

School of Computing
IT8003 Digital Forensics and Investigation

Practical 2A: Refined Results on Magnet AXIOM Examine

Introduction

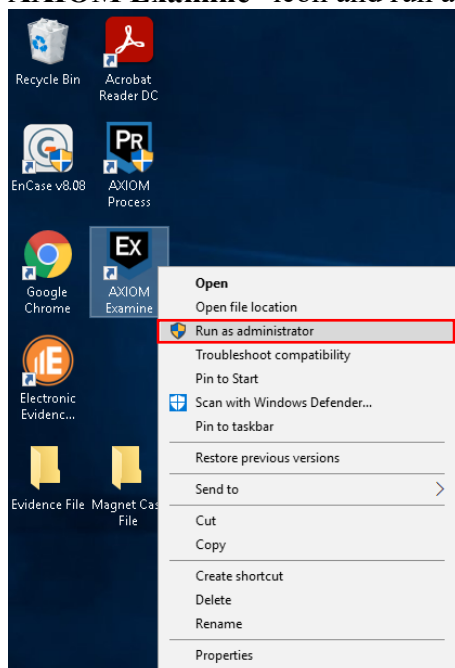
Performing keyword and searching can help a forensic examiner to narrow down the relevant artifacts during analysis. Thus, it is important for a forensic examiner to understand the case background and build a list of search terms which can identify evidence that is relevant to the matter. Refining your search results is another element to keyword searches because it helps a forensic examiner to eliminate the noise and it can provide a more quality search results.

Learning Objective

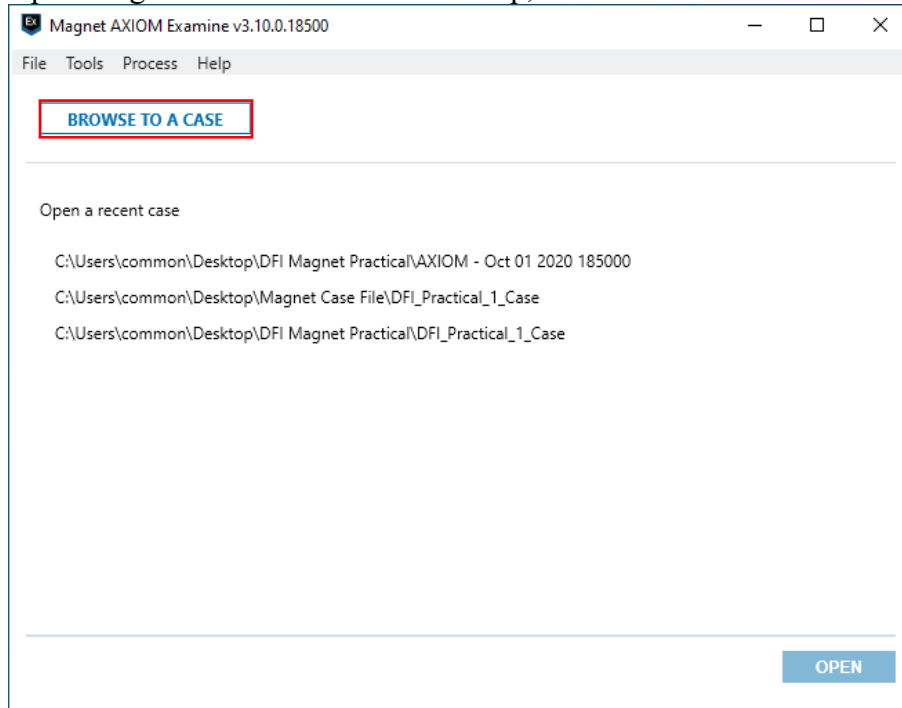
In this lesson, students will take part in lectures, instructor-led exercises, and student practical exercises to learn the way in which Magnet AXIOM Examine organizes artifacts within the Refined Results parent category. Students will be able to perform and examine sources of searches such as Google and parsed search queries. At the conclusion of this lesson, students will be able to identify, discuss, and utilize artifacts found within the Refined Results category of AXIOM Examine to further a forensic examination.

