# **Module B4: Alternate Data Stream and Secret**

#### **Pre-requisite Knowledge and Skills:**

1. Understand the basic of NTFS File Systems

### **Learning Objectives**

1. Be familiar to Data hide techniques and alternation data stream technique.

### **Recommended Running Environment/Tools:**

- 1. Windows OS
- 2. AccessData FTK Imager
- 3. Forensic Toolkit 1.8.6.exe

### Material:

1. ADS Image.E01

# Video Lecture:

1. N/A

### Lab Assessment:

1. ADS Quiz

## Lab Instructions:

**Part I:** (create alternate data streams and prepare a small sized clean thumb drive). If students do not have thumb drive, just let demonstrate by the instructor.

Steps:

- 1. Plug in the thumb drive to user's computer.
- 2. Make sure the thumb drive file system is NTFS. If not, please choose a free thumb drive to format the thumb drive into NTFS system (Please refer to *Module 0 Lab* for details).
- 3. Open a command line prompt (run cmd.exe at run box or other approaches).
- 4. On the command line prompt, type notepad testfile.txt:secret1.txt.
- 5. When the windows states that it cannot find the file and ask you want to create it, click *YES*
- 6. Inside the data stream testfile.txt:secret1.txt, add "a first secret message"
- 7. From the file menu, click on save and then close the file

**Part II:** Examine the ADS file by using FTK Imager. (If students do not have thumb drive, just let demonstrate by the instructor.)

Steps:

- 1. Run FTK Imager Normal Alexandree State State
- 2. Click on file and select the add Evidence Item function (the 1st option)



- 3. Select physical drive option and click on next
- 4. Make sure to select the small-sized usb drive (note that your C drive usually is the default selection, please navigate the list to select the correct drive), and then click on finish

Select Drive	$\times$
Source Drive Selection	
Please select from the following available drives: [\\.PHYSICALDRIVE1 - General UDisk USB Device [IGB USB] (\.PHYSICALDRIVE0 - LITEON CV1-GB1024-11 SATA 1024GB [102 (\.PHYSICALDRIVE1 - General UDisk USB Device [IGB USB]	
< Back Finish Cancel Help	

5. Click on finish. Then navigate the disk image file and its file structure to locate the ADS file and its secret.

MaccessData FTK Imager 4.2.0.13				
<u>File View M</u> ode <u>H</u> elp				
4 4 4 4 4 2 2 2 2 6 3 1 2 2 2 2 6 3 1 2 2 2 2 2 -				
Evidence Tree ×	File List			
A QS Image E01     Jost Simage E01     Jost Simage E01     Jost Simage INTES     Jost Simage INTES     Jost Simage Intervention     Jost Simage Intervention	Name		Type Alternate	Date Mo 10/17/20
Hex Value Interpreter ×	]			
Type         Si         Value           signed int         1-8           unsigned i         1-8           FILETIME         8           DOS fare         2           DOS fare         2           time_f t(UT 4         4				
Byte order:   Little endian	a secret a	ds file		

6. Click on close to close the FTK Imager.

.

**Part III:** Create disk image file of the thumb drive with the ADS file by using FTK Imager. (If students do not have thumb drive, just let demonstrate by the instructor.)

Steps:

- 7. Run FTK Imager Werkender FK Imager 4.2.01 Werkender FK Werkender FK Verkender F
- 8. Click on file and select the create disk image function



- 9. Select physical drive option and click on next
- 10. Make sure to select the small-sized usb drive (note that your C drive usually is the default selection, please navigate the list to select the correct drive), and then click on finish

ource Drive Selection Please select from the following available drives:
\\PHYSICALDRIVE1 - General UDisk USB Device [1GB USB] V  \PHYSICALDRIVE0 - LITEON CV1-GB1024-11 SATA 1024GB [102
IVPHYSICALDRIVED - Effective Cyread 1024-11 SATA 1024GB [102 IVPHYSICALDRIVE1 - General UDisk USB Device [1GB USB]

