

Course Name:	Information Security (116U01L602)	Semester:	VI
Date of Performance:	23/ 04 / 2025	DIV/ Batch No:	A4
Student Name:	Hyder Presswala & Riddhi Patil	Roll No:	16010122151

Title: Digital Forensic investigation using Encase forensic tool

Objectives:

CO5 Interpret legal and ethical issues in security

Expected Outcome of Experiment:

- Understanding the process and methodology for conducting a digital forensic investigation using EnCase Forensic Tool.
- Familiarity with the key features of EnCase, such as data acquisition, analysis, and reporting.
- Ability to use EnCase to gather and analyze evidence from digital devices.
- Understanding of how to ensure the integrity and validity of digital evidence during an investigation.
- Gaining practical experience in analyzing digital evidence for possible legal use.
- Developing insights into the application of digital forensic principles in real-world investigations.

Books/ Journals/ Websites referred:

<https://www.opentext.com/products/encase-forensic>

Technical articles, tips, and troubleshooting -

<https://forums.opentext.com/forums/support/categories/encase>

Creation of forensic image - <https://www.youtube.com/watch?v=qoOuhrvJgV8>

Process and analyse forensic image -

<https://www.youtube.com/watch?v=DxjBq4vPNA0>

Keyword Search - <https://www.youtube.com/watch?v=NduzWlvr4oI>

Access Windows Registry - https://www.youtube.com/watch?v=be2EYmo_tIQ

Pre Lab/ Prior Concepts:

Basic Computer Forensics:

- Understanding of computer hardware and software.
- Concepts of digital evidence and its importance in investigations.
- The basics of file systems (FAT, NTFS, exFAT) and how they store and manage data.

Digital Evidence Integrity:

- Chain of custody procedures.
- The concept of imaging, hashing, and ensuring data integrity during the forensic process.

Data Acquisition Techniques:

- Methods to acquire data from storage media (hard drives, USBs, network devices).
- Write-blocking techniques to prevent altering data during the acquisition process.

File Analysis and Recovery:

- Concepts of file signatures and file carving.
- Recovery of deleted files and hidden data.

New Concepts to be learned:

EnCase Tool Features:

- Using EnCase to create forensic images of digital media.
- Data analysis and investigation features of EnCase, including keyword searches, filtering, and timeline analysis.
- Creating and managing cases in EnCase.

Forensic Report Generation:

- Creating and understanding detailed forensic reports using EnCase.
- Generating evidence logs and preparing reports for legal proceedings.

File System Forensics:

- In-depth knowledge of how file systems operate and how to analyze them for digital evidence in EnCase.
- Techniques for reconstructing deleted or hidden files using EnCase.

Data Carving and Extraction:

- Using EnCase to perform data carving for recovering fragmented or incomplete files.
- Extraction of metadata, system logs, and artifacts useful in investigations.

Handling Encrypted Data:

- Using EnCase for investigating encrypted data and applying decryption methods when possible.

Abstract:

Digital forensics plays a crucial role in investigating cybercrimes, data breaches, and incidents involving the misuse of digital devices. The EnCase Forensic Tool is one of the leading software applications used in digital forensics for evidence acquisition, analysis, and reporting. This experiment aims to demonstrate the process of using EnCase to conduct a digital forensic investigation. The primary objective is to acquire digital evidence, analyze it for relevant data, and generate a detailed forensic report. The experiment will also explore techniques for data recovery, file analysis, and ensuring evidence integrity throughout the investigation process.

Related Theory:

Digital Forensics Fundamentals:

- Digital forensics refers to the process of collecting, preserving, analyzing, and presenting data in a manner that is legally acceptable in a court of law.
- The investigation of digital evidence requires specialized tools, methodologies, and adherence to strict protocols to ensure the authenticity and integrity of the data.

EnCase Tool Overview:

- EnCase is a powerful tool used for forensic investigations and is known for its capabilities in acquiring, analyzing, and reporting digital evidence.
- It supports various types of digital media and file systems, making it versatile in investigating computers, mobile devices, and networks.

The Importance of Data Integrity:

- In digital forensics, ensuring the integrity of data is paramount. Investigators must follow procedures such as hashing and write-blocking to avoid altering the original evidence during the acquisition and analysis stages.

Digital Evidence Analysis:

- The analysis phase involves searching for specific data related to an investigation, recovering deleted or hidden files, and piecing together evidence in a manner that helps reconstruct events.

