The Senator Patrick Leahy Center for Digital Investigation (LCDI)

Log2Timeline Guide for TAPEWORM

Written by: Chapin Bryce

Updated: July, 2013

The Senator Patrick Leahy Center for Digital Investigation

Champlain College

Table of Contents

Configuring TAPEWORM for Log2Timeline

TAPEWORM is a… and can be downloaded at:
http://tapeworm.s3.amazonaws.com/TAPEWORM_1.1.2013_Jan_17.vmware7vm.zip.

Comment [C1]: I would put a description here rather than just jumping in.

Once the zip file for TAPEWORM is downloaded and unzipped, it can be opened in VMWare Workstation 7, 8, 9,;VMWare Fusion; or VMWare Player, 3, 4, or 5. Additionally, it can be converted for use with VirtualBox (using the latest version of any software is recommended). Once it has been opened in the virtualization product, VMWare (shown in **Figure 1**) can be configured for the host machine.

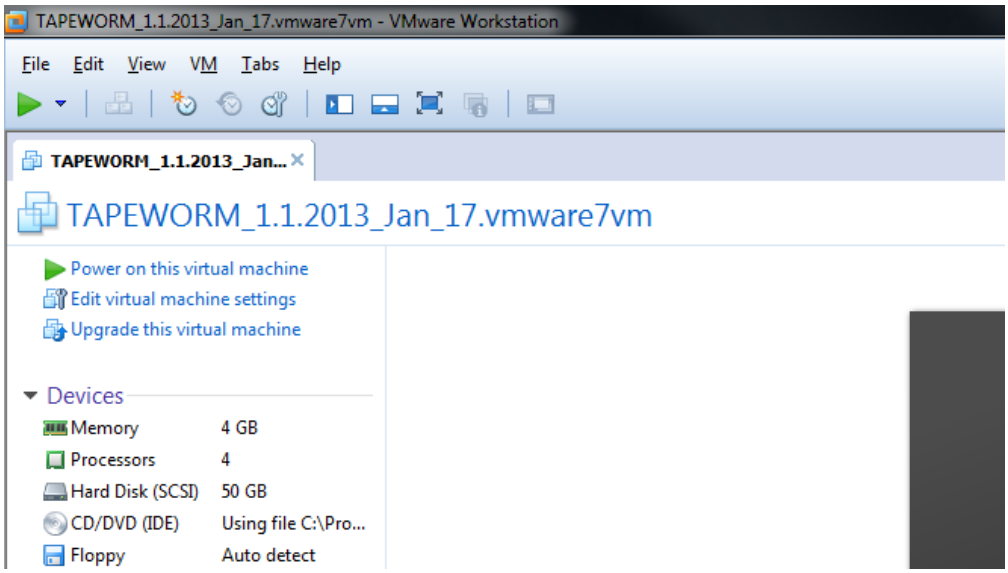


Figure 1 – TAPEWORM VM in VMWare Workstation 9.0.2

Opening the "Edit virtual machine settings" window allows the user to change the number of processors, amount of RAM, and shared folders to be configured for use. The recommended specifications are preset into the virtual machine. **Figure 2** shows the shared folder configuration.

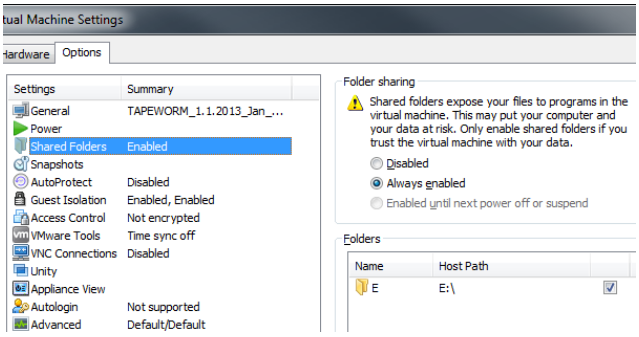


Figure 2 – Shared Folder Configuration

Running Log2Timeline in TAPEWORM

Once the virtual machine is running, the desktop will show the main tapeworm window (See **Figure 3**). From this interface, the automated graphic user interface (GUI) can be used, and the preprocessing and timeline creation for any exhibit can begin. It should be noted that if the main window is minimized, other tools may be accessed either from the terminal or separate GUI applications from the desktop.

