10 Speakers
10 Presentations
360 Seconds Each
Book Signing After SANS360

360 Shades of Grey

E L James

#1 New York Times Bestseller
• 10 Presentations
• 360 Seconds Each
• At 1 Minute Left – Warning
• At Bell –
  – Speaker Stops Speaking
  – Audience Erupts Into Applause
  – Next Speaker Takes Stage
Registry Decoder

- Originally funded by NIJ
- Released in September 2011
- Approaching 10,000 downloads since release
- Open source, written in Python
- Developed for investigators of all skill levels
- Two separate tools, both with full GUIs
  1. Registry Decoder Live
  2. Registry Decoder Offline
Registry Decoder Live

• Gathers registry hives from a running system
• Supports Windows 7, Vista, XP – 32 & 64 bit
• Has the ability to capture the currently active registry hives
  – Use Sleuth Kit libraries to read from the running disk
  – No longer sets restore points
• Also gathers historical files from Restore Points or the Volume Shadow Service
Registry Decoder Offline

• Used to perform registry analysis
  – Designed to automatically handle investigating multiple hives, registry sets, and even machines at once

• A list of things we never wanted to do again:
  – Export hives by hand
  – Run the same tool over and over again
  – Write reports by hand
Initial Processing

• Can process regdecoder live output, raw disk images (dd), split dd images, E01 (libewf), as well as individual registry files
  – Once processed you no longer need the disk images or registry files
  – Can re-open cases later without reprocessing
  – Add as many as you want to a case!
Browsing

• Similar to Access Data’s registry viewer
• Can view tree of keys, name/value pairs, and last written times
• You can copy/paste the last written times!
Timelining

• Timeline any number of hives based on last write time of the key
• Exports to mactime/Sleuthkit format or to Excel
• Can filter to specific time frames using starting and/or ending dates
Plugins

• Full plugin system, each plugin performs targeted analysis of some subset of the registry
• From an investigators POV, basically a ripoff of RegRipper, but written in a better programming language
• Very easy API – many plugins are only ten LOC
Path-Based Analysis

• Lets you instantly determine if a particular registry path exists in any number of hives
• Great for detecting the presence of malware samples, rogue software, specific USB devices...
• If you were given 20 computers and wanted to know which of them had a particular service installed or used a specific wireless network, how would you do it?
Searching – The Best Part!!

- No other registry tool lets you intelligently search the registry
- Search as many hives as you want at once
- A single term or many terms
- You can filter by:
  - Keys, Names, and/or Values
  - Wildcard or full search
  - Last write time of keys (start, end, in between)
<table>
<thead>
<tr>
<th>Last Write Time</th>
<th>Key</th>
<th>Name</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012/05/30 02:59:20</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet002\Control\ControlSet002\Control\CriticalDeviceDatabase\USB\VID_0871&amp;D\PID_0002&amp;M_00</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/11/20 13:51:14</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet002\Control\Control\CriticalDeviceDatabase\USB\VID_0781&amp;D\PID_0002&amp;M_00</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/11/20 13:51:14</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet002\Control\Control\CriticalDeviceDatabase\USB\VID_0599&amp;D\PID_0001</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/05/23 09:14:11</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet001\Control\Control\CriticalDeviceDatabase\USB\VID_04CB&amp;D\PID_010A</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/05/23 09:14:11</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet001\Control\Control\CriticalDeviceDatabase\USB\VID_04CB&amp;D\PID_010D</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/05/23 09:14:06</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet001\Control\Control\CriticalDeviceDatabase\USB\VID_03EE&amp;D\PID_0000</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/06/01 16:52:27</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet001\Control\Control\CriticalDeviceDatabase\USB\VID_04CB&amp;D\PID_0100</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/05/23 09:14:11</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet001\Control\Control\CriticalDeviceDatabase\USB\VID_04CE&amp;D\PID_0002</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
<tr>
<td>2012/05/23 09:14:06</td>
<td>CMICreateHive(F10156BE-0E87-4EF8-969E-50A29D131144)\ControlSet001\Control\Control\CriticalDeviceDatabase\USB\VID_04CE&amp;D\PID_0002 &amp; REV_0500</td>
<td>Service</td>
<td>USBSTOR</td>
</tr>
</tbody>
</table>
### Registry Decoder - Digital Forensics Solutions

**SYSTEM in Partition 0 | Current | CORE from \vmware-host\Shared Folders\Desktop\rdcase\registry**

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClassGUID</td>
<td>REG_SZ</td>
<td>{36FC9660-C465-11CF-8056-444353400000}</td>
</tr>
<tr>
<td>Service</td>
<td>REG_SZ</td>
<td>USBTOR</td>
</tr>
<tr>
<td>DriverPackageId</td>
<td>REG_SZ</td>
<td>_mscs.inf_x86_neutral_eF3a0c30c03F0225</td>
</tr>
</tbody>
</table>

### ControlSet001\Control\CriticalDeviceDatabase

USB#VID_054C&PID_0018&REV_0000 -- 2011-05-23 09:14:11
Diff’ing

- Can diff either search or plugin results from two different registry hives
- Will report results in the GUI and color code the output depending on if the entry is in both files or just one
- Very useful:
  - Was a USB device shared across machines?
  - Has malware infected a machine (extra services, registry keys, etc)?
Reporting

• We wanted to be able to automatically build reports of everything that the GUI knew about
  – So we did!

• With the exception of timelining, which saves to its own formats, everything we talked about can be saved to XLS, PDF, CSV, or HTML

• Can report any number of analysis results or result types (search, plugins, etc)
Resources

• Website: http://www.digitalforensicsolutions.com/registrydecoder/
• Live tool: http://code.google.com/p/regdecoderlive/
• Offline: http://code.google.com/p/registrydecoder/
• Speaker contact:
  – @attrc
  – andrew@memoryanalysis.net
TRIAGE

Standardizing Remote IR Collection
About Us

• Immature
• Global Company
Our Problem

• Slow Response Time
• Understaffed remote location
• Analysts with different skill sets
• Data collection errors
• Manual Process
• Infections missed because of immature capabilities
Our Actions – Before Triage

- Contact Help Desk Support
- Request Files
- Re-Request Correct files
- Re-RE-Request Correct files
- Analyze files
- Request New files if needed
- Re-Request New Files
- Analyze new files
- Determine infection mitigation process
Our Actions – After Triage

• Automatic Email sent to correct Help Desk
• Triage is requested and ran
• Analyze files
• Request new files
• Analyze new files
• Determine infection mitigation
What is Triage?

- Collection of IR Scripts
- Sysinternals
- RegRipper
- DumpIT
- Customizable
- Optional GUI
- INI Configuration
What does it do?

- Runs Sysinternals
- Grabs and Rips Hives
- Grabs Prefetch (Win 7)
- Grabs JumpLists
- Compresses
Limitations

- ADMIN
- Locally
- Prompted
Quick Hits

• Start Up Info
• AV Logs
• RegRipped Hives
Our Results

• Great Starting Point!!

• Trained Monkeys can almost do our jobs now!
CASE STUDY
AV to the rescue

• 9:53 AM Tamper Alert
  • Blocked e621ca05.exe
  • Triage Requested

• 3:18 PM Infection Alert
  • Packed.Generic.356
  • Quarantined APQ1B.tmp

• Machine Info
  • Remote non-domestic site
  • Language Barrier
  • Understaffed Team
Triage Received – AV Logs analyzed

- Received at 3:20pm
- AV Alerts said:
  - WOO WOO I GOT IT!!! I AM THE BEST!!
- Av Logs said:
  - It was a hard fight, but I got them all see –
    - Cleaned E621CA05.exe
    - Cleaned Axsoso.exe
Triage Received – Analyzing reports

- Checked Start Up Info.txt
  - HKCU\Run said:
    - Ummm these entries don’t look good..
    - CDOOSOFT with value \Temp\Herss.exe
    - AXSOSO
Wait what was that??

- Yes we have an autorun out of the Temp Directory
- Axsoso.exe is still on the system
GOOGLE to the Rescue

- AXSOSO.exe
- E621CA05.exe
- HERSS.exe
What hit me?