Exercise 1. Opening Magnet Practical Case

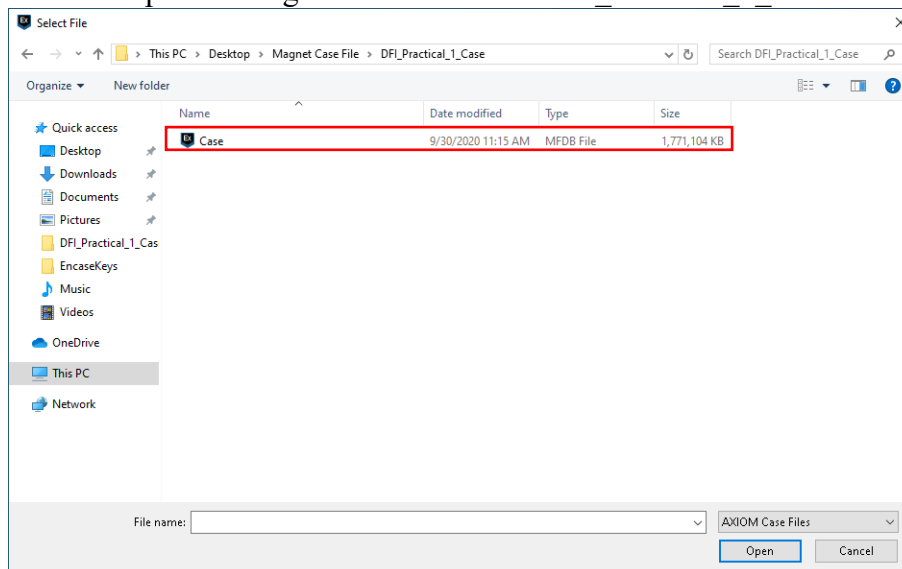
1. Open the application “**Magnet AXIOM Examine**”. (Note: right-click on “**Magnet AXIOM Examine**” icon and run as administrator)



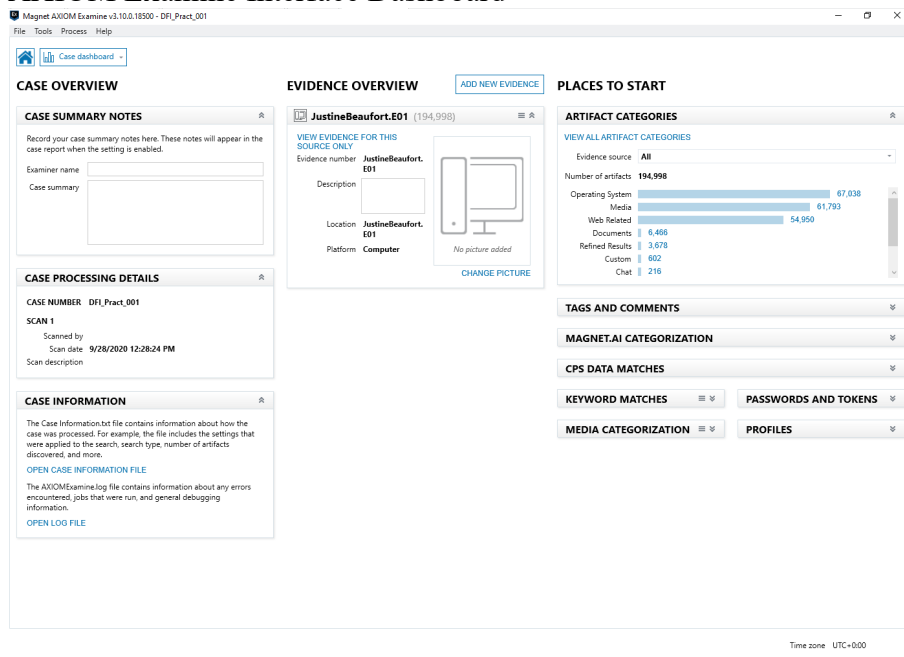
2. Upon Magnet AXIOM Examine start up, click on “**Browse to a Case**”



