....		
0180	00 B0 00 00 00 00 00 00 00 B0 00 00 00 00 00 00		
0190	00 B0 00 00 00 00 00 00 24 00 49 00 33 00 30 00\$.I.3.0.		
01A0	31 0B 6E 3B 6F 00 01 00 B0 00 00 00 28 00 00 00	l.n;o.....(...		
01B0	00 04 18 00 00 00 04 00 08 00 00 00 20 00 00 00		
01C0	24 00 49 00 33 00 30 00 5F 04 00 00 00 00 00 00	\$.I.3.0._.....		
01D0	FF FF FF FF 82 79 47 11 FF FF FF FF 82 79 47 11vG.....vG.		

MFTView.py Strings

`get_file_info.py`

- Check the MFT structures for interesting files:
 - Timeline all embedded timestamps
 - Extract strings from MFT stack
 - Review (active & slack) INDX records
 - Pull out many other fields

```
Git/INDXParse - [master] » python get_file_info.py MFT.copy0 12
MFT Record: 123
Path: \.\WINDOWS\system32\usmt
Metadata:
  Active: 1
  Type: directory
  Flags:
    $SI Modified: 2010-12-16 11:44:38.578125
    $SI Accessed: 2012-07-05 23:24:13.171875
    $SI Changed: 2010-12-16 11:44:38.578125
    $SI Birthed: 2010-12-16 11:41:33.343750
  Owner ID: 0
  Security ID: 278
  Quota charged: 0
  USN: 0
Filenames:
  Type: WIN32 + DOS 8.3
  Name: usmt
  Flags: has-idx
  Logical size: 0
  Physical size: 0
  Modified: 2010-12-16 11:41:33.343750
  Accessed: 2010-12-16 11:41:33.343750
  Changed: 2010-12-16 11:41:33.343750
  Birthed: 2010-12-16 11:41:33.343750
  Parent reference: 29
  Parent sequence number: 1
```

```
Changed: 2010-12-16 11:41:33.343750
Birthed: 2010-12-16 11:41:33.343750
Parent reference: 29
Parent sequence number: 1
Attributes:
  Type: $STANDARD INFORMATION
  Name: <none>
  Flags: has-idx
  Resident: True
  Data size: 0
  Allocated size: 0
  Value size: 72
  Type: $FILENAME INFORMATION
  Name: <none>
  Flags: has-idx
  Resident: True
  Data size: 0
  Allocated size: 0
  Value size: 74
  Type: $INDEX ROOT
  Name: $I30
  Flags: has-idx
  Resident: True
  Data size: 0
  Allocated size: 0
  Value size: 56
  Type: $INDEX ALLOCATION
```

get_file_info.py

Page 1 of 2

```
Value size: 8
INDX root entries: <none>
INDX root slack entries: <none>
Timeline:
 2010-12-16 11:41:33.343750   birthed   $SI   usmt
 2010-12-16 11:41:33.343750   birthed   $FN   usmt
 2010-12-16 11:41:33.343750   accessed  $FN   usmt
 2010-12-16 11:41:33.343750   modified  $FN   usmt
 2010-12-16 11:41:33.343750   changed   $FN   usmt
 2010-12-16 11:44:38.578125   modified  $SI   usmt
 2010-12-16 11:44:38.578125   changed   $SI   usmt
 2012-07-05 23:24:13.171875   accessed  $SI   usmt
ASCII strings:
FILE0
<H/0
<H/0
<H/0
<H/0
<H/0
Unicode strings:
usmt
$I300
$I30
$I30
cobramsg.dll
guitrn.dll
guitrna.dll
iconlib.dll
log.dll
```

