OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Michael Hegarty

Forensics

Introduction to Forensics Analysis using FTK

In the previous lab, we worked with FTK **Imager** tool to create a forensic duplicate, and now we are moving on to the analysis phase of an investigation. In this lab, we will explore Access-Data FTK (Forensic Toolkit) to analyse the forensic image/duplicate of a Memory Stick bit-stream file.

Case Overview:

Steve Billings, the manager of a family run business, has raised concerns regarding two of his employees, Martha Heiser and George Montgomery. The circumstances surrounding both employees have raised suspicions, prompting the need for a forensic examination of digital evidence.

Martha Heiser:

Two weeks ago, Martha Heiser, who serves as the distribution official, abruptly initiated a one-week "urgent situation" leave from the company (*She is entitled to do this under her employment contract*). Her actions were unusual as she did not provide any information about her whereabouts or contact details.

Remarkably, Martha has not returned from her leave, and there is no communication from her and cannot be contacted through the usual channels.

George Montgomery:

George Montgomery, a supervisor in the Accounts Payable Department, has been absent from work for the past week, and the reasons for his absence are unknown.

Discovery of Evidence:

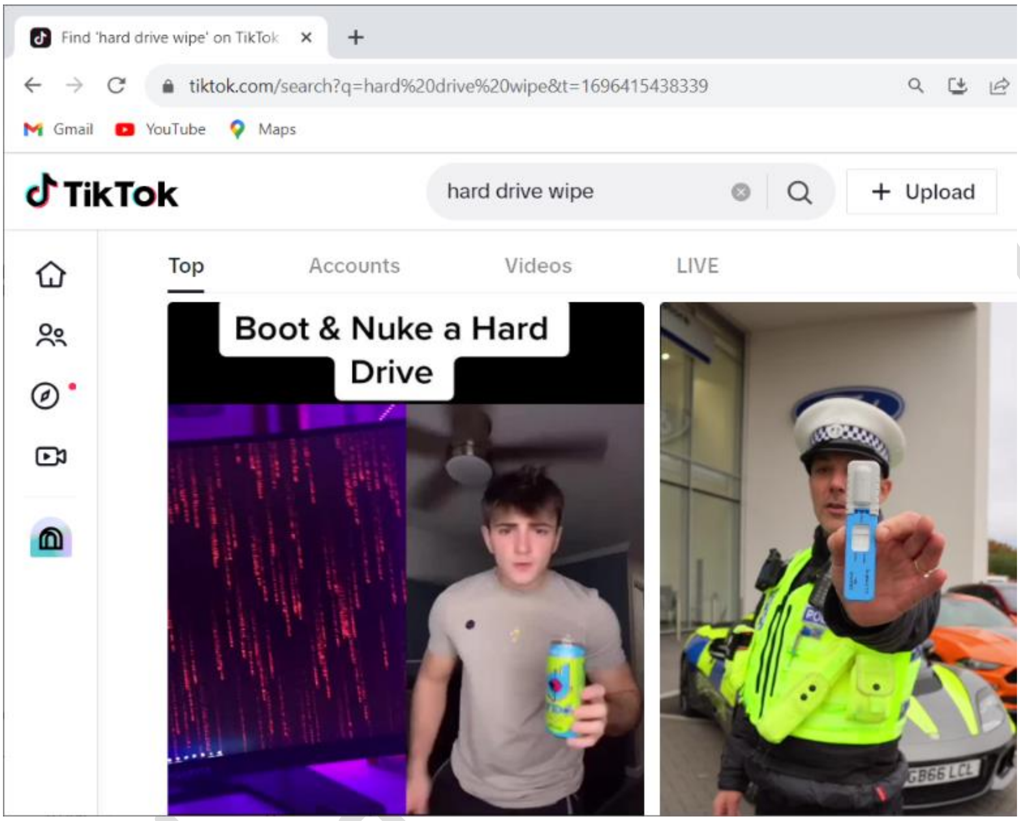
Steve Billings, concerned about the unexplained absences of both employees, initiated investigations within the workplace. During these investigations the following was found:

In the case of George Montgomery, Steve found,

- Three unused vape devices.
- Links to online gaming websites.
- Tik-Tok search for "hard drive wipe" (see below).
- Google Search for "Cat Adoption Dublin" (see below).
- Microsoft Bing Search "florist in Blanchardstown" (see below).
- Google Translate with text translated from French (see below).
- Access to a website regarding Geneva (see below).
- Handwritten documents (one displayed below) relating to a supplier based in Switzerland with whom Steve himself had previous dealings.

Steve had his IT person access the PC used by George and they discovered all data on the C/Drive and Cloud had been deleted by George. Additionally, a Memory Stick labelled with the former supplier's name and a 4-digit code (2398) was discovered taped under the desk used by George.

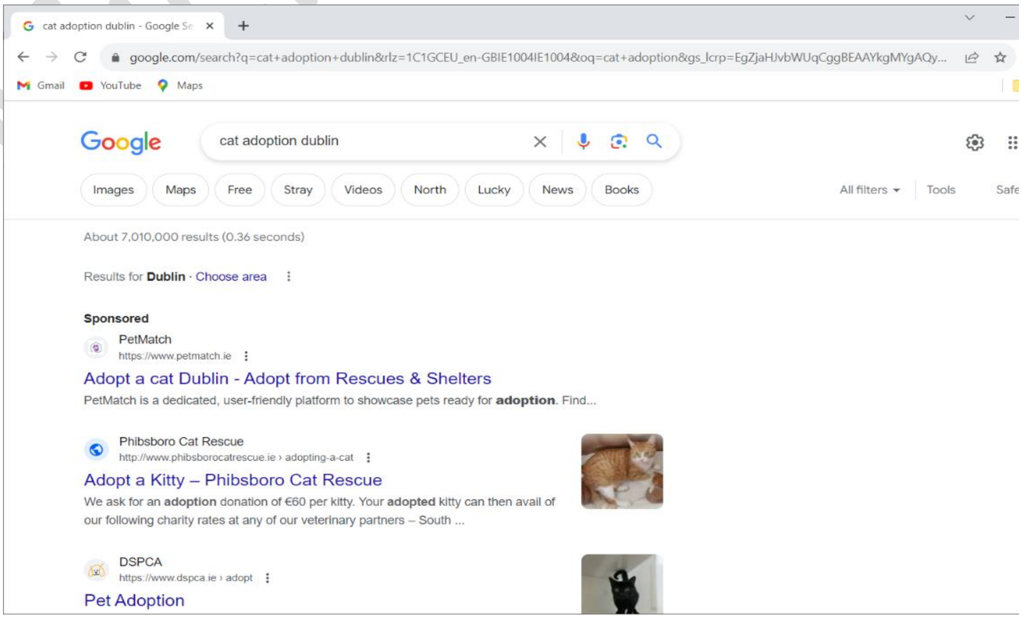
TikTok Search



Find 'hard drive wipe' on TikTok

tiktok.com/search?q=hard%20drive%20wipe&t=1696415438339

Cat Adoption Dublin



cat adoption dublin - Google Se

google.com/search?q=cat+adoption+dublin&rlz=1C1GCEU_en-GBIE1004IE1004&oq=cat+adoption&gs_lcrp=EgZjaHJvbWUqCggBEAAYkgMYgAQy...

About 7,010,000 results (0.36 seconds)

Results for **Dublin** · Choose area

Sponsored

PetMatch
https://www.petmatch.ie

Adopt a cat Dublin - Adopt from Rescues & Shelters

PetMatch is a dedicated, user-friendly platform to showcase pets ready for **adoption**. Find...

Phibsboro Cat Rescue
http://www.phibsborocatrescue.ie › adopting-a-cat

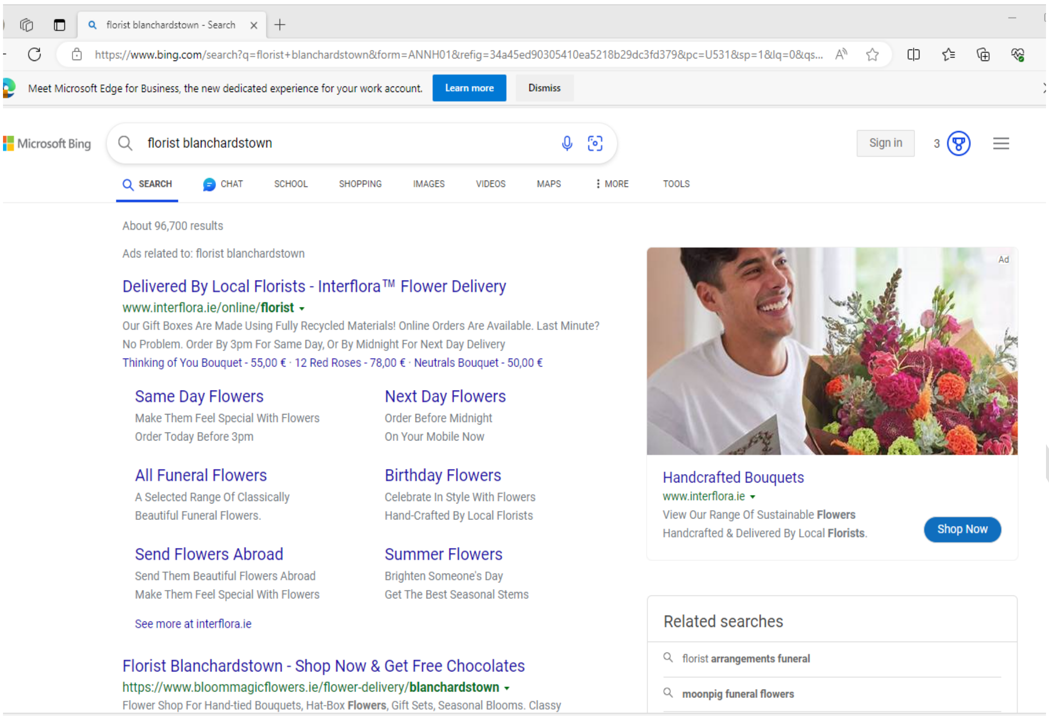
Adopt a Kitty – Phibsboro Cat Rescue

We ask for an **adoption** donation of €60 per kitty. Your **adopted** kitty can then avail of our following charity rates at any of our veterinary partners – South ...

DSPCA
https://www.dspca.ie › adopt

Pet Adoption

Microsoft Bing Search “florist Blanchardstown”



https://www.bing.com/search?q=florist+blanchardstown&form=ANNH01&refig=34a45ed90305410ea5218b29dc3fd379&pc=U531&sp=1&lq=0&qs...

Meet Microsoft Edge for Business, the new dedicated experience for your work account.

florist blanchardstown

About 96,700 results

Ads related to: florist blanchardstown

Delivered By Local Florists - Interflora™ Flower Delivery
www.interflora.ie/online/**florist**
Our Gift Boxes Are Made Using Fully Recycled Materials! Online Orders Are Available. Last Minute? No Problem. Order By 3pm For Same Day, Or By Midnight For Next Day Delivery
Thinking of You Bouquet - 55,00 € · 12 Red Roses - 78,00 € · Neutrals Bouquet - 50,00 €

Same Day Flowers
Make Them Feel Special With Flowers
Order Today Before 3pm

Next Day Flowers
Order Before Midnight
On Your Mobile Now

All Funeral Flowers
A Selected Range Of Classically
Beautiful Funeral Flowers.

