LIVE CYBER FORENSICS

Thesis submitted in partial fulfilment

Of the requirements of the degree of

Bachelor of Computer

Application in

Cloud Technology and Information Security

By

Priya Godse (2020-B-03102002)

And

Suyog Deshmukh (2020-B-220122000A)

Under the Supervision of

Prof. Ayushi Godiya

MAY 2023

School of Engineering Ajeenkya D Y Patil

University, Pune

AJEENKYA
D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY

School of Engineering

MAY, 2023

CERTIFICATE

This is to certify that the dissertation entitled **“Live Cyber Forensics”** is a bonafide work of “**Priya Godse” (2020-B-03102002) & “Suyog Deshmukh” (2020-B-22122000A)** submitted to the School of Engineering, Ajeenkya D Y Patil University, Pune in partial fulfillment of the requirement for the award of the degree of **“Bachelor of Computer Application In Cloud Technology And Information Security”**.

Prof. Ayushi Godiya
Supervisor

Internal-Examiner

External Examiner

Dr. Biswajeet Champaty

Head-School of Engineering

AJEENKYA
D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY

School of Engineering

Supervisor’s Certificate

This is to certify that the dissertation entitled **“Live Cyber Forensics”** submitted by of “**Priya Godse” (2020-B-03102002) & “Suyog Deshmukh” (2020-B-22122000A),** is a record of origin

all work carried outby him/her under my supervision and guidance in partial fulfillment of the requirements of the degree of **Bachelor of Computer Application In Cloud Technology And Information Security** at **School of Engineering**, **Ajeenkya DY Patil University, Pune, Maharashtra- 412105**. Neither this dissertation nor any part of it has been submitted earlier for anydegree or diploma to any institute or university in India or abroad.

Prof. Ayushi Godiya
Supervisor

AJEENKYA
D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY

School of Engineering

Declaration of Originality

We, ***“Priya Godse” (2020-B-03102002) & “Suyog Deshmukh” (2020-B-22122000A)***, hereby declare that this dissertation entitled ***“Live Cyber Forensics”*** presents my original work carried out as a bachelor student of School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra. To the best of our knowledge, this dissertation contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of Ajeenkya D Y Patil University,Pune or any other institution. Any contribution made to this research by others, with whom we haveworked at Ajeenkya D Y Patil University, Pune or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged underthe sections “Reference” or “Bibliography”. we also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

we am fully aware that in case of any non-compliance detected in future, the Academic Council of Ajeenkya D Y Patil University, Pune may withdraw the degree awarded to me on the basis of the present dissertation.

Date: MAY, 2023

Place: Lohegaon,
Pune

Priya Godse **Suyog Deshmukh**

Acknowledgement

We remain immensely obliged to **PROF. AYUSHI GODIYA , DR. SAROJ NANDA & PROF. RAVI KHATRI** for providing us with the idea of this topic, and for her valuable support in garnering resources for us either by way of information or computers also her guidance and supervision which made this internship/Project happen.

we would like to say that it has indeed been a fulfilling experience for working out this Project.

Abstract

Live digital forensics, commonly referred to as live analysis or live response, is an essential procedure for gathering and examining digital evidence from a system that is now in use or that has just been shut down. Digital forensics has grown in significance in recent years as a result of the rise in the frequency, sophistication, and complexity of cyberattacks. However, the sophistication of cyber attacks and the advancement of technology make it difficult for traditional digital forensics approaches to keep up.

The coming into being of new storage media, file formats, and operating systems as a result of technological advancement makes it difficult for experts in digital forensics to extract and analyse data from digital devices.

In summary, the goal of this research project is to offer effective and trustworthy techniques for gathering digital evidence during real-time digital forensics investigations. Some of the difficulties faced by digital forensics experts, such as the need to retrieve data from corrupted or destroyed storage media or the need to avoid being discovered by attackers using anti-forensics tactics, can be addressed through the use of cloning, data recovery, and steganography techniques. The suggested fixes can increase the effectiveness and dependability of digital forensics investigations, contributing to the overall advancement of the field.

KEYWORDS*:-*. Imaging/Cloning, Data recovery, Steganography. Hash value, Report

CONTENTS

Page No

Chapter 1 :- INTRODUCTION 1

Chapter 2 :- LITERATURE REVIEW 2

2.1 Cloning 2

2.2 Data Recovery 3

2.3 Steganography 4

2.4 Problem Definitioz 4

Chapter 3 :- METHODOLOGY 5

3.1 Data Sources 5

3.2 Data Collection 6

3.3 Data Analysis 6

3.4 Reporting and Communication 7

3.5 Security 7

3.6 Documentation 8

Chapter 4 :- TOOLS 9

4.1 Available Tools

4.1.1 Access data ftk imager 9

4.1.2 Logicube Talon Ultimate 14

4.1.3 Mobil edit (mobile phone extraction) 15

4.1.4 Cellebrite ufed 22

4.2 Unique Tool

4.2.1 Browser Forensics 25

Chapter 5 :- RESULTS AND DISCUSSION 37

Chapter 6 :- CONCLUSION REFERENCES 40

LIST OF FIGURE

FIGURE .NO	FIGURE	PAGE .NO
Fig 1.1 to Fig 1.8	ACCESS DATA FTK IMAGER	10-13
Fig 1.9	LOGICUBE TALON ULTIMATE	14
Fig 1.10 to Fig 1.21	MOBILE EDIT	16-21
Fig 1.22 to Fig 1.25	CELLEBRITE UFED	23-24
Fig 1.26 to Fig 1.47	BROWSER FORENSICS	28-36

CHAPTER 1

INTRODUCTION

In the current digital era, digital forensics has become a crucial component of investigations. Digital evidence can be extremely useful in a variety of situations, such as criminal investigations, civil lawsuits, and corporate investigations, because to the ubiquitous use of technology and the internet. To properly conduct investigations, however, digital forensics offers particular difficulties that call for specialised abilities and Knowledge.[1]

Live digital forensics, often referred to as live analysis or live response, entails gathering and examining digital evidence from a system that is now in use or that has just been shut down. This procedure is essential because it enables forensic investigators to gather volatile data that would be destroyed in the event that the system were to be switched off or shut down. To maintain the integrity of the evidence gathered, live digital forensics involves highly technical expertise and knowledge of digital systems, operating systems, and network protocols.

Data collection in real-time throughout the live digital forensics process poses special difficulties for forensic analysts. Forensic investigators, for instance, must gather data without contaminating or modifying it, which necessitates the use of specialised equipment. Additionally, the forensic examiner must instantly analyse data to find pertinent information. The examiner must possess the ability to eliminate unimportant material and concentrate on the data that is relevant to the investigation in order to accomplish this.[1]

Therefore, an essential phase in digital forensics investigations is live digital forensics. To efficiently gather and examine digital evidence from a recently shut down or actively running system, you need specialised knowledge, skills, and tools. To maintain the integrity and admissibility of digital evidence in court, forensic analysts and investigators must have a thorough understanding of the difficulties and complexity of live digital forensics

CHAPTER 2

LITERATURE REVIEW

2.1 CLONING :-

Cloning is the most widely recognized approach to making an exact duplicate of a hard drive or other computerized storing media. This strategy is customarily used in computerized criminology assessments for safeguarding verification and ensuring that the primary information stays in salvageable shape. A couple of studies have broke down the viability of various cloning strategies in computerized criminology assessments. For example, Casey and Stellatos (2006) saw three changed procedures for plate cloning and found that an equipment based approach gave the best results as to speed and found that an equipment based approach gave the best results concerning speed, and exactness. [2]

Cloning is the procedure of creating a living being's accurate hereditary copy. Both precipitously, as on account of indistinguishable twins, and falsely, utilizing innovation, are conceivable. Substantial cell atomic exchange (SCNT), the most famous procedure for making counterfeit clones, is embedding a physical cell's core into an egg cell whose own core has been taken out. Physical cells are any cells in the body other than sperm or egg cells. A substitute mother is then used to embed the subsequent undeveloped organism and permit it to develop.

Cloning has produced banter on account of its potential moral, legitimate, and social consequences. Cloning brings up issues in regards to its security, the chance of abuse, and the impacts on human character and respect, even while it can possibly be used for clinical reasons like making organs for relocate or treating sicknesses. Albeit creature cloning is all the more as often as possible utilized,
1are as of now rules and guidelines set up in numerous countries that confine or deny human cloning. [2]

2.2 DATA RECOVERY

Information recuperation is the technique engaged with recovering information that has been lost or eradicated in view of equipment disillusionment, programming bumbles, or conscious deletion. This procedure is central for computerized legal sciences analysts to recover significant evidence from hurt or subverted advanced limit media. A couple of studies have reviewed the viability of various information recuperation procedures in computerized legal sciences assessments. For example, Kessler and Dreyfus (2000) cultivated a clever information cutting method that had the choice to recover over 80% of eradicated reports from a hurt hard drive.[3]

Data recovery insinuates the most well-known approach to recuperating lost, demolished, or eradicated data from various limit media like hard, major areas of strength for drives (SSDs), USB drives, memory cards, and others.

The course of data recovery routinely incorporates the use of specific programming or hardware gadgets that can channel and recover data from the influenced accumulating media. Now and again, data recovery could require the organizations of a specialist data recovery master who has dominance in overseeing complex data hardship circumstances.

It's fundamental to observe that data recovery isn't for the most part possible, and the potential outcomes of powerful data recovery depend upon various factors, similar to the justification for data adversity, the sort of amassing media, and the level of the damage or degradation.

To restrict the bet of data incident, it's fundamental to regularly back up your data to a strong region, and to do whatever it takes not to use unstable or untested programming or hardware that could really hurt your ability media.[3]

2.3 STEGANOGRAPHY

Steganography is the demonstration of covering information inside different information in a way that isn't successfully distinguished. This strategy is normally used by cybercriminals to hide fragile information, for instance, passwords, Mastercard numbers, and other individual information. A few investigations have dissected the viability of various steganography identification methods in computerized legal sciences assessments. For example, Fridrich et al. (2002) cultivated a steganalysis instrument called Stegdetect that had the choice to identify the presence of steganographic fulfillment with a serious degree of precision.

Generally speaking, the writing suggests that cloning, information recuperation, and steganography are critical methods for advanced criminology specialists to effectively assemble and examine computerized evidence. In any case, the examinations likewise highlight the necessity for continuing with exploration and improvement staying put mindful of the headway of advancement and the creating refinement of cybercrime.[4]

2.4 PROBLEM DEFINITION

The rising interest for productive and dependable strategies for cloning, data recuperation, and steganography in the computerized legal sciences space has prompted a requirement for proceeded with innovative work here. Cloning is the method involved with making a careful imitation of a hard drive or other computerized stockpiling media. Data recuperation is the method involved with recuperating data that has been lost or erased because of equipment disappointment, programming blunders, or deliberate erasure. Steganography is the act of covering information inside different information in a way that isn't handily recognized. These strategies are fundamental for computerized legal sciences examiners to gather and break down advanced proof effectively.[5]

CHAPTER 3

METHODOLOGY

3.1 DATA SOURCES

Data sources are essential in digital forensics for locating, protecting, gathering, analysing, and presenting electronic evidence. Here are a few typical digital forensics data sources:

1. Computers: A common task in digital forensics is the analysis of data from computers, including servers, desktops, laptops, and storage devices.
2. Mobile devices: Data from mobile devices, such as tablets and smartphones, might be useful in digital forensics investigations. The information may consist of call records, text messages, emails, location information, and internet usage.
3. Cloud storage: Services like Google Drive, Dropbox, and iCloud, which offer cloud storage, can hold a lot of digital information. Files, emails, chat logs, and metadata are all included in this.
4. Social media: Websites like Facebook, Twitter, and Instagram are excellent sources of digital evidence. They may include user profiles, postings, messages, pictures, and videos.
5. Internet of Things (IoT) gadgets: IoT gadgets, such smart speakers, thermostats, and fitness trackers, may hold data that might be helpful in digital forensics investigations. User activity records, location information, and sensor data are examples of this.
6. Network traffic: In digital forensics investigations, network traffic analysis might offer useful evidence. This comprises flow data, logs, and network packets.
7. Digital cameras: In cases involving intellectual property theft or cyberstalking, digital cameras can serve as a source of electronic evidence. Along with metadata like geolocation and timestamps, this also includes image and video files.

These are but a few illustrations of digital forensics data sources. Depending on the scope of the inquiry and the kind of digital evidence being sought, the sources of data can be very different.[5]

3.1 DATA COLLECTION

In order to identify, preserve, gather, analyse, and present digital evidence in a way that is admissible in court, a crucial component of digital forensics is data collection. Digital evidence must be gathered since it serves as the foundation for all investigations and can be used in court to support or refute claims Some of the procedures for data collecting in digital forensics include the ones listed below:

Identifying prospective sources of evidence:- such as computers, mobile devices, external storage devices, and cloud-based services, is the first stage in the data gathering process.

Secure the site in order to stop additional evidence tampering or destruction:- This entails uninstalling any external storage devices and isolating the impacted systems from the network.

Document the scene:- To make sure that no evidence is forgotten or omitted, the scene should be meticulously documented using photos, videos, and notes.[6]

3.2 DATA ANALYSIS:-

Data analysis, which involves the extraction of relevant information from digital evidence to support investigations or legal procedures, is an essential part of digital forensics. Digital evidence analysis can be a challenging and time-consuming procedure that calls for specialised skills and equipment.

Some of the steps in data analysis in digital forensics are as follows:

1. Data triage is the process of first evaluating the data to ascertain its applicability to the study. This can assist in prioritising the analytical process and identifying relevant leads.
2. Data recovery: If data has been lost or erased, it can be retrieved from storage media using recovery techniques.
3. Data decryption: In order to access encrypted data's contents, decryption may be necessary.
4. File carving :- IT is the process of extracting files from fragmented data or unallocated space.
5. Keyword search: You can look for information inside the evidence using pertinent keywords.
6. Timeline analysis: In order to find patterns and possible connections between occurrences, timeline analysis includes compiling a chronology of events.
7. Correlation between data: Correlation analysis can help to identify links between different pieces

of digital evidence[6]

3.3REPORTING AND COMMUNICATION

Cyber forensic investigations must include reporting and communication because they enable stakeholders, including law enforcement agencies, attorneys, and other interested parties, to learn the findings of the investigation. Some of the important factors for reporting and communication in cyber forensic investigations include the following:

Reports and communications should be written so that they can be used as evidence in court. This entails confirming that the inquiry was carried out in accordance with the relevant legal and ethical requirements.

