Timeline Creation and Analysis by Mark Hallman

Sleuth Kit and Open Source Digital Forensics Conference

McLean, Virginia - June 14,2011

Live DVD

Mark Hallman

Principal, Digital Discovery

Dallas, TX

CHFI, CCE, EnCE, GCFA

Housekeeping

- Please …
  - Mobile devices on silent
  - Step outside to take calls
  - If something is not working for you … speak up
- This is an interactive session
  - Ask questions
  - If you have additional info … please share with the group

Schedule

- 8:30 – 9:30 Into to log2timeline
- 9:30 – 9:45 Break
- 9:45 – 10:45 Timeline analysis
- 10:45 – 11:00 Break
- 11:00 - 12:00 Final hands on exercise
- Lunch will be provided

Acknowledgements

- Thanks to **Kristinn Gudjonsson** for:
  - Creating and Maintaining this awesome tool
  - Reviewing my material for this workshop
- Thanks to **Rob Lee** for:
  - His many contributions to the field of DFIR
  - His encouragement to me in my career
  - His allowing me to use some of his material in this workshop

Why is Timeline Analysis Important?

- Temporal Proximity
  - Comparable to Emergency Medicine's "Golden Hour"
  - What else was happening around that time?
- A form of triage
  - Where do you start an investigation?
  - Focus and shorten investigation time
- Critical info for:
  - Creating the investigation plan
  - Data reduction

Timeline Analysis Challenges

- Historically just file system timestamps
- Many other sources were not integrated because of manual effort
- File system timestamps are easily manipulated
- File system timestamps are not always updated (Win7)

Enter log2timline

- A single tool that can:
  - Parse many sources of temporal artifacts
  - Combine them in a single time
  - Provide basic filtering and searching functions
  - Provide input to other analysis tools
- Has evolved considerably over the past 2 years
- Created by Kristinn Gudjonsson as a SANS GCFA Gold Paper
  - Idea came through conversations with Rob Lee about taking timeline analysis to a new level.
  - *Mastering the Super Timeline with log2timeline*
  - Can download the paper from SANS Reading Room

    http://www.sans.org/reading_room/whitepapers/logging/mastering-super-timeline-log2timeline_33438

Think you know log2timeline?

- Complete new rewrite with version 0.60
- Preprocessor
- Timestomp identification
- Timescanner
  - No longer required
  - Still there if you want to use it
- New utility - l2t_process
  - Date range filter
  - Keyword filter
  - Scatter file creation

Input Modules

Name	Description	Name	Description
apache2_access	Apache2 access log file	**oxml**	Parse the content of an OpenXML document (Office 2007 documents)
apache2_error	Apache2 error log file	**pcap**	PCAP file
chrome	Chrome history file	**pdf**	Parse some of the available PDF document metadata
encase_dirlisting	CSV file that is exported from FTK Imager (dirlisting)	**prefetch**	Parse the content of the Prefetch directory
evt	Windows 2k/XP/2k3 Event Log	**recycler**	Parse the content of the recycle bin directory
evtx	Windows Event Log File (EVTX)	**restore**	Parse the content of the restore point directory
exif	Extract metadata information from files using ExifTool	**safari**	Parse the contents of a Safari History.plist file
ff_bookmark	Firefox bookmark file	**sam**	Parses the SAM registry file
firefox2	Firefox 2 browser history	**security**	Parses the SECURITY registry file
firefox3	Firefox 3 history file	**setupapi**	Parse the content of the SetupAPI log file in Windows XP
ftk_dirlisting	CSV file that is exported from FTK Imager (dirlisting)	**skype_sql**	Skype database
generic_linux	Parse content of Generic Linux logs that start with MMM DD HH:MM:SS	**software**	Parses the SOFTWARE registry file
iehistory	Parse the content of an index.dat file containg IE history	**sol**	.sol (LSO) or a Flash cookie file
iis	IIS W3C log file	**squid**	Squid access log (http_emulate off)
isatxt	ISA text export log file	**syslog**	Linux Syslog log file
jp_ntfs_change	CSV output file from JP (NTFS Change log)	**system**	Parses the SYSTEM registry file
mactime	body file in the mactime format	**tln**	body file in the TLN format
mcafee	log file	**userassist**	Parses the NTUSER.DAT registry file
mft	NTFS MFT file	**volatility**	Volatility output files
mssql_errlog	Parse the content of an ERRORLOG file produced by MS SQL server	**win_link**	Windows shortcut file (or a link file)
ntuser	Parses the NTUSER.DAT registry file	**wmiprov**	Parse the content of the wmiprov log file