Birthday Flowers
Celebrate In Style With Flowers
Hand-Crafted By Local Florists

Send Flowers Abroad
Send Them Beautiful Flowers Abroad
Make Them Feel Special With Flowers

Summer Flowers
Brighten Someone's Day
Get The Best Seasonal Stems

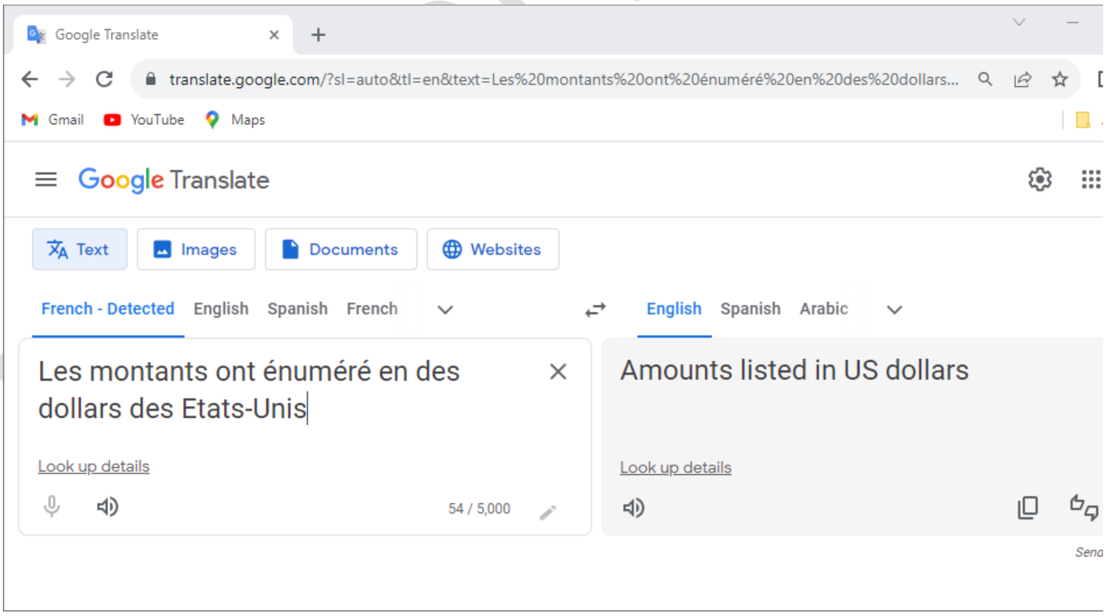
See more at interflora.ie

Florist Blanchardstown - Shop Now & Get Free Chocolates
https://www.bloommagicflowers.ie/flower-delivery/**blanchardstown**
Flower Shop For Hand-tied Bouquets, Hat-Box **Flowers**, Gift Sets, Seasonal Blooms. Classy

Handcrafted Bouquets
www.interflora.ie
View Our Range Of Sustainable **Flowers**
Handcrafted & Delivered By Local **Florists**.

Related searches
florist **arrangements funeral**
moonpig funeral flowers

Google Translate



translate.google.com/?sl=auto&tl=en&text=Les%20montants%20ont%20énuméré%20en%20des%20dollars...

Les montants ont énuméré en des dollars des Etats-Unis

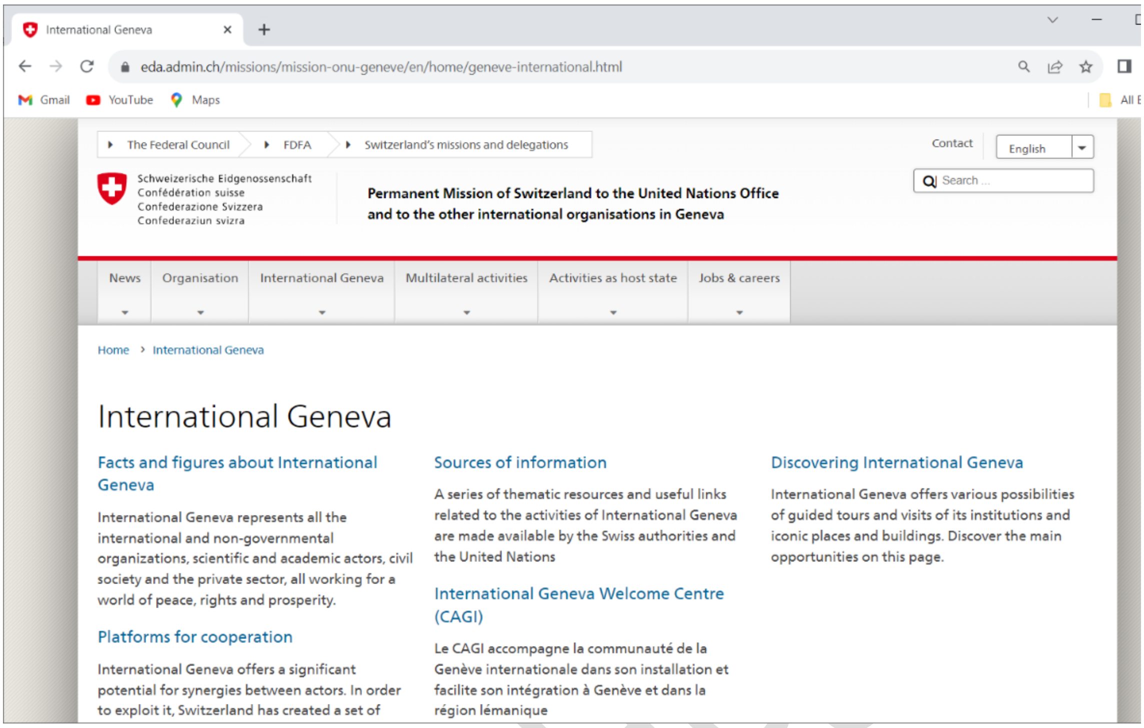
Look up details

54 / 5,000

Amounts listed in US dollars

Look up details

Website regarding Geneva



Permanent Mission of Switzerland to the United Nations Office and to the other international organisations in Geneva

International Geneva

Facts and figures about International Geneva

International Geneva represents all the international and non-governmental organizations, scientific and academic actors, civil society and the private sector, all working for a world of peace, rights and prosperity.

Platforms for cooperation

International Geneva offers a significant potential for synergies between actors. In order to exploit it, Switzerland has created a set of

Sources of information

A series of thematic resources and useful links related to the activities of International Geneva are made available by the Swiss authorities and the United Nations

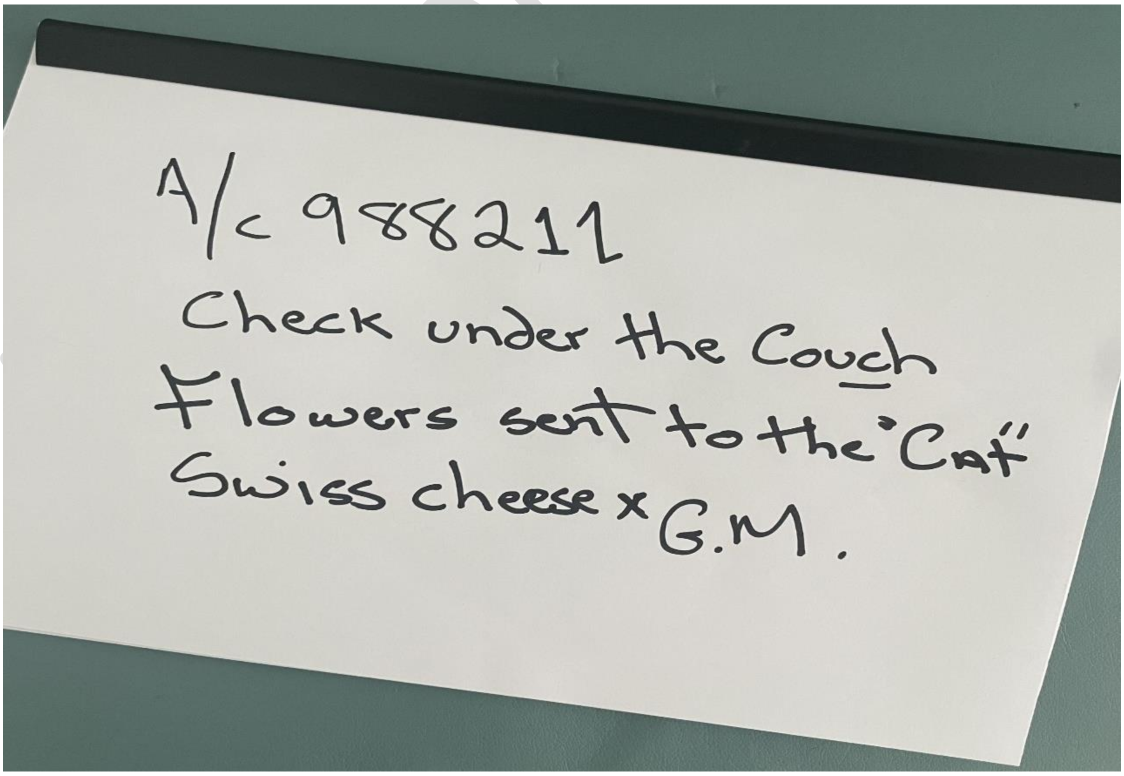
International Geneva Welcome Centre (CAGI)

Le CAGI accompagne la communauté de la Genève internationale dans son installation et facilite son intégration à Genève et dans la région lémanique

Discovering International Geneva

International Geneva offers various possibilities of guided tours and visits of its institutions and iconic places and buildings. Discover the main opportunities on this page.

Handwritten note



A/c 988211
Check under the Couch
Flowers sent to the "Cat"
Swiss cheese x G.M.

While inspecting Martha Heiser's desk, Steve discovered, a handbag containing personal items including a small bag of white powder, a penknife and travel details related to foreign tours. This discovery suggests that Martha may have been planning a trip, which could provide insights into her disappearance. Martha has a company provided mobile phone that is also missing and seems to be powered off.

Your Role:

Steve Billings has engaged you to conduct a forensic examination of the Memory Stick found on George Montgomery's desk. Your primary objective is to determine if the Memory Stick contains any information that might shed light on the reasons behind Martha Heiser and George Montgomery's sudden and unexplained absences from work. This analysis may uncover critical clues, communications, or documents that could provide insight into their whereabouts and intentions.

As you start on this forensic investigation, remember to meticulously document your actions, findings, and any potential evidence discovered on the Memory Stick. Screenshots and detailed records are essential to creating a comprehensive forensic report that will assist in understanding the circumstances surrounding these two missing employees and their possible connection to the information found on the Memory Stick or other details provided by Steve.

Before proceeding, it is essential to thoroughly read through the entire lab instructions and then execute each step precisely. The guidance for this lab is provided by Michael Hegarty.

Here are some essential recommendations to follow as you start a forensic investigation:

1. Methodical Approach: Begin your investigation with a systematic and methodical approach. Carefully consider the objectives of your analysis and the questions you seek to answer.
   Remembering 5W-H from lecture-1

2. Document Everything: Maintain detailed records of each step you take during the investigation. Record the tools and software used, the files examined, and the actions performed. Be sure to timestamp your activities to establish a timeline of your investigation.

3. Screenshots: Screenshots are invaluable for documenting your actions and the state of the evidence at various points in the investigation. Capture screenshots to illustrate significant findings, folder structures, and any anomalies you encounter. These visual aids enhance the comprehensibility of your report.

4. File and Folder Organization: Keep your files and folders organized. Create a structured directory where you can store your documentation, screenshots, and any reports you generate during the investigation. This ensures that your findings are easily accessible and well-organized.

5. Analysis and Findings: As you examine files and uncover evidence, document your findings thoroughly. Include relevant information such as file names, timestamps, and any text or data extracted from the evidence. If you encounter any suspicious or noteworthy items, make a note of them.

6. Maintain Chain of Custody: If applicable, ensure the chain of custody for the digital evidence is preserved. Document who had access to the evidence and when, as well as any actions taken by individuals involved in the investigation.

7. Report Compilation: After completing your analysis, compile a forensic report that encapsulates your investigation process, findings, and conclusions. The report should be clear, concise, and organized. Include relevant screenshots and references to evidence.

8. Review and Validation: Review your report for accuracy and completeness. Ensure that your findings are supported by the evidence and that your report adheres to forensic best practices. Remembering in digital forensics all findings must be repeatable by you or another professional.

9. Legal/Ethical Considerations: Throughout your investigation, maintain the highest ethical standards. Respect the privacy and legal considerations associated with the evidence you are handling.

By following these guidelines and documenting your forensic analysis thoroughly, you will be well-prepared to create a credible and informative forensic report. This report will not only serve as a record of your investigation but also as a valuable resource for presenting your findings and insights to others involved in the case.

Please follow the steps below to acquire the image file and commence a documented investigation of its contents.

Retrieve Necessary Files: All the required files for this lab are conveniently located within the folder you downloaded from Moodle/Brightspace.

Copy to Local Storage: Copy both the file and folder structure to either your pen drive or your laptop. This ensures that you have a local copy of the data to work with.

