

School of Computing
IT8003 Digital Forensics and Investigation

Practical 1B: Create Case and Process Evidence

Introduction

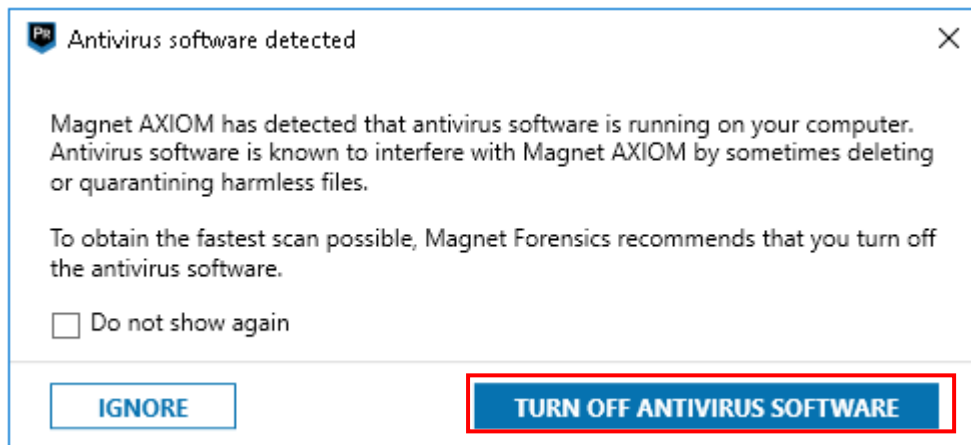
In Digital Forensics, once you have acquired the data of the subject's device in a forensically sound manner. The next step before doing your analysis is to do a working copy of the original copy that you had acquired from. There after you will want to process the working copy with a forensic software to verify your working copy, extract/crave and begin to perform your analysis.

Learning Objective

In this Practical, students will be able to process the acquire data called image files (. E01 - an encase proprietary format). Creating a case file and process it to verify image file (. E01) to ensure that the acquired image is a bit-for-bit copy of the original copy by generating a hash value within AXIOM Process.

Exercise 1. Creating a Case using Magnet Axion and Processing Case Evidence

1. Run “**AXIOM Process**”
2. Click “**Turn Off Antivirus software**” when prompted to turn off the anit-virus



3. Click on “**Create New Case**”

 Magnet AXIOM Process 3.10.0.18500

File Tools Help

CREATE NEW CASE

[CREATE NEW CASE](#)

ADD EVIDENCE TO EXISTING CASE

Open existing AXIOM case folder

[BROWSE TO A CASE](#)

Open a recent case

No recent cases

4. Fill in the following:

Text Field	Output	Description
Case Information		
Case Name	DFI_Practical_001	In Digital forensics, the case name is usually generated by the Forensic Investigator. An organization usually will have its standard naming convention for a forensic case. The forensic investigator will refer to the organization's standard to generate the case name.
Location for Case File		
Folder Name	DFI_Practical_Case1	This location for case files is where AXIOM saves the main database of the processed case along with supporting files. This database contains all of the artifacts that were located during processing. When working in AXIOM, the majority of information that you view is being pulled from the database in this location.
File Path	<Desired Path of Storing the Case>	The defined the full path where the case is stored in.
Location for Acquired Evidence		
Folder Name	DFI_Practical_Evidence1	This location is where AXIOM saves the forensic image that was extracted from the item of evidence (e.g., the hard drive or the cell phone). This forensic image contains all data that was able to be extracted, and it is significantly larger than the main case database.
File Path	<Desired Path of Storing the Case>	The defined the full path where the acquired evidence is stored in.
Scan Information		
Scanned By	<Name_StudentID>	The name of the forensic investigation
Description	Practical Exercise 1: Creating and Processing Evidence	Description of the forensic investigation. Usually includes the acquire evidence's specifications such as hard disk brand, model, size and serial number.

Magnet AXIOM Process 3.10.0.18500
File Tools Help

CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Search archives and mobile backups On
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE

CASE DETAILS

CASE INFORMATION

Case number: DFL_Practical_001
Case type: Select case type...

LOCATION FOR CASE FILES

Folder name: DFL_Practical_Case1
File path: C:\Users\common\Desktop\Pract1B BROWSE
Available space: 23.54 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name: DFL_Practical_Evidence1
File path: C:\Users\common\Desktop\Pract1B BROWSE
Available space: 23.54 GB

SCAN INFORMATION

SCAN 1

Created on: 9/28/2020 2:54:03 PM
Scanned by: Bernard Tang
Description: Practical Exercise 1: Creating and Processing Evidence Case
GO TO EVIDENCE SOURCES




- Upon complete of filling in the information, click on “Go to Evidence Source” at the bottom left of the AXIOM Process interface to proceed on adding the acquired evidence hard disk to the case.
- To add the acquired evidence, click on “Computer” within the Evidence Source tab

Magnet AXIOM Process 3.10.0.18500
File Tools Help

CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Search archives and mobile backups On
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE

EVIDENCE SOURCES

SELECT EVIDENCE SOURCE

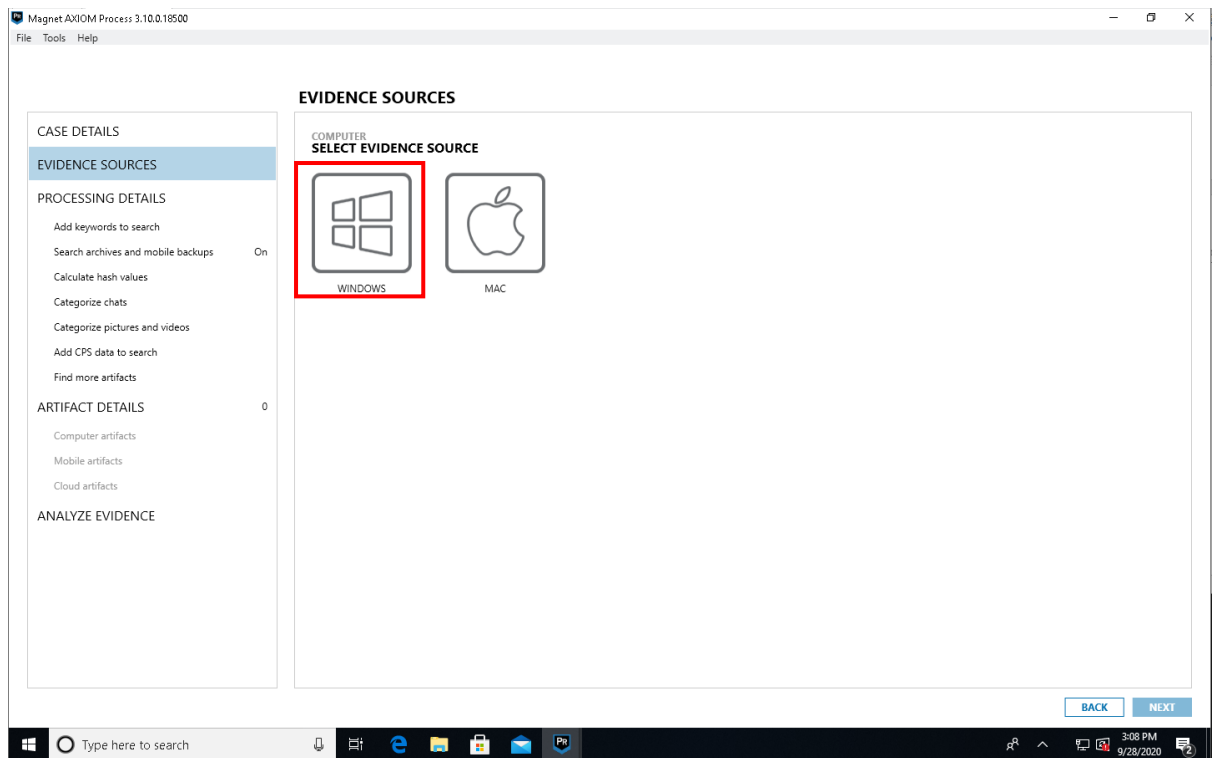
 COMPUTER
 MOBILE
 CLOUD

EVIDENCE SOURCES ADDED TO CASE

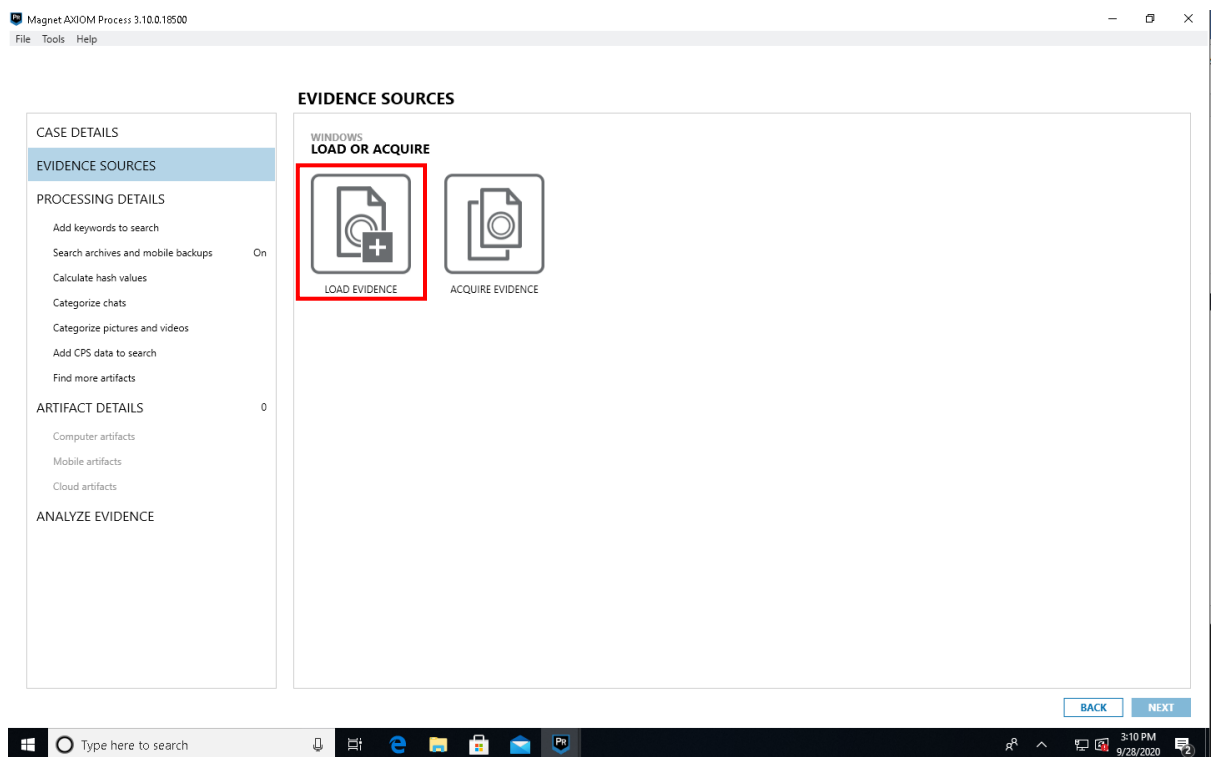
Type	Image - location name	Evidence number	Search type	Status
------	-----------------------	-----------------	-------------	--------

BACK
GO TO PROCESSING DETAILS

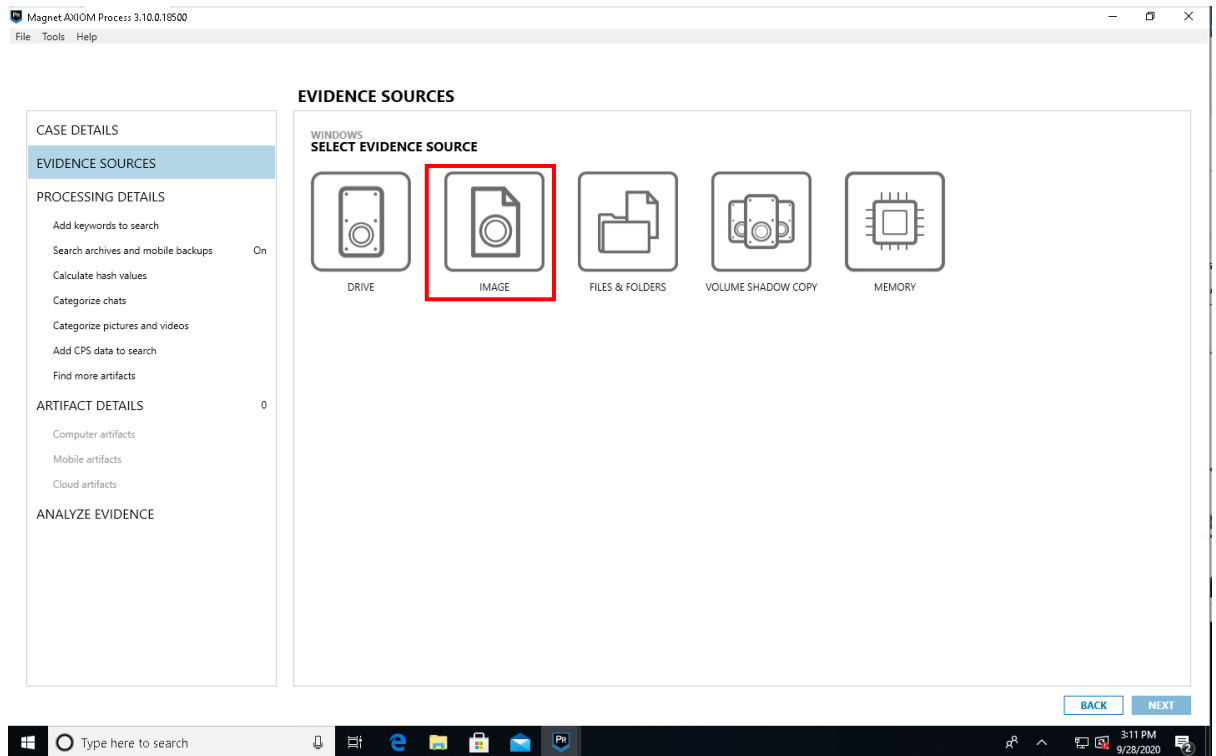
7. Click on “Window”



