School of Computing
IT8003 Digital Forensics and Investigation

Practical 1: Create Case and Process Evidence Mobile

Introduction

1. 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. 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.

Objective

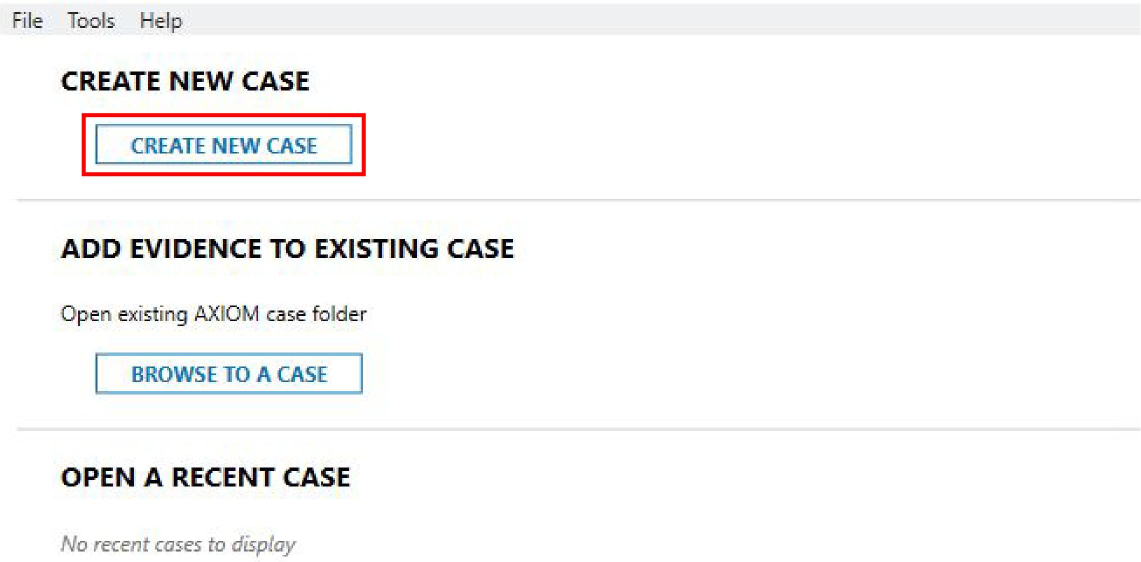
2. In this Practical, you will be able to process the acquire data called image files regarding mobile device and Creating a case file for analysis later on in the practical.

Before you Begin

3. Please navigate to "**C:\Baseimages\ForensicV5**". Look for "**Practical_1_Android_Image**" and extract/copy the file to your preferred location.

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

4. Before running "**AXIOM Process**" turn off windows anti-virus first
   a. **Start** > **Settings** > **Update & Security** > **Windows Security** > **Virus & threat protection** > **Manage settings** (or **Virus & threat protection** settings in previous versions of Windows 10)
   b. Switch **Real-time protection** to **Off**
5. Run "**AXIOM Process**"
6. Click on "**Create New Case**"



