Log2Timeline & SIFT: Installation & Data Parsing (Riffle & Forensic Images)

Table of Contents

[**SIFT Use of L2TL for Forensic Images & Riffle:** 2](#_Toc359950052)

[**SIFT L2TL Mount and Process an EnCase image** 2](#_Toc359950053)

[**SIFT L2TL Mount and Process a DD image** 3](#_Toc359950054)

[**SIFT L2TL Process a Riffle Archives** 5](#_Toc359950055)

[**Windows Installation and Use of L2TL:** 5](#_Toc359950056)

[Appendix A: L2TL Time Zones 8](#_Toc359950057)

[Appendix B: L2TL Commands: 9](#_Toc359950058)

[Appendix C: L2TL OS Types & Modules: 12](#_Toc359950059)

## **SIFT Use of L2TL for Forensic Images & Riffle:**

1. Download the latest version of the SANS Forensic Toolkit Download (SIFT) (1.5GB) VM Appliance (v2.14 as of this writing):
   1. <https://computer-forensics21.sans.org/community/download-sift-kit/2.1>
2. Decompress “SIFT\_WORKSTATION\_2.14\_VIRTUAL\_MACHINE\_DISTRO\_rev2.zip” to the folder of your choosing
3. If you don’t already have it, download “VMWare Player”, it’s free:
   1. <https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/5_0>
4. Open “VMWare Player” and open the “VMX” file associated with the downloaded SIFT
5. Reconfigure the RAM on the “VM” by accessing the “Edit virtual machine settings”; Assign at minimum 4GB of RAM to the SIFT VM
6. Play the VM and login using the “sansforensics” username and the password “forensics”
7. Open the “root” terminal by accessing the “Applications” menu, “System Tools” and click on “Root Terminal”
8. Log2Timeline is already installed in SIFT and does not require any additional configuration
9. If you are analyzing a forensic image you must do the following:

### **SIFT L2TL Mount and Process an EnCase image**

1) Create folders

/mnt/ewf

/mnt/hostname

/mnt/hostname\_c (Or whatever volume)

1b) Create your cases folder

mkdir /cases

1c) Create your folder for your case

mkdir /cases/casename

1d) Find your disk

fdisk - l

2) Mount the evidence drive that has the EnCase file

mount -o ro /dev/sdc# /mnt/hostname

3) Mount the E01

mount\_ewf.py /mnt/hostname/Evidence/Whatever.E01 /mnt/ewf

/mnt/ewf will contain two files. The .txt file will contain E01 notes

The other file is the raw E01 file system or disk.

(Example E01 files - WMATV0572860 WMATV0572860.txt)

4) Locate the volume you want to mount

mmls /mnt/ewf/WMATV0572860

root@SIFT-12:/mnt/ewf# mmls WMATV0572860

DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

Slot Start End Length Description

00: Meta 0000000000 0000000000 0000000001 Primary Table (#0)

01: ----- 0000000000 0000002047 0000002048 Unallocated

02: 00:00 0000002048 0000206847 0000204800 NTFS (0x07)

03: 00:01 0000206848 1953517567 1953310720 NTFS (0x07)

5) Calculate the correct image offset

Use calculator

206848 \* 512 = 105906176

6) Mount the volume

mount -o ro,loop,show\_sys\_files,streams\_interface=windows,offset=105906176 /mnt/ewf/WMATV0572860 /mnt/hostname\_c/

7) Run log2timeline of mounted volume

log2timeline -r -p -f image\_type -z US/Pacific /mnt/hostname\_c -w /cases/casename/hostname\_c\_timeline.csv

7a) To save as SQLite use:

log2timeline -r -p -o sqlite -f image\_type -z US/Pacific /mnt/hostname\_c -w /cases/casename/hostname\_c\_timeline.sqlite

### **SIFT L2TL Mount and Process a DD image**

1) Create folders

/mnt/raw

/mnt/hostname

/mnt/hostname\_c (Or whatever volume)

1b) Create your cases folder

mkdir /cases

1c) Create your folder for your case

mkdir /cases/casename

1d) Find your disk

fdisk - l

2) Mount the evidence drive that has the dd file(s)

sudo su

mount -oro /dev/sdc1 /mnt/hostname

3) Mount the dd image

affuse hostname/ddimagefile.001 /mnt/raw

/mnt/raw will contain a file named ddimagefile.001.raw

4) Locate the volume you want to mount

mmls /mnt/raw/ddimagefile.001.raw

root@SIFT-12:/mnt# mmls /mnt/raw/ddimagefile.001.raw

DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

Slot Start End Length Description

00: Meta 0000000000 0000000000 0000000001 Primary Table (#0)

