



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



School of
Applied Computing

Computer Forensics (CF)

Lab 3

Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW

Lecturer: Assoc. Professor Carlene Campbell

Email: carlene.campbell@uwtsd.ac.uk

Website: <https://www.knowledgewithprofit.com>

Exercise 01: Perform Hash or HMAC Calculations

Lab Scenario

A multinational company has undergone a network attack and has called a forensics investigator to investigate the issue. The investigator found some codes that appear to be familiar and needs to cross-check for their availability across a malware database. The major problem here is that the codes are huge and require a large amount of storage space, making it difficult for search and indexing purposes. Therefore, the investigator uses hash values of the code to find their traces in the database.

To be an expert computer forensic investigator, one must have sound knowledge of hashing and the tools used to compute hashes.

Lab Objectives

Hashing is performed on data such as files or text to generate a unique fixed-length string called a hash or checksum. The generated hashes are helpful in determining whether the given data has maintained integrity.

The objective of this lab is to demonstrate how to:

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

Note: Hashes or hash values may also be referred to as checksums

Lab Environment

To carry out this lab, you need the following:

- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Overview of the Lab

This lab familiarizes you with HashCalc, a tool that helps you determine the hash values of various files. Determining the hash values of files enables an investigator to establish their integrity.

Lab Tasks

Note: In this lab, you are considering that the footprint of the investigation is not a major issue.

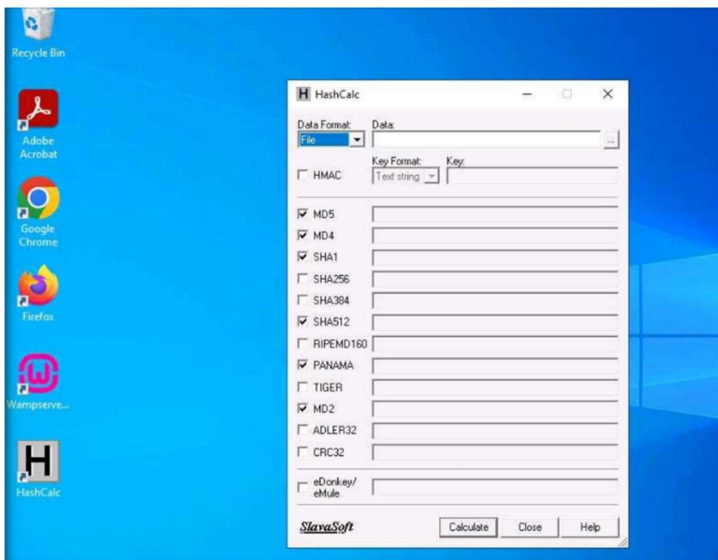
1. Switch to the Windows Server 2022 virtual machine, press Ctrl+Alt+Delete.
2. Use the username and password you have created or used when setting up the Windows Server 2022 in the VB. Or by default, the Administrator user profile is selected. Type

Pa\$\$w0rd in the Password field and press Enter to login.

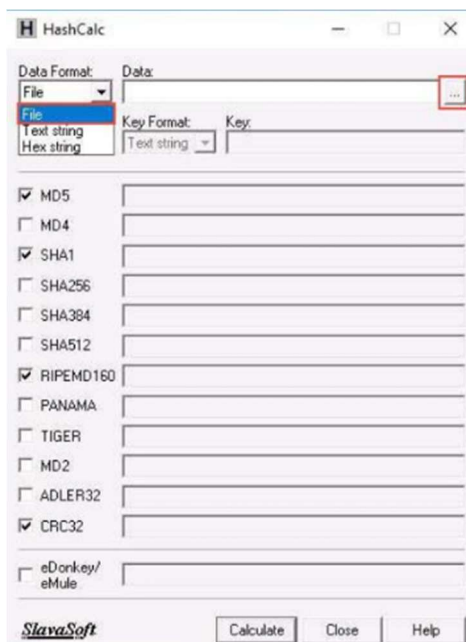
Note: If the Networks pane appears, click Yes to allow your PC to be discoverable by other PCs and devices on this network.



