

SIES COLLEGE OF ARTS, SCIENCE & COMMERCE
(AUTONOMOUS)
SION(W), MUMBAI – 22

DEPARTMENT OF INFORMATION TECHNOLOGY

M.Sc. (I.T.) PART – II, SEMESTER – III

Practical Journal
for
the subject

IT in Forensic Science

Submitted by

Asai Prathamesh Mangesh
SMIT2324003

For the academic year
2023-2024



SIES College of Arts, Science and Commerce (Autonomous),

Sion (W), Mumbai – 400 022.

Department of Information Technology

CERTIFICATE

This is to certify that **Mr. Asai Prathamesh Mangesh** of MSc [Information Technology] Semester - III, Seat No. **SMIT2324003** has successfully completed the practicals for the subject of **IT in Forensic Science** as a partial fulfillment of the degree M.Sc. (I.T.) during the academic year 2023-24.

Faculty-in-Charge

Anam Khan

Course Co-Ordinator

Sudha Bhagavatheeswaran

Examiner

Anam Khan

College Seal

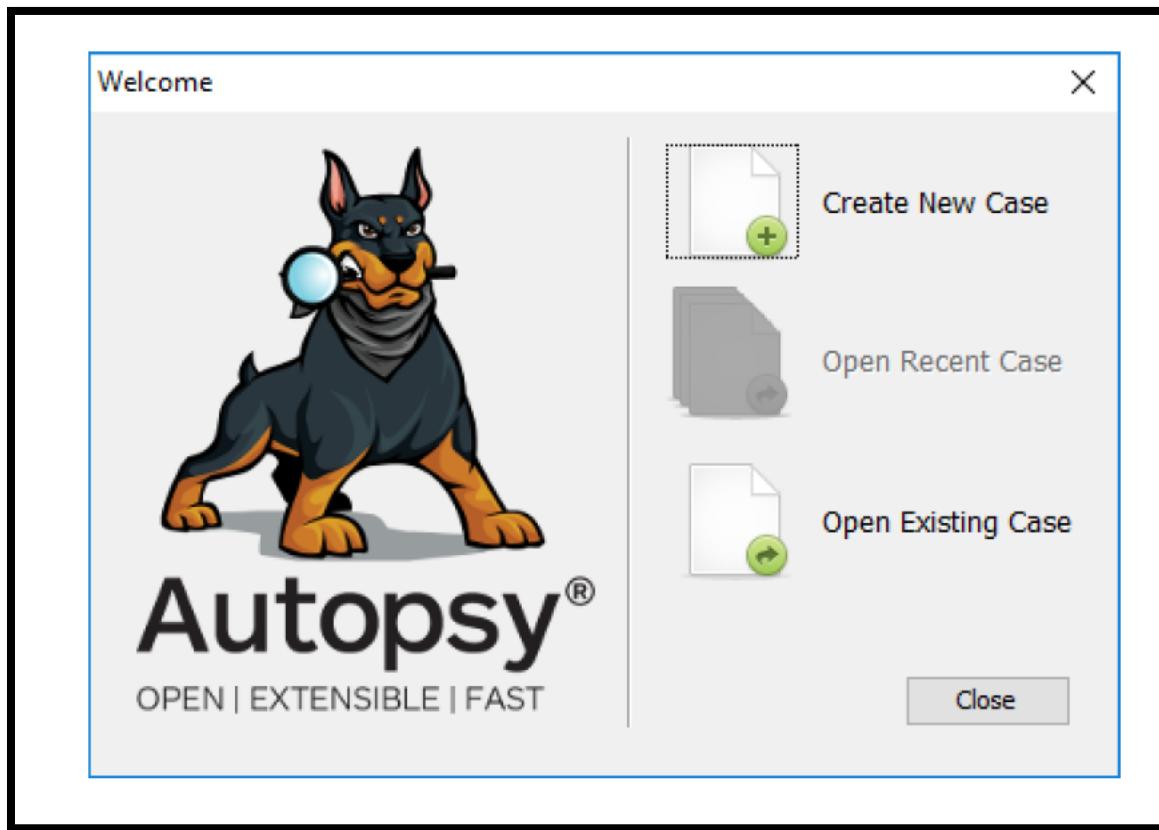
Date: 11/11/2023

INDEX

Sr.no	Topic	Sign
1	Analyze hard drive or smartphones using forensic tool or File System Analysis Using the Slueth Kit.	
2	Analyze DNS using WHOIS Tool. Detect OS, Host name using cmd. Detect session and ports through packet sniffing. (Nmap) & command line utilities.	
3	Capture the physical memory of a computer and analyze artefacts in memory. (FTK)	
4	Calculate MD5 & SHA1 (CrypTool)	
5	Use tool to collect, preserve digital evidence without compromising system data. (FTK Imager)	
6	Acquire web pages for forensic investigation. (Wireshark) or Use traffic capturing and analyzing tool. (Wireshark) Using filters and using test login page.	
7	Use tools that scan a hard drive, locate deleted media and scan hard drive. (FTK)	
8	Use a tool to scan drive and it's slack space. (ProDiscover)	
9	Hide text into image. (QuickStego, STool)	
10	Use Email Forensic Tools for Email Recovery Mobile Forensics	

PRACTICAL NO 01: Analyse hard drives or smart phones using forensic tools (Using Autopsy Tool)

Step 1: Download Autopsy



Step 2: Add case details (suggested make one folder of CF Prac)

A screenshot of the "New Case Information" dialog box. The left sidebar shows "Steps" with "Case Info" selected. The main area is titled "Case Info" and contains the following fields:

- "Enter New Case Information:"
- "Case Name:" input field containing "testprac"
- "Base Directory:" input field containing "F:\CFprac" with a "Browse" button to its right
- "Case Type:" radio buttons for "Single-user" (selected) and "Multi-user"
- "Case data will be stored in the following directory:" input field containing "F:\CFprac\testprac"

At the bottom of the dialog are buttons for "< Back", "Next >", "Finish", "Cancel", and "Help".

New Case Information

Steps

1. Case Info
2. Additional Information

Additional Information

Optional: Set Case Number and Examiner

Case Number: 001

Examiner: XYZ

< Back Next > Finish Cancel Help

Step 3: Add any file on which you want to investigate

Add Data Source

Steps

1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

Enter Data Source Information wizard (Step 1 of 3)

Select source type to add: Image File

Browse for an image file: F:\sem4\ComputerForensics\precious.img

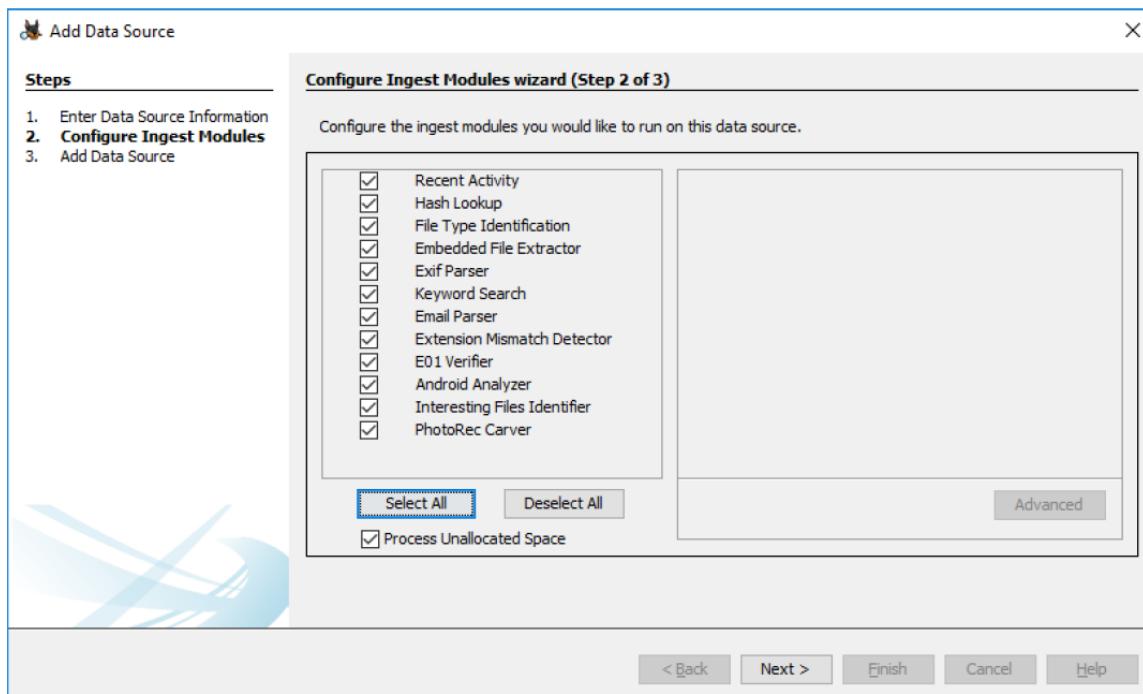
Please select the input timezone: (GMT +5:30) Asia/Calcutta

Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

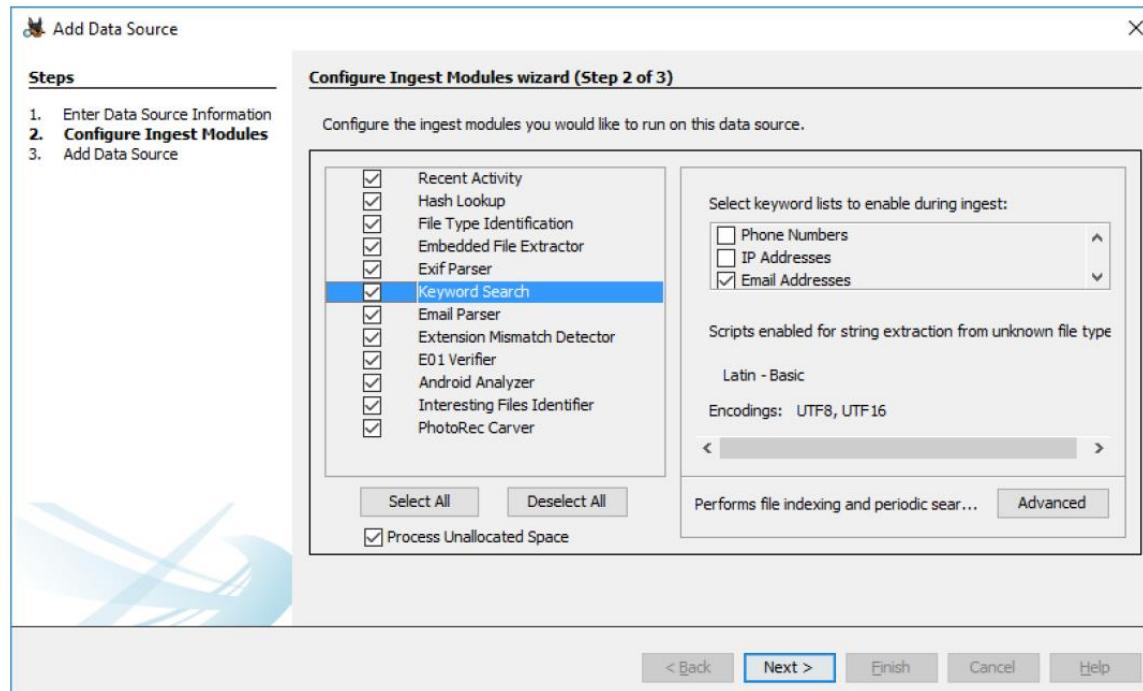
Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

< Back Next > Finish Cancel Help

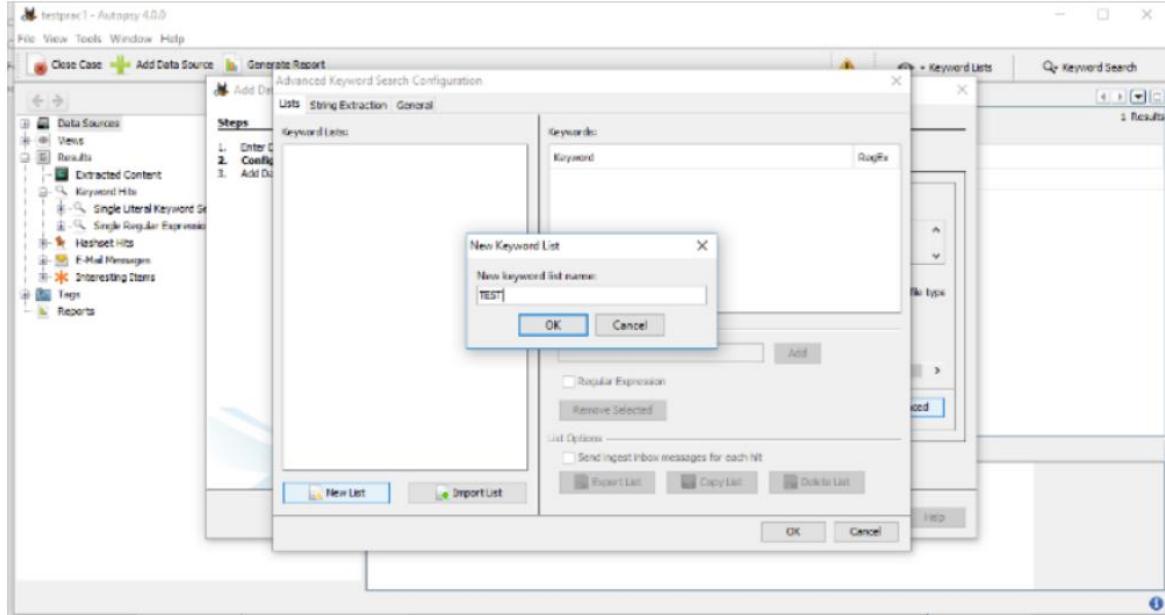
Step 4: Configure ingest module



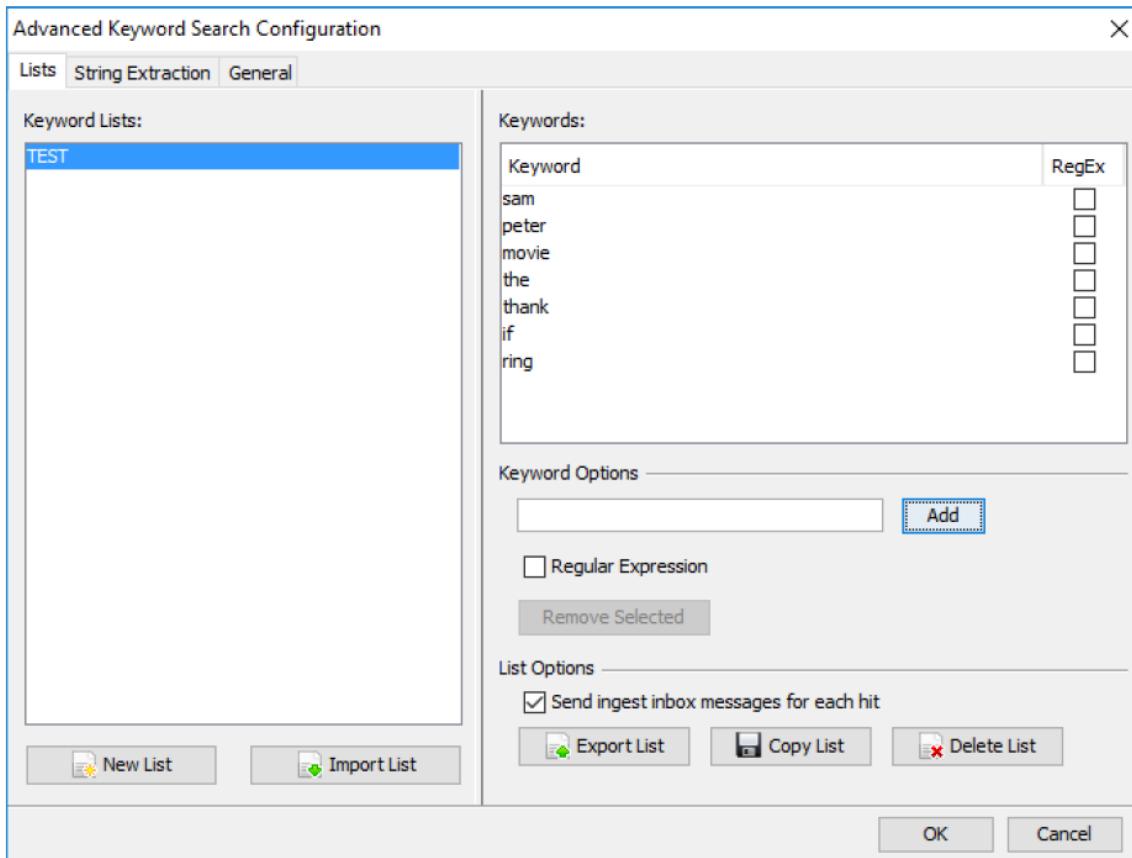
Step 5: click on keyword search



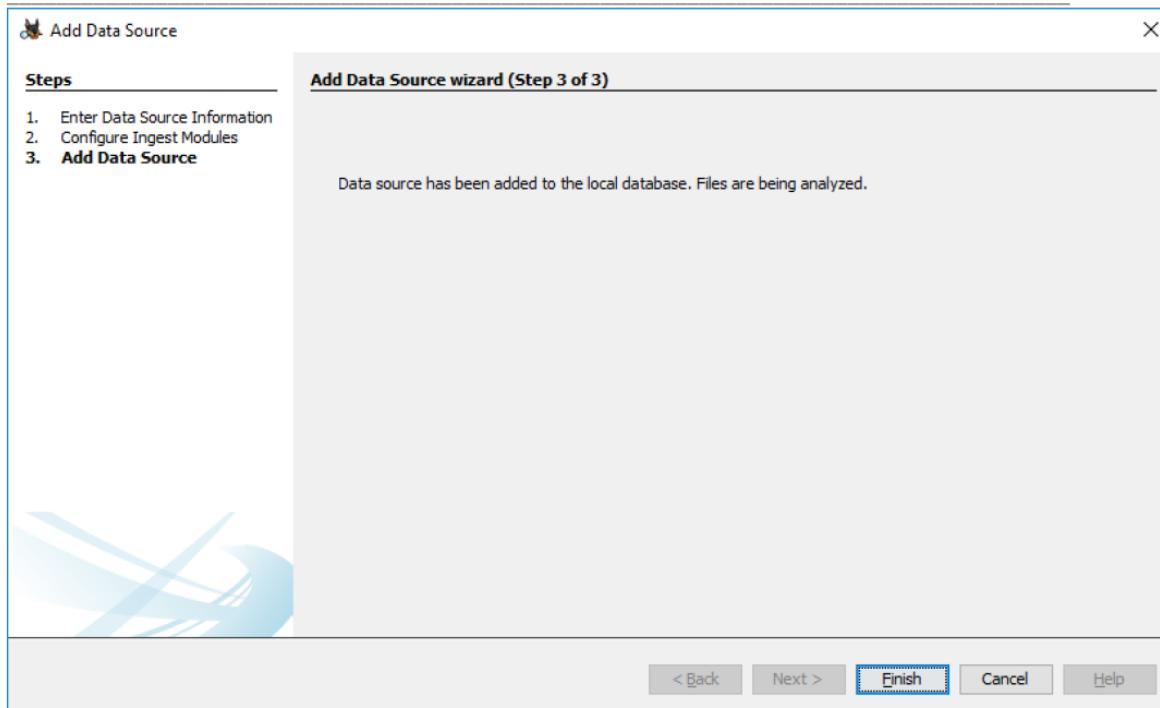
Step 6: then click on advance & add the following or your own required keywords



Step 7: you can click on add & add the following keywords



Step 8: Click on finish



Step 9: Check the data

The screenshot shows the Autopsy 4.0 interface. The left sidebar contains a tree view of data sources, views, results, keyword hits, and tags. The 'Results' section is expanded, showing various analysis categories like 'Extracted Content', 'Devices Attached', etc. The 'Directory Listing' tab is selected, showing a table with the following data:

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-49663)	1	0	67	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 97-128269920)	2	97	250527	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 250624-381183)	3	250624	255	Unallocated	Unallocated

Step 10: Generate a report

 Generate Report X

Select and Configure Report Modules

Report Modules:

<input checked="" type="radio"/> Results - HTML <input type="radio"/> Results - Excel <input type="radio"/> Files - Text <input type="radio"/> Google Earth/KML <input type="radio"/> STIX <input type="radio"/> TSK Body File	A report about results and tagged items in HTML format. <i>This report will be configured on the next screen.</i>
---	--

[Next >](#) [Back <](#) [Finish](#) [Cancel](#) [Help](#)

 Generate Report X

Configure Artifact Reports

Select which data to report on:

All Results Tagged Results

Select All Deselect All

Data Types

< Back Next > Finish Cancel Help

 Report Generation Progress... X

Report Generation Progress

Complete

Results - HTML - <E:\CFprac\testprac1\Reports\testprac1 03-16-2017-21-53-08\HTML Report\index.html>
Complete

Cancel Close

Autopsy Report for case X

file:///F:/CFprac/testprac1/Reports/testprac1%2003-16-2017-21-53-08/HTML%20Report/index.html

Report Navigation

- Case Summary
- Devices Attached (19)
- E-Mail Messages (33)
- Encryption Detected (2)
- Extension Mismatch Detected (27)
- Installed Programs (61)
- Keyword Hits (455)
- Operating System Information (2)
- Operating System User Account (13)
- Recent Documents (9)
- Remote Drive (1)
- Tagged Files (0)
- Tagged Results (0)
- Thumbnails (0)
- Web Bookmarks (24)
- Web Cookies (84)

Autopsy Forensic Report

HTML Report Generated on 2017/03/16 21:53:08

Case: testprac1
Case Number: 001
Examiner: XYZ
Number of Images: 1

Image Information:

precious.img

Timezone: Asia/Calcutta
Path: F:\sem4\ComputerForensics\precious.img



PRACTICAL NO 02: Detect OS, hostname, sessions and open ports through packet sniffing.

(Tool used: Nmap)

Command Executed on Window command prompt

Commands:

```
Microsoft Windows [Version 10.0.22621.525]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sies>systeminfo

Host Name: DESKTOP-NUJUK7F
OS Name: Microsoft Windows 11 Pro
OS Version: 10.0.22621 N/A Build 22621
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: sies
Registered Organization:
Product ID: 00331-20210-00000-AA302
Original Install Date: 17-08-2023, 13:04:53
System Boot Time: 05-09-2023, 15:23:32
System Manufacturer: Dell Inc.
System Model: OptiPlex 3090
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 165 Stepping 3 GenuineIntel ~3701 Mhz
BIOS Version: Dell Inc. 2.0.7, 25-11-2021
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: 00004009
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 7,904 MB
Available Physical Memory: 1,543 MB
Virtual Memory: Max Size: 12,768 MB
Virtual Memory: Available: 2,190 MB
Virtual Memory: In Use: 10,578 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\DESKTOP-NUJUK7F
Hotfix(s): 3 Hotfix(s) Installed.
[01]: KB5017026
[02]: KB5019311
[03]: KB5017233
Network Card(s): 3 NIC(s) Installed.
[01]: Realtek PCIe GbE Family Controller
      Connection Name: Ethernet
      DHCP Enabled: Yes
      DHCP Server: 192.168.10.2
      IP address(es)
      [01]: 192.168.11.120
      [02]: fe80::d4e8:f697:7374:4c2b
[02]: VMware Virtual Ethernet Adapter for VMnet1
      Connection Name: Ethernet 3
      DHCP Enabled: No
```

```
C:\Users\sies>hostname
```

```
DESKTOP-NUJUK7F
```

```
C:\Users\sies>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49685	DESKTOP-NUJUK7F:49686	ESTABLISHED
TCP	127.0.0.1:49686	DESKTOP-NUJUK7F:49685	ESTABLISHED
TCP	127.0.0.1:49687	DESKTOP-NUJUK7F:49688	ESTABLISHED
TCP	127.0.0.1:49688	DESKTOP-NUJUK7F:49687	ESTABLISHED
TCP	127.0.0.1:49763	DESKTOP-NUJUK7F:49764	ESTABLISHED
TCP	127.0.0.1:49764	DESKTOP-NUJUK7F:49763	ESTABLISHED
TCP	127.0.0.1:50033	DESKTOP-NUJUK7F:50034	ESTABLISHED
TCP	127.0.0.1:50034	DESKTOP-NUJUK7F:50033	ESTABLISHED
TCP	127.0.0.1:56018	DESKTOP-NUJUK7F:56011	ESTABLISHED
TCP	127.0.0.1:56011	DESKTOP-NUJUK7F:56010	ESTABLISHED
TCP	127.0.0.1:56281	DESKTOP-NUJUK7F:56282	ESTABLISHED
TCP	127.0.0.1:56282	DESKTOP-NUJUK7F:56281	ESTABLISHED
TCP	127.0.0.1:56283	DESKTOP-NUJUK7F:56284	ESTABLISHED
TCP	127.0.0.1:56284	DESKTOP-NUJUK7F:56283	ESTABLISHED
TCP	127.0.0.1:56285	DESKTOP-NUJUK7F:56286	ESTABLISHED
TCP	127.0.0.1:56286	DESKTOP-NUJUK7F:56285	ESTABLISHED
TCP	127.0.0.1:56287	DESKTOP-NUJUK7F:56288	ESTABLISHED
TCP	127.0.0.1:56288	DESKTOP-NUJUK7F:56287	ESTABLISHED
TCP	127.0.0.1:56289	DESKTOP-NUJUK7F:56290	ESTABLISHED
TCP	127.0.0.1:56290	DESKTOP-NUJUK7F:56289	ESTABLISHED
TCP	127.0.0.1:56291	DESKTOP-NUJUK7F:56292	ESTABLISHED
TCP	127.0.0.1:56292	DESKTOP-NUJUK7F:56291	ESTABLISHED
TCP	127.0.0.1:56293	DESKTOP-NUJUK7F:56294	ESTABLISHED
TCP	127.0.0.1:56294	DESKTOP-NUJUK7F:56293	ESTABLISHED
TCP	127.0.0.1:56295	DESKTOP-NUJUK7F:56296	ESTABLISHED
TCP	127.0.0.1:56296	DESKTOP-NUJUK7F:56295	ESTABLISHED
TCP	127.0.0.1:56297	DESKTOP-NUJUK7F:56298	ESTABLISHED
TCP	127.0.0.1:56298	DESKTOP-NUJUK7F:56297	ESTABLISHED
TCP	127.0.0.1:56299	DESKTOP-NUJUK7F:56300	ESTABLISHED
TCP	127.0.0.1:56300	DESKTOP-NUJUK7F:56299	ESTABLISHED
TCP	127.0.0.1:56301	DESKTOP-NUJUK7F:56302	ESTABLISHED
TCP	127.0.0.1:56302	DESKTOP-NUJUK7F:56301	ESTABLISHED
TCP	127.0.0.1:56303	DESKTOP-NUJUK7F:56304	ESTABLISHED
TCP	127.0.0.1:56304	DESKTOP-NUJUK7F:56303	ESTABLISHED
TCP	127.0.0.1:56305	DESKTOP-NUJUK7F:56306	ESTABLISHED
TCP	127.0.0.1:56306	DESKTOP-NUJUK7F:56305	ESTABLISHED
TCP	127.0.0.1:56307	DESKTOP-NUJUK7F:56308	ESTABLISHED
TCP	127.0.0.1:56308	DFSKTOP-NUJUK7F:56307	ESTABLISHED
TCP	127.0.0.1:56309	DESKTOP-NUJUK7F:56310	ESTABLISHED
TCP	127.0.0.1:56310	DESKTOP-NUJUK7F:56309	ESTABLISHED
TCP	127.0.0.1:56311	DESKTOP-NUJUK7F:56312	ESTABLISHED

TCP	192.168.11.120:49829	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:50041	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:50066	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:50067	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:50070	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:50080	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:50597	a23-46-9-75:https	CLOSE_WAIT
TCP	192.168.11.120:50600	a23-46-9-50:https	CLOSE_WAIT
TCP	192.168.11.120:50601	a23-46-9-50:https	CLOSE_WAIT
TCP	192.168.11.120:50602	a23-46-9-50:https	CLOSE_WAIT
TCP	192.168.11.120:50603	a23-46-9-50:https	CLOSE_WAIT
TCP	192.168.11.120:50604	a23-46-9-50:https	CLOSE_WAIT
TCP	192.168.11.120:50605	a23-46-9-50:https	CLOSE_WAIT
TCP	192.168.11.120:51171	20.24.121.134:https	CLOSE_WAIT
TCP	192.168.11.120:51173	20.24.121.134:https	CLOSE_WAIT
TCP	192.168.11.120:51174	20.24.121.134:https	CLOSE_WAIT
TCP	192.168.11.120:51175	20.24.121.134:https	CLOSE_WAIT
TCP	192.168.11.120:56012	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:56017	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:56018	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:56020	DESKTOP-NUJUK7F:1521	ESTABLISHED
TCP	192.168.11.120:56824	dhcpc-192-234-137:https	ESTABLISHED
TCP	192.168.11.120:56825	a-0001:https	CLOSE_WAIT
TCP	192.168.11.120:56831	server-108-159-61-9:https	ESTABLISHED
TCP	192.168.11.120:56834	a-0003:https	CLOSE_WAIT
TCP	192.168.11.120:56840	dns:https	ESTABLISHED
TCP	192.168.11.120:56841	dns:https	ESTABLISHED
TCP	192.168.11.120:56851	204.79.197.239:https	ESTABLISHED
TCP	192.168.11.120:56891	a23-218-90-51:https	ESTABLISHED
TCP	192.168.11.120:56892	204.79.197.239:https	ESTABLISHED
TCP	192.168.11.120:56895	20.198.119.84:https	ESTABLISHED
TCP	192.168.11.120:56898	52.182.143.208:https	ESTABLISHED
TCP	192.168.11.120:56926	a-0003:https	ESTABLISHED
TCP	192.168.11.120:56995	a23-9-240-127:http	ESTABLISHED
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	DESKTOP-NUJUK7F:49677	ESTABLISHED
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	DESKTOP-NUJUK7F:49678	ESTABLISHED
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	DESKTOP-NUJUK7F:49679	ESTABLISHED
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	DESKTOP-NUJUK7F:49680	ESTABLISHED
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	DESKTOP-NUJUK7F:49834	ESTABLISHED
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	DESKTOP-NUJUK7F:49838	ESTABLISHED

```
C:\Users\sies>netstat -ano
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1272
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:902	0.0.0.0:0	LISTENING	4900
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING	4900
TCP	0.0.0.0:1158	0.0.0.0:0	LISTENING	11832
TCP	0.0.0.0:1521	0.0.0.0:0	LISTENING	3972
TCP	0.0.0.0:1831	0.0.0.0:0	LISTENING	9384
TCP	0.0.0.0:1832	0.0.0.0:0	LISTENING	9540
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	5440
TCP	0.0.0.0:3938	0.0.0.0:0	LISTENING	7428
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	8380
TCP	0.0.0.0:5501	0.0.0.0:0	LISTENING	7800
TCP	0.0.0.0:5502	0.0.0.0:0	LISTENING	3076
TCP	0.0.0.0:5520	0.0.0.0:0	LISTENING	11832
TCP	0.0.0.0:5522	0.0.0.0:0	LISTENING	7800
TCP	0.0.0.0:5523	0.0.0.0:0	LISTENING	3076
TCP	0.0.0.0:23232	0.0.0.0:0	LISTENING	15624
TCP	0.0.0.0:33060	0.0.0.0:0	LISTENING	5440
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	996
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	696
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1620
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2324
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3268
TCP	0.0.0.0:49672	0.0.0.0:0	LISTENING	3828
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING	4012
TCP	0.0.0.0:49674	0.0.0.0:0	LISTENING	4020
TCP	0.0.0.0:49675	0.0.0.0:0	LISTENING	3984
TCP	0.0.0.0:49676	0.0.0.0:0	LISTENING	3996
TCP	0.0.0.0:49689	0.0.0.0:0	LISTENING	980
TCP	127.0.0.1:8079	0.0.0.0:0	LISTENING	15624
TCP	127.0.0.1:10000	0.0.0.0:0	LISTENING	9384
TCP	127.0.0.1:27017	0.0.0.0:0	LISTENING	3744
TCP	127.0.0.1:49670	0.0.0.0:0	LISTENING	3972
TCP	127.0.0.1:49685	127.0.0.1:49686	ESTABLISHED	5440
TCP	127.0.0.1:49686	127.0.0.1:49685	ESTABLISHED	5440
TCP	127.0.0.1:49687	127.0.0.1:49688	ESTABLISHED	5440
TCP	127.0.0.1:49688	127.0.0.1:49687	ESTABLISHED	5440
TCP	127.0.0.1:49763	127.0.0.1:49764	ESTABLISHED	7800
TCP	127.0.0.1:49764	127.0.0.1:49763	ESTABLISHED	7800
TCP	127.0.0.1:50033	127.0.0.1:50034	ESTABLISHED	11832
TCP	127.0.0.1:50034	127.0.0.1:50033	ESTABLISHED	11832
TCP	127.0.0.1:56010	127.0.0.1:56011	ESTABLISHED	3076
TCP	127.0.0.1:56011	127.0.0.1:56010	ESTABLISHED	3076
TCP	127.0.0.1:56275	0.0.0.0:0	LISTENING	15036
TCP	127.0.0.1:56281	127.0.0.1:56282	ESTABLISHED	15624

