VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Cyber Forensics and Investigation

Course Code: BCI4001

Slot: L55+L56

Faculty: Dr. AJU D

Assessment: 3

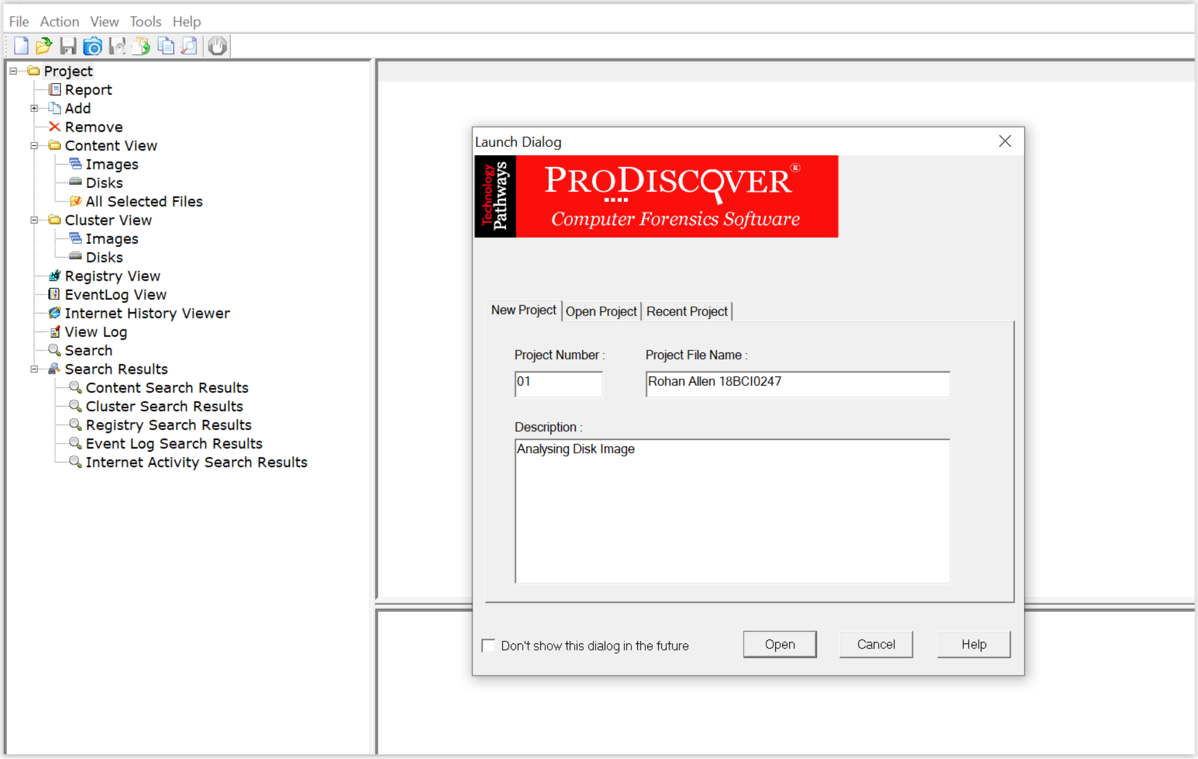
18BCI0247

Rohan Allen

Exercise 3: Pro Discover Basic

Aim: To analyse a disk image file using Pro Discover Basic and to deeply and comprehensively analyse an image, including all the file stored, deleted files, images, file types and partitions etc which will help aid forensic examinations.

Setting up Project Name and Number



Launch Dialog

PRODISCOVER® Computer Forensics Software

New Project | Open Project | Recent Project

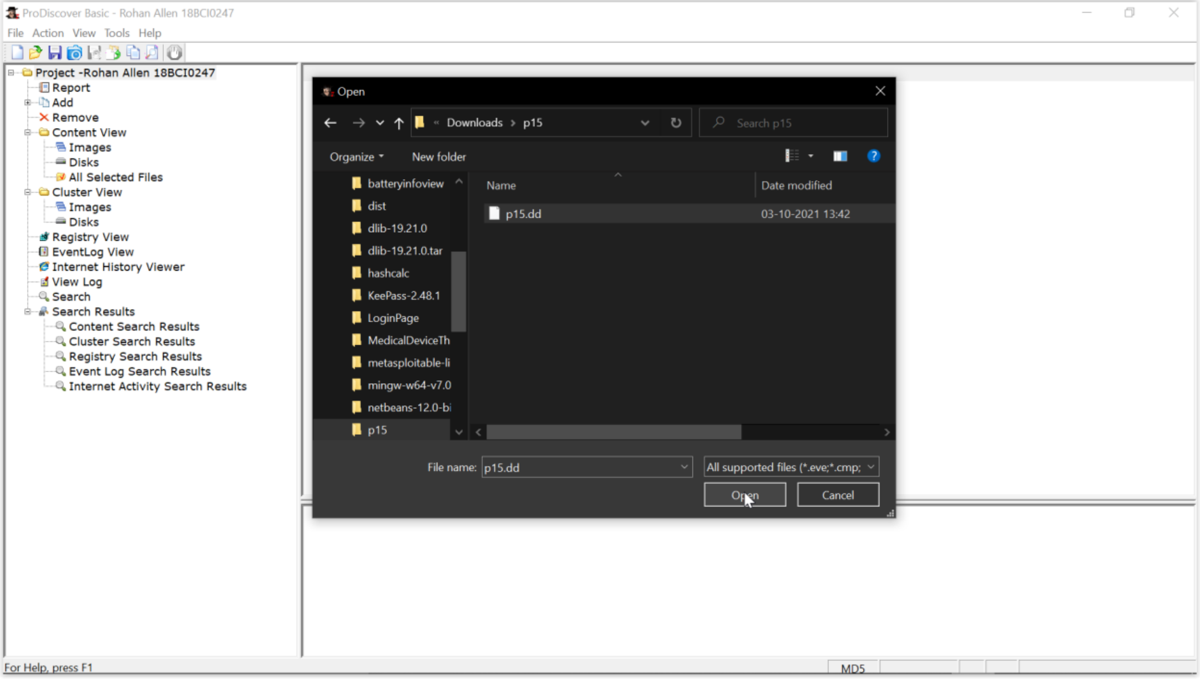
Project Number : 01

Project File Name : Rohan Allen 18BCI0247

Description : Analysing Disk Image

□ Don't show this dialog in the future

Adding p15 disk image file



ProDiscover Basic - Rohan Allen 18BCI0247

Project -Rohan Allen 18BCI0247

Open

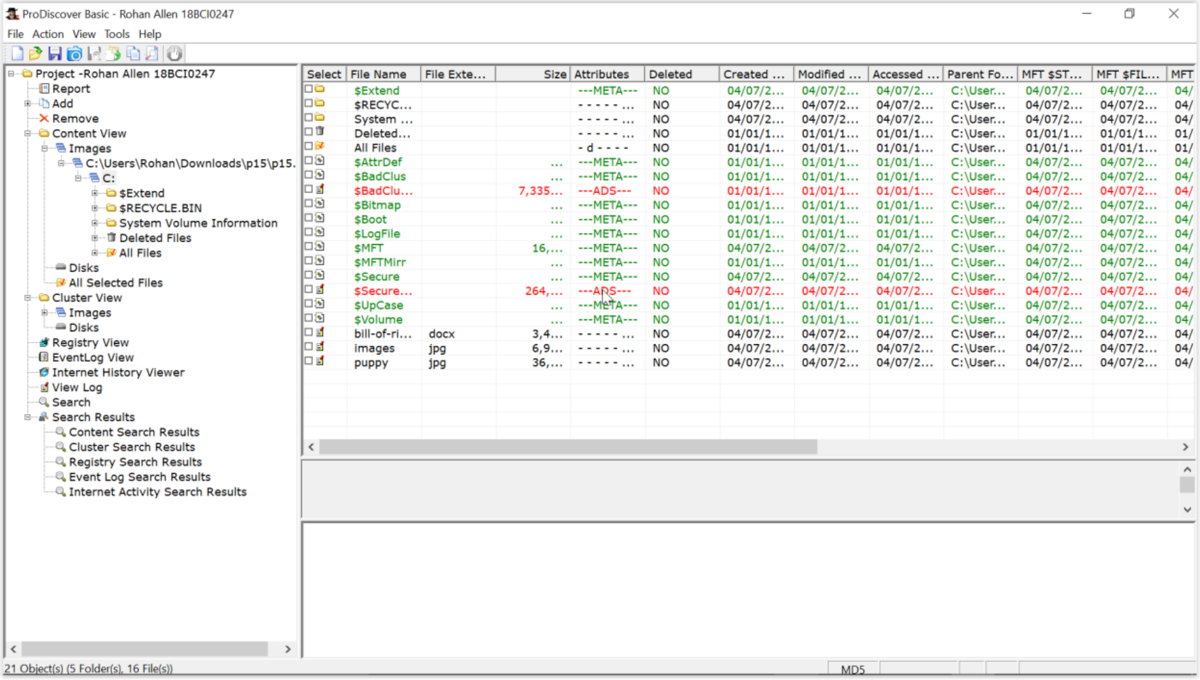
Downloads › p15

Name	Date modified
p15.dd	03-10-2021 13:42

File name: p15.dd

All supported files (*.eve;*.cmp;

