

Security Analysis, Techniques and procedures

Lab 5a

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

Introduction

The Computer Forensics investigation is a methodological approach of preparing for an investigation, collecting and analyzing digital evidence. It is also managing the case from the reporting of the crime till the case's conclusion. The process takes place in a computer forensic lab.

Computer forensics plays a vital role in the investigation and prosecution of cyber criminals. The process includes acquisition, inspection, and reporting of information stored across computers and networks related to a civil or criminal incident. Forensic investigators are trained professionals who can extract, analyze, report, and investigate cases that involve technology as the source or the victim of a crime.

As a computer forensics investigator, it is important to have knowledge of the process involved during a forensics investigation, such as collecting digital evidence, building a computer forensics lab, recovering the deleted data, etc.

Task 1:

- Sign in **www.tryhackme.com**
- Go to Hackactivities → select free only from the **show** pop down list → walkthrough from the **Type** pop down list.
- Select **Forensics** and attempt a lab of your choice. Each week try to complete a different one.

Task 2: Generating MD5 Hashes using MD5 Calculator

MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with big files with sizes measured in GBs. It features a progress counter and a text field from which the final MD5 hash can be copied easily to the clipboard.

Lab Scenario

During an investigative process, a forensics examiner was successful in extracting some programs from a target computer. The examiner uses MD5 hash values to check the presence of similar file across a malware database and finds the malicious file.

To be an expert computer forensic investigator, one must have sound knowledge of tools used for computing hashes and checking the checksums.

Lab Objectives

This lab will give you experience encrypting data and show you how to do it. It will teach you how to:

- Use encrypting commands.
- Calculate the MD5 value of selected files.

Lab Environment

This lab requires:

- MD5 Calculator, which is located at https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EnzTNmxJT11LmKy1hW3nF5QBU3Y8mJDi24Sgh05qo5Z1IQ?e=nSTky9
- A computer running Windows Server 2012 or 2016 virtual machine.
- Administrative privileges to run tools

- You can also download the latest version of **MD5 Calculator** from <http://www.bullzip.com/download.php>.
- Kindly note that, if you decide to download the latest version, then screenshots shown in the lab might differ.