TCP	[::]:1521	[::]:0	LISTENING	3972
TCP	[::]:1831	[::]:0	LISTENING	9384
TCP	[::]:1832	[::]:0	LISTENING	9540
TCP	[::]:3306	[::]:0	LISTENING	5440
TCP	[::]:3938	[::]:0	LISTENING	7428
TCP	[::]:5520	[::]:0	LISTENING	11832
TCP	[::]:5522	[::]:0	LISTENING	7800
TCP	[::]:5523	[::]:0	LISTENING	3076
TCP	[::]:23232	[::]:0	LISTENING	15624
TCP	[::]:33060	[::]:0	LISTENING	5440
TCP	[::]:49664	[::]:0	LISTENING	996
TCP	[::]:49665	[::]:0	LISTENING	696
TCP	[::]:49666	[::]:0	LISTENING	1620
TCP	[::]:49667	[::]:0	LISTENING	2324
TCP	[::]:49668	[::]:0	LISTENING	3268
TCP	[::]:49672	[::]:0	LISTENING	3828
TCP	[::]:49673	[::]:0	LISTENING	4012
TCP	[::]:49674	[::]:0	LISTENING	4020
TCP	[::]:49675	[::]:0	LISTENING	3984
TCP	[::]:49676	[::]:0	LISTENING	3996
TCP	[::]:49689	[::]:0	LISTENING	980
TCP	[::]:49669	[::]:0	LISTENING	4136
TCP	[fe80::757f:28d1:5b9:1ac4%13]:57085	[fe80::757f:28d1:5b9:1ac4%13]:5501	SYN_SENT	9384
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49677	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49678	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49679	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49680	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49834	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49838	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49859	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49866	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49868	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:49902	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1521	[fe80::d4e8:f697:7374:4c2b%12]:50198	ESTABLISHED	3972
TCP	[fe80::d4e8:f697:7374:4c2b%12]:1831	[fe80::d4e8:f697:7374:4c2b%12]:57087	ESTABLISHED	9384
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49677	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	3996
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49678	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	4012
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49679	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	4020
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49680	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	3984
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49834	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	7428
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49838	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	9540
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49859	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	9384
TCP	[fe80::d4e8:f697:7374:4c2b%12]:49866	[fe80::d4e8:f697:7374:4c2b%12]:1521	ESTABLISHED	7428

TCP	[fe80::d4e8:f697:7374:4c2b%12]:57087	[fe80::d4e8:f697:7374:4c2b%12]:1831	ESTABLISHED	13360
UDP	0.0.0.0:123	*.*	6768	
UDP	0.0.0.0:500	*.*	3596	
UDP	0.0.0.0:1434	*.*	3760	
UDP	0.0.0.0:4500	*.*	3596	
UDP	0.0.0.0:5353	*.*	2304	
UDP	0.0.0.0:5355	*.*	2304	
UDP	0.0.0.0:57455	*.*	2304	
UDP	0.0.0.0:58735	*.*	2304	
UDP	127.0.0.1:1900	*.*	6540	
UDP	127.0.0.1:49195	*.*	6540	
UDP	127.0.0.1:63204	127.0.0.1:63204		3672
UDP	192.168.11.120:137	*.*	4	
UDP	192.168.11.120:138	*.*	4	
UDP	192.168.11.120:1900	*.*	6540	
UDP	192.168.11.120:49192	*.*	6540	
UDP	192.168.127.1:137	*.*	4	
UDP	192.168.127.1:138	*.*	4	
UDP	192.168.127.1:1900	*.*	6540	
UDP	192.168.127.1:49194	*.*	6540	
UDP	192.168.199.1:137	*.*	4	
UDP	192.168.199.1:138	*.*	4	
UDP	192.168.199.1:1900	*.*	6540	
UDP	192.168.199.1:49193	*.*	6540	
UDP	[::]:123	*.*	6768	
UDP	[::]:500	*.*	3596	
UDP	[::]:1434	*.*	3760	
UDP	[::]:4500	*.*	3596	
UDP	[::]:5353	*.*	2304	
UDP	[::]:5355	*.*	2304	
UDP	[::]:57455	*.*	2304	
UDP	[::]:58735	*.*	2304	
UDP	[::]:1900	*.*	6540	
UDP	[::]:49191	*.*	6540	
UDP	[fe80::ce4:5605:48a3:f98%6]:1900	*.*	6540	
UDP	[fe80::ce4:5605:48a3:f98%6]:49190	*.*	6540	
UDP	[fe80::757f:28d1:5b9:1ac4%13]:1900	*.*	6540	
UDP	[fe80::757f:28d1:5b9:1ac4%13]:49189	*.*	6540	
UDP	[fe80::d4e8:f697:7374:4c2b%12]:1900	*.*	6540	
UDP	[fe80::d4e8:f697:7374:4c2b%12]:49188	*.*	6540	

```
C:\Users\sies>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 16:39 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00045s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds

C:\Users\sies>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d4e8:f697:7374:4c2b%12
IPv4 Address . . . . . : 192.168.11.120
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 192.168.10.2

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::757f:28d1:5b9:1ac4%13
IPv4 Address . . . . . : 192.168.199.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter Ethernet 4:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ce4:5605:48a3:f98%6
IPv4 Address . . . . . : 192.168.127.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

```
C:\Users\sies>nmap -sA -T4 scanme.sies.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 16:44 India Standard Time
Nmap scan report for scanme.sies.org (69.64.147.244)
Host is up (0.00053s latency).
rDNS record for 69.64.147.244: ash.parking.local
All 1000 scanned ports on scanme.sies.org (69.64.147.244) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds

C:\Users\sies>nslookup
Default Server: dns.google
Address: 8.8.8.8
```

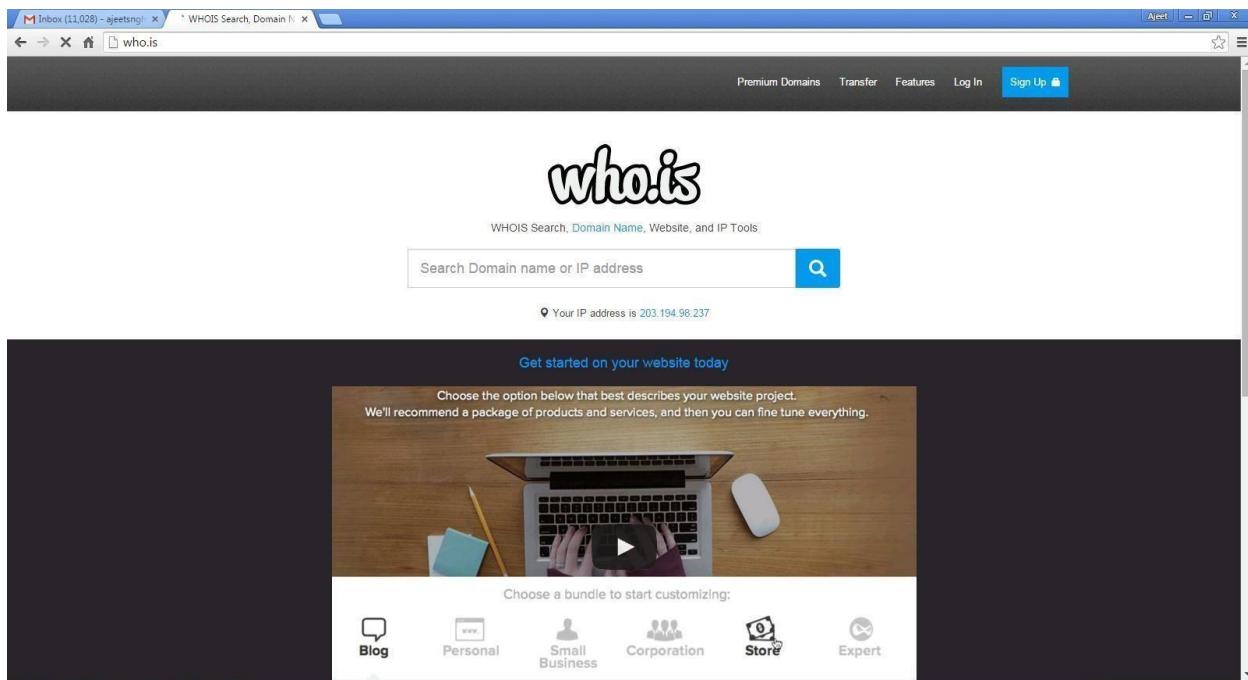
```
C:\Users\sies>nmap -p23,113,139 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 16:59 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.082s latency).

PORT      STATE SERVICE
23/tcp    closed telnet
113/tcp   closed ident
139/tcp   closed netbios-ssn

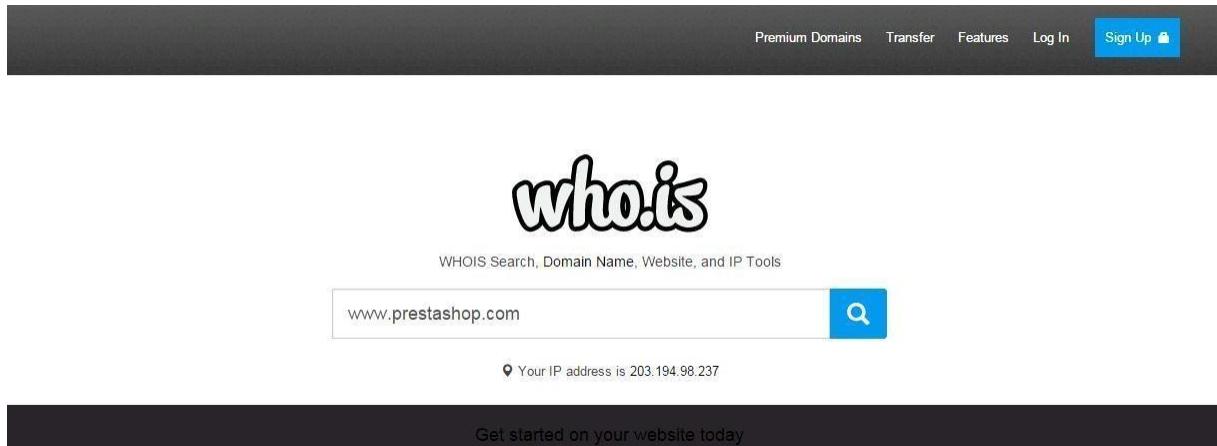
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Using tool who.is

Step1: Open the WHO.is website



Step 2: Enter the website name and hit the “Enter button”.



Step 3: Show you information about www.prestashop.com

Overview for **prestashop.com**: **Whois** Website Info History DNS Records Diagnostics

Registrar Info

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Name Servers

a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64

Raw Registrar Data

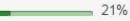
Domain Name: PRESTASHOP.COM
 Registry Domain ID: 920363578_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.mailclub.net
 Registrar URL: http://www.mailclub.fr
 Updated Date: 2015-02-24T05:43:34Z
 Creation Date: 2007-04-11T08:59:05Z
 Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
 Registrar: Mailclub SAS
 Registrar IANA ID: 1290
 Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>
 Registry Registrant ID:
 Registrant Name: NOMS DE DOMAINE Responsable
 Registrant Organization: PRESTASHOP
 Registrant Street: 12, rue d'Amsterdam
 Registrant City: Paris
 Registrant State/Province:
 Registrant Postal Code: 75009
 Registrant Country: FR
 Registrant Phone: +33.140183004
 Registrant Phone Ext:
 Registrant Fax: +33.972111878
 Registrant Fax Ext:
 Registrant Email: domains@prestashop.com
 Registry Admin ID:
 Admin Name: NOMS DE DOMAINE Responsable
 Admin Organization: PRESTASHOP
 Admin Street: 12, rue d'Amsterdam
 Admin City: Paris
 Admin State/Province:
 Admin Postal Code: 75009
 Admin Country: FR
 Admin Phone: +33.140183004
 Admin Phone Ext:
 Admin Fax: +33.972111878
 Admin Fax Ext:
 Admin Email: domains@prestashop.com
 Registry Tech ID:
 Tech Name: TINE, Charles
 Tech Organization: MAILCLUB S.A.S.
 Tech Street: Pole Media de la Belle de Mai 37 rue Guibal
 Tech City: Marseille
 Tech State/Province:

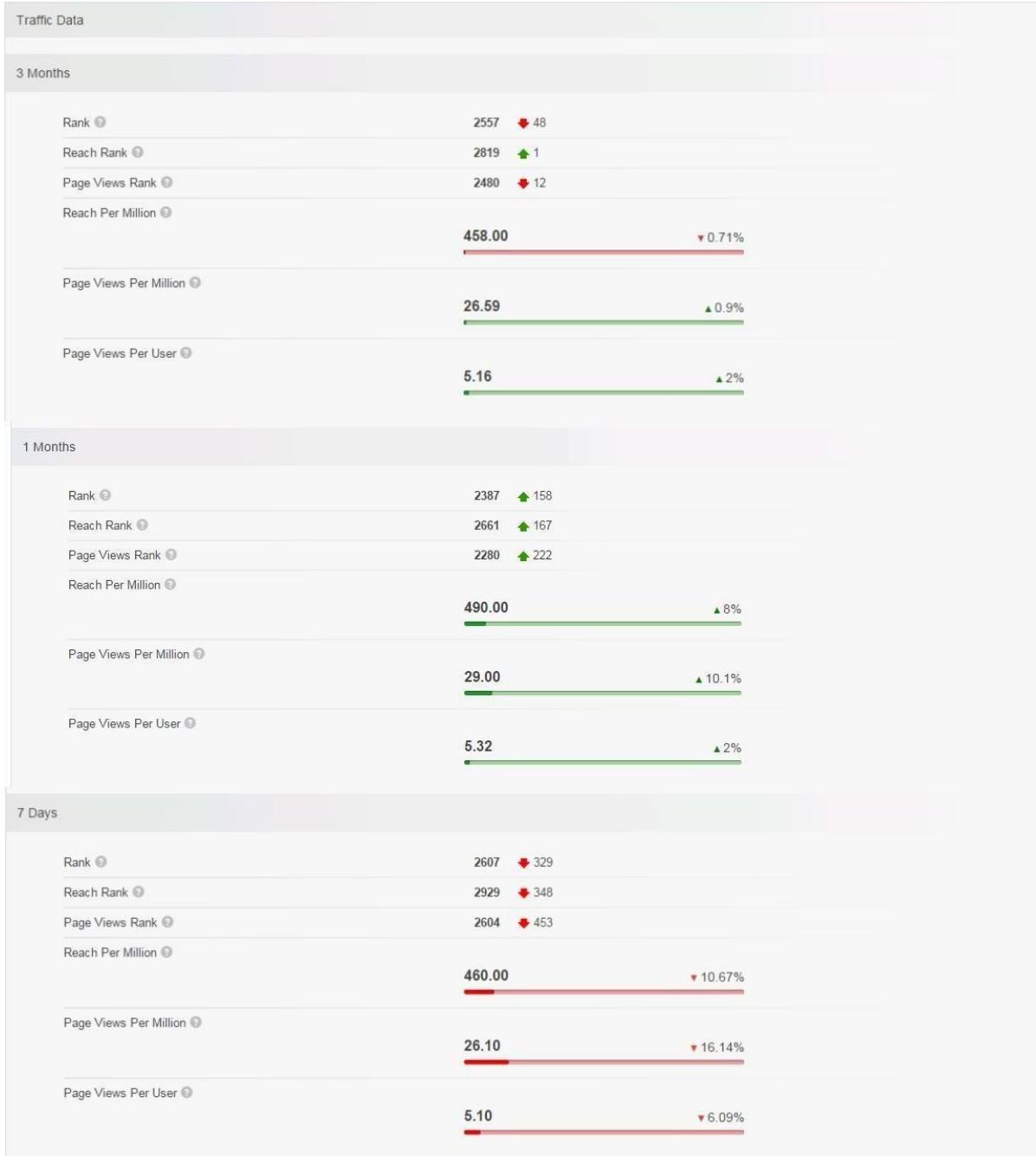
Overview for [prestashop.com](#):[Whois](#)[Website Info](#)[History](#)[DNS Records](#)[Diagnostics](#)🕒 Updated 10 hours ago 

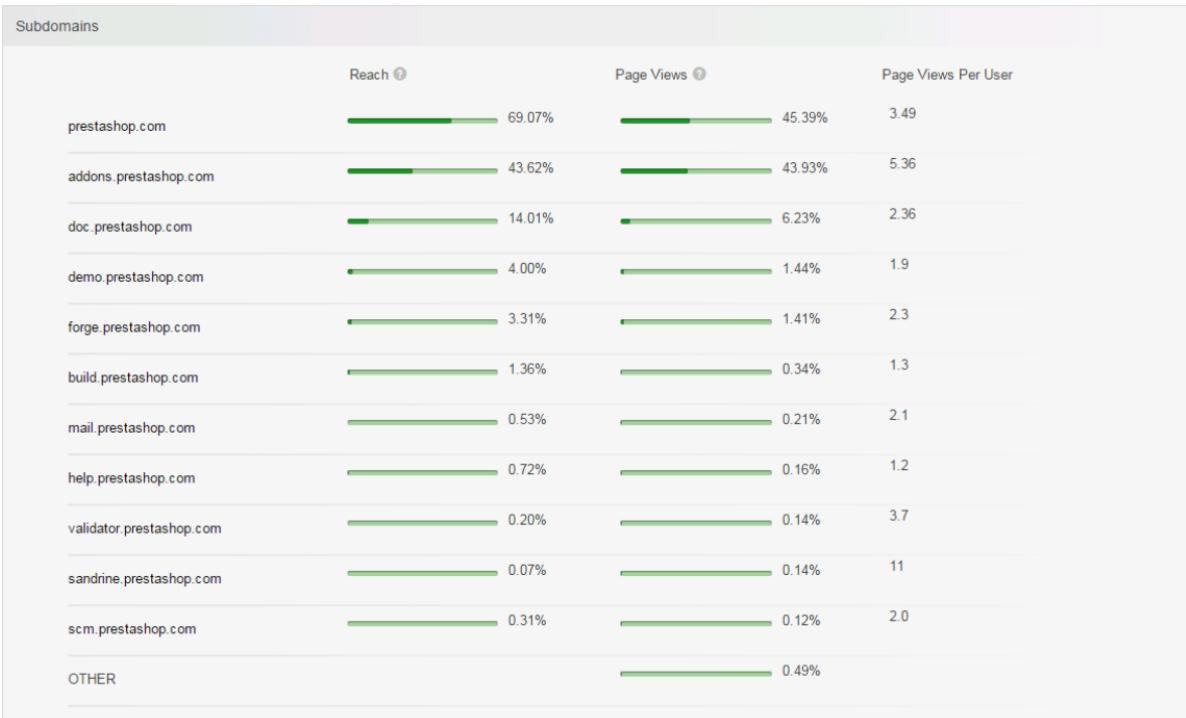
Contact Information

Owner Name	PrestaShop SA
Email	contact@prestashop.com
Address	6, rue Lacépède PARIS, Île de France 75005 FRANCE

Content Data

Title	PrestaShop
Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com .
Speed: Median Load Time	2608
Speed: Percentile	 21%
Links In Count	61656





Overview for **prestashop.com**: Whois Website Info **History** DNS Records Diagnostics ⌚ Updated 11 hours ago ⌚

Want this archived information removed?

Old Registrar Info January 28, 2008

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Registrar Info September 03, 2015

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Overview for **prestashop.com**:

Whois Website Info History **DNS Records** Diagnostics

⌚ Updated 11 hours ago ⌚

Name Servers – prestashop.com

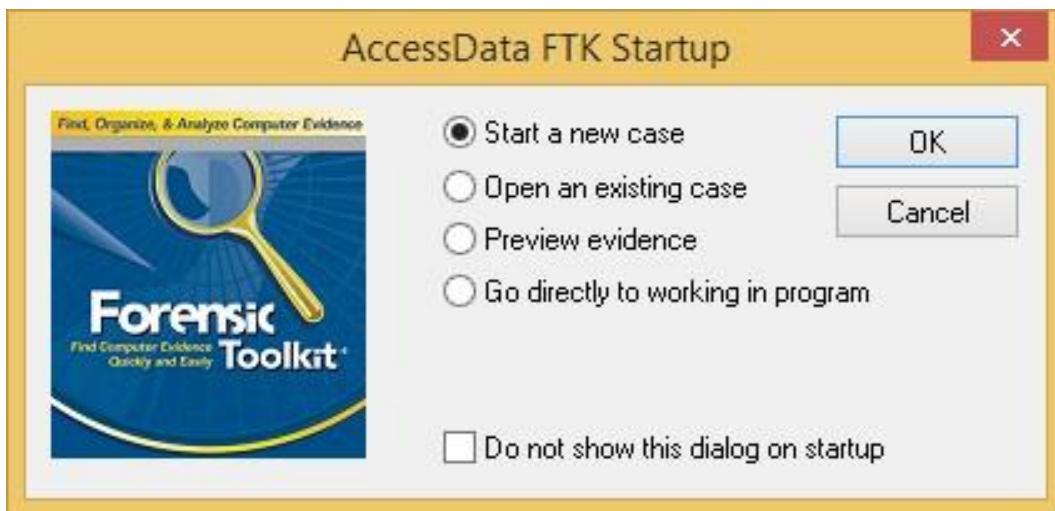
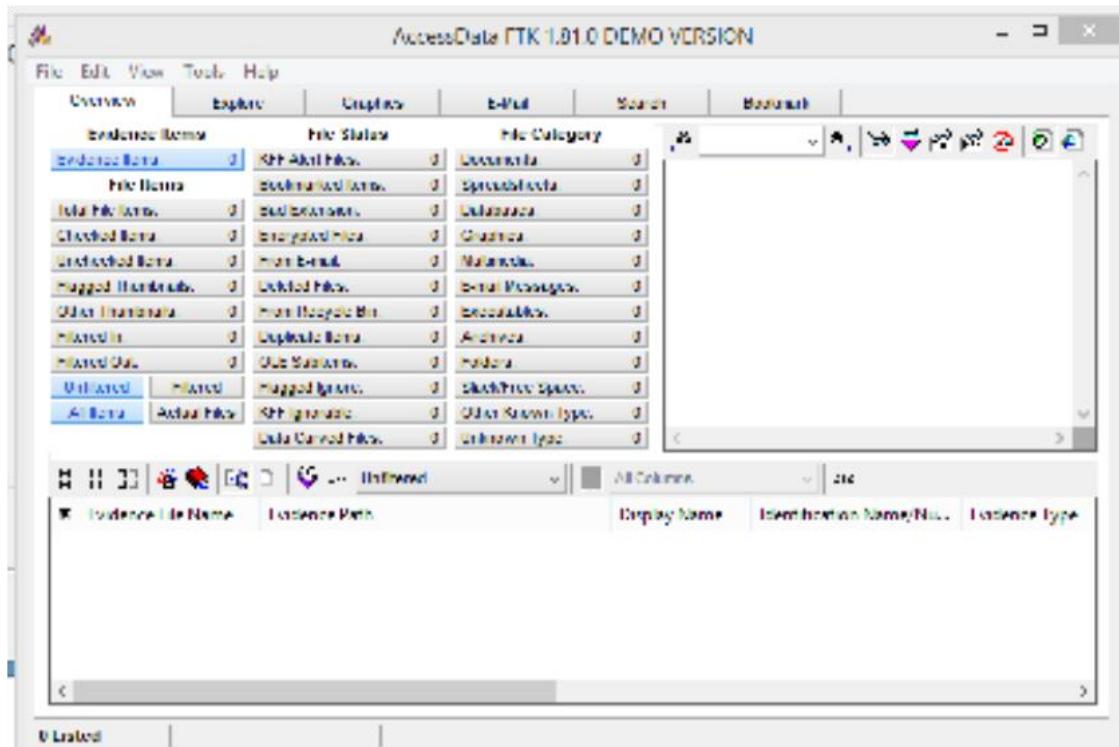
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	Villefranche-sur-Mer, A8, FR

SOA Record – prestashop.com

Name Server	master.ns.mailclub.fr
Email	domaines@mailclub.fr
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

PRACTICAL NO 03: Capture the physical memory of a computer and analyse artifacts in memory.

USING FTK



New Case X

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

Wizard for Creating a New Case

Investigator Name:

Case Information

Case Number:
Case Name:
Case Path:
Case Folder:

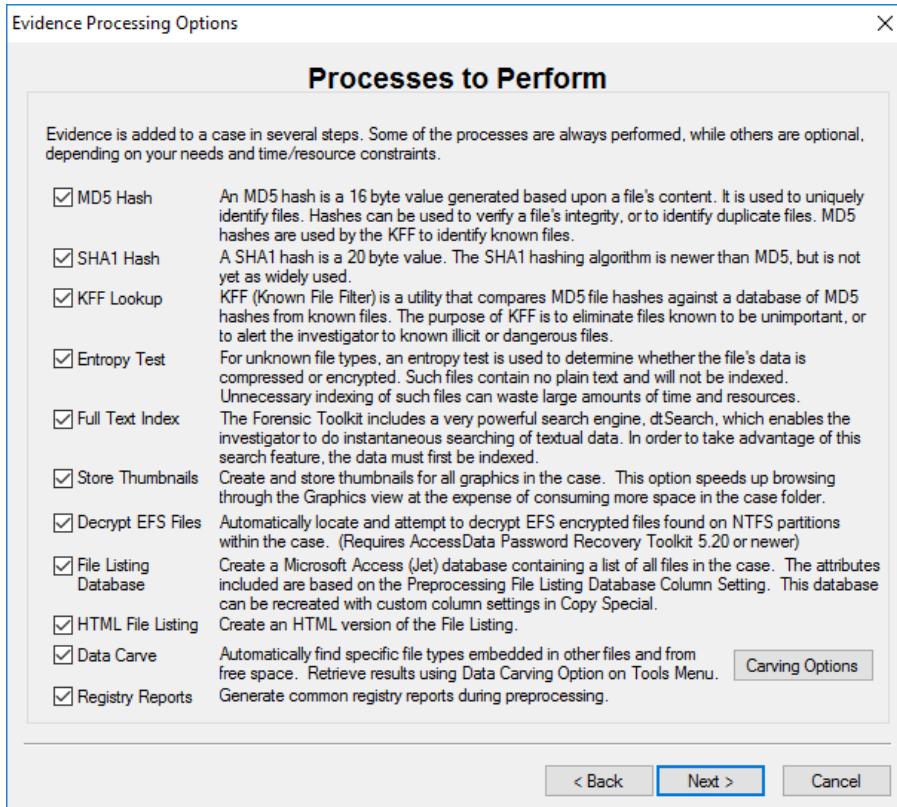
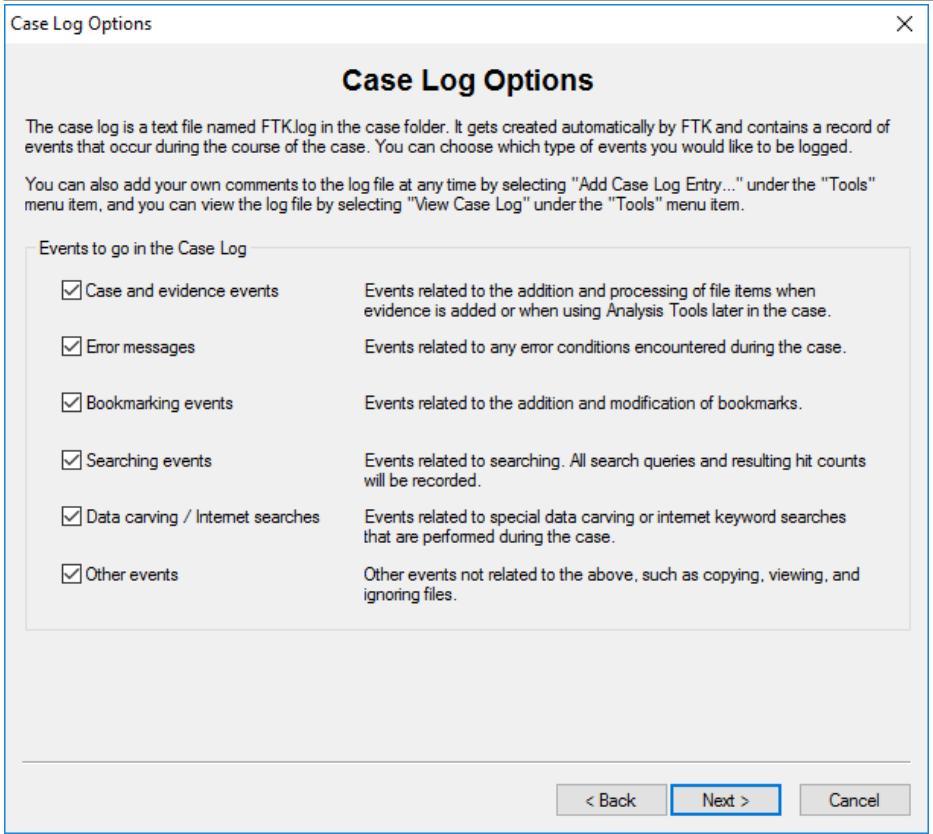
Case Description:

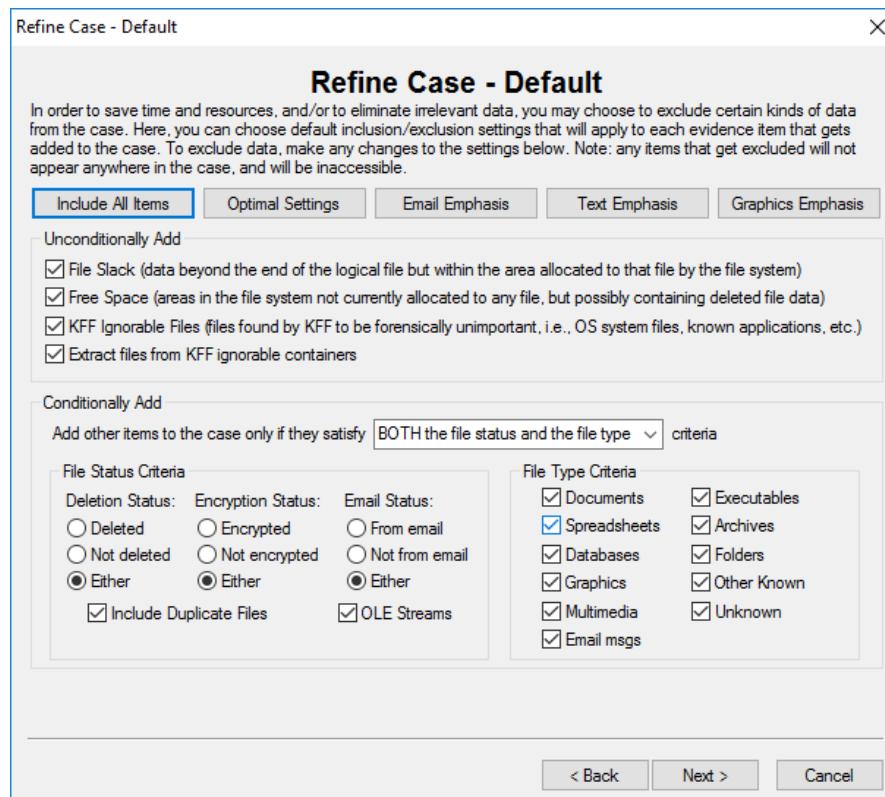
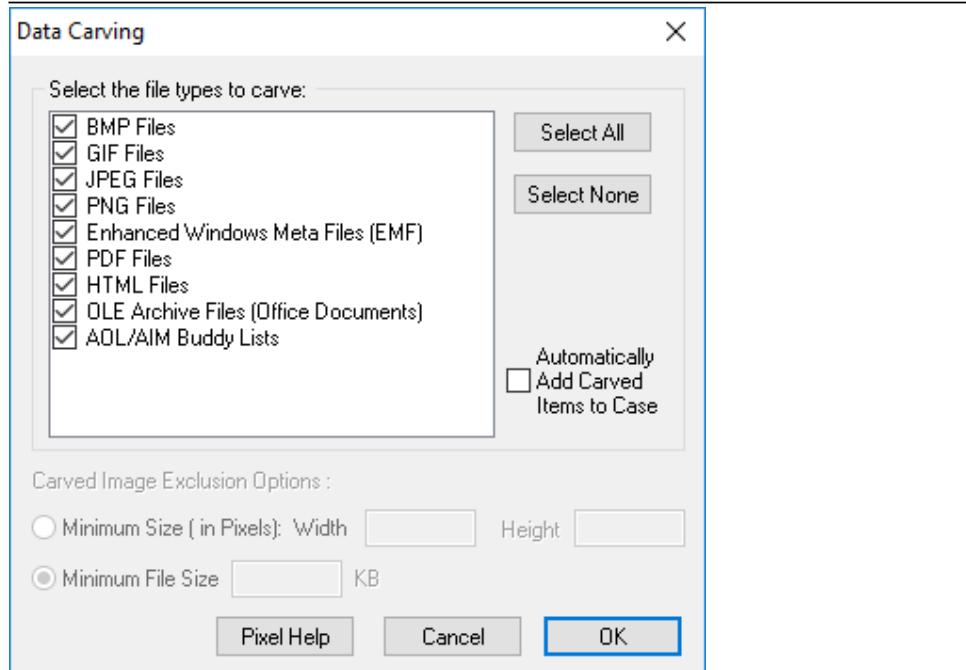
FTK Report Wizard - Case Information X

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:





Refine Index - Default

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

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

[< Back](#) [Next >](#) [Cancel](#)

Add Evidence to Case

Add Evidence

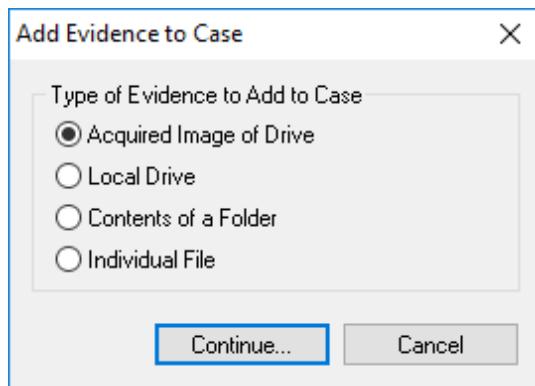
Any number of evidence items can be added to the case. There are several types of evidence items:

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

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

Add Evidence...	Edit Evidence...	Remove Evidence	Refine Evidence - Advanced...			
Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment

[< Back](#) [Next >](#) [Cancel](#)



The dialog box is titled "Evidence Information". It contains fields for "Evidence Location" (F:\sem4\ComputerForensics\sample1.img), "Evidence Display Name" (sample1), "Evidence Identification Name/Number" (XYZ), and a "Comment" text area. Below these is a "Local Evidence Time Zone" dropdown set to "Asia/Calcutta". At the bottom are "OK" and "Cancel" buttons.