11. On the new window, please click on the add option

mage Source		
(,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
	Starting Evidence Number: 1	
mage Destination(s)		
Add	Edit	Remove
Add	Edit Add Overflow Location	Remove
Add Verify images after the	Add Overflow Location	Remove rogress Statistics

12. Select the .e01 option (Encase format), or the .dd format (raw disk image, no meta data)

Select Image Type × Please Select the Destination Image Type ORaw (dd) SMART ©E01 AFF			
<ul> <li>○ Raw (dd)</li> <li>○ SMART</li> <li>④ E01</li> </ul>	5e	lect Image Type	$\times$
		○ Raw (dd) ○ SMART ④ E01	
< Back Next > Cancel Help		< Back Next > Cancel Help	

13. Click next, and then fill in the optional information, and then click next

Create Image		×
Evidence Item Informati	on	×
Case Number:	001	
Evidence Number:	001	
Unique Description:	to create ADS disk image file	
Examiner:	K12	
Notes:	an ADS test image	
<	Back Next > Cancel Help	

14. Choose the desired image file name (ADS Image, for example), and select the correct directory where the disk image file will be created.

Create Image X	
Select Image Destination	Browse For Folder
Image Destination Folder	Select the destination folder for the image
C:\Users\tu15\Desktop Browse	
Image Filename (Excluding Extension)	Desktop ^
ADS Image	> 🚡 Creative Cloud Files
	> 🝊 OneDrive
Image Fragment Size (MB) 1500 For Raw, E01, and AFF formats: 0 = do not fragment	> 瀺 Manghui Tu
Compression (0=None, 1=Fastest,, 9=Smallest) 6	> 🗢 This PC
Compression (o-mone, 1-hadese,, 5-similarese)	> 🐂 Libraries
Use AD Encryption	> 🥪 Forensics-Image (D:) 🗸 🗸
	Folder: Desktop
< Back Finish Cancel Help	Make New Folder OK Cancel
Start Cancel	

15. Click on finish

mage Source		
\\.\PHYSICALDRIVE1		
	Starting Evidence Number: 1	
mage Destination(s)		
C:\Users\tu15\Desktop\/	ADS Image [E01]	
Add	Edit	Remove
Add		Remove
Add	Edit Add Overflow Location	Remove
	Add Overflow Location	
Verify images after they	Add Overflow Location	ogress Statistics
Verify images after they	Add Overflow Location	ogress Statistics

16. Click on start option, you will create a disk image with extension E01, depends on the size of the disk, it could be a few minutes to hours.

Creating Image			-	$\times$
Image Source:	\\.\PHYSICALD	RIVE1		
Destination:	C:\Users\tu15\	Desktop\ADS Imag	e	
Status:	Creating image			
Progress				
	psed time: imated time left:	0:00:04		
		Cancel		

17. When finishing, it should look like what shown below. This will create disk creation report, and verify whether the hashes of the disk image and original disk are the same (if same, verified).

	1) IDENCICAL DOTING			
mage Source:	\\.\PHYSICALDRIVE1		Computed hash	5317600d21601ba735e7e107fff1fbe2
Destination:	C:\Users\tu15\Desktop\ADS Image	vith	Stored verification hash	5317600d21601ba735e7e107fff1fbe2
Status:	Image created successfully		Report Hash	5317600d21601ba735e7e107fff1fbe2
tatus:	Image created successiony		Verify result	Match
Progress			<sup>⊟</sup> SHA1 Hash	
			Computed hash	94f53ab03848408365b547e88fa7f00d7
			Stored verification hash	94f53ab03848408365b547e88fa7f00d7
Ela	psed time: 0:01:12		Report Hash	94f53ab03848408365b547e88fa7f00d7
	imated time left:		Verify result	Match
LSU	inateu une iert.		Bad Blocks List	
	ary Close		Bad block(s) in image	No bad blocks found in image

