School of Computing
IT8003 Digital Forensics and Investigation

Practical 2A: Refined Results on Magnet AXIOM Examine

Introduction

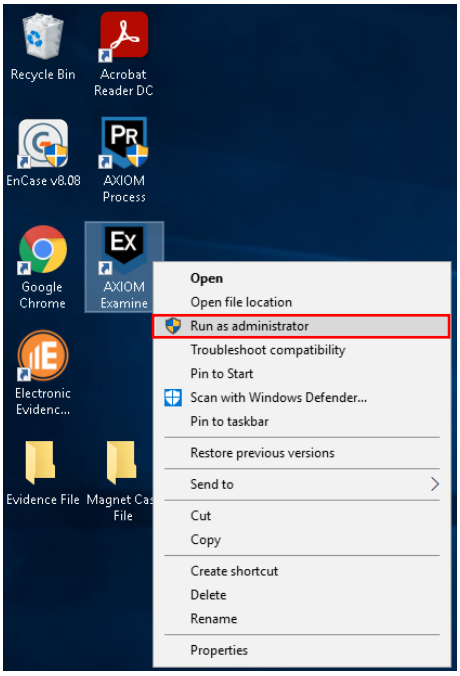
Performing keyword and searching can help a forensic examiner to narrow down the relevant artifacts during analysis. Thus, it is important for a forensic examiner to understand the case background and build a list if search term which can identify evidence that is relevant to the matter. Refine you search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

Learning Objective

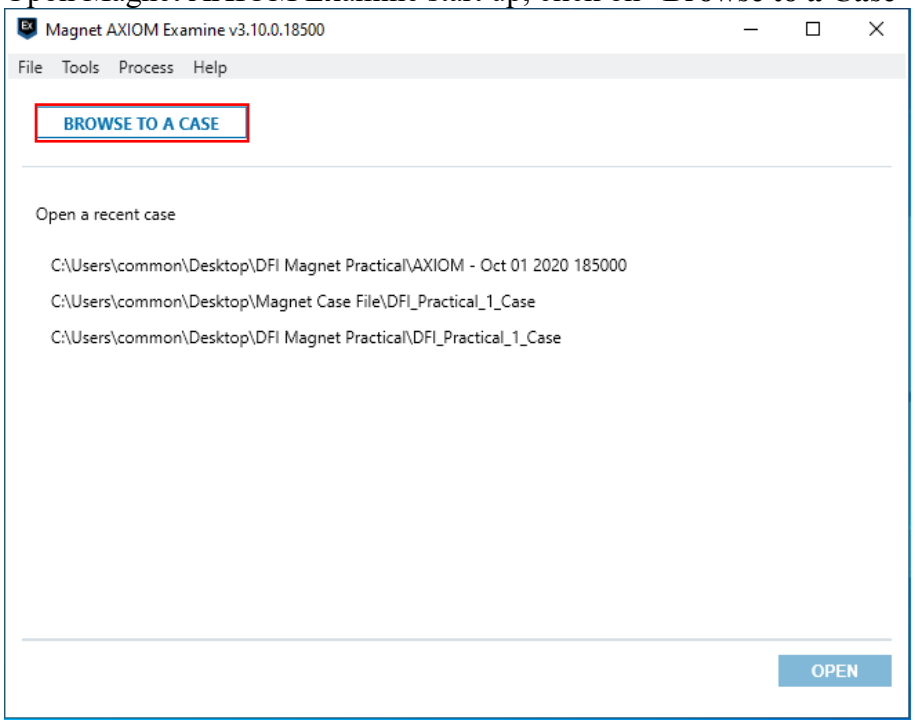
In this lesson, students will take part in lectures, instructor-led exercises, and student practical exercises to learn the way in which Magnet AXIOM Examine organizes artifacts within the Refined Results parent category. Students will be able to perform and examine sources of searches such as Google 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