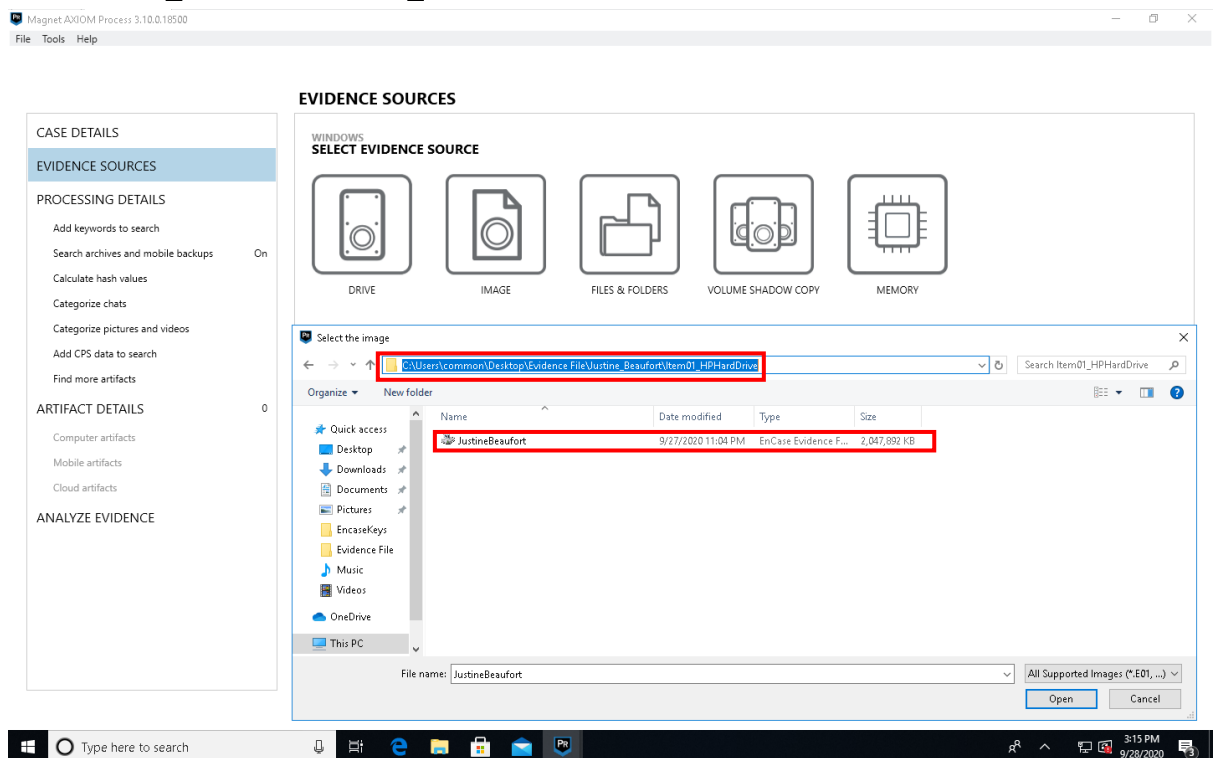
8. Click on “Load Evidence”



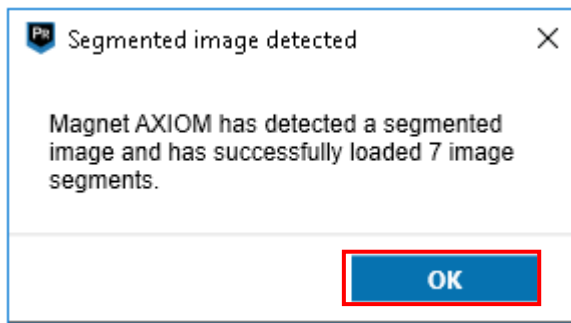
9. Click on “Image”



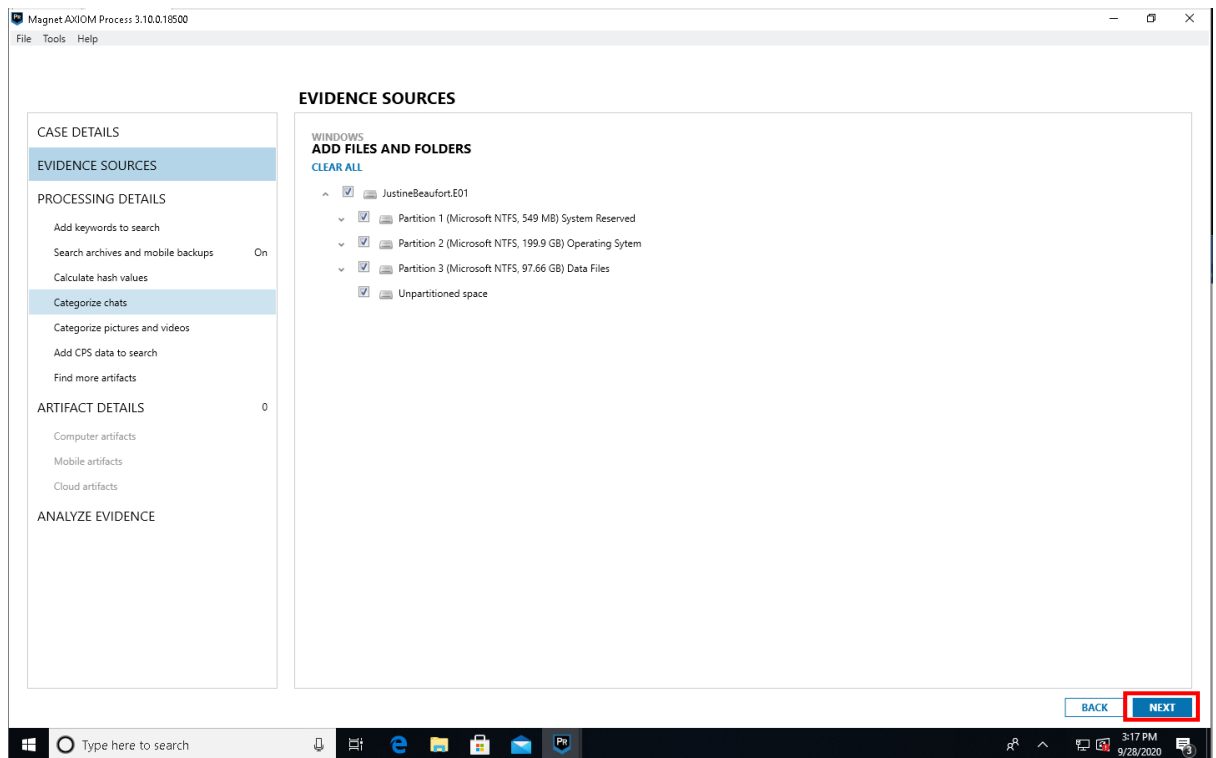
10. Browse to “C:\Users\common\Desktop\Evidence File\Justine_Beaufort\Item01_HPHardDrive”



