Academic Task CA 3

LOVELY PROFESSIONAL UNIVERSITY

Name – Saurabh Gupta

Reg. no – 11914681

Roll no- 61

Section- KE016

Table of Content

1. INTRODUCTION

Computer forensics, also known as digital forensics, is the act of gathering, analysing, and archiving electronic data so that it may be used as evidence in court. Because of the rising popularity of digital devices and their usage in criminal activity, the area of computer forensics has expanded significantly over the years. As technology advances, computer forensics will become increasingly important in solving cybercrimes, intellectual property theft, and other digital security problems. Computer forensics uses a variety of techniques and technologies to unearth evidence that may be utilised in legal procedures, including as data recovery, network analysis, forensic imaging, and decryption.With the ongoing proliferation of digital devices and the rising sophistication of hackers, computer forensics is more crucial than ever in safeguarding persons and companies from cyberattacks as well as identifying and prosecuting those guilty for digital crimes.

1.1. TYPE OF COMPUTER FORENSICS

There are several forms of computer forensics, each with its own focus and goals. Some of the most popular forms of computer forensics are as follows:

Disk forensics : Disk forensics is studying hard discs, USB drives, and other storage devices to recover lost or concealed material and identify evidence of criminality.

Network forensics: Network forensics includes studying network traffic to discover illegal access, data breaches, and other security problems

Mobile forensics : Mobile device forensics is investigating mobile devices such as smartphones and tablets in order to retrieve data and evidence connected to criminality.

Memory forensics : Memory forensics is the act of studying a computer or device's memory to discover running programmes, system settings, and other information linked to security events.

Cloud forensics :Cloud forensics is the process of examining data saved on cloud-based platforms such as Dropbox, Google Drive, or OneDrive in order to detect security breaches, cybercrimes, or intellectual property theft.

Forensic data analysis: This sort of forensics includes examining data obtained from many sources to uncover patterns, trends, or correlations that may be significant to a legal case.

2. System Description

Open source software is computer software whose source code is freely available to the public, allowing anyone to examine, alter, and distribute the software. In contrast, proprietary software is owned by a firm or individual, and the source code is kept private. Open source software is often created by a group of developers that work together to enhance the product and resolve any bugs or difficulties.Open source software is typically distributed under an open source licence that specifies the terms and conditions for using, altering, and sharing the programme. The GNU General Public License (GPL), Apache License, and MIT License are the most prevalent open source licences. From operating systems like Linux and Android to apps like the Apache web server, MySQL database, and the Firefox web browser, open source software may be utilised for a variety of reasons. Users can alter the programme to meet their individual requirements and tastes because the source code is publicly available.

One of the key advantages of open source software is its adaptability and customization. Because the code may be modified by anybody, customised versions of open source software can be created that are targeted to certain use cases or industries. Furthermore, because the software is created by a community of developers, vulnerabilities and security flaws may be detected and resolved fast.

2.1. TARGET SYSTEM DESCRIPTION

Belarc Advisor is a Windows-based tool that scans the system and generates a detailed report with information about installed hardware components such as the processor, motherboard, memory, and hard drive, as well as software components such as the operating system, applications, and security patches. IT professionals and system

administrators generally use the programme to keep track of the hardware and software settings of many PCs. Belarc Advisor's data may be used for a number of applications, such as resolving hardware or software faults, finding security vulnerabilities, and checking software licencing compliance. By detecting old or underperforming components, the tool may also be used to plan system upgrades or replacements.

Microsoft's Sysinternals Suite is a collection of over 70 system utilities and troubleshooting tools. These tools are intended to assist users and IT professionals in diagnosing and troubleshooting Windows operating system issues, monitoring system performance, managing processes and services, and a variety of other tasks. Process Explorer, which provides detailed information about running processes and their associated threads, handles, and DLLs; Autoruns, which displays all programmes and services that are configured to run at system startup; and TCPView, which displays active network connections and their associated processes, are all part of the Sysinternals Suite. Process Monitor, which enables real-time monitoring of file system, registry, and process activity; Disk2vhd, which produces virtual hard discs from physical discs; and PsExec, which permits remote execution of commands on other systems, are among prominent utilities in the Sysinternals Suite.

The Sysinternals Suite utilities are all available as standalone executables, which means they may be executed from a USB drive or network share without needing to be installed on the host system. Microsoft also updates the utilities on a regular basis to maintain compatibility with the most recent versions of Windows and to fix any known bugs or security vulnerabilities.

3. Analysis Report

Belarc Advisor is a system information and auditing application that allows users to do extensive analyses of their computer hardware and software setups. The utility scans the system and creates a detailed report with information on the operating system, installed applications, hardware components, network devices, user accounts, and other system parameters. Belarc Advisor's report contains useful information for system administrators, IT professionals, and other users who need to discover and fix issues with their systems. It can identify missing security updates, obsolete drivers, and possible security flaws, as well as track software and hardware changes over time. One of Belarc Advisor's primary capabilities is its ability to retrieve and display product keys for installed applications. This is especially helpful when transferring to a new computer or reinstalling software following a system crash or hardware breakdown.

Overall, Belarc Advisor is an excellent tool for anyone who wants to do a thorough review of their system settings. It is free for personal use, simple to use, and contains a plethora of information on the hardware and software on the computer. It should be emphasised, however, that the tool is not intended to handle complex system maintenance or repair

activities, and users may need to seek out additional tools and resources to solve any problems.

3.1 Steps and Snapshots

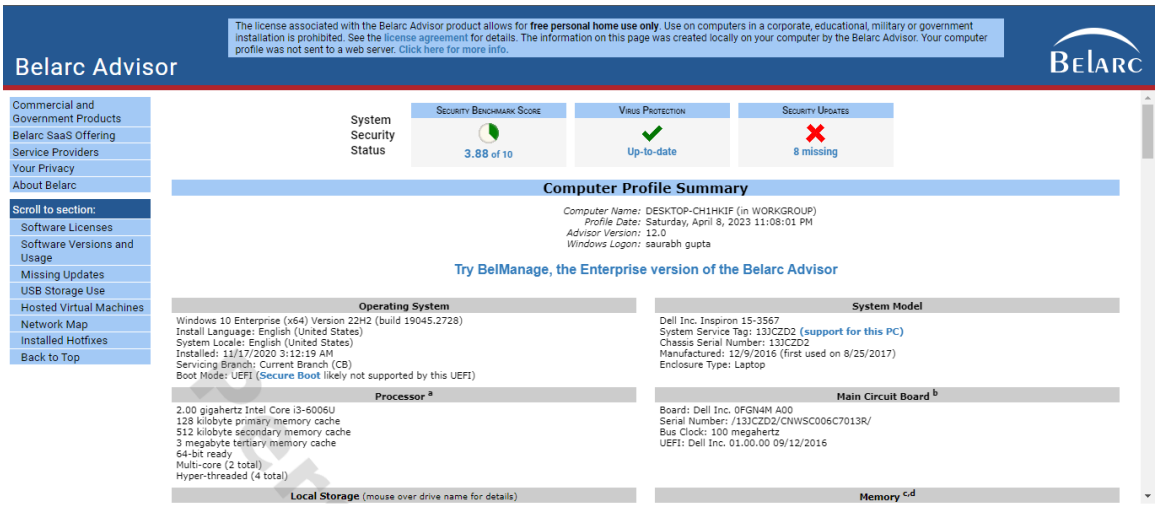

Fig 1: In this step it shows about the system information of Computer. It shows every detail of computer like operating system, system models processors and main circuit board of sytem.

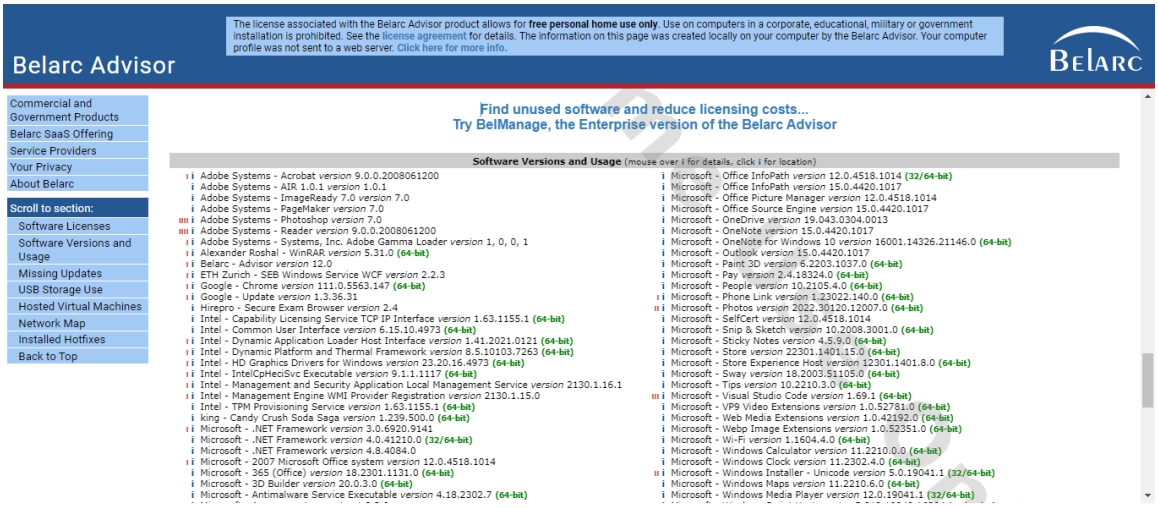

Fig 2: In this step it shows about the system software version and their usages.

Software Licenses	
Adobe Systems - Adobe PageMaker 7.0	1039-1121-2998-7586-7388-7545
Adobe Systems - Adobe Photoshop 7.0	1045-1209-6738-4668-7696-2783
Belarc - Advisor	e602fc1d
Intel - GFX	{F0E3AD40-2BBD-4360-9C76-B9AC9A5886EA}
Microsoft - Internet Explorer	00329-00000-00003-AA280 (Key: NPPR9-FWDCX-D2C8J-H872K-2YT43)
Microsoft - Office Professional Plus 2013	00216-40000-00000-AA173 (Key: YC7DK-G2NP3-2QQC3-J6H88-GVGXT, expires 9/23/2023)
Microsoft - Office Project Professional 2007	89403-707-4159871-63139 (Key: HCFPT-K86VV-DCKH3-87CCR-FM6HW)
Microsoft - PowerShell	89383-100-0001260-04309
Microsoft - Windows 10 Enterprise (x64)	00329-00000-00003-AA280 (Key: NPPR9-FWDCX-D2C8J-H872K-2YT43)
VMware - Workstation	ZF3R0-FHED2-M80TY-8QYGC-NPKYF

Fig 3: This section of software shows the software licenses key and their respected Id no.

