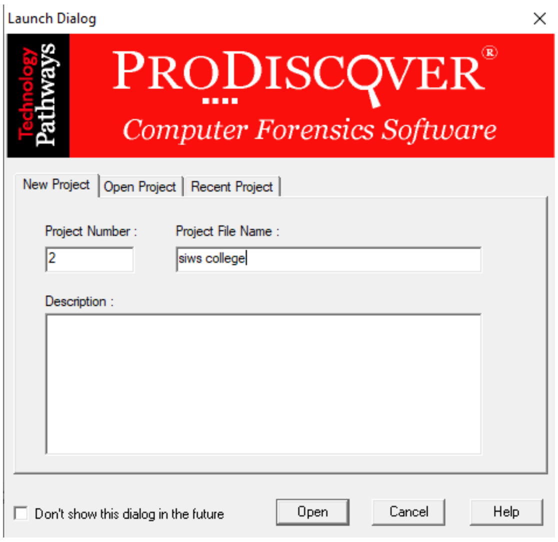
INDEX

PRACTICAL NO. 1

AIM :

THEORY :

Step1 : first open ProDiscover basic and start with new case

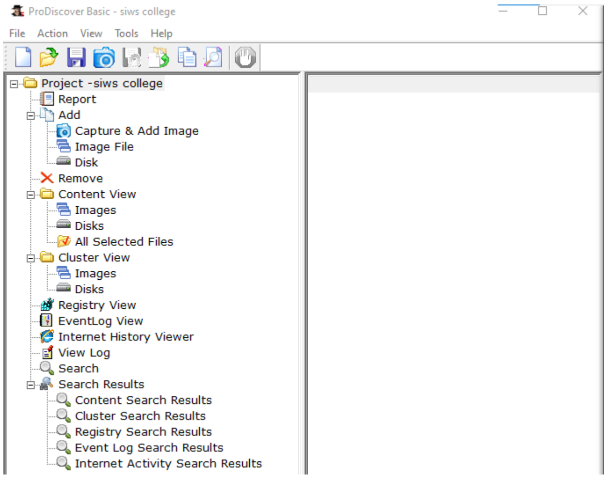


Project Number : 2

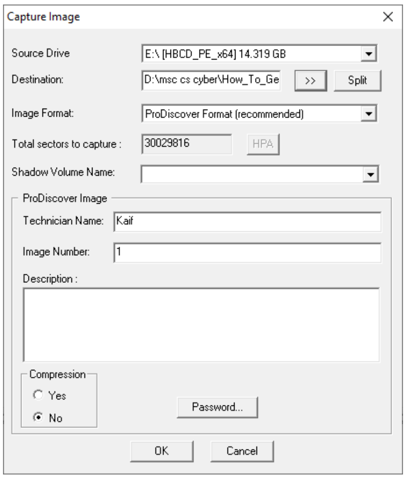
Project File Name : siws college

Description :

Step 2 : the created project appears in left pane and select add capture and add image



Step 3:



Source Drive: E:\ [HBCD_PE_x64] 14.319 GB

Destination: D:\msc cs cyber\How_To_Ge

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 30029816

Shadow Volume Name:

ProDiscover Image

Technician Name: Kaif

Image Number: 1

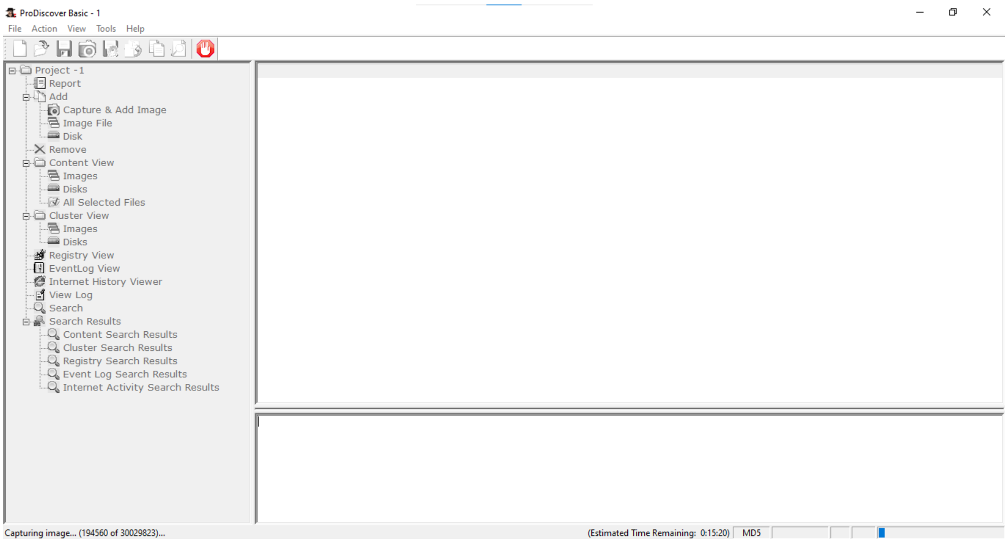
Description :

Compression

○ Yes

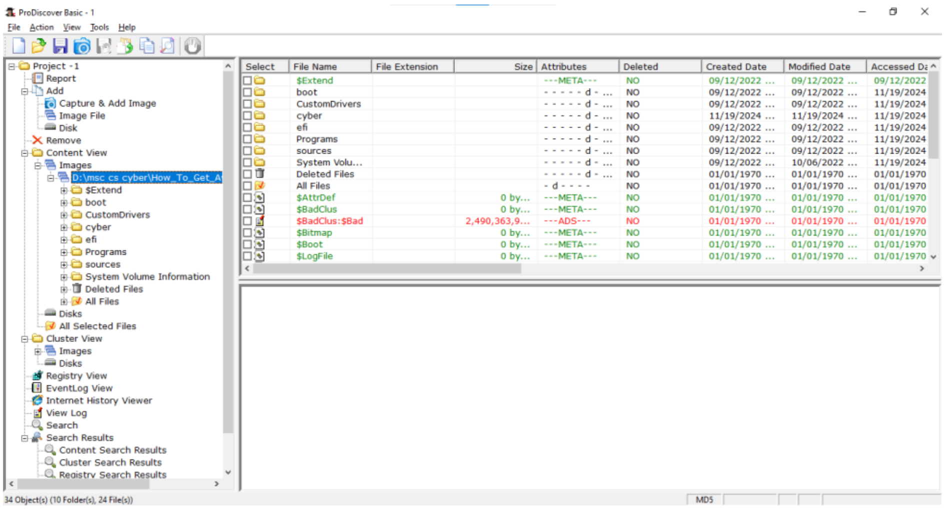
● No

Step 4:



Capturing image... (194560 of 30029823)... (Estimated Time Remaining: 0:15:20)

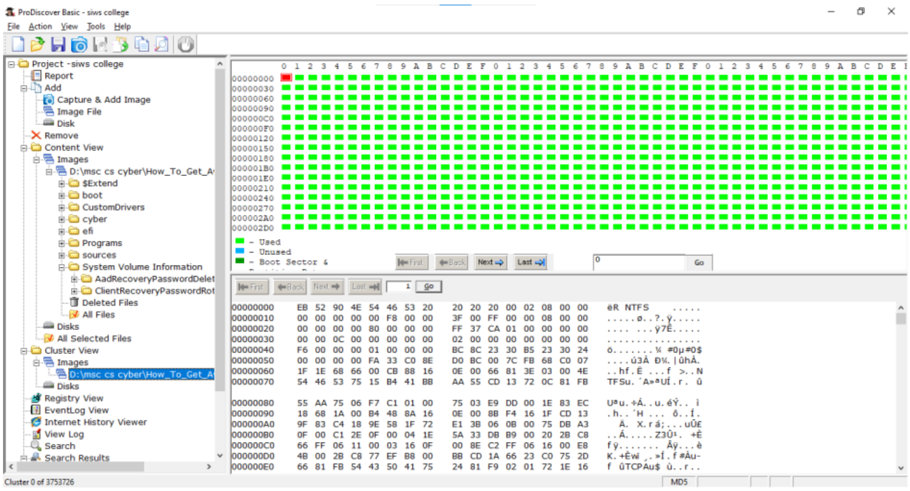
Step 5:



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Da
□	$Extend			---META---	NO	09/12/2022 ...	09/12/2022 ...	09/12/2022
□	boot			- - - - - d - ...	NO	09/12/2022 ...	09/12/2022 ...	11/19/2024
□	CustomDrivers			- - - - - d - ...	NO	09/12/2022 ...	09/12/2022 ...	11/19/2024
□	cyber			- - - - - d - ...	NO	11/19/2024 ...	11/19/2024 ...	11/19/2024
□	efi			- - - - - d - ...	NO	09/12/2022 ...	09/12/2022 ...	11/19/2024
□	Programs			- - - - - d - ...	NO	09/12/2022 ...	09/12/2022 ...	11/19/2024
□	sources			- - - - - d - ...	NO	09/12/2022 ...	09/12/2022 ...	11/19/2024
□	System Volu...			- - - - - d - ...	NO	09/12/2022 ...	10/06/2022 ...	11/19/2024
□	Deleted Files			- - - - - d - ...	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	All Files			- d - - - -	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	$AttrDef		0 by...	---META---	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	$BadClus		0 by...	---META---	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	$BadClus:$Bad		2,490,363,9...	---ADS---	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	$Bitmap		0 by...	---META---	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	$Boot		0 by...	---META---	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970
□	$LogFile		0 by...	---META---	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970

34 Object(s) (10 Folder(s), 24 File(s))

Step 6:

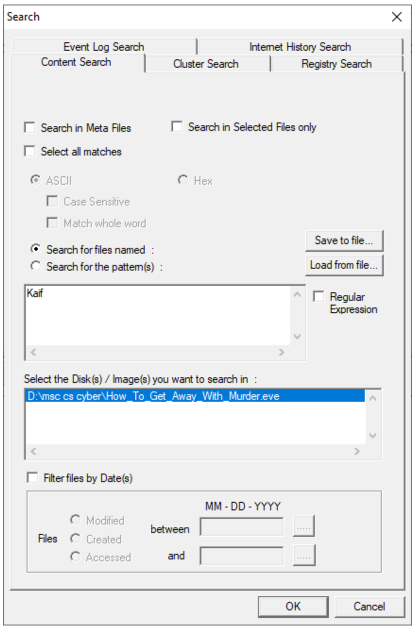


```
00000000   EB 52 90 4E 54 46 53 20   20 20 20 00 02 08 00 00   ëR NTFS     .....
00000010   00 00 00 00 00 F8 00 00   3F 00 FF 00 00 08 00 00   ......ø..?.ÿ.....
00000020   00 00 00 00 80 00 00 00   FF 37 CA 01 00 00 00 00   .... ...ÿ7Ê.....
00000030   00 00 0C 00 00 00 00 00   02 00 00 00 00 00 00 00   ................
00000040   F6 00 00 00 01 00 00 00   BC 8C 23 30 B5 23 30 24   ö.......¼ #0µ#0$
00000050   00 00 00 00 FA 33 C0 8E   D0 BC 00 7C FB 68 C0 07   ....ú3À Ð¼.|ûhÀ.
00000060   1F 1E 68 66 00 CB 88 16   0E 00 66 81 3E 03 00 4E   ..hf.Ë ...f >..N
00000070   54 46 53 75 15 B4 41 BB   AA 55 CD 13 72 0C 81 FB   TFSu.´A»ªUÍ.r. û

00000080   55 AA 75 06 F7 C1 01 00   75 03 E9 DD 00 1E 83 EC   Uªu.÷Á..u.éÝ.. ì
00000090   18 68 1A 00 B4 48 8A 16   0E 00 8B F4 16 1F CD 13   .h..´H ... ô..Í.
000000A0   9F 83 C4 18 9E 58 1F 72   E1 3B 06 0B 00 75 DB A3     Ä. X.rá;...uÛ£
000000B0   0F 00 C1 2E 0F 00 04 1E   5A 33 DB B9 00 20 2B C8   ..Á.....Z3Û¹. +È
000000C0   66 FF 06 11 00 03 16 0F   00 8E C2 FF 06 16 00 E8   fÿ.......  Âÿ...è
000000D0   4B 00 2B C8 77 EF B8 00   BB CD 1A 66 23 C0 75 2D   K.+Èwï ¸.»Í.f#Àu-
000000E0   66 81 FB 54 43 50 41 75   24 81 F9 02 01 72 1E 16   f ûTCPAu$ ù..r..
```

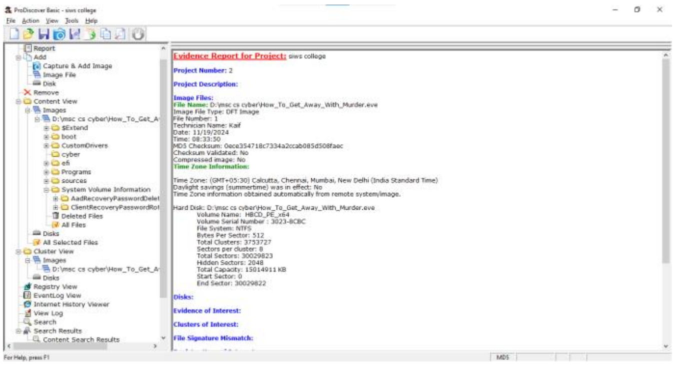
Cluster 0 of 3753726

Step 7:



□ 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) :
Kaif
□ Regular Expression
Select the Disk(s) / Image(s) you want to search in :
D:\msc cs cyber\How_To_Get_Away_With_Murder.eve
□ Filter files by Date(s)
Files ○ Modified ○ Created ○ Accessed between and

Step 8:



Evidence Report for Project: siws college

Project Number: 2

Project Description:

Image Files:
File Name: D:\msc cs cyber\How_To_Get_Away_With_Murder.eve
Image File Type: DFT Image
File Number: 1
Technician Name: Kaif
Date: 11/19/2024
Time: 08:33:50
MD5 Checksum: 0ece354718c7334a2ccab085d508faec
Checksum Validated: No
Compressed image: No
Time Zone Information:

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

Hard Disk: D:\msc cs cyber\How_To_Get_Away_With_Murder.eve
Volume Name: HBCD_PE_x64
Volume Serial Number : 3023-8CBC
File System: NTFS
Bytes Per Sector: 512
Total Clusters: 3753727
Sectors per cluster: 8
Total Sectors: 30029823
Hidden Sectors: 2048
Total Capacity: 15014911 KB
Start Sector: 0
End Sector: 30029822

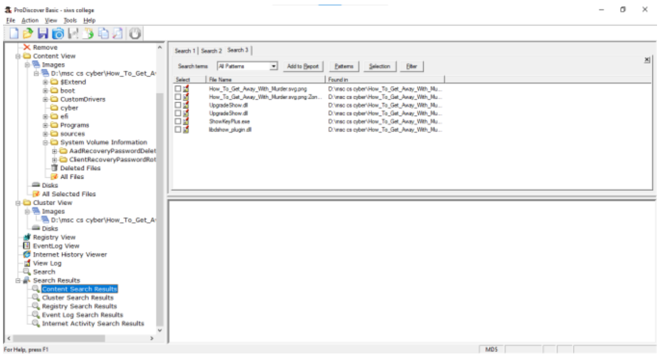
Disks:

Evidence of Interest:

Clusters of Interest:

File Signature Mismatch:

Step 9:



Search terms: All Patterns

Select	File Name	Found in
□	How_To_Get_Away_With_Murder.svg.png	D:\msc cs cyber\How_To_Get_Away_With_Mu...
□	How_To_Get_Away_With_Murder.svg.png:Zon...	D:\msc cs cyber\How_To_Get_Away_With_Mu...
□	UpgradeShow.dll	D:\msc cs cyber\How_To_Get_Away_With_Mu...
□	UpgradeShow.dll	D:\msc cs cyber\How_To_Get_Away_With_Mu...
□	ShowKeyPlus.exe	D:\msc cs cyber\How_To_Get_Away_With_Mu...
□	libdshow_plugin.dll	D:\msc cs cyber\How_To_Get_Away_With_Mu...

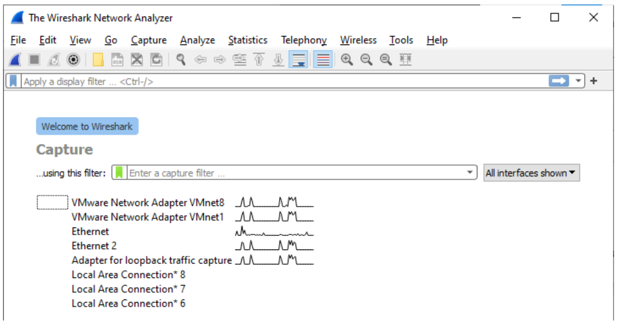
CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

PRACTICAL NO. 2

AIM :

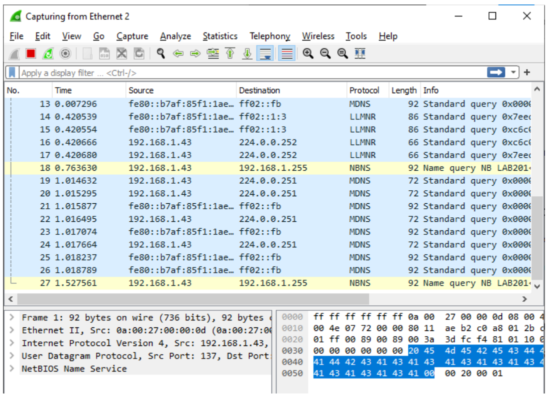
THEORY :

Step1:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown

```
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
```

Step2:

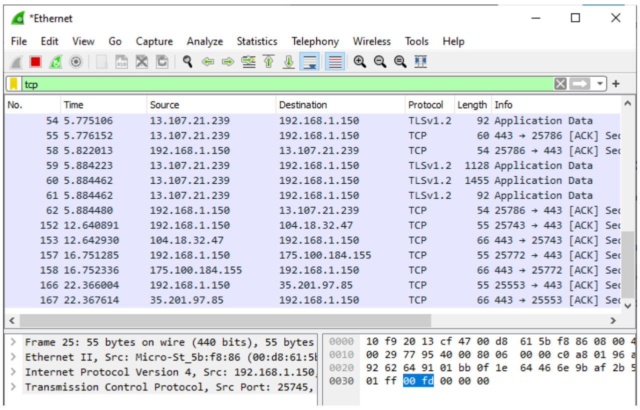

Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source                  Destination    Protocol Length Info
  13 0.007296  fe80::b7af:85f1:1ae…    ff02::fb       MDNS     92 Standard query 0x000
  14 0.420539  fe80::b7af:85f1:1ae…    ff02::1:3      LLMNR    86 Standard query 0x7ee
  15 0.420554  fe80::b7af:85f1:1ae…    ff02::1:3      LLMNR    86 Standard query 0xc6c
  16 0.420666  192.168.1.43            224.0.0.252    LLMNR    66 Standard query 0xc6c
  17 0.420680  192.168.1.43            224.0.0.252    LLMNR    66 Standard query 0x7ee
  18 0.763630  192.168.1.43            192.168.1.255  NBNS     92 Name query NB LAB201
  19 1.014632  192.168.1.43            224.0.0.251    MDNS     72 Standard query 0x000
  20 1.015295  192.168.1.43            224.0.0.251    MDNS     72 Standard query 0x000
  21 1.015877  fe80::b7af:85f1:1ae…    ff02::fb       MDNS     92 Standard query 0x000
  22 1.016495  192.168.1.43            224.0.0.251    MDNS     72 Standard query 0x000
  23 1.017074  fe80::b7af:85f1:1ae…    ff02::fb       MDNS     92 Standard query 0x000
  24 1.017664  192.168.1.43            224.0.0.251    MDNS     72 Standard query 0x000
  25 1.018237  fe80::b7af:85f1:1ae…    ff02::fb       MDNS     92 Standard query 0x000
  26 1.018789  fe80::b7af:85f1:1ae…    ff02::fb       MDNS     92 Standard query 0x000
  27 1.527561  192.168.1.43            192.168.1.255  NBNS     92 Name query NB LAB201

> Frame 1: 92 bytes on wire (736 bits), 92 bytes
> Ethernet II, Src: 0a:00:27:00:00:0d (0a:00:27:0
> Internet Protocol Version 4, Src: 192.168.1.43,
> User Datagram Protocol, Src Port: 137, Dst Port
> NetBIOS Name Service

0000  ff ff ff ff ff ff 0a 00  27 00 00 0d 08 00 4
0010  00 4e 07 72 00 00 80 11  ae b2 c0 a8 01 2b c
0020  01 ff 00 89 00 89 00 3a  3d fc f4 81 01 10 0
0030  00 00 00 00 00 00 20 45  4d 45 42 45 43 44 4
0040  41 44 42 43 41 43 41 43  41 43 41 43 41 43 4
0050  41 43 41 43 41 43 41 00  00 20 00 01
```

Step3:


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

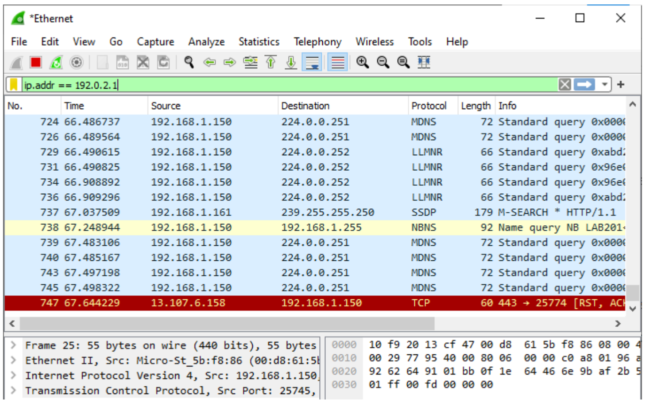
tcp

```
No.  Time       Source            Destination       Protocol Length Info
  54 5.775106   13.107.21.239     192.168.1.150     TLSv1.2    92 Application Data
  55 5.776152   13.107.21.239     192.168.1.150     TCP        60 443 → 25786 [ACK] Se
  58 5.822013   192.168.1.150     13.107.21.239     TCP        54 25786 → 443 [ACK] Se
  59 5.884223   13.107.21.239     192.168.1.150     TLSv1.2  1128 Application Data
  60 5.884462   13.107.21.239     192.168.1.150     TLSv1.2  1455 Application Data
  61 5.884462   13.107.21.239     192.168.1.150     TLSv1.2    92 Application Data
  62 5.884480   192.168.1.150     13.107.21.239     TCP        54 25786 → 443 [ACK] Se
 152 12.640891  192.168.1.150     104.18.32.47      TCP        55 25743 → 443 [ACK] Se
 153 12.642930  104.18.32.47      192.168.1.150     TCP        66 443 → 25743 [ACK] Se
 157 16.751285  192.168.1.150     175.100.184.155   TCP        55 25772 → 443 [ACK] Se
 158 16.752336  175.100.184.155   192.168.1.150     TCP        66 443 → 25772 [ACK] Se
 166 22.366004  192.168.1.150     35.201.97.85      TCP        55 25553 → 443 [ACK] Se
 167 22.367614  35.201.97.85      192.168.1.150     TCP        66 443 → 25553 [ACK] Se

> Frame 25: 55 bytes on wire (440 bits), 55 bytes
> Ethernet II, Src: Micro-St_5b:f8:86 (00:d8:61:5
> Internet Protocol Version 4, Src: 192.168.1.150,
> Transmission Control Protocol, Src Port: 25745,

0000  10 f9 20 13 cf 47 00 d8  61 5b f8 86 08 00 4
0010  00 29 77 95 40 00 80 06  00 00 c0 a8 01 96 a
0020  92 62 64 91 01 bb 0f 1e  64 46 6e 9b af 2b 5
0030  01 ff 00 fd 00 00 00
```

Step4:


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

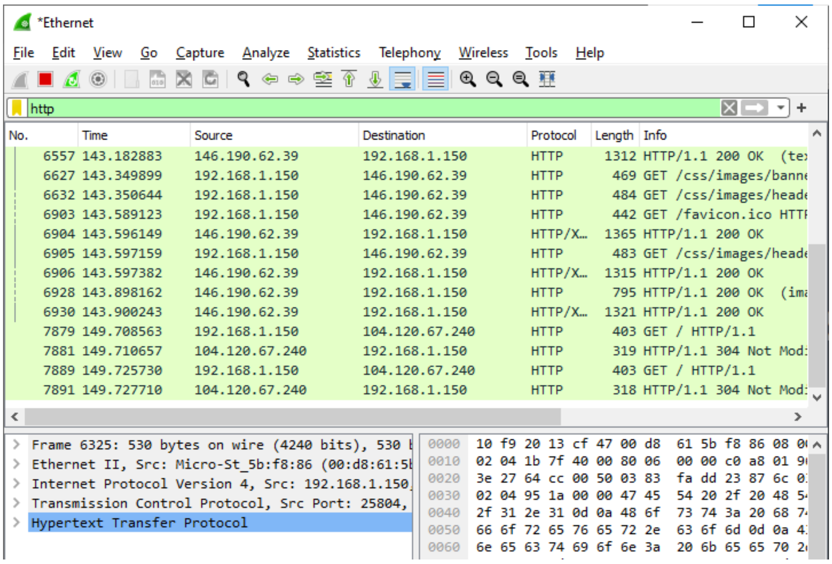
ip.addr == 192.0.2.1

```
No.  Time       Source          Destination       Protocol Length Info
 724 66.486737  192.168.1.150   224.0.0.251       MDNS       72 Standard query 0x000
 726 66.489564  192.168.1.150   224.0.0.251       MDNS       72 Standard query 0x000
 729 66.490615  192.168.1.150   224.0.0.252       LLMNR      66 Standard query 0xabd
 731 66.490825  192.168.1.150   224.0.0.252       LLMNR      66 Standard query 0x96e
 734 66.908892  192.168.1.150   224.0.0.252       LLMNR      66 Standard query 0x96e
 736 66.909296  192.168.1.150   224.0.0.252       LLMNR      66 Standard query 0xabd
 737 67.037509  192.168.1.161   239.255.255.250   SSDP      179 M-SEARCH * HTTP/1.1
 738 67.248944  192.168.1.150   192.168.1.255     NBNS       92 Name query NB LAB201
 739 67.483106  192.168.1.150   224.0.0.251       MDNS       72 Standard query 0x000
 740 67.485167  192.168.1.150   224.0.0.251       MDNS       72 Standard query 0x000
 743 67.497198  192.168.1.150   224.0.0.251       MDNS       72 Standard query 0x000
 745 67.498322  192.168.1.150   224.0.0.251       MDNS       72 Standard query 0x000
 747 67.644229  13.107.6.158    192.168.1.150     TCP        60 443 → 25774 [RST, AC

