INDEX

Sr.no	Topic	Sign
1	Analyze hard drive or smartphones using forensic tool or File System Analysis Using the Slueth Kit.	

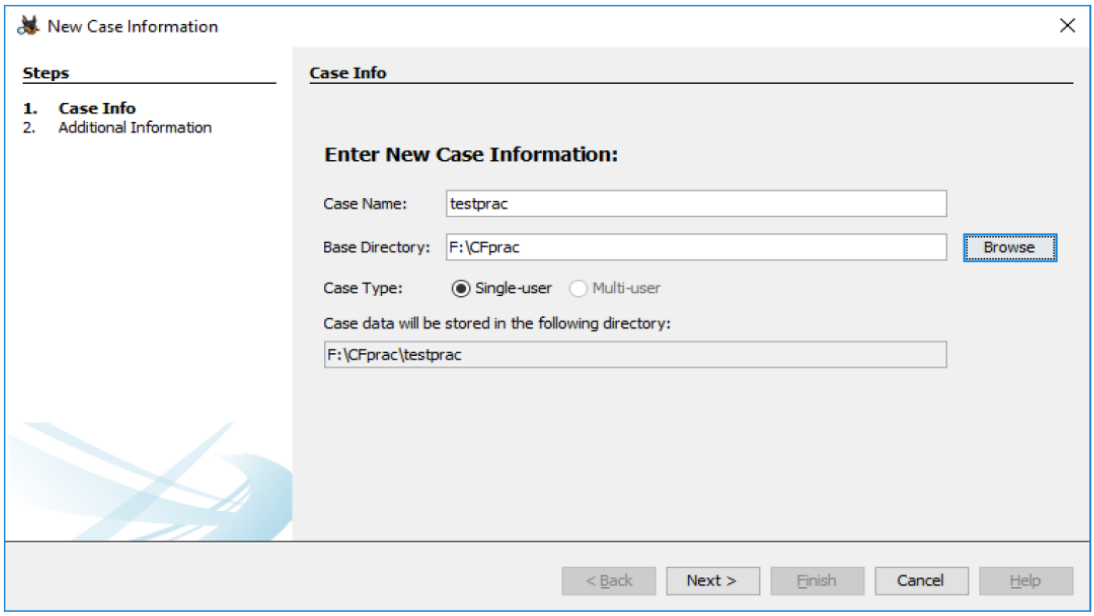
2	Analyze DNS using WHOIS Tool. Detect OS, Host name using cmd. Detect session and ports through packet sniffing. (Nmap) & command line utilities.	
3	Capture the physical memory of a computer and analyze artefacts in memory. (FTK)	
4	Calculate MD5 & SHA1 (CrypTool)	
5	Use tool to collect, preserve digital 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	

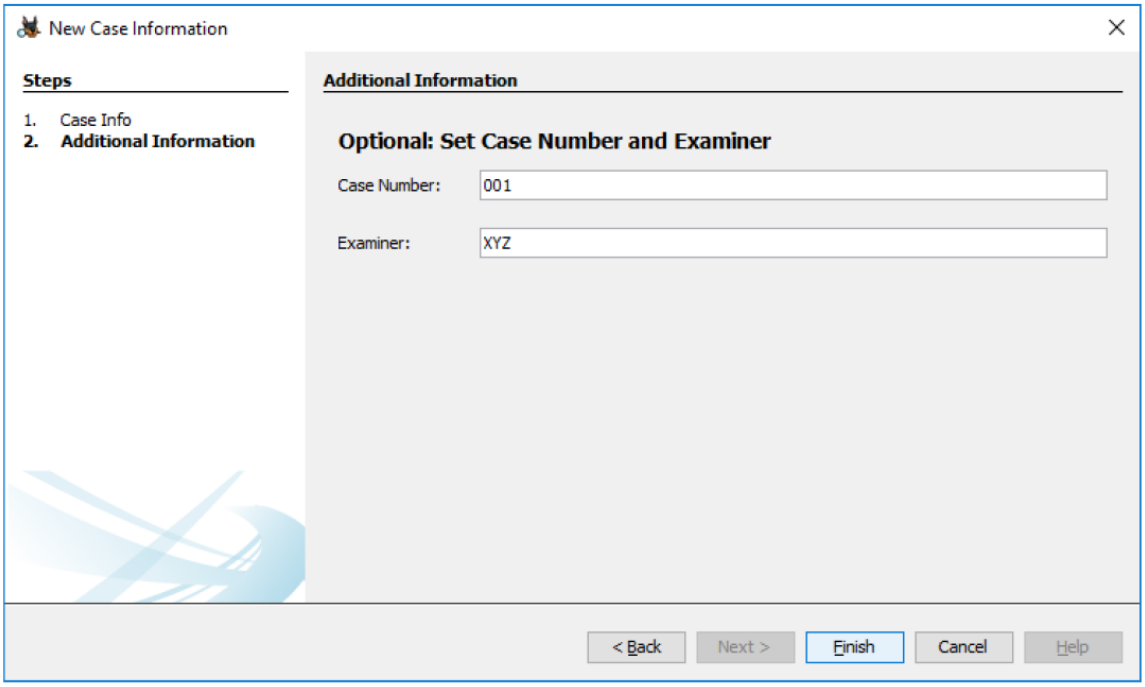
PRACTICAL NO 01: Analyse hard drives or smart phones using forensic tools

(Using Autopsy Tool)

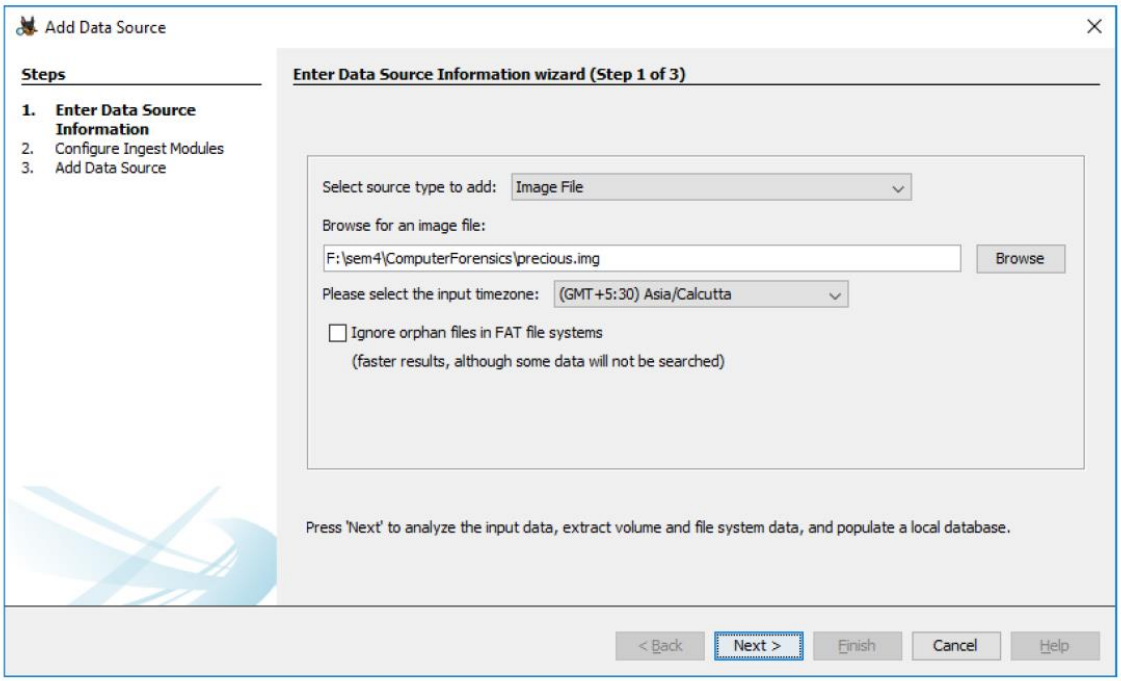
Step 1: Download Autopsy

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

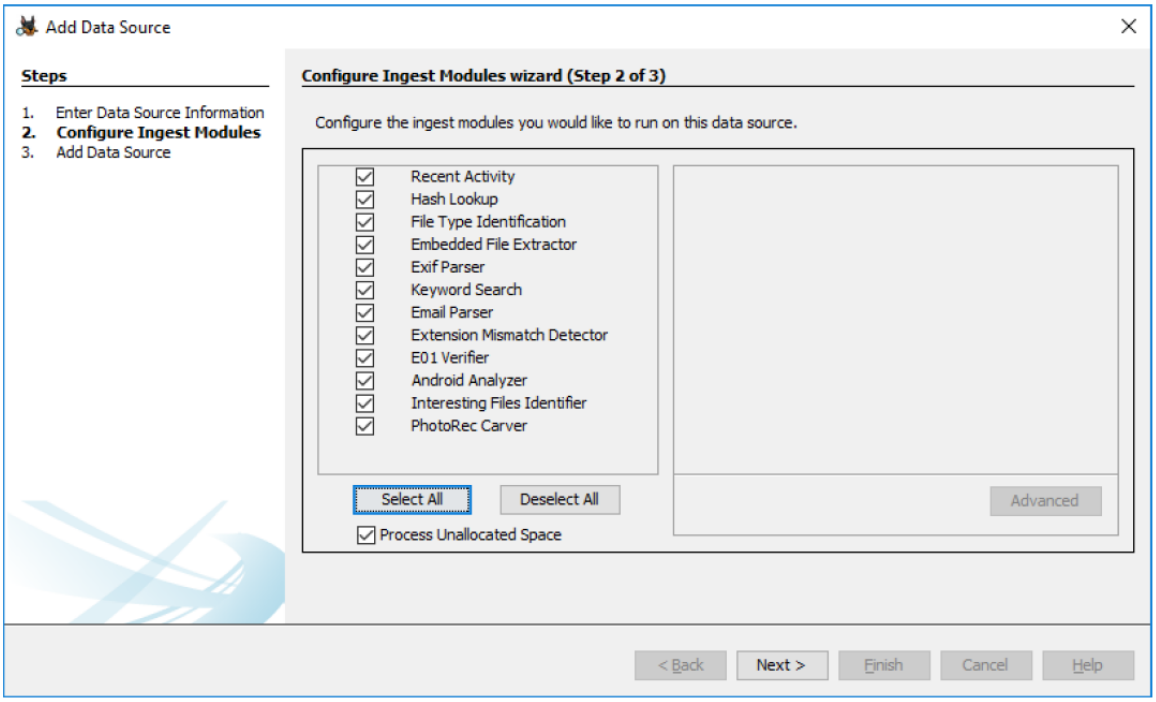




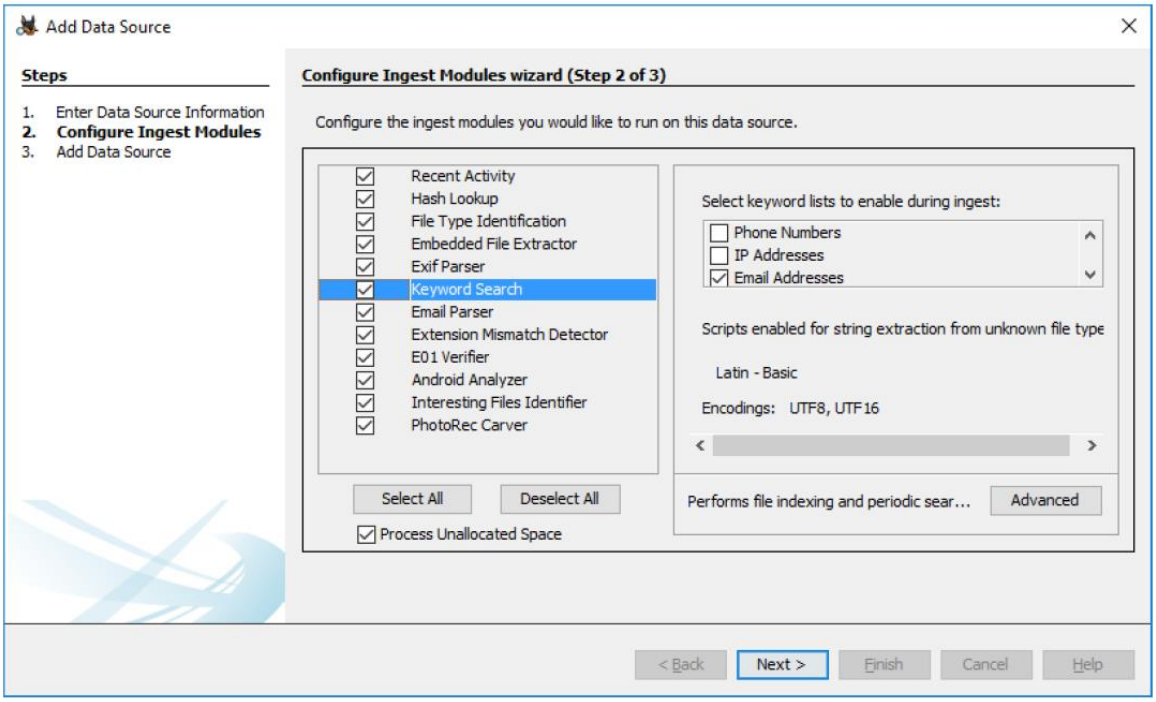
Step 3: Add any file on which you want to investigate



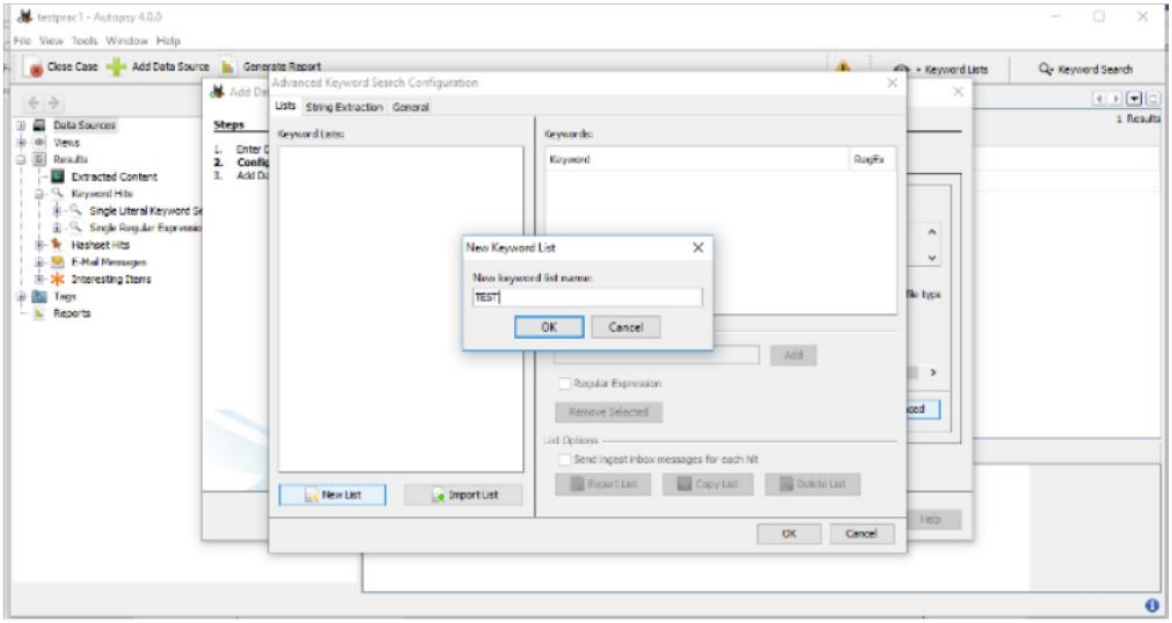
Step 4: Configure ingest module



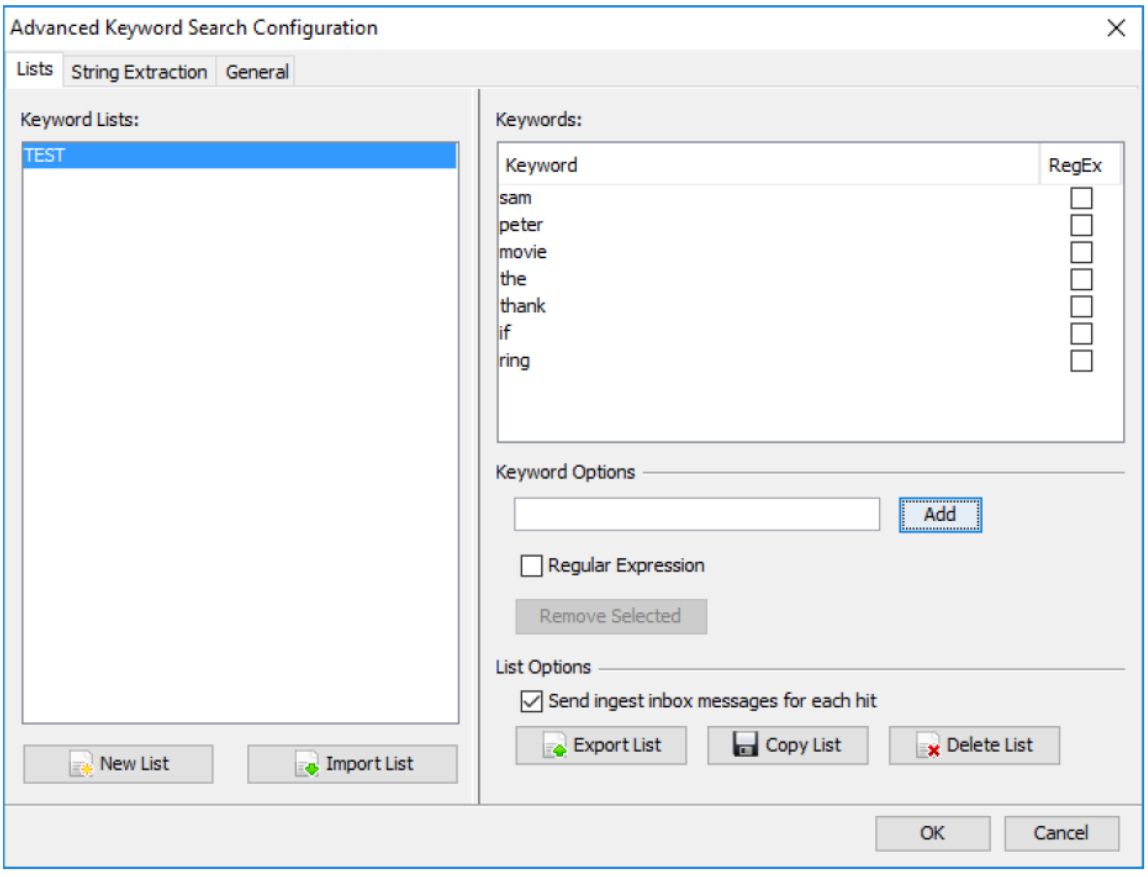
Step 5: click on keyword search



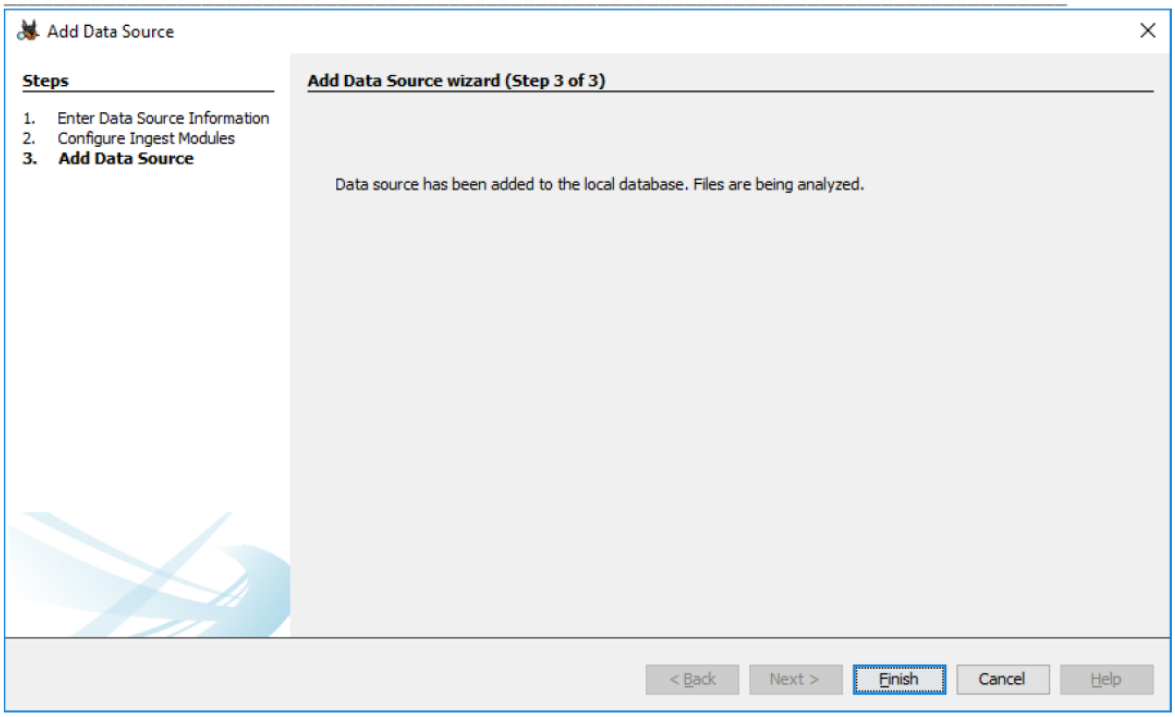
Step 6: then click on advance & add the following or your own required keywords



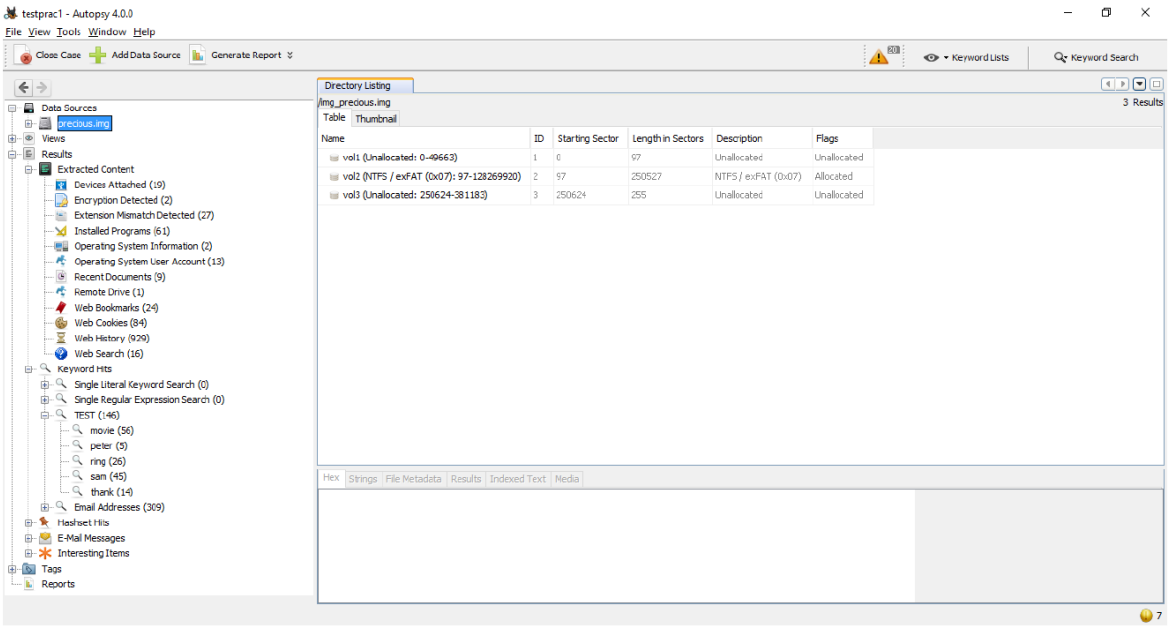
Step 7: you can click on add & add the following keywords



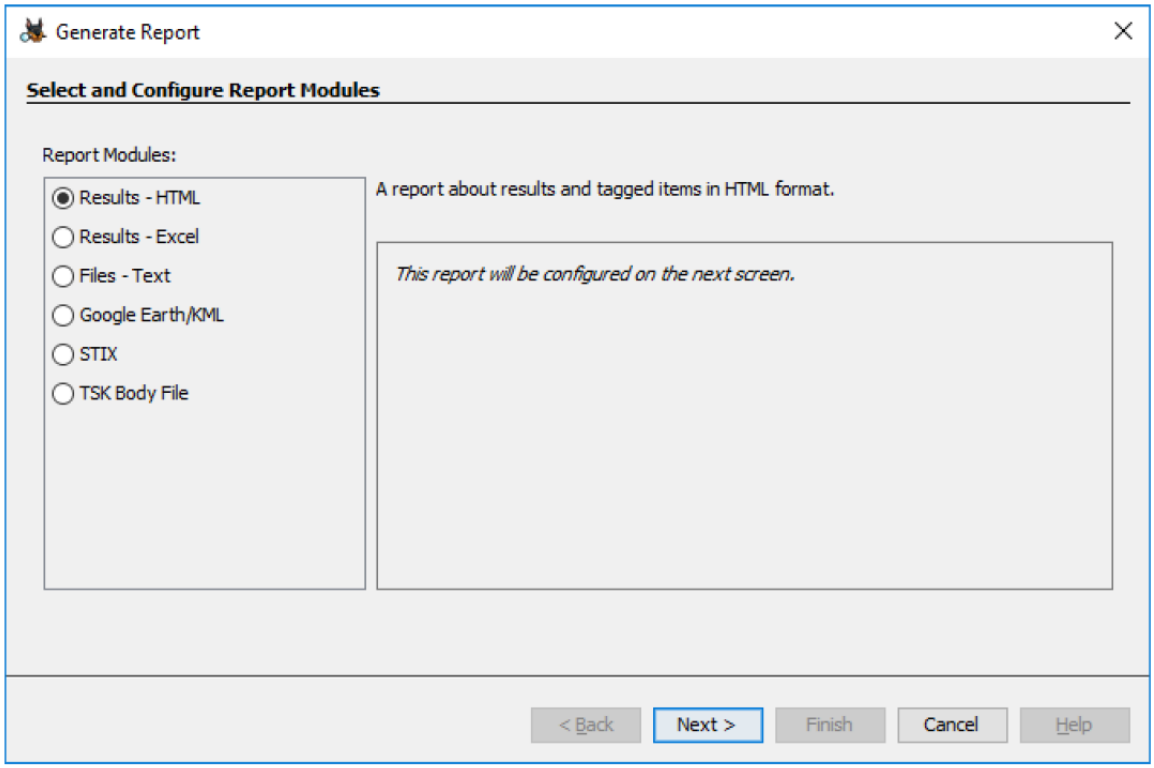
Step 8: Click on finish

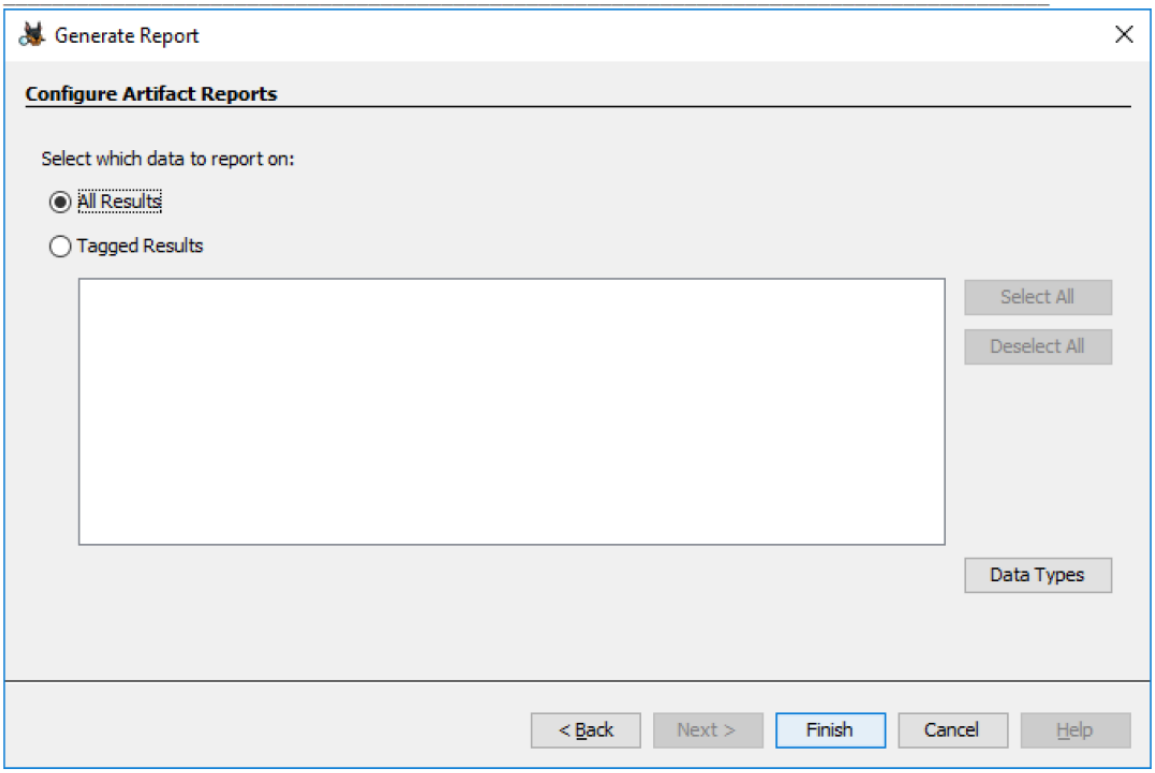


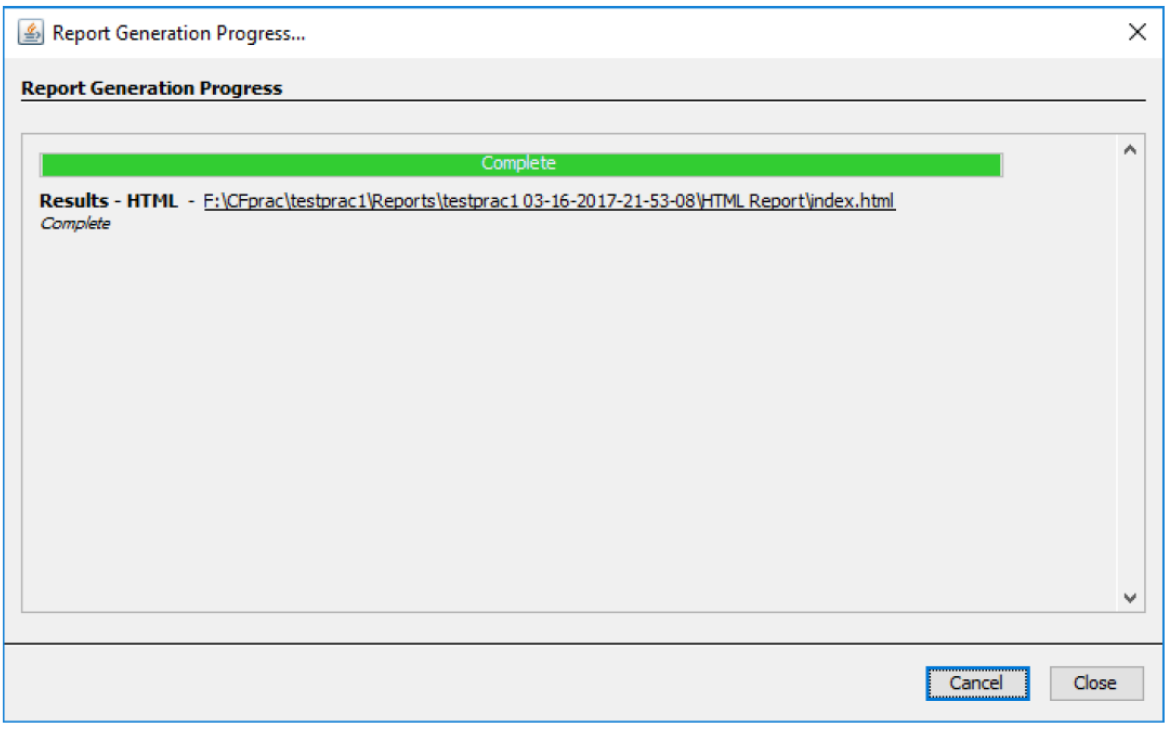
Step 9: Check the data

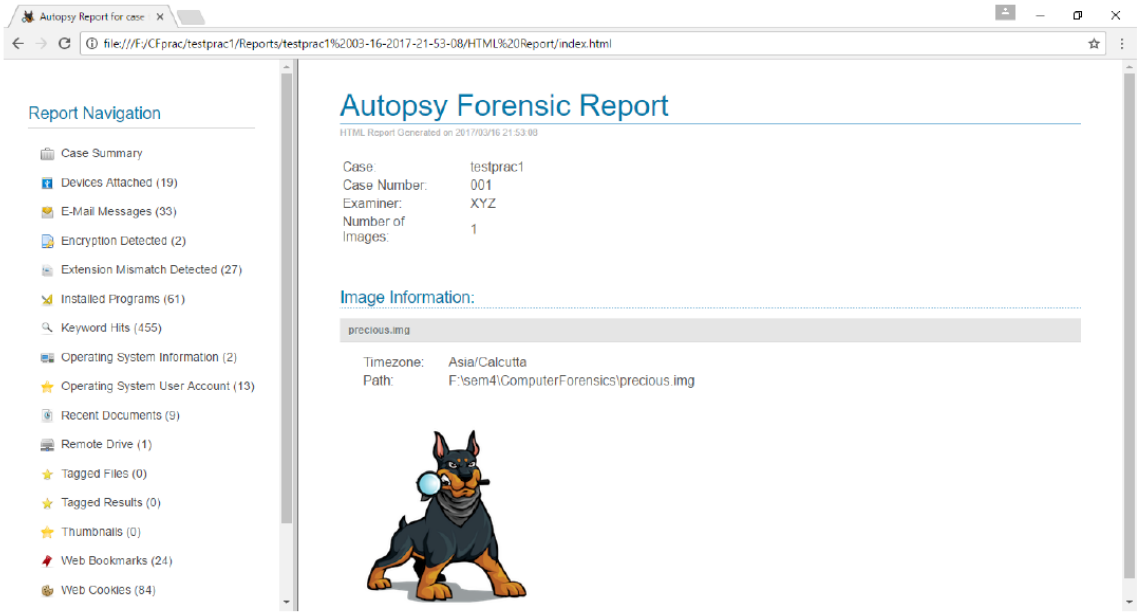


Step 10: Generate a report




Generate Report
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...
Report Generation Progress
Complete
Results - HTML - F:\CFprac\testprac1\Reports\testprac1 03-16-2017-21-53-08\HTML Report\index.html
Complete
Cancel
Close


Autopsy Report for case
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    127.0.0.1:56010        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        DESKTOP-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   dhcp-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    [::1]: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    [::1]:1900             *:*                                    6540
  UDP    [::1]: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 . . . . . . . . . :
```

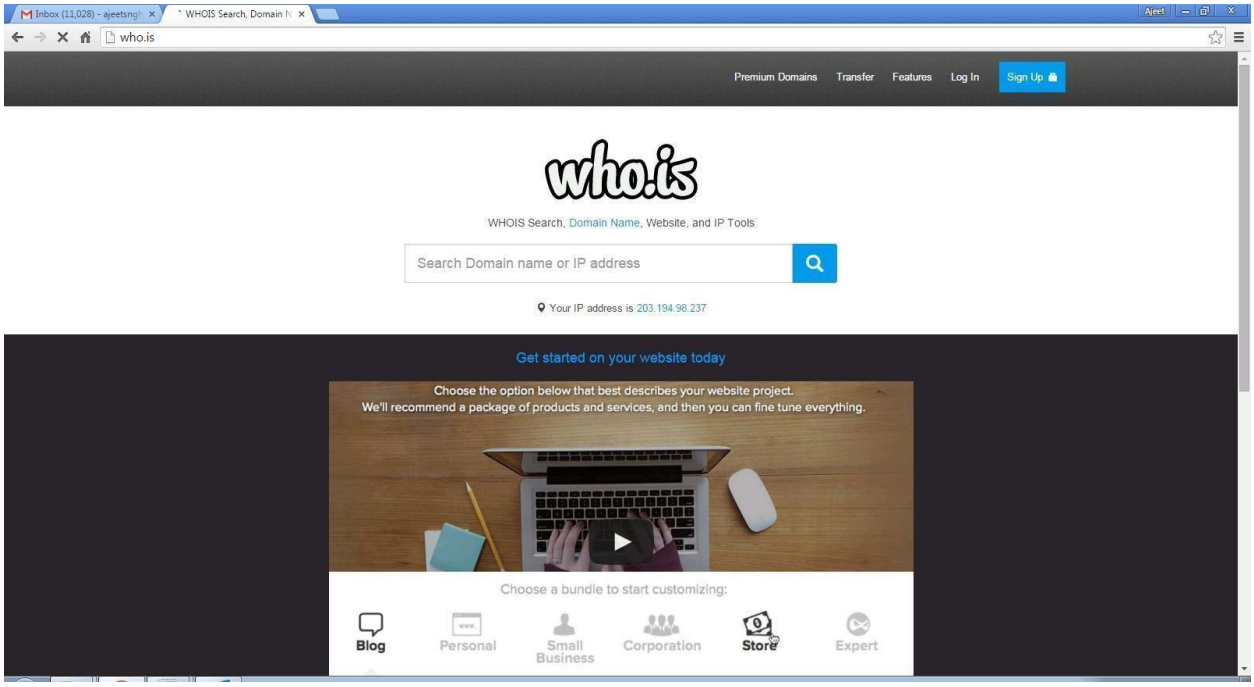
```
C:\Users\sies>nmap -sA -T4 scanme.sies.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 16:44 India Standard Time
Nmap scan report for scanme.sies.org (69.64.147.244)
Host is up (0.00053s latency).
rDNS record for 69.64.147.244: ash.parking.local
All 1000 scanned ports on scanme.sies.org (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
```

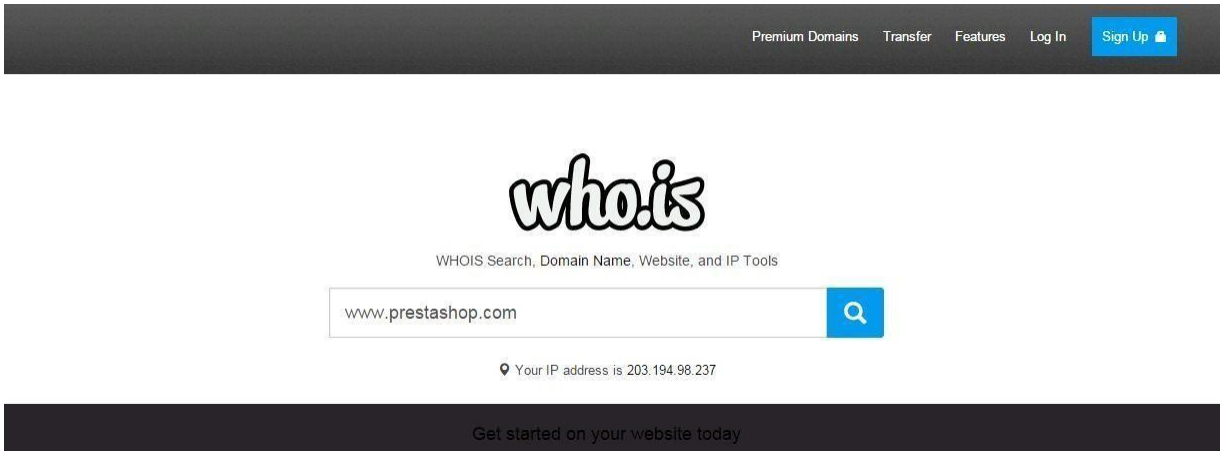
```
C:\Users\sies>nmap -p23,113,139 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 16:59 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.082s latency).