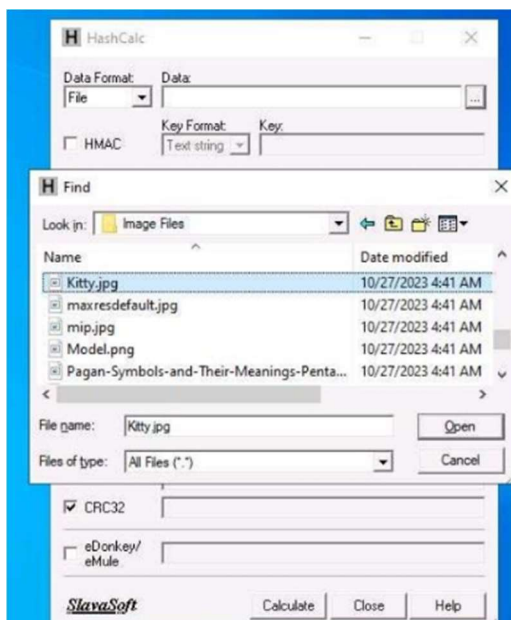
3. Navigate to [Forensics tools](#) to find the evidence files for this lab.
4. Navigate to [Forensics tools](#) to find HashCalc, then double-click on setup.exe and follow the wizard-driven installation steps to install the application.
Note: If an Open File - Security Warning pop-up appears, click Run.
5. In the final step of installation, **uncheck the View the README file option, check the Launch HashCalc** option, and click Finish.
6. The HashCalc application's main window will appear, as shown in the following screenshot:



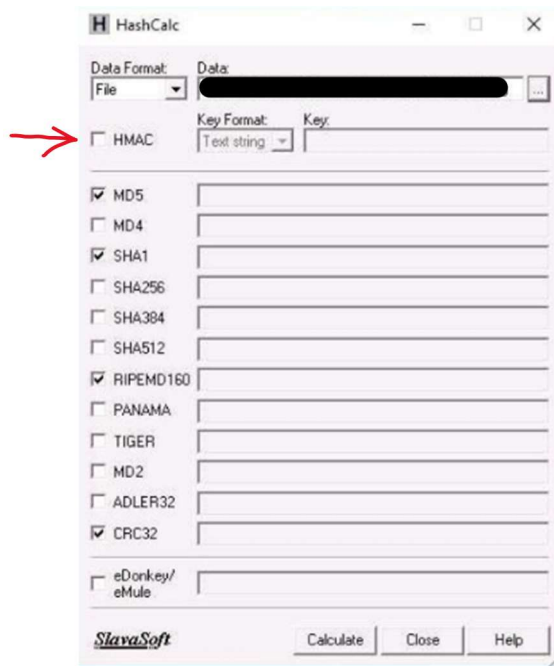
7. In the Data Format drop-down list, select File as data format and click the ellipsis button associated with the Data field to select the file.



8. Subsequently, the Find window will appear. Navigate to [Forensics tools](#) to the evidence folder. In this location, select **an** evidence file, whose hash value needs to be calculated. In this lab, we have selected a file named Kitty.jpg. Once you select the file, click Open.

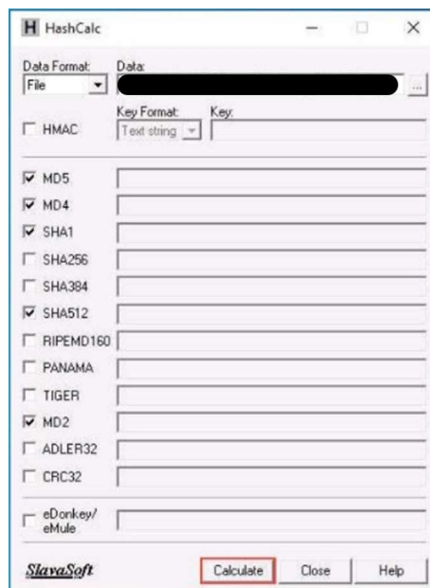


9. The selected file will be displayed in the Data field.

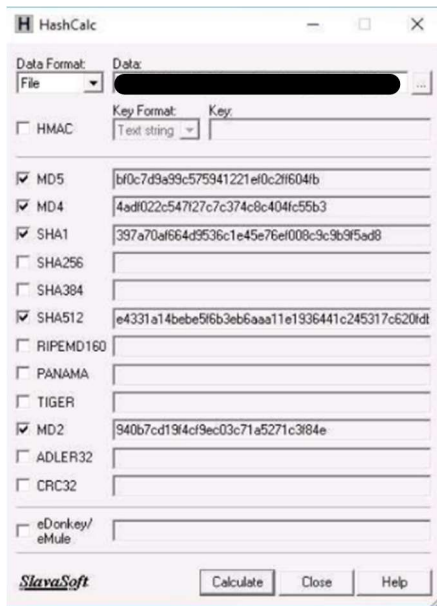


Note: To calculate the message digests/checksums for the data, the **HMAC box** must be unchecked.

