

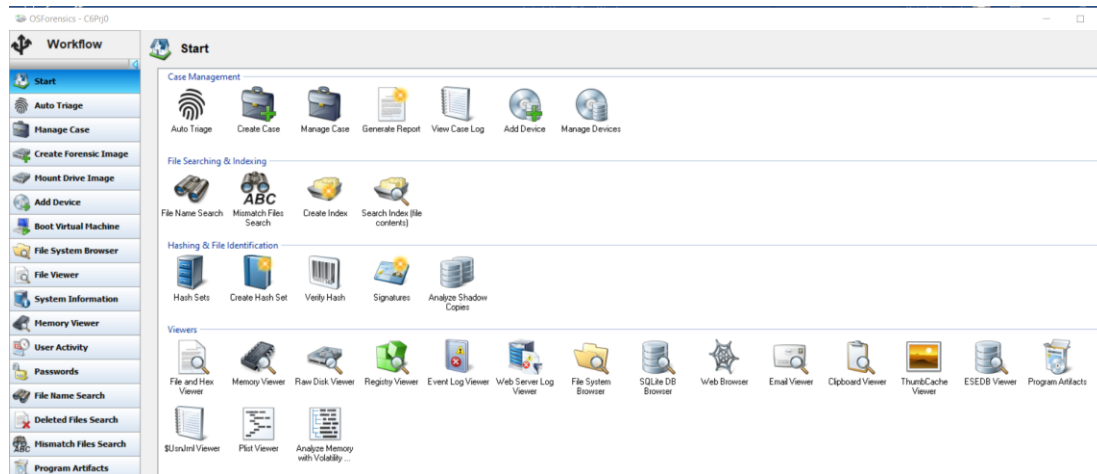
Hands on Project

6.1

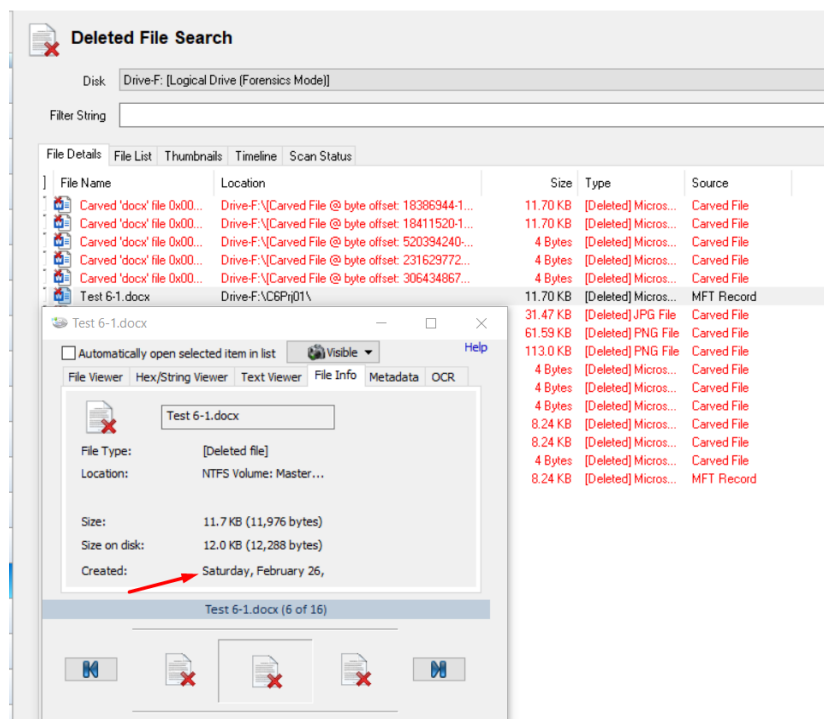
In this project, you create and delete Word and Excel files on a USB drive (or small disk partition, if you don't have a USB drive), and then use OSForensics to examine the drive. Follow these steps:

1. Create a C6Prj01 folder on your USB drive.
2. Open a new document in Word, and type This is to test deleting files and then wiping them. Save the file in the C6Prj01 folder as Test 6-1.docx, and exit Word.
3. Open a new workbook in Excel. Type a few numbers, and then save the workbook in the C6Prj01 folder as Test 6-2.xlsx. Exit Excel.
4. Use File Explorer to delete both files from the USB drive.
5. Open up OSForensics and create a new case. For the case name, type C6Prj01, and for the investigator, type your name. Select Live Acquisition of Current Machine as the Acquisition Type, and the work folder you created for this chapter as the Work Folder. Click OK to create a subfolder called C6Prj01.
6. If necessary, go to the left pane and click Manage Case, then go to the right pane and click the Add Device button. Select the Forensics mode choice button and click OK after clicking the drive letter of your USB device.
7. If the case you just created does not have a green check mark next to it, double-click it and then select Start in the left pane. Scroll down and click the Deleted Files & Data Carving icon using the scroll bar on the far right. Click the Disk list arrow in the Deleted Files Search window, then the USB device in the list of possibilities. To begin, press the Search button. You don't need to input a file string or a filter because you're looking for deleted files.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



8. Double-click the Test 6-1.docx file in the lower pane to view its contents. You can also click the File Info tab to verify the file's MAC time. Repeat this process with the Test 6-2.xlsx file.



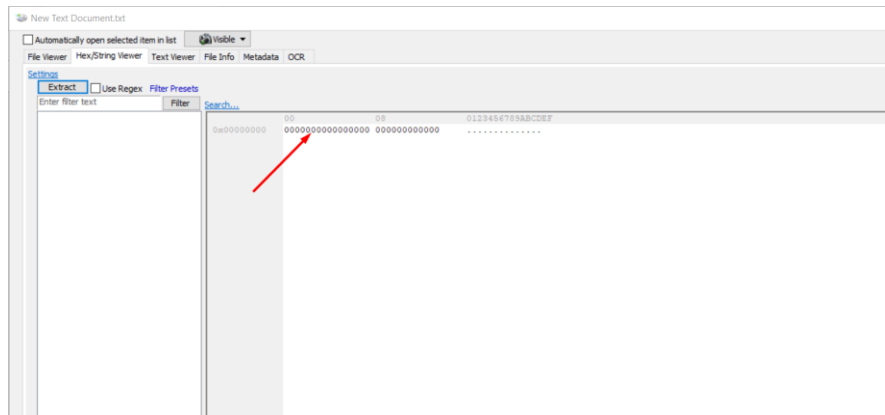
9. close windows and exit

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

6-2

In this project, you will do research, download, and test a disk-cleaning and wiping utility. Make sure you're not working on a production line. Search the Internet for disk-cleaning and wiping software and download and install at least one of the programs. We have used Disk Wipe free version software in this hands on.

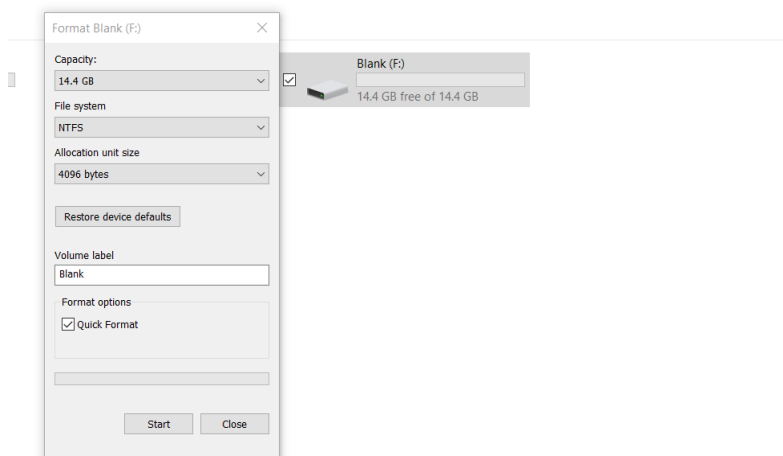
1. Create a C6Prj02 folder on your USB drive. Start the tool you just installed.
2. Select USB drive. Make sure to follow instructions in the software documentation, wipe the drive.
3. Open up OSForensics and create a new case. For the investigator's name, type your name, for the case name, type C6Prj02, and for the case path, type your work folder. Click OK to create a subdirectory called C6Prj02.
4. Click the Add Device button. Click the Drive Letter option button, if necessary, and in the drop-down list box, click the drive letter for your USB drive. Click OK.
5. Another way to open deleted files window is Click Start and click Deleted Files Search button on the left.
6. Click Disk list arrow, and click the USB drive in the list of options. Click the Search button.
7. Double-click any file in the lower pane to open it.
8. Click the Hex/String Viewer tab if necessary (see Figure 6-8). It should display hexadecimal 0 values, indicating that the disk wipe was successful. Exit OSForensics after taking a screenshot. Write a brief report on the tool's usefulness and submit it to your instructor along with a screenshot.



