Assignment - VMWare Workstation

Jackson Nestler

University of Advancing Technology

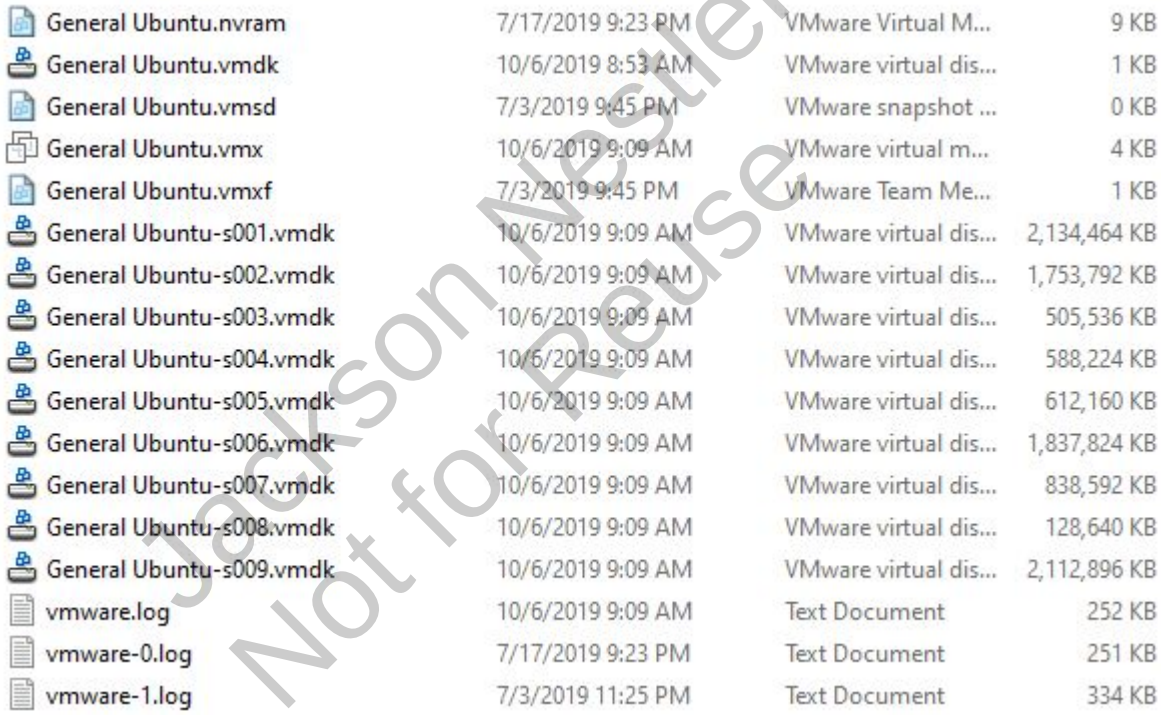
Assignment: VMWare Workstation

VMWare is an industry-leading virtualization company. One of their biggest platforms, ESXi, is an enterprise solution for virtualization. In more "prosumer" circles, VMWare Workstation is a great solution for situations where ESXi is unaffordable, providing a way to manage virtual networks, create virtual machines, and even connect to ESXi servers. VMWare Player is a similar platform, but most notably lacks the ability to connect to remote servers. In either case, users can specify a directory where all of the files necessary to run the VM are stored. This makes copying the VM from one machine to another far easier. For the sake of emulation, I'm supposing that as forensic experts we've extracted the VM from a traditional drive image, and this copy is safe to be utilized.

File hashes were obtained from the copied data. Utilizing Powershell's *Get-FIleHash* function, SHA1 hashes are below.

File Name	SHA1 Hash Value
General Ubuntu-s001.vmdk	68F4C9A27F84413F8A1AE6088D330B0AE2C90AA7
General Ubuntu-s002.vmdk	0B0FEA1AE1DBB7072FA4192E07599B19E88C6279
General Ubuntu-s003.vmdk	61AF602E992A54E19E0F4ACA6E49E60471A71FE5
General Ubuntu-s004.vmdk	9E2665975977A58567F85FFA145F3037AFDC228B
General Ubuntu-s005.vmdk	A644092D9DD3A56EDD3292AC6280767E50DE0751
General Ubuntu-s006.vmdk	6CF613A1F06D0332D784337F61E597D66324A4C3
General Ubuntu-s007.vmdk	29EA70A927F5C9F33BE89422DB375B5FFB802872
General Ubuntu-s008.vmdk	21CCB65EAD1433FEA23FEFE72FC946A08FE2A229
General Ubuntu-s009.vmdk	A27AF23A404CDF89B45A7FE6FBF57EC111BEF40C
General Ubuntu.nvram	C352B9BD8095CB1D0C77B327662072B922DAE5CA

General Ubuntu.vmdk	D7B5954F2C65B9F42273D5A3FA97497C9A318A5B
General Ubuntu.vmsd	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
General Ubuntu.vmx	5D1731F788006CCAE6F0178B0354DEC17A2D0368
General Ubuntu.vmxf	6DA5AEEE31F35AEE9A20F56EA1DE3D351244F265
vmware-0.log	7E8B24129814EAEF59688ECF2945E67805B6E10F
vmware-1.log	B2BC74AF53C93FA6B3C6F6FD09EDCCDC2EC3D5E0
vmware.log	D69FA0EF94CCEE3F3AACDAA7E37C7002334C81CB



Investigator Jackson Nestler established an Autopsy case[1], selecting the option to import a "Disk Image or VM File." The file "General Ubuntu.vmdk" was opened and ingest modules ran.[2]

