Date of submission: 23/4/25
Batch: C1 Roll No.: 16010122323
Student Name: Vedansh Savla
Experiment No: 09
Staff In-charge: Shivani Deosthale

TITLE: Digital Forensic investigation using Encase forensic tool

OUTCOME: Student will be able to
CO4 Illustrate and Compare network security mechanisms

Pre Lab/ Prior Concepts:

- **Basic computer and file system knowledge** (FAT, NTFS, EXT)
- **Understanding of operating systems** (especially Windows directory structure)
- Familiarity with **file extensions** and common file types (e.g., .docx, .jpg, .exe)
- Introduction to **cybersecurity concepts** (integrity, confidentiality, availability)
- Awareness of **digital evidence handling procedures** (chain of custody, non-repudiation)
- Basic knowledge of **hexadecimal and binary data**

Abstract:

This lab explores the practical application of digital forensic techniques using the **EnCase Forensic Tool**, a leading software used by law enforcement and investigators worldwide. The objective is to simulate a forensic investigation by examining a suspect's disk image to recover deleted files, search for keywords, analyze file signatures, and identify suspicious content. Students will perform step-by-step actions including evidence acquisition, keyword search, file recovery, and report generation.

This hands-on experience enhances the understanding of digital forensics and helps develop critical skills necessary for legal and ethical evidence handling in real-world cybercrime investigations.

Related Theory:

1. Digital Forensics Overview: Digital forensics is the science of recovering, investigating, and analyzing information from digital devices that can be used in a court of law. It involves a structured process that ensures the integrity and admissibility of evidence.

2. EnCase Forensic Tool: EnCase is a powerful forensic platform used to acquire and analyze data from computers, mobile devices, and servers. It supports features like disk imaging, file carving, email analysis, and report generation. It maintains the forensic soundness of evidence, making it acceptable in legal proceedings.

3. Forensic Investigation Lifecycle:

- **Identification**: Determine the scope and nature of the investigation.
- **Preservation**: Ensure that data is not altered or damaged.
- **Examination**: Explore the data systematically using tools.
- **Analysis**: Interpret findings in relation to the case.
- **Documentation and Reporting**: Record findings clearly and create professional forensic reports.

4. File Signature and Hash Analysis: File signature analysis checks if a file's header (magic number) matches its extension. Hash values (e.g., MD5, SHA-1) are used to verify file integrity and detect tampering.

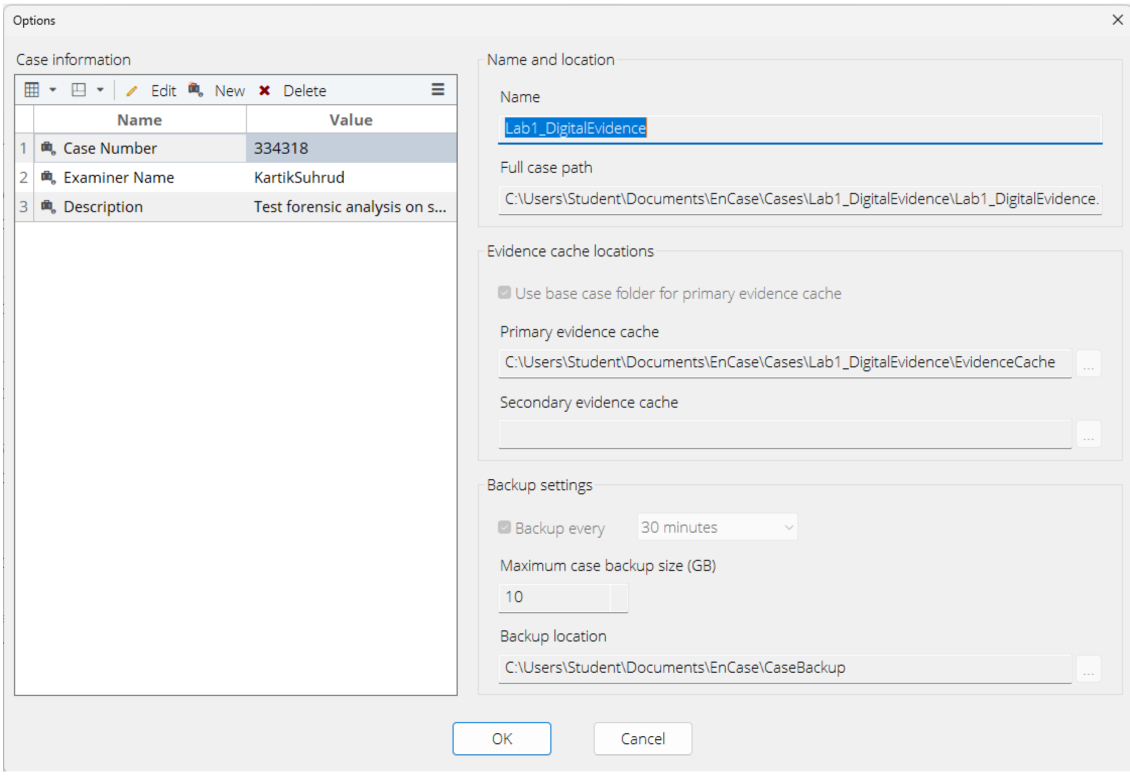
5. Deleted File Recovery: Even after deletion, data may remain in unallocated disk space. Forensic tools like EnCase can recover this data using carving techniques.

6. Legal and Ethical Considerations:

- **Chain of custody** must be maintained for evidence.

- **Privacy and legal compliance** must be observed when accessing personal or sensitive data.
- **Objectivity and integrity** are critical in forensic analysis.

Implementation Details:



Options

Case information

	Name	Value
1	Case Number	334318
2	Examiner Name	KartikSuhrud
3	Description	Test forensic analysis on s...

Name and location

Name: Lab1_DigitalEvidence

Full case path: C:\Users\Student\Documents\EnCase\Cases\Lab1_DigitalEvidence\Lab1_DigitalEvidence.

