Digital Forensics Lab Report: 9

Date: 26-10-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

Aim/Purpose: Study of a Hash and Hex analysis tools

Tool Names:

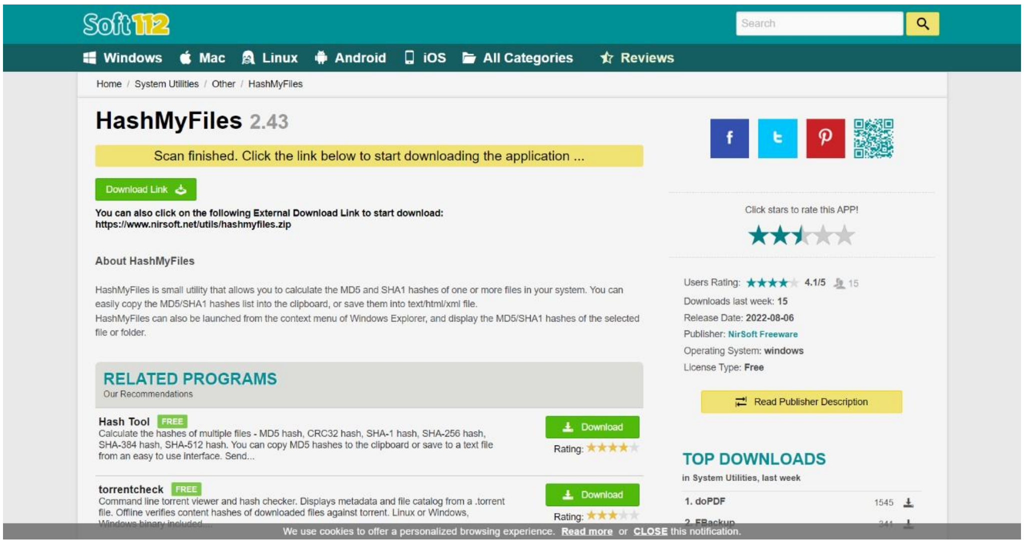
1. WinHEX :- WinHex is a hexadecimal editor for the Windows operating system. It is used for forensics, data recovery, low-level data processing, and IT security. It allows the user to view files in hexadecimal format.

2. Garrykesler

3. Hashmefileignoreware:- HashMyFiles is small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system. You can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file.HashMyFiles can also be launched from the context menu of Windows Explorer, and display the MD5/SHA1 hashes of the selected file or folder.

Steps: -

Download and Install HashMyFiles :- **https://hashmyfiles.soft112.com/modal-download.htmland Download HashMyFiles as ZIP. Extract the zip file to get the.exefile.**



Home / System Utilities / Other / HashMyFiles

HashMyFiles 2.43

Scan finished. Click the link below to start downloading the application ...

You can also click on the following External Download Link to start download:
https://www.nirsoft.net/utils/hashmyfiles.zip

About HashMyFiles

HashMyFiles is small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system. You can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file.
HashMyFiles can also be launched from the context menu of Windows Explorer, and display the MD5/SHA1 hashes of the selected file or folder.

RELATED PROGRAMS
Our Recommendations

Hash Tool FREE
Calculate the hashes of multiple files - MD5 hash, CRC32 hash, SHA-1 hash, SHA-256 hash, SHA-384 hash, SHA-512 hash. You can copy MD5 hashes to the clipboard or save to a text file from an easy to use interface. Send...
Rating: ★★★★☆

torrentcheck FREE
Command line torrent viewer and hash checker. Displays metadata and file catalog from a .torrent file. Offline verifies content hashes of downloaded files against torrent. Linux or Windows, Windows binary included....
Rating: ★★★☆☆

Click stars to rate this APP!

Users Rating: ★★★★☆ 4.1/5 15
Downloads last week: 15
Release Date: 2022-08-06
Publisher: NirSoft Freeware
Operating System: windows
License Type: Free