3. A window will appear that will allow you to select a Magnet AXIOM Case, navigate to “Desktop” → “Magnet Case File” → “DFI_Practical_1_Case” and select “Case”



4. Upon selecting the case, Magnet AXIOM Examine will start and you arrived in Magnet AXIOM Examine Interface Dashboard



Google Searches

The Google Searches artifact group, under Refined Results, compiles searches made via the Google webpage by any supported browser. The Details Card provides the following information:

Artifact Information	Description
Search Term	This information is embedded in the URL itself; this is common to most search engine websites.
URL	The full URL from Google.
Date/Time	Date and time the search was executed. The source of this information will vary by browser.
Web Page Title	The title of the web page that appears in the browser's title bar.
Original Artifact	The AXIOM Examine artifact category (under the Web Related parent category) from which the information was parsed.

Evidence Information	Description
Source	The directory path (including file name) of the browser artifact from which the data was parsed.
Location	Location of the data within the source file or object. The example shown is a History SQLite database from the Chrome browser; the specific database table entries are listed. In some cases, if the data doesn't come from a database of some sort, the offset from the beginning of the file or object will be listed.

DETAILS

ARTIFACT INFORMATION

URL

https://www.google.com/search?rlz=1C1CHBF_enUS842US842&biw=1280&bih=689&ei=dDuaXJPOKILSsAX414Vo&q=where+to+buy+owl+eggs&oq=where&gs_l=psy-ab.1.0.35139j0i6712j0i131j0i67j0i131j0i67j0i131.5779.9999..1769...9.0..0.192.2159.0j14....3..0....1..gws-wiz.....0i131i67j0i10.3gnuQg6gm6Q

Date Visited Date/Time

3/26/2019 2:47:31 PM

Title

where to buy owl eggs - Google Search

Typed Count

0

Transition Type

FORM_SUBMIT

EVIDENCE INFORMATION

Source

Item01_HPHardDrive.E01 - Partition 2 (Microsoft NTFS, 199.9 GB) Operating System\Users\Justine B\AppData\Local\Google\Chrome\User Data\Default\History

Recovery Method

Parsing

Deleted source

Location

Table: visits(id: 57)
Table: urls(id: 41)

Evidence number

Item1: HP Hard Drive.

Figure 3-1-7: Details Card for A Google Search

To replicate these results, conduct a search for “owl eggs” and then select the Chrome Web Visits Artifacts.

The screenshot displays the Magnet AXIOM interface. On the left, a sidebar shows 'MATCHING RESULTS' (14), 'REFINED RESULTS' (7), 'WEB RELATED' (4), and 'DOCUMENTS' (3). The 'WEB RELATED' section is expanded, showing 'Chrome Web Visits' (1) and 'Webkit Browser Web History (Carved)' (1). The main area shows 'MATCHING RESULTS (1 of 417)' with a table of results. The first result is a Google search for 'owl eggs' from 3/26/2019. On the right, a 'DETAILS' card for 'Item1: HP Hard Drive' is shown, containing the same artifact information as Figure 3-1-7. The top of the interface includes a filter bar with 'Media attributes (VICS)' and 'owl eggs' selected.

Figure 3-1-8: Filters Applied

Parsed Search Queries

The Parsed Search Queries artifact group compiles searches made on sites other than Google. This would include searches performed on popular sites such as Yahoo, Facebook, Bing, YouTube, etc. The Details Card provides the following information:

Artifact Information	Description
Search Term	This information is embedded in the URL itself; this is common to most search engine websites.
URL	The full URL from Google.
Date/Time	Date and time the search was executed. The source of this information will vary by browser.
Search Engine	The search engine used to search for the keyword(s).
Web Page Title	The title of the web page that appears in the browser's title bar.
Original Artifact	The AXIOM Examine artifact category (under the Web Related parent category) from which the information was parsed.