Evidence cache locations

☑ Use base case folder for primary evidence cache

Primary evidence cache: C:\Users\Student\Documents\EnCase\Cases\Lab1_DigitalEvidence\EvidenceCache

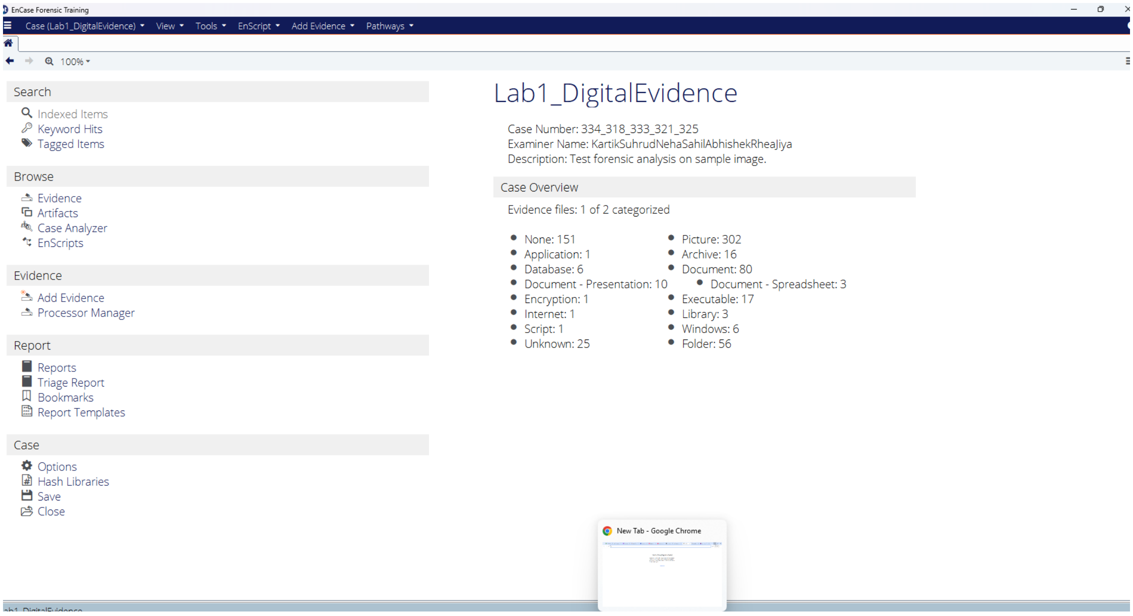
Secondary evidence cache:

Backup settings

☑ Backup every 30 minutes

Maximum case backup size (GB): 10

Backup location: C:\Users\Student\Documents\EnCase\CaseBackup



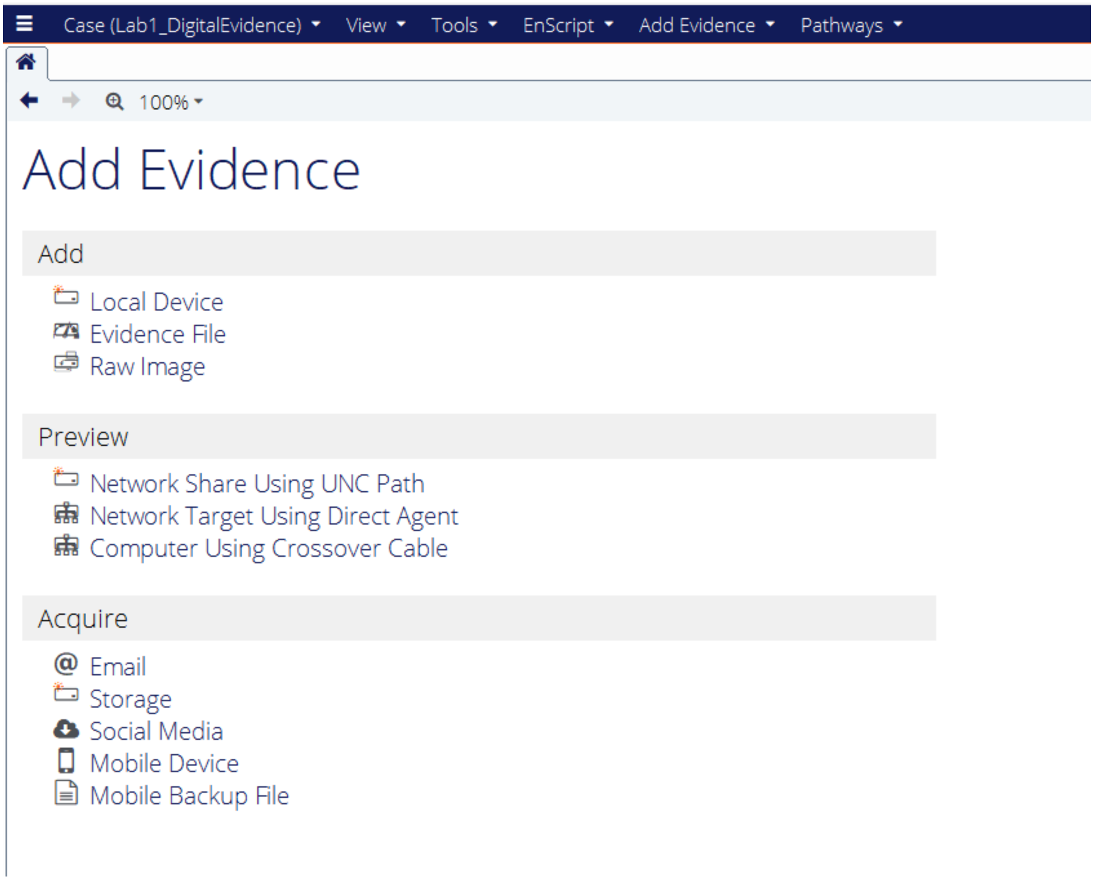
Lab1_DigitalEvidence

Case Number: 334_318_333_321_325
Examiner Name: KartikSuhrudNehaSahilAbhishekRheaJiya
Description: Test forensic analysis on sample image.

Case Overview

Evidence files: 1 of 2 categorized

- None: 151
- Application: 1
- Database: 6
- Document - Presentation: 10
- Encryption: 1
- Internet: 1
- Script: 1
- Unknown: 25
- Picture: 302
- Archive: 16
- Document: 80
  - Document - Spreadsheet: 3
- Executable: 17
- Library: 3
- Windows: 6
- Folder: 56