Evidence Location:	F:\sem4\ComputerForensics\sample1.img	
Evidence Display Name:	sample1	
Evidence Identification Name/Number:	XYZ	
Comment:	 	
Local Evidence Time Zone:	Asia/Calcutta	

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
sample1\KEEPPRYVAT-F...	F:\sem4\Com...	XYZ	FAT12	N	Asia/Calc...	

< Back Next > Cancel

Case Summary

New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:
c:\Testprac2

Number of Evidence Items: 1

Processes to be Performed:

File Extraction:	Yes	Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
File Identification:	Yes	
MD5 Hash:	Yes	
SHA1 Hash:	Yes	
KFF Lookup:	Yes	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.
Entropy Test:	Yes	
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

< Back Finish Cancel

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	19	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	19	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	19	Duplicate Items:	2	Archives:	4
Filtered Out:	0	OLE Subitems:	10	Folders:	1
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	5
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	1
		Data Carved Files:	0	Unknown Type:	6

File Explorer View Options Filter Off Unfiltered All Columns D12

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
sample1.img	F:\sem4\ComputerForensics	sample1\KEEPPRY...	XYZ	FAT12

1 Listed 0 Checked Total F:\sem4\ComputerForensics\sample1.img

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	19	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	19	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	19	Duplicate Items:	2	Archives:	4
Filtered Out:	0	OLE Subitems:	10	Folders:	1
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	5
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	1
		Data Carved Files:	0	Unknown Type:	6

File Explorer View Options Filter Off Unfiltered All Columns D12

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children
1>DataSpaces	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	3,584	13,312	
1\Primay	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Stream	Unknown	N/A	N/A	N/A	N/A	208	13,312	
1\dodolist.txt	sample1\KEEPPRY\AT-FAT12\dodolist.txt		txt	Plain Text D...	Document		10/7/2007 7:11:28 PM	10/6/2007 10:08:12 ...	10/7/2007 12:00:00 ...	137	512	
1\Root Folder	sample1\KEEPPRY\AT-FAT12			Root Folder	Folder	N/A	N/A	N/A	N/A	7,168	7,168	
1\DataspaceInfo	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	2,560	13,312	
1\DataspaceMap	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Stream	Unknown	N/A	N/A	N/A	N/A	1,311,232	26,214,400	
1\DriveFreeSpace1	sample1\KEEPPRY\AT-FAT12\DriveFreeSpace1			Drive Free S...	Slack/Free S...	N/A	N/A	N/A	N/A	112	13,312	
1\EncryptedPackage	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>Encry...		xlsx	OLE Stream	Unknown	N/A	N/A	N/A	N/A	9,016	13,312	
1\EncryptionInfo	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>Encry...		xlsx	OLE Stream	Unknown	N/A	N/A	N/A	N/A	248	13,312	
1\FAT1	sample1\KEEPPRY\AT-FAT12\FAT1			File Allocatio...	Slack/Free S...	N/A	N/A	N/A	N/A	4,608	4,608	
1\FAT2	sample1\KEEPPRY\AT-FAT12\FAT2			File Allocatio...	Slack/Free S...	N/A	N/A	N/A	N/A	64	13,312	
1\FileSlack	sample1\KEEPPRY\AT-FAT12\dodolist.txt>File...			File Slack	Slack/Free S...	N/A	N/A	N/A	N/A	375	512	
1\StrongEncryptionDataSpace	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Stream	Unknown	N/A	N/A	N/A	N/A	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	
1\StrongEncryptionTransform	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	2,560	13,312	
1\obj.cfg	sample1\KEEPPRY\AT-FAT12\obj.cfg		cfg	JPEG/JIFF File	Graphic		10/7/2007 7:11:12 PM	9/26/2005 12:15:32 ...	10/7/2007 12:00:00 ...	132,706	133,120	
1\TransformInfo	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	2,560	13,312	
1\VBR	sample1\KEEPPRY\AT-FAT12\VBR			Volume Boot ...	Slack/Free S...	N/A	N/A	N/A	N/A	512	512	
1\Version	sample1\KEEPPRY\AT-FAT12\vincs.xlsx>1Data...		xlsx	OLE Stream	Unknown	N/A	N/A	N/A	N/A	76	13,312	
1\vincs.xlsx	sample1\KEEPPRY\AT-FAT12\vincs.xlsx		xlsx	Encrypted U...	Other		10/7/2007 7:11:02 PM	10/7/2007 10:55:34 ...	10/7/2007 12:00:00 ...	13,112	13,312	

19 Listed 0 Checked Total 0 Highlighted

Add Evidence X

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

Wizard for Adding Evidence to the Case

Investigator Name: XYZ

Case Information

Number of Evidence Items: 1

Number of File Items: 19

Case Name: testprac2

Case Folder: c:\testprac2\

Case Number: 001

Case Description:
TESTPRAC2

Next > Cancel

Add Evidence to Case X

Type of Evidence to Add to Case

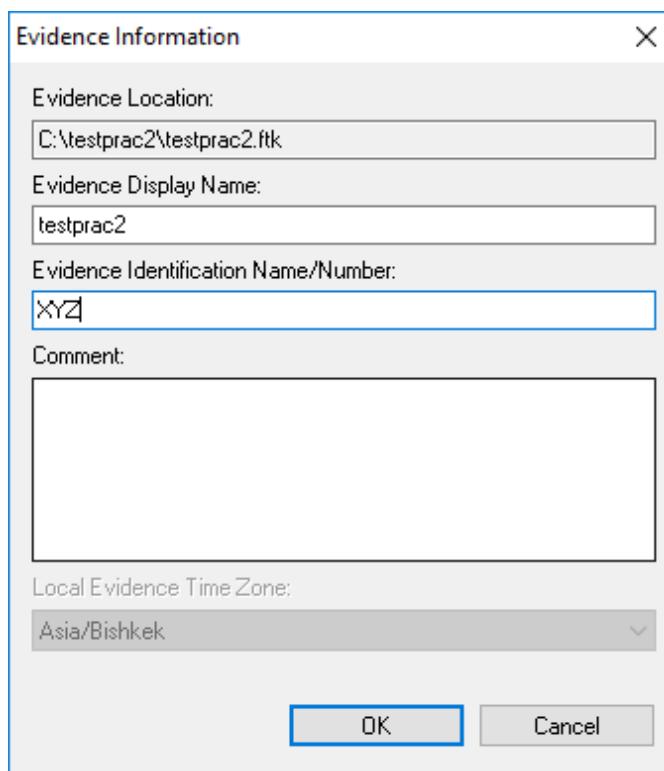
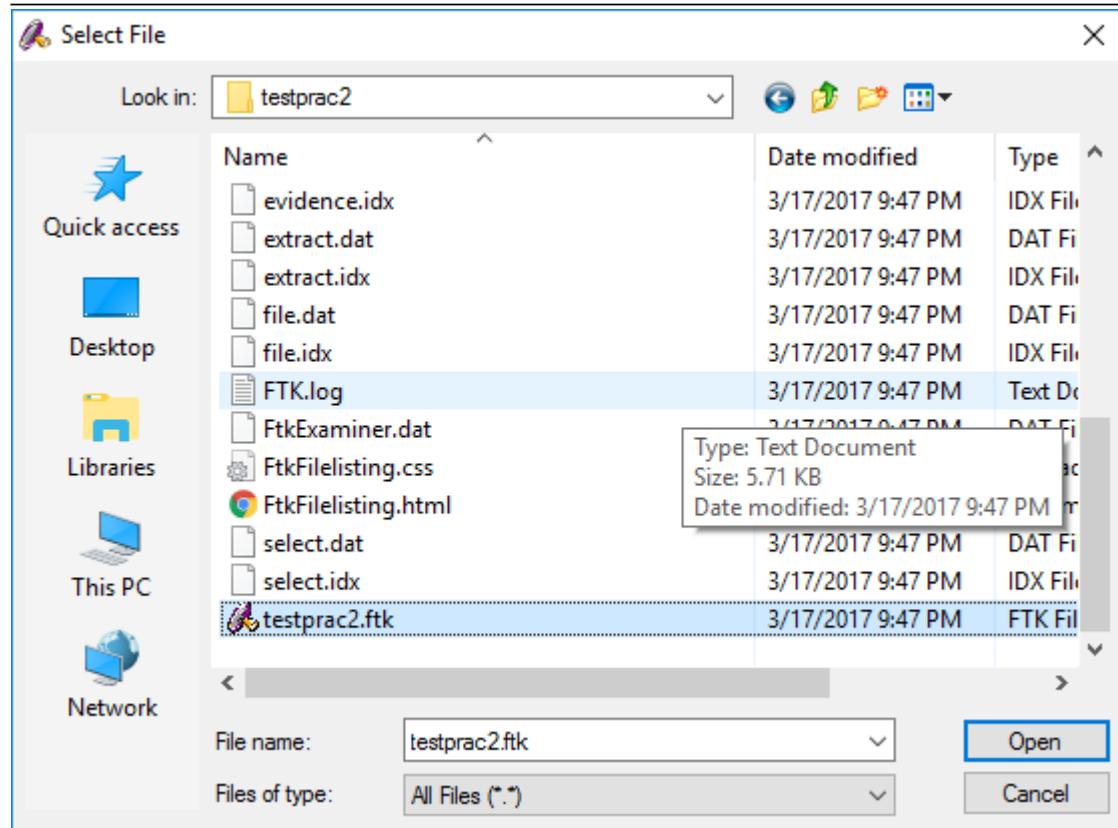
Acquired Image of Drive

Local Drive

Contents of a Folder

Individual File

Continue... Cancel



AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	2	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:		Spreadsheets:	
Total File Items:	20	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	20	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	20	Duplicate Items:	2	Archives:	4
Filtered Out:	0	OLE Subitems:	10	Folders:	1
All Items	Actual Files	Flagged Ignore:	0	Slack/Free Space:	5
		KFF Ignorable:	0	Other Known Type:	1
		Data Carved Files:	0	Unknown Type:	7

Unfiltered Filtered

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
sample1.img	F:\sem4\ComputerForensics	sample1\KEEPP...XYZ		FAT12
testprac2.ftk	C:\testprac2	testprac2	XYZ	Individual file

2 Listed 0 Checked Total C:\testprac2\testprac2.ftk

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

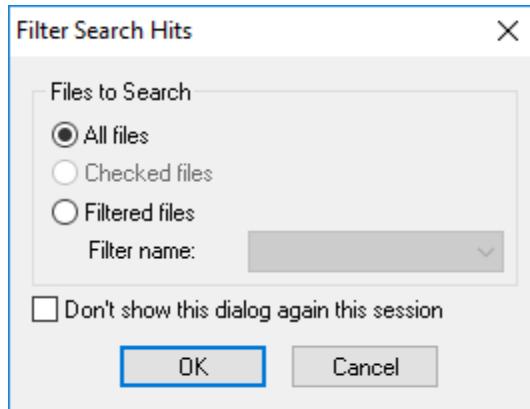
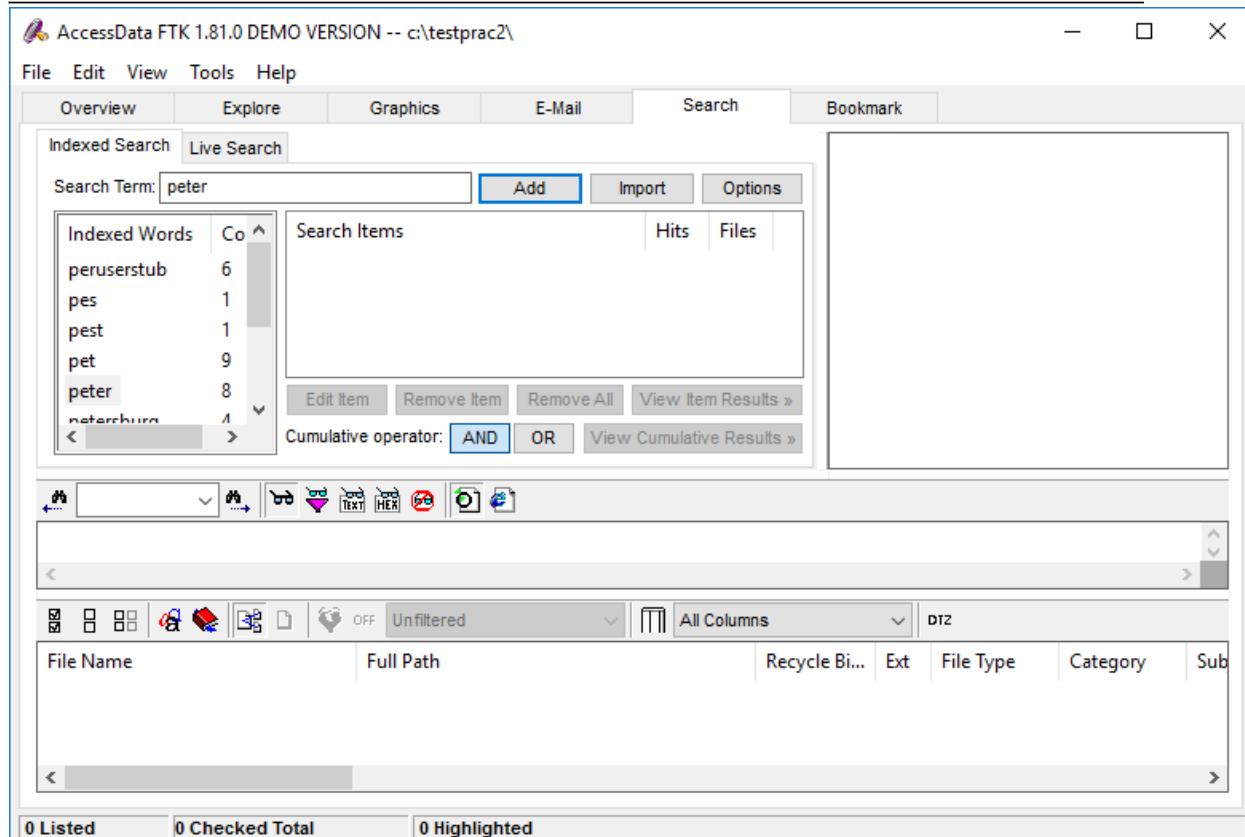
Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	2	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:		Spreadsheets:	
Total File Items:	20	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	20	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	20	Duplicate Items:	2	Archives:	4
Filtered Out:	0	OLE Subitems:	10	Folders:	1
All Items	Actual Files	Flagged Ignore:	0	Slack/Free Space:	5
		KFF Ignorable:	0	Other Known Type:	1
		Data Carved Files:	0	Unknown Type:	7

Unfiltered Filtered

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Sub
todolist.txt	sample1\KEEPPRYVAT-FAT12\todolist.txt		txt	Plain Text D...	Document	

1 Listed 0 Checked Total sample1\KEEPPRYVAT-FAT12\todolist.txt



AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search Live Search

Search Term: [] Add Import Options

Indexed Words	Co...	Search Items	Hits	Files
peter		peter	8	5
sam		sam	235	82
mov		mov	67	12

Edit Item Remove Item Remove All View Item Results »

Cumulative operator: AND OR View Cumulative Results »

File Explorer View Filter OFF Unfiltered All Columns DTZ

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
index_flat[1].htm	precious\Part_1\The Precious-NTFS\Document...		htm	Hypertext Do...	Document
license.txt	precious\Part_1\The Precious-NTFS\Program Fil...		txt	Plain Text D...	Document
lordoftherings[1].htm	precious\Part_1\The Precious-NTFS\Document...		htm	Hypertext Do...	Document

5 Listed 0 Checked Total 0 Highlighted

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search Live Search

Search Term: [] Add Import Options

Indexed Words	Co...	Search Items	Hits	Files
peter		peter	8	5
sam		sam	235	82
mov		mov	67	12

Edit Item Remove Item Remove All View Item Results »

Cumulative operator: AND OR View Cumulative Results »

File Explorer View Filter OFF Unfiltered All Columns DTZ

elijah wood cate blanchett sean astin dominic monaghan billy boyd ian holm hugo weaving liv tyler christopher lee john rhys davies viggo mortensen sean bean orlando bloom miranda otto bernard hill peter jackson frodo baggins bilbo aragorn strider arwen elrond gimli legolas samwise pippin merry gandalf boromir eowyn eomer sauron boromir saruman faramir denethor galadriel gollum hobbit wizard dwarf elf hobbiton bree Weathertop ringwraith dark rider witch king middle earth shire orthanc isengard mordor lathlendar rivendell mt doom rohan gondor fangorn forest treebeard ents shire hole return

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
index_flat[1].htm	precious\Part_1\The Precious-NTFS\Document...		htm	Hypertext Do...	Document
license.txt	precious\Part_1\The Precious-NTFS\Program Fil...		txt	Plain Text D...	Document

5 Listed 0 Checked Total precious\Part_1\The Precious-NTFS\Documents and Settings\Frodo Baggins...index_flat[1].htm

AccessData FTK 1.81.0 DEMO VERSION -- D:\MSCIT PART-II SEM IV\prac files\murder\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Indexed Search Live Search

Search Items: 46 72 6f 6d Type: Hex

Search Options: Text (radio), ASCII (checkbox), Unicode (checkbox), Case Sensitive (checkbox), Regular Expression (checkbox), Hexadecimal (radio). Results: 200 hits.

Search Results:

- Query: "46 72 6f 6d" <Hex> -- 277 Hits in 97 Filtered Files
- 3 Hits -- [getmsg[1].htm] precious\Part_1\The Precious-
- 3 Hits -- [getmsg[1].htm] precious\Part_1\The Precious-
- 2 Hits -- [Deleted Items.dbx] precious\Part_1\The Precios-
- 1 Hit -- [Message0001] precious\Part_1\The Precious-NT
- 1 Hit -- [Message0002] precious\Part_1\The Precious-NT
- 8 Hits -- [Inbox.dbx] precious\Part_1\The Precious-NTFS
- 1 Hit -- [Attachment1] precious\Part_1\The Precious-NT
- 3 Hits -- [Message0001] precious\Part_1\The Precious-N
- 3 Hits -- [Message0002] precious\Part_1\The Precious-N
- 1 Hit -- [Message0003] precious\Part_1\The Precious-N

Hex View:

```
000 46 72 6f 6d 3a 20 22 46-72 6f 64 6f 20 42 61 67 From: "Frodo Bag
010 67 69 6e 73 22 20 3c 46-72 6f 64 6f 62 61 67 67 gins" <Frobodagg
020 69 40 63 6f 6d 63 61 73-74 2e 6e 65 74 3e 0d 0a i@comcast.net>..
```

Selection start = 0, length = 4

Unfiltered All Columns

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
Message0001	precious\Part_1\The Precious-NTFS\Document...			E-mail Messa...	E-mail	"RE: HEL...	N/A
Message0001	precious\Part_1\The Precious-NTFS\Document...			E-mail Messa...	E-mail	"Possible J...	N/A
Message0001	precious\Part_1\The Precious-NTFS\Document...			E-mail Messa...	E-mail	"Re: South...	N/A
Message0001	precious\Part_1\The Precious-NTFS\Document...			E-mail Messa...	E-mail	"Training"	N/A
Message0002	precious\Part_1\The Precious-NTFS\Document...			E-mail Messa...	E-mail	"It's a Real...	N/A
Message0002	precious\Part_1\The Precious-NTFS\Document...			E-mail Messa...	E-mail	"Mr. T...: N/A	

97 Listed 0 Checked Total

Create New Bookmark

Bookmark name:

Bookmark comment:

Apply bookmark to:

All highlighted items (selected) All checked items All currently listed items

File Name	File Path
index_flat[1].htm	precious\Part_1\The Precious-N...

Remember file position/selection

Report options

Include in report Export files

Include parent of email attachments?

OK Cancel

Create New Bookmark

Bookmark name: peter

Bookmark comment:

Apply bookmark to:

All highlighted items (selected)

All checked items

All currently listed items

File Name: index_flat[1].htm

File Path: precious\Part_1\The Precious-N...

Remember file position/selection

Report options

Include in report Export files

Include parent of email attachments?

OK Cancel

FTK Report Wizard - Case Information

Case Information

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

Include Investigator Information in report

Agency/Company: College

Investigator's Name: XYZ

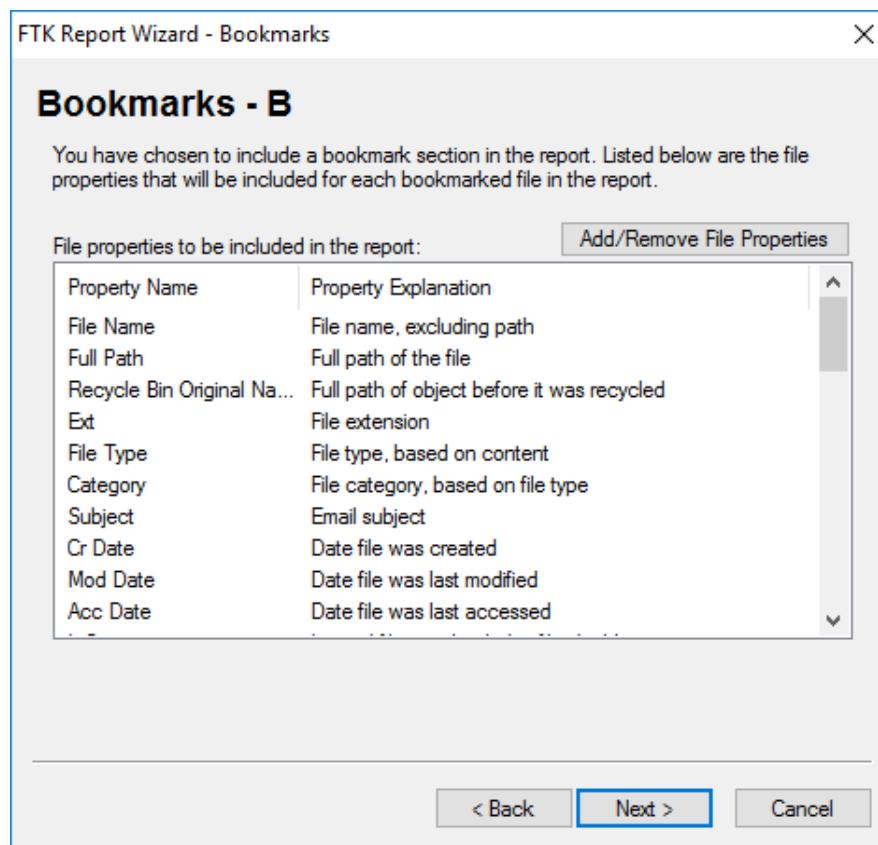
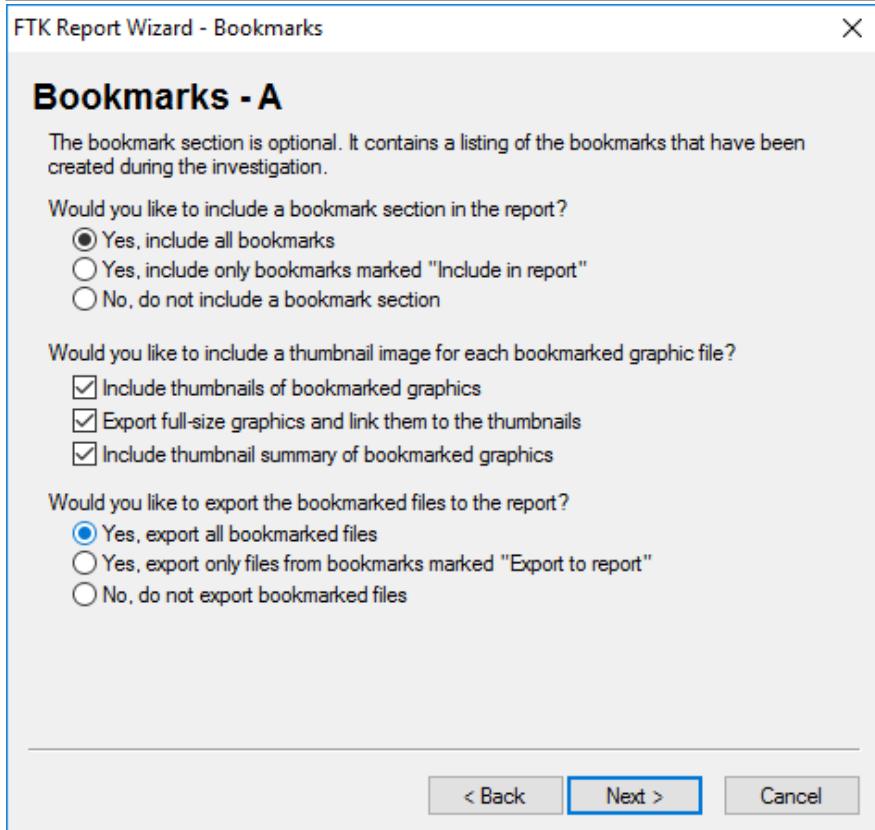
Address: churchgate

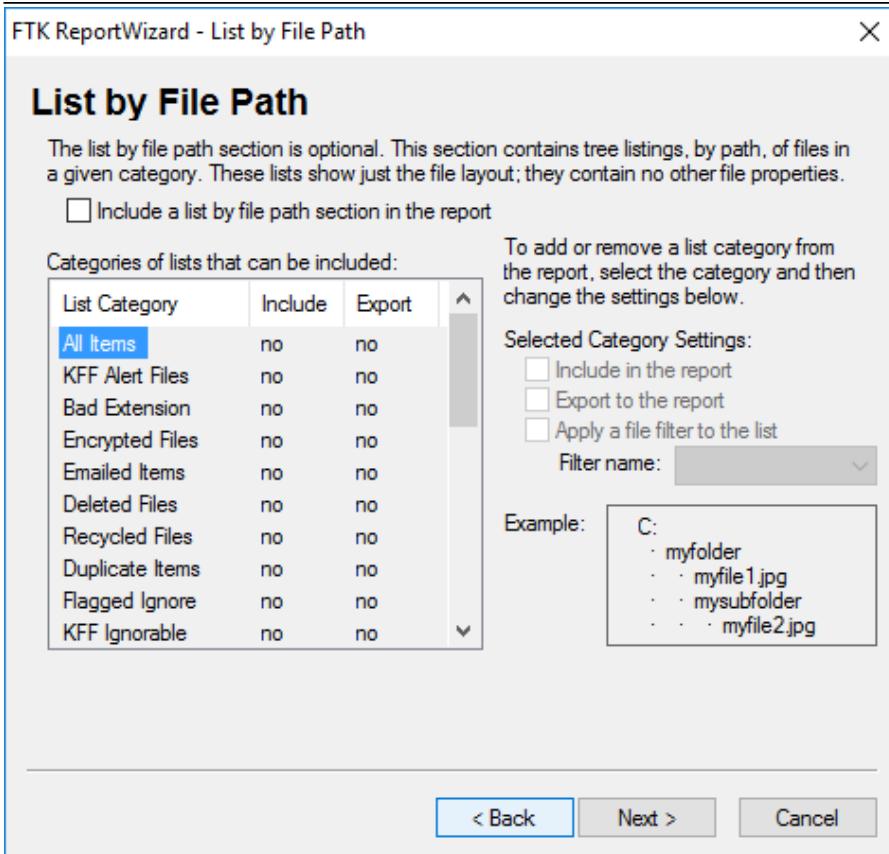
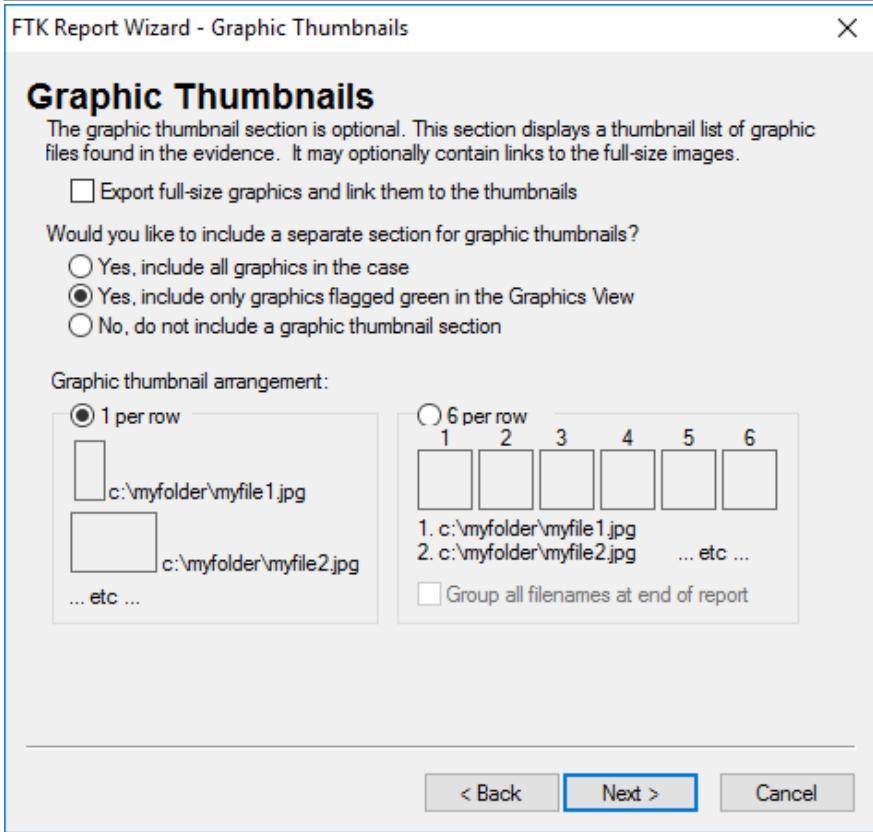
Phone: 1234567890 Fax:

E-Mail: xyz@gmail.com

Comments:

Next > Cancel





FTK Report Wizard - List File Properties

List File Properties - A

The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.

Include a list file properties section in the report
 Include MS Access database in report

Categories of lists to be included in the report:

List Category	Include	Export
All Items	no	no
KFF Alert Files	no	no
Bad Extension	no	no
Encrypted Files	no	no
Emailed Items	no	no
Deleted Files	no	no
Recycled Files	no	no
Duplicate Items	no	no
Flagged Ignore	no	no
KFF Ignorable	no	no

To add or remove a list category from the report, select the category and then change its settings below.

Selected Category Settings:

Include in the report
 Export to the report
 Apply a file filter to the list

Filter name:

Example:
 File: myfile1.jpg
 Path: C:\myfolder
 File Type: JPEG/JFIF File
 Category: Graphic
 L-Size: 37942

< Back Next > Cancel

FTK Report Wizard - Report Location

Report Location

FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.