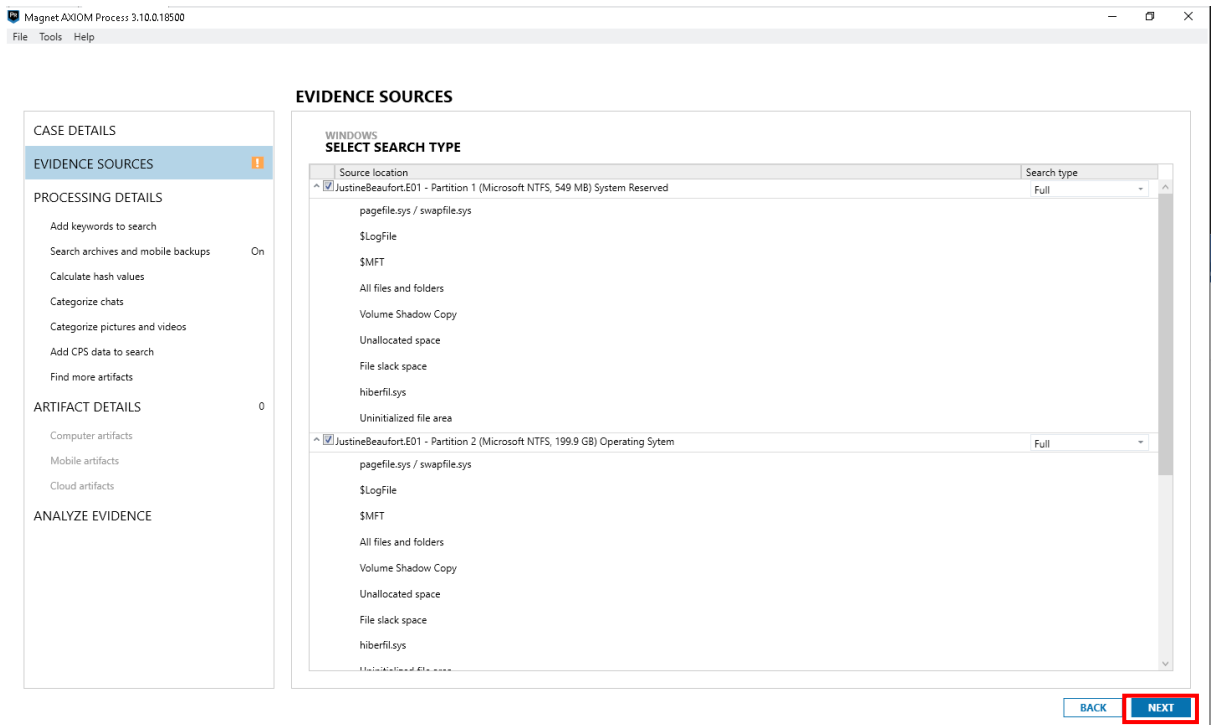
11. Click “Ok”, when



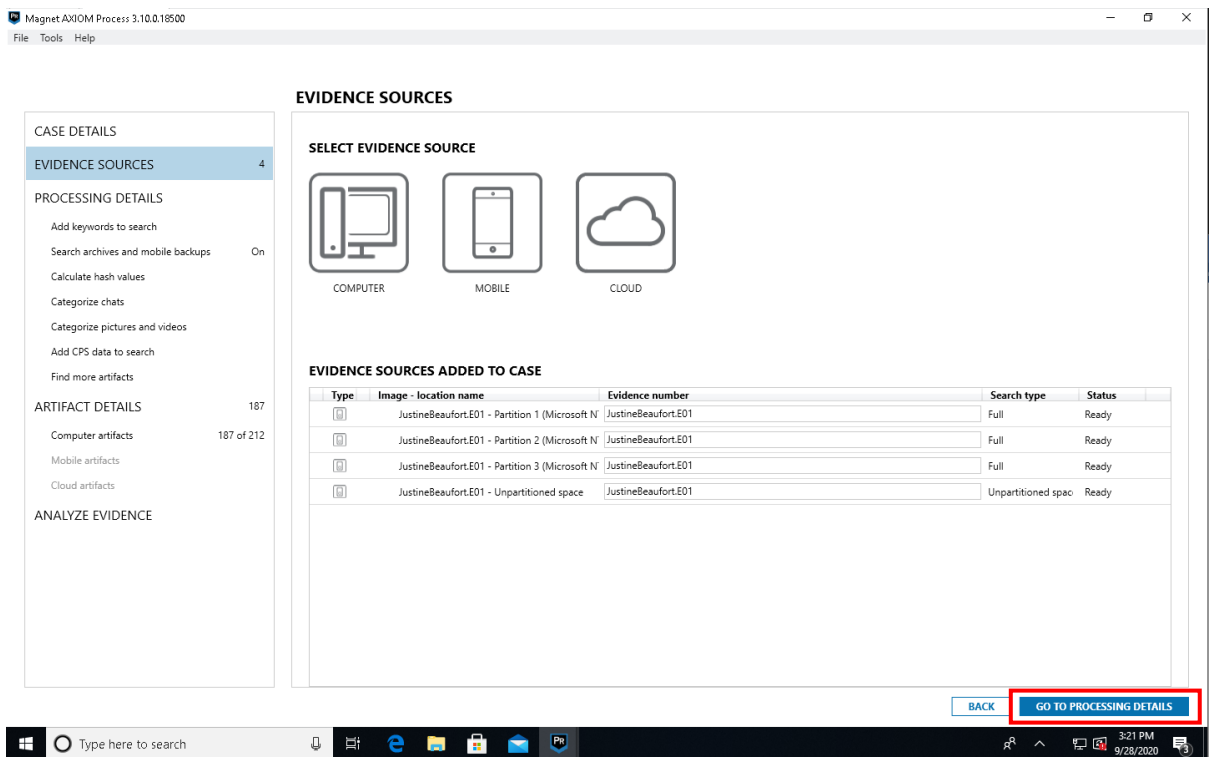
12. Click “Next”