CREATE NEW CASE

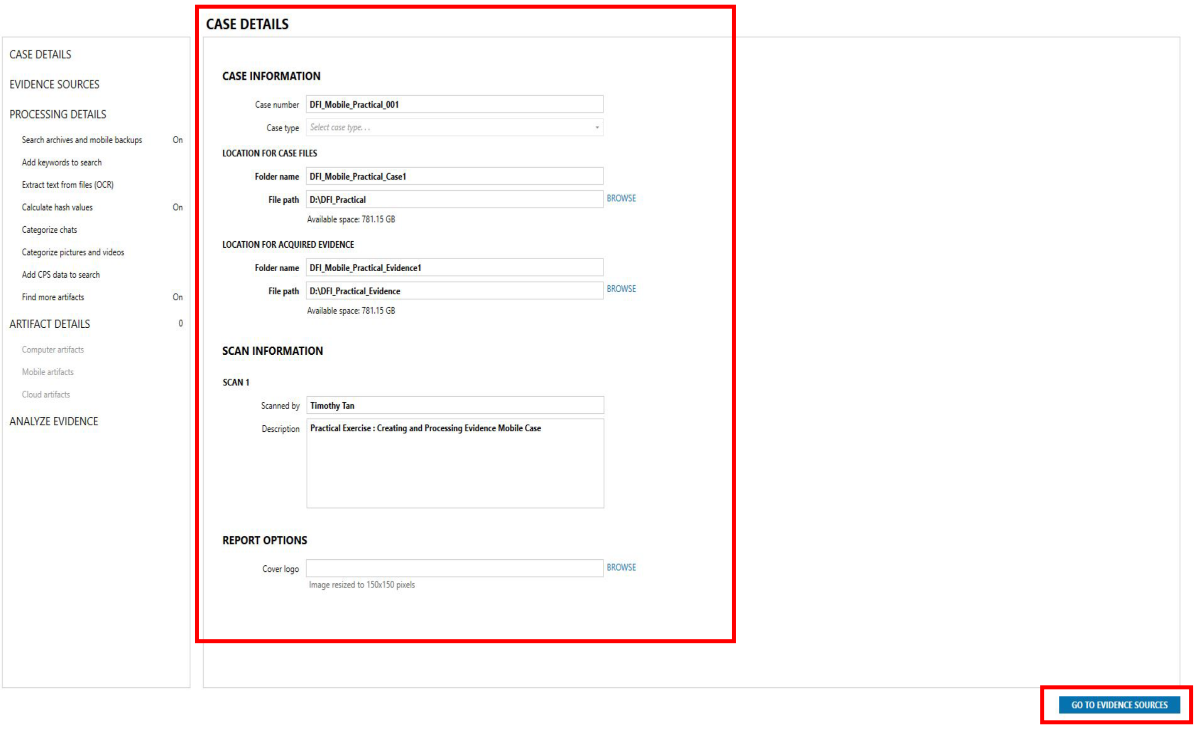
ADD EVIDENCE TO EXISTING CASE

Open existing AXIOM case folder

OPEN A RECENT CASE

No recent cases to display

7. Fill in the following details in the first Section "**CASE DETAILS**"
   a. Case Information
      i. Case Name : **DFI_Mobile_Practical_001**
   b. Location for Case File
      i. Folder Name: **DFI_Mobile_Practical_Case1**
      ii. File Path: **<Your Preferred Path>**
   c. Location For Acquired Evidence *(This location is where you had acquire an evidence and store the image File (.E01, AFF4 etc.) using AXIOM Process)*
      i. Folder Name: **DFI_Mobile_Practical_Evidence1**
      ii. File Path: **<Your Preferred Path>**
   d. Scan Information
      i. Scanned By: **<Student's Name>**
      ii. Description: **Practical Exercise 1: Creating and Processing Evidence Mobile Case**
   e. Click on "**Go to Evidence Source**" at the bottom right of the AXIOM Process interface to bring you the next section "**EVIDENCE SOURCES**".



Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values On
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts On

CASE DETAILS

CASE INFORMATION

Case number DFI_Mobile_Practical_001
Case type *Select case type...*

LOCATION FOR CASE FILES

Folder name DFI_Mobile_Practical_Case1
File path D:\DFI_Practical
Available space: 781.15 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name DFI_Mobile_Practical_Evidence1
File path D:\DFI_Practical_Evidence
Available space: 781.15 GB

SCAN INFORMATION

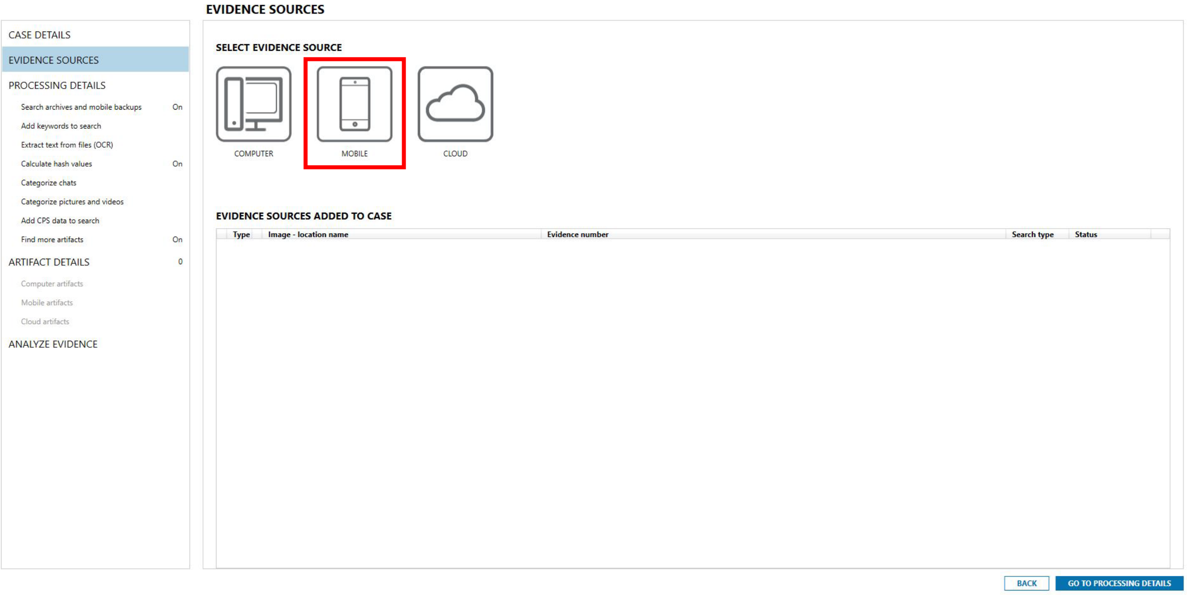
SCAN 1

Scanned by Timothy Tan
Description Practical Exercise : Creating and Processing Evidence Mobile Case

REPORT OPTIONS

Cover logo
Image resized to 150x150 pixels

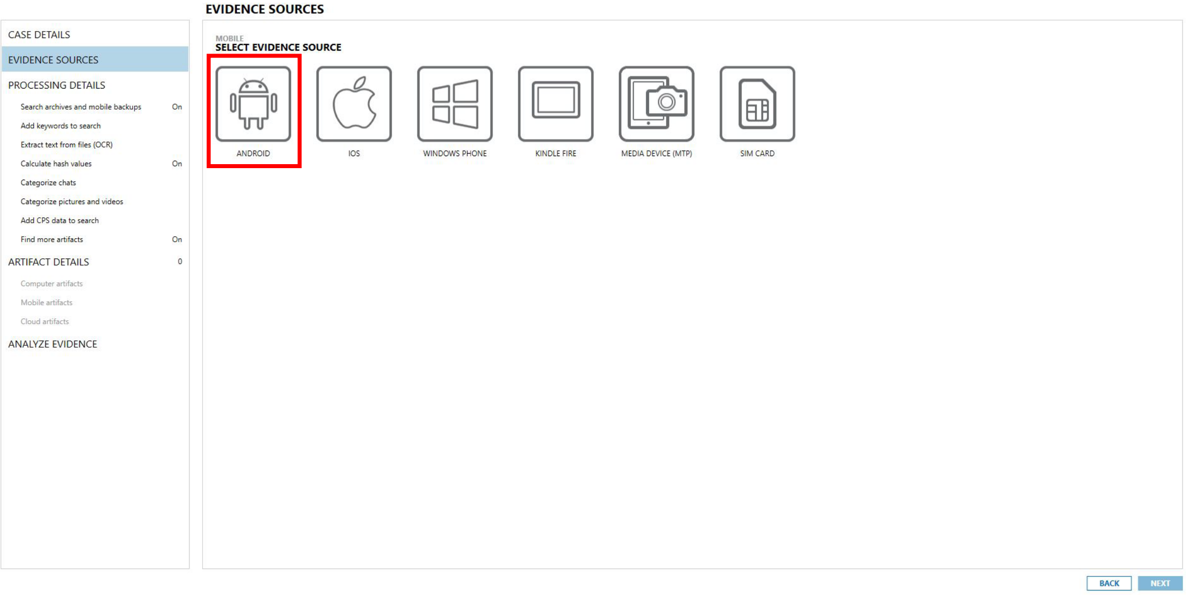
8. Click on “**MOBILE**”



Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values On
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts On

Type	Image - location name	Evidence number	Search type	Status

9. Click on "**ANDROID**"

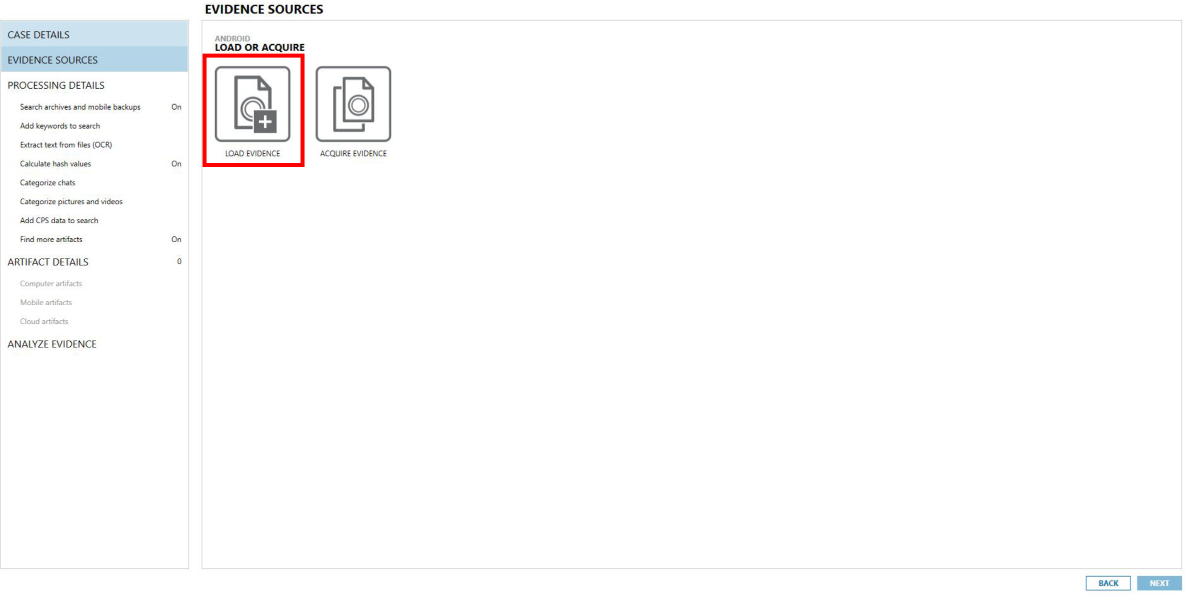


EVIDENCE SOURCES

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

MOBILE
SELECT EVIDENCE SOURCE

10. Click on "**LOAD EVIDENCE**"

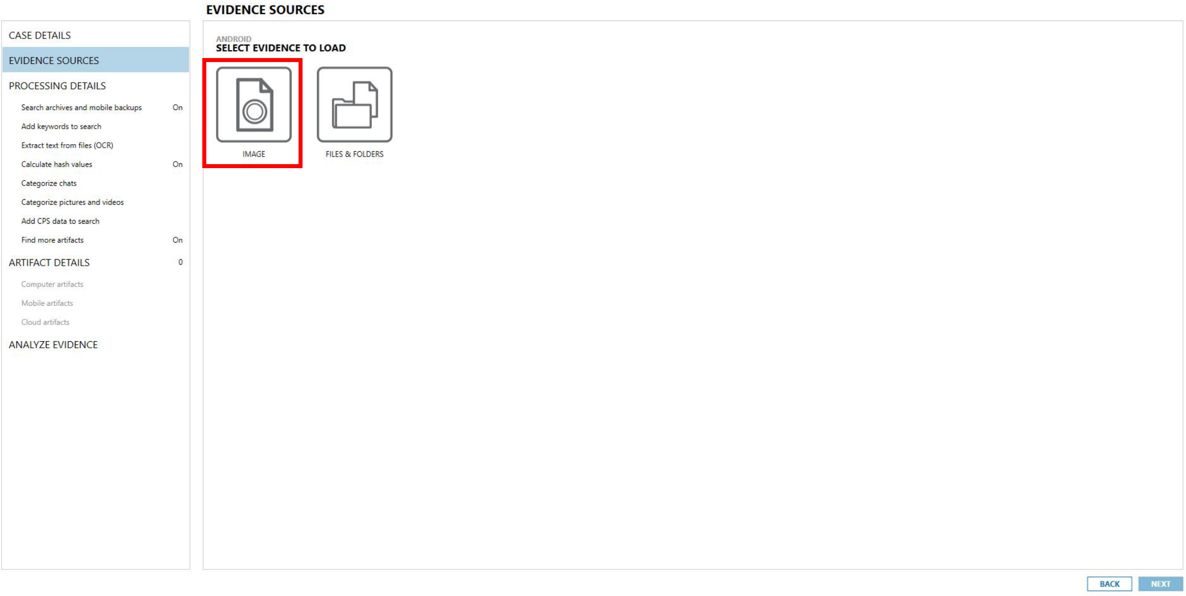


EVIDENCE SOURCES

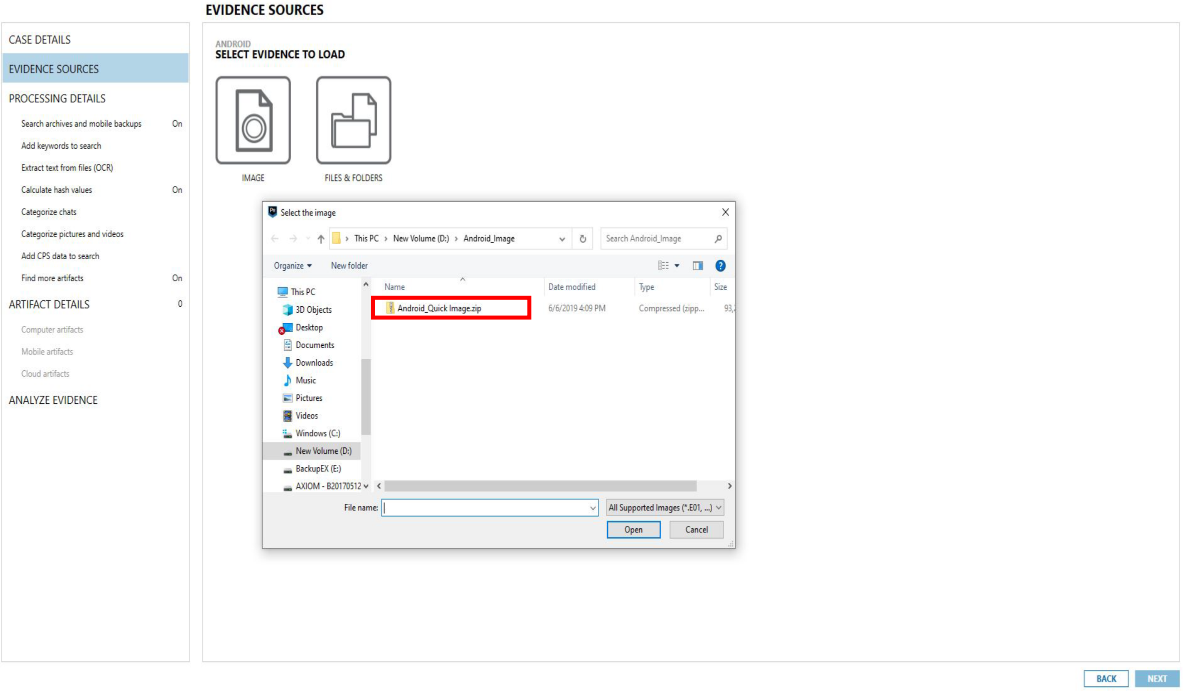