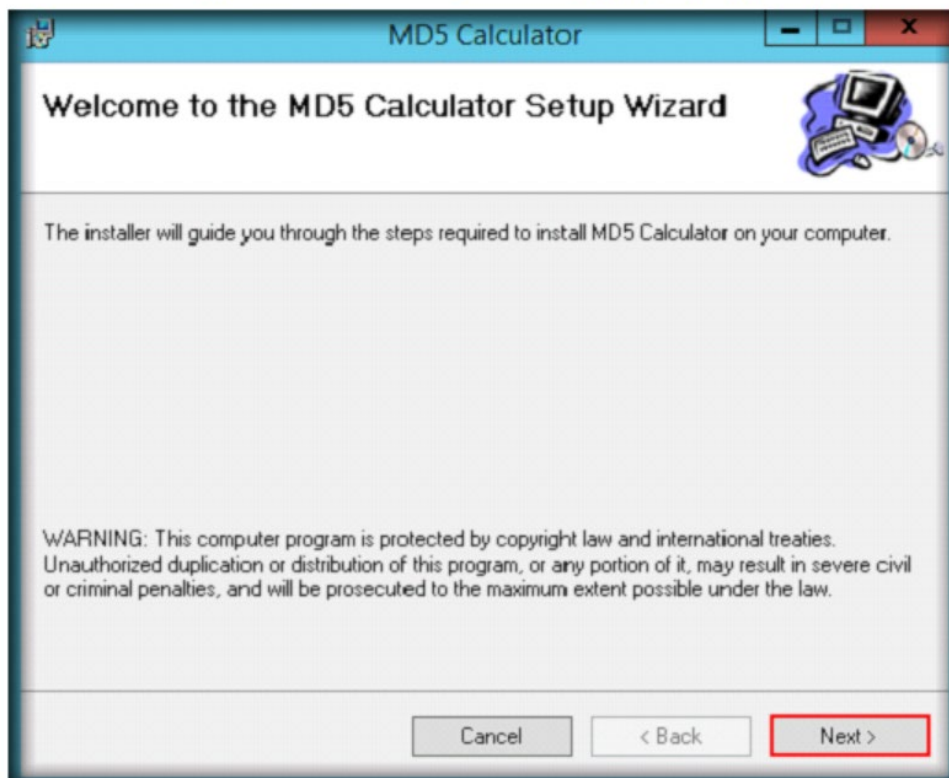
Overview of MD5 Calculator

MD5 Calculator is a bare-bones program for calculating and comparing MD5 files. While its layout leaves something to be desired, its results are fast and simple.

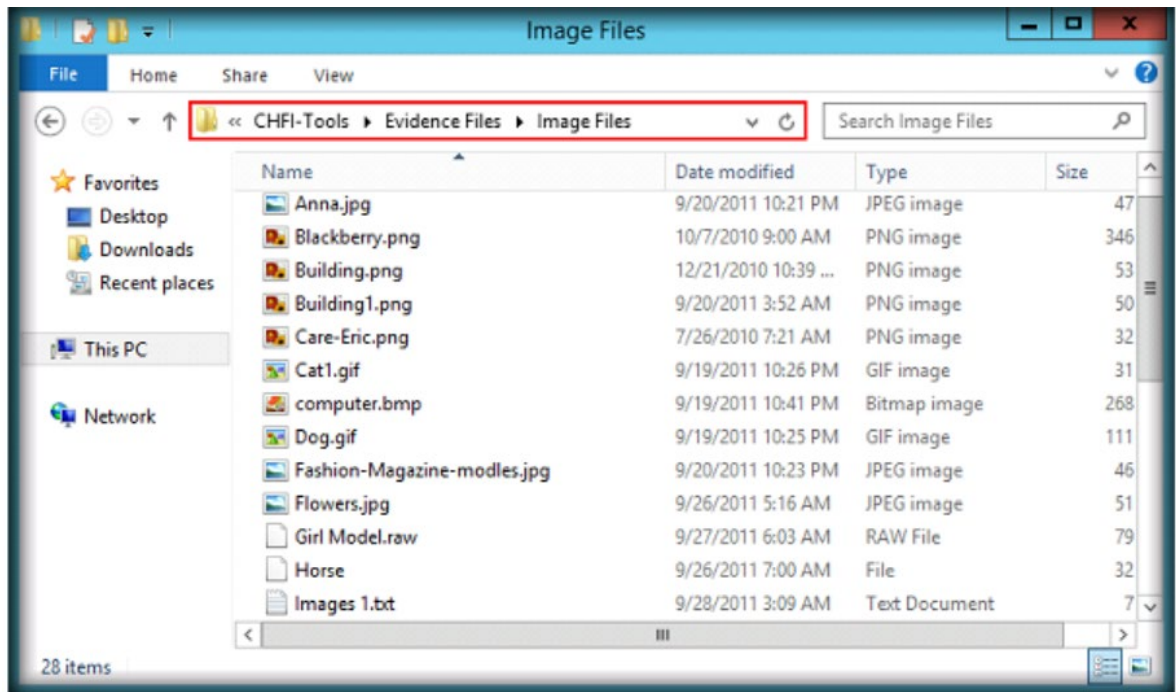
Lab Tasks

1. Navigate to folder for MD5 Calculator: https://uowtsd-my.sharepoint.com/:f/g/person/carlene_campbell_uwtsd_ac_uk/EnzTNmxJT11LmKy1hW3nF5QBU3Y8mJDi24Sgh05qo5Z1IQ?e=nSTky9
2. Double-click **md5calc(1.0.0.0).msi** to launch the setup, and then follow the wizard-driven installation steps to install the application.

