DIGITAL EVIDENCE COLLECTION → ADMINISTRATIVE → WORK PLAN → CASE SETUP → IMAGE INTEGRITY → ANALYSIS PREP → ANALYSIS → INTERPRETATION- REVIEW → REPORTING

## 1. ADMINISTRATIVE STUFF

- Review Policies and Laws
- Chain of Custody form
- Digital Evidence Collection Form
- Consent form (if needed)
- ✓ Evidence Tracked and Stored

## 2. WORK PLAN (docs)

- Review Policies and Laws (if needed)
- Gain understanding of:
  - -Background
  - -If applicable, previous work
  - - Requirements/Goal of analysis
  - - Deliverable
- Create Analysis Work Plan
- Create Investigative Plan

## 3. SETUP CASE FOLDER (example)

- EV1 (Evidence Files)
- WC (Working Copy of Files)
  - Case # - Project Name
    - Custodian Name
      - Media Type – EV #
        - Case File
        - Index
        - Reg Files
        - Internet Hist
        - Case Processor
        - Logs
      - Media Type – EV #
      - Media Type – EV #

Analysis Folders

*Organize output neatly!

## 4. CONFIRM IMAGE INTEGRITY

- ✓ Compare Acquisition and Verification Hash values (MD5, SHA)
- Save Verification Reports

5

***GENERAL FORENSIC ANALYSIS CHECKLIST V.1.1***

**THE PURPOSE OF THIS REFERENCE GUIDE IS TO PROVIDE AN OVERVIEW AND OUTLINE OF COMMON PROCESSES, SOFTWARE, AND BEST PRACTICES FOLLOWED BY PROFESSIONALS CONDUCTING COMPUTER FORENSIC ANALYSIS**

***BY DAVID NIDES (12/16/2011)***
***TWITTER: @DAVNADS***
***BLOG: DAVNADS.BLOGSPOT.COM***
***EMAIL: DNIDES@KPMG.COM***

***CREDITS TO: ED GOINGS, ROB LEE & SANS***
***QUESTIONS/FEEDBACK–CONTACT US!***

SANS COMPUTER FORENSICS and INCIDENT RESPONSE

## 5. BEFORE YOU GET STARTED..

- ✓ Check physical size of drive and compare to physical label accounting for all drive space (Check for DCA/HPA).
- ✓ Identify & compare logical partition size(s) to physical drive size to identify any deleted partitions or unused disk space
- ✓ Retrieve time zone settings for each disk and apply correct time zone, if applicable
- ✓ Rename hard disk volumes as necessary to "Recovery", "C", etc.

## GATHER SYSTEM INFORMATION

- ✓ Determine OS, service pack, OS install date, application list, owner, machine name, and other basic information.
- ✓ Retrieve user profile information (names, SIDs, create and last logon dates)

## PRE-PROCESSING ANALYTICS

- ✓ Conduct hash analysis, indentify "known" and/or "notable" files.
- ✓ Conduct file signature analysis, review renamed files.
- ✓ Identify encrypted files (entropy)
- ✓ Mount ALL compound files (VHD, VMDK, ZIP,RAR, Email containers, Reg Files, etc
- ✓ Index Case (DT Search, WDS, Encase, AD..)
- ✓ Generate metadata (and extended) listings/ reports

## RP / VSC

- ✓ Identify if services turned on/used
- ✓ Extract or make available accordingly for analysis

## MOUNTING / VIRTUAL EMULATE

- ✓ Mount - Malware/Virus Scan (Don't forget about MBR)
- ✓ Mount - Stego Scan
- ✓ Virtually Emulate – conduct behavior and live analysis

## KEYWORD SEARCHING

- ✓ Create keyword list & QC syntax formatting/code page usage (may be iterative process)
- ✓ Perform targeted or full disk search including unallocated and slack areas.
- ✓ Create hit report/stats

## FILTERING

- ✓ Filter data based on meta data and exteneded meta data such as Date and Time values, File Extension, and etc.

