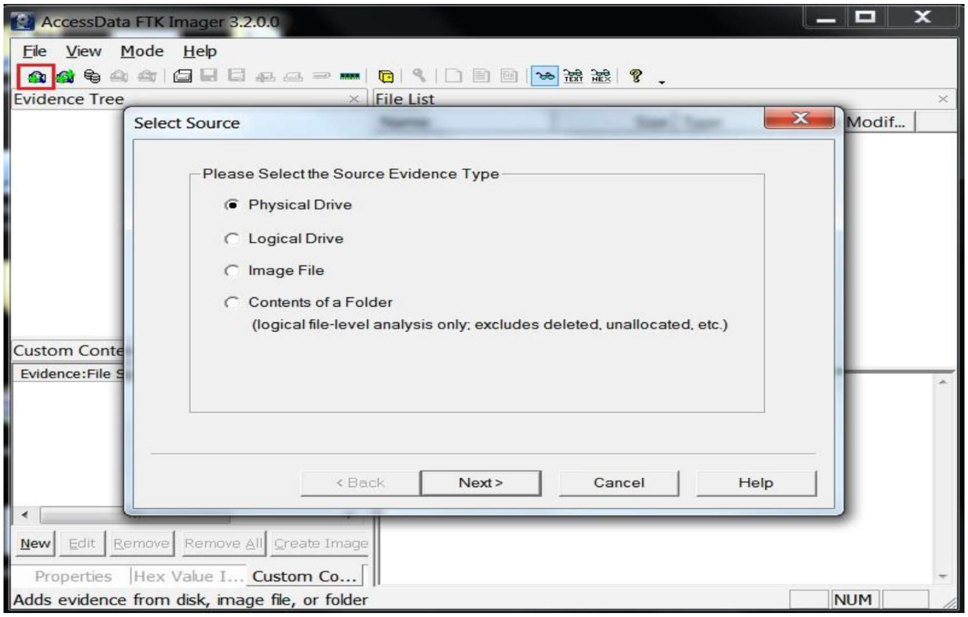
Practical No: - 07

AIM: Create forensic images of digital devices from volatile data such as memory using Imager for:

1. **Computer System**
2. **Server**

1. Computer System:

1. Click on the **Add Evidence Item** button on the toolbar.
2. Select the source type you want to preview and then click on **Next**.



AccessData FTK Imager 3.2.0.0
File View Mode Help
Evidence Tree
File List
Modif...
Custom Conte
Evidence:File S
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
NUM
< Back
Next >
Cancel
Help

Select Source

Please Select the Source Evidence Type

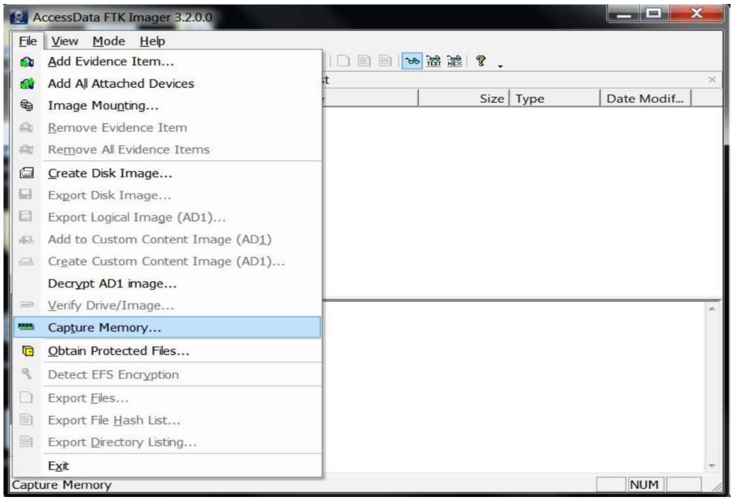
● Physical Drive

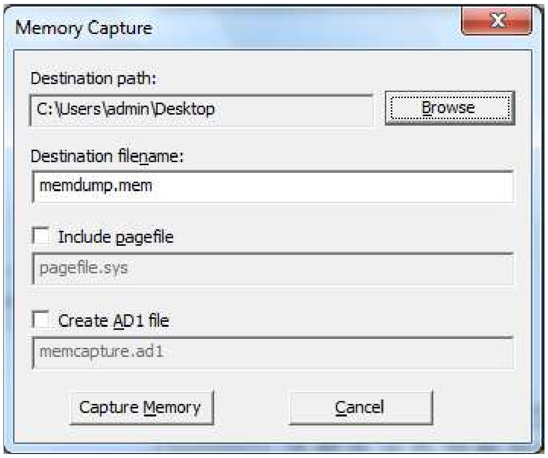
○ Logical Drive

○ Image File

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

Adds evidence from disk, image file, or folder



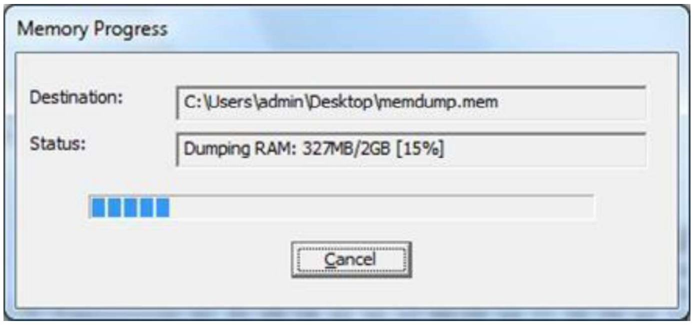


Destination path: C:\Users\admin\Desktop

Destination filename: memdump.mem

□ Include pagefile
pagefile.sys

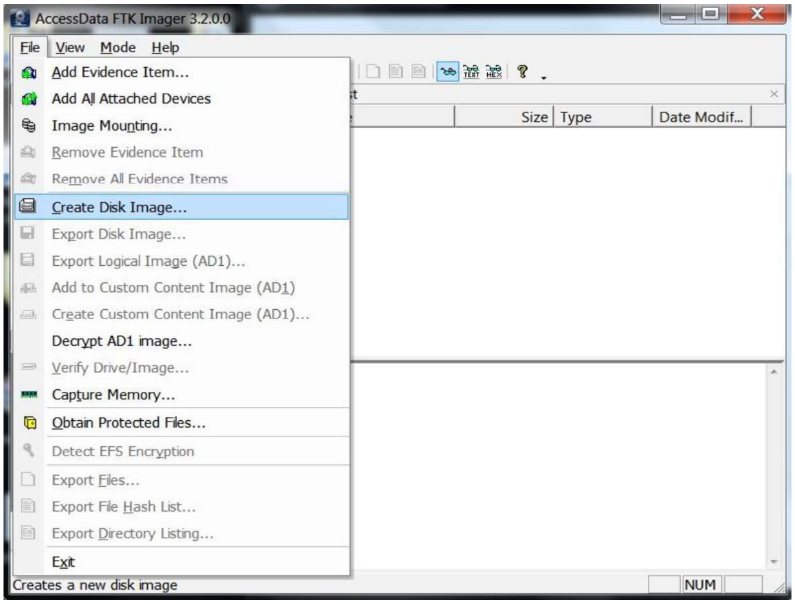
□ Create AD1 file
memcapture.ad1



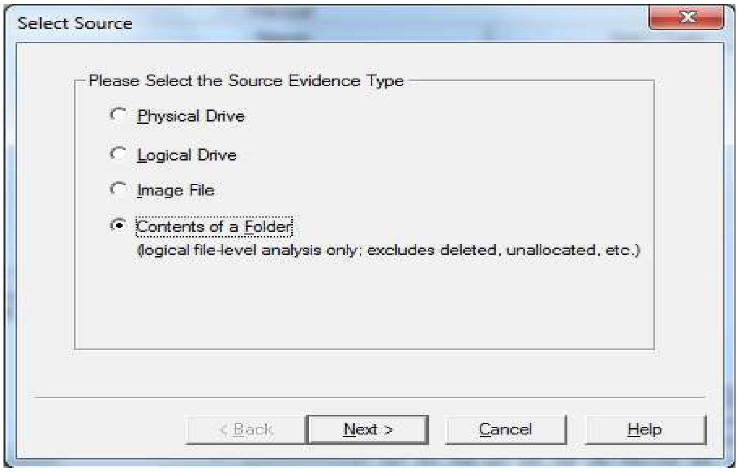
Destination: C:\Users\admin\Desktop\memdump.mem

Status: Dumping RAM: 327MB/2GB [15%]

