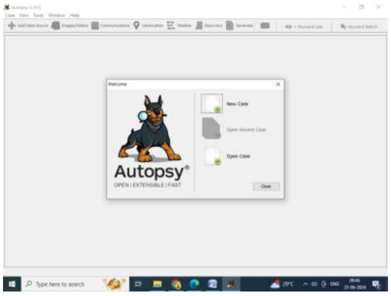
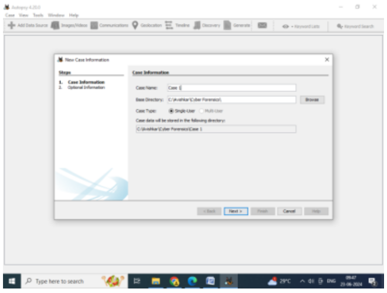
Practical 1

File System Analysis using The SleuthKit (Autospy, fsstat, istat, fls and img_stat)

☆ Step1: Open autopsy software



☆ Step2: Click on New Case and give case name and click on next


New Case Information

Steps
1. Case Information
2. Optional Information

Case Information

Case Name: Case 1

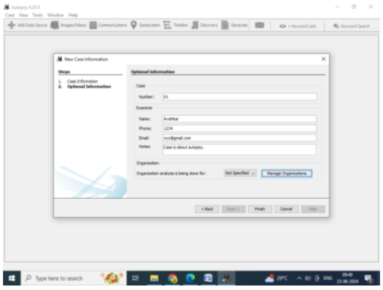
Base Directory: C:\Avishkar\Cyber Forensics\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Avishkar\Cyber Forensics\Case 1

☆ Step 3: Enter required details and click on finish


New Case Information

Steps
1. Case Information
2. Optional Information

Optional Information

Case

Number: 01

Examiner

Name: Avishkar

Phone: 1234

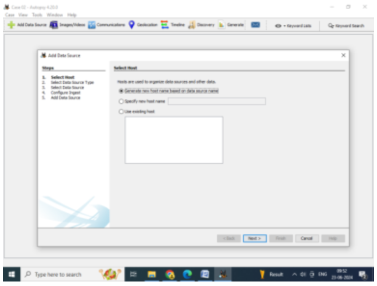
Email: xxx@gmail.com

Notes: Case is about autopsy.

Organization

Organization analysis is being done for: Not Specified

☆ Step 4:


Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

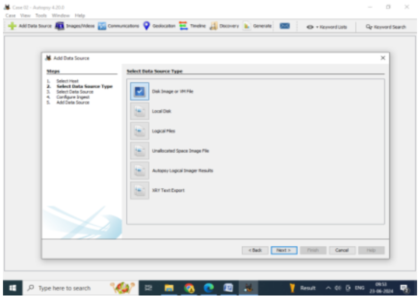
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

☆ Step 5:


Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

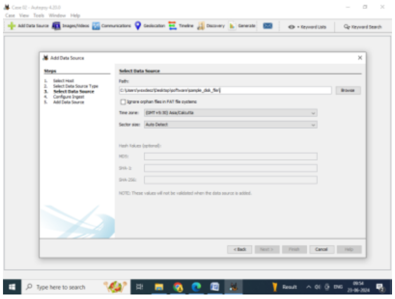
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

☆ Step6:



Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\wsxdesz\Desktop\software\sample_disk_file\

□ Ignore orphan files in FAT file systems

Time zone: (GMT+5:30) Asia/Calcutta

Sector size: Auto Detect

Hash Values (optional):

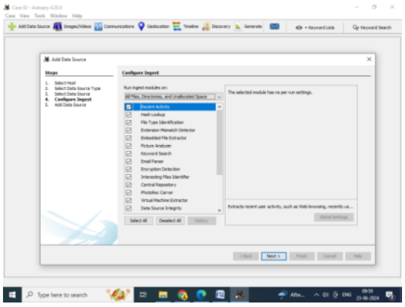
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

☆ Step 7:



Add Data Source

Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

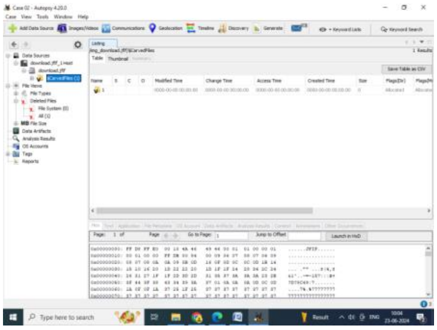
Run ingest modules on: All Files, Directories, and Unallocated Space

☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Picture Analyzer
☑ Keyword Search
☑ Email Parser
☑ Encryption Detection
☑ Interesting Files Identifier
☑ Central Repository
☑ PhotoRec Carver
☑ Virtual Machine Extractor
☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

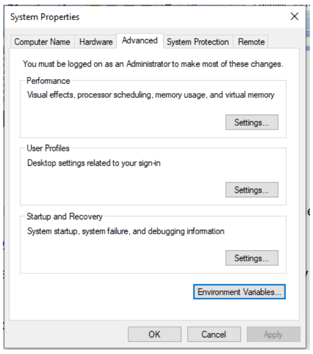
☆ Step 8:



The SleuthKit

☆ Step 1:

- ➢ Using below link download sleuth kit win32 zip file from windows binaries The Sleuth Kit: Download
- ➢ Now copy the file to desktop and rename it to sleuthkit-4.12.1 and copy folder to c drive program files (x86)
- ➢ Now go to search and open edit sytem variables and click environment variables.



System Properties

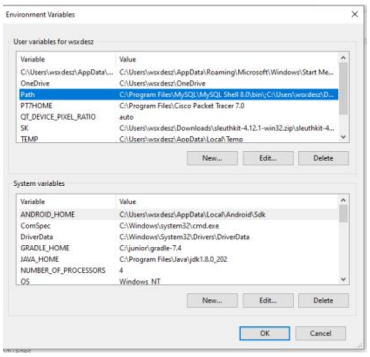
Computer Name | Hardware | **Advanced** | System Protection | Remote

You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your sign-in

Startup and Recovery
System startup, system failure, and debugging information



Environment Variables

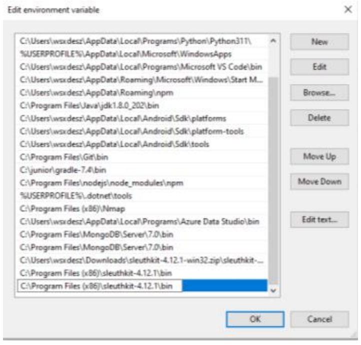
User variables for wsxdesz

Variable	Value
C:\Users\wsxdesz\AppData\...	C:\Users\wsxdesz\AppData\Roaming\Microsoft\Windows\Start Me...
OneDrive	C:\Users\wsxdesz\OneDrive
Path	C:\Program Files\MySQL\MySQL Shell 8.0\bin\;C:\Users\wsxdesz\D...
PT7HOME	C:\Program Files\Cisco Packet Tracer 7.0
QT_DEVICE_PIXEL_RATIO	auto
SK	C:\Users\wsxdesz\Downloads\sleuthkit-4.12.1-win32.zip\sleuthkit-4...
TEMP	C:\Users\wsxdesz\AppData\Local\Temp

System variables

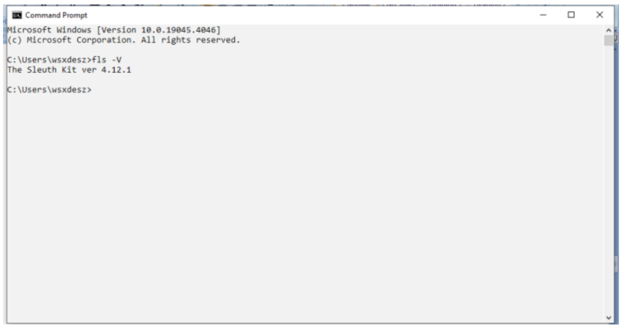
Variable	Value
ANDROID_HOME	C:\Users\wsxdesz\AppData\Local\Android\Sdk
ComSpec	C:\Windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
GRADLE_HOME	C:\junior\gradle-7.4
JAVA_HOME	C:\Program Files\Java\jdk1.8.0_202
NUMBER_OF_PROCESSORS	4
OS	Windows_NT

Double click on path and click on New and give path of sleuth kit bin folder and click on OK.



```
C:\Users\wsxdesz\AppData\Local\Programs\Python\Python311\
%USERPROFILE%\AppData\Local\Microsoft\WindowsApps
C:\Users\wsxdesz\AppData\Local\Programs\Microsoft VS Code\bin
C:\Users\wsxdesz\AppData\Roaming\Microsoft\Windows\Start M...
C:\Users\wsxdesz\AppData\Roaming\npm
C:\Program Files\Java\jdk1.8.0_202\bin
C:\Users\wsxdesz\AppData\Local\Android\Sdk\platforms
C:\Users\wsxdesz\AppData\Local\Android\Sdk\platform-tools
C:\Users\wsxdesz\AppData\Local\Android\Sdk\tools
C:\Program Files\Git\bin
C:\junior\gradle-7.4\bin
C:\Program Files\nodejs\node_modules\npm
%USERPROFILE%\.dotnet\tools
C:\Program Files (x86)\Nmap
C:\Users\wsxdesz\AppData\Local\Programs\Azure Data Studio\bin
C:\Program Files\MongoDB\Server\7.0\bin
C:\Program Files\MongoDB\Server\7.0\bin
C:\Users\wsxdesz\Downloads\sleuthkit-4.12.1-win32.zip\sleuthkit-...
C:\Program Files (x86)\sleuthkit-4.12.1\bin
C:\Program Files (x86)\sleuthkit-4.12.1\bin
```

The go to cmd and give command fls –V and check sleuth kit version



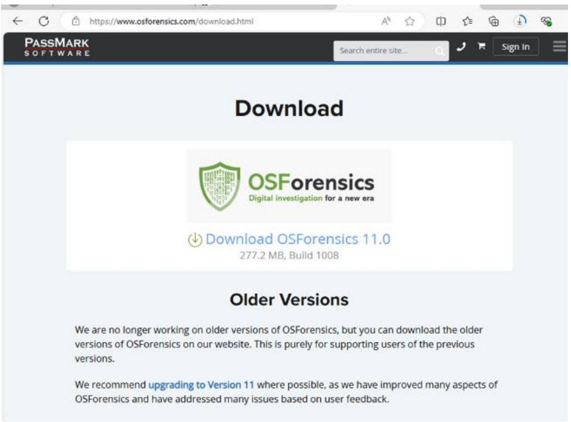
```
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\Users\wsxdesz>fls -V
The Sleuth Kit ver 4.12.1

C:\Users\wsxdesz>
```

Practical 2

a. Explore Windows forensic tools (OSForensics)


https://www.osforensics.com/download.html

Download

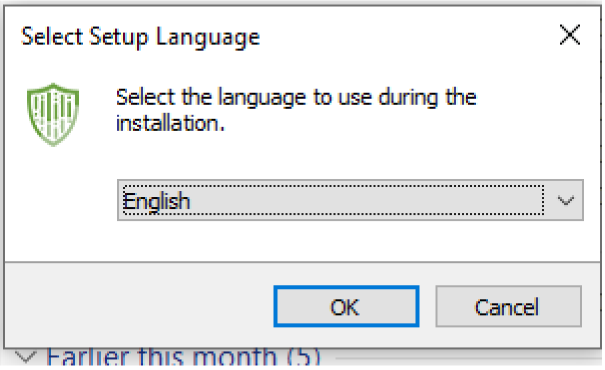
OSForensics Digital investigation for a new era

Download OSForensics 11.0
277.2 MB, Build 1008

Older Versions

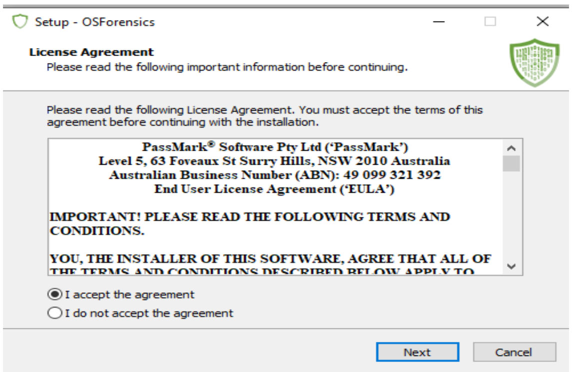
We are no longer working on older versions of OSForensics, but you can download the older versions of OSForensics on our website. This is purely for supporting users of the previous versions.

