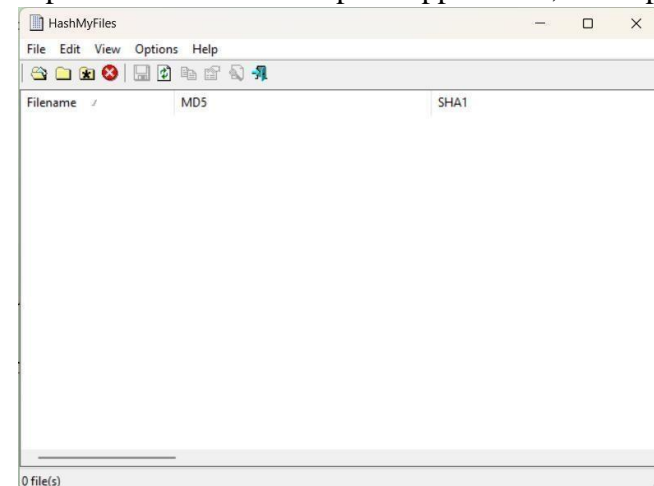


## PRACTICAL – 5

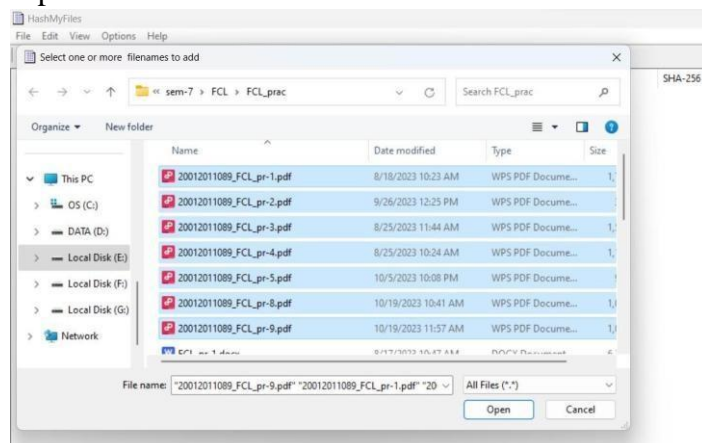
## Aim: Hash &amp; Hex Dump analysis

1 *HASHMYFILES*

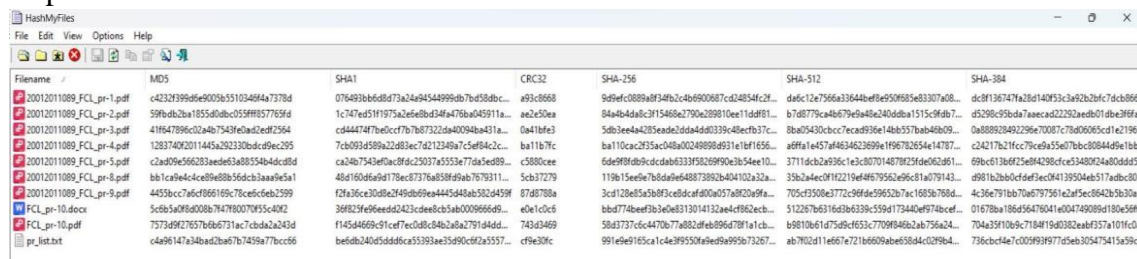
Step-1: Download &amp; Setup the application; then open it



Step-2 : Goto “add file” or “add folder”



Step-3 : See the result



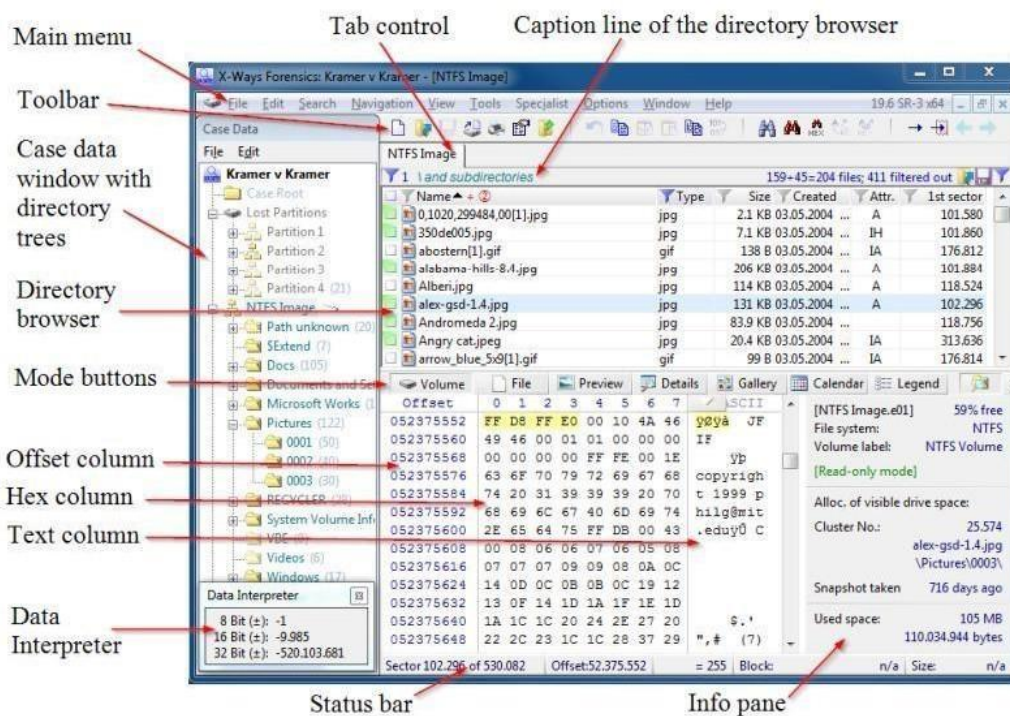
So after performing this we got hash's of our selected files.