- Gammima.AG
- GamPass
- SillyFDC.BCT
- Infostealer
Timing BEFORE Triage

- 48 hrs
- 3 hours
- 51 hours
Triage Timings

- 5hr 25 Minutes
- 35 minutes
- 6 hours
Summary

- Semi Automatic Data collect
- Robust
- Customizable
Who Created Triage?
How We Know the Sky is Blue: Child Victim Age Estimation in 360 Seconds

Det. Cindy Murphy
Madison Police Department
608-267-4148
cmurphy@cityofmadison.com
"All our knowledge is the offspring of our perceptions."

Leonardo DiVinci
- Thoughts on Art and Life
The Ability to Identify Sexual Maturity:

- Is universal through history.
- Is universal by sex, race and nationality.
- Is not dependent upon the reality of the depiction.
- Is based upon a variety of detailed perceptions
- All human beings do it.
The REALITY of the depiction DOESN'T MATTER.

It's about PROPORTION and other visual cues.
Proportional Markers

• The Midline - At birth, the midline of the human body, an imaginary line drawn midway between the soles of the feet and the top of the head, is located near the navel.
• Also referred to as the Transverse plane and separates the body into the superior (upper) and inferior (lower) portions.
By the time a person reaches **physical maturity**, the midline of the body lies at the center of the pubic arch.

During **intermediate stages of maturity**, the midline lies proportionately between the navel and pubic arch, and moves progressively lower as an individual matures.
It doesn’t matter how tall an adult is – proportionally the Midline falls at the pubic arch.
The Midline moves down towards the pubic arch as the child gets older.
# Headlengths

## Table 7: Summary of Head Length Proportion by Life Stage [49]

<table>
<thead>
<tr>
<th>Stage</th>
<th>Head Length Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infant (under 10 months old)</td>
<td>3.5 to 4 head lengths tall</td>
</tr>
<tr>
<td>Toddler (12 months to 2 years old)</td>
<td>4 to 5 head lengths tall</td>
</tr>
<tr>
<td>Child (3 years to 11 years old)</td>
<td>5 to 6.5 head lengths tall</td>
</tr>
<tr>
<td>Adolescent (12 years to 17 years old)</td>
<td>6.5 to 7.5 head lengths tall</td>
</tr>
<tr>
<td>Adult (17+ years old)</td>
<td>7.5 head lengths tall</td>
</tr>
</tbody>
</table>
Growth & Development of the Face
Other Perceptual Cues

- Body habitus and musculature
- Height and weight proportion
- Extremity length proportion with respect to torso
- Specific dentition features
- Signs of sexual maturation
- Hirsutism /distribution of body hair
- Fat distribution
- The center or midpoint of the body
- Proportion of the head compared to the body
- Proportion and position of facial features and shape of the head
- Skin and flesh tone and texture
- Voice characteristics
- Body coordination and control of movement
Before you reach for your slide rule...

- Our brains process these visual cues for us automatically through the visual cortex.
How Good Are We At Age Estimation?

Humans have a normative ability to estimate age to within about three years for children between 0 and 18 years old.

Imbalanced Age Estimation - young faces change at a faster rate than older ones, and that consequently, age estimation is more prone to error at older ages both by computers and by humans.
5 Step Age Estimation Process

1. Roughly estimate a three year age range based upon your first impressions of the image.

2. Take the top age in the estimated age range and add three years to that age. Then ask yourself “is there a possibility the person is that age?”

3. Next, take the bottom age in the range and subtract three years. Then ask yourself “is there a possibility the person could be that age?”

4. If your answer is “no” to both of the above questions, keep the initial age range estimate as your answer.

5. If the answer is “yes” to either of the above questions, adjust your three year age range estimate up or down accordingly.
0 Years Old

Histogram for ActualAge = 0.0

- Mean = 1.6
- Std. Dev. = 0.548
- N = 102

Frequency distribution showing estimates for 0 years old.
3 Years Old
6 Years Old
9 Years Old
12 Years Old
15 Years Old
18 Years Old

Melissa Ashley

‘Little’ Lupe Fuentes (Zuleidy Piedrahita)

Traci Lords (10th grade)
(Nora Louise Kuzma)
Born May 7, 1968 [4]
25 Years Old

Histogram for ActualAge = 25.0
Mean = 25.98
Std. Dev. = 4.531
N = 102
Conclusions

• Based upon the preponderance of information from the
  • two age estimation surveys
  • previous research in the area of facial age estimation
  • sexual maturation rating studies

• If the examiner has doubt that the individual is underage, that
doubt is reasonable doubt and the image should not be considered
for criminal charges.

• Conversely, if the investigator perceives that the individual
depicted in an image or video is a child, based upon the visual and
other cues presented within the media, the individual is highly
likely to in fact be a child.

• the estimation technique described herein can be utilized to convey a
reasonably accurate estimation of the age range in which the child
falls.
"All our knowledge is the offspring of our perceptions."
Registry, UserAssist, and VSCs...
UserAssist key provides info about user’s interaction with the Explorer shell (stuff the user clicked on).

We can see the *Most Recent* time the user performed that action but what if we want info regarding preceding times?

That is, if a user performed an action 14 times, what if we want to know when they performed that action the 12\textsuperscript{th} or 11\textsuperscript{th} or 10\textsuperscript{th} time?
Does old data every completely go away?

I say, “nay, nay!”

Thanks to VSCs, some historical data may still exist and be available on the system.

So...choose a method for mounting the image to access the VSCs (ie, VHD, VMDK)
Corey Harrell did a fantastic job documenting means of accessing files within VCSs (http://journeyintoir.blogspot.com)

- Determine VSCs via `vssadmin`
- Mount individual VSCs via `mklink` ("unmount" using `rmdir`)

```
C:\vsc18\Users\Corey\NTUSER.DAT
```

...OR...

- Access the file directly:

```
\\GLOBALROOT\Device\HARDDISK\VolumeShadowCopy18\Users\Corey\NTUSER.DAT
```
NTUSER.DAT from acquired image...
Thu Jan 21 03:10:26 2010 Z
UEME_RUNPATH:C:\Program Files\Skype\Phone\Skype.exe (14)

NTUSER.DAT from VSC18...
Fri Jan 8 04:13:40 2010 Z
UEME_RUNPATH:C:\Program Files\Skype\Phone\Skype.exe (8)
This works, as well, with other Registry keys/values that are known to change (based on time, user activity, etc.)

Requires slight modification to RegRipper tool rip.pl; Corey demonstrates in a blog post which lines of code to comment out (basically removes some error checking)

• NetworkList entries in the Software hive (previous times connected to WAPs)
• SAM hive (last login time)
• RecentDocs MRUs
• Etc.
HAL POMERANZ

@hal_pomeranz
A Hash Is Worth 1000 Words

Hal Pomeranz

Deer Run Associates
Kitteh Porn!
Needle in a Haystack?

• Machines seized from multiple suspects
• >10K images per machine
• Lots of duplicate images

Use hash matching to find "interesting" stuff!
Let's Meet Our Suspects

Emperor Rob
Dark Lord of the Forensicators
"You can tell I'm a criminal mastermind by the eerie laugh…"

Darth Hal
His faithful apprentice
"Does this armor make me look fat?"

Princess Lee-Ah
Enthusiastic Amateur
"No, everybody from Alderaan talks like this..."
### Making a Hash of Things

```bash
$ ls
Darthal  EmpRob  Lee-Ah
$ for i in *; do md5sum $i/* >$i.md5s; done
$ head -3 Darthal.md5s
fafa5efeaf3cbe3b23b2748d13e629a1  Darthal/image001.jpg
18c9d0f826615e5021a344b97e811799  Darthal/image002.gif
18c9d0f826615e5021a344b97e811799  Darthal/image003.gif
$ for i in *.md5s; do sort -k1,1 -u $i >$i.uniq; done
$ ls
Darthal             EmpRob             Lee-Ah
Darthal.md5s        EmpRob.md5s        Lee-Ah.md5s
Darthal.md5s.uniq   EmpRob.md5s.uniq   Lee-Ah.md5s.uniq
```
Find the Common Images

$ awk '{print $1}' *.
uniq | sort | uniq -c | sort -nr
  3 fafa5efeaf3cbe3b23b2748d13e629a1
  3 18c9d0f826615e5021a344b97e811799
...