10. Select the algorithms you want to use for calculations by checking the boxes with the appropriate names, and then click the Calculate button.



11. Hash values will be displayed for the selected file, as shown in the following screenshot:

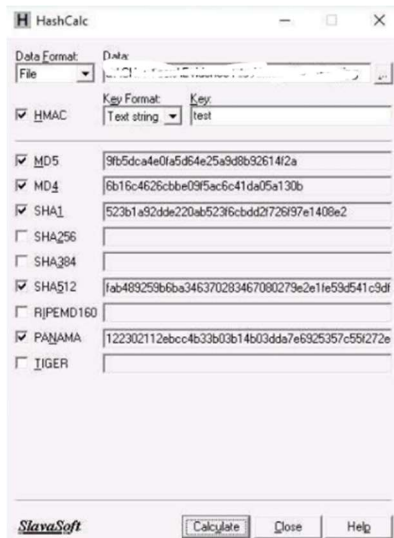


12. To calculate the Keyed - Hash Message Authentication Code (HMAC) for the data:

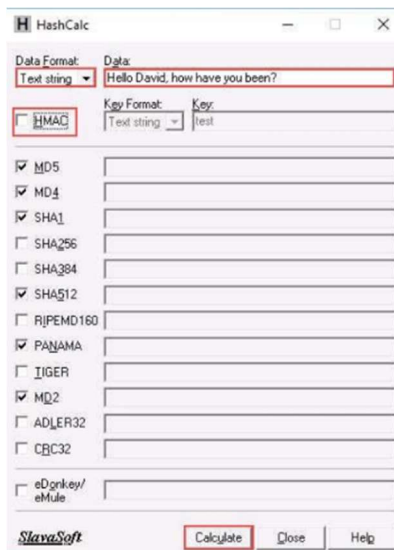
- Check the HMAC box.
- In the Key Format combo box, select the type of key you want to use for calculations. HashCalc allows you to perform calculations using text keys or hex keys (Here, we have selected Text String in the Key Format combo box).
- In the Key box, enter the key for HMAC calculations (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.



13. HashCalc calculates the hashes of the specified file and displays them, as shown in the following screenshot.



14. If you want to perform a calculation for a text string, first select Text string from the Data Format drop-down list, uncheck the HMAC box and then enter the text (here we entered, Hello David, how have you been?) in the Data field.
15. Select the algorithms you want to use for calculations by checking the required algorithms and then click the Calculate button.



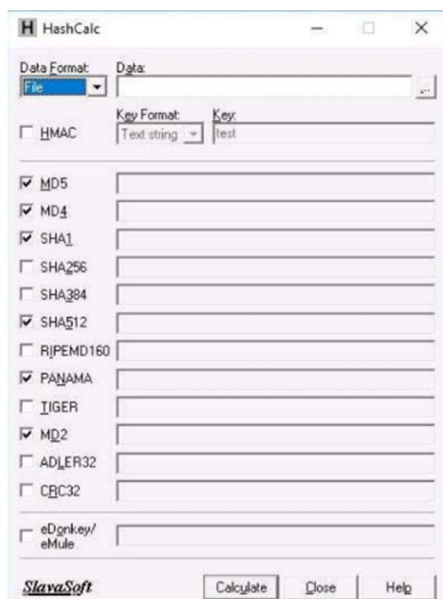
16. Hash values will be displayed for the selected algorithms, as shown in the following screenshot:



17. Next, 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.

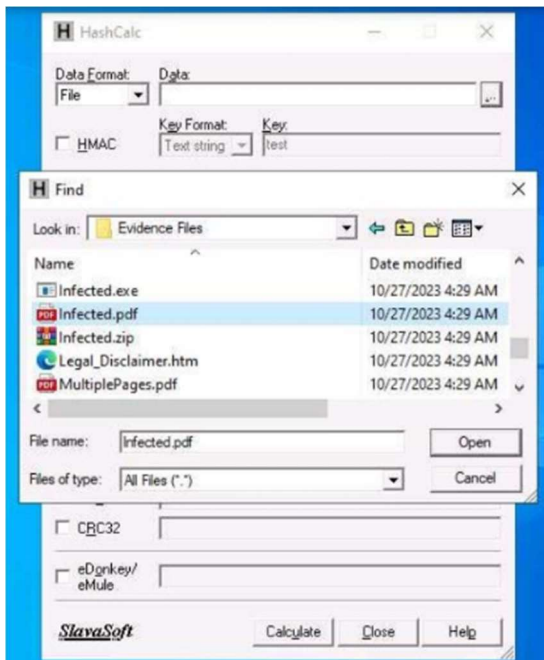
18. In this lab, we shall be testing a file named Infected.pdf located in the Evidence Files folder.