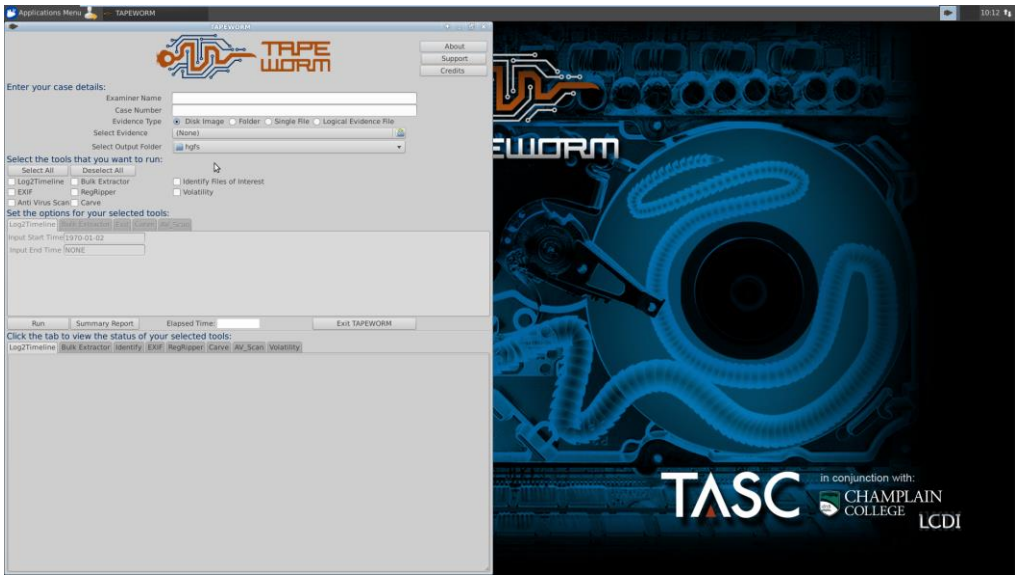


Figure 3 – TAPEWORM Interface

As seen in **Figure 4**, the TAPEWORM interface has case options that need to be filled out in regards to the specific case being processed. After filling out case details, select the evidence type. For creating a timeline, the disk image option is most often used due to the E01, DD, or AFF files used to acquire

exhibits. Additionally, Log2Timeline can be run against a folder or logical image (but not a single file) using TAPEWORM's interface.

Once the evidence type is selected, select your evidence and output location. After choosing the input and output locations and selecting Log2Timeline, hit run. TAPEWORM will automate the process. It allows multiple tools to run in succession as well, so if the evidence requires other processing, you can select the appropriate tools and options to run alongside the timeline at this point.