We recommend upgrading to Version 11 where possible, as we have improved many aspects of OSForensics and have addressed many issues based on user feedback.


Select Setup Language

Select the language to use during the installation.

English


Setup - OSForensics

License Agreement
Please read the following important information before continuing.

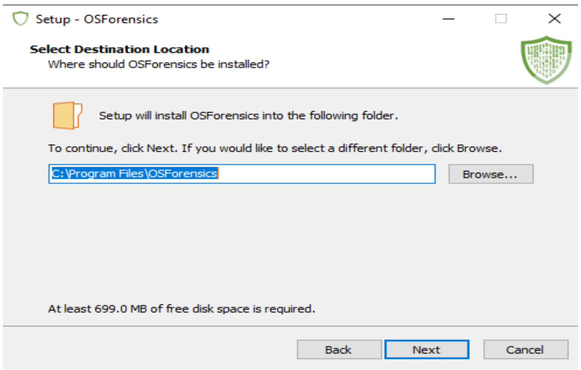
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

PassMark® Software Pty Ltd ('PassMark')
Level 5, 63 Foveaux St Surry Hills, NSW 2010 Australia
Australian Business Number (ABN): 49 099 321 392
End User License Agreement ('EULA')

IMPORTANT! PLEASE READ THE FOLLOWING TERMS AND CONDITIONS.

YOU, THE INSTALLER OF THIS SOFTWARE, AGREE THAT ALL OF THE TERMS AND CONDITIONS DESCRIBED BELOW APPLY TO

● I accept the agreement
○ I do not accept the agreement


Setup - OSForensics

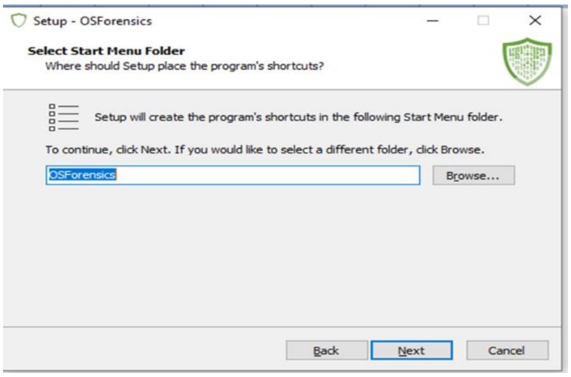
Select Destination Location
Where should OSForensics be installed?

Setup will install OSForensics into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\OSForensics

At least 699.0 MB of free disk space is required.

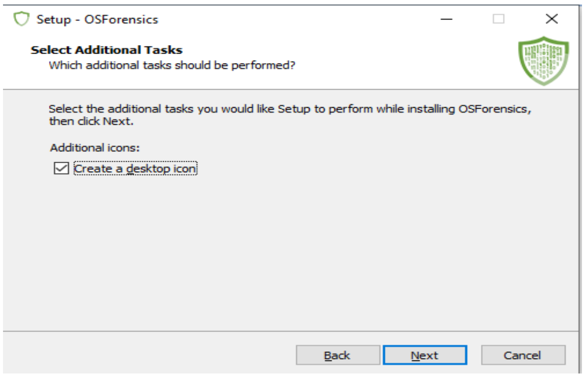

Setup - OSForensics

Select Start Menu Folder
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

OSForensics

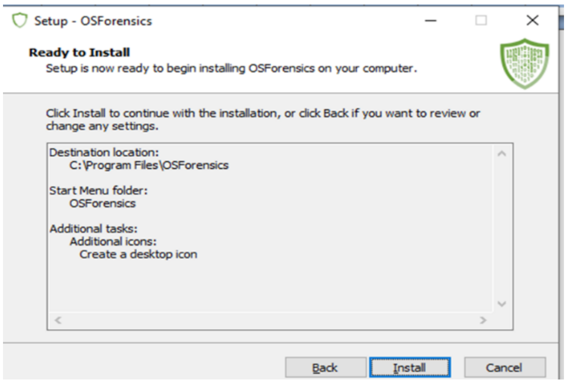

Setup - OSForensics

Select Additional Tasks
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing OSForensics, then click Next.

Additional icons:

☑ Create a desktop icon


Setup - OSForensics

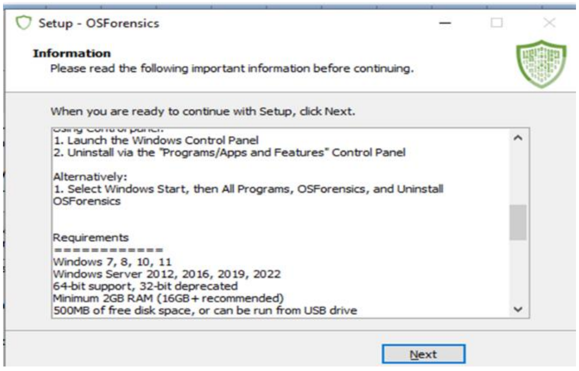
Ready to Install
Setup is now ready to begin installing OSForensics on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\OSForensics

Start Menu folder:
OSForensics

Additional tasks:
Additional icons:
Create a desktop icon


Setup - OSForensics

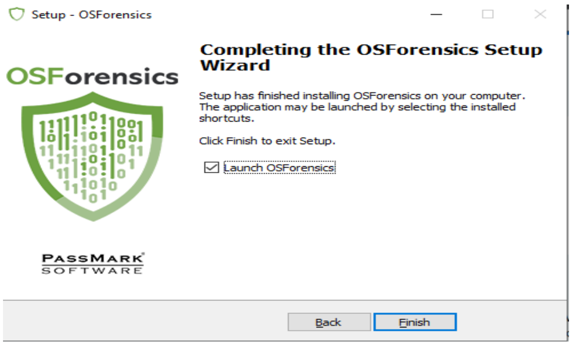
Information
Please read the following important information before continuing.

When you are ready to continue with Setup, click Next.

1. Launch the Windows Control Panel
2. Uninstall via the "Programs/Apps and Features" Control Panel

Alternatively:
1. Select Windows Start, then All Programs, OSForensics, and Uninstall OSForensics

Requirements
============
Windows 7, 8, 10, 11
Windows Server 2012, 2016, 2019, 2022
64-bit support, 32-bit deprecated
Minimum 2GB RAM (16GB+ recommended)
500MB of free disk space, or can be run from USB drive



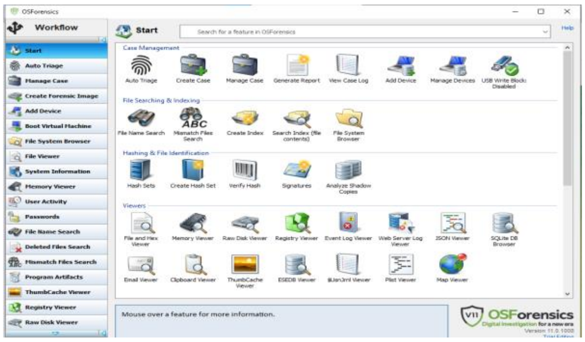
Setup - OSForensics

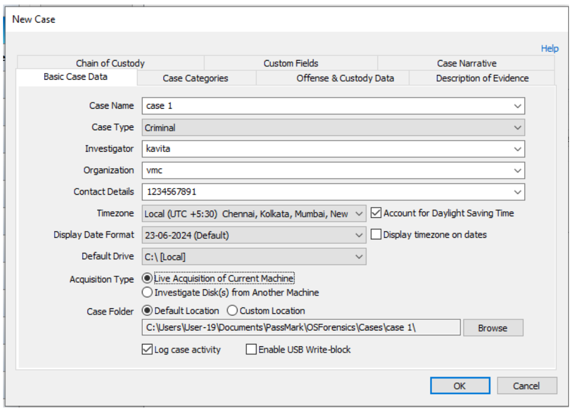
Completing the OSForensics Setup Wizard

Setup has finished installing OSForensics on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Launch OSForensics





New Case

Case Name: case 1

Case Type: Criminal

Investigator: kavita

Organization: vmc

Contact Details: 1234567891

Timezone: Local (UTC +5:30) Chennai, Kolkata, Mumbai, New — ☑ Account for Daylight Saving Time

Display Date Format: 23-06-2024 (Default) — □ Display timezone on dates

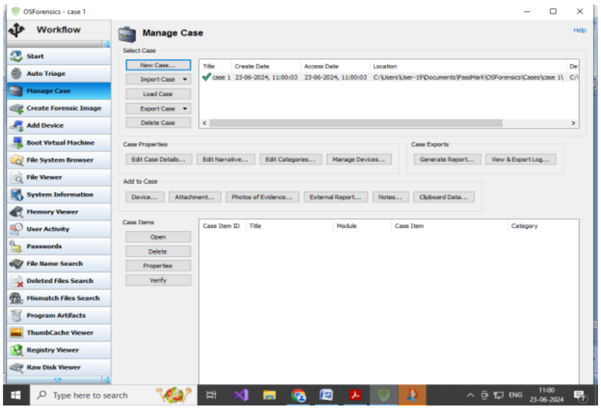
Default Drive: C:\ [Local]

Acquisition Type: ● Live Acquisition of Current Machine ○ Investigate Disk(s) from Another Machine

Case Folder: ● Default Location ○ Custom Location

C:\Users\User-19\Documents\PassMark\OSForensics\Cases\case 1\

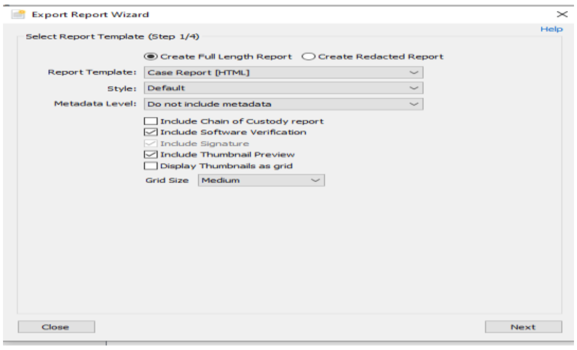
☑ Log case activity □ Enable USB Write-block



OSForensics - case 1

Manage Case

Title	Create Date	Access Date	Location
✓ case 1	23-06-2024, 11:00:03	23-06-2024, 11:00:03	C:\Users\User-19\Documents\PassMark\OSForensics\Cases\case 1\



Export Report Wizard

Select Report Template (Step 1/4)

● Create Full Length Report ○ Create Redacted Report

Report Template: Case Report [HTML]

Style: Default

Metadata Level: Do not include metadata

□ Include Chain of Custody report

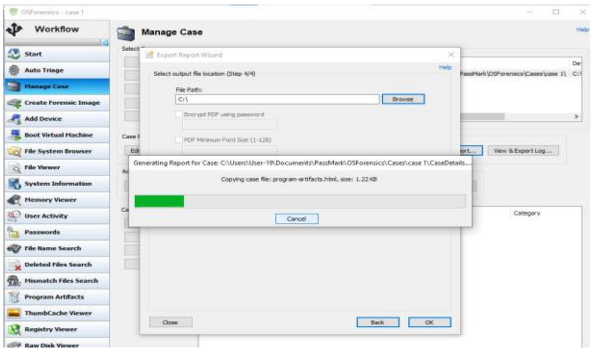
☑ Include Software Verification

☑ Include Signature

☑ Include Thumbnail Preview

□ Display Thumbnails as grid

Grid Size: Medium



OSForensics - case 1

Manage Case

Export Report Wizard

Select output file location (Step 4/4)

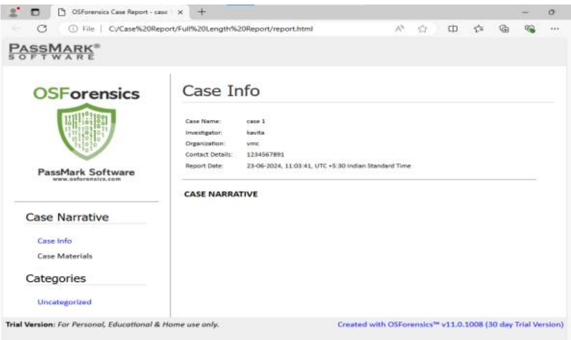
File Path: C:\

□ Encrypt PDF using password

□ PDF Minimum Font Size (1-128)

Generating Report for Case: C:\Users\User-19\Documents\PassMark\OSForensics\Cases\case 1\CaseDetails...

