Laboratory Notes

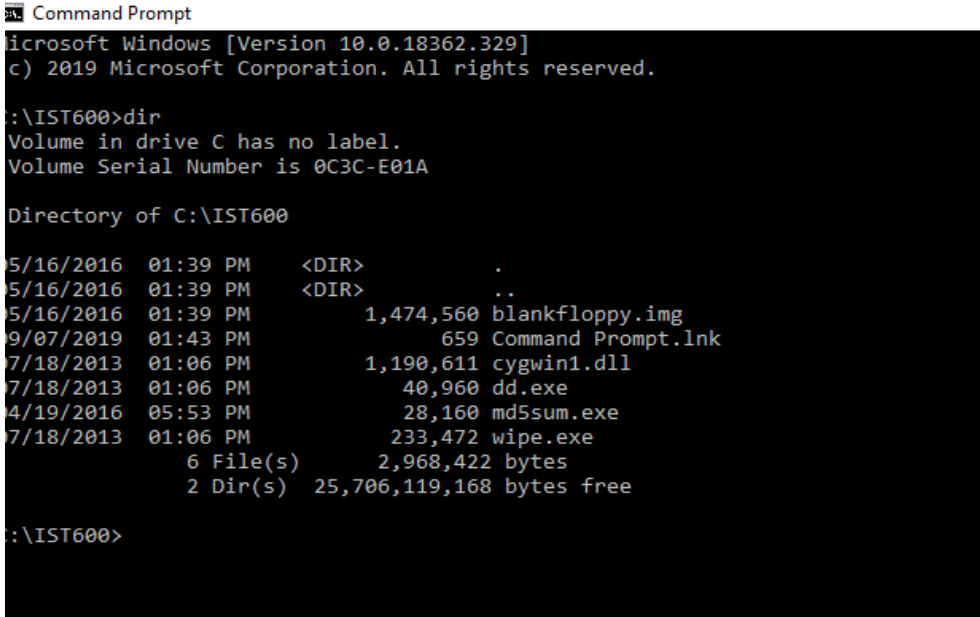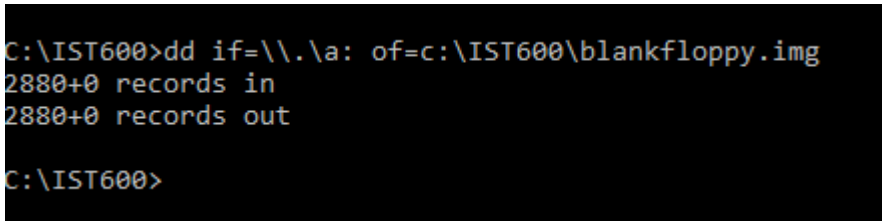Laboratory Number: <u>IST602 Lab1</u>   Examiner Name: <u>Akshay Chaurasia</u>

Date & Time   Activity

<table>
<tr>
<td>1:47
PM
9/7/19</td>
<td>

➢ Open the forensic virtual machine and navigate to following path:
<u>C:\IST600</u>

➢ Opened the command prompt from this path
In Command prompt, type directory listing command: <u>dir a</u>

Command Prompt

```
Microsoft Windows [Version 10.0.18362.329]
(c) 2019 Microsoft Corporation. All rights reserved.

:\IST600>dir
Volume in drive C has no label.
Volume Serial Number is 0C3C-E01A

Directory of C:\IST600

05/16/2016  01:39 PM    <DIR>          .
05/16/2016  01:39 PM    <DIR>          ..
05/16/2016  01:39 PM         1,474,560 blankfloppy.img
09/07/2019  01:43 PM               659 Command Prompt.lnk
07/18/2013  01:06 PM         1,190,611 cygwin1.dll
07/18/2013  01:06 PM            40,960 dd.exe
04/19/2016  05:53 PM            28,160 md5sum.exe
07/18/2013  01:06 PM           233,472 wipe.exe
              6 File(s)      2,968,422 bytes
              2 Dir(s)  25,706,119,168 bytes free

:\IST600>
```

➢ Ran dd to create an image of the evidence floppy drive
In command prompt, entered: dd if=\\.\a:
of=c:\IST600\blankfloppy.img

```
C:\IST600>dd if=\\.\a: of=c:\IST600\blankfloppy.img
2880+0 records in
2880+0 records out

C:\IST600>
```

This comand read 2880 files

</td>
</tr>
<tr>
<td>2:01</td>
<td></td>
</tr>
</table>

2:03

> ➢ We will do the directory listing again
>   Type <u>dir</u>

```
C:\IST600>dir
 Volume in drive C has no label.
 Volume Serial Number is 0C3C-E01A

 Directory of C:\IST600

05/16/2016  01:39 PM    <DIR>          .
05/16/2016  01:39 PM    <DIR>          ..
09/07/2019  01:54 PM         1,474,560 blankfloppy.img
09/07/2019  01:43 PM               659 Command Prompt.lnk
07/18/2013  01:06 PM         1,190,611 cygwin1.dll
07/18/2013  01:06 PM            40,960 dd.exe
04/19/2016  05:53 PM            28,160 md5sum.exe
07/18/2013  01:06 PM           233,472 wipe.exe
               6 File(s)      2,968,422 bytes
               2 Dir(s)  25,709,211,648 bytes free

C:\IST600>
```

