Overview	Explor	re Graphics	E-Mail		Search	Bookmark			
Evidence Item	ns	File Status	File C	ategory			කක බබ		
idence Items:	0	KFF Alert Files:	Documents		0	· · · · · · · · · · · · ·	100 100 C   C   C   C   C   C   C   C   C   C		
File Items		Bookmarked Items: 0	Spreadshe	ets:	0				
tal File Items:	0	Bad Extension:	Databases:		0				
ecked Items:	0	Encrypted Files:	Graphics:		0				
checked Items:	0	From E-mail:	Multimedia:		0				
gged Thumbnails:	к <b>О</b>	Deleted Files:	E-mail Mess	ages:	0				
er Thumbnails:	0	From Recycle Bin:	Executable	8	0				
ered In:	0	Duplicate items:	Archives:		0				
ared Out:	0	OLE Subitems:	Folders:		0				
filtered Filt	tered	Flagged Ignore:	Slack/Free	Space:	0				
I Items Actua	al Files	KFF Ignorable:	Other Knov	n Type:	0	Access Data ETV Startup	×		
		Data Carved Files:	Unknown T	100		I PALLE SALVELE LES - HOULDAN			
8 88 48 4		D S orr Unfiltered		•)	0 Short		Statt a new case     Open an existing case     Preview evidence     Go directly to working in program		4
E BB @ 4	Name	Vinfiltered      Evidence Path		•) m	0 Short Display		Start a new case     Oren an existing case     Preview evidence     Go directly to working in program	Children Descendants Investigator's Name C	omment
Evidence File N	Name	Evidence Path		•) m	0 Short Display	Forensic internet for the forent term	Statt a new case Depending case Devices evidence Go dectly to working in program Do not show this dialog on statup	Children Descendants Investigator's Name C	omment
Evidence File 1	Name	Vidence Path		•) m	0 Short Display	Forensic	Stat a new case     Open an existing case     Preview evidence     Go directly to working in program      Do not show this dialog on statup	Children Descendants Investigator's Name C	omment
Evidence File f	Name	Vinfittered     Vinfittered     Evidence Path		•) m (	0 Short Display		Shat a new case     DK     Deprion an existing case     Preview existing a     co dectly to working in program     Do not show this dialog on starue	Children Descendants Investigator's Name C	omment
Evidence File f	Name	D Orr Unfittered Evidence Path		•) m (	0 Short Display		Start a new case     OK     Open on existing case     Preview exidence     Go directly to working in program     Do not show this dialog on startup	Children Descendants Investigator's Name C	omment
E BB 🤬 ۹	Name	D 💱 orr Unfiltered Evidence Path		•)  m (	0 Short Display		Start a new case     Open an existing case     Open an existing case     Device inviting in program     Do decity to working in program     Do not show this datag on statue	Children Descendants Investigator's Name C	omment
E BB 🤬 ۹	Name	Gri Unfiltered     Evidence Path		•) m	0 Short Display		Start a new case     OK     Open on existing case     Preview exidence     Go directly to working in program     Do not show this dialog on startup	Children Descendants Investigator's Name C	omment
문 88 4종 《 Evidence File N	Name	D Se or Unfiltered Evidence Path		•) m	0 Short Display	Forensic	Stat a new case Concel State a new case Concel Forward in the state of the state o	Children Descendants Investigator's Name C	omment
문 방문   4군 역 Evidence File f	Name	Gr Unflered     Evidence Path		•) m	0 Short Display	Forensic	Start a new core     OK     Open an existing case     Preview existing a     Cancel     Preview existing in program     Do not show this dialog on startup	Children Descendants Investigator's Name C	omment
Evidence File f	Name	D Se or Unfiltered Evidence Path		•) m	0 Short Display		Start a new case     OK     Open an esiting case     Perior     Perior     G a decty to working in program     Do not show this dialog on startup	Children Descendants Investigator's Name C	omment
문 명망 교육 예 Evidence File N	Name	Grant Contraction Contraction     Grant Contraction Contraction     Evidence Path		•) m	0 Short Display		Stat a new case Open an existing case Open an existing case Open an existing a case Go decity to working in program Do not show this dalog on statup	Children Descendants Investigator's Name C	omment
Evidence File f	Name	With an United Strength      Evidence Path		•) m	0 Short Display		Start a new case     OK     Ogen an existing case     Preview exidence     Go dectly le working in program     Do not show this dailing on startup	Children Descendants Investigator's Name C	•
Evidence File M	Name	D @ or Unfilered Evidence Path		•) m	0 Short Display	Forensic	Stat a new case Open an existing case Open an existing case Open an existing a program Open and the state o	Children Descendants Investigator's Name C	> omment
B BB 48 48	Name	Gr [unffered Evidence Path		•) m	0 Short Display	Forensic Forensic	Start a new case     OK     Open an existing case     Preview evidence     Go dectly to working in program     Do not show this dialog on startup	Children Descendants Investigator's Name C	> omment
Evidence File 1	Name	Government     G		•) m	0 Short Display	Forensic	Stat a new case     Open an existing case     Priview reference     Go dectly to working in program     Do not show this dialog on statup	Children Descendants Investigator's Name C	> omment
Evidence File 1	Name	D V on Luntered Evidence Path		•)	0 Short Display	Forensic	Start a new case     OK     Open an existing case     Preview evidence     G of dectly to working in program     Do not show this dialog on startup	Children Descendants Investigator's Name C	omment