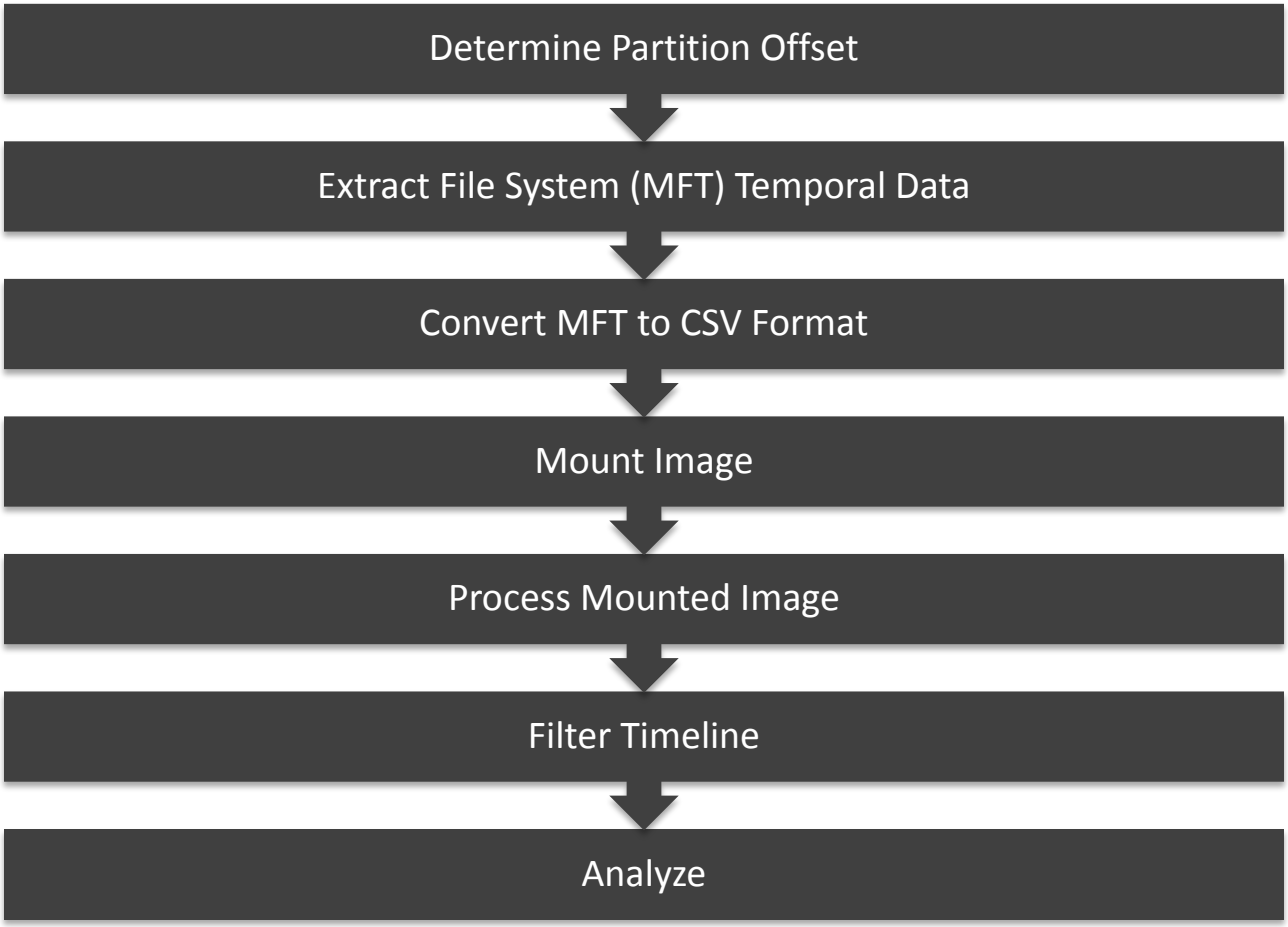
Input Module Lists

List Name	Modules Included
linux	apache2_access, apache2_error, pcap, syslog, generic_linux,
web	chrome, firefox3, firefox2, ff_bookmark, opera, iehistory, iis, safari,
webhist	chrome, firefox3, firefox2, ff_bookmark, opera, iehistory, iis, safari, sol,
win7	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, win_link, xpfirewall, wmiprov, ntuser, software, system,
win7_no_reg	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, ntuser, win_link, xpfirewall, wmiprov,
winvista	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, userassist, win_link, xpfirewall, wmiprov,
winxp	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, setupapi, sol, win_link, xpfirewall, wmiprov, ntuser, software, system,
winxp_no_reg	chrome, evt, exif, ff_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, setupapi, sol, ntuser, win_link, xpfirewall, wmiprov,