Evidence Information	Description
Source	The directory path (including file name) of the browser artifact from which the data was parsed.
Location	Location of the data within the source file or object. The example shown is a History SQLite database from the Chrome browser; the specific database table entries are listed. In some cases, if the data doesn't come from a database of some sort, the offset from the beginning of the file or object will be listed.

Magnet AXIOM Examine v3.0.0.13673 - Item01_HPHardDrive

File Tools Process Help

FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone Media categorization M

« Home Artifacts »

EVIDENCE (264) Column view

ALL EVIDENCE	155,661	Search Term	URL	Date/Time	Date...	Search Engine	Goo...
REFINED RESULTS	3,361	owls in south carolina	https://www.bing.com/search?q=owls+in+south+ca...			Bing	
Classifieds URLs	514	owls in south bend	https://www.bing.com/search?q=owls%20in%20sou...			Bing	
Cloud Services URLs	112	baby owls	https://www.bing.com/search?q=baby%20owls&q...			Bing	
Facebook URLs	520	free owls	https://www.bing.com/search?q=free+owls&q=n&...			Bing	
Google Analytics First Visit Cookies	2	owls in south carolina	https://www.bing.com/search?q=owls+in+south+ca...			Bing	
Google Analytics Referral Cookies	2	baby owls	https://www.bing.com/search?q=baby%20owls&q...			Bing	
Google Analytics Session Cookies	2	owls in south bend	https://www.bing.com/search?q=owls%20in%20sou...			Bing	
Google Maps Queries	172	south bend owls	https://www.facebook.com/search/top/?q=south%2...	3/26/2019 2:53:56 PM		Facebook	
Google Searches	544	barn owls	https://www.facebook.com/search/top/?q=barn%20...	3/26/2019 2:55:14 PM		Facebook	
Identifiers	395	owl movies	https://www.youtube.com/results?search_query=owl...	3/26/2019 3:14:49 PM		Youtube	
Parsed Search Queries	264	black owls	https://www.youtube.com/results?search_query=bla...	3/26/2019 3:16:20 PM		Youtube	
Rebuilt Webpages	366	owl	https://www.youtube.com/results?search_query=owl	3/26/2019 3:16:31 PM		Youtube	
Social Media URLs	461	baby owls	https://www.youtube.com/results?search_query=ba...	3/26/2019 3:16:40 PM		Youtube	
Tax Site URLs	1	another name for owls	https://www.youtube.com/results?search_query=an...	3/26/2019 3:17:09 PM		Youtube	
Torrent URLs	6	cartoon owl	https://www.youtube.com/results?search_query=car...	3/26/2019 3:17:20 PM		Youtube	
		free owls	https://www.bing.com/search?q=free+owls&q=n&...	3/26/2019 4:55:30 PM		Bing	
		baby owls	https://www.bing.com/search?q=baby%20owls&q...	3/26/2019 4:56:41 PM		Bing	
		owls in south carolina	https://www.bing.com/search?q=owls+in+south+ca...	3/26/2019 4:56:50 PM		Bing	

Figure 3-1-12: Evidence Pane Of Parsed Search Queries

Cloud Services URLs

The Cloud Services URLs artifacts group lists URLs related to usage of cloud-based storage services. URLs listed here are compiled from the activity of various browsers. About 50 cloud services are supported, including OneDrive, SkyDrive, Carbonite, Google Drive, Dropbox, Box, and more. For a full listing of supported domains, see the Artifact Reference, accessible through the **Help -> Documentation** menu.

Component	Description
Site Name	The name of the cloud service website.
URL	The URL of the cloud service website.
Date/Time	The date and time that's associated with the artifact where the URL is from. (UTC)
Artifact	The artifact that the cloud service URL is from.
Original Artifact	The AXIOM Examine artifact category from which the information was parsed.