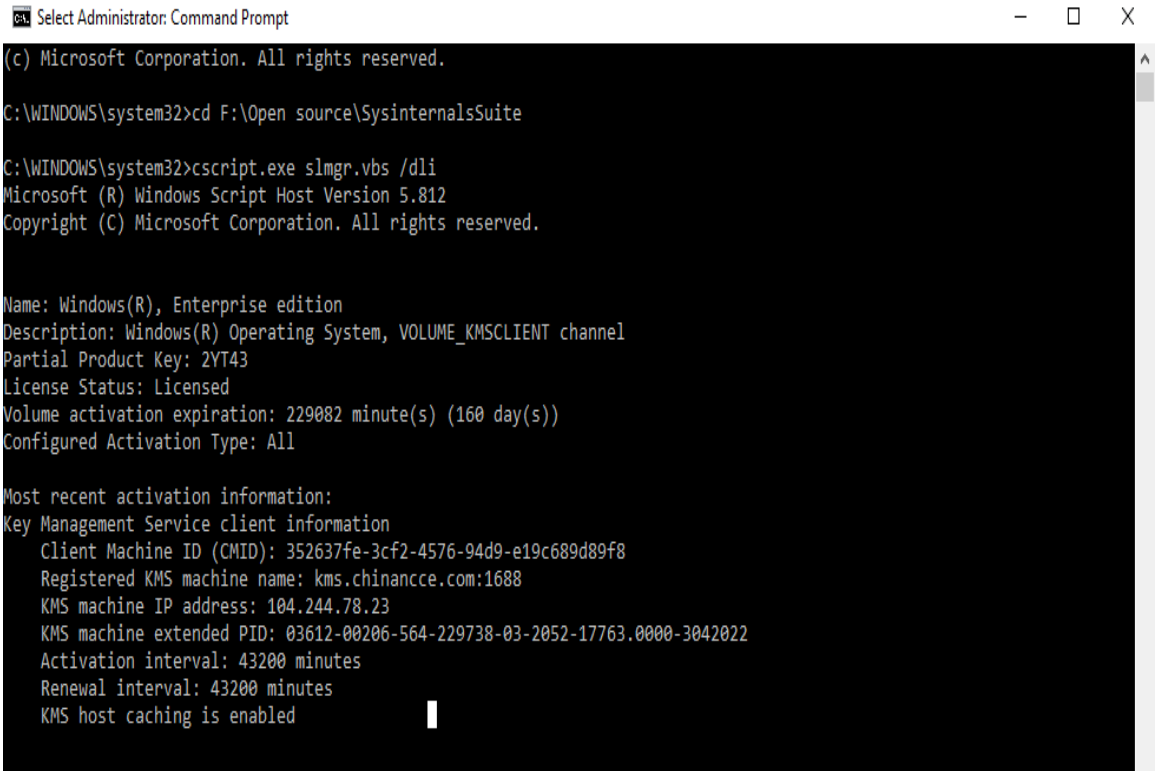

Fig 4: This step shows the product key and id of the window in sysinternalssuite open source software after using command cscript.exe slmgr.vbs /dli in command prompt.

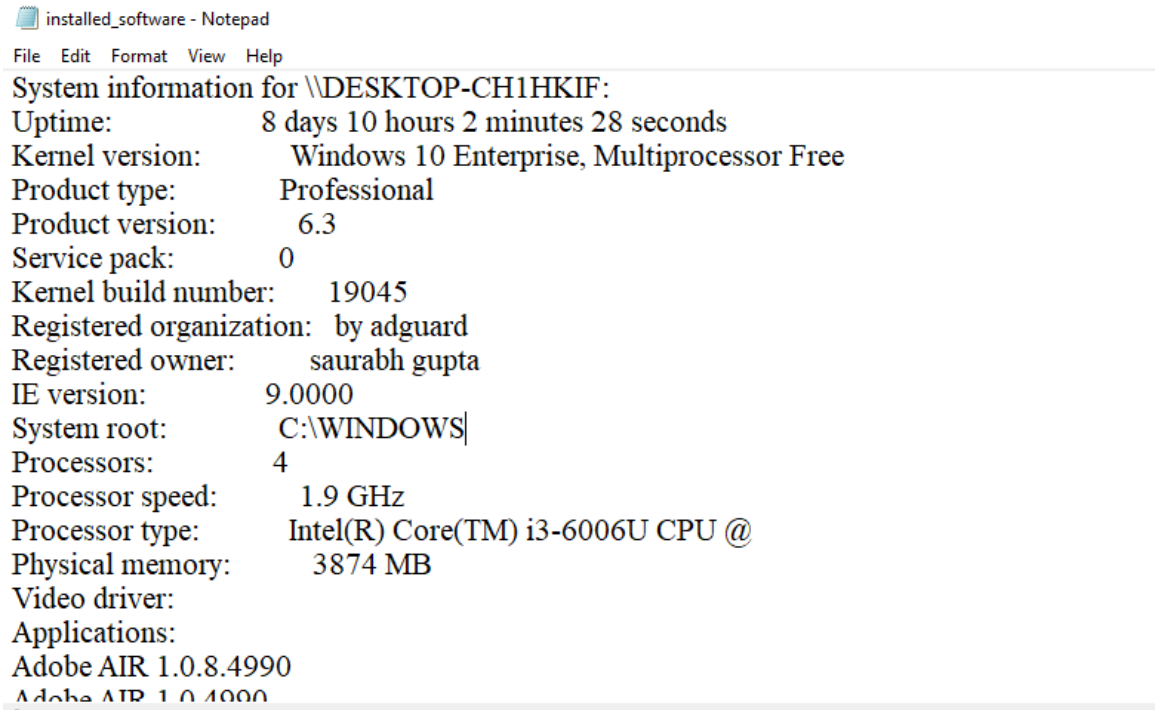

Fig 5 & 6: in this figure it shows the installed software in system after using command psinfo.exe -s > installed_software.txt in command prompt. It will create a text file named "installed_software.txt" in the same folder where you extracted the Sysinternals Suite.

