ASSIGNMENT NO: 07

/*

Name:

Kshitish Deshpande

Roll No.:

PF22

Subject:

DFCL

*/

Problem Statement:

Install a suitable Digital Forensics framework (such as Encase) and perform investigation. Generate the various reports and analyse the same.

Objectives:

1. To study and explore Encase and its functionalities.

Theory:

Encase contain:

1. EnCase contains tools for several areas of the digital forensic process; acquisition, analysis and reporting.

2. It is capable of breaking down complex file structures for examination, such as the registry files, etc.

3. Encase have time Line.

4. Encase has full scripting abilities and allows automation of report ,decryption and carving.

5. It includes a scripting facility called EnScript with various API's for interacting with evidence.

6. Encase allows the investigator to conduct in depth analysis of user files to collect

evidence such as documents, pictures, internet history and Windows Registry information.

7. EnCase contains functionality to create forensic images of suspect media. Images are stored in proprietary **Expert Witness File format**; the compressible file format is prefixed with case data information and consists of a bit-by-bit (i.e. exact) copy of the media inter-spaced with CRC hashes for every 64K of data.

8. The file format also appends an MD5 hash of the entire drive as a footer.

9. Encase Forensics can process a large number of data measured in hundreds of terabytes.

10. As of EnCase V7, Mobile Phone Analysis is possible with the addition some add-ons available from Guidance Software.

Encase System Requirements:

| Minimum Setup	Recommended Setup
● Dual-core Processor ● 4 GB RAM ● First Hard Drive for OS and Software with 300 MB available space ● Second Hard Drive for cases ● Windows XP Pro, Server 2003, Server 2008, Vista, 7 (32bit)	● Quad-core Processor. ● 16 GB RAM ● First Hard Drive for OS and Software with 300 MB available space (I really like the WD velociraptor for its speed of 10,000 rpm) ● Second Hard Drive should be a RAID array for I/O speeds and redundancy ● Windows 7 (64bit)

Case Creation :