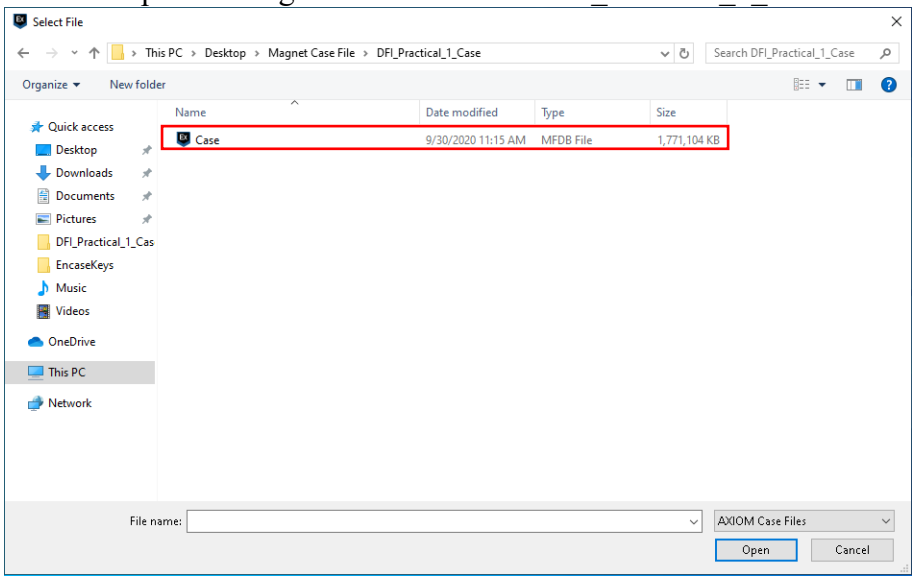
1. Open the application "**Magnet AXIOM Examine**". (Note: right-click on "**Magnet AXIOM Examine**" icon and run as administrator)



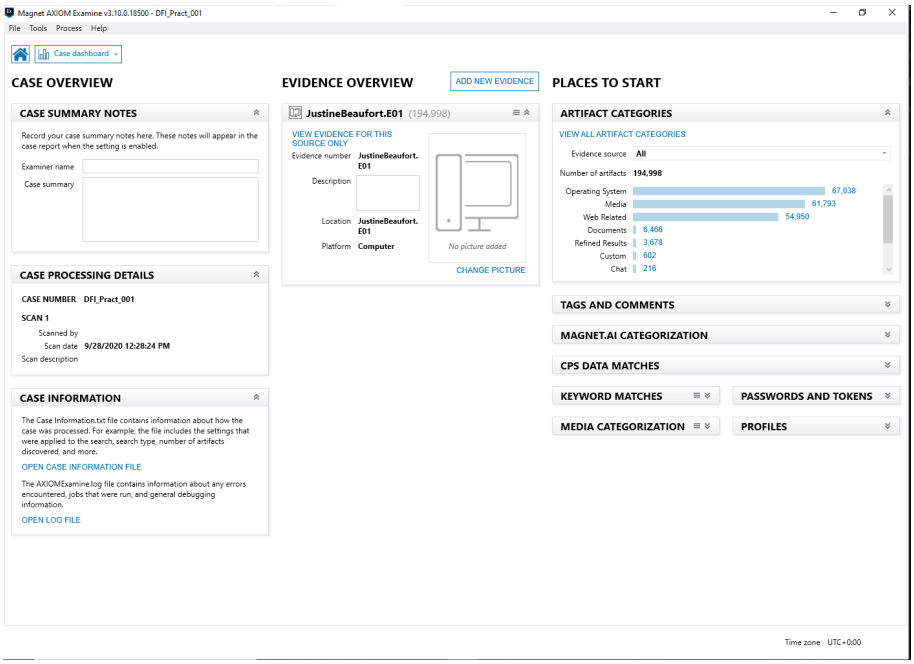
2. Upon Magnet AXIOM Examine start up, click on "**Browse to a Case**"



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 an 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.