$ grep -h fafa5efeaf3cbe3b23b2748d13e629a1 *.
uniq
fafa5efeaf3cbe3b23b2748d13e629a1     Darthal/image001.jpg
fafa5efeaf3cbe3b23b2748d13e629a1     EmpRob/image003.jpg
fafa5efeaf3cbe3b23b2748d13e629a1     Lee-Ah/image002.jpg
Common as Dirt
Eliminate "Known Goods"

```
$ awk '{print $1}' knwn-gds.md5s >knwn-gds.md5s-only
$ for i in *.*.uniq; do
grep -vf knwn-gds.md5s-only $i >$i.filt;
done
$ awk '{print $1}' *.*.filt | sort | uniq -c | sort -nr
  3 18c9d0f826615e5021a344b97e811799
  2 ec6548202cd232d49ecd2234ae474a67...
$ grep -h 18c9d0f826615e5021a344b97e811799 *.*.filt
18c9d0f826615e5021a344b97e811799  Darthal/image002.gif
18c9d0f826615e5021a344b97e811799  EmpRob/image010.gif
18c9d0f826615e5021a344b97e811799  Lee-Ah/image171.gif
```
Profit!
Lee-Ah and Emperor Rob?

$ awk '{print $1}' *.filt | sort | uniq -c | sort -nr
  3 18c9d0f826615e5021a344b97e811799
  2 ec6548202cd232d49ecd2234ae474a67
...
$ grep -h ec654202cd232d49ecd2234ae474a67 *.filt
ec6548202cd232d49ecd2234ae474a67 EmpRob/image129.gif
ec6548202cd232d49ecd2234ae474a67 Lee-Ah/image211.gif
Some Things Cannot Be Unseen
Thanks J-Michael!
I have no idea what you're talking about...

http://deer-run.com/

...so here's a bunny with a pancake on its head.
Automating Your Timeline Analysis in 360 Seconds

SANS Forensics and Incident Response Summit - Austin 2012
Background

• Timelines "sometimes" contain a LOT of data.
• Is there a way to automate some of the analysis?
What about YARA?
- Built to identify and classify malware.
- Offers string and regular expression matching.
- Boolean expressions to determine logic.
Background

- What have we got?
  - Large text file.
  - Prior experience with all it's glory.
Log2timeline and YARA Together At Last

- Small script called "l2t_find_evil.py"
- Reads in the l2t_csv file and a YARA rule file.
  - Compares the description and format field against rules.
  - Gives out reports of "known bad"
Example Run

l2t_find_evil.py -r test_yara.rules -f timeline_mft.sorted.txt


private rule MFT_Hit
{
    meta:
        description = "Using the MFT module"

    strings:
        $mft = "Log2t::input::mft"

    condition:
        $mft
}
Example Rule

rule System32BinaryOutsideOfWindowsDir
{
meta:
    description = "System32 binary running in another location"
    case_nr = "5213"

strings:
    $sys = /(Windows|WINNT)\system32\/ nocase
    $exclude_hfmig = /(Windows|WINNT)\$hf_mig\/ nocase
    $exclude_update = /(Windows|WINNT)\$[A-Z0-9]+[0-9]\// nocase
    $exclude_uninstall = /(Windows|WINNT)\$NtUninstall/ nocase

    $exe_accwiz = /\accwiz([0-9]+)\?.exe/
    $exe_append = /\append([0-9]+)\?.exe/

    $exe_zclientm = /zclientm([0-9]+)\?.exe/

condition:
    MFT_Hit and not $sys and not 1 of ($exclude_*) and 1 of ($exe_*)
}
Summary

- YARA rules can be used for first skimming.
- Uses prior case knowledge:
  - Quickly identify similar cases.
  - Quickly identify 'known bad'
- Will release a blog post with additional information.
Detecting Fraudulent Word Documents

In 360 Seconds

Corey Harrell
Overview

- What Are Fraudulent Documents
- Types of Fraud
- Microsoft Word Metadata
- Metadata Red Flags
- Detection Process
- What’s Next
What Are Fraudulent Documents

**Fraudulent**

engaging in fraud; deceitful

**Document**

a piece of written, printed, or electronic matter that provides information or serves as an official record
What Are Fraudulent Documents

Fraudulent Documents

documents providing fake information to commit a fraud
Types of Fraud - Purchasing

- **Explanation**
  - Payments to a fictitious company
  - Payments for goods not received

- **Method to Commit Fraud**
  - Employee creates fake invoice then takes the money
Types of Fraud - Purchasing

- Indictment for Norman Cobbins

“Cobbins carried out a scheme to defraud Holmes County”

“from January 2002 through January, 2011”

“by submitting false invoices and requisitions to the County”

“converting the money to his own personal use”

Types of Fraud – Bid Rigging

- Explanation
  - Collusion between employee and vendor
  - Contract is arranged for certain vendor even though it appears other parties were involved

- Methods to Commit Fraud
  - Employee creates fake bids so vendor wins contract
  - Vendor creates fake bids so they win contract
Types of Fraud – Bid Rigging

FBI and IRS Investigation

“Salvatore Scotto-DiVetta pleaded guilty to rigging bids”

"was accused of receiving $25,000 in cash and gift cards"

contractor "allegedly submitted losing bids in the name of other companies"

Source: http://online.wsj.com/article/SB10001424052748704464704575208374268651564.html
Types of Fraud

Similarity Between Purchasing & Bid Rigging Examples

- Fake documents were created to commit the fraud
  - One was invoices and requisitions
  - One was bids
Word Documents Metadata

Metadata includes:

- AppVersion
- Application
- Characters
- CharactersWithSpaces
- CheckedBy
- Client
- Company
- DateCompleted
- Department
- Destination
- Disposition
- Division
- DocSecurity
- DocumentNumber
- Editor
- Group
- HeadingPairs
- HyperlinkBase
- Language
- Lines
- Mailstop
- Manager
- Matter
- Notes
- Office
- Owner
- Pages
- Paragraphs
- Creator
- Project
- Publisher
- Purpose
- Reference
- Slides
- Source
- Status
- TelephoneNumber
- Template
- TitlesOfParts
- TotalEditTime
- Words
- Category
- CreateDate
- Keywords
- LastModifiedBy
- LastPrinted
- ModifyDate
- RevisionNumber
Word Documents Metadata

Metadata includes:

- AppVersion
- Application
- Characters
- CharactersWithSpaces
- CheckedBy
- Client
- **Company**
- DateCompleted
- Department
- Destination
- Disposition
- Division
- DocSecurity
- DocumentNumber
- Editor
- Group
- HeadingPairs
- HyperlinkBase
- Language
- Lines
- Mailstop
- Manager
- Matter
- Notes
- Office
- Owner
- Pages
- Paragraphs
- **Creator**
- Project
- Publisher
- Purpose
- Reference
- Slides
- Source
- Status
- TelephoneNumber
- Template
- TitlesOfParts
- TotalEditTime
- Words
- Category
- **CreateDate**
- Keywords
- LastModifiedBy
- LastPrinted
- ModifyDate
- RevisionNumber
## Word Documents Metadata

- **Creating and Copying Document**

<table>
<thead>
<tr>
<th>Action</th>
<th>Create Userinfo Username</th>
<th>MetaData Creator</th>
<th>Modify / Saved AS Userinfo Username</th>
<th>MetaData Modifier/Contributor</th>
<th>MetaData Date/Time Created</th>
<th>MetaData Date/Time Modified</th>
<th>MetaData Date/Time Printed</th>
<th>MetaData Revision Number</th>
<th>Save History (2000 only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Copied on Same Fat32 volume</td>
<td>test-2007</td>
<td>No Change: Retains the Userinfo Key Username (test-2007)</td>
<td>*****</td>
<td>No Change: Retains the Userinfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:24)</td>
<td>No Change: Retains Modified Date/Time (14:26)</td>
<td>*****</td>
<td>No Change: Retains Revision # (1)</td>
<td>No Change: Retains file's path (1. user:E\filename)</td>
</tr>
<tr>
<td>Document Copied between Fat32 and NTFS volumes</td>
<td>test-2007</td>
<td>No Change: Retains the Userinfo Key Username (test-2007)</td>
<td>*****</td>
<td>No Change: Retains the Userinfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:24)</td>
<td>No Change: Retains Modified Date/Time (14:26)</td>
<td>*****</td>
<td>No Change: Retains Revision # (1)</td>
<td>No Change: Retains file's path (1. user:E\filename)</td>
</tr>
</tbody>
</table>
### Word Documents Metadata