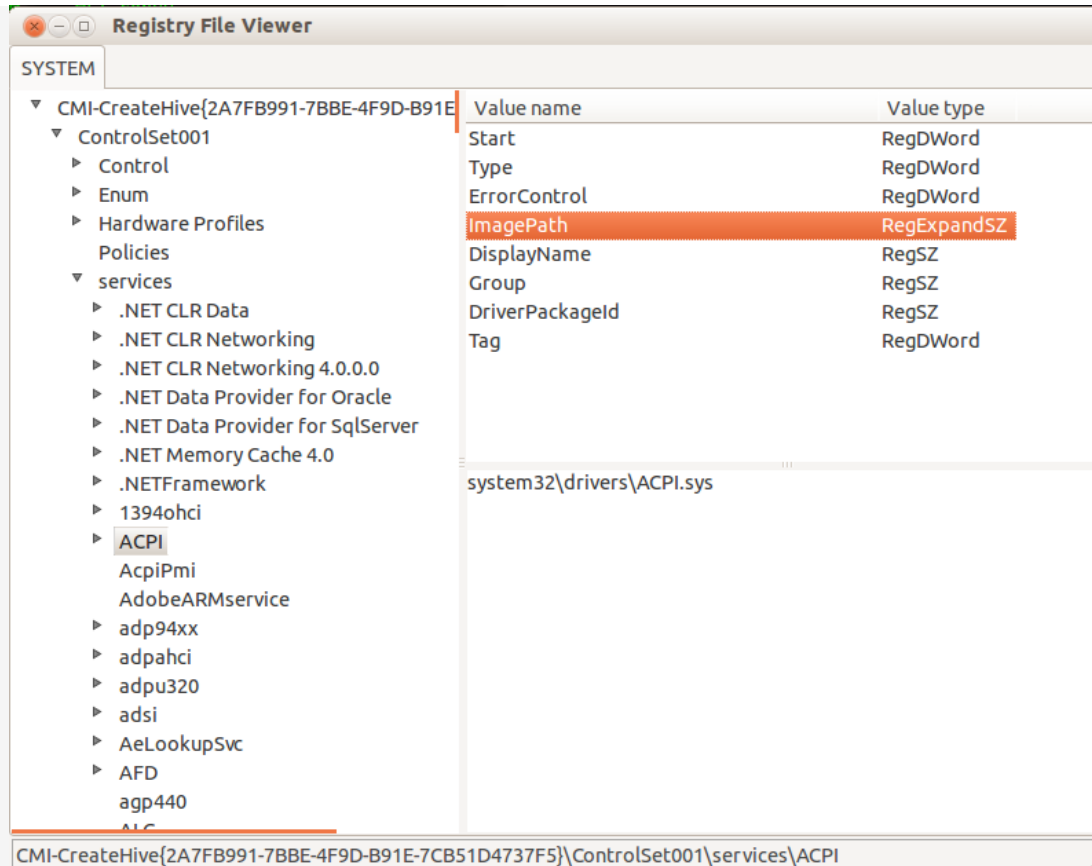
get_file_info.py

Page 2 of 2

- Naturally: start with a timeline
- Manually review entries with MFTView
- Always rinse and repeat

What to do with a Registry hive?

- RegRipper
- MiTeC Windows Registry Analyzer (WRA, not OSS)
- Registry Decoder
- Registry tools included with python-registry
 - Pure Python
 - Backed by stable API in python-registry
 - <https://github.com/willballenthin/python-registry>



regview.py

Kinda like regedit.exe. Except read-only. And cross platform.

```
python-registry/samples - [master] » python findkey.py ../testing/SYSTEM -i beep
nvvpnvvpvvp
[Paths]
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\services\eventlog\System\beep
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\services\eventlog\System\beep

[Value Names]
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Control\Print : BeepEnabled
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\Control\Print : BeepEnabled

[Values]
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Enum\Root\LEGACY_BEEP\0000 : Service
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\Enum\Root\LEGACY_BEEP\0000 : DeviceDesc
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet001\services\Beep : DisplayName
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\Enum\Root\LEGACY_BEEP\0000 : Service
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\Enum\Root\LEGACY_BEEP\0000 : DeviceDesc
- CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}\ControlSet002\services\Beep : DisplayName
```

findkey.py

Search keys, values, paths with various queries.

```
python-registry/samples - [master] » python timeline.py ../testing/SYSTEM --bodyfile | mactime -b - | tail
Sat Aug 10 2013 22:03:06      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
                          0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
                          0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
Sat Aug 10 2013 22:03:26      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
Sat Aug 10 2013 22:03:27      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
Sat Aug 10 2013 22:03:30      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
                          0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
Sat Aug 10 2013 22:03:38      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
Sat Aug 10 2013 22:06:02      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
Sat Aug 10 2013 22:06:13      0 .a.. 0 0      0      0      [Registry SYSTEM] CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB5
```

timeline.py


Timeline Registry key modification timestamps

- *Windows Registry Analysis* by H. Carvey

What to do with Event Log files?

- Parse-EVTX
- GrokEVT
- libevtx
- Carving library used by LfLe.py
 - *Carve for Records (not files)* – Jeff Hamm @ SANS DFIR Summit 2012
 - Pure Python module Evt.py
 - <https://github.com/williballenthin/LfLe>
- Parsing library python-evtx
 - Even more Python
 - <https://github.com/williballenthin/python-evtx>

Sneak peek: Event Log Viewer

- Open source GUI for reviewing event log files
- !
- Indexed search across events
- Multiple views of same data (searching, filtering, sorting)
- Quite slow.
- Lets collaborate!