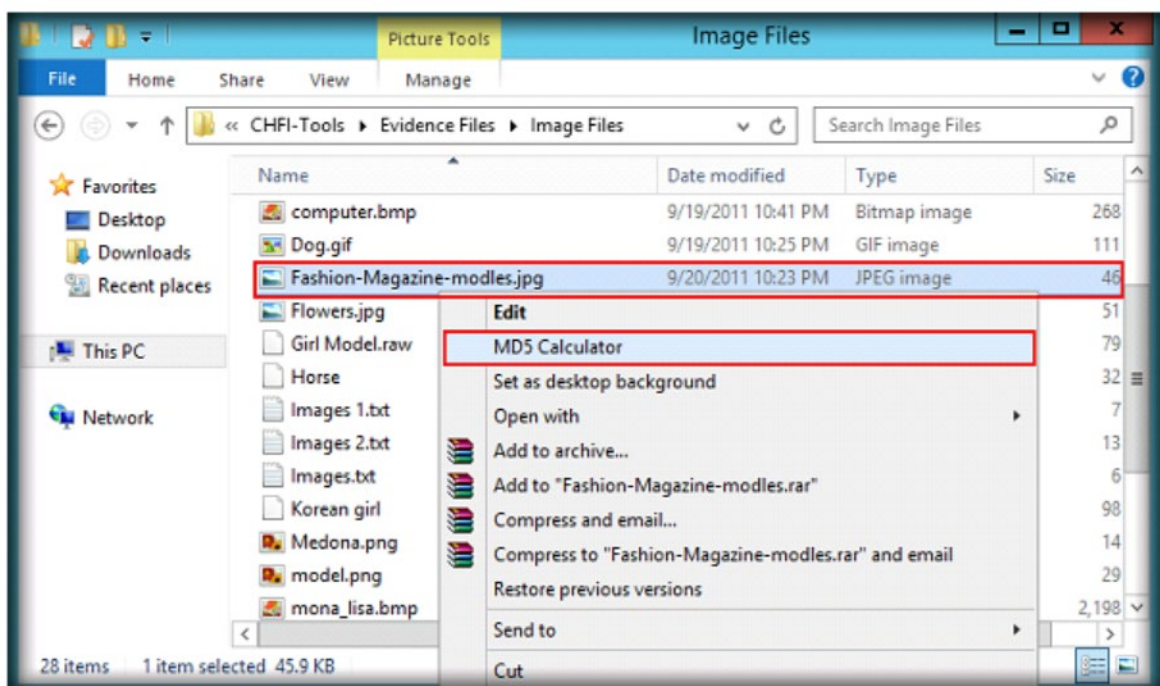
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



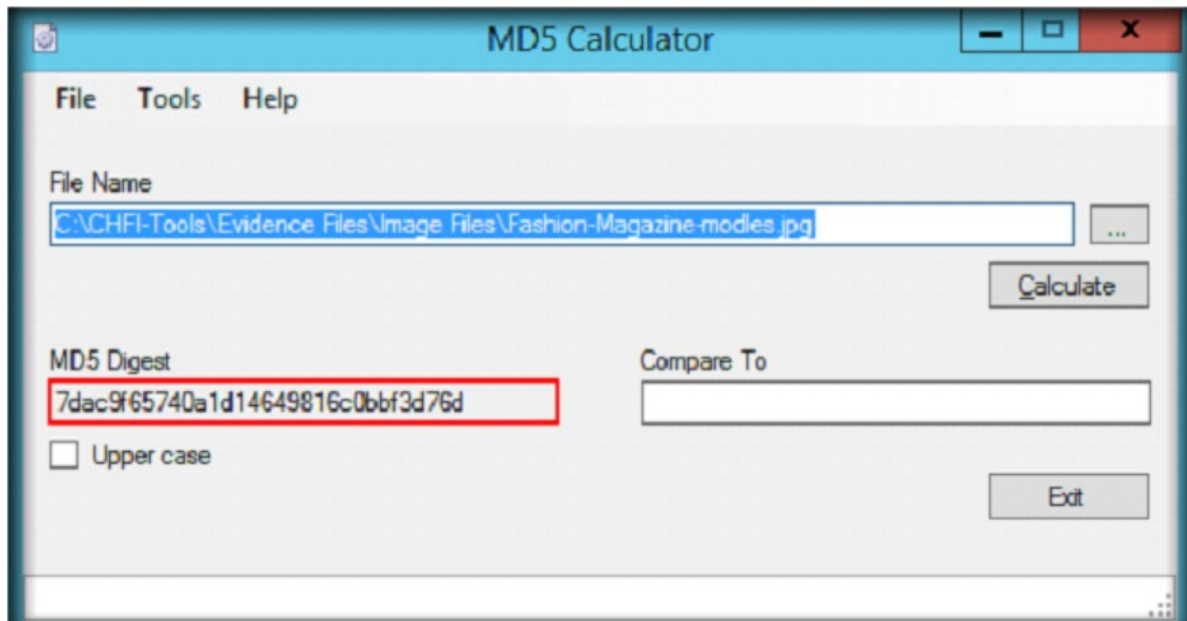
3. Navigate for the evidence file at: https://uwotds-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwotds_ac_uk/EsWoEgmixRFGuPaibErStZEBYeJzohgiH0yiludn8qVB8Q?e=mBUdhI