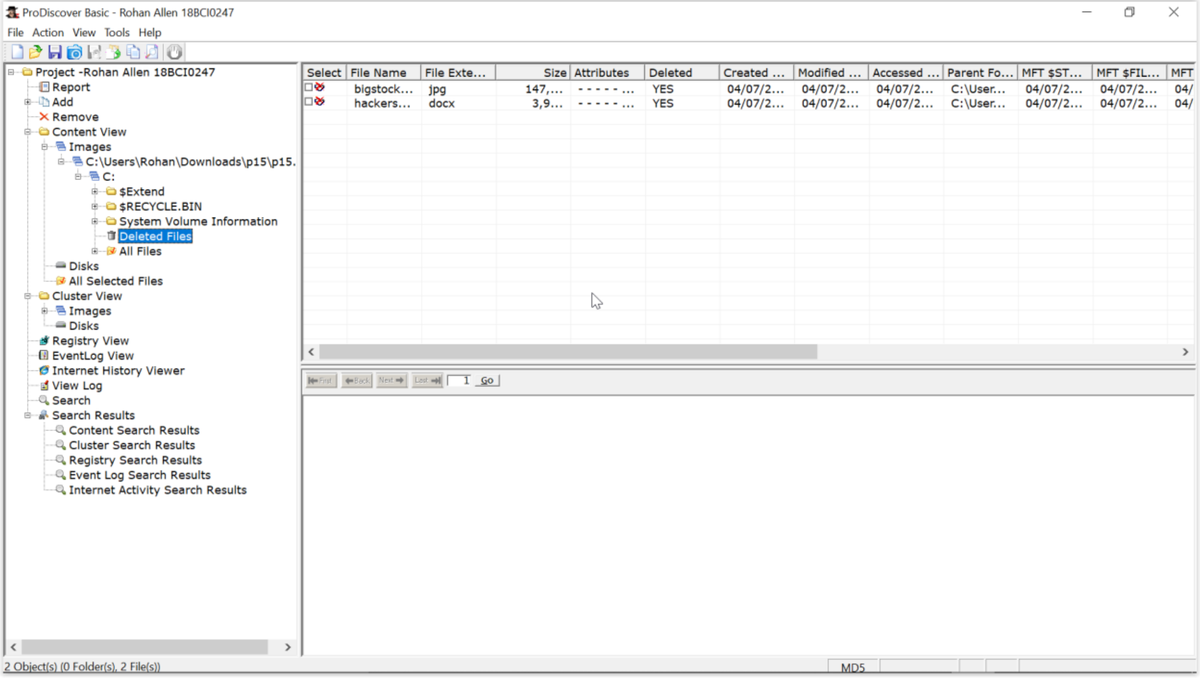
Content View of Disk File



Select	File Name	File Exte...	Size	Attributes	Deleted	Created ...	Modified ...	Accessed ...	Parent Fo...	MFT $ST...	MFT $FIL...	MFT
□	$Extend			---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	$RECYC...			- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	System ...			- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	Deleted...			- - - - - ...	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	01/01/1...	01/01/1...	01/
□	All Files			- d - - - -	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	01/01/1...	01/01/1...	01/
□	$AttrDef		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$BadClus		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$BadClu...		7,335...	---ADS---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$Bitmap		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$Boot		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$LogFile		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$MFT		16,...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	$MFTMirr		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$Secure		...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	$Secure...		264,...	---ADS---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	$UpCase		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	$Volume		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	04/
□	bill-of-ri...	docx	3,4...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	images	jpg	6,9...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	puppy	jpg	36,...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/

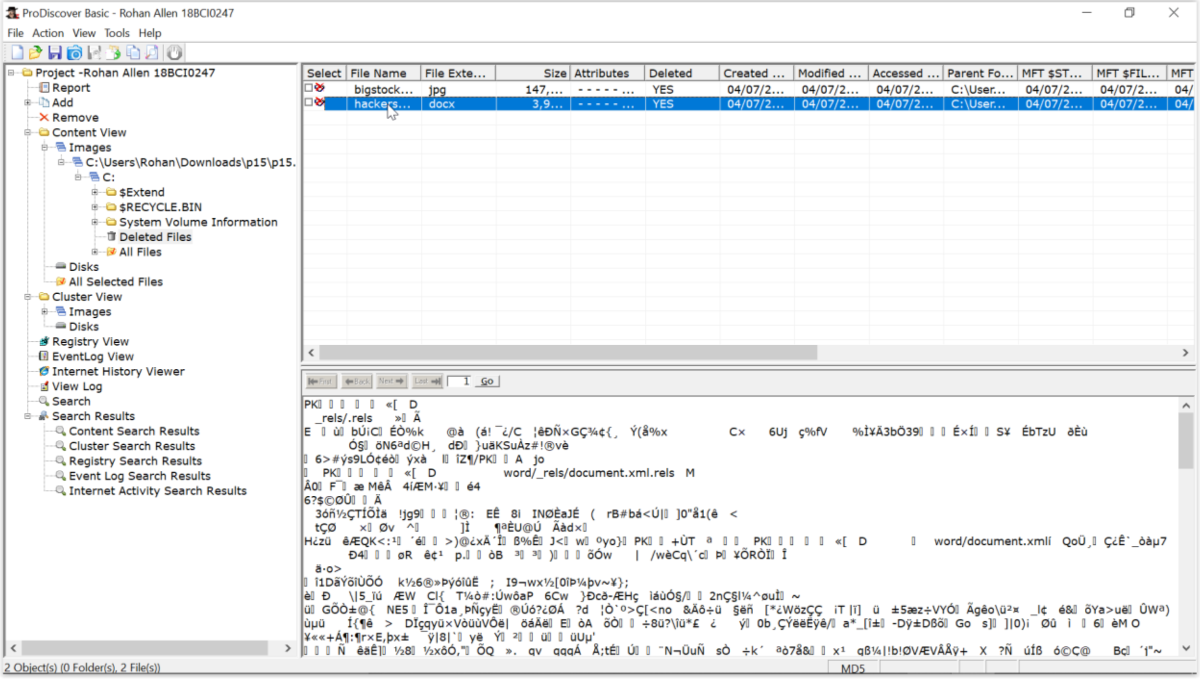
21 Object(s) (5 Folder(s), 16 File(s))

Deleted Files



Select	File Name	File Exte...	Size	Attributes	Deleted	Created ...	Modified ...	Accessed ...	Parent Fo...	MFT $ST...	MFT $FIL...	MFT
□	bigstock...	jpg	147,...	- - - - - ...	YES	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	hackers...	docx	3,9...	- - - - - ...	YES	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/

