Mahavir Education Trust's

Shah & Anchor Kutchhi Engineering College

An Autonomous Institute Affiliated to University of Mumbai

UG Program in Computer Engineering

(Accredited by NBA for 3 years from AY 2022-23)

Name:	______________________________
Roll No:	______________________________
Academic Year:	20___ - 20___

Semester VII

Final Year

Computer Engineering

Digital Forensics Laboratory

(CMDLOLR07041)

Mahavir Education Trust's

Shah & Anchor Kutchhi Engineering College

An Autonomous Institute Affiliated to University of Mumbai

UG Program in Computer Engineering

(Accredited by NBA for 3 years from AY 2022-23)

Institute

Vision: To become a globally recognized institution offering quality education and enhancing professional standards

Mission: To impart high-quality technical education to the students by providing an excellent academic environment, well-equipped laboratories and training through the motivated teachers.

Department

Vision:

To develop computer engineering graduates with engineering and managerial skills to acquire high end positions that are globally recognized.

Mission:

To impart computer engineering knowledge and to provide exposure to the latest technologies so that, students can solve various engineering problems and possesses social, ethical responsibilities and have the attitude of lifelong learning so as to bring about competent professionals.

Program Educational Objectives (PEO)

1. Graduates will possess the engineering fundamental knowledge and technical skills to build successful career in various domains.

2. Graduates will analyze real life problems and build feasible and economically acceptable solutions using latest technologies.

3. Graduates will exhibit strong soft skills, teamwork, professional ethics and social responsibilities.

Program Specific Outcomes (PSOs)

1. Students will be able to design & develop Computer programs and Automated systems to solve the real world problems for the benefit of society.

2. Students will be able to work professionally by applying Software Engineering practices, pursue higher studies and build Entrepreneur skills.

Mahavir Education Trust's

Shah & Anchor Kutchhi Engineering College

An Autonomous Institute Affiliated to University of Mumbai

UG Program in Computer Engineering

(Accredited by NBA for 3 years from AY 2022-23)

Program Outcomes (POs)

Engineering Graduates will be able to:

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Mapping of PSOs to POs:

PSO Number	**PO Number**
PSO1	PO1, PO2, PO3, PO4, PO5, PO6, PO7, PO12
PSO2	PO8, PO9, PO10, PO11, PO12

Sd/-
Program Coordinator
Computer Engineering Program

Mahavir Education Trust's

Shah & Anchor Kutchhi Engineering College

An Autonomous Institute Affiliated to University of Mumbai

UG Program in Computer Engineering

(Accredited by NBA for 3 years from AY 2022-23)

A Laboratory Journal for

Digital Forensics Lab

(CMDLOLR07041)

Semester VII

Bachelor of Technology

(B. Tech.)

in

Computer Engineering Department

Final Year with Effect from AY 2024 -2025

Prepared By:	Audited By:	Approved By:
Prof. Vaishali Chavan (Assistant Professor)	**Dr. Vidyullata Devmane** (Subject Expert)	**Dr. Bhavesh Patel** (Principal)
Dr. Vaishali Hirlekar (Assistant Professor)		**Dr. Vidyullata Devmane** (Head of Department)

Mahavir Education Trust's

Shah & Anchor Kutchhi Engineering College

An Autonomous Institute Affiliated to University of Mumbai

UG Program in Computer Engineering

(Accredited by NBA for 3 years from AY 2022-23)

Program: Final Year B. Tech.	Semester: VII	L	P	C
Digital Forensics	Course Code: CMDLOCR07041	2	0	2
Digital Forensics Lab	Lab Code: CMDLOLR07041	0	2	1
		2	2	3

Course Objectives:	
1	To discuss the need and process of digital forensics and Incident Response Methodology.
2	To explore the procedures for identification, acquisition and analysis of digital evidence and legal issues related to cybercrime.

Course Outcomes:	
After successful completion of this course, the students should be able to	
CO 1:	Discuss the terminologies related to Digital forensics and computer security incident process.
CO 2:	Describe and apply the process of collection, analysis and recovery of the digital evidence.
CO 3:	Use the forensics investigation process for operating system, network and application programs.
CO 4:	Discuss the different laws related to cyber crime.

Pre-requisite courses: Cryptography & System Security

Course Assessment Methods:

DIRECT

1. Continuous Internal Assessment (Theory component)
2. Assignments/Tutorials/Power-point-presentation/Group-discussion/Quiz/seminar/Casestudies/Design Thinking/Innovation/Creativity (Blog writing/Vlogging, etc)
3. Pre/Post - Experiment Test/Viva; Experimental Write-Up for each Experiment, Day to Day Experiments /Assignments/Tutorials/Power-point-presentation/Group-discussion/Quiz/seminar/Case studies/Design Thinking/Innovation/Creativity(Blog writing/Vlogging, etc) (Laboratory Component)
4. End Semester Examination (Theory and Laboratory components).

INDIRECT

1. Course-end survey 2. Activity based survey (if any)	
DETAILED SYLLABUS	
Module 1: Introduction to Digital Forensics	**06 Hours**
1.1 Digital Forensics-Definition, Digital Forensics Goals, Digital Forensics Categories – Computer Forensics, Mobile Forensics, Network Forensics, Database Forensics. 1.2 Cybercrime, Cybercrime Attack Mode, Computer Role in Cybercrime, Types of Cybercrime- Malware Distribution, Ransomware Distribution, Hacking, SQL Injections, Pharming, Phishing, E-mail Bombing And Spamming, Cyberstalking, DDoS Attacks, Social Engineering, Software Piracy 1.3 Introduction to Incident - Computer Security Incident, Goals of Incident Response, CSIRT, Incident Response Methodology, Phase after detection of an incident.	
Module 2: Digital Evidence Acquisition	**08 Hours**
2.1 Digital evidence, Types of Digital Evidence, Challenges in acquiring Digital evidence, Admissibility of evidence, Challenges in evidence handling, Chain of Custody. 2.2 Digital Forensics Examination Process - Seizure, Acquisition, Analysis, Reporting. Necessity of forensic duplication, Forensic image formats, Forensic duplication techniques. 2.3 Acquiring Digital Evidence - Forensic Image File Format, Acquiring Volatile Memory, Acquiring Nonvolatile Memory, Hard Drive Imaging Risks and Challenges	
Module 3: Forensics Investigation	**08 Hours**
3.1 Investigating Windows Systems - File Recovery, Windows Recycle Bin Forensics, Data Carving, Windows Registry Analysis, USB Device Forensics, File Format Identification, Windows Features Forensics Analysis, Windows 10 Forensics, Cortana Forensics 3.2 Investigating Unix Systems - Reviewing Pertinent Logs, Performing Keyword Searches, Reviewing Relevant Files, Identifying Unauthorized User Accounts or Groups, Identifying Rogue Processes, Checking for Unauthorized Access Points, Analyzing Trust Relationships 3.3 Investigation of Network Traffic- Finding Network-Based Evidence, Generating Session Data with tcptrace, Reassembling Sessions Using tcpflow, Reassembling Sessions Using Ethereal, Investigating Routers 3.4 Web Browser and Email Forensics - IE, Microsoft Edge Web Browser, Firefox, Google Chrome. Steps in E-mail Communications, List of E-mail Protocols, E-mail Header Examination	
Module 4: Digital Forensics Report and Bodies of law	**04 Hours**
4.1 Investigative Report Template, Layout of an Investigative Report, Guidelines for Writing a Report 4.2 Constitutional law, Criminal law, Civil law, Administrative regulations, Levels of law: Local laws, State laws, Federal laws, International laws, Levels of culpability: Intent, Knowledge, Recklessness, Negligence Level and burden of proof: Criminal versus civil cases, CFAA, DMCA, CAN-Spam, etc.	

LAB COMPONENT CONTENTS

Suggested Topic of Experiments (Minimum 8 Experiments)

1. Analysis of forensic image
2. Network forensics
3. Data Carving
4. Windows Recycle Bin Forensics
5. Web Browser Forensics
6. RAM Forensic
7. USB Device Forensics
8. Timeline Report
9. Vulnerability Assessment and Penetration Testing
10. Email Analysis

One beyond curriculum experiment may be conducted (To be decided by the Subject Teacher)

Practical: 2 Hrs./Week		**Total Hours : 26 Hrs.**

Textbooks:

1. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, Tata McGrawHill
2. Nihad A. Hassan, “Digital Forensics Basics A Practical Guide Using Windows OS “, APress Publication
3. Xiaodong Lin,” Introductory Computer Forensics: A Hands-on Practical Approach‖”, Springer Nature,
4. Scene of the Cybercrime: Computer Forensics, Handbook 1st Edition, Kindle Edition

Reference Books:

1. Nilakshi Jain & Kalbande, “Digital Forensics”, Wiley Publication
2. Nina Godbole, Sunit Belapure, “Cyber Security”, Wiley Publication
3. Bill Nelson,Amelia Phillips,Christopher Steuart, “Guide to Computer Forensics and Investigations” . Cengage Learning
4. Marjie T. Britz, Computer Forensics and Cyber Crime, Pearson, Third Edition.

Mahavir Education Trust's

Shah & Anchor Kutchhi Engineering College

An Autonomous Institute Affiliated to University of Mumbai

UG Program in Computer Engineering

(Accredited by NBA for 3 years from AY 2022-23)

Course Code	Lab Name	Credits
CMDLOLR07041	**Digital Forensics Lab**	**1**

<table>
<tr><td colspan="2"><b>Continuous Internal Assessment Practical (CIAP):</b>
CIAP will be assessed for 50 marks on the following rubrics and scaled down to 10 marks</td></tr>
<tr><td>1</td><td>5 marks –Evaluation of write-up on day-to-day experiment in the laboratory (in terms of aim, components/procedure, expected outcome)</td></tr>
<tr><td>2</td><td>The Course In charge will choose any two of the below mentioned components, with each component having weightage of 20 marks each
Assignments/Tutorials/Power point presentation/Group discussion/Quiz/Seminar/Case studies/DesignThinking/Innovation/Creativity/Project/App development</td></tr>
<tr><td>3</td><td>Attendance will be having weightage of 5 marks</td></tr>
<tr><td colspan="2"><b>End Semester Examination (ESEP)</b></td></tr>
<tr><td>1</td><td>Based on the above contents and entire syllabus of CMCR0301
The End Semester Examination Practical shall be conducted for 100 marks for a duration of three hours and scaled down to 15 marks</td></tr>
<tr><td><b>Evaluation Method</b></td><td><b>Passing Requirement</b></td></tr>
<tr><td>Continuous Internal Assessment (CIAP)+End
Semester Examination (ESEP)</td><td>Obtained Marks ≥40 % of maximum marks</td></tr>
</table>

Course Outcomes (CO)

CO No.	**CO Statement** (At the end of the course, students will be able to …)	BL
1	Discuss the terminologies related to Digital forensics and computer security incident process.	
2	Describe and apply the process of collection, analysis and recovery of the digital evidence.	
3	Use the forensics investigation process for operating system, network and application programs.	
4	Discuss the different laws related to cyber crime.	

