Adventures in Disk Image Processing with Open Source Tools

Elizabeth Schweinsberg
bethlogic@gmail.com

Goals

Reduce Time-to-Analysis

- Remove some of the “Hurry Up and Wait”
- After the drive is uploaded, metadata is pulled right away

Replace the analyst with a small shell script

- Computers are faster than people
- And more accurate

Create a base process that is standard

- And not stored in a spreadsheet

Overview

- What are we trying to do?
- What tools did we look at?
- Don’t try this at home
- Don’t take my word for it…


Find the Badness
Inspect File Info
Create a Timeline
Inspect Registry Keys
Run AntiVirus
Check Hash Sets
String Searches

What are we trying to do?

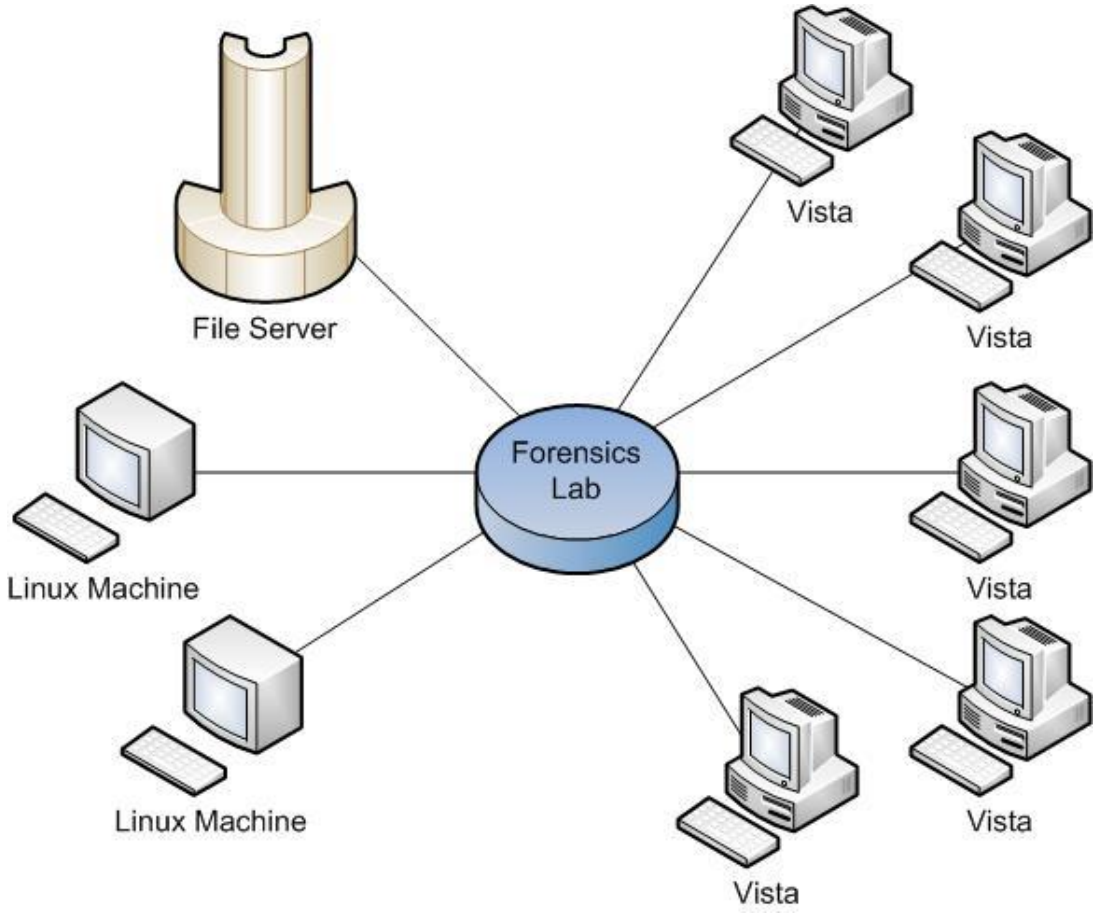
Data Reduction

- 300,000 to 500,000 files on a basic Windows XP system
- 100's of 1000's of Registry Keys and values

Automate

- The base process doesn't change – only the drive image does
- Some scripts and a couple virtual machines go a long way

Our Lab


File Server
Vista
Vista
Forensics Lab
Linux Machine
Vista
Linux Machine
Vista
Vista

What tools were we using?