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values On
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts On
ARTIFACT DETAILS 0
Computer artifacts
Mobile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

ANDROID
LOAD OR ACQUIRE

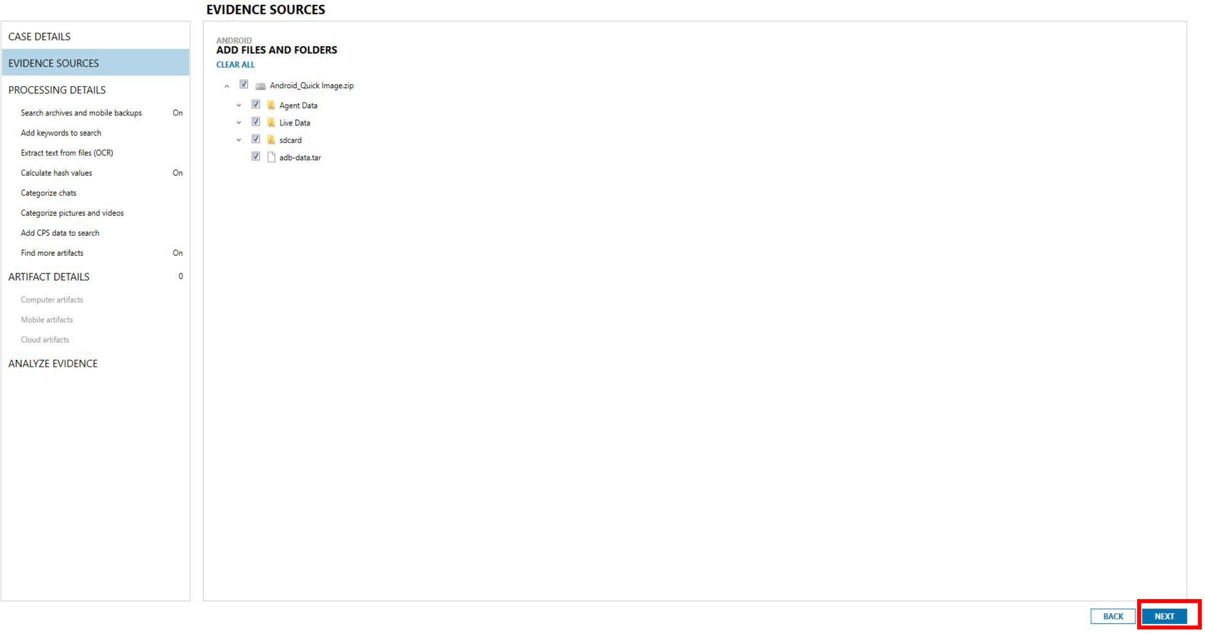
11. Click on “**IMAGE**”



12. Browse to the location where you had saved your extracted “**Practical_1_Android_Image.zip**” file. Navigate to the file “**Android_Quick Image.zip**”.

