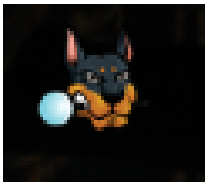
Introduction to Digital Forensics Investigation I

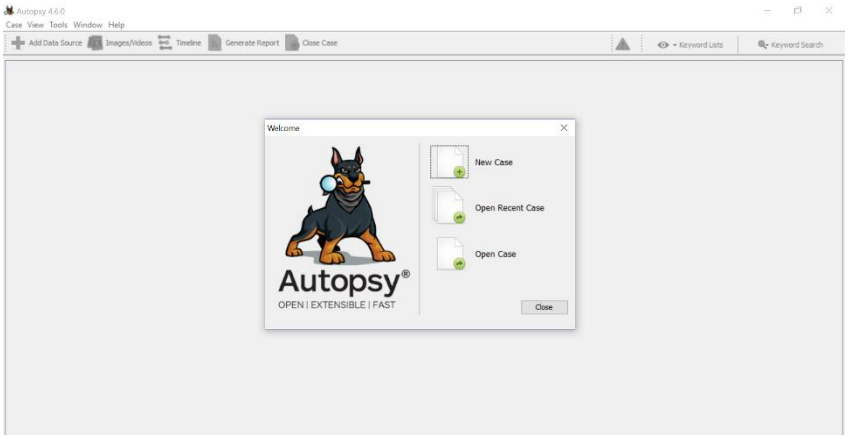
The first digital forensics module gives a brief history of digital forensics and how it progressed into the modern-day version. It also explains what digital forensics is, the role it plays in our society, and an understanding of the professionals who uses it. This module uses the free tool Autopsy to analyze an evidence file to teach students about digital forensics. It teaches students how to open a new case, upload an evidence file and start analyzing it. It also gives a brief explanation of the hexadecimal system and how it correlates with computer files. This includes the explanation of how numbers can be used to represent letters and symbols by using ASCII code. Moreover, it teaches students how to learn from the information that Autopsy extracts such as email addresses and how to view detailed information about them. This detailed analysis continues with phone numbers, URL's, credit card numbers, and banking identification numbers. This session also explains how Autopsy uses an advanced series of keyword searches to find these things, and the files that it extracts them from.

Digital Forensics Module I Notes

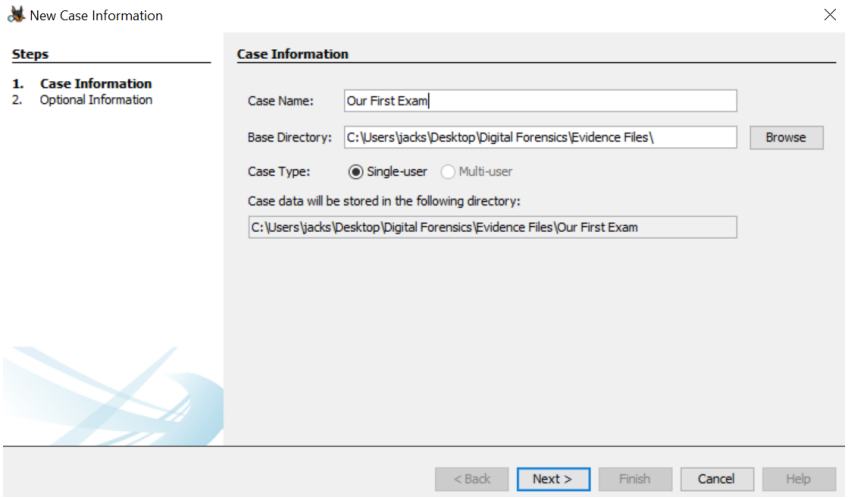
- In this module we will learn about digital forensics through a program named Autopsy. You can find a download link for it here, https://www.sleuthkit.org/autopsy/ . The version you will need will depend on the type of windows you are using at home. It comes in both a 32-bit and 64-bit version.
- So, what is digital forensics?
    - Digital forensics is a branch of forensic science that involves the recovery and investigation of materials found in digital devices. Digital forensics can be used to investigate networks, hard-drives, data bases, mobile devices, and many more things.
    - This is important because computers are everywhere and almost everyone uses them. Digital forensics is used to link criminals to crime by tracking their digital footprint (we all have one). It is used to help aid the criminal justice system by linking people to forms of cybercrime or can link them to a physical crime. It all depends on the crime being committed.
    - The police, various forms of the government (such as the FBI, DEA, NSA and others), and cyber security professionals use digital forensics in their day to day routines.
- Getting started
    - To get started with a digital forensic investigation we first need to launch Autopsy. There should be an icon on the desktop that looks like:



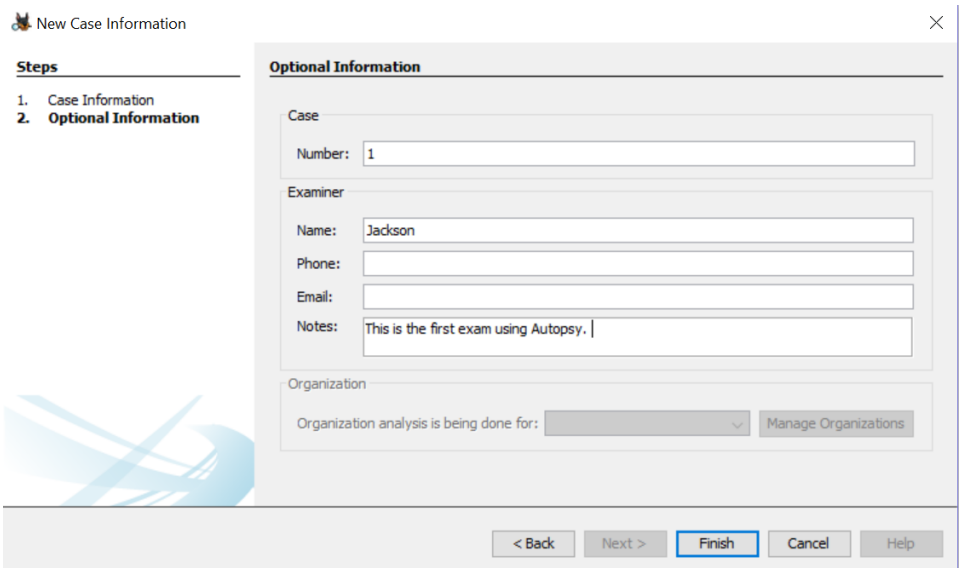
    - When it opens you should see this screen:



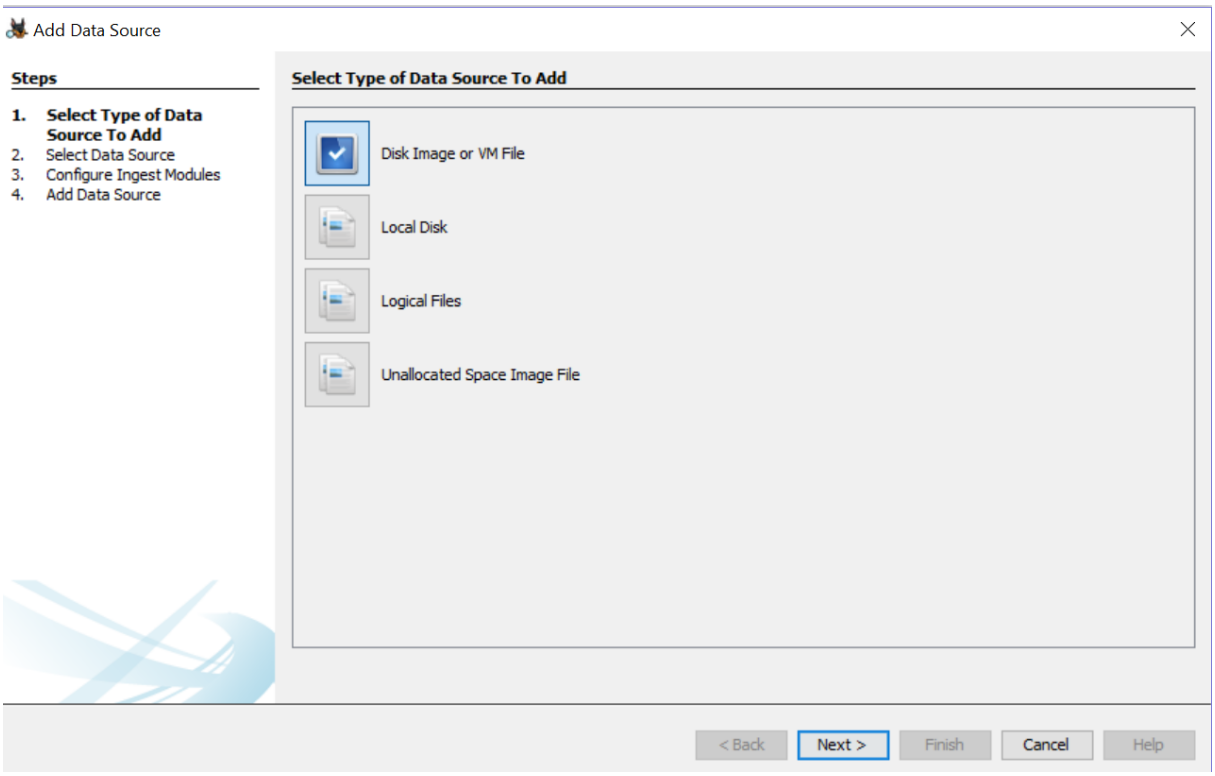
    - You are going to want to click on the button that says, “New Case”, you should then see this:



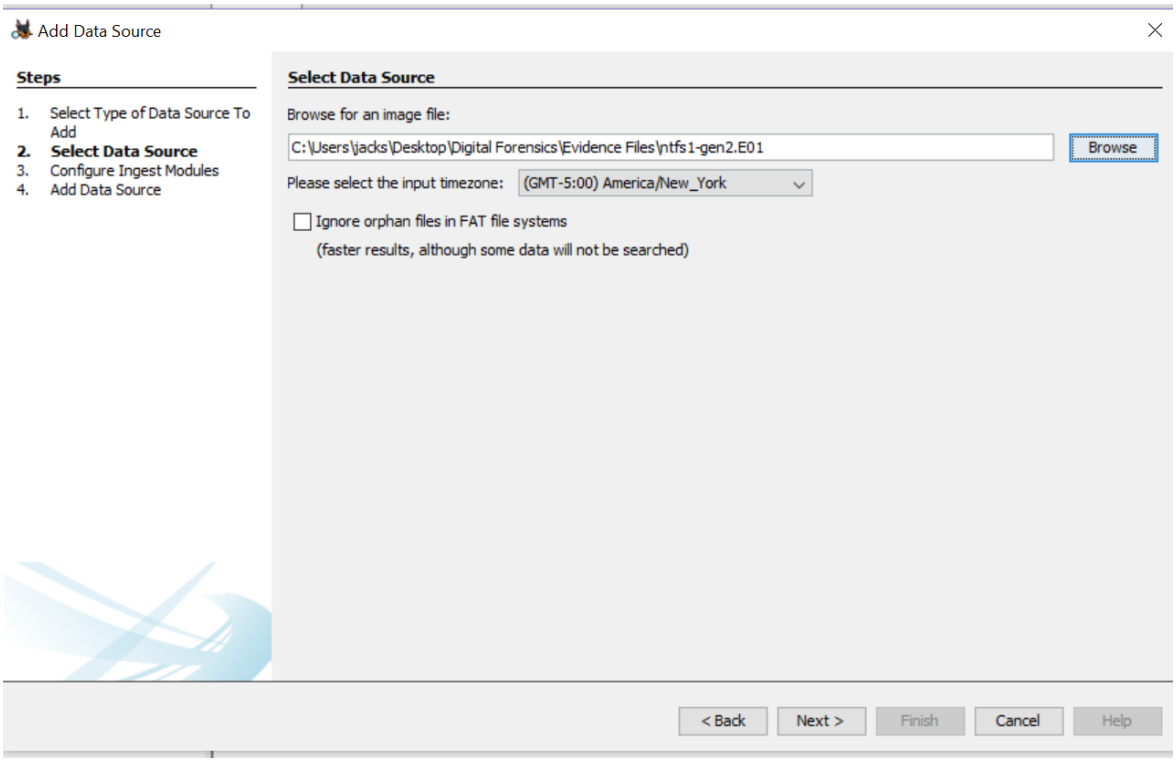
- You should now name your case. Then you will want to select a folder to put the Autopsy file in, I recommend making a folder on your flash drive, so that way you can open it on any computer you want. Then click next.



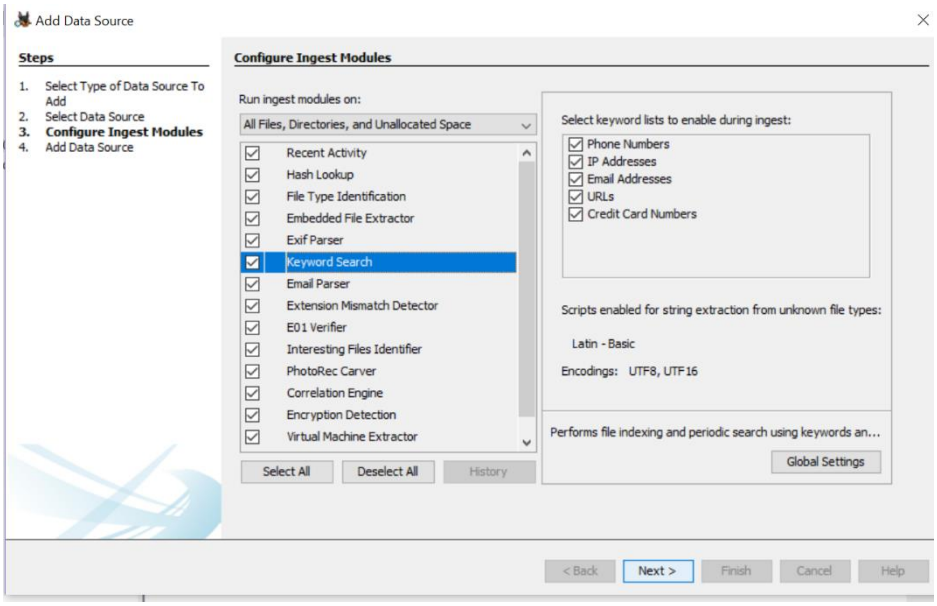
- On this next screen enter in information such as the case number, examiner name, a phone number, email address, and any notes you want to include that may be useful to identify the case.