- 18. At the directory, you will find two files, ADS Image.e01 (disk image file) and ADS Image.E01.txt (verification file)
- 19. Click on close and return to the FTK imager.
- 20. Select the file and click the add evidence option



21. On the new pop-up window, select the image file option (not the default option), then next, and browse to the newly created ADS Image.E01 (not the txt file)

Select File	X Open	×
	$\leftarrow \rightarrow \checkmark \uparrow \blacksquare \Rightarrow \text{This PC} \Rightarrow \text{Desktop} \Rightarrow \checkmark \heartsuit \text{Search Desktop}$	op 🖉
Evidence Source Selection	Organize - New folder	II • 🔳 🕜
Please enter the source path:	S This PC Name	Date modifi
C:\Users\tu15\Desktop\ADS Image.E01	3D Objects ADS Image.E01.txt	6/3/2019 1:
	Desktop ADS Image.E01	6/3/2019 1:
Browse_	Documents	pdf 5/10/2019 5
	L Downloads	>
	File name: ADS Image.E01 ~ All Files (*.*) Open	✓ Cancel
<back cancel="" finish="" he<="" th=""><td></td><td></td></back>		

22. Then click on open and finish. Then navigate the disk image file and its file structure to locate the ADS file and its secret.

🛃 AccessData FTK Image	er 4.2.0.13							
<u>File View M</u> ode <u>H</u> elp								
<b>3) 5)</b> € ≙ <b>6</b> ] 🖂 🖓 6	a = = 🖬 📴	९ 🗈 🖻 🖹 🐱 😹 🔋 .	J					
vidence Tree				×	File List			
A ADS image E01     Forensic-image [N1     Forensic-image [N1	f a Information				Name		Type Alternate	Date Mo 10/17/20
lex Value Interpreter				×				
ype [3] value signed int 1-8 nusigned it 1-8 FILETIME 8 FILETIME 8 DOS date 2 DOS time 2 DOS time 2 time_t (UC 4								
					a secret ad	s file		

Part IV (FTK 1 ADS File Analysis by using the image file provided)

Creating a new case by using FTK 1.8.6. start by run 1.8.6 from your computer by right click the FTK1.8.6 program icon, then choose the "**run as administrator**" option. after that, select the no to run FTK in **Demo mode** (no license), click ok to accept demo mode, and then start new case.

Run with graphics processor	>			AccessData FTK		X
Open file location				AccessData FTK		^
Run as administrator Troubleshoot compatibility				Thank you for evaluating A a demonstration	ccessData's Forensic Toolkit® (FT)	(®). This is
Pin to Start				version of FTK. The followin	g limitation is in effect:	
7-Zip	>			• A maximum of 50	100 file items can be analyzed	
CRC SHA	>				Ill version of FTK, please contact A	ccessData
Edit with Notepad++				at 800-574-5199 or 801-377 or visit our website at http:		
Scan selected items for viruses						
Identity Finder Endpoint	>	Error	Х			ОК
Upload to MEGA			No security device was found. Would you like to specify a			UN .
MagiclSO		<u> </u>	location for a network security device?			
Pin to taskbar			Yes to continue or No to run FTK in demo mode.		-	
Scan with Malwarebytes Anti-Malware	-		Yes No	AccessData FTK Startup	*	×
Restore previous versions	-			First, Organize, & Analyze Computer Evidence	Start a new case Open an existing case	OK
Send to	>				O Preview evidence	Cancel
Cut	-			Forensic Toolkit	Go directly to working in prog	ram
Сору				Ganity and Easy TOOIRit"		
Create shortcut	-				Do not show this dialog on st	artup
Delete						
Rename						

