# **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:	
IVPHYSICALDRIVE1 - General UDisk USB Device [1GB USB] IVPHYSICALDRIVE0 - LITEON CV1-GB 1024-11 SATA 1024GB [102 IVPHYSICALDRIVE1 - General UDisk USB Device [1GB 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.

AccessData FTK Imager 4.2.0.13					
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp					
<b>4 4</b> € 4 <b>4</b>   2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	🐱 🗃 🐮 🥊 🖕				
Evidence Tree		×	File List		
ADS Image.E01			Name	Size Type	Date Mo
Protestacs-sinage (vir Fs)     Grophan)     Grophan)     Grophan)     Saddus     Secure     SupCase     SupCa			secret.txt	1 Alter	nate 10/17/20
Hex Value Interpreter		×	1		
Type         Si         Value           signed int         1-8           unsigned L         148           FILETIME         8           FILETIME         8           DOS three         2           DOS three         2           time_t(UT			a secret ads	file	
Byte order: () Little end	dian	O Big endian	_		

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

Please select from the following available drives:
III./PHYSICALDRIVE1 - General UDisk USB Device [1GB USB]
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

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

5e	lect Image Type	$\times$	
	Please Select the Destination Image Type Raw (dd) SMART © E01 AFF		
	< 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 ×	
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
For Raw, E01, and AFF formats: 0 = do not fragment	> 瀺 Manghui Tu
Compression (0-None 1-Eastert 0-Smallert) 6	> 🗢 This PC
Compression (0-None, 1-rastest,, 9-Smallest)	> 🐂 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	Edit	Remove
Add	Edit Add Overflow Location	Remove
Add	Edit Add Overflow Location	Remove
Add	Edit Add Overflow Location are created Precalculate Pre-	Remove ogress Statistics
Add Verify images after they Create directory listings	Edit Add Overflow Location v are created Precalculate Pro of all files in the image after they are	Remove ogress Statistics e created
Add ] Verify images after they ] Create directory listing	Edit Add Overflow Location v are created Precalculate Pro of all files in the image after they are	Remove ogress Statistics e created

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 Image	•	
Status:	Creating image			
Progress				
Ela Est	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).

creating image		~	Diveringe verity results	
Image Source:	\\.\PHYSICALDRIVE1		Computed hash	5317600d21601ba735e7e107fff1fbe2
Destination:	C:\Users\tu15\Desktop\ADS Image	uith	Stored verification hash	5317600d21601ba735e7e107fff1fbe2
	Yese exampled example disc		Report Hash	5317600d21601ba735e7e107fff1fbe2
status:	Image created successfully		Verify result	Match
Progress			<sup>⊟</sup> SHA1 Hash	
			Computed hash	94f53ab03848408365b547e88fa7f00d70
			Stored verification hash	94f53ab03848408365b547e88fa7f00d70
Ela	osed time: 0:01:12		Report Hash	94f53ab03848408365b547e88fa7f00d70
Ect	mated time left:		Verify result	Match
LSU	indeed unite ferc.		Bad Blocks List	
	ct		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	Open 🛃	×
	$\leftarrow \rightarrow \checkmark \uparrow \blacksquare \Rightarrow \text{This PC} \Rightarrow \text{Desktop} \Rightarrow \checkmark \heartsuit \text{Search Desktop}$	Q
Evidence Source Selection	Organize • New folder	• 🔳 🕐
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	5/10/2019 5
	L Downloads V <	>
	File name: ADS Image.E01 ~ All Files (*.*) Open	∼ Cancel
< Back Finish Cancel Help	i	

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>F</u> ile <u>V</u> iew <u>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	rFS] f e Information e]				Name	Size 1	Type Alternate	Date Mo 10/17/20
lex Value Interpreter				×				
ype [3] value signed int 1-8 singned i 1-8 FILETIME 8 FILETIME 8 DOS date 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	>			A Data ETK		~
Open file location				AccessData FTK		^
🗣 Run as administrator				Thank you for evaluating A	ccessData's Forensic Toolkit® (FTK®). Thi	s is
Troubleshoot compatibility				a demonstration version of FTK. The followin	a limitation is in effect	
Pin to Start					ig initiation is in criteri	
7-Zip	>			A maximum of 50	000 file items can be analyzed	
CRC SHA	>			If you wish to purchase a fu	ull version of FTK, please contact AccessD	ata
Edit with Notepad++				or visit our website at http:	//www.accessdata.com.	
4 Scan selected items for viruses						
Identity Finder Endpoint	>	Error	×			v
Upload to MEGA			No security device was found. Would you like to specify a			×
<ul> <li>MagicISO</li> </ul>	- <b>-</b> /	· /	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	7	×
Restore previous versions	-			Find, Organize, & Analyze Computer Evidence	Start a new case	)K
Send to	>				O Open an existing case O Preview evidence	ncel
Cut	-			Forensic	Go directly to working in program	
Conv				Camp out tony Toolkit'		
	-				Do not show this dialog on startup	
Create shortcut						
Delete						
Rename						

#### Steps:

.

1. Create a FTK New Case

Evidence vidence Items		re Graphics	E-Mail	Search	Bookmark			
vidence Items	Items	File Status	File Category		~ A	<b>be 22 and 22 and 23</b>	ା ମି ଜୀ	
	s: 0	KFF Alert Files:	0 Documents:	0				
File Ite	ems	Bookmarked Items:	0 Spreadsheets:	0				
otal File Items	: 0	Bad Extension:	0 Databases:	0				
hecked Items	i: 0	Encrypted Files:	0 Graphics:	0	Vew Case			×
hchecked Ite	ms: 0	From E-mail:	0 Multimedia:	0				
agged Thum	bnails: 0	Deleted Files:	0 E-mail Messages:	0	Find, Organize, & Analyze Computer Ex	Idence	Access Data's	
ther Thumbn	ails: 0	From Recycle Bin:	0 Executables:	0			AccessData s	
tered In:	0	Duplicate Items:	0 Archives:	0			Forensic Toolkit®-FTK®	
tered Out:	0	OLE Subitems:	0 Folders:	0			The Complete Analysis Tool	
Infiltered	Filtered	Flagged Ignore:	0 Slack/Free Space:	0	Forensic V			
All Items	Actual Files	KFF Ignorable:	0 Other Known Type:	0	Carley and Easy Toolk	t'		
				·		Case Path:	c:\Browse	
						Case Path:	C:\ Browse	
						Case Folder	c'messier	- i
					Case Description:	odde i older.		
					Lab 01 Working with	n FTK	^	
							~	
							8	*
							8	·
							N	<u>.</u>

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

Case Log Options		$\times$
c	Case Log Options	
The case log is a text file named FTK.log in the events that occur during the course of the cas	e case folder. It gets created automatically by FTK and contains a record of se. You can choose which type of events you would like to be logged.	
You can also add your own comments to the lo menu item, and you can view the log file by se	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

vidence is added to a epending on your nee	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.
d Desister Deserts	Generate common registry reports during preprocessing

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

Refine Case - Default			×
Refir In order to save time and resources, and/or to elim from the case. Here, you can choose default inclu added to the case. To exclude data, make any ch appear anywhere in the case, and will be inaccess	ne Case - Defininate irrelevant data, you ision/exclusion settings that anges to the settings belo sible.	ault may choose to exclude cent at will apply to each eviden w. Note: any items that get	tain kinds of data ce item that gets excluded will not
Include All Items Optimal Settings	Email Emphasis	Text Emphasis	araphics Emphasis
Unconditionally Add			
<ul> <li>File Slack (data beyond the end of the logical</li> <li>Free Space (areas in the file system not curred</li> <li>KFF Ignorable Files (files found by KFF to be</li> <li>Extract files from KFF ignorable containers</li> </ul>	al file but within the area al ently allocated to any file, t forensically unimportant, i.	located to that file by the file but possibly containing dele .e., OS system files, known	e system) ted file data) applications, etc.)
Conditionally Add			
Add other items to the case only if they satisfy	BOTH the file status and	the file type 🗸 criteria	
File Status Criteria	File	Type Criteria	
Deletion Status:       Encryption Status:       Email         ○ Deleted       ○ Encrypted       ○ f         ○ Not deleted       ○ Not encrypted       ○ f         ● Ether       ● Ether       ● f         ☑ Include Duplicate Files       ☑ 0	il Status: 2 From email 2 Not from email 2 Ether 2 LE Streams 2 1 1 1 1 1 1 1 1 1 1 1 1 1	Documents      Exe     Spreadsheets      Arci     Databases      Fold     Graphics      Oth     Multimedia      Unk	cutables hives ders er Known cnown
Refine Index - Default Ref In order to save time and resources, and/or to data from being indexed. Here, you can choos case. To exclude items from being indexed m initially can be indexed fare by clicking on "An	fine Index - I make searching more e se default settings that w ake any changes to the alysis Tools" under the	Default fficient, you may choose vill apply to each evidence settings below. Note: any "Tools" menu item.	to exclude certain kinds of e item that gets added to the y items that don't get indexed
	-		
File Slack (data beyond the end of the lo	gical file but within the a	area allocated to that file t	by the file system)
Free Space (areas in the file system not on KFF Ignorable Files (files found by KFF to	- currently allocated to any be forensically unimpor	y file, but possibly contain tant, i.e., OS system files,	ing deleted file data) known applications, etc.)
Conditionally Index			
Index other items in the case only if they sa	tisfy BOTH the file stat	us and the file type $\!$	criteria
File Status Criteria		File Type Criteria	
Deletion Status: Encryption Status: I Deleted Encrypted Not deleted Not encrypted Either Either Include Duplicate Files	Email Status: O From email O Not from email Ether OLE Streams	<ul> <li>Documents</li> <li>Spreadsheets</li> <li>Databases</li> <li>Graphics</li> <li>Multimedia</li> <li>Email msgs</li> </ul>	<ul> <li>Executables</li> <li>Archives</li> <li>Folders</li> <li>Other Known</li> <li>Unknown</li> </ul>
		< 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						$\times$
	Α	dd Evic	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	upported; can	be an image of	a logical or	physical drive	
Folder:	Adds all files in th	e specified fol	/e der. including c	ontents of s	ubfolders	
Individual File:	Adds a single file	NOTE: Disk	image files show	uld be adde	d as acquired i	mages.
The default refinement optio types of refinements can als folders. To make these furth	ns, set previously, can o be made. These refin er refinements, highligh	be overridden ements can in t an evidence	independently f clude the exclu- item in the list a	for each evi sion of date ind press Re	dence item, an /size ranges, a efine Evidence	nd additional as well as specific - Advanced
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 Ex	vidence to Ad	d to Case			
	💿 Acquir	ed Image of D	rive			
	O Local	Drive				
	◯ Conte	nts of a Folder				
		lual File				
		Continue	Ca	incel		
				Deals	Marchin	Connel
			<	васк	IVEXT >	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			×
← → × ↑ 🔤 « Cy	ybe > Module B4 Secret M v さ	Search Module B4 Secret	Mes , <b>P</b>
Organize 👻 New fold	ler	833 -	•
Program Study ^	Name	Date modified	Туре
ConeDrive	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 W
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			
🛀 OS (C:)			
A Makanak Y	<		>
File r	name: ADS Image.E01 ~	All Files (*.*)	~
		Open 🔽 🔿	Cancel

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

	Explo	re Graphics	E-Mail	Search	ch Bookmark
Evidence I	tems	File Status	File Cat	egory	* V * * * * * * * * *
Evidence Items:	1	KFF Alert Files:	0 Documents:	8	
File Iter	ns	Bookmarked Items:	0 Spreadsheets	: 0	
Total File Items:	108	Bad Extension:	0 Databases:	0	
Checked Items:	0	Encrypted Files:	0 Graphics:	9	
Unchecked Item	s: 108	From E-mail:	0 Multimedia:	0	
Flagged Thumbr	ails: 0	Deleted Files:	4 E-mail Messag	es: 0	
Other Thumbnai	s: 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 Spa	ace: 38	
All Items A	ctual Files	KFF Ignorable:	1 Other Known	Type: 2	
		Data Carved Files:	0 Unknown Type	e: 43	
	4	🗅 😂 📴 Encrypt	ed Files ∽	Default	K File List Column Se 😔 Drz
	f 🌪 📑	🗅 🍄 🚾 Encrypte	ed Files 🗸	Default	< It File List Column Se V D12 D12

#### 🖟 AccessData FTK 1.81.6 DEMO VERSION -- C:\GenCyber\ADS Image Case\ ٥ × File Edit View Tools Help Overview Explore Graphics E-Mail Search Bookmark Evidence Items File Status File Category a secret ads file ✓ 4, be 挙 留 留 60 €1 Evidence Items: 1 KFF Alert Files: 0 Documents: 8 File Items Bookmarked Items: Total File Items: 108 Bad Extension: Spreadsheets: Databases: 0 0 Ó 0 Checked Items: 0 Encrypted Files: 108 From E-mail: 0 Graphics: Multimedia: 9 Unchecked Items: 108 0 0 0 9 Flagged Thumbnails: Deleted Files: 4 E-mail Messages 0 Other Thumbnails: From Recycle Bin: 0 Executables: 0 Filtered In: 0 Duplicate Items: 0 Archives: 0 Filtered Out: 108 OLE Subitems: Unfiltered Filtered Flagged Ignore: All Items Actual Files KFF Ignorable: Folders: 0 Slack/Free Space: 38 Other Known Type: Data Carved Files 0 Unknown Type: 43 🚆 🗄 🔠 🍕 🌪 📴 🗅 🐳 🧧 Encrypted Files ✓ ☐ Default File List Column Se ✓ DTZ Full Path File Name Ext File Type Cr Date Acc Date Full Path Im ADS Imagel-Forencics-Image-NTFS-VPassword Stuff/Document1.ht Im ADS Imagel-Forencics-Image-NTFS-VPEC\_11347446[65],pp:>JPEC\_11347446[65],pp:>JPEC\_11347446[65],pp:>JPEC\_11347446[65],pp:>IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:>IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],pp:IPEC\_1134746[65],p Document1.txt filetext2.txt JPEG\_11347446[65].jpg.htm 2/3/2018 .. 2/3/2018 .. N/A 2/3/2018 2/3/2018 N/A N/A txt txt htm Plain Text Document Plain Text Document Hypertext Document Hypertext Document N/A JPEG\_19622246[65].jpg.htm New Text Document.txt htm txt Plain Text Document 2/3/2018 2/3/2018 secret2.txt testfile.txt Plain Text Document Plain Text Document 2/3/2018 ... 2/3/2018 2/3/2018 ... 2/3/2018 txt txt < 8 Listed 0 Checked Total ADS Image\Forensics-Image-NTFS\testfile.txt\secret.txt

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

8.