EnCase and FTK

- Manually creating cases and running hashes
- Timelines only contain file system info

Registry Viewer and RegRipper

- Introduced RegRipper in 2008 with a plug-in list tailored to the order we needed the information

VMWare Images for A/V

- 5 VMs struggling to access the hard drive at the same time

NSRL

- Imported into FTK and EnCase

What do we like?

String Searches

- FTK indexing is (mostly) awesome…

Timeline Analysis

- EnCase has MAC and B (FTK only has MAC)
- TSK and mactimes give you the sorted list

Registry Analysis

- RegRipper floats the important stuff to the top

AntiVirus

- Can be a quick win and helps with mitigation

What don’t we like?

Hash Sets

- The best ones are integrated with big tools
- They don’t tell you when something important *doesn’t* match

Timelines

- Visualization needs some help
- No tool gives the $FILEINFO times in an easy to use format

Registry Analysis

- RegRipper works on one hive at a time

Hurry up and wait

- The system needs to know to go on to the next task when it’s done

What's new in tools?

SuperTimeLine

- Perl scripts for scraping timelines out of all sorts of Windows data files

DFXML

- Create XML files that represent file systems and then use those smaller files to filter and sort files
- Comes with convenient Python interface

Hivex Python Bindings

- The shop that will take this over prefers Python

Digital Forensics Framework

- Basic Forensics tools and easy to extend with C++ or Python
- Used by the winners of the DFRWS Forensics Challenge

What shall we do?

DFXML

- Generate file system information for later use in exporting specific files, hash comparisons, and timeline generation

SuperTimeLine

- STL will traverse any directory, doesn't have to be a mounted drive
- Uses some TSK goodness to make the magic happen
- Still needs some sort of "visualization"

Hivex + RegRipper = Badness?

- Let's take the fundamental ideas of RR and streamline it in Python
- Read lots of books to figure out where badness might be hiding

What shall we do, cont?

Hashes

- Fiwalk/DFXML can calculate the hashes (and run the file command) for later use
- Making HashDig better?

String Searches

- Decouple string searches from FTK by learning Lucene (future release)

AntiVirus

- Let's jump on the Yara bandwagon
- Improved Antivirus and Virtual Machine interactions?

Do we still need EnCase/FTK?

- Maybe – let's create an EnScript to get the case ready for the analyst

Don’t try this at home…

- DFF
- DFXML
- SuperTimeLine
- Registry Fun

Digital Forensic Framework

Not quite ready for primetime

- Calculates hashes one at time
- Working with split images has gotten better…
- Can't save your work – lose hashes and timelines each time

Registry Annoyances

- The Registry is turned into a tree, similar to how EnCase handles it
- On the other hand, can add registry items to the timeline easily

Seems to be aimed at people who want to script

DFXML and Fiwalk

There's been some flux...

- It's Open Source – so it's a work in progress
- While we were working this fiwalk was decoupled from the DFXML – and 3 different versions came out in 5 months

Dependency Purgatory

- Remember the part where our network isn't on the internet?
- Make sure your compile the packages in the right order or it won't work right

What do you do with the XML?

- We still need to invent something to deal with Cross Drive Correlation
- Do you process it DOM or SAX?

SuperTimeLine

Dependency Hell

- packages with even more dependencies
- If only you could leave some out and still get it to “make”

STL is a process

- Wrote a Python wrapper around the 4 steps to generate the timeline
- Used rip.pl with the plugin regtime.pl (new output format) for the registries

Then you have a ginormous CSV file

- At DoD CyberCrime Conference, Rob Lee recommended you use Excel to color code the lines
- Check out my Excel Macro to color code the csv file for you
- Starting with Excel 2007, row limit increased to over 1 Million

Registry Fun

RegRipper

- For Windows written in PERL
- One hive at a time, but could rip.pl in a script to go in the order we wanted

Volatility

- Seriously considered re-working Volatility's memory registry handling for hive files…

RegLookup

- Python bindings for C library – couldn't figure out how to get them to work

Hivex

- Brand New Python Bindings!
- Kinda awkward to use out of the box

Registry Fun, cont.

Random Hivex Bugs

- “L” and “l” mean different things between i386 and 64bit…
- It took 5 trips to get the ml generator installed with dependencies

Hivex needed an interface upgrade

- It would only get one level of the registry structure at a time
- Wrote some statistic generators while I was at it
- Needed access to the Last Written Timestamp
- C program generated XML output, but Python did not

Windows Port?