Clarity: Reports and communication should be simple and clear, and technical jargon or terminology that non-technical stakeholders might not understand should be avoided.

Accuracy: Information and communication should be true and supported by solid proof. Any presumptions or restrictions must be clearly stated.[7]

3.4 SECURITY

Due to the possibility that the evidence gathered and examined may contain sensitive or confidential information, security is a crucial factor in cyber forensic investigations. Some of the most important security factors for cyber forensic investigations include the ones listed below:

Chain of custody: The documentation of the transfer of evidence from the point of collection to the point of analysis is referred to as the chain of custody. This should be upheld throughout the investigation as it serves to secure the validity and admissibility of the evidence.

Encryption and access restrictions: To prevent unauthorised access, modification, or destruction of the evidence, access rules should be put in place and the evidence should be encrypted.

Secure location: To avoid physical or digital access by unauthorised people, the evidence should be kept in a secure location, like a locked cabinet or a secure server.

Data protection: To safeguard the evidence from unintentional or deliberate loss or damage, data protection measures like backups, antivirus software, and firewalls should be in place.

Confidentiality: Confidentiality agreements must to be in place to safeguard the secrecy of the evidence and any pertinent data, including private or commercial information.

Legal requirements: Data protection and privacy-related legal requirements, such as data retention laws and data transfer rules, should be taken into account.[8]

3.5 DOCUMENTATION

In order to guarantee the integrity, correctness, and admissibility of the evidence gathered and examined during the investigation, documentation is a crucial part of cyber forensic investigations. Some important factors for documentation in cyber forensic investigations are the ones listed below:

Evidence gathering: Records of the evidence gathering process, including the date, time, place, and person in charge of gathering the evidence, should be kept.

Chain of custody: The names of anyone who had access to the evidence and any changes in custody should be listed in the chain of custody documentation, which should also be kept up to date.

Methods of analysis: Records of the procedures and equipment used to examine the evidence, as well as the methods themselves, should be kept.[8]

CHAPTER 4

TOOLS

4.1 Available Tools

4.1.1 ACCESS DATA FTK IMAGER

Enter Data A common instrument in forensic inquiry is the FTK Imager. You will learn how to efficiently and accurately gather and analyse evidence as part of a computer-related investigation in this course, AccessData Forensic Toolkit (FTK) Imager. You will first investigate how to set up and install FTK Imager. The acquisition of various image types and maintaining the integrity of the original data are the next things you'll learn how to do. Finally, you'll learn how to securely mount, inspect, and analyse the information gathered and evidence that was captured. After completing this course, you will be capable of operating the FTK Imager with the confidence necessary to do forensic imaging and analyse data as part of an investigation. Free to use, FTK Imager is a disc image creation programme. The Access Data Group was in charge of its creation. It is a tool that facilitates data viewing and imaging.[9]

Steps for Creating Image:

- Step 1: Install the FTK imager on your computer after downloading it.

- Step 2: After installation, click to launch the FTK Imager. Your first sight should be the FTK Imager dashboard.

- Step 3: In the menu navigation bar, select the File tab. This will open a drop-down menu similar to the one shown in the image below. Simply select the first option, Add Evidence Item.

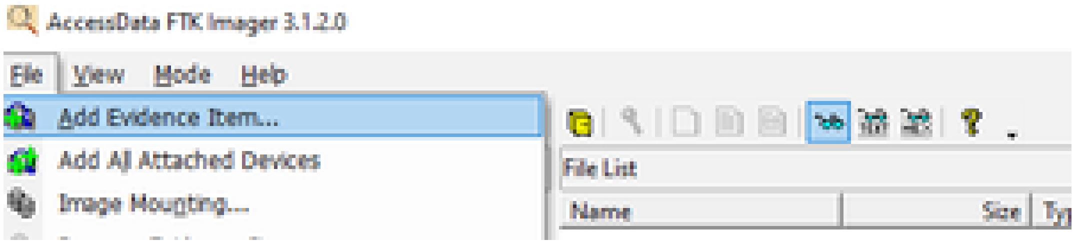


Fig 1.1

- Stage 4: A spring up window requesting that you pick the wellspring of proof will then show up. You ought to pick the Actual Drive choice in the event that an actual hard drive is associated with the PC or PC you are utilizing to make the scientific picture. Select Straightaway. Select the actual drive you need to utilize at this moment. To abstain from with nothing to do while sending out a scientific image of your operating system drive, if it's not too much trouble, twofold check the drive you are picking.
- Stage 5: The measurable photographs will presently be traded.

In the FTK Imager window, right-click the Actual Drive that you need to trade. Here, click on Product Plate Picture.

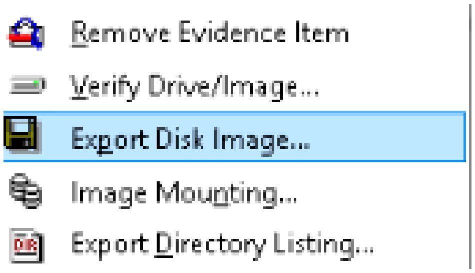


Fig 1.2

1) Select the Picture Objective and snap the Add button.

2) Conclude what sort of criminological picture you need to trade. Click Next after selecting.E01.

3) Following that, you should now enter case-related data. This component is altogether dependent upon you; you can either leave them clear or keep them general.

4) From that point onward, you should name the picture and select the objective to which you need to trade the scientific picture.

At last, we should stand by till the Scientific Picture has been created and has been affirmed. Contingent upon your equipment, the legal picture creation interaction will go contrastingly rapidly. When both have occurred, you are ready with your measurable photos.[10]

Process of Verifying Disk Image:

1) Step 1: Open FKT Software

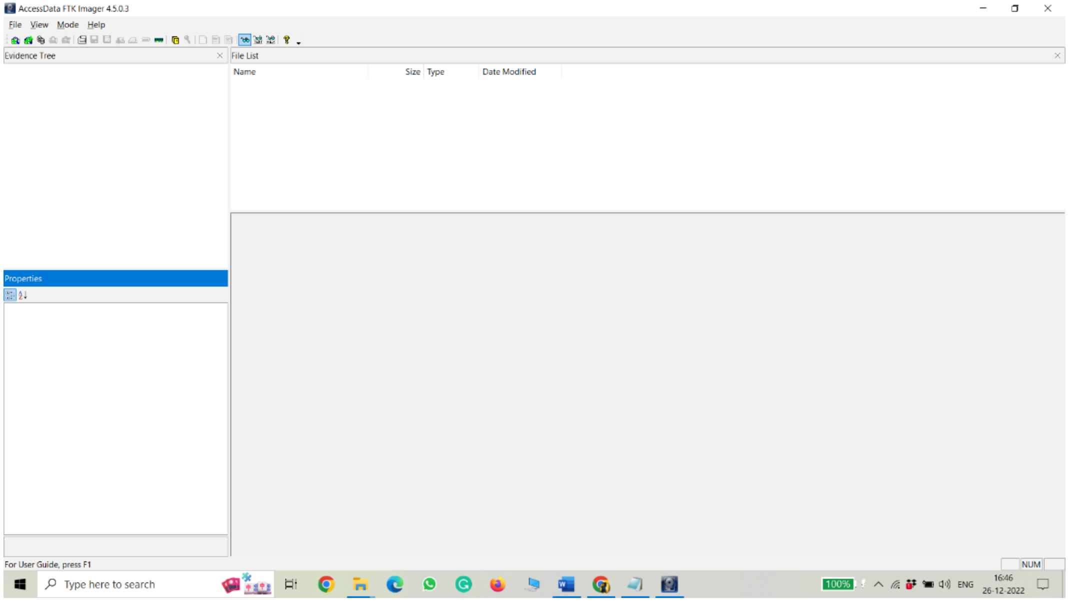
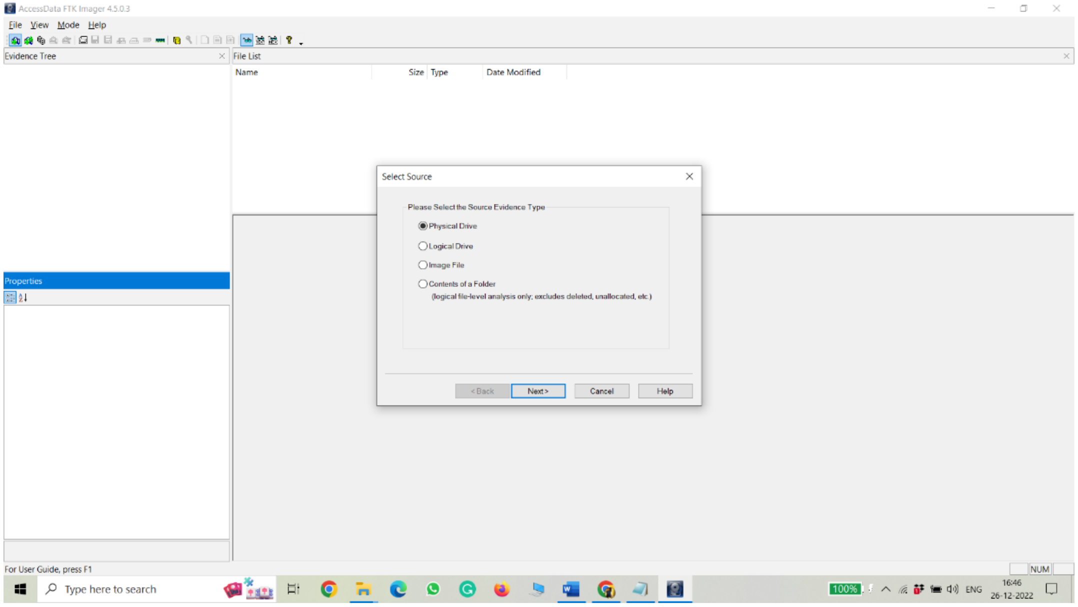


Fig 1.3

2) Step 2: Select The Drive Which is Inserted



Please Select the Source Evidence Type

● Physical Drive

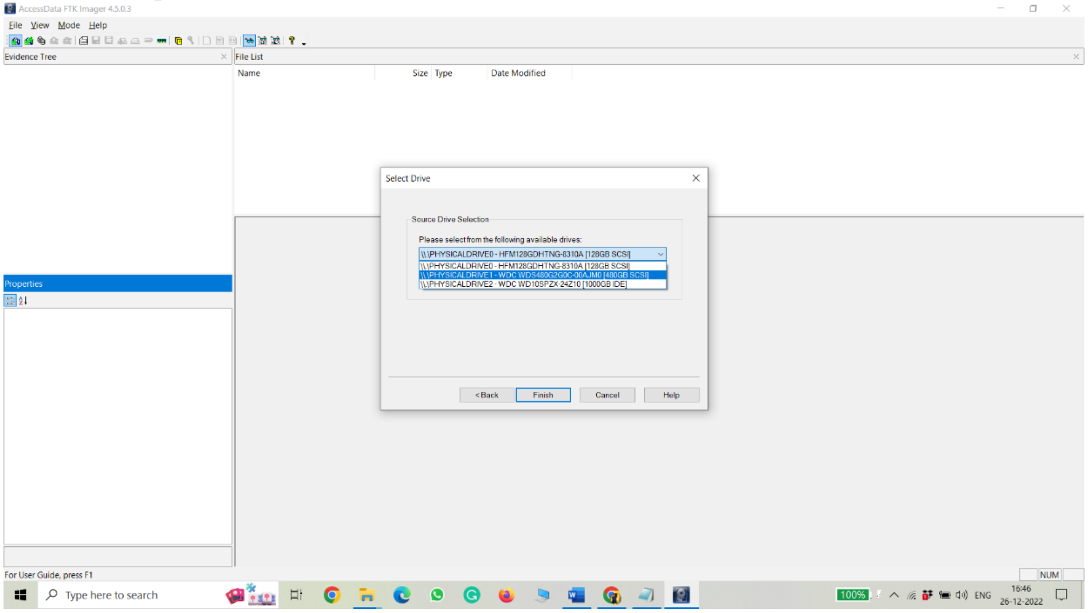
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Fig 1.4

3) Step 3: Select the name of drive



Select Drive

Source Drive Selection

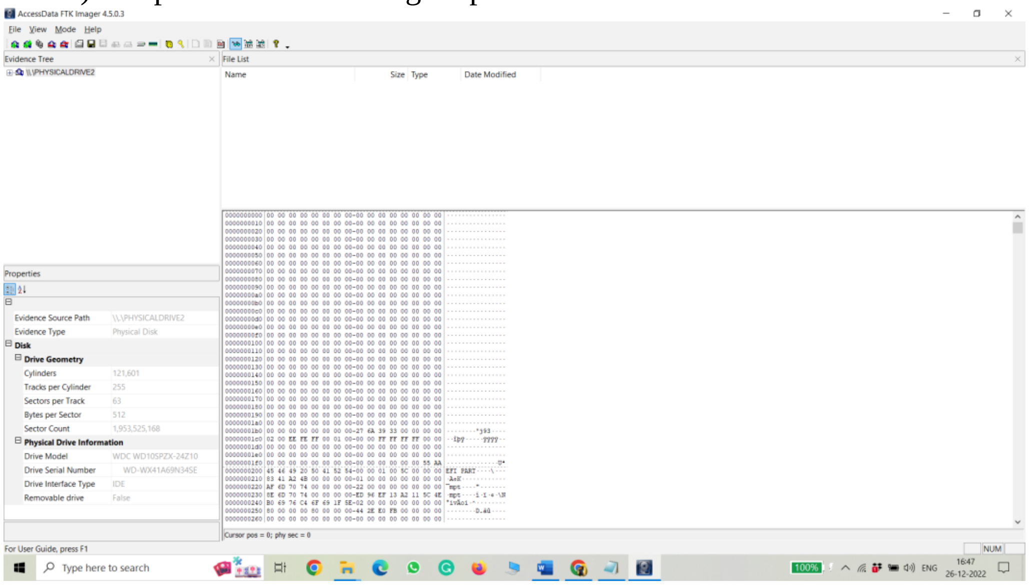
Please select from the following available drives:

\\.\PHYSICALDRIVE0 - HFM128GDHTNG-8310A [128GB SCSI]

\\.\PHYSICALDRIVE0 - HFM128GDHTNG-8310A [128GB SCSI]
\\.\PHYSICALDRIVE1 - WDC WDS480G2G0C-00AJM0 [480GB SCSI]
\\.\PHYSICALDRIVE2 - WDC WD10SPZX-24Z10 [1000GB IDE]

