

Magnet CTF:

Question 1 Solution Walk-Through

1: What time was the file that maps names to IP's recently accessed?

Mobile Forensics is not my strongest area, and Android even less than iOS. Based on my limited experience the first thing I started with was Google ("GTS"). Based on the question I supposed that the artifact would be DNS related. Where on the device would that be set locally? To my delight I learned that on Android there is a local **hosts** file that is responsible for mapping IP's to DNS (what do you know just like Windows and Linux).



Doing a Global Search for **hosts** there are a number of hits, but nothing for the hosts file itself.

The screenshot shows the Magnet AXIOM Examine v4.5.0.21589 - MagnetCTF interface. The top navigation bar includes File, Tools, Process, and Help. Below this is a filter bar with tabs for Evidence, Artifacts, Content types, Date and time, Tags and comments, and Profiles. The main search results area shows a list of items with columns for Item, Type, Artifact ca..., and Date and time. The search term 'hosts' is entered in the search bar. The results are categorized by type: CHAT (2), SOCIAL NETWORKING (2), and DOCUMENTS (20). The details panel on the right shows information for item 1135983726, including Author ID, Status ID, Created Date/Time, and a tweet from @vermontedition.

Item	Type	Artifact ca...	Date and time
1135983726	Twitter Tweets	Social Networking	3/12/2020 3:12:44 PM
1135983726	Twitter Tweets	Social Networking	3/12/2020 3:12:44 PM
897	KakaoTalk Messages	Chat	9/21/2028 4:05:02 AM
897	KakaoTalk Messages	Chat	9/21/2028 4:05:02 AM
params_map.txt	Text Documents	Documents	3/26/2020 12:23:33 PM
params_map.txt	Text Documents	Documents	3/12/2020 6:38:25 AM
params_map.txt	Text Documents	Documents	3/23/2020 5:53:10 PM
AGPL-V3.txt	Text Documents	Documents	1/25/2020 5:41:38 PM
GPL-3.0.txt	Text Documents	Documents	1/25/2020 5:41:38 PM
INSTALL.txt	Text Documents	Documents	1/25/2020 5:41:38 PM
NEWS.txt	Text Documents	Documents	1/25/2020 5:41:38 PM
ChangeLog.txt	Text Documents	Documents	1/25/2020 5:41:38 PM
pctest.txt	Text Documents	Documents	2/15/2020 9:55:22 PM
...

The first time I processed the Android image tar file I did it as

Mobile > Android > Load Evidence > Image

Using this format when I went to the file explorer view in Magnet, all that was visible was the tar file and I couldn't navigate the directory structure.



I extracted the tar file (using 7zip) and then re-processed the evidence as



Mobile > Android > Load Evidence > Files and Folders

This yielded the same number of artifacts; however, it exposed the directory structure for browsing in **File System** view.