#### Modifying Document

<table>
<thead>
<tr>
<th>Action</th>
<th>Create UserInfo Username</th>
<th>MetaData Creator</th>
<th>Modify / Saved AS UserInfo Username</th>
<th>MetaData Modifier/Contributor</th>
<th>MetaData Date/Time Created</th>
<th>MetaData Date/Time Modified</th>
<th>MetaData Date/Time Printed</th>
<th>MetaData Revision Number</th>
<th>Save History (2000 only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Copied between Fat32 and NTFS volumes. Modified on NTFS volume</td>
<td>test-2007</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>test-2007</td>
<td>Change: Contains the UserInfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:24)</td>
<td>Change: Contains Date/Time When File Is Modified (14:35)</td>
<td>*****</td>
<td></td>
<td>Change: Each Modification Increases Revision by 1 (2)</td>
</tr>
<tr>
<td>Document Modified 3x &amp; Saved 3x</td>
<td>test-2007</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>test-2007</td>
<td>Change: Contains the UserInfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:26)</td>
<td>Change: Contains Date/Time When File Is Lost Modified (14:46)</td>
<td>*****</td>
<td></td>
<td>Change: Each Modification Increases Revision by 1 (4)</td>
</tr>
</tbody>
</table>
# Word Documents Metadata

## Printing Document

<table>
<thead>
<tr>
<th>Action</th>
<th>Create UserInfo Username</th>
<th>MetaData Creator</th>
<th>Modify / Saved AS User Info Username</th>
<th>MetaData Modifier/Contributor</th>
<th>MetaData Date/Time Created</th>
<th>MetaData Date/Time Modified</th>
<th>MetaData Date/Time Printed</th>
<th>MetaData Revision Number</th>
<th>Save History (2000 only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Printed</td>
<td>test-2007</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>*****</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:24)</td>
<td>No Change: Retains Modified Date/Time (14:26)</td>
<td>*****</td>
<td>No Change: Retains Revision # (1)</td>
<td>No Change: Retains file's path (1. user:E:\filename)</td>
</tr>
<tr>
<td>Document Copied between Fat32 and NTFS volumes, Printed on NTFS volume</td>
<td>test-2007</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>*****</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:24)</td>
<td>No Change: Retains Modified Date/Time (14:26)</td>
<td>*****</td>
<td>No Change: Retains Revision # (1)</td>
<td>No Change: Retains file's path (1. user:E:\filename)</td>
</tr>
<tr>
<td>Document Printed by different user</td>
<td>test-2007</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>*****</td>
<td>No Change: Retains the UserInfo Key Username (test-2007)</td>
<td>No Change: Retains Create Date/Time (14:24)</td>
<td>No Change: Retains Modified Date/Time (14:26)</td>
<td>*****</td>
<td>No Change: Retains Revision # (1)</td>
<td>No Change: Retains file's path (1. user:E:\filename)</td>
</tr>
</tbody>
</table>
## Word Documents Metadata

- **Performing Save As to Document**

<table>
<thead>
<tr>
<th>Action</th>
<th>CreateUserInfo Username</th>
<th>MetaData Creator</th>
<th>Modify/SavedASUserInfo Username</th>
<th>MetaDataModifier/Contributor</th>
<th>MetaData Date/Time Created</th>
<th>MetaData Date/Time Modified</th>
<th>MetaData Date/Time Printed</th>
<th>MetaDataRevisionNumber</th>
<th>Save History (2000 only)</th>
</tr>
</thead>
</table>
**Red Flag #1**

Company’s name shouldn’t appear in another’s document

<table>
<thead>
<tr>
<th>Application</th>
<th>Microsoft Office Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>1</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>1</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Title, 1</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td></td>
</tr>
<tr>
<td><strong>Company</strong></td>
<td>CompanyA</td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>2</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>Creator</td>
<td>corey</td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Last Modified By</td>
<td>corey</td>
</tr>
<tr>
<td>Revision Number</td>
<td>1</td>
</tr>
<tr>
<td>Last Printed</td>
<td>2004:09:16 21:02:00Z</td>
</tr>
<tr>
<td>Create Date</td>
<td>2012:06:09 18:05:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2012:06:09 18:05:00Z</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Microsoft Office Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>5</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>1</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Title, 1</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td></td>
</tr>
<tr>
<td><strong>Company</strong></td>
<td>CompanyA</td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>794</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>Creator</td>
<td>corey</td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Last Modified By</td>
<td>corey</td>
</tr>
<tr>
<td>Revision Number</td>
<td>1</td>
</tr>
<tr>
<td>Last Printed</td>
<td>2004:05:29 03:55:00Z</td>
</tr>
<tr>
<td>Create Date</td>
<td>2012:06:10 01:32:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2012:06:10 01:37:00Z</td>
</tr>
</tbody>
</table>
Red Flag #2

Usernames shouldn’t appear in another’s document

CompanyA bake sale flyer.docx

Vendor 1 computer-invoice.docx
Red Flag #3

Creation dates shouldn’t appear in another’s document

Vendor 1  furniture-bid.docx
Vendor 2  furniture-proposal.docx
Red Flag #4

Print dates shouldn’t appear in another’s document

Vendor 1 furniture-bid.docx

Vendor 2 furniture-proposal.docx
**Red Flag #5**

No Metadata when metadata appears in other documents

<table>
<thead>
<tr>
<th>Vendor 3 furniture-bid.docx</th>
<th>Vendor 3 renovation-bid.docx</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>Microsoft Office Word</td>
</tr>
<tr>
<td><strong>Doc Security</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Lines</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Paragraphs</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Scale Crop</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Heading Pairs</strong></td>
<td>Title, 1</td>
</tr>
<tr>
<td><strong>Titles Of Parts</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Manager</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Company</strong></td>
<td>Vendor3</td>
</tr>
<tr>
<td><strong>Links Up To Date</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Characters With Spaces</strong></td>
<td>1136</td>
</tr>
<tr>
<td><strong>Shared Doc</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Hyperlinks Changed</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>App Version</strong></td>
<td>12.0000</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Creator</strong></td>
<td>bill</td>
</tr>
<tr>
<td><strong>Keywords</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Modified By</strong></td>
<td>bill</td>
</tr>
<tr>
<td><strong>Revision Number</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Last Printed</strong></td>
<td>2012:06:10 02:28:00Z</td>
</tr>
<tr>
<td><strong>Create Date</strong></td>
<td>2012:06:10 02:24:00Z</td>
</tr>
<tr>
<td><strong>Modify Date</strong></td>
<td>2012:06:10 02:29:00Z</td>
</tr>
</tbody>
</table>

| **Title**                   |                             |
| **Subject**                 |                             |
| **Creator**                 |                             |
| **Keywords**                |                             |
| **Description**             |                             |
| **Last Modified By**        |                             |
| **Revision Number**         | 1                           |
| **Create Date**             | 2012:06:10 02:57:00Z        |
| **Modify Date**             | 2012:06:10 02:58:00Z        |
| **Template**                | Normal.dotm                 |
| **Total Edit Time**         | 0                           |
| **Pages**                   | 1                           |
| **Words**                   | 177                         |
| **Characters**              | 967                         |
| **Application**             | Microsoft Office Word       |
| **Doc Security**            | None                        |
| **Lines**                   | 8                           |
| **Paragraphs**              | 2                           |
| **Scale Crop**              | No                          |
| **Manager**                 |                             |
| **Company**                 |                             |
| **Links Up To Date**        | No                          |
| **Characters With Spaces**  | 1142                        |
| **Shared Doc**              | No                          |
Red Flags Chart

Document Created
- Wrong creator
- Wrong company
- No metadata when there should be

Document Copied & Modified
- Wrong modifier
- Same create date
- Same print date
- No metadata when there should be
Detection Process In Action

- Suspected Bid Rigging at Company A
Detection Process

- Locate Documents
  - Ask for it
  - Computers
  - Network Shares
  - Email

- Collect Documents
  - Financial documents (Bids, proposals, invoices, receipts)
  - Sample documents (memos, to-do lists, etc.)