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:
```

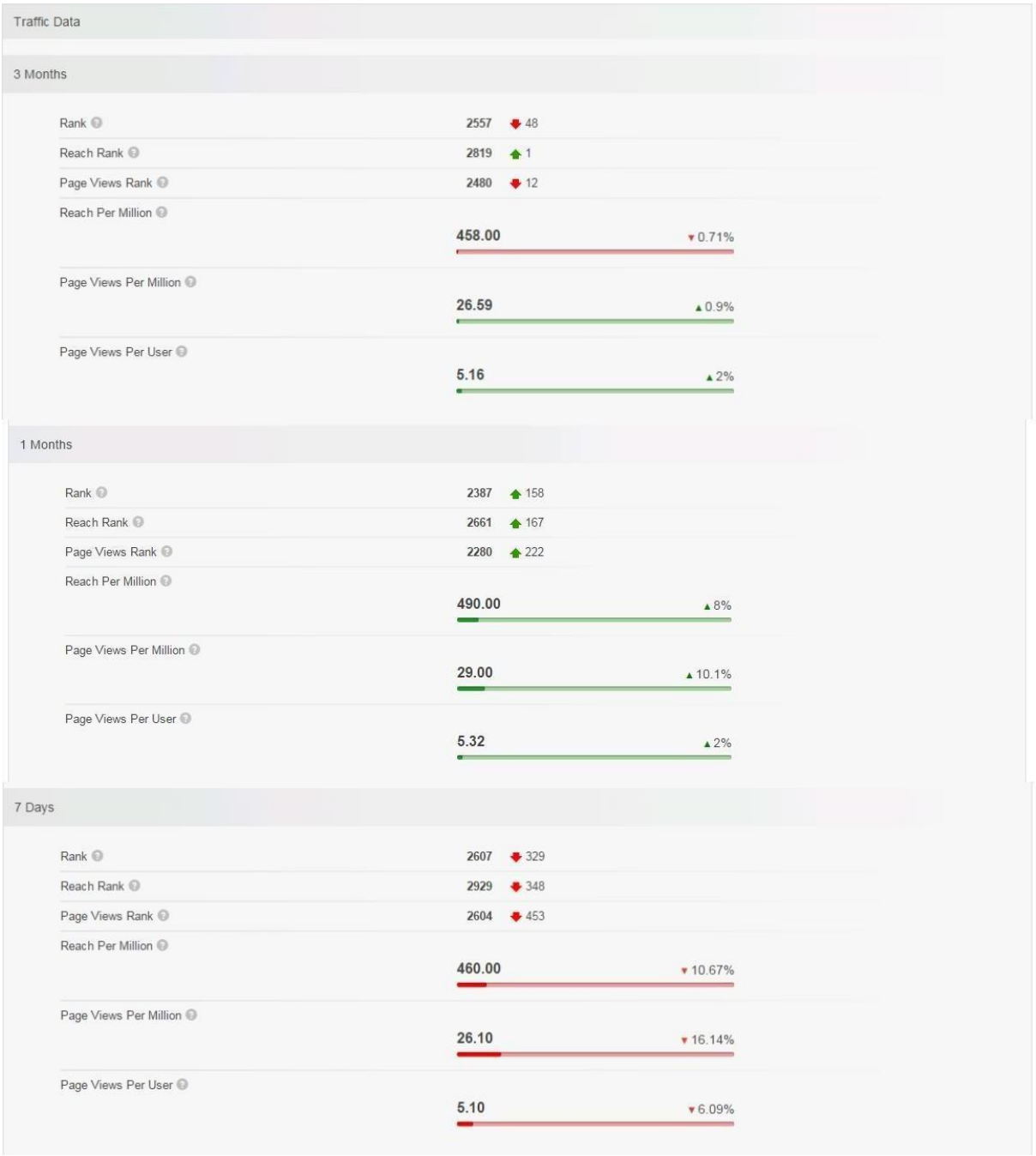
Overview for **prestashop.com**: Whois | Website Info | History | DNS Records | Diagnostics — Updated 10 hours ago

Contact Information

Owner Name	PrestaShop SA
Email	**contact**@prestashop.com
Address	6, rue Lacépède PARIS, Ile 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


Traffic Data
3 Months
Rank 2557 48
Reach Rank 2819 1
Page Views Rank 2480 12
Reach Per Million
458.00 0.71%
Page Views Per Million
26.59 0.9%
Page Views Per User
5.16 2%
1 Months
Rank 2387 158
Reach Rank 2661 167
Page Views Rank 2280 222
Reach Per Million
490.00 8%
Page Views Per Million
29.00 10.1%
Page Views Per User
5.32 2%
7 Days
Rank 2607 329
Reach Rank 2929 348
Page Views Rank 2604 453
Reach Per Million
460.00 10.67%
Page Views Per Million
26.10 16.14%
Page Views Per User
5.10 6.09%

1 Days

Rank	2480	▲ 911
Reach Rank	2777	▲ 877
Page Views Rank	2444	▲ 1414
Reach Per Million	480.00	▲ 30%
Page Views Per Million	27.60	▲ 50%
Page Views Per User	5.20	▲ 20%

Subdomains

	Reach	Page Views	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addons.prestashop.com	43.62%	43.93%	5.36
doc.prestashop.com	14.01%	6.23%	2.36
demo.prestashop.com	4.00%	1.44%	1.9
forge.prestashop.com	3.31%	1.41%	2.3
build.prestashop.com	1.36%	0.34%	1.3
mail.prestashop.com	0.53%	0.21%	2.1
help.prestashop.com	0.72%	0.16%	1.2
validator.prestashop.com	0.20%	0.14%	3.7
sandrine.prestashop.com	0.07%	0.14%	11
scm.prestashop.com	0.31%	0.12%	2.0
OTHER		0.49%	

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

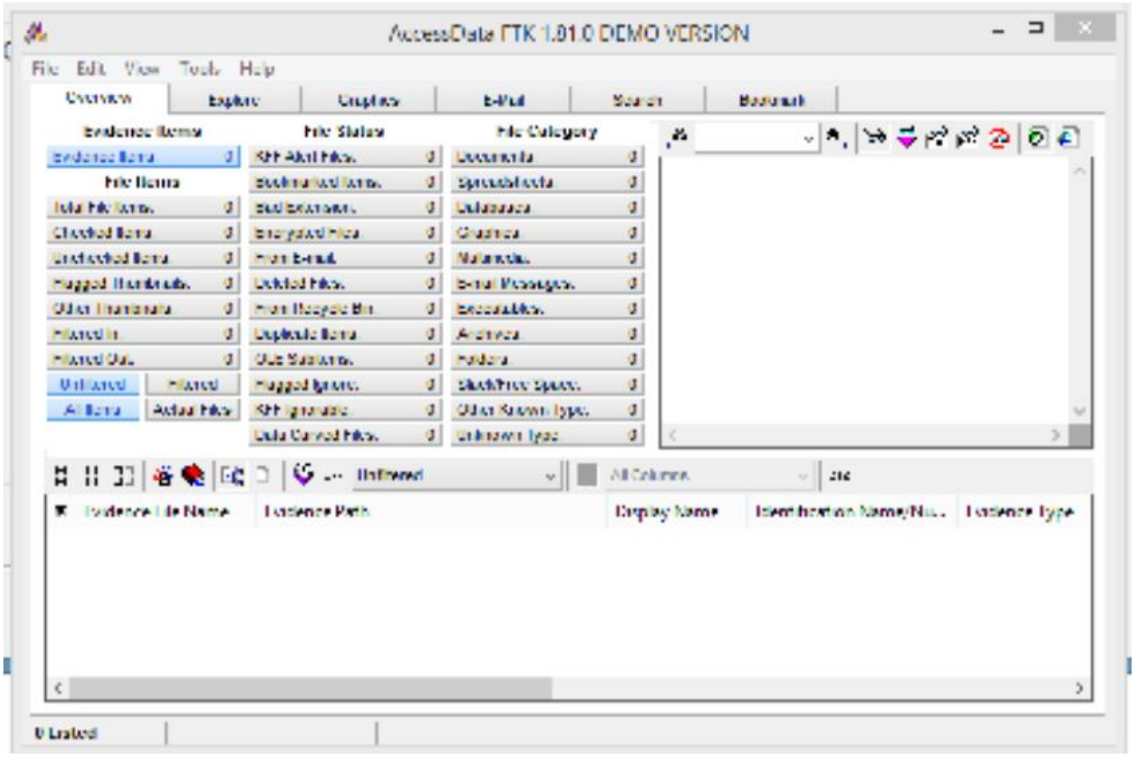
Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	V�lizy, A8, FR

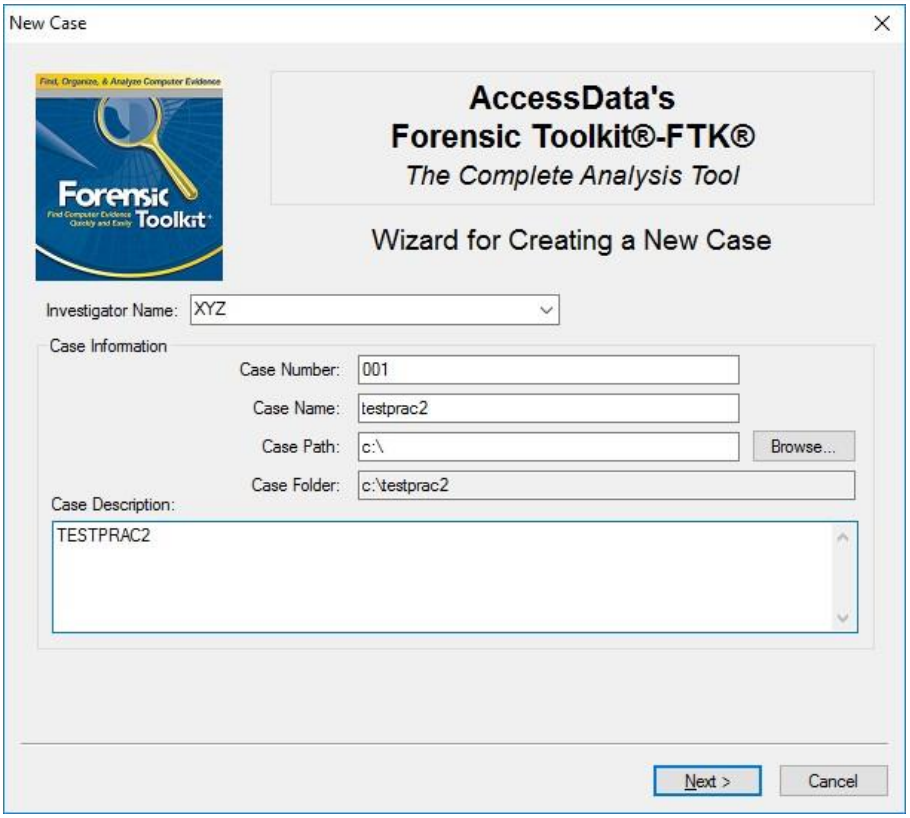
SOA Record – prestashop.com

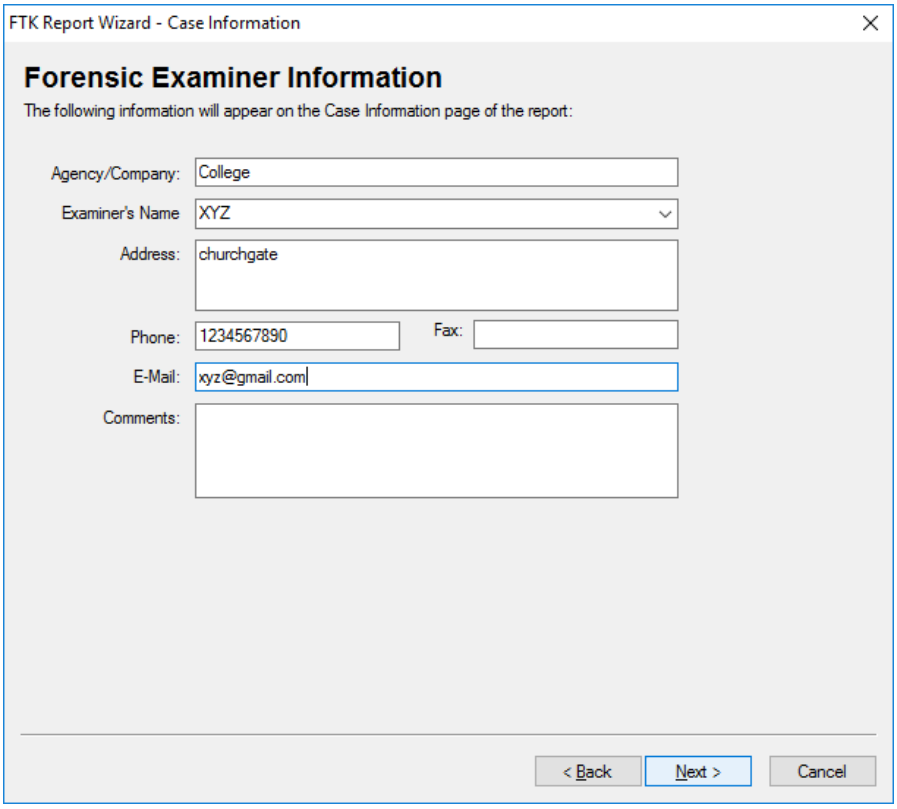
Name Server	master.ns.mailclub.fr
Email	**domaines**@mailclub.fr
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

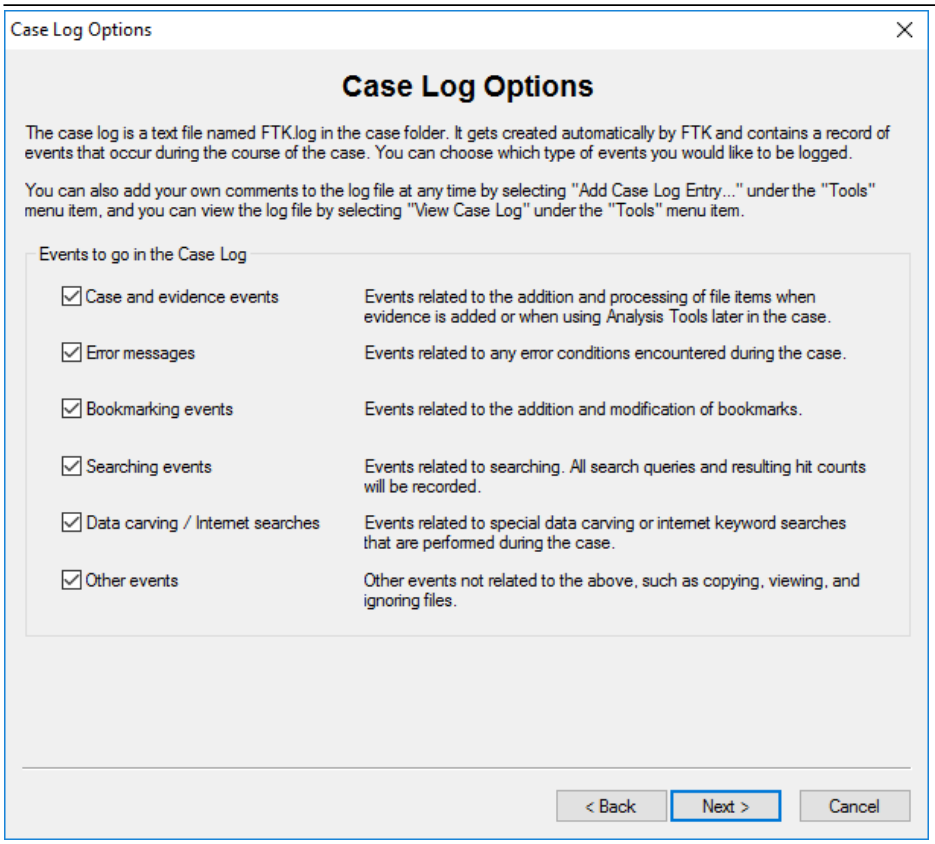
PRACTICAL NO 03: Capture the physical memory of a computer and analyse artifacts in memory.

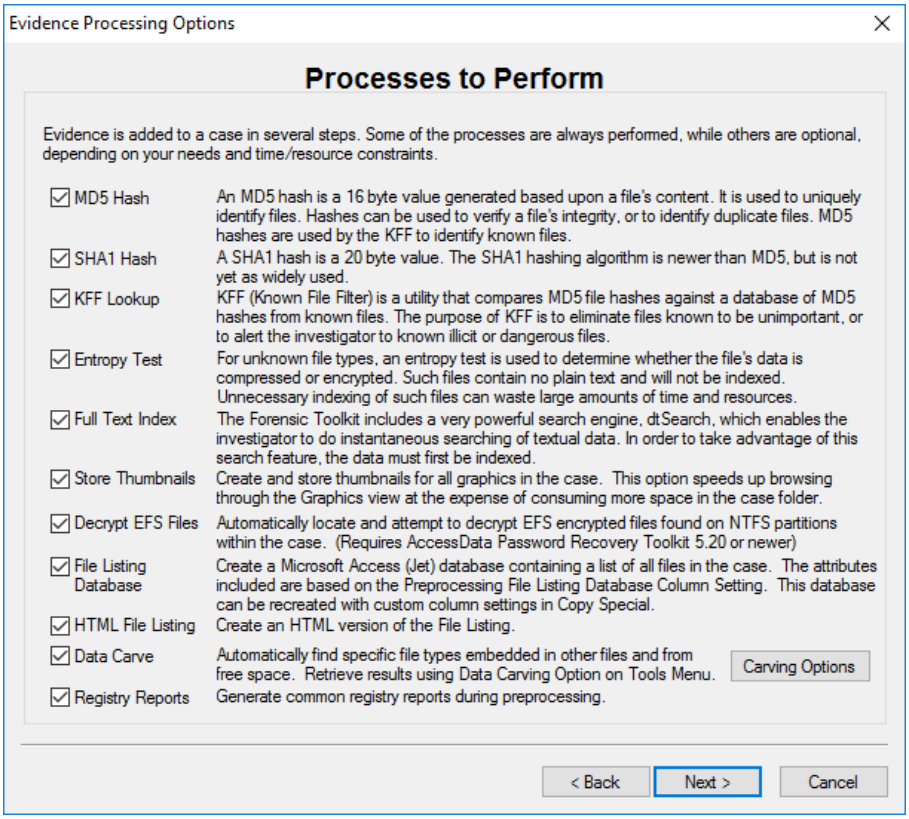
USING FTK

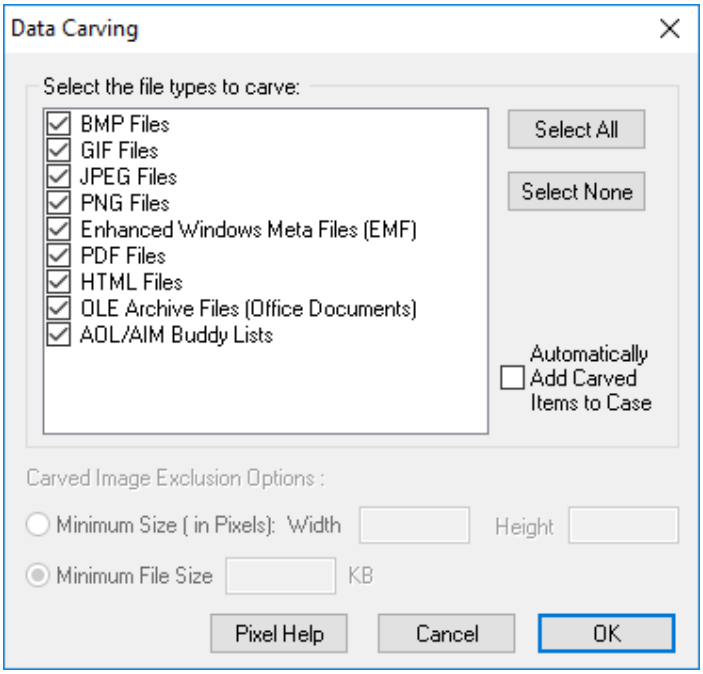


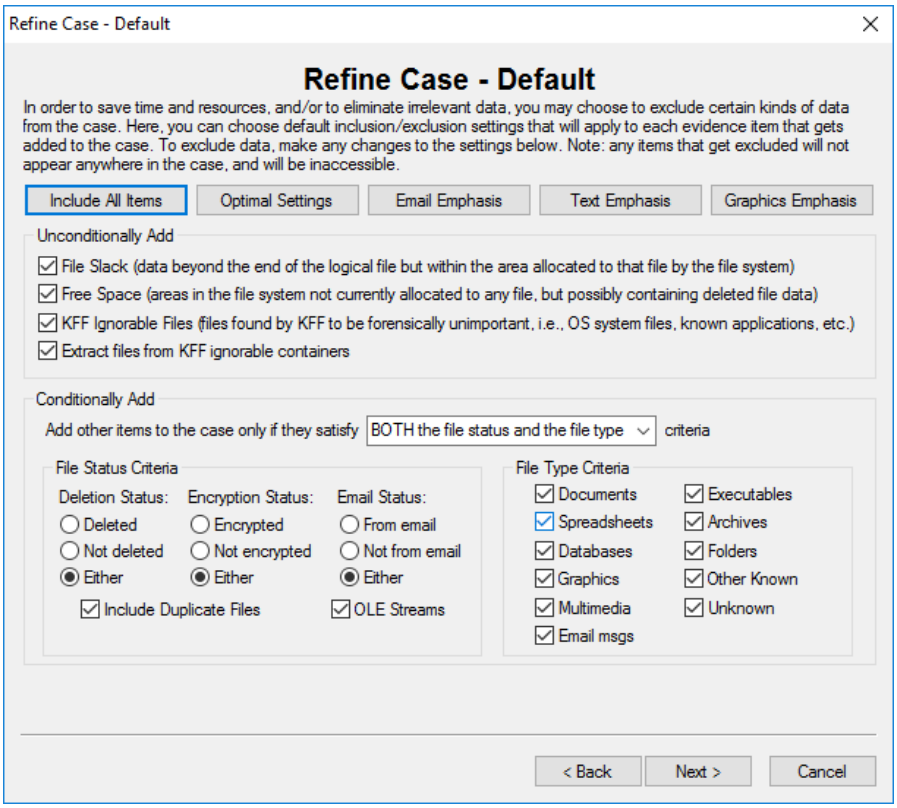

New Case
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Creating a New Case
Investigator Name: XYZ
Case Information
Case Number: 001
Case Name: testprac2
Case Path: c:\
Browse...
Case Folder: c:\testprac2
Case Description:
TESTPRAC2
Next >
Cancel

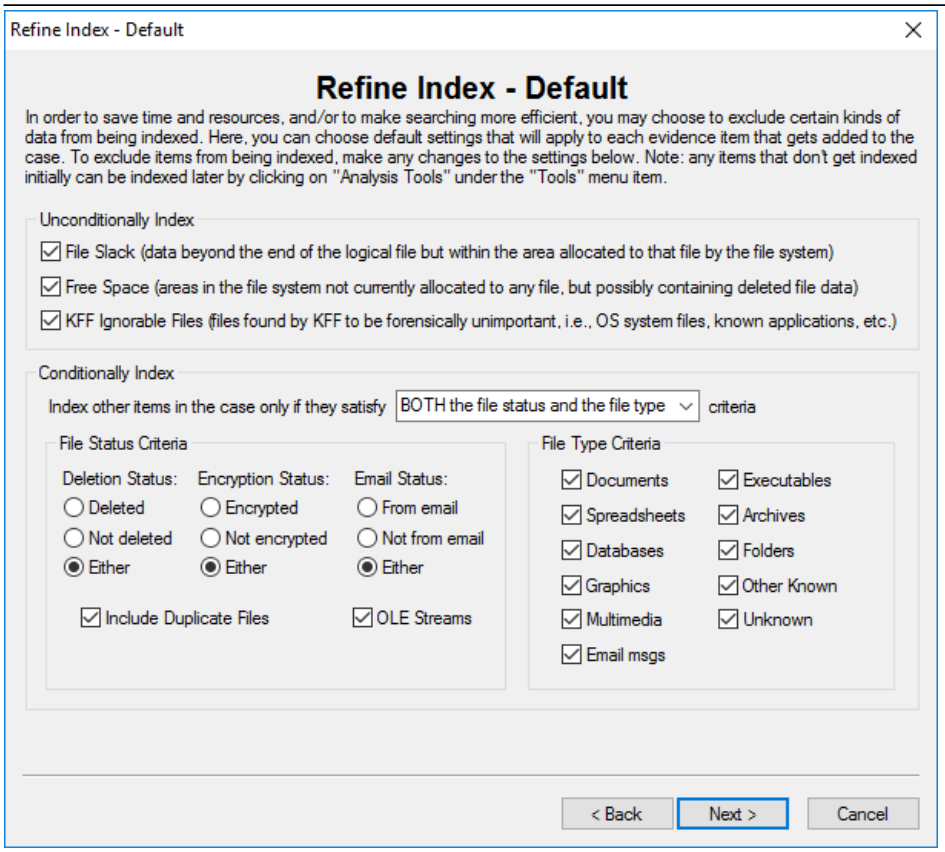

FTK Report Wizard - Case Information
Forensic Examiner Information
The following information will appear on the Case Information page of the report:
Agency/Company: College
Examiner's Name XYZ
Address: churchgate
Phone: 1234567890
Fax:
E-Mail: xyz@gmail.com
Comments:
< Back
Next >
Cancel

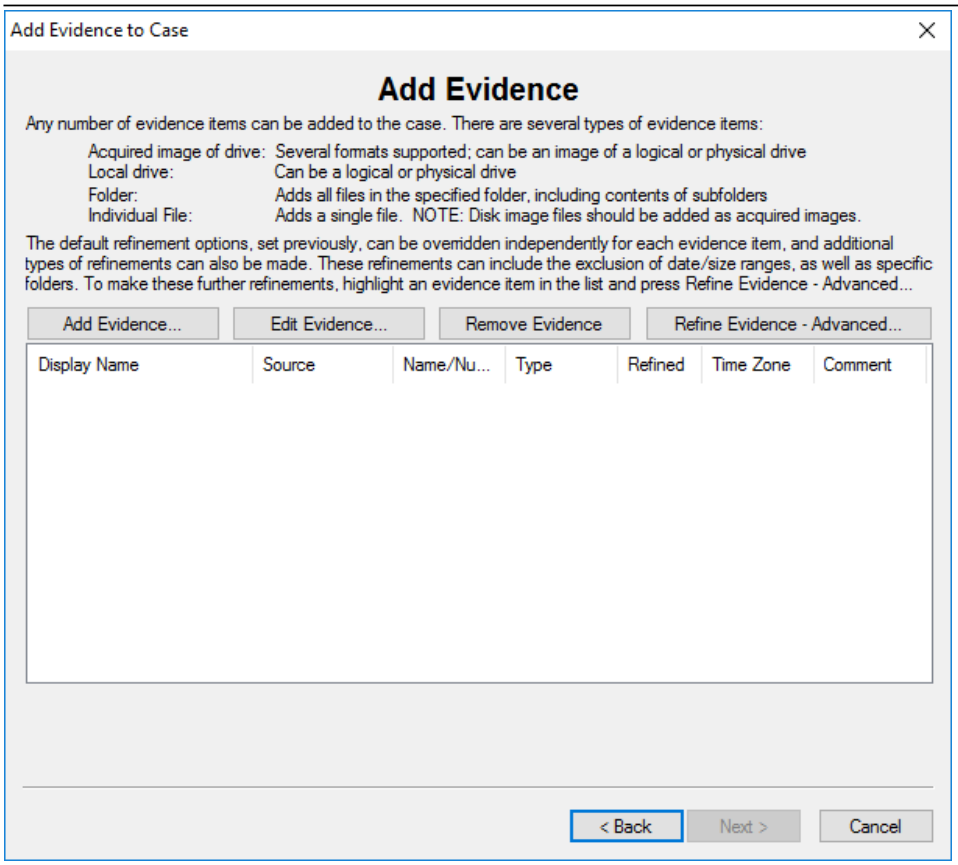

Case Log Options
Case Log Options
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.
Events to go in the Case Log
Case and evidence events
Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Error messages
Events related to any error conditions encountered during the case.
Bookmarking events
Events related to the addition and modification of bookmarks.
Searching events
Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches
Events related to special data carving or internet keyword searches that are performed during the case.
Other events
Other events not related to the above, such as copying, viewing, and ignoring files.
< Back
Next >
Cancel

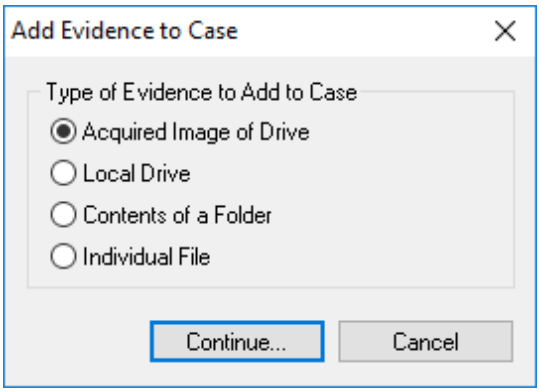

Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel

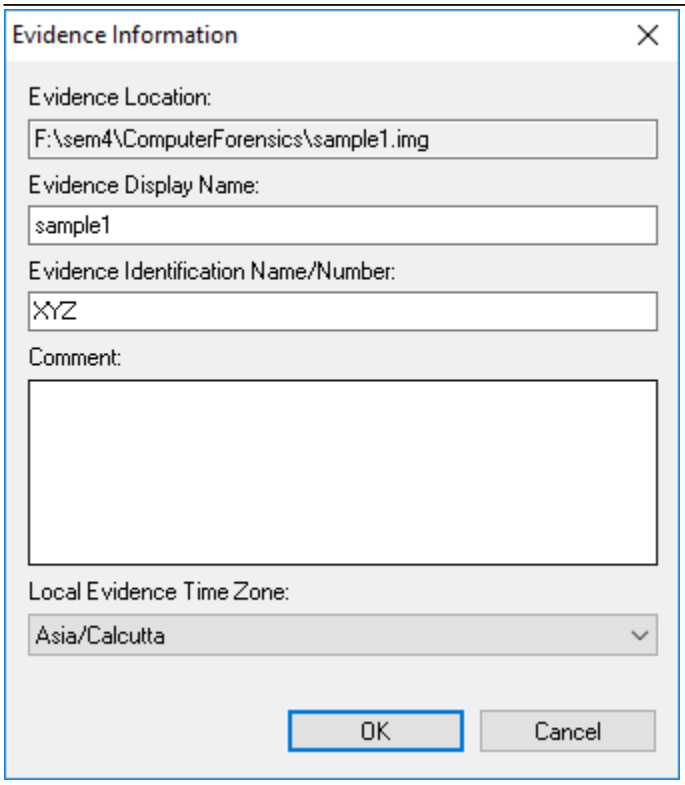

Data Carving
Select the file types to carve:
BMP Files
GIF Files
JPEG Files
PNG Files
Enhanced Windows Meta Files (EMF)
PDF Files
HTML Files
OLE Archive Files (Office Documents)
AOL/AIM Buddy Lists
Select All
Select None
Automatically Add Carved Items to Case
Carved Image Exclusion Options :
Minimum Size (in Pixels): Width
Height
Minimum File Size
KB
Pixel Help
Cancel
OK

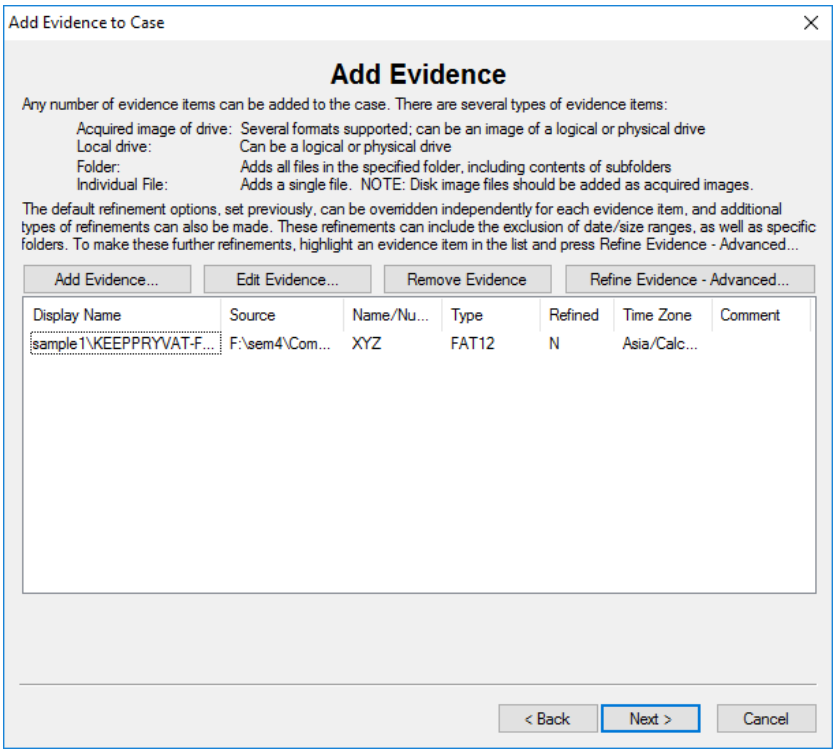

Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy
BOTH the file status and the file type
criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel

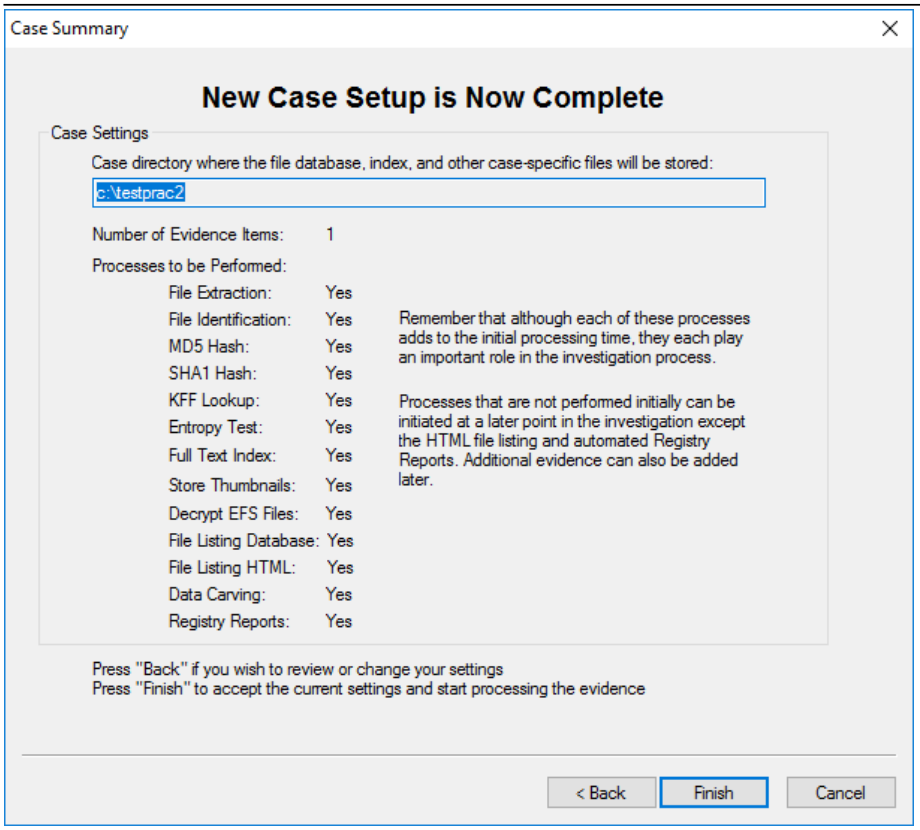

Refine Index - Default
Refine Index - Default
In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude 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
Deletion Status: Deleted Not deleted Either
Encryption Status: Encrypted Not encrypted Either
Email Status: From email Not from email Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Executables
Spreadsheets
Archives
Databases
Folders
Graphics
Other Known
Multimedia
Unknown
Email msgs
< Back
Next >
Cancel

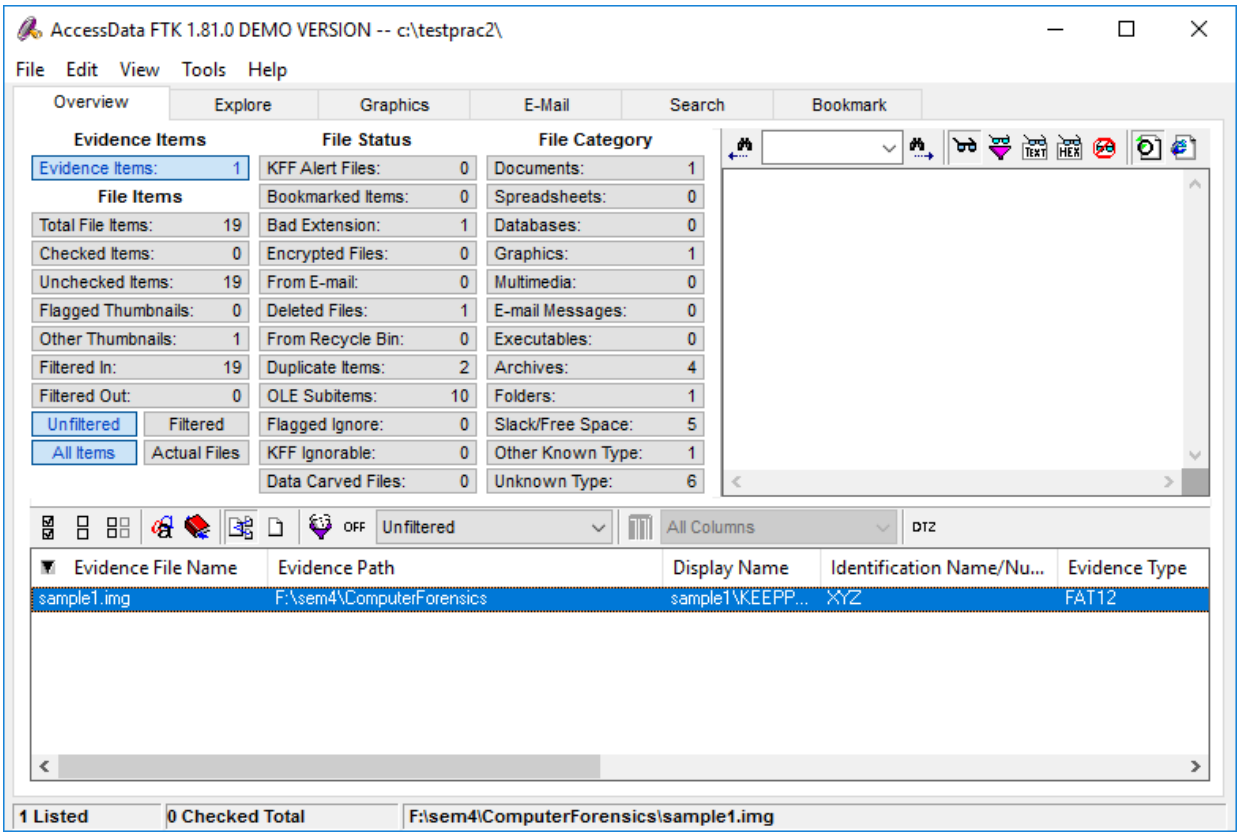

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files 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

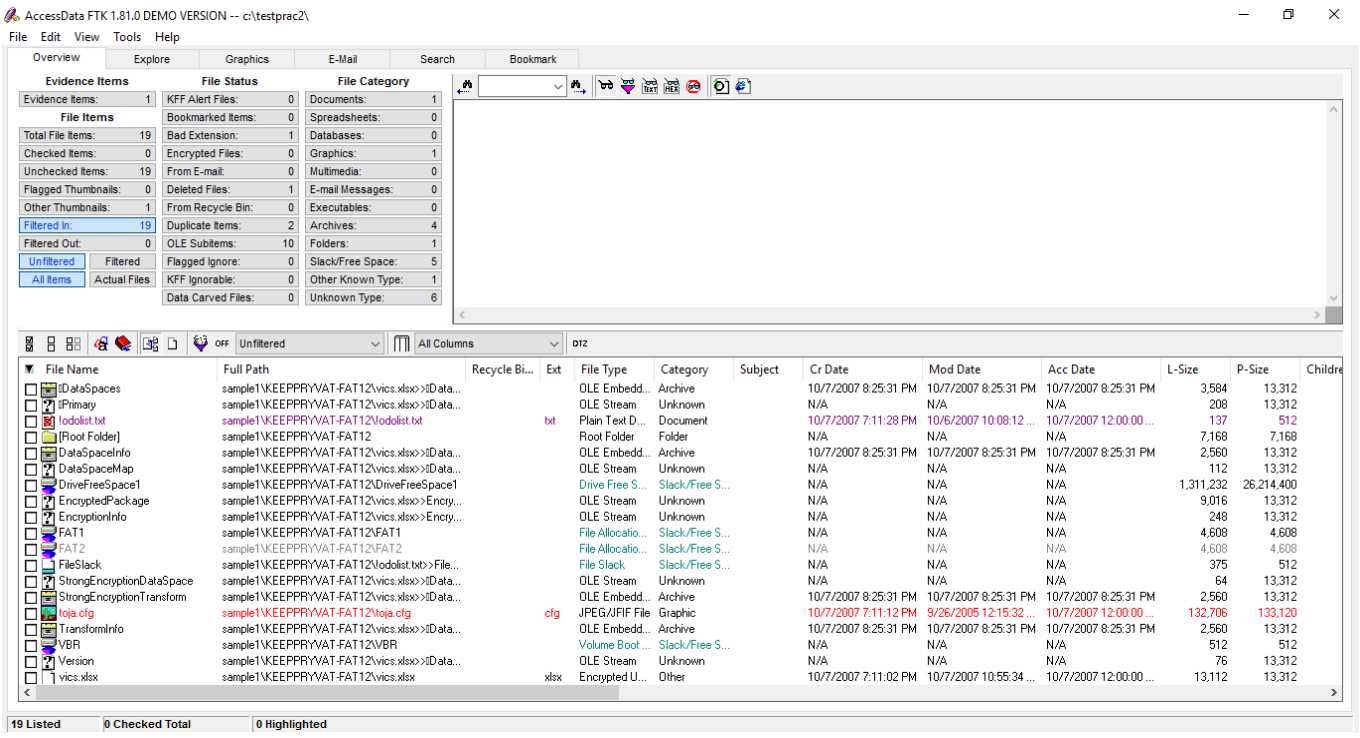

Add Evidence to Case
Type of Evidence to Add to Case
Acquired Image of Drive
Local Drive
Contents of a Folder
Individual File
Continue...
Cancel

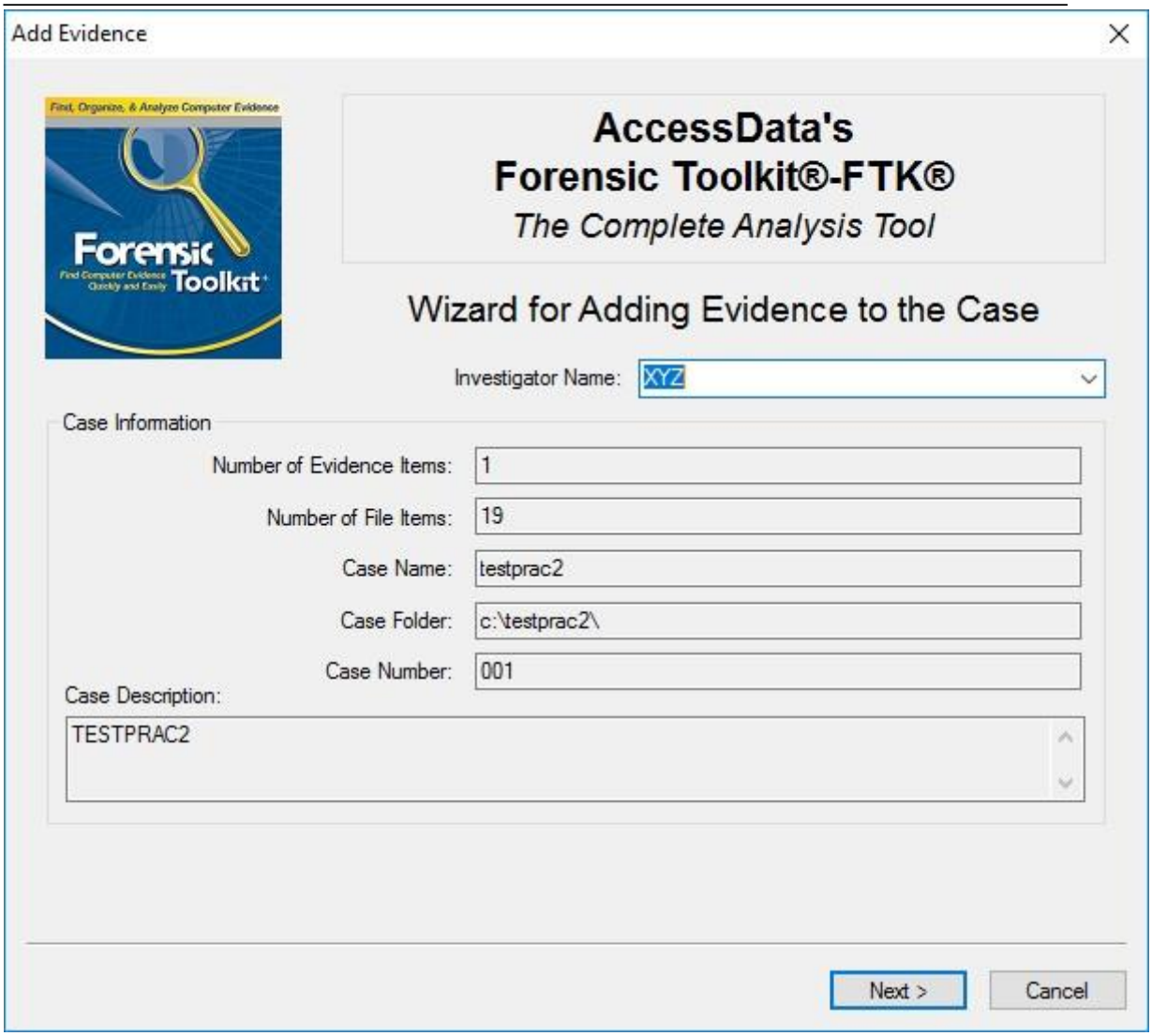

Evidence Information
Evidence Location:
F:\sem4\ComputerForensics\sample1.img
Evidence Display Name:
sample1
Evidence Identification Name/Number:
XYZ
Comment:
Local Evidence Time Zone:
Asia/Calcutta
OK
Cancel

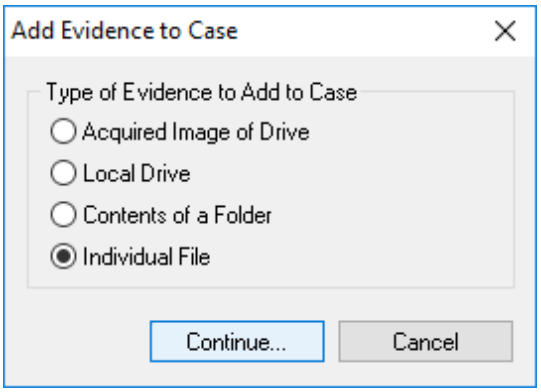

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files 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

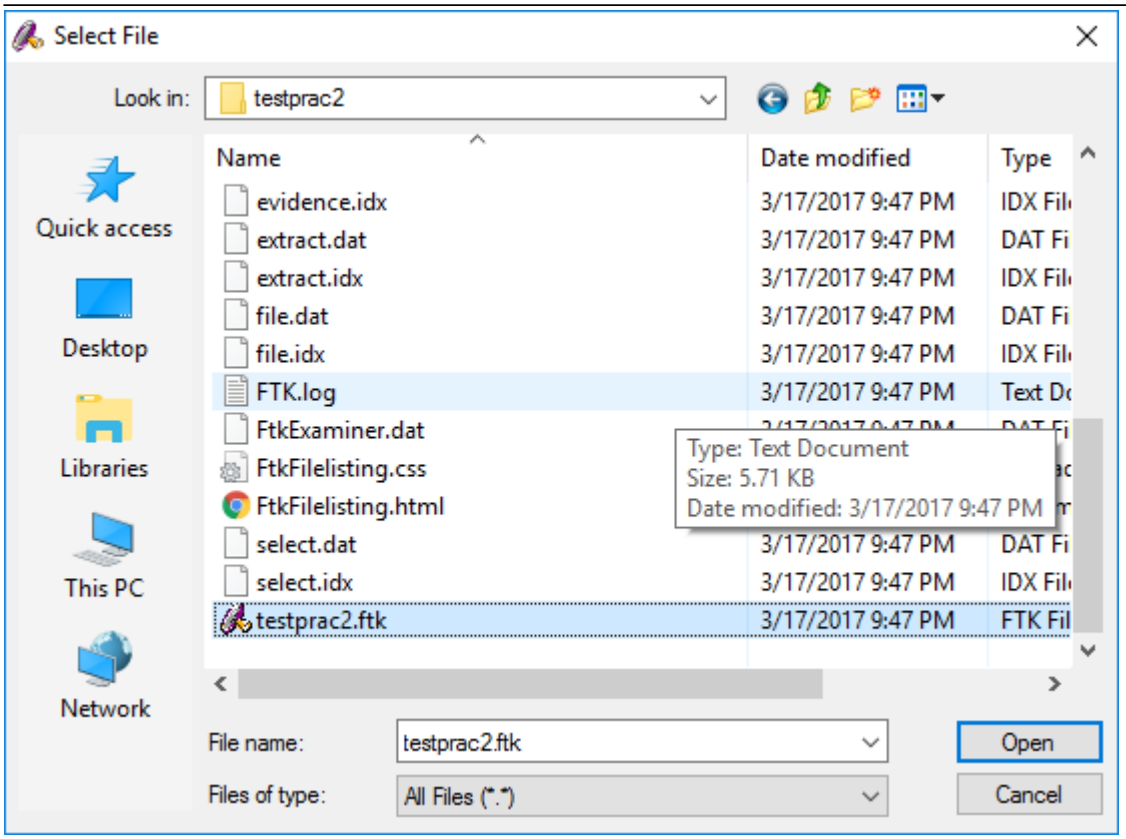

Case Summary
New Case Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
c:\testprac2
Number of Evidence Items: 1
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
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
Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
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.
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

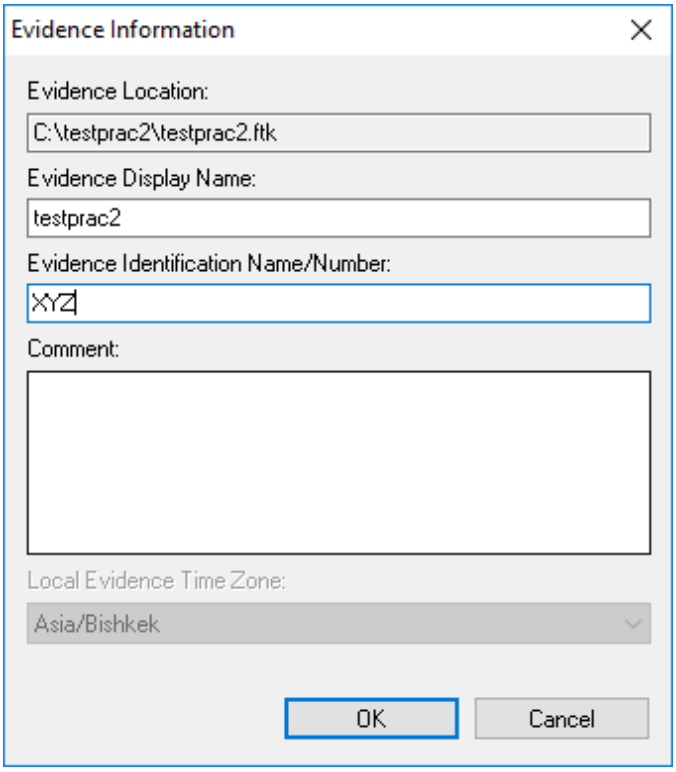

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Evidence Items
Evidence Items: 1
File Items
Total File Items: 19
Checked Items: 0
Unchecked Items: 19
Flagged Thumbnails: 0
Other Thumbnails: 1
Filtered In: 19
Filtered Out: 0
Unfiltered Filtered
All Items Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 1
Encrypted Files: 0
From E-mail: 0
Deleted Files: 1
From Recycle Bin: 0
Duplicate Items: 2
OLE Subitems: 10
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 1
Spreadsheets: 0
Databases: 0
Graphics: 1
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 4
Folders: 1
Slack/Free Space: 5
Other Known Type: 1
Unknown Type: 6
OFF Unfiltered All Columns DTZ
Evidence File Name Evidence Path Display Name Identification Name/Nu... Evidence Type
sample1.img F:\sem4\ComputerForensics sample1\KEEPP... XYZ FAT12
1 Listed 0 Checked Total F:\sem4\ComputerForensics\sample1.img

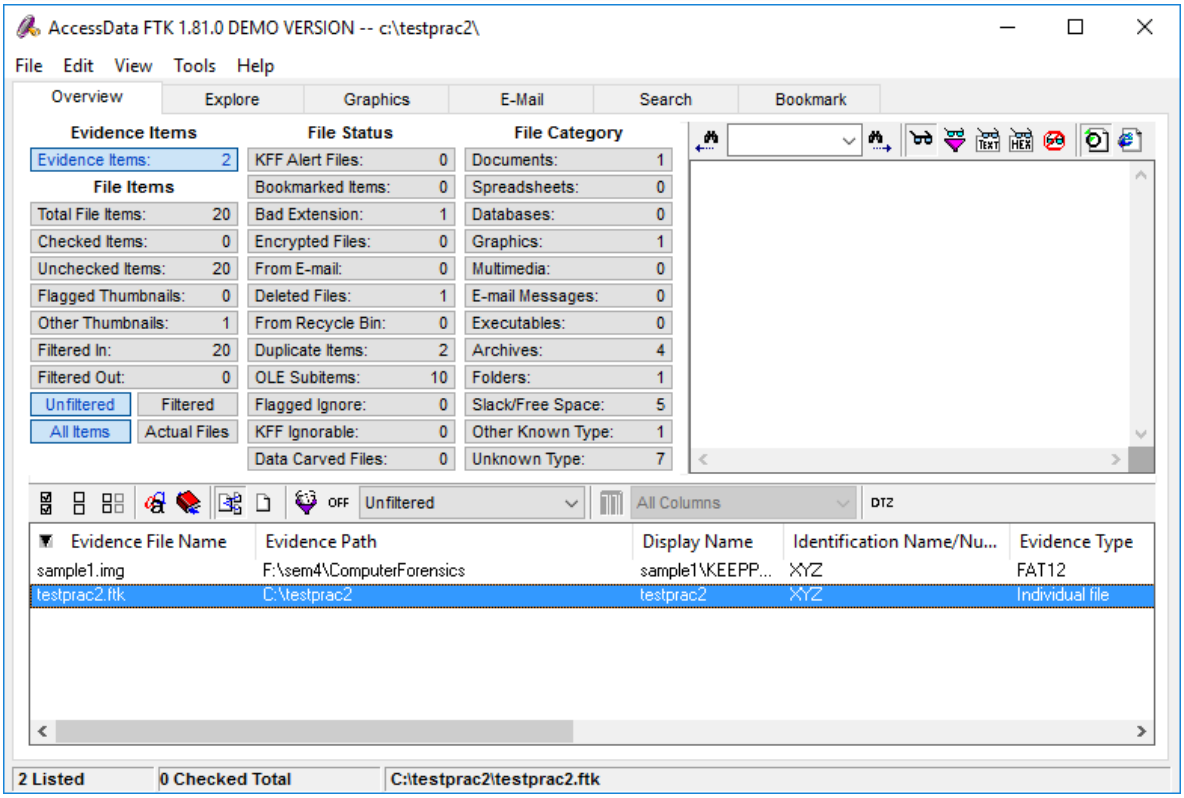

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date Acc Date L-Size P-Size
19 Listed 0 Checked Total 0 Highlighted

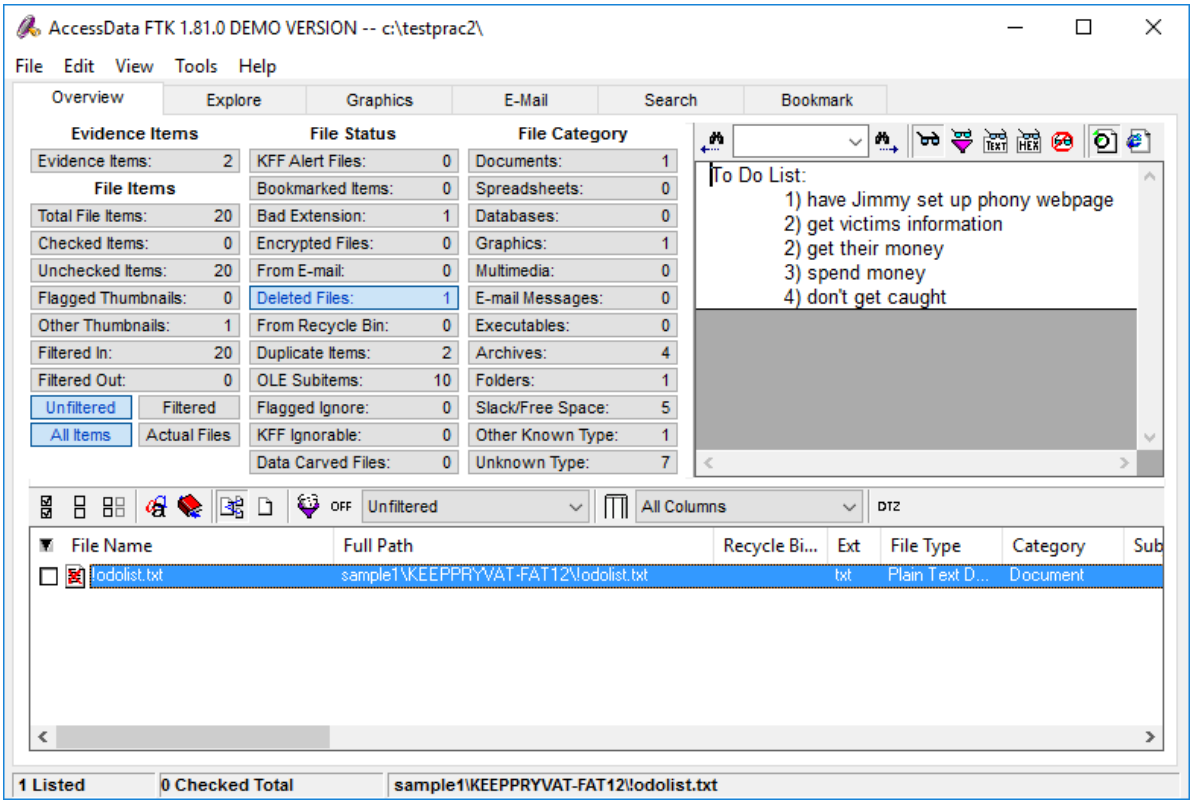

Add Evidence
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Adding Evidence to the Case
Investigator Name: XYZ
Case Information
Number of Evidence Items: 1
Number of File Items: 19
Case Name: testprac2
Case Folder: c:\testprac2\
Case Number: 001
Case Description:
TESTPRAC2
Next >
Cancel

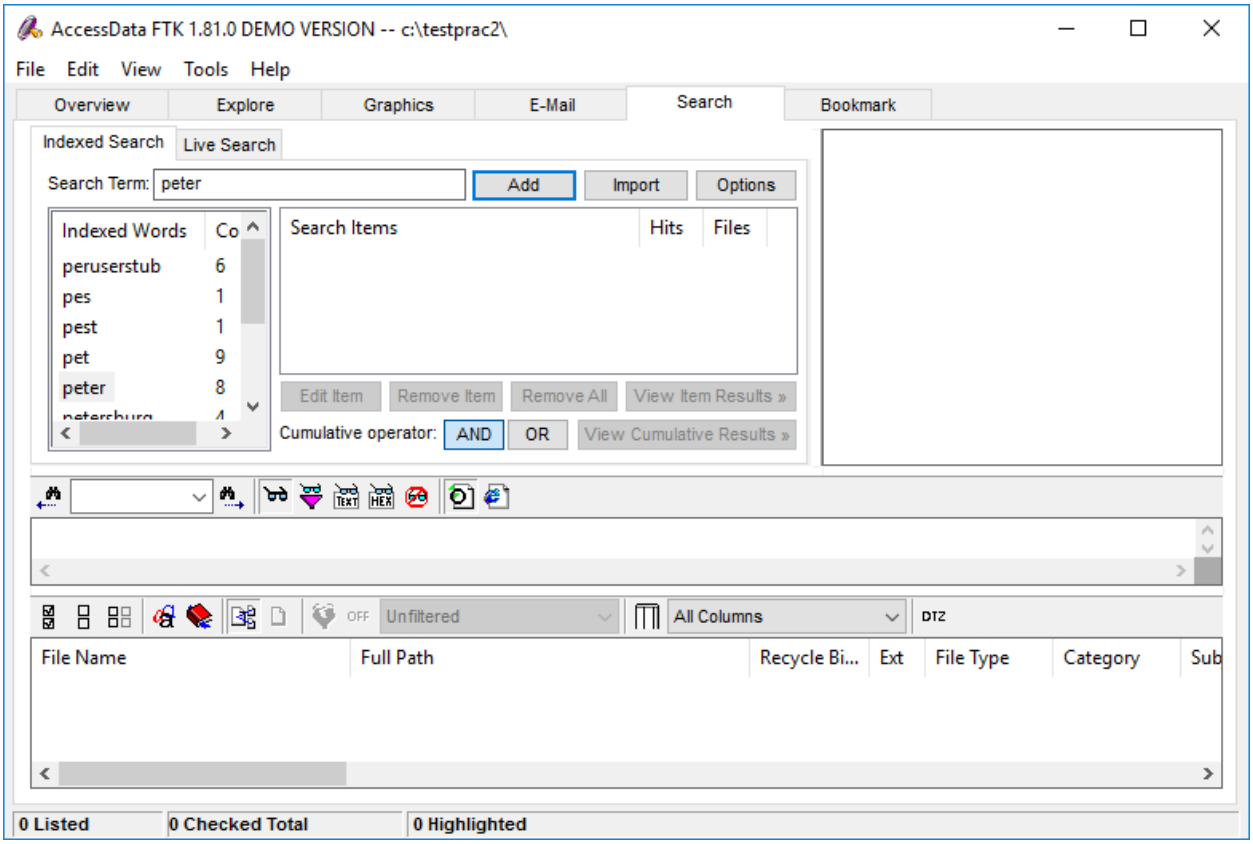

Add Evidence to Case
Type of Evidence to Add to Case
Acquired Image of Drive
Local Drive
Contents of a Folder
Individual File
Continue...
Cancel