- Hahahahaha

Registry Fun, cont.

Describing the Registry Checks

- Liked the dictionary in the reglist plugin for Volatility, but will people modify the Python?
- Created an XML schema to describe the checks

Storing the Registry Results

- XML? Which XML format to use?
- Log file like RegRipper? But with less overhead?

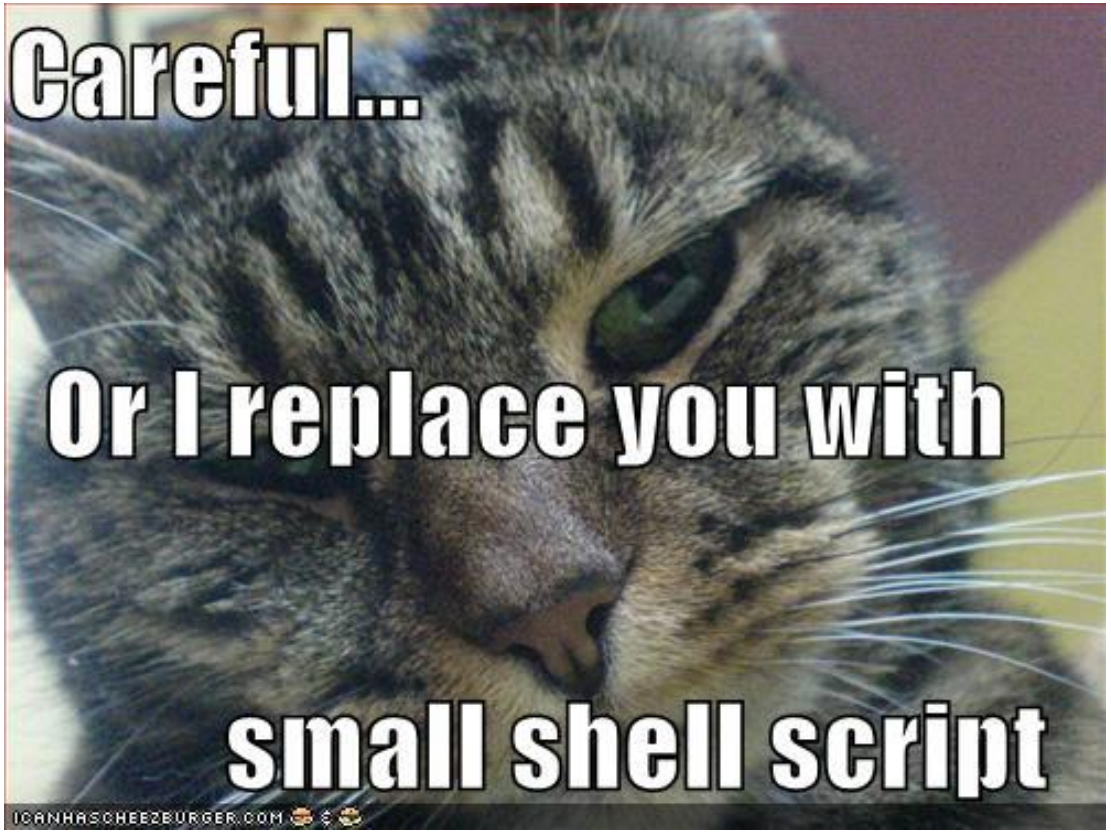
Add the Easy Button

- YMMV, but there are certain conditions we're looking for, so get those highlighted in the output