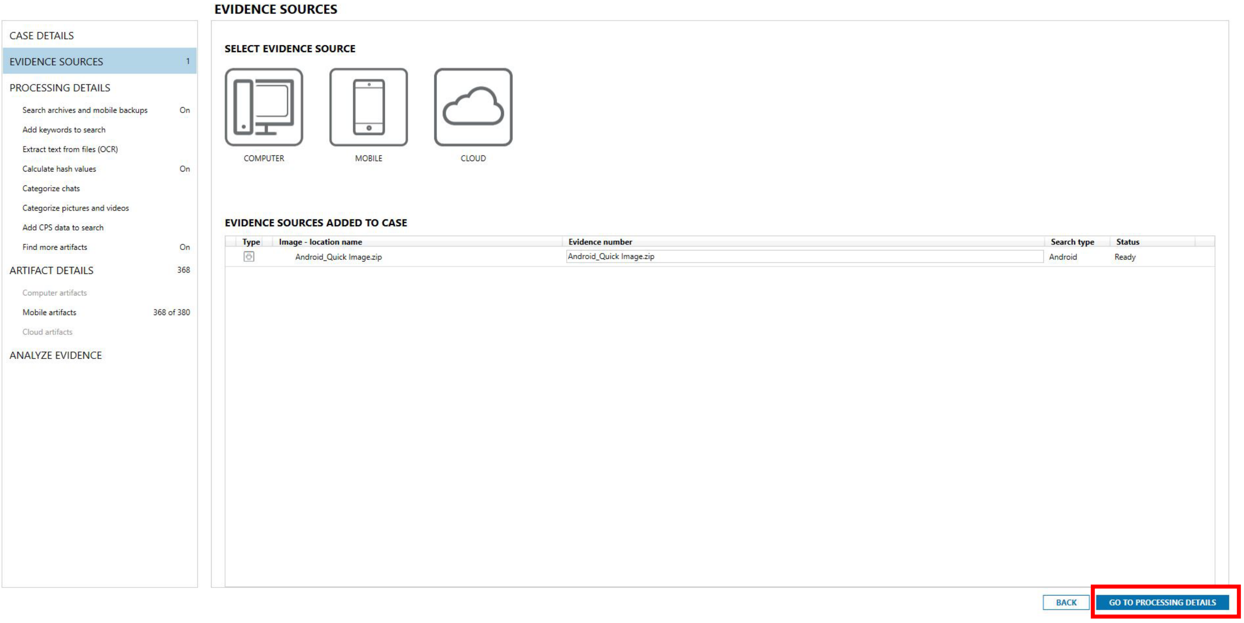


13. Click “**Next**”



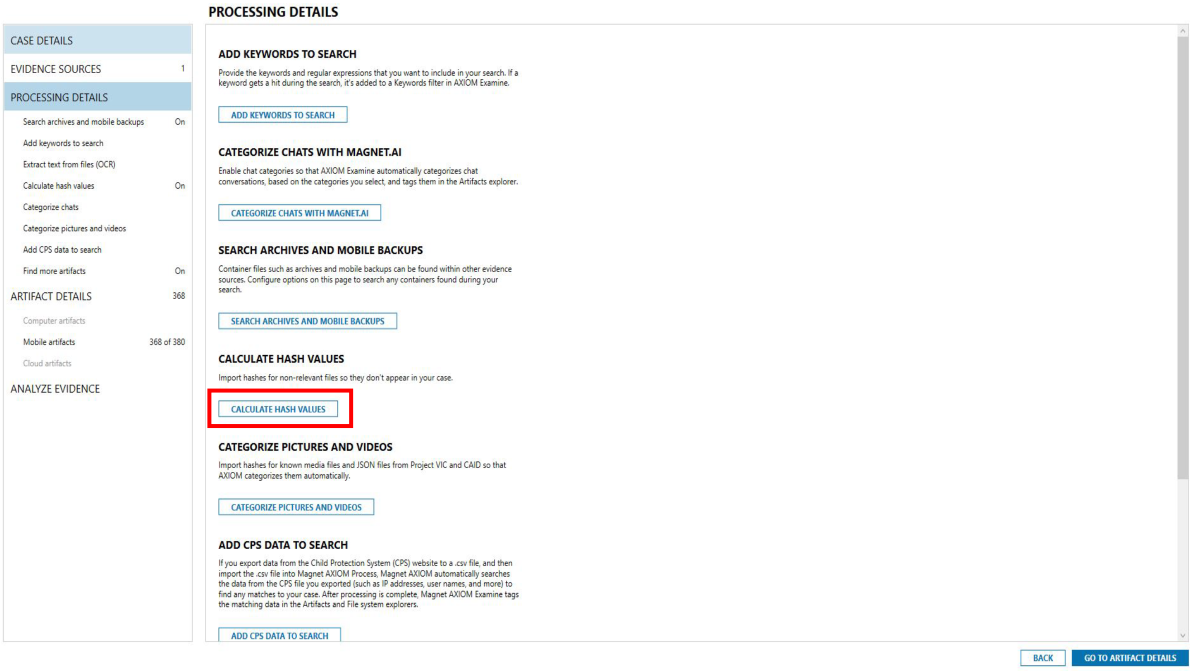
14. Leave the setting as it is and click “**Next**”

15. Leave the setting as it is and click “**Go to Processing Details**” at bottom right of the AXIOM Process interface to bring you the next section “**PROCESSING DETAILS**”.



Type	Image - location name	Evidence number	Search type	Status
	Android_Quick Image.zip	Android_Quick Image.zip	Android	Ready

16. In Digital Forensic principle, data through forensic acquisition, extraction or copied from electronic devices, storage media, and electronic files are authenticated by "hash value". We are required to calculate the hash value of the image that we have acquired from the computer to ensure the integrity of it. Click on “**Calculate Hash Values**”



PROCESSING DETAILS

CASE DETAILS
EVIDENCE SOURCES 1
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values On
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts On
ARTIFACT DETAILS 368
Computer artifacts
Mobile artifacts 368 of 380
Cloud artifacts
ANALYZE EVIDENCE

ADD KEYWORDS TO SEARCH

Provide the keywords and regular expressions that you want to include in your search. If a keyword gets a hit during the search, it's added to a Keywords filter in AXIOM Examine.

ADD KEYWORDS TO SEARCH

CATEGORIZE CHATS WITH MAGNET.AI

Enable chat categories so that AXIOM Examine automatically categorizes chat conversations, based on the categories you select, and tags them in the Artifacts explorer.

CATEGORIZE CHATS WITH MAGNET.AI

SEARCH ARCHIVES AND MOBILE BACKUPS

Container files such as archives and mobile backups can be found within other evidence sources. Configure options on this page to search any containers found during your search.

SEARCH ARCHIVES AND MOBILE BACKUPS

CALCULATE HASH VALUES

Import hashes for non-relevant files so they don't appear in your case.

CALCULATE HASH VALUES

CATEGORIZE PICTURES AND VIDEOS

Import hashes for known media files and JSON files from Project VIC and CAID so that AXIOM categorizes them automatically.