4. To calculate the MD5 hash of a file, first select a particular file, right-click on it and then select MD5 Calculator from the context menu.

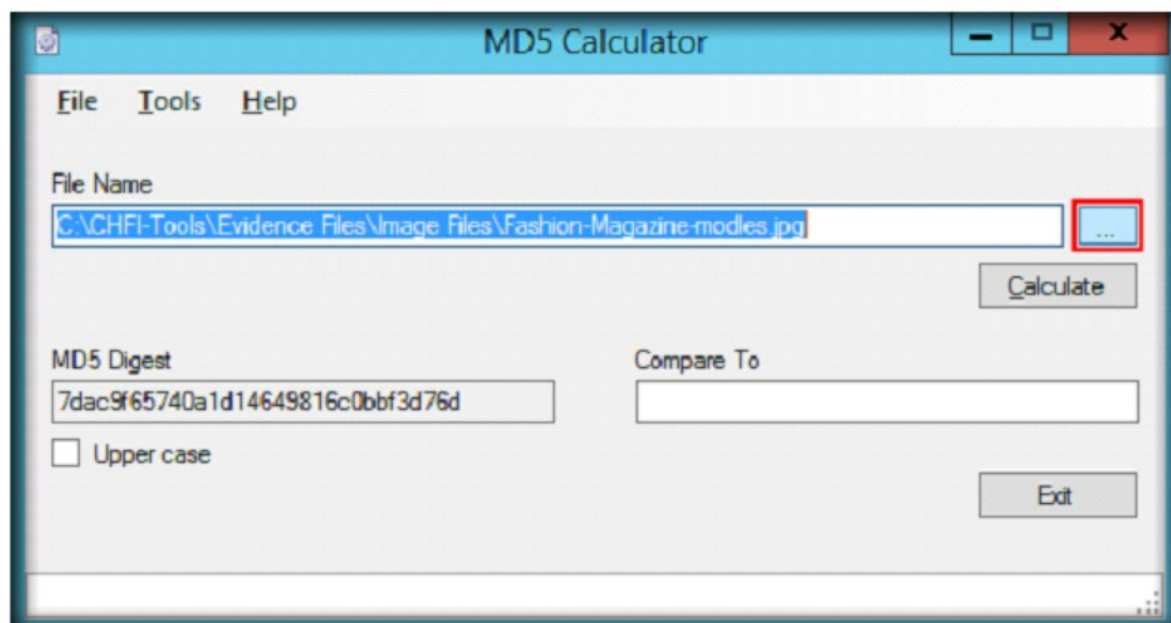


- The **MD5 Calculator** window will subsequently appear, displaying the MD5hash value for the selected file as shown in the following screenshot:

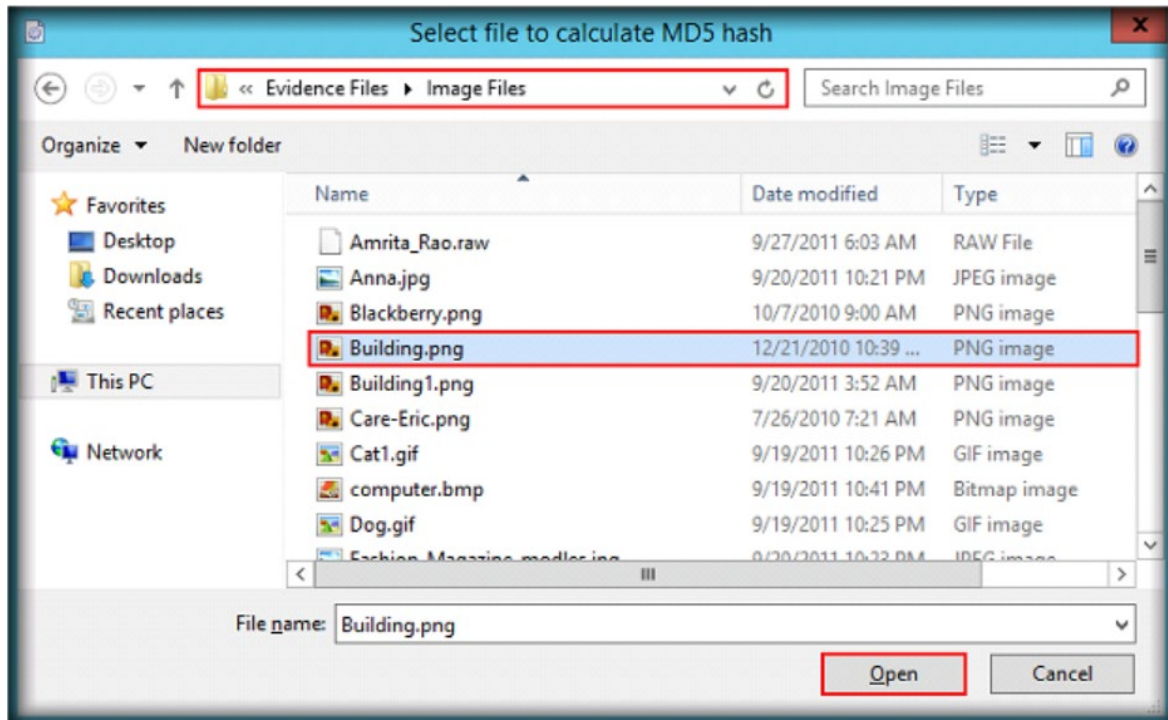


Note: When the tool is used for the first time, it displays the result of the selected file directly under the **MD5 Digest** column and there is no need to click the **Calculate** button.

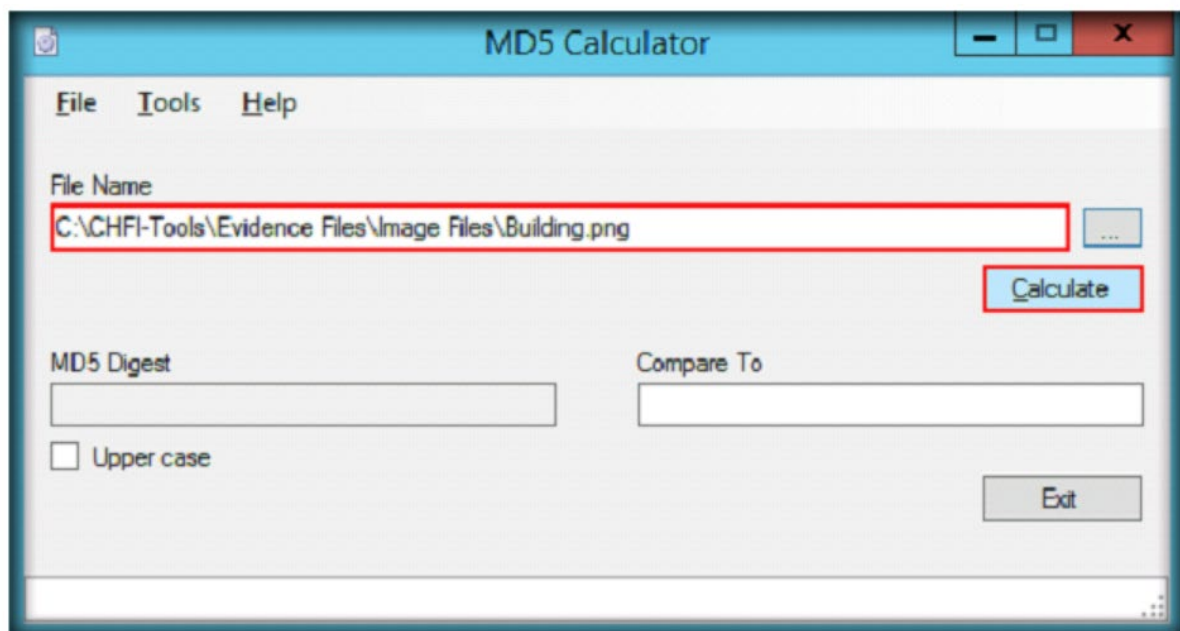
- If you want to calculate the hash value of another file, click the **ellipsis** button corresponding to the **File Name** field.