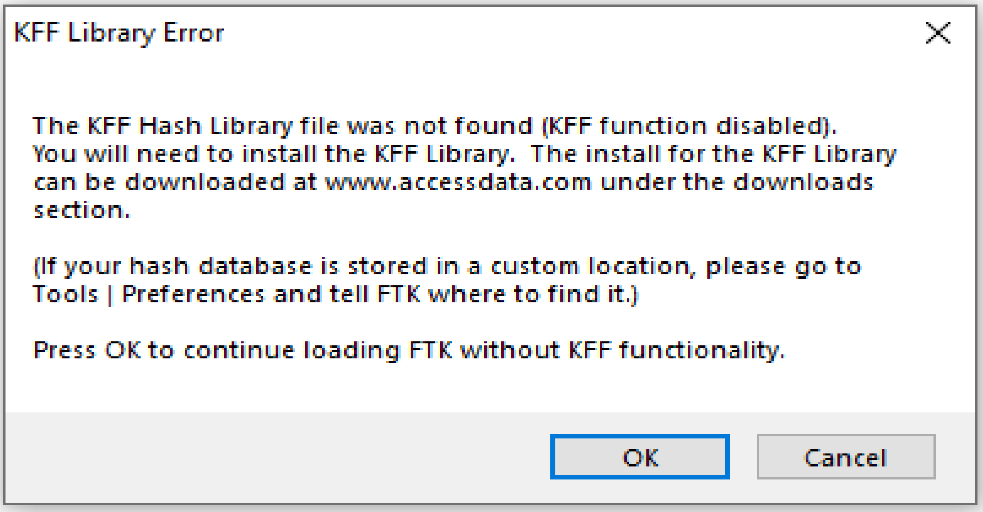
Verify Data Integrity: Verify the integrity of your copy by cross-referencing it with the checksum verification value provided in the accompanying text file. This step confirms that your copied data matches the original source accurately.

Launch FTK: Start the FTK application by running the executable found within the folder. FTK is the tool we'll be using for the analysis, and it should be ready to use upon launch.

Acknowledging Evaluation Version Messages: If you are using the evaluation version of FTK, you'll likely encounter several warning messages.

Simply click the 'OK' button for each message to proceed with your analysis.

These instructions maintain clarity and step-by-step guidance to ensure a smooth and organized start to the investigation using Access-Data FTK.

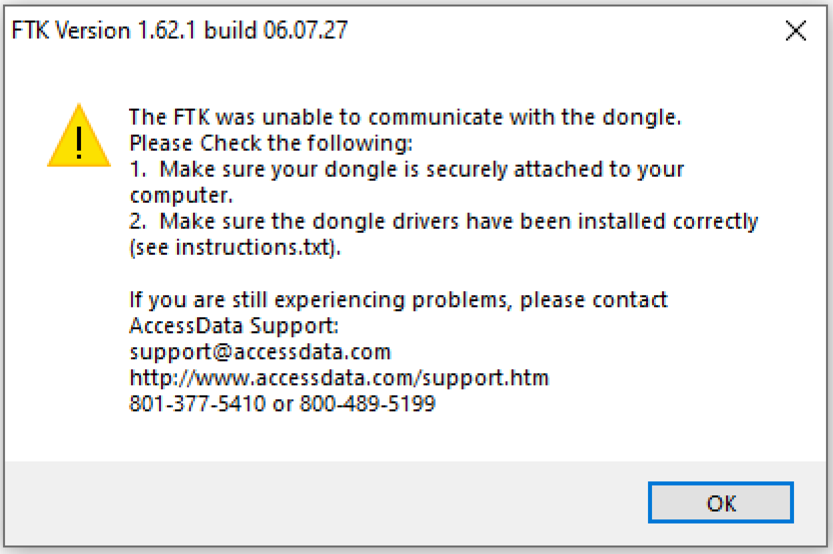


KFF Library Error

The KFF Hash Library file was not found (KFF function disabled). You will need to install the KFF Library. The install for the KFF Library can be downloaded at www.accessdata.com under the downloads section.

(If your hash database is stored in a custom location, please go to Tools | Preferences and tell FTK where to find it.)

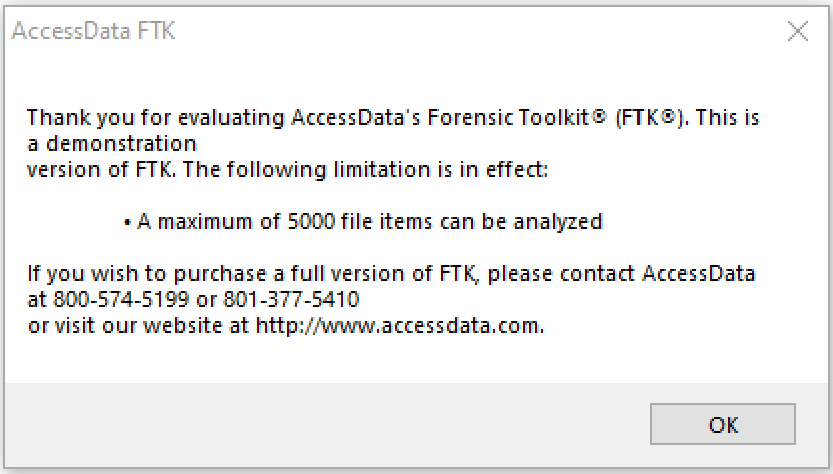
Press OK to continue loading FTK without KFF functionality.



FTK Version 1.62.1 build 06.07.27

The FTK was unable to communicate with the dongle.
Please Check the following:
1. Make sure your dongle is securely attached to your computer.
2. Make sure the dongle drivers have been installed correctly (see instructions.txt).

If you are still experiencing problems, please contact
AccessData Support:
support@accessdata.com
http://www.accessdata.com/support.htm
801-377-5410 or 800-489-5199

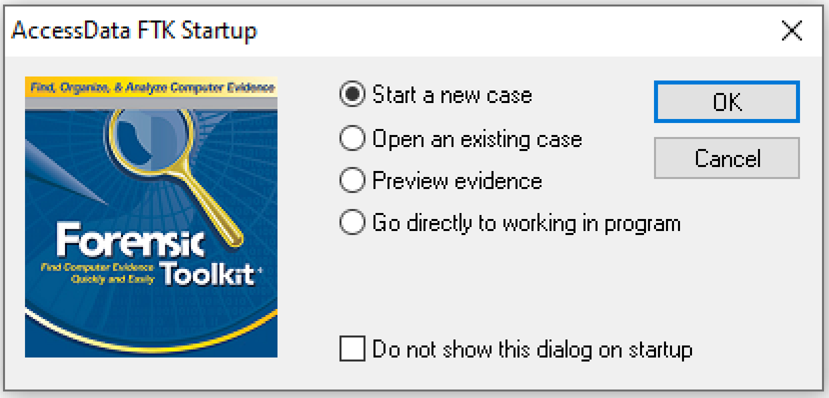

AccessData FTK

Thank you for evaluating AccessData's Forensic Toolkit® (FTK®). This is a demonstration
version of FTK. The following limitation is in effect:

- A maximum of 5000 file items can be analyzed

If you wish to purchase a full version of FTK, please contact AccessData at 800-574-5199 or 801-377-5410
or visit our website at http://www.accessdata.com.

Choose “Start a new a case”.

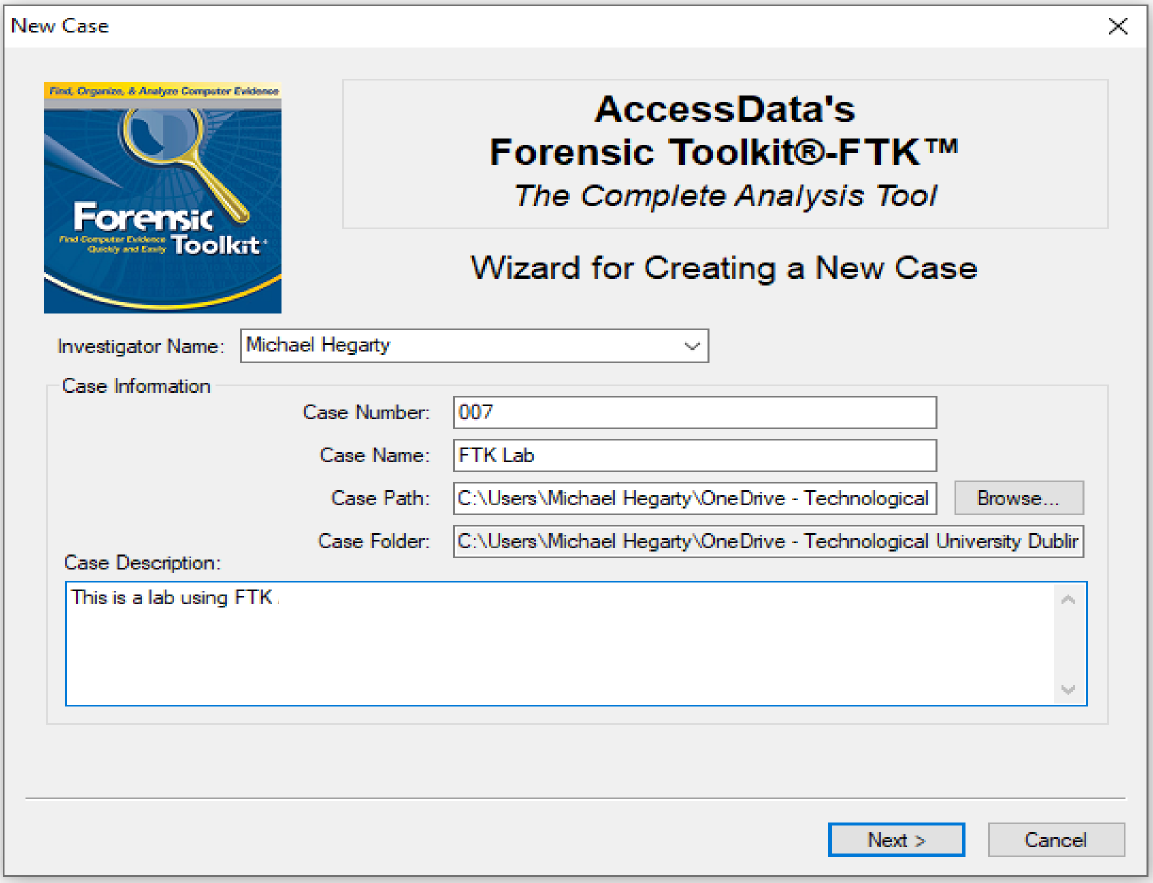

AccessData FTK Startup

● Start a new case
○ Open an existing case
○ Preview evidence
○ Go directly to working in program

□ Do not show this dialog on startup

Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily
OK
Cancel

Enter details for the following, Case Path is where info regarding the case will be saved on your machine.



New Case
Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily
AccessData's
Forensic Toolkit®-FTK™
The Complete Analysis Tool
Wizard for Creating a New Case
Browse...
Next >
Cancel

