



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Computer Forensics (ACCD5000)

Investigation



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

Objectives

In continuation to our lectures, this hands-on Activity helps in providing you an overview of digital forensic investigation process.

ETHICAL STATEMENT

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

We, the participants and stakeholders in the digital forensics laboratory, recognize the significance of ethical conduct when using digital forensics tools and processes for academic purposes. Our commitment to ethical standards is grounded in the principles of integrity, privacy, and responsible handling of digital data.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Based on Activity 2, you must have a lab setup working.	☒
So far:	
HoA1: Understand Digital Evidences - Importance of Computer Forensics – Basic Investigation	☒
HoA2: Understand the importance of ensuring DATA Integrity – Computer Forensics Virtual Lab Setup	☒
Make sure the above activities are completed before starting this week's activity	
Task 1: Investigation Process	
Task 2: Pre-Analysis – Hash Values	
Task 3: Pre-Analysis – Comparing Hash Values	

ICONS Used in this document:

Find out the outcome/ Answers/ Solution and record your reflection



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



Recommended Screenshot (with Timestamp) for your Coursework.



Recommended to address this part in your Coursework.

Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1: Investigation Process

This is a Group Activity. Form a Group (Not more than 8), refer to our the lecture session earlier, apply the discussions about Computer Forensics Investigation Process in this given task.

Your Lecturer has setup a crime scene (*as discussed earlier, a crime here refers to a computer related crime – based on an organisation or an individual*).

Nature of the Incident: Organisational Crime (An Individual violating Confidential Document Restrictions in his/her organisation – Possible suspicious activity)

Location: Defined by your Lecturer

Potential Digital Evidence: USB Flash Drives, HDD, PC's/ Laptops

The Crime scene has computer evidences that need to be identified, and appropriately collected to further investigation.

You as a group is tasked to follow the instructions, enable discussion, plan appropriately, imply your understanding on the forensics investigation process and its importance, (*ask questions to your lecturer for more clarity – Do not make any assumptions*) to complete the investigation process.

1. Build your Investigation Team:
 - a. With the available members, form your team
 - b. Assign specific roles and responsibilities. (Eg: Team Leader, Evidence Collector etc)
2. Recall – Research – Review:
 - a. Recall the discussion during the lectures
 - b. Research via credible sources to understand the legal considerations, evidence handling procedures (*you may refer to any country – however, during your documentation, make sure to state the country for which you have referred the legal considerations*)

Hint: You could review the legal considerations and evidence handling procedures based on your specific roles and responsibilities.

- c. Review with your team, your understanding about the legal considerations and plan accordingly.
- d. Create a Standard Operating Procedure outlining step-by-step process for investigating and identifying the digital evidence, collecting it and transporting it.

Hint: Your SOP should cover roles, responsibilities, procedures of evidence handling, documentation requirements and legal considerations.

- e. Identify the resources required for the Investigation, including tools, equipment and personnel.
 - f. Do a mock exercise to familiarize the team with the process and ensure that as a Team, each one has adequate understanding on their roles and responsibilities.
 - g. Document all the steps done in Step 2.
3. Identify, Collect and Transport
- a. Conduct an initial assessment of the environment to identify potential sources of digital evidence.
 - b. Document the location and condition of each potential piece of evidence.
 - c. Follow established procedures for the collection of digital evidence, ensuring proper documentation and chain of custody.
 - d. Use appropriate tools and techniques to acquire evidence from various sources, taking care to preserve its integrity.
 - e. Label and package each piece of evidence securely, following best practices for transportation.
 - f. Coordinate the transportation of collected evidence to the computer forensics laboratory, ensuring it is handled securely and in accordance with chain of custody requirements.
 - g. Use designated transport containers or packaging to protect evidence from damage during transit.
 - h. Maintain proper documentation of the transportation process, including date, time, individuals involved, and any relevant notes or observations.
4. Reflect
- a. Do an open discussion with your team members, sharing information and insights to enhance the effectiveness of the investigation.
 - b. Document all activities, findings, and observations throughout the investigation, maintaining detailed records in accordance with established procedures in Moodle HoA3 Submission link.
 - c. Reflect your understanding about the investigation process, evidence collection, analysis performed, and any relevant conclusions or recommendations in Moodle Discussion Forum.
5. Consideration?
- a. Throughout the entire process, have you considered implementing quality assurance measures to ensure accuracy, completeness, and compliance with legal and ethical standards?