List of Experiments

Sr. No.	Title	CO	PO	PSO
1	Analysis of forensic image	1,2		
2	Network forensics	1,2		
3	Data Carving	1,2		
4	Windows Recycle Bin Forensics	3		
5	Web Browser Forensics	3		
6	RAM Forensic	3		
7	USB Device Forensics	3		
8	Timeline Report	1,2		
9	Implementing Stegnography and reverting the hidden message.	1,2		
10	Case Study			

Name and Signature:
Date:

Subject:

INDEX

Sr. No.	Title of Experiment/Assignment/Tutorial	Date of Performance	Date of Submission	Page No.	Marks	Initials of Teacher with Remarks

Marks

Evaluation of write-up on day-to-day experiment in the laboratory (in terms of aim, components/procedure, expected outcome)	**/05**
Assessment Method 1	**/20**
Assessment Method 2	**/20**
Attendance	**/05**

This is to certify that Shri/Kum ....………………. Batch.......................Roll No...Semester……………… has completed the specified CIAP in the subject of …………………………………..……………………………in a satisfactory manner in the college during the academic year of 20….. to 20……

Subject In-charge

Instructions for Students

1. For effective implementation and attainment of practical outcomes, in the beginning of each exercise, students need to read through the complete write-up.
2. Students ought to refer to reference books, lab manuals, etc.
3. Students should not hesitate to ask about any difficulties which they face while performing practical.
4. Algorithms & Flow graphs to be handwritten for programming subjects.

Guidelines for Faculties

1. There will be two sheets of blank pages after every practical for the student to report other matters (if any), which is not mentioned in the printed practical.
2. For difficult practical if required, teachers could provide the demonstration of the practical emphasizing of the skills which the students should achieve.
3. Teachers should give opportunities to students for hands-on work after the demonstration.
4. During the practical, ensure that each student gets a chance and takes active part in taking observation/readings and performing practical.

Experiment No. – 1				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 1

Analysis of forensic images

1.1 Aim: Analysis of forensic images using FTK Imager/Autopsy/Winhex.

1.2 Course Outcome:

- Discuss the terminologies related to Digital forensics and computer security incident process.
- Describe and apply the process of collection, analysis and recovery of the digital evidence.

1.3 Learning Objectives: To acquire a forensic image and perform the analysis on evidence.

1.4 Requirement: FTK Imager, Autopsy and Winhex

1.5 Related Theory:

- Image – The copy of a hard drive that is compressed into one file.
- Acquisition – The viewing of the image in a program in order to gather data and information.
- Data Compression – When the information from a hard drive or other form of storage is compressed together to take up less space on the computer.
- Verification – The information on the image is checked with the original information on the hard drive to make sure nothing was altered.

FTK Imager

FTKImager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence. After you create an image of the data, use Forensic Toolkit® (FTK®) to perform a thorough forensic examination and create a report of your findings.

Autopsy:

Autopsy® is the premier end-to-end open source digital forensics platform. Built by Basis Technology with the core features you expect in commercial forensic tools, Autopsy is a fast, thorough, and efficient hard drive investigation solution that evolves with your needs.

Winhex:

WinHex is a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security. An advanced tool for everyday and emergency use: you can inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.

1.6 Procedure:

FTK imager

https://accessdata.com/product-download/ftk-imager-version-3-2-0

Autopsy

https://www.autopsy.com/download/

Winhex

https://winhex.en.softonic.com/

- **FTK imager**

Acquire volume image (using Create disk image option)

1. Open FTK Imager
2. Create disk image
3. Select source
4. Select Drive
5. Click Add... to add the image destination
6. Select Image Type
7. Fill evidence information
8. Select image destination folder
9. Check verify images after they are created

Report is generated after Image creation

Read/View Evidence image file

1. File -> Add Evidence item
2. Evidence Source Selection
3. View Evidence image

Image Mounting

Image Mounting allows forensic images to be mounted as a drive or physical device, for read-only viewing.

Step 1: FTK Imager -> File -> Image Mounting

Step 2: This action opens the image as a drive and allows you to browse the content in Windows and other applications. Supported types are RAW/dd images, E01, S01, AFF, AD1, and L01.

Verify Drive/Image

Select mounted image file

Click on verify Drive/Image

Drive/Image verify results

- **Autopsy:**

1. Install it and run as an Administrator
2. Select New Case Information
3. Select type of Data source to add
4. Image created
5. Select Image

6. Analyzing emails
7. Report Generation

- **Winhex**

Open and Authenticate the Image File from WinHex

1. From the File menu in WinHex, select Open.
2. Find the CatPlus.e01 file that you put in your case folder on your C drive.
3. Click on the Open button.
4. From the Tools menu, select Compute Hash.
5. Select the MD5 (128-bit) hash algorithm and let the computer make the calculation.
6. Copy and paste the results (the hash) into your activity log.

Analyze the Physical View

1. You‟re looking at the data exactly as it was on the evidence disk. This is called as physical view.

1. The middle section of the display shows the contents of the disk. Each row displays 16 bytes of data, expressed in hexadecimal. (Hexadecimal means the base-16 number system. It's often just called hex.) The first byte, byte 0, is EBh (The h means hex).

2. The left section shows the offset (distance from the beginning expressed in hex) of the first byte in the row shown in the middle section. For example, the first byte in the 4th row is offset 30h. (Note that offset 30h means [3 x 16] + [0 x 1] or 48 in decimal. You're looking 48 bytes into the data.)

3. The right section interprets each row of 16 bytes using the ASCII character set. Many hex values cannot be represented by ASCII symbols; these are shown with a dot.

2. In your activity log, jot down any suspicious or other relevant information that you notice in the Physical View. You may have to scroll down to see anything legible.

Analyze the Logical View

1. To see a logical view of the data that was on the original disk, go to the Specialist menu in WinHex and select Interpret Image File As Disk. (If the menu item is grayed out, then you are already interpreting the image file as disk.)

2. Interpreting as disk lets you see files and directories (folders), even files and

directories that the user deleted. (WinHex shows deleted files and directories in a paler color.) The bottom portion of the window should still show the physical view (offset, hex values, and ASCII values) with an added "Access" menu.

3. Whenever you look at a file in a new way, it's a good idea to authenticate the file again (recalculate the hash), to ensure you haven't tainted the evidence. So calculate the hash again and jot it down in your activity log.

4. In the top section of WinHex, which shows the logical view, you may notice duplicated file and directory names. If you do, jot this down in your activity log with a possible explanation. (Perhaps the suspect kept multiple versions of the files and directories as he worked?)

5. What files were deleted but then never created again (there is no new version?) Jot this down in your activity log.

Analyze and Recover a Deleted File

1. Scroll down in the logical view to the Copy of abc.jpg file. The user deleted this file, but notice that its size is not zero! How big is it? (Number of kilobytes (KB)? Jot this down in your activity log.
2. Right click on Copy of abc.jpg and select Go to beginning of file.
3. What is the offset of the beginning of this file (in hex)? Include the question and answer in your activity log.
4. What are the first four bytes of the file (in hex)? Include the question and answer in your activity log. The first four bytes of a file often hold a "file signature," which identifies the type of file. We'll learn more about file signatures next week.
5. Right click on Copy of abc.jpg in the logical view again.
6. Select Recover/Copy and save the recovered file in your case folder on your C drive.

Authenticate the Recovered File

1. The recovered file is now a new piece of evidence. Authenticate it immediately using the following procedures.
2. From the WinHex File menu, select Open. Find the recovered file in your case folder and click the Open button.
3. From the Tools menu, select Calculate Hash.

4. Select the MD5 (128-bit) hash algorithm and let the computer make the calculation.

5. Copy and paste the results (the hash) into your activity log (with a note about what it is, e.g. the MD-5 hash of the recovered file).

6. Close the file.

Examine the Recovered File

1. Open the file from Windows.

2. From the Start Menu, go to MyComputer and navigate to your case folder on your C drive.

3. Double click on the icon for your recovered file.

4. Document your conclusions about the contents of the file and its usefulness in the criminal case.

End Your Session

1. Back in WinHex, open the recovered file again and verify that you didn't change it (Calculate the hash).

2. Also calculate the hash for the original image file to prove that you didn't taint it.

3. Copy and paste the results in your activity log.

4. Quit WinHex.

1.7Program and Output:

1.8Conclusion:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

…………………………………………………………………………

1.9 Review Questions based on Experiment:

Experiment No. – 2				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 2

Network forensics

2.1 Aim: Network forensics using Network Miner.

2.2 Course Outcome:

- Discuss the terminologies related to Digital forensics and computer security incident process.
- Describe and apply the process of collection, analysis and recovery of the digital evidence.

2.3 Learning Objectives: To monitor and analyze computer network traffic using Network Miner.

2.4 Requirement: Network Miner

2.5 Related Theory:

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information.

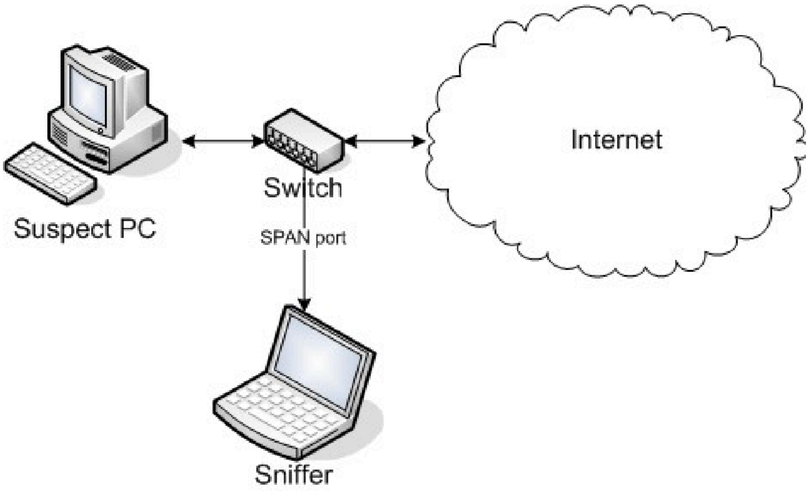
• When performing digital evidence collection from a stand alone computer
– Acquire data in transit (network traffic dump)
– Acquire data in use (RAM image)
– Acquire data at rest (hard drive image)
• A corporate incident response team has discovered network traffic that violates the law

Connecting a Network Sniffer

• SPAN/mirror port

– Re-configuration of switch

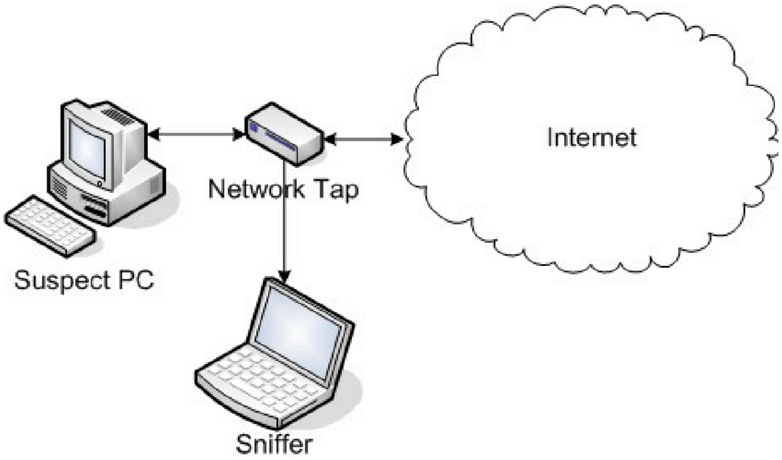
– Free port on switch



• **Network Tap**

– Special hardware

– No configuration



Capturing Network Traffic

dumpcap -i 1 -f "host 213.1.2.3" –w wiretap.pcap -b filesize:100000

Analyzing Network Traffic

- **Using Wireshark**

http://www.wireshark.org/

In the scope of a digital forensics-based investigation, Wireshark can be immensely helpful, especially in finding and displaying emails that could be potential evidence. For example, Wireshark can be used to catch a suspect who is stealing a victim's wireless Internet to make fraudulent online purchases. By using Wireshark as a network monitoring tool, it is possible to find the IP or MAC address of the suspect, and to see what sites he or she is visiting. Additionally, it may be possible to recover emails and other potentially sensitive and incriminating information that the suspect is sending over the network. When used in conjunction with other forensics tools, such as aircrack_ng (a tool that concentrates on examining wireless traffic versus Ethernet), it is possible to enhance the usefulness of Wireshark to make it an effective forensic network analysis tool.