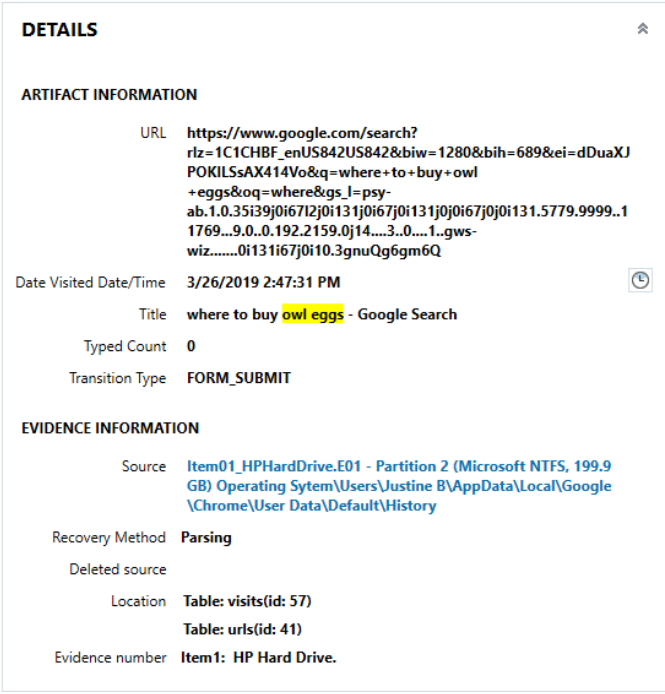


Figure 3-1-7: Details Card for A Google Search

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

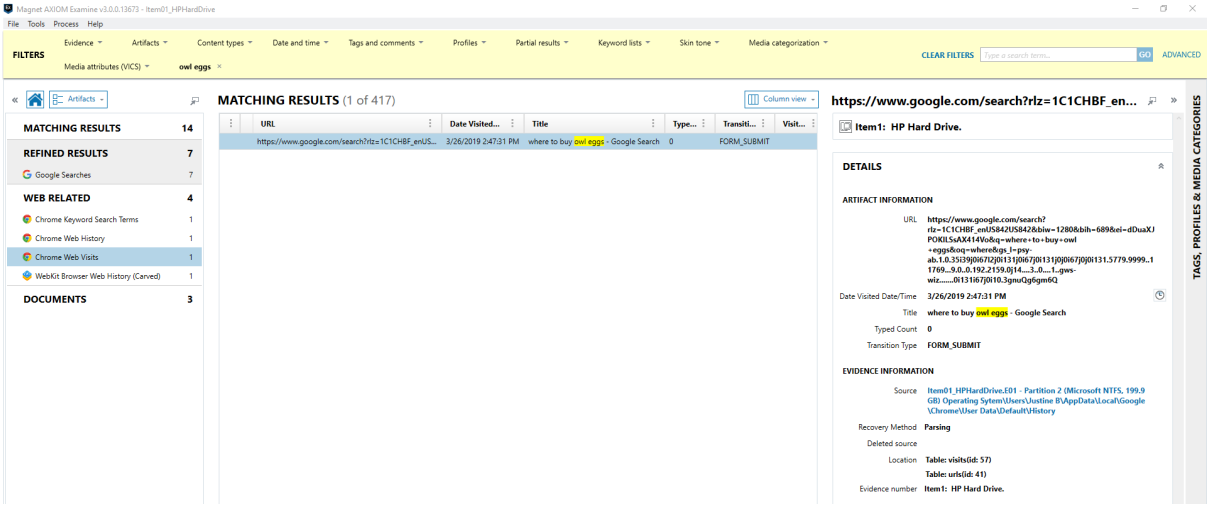


Figure 3-1-8: Filters Applied

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.