> Frame 25: 55 bytes on wire (440 bits), 55 bytes
> Ethernet II, Src: Micro-St_5b:f8:86 (00:d8:61:5
> Internet Protocol Version 4, Src: 192.168.1.150,
> Transmission Control Protocol, Src Port: 25745,

0000  10 f9 20 13 cf 47 00 d8  61 5b f8 86 08 00 4
0010  00 29 77 95 40 00 80 06  00 00 c0 a8 01 96 a
0020  92 62 64 91 01 bb 0f 1e  64 46 6e 9b af 2b 5
0030  01 ff 00 fd 00 00 00
```

Step5:


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

http

```
No.   Time        Source          Destination     Protocol Length Info
 6557 143.182883  146.190.62.39   192.168.1.150   HTTP      1312 HTTP/1.1 200 OK  (te
 6627 143.349899  192.168.1.150   146.190.62.39   HTTP       469 GET /css/images/banne
 6632 143.350644  192.168.1.150   146.190.62.39   HTTP       484 GET /css/images/heade
 6903 143.589123  192.168.1.150   146.190.62.39   HTTP       442 GET /favicon.ico HTTI
 6904 143.596149  146.190.62.39   192.168.1.150   HTTP/X…   1365 HTTP/1.1 200 OK
 6905 143.597159  192.168.1.150   146.190.62.39   HTTP       483 GET /css/images/heade
 6906 143.597382  146.190.62.39   192.168.1.150   HTTP/X…   1315 HTTP/1.1 200 OK
 6928 143.898162  146.190.62.39   192.168.1.150   HTTP       795 HTTP/1.1 200 OK  (ima
 6930 143.900243  146.190.62.39   192.168.1.150   HTTP/X…   1321 HTTP/1.1 200 OK
 7879 149.708563  192.168.1.150   104.120.67.240  HTTP       403 GET / HTTP/1.1
 7881 149.710657  104.120.67.240  192.168.1.150   HTTP       319 HTTP/1.1 304 Not Mod:
 7889 149.725730  192.168.1.150   104.120.67.240  HTTP       403 GET / HTTP/1.1
 7891 149.727710  104.120.67.240  192.168.1.150   HTTP       318 HTTP/1.1 304 Not Mod:
```

```
> Frame 6325: 530 bytes on wire (4240 bits), 530 b
> Ethernet II, Src: Micro-St_5b:f8:86 (00:d8:61:5b
> Internet Protocol Version 4, Src: 192.168.1.150,
> Transmission Control Protocol, Src Port: 25804,
> Hypertext Transfer Protocol
```

```
0000  10 f9 20 13 cf 47 00 d8  61 5b f8 86 08 0
0010  02 04 1b 7f 40 00 80 06  00 00 c0 a8 01 9
0020  3e 27 64 cc 00 50 03 83  fa dd 23 87 6c 0
0030  02 04 95 1a 00 00 47 45  54 20 2f 20 48 5
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 7
0050  66 6f 72 65 76 65 72 2e  63 6f 6d 0d 0a 4
0060  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2
```

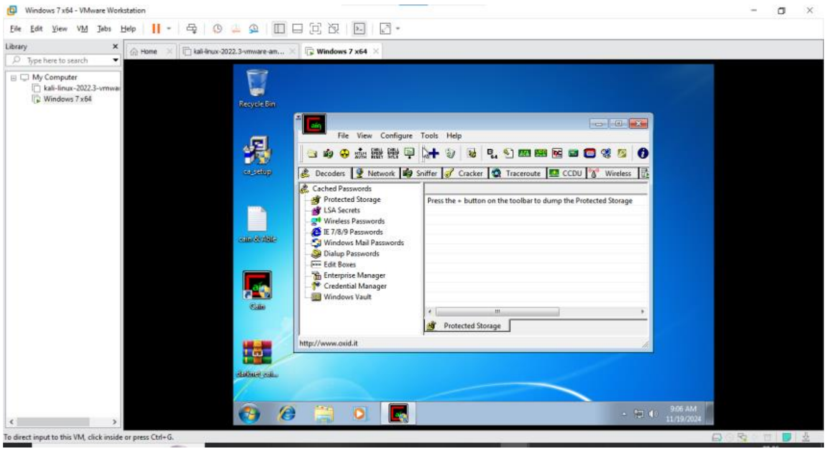
CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

PRACTICAL NO. 3

AIM :

THEORY :

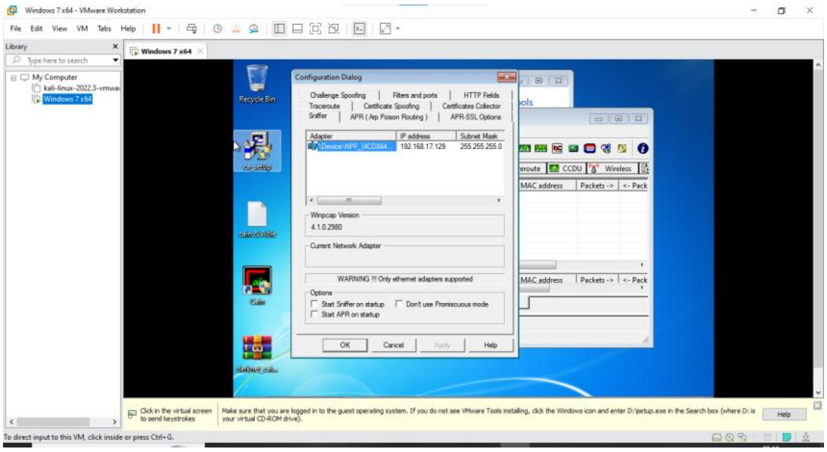
Step1:



Press the + button on the toolbar to dump the Protected Storage

To direct input to this VM, click inside or press Ctrl+G.

Step2:



Adapter	IP address	Subnet Mask
\Device\NPF_{4CD844...	192.168.17.129	255.255.255.0

Winpcap Version
4.1.0.2980

Current Network Adapter

WARNING !!! Only ethernet adapters supported

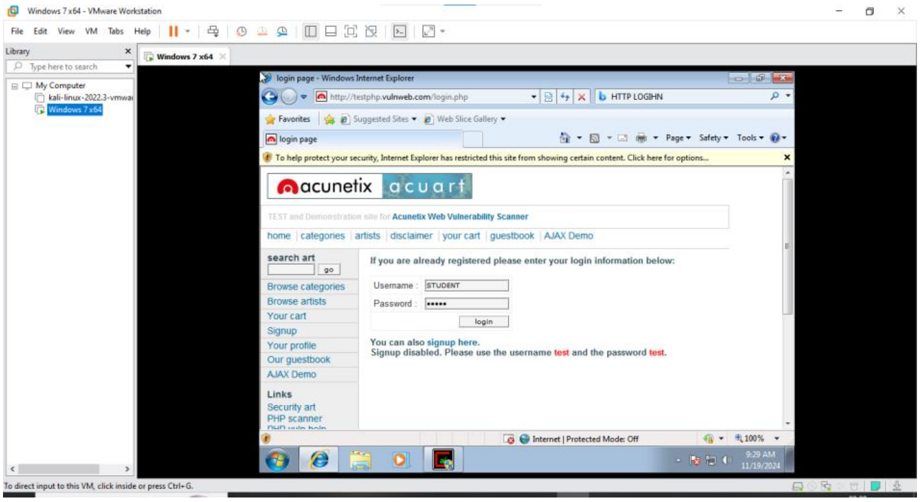
Options
□ Start Sniffer on startup □ Don't use Promiscuous mode
□ Start APR on startup

Click in the virtual screen to send keystrokes

Make sure that you are logged in to the guest operating system. If you do not see VMware Tools installing, click the Windows icon and enter D:\setup.exe in the Search box (where D: is your virtual CD-ROM drive).

To direct input to this VM, click inside or press Ctrl+G.

Step3:



http://testphp.vulnweb.com/login.php

HTTP LOGIHN

To help protect your security, Internet Explorer has restricted this site from showing certain content. Click here for options...

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

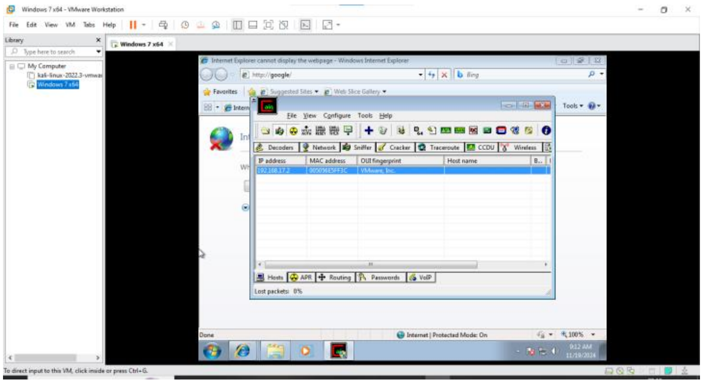
Username : STUDENT

Password : •••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

To direct input to this VM, click inside or press Ctrl+G.

Step4:



Internet Explorer cannot display the webpage - Windows Internet Explorer

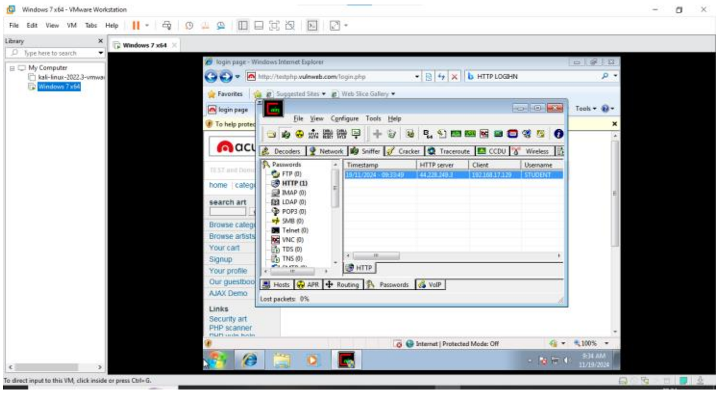
http://google/

IP address	MAC address	OUI fingerprint	Host name	B...
192.168.17.2	005056E5FF3C	VMware, Inc.		

Lost packets: 0%

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2022.3-vmware
Windows 7 x64
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless
Hosts APR Routing Passwords VoIP
Internet | Protected Mode: On
100%
9:12 AM
11/19/2024
To direct input to this VM, click inside or press Ctrl+G.

Step5:



login page - Windows Internet Explorer

http://testphp.vulnweb.com/login.php

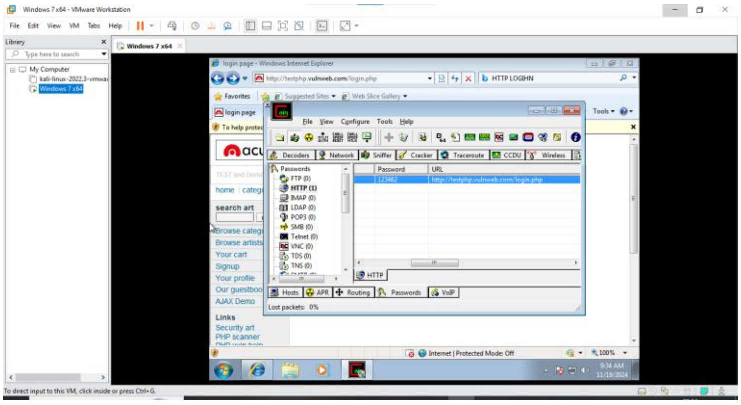
HTTP LOGIHN

Timestamp	HTTP server	Client	Username
19/11/2024 - 09:33:49	44.228.249.3	192.168.17.129	STUDENT

Lost packets: 0%

Windows 7 x64 - VMware Workstation
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless
Passwords
FTP (0)
HTTP (1)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
HTTP
Hosts APR Routing Passwords VoIP
home
search art
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
Internet | Protected Mode: Off
9:34 AM
11/19/2024
To direct input to this VM, click inside or press Ctrl+G.

Step6:



login page - Windows Internet Explorer

http://testphp.vulnweb.com/login.php

HTTP LOGIHN

Password	URL
123462	http://testphp.vulnweb.com/login.php

Lost packets: 0%

Windows 7 x64 - VMware Workstation
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless
Passwords
FTP (0)
HTTP (1)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
HTTP
Hosts APR Routing Passwords VoIP
Internet | Protected Mode: Off
9:34 AM
11/19/2024
To direct input to this VM, click inside or press Ctrl+G.

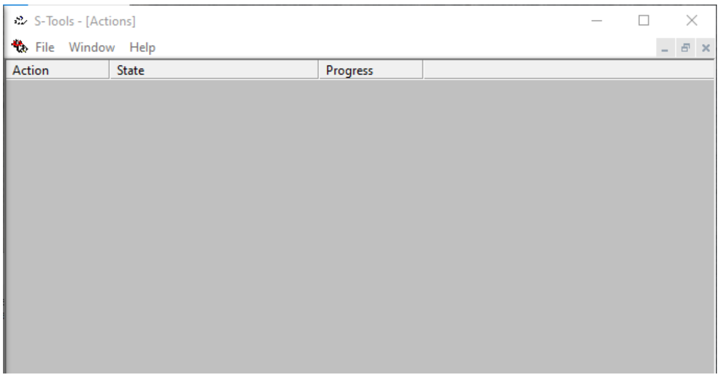
CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

PRACTICAL NO. 4

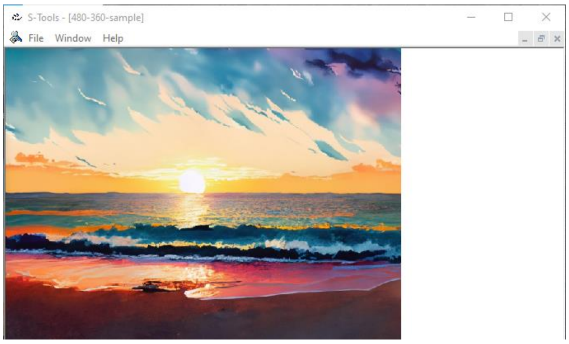
AIM :

THEORY :

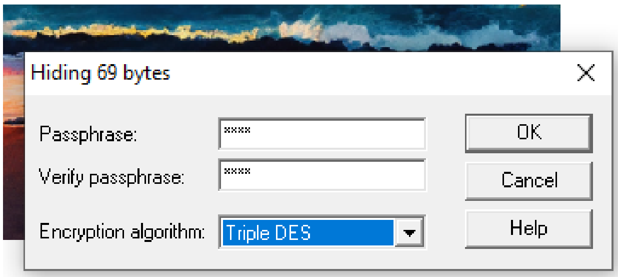
Step 1:



Step 2:



Step 3:

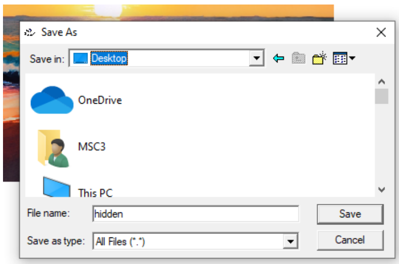

Hiding 69 bytes

Passphrase: ****

Verify passphrase: ****

Encryption algorithm: Triple DES

Step 4:

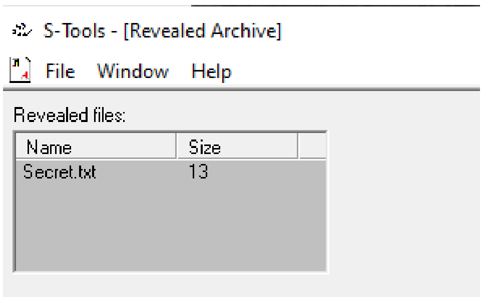


Save in: Desktop

File name: hidden

Save as type: All Files (*.*)

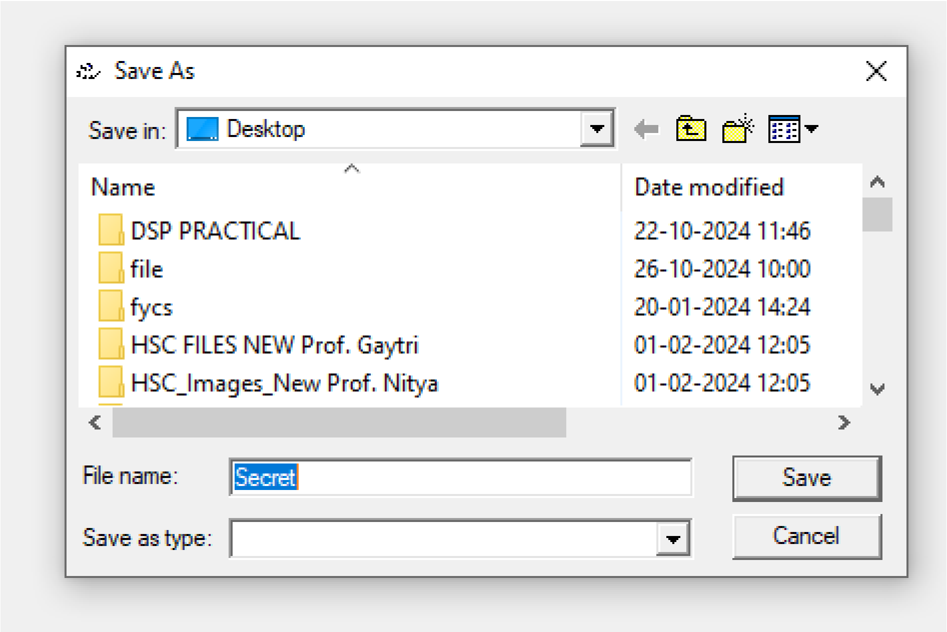
Step 5:



Revealed files:

Name	Size
Secret.txt	13

Step 6:



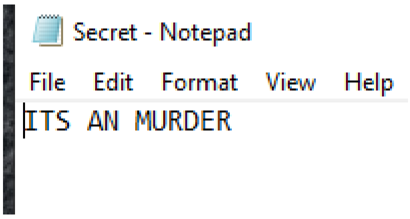
Save in: Desktop

Name	Date modified
DSP PRACTICAL	22-10-2024 11:46
file	26-10-2024 10:00
fycs	20-01-2024 14:24
HSC FILES NEW Prof. Gaytri	01-02-2024 12:05
HSC_Images_New Prof. Nitya	01-02-2024 12:05

File name: Secret

Save as type:

Step 7:



```
ITS AN MURDER
```

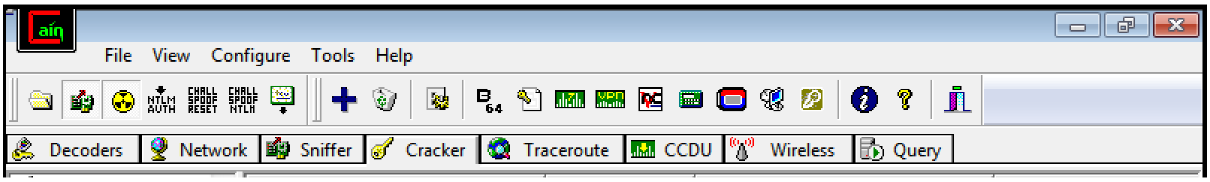
CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

PRACTICAL NO. 5

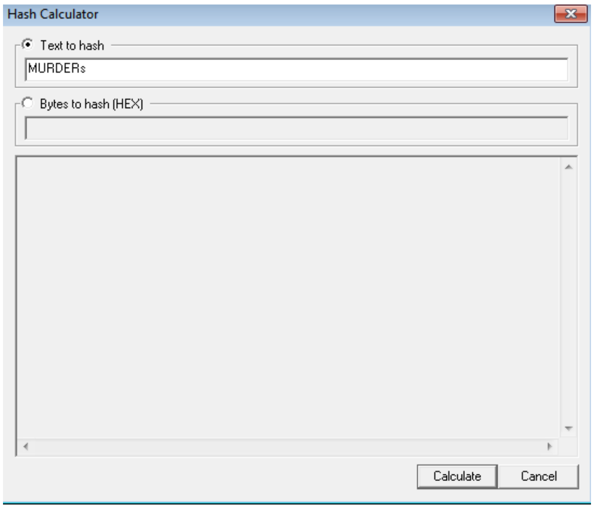
AIM :

THEORY :

Step 1:



Step 2:

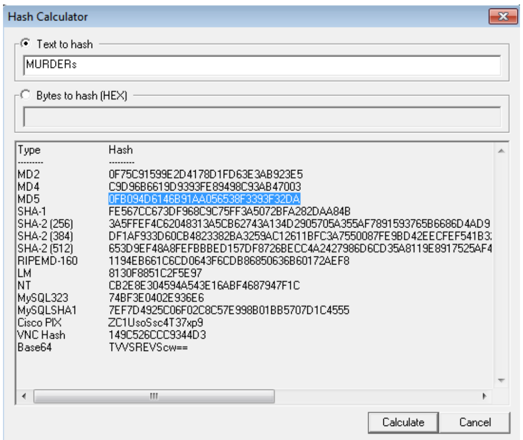


● Text to hash

MURDERs

○ Bytes to hash (HEX)

Step 3:



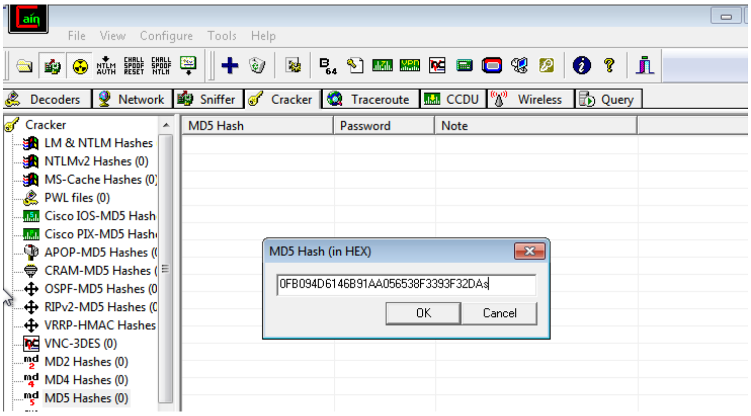
● Text to hash

MURDERs

○ Bytes to hash (HEX)

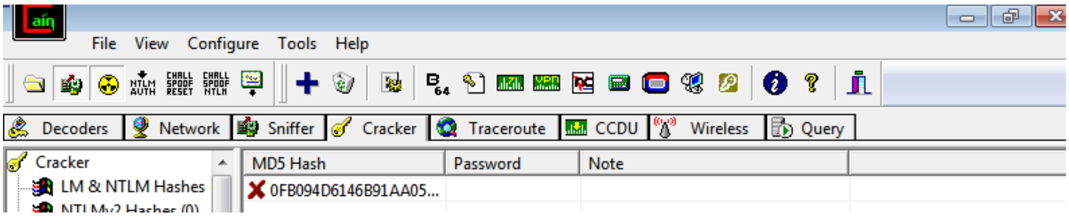
```
Type            Hash
---------       ---------
MD2             0F75C91599E2D4178D1FD63E3AB923E5
MD4             C9D96B6619D9393FE89498C93AB47003
MD5             0FB094D6146B91AA056538F3393F32DA
SHA-1           FE567CC673DF968C9C75FF3A5072BFA282DAA84B
SHA-2 (256)     3A5FFEF4C62048313A5CB62743A134D2905705A355AF7891593765B6686D4AD9
SHA-2 (384)     DF1AF933D60CB4823382BA3259AC12611BFC3A7550087FE9BD42EECFEF541B3
SHA-2 (512)     653D9EF48A8FEFBBBED157DF8726BECC4A2427986D6CD35A8119E8917525AF4
RIPEMD-160      1194EB661C6CD0643F6CDB86850636B60172AEF8
LM              8130F8851C2F5E97
NT              CB2E8E304594A543E16ABF4687947F1C
MySQL323        74BF3E0402E936E6
MySQLSHA1       7EF7D4925C06F02C8C57E998B01BB5707D1C4555
Cisco PIX       ZC1UsoSsc4T37xp9
VNC Hash        149C526CCC9344D3
Base64          TVVSREVScw==
```

Step 4:



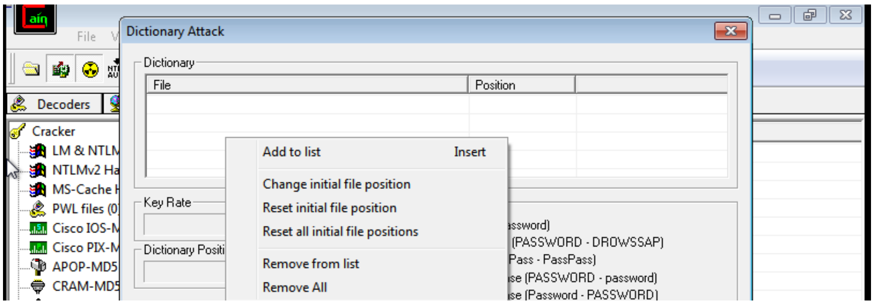
0FB094D6146B91AA056538F3393F32DAs

Step 5:

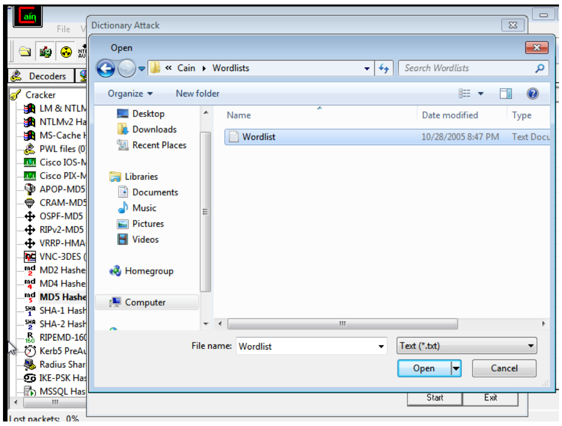


MD5 Hash	Password	Note
0FB094D6146B91AA05...		

Step 6:



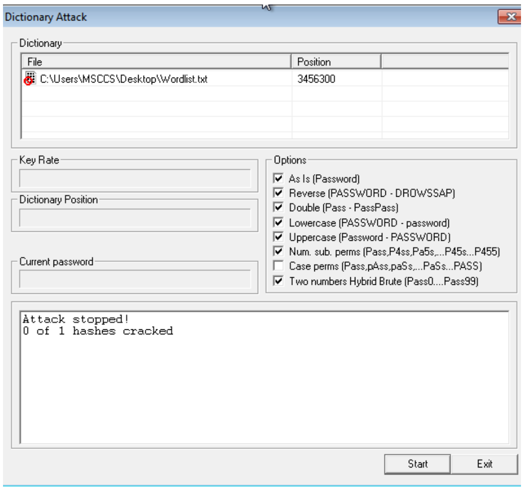
Step 7:



Name	Date modified	Type
Wordlist	10/28/2005 8:47 PM	Text Docu

File name: Wordlist   Text (*.txt)

Step 8:



File	Position
C:\Users\MSCCS\Desktop\Wordlist.txt	3456300

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Attack stopped!
0 of 1 hashes cracked
```

CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

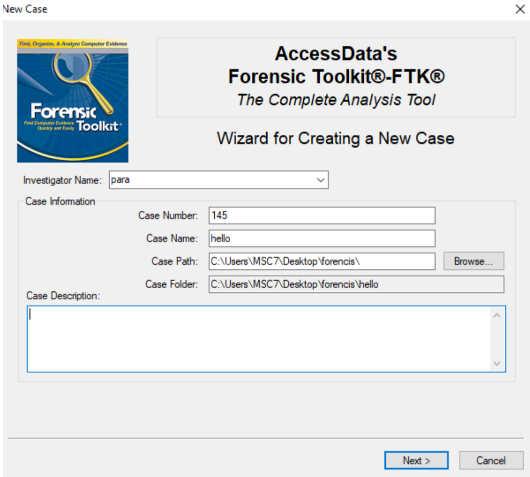
PRACTICAL NO. 6

AIM :

THEORY :

Step 1: open ftk(toolkit app)

Step 2: Add investigator's name, case information, case number, case path & case folder



New Case

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

Wizard for Creating a New Case

Investigator Name: para

Case Information

Case Number: 145

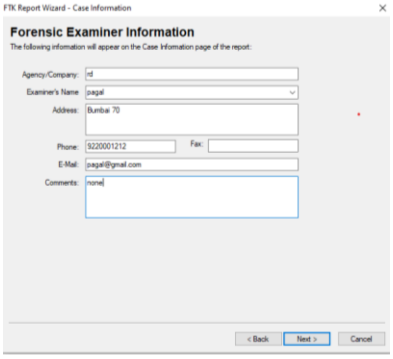
Case Name: hello

Case Path: C:\Users\MSC7\Desktop\forencis\

Case Folder: C:\Users\MSC7\Desktop\forencis\hello

Case Description:

Step 3: add forensic examiner information, then click next



FTK Report Wizard - Case Information

Forensic Examiner Information

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

Agency/Company: rd

Examiner's Name pagal

Address: Bumbai 70

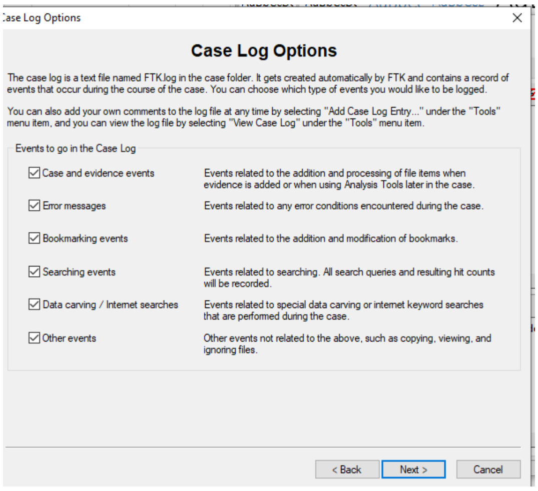
Phone: 9220001212

Fax:

E-Mail: pagal@gmail.com

Comments: none

Step 4: Click next



Case Log Options

Case Log Options

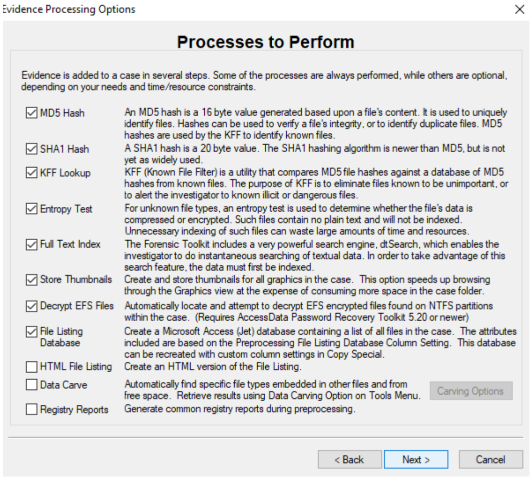
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

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

Events to go in the Case Log

☑ 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.

Step 5: click next

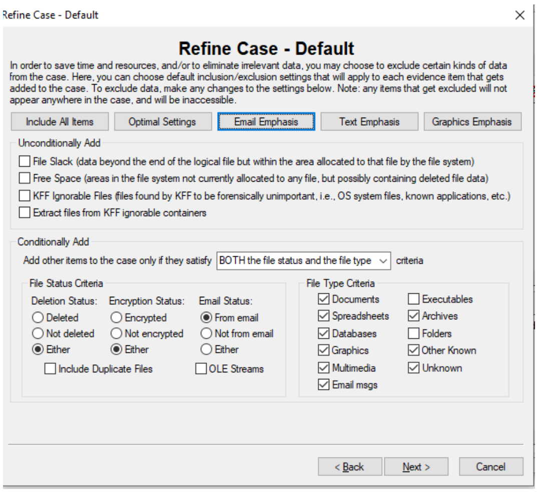


Processes to Perform

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.
□ Registry Reports	Generate common registry reports during preprocessing.

Step 6: click email emphasis, then next



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.

Unconditionally Add

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

Conditionally Add

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

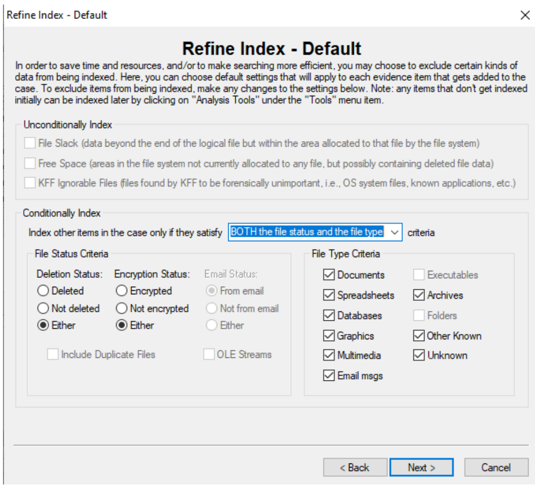
File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	● From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	○ Either
□ Include Duplicate Files		□ OLE Streams

File Type Criteria

☑ Documents	□ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	□ Folders
☑ Graphics	☑ Other Known
☑ Multimedia	☑ Unknown
☑ Email msgs	

Step 7: click next



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

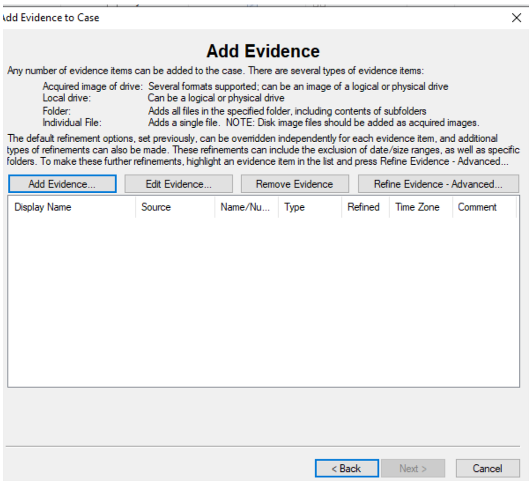
File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	● From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	○ Either
□ Include Duplicate Files		□ OLE Streams

File Type Criteria

☑ Documents	□ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	□ Folders
☑ Graphics	☑ Other Known
☑ Multimedia	☑ Unknown
☑ Email msgs	

Step 8: add evidence

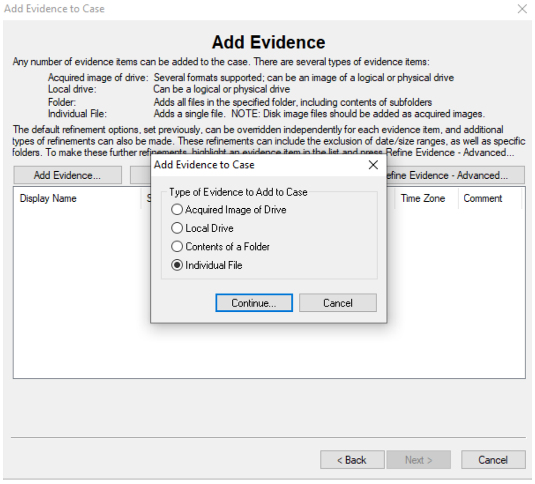


Any number of evidence items can be added to the case. There are several types of evidence items:

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.

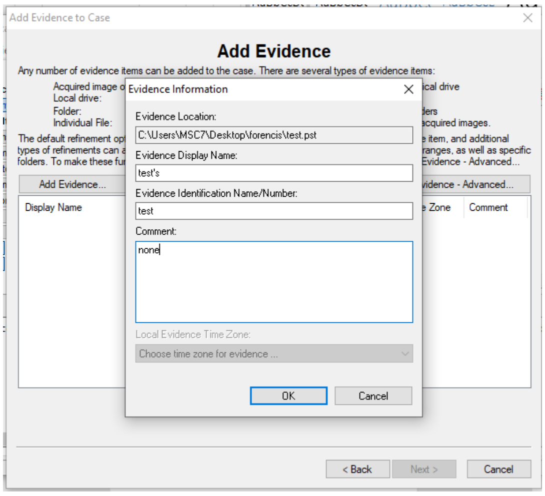
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence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

Step 9: click individual file, add a .pst file and location then click ok



Type of Evidence to Add to Case

○ Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
● Individual File



Evidence Location: C:\Users\MSC7\Desktop\forencis\test.pst

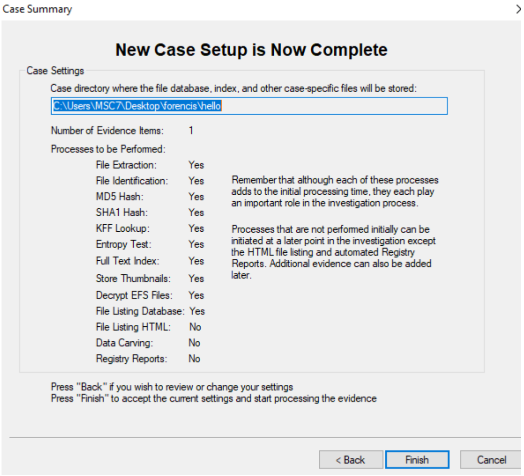
Evidence Display Name: test's

Evidence Identification Name/Number: test

Comment: none

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

Step 10: click finish



Case Summary

New Case Setup is Now Complete

Case Settings

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

C:\Users\MSC7\Desktop\forencis\hello

Number of Evidence Items: 1

Processes to be Performed:

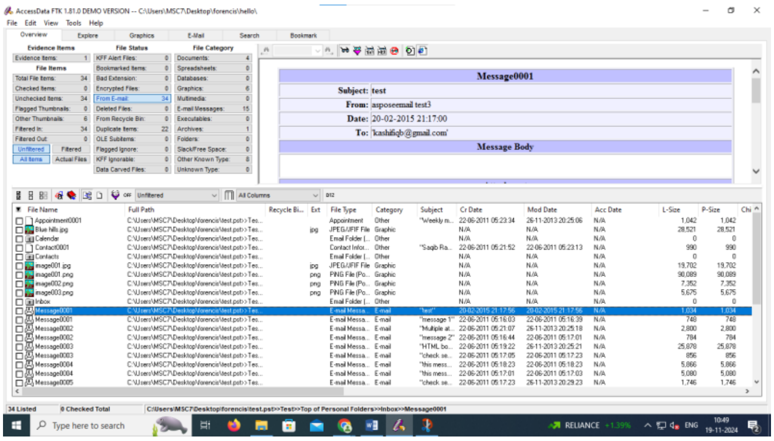
File Extraction:	Yes
File Identification:	Yes
MD5 Hash:	Yes
SHA1 Hash:	Yes
KFF Lookup:	Yes
Entropy Test:	Yes
Full Text Index:	Yes
Store Thumbnails:	Yes
Decrypt EFS Files:	Yes
File Listing Database:	Yes
File Listing HTML:	No
Data Carving:	No
Registry Reports:	No

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

Step 11: click on from email, any message below.



AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\MSC7\Desktop\forencis\hello\

File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	4
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	34	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	6
Unchecked Items:	34	From E-mail:	34	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	15
Other Thumbnails:	6	From Recycle Bin:	0	Executables:	0
Filtered In:	34	Duplicate Items:	22	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	8
		Data Carved Files:	0	Unknown Type:	0

Message0001

Subject: test

From: asposeemail test3

Date: 20-02-2015 21:17:00

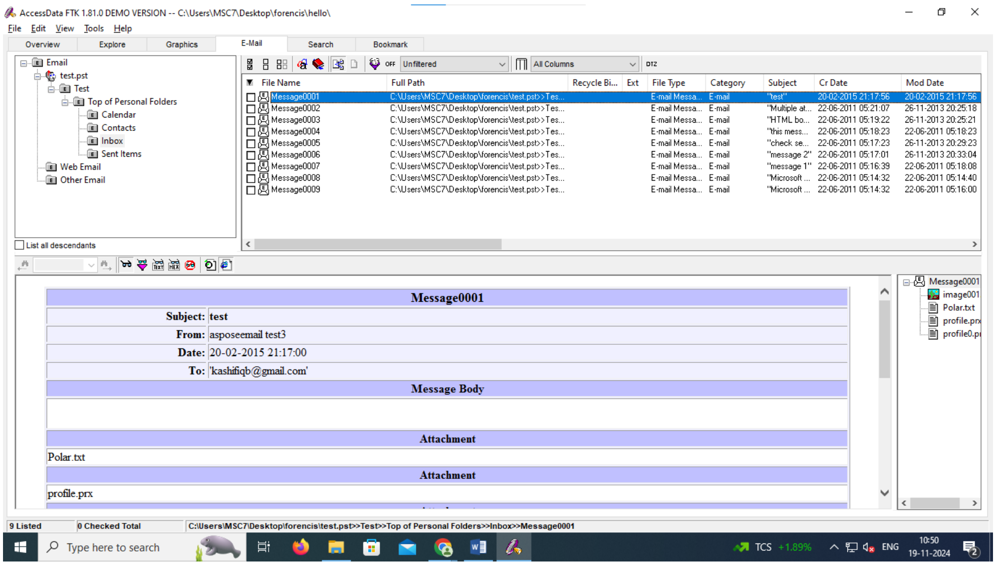
To: 'kashifiqb@gmail.com'

Message Body

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Chi
□ Appointment0001	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			Appointment	Other	"Weekly m...	22-06-2011 05:23:34	26-11-2013 20:25:06	N/A	1,042	1,042	
□ Blue hills.jpg	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...		jpg	JPEG/JFIF File	Graphic		N/A	N/A	N/A	28,521	28,521	
□ Calendar	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			Email Folder [...	Other		N/A	N/A	N/A	0	0	
□ Contact0001	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			Contact Infor...	Other	"Saqib Ra...	22-06-2011 05:21:52	22-06-2011 05:23:13	N/A	990	990	
□ Contacts	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			Email Folder [...	Other		N/A	N/A	N/A	0	0	
□ image001.jpg	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...		jpg	JPEG/JFIF File	Graphic		N/A	N/A	N/A	19,702	19,702	
□ image001.png	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...		png	PNG File (Po...	Graphic		N/A	N/A	N/A	90,089	90,089	
□ image002.png	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...		png	PNG File (Po...	Graphic		N/A	N/A	N/A	7,352	7,352	
□ image003.png	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...		png	PNG File (Po...	Graphic		N/A	N/A	N/A	5,675	5,675	
□ Inbox	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			Email Folder [...	Other		N/A	N/A	N/A	0	0	
□ Message0001	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"test"	20-02-2015 21:17:56	20-02-2015 21:17:56	N/A	1,034	1,034	
□ Message0001	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"message 1"	22-06-2011 05:16:03	22-06-2011 05:16:39	N/A	748	748	
□ Message0002	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"Multiple at...	22-06-2011 05:21:07	26-11-2013 20:25:18	N/A	2,800	2,800	
□ Message0002	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"message 2"	22-06-2011 05:16:44	22-06-2011 05:17:01	N/A	784	784	
□ Message0003	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"HTML bo...	22-06-2011 05:19:22	26-11-2013 20:25:21	N/A	25,878	25,878	
□ Message0003	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"check se...	22-06-2011 05:17:05	22-06-2011 05:17:23	N/A	856	856	
□ Message0004	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"this mess...	22-06-2011 05:18:23	22-06-2011 05:18:23	N/A	5,866	5,866	
□ Message0004	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"this mess...	22-06-2011 05:17:01	22-06-2011 05:17:03	N/A	5,080	5,080	
□ Message0005	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"check se...	22-06-2011 05:17:23	26-11-2013 20:29:23	N/A	1,746	1,746	

34 Listed | 0 Checked Total | C:\Users\MSC7\Desktop\forencis\test.pst>>Test>>Top of Personal Folders>>Inbox>>Message0001

Step 12: click on email, any message & then right click on export file.



AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\MSC7\Desktop\forencis\hello\

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
□ Message0001	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"test"	20-02-2015 21:17:56	20-02-2015 21:17:56
□ Message0002	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"Multiple at...	22-06-2011 05:21:07	26-11-2013 20:25:18
□ Message0003	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"HTML bo...	22-06-2011 05:19:22	26-11-2013 20:25:21
□ Message0004	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"this mess...	22-06-2011 05:18:23	22-06-2011 05:18:23
□ Message0005	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"check se...	22-06-2011 05:17:23	26-11-2013 20:29:23
□ Message0006	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"message 2"	22-06-2011 05:17:01	26-11-2013 20:33:04
□ Message0007	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"message 1"	22-06-2011 05:16:39	22-06-2011 05:18:08
□ Message0008	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"Microsoft ...	22-06-2011 05:14:32	22-06-2011 05:14:40
□ Message0009	C:\Users\MSC7\Desktop\forencis\test.pst>>Tes...			E-mail Messa...	E-mail	"Microsoft ...	22-06-2011 05:14:32	22-06-2011 05:16:00

Message0001

Subject: test

From: asposeemail test3

Date: 20-02-2015 21:17:00

To: 'kashifiqb@gmail.com'

Message Body

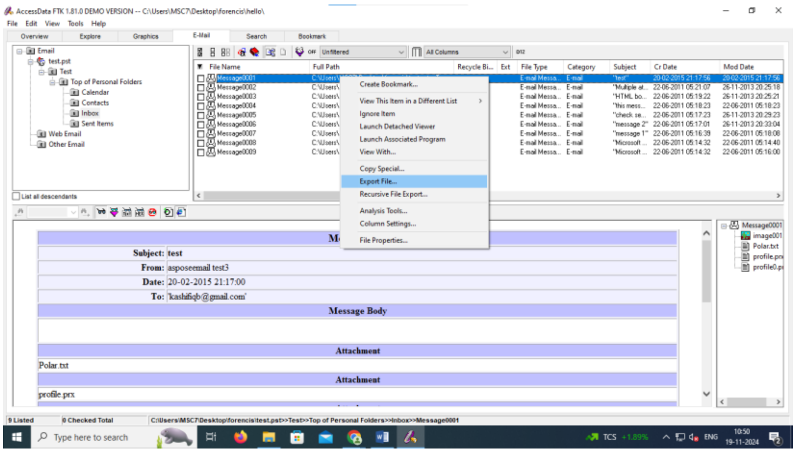
Attachment

Polar.txt

Attachment

profile.prx

9 Listed | 0 Checked Total | C:\Users\MSC7\Desktop\forencis\test.pst>>Test>>Top of Personal Folders>>Inbox>>Message0001



AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\MSC7\Desktop\forencis\hello\

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date
Message0001	C:\Users\			E-mail Messa...	E-mail	"test"	20-02-2015 21:17:56	20-02-2015 21:17:56
Message0002	C:\Users\			E-mail Messa...	E-mail	"Multiple at...	22-06-2011 05:21:07	26-11-2013 20:25:18
Message0003	C:\Users\			E-mail Messa...	E-mail	"HTML bo...	22-06-2011 05:19:22	26-11-2013 20:25:21
Message0004	C:\Users\			E-mail Messa...	E-mail	"this mess...	22-06-2011 05:18:23	22-06-2011 05:18:23
Message0005	C:\Users\			E-mail Messa...	E-mail	"check se...	22-06-2011 05:17:23	26-11-2013 20:29:23
Message0006	C:\Users\			E-mail Messa...	E-mail	"message 2"	22-06-2011 05:17:01	26-11-2013 20:33:04
Message0007	C:\Users\			E-mail Messa...	E-mail	"message 1"	22-06-2011 05:16:39	22-06-2011 05:18:08
Message0008	C:\Users\			E-mail Messa...	E-mail	"Microsoft ...	22-06-2011 05:14:32	22-06-2011 05:14:40
Message0009	C:\Users\			E-mail Messa...	E-mail	"Microsoft ...	22-06-2011 05:14:32	22-06-2011 05:16:00

Subject: test
From: asposeemail test3
Date: 20-02-2015 21:17:00
To: 'kashifiqb@gmail.com'

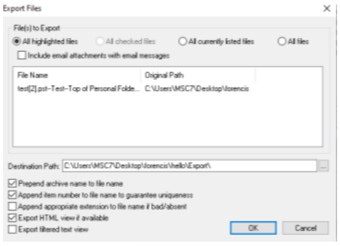
Message Body

Attachment
Polar.txt

Attachment
profile.prx

9 Listed | 0 Checked Total | C:\Users\MSC7\Desktop\forencis\test.pst>>Test>>Top of Personal Folders>>Inbox>>Message0001

Step 13 : tick the prepend, append and export html & then click ok



Export Files

File(s) to Export

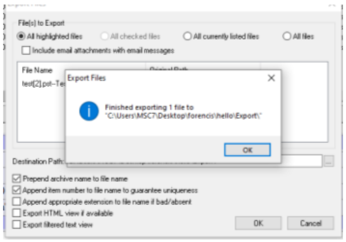
● All highlighted files ○ All checked files ○ All currently listed files ○ All files

□ Include email attachments with email messages

File Name	Original Path
test[2].pst--Test--Top of Personal Folde...	C:\Users\MSC7\Desktop\forencis

Destination Path: C:\Users\MSC7\Desktop\forencis\hello\Export\

☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
□ Append appropriate extension to file name if bad/absent
☑ Export HTML view if available
□ Export filtered text view



Export Files

Finished exporting 1 file to "C:\Users\MSC7\Desktop\forencis\hello\Export\"

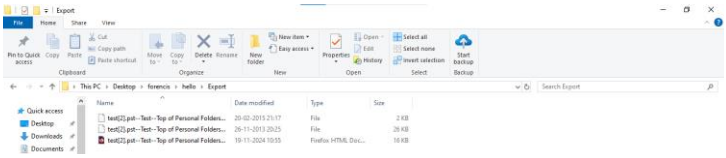
File(s) to Export

● All highlighted files ○ All checked files ○ All currently listed files ○ All files

□ Include email attachments with email messages

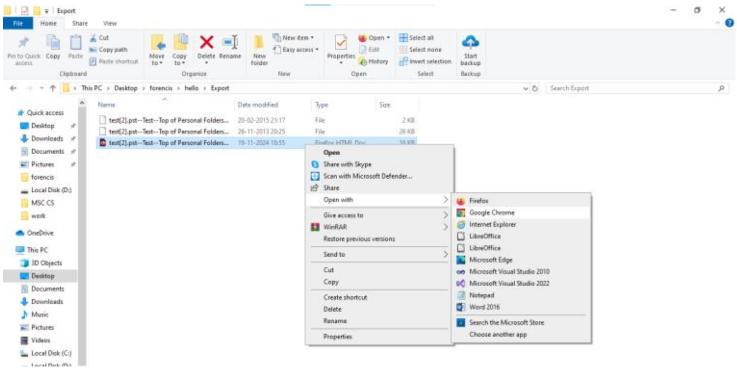
☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
□ Append appropriate extension to file name if bad/absent
□ Export HTML view if available
□ Export filtered text view

Step 14: open the export file, view the html file and then rename a file to html.



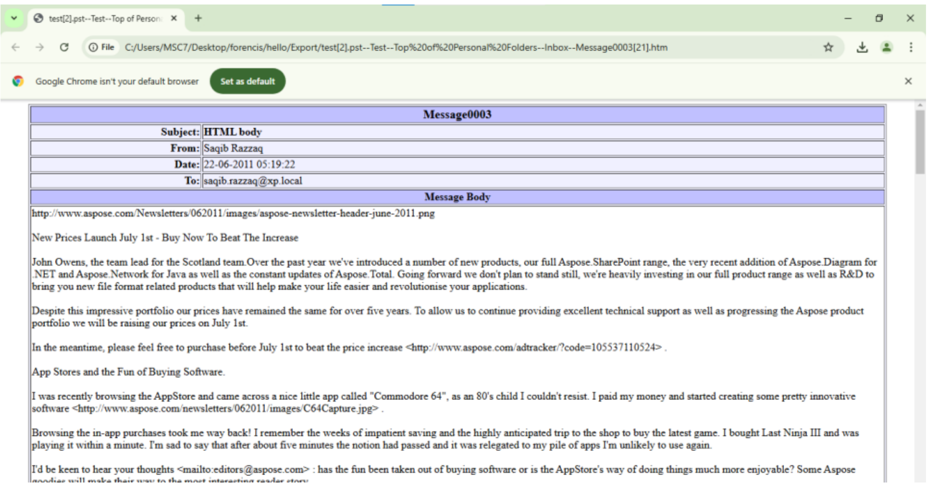
This PC › Desktop › forencis › hello › Export

Name	Date modified	Type	Size
test[2].pst--Test--Top of Personal Folders...	20-02-2015 21:17	File	2 KB
test[2].pst--Test--Top of Personal Folders...	26-11-2013 20:25	File	26 KB
test[2].pst--Test--Top of Personal Folders...	19-11-2024 10:55	Firefox HTML Doc...	16 KB



This PC › Desktop › forencis › hello › Export

Name	Date modified	Type	Size
test[2].pst--Test--Top of Personal Folders...	20-02-2015 21:17	File	2 KB
test[2].pst--Test--Top of Personal Folders...	26-11-2013 20:25	File	26 KB
test[2].pst--Test--Top of Personal Folders...	19-11-2024 10:55	Firefox HTML Doc...	16 KB



test[2].pst--Test--Top of Person
C:/Users/MSC7/Desktop/forencis/hello/Export/test[2].pst--Test--Top%20of%20Personal%20Folders--Inbox--Message0003[21].htm
Google Chrome isn't your default browser
Set as default

Message0003	
Subject:	**HTML body**
From:	Saqib Razzaq
Date:	22-06-2011 05:19:22
To:	saqib.razzaq@xp.local

Message Body

http://www.aspose.com/Newsletters/062011/images/aspose-newsletter-header-june-2011.png

New Prices Launch July 1st - Buy Now To Beat The Increase

John Owens, the team lead for the Scotland team.Over the past year we've introduced a number of new products, our full Aspose.SharePoint range, the very recent addition of Aspose.Diagram for .NET and Aspose.Network for Java as well as the constant updates of Aspose.Total. Going forward we don't plan to stand still, we're heavily investing in our full product range as well as R&D to bring you new file format related products that will help make your life easier and revolutionise your applications.