#	EID	timestamp	Category	Subcategory	Message Summary
91740	4672	2013-09-24T07:02:38....	Privilege Use	Sensitive Privilege Use / Non ...	Special privileges assigned to new logon.
91741	4688	2013-09-24T07:02:38....	Detailed Tracking	Process Creation	A new process has been created.
91742	4688	2013-09-24T07:02:39....	Detailed Tracking	Process Creation	A new process has been created.
91743	4624	2013-09-24T07:03:02....	Logon/Logoff	Logon	An account was successfully logged on.
91744	4672	2013-09-24T07:03:02....	Privilege Use	Sensitive Privilege Use / Non ...	Special privileges assigned to new logon.
91745	4688	2013-09-24T07:03:07....	Detailed Tracking	Process Creation	A new process has been created.
91746	4624	2013-09-24T07:03:10....	Logon/Logoff	Logon	An account was successfully logged on.
91747	4672	2013-09-24T07:03:10....	Privilege Use	Sensitive Privilege Use / Non ...	Special privileges assigned to new logon.
91748	4688	2013-09-24T07:03:10....	Detailed Tracking	Process Creation	A new process has been created.
91749	4688	2013-09-24T07:03:10....	Detailed Tracking	Process Creation	A new process has been created.
91750	4624	2013-09-24T07:03:10....	Logon/Logoff	Logon	An account was successfully logged on.
91751	4672	2013-09-24T07:03:10....	Privilege Use	Sensitive Privilege Use / Non ...	Special privileges assigned to new logon.
91752	4688	2013-09-24T07:03:10....	Detailed Tracking	Process Creation	A new process has been created.
91753	4688	2013-09-24T07:03:11....	Detailed Tracking	Process Creation	A new process has been created.
91754	4688	2013-09-24T07:03:17....	Detailed Tracking	Process Creation	A new process has been created.
91755	4689	2013-09-24T07:03:20....	Detailed Tracking	Process Termination	A process has exited.
91756	4624	2013-09-24T07:03:26....	Logon/Logoff	Logon	An account was successfully logged on.
91757	4672	2013-09-24T07:03:26....	Privilege Use	Sensitive Privilege Use / Non ...	Special privileges assigned to new logon.
91758	4688	2013-09-24T07:03:26....	Detailed Tracking	Process Creation	A new process has been created.
91759	4688	2013-09-24T07:03:29....	Detailed Tracking	Process Creation	A new process has been created.

Event Viewer: Overview


```
<?xml version="1.0" ?>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Guid="54849625-5478-4994-a5ba-3e3b0328c30d" Name="Microsoft-Windows-Security-Auditing"/>
    <EventID Qualifiers="">4672</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>12548</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2013-09-24 07:02:38.622013"/>
    <EventRecordID>91740</EventRecordID>
    <Correlation ActivityID="" RelatedActivityID=""/>
    <Execution ProcessID="528" ThreadID="604"/>
    <Channel>Security</Channel>
    <Computer>WIN-IGQQTGEMUUO</Computer>
    <Security UserID=""/>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-1103806595329-18</Data>
    <Data Name="SubjectUserName">SYSTEM</Data>
    <Data Name="SubjectDomainName">NT AUTHORITY</Data>
    <Data Name="SubjectLogonId">0x000000000000003e7</Data>
    <Data Name="PrivilegeList">SeAssignPrimaryTokenPrivilege
      SeTcbPrivilege
      SeSecurityPrivilege
      SeTakeOwnershipPrivilege
      SeLoadDriverPrivilege
      SeBackupPrivilege
      SeRestorePrivilege
      SeDebugPrivilege
    </Data>
  </EventData>
</Event>
```

Event Viewer: Details

XML

Hex

Binary Structure

```
RootNode (offset=0x18)
  StreamStartNode (offset=0x18)
  TemplateInstanceNode (offset=0x1c, resident=False)
  Substitutions (offset=0x26)
    UnsignedByteTypeNode (offset=0x72) --> 0
    UnsignedByteTypeNode (offset=0x73) --> 0
    UnsignedWordTypeNode (offset=0x74) --> 12548
    UnsignedWordTypeNode (offset=0x76) --> 4672
    NullTypeNode (offset=0x78)
    Hex64TypeNode (offset=0x7a) --> 0x8020000000000000
    FiletimeTypeNode (offset=0x82) --> 2013-09-24T07:02:38.622013Z
    NullTypeNode (offset=0x8a)
    UnsignedDwordTypeNode (offset=0x9a) --> 528
    UnsignedDwordTypeNode (offset=0x9e) --> 604
    UnsignedQwordTypeNode (offset=0xa2) --> 91740
    UnsignedByteTypeNode (offset=0xaa) --> 0
    NullTypeNode (offset=0xab)
    NullTypeNode (offset=0xab)
    WstringTypeNode (offset=0xab) --> Microsoft-Windows-Security-Auditing
    GuidTypeNode (offset=0xf1) --> {54849625-5478-4994-a5ba-3e3b0328c30d}
    WstringTypeNode (offset=0x101) --> Security
    BXmlTypeNode (offset=0x111) --> RootNode (offset=0x1033f21, length=0x284)
      RootNode (offset=0x111)
        TemplateInstanceNode (offset=0x111, resident=False)
        Substitutions (offset=0x11b)
          SIDTypeNode (offset=0x133) --> S-1-5-18
          WstringTypeNode (offset=0x13f) --> SYSTEM
          WstringTypeNode (offset=0x14d) --> NT AUTHORITY
          Hex64TypeNode (offset=0x167) --> 0x000000000000003e7
          WstringTypeNode (offset=0x16f) --> SeAssignPrimaryTokenPrivilege
            SeTcbPrivilege
```