6-3

This project involves planting evidence in the file slack space on a USB drive or a small disk partition to build a test drive. Then you utilize Hex Workshop to make sure the drive has evidence on it.

1. To format the drive, right-click the drive icon and click Format, then click Start. If you see a warning message, click OK to continue, and then click OK in the Format Complete message box.



2. Create a C6Prj03 folder on the USB drive.
3. Open a new document in Word, type Testing for string Millennium. Save the file in the C6Prj03 folder as C6Prj03a.docx.

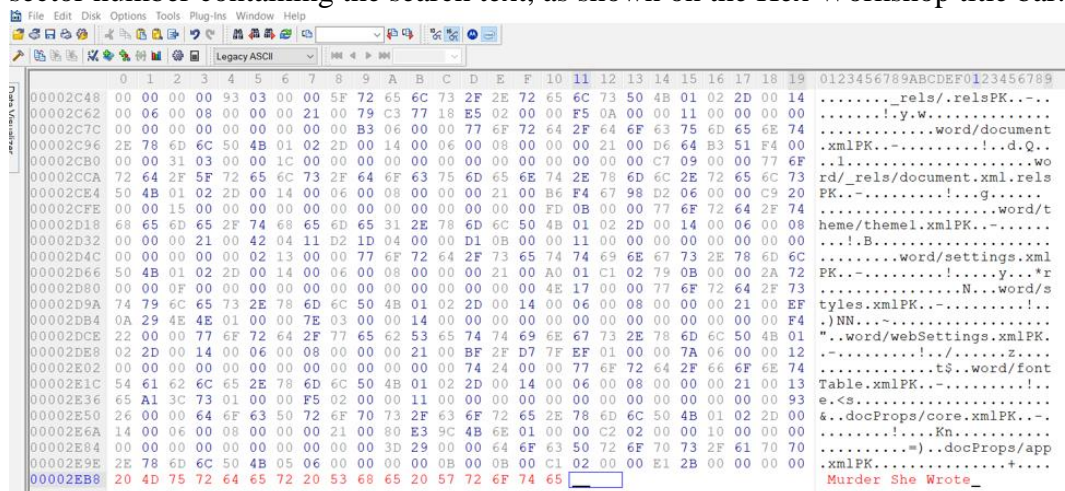
Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

4. Close the file, open new Word document, and type Testing for string XYZX. Save the file in the C6Prj03 folder as C6Prj03b.docx. Exit Word.

If required, scroll to the bottom of the sector. In the right pane, type Murder She Wrote near the end of the sector, then click the Save toolbar button. (Note: If Insert mode is required, click OK, press Insert, click to select the Disable notification message check box, and then click OK.)

Now you use Hex dump(hexworkshop) to hide the information in file space

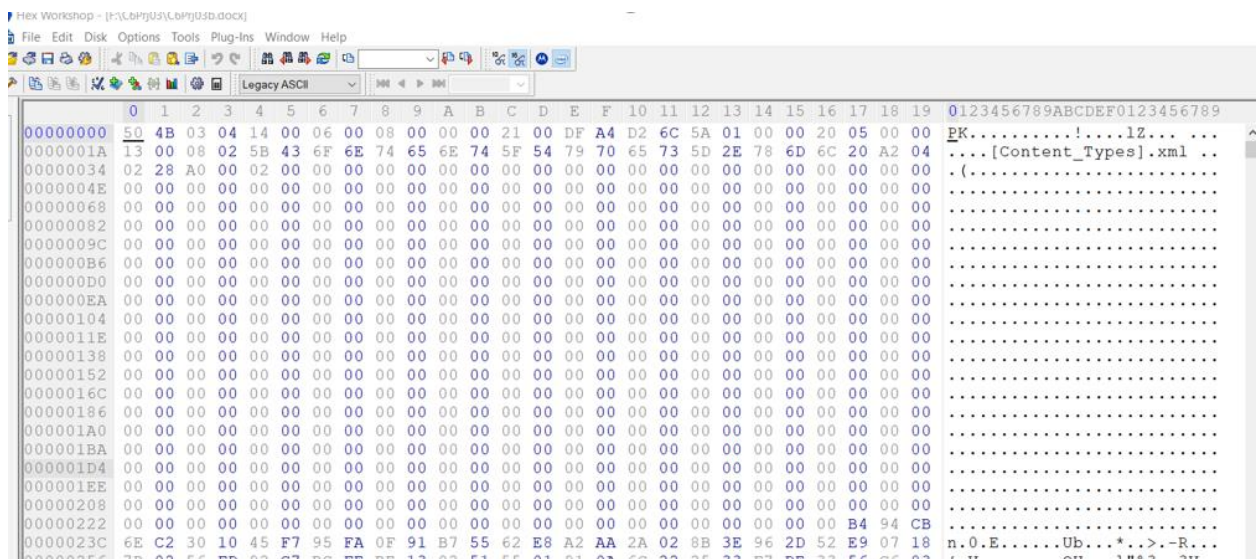
- Open www.hexworkshop.com and download it and open it
- create a chart with two columns. Label the columns Item and Sector.
- click Disk, Open Drive from the menu. Make sure the USB or disk drive is selected, and then click OK
- Click File, Open from the menu. Navigate to and double-click C6Prj03a.docx. Scroll down until you see “Testing for string Millennium.”
- Then, in the right column, click at the beginning of the tab that corresponds to your USB device. From the menu, select Edit, Find. Make sure Text String is chosen in the Type list box in the Find dialog box. In the Value text box, type Millennium, and then click OK.
- In the Item column on your chart, write C6Prj03a.docx. In the Sector column, write the sector number containing the search text, as shown on the Hex Workshop title bar.



