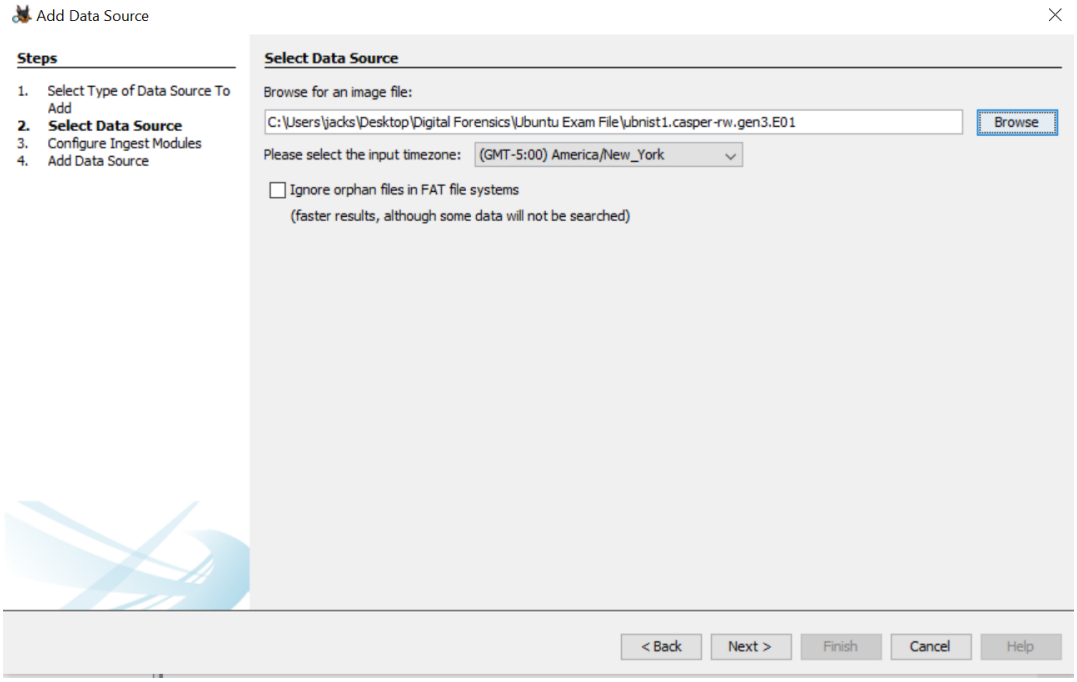
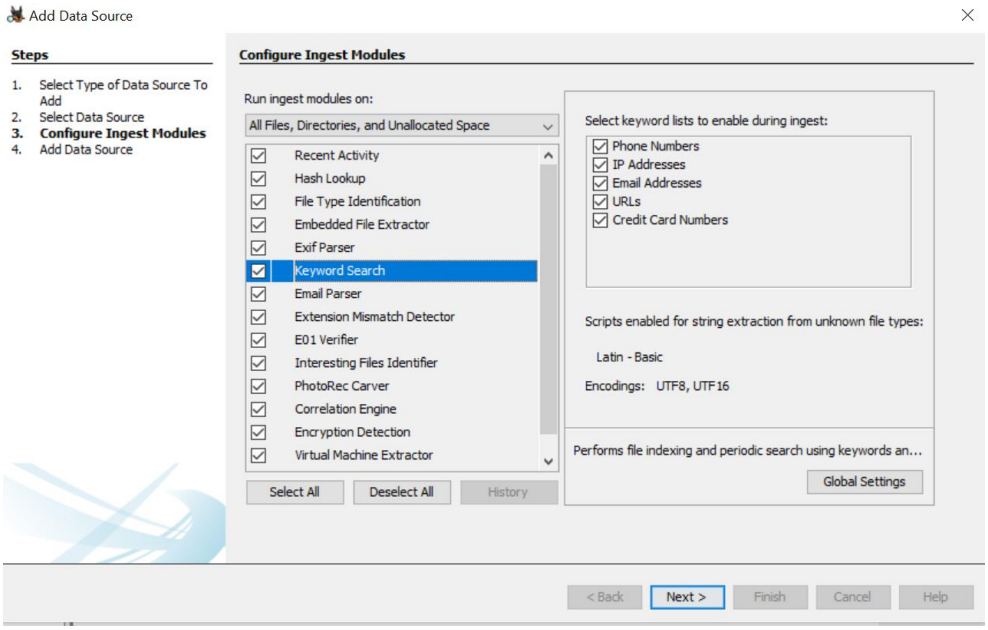
Digital Forensics Investigation II