## EXPORT

Export files from case for independent analysis with specialty tools. For example:

**Memory**
Memorize
Redline
Volatility (SIFT)
**Passwords**
AD PRTK
Passware
Ophcrack
**Shellbags**
Shellbags.py (SIFT)
**Internet History**
WebHistorian
**LNK Files**
Tzworks
Lslnk (SIFT)
**Event Logs (.evt & .evtx)**
Tzworks
GrokEVT
**MFT**
AnalyzeMFT
Ntfswalk (SIFT)
**index/$I30**
INDXParse.py (SIFT)
**SIFT Workstation is a great resource for tons of tools!**

**Email**
NUIX
Clearwell
Recover My Email
Bulk extractor (SIFT)
**Image Mounting**
FTK Imager
ImDisk
Live View
OSFMount
Virtual Box
**Stego**
Outguess
**Hashing**
Md5deep (SIFT)
Sha256deep (SIFT)
Hashdeep (SIFT)
**Registry**
Reg Ripper (SIFT)
Registry Decoder
AD Registry Viewer
Reglookup (SIFT)
YARU (SIFT)
**Windows Journal Parser**
Tzworks

## 6. EQUATION FOR SUCCESSFUL ANALYSIS: (TIMELINES + MANUAL ANALYSIS) x (PASSION + TIME + RESEARCH + RESOURCES) = "WINNING"

### GENERAL AREAS

**Analyze general folder locations for artifacts or data of interest. For example:**
>Desktop
>User folders
>Documents
>Desktop
>Network Shortcuts
>Recently Opened File folders
>System Temp folders
>Browser Temp Folders
>System Folders (malware)
>Autorun

**TIE IT ALL TOGETHER USING TIMELINE ANALYSIS – FLIP SIDE!**

### REGISTRY ANALYSIS (Win only)

**The System registry hives (NTUSER.DAT, SYSTEM, SOFTWARE, SECURITY, SAM..) contain a vast of amount of information that can be imperative to your analysis. For Example:**
-OS Version (SOFTWARE)
-Last logged on user (SAM)
-Last Failed Logon (SAM)
-Username & SID (SAM)
-Shutdown (SYSTEM)
-TimeZone (SYSTEM)
-Drives Mounted by User (NTUSER.DAT)
-File Ext Associations (NTUSER.DAT)
-Installed application list (SOFTWARE)
-Search History (SOFTWARE)
-Removable Storage Devices (SYSTEM)
**Using Registry analysis tools, such as Reg Ripper, can aid your analysis..**

### SYSTEM ARTIFACTS

**There are many system related articfacts that may contain potentially relevant information including:**
-Backups (RP, VSC, others)
-Event Logs (.evt, evtx)
-Shell bags (Registry)
-Jump Lists
-Misc. Logs (firewall, AV, Apps, etc)
-Removable Media Connections
-LNK files
-Prefetch
-PageFile

### SOFTWARE RESIDUE

**Identify software (i.e Wiping tools, P2P, Sticky Notes, hacker tools, etc) and perform analysis on associated files (binary-malware analysis), logs, settings, registry and etc.**

### MEMORY RESIDUE

**If applicable, perform memory analysis to gather volatile information including:**
-Handles; files, directories, processes, registry keys, Semaphores, events and sections
-Open network ports
-Hooks: Driver IRP, SSDT and IDT driver tree

### E-MAIL/IM/SOCIAL ARTIFACTS

**Identify email clients or web access on system and perform analysis on associated data stores or application residue/settings:**
**Client based (file examples):**
Windows - .OST, .PST, .MSG, Temp folder for Outlook attachments, Lotus Notes - .NSF, Mac - .EML, .EMLX, .MBOX
**Web based (OWA, Facebook, Twitter, etc.):**
-Logs -Internet History reconstruction -Cache

### INTERNET

**Identify installed browsers and perform analysis on artifact such as:**
-Parse Internet history files (index.dat, sqlite, etc)
-Check temp folders
-Parse cookies
-Cached pages
-Form History/Auto complete files
-Favorites/bookmarks
-Toolbars
-WebSlices
-Browser plug ins
-Registry analysis
-Carve unallocated for deleted history artifacts