## 2CEIT78PE8: Forensic & Cyber Law

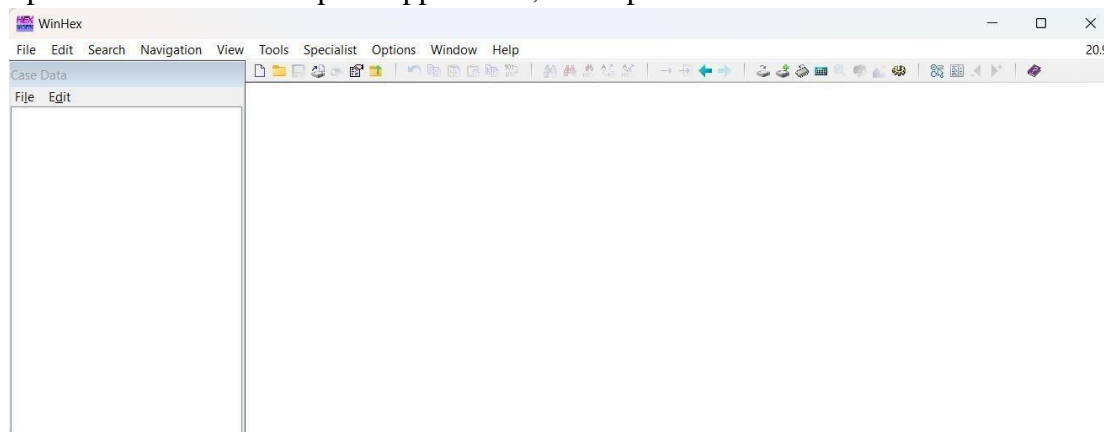
### 1 WINHEX

WinHex is a commercial disk editor and universal hexadecimal editor (hex editor) used for data recovery and digital forensics.

The following image will get you to understand proper interface



Step-1: Download & Setup the application; then open it



## 2CEIT78PE8: Forensic & Cyber Law

Step-2: Now add files or folder; or add a case

New Case

Case title/number: images\_hex\_details

Directory: D:\winhex

Description: Examiner(s), organization, address:

User: Me

Multi-user support options...

☒ Log general activity

☐ With screenshots

☒ Default to evidence object folders for output

☐ Case-specific directory for temporary files

☐ Case-specific default path for images

Code pages suitable for processing this case:

\*\*\* 1252 ANSI - Latin I \*\*\*

\*\*\* 1252 ANSI - Latin I \*\*\*

☐ Individual time zones per evidence object

☒ Improved recognition of physical media

☒ Add disk partitions to the case automatically

☐ Immediately verify image / Compute Hash

☒ Auto save interval in min. 5

No. of case file backups: 5

Attr.: H

☐ RVS: Protect against duplicates of crasher files

☒ Single-column search term list

☐ Protect case against opening

☒ Discard snapshot caches when closing

OK Cancel Help

Step-3 : Now analyze the output; and you can edit the hex also

WinHex - [wc1.webp]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data

File Edit

images\_hex\_details

Case Root

wc1.webp | wc2.jpg | wc3.jpg | wc4.jpg | wc5.jpg

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F

00000000 52 49 46 46 5C 2F 00 00 57 45 42 50 56 50 38 20 88FF\ WEBPVP8

00000010 50 2F 00 00 10 98 00 9D 01 2A 1F 01 68 01 3E 61 F/ - + h >a

00000020 2E 93 47 24 22 A1 A1 26 FB 79 30 80 0C 09 63 6E .\*GS";sdy0e cn

00000030 F1 86 64 BE 95 14 40 E0 BE AE 64 DE 90 03 F8 67 ttd4\* s&@db eg

00000040 79 87 D9 59 9D F6 6F AD 71 8B D0 9C 5D EE 31 E8 y+UY 0o-g(bw]i&e

00000050 33 FB D7 A8 2F F6 CE 81 DE 61 FC E3 7D 07 7F 83 30x"/oI bat&] f

00000060 F5 00 FE B3 FE EF D6 0F D4 73 FB 07 FE CF 60 6F 6 p\*b10 0su pI'o

00000070 39 AF FD FE CB 1F E1 3F F5 7E EE 7B 5A FF FF F6 9'ypP a?0-i(2yvo

00000080 00 DF A4 68 1F E5 BC 11 FC 6F E8 DF DB 7F 6F E5 0h &4 uoaB0 o0

00000090 CE FB A3 16 7E 95 FD 7F 98 7F CC 3F 12 FF 47 CD f0e ~.y "i? yGf

000000A0 6E FA FE 63 EA 17 8B 9D 73 36 CF D0 17 DE FB FA nupc& x s6ID p0u

000000B0 35 14 F7 5F F1 9E C0 5F CF 3F B9 7A 2B FE FF C1 S + n&A I?'+z+pyA

000000C0 DB EB BF E9 FD 81 7F 9F FF A1 F5 6E FF 3F C7 8F 0e;6y Yy;0ny?C

000000D0 D7 FE C1 BD 32 7D 1D BF 79 97 E3 18 C5 83 47 7B xpa+2) cy-a AfG(

000000E0 14 56 F9 E5 CA 13 AF A4 71 01 C5 B3 C5 F9 96 CF v0&E ~uq A^u-i

000000F0 C8 DA 76 48 0C 54 31 CF EB 07 F4 FD 8E A6 82 8E E0vH Tlie 0yZi,(Z

00000100 02 57 DE D4 88 09 45 07 35 C5 6A C6 01 B8 EE E0 W0" E 5&JE ,i&

00000110 9B 61 0F 57 A9 AA 16 59 77 2C 2E 54 FA C1 6C C0 >a W0" Yw, TuAlA

00000120 12 6D B7 31 EB A8 01 EA 14 93 C5 95 D2 99 F0 39 m'le" e "A~0=09

00000130 52 EC 9F EF 9B 52 46 A6 75 9B 90 6D 6F C3 3F CF RiYi>RF'u> moA?I

00000140 9A 16 8D BA E2 2D 92 BE CD F0 A2 FB 6D 53 88 34 s "a-'\*400ms'4

00000150 B6 B9 A3 61 11 CE AB A6 26 B3 91 3D 26 B5 5A C9 q'La I<|s'\*=suzE

00000160 C4 F9 FC 2C C4 E7 5A 0C 9C AF 83 DC 61 D9 37 F1 A0u,Ac2 m'fba07n

00000170 9A 47 73 1A 7D C6 88 92 C0 A3 F9 53 EC 81 3A C5 sGe }&e'&0u&i :&A

00000180 6F 84 DA 23 CC 14 BF B7 CF FB 19 89 88 CE BE BE o,0#i : 'i0 h'&ik

00000190 FC 47 C8 6D 11 CA 61 25 BA 03 68 C3 62 5D D6 22 uG2m 0a&° h&0]0"

000001A0 DA 86 3E FB 5E 17 3F AB 43 02 C3 06 AD 02 A0 4B 0t>0^ 2KC A - K

000001B0 36 87 51 E8 61 4A BE E9 76 EB BD 4E FF FE 77 40 6+Q0a0&v&v&Nypw0

000001C0 C6 A5 E6 E2 AE 36 AD 30 0B 7B B7 3D 56 D0 28 D7 &W&006-0 { :-vD(x

000001D0 AF 6E 44 D1 80 07 48 66 2C 24 95 2B 65 97 5A 2F nDn0 Hf, S+e=-2/

Page 1 of 26

Offset: 0

= 82 | Block

n/a | Size: n/a

wc1.webp [unregistered]

C:\Users\Dhhey Patel\OneDrive\Pictures

File size: 11.8 KB  
12,132 bytes

Default Edit Mode: original

Undo level: 0

Undo reverses: n/a

Creation time: 03/10/2023 21:27:15

Last write time: 03/10/2023 21:27:18

Attributes: A

Icons: 0

Mode: hexadecimal

Offsets: hexadecimal

Bytes per page: 30x16=480

Window #: 1

Window count: 5

Case association: No

Clipboard: available

TEMP folder: 58.4 GB free

C:\Users\DHHEY~1\AppData\Local\Temp