Add Evidence

Add

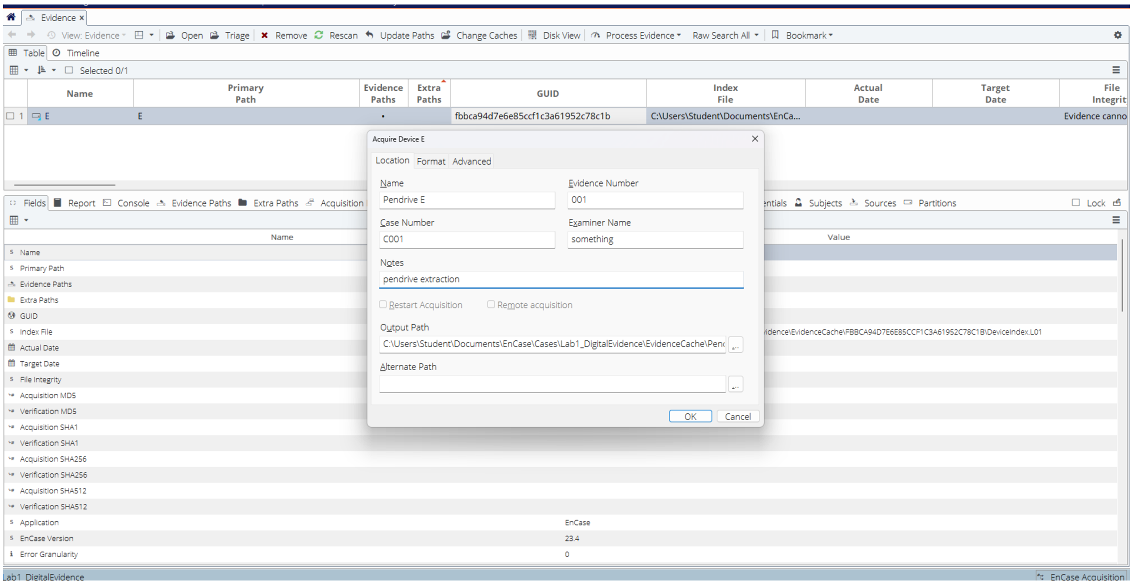
- Local Device
- Evidence File
- Raw Image

Preview

- Network Share Using UNC Path
- Network Target Using Direct Agent
- Computer Using Crossover Cable

Acquire

- Email
- Storage
- Social Media
- Mobile Device
- Mobile Backup File



Evidence

Table | Timeline | Selected 0/1

	Name	Primary Path	Evidence Paths	Extra Paths	GUID	Index File	Actual Date	Target Date	File Integrit
☐ 1	E	E	•		fbbca94d7e6e85ccf1c3a61952c78c1b	C:\Users\Student\Documents\EnCa...			Evidence canno

Acquire Device E

Location | Format | Advanced

Name: Pendrive E

Evidence Number: 001

Case Number: C001

Examiner Name: something

Notes: pendrive extraction

☐ Restart Acquisition ☐ Remote acquisition

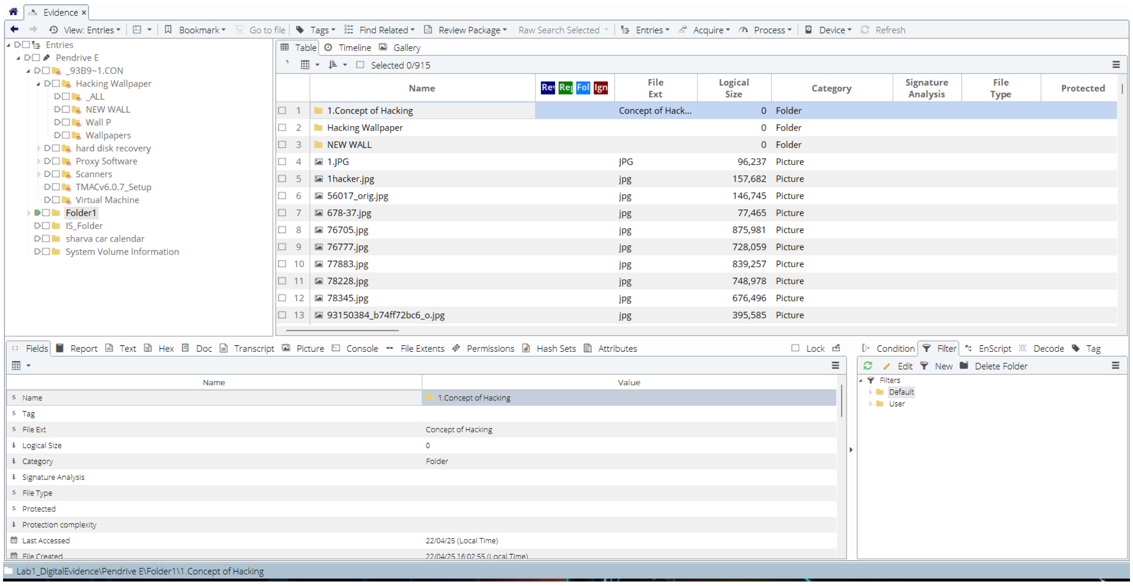
Output Path: C:\Users\Student\Documents\EnCase\Cases\Lab1_DigitalEvidence\EvidenceCache\Pen(

Alternate Path:

OK Cancel

Name	Value
Name	
Primary Path	
Evidence Paths	
Extra Paths	
GUID	
Index File	...idence\EvidenceCache\FBBCA94D7E6E85CCF1C3A61952C78C1B\DeviceIndex.L01
Actual Date	
Target Date	
File Integrity	
Acquisition MD5	
Verification MD5	
Acquisition SHA1	
Verification SHA1	
Acquisition SHA256	
Verification SHA256	
Acquisition SHA512	
Verification SHA512	
Application	EnCase
EnCase Version	23.4
Error Granularity	0

Lab1_DigitalEvidence EnCase Acquisition



Entries
- Pendrive E
  - _93B9~1.CON
    - Hacking Wallpaper
      - _ALL
      - NEW WALL
      - Wall P
      - Wallpapers
    - hard disk recovery
    - Proxy Software
    - Scanners
    - TMACv6.0.7_Setup
    - Virtual Machine
  - Folder1
  - IS_Folder
  - sharva car calendar
  - System Volume Information