Fig 1.5

4) Step 4: The drive will get opened



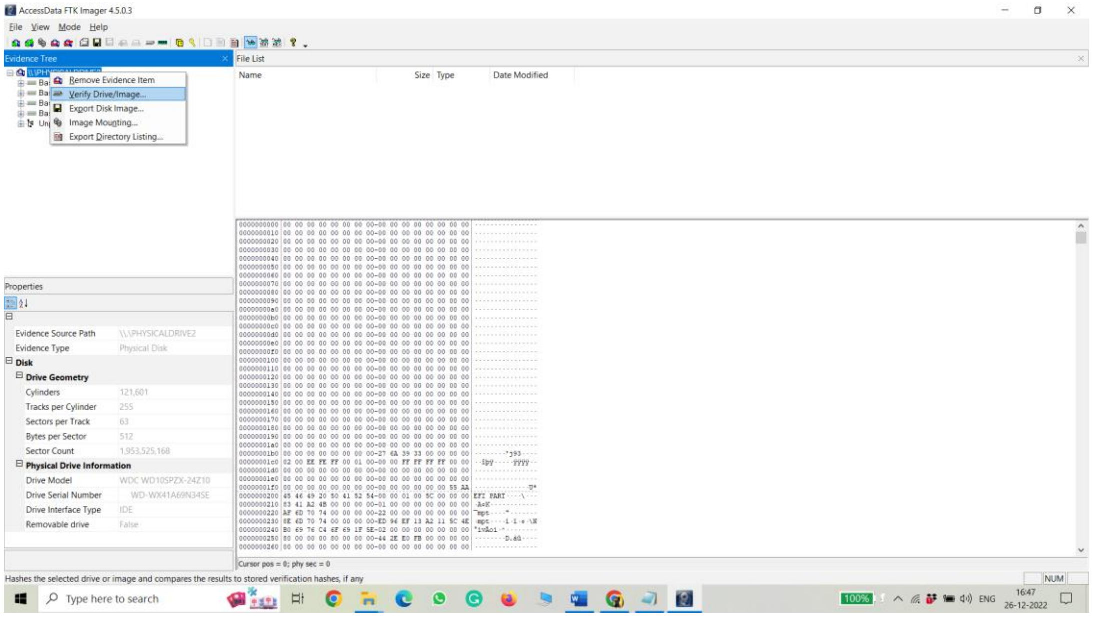
\\.\PHYSICALDRIVE2

Evidence Source Path	\\.\PHYSICALDRIVE2
Evidence Type	Physical Disk
Disk	
Drive Geometry	
Cylinders	121,601
Tracks per Cylinder	255
Sectors per Track	63
Bytes per Sector	512
Sector Count	1,953,525,168
Physical Drive Information	
Drive Model	WDC WD10SPZX-24Z10
Drive Serial Number	WD-WX41A69N34SE
Drive Interface Type	IDE
Removable drive	False

```
Cursor pos = 0; phy sec = 0
```

Fig 1.6

5) Step 5: Click on drive name and click on verify drive



Evidence Source Path	\\.\PHYSICALDRIVE2
Evidence Type	Physical Disk
Disk	
Drive Geometry	
Cylinders	121,601
Tracks per Cylinder	255
Sectors per Track	63
Bytes per Sector	512
Sector Count	1,953,525,168
Physical Drive Information	
Drive Model	WDC WD10SPZX-24Z10
Drive Serial Number	WD-WX41A69N34SE
Drive Interface Type	IDE
Removable drive	False