Using NetworkMiner

http://networkminer.sourceforge.

NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

2.6 Procedure:

Case #1

Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company's prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company's secret recipe.

Security staff have been monitoring Ann's activity for some time, but haven't found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann's computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

"We have a packet capture of the activity," said security staff, "but we can't figure out what's going on. Can you help?"

http://forensicscontest.com/contest01/evidence01.pcap

You are the forensic investigator. Your mission is to figure out who Ann was IM-ing, what she sent, and recover evidence including:

1. What is the name of Ann's IM buddy?
2. What was the first comment in the captured IM conversation?
3. What is the name of the file Ann transferred?
4. What is the magic number of the file you want to extract (first four bytes)?
5. What was the MD5sum of the file?
6. What is the secret recipe?

Case 2:
After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town. "We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The packet capture may contain clues to her whereabouts."
Pcap file: http://forensicscontest.com/contest02/evidence02.pcap
You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including

1. What is Ann's email address?
2. What is Ann's email password?
3. What is Ann's secret lover's email address?
4. What two items did Ann tell her secret lover to bring?
5. What is the NAME of the attachment Ann sent to her secret lover?
6. What is the MD5sum of the attachment Ann sent to her secret lover?

7. In what CITY and COUNTRY is their rendez-vous point?
8. What is the MD5sum of the image embedded in the document?

2.7Program and Output:

2.8Conclusion:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………

2.9 Review Questions based on Experiment:

Experiment No. – 3				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 3

Data Carving

3.1 Aim: Use data carving tools and software to extract and recover different types of files.

3.2 Course Outcome:

- Discuss the terminologies related to Digital forensics and computer security incident process.
- Describe and apply the process of collection, analysis and recovery of the digital evidence.

3.3 Learning Objectives: To apply data carving methods in forensic investigations to retrieve evidence from compromised or formatted storage devices.

3.4 Requirement: Foremost, Scalpel

3.5 Related Theory:

Data carving is an advanced type of data recovery, usually used in digital forensic investigations to extract a particular file (using file's header and footer information) from unallocated space (raw data) without the assistance of any file system structure (e.g., MFT).

Data carving can be the only method to recover important evidence files and fragments of files in a criminal investigation where the file system that was originally responsible for organizing these files on the hard drive is missing or corrupted. Data carving is also needed when extracting a file(s) from a captured network traffic stream.

Data carving is an advanced technique in digital forensics and is beyond this book's scope. However, you should know that expert forensic examiners can extract (recover) structured data, and hence a file like a document or photo, out of non structured data or raw data using data carving techniques.

FILE CARVING WITH A HEX EDITOR

File carving can be conducted using only a Hex editor; however, there are some tools that can aid examiners. The following are some free tools for conducting file carving:

1. Foremost (http://foremost.sourceforge.net)

2. Scalpel (https://github.com/sleuthkit/scalpel)

3.6 Procedure:

Foremost

Foremost is a forensic data recovery program for Linux used to recover files using their headers, footers, and data structures through a process known as file carving. Although written for law enforcement use, it is freely available and can be used as a general data recovery tool.

Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. It can recover several file types Steps:

1. Create an empty folder e.g mkdir recover.
2. Go to that directory and give the command foremost -h to display all options
3. Save your image file in a folder say /mnt/sdb1.dd
4. From the shell type
5. Foremost –v -T –t all –i /mnt/sdb1.dd –o /root/Desktop/recover

To recover only specific files

```
Foremost –v -T –t pdf,jpg –i /mnt/sdb1.dd –o /root/Desktop/recover
```

Scalpel

Scalpel is an improved version of the file carver Foremost. Scalpel carves files in two phases. In the first phase, Scalpel searches the disk image to determine the location of headers and footers. This phase results in a database which contains the metadata. Synthetic names are assigned to the carved files in the generated metadata database. The second phase of Scalpel uses the metadata database created in the first phase to carve files from the corrupted disk and write these carved files to a new disk.

Steps

1. The conf file is placed in folder /etc/scalpel
2. Run nano /etc/scalpel/scalpel.conf
3. Uncomment the file types you would like to recover
4. Now save the conf file
5. Create a folder scalp in /root/Desktop
6. Save the raw image file in

folder /mnt #scalpel /mnt/sdb1.dd –o /root/Desktop/scalp

3.7Program and Output:

3.8Conclusion:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

…………………………………………………………………………

3.9 Review Questions based on Experiment:

Experiment No. – 4				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 4

Windows Recycle Bin Forensics

4.1 Aim: To investigate the forensic analysis of the Windows Recycle Bin, enabling the recovery and examination of deleted files.

4.2 Course Outcome:

Use the forensics investigation process for operating system, network and application programs.

4.3 Learning Objectives:

- Understand the structure and functionality of the Windows Recycle Bin.
- Identify and interpret the metadata associated with deleted files in the Recycle Bin.
- Use forensic tools and techniques to recover files from the Recycle Bin.
- Analyze recovered files to determine their origin, deletion time, and potential relevance in an investigation.

4.4 Requirement: $I Parse tool

4.5 Related Theory:

The Windows recycle bin contains files that have been deleted by users but still exist within the system. For instance, when a user deletes a file (using the standard delete button on the keyboard after selecting the target file OR selecting a file, right-clicking it, and choosing “Delete” from the pop-up menu), Windows moves the subject file to the recycle bin without deleting it permanently. This is the default behavior of Windows; however, a user can configure the recycle bin settings to permanently delete files without moving them into the recycle bin; besides, some users press and hold the Shift key when deleting a file to delete it permanently without moving it into the recycle bin. In practice, few people employ permanent deletion of recycled files (or even know about it); this makes it possible for the recycle bin to hold important recycled artifacts, which are considered a valuable source for digital evidence.

When a user deletes a file, the default behavior of Windows is to move it into the recycle bin. Different versions of Windows have different recycle bin file names and locations.

4.6 Procedure:

For Windows XP (formatted using the FAT file system), deleted files are stored in the “Recycler” folder in the root directory where Windows is installed (usually the C:\ drive), which in turn holds another important file named “INFO2.”Both “Recycler” and “INFO2” are hidden files: you must first display hidden files—including OS files—to display them.

Inside the “Recycler” folder, we can see one or more folders; these folders are named according to each user’s specific security identifier (SID) (e.g., S-1-5-21-2602240047-739648611-3566628919-501); if a system has more than one user, then each one will have its own folder that stores the deleted files belonging to that user account.

There is also another important file inside each user recycle bin folder called “INFO2”; this file contains an index of all the files that have been previously deleted by the user. It also contains metadata about each deleted file like its original path, file size, and date/time when it was deleted.

Note! When you delete a file from a removable media or mapped network path,it will bypass recycle bin and be cleared permanently.

With Vista and beyond (7, 8, 8.1, and 10), Windows has changed both the recycle bin main folder and the way deleted files are organized. For instance, deleted files are stored in a folder named “$Recycle.Bin,” under which there is a subfolder for each user on the system named using that user’s SID. The “$Recycle.Bin” is stored under the C:\ drive (assuming Windows is installed there).

Now, in these modern versions of Windows,when a file is deleted, Windows will move it into the recycle

bin as two files: one contains the actual data of the recycled file (its name begins with "$R"), while the other contains the deleted file's metadata (its name begins with "$I").
Obviously, this discards the need for the "INFO2" file from older Windows versions, which was used to store recycled a file's metadata.

Note! The Windows recycle bin has limited storage capacity with regard to the volume of deleted files that it can accommodate. In Windows XP, the recycle bin is configured by default to hold 10% of hard drive; if it fills up to maximum capacity, it will delete the old files to make room for incoming deleted files. In newer Windows versions like Vista and later, the default size is 10% of the first 40GB of the drive and 5% of the remaining storage space that is above 40GB.

Deleting a file and analyzing it using Windows 10 and a free tool called $I Parse.

Open a command-line prompt; use the CD command to change the working directory into the $Recycle.Bin folder under the C:\ drive. Display the folder contents using the DIR command followed by the /a switch (to display hidden system files).

$Recycle.Bin contains four subfolders: these are SID subfolders and correspond to the SID of the user who deleted the file. Each subfolder is created the first time a user deletes a file that is sent to the recycle bin.
Now, to learn the name of the user account which owns a specific SID subfolder, we need to use
the following command:
wmic useraccount get name,sid

This will display all user accounts on the target machine, so now we can learn which SID subfolder in the Recycle.Bin belongs to the target user.After knowing which recycle bin belongs to the target account, we can access it using the CD
command. Use the DIR command with the /a switch to display its contents
The target recycle bin has four files belonging to two deleted files. Each deleted file has two files in the recycle bin, a metadata file and the actual data (recoverable data) of the deleted file.

Now, let us investigate the deleted file's metadata, also known as index files (begin with $I), in the recycle bin of Windows Vista and later using a free tool called $I Parse. To use this tool follow these steps:

1. Go to https://df-stream.com/recycle-bin-i-parser/ and download the tool and extract its contents (if it is zipped).

2. To use this tool, we need first to extract the recycled file metadata file. To do this, type the following in the command prompt: copy $I* \users\nihad\desktop\recover

3. Execute the $I Parse tool, go to File menu ➤ Browse..., and select the folder that contains metadata files. Note! If you want to analyze only one file at a time, select File ➤ Choose... instead.

4. From the main program menu, click the Choose... button and select where to save the output file (a file with CSV extension that will hold parsing results)

5. Finally, click "Create CSV"; a success window will appear after parsing all files is finished, and you are done!

Now, go to where you have saved the output file (in our case, it's named output.csv) and open it to view a list of all recycled files names in the target recycle bin along with all file metadata information (original path, deletion date/time, and file size). Output.csv shows that information existed within subject recycled files' metadata files

To extract information from the recycled files' metadata files (INFO2 files) under Windows XP (and other ancient versions of Windows like 95, NT4, and ME since 0.7.0), you can use "Rifiuti2" (https://abelcheung.github.io/rifiuti2).

4.7Program and Output:

4.8Conclusion:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

………………………………………………………………………………

4.9 Review Questions based on Experiment:

Experiment No. – 5				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 5

Web Browser Forensics

5.1 Aim: To investigate and analyze web browser artifacts to uncover user activity and digital evidence.

5.2 Course Outcome:

Use the forensics investigation process for operating system, network and application programs.

5.3 Learning Objectives:

- Understand the types of data stored by web browsers, such as browsing history, cookies, cache, and downloads.
- Identify the locations of web browser artifacts on different operating systems.
- Utilize forensic tools to extract and analyze web browser data.
- Interpret the extracted data to reconstruct user activities and potential security incidents.

5.4 Requirement:

DB Browser for SQLite (DB4S) is a high quality, visual, open source tool to create, design, and edit database files compatible with SQLite.

Download DB Browser for SQLite (http://sqlitebrowser.org). We can browse target sqlite database tables and their content using this tool

5.5 Related Theory:

With the help of Browser Forensics and with the assistance of forensics tools one can extract sensitive data and chosen keywords from most web browsers. One can retrieve deleted data and keywords, check whether history was cleared, retrieve artifacts like Cookies, Downloads data, History, Saved Password, websites visited etc. Also, Browser Forensics helps a lot to understand how an attack on a system was conducted, helping in finding the source of Malwares/Adwares/Spywares, Malicious Emails and Phishing Websites etc. There are many web browsers available like Chrome, Firefox, Safari, IE, Opera etc. depending upon the platform being used

Google chrome artifacts

An artifact is a remnant or trace left behind on the computer which helps to identify the source of malicious traffic and attack conducted onto the system. Few examples include cache data, History, Downloads etc.