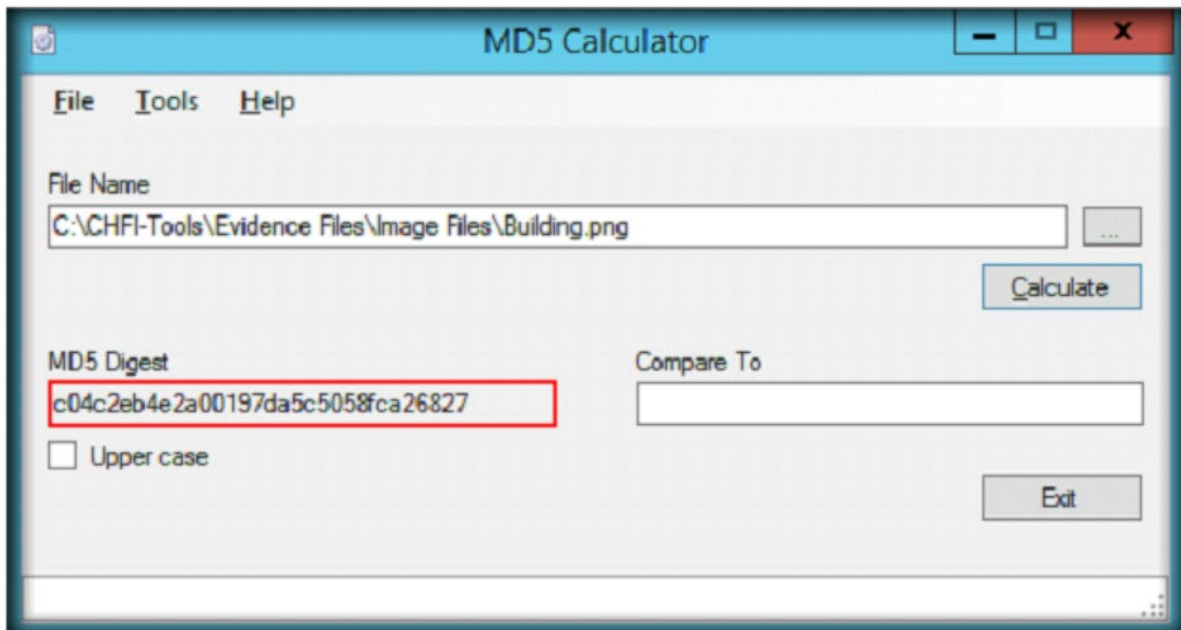
7. The select file to calculator MD5 hash window will pop up. Navigate to https://uwotd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwotd_ac_uk/EsWoEgmixRFGuPaibErStZEBYeJzohgih0yiludn8qVB8Q?e=mBUdhl, select a file other than the previous selected file, (in the below screenshot Building.png file was selected) and click open.



8. The selected file will be displayed in the **File Name** field, click the **Calculate** button to calculate the MD5 hash of the file.



9. **MD5 Calculator** displays the **MD5 Digest** (hash value) for the selected file as shown in the following screenshot:



Lab Analysis

Analyze and document all the calculated hash values related to this lab exercise by using MD5 calculator.

1. Now try to use another Calculator such as HashCalc to repeat the process.
2. Analyse and document all the calculated hash values from the chosen calculator used.