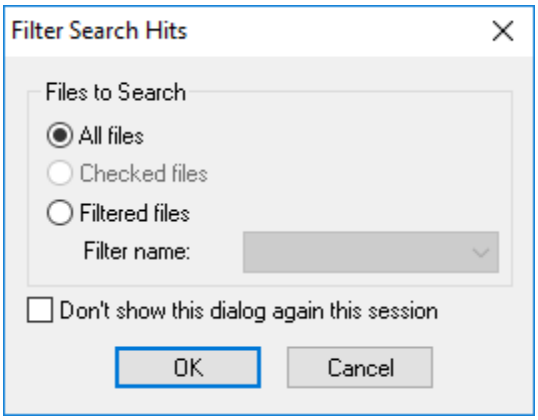

Select File
Look in: testprac2
Quick access
Desktop
Libraries
This PC
Network
Name
Date modified
Type
evidence.idx 3/17/2017 9:47 PM IDX Fil
extract.dat 3/17/2017 9:47 PM DAT Fi
extract.idx 3/17/2017 9:47 PM IDX Fil
file.dat 3/17/2017 9:47 PM DAT Fi
file.idx 3/17/2017 9:47 PM IDX Fil
FTK.log 3/17/2017 9:47 PM Text Do
FtkExaminer.dat
FtkFilelisting.css
FtkFilelisting.html
select.dat 3/17/2017 9:47 PM DAT Fi
select.idx 3/17/2017 9:47 PM IDX Fil
testprac2.ftk 3/17/2017 9:47 PM FTK Fil
Type: Text Document
Size: 5.71 KB
Date modified: 3/17/2017 9:47 PM
File name: testprac2.ftk
Files of type: All Files (*.*)
Open
Cancel

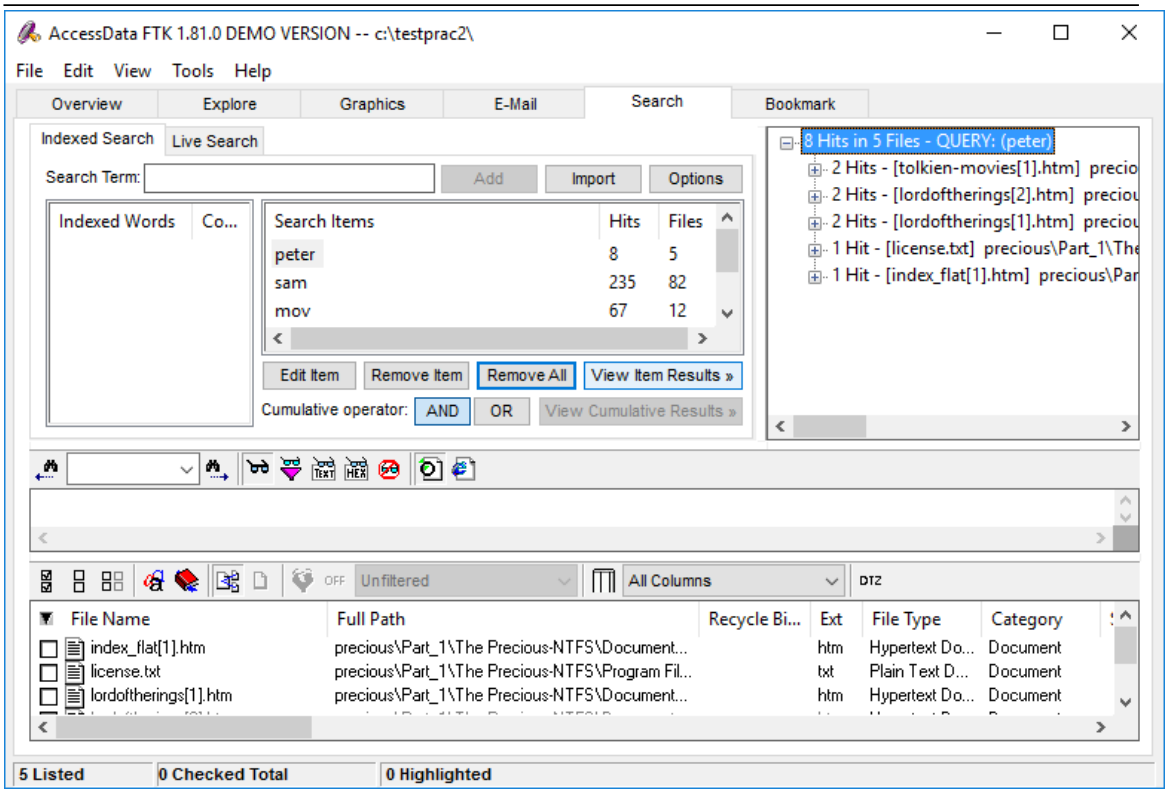

Evidence Information
Evidence Location:
C:\testprac2\testprac2.ftk
Evidence Display Name:
testprac2
Evidence Identification Name/Number:
XYZ
Comment:
Local Evidence Time Zone:
Asia/Bishkek
OK
Cancel

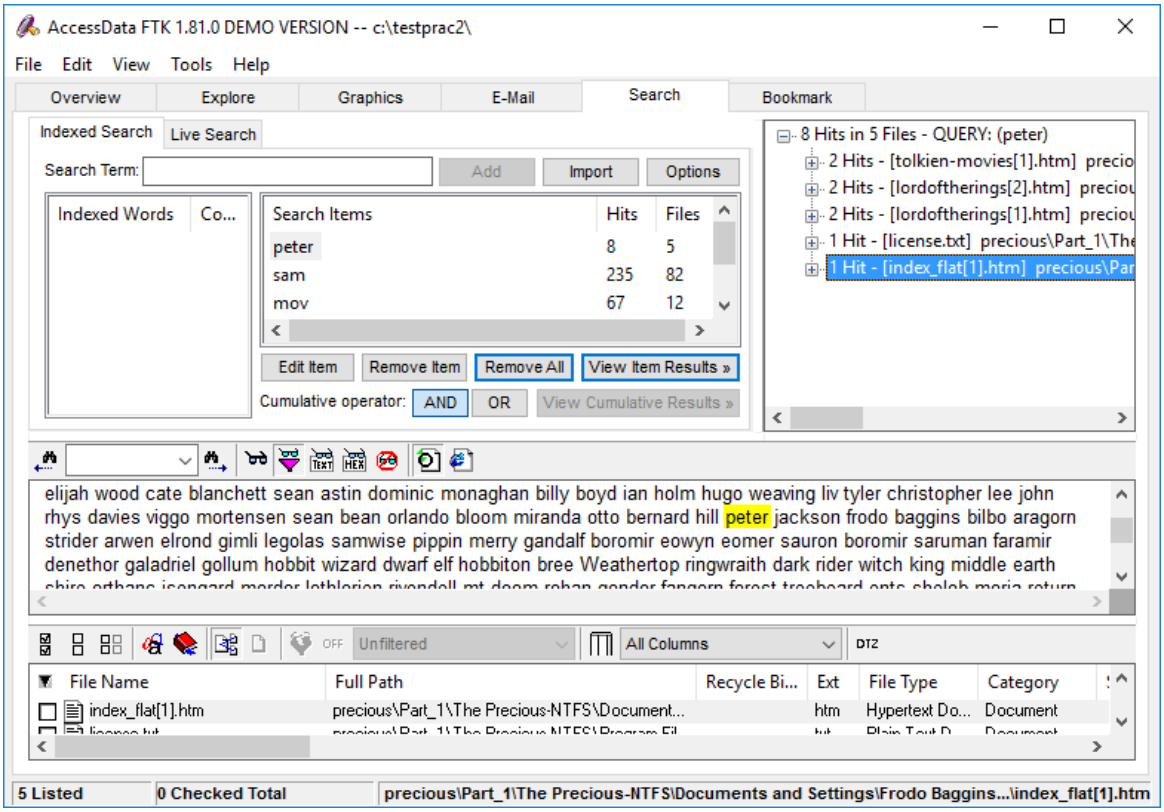

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Evidence Items
Evidence Items: 2
File Items
Total File Items: 20
Checked Items: 0
Unchecked Items: 20
Flagged Thumbnails: 0
Other Thumbnails: 1
Filtered In: 20
Filtered Out: 0
Unfiltered Filtered
All Items Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 1
Encrypted Files: 0
From E-mail: 0
Deleted Files: 1
From Recycle Bin: 0
Duplicate Items: 2
OLE Subitems: 10
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 1
Spreadsheets: 0
Databases: 0
Graphics: 1
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 4
Folders: 1
Slack/Free Space: 5
Other Known Type: 1
Unknown Type: 7
OFF Unfiltered All Columns DTZ
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

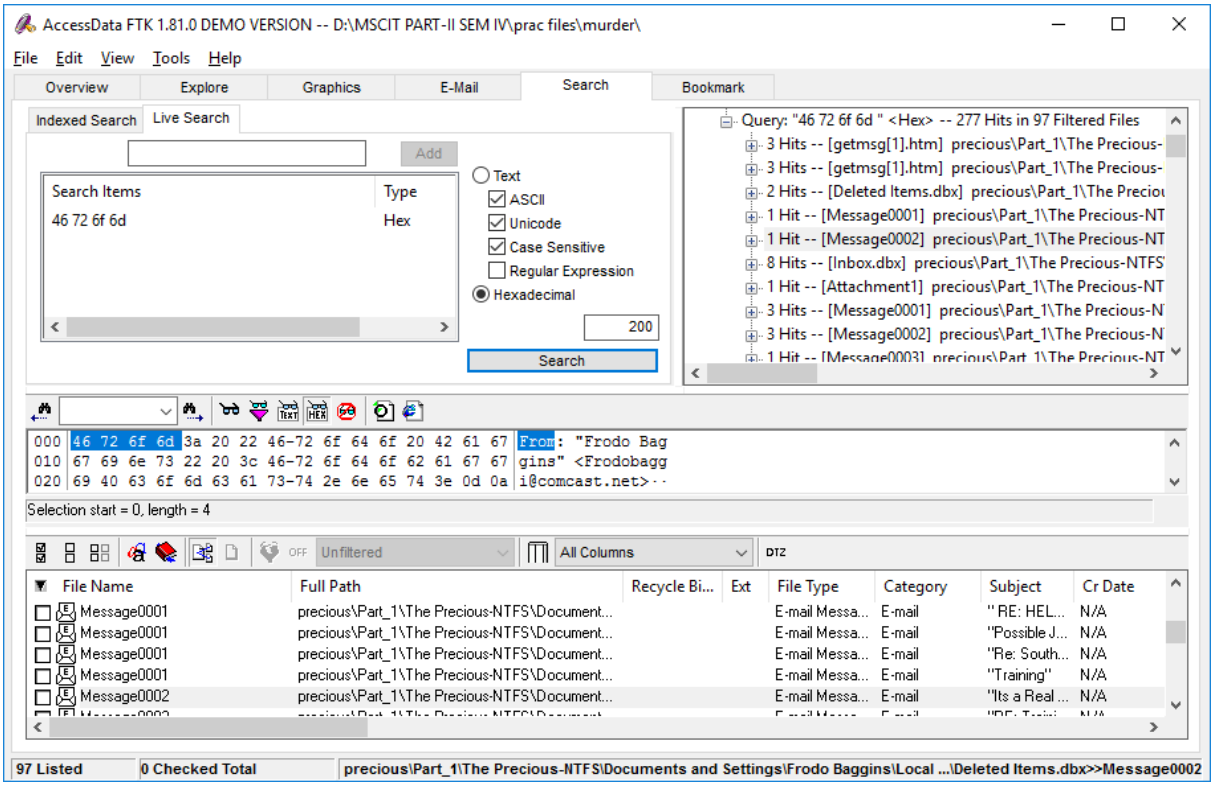

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Evidence Items
Evidence Items: 2
File Items
Total File Items: 20
Checked Items: 0
Unchecked Items: 20
Flagged Thumbnails: 0
Other Thumbnails: 1
Filtered In: 20
Filtered Out: 0
Unfiltered Filtered
All Items Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 1
Encrypted Files: 0
From E-mail: 0
Deleted Files: 1
From Recycle Bin: 0
Duplicate Items: 2
OLE Subitems: 10
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 1
Spreadsheets: 0
Databases: 0
Graphics: 1
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 4
Folders: 1
Slack/Free Space: 5
Other Known Type: 1
Unknown Type: 7
To Do List:
1) have Jimmy set up phony webpage
2) get victims information
2) get their money
3) spend money
4) don't get caught
OFF Unfiltered All Columns DTZ
File Name Full Path Recycle Bi... Ext File Type Category Sub
!odolist.txt sample1\KEEPPRYVAT-FAT12\!odolist.txt txt Plain Text D... Document
1 Listed 0 Checked Total sample1\KEEPPRYVAT-FAT12\!odolist.txt

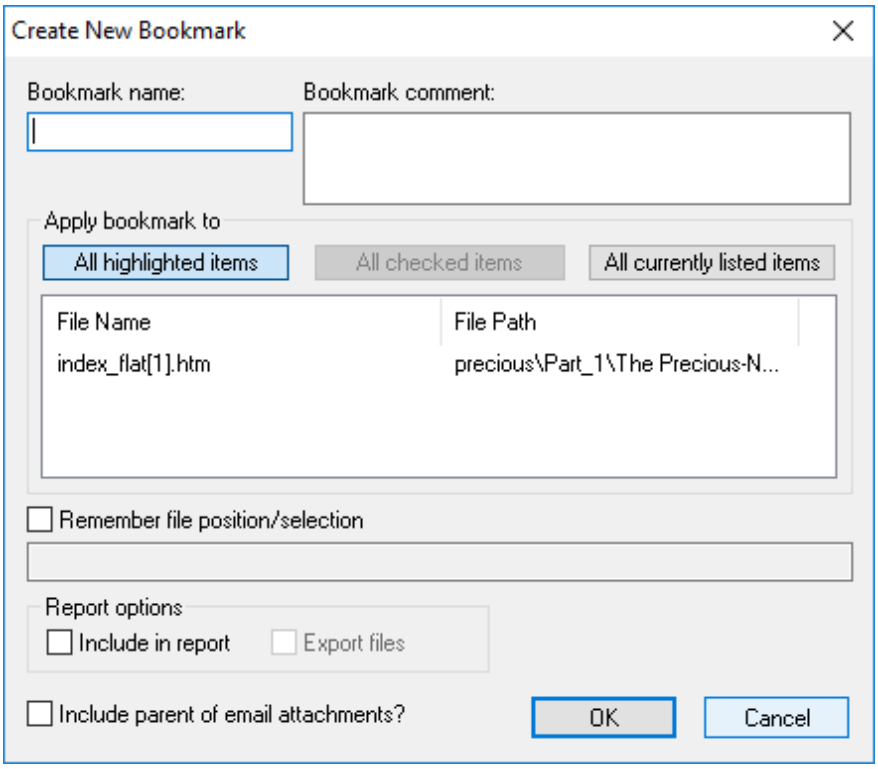

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search
Search Term: peter
Add Import Options
Indexed Words Co
peruserstub 6
pes 1
pest 1
pet 9
peter 8
Search Items Hits Files
Edit Item Remove Item Remove All View Item Results »
Cumulative operator: AND OR View Cumulative Results »
Unfiltered
All Columns
DTZ
File Name Full Path Recycle Bi... Ext File Type Category Sub
0 Listed 0 Checked Total 0 Highlighted

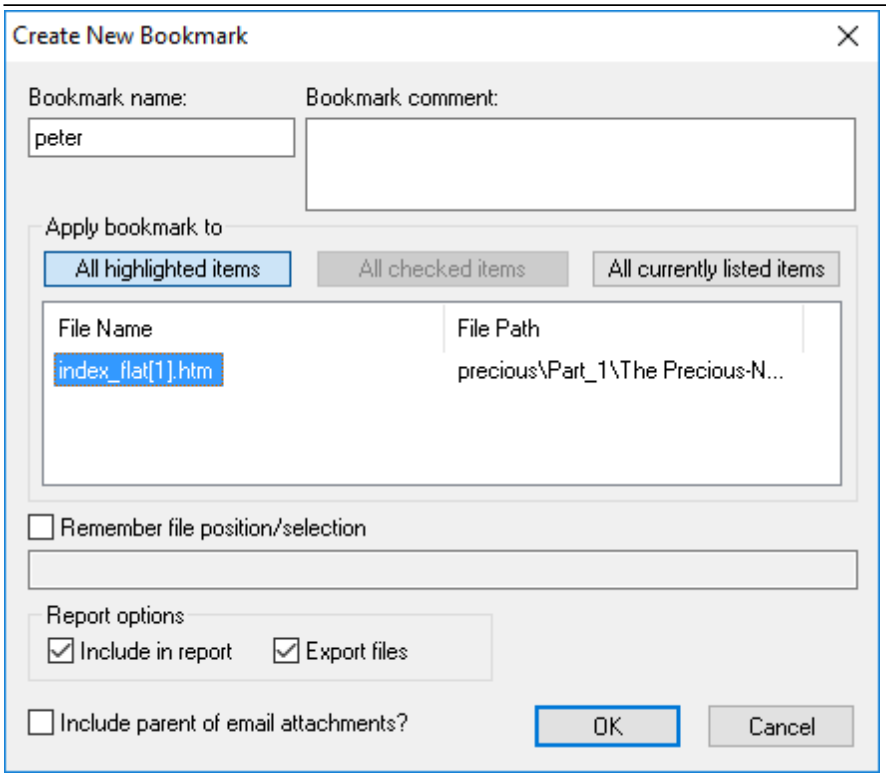

Filter Search Hits
Files to Search
All files
Checked files
Filtered files
Filter name:
Don't show this dialog again this session
OK
Cancel

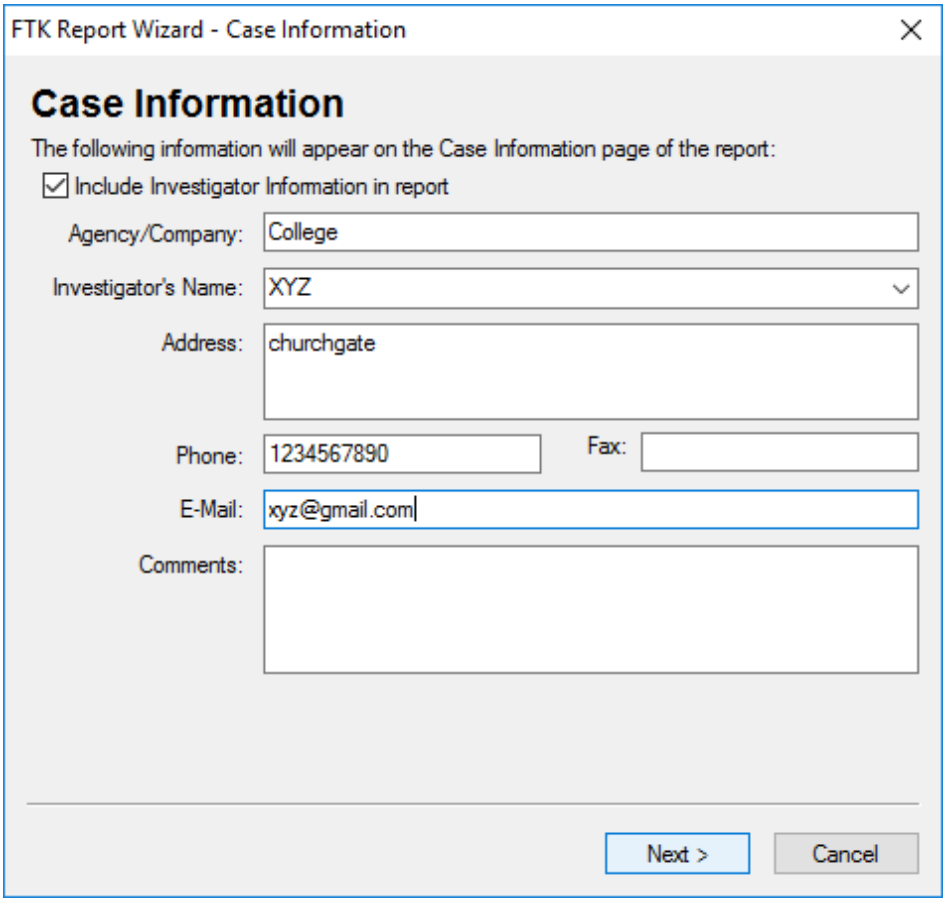

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search
Search Term:
Add Import Options
Indexed Words Co...
Search Items Hits Files
peter 8 5
sam 235 82
mov 67 12
Edit Item Remove Item Remove All View Item Results »
Cumulative operator: AND OR View Cumulative Results »
8 Hits in 5 Files - QUERY: (peter)
2 Hits - [tolkien-movies[1].htm] precio
2 Hits - [lordoftherings[2].htm] preciou
2 Hits - [lordoftherings[1].htm] preciou
1 Hit - [license.txt] precious\Part_1\The
1 Hit - [index_flat[1].htm] precious\Par
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

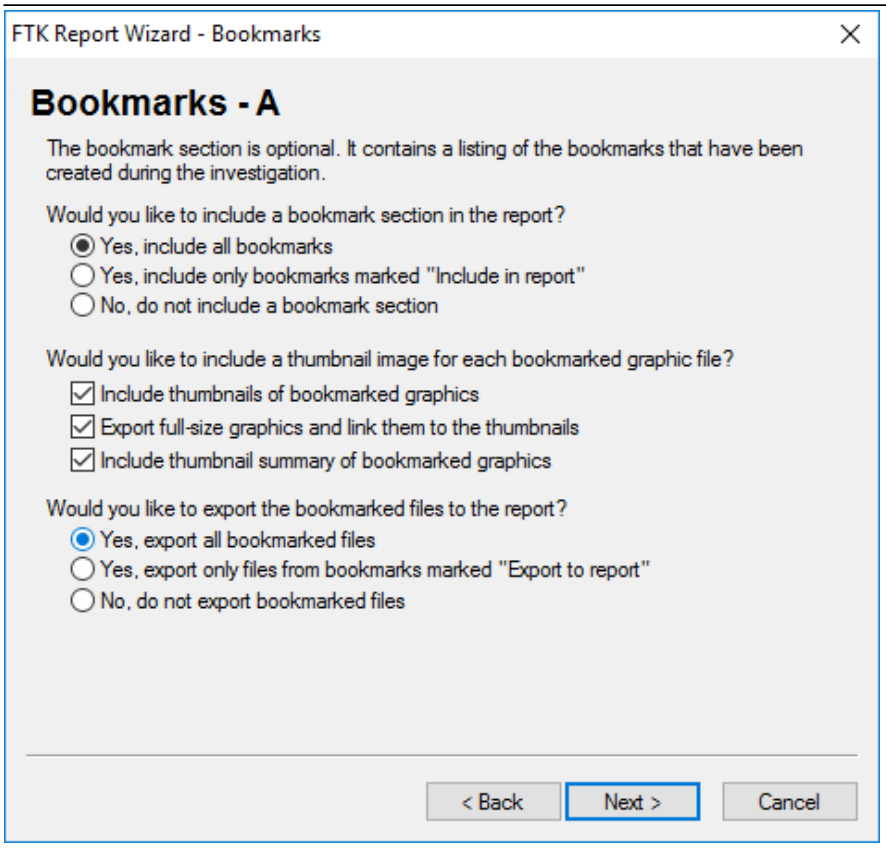

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search
Search Term:
Add Import Options
Indexed Words Co...
Search Items Hits Files
peter 8 5
sam 235 82
mov 67 12
Edit Item Remove Item Remove All View Item Results »
Cumulative operator: AND OR View Cumulative Results »
8 Hits in 5 Files - QUERY: (peter)
2 Hits - [tolkien-movies[1].htm] precio
2 Hits - [lordoftherings[2].htm] preciou
2 Hits - [lordoftherings[1].htm] preciou
1 Hit - [license.txt] precious\Part_1\The
1 Hit - [index_flat[1].htm] precious\Par
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
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
5 Listed
0 Checked Total
precious\Part_1\The Precious-NTFS\Documents and Settings\Frodo Baggins...\index_flat[1].htm

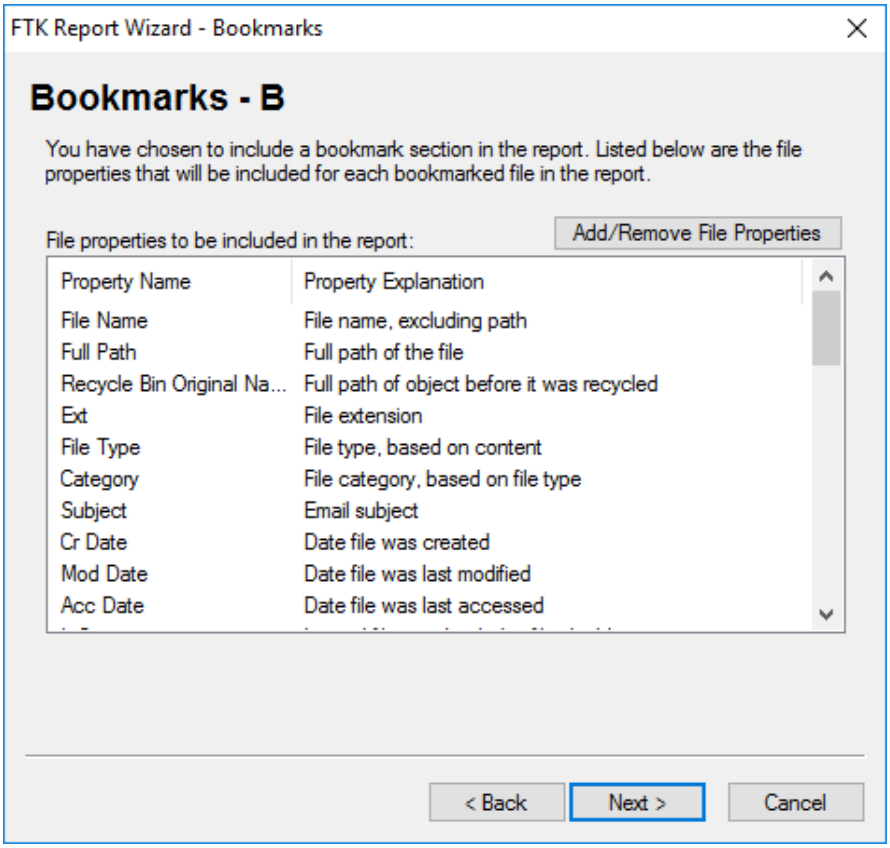

AccessData FTK 1.81.0 DEMO VERSION -- D:\MSCIT PART-II SEM IV\prac files\murder\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search
Add
Search Items Type
46 72 6f 6d Hex
Text
ASCII
Unicode
Case Sensitive
Regular Expression
Hexadecimal
200
Search
Query: "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 Precio
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
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" <Frodobagg
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 "Its a Real ... N/A
97 Listed
0 Checked Total
precious\Part_1\The Precious-NTFS\Documents and Settings\Frodo Baggins\Local ...\Deleted Items.dbx>>Message0002

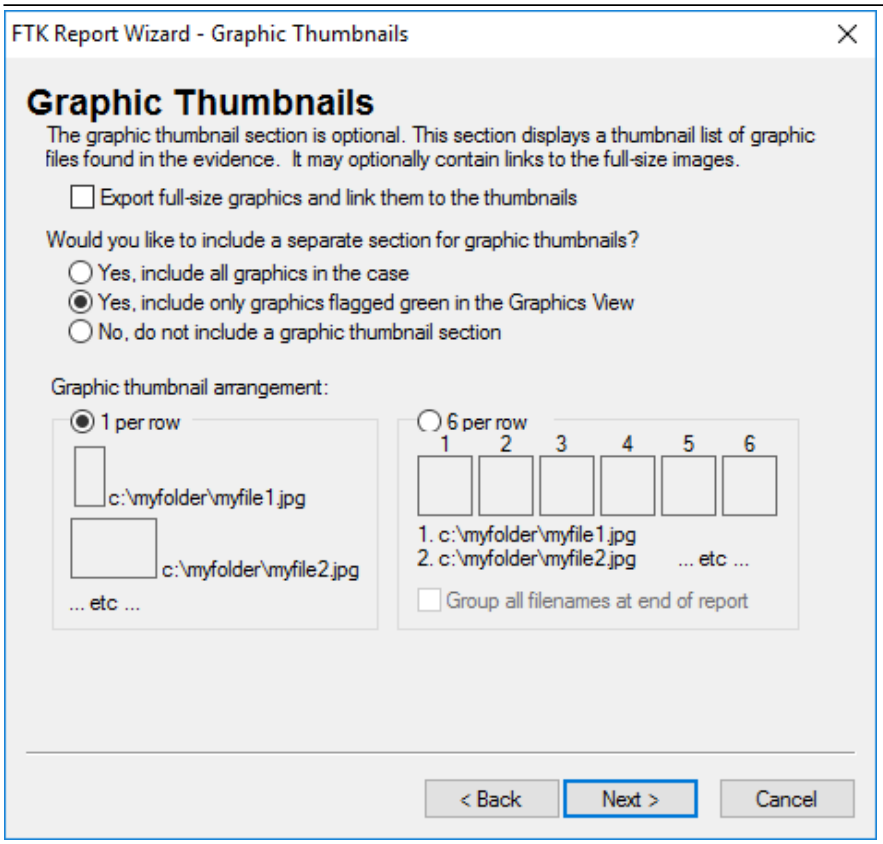

Create New Bookmark
Bookmark name:
Bookmark comment:
Apply bookmark to
All highlighted items
All checked items
All currently listed items
File Name
File Path
index_flat[1].htm
precious\Part_1\The Precious-N...
Remember file position/selection
Report options
Include in report
Export files
Include parent of email attachments?
OK
Cancel

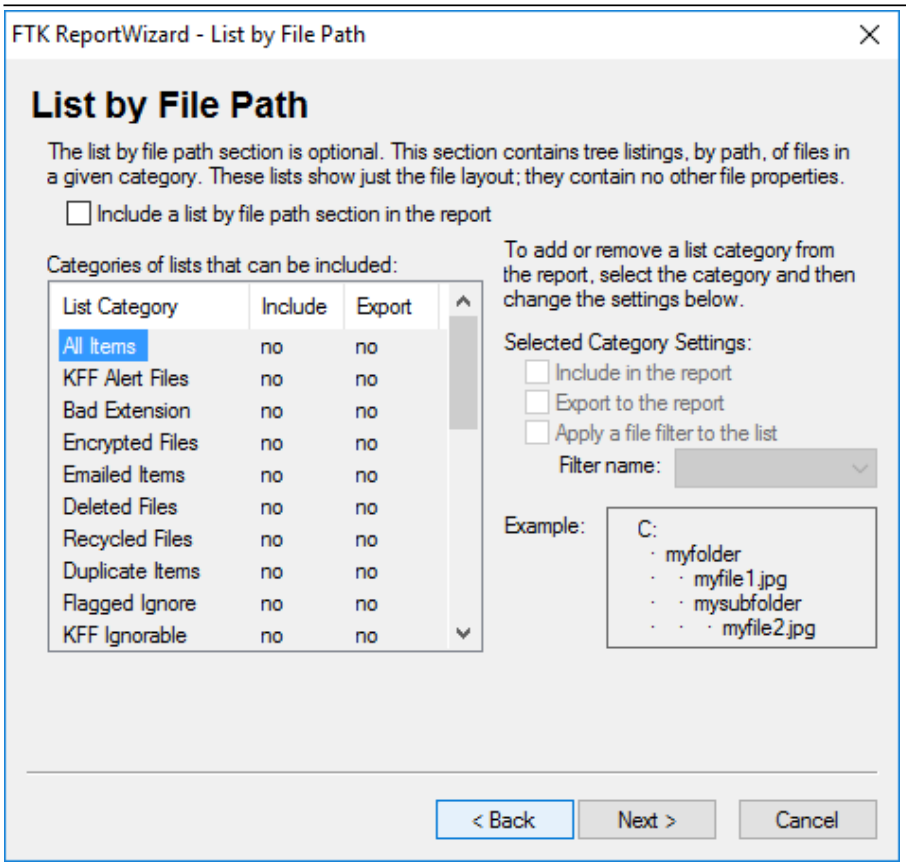

Create New Bookmark
Bookmark name:
peter
Bookmark comment:
Apply bookmark to
All highlighted items
All checked items
All currently listed items
File Name
File Path
index_flat[1].htm
precious\Part_1\The Precious-N...
Remember file position/selection
Report options
Include in report
Export files
Include parent of email attachments?
OK
Cancel

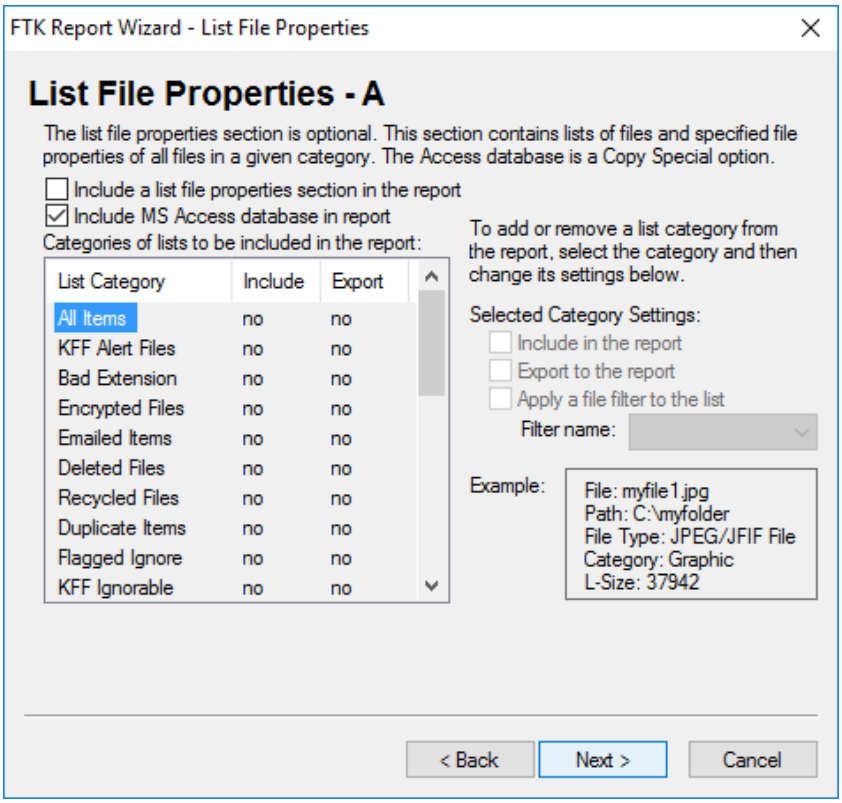

FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator Information in report
Agency/Company:
College
Investigator's Name:
XYZ
Address:
churchgate
Phone:
1234567890
Fax:
E-Mail:
xyz@gmail.com
Comments:
Next >
Cancel

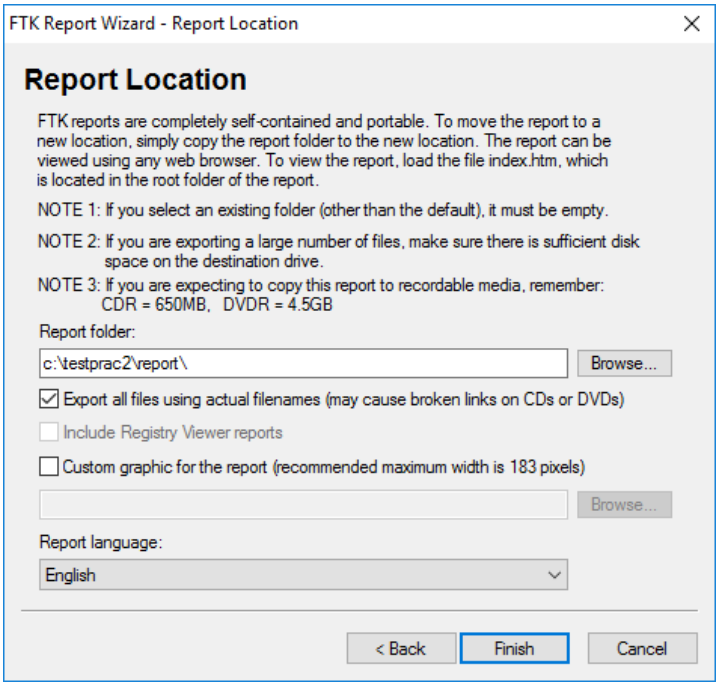

FTK Report Wizard - Bookmarks
Bookmarks - A
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.
Would you like to include a bookmark section in the report?
Yes, include all bookmarks
Yes, include only bookmarks marked "Include in report"
No, do not include a bookmark section
Would you like to include a thumbnail image for each bookmarked graphic file?
Include thumbnails of bookmarked graphics
Export full-size graphics and link them to the thumbnails
Include thumbnail summary of bookmarked graphics
Would you like to export the bookmarked files to the report?
Yes, export all bookmarked files
Yes, export only files from bookmarks marked "Export to report"
No, do not export bookmarked files
< Back
Next >
Cancel


FTK Report Wizard - Bookmarks
Bookmarks - B
You have chosen to include a bookmark section in the report. Listed below are the file properties that will be included for each bookmarked file in the report.
File properties to be included in the report:
Add/Remove File Properties