Annexure

1. Sample Forms

CONSENT TO SEARCH ELECTRONIC MEDIA I, _____, hereby authorize _____, who has identified himself / herself as a law enforcement officer, and any other person(s), including but not limited to a computer forensic examiner, he / she may designate to assist him / her, to remove, take possession of and / or conduct a complete search of the following: computer systems, electronic data storage devices, computer data storage diskettes, CD-ROMs, or any other electronic equipment capable of storing, retrieving, processing and / or accessing data. The aforementioned equipment will be subject to data duplication / imaging and a forensic analysis for any data pertinent to the incident / criminal investigation. I give this consent to search freely and voluntarily without fear, threat, coercion or promises of any kind and with full knowledge of my constitutional right to refuse to give my consent for the removal and / or search of the aforementioned equipment / data, which I hereby waive. I am also aware that if I wish to exercise this right of refusal at any time during the seizure and or search of the equipment / data, it will be respected. This consent to search is given by me this _____ day of, _____ 20_____, at _____ am / pm. Location items taken from: _____ Consenter Signature: _____ Witness Signature: _____ Witness Signature: _____	Form 1.1 Voluntary Consent to Search Voluntary Consent to Search I, _____, do hereby, freely, voluntarily and without threat, pressure or coercion of any kind, consent to a warrantless search of my _____ _____ (Location and description of premises to be searched), by representatives of _____ (Police Department or Agency) and individuals in their company. These representatives are authorized by me to seize any items, materials or other property which they may deem to be of possible evidentiary value. _____ Witness Signature of person consenting to search _____ Witness Relationship to Premises being searched DOB _____ SSN _____ Date _____ Time _____
--	---

2. Witness Signatures

Before getting the witness signature, did you

- Explain the reason for taking statement
- Explain what is required from the witness
- Explain the importance of telling the truth

Note: You must respect the legal rights of the individual being interviewed.

- Ensure the environment is appropriate to an interview (no unnecessary audience – Police Officer, Colleague, any individuals etc)
- Adapt procedures and techniques appropriately
- Written statement when and where appropriate
- Audio/Video Recordings if required
- Record Keeping with basic information (like date, time, location, name, dob etc)
- Differentiate witness statement and wared statements
- Record – During interview (Listens effectively, maintain momentum of dialogue, provides accurate information, keeps sequential statement etc)
- Questions to clarify and record answers
- Has witness verified the statements and corrected (if necessary)
- Has witness signed the statements?
- Was the oral statements transcribed accurately?

3. Chain of Custody

Chain of Custody Document		
Laboratory or Agency Name :	Case Number :	
Received from (Name and Title)	Address and Telephone Number	
Location from where the Evidence was Obtained	Reason the Evidence was Obtained	Date and Time the Evidence was Obtained
Item Number	Quantity	Description of Item

Computer System Worksheet		
GSI File #		
Date:	Agency:	Agency Case #:
Site #:	Site Address #:	
Examiner:	Room/Location ID:	
Notes:		
Computer Description (Fill in or check all that apply)		
Make: ☐ None	Case Type ☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ Laptop ☐ Desktop ☐ All in one ☐ Rack Mount	
Model: ☐ None	System Date:	Local Date:
Serial #: ☐ None	System Time:	Local Time: ☐ PSD ☐ PDT
OAN: ☐ None	System Status: ☐ On ☐ Off ☐ Active ☐ No Power/Not Connected ☐ Suspended/Stand-by ☐ Screen Saver Active ☐ Other	
Apparent OS ☐ Ukw	Active/Open Programs: ☐ None ☐ N/A	
From ☐ N/A ☐ Screen ☐ Start Button ☐ Other	1.	
Shutdown Method ☐ Hard ☐ N/A ☐ Soft ☐ Unknown ☐ Other	2.	
Shutdown Data and Time	3.	