CATEGORIZE PICTURES AND VIDEOS

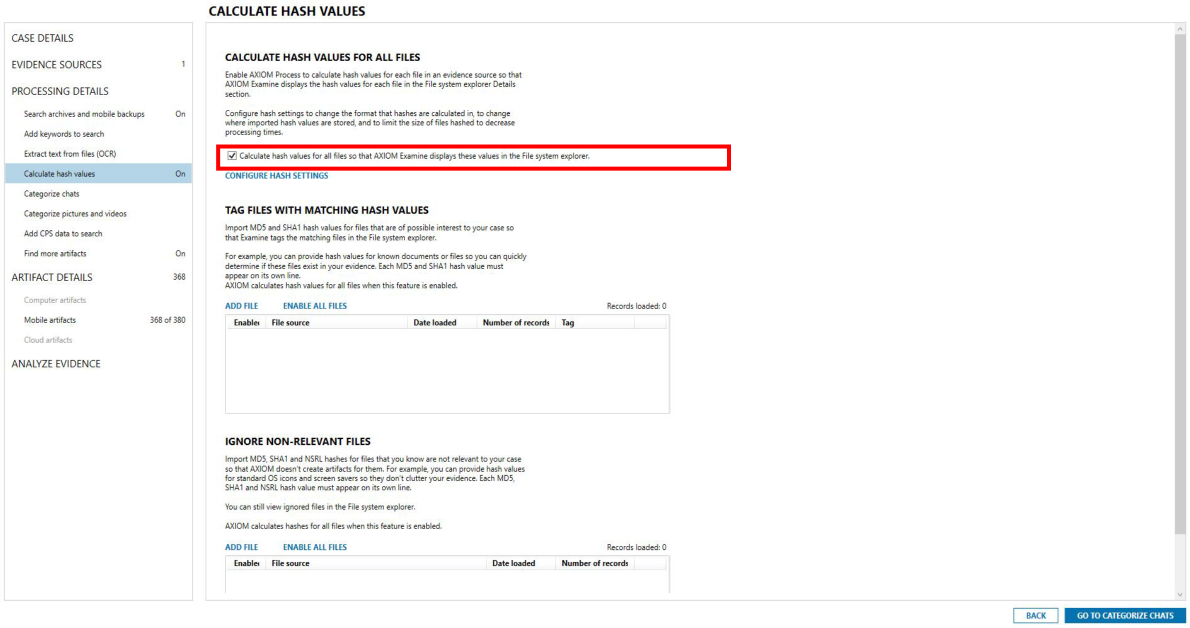
ADD CPS DATA TO SEARCH

If you export data from the Child Protection System (CPS) website to a .csv file, and then import the .csv file into Magnet AXIOM Process, Magnet AXIOM automatically searches the data from the CPS file you exported (such as IP addresses, user names, and more) to find any matches to your case. After processing is complete, Magnet AXIOM Examine tags the matching data in the Artifacts and File system explorers.

ADD CPS DATA TO SEARCH

BACK GO TO ARTIFACT DETAILS

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



CALCULATE HASH VALUES

CASE DETAILS
EVIDENCE SOURCES 1
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values On
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts On
ARTIFACT DETAILS 368
Computer artifacts
Mobile artifacts 368 of 380
Cloud artifacts
ANALYZE EVIDENCE

CALCULATE HASH VALUES FOR ALL FILES

Enable AXIOM Process to calculate hash values for each file in an evidence source so that AXIOM Examine displays the hash values for each file in the File system explorer Details section.

Configure hash settings to change the format that hashes are calculated in, to change where imported hash values are stored, and to limit the size of files hashed to decrease processing times.

☑ Calculate hash values for all files so that AXIOM Examine displays these values in the File system explorer.

CONFIGURE HASH SETTINGS

TAG FILES WITH MATCHING HASH VALUES

Import MD5 and SHA1 hash values for files that are of possible interest to your case so that Examine tags the matching files in the File system explorer.

For example, you can provide hash values for known documents or files so you can quickly determine if these files exist in your evidence. Each MD5 and SHA1 hash value must appear on its own line.
AXIOM calculates hash values for all files when this feature is enabled.

ADD FILE ENABLE ALL FILES Records loaded: 0

Enablec	File source	Date loaded	Number of records	Tag

IGNORE NON-RELEVANT FILES

Import MD5, SHA1 and NSRL hashes for files that you know are not relevant to your case so that AXIOM doesn't create artifacts for them. For example, you can provide hash values for standard OS icons and screen savers so they don't clutter your evidence. Each MD5, SHA1 and NSRL hash value must appear on its own line.

You can still view ignored files in the File system explorer.

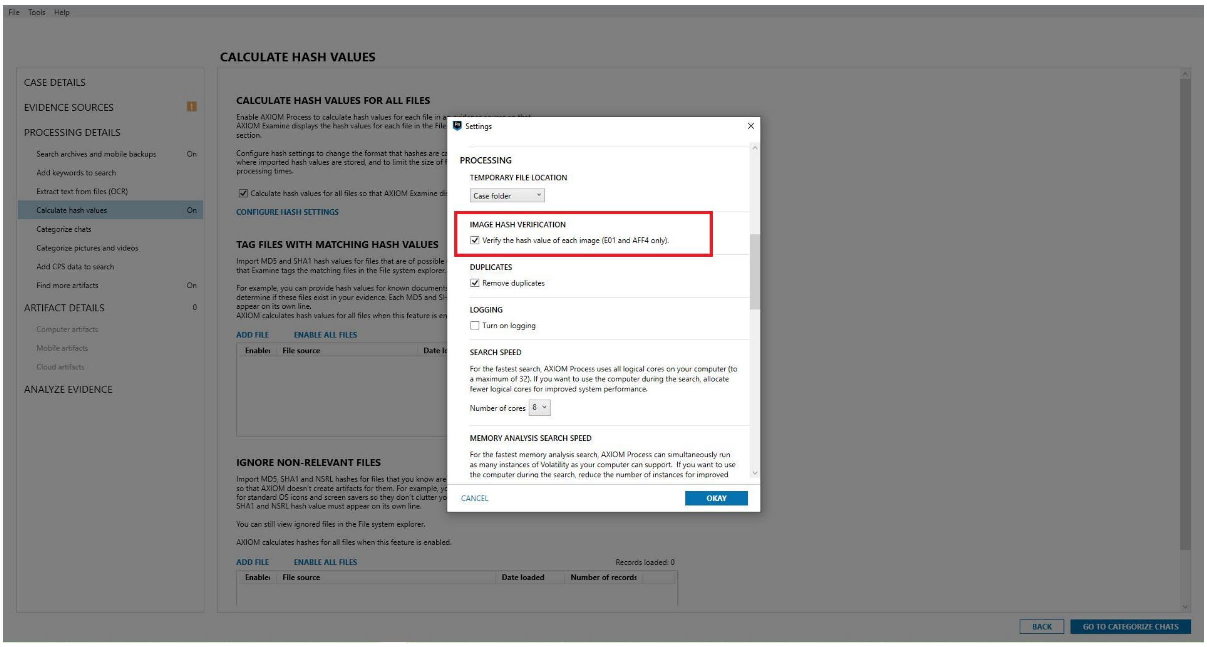
AXIOM calculates hashes for all files when this feature is enabled.