Magnet AXIOM Examine v3.0.0.13673 - Item01_HPHardDrive

File Tools Process Help

FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

<< [Home] [Artifacts]

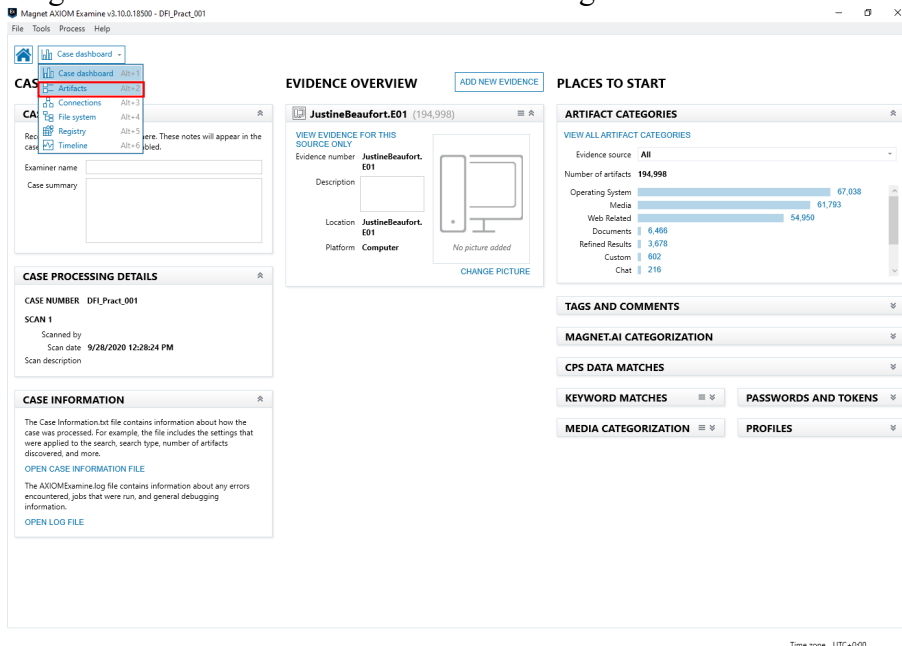
EVIDENCE (112)

	Site...	URL	Date/Time	Date...	Artifact
ALL EVIDENCE					155,661
REFINED RESULTS					3,361
Classifieds URLs					514
Cloud Services URLs					112
Facebook URLs					520
Google Analytics First Visit Cookies					2
Google Analytics Referral Cookies					2
Google Analytics Session Cookies					2
Google Maps Queries					172
Google Searches					544
Identifiers					395
Parsed Search Queries					264
Rebuilt Webpages					366
Social Media URLs					461
Tax Site URLs					1
Torrent URLs					6