Legal Aspects of Digital Forensics:

- Digital forensics investigations must comply with legal frameworks such as the Fourth Amendment (U.S.) and data protection laws to ensure that evidence is admissible in court. Evidence handling and documentation must adhere to legal standards for chain of custody and preservation.

Implementation Details:

Case (Lab1 Digital Evidence) View Tools EnScript Add Evidence Pathways									
Evidence Timeline									
Table Selected 0/1									
	Name	Primary Path	Evidence Paths	Extra Paths	GUID	Index File	Actual Date	Target Date	File Integrity
1	Company's USB	D:\student_drive.E01\cfreds_2015_data_leakage_r...			8bfa4230bf4e35cb966b8c1a9321a0b1	C:\Users\Student\Documents\EnCa...	27/03/15 19:50:07 (+5:30 L...	27/03/15 19:50:07 (+5:30 L...	Completely Ver
Fields Report Console Evidence Paths Extra Paths Acquisition Info Read Errors Missing Sectors CRC Errors Evidence Processor Logs Credentials Subjects Sources Partitions Lock									
	Name	Value							
5	Name	Company's USB							
5	Primary Path	D:\student_drive.E01\cfreds_2015_data_leakage_rmm#1.E01							
5	Evidence Paths								
5	Extra Paths								
5	GUID	8bfa4230bf4e35cb966b8c1a9321a0b1							
5	Index File	C:\Users\Student\Documents\EnCase\EvidenceCache\8BFA4230BF4E35CB966B8C1A9321A0B1\DeviceIndex.L01							
5	Actual Date	27/03/15 19:50:07 (+5:30 India Standard Time)							
5	Target Date	27/03/15 19:50:07 (+5:30 India Standard Time)							
5	File Integrity	Completely Verified, 0 Errors							
5	Acquisition MD5	8bfa4230bf4e35cb966b8c1a9321a0b1							
5	Verification MD5	8bfa4230bf4e35cb966b8c1a9321a0b1							
5	Acquisition SHA1	f0bb840e98dd7c325af45539313fc3978f7b12c							
5	Verification SHA1	f0bb840e98dd7c325af45539313fc3978f7b12c							
5	Acquisition SHA256								
5	Verification SHA256								

The screenshot displays the EnCase Forensic Training application window. The main interface is divided into several panes:

- Left Pane (Evidence View):** Shows a hierarchical tree of evidence. The selected path is: Company's USB > C > Secret Project Data > RM#1 > Secret Project Data > design > proposal.
- Top Center Pane (File List Table):** Displays a table of files found in the selected location. The table has columns: Name, File Ext, Logical Size, Category, Signature Analysis, and File Type. The selected file is highlighted in blue.
- Bottom Left Pane (Fields):** Shows detailed metadata for the selected file, organized into sections like General, Security, and Forensic.
- Bottom Right Pane (Conditions):** Shows a list of conditions applied to the file, including 'Default' and 'User'.