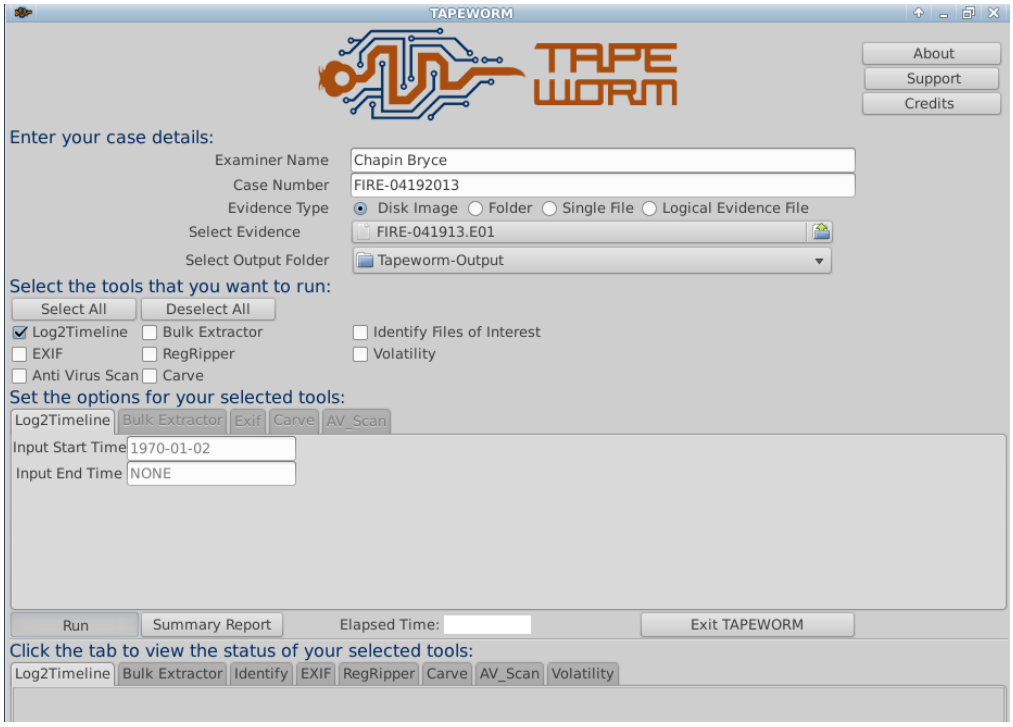


Figure 4 – TAPEWORM Case Information

TAPEWORM utilizes a number of the same steps taken when creating a timeline in SIFT 2.14. TAPEWORM begins by mounting the image, determining the partition types, creating necessary mount points, and doing the math for offsets, as well as starting and ending sectors.

```
Start Mountlog for image'/mnt/hgfs/E/FIRE04192013/FIRE-041913.E01'
Expert Witness File detected, running ewfmount.
The file extension is: .E01'
The file Name is: FIRE-041913

/mnt/tapeworm/2013-05-16-101442.339559/mount__ewf  is not mounted
Just created mount point: /mnt/tapeworm/2013-05-16-101442.339559/mount__ewfWe  found a GUID partition table, need to use parted
GNU Parted 3.1
Using /mnt/tapeworm/2013-05-16-101442.339559/mount__ewf/ewf1
Welcome to GNU Parted! Type 'help' to view a list of commands.


(parted) unit B print q
Model:  (file)
Disk /mnt/tapeworm/2013-05-16-101442.339559/mount__ewf/ewf1: 585064166408
Sector size (logical/physical): 512B/512B
Partition Table: gpt
The partition table is: gpt
Disk Flags:

Number  Start        End          Size         File system  Name             Flags
 1      20480B       209735679B   209715200B   fat32        EFI System Partition  boot
 2      209715680B   193359380478  191262023688  hfs+         Mac
 3      194710077448  195047265278  337187848  fat16        Untitled
 5      195056107528  195066593278  1048576B                  bios_grub
 6      195066593288  328697118718  133630525448  ext4
 7      328697118728  335072460798  637534208B   linux-swap(v1)
Skipping the linux-swap partition
 4      335072460808  585063464958  249991004168  ntfs         Untitled
************** PARTITION INFORMATION**********************************************


/mnt/tapeworm/2013-05-16-101442.339559/mount_0  is not mounted
Just created mount point: /mnt/tapeworm/2013-05-16-101442.339559/mount_0**********************************************************************************
The mount command is: mount -t msdos -o loop,ro,offset=19471007744,noexec,noatime,nodiratime '/mnt/tapeworm/2013-05-16-101442.339559/mount__ewf/ewf1'
/mnt/tapeworm/2013-05-16-101442.339559/mount_0
```

Figure 5 – TAPEWORM Mount Log

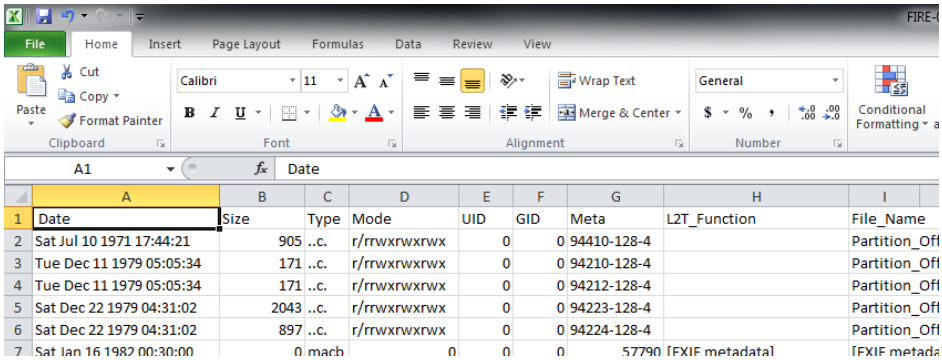
For the test image used in this tutorial (FIRE 04192013.E01), TAPEWORM was able to create a timeline in 25 hours and 17 minutes. It is important to note that this exhibit had 3 operating systems installed: Windows 7, Mac OSX, and BackTrack Linux. Each of these Operating Systems runs on a separate time zone, each with unique user data. If the 25 hour and 17 minute run may seem extremely long, note that TAPEWORM ran Log2Timeline against every partition in the correct time zone, as well as in every format type in one instance without the use of a single command.

Once the timeline is completed, a new folder can be found in the output directory containing an organized (by tool) output. Inside the log2timeline directory are the file types and logs for running log2timeline, with the partition offset in the file names. TAPEWORM exports the timelines in CSV, bodyfile, mactime, or TLN formats. The CSV format is fairly common and can be opened with Microsoft Excel or any other spreadsheet program. The bodyfile and mactime format can be used with the Sleuth Kit and other open source forensic tools for timeline analysis. The TLN format is a custom format that can function with Harlan Carvey's tools.