- Extract Documents Metadata
  - Extract to spreadsheet or database
  - Cheeky4n6monkey's SquirrelGripper

- Analyze Metadata
  - Red Flags

Reference: [http://cheeky4n6monkey.blogspot.com/2012/05/perl-script-plays-matchmaker-with.html](http://cheeky4n6monkey.blogspot.com/2012/05/perl-script-plays-matchmaker-with.html)
Collect Documents

Mixture of bids, proposal, and random documents
Separate Documents

Separate documents based on company
Extract Metadata

Run SquirrelGripper against each folder

C:\SquirrelGripper>perl squirrelgripper.pl -newdb -db mock.sqlite -case BidRig -tag CompanyA -dir E:\Bid_Rigging_1-Copy\CompanyA
squirrelgripper.pl v2012.05.24
E:\Bid_Rigging_1-Copy\CompanyA is an absolute path
Directory entry for processing = E:\Bid_Rigging_1-Copy\CompanyA

Now processing E:\Bid_Rigging_1-Copy\CompanyA\bake sale flyer.docx
E:\Bid_Rigging_1-Copy\CompanyA\bake sale flyer.docx inserted into FileIndex table
E:\Bid_Rigging_1-Copy\CompanyA\bake sale flyer.docx inserted into DOCXFiles table

Now processing E:\Bid_Rigging_1-Copy\CompanyA\flooring-proposal.docx
E:\Bid_Rigging_1-Copy\CompanyA\flooring-proposal.docx inserted into FileIndex table
E:\Bid_Rigging_1-Copy\CompanyA\flooring-proposal.docx inserted into DOCXFiles table

Now processing E:\Bid_Rigging_1-Copy\CompanyA\Furniture-proposal.docx
E:\Bid_Rigging_1-Copy\CompanyA\Furniture-proposal.docx inserted into FileIndex table
E:\Bid_Rigging_1-Copy\CompanyA\Furniture-proposal.docx inserted into DOCXFiles table

Now processing E:\Bid_Rigging_1-Copy\CompanyA\renovation-proposal.docx
E:\Bid_Rigging_1-Copy\CompanyA\renovation-proposal.docx inserted into FileIndex table
E:\Bid_Rigging_1-Copy\CompanyA\renovation-proposal.docx inserted into DOCXFiles table
Extract Metadata

Metadata in SquirrelGripper’s SQLite Database

<table>
<thead>
<tr>
<th>rowid</th>
<th>AbsFileName</th>
<th>Creator</th>
<th>LastModifiedBy</th>
<th>CreateDate</th>
<th>ModifyDate</th>
<th>FileType</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>E\Bid_Rigging_1-Copy\CompanyA\bake sale flyer.docx</td>
<td>corey</td>
<td>corey</td>
<td>2012-06-09 18:05:00</td>
<td>2012-06-09 18:05:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>2</td>
<td>E\Bid_Rigging_1-Copy\CompanyA\flooring-proposal.docx</td>
<td>corey</td>
<td>corey</td>
<td>2012-06-10 01:59:00</td>
<td>2012-06-10 01:59:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>3</td>
<td>E\Bid_Rigging_1-Copy\CompanyA\furniture-proposal.docx</td>
<td>corey</td>
<td>corey</td>
<td>2012-06-10 01:39:00</td>
<td>2012-06-10 01:57:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>4</td>
<td>E\Bid_Rigging_1-Copy\CompanyA\renovation-proposal.docx</td>
<td>corey</td>
<td>corey</td>
<td>2012-06-10 01:57:00</td>
<td>2012-06-10 01:58:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>5</td>
<td>E\Bid_Rigging_1-Copy\Vendor1\vendor1-flooring-bid.docx</td>
<td>jdoe</td>
<td>jdoe</td>
<td>2012-06-10 02:09:00</td>
<td>2012-06-10 02:09:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>6</td>
<td>E\Bid_Rigging_1-Copy\Vendor1\vendor1-furniture-bid.docx</td>
<td>jdoe</td>
<td>jdoe</td>
<td>2012-06-10 02:03:00</td>
<td>2012-06-10 02:07:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>7</td>
<td>E\Bid_Rigging_1-Copy\Vendor1\vendor1-renovation-bid.docx</td>
<td>jdoe</td>
<td>jdoe</td>
<td>2012-06-10 02:08:00</td>
<td>2012-06-10 02:08:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>8</td>
<td>E\Bid_Rigging_1-Copy\Vendor2\vendor2-flooring-bid.docx</td>
<td>dsmith</td>
<td>dsmith</td>
<td>2012-06-10 02:14:00</td>
<td>2012-06-10 02:34:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>9</td>
<td>E\Bid_Rigging_1-Copy\Vendor2\vendor2-furniture-bid.docx</td>
<td>dsmith</td>
<td>dsmith</td>
<td>2012-06-10 02:14:00</td>
<td>2012-06-10 02:17:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>10</td>
<td>E\Bid_Rigging_1-Copy\Vendor2\vendor2-renovation-bid.docx</td>
<td>dsmith</td>
<td>dsmith</td>
<td>2012-06-10 02:19:00</td>
<td>2012-06-10 02:19:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>11</td>
<td>E\Bid_Rigging_1-Copy\Vendor3\vendor3-flooring-bid.docx</td>
<td>bill</td>
<td>corey</td>
<td>2012-06-10 02:24:00</td>
<td>2012-06-10 02:32:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>12</td>
<td>E\Bid_Rigging_1-Copy\Vendor3\vendor3-furniture-bid.docx</td>
<td>bill</td>
<td>bill</td>
<td>2012-06-10 02:24:00</td>
<td>2012-06-10 02:29:00</td>
<td>DOCX</td>
</tr>
<tr>
<td>13</td>
<td>E\Bid_Rigging_1-Copy\Vendor3\vendor3-renovation-bid.docx</td>
<td>bill</td>
<td>bill</td>
<td>2012-06-10 02:30:00</td>
<td>2012-06-10 02:30:00</td>
<td>DOCX</td>
</tr>
</tbody>
</table>
## Analyze Metadata

### Suspicious Document #1

**Company A flooring-proposal.docx**

<table>
<thead>
<tr>
<th>Application</th>
<th>Microsoft Office Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>4</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>1</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Title, 1</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>CompanyA</td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>626</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td><strong>Creator</strong></td>
<td>corey</td>
</tr>
<tr>
<td><strong>Keywords</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Modified By</strong></td>
<td>corey</td>
</tr>
<tr>
<td>Revision Number</td>
<td>3</td>
</tr>
<tr>
<td>Create Date</td>
<td>2012:06:10 01:59:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2012:06:10 01:59:00Z</td>
</tr>
</tbody>
</table>

**Vendor 2 vendor2-flooring-bid.docx**

<table>
<thead>
<tr>
<th>Application</th>
<th>Microsoft Office Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>5</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>1</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Title, 1</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>Vendor2</td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>794</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>Creator</td>
<td>dsmith</td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Modified By</strong></td>
<td>corey</td>
</tr>
<tr>
<td>Revision Number</td>
<td>3</td>
</tr>
<tr>
<td>Last Printed</td>
<td>2004:08:19 21:37:00Z</td>
</tr>
<tr>
<td>Create Date</td>
<td>2012:06:10 02:14:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2012:06:10 02:34:00Z</td>
</tr>
</tbody>
</table>
## Analyze Metadata

### Suspicious Document #2

**Company A flooring-proposal.docx**

<table>
<thead>
<tr>
<th>Application</th>
<th>Microsoft Office Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>4</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>1</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Title, 1</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>CompanyA</td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>626</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td><strong>Creator</strong></td>
<td>corey</td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Modified By</strong></td>
<td>corey</td>
</tr>
<tr>
<td>Revision Number</td>
<td>3</td>
</tr>
<tr>
<td>Create Date</td>
<td>2012:06:10 01:59:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2012:06:10 01:59:00Z</td>
</tr>
</tbody>
</table>