Copying case file: program-artifacts.html, size: 1.22 KB



OSForensics Case Report - case

C:/Case%20Report/Full%20Length%20Report/report.html

Case Info

Case Name: case 1

Investigator: kavita

Organization: vmc

Contact Details: 1234567891

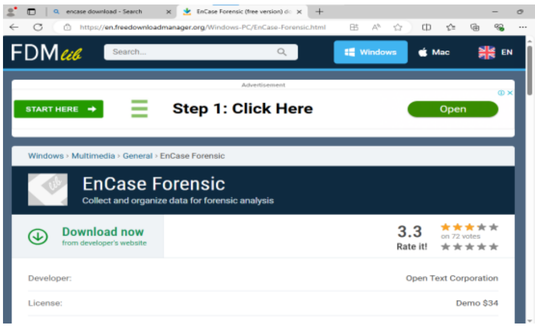
Report Date: 23-06-2024, 11:03:41, UTC +5:30 Indian Standard Time

CASE NARRATIVE

Trial Version: *For Personal, Educational & Home use only.*

Created with OSForensics™ v11.0.1008 (30 day Trial Version)

b. Forensics Investigation Using Encase



Step 1: Click Here

Windows › Multimedia › General › EnCase Forensic

EnCase Forensic

Collect and organize data for forensic analysis

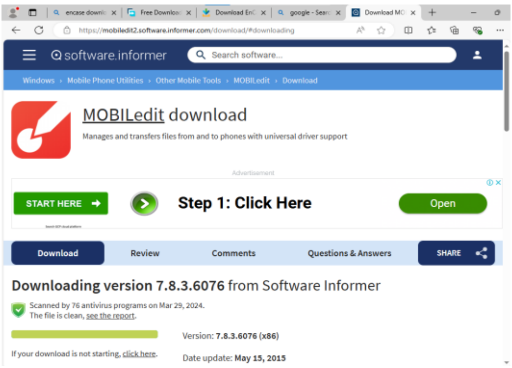
Download now from developer's website

3.3 Rate it! on 72 votes

Developer: Open Text Corporation

License: Demo $34

c. Using Mobile Forensics software tools



MOBILedit download

Manages and transfers files from and to phones with universal driver support

Step 1: Click Here

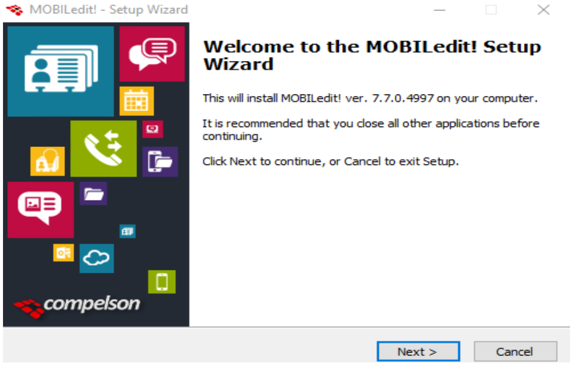
Downloading version 7.8.3.6076 from Software Informer

Scanned by 76 antivirus programs on Mar 29, 2024. The file is clean, see the report.

Version: 7.8.3.6076 (x86)

If your download is not starting, click here.

Date update: May 15, 2015

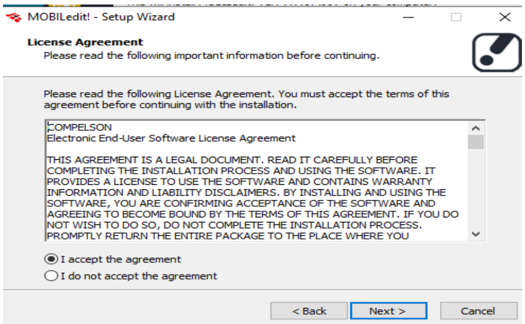


Welcome to the MOBILedit! Setup Wizard

This will install MOBILedit! ver. 7.7.0.4997 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



License Agreement

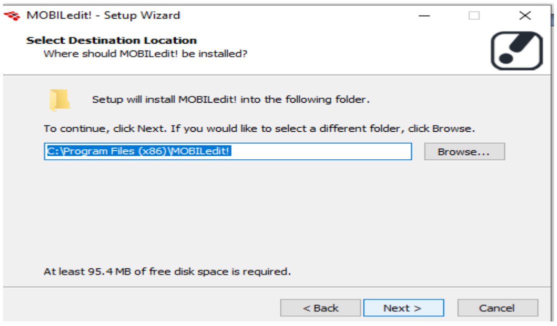
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

COMPELSON
Electronic End-User Software License Agreement

THIS AGREEMENT IS A LEGAL DOCUMENT. READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY INSTALLING AND USING THE SOFTWARE, YOU ARE CONFIRMING ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT WISH TO DO SO, DO NOT COMPLETE THE INSTALLATION PROCESS. PROMPTLY RETURN THE ENTIRE PACKAGE TO THE PLACE WHERE YOU

● I accept the agreement
○ I do not accept the agreement



Select Destination Location

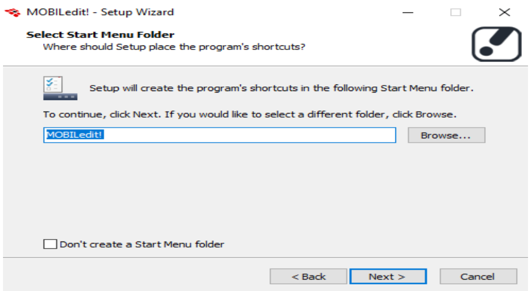
Where should MOBILedit! be installed?

Setup will install MOBILedit! into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\MOBILedit!

At least 95.4 MB of free disk space is required.



Select Start Menu Folder

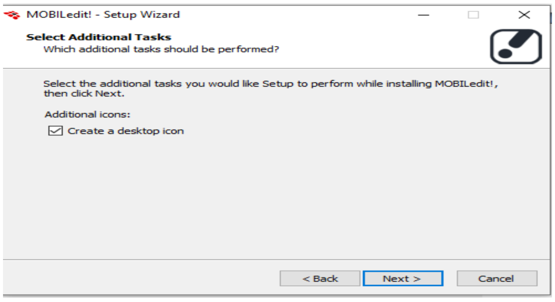
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

MOBILedit!

□ Don't create a Start Menu folder



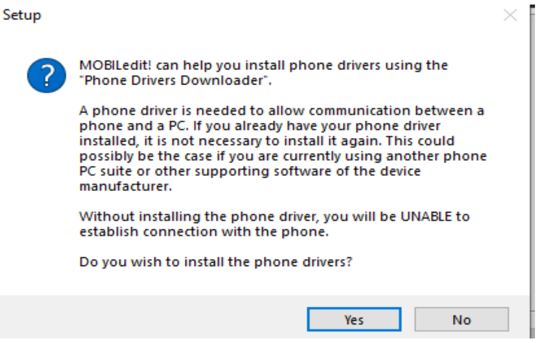
Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing MOBILedit!, then click Next.

Additional icons:

☑ Create a desktop icon

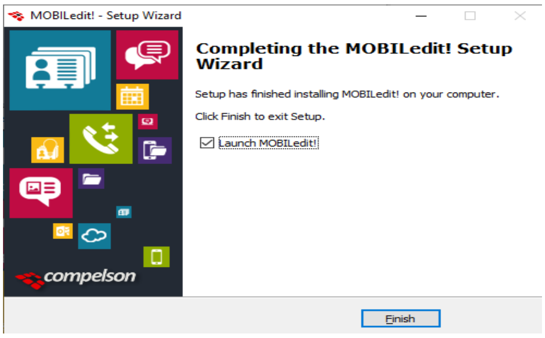


MOBILedit! can help you install phone drivers using the "Phone Drivers Downloader".

A phone driver is needed to allow communication between a phone and a PC. If you already have your phone driver installed, it is not necessary to install it again. This could possibly be the case if you are currently using another phone PC suite or other supporting software of the device manufacturer.

Without installing the phone driver, you will be UNABLE to establish connection with the phone.

Do you wish to install the phone drivers?

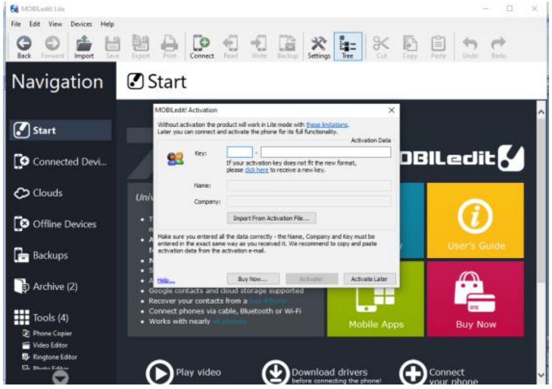


Completing the MOBILedit! Setup Wizard

Setup has finished installing MOBILedit! on your computer.

Click Finish to exit Setup.

☑ Launch MOBILedit!



MOBILedit! Activation

Without activation the product will work in Lite mode with these limitations.
Later you can connect and activate the phone for its full functionality.

Activation Data

Key:

If your activation key does not fit the new format, please click here to receive a new key.

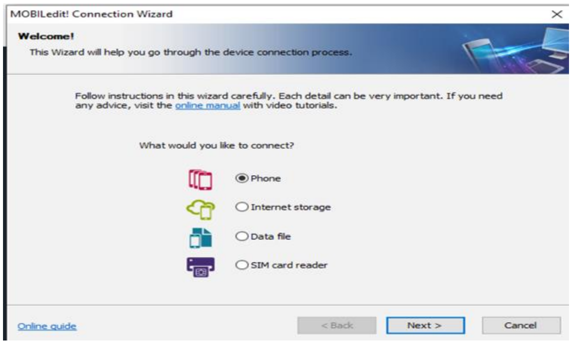
Name:

Company:

Make sure you entered all the data correctly - the Name, Company and Key must be entered in the exact same way as you received it. We recommend to copy and paste activation data from the activation e-mail.

- Google contacts and cloud storage supported
- Recover your contacts from a lost iPhone
- Connect phones via cable, Bluetooth or Wi-Fi
- Works with nearly all phones

Click on - Activate later



MOBILedit! Connection Wizard

Welcome!

This Wizard will help you go through the device connection process.

Follow instructions in this wizard carefully. Each detail can be very important. If you need any advice, visit the online manual with video tutorials.

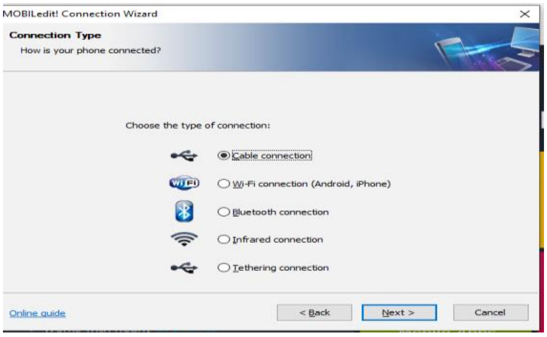
What would you like to connect?