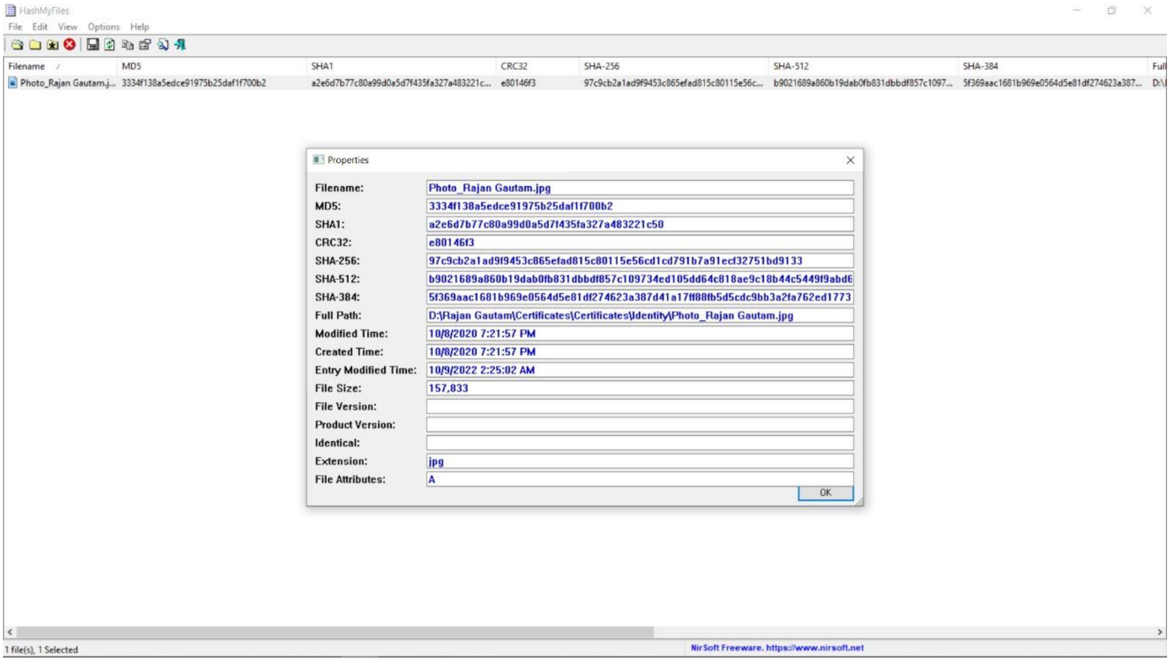
TOP DOWNLOADS
in System Utilities, last week

1. doPDF 1545
2. FBackup 341

We use cookies to offer a personalized browsing experience. Read more or CLOSE this notification.

Figure 1 HashMyFiles download website

1. Open the Application and open any file.



Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384	Ful
Photo_Rajan Gautam.j...	3334f138a5edce91975b25daf1f700b2	a2e6d7b77c80a99d0a5d7f435fa327a483221c...	e80146f3	97c9cb2a1ad9f9453c865efad815c80115e56c...	b9021689a860b19dab0fb831dbbdf857c1097...	5f369aac1681b969e0564d5e81df274623a387...	D:\

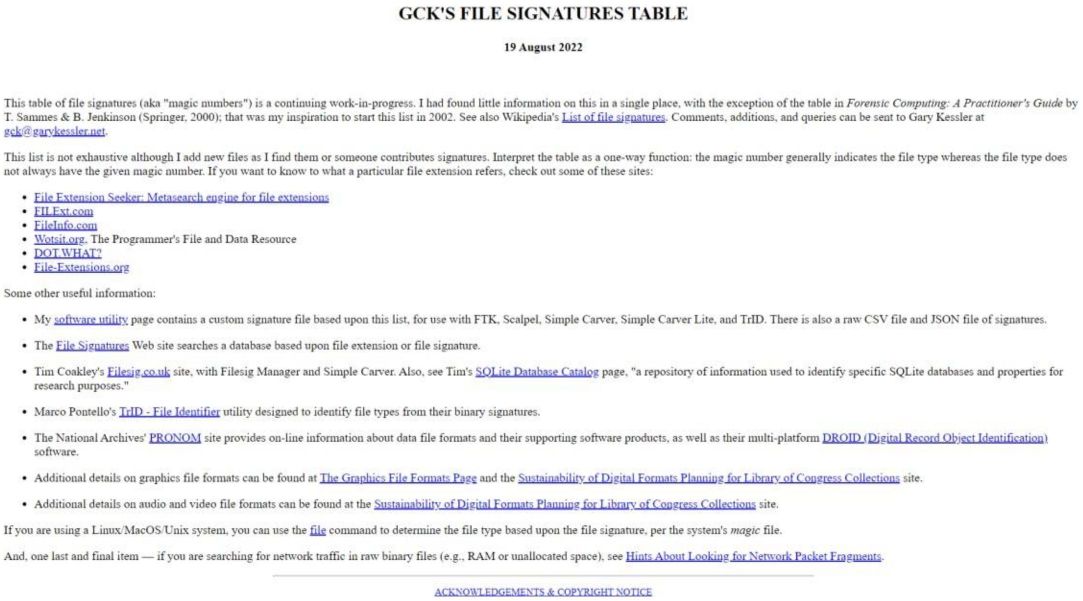
Properties

Filename:	Photo_Rajan Gautam.jpg
MD5:	3334f138a5edce91975b25daf1f700b2
SHA1:	a2e6d7b77c80a99d0a5d7f435fa327a483221c50
CRC32:	e80146f3
SHA-256:	97c9cb2a1ad9f9453c865efad815c80115e56cd1cd791b7a91ecf32751bd9133
SHA-512:	b9021689a860b19dab0fb831dbbdf857c109734ed105dd64c818ae9c18b44c5449f9abd6
SHA-384:	5f369aac1681b969e0564d5e81df274623a387d41a17ff88fb5d5cdc9bb3a2fa762ed1773
Full Path:	D:\Rajan Gautam\Certificates\Certificates\Identity\Photo_Rajan Gautam.jpg
Modified Time:	10/8/2020 7:21:57 PM
Created Time:	10/8/2020 7:21:57 PM
Entry Modified Time:	10/9/2022 2:25:02 AM
File Size:	157,833
File Version:	
Product Version:	
Identical:	
Extension:	jpg
File Attributes:	A