2 Object(s) (0 Folder(s), 2 File(s))

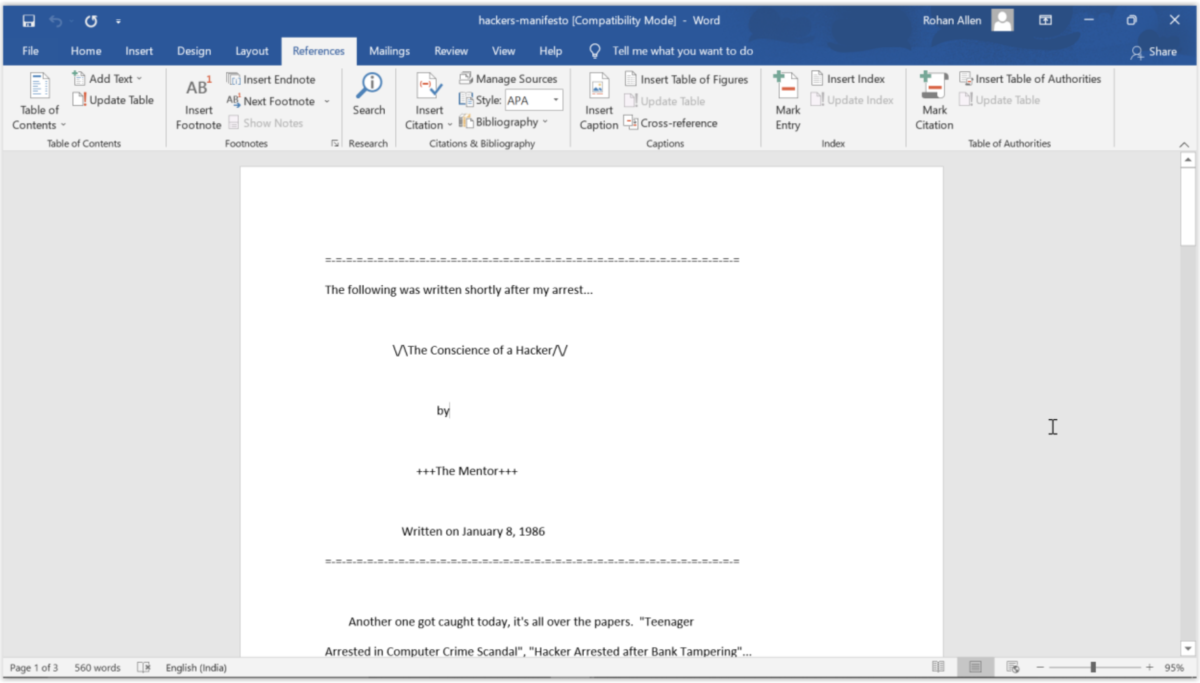


Select	File Name	File Exte...	Size	Attributes	Deleted	Created ...	Modified ...	Accessed ...	Parent Fo...	MFT $ST...	MFT $FIL...	MFT
□	bigstock...	jpg	147,...	- - - - - ...	YES	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/
□	hackers...	docx	3,9...	- - - - - ...	YES	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	04/

```
PK▯ ▯ ▯  ▯  ▯  «[  D
  _rels/.rels     »▯ Ã
E  ▯ ù▯ bÚiC▯ ÉÒ%k    @à  (á! ¯¿/C  ¦êĐÑ×GÇ¾¢{¸  Ý(å%x          C×    6Uj  ç%fV    %Ì¥Ã3bÖ39▯ ▯ ▯ É×Í▯ ▯ S¥  ÉbTzU  ðÈù
        Ó§▯ öN6ªd©H¸  dĐ▯ }uäKSuÀz#!®vè
▯ 6>#ýs9LÓ¢éò▯ ýxà   I▯ îZ¶/PK▯ ▯ A  jo
▯   PK▯ ▯ ▯  ▯  ▯  «[  D            word/_rels/document.xml.rels  M
Â0▯ F¯▯ æ MêÂ  4íÆM·¥▯ ▯ é4
6?$©ØÛ▯ ▯ Ä
  3óñ½ÇTÍÕÌä  !jg9▯ ▯ ▯ ¦®:  EÊ  8i  INØÈaJÉ  (  rB#bá<Ú|▯ ]0"å1(ê  <
  tÇØ    ×▯ Øv  ^▯        ]Ì     ¶ªÈU@Ú  Ãàd×▯
H¿zü  êÆQK<:¹▯ ´é▯ ▯ >)@¿xÄ´Î▯ ß%Ê▯ J<▯ w▯ ºyo}▯ PK▯ ▯ +ÙT  ª  ▯ ▯  PK▯ ▯ ▯  ▯  ▯  «[  D        ▯   word/document.xmlí  QoÜ¸▯ Ç¿Ê`_òàµ7
        Đ4▯ ▯ ▯ øR  ê¢¹  p.▯ ▯ òB  ³▯ ³▯ )▯ ▯ ▯ õÓw    |  /wèCq\´c▯ Þ▯ ¥ÕRÒÏ▯ Î
  ä·o>
▯ î1DãÝõîÙÕÓ  k½6®»Þýóîûë  ;  I9¬wx½[0îÞ¼þv~¥};
è▯ Đ   \|5_ïú  ÆW  Cl{  T¼ò#:ÚwôaP  6Cw  }Đcð-ÆHç  ìáùÓ§/▯ ▯ 2nÇ§l¼^øuÌ▯ ~
ü▯ GÕÒ±@{  NE5▯ Î¯Ô1a¸ÞÑçyË▯ ®Úó?¿ØÁ  ?d  ¦Ò`º>Ç[<no  &Äô÷ü  §ëñ  [*¿WözÇÇ  iT |ï]  ü  ±5æz÷VYÓ▯ Ãgêo\ü²¤  _l¢  é&▯ õYa>uë▯ ÛWª)
ùµü    Í{¶ê  >  DÏçqyü×VòüùVÔë|  öáÄë▯ E▯ òA  õÒ▯ ▯ ÷8ü?\îü*£  ¿    ý▯ 0b¸ÇÝëëËÿê/▯ a*_[î±▯ -Dÿ±Dßõ▯ Go  s]▯ ]|0)i  Øû  ì  ▯ 6▯ èM O
¥««+Á¶:¶r×E,þx±   ÿ|8|`▯ yë  Ý▯ ²▯ ▯ ü▯ ▯ üUµ'
▯ ▯ ▯ Ñ  êäÊ]▯ ½8▯ ½xôÓ,"▯ ÕQ  ».  qv  qqqÁ  Å;tÉ▯ Ú▯ ▯ ¨N¬ÜuÑ  sÒ  ÷k´  ªò7å&▯ ▯ x¹  qß¼|!b!ØVÆVÂÅÿ+  X  ?Ñ  úíß  ó©Ç@    Bc▯ ´¡"~
```

