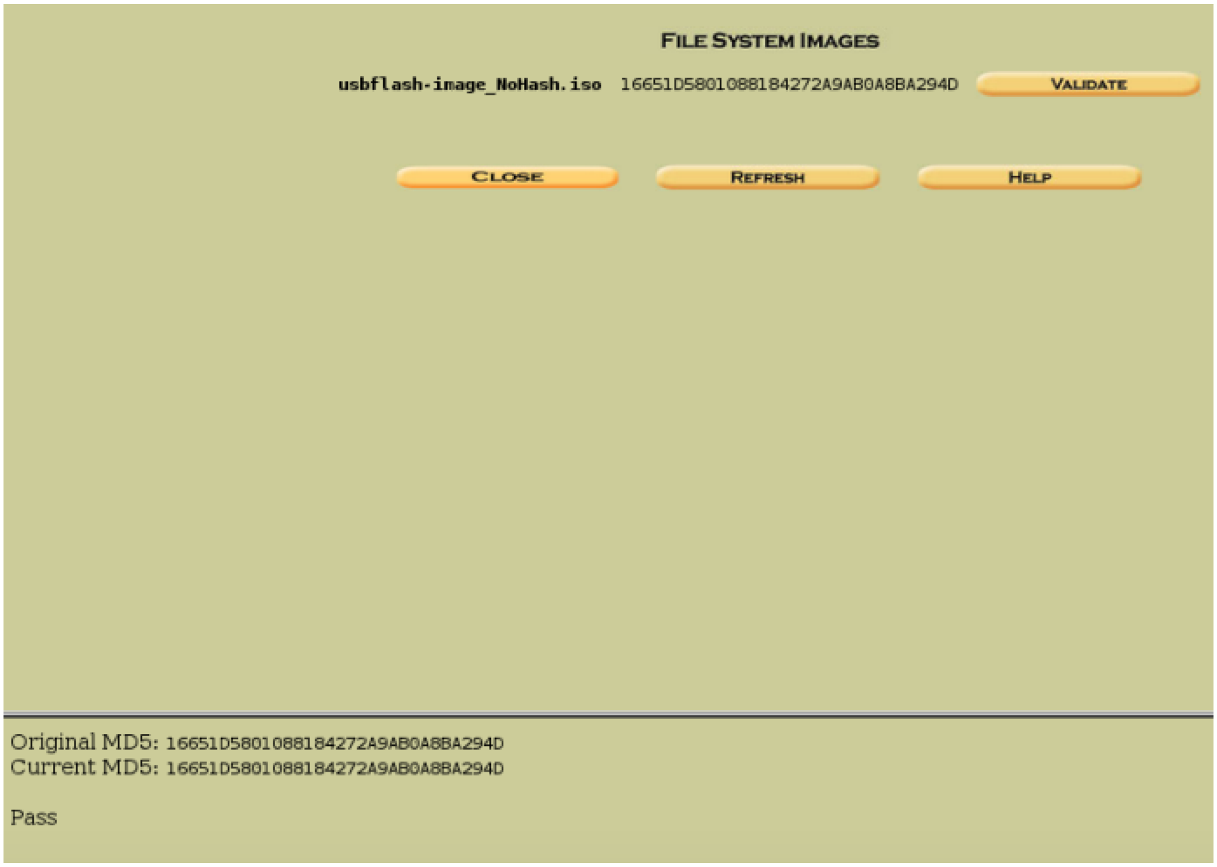
Lab Assignment: Autopsy

Basundhara Dey
b3661281

1. Encode the evidence image using MD5 hashing:



FILE SYSTEM IMAGES

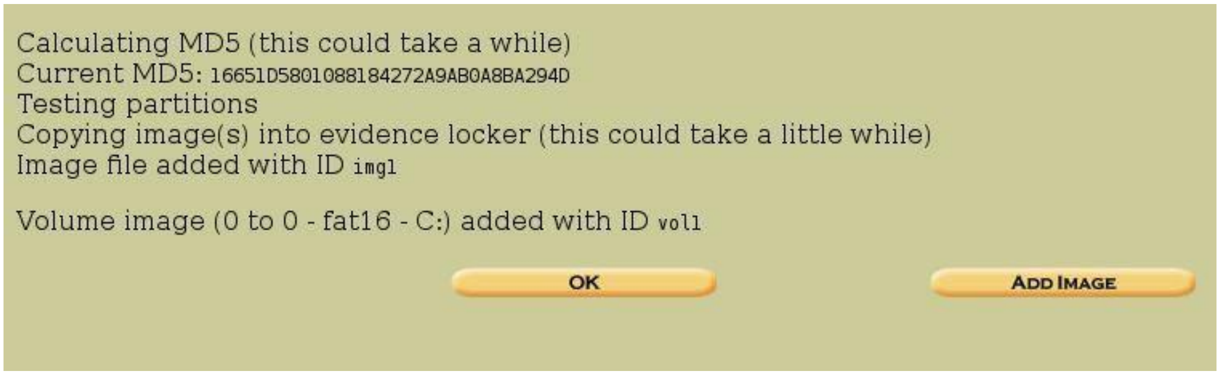
usbflash-image_NoHash.iso 16651D5801088184272A9AB0A8BA294D

```
Original MD5: 16651D5801088184272A9AB0A8BA294D
Current MD5: 16651D5801088184272A9AB0A8BA294D

Pass
```

The above image or screenshot shows the MD5 hashing value for the given image file.