After adding images or devices to the case, we should click Process (also, we can start the EnCase Processor via EnScript: EnScript – EnCase Processor).
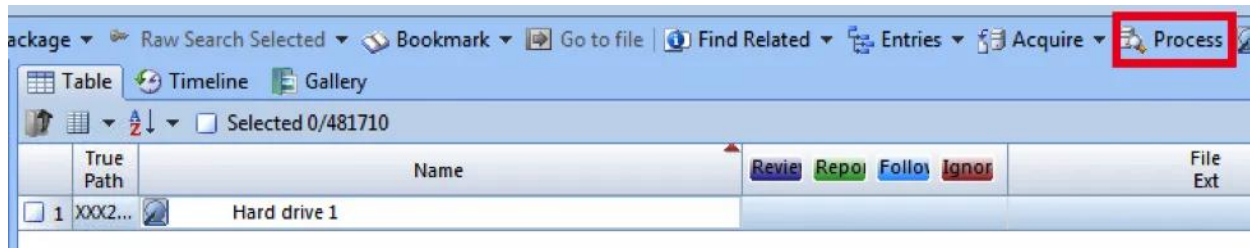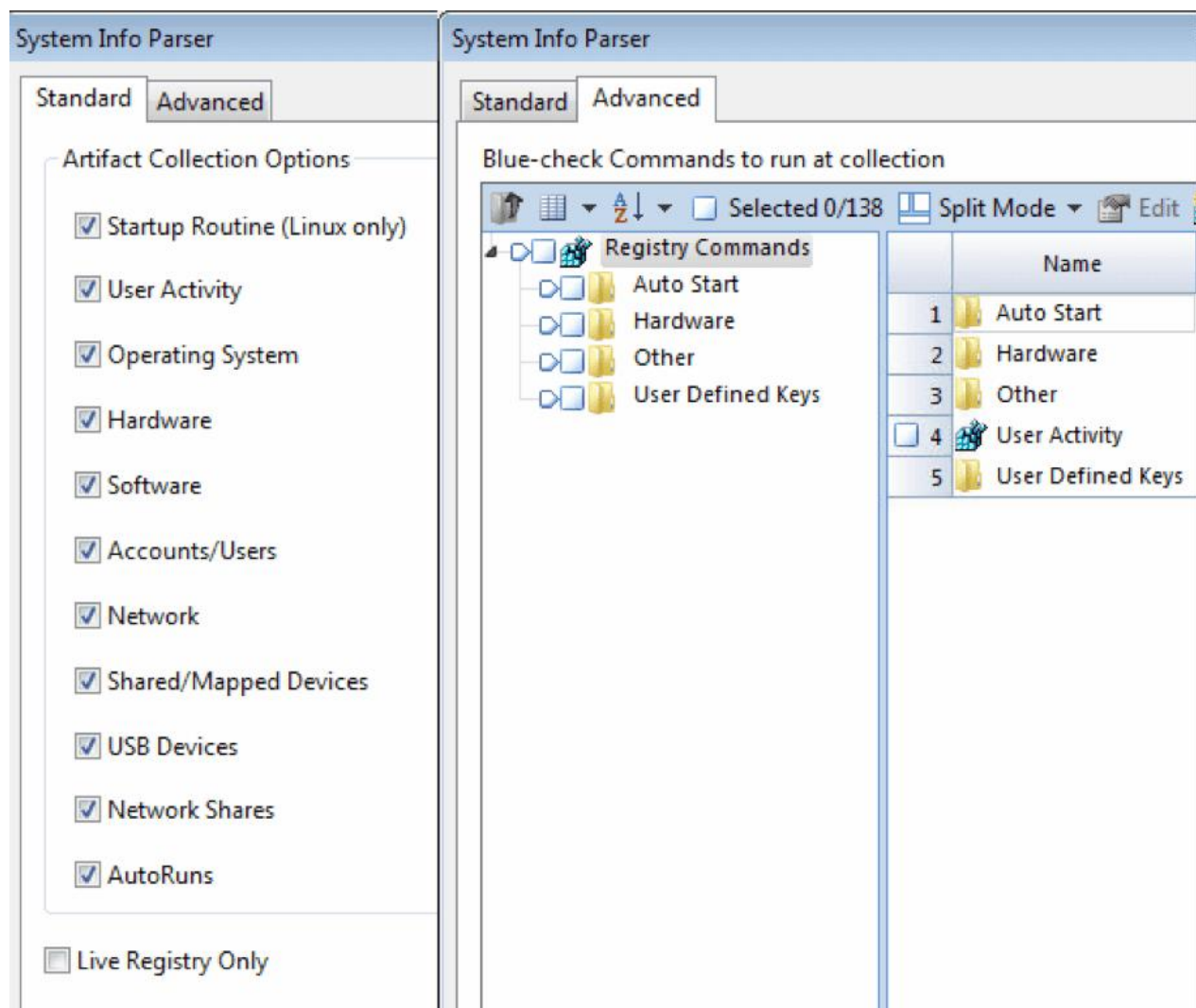