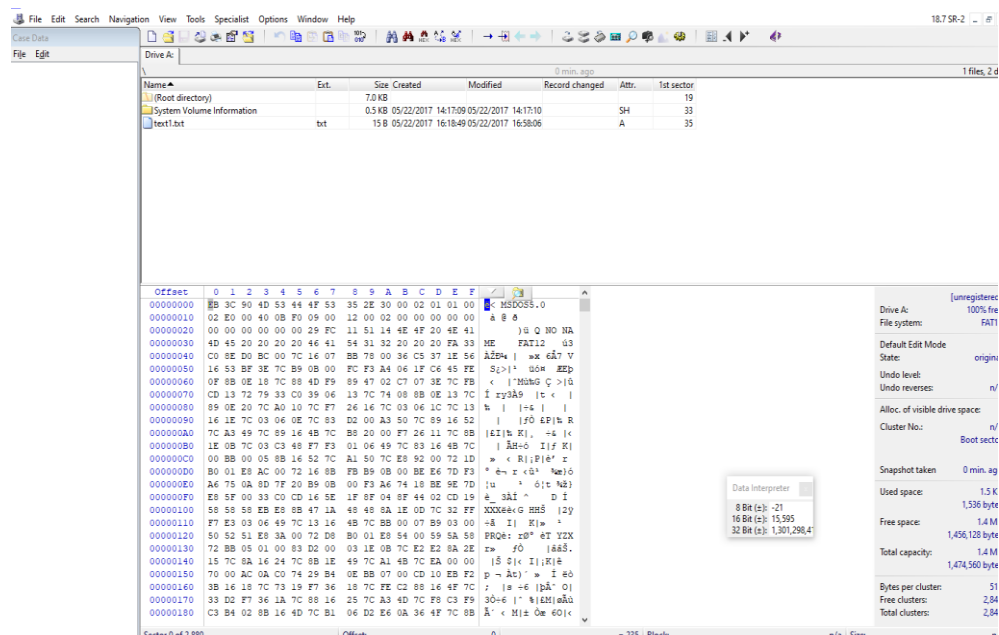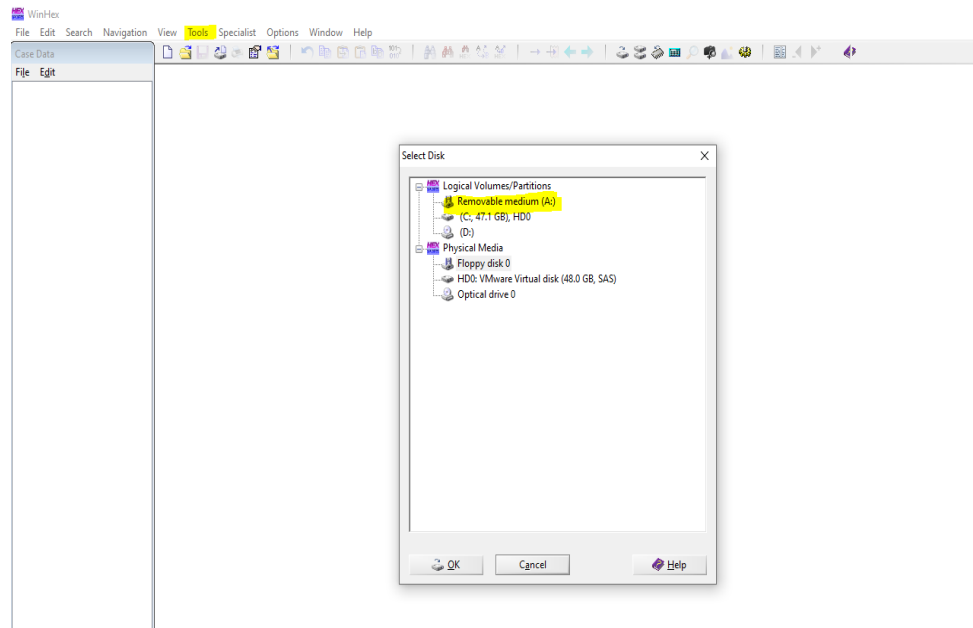**Create a hash value for the floppy disk and the image**

> ➢ Create hash value to check the autheticity

```
C:\IST600>md5sum \\.\a:
\a985cf5fef169a4a0f942ebc99ceb3aa *\\\\.\\a:

C:\IST600>md5sum blankfloppy.img
a985cf5fef169a4a0f942ebc99ceb3aa *blankfloppy.img

C:\IST600>
```
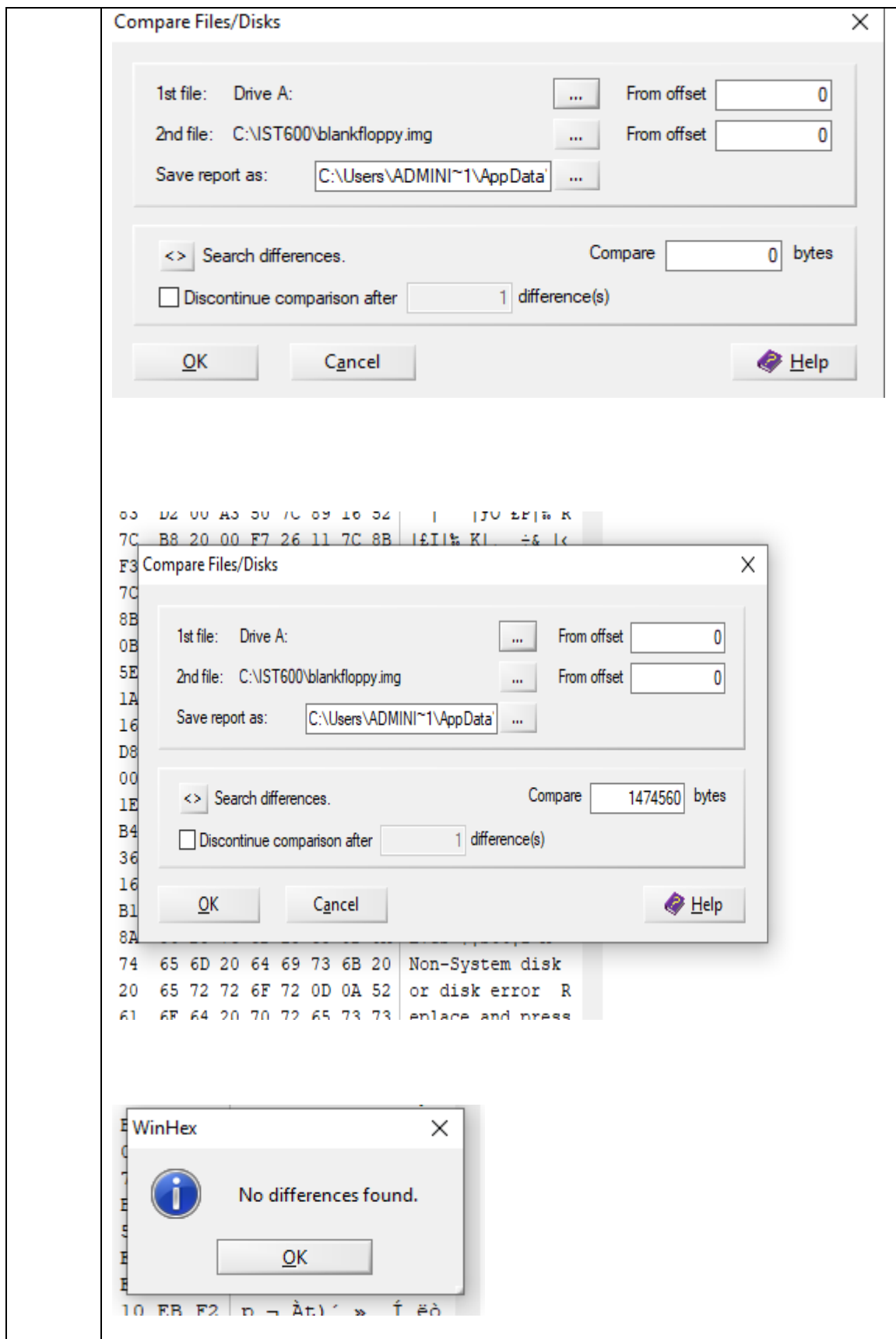
➢ Open the logical disk