1 file(s), 1 Selected
NirSoft Freeware. https://www.nirsoft.net

Figure 2 HasmyFiles

2. Access Garrykesler from this URLhttps://www.garykessler.net/library/file_sigs.html



GCK'S FILE SIGNATURES TABLE

19 August 2022

This table of file signatures (aka "magic numbers") is a continuing work-in-progress. I had found little information on this in a single place, with the exception of the table in *Forensic Computing: A Practitioner's Guide* by T. Sammes & B. Jenkinson (Springer, 2000); that was my inspiration to start this list in 2002. See also Wikipedia's List of file signatures. Comments, additions, and queries can be sent to Gary Kessler at gck@garykessler.net.

This list is not exhaustive although I add new files as I find them or someone contributes signatures. Interpret the table as a one-way function: the magic number generally indicates the file type whereas the file type does not always have the given magic number. If you want to know to what a particular file extension refers, check out some of these sites:

- File Extension Seeker: Metasearch engine for file extensions
- FILExt.com
- FileInfo.com
- Wotsit.org, The Programmer's File and Data Resource
- DOT.WHAT?
- File-Extensions.org

Some other useful information:

- My software utility page contains a custom signature file based upon this list, for use with FTK, Scalpel, Simple Carver, Simple Carver Lite, and TrID. There is also a raw CSV file and JSON file of signatures.
- The File Signatures Web site searches a database based upon file extension or file signature.
- Tim Coakley's Filesig.co.uk site, with Filesig Manager and Simple Carver. Also, see Tim's SQLite Database Catalog page, "a repository of information used to identify specific SQLite databases and properties for research purposes."
- Marco Pontello's TrID - File Identifier utility designed to identify file types from their binary signatures.
- The National Archives' PRONOM site provides on-line information about data file formats and their supporting software products, as well as their multi-platform DROID (Digital Record Object Identification) software.
- Additional details on graphics file formats can be found at The Graphics File Formats Page and the Sustainability of Digital Formats Planning for Library of Congress Collections site.
- Additional details on audio and video file formats can be found at the Sustainability of Digital Formats Planning for Library of Congress Collections site.

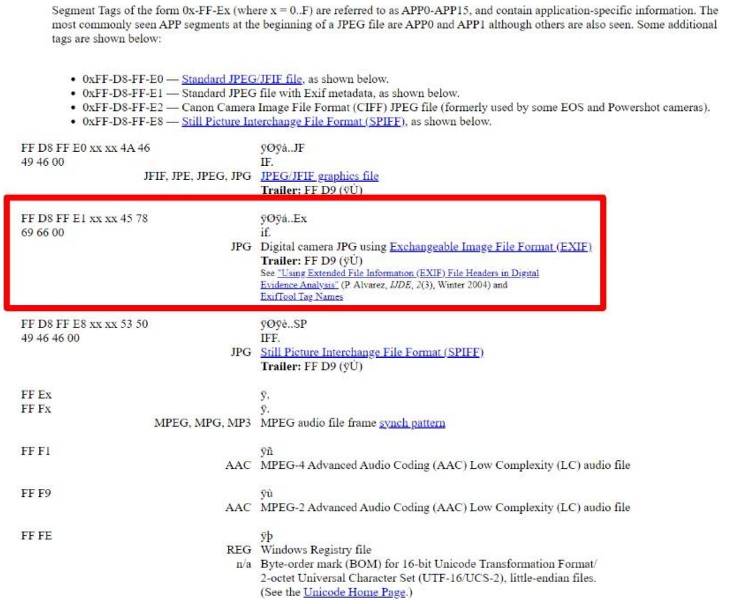
If you are using a Linux/MacOS/Unix system, you can use the file command to determine the file type based upon the file signature, per the system's *magic* file.

And, one last and final item — if you are searching for network traffic in raw binary files (e.g., RAM or unallocated space), see Hints About Looking for Network Packet Fragments.

