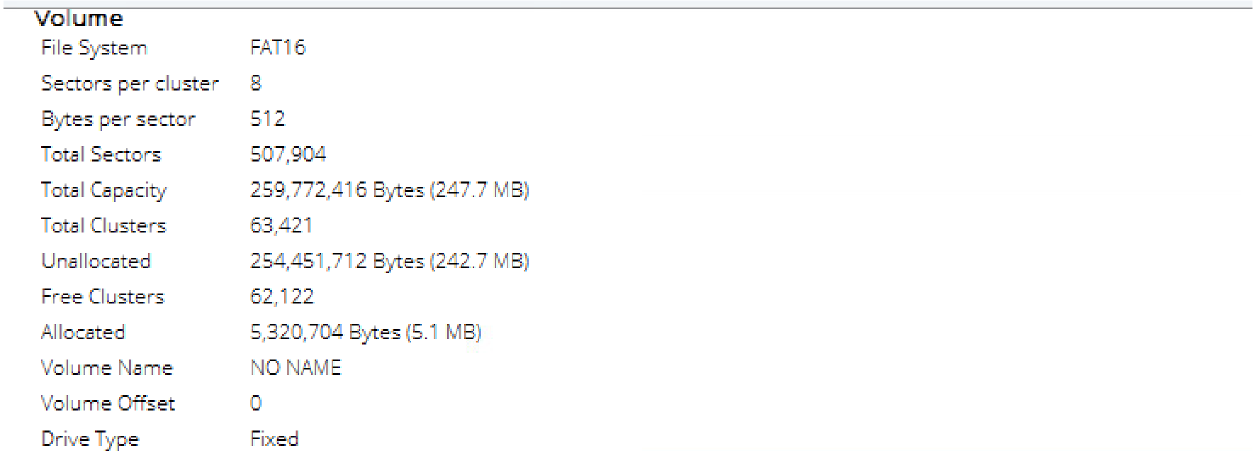
CSEC 730 - Advanced Computer Forensics

Shriram Karpoora Sundara Pandian (KP)

Homework - 4 - Recover Hidden Passwords Using Steganography

1.
What is the filesystem of the given USB-Image.dd image (provide a screenshot)? How do you get this information? (10 points)

The File System type is FAT16 and I used Encase for this investigation. From the Encase>Report which is in the bottom I found this information.

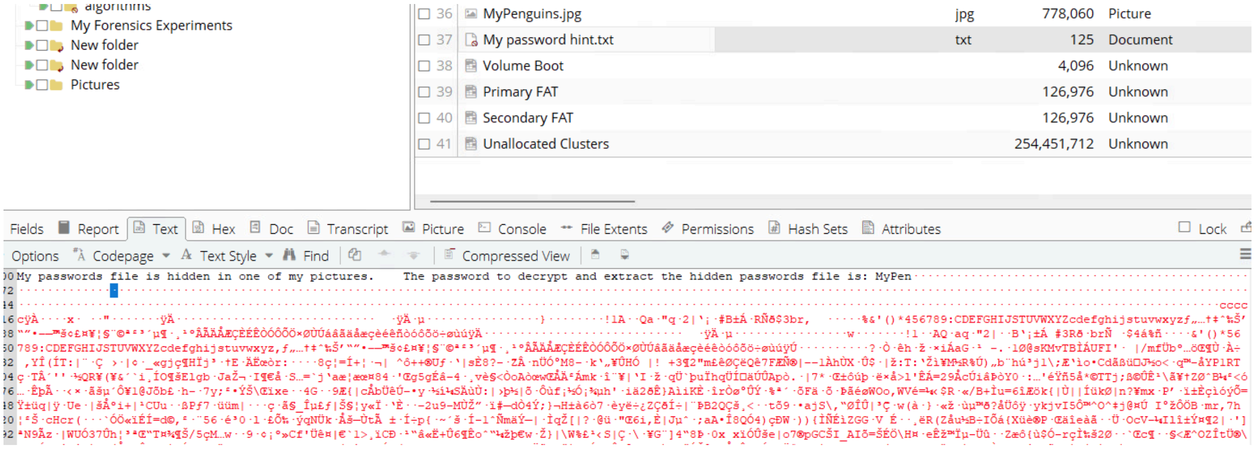


Volume

File System	FAT16
Sectors per cluster	8
Bytes per sector	512
Total Sectors	507,904
Total Capacity	259,772,416 Bytes (247.7 MB)
Total Clusters	63,421
Unallocated	254,451,712 Bytes (242.7 MB)
Free Clusters	62,122
Allocated	5,320,704 Bytes (5.1 MB)
Volume Name	NO NAME
Volume Offset	0
Drive Type	Fixed