Examiner Initials: <u>Akshay Chaurasia</u>

Drive A: | blankfloppy.img |

Name ▲	Ext.	Size	Created	Modified	Record char
(Root directory)		7.0 KB			
System Volume Information		0.5 KB	05/22/2017 14:17:09	05/22/2017 14:17:10	
text1.txt	txt	15 B	05/22/2017 16:18:49	05/22/2017 16:58:06	

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  EB 3C 90 4D 53 44 4F 53  35 2E 30 00 02 01 01 00   ë< MSDOS5.0
00000010  02 E0 00 40 0B F0 09 00  12 00 02 00 00 00 00 00    à @ ð
00000020  00 00 00 00 00 00 29 FC  11 51 14 4E 4F 20 4E 41        )ü Q NO NA
00000030  4D 45 20 20 20 20 46 41  54 31 32 20 20 20 FA 33   ME    FAT12   ú3
00000040  C0 8E D0 BC 00 7C 16 07  BB 78 00 36 C5 37 1E 56   ÀŽÐ¼ |  »x 6Å7 V
00000050  16 53 BF 3E 7C B9 0B 00  FC F3 A4 06 1F C6 45 FE    S¿>|¹  üó¤  ÆEþ
00000060  0F 8B 0E 18 7C 88 4D F9  89 47 02 C7 07 3E 7C FB    ‹  |ˆMù‰G Ç >|û
00000070  CD 13 72 79 33 C0 39 06  13 7C 74 08 8B 0E 13 7C   Í ry3À9  |t < ‹  |
00000080  89 0E 20 7C A0 10 7C F7  26 16 7C 03 06 1C 7C 13   ‰ | | ÷& |  | 
00000090  16 1E 7C 03 06 0E 7C 83  D2 00 A3 50 7C 89 16 52     |  | ƒÒ £P|‰ R
000000A0  7C A3 49 7C 89 16 4B 7C  B8 20 00 F7 26 11 7C 8B   |£I|‰ K|¸  ÷& |‹
000000B0  1E 0B 7C 03 C3 48 F7 F3  01 06 49 7C 83 16 4B 7C    |  ÃH÷ó  I|ƒ K|
000000C0  00 BB 00 05 8B 16 52 7C  A1 50 7C E8 92 00 72 1D    »  ‹ R|¡P|è' r
000000D0  B0 01 E8 AC 00 72 16 8B  FB B9 0B 00 BE E6 7D F3   ° è¬ r ‹û¹  ¾æ}ó
000000E0  A6 75 0A 8D 7F 20 B9 0B  00 F3 A6 74 18 BE 9E 7D   ¦u   ¹  ó¦t ¾ž}
000000F0  E8 5F 00 33 C0 CD 16 5E  1F 8F 04 8F 44 02 CD 19   è_ 3ÀÍ ^    D Í
00000100  58 58 58 EB E8 8B 47 1A  48 48 8A 1E 0D 7C 32 FF   XXXëè‹G HHŠ  |2ÿ
00000110  F7 E3 03 06 49 7C 13 16  4B 7C BB 00 07 B9 03 00   ÷ã  I|  K|»  ¹
00000120  50 52 51 E8 3A 00 72 D8  B0 01 E8 54 00 59 5A 58   PRQè: rØ° èT YZX
00000130  72 BB 05 01 00 83 D2 00  03 1E 0B 7C E2 E2 8A 2E   r»   ƒÒ   |ââŠ.
00000140  15 7C 8A 16 24 7C 8B 1E  49 7C A1 4B 7C EA 00 00    |Š $|‹ I|¡K|ê
00000150  70 00 AC 0A C0 74 29 B4  0E BB 07 00 CD 10 EB F2   p ¬ Àt)´ »  Í ëò
00000160  3B 16 18 7C 73 19 F7 36  18 7C FE C2 88 16 4F 7C   ; |s ÷6 |þÂˆ O|
00000170  33 D2 F7 36 1A 7C 88 16  25 7C A3 4D 7C F8 C3 F9   3Ò÷6 |ˆ %|£M|øÃù
00000180  C3 B4 02 8B 16 4D 7C B1  06 D2 E6 0A 36 4F 7C 8B   Ã´ ‹ M|± Òæ 6O|‹
00000190  CA 86 E9 8A 16 24 7C 8A  36 25 7C CD 13 C3 0D 0A   Ê†éŠ $|Š6%|Í Ã
000001A0  4E 6F 6E 2D 53 79 73 74  65 6D 20 64 69 73 6B 20   Non-System disk
000001B0  6F 72 20 64 69 73 6B 20  65 72 72 6F 72 0D 0A 52   or disk error  R
000001C0  65 70 6C 61 63 65 20 61  6E 64 20 70 72 65 73 73   eplace and press
000001D0  20 61 6E 79 20 6B 65 79  20 77 68 65 6E 20 72 65    any key when re
000001E0  61 64 79 0D 0A 00 49 4F  20 20 20 20 20 20 53 59   ady   IO      SY
000001F0  53 4D 53 44 4F 53 20 20  20 53 59 53 00 00 55 AA   SMSDOS   SYS  Uª
00000200  F0 FF FF FF FF FF FF 0F  00 00 00 00 00 00 00 00   ðÿÿÿÿÿÿ
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```
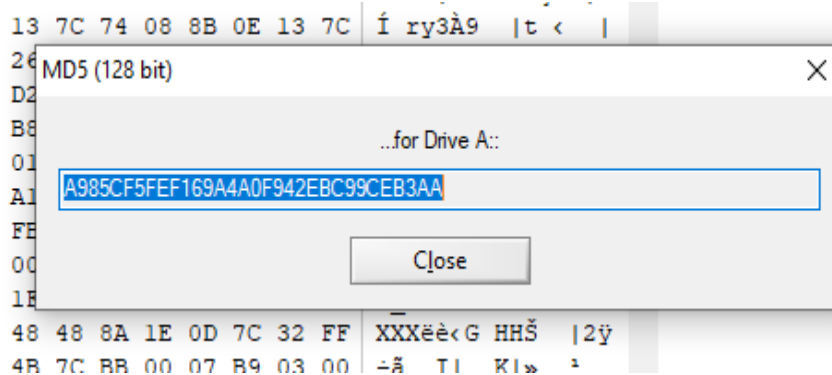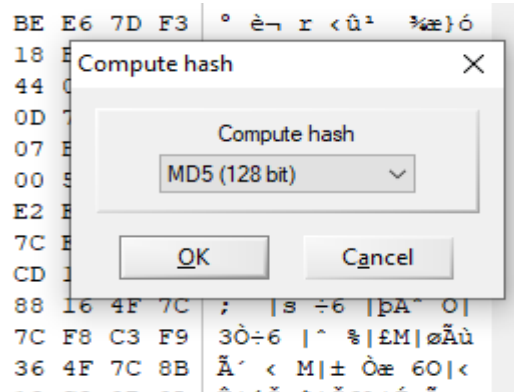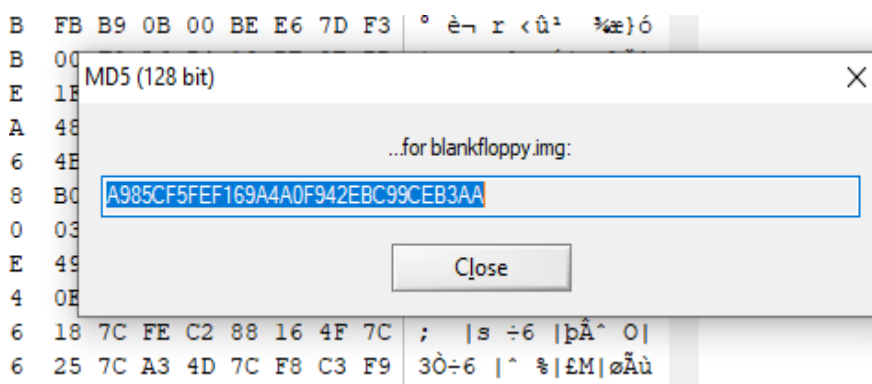
Drive A: | blankfloppy.img |