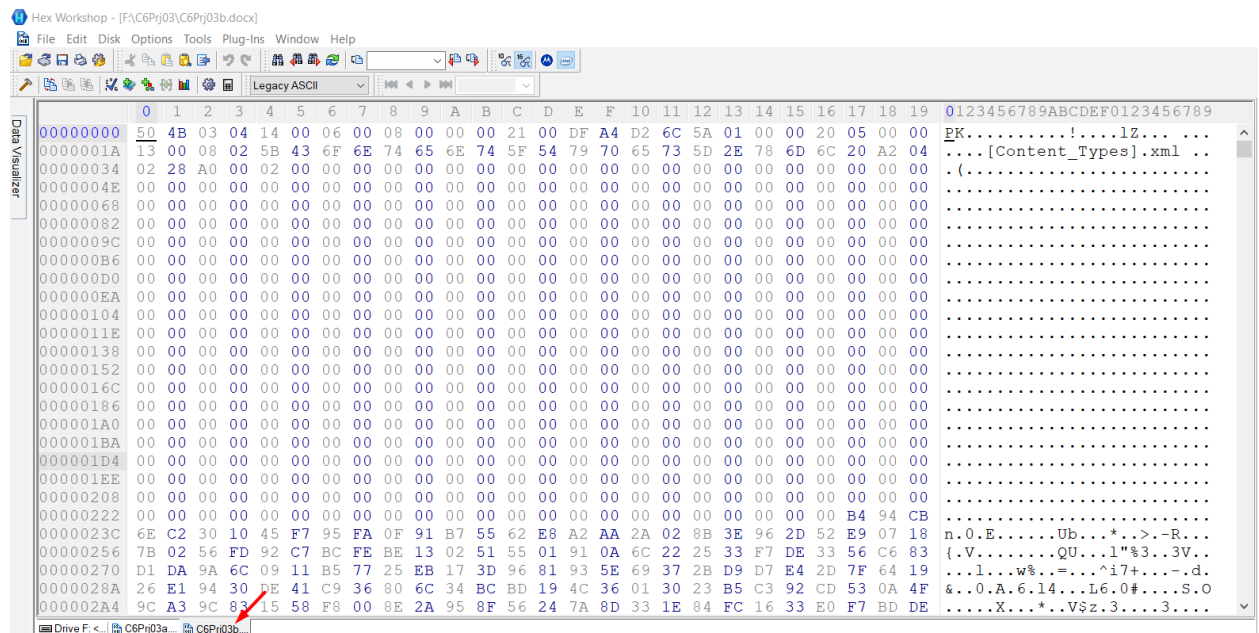
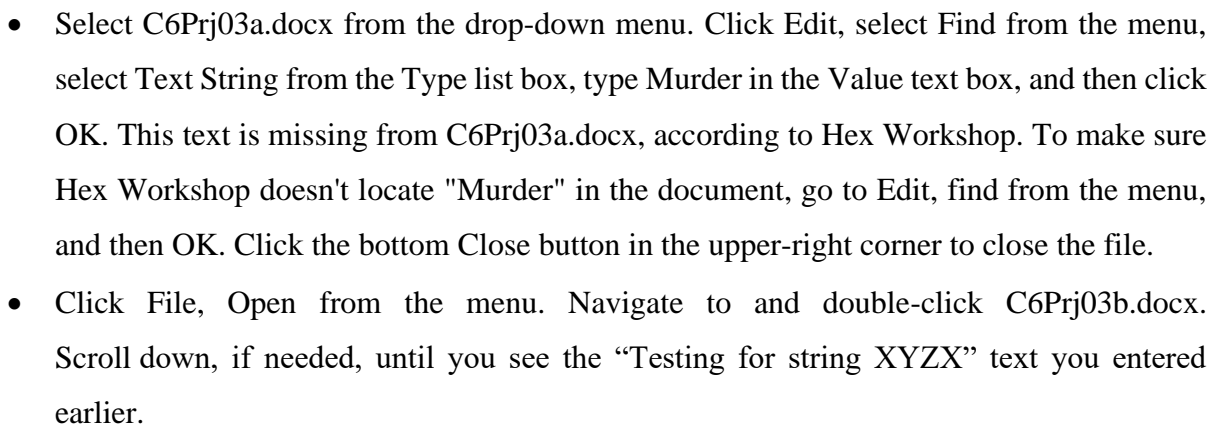
```
0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 0123456789ABCDEF0123456789
00002C48 00 00 00 00 93 03 00 00 5F 72 65 6C 73 2F 2E 72 65 6C 73 50 4B 01 02 2D 00 14 ....._rels/.relsPK...
00002C62 00 06 00 08 00 00 00 21 00 79 C3 77 18 E5 02 00 00 F5 0A 00 00 11 00 00 00 .....!_y.w.....
00002C7C 00 00 00 00 00 00 00 00 00 00 B3 06 00 00 77 6F 72 64 2F 64 6F 63 75 6D 65 6E 74 .....word/document
00002C96 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 21 00 D6 64 B3 51 F4 00 .xmlPK.....!_d.Q...
00002CB0 00 00 31 03 00 00 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 77 6F ..!.....!_d.Q...
00002CCA 72 64 2F 5F 72 65 6C 73 2F 64 6F 63 75 6D 65 6E 74 2E 78 6D 6C 2E 72 65 6C 73 rd/_rels/document.xml.rels
00002CE4 50 4B 01 02 2D 00 14 00 06 00 08 00 00 21 00 B6 F4 67 98 D2 06 00 00 C9 20 PK.....!_g.....
00002CFE 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 FD 0B 00 00 77 6F 72 64 2F 74 PK.....!_g.....
00002D18 68 65 6D 65 2F 74 68 65 6D 65 31 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 08 heme/themel.xmlPK.....
00002D32 00 00 00 21 00 42 04 11 D2 1D 04 00 00 D1 0B 00 00 11 00 00 00 00 00 00 00 00 .....!_B.....
00002D4C 00 00 00 00 00 02 13 00 00 77 6F 72 64 2F 73 65 74 74 69 6E 67 73 2E 78 6D 6C .....word/settings.xml
00002D66 50 4B 01 02 2D 00 14 00 06 00 08 00 00 21 00 A0 01 C1 02 79 0B 00 00 2A 72 PK.....!_y.*r
00002D80 00 00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 4E 17 00 00 77 6F 72 64 2F 73 .....!_N...word/s
00002D9A 74 79 6C 65 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 21 00 EF tyles.xmlPK.....!_
00002DB4 0A 29 4E 4E 01 00 00 7E 03 00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 F4 .)NN.....!_
00002DCE 22 00 00 77 6F 72 64 2F 77 65 62 53 65 74 74 69 6E 67 73 2E 78 6D 6C 50 4B 01 ".word/webSettings.xmlPK
00002DE8 02 2D 00 14 00 06 00 08 00 00 21 00 BF 2F D7 7F EF 01 00 00 7A 06 00 00 12 .....!_./.....Z...
00002E02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 77 6F 72 64 2F 66 6F 6E 74 .....!_t$.word/font
00002E1C 54 61 62 6C 65 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 21 00 13 Table.xmlPK.....!_
00002E36 65 A1 3C 73 01 00 00 F5 02 00 00 11 00 00 00 00 00 00 00 00 00 00 00 00 93 e.<.....!_
00002E50 26 00 00 64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E 78 6D 6C 50 4B 01 02 2D 00 &..docProps/core.xmlPK...
00002E6A 14 00 06 00 08 00 00 21 00 80 E3 9C 4B 6E 01 00 00 C2 02 00 00 10 00 00 00 .....!_Kn.....
00002E84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 64 6F 63 50 72 6F 70 73 2F 61 70 70 .....!_Kn.....
00002E9E 2E 78 6D 6C 50 4B 05 06 00 00 00 00 00 00 00 00 C1 02 00 00 E1 2B 00 00 00 .xmlPK.....!_+....
00002EB8 20 4D 75 72 64 65 72 20 53 68 65 20 57 72 6F 74 65 Murder She Wrote_
```

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- Choose C6Prj03a.docx from the drop-down menu. Click Edit, select Find from the menu, select Text String from the Type list box, type Murder in the Value text box, and then click OK. This text is missing from C6Prj03a.docx, according to Hex Workshop. To make sure Hex Workshop doesn't locate "Murder" in the document, go to Edit, find from the menu, and then OK. Click the bottom Close button in the upper-right corner to close the file.
- From the File menu, Go to C6Prj03b.docx and double-click it. If necessary, scroll down until you see the text "Testing for string XYZX" that you typed previously.