19. In the Data Format drop-down list, select the file format as File.

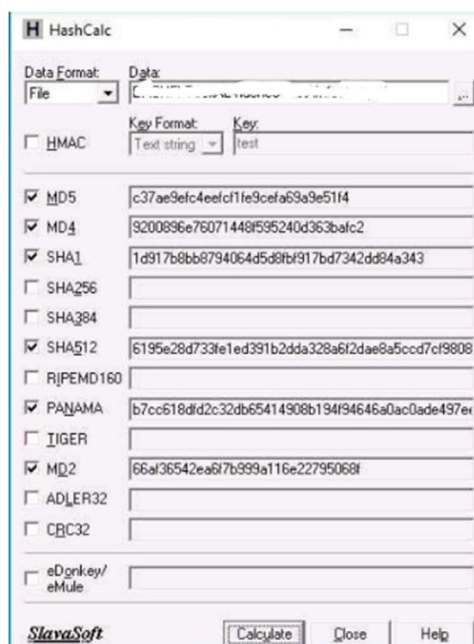


20. Click the ellipsis button associated with the Data field to select the file.

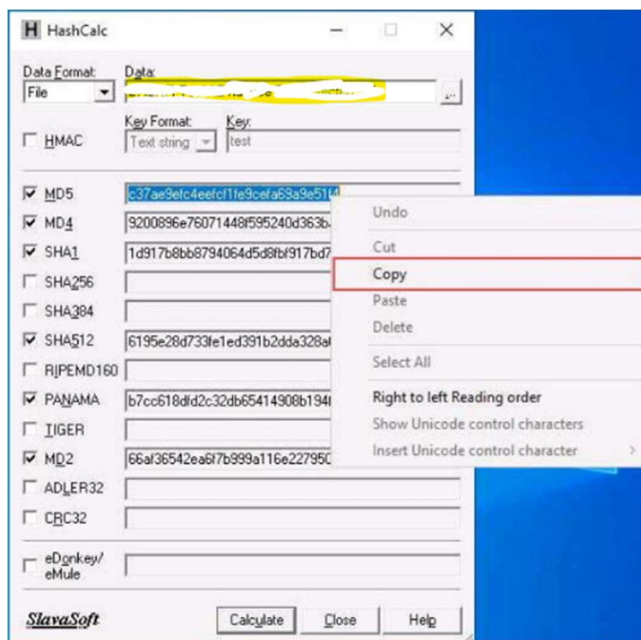
21. The Find window will appear; navigate to [Forensics tools](#) Evidence Files, select Infected.pdf and click Open.



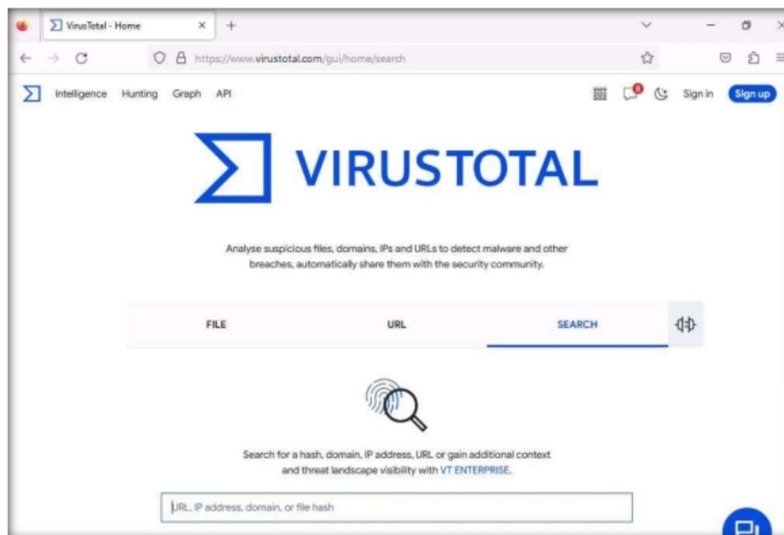
22. The selected file will be displayed in the Data field.
23. Click Calculate to calculate the hash value of the file.