2. Which file (including deleted file) provides you the clue to extract the hidden password file? What crucial information do you get from this file? (provide a screenshot of the file content) (20 points)

My Password hint.txt give all we needed which is a deleted file



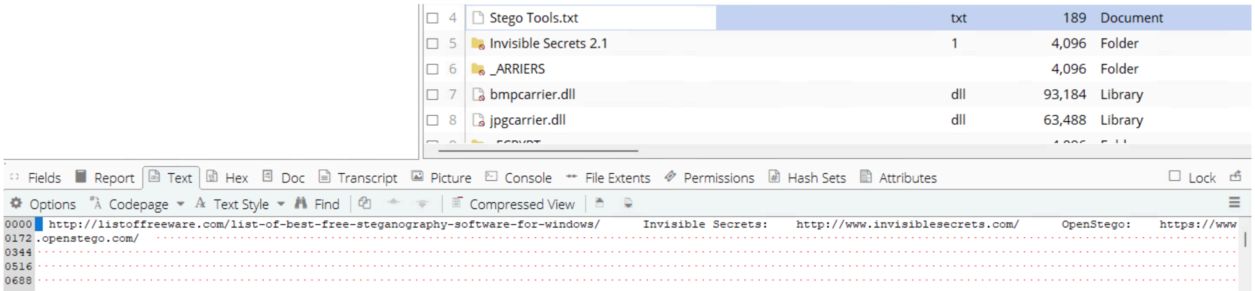
□	36	MyPenguins.jpg	jpg	778,060	Picture
□	37	My password hint.txt	txt	125	Document
□	38	Volume Boot		4,096	Unknown
□	39	Primary FAT		126,976	Unknown
□	40	Secondary FAT		126,976	Unknown
□	41	Unallocated Clusters		254,451,712	Unknown

```
My passwords file is hidden in one of my pictures.    The password to decrypt and extract the hidden passwords file is: MyPen
```

And the password is ‘MyPen’

3. Provide two pieces of evidence that indicate that Mike might have used the steganography tool called Invisible Secrets (ignore the version number) to hide his password file. (20 points)

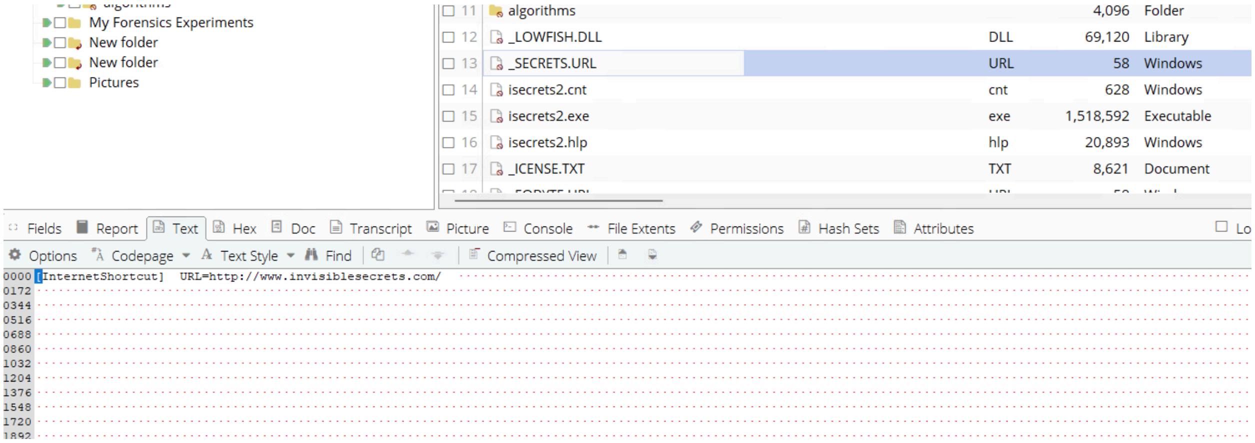
From the stegotools.txt file we can see that he tried to use or may be used invisiblesecrets.com which is a steganography tool.