**...BUCKETING ANALYSIS "TO DO" ITEMS LIKE THIS CAN HELP.**

## 7. INTERPRETATION/REVIEW OF ARTIFACTS (examples) ..

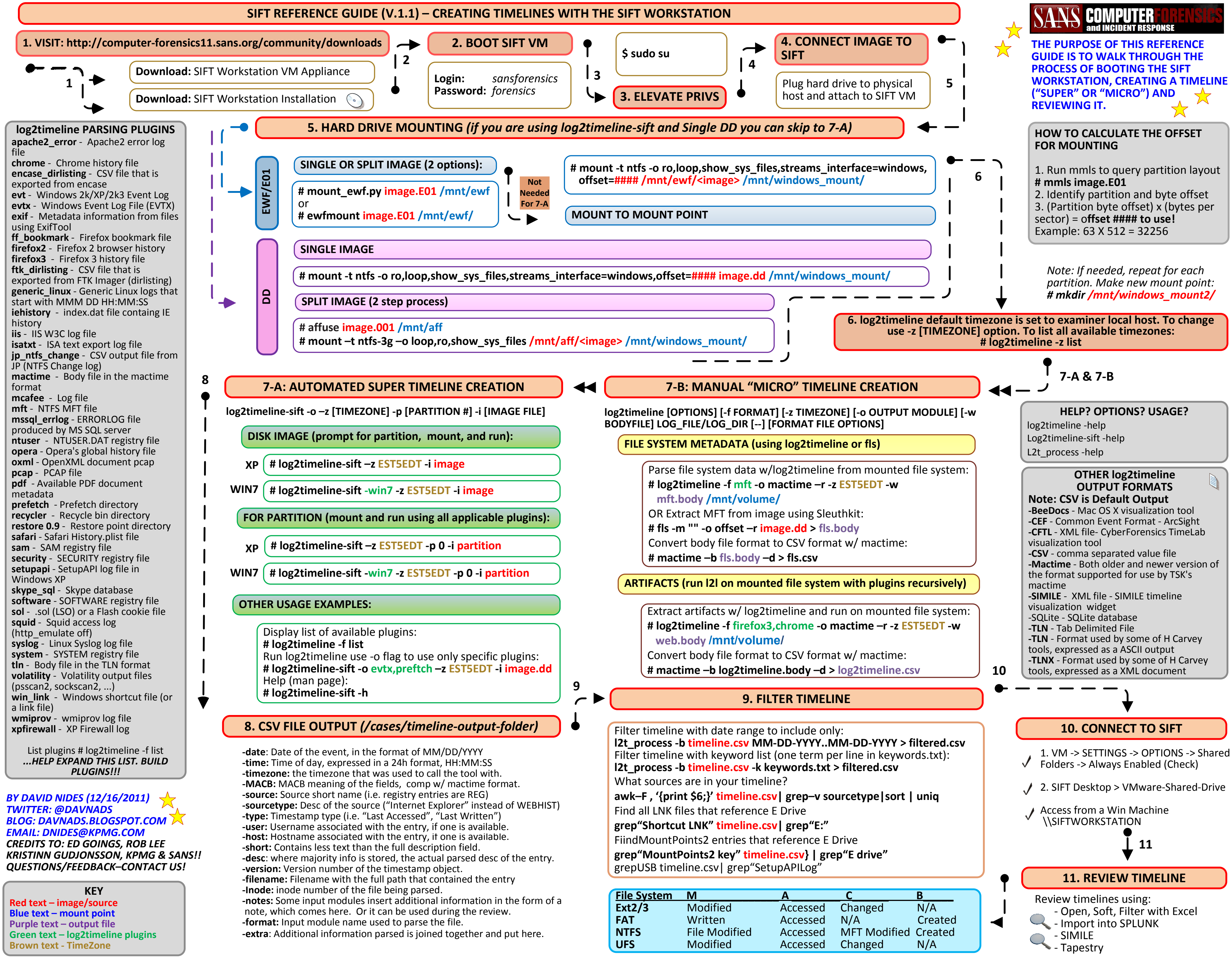
- **File Download:** Open/Save MRU · Open/Run MRU · Email · Skype History · Index.dat / places.sqlite · downloads.sqlite · P2P Logs
- **File Opening/ Creation:** MACB · MRU by ext · MS Office MRU · LNK Files · Index.dat file:// · JumpLists · Shellbags · Prefetch
- **File Knowledge:** XP Search ACMRU · Win7 Search WordWheelQuery · Thumbs.db · WIn7 Thumbnails · Recycle Bin · Browser Artifacts · Last visited MRU
- **USB Usage:** Identification · First & Last Insert Times · User Identification · Volume Name · Drive Letter · LNK Files · Event Logs · Mount Point
- **Program Execution:** User Assist · LastVisited MRU · Run MRU (Start->Run) · Prefetch · MUI Cache · Jump Lists · Event Logs
- **Physical Location:** Time Zone · Wireless SSID · Vista/W7 Network History · Cookies · Search Terms · IP · Image exif
- **Account Usage:** Last Password Change · Group Membership · Success/Fail Logons · Logon Types · RDP Usage · Account Logon/ Authentication · SID Attributes
- **Browser Usage:** History · Search Box Terms · Cache · Session Restore · Flash & Super Cookies · Suggested Sites · Memory Fragments of Private Browsing · AJAX Transactions · Typed URLS