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  EB 3C 90 4D 53 44 4F 53  35 2E 30 00 02 01 01 00   ë< MSDOS5.0
00000010  02 E0 00 40 0B F0 09 00  12 00 02 00 00 00 00 00    à @ ð
00000020  00 00 00 00 00 00 29 FC  11 51 14 4E 4F 20 4E 41        )ü Q NO NA
00000030  4D 45 20 20 20 20 46 41  54 31 32 20 20 20 FA 33   ME    FAT12   ú3
00000040  C0 8E D0 BC 00 7C 16 07  BB 78 00 36 C5 37 1E 56   ÀŽÐ¼ |  »x 6Å7 V
00000050  16 53 BF 3E 7C B9 0B 00  FC F3 A4 06 1F C6 45 FE    S¿>|¹  üó¤  ÆEþ
00000060  0F 8B 0E 18 7C 88 4D F9  89 47 02 C7 07 3E 7C FB    ‹  |ˆMù‰G Ç >|û
00000070  CD 13 72 79 33 C0 39 06  13 7C 74 08 8B 0E 13 7C   Í ry3À9  |t < ‹  |
00000080  89 0E 20 7C A0 10 7C F7  26 16 7C 03 06 1C 7C 13   ‰ | | ÷& |  | 
00000090  16 1E 7C 03 06 0E 7C 83  D2 00 A3 50 7C 89 16 52     |  | ƒÒ £P|‰ R
000000A0  7C A3 49 7C 89 16 4B 7C  B8 20 00 F7 26 11 7C 8B   |£I|‰ K|¸  ÷& |‹
000000B0  1E 0B 7C 03 C3 48 F7 F3  01 06 49 7C 83 16 4B 7C    |  ÃH÷ó  I|ƒ K|
000000C0  00 BB 00 05 8B 16 52 7C  A1 50 7C E8 92 00 72 1D    »  ‹ R|¡P|è' r
000000D0  B0 01 E8 AC 00 72 16 8B  FB B9 0B 00 BE E6 7D F3   ° è¬ r ‹û¹  ¾æ}ó
000000E0  A6 75 0A 8D 7F 20 B9 0B  00 F3 A6 74 18 BE 9E 7D   ¦u   ¹  ó¦t ¾ž}
000000F0  E8 5F 00 33 C0 CD 16 5E  1F 8F 04 8F 44 02 CD 19   è_ 3ÀÍ ^    D Í
00000100  58 58 58 EB E8 8B 47 1A  48 48 8A 1E 0D 7C 32 FF   XXXëè‹G HHŠ  |2ÿ
00000110  F7 E3 03 06 49 7C 13 16  4B 7C BB 00 07 B9 03 00   ÷ã  I|  K|»  ¹
00000120  50 52 51 E8 3A 00 72 D8  B0 01 E8 54 00 59 5A 58   PRQè: rØ° èT YZX
00000130  72 BB 05 01 00 83 D2 00  03 1E 0B 7C E2 E2 8A 2E   r»   ƒÒ   |ââŠ.
00000140  15 7C 8A 16 24 7C 8B 1E  49 7C A1 4B 7C EA 00 00    |Š $|‹ I|¡K|ê
00000150  70 00 AC 0A C0 74 29 B4  0E BB 07 00 CD 10 EB F2   p ¬ Àt)´ »  Í ëò
00000160  3B 16 18 7C 73 19 F7 36  18 7C FE C2 88 16 4F 7C   ; |s ÷6 |þÂˆ O|
00000170  33 D2 F7 36 1A 7C 88 16  25 7C A3 4D 7C F8 C3 F9   3Ò÷6 |ˆ %|£M|øÃù
00000180  C3 B4 02 8B 16 4D 7C B1  06 D2 E6 0A 36 4F 7C 8B   Ã´ ‹ M|± Òæ 6O|‹
00000190  CA 86 E9 8A 16 24 7C 8A  36 25 7C CD 13 C3 0D 0A   Ê†éŠ $|Š6%|Í Ã
000001A0  4E 6F 6E 2D 53 79 73 74  65 6D 20 64 69 73 6B 20   Non-System disk
000001B0  6F 72 20 64 69 73 6B 20  65 72 72 6F 72 0D 0A 52   or disk error  R
000001C0  65 70 6C 61 63 65 20 61  6E 64 20 70 72 65 73 73   eplace and press
000001D0  20 61 6E 79 20 6B 65 79  20 77 68 65 6E 20 72 65    any key when re
000001E0  61 64 79 0D 0A 00 49 4F  20 20 20 20 20 20 53 59   ady   IO      SY
000001F0  53 4D 53 44 4F 53 20 20  20 53 59 53 00 00 55 AA   SMSDOS   SYS  Uª
00000200  F0 FF FF FF FF FF FF 0F  00 00 00 00 00 00 00 00   ðÿÿÿÿÿÿ
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000250  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000260  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000270  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000290  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Compare Files/Disks

1st file: Drive A: [...]   From offset   [0]

2nd file: C:\IST600\blankfloppy.img   [...]   From offset   [0]

Save report as: [C:\Users\ADMINI~1\AppData]   [...]