Output Formats

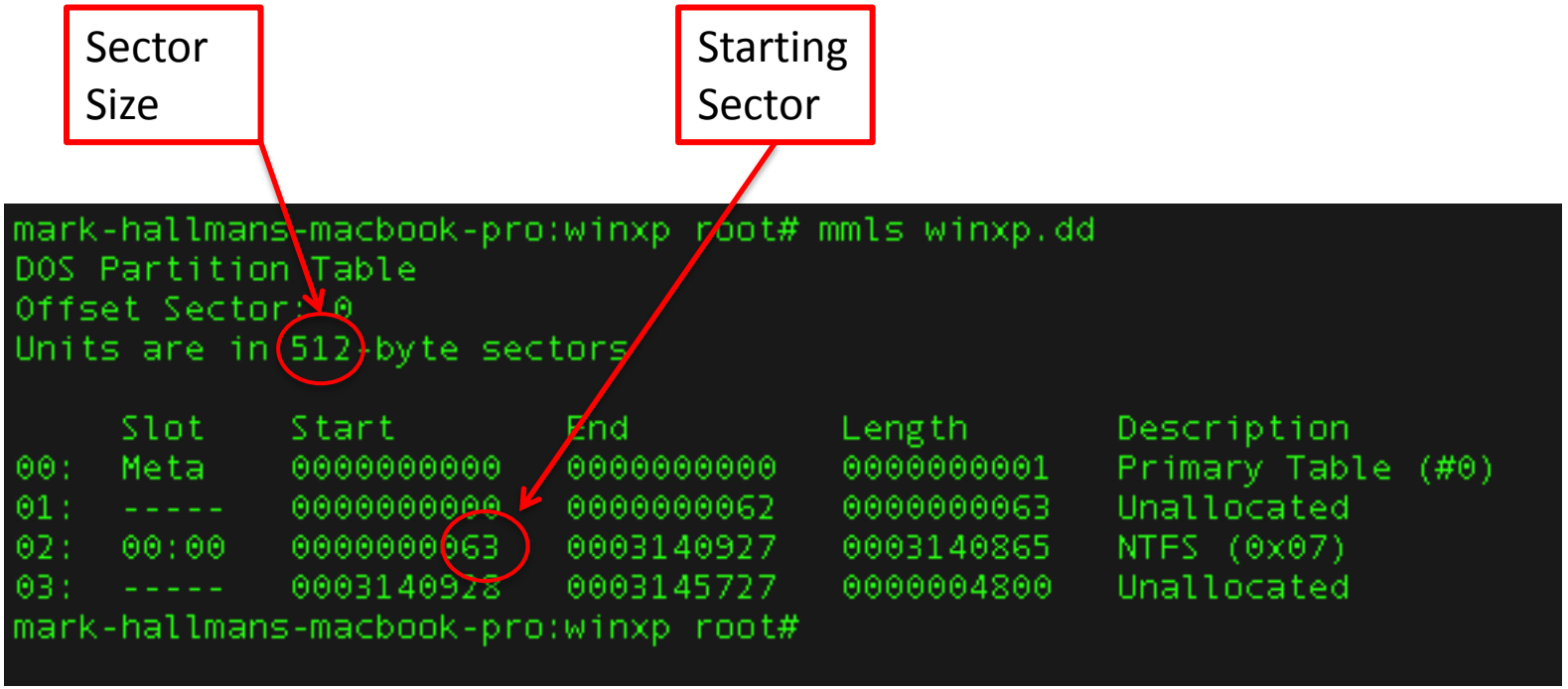
Name	Description
beedocs	tab-delimited file to import into BeeDocs
cef	ArcSight Common Event Format (CEF)
cftl	Output timeline in a XML format that can be read by CFTL
csv	CSV (Comma Separated Value) file
mactime	mactime format
mactime_l	legacy version of the mactime format (version 1.x and 2.x)
simile	Output timeline in a XML format that can be read by a SIMILE widget
sqlite	Output timeline into a SQLite database
tab	TDV (Tab Delimited Value) file
tln	H. Carvey's TLN format
tlnx	H. Carvey's TLN format in XML

Log2timeline – Quick Start



Step 1 – Determine Partition Offset

root# mmls image.dd



Step 2 – Extract File System Data

Performed against your forensic image

```
icat -i raw -f ntfs -o 63 image.dd 0 > image.mft
```

This method, vs. using fls give you both

$FILENAME and $STDINFO timestamps

-i image type

-f file system type

-o file system starting offset in sectors

Step 3 - Convert MFT to CSV Format

log2timeline -f mft -z CST6CDT -m C: image.mft -w timeline.csv

-f log file format to process

-z time zone

-m path prefix

-w output filename (appends to that file)

