LOVELY PROFESSIONAL UNIVERSITY

NAME: KOMAL KUMARI

REG NO: 11915548

SECTION: KE016

ROLL NO: B-65

SUBJECT: OPEN-SOURCE TECHNOLOGIES (INT-301)

GITHUB LINK: https://github.com/komal592000/INT301CA3

QUESTION NUMBER – 42

PROBLEM STATEMENT:

Using desired Open Source Software display an overview of all the hardware and operating system detail; also do live monitoring to show the temperature and current usage of various hardware components.

INDEX

CHAPTER-1 INTRODUCTION

Computer forensics is a branch of forensic science which deals with the application of investigative analysis techniques on computers in order to retrieve and preserve evidence in a way that is legally admissible. a major aspect of the science of computer forensics is the performance of a structured investigation on a computing device to find out either what happened or who was responsible for what happened, while at the same time maintaining a properly documented chain of evidence in a formal report.

TYPES OF COMPUTER FORENSICS :

1. **Network forensics:** This involves monitoring and analysing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.

2. **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.

3. **Malware forensics:** This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, trojans to identify the hacker involved behind this.

4. **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

5. Memory forensics: This branch of forensics deals with collecting data from the memory(like cache, RAM, etc.) in raw and then retrieve information from that data.

6. **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyse data from the mobile phone.

7. **Database forensics:** This branch of forensics examines and analyses the data from databases and their related metadata.

DISK FORENSICS :

Disk forensics which is also known as digital forensics or computer forensics, is the process of analysing, collecting and preserving electronic data from storage devices such as hard drives, solid-state drives (SSDs), and USB drives. The goal of disk forensics is to identify and investigate digital evidence that may be relevant to a legal investigation, such as a criminal case or a civil lawsuit. Disk forensics can be used to identify malicious software or malware, recover deleted files, track user activity, and identify evidence of cybercrime. It can also be used to investigate employee misconduct, intellectual property theft, and other types of digital crimes. The field of disk forensics is constantly evolving, as new storage technologies and security measures are developed. Forensic analysts must stay up-to-date with the latest tools and techniques to ensure that they are able to identify and recover relevant digital evidence in an effective and efficient manner.

1.1 Objective of the project :

The objective of this project is to use open-source software to display an overview of all the hardware and operating system details and also perform live monitoring of the temperature and current usage of various hardware components.

1.2 Description of the project :

The project involves using open-source software to provide a detailed overview of the hardware and operating system details of a target system. Additionally, it involves monitoring the temperature and current usage of various hardware components in real-time. The project

aims to provide a comprehensive and accurate analysis of the system's performance to aid in troubleshooting and optimization.

1.3 Scope of the project :

The project's scope includes the use of open-source software to collect and display system hardware and operating system information. It also includes the development of live monitoring capabilities for various hardware components such as CPU, GPU, RAM, and storage devices. The project's scope is limited to desktop and server environments running Linux or Windows operating systems.

CHAPTER-2 SYSTEM AND SOFTWARE DISCRIPTION

SPECCY

Fig. 2.1 software logo (speccy)

Speccy is a free evaluation tool developed by Piriform for Microsoft Windows PC components. The application delivers detailed system information reports on the individual software and hardware elements in the computer or laptop: ‘Audio’, ‘CPU’, ‘Graphics’, ‘Motherboard’, ‘Network’, ‘Operating System’, ‘Optical Drives’, ‘Peripherals’, ‘RAM’, and

‘Storage’. You can review a thorough summary within the first tab in the user interface. It evaluate the internal and external elements of the system to deliver an analysis that lets us better understand the condition of our devices. The intuitive user interface has a simple design that you can easily explore. The information utility delivers a brief synopsis of each unit in the ‘Summary’ tab. You can conveniently see the brand and model numbers of the items.

One or more devices may be listed under the names in the "Summary" section. The data in the 'Operating System' segment will quickly let you know the important specifications: serial number, installation date, etc. You can check the automatic update settings in the OS area. In the "Antivirus" area, you can find out if the anti-malware software is disabled or enabled.