□	4	Stego Tools.txt	txt	189	Document
□	5	Invisible Secrets 2.1	1	4,096	Folder
□	6	_ARRIERS		4,096	Folder
□	7	bmpcarrier.dll	dll	93,184	Library
□	8	jpgcarrier.dll	dll	63,488	Library

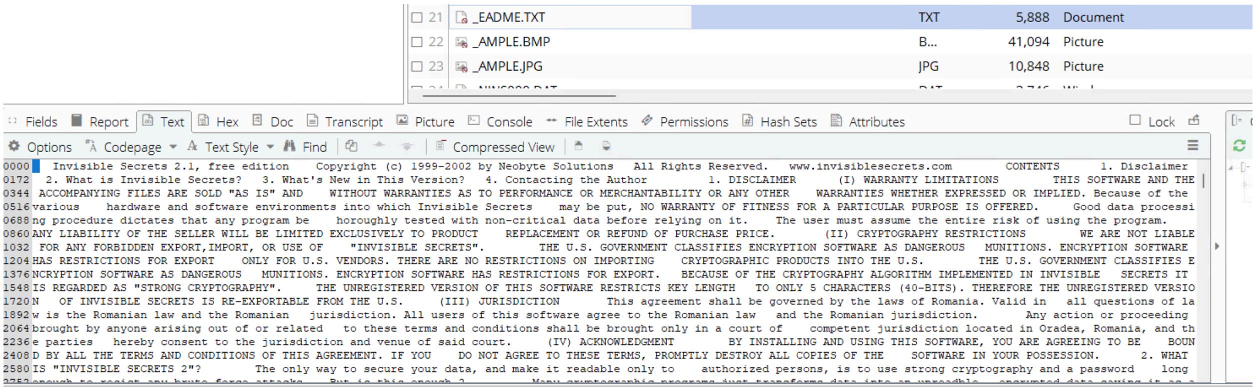
```
0000 http://listoffreeware.com/list-of-best-free-steganography-software-for-windows/      Invisible Secrets:    http://www.invisiblesecrets.com/      OpenStego:    https://www
0172 .openstego.com/
0344
0516
0688
```

From _SECRETS.URL, we can see he searched for invisiblesecrets.com.



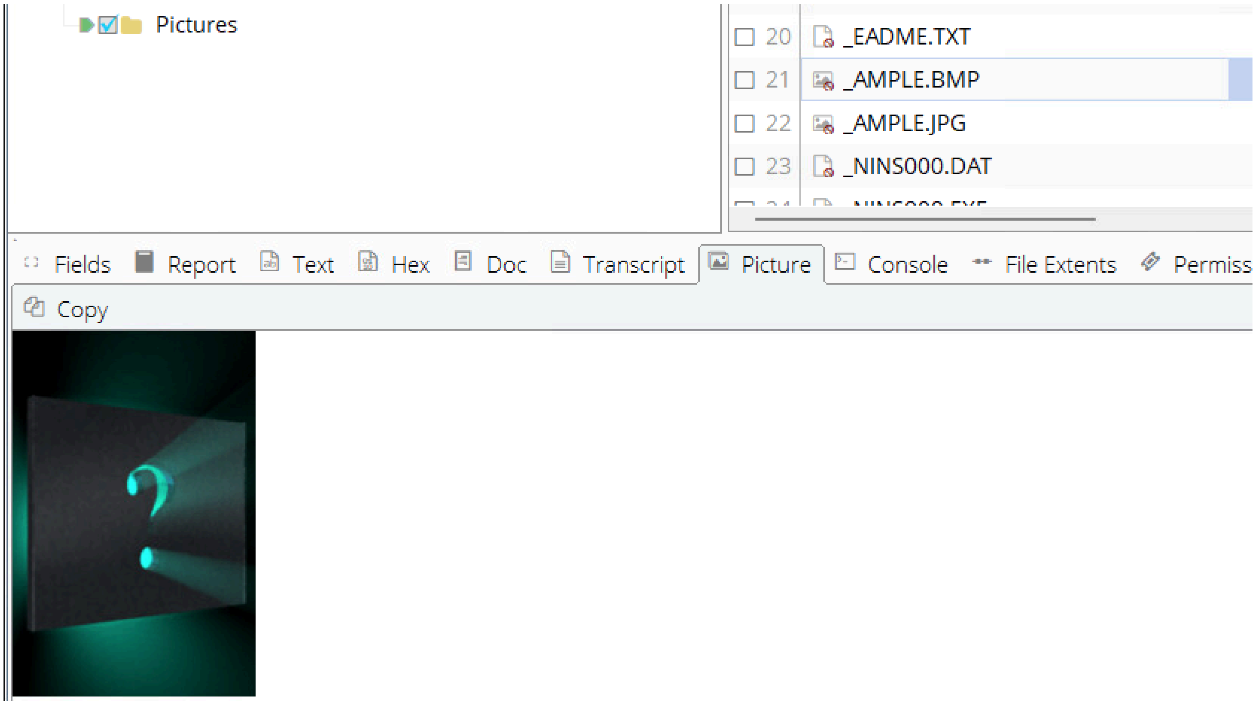
□ 11	algorithms		4,096	Folder
□ 12	_LOWFISH.DLL	DLL	69,120	Library
□ 13	_SECRETS.URL	URL	58	Windows
□ 14	isecrets2.cnt	cnt	628	Windows
□ 15	isecrets2.exe	exe	1,518,592	Executable
□ 16	isecrets2.hlp	hlp	20,893	Windows
□ 17	_ICENSE.TXT	TXT	8,621	Document

```
0000 [InternetShortcut]  URL=http://www.invisiblesecrets.com/
```