Property Name
Property Explanation
File Name
File name, excluding path
Full Path
Full path of the file
Recycle Bin Original Na...
Full path of object before it was recycled
Ext
File extension
File Type
File type, based on content
Category
File category, based on file type
Subject
Email subject
Cr Date
Date file was created
Mod Date
Date file was last modified
Acc Date
Date file was last accessed
< Back
Next >
Cancel


FTK Report Wizard - Graphic Thumbnails
Graphic Thumbnails
The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.
Export full-size graphics and link them to the thumbnails
Would you like to include a separate section for graphic thumbnails?
Yes, include all graphics in the case
Yes, include only graphics flagged green in the Graphics View
No, do not include a graphic thumbnail section
Graphic thumbnail arrangement:
1 per row
c:\myfolder\myfile1.jpg
c:\myfolder\myfile2.jpg
... etc ...
6 per row
1 2 3 4 5 6
1. c:\myfolder\myfile1.jpg
2. c:\myfolder\myfile2.jpg ... etc ...
Group all filenames at end of report
< Back
Next >
Cancel

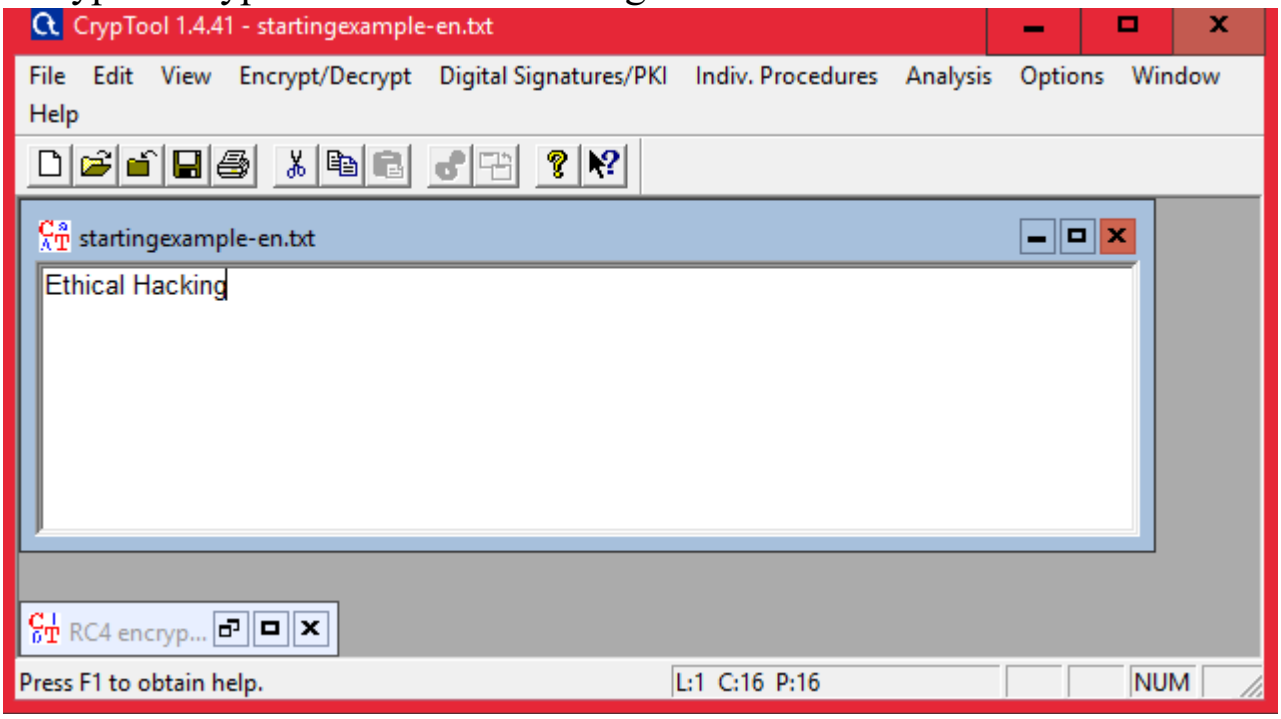

FTK ReportWizard - List by File Path
List by File Path
The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.
Include a list by file path section in the report
Categories of lists that can be included:
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 the settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
C:
myfolder
myfile1.jpg
mysubfolder
myfile2.jpg
< Back
Next >
Cancel

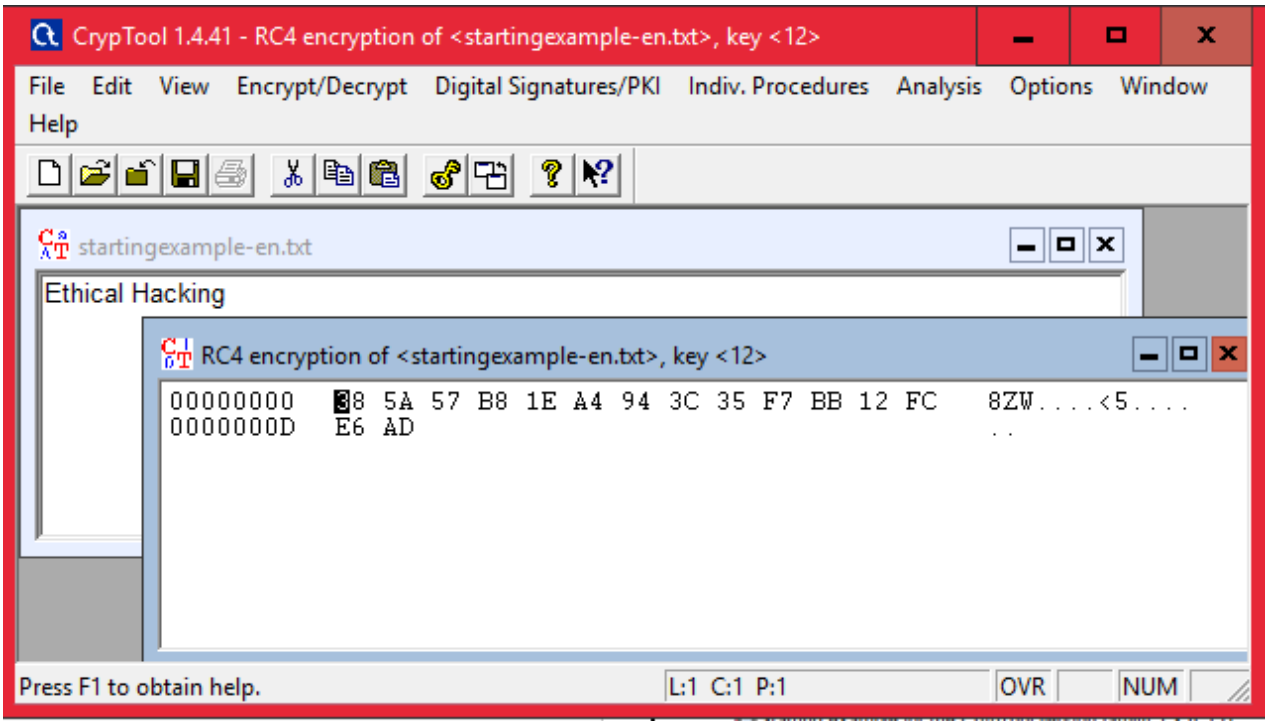

FTK Report Wizard - List File Properties
List File Properties - A
The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.
Include a list file properties section in 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:
c:\testprac2\report\
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:
English
< Back
Finish
Cancel

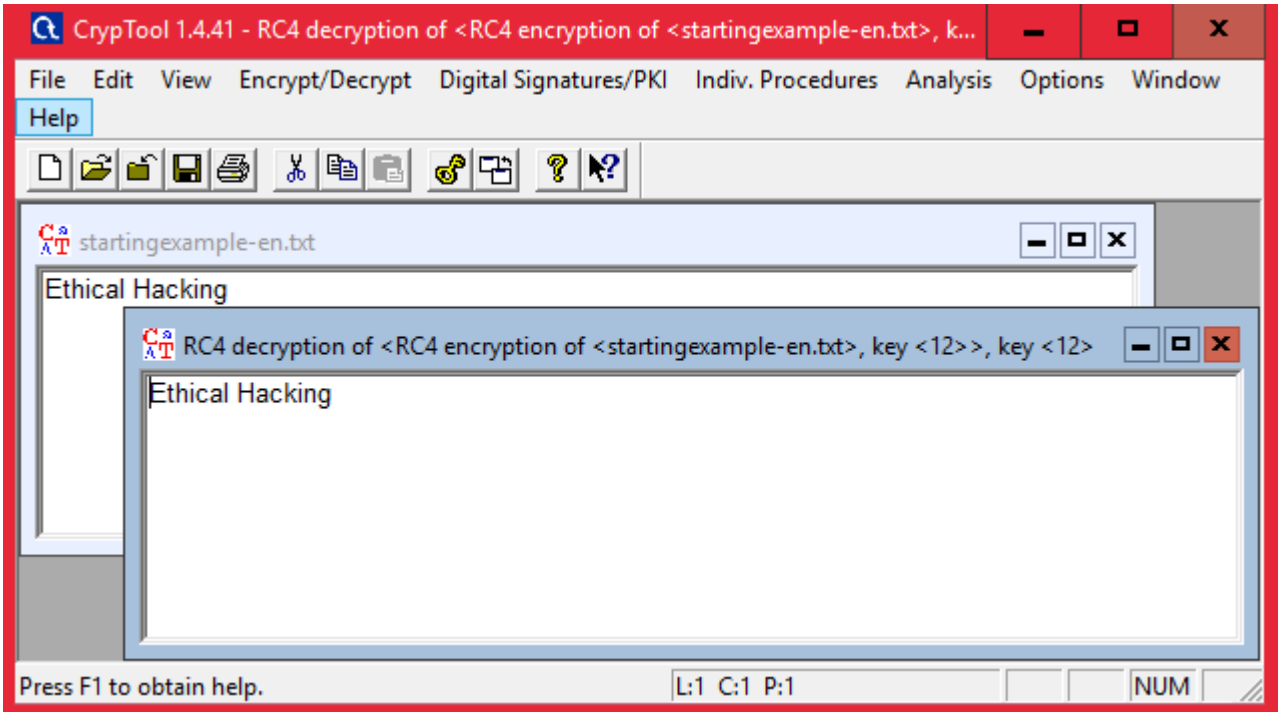
PRACTICAL NO 04: Calculate the MD5 and SHA1 hashes

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



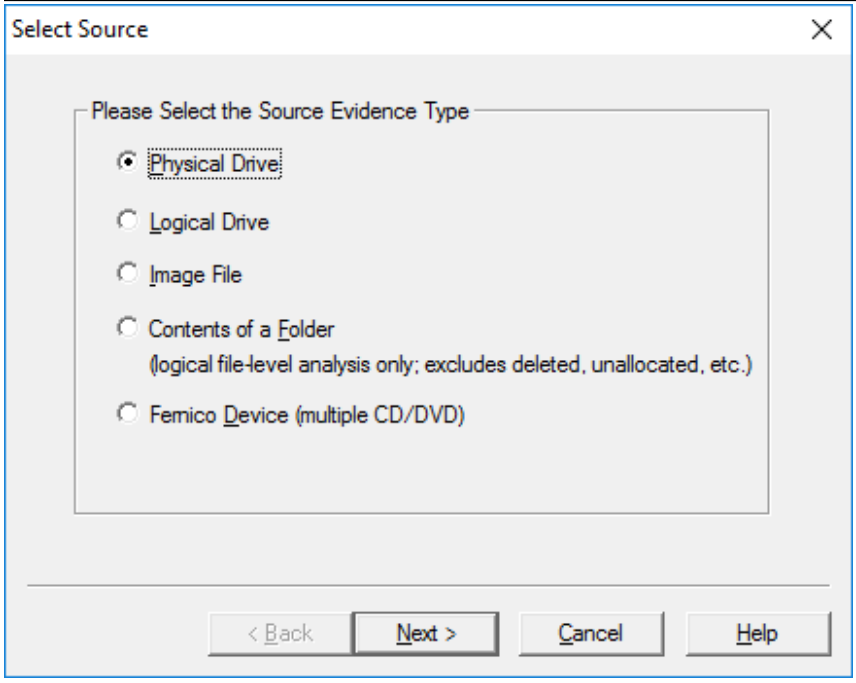


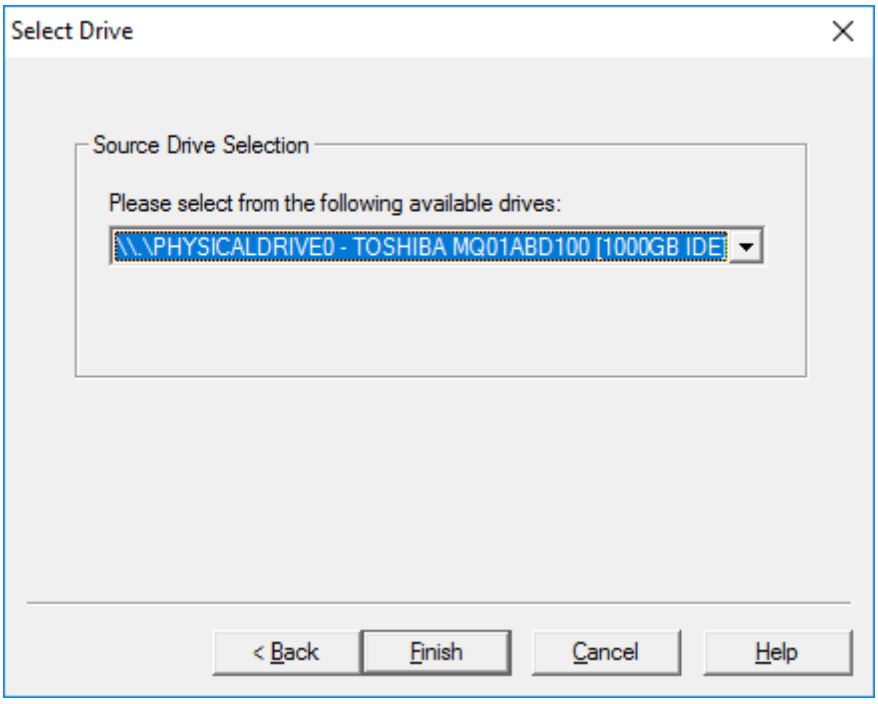
Decryption

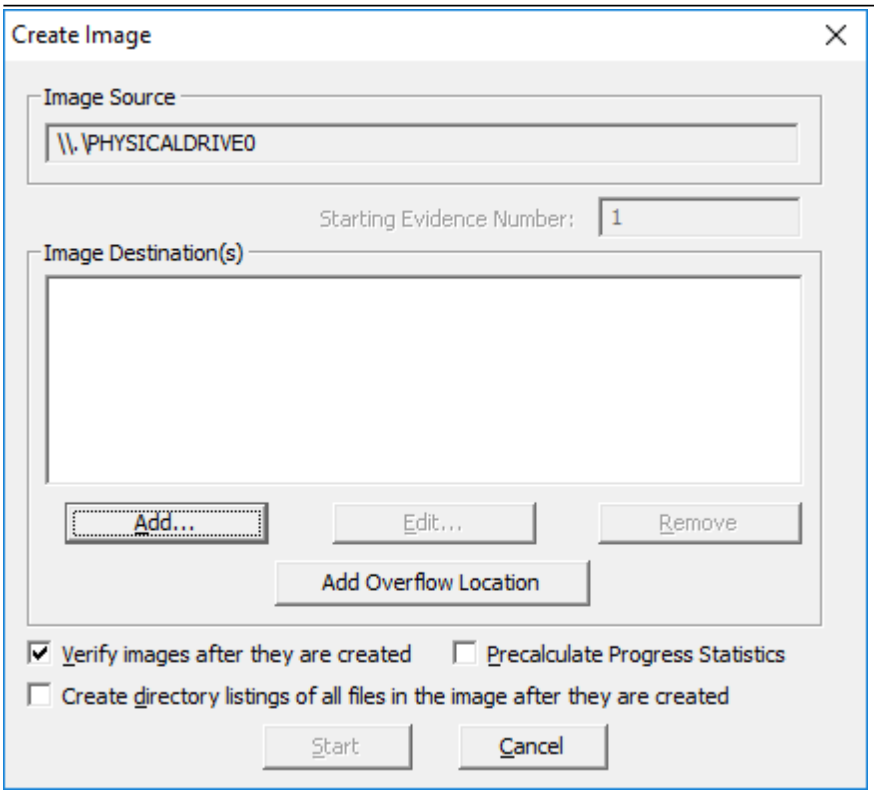

CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <startingexample-en.txt>, k...
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window
Help
startingexample-en.txt
Ethical Hacking
RC4 decryption of <RC4 encryption of <startingexample-en.txt>, key <12>>, key <12>
Ethical Hacking
Press F1 to obtain help.
L:1 C:1 P:1
NUM

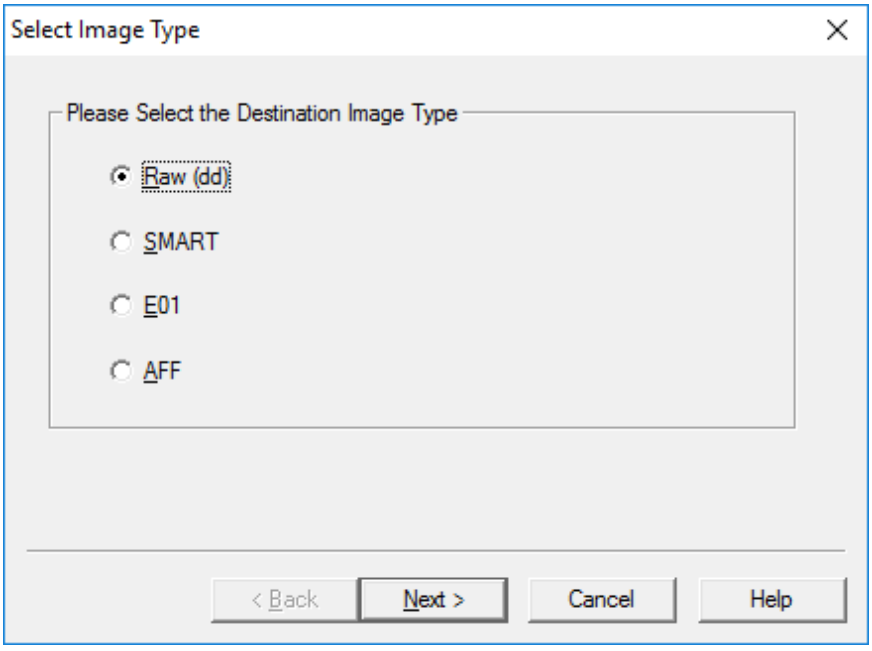
PRACTICAL NO 05: Use tools to collect, preserve and reveal digital evidence without compromising systems and data

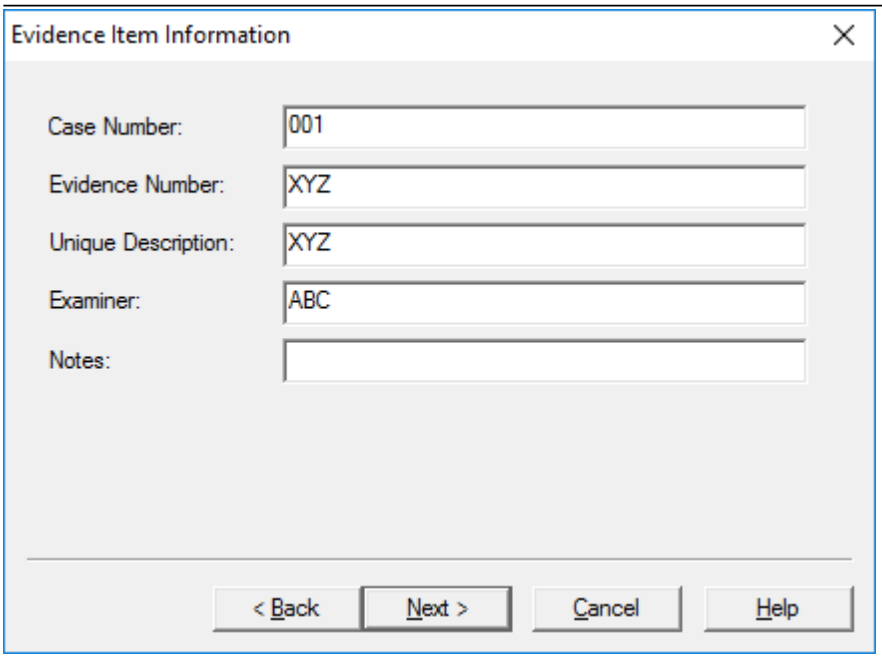
(Tool used: FTK Imager)

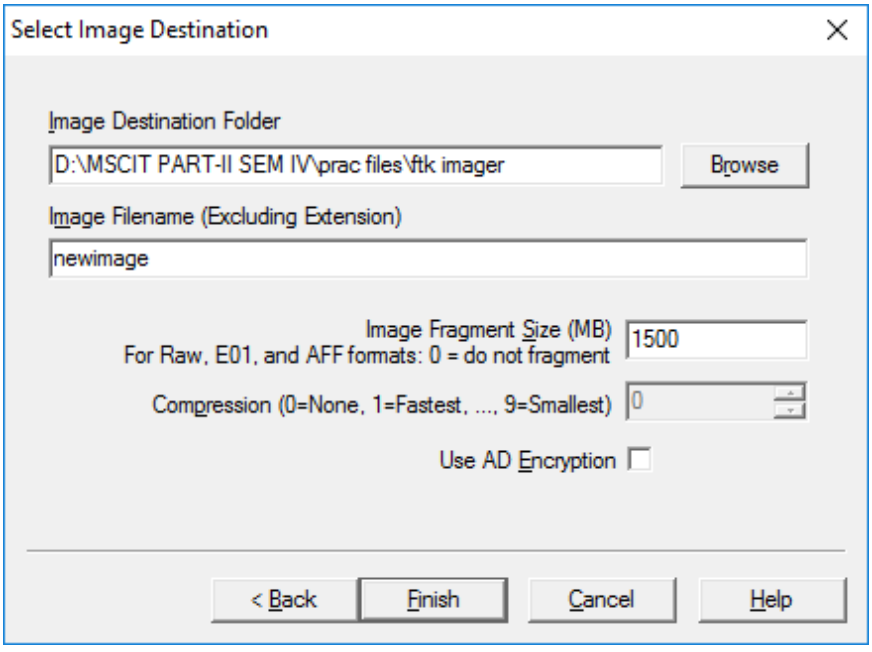


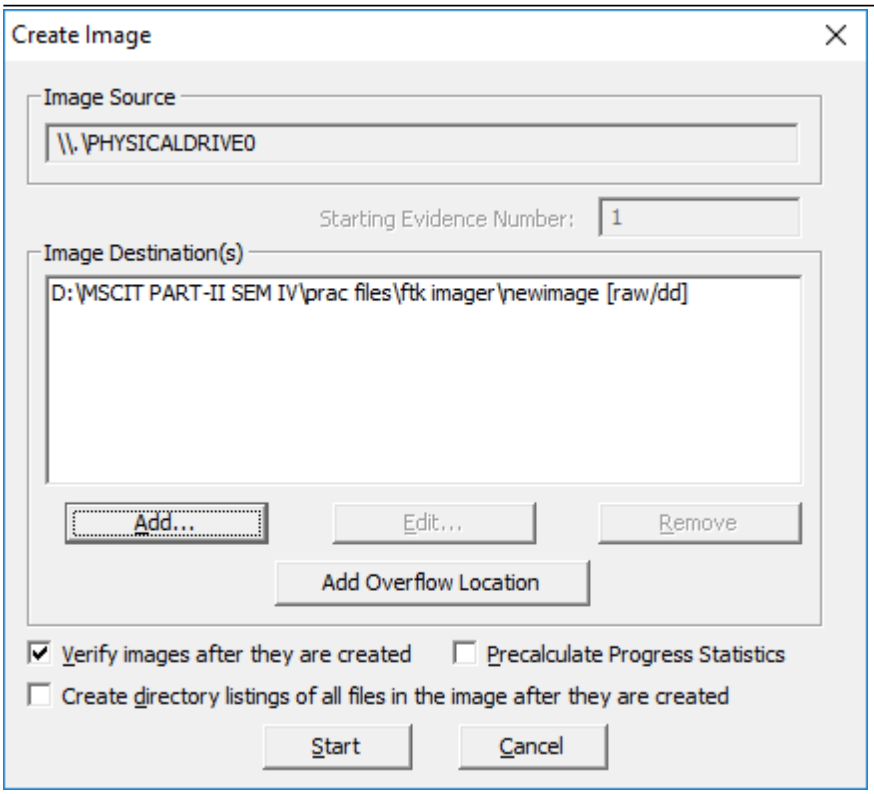


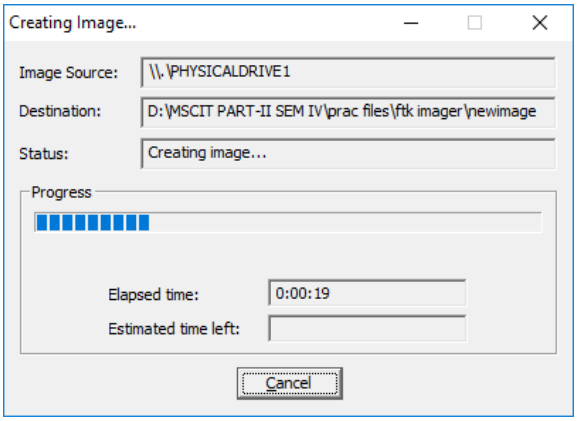

Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

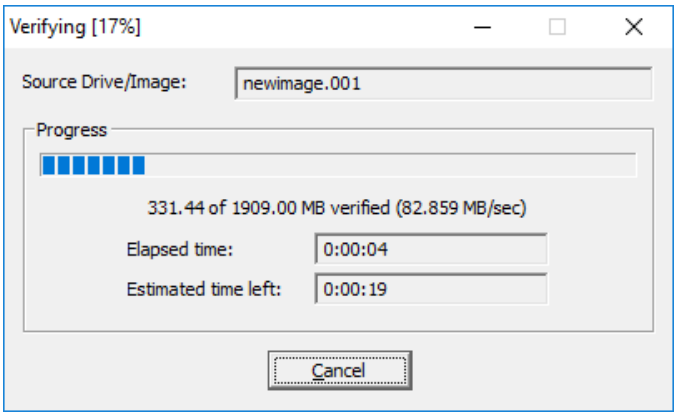

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help

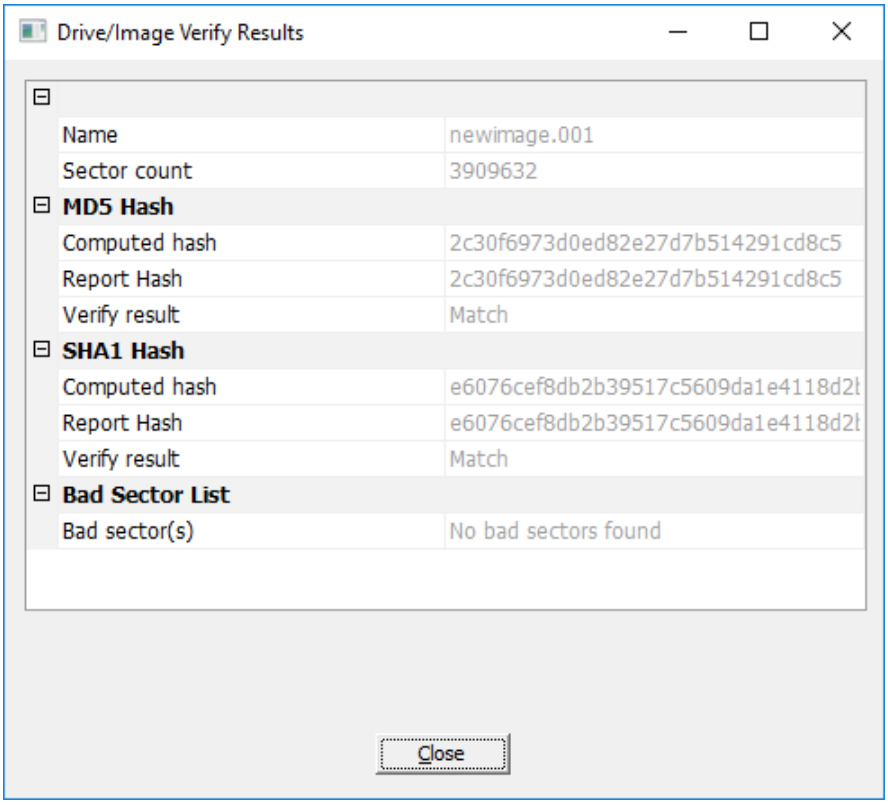

Evidence Item Information
Case Number:
001
Evidence Number:
XYZ
Unique Description:
XYZ
Examiner:
ABC
Notes:
< Back
Next >
Cancel
Help


Select Image Destination
Image Destination Folder
D:\MSCIT PART-II SEM IV\prac files\ftk imager
Browse
Image Filename (Excluding Extension)
newimage
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Back
Finish
Cancel
Help


Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Image Destination(s)
D:\MSCIT PART-II SEM IV\prac files\ftk imager\newimage [raw/dd]
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


Creating Image...
Image Source:
\\.\PHYSICALDRIVE1
Destination:
D:\MSCIT PART-II SEM IV\prac files\ftk imager\newimage
Status:
Creating image...
Progress
Elapsed time:
0:00:19
Estimated time left:
Cancel


Verifying [17%]
Source Drive/Image:
newimage.001
Progress
331.44 of 1909.00 MB verified (82.859 MB/sec)
Elapsed time:
0:00:04
Estimated time left:
0:00:19
Cancel


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
e6076cef8db2b39517c5609da1e4118d2b
Report Hash
e6076cef8db2b39517c5609da1e4118d2b
Verify result
Match
Bad Sector List
Bad sector(s)
No bad sectors found
Close

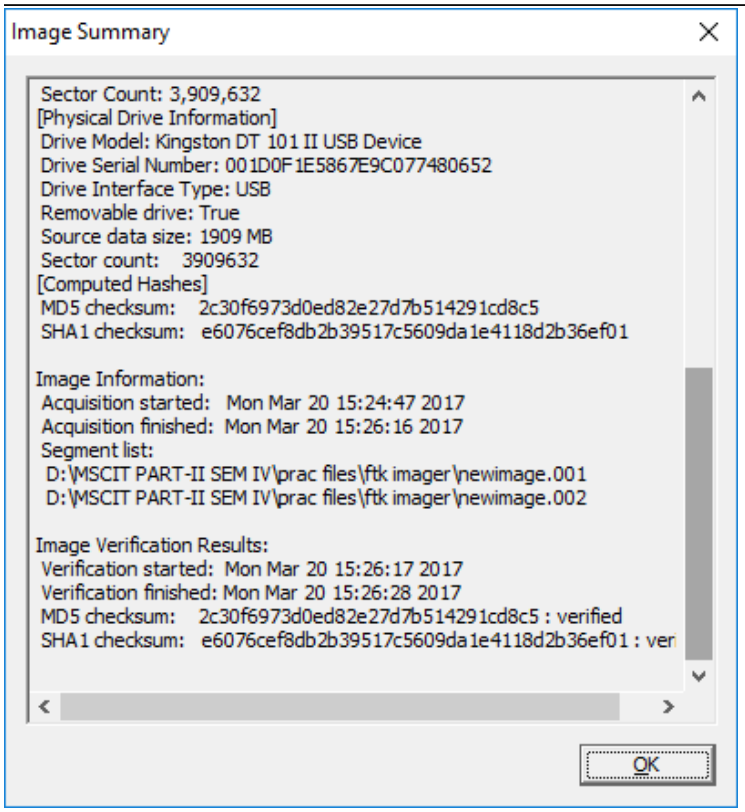


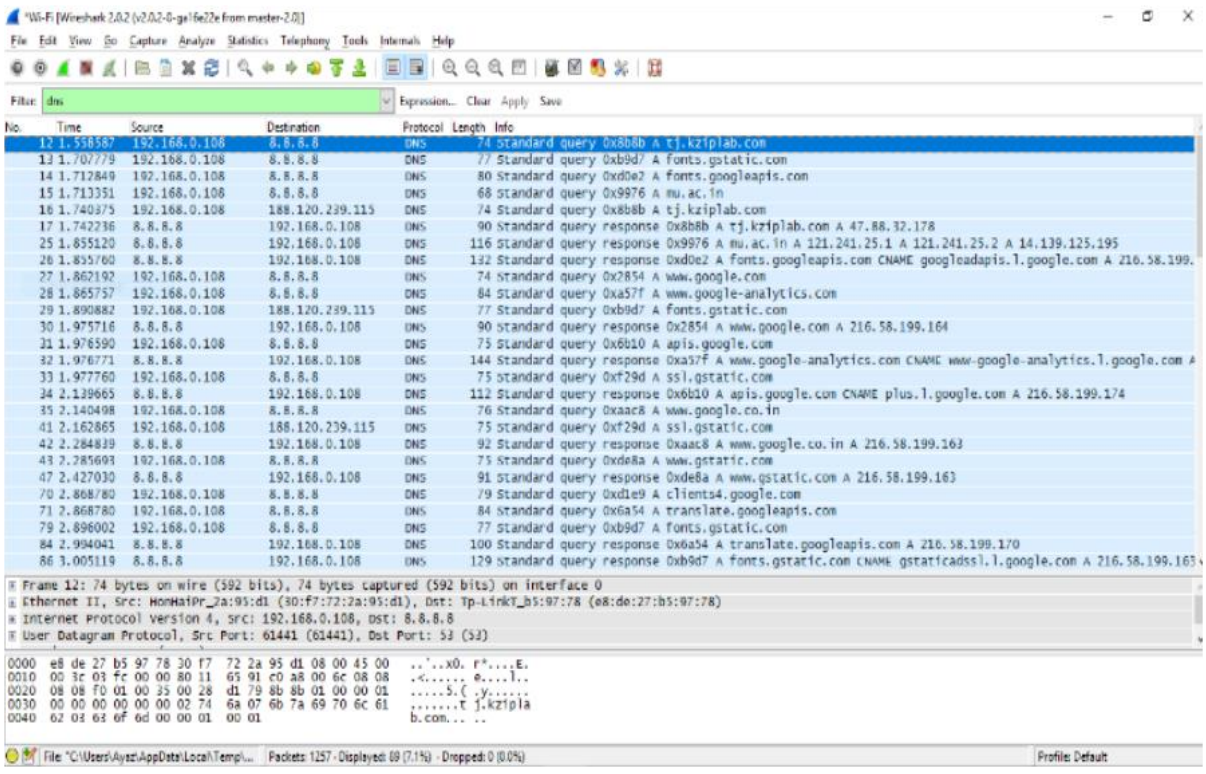
Image Summary
Sector Count: 3,909,632
[Physical Drive Information]
Drive Model: Kingston DT 101 II USB Device
Drive Serial Number: 001D0F1E5867E9C077480652
Drive Interface Type: USB
Removable drive: True
Source data size: 1909 MB
Sector count: 3909632
[Computed Hashes]
MD5 checksum: 2c30f6973d0ed82e27d7b514291cd8c5
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 N0:06
Acquire web pages for forensic investigation. (Wireshark) or Use traffic capturing and analyzing tool. (Wireshark) Using filters and using test login page.

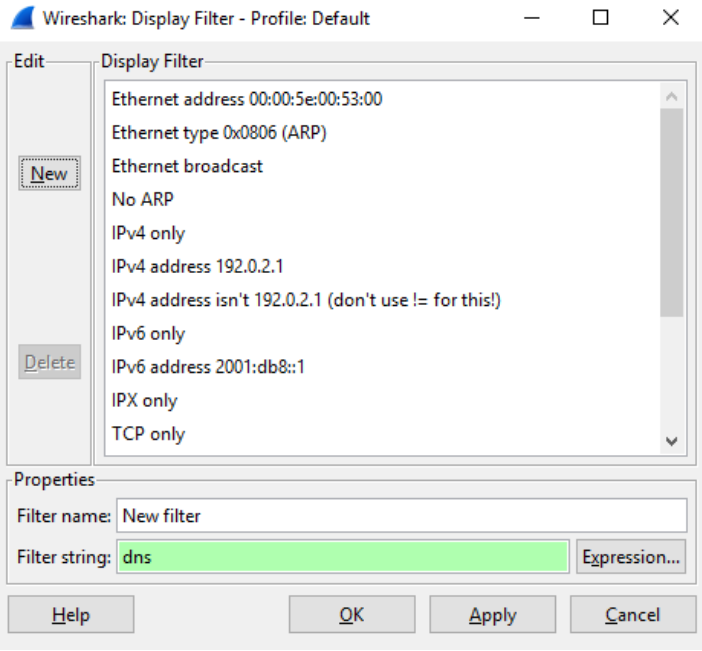
Description: Wireshark is a network packet analyser that intercepts, captures and logs information about packets passing through a network interface. This is useful for analysing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage andgather statistics

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.

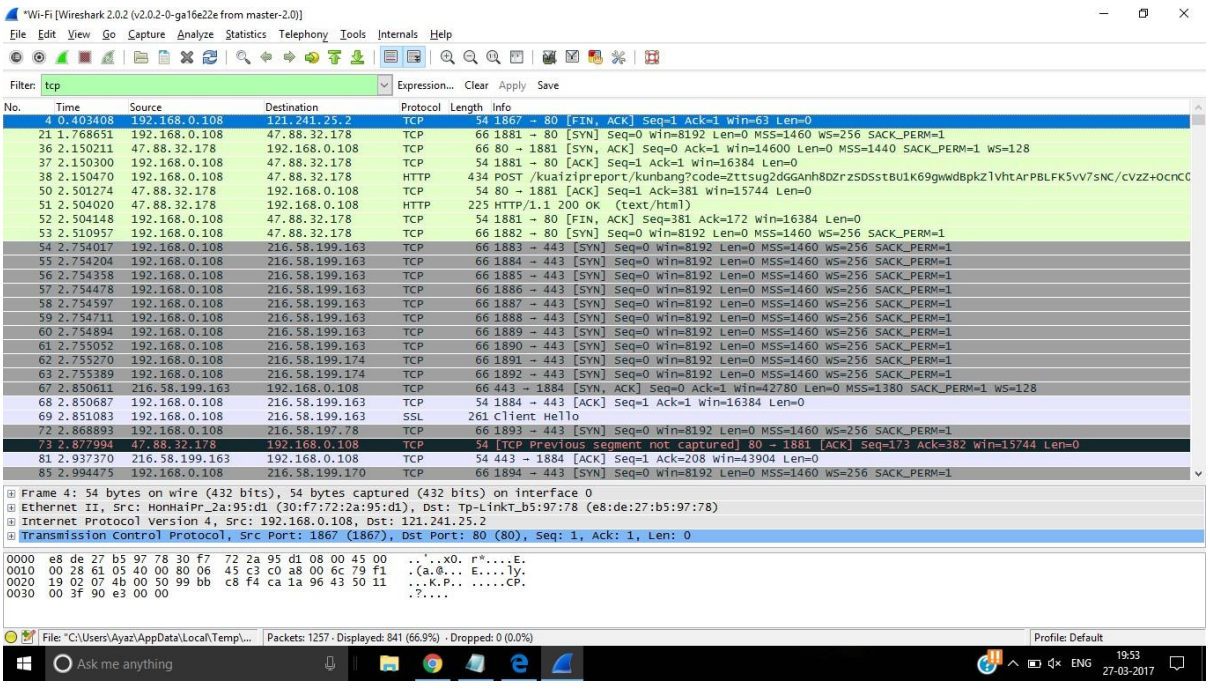
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



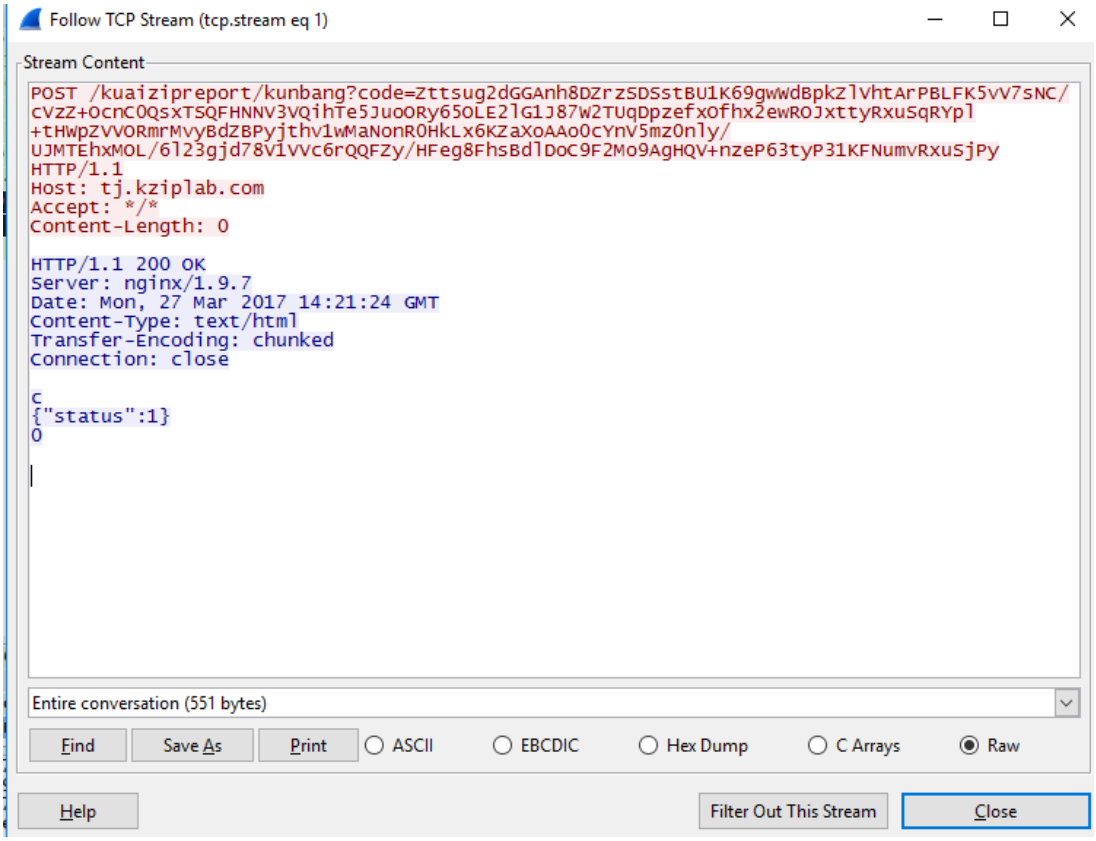
You can also click the Analyse menu and select Display Filters to create a new filter.



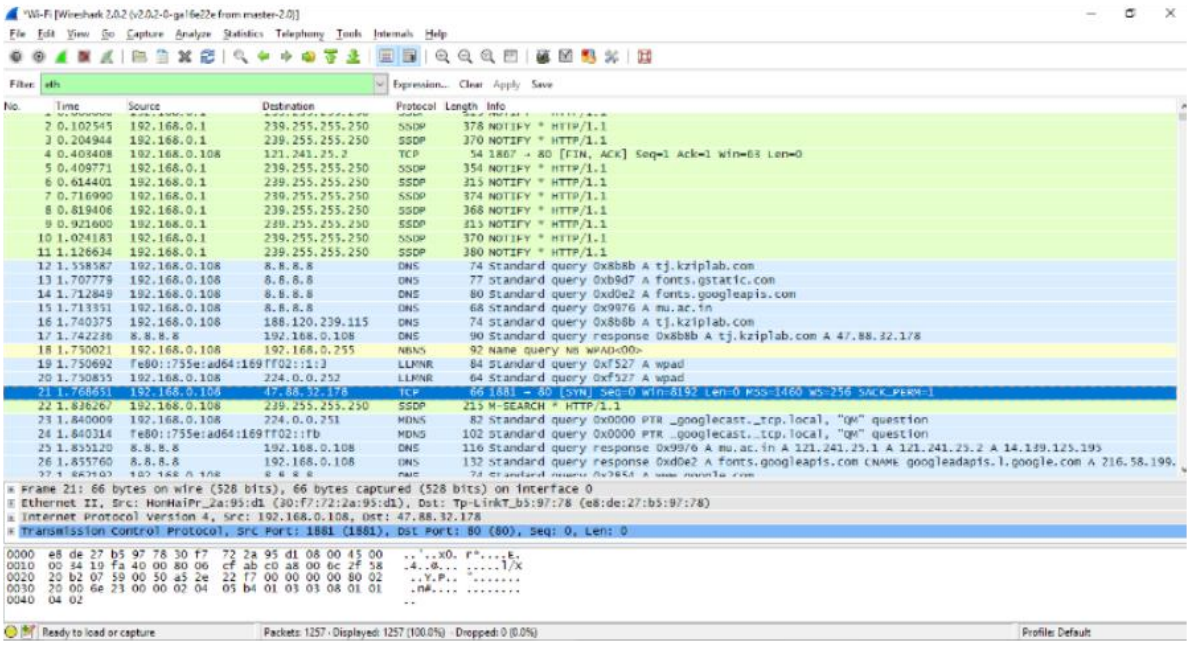
Another interesting thing you can do is right- click a packet and select Follow TCP Stream.



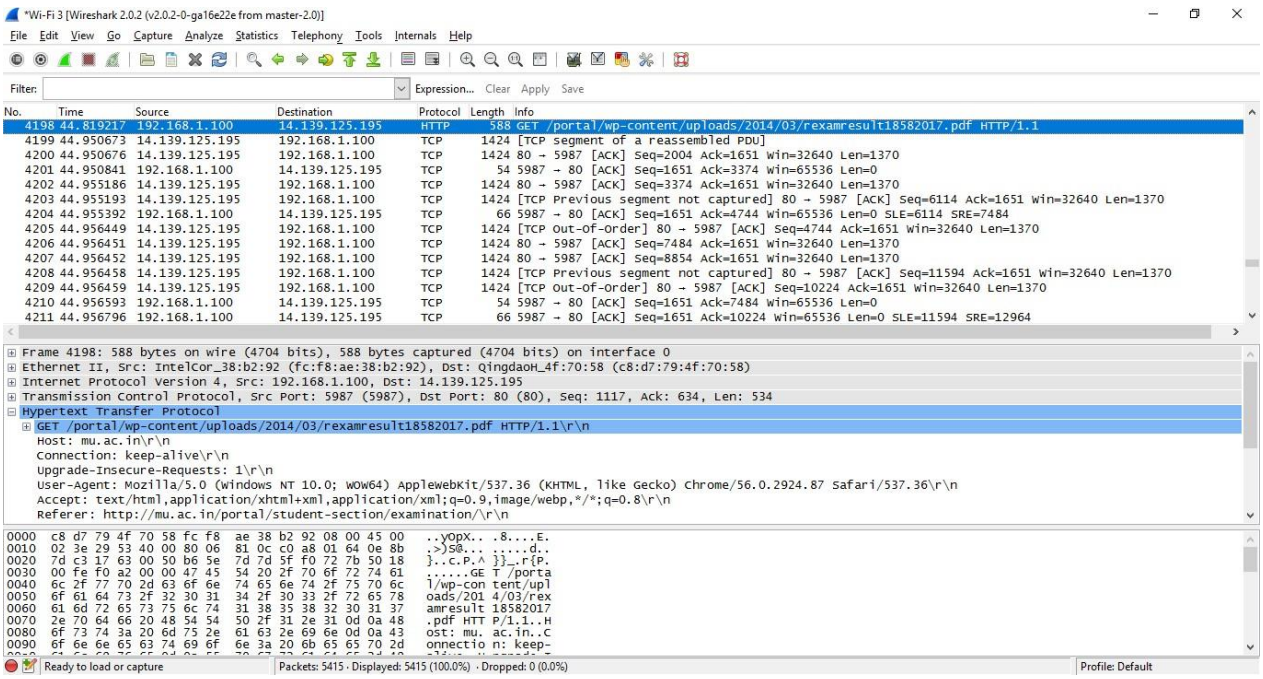
You'll see the full conversation between the client and the server.

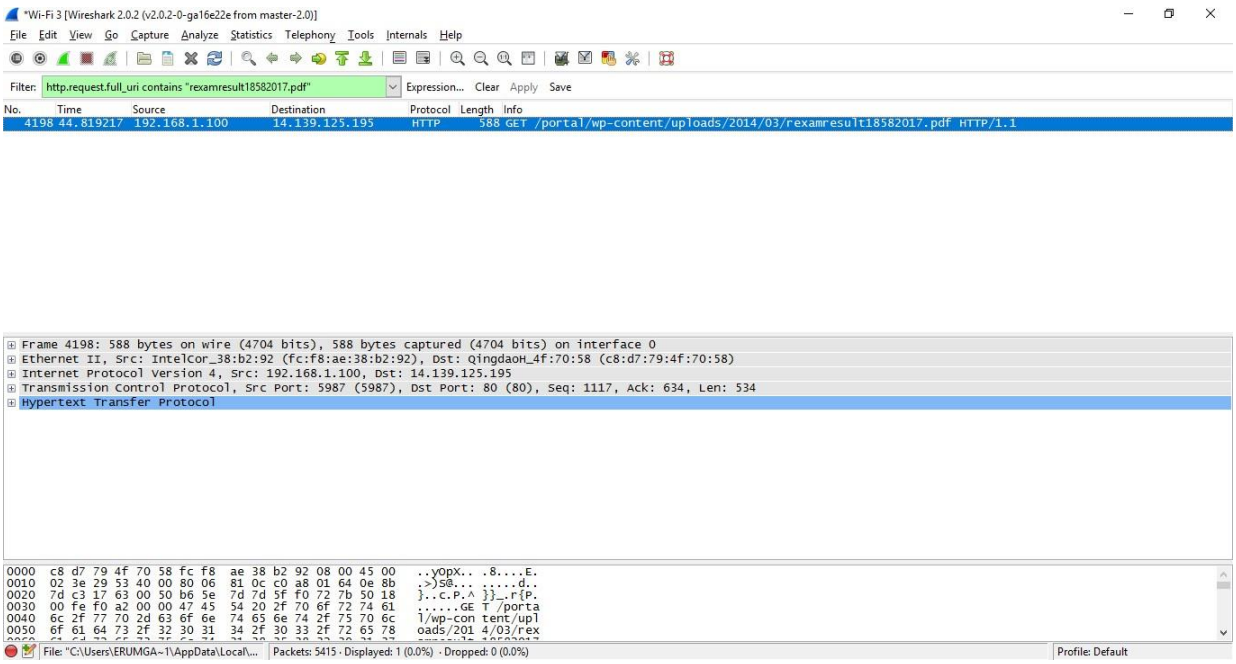


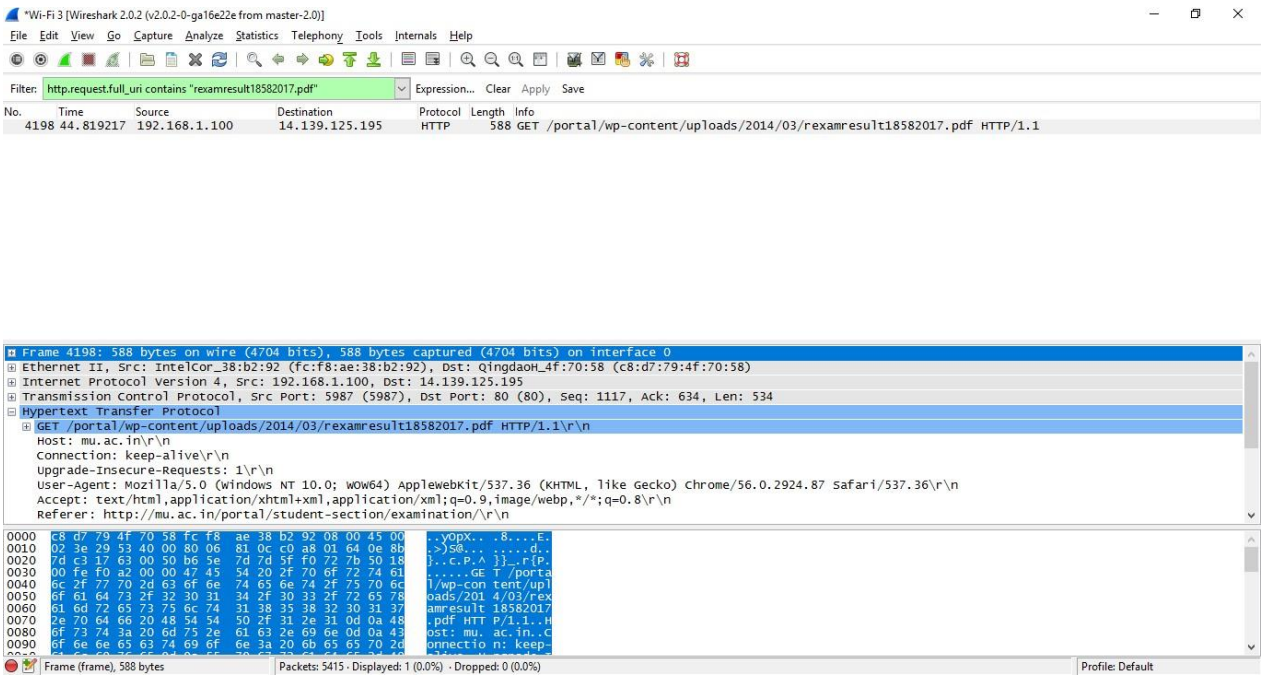
Close the window and you'll find a filter has been applied automatically —Wireshark is showing you the packets that make up the conversation.



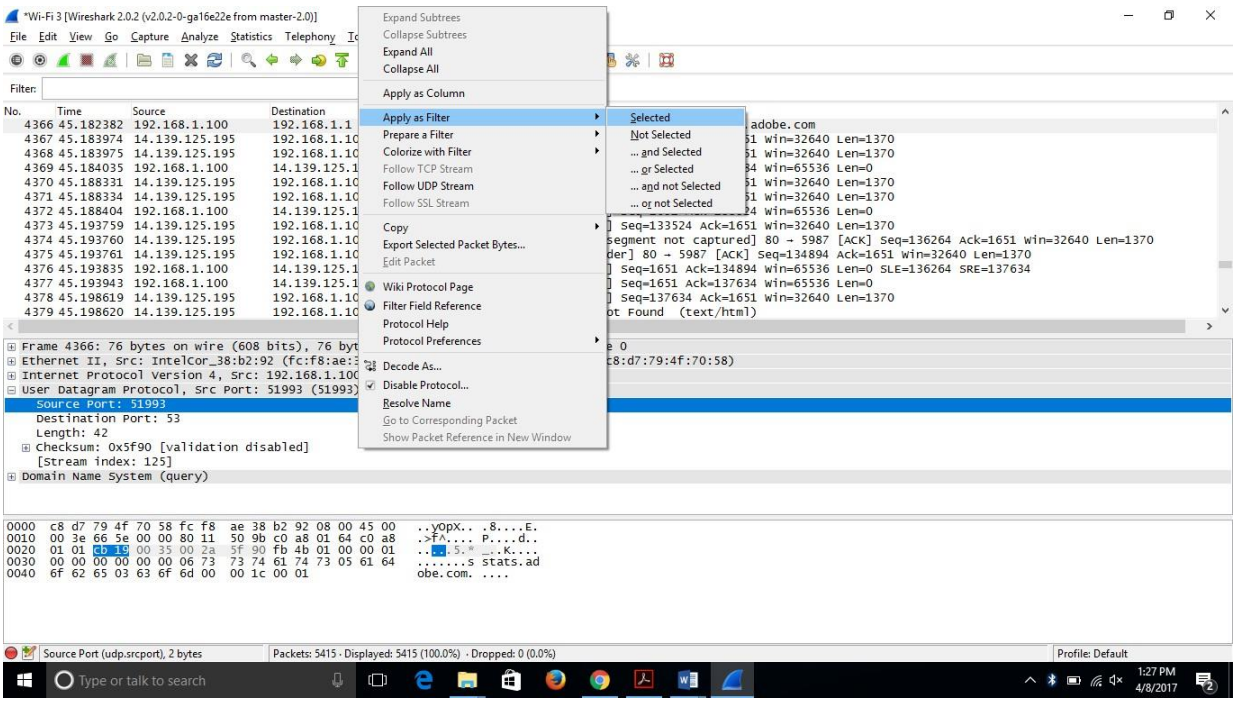
USING TRAFFIC CAPTURING AND ANALYSIS TOOLS

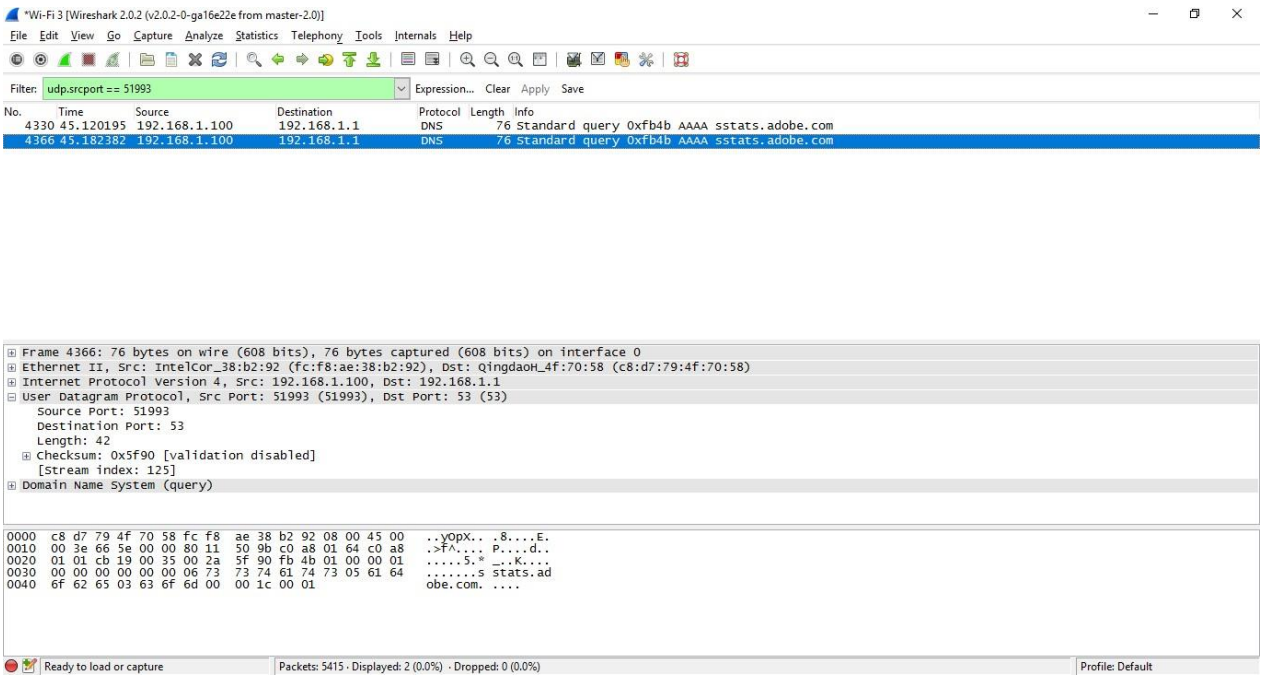


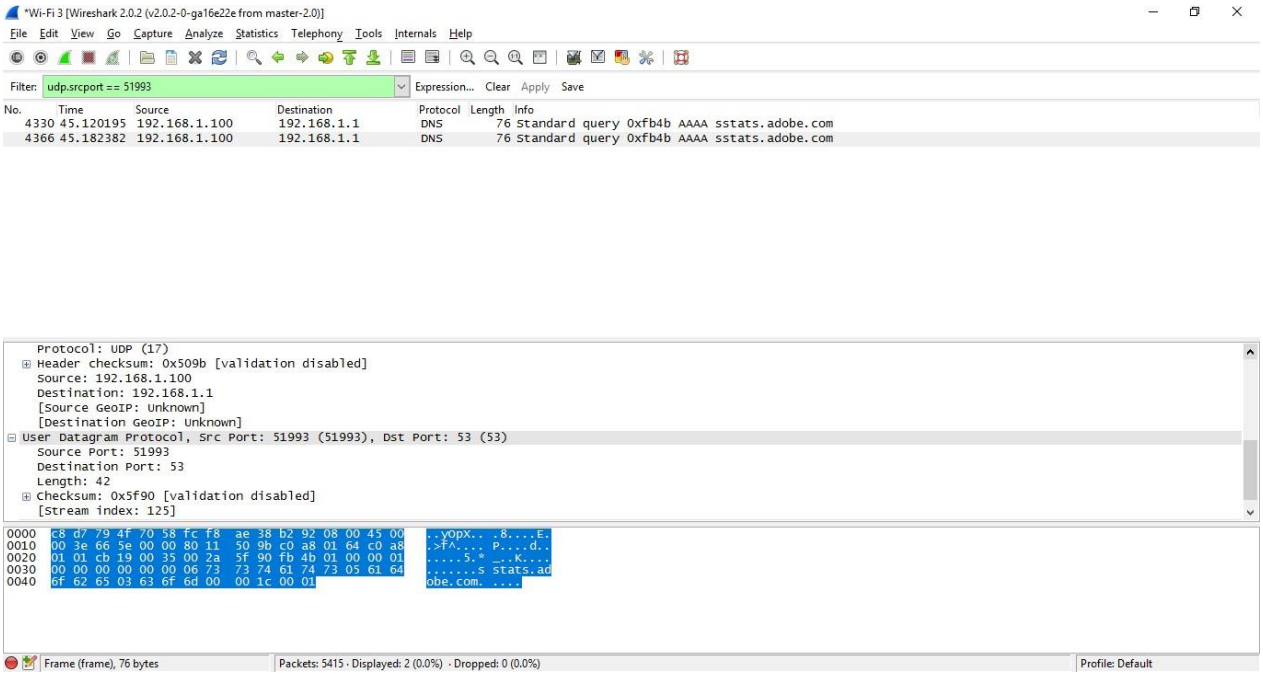




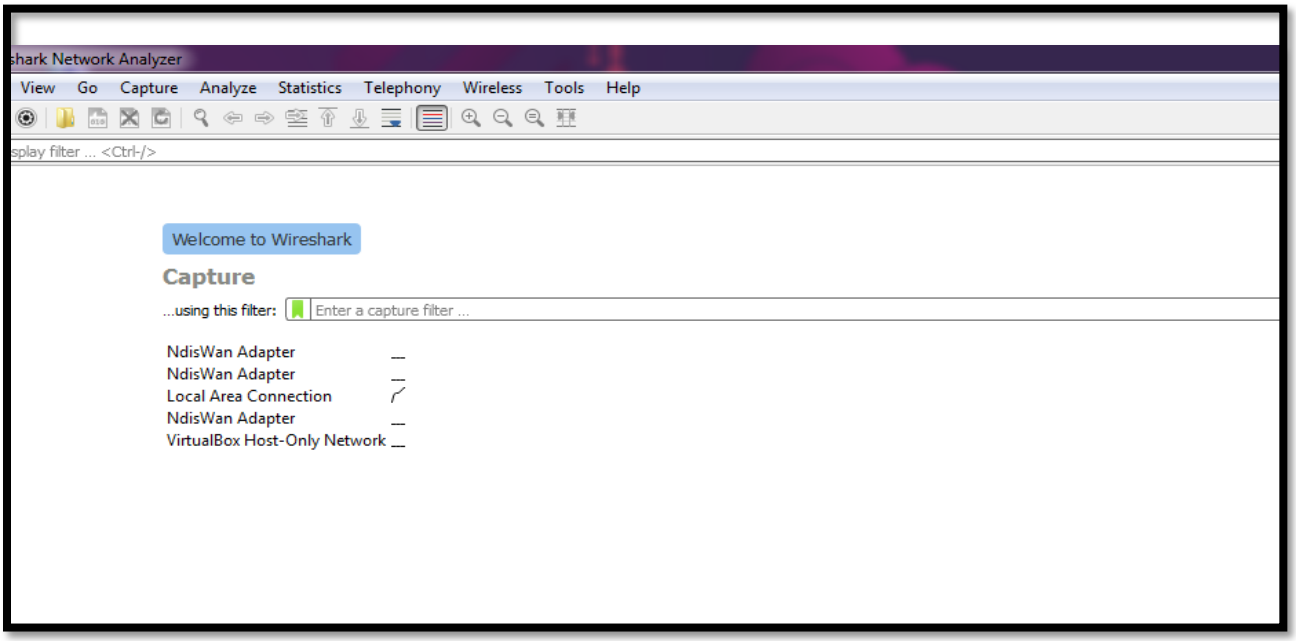
You can also create filters from here —just right- click one of the details and use the Apply as Filter submenu to create a filter based on it.

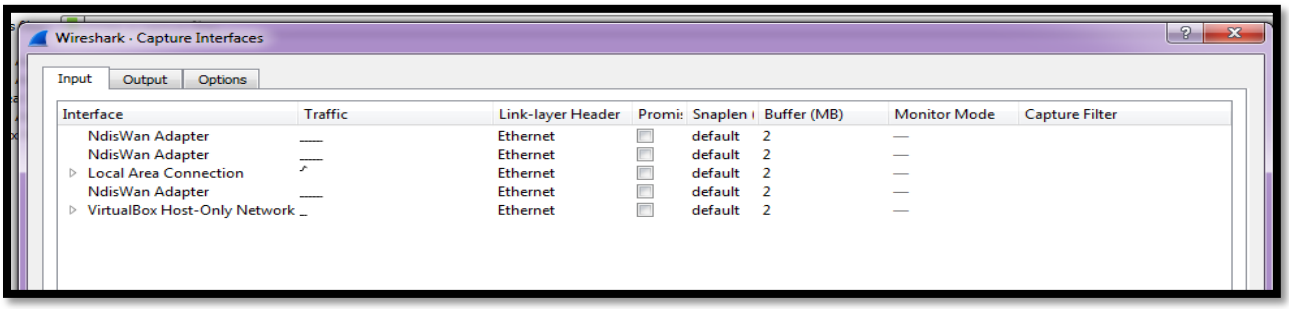

*Wi-Fi 3 [Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0)]
File Edit View Go Capture Analyze Statistics Telephony
Filter:
No. Time Source Destination
4366 45.182382 192.168.1.100 192.168.1.1
4367 45.183974 14.139.125.195 192.168.1.10
4368 45.183975 14.139.125.195 192.168.1.10
4369 45.184035 192.168.1.100 14.139.125.1
4370 45.188331 14.139.125.195 192.168.1.10
4371 45.188334 14.139.125.195 192.168.1.10
4372 45.188404 192.168.1.100 14.139.125.1
4373 45.193759 14.139.125.195 192.168.1.10
4374 45.193760 14.139.125.195 192.168.1.10
4375 45.193761 14.139.125.195 192.168.1.10
4376 45.193835 192.168.1.100 14.139.125.1
4377 45.193943 192.168.1.100 14.139.125.1
4378 45.198619 14.139.125.195 192.168.1.10
4379 45.198620 14.139.125.195 192.168.1.10
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Edit Packet
Wiki Protocol Page
Filter Field Reference
Protocol Help
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Show Packet Reference in New Window
Selected
Not Selected
... and Selected
... or Selected
... and not Selected
... or not Selected
Frame 4366: 76 bytes on wire (608 bits), 76 byt
Ethernet II, Src: IntelCor_38:b2:92 (fc:f8:ae:3
Internet Protocol Version 4, Src: 192.168.1.10
User Datagram Protocol, Src Port: 51993 (51993)