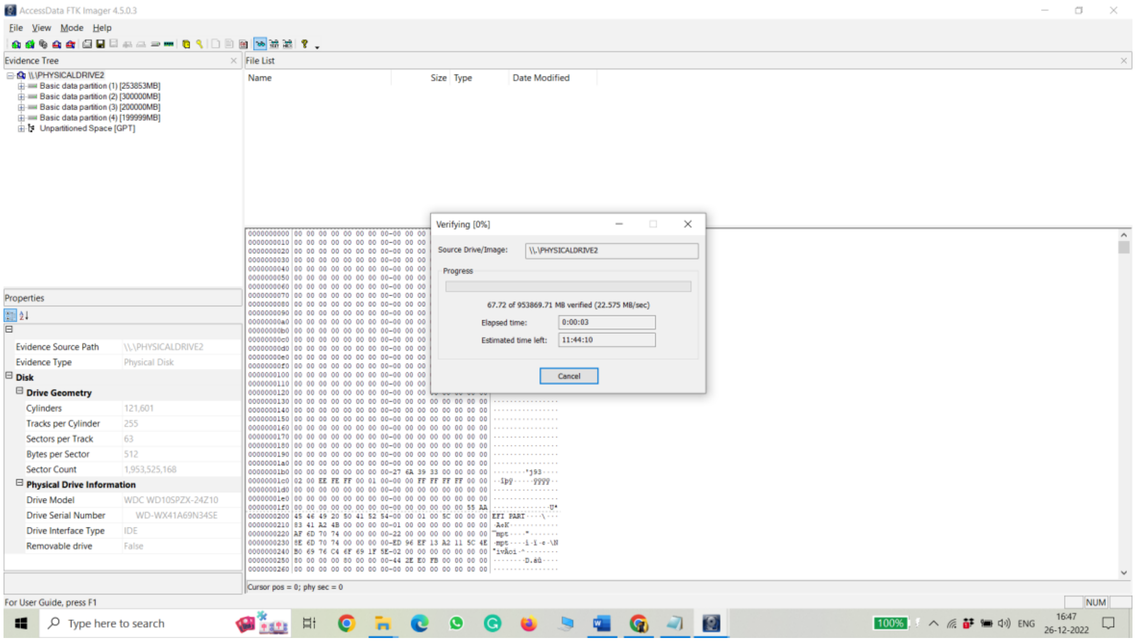
```
0000000000 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000001a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000001b0 00 00 00 00 00 00 00 00-27 6A 39 33 00 00 00 00 ········'j93····
00000001c0 02 00 EE FE FF 00 01 00-00 00 FF FF FF FF 00 00 ··îþÿ····ÿÿÿÿ··
00000001d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000001f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA ··············U*
0000000200 45 46 49 20 50 41 52 54-00 00 01 00 5C 00 00 00 EFI PART····\···
0000000210 83 41 A2 4B 00 00 00 00-01 00 00 00 00 00 00 00 ·A¢K············
0000000220 AF 6D 70 74 00 00 00 00-22 00 00 00 00 00 00 00 ¯mpt····"·······
0000000230 8E 6D 70 74 00 00 00 00-ED 96 EF 13 A2 11 5C 4E ·mpt····í·ï·¢·\N
0000000240 B0 69 76 C4 6F 69 1F 5E-02 00 00 00 00 00 00 00 °ivÄoi·^········
0000000250 80 00 00 00 80 00 00 00-44 2E E0 FB 00 00 00 00 ········D.àû····
0000000260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

Cursor pos = 0; phy sec = 0

Hashes the selected drive or image and compares the results to stored verification hashes, if any

Fig 1.7

6) Step 6: The drive will get started for Verification



\\.\PHYSICALDRIVE2
Basic data partition (1) [253853MB]
Basic data partition (2) [300000MB]
Basic data partition (3) [200000MB]
Basic data partition (4) [199999MB]
Unpartitioned Space [GPT]

Verifying [0%]

Source Drive/Image: \\.\PHYSICALDRIVE2

Progress

67.72 of 953869.71 MB verified (22.575 MB/sec)

Elapsed time: 0:00:03

Estimated time left: 11:44:10

Evidence Source Path	\\.\PHYSICALDRIVE2
Evidence Type	Physical Disk
Disk	
Drive Geometry	
Cylinders	121,601
Tracks per Cylinder	255
Sectors per Track	63
Bytes per Sector	512
Sector Count	1,953,525,168
Physical Drive Information	
Drive Model	WDC WD10SPZX-24Z10
Drive Serial Number	WD-WX41A69N34SE
Drive Interface Type	IDE
Removable drive	False

Cursor pos = 0; phy sec = 0

For User Guide, press F1

Fig 1.8

4.1.2 LOGICUBE TALON ULTIMATE

For use in the field or a measurable lab, the Talon® Extreme offers cutting edge, elite execution scientific imaging at a sensible expense. The Claw Extreme meets every one of your necessities for measurable imaging, hashing, and eradicating in light of the fact that it was made explicitly for advanced scientific agents. It flaunts a reduced plan, straightforward controls, and superb imaging speed..[11]

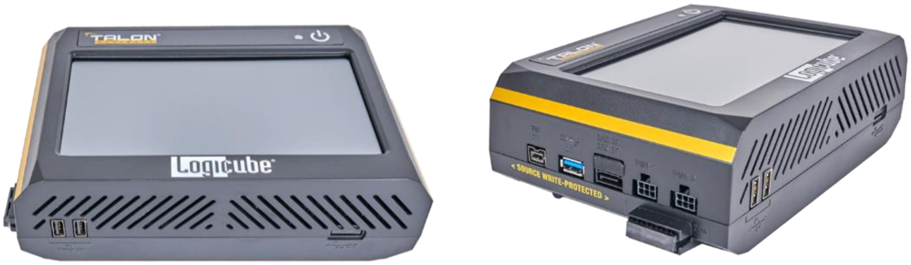


Fig 1.9

- The Talon® Extreme is a legal imaging arrangement that is unimaginably speedy, with paces of more than 40GB/min.

- Picture and confirm to an assortment of picture designs, including local copy,.dmg picture, e01 picture, and ex01 picture. The Claw Extreme offers unbelievably speedy validation utilizing SHA1, SHA256, and double hash (MD5+SHA1).

- Image+Verify Simultaneous. Simultaneous imaging and confirmation use objective hard drives that could be quicker than the source hard plate. It is feasible to cut the general picture handling time fifty.

- Utilizing pre-set, custom channels, document signature channels, as well as watchword look, the designated imaging/legitimate imaging device empowers you to make an intelligent picture by catching simply the important records. A MFT report might contain a rundown of records that could have been obliterated. It is feasible to yield information in L01, LX01, ZIP, or registry tree designs. Clients can peruse and see content straightforwardly on the Claw Extreme showcase or control and watch content on an organized Claw Extreme by utilizing an internet browser on their PC or work area, albeit this requires the Designated Imaging choice to be acquired.Drive Review for Compose Hindered. On the Claw Extreme, you can immediately review drive material. Intelligent admittance to source or objective drives associated with Claw Extreme is made conceivable through the record program capacity. The drive's allotments and content can be seen by clients.

- Strong state drives, as well as SATA/USB3/FireWire stockpiling gadgets, are upheld locally by the Claw Extreme. At the point when a product choice is bought, SAS gadgets are upheld. Claw Extreme accompanies a connector that upholds 2.5"/3.5" IDE drives. With discretionary connectors, PCIe, 1.8" IDE, 1.8" ZIF, mSATA, Miniature SATA, SATA, and streak drives are upheld.

- Usefulness of organization push. Push proof documents to an organization area from the Claw Extreme store or from objective circles associated with the Claw Extreme. A safer technique than essentially reordering to the investigation PC is given by the Push capability, which plays out a MD5 or SHA hash during the push method.

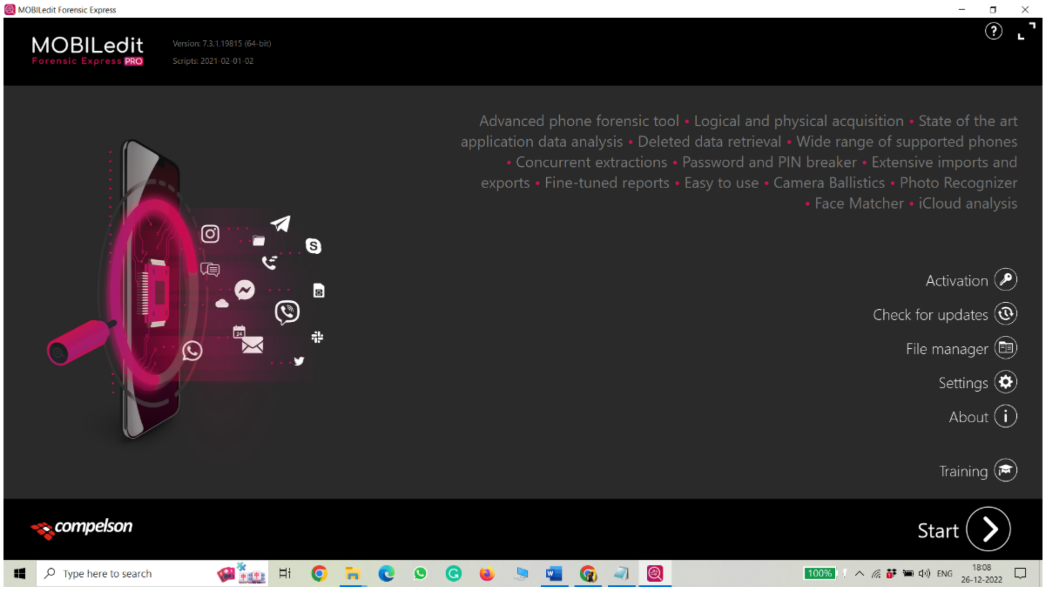
- Clients can catch from a Macintosh framework that is booted in target plate mode utilizing the FireWire connector. A post-retail Thunderclap to FW association is expected for Macintoshes having a Thunderclap connector. empowers the utilization of photographs shot with the MacBook Ace and Macintoshes with USB-C connections..[12]