***Have more? Let me know!***

8

## 8.REPORTNG

- ✓ Document findings comprehensively
- ✓ Fact based Interpretation
- ✓ Remember who the audience is
- ✓ Remember requirements/expectations



# SIFT REFERENCE GUIDE (V.1.1) – CREATING TIMELINES WITH THE SIFT WORKSTATION

SANS COMPUTER FORENSICS and INCIDENT RESPONSE

**THE PURPOSE OF THIS REFERENCE GUIDE IS TO WALK THROUGH THE PROCESS OF BOOTING THE SIFT WORKSTATION, CREATING A TIMELINE ("SUPER" OR "MICRO") AND REVIEWING IT.**

## 1. VISIT: http://computer-forensics11.sans.org/community/downloads

1

**Download:** SIFT Workstation VM Appliance

**Download:** SIFT Workstation Installation

2

## 2. BOOT SIFT VM

Login: *sansforensics*
Password: *forensics*

3

```
$ sudo su
```

## 3. ELEVATE PRIVS

4

## 4. CONNECT IMAGE TO SIFT

Plug hard drive to physical host and attach to SIFT VM

5

## 5. HARD DRIVE MOUNTING *(if you are using log2timeline-sift and Single DD you can skip to 7-A)*

### EWF/E01

**SINGLE OR SPLIT IMAGE (2 options):**

```
# mount_ewf.py image.E01 /mnt/ewf
or
# ewfmount image.E01 /mnt/ewf/
```

Not Needed For 7-A

```
# mount -t ntfs -o ro,loop,show_sys_files,streams_interface=windows,
  offset=#### /mnt/ewf/<image> /mnt/windows_mount/
```

**MOUNT TO MOUNT POINT**

### DD

**SINGLE IMAGE**

```
# mount -t ntfs -o ro,loop,show_sys_files,streams_interface=windows,offset=#### image.dd /mnt/windows_mount/
```

**SPLIT IMAGE (2 step process)**

```
# affuse image.001 /mnt/aff
# mount –t ntfs-3g –o loop,ro,show_sys_files /mnt/aff/<image> /mnt/windows_mount/
```

### HOW TO CALCULATE THE OFFSET FOR MOUNTING

1. Run mmls to query partition layout
**# mmls image.E01**
2. Identify partition and byte offset
3. (Partition byte offset) x (bytes per sector) = **offset #### to use!**
Example: 63 X 512 = 32256

*Note: If needed, repeat for each partition. Make new mount point:*
***# mkdir /mnt/windows_mount2/***

6

## 6. log2timeline default timezone is set to examiner local host. To change use -z [TIMEZONE] option. To list all available timezones: # log2timeline -z list