NOTE 1: If you select an existing folder (other than the default), it must be empty.
 NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
 NOTE 3: If you are expecting to copy this report to recordable media, remember:
 CDR = 650MB, DVDR = 4.5GB

Report folder:

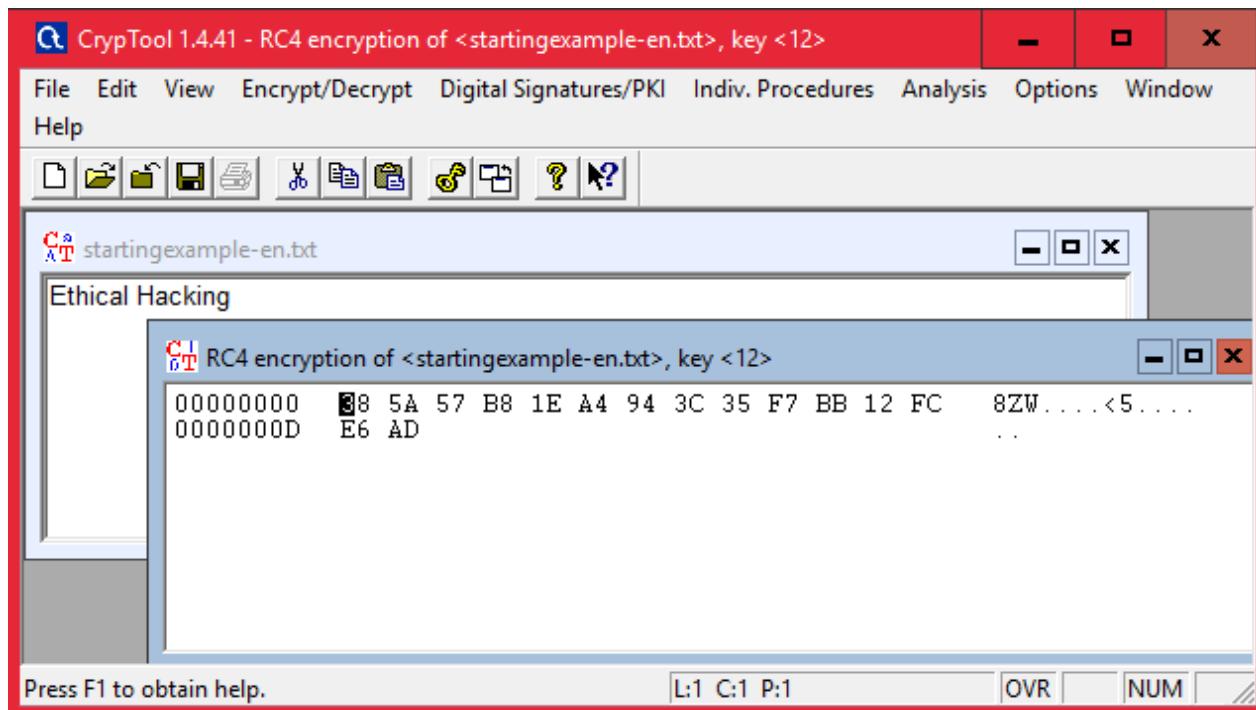
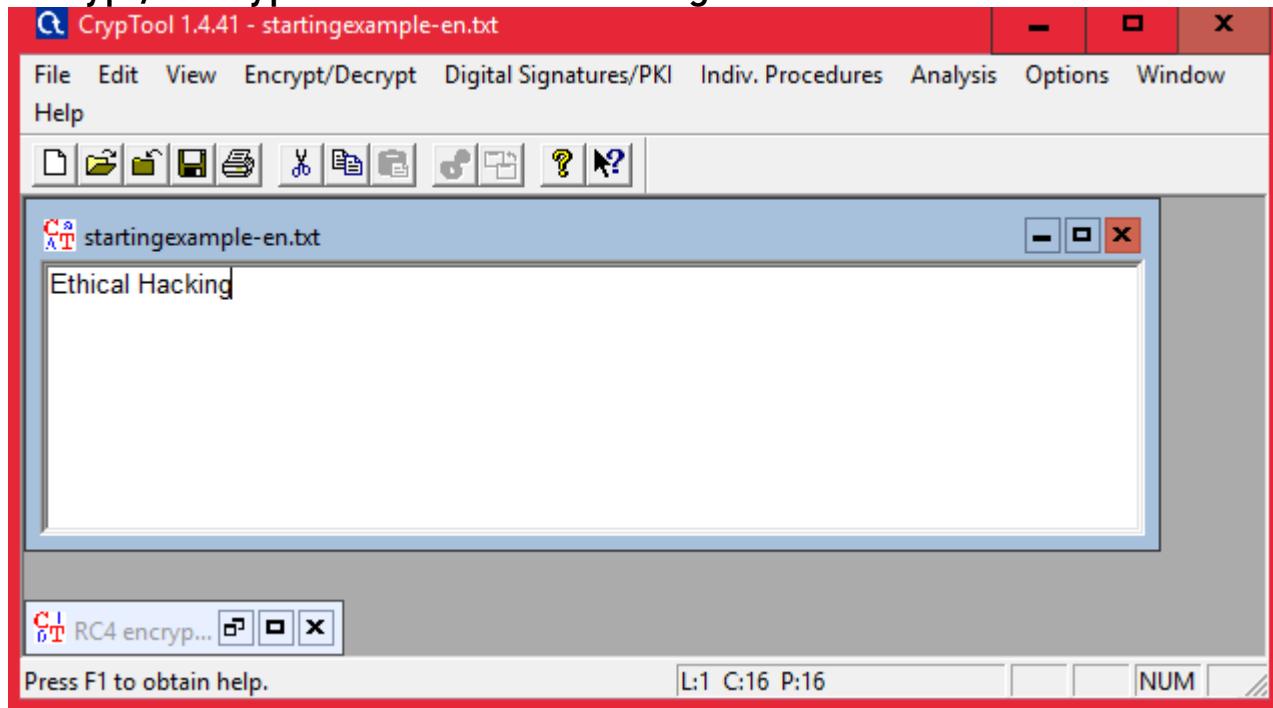
Export all files using actual filenames (may cause broken links on CDs or DVDs)
 Include Registry Viewer reports
 Custom graphic for the report (recommended maximum width is 183 pixels)

Report language:

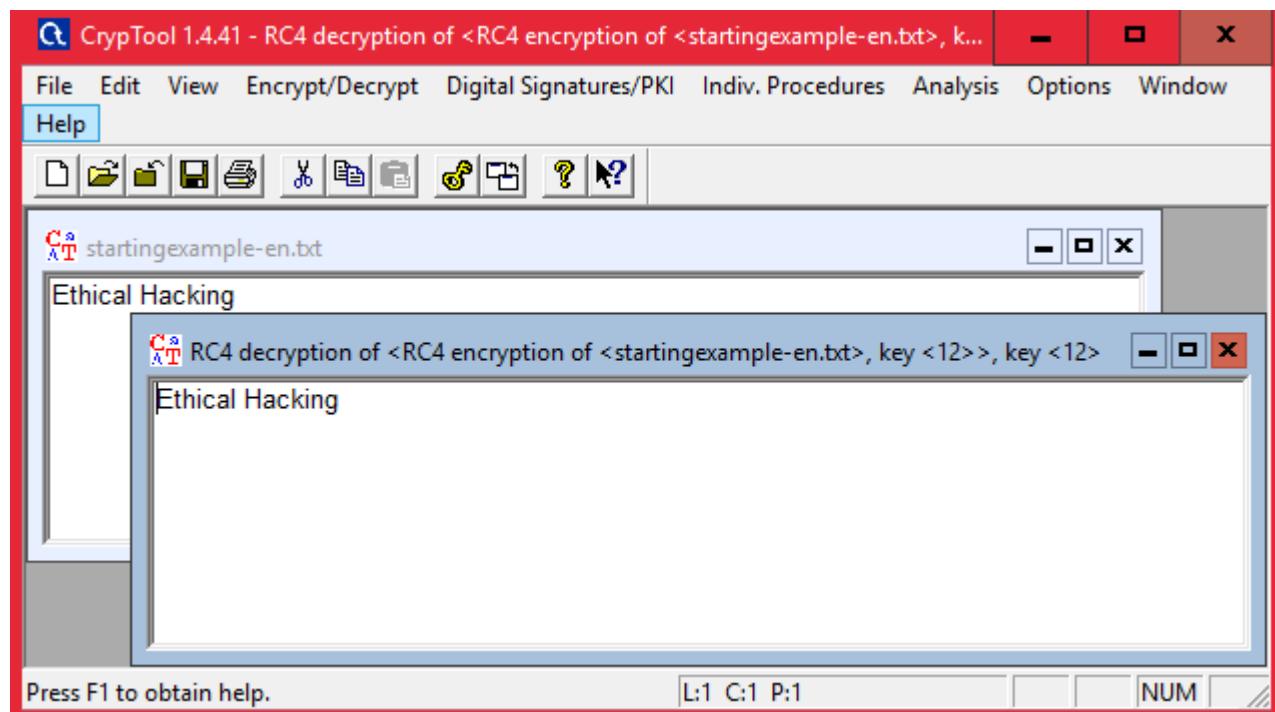
< Back Finish Cancel

PRACTICAL NO 04: Calculate the MD5 and SHA1 hashes

Open tool – choose a file for encryption – Goto
Encrypt/Decrypt Tab & choose the algorithm

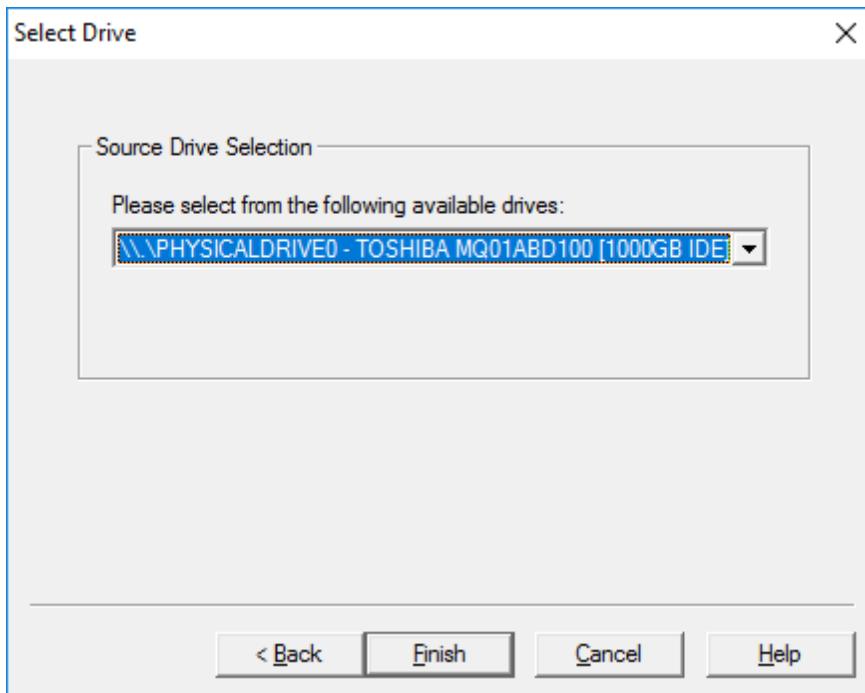
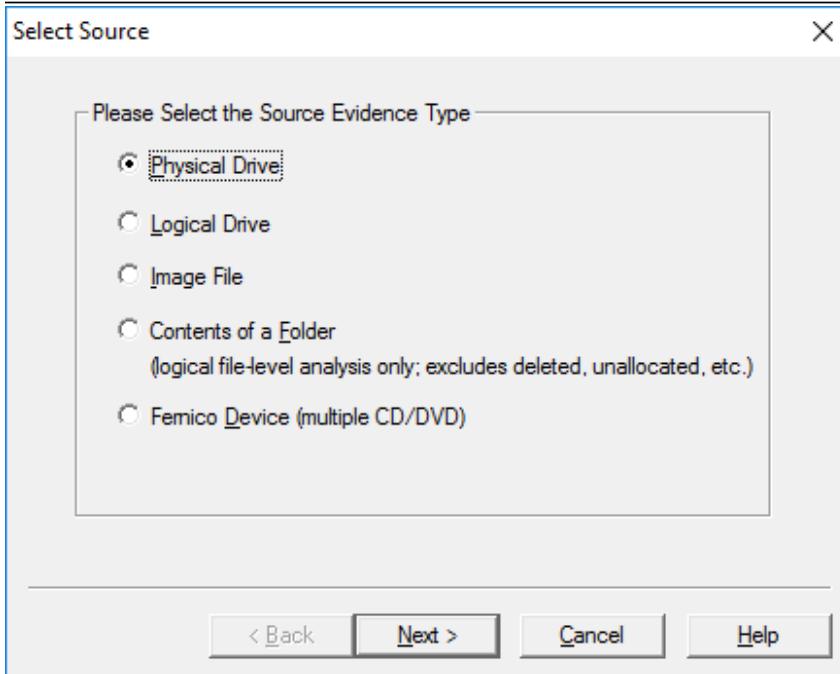


Decryption



PRACTICAL NO 05: Use tools to collect, preserve and reveal digital evidence without compromising systems and data

(Tool used: FTK Imager)



Create Image

Image Source
\\.\PHYSICALDRIVE0

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove Add Overflow Location

Verify images after they are created Precalculate Progress Statistics

Create directory listings of all files in the image after they are created

Start Cancel

Select Image Type

Please Select the Destination Image Type

Raw (dd)
 SMART
 E01
 AFF

< Back Next > Cancel Help

Evidence Item Information X

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

[< Back](#) [Next >](#) [Cancel](#) [Help](#)

Select Image Destination X

Image Destination Folder [Browse](#)

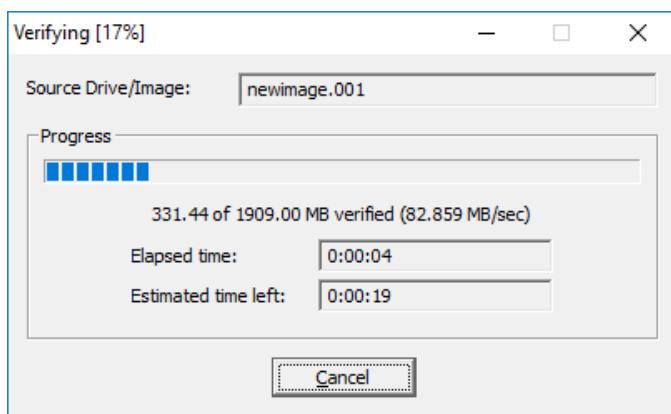
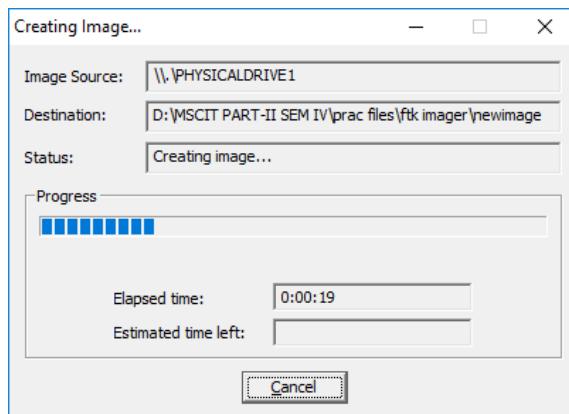
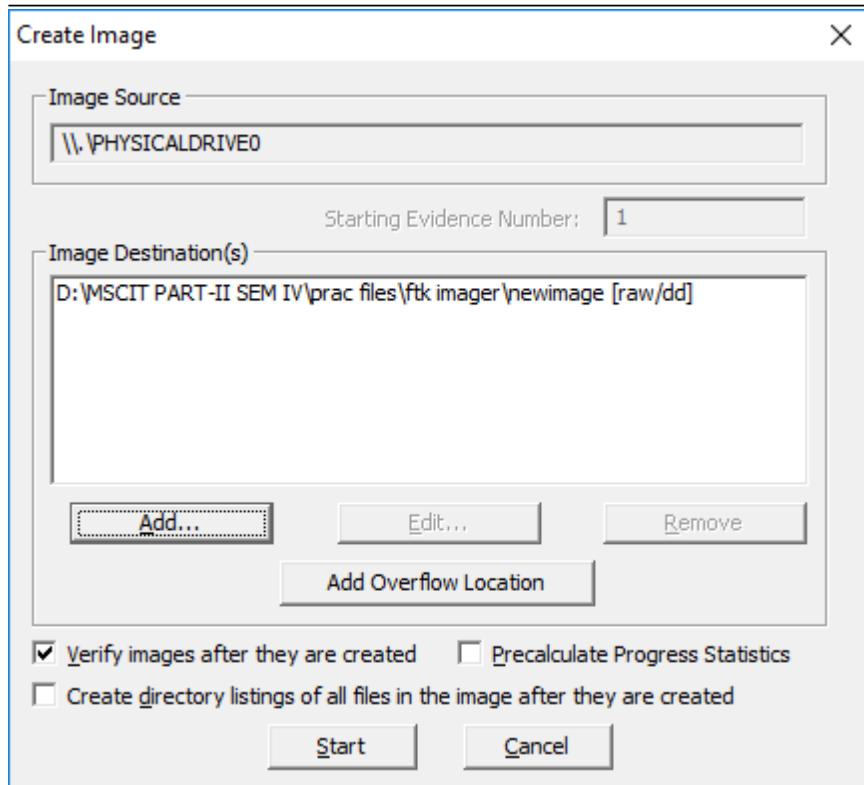
Image Filename (Excluding Extension)

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest)

Use AD Encryption

[< Back](#) [Finish](#) [Cancel](#) [Help](#)



Drive/Image Verify Results

Name	newimage.001
Sector count	3909632
MD5 Hash	
Computed hash	2c30f6973d0ed82e27d7b514291cd8c5
Report Hash	2c30f6973d0ed82e27d7b514291cd8c5
Verify result	Match
SHA1 Hash	
Computed hash	e6076cef8db2b39517c5609da1e4118d2l
Report Hash	e6076cef8db2b39517c5609da1e4118d2l
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Close

Image Summary

Sector Count: 3,909,632
 [Physical Drive Information]
 Drive Model: Kingston DT 101 II USB Device
 Drive Serial Number: 001D0F1E5867E9C077480652
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1909 MB
 Sector count: 3909632
 [Computed Hashes]
 MD5 checksum: 2c30f6973d0ed82e27d7b514291cd8c5
 SHA1 checksum: e6076cef8db2b39517c5609da1e4118d2b36ef01

Image Information:
 Acquisition started: Mon Mar 20 15:24:47 2017
 Acquisition finished: Mon Mar 20 15:26:16 2017
 Segment list:
 D:\MSCIT PART-II SEM IV\prac files\ftk imager\newimage.001
 D:\MSCIT PART-II SEM IV\prac files\ftk imager\newimage.002

Image Verification Results:
 Verification started: Mon Mar 20 15:26:17 2017
 Verification finished: Mon Mar 20 15:26:28 2017
 MD5 checksum: 2c30f6973d0ed82e27d7b514291cd8c5 : verified
 SHA1 checksum: e6076cef8db2b39517c5609da1e4118d2b36ef01 : ver

OK

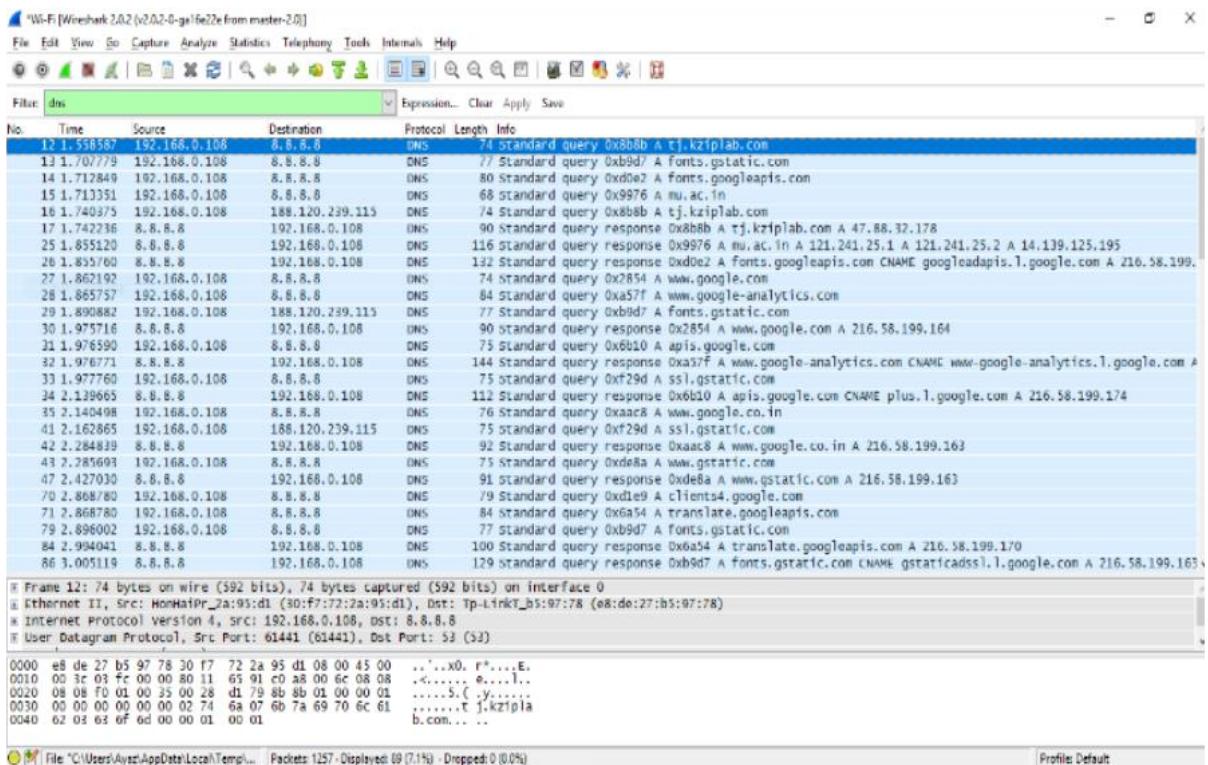
PRACTICAL NO:06

Acquire web pages for forensic investigation. (Wireshark) or Use traffic capturing and analyzing tool. (Wireshark) Using filters and using test login page.

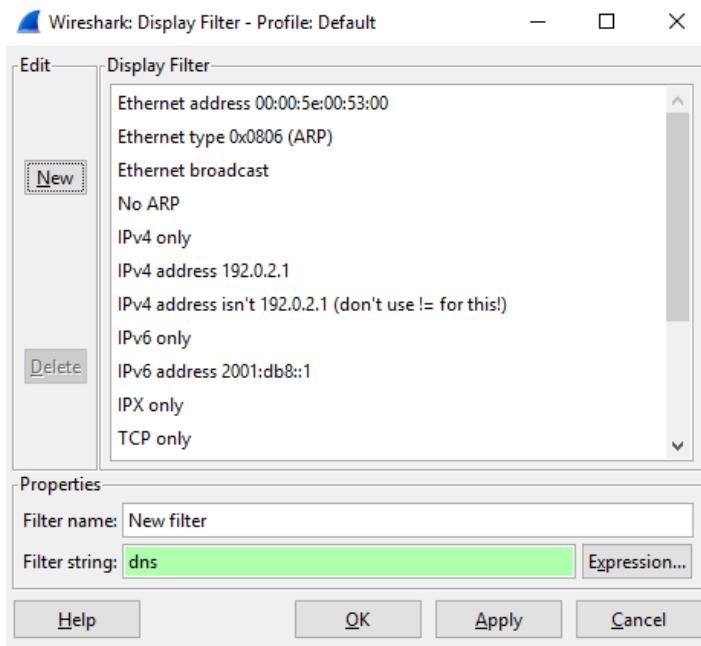
Description: Wireshark is a network packet analyser that intercepts, captures and logs information about packets passing through a network interface. This is useful for analysing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics

Filtering Packets: If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large number of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

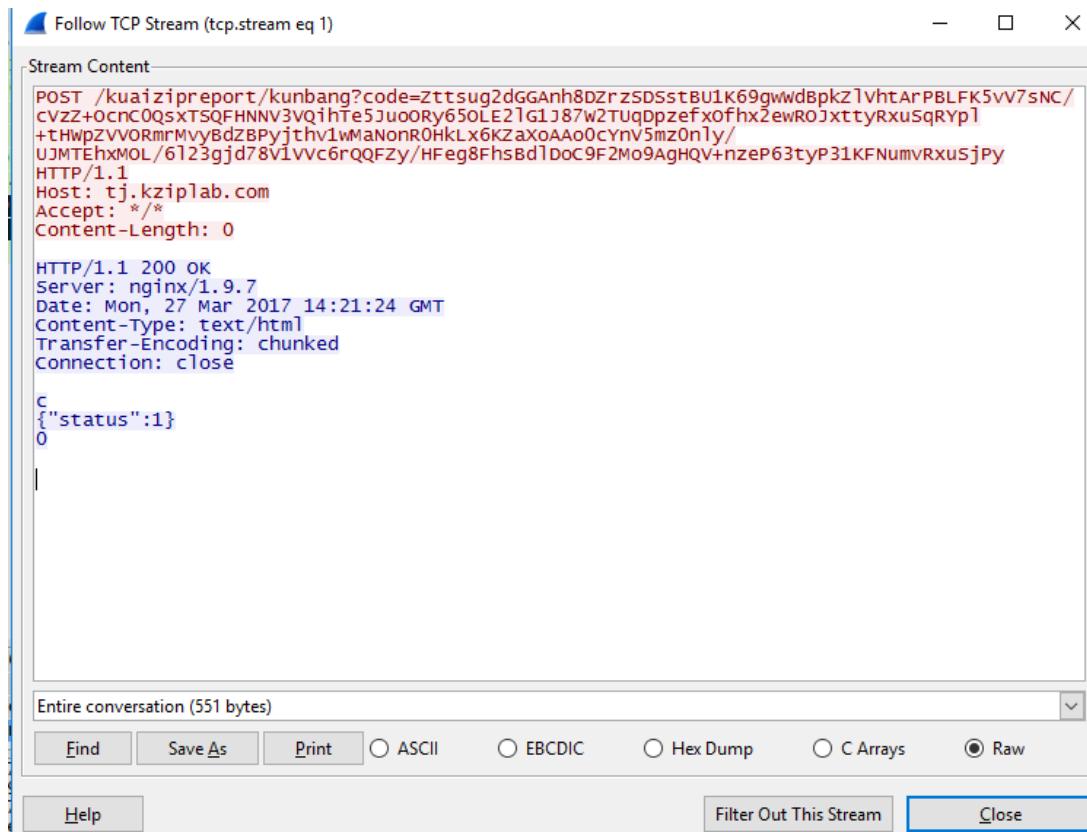


You can also click the Analyse menu and select Display Filters to create a new filter.



Another interesting thing you can do is right-click a packet and select Follow TCP Stream.

You'll see the full conversation between the client and the server.



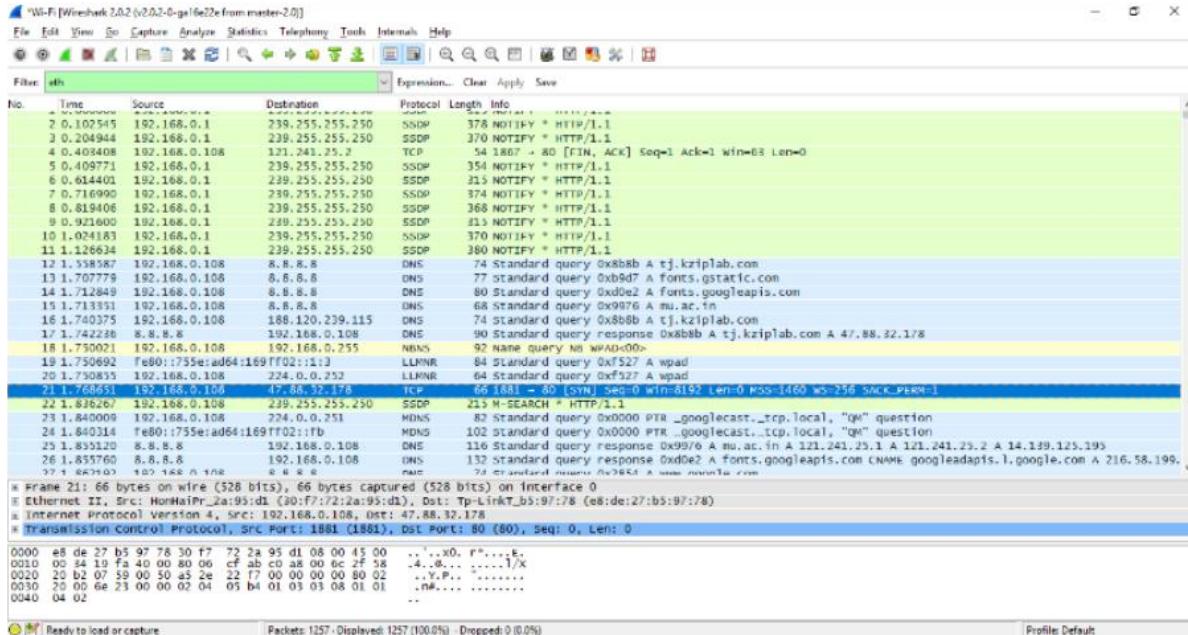
The screenshot shows a window titled "Follow TCP Stream (tcp.stream eq 1)". The main pane displays a conversation between a client and a server. The client's request is a POST to "/kuaizipreport/kunbang?code=...". The server's response is an HTTP/1.1 200 OK with headers: Server: nginx/1.9.7, Date: Mon, 27 Mar 2017 14:21:24 GMT, Content-Type: text/html, Transfer-Encoding: chunked, Connection: close. The response body contains JSON: {"status":1}, 0. The bottom of the window has buttons for Find, Save As, Print, ASCII, EBCDIC, Hex Dump, C Arrays, Raw, Help, Filter Out This Stream, and Close, with "Raw" selected.

```
POST /kuaizipreport/kunbang?code=zttsg2dGGAnh8DzrZSD5stBU1K69gwdbpkz1vhtArPBLFK5vv7sNC/cvZZ+0cnc0QsxtSQFHNNV3VQ1hTe5Ju0oRy65OLE21G1J87w2Tuqdpzefxofhx2ewROjxttyRxusqrYp1+tHwpZVVORMmrBdz8Pyjthv1wMaNonR0HkLx6K2aXoAAo0cYnv5mz0nly/UJMTEhxMOL/6123gjd78v1vvC6rQQFZy/HFeg8FhsBd1Doc9F2Mo9AgHQV+nzeP63tyP31KFNumvRxusjPY
HTTP/1.1
Host: tj.kziplab.com
Accept: */*
Content-Length: 0

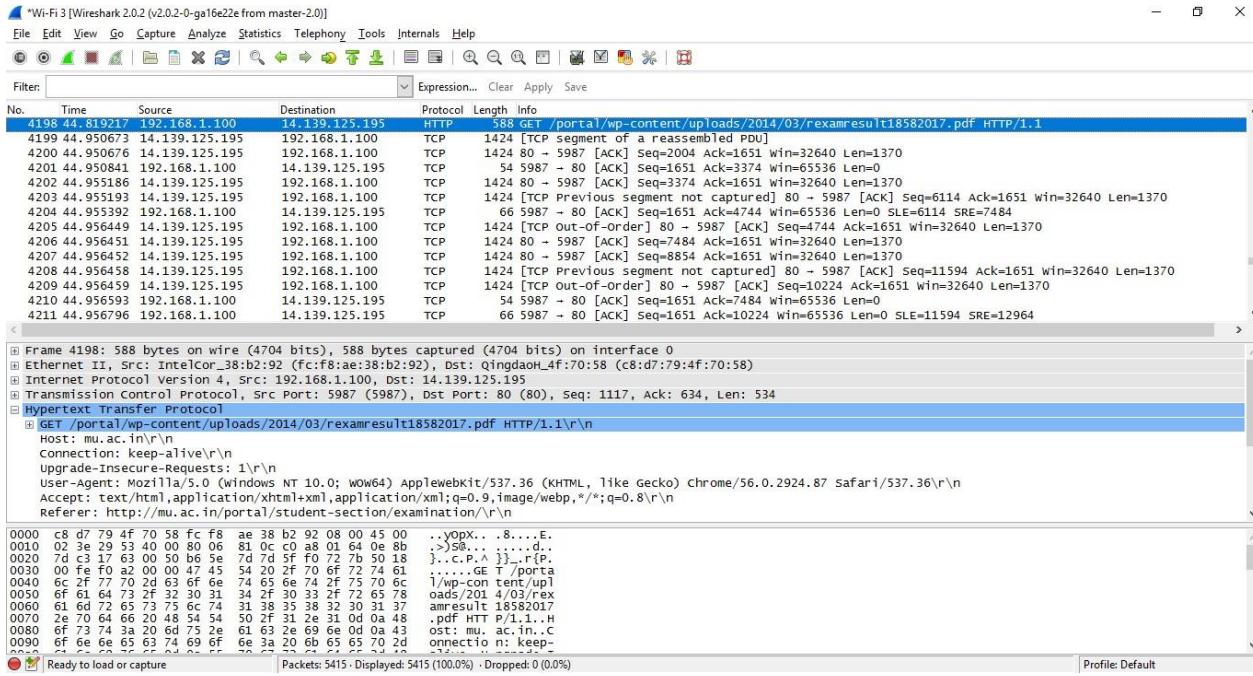
HTTP/1.1 200 OK
Server: nginx/1.9.7
Date: Mon, 27 Mar 2017 14:21:24 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close

{
  "status": 1
}
0
```

Close the window and you'll find a filter has been applied automatically —Wireshark is showing you the packets that make up the conversation.