**Vendor 3 vendor3-flooring-bid.docx**

<table>
<thead>
<tr>
<th>Application</th>
<th>Microsoft Office Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>8</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>2</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Title, 1</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>Vendor3</td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>1138</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td><strong>Creator</strong></td>
<td>bill</td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Last Modified By</strong></td>
<td>corey</td>
</tr>
<tr>
<td>Revision Number</td>
<td>2</td>
</tr>
<tr>
<td>Last Printed</td>
<td>2012:06:10 02:28:00Z</td>
</tr>
<tr>
<td>Create Date</td>
<td>2012:06:10 02:24:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2012:06:10 02:32:00Z</td>
</tr>
</tbody>
</table>
What’s Next

More Information

- **Paper**
  - More detail about the frauds, technique, and guidelines
  - More useful for DFIR, auditors, and financial investigators

Automation

- **Fraud-doc.pl**
  - Automates identifying fraudulent documents
  - Query script for SquirrelGripper’s database
No Time For
Helm of Clear Thinking
Pauldrons of Pelican Strength
Dongle of Justice
Linux Leggards
Pay no attention to the data behind the curtain...
Well, King Louis...
it looks like we’re not just looking for MAC dates anymore.
NEW SHOES!!
Gleeda the Good Owl
I got the data!
A
Happy, Cheeky Monkey
Test ALL the data!
Known Values in Test Data

Multiple Tools

Validate Results

Run

Mimic Analysis Machine

Multiple Data Sets

Reasons to Share

Recognition/Networking

Karma (the good kind)

You can share by writing a blog, article or whitepaper; providing constructive comments on the work of others; participating in listservs or discussions on twitter; contributing to knowledge repositories...the possibilities are endless!

Contact

Creator(s)

Other End Users

Review

Documentation

Code

Knowledge Repositories

Research

Test

Share

BY MELIA KELLEY 06/2012
EMAIL: MELIA.KELLEY@FADV.COM
PLEASE CONTACT WITH QUESTIONS, UPDATES, OR SUGGESTIONS.
I'm done!
Title Page
Table of Contents
Executive Summary
Objectives
Evidence Analyzed
Methodology
Relevant Findings
Conclusions
Signature
Exhibits

Timeline (Often graphic)
Malware
Documents of Interest
Software of Note
USB Devices
Etc...

Create a Template –
Include “Draft” in header, footer or watermark until finalized.
Seriously, what are you waiting for? If you don’t have a template, GO MAKE ONE. I’ll wait.

Include Analysis –
What does it mean?

Useful phrases:
"It is my professional opinion..."
"The evidence indicates...“
“Based upon a forensic examination, I have determined the following...”

Don’t Procrastinate -
Start the report before you even begin the exam!
You’ll thank me later.

EXHIBITS C thru ?-
Data & documents referenced but not included in body of report.

Curriculum Vitae – Exhibit A
Chain of Custody – Exhibit B

BY MELIA KELLEY 05/2012
EMAIL: MELIA.KELLEY@FADV.COM
PLEASE CONTACT WITH QUESTIONS, UPDATES, OR SUGGESTIONS.
Helmet of Problem Solving
Spaulders of Specialized Coding
Dongle of Justice
Leggings of Great Paths
The Analytic That Changed My Life: Who are We Talking To?

Tim Ray
SANS 2012
Austin, TX
Context

- LYNXeon is our tool for network data analysis.
- Designed as a framework to run analytics.
- An analytic in LYNXeon is a set of search parameters for a database query.
  - Example: Show me all traffic from this IP address.
- The base analytics are good for situational awareness and some hunting for incidents.
- The Air Force likes it!
Context Continued: Behavioral Analysis

- Hunting, rather than monitoring.
- No signatures.
- Takes a human with knowledge of the network to see the patterns.
- Much more fun than watching alerts!
The Challenge

- We get our first quasi-commercial POC (proof of concept).
- We show them many things about their network they never knew!
- We work on workflow integration.
- They ask for a new analytic:
  - “Wouldn’t it be great if we could take a known bad IP, find out who in our network has talked to it, then take that group of hosts and see who they all talked to?
- We think this is cool... but we’ve not done it before.
Picture Time!

BAD HOST

INTERNAL HOSTS

EVEN WORSE HOSTS
Bad Host! Bad! No Cookie!

- Easy to expand around a bad external host.
- That gets you everything internal it talked to.
- Next step is tricky.
- Take each of those internal hosts and expand all external...
- Client Crash! (Hey, billions of records! Give me a break!)
Why Are We Doing This?

- Typical advanced threat might use three hosts:
  - One compromised web host for the attack
  - One dropper for the initial file
  - One C&C for the big payload and all subsequent traffic.

- Customer asked for it!

- Streamlined workflow: We can do this with one button, rather than a whole lot of command line work.

- There can be wide temporal separation between the initial compromise and the subsequent communication.
What are we doing again?

- Initial condition: Internal machine connected with known bad external host.
- First search: What other internal hosts talked to that external host?
- Second Search: For those internal hosts, what OTHER external hosts did they all (or most of them) talk to?
- Post search: Clean up known good sites.
End Result: An Analytic

- Does the searches as explained above.
- Has whitelisting built in (see below).
- Does it in one click.
- Displays it graphically.
Caveats

- Google, Akamai and Facebook will come up quite a bit.
- Create a whitelist for sites you know everyone talks to.
- What is left might be interesting.
- What to look for?
  - Rented space (Amazon, etc.).
  - Common ISPs.
  - One connection ever per host, with a download.
  - Subsequent beaconing from internal hosts.
Why Did This Change Your Life?

- Reiterated the value of customer engagement.
- Taught us to do something new.
- Spawned a whole range of thinking about second and third order analytics that is still paying off today.
- Showed us the versatility and power of LYNXeon in a new way.
Questions & Discussion

For future questions, contact:
Tim Ray
Security Analyst
21CT
tray@21ct.com
What are Shellbags?

• Registry values used to track a user’s display preferences such as windows size/format/icon & position for Windows Explorer

• Contains full paths of files/folders as they existed when the user viewed them in Explorer
  • Local/Network/Removable drive file/folder paths
  • Contains snapshot of Modified/Accessed/Created time/datestamps of file/folder at time of viewing
Importance of Shellbags

- Evidence of File/Folder Existence after Deletion
- Evidence of File/Folder Existence on Removable Devices
- Evidence of the User Viewing the File/Folder via Windows Explorer

Unauthorized Object Access

Proprietary Data Theft

ATTACKER’S RDP ACTIVITY
Where to find Shellbags

For Windows XP:

C:\Documents and Settings\<username>\NTUser.dat

Look at the following Registry Keys:

NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU
NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags
Where to find Shellbags

For Windows 7:

C:\Users\<username>\AppData\Local\Microsoft\Windows\UsrClass.dat
C:\Users\<username>\NTUser.dat

Look at the following UsrClass Registry Keys:

\LocalSettings\Software\Microsoft\Windows\Shell\Bags
\LocalSettings\Software\Microsoft\Windows\Shell\BagMRU

\Wow6432Node\LocalSettings\Software\Microsoft\Windows\Shell\Bags
\Wow6432Node\LocalSettings\Software\Microsoft\Windows\Shell\BagMRU
BagMRU – tree-like structure that mirrors the file system
  • Provides full file paths
  • “NodeSlot” corresponds to the Bag

Bag – contains file/folder metadata
  • Filename (8.3, unicode)
  • Modified Time/datestamp of Bag Key
  • Snapshot of Modified, Accessed and Created Time/datestamps of subject file
Shellbags

\Software\Microsoft\Windows\Shell\BagMRU

- Shell
  - BagMRU
    - 0
      - 0
        - Desktop
      - 1
        - Desktop/E:\
        - Desktop/E:\collection
        - Desktop/E:\happysolver201_installer.zip
      - 1
        - Desktop/C:\
        - Desktop/C:\New folder
        - Desktop/C:\Collection
        - Desktop/C:\Users
        - Desktop/C:\Program Files
        - Desktop/C:\Windows
Shellbags

\Software\Microsoft\Windows\Shell\BagMRU

![Diagram of Shellbags folder structure]

- BagMRU
  - 0 → Desktop
  - 0 → Desktop/E:\
  - 0 → Desktop/E:\collection

- Registry snapshot showing:
  - Value: NodeSlot, Type: REG_DWORD, Data: 0x0000002
  - Value: MRUListEx, Type: REG_BINARY, Data: FF FF FF FF
Bag – contains the details of the file/folder viewed
• Filename (8.3, unicode)
• Modified Time/Datestamp of Bag Key
• Snapshot of Created & Modified Time/Datestamps of subject file
Closed-source CLI shellbag parser