7-A & 7-B

## 7-A: AUTOMATED SUPER TIMELINE CREATION

**log2timeline-sift -o –z [TIMEZONE] -p [PARTITION #] -i [IMAGE FILE]**

**DISK IMAGE (prompt for partition, mount, and run):**

XP
```
# log2timeline-sift –z EST5EDT -i image
```

WIN7
```
# log2timeline-sift -win7 -z EST5EDT -i image
```

**FOR PARTITION (mount and run using all applicable plugins):**

XP
```
# log2timeline-sift –z EST5EDT -p 0 -i partition
```

WIN7
```
# log2timeline-sift -win7 -z EST5EDT -p 0 -i partition
```

**OTHER USAGE EXAMPLES:**

Display list of available plugins:
**# log2timeline -f list**
Run log2timeline use -o flag to use only specific plugins:
**# log2timeline-sift -o evtx,prefetch –z EST5EDT -i image.dd**
Help (man page):
**# log2timeline-sift -h**

## 7-B: MANUAL "MICRO" TIMELINE CREATION

**log2timeline [OPTIONS] [-f FORMAT] [-z TIMEZONE] [-o OUTPUT MODULE] [-w BODYFILE] LOG_FILE/LOG_DIR [--] [FORMAT FILE OPTIONS]**

**FILE SYSTEM METADATA (using log2timeline or fls)**

Parse file system data w/log2timeline from mounted file system:
```
# log2timeline -f mft -o mactime –r -z EST5EDT -w
  mft.body /mnt/volume/
```
OR Extract MFT from image using Sleuthkit:
```
# fls -m "" -o offset –r image.dd > fls.body
```
Convert body file format to CSV format w/ mactime:
```
# mactime –b fls.body –d > fls.csv
```

**ARTIFACTS (run l2l on mounted file system with plugins recursively)**

Extract artifacts w/ log2timeline and run on mounted file system:
```
# log2timeline -f firefox3,chrome -o mactime –r -z EST5EDT -w
  web.body /mnt/volume/
```
Convert body file format to CSV format w/ mactime:
```
# mactime –b log2timeline.body –d > log2timeline.csv
```

### HELP? OPTIONS? USAGE?

log2timeline -help
Log2timeline-sift -help
L2t_process -help

### OTHER log2timeline OUTPUT FORMATS

**Note: CSV is Default Output**
**-BeeDocs** - Mac OS X visualization tool
**-CEF** - Common Event Format - ArcSight
**-CFTL** - XML file- CyberForensics TimeLab visualization tool
**-CSV** - comma separated value file
**-Mactime** - Both older and newer version of the format supported for use by TSK's mactime
**-SIMILE** - XML file - SIMILE timeline visualization widget
-SQLite - SQLite database
**-TLN** - Tab Delimited File
**-TLN** - Format used by some of H Carvey tools, expressed as a ASCII output
**-TLNX** - Format used by some of H Carvey tools, expressed as a XML document

8

## 8. CSV FILE OUTPUT *(/cases/timeline-output-folder)*

**-date**: Date of the event, in the format of MM/DD/YYYY
**-time:** Time of day, expressed in a 24h format, HH:MM:SS
**-timezone:** the timezone that was used to call the tool with.
**-MACB:** MACB meaning of the fields, comp w/ mactime format.
**-source:** Source short name (i.e. registry entries are REG)
**-sourcetype:** Desc of the source ("Internet Explorer" instead of WEBHIST)
**-type:** Timestamp type (i.e. "Last Accessed", "Last Written")
**-user:** Username associated with the entry, if one is available.
**-host:** Hostname associated with the entry, if one is available.
**-short:** Contains less text than the full description field.
**-desc**: where majority info is stored, the actual parsed desc of the entry.
**-version:** Version number of the timestamp object.
**-filename:** Filename with the full path that contained the entry
**-Inode:** 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.
**-format:** Input module name used to parse the file.
**-extra**: Additional information parsed is joined together and put here.