#### Steps:

1. Create a FTK New Case

	Expl	ore Graphics	5	E-Mail	Searc	h Bookmark		
Evidenc	eltems	File Status		File Category		.n n	🔂 हिंस निर्दे 💝 क	ରି ଜ
vidence Iten	ms: 0	KFF Alert Files:	0	Documents:	0			E E
File I	tems	Bookmarked Items:	0	Spreadsheets:	0			
tal File Item	ns: 0	Bad Extension:	0	Databases:	0			975
hecked Item	ns: 0	Encrypted Files:	0	Graphics:	0	New Case		×
nchecked It	ems: 0	From E-mail:	0	Multimedia:	0			
agged Thur	mbnails: 0	Deleted Files:	0	E-mail Messages:	0	Find, Organize, & Analyze Computer Evide		AccessData's
ther Thumb	nails: 0	From Recycle Bin:	0	Executables:	0			
itered in:	0	Duplicate Items:	0	Archives:	0			Forensic Toolkit®-FTK®
itered Out:	0	OLE Subitems:	0	Folders:	0		Z	The Complete Analysis Tool
Infiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0	Forensic V		The complete maryona room
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0	Pred Computer Codesce Toolkit	•	Wizard for Creating a New Case
	e F Evider			V III	Evide	Case Information		101
	1							
	1						Case Name:	nessier
	1							nessier
	1					inc	Case Name:	Ressier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	Ressier Browse
	1					inc	Case Name: n Case Path: c Case Folder: c	Ressier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse
	1					nc Case Description:	Case Name: n Case Path: c Case Folder: c	essier Browse

2. In the Case Log Options window, leave all options marked.

Case Log Options	:	$\times$
c	ase Log Options	
	e case folder. It gets created automatically by FTK and contains a record of e. You can choose which type of events you would like to be logged.	
	og file at any time by selecting "Add Case Log Entry" under the "Tools" lecting "View Case Log" under the "Tools" menu item.	
Events to go in the Case Log		
Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.	
Error messages	Events related to any error conditions encountered during the case.	
	Events related to the addition and modification of bookmarks.	
Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.	
Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.	
Other events	Other events not related to the above, such as copying, viewing, and ignoring files.	
		_
	< Back Next > Cancel	

3. In the Evidence Processing Options window, mark all the options except SHAI Hash, Data Carving, and HTML File Listing.  $\times$ 

Evidence Processing Options

	case in several steps. Some of the processes are always performed, while others are optional, ds and time/resource constraints.
MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not vet as widely used.
KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index	The Forensic Toolkit includes a very powerful search engine, dt Search, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing	Create a Microsoft Access (Jet) database containing a list of all files in
Database	the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing	Create an HTML version of the File Listing.
Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Registry Reports -	Generate common registry reports during preprocessing.

4. In the Refine Case and Refine Index default window, don't make any changes.

Refine Case - Default	×
Refine Case - Defa In order to save time and resources, and/or to eliminate irrelevant data, you n from the case. Here, you can choose default inclusion/exclusion settings tha added to the case. To exclude data, make any changes to the settings below appear anywhere in the case, and will be inaccessible.	nay choose to exclude certain kinds of data t will apply to each evidence item that gets
Include All Items Optimal Settings Email Emphasis	Text Emphasis Graphics Emphasis
Unconditionally Add	
File Slack (data beyond the end of the logical file but within the area all     Free Space (areas in the file system not currently allocated to any file, b     KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e     Extract files from KFF ignorable containers	ut possibly containing deleted file data)
Conditionally Add	
Add other items to the case only if they satisfy BOTH the file status and t	he file type 🗸 criteria
	Type Criteria
Deletion Status:       Encryption Status:       Email Status:       Imail Status:         O Deleted       O Encrypted       O From email       Imail Status:         O Not deleted       O Not encrypted       O Not from email       Imail Status:         Imail Status:       Imail Status:       Imail Status:       Imail Status:	Jocuments Spreadsheets Archives Databases Graphics Multimedia Email msgs
Refine Index - Default <b>Refine Index - Default</b> In order to save time and resources, and/or to make searching more ef data from being indexed. Here, you can choose default settings that wi case. To exclude items from being indexed, make any changes to the i initially can be indexed later by clicking on "Analysis Tools" under the '	ficient, you may choose to exclude certain kinds of ill apply to each evidence item that gets added to the
initially can be indexed later by clicking on "Analysis Tools" under the ' Unconditionally Index	'Tools'' menu item.
File Slack (data beyond the end of the logical file but within the ar	rea allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any KFF Ignorable Files (files found by KFF to be forensically unimport)	
Conditionally Index	
Index other items in the case only if they satisfy BOTH the file statu	us and the file type $\checkmark$ criteria
File Status Criteria	File Type Criteria
Deletion Status:       Encryption Status:       Email Status:         Deleted       Encrypted       From email         Not deleted       Not encrypted       Not from email         Ether       Ether       Ether	Documents     Executables       Spreadsheets     Archives       Databases     Folders       Graphics     Other Known
✓ Include Duplicate Files ✓ OLE Streams	☑ Multimedia ☑ Unknown ☑ Email msgs
	< Back Next > Cancel