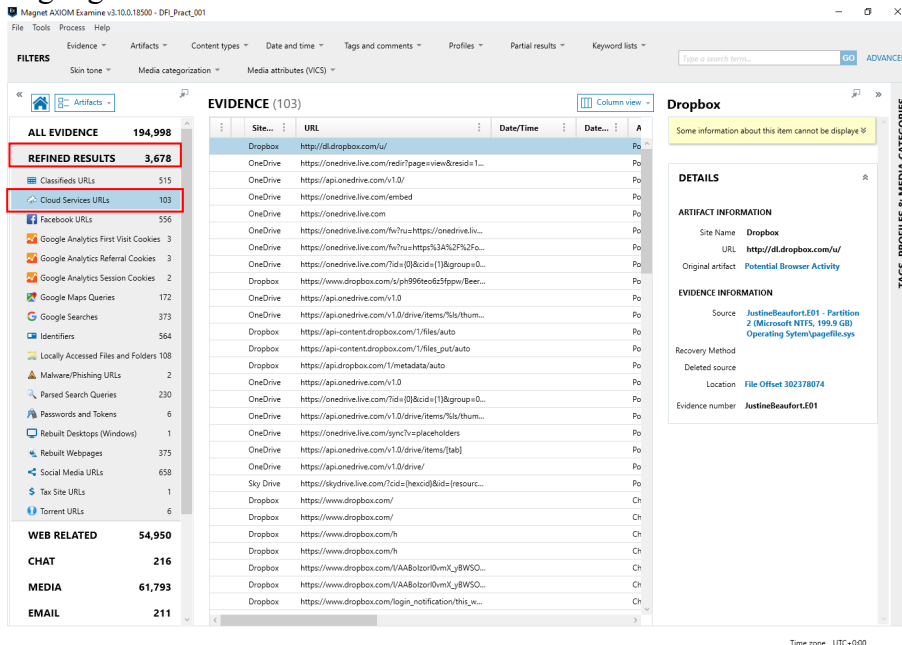
Figure 3-1-14: Cloud Services Urls

Exercise 2. Determining Dropbox Usage

- Continue from step 4 of Exercise 1, click on the “**Case Dashboard**” at the top of Magnet AXIOM Examine interface and navigate to “**Artifacts**”

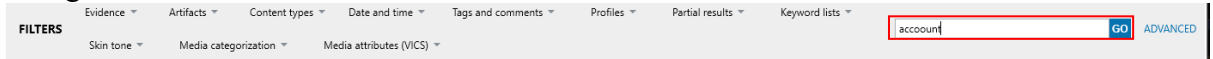


- Highlight the “**Refined Results**” → “**Cloud Services URLs**” artifact category.

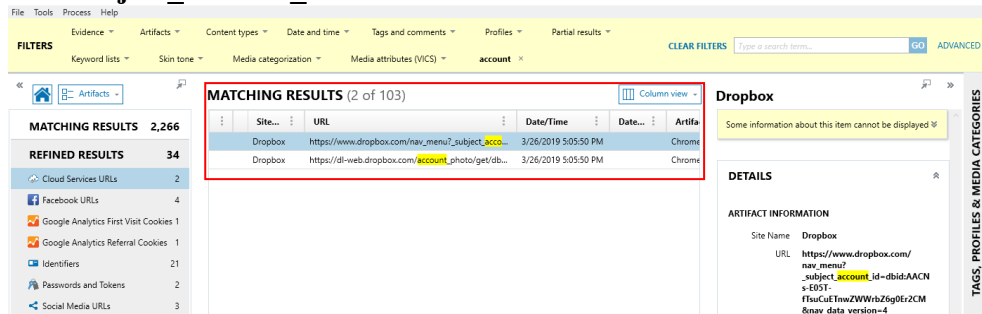


- We want to see if we can determine the account associated with the Dropbox account and if the user has logged in and/or downloaded any materials from Dropbox.

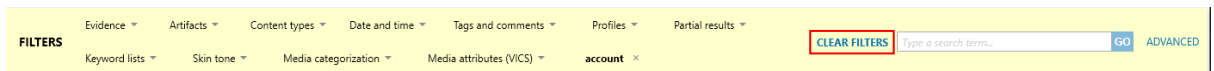
8. Using the “**search term**” Filter bar, conduct a search for “**account**”



- a. Note the search results: two hits, one of which has a URL containing “**subject_account_id**”.



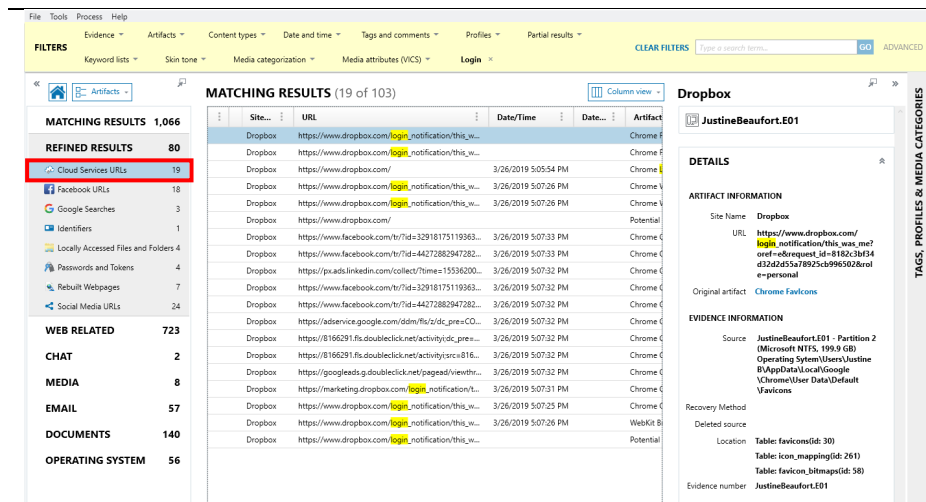
9. Clear all filters after you are done with the exercise and continue to Exercise Question 1.