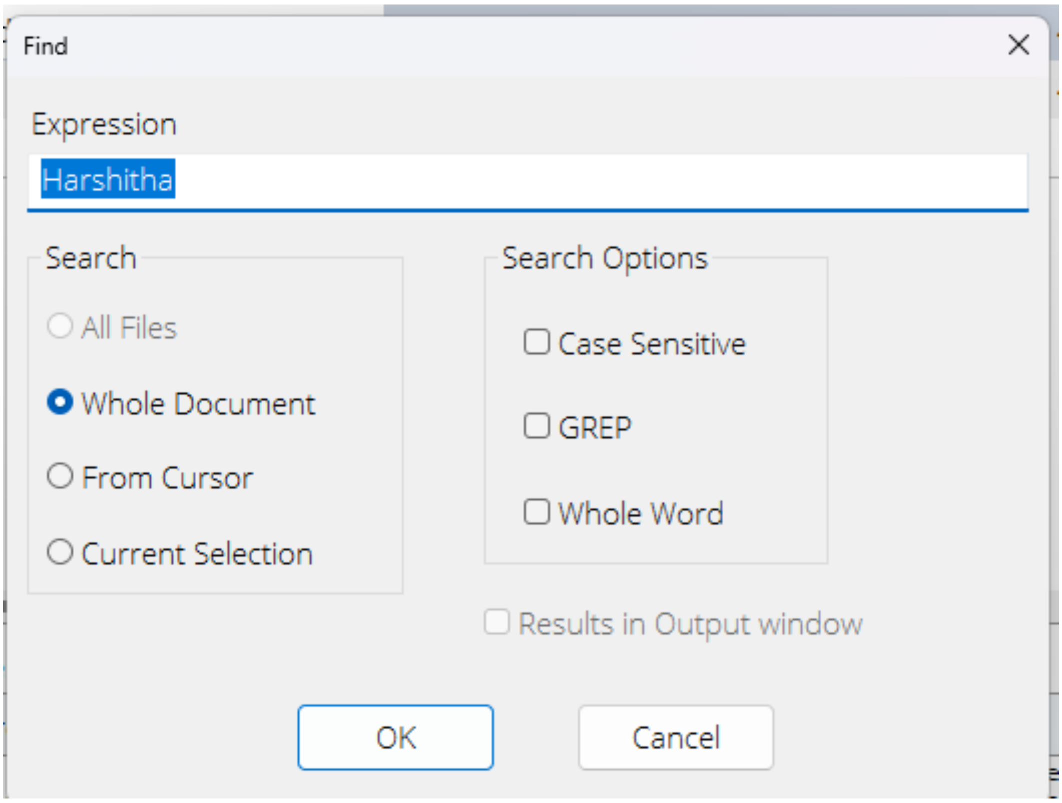
Table | Timeline | Gallery | Selected 0/915

		Name	Rev Rep Fol Ign	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected
☐	1	1.Concept of Hacking		Concept of Hack...	0	Folder			
☐	2	Hacking Wallpaper			0	Folder			
☐	3	NEW WALL			0	Folder			
☐	4	1.JPG		JPG	96,237	Picture			
☐	5	1hacker.jpg		jpg	157,682	Picture			
☐	6	56017_orig.jpg		jpg	146,745	Picture			
☐	7	678-37.jpg		jpg	77,465	Picture			
☐	8	76705.jpg		jpg	875,981	Picture			
☐	9	76777.jpg		jpg	728,059	Picture			
☐	10	77883.jpg		jpg	839,257	Picture			
☐	11	78228.jpg		jpg	748,978	Picture			
☐	12	78345.jpg		jpg	676,496	Picture			
☐	13	93150384_b74ff72bc6_o.jpg		jpg	395,585	Picture			

Name	Value
Name	1.Concept of Hacking
Tag	
File Ext	Concept of Hacking
Logical Size	0
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	22/04/25 (Local Time)
File Created	22/04/25 16:02:55 (Local Time)