Investigator Name: Michael Hegarty

Case Information

Case Number: 007

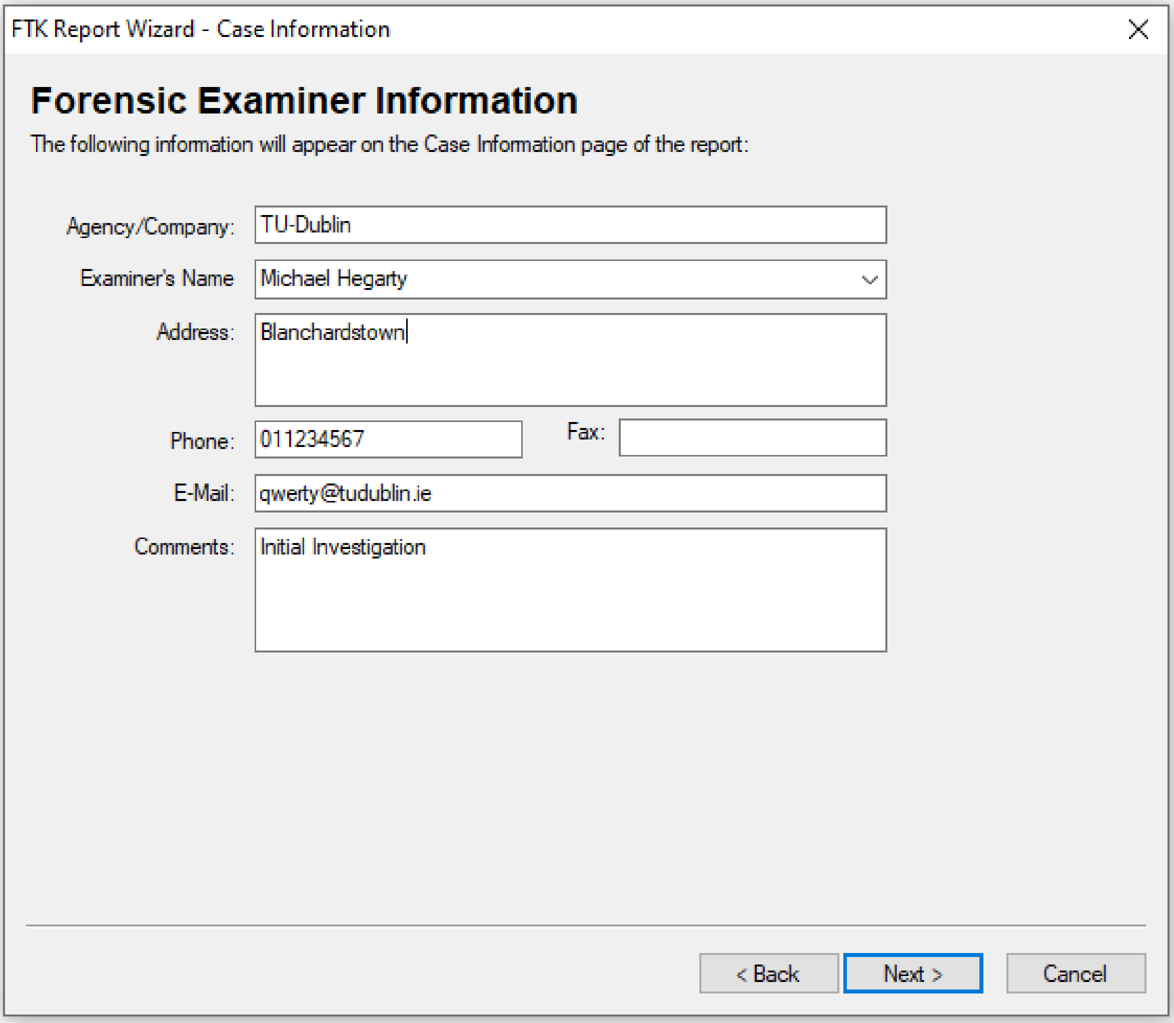
Case Name: FTK Lab

Case Path: C:\Users\Michael Hegarty\OneDrive - Technological

Case Folder: C:\Users\Michael Hegarty\OneDrive - Technological University Dublir

Case Description:

This is a lab using FTK.



FTK Report Wizard - Case Information

Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company: TU-Dublin

Examiner's Name: Michael Hegarty

Address: Blanchardstown

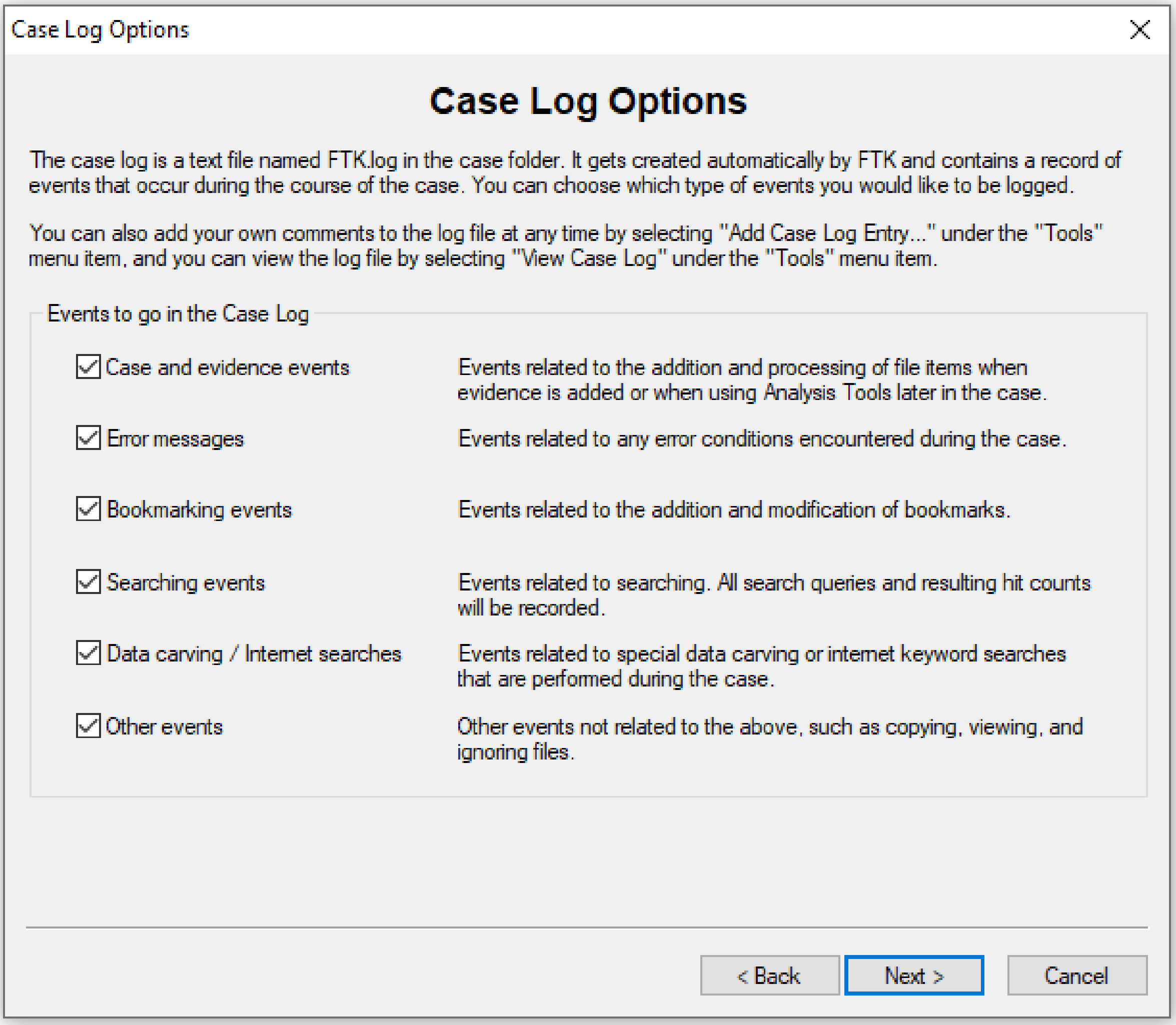
Phone: 011234567

Fax:

E-Mail: qwerty@tudublin.ie

Comments: Initial Investigation

In the following series of steps, you will encounter several informative windows. It is important to carefully read the information presented in each window without making any alterations to the options. To assist you, screen captures of each window have been provided for your convenience. This approach ensures that you have a clear understanding of the process before advancing to the next step, promoting a smooth and informed progression through the software interface.



Case Log Options

Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

☑ Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
☑ Error messages	Events related to any error conditions encountered during the case.
☑ Bookmarking events	Events related to the addition and modification of bookmarks.
☑ Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
☑ Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
☑ Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

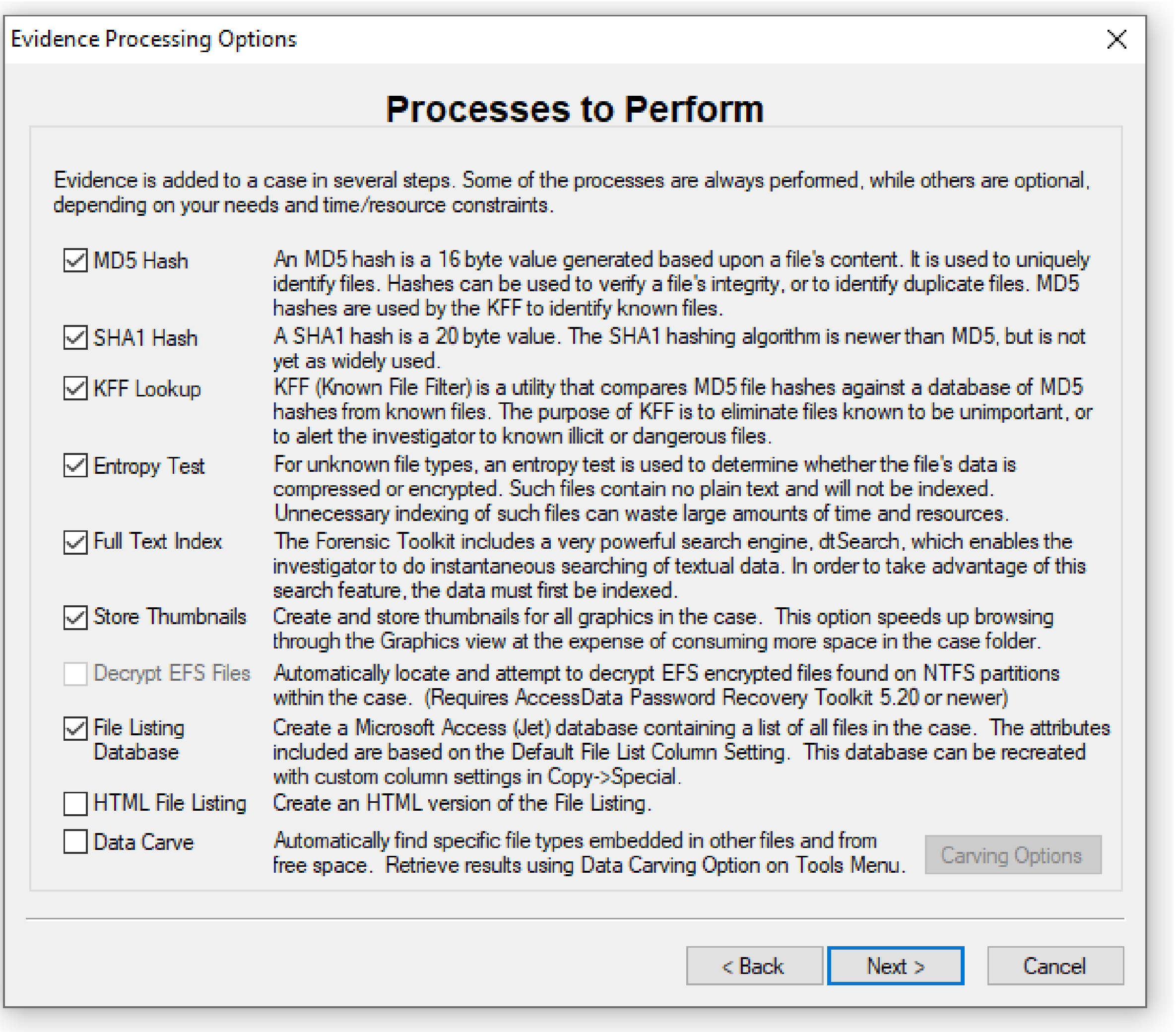
What is the format of the FTK.log file?

What is a log file used for?

What kind of events can be recorded in a log file?

How can you add comments to a log file?

List 3 events that can go in a Case Log.



Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

☑ MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
☑ SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
☑ KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
☑ Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
☑ Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
☑ Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
□ Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
☑ File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Default File List Column Setting. This database can be recreated with custom column settings in Copy->Special.
□ HTML File Listing	Create an HTML version of the File Listing.
□ Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.

How many bits in a MD5 and SHA1 key? List 3 other Hash Algorithms

What is the function of the KFF utility?

What is an Entropy Test?

How can we check if a file is compressed?