<> Search differences.   Compare [0] bytes

☐ Discontinue comparison after [1] difference(s)

[OK]   [Cancel]   [Help]

---

83 D2 00 A3 50 7C 89 16 52 | |JO ±P|‰ R
7C B8 20 00 F7 26 11 7C 8B |£I|‰ K| ÷& |<
F3
7C
8B

Compare Files/Disks

1st file: Drive A: [...]   From offset   [0]

2nd file: C:\IST600\blankfloppy.img   [...]   From offset   [0]

Save report as: [C:\Users\ADMINI~1\AppData]   [...]

<> Search differences.   Compare [1474560] bytes

☐ Discontinue comparison after [1] difference(s)

[OK]   [Cancel]   [Help]

74 65 6D 20 64 69 73 6B 20 Non-System disk
20 65 72 72 6F 72 0D 0A 52 or disk error R
61 6F 64 20 70 72 65 73 73 eplace and press

WinHex

ℹ No differences found.

[OK]

10 EB F2 | p ¬ Àt)´ » Í ëò

    Examiner Initials: <u>Akshay Chaurasia</u>

```
BE E6 7D F3   °  è¬  r <û¹   ¾æ}ó
18            Compute hash                    ×
44
0D                   Compute hash
07                   MD5 (128 bit)        ∨
00
E2
7C                OK              Cancel
CD
88 16 4F 7C   ;    |s ÷6  |þA^ O|
7C F8 C3 F9   3Ò÷6  |^ %|£M|øÃù
36 4F 7C 8B   Ã´ < M|± Òæ 6O|<
```

```
13 7C 74 08 8B 0E 13 7C   Í ry3À9   |t <    |
26  MD5 (128 bit)                              ×
D2
B8                ...for Drive A::
01
A1      A985CF5FEF169A4A0F942EBC99CEB3AA
FE
00                     Close
1E
48 48 8A 1E 0D 7C 32 FF   XXXëè<G HHŠ    |2ÿ
4B 7C BB 00 07 B9 03 00   ÷ã  T|   K|»    ¹
```

A985CF5FEF169A4A0F942EBC99CEB3AA

```
B   FB B9 0B 00 BE E6 7D F3 | °  è¬  r <û¹   ¾æ}ó
B   00  MD5 (128 bit)                              ×
E   1E
A   48                ...for blankfloppy.img:
6   4E
8   B0      A985CF5FEF169A4A0F942EBC99CEB3AA
0   03
E   49                     Close
4   0E
6   18 7C FE C2 88 16 4F 7C | ;    |s ÷6  |þÅ^ O|
6   25 7C A3 4D 7C F8 C3 F9   3Ò÷6  |^ %|£M|øÃù
```

A985CF5FEF169A4A0F942EBC99CEB3AA

We have same hash value.

Creating a "sterile" forensics disk

> Now, we will wipe the disk

Wipe the drive 2:20

```
C:\IST600>wipe \\.\a:
```

```
C:\IST600>md5sum \\.\a:
\a985cf5fef169a4a0f942ebc99ceb3aa *\\\\.\\a:

C:\IST600>md5sum blankfloppy.img
a985cf5fef169a4a0f942ebc99ceb3aa *blankfloppy.im

C:\IST600>wipe \\.\a:
Forensic Acquisition Tools, 1, 0, 0, 1032
wipe, 1, 0, 0, 1032
Copyright (C) 2002 George M. Garner Jr.

Command Line: wipe  \\.\a:
Module: C:\IST600\wipe.exe
File and digital media sterilization program.
Microsoft Windows Version 6.2 (Build 9200.Profes

07/09/2019  18:20:39 (UTC)
07/09/2019  14:20:39 (local time)

Current User: WINCLIENT\Administrator


Do you want to wipe \\.\a:: [Y]es or [N]o?Y
```

Examiner Initials: <u>Akshay Chaurasia</u>

```
C:\IST600>md5sum \\.\a:
\a985cf5fef169a4a0f942ebc99ceb3aa *\\\\.\\a:

C:\IST600>md5sum blankfloppy.img
a985cf5fef169a4a0f942ebc99ceb3aa *blankfloppy.img

C:\IST600>wipe \\.\a:
Forensic Acquisition Tools, 1, 0, 0, 1032
wipe, 1, 0, 0, 1032
Copyright (C) 2002 George M. Garner Jr.

Command Line: wipe  \\.\a:
Module: C:\IST600\wipe.exe
File and digital media sterilization program.
Microsoft Windows Version 6.2 (Build 9200.Professional)

07/09/2019  18:20:39 (UTC)
07/09/2019  14:20:39 (local time)

Current User: WINCLIENT\Administrator


Do you want to wipe \\.\a:: [Y]es or [N]o?Y

WARNING!!! ALL DATA WILL BE DESTROYED.
Are you sure that you want to wipe \\.\a:: [Y]es or [N]o?Y
```

```
WARNING!!! ALL DATA WILL BE DESTROYED.
Are you sure that you want to wipe \\.\a:: [Y]es or [N]o?Y
Writing FF bits to allocated range 0x00000000,9223372036854775807 of \\.\a::
Completed in 329 milliseconds, 1474560 bytes written.
Writing random bits to allocated range 0x00000000,9223372036854775807 of \\.\a::
Completed in 296 milliseconds, 1474560 bytes written.
Writing zero bits to allocated range 0x00000000,9223372036854775807 of \\.\a::
Completed in 329 milliseconds, 1474560 bytes written.

07/09/2019  18:21:26 (UTC)
07/09/2019  14:21:26 (local time)


C:\IST600>
```