ADD FILE ENABLE ALL FILES Records loaded: 0

Enablec	File source	Date loaded	Number of records

BACK GO TO CATEGORIZE CHATS

18. 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 VERIFCATION**” (*Gives image file a verification hash*)



Settings

PROCESSING

TEMPORARY FILE LOCATION

Case folder

IMAGE HASH VERIFICATION

☑ Verify the hash value of each image (E01 and AFF4 only).

DUPLICATES

☑ Remove duplicates

LOGGING

□ Turn on logging

SEARCH SPEED

For the fastest search, AXIOM Process uses all logical cores on your computer (to a maximum of 32). If you want to use the computer during the search, allocate fewer logical cores for improved system performance.

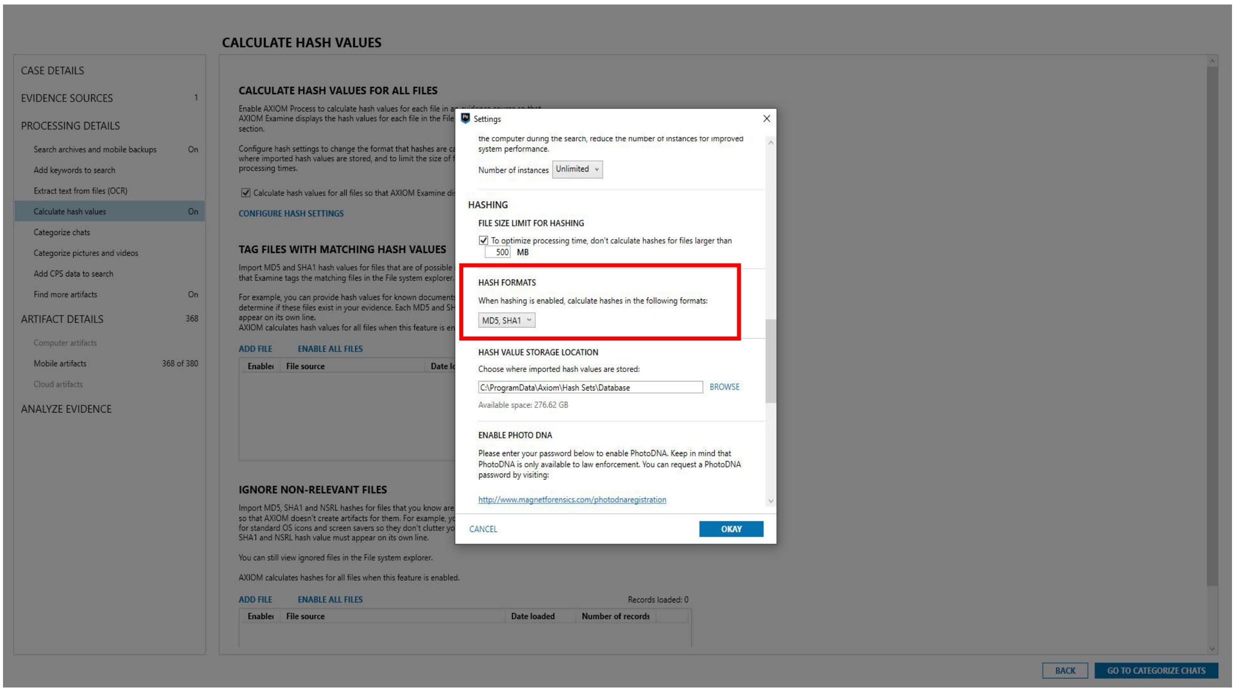
Number of cores 8

MEMORY ANALYSIS SEARCH SPEED

For the fastest memory analysis search, AXIOM Process can simultaneously run as many instances of Volatility as your computer can support. If you want to use the computer during the search, reduce the number of instances for improved

CANCEL OKAY

19. Continue from earlier, scroll down further the window settings to “**HASHING**” and change the Hashing Format to “**MD5, SHA1**” (*Gives you a MD5 Hash value and SHA1 Hash Value*) and then click on “**Okay**”



Settings

the computer during the search, reduce the number of instances for improved system performance.