Figure Process button

You'll see EnCase Processor Options dialog, where you should choose options you need.
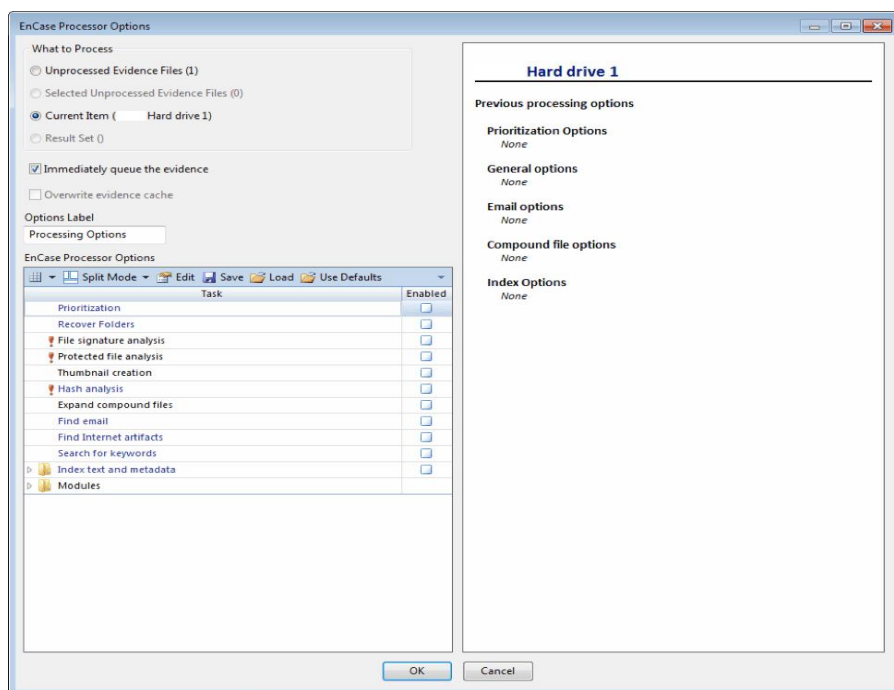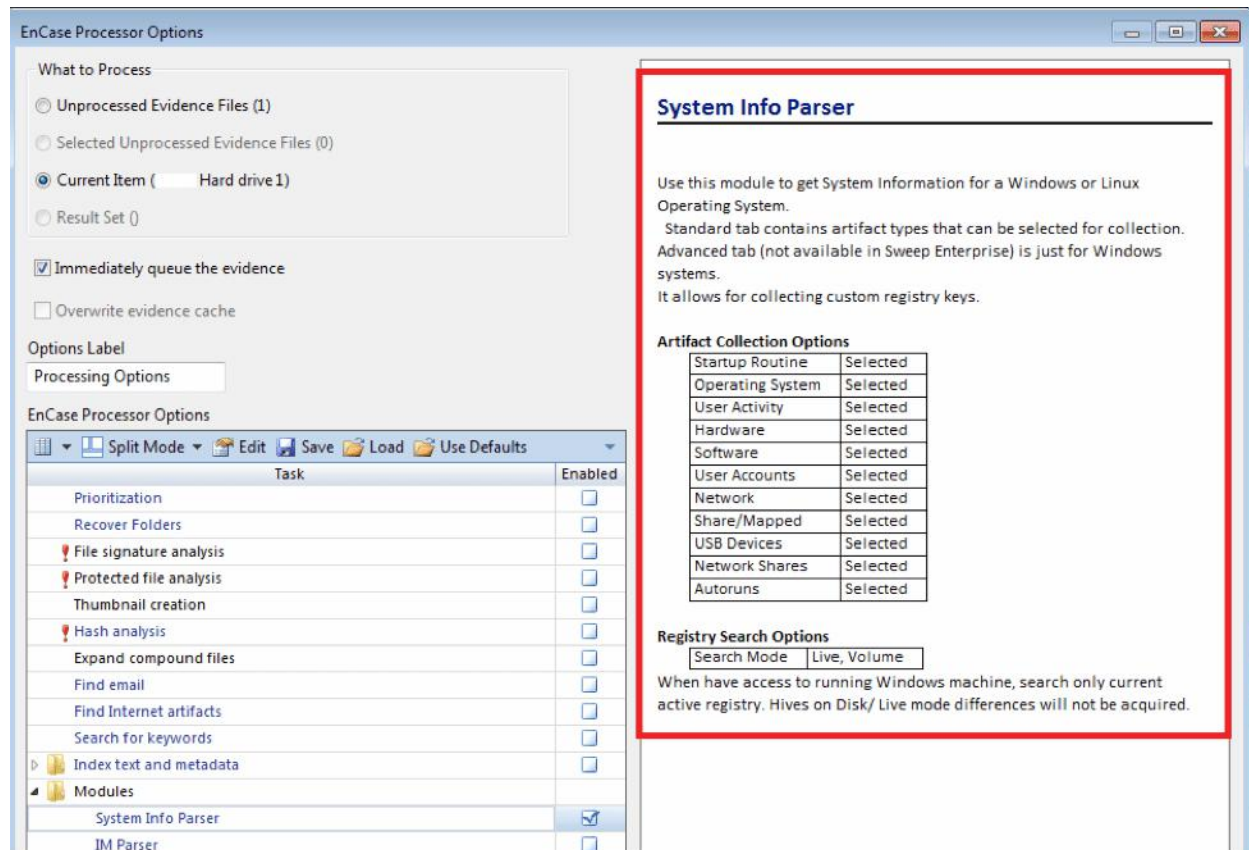

Figure EnCase Processor Options dialog

Be very careful choosing options. If you choose too many options, or very resource-intensive options, processing could take too much time.