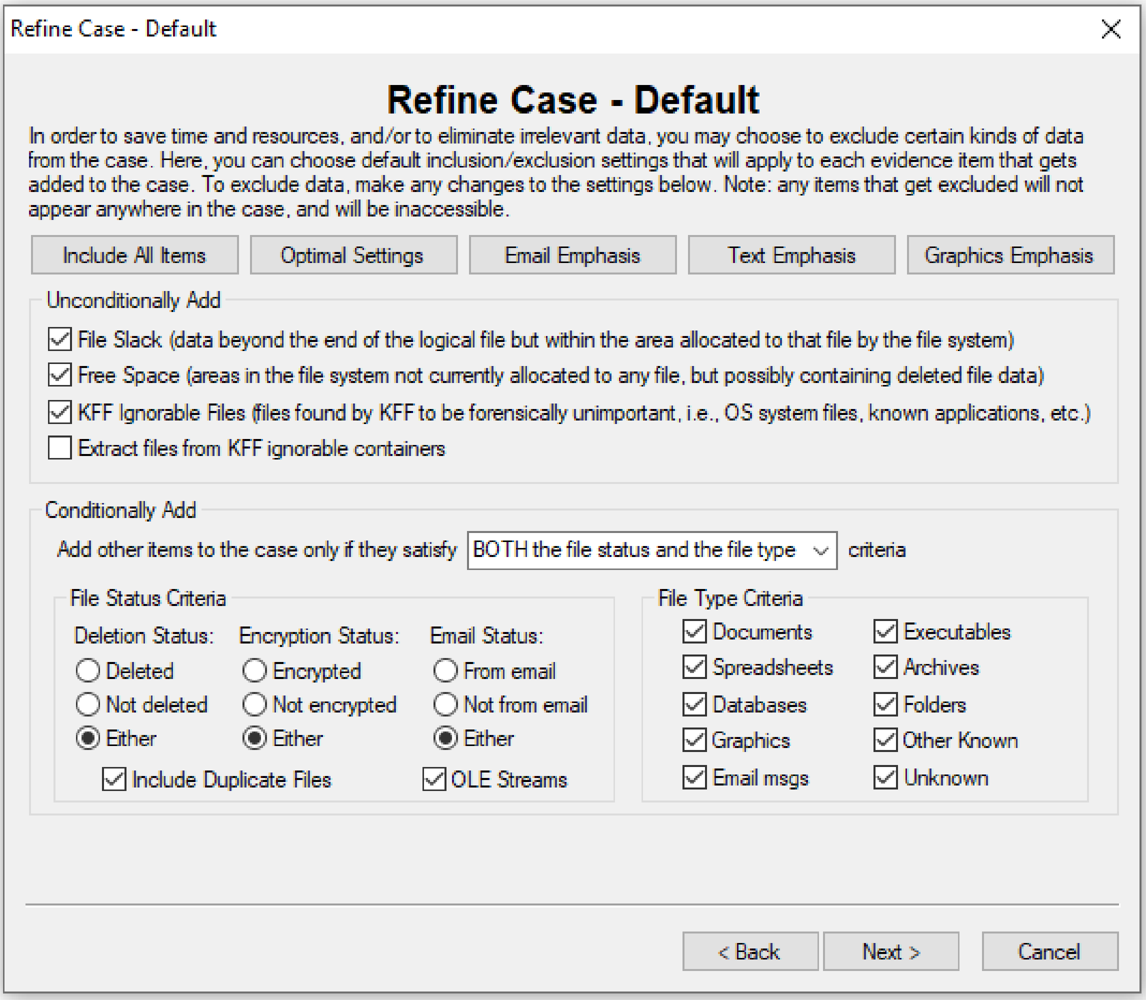
Why does data need to be indexed?

What does HTML File Listing function do?

What is a thumbnail?

What other types of databases can be used to store lists of files?

What is data carving? “Research further”



Refine Case - Default

Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add

- ☑ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- ☑ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- ☑ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- □ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	○ From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	● Either

☑ Include Duplicate Files ☑ OLE Streams

File Type Criteria

- ☑ Documents
- ☑ Spreadsheets
- ☑ Databases
- ☑ Graphics
- ☑ Email msgs
- ☑ Executables
- ☑ Archives
- ☑ Folders
- ☑ Other Known
- ☑ Unknown

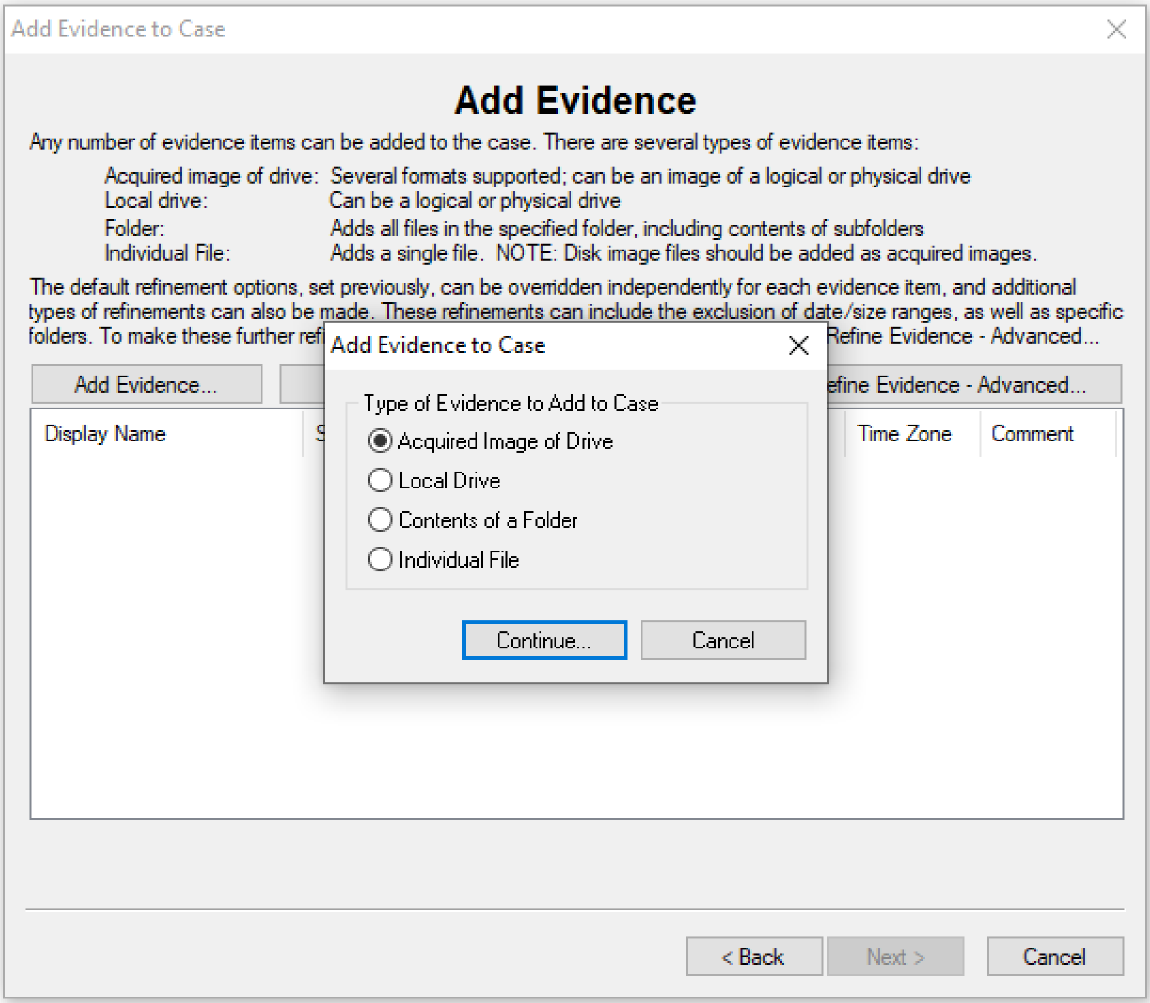
What are the options for excluding certain kinds of data?

What is the difference Slack Space and Free Space? Expand your answer with additional research.

What utility compares file hashes against a reference database to eliminate known files?

What is difference between File Status and File Type?

We will now import the image file contents by selecting the Add Evidence button and selecting Acquire Image Drive option in dialog box.


Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further ref[...] Refine Evidence - Advanced...

Add Evidence to Case

Type of Evidence to Add to Case

● Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
○ Individual File

Begin by selecting the image file necessary for our analysis. You can access this file by navigating to the folder you previously downloaded from Moodle. In this folder, you will find the 'ftk-demo1-**image.1**' file, which is the image file we'll be using for our investigation. It's worth noting that the folder also contains a text file that provides the correct MD5 checksum value for verification purposes.

Now, take a moment to ensure the ***integrity*** of the image file. We will do this by comparing the MD5 checksum of the image file with the MD5 checksum generated from your copied file. This verification step is critical for confirming that the image file has been copied accurately and is unchanged from its original state. Any discrepancies between the MD5 checksums could indicate potential data corruption or tampering.

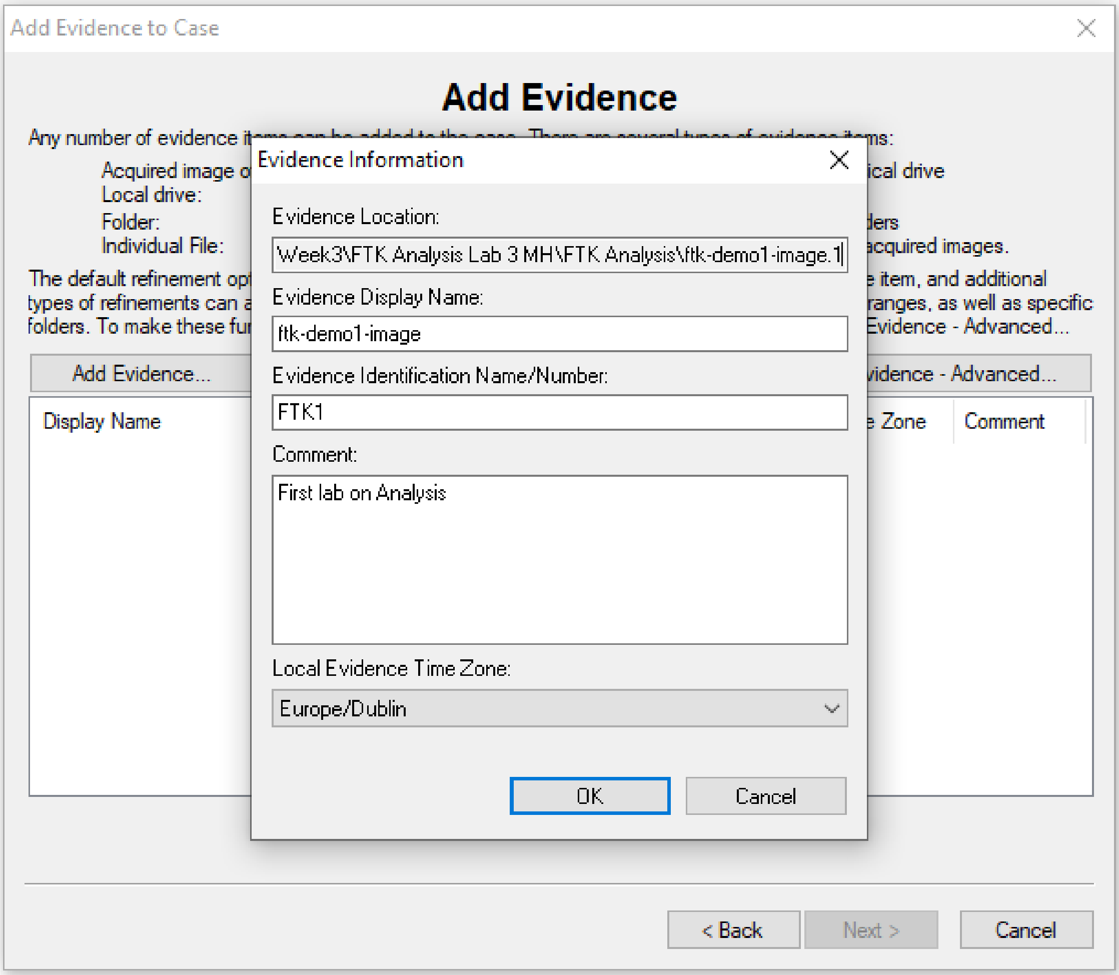
To perform this verification: (There are many online tools available for this)

Calculate the MD5 checksum of the 'ftk-demo1-**image.1'** file you've just selected.

Compare this calculated MD5 checksum with the MD5 checksum value provided in the accompanying text file. If they match, it confirms the file's integrity, and you can proceed confidently with your analysis (A mismatch between Upper and Lower case is ok.)

This MD5 checksum comparison is a fundamental step in forensic analysis to ensure that the digital evidence remains pristine and unaltered, guaranteeing the reliability and integrity of the data under investigation."

Screenshot your results!



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image o... ...ical drive
Local drive:
Folder: ...ders
Individual File: ...acquired images.

The default refinement opt... ...e item, and additional types of refinements can a... ...ranges, as well as specific folders. To make these fu... Evidence - Advanced...