● Phone

○ Internet storage

○ Data file

○ SIM card reader



MOBILedit! Connection Wizard

Connection Type

How is your phone connected?

Choose the type of connection:

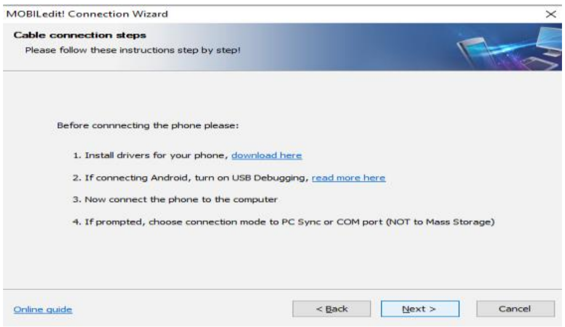
● Cable connection

○ Wi-Fi connection (Android, iPhone)

○ Bluetooth connection

○ Infrared connection

○ Tethering connection



MOBILedit! Connection Wizard

Cable connection steps

Please follow these instructions step by step!

Before connecting the phone please:

1. Install drivers for your phone, download here
2. If connecting Android, turn on USB Debugging, read more here
3. Now connect the phone to the computer
4. If prompted, choose connection mode to PC Sync or COM port (NOT to Mass Storage)

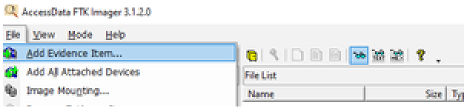
Practical 3

Using Forensic Toolkit(FTK) &Writing report usingFTK (AccessData FTK)

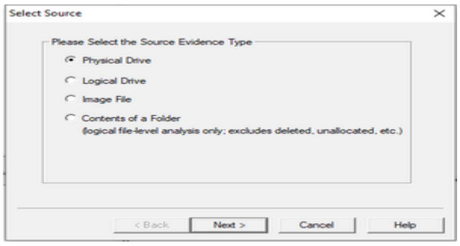
1. FTK Imager from Access Data, which can be downloaded using the following link: FTK Imager from Access Data
2. A Hard Drive that you would like to create an image of.

Method :

- ☆ **Step 1:** Download and install the FTK imager on your machine.
- ☆ **Step 2:** Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.
- ☆ **Step 3:** In the menu navigation bar, you need to click on the File tab which will give you a drop-down, like given in the image below, just click on the first one that says, Add Evidence Item.



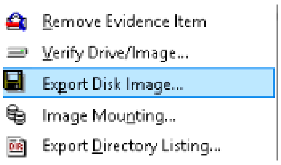
- ☆ **Step 4:** After that, there will be a pop-up window that will ask you to Select the Source of the Evidence. If you have connected a physical hard drive to the laptop/computer you are using to make the forensic image, then you will select the Physical Drive here. Click on Next. Now, Select the Physical Drive that you would like to use. Please make sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your own OS drive.


Select Source

Please Select the Source Evidence Type

● Physical Drive
○ Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

- ☆ **Step 5:** Now, we will export the forensic images.
  - ➢ Right-click on the Physical Drive that you would like to export in the FTK Imager window. Select Export Disk Image here.



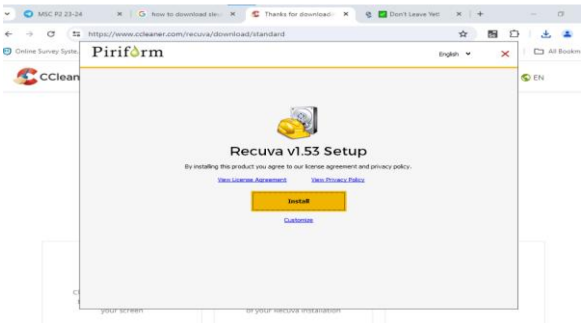
  - ➢ Click the Add button for the Image Destination.
  - ➢ Select the Type of Forensic Image you would like to export. Select .E01 and Click Next.

- After that, you will have to enter information regarding the case now. You can either leave them blank or keep it general, this part is totally upon you.
- Next, you will need to Choose the Destination that you would like to export the forensic image and Name the Image.
- Lastly, you will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.

Practical 4

Recover Deleted files using Recuva, PC Inspector File Recovery, Recover My Files, R Studio

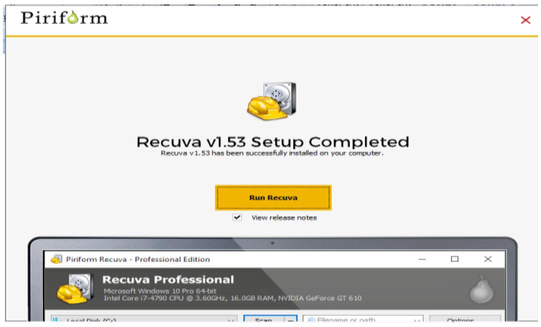
1. First Start the tool
2. Then select which type of files you want to recover (All files)
3. Now specify the location of the source drive to recover files. (E:)
4. Now select the list of files you want to recover
5. Select destination folder/drive where you want to store recover files (Desktop)



https://www.ccleaner.com/recuva/download/standard

Recuva v1.53 Setup

By installing this product you agree to our license agreement and privacy policy.



Recuva v1.53 Setup Completed

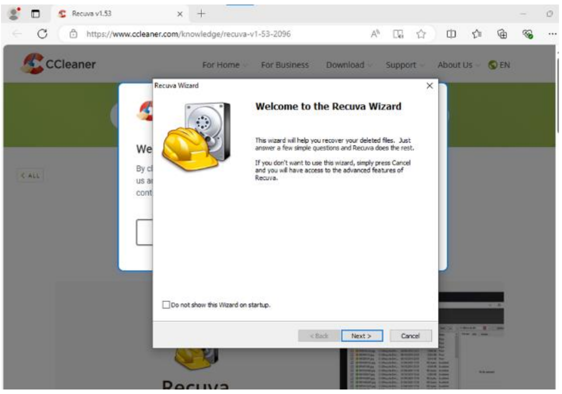
Recuva v1.53 has been successfully installed on your computer.

☑ View release notes

Piriform Recuva - Professional Edition

Recuva Professional

Microsoft Windows 10 Pro 64-bit
Intel Core i7-4790 CPU @ 3.60GHz, 16.0GB RAM, NVIDIA GeForce GT 610



https://www.ccleaner.com/knowledge/recuva-v1-53-2096

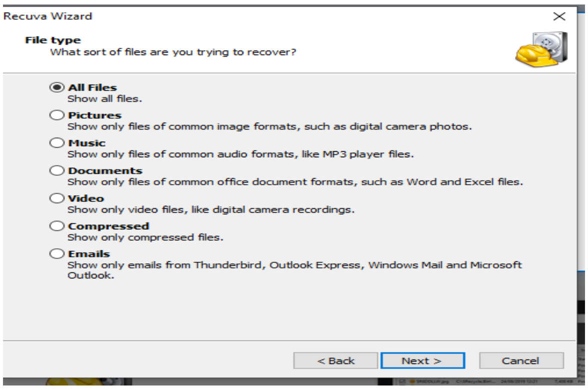
Recuva Wizard

Welcome to the Recuva Wizard

This wizard will help you recover your deleted files. Just answer a few simple questions and Recuva does the rest.

If you don't want to use this wizard, simply press Cancel and you will have access to the advanced features of Recuva.

□ Do not show this Wizard on startup.



Recuva Wizard

File type
What sort of files are you trying to recover?

● **All Files**
Show all files.

○ **Pictures**
Show only files of common image formats, such as digital camera photos.

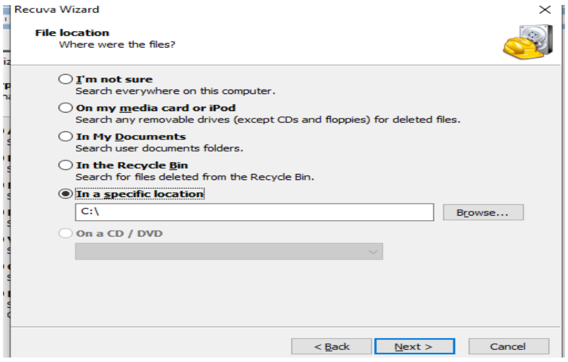
○ **Music**
Show only files of common audio formats, like MP3 player files.

○ **Documents**
Show only files of common office document formats, such as Word and Excel files.

○ **Video**
Show only video files, like digital camera recordings.

○ **Compressed**
Show only compressed files.

○ **Emails**
Show only emails from Thunderbird, Outlook Express, Windows Mail and Microsoft Outlook.



Recuva Wizard

File location
Where were the files?

○ **I'm not sure**
Search everywhere on this computer.

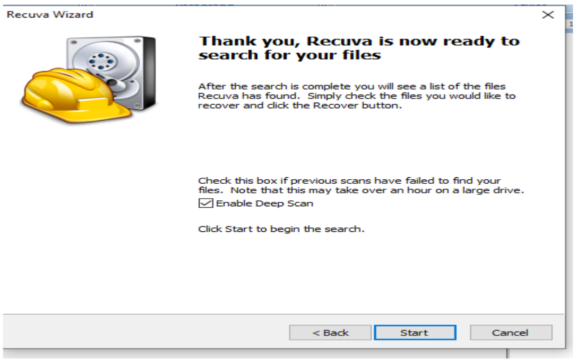
○ **On my media card or iPod**
Search any removable drives (except CDs and floppies) for deleted files.

○ **In My Documents**
Search user documents folders.

○ **In the Recycle Bin**
Search for files deleted from the Recycle Bin.

● **In a specific location**
C:\

○ On a CD / DVD



Recuva Wizard

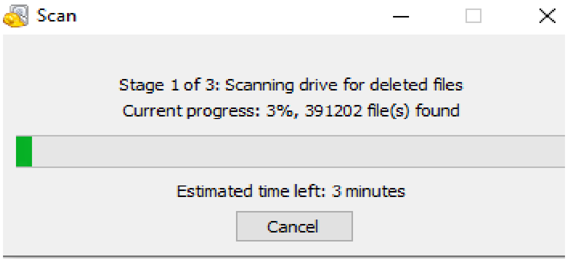
Thank you, Recuva is now ready to search for your files

After the search is complete you will see a list of the files Recuva has found. Simply check the files you would like to recover and click the Recover button.

Check this box if previous scans have failed to find your files. Note that this may take over an hour on a large drive.

☑ Enable Deep Scan

Click Start to begin the search.