Exercise Question 1

10. Search for the following terms in the “**search term**” filter bar window, removing each after examining the results:

- a) How many hits on the Keyword “**Login**”



- b) How many hits on the Keyword “**this_was_me**”

The screenshot shows the Magnet AXIOM interface. The top bar includes 'File', 'Tools', 'Process', and 'Help'. Below it, a 'FILTERS' section shows 'Evidence' (43), 'Artifacts' (25), 'Content types' (17), 'Date and time' (3/26/2019 5:07:26 PM), 'Tags and comments' (this_was_me), 'Profiles' (JustineBeaufort.E01), and 'Partial results' (17). The 'MATCHING RESULTS' section shows 17 of 103 results. The 'REFINED RESULTS' section shows 25 results, with 'Cloud Services URLs' highlighted in red. The 'WEB RELATED' section shows 18 results. The 'DETAILS' panel on the right shows information for 'Dropbox', including 'Site Name', 'URL', 'Original artifact', 'Evidence Information', and 'Recovery Method'.

Site...	URL	Date/Time	Artifact
Dropbox	https://www.dropbox.com/login_notification/this_w...	3/26/2019 5:07:26 PM	Chrome Fav...
Dropbox	https://www.dropbox.com/login_notification/this_w...	3/26/2019 5:07:26 PM	Chrome Fav...
Dropbox	https://www.dropbox.com/login_notification/this_w...	3/26/2019 5:07:26 PM	Chrome Web...
Dropbox	https://www.facebook.com/tr/?id=32918175119363...	3/26/2019 5:07:33 PM	Chrome Cac...
Dropbox	https://www.facebook.com/tr/?id=44272882947282...	3/26/2019 5:07:33 PM	Chrome Cac...
Dropbox	https://www.facebook.com/collect/?time=15536200...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://www.facebook.com/tr/?id=32918175119363...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://www.facebook.com/tr/?id=44272882947282...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://adservice.google.com/ddm/fis/z/dc_preCO...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://8166291.fs.doubleclick.net/activity?dc_pre...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://8166291.fs.doubleclick.net/activity?src=816...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://googleads.doubleclick.net/pagead/viewthr...	3/26/2019 5:07:32 PM	Chrome Cac...
Dropbox	https://marketing.dropbox.com/login_notification/...	3/26/2019 5:07:31 PM	Chrome Cac...
Dropbox	https://www.dropbox.com/login_notification/this_w...	3/26/2019 5:07:25 PM	Chrome Cac...
Dropbox	https://www.dropbox.com/login_notification/this_w...	3/26/2019 5:07:26 PM	WebKit Brow...
Dropbox	https://www.dropbox.com/login_notification/this_w...	3/26/2019 5:07:26 PM	Potential Bro...

11. Based on this information, it suggests that the user has a Dropbox account ID and that he has logged into the account. Without further evidence, this cannot be conclusively stated.

12. Clear all filters when you are done with the exercise and proceed on to the next exercise.

The screenshot shows the Magnet AXIOM interface with the 'CLEAR FILTERS' button highlighted in red. The 'FILTERS' section shows 'Evidence' (43), 'Artifacts' (25), 'Content types' (17), 'Date and time' (3/26/2019 5:07:26 PM), 'Tags and comments' (this_was_me), 'Profiles' (JustineBeaufort.E01), and 'Partial results' (17). The 'CLEAR FILTERS' button is located in the top right corner of the 'FILTERS' section.