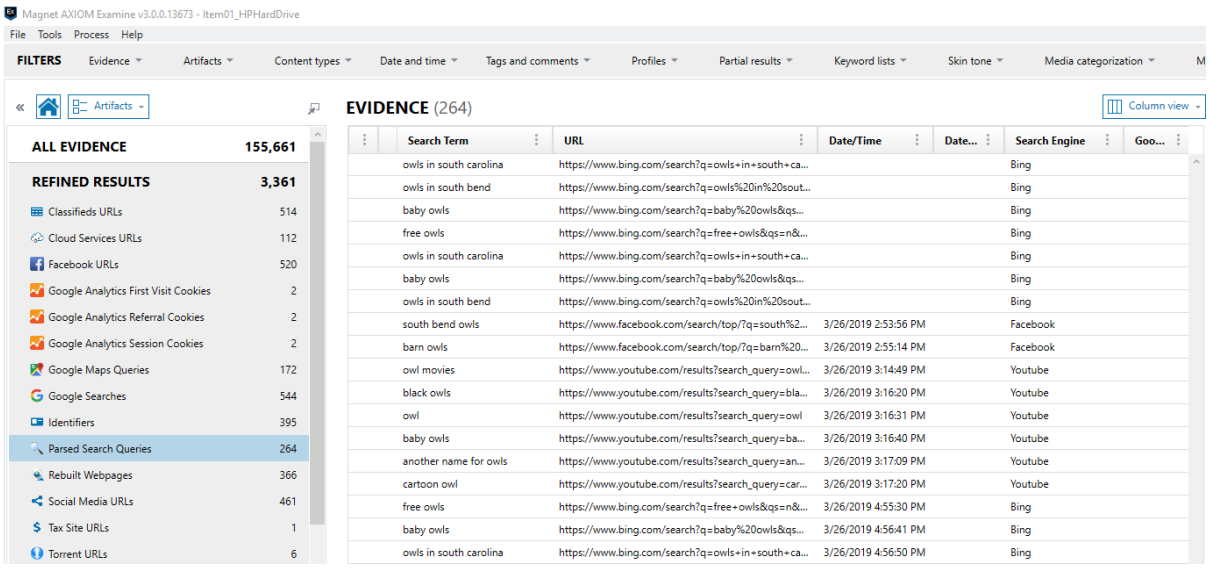


Figure 3-1-12: Evidence Pane Of Parsed Search Queries

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.

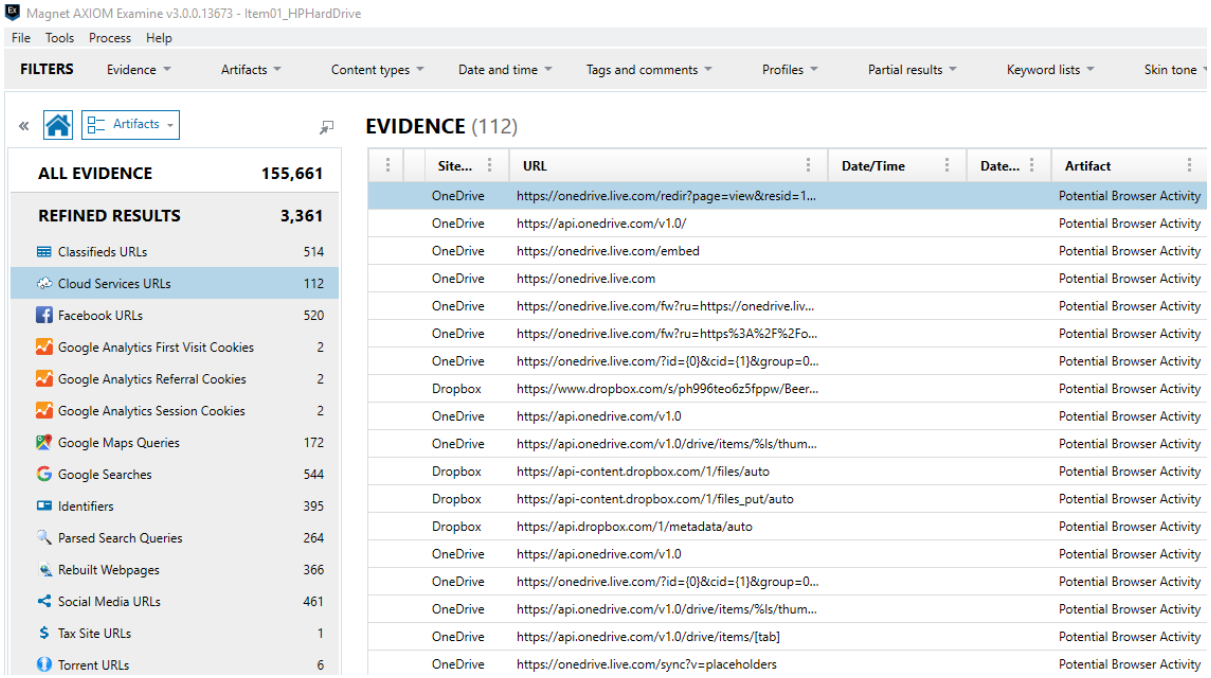
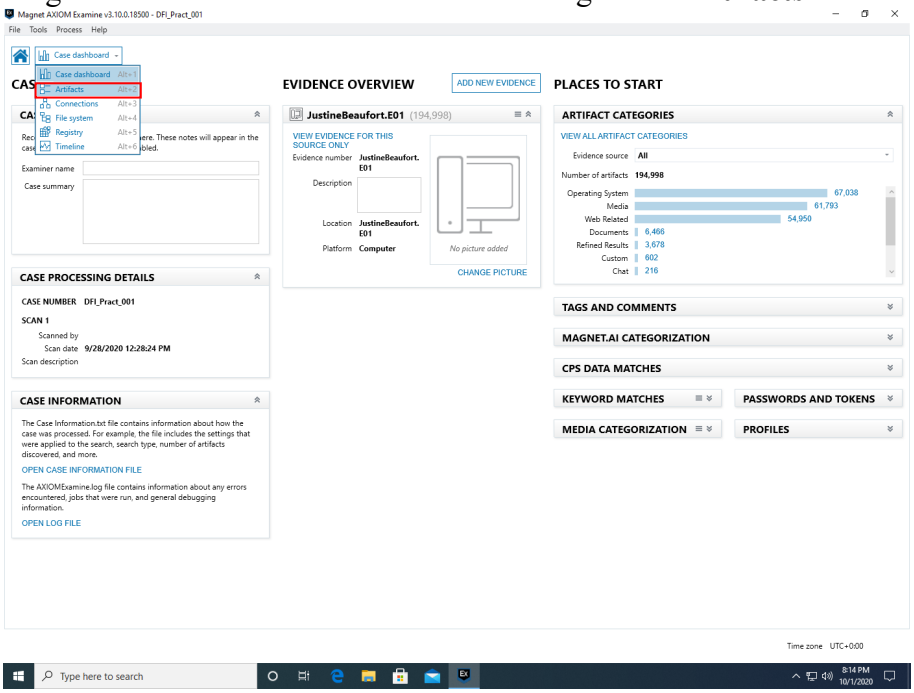