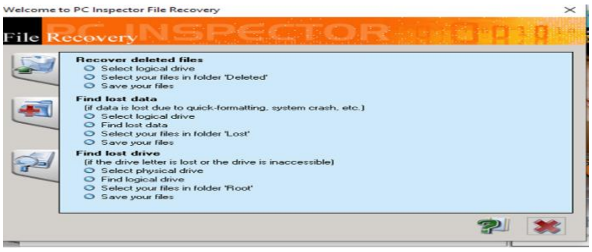


Scan

Stage 1 of 3: Scanning drive for deleted files

Current progress: 3%, 391202 file(s) found

Estimated time left: 3 minutes

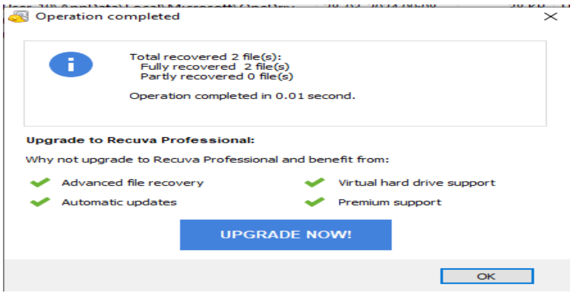


Welcome to PC Inspector File Recovery

Recover deleted files
○ Select logical drive
○ Select your files in folder 'Deleted'
○ Save your files

Find lost data
(if data is lost due to quick-formatting, system crash, etc.)
○ Select logical drive
○ Find lost data
○ Select your files in folder 'Lost'
○ Save your files

Find lost drive
(if the drive letter is lost or the drive is inaccessible)
○ Select physical drive
○ Find logical drive
○ Select your files in folder 'Root'
○ Save your files



Operation completed

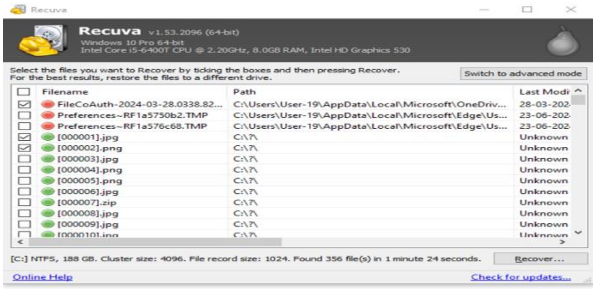
Total recovered 2 file(s):
Fully recovered 2 file(s)
Partly recovered 0 file(s)

Operation completed in 0.01 second.

Upgrade to Recuva Professional:

Why not upgrade to Recuva Professional and benefit from:

- ✓ Advanced file recovery
- ✓ Virtual hard drive support
- ✓ Automatic updates
- ✓ Premium support

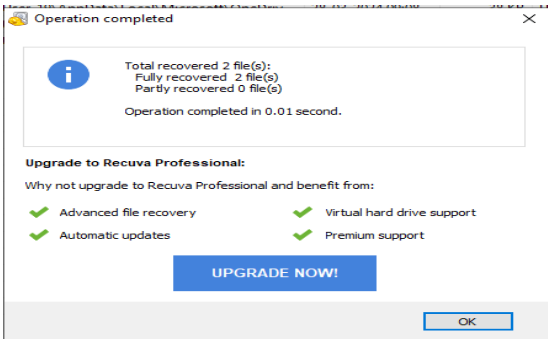


Recuva v1.53.2096 (64-bit)
Windows 10 Pro 64-bit
Intel Core i5-6400T CPU @ 2.20GHz, 8.0GB RAM, Intel HD Graphics 530

Select the files you want to Recover by ticking the boxes and then pressing Recover.
For the best results, restore the files to a different drive.

□	Filename	Path	Last Modi
☑	FileCoAuth-2024-03-28.0338.82...	C:\Users\User-19\AppData\Local\Microsoft\OneDriv...	28-03-202
□	Preferences~RF1a5750b2.TMP	C:\Users\User-19\AppData\Local\Microsoft\Edge\Us...	23-06-202
□	Preferences~RF1a576c68.TMP	C:\Users\User-19\AppData\Local\Microsoft\Edge\Us...	23-06-202
☑	[000001].jpg	C:\?\	Unknown
☑	[000002].png	C:\?\	Unknown
□	[000003].jpg	C:\?\	Unknown
□	[000004].png	C:\?\	Unknown
□	[000005].png	C:\?\	Unknown
□	[000006].jpg	C:\?\	Unknown
□	[000007].zip	C:\?\	Unknown
□	[000008].jpg	C:\?\	Unknown
□	[000009].jpg	C:\?\	Unknown
□	[000010].jpg	C:\?\	Unknown

[C:] NTFS, 188 GB. Cluster size: 4096. File record size: 1024. Found 356 file(s) in 1 minute 24 seconds.



Operation completed

Total recovered 2 file(s):
Fully recovered 2 file(s)
Partly recovered 0 file(s)

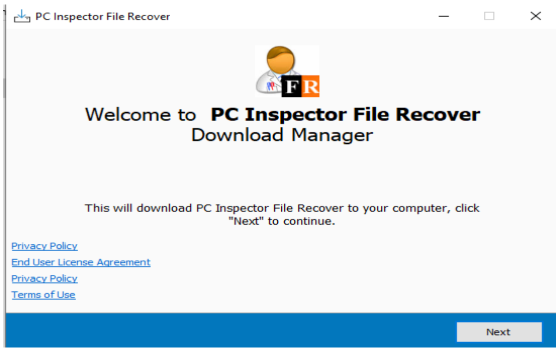
Operation completed in 0.01 second.

Upgrade to Recuva Professional:

Why not upgrade to Recuva Professional and benefit from:

- ✓ Advanced file recovery
- ✓ Virtual hard drive support
- ✓ Automatic updates
- ✓ Premium support

Files recovered..........

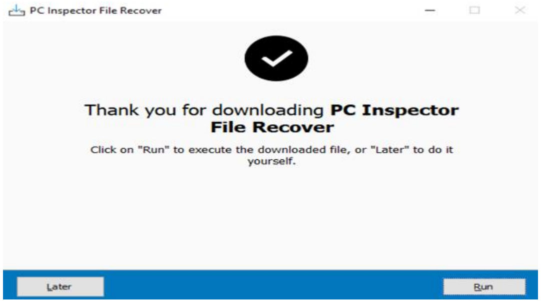


PC Inspector File Recover

Welcome to **PC Inspector File Recover**
Download Manager

This will download PC Inspector File Recover to your computer, click "Next" to continue.

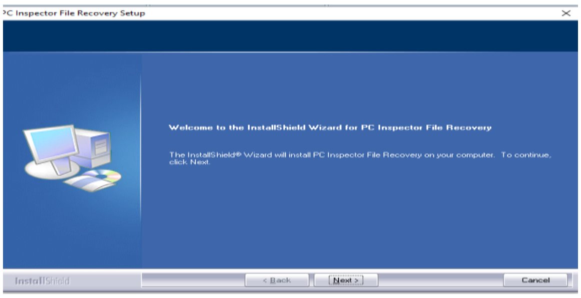
Click next – accept



PC Inspector File Recover

Thank you for downloading **PC Inspector File Recover**

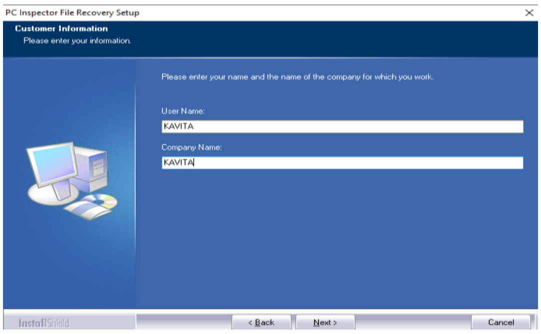
Click on "Run" to execute the downloaded file, or "Later" to do it yourself.



PC Inspector File Recovery Setup

Welcome to the InstallShield Wizard for PC Inspector File Recovery

The InstallShield® Wizard will install PC Inspector File Recovery on your computer. To continue, click Next.



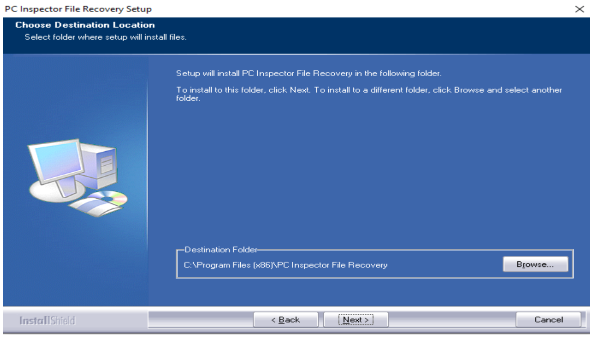
PC Inspector File Recovery Setup

Customer Information
Please enter your information.

Please enter your name and the name of the company for which you work.

User Name: KAVITA

Company Name: KAVITA



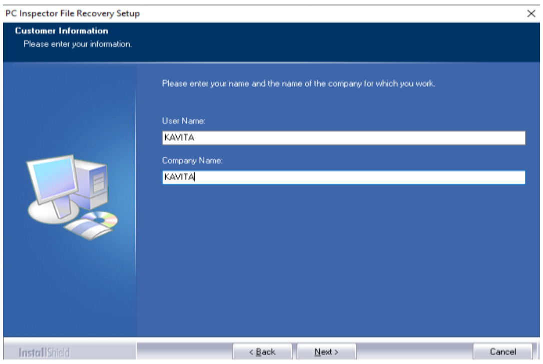
PC Inspector File Recovery Setup

Choose Destination Location
Select folder where setup will install files.

Setup will install PC Inspector File Recovery in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder
C:\Program Files (x86)\PC Inspector File Recovery



PC Inspector File Recovery Setup

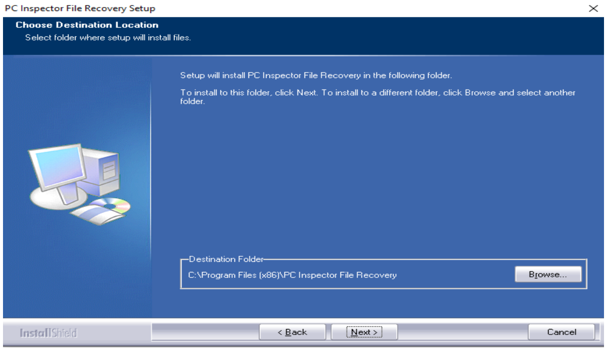
Customer Information

Please enter your information.

Please enter your name and the name of the company for which you work.

User Name: KAVITA

Company Name: KAVITA



PC Inspector File Recovery Setup

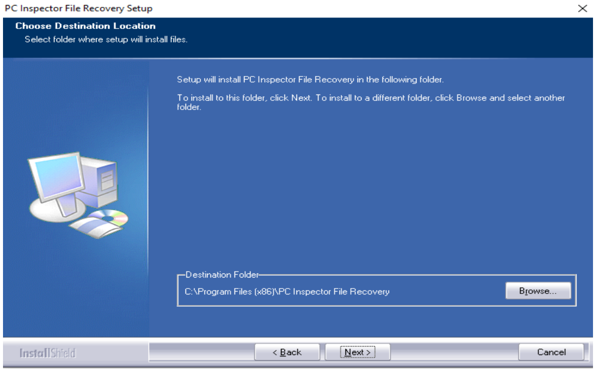
Choose Destination Location

Select folder where setup will install files.

Setup will install PC Inspector File Recovery in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: C:\Program Files (x86)\PC Inspector File Recovery



PC Inspector File Recovery Setup

Choose Destination Location

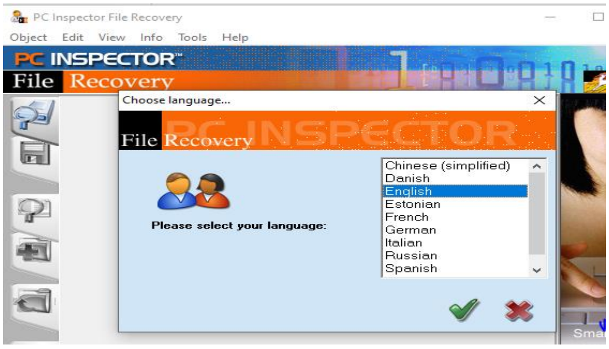
Select folder where setup will install files.

Setup will install PC Inspector File Recovery in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: C:\Program Files (x86)\PC Inspector File Recovery

Click next – finish

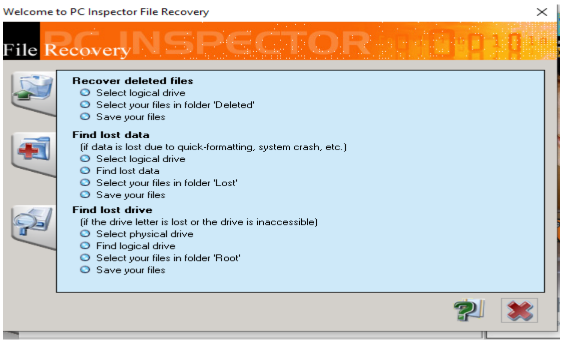


PC Inspector File Recovery

Choose language...