Source Port: 51993
Destination Port: 53
Length: 42
Checksum: 0x5f90 [validation disabled]
[Stream index: 125]
Domain Name System (query)
0000 c8 d7 79 4f 70 58 fc f8 ae 38 b2 92 08 00 45 00
0010 00 3e 66 5e 00 00 80 11 50 9b c0 a8 01 64 c0 a8
0020 01 01 cb 19 00 35 00 2a 5f 90 fb 4b 01 00 00 01
0030 00 00 00 00 00 00 06 73 73 74 61 74 73 05 61 64
0040 6f 62 65 03 63 6f 6d 00 00 1c 00 01
Source Port (udp.srcport), 2 bytes
Packets: 5415 · Displayed: 5415 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type or talk to search
1:27 PM
4/8/2017

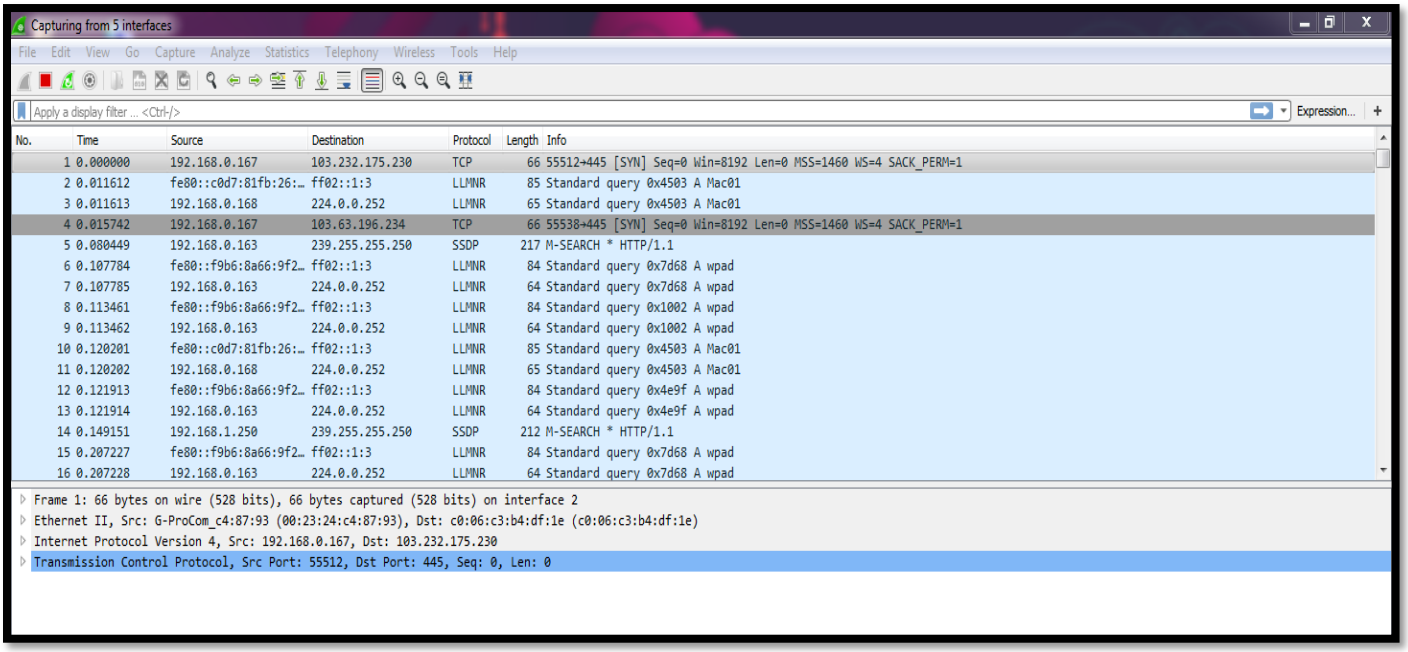

*Wi-Fi 3 [Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: udp.srcport == 51993
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
4330 45.120195 192.168.1.100 192.168.1.1 DNS 76 Standard query 0xfb4b AAAA sstats.adobe.com
4366 45.182382 192.168.1.100 192.168.1.1 DNS 76 Standard query 0xfb4b AAAA sstats.adobe.com
Frame 4366: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: IntelCor_38:b2:92 (fc:f8:ae:38:b2:92), Dst: QingdaoH_4f:70:58 (c8:d7:79:4f:70:58)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 51993 (51993), Dst Port: 53 (53)
Source Port: 51993
Destination Port: 53
Length: 42
Checksum: 0x5f90 [validation disabled]
[Stream index: 125]
Domain Name System (query)
0000 c8 d7 79 4f 70 58 fc f8 ae 38 b2 92 08 00 45 00
0010 00 3e 66 5e 00 00 80 11 50 9b c0 a8 01 64 c0 a8
0020 01 01 cb 19 00 35 00 2a 5f 90 fb 4b 01 00 00 01
0030 00 00 00 00 00 00 06 73 73 74 61 74 73 05 61 64
0040 6f 62 65 03 63 6f 6d 00 00 1c 00 01
Ready to load or capture
Packets: 5415 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

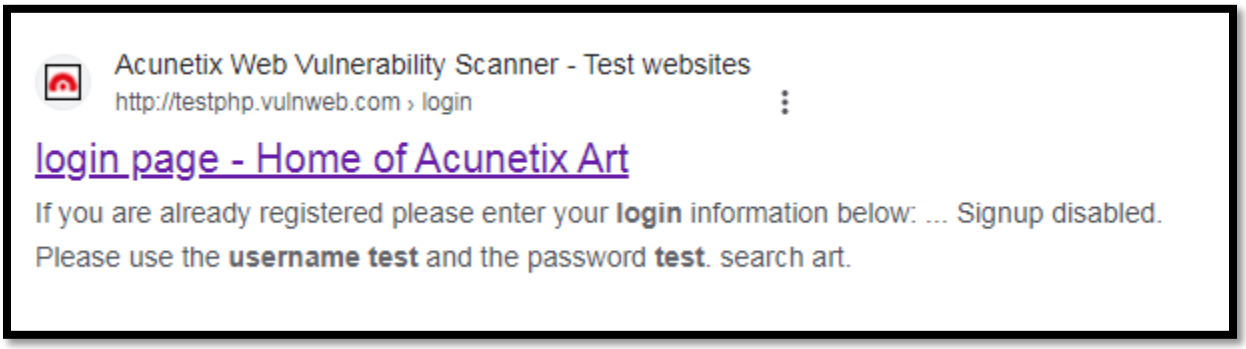


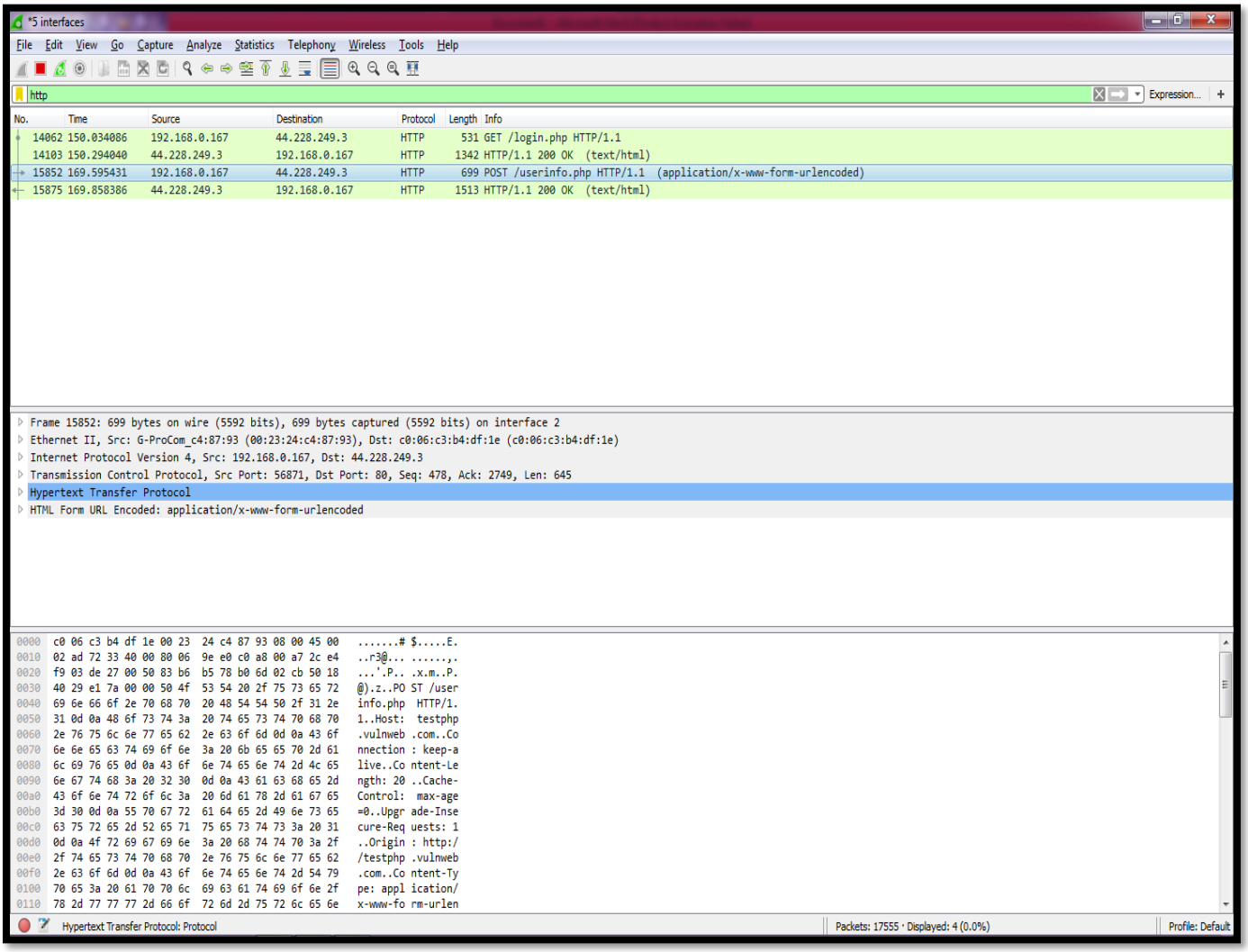
Use of wire shark to scan and check the packet information of following protocols

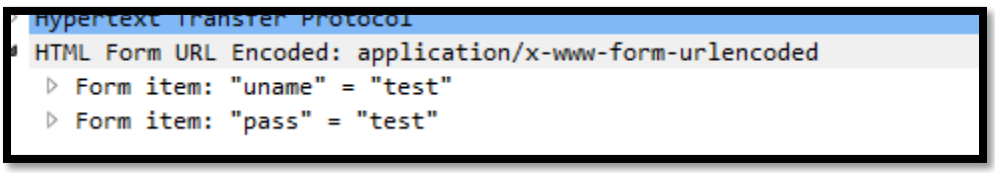



Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promi
Snaplen
Buffer (MB)
Monitor Mode
Capture Filter
NdisWan Adapter
Ethernet
default
2
Local Area Connection
VirtualBox Host-Only Network

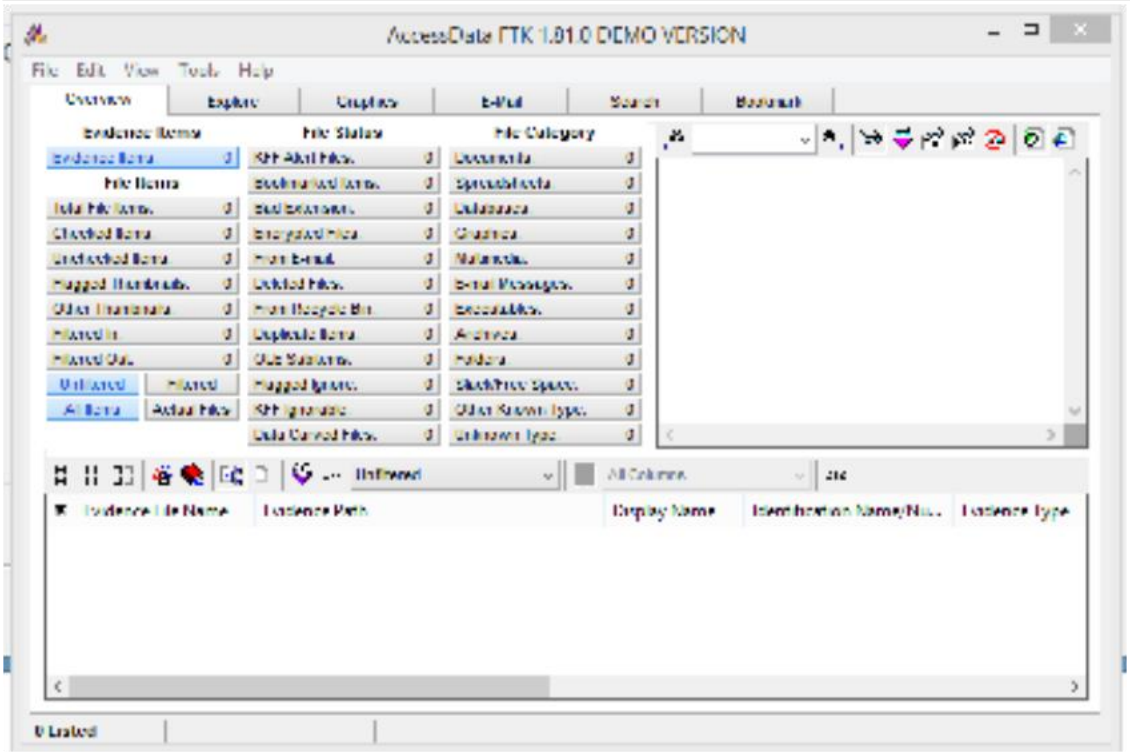

Capturing from 5 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.167 103.232.175.230 TCP 66 55512→445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2 0.011612 fe80::c0d7:81fb:26:… ff02::1:3 LLMNR 85 Standard query 0x4503 A Mac01
3 0.011613 192.168.0.168 224.0.0.252 LLMNR 65 Standard query 0x4503 A Mac01
4 0.015742 192.168.0.167 103.63.196.234 TCP 66 55538→445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
5 0.080449 192.168.0.163 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
6 0.107784 fe80::f9b6:8a66:9f2… ff02::1:3 LLMNR 84 Standard query 0x7d68 A wpad
7 0.107785 192.168.0.163 224.0.0.252 LLMNR 64 Standard query 0x7d68 A wpad
8 0.113461 fe80::f9b6:8a66:9f2… ff02::1:3 LLMNR 84 Standard query 0x1002 A wpad
9 0.113462 192.168.0.163 224.0.0.252 LLMNR 64 Standard query 0x1002 A wpad
10 0.120201 fe80::c0d7:81fb:26:… ff02::1:3 LLMNR 85 Standard query 0x4503 A Mac01
11 0.120202 192.168.0.168 224.0.0.252 LLMNR 65 Standard query 0x4503 A Mac01
12 0.121913 fe80::f9b6:8a66:9f2… ff02::1:3 LLMNR 84 Standard query 0x4e9f A wpad
13 0.121914 192.168.0.163 224.0.0.252 LLMNR 64 Standard query 0x4e9f A wpad
14 0.149151 192.168.1.250 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
15 0.207227 fe80::f9b6:8a66:9f2… ff02::1:3 LLMNR 84 Standard query 0x7d68 A wpad
16 0.207228 192.168.0.163 224.0.0.252 LLMNR 64 Standard query 0x7d68 A wpad
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 103.232.175.230
Transmission Control Protocol, Src Port: 55512, Dst Port: 445, Seq: 0, Len: 0

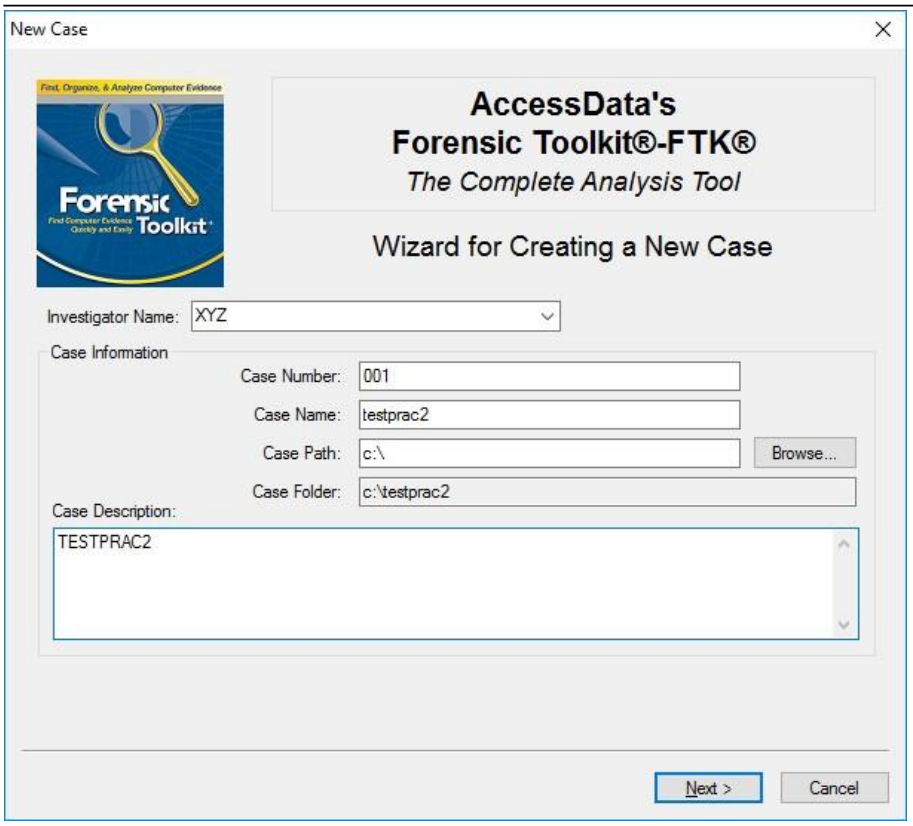

Acunetix Web Vulnerability Scanner - Test websites
http://testphp.vulnweb.com › login
login page - Home of Acunetix Art
If you are already registered please enter your login information below: ... Signup disabled.
Please use the username test and the password test. search art.

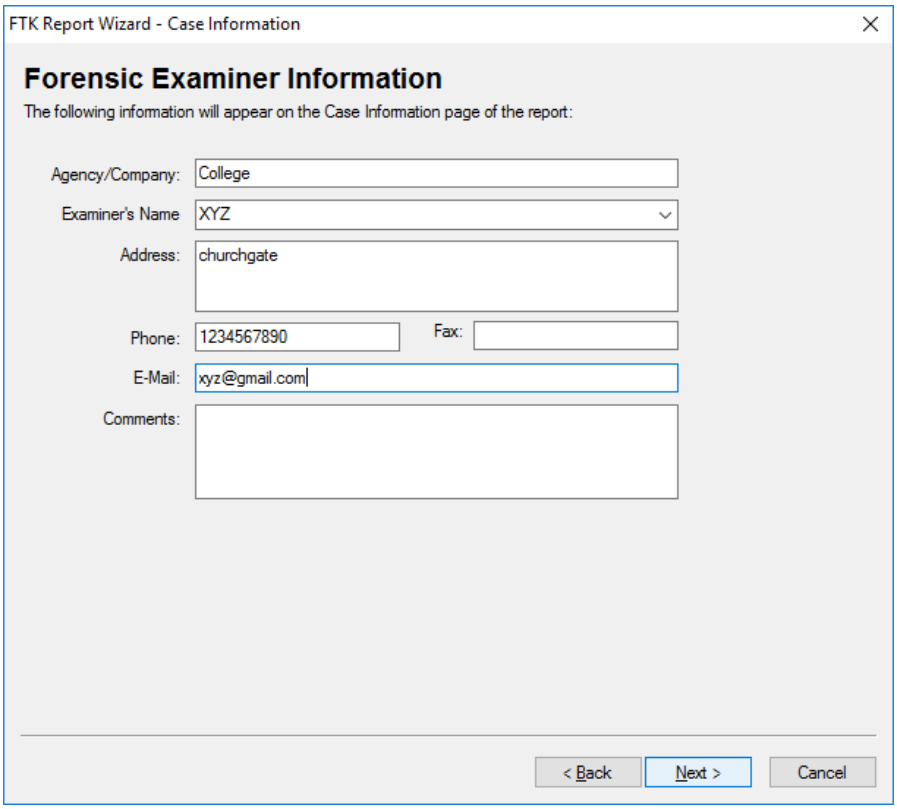

*5 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Length Info
14062 150.034086 192.168.0.167 44.228.249.3 HTTP 531 GET /login.php HTTP/1.1
14103 150.294040 44.228.249.3 192.168.0.167 HTTP 1342 HTTP/1.1 200 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 20 6b 65 65 70 2d 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 live..Co ntent-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 20 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..Co ntent-Ty
0100 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 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: Protocol
Packets: 17555 · Displayed: 4 (0.0%)
Profile: Default

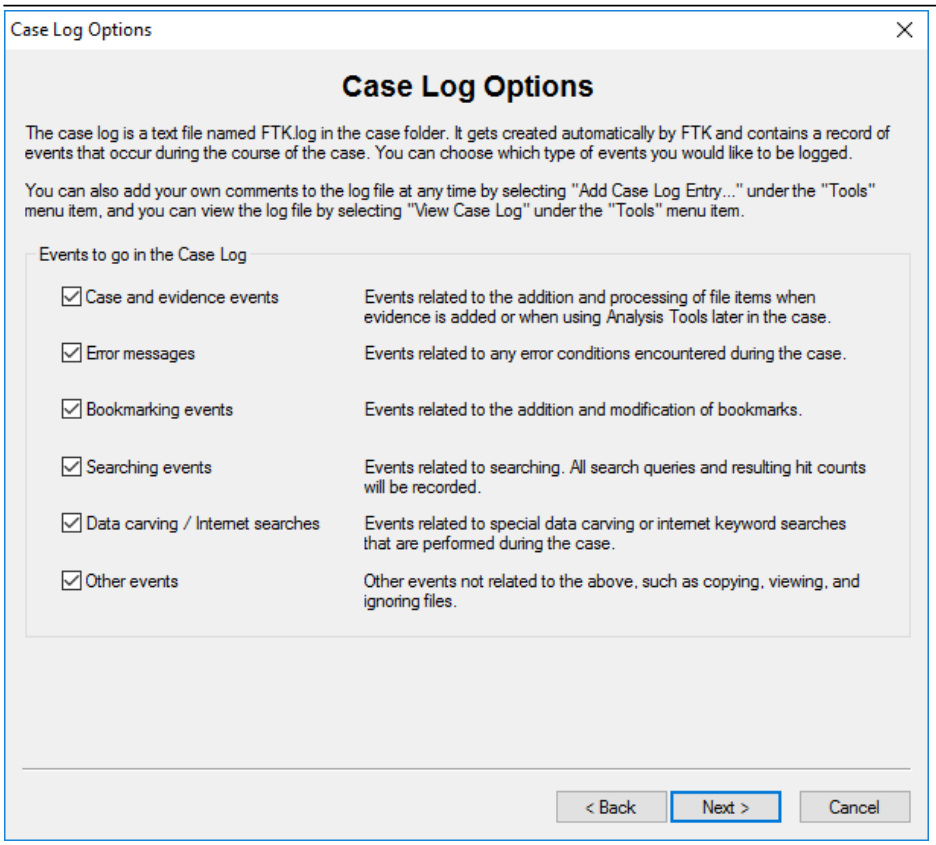

Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test"
Form item: "pass" = "test"

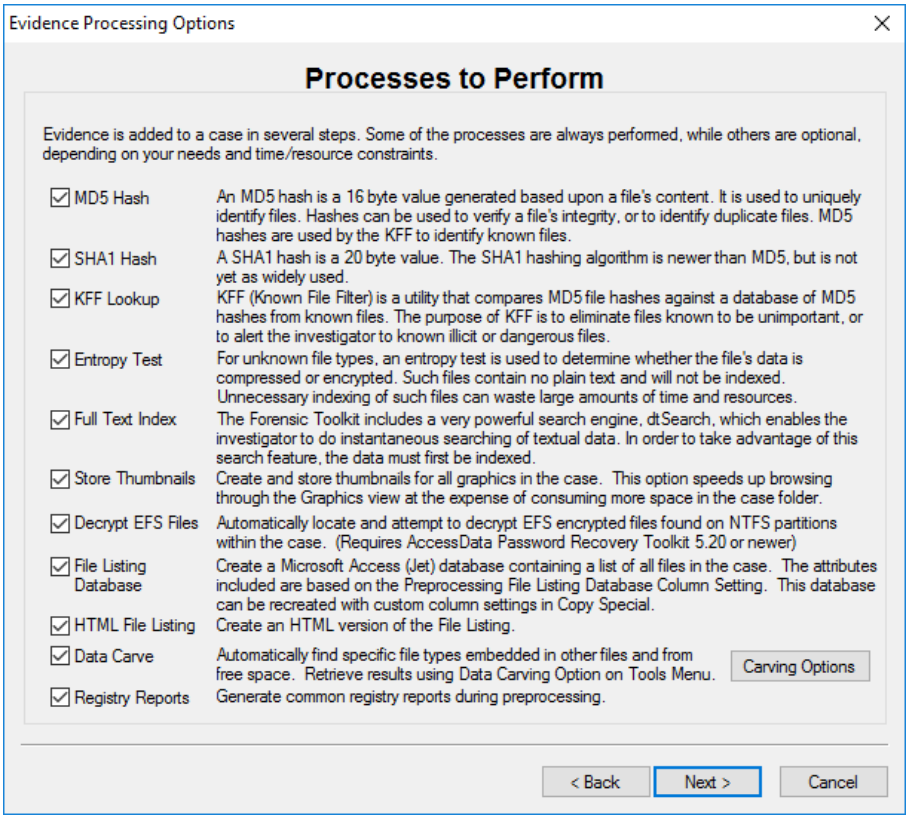
PRACTICAL NO 07: Use tools that scan a hard drive, locate deleted media and scan hard drive. (FTK)

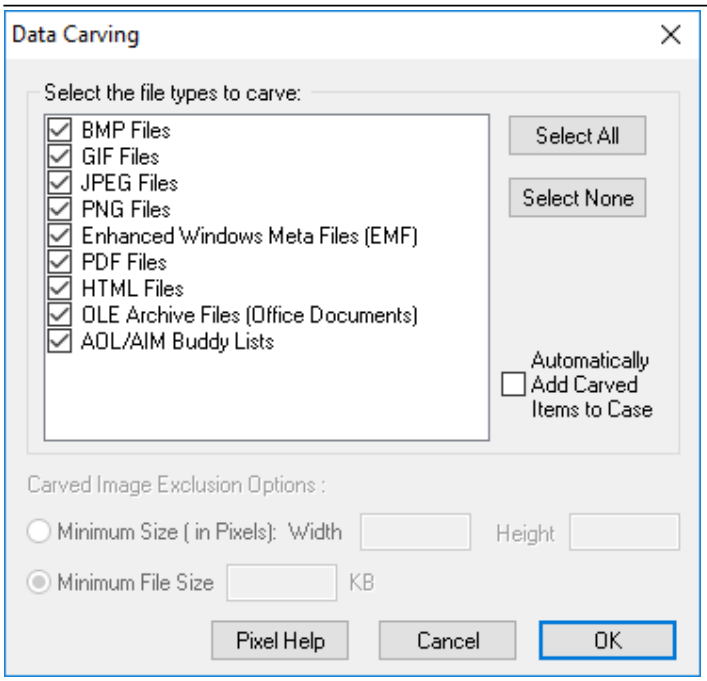


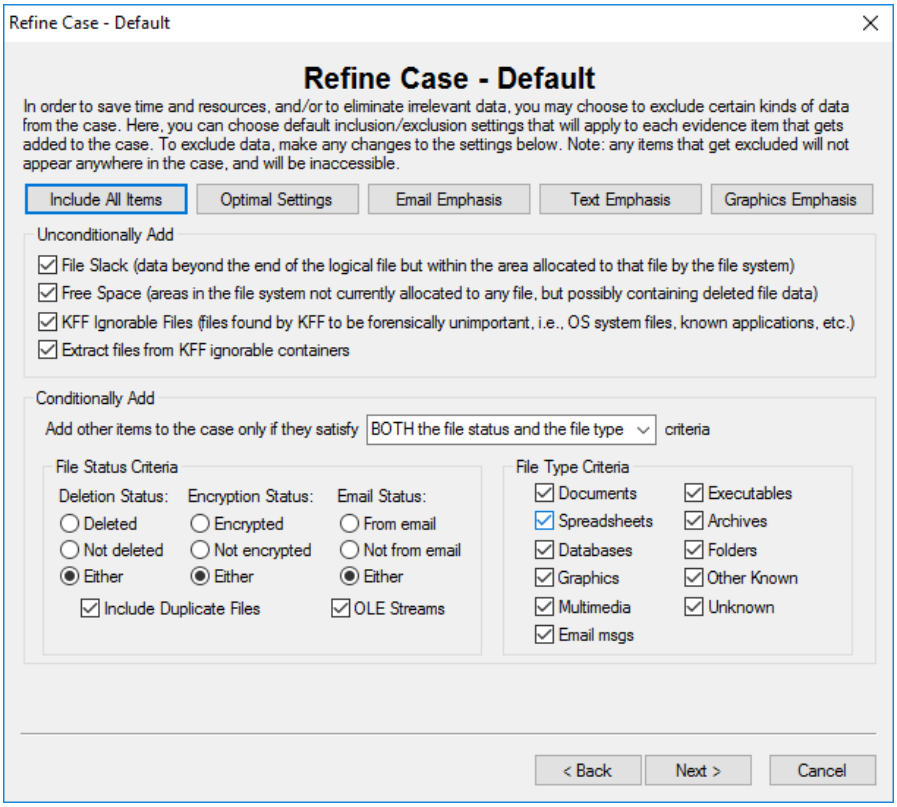

New Case
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Creating a New Case
Investigator Name: XYZ
Case Information
Case Number: 001
Case Name: testprac2
Case Path: c:\
Browse...
Case Folder: c:\testprac2
Case Description:
TESTPRAC2
Next >
Cancel

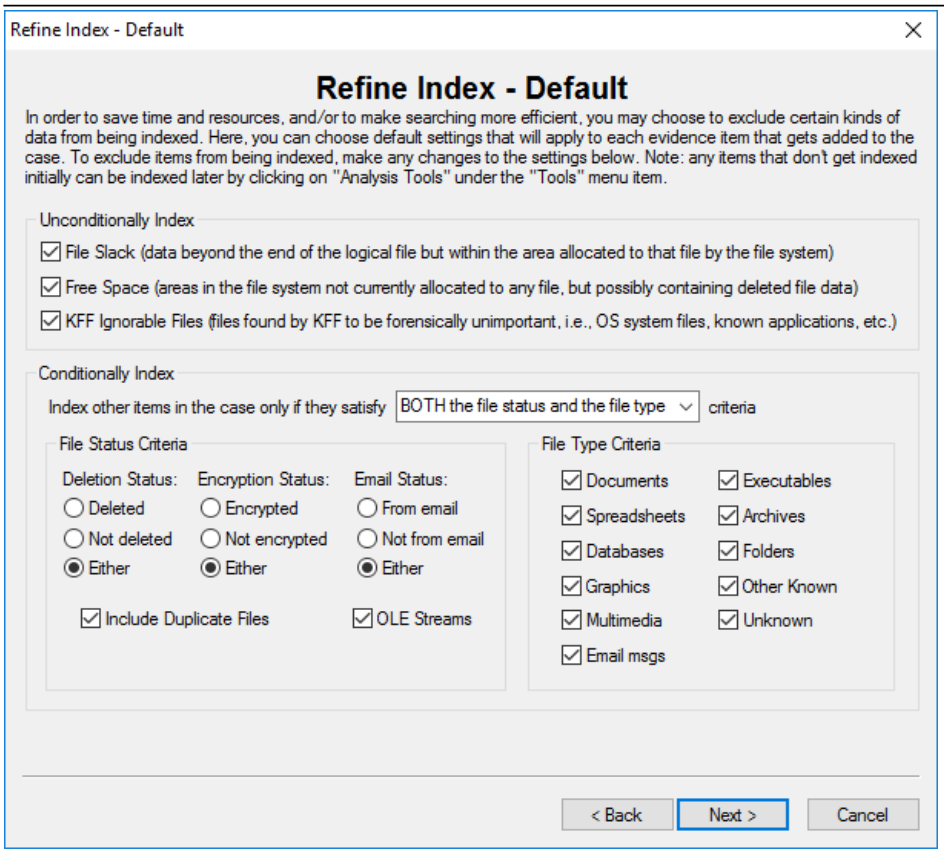

FTK Report Wizard - Case Information
Forensic Examiner Information
The following information will appear on the Case Information page of the report:
Agency/Company: College
Examiner's Name XYZ
Address: churchgate
Phone: 1234567890
Fax:
E-Mail: xyz@gmail.com
Comments:
< Back
Next >
Cancel

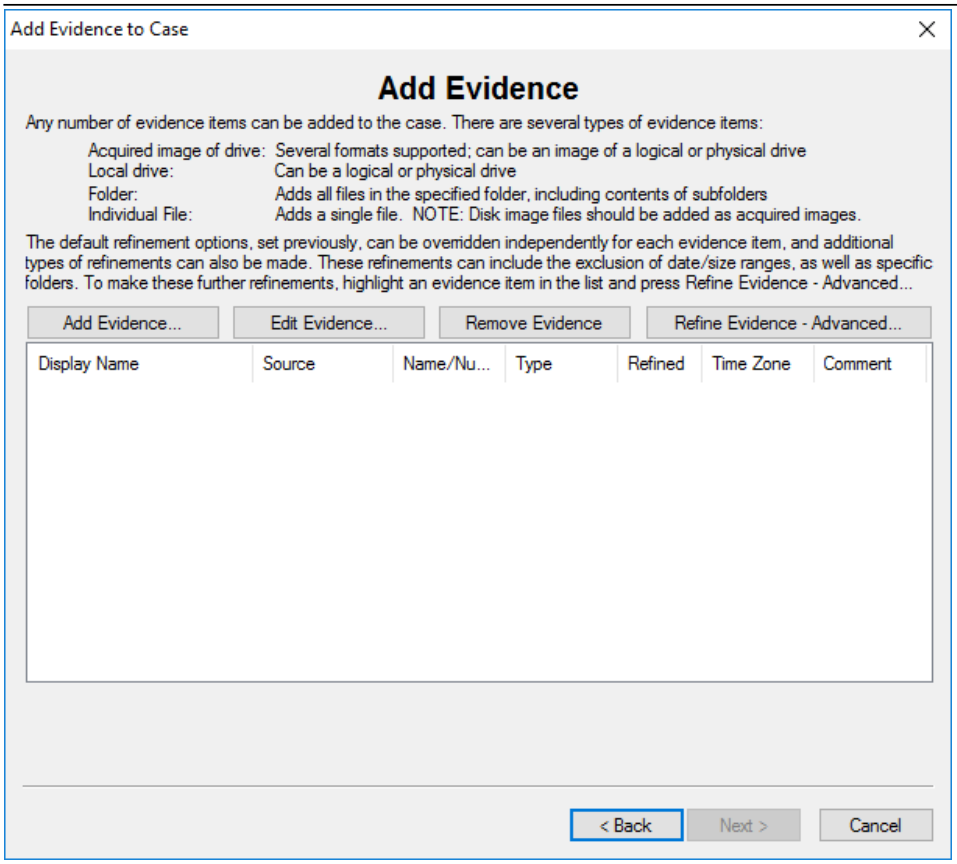

Case Log Options
Case Log Options
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.
Events to go in the Case Log
Case and evidence events
Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Error messages
Events related to any error conditions encountered during the case.
Bookmarking events
Events related to the addition and modification of bookmarks.
Searching events
Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches
Events related to special data carving or internet keyword searches that are performed during the case.
Other events
Other events not related to the above, such as copying, viewing, and ignoring files.
< Back
Next >
Cancel

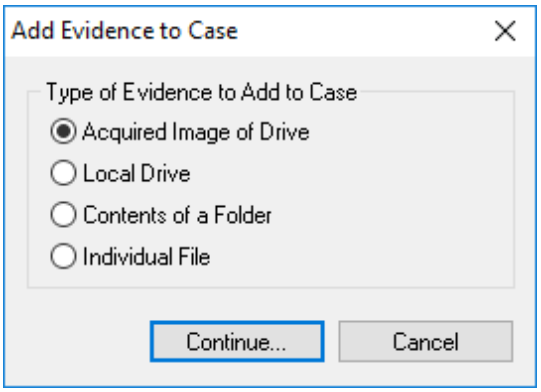

Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel

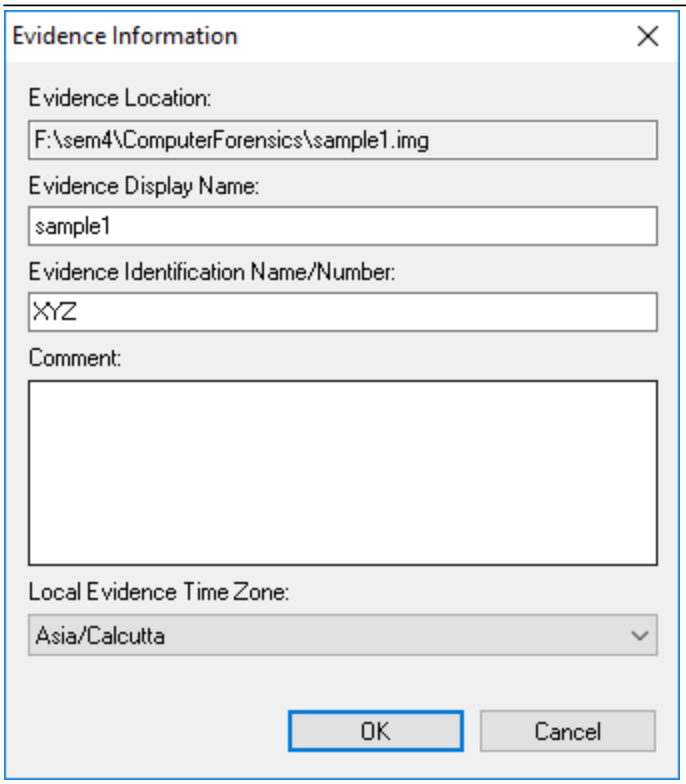

Data Carving
Select the file types to carve:
BMP Files
GIF Files
JPEG Files
PNG Files
Enhanced Windows Meta Files (EMF)
PDF Files
HTML Files
OLE Archive Files (Office Documents)
AOL/AIM Buddy Lists
Select All
Select None
Automatically Add Carved Items to Case
Carved Image Exclusion Options :
Minimum Size (in Pixels): Width
Height
Minimum File Size
KB
Pixel Help
Cancel
OK

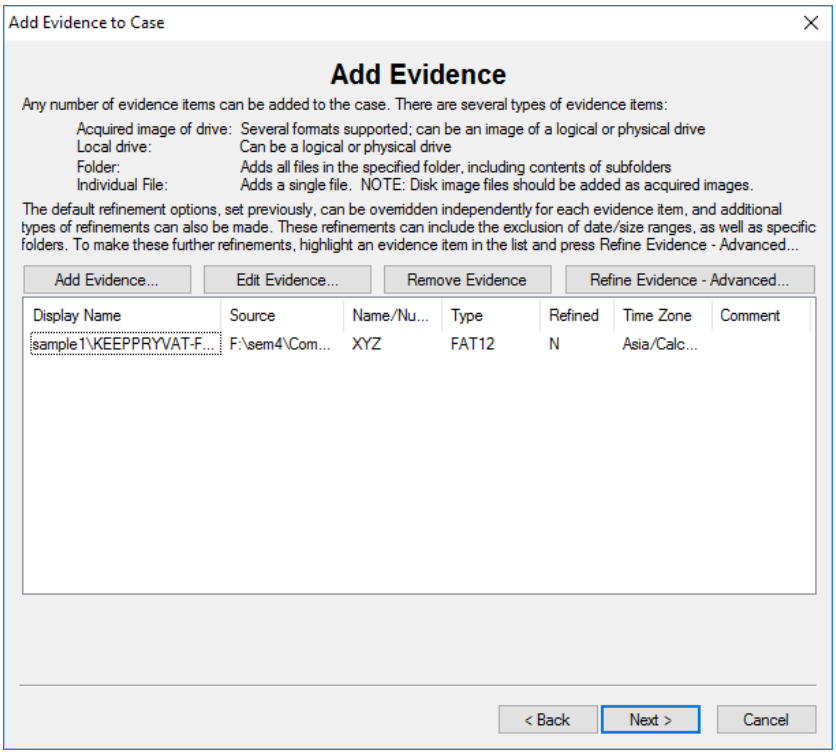

Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy
BOTH the file status and the file type
criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel

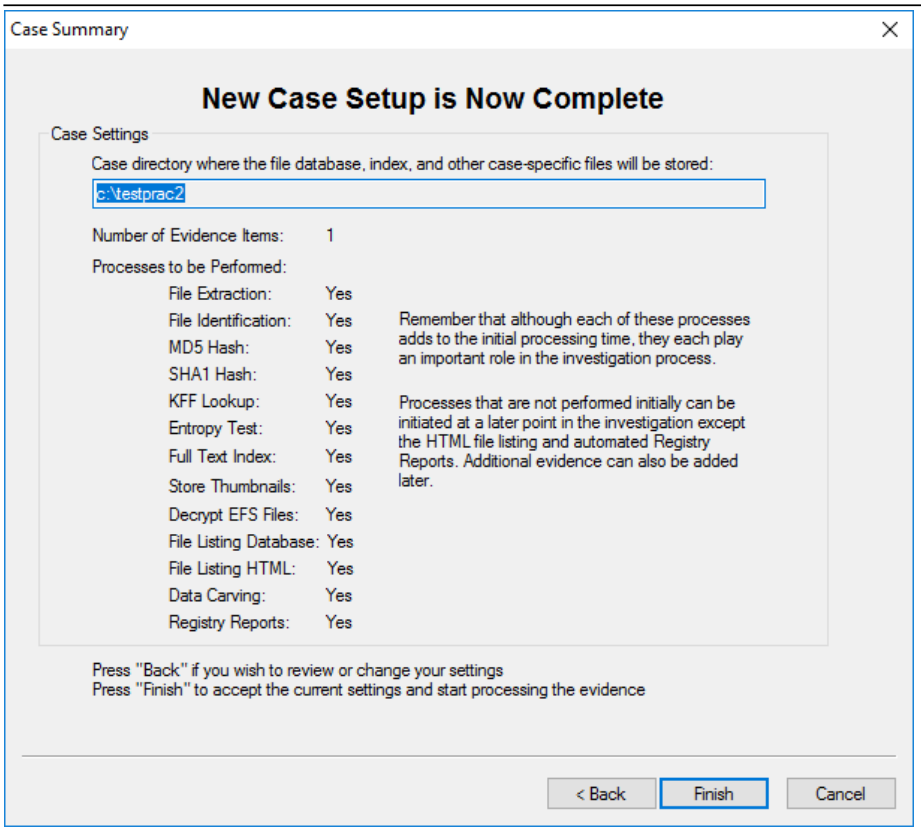

Refine Index - Default
Refine Index - Default
In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude 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
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Executables
Spreadsheets
Archives
Databases
Folders
Graphics
Other Known
Multimedia
Unknown
Email msgs
< Back
Next >
Cancel

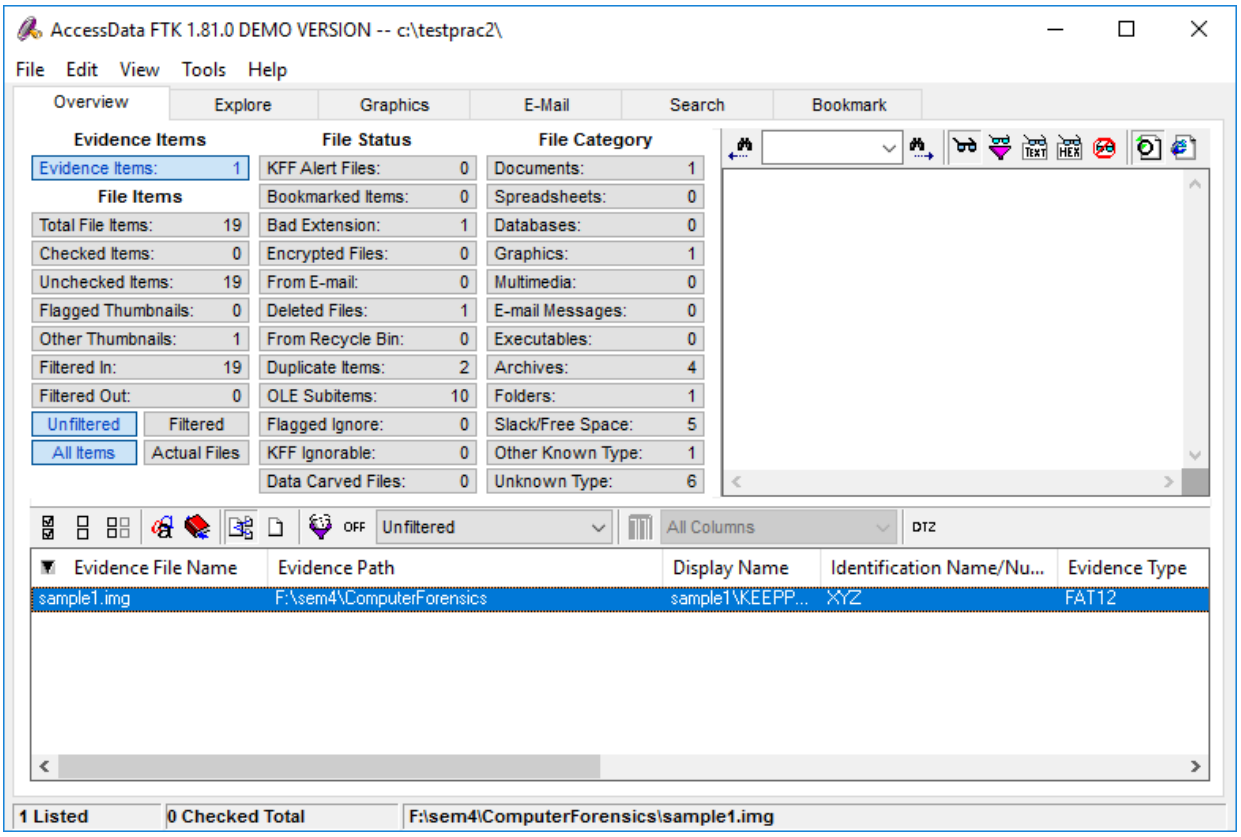

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files 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