4.1.3 MOBIL alter (Cell Phone Extraction)

MOBILedit Legal, a computerized criminology program from Compelson Labs, look, surveys, and creates provides details regarding information from GSM/C.DMA/laptops PDA gadgets. MOBILedit might interface with wireless gadgets through an Infrared (IR) port, a Bluetooth association, WiFi, or a link interface. After correspondence has been laid out, the telephone model is distinguished by the producer, model number, chronic number (IMEI), and a related picture of the gadget.

The MOBILedit stage inspects the items in the telephone through an organizer structure like to MS Viewpoint and is viable with various telephones and cell phones (a total rundown of upheld handsets is accessible on the producer's site). This empowers the reinforcement of information made stay on the line, its capacity on a PC, or its duplicating to another device.[13]

Step 1: Landing page of MOBILedit application. Click on the beginning button.



MOBILedit Forensic Express

MOBILedit Forensic Express PRO

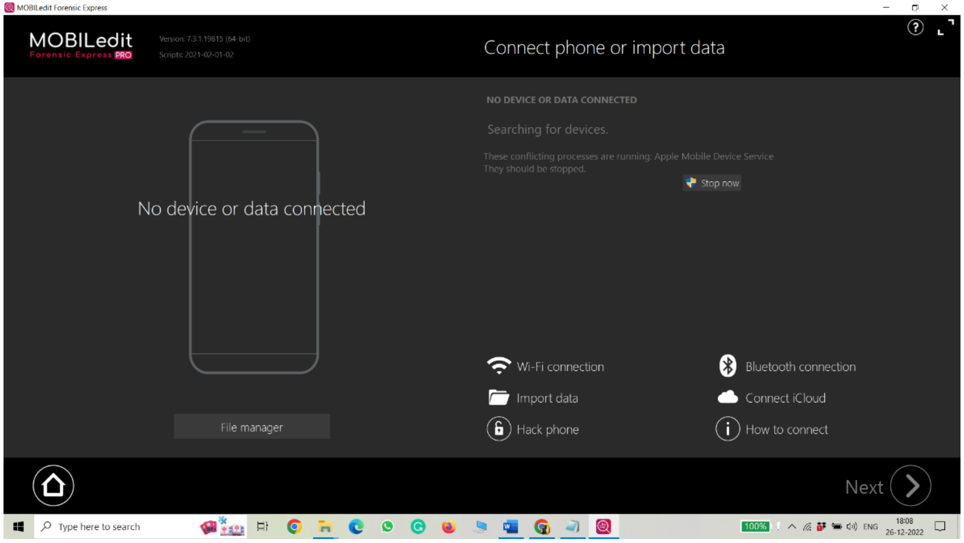
Version: 7.3.1.19815 (64-bit)

Scripts: 2021-02-01-02

Advanced phone forensic tool • Logical and physical acquisition • State of the art application data analysis • Deleted data retrieval • Wide range of supported phones • Concurrent extractions • Password and PIN breaker • Extensive imports and exports • Fine-tuned reports • Easy to use • Camera Ballistics • Photo Recognizer • Face Matcher • iCloud analysis

Fig 1.10

Step 2: Interface the Telephone,note(switch on the designer mode and USB investigating)



MOBILedit Forensic Express

MOBILedit Forensic Express PRO

Version: 7.3.1.19815 (64-bit)

Scripts: 2021-02-01-02

Connect phone or import data

NO DEVICE OR DATA CONNECTED

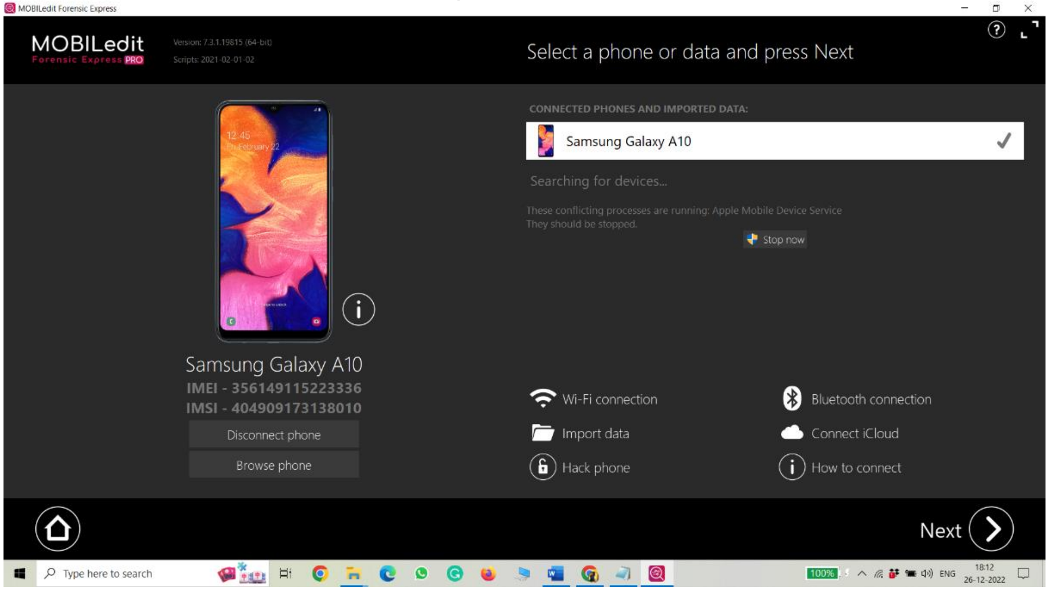
Searching for devices.

These conflicting processes are running: Apple Mobile Device Service
They should be stopped.

No device or data connected

Fig 1.11

Step 3: The telephone will be distinguished and subtleties of the telephone will be shown.



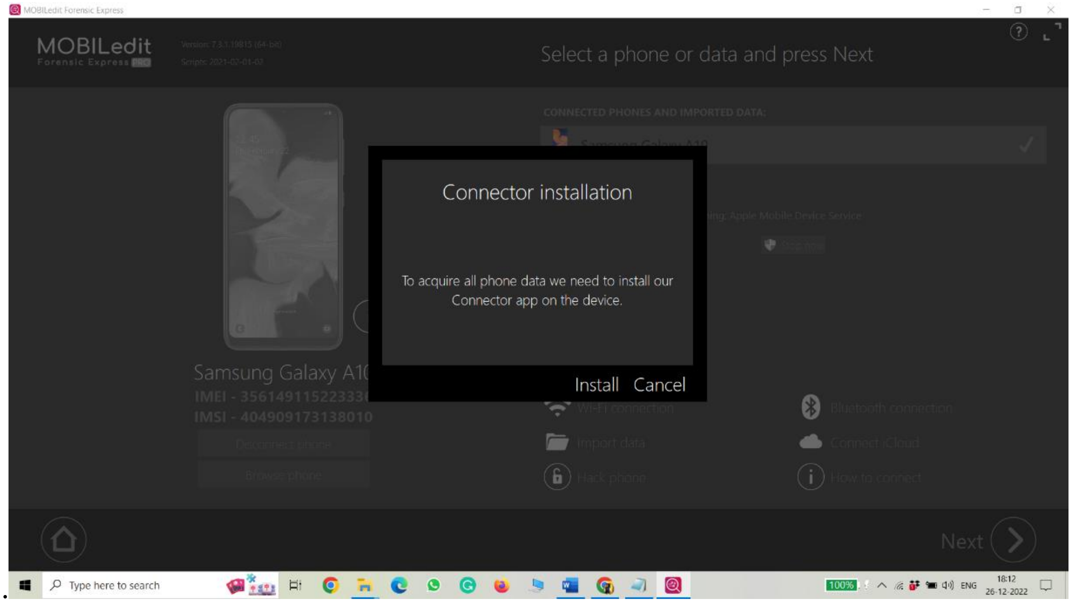
Searching for devices...

These conflicting processes are running: Apple Mobile Device Service
They should be stopped.

Samsung Galaxy A10
IMEI - 356149115223336
IMSI - 404909173138010

Fig 1.12

Step 4: Presently it will show a popup for introducing a legal connector on the telephone click on introduce.

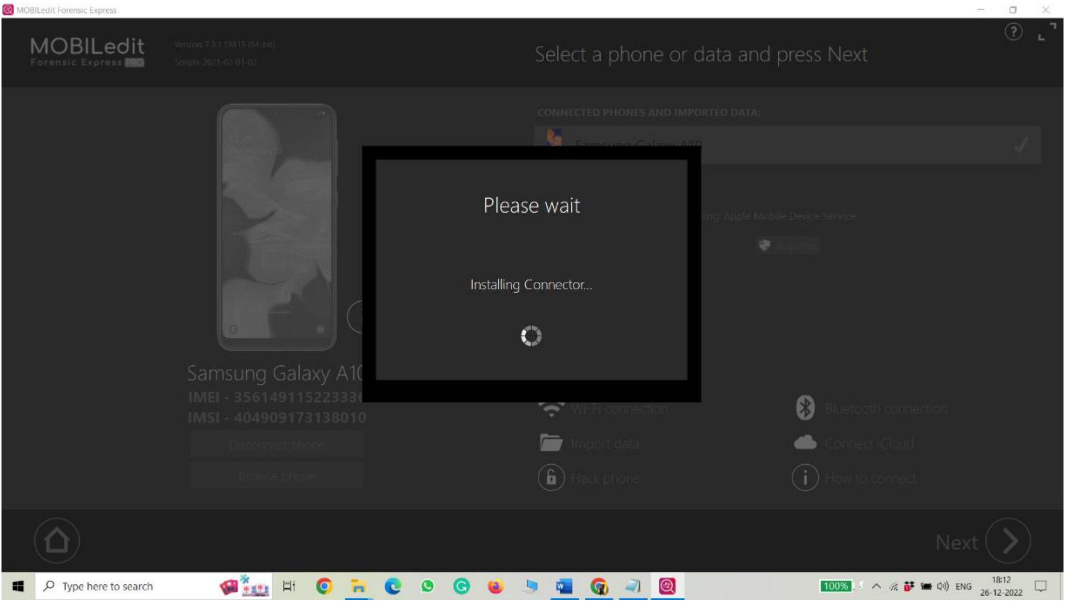


Connector installation

To acquire all phone data we need to install our Connector app on the device.

Fig 1.13

Step 5: Presently the scientific connector will be introduced stand by till the connector is introduced



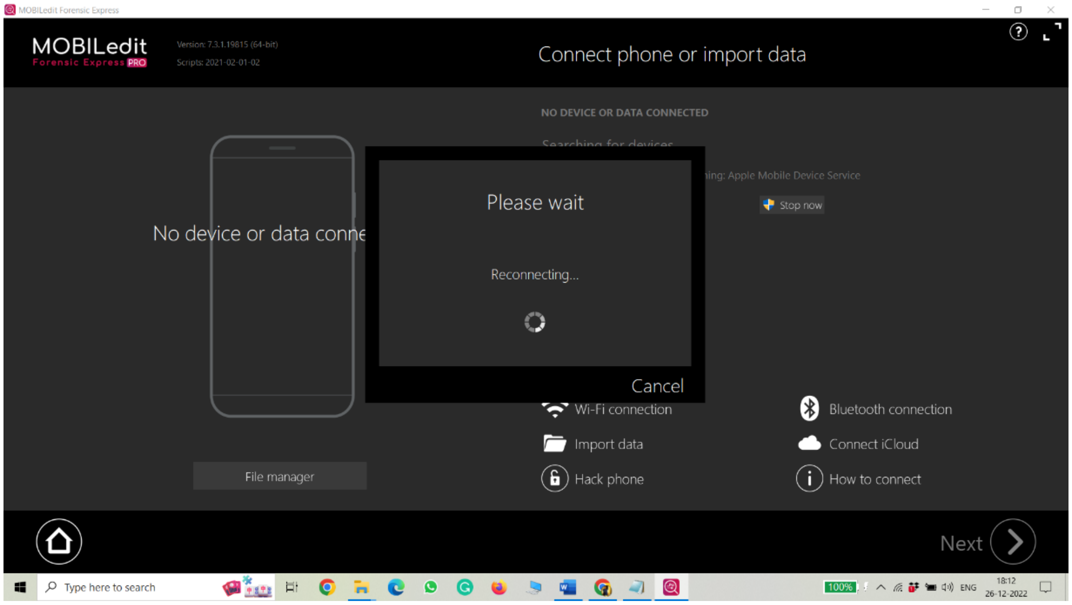
Select a phone or data and press Next

Please wait

Installing Connector...

Fig 1.14

Step 6: Presently it will be reconnected subsequent to giving admittance to all on telephone for measurable connector



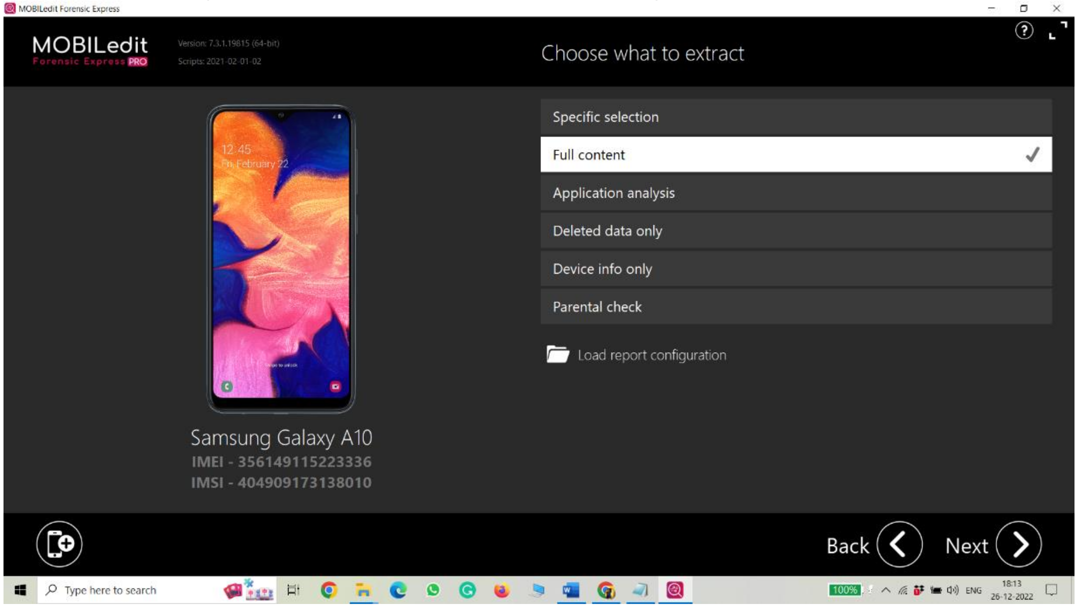
Connect phone or import data

Please wait

Reconnecting...

Fig 1.15

Step 7: Presently we need to pick what we precisely need to separate.



Choose what to extract

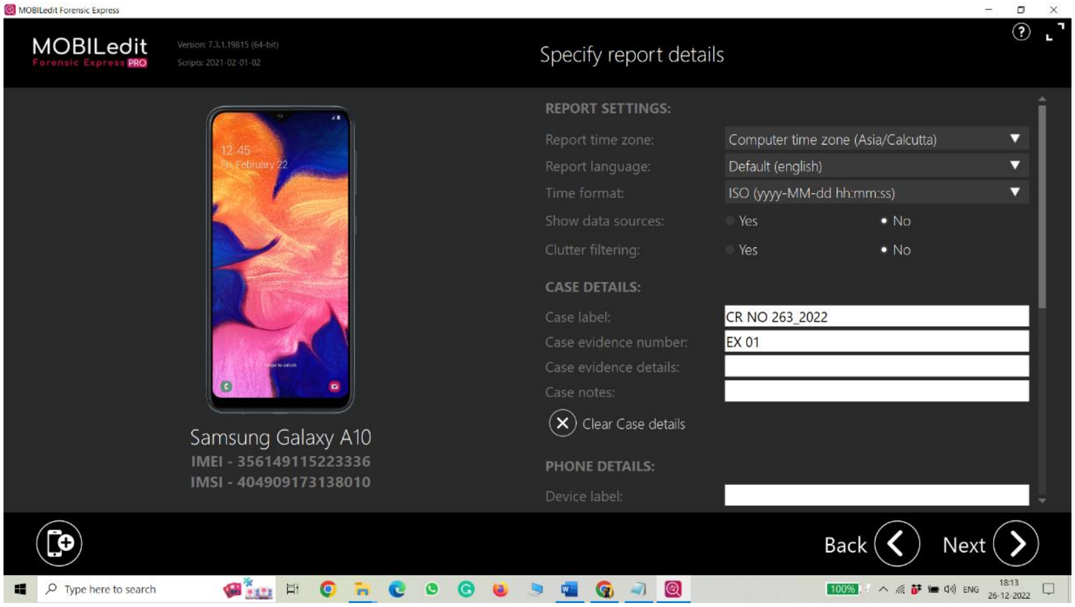
- Specific selection
- Full content ✓
- Application analysis
- Deleted data only
- Device info only
- Parental check

Load report configuration

Samsung Galaxy A10
IMEI - 356149115223336
IMSI - 404909173138010

Fig 1.16

Step 8: Presently enter the subtleties as asked underneath. Presently enter the subtleties as asked underneath.



Specify report details

REPORT SETTINGS:

Report time zone: Computer time zone (Asia/Calcutta)
Report language: Default (english)
Time format: ISO (yyyy-MM-dd hh:mm:ss)
Show data sources: ○ Yes ● No
Clutter filtering: ○ Yes ● No

CASE DETAILS:

Case label: CR NO 263_2022
Case evidence number: EX 01
Case evidence details:
Case notes:

Clear Case details

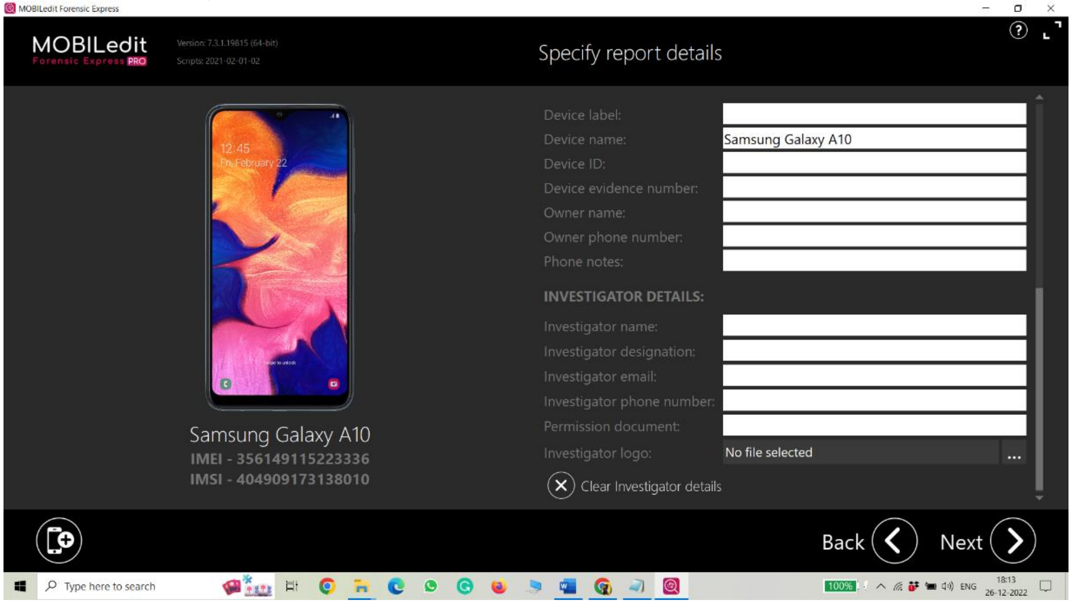
PHONE DETAILS:

Device label:

Samsung Galaxy A10
IMEI - 356149115223336
IMSI - 404909173138010

Fig 1.17

Step 9: Presently enter the subtleties as asked beneath.



Specify report details

Device label:
Device name: Samsung Galaxy A10
Device ID:
Device evidence number:
Owner name:
Owner phone number:
Phone notes:

INVESTIGATOR DETAILS:

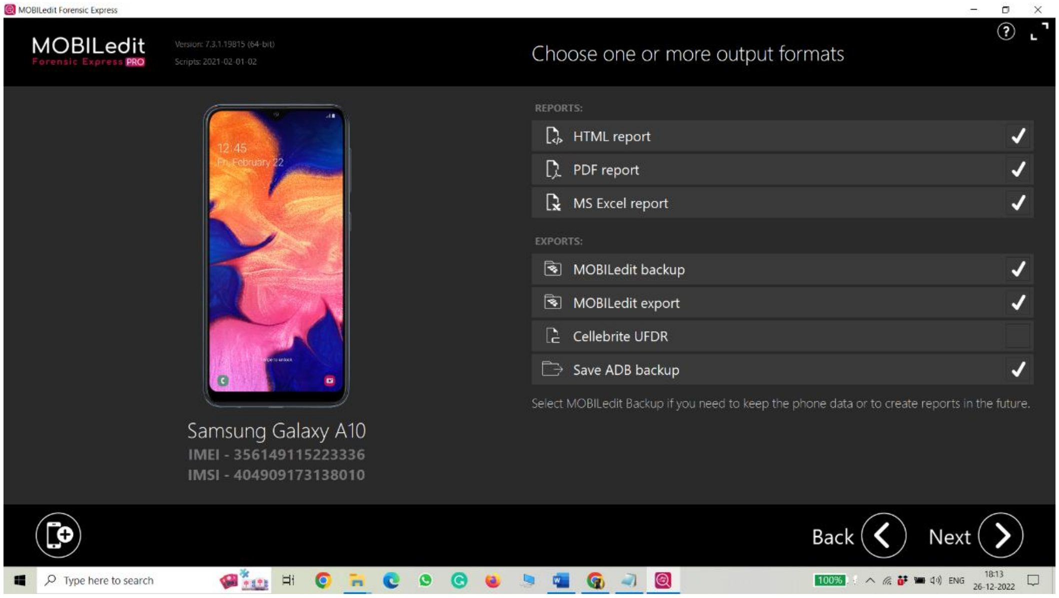
Investigator name:
Investigator designation:
Investigator email:
Investigator phone number:
Permission document:
Investigator logo: No file selected

Clear Investigator details

Samsung Galaxy A10
IMEI - 356149115223336
IMSI - 404909173138010

Fig 1.18

Step 10: Presently pick the report design in which design you need the report.



Choose one or more output formats

REPORTS:

- HTML report ✓
- PDF report ✓
- MS Excel report ✓

EXPORTS:

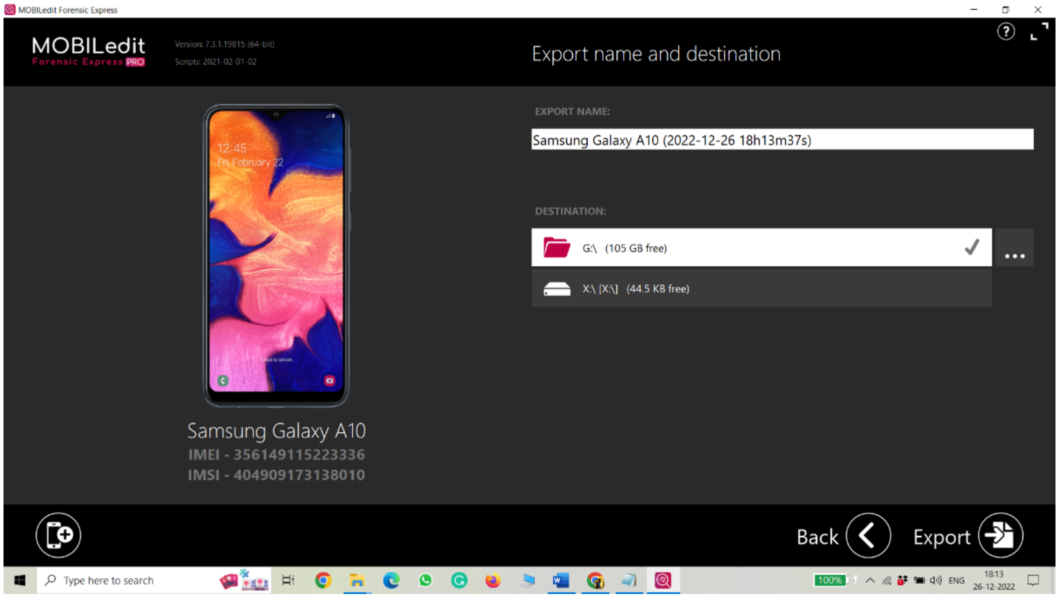
- MOBILedit backup ✓
- MOBILedit export ✓
- Cellebrite UFDR □
- Save ADB backup ✓

Select MOBILedit Backup if you need to keep the phone data or to create reports in the future.

Samsung Galaxy A10
IMEI - 356149115223336
IMSI - 404909173138010

Fig 1.19