Please select your language:

- Chinese (simplified)
- Danish
- English
- Estonian
- French
- German
- Italian
- Russian
- Spanish



Welcome to PC Inspector File Recovery

Recover deleted files

- ○ Select logical drive
- ○ Select your files in folder 'Deleted'
- ○ Save your files

Find lost data

(if data is lost due to quick-formatting, system crash, etc.)

- ○ Select logical drive
- ○ Find lost data
- ○ Select your files in folder 'Lost'
- ○ Save your files

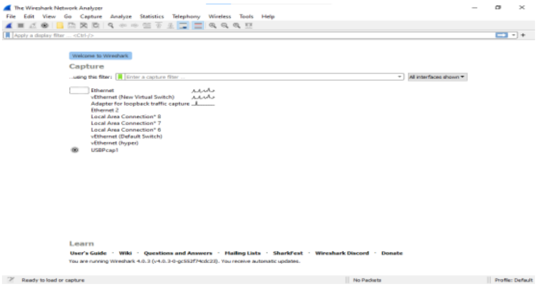
Find lost drive

(if the drive letter is lost or the drive is inaccessible)

- ○ Select physical drive
- ○ Find logical drive
- ○ Select your files in folder 'Root'
- ○ Save your files

Practical 5

Capturing & network rackets using Wire shark fundamentals



The Wireshark Network Analyzer

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

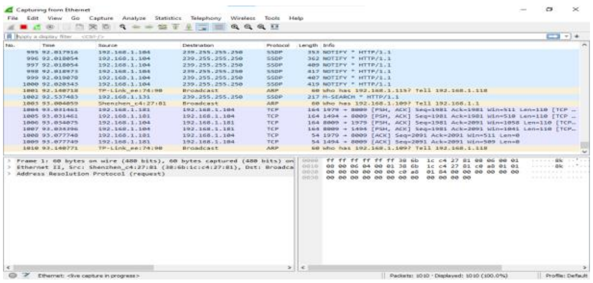
- Ethernet
- vEthernet (New Virtual Switch)
- Adapter for loopback traffic capture
- Ethernet 2
- Local Area Connection* 8
- Local Area Connection* 7
- Local Area Connection* 6
- vEthernet (Default Switch)
- vEthernet (hyper)
- USBPcap1

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

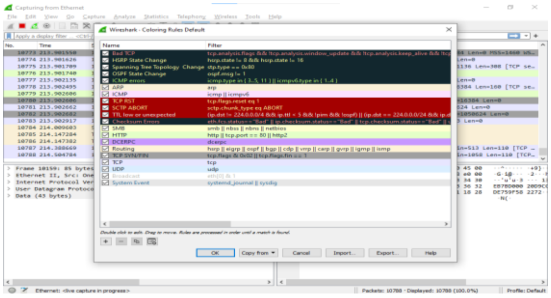


Capturing from Ethernet

```
No.   Time       Source             Destination       Protocol Length Info
  995 92.017916  192.168.1.104      239.255.255.250   SSDP     353 NOTIFY * HTTP/1.1
  996 92.018054  192.168.1.104      239.255.255.250   SSDP     362 NOTIFY * HTTP/1.1
  997 92.018054  192.168.1.104      239.255.255.250   SSDP     409 NOTIFY * HTTP/1.1
  998 92.018973  192.168.1.104      239.255.255.250   SSDP     417 NOTIFY * HTTP/1.1
  999 92.019070  192.168.1.104      239.255.255.250   SSDP     407 NOTIFY * HTTP/1.1
 1000 92.020343  192.168.1.104      239.255.255.250   SSDP     419 NOTIFY * HTTP/1.1
 1001 92.140718  TP-Link_ee:74:98   Broadcast         ARP       60 Who has 192.168.1.115? Tell 192.168.1.118
 1002 92.537483  192.168.1.131      239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
 1003 93.004059  Shenzhen_c4:27:81  Broadcast         ARP       60 Who has 192.168.1.109? Tell 192.168.1.1
 1004 93.031461  192.168.1.181      192.168.1.104     TCP      164 1979 → 8009 [PSH, ACK] Seq=1981 Ack=1981 Win=511 Len=110 [TCP …
 1005 93.031461  192.168.1.181      192.168.1.104     TCP      164 1494 → 8009 [PSH, ACK] Seq=1981 Ack=1981 Win=510 Len=110 [TCP …
 1006 93.034075  192.168.1.104      192.168.1.181     TCP      164 8009 → 1979 [PSH, ACK] Seq=1981 Ack=2091 Win=1058 Len=110 [TCP…
 1007 93.034396  192.168.1.104      192.168.1.181     TCP      164 8009 → 1494 [PSH, ACK] Seq=1981 Ack=2091 Win=1041 Len=110 [TCP…
 1008 93.077740  192.168.1.181      192.168.1.104     TCP       54 1979 → 8009 [ACK] Seq=2091 Ack=2091 Win=511 Len=0
 1009 93.077749  192.168.1.181      192.168.1.104     TCP       54 1494 → 8009 [ACK] Seq=2091 Ack=2091 Win=509 Len=0
 1010 93.140771  TP-Link_ee:74:98   Broadcast         ARP       60 Who has 192.168.1.109? Tell 192.168.1.118

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
> Ethernet II, Src: Shenzhen_c4:27:81 (38:6b:1c:c4:27:81), Dst: Broadca
> Address Resolution Protocol (request)
```

Ethernet: <live capture in progress> | Packets: 1010 · Displayed: 1010 (100.0%) | Profile: Default



Wireshark · Coloring Rules Default

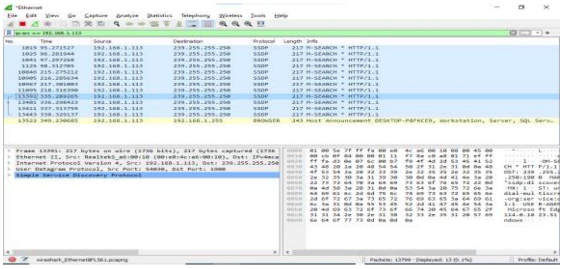
Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.d
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || u
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1
☑ System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

OK | Copy from | Cancel | Import... | Export... | Help

Ethernet: <live capture in progress> | Packets: 10788 · Displayed: 10788 (100.0%) | Profile: Default

Analyse Captured Packets:-



*Ethernet

ip.src == 192.168.1.113

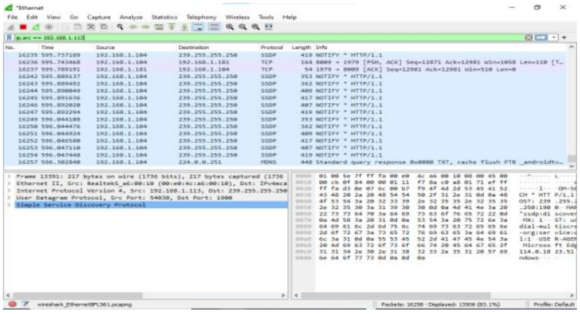
```
No.   Time        Source          Destination       Protocol Length Info
 1019 95.271527   192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
 1025 96.281944   192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
 1041 97.297268   192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
 1125 98.312705   192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
10846 215.275212  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
10905 216.285634  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
10967 217.301083  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
11095 218.316390  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
13391 335.289265  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
13401 336.298423  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
13411 337.313759  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
13443 338.329137  192.168.1.113   239.255.255.250   SSDP     217 M-SEARCH * HTTP/1.1
13522 349.230685  192.168.1.113   192.168.1.255     BROWSER  243 Host Announcement DESKTOP-P8FKCE9, Workstation, Server, SQL Serv…

> Frame 13391: 217 bytes on wire (1736 bits), 217 bytes captured (1736
> Ethernet II, Src: RealtekS_a6:00:10 (00:e0:4c:a6:00:10), Dst: IPv4mca
> Internet Protocol Version 4, Src: 192.168.1.113, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 54030, Dst Port: 1900
> Simple Service Discovery Protocol
```

wireshark_Ethernet8PL561.pcapng | Packets: 13799 · Displayed: 13 (0.1%) | Profile: Default

Display Filtered Command

Display Packets based on Specific IP Address:-



*Ethernet

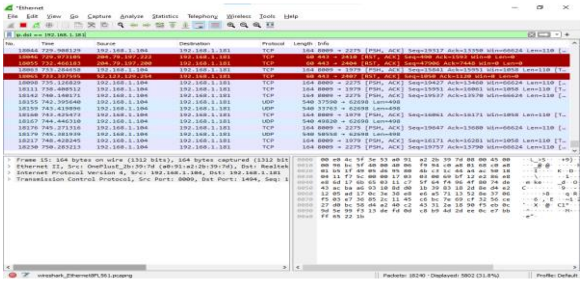
ip.src == 192.168.1.113

```
No.   Time        Source          Destination       Protocol Length Info
16235 595.737189  192.168.1.104   239.255.255.250   SSDP     419 NOTIFY * HTTP/1.1
16236 595.743468  192.168.1.104   192.168.1.181     TCP      164 8009 → 1979 [PSH, ACK] Seq=12871 Ack=12981 Win=1058 Len=110 [T…
16237 595.789191  192.168.1.181   192.168.1.104     TCP       54 1979 → 8009 [ACK] Seq=12981 Ack=12981 Win=510 Len=0
16242 595.889137  192.168.1.104   239.255.255.250   SSDP     353 NOTIFY * HTTP/1.1
16243 595.889492  192.168.1.104   239.255.255.250   SSDP     362 NOTIFY * HTTP/1.1
16244 595.890040  192.168.1.104   239.255.255.250   SSDP     409 NOTIFY * HTTP/1.1
16245 595.891636  192.168.1.104   239.255.255.250   SSDP     417 NOTIFY * HTTP/1.1
16246 595.892020  192.168.1.104   239.255.255.250   SSDP     407 NOTIFY * HTTP/1.1
16247 595.892294  192.168.1.104   239.255.255.250   SSDP     419 NOTIFY * HTTP/1.1
16249 596.044108  192.168.1.104   239.255.255.250   SSDP     353 NOTIFY * HTTP/1.1
16250 596.044476  192.168.1.104   239.255.255.250   SSDP     362 NOTIFY * HTTP/1.1
16251 596.044924  192.168.1.104   239.255.255.250   SSDP     409 NOTIFY * HTTP/1.1
16252 596.046580  192.168.1.104   239.255.255.250   SSDP     417 NOTIFY * HTTP/1.1
16253 596.047110  192.168.1.104   239.255.255.250   SSDP     407 NOTIFY * HTTP/1.1
16254 596.047448  192.168.1.104   239.255.255.250   SSDP     419 NOTIFY * HTTP/1.1
16257 596.302840  192.168.1.104   224.0.0.251       MDNS     448 Standard query response 0x0000 TXT, cache flush PTR _androidtv…

> Frame 13391: 217 bytes on wire (1736 bits), 217 bytes captured (1736
> Ethernet II, Src: RealtekS_a6:00:10 (00:e0:4c:a6:00:10), Dst: IPv4mca
> Internet Protocol Version 4, Src: 192.168.1.113, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 54030, Dst Port: 1900
> Simple Service Discovery Protocol
```

wireshark_Ethernet8PL561.pcapng | Packets: 16258 · Displayed: 13506 (83.1%) | Profile: Default