Step 4 – Mount image

- Log2timeline processes mounted images only

Create mount point directory

mkdir /mnt/analyze

Mount disk image

mount -t ntfs-3g -o ro,nodev,noexec,show_sys_files,loop,offset=32256 image.dd /mnt/analyze

-t file system type

-o options - offset is in bytes (63 x 512 = 32256)

Step 5 – Process Mounted Image

log2timeline -p -r -f winxp -z CST6CDT /mnt/analyze/ -w timeline.csv

-p preprocess flag

-r recursively process input

-f file format to process with (individual or groups)

-z time zone

-w output file name

Step 6 – Filter Timeline

l2t_process –e -b timeline.csv -k keywords.txt MM-DD-YYYY..MM-DD-YYYY

-e exclude timestomping
-b csv timeline file to process
-k key words /search terms to use (one term per line)
mm-dd-yyyy date or date range to include

Hands on Exercise #1

- Three options:
  - LiveDVD
  - Bootable thumb drive
  - Preconfigured Vmware VM
- Thumb drive contains:
  - Winxp.dd
  - Image-004.dd.zip (if we have time)
  - Timeline for Reed Richards
- Winxp.dd
  - IP theft case.
  - Just creating timeline at this point

Timeline Analysis – Where to Start

- This is often an iterative process
- Attempt to identify date range(s)
- Attempt to identify keywords
- Create entire timeline (log2timeline)
- Filter timeline with date range(s) (l2t_process)
- Create timeline using date range(s) and keywords (l2t_process)
- Determine what source types are in the filtered time line (grep)
- Begin review of timelines

l2t_process

- Allows for filtering and searching
  - Date range
  - Keywords
  - Exclude lists
  - White lists (not in the version we have today)
- Similar to mactime
- Basic command
  - l2t_process -e -b timeline.csv MM-DD-YYYY..MM-DD-YYYY

grep to Filter & Search

- Cheat Sheet
  - Examples of grep and awk
  - List of input module string to use as search terms
- What sources are in your timeline?

  # awk –F , '{print $6;}' timeline.csv | grep –v sourcetype |sort | uniq
- Find MountPoints2 entries that reference E Drive

  # grep "MountPoints2 key" timeline.csv | grep –I "E drive"

Source Types

for Filtering and Searching

Apache2 Access Log File	NTFS $MFT	PDF Metadata
Apache2 Error Log File	MSSQL ErrorLog	$st . Prefetch
Chrome History	NTUSER key	$Recycle.bin
Encase Imager FolderPath	$ktype .	$Recycle.bin
Event Log	key	Restore Point
$sys{channel}	$type . key	Safari history
EXIF metadata	FileExts key	SAM key
Firefox	NTUSER key	SECURITY key
Firefox 2	OpenSaveMRU key	SetupAPI Log
Firefox 3 history	Map Network Drive MRU key	Skype History
FTK Imager FolderPath	MountPoints2 key	SOFTWARE key
Generic Linux Log	RecentDocs key	Flash Cookie
Internet Explorer	RunMRU key	Squid access log
IIS Log File	RegEdit key	Linux Syslog Log File
ISA text export	UserAssist key	SYSTEM key
NTFS Change Log	Opera	Shortcut LNK
MACTIME	Open XML Metadata	WMIprov Log file
McAfee AV Log	PCAP file	XP Firewall Log

Timeline Analysis with a Spreadsheet

- Filter with l2t_process then use spreadsheet
  - Hide less used columns
  - Use auto and standard filters
- Two great articles on spreadsheets with log2timeline csv
  - Reviewing Timelines with Excel by Cory Harrell
    - http://journeyintoir.blogspot.com/2010/11/reviewing-timelines-with-excel.html
  - Timeline analysis 201 – Review the timeline by Kristinn Gudjonsson
    - http://blog.kiddaland.net/2011/02/timeline-analysis-201-review-the-timeline/

log2timeline CSV File format

Field	Description
Date	The date of the event, in the format of MM/DD/YYYY
Time	The time of day, expressed in a 24h format, HH:MM:SS
Timezone	the timezone that was used to call the tool with.
MACB	The MACB meaning of the fields, mostly for compatibility with the mactime format.
Source	The short name for the source. All web browser history is for instance WEBHIST, registry entries are REG, simple log files are LOG, etc.
Sourcetype	A slightly more comprehensive description of the source, “Internet Explorer” instead of WEBHIST, “NTUSER.DAT” instead of REG, etc.
Type	The type of the timestamp itself, such as “Last Accessed”, “Last Written” or “Last modified”, etc.
User	The username associated with the entry, if one is available.
Host	The hostname associated with the entry, if one is available.
Short	A short description of the entry, usually contains less text than the full description field.
Desc	The description field, this is where most of the information is stored, the actual parsed description of the entry.
Version	The version number of the timestamp object.
Filename	The filename with the full path of the filename that contained the entry
Inode	The inode number of the file being parsed.
Notes	Some input modules insert additional information in the form of a note, which comes here. Or it can be used during the review by the investigator.
Format	The name of the input module that was used to parse the file.
Extra	Some additional information parsed is joined together and put here.

