Sapiens Forensic Hash Calculator

Evidence Integrity Suite for Police, Digital Forensic Investigators and Legal Professionals

---

What is Sapiens Forensic Hash Calculator?

Sapiens Forensic Hash Calculator is a digital forensic tool used to verify that electronic evidence has not been modified.
It can:

- ✔ Generate hash values for any file
- ✔ Generate hash values for USB drives, hard disks and memory cards
- ✔ Compare two folders and verify whether both contain exactly the same data
- ✔ Verify whether a known hash matches a calculated hash

The software is designed for **Police Departments, Forensic Laboratories, Cyber Cells and Digital Investigation Teams and Legal Professionals.**



---

1. HASH Module – Calculate Hash Value of a File

1. Double click on Sapiens Forensic Hash Calculator.exe
2. Click on “Run Anyway “
3. Open the **HASH** tab. (By Deafult it is open)
4. Select the **Data Format** (File, Text, Folder, etc.).
5. Click **Browse** and select the evidence file.
6. Alternatively, drag and drop the file into the **Drag & Drop** area and Hash value will be automatically calculated for selected algorithm.

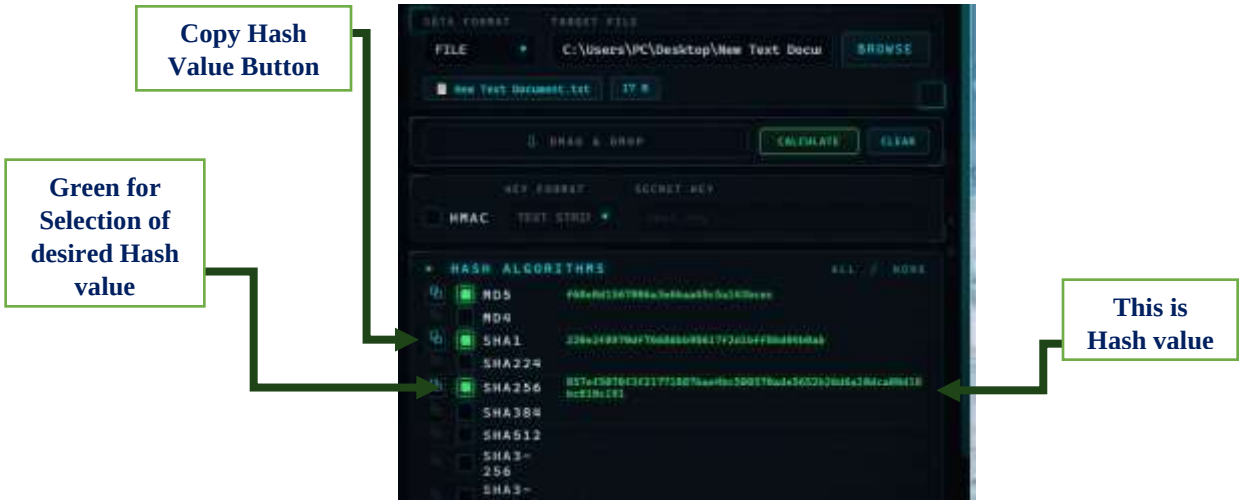


7. Select one or more required hash algorithms. Selection will light it to the green sqaure. (recommended: **SHA-256**).
8. Click **Calculate**.
9. Wait until the calculation is completed.
10. View the generated hash values in the results section.
11. Copy or save the required hash value for documentation.

---

2. Selecting Hash Algorithms

1. Tick the checkbox beside each required algorithm.
2. Click **ALL** to select all available algorithms. Selection will light it to the green sqaure.
3. Click **NONE** to clear all selections.
4. For forensic investigations, **SHA-256** is recommended.
5. Click **Calculate** to generate the selected hash values.



Note: SHA-256 is the recommended hash algorithm for most digital forensic investigations and evidence verification.