□ 21	_EADME.TXT	TXT	5,888	Document
□ 22	_AMPLE.BMP	B...	41,094	Picture
□ 23	_AMPLE.JPG	JPG	10,848	Picture

```
0000  Invisible Secrets 2.1, free edition    Copyright (c) 1999-2002 by Neobyte Solutions   All Rights Reserved.   www.invisiblesecrets.com       CONTENTS      1. Disclaimer
0172  2. What is Invisible Secrets?   3. What's New in This Version?   4. Contacting the Author          1. DISCLAIMER      (I) WARRANTY LIMITATIONS        THIS SOFTWARE AND THE
0344 ACCOMPANYING FILES ARE SOLD "AS IS" AND    WITHOUT WARRANTIES AS TO PERFORMANCE OR MERCHANTABILITY OR ANY OTHER    WARRANTIES WHETHER EXPRESSED OR IMPLIED. Because of the
0516 various    hardware and software environments into which Invisible Secrets    may be put, NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.     Good data processi
0688 ng procedure dictates that any program be    horoughly tested with non-critical data before relying on it.    The user must assume the entire risk of using the program.
0860 ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT    REPLACEMENT OR REFUND OF PURCHASE PRICE.       (II) CRYPTOGRAPHY RESTRICTIONS        WE ARE NOT LIABLE
1032  FOR ANY FORBIDDEN EXPORT,IMPORT, OR USE OF    "INVISIBLE SECRETS".        THE U.S. GOVERNMENT CLASSIFIES ENCRYPTION SOFTWARE AS DANGEROUS   MUNITIONS. ENCRYPTION SOFTWARE
1204 HAS RESTRICTIONS FOR EXPORT    ONLY FOR U.S. VENDORS. THERE ARE NO RESTRICTIONS ON IMPORTING    CRYPTOGRAPHIC PRODUCTS INTO THE U.S.        THE U.S. GOVERNMENT CLASSIFIES E
1376 NCRYPTION SOFTWARE AS DANGEROUS   MUNITIONS. ENCRYPTION SOFTWARE HAS RESTRICTIONS FOR EXPORT.   BECAUSE OF THE CRYPTOGRAPHY ALGORITHM IMPLEMENTED IN INVISIBLE   SECRETS IT
1548 IS REGARDED AS "STRONG CRYPTOGRAPHY".     THE UNREGISTERED VERSION OF THIS SOFTWARE RESTRICTS KEY LENGTH   TO ONLY 5 CHARACTERS (40-BITS). THEREFORE THE UNREGISTERED VERSIO
1720 N   OF INVISIBLE SECRETS IS RE-EXPORTABLE FROM THE U.S.     (III) JURISDICTION       This agreement shall be governed by the laws of Romania. Valid in   all questions of la
1892 w is the Romanian law and the Romanian   jurisdiction. All users of this software agree to the Romanian law   and the Romanian jurisdiction.       Any action or proceeding
2064 brought by anyone arising out of or related   to these terms and conditions shall be brought only in a court of    competent jurisdiction located in Oradea, Romania, and th
2236 e parties   hereby consent to the jurisdiction and venue of said court.     (IV) ACKNOWLEDGMENT        BY INSTALLING AND USING THIS SOFTWARE, YOU ARE AGREEING TO BE    BOUN
2408 D BY ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU    DO NOT AGREE TO THESE TERMS, PROMPTLY DESTROY ALL COPIES OF THE    SOFTWARE IN YOUR POSSESSION.     2. WHAT
2580 IS "INVISIBLE SECRETS 2"?       The only way to secure your data, and make it readable only to    authorized persons, is to use strong cryptography and a password    long
```