Figure System Info Parser module additional options

If you choose an option, you see its description in the right pane:

Figure System Info Parser module description

If you double click on module's name, you see additional options.

Click OK and processing will be started; its progress bar is located in the bottom right corner. Also, you can view processing details in Processor Manager (View – Processor Manager).

Figure Processor Manager tab

When the process is finished, you should run Case Analyzer EnScript. In opened dialog box double click Case – it'll start adding processed data to the report.
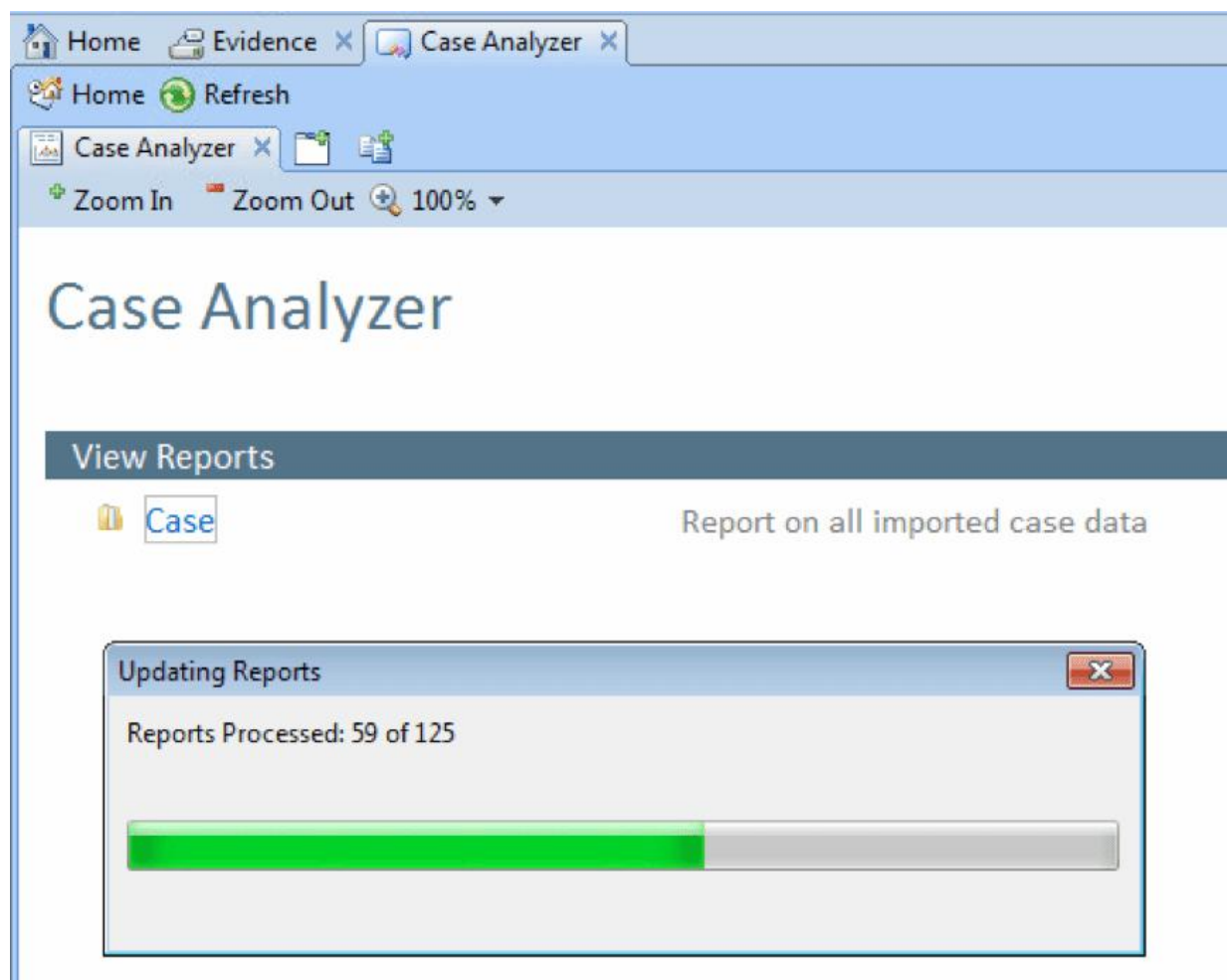
Figure Adding data to the report

In the next dialog, opened after the task is finished, choose data you need and click Save Report.
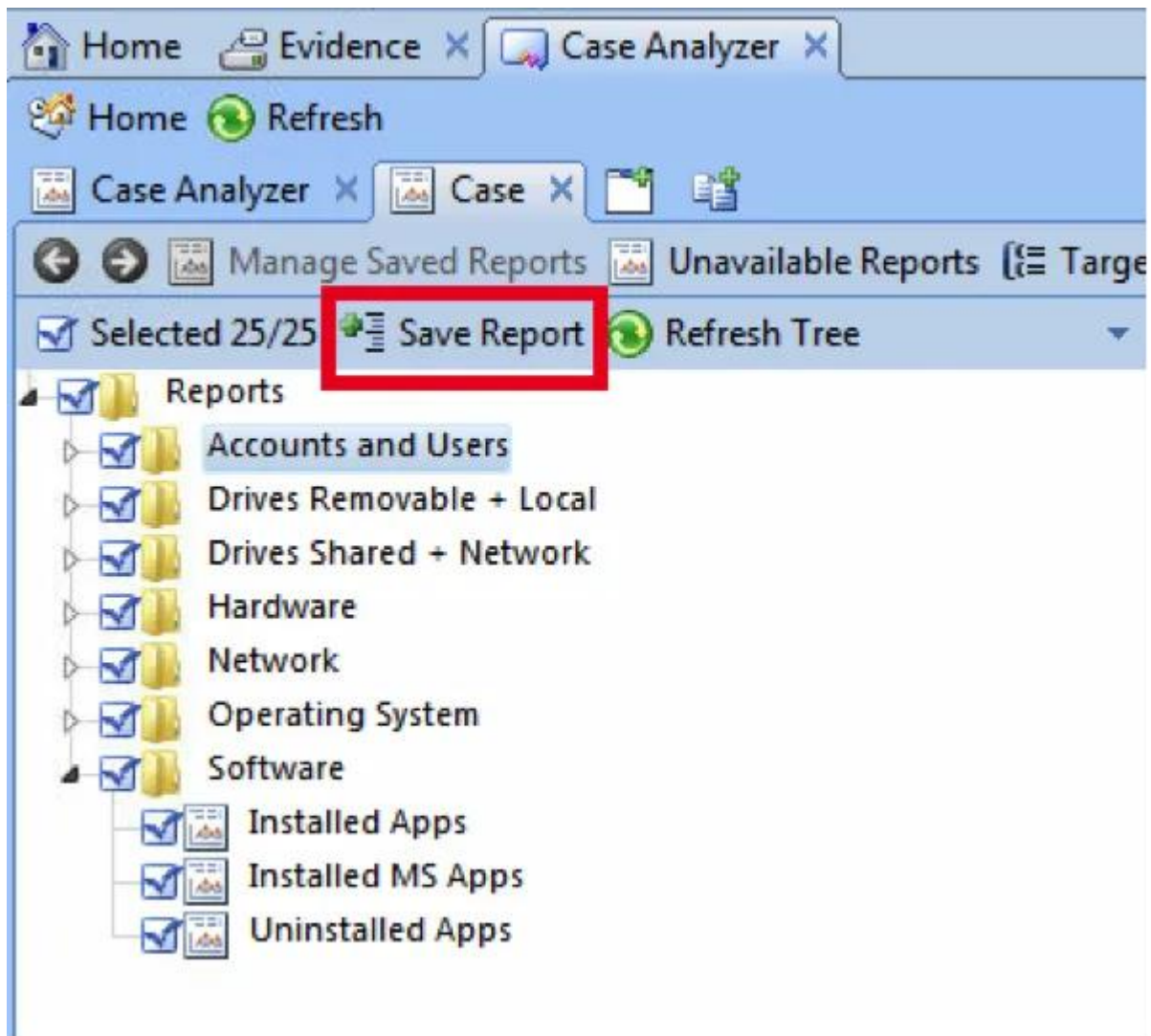
Figure Case Analyzer tab

Now you can customize you report according to your needs, clicking Manage Saved Reports.