- Available as a free download for non-commercial, personal use
- Outputs to default format (pipe delimited), csv & bodyfile format
- Can parse live registry hives or offline registry files
- New feature: Slack Space Parsing (-inc_slack)

<table>
<thead>
<tr>
<th>Windows ShellBag Parser (sbag)</th>
<th>32-bit Version</th>
<th>64-bit Version</th>
<th>MD5/SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows: sbag32.v.0.22.win.zip</td>
<td>sbag64.v.0.22.win.zip</td>
<td>md5/SHA1</td>
<td></td>
</tr>
<tr>
<td>Linux: sbag32.v.0.22.lin.tar.gz*</td>
<td>sbag64.v.0.22.lin.tar.gz</td>
<td>md5/SHA1</td>
<td></td>
</tr>
<tr>
<td>Mac OS X: sbag.v.0.22.osx.tar.gz</td>
<td>sbag.v.0.22.osx.tar.gz</td>
<td>md5/SHA1</td>
<td></td>
</tr>
</tbody>
</table>
### TZWorks Sbag Parser

C:\>sbad usrclass.dat –csv > usrclass_output.csv

<table>
<thead>
<tr>
<th>regdate</th>
<th>regtime[UTC]</th>
<th>moddate</th>
<th>mtme [UTC]</th>
<th>accessdate</th>
<th>atime [UTC]</th>
<th>ctime [UTC]</th>
<th>type</th>
<th>bag</th>
<th>full path</th>
<th>source subkey/value name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/27/2011</td>
<td>17:41:09.580</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 1</td>
<td>Desktop|CLSID_MyComputer|EA</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>16:53:24.903</td>
<td>04/13/2011</td>
<td>18:54:58.000</td>
<td>04/13/2011</td>
<td>07:00:00.000</td>
<td>04/13/2011</td>
<td>19:10:20.000</td>
<td>dir 2</td>
<td>Desktop|CLSID_MyComputer|E\collection\</td>
<td>Source subkey/value name</td>
</tr>
<tr>
<td>4/13/2011</td>
<td>16:53:24.903</td>
<td>04/13/2011</td>
<td>18:53:46.000</td>
<td>04/13/2011</td>
<td>07:00:00.000</td>
<td>04/13/2011</td>
<td>19:09:56.000</td>
<td>dir 6</td>
<td>Desktop|CLSID_MyComputer|HappySolver210_win_installer.zip</td>
<td>Source subkey/value name</td>
</tr>
<tr>
<td>4/27/2011</td>
<td>17:41:09.580</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 19</td>
<td>Desktop|CLSID_MyComputer|F\</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/14/2011</td>
<td>17:10:57.332</td>
<td>04/13/2011</td>
<td>20:27:46.000</td>
<td>04/13/2011</td>
<td>07:00:00.000</td>
<td>04/13/2011</td>
<td>20:27:46.000</td>
<td>dir 20</td>
<td>Desktop|CLSID_MyComputer|Imager_Lite\</td>
<td>Source subkey/value name</td>
</tr>
<tr>
<td>4/27/2011</td>
<td>16:58:10.384</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 10</td>
<td>Desktop|CLSID_UserLibraries\</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/27/2011</td>
<td>17:41:04.069</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 7</td>
<td>Desktop|CLSID_UserLibraries\</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/27/2011</td>
<td>17:40:09.490</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 9</td>
<td>Desktop|CLSID_UserFiles\</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/15/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 32</td>
<td>Desktop|CLSID_UserFiles\</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/15/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 36</td>
<td>Desktop|CLSID_UserFiles|blueprints.search-ms</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 35</td>
<td>Desktop|CLSID_UserFiles|calculator.search-ma</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 36</td>
<td>Desktop|CLSID_UserFiles|blueprints.search-ms</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 35</td>
<td>Desktop|CLSID_UserFiles|calculator.search-ma</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 28</td>
<td>Desktop|CLSID_UserFiles|HappyCube.searchConnector-ms</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 29</td>
<td>Desktop|CLSID_UserFiles|HappyCube.searchConnector-ms</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 28</td>
<td>Desktop|CLSID_UserFiles|HappyCube.searchConnector-ms</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
<tr>
<td>4/13/2011</td>
<td>17:33:24.146</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>dir 29</td>
<td>Desktop|CLSID_UserFiles|HappyCube.searchConnector-ms</td>
<td>Source subkey/value name</td>
<td></td>
</tr>
</tbody>
</table>
TZWorks Sbag Parser

C:\>sbag usrclass.dat –csv > usrclass_output.csv

<table>
<thead>
<tr>
<th>type</th>
<th>bag</th>
<th>full path</th>
<th>source subkey/value name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td>1</td>
<td>Desktop{CLSID_MyComputer}\E:\</td>
<td>Shell\BagMRU\0\0</td>
</tr>
<tr>
<td>dir</td>
<td>2</td>
<td>Desktop{CLSID_MyComputer}\E:\collection\</td>
<td>Shell\BagMRU\0\0\0</td>
</tr>
<tr>
<td>file</td>
<td>6</td>
<td>Desktop{CLSID_MyComputer}\E:\happysolver\</td>
<td>Shell\BagMRU\0\0\1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>regdate</th>
<th>regtime[UTC]</th>
<th>mod date</th>
<th>mtime [UTC]</th>
<th>accessdate</th>
<th>atime [UTC]</th>
<th>createdate</th>
<th>ctime [UTC]</th>
</tr>
</thead>
</table>
Shown above: MiTec Windows Registry Recovery Tool
### Case Studies

**Unauthorized Access of Other Employees’ Home Folders**

<table>
<thead>
<tr>
<th>bag</th>
<th>key</th>
<th>moddate</th>
<th>mtime</th>
<th>full path</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>04/06/2012</td>
<td>20:44:20.870</td>
<td>Desktop{CLSID_MyComputer}\C:\Users\rblume\Desktop\</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>04/10/2012</td>
<td>16:51:30.804</td>
<td>Desktop{CLSID_MyComputer}\E:\</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>04/10/2012</td>
<td>16:51:30.804</td>
<td>Desktop{CLSID_MyComputer}\Z:\</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>04/10/2012</td>
<td>12:01:43.297</td>
<td>Desktop{CLSID_MyComputer}\Z:\Profiles\</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>04/10/2012</td>
<td>12:00:09.575</td>
<td>Desktop{CLSID_MyComputer}\Z:\Profiles\azapple\</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>04/10/2012</td>
<td>12:00:09.575</td>
<td>Desktop{CLSID_MyComputer}\Z:\Profiles\jwalker\</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>04/10/2012</td>
<td>12:00:09.575</td>
<td>Desktop{CLSID_MyComputer}\Z:\Profiles\pturner\</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>04/10/2012</td>
<td>12:01:43.297</td>
<td>Desktop{CLSID_MyComputer}\Z:\New folder\</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>04/10/2012</td>
<td>12:01:43.297</td>
<td>Desktop{CLSID_MyComputer}\Z:\Backup_Battlecade\</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>04/10/2012</td>
<td>12:01:43.297</td>
<td>Desktop{031e4825-7b94-4dc3-b131-e946b44c8dd5}\</td>
<td></td>
</tr>
</tbody>
</table>
# Case Studies

Proprietary Data Located on Removable Device

<table>
<thead>
<tr>
<th>mod date</th>
<th>mtime [UTC]</th>
<th>bag</th>
<th>full path</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/13/2011</td>
<td>16:50:24.000</td>
<td>3</td>
<td>Desktop{CLSID_MyComputer}\C:\</td>
</tr>
<tr>
<td>04/14/2011</td>
<td>15:43:52.000</td>
<td>5</td>
<td>Desktop{CLSID_MyComputer}\C:\Collection\</td>
</tr>
<tr>
<td>04/13/2011</td>
<td>16:50:24.000</td>
<td>43</td>
<td>Desktop{CLSID_MyComputer}\C:\Collection\</td>
</tr>
<tr>
<td>04/13/2011</td>
<td>16:52:52.000</td>
<td>4</td>
<td>Desktop{CLSID_MyComputer}\C:\New folder\</td>
</tr>
<tr>
<td>04/13/2011</td>
<td>16:52:52.000</td>
<td>44</td>
<td>Desktop{CLSID_MyComputer}\C:\Program Files\</td>
</tr>
<tr>
<td>04/13/2011</td>
<td>16:52:56.000</td>
<td>11</td>
<td>Desktop{CLSID_MyComputer}\C:\Program Files\Happy Cube Solver\</td>
</tr>
<tr>
<td>04/13/2011</td>
<td>18:54:58.000</td>
<td>1</td>
<td>Desktop{CLSID_MyComputer}\E:\</td>
</tr>
<tr>
<td>04/13/2011</td>
<td>18:53:46.000</td>
<td>2</td>
<td>Desktop{CLSID_MyComputer}\E:\collection\</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>Desktop{CLSID_MyComputer}\E:\happysolver210_win_installer.zip</td>
</tr>
</tbody>
</table>
#SANS360
DFIR Summit 2012!