Chain of Custody Form				
Package #	Date/Time	Released By	Received By	Reason
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	

Peripherals and Connections				
☒	INTERFACE	DESCRIPTION	NOTES	
☐	RJ-45	NIC Interface		
☐	RJ-11	Telephone Modem		
☐	☐ HDMI ☐ SATA	Monitor	Media Model	Serial No
☐	☐ USB ☐ AT	Keyboard	Media Model	Serial No
☐	☐ USB ☐ AT	Mouse	Media Model	Serial No
☐	☐ Firewire ☐ USB	Printer	Media Model	Serial No
☐	☐ Thunderport	Connector	Media Model	Serial No
☐			Media Model	Serial No
☐	PASSWORD INFO:			

CONTROL NO. **M** LOCK TO 103

EVIDENCE

NOTE: Do not use this bag for any evidence that has wetting liquid spills on it. Do not use this bag for any evidence that has wetting liquid spills on it.

Investigator: _____

Submitting Agency: _____

Evidence Received By: _____

Evidence's Full Name: _____

Evidence's Full Name: _____

Evidence's Full Name: _____

Date Received: _____

CHAIN OF CUSTODY

FROM	TO	DATE

FOR CRIME LAB PERSONNEL ONLY

Signature: _____

Signature: _____

Signature: _____

Task 2: Pre-Analysis – Determine Hash Values

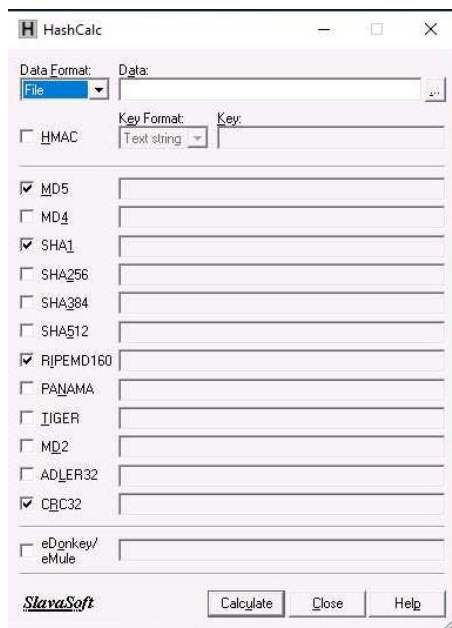
Reading:

To be an expert computer forensic investigator, you must have sound knowledge of hashing and the tools used to compute hashes. So, do a research/ self-study on Hashing. What is the purpose of Hashing in terms of Computer Forensics?

1. Compute hashes of files and text string
2. Check the hashes on VirusTotal to see if the file(s) are malicious

Tools used: HashCalc

1. Login to your Forensic machine. (It must be write-protected and isolated)
2. Navigate to \\192.168.135.50\FTKToolsShare\$ to find the evidence files.
3. Download HashCalc or any other relevant tools to calculate the checksums for files.
4. Open HashCalc or its equivalent tool.



5. In the Data Format drop-down list, select data format as File and click the ... button near the Data field to select the file.
6. Subsequently, Find window will appear; navigate to appropriate folder path to select the files. (The files are available in the File Share Folder).
7. Open Fan-oven.png.
8. To calculate the message digests/checksums for the data, the HMAC box must be unchecked.