Despite this impressive portfolio our prices have remained the same for over five years. To allow us to continue providing excellent technical support as well as progressing the Aspose product portfolio we will be raising our prices on July 1st.

In the meantime, please feel free to purchase before July 1st to beat the price increase <http://www.aspose.com/adtracker/?code=105537110524> .

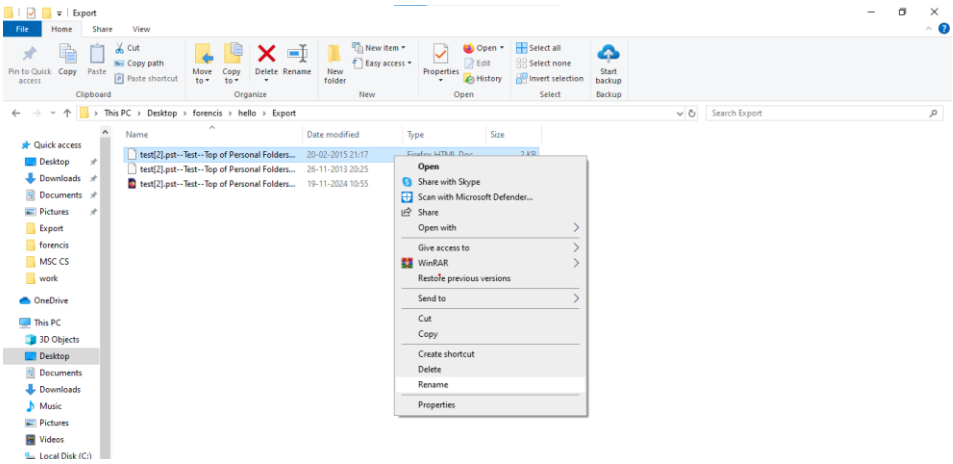
App Stores and the Fun of Buying Software.

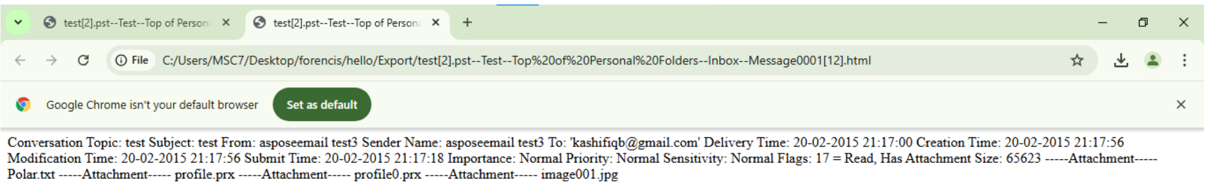
I was recently browsing the AppStore and came across a nice little app called "Commodore 64", as an 80's child I couldn't resist. I paid my money and started creating some pretty innovative software <http://www.aspose.com/newsletters/062011/images/C64Capture.jpg> .

Browsing the in-app purchases took me way back! I remember the weeks of impatient saving and the highly anticipated trip to the shop to buy the latest game. I bought Last Ninja III and was playing it within a minute. I'm sad to say that after about five minutes the notion had passed and it was relegated to my pile of apps I'm unlikely to use again.

I'd be keen to hear your thoughts <mailto:editors@aspose.com> : has the fun been taken out of buying software or is the AppStore's way of doing things much more enjoyable? Some Aspose goodies will make their way to the most interesting reader story.

Rename the file to .html





test[2].pst--Test--Top of Person
test[2].pst--Test--Top of Person
C:/Users/MSC7/Desktop/forencis/hello/Export/test[2].pst--Test--Top%20of%20Personal%20Folders--Inbox--Message0001[12].html
Google Chrome isn't your default browser
Set as default

Conversation Topic: test Subject: test From: asposeemail test3 Sender Name: asposeemail test3 To: 'kashifiqb@gmail.com' Delivery Time: 20-02-2015 21:17:00 Creation Time: 20-02-2015 21:17:56 Modification Time: 20-02-2015 21:17:56 Submit Time: 20-02-2015 21:17:18 Importance: Normal Priority: Normal Sensitivity: Normal Flags: 17 = Read, Has Attachment Size: 65623 -----Attachment----- Polar.txt -----Attachment----- profile.prx -----Attachment----- profile0.prx -----Attachment----- image001.jpg

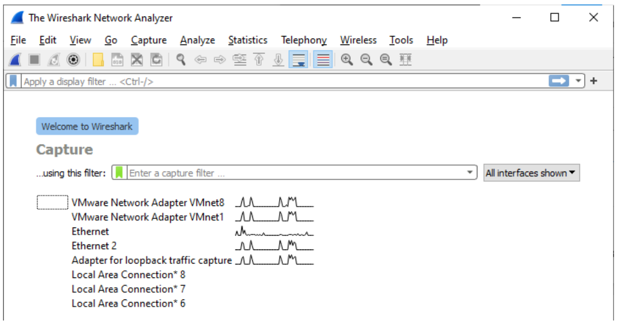
CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

PRACTICAL NO. 7

AIM :

THEORY :

Step1:



The Wireshark Network Analyzer

Apply a display filter ... <Ctrl-/>

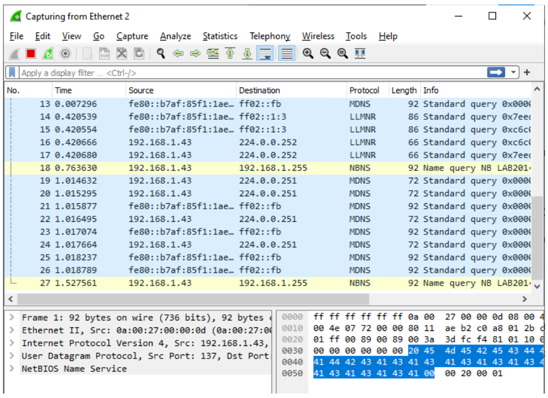
Welcome to Wireshark

Capture

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

VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6

Step2:



Capturing from Ethernet 2

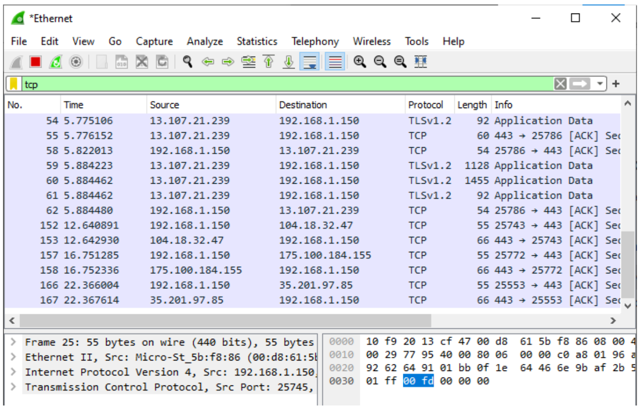
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
13	0.007296	fe80::b7af:85f1:1ae…	ff02::fb	MDNS	92	Standard query 0x000
14	0.420539	fe80::b7af:85f1:1ae…	ff02::1:3	LLMNR	86	Standard query 0x7ee
15	0.420554	fe80::b7af:85f1:1ae…	ff02::1:3	LLMNR	86	Standard query 0xc6c
16	0.420666	192.168.1.43	224.0.0.252	LLMNR	66	Standard query 0xc6c
17	0.420680	192.168.1.43	224.0.0.252	LLMNR	66	Standard query 0x7ee
18	0.763630	192.168.1.43	192.168.1.255	NBNS	92	Name query NB LAB201
19	1.014632	192.168.1.43	224.0.0.251	MDNS	72	Standard query 0x000
20	1.015295	192.168.1.43	224.0.0.251	MDNS	72	Standard query 0x000
21	1.015877	fe80::b7af:85f1:1ae…	ff02::fb	MDNS	92	Standard query 0x000
22	1.016495	192.168.1.43	224.0.0.251	MDNS	72	Standard query 0x000
23	1.017074	fe80::b7af:85f1:1ae…	ff02::fb	MDNS	92	Standard query 0x000
24	1.017664	192.168.1.43	224.0.0.251	MDNS	72	Standard query 0x000
25	1.018237	fe80::b7af:85f1:1ae…	ff02::fb	MDNS	92	Standard query 0x000
26	1.018789	fe80::b7af:85f1:1ae…	ff02::fb	MDNS	92	Standard query 0x000
27	1.527561	192.168.1.43	192.168.1.255	NBNS	92	Name query NB LAB201

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes
> Ethernet II, Src: 0a:00:27:00:00:0d (0a:00:27:0
> Internet Protocol Version 4, Src: 192.168.1.43,
> User Datagram Protocol, Src Port: 137, Dst Port
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff 0a 00  27 00 00 0d 08 00 4
0010  00 4e 07 72 00 00 80 11  ae b2 c0 a8 01 2b c
0020  01 ff 00 89 00 89 00 3a  3d fc f4 81 01 10 0
0030  00 00 00 00 00 00 20 45  4d 45 42 45 43 44 4
0040  41 44 42 43 41 43 41 43  41 43 41 43 41 43 4
0050  41 43 41 43 41 43 41 00  00 20 00 01
```

Step3:



*Ethernet

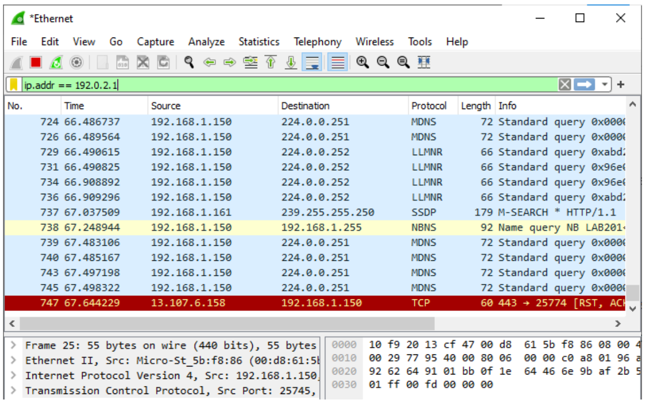
tcp

No.	Time	Source	Destination	Protocol	Length	Info
54	5.775106	13.107.21.239	192.168.1.150	TLSv1.2	92	Application Data
55	5.776152	13.107.21.239	192.168.1.150	TCP	60	443 → 25786 [ACK] Se
58	5.822013	192.168.1.150	13.107.21.239	TCP	54	25786 → 443 [ACK] Se
59	5.884223	13.107.21.239	192.168.1.150	TLSv1.2	1128	Application Data
60	5.884462	13.107.21.239	192.168.1.150	TLSv1.2	1455	Application Data
61	5.884462	13.107.21.239	192.168.1.150	TLSv1.2	92	Application Data
62	5.884480	192.168.1.150	13.107.21.239	TCP	54	25786 → 443 [ACK] Se
152	12.640891	192.168.1.150	104.18.32.47	TCP	55	25743 → 443 [ACK] Se
153	12.642930	104.18.32.47	192.168.1.150	TCP	66	443 → 25743 [ACK] Se
157	16.751285	192.168.1.150	175.100.184.155	TCP	55	25772 → 443 [ACK] Se
158	16.752336	175.100.184.155	192.168.1.150	TCP	66	443 → 25772 [ACK] Se
166	22.366004	192.168.1.150	35.201.97.85	TCP	55	25553 → 443 [ACK] Se
167	22.367614	35.201.97.85	192.168.1.150	TCP	66	443 → 25553 [ACK] Se

```
> Frame 25: 55 bytes on wire (440 bits), 55 bytes
> Ethernet II, Src: Micro-St_5b:f8:86 (00:d8:61:5
> Internet Protocol Version 4, Src: 192.168.1.150
> Transmission Control Protocol, Src Port: 25745,
```