Hi.. My name is

David
Nides
6 fun facts about me

• Parents put me in Special Ed
• Own a party bus company in Chicago
• I HATE PROGRAMMING!!
• Ninjas NOT Pirates
• Only read one book in my life (seriously)
• Manage global DFIR investigations at KPMG
Log2timeline!

Reviewing log2timeline data sets

Gigabytes and millions of rows

With a tool I created!!!

w00t w00t
Log2timeline-sift >>

Few hundred rows. Sure, No prob!

Me

My first Computer!!

APT!?-

My cat Tony
# Spearphishing Attack SuperTimeline

<table>
<thead>
<tr>
<th>date</th>
<th>time</th>
<th>timezone</th>
<th>MACB</th>
<th>sourcetype</th>
<th>short</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/2/2012</td>
<td>20:32:49</td>
<td>EST/EDT</td>
<td>..C</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/IETIdCache/index.dat</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:32:49</td>
<td>EST/EDT</td>
<td>..C</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/IETIdCache/index.dat</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:32:57</td>
<td>EST/EDT</td>
<td>M.CB</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/Sun/Java</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/deployment.properties</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>..B</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63b75a3e-77699f39.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63b75a3e-77699f39.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63b75a3e-77699f39.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63b75a3e-77699f39.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63b75a3e-77699f39.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:07</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/63b75a3e-77699f39.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:15</td>
<td>EST/EDT</td>
<td>M.CB</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Local Settings/Temp/pkxeyztj98.exe</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:15</td>
<td>EST/EDT</td>
<td>..B</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Local Settings/Temp/pkxeyztj98.exe</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:15</td>
<td>EST/EDT</td>
<td>..B</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Local Settings/Temp/pkxeyztj98.exe</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:16</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/712bc739.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:16</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/712bc739.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:16</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/712bc739.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:16</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/712bc739.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:16</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/712bc739.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:16</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Application Data/Sun/Java/Deployment/cache/6.0/62/712bc739.idx</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:17</td>
<td>EST/EDT</td>
<td>MACB</td>
<td>XP Prefetch</td>
<td>PKXEYITYJ98.EXE-0BCBF29B.pf.PKXEYITYJ98.EXE was executed</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:17</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/Documents and Settings/tdungan/Local Settings/Temp/hyperd_data_tdungan</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:33:27</td>
<td>EST/EDT</td>
<td>M.CB</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/Prefetch/PKXEYITYJ98.EXE-0BCBF29B.pf</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:34:26</td>
<td>EST/EDT</td>
<td>..B</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/system32/dlhost</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:35:10</td>
<td>EST/EDT</td>
<td>M.CB</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/system32/dlhost/svchost.exe</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:35:10</td>
<td>EST/EDT</td>
<td>M.CB</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/system32/dlhost/wincient.reg</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:35:49</td>
<td>EST/EDT</td>
<td>M.C.</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/system32/dlhost</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:36:03</td>
<td>EST/EDT</td>
<td>..B</td>
<td>NTFS $MFT</td>
<td>C:/WINDOWS/Prefetch/REG.EXE-0D2A3F7.pdf</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:37:14</td>
<td>EST/EDT</td>
<td>MACB</td>
<td>SYSTEM key</td>
<td>/ControlSet002/Services/Netman/domain</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:37:14</td>
<td>EST/EDT</td>
<td>MACB</td>
<td>SYSTEM key</td>
<td>/ControlSet001/Services/Netman/domain</td>
</tr>
<tr>
<td>4/2/2012</td>
<td>20:39:24</td>
<td>EST/EDT</td>
<td>MACB</td>
<td>SOFTWARE key</td>
<td>/Microsoft/Windows/CurrentVersion/Run</td>
</tr>
</tbody>
</table>

**Email Received w/Java Applet and Zipped PDF (McAfee Log)**

**Metasploit Activated**

**Files Dropped**

**Beacon Interval Set and Persistence Achieved**
Now let’s try this on a real computer .. (not a test image)..
Log2timeline Test

**Step 1 - Create**

**Source:** 320 GB hard drive (100GB free space)

**CMD:**

```
log2timeline-sift -win7 -z EST5EDT -image
```

**Output:** 8 GB CSV File (~ 8 million rows)

**Step 2 - Filter**

**Filter:**

```
l2t_process -b timeline.csv 01-01-2011-01-01-2012 > filtered.csv
```

**Output:** 4 GB

**Step 3 - Review**

**Result:**

![Essbase Error](image)

Maximum number of rows [65536] exceeded.
Log2timeline does a GREAT job of making timeline data available

BUT

It leaves it up to YOU to review it...
Filtering Limitations

- `I2I_process` requires lots of memory
- `grep` hard
- All filtering removes evidence

Review Limitations

- Lack of tools
- Excel 2003: 65,536 rows
- Excel 2007: 1,048,576 rows

I needed a solution...
Features Completed Part of Phase 1:
- Import log2timeline CSV into DB
- Using GUI
- Filter, Search, Tag, Comment, and Auto-Highlight
- Export CSV reports
- Charting (PoC)

Dependences:
- Python not Perl :-)
- WX
- SQLite3
PoC: Import and Create DB
Source types in Database:

$Recycle.bin, 3
Deleted Registry, 1
EXIF metadata, 300
Event Log, 378655
FileExt key, 586
Firefox, 870
Firefox 3 history, 0
Flash Cookie, 563
Internet Explorer, 8
Map Network Drive, 0
MountPoints2 key, 0
NTFS $MFT, 240994
NTUSER key, 14258
OpenSaveMRU key, 0
PDF Metadata, 223
RecentDocs key, 3
RegEdit key, 484
RunMRU key, 483
SAM key, 4347
SOFTWARE key, 597
SYSTEM key, 96117
Shortcut LNK, 3611
UserAssist key, 3
WMIService Log File, 0
XP Prefetch, 43

Users in Database:

- Administrator [500]
- administrator [500]
- \cek\eapoe
- \cek\chouska
- \cek\nbalbas
- \cek\snitech
- \cke\tim
- Guest [501]
- helpAssistant [1004]
- Mickey White
  5-1-5-18
  5-1-5-19
  5-1-5-20
  5-1-5-21-1604122597-1892060865-2706814591-1005
  5-1-5-21-1604122597-1892060865-2706814591-500
  5-1-5-21-1962615262-1079332702-926709054-1206
  5-1-5-21-1962615262-1079332702-926709054-1389
  5-1-5-21-1962615262-1079332702-926709054-18442
  5-1-5-21-1962615262-1079332702-926709054-23720
  5-1-5-21-1962615262-1079332702-926709054-2471
  5-1-5-21-1962615262-1079332702-926709054-2707

Hosts in Database:

- D3SF95F1
- WINXP755-2
- WINXPWSF077
To do:

- Find time (egoings@kpmg.com), rewrite, optimize Phase 1
- Finish Phase 2 – Automate image mounting and running of log2timeline

Release:

- Open source to private sector & LE will pay 😊
- Soon: [http://code.google.com/p/l2t-tools/](http://code.google.com/p/l2t-tools/)
“Think left and think right and think low and think high. Oh, the thinks you can think up if only you try” – Dr. Seuss
• Thank you for attending!
• Please fill out speaker evaluations on your way out.
• Join us for the DFIR NetGeeking Happy Hour happening now
• Follow us on twitter @sansforensics