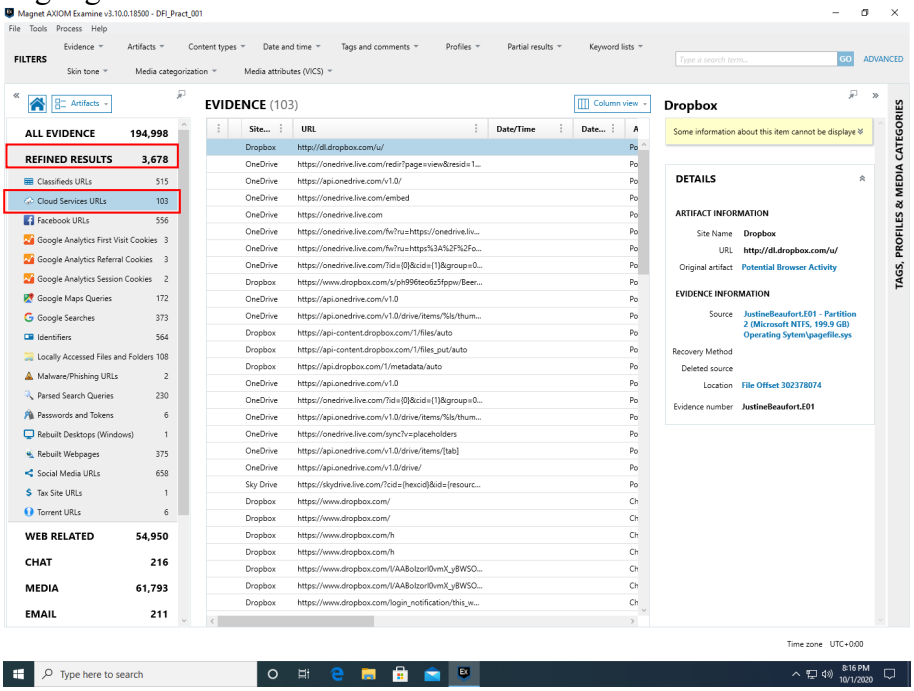
Figure 3-1-14: Cloud Services Urls

Exercise 2. Determining Dropbox Usage

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

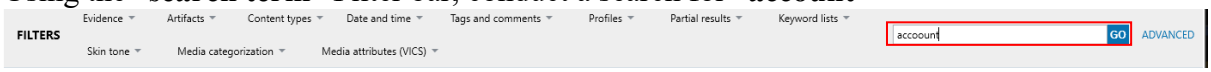


6. Highlight the "**Refined Results**" –> "**Cloud Services URLs**" artifact category.

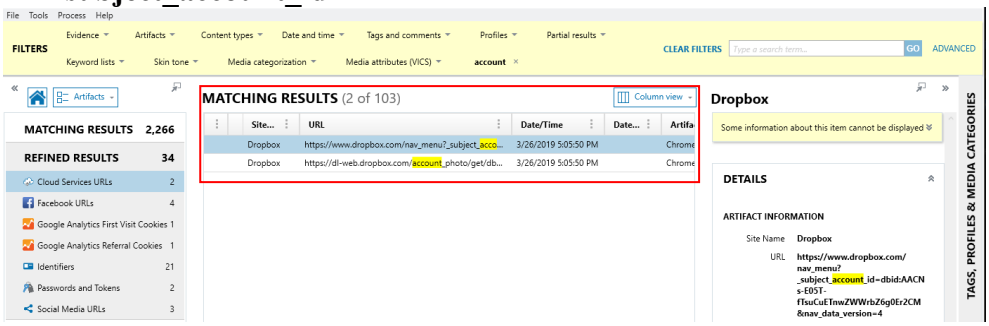


7. We want to see if we can determine the account associated with the Dropbox account and if the user has logged in and/or downloaded any materials from Dropbox.