Examiner Initials: <u>Akshay Chaurasia</u>

➢ To make sure everything is wiped, go to Winhex -> Tools -> Calculate Hash

              Examiner Initials: <u>Akshay Chaurasia</u>
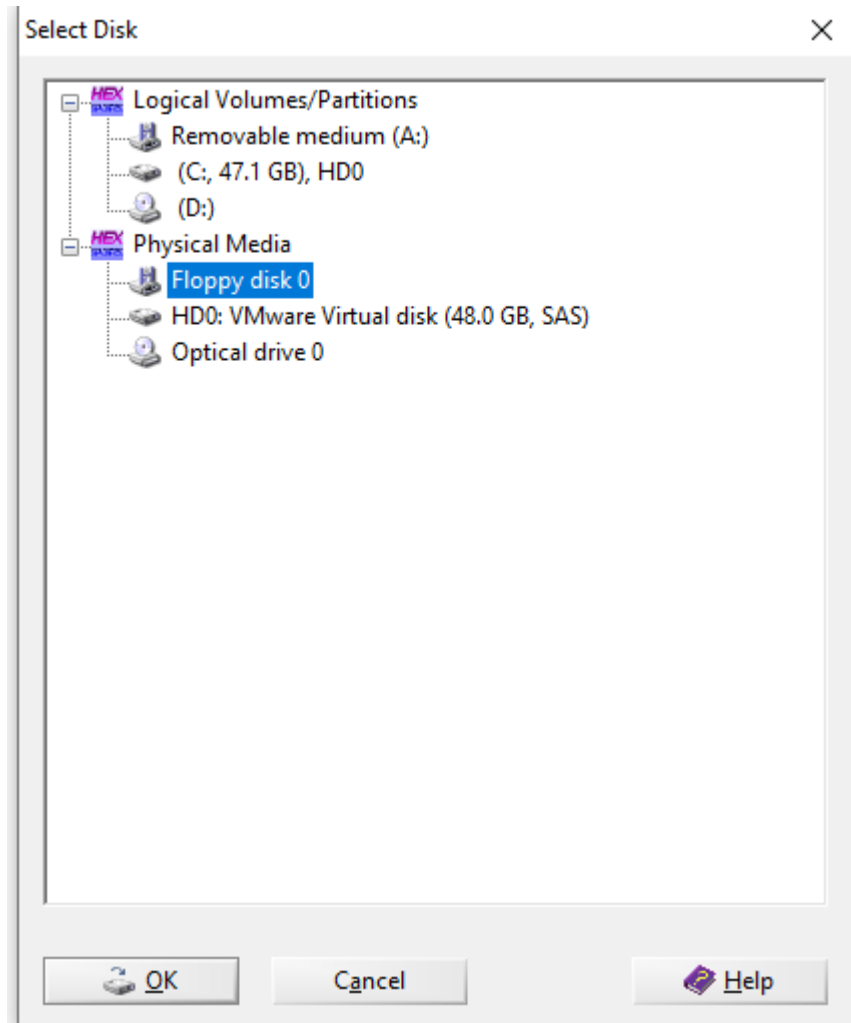
Floppy disk 0

Partitioning style: ?

Name	Ext.	Size	Created	Modified	Record ch
Unpartitioned space		1.4 MB			

```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000020   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000030   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000040   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000050   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000070   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000190   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000200   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Examiner Initials: <u>Akshay Chaurasia</u>
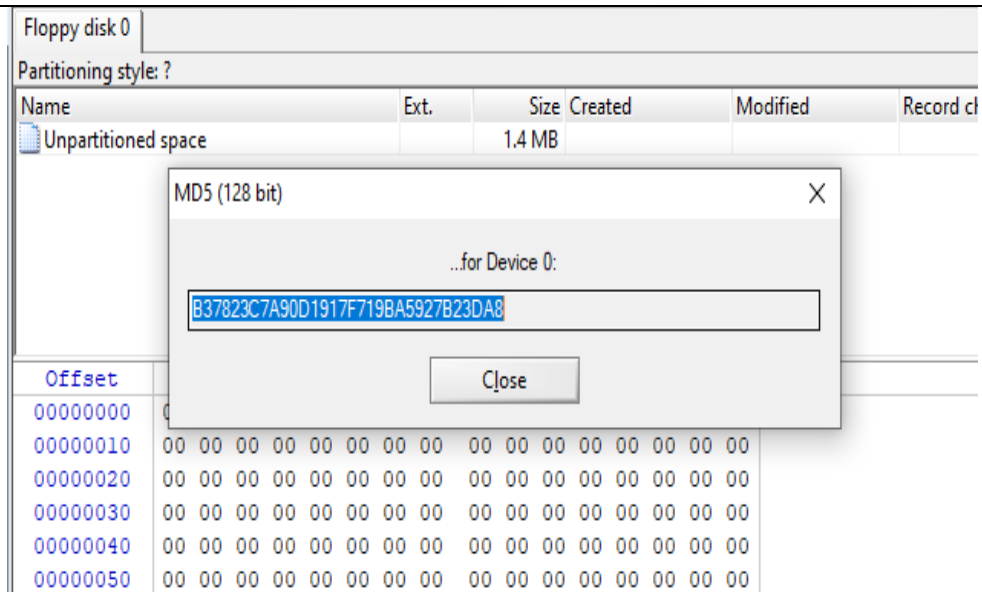
B37823C7A90D1917F719BA5927B23DA8

Different hex value

> ➢ Now, goto cmd ant type: <u>dir a:</u>

We will get the following output: Incorrect Function.

Examiner Initials: <u>Akshay Chaurasia</u>

9/7/20
19
2:32
PM
	Restore the image
	
	➤ Format the floppy: format a:/ u
	
	``
	C:\IST600>
	C:\IST600>
	C:\IST600>format a:/u
	Insert new disk for drive A:
	and press ENTER when ready...
	``
	
	``
	C:\IST600>
	C:\IST600>
	C:\IST600>format a:/u
	Insert new disk for drive A:
	and press ENTER when ready...
	The type of the file system is RAW.
	The new file system is FAT.
	Verifying 1.44M
	87 percent completed.
	``
	
	``
	C:\IST600>
	C:\IST600>
	C:\IST600>format a:/u
	Insert new disk for drive A:
	and press ENTER when ready...
	The type of the file system is RAW.
	The new file system is FAT.
	Verifying 1.44M
	Initializing the File Allocation Table (FAT)...
	Volume label (11 characters, ENTER for none)?
	Format complete.
	        1.4 MB total disk space.
	        1.4 MB are available.
	
	           512 bytes in each allocation unit.
	         2,847 allocation units available on disk.
	
	            12 bits in each FAT entry.
	
	Volume Serial Number is F648-FB0D
	
	Format another (Y/N)? N
	``

➢ Wipe the floppy
  wipe \\.\a:

```
C:\IST600>
C:\IST600>wipe \\.\a:
Forensic Acquisition Tools, 1, 0, 0, 1032
wipe, 1, 0, 0, 1032
Copyright (C) 2002 George M. Garner Jr.

Command Line: wipe  \\.\a:
Module: C:\IST600\wipe.exe
File and digital media sterilization program.
Microsoft Windows Version 6.2 (Build 9200.Professional)

07/09/2019  18:39:34 (UTC)
07/09/2019  14:39:34 (local time)

Current User: WINCLIENT\Administrator


Do you want to wipe \\.\a:: [Y]es or [N]o?Y

WARNING!!! ALL DATA WILL BE DESTROYED.
Are you sure that you want to wipe \\.\a:: [Y]es or [N]o?Y
Writing FF bits to allocated range 0x00000000,9223372036854775807 of \\.\a::
Completed in 265 milliseconds, 1474560 bytes written.
Writing random bits to allocated range 0x00000000,9223372036854775807 of \\.\a::
Completed in 313 milliseconds, 1474560 bytes written.
Writing zero bits to allocated range 0x00000000,9223372036854775807 of \\.\a::
Completed in 328 milliseconds, 1474560 bytes written.