2. Server:



Creates a new disk image



Select Source

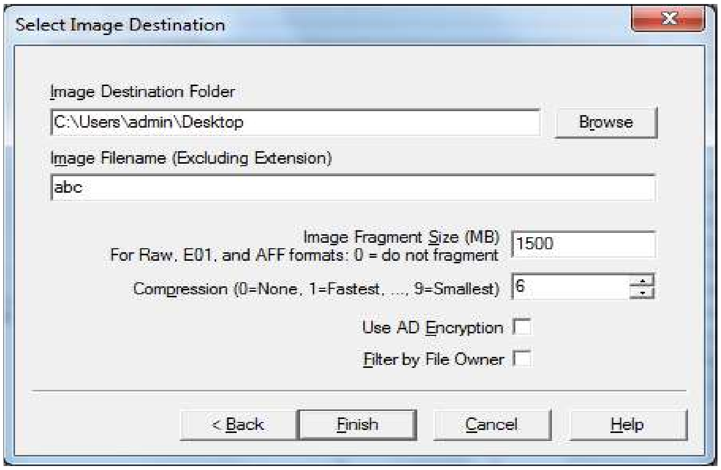
Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

○ Image File

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



Select Image Destination

Image Destination Folder: C:\Users\admin\Desktop

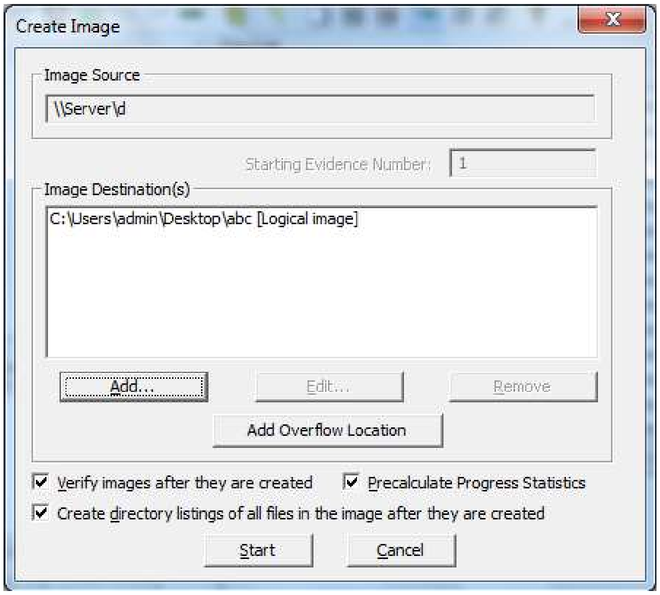
Image Filename (Excluding Extension): abc

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 □



Create Image

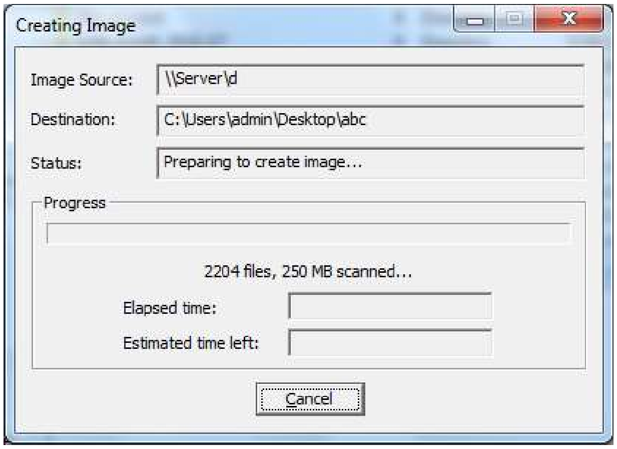
Image Source: \\Server\d

Starting Evidence Number: 1

Image Destination(s):
C:\Users\admin\Desktop\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



Creating Image

Image Source: \\Server\d

Destination: C:\Users\admin\Desktop\abc

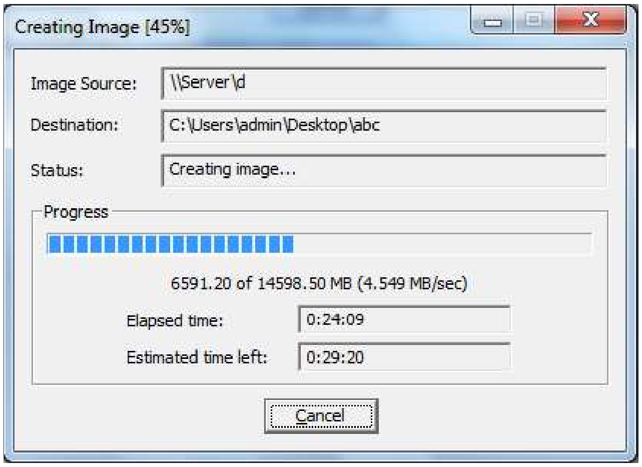
Status: Preparing to create image...

Progress

2204 files, 250 MB scanned...

Elapsed time:

Estimated time left:



Creating Image [45%]

Image Source: \\Server\d

Destination: C:\Users\admin\Desktop\abc

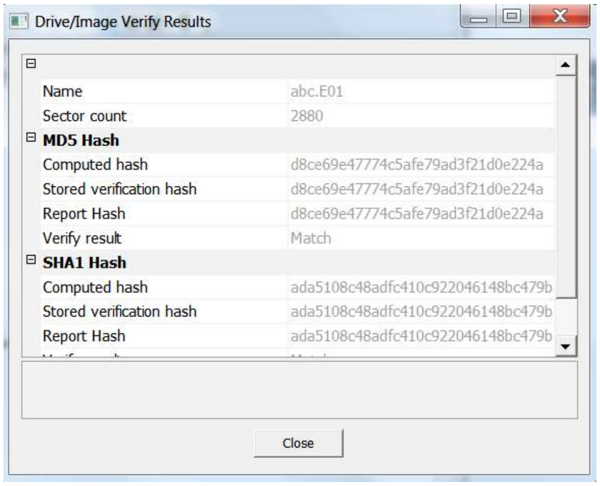
Status: Creating image...

Progress

6591.20 of 14598.50 MB (4.549 MB/sec)

Elapsed time: 0:24:09

Estimated time left: 0:29:20



Drive/Image Verify Results

Name	abc.E01
Sector count	2880
MD5 Hash	
Computed hash	d8ce69e47774c5afe79ad3f21d0e224a
Stored verification hash	d8ce69e47774c5afe79ad3f21d0e224a
Report Hash	d8ce69e47774c5afe79ad3f21d0e224a
Verify result	Match
SHA1 Hash	
Computed hash	ada5108c48adfc410c922046148bc479b
Stored verification hash	ada5108c48adfc410c922046148bc479b
Report Hash	ada5108c48adfc410c922046148bc479b

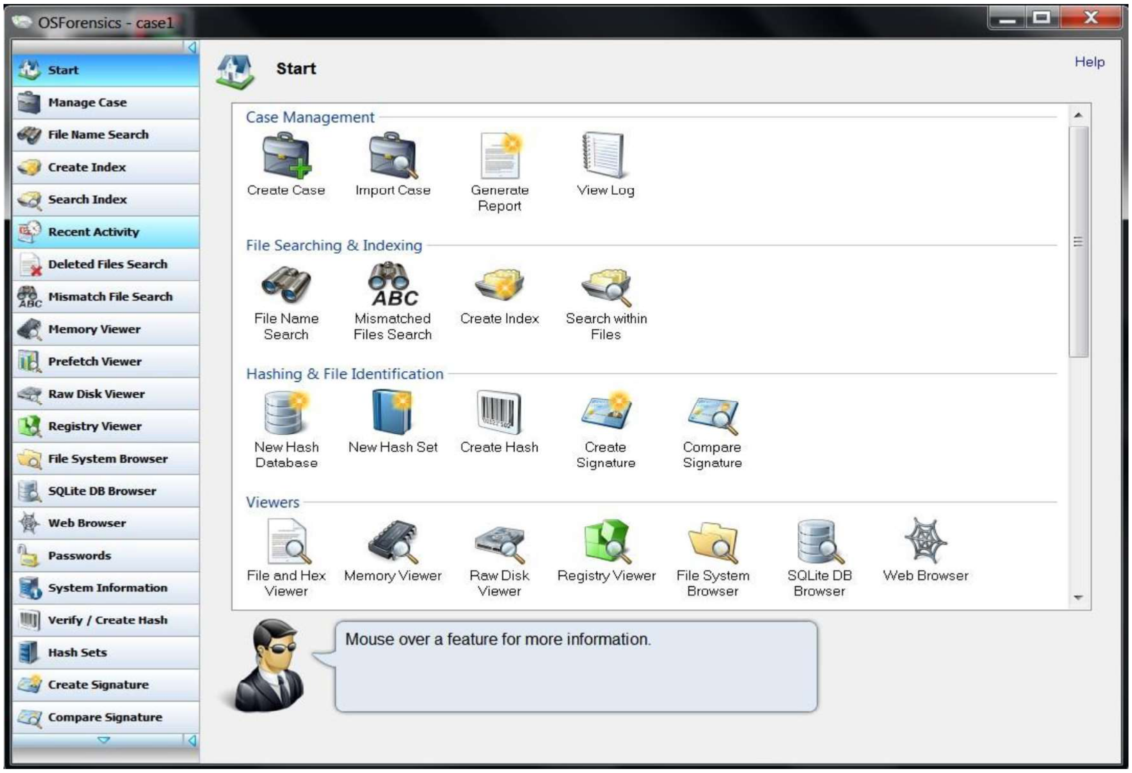
Practical No: - 08

AIM: Access and extract relevant information from Windows Registry for investigation process using Registry View, perform data analysis and bookmark the findings with respect to:

1. **Computer System**
2. **Computer Network**

1. COMPUTER SYSTEM

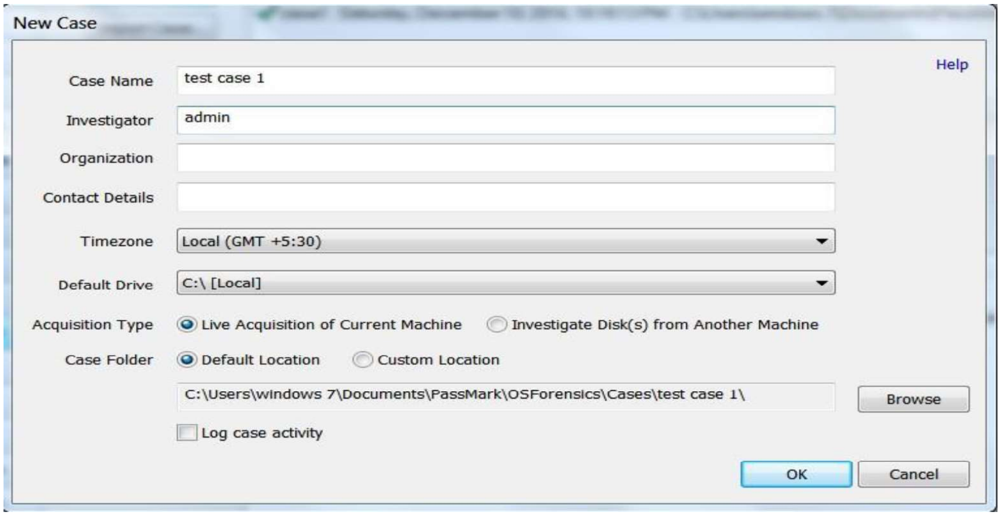
Step 1: Start OSForenscis as Start->All Programs -> OSForensics->OSForensics



Mouse over a feature for more information.

Step 2: Create a new Case by selecting Create Case. The following window will be popped:

Enter Appropriate Details and Select OK



New Case

Case Name: test case 1

Investigator: admin

Organization:

Contact Details:

Timezone: Local (GMT +5:30)

Default Drive: C:\ [Local]

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

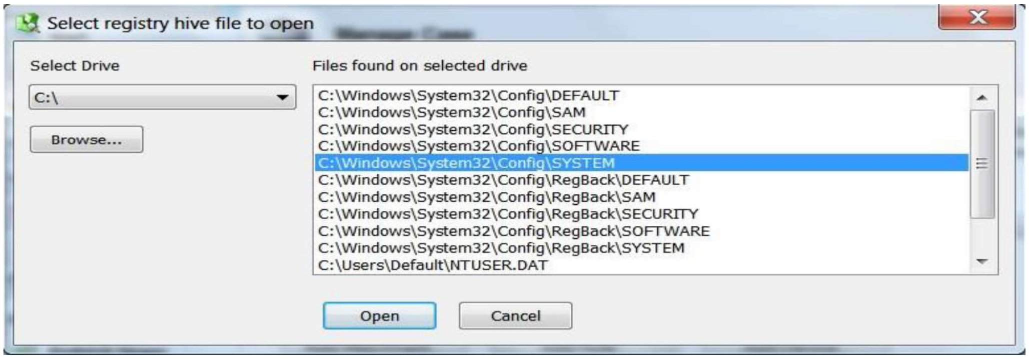
Case Folder: ● Default Location ○ Custom Location

C:\Users\windows 7\Documents\PassMark\OSForensics\Cases\test case 1\

□ Log case activity

Step 3: Select Registry Viewer and select registry hive file to open for computer system

Select open

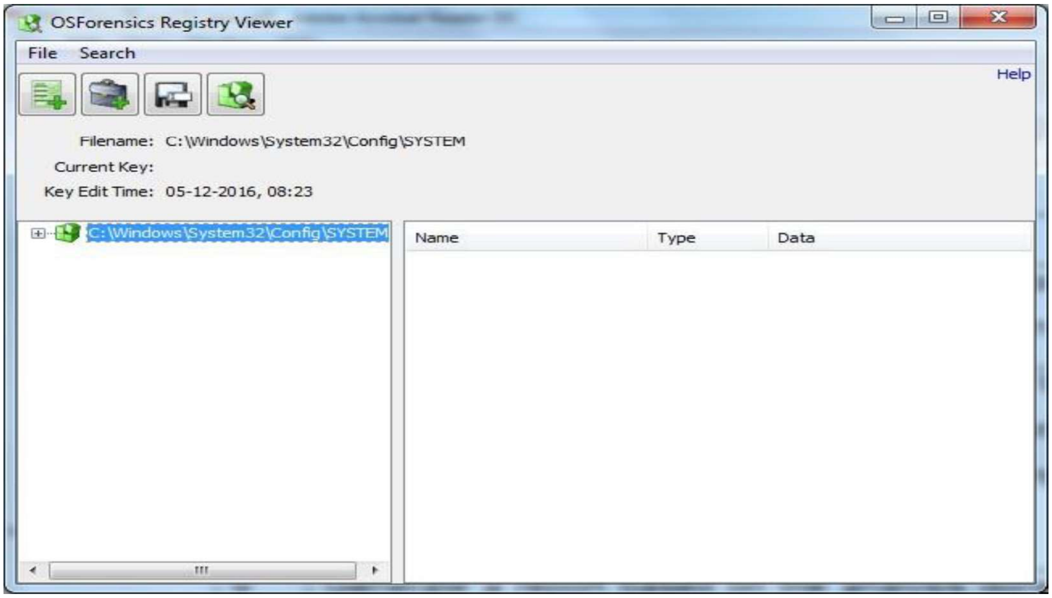


Select registry hive file to open

Select Drive: C:\

Files found on selected drive

```
C:\Windows\System32\Config\DEFAULT
C:\Windows\System32\Config\SAM
C:\Windows\System32\Config\SECURITY
C:\Windows\System32\Config\SOFTWARE
C:\Windows\System32\Config\SYSTEM
C:\Windows\System32\Config\RegBack\DEFAULT
C:\Windows\System32\Config\RegBack\SAM
C:\Windows\System32\Config\RegBack\SECURITY
C:\Windows\System32\Config\RegBack\SOFTWARE
C:\Windows\System32\Config\RegBack\SYSTEM
C:\Users\Default\NTUSER.DAT
```


OSForensics Registry Viewer
File
Search
Help
C:\Windows\System32\Config\SYSTEM

Filename: C:\Windows\System32\Config\SYSTEM

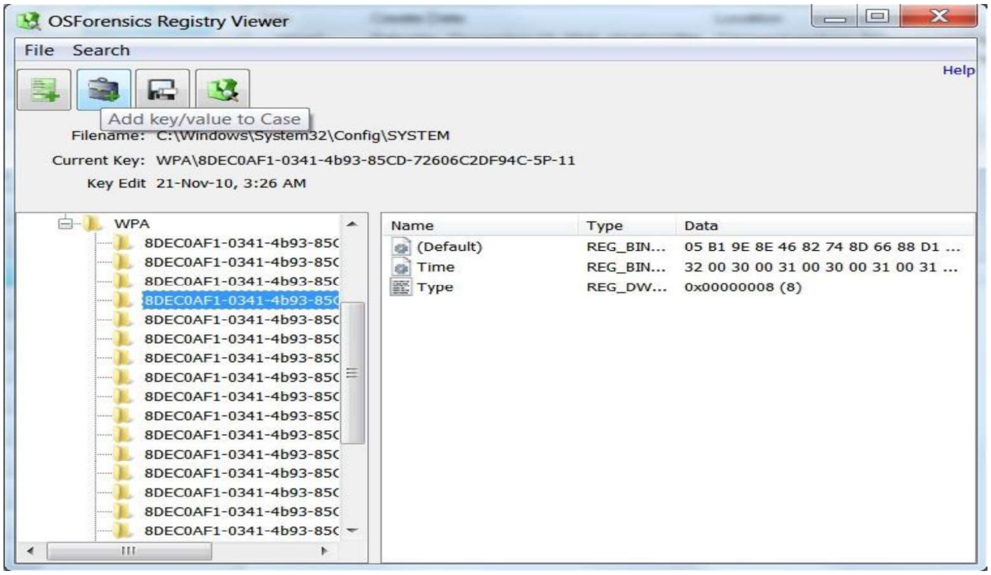
Current Key:

Key Edit Time: 05-12-2016, 08:23

Name	Type	Data

Step 4:

Select system file to add a key/value



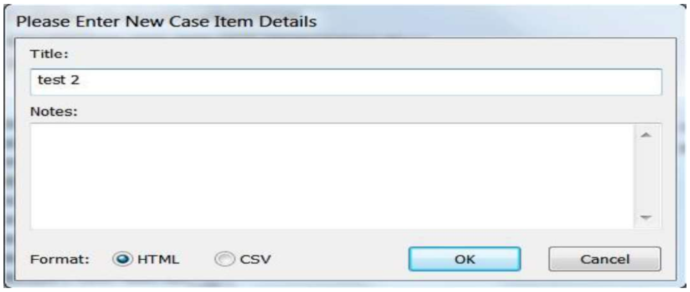
Filename: C:\Windows\System32\Config\SYSTEM

Current Key: WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-5P-11

Key Edit 21-Nov-10, 3:26 AM

Name	Type	Data
(Default)	REG_BIN...	05 B1 9E 8E 46 82 74 8D 66 88 D1 ...
Time	REG_BIN...	32 00 30 00 31 00 30 00 31 00 31 ...
Type	REG_DW...	0x00000008 (8)

Enter Appropriate Details and Select OK



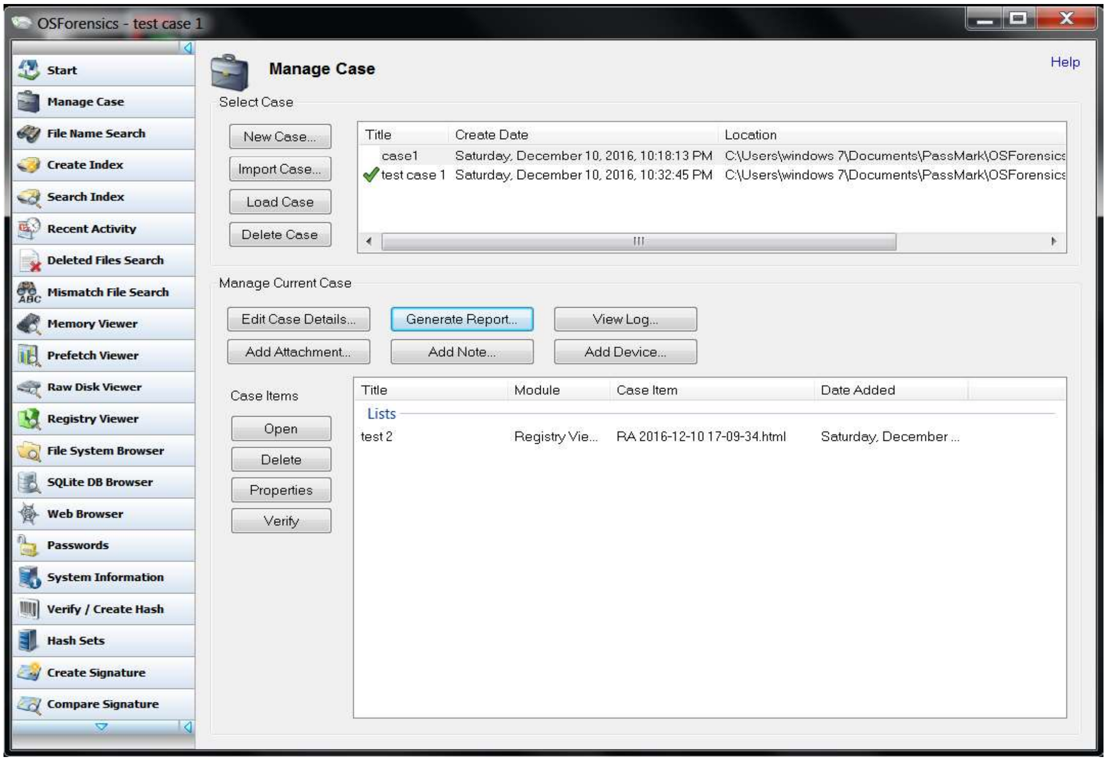
Please Enter New Case Item Details

Title: test 2

Notes:

Format: ● HTML ○ CSV

Step 5: Select Manage Case



OSForensics - test case 1

Manage Case

Select Case

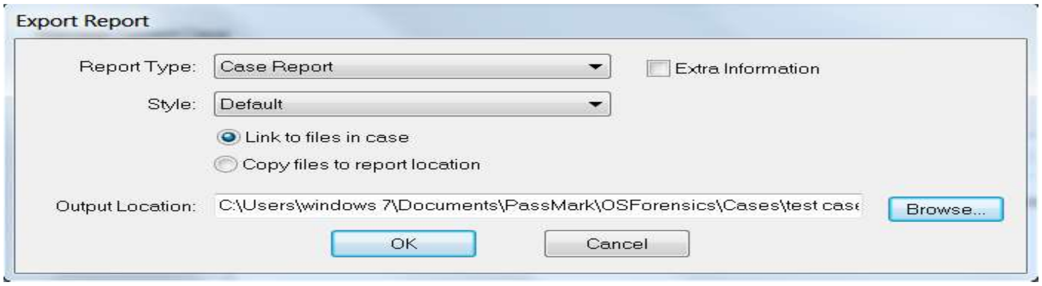
Title	Create Date	Location
case1	Saturday, December 10, 2016, 10:18:13 PM	C:\Users\windows 7\Documents\PassMark\OSForensics
✓ test case 1	Saturday, December 10, 2016, 10:32:45 PM	C:\Users\windows 7\Documents\PassMark\OSForensics

Manage Current Case

Case Items

Title	Module	Case Item	Date Added
Lists			
test 2	Registry Vie...	RA 2016-12-10 17-09-34.html	Saturday, December ...

Select registry viewer file and click on Generate Report



Export Report

Report Type: Case Report

□ Extra Information

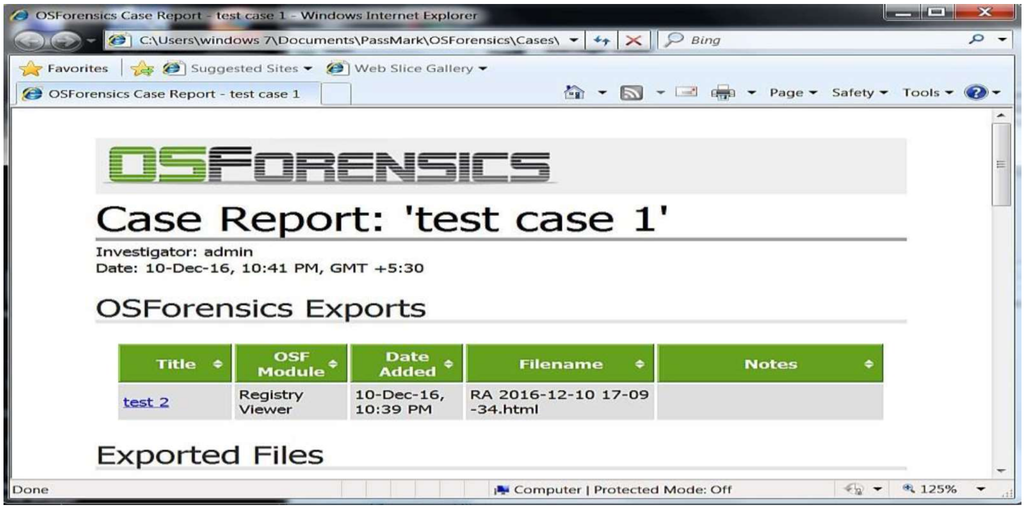
Style: Default

● Link to files in case

○ Copy files to report location

Output Location: C:\Users\windows 7\Documents\PassMark\OSForensics\Cases\test case

Select Ok


OSForensics Case Report - test case 1 - Windows Internet Explorer
C:\Users\windows 7\Documents\PassMark\OSForensics\Cases\
Bing
Favorites
Suggested Sites
Web Slice Gallery
OSForensics Case Report - test case 1
Page
Safety
Tools
OSFORENSICS
Done
Computer | Protected Mode: Off
125%

Case Report: 'test case 1'

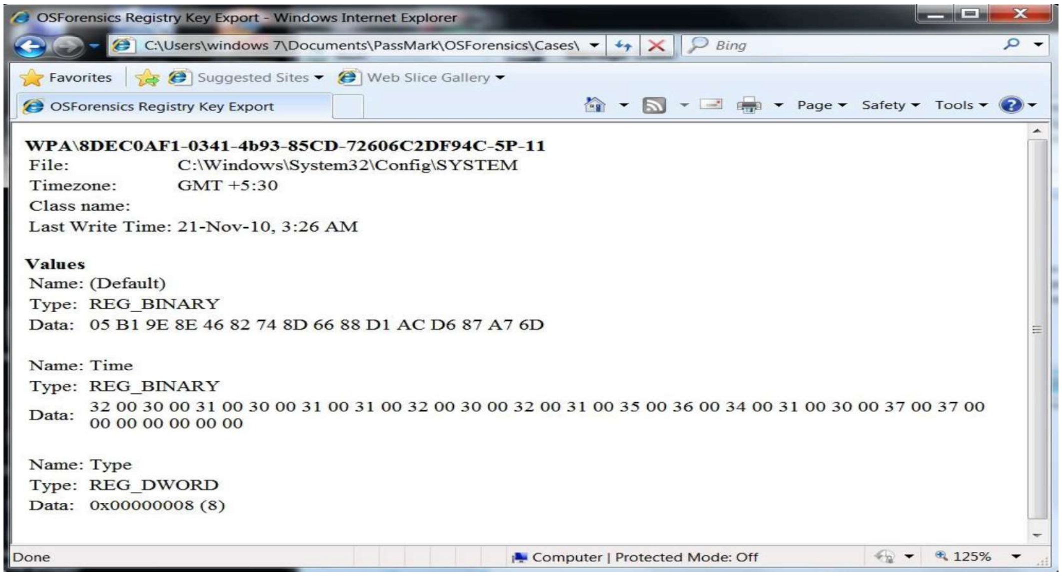
Investigator: admin
Date: 10-Dec-16, 10:41 PM, GMT +5:30

OSForensics Exports

Title	OSF Module	Date Added	Filename	Notes
test 2	Registry Viewer	10-Dec-16, 10:39 PM	RA 2016-12-10 17-09 -34.html	

Exported Files

Select registry viewer file


OSForensics Registry Key Export - Windows Internet Explorer
C:\Users\windows 7\Documents\PassMark\OSForensics\Cases\
Bing
Favorites
Suggested Sites
Web Slice Gallery
OSForensics Registry Key Export
Page
Safety
Tools
Done
Computer | Protected Mode: Off
125%

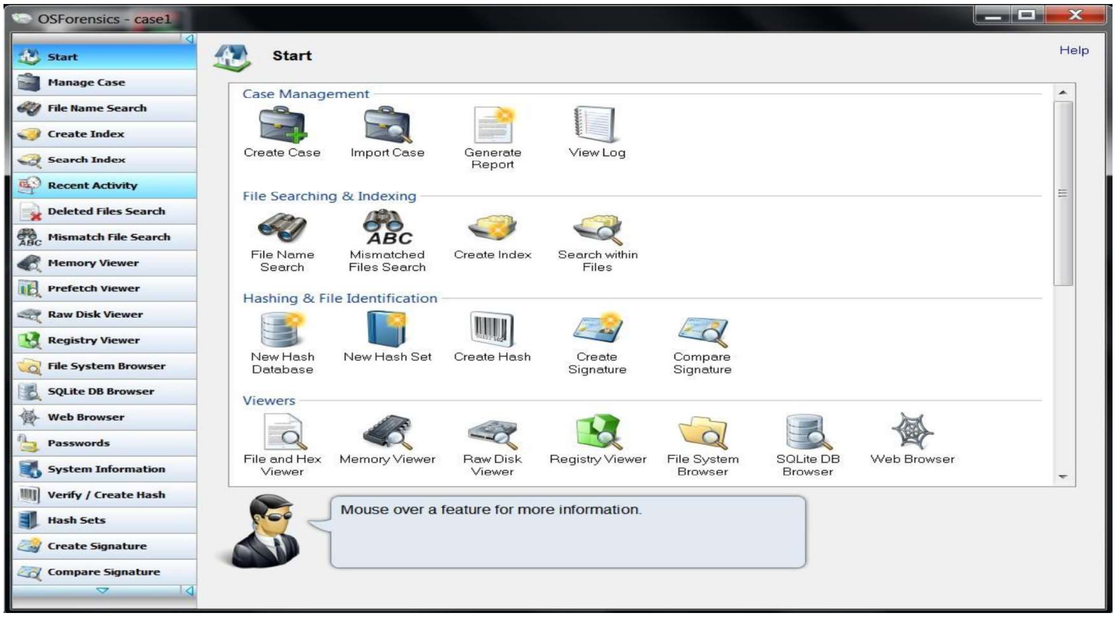
```
WPA\8DEC0AF1-0341-4b93-85CD-72606C2DF94C-5P-11
 File:            C:\Windows\System32\Config\SYSTEM
 Timezone:        GMT +5:30
 Class name:
 Last Write Time: 21-Nov-10, 3:26 AM

Values
 Name: (Default)
 Type:  REG_BINARY
 Data:  05 B1 9E 8E 46 82 74 8D 66 88 D1 AC D6 87 A7 6D

 Name: Time
 Type:  REG_BINARY
 Data:  32 00 30 00 31 00 30 00 31 00 31 00 32 00 30 00 32 00 31 00 35 00 36 00 34 00 31 00 30 00 37 00 37 00
        00 00 00 00 00 00

 Name: Type
 Type:  REG_DWORD
 Data:  0x00000008 (8)
```

2. COMPUTER NETWORK:

For Computer Network search registry settings and repeat the process. The various Registry Settings for windows 7 are as follows:

FILE1:
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Class/{4D36E972-E325-11CE-BFC1-08002bE10318}

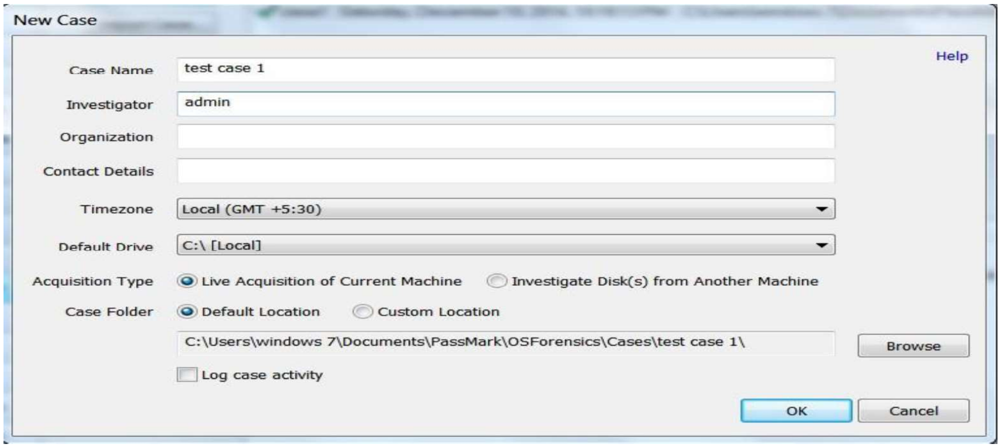
Step 1: Start OSForenscis as Start->All Programs -> OSForensics->OSForensics



Mouse over a feature for more information.

Step 2: Create a new Case by selecting Create Case. The following window will be popped:

Enter Appropriate Details and Select OK


New Case

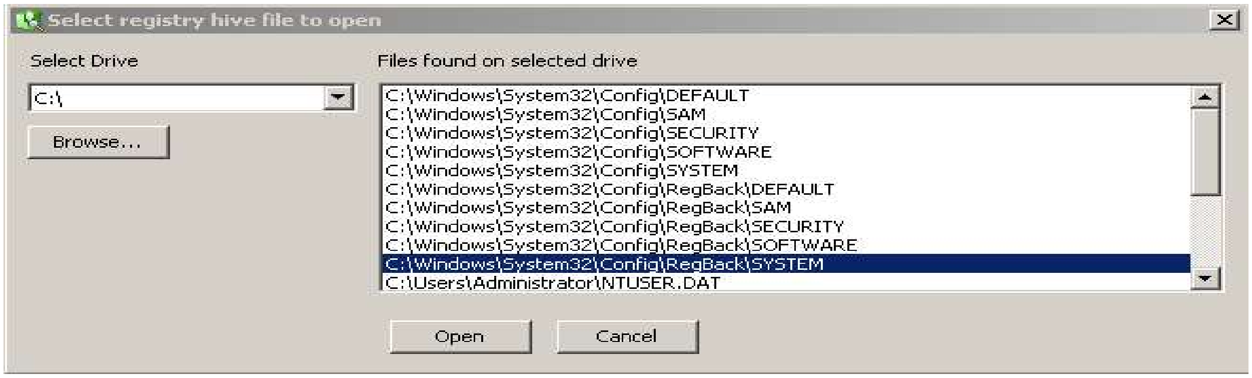
Help

Case Name	test case 1
Investigator	admin
Organization	
Contact Details	
Timezone	Local (GMT +5:30)
Default Drive	C:\ [Local]
Acquisition Type	● Live Acquisition of Current Machine ○ Investigate Disk(s) from Another Machine
Case Folder	● Default Location ○ Custom Location
	C:\Users\windows 7\Documents\PassMark\OSForensics\Cases\test case 1\