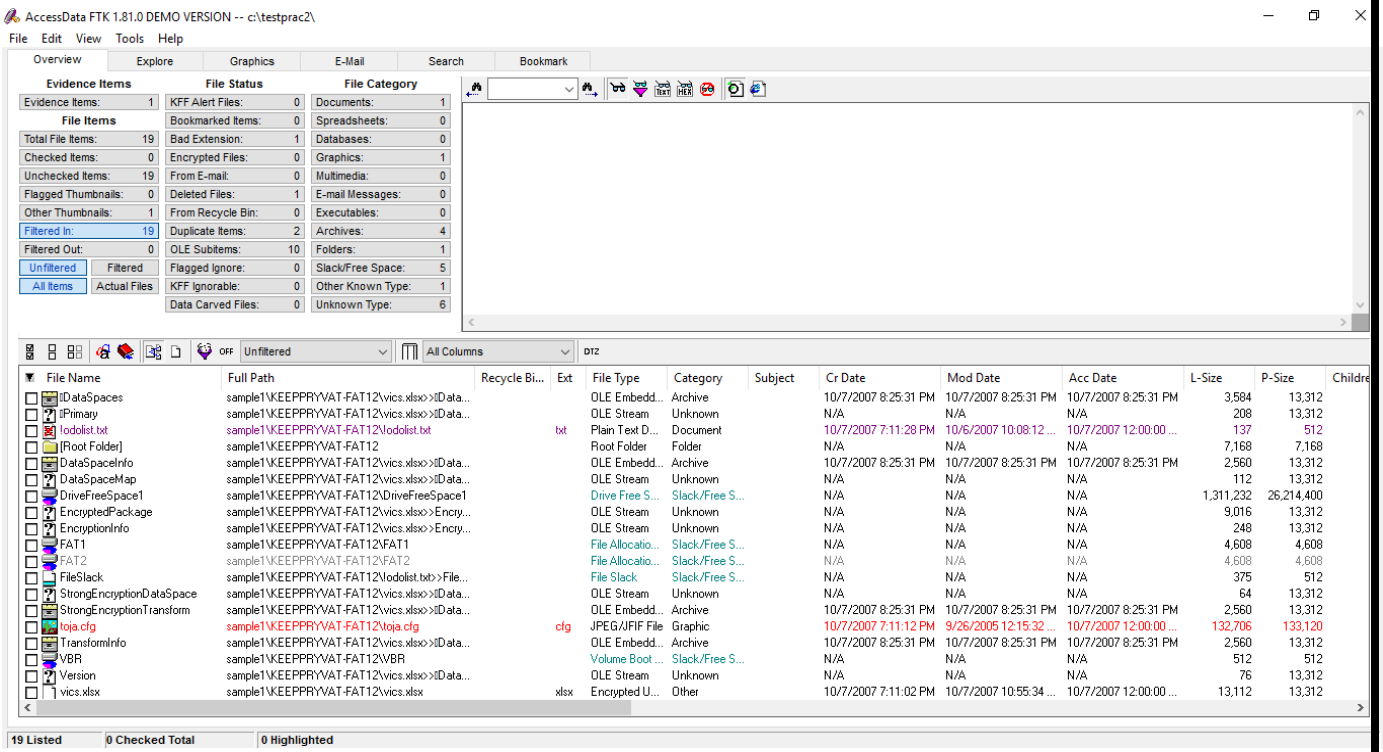

Add Evidence to Case
Type of Evidence to Add to Case
Acquired Image of Drive
Local Drive
Contents of a Folder
Individual File
Continue...
Cancel

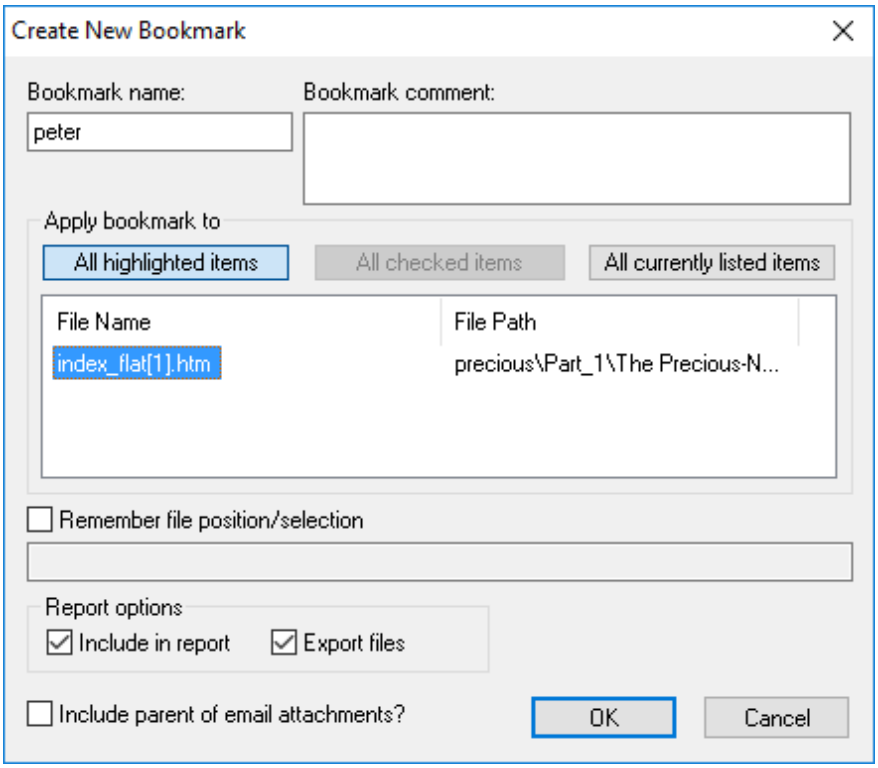

Evidence Information
Evidence Location:
F:\sem4\ComputerForensics\sample1.img
Evidence Display Name:
sample1
Evidence Identification Name/Number:
XYZ
Comment:
Local Evidence Time Zone:
Asia/Calcutta
OK
Cancel

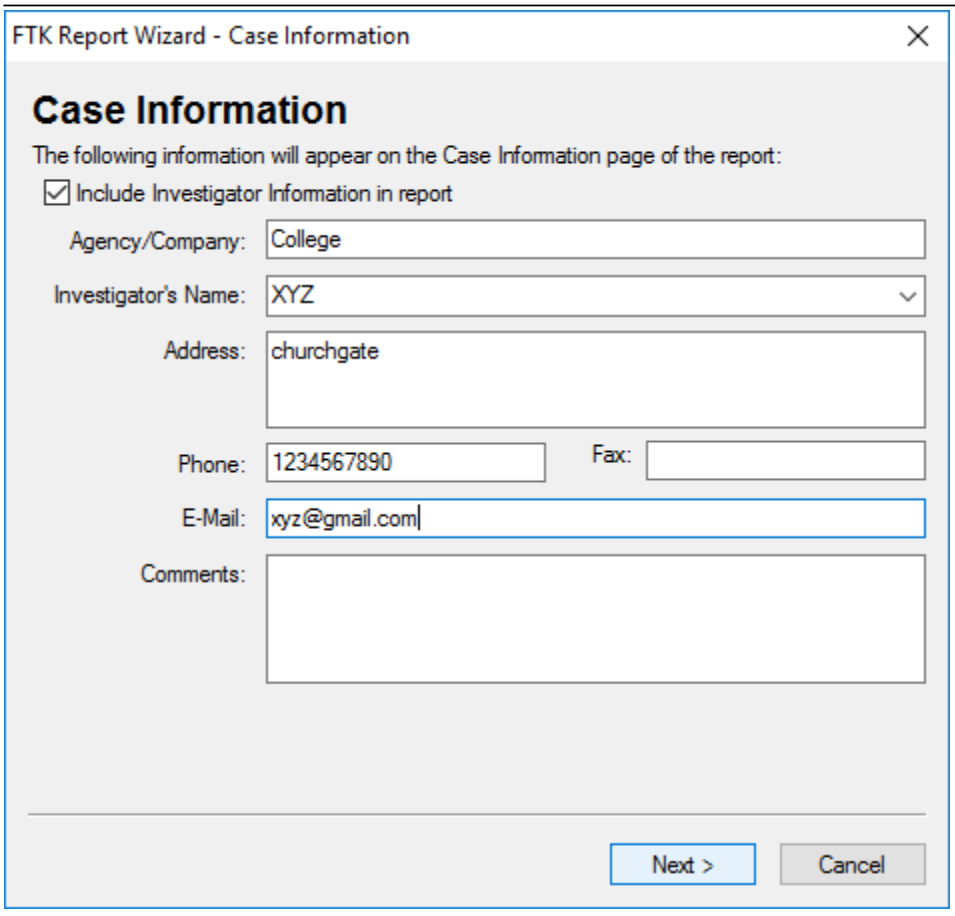

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files 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

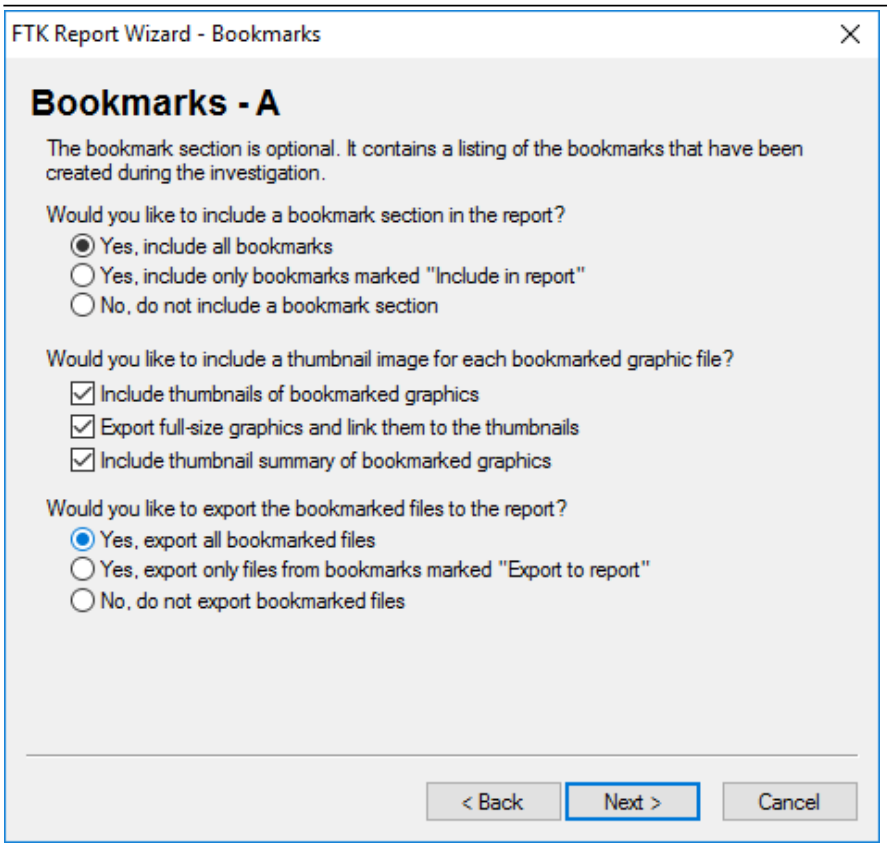

Case Summary
New Case Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
c:\testprac2
Number of Evidence Items: 1
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
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
Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
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.
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

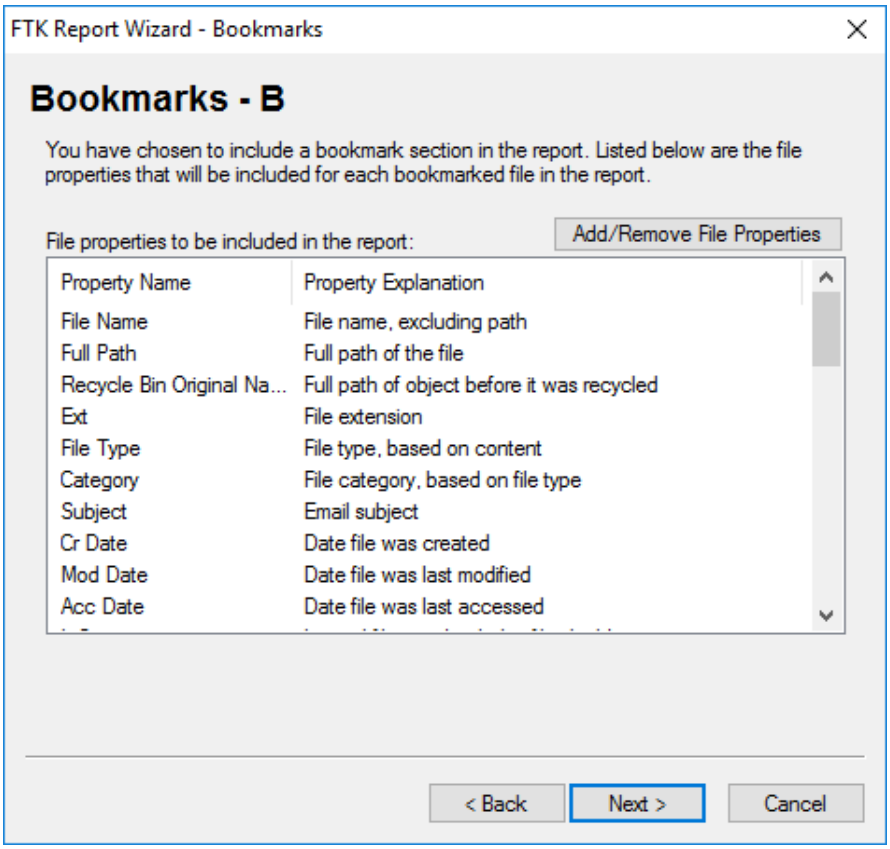

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Evidence Items
Evidence Items: 1
File Items
Total File Items: 19
Checked Items: 0
Unchecked Items: 19
Flagged Thumbnails: 0
Other Thumbnails: 1
Filtered In: 19
Filtered Out: 0
Unfiltered Filtered
All Items Actual Files
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 1
Encrypted Files: 0
From E-mail: 0
Deleted Files: 1
From Recycle Bin: 0
Duplicate Items: 2
OLE Subitems: 10
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 1
Spreadsheets: 0
Databases: 0
Graphics: 1
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 4
Folders: 1
Slack/Free Space: 5
Other Known Type: 1
Unknown Type: 6
OFF Unfiltered All Columns DTZ
Evidence File Name Evidence Path Display Name Identification Name/Nu... Evidence Type
sample1.img F:\sem4\ComputerForensics sample1\KEEPP... XYZ FAT12
1 Listed 0 Checked Total F:\sem4\ComputerForensics\sample1.img

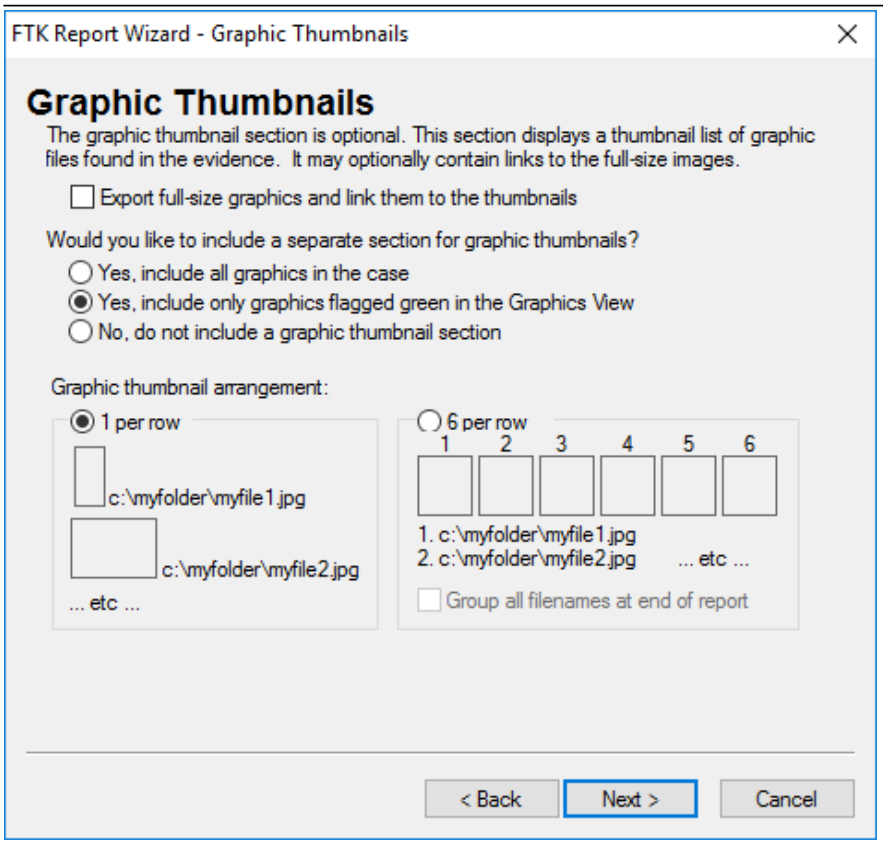

AccessData FTK 1.81.0 DEMO VERSION -- c:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
File Name Full Path Recycle Bi... Ext File Type Category Subject Cr Date Mod Date Acc Date L-Size P-Size
19 Listed 0 Checked Total 0 Highlighted

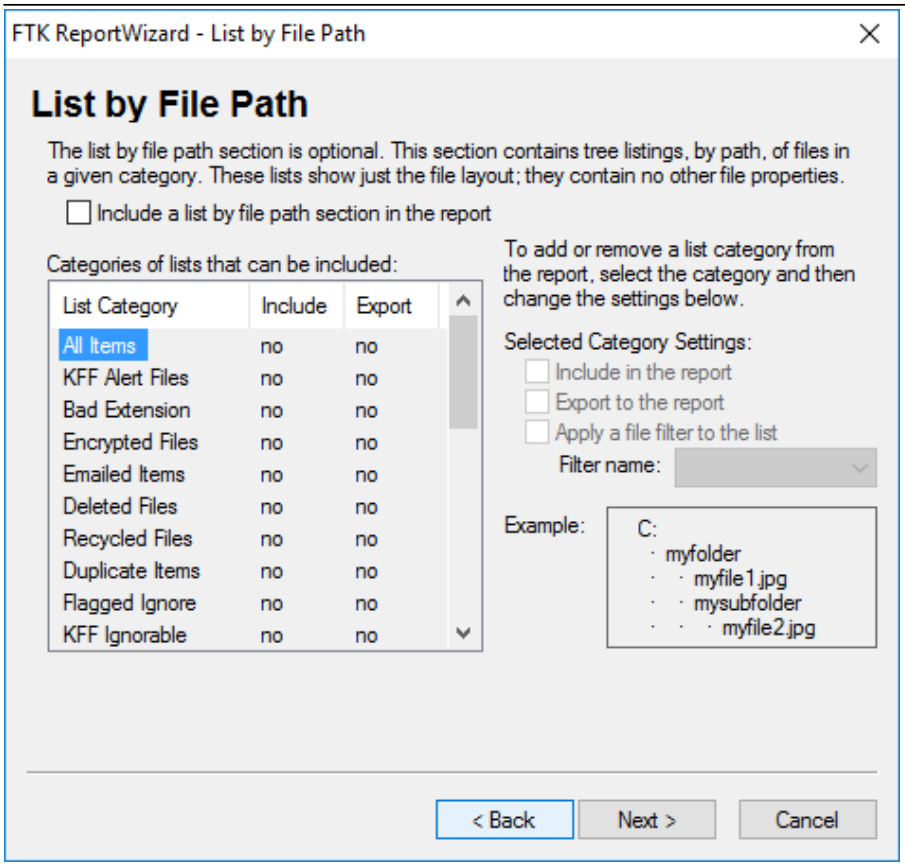

Create New Bookmark
Bookmark name:
peter
Bookmark comment:
Apply bookmark to
All highlighted items
All checked items
All currently listed items
File Name
File Path
index_flat[1].htm
precious\Part_1\The Precious-N...
Remember file position/selection
Report options
Include in report
Export files
Include parent of email attachments?
OK
Cancel

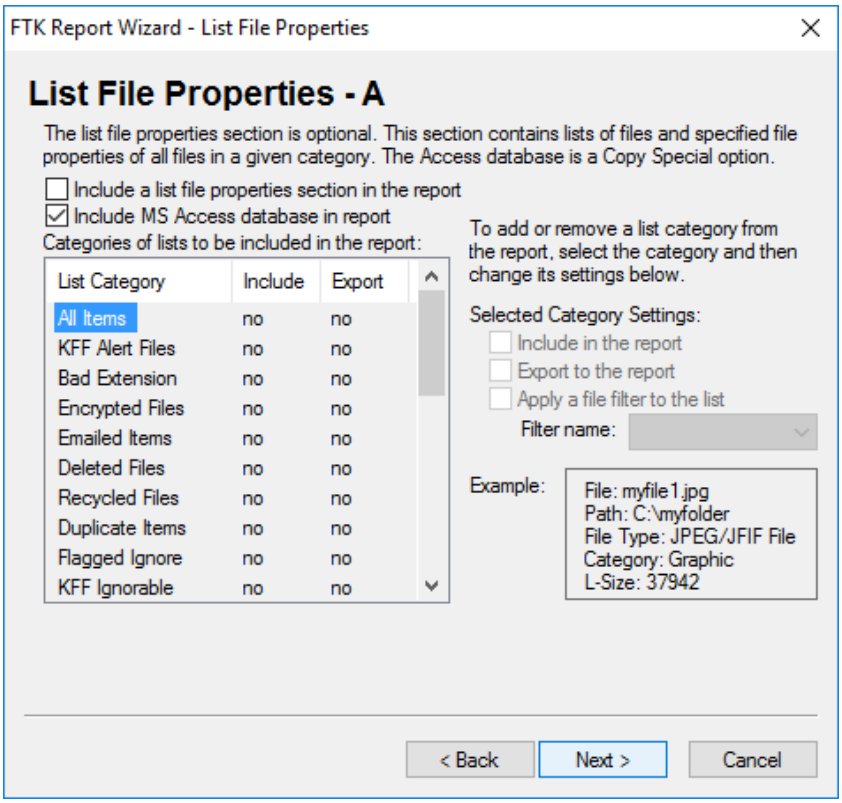

FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator Information in report
Agency/Company:
College
Investigator's Name:
XYZ
Address:
churchgate
Phone:
1234567890
Fax:
E-Mail:
xyz@gmail.com
Comments:
Next >
Cancel

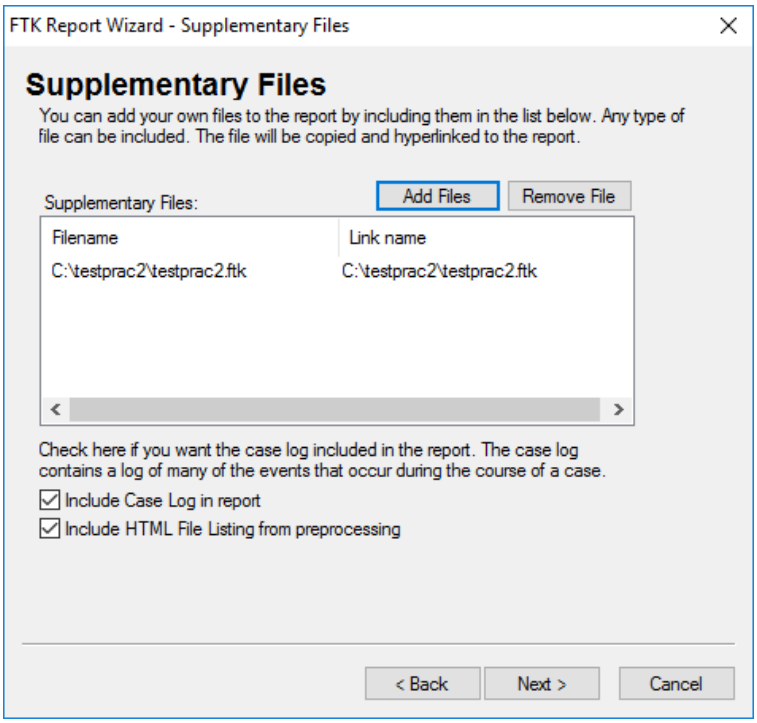

FTK Report Wizard - Bookmarks
Bookmarks - A
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.
Would you like to include a bookmark section in the report?
Yes, include all bookmarks
Yes, include only bookmarks marked "Include in report"
No, do not include a bookmark section
Would you like to include a thumbnail image for each bookmarked graphic file?
Include thumbnails of bookmarked graphics
Export full-size graphics and link them to the thumbnails
Include thumbnail summary of bookmarked graphics
Would you like to export the bookmarked files to the report?
Yes, export all bookmarked files
Yes, export only files from bookmarks marked "Export to report"
No, do not export bookmarked files
< Back
Next >
Cancel

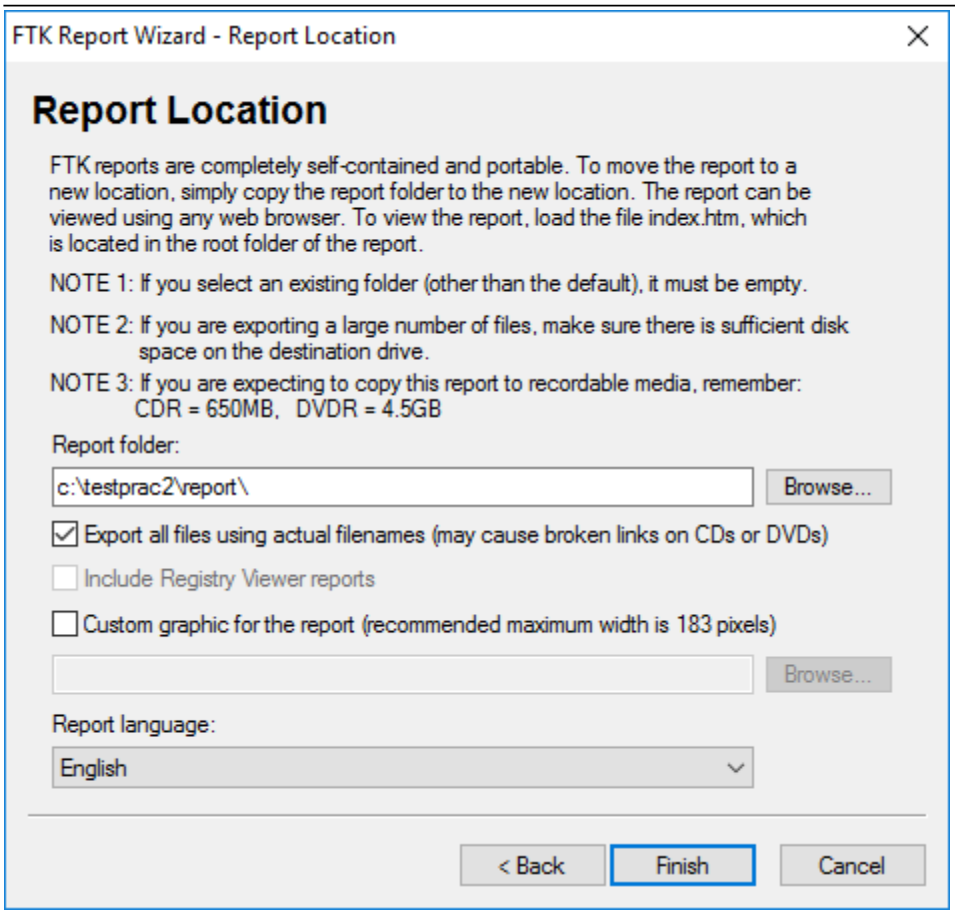

FTK Report Wizard - Bookmarks
Bookmarks - B
You have chosen to include a bookmark section in the report. Listed below are the file properties that will be included for each bookmarked file in the report.
File properties to be included in the report:
Add/Remove File Properties
Property Name
Property Explanation
File Name
File name, excluding path
Full Path
Full path of the file
Recycle Bin Original Na...
Full path of object before it was recycled
Ext
File extension
File Type
File type, based on content
Category
File category, based on file type
Subject
Email subject
Cr Date
Date file was created
Mod Date
Date file was last modified
Acc Date
Date file was last accessed
< Back
Next >
Cancel


FTK Report Wizard - Graphic Thumbnails
Graphic Thumbnails
The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.
Export full-size graphics and link them to the thumbnails
Would you like to include a separate section for graphic thumbnails?
Yes, include all graphics in the case
Yes, include only graphics flagged green in the Graphics View
No, do not include a graphic thumbnail section
Graphic thumbnail arrangement:
1 per row
c:\myfolder\myfile1.jpg
c:\myfolder\myfile2.jpg
... etc ...
6 per row
1 2 3 4 5 6
1. c:\myfolder\myfile1.jpg
2. c:\myfolder\myfile2.jpg
... etc ...
Group all filenames at end of report
< Back
Next >
Cancel

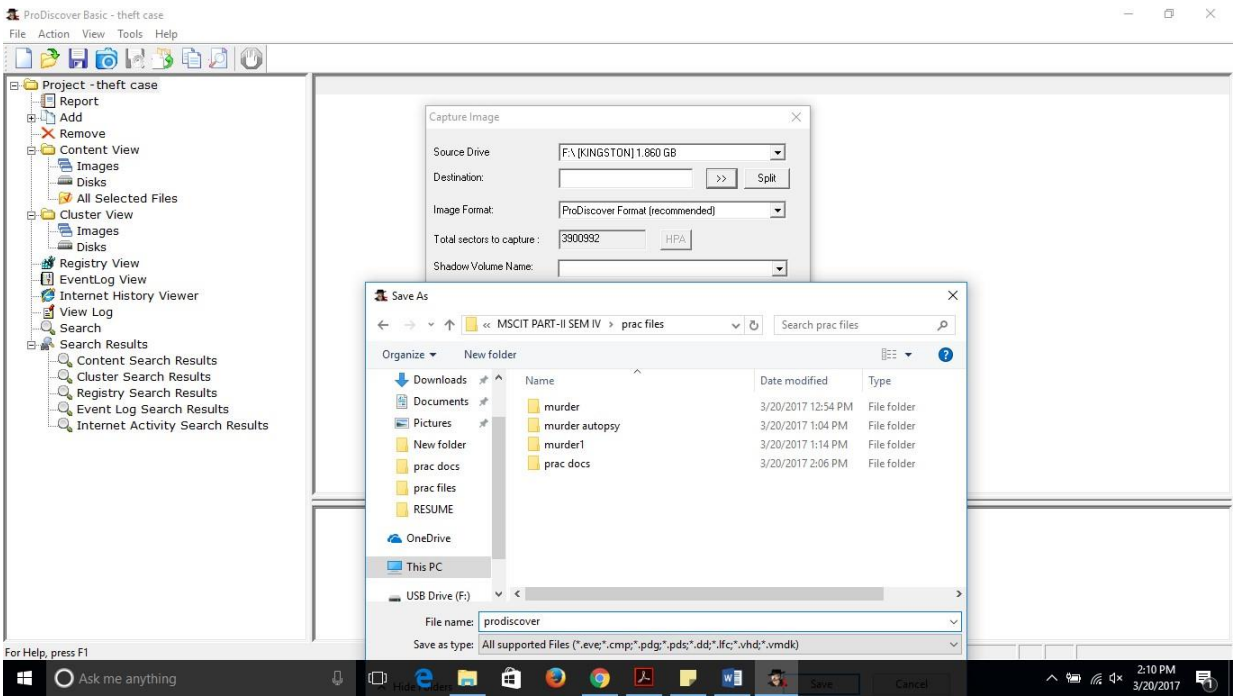

FTK ReportWizard - List by File Path
List by File Path
The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.
Include a list by file path section in the report
Categories of lists that can be included:
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 the settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
C:
myfolder
myfile1.jpg
mysubfolder
myfile2.jpg
< Back
Next >
Cancel

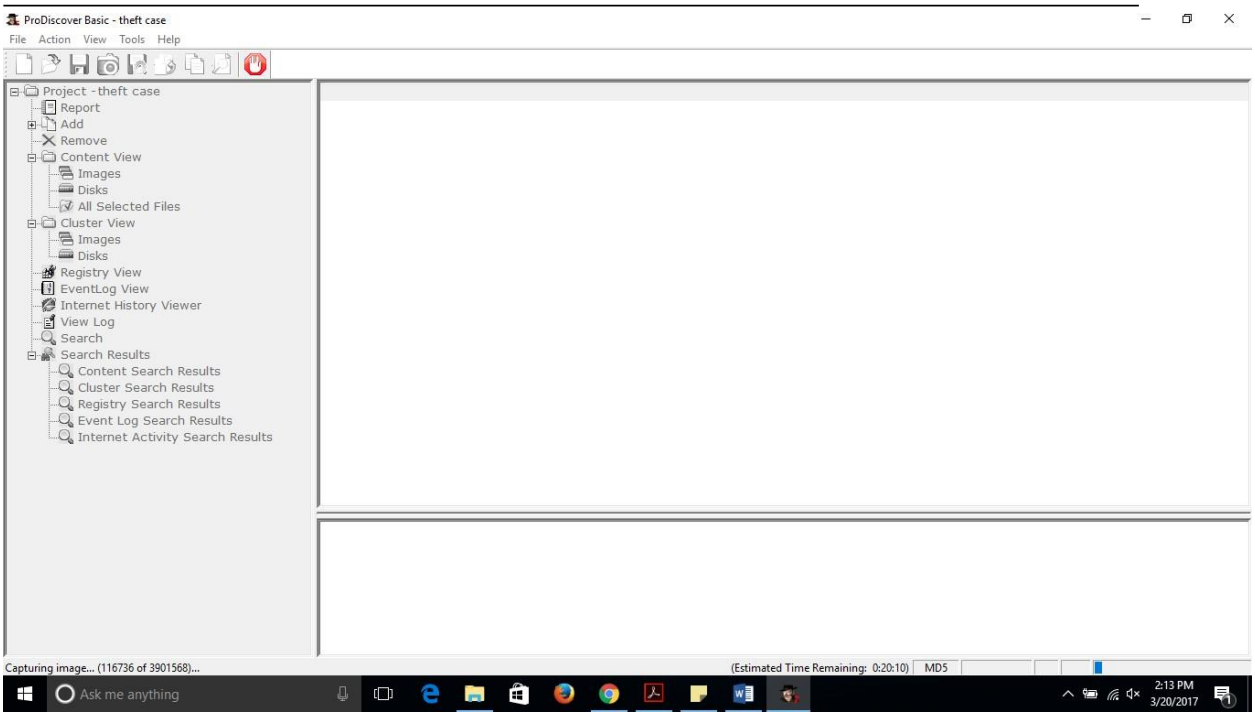

FTK Report Wizard - List File Properties
List File Properties - A
The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.
Include a list file properties section in 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

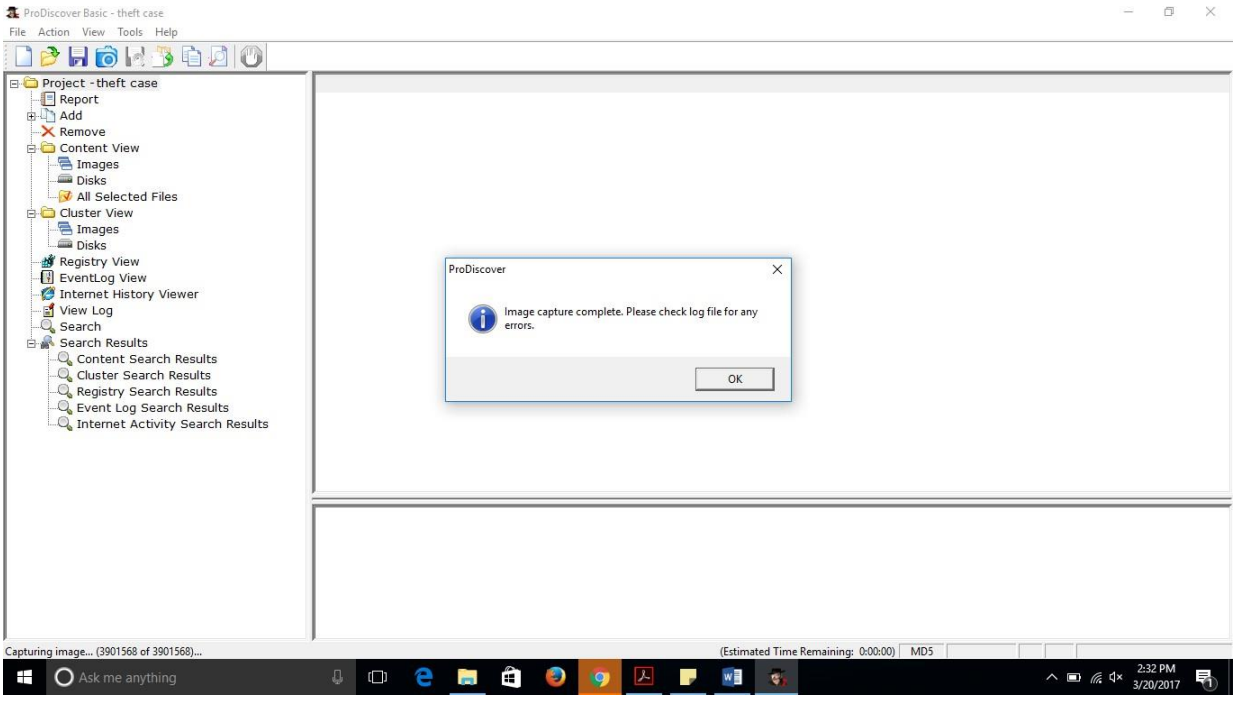

FTK Report Wizard - Supplementary Files
Supplementary Files
You can add your own files to the report by including them in the list below. Any type of file can be included. The file will be copied and hyperlinked to the report.
Supplementary Files:
Add Files
Remove File
Filename
Link name
C:\testprac2\testprac2.ftk
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

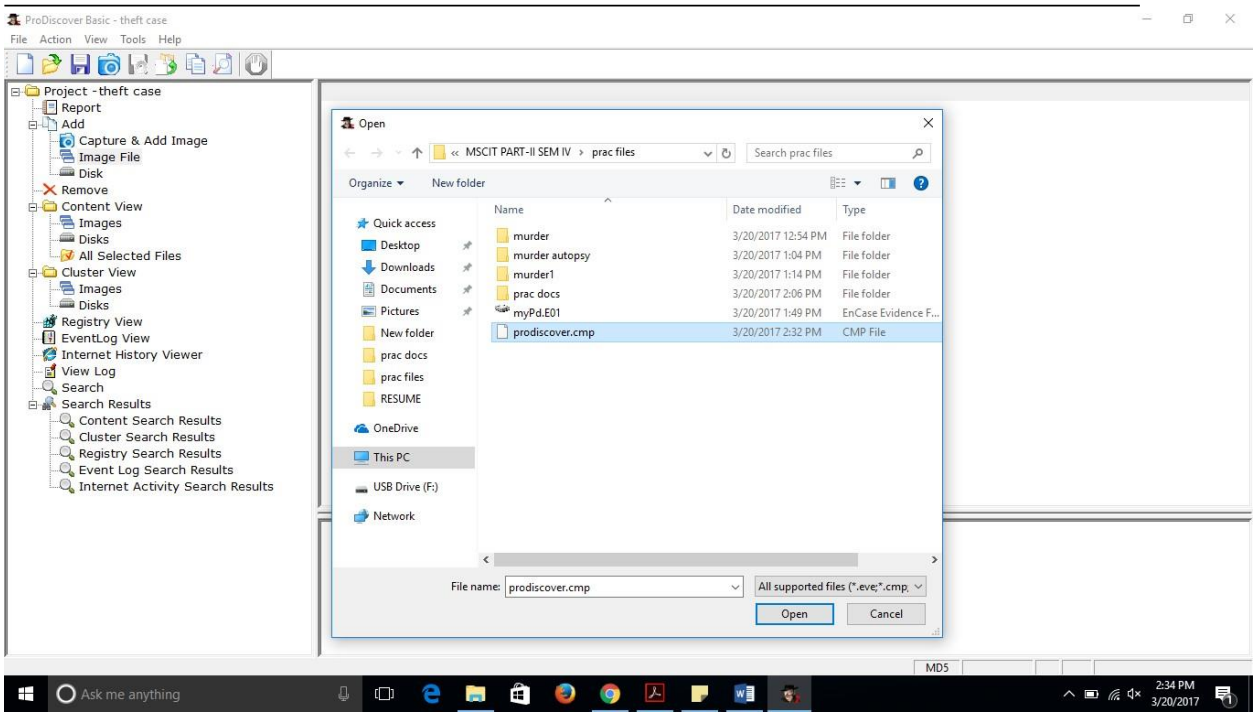

FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located 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:
c:\testprac2\report\
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:
English
< Back
Finish
Cancel

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
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
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
Capturing image... (116736 of 3901568)...
(Estimated Time Remaining: 0:20:10)
MD5
Ask me anything
2:13 PM
3/20/2017


ProDiscover Basic - theft case
File Action View Tools Help
Project - theft case
Report
Add
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
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
ProDiscover
Image capture complete. Please check log file for any errors.
OK
Capturing image... (3901568 of 3901568)...
(Estimated Time Remaining: 0:00:00)
MD5
Ask me anything
2:32 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
Disks
All Selected Files
Cluster View
Images
Disks
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
Open
« MSCIT PART-II SEM IV › prac files
Search prac files
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
New folder
prac docs
prac files
RESUME
OneDrive
This PC
USB Drive (F:)
Network
Name
Date modified
Type
murder
3/20/2017 12:54 PM
File folder
murder autopsy