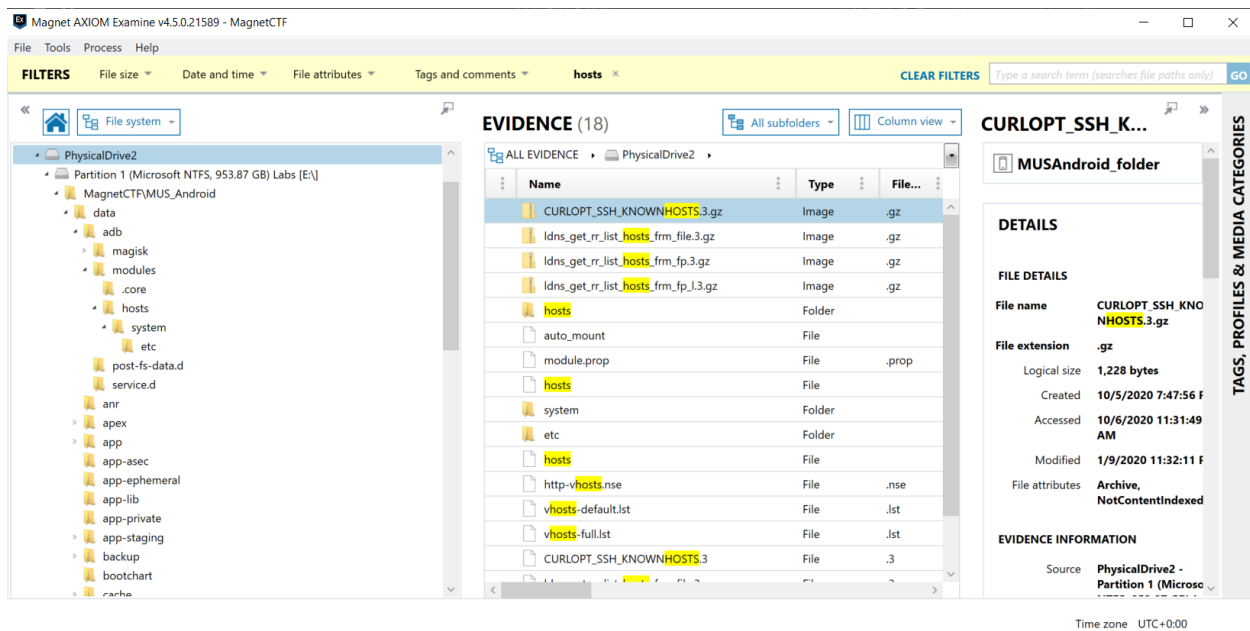
EVIDENCE OVERVIEW

ADD NEW EVIDENCE

 **MUSAndroid_folder** (63,968) 

 **MUSAndroid.tar** (63,968) 

In the **File System** view we can now run a search for **hosts** (be sure to enable subdirectory results if you're not focusing on a particular path).



The screenshot displays the Magnet AXIOM Examine v4.5.0.21589 - MagnetCTF interface. The 'File system' view is active, showing a directory tree for 'PhysicalDrive2'. The search filter 'hosts' is applied, and the results are displayed in the 'EVIDENCE (18)' pane. The results list includes files like 'CURLOPT_SSH_KNOWNHOSTS.3.gz', 'ldns_get_rr_list_hosts_frm_file.3.gz', 'ldns_get_rr_list_hosts_frm_fp.3.gz', 'ldns_get_rr_list_hosts_frm_fp.1.3.gz', 'hosts', 'auto_mount', 'module.prop', 'hosts', 'system', 'etc', 'hosts', 'http-vhosts.nse', 'vhosts-default.lst', 'vhosts-full.lst', and 'CURLOPT_SSH_KNOWNHOSTS.3'. The 'hosts' file is highlighted. The right pane shows details for 'CURLOPT_SSH_KNOWNHOSTS.3.gz', including file name, extension, logical size, creation date, access date, modification date, and file attributes.

Name	Type	File...
CURLOPT_SSH_KNOWNHOSTS.3.gz	Image	.gz
ldns_get_rr_list_hosts_frm_file.3.gz	Image	.gz
ldns_get_rr_list_hosts_frm_fp.3.gz	Image	.gz
ldns_get_rr_list_hosts_frm_fp.1.3.gz	Image	.gz
hosts	Folder	
auto_mount	File	
module.prop	File	.prop
hosts	File	
system	Folder	
etc	Folder	
hosts	File	
http-vhosts.nse	File	.nse
vhosts-default.lst	File	.lst
vhosts-full.lst	File	.lst
CURLOPT_SSH_KNOWNHOSTS.3	File	.3