□ Log case activity

Step 3: Select Registry Viewer and select registry hive file to open for computer system

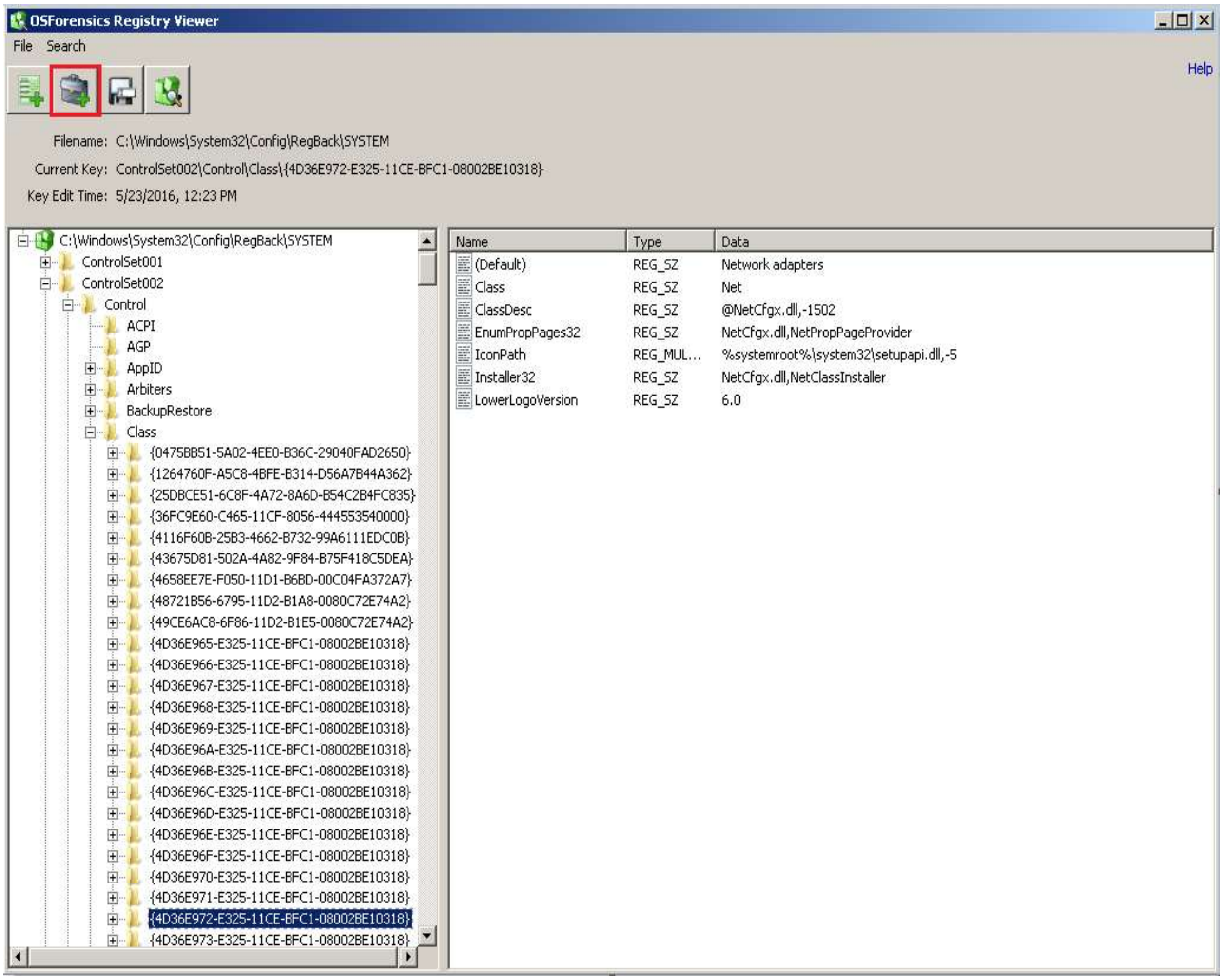
Select open


Select registry hive file to open
Select Drive
C:\
Browse...
Files found on selected drive
Open
Cancel

```
C:\Windows\System32\Config\DEFAULT
C:\Windows\System32\Config\SAM
C:\Windows\System32\Config\SECURITY
C:\Windows\System32\Config\SOFTWARE
C:\Windows\System32\Config\SYSTEM
C:\Windows\System32\Config\RegBack\DEFAULT
C:\Windows\System32\Config\RegBack\SAM
C:\Windows\System32\Config\RegBack\SECURITY
C:\Windows\System32\Config\RegBack\SOFTWARE
C:\Windows\System32\Config\RegBack\SYSTEM
C:\Users\Administrator\NTUSER.DAT
```

Step 4:

Select system file to add a key/value



Filename: C:\Windows\System32\Config\RegBack\SYSTEM

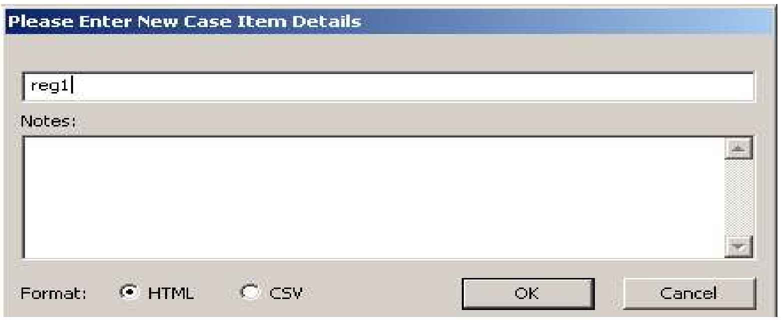
Current Key: ControlSet002\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}

Key Edit Time: 5/23/2016, 12:23 PM

```
C:\Windows\System32\Config\RegBack\SYSTEM
  ControlSet001
  ControlSet002
    Control
      ACPI
      AGP
      AppID
      Arbiters
      BackupRestore
      Class
        {0475BB51-5A02-4EE0-B36C-29040FAD2650}
        {1264760F-A5C8-4BFE-B314-D56A7B44A362}
        {25DBCE51-6C8F-4A72-8A6D-B54C2B4FC835}
        {36FC9E60-C465-11CF-8056-444553540000}
        {4116F60B-25B3-4662-B732-99A6111EDC0B}
        {43675D81-502A-4A82-9F84-B75F418C5DEA}
        {4658EE7E-F050-11D1-B6BD-00C04FA372A7}
        {48721B56-6795-11D2-B1A8-0080C72E74A2}
        {49CE6AC8-6F86-11D2-B1E5-0080C72E74A2}
        {4D36E965-E325-11CE-BFC1-08002BE10318}
        {4D36E966-E325-11CE-BFC1-08002BE10318}
        {4D36E967-E325-11CE-BFC1-08002BE10318}
        {4D36E968-E325-11CE-BFC1-08002BE10318}
        {4D36E969-E325-11CE-BFC1-08002BE10318}
        {4D36E96A-E325-11CE-BFC1-08002BE10318}
        {4D36E96B-E325-11CE-BFC1-08002BE10318}
        {4D36E96C-E325-11CE-BFC1-08002BE10318}
        {4D36E96D-E325-11CE-BFC1-08002BE10318}
        {4D36E96E-E325-11CE-BFC1-08002BE10318}
        {4D36E96F-E325-11CE-BFC1-08002BE10318}
        {4D36E970-E325-11CE-BFC1-08002BE10318}
        {4D36E971-E325-11CE-BFC1-08002BE10318}
        {4D36E972-E325-11CE-BFC1-08002BE10318}
        {4D36E973-E325-11CE-BFC1-08002BE10318}
```

Name	Type	Data
(Default)	REG_SZ	Network adapters
Class	REG_SZ	Net
ClassDesc	REG_SZ	@NetCfgx.dll,-1502
EnumPropPages32	REG_SZ	NetCfgx.dll,NetPropPageProvider
IconPath	REG_MUL...	%systemroot%\system32\setupapi.dll,-5
Installer32	REG_SZ	NetCfgx.dll,NetClassInstaller
LowerLogoVersion	REG_SZ	6.0

Enter Appropriate Details and Select OK



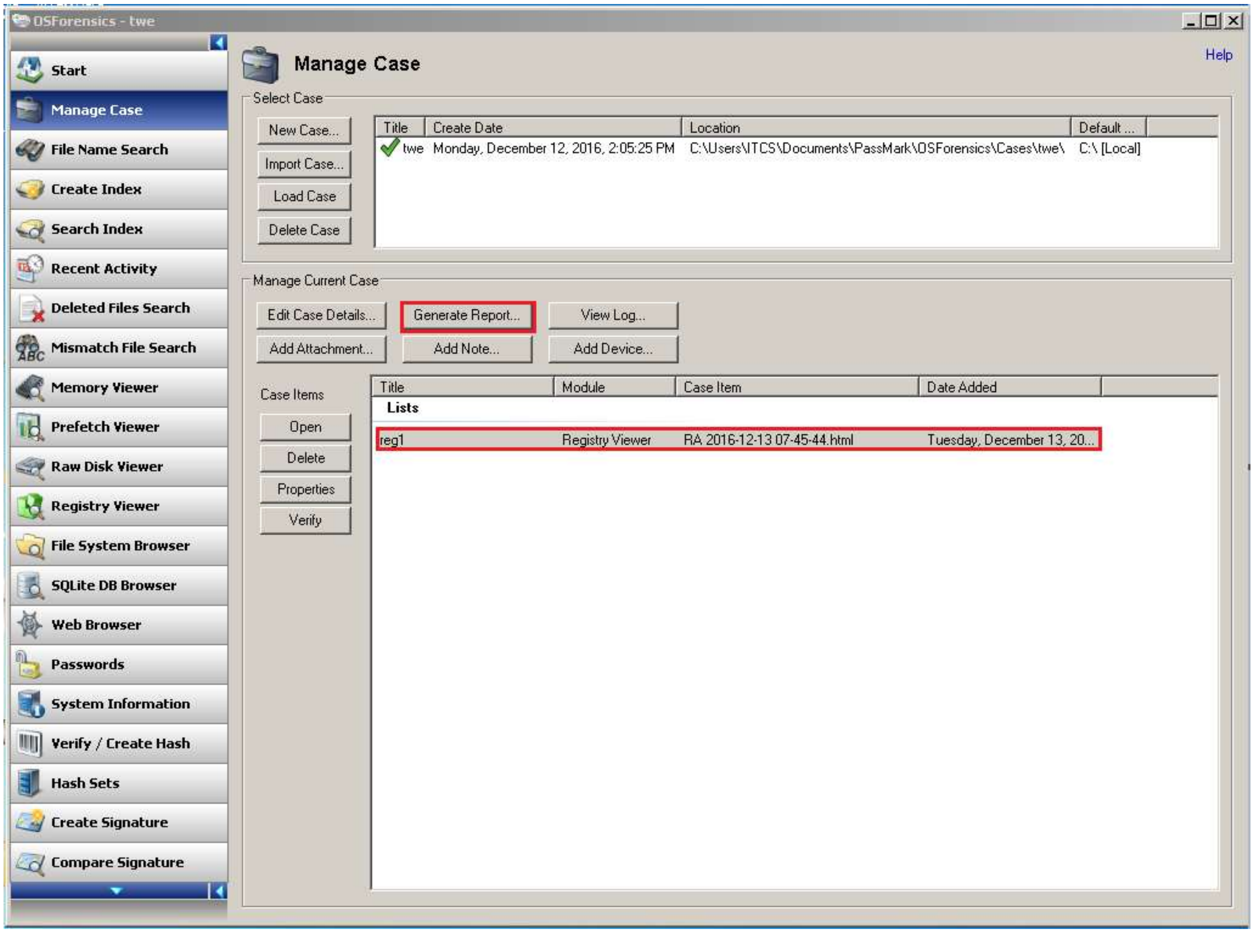
Please Enter New Case Item Details

reg1

Notes:

Format: ● HTML ○ CSV

Step 5: Select Manage Case



OSForensics - twe

Manage Case

Select Case

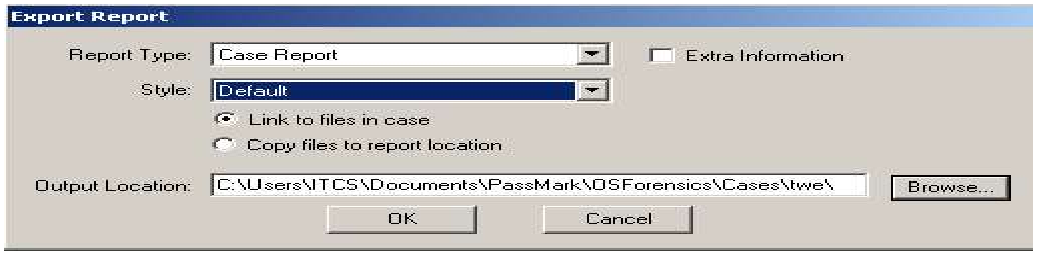
Title	Create Date	Location	Default ...
✓ twe	Monday, December 12, 2016, 2:05:25 PM	C:\Users\ITCS\Documents\PassMark\OSForensics\Cases\twe\	C:\ [Local]

Manage Current Case

Case Items

Title	Module	Case Item	Date Added
Lists			
reg1	Registry Viewer	RA 2016-12-13 07-45-44.html	Tuesday, December 13, 20...

Select registry viewer file and click on Generate Report


Export Report

Report Type: Case Report

□ Extra Information

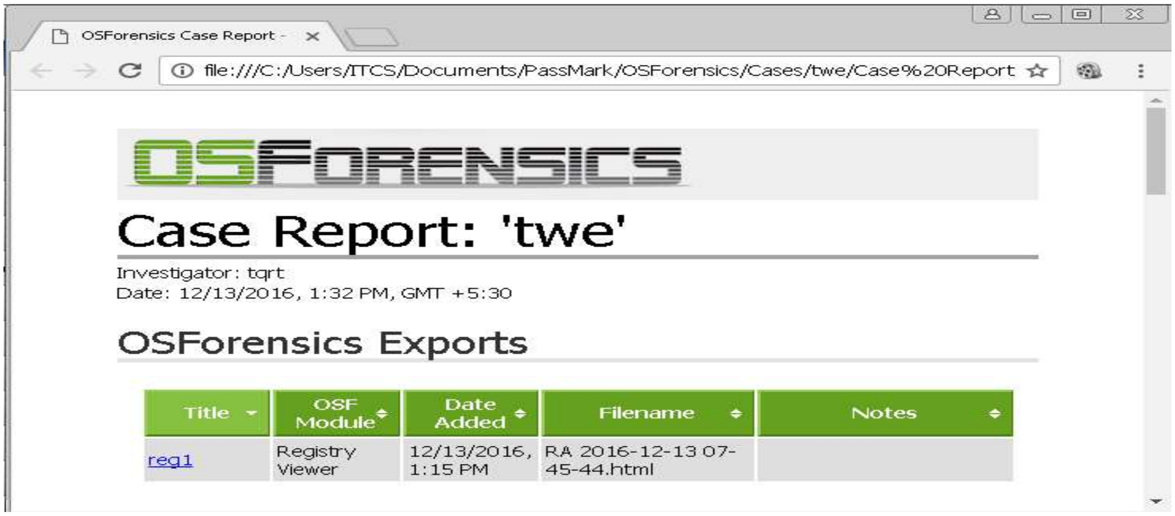
Style: Default

● Link to files in case

○ Copy files to report location

Output Location: C:\Users\ITCS\Documents\PassMark\OSForensics\Cases\twe\

Select Ok


OSForensics Case Report -
file:///C:/Users/ITCS/Documents/PassMark/OSForensics/Cases/twe/Case%20Report
OSFORENSICS

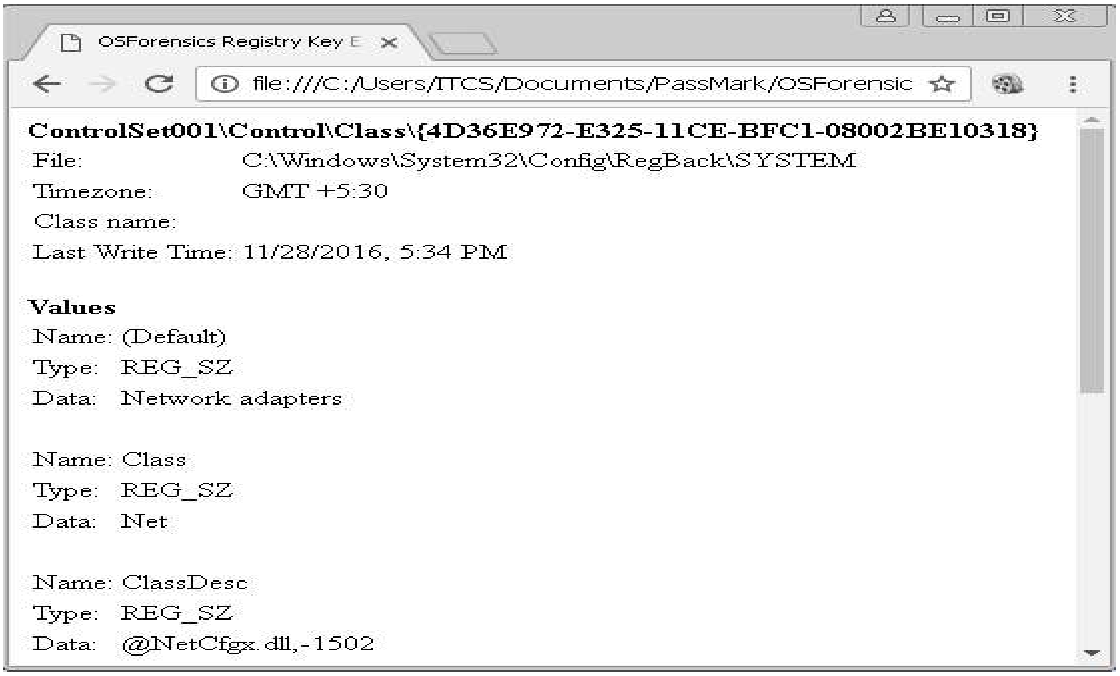
Case Report: 'twe'

Investigator: tqrt
Date: 12/13/2016, 1:32 PM, GMT +5:30

OSForensics Exports

Title	OSF Module	Date Added	Filename	Notes
reg1	Registry Viewer	12/13/2016, 1:15 PM	RA 2016-12-13 07-45-44.html	

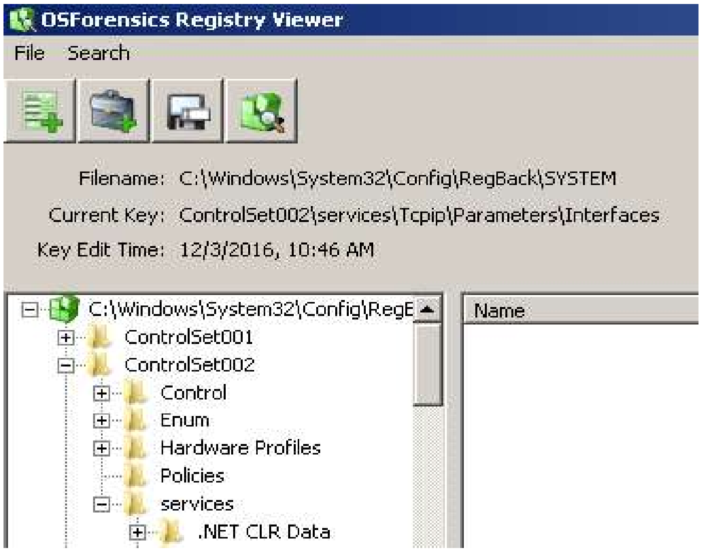
Select registry viewer file


OSForensics Registry Key E
file:///C:/Users/ITCS/Documents/PassMark/OSForensic

```
ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}
File:             C:\Windows\System32\Config\RegBack\SYSTEM
Timezone:         GMT +5:30
Class name:
Last Write Time: 11/28/2016, 5:34 PM

Values
Name: (Default)
Type:  REG_SZ
Data:  Network adapters

Name: Class
Type:  REG_SZ
Data:  Net

Name: ClassDesc
Type:  REG_SZ
Data:  @NetCfgx.dll,-1502
```

FILE2:

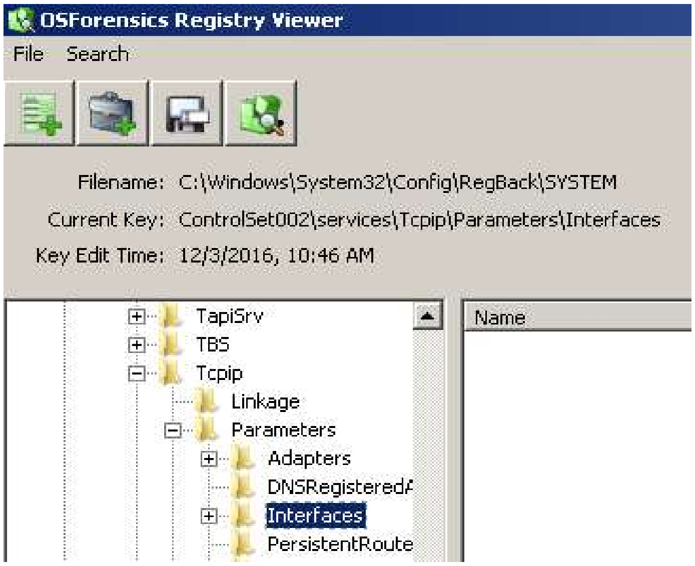
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip4/Param eters/Interfaces



Filename: C:\Windows\System32\Config\RegBack\SYSTEM

Current Key: ControlSet002\services\Tcpip\Parameters\Interfaces

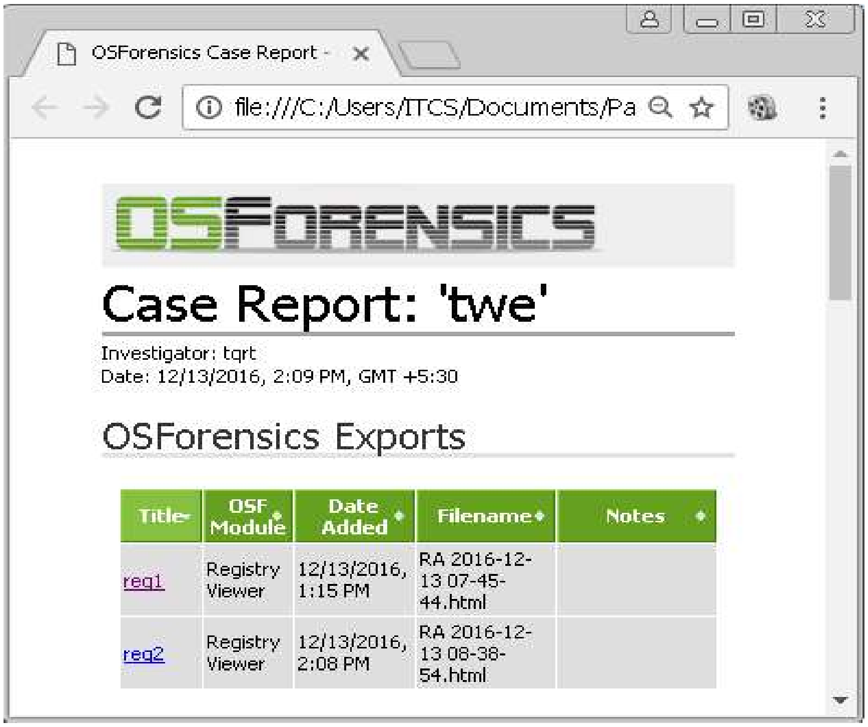
Key Edit Time: 12/3/2016, 10:46 AM



Filename: C:\Windows\System32\Config\RegBack\SYSTEM

Current Key: ControlSet002\services\Tcpip\Parameters\Interfaces

Key Edit Time: 12/3/2016, 10:46 AM

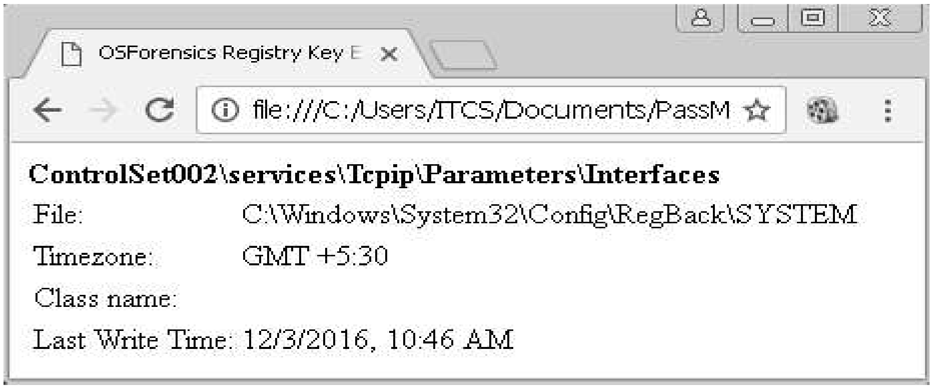


Case Report: 'twe'

Investigator: tqrt
Date: 12/13/2016, 2:09 PM, GMT +5:30

OSForensics Exports

Title	OSF Module	Date Added	Filename	Notes
reg1	Registry Viewer	12/13/2016, 1:15 PM	RA 2016-12-13 07-45-44.html	
reg2	Registry Viewer	12/13/2016, 2:08 PM	RA 2016-12-13 08-38-54.html	



OSForensics Registry Key E
file:///C:/Users/ITCS/Documents/PassM

ControlSet002\services\Tcpip\Parameters\Interfaces

File: C:\Windows\System32\Config\RegBack\SYSTEM
Timezone: GMT +5:30
Class name:
Last Write Time: 12/3/2016, 10:46 AM