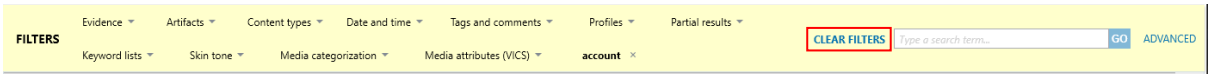
8. Using the "**search term**" Filter bar, conduct a search for "**account**"



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



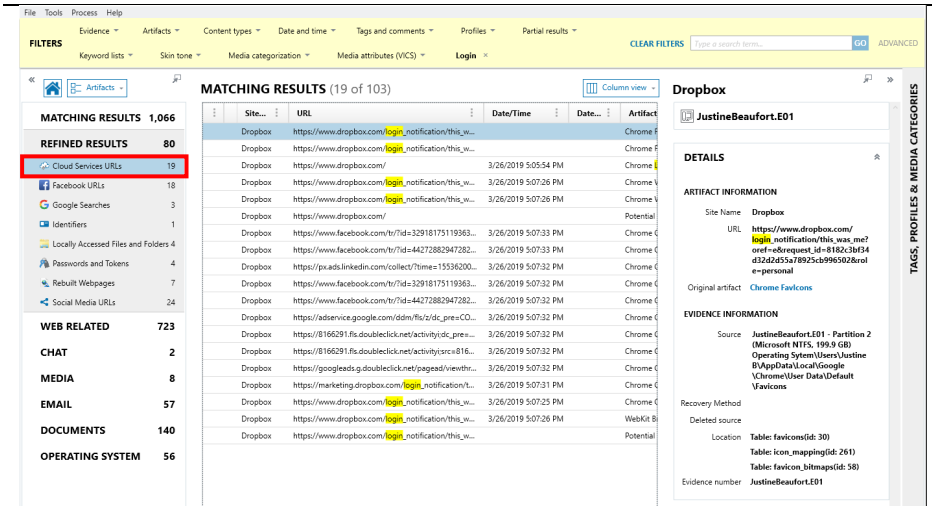
9. Clear all filters after you are done with the exercise and continue to Exercise Question 1.



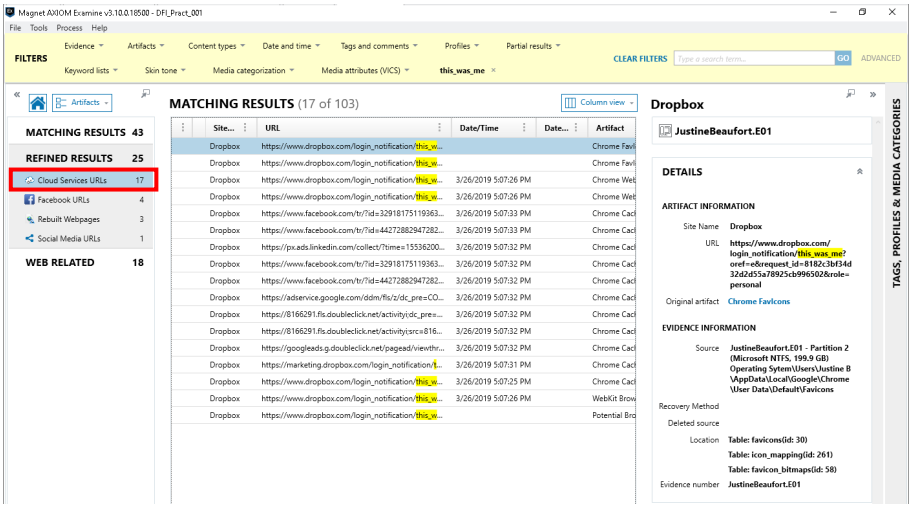
Exercise Question 1

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

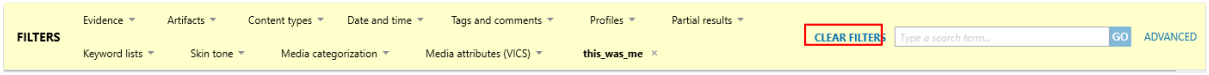
a) How many hits on the Keyword "**Login**" 19