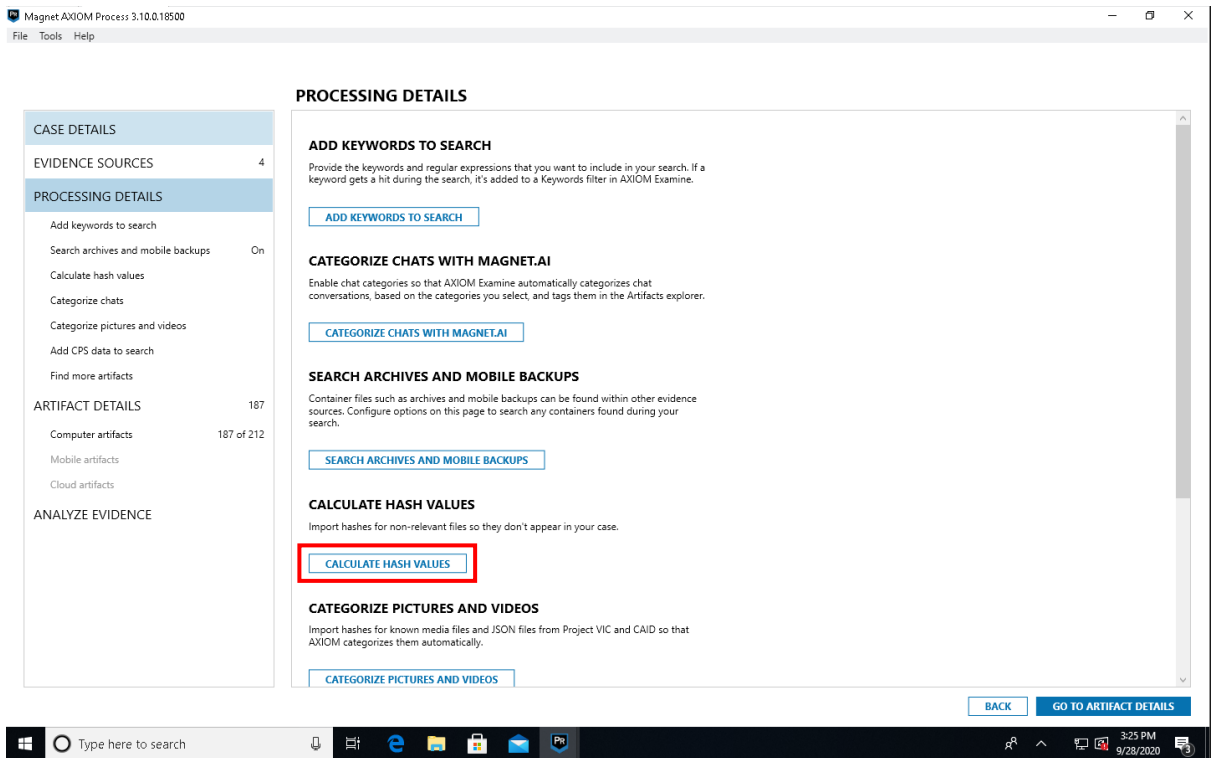
13. Leave the setting as it is and click “Next”



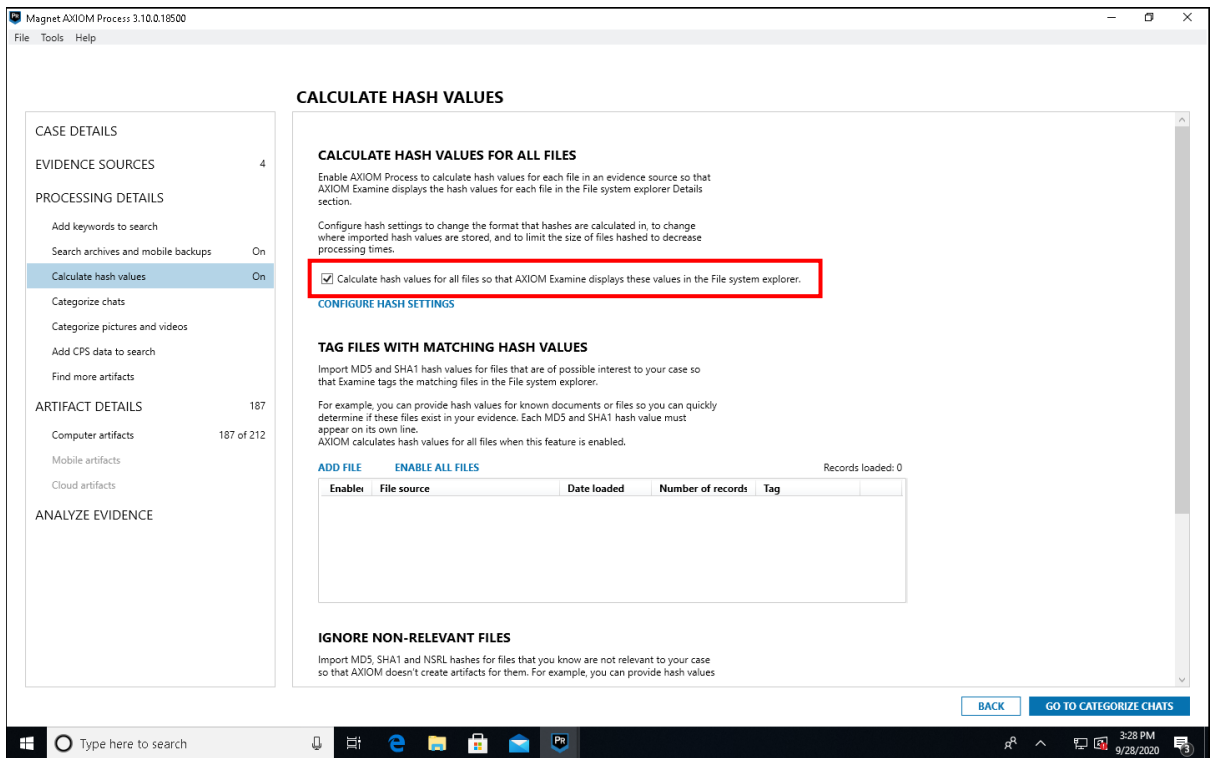
14. Leave the setting as it is and click “Go to Processing Details”