USING TRAFFIC CAPTURING AND ANALYSIS TOOLS



The screenshot shows a Wireshark capture window titled "Wi-Fi 3 [Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0)]." The filter bar at the top contains the expression "http.request.full_uri contains \"rexamresult18582017.pdf\"". The packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. A single packet is selected, numbered 4198, with details: Time 44.819217, Source 192.168.1.100, Destination 14.139.125.195, Protocol HTTP, Length 588, and Info showing a GET request for "/portal/wp-content/uploads/2014/03/rexamresult18582017.pdf" via HTTP/1.1. The packet details pane below shows the following structure:

- ① Frame 4198: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface 0
- ② Ethernet II, Src: IntelCor_38:b2:92 (fc:f8:ae:38:b2:92), Dst: QingdaoH_4f:70:58 (c8:d7:79:4f:70:58)
- ③ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 14.139.125.195
- ④ Transmission Control Protocol, Src Port: 3987 (3987), Dst Port: 80 (80), Seq: 1117, Ack: 634, Len: 534
- ⑤ Hypertext Transfer Protocol

The hex and ASCII panes show the raw data of the selected packet.

The screenshot shows a Wireshark capture of a single HTTP request. The packet details pane shows a GET request for a PDF file from port 5987 to 80. The bytes pane displays the raw hex and ASCII data of the PDF file.

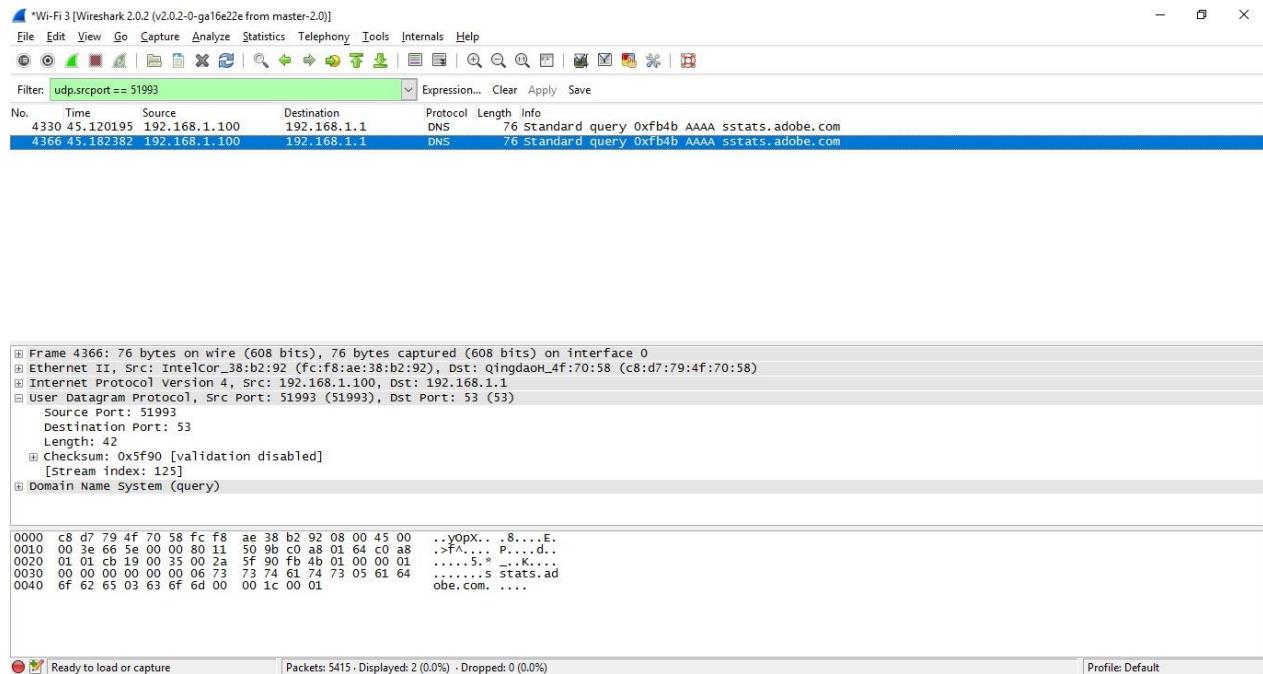
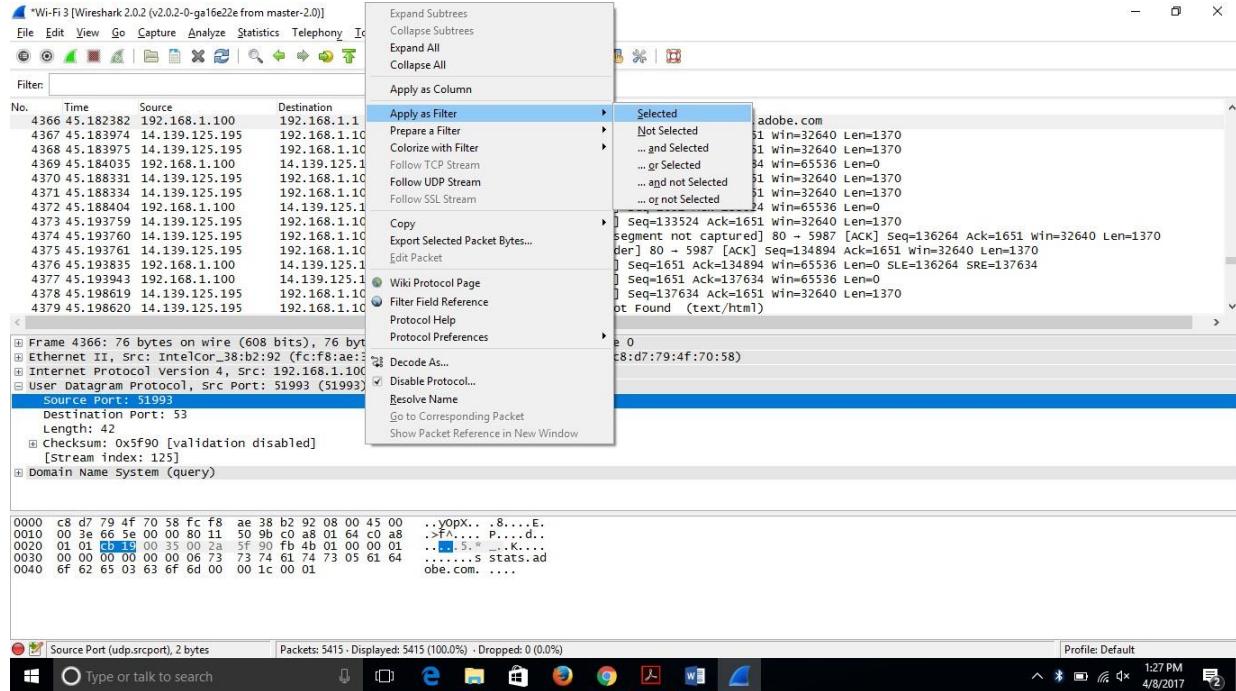
Frame 4198: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface 0

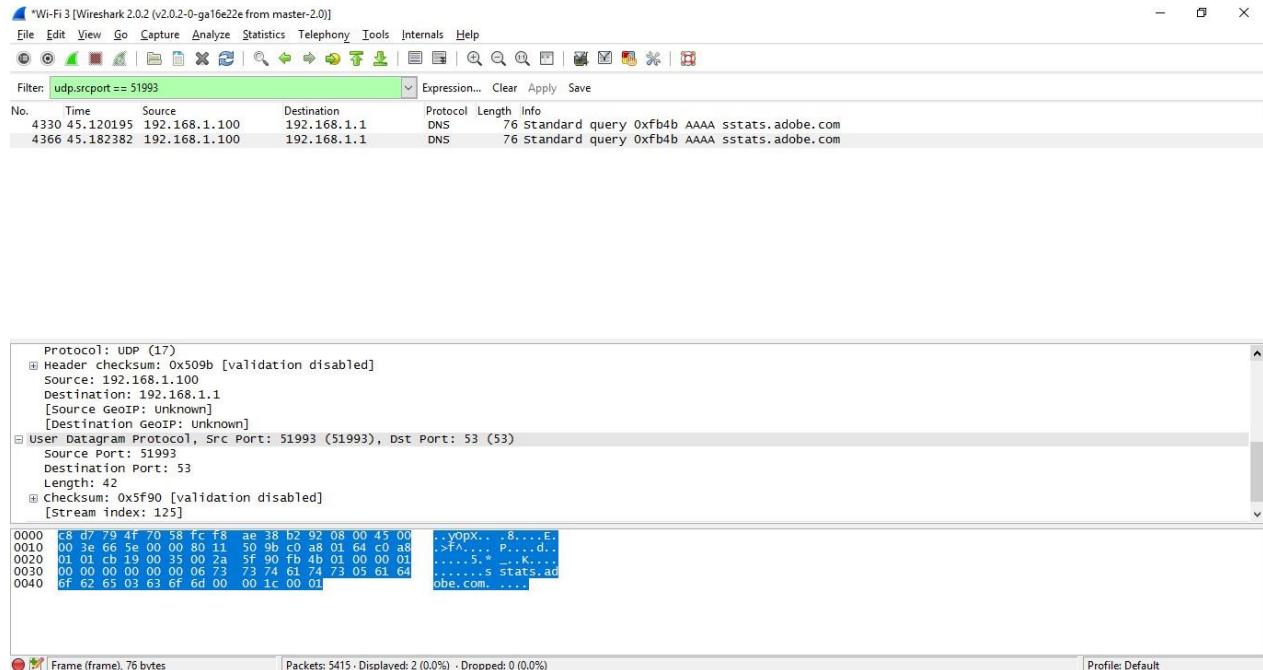
GET /portal/wp-content/uploads/2014/03/rexamresult18582017.pdf HTTP/1.1

Host: mu.ac.in\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nReferer: http://mu.ac.in/portal/student-section/examination/\r\n

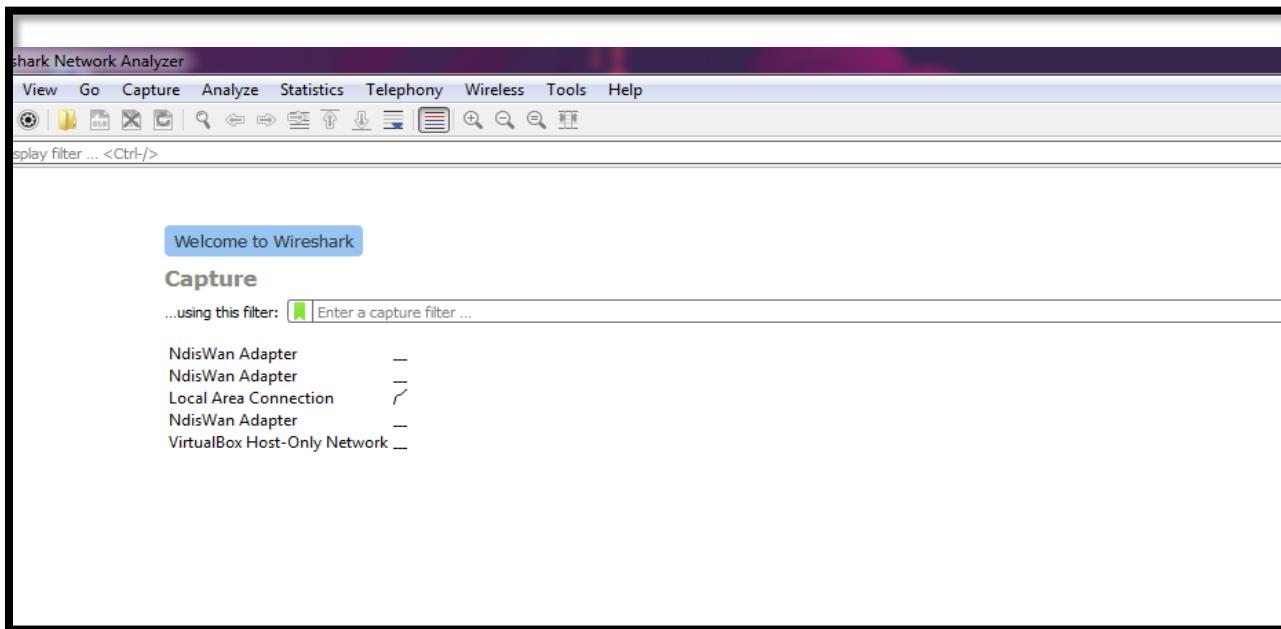
0000 c8 d7 79 4f 70 58 fc f8 ae 38 b2 92 08 00 45 00 .yopx...8...E
0010 02 3e 25 33 40 8c 81 9c c0 a8 01 64 0e 88 00 .>\$.8...d
0020 71 64 73 2f 30 31 34 2f 30 33 2f 72 74 61 60 .GE 1/...port
0030 00 fe f0 32 00 47 45 54 20 2f 70 6f 72 74 61 60 .ads/201 4/03/rex
0040 6c ff 7f 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 1/...wp-content/upl
0050 6f 61 64 73 2f 32 30 31 34 2f 30 33 2f 72 65 78 oads/201 4/03/rex
0060 61 60 73 75 6d 74 31 38 35 38 32 30 31 37 ameresult 18582017
0070 60 70 64 66 20 48 54 54 50 2f 31 26 31 0d 0a 48 .pdf HTTP/1.1. H
0080 6f 70 64 66 20 6d 26 61 63 26 60 0d 0a 48 bst: mu.ac.in;c
0090 61 60 64 65 62 74 69 66 3a 20 6b 65 70 26 nnectio...n:keep-
0098 60 64 65 62 74 69 66 3a 20 6b 65 70 26 nnectio...n:keep-

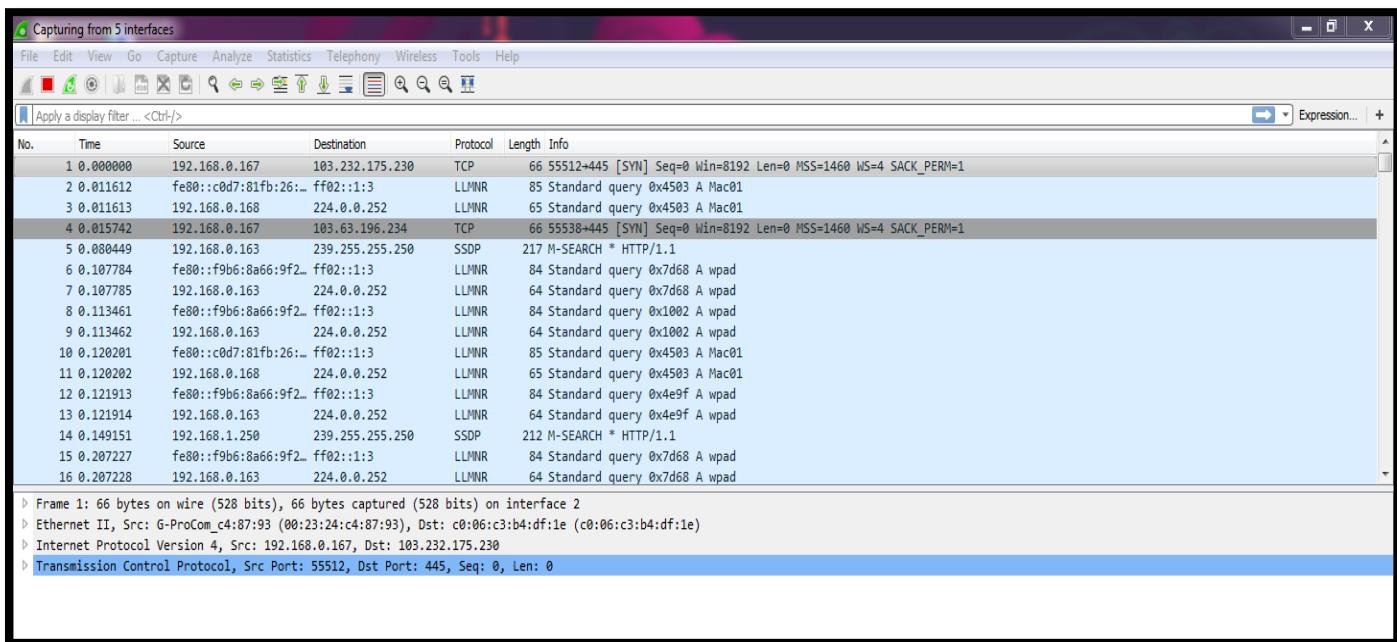
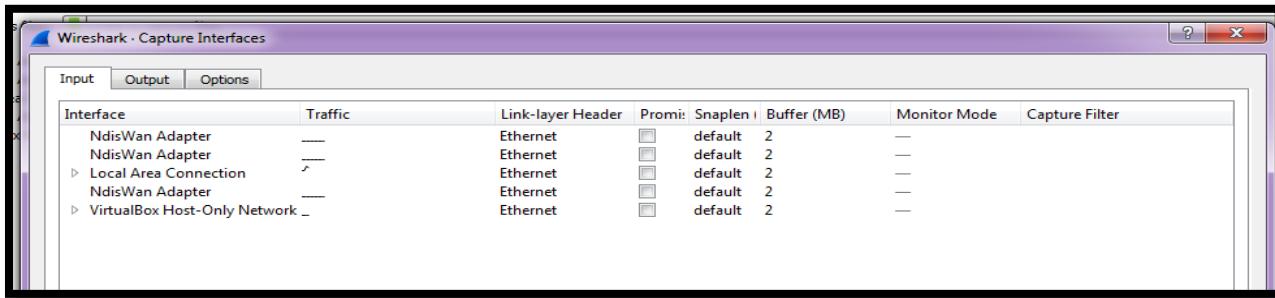
You can also create filters from here —just right- click one of the details and use the **Apply as Filter** submenu to create a filter based on it.





Use of wire shark to scan and check the packet information of following protocols





Acunetix Web Vulnerability Scanner - Test websites
<http://testphp.vulnweb.com> > login

login page - Home of Acunetix Art

If you are already registered please enter your **login** information below: ... Signup disabled.
 Please use the **username test** and the password **test**. search art.

*5 interfaces

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
+ 14062	150.034086	192.168.0.167	44.228.249.3	HTTP	531	GET /login.php HTTP/1.1
+ 14103	150.294040	44.228.249.3	192.168.0.167	HTTP	1342	HTTP/1.1 200 OK (text/html)
+ 15852	169.595431	192.168.0.167	44.228.249.3	HTTP	699	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
+ 15875	169.858386	44.228.249.3	192.168.0.167	HTTP	1513	HTTP/1.1 200 OK (text/html)

Frame 15852: 699 bytes on wire (5592 bits), 699 bytes captured (5592 bits) on interface 2

Ethernet II, Src: G-ProCom_c4:87:93 (00:23:24:c4:87:93), Dst: c0:06:c3:b4:df:1e (c0:06:c3:b4:df:1e)

Internet Protocol Version 4, Src: 192.168.0.167, Dst: 44.228.249.3

Transmission Control Protocol, Src Port: 56871, Dst Port: 80, Seq: 478, Ack: 2749, Len: 645

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

```
0000 c0 06 c3 b4 df 1e 00 23 24 c4 87 93 08 00 45 00 .....# $.....E.
0010 02 ad 72 33 40 00 80 06 9e e0 c0 a8 00 a7 2c e4 ..r3@... .....
0020 f9 03 de 27 00 50 83 b6 b5 78 b0 6d 02 cb 50 18 ...P.. .x.m..P.
0030 40 29 e1 7a 00 00 50 4f 53 54 20 2f 75 73 65 72 @).z..PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1..Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com..Co
0070 6e 6e 65 63 74 69 6f 6e 3a 26 6b 65 65 70 2d 61 nnection : keep-a
0080 6e 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 46 live..Content-Le
0090 6e 67 74 68 3a 20 32 30 0d 0a 43 61 63 68 65 2d ngth: 20 ..Cache-
00a0 43 6f 6e 74 72 6f 6c 3a 26 6d 61 78 2d 61 67 65 Control: max-age
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 =0..Upgr ade-Inse
00c0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f ..Origin : http:/
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 /testphp .vulnweb
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 .com..Content-Ty
0100 76 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 62 pe: appl ication/
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urlen
```

Hypertext Transfer Protocol

Packets: 17555 · Displayed: 4 (0.0%)

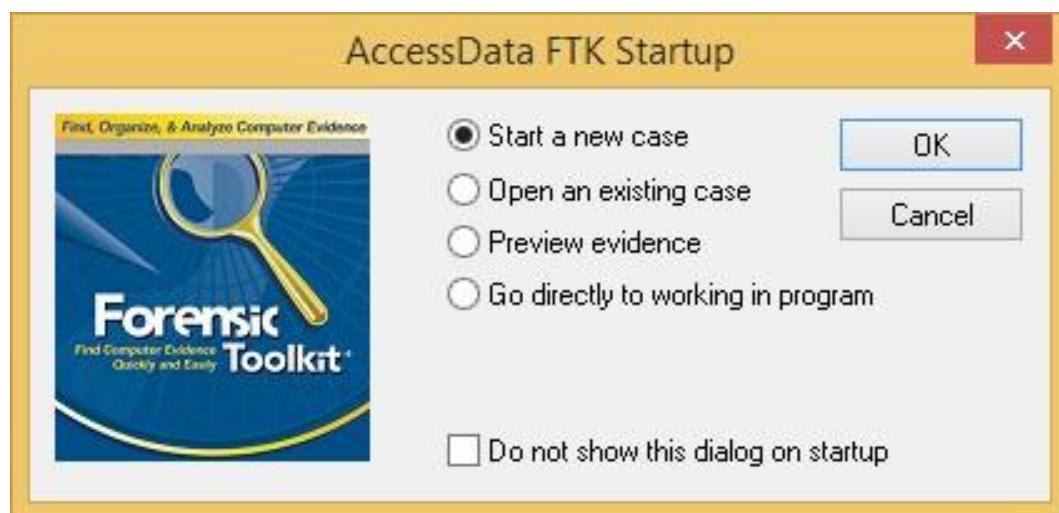
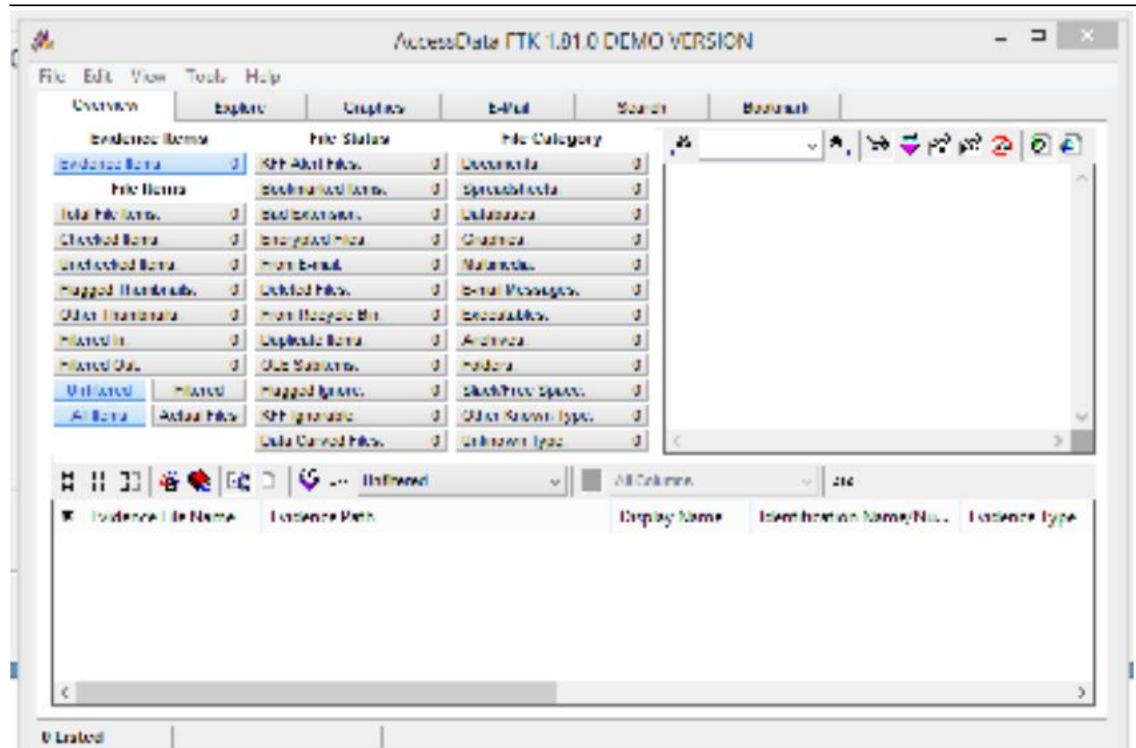
Profile: Default

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- ▷ Form item: "uname" = "test"
- ▷ Form item: "pass" = "test"

PRACTICAL NO 07: Use tools that scan a hard drive, locate deleted media and scan hard drive. (FTK)



New Case X

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

Wizard for Creating a New Case

Investigator Name:

Case Information

Case Number:

Case Name:

Case Path:

Case Folder:

Case Description:

FTK Report Wizard - Case Information X

Forensic Examiner Information

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

Agency/Company:

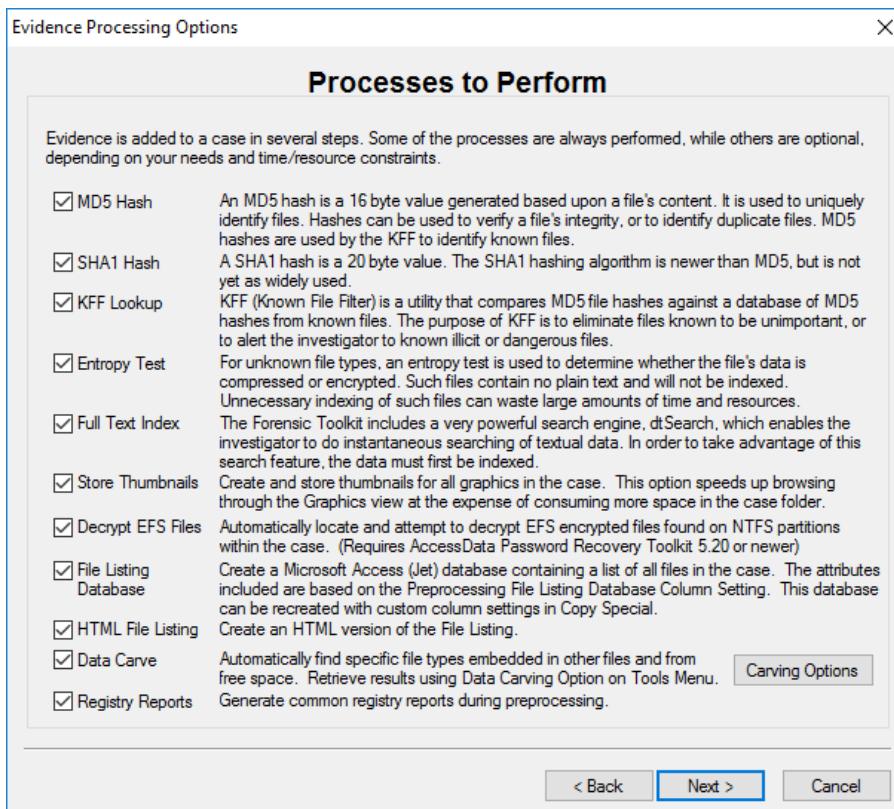
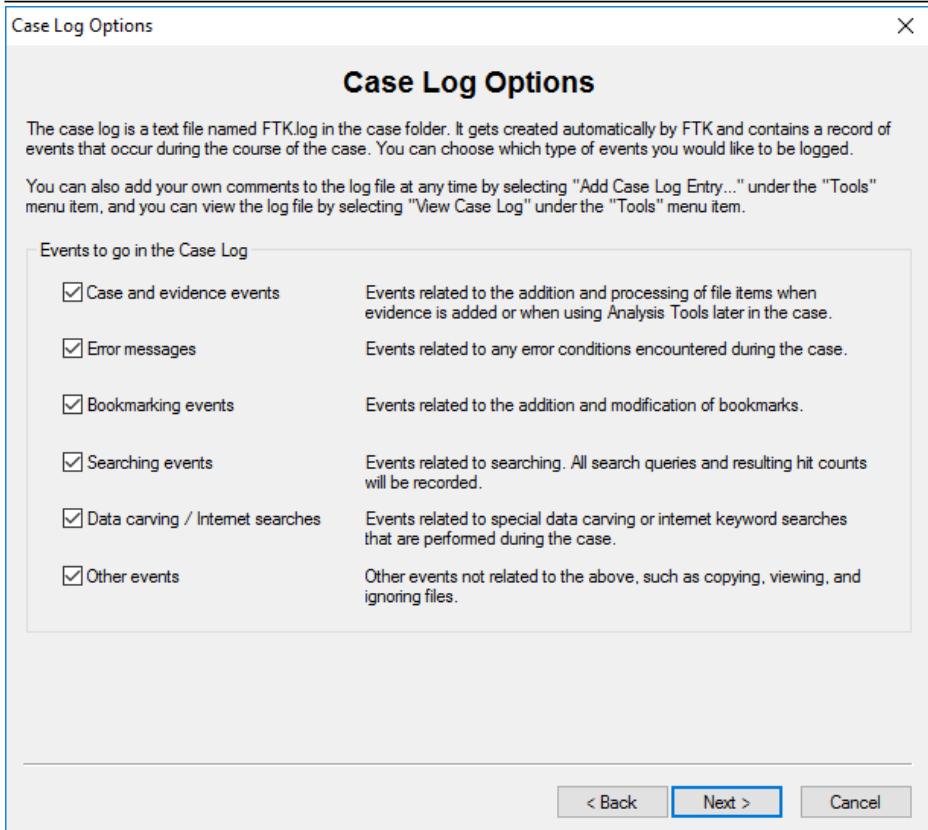
Examiner's Name

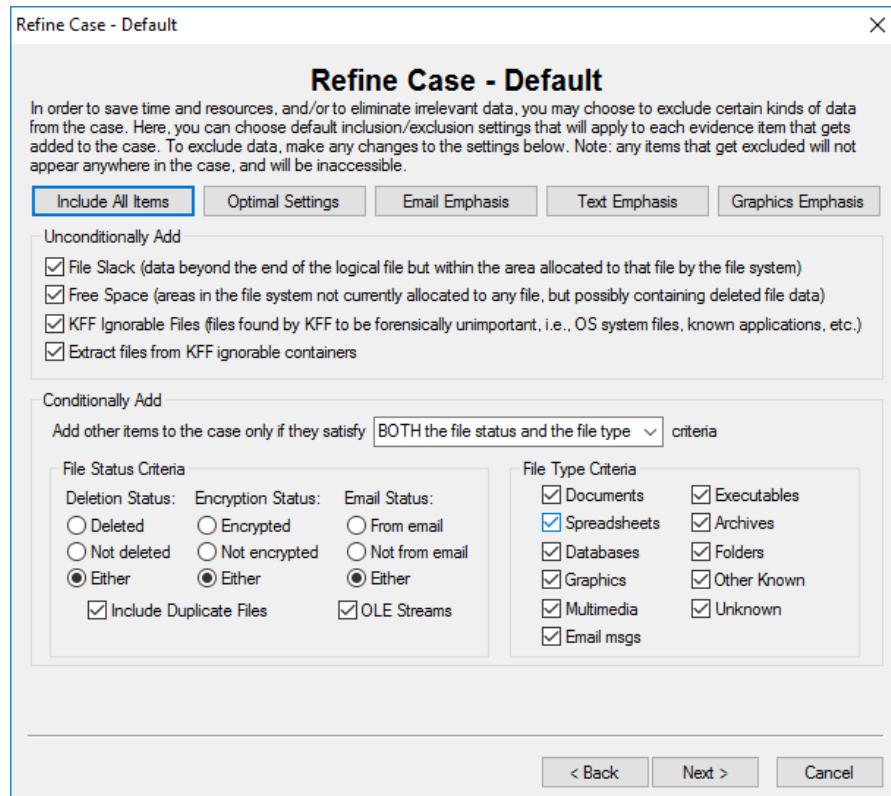
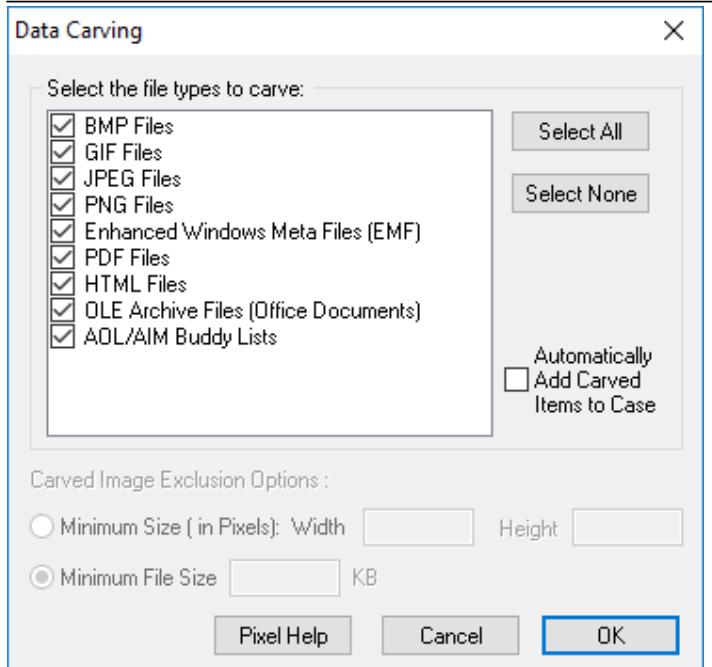
Address:

Phone: Fax:

E-Mail:

Comments:





Refine Index - Default

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

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

[< Back](#) [Next >](#) [Cancel](#)

Add Evidence to Case

Add Evidence

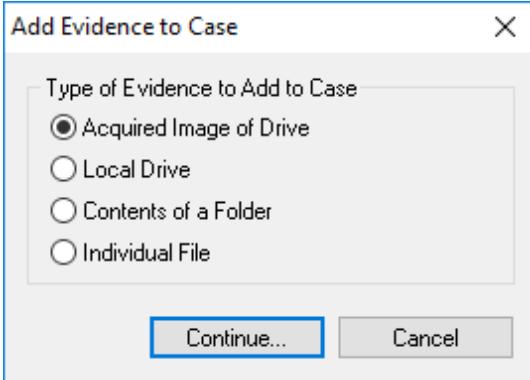
Any number of evidence items can be added to the case. There are several types of evidence items:

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

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

Add Evidence...	Edit Evidence...	Remove Evidence	Refine Evidence - Advanced...			
Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment

[< Back](#) [Next >](#) [Cancel](#)



Evidence Information X

Evidence Location:
F:\sem4\ComputerForensics\sample1.img

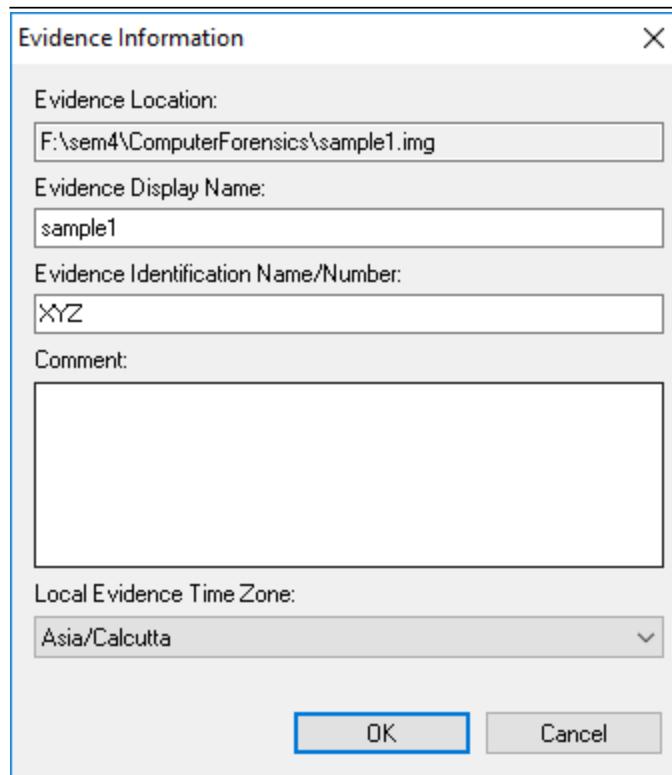
Evidence Display Name:
sample1

Evidence Identification Name/Number:
XYZ

Comment:

Local Evidence Time Zone:
Asia/Calcutta

OK Cancel



Add Evidence to Case X

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/Number	Type	Refined	Time Zone	Comment
sample1\KEEPPRYVAT-F...	F:\sem4\Com...	XYZ	FAT12	N	Asia/Calc...	