Don’t take my word for it…

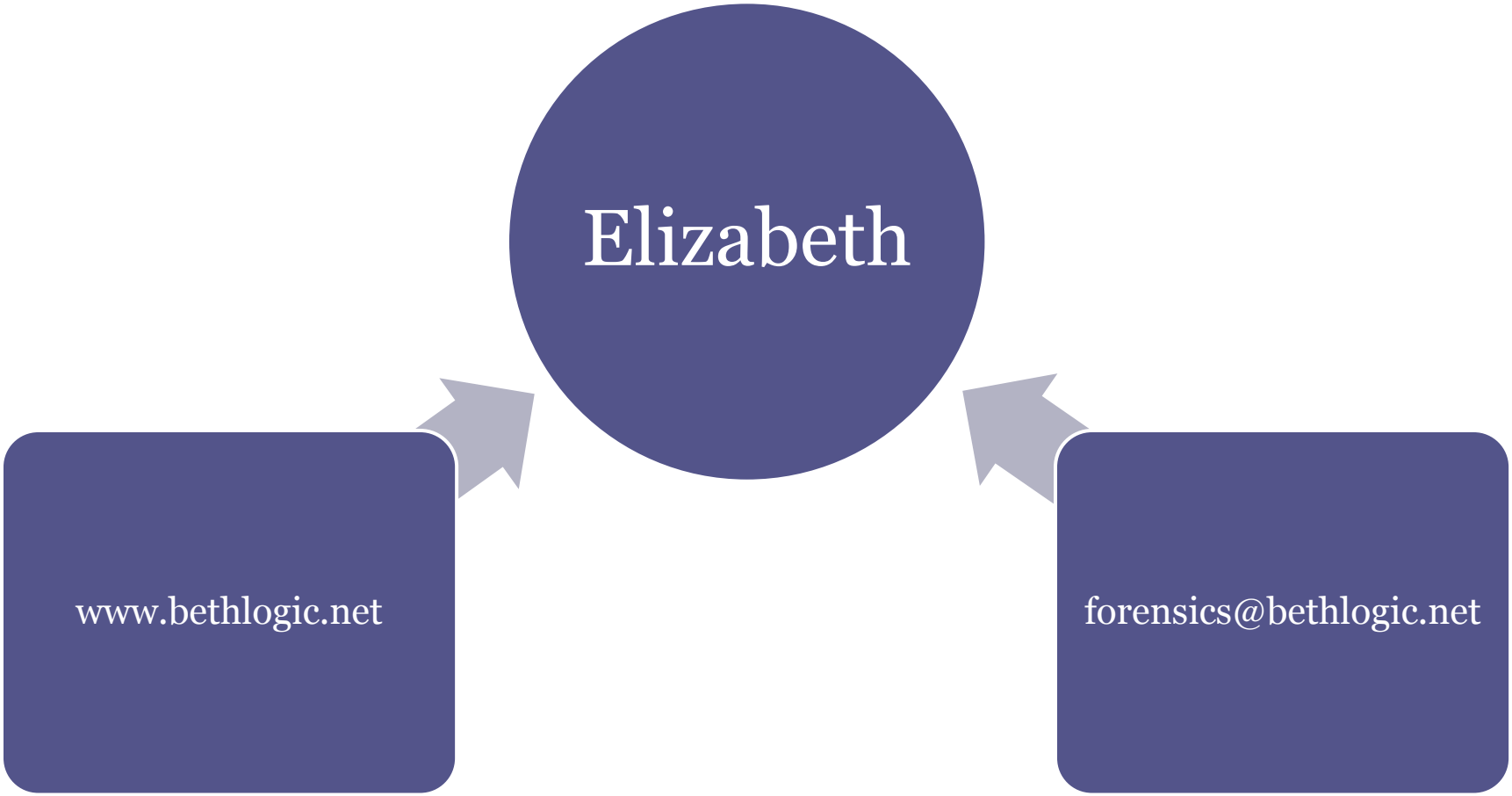
Size	Collect Metadata	Extract All Files	Calculate Hashes
Before using EnCase			
10GB	3:00 (Verify)	20:09 (20GB, 32,767 files)	2:14
After			
10GB	0:17	3:01 (5.1GB, 32,362 files)	3:30

Analyst Testimonial



http://cheezburger.com/View/1019335936

Questions?



References

Windows Forensic Analysis, 2nd Edition

- Harlan Carvey, 2010

Windows Internals, 5th Edition

- Mark Russinovich and David Soloman, 2009

Windows Registry Analysis

- Harlan Carvey, 2011

Dependencies you can count on

Fiwalk: http://afflib.org/

- zlib1g-dev
  - zlib1g
- openssl-dev
  - libssl0.9.8
  - zlib1g
- Libewf: http://sourceforge.net/projects/libewf/files/libewf/
- AffLib: http://afflib.org/
- SleuthKit: http://www.sleuthkit.org/sleuthkit/download.php
- Exiv2: http://www.exiv2.org/

Log2Timeline

- libclass-loader-perl
- libdatetime-perl
  - liblist-moreutils-perl
  - libparams-validate-perl
  - libdatetime-locale-perl
  - libdatetime-timezone-perl
  - libclass-singleton-perl
  - libdatetime-format-strptime-perl
- libdate-manip-perl
  - libyaml-syck-perl
- libnet-pcap-perl
  - Libpcap
- libnetpacket-perl
- libarchive-zip-perl
- libcompress-zlib-perl
- libxml-libxml-perl
  - libxml-namespacesupport-perl
  - libxml-sax-perl
  - libxml2

Log2Timeline, cont.