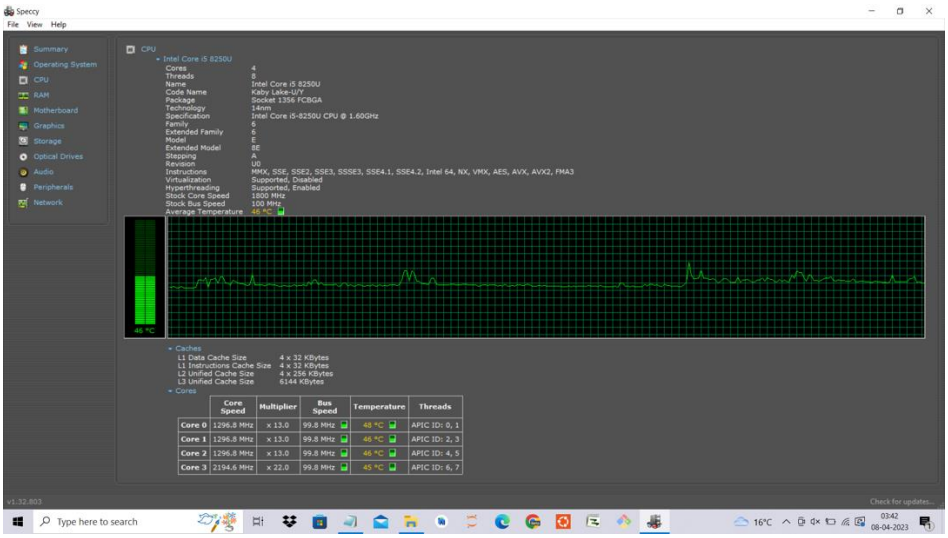

Fig. 2.2 CPU section in software to show the no. of processors

In the 'CPU' section next to 'Cores' you can determine how many processors your central processing unit has. The table at the bottom of the screen will give you information about the core speed and temperature of each processor in real time. In addition, the graph shows "Multiplier", "Bus Speed" and "Threads".

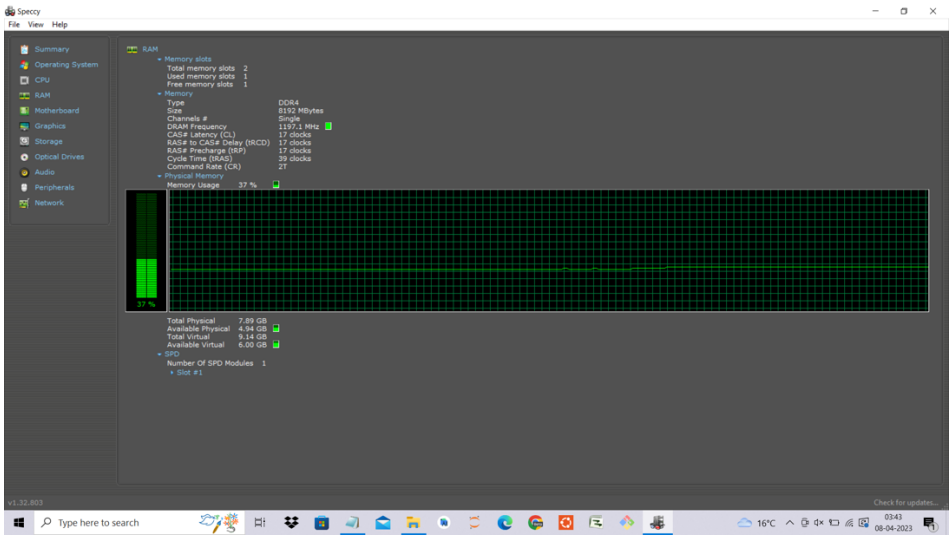

Fig. 2.3 description of RAM data

The "RAM" section tells you how much RAM space there is on your computer. The number of total used and free memory slots will be shown so you know how much storage space you are using. The frequency, size and type of system RAM will be listed under the "Memory" drop-down list.