2 Object(s) (0 Folder(s), 2 File(s))

Hackers manifesto



=-=

The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

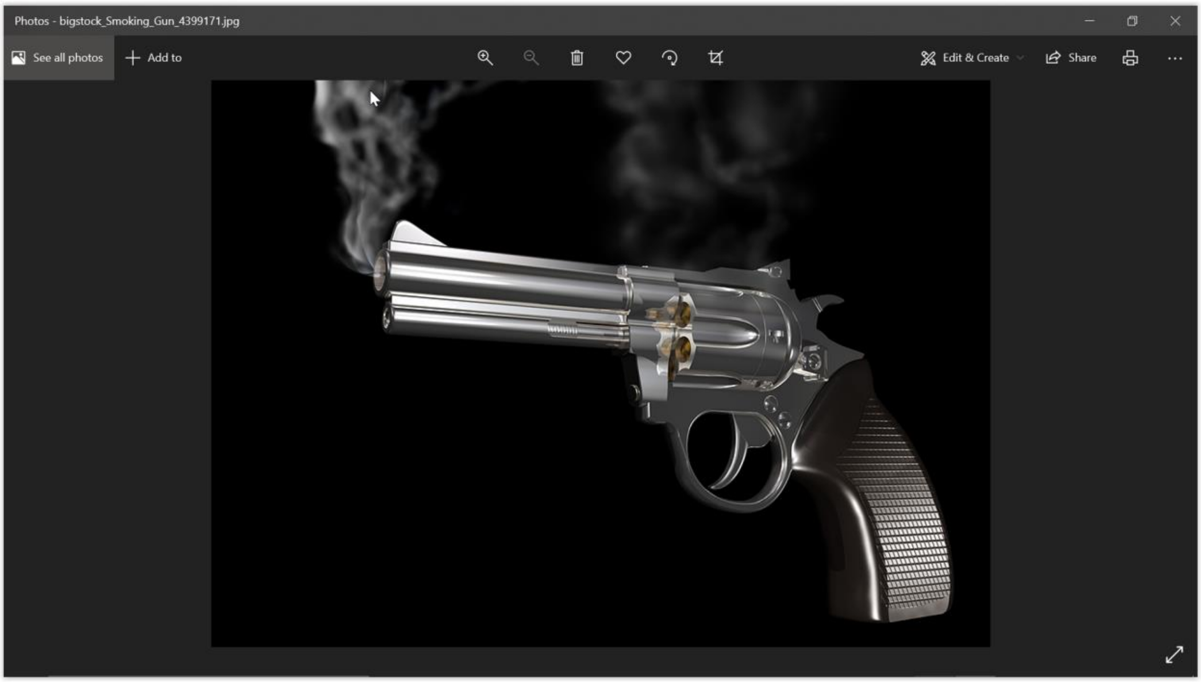
Written on January 8, 1986

=-=

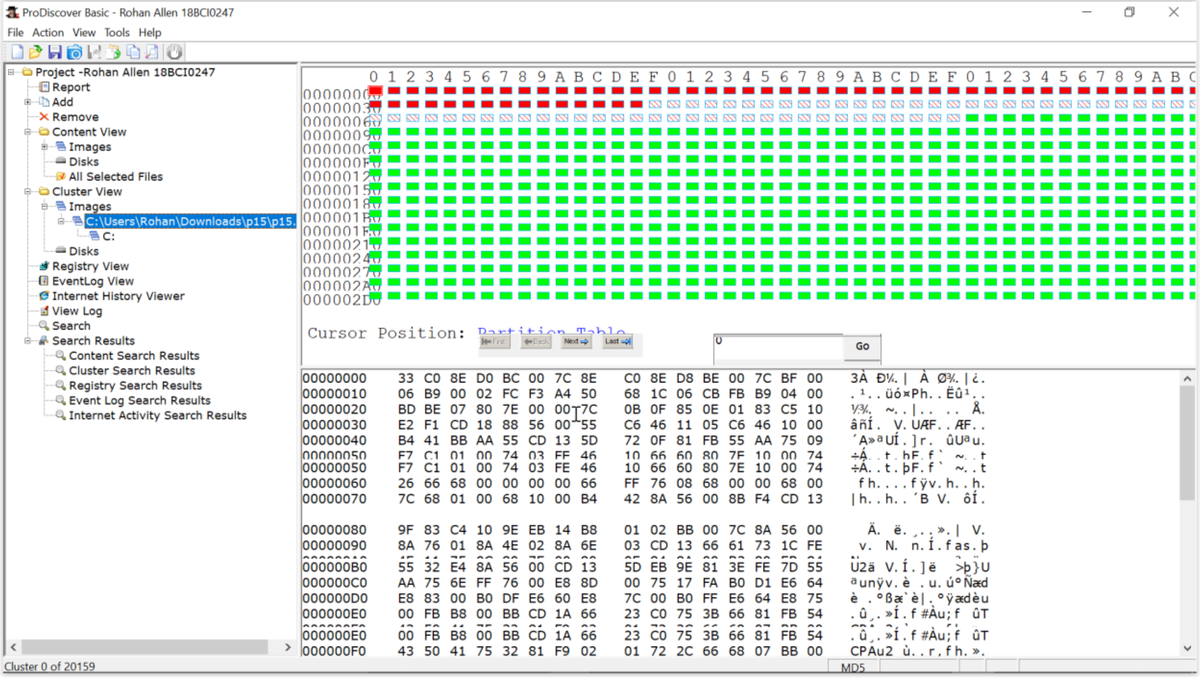
Another one got caught today, it's all over the papers. "Teenager

Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Big stock gun image

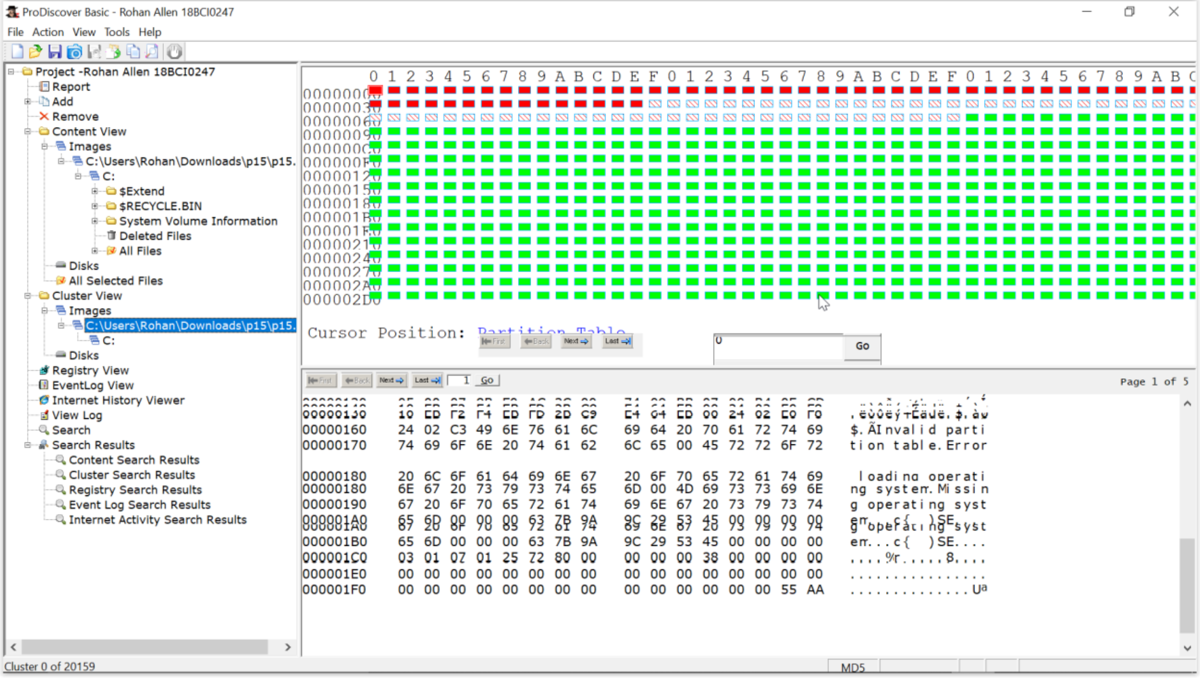


Physical Drive in Cluster View



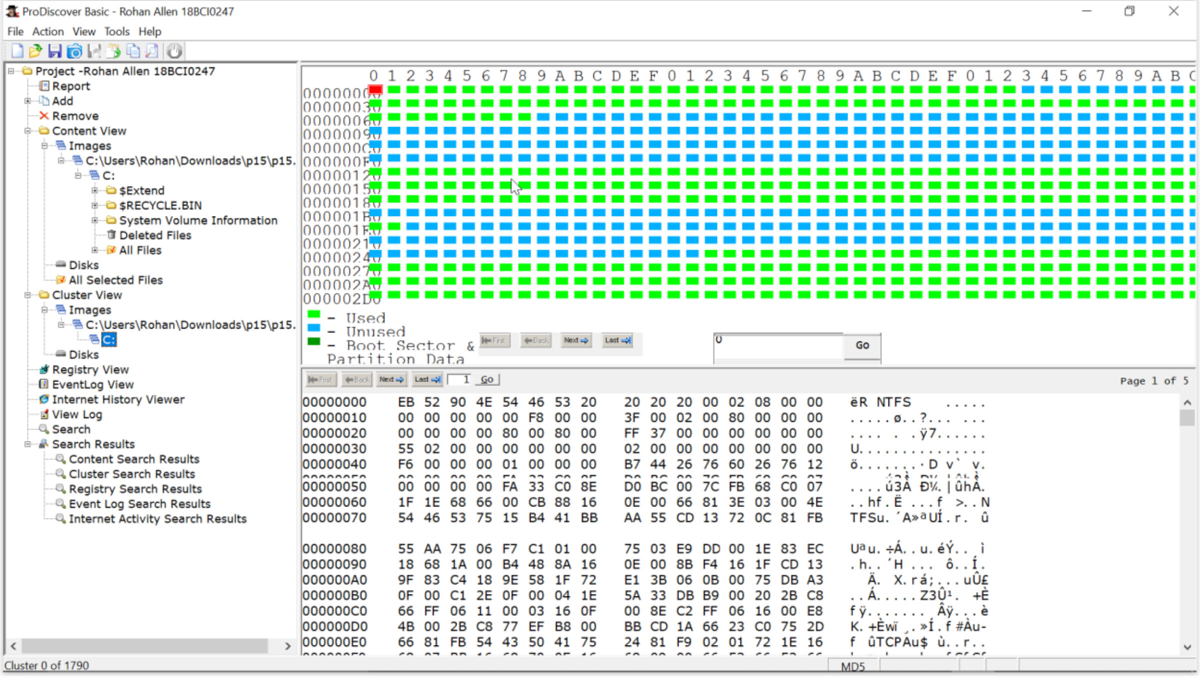
```
00000000    33 C0 8E D0 BC 00 7C 8E    C0 8E D8 BE 00 7C BF 00    3À Ð¼.|  À Ø¾.|¿.
00000010    06 B9 00 02 FC F3 A4 50    68 1C 06 CB FB B9 04 00    .¹..üó¤Ph..Ëû¹..
00000020    BD BE 07 80 7E 00 00 7C    0B 0F 85 0E 01 83 C5 10    ½¾.  ~..|..  .. Å.
00000030    E2 F1 CD 18 88 56 00 55    C6 46 11 05 C6 46 10 00    âñÍ.  V. UÆF..ÆF..
00000040    B4 41 BB AA 55 CD 13 5D    72 0F 81 FB 55 AA 75 09    ´A»ªUÍ.]r.  ûUªu.
00000050    F7 C1 01 00 74 03 FE 46    10 66 60 80 7E 10 00 74    ÷Á..t.þF.f`  ~..t
00000050    F7 C1 01 00 74 03 FE 46    10 66 60 80 7E 10 00 74    ÷Á..t.þF.f`  ~..t
00000060    26 66 68 00 00 00 00 66    FF 76 08 68 00 00 68 00     fh....fÿv.h..h.
00000070    7C 68 01 00 68 10 00 B4    42 8A 56 00 8B F4 CD 13    |h..h..´B V.  ôÍ.

00000080    9F 83 C4 10 9E EB 14 B8    01 02 BB 00 7C 8A 56 00      Ä.  ë.¸..».|  V.
00000090    8A 76 01 8A 4E 02 8A 6E    03 CD 13 66 61 73 1C FE     v.  N.  n.Í.fas.þ
000000B0    55 32 E4 8A 56 00 CD 13    5D EB 9E 81 3E FE 7D 55    U2ä V.Í.]ë   >þ}U
000000C0    AA 75 6E FF 76 00 E8 8D    00 75 17 FA B0 D1 E6 64    ªunÿv.è  .u.ú°Ñæd
000000D0    E8 83 00 B0 DF E6 60 E8    7C 00 B0 FF E6 64 E8 75    è .°ßæ`è|.°ÿædèu
000000E0    00 FB B8 00 BB CD 1A 66    23 C0 75 3B 66 81 FB 54    .û¸.»Í.f #Àu;f  ûT
000000E0    00 FB B8 00 BB CD 1A 66    23 C0 75 3B 66 81 FB 54    .û¸.»Í.f #Àu;f  ûT
000000F0    43 50 41 75 32 81 F9 02    01 72 2C 66 68 07 BB 00    CPAu2 ù..r,fh.».
```

Error loading message



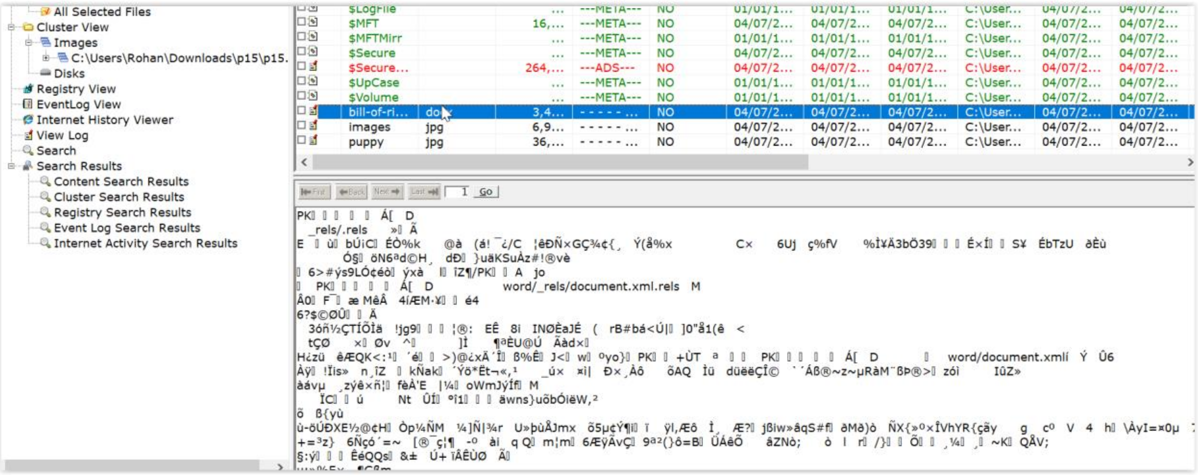
```
00000150    10 ED F2 F4 ED FD 2D C9   E4 64 ED 00 24 02 E0 F0   .ëòôíý-ÉäDí.$.àð
00000160    24 02 C3 49 6E 76 61 6C   69 64 20 70 61 72 74 69   $.ÃInvalid parti
00000170    74 69 6F 6E 20 74 61 62   6C 65 00 45 72 72 6F 72   tion table.Error

00000180    20 6C 6F 61 64 69 6E 67   20 6F 70 65 72 61 74 69    loading operati
00000180    6E 67 20 73 79 73 74 65   6D 00 4D 69 73 73 69 6E   ng system.Missin
00000190    67 20 6F 70 65 72 61 74   69 6E 67 20 73 79 73 74   g operating syst
000001A0    65 6D 00 00 00 63 7B 9A   9C 29 53 45 00 00 00 00   em...c{  )SE....
000001B0    65 6D 00 00 00 63 7B 9A   9C 29 53 45 00 00 00 00   em...c{  )SE....
000001C0    03 01 07 01 25 72 80 00   00 00 00 38 00 00 00 00   ....%r.....8....
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 55 AA   ..............Uª
```

Logical Drive cluster



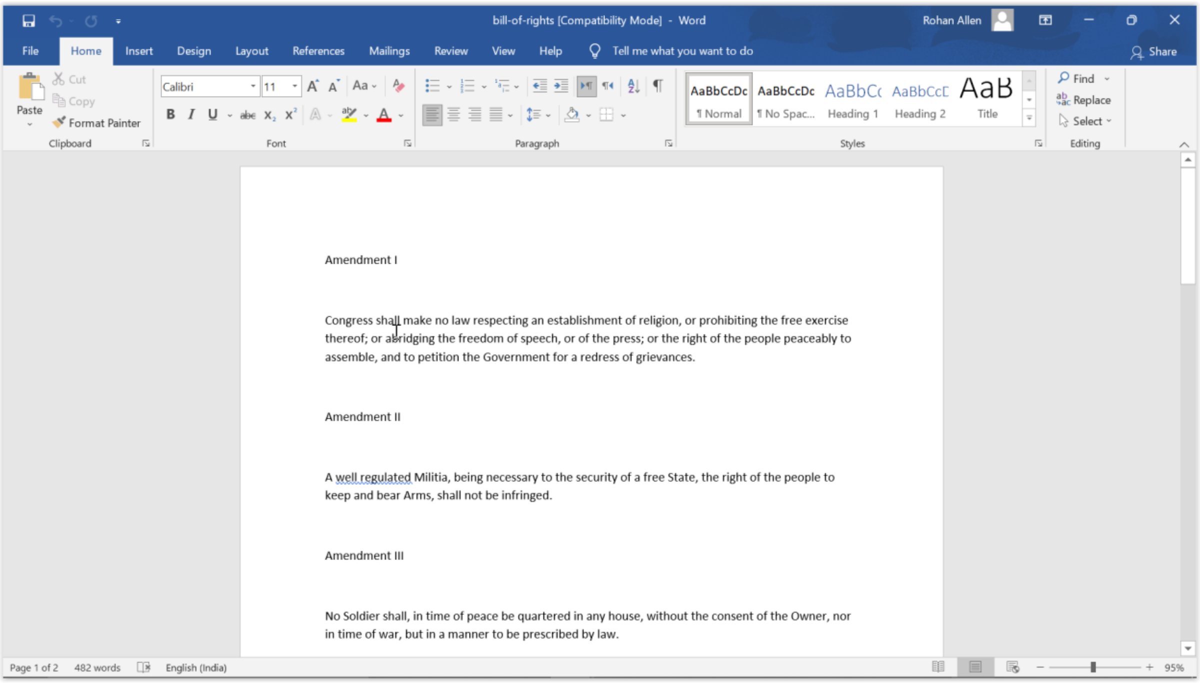
```
00000000    EB 52 90 4E 54 46 53 20   20 20 20 00 02 08 00 00   ëR NTFS    .....
00000010    00 00 00 00 00 F8 00 00   3F 00 02 00 80 00 00 00   .....ø..?... ...
00000020    00 00 00 00 80 00 80 00   FF 37 00 00 00 00 00 00   .... . .ÿ7......
00000030    55 02 00 00 00 00 00 00   02 00 00 00 00 00 00 00   U...............
00000040    F6 00 00 00 01 00 00 00   B7 44 26 76 60 26 76 12   ö.......·D v` v.
00000050    00 00 00 00 FA 33 C0 8E   D0 BC 00 7C FB 68 C0 07   ....ú3À Ð¼.|ûhÀ.
00000060    1F 1E 68 66 00 CB 88 16   0E 00 66 81 3E 03 00 4E   ..hf.Ë ...f >..N
00000070    54 46 53 75 15 B4 41 BB   AA 55 CD 13 72 0C 81 FB   TFSu.´A»ªUÍ.r. û

00000080    55 AA 75 06 F7 C1 01 00   75 03 E9 DD 00 1E 83 EC   Uªu.÷Á..u.éÝ.. ì
00000090    18 68 1A 00 B4 48 8A 16   0E 00 8B F4 16 1F CD 13   .h..´H ... ô..Í.
000000A0    9F 83 C4 18 9E 58 1F 72   E1 3B 06 0B 00 75 DB A3     Ä. X.rá;...uÛ£
000000B0    0F 00 C1 2E 0F 00 04 1E   5A 33 DB B9 00 20 2B C8   ..Á.....Z3Û¹. +È
000000C0    66 FF 06 11 00 03 16 0F   00 8E C2 FF 06 16 00 E8   fÿ........Âÿ...è
000000D0    4B 00 2B C8 77 EF B8 00   BB CD 1A 66 23 C0 75 2D   K.+Èwï¸.»Í.f#Àu-
000000E0    66 81 FB 54 43 50 41 75   24 81 F9 02 01 72 1E 16   f ûTCPAu$ ù..r..
```