Filters
- Default
- User

Lab1_DigitalEvidence\Pendrive E\Folder1\1.Concept of Hacking



Find

Expression

Harshitha

Search

○ All Files

● Whole Document

○ From Cursor

○ Current Selection

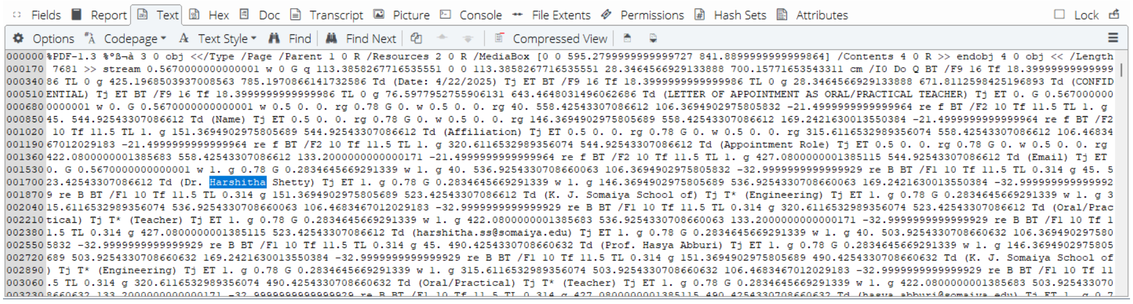
Search Options

□ Case Sensitive

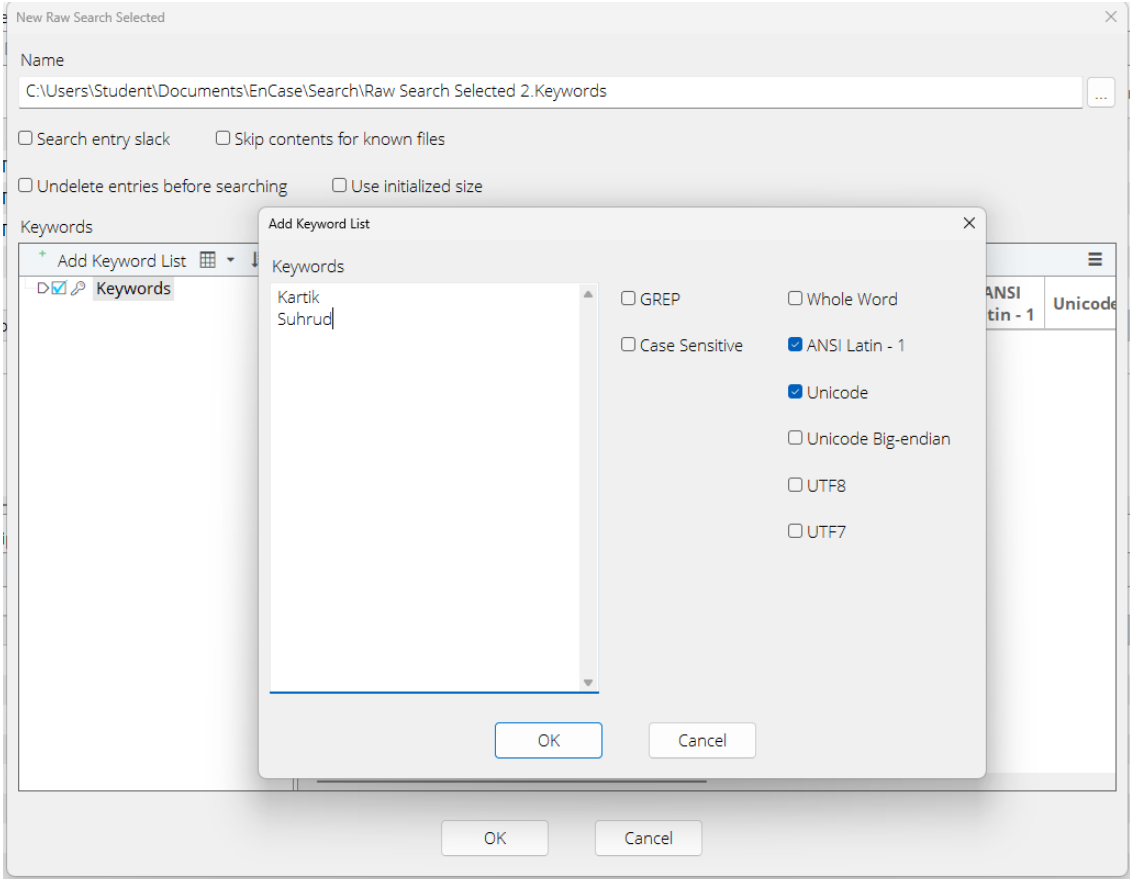
□ GREP

□ Whole Word

□ Results in Output window



```
000000 %PDF-1.3 %°ß¬à 3 0 obj <</Type /Page /Parent 1 0 R /Resources 2 0 R /MediaBox [0 0 595.2799999999999727 841.8899999999999864] /Contents 4 0 R >> endobj 4 0 obj << /Length
000170  7681 >> stream 0.5670000000000001 w 0 G q 113.3858267716535551 0 0 113.3858267716535551 28.3464566929133888 700.15771653543311 cm /I0 Do Q BT /F9 16 Tf 18.39999999999999
000340 86 TL 0 g 425.1968503937008563 785.1970866141732586 Td (Date: 4/22/2025) Tj ET BT /F9 16 Tf 18.3999999999999986 TL 0 g 28.3464566929133888 671.8112598425196893 Td (CONFID
000510 ENTIAL) Tj ET BT /F9 16 Tf 18.3999999999999986 TL 0 g 76.5977952755906131 643.4648031496062686 Td (LETTER OF APPOINTMENT AS ORAL/PRACTICAL TEACHER) Tj ET 0. G 0.567000000
000680 0000001 w 0. G 0.5670000000000001 w 0.5 0. 0. rg 0.78 G 0. w 0.5 0. 0. rg 40. 558.42543307086612 106.3694902975805832 -21.4999999999999964 re f BT /F2 10 Tf 11.5 TL 1. g
000850 45. 544.92543307086612 Td (Name) Tj ET 0.5 0. 0. rg 0.78 G 0. w 0.5 0. 0. rg 146.3694902975805689 558.42543307086612 169.2421630013550384 -21.4999999999999964 re f BT /F2
001020  10 Tf 11.5 TL 1. g 151.3694902975805689 544.92543307086612 Td (Affiliation) Tj ET 0.5 0. 0. rg 0.78 G 0. w 0.5 0. 0. rg 315.6116532989356074 558.42543307086612 106.46834
001190 67012029183 -21.4999999999999964 re f BT /F2 10 Tf 11.5 TL 1. g 320.6116532989356074 544.92543307086612 Td (Appointment Role) Tj ET 0.5 0. 0. rg 0.78 G 0. w 0.5 0. 0. rg
001360 422.0800000001385683 558.42543307086612 133.2000000000000171 -21.4999999999999964 re f BT /F2 10 Tf 11.5 TL 1. g 427.0800000001385115 544.92543307086612 Td (Email) Tj ET
001530 0. G 0.5670000000000001 w 1. g 0.78 G 0.2834645669291339 w 1. g 40. 536.9254330708660063 106.3694902975805832 -32.9999999999999929 re B BT /F1 10 Tf 11.5 TL 0.314 g 45. 5
001700 23.42543307086612 Td (Dr. Harshitha Shetty) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 146.3694902975805689 536.9254330708660063 169.2421630013550384 -32.999999999999992
001870 9 re B BT /F1 10 Tf 11.5 TL 0.314 g 151.3694902975805689 523.42543307086612 Td (K. J. Somaiya School of) Tj T* (Engineering) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 3
002040 15.6116532989356074 536.9254330708660063 106.4683467012029183 -32.9999999999999929 re B BT /F1 10 Tf 11.5 TL 0.314 g 320.6116532989356074 523.42543307086612 Td (Oral/Prac
002210 tical) Tj T* (Teacher) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 422.0800000001385683 536.9254330708660063 133.2000000000000171 -32.9999999999999929 re B BT /F1 10 Tf 1
002380 1.5 TL 0.314 g 427.0800000001385115 523.42543307086612 Td (harshitha.ss@somaiya.edu) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 40. 503.9254330708660632 106.369490297580
002550 5832 -32.9999999999999929 re B BT /F1 10 Tf 11.5 TL 0.314 g 45. 490.4254330708660632 Td (Prof. Hasya Abburi) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 146.3694902975805
002720 689 503.9254330708660632 169.2421630013550384 -32.9999999999999929 re B BT /F1 10 Tf 11.5 TL 0.314 g 151.3694902975805689 490.4254330708660632 Td (K. J. Somaiya School of
002890 ) Tj T* (Engineering) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 315.6116532989356074 503.9254330708660632 106.4683467012029183 -32.9999999999999929 re B BT /F1 10 Tf 11
003060 .5 TL 0.314 g 320.6116532989356074 490.4254330708660632 Td (Oral/Practical) Tj T* (Teacher) Tj ET 1. g 0.78 G 0.2834645669291339 w 1. g 422.0800000001385683 503.925433070
003230 8660632 133.2000000000000171 -32.9999999999999929 re B BT /F1 10 Tf 11.5 TL 0.314 g 427.0800000001385115 490.4254330708660632 Td (hasya.abburi@somaiya.edu) Tj ET 1. g 0.7
```