The second digital forensics module continues the examination of evidence files. It starts of by having the students create a second case and upload a new evidence file. While it loads, it explains how data analysts securely generate an evidence file from a hard drive or USB drive, along with the importance of using a write blocker when generating these files. This module also gives a brief introduction to data carving, or the process of extracting information from deleted files. Moreover, it teaches students how to access archived files, and extract files from a zip file as an example. In addition, the module explains how to view the data after it is sorted by file type and discusses how to view documents based on the system it was created in, such as documents from Microsoft Office. This module shows students how to use the media viewer to view images and videos. It also demonstrates how to generate a timeline from the timestamps Autopsy extracts from the data in the evidence file. The session concludes by showing the students how to generate a report from all the materials they viewed.

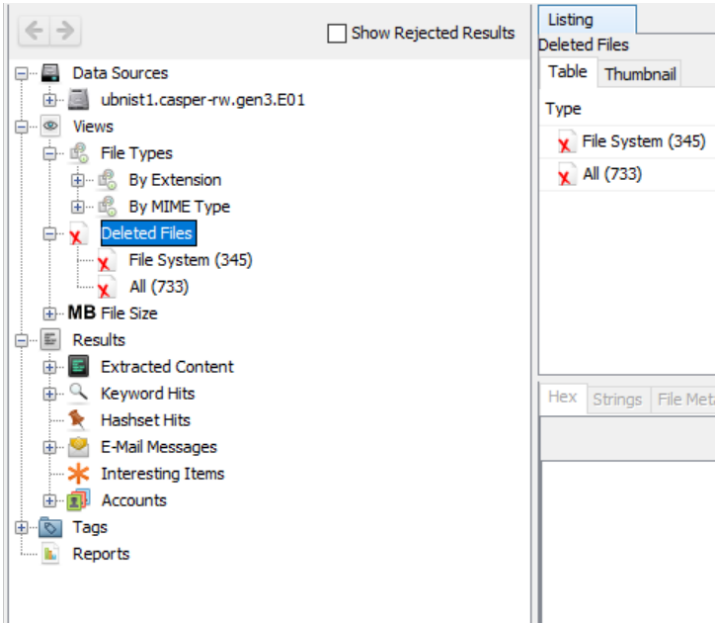
1. We will begin this module by opening a new case. So first open Autopsy. Then click create new case and select a directory of wherever you want the file to be located. Then fill in the examiner information, and finish creating the new case. Next, we will want to upload the evidence file for examination. The file we'll be using for this case is titled "ubinst1.casper-rw.gen3.E01"



2. After selecting the file, make sure that all the boxes on the screen titled "Configure Ingest Modules" are checked. Scroll down to where it says, "Keyword Search", and make sure all the sub boxes are checked as well. Then, click next and finally finish.

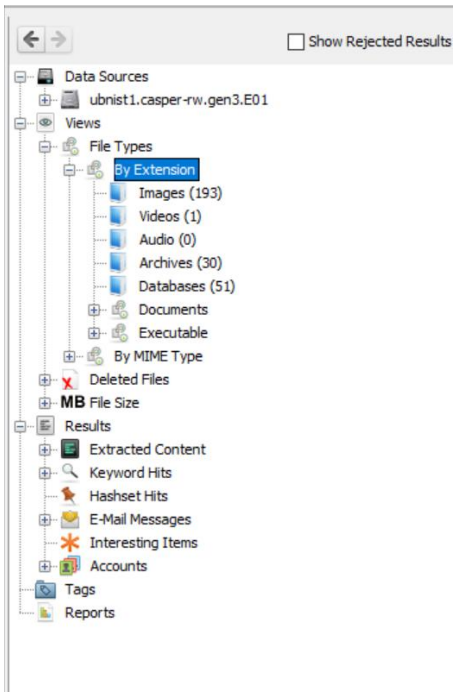


3. This will take a couple minutes to load in the mean time we will discuss a few things. Last time, we examined a basic evidence file. But how are evidence files made? Evidence files are what are referred to as “Images” of a hard drive. Using a tool like FTK Imager (Forensic Toolkit Imager) this allows a data analyst to take a suspect hard drive or flash drive and convert it into a file that can be analyzed.
4. In the real world and forensic analyst would use something called a write blocker. A write blocker is a device or a piece of software that would allow you to access the data for file conversion, but not allow the device to access your computer. The purpose of this would be to keep any viruses, malware, or other harmful data from entering your computer.
5. File Carving is the process of analyzing known file types, in the internal file management system. Data Carving is the process of analyzing files that are not known. Most of the time it is because the files have been deleted but not re-written over yet. In the standard spinning disk hard drive, data is stored in sections using a process that converts data into magnetized sections which holds the data. When information is deleted, it still lingers there until data is written back over it. When it never gets rewritten, this allows Autopsy to extract the “deleted” data.
6. As you might imagine criminals are not going to want to keep data around that could incriminate themselves, so they delete it. Sometimes this deleted data is what can make or break a case. It could link someone to a crime, or in cases of owning things like child pornography could prove their quilt. This is a tool many different cases are going to need to help them prove or disprove their case.
7. Hopefully by now, the files are fully loaded in, so we can start our examination. First let’s look at deleted files. Let’s expand where it says “Views”, then “Deleted Files”. As you can see there is 345 in the File System, but 733 overall. Take a couple minutes to look through these and see what you can find.

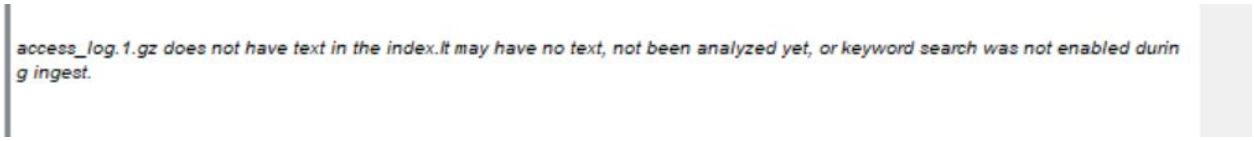


8. As you might notice some of these files don’t really make any sense. This could be for several different reasons. The file could be encrypted, the file may not be complete, part of the file could have been written over resulting in a incomplete file, or the file may be for system settings, or part of some program. Like the .xml extension is for web development.

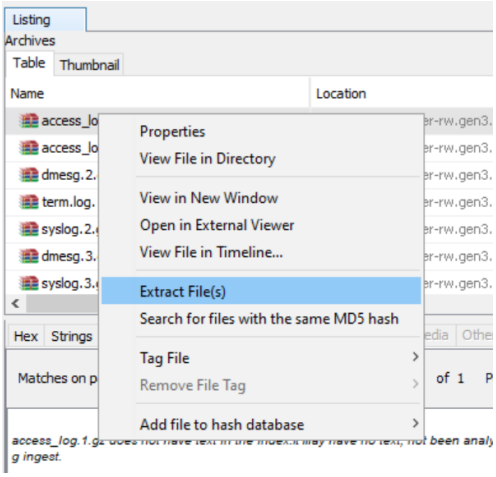
9. Autopsy likes to make data as easy to view as possible. By clicking “Views” then “File Types” and finally “By Extension”, this allows you to see what file types are available. For example, there is 193 images, a video, 30 archives (Things like Zip files), and 51 Databases. Take some time to look through these files.



10. Many of the archive files give you a message like this:



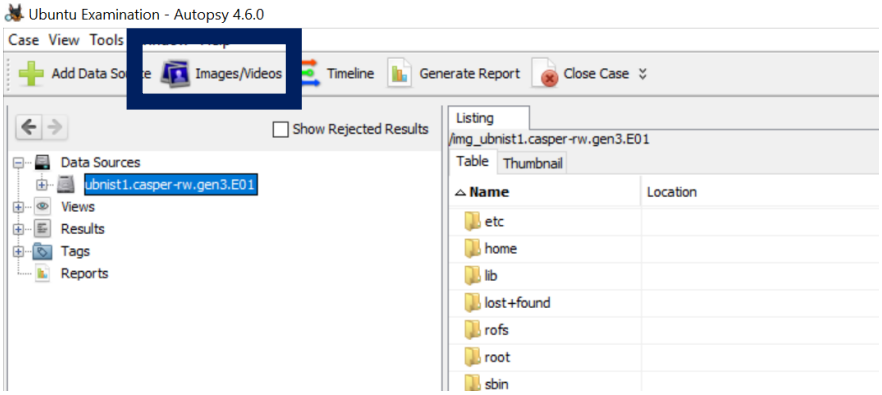
11. However, we can still look through these files. In order to do this let’s make a folder on the desktop, and label in Autopsy Things or something along those lines. You can make a folder by right clicking on the desktop, clicking new, and then folder.



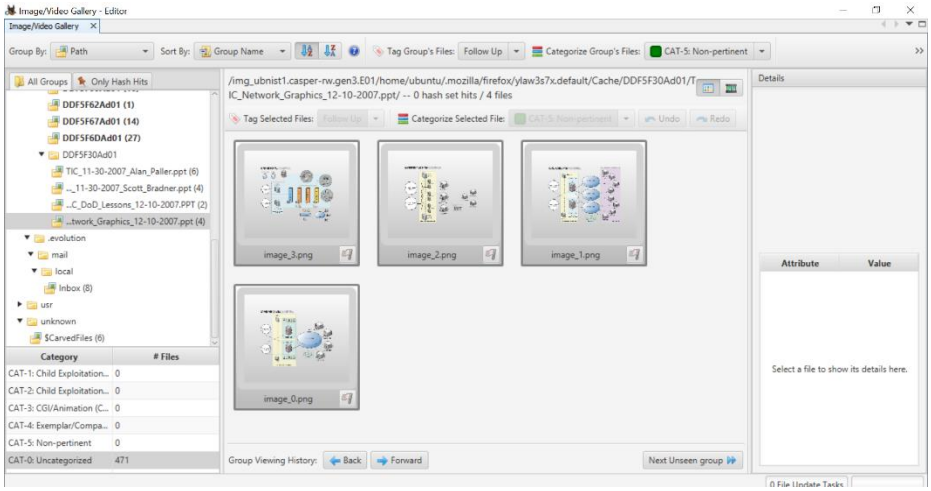
12. Next, lets right click on one of the archive files in Autopsy. I recommend the "Trusted_Internet_Connections.zip". Then click on where it say's "Extract File(s)". Then select the folder you just made on the desktop. And finally click save. You can now open the Zip file and view the contents like you would anything else in windows. We can gain some useful information here, such as the file name, file type, and the date it was modified.

Name	Type	Compressed size	Password pr...	Size	Ratio	Date modified
TIC_11-30-2007_Alan_Paller.ppt	Microsoft PowerPoint 97-200...	420 KB	No	742 KB	44%	11/30/2007 9:34 AM
TIC_11-30-2007_Scott_Bradner.ppt	Microsoft PowerPoint 97-200...	734 KB	No	845 KB	14%	11/30/2007 9:34 AM
TIC_DoD_Lessons_12-10-2007.PPT	Microsoft PowerPoint 97-200...	256 KB	No	349 KB	27%	12/10/2007 12:31 PM
TIC_Implementation.pdf	PDF File	22 KB	No	29 KB	27%	11/30/2007 9:34 AM
TIC_Network_Graphics_12-10-2007.ppt	Microsoft PowerPoint 97-200...	1,267 KB	No	1,321 KB	5%	12/10/2007 10:46 AM
TIC_Planning_Guidance.pdf	PDF File	39 KB	No	52 KB	25%	12/6/2007 3:51 PM
TIC_Template.xls	Microsoft Excel 97-2003 Wor...	19 KB	No	110 KB	83%	12/6/2007 3:51 PM
TIC_Timeline_11-23-2007.ppt	Microsoft PowerPoint 97-200...	13 KB	No	56 KB	78%	11/30/2007 9:34 AM

13. Instead of using the file extension tab to view images, Autopsy provides a built-in tool to do this. In the upper left- hand corner you can see a button called "Images/Videos".

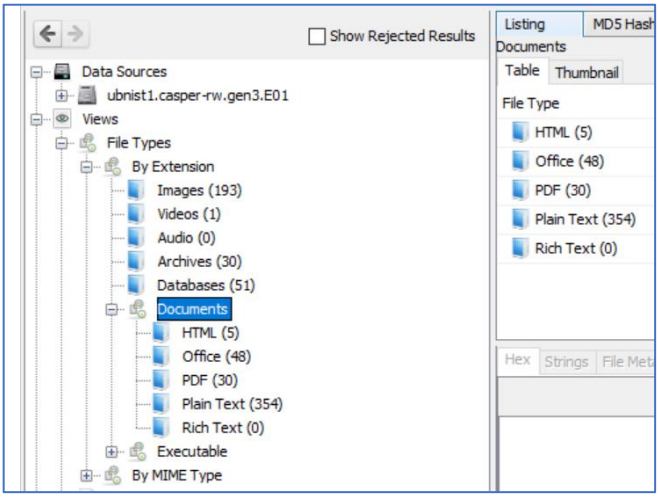


14. When you click it, it should bring you to a screen like this…



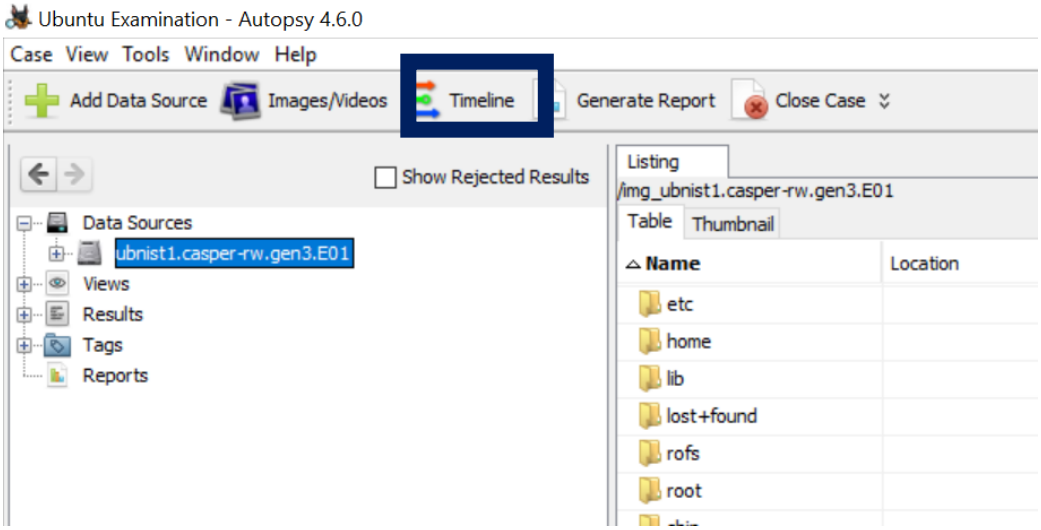
15. Here you can see how many photos there are, and what category they fall in. This can be a useful tool, for finding photos, where they are, and a secure place to view media.
16. Going back to viewing data by file type, you can also view documents by what program was used to create them. By expanding the tab named "File Types", Then "By Extension", and finally "Documents". Here you can see that there are 5 HTML documents, 48 Office Files, 30 PDF's, and

354 Plain Text documents. Take a few minutes to look through these documents and see what you can find.

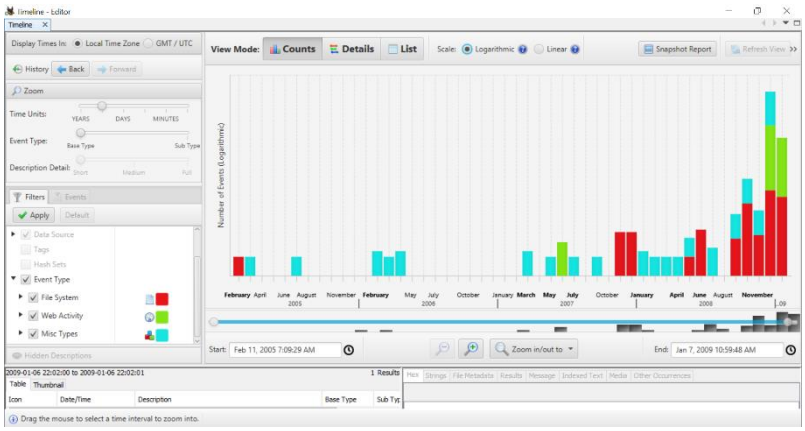


17. As you can see this tab includes files that have been deleted. It also shows files that may be in other languages, so you may need a translation program if you want to fully read and understand what the file says.

18. In the upper left corner there is a button labeled “Timeline”, and it allows you to see when all the files were accessed.



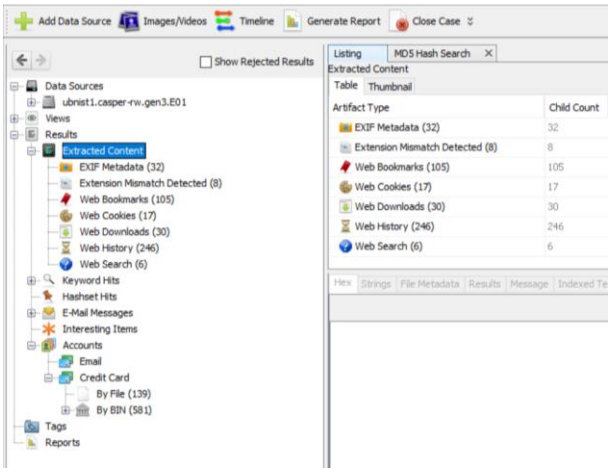
19. After clicking it, you should see this screen.



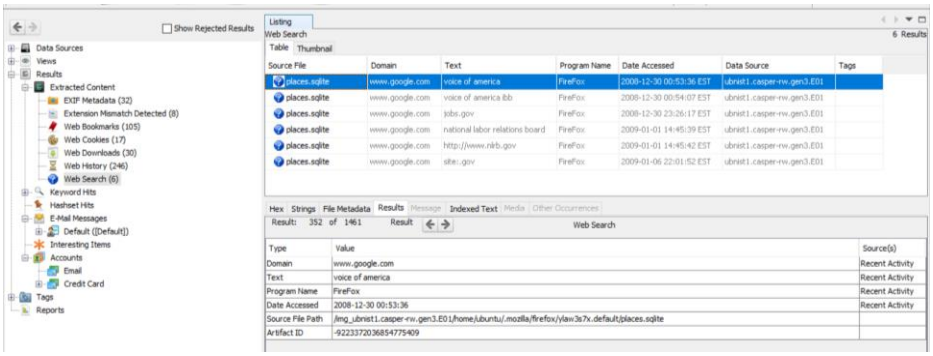
20. This is useful for seeing when data was accessed and gives a nice color-coded scheme for viewing different data types. Take a few minutes and see what you can gather from this data.

21. By changing from the logarithmic scale to a linear scale, you can see a physical change in the picture. The detail list also offers a unique look. Each of these modes has their own advantages. The standard bar graph style view offers a good perspective for viewing the timeline as a whole. The detail view is great for viewing the data if you want to see the day, month, and year it was accessed.

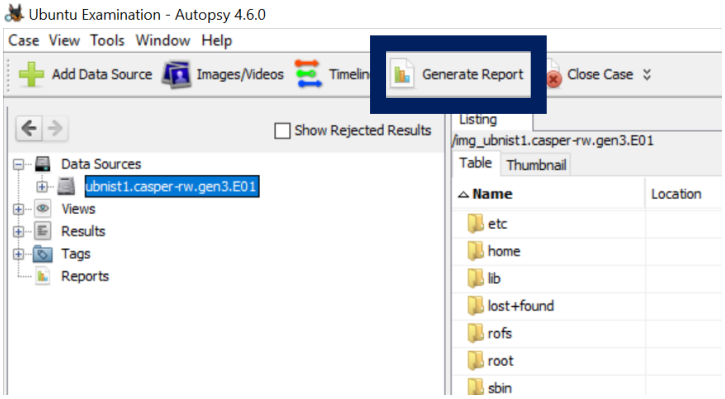
22. Much like the previous module we can view the extracted content. If you expand the “Results” tab, then “Extracted Content” you can view more content. In this file, we can see content that a web browser would generate.



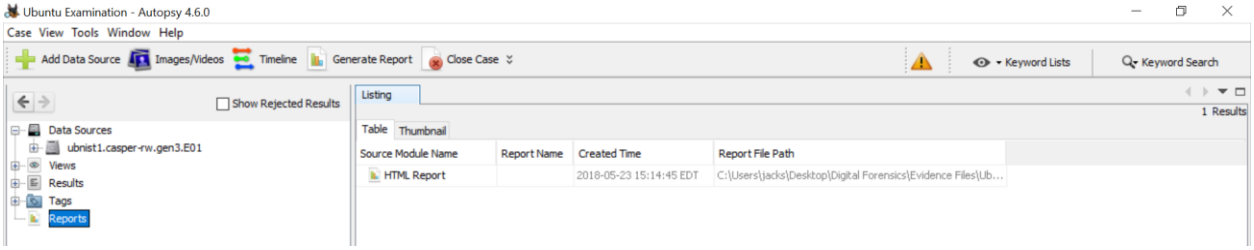
23. This content includes: EXIF Metadata, Extension Mismatches, Web Bookmarks, Web Cookies, Web Downloads, Web History, and Web Searches. If we look at web searches we see this. As you can see this person used the Firefox web browser, they searched “voice of America”, into Google and you can see the date they did this.



24. By clicking the “Generate Report” button, you can view a report of the file you just looked through.

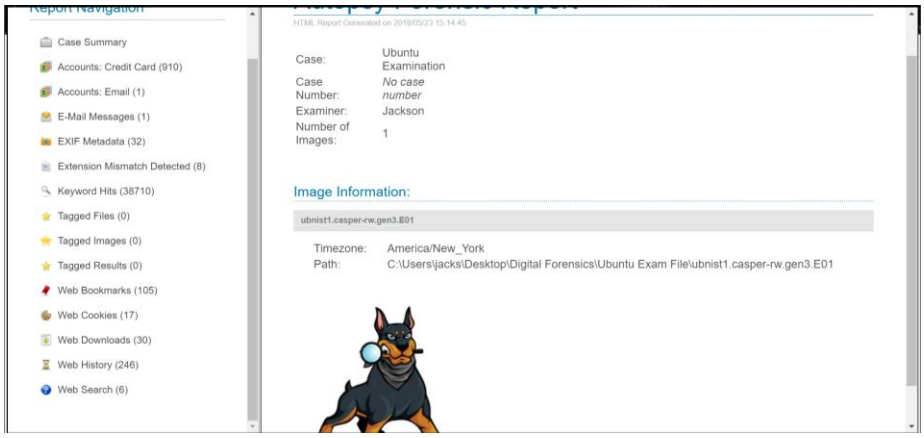


25. After clicking it you should see this…



26. Keep the report format as HTML and then let it process. When it’s done you can find it under the reports button. After clicking on the report, it should open it up in an internet browser.

27. It should look like this



28. If you want to learn more, Google is a great place to start. This is just the tip of the iceberg, there is so much more to learn and hopefully this developed interest in Digital Forensics. You can also find more information in a handout in this binder.