---

3. Verify Known Hash (Optional if Required)

1. Generate the hash value of the selected evidence.
2. Copy the known hash value from the case record or report.
3. Paste the known hash into the **Verify Known Hash** field.
4. The software automatically compares both values.
5. If the values are identical, **MATCH** is displayed.
6. If they differ, verify that the correct evidence and algorithm have been selected.

---

4. Compare Two Folders

1. Open the **COMPARE** tab.
2. Click **Select Folder 1** and choose the original folder.
3. Click **Select Folder 2** and choose the copied folder.
4. Select the required hash algorithm.
5. Click **Compare**.
6. Wait for the comparison process to complete.
7. Review the comparison status displayed at the bottom of the screen.

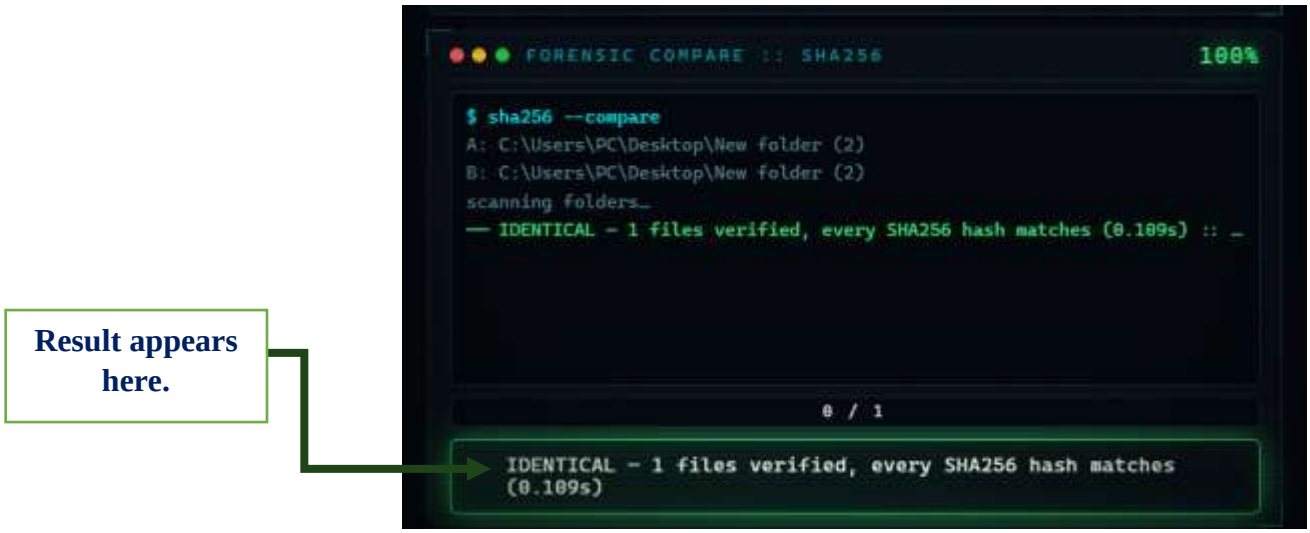
Select First & Second Folder which you want to compare



---

5. Understanding Comparison Results

1. The software scans all files in both folders.
2. A progress bar displays the comparison status.
3. The console window shows the comparison process in real time.
4. **IDENTICAL** indicates that every file matches successfully.
5. **DIFFERENT** indicates that one or more files do not match.
6. Save or record the comparison result if required.