Hands on Exercise #2

- Working with winxp.dd image
- Familiarize yourself with:
  - Loading timeline csv into a spreadsheet
  - The log2timeline file format
  - Auto and Standard Filtering
- Identify a potentially relevant date range
- Can we prove, using timeline analysis, that anything was copied off this computer?

Timeline Analysis

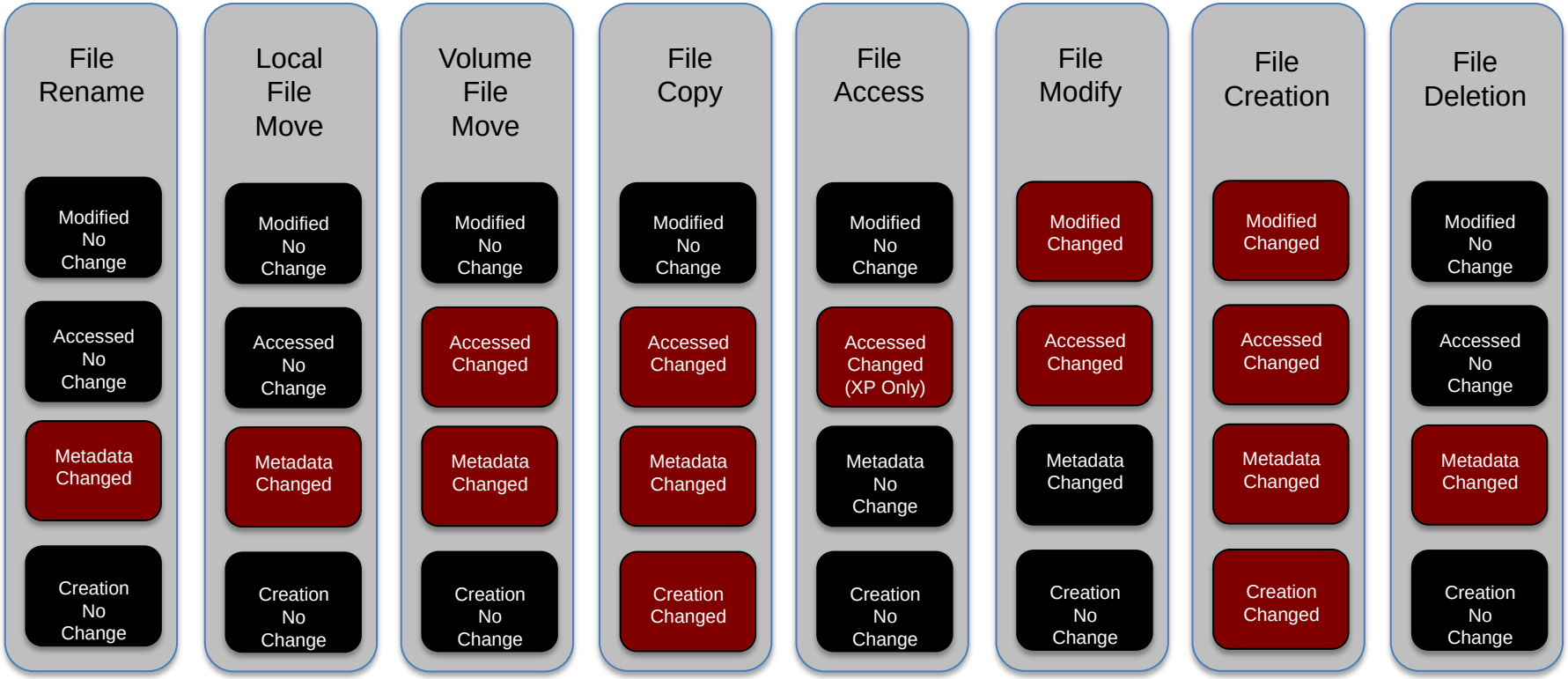
Now that I have all this data …

MACB Interpretation

File System	Time Stored	Time Resolution	M	A	C	B
Ext2/3	Epoch	1 sec since Jan 1, 1970	Modified	Accessed	Inode Changed	
FAT	Local	1-Jan-80	Modified (2 sec)	Accessed (no time component)	N/A	Created (10 ms)
NTFS	UTC	100 ns since Jan 1, 1601	Modified	Accessed	MFT Modified	Created