07/09/2019  18:39:50 (UTC)
07/09/2019  14:39:50 (local time)


C:\IST600>
```

➢ Use DD to restore : dd if=c:\IST600\blankfloppy.img of=\\.\a:

```
C:\IST600>dd if=c:\IST600\blankfloppy.img of=\\.\a:
2880+0 records in
2880+0 records out

C:\IST600>
```

Examiner Initials: <u>Akshay Chaurasia</u>

➤ To check if accurate -> cmd -> md5sum blankfloppy.img
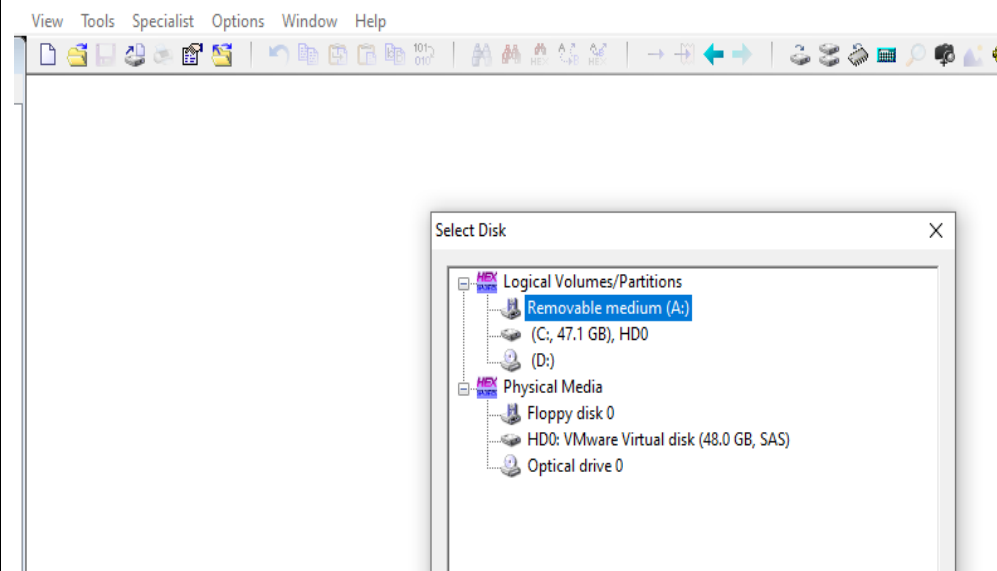 md5sum \\.\a:

Hash is same

```
C:\IST600>
C:\IST600>
C:\IST600>md5sum blankfloppy.img
a985cf5fef169a4a0f942ebc99ceb3aa *blankfloppy.img

C:\IST600>md5sum \\.\a:
\a985cf5fef169a4a0f942ebc99ceb3aa *\\\\.\\a:

C:\IST600>
```
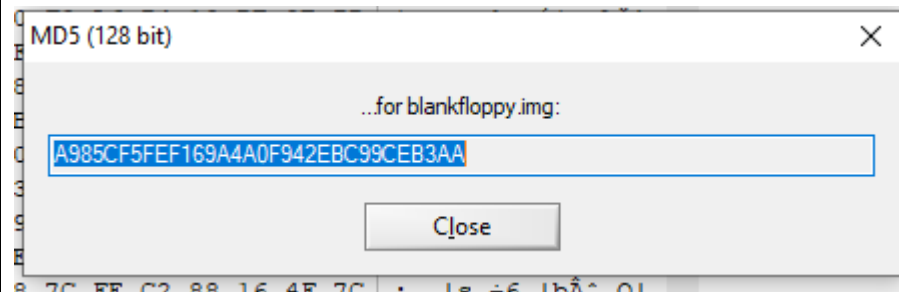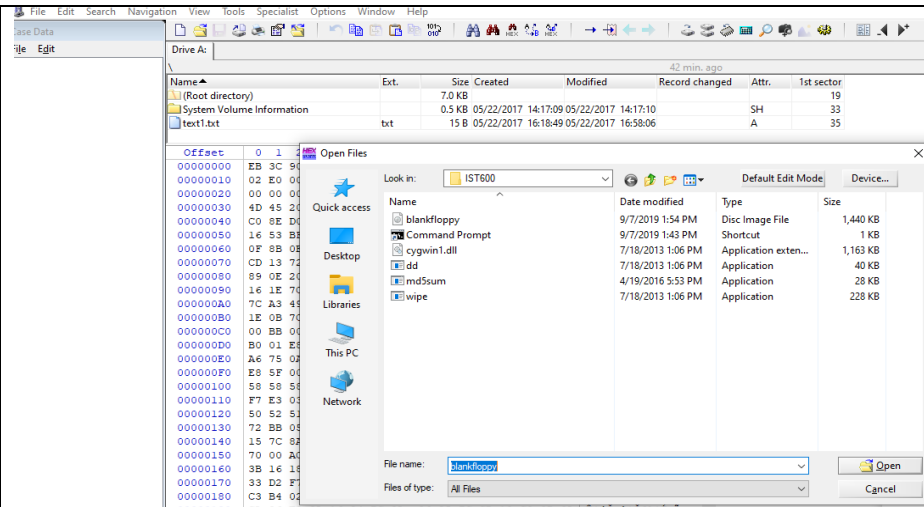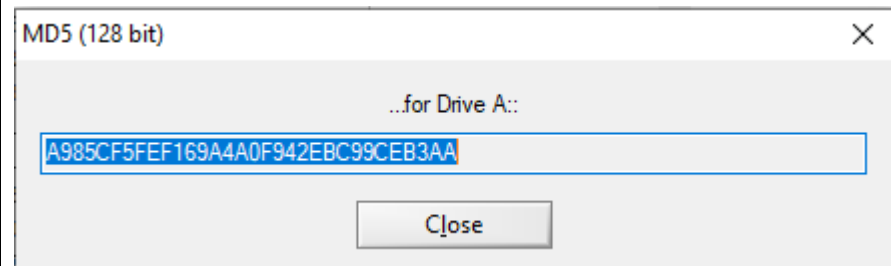
Validating the use of MD5 to detect changes

View Tools Specialist Options Window Help

Select Disk   ✕

  Logical Volumes/Partitions
    Removable medium (A:)
    (C:, 47.1 GB), HD0
    (D:)
  Physical Media
    Floppy disk 0
    HD0: VMware Virtual disk (48.0 GB, SAS)
    Optical drive 0

2:48
PM

A985CF5FEF169A4A0F942EBC99CEB3AA

A985CF5FEF169A4A0F942EBC99CEB3AA

They are identical.

Examiner Initials: Akshay Chaurasia

> ➢ Create a file within

```
C:\IST600>
C:\IST600>copy con a:\text1.txt
This is text 1^Z
Overwrite a:\text1.txt? (Yes/No/All): Y
        1 file(s) copied.