5. In the Add Evidence to Case window, click Add Evidence. Add case image from your drive with acquired image of drive option in our case. we need to download the image before we add the image file to the FTK.

Add Evidence to Case						$\times$
	A	dd Evid	lence			
Any number of evidence iter	ms can be added to the	case. There a	are several type	s of evidence	ce items:	
Acquired image of o	drive: Several formats s Can be a logical of			f a logical or	physical drive	
Folder:	Adds all files in th			ontents of s	ubfolders	
Individual File:	Adds a single file.		-			-
The default refinement optio types of refinements can als folders. To make these furth	o be made. These refine	ements can in	clude the exclusion	sion of date	/size ranges, a	is well as specific
Add Evidence	Edit Evidence	Remo	ove Evidence	Ref	ine Evidence -	Advanced
Display Name	Source	Name/Nu	Туре	Refined	Time Zone	Comment
	Add Evidenc	e to Case		$\times$		
	Type of Ev	idence to Ado	d to Case			
	💿 Acquir	ed Image of D	rive			
	◯ Local I	Drive				
	◯ Conter	nts of a Folder				
	Individ	ual File				
		Continue.	Ca	incel		
				Deals	New 4 N	Connel
			<	Back	Next >	Cancel

6. Select the evidence item, *ADS Image.E01*.(you can navigate to the directory following the file open dialog within the FTK tool after you click on the *continue* button)

🗞 Open ← → → ↑ 📙 « Cyb	e > Module B4 Secret M → Ö	Search Module B4 Secret	× م Mes ک
Organize 👻 New folder			
Program Study ^	Name	Date modified	Туре
a OneDrive	ADS Image.E01	6/3/2019 1:08 AM	E01 File
	ADS Image.E01.txt	6/3/2019 1:08 AM	Text Docum
💻 This PC	Module B4-ADS Lab.docx	6/4/2019 11:56 PM	Microsoft V
3D Objects	Module B4-ADS Quiz.txt	7/14/2018 11:43 AM	Text Docum
Desktop	😰 Secure Message-Alaternate Data Stream.	6/3/2019 12:12 AM	Microsoft P
Documents			
🖊 Downloads			
Music			
E Pictures			
📑 Videos			
띀 OS (C:)			
- Makaal	c		>
File na	me: ADS Image.E01 ~	All Files (*.*)	~
		Open 🔽 🔘	Cancel