Evidence Information

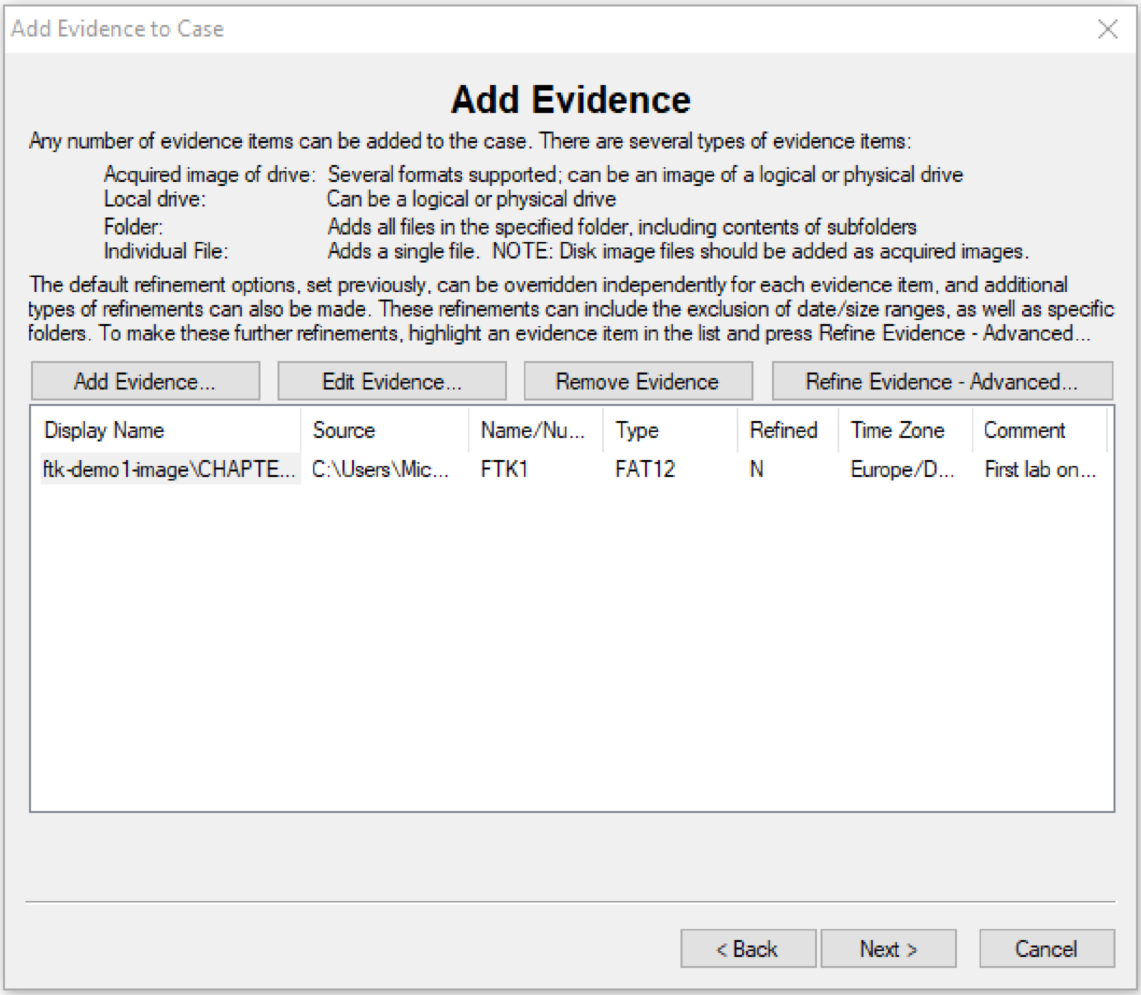
Evidence Location:
Week3\FTK Analysis Lab 3 MH\FTK Analysis\ftk-demo1-image.1

Evidence Display Name:
ftk-demo1-image

Evidence Identification Name/Number:
FTK1

Comment:
First lab on Analysis

Local Evidence Time Zone:
Europe/Dublin



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
ftk-demo1-image\CHAPTE...	C:\Users\Mic...	FTK1	FAT12	N	Europe/D...	First lab on...

After selecting the 'ftk-demo1-**image.1**' file for analysis, the system will prompt you to specify the location where any files or reports generated during the analysis should be stored. It's recommended to use the default folder associated with the image file storage for convenience. Once you've designated the storage location, proceed by clicking the 'Finish' button.

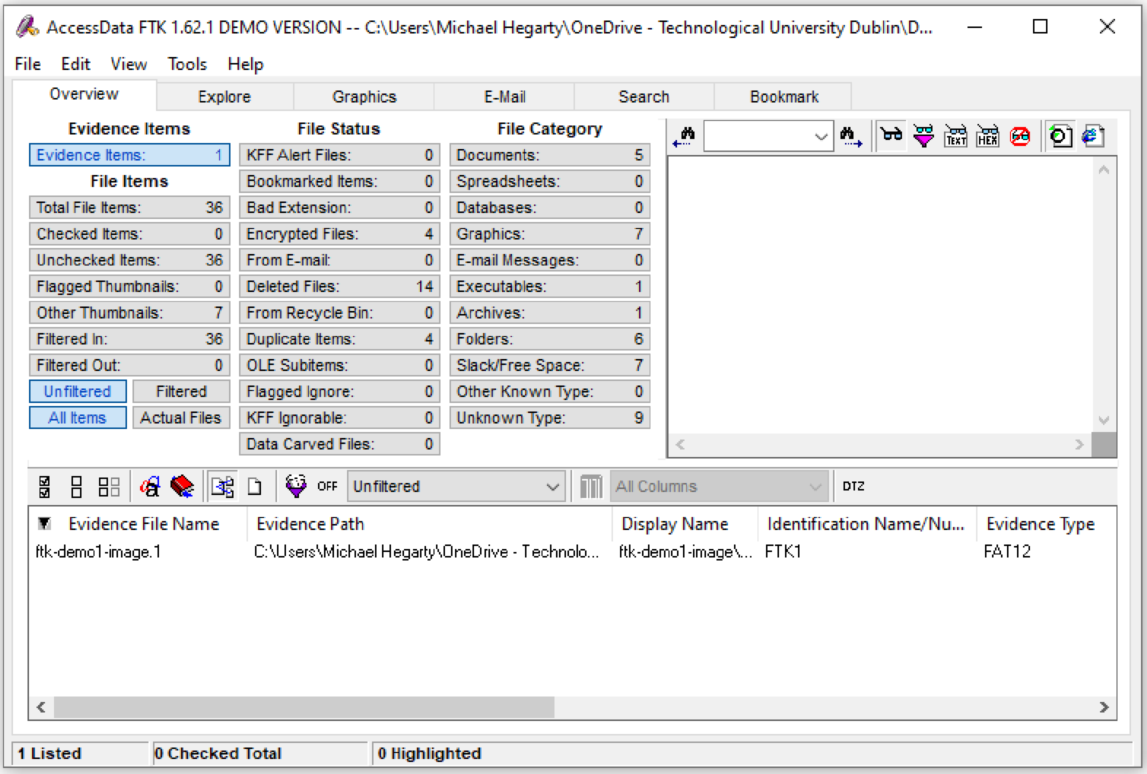
At this point, FTK will initiate a series of essential steps in the analysis process. These steps encompass the cataloguing and indexing of data within the image file, both of which play pivotal roles in the investigative process.

Cataloguing Data: The cataloguing process is integral to organizing the digital evidence. FTK will meticulously list and categorize each file present within the image. Each file is categorized into its own section, making it easily accessible for subsequent analysis. This organized structure simplifies the review and examination of individual files, ensuring that no crucial piece of evidence goes unnoticed.

Indexing for Efficient Searches: Simultaneously, FTK will commence the indexing feature, which is a powerful tool for investigators. Indexing creates a comprehensive database that catalogues every word found within the image, along with its precise location. This database enables instant keyword searches, speeding up locating specific information of interest to the investigation. Whether it's names, phrases, or technical terms, the indexing feature ensures quick and efficient retrieval of relevant data.

Both cataloguing and indexing are critical components of the forensic analysis process. They help forensic analysts manage, search, and uncover valuable insights within digital evidence. As FTK proceeds with these steps, it sets the stage for a thorough and systematic examination of the image's contents."

After the cataloguing and indexing processes are completed, FTK presents a user-friendly interface with various tab options for further analysis. This interface offers valuable tools and options for investigators to explore and dissect the digital evidence effectively. Let's delve into these tab options:



AccessData FTK 1.62.1 DEMO VERSION -- C:\Users\Michael Hegarty\OneDrive - Technological University Dublin\D...

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	5
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	36	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	4	Graphics:	7
Unchecked Items:	36	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	14	Executables:	1
Other Thumbnails:	7	From Recycle Bin:	0	Archives:	1
Filtered In:	36	Duplicate Items:	4	Folders:	6
Filtered Out:	0	OLE Subitems:	0	Slack/Free Space:	7
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	0
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	9
		Data Carved Files:	0		

OFF Unfiltered | All Columns | DTZ

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
ftk-demo1-image.1	C:\Users\Michael Hegarty\OneDrive - Technolo...	ftk-demo1-image\...	FTK1	FAT12

1 Listed | 0 Checked Total | 0 Highlighted

Overview Tab: The Overview Tab serves as a starting point for your analysis. It provides a high-level summary of the key details and statistics related to the digital evidence you are examining. Here, you can quickly access essential information about the image, including its size, number of files, and various data attributes.

Explore Tab: The Explore Tab is a versatile tool for navigating and inspecting the contents of the image. It allows you to explore the file structure, view file properties, and conduct searches to locate specific items of interest. The Explore Tab is central to the in-depth examination of individual files and directories within the digital evidence.

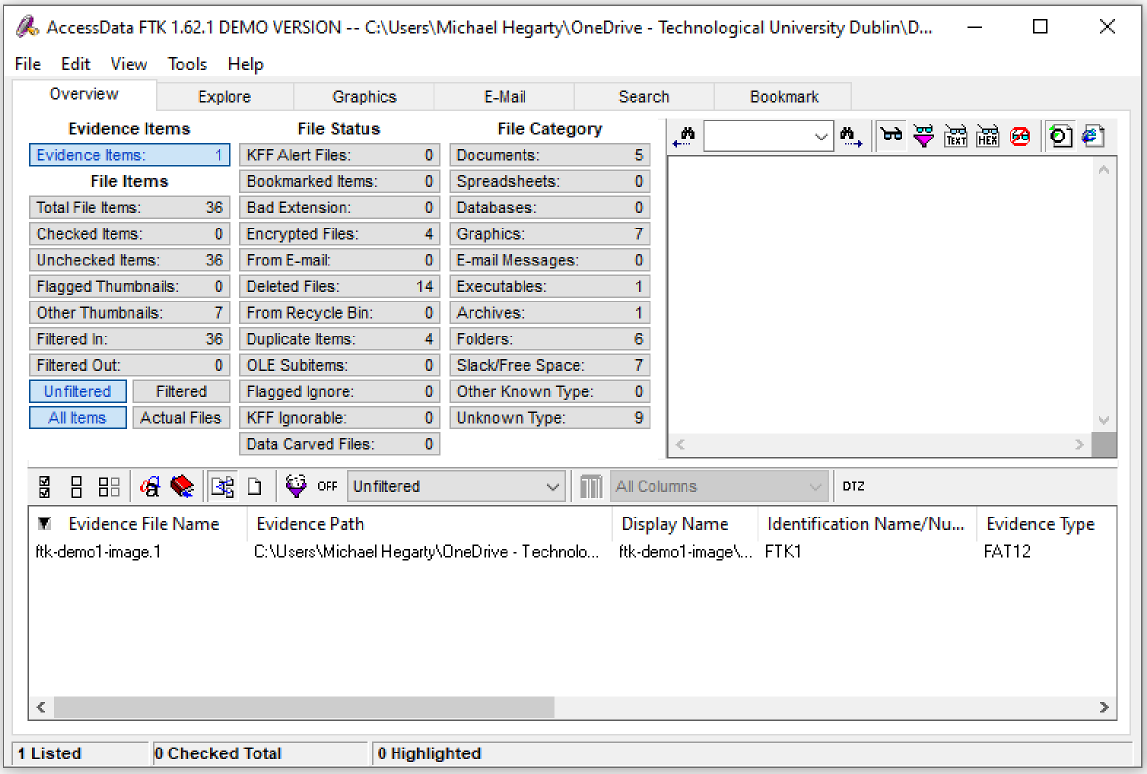
Graphics Tab: The Graphics Tab is particularly useful for handling image files within the evidence. It provides tools for previewing and analysing image content. This tab allows investigators to examine images for potential clues, hidden data, or relevant information in visual formats.

[Additional Tabs]: Depending on the version and configuration of FTK, you may encounter other tabs tailored to specific analysis needs. These could include tabs for viewing documents, emails, web history, and more. Each tab serves a unique purpose and assists in uncovering pertinent details during the investigative process.

These tab options collectively empower forensic analysts with the tools needed to conduct a comprehensive examination of the digital evidence. They enable investigators to drill down into specific data elements, uncover relationships between files, and extract valuable insights crucial to the investigation.

As you progress with your analysis, you can select the appropriate tab that aligns with your investigative objectives, allowing you to methodically explore, assess, and extract relevant information from the digital evidence.