DETAILS

FILE DETAILS

File name: CURLOPT_SSH_KNOWNHOSTS.3.gz

File extension: .gz

Logical size: 1,228 bytes

Created: 10/5/2020 7:47:56 F

Accessed: 10/6/2020 11:31:49 AM

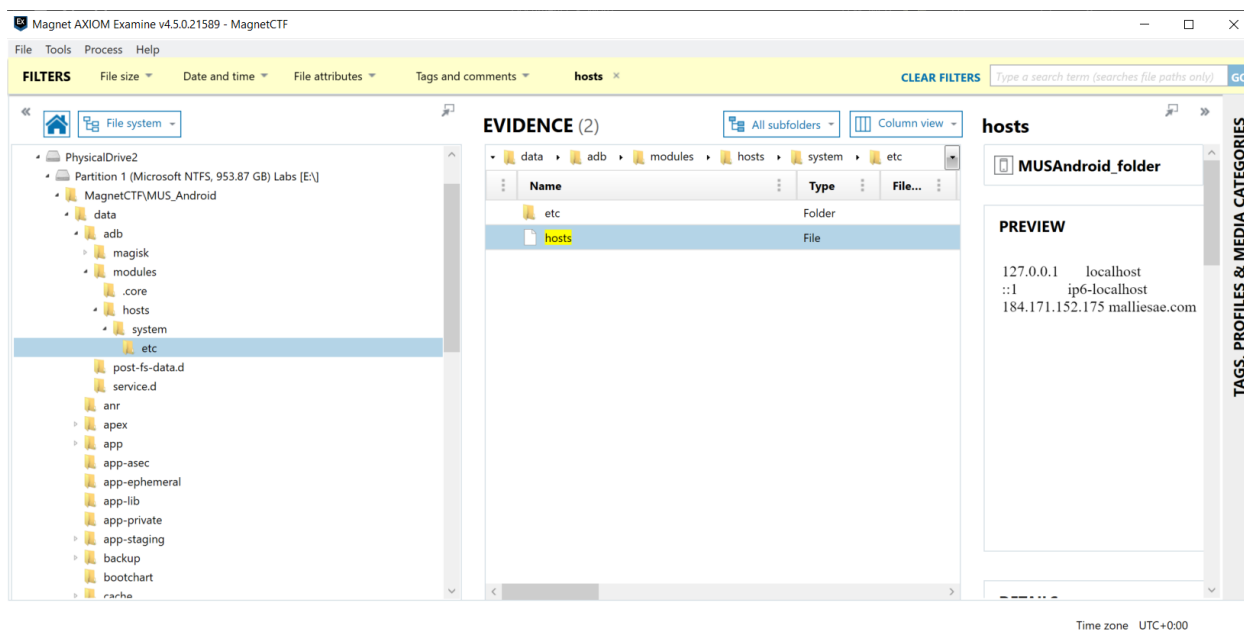
Modified: 1/9/2020 11:32:11 F

File attributes: Archive, NotContentIndexed

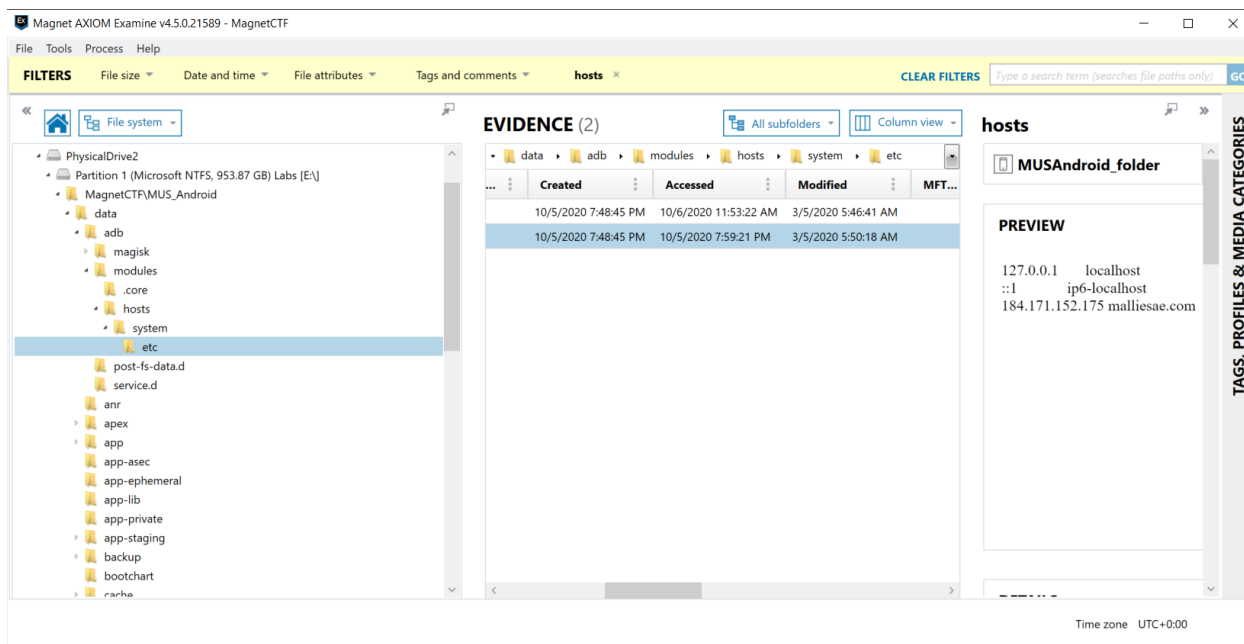
EVIDENCE INFORMATION

Source: PhysicalDrive2 - Partition 1 (Micro...

In this case the **hosts** file can be found at `/data/adb/modules/hosts/system/etc`



Looking at the preview we can see an additional entry for **malliesae.com**



With the hosts file selected, scrolling to the right reveals the Created, Accessed and Modified times for this file. Here we see that the file was modified **03/05/2020 05:50:18**.