C:\IST600>
```

> ➢ Open the logical disk in WinHex

Examiner Initials: <u>Akshay Chaurasia</u>

Drive A: | text1.txt

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	54	68	69	73	20	69	73	20	74	65	78	74	20	31	00		This is text 1

> Open physical disk

Floppy disk 0

Partitioning style: unpartitioned

Name	Ext.	Size	Created	Modified	Record ch
Volume	FAT12	1.4 MB			

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	01	01	00	ë< MSDOS5.0
00000010	02	E0	00	40	0B	F0	09	00	12	00	02	00	00	00	00	00	à @ ð
00000020	00	00	00	00	00	00	29	FC	11	51	14	4E	4F	20	4E	41	)ü Q NO NA
00000030	4D	45	20	20	20	20	46	41	54	31	32	20	20	20	FA	33	ME FAT12 ú3
00000040	C0	8E	D0	BC	00	7C	16	07	BB	78	00	36	C5	37	1E	56	ÀŽÐ¼ | »x 6Å7 V
00000050	16	53	BF	3E	7C	B9	0B	00	FC	F3	A4	06	1F	C6	45	FE	S¿>|¹ üó¤ ÆEþ
00000060	0F	8B	0E	18	7C	88	4D	F9	89	47	02	C7	07	3E	7C	FB	‹ |^MùG Ç >|û
00000070	CD	13	72	79	33	C0	39	06	13	7C	74	08	8B	0E	13	7C	Í ry3À9 |t ‹ |
00000080	89	0E	20	7C	A0	10	7C	F7	26	16	7C	03	06	1C	7C	13	‰ | |÷& | |
00000090	16	1E	7C	03	06	0E	7C	83	D2	00	A3	50	7C	89	16	52	| |ƒÒ £P|‰ R
000000A0	7C	A3	49	7C	89	16	4B	7C	B8	20	00	F7	26	11	7C	8B	|£I|‰ K|¸ ÷& |‹
000000B0	1E	0B	7C	03	C3	48	F7	F3	01	06	49	7C	83	16	4B	7C	| ÃH÷ó I|ƒ K|
000000C0	00	BB	00	05	8B	16	52	7C	A1	50	7C	E8	92	00	72	1D	» ‹ R|¡P|è' r
000000D0	B0	01	E8	AC	00	72	16	8B	FB	B9	0B	00	BE	E6	7D	F3	° è¬ r ‹û¹ ¾æ}ó
000000E0	A6	75	0A	8D	7F	20	B9	0B	00	F3	A6	74	18	BE	9E	7D	¦u ¹ ó¦t ¾ž}
000000F0	E8	5F	00	33	C0	CD	16	5E	1F	8F	04	8F	44	02	CD	19	è_ 3ÀÍ ^ D Í
00000100	58	58	58	EB	E8	8B	47	1A	48	48	8A	1E	0D	7C	32	FF	XXXëè‹G HHŠ |2ÿ
00000110	F7	E3	03	06	49	7C	13	16	4B	7C	BB	00	07	B9	03	00	÷ã I| K|» ¹
00000120	50	52	51	E8	3A	00	72	D8	B0	01	E8	54	00	59	5A	58	PRQè: rØ° èT YZX
00000130	72	BB	05	01	00	83	D2	00	03	1E	0B	7C	E2	E2	8A	2E	r» ƒÒ |ââŠ.
00000140	15	7C	8A	16	24	7C	8B	1E	49	7C	A1	4B	7C	EA	00	00	|Š $|‹ I|¡K|ê
00000150	70	00	AC	0A	C0	74	29	B4	0E	BB	07	00	CD	10	EB	F2	p ¬ Àt)´ » Í ëò
00000160	3B	16	18	7C	73	19	F7	36	18	7C	FE	C2	88	16	4F	7C	; |s ÷6 |þÂ^ O|
00000170	33	D2	F7	36	1A	7C	88	16	25	7C	A3	4D	7C	F8	C3	F9	3Ò÷6 |^ %|£M|øÃù
00000180	C3	B4	02	8B	16	4D	7C	B1	06	D2	E6	0A	36	4F	7C	8B	Ã´ ‹ M|± Òæ 6O|‹
00000190	CA	86	E9	8A	16	24	7C	8A	36	25	7C	CD	13	C3	0D	0A	Ê†éŠ $|Š6%|Í Ã
000001A0	4E	6F	6E	2D	53	79	73	74	65	6D	20	64	69	73	6B	20	Non-System disk
000001B0	6F	72	20	64	69	73	6B	20	65	72	72	6F	72	0D	0A	52	or disk error R
000001C0	65	70	6C	61	63	65	20	61	6E	64	20	70	72	65	73	73	eplace and press
000001D0	20	61	6E	79	20	6B	65	79	20	77	68	65	6E	20	72	65	any key when re
000001E0	61	64	79	0D	0A	00	49	4F	20	20	20	20	20	20	53	59	ady IO SY
000001F0	53	4D	53	44	4F	53	20	20	20	53	59	53	00	00	55	AA	SMSDOS SYS Uª
00000200	F0	FF	FF	FF	FF	FF	FF	0F	00	00	00	00	00	00	00	00	ðÿÿÿÿÿÿ

Examiner Initials: Akshay Chaurasia

➢ Calculate md5hash for it

Compute hash ✕

Compute hash

MD5 (128 bit) ⌄

OK   Cancel

MD5 (128 bit) ✕

...for Device 0:

5D2FD06AA6C7CCC3E12CFAB1ED6406F7

Close

5D2FD06AA6C7CCC3E12CFAB1ED6406F7

➢ Tools -> open disk

5D2FD06AA6C7CCC3E12CFAB1ED6406F7

Examiner Initials: <u>Akshay Chaurasia</u>

➤ Compare <u>floppydisk 0</u> and <u>blankfloppy</u>

WinHex ✕

16 difference(s) found. You may now view the report using "notepad.exe".

OK   Cancel

Report - Notepad — □ ✕

File Edit Format View Help

Search for differences

1. Floppy disk 0: 1,474,560 bytes
2. C:\IST600\blankfloppy.img: 1,474,560 bytes
Offsets: hexadec.

```
  2672: 27      B6
  2673: 4F      4A
  2676: 0B      43
  2677: 77      87
  2678: 27      B6
  2679: 4F      4A
  267C: 0E      0F
  4605: 69      74
  4606: 73      65
  4607: 20      78
  4609: 65      20
  460A: 78      32
  460B: 74      0D
  460C: 20      0A
  460D: 31      0D
  460E: 00      0A
```

16 difference(s) found.

Ln 1, Col 1   100%   Windows (CRLF)   UTF-8