Bill of rights word doc



$LogFile		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
$MFT		16,...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
$MFTMirr		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
$Secure		...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
$Secure...		264,...	---ADS---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
$UpCase		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
$Volume		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
bill-of-ri...	do	3,4...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
images	jpg	6,9...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
puppy	jpg	36,...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...

```
PK        Á[   D
  _rels/.rels     »  Ã
E   ù  bÚiC  ÉÒ%k    @à  (á! ¯¿/C  ¦êÐÑ×GÇ¾¢{¸  Ý(å%x         C×    6Uj  ç%fV     %Ì¥Ä3bÖ39      É×Í    S¥  ÉbTzU  ðÈù
      Ó§  öN6ªd©H¸  dÐ  }uäKSuÀz#!®vè
  6>#ýs9LÓ¢éò  ýxà     ÌZ¶/PK    A  jo
   PK            Á[  D              word/_rels/document.xml.rels   M
Â0  F    æ MëÂ   4íÆM·¥   é4
6?$©ØÛ    Ä
   3óñ½ÇTÏÕà  !jg9        ¦®:  EÈ  8ì  INØÈaJÉ  (   rB#bá<Ú|  ]0"å1(ê   <
   tÇØ     ×  Øv   ^       ]ì       ¶ªÈU@Ú  Ãàd×
H¿zü   ëÆQK<:¹   ´é    >)@¿xÄ´Ì  ß%È  J<  w  ºyo}  PK    +ÙT   ª        PK              Á[   D         word/document.xmlí   Ý   Ù6
Äÿ  !Ïis»   n¸ÌZ     kÑak  ´Yö*Èt¬«,¹    _úx   ×i|   Ð×¸Àô     õAQ   Ìü   düëëÇÏ©   ´´ÁB®~z~µRàM¨ßÞ®>  zöì        ÍûZ»
àávµ   ¸zýê×ñ¦  fèÀ'E   |¼  oWmJýf   M
    ÌC   ú       Nt   Ûí   º¹ì       äwns}uõbÖiêW,²
ö   ß{yù
ù-öÚÐXE½@¢H  Òp¼ÑM    ¼]Ñ|¾r   U»þùÅJmx   õ5µ¢Ý¶  Ï   ÿI,Æõ   Ì¸    Æ?  jßiw»âqS#fi  ðMð}ò   ÑX{»º×ÏVhYR{çây     g   cº   V   4   h   \ÀyI=×0µ   7
+=³z}   6Ñçó´=~   [®   ç¦¶   -º   ài   q Q   m¦m   6ÆÿÃvÇ   9ª²(}ô=B   ÚÁêÕ      âZNò;      ò   ì   r   /}         Õ         ¸¼    ¸   ~K   QÂV;
§:ý           ÉéQQs   &±   Ú+ ÏÂÊÜØ   Ã
```



Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

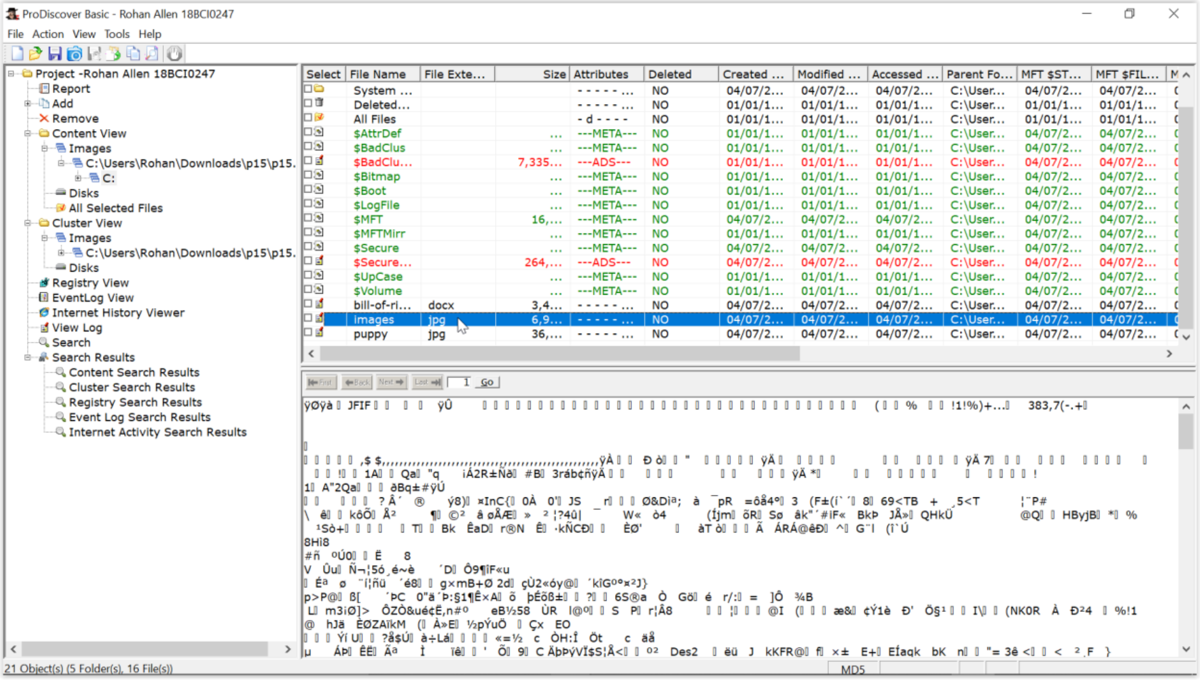
Amendment II

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

Amendment III

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Cat Image


ProDiscover Basic - Rohan Allen 18BCI0247
File Action View Tools Help

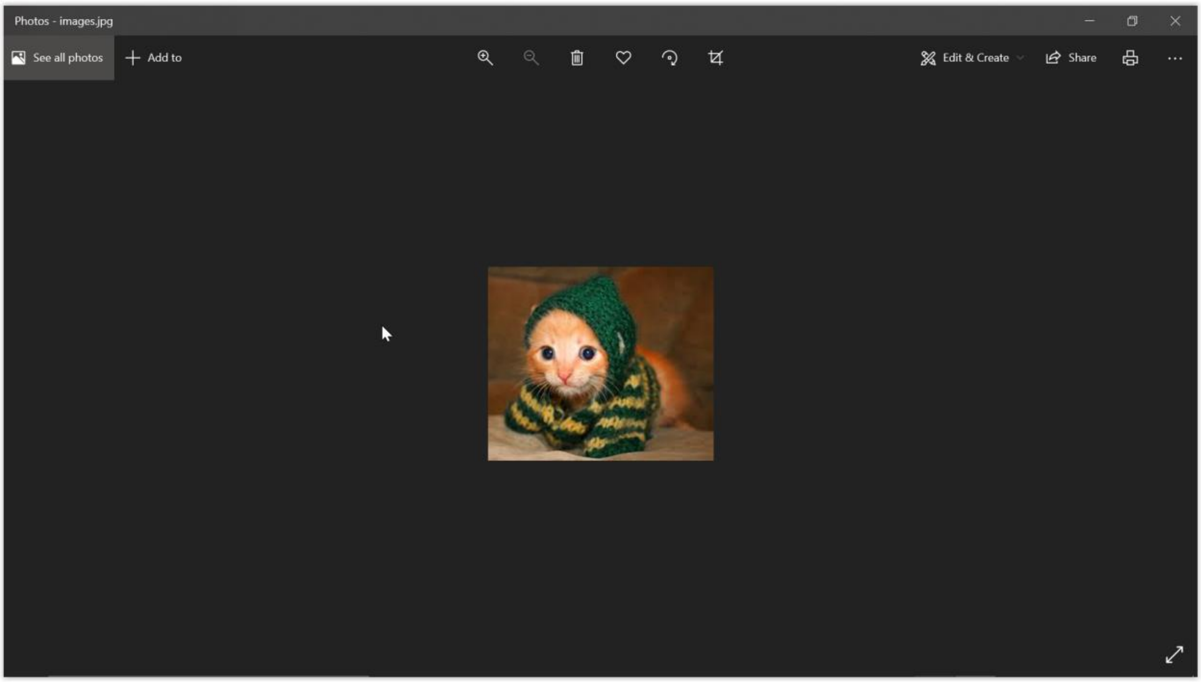
- Project -Rohan Allen 18BCI0247
  - Report
  - Add
  - Remove
  - Content View
    - Images
      - C:\Users\Rohan\Downloads\p15\p15.
        - C:
    - Disks
    - All Selected Files
  - Cluster View
    - Images
      - C:\Users\Rohan\Downloads\p15\p15.
    - Disks
  - Registry View
  - EventLog View
  - Internet History Viewer
  - View Log
  - Search
  - Search Results
    - Content Search Results
    - Cluster Search Results
    - Registry Search Results
    - Event Log Search Results
    - Internet Activity Search Results

Select	File Name	File Exte...	Size	Attributes	Deleted	Created ...	Modified ...	Accessed ...	Parent Fo...	MFT $ST...	MFT $FIL...
□	System ...			- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
□	Deleted...			- - - - - ...	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	01/01/1...	01/01/1...
□	All Files			- d - - - -	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	01/01/1...	01/01/1...
□	$AttrDef		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$BadClus		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$BadClu...		7,335...	---ADS---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$Bitmap		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$Boot		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$LogFile		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$MFT		16,...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
□	$MFTMirr		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$Secure		...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
□	$Secure...		264,...	---ADS---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
□	$UpCase		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	$Volume		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...
□	bill-of-ri...	docx	3,4...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
□	images	jpg	6,9...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...
□	puppy	jpg	36,...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...

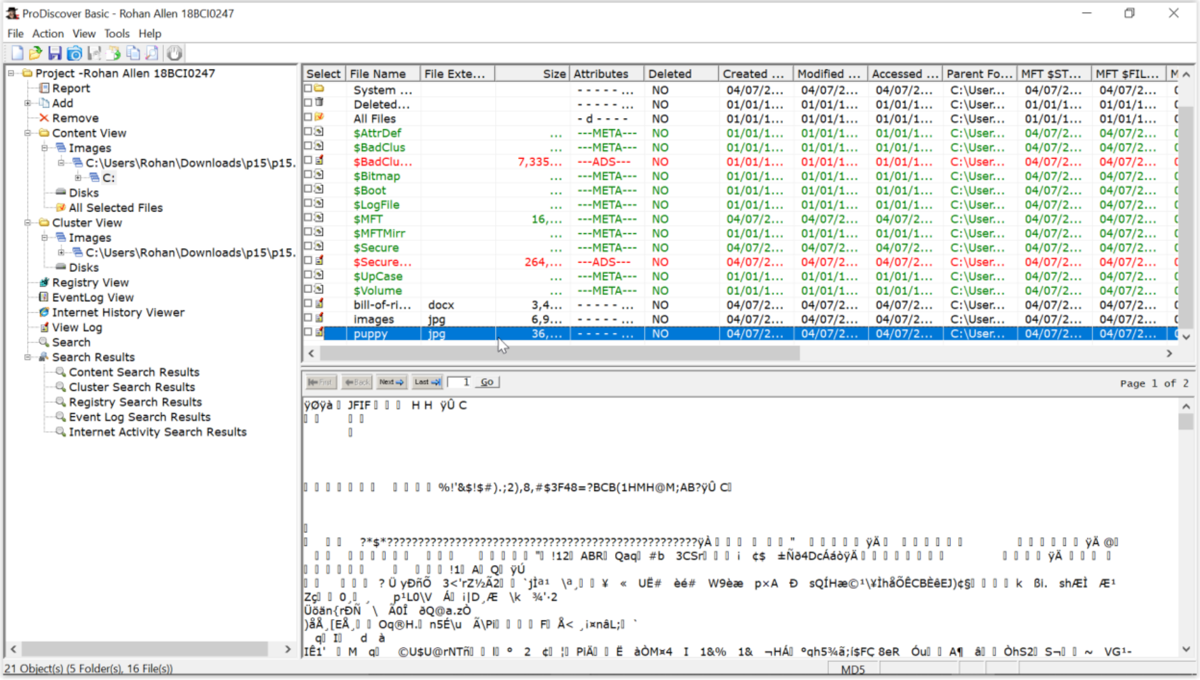
```
ÿØÿà  JFIF        ÿÛ                                        (   %    !1!%)+...  383,7(-.+
```

21 Object(s) (5 Folder(s), 16 File(s))

MD5



Puppy image



ProDiscover Basic - Rohan Allen 18BCI0247

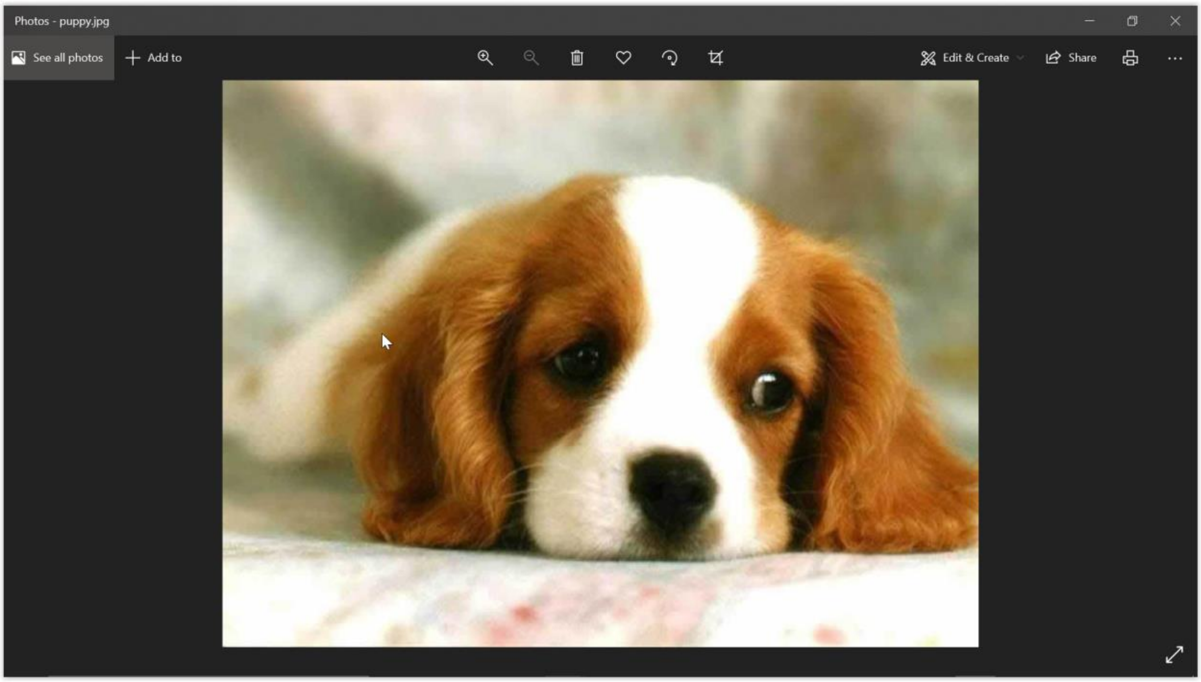
Select	File Name	File Exte...	Size	Attributes	Deleted	Created ...	Modified ...	Accessed ...	Parent Fo...	MFT $ST...	MFT $FIL...	M
□	System ...			- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(
□	Deleted...			- - - - - ...	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	01/01/1...	01/01/1...	(
□	All Files			- d - - - -	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	01/01/1...	01/01/1...	(
□	$AttrDef		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$BadClus		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$BadClu...		7,335...	---ADS---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$Bitmap		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$Boot		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$LogFile		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$MFT		16,...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(
□	$MFTMirr		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$Secure		...	---META---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(
□	$Secure...		264,...	---ADS---	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(
□	$UpCase		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	$Volume		...	---META---	NO	01/01/1...	01/01/1...	01/01/1...	C:\User...	04/07/2...	04/07/2...	(
□	bill-of-ri...	docx	3,4...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(
□	images	jpg	6,9...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(
□	puppy	jpg	36,...	- - - - - ...	NO	04/07/2...	04/07/2...	04/07/2...	C:\User...	04/07/2...	04/07/2...	(