[Add Evidence...](#) [Edit Evidence...](#) [Remove Evidence](#) [Refine Evidence - Advanced...](#)

[<> Back](#) [Next >](#) [Cancel](#)

Case Summary X

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: 1

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	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.
Entropy Test:	Yes	
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

[<> Back](#) [Finish](#) [Cancel](#)

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	19	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	19	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	19	Duplicate Items:	2	Archives:	4
Filtered Out:	0	OLE Subitems:	10	Folders:	1
<input type="button" value="Unfiltered"/>	<input type="button" value="Filtered"/>	Flagged Ignore:	0	Slack/Free Space:	5
<input type="button" value="All Items"/>	<input type="button" value="Actual Files"/>	KFF Ignorable:	0	Other Known Type:	1
		Data Carved Files:	0	Unknown Type:	6

OFF Unfiltered DTZ

Evidence File Name	Evidence Path	Display Name	Identification Name/Number	Evidence Type
sample1.img	F:\sem4\ComputerForensics	sample1\KEEPPRY...	XYZ	FAT12

1 Listed 0 Checked Total F:\sem4\ComputerForensics\sample1.img

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	19	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	19	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	19	Duplicate Items:	2	Archives:	4
Filtered Out:	0	OLE Subitems:	10	Folders:	1
<input type="button" value="Unfiltered"/>	<input type="button" value="Filtered"/>	Flagged Ignore:	0	Slack/Free Space:	5
<input type="button" value="All Items"/>	<input type="button" value="Actual Files"/>	KFF Ignorable:	0	Other Known Type:	1
		Data Carved Files:	0	Unknown Type:	6

OFF Unfiltered DTZ

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Children
dataSpaces	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	3,584	13,312	
IPmay	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Stream	Unknown	N/A	N/A	N/A	N/A	208	13,312	
lodlist.txt	sample1\KEEPPRY\VAT-FAT12\lodlist.txt			Plain Text D...	Document		10/7/2007 7:11:28 PM	10/6/2007 10:08:12 ...	10/7/2007 12:00:00 ...	137	512	
Root Folder	sample1\KEEPPRY\VAT-FAT12			Root Folder	Folder	N/A	N/A	N/A	N/A	7,168	7,168	
dataSpaceInfo	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	2,560	13,312	
DriveFreeSpace1	sample1\KEEPPRY\VAT-FAT12\DriveFreeSpace1			OLE Stream	Unknown	N/A	N/A	N/A	N/A	112	13,312	
EncryptedPackage	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Encry...			OLE Stream	Unknown	N/A	N/A	N/A	N/A	1,311,232	26,214,400	
EncryptionInfo	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Encry...			OLE Stream	Unknown	N/A	N/A	N/A	N/A	9,016	13,312	
FAT1	sample1\KEEPPRY\VAT-FAT12\FAT1			File Allocatio...	Slack/Free S...	N/A	N/A	N/A	N/A	248	13,312	
FAT2	sample1\KEEPPRY\VAT-FAT12\FAT2			File Allocatio...	Slack/Free S...	N/A	N/A	N/A	N/A	4,608	4,608	
FileSlack	sample1\KEEPPRY\VAT-FAT12\lodlist.txt>\File...			File Slack	Slack/Free S...	N/A	N/A	N/A	N/A	375	512	
StrongEncryptionDataSpace	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Stream	Unknown	N/A	N/A	N/A	N/A	64	13,312	
StrongEncryptionTransform	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	2,560	13,312	
loja.cgi	sample1\KEEPPRY\VAT-FAT12\loja.cgi			JPEG/JIF File	Graphic		10/7/2007 7:11:12 PM	9/26/2005 12:15:32 ...	10/7/2007 12:00:00 ...	132,706	133,120	
TransformInfo	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Embedd...	Archive		10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	10/7/2007 8:25:31 PM	2,560	13,312	
VBR	sample1\KEEPPRY\VAT-FAT12\VBR			Volume Boot	Slack/Free S...	N/A	N/A	N/A	N/A	512	512	
Version	sample1\KEEPPRY\VAT-FAT12\wics.xlsx>\Data...			OLE Stream	Unknown	N/A	N/A	N/A	N/A	76	13,312	
wics.xlsx	sample1\KEEPPRY\VAT-FAT12\wics.xlsx		xlsx	Encrypted U...	Other		10/7/2007 8:11:02 PM	10/7/2007 10:55:34 ...	10/7/2007 12:00:00 ...	13,112	13,312	

19 Listed 0 Checked Total 0 Highlighted

Create New Bookmark

Bookmark name: peter

Bookmark comment:

Apply bookmark to:

All highlighted items (selected)

All checked items

All currently listed items

File Name: index_flat[1].htm

File Path: precious\Part_1\The Precious-N...

Remember file position/selection

Report options:

Include in report Export files

Include parent of email attachments?

OK Cancel

FTK Report Wizard - Case Information

Case Information

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

Include Investigator Information in report

Agency/Company: College

Investigator's Name: XYZ

Address: churchgate

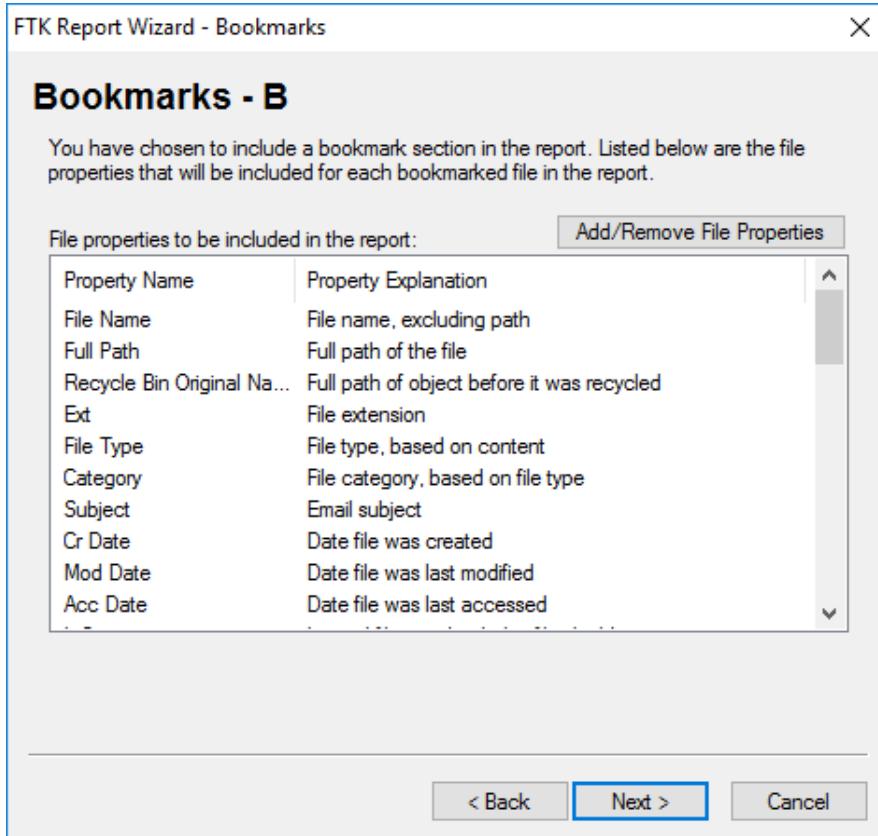
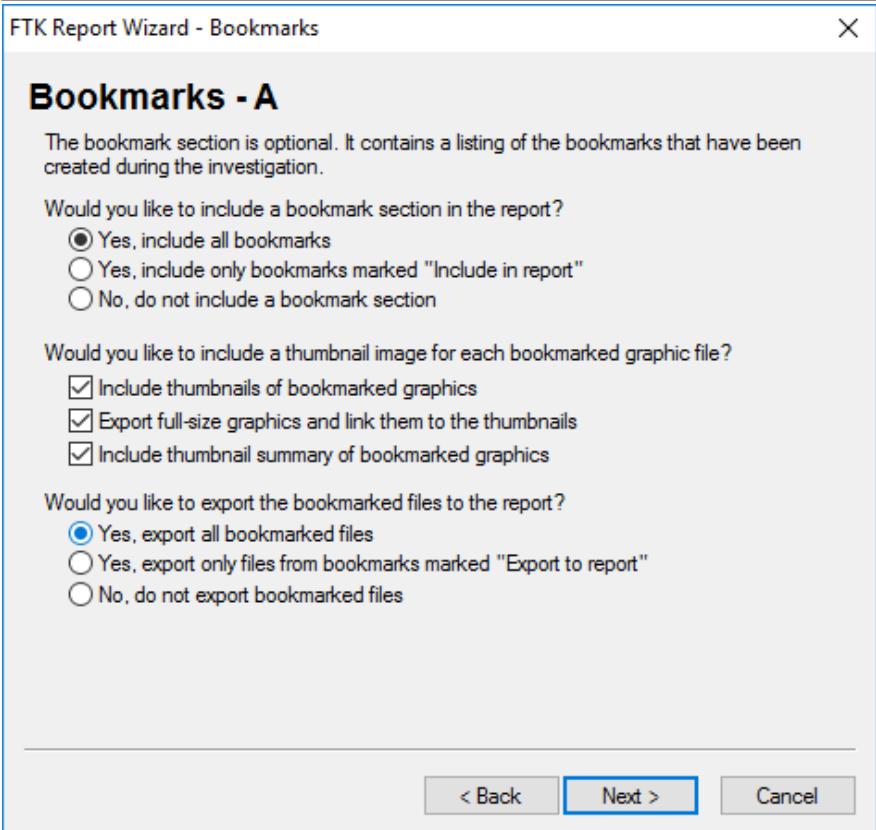
Phone: 1234567890

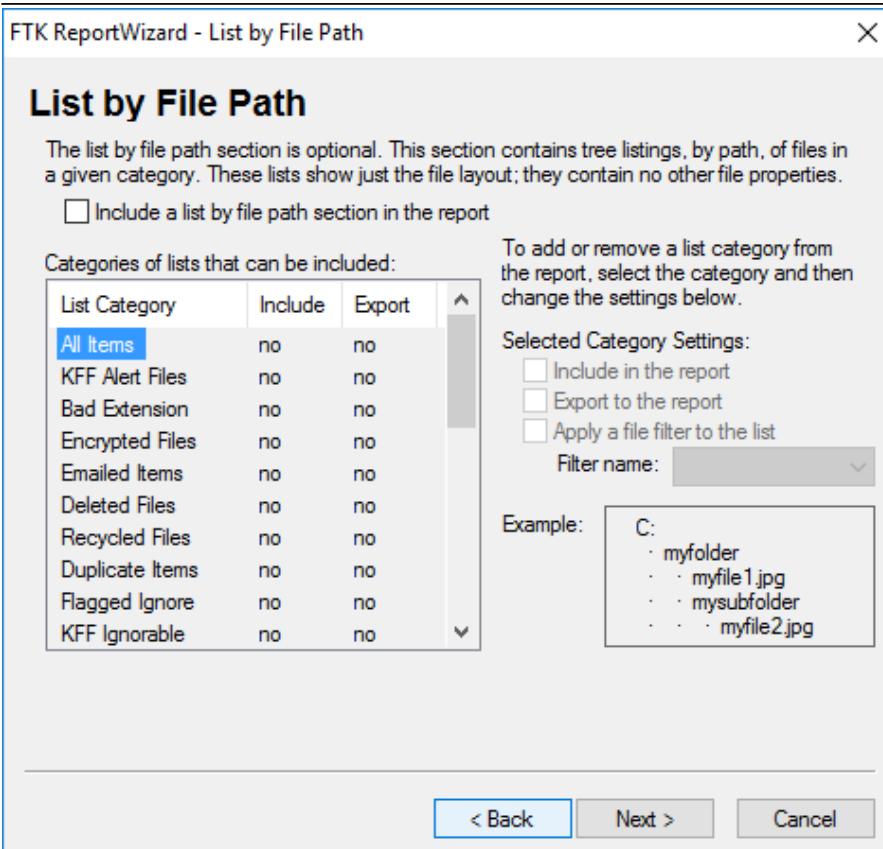
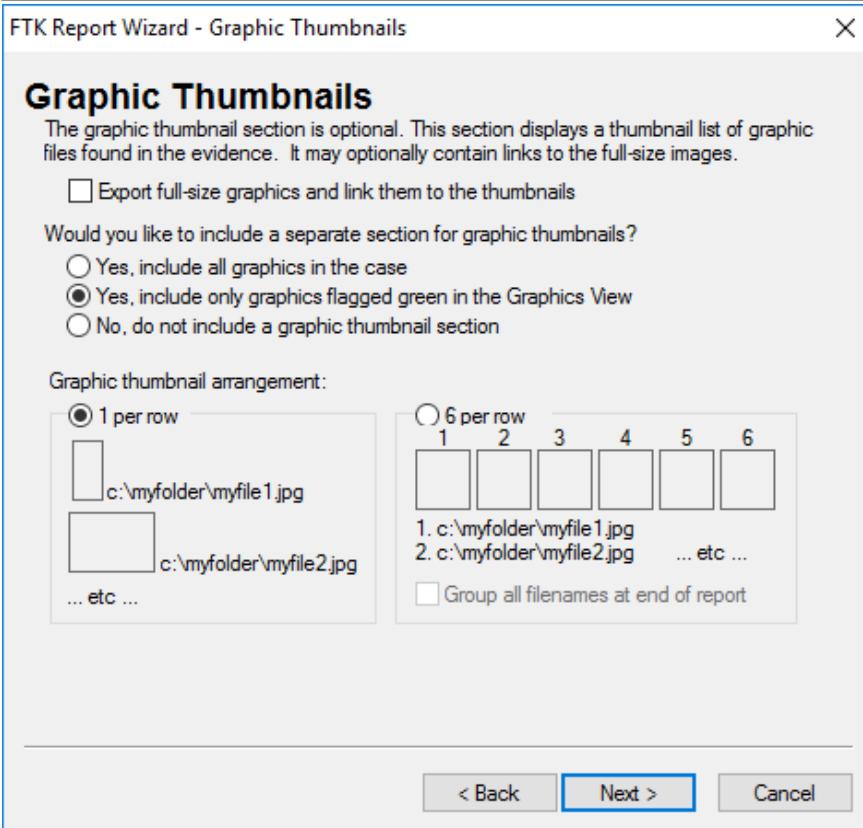
Fax:

E-Mail: xyz@gmail.com

Comments:

Next > Cancel





FTK Report Wizard - List File Properties

List File Properties - A

The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.

Include a list file properties section in the report
 Include MS Access database in report

Categories of lists to be included in the report:

List Category	Include	Export
All Items	no	no
KFF Alert Files	no	no
Bad Extension	no	no
Encrypted Files	no	no
Emailed Items	no	no
Deleted Files	no	no
Recycled Files	no	no
Duplicate Items	no	no
Flagged Ignore	no	no
KFF Ignorable	no	no

To add or remove a list category from the report, select the category and then change its settings below.

Selected Category Settings:

Include in the report
 Export to the report
 Apply a file filter to the list

Filter name:

Example:

```
File: myfile1.jpg
Path: C:\myfolder
File Type: JPEG/JFIF File
Category: Graphic
L-Size: 37942
```

< Back Next > Cancel

FTK Report Wizard - Supplementary Files

Supplementary Files

You can add your own files to the report by including them in the list below. Any type of file can be included. The file will be copied and hyperlinked to the report.

Supplementary Files: Add Files Remove File

Filename	Link name
C:\testprac2\testprac2.ftk	C:\testprac2\testprac2.ftk

< >

Check here if you want the case log included in the report. The case log contains a log of many of the events that occur during the course of a case.

Include Case Log in report
 Include HTML File Listing from preprocessing

< Back Next > Cancel

Report Location

FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.

NOTE 1: If you select an existing folder (other than the default), it must be empty.

NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.

NOTE 3: If you are expecting to copy this report to recordable media, remember:
CDR = 650MB, DVDR = 4.5GB

Report folder:

Browse...

Export all files using actual filenames (may cause broken links on CDs or DVDs)

Include Registry Viewer reports

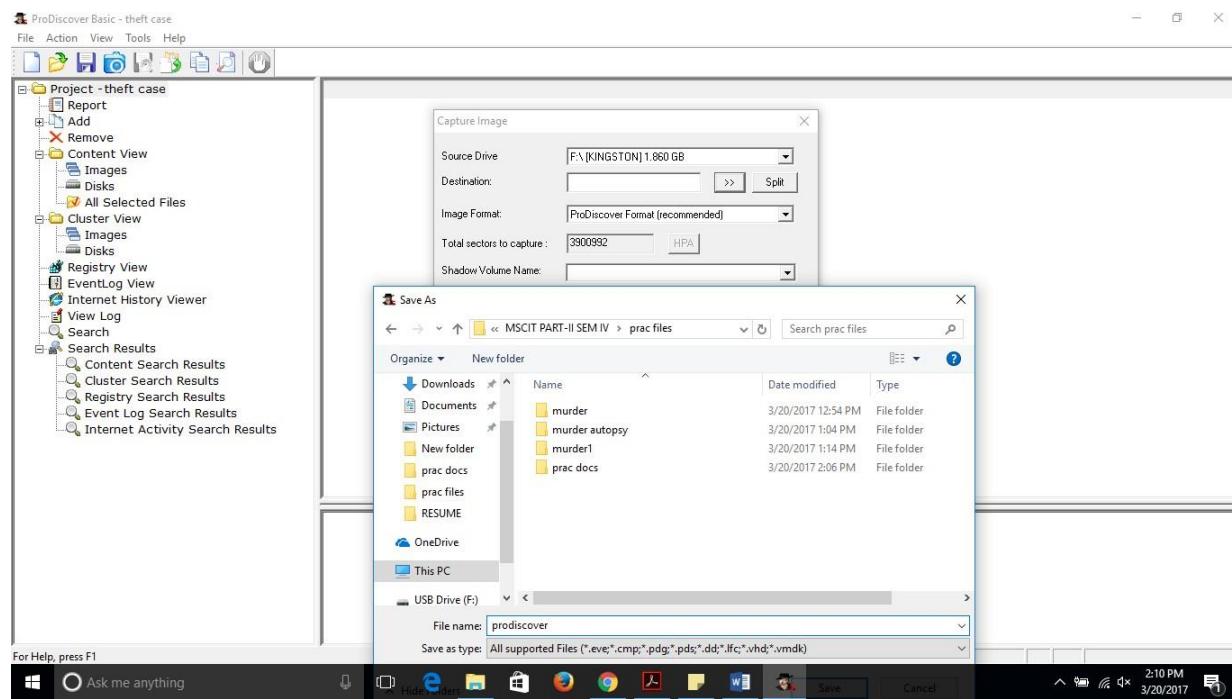
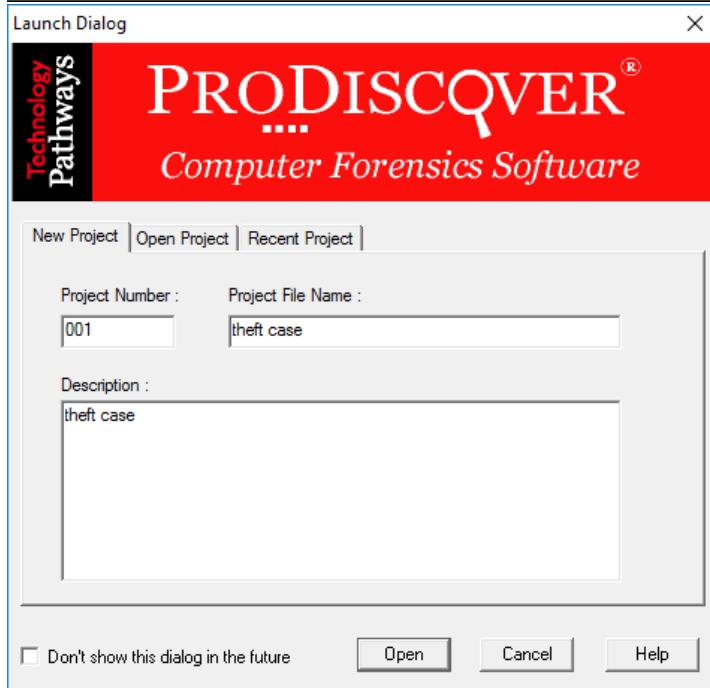
Custom graphic for the report (recommended maximum width is 183 pixels)

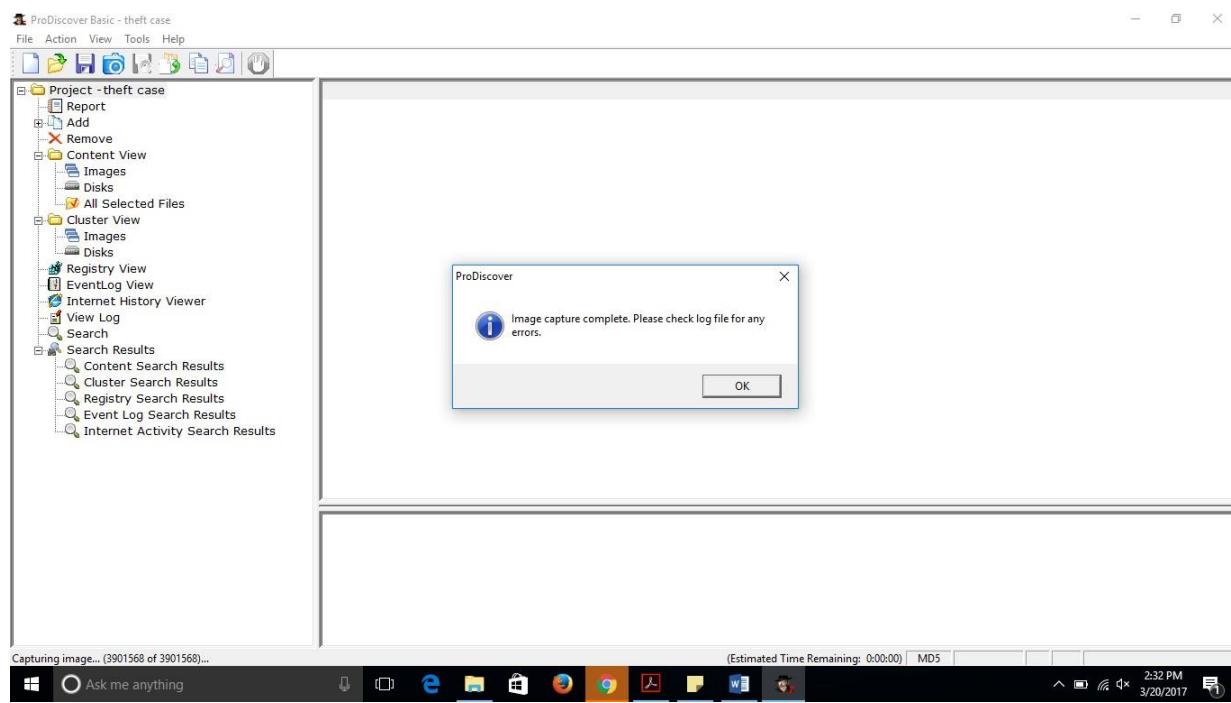
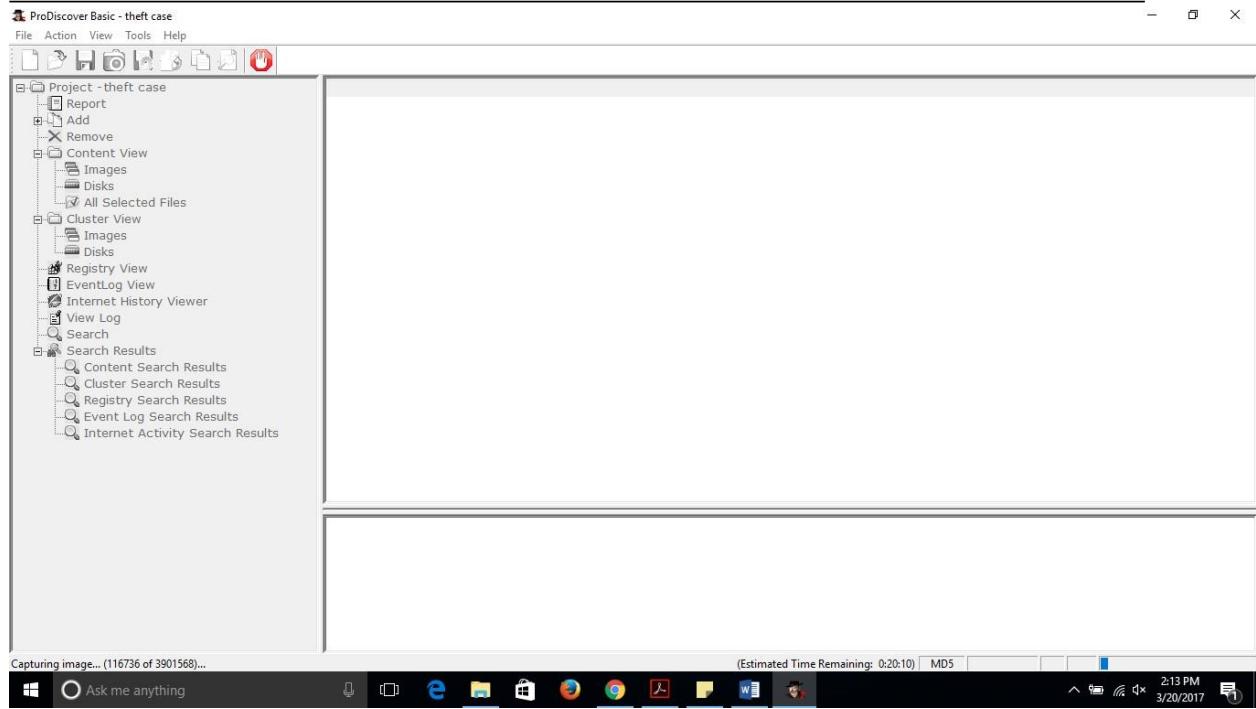
Browse...