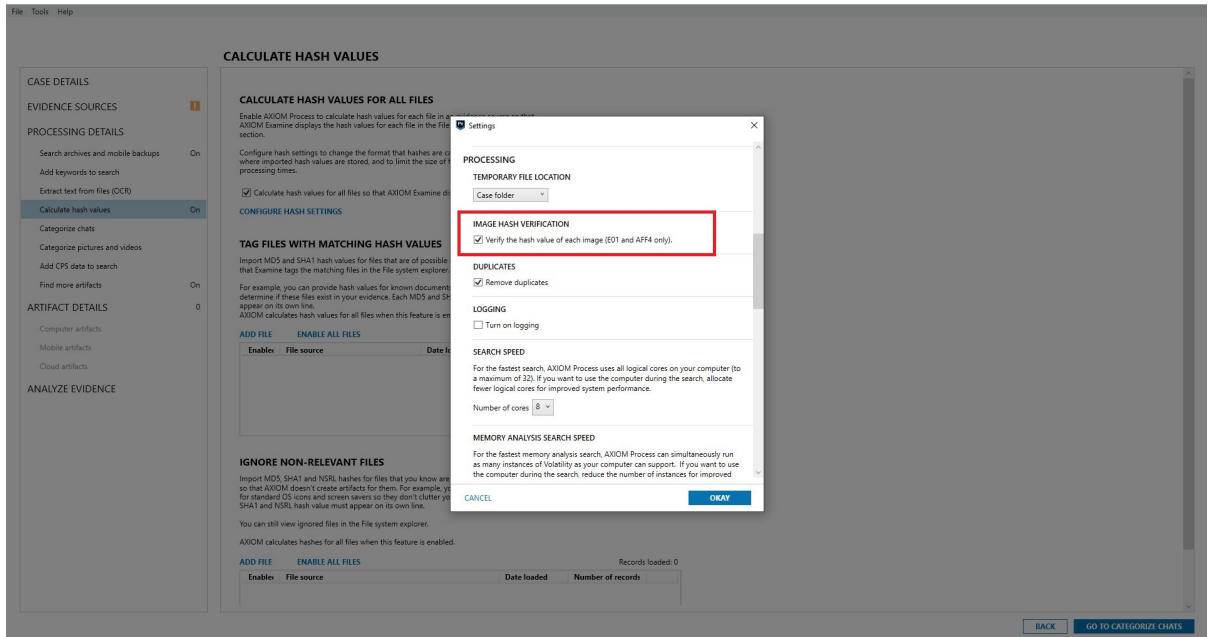
15. We are required to calculate and computer the hash of every file for this practical as Digital Forensic emphasize on the hash to ensure the accuracy of the evidence. With that in mind, Click on “Calculate Hash Values”



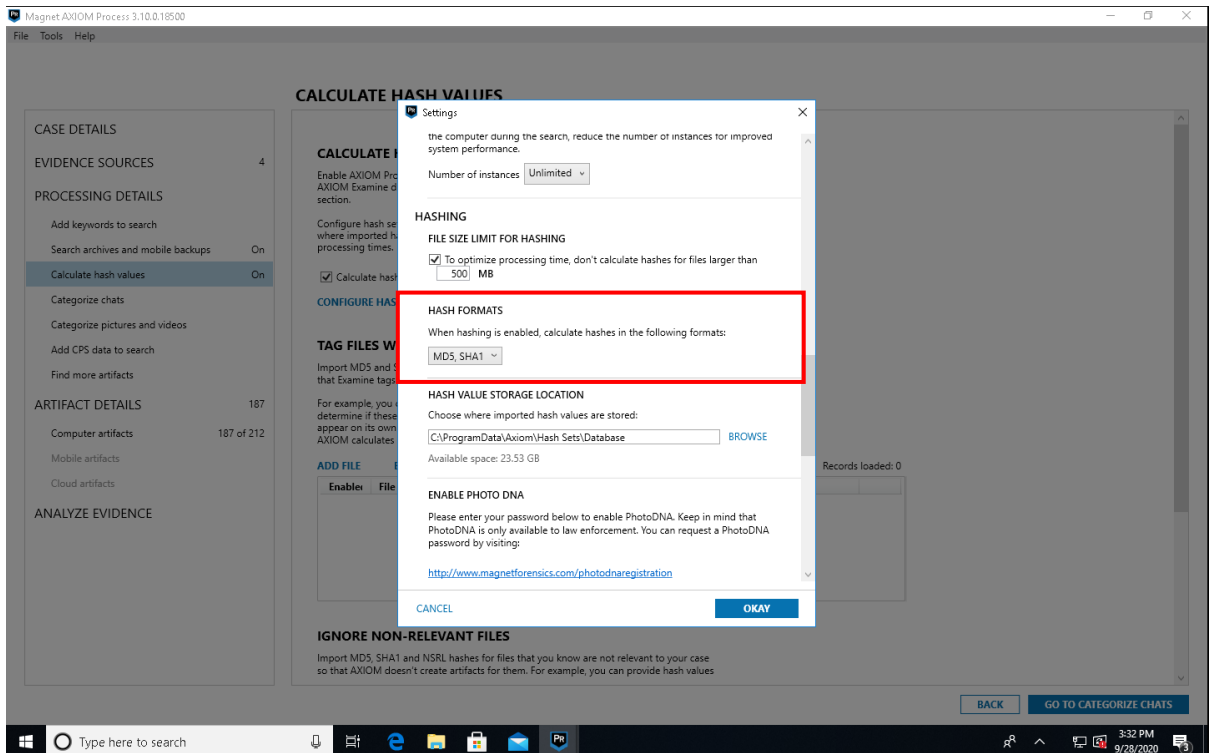
16. Select the “Calculate hash values for all files so that AXIOM Examine displays these values in the File system Explorer”