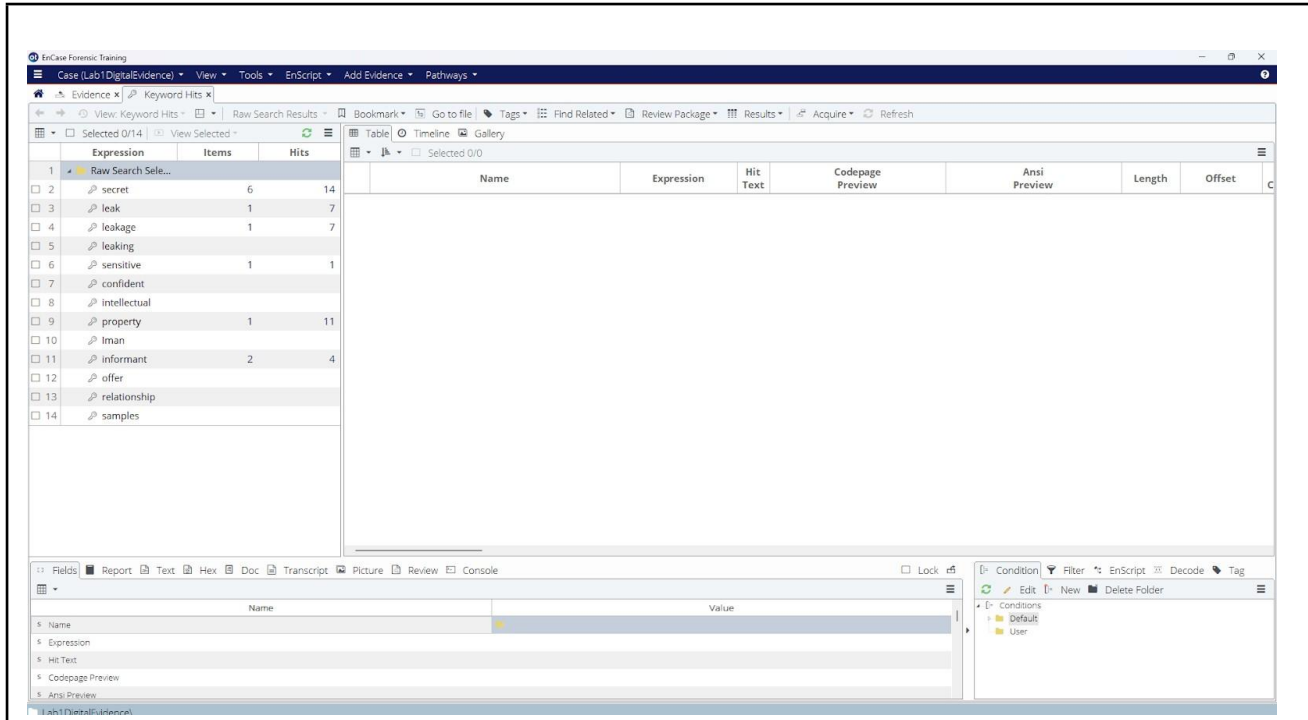
	Name	File Ext	Logical Size	Category	Signature Analysis	File Type
14	[secret_projec...	ppt	14,547,968	Document		
15	~\$[secret_pro...	ppt	165	Document		
16	\$Boot0		6,144	Unknown		
17	[secret_projec...	d...	35,226,880	Document		
18	[secret_projec...	d...	6,484,502	Document		
19	~\$secret_proje...	d...	162	Document		
20	Volume Slack		16,384	Unknown		

Name	Value
Name	[secret_project]_detailed_proposal.docx
Tag	
File Ext	docx
Logical Size	35,226,880
Category	Document
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	16/02/15 03:22:12 (+5:30 India Standard Time)
File Created	16/02/15 03:22:12 (+5:30 India Standard Time)
Last Written	19/12/14 03:20:58 (+5:30 India Standard Time)
Is Picture	
Is Indexed	
Is Bookmarked	
Code Page	
MDS	

Lab1DigitalEvidence\Company's USB\C\RM#1\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx

The screenshot shows the EnCase Forensic software interface. A dialog box titled "New Raw Search Selected" is open, allowing the user to add keywords to a search. The dialog box has a "Name" field containing "C:\Users\Student\Documents\EnCase\Search\Raw Search Selected 1. Keywords". Below this, there are checkboxes for "Search entry slack", "Skip contents for known files", "Undelete entries before searching", and "Use initialized size". The "Keywords" section contains a list of keywords to be added to the search. The keywords are: secret, leak, leakage, leaking, sensitive, confident, intellectual, property, lman, informant, offer, relationship, and samples. The dialog box also has a "Keywords" list on the left and a "Keywords" list on the right. The background shows the EnCase interface with a file tree on the left and a search results table on the right.

Name	Search Expression	GREP	Case Sensitive	Whole Word	ANSI Latin - 1	Unicode
1 secret	secret	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 leak	leak	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3 leakage	leakage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4 leaking	leaking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5 sensitive	sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6 confident	confident	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7 intellectual	intellectual	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8 property	property	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9 lman	lman	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10 informant	informant	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11 offer	offer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12 relationship	relationship	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13 samples	samples	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



The screenshot displays the EnCase Forensic Training application window. The main pane shows a search results table with the following data:

Expression	Items	Hits
secret	6	14
leak	1	7
leakage	1	7
leaking		
sensitive	1	1
confident		
intellectual		
property	1	11
Iman		
informant	2	4
offer		
relationship		
samples		

The bottom pane shows a list of fields with their corresponding values:

Name	Value
5 Name	
5 Expression	
5 Hit Text	
5 Codepage Preview	
5 Ansi Preview	

The screenshot displays a digital forensics tool interface with two main sections. The top section shows search results for a case named 'Case (Lab1 Digital Evidence)'. The bottom section shows a preview of a document titled '[Secret Project] design_concept.ppt'.