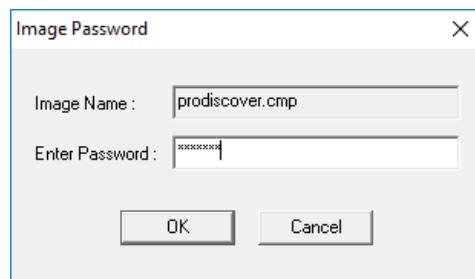
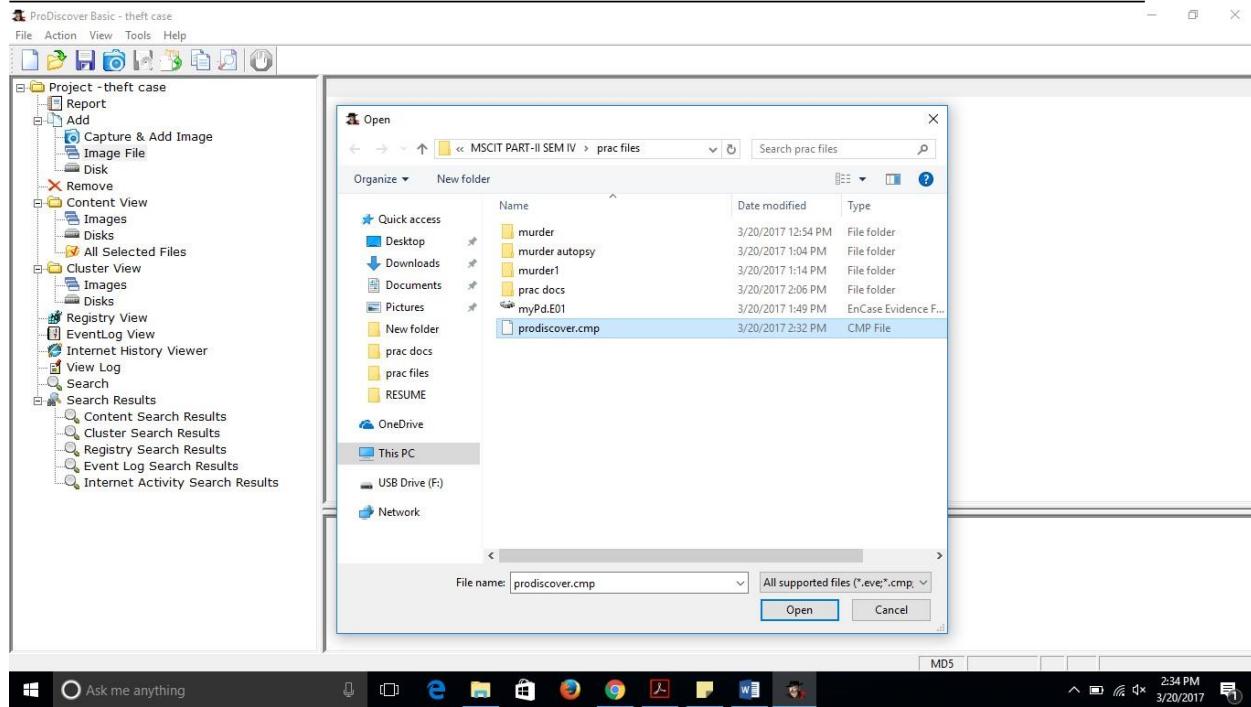
Report language:

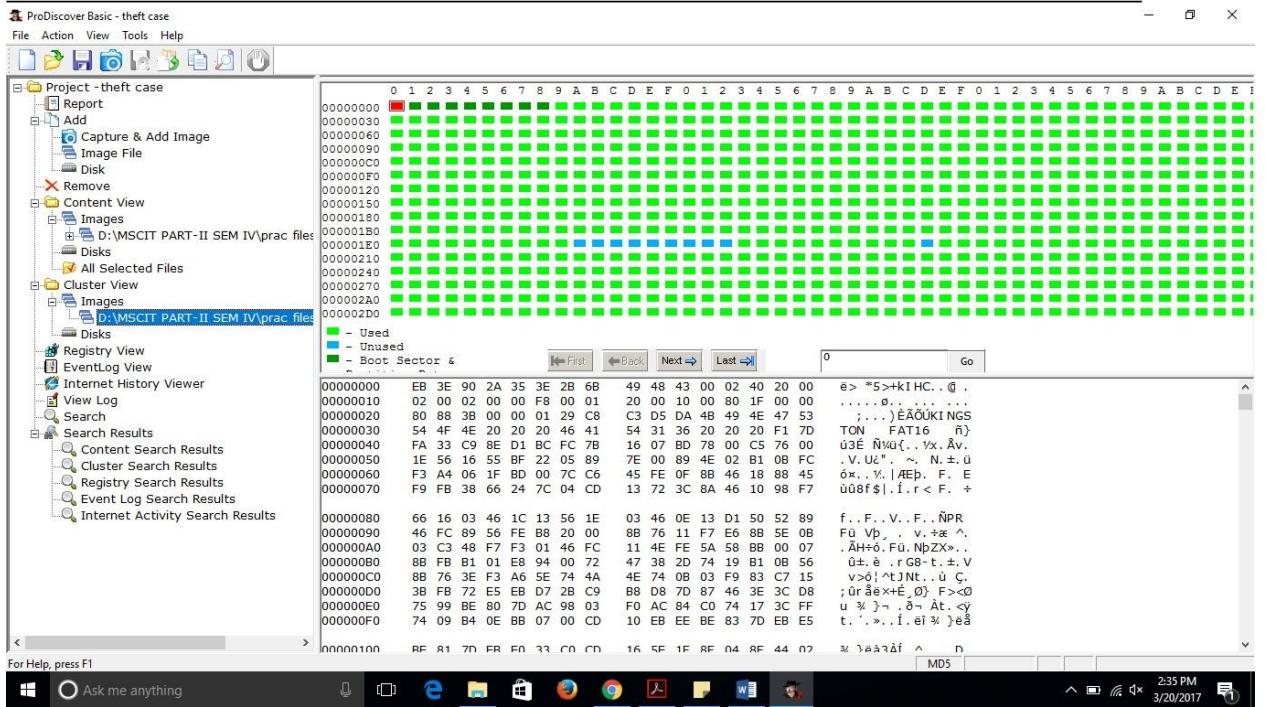
▼< BackFinishCancel

PRACTICAL NO 08: Use a tool to scan drive and it's slack space. (ProDiscover)









ProDiscover Basic - theft case

File Action View Tools Help

Project - theft case

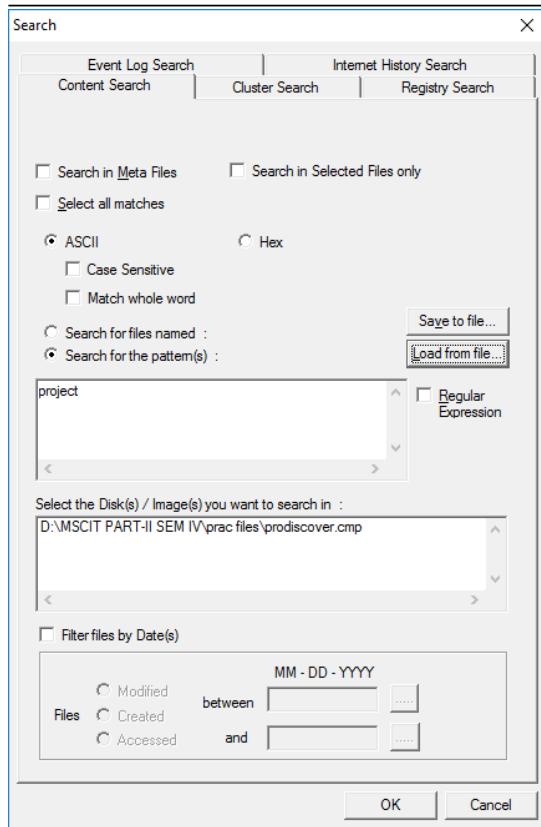
- Report
- Add
 - Capture & Add Image
 - Image File
 - Disk
- Remove
- Content View
 - Images
 - D: \MSCIT PART-II SEM IV\prac files
 - Disk
- All Selected Files
- Cluster View
 - Images
 - D: \MSCIT PART-II SEM IV\prac files
 - Disk
- Registry View
- EventLog View
- Internet History Viewer
- View Log
- Search
- Search Results
 - Content Search Results
 - Cluster Search Results
 - Registry Search Results
 - Event Log Search Results
 - Internet Activity Search Results

Select File Name File Extension Size Attributes Deleted Created Date Modified Date Accessed Date

Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date
	SLATKO		- d - - -	NO	01/28/2010 ...	01/28/2010 ...	01/28/2010 ...	01/28/2010 ...
	RECYCLERW		- d - - -	NO	12/15/2010 ...	12/15/2010 ...	12/15/2010 ...	12/15/2010 ...
	TOPILA		- d - - -	NO	12/17/2010 ...	12/17/2010 ...	12/17/2010 ...	12/17/2010 ...
	TIFR		- d - - -	NO	12/04/2011 ...	12/04/2011 ...	12/04/2011 ...	12/04/2011 ...
	FINAL		- d - - -	NO	12/15/2010 ...	12/15/2010 ...	12/15/2010 ...	12/15/2010 ...
	SHP BATCH 7		- d - - -	NO	04/24/2010 ...	04/24/2010 ...	04/24/2010 ...	04/24/2010 ...
	SELOMOJE		- d - - -	NO	06/11/2010 ...	06/11/2010 ...	06/11/2010 ...	06/11/2010 ...
	Sohel new t...		- d - - -	NO	04/28/2011 ...	04/28/2011 ...	04/28/2011 ...	01/01/2013 ...
	.Trashes		- d - - -	NO	04/29/2011 ...	04/29/2011 ...	04/29/2011 ...	04/29/2011 ...
	RECYCLER		- d - s h r	NO	08/24/2010 ...	08/24/2010 ...	08/24/2010 ...	08/24/2010 ...
	CV		- d - - -	NO	01/03/2012 ...	01/03/2012 ...	01/03/2012 ...	01/03/2012 ...
	SJ		- d - - -	NO	02/06/2012 ...	02/06/2012 ...	02/06/2012 ...	02/06/2012 ...
	.feventsds		- d - - -	NO	04/29/2011 ...	04/29/2011 ...	04/29/2011 ...	04/29/2011 ...
	prachideepika		- d - - -	NO	04/29/2011 ...	04/29/2011 ...	04/29/2011 ...	08/07/2012 ...
	EUROPE		- d - - -	NO	12/11/2011 ...	12/11/2011 ...	12/11/2011 ...	12/20/2011 ...
	System Volu...		- d - s h -	NO	03/20/2017 ...	03/20/2017 ...	03/20/2017 ...	03/20/2017 ...
	PRIYANKA		- d - - -	NO	04/30/2011 ...	04/30/2011 ...	04/30/2011 ...	04/30/2011 ...
	picture tybsc		- d - - -	NO	12/16/2011 ...	12/16/2011 ...	12/16/2011 ...	02/23/2013 ...
	Auturon.inf		- d - - -	NO	12/20/2011 ...	12/20/2011 ...	12/20/2011 ...	12/20/2011 ...
	ãEWFOL~3		- d - - -	YES	02/09/2012 ...	02/09/2012 ...	02/09/2012 ...	02/09/2012 ...
	RSM		- d - - -	NO	07/24/2011 ...	07/24/2011 ...	07/24/2011 ...	06/21/2012 ...
	.Spotlight-V...		- d - h -	NO	01/03/2012 ...	01/03/2012 ...	01/03/2012 ...	01/03/2012 ...
	Kala ma'mam		- d - - -	NO	01/02/2012 ...	12/18/2011 ...	01/03/2012 ...	01/03/2012 ...

188 Object(s) (32 Folder(s), 156 File(s))

Ask me anything 2:36 PM 3/20/2017



ProDiscover Basic - theft case

File Action View Tools Help

Project - theft case

- Report
- Add
- Capture & Add Image
- Image File
- Disk
- Remove
- Content View
- Images D:\MSCIT PART-II SEM IV\prac f
 - .seventsnd
 - .Spotlight-V100
 - .Trashes
 - âEWFOLO~3
 - Autorun.inf
 - CIAO
 - CV
 - EUROPE
 - FINAL
 - FINAL JOURNAL
 - Kala ma'am
 - New Folder
 - New Folder (2)
 - picture tybsc
 - POZUDA
 - prachideepika
 - PRINT
 - PRIYANKA
 - RECYCLER
 - RECYCLERW
 - RSM
 - SELOMOJE
 - SHP BATCH 7
 - SJ

Search 1 |

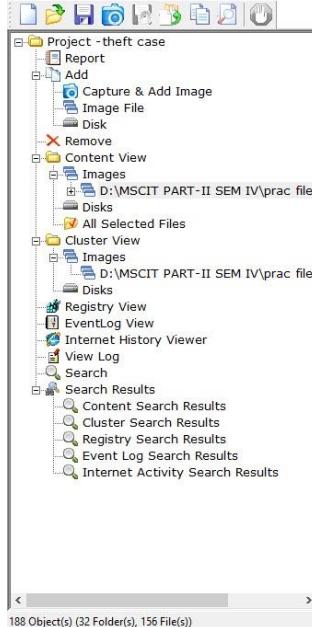
Search terms	File Name	Found in
project	CERTIFICATE Page.doc	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	\WRD2430.TMP	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	\WRL2587.TMP	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	CERTIFICATE Page.doc	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	\RZB2.TMP	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	print.exe	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	\LE0001.CHK	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	Writing a Research paper.ppt	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	Writing Book Reviews.ppt	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	KJ1.C.SHP-2010.ppt	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	Myths associated with Snakes final.ppt	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	CERTIFICATE Page.doc	D:\MSCIT PART-II SEM IV\prac files\prodiscover...
	cover page- SHP Project.doc	D:\MSCIT PART-II SEM IV\prac files\prodiscover...

0 occurrences found.

Ask me anything

MDS

2:47 PM 3/20/2017



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date
<input type="checkbox"/>	A	OUT	1 byte	a-----	NO	12/20/2011 ...	12/20/2011 ...	03/04/2014
<input checked="" type="checkbox"/>	Green chemi...	doc	97,792 bytes	a-----	NO	08/24/2010 ...	08/24/2010 ...	03/04/2014
<input type="checkbox"/>	New Microso...	docx	12,719 bytes	a-----	NO	04/29/2011 ...	06/13/2011 ...	03/04/2014
<input type="checkbox"/>	Biofuels are ...	doc	122,880 bytes	a-----	NO	08/24/2010 ...	08/24/2010 ...	03/04/2014
<input type="checkbox"/>	3WRD0401.TMP	TMP	34,652 bytes	a-----	YES	03/15/2014 ...	03/15/2014 ...	03/15/2014
<input type="checkbox"/>	FAQs.doc	doc	80,896 bytes	a-----	NO	09/22/2010 ...	09/22/2010 ...	03/04/2014
<input type="checkbox"/>	sohel chitra(....doc	doc	372,736 bytes	a-----	NO	04/30/2011 ...	04/30/2011 ...	03/15/2014
<input type="checkbox"/>	3EGSVR.EXE	EXE	674,816 bytes	a-----	YES	06/15/2011 ...	09/08/2008 ...	07/26/2011
<input type="checkbox"/>	All reagents ...	doc	46,080 bytes	a-----	NO	09/30/2010 ...	09/30/2010 ...	03/04/2014
<input type="checkbox"/>	Latest Inv\Add Comment				NO	10/20/2010 ...	10/20/2010 ...	03/04/2014
<input type="checkbox"/>	Removal of ...				NO	10/20/2010 ...	10/20/2010 ...	03/04/2014
<input type="checkbox"/>	total report				NO	01/01/2003 ...	05/29/2011 ...	03/04/2014
<input checked="" type="checkbox"/>	ganesh data				YES	01/01/2003 ...	06/15/2011 ...	09/22/2012
<input type="checkbox"/>	ganesh pr...				YES	01/01/2003 ...	06/15/2011 ...	09/22/2012
<input type="checkbox"/>	G-3,G-B				NO	07/28/2011 ...	07/28/2011 ...	03/04/2014
<input type="checkbox"/>	tem 1				NO	07/26/2012 ...	01/25/2011 ...	03/04/2014

For File/Folder: D:\MSCIT PART-II SEM IV\prac files

file\prodDiscover.cmp\ganesh data.docx

Investigator comments:

deleted data

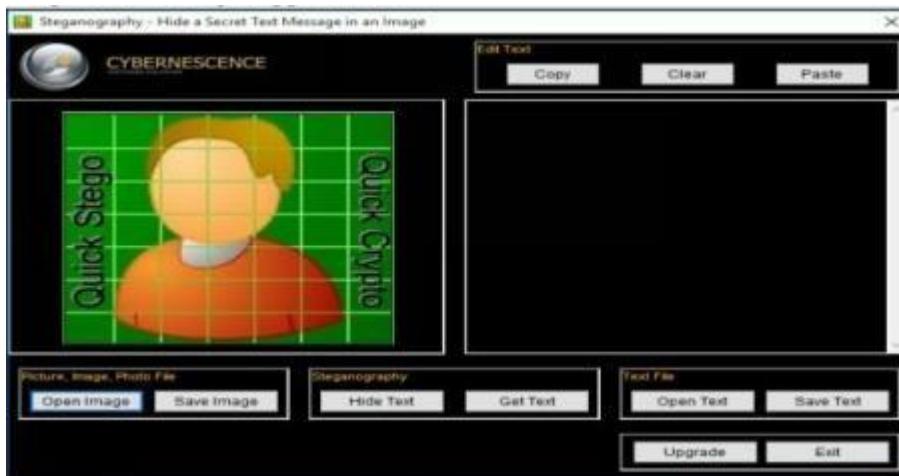
Page 1 of 2

188 Object(s) (32 Folder(s), 156 File(s))

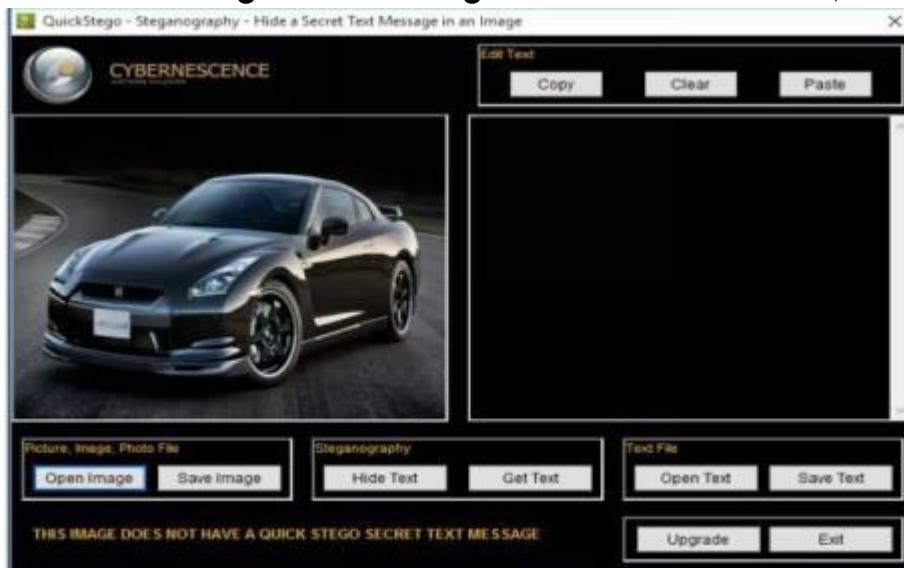
Windows Ask me anything 3:06 PM 3/20/2017

PRACTICAL NO 09: Hide text into image. (QuickStego, STool)

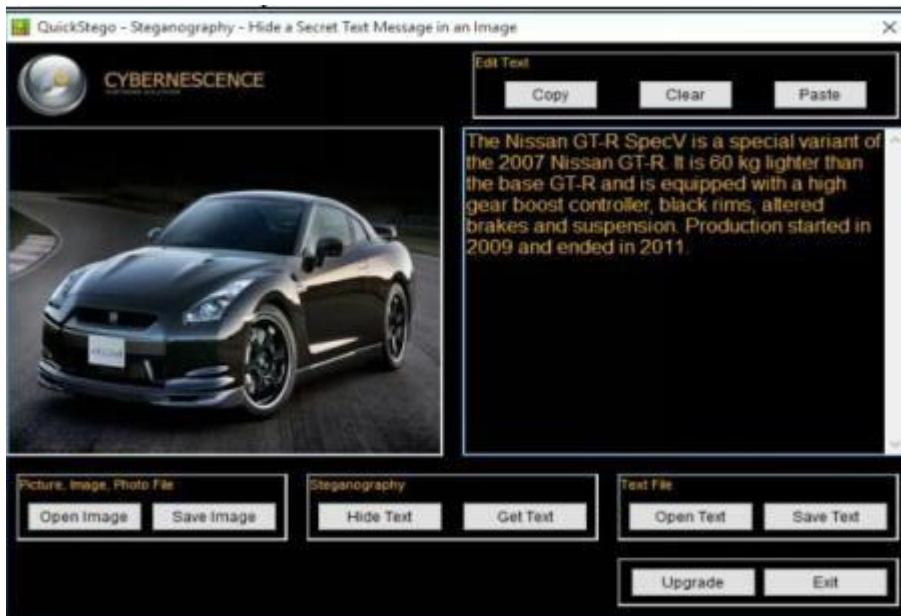
Using QuickStego Open QuickStego Application



Upload an Image. This Image is term as Cover, as it will hide the text.



Enter the Text or Upload Text File



Click Hide Text Button



Save Image - This Saved Image containing Hidden information is termed as Stego Object.

Recovering Data from Image Steganography using QuickStego → Open QuickStego → Click Get Text

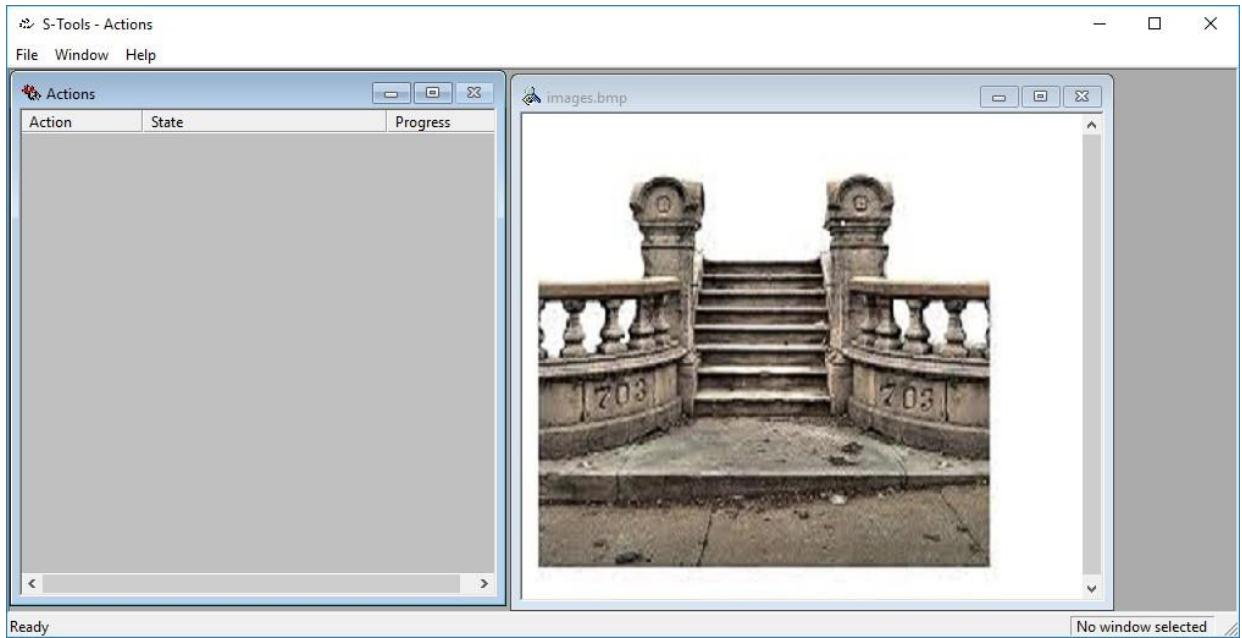
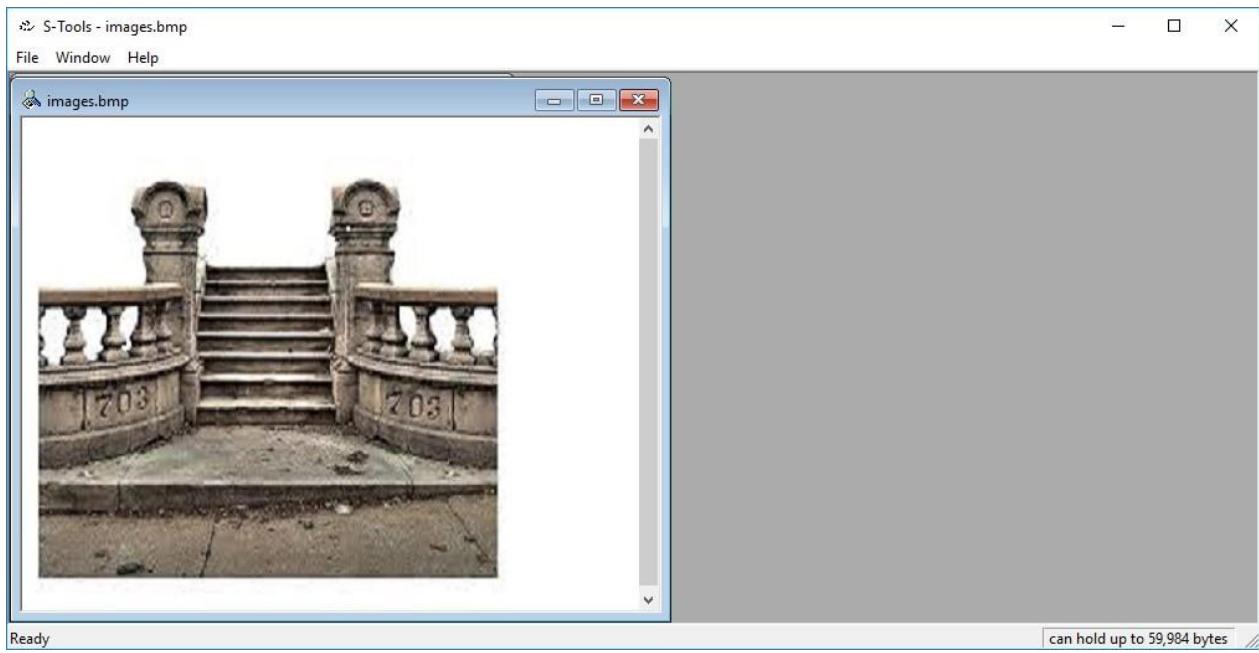


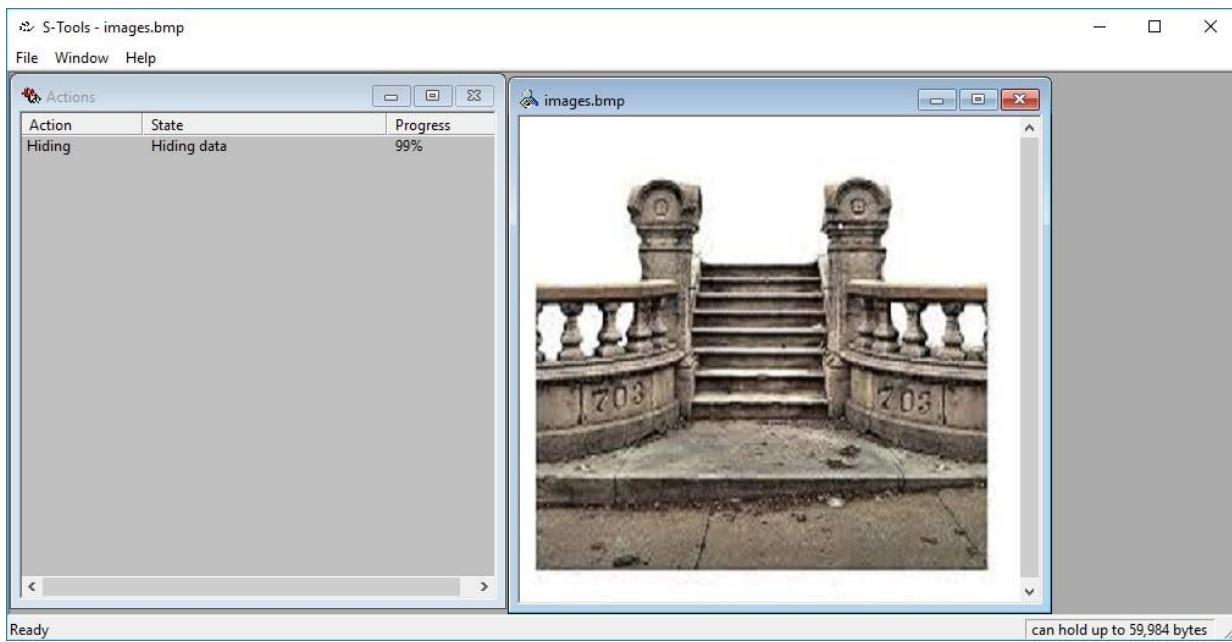
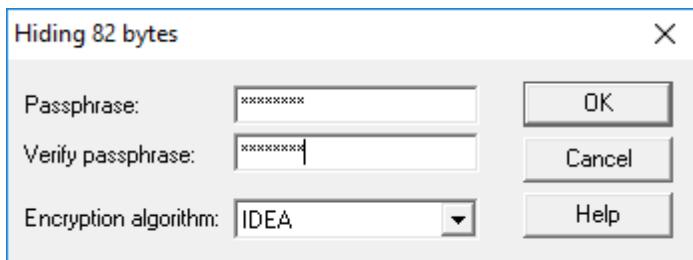
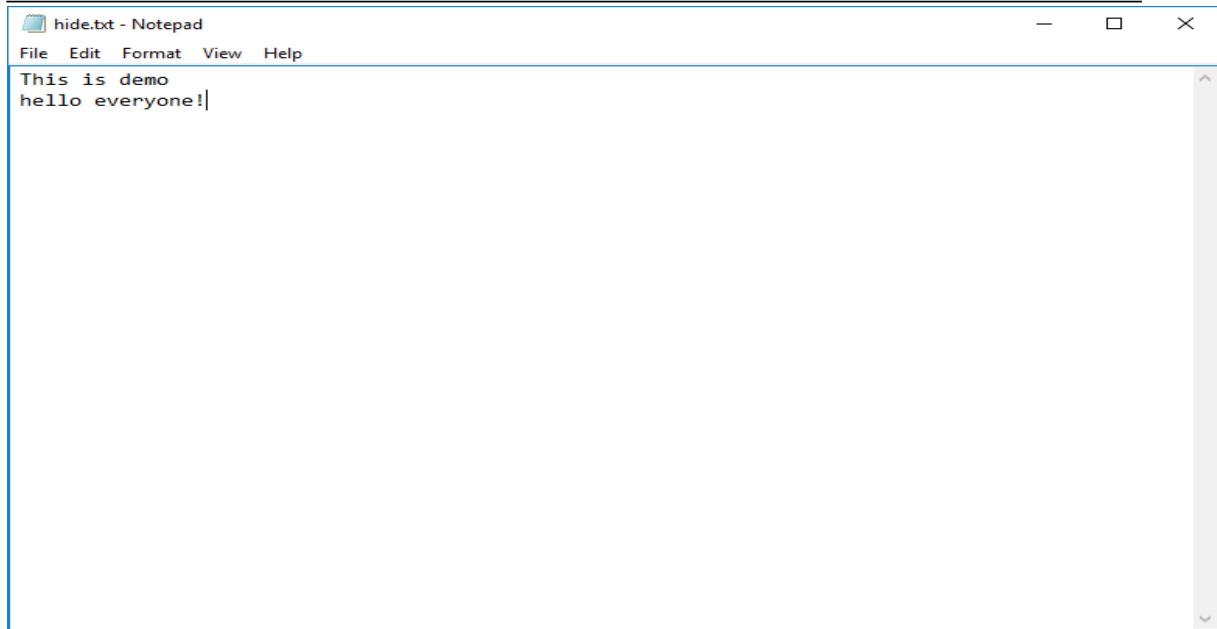
Open and Compare Both Images

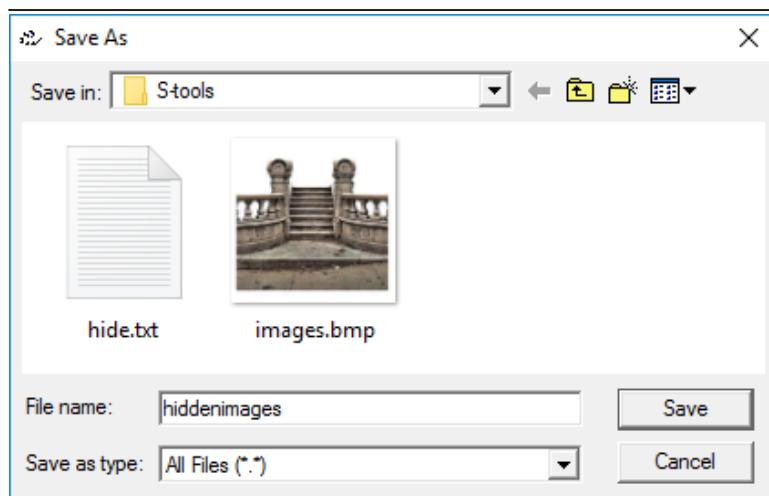
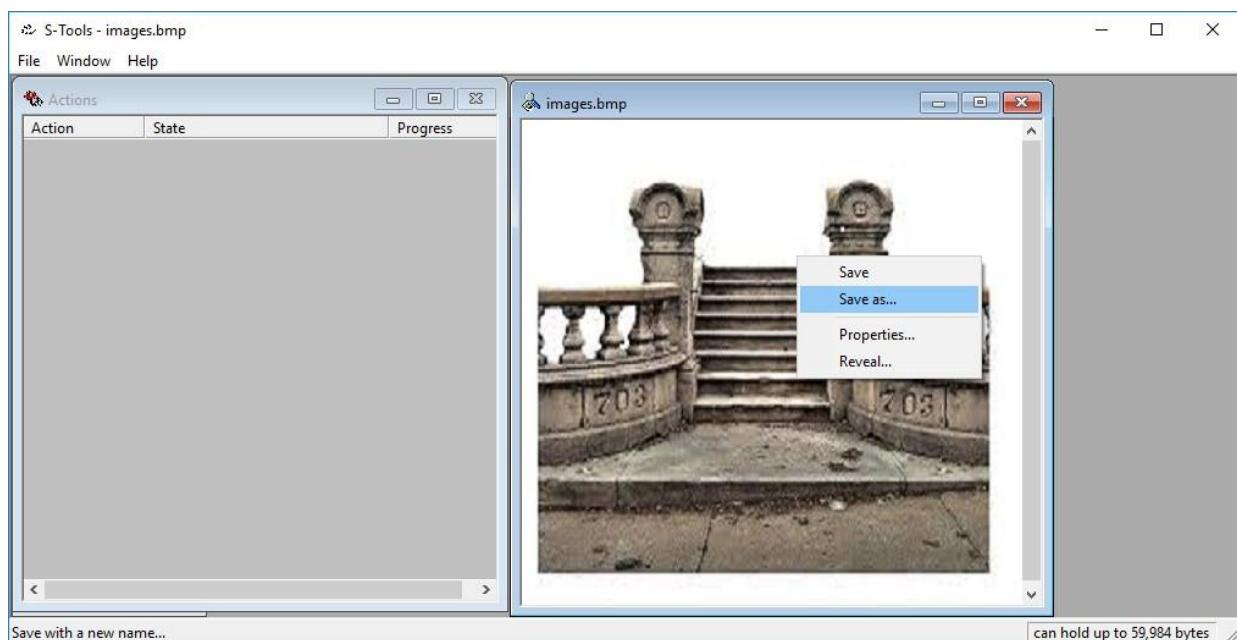