1. Profile Path – This contains the majority of the artifacts and profile data of the user.
2. Downloads + Navigation History + Search History – This is stored in SQLite Database location
3. Cookies – This is also stored in SQLite Database form Database location
4. Cache
5. Bookmarks
6. Form History – Stored in SQLite Database Form
7. Favicons – Stored in SQLite Database Form
8. Logins – Stored in SQLite Database Form
9. Sessions Data

5.6 Procedure:

Google Chrome Forensics using DB Browser for SQLite

Google Chrome is the fastest and most used web browser on desktop computers worldwide today;most digital forensics examiners will likely come across this browser in one of their investigations. Google Chrome is based on Chromium, which is an open source browser project developed by Google.

Most web browsers that are based on the Chromium project are going to store data in a similar way; this fact allows examiners to use the same investigative techniques used with Google Chrome to investigate these browsers, making investigating Google Chrome act as a standard template for most Chromium-based web browsers.

Similar to other web browsers, Chrome (developed by Google Inc.) stores its configuration settings and user private information in SQLite databases; these databases are files without extensions, so do not get confused on how to open them when using SQLite browser. Just navigate to target the Google Chrome profile folder and make sure that the option "All files (*)" is selected as appears in Figure 9.1; then select the file you want to examine.

The Google Chrome profile is where Google Chrome stores its configuration settings, apps, bookmarks, and extensions. Google Chrome can have more than one profile; however, there is also a default profile that can be found at \Users\<UserName>\AppData\Local\Google\Chrome\User Data\Default

If there is more than one profile in Google Chrome, each profile will have its own folder where browser settings and user (profile owner) private data (e.g., passwords,browsing history, bookmarks, etc.) is stored. Google Chrome does not name any additional profile according to its username; instead, it uses a generic name (e.g.,Profile 1, Profile 2, and so on). The location of additional Chrome profiles can be found here:
\Users\<UserName>\AppData\Local\Google\Chrome\User Data\Profile x
(x could be any positive integer number beginning from 1).

To know the folder location of any Google Chrome profile (see Figure 5.2), just open a Chrome window that shows profile name/image in the top corner of the browser window, type the following in the browser address bar, and finally press the Enter button:

chrome://version

Then check the “Profile Path” in the resulting window. Now that we know how to access Google Chrome profile(s) folder, let us begin investigating the files contained within it.

Note! We are using Google Chrome Version 69 (official build; 64 bit) and the default profile folder located at \Users\<UserName>\AppData\Local\Google\Chrome\User Data\Default during our coming experiments.

History

Google Chrome store user browsing history, downloads, keywords, and search terms in the “History” database file are located under the Chrome user’s profile. This file can be examined using DB Browser for SQLite. Note that there are 12 tables in this file and 11 indices.

To know when a particular file has been downloaded in addition to much information related to download history, go to the “Downloads” table under the “Browse Data” tab (see Figure 5.4). The DB Browser for SQLite displays time information using Google Chrome values stamps (also known as the Webkit format, which points to the number of microseconds passed since 00:00:00 UTC of Jan 1, 1601). To convert it into a readable form, use the DCode tool.

Nirsoft offers a tool to reveal Chrome history; it is called ChromeHistoryView (www.nirsoft.net/utils/chrome_history_view.html). This tool reads the “History” file of the Google Chrome web browser.

Cookies

Google Chrome stores cookies information in the “Cookies” file located under the Chrome user’s profile; we can view “Cookies” file contents using DB Browser for SQLite,as we did with the “History” file before, to show detailed information about saved Chrome cookies

5.7Program and Output:

5.8Conclusion:

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

……………………………………………………………………………

5.9 Review Questions based on Experiment:

<table>
<tr><td colspan="5"><b>Experiment No. – 6</b></td></tr>
<tr><td><b>Date of Performance:</b></td><td colspan="4"></td></tr>
<tr><td><b>Date of Submission:</b></td><td colspan="4"></td></tr>
<tr><td>Program Execution/formation/ correction/ethical practices (06)</td><td>Timely Submission (01)</td><td>Viva (03)</td><td>Experiment Total (10)</td><td>Sign with Date</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Experiment No. 6

RAM Forensic

6.1 Aim: To investigate and analyze volatile memory (RAM) to uncover valuable digital evidence and understand system activities.

6.2 Course Outcome:

Use the forensics investigation process for operating system, network and application programs.

6.3 Learning Objectives:

To capture an image of RAM of victim Machine
Use a Volatility tool to analyze memory images to find traces of an attack.

6.4 Requirement: Dumpit and Volatility

6.5 Related Theory:

RAM capture is the process of capturing live memory from a running computer system. RAM analysis consists of performing forensic analysis on the data gathered from the live computer.

After conducting a memory dump on any live machine to capture RAM, the memory image can be used to determine information about running programs, the operating system, and the overall state of a computer, as well as to locate deleted or temporary information that might otherwise not be found on a normal image.

Until recently, RAM analysis and capture was not a mandatory step in investigations, or even in triage situations where analysts were attempting to gather forensic data on site.

However, with new tools that allow entry into locked systems and with the growing importance of temporary files, RAM analysis is quickly becoming a pivotal and mandatory part of the digital forensics process.

Volatile memory access is useful in law enforcement situations where data would be lost by powering off a suspect machine. The longer a machine is off, the more data becomes lost. The following can be found using RAM capture: Processes, Network connections, Open files /Configurations/Encryption keys,Open/Active Registry keys,Exploit-related information,Zero-day attacks and root-kits, and kernel-level structures.

RAM Analysis Tools:

Volatility: A tool capable of analyzing RAM from a memory dump disk image.

Volix : Tool that provides GUI for Volatility.

RAM Capture Tools:

Dumpit :

DumpIt is a fusion of two trusted tools, win32dd and win64dd,combined into one one executable. DumpIt is designed to be provided to a non-technical user using a removable USB drive. The person needs to simply double-click the DumpIt executable and allow the tool to run. DumpIt will then take the snapshot of the host's physical memory and save it to the folder where the DumpIt executable was located.

DumpIt provides a convenient way of obtaining a memory image of a Windows system even if the investigator is not physically sitting in front of the target computer. It's so easy to use, even a naïve user can do it. It's not appropriate for all scenarios, but it will definitely make memory acquisition easier in many situations.

6.6 Procedure:

Step 1: Download Dumpit

Step 2: extract the files and click on the Dumpit.exe file, press y to proceed

Steps in RAM Analysis :

1. Capturing RAM memory image
2. Gather additional information about system using captured RAM image

1. Capturing Memory Image on Windows:
DumpIt : A program that can be installed on any Windows machine in order to capture local RAM from that computer. This is oftentimes a tool of choice for triage forensics.

2. Gathering additional information using Volatility tool
Volatility is a memory forensics framework, to analyze ram memory dumps for Windows, Linux, and Mac.It can analyze raw dumps, crash dumps, VMware dumps, virtual box dumps, and many others.

Steps to analyze a windows machine RAM image using Volatility:
Open a new terminal window and enter the following commands in order to launch the volatility shell.
Enter the following commands to find basic data about the machine on which the A memory dump was conducted.

```
c:\Users\vaish\Downloads\volatility-2.2.standalone.exe -f filename.raw imageinfo
```

This command gives you several pieces of information. At this point, we only need to know the profile type of memory dump, in this case Win10Home.We will use this in next few steps.

```
c:\Users\vaish\Downloads\volatility-2.2.standalone.exe -f filename.raw --profile=Win10Home kdbgscan
```

Copy offset(v) location

```
c:\Users\vaish\Downloads\volatility-2.2.standalone.exe -f filename.raw --profile=Win10Home
--kdbg=offsetvalue pslist
```

To copy the pslist to some file

```
c:\Users\vaish\Downloads\volatility-2.2.standalone.exe -f filename.raw --profile=Win10Home
--kdbg=offsetvalue pslist > proc.txt
```

To view the file (at the prompt run)

```
Notepad proc.txt
```

To view the network scan details

```
c:\Users\vaish\Downloads\volatility-2.2.standalone.exe -f filename.raw --profile=Win10Home --kdbg=offsetvalue netscan
```

To copy the netscan entries

```
c:\Users\vaish\Downloads\volatility-2.2.standalone.exe -f filename.raw --profile=Win10Home --kdbg=offsetvalue netscan > netscan.txt
```

6.7Program and Output:

6.8Conclusion:

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

……………………………………………………………………………

6.9 Review Questions based on Experiment:

Experiment No. – 7				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 7

USB Device Forensics

7.1 Aim: To investigate and analyze USB devices to uncover user activities and digital evidence.

7.2 Course Outcome:

Use the forensics investigation process for operating system, network and application programs.

7.3 Learning Objectives:

- Identify the types of data that can be extracted from USB devices, such as file transfers, usage history, and device metadata.
- Utilize forensic tools and techniques to capture and analyze data from USB devices.

7.4 Requirement:

USBDeview (www.nirsoft.net/utils/usb_devices_view.html)

USB Detective (https://usbdetective.com)

7.5 Related Theory:

Windows keeps a history log of all previously connected USB devices along with their connection times in addition to the associated user account which installs them. The Windows registry also stores important technical information for each connected USB device such as vendor ID, product ID, revision, and serial number.

Windows stores USB history-related information using five registry keys, where each key offers a different piece of information about the connected device. By merging this information together, investigators will have an idea of how an offender has used removable devices such as a USB to conduct/facilitate his/her actions.

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR Here you will find all USB devices that have been plugged into the operating system since its installation. It shows the USB vendor ID (manufacturer name), product ID, and the device serial number (note that if the second character of the device serial number is “&,” it means the connected device does not have a serial number and the device ID has been generated by the system).

2. HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices The MountedDevices subkey stores the drive letter allocations; it matches the serial number of a USB device to a given drive letter or volume that was mounted when the USB device was inserted.

3. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 This key will record which user was logged into Windows when a specific USB device was connected. The key also includes the “Last Write Time” for each device that was connected to the system.

4. HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Enum\Usb This key holds technical information about each connected USB device in addition to the last time the subject USB was connected to the investigated computer.

5. Identify the first time the device was connected: Check this file at \Windows\inf\setupapi.dev.log for Windows Vista, 7, and 8, and at \Windows\inf\setupapi.upgrade.log for Windows 10. On Windows XP, this file will be located at \Windows\setupapi.log. Search in this file for a particular USB device’s serial number to learn when it was first connected to the subject system (in local time).

7.6 Procedure:

To automate the process of finding information about the current and previous USB connected devices, you can download a free tool by Nirsoft that can perform all the tasks we just did manually; this tool is called USBDeview (www.nirsoft.net/utils/usb_devices_view.html). After executing this tool on the target system, extended information (e.g., device name/description, device type, serial number, and much more) about each connected USB device will appear. The Last Plug/Unplug Date represents the first time that the device was connected to the system. This date does not change when the same device is repeatedly reinserted. The“Created Date” represents the last time that the same device was attached to the system.

Unfortunately, not all USB device types will leave traces in Windows registry as we have described, for instance, USB devices that use media transfer protocol (MTP) when connecting with computers. Devices equipped with the modern Android OS versions in addition to Windows phones and Blackberry all use the MTP protocol; this protocol does not leave traces in the Windows registry when a USB device is connected to a Windows computer. This necessitates a specialized tool to handle the investigation of such artifacts.

USB Detective (https://usbdetective.com) supports detecting USB devices that use the MTP protocol to connect to Windows. It also offers rich features for thoroughly investigating connected USB devices, like creating timelines of all unique connection/disconnection and deletion timestamps for each device.