"Learning by doing and experimenting with the functionality is a crucial part of becoming a proficient Digital Forensics Investigator. Do not hesitate to explore various tools and techniques, and do not be discouraged by mistakes—mistakes are often valuable learning opportunities. Continuously build your skills, stay curious, and stay updated with the latest developments in digital forensics. It's a dynamic field, and hands-on experience is one of the most effective ways to grow your expertise" Michael.


AccessData FTK 1.62.1 DEMO VERSION -- C:\Users\Michael Hegarty\OneDrive - Technological University Dublin\D...
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
OFF
Unfiltered
All Columns
DTZ

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	5
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	36	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	4	Graphics:	7
Unchecked Items:	36	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	14	Executables:	1
Other Thumbnails:	7	From Recycle Bin:	0	Archives:	1
Filtered In:	36	Duplicate Items:	4	Folders:	6
Filtered Out:	0	OLE Subitems:	0	Slack/Free Space:	7
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	0
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	9
		Data Carved Files:	0		

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
ftk-demo1-image.1	C:\Users\Michael Hegarty\OneDrive - Technolo...	ftk-demo1-image\...	FTK1	FAT12

1 Listed | 0 Checked Total | 0 Highlighted

To proceed with your analysis, navigate to the 'Explore' tab option within the FTK interface. In the upper-left pane of the 'Explore' tab, you'll find the folders tree. Here's what you need to do next:

Expand Folder Tree: Begin by clicking on the folders tree in the upper-left pane. This action will expand the tree view, revealing the hierarchical structure of folders and directories within the digital evidence.

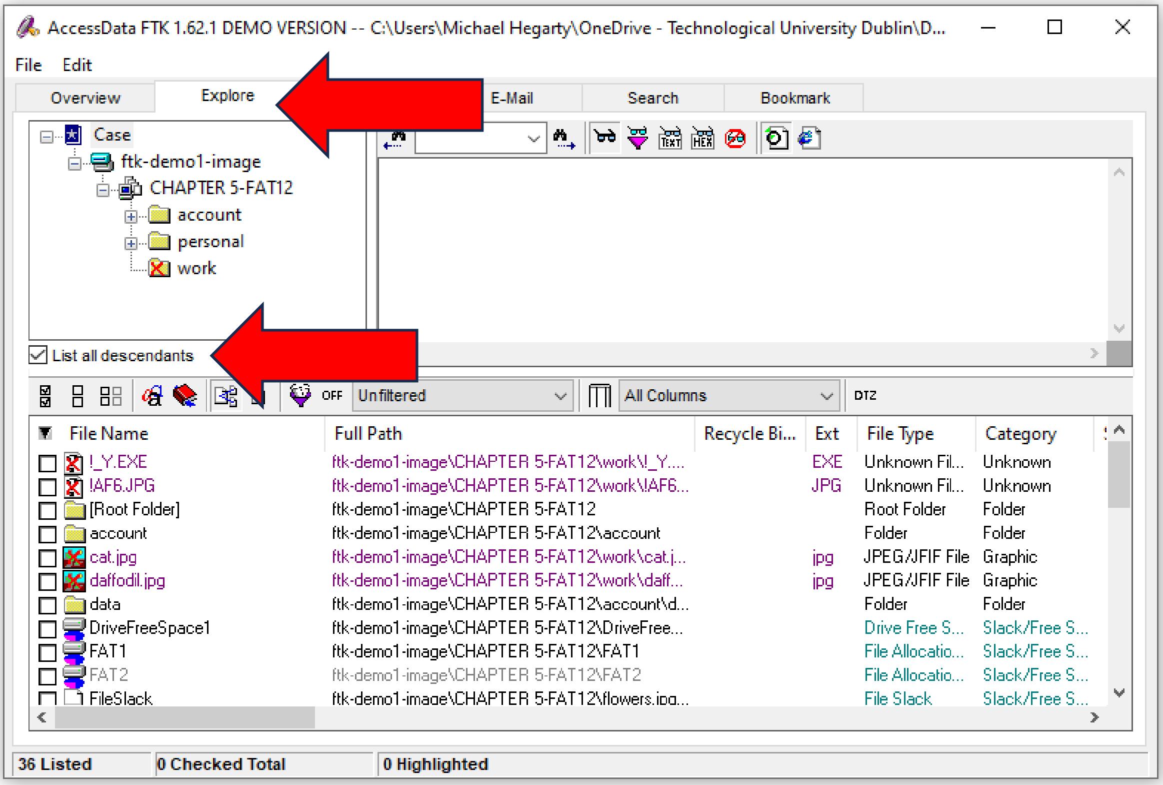
Select 'List all descendants': Within the expanded folders tree, locate and click on the 'List all descendants' option. You can typically find this option by clicking a checkbox or box icon.

How the navigation works between the 'Explore,' 'Graphics,' and 'E-Mail' tabs within the FTK window:

- When switching between these tabs, the focus remains on displaying the contents of folders. This means that clicking on a folder in the upper-left pane will display the contents of that specific folder in the lower pane of the interface.

- The 'List all descendants' option is particularly valuable. It enables you to view all files contained within the entire digital evidence, regardless of the folder or directory they are located in. This can be extremely useful for quickly scrolling through and examining all files at once, offering a comprehensive view of the evidence.

By following these steps and utilizing the 'List all descendants' option, you can efficiently navigate through the digital evidence, access specific folders, and explore all files within the investigation, streamlining your forensic analysis process."



	File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□	!_Y.EXE	ftk-demo1-image\CHAPTER 5-FAT12\work\!_Y....		EXE	Unknown Fil...	Unknown
□	!AF6.JPG	ftk-demo1-image\CHAPTER 5-FAT12\work\!AF6...		JPG	Unknown Fil...	Unknown
□	[Root Folder]	ftk-demo1-image\CHAPTER 5-FAT12			Root Folder	Folder
□	account	ftk-demo1-image\CHAPTER 5-FAT12\account			Folder	Folder
□	cat.jpg	ftk-demo1-image\CHAPTER 5-FAT12\work\cat.j...		jpg	JPEG/JFIF File	Graphic
□	daffodil.jpg	ftk-demo1-image\CHAPTER 5-FAT12\work\daff...		jpg	JPEG/JFIF File	Graphic
□	data	ftk-demo1-image\CHAPTER 5-FAT12\account\d...			Folder	Folder
□	DriveFreeSpace1	ftk-demo1-image\CHAPTER 5-FAT12\DriveFree...			Drive Free S...	Slack/Free S...
□	FAT1	ftk-demo1-image\CHAPTER 5-FAT12\FAT1			File Allocatio...	Slack/Free S...
□	FAT2	ftk-demo1-image\CHAPTER 5-FAT12\FAT2			File Allocatio...	Slack/Free S...
□	FileSlack	ftk-demo1-image\CHAPTER 5-FAT12\flowers.jpg...			File Slack	Slack/Free S...

36 Listed | 0 Checked Total | 0 Highlighted

To systematically review the contents of each file within the digital evidence, follow these steps:

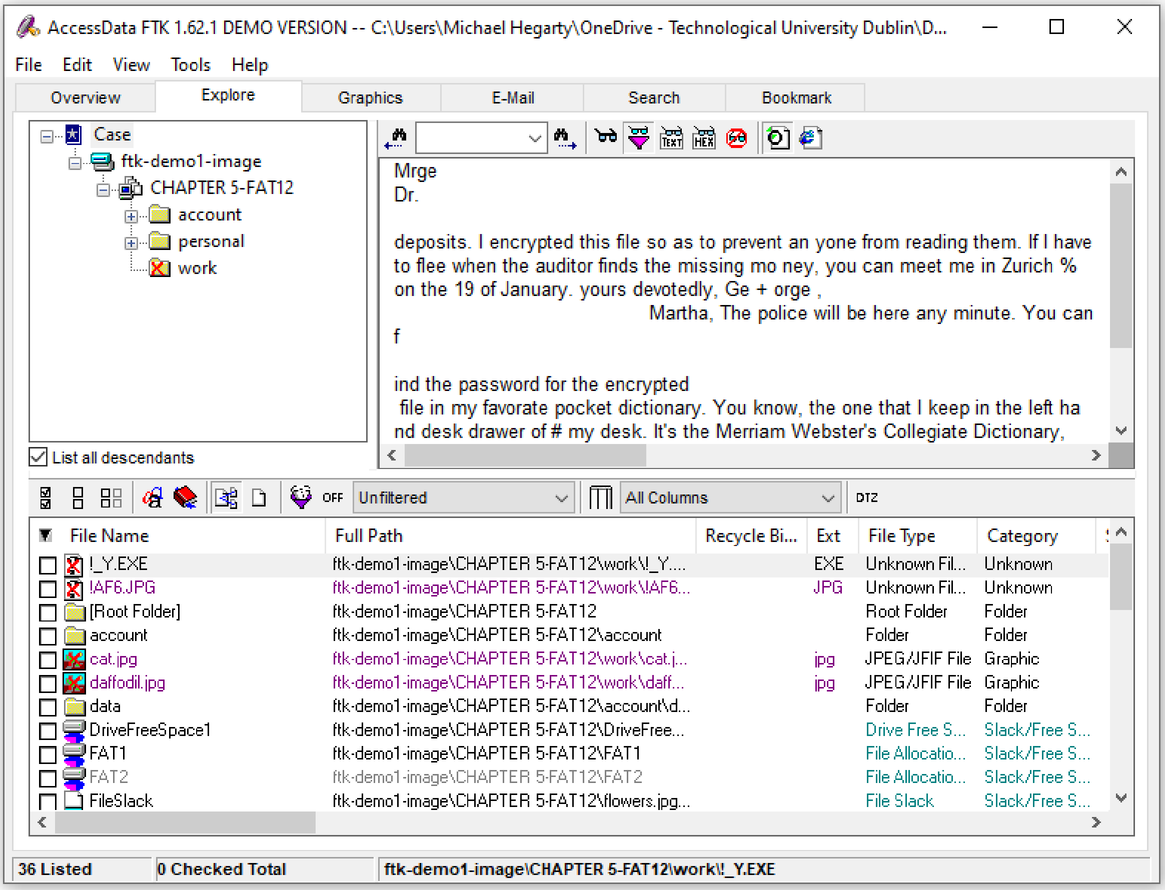
1. Select Files in the Lower Pane: In the lower pane of the interface, you will find a list of files. To review the contents of each file, click on the file name one at a time. This action will highlight the selected file and initiate the content display in the upper-right pane.

2. Examine Text Data: In the upper-right pane, you will observe any text data contained within the selected file. This text could include document contents, messages, or any other textual information present in the file.

3. Review File Contents: Carefully read through the text displayed in the upper-right pane. Take note of any information, keywords, or details that are pertinent to the investigation. Be thorough in your examination, as these textual insights can provide valuable leads, context, or evidence relevant to your analysis.

4. Repeat for Each File: After reviewing the contents of the first file, return to the lower pane and select the next file in the list. Continue this process one file at a time until you have examined the contents of all relevant files within the digital evidence.

This meticulous approach ensures a comprehensive review of the text data contained in each file. It allows you to uncover critical information, detect patterns, and piece together the puzzle of the digital evidence. Take thorough notes and document any findings that could be relevant to the investigation, as these insights may play a crucial role in uncovering the facts.