Figure Manage Saved Reports window

If you click View Report, you can view its final version.

About System Info

System Information from the Windows Registry, derived from the following registry keys:
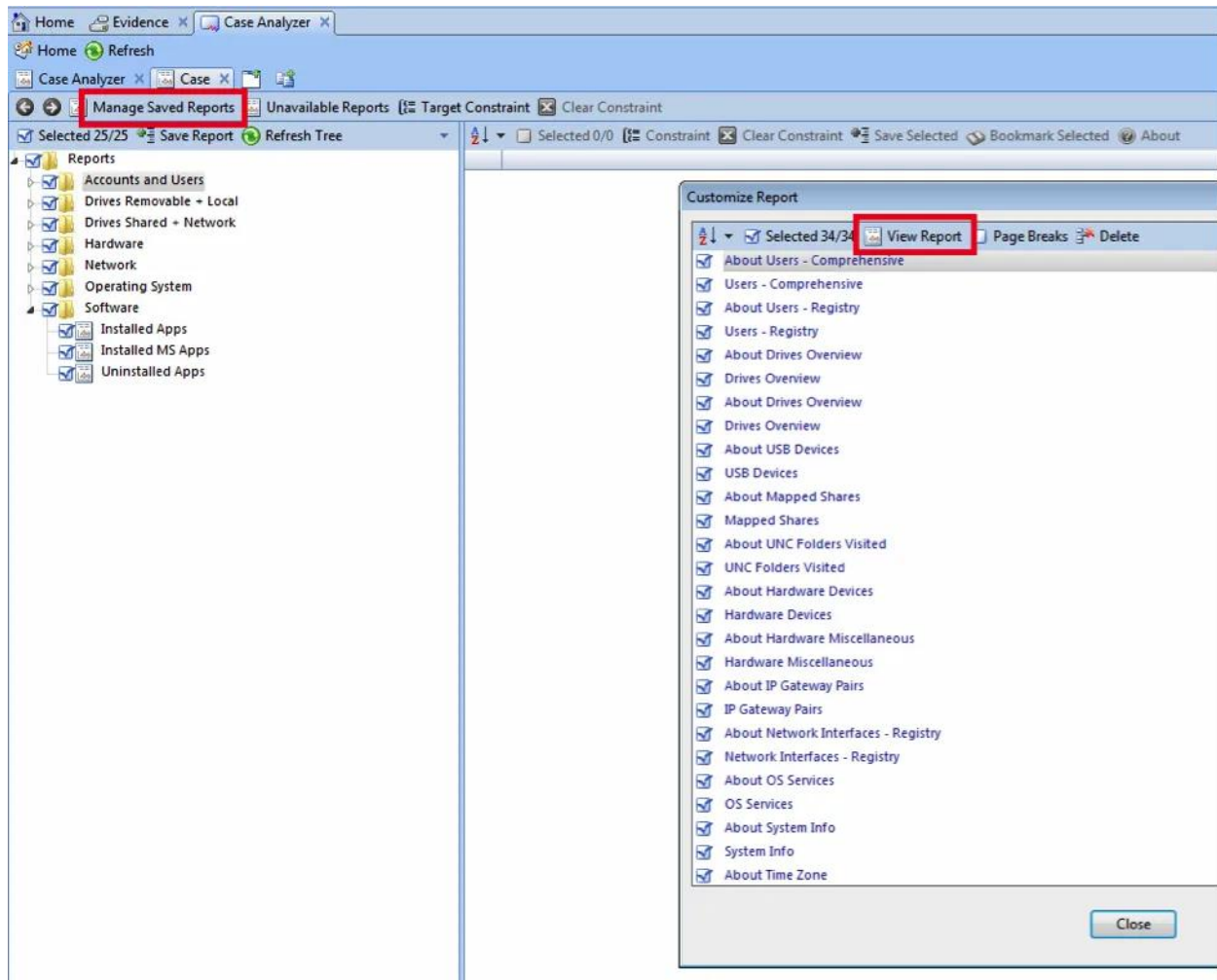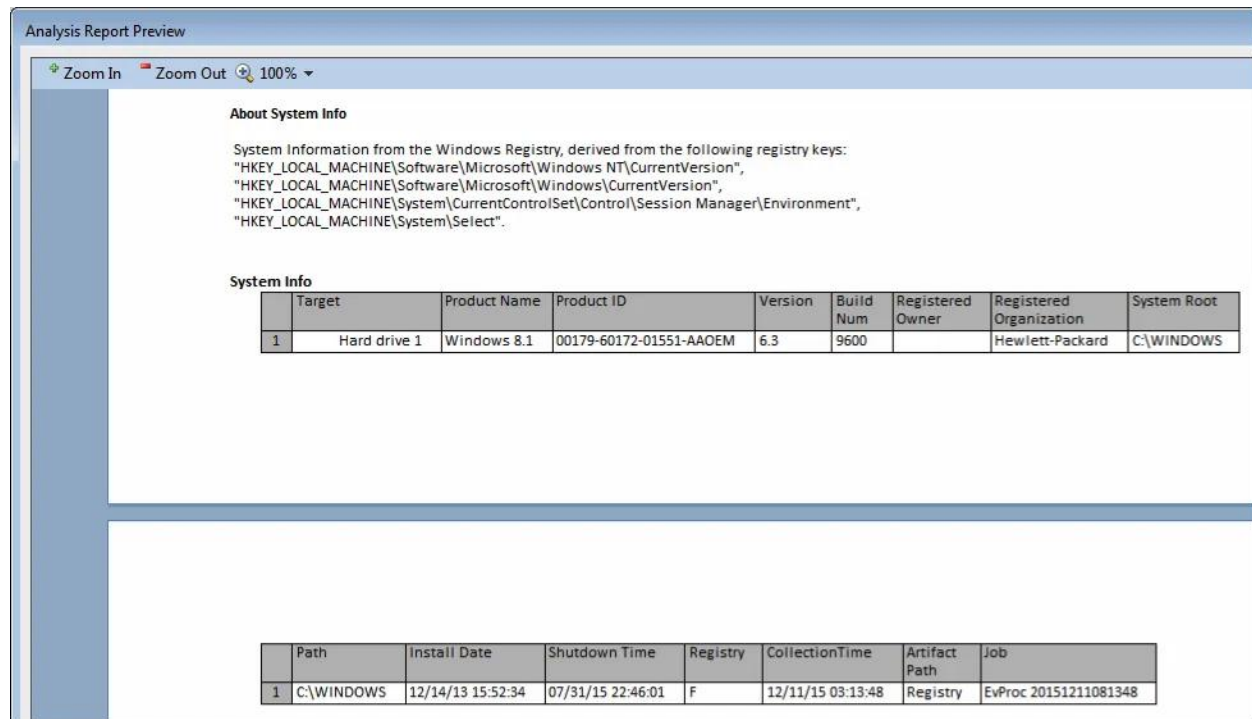"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion",
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion",
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment",
"HKEY_LOCAL_MACHINE\System\Select".

System Info

	Target	Product Name	Product ID	Version	Build Num	Registered Owner	Registered Organization	System Root
1	Hard drive 1	Windows 8.1	00179-60172-01551-AAOEM	6.3	9600		Hewlett-Packard	C:\WINDOWS

	Path	Install Date	Shutdown Time	Registry	CollectionTime	Artifact Path	Job
1	C:\WINDOWS	12/14/13 15:52:34	07/31/15 22:46:01	F	12/11/15 03:13:48	Registry	EvProc 20151211081348

Figure The report fragment

Conclusion:

Hence, understood the features of Encase.