ACKNOWLEDGEMENTS & COPYRIGHT NOTICE

Figure 3 Garrykesler

3. Check Hex Value for .JPG file in GCK’s file. As per them Hex value for JPG image is ‘FF D8 FF E1 xx xx 4578’.



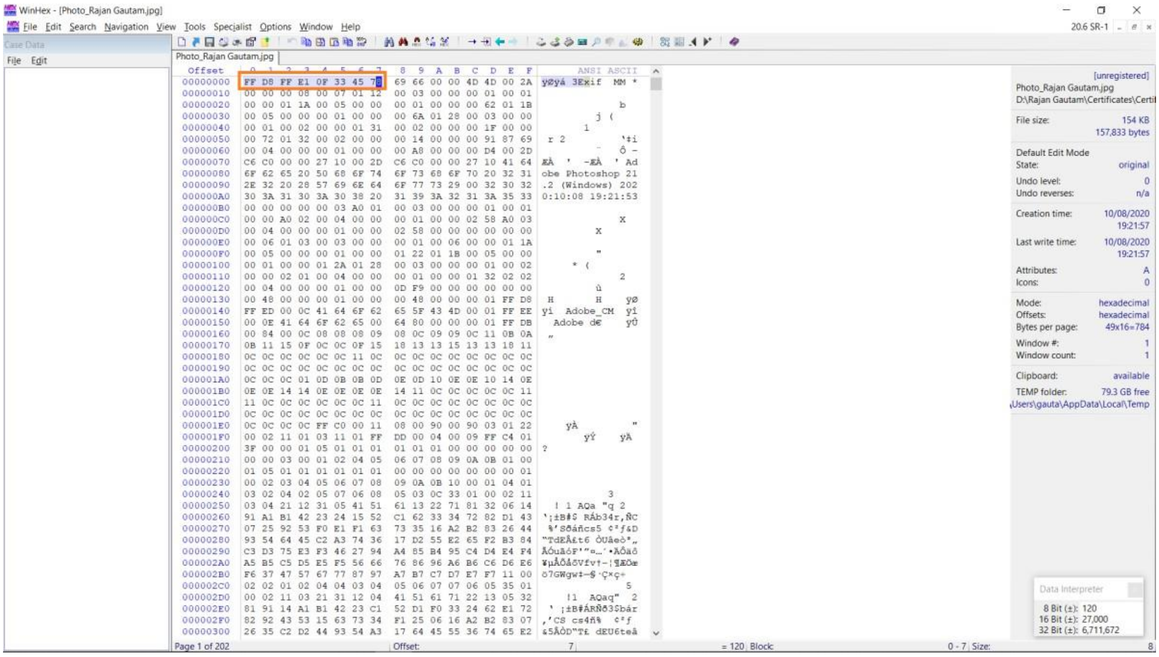
Segment Tags of the form 0x-FF-Ex (where x = 0..F) are referred to as APP0-APP15, and contain application-specific information. The most commonly seen APP segments at the beginning of a JPEG file are APP0 and APP1 although others are also seen. Some additional tags are shown below:

- 0xFF-D8-FF-E0 — Standard JPEG/JFIF file, as shown below.
- 0xFF-D8-FF-E1 — Standard JPEG file with Exif metadata, as shown below.
- 0xFF-D8-FF-E2 — Canon Camera Image File Format (CIFF) JPEG file (formerly used by some EOS and Powershot cameras).
- 0xFF-D8-FF-E8 — Still Picture Interchange File Format (SPIFF), as shown below.

FF D8 FF E0 xx xx 4A 46 49 46 00	JFIF, JPE, JPEG, JPG	ÿØÿà..JF IF. JPEG/JFIF graphics file **Trailer:** FF D9 (ÿÙ)
FF D8 FF E1 xx xx 45 78 69 66 00	JPG	ÿØÿá..Ex if. Digital camera JPG using Exchangeable Image File Format (EXIF) **Trailer:** FF D9 (ÿÙ) See "Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis" (P. Alvarez, *IJDE*, 2(3), Winter 2004) and ExifTool Tag Names
FF D8 FF E8 xx xx 53 50 49 46 46 00	JPG	ÿØÿè..SP IFF. Still Picture Interchange File Format (SPIFF) **Trailer:** FF D9 (ÿÙ)
FF Ex FF Fx	MPEG, MPG, MP3	ÿ. ÿ. MPEG audio file frame synch pattern
FF F1	AAC	ÿñ MPEG-4 Advanced Audio Coding (AAC) Low Complexity (LC) audio file
FF F9	AAC	ÿù MPEG-2 Advanced Audio Coding (AAC) Low Complexity (LC) audio file
FF FE	REG n/a	ÿþ Windows Registry file Byte-order mark (BOM) for 16-bit Unicode Transformation Format/ 2-octet Universal Character Set (UTF-16/UCS-2), little-endian files. (See the Unicode Home Page.)