7.7Program and Output:

7.8Conclusion:

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

……………………………………………………………………………………

7.9 Review Questions based on Experiment:

<table>
<tr><th colspan="5">Experiment No. – 8</th></tr>
<tr><td><b>Date of Performance:</b></td><td colspan="4"></td></tr>
<tr><td><b>Date of Submission:</b></td><td colspan="4"></td></tr>
<tr><td>Program Execution/formation/ correction/ethical practices (06)</td><td>Timely Submission (01)</td><td>Viva (03)</td><td>Experiment Total (10)</td><td>Sign with Date</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Experiment No. 8

Timeline Report

8.1 Aim: To generate a comprehensive timeline report using Autopsy, enabling the reconstruction of digital events and activities.

8.2 Course Outcome:

Discuss the terminologies related to Digital forensics and computer security incident process.

Describe and apply the process of collection, analysis and recovery of the digital evidence.

8.3 Learning Objectives: To develop skills in documenting and reporting findings from the timeline analysis to support forensic investigations and incident response.

8.4 Requirement: Autopsy

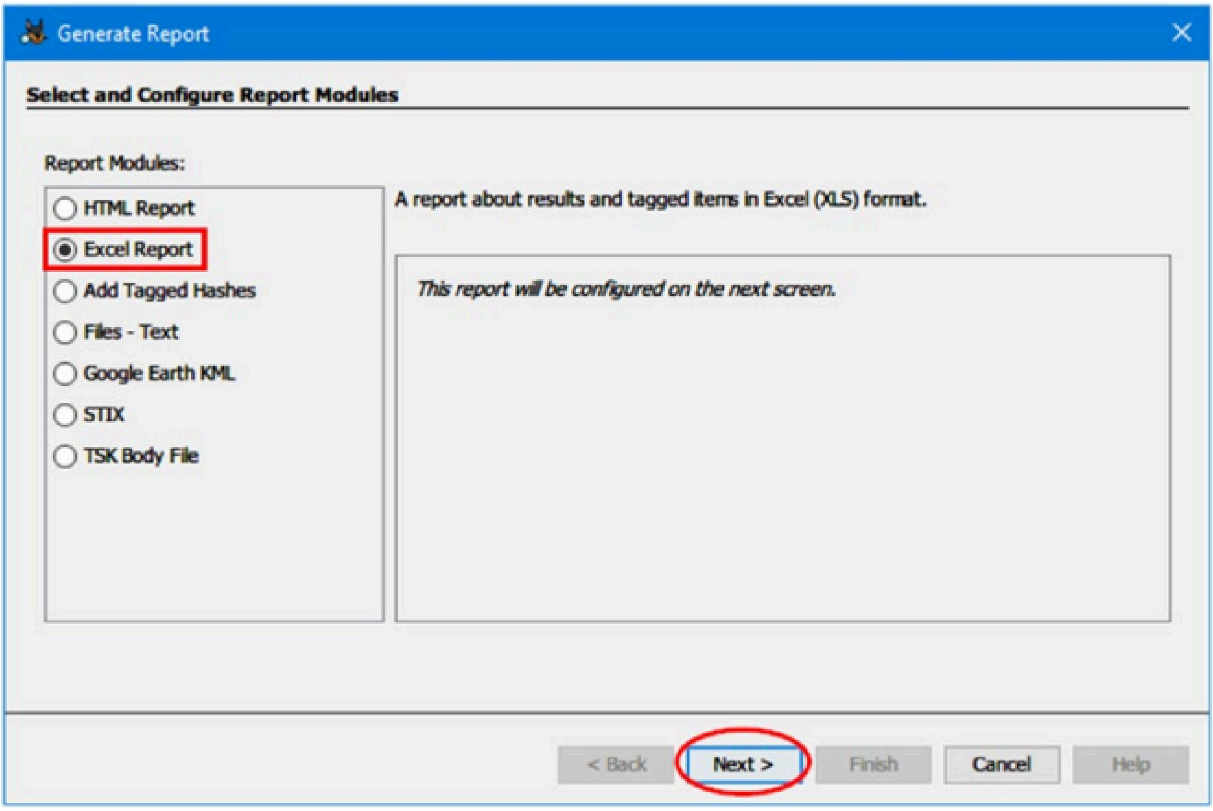
8.5 Related Theory:

Autopsy allows you to generate a report—in HTML, Excel, text, and other formats—that contains time information of every file in the supplied forensic image. This feature opens possibilities to use such information in other programs outside Autopsy.

8.6 Procedure:

To generate a timeline report using Autopsy, follow these steps:

1. Go to Tools menu ➤ Generate Report. The Generate Report wizard appears; the first window allows you to select the report format (see Figure 8.1).



Generate Report

Select and Configure Report Modules

Report Modules:

○ HTML Report
● Excel Report
○ Add Tagged Hashes
○ Files - Text
○ Google Earth KML
○ STIX
○ TSK Body File

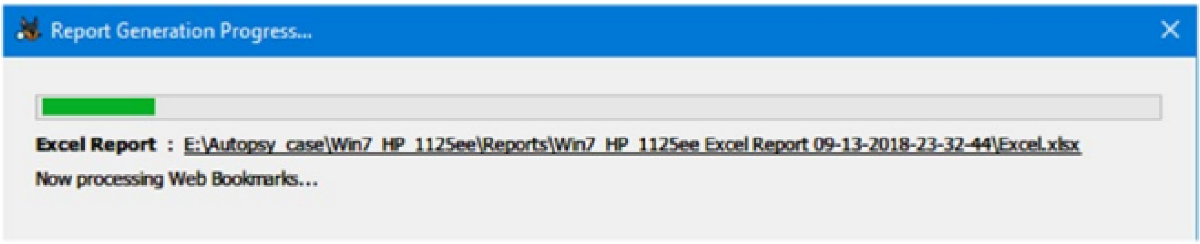
A report about results and tagged items in Excel (XLS) format.

This report will be configured on the next screen.

Figure 8.1. Select report format for your generated timeline in Autopsy

2. In our case, we select "Excel Report," so we can play with the data using the MS Excel spreadsheet program or any other alternative program that can read Excel files like Apache OpenOffice (www.openoffice.org). Click "Next" to continue.

3. The next window asks you to configure the returned results. You have two options: All Results and Tagged Results. In our case, we will select all results and click "Finish"; then, Autopsy will begin the report generation process (see Figure 8.2).



Report Generation Progress...

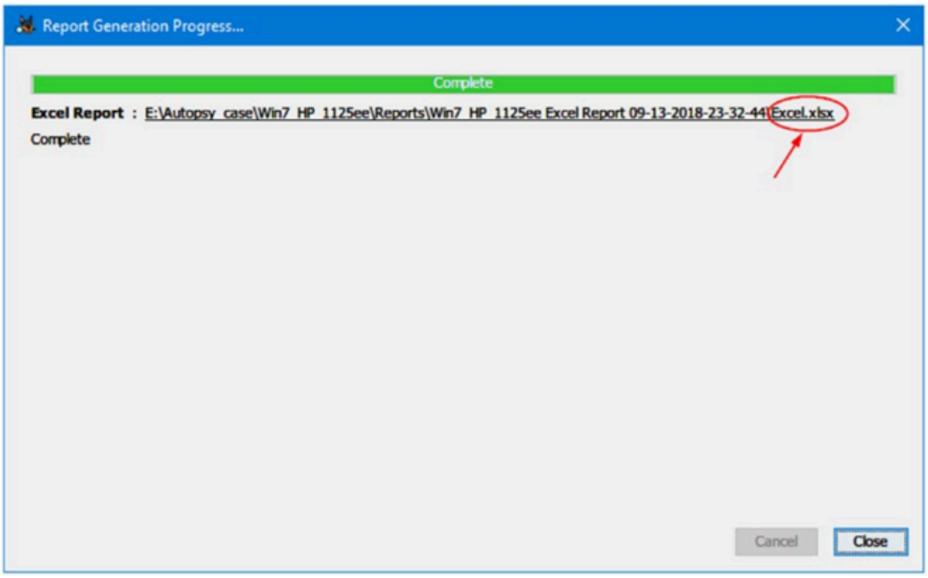
Excel Report : E:\Autopsy case\Win7 HP 1125ee\Reports\Win7 HP 1125ee Excel Report 09-13-2018-23-32-44\Excel.xlsx

Now processing Web Bookmarks...

Figure 8.2 Report Generation Progress window

4. After it finishes generating the report, Autopsy will show you the link where your generated report is saved; click over this link to open the file using your default program (see Figure 8.3).

5. Finally, click “Close” to close the Report Generation Progress window.



Report Generation Progress...

Complete

Excel Report : E:\Autopsy case\Win7 HP 1125ee\Reports\Win7 HP 1125ee Excel Report 09-13-2018-23-32-44\Excel.xlsx

Complete

Figure 8.3. The location of Autopsy-generated report

RETRIEVING LAST SEVEN DAYS OF ACTIVITY USING AUTOPSY

Please note that as a part of Autopsy’s initial analysis, it will list the last seven days of activity—of web browsers (including web searches), installed programs, operating system, and recent changes to registry hives—of the supplied forensic image files in the Data Explorer panel under the “Extracted Content” section (see Figure 8.4). Remember that you need to activate the “Recent Activity” ingest module in order to retrieve this result.

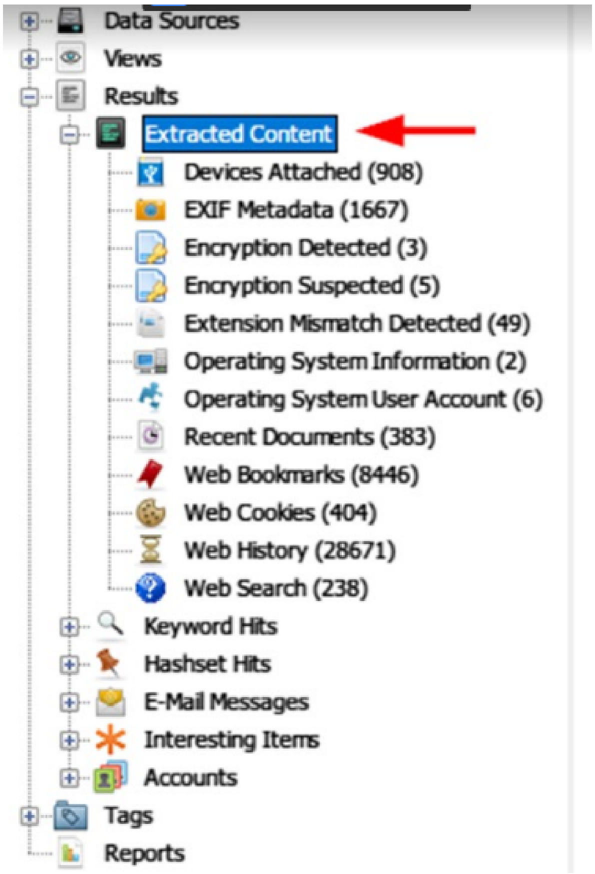


Figure 8.4. Viewing the results of "Recent Activity" module: you must activate the "Recent Activity" ingest module to view this info.

8.7Program and Output:

8.8Conclusion:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

…………………………………………………………………………

8.9 Review Questions based on Experiment:

Experiment No. – 9				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 9

Vulnerability Assessment and Penetration Testing

9.1 Aim: To conduct a comprehensive vulnerability assessment and penetration testing (VAPT) to identify and mitigate security weaknesses in a target system.

9.2 Course Outcome:

Discuss the terminologies related to Digital forensics and computer security incident process.

Describe and apply the process of collection, analysis and recovery of the digital evidence.

9.3 Learning Objectives:

- To identify security vulnerabilities in networks, applications, and systems.
- To perform systematic penetration testing to exploit identified vulnerabilities and assess the potential impact on the target system.
- To develop strategies to mitigate discovered vulnerabilities and enhance the overall security posture of the target environment.