Exercise 3. Research of Owls

13. We want to see if there are any Google Searches or Parsed Searched Queries related to barn owls.

- b. In the “**Artifacts**” dropdown of the Filter Bar, type the word “**search**” into the Find bar at the top. This will filter the artifact list to only those that have “**search**” in it.

- c. Check “**Google Searches**” and “**Parsed Search Queries**”; click “**Okay**”.
- d. The resulting filter should only show these two artifact categories.
- e. In the “**search term**” filter bar window, key in “**barn owl**” and click “**Go**”.

Exercise Question 2

- a) Select the Google Searches artifact category. How many Google Searches are there related to barn owls?

6

- b) Select the Parsed Search Queries artifact category. How many parsed searches are there related to barn owls? What social media platform did the user conduct these searches on? **7. The social media platform used by the user to conduct these searches on is Facebook.**

The screenshot shows the Magnet AXIOM Examine v3.10.0.18500 interface. The 'FILTERS' pane on the left shows 'Parsed Search Queries' with 7 results. The 'MATCHING RESULTS' pane shows 7 of 230 results for the search term 'barn owls'. The results are listed in a table with columns for Search Term, URL, Date/Time, and Date. The search term 'barn owls' is highlighted in yellow. The details pane on the right shows the artifact information for 'barn owls', including the search term, URL, search engine (Facebook), and evidence information.

- c) Key “Eggs” into the “search term” filter bar window, How many artifacts are shown in Google Searches? Remember to clear filters before search. **19**

The screenshot shows the Magnet AXIOM Examine v3.10.0.18500 interface. The 'FILTERS' pane on the left shows 'Google Searches' with 19 results. The 'MATCHING RESULTS' pane shows 19 of 194,998 results for the search term 'where to buy owl eggs'. The results are listed in a table with columns for Search Term, URL, Date/Time, and Date. The search term 'where to buy owl eggs' is highlighted in yellow. The details pane on the right shows the artifact information for 'where to buy owl eggs', including the search term, URL, search engine (Google), and evidence information.

Exercise 4. Rebuilt Webpages

14. The category of Rebuilt Webpages pulls information from the Web Cache of the computer and attempts to reassemble all parts to display a web page as the user saw it. Be patient, as it takes approximately 30 to 60 seconds for a page to be rebuilt and displayed.
15. Under “**Refined Results**”, click on the artifact category “**Rebuild Webpages**”.
16. In the “**search term**” filter bar window, key in the keyword “**pets**” and click “**Go**”.
17. Click on the page “**Owls as Pets – International Owl Center**”.
18. This will then display the web page as the user saw it.

Exercise Question 3

- a) What browser was the user using when they went to this page?

The user was using google chrome as their browser when they went to this page.

- b) What date/time did the user go to this page?

3/26/2019 4:56:28 PM

The screenshot shows the Magnet AXIOM v3.10.0.18500 interface. The 'FILTERS' section on the left includes 'Artifacts' with 'Rebuilt Webpages' selected. The 'MATCHING RESULTS' table shows 5 results. The first result is 'Owls as Pets - International Owl Center - International...' with a URL 'https://www.internationalowlcenter.org/owlsas/pets...' and a 'Created' date of '3/26/2019'. The 'DETAILS' section on the right shows the 'ARTIFACT INFORMATION' for this result, including the 'Created Date/Time' of '3/26/2019 4:56:28 PM', the 'Domain' of 'www.internationalowlcenter.org', and the 'Cache Table' of 'Chrome Cache Records'. The 'Cache RowID' is '155396'.

Please answer all the above questions, exercise 1 to exercise 3 and submit your answers to blackboard / Learning Resources, “Lab Exercise Folder” for class participation marks. You document should be named as “<Name><StudentID>Lab2A”. Example: John123456Lab2A.

-- End --