Figure 4 Garrykesler

4. Open the same file using WinHEX. We can see the same HEX value in the editor which shows the file is .JPGfile.

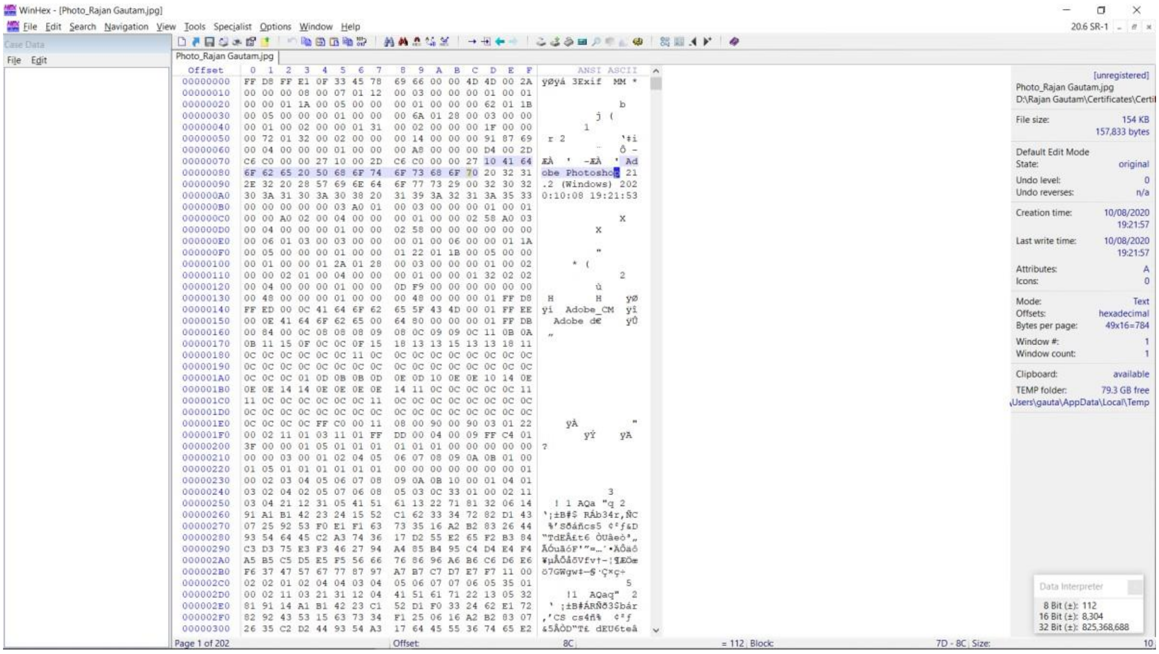

WinHex - [Photo_Rajan Gautam.jpg]
File Edit Search Navigation View Tools Specialist Options Window Help
20.6 SR-1
Case Data
File Edit
Photo_Rajan Gautam.jpg