9.4 Requirement: BurpSuite

9.5 Related Theory:

Vulnerability Assessment and Penetration Testing (VAPT) is a methodological approach to improving an organization’s security posture by identifying, prioritizing, and mitigating vulnerabilities in its infrastructure. It also helps organizations stay compliant with various industry standards throughout the year.

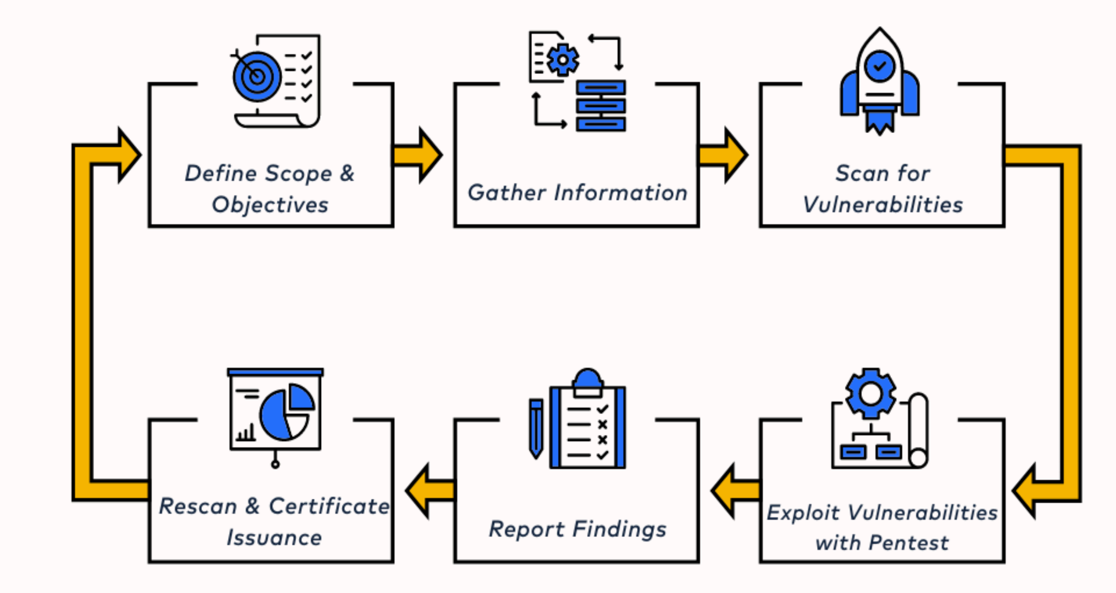

Define Scope & Objectives
Gather Information
Scan for Vulnerabilities
Exploit Vulnerabilities with Pentest
Report Findings
Rescan & Certificate Issuance

Figure 9.1. Vulnerability Assessment and Penetration Testing

Within a VAPT, the VA (Vulnerability Assessment) leverages security engineers & a wide array of automated tools to identify potential vulnerabilities. VA is followed by a PT (Penetration Test), where a real-world attack is simulated to exploit the vulnerabilities found during the VA process.

Burp Suite-

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp Suite is installed by default in Kali Linux.

The tool is written in Java and developed by PortSwigger Web Security. The tool has three editions: a Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise Edition that can be purchased after a trial period. The Community edition has significantly reduced functionality. It intends to provide a comprehensive solution for web application security checks. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer.

9.6 Procedure:

VAPT Process:

Step 1: Planning & Scoping:

This stage defines the VAPT's goals, objectives, and boundaries. It involves identifying critical assets to be tested, determining the testing methodology and compliance prioritizations, and outlining communication protocols with your VAPT testing provider.

Step 2:Information Gathering:

In this stage, the team gathers information about the target systems, network architecture, and potential vulnerabilities using publicly available data and authorized techniques. In the case of a grey box, they also gather information from you and start mapping your target systems.

Step 3: Vulnerability Assessment:

In this stage, the providers leverage mature scanners and automated tools to scan your systems for known vulnerabilities. This stage identifies potential weaknesses in software, configuration settings, and security protocols.

Step 4: Penetration Testing

Here, security professionals attempt to exploit identified vulnerabilities using hacking techniques. This stage simulates real-world attacks to assess the potential impact and effectiveness of your security controls.

Step 5: Reporting & Remediation:

Post exploitation, they deliver a comprehensive report detailing the vulnerabilities identified, the exploitation attempts made, and recommendations for remediation. This stage also involves creating a plan to address the vulnerabilities and strengthen your overall security posture.

Step 6: Rescan and Certificate Issuance:

Once the vulnerabilities have been patched, some penetration testing companies sometimes offer rescans to verify the above, generate clean reports, and issue publicly verifiable pentest certificates that facilitate compliance audits.

9.7Program and Output:

9.8Conclusion:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

………………………………………………………………………………

9.9 Review Questions based on Experiment:

Experiment No. – 10				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 10

Email Analysis

10.1 Aim: To investigate and analyze email communications to uncover relevant information and digital evidence in forensic investigations.

10.2 Course Outcome:

Use the forensics investigation process for operating system, network and application programs.

10.3 Learning Objectives:

- To understand the structure and components of email messages, including headers, bodies, and attachments.
- To learn how to extract and interpret metadata from emails to trace their origin, path, and authenticity.
- To utilize forensic tools to analyze email content for signs of phishing, malware, and other malicious activities.

10.4 Requirement:

10.5 Related Theory:

Header Analysis:

- Examine the email headers to identify key information such as sender and recipient addresses, timestamps, and the email's route through servers.

- Look for anomalies or inconsistencies in the headers that may indicate spoofing or other malicious activities.

Content Analysis:

- Analyze the email body for suspicious content, such as phishing attempts, links to malicious websites, or inappropriate language.
- Examine attachments for malicious files, malware, or hidden information. Use antivirus software and sandbox environments to safely open and analyze attachments.

Metadata Analysis:

- Extract and analyze metadata from emails and attachments to uncover additional information, such as the creation date, modification date, and the software used to create the email or attachment.
- Identify patterns or anomalies in the metadata that may indicate tampering or malicious activity.

10.6 Procedure:

Manual Analysis of Email Headers:

- Copy the email header information from the forensic tool into a text editor or directly analyze it within the tool.
- Look for key header fields such as:
  - From: The sender's email address.
  - To: The recipient's email address.
  - Date: The date and time the email was sent.
  - Subject: The subject line of the email.
  - Message-ID: A unique identifier for the email.
  - Received: Information about the servers the email passed through.
  - Return-Path: The return email address specified by the sender.
- Check for anomalies or inconsistencies in the headers that may indicate spoofing, such as mismatched sender addresses or unusual routing paths.

Using Tools for Email Header Analysis:

- FTK Imager: Use FTK Imager to mount the email file and navigate to the email headers.

    - Open FTK Imager.
    - Add the email data source (e.g., PST or MBOX file).
    - Navigate to the email headers and view them.
- MailXaminer: Use MailXaminer to analyze email headers in a more user-friendly interface.
    - Open MailXaminer.
    - Import the email data source.
    - Navigate to the "Email Headers" section to view detailed header information.
- Forensic Email Collector: Use Forensic Email Collector for more advanced extraction and analysis.
    - Open Forensic Email Collector.
    - Connect to the email account or import the email file.
    - Extract and analyze the email headers.

Using Online Header Analyzers:

- Use online tools such as MxToolbox Email Header Analyzer or Google's G Suite Toolbox to simplify header analysis.
    - Copy the email header information.
    - Paste it into the online header analyzer.
    - Review the parsed information and look for anomalies or indicators of malicious activity.

10.7Program and Output:

10.8Conclusion:

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

…………………………………………………………………………

10.9 Review Questions based on Experiment:

Experiment No. – 09				
Date of Performance:				
Date of Submission:				
Program Execution/formation/ correction/ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 09

Email Analysis

9.1 Aim: To implement Stegnography and revert the hidden message.

9.2 Course Outcome:

Use the forensics investigation process for operating system, network and application programs.

9.3 Learning Objectives:

- To use steganographic tools like OpenStego, to detect data hiding or unauthorized file copying

9.4 Requirement:

9.5 Related Theory:

Stegnography is the art of covered or hidden writing. The purpose of stegnography is covert communication to hide a message from a third party.

Stegnography hides the covert message but not the fact that two parties are communicating with each other. The stegnography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the stegnography medium. The use of stegnography key may be employed for encryption of the hidden message and/or for randomization in the stegnography scheme. In summary:

stegnography_medium=hidden_message+carrier+stegnography_key

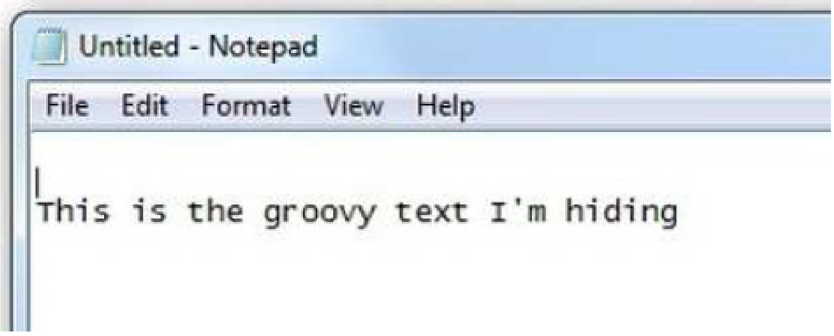
Stegnography provides some very useful and commercially important functions in the digital world, most notably digital watermarking. An artist, for example, could post original artwork on a website. If someone else steals the file and claims the work as his or her own, the artist can after prove ownership because only he/she can recover the watermark.

9.6 Procedure:

Step 1: Create a stegnographic image.

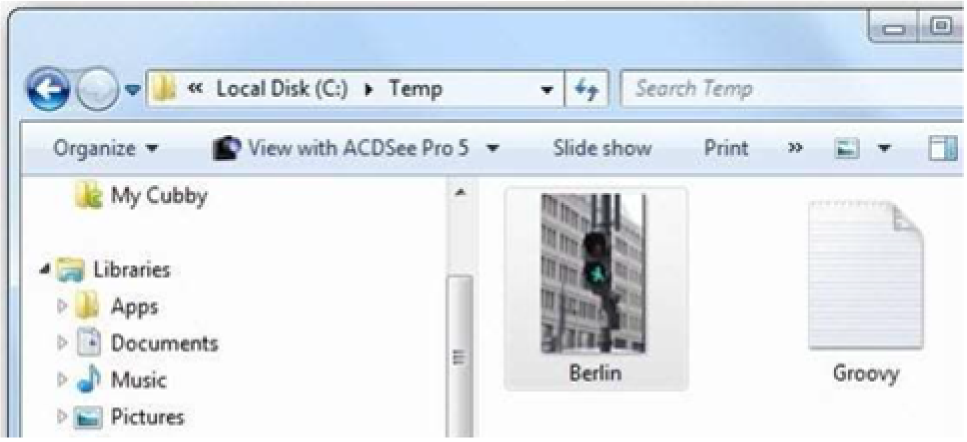
This method will allow you to hide text in a JPG file.