9. Select the algorithms you want to use for calculations by checking the boxes with the appropriate names, and then click the Calculate button. (Here, MD5, MD4, SHA1, SHA512, MD2 are selected.)



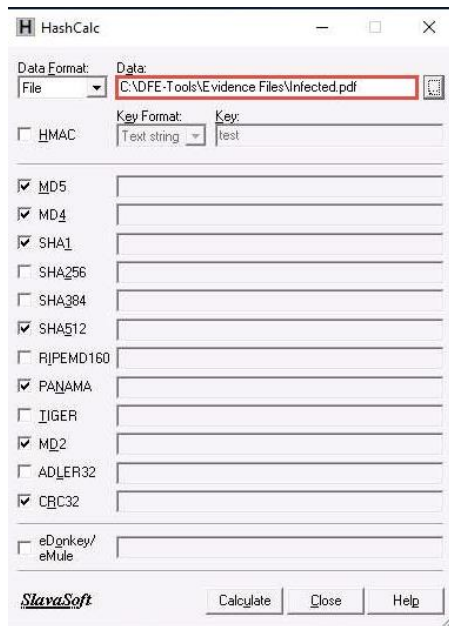
10. Hash values will be displayed for the selected file
11. To calculate the Keyed - Hash Message Authentication Code (HMAC) for the data: Check the HMAC box.
- In the Key Format combo box, select the type of the key you want to use for calculations.
Note: HashCalc allows you to perform calculations using text keys or hex keys (Here, we have selected Text String in the Key Format combo box).
 - In the Key box, enter the key for HMAC calculations (for example, test is entered as key here).
 - Select the algorithms you want to use for calculations by checking the required algorithms (here, MD5, MD4, SHA1, SHA512, PANAMA are selected), and then click Calculate.



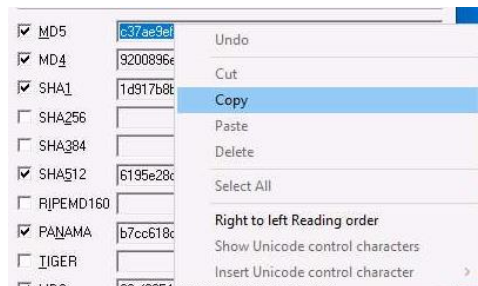
- d. HashCalc calculates the hashes of the specified file and displays them:
- e. Find out using the tool, to perform a calculation for a text string



12. Now, we shall calculate the MD5 hash value of an infected/malicious pdf and search this hash value in the VirusTotal database to see whether the file is safe to access or malicious. Open Infected.pdf
13. Select appropriate Data Format and calculate the hash value.



14. Copy the MD5 hash value as shown in the following screenshot:



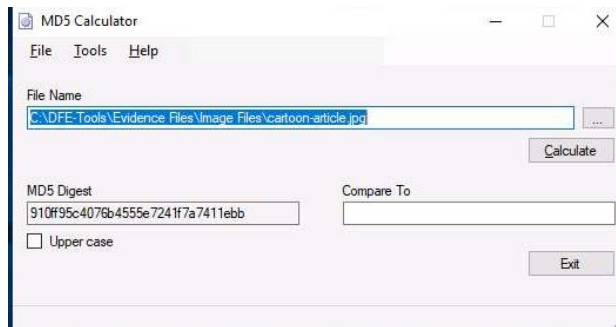
15. Open <https://www.virustotal.com/gui/home/search> and paste the MD5 hash in the Search field and click Enter. VirusTotal searches this value in its database and returns the result.
16. Navigate to the DETAILS tab, to view basic properties showing values of MD5, SHA-1, SHA-256, etc.
17. Navigate to BEHAVIOUR tab, to view information such as Files System Actions, Registry Actions, Process and Service Actions, etc
18. What is the outcome?

Task 3: Pre-Analysis - Comparing Hash Values

During an investigative process, as a forensics examiner you need to check the integrity of copies of several files that contained sensitive data of an organization.