3/20/2017 1:04 PM
File folder
murder1
3/20/2017 1:14 PM
File folder
prac docs
3/20/2017 2:06 PM
File folder
myPd.E01
3/20/2017 1:49 PM
EnCase Evidence F...
prodiscover.cmp
3/20/2017 2:32 PM
CMP File
File name: prodiscover.cmp
All supported files (*.eve;*.cmp;
Open
Cancel
MD5
Ask me anything
2:34 PM
3/20/2017

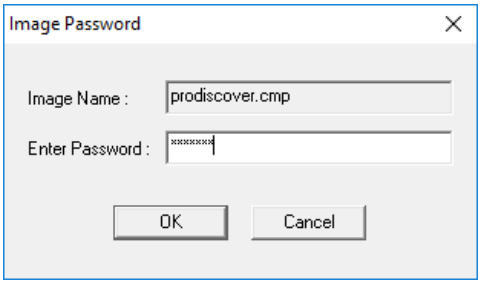
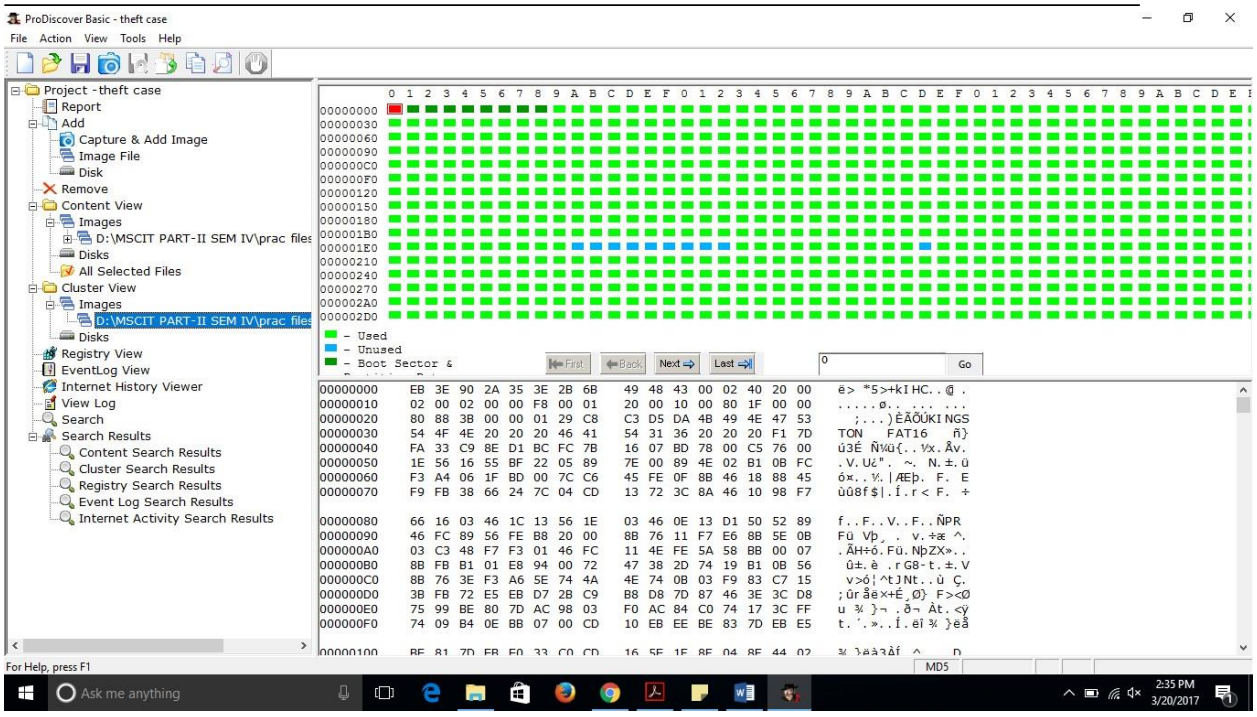
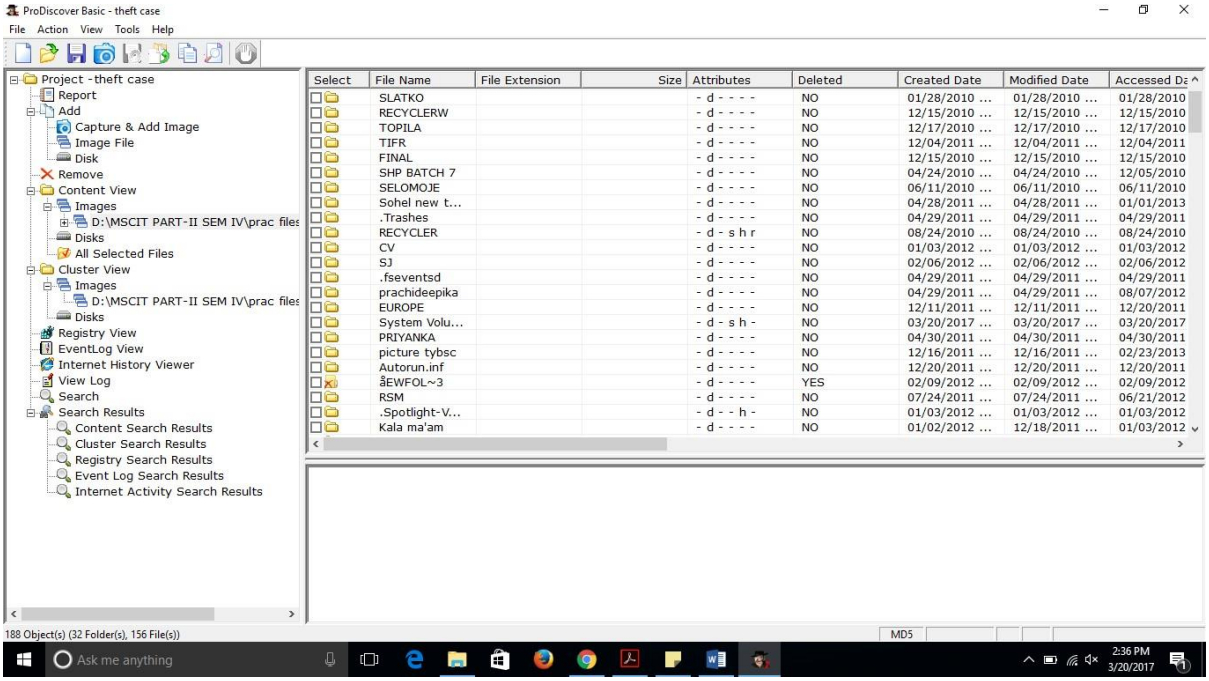
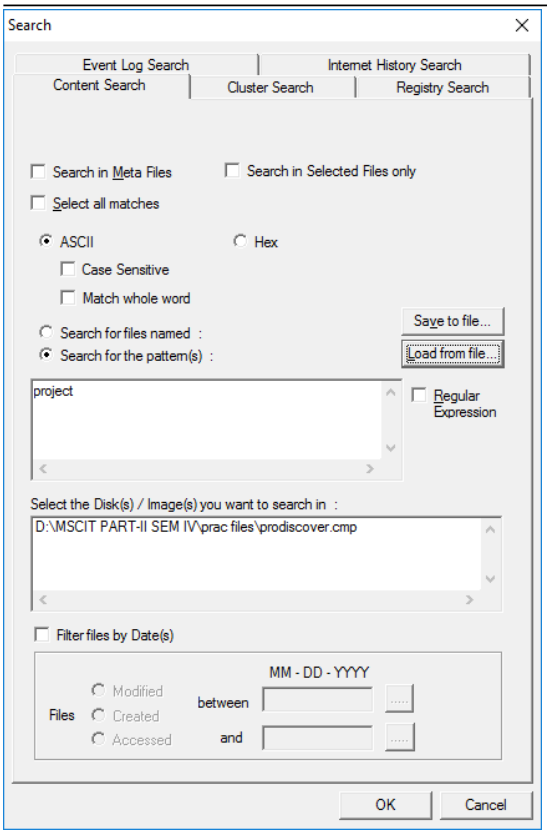
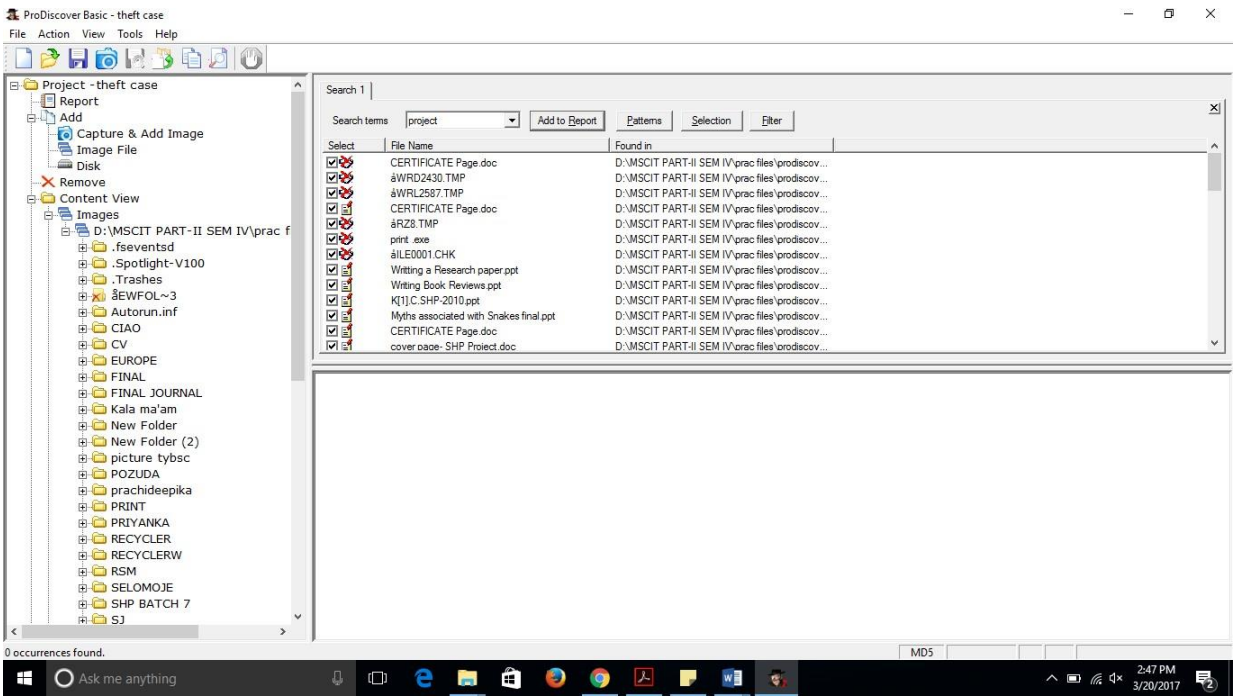


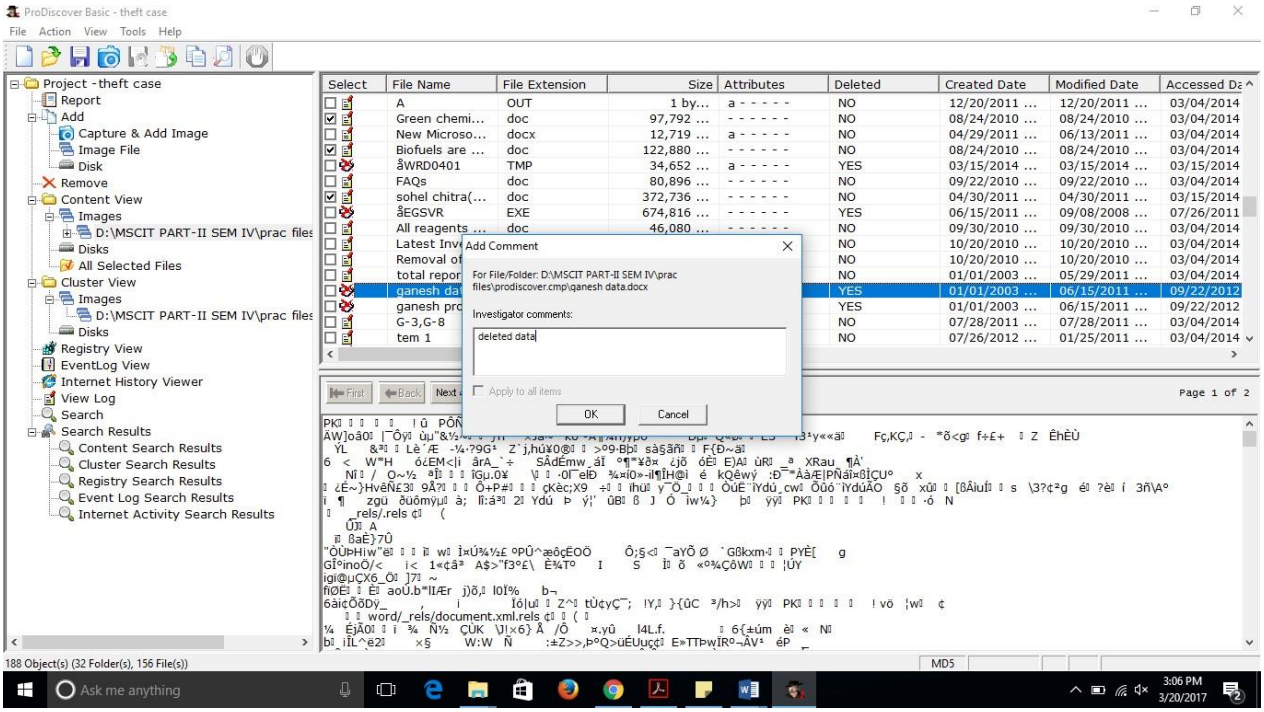
Image Password
Image Name :
prodiscover.cmp
Enter Password :
OK
Cancel


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
Disks
All Selected Files
Cluster View
Images
D:\MSCIT PART-II SEM IV\prac files
Disks
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
Used
Unused
Boot Sector &
First
Back
Next
Last
Go
For Help, press F1
MD5
Ask me anything
2:35 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 files
Disks
All Selected Files
Cluster View
Images
D:\MSCIT PART-II SEM IV\prac files
Disks
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 Da
SLATKO - d - - - - NO 01/28/2010 ... 01/28/2010 ... 01/28/2010
RECYCLERW - d - - - - NO 12/15/2010 ... 12/15/2010 ... 12/15/2010
TOPILA - d - - - - NO 12/17/2010 ... 12/17/2010 ... 12/17/2010
TIFR - d - - - - NO 12/04/2011 ... 12/04/2011 ... 12/04/2011
FINAL - d - - - - NO 12/15/2010 ... 12/15/2010 ... 12/15/2010
SHP BATCH 7 - d - - - - NO 04/24/2010 ... 04/24/2010 ... 12/05/2010
SELOMOJE - d - - - - NO 06/11/2010 ... 06/11/2010 ... 06/11/2010
Sohel new t... - d - - - - NO 04/28/2011 ... 04/28/2011 ... 01/01/2013
.Trashes - d - - - - NO 04/29/2011 ... 04/29/2011 ... 04/29/2011
RECYCLER - d - s h r NO 08/24/2010 ... 08/24/2010 ... 08/24/2010
CV - d - - - - NO 01/03/2012 ... 01/03/2012 ... 01/03/2012
SJ - d - - - - NO 02/06/2012 ... 02/06/2012 ... 02/06/2012
.fseventsd - d - - - - NO 04/29/2011 ... 04/29/2011 ... 04/29/2011
prachideepika - d - - - - NO 04/29/2011 ... 04/29/2011 ... 08/07/2012
EUROPE - d - - - - NO 12/11/2011 ... 12/11/2011 ... 12/20/2011
System Volu... - d - s h - NO 03/20/2017 ... 03/20/2017 ... 03/20/2017
PRIYANKA - d - - - - NO 04/30/2011 ... 04/30/2011 ... 04/30/2011
picture tybsc - d - - - - NO 12/16/2011 ... 12/16/2011 ... 02/23/2013
Autorun.inf - d - - - - NO 12/20/2011 ... 12/20/2011 ... 12/20/2011
åEWFOL~3 - d - - - - YES 02/09/2012 ... 02/09/2012 ... 02/09/2012
RSM - d - - - - NO 07/24/2011 ... 07/24/2011 ... 06/21/2012
.Spotlight-V... - d - - h - NO 01/03/2012 ... 01/03/2012 ... 01/03/2012
Kala ma'am - d - - - - NO 01/02/2012 ... 12/18/2011 ... 01/03/2012
188 Object(s) (32 Folder(s), 156 File(s))
MD5
Ask me anything
2:36 PM
3/20/2017


Search
Event Log Search
Internet History Search
Content Search
Cluster Search
Registry Search
Search in Meta Files
Search in Selected Files only
Select all matches
ASCII
Hex
Case Sensitive
Match whole word
Search for files named :
Search for the pattern(s) :
Save to file...
Load from file...
project
Regular Expression
Select the Disk(s) / Image(s) you want to search in :
D:\MSCIT PART-II SEM IV\prac files\prodiscover.cmp
Filter files by Date(s)
MM - DD - YYYY
Files
Modified
Created
Accessed
between
and
OK
Cancel

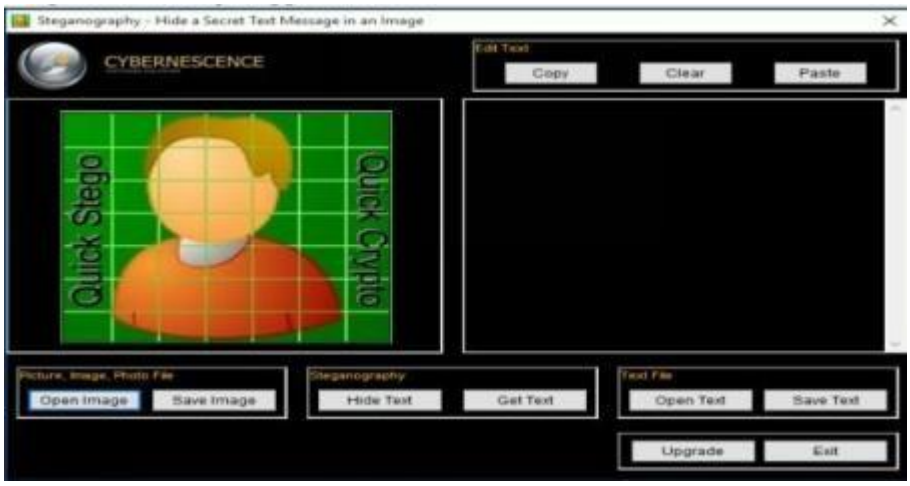

ProDiscover Basic - theft case
File Action View Tools Help
Project -theft case
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
Search 1
Search terms
project
Add to Report
Patterns
Selection
Filter
Select
File Name
Found in
CERTIFICATE Page.doc
áWRD2430.TMP
áWRL2587.TMP
CERTIFICATE Page.doc
ãRZ8.TMP
print .exe
áILE0001.CHK
Writting a Research paper.ppt
Writing Book Reviews.ppt
K[1].C.SHP-2010.ppt
Myths associated with Snakes final.ppt
CERTIFICATE Page.doc
cover page- SHP Project.doc
0 occurrences found.
MD5
Ask me anything
2:47 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
Disks
All Selected Files
Cluster View
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 Da
A
Green chemi...
New Microso...
Biofuels are ...
ŝWRD0401
FAQs
sohel chitra(...
ŝEGSVR
All reagents ...
Latest Inv
Removal of
total repor
ganesh dat
ganesh pro
G-3,G-8
tem 1
Add Comment
For File/Folder: D:\MSCIT PART-II SEM IV\prac files\prodiscover.cmp\ganesh data.docx
Investigator comments:
deleted data
Apply to all items
OK
Cancel
Page 1 of 2
188 Object(s) (32 Folder(s), 156 File(s))
MD5
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

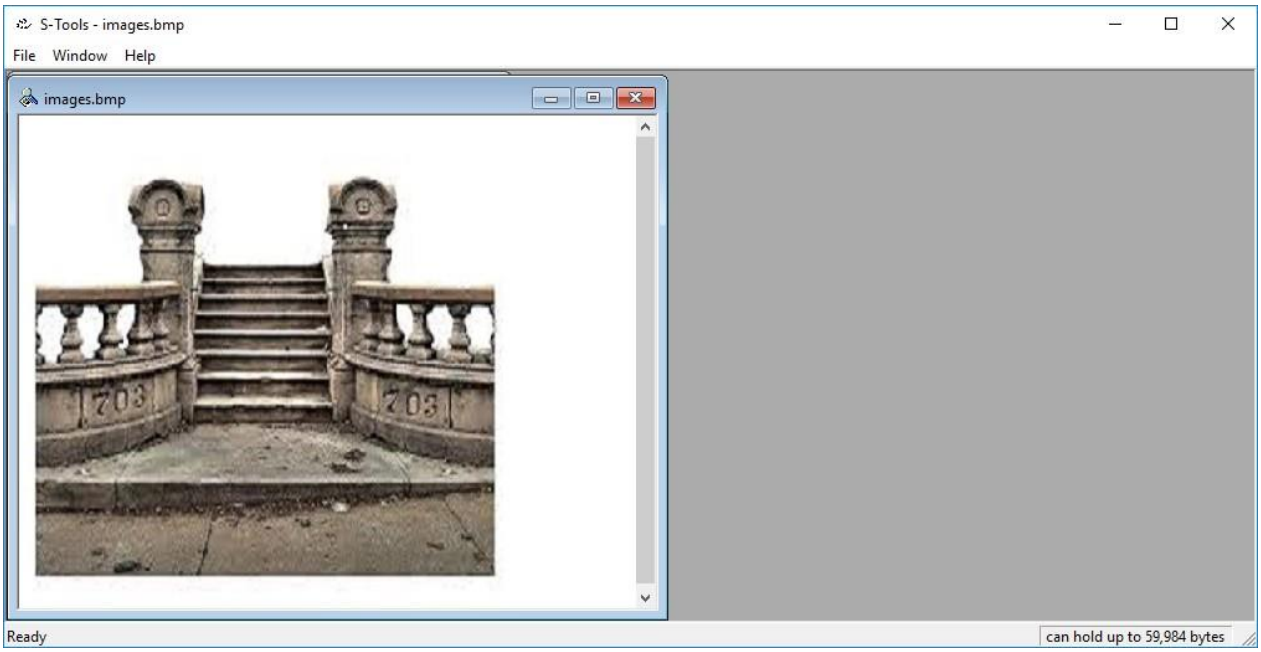
Save Image - This Saved Image containing Hidden information is termed as Stego Object.

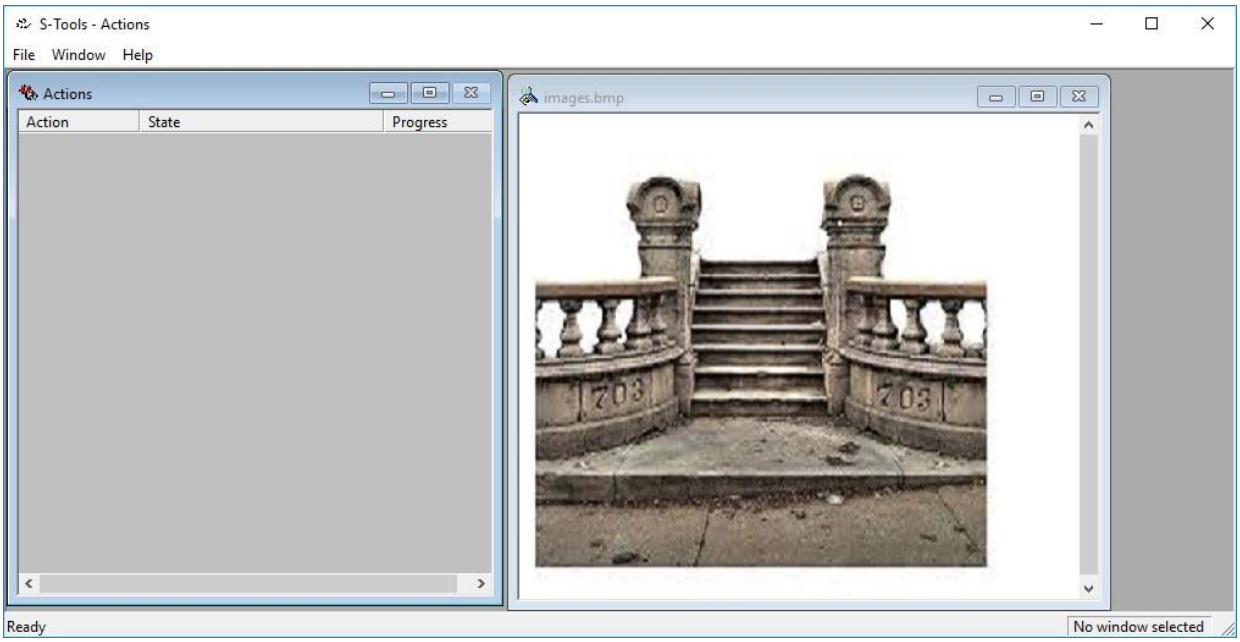
Recovering Data from Image Steganography using QuickStego→ *Open QuickStego → Click Get Text*

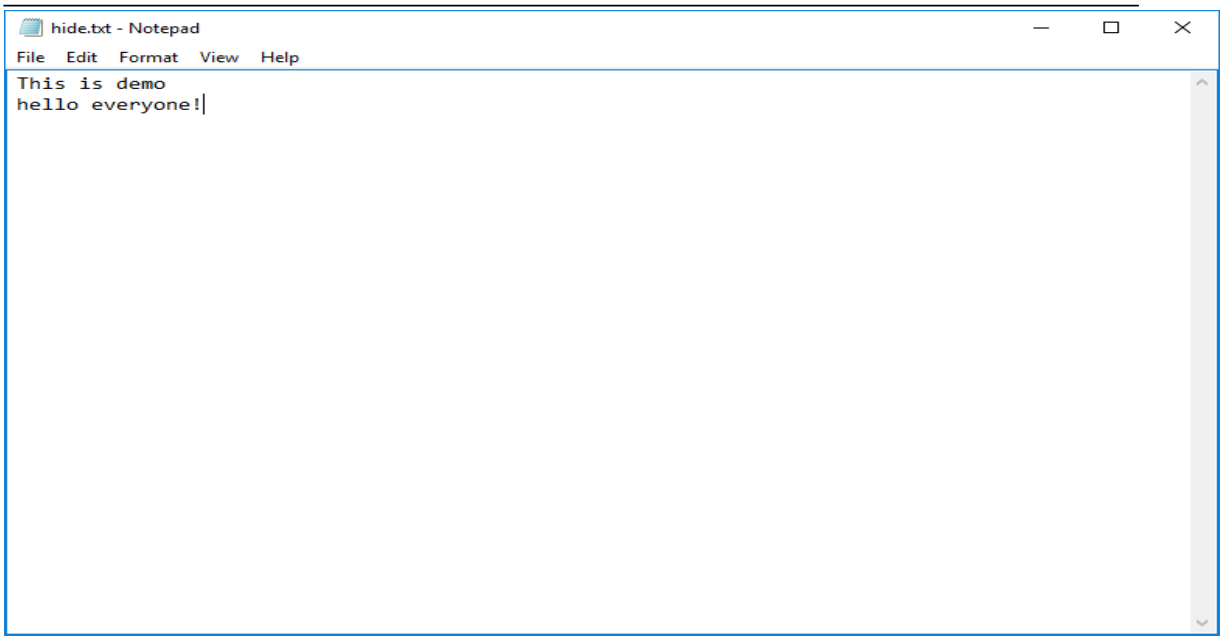
Open and Compare Both Images

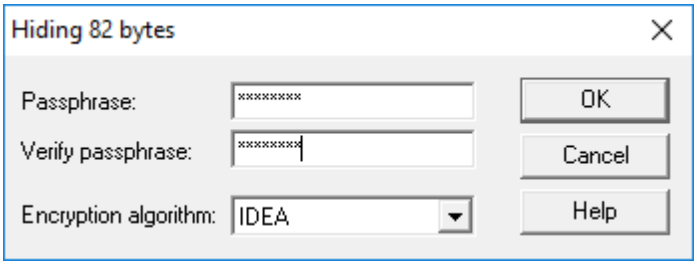
Left Image is without Hidden Text; Right Image is with hidden text

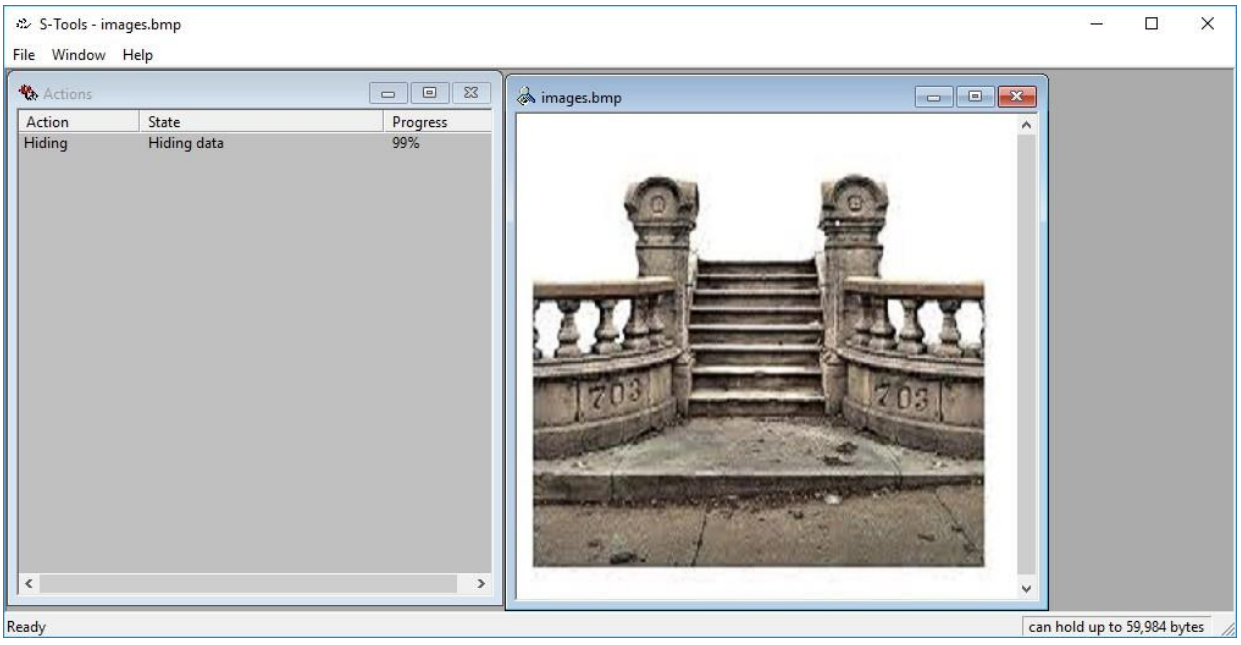
Using Tool: S tool

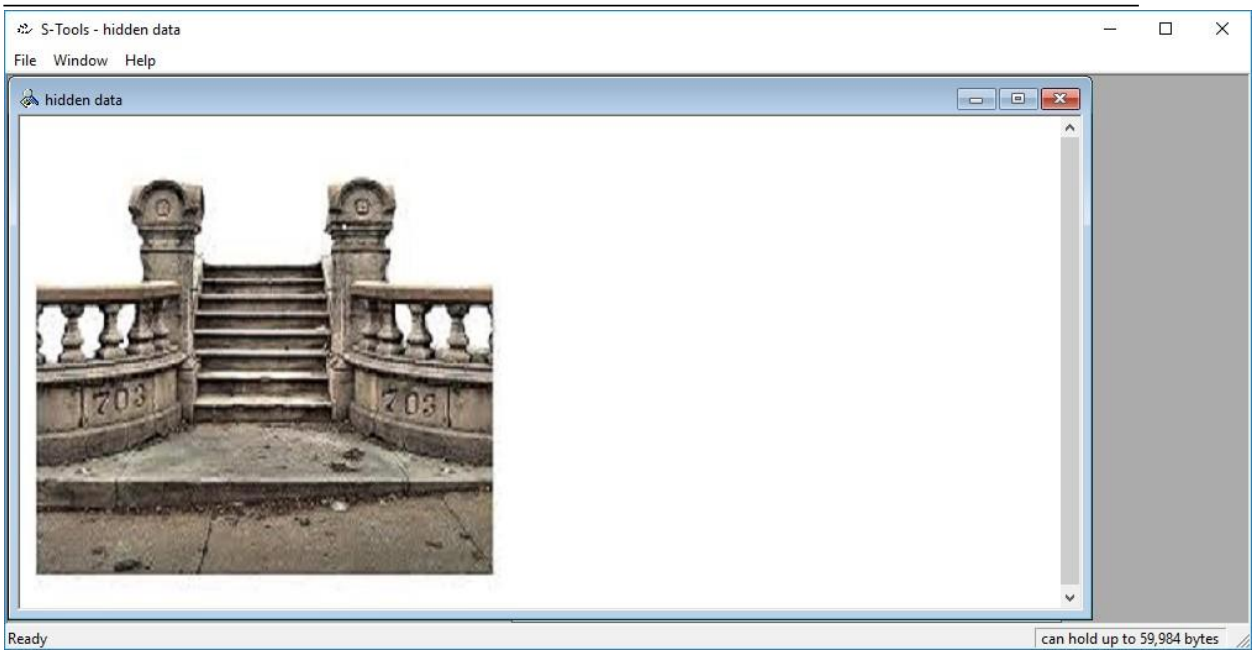


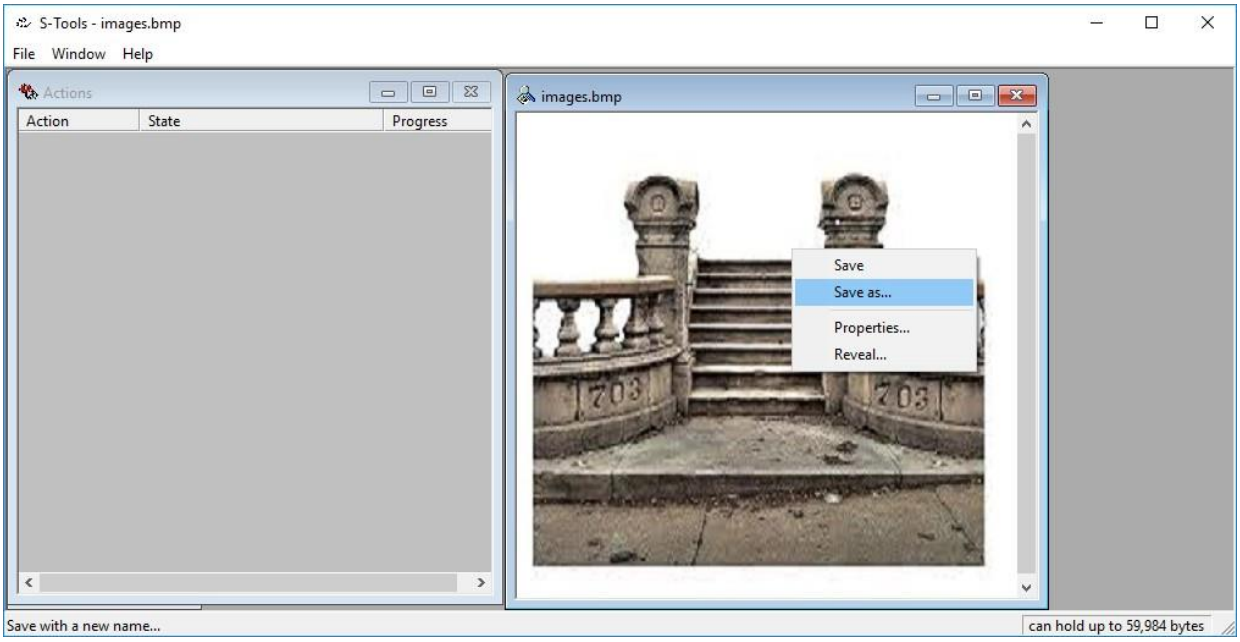


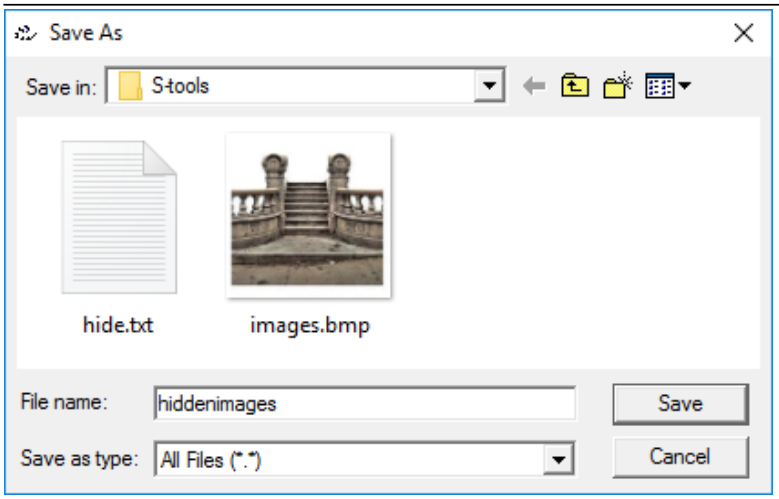

hide.txt - Notepad
File Edit Format View Help
This is demo
hello everyone!

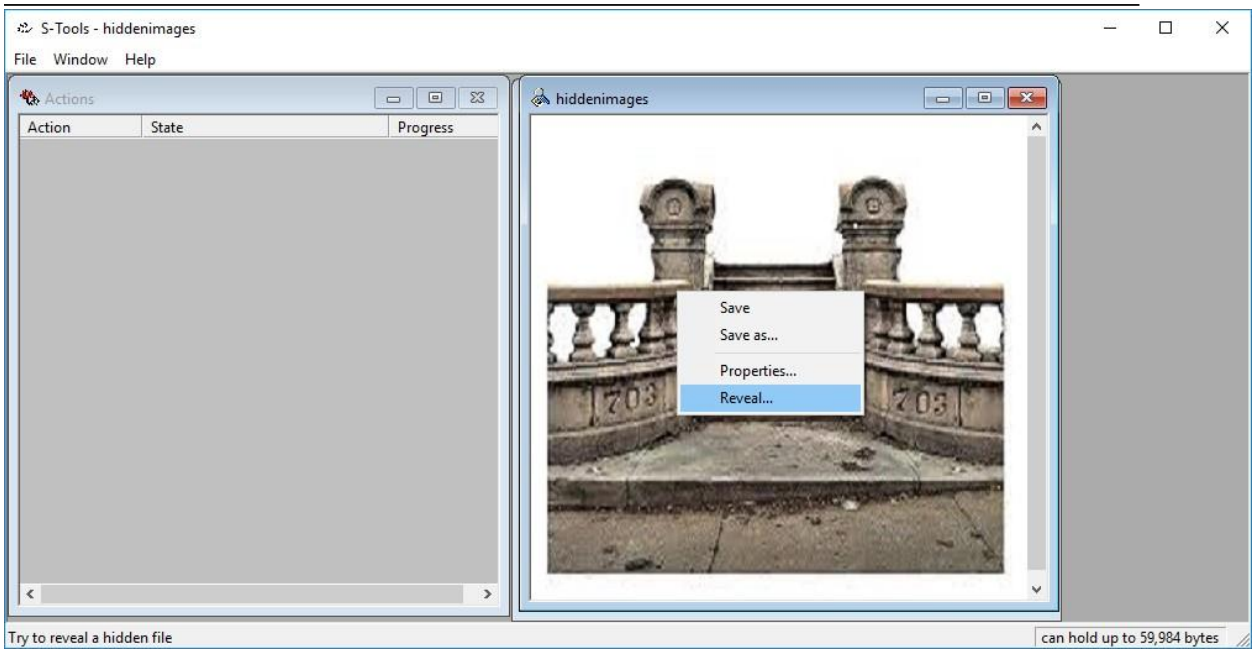

Hiding 82 bytes
Passphrase:
****
Verify passphrase:
****
Encryption algorithm:
IDEA
OK
Cancel
Help

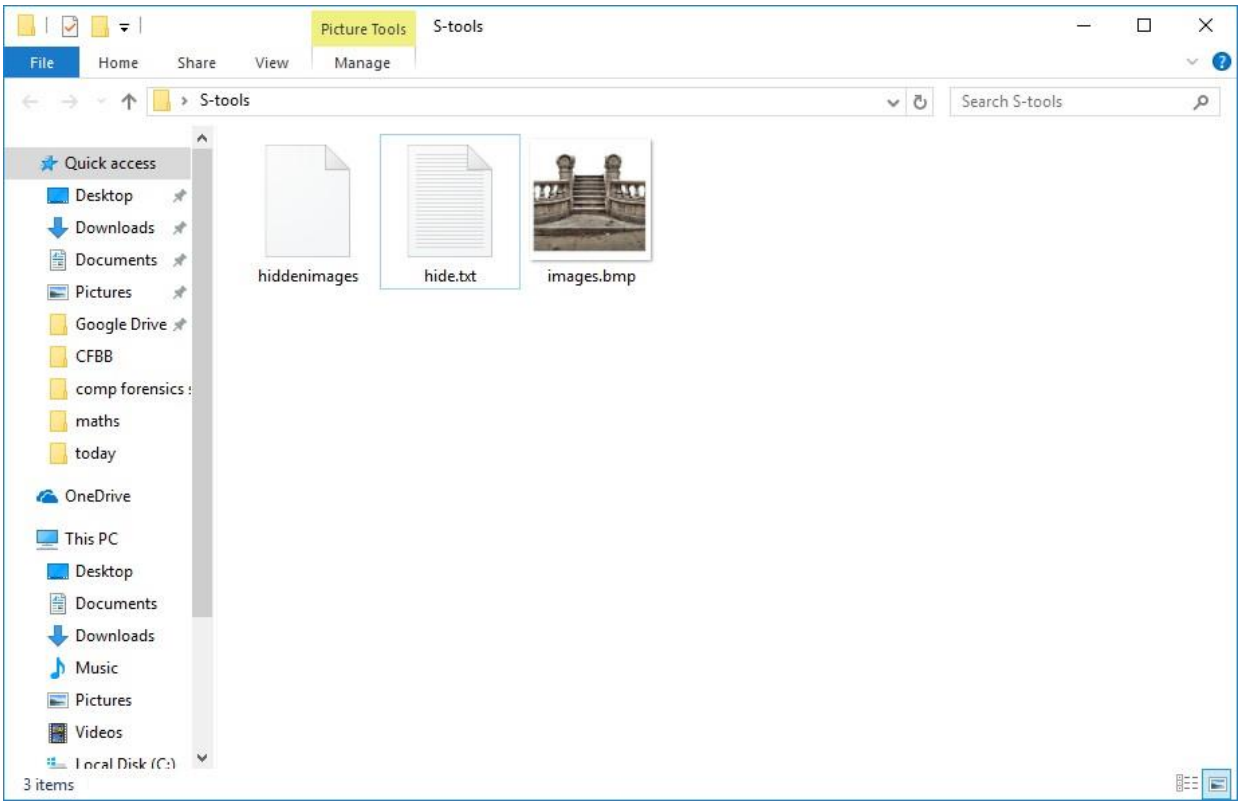

S-Tools - images.bmp
File Window Help
Actions
Action
State
Progress
Hiding
Hiding data
99%
images.bmp
Ready
can hold up to 59,984 bytes

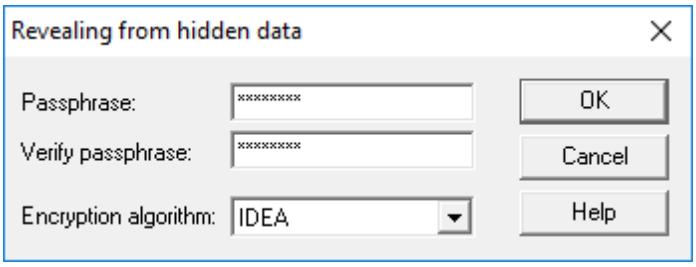

S-Tools - hidden data
File Window Help
hidden data
Ready
can hold up to 59,984 bytes

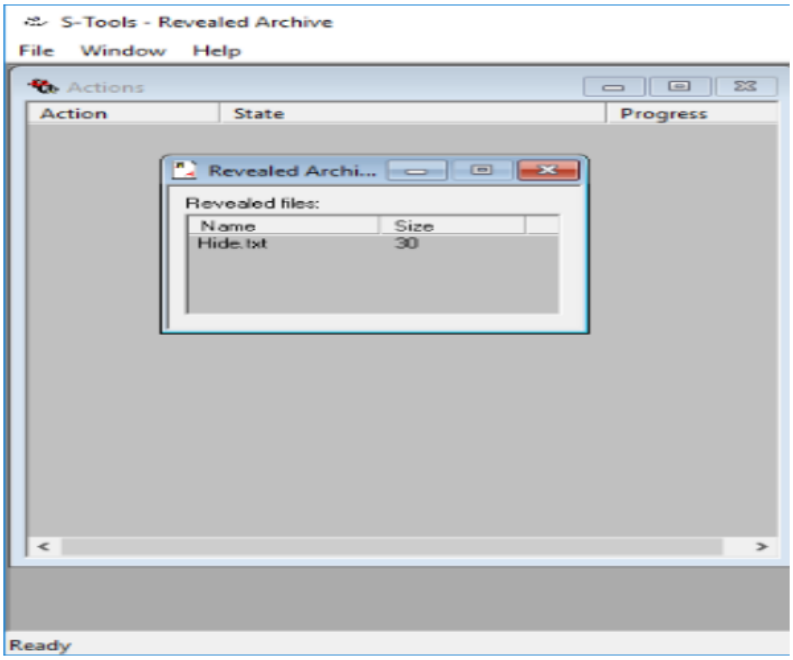

S-Tools - images.bmp
File Window Help
Actions
Action
State
Progress
images.bmp
Save
Save as...
Properties...
Reveal...
Save with a new name...
can hold up to 59,984 bytes


Save As
Save in:
S-tools
hide.txt
images.bmp
File name:
hiddenimages
Save as type:
All Files (*.*)
Save
Cancel


S-Tools - hiddenimages
File Window Help
Actions
Action
State
Progress
hiddenimages
Save
Save as...
Properties...
Reveal...
Try to reveal a hidden file
can hold up to 59,984 bytes

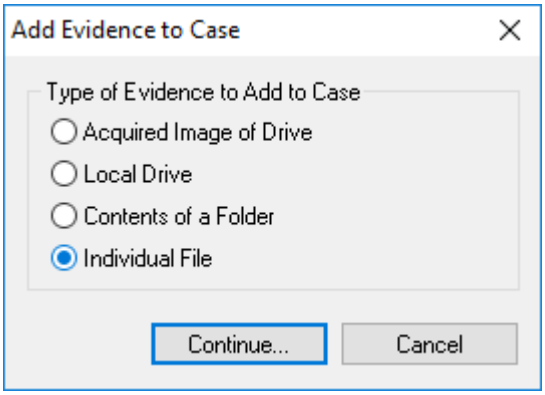

Picture Tools
S-tools
File
Home
Share
View
Manage
S-tools
Search S-tools
Quick access
Desktop
Downloads
Documents
Pictures
Google Drive
CFBB
comp forensics
maths
today
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
hiddenimages
hide.txt
images.bmp
3 items

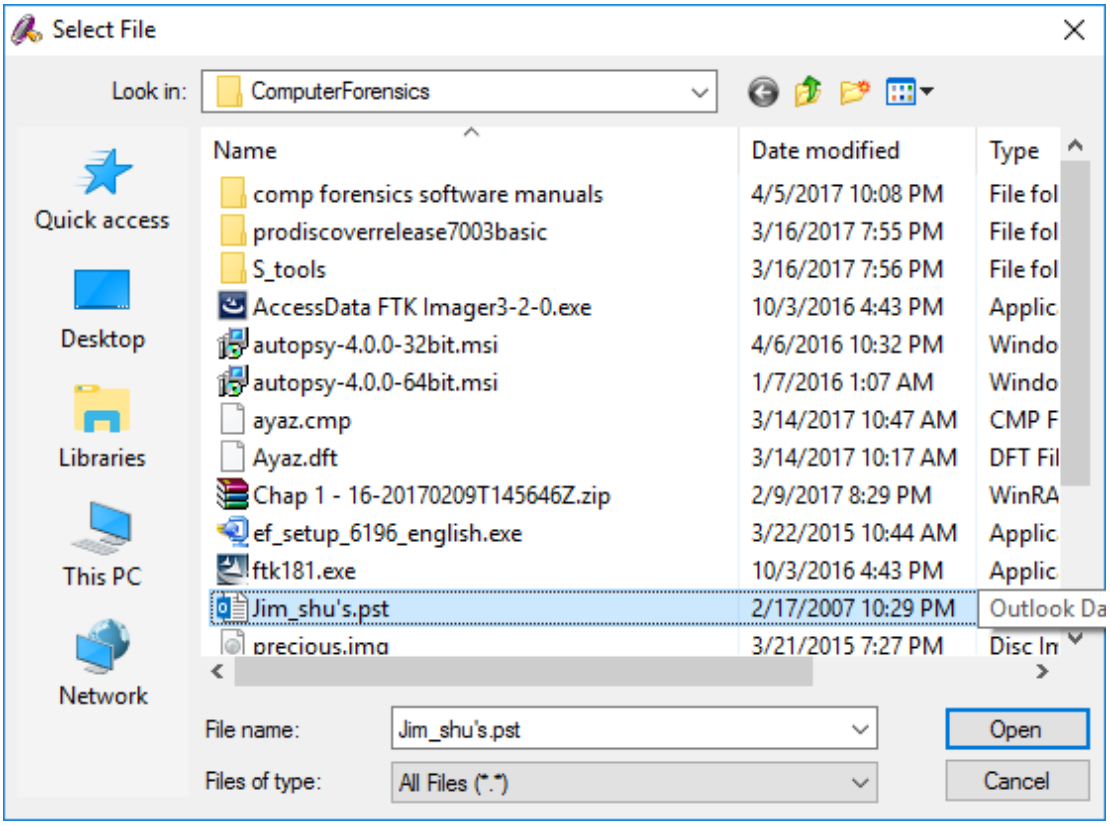

Revealing from hidden data
Passphrase:
****
Verify passphrase:
****
Encryption algorithm:
IDEA
OK
Cancel
Help

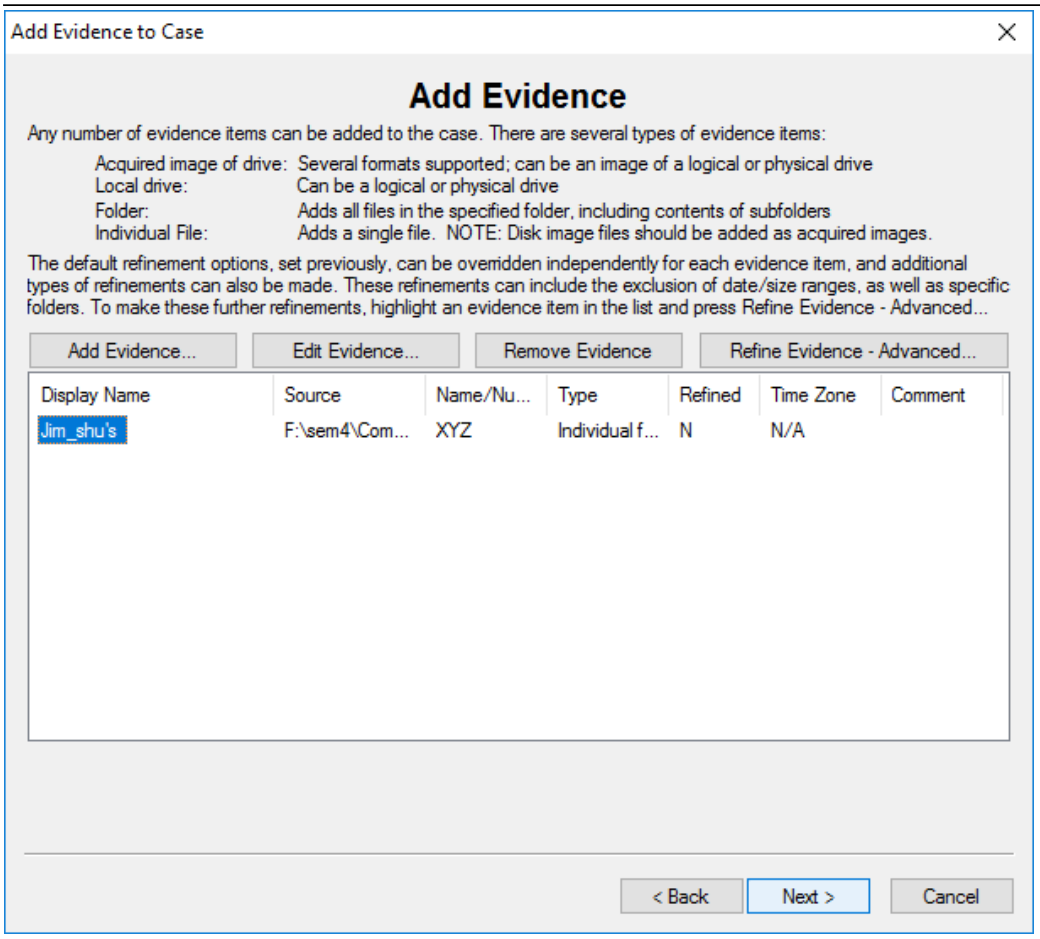

S-Tools - Revealed Archive
File Window Help
Actions
Action
State
Progress
Revealed Archi...
Revealed files:
Name
Size
Hide.txt
30
Ready

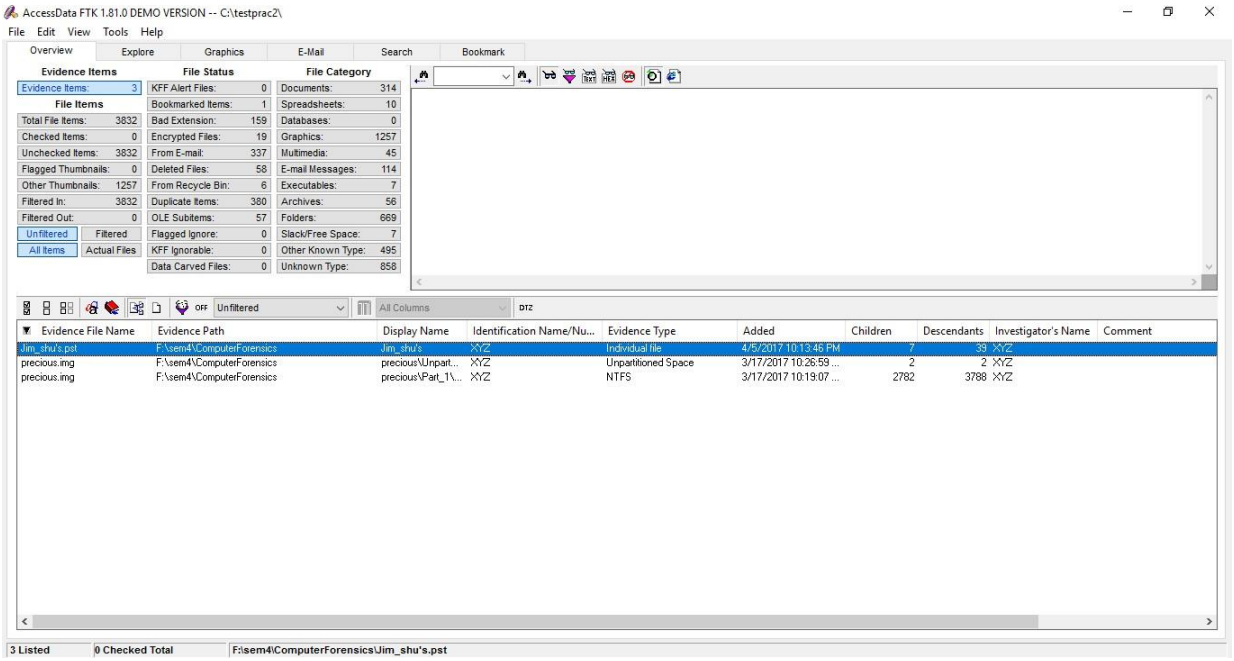
PRACTICAL NO 10: Use Email Forensic Tools for Email Recovery Mobile Forensics

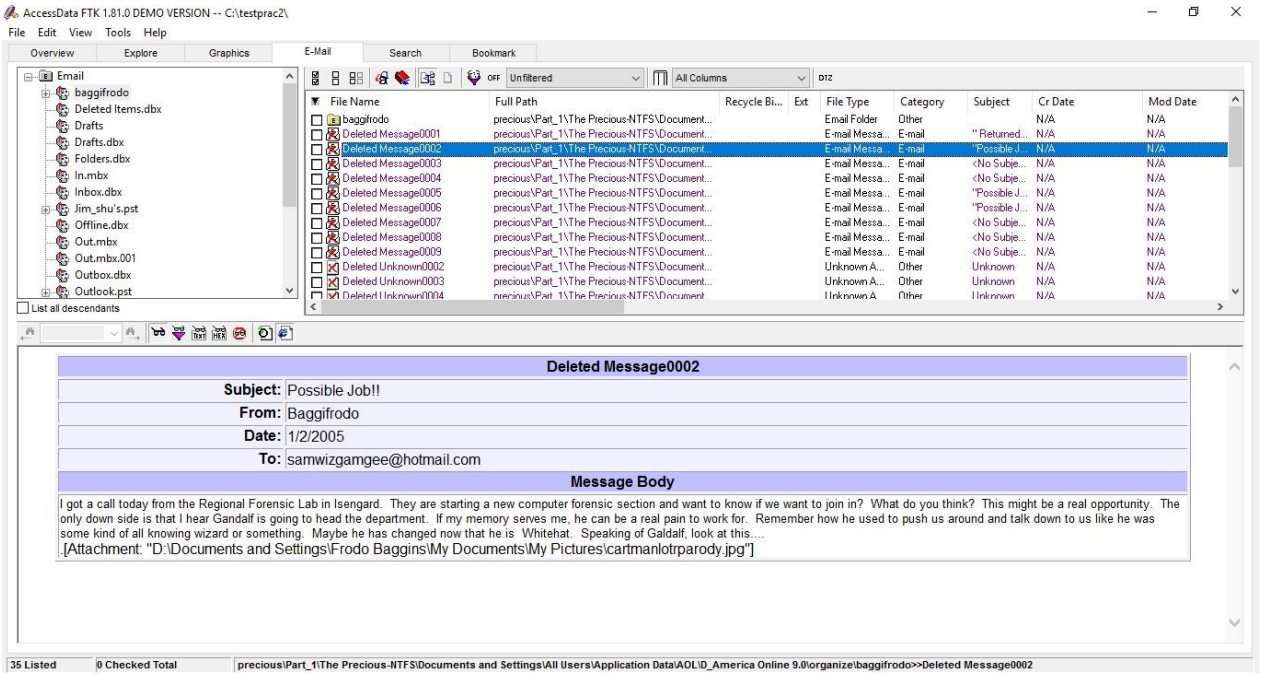
EMAIL FORENSIC



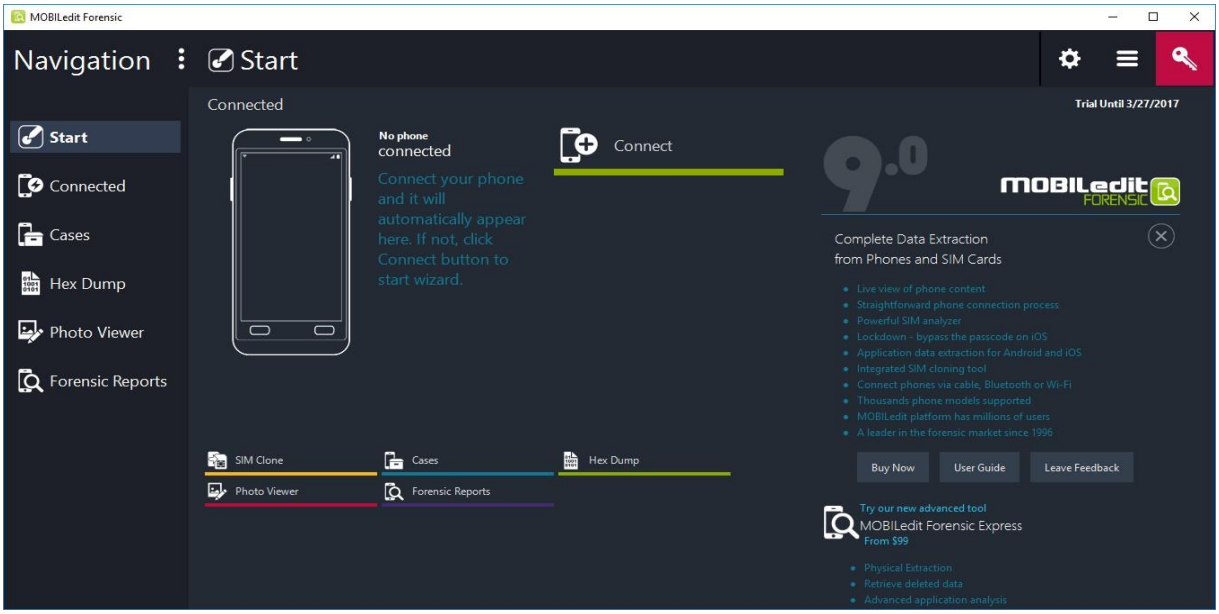


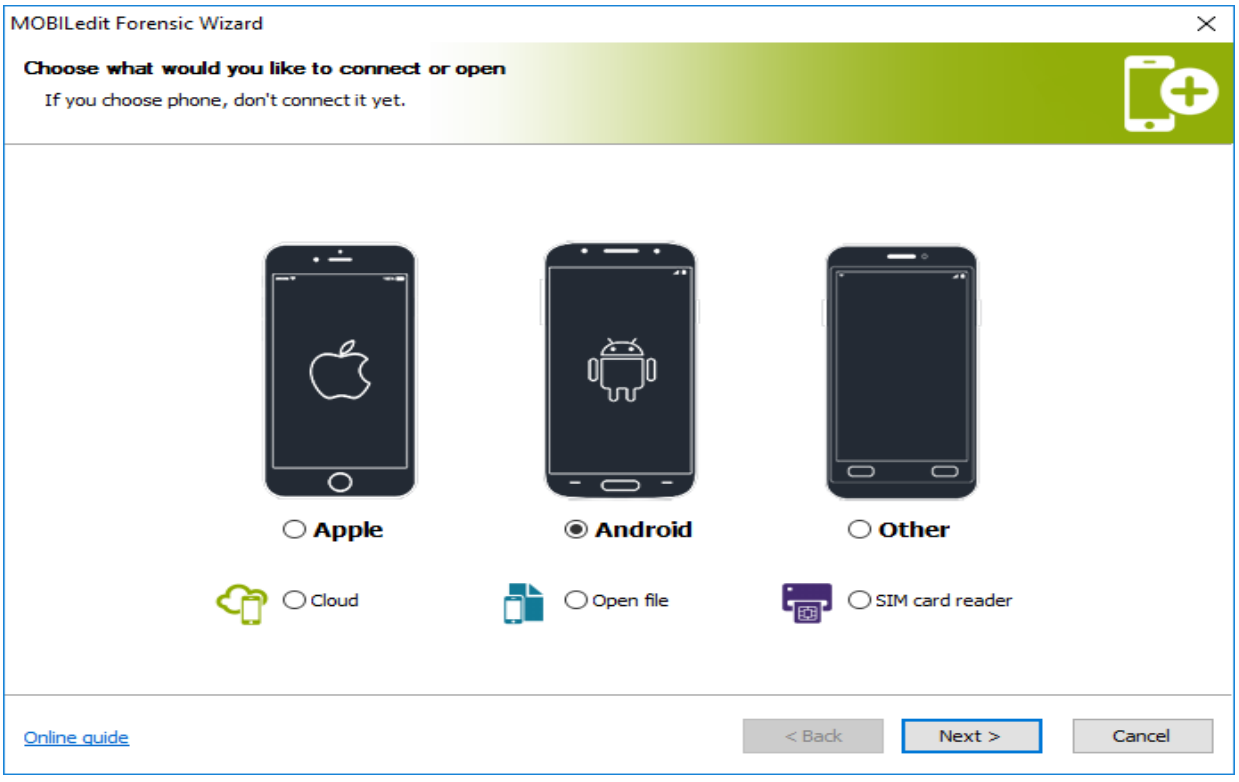

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files 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

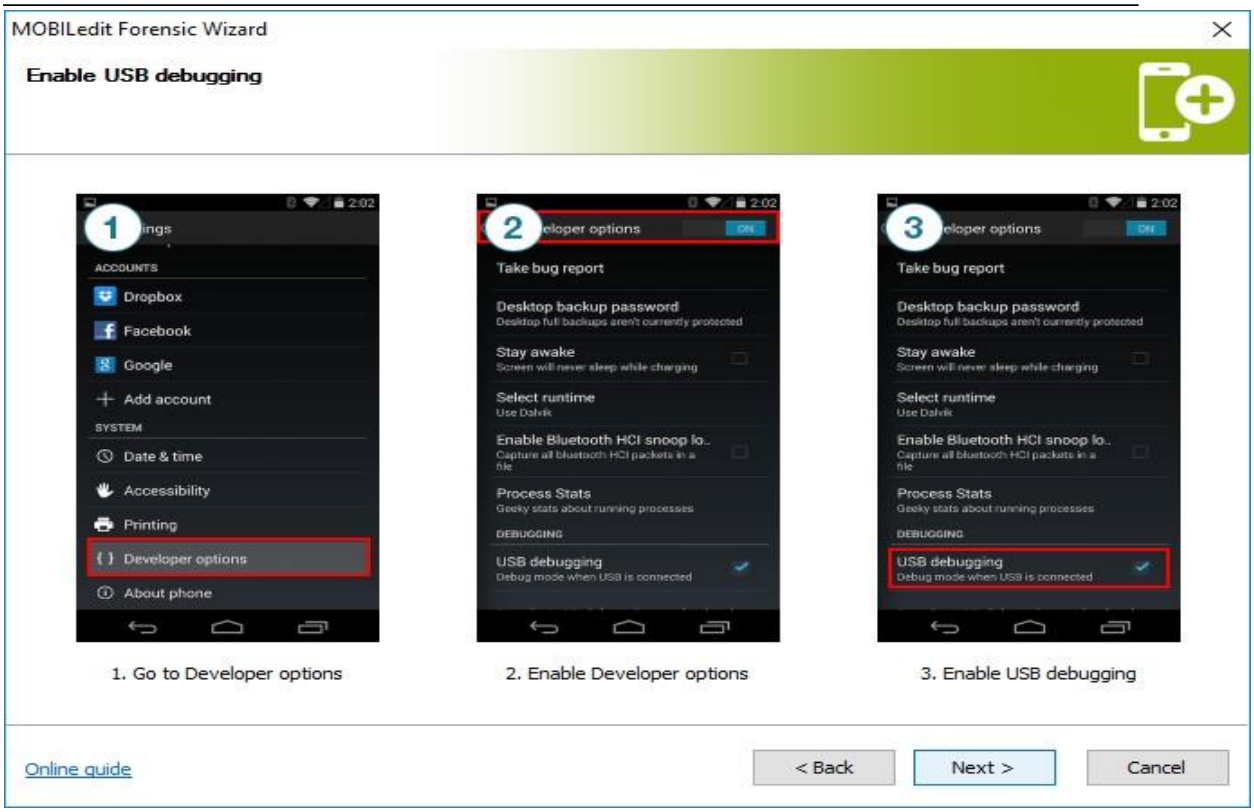

AccessData FTK 1.81.0 DEMO VERSION -- C:\testprac2\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 3
File Items
Total File Items: 3832
Checked Items: 0
Unchecked Items: 3832
Flagged Thumbnails: 0
Other Thumbnails: 1257
Filtered In: 3832
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
KFF Alert Files: 0
Bookmarked Items: 1
Bad Extension: 159
Encrypted Files: 19