b) How many hits on the Keyword "**this_was_me**" 17

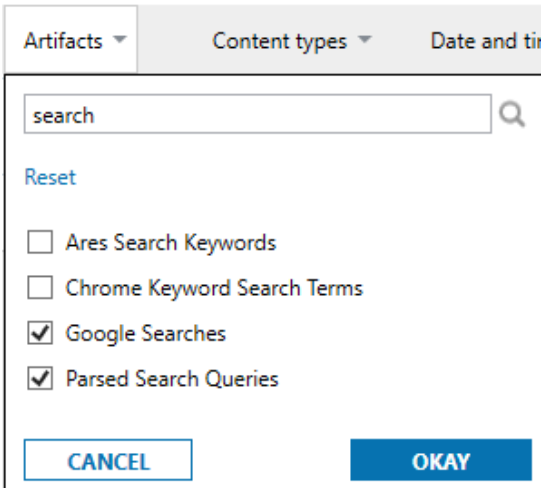


11. Based on this information, it suggests that the user has a Dropbox account ID and that he has logged into the account. Without further evidence, this cannot be conclusively stated.
12. Clear all filters when you are done with the exercise and proceed on to the next exercise.



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.

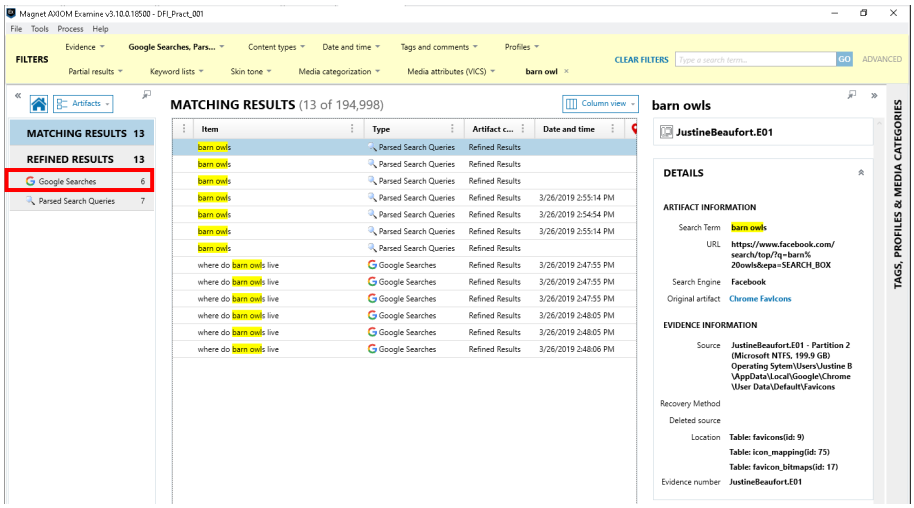


    c. Check "**Google Searches**" and "**Parsed Search Queries**"; click "**Okay**".
    d. The resulting filter should only show these two artifact categories.
    e. In the "**search term**" filter bar window, key in "**barn owl**" and click "**Go**".

Exercise Question 2

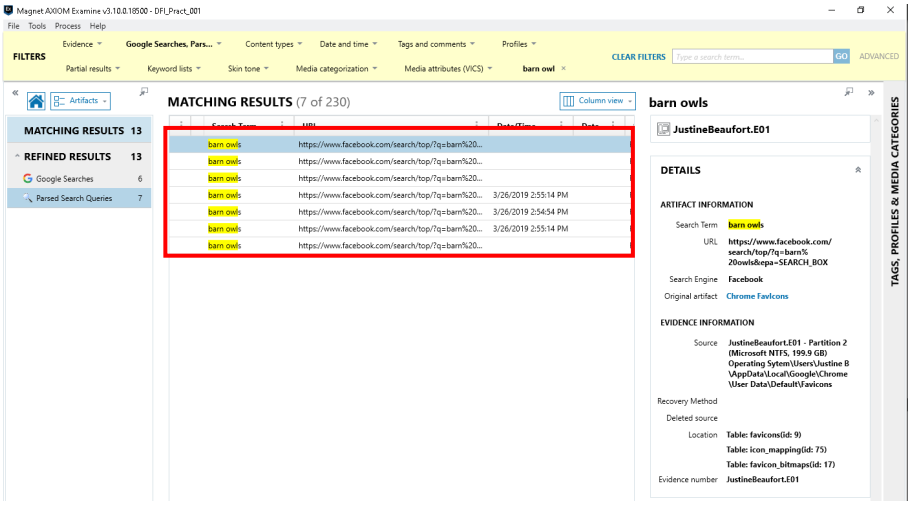
a) Select the Google Searches artifact category. How many Google Searches are there related to barn owls?

