

# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II

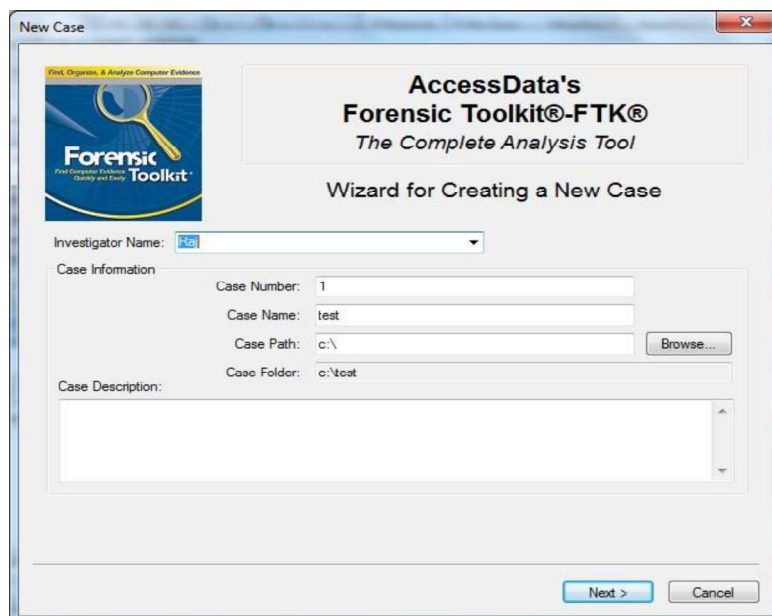
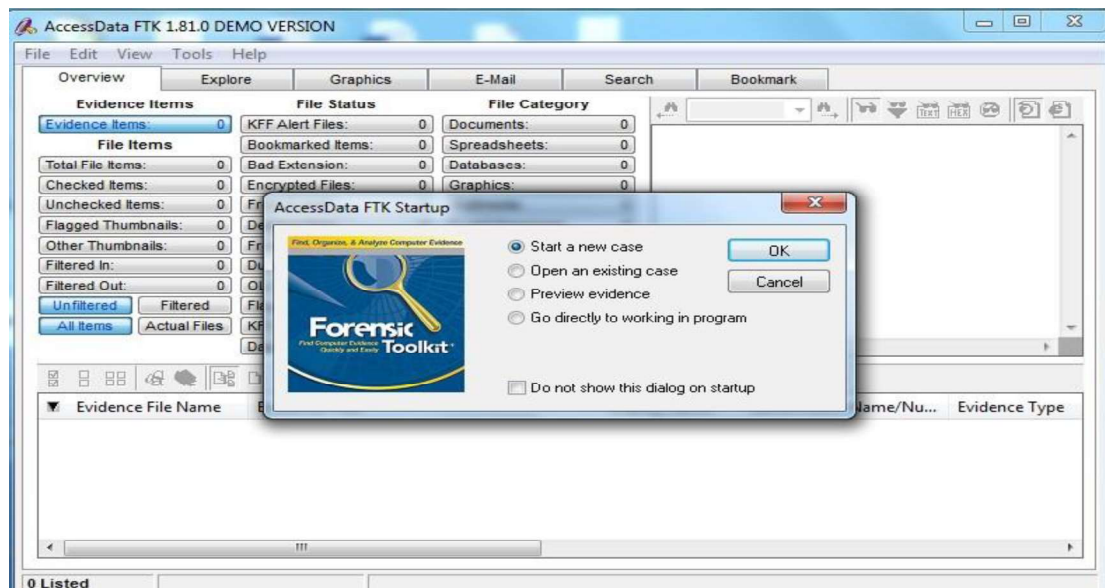
## Practical No: - 10

**AIM: Create a new investigation case using Forensic Tool:**

1. Computer System
2. Computer Network

### 1. Computer System

Select file and then select a new case



Sample Document for Reference Only. Perform Practical Individually

<https://rajeshmaurya.in/>

# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



FTK Report Wizard - Case Information

### Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company:

Examiner's Name:

Address:

Phone:  Fax:

E-Mail:

Comments:

< Back Next > Cancel

Case Log Options

### Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

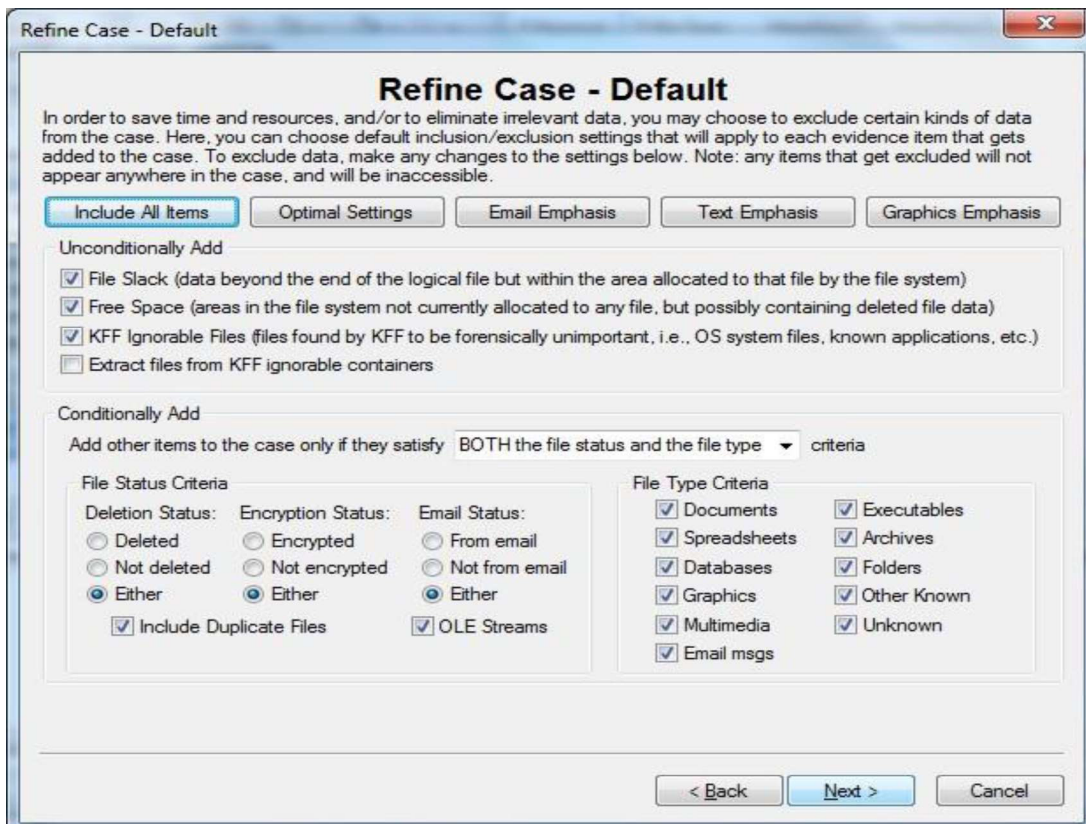
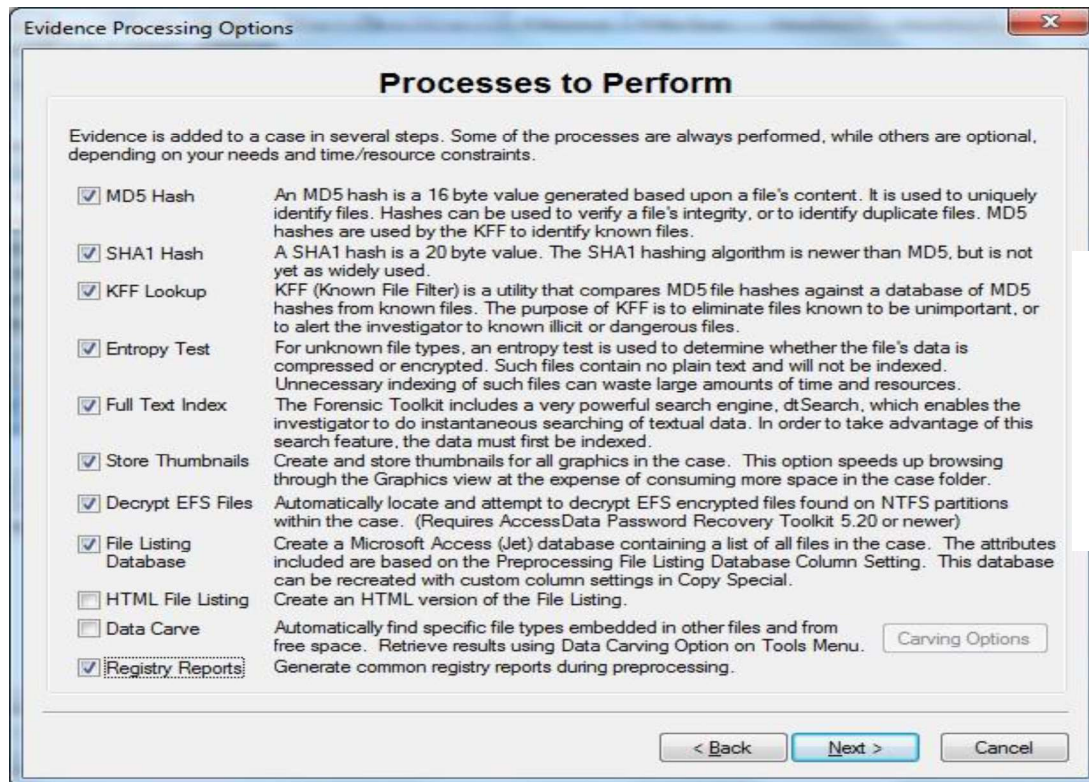
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during the case.
<input checked="" type="checkbox"/> Bookmarking events	Events related to the addition and modification of bookmarks.
<input checked="" type="checkbox"/> Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
<input checked="" type="checkbox"/> Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
<input checked="" type="checkbox"/> Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

< Back Next > Cancel

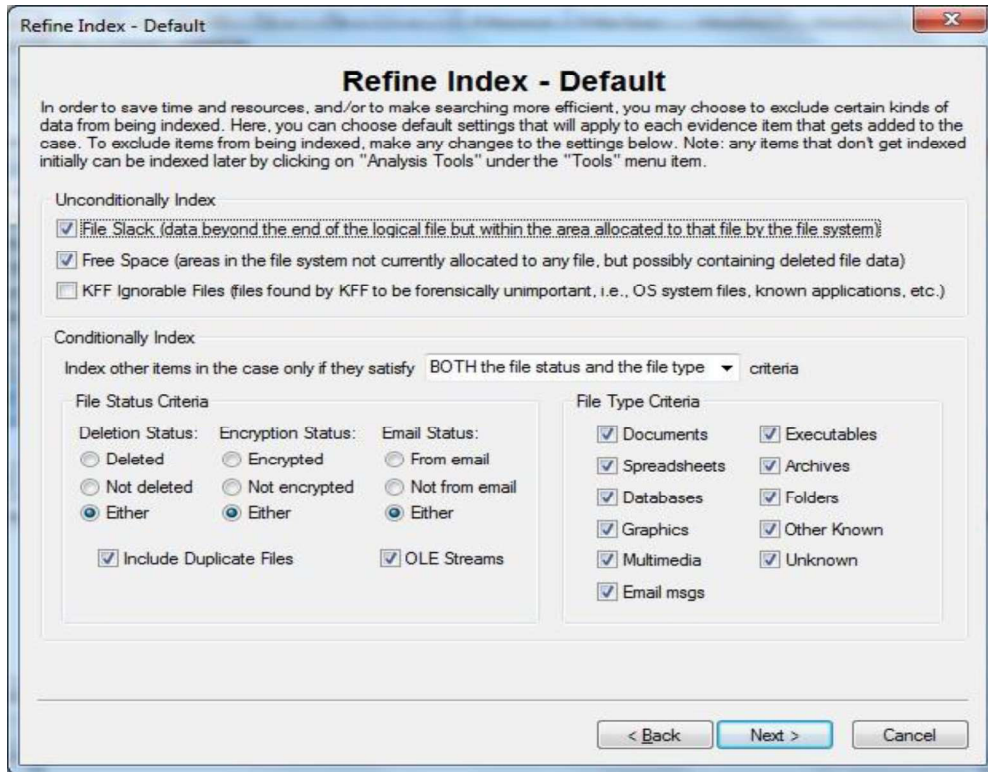
# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



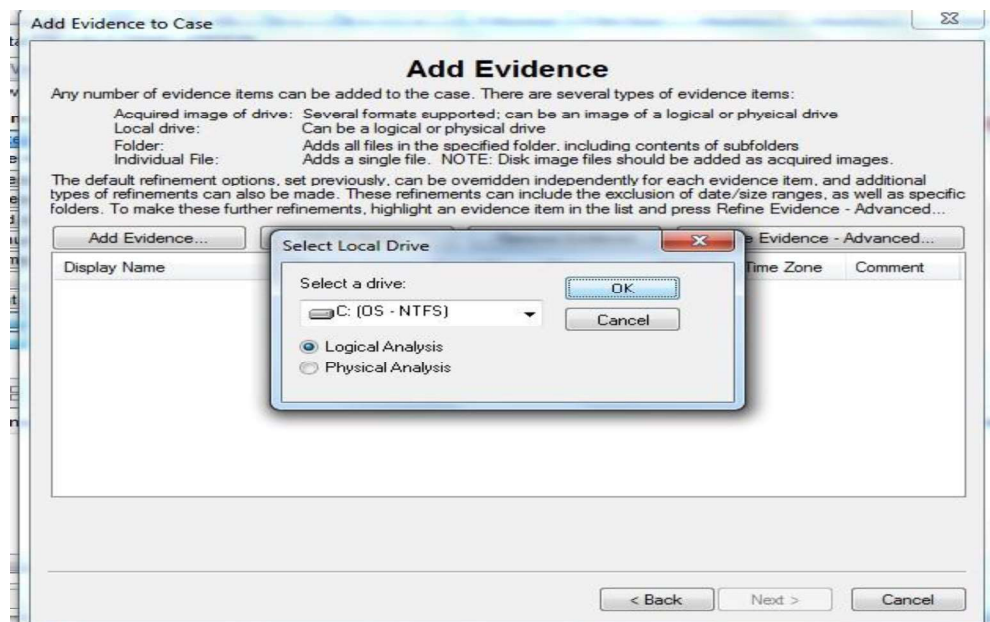
Sample Document for Reference Only. Perform Practical Individually  
<https://rajeshmaurya.in/>



## MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II

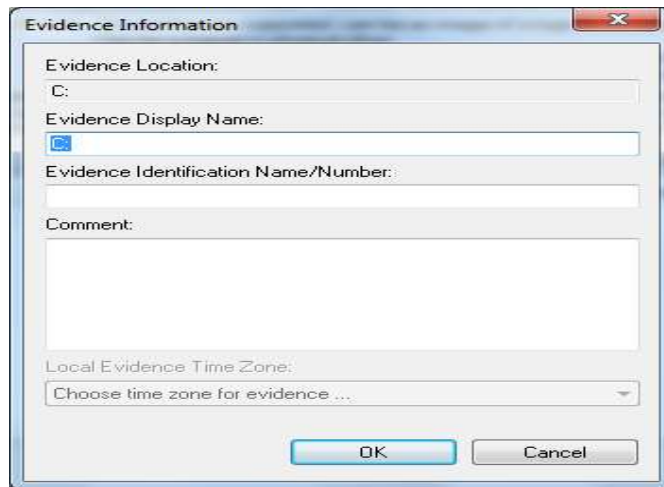


From add evidence prompt ,select local drive for computer system



Sample Document for Reference Only. Perform Practical Individually  
<https://rajeshmaurya.in/>

## MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



**Evidence Information**

Evidence Location:  
C:

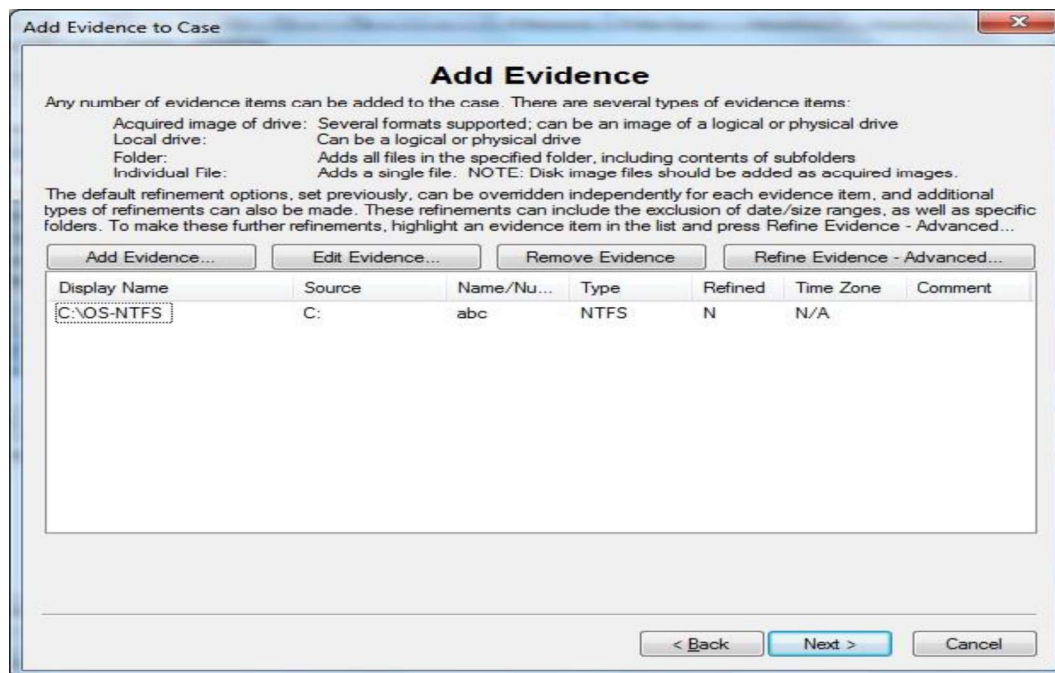
Evidence Display Name:  
[Icon]

Evidence Identification Name/Number:  
[Text Box]

Comment:  
[Text Area]

Local Evidence Time Zone:  
Choose time zone for evidence ...

OK Cancel



**Add Evidence to Case**

**Add Evidence**

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

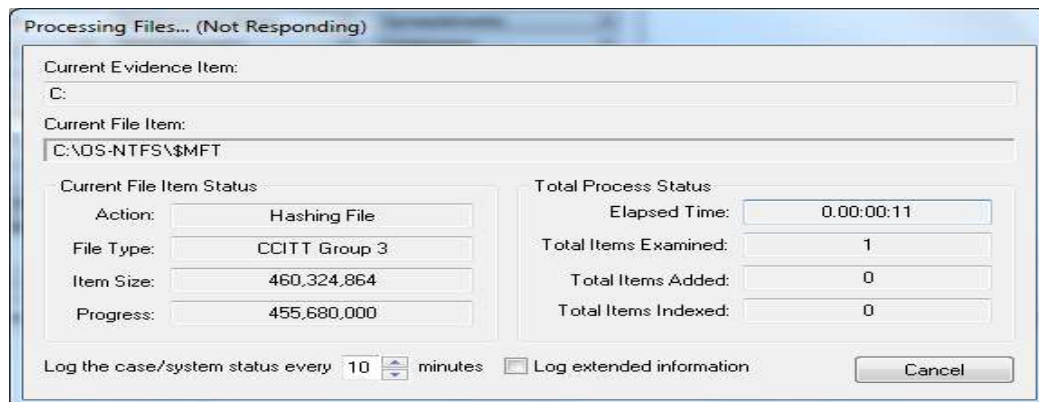
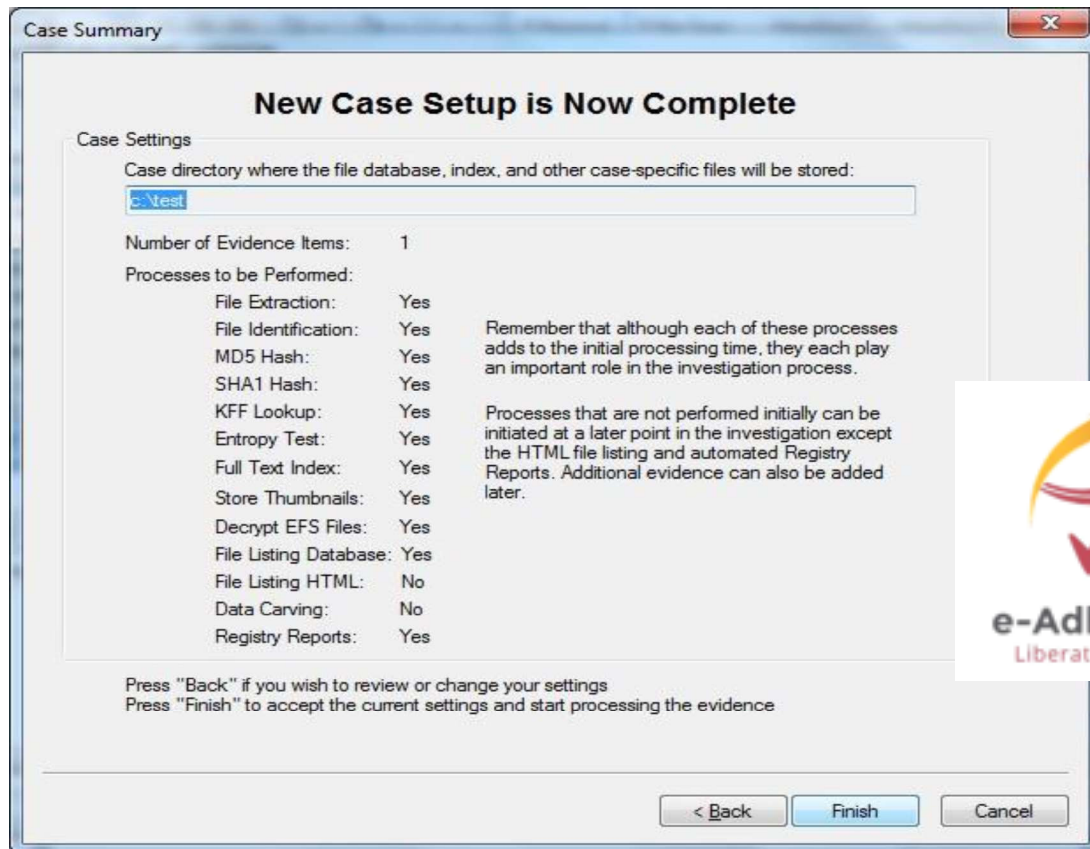
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
C:\OS-NTFS	C:	abc	NTFS	N	N/A	

< Back Next > Cancel

# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



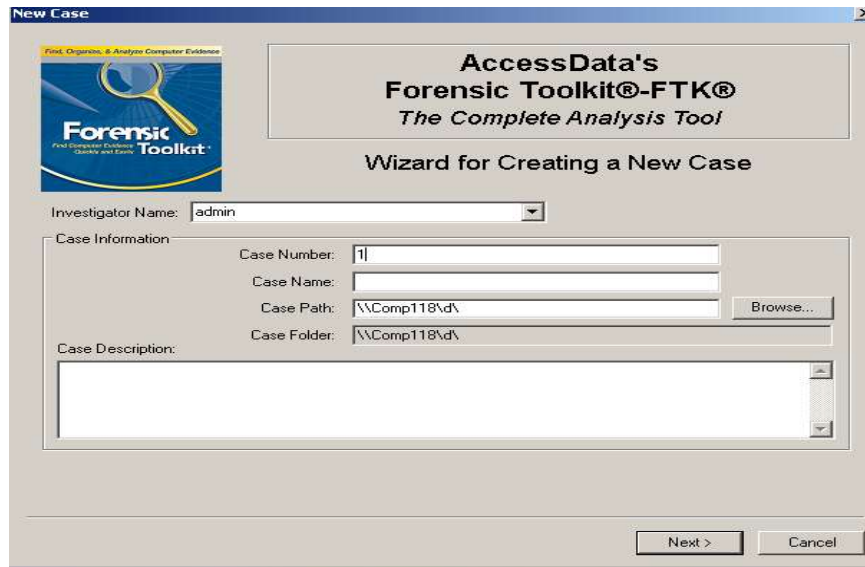
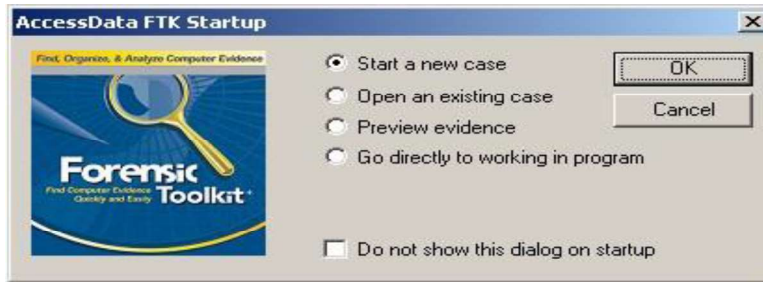
Same can be done for mobile devices, computer network and wireless network

## 2. Computer Network

Sample Document for Reference Only. Perform Practical Individually

<https://rajeshmaurya.in/>

## MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II

**FTK Report Wizard - Case Information**

**Forensic Examiner Information**

The following information will appear on the Case Information page of the report:

Agency/Company:

Examiner's Name:

Address:

Phone:  Fax:

E-Mail:

Comments:

< Back   Next >   Cancel


**Case Log Options**

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during the case.
<input checked="" type="checkbox"/> Bookmarking events	Events related to the addition and modification of bookmarks.
<input checked="" type="checkbox"/> Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
<input checked="" type="checkbox"/> Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
<input checked="" type="checkbox"/> Other events	Other events not related to the above, such as copying, viewing, and ignoring files.



Next >   Cancel



# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II

**Evidence Processing Options**

**Processes to Perform**

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, 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.
<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> 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)
<input checked="" type="checkbox"/> File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in 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.
<input type="checkbox"/> HTML File Listing	Create an HTML version of the File Listing.
<input type="checkbox"/> Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
<input type="checkbox"/> Registry Reports	Generate common registry reports during preprocessing.

[Carving Options](#)

< Back    Next >    Cancel

**Refine Case - Default**

**Refine Case - Default**

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Include All Items    Optimal Settings    Email Emphasis    Text Emphasis    Graphics Emphasis

Unconditionally Add

<input checked="" type="checkbox"/> File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
<input checked="" type="checkbox"/> Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
<input checked="" type="checkbox"/> KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
<input type="checkbox"/> Extract files from KFF ignorable containers

Conditionally Add

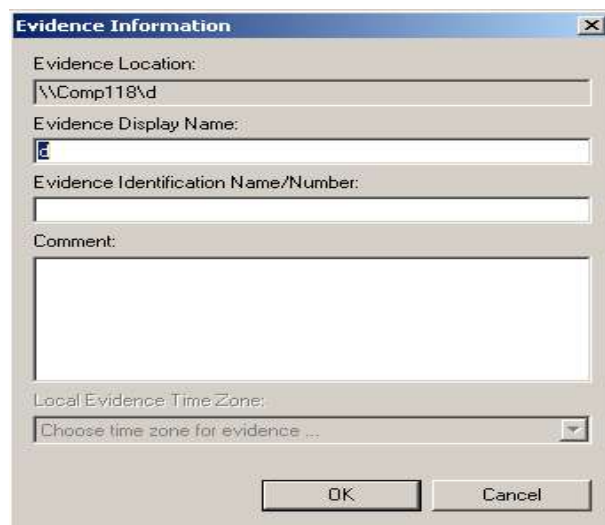
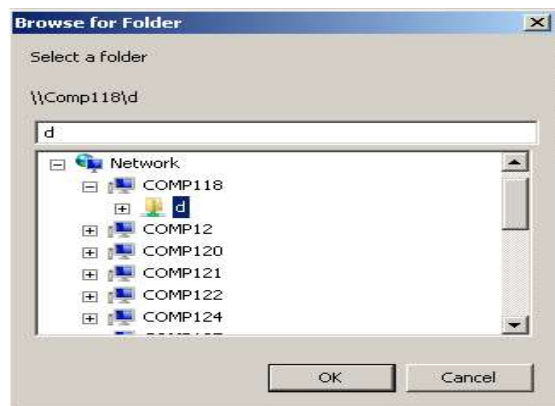
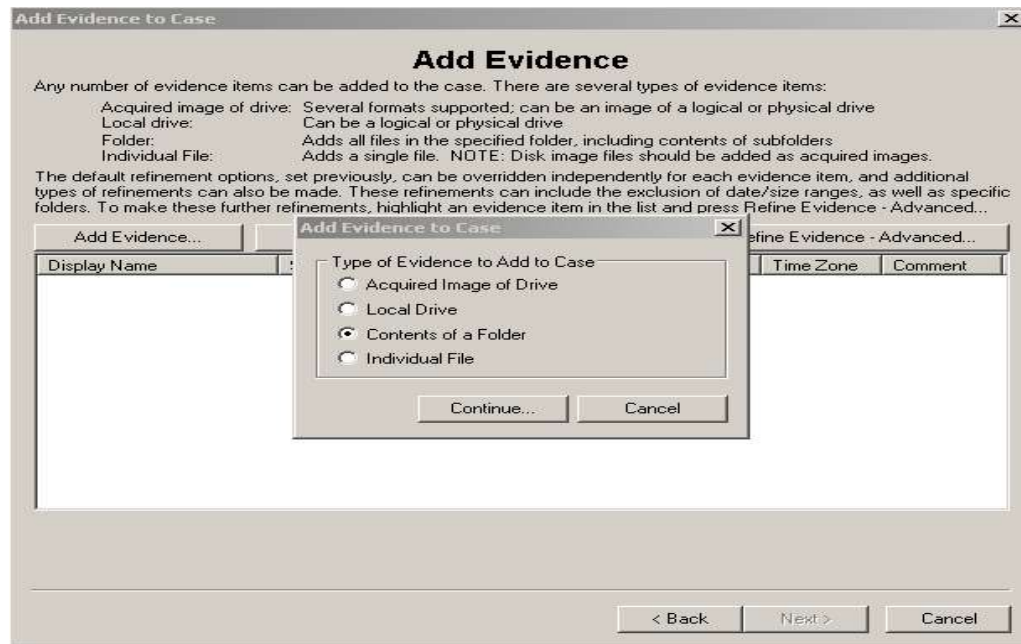
Add other items to the case only if they satisfy **BOTH the file status and the file type** criteria

<b>File Status Criteria</b>			<b>File Type Criteria</b>	
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> Spreadsheets	<input checked="" type="checkbox"/> Archives
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email	<input checked="" type="checkbox"/> Databases	<input checked="" type="checkbox"/> Folders
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="checkbox"/> Graphics	<input checked="" type="checkbox"/> Other Known
<input checked="" type="checkbox"/> Include Duplicate Files	<input checked="" type="checkbox"/> OLE Streams		<input checked="" type="checkbox"/> Multimedia	<input checked="" type="checkbox"/> Unknown
			<input checked="" type="checkbox"/> Email msgs	

< Back    Next >    Cancel



# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II

**Add Evidence to Case**

**Add Evidence**

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Num...	Type	Refined	Time Zone	Comment
d	\\Comp118\d		Contents o...	N	N/A	

< Back Next > Cancel

**Case Summary**

**New Case Setup is Now Complete**

Case Settings:

Case directory where the file database, index, and other case-specific files will be stored:

\\Comp118\d\ahastudfah

Number of Evidence Items: 1

Processes to be Performed:

File Extraction:	Yes	Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
File Identification:	Yes	
MD5 Hash:	Yes	
SHA1 Hash:	Yes	
KFF Lookup:	Yes	
Entropy Test:	Yes	Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.
Full Text Index:	Yes	
Store Thumbnails:	Yes	
Decrypt EFS Files:	Yes	
File Listing Database:	Yes	
File Listing HTML:	No	
Data Carving:	No	
Registry Reports:	No	

Press "Back" if you wish to review or change your settings  
Press "Finish" to accept the current settings and start processing the evidence

< Back Finish Cancel



# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II

**Processing Files...**

Current Evidence Item:  
\\Comp118\d

Current File Item:  
\\Comp118\d\NT-3009\Cisco\_UCS\_Platform\_Emulator\_3.0.1cPE1-4eee4795.vmem

Current File Item Status:

Action: Hashing and Entropy Test

File Type: Unknown File Type

Item Size: 2,147,483,648

Progress: 45,260,800

Total Process Status:

Elapsed Time: 0:00:00:06

Total Items Examined: 116

Total Items Added: 115

Total Items Indexed: 112

Log the case/system status every 10 minutes ☐ Log extended information

Cancel

**AccessData FTK 1.81.0 DEMO VERSION -- D:\ahasjudfah\**

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

**Evidence Items** **File Status** **File Category**

Evidence Items: 1	KFF Alert Files: 0	Documents: 104
<b>File Items</b>	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 5000	Bad Extension: 13	Databases: 0
Checked Items: 0	Encrypted Files: 0	Graphics: 2
Unchecked Items: 5000	From E-mail: 0	Multimedia: 0
Flagged Thumbnails: 0	Deleted Files: 0	E-mail Messages: 0
Other Thumbnails: 2	From Recycle Bin: 0	Executables: 84
Filtered In: 5000	Duplicate Items: 3830	Archives: 4
Filtered Out: 0	OLE Subitems: 0	Folders: 0
Unfiltered	Flagged Ignore: 0	Slack/Free Space: 0
All Items	KFF Ignorable: 0	Other Known Type: 0
Actual Files	Data Carved Files: 0	Unknown Type: 4806

Unfiltered Filtered

Off Unfiltered

All Columns DTZ

Evidence File Name	Evidence Path	Display Name	Identification Name/Number	Evidence Type
d	\\Comp118	d		Contents of a folder

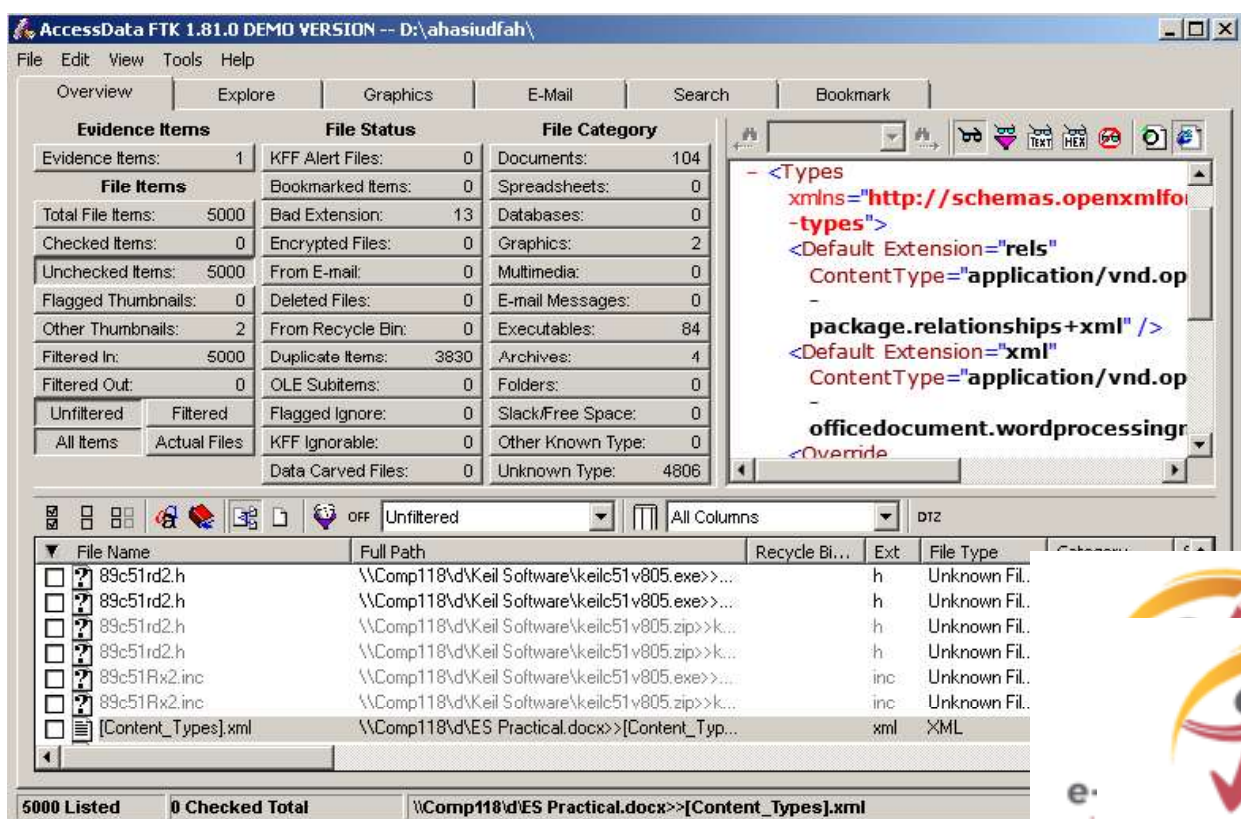
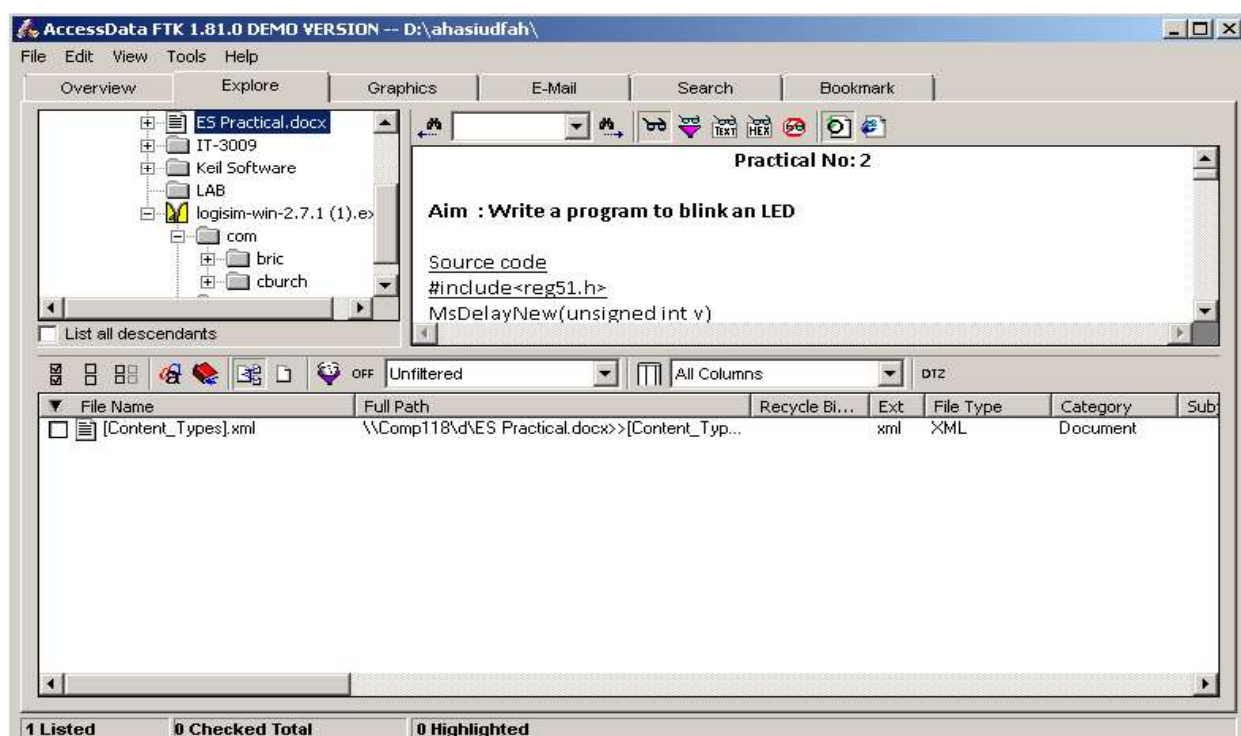
1 Listed 0 Checked Total 0 Highlighted



Sample Document for Reference Only. Perform Practical Individually  
<https://rajeshmaurya.in/>



# MSC COMPUTER SCIENCE SEM-III ELECTIVE-I: CYBER AND INFORMATION SECURITY-II



Sample Document for Reference Only. Perform Practical Individually  
<https://rajeshmaurya.in/>