New Raw Search Selected

Name: C:\Users\Student\Documents\EnCase\Search\Raw Search Selected 2.Keywords

☐ Search entry slack ☐ Skip contents for known files

☐ Undelete entries before searching ☐ Use initialized size

Keywords

Add Keyword List

Keywords

Add Keyword List

Keywords

Kartik
Suhrud

☐ GREP ☐ Whole Word

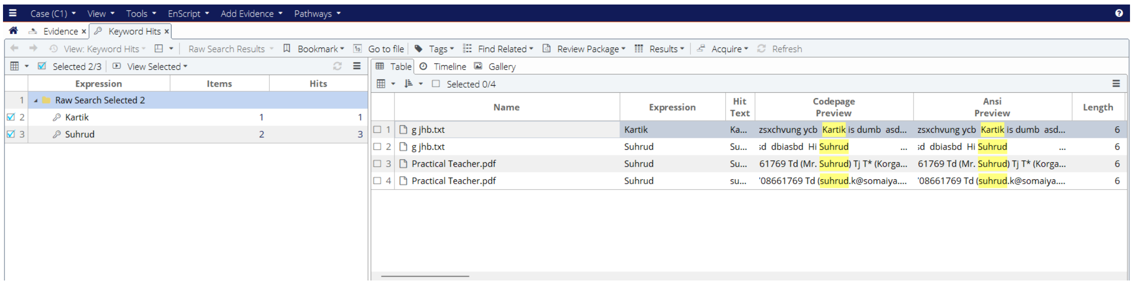
☐ Case Sensitive ☑ ANSI Latin - 1

☑ Unicode

☐ Unicode Big-endian

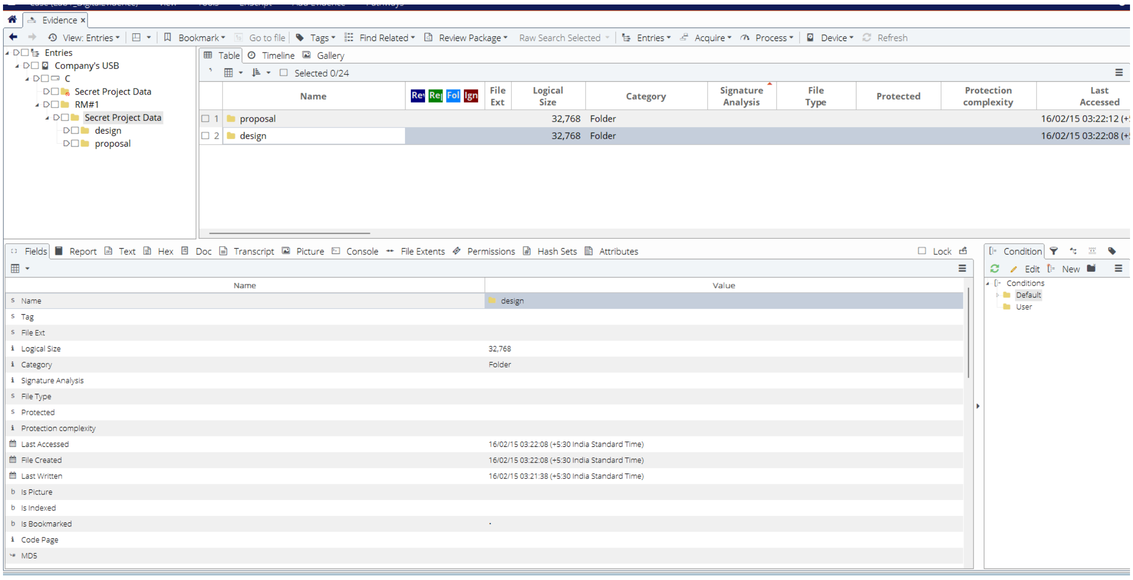
☐ UTF8

☐ UTF7



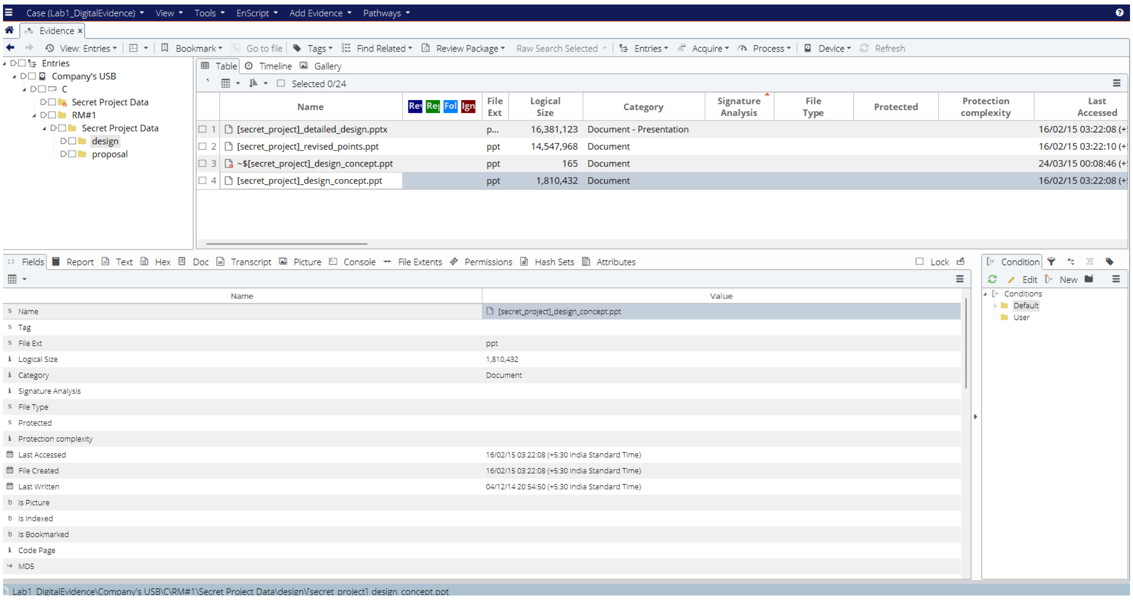
	Expression	Items	Hits
1	Raw Search Selected 2		
☑ 2	Kartik	1	1
☑ 3	Suhrud	2	3

	Name	Expression	Hit Text	Codepage Preview	Ansi Preview	Length
☐ 1	g jhb.txt	Kartik	Ka...	zsxchvung ycb Kartik is dumb asd...	zsxchvung ycb Kartik is dumb asd...	6
☐ 2	g jhb.txt	Suhrud	Su...	;d dbiasbd Hi Suhrud ...	;d dbiasbd Hi Suhrud ...	6
☐ 3	Practical Teacher.pdf	Suhrud	Su...	61769 Td (Mr. Suhrud) Tj T* (Korga...	61769 Td (Mr. Suhrud) Tj T* (Korga...	6
☐ 4	Practical Teacher.pdf	Suhrud	su...	'08661769 Td (suhrud.k@somaiya....	'08661769 Td (suhrud.k@somaiya....	6



	Name	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexity	Last Accessed
1	proposal		32,768	Folder					16/02/15 03:22:12 (+
2	design		32,768	Folder					16/02/15 03:22:08 (+