Number of instances Unlimited

HASHING

FILE SIZE LIMIT FOR HASHING

☑ To optimize processing time, don't calculate hashes for files larger than 500 MB

HASH FORMATS

When hashing is enabled, calculate hashes in the following formats:

MD5, SHA1

HASH VALUE STORAGE LOCATION

Choose where imported hash values are stored:

C:\ProgramData\Axiom\Hash Sets\Database BROWSE

Available space: 276.62 GB

ENABLE PHOTO DNA

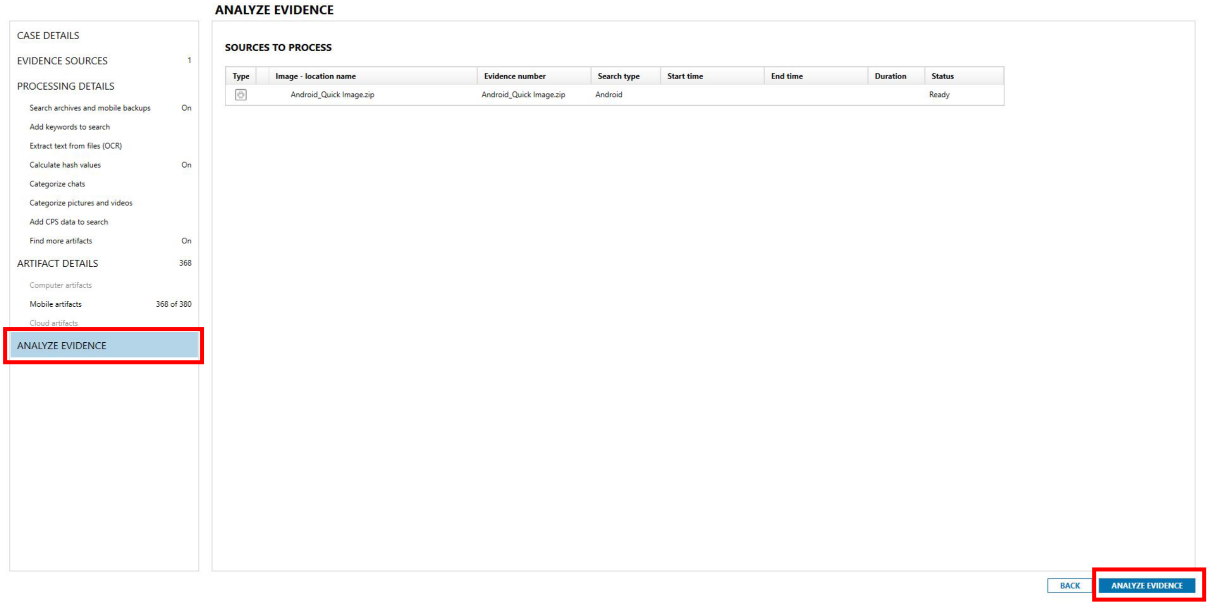
Please enter your password below to enable PhotoDNA. Keep in mind that PhotoDNA is only available to law enforcement. You can request a PhotoDNA password by visiting:

http://www.magnetforensics.com/photodnaregistration

CANCEL OKAY

20. After all the configurations were selected you may skip all the other configurations and move on to "**ANALYZE EVIDENCE**" on the left column of the interface. (*This section displays the source evidence image that you wish to process. In our case is the image file "JustineBeaufort.E01" which we had selected for it earlier*)

21. Click on "**Analyze Evidence**" on the bottom right of the AXIOM Process interface to process the evidence.

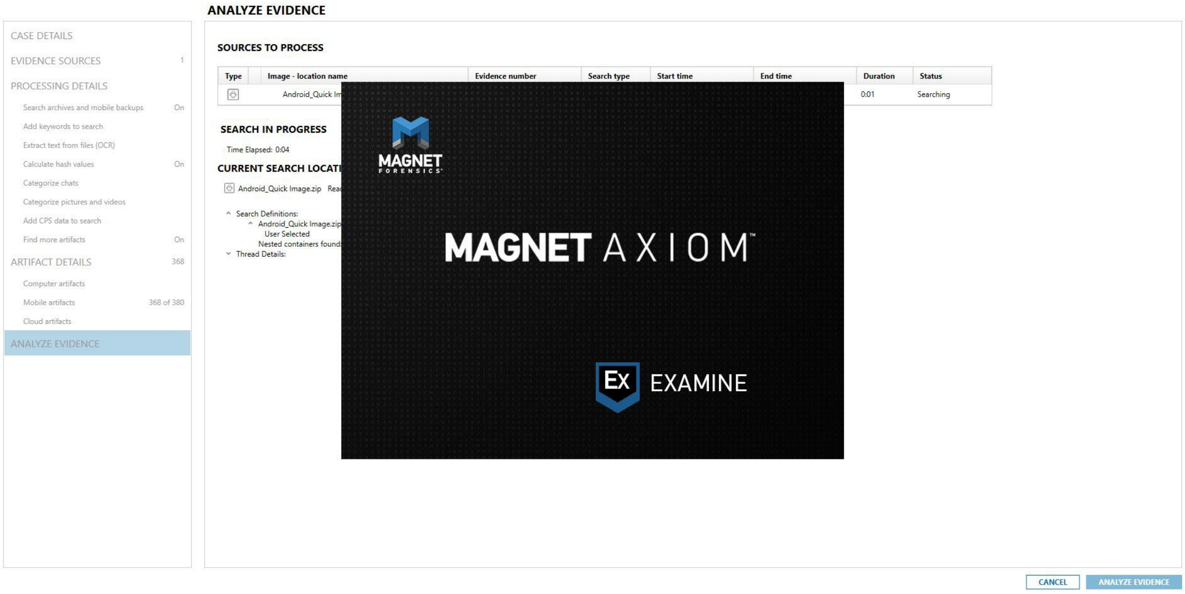


ANALYZE EVIDENCE

SOURCES TO PROCESS

Type	Image - location name	Evidence number	Search type	Start time	End time	Duration	Status
	Android_Quick Image.zip	Android_Quick Image.zip	Android				Ready

22. Another window "**AXIOM Examine**" will pop up. This shows that you have successfully started the processing for the evidence image file (.E01).



ANALYZE EVIDENCE

SOURCES TO PROCESS

Type	Image - location name	Evidence number	Search type	Start time	End time	Duration	Status
	Android_Quick Im					0:01	Searching

SEARCH IN PROGRESS

Time Elapsed: 0:04

CURRENT SEARCH LOCATI

Android_Quick Image.zip Rea

Search Definitions:
Android_Quick Image.zip
User Selected
Nested containers found
Thread Details:

23. The processing of analyzing and processing the evidence would take up to 30 mins or so to complete due the image file size is relatively small.
24. You can close the **AXIOM Process** Window once processing is done. Proceed to practical 2 of the mobile forensics.

-- End --