1. Run FTK 1.8.6 on your desktop by double click on the icon

2. Build a case of EFS by using default case setting

AccessData FTK version 1	.81.6 build 10.04.02				
ile Edit View Tools I	Help				
Overview Explo	ore Graphics	E-Mail	Search Bookmark		
Evidence Items	File Status	File Ca	tenoni u		
Evidence items: 0	KFF Alert Files: 0	Documents:	New Case		See
File Items	Bookmarked Items: 0	Spreadsheet			^
Total File Items: 0	Bad Extension: 0	Databases:	Find, Organica, & Analyze Computer Evidence		
Checked Items: 0	Encrypted Files: 0	Graphics:		AccessData's	
Unchecked Items: 0	From E-mail: 0	Multimedia:		Forensic Toolkit®-FTK®	
Flagged Thumbnails: 0	Deleted Files: 0	E-mail Messa		The Operation Americals Treel	
Other Thumbnails: 0	From Recycle Bin: 0	Executables:	Eoronsic	The Complete Analysis 1001	
Fitered In: 0	Duplicate Items: 0	Archives:	The Design of the Toolket		
Filtered Out: 0	OLE Subitems: 0	Folders:		Wizard for Creating a New Case	
Unfitered Fitered	Flagged Ignore: 0	Slack/Free S		5	
All Items Actual Files	KFF Ignorable: 0	Other Known			
	Data Carved Files: 0	Unknown Tyr	Investigator Name: Michael Tu	•	
			Case Information		
			Case Numbr	er: 001	
			Case Nam	TEC .	-
			Case Hain	e. 215	
	- 100		Case Pat	th: C:\ Browse	
🖁 🗄 🔠 🧐 🏀 📑	🗅 😜 🖙 Unfiltered		Case Fold	er CAFES	
Evidence File Name	Evidence Path		Case Description:		Descendants Investigator's Name Comment
				Not > Cancel	
•			III	1	
Listed					
😰 🖸 🏹	1 📋 🧷				▲ 📑 📭 📴 10:37 PM 6/4/2016

3. Using default settings of FTK by clicking the next button till this "Add Evidence"

The second dia 1 m vi	ersion 1.	81.0 DU	10 10.04.02			
e Edit View 1	Tools H	Help				
Overview	Explo	re	Graphics	E-Mail	Search Bookmark	
Evidence Iter	ns		File Status	File C		
vidence items:	0	KFF AJ	ert Files: 0	Documents:	Is: Add Evidence to Case	
File Items		Bookm	arked Items: 0	Spreadshee	eet	
tal File Items:	0	Bad Ex	tension: 0	Databases:	Add Evidence	
hecked items:	0	Encryp	ited Files: 0	Graphics:	Any number of evidence items can be added to the case. There are several types of evidence items:	
checked items:	0	From E	-mait 0	Multimedia:	2. Accurate inside of drive: Several formate supported: can be an image of a logical or physical drive	
igged Thumbnails	s: 0	Deleter	d Files: 0	E-mail Messi	ssa Local drive: Can be a logical or physical drive	
ner Thumbnails:	0	From F	tecycle Bin: 0	Executables	es Folder: Adds all files in the specified folder, including contents of subfolders	
ared In:	0	Duplica	ate items: 0	Archives:	Individual Hie: Adds a single file. NO IE: Disk image files should be added as acquired images.	
ared Out:	0	OLE S	ubitems: 0	Folders:	The default refinement options, set previously, can be overridden independently for each evidence item, and additional hose of refinements and additional These refinements and the the evidence item and additional in a specific option.	
filtered Filt	tered	Flagge	d Ignore: 0	Slack/Free S	S folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced	
I Items Actu	al Files	KFF Ig	norable: 0	Other Know	Will Add Extense Eth Extense Domas Extense Advanced	
		Data C	arved Files: 0	Unknown Ty	Ty Add Evidence Edit Evidence Hemove Evidence Renne Evidence - Advanced	
Evidence File	Name	Evide	nce Path		Cancel	Comment
[					-	
ted						
) 🖸	1		🗎 <i>ெ</i>			10:38 P 6/4/20