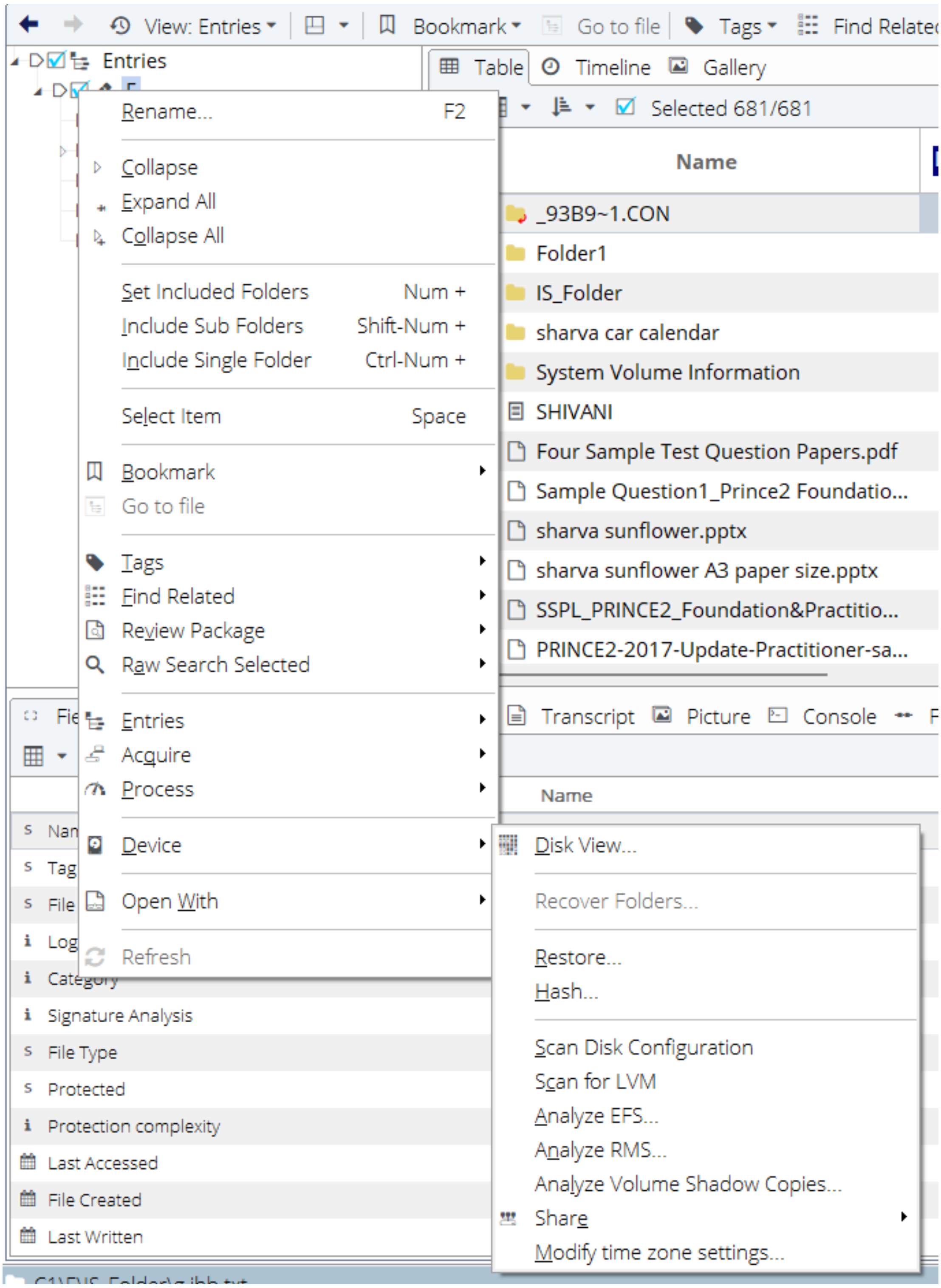
Name	Value
Name	design
Tag	
File Ext	
Logical Size	32,768
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	16/02/15 03:22:08 (+5:30 India Standard Time)
File Created	16/02/15 03:22:08 (+5:30 India Standard Time)
Last Written	16/02/15 03:21:38 (+5:30 India Standard Time)
Is Picture	
Is Indexed	
Is Bookmarked	.
Code Page	
MD5	

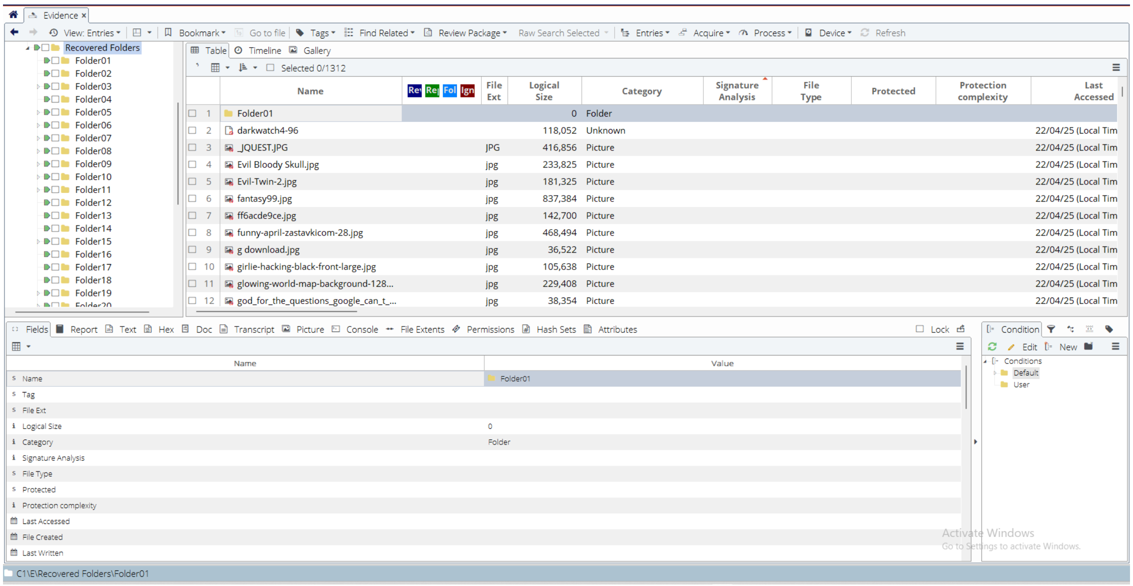


	Name	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexity	Last Accessed
1	[secret_project]_detailed_design.pptx	p...	16,381,123	Document - Presentation					16/02/15 03:22:08 (+
2	[secret_project]_revised_points.ppt	ppt	14,547,968	Document					16/02/15 03:22:10 (+
3	~$[secret_project]_design_concept.ppt	ppt	165	Document					24/03/15 00:08:46 (+
4	[secret_project]_design_concept.ppt	ppt	1,810,432	Document					16/02/15 03:22:08 (+