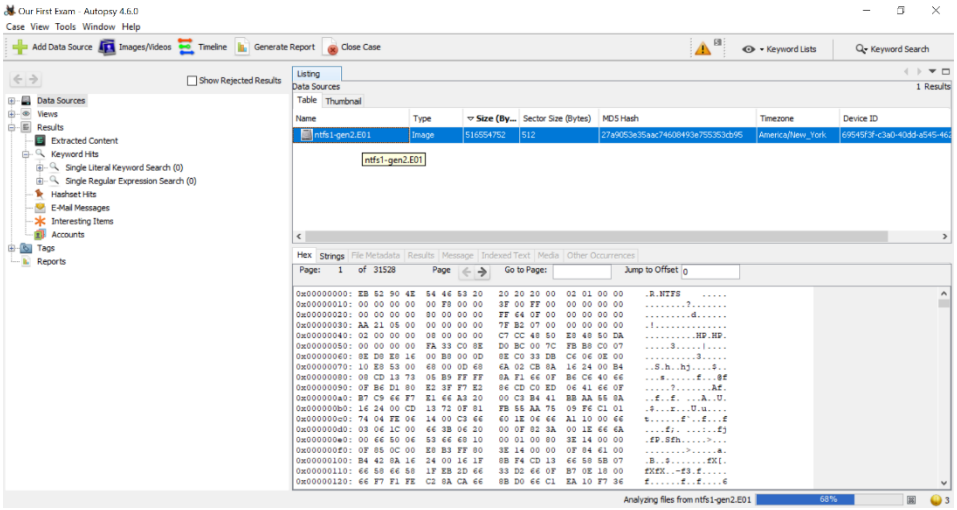
- Next, we need to load in our evidence file. Start off by making sure “Disk Image or VM File” is selected, then click next.



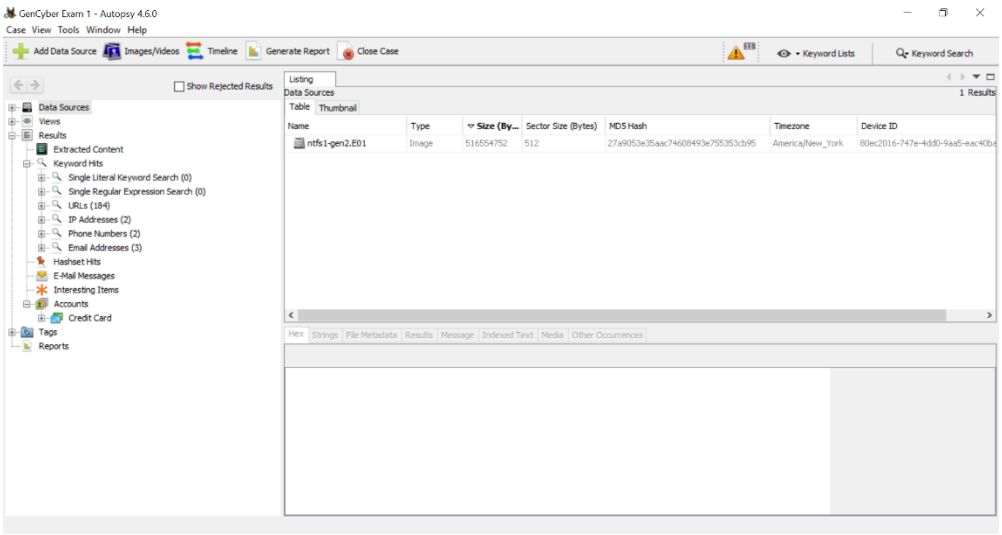
- Click where it says “Browse”, then navigate to the “Evidence Files” folder on your flash drive, and select the file titled “nfts-gen2.E01”. Then click next.



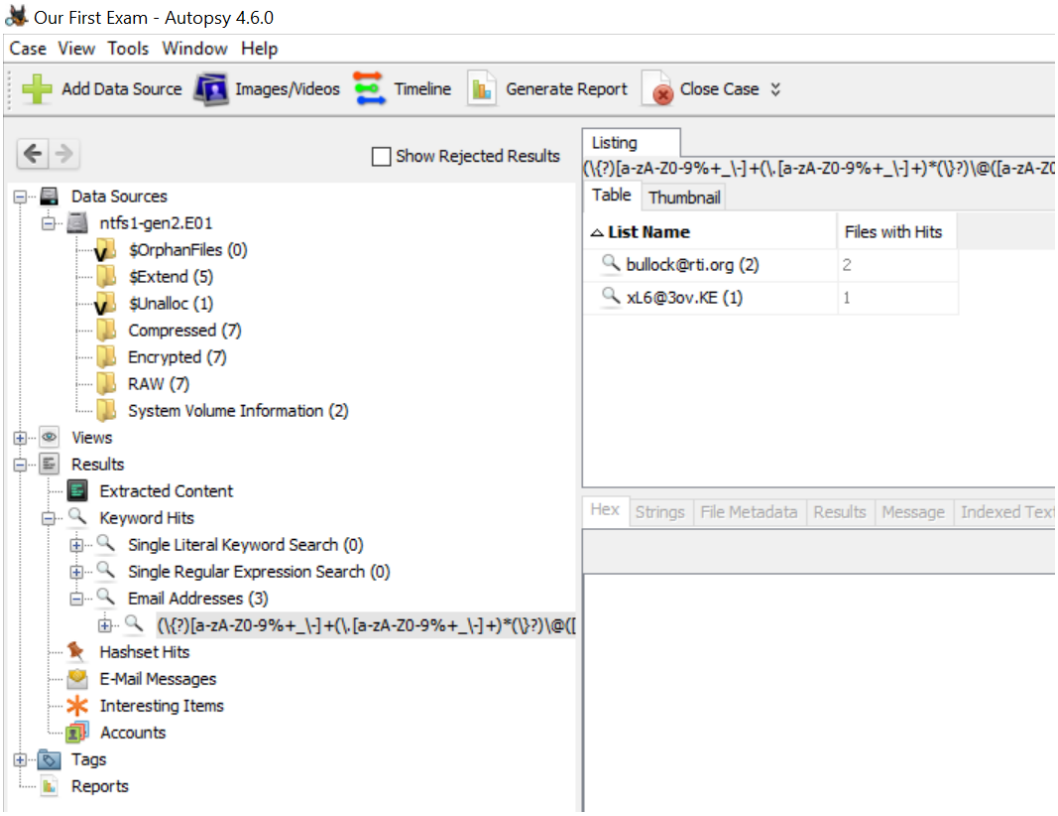
- On this screen leave everything clicked. You need to scroll down to where it says, “Keyword Search”. Make sure everything under this tab is selected, including Phone Numbers, IP Addresses, Email Addresses, URL’s, and Credit Card numbers. Then click “Next” and finally “Finish”