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   FF D8 FF E1 0F 33 45 78  69 66 00 00 4D 4D 00 2A   ÿØÿá 3Exif  MM *
00000010   00 00 00 08 00 07 01 12  00 03 00 00 00 01 00 01
00000020   00 00 01 1A 00 05 00 00  00 01 00 00 00 62 01 1B              b
00000030   00 05 00 00 00 01 00 00  00 6A 01 28 00 03 00 00            j (
00000040   00 01 00 02 00 00 01 31  00 02 00 00 00 1F 00 00         1
00000050   00 72 01 32 00 02 00 00  00 14 00 00 00 91 87 69    r 2         '‡i
00000060   00 04 00 00 00 01 00 00  00 A8 00 00 00 D4 00 2D          ¨     Ô -
00000070   C6 C0 00 00 27 10 00 2D  C6 C0 00 00 27 10 41 64   ÆÀ  '  -ÆÀ  ' Ad
00000080   6F 62 65 20 50 68 6F 74  6F 73 68 6F 70 20 32 31   obe Photoshop 21
00000090   2E 32 20 28 57 69 6E 64  6F 77 73 29 00 32 30 32   .2 (Windows) 202
000000A0   30 3A 31 30 3A 30 38 20  31 39 3A 32 31 3A 35 33   0:10:08 19:21:53
000000B0   00 00 00 00 00 03 A0 01  00 03 00 00 00 01 00 01
000000C0   00 00 A0 02 00 04 00 00  00 01 00 00 02 58 A0 03              X
000000D0   00 04 00 00 00 01 00 00  02 58 00 00 00 00 00 00          X
000000E0   00 06 01 03 00 03 00 00  00 01 00 06 00 00 01 1A
000000F0   00 05 00 00 00 01 00 00  01 22 01 1B 00 05 00 00          "
00000100   00 01 00 00 01 2A 01 28  00 03 00 00 00 01 00 02        * (
00000110   00 00 02 01 00 04 00 00  00 01 00 00 01 32 02 02              2
00000120   00 04 00 00 00 01 00 00  0D F9 00 00 00 00 00 00          ù
00000130   00 48 00 00 00 01 00 00  00 48 00 00 00 01 FF D8    H       H    ÿØ
00000140   FF ED 00 0C 41 64 6F 62  65 5F 43 4D 00 01 FF EE   ÿí  Adobe_CM  ÿî
00000150   00 0E 41 64 6F 62 65 00  64 80 00 00 00 01 FF DB     Adobe d€    ÿÛ
00000160   00 84 00 0C 08 08 08 09  08 0C 09 09 0C 11 0B 0A    „
00000170   0B 11 15 0F 0C 0C 0F 15  18 13 13 15 13 13 18 11
00000180   0C 0C 0C 0C 0C 0C 11 0C  0C 0C 0C 0C 0C 0C 0C 0C
00000190   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
000001A0   0C 0C 0C 01 0D 0B 0B 0D  0E 0D 10 0E 0E 10 14 0E
000001B0   0E 0E 14 14 0E 0E 0E 0E  14 11 0C 0C 0C 0C 0C 11
000001C0   11 0C 0C 0C 0C 0C 0C 11  0C 0C 0C 0C 0C 0C 0C 0C
000001D0   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
000001E0   0C 0C 0C 0C FF C0 00 11  08 00 90 00 90 03 01 22       ÿÀ          "
000001F0   00 02 11 01 03 11 01 FF  DD 00 04 00 09 FF C4 01          ÿÝ     ÿÄ
00000200   3F 00 00 01 05 01 01 01  01 01 01 00 00 00 00 00   ?
00000210   00 00 03 00 01 02 04 05  06 07 08 09 0A 0B 01 00
00000220   01 05 01 01 01 01 01 01  00 00 00 00 00 00 00 01
00000230   00 02 03 04 05 06 07 08  09 0A 0B 10 00 01 04 01
00000240   03 02 04 02 05 07 06 08  05 03 0C 33 01 00 02 11             3
00000250   03 04 21 12 31 05 41 51  61 13 22 71 81 32 06 14     ! 1 AQa "q 2
00000260   91 A1 B1 42 23 24 15 52  C1 62 33 34 72 82 D1 43   '¡±B#$ RÁb34r‚ÑC
00000270   07 25 92 53 F0 E1 F1 63  73 35 16 A2 B2 83 26 44    %'Sðáñcs5 ¢²ƒ&D
00000280   93 54 64 45 C2 A3 74 36  17 D2 55 E2 65 F2 B3 84   "TdEÂ£t6 ÒUâeò³„
00000290   C3 D3 75 E3 F3 46 27 94  A4 85 B4 95 C4 D4 E4 F4   ÃÓuãóF'"¤…´•ÄÔäô
000002A0   A5 B5 C5 D5 E5 F5 56 66  76 86 96 A6 B6 C6 D6 E6   ¥µÅÕåõVfv†–¦¶ÆÖæ
000002B0   F6 37 47 57 67 77 87 97  A7 B7 C7 D7 E7 F7 11 00   ö7GWgw‡—§·Ç×ç÷
000002C0   02 02 01 02 04 04 03 04  05 06 07 07 06 05 35 01              5
000002D0   00 02 11 03 21 31 12 04  41 51 61 71 22 13 05 32      !1  AQaq"  2
000002E0   81 91 14 A1 B1 42 23 C1  52 D1 F0 33 24 62 E1 72    ' ¡±B#ÁRÑð3$bár
000002F0   82 92 43 53 15 63 73 34  F1 25 06 16 A2 B2 83 07   ‚'CS cs4ñ%  ¢²ƒ
00000300   26 35 C2 D2 44 93 54 A3  17 64 45 55 36 74 65 E2   &5ÂÒD"T£ dEU6teâ
Page 1 of 202 | Offset: 7 | = 120 | Block: 0 - 7 | Size: 8
```