Display Packets based on Specific IP Address Destination Packet:-



*Ethernet

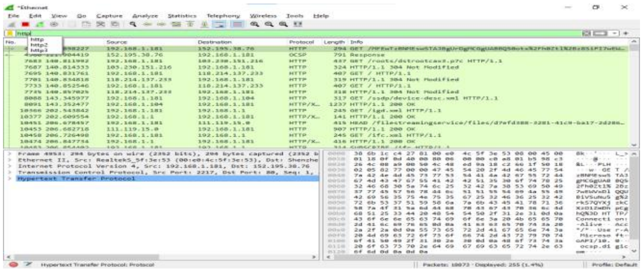
ip.dst == 192.168.1.181

```
No.   Time        Source          Destination     Protocol Length Info
18044 729.908129  192.168.1.104   192.168.1.181   TCP      164 8009 → 2275 [PSH, ACK] Seq=19317 Ack=13350 Win=66624 Len=110 […
18046 729.973185  204.79.197.222  192.168.1.181   TCP       60 443 → 2410 [RST, ACK] Seq=490 Ack=1593 Win=0 Len=0
18055 732.466183  204.79.197.200  192.168.1.181   TCP       60 443 → 2404 [RST, ACK] Seq=47906 Ack=7448 Win=0 Len=0
18063 733.284658  192.168.1.104   192.168.1.181   TCP      164 8009 → 1979 [PSH, ACK] Seq=15841 Ack=15951 Win=1058 Len=110 [T…
18065 733.337595  52.123.129.254  192.168.1.181   TCP       60 443 → 2407 [RST, ACK] Seq=1050 Ack=1120 Win=0 Len=0
18098 735.126829  192.168.1.104   192.168.1.181   TCP      164 8009 → 2275 [PSH, ACK] Seq=19427 Ack=13460 Win=66624 Len=110 […
18111 738.408512  192.168.1.104   192.168.1.181   TCP      164 8009 → 1979 [PSH, ACK] Seq=15951 Ack=16061 Win=1058 Len=110 [T…
18142 740.160171  192.168.1.104   192.168.1.181   TCP      164 8009 → 2275 [PSH, ACK] Seq=19537 Ack=13570 Win=66624 Len=110 […
18155 742.395640  192.168.1.104   192.168.1.181   UDP      540 37590 → 62698 Len=498
18159 743.419890  192.168.1.104   192.168.1.181   UDP      540 33763 → 62698 Len=498
18160 743.425473  192.168.1.104   192.168.1.181   TCP      164 8009 → 1979 [PSH, ACK] Seq=16061 Ack=16171 Win=1058 Len=110 [T…
18167 744.446310  192.168.1.104   192.168.1.181   UDP      540 49820 → 62698 Len=498
18176 745.271316  192.168.1.104   192.168.1.181   TCP      164 8009 → 2275 [PSH, ACK] Seq=19647 Ack=13680 Win=66624 Len=110 […
18179 745.381939  192.168.1.104   192.168.1.181   UDP      540 58558 → 62698 Len=498
18217 748.428245  192.168.1.104   192.168.1.181   TCP      164 8009 → 1979 [PSH, ACK] Seq=16171 Ack=16281 Win=1058 Len=110 [T…
18230 750.263213  192.168.1.104   192.168.1.181   TCP      164 8009 → 2275 [PSH, ACK] Seq=19757 Ack=13790 Win=66624 Len=110 […

> Frame 15: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bit
> Ethernet II, Src: OnePlusE_2b:39:7d (a0:91:a2:2b:39:7d), Dst: Realtek
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.181
> Transmission Control Protocol, Src Port: 8009, Dst Port: 1494, Seq: 1
```

wireshark_Ethernet8PL561.pcapng | Packets: 18240 · Displayed: 5802 (31.8%) | Profile: Default

Display packets by using HTTP Protocol:-



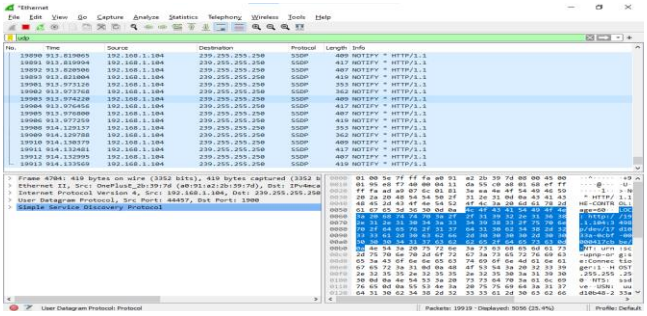
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3

```
No.    Time            Source            Destination       Protocol  Length Info
  4[illegible]898227       192.168.1.181     152.195.38.76     HTTP       294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ5Bots%2Fh0Zt1%2Bz8SiPI7wEW…
  4960 [illegible]904419       152.195.38.76     192.168.1.181     OCSP       791 Response
  7683 140.811982      192.168.1.181     103.230.151.216   HTTP       437 GET /roots/dstrootcax3.p7c HTTP/1.1
  7687 140.814333      103.230.151.216   192.168.1.181     HTTP       324 HTTP/1.1 304 Not Modified
  7695 140.831761      192.168.1.181     118.214.137.233   HTTP       407 GET / HTTP/1.1
  7701 140.834818      118.214.137.233   192.168.1.181     HTTP       319 HTTP/1.1 304 Not Modified
  7733 140.852546      192.168.1.181     118.214.137.233   HTTP       407 GET / HTTP/1.1
  7735 140.857025      118.214.137.233   192.168.1.181     HTTP       318 HTTP/1.1 304 Not Modified
  8088 143.345977      192.168.1.181     192.168.1.104     HTTP       317 GET /ssdp/device-desc.xml HTTP/1.1
  8091 143.352477      192.168.1.104     192.168.1.181     HTTP/X…   1237 HTTP/1.1 200 OK
 10366 202.543842      192.168.1.181     192.168.1.1       HTTP       245 GET /igd.xml HTTP/1.1
 10377 202.609554      192.168.1.1       192.168.1.181     HTTP/X…    141 HTTP/1.1 200 OK
 10451 206.678457      192.168.1.181     111.119.15.0      HTTP       415 HEAD /filestreamingservice/files/d7efd388-3281-41c9-ba17-2d286…
 10453 206.682718      111.119.15.0      192.168.1.181     HTTP       907 HTTP/1.1 200 OK
 10458 206.726498      192.168.1.181     192.168.1.1       HTTP       245 GET /ifc.xml HTTP/1.1
 10474 206.847734      192.168.1.1       192.168.1.181     HTTP/X…    416 HTTP/1.1 200 OK
```

```
> Frame 4953: 294 bytes on wire (2352 bits), 294 bytes captured (2352 b
> Ethernet II, Src: RealtekS_5f:3e:53 (00:e0:4c:5f:3e:53), Dst: Shenzhe
> Internet Protocol Version 4, Src: 192.168.1.181, Dst: 152.195.38.76
> Transmission Control Protocol, Src Port: 2217, Dst Port: 80, Seq: 1,
> Hypertext Transfer Protocol
```

Hypertext Transfer Protocol: Protocol | Packets: 10073 · Displayed: 255 (1.4%) | Profile: Default

UDP:-



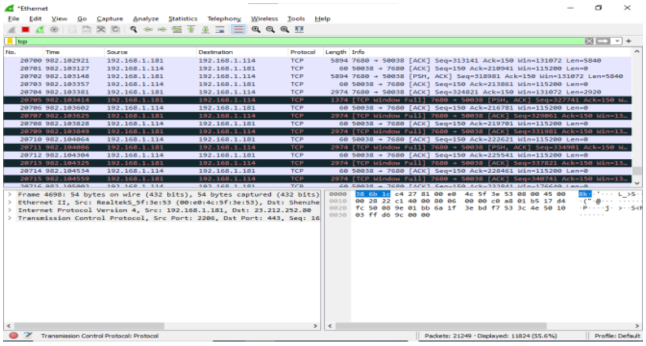
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
No.    Time            Source            Destination       Protocol  Length Info
 19890 913.819065      192.168.1.104     239.255.255.250   SSDP       409 NOTIFY * HTTP/1.1
 19891 913.819994      192.168.1.104     239.255.255.250   SSDP       417 NOTIFY * HTTP/1.1
 19892 913.820506      192.168.1.104     239.255.255.250   SSDP       407 NOTIFY * HTTP/1.1
 19893 913.821004      192.168.1.104     239.255.255.250   SSDP       419 NOTIFY * HTTP/1.1
 19901 913.973126      192.168.1.104     239.255.255.250   SSDP       353 NOTIFY * HTTP/1.1
 19902 913.973768      192.168.1.104     239.255.255.250   SSDP       362 NOTIFY * HTTP/1.1
 19903 913.974220      192.168.1.104     239.255.255.250   SSDP       409 NOTIFY * HTTP/1.1
 19904 913.976456      192.168.1.104     239.255.255.250   SSDP       417 NOTIFY * HTTP/1.1
 19905 913.976800      192.168.1.104     239.255.255.250   SSDP       407 NOTIFY * HTTP/1.1
 19906 913.977259      192.168.1.104     239.255.255.250   SSDP       419 NOTIFY * HTTP/1.1
 19908 914.129137      192.168.1.104     239.255.255.250   SSDP       353 NOTIFY * HTTP/1.1
 19909 914.129788      192.168.1.104     239.255.255.250   SSDP       362 NOTIFY * HTTP/1.1
 19910 914.130379      192.168.1.104     239.255.255.250   SSDP       409 NOTIFY * HTTP/1.1
 19911 914.132481      192.168.1.104     239.255.255.250   SSDP       417 NOTIFY * HTTP/1.1
 19912 914.132995      192.168.1.104     239.255.255.250   SSDP       407 NOTIFY * HTTP/1.1
 19913 914.133569      192.168.1.104     239.255.255.250   SSDP       419 NOTIFY * HTTP/1.1
```

```
> Frame 4704: 419 bytes on wire (3352 bits), 419 bytes captured (3352 b
> Ethernet II, Src: OnePlusE_2b:39:7d (a0:91:a2:2b:39:7d), Dst: IPv4mca
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 44457, Dst Port: 1900
> Simple Service Discovery Protocol
```

User Datagram Protocol: Protocol | Packets: 19919 · Displayed: 5056 (25.4%) | Profile: Default

TCP:-



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.    Time            Source            Destination       Protocol  Length Info
 20700 982.102921      192.168.1.181     192.168.1.114     TCP       5894 7680 → 50038 [ACK] Seq=313141 Ack=150 Win=131072 Len=5840
 20701 982.103127      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=210941 Win=115200 Len=0
 20702 982.103148      192.168.1.181     192.168.1.114     TCP       5894 7680 → 50038 [PSH, ACK] Seq=318981 Ack=150 Win=131072 Len=5840
 20703 982.103357      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=213861 Win=115200 Len=0
 20704 982.103381      192.168.1.181     192.168.1.114     TCP       2974 7680 → 50038 [ACK] Seq=324821 Ack=150 Win=131072 Len=2920
 20705 982.103414      192.168.1.181     192.168.1.114     TCP       1374 [TCP Window Full] 7680 → 50038 [PSH, ACK] Seq=327741 Ack=150 W…
 20706 982.103602      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=216781 Win=115200 Len=0
 20707 982.103625      192.168.1.181     192.168.1.114     TCP       2974 [TCP Window Full] 7680 → 50038 [ACK] Seq=329061 Ack=150 Win=13…
 20708 982.103828      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=219701 Win=115200 Len=0
 20709 982.103849      192.168.1.181     192.168.1.114     TCP       2974 [TCP Window Full] 7680 → 50038 [ACK] Seq=331981 Ack=150 Win=13…
 20710 982.104064      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=222621 Win=115200 Len=0
 20711 982.104086      192.168.1.181     192.168.1.114     TCP       2974 [TCP Window Full] 7680 → 50038 [PSH, ACK] Seq=334901 Ack=150 W…
 20712 982.104304      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=225541 Win=115200 Len=0
 20713 982.104325      192.168.1.181     192.168.1.114     TCP       2974 [TCP Window Full] 7680 → 50038 [ACK] Seq=337821 Ack=150 Win=13…
 20714 982.104534      192.168.1.114     192.168.1.181     TCP         60 50038 → 7680 [ACK] Seq=150 Ack=228461 Win=115200 Len=0
 20715 982.104559      192.168.1.181     192.168.1.114     TCP       2974 [TCP Window Full] 7680 → 50038 [ACK] Seq=340741 Ack=150 Win=13…
```

```
> Frame 4698: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: RealtekS_5f:3e:53 (00:e0:4c:5f:3e:53), Dst: Shenzhe
> Internet Protocol Version 4, Src: 192.168.1.181, Dst: 23.212.252.80
> Transmission Control Protocol, Src Port: 2206, Dst Port: 443, Seq: 16
```