1. Open Notepad and type the text you want to hide and save it in folder.



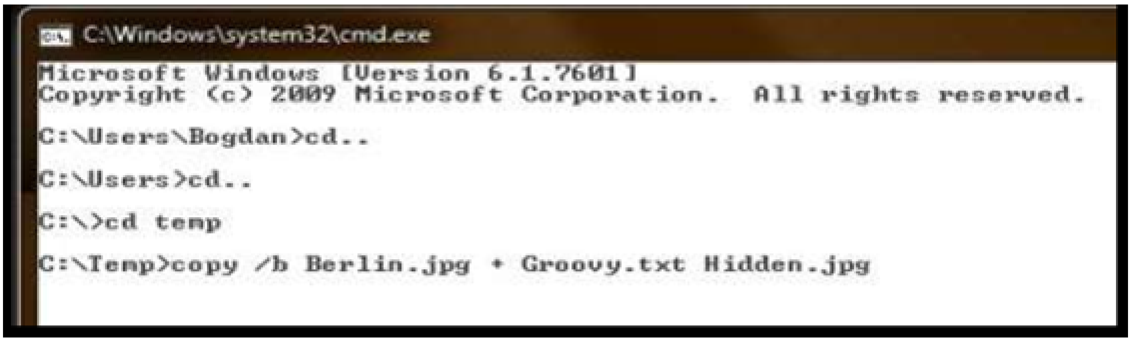
```
This is the groovy text I'm hiding
```

2. Copy the JPG file you want to hide text in the same folder. The folder should now look like this.



3. Now go to the command prompt

copy /b Name-of-initial-image.jpg + Name-of-file-containing-text-you-want-to-hide.txt Resulting-image-name.jpg



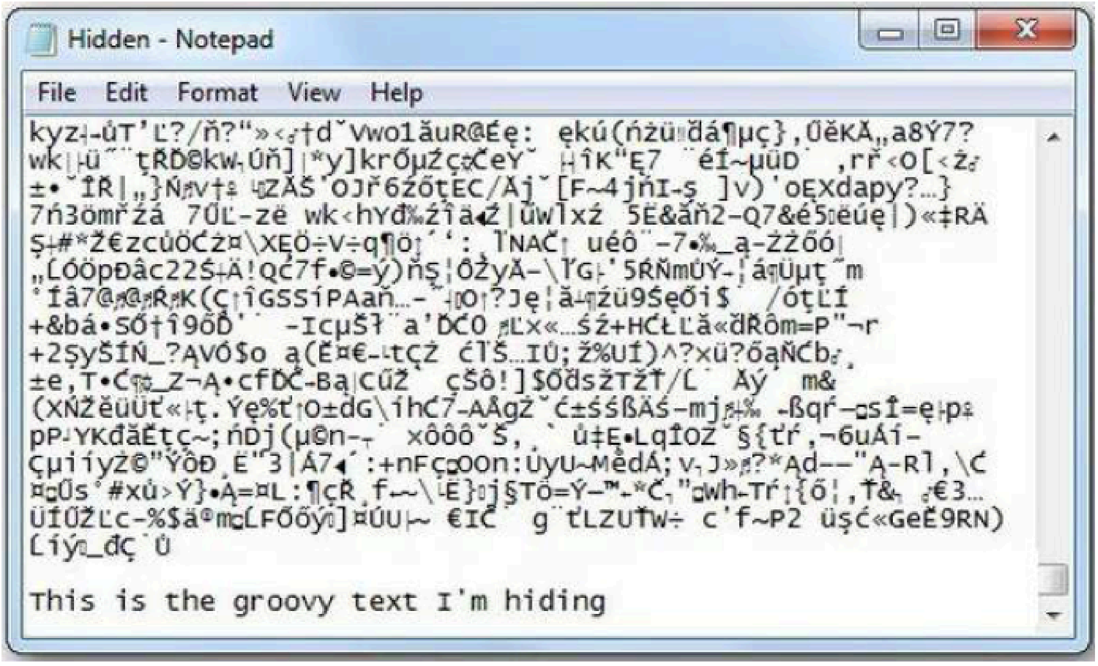
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Bogdan>cd..

C:\Users>cd..

C:\>cd temp

C:\Temp>copy /b Berlin.jpg + Groovy.txt Hidden.jpg
```

Now look in that directory and you'll see that new file has been created.

Step 2: Reverting the hidden message from stegnographic image.

1. Inorder to view the hidden message, right click the image and use **openwith** option to view image file in notepad/wordpad.

2. Image information will be displayed in hex format and at the end you can view the text/ ASCII character.



```
kyz┤-ůT'Ľ?/ň?"»<┘†d˘Vwo1ăuR@Ęę: ękú(ńżü▯ďá¶µç},ŰěKĂ„a8Ý7?
wk|┤ü˝¨ţŘĎ©kw┐Űň]|*y]krőµźç¤ČeY˘ ┤îK"Ę7 ¨éÎ~µüD˙ ,rř<O[<ž┘
±•˘ÎŘ|„}Ń┘v†± ┴ZĂŠ˙OJř6źőţEC/Ăj˘[F~4jňI-ş ]v)'oĘXdapy?…}
7ń3ömřźá 7ŰĽ-zë wk<hYđ‰źîä◄Ź|ůWlxź 5Ë&ăň2-Q7&é5▯éúę|)«‡RÄ
Ş┼#*Ž€zcůÖĆž¤\XĘÖ÷V÷q¶ö┐´‘: ŤNAČ┐ uéô¨-7•‰_ą-ŻŻőó|
„ĹÓöpĐâc22Ś┼Ä!Qc7f•©=ý)ńş¦ÓŻyĂ-\ŤG┤'5ŔŃmŰÝ-¦ą¶Üµţ˝m
˚Îâ7@┘@┘Ŕ┘K(Ç┐îGSSíPAań…-˝┤▯O┐?Ję¦ă┤¶źü9Śęőî$˝ /óţĽÍ
+&bá•SŐ†î9őĎ'˙ -IcµŠł¨a'ĎĆ0 ┘Ľx«…śź+HĆŁĽă«ďŘôm=P"¬r
+2ŞyŠÍŃ_?ĄVÓ$o ą(Ě¤€-┴tçź ćľŚ…IŰ;ž%Uí)^?xü?őąŃCb┘.
±e,T•Ć¶▯_Z¬Ą•cfĎĆ-Bą|Cűź˝ çŠô!]$ŐďsžTžť/Ĺ˙ Ăý˝ m&
(XŃŽëüŰť«┤ţ.Ýę%ť┐O±dG\íhĆ7-AĂgź˘ć±śśßĂś-mj┘┼‰ -ßqŕ–▯sÎ=ę┤p±
pP┘YKďăĚţç~;ńDj(µ©n-┬˙ xôôô˘Š, ˙ ů‡Ę•LqÎoŹ˘§{ťŕ,¬6uÁí-
Çµiíyž©"ŸÔĐ Ë"3|Á7◄´:+nFç▯OOn:ŮyU~MėdÁ;v┐J»┘?*Ąd--"Ą-Rl,\Ć
¤▯Űs˚#xů>Ý}•Ą=¤L:¶çŘ f←~\└Ë}▯j§TÖ=Ý-™-*Č┐"▯Wh-Tŕ┐{ő¦,ť&┐ ┘€3…
ŰÍŰŽĽc-%$ä®m▯ĹFŐőý▯]¤ŰU┤~ €IĆ˙ g¨ťLZUŤW÷ c'f~P2 üşć«GeĚ9RN)
Ĺíý▯_đç˙Ű