```
[unregistered]
Photo_Rajan Gautam.jpg
D:\Rajan Gautam\Certificates\Certi
File size: 154 KB
157,833 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 10/08/2020 19:21:57
Last write time: 10/08/2020 19:21:57
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 49x16=784
Window #: 1
Window count: 1
Clipboard: available
TEMP folder: 79.3 GB free
\Users\gauta\AppData\Local\Temp
Data Interpreter
8 Bit (±): 120
16 Bit (±): 27,000
32 Bit (±): 6,711,672
```

Figure 5 WinHex

5. The image was edited with Adobe photoshop, that also we can verify from the HEXCode.

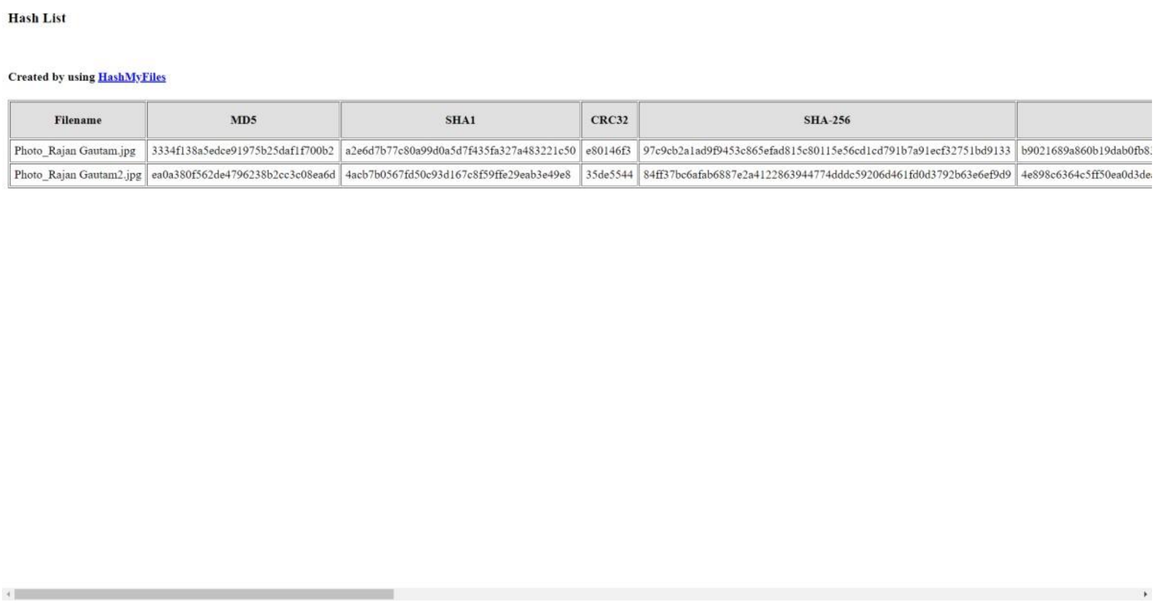

WinHex - [Photo_Rajan Gautam.jpg]
File Edit Search Navigation View Tools Specialist Options Window Help
20.6 SR-1
Case Data
File Edit
Photo_Rajan Gautam.jpg

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   FF D8 FF E1 0F 33 45 78  69 66 00 00 4D 4D 00 2A   ÿØÿá 3Exif  MM *
00000010   00 00 00 08 00 07 01 12  00 03 00 00 00 01 00 01
00000020   00 00 01 1A 00 05 00 00  00 01 00 00 00 62 01 1B              b
00000030   00 05 00 00 00 01 00 00  00 6A 01 28 00 03 00 00            j (
00000040   00 01 00 02 00 00 01 31  00 02 00 00 00 1F 00 00         1
00000050   00 72 01 32 00 02 00 00  00 14 00 00 00 91 87 69    r 2         '‡i
00000060   00 04 00 00 00 01 00 00  00 A8 00 00 00 D4 00 2D          ¨     Ô -
00000070   C6 C0 00 00 27 10 00 2D  C6 C0 00 00 27 10 41 64   ÆÀ  '  -ÆÀ  ' Ad
00000080   6F 62 65 20 50 68 6F 74  6F 73 68 6F 70 20 32 31   obe Photoshop 21
00000090   2E 32 20 28 57 69 6E 64  6F 77 73 29 00 32 30 32   .2 (Windows) 202
000000A0   30 3A 31 30 3A 30 38 20  31 39 3A 32 31 3A 35 33   0:10:08 19:21:53
000000B0   00 00 00 00 00 03 A0 01  00 03 00 00 00 01 00 01
000000C0   00 00 A0 02 00 04 00 00  00 01 00 00 02 58 A0 03              X
000000D0   00 04 00 00 00 01 00 00  02 58 00 00 00 00 00 00          X
000000E0   00 06 01 03 00 03 00 00  00 01 00 06 00 00 01 1A
000000F0   00 05 00 00 00 01 00 00  01 22 01 1B 00 05 00 00          "
00000100   00 01 00 00 01 2A 01 28  00 03 00 00 00 01 00 02        * (
00000110   00 00 02 01 00 04 00 00  00 01 00 00 01 32 02 02              2
00000120   00 04 00 00 00 01 00 00  0D F9 00 00 00 00 00 00          ù
00000130   00 48 00 00 00 01 00 00  00 48 00 00 00 01 FF D8    H       H    ÿØ
00000140   FF ED 00 0C 41 64 6F 62  65 5F 43 4D 00 01 FF EE   ÿí  Adobe_CM  ÿî
00000150   00 0E 41 64 6F 62 65 00  64 80 00 00 00 01 FF DB     Adobe d€    ÿÛ
00000160   00 84 00 0C 08 08 08 09  08 0C 09 09 0C 11 0B 0A    „
00000170   0B 11 15 0F 0C 0C 0F 15  18 13 13 15 13 13 18 11
00000180   0C 0C 0C 0C 0C 0C 11 0C  0C 0C 0C 0C 0C 0C 0C 0C
00000190   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
000001A0   0C 0C 0C 01 0D 0B 0B 0D  0E 0D 10 0E 0E 10 14 0E
000001B0   0E 0E 14 14 0E 0E 0E 0E  14 11 0C 0C 0C 0C 0C 11
000001C0   11 0C 0C 0C 0C 0C 0C 11  0C 0C 0C 0C 0C 0C 0C 0C
000001D0   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
000001E0   0C 0C 0C 0C FF C0 00 11  08 00 90 00 90 03 01 22       ÿÀ          "
000001F0   00 02 11 01 03 11 01 FF  DD 00 04 00 09 FF C4 01          ÿÝ     ÿÄ
00000200   3F 00 00 01 05 01 01 01  01 01 01 00 00 00 00 00   ?
00000210   00 00 03 00 01 02 04 05  06 07 08 09 0A 0B 01 00
00000220   01 05 01 01 01 01 01 01  00 00 00 00 00 00 00 01
00000230   00 02 03 04 05 06 07 08  09 0A 0B 10 00 01 04 01
00000240   03 02 04 02 05 07 06 08  05 03 0C 33 01 00 02 11             3
00000250   03 04 21 12 31 05 41 51  61 13 22 71 81 32 06 14     ! 1 AQa "q 2
00000260   91 A1 B1 42 23 24 15 52  C1 62 33 34 72 82 D1 43   '¡±B#$ RÁb34r‚ÑC
00000270   07 25 92 53 F0 E1 F1 63  73 35 16 A2 B2 83 26 44    %'Sðáñcs5 ¢²ƒ&D
00000280   93 54 64 45 C2 A3 74 36  17 D2 55 E2 65 F2 B3 84   "TdEÂ£t6 ÒUâeò³„
00000290   C3 D3 75 E3 F3 46 27 94  A4 85 B4 95 C4 D4 E4 F4   ÃÓuãóF'"¤…´•ÄÔäô
000002A0   A5 B5 C5 D5 E5 F5 56 66  76 86 96 A6 B6 C6 D6 E6   ¥µÅÕåõVfv†–¦¶ÆÖæ
000002B0   F6 37 47 57 67 77 87 97  A7 B7 C7 D7 E7 F7 11 00   ö7GWgw‡—§·Ç×ç÷
000002C0   02 02 01 02 04 04 03 04  05 06 07 07 06 05 35 01              5
000002D0   00 02 11 03 21 31 12 04  41 51 61 71 22 13 05 32      !1  AQaq"  2
000002E0   81 91 14 A1 B1 42 23 C1  52 D1 F0 33 24 62 E1 72    ' ¡±B#ÁRÑð3$bár
000002F0   82 92 43 53 15 63 73 34  F1 25 06 16 A2 B2 83 07   ‚'CS cs4ñ%  ¢²ƒ
00000300   26 35 C2 D2 44 93 54 A3  17 64 45 55 36 74 65 E2   &5ÂÒD"T£ dEU6teâ
Page 1 of 202 | Offset: 8C | = 112 | Block: 7D - 8C | Size: 10
```

```
[unregistered]
Photo_Rajan Gautam.jpg
D:\Rajan Gautam\Certificates\Certi
File size: 154 KB
157,833 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 10/08/2020 19:21:57
Last write time: 10/08/2020 19:21:57
Attributes: A
Icons: 0
Mode: Text
Offsets: hexadecimal
Bytes per page: 49x16=784
Window #: 1
Window count: 1
Clipboard: available
TEMP folder: 79.3 GB free
\Users\gauta\AppData\Local\Temp
Data Interpreter
8 Bit (±): 112
16 Bit (±): 8,304
32 Bit (±): 825,368,688
```