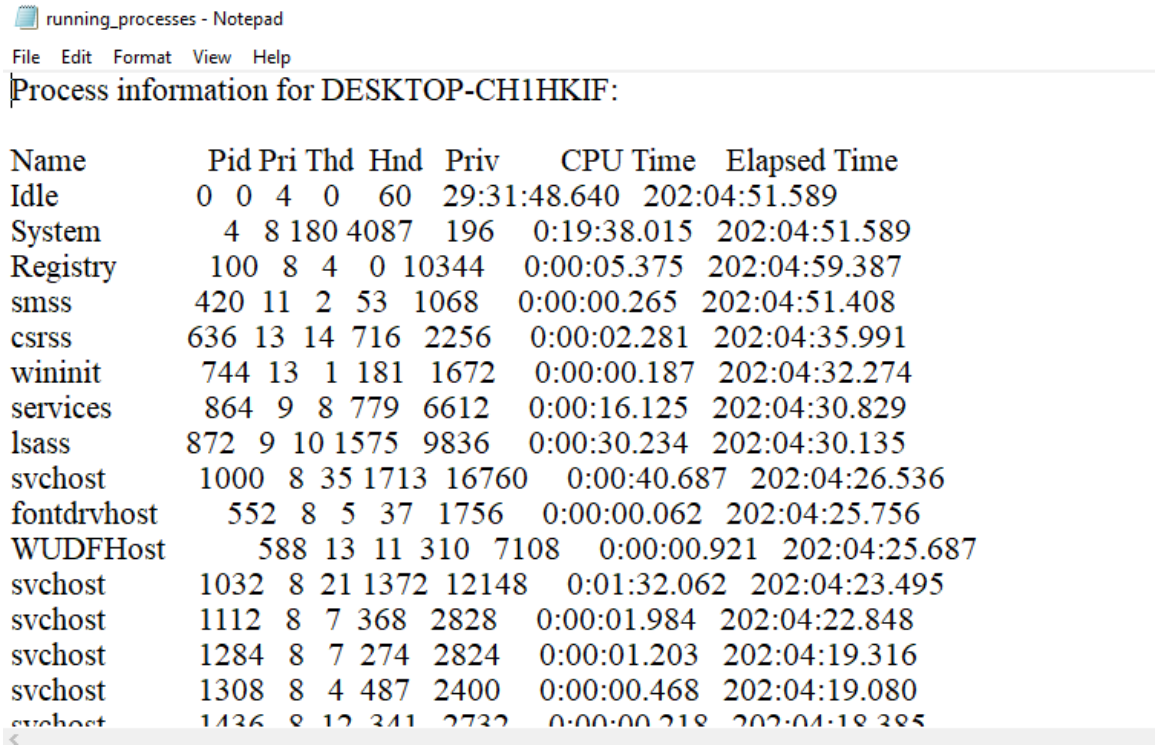

Fig 7: in this figure it shows all currently running processes in system after using command pslist.exe > running_processes.txt in command prompt. It will create a text file named "running_processes.txt" in the same folder where you extracted the Sysinternals Suite.

3.2 CONCLUSION

Using Belarc Advisor and Sysinternalssuite open source software we can easily find the system information utilities, it display the window product keys and Id, it shows the all list of installed software and all currently running processes in the system. Belarc Advisor is an application which scans the computer system and provide details about our hardware and software configuration.

Sysinternalssuite software has ability to provide deep insight into the operating system and its components.

4.Reference

[1] T. Grance, K. Kent and B. Kim, "Computer Security Incident Handling Guide", *Special pub.*, vol. 800, no. 61, 2004, [online] Available: http://csrc.nist.gov/publications/nistpubs/800-6l/sp800-6l.pdf.

[2] P. Sayer, "New center battles computer security threats", *PC World Mag*, Jan. 2001, [online] Available: http://www.pcworld.com/news/article. asp?aid=38750.

[3] *The national strategy to secure cyberspace*, Feb. 2003, [online] Available: http://www.us-cert.gov/ reading_room/cyberspace_strategy.pdf.

[4] *Certified Information System Security Professional. CertCities.com*, 2005, [online] Available: http://certcities.com/certs/other/cert.asp?ID=59.

[5] H. Berghel, *Digital Village: The discipline of Internet Forensics*, vol. 46, no. 8, pp. 15-20, 2003, [online] Available: http://doi.acm. org.ezproxy.umuc.edu/10.ll45/859670.859687.