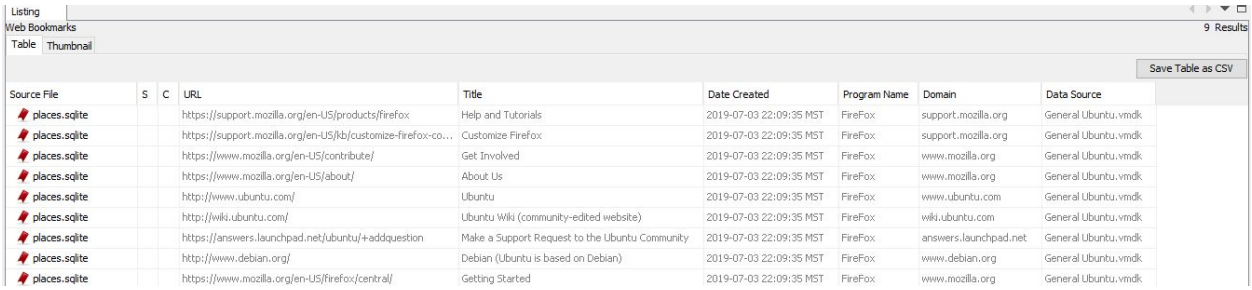
[1] File location is A:\Forensics_Courses\VMWare_Assignment
[2] Autopsy 4.1.0 release allows for the automatic import of VMDK and VHD files. https://www.autopsy.com/autopsy-4-1-0-release/

Upon ingest, the following file counts were detected:

File Type	Count
Images (.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif)	12,910
Videos (.aaf, .3pg, .asf, .avi, .m1v, .mv2, .m4v, .mp4, .mov)	2
Audio (.flac, .way, .mp3)	106
Archives (.zip, .rar, .7zip, .7z, .tar, .gzip)	8,221
Database (.db, .db3, .sqlite, .sqlite3)	81
HTML (.htm, .html)	431
Office (.doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx)	7
PDF (.pdf)	14
Plain Text (.txt)	361
Rich Text (.rtf)	0
Executable (.cmd)	196
Deleted Files (from File System)	109,402
All Deleted Files	109,402

Autopsy's ingest module also identified 9 web bookmarks, 49 web cookies, 4 web autofill forms, 68 web history incidents, and 11 web searches. Viewing the web bookmarks shows a list of entries that are known to be shipped with the default instance of Firefox on Debian-based systems. Web cookies line up with the user's previous activity[3].

[3] Not shown for privacy purposes. Includes information from password manager & such.



Listing
Web Bookmarks
9 Results
Table | Thumbnail
Save Table as CSV

Source File	S	C	URL	Title	Date Created	Program Name	Domain	Data Source
places.sqlite			https://support.mozilla.org/en-US/products/firefox	Help and Tutorials	2019-07-03 22:09:35 MST	FireFox	support.mozilla.org	General Ubuntu.vmdk
places.sqlite			https://support.mozilla.org/en-US/kb/customize-firefox-co...	Customize Firefox	2019-07-03 22:09:35 MST	FireFox	support.mozilla.org	General Ubuntu.vmdk
places.sqlite			https://www.mozilla.org/en-US/contribute/	Get Involved	2019-07-03 22:09:35 MST	FireFox	www.mozilla.org	General Ubuntu.vmdk
places.sqlite			https://www.mozilla.org/en-US/about/	About Us	2019-07-03 22:09:35 MST	FireFox	www.mozilla.org	General Ubuntu.vmdk
places.sqlite			http://www.ubuntu.com/	Ubuntu	2019-07-03 22:09:35 MST	FireFox	www.ubuntu.com	General Ubuntu.vmdk
places.sqlite			http://wiki.ubuntu.com/	Ubuntu Wiki (community-edited website)	2019-07-03 22:09:35 MST	FireFox	wiki.ubuntu.com	General Ubuntu.vmdk
places.sqlite			https://answers.launchpad.net/ubuntu/+addquestion	Make a Support Request to the Ubuntu Community	2019-07-03 22:09:35 MST	FireFox	answers.launchpad.net	General Ubuntu.vmdk
places.sqlite			http://www.debian.org/	Debian (Ubuntu is based on Debian)	2019-07-03 22:09:35 MST	FireFox	www.debian.org	General Ubuntu.vmdk
places.sqlite			https://www.mozilla.org/en-US/firefox/central/	Getting Started	2019-07-03 22:09:35 MST	FireFox	www.mozilla.org	General Ubuntu.vmdk

Firefox's SQLite DB Entries

In the more recent versions of Autopsy, analyzing VM files is made easy with their VM import functionality, analyzing VMDKs and VHDs. The ingest modules treat these VM files identically to their traditionally-imaged counterparts, making no changes to the VM filesystem or the host filesystem. Forensic experts can utilize Autopsy to validate their findings in other forensic suites, or get a better idea of what may be present on a disk.

References

Autopsy 4.1.0 Release Notice. (2016, July 21). Autopsy 4.1.0 Release. Retrieved from https://www.autopsy.com/autopsy-4-1-0-release/

Autopsy 4.13.0 Documentation. (n.d.). Autopsy User Documentation: Virtual Machine Extractor Module. Retrieved from https://sleuthkit.org/autopsy/docs/user-docs/4.13.0/vm_extractor_page.html

Autopsy 4.5.0 Documentation. (n.d.). Autopsy User Documentation: Data Sources. Retrieved from https://sleuthkit.org/autopsy/docs/user-docs/4.5.0/ds_page.html