File Edit View Tools	Help							
Overview Explo	ore Graphics	E-Mail	Search	Bookmark				
Evidence Items	File Status	File Ca	tegony	والمعادية ومحاجبة والأرار				
Evidence tems: 0	KFF Alert Files: 0	Documents:	Add Evidence to Case			22		
File Items	Bookmarked tems: 0	Spreadsheet	C					~
Total File terms: 0	Bad Extension: 0	Databases:		Add Evider	<b>C0</b>			
Checked Items: 0	Encrypted Files: 0	Graphics:	Annual second second second	Add Evider				
Unchecked Items: 0	From E-mail: 0	Multimedia:	My number of evidence in	tems can be added to the case. There are so	iveral types of evidence terms:			
Flagged Thumbnails: 0	Deleted Files: 0	E-mail Messa	Local dtyp:	Can be a logical or physical drive	n image or a logical or physical drive			
Other Thumbnails: 0	From Recycle Bin: 0	Executables:	Folder:	Adds all files in the specified folder, i	cluding contents of subfolders			
Filtered In: 0	Duplicate Items: 0	Archives:	Individual File:	Adds a single file. NOTE: Disk imag	e files should be added as acquired i	mages.		
Filtered Out: 0	OLE Subtems: 0	Folders:	The default refinement op	tions, set previously, can be overridden inder	condently for each evidence item, an	nd additional		
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free S	folders. To make these fu	ther refinements, highlight an evidence item.	n the lat and press Refine Evidence	- Advanced		
All Items Actual Files	KFF Ignorable: 0	Other Known	Add Cuideana	Add Evidence to Case	-X-	Adversed		
	Data Carved Files: 0	Unknown Ty	Add Evidence		ne Evidence -	Advanced		
			Display Name	Type of Evidence to Add to Cas	a Time Zone	Comment		
				Acquired Image of Drive				
				Cocal Drive				-
				Contents of a Folder				E.
				Chatrideal Da				
1 H H H 🐼 😽 📑	C Voff Unfiltered		1	C Individual File				
Evidence File Name	Evidence Path						Descendants Investigator's Name Comment	
				Continue	Cancel			
					< Back Next >	Cancel		
*								•
0 Listed								
							10:40	PM
🥣 💟 🔼		j 🕑 (					▲ ■ ■ 6/4/2	2016

4. Click on "Add Evidence" button to add choose the acquired image of a drive

5. Click on continue and next to navigate to the NTFS-EFS-ADS.e01 file on your forensics case lab folder under the 2016 GenCyber Summer Camp folder on your desktop



6. Click on open and then click on OK, and then next and finish, till finished.

AccessData FTK version 1.81.6 build 10.04.02	,	
ile Edit View Tools Help		
Overview Explore Graphics	E-Mail Search Bookmark	
Evidence Items File Status	File Category A A A A A A A A A A A A A A A A A A A	
Evidence Items: 0 KFF Alert Files: 0	Documents: 0	
File Items Bookmarked Items: 0	Spreadsheets: 0	
Total File Items: 0 Bad Extension: 0	Databases: 0	
Checked Items: 0 Encrypted Files: 0	Graphics: 0	
Unchecked Items: 0 From E-mail: 0	Mutimedia: 0	
Flagged Thumbnails: 0 Deleted Files: 0	E-mail Messages: 0	
Other Thumbnails: 0 From Recycle Bin: 0	Executables: 0	
Filtered In: 0 Duplicate Items: 0	Archives: Processing Files	
Fitered Out: 0 OLE Subitems: 0	Folders:	
Unfiltered Filtered Flagged Ignore: 0	Slack/Free Space	
All Items Actual Files KFF Ignorable: 0	Other Known Typ U: Users/tu15.51AFF/Desktop/GenLyber Summer Camp Material/2016 GenLyber Summer Camp Material/A For	
Data Carved Files: 0	Unknown Type: Current File Item:	
Image: Second	Action: Indexing File Type: EFS Mate Kay Ne Total Iteme Samined 55 Total Iteme Indexed 41 Log the case/system status every 10 not minutes Log extended information	en Descendants Investigator's Name Comment
۲ د کرد Listed 0 Checked Total (0 High	ni Jhted	,