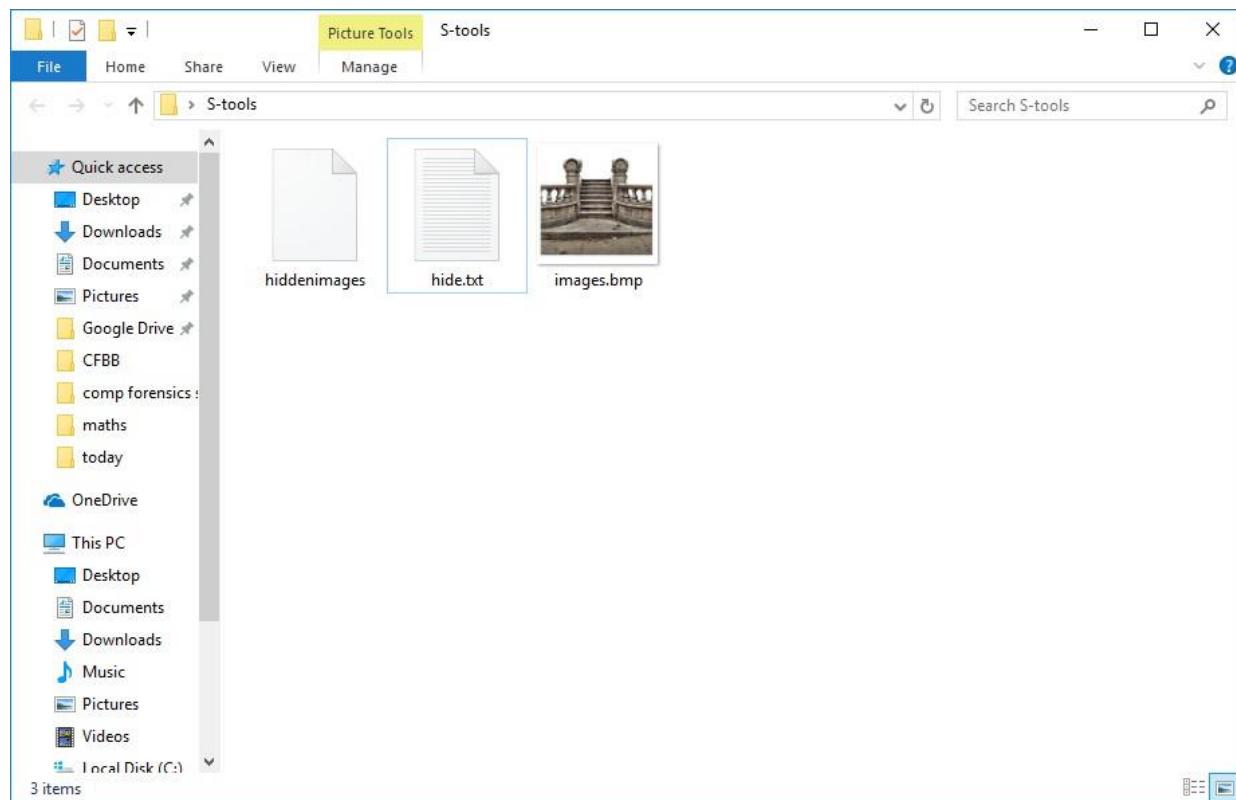
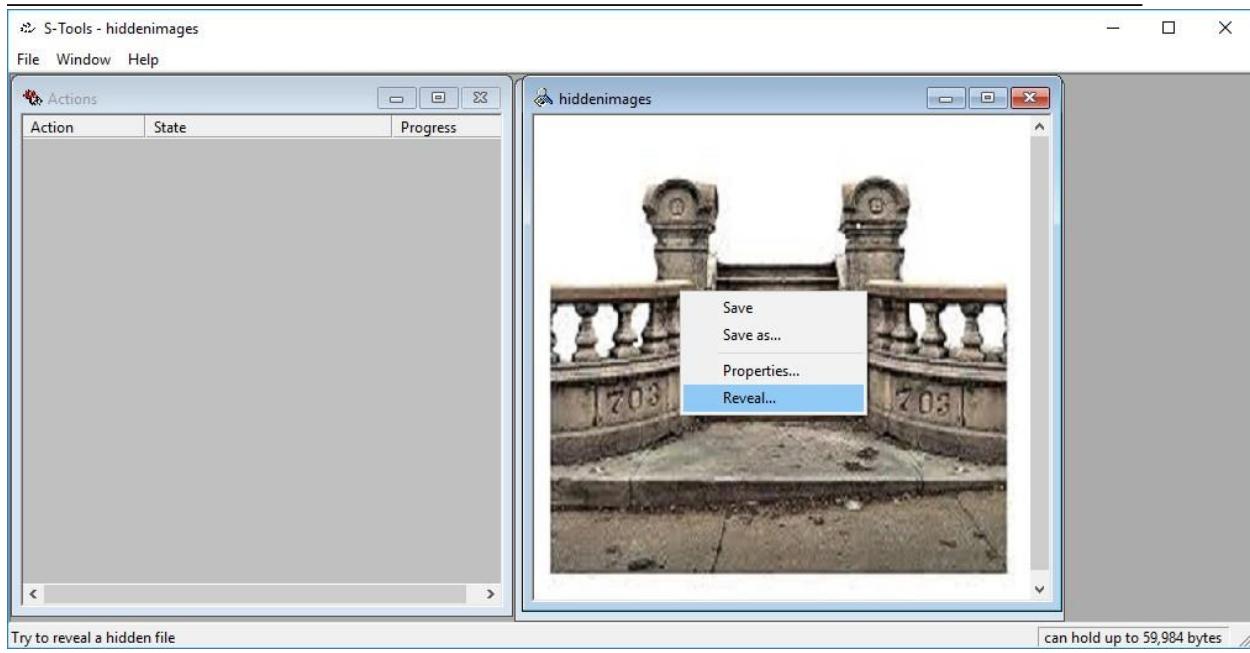
Left Image is without Hidden Text; Right Image is with hidden text

Using Tool: S tool







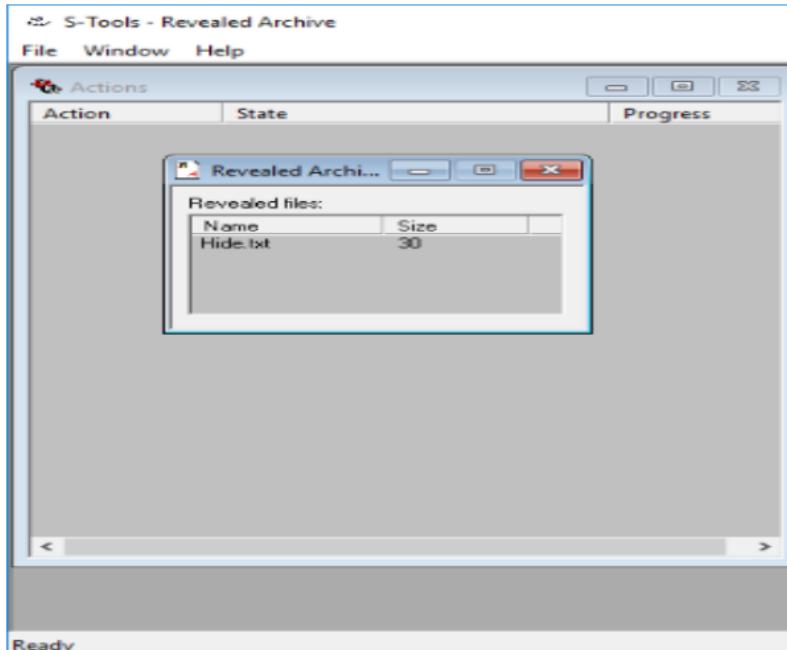


Revealing from hidden data X

Passphrase: OK

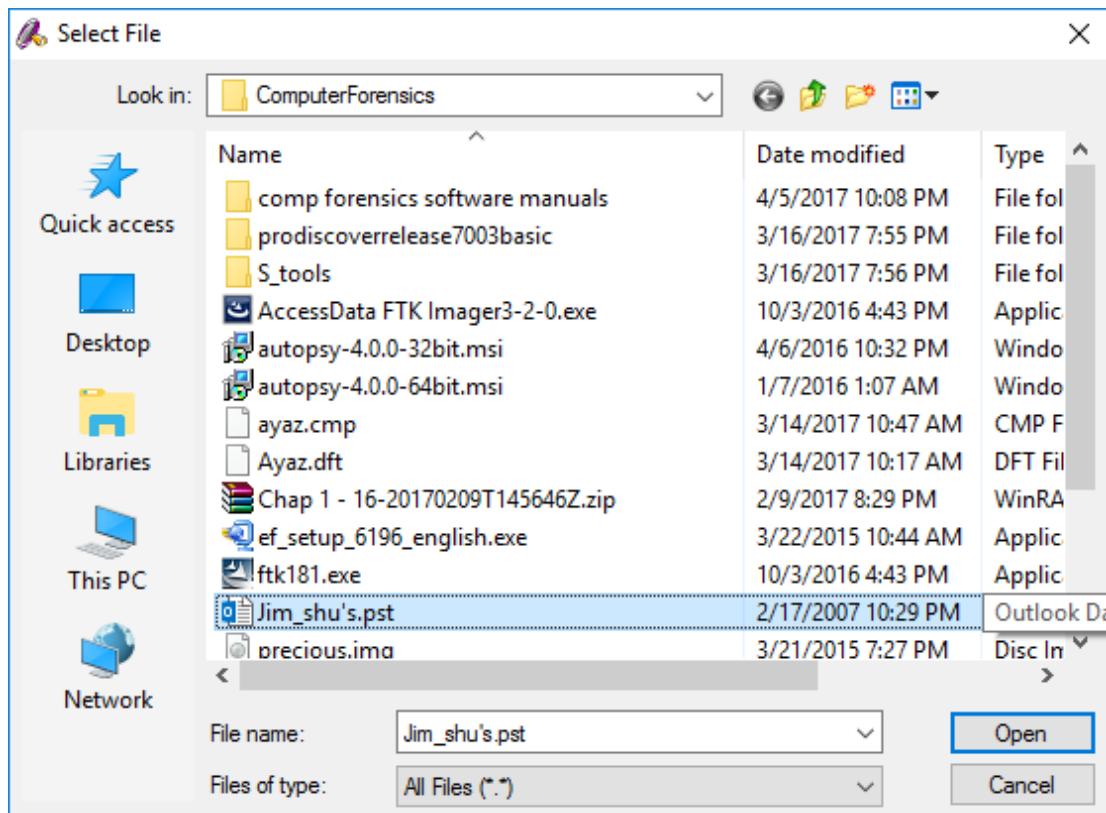
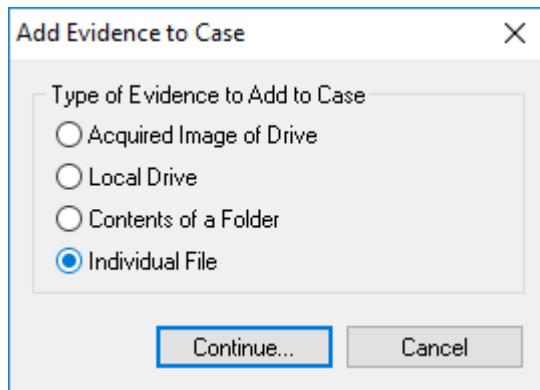
Verify passphrase: Cancel

Encryption algorithm: IDEA ▾ Help



PRACTICAL NO 10: Use Email Forensic Tools for Email Recovery Mobile Forensics

EMAIL FORENSIC



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	F:\sem4\Com...	XYZ	Individual f...	N	N/A	

< Back **Next >** Cancel

AccessData FTK 1.81.0 DEMO VERSION -- C:\testprac2\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

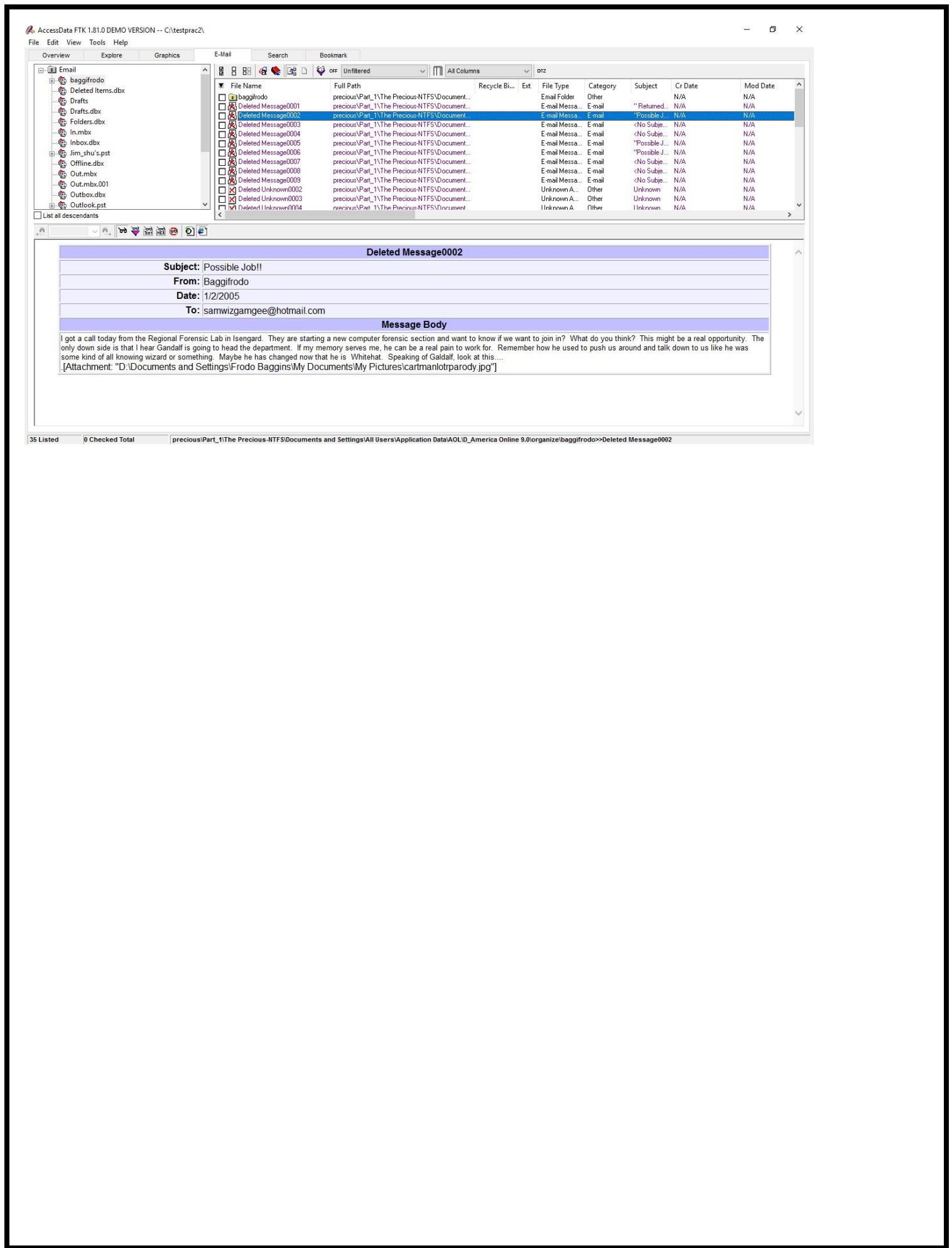
Evidence Items	File Status	File Category
3	KFF Alert Files: 0	Documents: 314
	Bookmarked Items: 1	Spreadsheets: 10
3832	Bad Extension: 159	Databases: 0
0	Encrypted Files: 19	Graphics: 1257
3832	From E-mail: 337	Multimedia: 45
0	Deleted Files: 58	E-mail Messages: 114
1257	From Recycle Bin: 6	Executables: 7
3832	Duplicate Items: 380	Archives: 56
0	OLE Subitems: 57	Folders: 669
All items	Flagged Ignore: 0	SlackFree Space: 7
All items	KFF Honorable: 0	Other Known Type: 495
	Data Carved Files: 0	Unknown type: 858

Unfiltered Filtered

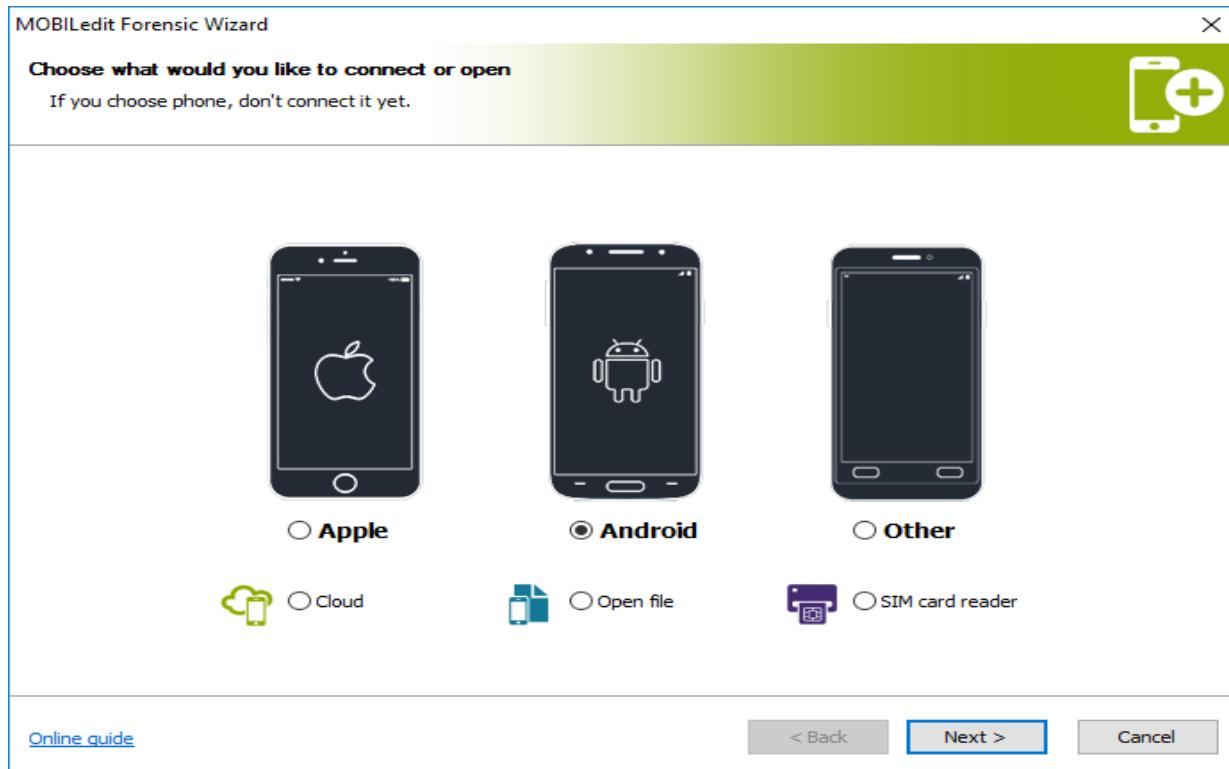
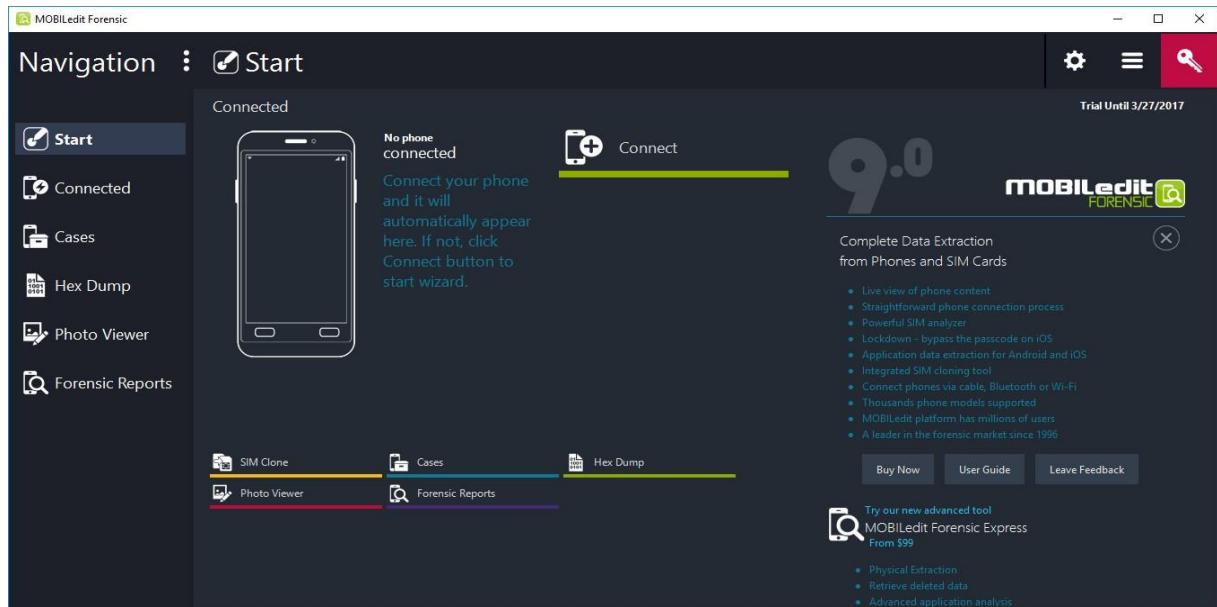
All Columns **DTZ**

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type	Added	Children	Descendants	Investigator's Name	Comment
Jim_shu's.pst	F:\sem4\ComputerForensics	Jim_shu's	XYZ	Individual File	4/5/2017 10:13:46 PM	7	39	XYZ	
precious.img	F:\sem4\ComputerForensics	precious\Unpart...	XYZ	Unpartitioned Space	3/17/2017 10:36:59 ...	2	2	XYZ	
precious.img	F:\sem4\ComputerForensics	precious\Part_1...	XYZ	NTFS	3/17/2017 10:19:07 ...	2782	3788	XYZ	

3 Listed 0 Checked Total F:\sem4\ComputerForensics\Jim_shu's.pst



USING MOBILEDIT



MOBILedit Forensic Wizard

Enable USB debugging



1. Go to Developer options



2. Enable Developer options



3. Enable USB debugging

[Online guide](#)

< Back

Next >

Cancel

MOBILedit Forensic Wizard

Connect your phone now



If asked don't choose Charging Only mode. See connected phones below.

Model	Manufacturer	Port
ASUS_T00J1	asus	Android 136C5119

If the phone is already listed, do not wait for detection to complete.
Select the phone and press Finish.

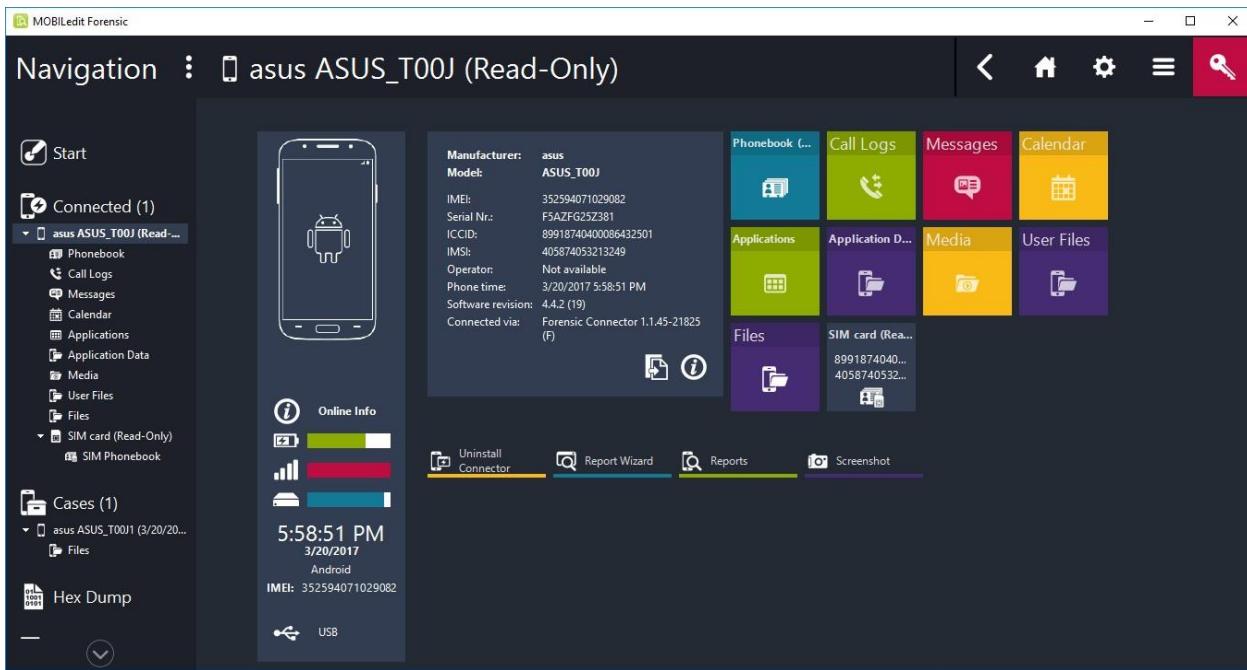
Refresh

[Online guide](#)

< Back

Finish

Cancel



The screenshot shows the MOBILedit Forensic software interface with the title 'Navigation : Files - asus ASUS_T00J'. The left sidebar shows navigation options. The main area is a file browser displaying the contents of the device's internal storage. The left pane shows a tree view of directories: /, /acct, /ADF, /APD, /cache, /config, /data, /dev, /factory, /lib, /media, /mnt, /proc, /res, /root, /sbin, /storage, /sys, /system, /temp_data, /usr, and /charger. The right pane shows a detailed list of files with columns for File Name, Size, Created, and Modified. A 'Reread' button is located at the top right of the file list area.

File Name	Size	Created	Modified
<folder>	<unknown>	3/20/2017 2:	
acct	<folder>	<unknown>	10/16/2013 1:
ADF	<folder>	<unknown>	10/16/2013 1:
APD	<folder>	<unknown>	1/1/1970 5:3
cache	<folder>	<unknown>	3/20/2017 9:
config	<folder>	<unknown>	10/16/2013 1:
data	<folder>	<unknown>	3/20/2017 2:
dev	<folder>	<unknown>	3/20/2017 8:
factory	<folder>	<unknown>	10/16/2013 1:
lib	<folder>	<unknown>	1/1/1970 5:3
media	<folder>	<unknown>	3/20/2017 2:
mnt	<folder>	<unknown>	3/20/2017 2:
proc	<folder>	<unknown>	3/20/2017 2:
res	<folder>	<unknown>	1/1/1970 5:3
root	<folder>	<unknown>	1/16/2015 11:
sbin	<folder>	<unknown>	1/1/1970 5:3
storage	<folder>	<unknown>	3/20/2017 2:
sys	<folder>	<unknown>	3/20/2017 2:
system	<folder>	<unknown>	8/12/2015 8:
temp_data	<folder>	<unknown>	3/20/2017 2:
usr	<folder>	<unknown>	1/1/1970 5:3
charger	1003.20 KB	<unknown>	1/1/1970 12:
d	<unknown>	<unknown>	3/20/2017 8:
default.prop	435 B	<unknown>	1/1/1970 12:
etc	<unknown>	<unknown>	8/12/2015 3:
file_contexts	8.95 KB	<unknown>	1/1/1970 12:
fstab.charger.redhookbay	274 B	<unknown>	1/1/1970 12:
fstab.ramconsole.redhookbay	274 B	<unknown>	1/1/1970 12:
fstab.redhookbay	1.24 KB	<unknown>	1/1/1970 12:
init	483.77 KB	<unknown>	1/1/1970 12:
init.asusreset.rc	132 B	<unknown>	1/1/1970 12:

MOBILedit Forensic Wizard

Data acquire settings

Please set the following options for data acquiring.
Data will be stored in the "Cases" folder.

Device Label: Device Evidence Number:
Device Name: Owner Name:
Owner Phone Number:
Phone Notes:

Device Capabilities
 Files

Communication Log Of Backup Operation
 Create:

MOBILedit Forensic Wizard

File system acquiring

Choose the part of filesystem to acquire.

Whole file system
 Specified file types:
 Audio Video Pictures
 Selected files & folders
 Phones
 asus ASUS_T00J1

MOBILedit Forensic

Navigation : Files - asus ASUS_T00J1 (3/20/2017 12:19:03 PM)

Start

Connected (1)

- asus ASUS_T00J (Read-Only)
 - Phonebook
 - Call Logs
 - Messages
 - Calendar
 - Applications
 - Application Data
 - Media
 - User Files
 - Files
- SIM card (Read-Only)
 - SIM Phonebook

Cases (1)

- asus ASUS_T00J1 (3/20/2017 12:19:03 PM)
 - Files

Hex Dump

Navigation

File Name

File Name	Size	Created	Modified
ADF	<unknown>	<unknown>	<unknown>
APD	<unknown>	<unknown>	<unknown>
factory	<unknown>	<unknown>	<unknown>
media	<unknown>	<unknown>	<unknown>
storage	<unknown>	<unknown>	<unknown>
temp_data	<unknown>	<unknown>	<unknown>

MOBILedit Forensic

Navigation : Photo Viewer

Connected (1)

- asus ASUS_T00J (Read-Only)
 - Phonebook
 - Call Logs
 - Messages
 - Calendar
 - Applications
 - Application Data
 - Media
 - User Files
 - Files
- SIM card (Read-Only)
 - SIM Phonebook

Cases (1)

- asus ASUS_T00J1 (3/20/2017 12:19:03 PM)
 - Files

Photo Preview



Photo Info

Width: 263
Height: 192
Size: 19.37 KB

Show Photo Preview

from harddrive
 from phone

Show Preview

Open

C:\Users\ZainFa\Desktop\images.jpg

Navigation : Hex Dump

Connected (1)

- asus ASUS_T00J (Read-Only)
 - Phonebook
 - Call Logs
 - Messages
 - Calendar
 - Applications
 - Application Data
 - Media
 - User Files
 - Files
- SIM card (Read-Only)
- SIM Phonebook

Cases (1)

- asus ASUS_T00J1 (3/20/20...)
- Files

Hex Dump

Photo Viewer

Physical Analysis...

Hex Dump

Address	Value
00000000	FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60
00000010	00 60 00 00 FF E1 00 22 45 78 69 66 00 00 4D 4D
00000020	00 2A 00 00 00 08 00 01 01 12 00 03 00 00 00 01
00000030	00 01 00 00 00 00 00 00 FF DB 00 43 00 02 01 01
00000040	02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03
00000050	03 03 06 04 04 03 05 07 06 07 07 05 07 07 08
00000060	09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C
00000070	0C 0C 07 09 0E 0F 0D 0C 0B 0B 0C 0C FF DB 00
00000080	43 01 02 02 02 03 03 03 06 03 03 06 0C 08 07 08
00000090	0C
000000A0	0C
000000B0	0C
000000C0	0C 0C FF C0 00 11 08 00 C0 01 07 03 01 22 00 02
000000D0	11 01 03 11 01 FF C4 00 1F 00 00 01 02 01 01 01
000000E0	01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05
000000F0	06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03
00000100	02 04 03 05 04 04 04 00 00 01 7D 01 02 03 00 04
00000110	11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81
00000120	91 A1 08 23 42 B1 C1 15 52 D1 F0 24 33 62 72 82
00000130	09 0A 16 17 18 19 1A 25 26 27 28 29 2A 34 35 36
00000140	37 38 39 3A 43 44 45 46 47 48 49 4A 53 54 55 56
00000150	57 58 59 5A 63 64 65 66 67 68 69 6A 73 74 75 76
00000160	77 78 79 7A 83 84 85 86 87 88 89 8A 92 93 94 95
00000170	96 97 98 99 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3
00000180	B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA
00000190	D2 D3 D4 D5 D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7
000001A0	E8 E9 EA F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00
000001B0	1F 01 00 03 01 01 01 01 01 01 01 01 01 00 00 00
000001C0	00 00 00 01 02 03 04 05 06 07 08 09 0A 0B FF C4
000001D0	00 B5 11 00 02 01 02 04 04 03 04 07 05 04 04 00
000001E0	01 02 77 00 01 02 03 11 04 05 21 31 06 12 41 51
000001F0	07 61 71 13 22 32 81 08 14 42 91 A1 B1 C1 09 23
00000200	33 52 F0 15 62 72 D1 0A 16 24 34 E1 25 F1 17 18

Navigation : Forensic Reports

Call Logs

Messages

Calendar

Applications

Application Data

Media

User Files

Files

SIM card (Read-Only)

SIM Phonebook

Cases (1)

- asus ASUS_T00J1 (3/20/20...)
- Files

Hex Dump

Photo Viewer (1)

- images.jpg

Forensic Reports

Forensic Reports

Select data source you want to generate report from.

Click on the report template.

Templates contains full information of the design of the resulting report and what data from data source to include.

Your report will be generated.

Data Sources

- External Sources (1)
 - Open XML file...
- Devices (2)
 - SIM card
 - asus ASUS T00J
- Cases (1)
 - asus ASUS_T00J1 (3/20/2017 12:19:0...

Report Templates

- XML-HTML Report
- XML for Search Tool
- XML for I2
- XML for I2 (with Connections)
- Excel
- RTF in English

Advanced PDF and HTML reports available via Phone Forensics Express

How to customize a template