01: ----- 0000000000 0000000062 0000000063 Unallocated

02: 00:00 0000000063 0000144584 0000144522 Dell Utilities FAT (0xde)

03: ----- 0000144585 0000145407 0000000823 Unallocated

04: 00:01 0000145408 0000350207 0000204800 NTFS (0x07)

05: 00:02 0000350208 1023995903 1023645696 NTFS (0x07)

06: ----- 1023995904 1023999871 0000003968 Unallocated

5) Calculate the correct image offset

Use calculator

350208 \* 512 = 179306496

6) Mount the volume

mount -o ro,loop,show\_sys\_files,streams\_interface=windows,offset=179306496 /mnt/raw/ddimagefile.001.raw /mnt/hostname\_c/

7) Run log2timeline of mounted volume

log2timeline -r -p -f image\_type -z US/Pacific /mnt/hostname\_c -w /cases/case/hostname\_c\_timeline.csv

7a) To save as SQLite use:

log2timeline -r -p -o sqlite -f image\_type -z US/Pacific /mnt/hostname\_c -w /cases/casename/hostname\_c\_timeline.sqlite

### **SIFT L2TL Process a Riffle Archives**

1. Extract the contents your Riffle file(s) to a chosen directory on a USB thumb drive or external USB drive
2. Add your USB drive to your SIFT VM
3. Create your cases folder

mkdir /cases

1. Create your folder for your case

mkdir /cases/casename

1. Find your disk that contains your Riffle files

fdisk - l

1. Mount the evidence drive that has the Riffle files

mount -o ro /dev/sdc# /mnt/casename

1. In the root terminal, access the directory in drive you just mounted, where your decompressed Riffle data resides
2. Run the following command in the root terminal for CSV output:

log2timeline -r -p -f win7 -z US/Pacific . -w /cases/casename/casename\_riffle\_l2tl.csv

1. Run the following command in the root terminal for DB output:

log2timeline -r -p -o sqlite -f win7 -z US/Pacific . –w /cases/casename/casename\_riffle\_l2tl.sqlite

1. “.” = Current directory, (Easier if you are in the top level directory of the folder structure you would like to process)
2. Refer to [Appendix A](#_Appendix_A:_L2TL) for a full listing of available time zones
3. For a list of L2TL commands refer to [Appendix B](#_Appendix_B:_L2TL)
4. Refer to [Appendix C](#_Appendix_C:_L2TL) for a listing of Operating Systems and associated artifacts