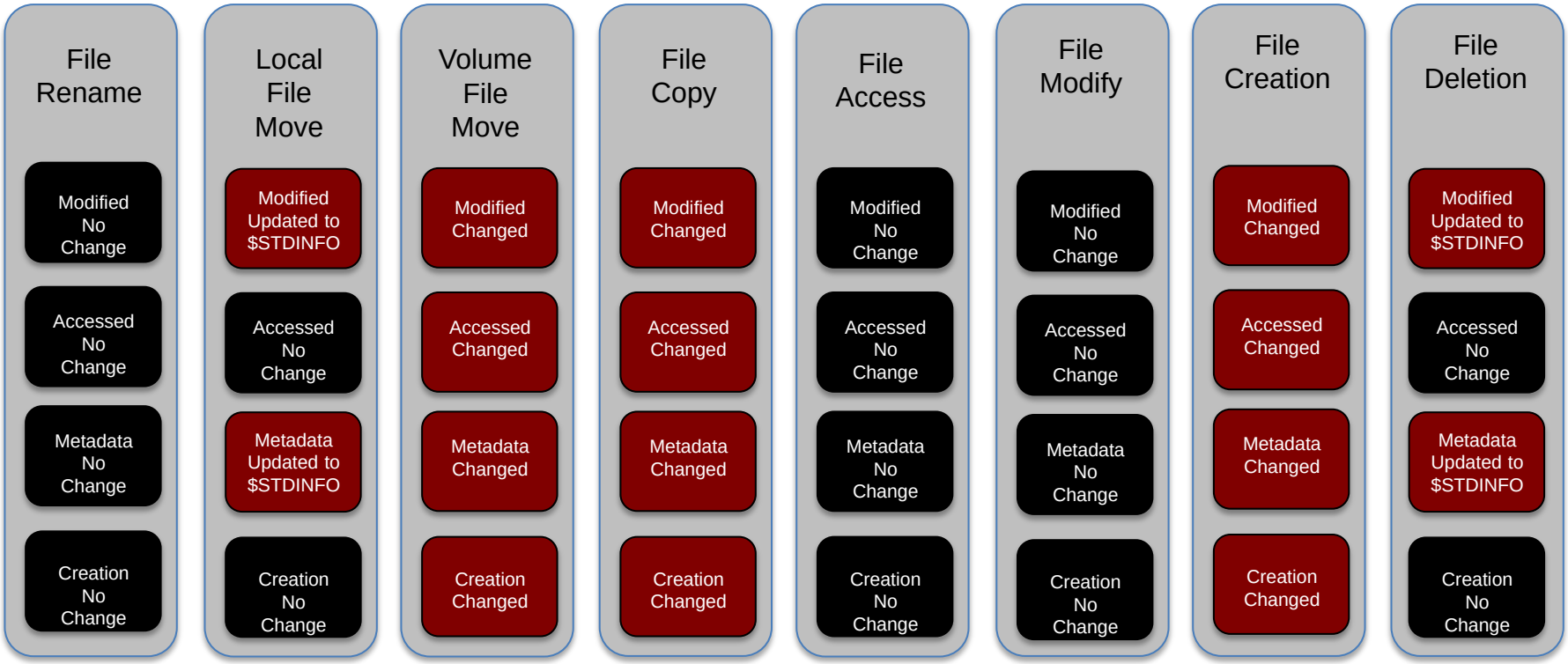
Source Rob Lee (rlee@sans.org) SANS Institute