Reading the output from TAPEWORM

For this guide, the CSV files will be used to look at the output. In TAPEWORM, the CSV documents are split when they are too large for excel to open, preventing any error for maximum file size. Also in the output folder are two different CSV files, one with modules and one without. TAPEWORM adds an additional column to the Log2timeline CSV output, to include the module used to process the particular artifact. For example, if the artifact listed in the CSV file originated from an index.dat file, the index.dat will be listed in the module column. This seems to be a lot of extra information, but when performing an investigation and attempting to look into specific information such as a timeline of Firefox history, sorting by module becomes extremely helpful. The CSV files will also contain the data within any specified date range, while the other file types do not allow for that sort of filtering. The CSV will be the most accurate source of information.

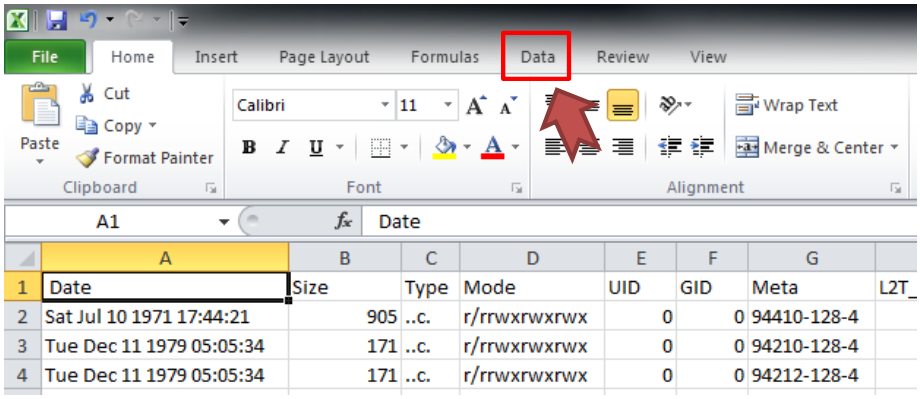
Opening the CSV files in Microsoft Excel shows the data neatly organized by column: sorted by date and time from oldest to newest (See **Figure 6**). Using Excel's data sort feature, the first row can be used to sort and filter content throughout the document.



	A	B	C	D	E	F	G	H	I
1	Date	Size	Type	Mode	UID	GID	Meta	L2T_Function	File_Name
2	Sat Jul 10 1971 17:44:21	905	..c.	r/rrwxrwxrwx	0	0	94410-128-4		Partition_Off
3	Tue Dec 11 1979 05:05:34	171	..c.	r/rrwxrwxrwx	0	0	94210-128-4		Partition_Off
4	Tue Dec 11 1979 05:05:34	171	..c.	r/rrwxrwxrwx	0	0	94212-128-4		Partition_Off
5	Sat Dec 22 1979 04:31:02	2043	..c.	r/rrwxrwxrwx	0	0	94223-128-4		Partition_Off
6	Sat Dec 22 1979 04:31:02	897	..c.	r/rrwxrwxrwx	0	0	94224-128-4		Partition_Off
7	Sat Jan 16 1982 00:30:00	0	macb		0	0	57790	[EXIF metadata]	[EXIF metada

Figure 6 – CSV Timeline Output

To enable the sorting feature, select the "data" tab in excel (See **Figure 7**).



	A	B	C	D	E	F	G	
1	Date	Size	Type	Mode	UID	GID	Meta	L2T_
2	Sat Jul 10 1971 17:44:21	905	..c.	r/rrwxrwxrwx	0	0	94410-128-4	
3	Tue Dec 11 1979 05:05:34	171	..c.	r/rrwxrwxrwx	0	0	94210-128-4	
4	Tue Dec 11 1979 05:05:34	171	..c.	r/rrwxrwxrwx	0	0	94212-128-4	

Figure 7 – Data Filtering with Excel

Then select filter (See **Figure 8**).

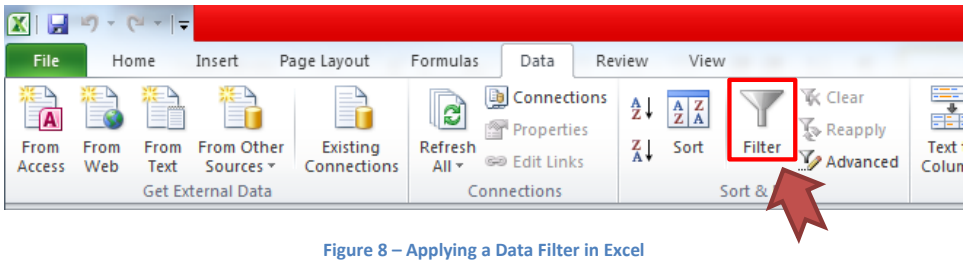


Figure 8 – Applying a Data Filter in Excel