□ 20	_EADME.TXT
□ 21	_AMPLE.BMP
□ 22	_AMPLE.JPG
□ 23	_NINS000.DAT

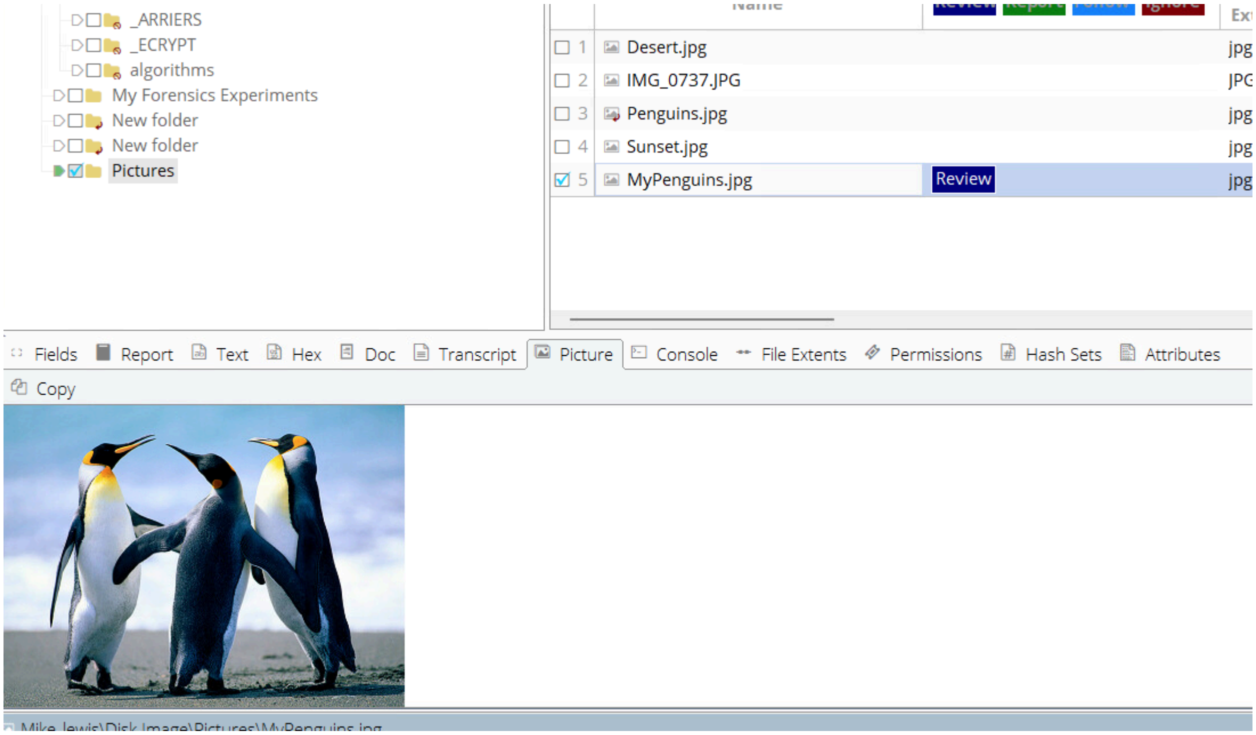
This image belongs to the invisible secrets installation image.

So we can see a bunch of invisible secrets files that talks briefly about invisible secrets in detail, add up to our evidence.

4.

Use the results from both 2) and 3) to identify the carrier file that hides the hidden password file. What is the carrier file's filename? (20 points)