Page 1 of 2

```
ÿØÿà ▯ JFIF ▯ ▯ ▯  H H  ÿÛ C
▯ ▯     ▯ ▯
        ▯



▯ ▯ ▯ ▯ ▯ ▯ ▯   ▯ ▯ ▯ ▯ %!'&$!$#).;2),8,#$3F48=?BCB(1HMH@M;AB?ÿÛ C▯


▯
▯   ▯ ▯   ?*$*????????????????????????????????????????????????????ÿÀ ▯ ▯ ▯  ▯  ▯ ▯ "  ▯ ▯ ▯ ▯ ▯ ÿÄ ▯  ▯ ▯ ▯ ▯ ▯ ▯         ▯ ▯ ▯ ▯ ▯ ▯ ÿÄ @▯
  ▯ ▯   ▯ ▯ ▯ ▯ ▯ ▯ ▯   ▯ ▯ ▯    ▯ ▯ ▯ ▯ ▯ "▯ !12▯ ABR▯ Qaq▯ #b  3CSr▯ ▯ ▯ i  ¢$  ±Ñð4DcÁáòÿÄ ▯ ▯ ▯ ▯ ▯ ▯ ▯ ▯         ▯ ▯ ▯ ▯ ÿÄ ▯ ▯ ▯  ▯
▯ ▯ ▯ ▯ ▯ ▯ ▯     ▯    ▯ ▯ ▯ !1▯ A▯ Q▯ ÿÚ
▯ ▯    ▯ ▯ ▯ ? Ü yÐñÕ  3<'rZ½Ã2▯ ▯ `jÌª¹  \ª¸▯ ▯ ¥  «  UË#  èé#  W9èæ  p×A  Ð  sQÍHæ©¹\¥ÌhåÕÊCBÈêEJ)¢§▯ ▯ ▯ ▯ k  ßI.  shÆÌ  Æ¹
Zç▯ ▯ 0¸▯  ¸    p¹L0\V  Á▯ i|D¸Æ  \k  ¾'·2
Üöän{rÐÑ  \  Ã0Î  ðQ@a.zÒ
)åÅ¸[EÅ¸▯ ▯ Oq®H.▯ n5É\u  Ã\Pi▯ ▯ ▯ ▯ F▯ Å< ¸i¤nâL;▯ `
  q▯ I▯   d  à
IÊ1'  ▯ M  q▯   ©U$U@rNTñ▯ ▯ I▯ °  2  ¢▯ ¦▯ PIÄ▯ ▯ Ë  àÒM¤4  I  1&%  1&  ¬HÁ▯ °qh5¾ã;í$FÇ 8eR  Óu▯ ▯ A¶  â▯ ▯ ÒhS2▯ S¬▯ ▯ ~  VG¹-
```

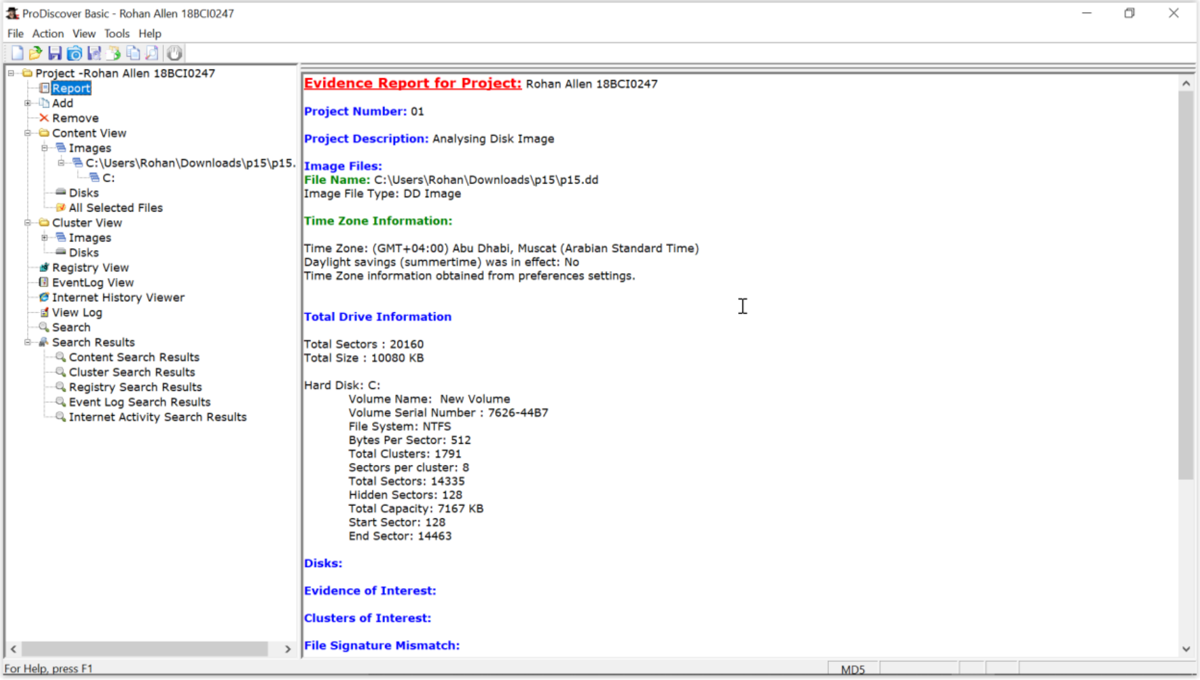
21 Object(s) (5 Folder(s), 16 File(s))

MD5



Photos - puppy.jpg

Evidence Report of Proj



```
Evidence Report for Project: Rohan Allen 18BCI0247

Project Number: 01

Project Description: Analysing Disk Image

Image Files:
File Name: C:\Users\Rohan\Downloads\p15\p15.dd
Image File Type: DD Image

Time Zone Information:

Time Zone: (GMT+04:00) Abu Dhabi, Muscat (Arabian Standard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained from preferences settings.


Total Drive Information

Total Sectors : 20160
Total Size : 10080 KB

Hard Disk: C:
        Volume Name:  New Volume
        Volume Serial Number : 7626-44B7
        File System: NTFS
        Bytes Per Sector: 512
        Total Clusters: 1791
        Sectors per cluster: 8
        Total Sectors: 14335
        Hidden Sectors: 128
        Total Capacity: 7167 KB
        Start Sector: 128
        End Sector: 14463

Disks:

Evidence of Interest:

Clusters of Interest:

File Signature Mismatch:
```

Result: There are some incriminating evidence found like the 2 deleted files which were the a picture of a gun and also a word doc called hackers manifesto which clearly states that he is a hacker. Therefore we should tread with caution and investigate this person thoroughly.