## **Windows Installation and Use of L2TL:**

*(\* Note, L2TL in Windows will ONLY allow you to Process mounted drives):*

1. Download and install the latest version of Perl64 (64bit) or Perl(x86, 32bit), depending on your OS version:
   1. <http://www.activestate.com/activeperl/downloads>
   2. The folder will then be named “Perl64” if 64 bit OR “Perl” if 32 bit.
   3. Both should reside in the root of the “C:\”
2. Download the latest version of Log2Timeline from, as of this writing the latest version is “0.65”:
   1. <https://code.google.com/p/log2timeline/downloads/list?can=1&q=&colspec=Filename+Summary+Uploaded+ReleaseDate+Size+DownloadCount>
   2. Extract the “log2timeline\_0.##” folder from the .TGZ file to the root of your “C:\” drive
3. Open a command prompt window (It is best to right click on the “cmd.exe” icon and “run as” Administrator if using Windows7)
4. Make sure you are connected to the Internet and install the dependencies for L2TL by opening a command prompt window and running each command:
   1. ppm install datetime
   2. ppm install win32::api
   3. ppm install date::manip
   4. ppm install xml::libxml
   5. ppm install carp::assert
   6. ppm install digest::crc
   7. ppm install data::hexify
   8. ppm install image::exiftool
   9. ppm install file::mork
   10. ppm install datetime::format::strptime
   11. ppm install parse::win32registry
   12. ppm install html::scrubber
5. Download two additional libraries:
   1. <http://www.cpan.org/authors/id/B/BD/BDFOY/Mac-PropertyList-1.37.tar.gz>
   2. <http://www.cpan.org/authors/id/S/SI/SIXTEASE/XML-Entities-1.0001.tar.gz>
6. Decompress the “XML-Entities-1.0001.tar.gz” copy the CONTENTS of the “lib\XML\\*” folder to “C:\Perl\lib\XML\” (Note – The name of your directory “Perl” will vary depending on the version of Perl you installed, x64 or x32/x86
7. Create a directory in the “C:\perl\lib\” named “Mac” (keep capitalization the same)
8. Decompress the “Mac-PropertyList-1.37.tar.gz” and access the folder named “lib\Mac\”
9. Copy the folder and file (PropertyList & PropertyList.pm) within “lib\Mac\” TO the “C:\Perl\lib\Mac\” directory
10. Open the “C:\log2timeline\_0.##” folder and do the following:
    1. Delete the file “C:\log2timeline\_0.##\lib\Log2t\input\pcap.pm”
    2. Copy the CONTENTS of the “C:\log2timeline\_0.##\lib\Parse\\*” TO “C:\Perl\lib\Parse\”
    3. Copy the ENTIRE folder “Log2t” from “C:\log2timeline\_0.##\lib\” TO “C:\Perl\lib\”
    4. Copy the file “C:\log2timeline\_0.##\lib\Log2Timeline.pm” TO “C:\Perl\lib\”
    5. Copy the file “C:\log2timeline\_0.##\log2timeline” TO “C:\Perl\bin\” AND RENAME IT TO “log2timeline.pl”
    6. Copy the file “C:\log2timeline\_0.##\l2t\_process\_old.pl” TO “C:\Perl\bin\” AND RENAME IT TO “l2t\_process.pl”
    7. Copy the file “C:\log2timeline\_0.##\timescanner” TO “C:\Perl\bin\timescanner.pl” AND RENAME IT TO “timescanner.pl”
11. Test to ensure that it works by mounting a forensic image:
    1. Mount the forensic image using FTK Imager (v.3.1.2.0 as of this writing)
12. To test on your local drive or mounted forensic image do the following:
    1. Create folders in the root of “C:\” drive named “cases”
    2. Create a subfolder after your “casename” within the “C:\cases\” folder
    3. Open a command prompt and change DIR to “C:\log2timeline\_0.##”
    4. BEFORE running the command ensure you know the following:
       1. The TIME ZONE associated with the client data (Refer to [Appendix A](#_Appendix_A:_L2TL) for a full listing of available time zones)
       2. Type of OS associated with the client data
       3. Where you will write your output TO
    5. Run the following command for CSV output (For a list of commands refer to [Appendix B](#_Appendix_B:_L2TL)):

**log2timeline.pl -z PST8PDT -f win7 -r -p -w C:\cases\casename\hostname\_c\_timeline.csv I:\**

* + - * + Refer to [Appendix C](#_Appendix_C:_L2TL) for a listing of Operating Systems and associated artifacts
  1. Run the following command for DB output:

**log2timeline.pl -o sqlite -z PST8PDT -f win7 -r -p -w C:\cases\casename\hostname\_c\_timeline.** **sqlite I:\**

* + - * + Refer to [Appendix C](#_Appendix_C:_L2TL) for a listing of Operating Systems and associated artifacts

1. On average, one or more Perl packages may be missing and you will need to install them. My installation was missing “Win32Registry.pm”; I started here:[[1]](#footnote-1)[[2]](#footnote-2)
   1. Received the following error when I ran the log2timeline command:

**Unable to load module Log2t::PreProc::user\_browser. Reason given: Can't locate Parse/Win32Registry.pm in @INC (@INC contains: C:/Perl64/site/lib C:/Perl64/lib**

**.) at C:/Perl64/lib\Log2t\PreProc\user\_browser.pm line 38.**

**BEGIN failed--compilation aborted at C:/Perl64/lib\Log2t\PreProc\user\_browser.pm**

**line 38. Compilation failed in require at C:/Perl64/lib/Log2Timeline.pm line 505.**

* 1. Open the command prompt and type in “ppm”
  2. Go to the view menu and check “All packages”
  3. Search for “Parse-Win32Registry”
  4. Right click and choose to Install
  5. Click on the green arrow in the upper right hand corner of the window “Run Marked Actions”

1. If all is working correctly, begin processing your evidence.

# Appendix A: L2TL Time Zones

*Use the command “log2timeline.pl -z list” to use only the modules included in the list*

PST8PDT

US/Alaska

US/Aleutian

US/Arizona

US/Central

US/East-Indiana

US/Eastern

US/Hawaii

US/Indiana-Starke

US/Michigan

US/Mountain

US/Pacific

US/Pacific-New

US/Samoa

UTC

# Appendix B: L2TL Commands:

Usage:

log2timeline [OPTIONS] [-f FORMAT] [-z TIMEZONE] [-o OUTPUT MODULE] [-w

BODYFILE] LOG\_FILE/LOG\_DIR [--] [FORMAT FILE OPTIONS]

Options:

-s|-skew TIME

Time skew of original machine. The format of the variable TIME

is: X | Xs | Xm | Xh, where X is a integer and s represents

seconds, m minutes and h hours (default behaviour is seconds)

-m TEXT Prepend the filename with the TEXT. That is TEXT is a string

that is prepended in front of the file name to provide a path.