6



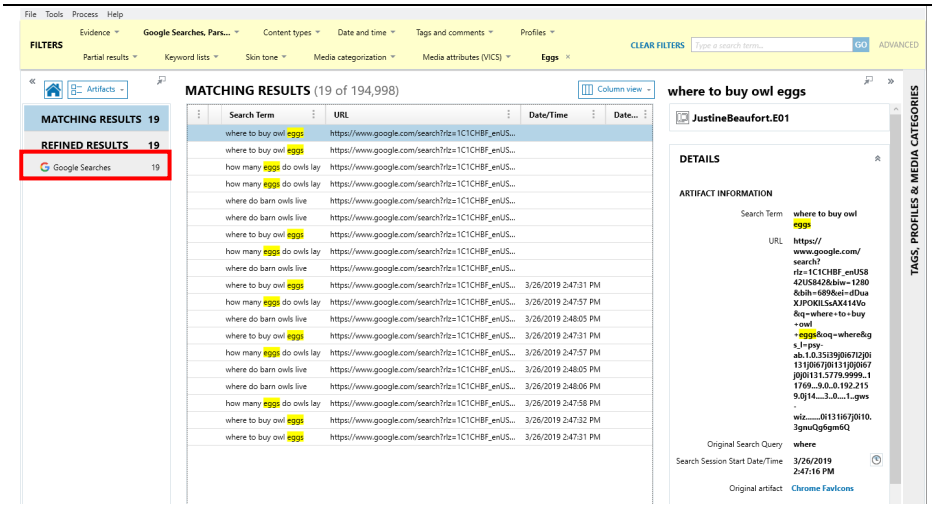
b) Select the Parsed Search Queries artifact category. How many parsed searches are there related to barn owls? What social media platform did the user conduct these searches on?

7. The social media platform used by the user to conduct these searches on is Facebook.



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



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.

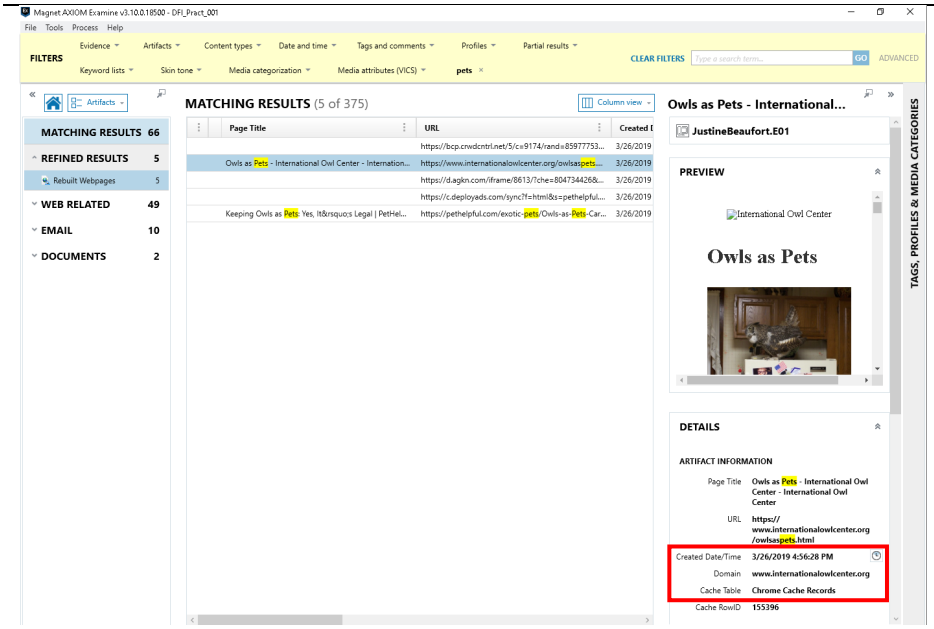
Exercise Question 3

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



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 --