The Carrier file that hides the hidden password is Pictures>MyPenguins.jpg

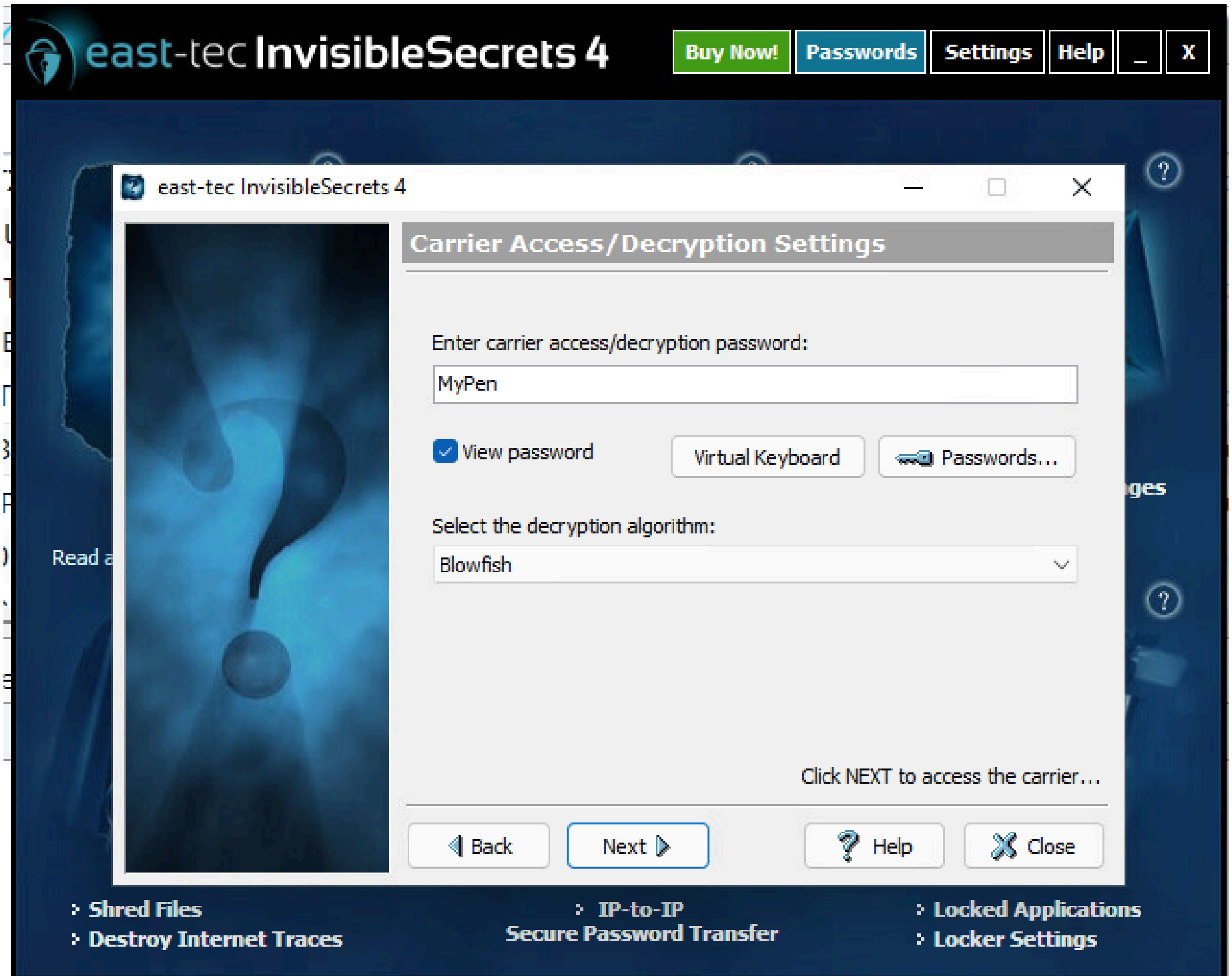


- ▷☐ _ARRIERS
- ▷☐ _ECRYPT
- ▷☐ algorithms
- ▷☐ My Forensics Experiments
- ▷☐ New folder
- ▷☐ New folder
- ▶☑ Pictures

		Name		Ext
☐	1	Desert.jpg		jpg
☐	2	IMG_0737.JPG		JPG
☐	3	Penguins.jpg		jpg
☐	4	Sunset.jpg		jpg
☑	5	MyPenguins.jpg	Review	jpg

Mike Lewis\Disk Image\Pictures\MyPenguins.jpg

5.
Use the crucial information you got from the previous steps to extract the hidden password file from the carrier file (Hint: choose “Blowfish” as the encryption/decryption algorithm). What is the hidden password file’s filename (provide a screenshot)? (20 points)