```
0000  10 f9 20 13 cf 47 00 d8  61 5b f8 86 08 00 4
0010  00 29 77 95 40 00 80 06  00 00 c0 a8 01 96 a
0020  92 62 64 91 01 bb 0f 1e  64 46 6e 9b af 2b 5
0030  01 ff 00 fd 00 00 00
```

Step4:



*Ethernet

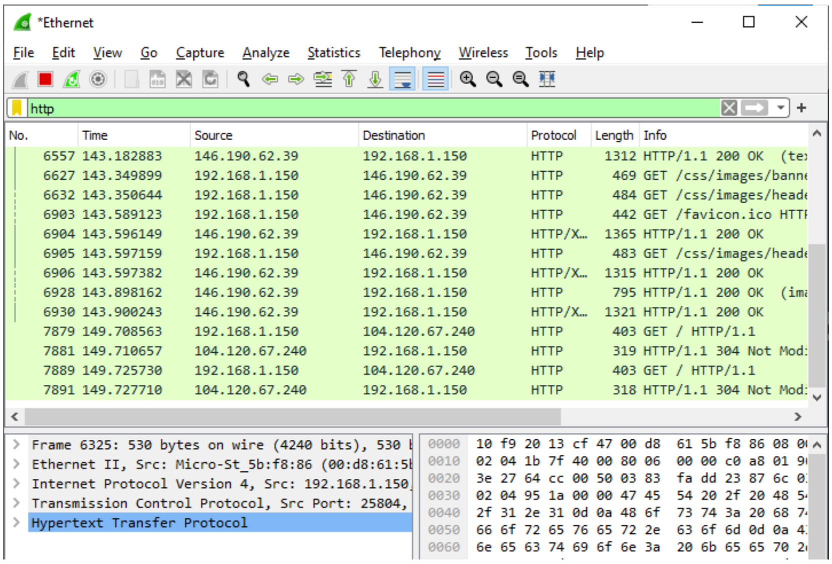
ip.addr == 192.0.2.1

No.	Time	Source	Destination	Protocol	Length	Info
724	66.486737	192.168.1.150	224.0.0.251	MDNS	72	Standard query 0x000
726	66.489564	192.168.1.150	224.0.0.251	MDNS	72	Standard query 0x000
729	66.490615	192.168.1.150	224.0.0.252	LLMNR	66	Standard query 0xabd
731	66.490825	192.168.1.150	224.0.0.252	LLMNR	66	Standard query 0x96e
734	66.908892	192.168.1.150	224.0.0.252	LLMNR	66	Standard query 0x96e
736	66.909296	192.168.1.150	224.0.0.252	LLMNR	66	Standard query 0xabd
737	67.037509	192.168.1.161	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
738	67.248944	192.168.1.150	192.168.1.255	NBNS	92	Name query NB LAB201
739	67.483106	192.168.1.150	224.0.0.251	MDNS	72	Standard query 0x000
740	67.485167	192.168.1.150	224.0.0.251	MDNS	72	Standard query 0x000
743	67.497198	192.168.1.150	224.0.0.251	MDNS	72	Standard query 0x000
745	67.498322	192.168.1.150	224.0.0.251	MDNS	72	Standard query 0x000
747	67.644229	13.107.6.158	192.168.1.150	TCP	60	443 → 25774 [RST, AC

```
> Frame 25: 55 bytes on wire (440 bits), 55 bytes
> Ethernet II, Src: Micro-St_5b:f8:86 (00:d8:61:5
> Internet Protocol Version 4, Src: 192.168.1.150
> Transmission Control Protocol, Src Port: 25745,
```

```
0000  10 f9 20 13 cf 47 00 d8  61 5b f8 86 08 00 4
0010  00 29 77 95 40 00 80 06  00 00 c0 a8 01 96 a
0020  92 62 64 91 01 bb 0f 1e  64 46 6e 9b af 2b 5
0030  01 ff 00 fd 00 00 00
```

Step5:


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

```
http
```

```
No.     Time        Source          Destination     Protocol Length Info
   6557 143.182883  146.190.62.39   192.168.1.150   HTTP       1312 HTTP/1.1 200 OK  (te
   6627 143.349899  192.168.1.150   146.190.62.39   HTTP        469 GET /css/images/banne
   6632 143.350644  192.168.1.150   146.190.62.39   HTTP        484 GET /css/images/heade
   6903 143.589123  192.168.1.150   146.190.62.39   HTTP        442 GET /favicon.ico HTTP
   6904 143.596149  146.190.62.39   192.168.1.150   HTTP/X…    1365 HTTP/1.1 200 OK
   6905 143.597159  192.168.1.150   146.190.62.39   HTTP        483 GET /css/images/heade
   6906 143.597382  146.190.62.39   192.168.1.150   HTTP/X…    1315 HTTP/1.1 200 OK
   6928 143.898162  146.190.62.39   192.168.1.150   HTTP        795 HTTP/1.1 200 OK  (ima
   6930 143.900243  146.190.62.39   192.168.1.150   HTTP/X…    1321 HTTP/1.1 200 OK
   7879 149.708563  192.168.1.150   104.120.67.240  HTTP        403 GET / HTTP/1.1
   7881 149.710657  104.120.67.240  192.168.1.150   HTTP        319 HTTP/1.1 304 Not Mod:
   7889 149.725730  192.168.1.150   104.120.67.240  HTTP        403 GET / HTTP/1.1
   7891 149.727710  104.120.67.240  192.168.1.150   HTTP        318 HTTP/1.1 304 Not Mod:
```

```
> Frame 6325: 530 bytes on wire (4240 bits), 530 b
> Ethernet II, Src: Micro-St_5b:f8:86 (00:d8:61:5b
> Internet Protocol Version 4, Src: 192.168.1.150,
> Transmission Control Protocol, Src Port: 25804,
> Hypertext Transfer Protocol
```

```
0000  10 f9 20 13 cf 47 00 d8  61 5b f8 86 08 0
0010  02 04 1b 7f 40 00 80 06  00 00 c0 a8 01 9
0020  3e 27 64 cc 00 50 03 83  fa dd 23 87 6c 0
0030  02 04 95 1a 00 00 47 45  54 20 2f 20 48 5
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 68 7
0050  66 6f 72 65 76 65 72 2e  63 6f 6d 0d 0a 4
0060  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2
```

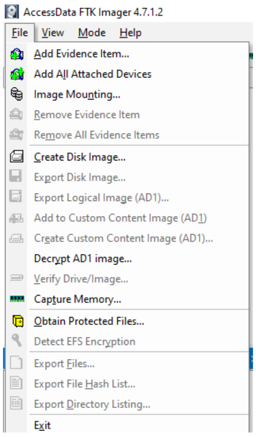
CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**

PRACTICAL NO. 8

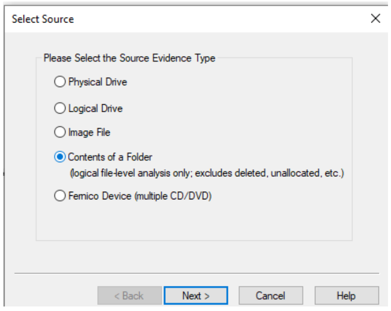
AIM :

THEORY :

Step1: Create a Disk Image



Step2: Select Source as Contents of a Folder


Select Source

Please Select the Source Evidence Type

○ Physical Drive

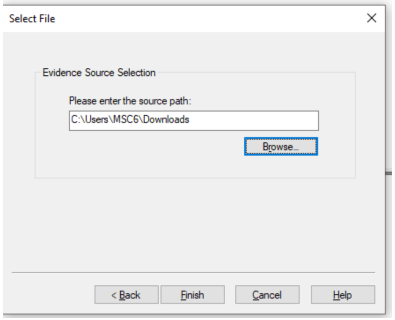
○ Logical Drive

○ Image File

● Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

Step3: Select Evidence Source


Select File

Evidence Source Selection

Please enter the source path:
C:\Users\MSC6\Downloads

Step4: Select Image Source

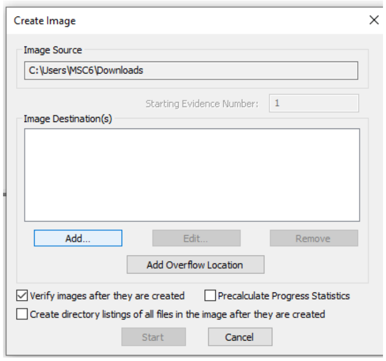

Create Image

Image Source
C:\Users\MSC6\Downloads

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created □ Precalculate Progress Statistics

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

Step5: Select Image Destination

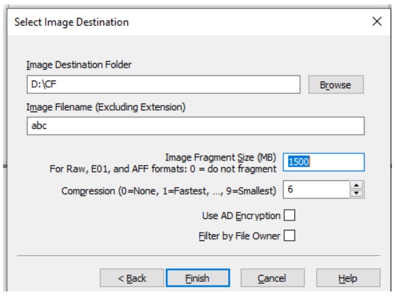

Select Image Destination

Image Destination Folder: D:\CF

Image Filename (Excluding Extension): abc

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption □

Filter by File Owner □

Step6: Select Add Image Destination

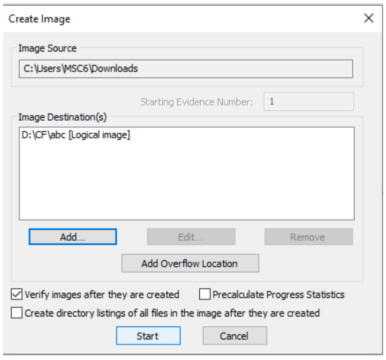

Create Image

Image Source: C:\Users\MSC6\Downloads

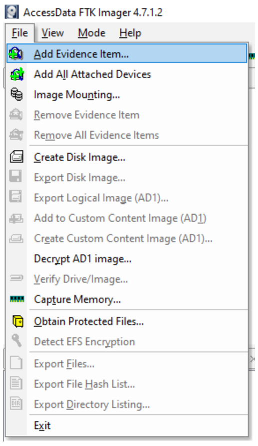
Starting Evidence Number: 1

Image Destination(s): D:\CF\abc [Logical image]

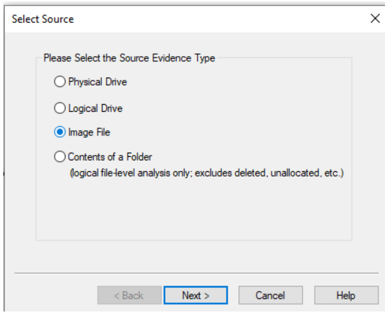
☑ Verify images after they are created □ Precalculate Progress Statistics

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

Step7: Select Add Evidence Item from File



Step8: Select Source as Image File


Select Source

Please Select the Source Evidence Type

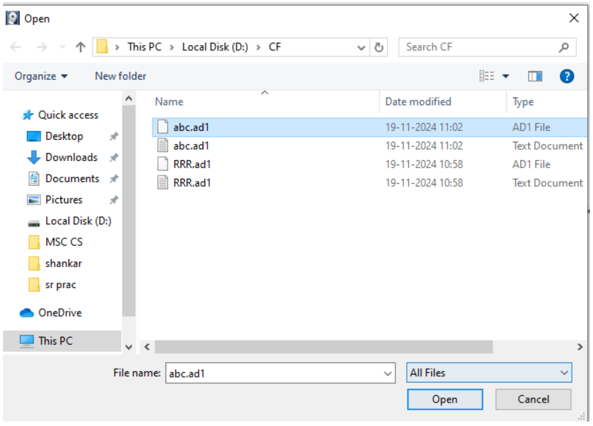
○ Physical Drive

○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

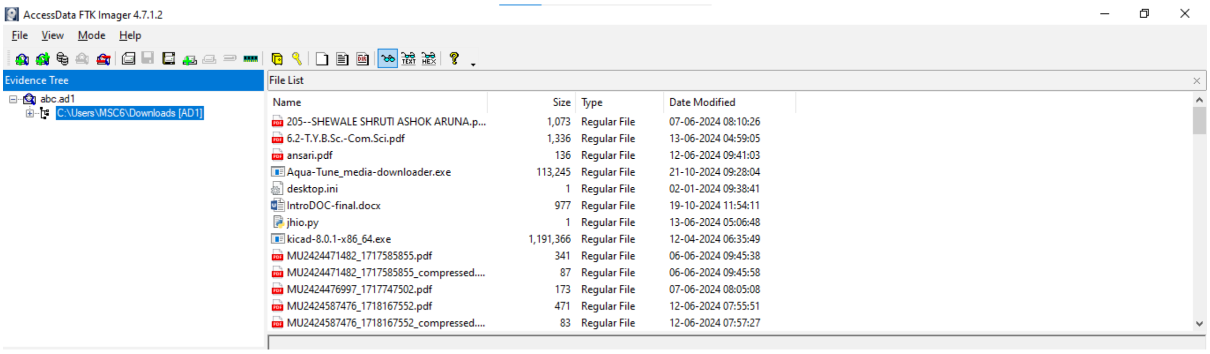
Step9: Select the File



Name	Date modified	Type
abc.ad1	19-11-2024 11:02	AD1 File
abc.ad1	19-11-2024 11:02	Text Document
RRR.ad1	19-11-2024 10:58	AD1 File
RRR.ad1	19-11-2024 10:58	Text Document

File name: abc.ad1

All Files



Name	Size	Type	Date Modified
205--SHEWALE SHRUTI ASHOK ARUNA.p...	1,073	Regular File	07-06-2024 08:10:26
6.2-T.Y.B.Sc.-Com.Sci.pdf	1,336	Regular File	13-06-2024 04:59:05
ansari.pdf	136	Regular File	12-06-2024 09:41:03
Aqua-Tune_media-downloader.exe	113,245	Regular File	21-10-2024 09:28:04
desktop.ini	1	Regular File	02-01-2024 09:38:41
IntroDOC-final.docx	977	Regular File	19-10-2024 11:54:11
jhio.py	1	Regular File	13-06-2024 05:06:48
kicad-8.0.1-x86_64.exe	1,191,366	Regular File	12-04-2024 06:35:49
MU2424471482_1717585855.pdf	341	Regular File	06-06-2024 09:45:38
MU2424471482_1717585855_compressed....	87	Regular File	06-06-2024 09:45:58
MU2424476997_1717747502.pdf	173	Regular File	07-06-2024 08:05:08
MU2424587476_1718167552.pdf	471	Regular File	12-06-2024 07:55:51
MU2424587476_1718167552_compressed....	83	Regular File	12-06-2024 07:57:27

CONCLUSION : **ABOVE PROGRAM HAS SUCCESFULLY EXECUTED**