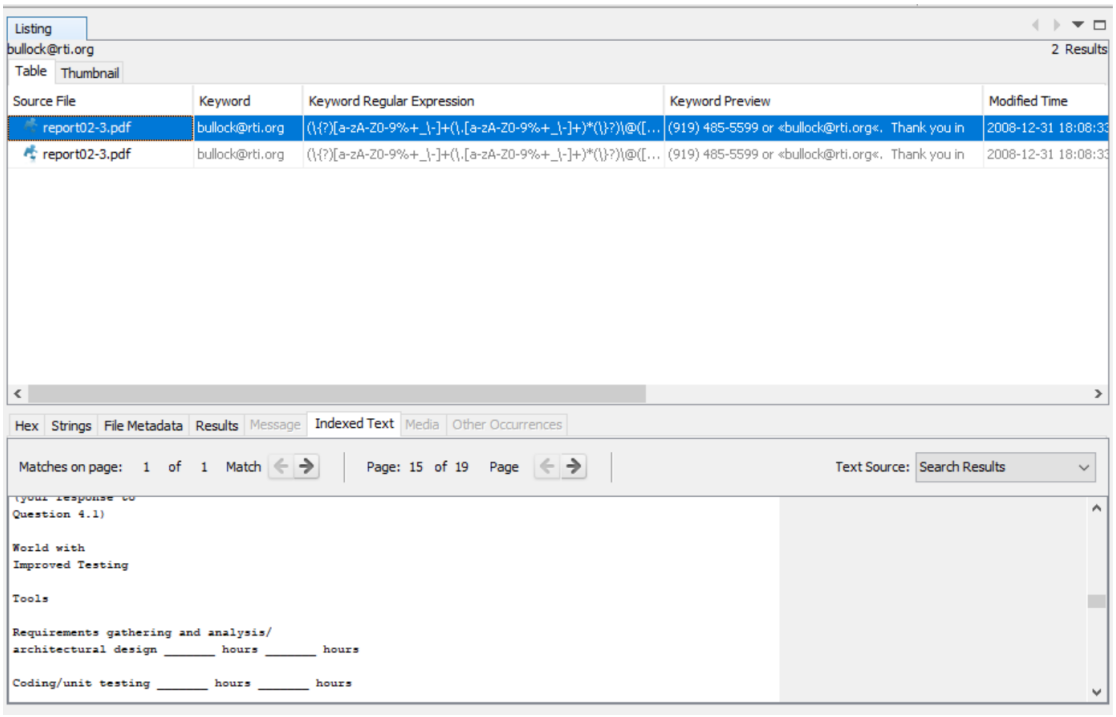
- When it loads, you should screen like this one above.
- In the window to the bottom right you will see a bunch of numbers and letters. Such as “00” or “AA” or combinations of the two like “D0”. These are hexadecimal numbers. It is a method used to turn letters, and symbols into numbers. So instead of using digits 0-9, it uses 0-9, and A-F. For a nice video explaining the binary and hexadecimal system check out, https://www.youtube.com/watch?v=aB__6e6WkFQ
- Using hexadecimal (or hex for short) we can encode letters and symbols. For example, the number 68 has a hex code of 44. In the ASCII encoding scheme, this represents the letter D.
- This is how computers store information, so it is important to understand how this works, if wish to further understand how data is stored and manipulated in computers.
- After the computer is done analyzing the evidence file the screen should look like this:



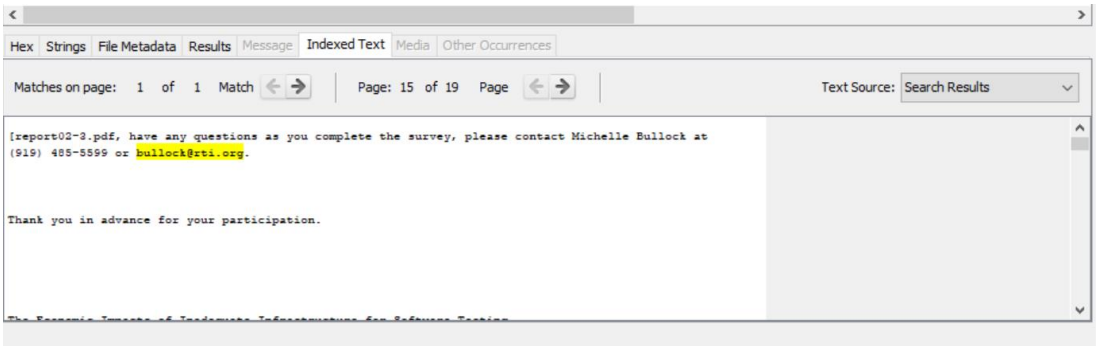
- Now let's use autopsy to look at email addresses. Let's first click on where it says Results, and then scroll down to where it says Email Addresses (3). Then click on the magnifying class to expand the tab.



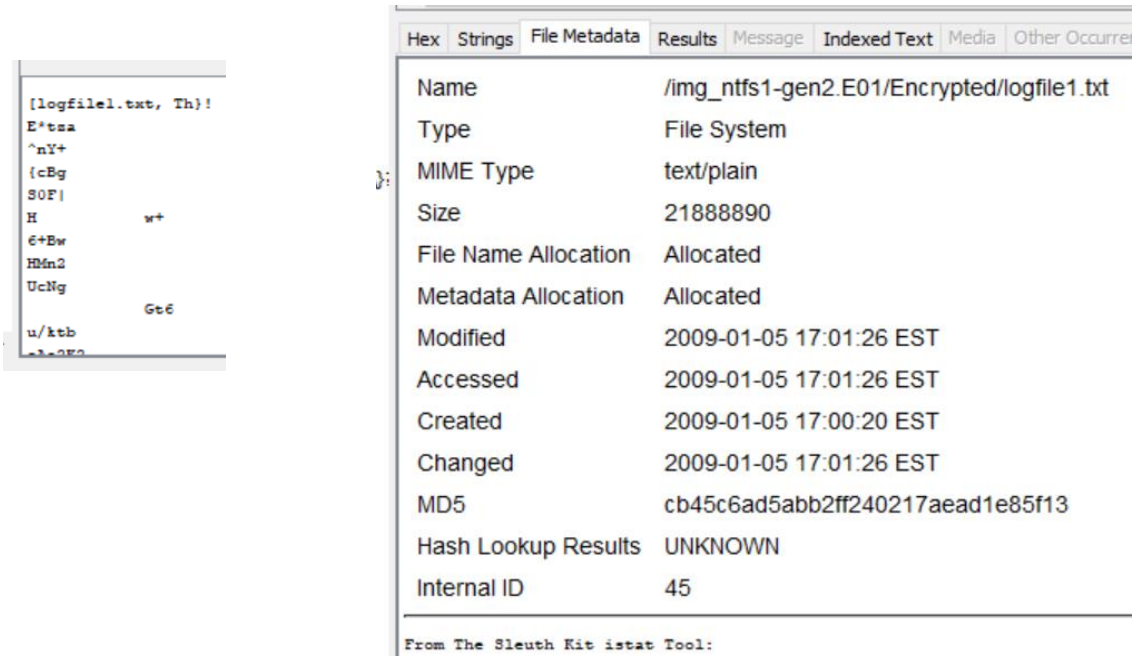
- If you click on the first email address bullock@rti.org, it shows two different files that appear.
- We see two files named "report02-3.pdf". Then if you look you can also see a phone number in the Keyword Preview area.