Search Results Table:

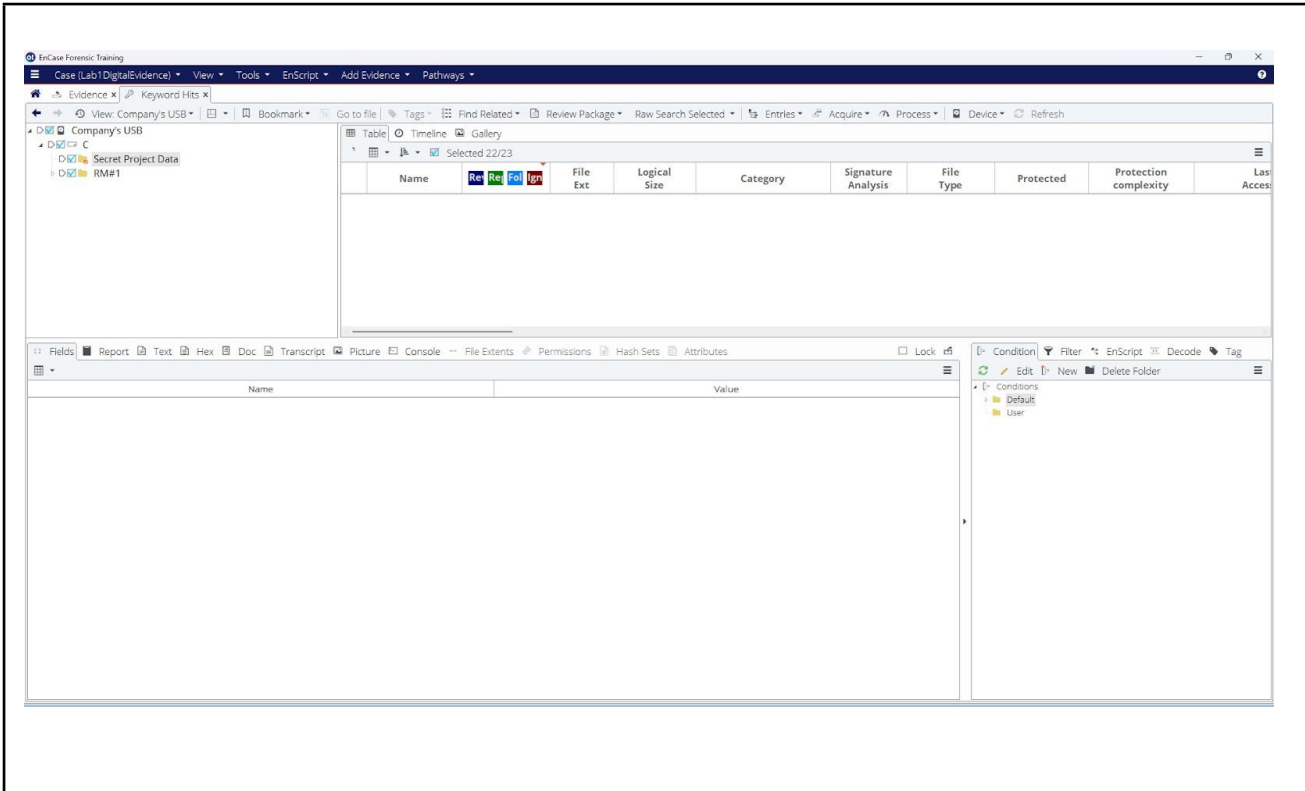
Expression	Items	Hits
secret	6	14
leak	1	7
leakage	1	7
leaking		
sensitive	1	1
confident		
intellectual		
property	1	11
Iman		
Informant	2	4
offer		
relationship		
samples		

Document Preview:

[Secret Project]

design_concept.ppt

This file is one of Govdocs (<http://d.pr/afcorpora.org/corpora.govdocs>)
The first page is added by NIST CFReDS project.
All following pages have no connection with to the scenario.