NTFS Time Rules $STDINFO



Source Rob Lee (rlee@sans.org) SANS Institute

NTFS Time Rules $FILENAME



Source Rob Lee (rlee@sans.org) SANS Institute

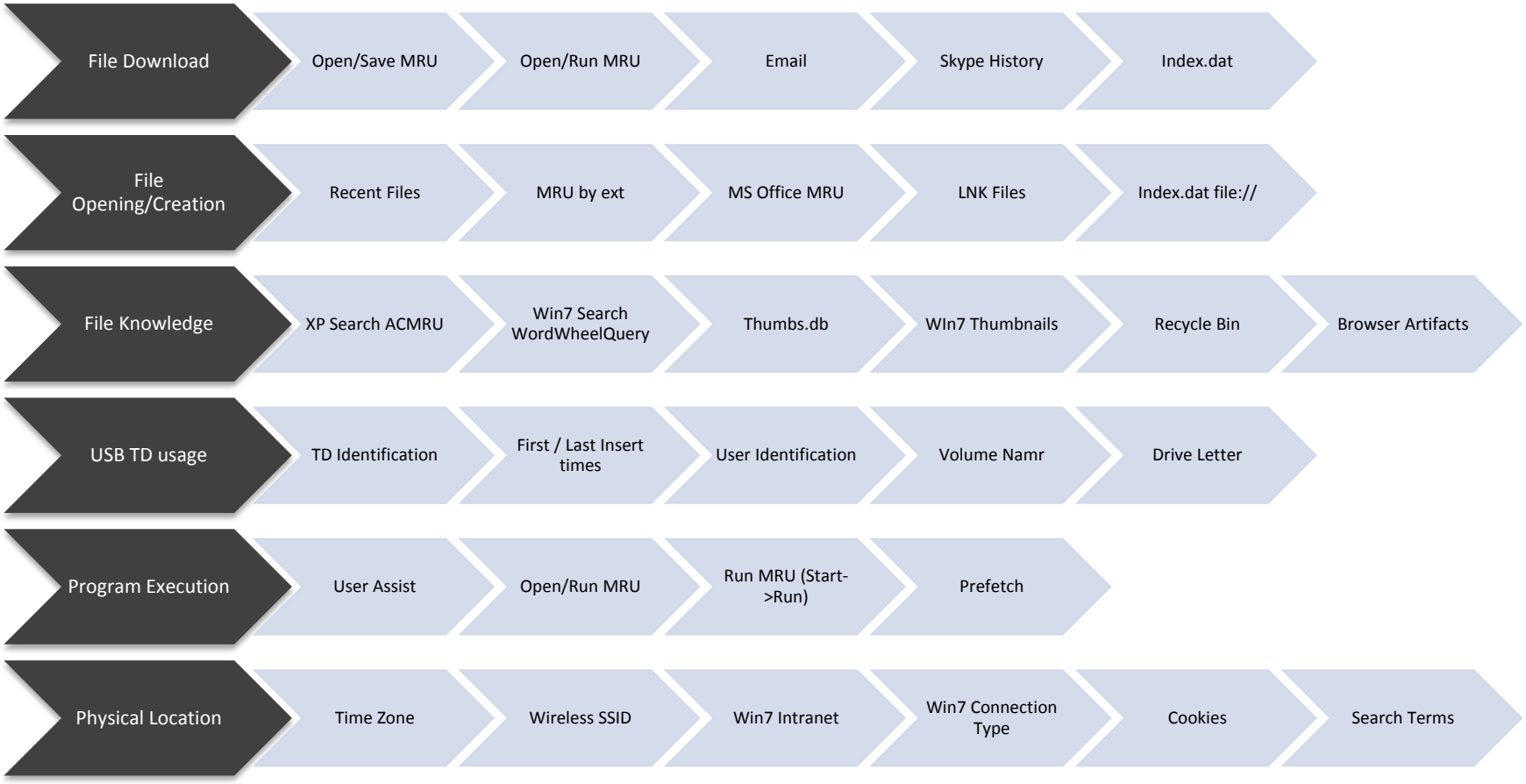
Timestomping tools do NOT change the $FILENAME attributes

Example of Temporal Artifacts

Internet Browser History	• Link clicked on • Entry in history file
Recent Docs	• Last time file / folder opened
Shortcut (LNK) file	• First time file opened • Last time file opened
Recycle Bin	• Time file deleted
UserAssist	• User level program execution
Prefetch	• System wide program execution
USB Activity	• First time inserted • Last time inserted • What user inserted

Source Rob Lee (rlee@sans.org) SANS Institute

Known Evidence Locations



Source Rob Lee (rlee@sans.org) SANS Institute

Hands on Exercise #3

Reed Richards/Carol Danvers Case
Background & Scope

On June 19, 2009 at 7:30 am two dead bodies were discovered by housekeeping in a Caneel Bay hotel room in the St. John's Virgin Islands. A gun was found at the crime scene. The gun as classified as a Glock 9 hand gun.

The deceased male (Reed Richards) was found with two gunshot wounds to the chest. The deceased female (Carol Danvers) was found holding the gun with one gunshot wound to the head.

Reed and Carol travelled to the Virgin Islands the morning of June 15th for a company off-site. Their original plans had them traveling on Sunday June 14, 2009. It is unknown why they took a later flight.

Reed Richards was the CEO of Fantastic Four Enterprise. Carol Danvers was his Executive Assistant. Reed is married to Sue Storm Richards and has two children.

The evidence at the crime scene suggests to local law enforcement that it was a murder / suicide.