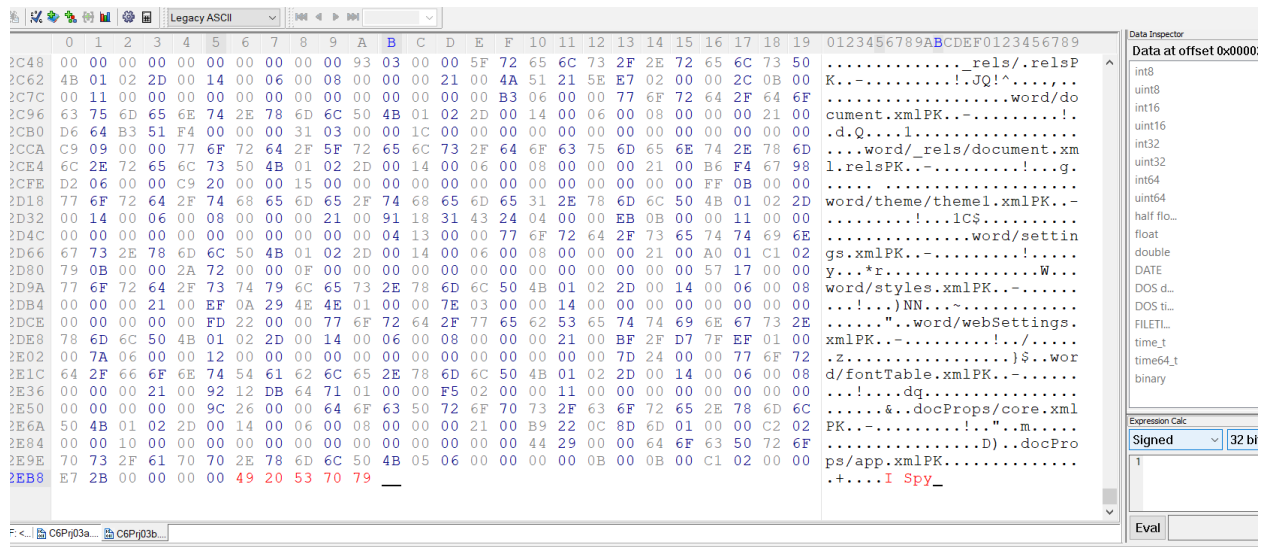


- If necessary, click the tab for your USB drive, and then click at the top of the right column. Click Edit, select Find from the menu, type XYZX for the value you're looking for, and then click OK. In the Item column of your chart, type C6Prj03b.docx, and in the Sector column, type the sector number containing the search text, as seen on the Hex Workshop title bar.
- In the tab for your USB drive, type I Spy near the end of the sector in the right pane, in the slack space, and then click the Save toolbar button.



Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- click the tab for your USB drive, and then click at the top of the right column. Click Edit, select Find from the menu, type XYZX for the value you're looking for, and then click OK. In the Item column of your chart, type C6Prj03b.docx, and in the Sector column, type the sector number containing the search text, as seen on the Hex Workshop title bar.
- In the tab for your USB drive, type I Spy near the end of the sector in the right pane, in the slack space, and then click the Save toolbar button.



- Verify that “I Spy” doesn’t appear as part of the file by clicking the C6Prj03b.docx tab and searching for this string twice.
- Close the C6Prj03b.docx file, and exit Hex Workshop.

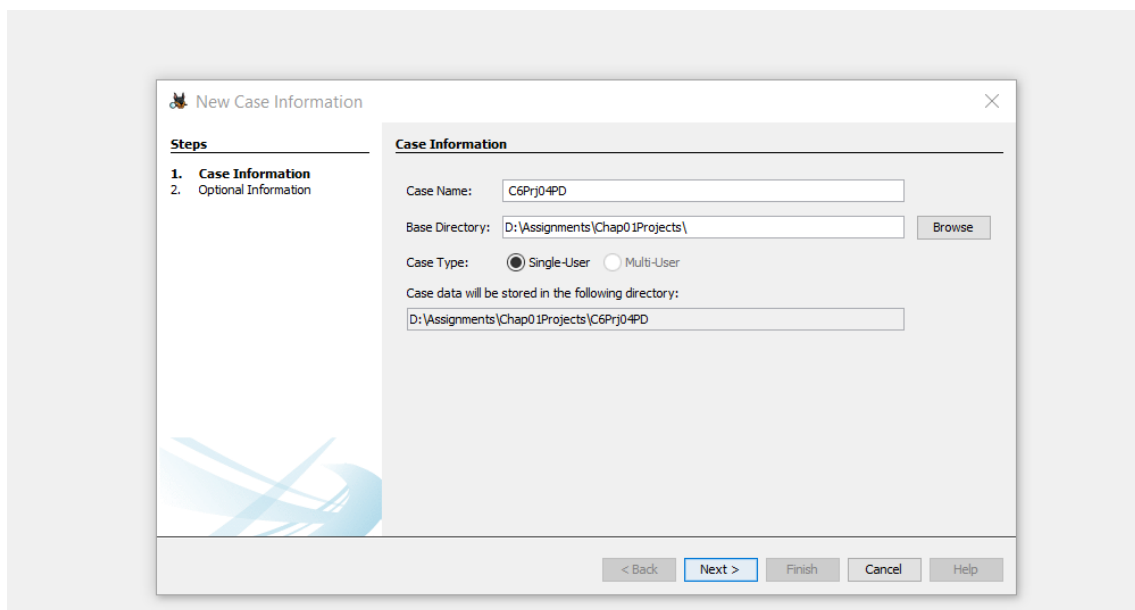
6-4

To ensure that new or updated digital forensics tools are working properly, you should test them. When complicated software applications are updated, new issues and function failures may arise that the vendor was unaware of. You will examine two rival digital forensics analysis tools in this research to see how they compare in terms of locating and recovering data. Keep in mind that, despite their differences in strengths, tools should produce similar results.

We need:

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

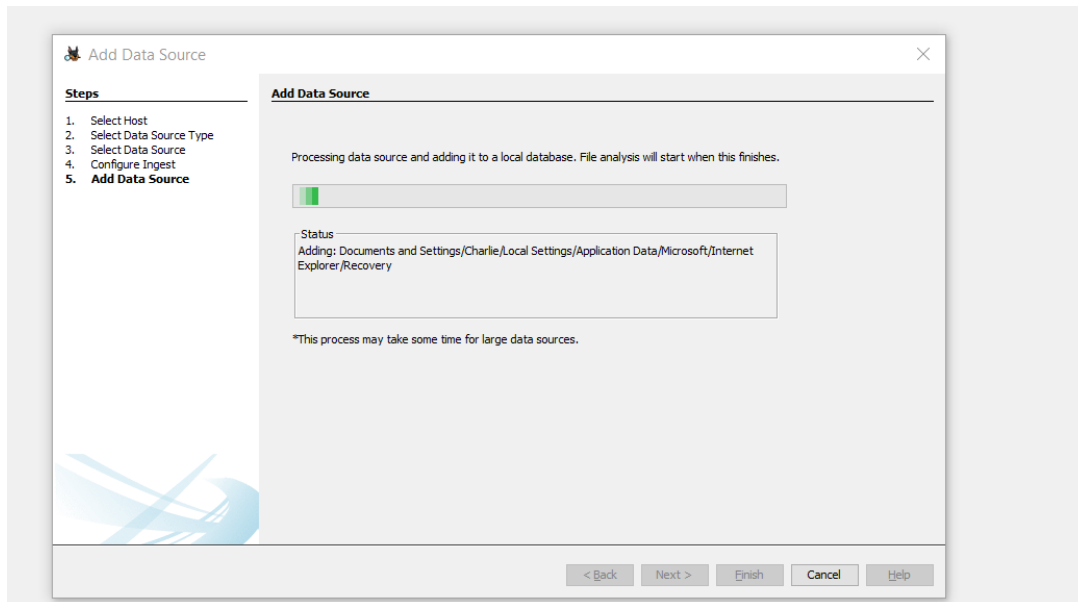
- Autopsy for Windows installed on your workstation (version 4.3.0 used at the time of this writing)
 - OSForensics installed on your workstation
 - The charlie-2009-12-07.E01 drive image from the M57 Patents case First, you use Autopsy for Windows to examine the file:
1. Install Autopsy for Windows on your workstation if necessary, as described in Chapter 1. You can also install it by going to www.sleuthkit.org/autopsy/ and clicking Download Now.
 2. Start the Windows version of Autopsy. Click the Create New Case button to begin your investigation. For the case name, type C6Prj04PD in the New Case Information window. Then, next to the Base Directory text box, click the Browse button, navigate to and select your work folder, click OK, and then Next. Type 001 in the Case Number text box and your name in the Examiner text box in the Additional Information window. Finish by clicking the Finish button.



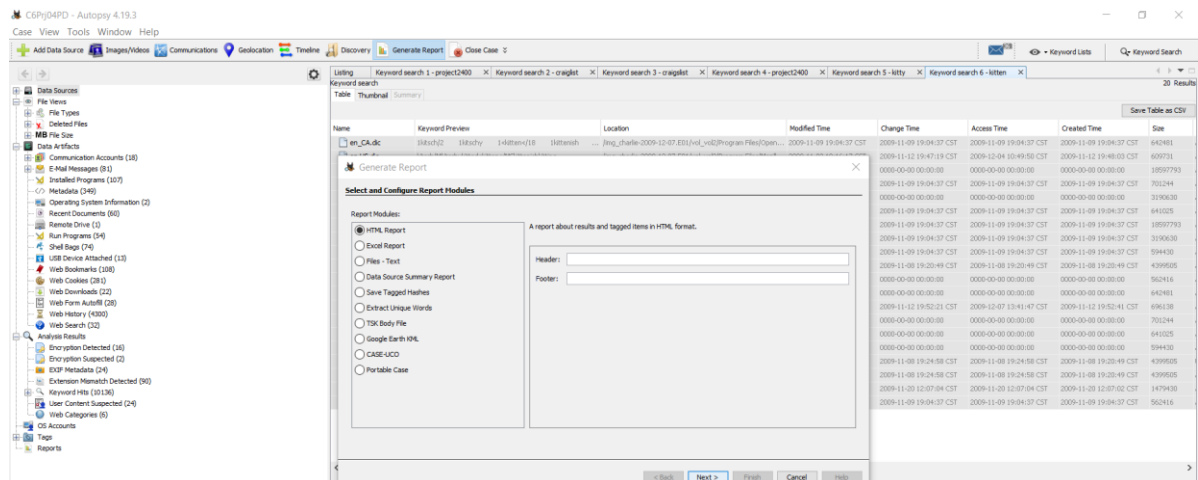
3. Click Disk Image or VM File in the Select Type of Data Source to Add section of the Add Data Source window, then Next. Pick the Browse button in the Select Data Source box, scroll to your work folder, click charlie-2009-12-07.E01, and then click Open. Then press the Next button.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

- Click Next on the Configure Ingest Modules window. Click Finish in the Add Data Source window. The file intake is indicated by a status bar in the lower-right corner. Autopsy then examines the files once it's finished, which can take up to 30 minutes depending on the amount of RAM in your workstation.



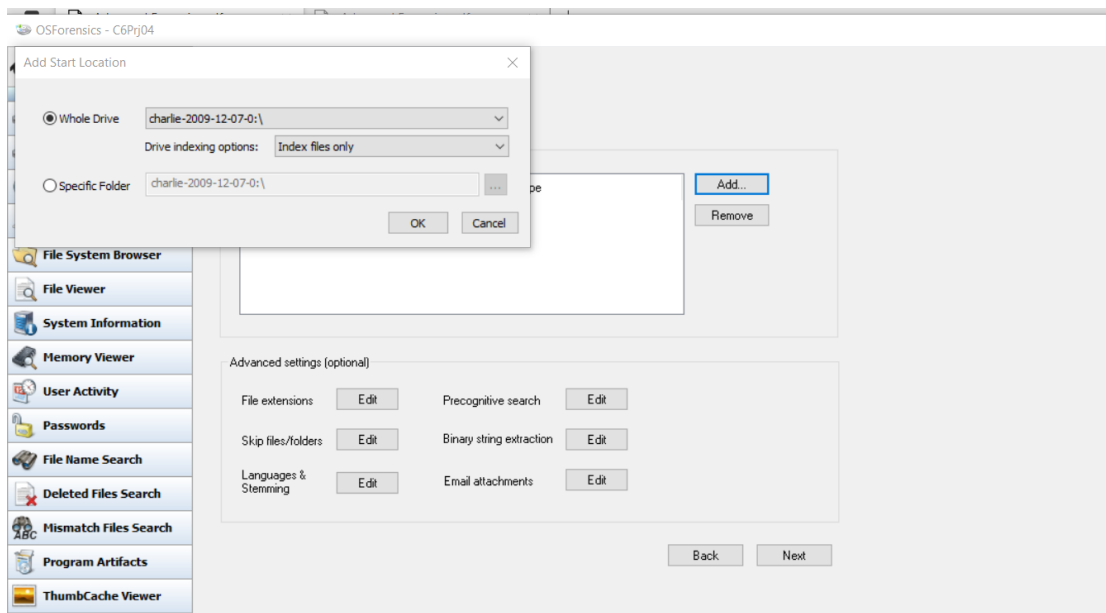
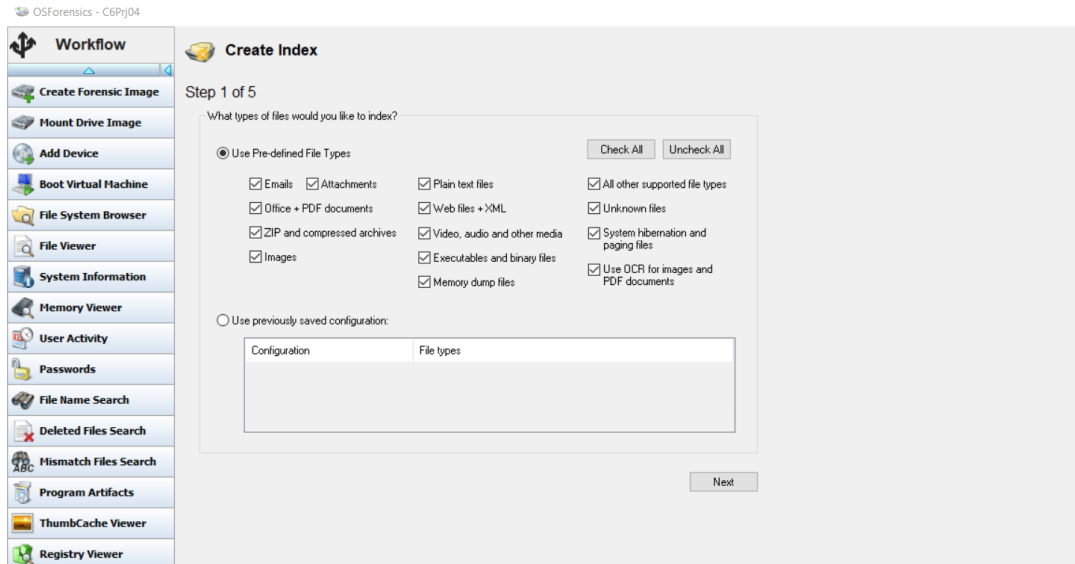
- At the upper right, click the down arrow for Keyword Search. Type project2400 into the Search for the pattern(s) text box, then click Search. If you get an error message that says the procedure isn't finished, ignore it.
- In the Search tab, Ctrl+click to select all the files. Right-click the selection, point to Tag Files, and click Tag and Comment. In the Comment text box, type the search term.
- Repeat Steps 5 and 6 for the search term craiglist.
- Click the Generate Report button at the top. Click the Results - HTML option button for the report format, and then examine the report. When you're finished, exit Autopsy for Windows.



In the OS forensics :

1. Start OSForensics. Click Start in the left pane, if necessary, and in the right pane, click Create Case.
2. Enter your name for the investigator, C6Prj04 for the case name, and Investigate Disk(s) from Another Machine selection button for the acquisition type in the New Case dialog box. Click the Browse button, scroll to and click your WorkC6Prj04 folder, and then click OK twice for the case folder.
3. Click the Add Device button. Click the Image File option button, and then browse to your work folder, click the charlie-2009-12-07.E01 image file, and click Open. Click OK twice.
4. In the left pane, click the Create Index button. Click the Use Pre-defined File Types option button in the Step 1 of 5 window, then select all of the file types mentioned and click Next. Click the Add button in the Step 2 of 5 window, type charlie-2009-12-07.E01, click OK, and then click Next. Type Index all file types in the Index Title text box in the Step 3 of 5 dialog, and then click Start Indexing.

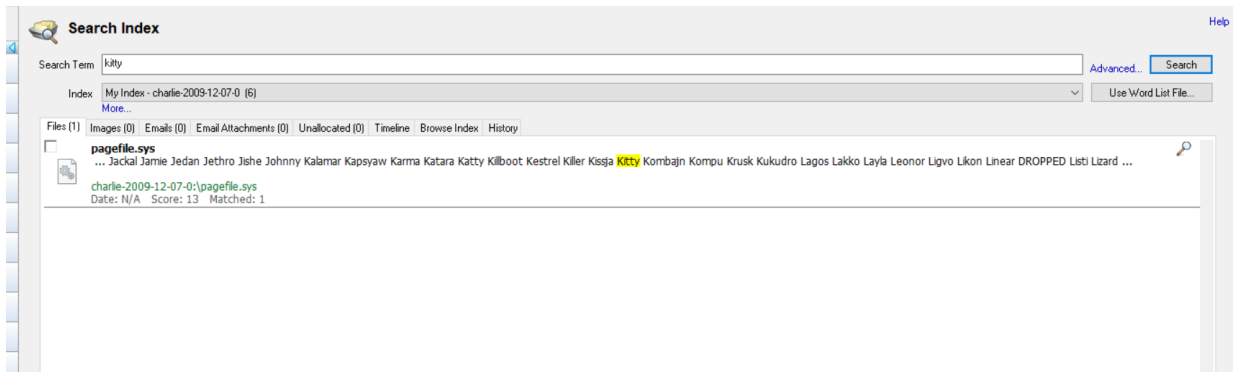
Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



5. When OSForensics finishes indexing the image file, click OK in the message box.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

6. In the left pane, click the Search Index button. Type project2400 in the Enter Search Words text box, then click Search in the right pane. Right-click each of the files in the results, select Bookmark, and then click Red
7. Type craigslist into the Enter Search Words text box, then click Search in the right pane. Right-click each file in the results, then select Bookmark and Yellow from the drop-down menu. Rep with the search keywords kitty and kitten, using the red bookmark color for "kitty" and the yellow bookmark color for "kitten."



8. When you're done, click the Start button, and then click the Generate Report button. Accept the default settings, and click OK. In the report, notice your bookmarked files toward the bottom.
9. Exit your Web browser and exit OSforensic.

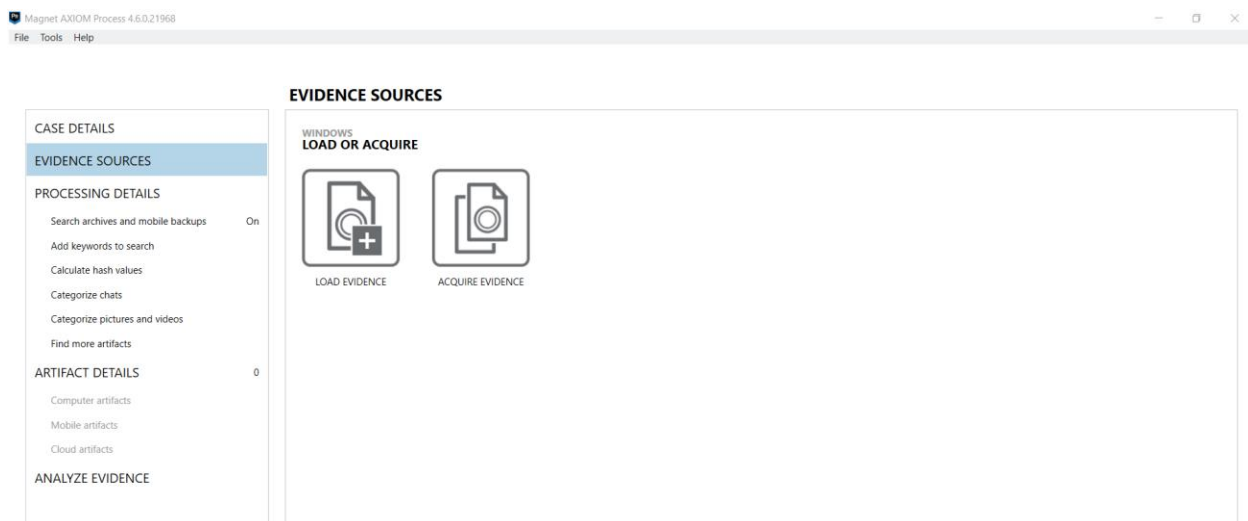
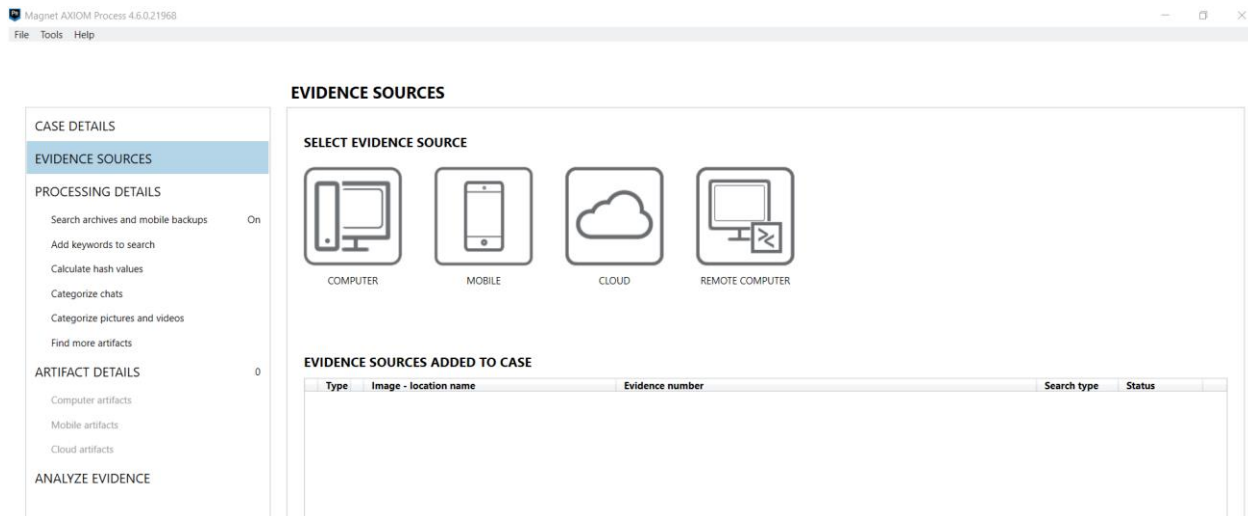
Autopsy is a user-friendly, GUI-based tool that allows you to quickly inspect hard drives and mobile devices. It offers a plug-in architecture that lets you find add-on modules or write bespoke Java or Python modules. On the other hand, Sleuth Kit is a set of command-line tools and a C library for analyzing disk images and retrieving files from them. It's utilized in Autopsy and a slew of other open source and commercial forensics software.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

6-5

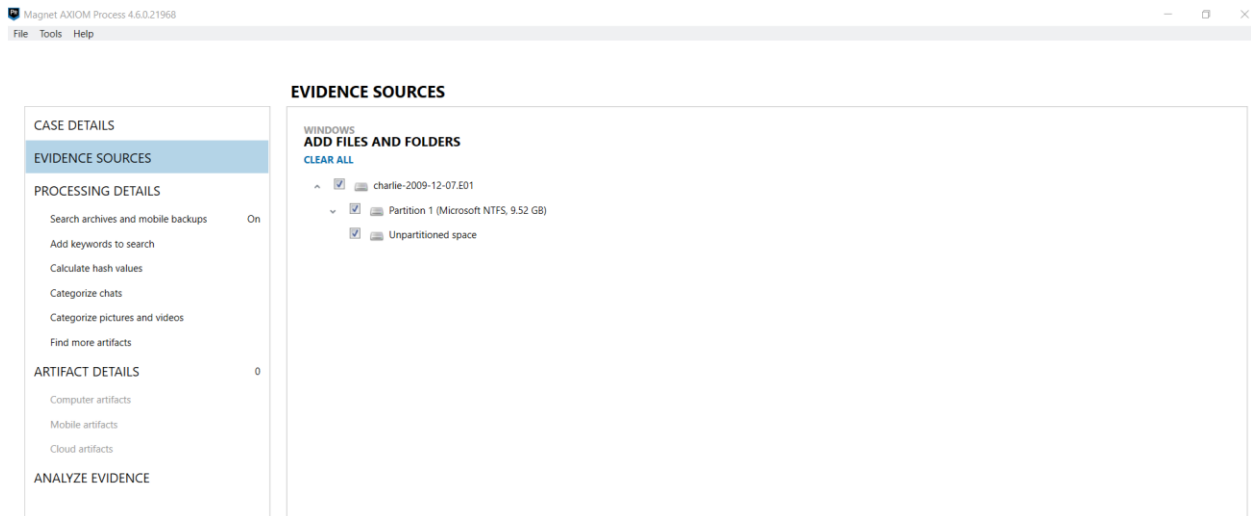
In this project, you use Magnet AXIOM to examine the same file you did in Hands-On Project 6-4. Go to www.magnetforensics.com, and request a 30-day free trial. After getting your 30-day license key, follow Magnet's instructions to download and install AXIOM

1. Start the Magnet AXIOM Process and select CREATE NEW CASE from the drop-down menu. Type 001 in the case number text box in the CASE DETAILS window. In the Folder name text box in the LOCATION FOR CASE FILES section, put Hands-On Project 6-5. Select Folder by clicking the BROWSE button next to the File path text box, then navigating to and clicking your work folder.
2. Enter the folder name Hands-On Project 6-5 in the Location of Acquired Evidence text box, and then click GO TO EVIDENCE SOURCES in the lower-right corner.
3. In the EVIDENCE SOURCES window, you can choose COMPUTER, MOBILE, or CLOUD in the SELECT EVIDENCE SOURCE section. Click the COMPUTER icon. In the next window, click LOAD EVIDENCE, and then click NEXT.

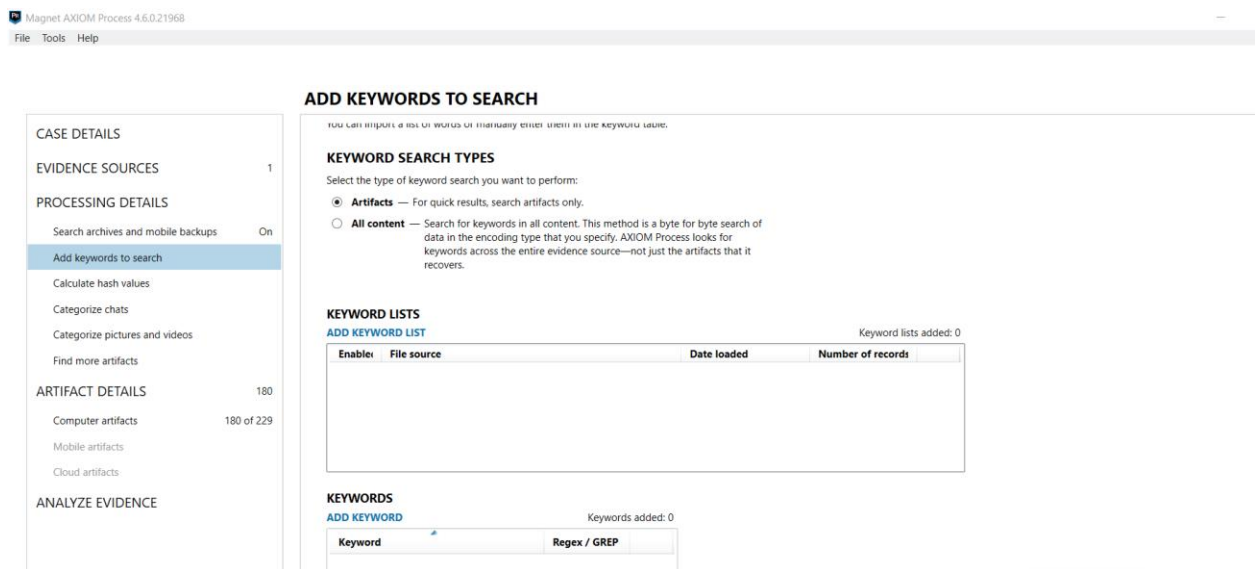


4. In the SELECT EVIDENCE SOURCE window, click IMAGE, browse to and click the charlie-2009-12-07.E01 file, and click OK. In the EVIDENCE SOURCES window, click to clear the Unpartitioned space check box and then click NEXT.

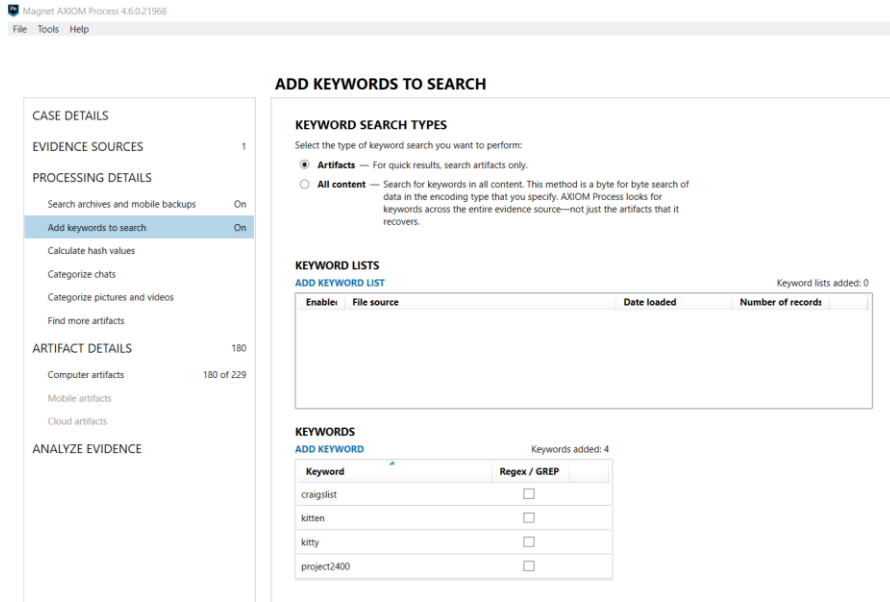
Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



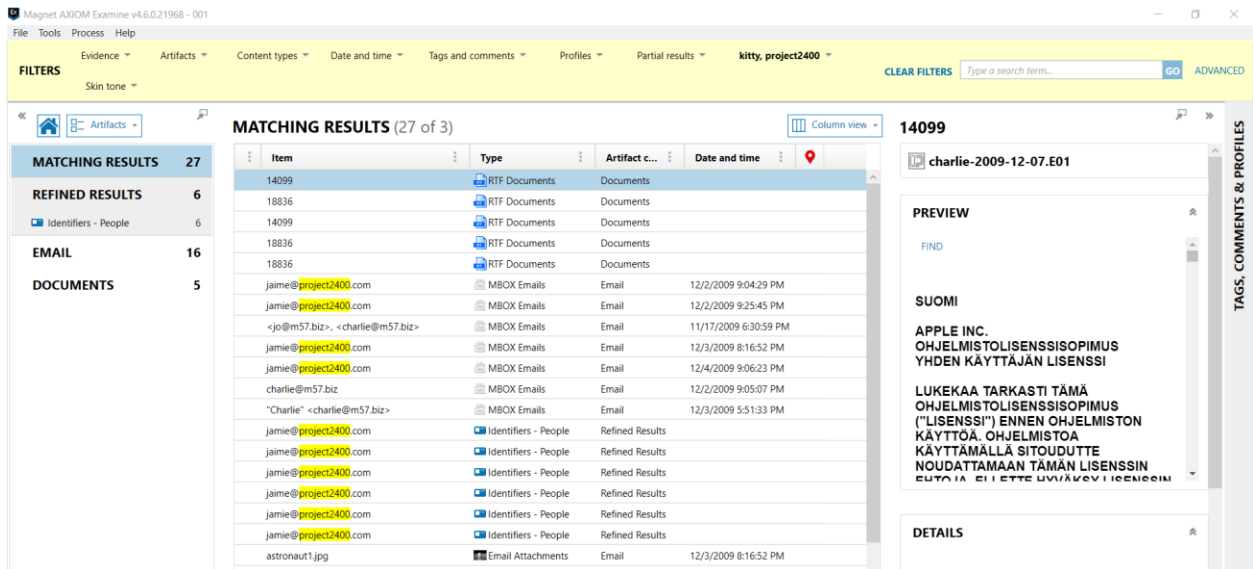
5. Accept the default setting Full, and click Next. Then click Go to Processing Details.
6. Scroll to the bottom of the page and click the Add Keyword button after clicking Add Keywords to Search. Enter project2400, craigslist, kitty, and kitten in the search box. Scroll down to ANALYZE EVIDENCE in the left pane if necessary. click the ANALYZE EVIDENCE button in the lower right corner.



Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)



7. The Magnet AXIOM Examine tool opens and starts running. When it's finished, click Results in the left pane and examine the findings.



8. Compare your results with your findings in Autopsy for Windows or OSForensics and note any discrepancies. Write a two- to three-page report, including screenshots, to submit to your instructor. Explain which tool you prefer to use and why.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Magnet By expediting the technical forensics process, AXIOM, a comprehensive software architecture optimized for digital investigations, enables researchers and forensics to discover information. digital. AXIOM automates the legal and automated forensics procedure for forensic evidence, including cellphones, the cloud, third-party apps, laptops, hard drives, and IoT systems. For analysis, combine data into a single optimal solution.

AXIOM captures, processes, and analyzes photos in order to recover data and present stakeholders with digital proof. Furthermore, because to automation and computer-based learning, forensics and forensic teams now have more money and time to analyze and analyse evidence in greater depth, requiring more advanced abilities, such as developing and applying specialized keyword searches, filters, and tags. AXIOM Magnet is the only tool that can collect and analyze data from a variety of sources, including cellphones, the cloud, computer devices, and even digital forensics software. AXIOM gives you a quick snapshot of all the digital evidence you've gathered. It is the first approach for analyzing data by processing, visualizing, analyzing, and reporting data in a consistent profile. Magnet. AI, the first machine learning capabilities in the market

Magnet AXIOM unifies and organizes data across cellphones and PCs into a single folder. Inspection tools aid forensics specialists in locating and visualizing the most important data for faster processing. Examiners can use AXIOM to access file system data, search data, fully decode data, and use Magnet.AI for contextual conversation analysis. Digital forensics experts use AXIOM to look for evidence of other device failures, verify data, and combine images of an altered method into an autopsy scenario. Planning analytically The AXIOM approach automates the process of acquiring and analyzing knowledge. AXIOM Examine enables for the efficient investigation of enormous volumes of data, allowing for the easy identification of the most essential evidence in a single case.

Digital Forensic Tools

Safal Lamichhane

Department of Computer Science, Southeast Missouri State University

Cy 620: Advanced Computer Forensics

Instructor's name: Dr. Mario Garcia

February 28, 2022

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Digital forensics investigators now have access to a wide range of commercial and open-source digital forensics tools. To varying degrees, these tools provide levels of abstraction that allow investigators to safely make copies of digital evidence and conduct routine investigations without becoming overwhelmed by low-level details like physical disk organization or the specific structure of complicated file types like the Windows registry.

Some of the current digital forensic tools are:

Sleuth kid and autopsy:

The Sleuth Kit (TSK) and Autopsy, two of the most prominent open-source digital investigative tools, have long been reliable options for volume system forensic research. Using a suite of command-line tools for examining disk images, the Sleuth Kit allows administrators to study file system data. TSK's powers are boosted by Autopsy, a graphical user interface and a digital forensics platform that is frequently utilized in public and private computer system investigations.

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

Autopsy is a user-friendly, GUI-based tool that allows you to quickly inspect hard drives and mobile devices. It offers a plug-in architecture that lets you find add-on modules or write bespoke Java or Python modules. On the other hand, Sleuth Kit is a set of command-line tools and a C library for analyzing disk images and retrieving files from them. It's utilized in Autopsy and a slew of other open source and commercial forensics software.

Windows registry analysis: Registry recon

Registry Recon gives you access to a massive amount of Registry data that has been effectively erased, whether due to benign system activity, user misconduct, or even IT personnel re-imaging. The Windows registry serves as a configuration store for the Windows operating system and the apps that run on it. Registry forensics has long been consigned to examining just easily available Windows Registries, one at a time, in an inefficient and outdated manner. Registry Recon is more than just a registry parser. Arsenal created new methods for parsing Registry data, allowing for the reconstruction of Registries that have existed on a Windows system over time, providing unique insight into how Registry data has changed over time. The registry is one of the most popular places where malware deploys persistence methods, and these applications can store several different data in it. The built-in Windows tool regedit can be used to open and view the Windows registry, and registry analysis is included in several forensics systems. Specialized tools, such as Registry Recon, are also available. Registry Recon is a commercial application for reconstructing Windows registries from forensic images. It also has the capacity to reconstruct deleted parts of the registry using unallocated memory space analysis.

Mobile forensics: Cellebrite UFED

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

With mobile forensics becoming more important, a mobile-focused forensics solution could be a good investment. The Cellebrite UFED is largely recognized as the best commercial mobile forensics tool available. It works on a variety of platforms (not only mobile devices) and includes exclusive methodologies and tools for mobile device analysis.

Usage:

- It helps in directly download its contents directly on to the device. We are able to extract contacts lists call history, text messages, browser history and many more.
- Sometimes, we don't even have to physically connect UFED to phone. The devices come with a set of cables that can link virtually every type of cell phone. It can also be connected through a Bluetooth which allows data to download secretly.
- Cell phone security features are potentially ineffective when using this. The company claims to penetrate user and locks of the phone on over 200 devices. So, the users of all types of mobile devices are potentially at risk.
- The most powerful feature is cloning to your phone SIM card. Furthermore, if the same cell tower provides service to both cloned phones then we can also listen on calls.

Linux distributions: CAINE

CAINE (Computer Aided INvestigative Environment) is an Italian live GNU/Linux distribution developed as part of a Digital Forensics project. It was designed to provide all the forensic tools that are required to perform investigation process. The process includes preservation, collection, examination, and analysis. IT is a user-friendly GUI which can be booted from flash drives and run in memory. We don't need to boot the OS to operate on data storage by using CAINE. CAINE has a several applications, libraries and scripts that can be used in a CLI or a GUI to perform forensic

Violations of academic honesty represent a serious breach of discipline and may be considered grounds for disciplinary action, including dismissal from the University. The University requires that all assignments submitted to faculty members by students be the work of the individual student submitting the work. An exception would be group projects assigned by the instructor. (Source: SEMO website)

activities. It can also be used to perform data analysis on the data objects which are created on linux, Windows and some Unix systems.

CAINE Linux provides some tools like Autopsy, Wireshark, PhotoRec, Fsstat, RegRipper, Tinfoleak etc.

References:

<https://www.caine-live.net/>

<https://www.sleuthkit.org/>

<https://arsenalrecon.com/products/>

<https://cellebrite.com/en/ufed/>