Step 11: Presently give the objective according to required.



Export name and destination

EXPORT NAME: Samsung Galaxy A10 (2022-12-26 18h13m37s)

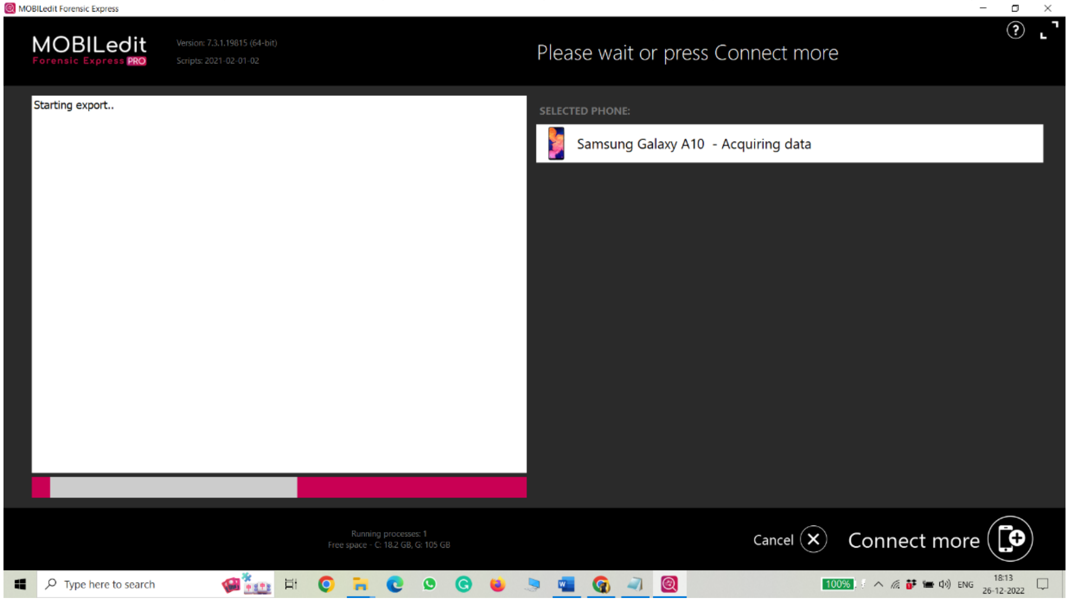
DESTINATION:

- G:\ (105 GB free) ✓
- X:\ [X:\] (44.5 KB free)

Samsung Galaxy A10
IMEI - 356149115223336
IMSI - 404909173138010

Fig 1.20

Step 12: Presently the sending out will begin to stand by till the total trading.



Please wait or press Connect more

Starting export..

SELECTED PHONE: Samsung Galaxy A10 - Acquiring data

Running processes: 1
Free space - C: 18.2 GB, G: 105 GB

Fig 1.21

Last however not the leas, telephones will be traded to the given objective. We can get to the report in the wake of finishing the extraction.

4.1.4 Cellebrite UFED (Mobile Phone Extraction)

Law enforcement organisations employ the UFED (Universal Forensics Extraction Device), a product line from the Israeli business Cellebrite, to extract and analyse data from mobile devices.[14]

Features:

You can select data extraction on the UFED Touch and pick a vendor from a long list. After the data has been extracted, the Physical Analyzer application can be used to analyse the data.

The following functionalities are supported by the Cellebrite UFED Physical Analyzer:

- Extract device keys that can be used to decode keychain objects and raw disc images.

- Disclose device passwords, albeit not all locked devices support this;

Attacks that recover passwords

• Decoding and analysing application data; • Producing reports in several forms, such as PDF and HTML; • Dumping the raw filesystem for use in other programmes' analysis.

For practically any phone, GPS, or tablet, it has more than 100 different cables. Additionally, the system can support more than 7,700 tested devices, and it keeps its list up to date. Furthermore, UFED supports over 3,000 ripoff phones. A robust carrying case designed for usage in the field is included with UFED. The product has a broad range of device auto-detection capabilities. When an apparatus is found, UFED dumps its contents onto a linked PC or USB device. The PC features a reporting application that formats the dumped assets into a helpful report and is free to use.[15]

Steps for connecting & Exporting Phones:

Step 1: Home page of cellebrite UFED application.

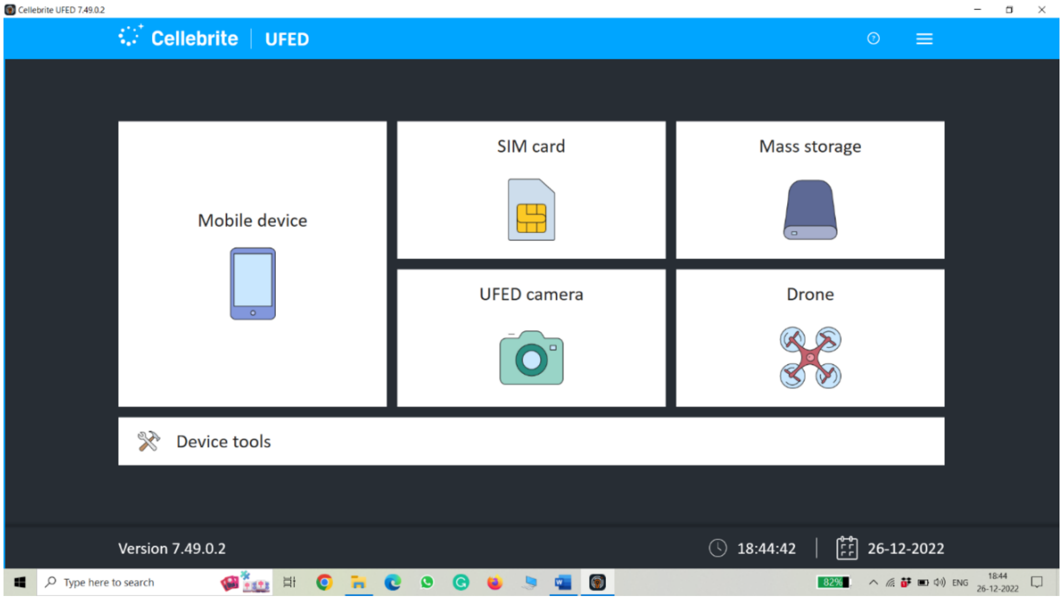
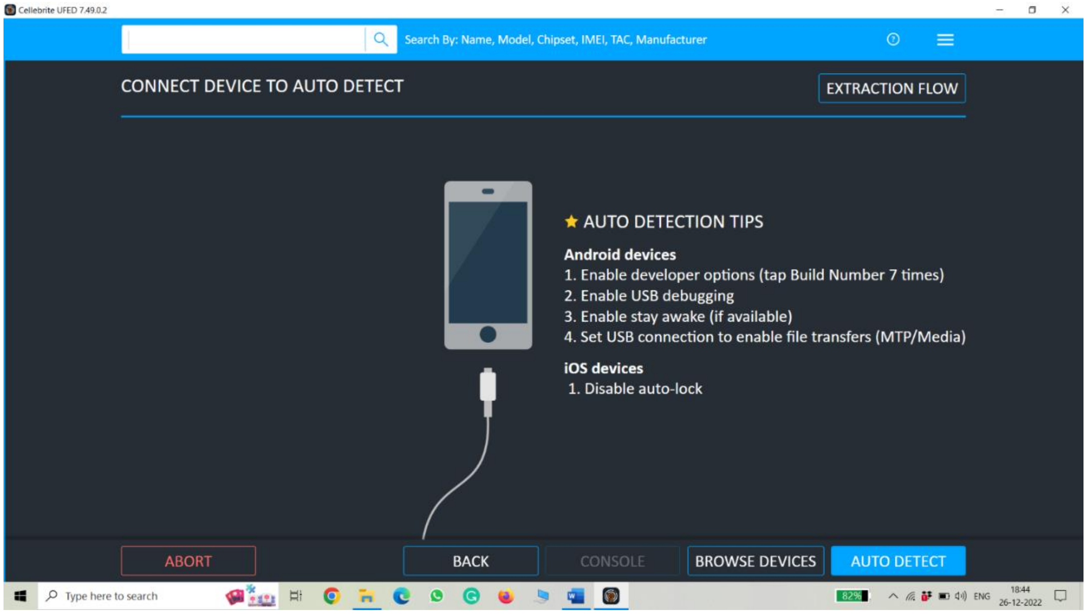


Fig 1.22

Step 2: Connecting device, note (Developer mode & USB debugging should be on)



★ AUTO DETECTION TIPS

Android devices
1. Enable developer options (tap Build Number 7 times)
2. Enable USB debugging
3. Enable stay awake (if available)
4. Set USB connection to enable file transfers (MTP/Media)

iOS devices
1. Disable auto-lock

Fig 1.23

Step 3: Connect the device manually. In these, we can select the device we want to export but, first, we have to check whether the device is available for which we have to export.

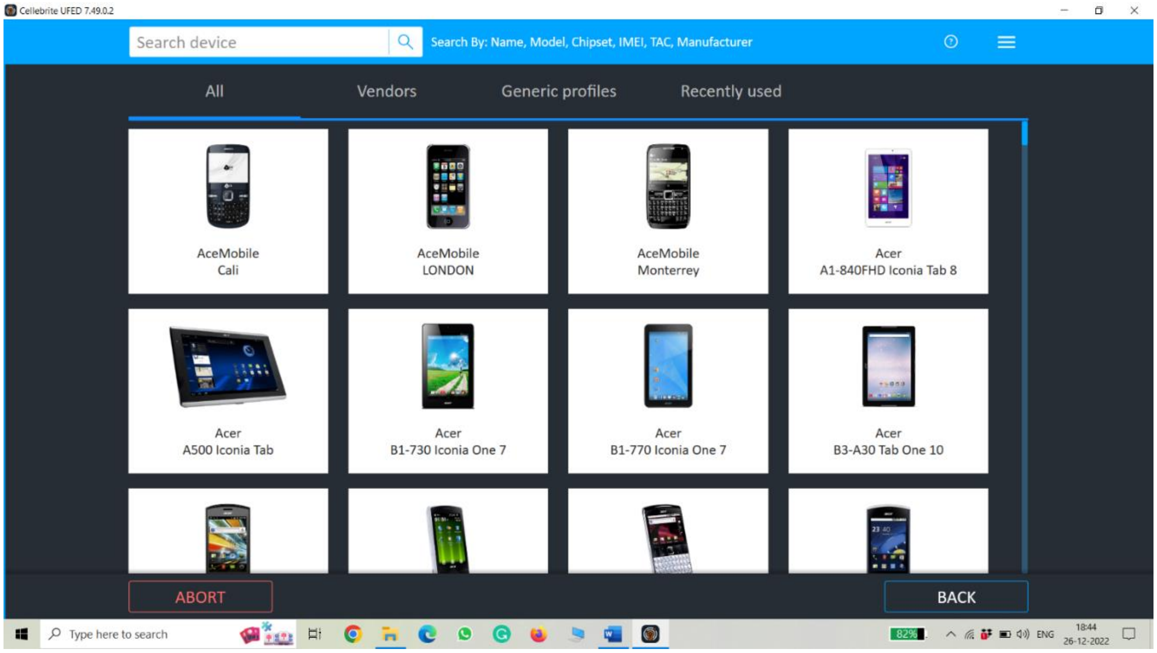
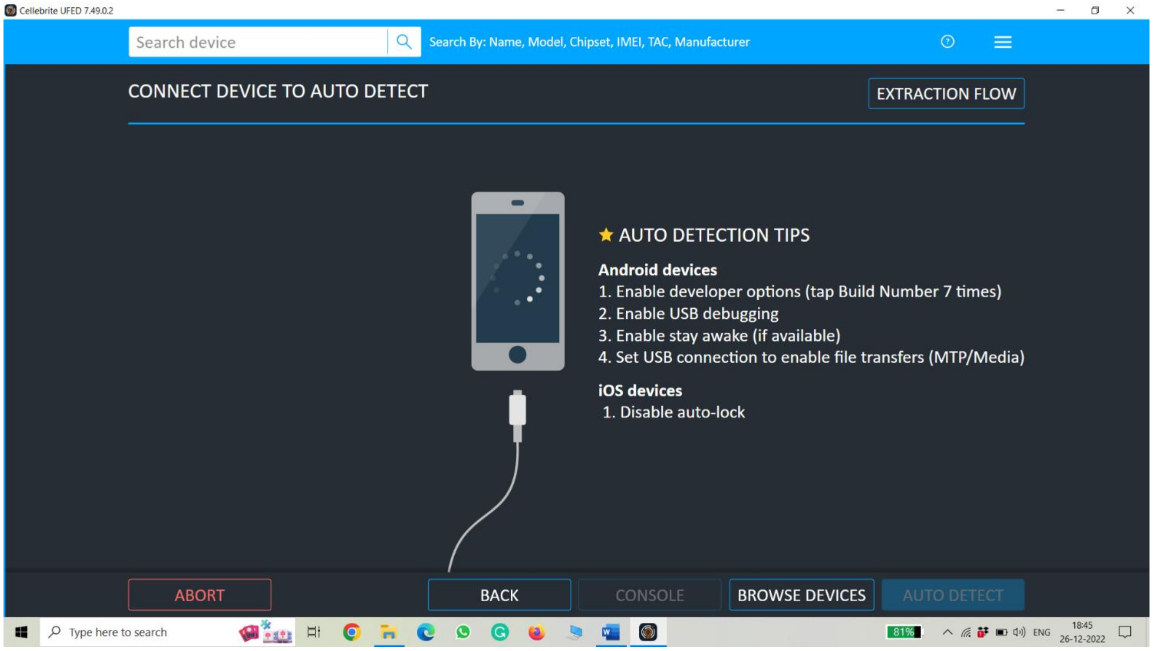


Fig 1.24

Step 4: If the device is not available we can Auto Detect the device by choosing the auto-detect option.


Cellebrite UFED 7.49.0.2
Search device
Search By: Name, Model, Chipset, IMEI, TAC, Manufacturer
CONNECT DEVICE TO AUTO DETECT
EXTRACTION FLOW

★ AUTO DETECTION TIPS

Android devices

1. Enable developer options (tap Build Number 7 times)
2. Enable USB debugging
3. Enable stay awake (if available)
4. Set USB connection to enable file transfers (MTP/Media)

iOS devices

1. Disable auto-lock

Fig 1.25

4.2 UNIQUE TOOLS

4.2.1 BROWSER FORENSICS

Software programmes known as "browser forensics tools" are made expressly to extract and examine data from online browsers. To gather and examine data pertaining to cybercrimes and computer abuse, they are utilised in digital forensics investigations. The tools can be used to find information about a suspect's browser history, search queries, download history, cookies, and passwords.

A web browser's cache, history files, bookmarks, and cookies are just a few of the data storage sites that must be examined as part of the data collection process. Data is extracted from these storage locations and organised for easier analysis by investigators using the browser forensics tool.

The ability to examine browser-related artefacts such web artefacts, cookie data, and password data is another feature offered by some browser forensics tools. Web artefacts are files that are downloaded or uploaded via a web browser, whereas cookie data are tiny bits of information that a website stores on a user's machine. The term "password data" describes the login information that the browser saves for various websites.

All things considered, browser forensics tools are essential in the field of digital forensics and can assist investigators in gathering and analysing crucial data relating to cybercrimes and computer abuse. These tools give investigators a better grasp of a suspect's surfing habits and can support their case by supplying data that can be utilised in court.

SOURCE CODE:-