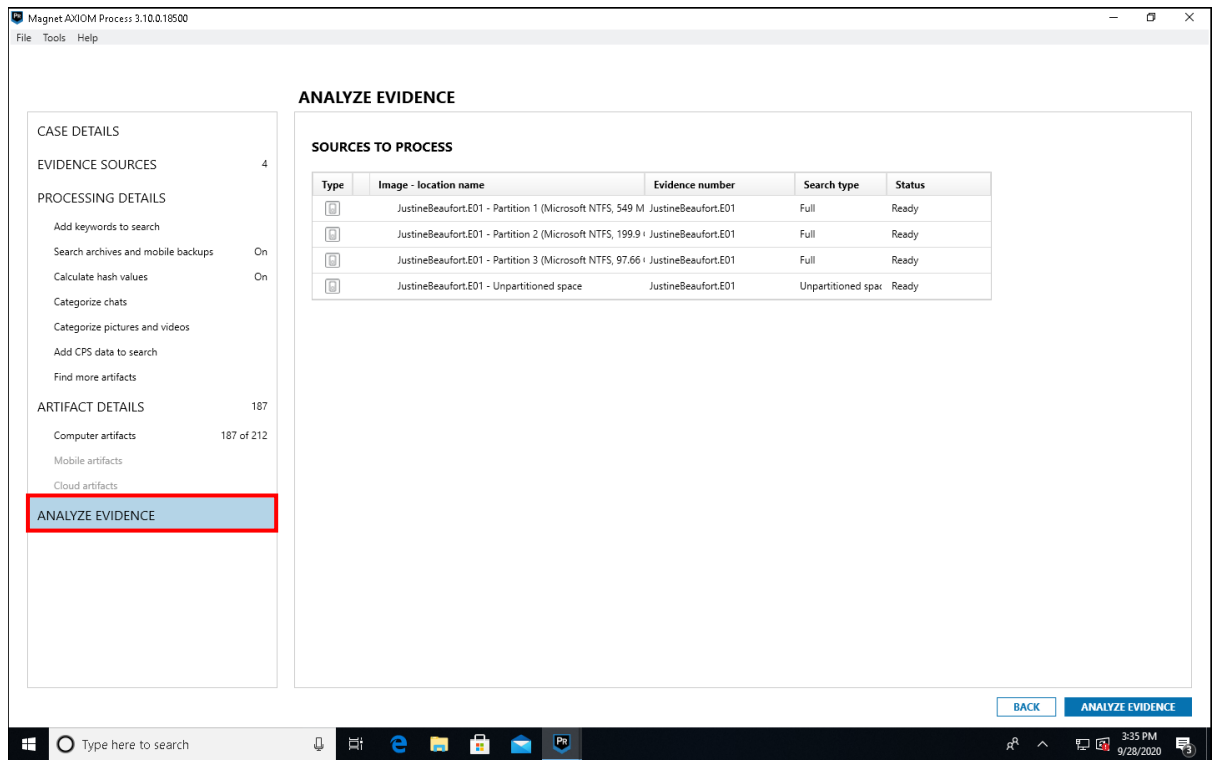
17. Click on “**Configure Hash Settings**”, a window settings will pop up, scroll down the window settings to “**PROCESSING**” and ensure the check box is tick on “**IMAGE HASH VERIFICATION**” (Gives “*JustineBeaufort.E01*” image file a verification hash)



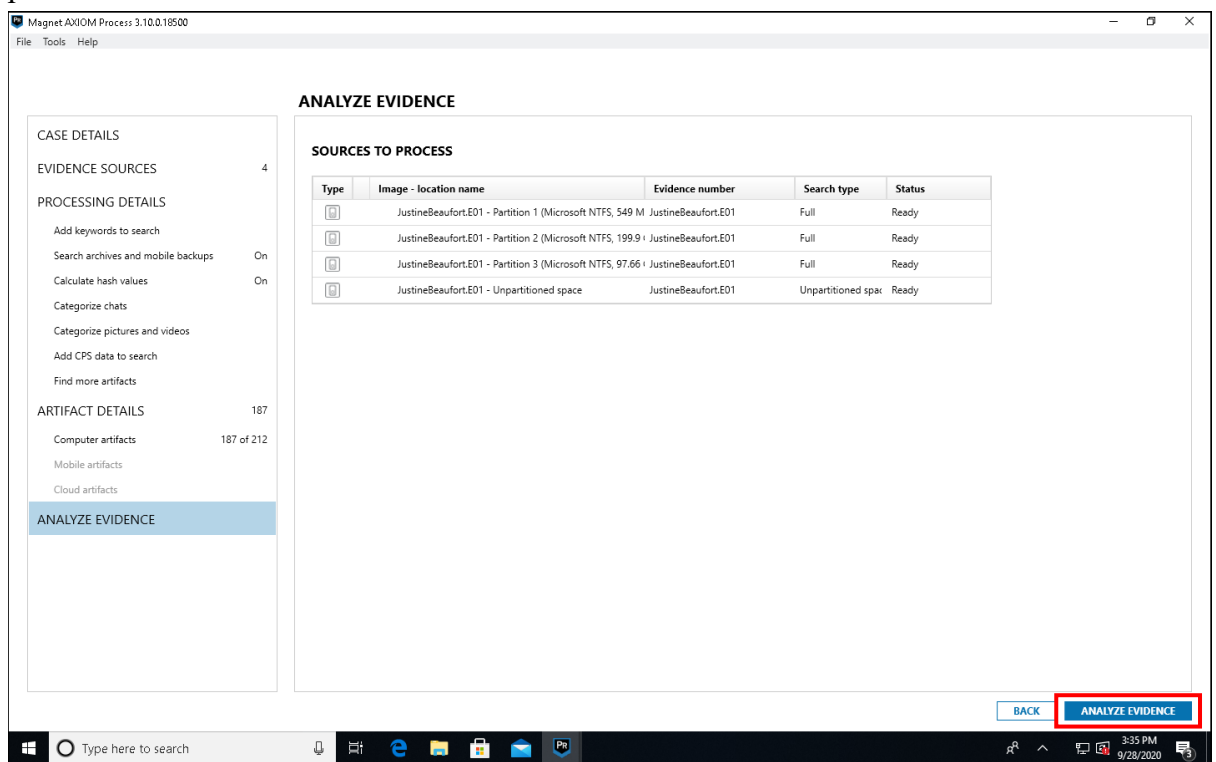
18. Click on “**Configure Hash Settings**”, scroll down to “**Hash Formats**” change the options to “**MD5, SHA1**” and then click on “**Okay**”