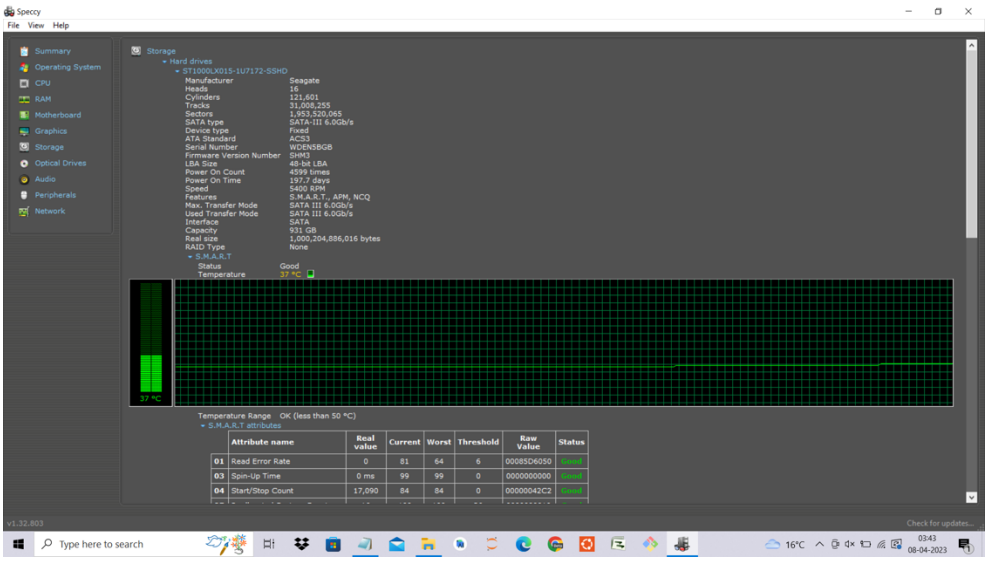

Fig. 2.4 storage description of the disk.

The percentage of memory you are using will be next to the "Memory Usage" label under "Physical Memory". The technical specifications of the machine are available on the "Motherboard" tab: BIOS, voltage, PCI data, etc. Basic data about the connected monitors

will be listed in the "Graphics" section: monitor height, width, resolution, etc. If you have graphics cards synchronized, then you can show statistics: manufacturer, ID, etc.

2.1 TARGET SYSTEM DESCRIPTION:

The target system description should have a supported operating system and other peripherals. The system should have various hardware components such as CPU, GPU, RAM, and storage devices. The target system's specifications and capabilities should meet the minimum requirements for the open-source software used in the project.

2.2 ASSUMPTIONS AND DEPENDENCIES:

The project assumes that the target system is properly configured and has the software compatibility. It is important to consider the Hardware recognition, operating system configuration with administrative access to ensure accurate and complete information is displayed.

2.3 FUNCTIONAL & NON-FUNCTIONAL DEPENDENCIES:

The project depends on the availability of the open-source software used to collect and display system hardware and operating system information. It also depends on the availability of hardware monitoring software and tools to collect and display real-time data on hardware component temperature and current usages.

CHAPTER-3 ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND ANALYSIS REPORT

In this report we are going to analyse how to use an open source software “speccy” to display an overview of all hardware and operating system details and live monitoring of temperature of the device. The steps to perform this analysis are

STEP-1: Download and install Speccy:

The first and foremost step is to download and install the Speccy software. It can be downloaded from the official website of Piriform.

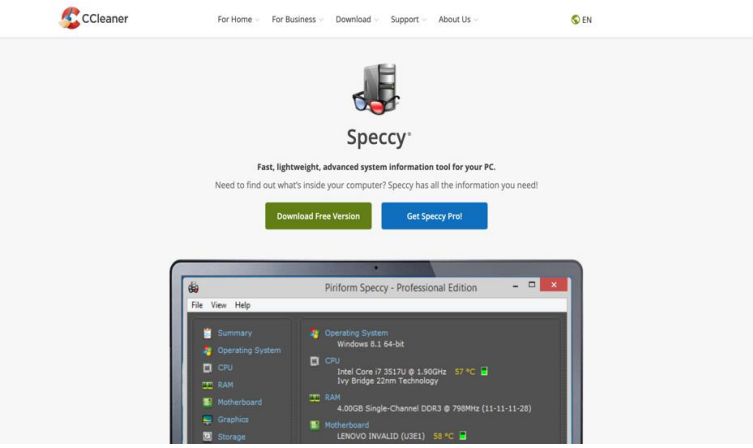

Fig. 3.1 official site of Piriform to download speccy.