The screenshot displays the EnCase Forensic Training interface. The main window shows a file analysis of 'secret_project_details_proposal.docx'. The file is categorized as a 'Document' with a logical size of 35,226,880 bytes. The file content includes satellite imagery and a list of names from NOAA and NASA. A 'Properties' dialog box is open, showing the file is marked as 'SUSPICIOUS FILE'. A large '[Secret Project]' watermark is overlaid on the bottom half of the image.

Name	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexity	Last Access
1 [secret_proj...	docx	6,484,502	Document					16/02/15 03:22
2 [secret_proj...	docx	162	Document					24/03/15 00:07
3 [secret_proj...	docx	35,226,880	Document					16/02/15 03:22

National Institute for Space Research, The Netherlands

Mitch Goldberg and Chris Barnett
NOAA National Environmental Satellite,
Data, and Information Service, USA

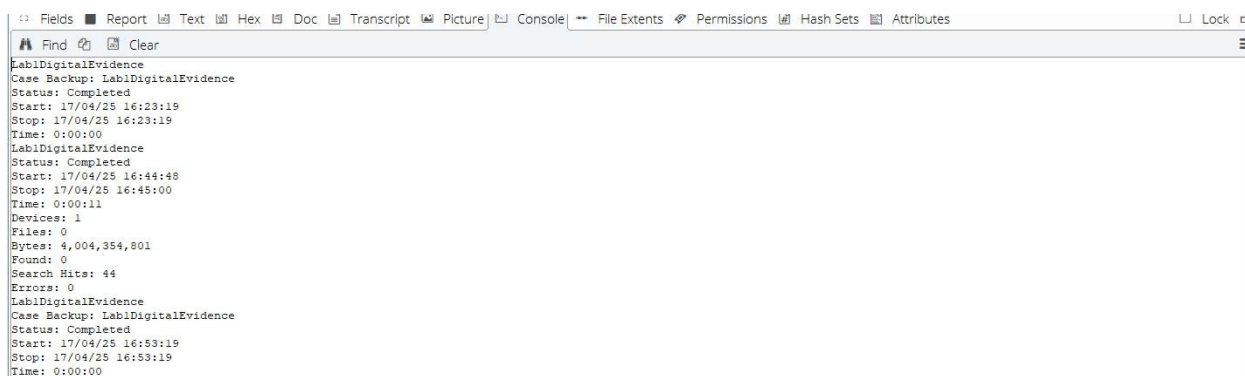
John L.e Marshall
NOAA/NASA/DoD Joint Center
for Satellite Data Assimilation, USA

Bob Atlas
NOAA Atlantic Oceanography and
Meteorological Laboratory, USA

Joel Susskind
NASA Goddard Space Flight Center, USA

Larabee Strow and Wallace McMillan
University of Maryland Baltimore County, USA

[Secret Project]



The screenshot displays the FTK Imager application window. The main pane shows the file system of a USB drive named 'Company's USB'. The file list is as follows:

Name	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexity	Ac
1 proposal		32,768	Folder					16/02/15 01
2 \$Boot0		6,144	Unknown					
3 \$Boot1		6,144	Unknown					
4 \$FAT Alignment		53,248	Unknown					
5 Primary FAT		491,520	Unknown					
6 Primary FAT...		32,768	Unknown					
7 \$Bitmap		15,274	Unknown					
8 \$UpCase		5,836	Unknown					
9 Secret Project...		32,768	Folder					24/03/15 01
10 RM#1		32,768	Folder					16/02/15 01
11 Secret Project...		32,768	Folder					16/02/15 01
12 design		32,768	Folder					16/02/15 01
13 {secret_projec...	ppt	1,810,432	Document					16/02/15 01
14 {secret_projec...	pptx	16,381,123	Document - Presentation					16/02/15 01
15 {secret_projec...	ppt	14,547,968	Document					16/02/15 01
16 {-{secret_pro...	ppt	165	Document					24/03/15 01
17 {-{secret_pro...	ppt	32,768	Document					

The interface also includes a sidebar on the left with a tree view showing 'Company's USB' and its contents. The bottom toolbar contains various analysis tools like 'Fields', 'Report', 'Text', 'Hex', 'Doc', 'Transcript', 'Picture', 'Console', 'File Exts', 'Permissions', 'Hash Sets', and 'Attributes'. The bottom right pane shows a 'Condition' filter set to 'Default'.

Conclusion:

In this experiment we learned EnCase tool.