7. The ADS Image Case will be processed as shown below.

	Explo	ore Graphics		E-Mail	Sear	h Bookmark					
Evidenc	e Items	File Status		File Categor	у	, <b>m</b> ~	M, 74	• 🐺 🛗 🙀 •	ົວງ 🥔		
Evidence Item	ns: 1	KFF Alert Files:	0	Documents:	8						
File It	tems	Bookmarked Items:	0	Spreadsheets:	0						
Total File Item	s: 108	Bad Extension:	0	Databases:	0						
Checked Item	s: 0	Encrypted Files:	0	Graphics:	9						
Unchecked It	ems: 108	From E-mail:	0	Multimedia:	0						
Flagged Thun	nbnails: 0	Deleted Files:	4	E-mail Messages:	0						
Other Thumb	nails: 9	From Recycle Bin:	0	Executables:	0						
Filtered In:	0	Duplicate Items:	0	Archives:	0						
Filtered Out:	108	OLE Subitems:	0	Folders:	8						
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	38						
All Items	Actual Files	KFF Ignorable:	1	Other Known Type:	2						
		Data Carved Files:	0	Unknown Type:	43						
						<					
	<i>4</i> 🍖 📑	🗄 🗋 🐳 🏧 Encryp	ted Fil	les v	Defau	It File List Column Se $ \smallsetminus $	DTZ				
	e F Evider	nce Path Display N	lame	Identification	Evid	ence Type Added		Children	Descendants	Investigator's	Comment

Overview	Explo	ore Graphics		E-Mail	Search	h Bookmark						
Evidence	tems	File Status		File Category	1	.n n	, be 🚔 🖽 🖼 🚱 🗿 🍕					
vidence Items	s: 1	KFF Alert Files:	0	Documents:	8							
File Ite	ems	Bookmarked Items:	0	Spreadsheets:	0	a secret ads file						
otal File Items:	: 108	Bad Extension:	0	Databases:	0							
hecked Items:	s: 0	Encrypted Files:	0	Graphics:	9							
nchecked Iten	ms: 108	From E-mail:	0	Multimedia:	0							
lagged Thumb	bnails: 0	Deleted Files:	4	E-mail Messages:	0							
ther Thumbna	ails: 9	From Recycle Bin:	0	Executables:	0							
tered In:	0	Duplicate Items:	0	Archives:	0							
itered Out:	108	OLE Subitems:	0	Folders:	8							
Infiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	38							
All Items	Actual Files	KFF Ignorable:	1	Other Known Type:	2							
_												
		Data Carved Files:	0	Unknown Type:	43							
						¢						
	<i>4</i> 8 🍫 B3	Data Carved Files:				د T File List Column Se کار	2					
	<i>6</i> € ♦ ]33					< t File List Column Se ∽    D1	2	🐮 File Name	Ext	File Type	Cr Date	Acc
ull Path ] 📄 ADS Im	nage\Forensic	D 💱 🚾 Encry	ted Fi	es v] [[]		< t File List Column Se √ D1	2	▼ File Name Document1.bt	Ext	File Type Plain Text Document	Cr Date 2/3/2018	
ull Path ] 📄 ADS Im	nage\Forensic	D 💱 🚾 Encry	ted Fi	es v] [[]		د t Fie List Column Se ح	2					. 2/3
ull Path ADS Im ADS Im ADS Im	nage\Forensic nage\Forensic nage\Forensic	s-Image-NTFS\Passwo s-Image-NTFS\Passwo s-Image-NTFS\IPteLetA2	ted Fi d Stuff xt 13474	es    [1]	Default	5].jpg.htm	2	Document1.txt filetext2.txt JPEG_11347446[65].jpg.htm	tst	Plain Text Document Plain Text Document Hypertext Document	2/3/2018 2/3/2018 N/A	2/3 2/3 N/A
ull Path ADS Im ADS Im ADS Im ADS Im	nage\Forensic nage\Forensic nage\Forensic nage\Forensic	s-Image-NTFS\Passwo s-Image-NTFS\Pietex42 s-Image-NTFS\VIEtex12 s-Image-NTFS\VIEtex12	ted Fi d Stuff xt 13474	es ~ 111 \Document1.txt 16(65).jog>.JPE.6_113	Default	5].jpg.htm	z	Document1.bt filetext2.bt JPEG_11347446[65].jpg.htm JPEG_19622246[65].jpg.htm	tst tst htm htm	Plain Text Document Plain Text Document Hypertext Document Hypertext Document	2/3/2018 2/3/2018 N/A N/A	2/3 2/3 N//
ull Path ADS Im	nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic	s-Image-NTFS UP asswo s-Image-NTFS UP asswo s-Image-NTFS UPE6_1 s-Image-NTFS UPE6_1 s-Image-NTFS UPE6_1 s-Image-NTFS UPE6_1	ted Fi d Stuff xt 3474 96222 t Doc	es    [1] \Document1.bt (6(65).jpp>.VPE6_113 (6(65).jpp>.VPE6_196	Default	5].jpg.htm	2	Document1.bxt filetext2.txt JPEG_11347446(65).jpg.htm JPEG_19622246(65).jpg.htm New Text Document.txt	txt txt htm htm txt	Plain Text Document Plain Text Document Hypertext Document Hypertext Document Plain Text Document	2/3/2018 2/3/2018 N/A N/A 2/3/2018	2/3 2/3 N// N// 2/3
Ull Path ADS Im ADS Im ADS Im ADS Im ADS Im ADS Im ADS Im	nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic	sImageNTFSVPasswo sImageNTFSVPasswo ImageNTFSVPE0_1 sImageNTFSVPE0_1 sImageNTFSVPE0_1 sImageNTFSVPE0_1	ted Fi d Stuff xt 13474 406222 t Doc	es    [1] VDocument1.bt K6[65].jpg>.VPE6_113 K6[55].jpg>.VPE6_136 ument.bt	Default	5].jpg.htm	2	Document1.txt filetext2.txt JPE6_11347446(65),jpg.htm JPE6_19622246(65),jpg.htm New Text Document.txt secret.txt	txt txt htm htm txt	Plain Text Document Plain Text Document Hypertext Document Hypertext Document Plain Text Document Plain Text Document	2/3/2018 2/3/2018 N/A N/A 2/3/2018 2/3/2018	2/3 2/3 N/A N/A 2/3
ADS Im ADS Im ADS Im ADS Im ADS Im ADS Im ADS Im ADS Im ADS Im	nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic	Image NTFS VPasswo Image NTFS VPasswo Image NTFS VPEG_1 Image NTFS VPEG_1 Image NTFS VPEG_1 Image NTFS VWeT In Image NTFS VWeT In Image NTFS VWeT In	ted Fi d Stuff 3474 3474 16222 t Doc: t Doc: t Second	es    [1] VDocument1.bt K6[65].jpg>.VPE6_113 K6[55].jpg>.VPE6_136 ument.bt	Default	5].jpg.htm	2	Document1.txt filetex42.txt JPE6_11347446(65),jpg.htm JPE6_13622246(65),jpg.htm New Text Document.txt secret.txt secret.txt	txt txt htm htm txt txt	Plain Text Document Plain Text Document Hypertext Document Hypertext Document Plain Text Document Plain Text Document Plain Text Document	2/3/2018 2/3/2018 N/A N/A 2/3/2018 2/3/2018 2/3/2018	2/3 2/3 N// 2/3 2/3 2/3 2/3
III Path           ADS Im           ADS Im	nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic nage\Forensic	sImageNTFSVPasswo sImageNTFSVPasswo ImageNTFSVPE0_1 sImageNTFSVPE0_1 sImageNTFSVPE0_1 sImageNTFSVPE0_1	ted Fi d Stuff 3474 3474 16222 t Doc: t Doc: t Second	es    [1] VDocument1.bt K6[65].jpg>.VPE6_113 K6[55].jpg>.VPE6_136	Default	5].jpg.htm	2	Document1.txt filetext2.txt JPE6_11347446(65),jpg.htm JPE6_19622246(65),jpg.htm New Text Document.txt secret.txt	txt txt htm htm txt	Plain Text Document Plain Text Document Hypertext Document Hypertext Document Plain Text Document Plain Text Document	2/3/2018 2/3/2018 N/A N/A 2/3/2018 2/3/2018	2/3 2/3 N/2 2/3 2/3 2/3

9. Then navigate files and please pay attention to the two ADS files and the secret messages.