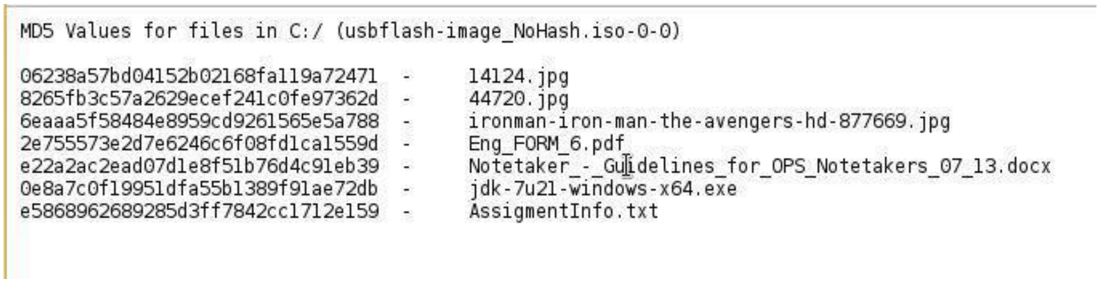
The image below shows the MD5 hashing value that is generated by Autopsy.



```
Calculating MD5 (this could take a while)
Current MD5: 16651D5801088184272A9AB0A8BA294D
Testing partitions
Copying image(s) into evidence locker (this could take a little while)
Image file added with ID img1

Volume image (0 to 0 - fat16 - C:) added with ID vol1
```