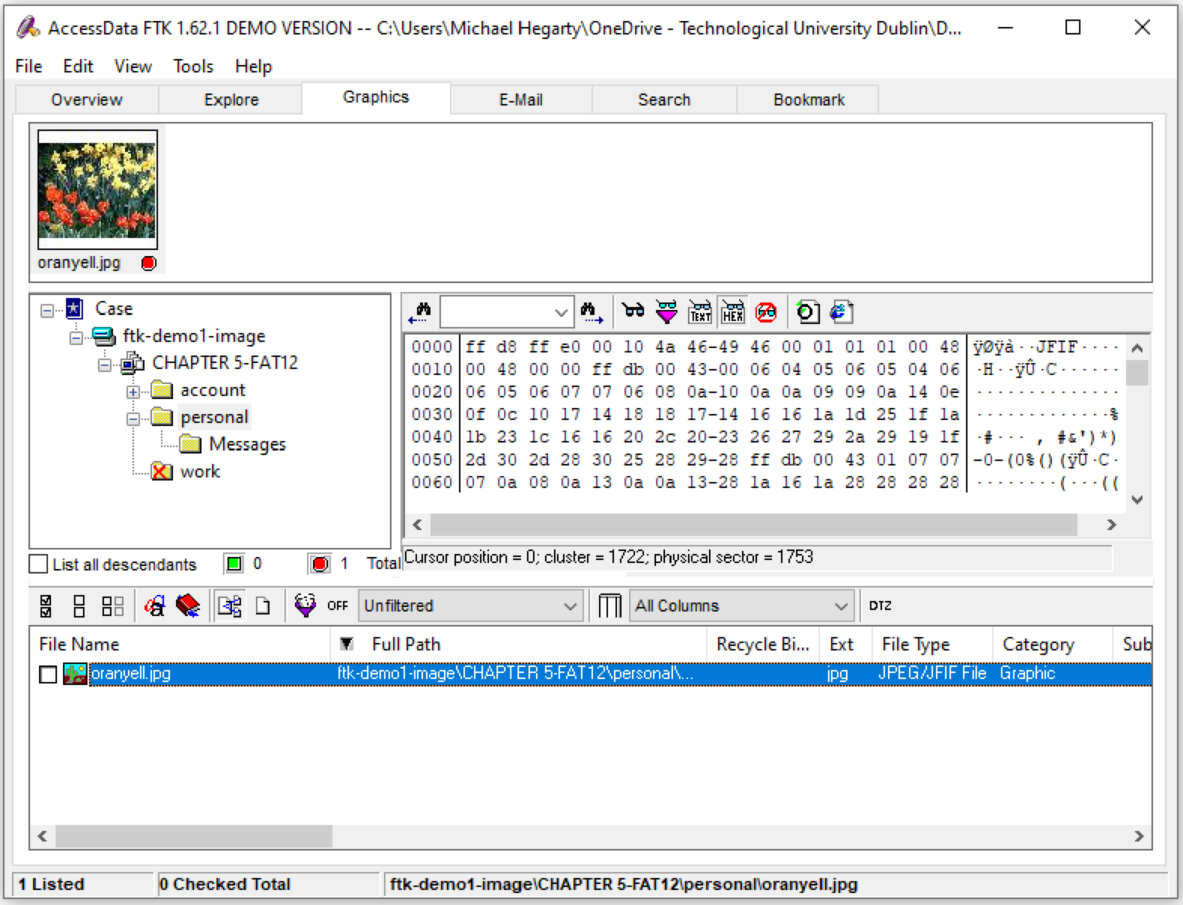


```
Mrge
Dr.

deposits. I encrypted this file so as to prevent an yone from reading them. If I have
to flee when the auditor finds the missing mo ney, you can meet me in Zurich %
on the 19 of January. yours devotedly, Ge + orge ,
                                         Martha, The police will be here any minute. You can
f

ind the password for the encrypted
 file in my favorate pocket dictionary. You know, the one that I keep in the left ha
nd desk drawer of # my desk. It's the Merriam Webster's Collegiate Dictionary,
```

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□	!_Y.EXE	ftk-demo1-image\CHAPTER 5-FAT12\work\!_Y....		EXE	Unknown Fil...	Unknown
□	!AF6.JPG	ftk-demo1-image\CHAPTER 5-FAT12\work\!AF6...		JPG	Unknown Fil...	Unknown
□	[Root Folder]	ftk-demo1-image\CHAPTER 5-FAT12			Root Folder	Folder
□	account	ftk-demo1-image\CHAPTER 5-FAT12\account			Folder	Folder
□	cat.jpg	ftk-demo1-image\CHAPTER 5-FAT12\work\cat.j...		jpg	JPEG/JFIF File	Graphic
□	daffodil.jpg	ftk-demo1-image\CHAPTER 5-FAT12\work\daff...		jpg	JPEG/JFIF File	Graphic
□	data	ftk-demo1-image\CHAPTER 5-FAT12\account\d...			Folder	Folder
□	DriveFreeSpace1	ftk-demo1-image\CHAPTER 5-FAT12\DriveFree...			Drive Free S...	Slack/Free S...
□	FAT1	ftk-demo1-image\CHAPTER 5-FAT12\FAT1			File Allocatio...	Slack/Free S...
□	FAT2	ftk-demo1-image\CHAPTER 5-FAT12\FAT2			File Allocatio...	Slack/Free S...
□	FileSlack	ftk-demo1-image\CHAPTER 5-FAT12\flowers.jpg...			File Slack	Slack/Free S...

36 Listed | 0 Checked Total | ftk-demo1-image\CHAPTER 5-FAT12\work\!_Y.EXE

Non-text-based files will appear as Hex (see below).



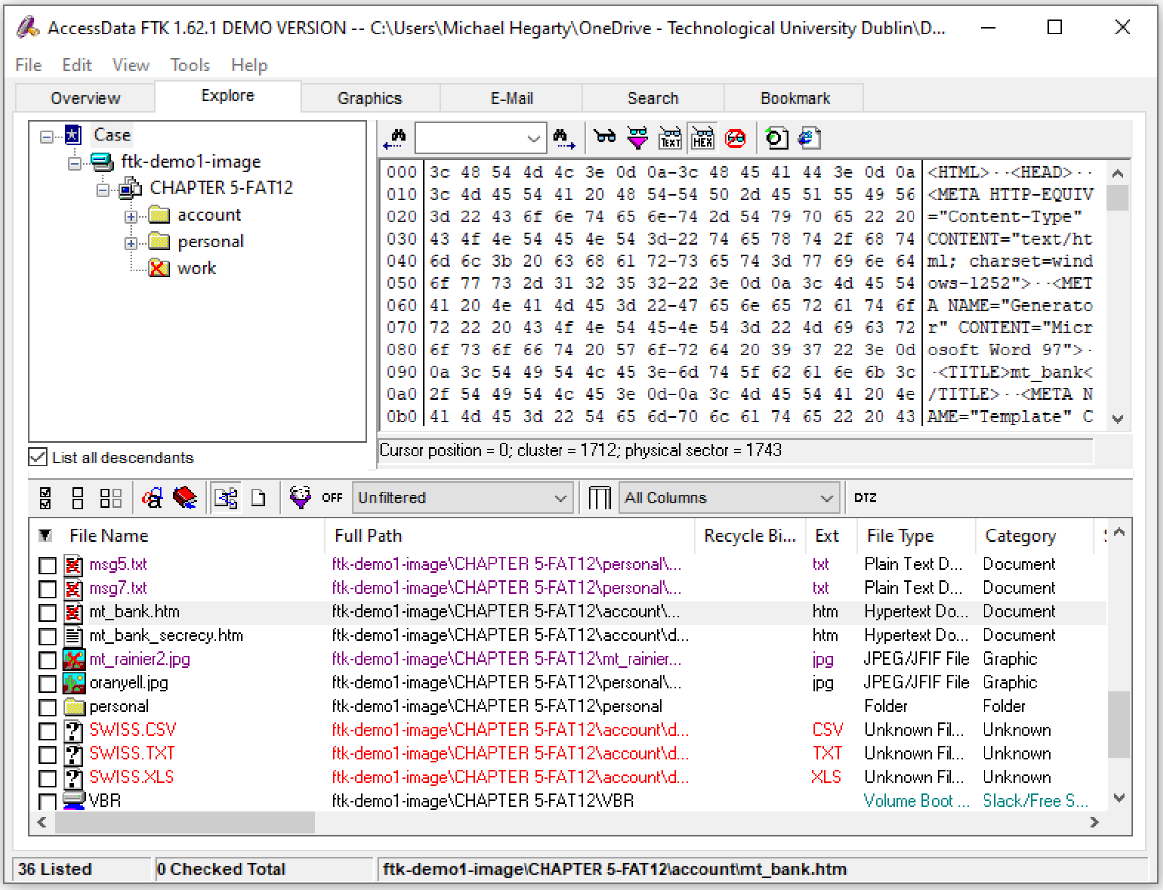
```
0000 ff d8 ff e0 00 10 4a 46-49 46 00 01 01 01 00 48  ÿØÿà··JFIF····
0010 00 48 00 00 ff db 00 43-00 06 04 05 06 05 04 06  ·H··ÿÛ·C······
0020 06 05 06 07 07 06 08 0a-10 0a 0a 09 09 0a 14 0e  ··············
0030 0f 0c 10 17 14 18 18 17-14 16 16 1a 1d 25 1f 1a  ·············%
0040 1b 23 1c 16 16 20 2c 20-23 26 27 29 2a 29 19 1f  ·#··· , #&')*)
0050 2d 30 2d 28 30 25 28 29-28 ff db 00 43 01 07 07  -0-(0%()(ÿÛ·C·
0060 07 0a 08 0a 13 0a 0a 13-28 1a 16 1a 28 28 28 28  ·········(···((
```

Cursor position = 0; cluster = 1722; physical sector = 1753

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Sub
□ oranyell.jpg	ftk-demo1-image\CHAPTER 5-FAT12\personal\...		jpg	JPEG/JFIF File	Graphic	

1 Listed | 0 Checked Total | ftk-demo1-image\CHAPTER 5-FAT12\personal\oranyell.jpg

When you have located a file containing information you think is important, click the check box to the left of the file name and continue searching and selecting additional files of interest as you find them.



```
000 3c 48 54 4d 4c 3e 0d 0a-3c 48 45 41 44 3e 0d 0a <HTML>··<HEAD>··
010 3c 4d 45 54 41 20 48 54-54 50 2d 45 51 55 49 56 <META HTTP-EQUIV
020 3d 22 43 6f 6e 74 65 6e-74 2d 54 79 70 65 22 20 ="Content-Type"
030 43 4f 4e 54 45 4e 54 3d-22 74 65 78 74 2f 68 74 CONTENT="text/ht
040 6d 6c 3b 20 63 68 61 72-73 65 74 3d 77 69 6e 64 ml; charset=wind
050 6f 77 73 2d 31 32 35 32-22 3e 0d 0a 3c 4d 45 54 ows-1252">··<MET
060 41 20 4e 41 4d 45 3d 22-47 65 6e 65 72 61 74 6f A NAME="Generato
070 72 22 20 43 4f 4e 54 45-4e 54 3d 22 4d 69 63 72 r" CONTENT="Micr
080 6f 73 6f 66 74 20 57 6f-72 64 20 39 37 22 3e 0d osoft Word 97">·
090 0a 3c 54 49 54 4c 45 3e-6d 74 5f 62 61 6e 6b 3c ·<TITLE>mt_bank<
0a0 2f 54 49 54 4c 45 3e 0d-0a 3c 4d 45 54 41 20 4e /TITLE>··<META N
0b0 41 4d 45 3d 22 54 65 6d-70 6c 61 74 65 22 20 43 AME="Template" C
```

Cursor position = 0; cluster = 1712; physical sector = 1743

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□	msg5.txt	ftk-demo1-image\CHAPTER 5-FAT12\personal\...		txt	Plain Text D...	Document
□	msg7.txt	ftk-demo1-image\CHAPTER 5-FAT12\personal\...		txt	Plain Text D...	Document
□	mt_bank.htm	ftk-demo1-image\CHAPTER 5-FAT12\account\...		htm	Hypertext Do...	Document
□	mt_bank_secrecy.htm	ftk-demo1-image\CHAPTER 5-FAT12\account\d...		htm	Hypertext Do...	Document
□	mt_rainier2.jpg	ftk-demo1-image\CHAPTER 5-FAT12\mt_rainier...		jpg	JPEG/JFIF File	Graphic
□	oranyell.jpg	ftk-demo1-image\CHAPTER 5-FAT12\personal\...		jpg	JPEG/JFIF File	Graphic
□	personal	ftk-demo1-image\CHAPTER 5-FAT12\personal			Folder	Folder
□	SWISS.CSV	ftk-demo1-image\CHAPTER 5-FAT12\account\d...		CSV	Unknown Fil...	Unknown
□	SWISS.TXT	ftk-demo1-image\CHAPTER 5-FAT12\account\d...		TXT	Unknown Fil...	Unknown
□	SWISS.XLS	ftk-demo1-image\CHAPTER 5-FAT12\account\d...		XLS	Unknown Fil...	Unknown
□	VBR	ftk-demo1-image\CHAPTER 5-FAT12\VBR			Volume Boot ...	Slack/Free S...

36 Listed | 0 Checked Total | ftk-demo1-image\CHAPTER 5-FAT12\account\mt_bank.htm

Now that you have successfully installed and acquired familiarity with the FTK tool for analysing the disk image, it's time to delve into the investigation of the digital evidence. As you proceed, it's crucial to keep meticulous records of your actions and findings. This investigation marks the initiation of your first forensic report, and comprehensive documentation is key to its credibility and effectiveness.

Please note, if you close the FTK application and it will not open for you again, please right click on the application and "run as administrator".