```
REM Create a folder to store the forensic data
md C:\Forensic_Data

REM Google Chrome Forensics

REM Copy the Chrome user data folder
xcopy "C:\Users\%username%\AppData\Local\Google\Chrome\User Data" "C:\Forensic_Data\Chrome_User_Data" /E /I /C /H /R /K /Y

REM Export the browser history
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://history" > "C:\Forensic_Data\Chrome_History.txt"

REM Export the bookmarks
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://bookmarks" > "C:\Forensic_Data\Chrome_Bookmarks.txt"

REM Export the cookies
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://settings/cookies" > "C:\Forensic_Data\Chrome_Cookies.txt"

REM Export the extensions
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --
```

```
disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://extensions" > "C:\Forensic_Data\Chrome_Extensions.txt"

REM Export the login data
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://settings/passwords" > "C:\Forensic_Data\Chrome_Login_Data.txt"

REM Export the search history
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://history/search" > "C:\Forensic_Data\Chrome_Search_History.txt"

REM Export the download history
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://downloads" > "C:\Forensic_Data\Chrome_Download_History.txt"

REM Export the cache
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-extensions --disable-popup-blocking --bwsi --enable-logging --log-level=0 --v1-logging --user-data-dir="C:\Forensic_Data\Chrome_User_Data" "chrome://cache" > "C:\Forensic_Data\Chrome_Cache.txt"

REM Export the autofill data
"C
```

Steps for Extracting Browsers:-

Insert the Pendrive having tool To Victims Computer or Laptop

Step 1 – Double Click On Tool

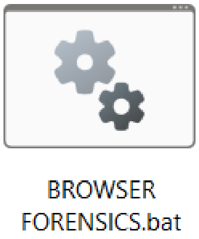
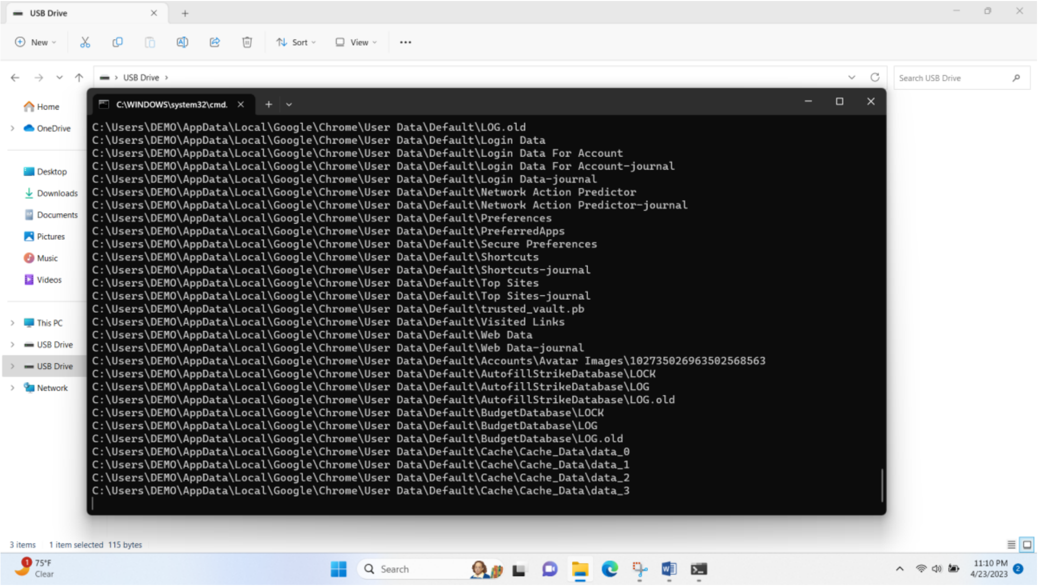


Fig 1.26

Step 2 – Script will run Automatically (Browser Forensics Started) Wait for result