1. What tool should you use to compute and compare the hashes?
2. Login to your Forensic machine. (It must be write-protected and isolated)

3. Use the tool you selected in Step 1. For this demonstration, we are using MD5 Calculator.
4. To calculate the MD5 hash of a file, first select cartoon-article.jpg file, right-click on it and then select MD5 Calculator from the context menu.
5. The MD5 Calculator window will subsequently appear, displaying the MD5 hash value for the selected file as shown in the following screenshot:



6. Make a note of this MD5 digest.
7. Make modifications to this file and check the value.
8. What is the outcome?

Note: If you want to compare the hash value of a file, enter the pre-existing hash value of that file under the Compare To section and calculate the file's hash.

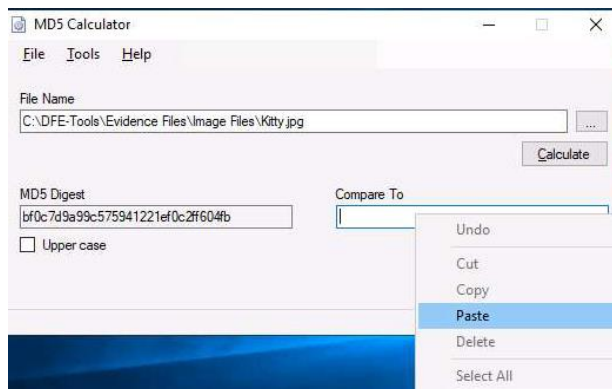
In this lab, we shall compare hash values of multiple files to see if their generated hash values match with the pre-existing hash values.

9. Open Hashes.txt. This file contains hashes of some of the image files.

```
Hashes.txt - Notepad
File Edit Format View Help
cartoon-article.jpg: 910ff95c4076b4555e7241f7a7411ebb
Fan-oven.png: 3759b97fbd029a7e74a492fd09bc0a3d
Flowers_123.jpg: eadd66a945bebf7eb01b2a75a1748f99
Kitty.jpg: bf0c7d9a99c575941221ef0c2ff604fb
Model.png: 209c1f5a72f2181b5a670e45cbd550f6
peacesign.jpg: 9cfda073866cd6f813815ef6b97e3c32
images.jpg: 52b29a36da797ff3c4c9fed18140176b
awen.gif: 169f012153f9e70767bbbeddae427fbf
Friends2.jpg: 7c6f8ea5361ae7719d5d3caf60bf60b5
Tweety1.gif: 3ef2b01136671ae97d3ccf4d22cf58c1
images-of-cartoons-14.jpg: e0413409680f4e48ea7b68e725c36a4a
maxresdefault.jpg: 72fdb03e810f94e7f066f986181d72f
```

10. We shall compare hashes of two files Kitty.jpg and Model.png.
11. To compare the hashes of Kitty.jpg, copy the hashes corresponding to the file.
12. Right click Kitty.jpg and then select MD5 Calculator from the context menu.

13. MD5 Calculator displays the MD5 Digest (hash value) for the selected file. Now, paste the hash value that you copied in Step 11 into the Compare To section.



14. MD5 Calculator instantly compares both the hashes. If the hashes are equal, the file's integrity is intact.
15. Similarly, compare the hashes of the file Model.png.
16. What is the outcome?

Note: If the hashes do not match, the file's integrity is under question and it needs to be further investigated. The file might have possibly been modified to act as a payload for an attack (or) to hide data inside it, etc.



Overall Reflection

Record your reflection via Moodle – Group Discussion.

1. Understanding of the concepts discussed in the lecture and its relation to the activity done.
2. Understanding Investigation Process (Steps to Plan Investigation, Collecting and Transporting Evidences).
3. Understanding and implementing Data Integrity and its need.
4. Rate yourself (1 very low – 5 exceptional): Understanding the Investigation Process.

-----End of Activity-----