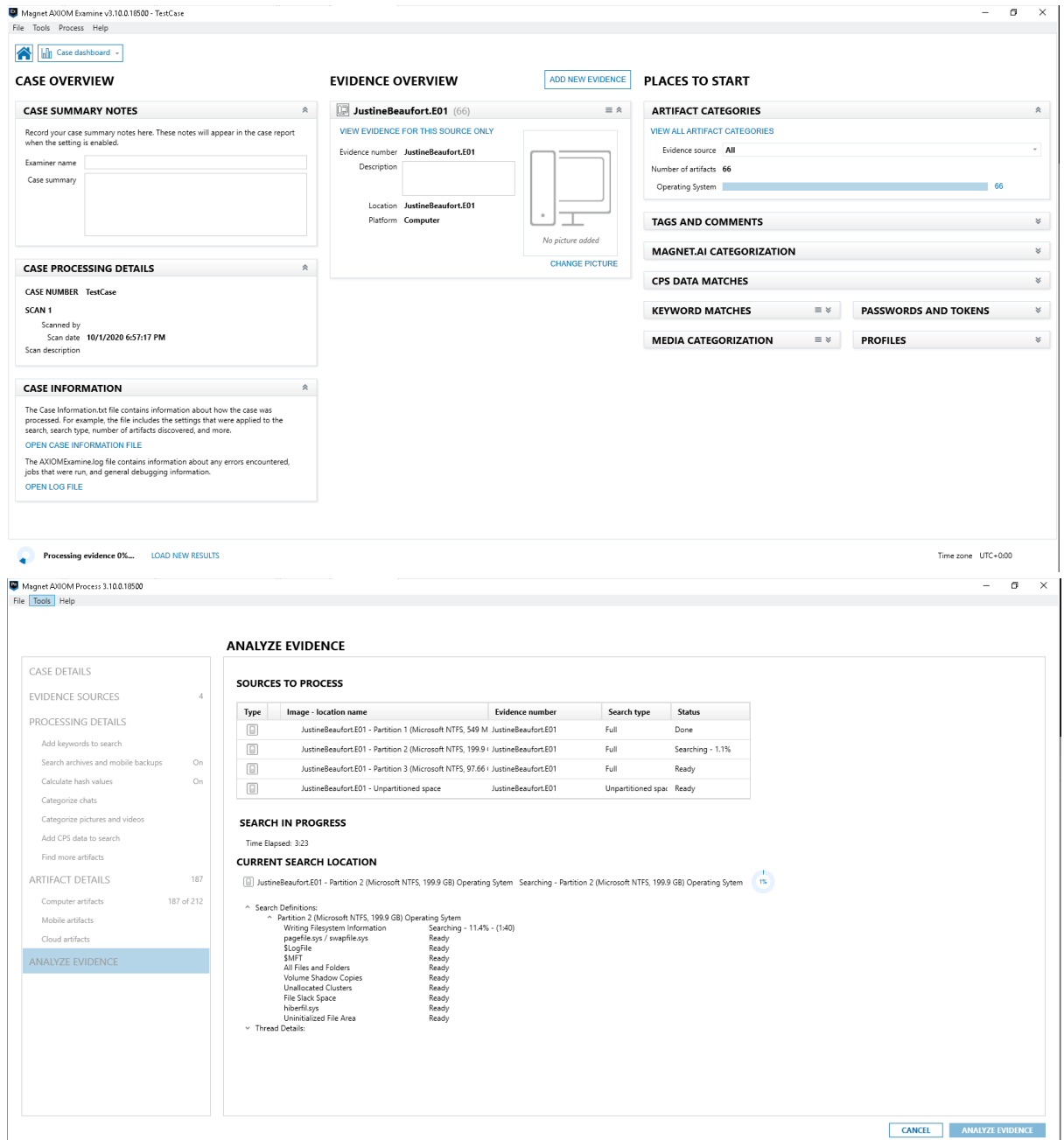
19. After all the configurations were selected you may skip all the other configurations and move on to “**Analyze Evidence**” on the left panel of the interface.



20. Click on “Analyze Evidence” on the bottom right of the AXIOM Process interface to process the evidence



21. Magnet AXIOM Process will now initiate the processing of the evidence. At the same time, Magnet AXIOM Examine application will start, you will notice that there will be 2 application.



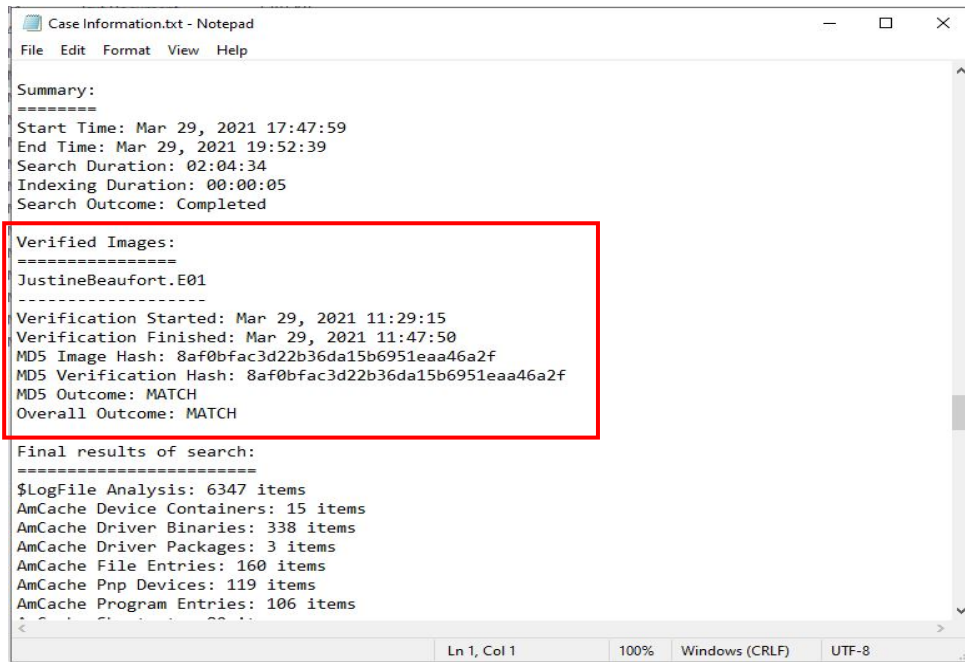
22. The process of analyzing and processing the evidence would take up to 3 hours to complete. You may skip this process, close all AXIOM application, and proceed on to Practical 2 exercises.

23. Assuming that processing is completed. Mentioned in the earlier section (4.) of this practical. Navigate and locate the text file “Case Information.txt”.

- a. Location for Case File
 - i. Folder Name: DFI_Practical_Case1
 - ii. File Path: <Your Preferred Path> where you had created for this

exercise

24. Scroll Down to “**Verified Images**”. You will be able to see the verification hash matches the acquired image file (. E01). Thus, verify that a forensic image was captured successfully (*bit-for-bit copy*).



```
Case Information.txt - Notepad
File Edit Format View Help

Summary:
=====
Start Time: Mar 29, 2021 17:47:59
End Time: Mar 29, 2021 19:52:39
Search Duration: 02:04:34
Indexing Duration: 00:00:05
Search Outcome: Completed

Verified Images:
=====
JustineBeaufort.E01
-----
Verification Started: Mar 29, 2021 11:29:15
Verification Finished: Mar 29, 2021 11:47:50
MD5 Image Hash: 8af0bfac3d22b36da15b6951eaa46a2f
MD5 Verification Hash: 8af0bfac3d22b36da15b6951eaa46a2f
MD5 Outcome: MATCH
Overall Outcome: MATCH

Final results of search:
=====
$LogFile Analysis: 6347 items
AmCache Device Containers: 15 items
AmCache Driver Binaries: 338 items
AmCache Driver Packages: 3 items
AmCache File Entries: 160 items
AmCache Pnp Devices: 119 items
AmCache Program Entries: 106 items
Ln 1, Col 1    100%    Windows (CRLF)    UTF-8
```

-- End --