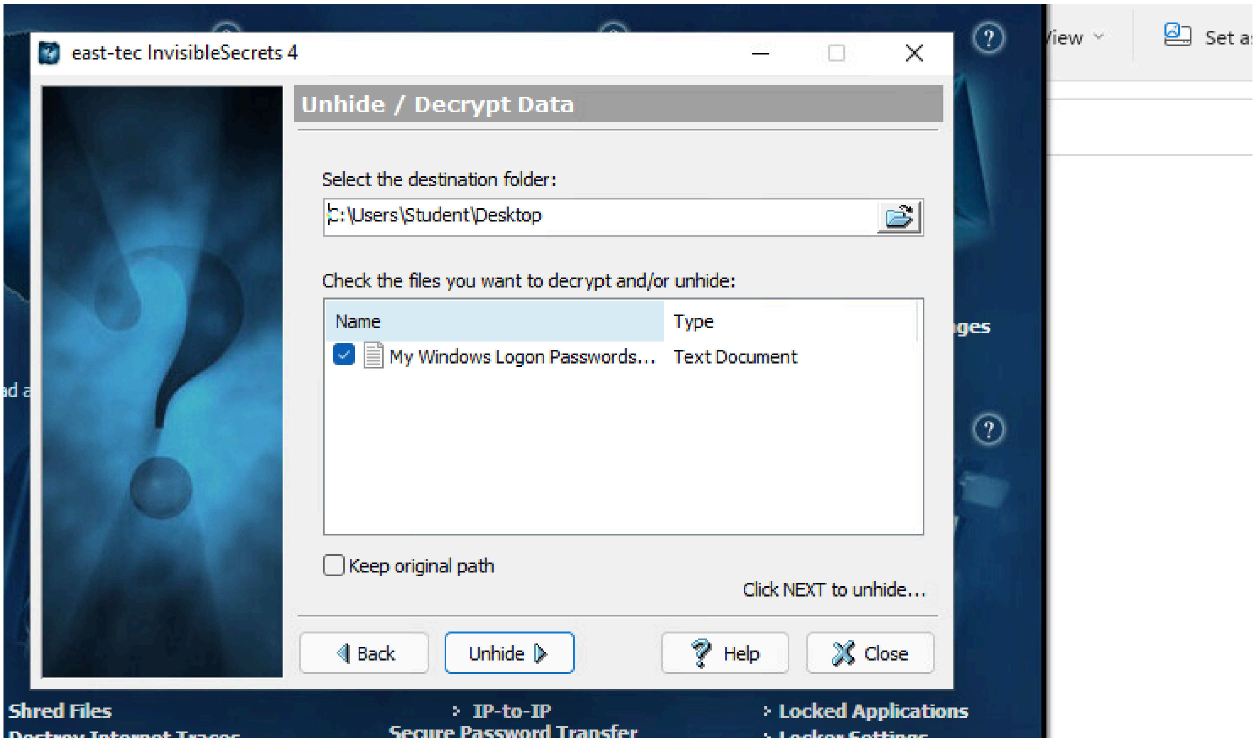


Enter carrier access/decryption password:
MyPen

☑ View password

Select the decryption algorithm:
Blowfish

Click NEXT to access the carrier...


east-tec InvisibleSecrets 4

Unhide / Decrypt Data

Select the destination folder:

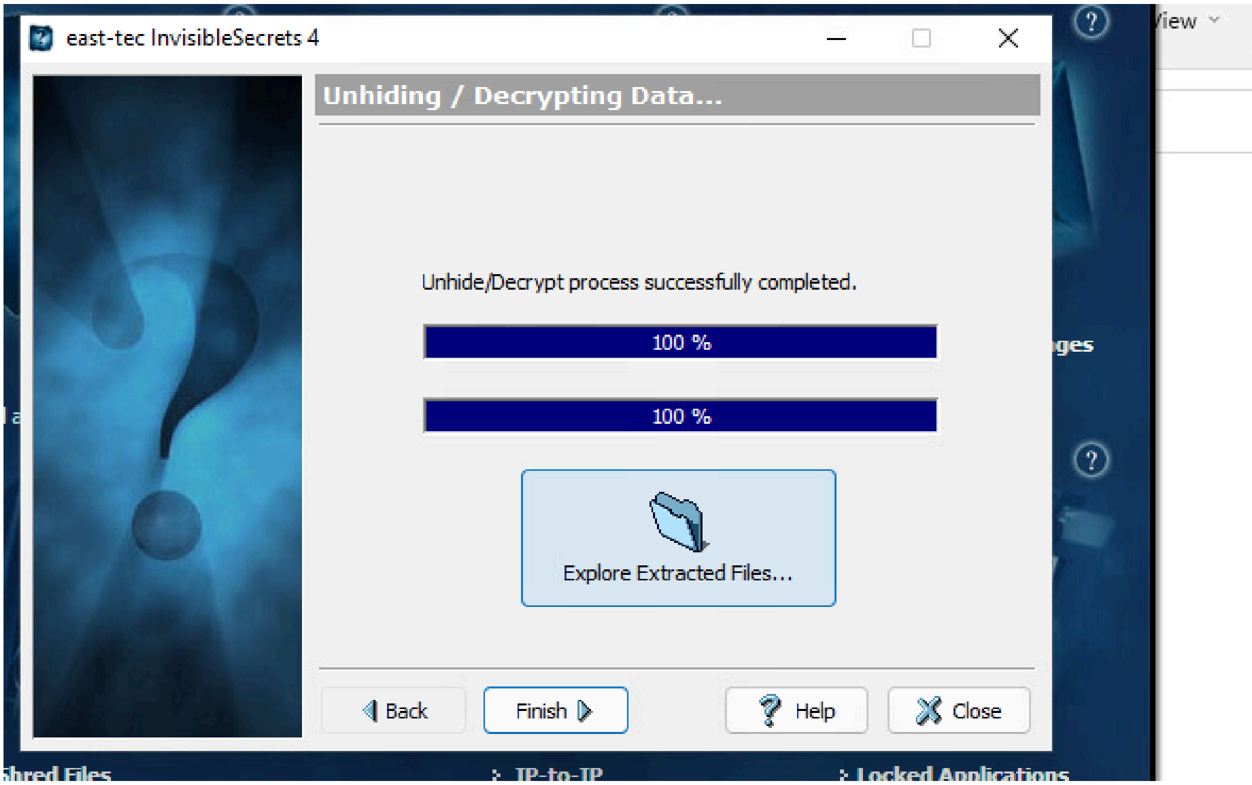
C:\Users\Student\Desktop

Check the files you want to decrypt and/or unhide:

Name	Type
☑ My Windows Logon Passwords...	Text Document

□ Keep original path

Click NEXT to unhide...


east-tec InvisibleSecrets 4

Unhiding / Decrypting Data...

Unhide/Decrypt process successfully completed.

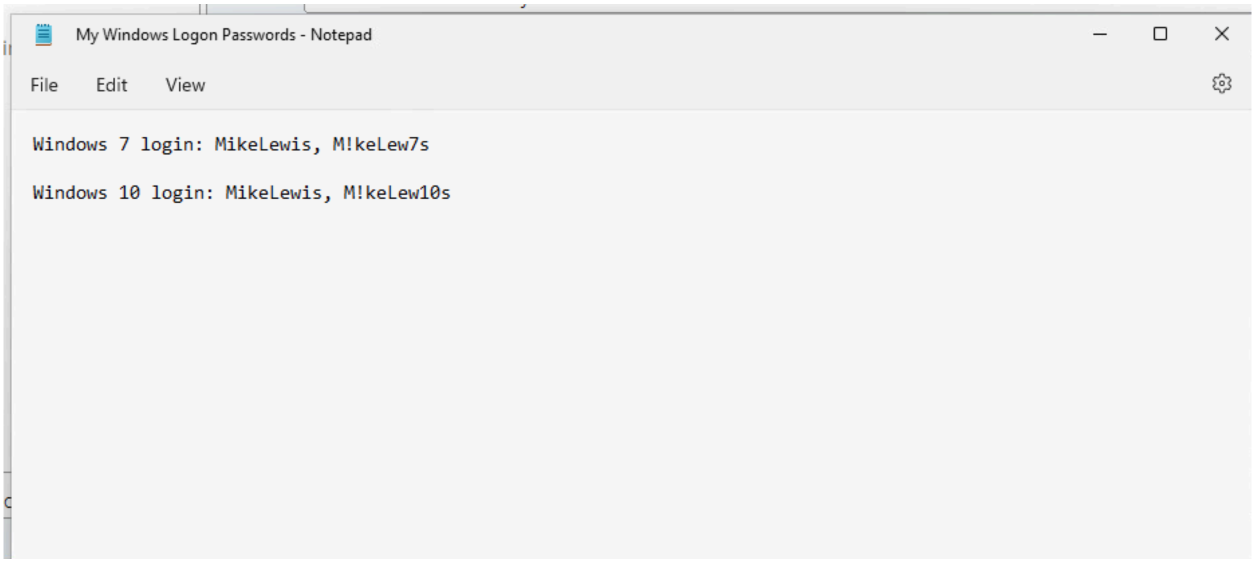
100 %

100 %

The filename of the hidden file is “My Windows Logon Passwords” and it is a Text Document.

6.
What are the username and password for Mike’s Windows login (provide a screenshot) ?
(10 points)

The Username and password extracted from the text file is



```
Windows 7 login: MikeLewis, M!keLew7s

Windows 10 login: MikeLewis, M!keLew10s
```

MikeLewis and Password is MikeLew7s
MikeLewis and Password is MikeLew10s