Name	Value
Name	[secret_project]_design_concept.ppt
Tag	
File Ext	ppt
Logical Size	1,810,432
Category	Document
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	16/02/15 03:22:08 (+5:30 India Standard Time)
File Created	16/02/15 03:22:08 (+5:30 India Standard Time)
Last Written	04/12/14 20:54:50 (+5:30 India Standard Time)
Is Picture	
Is Indexed	
Is Bookmarked	
Code Page	
MD5	

Lab1_DigitalEvidence\Company's USB\C\RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt


View: Entries
Bookmark
Go to file
Tags
Find Related
Entries
Table
Timeline
Gallery
Selected 681/681
Name
_93B9~1.CON
Folder1
IS_Folder
sharva car calendar
System Volume Information
SHIVANI
Four Sample Test Question Papers.pdf
Sample Question1_Prince2 Foundatio...
sharva sunflower.pptx
sharva sunflower A3 paper size.pptx
SSPL_PRINCE2_Foundation&Practitio...
PRINCE2-2017-Update-Practitioner-sa...
Rename... F2
Collapse
Expand All
Collapse All
Set Included Folders Num +
Include Sub Folders Shift-Num +
Include Single Folder Ctrl-Num +
Select Item Space
Bookmark
Go to file
Tags
Find Related
Review Package
Raw Search Selected
Entries
Acquire
Process
Device
Open With
Refresh
Disk View...
Recover Folders...
Restore...
Hash...
Scan Disk Configuration
Scan for LVM
Analyze EFS...
Analyze RMS...
Analyze Volume Shadow Copies...
Share
Modify time zone settings...
Transcript
Picture
Console
Name
Signature Analysis
File Type
Protected
Protection complexity
Last Accessed
File Created
Last Written



		Name	Rev Rej Fol Ign	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexity	Last Accessed
□	1	Folder01			0	Folder					
□	2	darkwatch4-96			118,052	Unknown					22/04/25 (Local Tim
□	3	_JQUEST.JPG		JPG	416,856	Picture					22/04/25 (Local Tim
□	4	Evil Bloody Skull.jpg		jpg	233,825	Picture					22/04/25 (Local Tim
□	5	Evil-Twin-2.jpg		jpg	181,325	Picture					22/04/25 (Local Tim
□	6	fantasy99.jpg		jpg	837,384	Picture					22/04/25 (Local Tim
□	7	ff6acde9ce.jpg		jpg	142,700	Picture					22/04/25 (Local Tim
□	8	funny-april-zastavkicom-28.jpg		jpg	468,494	Picture					22/04/25 (Local Tim
□	9	g download.jpg		jpg	36,522	Picture					22/04/25 (Local Tim
□	10	girlie-hacking-black-front-large.jpg		jpg	105,638	Picture					22/04/25 (Local Tim
□	11	glowing-world-map-background-128...		jpg	229,408	Picture					22/04/25 (Local Tim
□	12	god_for_the_questions_google_can_t_...		jpg	38,354	Picture					22/04/25 (Local Tim

Name	Value
Name	Folder01
Tag	
File Ext	
Logical Size	0
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	
File Created	
Last Written	

C1\E\Recovered Folders\Folder01

Conclusion: Experiment demonstrates the practical implementation of digital forensic techniques using EnCase, including evidence acquisition, examination, file recovery, and reporting, to support incident response and investigative procedures.

Post Lab Questions:

1. **How does EnCase handle evidence integrity? What role does hashing play in this?**

⇨ EnCase ensures the integrity of digital evidence through the use of cryptographic hashing. When an evidence file, such as an E01 image, is added to a case, EnCase automatically generates hash values like MD5 or SHA-1. These values act as digital fingerprints unique to the file's content. Throughout the forensic analysis process, EnCase verifies the evidence by recalculating and comparing these hash values. If the values match the original, it confirms that the evidence has not been altered or tampered with, maintaining its integrity.

Hashing plays a critical role in validating the authenticity of evidence and supporting the chain of custody. In digital forensics, any modification—even a single byte—will change the hash value, signaling possible evidence tampering. By consistently checking hash values during the investigation, EnCase provides a reliable method to ensure that all findings are based on unaltered data. This practice not only upholds the credibility of the investigation but also helps meet legal standards for presenting digital evidence in court.

2. **What filters or search tools did you use to locate potentially relevant files?**

⇨ To locate potentially relevant files, the following **filters and search tools** in EnCase were used:

- **File Extension Filters** – to quickly find files like .jpg, .png, .docx, .pdf, .pst, and .eml.

- **Keyword Search** – using terms like **"password," "confidential,"** and **"meeting"** to identify sensitive or suspicious content.
- **Hash Analysis** – to identify known files by comparing them against known hash databases.
- **Signature Analysis** – to detect mismatches between file extensions and actual content (e.g., a .jpg file that's actually an executable).
- **Date Filters/Timeline View** (if used in optional tasks) – to trace user activity or recent changes.

These tools helped in narrowing down the vast data to focus only on **evidentially significant files**.

3. What is file signature analysis, and how did it help identify suspicious files?

⇨ **File signature analysis** is a forensic technique used to verify whether a file's **extension matches its actual content** by comparing its **internal file header (signature)** to known standards. Every file type has a unique binary pattern (called a **magic number**) at the beginning, which indicates what type of file it really is—regardless of its name or extension.

In EnCase, file signature analysis helped identify **suspicious files** by detecting **mismatches** between the file's header and its extension. For example, a file named `report.pdf` might actually be an executable file if its internal signature doesn't match the standard for PDFs. These mismatches often indicate attempts to **hide malicious or inappropriate content**, such as renaming `.exe` files to `.jpg` or `.txt`. By flagging these inconsistencies, the analysis helped pinpoint files that required deeper examination for potential security risks or digital evidence.

4. Why is it important to follow ethical guidelines during forensic analysis?

⇨ Following ethical guidelines during forensic analysis is crucial to ensure that investigations are conducted fairly, legally, and responsibly. Digital forensics often involves access to sensitive personal, corporate, or governmental data. Without proper ethics, there is a risk of violating privacy, misusing information, or altering evidence—intentionally or unintentionally—which can lead to legal consequences and loss of trust.

Ethical guidelines also help maintain the credibility of the investigation and ensure that the findings are admissible in court. They promote transparency, objectivity, and accountability in every step of the forensic process. Upholding ethics protects not only the rights of individuals involved but also the integrity of the forensic examiner and the justice system as a whole.