STEP-2: Launch Speccy:

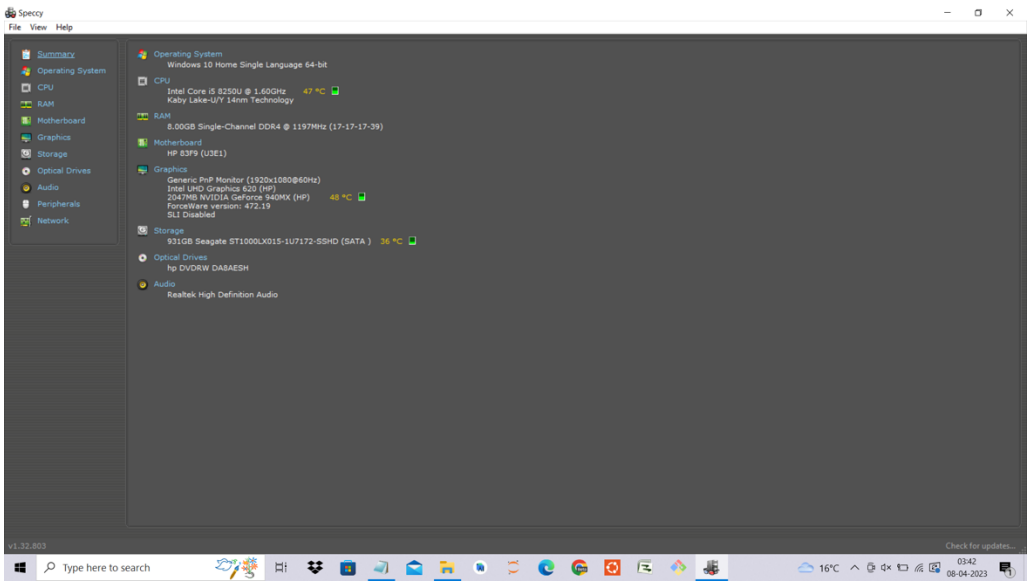

Fig. 3.2 the view of software after launching.

After installing the software, launch Speccy by clicking on its desktop shortcut or from the Start menu. Once the software is launched, it will display the summary of your system's hardware configuration. This includes details such as CPU, RAM, motherboard, graphics

card, hard drives, and other peripherals. To view detailed information about each hardware component, click on the relevant tab in the left sidebar of the software.

STEP-3: View Operating System Details:

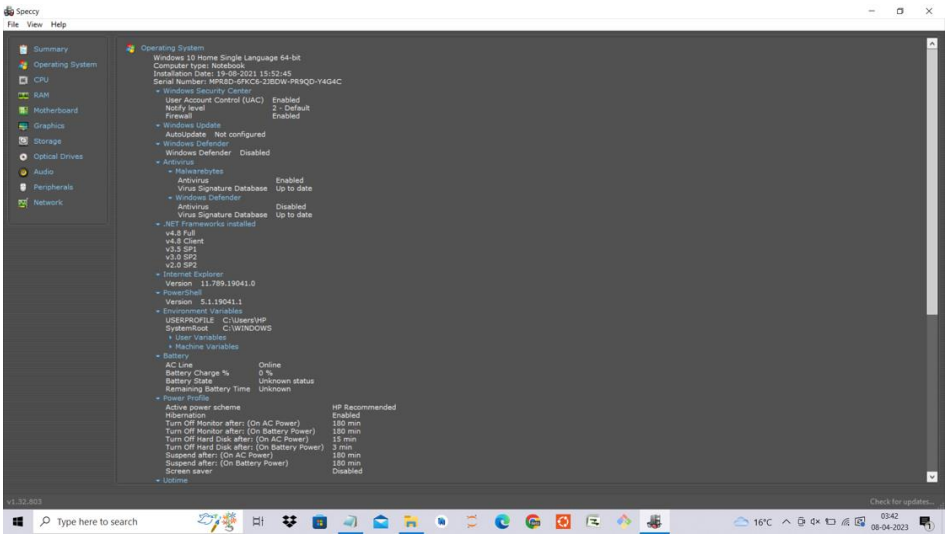

Fig. 3.3 details of the operating system on which the software is installed.

To view the operating system details, click on the Operating System tab in the left sidebar. This will display the version of the OS, the type of processor architecture (32-bit or 64-bit), and the amount of free and used disk space.

STEP-4: Live Monitoring of Temperature:

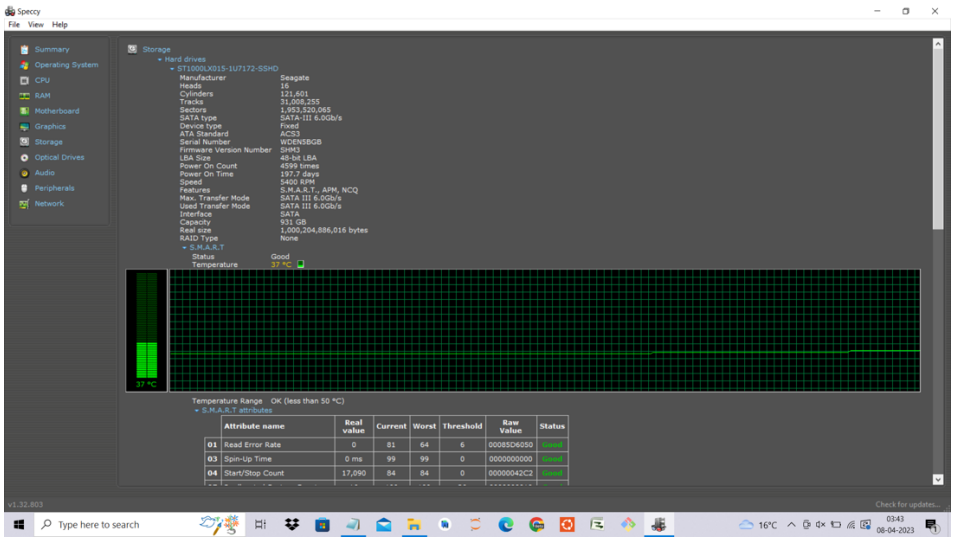

Fig. 3.4 temperature monitoring of different cores of processor

Speccy also provides live monitoring of the system's temperature. To view the temperature, click on the relevant hardware component tab, such as CPU, GPU, or hard drive. Once you have selected the hardware component tab, Speccy will display the current temperature of that component. It also provides a graph of the temperature over time, which can be useful for monitoring the temperature trends.

In addition, we can customize the temperature units (Celsius or Fahrenheit) and set temperature thresholds for each component.

CHAPTER-4 CONCLUSION

Disk forensics requires specialized skills, tools, and techniques to ensure that the data is collected and analysed accurately, and the evidence is admissible in court. Overall, disk forensics plays a crucial role in modern-day investigations, helping investigators to uncover evidence and build a case. With the increasing use of digital devices and storage media, disk forensics has become a valuable tool in law enforcement and legal proceedings. The field is constantly evolving, and forensic professionals must stay up-to-date with the latest techniques and technologies to ensure that they can effectively investigate and analyse digital data from storage devices.

REFERENCES:

- https://www.geeksforgeeks.org/cyber-forensics/
- https://filehippo.com/download_speccy/
- https://www.ecsbiztech.com/disk-forensics/
- https://www.cyberforensics.in/
- https://evestigate.com/disk-drive-forensics/
- https://resources.infosecinstitute.com/topic/linux-and-disk-forensics/