```
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\LOG.old
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Login Data
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account-journal
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Login Data-journal
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Preferences
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\PreferredApps
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Shortcuts
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Shortcuts-journal
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Top Sites
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Top Sites-journal
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Visited Links
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Web Data
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Accounts\Avatar Images\102735026963502568563
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOCK
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOCK
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_0
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_1
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_2
C:\Users\DEMO\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\data_3
```

Fig 1.27

Step 3 –After Script Complition Chrome Folder Appear

Fig 1.28

Step 4 – Check User Data Folder in Chrome Folder

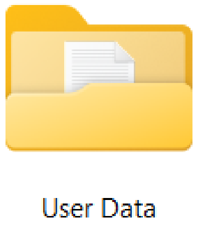


Fig 1.29

Step 5 – Unplug Pendrive from victims computer and insert it to our computer Then go to This PC & Local Disk (C:)

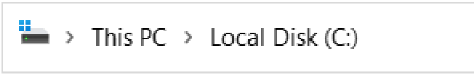


Fig 1.30

Step 6- Go to Users In Local Disk (C:)

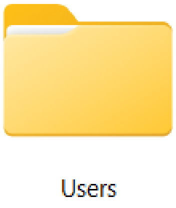


Fig 1.31

Step 7 – Select User in our Laptop

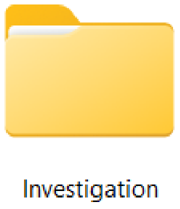
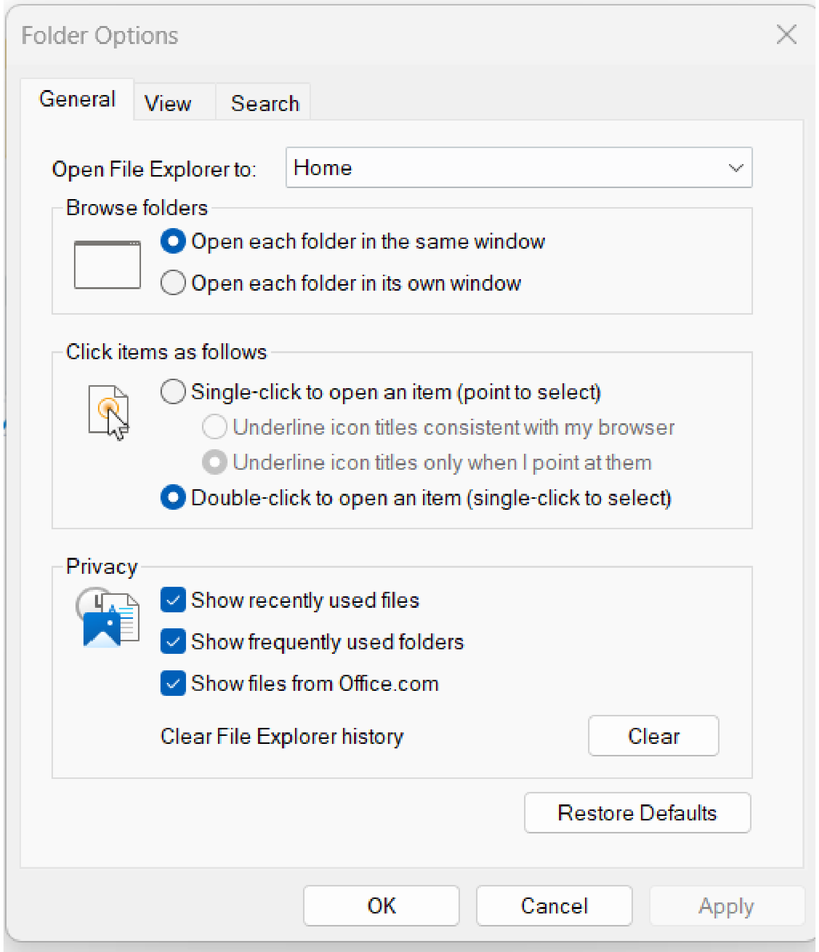


Fig 1.32

Step 8- Go to option setting



Folder Options

General | View | Search

Open File Explorer to: Home

Browse folders

● Open each folder in the same window

○ Open each folder in its own window

Click items as follows

○ Single-click to open an item (point to select)

○ Underline icon titles consistent with my browser

○ Underline icon titles only when I point at them

● Double-click to open an item (single-click to select)

Privacy

☑ Show recently used files

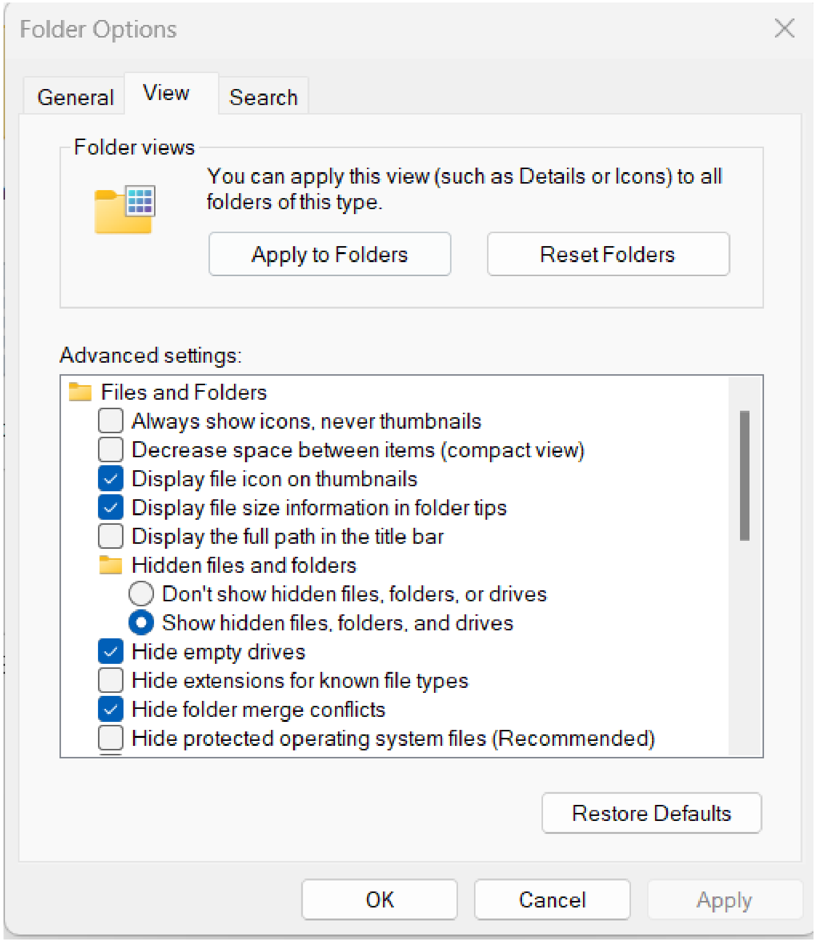
☑ Show frequently used folders

☑ Show files from Office.com

Clear File Explorer history

Fig 1.33

Step 9- Click on View And ON the all Hidden Options



Folder Options

General | View | Search

Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

Apply to Folders | Reset Folders

Advanced settings:

- Files and Folders
  - □ Always show icons, never thumbnails
  - □ Decrease space between items (compact view)
  - ☑ Display file icon on thumbnails
  - ☑ Display file size information in folder tips
  - □ Display the full path in the title bar
  - Hidden files and folders
    - ○ Don't show hidden files, folders, or drives
    - ● Show hidden files, folders, and drives
  - ☑ Hide empty drives
  - □ Hide extensions for known file types
  - ☑ Hide folder merge conflicts
  - □ Hide protected operating system files (Recommended)

Restore Defaults

OK | Cancel | Apply

Fig 1.34

Step10- Go to App Data Folder Which was hidden

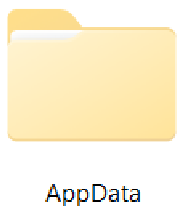


Fig 1.35

Step11- Click on Local

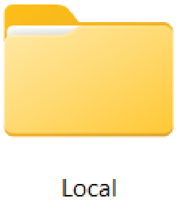


Fig 1.36

Step12- Click on Google

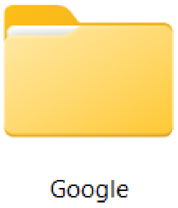


Fig 1.37

Step13- Click On Chrome

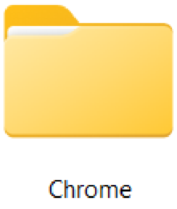


Fig 1.38

Step14- Delete the User data file

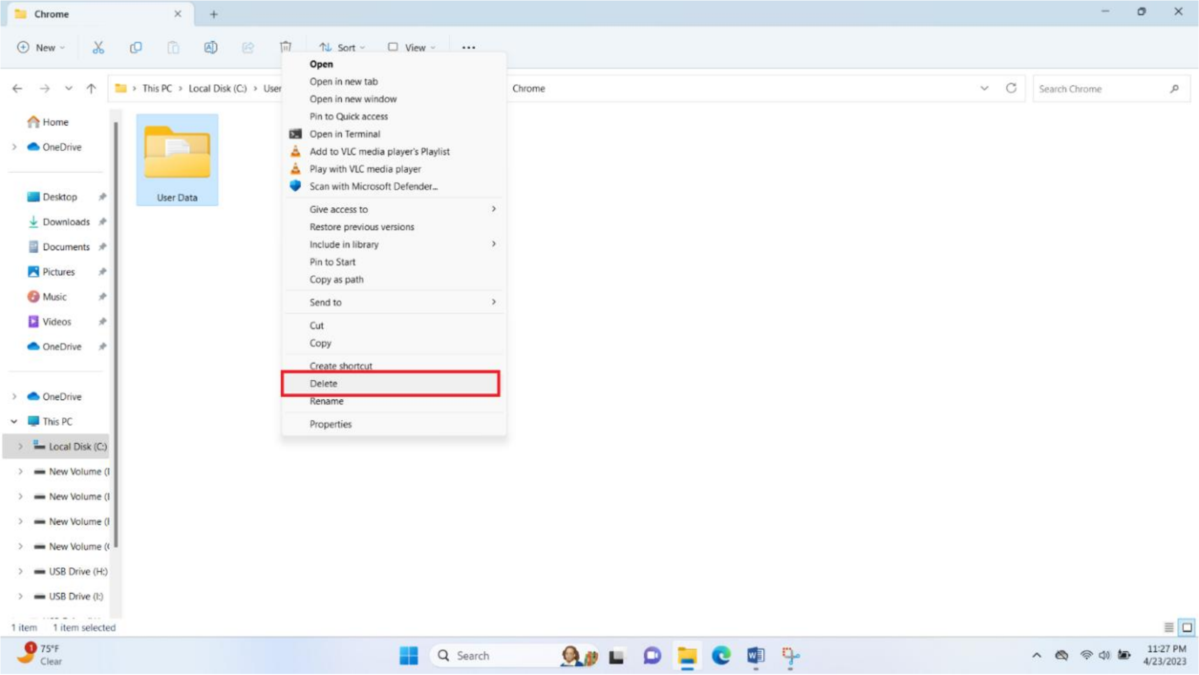


Fig 1.39

Step15- - Get Back Pendrive

Fig 1.40

Step16- - Open Chrome Folder

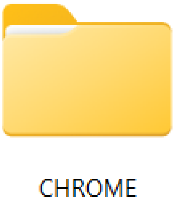


Fig 1.41

Step 17- Cut the User data file

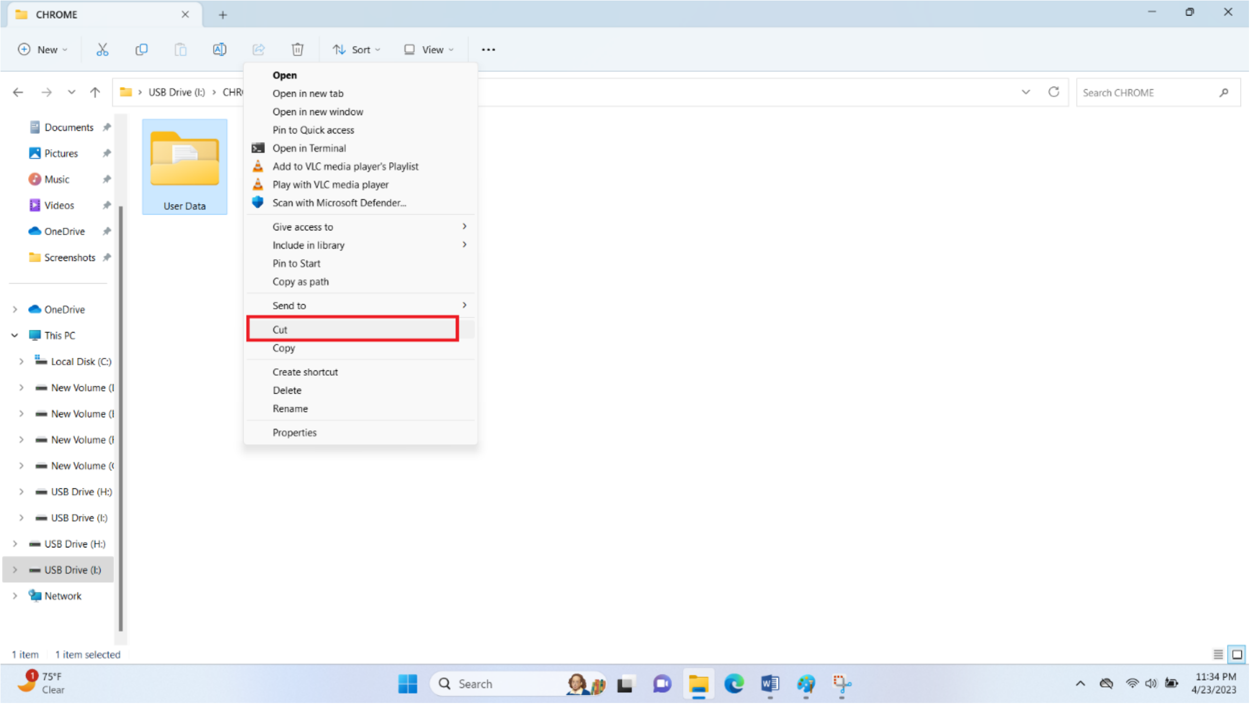
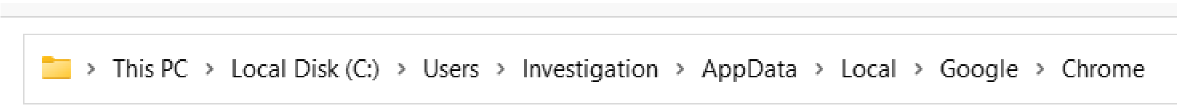


Fig 1.42

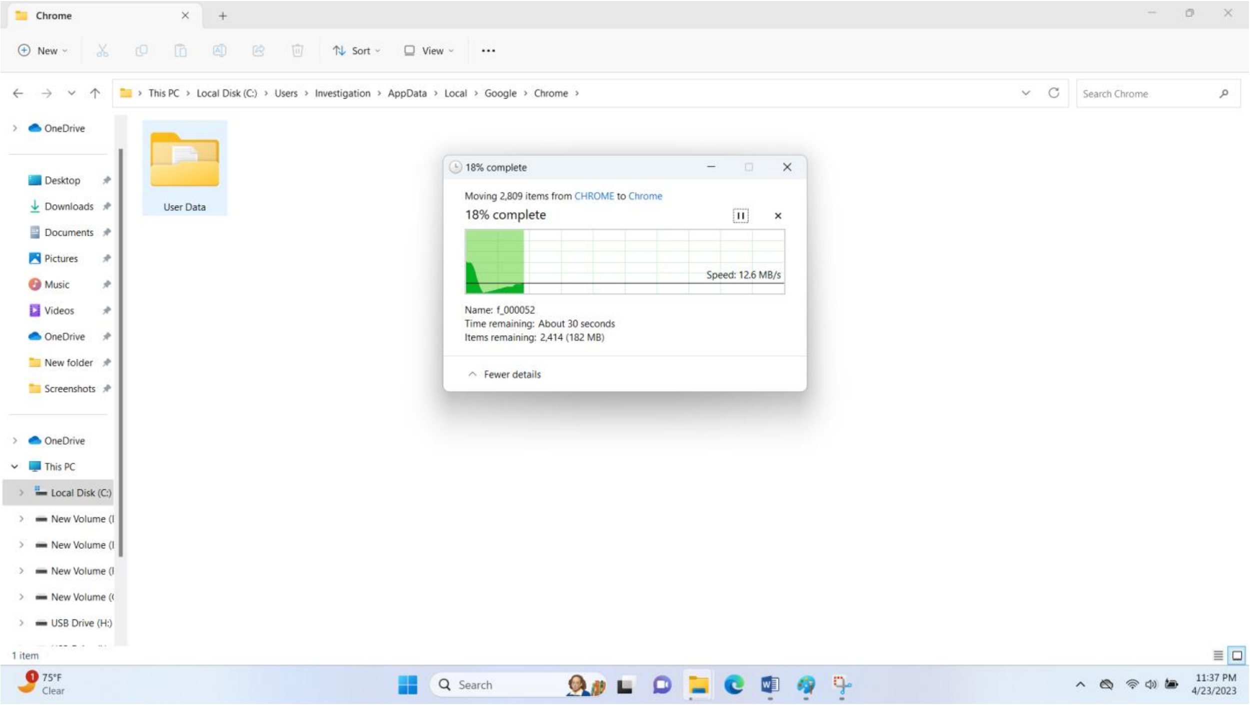
Step 18 - Get back from Pendrive and Go To Chrome As shown below



> This PC > Local Disk (C:) > Users > Investigation > AppData > Local > Google > Chrome

Fig 1.43

Step19- - Paste The User Data folder In Chrome



18% complete

Moving 2,809 items from CHROME to Chrome

18% complete

Speed: 12.6 MB/s

Name: f_000052

Time remaining: About 30 seconds

Items remaining: 2,414 (182 MB)

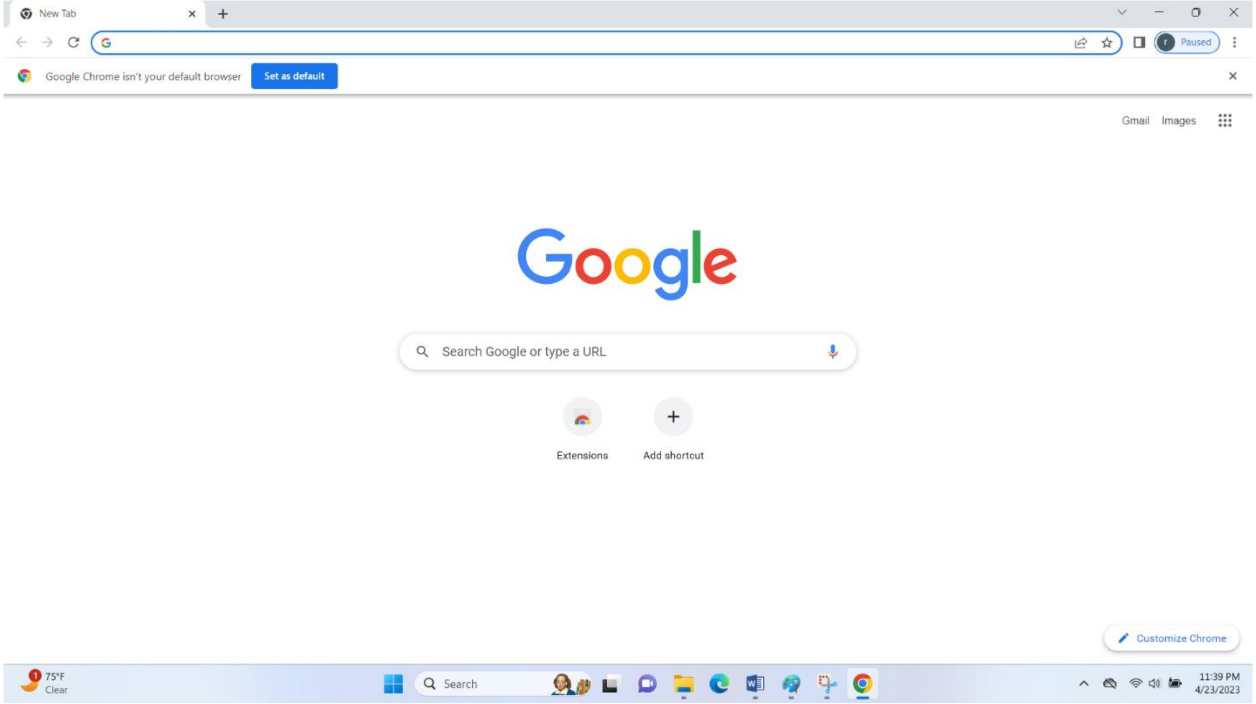
Fewer details

Fig 1.44

Step20- Come on main Desktop And Open the Chrome

Fig 1.45

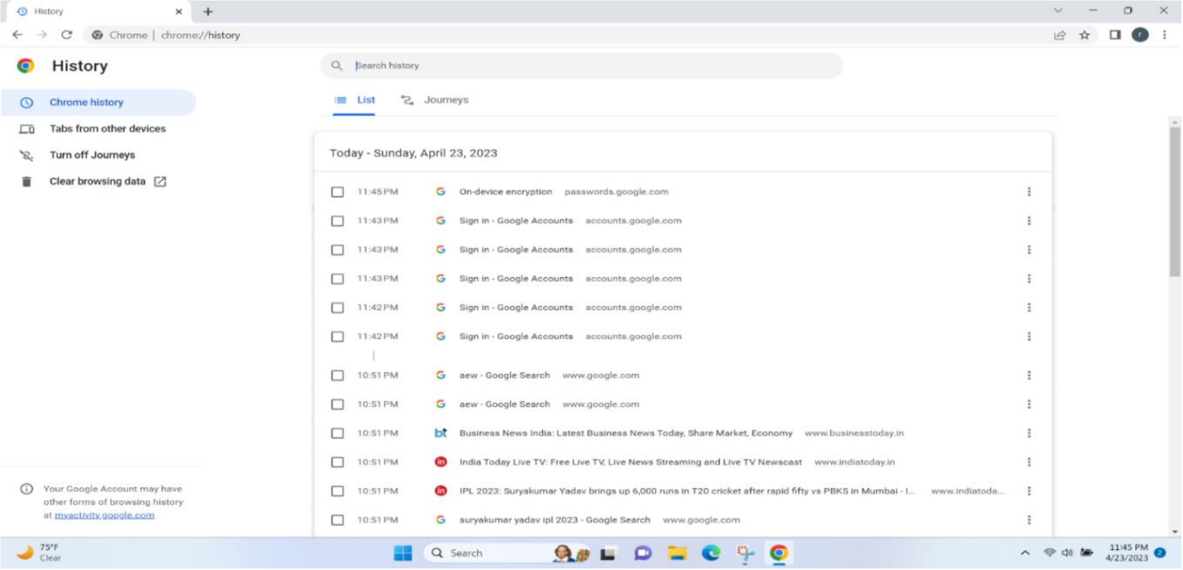
Step21- The Victims Chrome (Browser) Appears on Our Desktop



Google Chrome isn't your default browser

Fig 1.46

Step22- We can See Victims History, Cache, Extentions Etc



Today - Sunday, April 23, 2023

11:45 PM	On-device encryption	passwords.google.com
11:43 PM	Sign in - Google Accounts	accounts.google.com
11:43 PM	Sign in - Google Accounts	accounts.google.com
11:43 PM	Sign in - Google Accounts	accounts.google.com
11:42 PM	Sign in - Google Accounts	accounts.google.com
11:42 PM	Sign in - Google Accounts	accounts.google.com
10:51 PM	aew - Google Search	www.google.com
10:51 PM	aew - Google Search	www.google.com
10:51 PM	Business News India: Latest Business News Today, Share Market, Economy	www.businesstoday.in
10:51 PM	India Today Live TV: Free Live TV, Live News Streaming and Live TV Newscast	www.indiatoday.in
10:51 PM	IPL 2023: Suryakumar Yadav brings up 6,000 runs in T20 cricket after rapid fifty vs PBKS in Mumbai - I...	www.indiatoda...
10:51 PM	suryakumar yadav ipl 2023 - Google Search	www.google.com

Your Google Account may have other forms of browsing history at myactivity.google.com

Fig 1.

CHAPTER 5

RESULTS AND DISCUSSION

The writing audit uncovers that cloning, data recuperation, and steganography are imperative methods for advanced criminology examiners to gather and break down computerized proof really. Nonetheless, the concentrate similarly distinguishes difficulties and limitations, similar to the requirement for exact and powerful data recuperation methods, and the difficulties presented by steganography strategies in revealing secret data. The undertaking group has proposed deals with serious consequences regarding these hardships, including the utilization of cutting edge cloning strategies, data recuperation computations, and steganalysis techniques. These courses of action intend to improve the effectiveness and dependability of computerized legal sciences examinations and add to the general progression of the field. Given timetable as it were. Assume, In the event that the designer can't tackle the question, the question gets given to the next architect of a similar specialization. Other architect of a similar specialization brings down crafted by settling the question which is unsettled.

Moreover, organizations between advanced criminology examiners and industry pioneers can assist with the creation and use of new strategies and instruments. since a consequence of this organization, computerized scientific examinations might find lasting success and productive since industry experts might share their insight into the latest improvements in innovation.

The latest mechanical turns of events and changes in cybercrime ought to likewise be stayed up with the latest by computerized criminology agents. To guarantee that examiners have the fundamental capacities and data to play out their positions, this calls for continuous instruction and preparing really.

All in all, notwithstanding challenges and limitations, the field of computerized criminology keeps on progressing with the advancement of new strategies and device. Keeping a heartbeat on mechanical turns of events, laying out organizations with industry specialists, and using progressed procedures, for example, AI, computerized legal sciences examiners can improve their productivity and viability in gathering and breaking down advanced proof.

CHAPTER 6

CONCLUSION & REFERANCES

CONCLUSION :-

All in all, this exploration project includes the rising significance of live advanced criminology and the novel difficulties it presents. The task centers around the fields of cloning, data recuperation, and steganography, and investigates their valuable application with regards to digital criminology.

Through a complete writing survey and assessment of true contextual investigations, the task group has distinguished the requirement for proficient and dependable techniques for cloning, data recuperation, and steganography in computerized criminology examinations. The focus moreover reveals insight into the difficulties looked by computerized crime scene investigation experts, including the requirement for cutting edge specialized abilities and the limitations of current innovation.

During the examination cycle, the group experienced troubles, for instance, the requirement for precise and successful data recuperation procedures and the difficulties presented by steganography in revealing secret data. Nonetheless, the group proposed deals with any consequences regarding these challenges, including the utilization of cutting edge cloning strategies, data recuperation estimations, and steganalysis techniques.

The proposed plans can possibly upgrade the effectiveness and dependability of computerized legal sciences examinations and add to the general headway of the field. Proceeded with innovative work here are vital for stay aware of the advancement of innovation and the creating intricacy of digital assaults.

Generally, this examination project gives significant pieces of information into the significance of live computerized criminology and the requirement for cutting edge strategies and talented measurable analysts in doing effective examinations.

REFERANCES :-

1. Casey, E., & Stellatos, G. (2014). Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer. Elsevier.

2. Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

3. Casey, E., & Stellatos, G. (2014). Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer. Elsevier.

4. Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. IEEE Security & Privacy, 1(1), 17-27.

5. Kruse, II, W. G., & Heiser, J. G. (2002). Computer forensics: incident response essentials. Addison-Wesley Professional.

6. Casey, E. (2011). Digital evidence and computer crime: forensic science, computers, and the internet. Academic Press.

7. Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

8. Quick, D., & Choo, K. K. R. (2014). Principles and practice of forensic investigation of digital devices. Springer.

9. Kessler, G. C. (2005). Digital forensics: new paradigms in digital evidence and electronic crime investigation. Springer.

10. Raghavan, S., Kumar, S., Kalkoti, H., & Manvi, S. S. (2019). A review of data hiding techniques using steganography for digital images. Journal of Ambient Intelligence and Humanized Computing, 10(11), 4555-4575.

11. Shuhaibar, W., Fung, C., & Debbabi, M. (2018). Digital Forensics in the Internet of Things: Survey and Challenges. Journal of Network and Computer Applications, 121, 1-15.

12. Stellatos, G., & Casey, E. (2018). Live Forensics: Capturing and Analysing Volatile System Data. In E. Casey, & G. Stellatos (Eds.), Digital Forensics: Digital Evidence in Criminal Investigations (pp. 129-155). Academic Press.

13. Carrier, B. (2014). File system forensic analysis. Addison-Wesley Professional.

14. Casey, E., & Stellatos, G. (2017). Digital evidence and computer crime: forensic science, computers and the internet. Academic Press.

15. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7(1-2), 64-73.