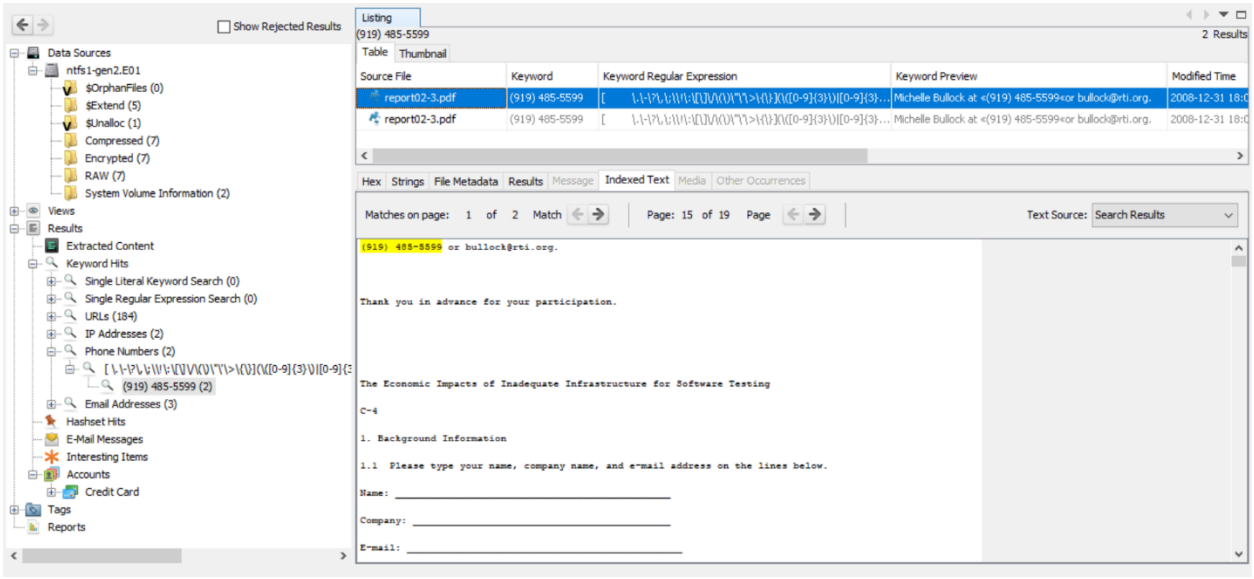
- By moving the scroll bar over to the right, we can see some other interesting things. Like the time it was modified, accessed, and changed. Along with the file path.
- If we look in the box underneath the area we were just looking at we can view the email by moving the vertical scroll bar up and down.
- We can also view other information such as the hexadecimal values for the strings in the file, we can view just the strings with no blank lines in between the strings, the file metadata (Which is an informational panel describing the file), the results, and the indexed text which you are looking at now.



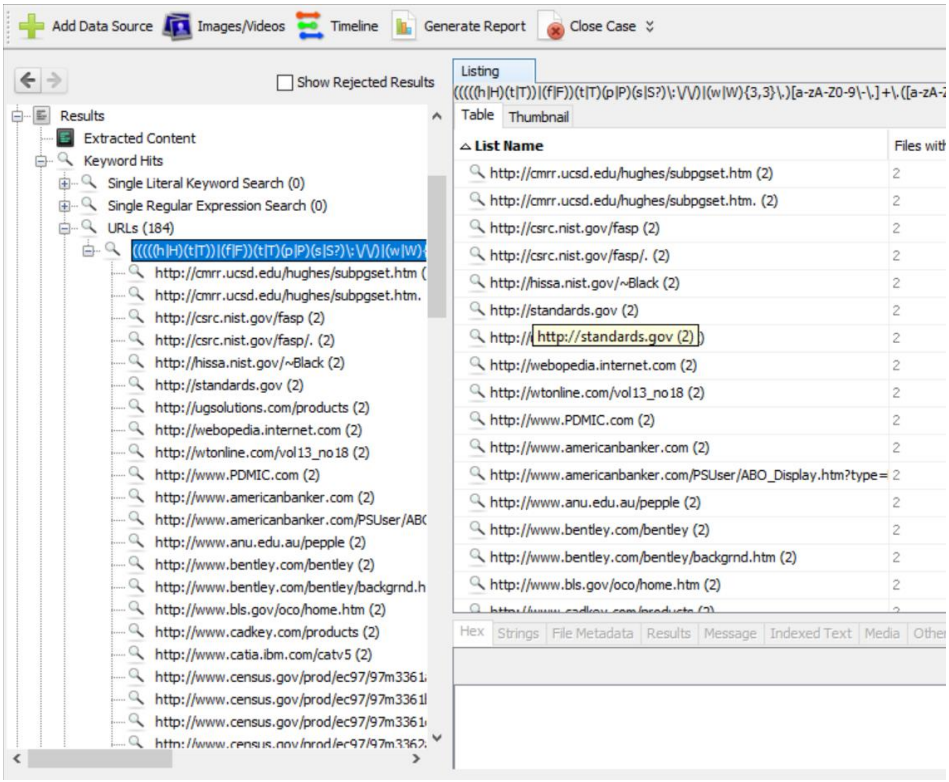
- We can view that data by clicking the corresponding tabs on the top left section of this window.
- Now lets click on the other email address. Labeled xL6@30v.ke. This address contains a file named “logfile1.txt”. If you view the contents of this email, you will see this.
- This looks like this because this file is encrypted.
- If we look at the File Meta-Data for this, we can learn something useful.
- As you can see in the name, this file belongs to the encrypted folder.
- A little bit further down, you can see the MD5 hash.



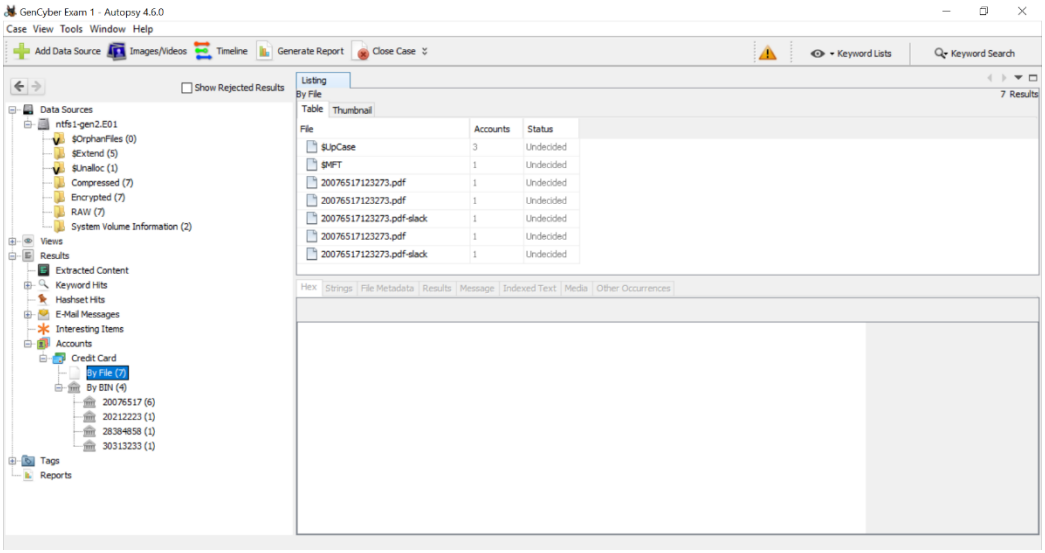
- The MD5 hash is a way on encoding a whole file into a 32-bit hash. This is used to ensure that files are the same, this is particularly useful when two people are downloading the same value. Instead of having to download the whole file, they could download this. If the hashes match, this means that the file the people downloaded is the same.



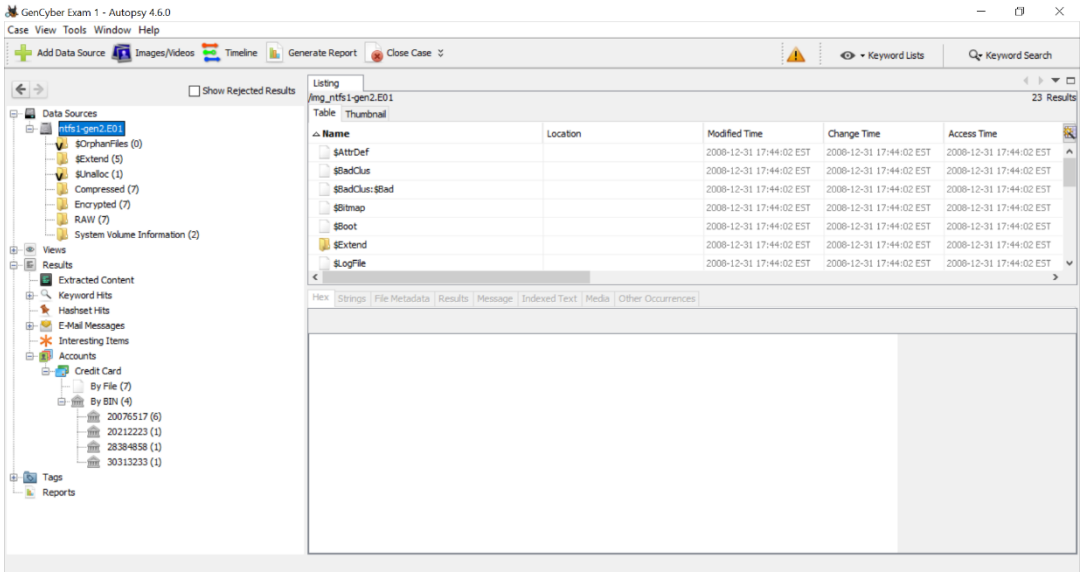
- If you click on where it says phone numbers, then expand the directory underneath that tab you can see the files that we found in the email section.
- These phone numbers match what we previously found.
- What this tells us is that Autopsy, scans the files search by search.



- Next lets take a look at URL's.
- Click on where it says URL's and expand the directories.
- There is 184 results that pop up. Take a few minutes and look through them and see what you can find.
- You may notice that many of the file names that the URL's are found in match.
- This is because many of the files are reports, and have references listed somewhere in the file.
- This goes to show that though Autopsy does a thorough search through the files, but it makes it appear as if there is more data than their actually is.
- Although there is 184 URL's listed, there is not that many files in our system.



- In the file directory to the left-hand side of the screen there is a tab labeled “Accounts”.
- Expand the directory underneath it to reveal something titled “Credit Card”, then expand it. You can then view the information by card, or BIN (Banking Identification Number)
- This allows us to view credit card numbers and bins.



- If you want to view every file available in the system click on “nfts-gen2.E01” in the top left of the directory. This shows every file available for examination
- Take some time and see what else you can find.

- Conclusion
  - We learned how to open Autopsy, create a new case, and load in an evidence file. We also examined some introductory data that Autopsy was able to find.
  - Autopsy has many different tools for data analyzation. If you would like to learn more there are several tutorials on the internet. There are also free evidence files for analyzation that can be found online.

- We will continue our analysis in the next module.