Figure 6 WinHex

6. When I updated the file using Paint and check the Hash value, I found the change inHash Valuealso.



Hash List

Created by using HashMyFiles

Filename	MD5	SHA1	CRC32	SHA-256	
Photo_Rajan Gautam.jpg	3334f138a5edce91975b25daf1f700b2	a2e6d7b77c80a99d0a5d7f435fa327a483221c50	e80146f3	97c9cb2a1ad9f9453c865efad815c80115e56cd1cd791b7a91ecf32751bd9133	b9021689a860b19dab0fb8
Photo_Rajan Gautam2.jpg	ea0a380f562de4796238b2cc3c08ea6d	4acb7b0567fd50c93d167c8f59ffe29eab3e49e8	35de5544	84ff37bc6afab6887e2a4122863944774dddc59206d461fd0d3792b63e6ef9d9	4e898c6364c5ff50ea0d3de

Figure 7 Hash Valuealso.

Conclusion:

1. By doing the HEX Code analysis, WinHEX is a powerful hex editor that allows users to view, modify, and analyze hexadecimal data in files, disks, and memory locations. It can be used for a variety of purposes, including digital forensics. HashMyFiles is a utility that allows users to calculate the hashes of files, which can be used to verify the integrity of those files. Gary Kessler's File Signature Table is a resource that can be used to identify the file formats of unknown files. All three of these tools can be useful in digital forensics