7. File export – export SAM and System file for password carcking

6 AccessData FTK	K version 1.81.6 build 10.04.02	
File Edit View	Tools Help	
Overview	File Properties	ail Search Bookmark
Evidence It Evidence Items:	Ignore Highlighted Items	le Category ents: 0
File Item	n Ignore Checked Items	sheets: 0
Total File Items:	Unignore Highlighted Items	ses: 0
Checked Items: Unchecked Items	Unignore Checked Items	bs: 0 dia 0
Flagged Thumbna	Create Bookmark	lessages: 0
Other Thumbnails	Add to Bookmark	ables: 0
Filtered In:	Analysis Tools	<u>es:</u> 0
Linfitered Out:	Add Case Log Entry	ree Spare: 0
All Items Ar	View Case Log	nown Type: 0
	New Case Log Segment	vn Type: 0
	Select Registry Reports	
	Preliminary Registry Reports	
	Internet Keyword Search	4 b
8 8 88 6	Data Carving	Short      PDZ
Evidence Fi	Export Word List	Display Name Identification Name/Nu Evidence Type Added Children Descendants Investigator's Name Comment
	Verify Image Integrity	
	Import KFF Hashes	
	Edit KFF Alert Values	
	Prerender Thumbnails	
	Enter EFS Password	
	Decrypt EFS Files	
	Preferences	
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
0 Listed		
🚱 🖸	A 📋 🧉	😜 wij 🖉

1. Then go to toos and select the "Enter EFS Password" menu

2. Put your password and then it will automatically decrypt the efs files

	Explo	re Graphics	E-Mail	Search Bookmark
Evidence Item		File Statue	File Catery	
Evidence tems:	4	KFF Alert Files: 0	Documents:	
File Items		Bookmarked tems: 0	Spreadsheets:	
Total File Items:	83	Bad Extension: 0	Databases:	8
Checked Items:	0	Encrypted Files: 7	Graphics:	0
Unchecked Items:	83	From E-mail: 0	Multimedia:	0
Flagged Thumbnails:	c 0	Deleted Files: 2	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin: 0	Executables:	
Filtered In:	83	Duplicate items: 2	Archives:	Processing Files
Filtered Out:	0	OLE Subitems: 18	Folders:	
Unfiltered Filt	ered	Flagged Ignore: 0	Slack/Free Space	Current E vidence Item:
All Items Actua	al Files	KFF Ignorable: 0	Other Known Typ	
		Data Carved Files: 0	Unknown Type:	Current File Item: EFS Summary
a u uu   *a *	Name	Evidence Dath		Item Size: OK 21 ren Descendants Investigator's Name Comment
8 6 66 98 9	₩  15		×	
	Name	Isudence Path		Item Size: OK 41 Iren Descendants Investigator's Name Comment
Evidence File I	- Contraction	Evidence Faul		
Evidence File I Document2[32].doc		C:\EFS\efs\decrypt		Progress: 18 6 6 Michael Tu
<ul> <li>Evidence File I Document2[32] doc</li> <li>Document3[34] doc</li> <li>Document4[36] doc</li> </ul>		C:\EFS\efs\decrypt C:\EFS\efs\decrypt C:\EFS\efs\decrypt		Progress:         18         6         6         Michael Tu           18         5         5         Michael Tu           5         5         Michael Tu
Evidence File I  Document2[32].doc  Document3[34].doc  Document4[36].doc  EFS XP.E01		C:\EFS\dectypt C:\EFS\dectypt C:\EFS\dectypt C:\EFS\dectypt C:\Users\tu15.STAFF\De	sktop\GenEyber Surr	Progress:         6         6         Michael Tu           6         6         Michael Tu         6         Michael Tu           6         6         Michael Tu         6         Michael Tu           100 the care/system status every 10 minutes         Log estended information         Careel         62         22         Xinbael Tu
<ul> <li>Evidence File I Document2[32].doc Document3[34].doc Document4[36].doc EFS XP.E01</li> </ul>		C:VEFS\efs\decrypt C:VEFS\efs\decrypt C:VEFS\efs\decrypt C:VEFS\efs\decrypt C:VEFS\efs\decrypt	sktop\GenCyber Surr	Progress: 18 6 6 Michael Tu 6 6 Michael Tu 5 8 Michael Tu
Evidence File I Document2[32].doc Document3[34].doc Document4[36].doc EFS XP.E01		C:\EFS\efs\decrypt C:\EFS\efs\decrypt C:\EFS\efs\decrypt C:\EFS\efs\decrypt C:\Users\tu15.STAFF\De	sktop\GenCyber Surr	Progress: 18 Log the care/system status every 10 minutes Log extended information Cancel
<ul> <li>Evidence File I Document2[32].doc Document3[34].doc Document4[36].doc EFS XP.E01</li> </ul>		C:VEFSVefsVdecrypt C:VEFSVefsVdecrypt C:VEFSVefsVdecrypt C:VEFSVefsVdecrypt C:VEssesVtu15.STAFFVDe	sktop\GenCyber Sum	Progress: 18 Log the case/system status every 10 _ minutes _ Log extended information Cancel
Evidence File / Document2[32].doc Document3[34].doc Document4[36].doc EFS XP.E01		CNEFSVefsVefectypt CNEFSVefsVefectypt CNEFSVefsVefectypt CNEFSVefsVefectypt CNEFSTVefsVefectypt	sktop\GenCyber Sum	Progress: 18 Log the case/system status every 10 minutes Log extended information Cancel 6 6 6 Michael Tu 5 6 Michael Tu 5 8 Michael Tu 5 2 82 Michael Tu 5 2 82 Michael Tu
■ Evidence File I Document2[32].doc Document3[34].doc Document4[36].doc EFS XP.E01		CVERSVersiversystems CVERSVersiversystems CVERSVersiversystems CVERSVersiversystems CVUsers/WITSSTAFF\De	sktop\GenCyber Sum	Progress:     18     6     6     5     Michael Tu       Log the case/fystem status every     10 in minutes     Log extended information     Cancel
T Evidence File 1 Document2[32].doc Document4[34].doc Document4[36].doc EFS XP_E01		CVEFSVehVdeoppt CVEFSVehVdeoppt CVEFSVehVdeoppt CVEFSVehVdeoppt CVEFSVehVdeoppt CVUsersVu15STAFF\De	sktop\GenCyber Sum	Progress:     18       Log the case/system status every     10 - minutes       Log the case/system status every     10 - minutes       Log the case/system status every     10 - minutes
m Evidence File 1 Document2(32) doc Document2(34) doc Document4(36) doc EFS XP.E01		CVEFSVetVdecypt CVEFSVetVdecypt CVEFSVetVdecypt CVEFSVetSVdecypt CVEFSVetSVdecypt CVUsersVu15STAFF\De	sktop\GenCyber Sum	Progress: 18 Log the case/system status every 10 in minutes Log extended information Cancel 6 6 6 Michael Tu 6 6 6 Michael Tu 6 7 Michael Tu 6 8 Michael Tu
m Evidence File I Document2[32] doc Document2[34] doc Document4[66] doc EFS XP.E01		CVERSVetVideoppt CVERSVetVideoppt CVERSVetVideoppt CVERSVetVideoppt CVUSersViutSSTAFF\De	sktop/GenCyber Sum	Progress: Log the case/system status every 10 minutesLog extended information Log the case/system status every 10 minutesLog extended information Extended to Extended to
m Evidence File [ Document2[32] doc Document3[34] doc Document4[36] doc EFS XP.E01		CVUEFSVehVdeorpt CVEFSVehVdeorpt CVEFSVehVdeorpt CVEFSVehVdeorpt CVUsersVu15STAFF\De	sktop/GenCyber Sum	Progress:       18         Log the case/system status every       10 ****         Log extended information       Cancel
m Evridence File I Document/2(32) doc Document/3(34) doc Document/4(36) doc EFS XP-E01		UNERCENT CNEFSIehlvdeoppt CNEFSIehlvdeoppt CNEFSIehlvdeoppt CNUserstuitSSTAFFUDe	sktop\GenCyber Sun	Progress:
to contence File I occument2[32] doc Joccument2[34] doc Joccument4[36] doc EFS XP.E01		UNEFECTATION CLEFSINI-Indexpit CLEFSINI-INDEXPIT	sktop\GenCyber Sum	Progress:     Cancel     Cancel     Cancel

3. Then you should click the "overview" tab and go to the document folder to check the decrypted EFS encrypted file