Examples are -m C: to prepend the C:/ in front of each file name

to indicate the partition the file came from.

-f|-format FORMAT

Use the following log file format to parse the content of the

file. Use -f list to see the list of supported log files.

Omitting this options make log2timeline attempt to guess the

format.

-u|-upgrade

Check the latest available version of log2timeline and compare

it to current version (use to check if there is an available

update)

-name HOST

Define the host name that the information is extracted from.

-o|-output FORMAT

Use the following output format. By default log2timeline uses

the CSV output. To see a list of all available output formats,

use -o list

-d|-detail

Some input modules have the capability to include very detailed

amount of information (such as MFT, setupapi and prefetch). This

switch will instruct modules to include those details in the

timeline, so for instance to tell the MFT module to include the

$FN timestamps, or the prefetch one to include loaded DLLs.

-w|-write FILENAME

Specify a file to write output to (otherwise STDOUT will be

chosen).

-z|-zone TIMEZONE

This option defines the timezone that was used on the computer

that the log files belonged to. The default value for this

variable is the local timezone of the computer log2timeline is

run on. There is an option to define -z list to get a list of

all available timezones.

-Z|-Zone TIMEZONE

This option defines the timezone that is used in the output

module of the tool. The default value for this variable is the

same value that is defined in the -z option or the timezone of

the host. This option is used so that output modules can output

in a different timezone than the host is in, for instance to

output in UTC even though the timezone of the host is in another

timezone.

-t|-temp DIR

This option defines the temporary directory the tool uses. By

default the front-end does not set the temporary directory, but

allows the engine to automatically detect it. This option

therefore overwrites the default temporary directory location.

The engine checks the operating system in question, if it is

Windows, it will try to determine the temporary path based on

the Win32::API (so this might fail on 64-bit systems, perhaps

better to use this option to set it manually on those systems).

Otherwise it will use /tmp/ as the temporary directory (should

work on \*NIX systems).

-log FILENAME

Specify a file to write error and information messages from the

log2timeline to a file, otherwise STDERR will be used.

-c|-calculate

If this option is used then a MD5 sum is calculated for the file

and stored in the timestamp object

-x Make log2timeline skip some more detailed tests to see if a file

truly is in the correct input module. The tool should work

faster with this option, however it might miss some files.

-e|-exclude LIST

A comma separated list of files to exclude from the scan. If a

particular file has caused the tool to crash or not work, or you

simply want to exclude some documents from the scan it is

possible to exclude some

-r|-recursive

This option makes log2timeline work in a recursive way, the same

behaviour as timescanner.

-p|-preprocess

If log2timeline is working in recursive mode (-r) it is possible

to use the -p option to run a set of pre-processors agains the

image file. Preprocessors are modules that search through the

suspect drive and extract needed information that can be used in

other modules, such as hostname, etc.

-v|-verbose

Add debugging information. Possible to use with -v -v to

increase some error messages.

-V|-Version

Display the version number

-h|-help|-?

Display this help message

Better description can be read in the man page of the program (man

log2timeline).

# Appendix C: L2TL OS Types & Modules:

*Use the command “log2timeline.pl -f list” to use only the modules included in the list*

**linux**

apache2\_access, apache2\_error, pcap, syslog, generic\_linux, proftpd\_xferlog,

**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, sam, mft,

**win7\_no\_reg**

chrome, evt, exif, ff\_bookmark, firefox3, iehistory, iis, mcafee, opera, oxml, pdf, prefetch, recycler, restore, sol, ntuser, win\_link, xpfirewall, wmiprov, mft,

**winsrv**

evt, exif, iis, isatxt, mcafee, pdf, prefetch, recycler, restore, setupapi, win\_link, xpfirewall, wmiprov, ntuser, software, system, apache2\_access, apache2\_error, mft, mssql\_errlog,

**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, sam, mft,

**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, mft,

1. http://eyeonforensics.blogspot.com/2010\_10\_01\_archive.html [↑](#footnote-ref-1)
2. http://meownotebook.blogspot.com/2012/09/solution-for-cant-locate-datemanippm-in.html [↑](#footnote-ref-2)