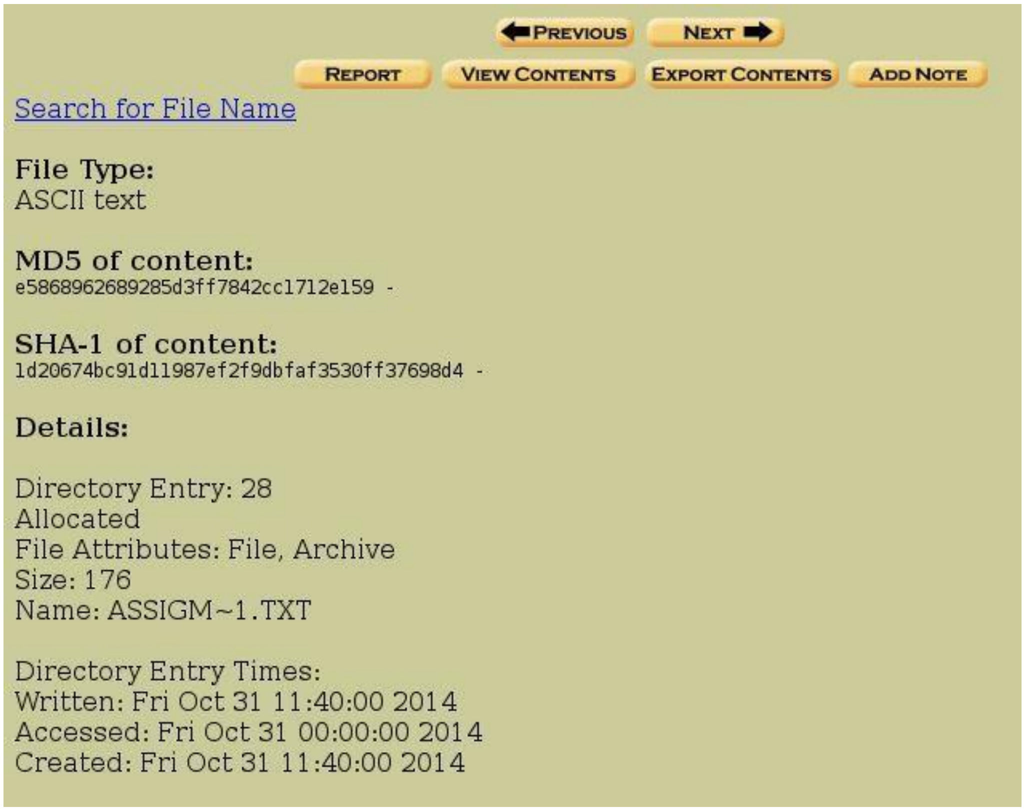
The next image shows us the MD5 value for the various files that the .ISO image contains.



```
MD5 Values for files in C:/ (usbflash-image_NoHash.iso-0-0)

06238a57bd04152b02168fa119a72471  -     14124.jpg
8265fb3c57a2629ecef241c0fe97362d  -     44720.jpg
6eaaa5f58484e8959cd9261565e5a788  -     ironman-iron-man-the-avengers-hd-877669.jpg
2e755573e2d7e6246c6f08fd1ca1559d  -     Eng_FORM_6.pdf
e22a2ac2ead07d1e8f51b76d4c91eb39  -     Notetaker_-_Guidelines_for_OPS_Notetakers_07_13.docx
0e8a7c0f19951dfa55b1389f91ae72db  -     jdk-7u21-windows-x64.exe
e5868962689285d3ff7842cc1712e159  -     AssigmentInfo.txt
```

2. The image below is a screenshot of the details of the AssignmentInfo.txt file. I have also generated the File Activity Timeline report, which is attached in the compressed file submitted along with the project.



Search for File Name

File Type:
ASCII text

MD5 of content:
e5868962689285d3ff7842cc1712e159 -

SHA-1 of content:
1d20674bc91d11987ef2f9dbfaf3530ff37698d4 -

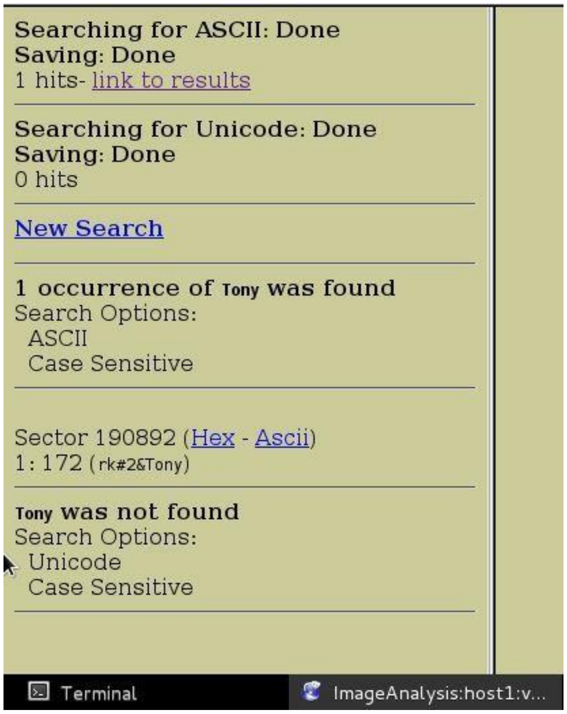
Details:

Directory Entry: 28
Allocated
File Attributes: File, Archive
Size: 176
Name: ASSIGM~1.TXT