This is the groovy text I'm hiding
```

Openstego Installation:

Download latest release from

https://www.openstego.com/concepts.html -> Download
Or
https://github.com/syvaidya/openstego/releases

To open the application:

openstego-0.8.0\lib\openstego.jar file

OpenStego, the free steganography solution. OpenStego provides two main functionalities:

- **Data Hiding:** It can hide any data within a cover file (e.g. images).
- **Watermarking (beta):** Watermarking files (e.g. images) with an invisible signature. It can be used to detect unauthorized file copying.

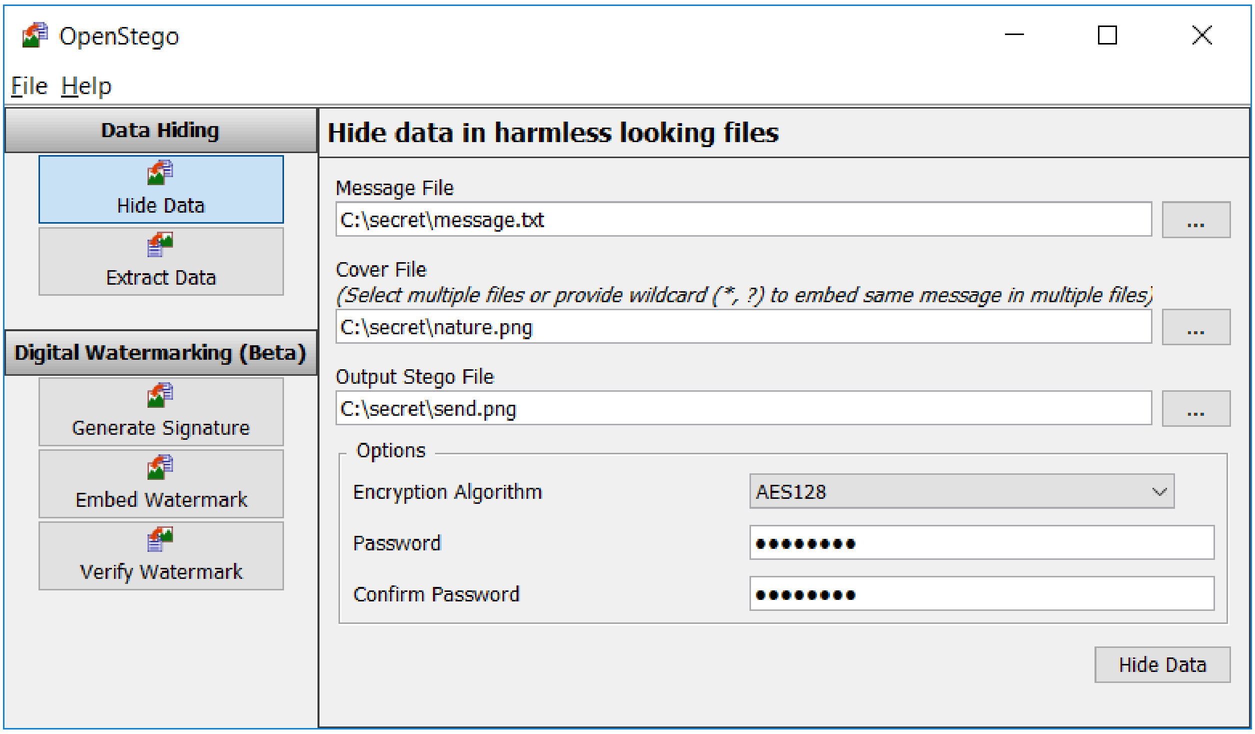
Using OpenStego

Using OpenStego is pretty straightforward. There are two modes of operation - data hiding and watermarking.

Data Hiding

In this mode, you can either hide the data (file) inside an image or extract the data from the image. Check screenshots below to see how it can be done:

Hide data



Message File: C:\secret\message.txt

Cover File
(Select multiple files or provide wildcard (, ?) to embed same message in multiple files)*
C:\secret\nature.png

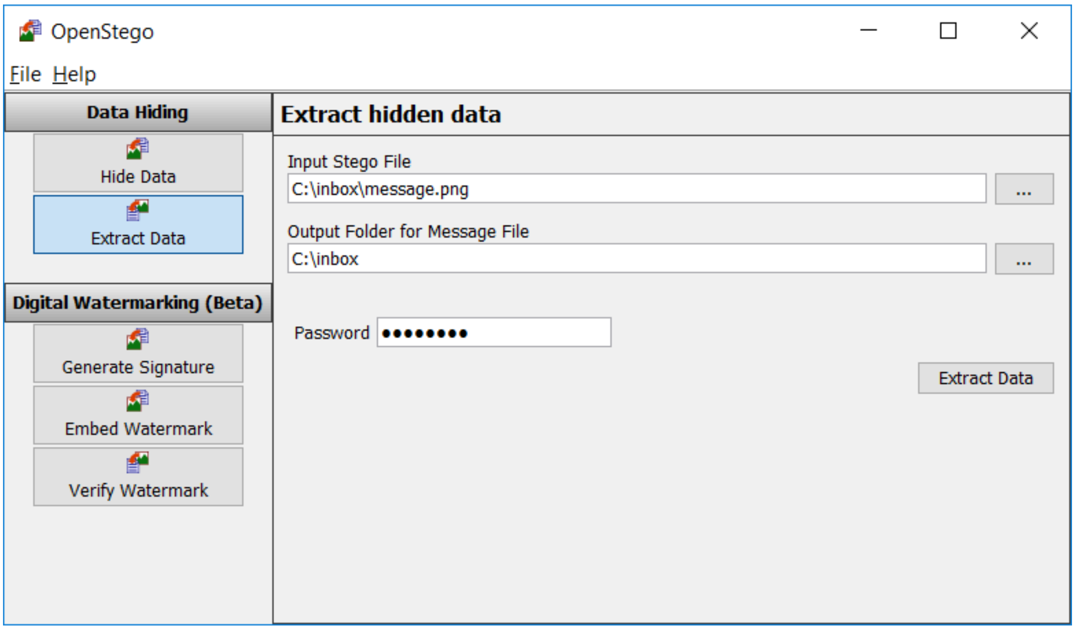
Output Stego File: C:\secret\send.png

Encryption Algorithm: AES128

Password: ••••••••

Confirm Password: ••••••••

Extract data



Input Stego File: C:\inbox\message.png

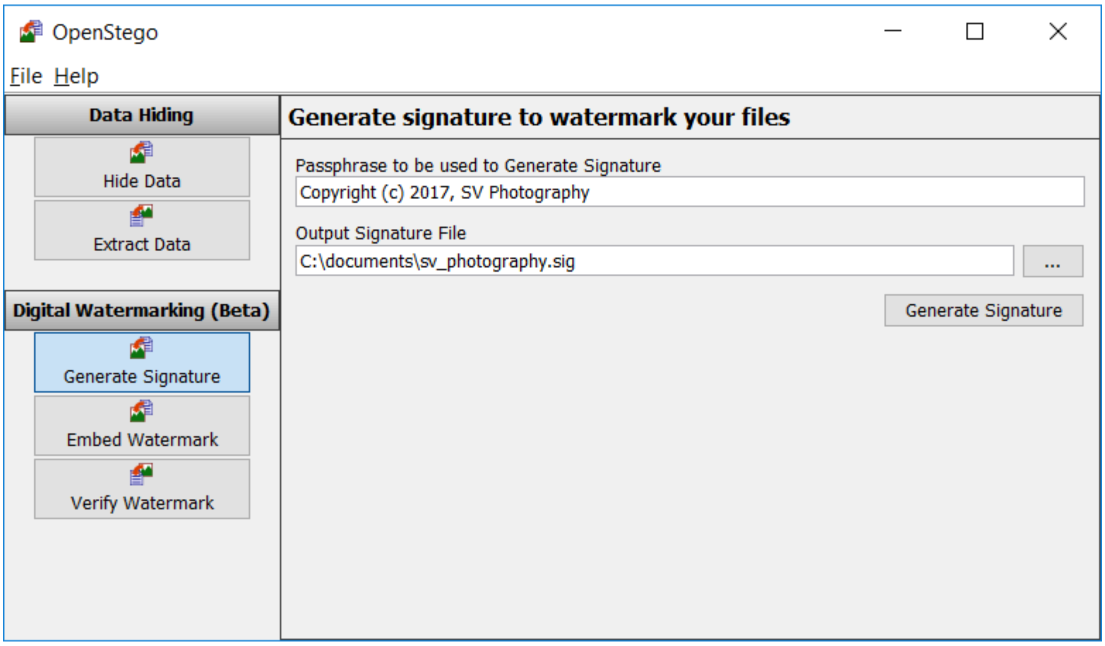
Output Folder for Message File: C:\inbox

Password: ••••••••

Watermarking (beta)

In this mode, you can watermark / verify images with your signature. First you need to generate signature file, and then it can be used to watermark images or verify the same later. Check screenshots below to see how it can be done:

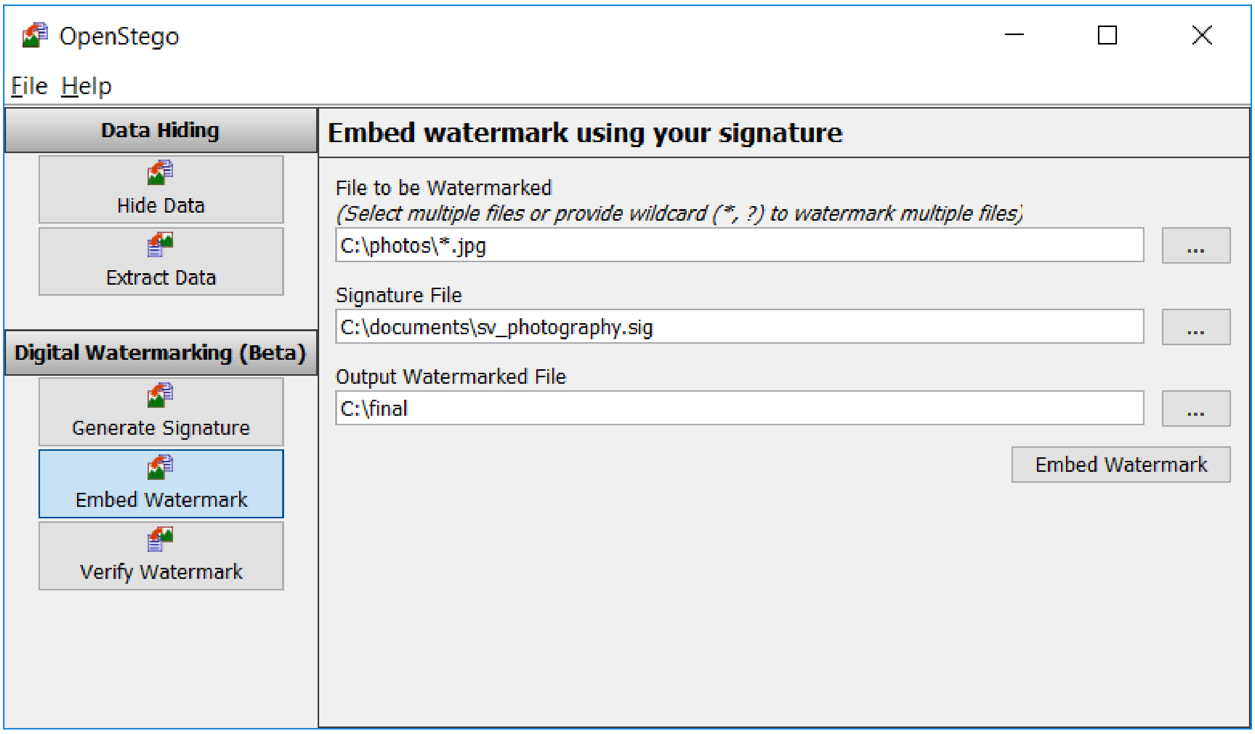
Generate signature



Passphrase to be used to Generate Signature: Copyright (c) 2017, SV Photography

Output Signature File: C:\documents\sv_photography.sig

Embed watermark



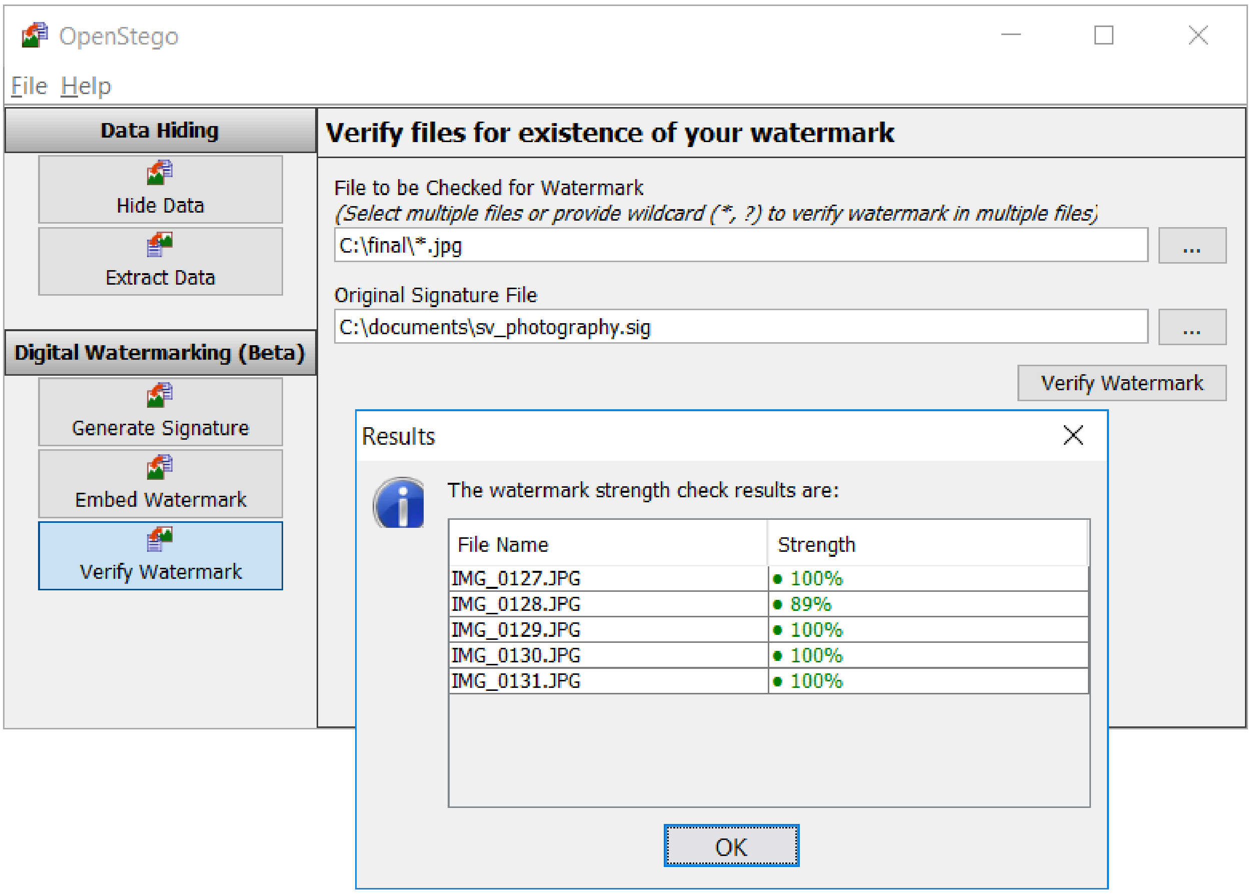
Embed watermark using your signature

File to be Watermarked
(Select multiple files or provide wildcard (, ?) to watermark multiple files)*
C:\photos\*.jpg

Signature File
C:\documents\sv_photography.sig

Output Watermarked File
C:\final

Verify watermark



Verify files for existence of your watermark

File to be Checked for Watermark
(Select multiple files or provide wildcard (, ?) to verify watermark in multiple files)*
C:\final\*.jpg

Original Signature File
C:\documents\sv_photography.sig

The watermark strength check results are:

File Name	Strength
IMG_0127.JPG	● 100%
IMG_0128.JPG	● 89%
IMG_0129.JPG	● 100%
IMG_0130.JPG	● 100%
IMG_0131.JPG	● 100%

9.7Program and Output:

9.8Conclusion:

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………

9.9 Review Questions based on Experiment: