

## **Practical 6**

**Date:** 04-01-25

**Aim:** Using Sysinternals tools for Network Tracking and Process Monitoring:

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM-Capture
- TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

**Steps:**

1) Check Sysinternals tools

Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

The following are the categories of Sysinternals Tools:

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

### **Sysinternals File and Disk Utilities**

**AccessChk:**

This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

**AccessEnum:**

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

**CacheSet:**

CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.

**Contig**

Wish you could quickly defragment your frequently used files? Use Contig to optimize individual files, or to create new files that are contiguous.

**Disk2vhd:**

Disk2vhd simplifies the migration of physical systems into virtual machines (p2v).

**DiskExt:**

Display volume disk-mappings.

**DiskMon:**

This utility captures all hard disk activity or acts like a software disk activity light in your system tray.

**DiskView:**

Graphical disk sector utility.

**Disk Usage (DU):**

View disk usage by directory.

**EFSDump:**

View information for encrypted files.

**FindLinks:**

FindLinks reports the file index and any hard links (alternate file paths on the same volume) that exist for the specified file. A file's data remains allocated so long as at least one file name referencing it.

**Junction:**

Create Win2K NTFS symbolic links.

**LDMDump:**

Dump the contents of the Logical Disk Manager's on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.

**MoveFile:**

Schedule file rename and delete commands for the next reboot. This can be useful for cleaning stubborn or in-use malware files.

**NTFSInfo:**

Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.

**PendMoves:**

See what files are scheduled for delete or rename the next time the system boots.

**Process Monitor:**

Monitor file system, Registry, process, thread and DLL activity in real-time.

**PsFile:**

See what files are opened remotely.

**PsTools:**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

**SDelete:**

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

**ShareEnum:**

Scan file shares on your network and view their security settings to close security holes.

**Sigcheck:**

Dump file version information and verify that images on your system are digitally signed.

**Streams:**

Reveal NTFS alternate streams.

**Sync:**

Flush cached data to disk.

**VolumID:**

Set Volume ID of FAT or NTFS drives.

**Sysinternals Networking Utilities****AD Explorer:**

Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.

**AD Insight:**

AD Insight is an LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications.

**AdRestore:**

Undelete Server 2003 Active Directory objects.

**PipeList:**

Displays the named pipes on your system, including the number of maximum instances and active instances for each pipe.

**PsFile:**

See what files are opened remotely.

**PsPing:**

Measures network performance.

**PsTools:**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

**ShareEnum:**

Scan file shares on your network and view their security settings to close security holes.

**TCPView:**

Active socket command-line viewer.

**Whois:**

See who owns an Internet address.

**Sysinternals Process Utilities****Autoruns:**

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

**Handle:**

This handy command-line utility will show you what files are open by which processes, and much more.

**ListDLLs:**

List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules.

**PortMon:**

Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

**ProcDump:** This new command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

**Process Explorer:**

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

**Process Monitor:**

Monitor file system, Registry, process, thread and DLL activity in real-time.

**PsExec:**

Execute processes remotely.

**Powershell:**

Displays the SID of a computer or a user.

**Powershell:**

Terminate local or remote processes.

**sPsList:**

Show information about processes and threads.

**Powershell:**

View and control services.

**Powershell:**

Suspend and resume processes.

**Powershell:**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

**ShellRunas:**

Launch programs as a different user via a convenient shell context-menu entry.

**VMMAP** See a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Identify the sources of process memory usage and the memory cost of application features.

**Sysinternals Security Utilities**

**AccessChk:**

This tool shows you the level of access the user or group you specify has to files, Registry keys or Windows services.

**AccessEnum:**

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

**Autologon:**

Bypass password screen during login.

**Autoruns:**

See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

**LogonSessions:**

List active logon sessions

**Process Explorer:**

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

**PsExec:**

Execute processes with limited-user rights.

**PsLoggedOn:**

Show users logged on to a system.

**PsLogList:**

Dump event log records.

**PsTools:**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

**Rootkit Revealer:**

RootkitRevealer is an advanced rootkit detection utility.

**SDelete:**

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

**ShareEnum:**

Scan file shares on your network and view their security settings to close security holes.

**ShellRunas:**

Launch programs as a different user via a convenient shell context-menu entry.

**Sigcheck:**

Dump file version information and verify that images on your system are digitally signed.

**Sysmon:**

Monitors and reports key system activity via the Windows event log.

## **Sysinternals System Information Utilities**

### **Autoruns:**

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

### **ClockRes:**

View the resolution of the system clock, which is also the maximum timer resolution.

### **Coreinfo:**

Coreinfo is a command-line utility that shows you the mapping between logical processors and the physical processor, NUMA node, and socket on which they reside, as well as the cache's assigned to each logical processor.

### **Handle:**

This handy command-line utility will show you what files are open by which processes, and much more.

### **LiveKd:**

Use Microsoft kernel debuggers to examine a live system.

### **LoadOrder:**

See the order in which devices are loaded on your WinNT/2K system.

### **LogonSessions:**

List the active logon sessions on a system.

### **PendMoves:**

Enumerate the list of file rename and delete commands that will be executed the next boot.

### **Process Explorer:**

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

### **Process Monitor:**

Monitor file system, Registry, process, thread and DLL activity in real-time.

### **ProcFeatures:**

This applet reports processor and Windows support for Physical Address Extensions and No Execute buffer overflow protection.

### **PsInfo:**

Obtain information about a system.

**PsLoggedOn:**

Show users logged on to a system.

**PsTools:**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

**RAMMap:**

An advanced physical memory usage analysis utility that presents usage information in different ways on its several different tabs.

**WinObj:**

The ultimate Object Manager namespace viewer is here.

**Sysinternals Miscellaneous Utilities****AD Explorer:**

Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.

**AdRestore:**

Restore tombstoned Active Directory objects in Server 2003 domains.

**Autologon:**

Bypass password screen during logon.

**BgInfo:**

This fully-configurable program automatically generates desktop backgrounds that include important information about the system including IP addresses, computer name, network adapters, and more.

**BlueScreen:**

This screen saver not only accurately simulates Blue Screens, but simulated reboots as well (complete with CHKDSK), and works on Windows Vista, Server 2008 and higher.

**Ctrl2cap:**

This is a kernel-mode driver that demonstrates keyboard input filtering just above the keyboard class driver in order to turn caps-locks into control keys. Filtering at this level allows conversion and hiding of keys before NT even "sees" them. Ctrl2cap also shows how to use NtDisplayString() to print messages to the initialization blue-screen.

**DebugView:**

Another first from Sysinternals: This program intercepts calls made to DbgPrint by device drivers and OutputDebugString made by Win32 programs. It allows for viewing and recording of debug session output on your local machine or across the Internet without an active debugger.



**Desktops:**

This new utility enables you to create up to four virtual desktops and to use a tray interface or hotkeys to preview what's on each desktop and easily switch between them.

**Hex2dec:**

Convert hex numbers to decimal and vice versa.

**NotMyFault:**

Notmyfault is a tool that you can use to crash, hang, and cause kernel memory leaks on your Windows system.

**PsLogList:**

Dump event log records.

**PsTools:**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

**RegDelNull:**

Scan for and delete Registry keys that contain embedded null-characters that are otherwise undeleteable by standard Registry-editing tools.

**Registry Usage (RU):**

View the registry space usage for the specified registry key.

**RegJump:**

Jump to the registry path you specify in Regedit.

**Strings:**

Search for ANSI and UNICODE strings in binary images.

**ZoomIt:**

Presentation utility for zooming and drawing on the screen.

**2) Monitor Live Processes (Tool: ProcMon)**

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 5952512, L...
12:25...	svchost.exe	1048	Thread Create		SUCCESS	Thread ID: 7696
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 18472960, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 6213632, L...
12:25...	SearchIndexer...	9472	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2332672, L...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 18489344, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 5891072, L...
12:25...	SearchIndexer...	9472	FileSystemControl C:		SUCCESS	Control: FSCTL_R...
12:25...	SearchIndexer...	9472	FileSystemControl C:		SUCCESS	Control: FSCTL_R...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 17502208, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\WinSxS\amd64_microsoft...	SUCCESS	Offset: 2104832, L...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 17207296, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\WinSxS\amd64_microsoft...	SUCCESS	Offset: 2092544, L...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 17113088, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6620160, L...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 17252352, ...
12:25...	Explorer.EXE	6980	CloseFile	C:\Windows\SystemApps\Microsoft.Mic...	SUCCESS	
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 16994304, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6505472, L...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 18538496, ...
12:25...	Explorer.EXE	6980	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 5907456, L...
12:25...	MsMpEng.exe	2328	ReadFile	C:\ProgramData\Microsoft\Windows De...	SUCCESS	Offset: 18522112, ...
12:25...	Explorer.EXE	6980	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:25...	Explorer.EXE	6980	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:25...	Explorer.EXE	6980	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:25...	Explorer.FXF	6980	RegOpenKey	HKCU\Software\Classes\Directory	SUCCESS	Desired Access: R...

Showing 196796 of 675617 events (29%) Backed by virtual memory

Process Monitor Filter

Display entries matching these conditions:

Architecture is then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process N...	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Procexp.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Autoruns.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Procmon64.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Procexp64.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	System	Exclude
<input checked="" type="checkbox"/> Operation	begins with	IRP_MJ_	Exclude

OK Cancel Apply

Click on filter → Process monitor filter

Process Monitor Filter

Display entries matching these conditions:

Architecture is chrome.exe then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Architecture	is	firefox.exe	Include
<input checked="" type="checkbox"/> Architecture	is	chrome.exe	Include
<input checked="" type="checkbox"/> Process N...	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Procexp.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Autoruns.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Procmon64.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Procexp64.exe	Exclude

OK Cancel Apply

Click on tools → Process tree

Process Tree

☐ Only show processes still running at end of current trace

☒ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Comma
Idle (0)	Idle					
System (4)		System			NT AUTHORITY\...	
smss.exe (500)	Windows Session ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\System
MemCompression (2792)	MemCompression				NT AUTHORITY\...	
csrss.exe (668)	Client Server Runt...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	%Syste
wininit.exe (772)	Windows Start-Up...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	wininit.e
services.exe (844)	Services and Cont...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Winc
svchost.exe (448)	Host Process for ...	c:\windows\syste...		Microsoft Corporat...	NT AUTHORITY\...	c:\wind
svchost.exe (460)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Winc
wmiprvse.exe (6760)	WMI Provider Host	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Winc
wmiprvse.exe (7252)	WMI Provider Host	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Winc
ShellExperienceHost.exe (7516)	Windows Shell Ex...	C:\Windows\Syst...		Microsoft Corporat...	STUDENT005\St...	"C:\Wir
SearchUI.exe (7516)	Search and Corta...	C:\Windows\Syst...		Microsoft Corporat...	STUDENT005\St...	"C:\Wir
RuntimeBroker.exe (7604)	Runtime Broker	C:\Windows\Syst...		Microsoft Corporat...	STUDENT005\St...	C:\Winc
RuntimeBroker.exe (8360)	Runtime Broker	C:\Windows\Syst...		Microsoft Corporat...	STUDENT005\St...	C:\Winc
RuntimeBroker.exe (8488)	Runtime Broker	C:\Windows\Syst...		Microsoft Corporat...	STUDENT005\St...	C:\Winc
SppExtComObj.exe (9172)	KMS Connection ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Winc
DllHost.exe (9492)	COM Surrogate	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Winc

Description:

Company:

Path: Idle

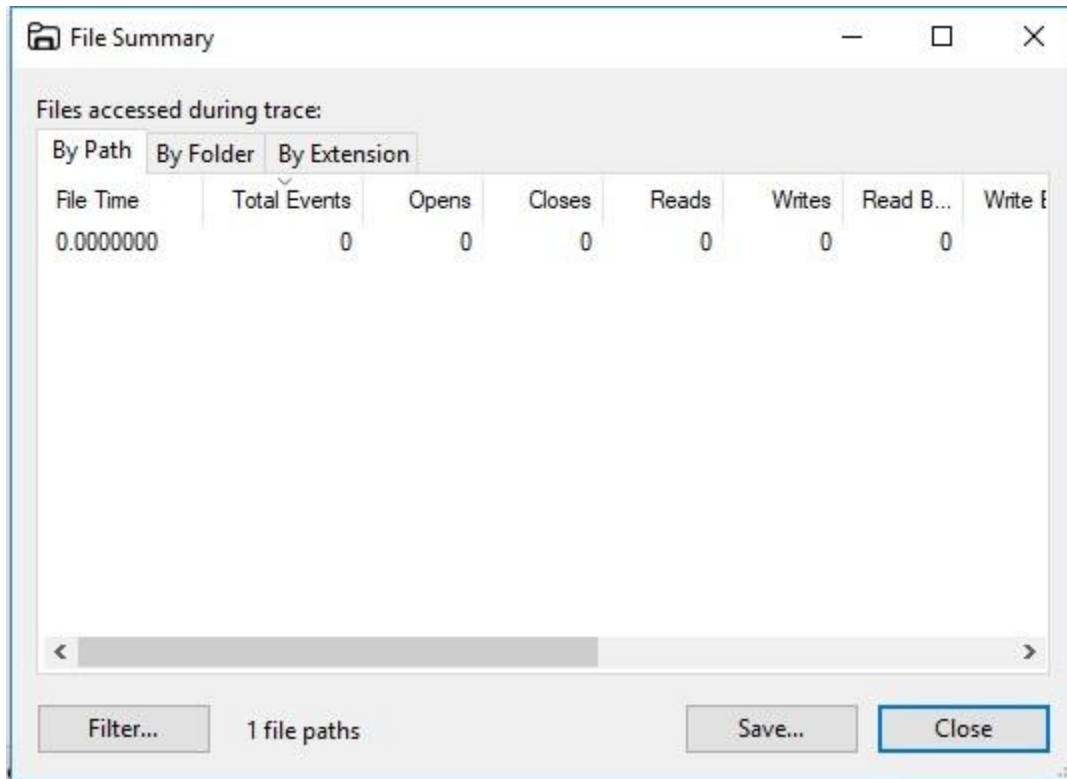
Command:

User:

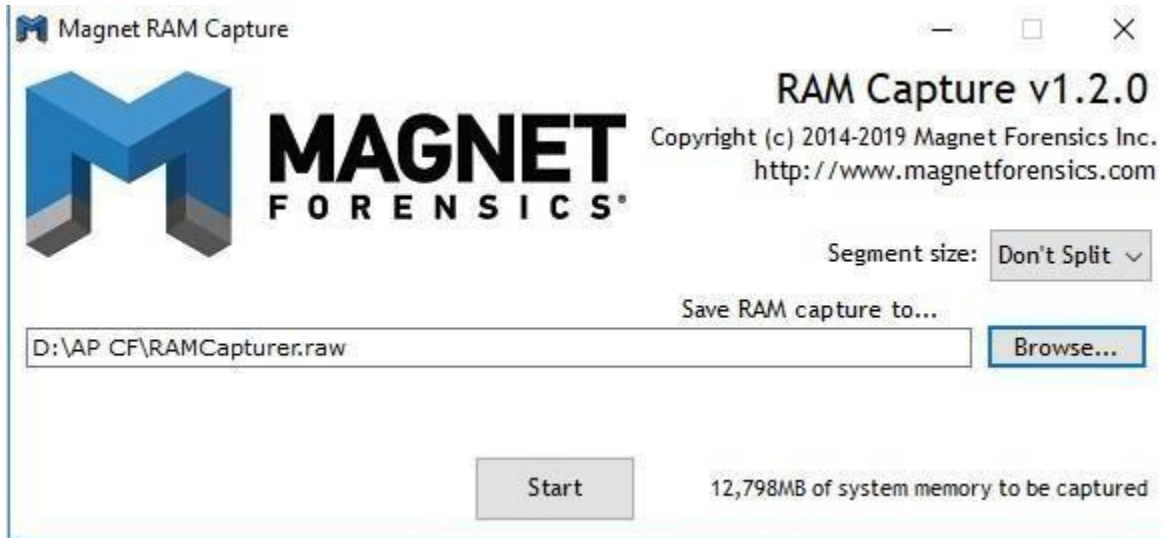
PID: 0 Started: 15-01-2025 10:59:29

Go To Event Include Process Include Subtree Close

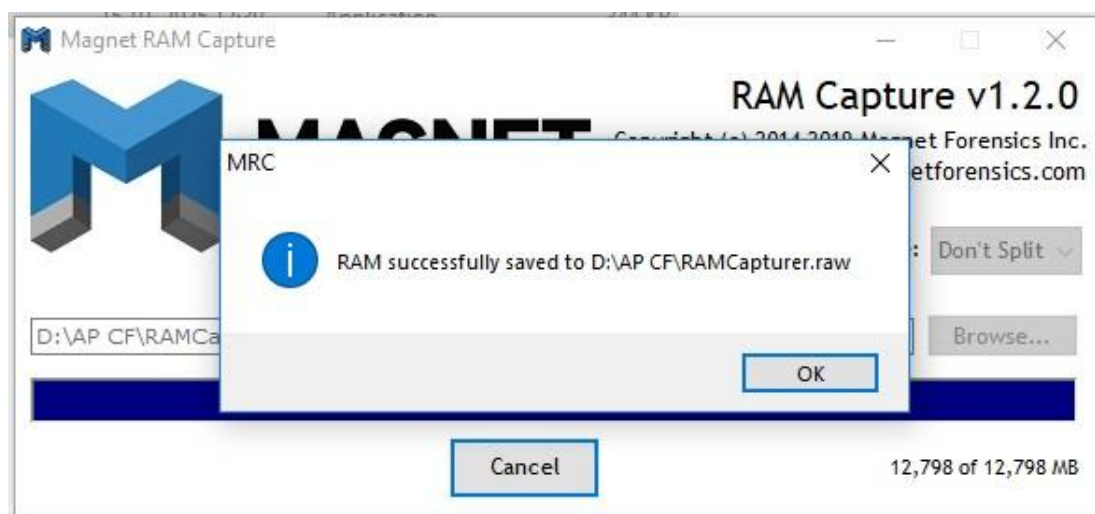
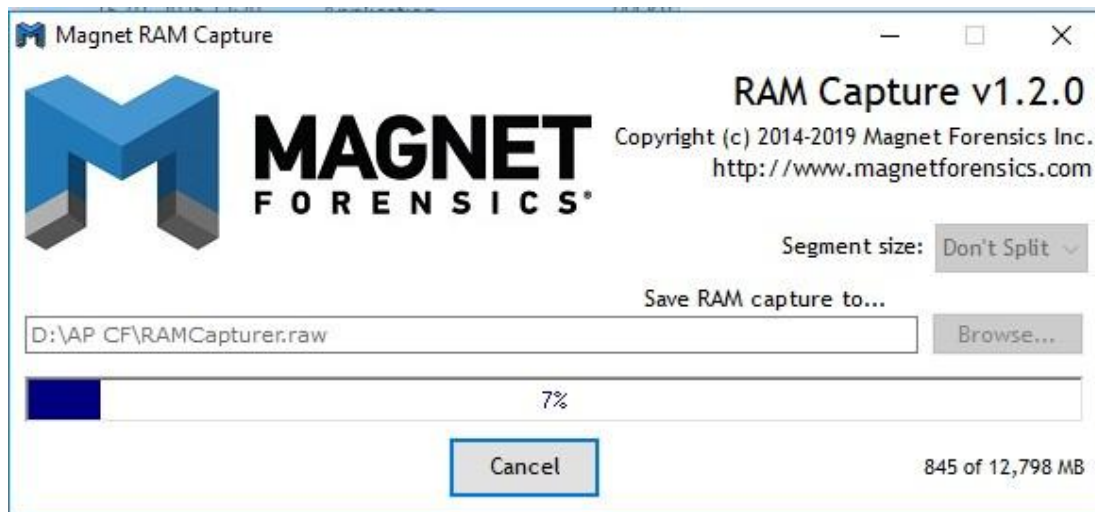
Click on Tools → File Summary



3) Capture RAM (Tool: RAMCapture) Open the



Ramcapture tool.



#### 4) Capture TCP/UDP packets (Tool: TcpView) Open the Tcpview tool.

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

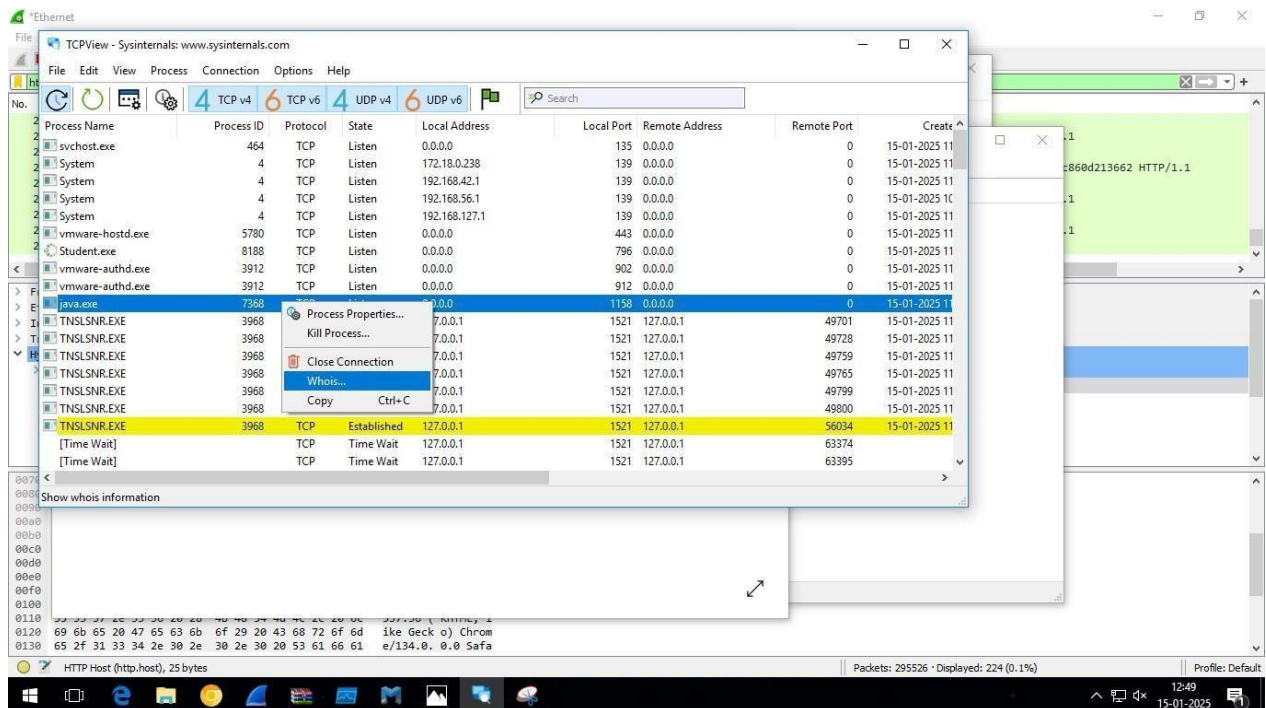
Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
svchost.exe	464	TCP	Listen	0.0.0.0	135	0.0.0.0	0	15-01-2025 11
System	4	TCP	Listen	172.18.0.238	139	0.0.0.0	0	15-01-2025 11
System	4	TCP	Listen	192.168.42.1	139	0.0.0.0	0	15-01-2025 11
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	15-01-2025 11
System	4	TCP	Listen	192.168.127.1	139	0.0.0.0	0	15-01-2025 11
vmware-hostd.exe	5780	TCP	Listen	0.0.0.0	443	0.0.0.0	0	15-01-2025 11
Student.exe	8188	TCP	Listen	0.0.0.0	796	0.0.0.0	0	15-01-2025 11
vmware-authd.exe	3912	TCP	Listen	0.0.0.0	902	0.0.0.0	0	15-01-2025 11
vmware-authd.exe	3912	TCP	Listen	0.0.0.0	912	0.0.0.0	0	15-01-2025 11
java.exe	7368	TCP	Listen	0.0.0.0	1158	0.0.0.0	0	15-01-2025 11
TNLSNR.EXE	3968	TCP	Listen	127.0.0.1	1521	0.0.0.0	0	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49676	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49701	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49728	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49730	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49759	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49762	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49765	15-01-2025 11
TNLSNR.EXE	3968	TCP	Established	127.0.0.1	1521	127.0.0.1	49799	15-01-2025 11

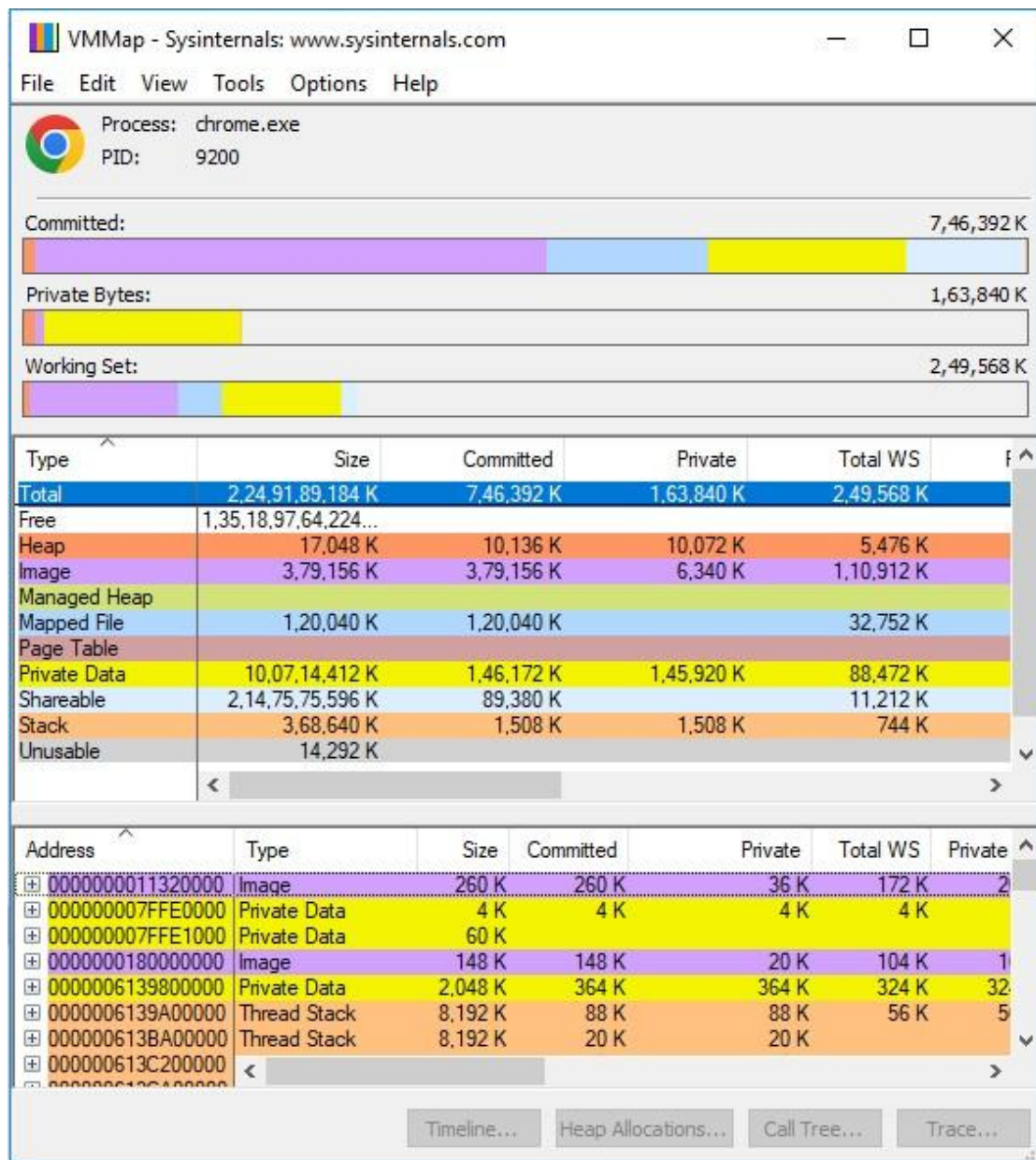
Endpoints: 159 Established: 31 Listening: 52 Time Wait: 6 Close Wait: 1 Update: 2 sec States: (All)

Right click on any packet → whois

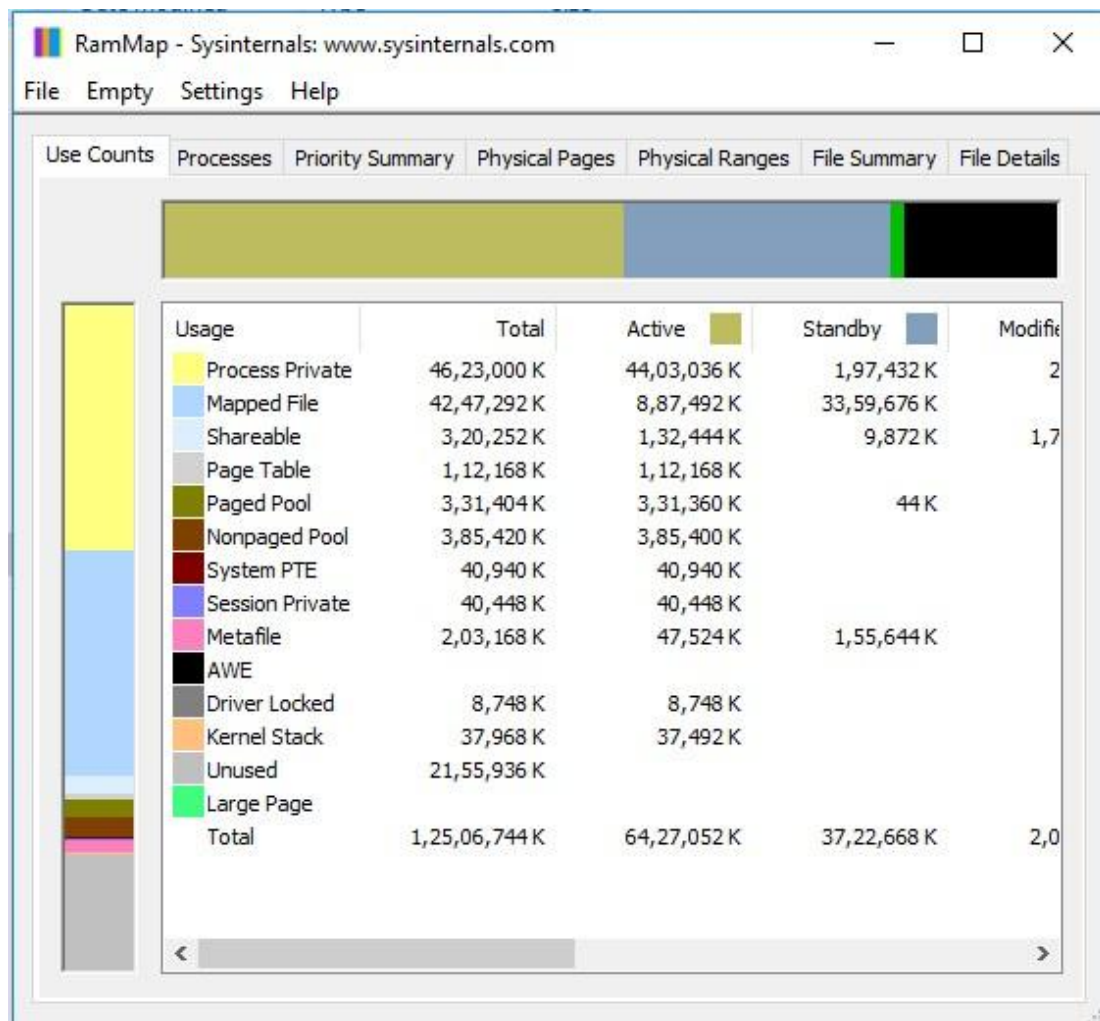




5) Monitor Hard Disk (Tool: DiskMon) Open the Diskmon tool. 6) Monitor Virtual Memory (Tool: VMMap) Open the VMMap tool.



7) Monitor Cache Memory (Tool: RAMMap) Open the RAMMap tool.



## Practical 7

**Date:** 18-01-25

**Aim:** Email Forensics

- Mail Service Providers
- Email protocols
- Recovering emails
- Analyzing email header

**Mail Service Providers:**

Mail servers, also known as email servers, are used to store, send, and receive emails. Email forensics is a type of digital forensics that uses email server logs to investigate crimes.

**How are mail servers used in cyber forensics?**

**Email server logs:**

Email server logs can contain information like IP addresses, timestamps, and user activity. This information can help investigators reconstruct the sequence of events.

**Email forensic tools:**



Email forensic tools can process, clean, and extract information from emails. This information can help analysts solve investigations.

Examples of mail servers are Gmail and Yahoo.

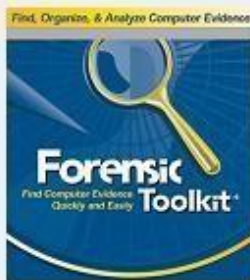


Start AccessData FTK by right-clicking the AccessData FTK desktop icon, clicking Runas administrator, and clicking Continue in the UAC message box (if you're using Vista). If you're prompted with a warning message and/or notification (see Figure below), click OK as needed to continue. If asked whether you want to save the existing default case, click Yes.

**Step 1:** When the "AccessData FTK Startup" opens click on "Start new Case"



**Step 2:** In the New Case dialog box, type your name for the investigator name, and type the case number and case name. Click Browse, navigate to and click your work folder, click OK, and then click Next.



**AccessData's**  
**Forensic Toolkit®-FTK®**  
*The Complete Analysis Tool*

**Wizard for Creating a New Case**

Investigator Name: XYZ

Case Information

Case Number: 1

Case Name: ABC

Case Path: D:\siddy\

Browse...

Case Folder: D:\siddy\ABC

Case Description:

Next >

Cancel

In the Case Information dialog box, enter your investigator information, and then click Next.

FTK Report Wizard - Case Information

### Forensic Examiner Information

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

Agency/Company: Model

Examiner's Name: abc

Address: mumbai

Phone: 9895647218 Fax: 2

E-Mail: test@gmail.com

Comments: none

< Back Next > Cancel

Following page will appear just click on next.

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

Click Next until you reach the Refine Case - Default dialog box, shown below and select the “Email Emphasis” then click on Next.

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

☐ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)

☐ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)

☐ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

☐ 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

File Status Criteria

Deletion Status:

Encryption Status:

Email Status:

☐ Deleted

☐ Encrypted

☒ From email

☐ Not deleted

☐ Not encrypted

☐ Not from email

☒ Either

☒ Either

☐ Either

☐ Include Duplicate Files

☐ OLE Streams

File Type Criteria

☒ Documents

☐ Executables

☒ Spreadsheets

☒ Archives

☒ Databases

☐ Folders

☒ Graphics

☒ Other Known

☒ Multimedia

☒ Unknown

☒ Email msgs

< Back

Next >

Cancel

Click Next until you reach the Add Evidence to Case dialog box, and then click the “Add Evidence” button and select “Individual File” and click on continue.

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
--------------	--------	----------	------	---------	-----------	---------

Add Evidence to Case

Type of Evidence to Add to Case

☐ Acquired Image of Drive

☐ Local Drive

☐ Contents of a Folder

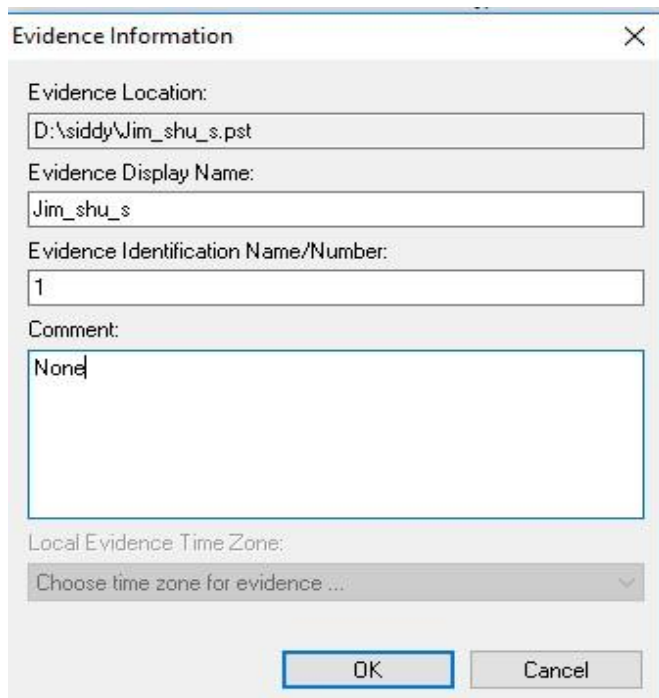
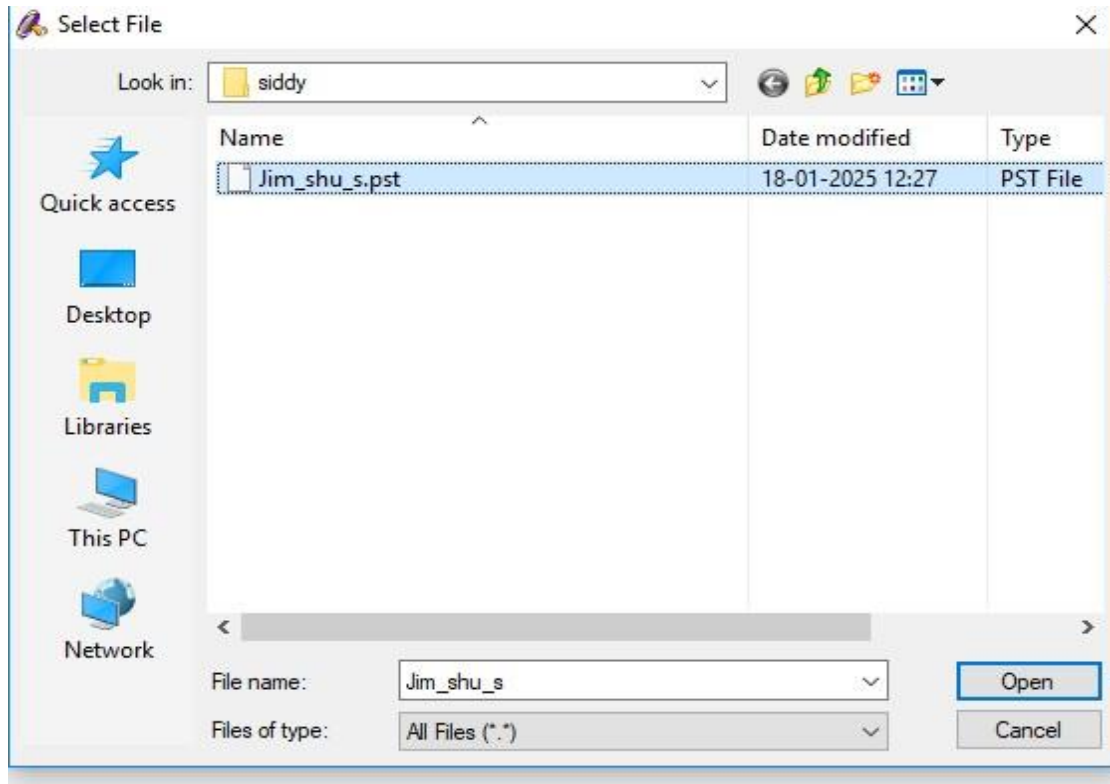
☒ Individual File

Continue... Cancel

< Back Next > Cancel



Search for the required file as shown below and click on Open.



**Step 8:** A window like this will appear.Click on Ok.



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...

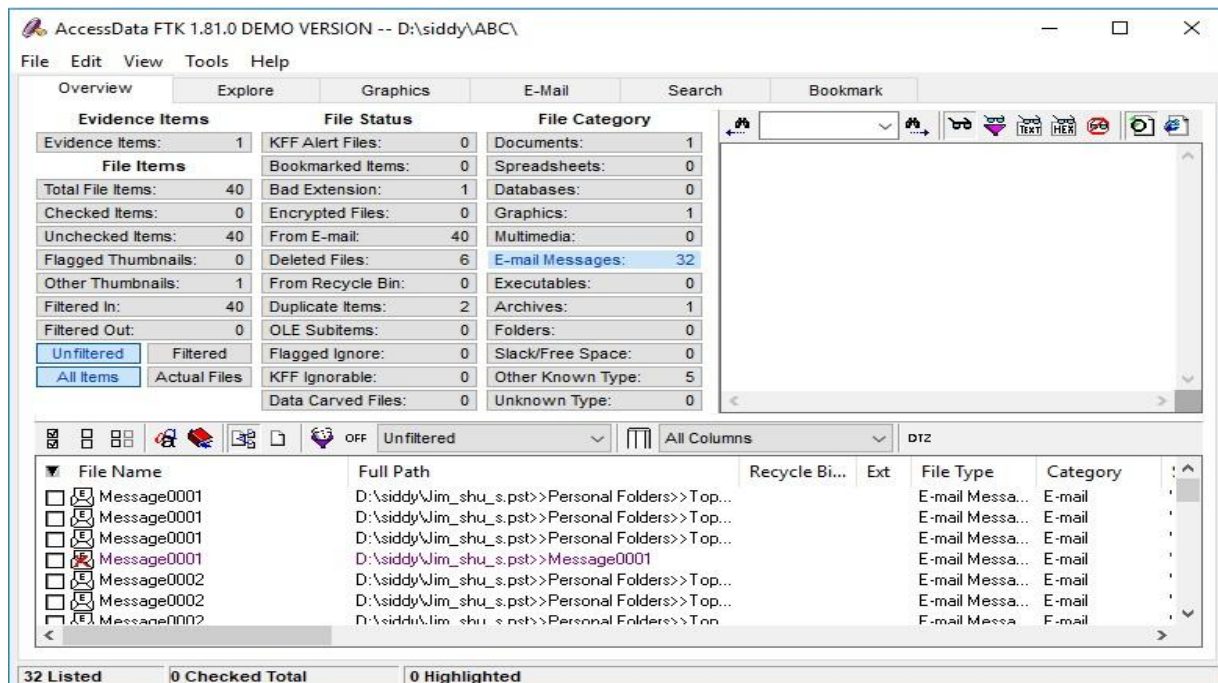
Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
Jim_shu_s	D:\siddy\Jim_...	1	Individual f...	N	N/A	None

< Back

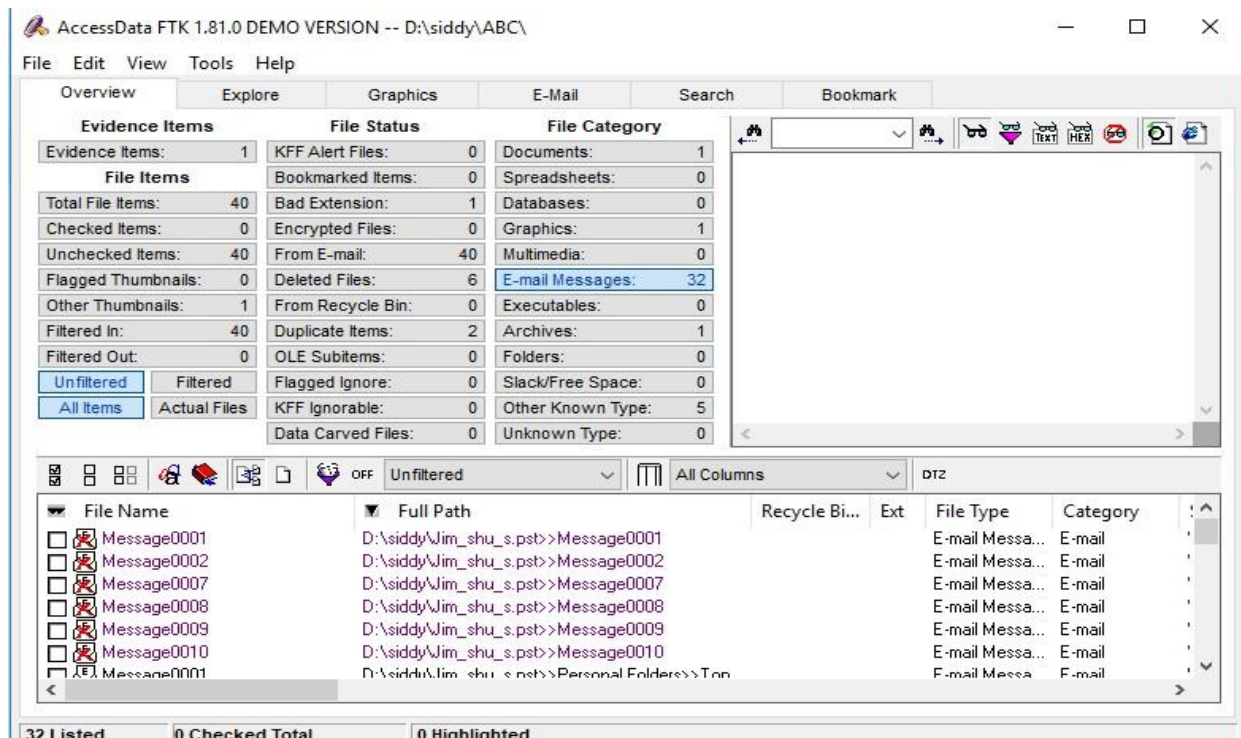
Next >

Cancel

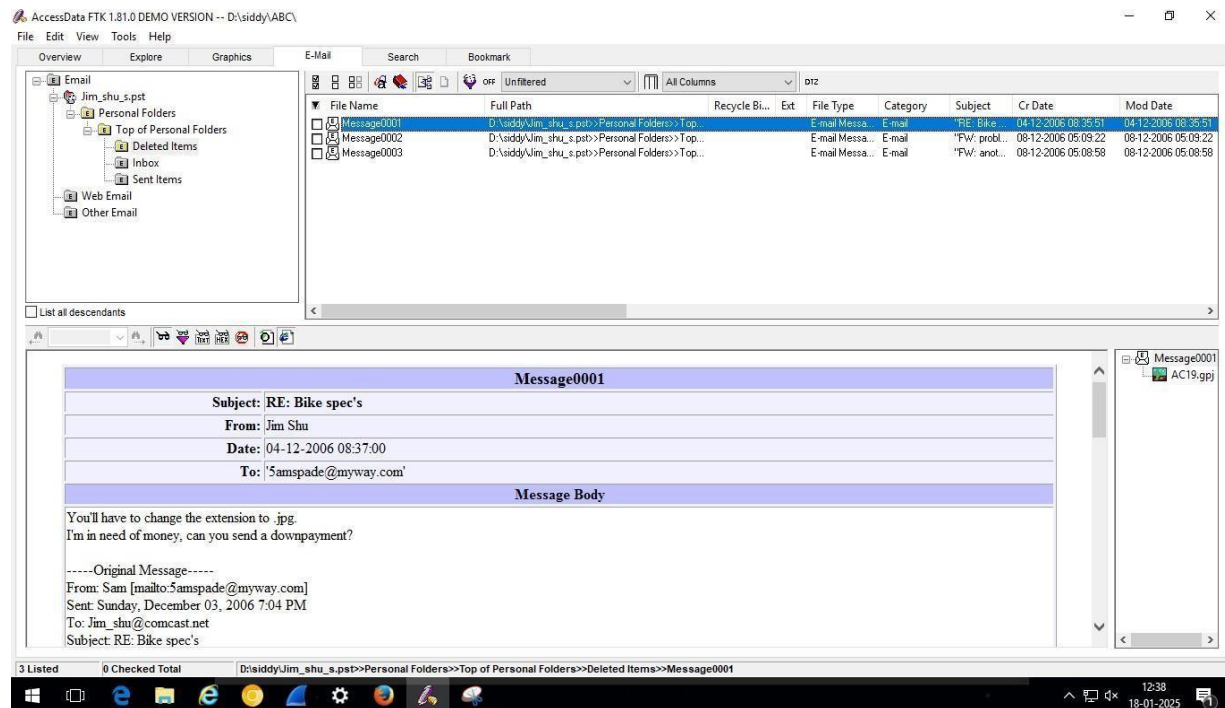
**Step 9:** After clicking on Next the following window will appear as follows. Click on Email Messages.



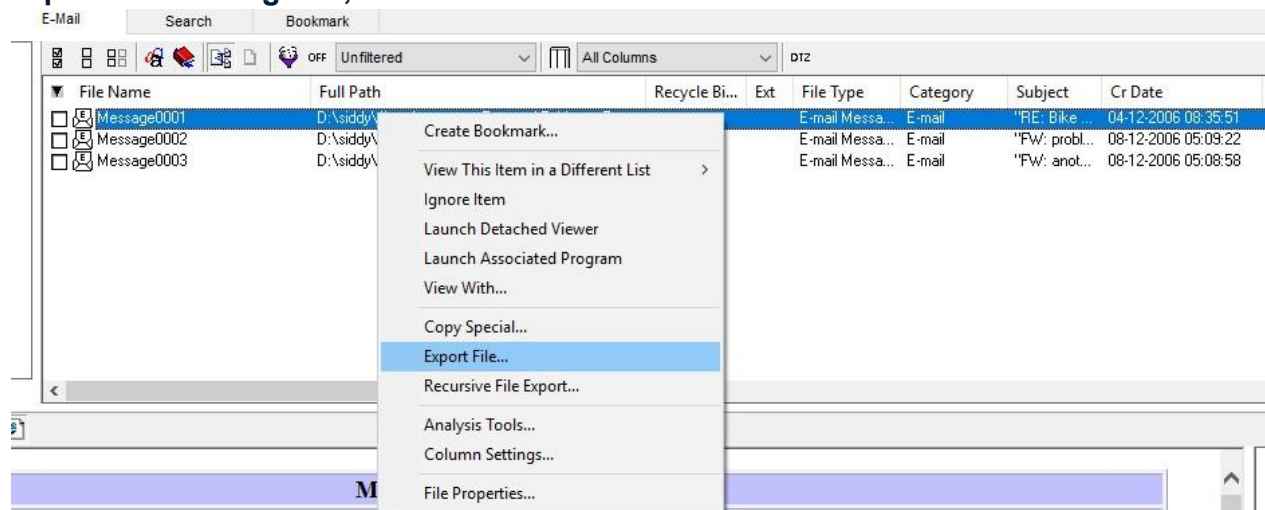
**Step 10:** When FTK finishes processing the file, in the main FTK window, click the Email Messages button, and then click the Full Path column header to sort the records.

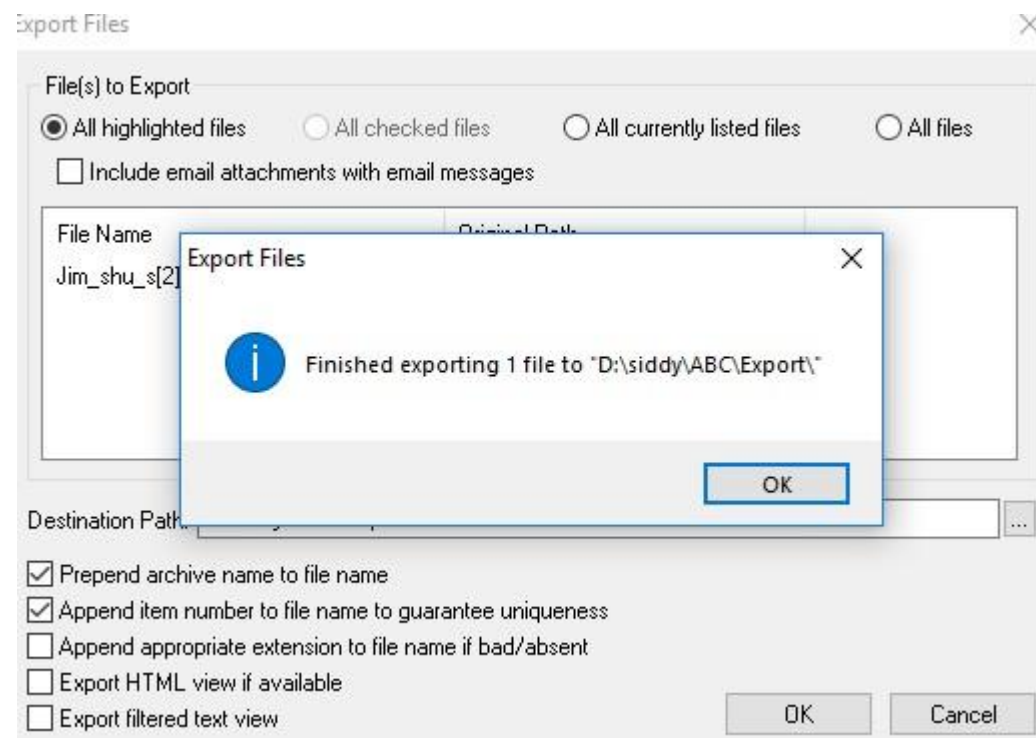
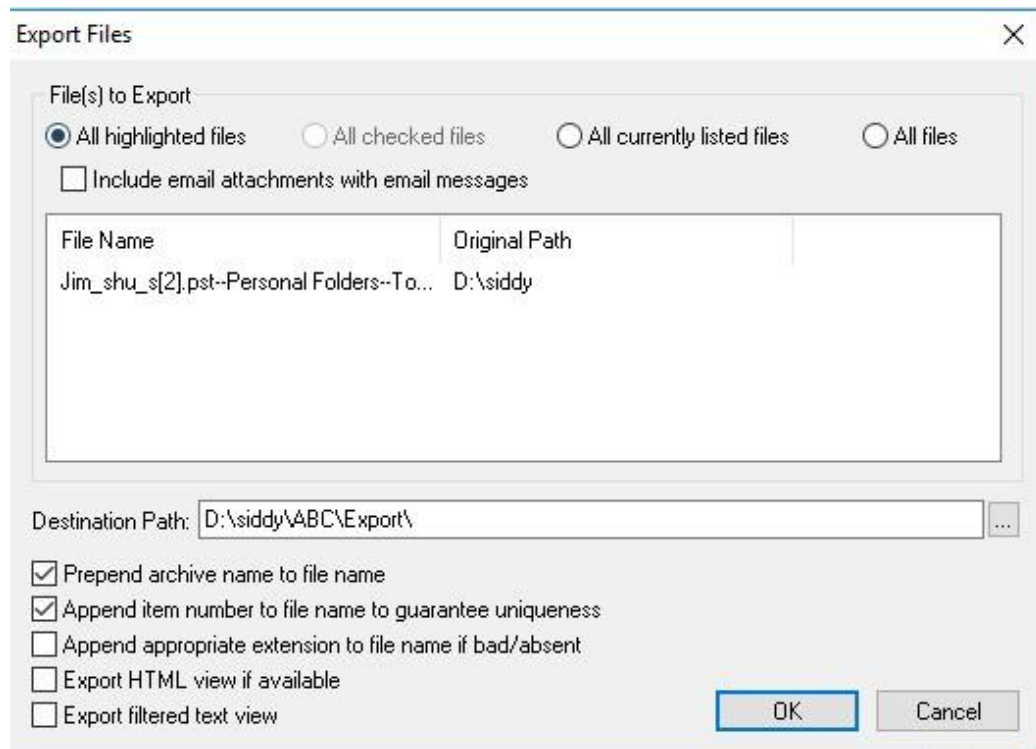


**Step 11:** Click the EMail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder.



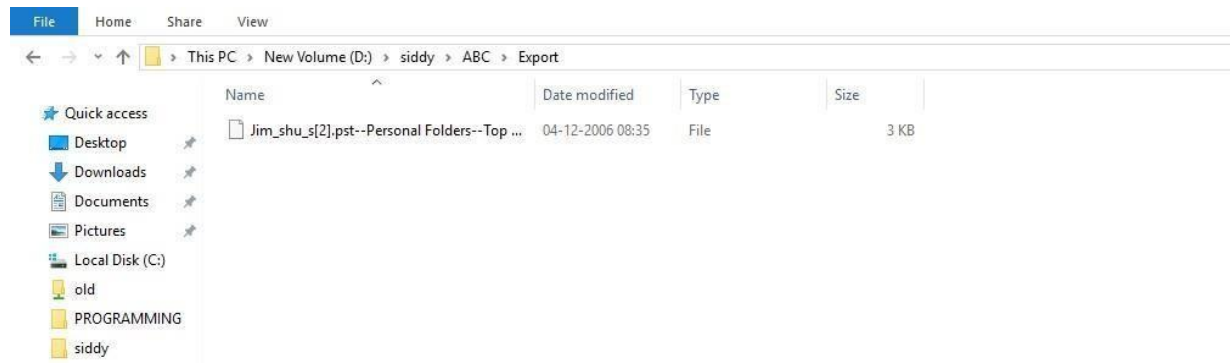
**Step 12:** Right-click Message0001 in the File List pane and click Export File. In the Export Files dialog box, click OK.



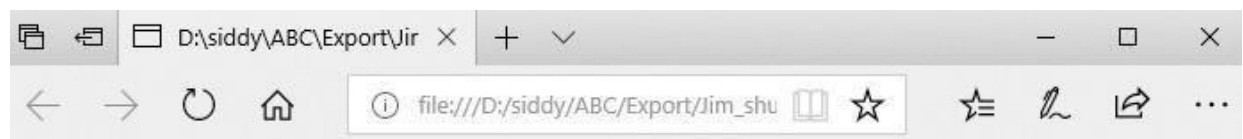
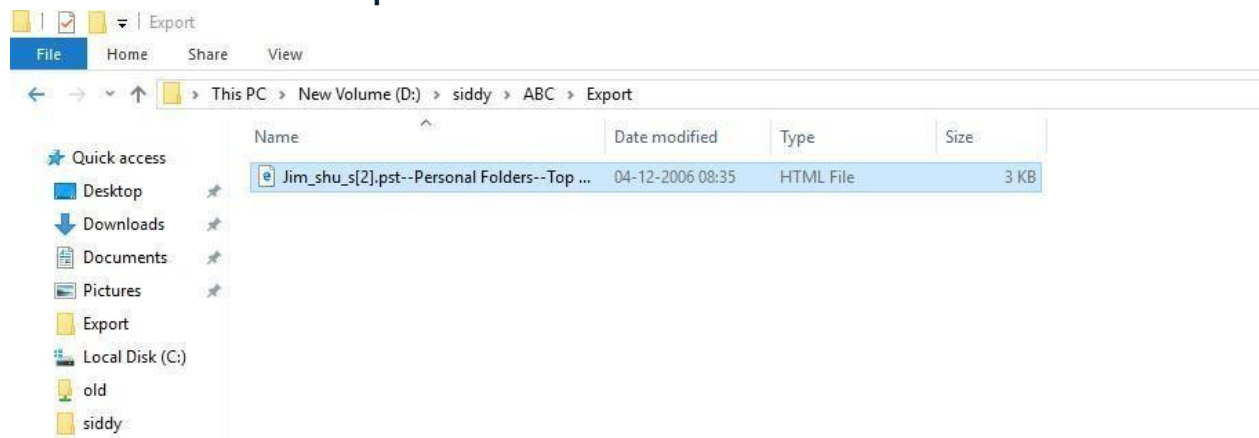


**Step 13:** Open the Export folder to view the Email Files, Open the HTML file in the browser.





**Step 14: For analyzing header follow following steps Right Click the file type and Rename it to HTML and open in browser to view header Information.**



Conversation Topic: Bike spec's Subject: RE: Bike spec's From: Jim Shu Sender Name: Jim Shu To: '5amspade@myway.com' Delivery Time: 04-12-2006 08:37:00 Creation Time: 04-12-2006 08:35:51 Modification Time: 04-12-2006 08:35:51 Submit Time: 04-12-2006 08:37:16 Importance: Normal Priority: Normal Sensitivity: Normal Flags: 17 = Read, Has Attachment Size: 14360 You'll have to change the extension to .jpg. I'm in need of money, can you send a downpayment? -----Original Message----- From: Sam [mailto:5amspade@myway.com] Sent: Sunday, December 03, 2006 7:04 PM To: Jim\_shu@comcast.net Subject: RE: Bike spec's I think I can raise another 5 for you. Do you have something I can look at yet? --- On Sun 12/03, Jim Shu <Jim\_shu@comcast.net> wrote: From: Jim Shu [mailto:Jim\_shu@comcast.net] To: 5amspade@myway.com Date: Sun, 3 Dec 2006 18:09:06 -0800 Subject: RE: Bike spec's How much are you willing to pay me to get these plans to you? Jim-----Original Message-----From: Sam [mailto:5amspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PM To: jim\_shu@comcast.net Subject: Bike spec's Do you have them yet? I've got people in Asia ready to duplicate them? Sam No banners. No pop-ups. No kidding. Make My Way your home on the Web - <http://www.myway.com> No banners. No pop-ups. No kidding. Make My Way your home on the Web - <http://www.myway.com> -----Attachment----- AC19.gpj

## **Practical 8**

**Date:** 08-02-25

**Aim:** Recovering and Inspecting deleted files

-Check for Deleted Files

-Recover the Deleted Files

-Analyzing and Inspecting the recovered files

**Step 1:** Open AccessData FTK Imager. Click on File → Create Disk Image.

**Step 2:** From the “Select Source” Dialogbox select the option of “Contents of a folder”. Click on Next.

**Step 3:** Here browse and enter the source path of the file. Click on Finish.

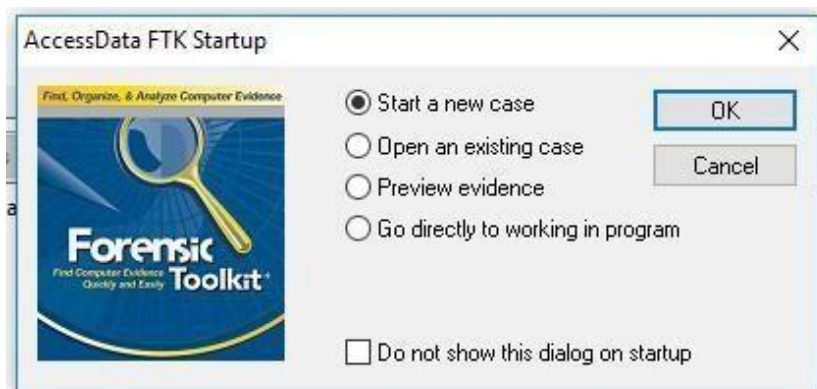
**Step 4:** Now click on the “Add” button and check the options of “Verify images after they are created” and “Precalculate progress statistics”.

**Step 5:** After clicking on “Add” browse the “Image Destination Folder” and type the Image Filename. Click on Finish.

**Step 6:** Here we can see the Image Destination. Now click on “Start”.

**Step 7:** Here the Image is being created. Proceed to click on “Image Summary” for the results.

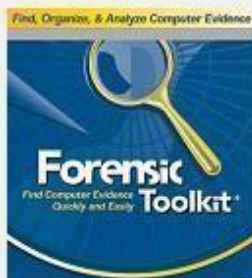
Here we can see the Drive/Image Verify Results.



**Step 8:** Open the Forensic toolkit and click on file > new case.

**Step 9:** Enter the details and click on next.

New Case



# AccessData's Forensic Toolkit®-FTK® *The Complete Analysis Tool*

## Wizard for Creating a New Case

Investigator Name: athulya

### Case Information

Case Number: 120

Case Name: Pr8

Case Path: D:\AP CF\

Browse...

Case Folder: D:\AP CF\Pr8

### Case Description:

none

Next >

Cancel

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

**Step 10: Click on next.**

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.

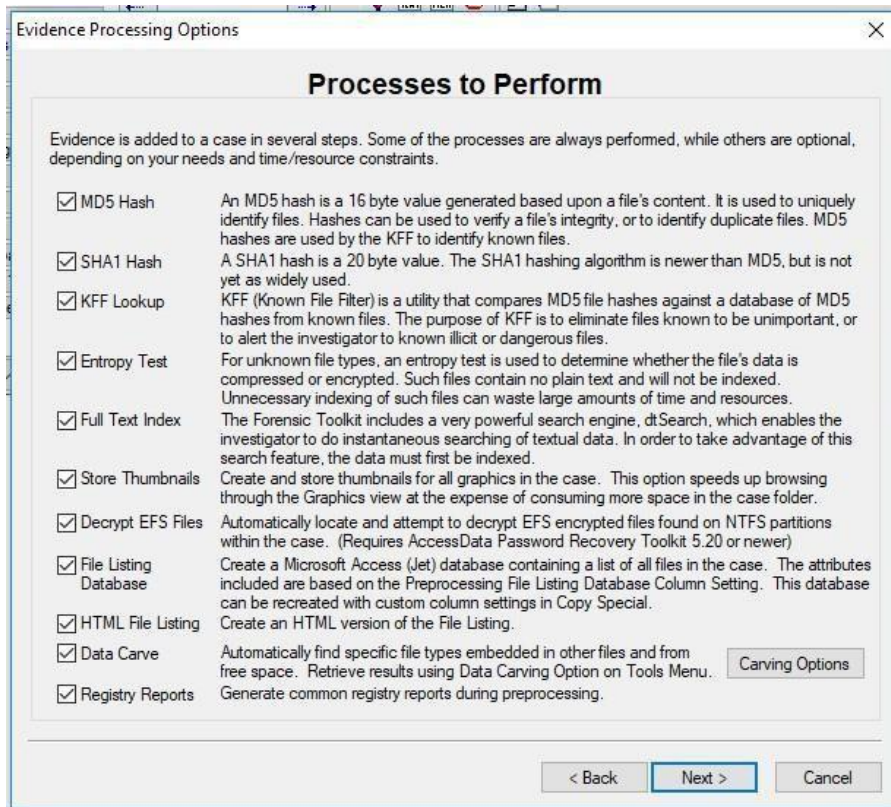
Events to go in the Case Log

<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.

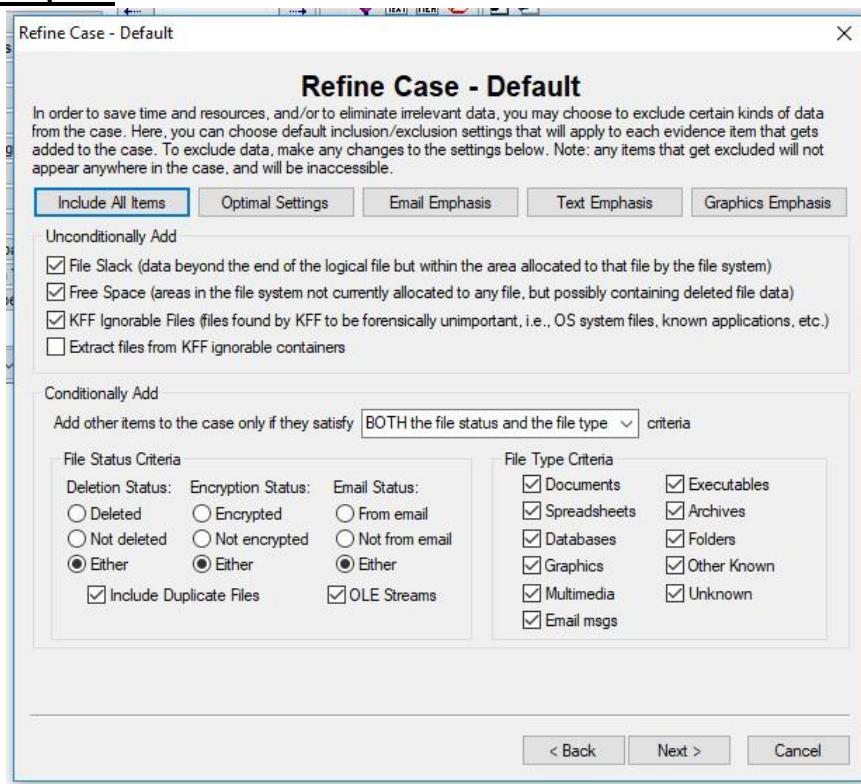
< Back Next > Cancel

**Step 11: Click on next.**

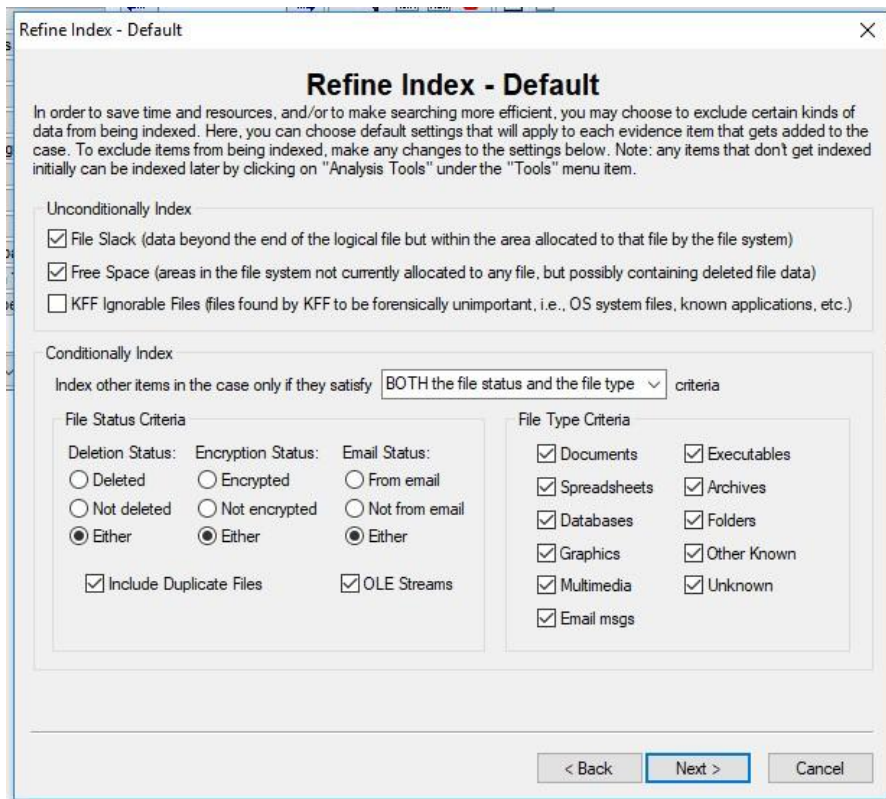




## Step 12: Click on next.



**Step 13:** Click on next.



The image shows a Windows-style dialog box titled "Refine Index - Default". It contains instructions on how to refine the index by excluding certain data. The dialog is divided into two main sections: "Unconditionally Index" and "Conditionally Index".

**Unconditionally Index**

- ☒ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- ☒ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- ☐ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

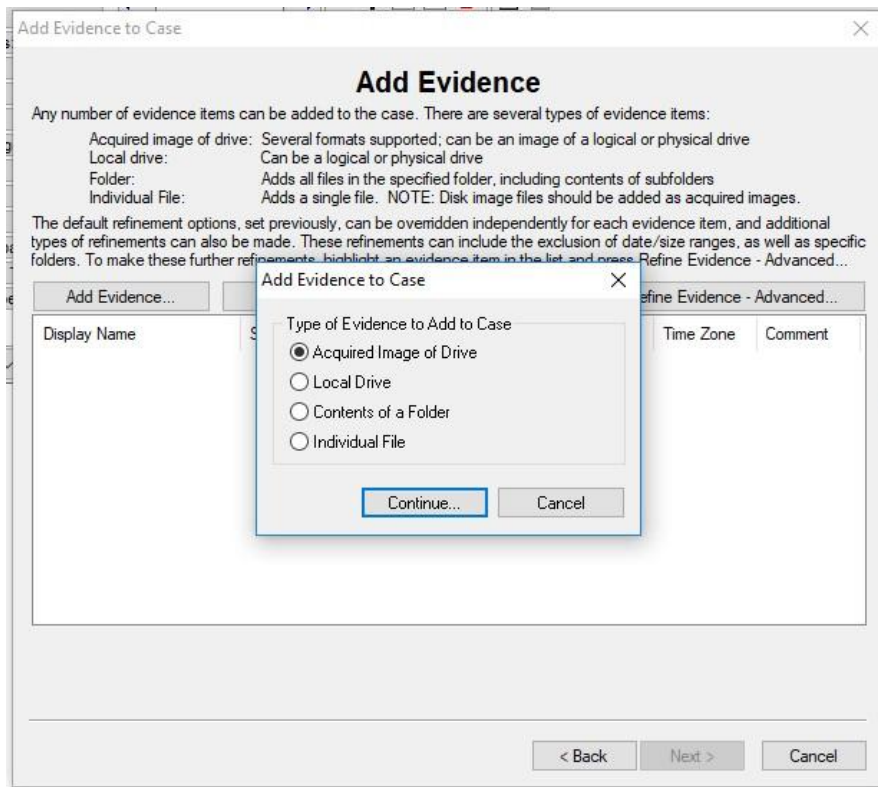
**Conditionally Index**

Index other items in the case only if they satisfy BOTH the file status and the file type criteria

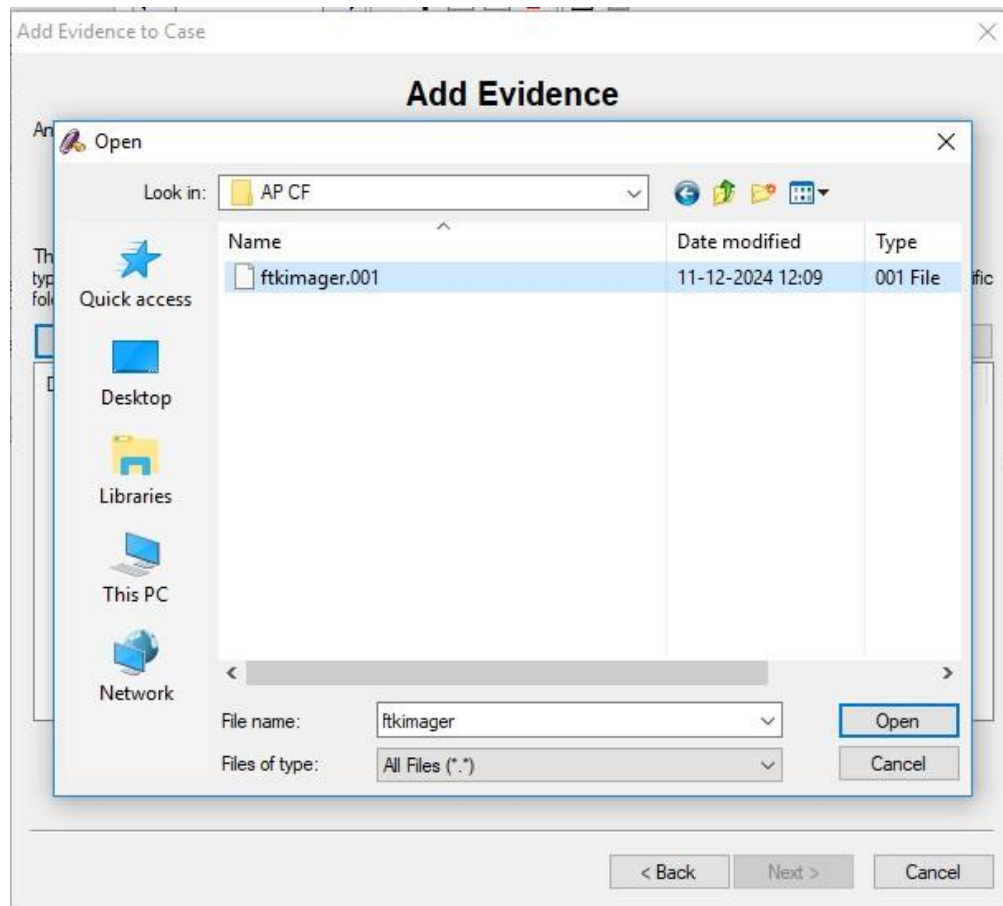
File Status Criteria			File Type Criteria	
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> 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	

At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

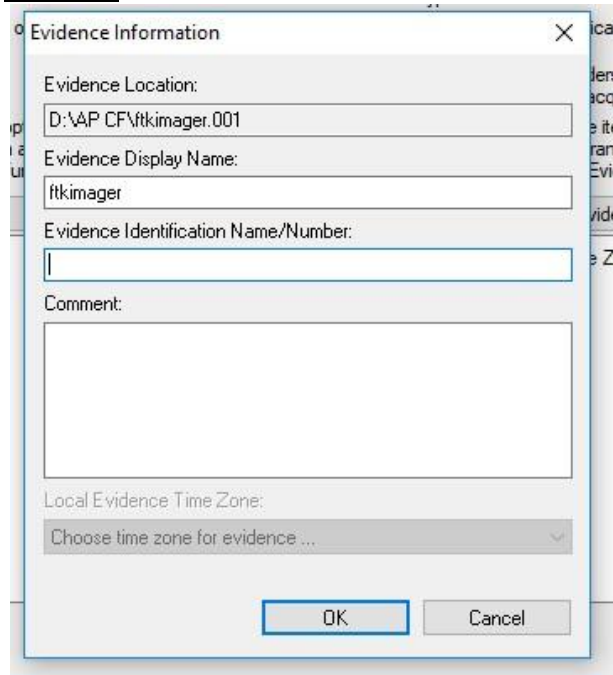
**Step 14:** Click on Add Evidence → Acquired Image of Drive → Continue.



**Step 15: Select the image file.**



**Step 16: Click on OK.**



**Step 17: Click on next.**

**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...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
ftkimager\Part_1\NONAM...	D:\AP CF\ftki...		File system	N	N/A	
ftkimager\UnpartSpace	D:\AP CF\ftki...		Unpartition...	N	N/A	

**Step 18: Click on Finish.**

**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:

Number of Evidence Items: 2

Processes to be Performed:

File Extraction:	Yes	
File Identification:	Yes	Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
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:	Yes	
Data Carving:	Yes	
Registry Reports:	Yes	

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

**Step 19:** Files are being carving.



Processing Files...

Current Evidence Item:  
D:\AP CF\ftkimager.001

Current File Item:  
ftkimager\Part\_1\NONAME-Unknown\DriveFreeSpace0008

Current File Item Status

Action:	Filtering Text
File Type:	Drive Free Space
Item Size:	26,214,400 (8 of 19078)
Progress:	17,798,247

Total Process Status

Elapsed Time:	0.00:00:06
Total Items Examined:	8
Total Items Added:	8
Total Items Indexed:	7

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

Cancel

AccessData FTK 1.81.0 DEMO VERSION -- D:\AP CF\p8\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Case

- ftkimager
  - Part\_1
    - NONAME-Unknown
      - UnpartSpace

List all descendants

File Name	Full Path	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Chi
DriveFreeSpace0001	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0002	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0003	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0004	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0005	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0006	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0007	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0008	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0009	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0010	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0011	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0012	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0013	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0014	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0015	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0016	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0017	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0018	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	
DriveFreeSpace0019	ftkimager\Part_1\NONAME-Unknown\DriveFree...	Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	26,214,400	500,107.8...	

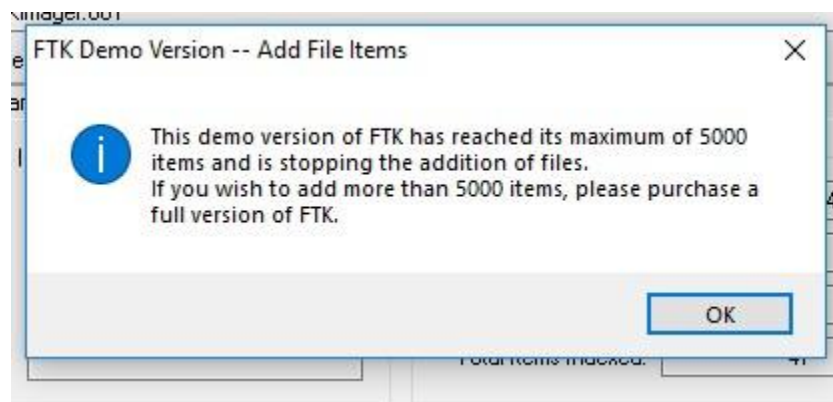
5000 Listed 0 Checked Total 0 Highlighted

11:19 05-02-2025

Carving BMP Files

Carving from file: 12/46

Abort





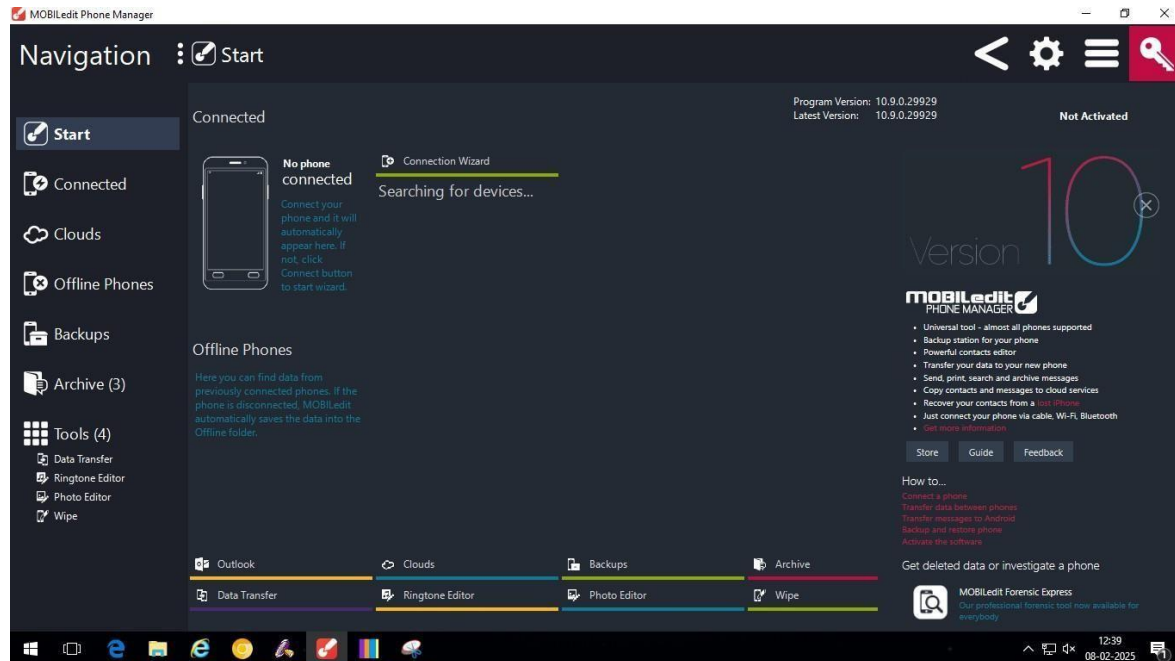
## Practical 9

Date: 08-02-25

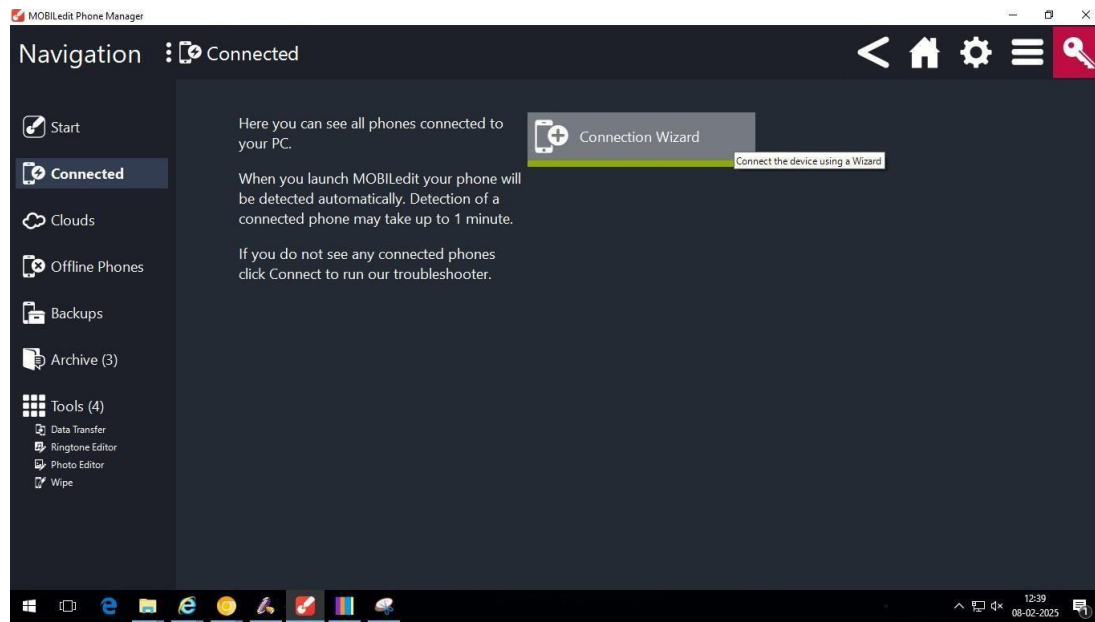
Aim: Acquisition of Cell phones and Mobile devices.

Step 1: Download mobiledit forensic tool on mobile.

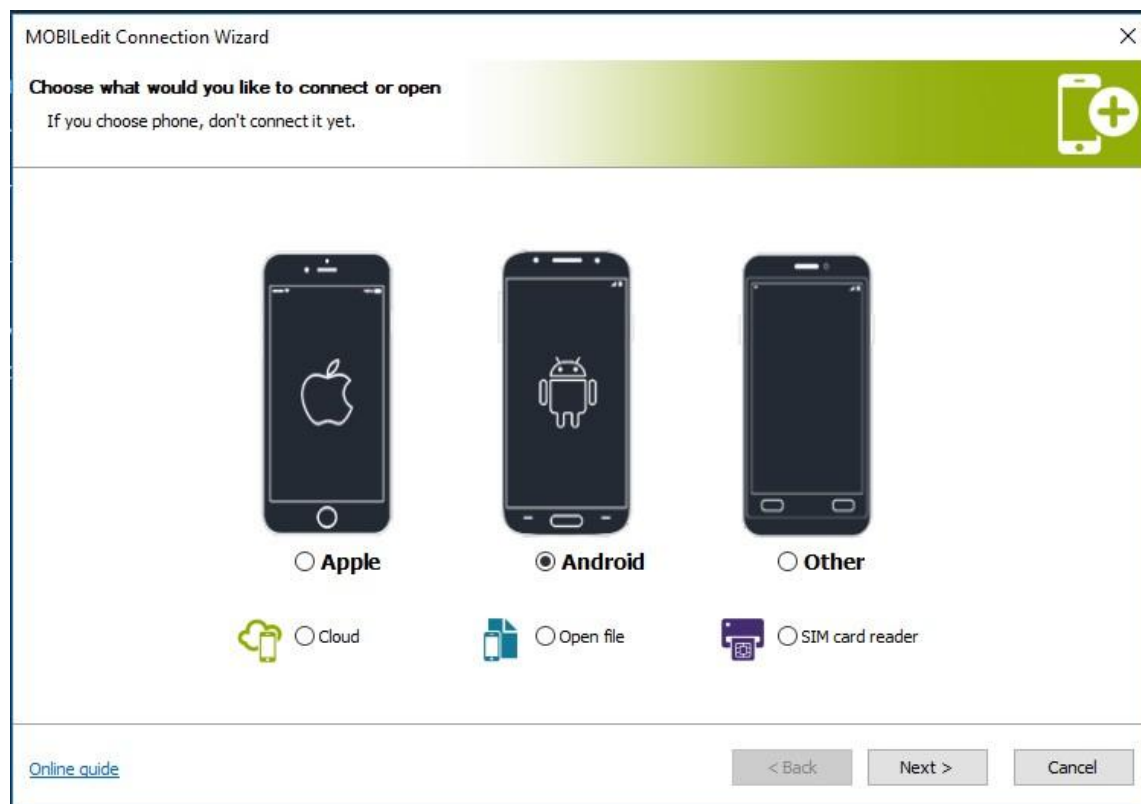
Step 2: Open Mobiledit tool on PC.



Step 3: Go to connected in navigation. Click on 'Connection Wizard' to connect the device using a wizard.




**Step 4:** Click on android → next → Wifi → next.




MOBILedit Connection Wizard

Choose connection type


How would you like to connect your phone?




☐ Cable



☒ Wi-Fi



☐ Bluetooth



☐ Tethering (network)

[Online guide](#)

&lt; Back

Next &gt;

Cancel

MOBILedit Connection Wizard

Enter phone's IP address

Please follow these instructions step by step:

1. Start MOBILedit Connector app on your phone, it should be preloaded. You can also download it from [Google Play](#), scan the QR code to find it.

2. Select Wi-Fi connection

3. Fill in here the IP address you can see on the phone screen:



[Online guide](#)

< Back

Next >

Cancel