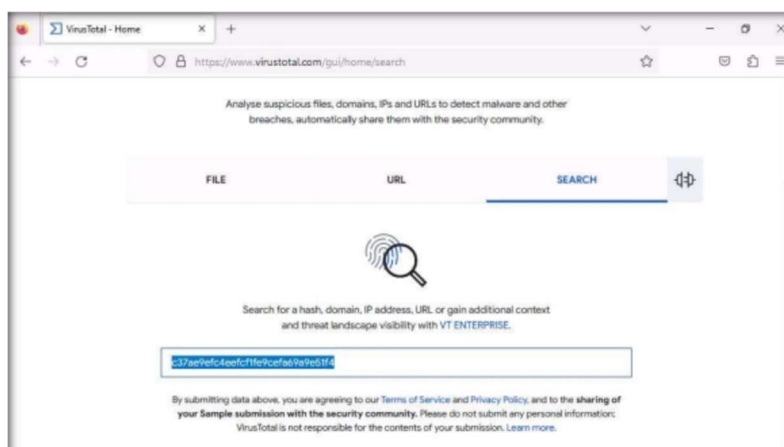
24. Since the MD5 algorithm is already selected, HashCalc calculates the MD5 value followed by the other hashes (that were selected) of the file. Copy the MD5 hash value, as shown in the following screenshot:



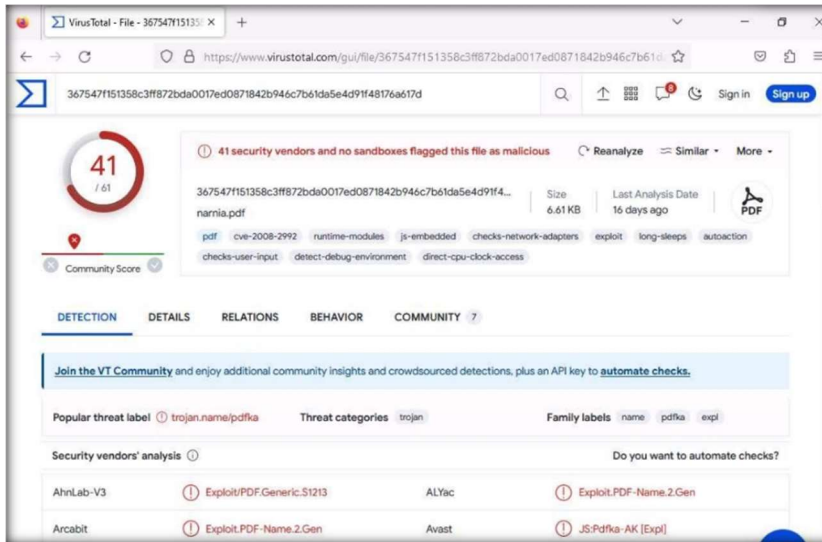
25. Now, launch the Firefox web browser and browse the URL <https://www.virustotal.com/gui/home/search>. The VirusTotal Search page appears, as shown in the screenshot below:



26. Paste the MD5 hash in the Search field and click Enter.



27. VirusTotal searches this value in its database and returns the result, as shown in the following screenshot:



Note: The number of anti-virus engines and detection rate might vary in your lab environment.

28. The result indicates that many anti-virus engines detected the file as malicious. In real-time, when a file appears to be suspicious, you may upload the file or its hash value in malware scanning applications such as VirusTotal to know if the file is malicious. We will be covering malicious pdf analysis in detail in CHFIv11 Module 09 Malware Forensics.
29. In this manner, you can calculate the MD5 hashes of files and text strings and look up the hash values of suspicious files in online malware scanners. Close all open windows.

Lab Analysis

Analyse and document the results of this lab exercise.

Task: tryhackme.com

Create a login account on www.tryhackme.com

The tryhackme.com website is a learning cybersecurity platform where you can develop your skills by working through hands-on guide tasks and supporting videos. You can also learn and test your skills with gamified, real-world cybersecurity challenges.

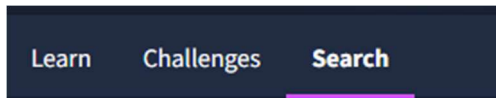
Now that you have created your account.

1. Once you have sign in go to learn



2. To select a free walk through task, select

- a. Search



- b. Type Forensics



- c. In the drop-down menus below the search, select the following in red circle:



- d. Chose any of the free walkthrough exercises and give it a go.

If you want specific labs such as **Forensics** type *forensics* in the section “Search security terms or topics” see figure above and attempt a lab of your choice. **Each week try to complete a different one.**

There are many other similar site. If you are using a different one please share it to the class. We will use a number of this site free walkthrough exercise but the option is yours if you want to subscribe (pay).