- libdbi-perl
- libhtml-scrubber-perl
- libimage-exiftool-perl
  - libimage-exif-perl
- libgtk2-perl
  - libglib-perl
- libcarp-assert-perl
- perl-modules
- libdbd-sqlite3-perl
- libdigest-crc-perl
- libversion-perl
- libmodule-build-perl
  - libextutils-parsexs-perl
    - libextutils-cbuilder-perl
  - libyaml-perl
- Data-Hexify-1.00
- Parse-Win32Registry-0.60
- Mac-PropertyList-1.33
- File-Mork-0.3

Hivex

- pod2man
- pod2text
- libxml2
  - libzlib1g
  - libxml-core
- OCaml (if you need to regenerate the bindings)
  - libx11-dev
  - ocaml-base-3.11
    - libx11-6
    - tcl8.5
    - tk8.5
  - ocaml-nox-3.11.2

My Favorite Registry Keys

Name	Key	RegRipper
Services and Drivers	SYSTEM\CurrentControlSet\Services	services (SYS) or svc (SYS)
Svchost Processes	SOFTWARE\Microsoft\Windows NT\CurrentVersion\svchost	svchost(SW)
Scheduled Tasks	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task Scheduler	
	SOFTWARE\Classes\CLSID\{GUID}	
Browser Helper Objects	SOWFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	bho(SW)
Run	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	soft_run(SW)
	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	user_run(NT), user_win(NT)
RunOnce	SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	
	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	

Name	Key	RegRipper
Winlogin	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin	winlogon(NT)
Notify	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Notify	
Execute on Boot	SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute	
Boot Verification	SYSTEM\CurrentControlSet\Control\BootVerificationProgram	
Actions that happen when cmd starts	SOFTWARE\Microsoft\Command Processor\Auto Run	
How files are run	SOFTWARE\Classes\{filetype}\Shell\Open\Command	Cmd_shell(SW)
	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts	Fileexts(SW)
Application Initialization	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	appinitdll(SW)
Terminal Server Connections	SYSTEM\CurrentControlSet\Control\Terminal Server	
Searching on the drive	HKCU\SOFTWARE\Microsoft\Search Assistant\ACMru	Acmru (NT)

Name	Key	RegRipper
Installation time	SOFTWARE\Microsoft\Windows NT\CurrentVersion	winnt_cv(SW) or winver(SW)
Time zone	SYSTEM\CurrentControlSet\Control\TimeZoneInformation	timezone(SYS)
Shutdown Time	SYSTEM\CurrentControlSet\Control\Windows	Shutdown (SYS)
Delete files?	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket	bitbucket(SW), vista_bitbucket(SW)
Disable Last Access	SYSTEM\CurrentControlSet\Control\FileSystem	disablelastaccess(SYS)
Recently Used Applications	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	
	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU	
Firewall Policies	SYSTEM\Services\Shared Access\Parameters\Firewall Policy	Fw_config
Zone Maps	SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\Domain	
Typed URLS	SOFTWARE\Microsoft\Internet Explorer\TypedURLs	typedurls(NT)

Name	Key	RegRipper
Removable Drives	SYSTEM\Mounted Devices	mountdev(SYS)
	SYSTEM\CurrentControlSet\Enumb\USBSTOR	usbstor(SYS)
	SOFTWARE\Microsoft\Windows Portable Devices\Devices	port_dev(SW)
Network Shares	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2	mp2 (SW)
	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	mndmru(SW)
	SYSTEM\CurrentControlSet\Services\Lanmanserver\Shares	shares (SYS)
Recent Users	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	profilelist(SW)
Audit Policies	SECURITY\Policy\PolAdt\Ev	auditpol(SEC)
User Actions	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count	userassist(NT)
	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	runmru(NT)
User Creation	Stored in a binary tool; best done with a tool	samparse(SAM)