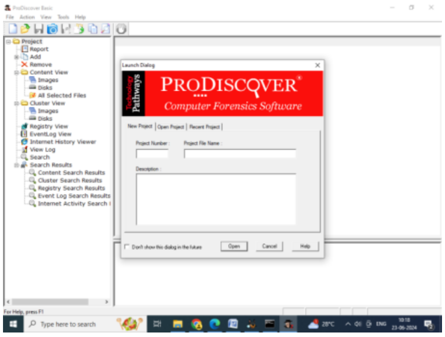
```
0000  38 6b 1c c4 27 81 00 e0  4c 5f 3e 53 08 00 45 00
0010  00 28 22 c1 40 00 80 06  00 00 c0 a8 01 b5 17 d4
0020  fc 50 08 9e 01 bb 6a 1f  3e bd f7 53 3c 4e 50 10
0030  03 ff d6 9c 00 00
```

Transmission Control Protocol: Protocol | Packets: 21249 · Displayed: 11824 (55.6%) | Profile: Default

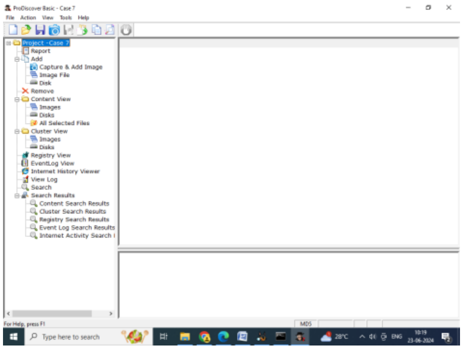
Practical 6

Using Data Acquisition Tools [ProDiscover Pro]

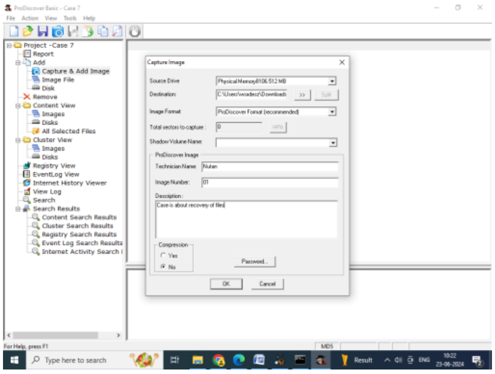
☆ Step 1: Open Prodiscover



☆ Step 2: Create case by entering details and click on open and click on add -□ Capture & add image



☆ Step 3: Enter details and click OK



Capture Image

Source Drive: Physical Memory8106.512 MB

Destination: C:\Users\wsxdesz\Download

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 0

Shadow Volume Name:

ProDiscover Image

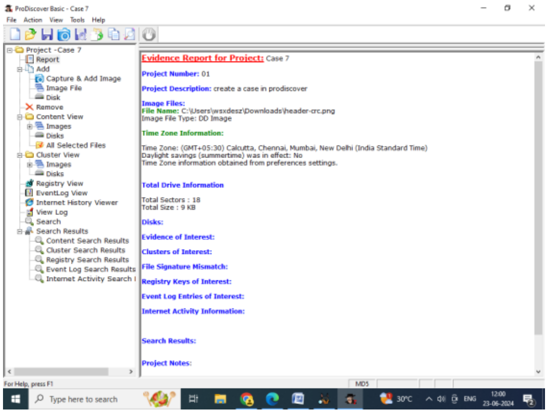
Technician Name: Nutan

Image Number: 01

Description : Case is about recovery of files

Compression: ○ Yes ● No

☆ Step 4



Evidence Report for Project: Case 7

Project Number: 01

Project Description: create a case in prodiscover

Image Files:
File Name: C:\Users\wsxdesz\Downloads\header-crc.png
Image File Type: DD Image

Time Zone Information:

Time Zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi (India Standard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained from preferences settings.

Total Drive Information

Total Sectors : 18
Total Size : 9 KB

Disks:

Evidence of Interest:

Clusters of Interest:

File Signature Mismatch:

Registry Keys of Interest:

Event Log Entries of Interest:

Internet Activity Information:

Search Results:

Project Notes:

Practical 7

Using Steganography Tools [S-Tools]

Method 1:-

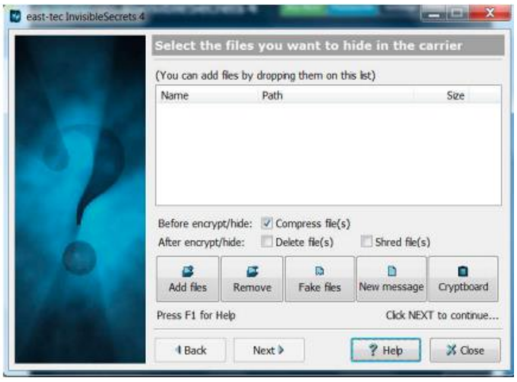
1. Download and save the zip file containing the steganography tools and image files.
2. Unzip the file steg.zip into an empty directory. If you do not have the unzip program already, you can get one here .
3. Put a shortcut to S-tools.exe on your desktop by dragging it from Windows Explorer.
4. Drag the zebras.bmp file to your desktop. Do not make a shortcut. The file itself must be moved there.
5. Start S-tools.exe by double clicking on the icon on the desktop. A window will appear.
6. Drag the zebras.bmp file to the S-tools window.
7. Right click on the zebras pictures and select Reveal from the menu.
8. Fill in the 3-character pass phrase 'abc' (without the quotes) in two places. Leave IDEA as the encryption algorithm. Click on OK.
9. Wait until the Revealed Archive dialog box appears. This may take a minute or two.
10. Right click on any item and select Save As to save the file. Repeat for the other ones. These are the hidden files.
11. The file original-zebras.bmp is the file before the steganography was done, in case you wish to compare the 'before' and 'after' images.

Original Image

Stegno graphy Image

Method 2:-

1. Click on the Add file button to select the file you want to hide in the carrier



east-tec InvisibleSecrets 4

Select the files you want to hide in the carrier

(You can add files by dropping them on this list)

Name	Path	Size

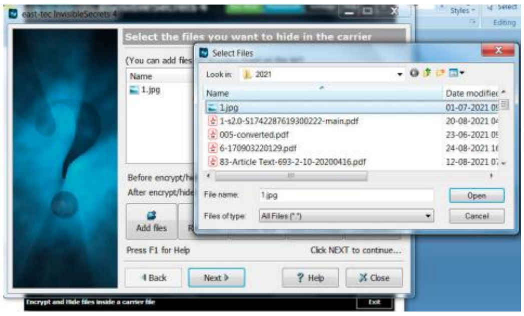
Before encrypt/hide: ☑ Compress file(s)

After encrypt/hide: □ Delete file(s) □ Shred file(s)

Press F1 for Help

Click NEXT to continue...

2. Select the file you want to hide



Select Files

Look in: 2021

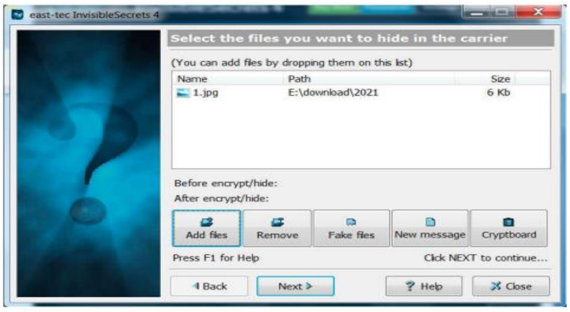
Name	Date modified
1.jpg	01-07-2021
1-s2.0-S1742287619300222-main.pdf	20-08-2021
005-converted.pdf	23-06-2021
6-170903220129.pdf	24-08-2021
83-Article Text-693-2-10-20200416.pdf	12-08-2021

File name: 1.jpg

Files of type: All Files (*.*)

Encrypt and Hide files inside a carrier file

east-tec InvisibleSecrets 4
Select the files you want to hide in the carrier
Open
Cancel
Add files
Press F1 for Help
Click NEXT to continue...
Back
Next
Help
Close
Exit



east-tec InvisibleSecrets 4

Select the files you want to hide in the carrier

(You can add files by dropping them on this list)

Name	Path	Size
1.jpg	E:\download\2021	6 Kb

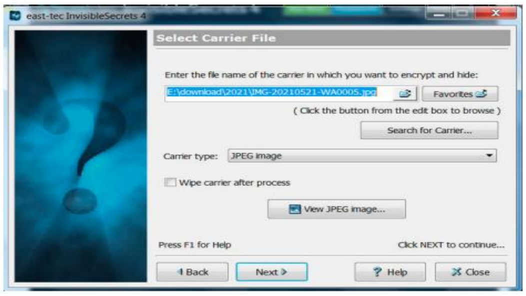
Before encrypt/hide:

After encrypt/hide:

Press F1 for Help

Click NEXT to continue...

3. Click on the Next button and Select the Carrier file and the carrier type as jpeg image. Then Click on the Nextbutton



east-tec InvisibleSecrets 4

Select Carrier File

Enter the file name of the carrier in which you want to encrypt and hide:

E:\download\2021\IMG-20210521-WA0005.jpg

(Click the button from the edit box to browse)

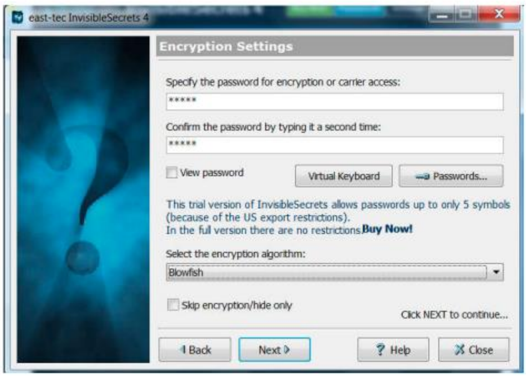
Carrier type: JPEG image

□ Wipe carrier after process

Press F1 for Help

Click NEXT to continue...

4. Now specify the password for the Encryption and retype the password and click on theNextbutton



east-tec InvisibleSecrets 4

Encryption Settings

Specify the password for encryption or carrier access:

*****

Confirm the password by typing it a second time:

*****

□ View password

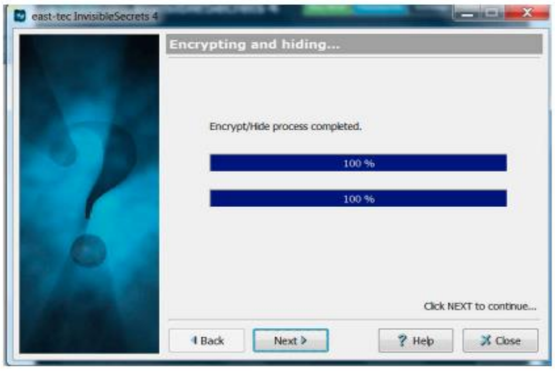
This trial version of InvisibleSecrets allows passwords up to only 5 symbols (because of the US export restrictions).
In the full version there are no restrictions **Buy Now!**

Select the encryption algorithm:

Blowfish

□ Skip encryption/hide only

Click NEXT to continue...



east-tec InvisibleSecrets 4

Encrypting and hiding...

Encrypt/Hide process completed.

100 %

100 %

Click NEXT to continue...

Finally you will get a Steganographic image.