From E-mail: 337
Deleted Files: 58
From Recycle Bin: 6
Duplicate Items: 380
OLE Subitems: 57
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 314
Spreadsheets: 10
Databases: 0
Graphics: 1257
Multimedia: 45
E-mail Messages: 114
Executables: 7
Archives: 56
Folders: 669
Slack/Free Space: 7
Other Known Type: 495
Unknown Type: 858
Unfiltered
All Columns
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 10:26:59 ... 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

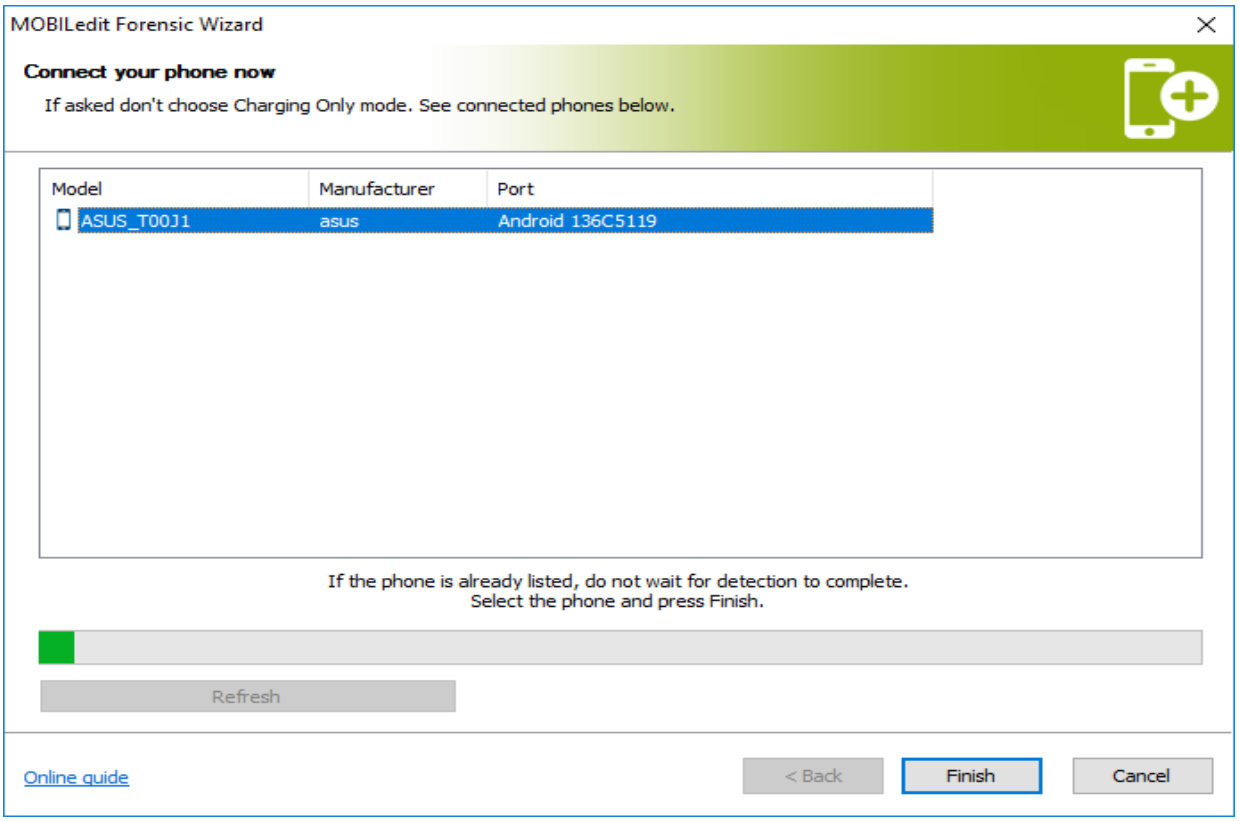

AccessData FTK 1.81.0 DEMO VERSION -- C:\testprac2\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
baggifrodo
Deleted Items.dbx
Drafts
Drafts.dbx
Folders.dbx
In.mbx
Inbox.dbx
Jim_shu's.pst
Offline.dbx
Out.mbx
Out.mbx.001
Outbox.dbx
Outlook.pst
List all descendants
Unfiltered
All Columns
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
Cr Date
Mod Date
baggifrodo
Deleted Message0001
Deleted Message0002
Deleted Message0003
Deleted Message0004
Deleted Message0005
Deleted Message0006
Deleted Message0007
Deleted Message0008
Deleted Message0009
Deleted Unknown0002
Deleted Unknown0003
Deleted Message0002
Subject: Possible Job!!
From: Baggifrodo
Date: 1/2/2005
To: samwizgamgee@hotmail.com
Message Body
I got a call today from the Regional Forensic Lab in Isengard. They are starting a new computer forensic section and want to know if we want to join in? What do you think? This might be a real opportunity. The only down side is that I hear Gandalf is going to head the department. If my memory serves me, he can be a real pain to work for. Remember how he used to push us around and talk down to us like he was some kind of all knowing wizard or something. Maybe he has changed now that he is Whitehat. Speaking of Galdalf, look at this....
[Attachment: "D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\cartmanlotrparody.jpg"]
35 Listed
0 Checked Total
precious\Part_1\The Precious-NTFS\Documents and Settings\All Users\Application Data\AOL\D_America Online 9.0\organize\baggifrodo>>Deleted Message0002

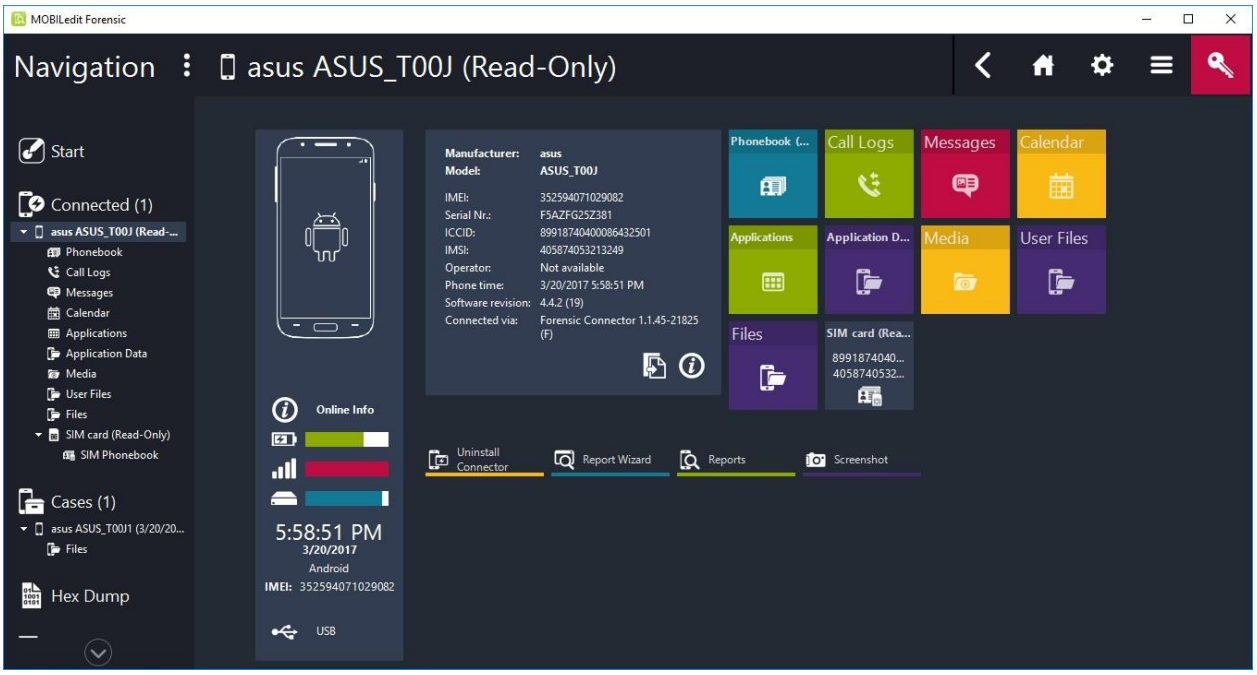
USING MOBILE EDIT

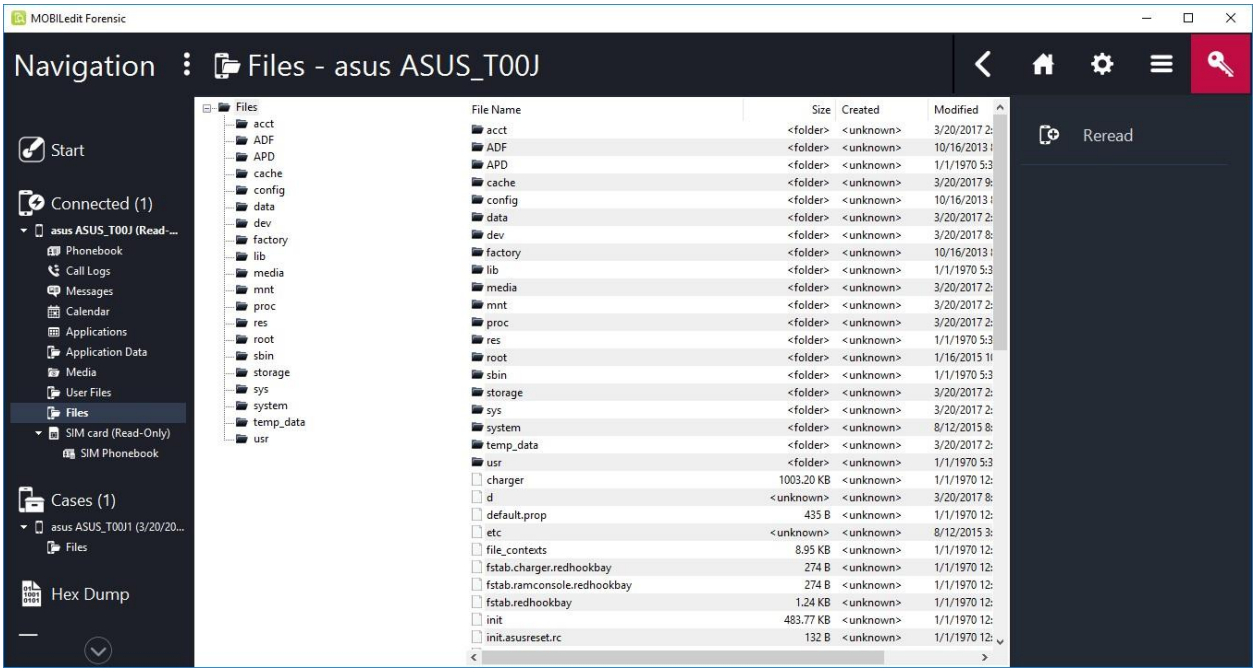


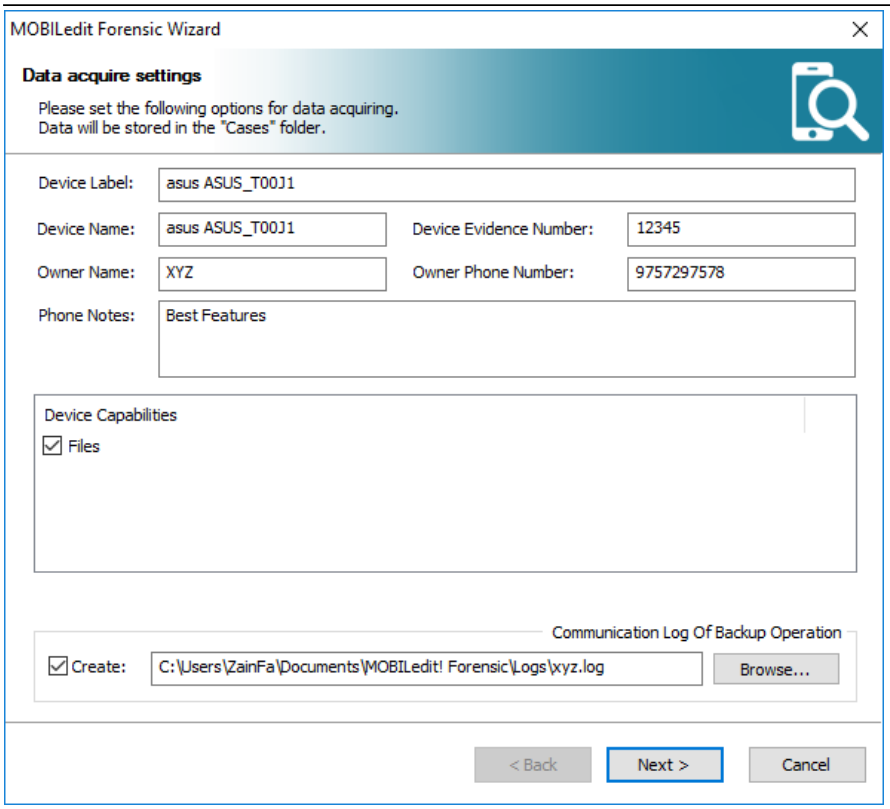


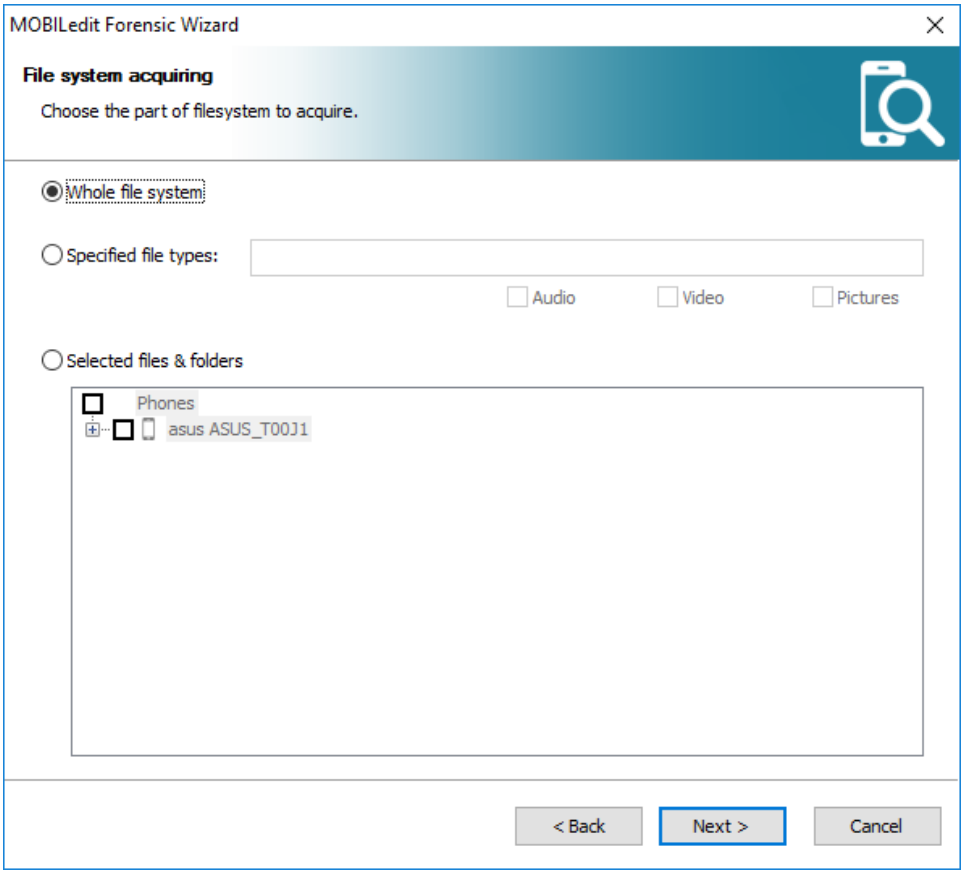

MOBILedit Forensic Wizard
Enable USB debugging
1
ACCOUNTS
Dropbox
Facebook
Google
Add account
SYSTEM
Date & time
Accessibility
Printing
Developer options
About phone
2
Take bug report
Desktop backup password
Stay awake
Select runtime
Enable Bluetooth HCI snoop lo..
Process Stats
DEBUGGING
USB debugging
Debug mode when USB is connected
3
Take bug report
Desktop backup password
Stay awake
Select runtime
Enable Bluetooth HCI snoop lo..
Process Stats
DEBUGGING
USB debugging
Debug mode when USB is connected
1. Go to Developer options
2. Enable Developer options
3. Enable USB debugging
Online guide
< Back
Next >
Cancel

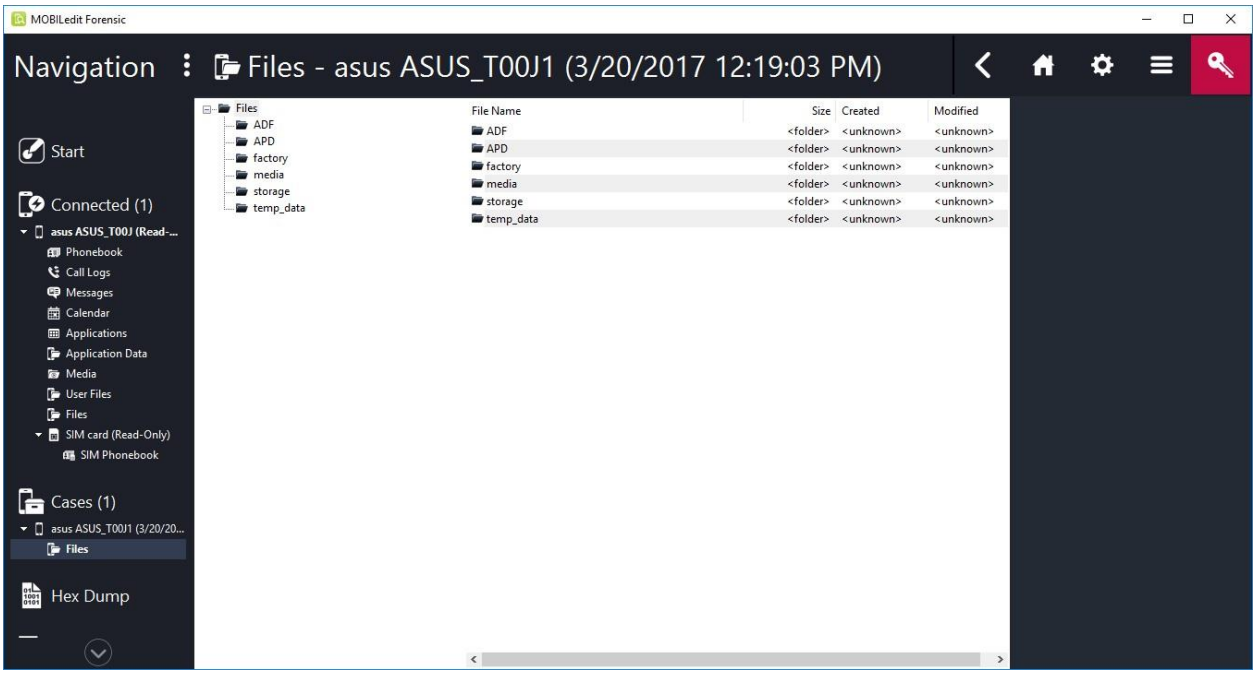

MOBILedit Forensic Wizard
Connect your phone now
If asked don't choose Charging Only mode. See connected phones below.
Model
Manufacturer
Port
ASUS_T00J1
asus
Android 136C5119
If the phone is already listed, do not wait for detection to complete.
Select the phone and press Finish.
Refresh
Online guide
< Back
Finish
Cancel

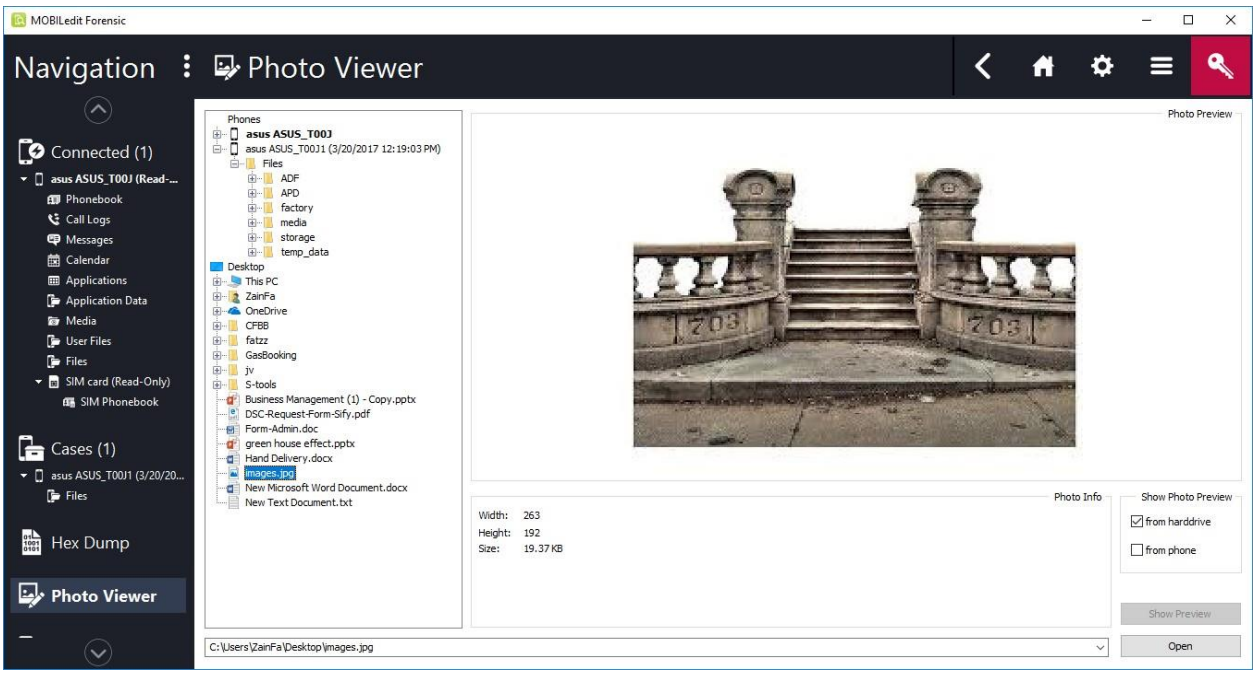

MOBILedit Forensic
Navigation
asus ASUS_T00J (Read-Only)
Start
Connected (1)
asus ASUS_T00J (Read-...
Phonebook
Call Logs
Messages
Calendar
Applications
Application Data
Media
User Files
Files
SIM card (Read-Only)
SIM Phonebook
Cases (1)
asus ASUS_T00J1 (3/20/20...
Files
Hex Dump
Online Info
5:58:51 PM
3/20/2017
Android
IMEI: 352594071029082
USB
Manufacturer: asus
Model: ASUS_T00J
IMEI: 352594071029082
Serial Nr.: F5AZFG25Z381
ICCID: 89918740400086432501
IMSI: 405874053213249
Operator: Not available
Phone time: 3/20/2017 5:58:51 PM
Software revision: 4.4.2 (19)
Connected via: Forensic Connector 1.1.45-21825 (F)
Phonebook (...
Call Logs
Messages
Calendar
Applications
Application D...
Media
User Files
Files
SIM card (Rea...
8991874040...
4058740532...
Uninstall Connector
Report Wizard
Reports
Screenshot

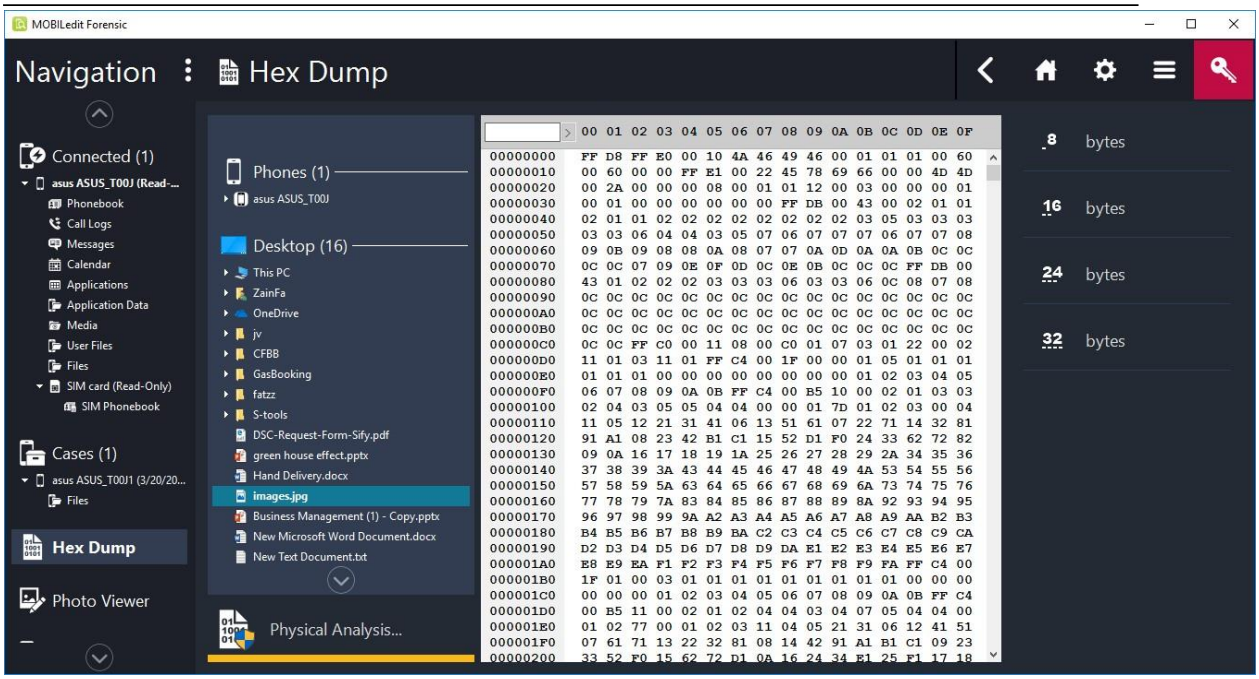

MOBILedit Forensic
Navigation
Files - asus ASUS_T00J
Start
Connected (1)
asus ASUS_T00J (Read-...
Phonebook
Call Logs
Messages
Calendar
Applications
Application Data
Media
User Files
Files
SIM card (Read-Only)
SIM Phonebook
Cases (1)
asus ASUS_T00J1 (3/20/20...
Files
Hex Dump
Files
acct
ADF
APD
cache
config
data
dev
factory
lib
media
mnt
proc
res
root
sbin
storage
sys
system
temp_data
usr
File Name
Size
Created
Modified
Reread

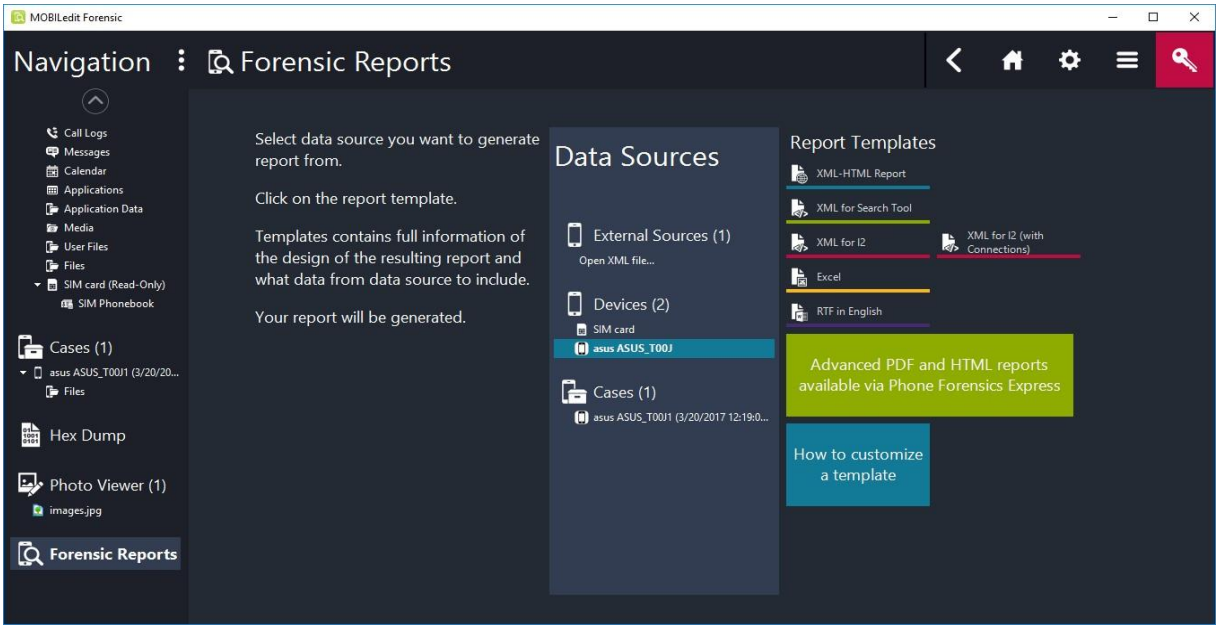

MOBILedit Forensic Wizard
Data acquire settings
Please set the following options for data acquiring.
Data will be stored in the "Cases" folder.
Device Label:
asus ASUS_T00J1
Device Name:
asus ASUS_T00J1
Device Evidence Number:
12345
Owner Name:
XYZ
Owner Phone Number:
9757297578
Phone Notes:
Best Features
Device Capabilities
Files
Communication Log Of Backup Operation
Create:
C:\Users\ZainFa\Documents\MOBILedit! Forensic\Logs\xyz.log
Browse...
< Back
Next >
Cancel


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
< Back
Next >
Cancel


MOBILedit Forensic
Navigation
Files - asus ASUS_T00J1 (3/20/2017 12:19:03 PM)
Start
Connected (1)
asus ASUS_T00J (Read-...
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
Files
ADF
APD
factory
media
storage
temp_data
File Name
Size
Created
Modified
ADF <folder> <unknown> <unknown>
APD <folder> <unknown> <unknown>
factory <folder> <unknown> <unknown>
media <folder> <unknown> <unknown>
storage <folder> <unknown> <unknown>
temp_data <folder> <unknown> <unknown>


MOBILedit Forensic
Navigation
Photo Viewer
Connected (1)
asus ASUS_T00J (Read-...
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
Phones
asus ASUS_T00J
asus ASUS_T00J1 (3/20/2017 12:19:03 PM)
Files
ADF
APD
factory
media
storage
temp_data
Desktop
This PC
ZainFa
OneDrive
CFBB
fatzz
GasBooking
jv
S-tools
Business Management (1) - Copy.pptx
DSC-Request-Form-Sify.pdf
Form-Admin.doc
green house effect.pptx
Hand Delivery.docx
images.jpg
New Microsoft Word Document.docx
New Text Document.txt
Photo Preview
Photo Info
Width: 263
Height: 192
Size: 19.37 KB
Show Photo Preview
from harddrive
from phone
Show Preview
C:\Users\ZainFa\Desktop\images.jpg
Open


MOBILedit Forensic
Navigation
Hex Dump
Connected (1)
asus ASUS_T00J (Read-...
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
Phones (1)
asus ASUS_T00J
Desktop (16)
This PC
ZainFa
OneDrive
jv
CFBB
GasBooking
fatzz
S-tools
DSC-Request-Form-Sify.pdf
green house effect.pptx
Hand Delivery.docx
images.jpg
Business Management (1) - Copy.pptx
New Microsoft Word Document.docx
New Text Document.txt
Physical Analysis...
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
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 03 05 03 03 03
00000050 03 03 06 04 04 03 05 07 06 07 07 07 06 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 0E 0B 0C 0C 0C FF DB 00
00000080 43 01 02 02 02 03 03 03 06 03 03 06 0C 08 07 08
00000090 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
000000A0 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
000000B0 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 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 05 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 05 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
8 bytes
16 bytes
24 bytes
32 bytes


MOBILedit Forensic
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
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