Event Viewer: Structure

XML	Hex	Binary Structure
0000	2A 2A 00 00 A0 03 00 00 5C 66 01 00 00 00 00 00	**.....f.....
0010	73 24 F8 0D F4 B8 CE 01 0F 01 01 00 0C 01 84 30	s\$......0
0020	7C 5E 26 02 00 00 12 00 00 00 01 00 04 00 01 00	^&.....
0030	04 00 02 00 06 00 02 00 06 00 02 00 00 00 08 00
0040	15 00 08 00 11 00 10 00 00 00 04 00 08 00 04 00
0050	08 00 08 00 0A 00 01 00 04 00 00 00 00 00 00 00
0060	00 00 46 00 01 00 10 00 0F 00 10 00 01 00 85 02	..F.....
0070	21 00 00 00 04 31 40 12 01 00 00 00 00 00 00 00	!....l@.....
0080	20 80 73 24 F8 0D F4 B8 CE 01 00 00 00 00 28 01	.s\$......(.
0090	00 00 EC E8 01 01 FC E7 EA 00 10 02 00 00 5C 02
00A0	00 00 5C 66 01 00 00 00 00 00 00 4D 00 69 00 63	...f.....M.ic
00B0	00 72 00 6F 00 73 00 6F 00 66 00 74 00 2D 00 57	.r.o.s.o.f.t.-.W
00C0	00 69 00 6E 00 64 00 6F 00 77 00 73 00 2D 00 53	.i.n.d.o.w.s.-.S
00D0	00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 2D	.e.c.u.r.i.t.y.-
00E0	00 41 00 75 00 64 00 69 00 74 00 69 00 6E 00 67	.A.u.d.i.t.i.n.g
00F0	00 25 96 84 54 78 54 94 49 A5 BA 3E 3B 03 28 C3	..%.TxT.I..>;.(.
0100	0D 53 00 65 00 63 00 75 00 72 00 69 00 74 00 79	.S.e.c.u.r.i.t.y
0110	00 0C 01 AE 0F 78 AB 03 1D 00 00 05 00 00 00 0Cx.....
0120	00 13 00 0E 00 01 00 1A 00 01 00 08 00 15 00 26&
0130	02 01 00 01 01 00 00 00 00 00 05 12 00 00 00 53S
0140	00 59 00 53 00 54 00 45 00 4D 00 00 00 4E 00 54	.Y.S.T.E.M...N.T
0150	00 20 00 41 00 55 00 54 00 48 00 4F 00 52 00 49	. .A.U.T.H.O.R.I
0160	00 54 00 59 00 00 00 E7 03 00 00 00 00 00 00 53	.T.Y.....S
0170	00 65 00 41 00 73 00 73 00 69 00 67 00 6E 00 50	.e.A.s.s.i.g.n.P
0180	00 72 00 69 00 6D 00 61 00 72 00 79 00 54 00 6F	.r.i.m.a.r.y.T.o
0190	00 6B 00 65 00 6E 00 50 00 72 00 69 00 76 00 69	.k.e.n.P.r.i.v.i
01A0	00 6C 00 65 00 67 00 65 00 0D 00 0A 00 09 00 09	.l.e.g.e.....
01B0	00 09 00 53 00 65 00 54 00 63 00 62 00 50 00 72	...S.e.T.c.b.P.r
01C0	00 69 00 76 00 69 00 6C 00 65 00 67 00 65 00 0D	.i.v.i.l.e.g.e..
01D0	00 0A 00 09 00 09 00 09 00 53 00 65 00 53 00 65S.e.S.e
01E0	00 63 00 75 00 72 00 69 00 74 00 79 00 50 00 72	.c.u.r.i.t.y.P.r

Event Viewer: Binary

In the last 30 mins, we covered:

- GUI MFT browser
- CLI MFT timeliner and inspector
- GUI Registry explorer
- CLI Registry timeliner & utils
- GUI EVT(X) tool

...and these work great for rapid triage!

Questions?