A team of digital forensic investigators have been brought in to solve the case. They have been requested to determine if the crime was a murder / suicide. They have also been requested to determine why Carol would want to murder Reed and then commit suicide. The only evidence of Carol's motives might be found on the Richards family laptop that he routinely used at home. This laptop was picked up by the State Police in Massachusetts as Sue Richards was on a girls weekend on the Cape when she was notified of Reed's death. Sue's children were with her parents for the weekend near Baltimore. A suicide note was found at the crime scene explaining Carol's motives.

Source Rob Lee (rlee@sans.org) SANS Institute

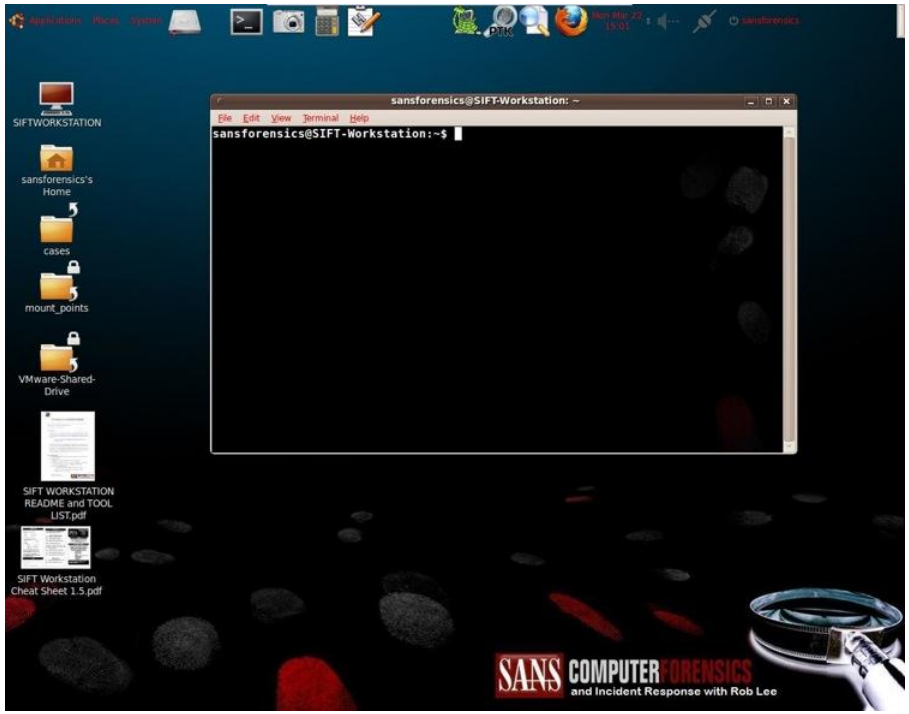
Timeline Visualization

- Visualization Modules
  - SIMILE Widgets
  - CyberForensics Timelab (CFTL)
  - BeeDocs Timeline 3D
- All formats require extensive “massaging” of raw data for effective presentation
- Should be used for reporting and presentation not analysis

Beedocs Timeline 3D Demo

- Best tool I have found
- Krinstinn is working a new input module for csv
  - This will allow “massaged” timelines to be converted to beedocs
- Once timeline is in Beedocs Timeline 3D the presentation is outstanding
- Now for the demo … (separate presentation)

SANS SIFT 2.1 Forensic Workstation



- SANS SIFT 2.0 Now
- SANS SIFT 2.1 Available soon
  - http://computer-forensics.sans.org/community/downloads

- SIFT Workstation 2.0 Capabilities
  - Ability to securely examine raw disks, multiple file systems, evidence formats. Places strict guidelines on how evidence is examined (read-only) verifying that the evidence has not changed

- File system support
  - Windows (MSDOS, FAT, VFAT, NTFS)
  - MAC (HFS)
  - Solaris (UFS)
  - Linux (EXT2/3)
  - Evidence Image Support
  - Expert Witness (E01)
  - RAW (dd)
  - Advanced Forensic Format (AFF)

- Software Includes (partial list)
  - The Sleuth Kit (File system Analysis Tools)
  - log2timeline (Timeline Generation Tool)
  - ssdeep & md5deep (Hashing Tools)
  - Foremost/Scalpel (File Carving)
  - WireShark (Network Forensics)
  - Vinetto (thumbs.db examination)
  - Pasco (IE Web History examination)
  - Rifiuti (Recycle Bin examination)
  - Volatility Framework (Memory Analysis)
  - DFLabs PTK (GUI Front-End for Sleuthkit)
  - Autopsy (GUI Front-End for Sleuthkit)
  - PyFLAG (GUI Log/Disk Examination)

Thanks for Playing