Directory Entry Times:
Written: Fri Oct 31 11:40:00 2014
Accessed: Fri Oct 31 00:00:00 2014
Created: Fri Oct 31 11:40:00 2014

3. Searching for the string “Tony” in the image file

The snapshot below displays the results when the keyword ‘Tony’ was searched in the entire image (ISO) file. It was found in the file **AssignmentInfo.txt.**



Searching for ASCII: Done
Saving: Done
1 hits- link to results

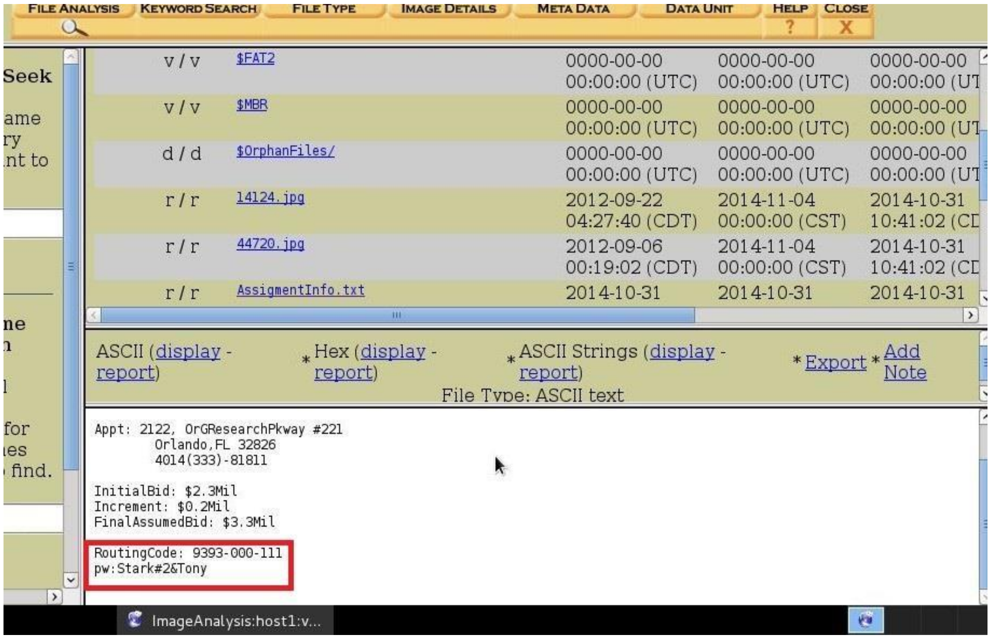
Searching for Unicode: Done
Saving: Done
0 hits

New Search

1 occurrence of `Tony` was found
Search Options:
ASCII
Case Sensitive

Sector 190892 (Hex - Ascii)
1: 172 (rk#2&Tony)

`Tony` was not found
Search Options:
Unicode
Case Sensitive



v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UT
v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UT
d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UT
r / r	14124.jpg	2012-09-22 04:27:40 (CDT)	2014-11-04 00:00:00 (CST)	2014-10-31 10:41:02 (CD
r / r	44720.jpg	2012-09-06 00:19:02 (CDT)	2014-11-04 00:00:00 (CST)	2014-10-31 10:41:02 (CD
r / r	AssigmentInfo.txt	2014-10-31	2014-10-31	2014-10-31

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ASCII text

```
Appt: 2122, OrGResearchPkway #221
        Orlando,FL 32826
        4014(333)-81811

InitialBid: $2.3Mil
Increment: $0.2Mil
FinalAssumedBid: $3.3Mil

RoutingCode: 9393-000-111
pw:Stark#2&Tony
```

Experience with the tool:

The Autopsy Forensic Browser tool was easy to use and learn. This assignment helped me learn the forensic details of any file including history, encoding method etc., which is crucial for digital forensics.

Through this assignment, I have received the opportunity to perform Disk Forensics on the given usb flash image and received experience in using the different functions of Autopsy Forensic Browser and its analysis methods of search and case management. In my opinion, it forms a powerful forensic analysis tool as it has a wide variety of functions.