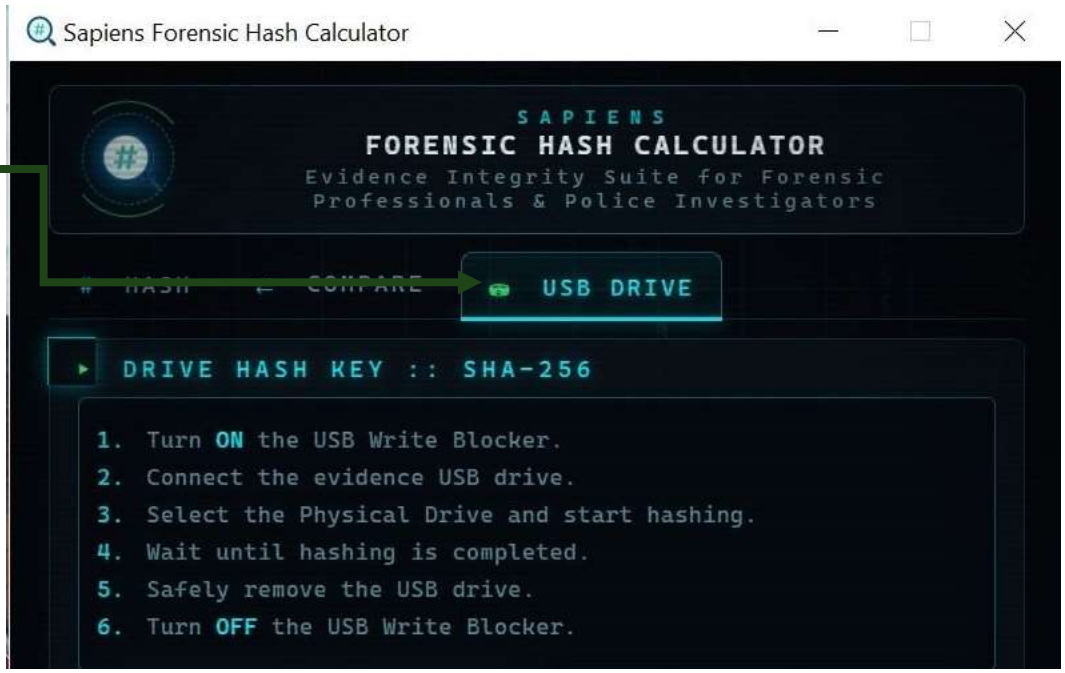


---

6. Calculate Hash of a USB Drive (Pen Drive, Hard Disk, Memory Card or Any Memory Device)

1. Open the **USB DRIVE** tab.
2. Enable **USB Write-Block** before connecting the evidence device.
3. Connect the USB drive, memory card, SSD, or hard disk.
4. Select the required **Physical Drive** from the list.
5. Click **Start Hashing** (or the available hashing button).
6. Wait until the hashing process is completed.
7. Record the generated hash value.
8. Safely remove the storage device.
9. Disable **USB Write-Block** when normal USB operation is required.

For Pen Drive or Hard Disk Hash Value



---

7. Enable USB Write-Block

1. Ensure no evidence device is currently connected.
2. Click **USB Write-Block**.
3. Wait until the status changes from **OFF** to **ON**.
4. Connect the evidence storage device.
5. Continue with the hashing process.

1. First ON Write Blocker



Note: Always enable **USB Write-Block** before connecting evidence media to prevent accidental modification.

---

8. USB Write-Block Enabled

1. Confirm that **USB Write-Block** is **ON**.
2. Connect the evidence storage device.
3. Select the required physical drive.



2. Your Pen Drive or Hard Disk letter, Company and size will appear here.

4. Start the hashing process.
5. Wait until hashing is completed.
6. Record the generated hash value.
7. Safely remove the device.
8. Turn **USB Write-Block OFF** when evidence acquisition is complete.

Don't Forget to OFF Write Block



9. Quick Workflow – File Hash

1. Open **HASH**.
2. Select the evidence file.
3. Choose **SHA-256**.
4. Click **Calculate**.
5. Save the generated hash.

---

10. Quick Workflow – Folder Comparison

1. Open **COMPARE**.
2. Select Folder 1.
3. Select Folder 2.
4. Choose **SHA-256**.
5. Click **Compare**.
6. Verify that the result shows **IDENTICAL**.

---

11. Quick Workflow – USB Drive Hash

1. Open **USB DRIVE**.
2. Enable **USB Write-Block**.
3. Connect the evidence storage device.
4. Select the physical drive.
5. Start hashing.
6. Record the generated hash value.
7. Safely remove the device.
8. Disable **USB Write-Block**.

Note: Always enable **USB Write-Block** before connecting evidence media to prevent accidental modification.