9

## 9. FILTER TIMELINE

Filter timeline with date range to include only:
```
l2t_process -b timeline.csv MM-DD-YYYY..MM-DD-YYYY > filtered.csv
```
Filter timeline with keyword list (one term per line in keywords.txt):
```
l2t_process -b timeline.csv -k keywords.txt > filtered.csv
```
What sources are in your timeline?
```
awk–F , '{print $6;}' timeline.csv| grep–v sourcetype|sort | uniq
```
Find all LNK files that reference E Drive
```
grep"Shortcut LNK" timeline.csv| grep"E:"
```
FiindMountPoints2 entries that reference E Drive
```
grep"MountPoints2 key" timeline.csv} | grep"E drive"
grepUSB timeline.csv| grep"SetupAPILog"
```

| File System | M | A | C | B |
|---|---|---|---|---|
| **Ext2/3** | Modified | Accessed | Changed | N/A |
| **FAT** | Written | Accessed | N/A | Created |
| **NTFS** | File Modified | Accessed | MFT Modified | Created |
| **UFS** | Modified | Accessed | Changed | N/A |

10

## 10. CONNECT TO SIFT

✓ 1. VM -> SETTINGS -> OPTIONS -> Shared Folders -> Always Enabled (Check)

✓ 2. SIFT Desktop > VMware-Shared-Drive

✓ Access from a Win Machine
\\SIFTWORKSTATION

11

## 11. REVIEW TIMELINE

Review timelines using:
- Open, Soft, Filter with Excel
- Import into SPLUNK
- SIMILE
- Tapestry

### log2timeline PARSING PLUGINS

**apache2_error** - Apache2 error log file
**chrome** - Chrome history file
**encase_dirlisting** - CSV file that is exported from encase
**evt** - Windows 2k/XP/2k3 Event Log
**evtx** - Windows Event Log File (EVTX)
**exif** - Metadata information from files using ExifTool
**ff_bookmark** - Firefox bookmark file
**firefox2** - Firefox 2 browser history
**firefox3** - Firefox 3 history file
**ftk_dirlisting** - CSV file that is exported from FTK Imager (dirlisting)
**generic_linux** - Generic Linux logs that start with MMM DD HH:MM:SS
**iehistory** - index.dat file containg IE history
**iis** - IIS W3C log file
**isatxt** - ISA text export log file
**jp_ntfs_change** - CSV output file from JP (NTFS Change log)
**mactime** - Body file in the mactime format
**mcafee** - Log file
**mft** - NTFS MFT file
**mssql_errlog** - ERRORLOG file produced by MS SQL server
**ntuser** - NTUSER.DAT registry file
**opera** - Opera's global history file
**oxml** - OpenXML document pcap
**pcap** - PCAP file
**pdf** - Available PDF document metadata
**prefetch** - Prefetch directory
**recycler** - Recycle bin directory
**restore 0.9** - Restore point directory
**safari** - Safari History.plist file
**sam** - SAM registry file
**security** - SECURITY registry file
**setupapi** - SetupAPI log file in Windows XP
**skype_sql** - Skype database
**software** - SOFTWARE registry file
**sol** - .sol (LSO) or a Flash cookie file
**squid** - Squid access log (http_emulate off)
**syslog** - Linux Syslog log file
**system** - SYSTEM registry file
**tln** - Body file in the TLN format
**volatility** - Volatility output files (psscan2, sockscan2, ...)
**win_link** - Windows shortcut file (or a link file)
**wmiprov** - wmiprov log file
**xpfirewall** - XP Firewall log

List plugins # log2timeline -f list
***...HELP EXPAND THIS LIST. BUILD PLUGINS!!!***

***BY DAVID NIDES (12/16/2011)***
***TWITTER: @DAVNADS***
***BLOG: DAVNADS.BLOGSPOT.COM***
***EMAIL: DNIDES@KPMG.COM***

***CREDITS TO: ED GOINGS, ROB LEE KRISTINN GUDJONSSON, KPMG & SANS!!***

***QUESTIONS/FEEDBACK–CONTACT US!***

### KEY

Red text – image/source
Blue text – mount point
Purple text – output file
Green text – log2timeline plugins
Brown text - TimeZone