Logo, company name

Description automatically generated

Concordia Institute for Information System Engineering

(CIISE)

**INSE 6610**

**Cybercrime Investigations**

**Project Plan**

**Survey and Compare the use of Software and Hardware tools in Cybercrime Investigations.**

Submitted to:   
 **Professor Dr. Ivan Pustogarov**

Submitted By:

|  |  |
| --- | --- |
| **Student Name** | **Student ID** |
| Bhavya Panner Selvam | 40205936 |
| Pooja Polampalli | 40217185 |
| Saumya Yadav | 40224051 |
| Yattan Sikka | 40221072 |
| Amukthamalyada Vellanki | 40222749 |
| Priya Meghana Raavi | 40221227 |
| Himani Rajput | 40167840 |
| Mirza Alvin Salvin | 40198142 |
| Simran Gujral | 40221481 |
| Srividya Poshala | 40192542 |

**ABSTRACT**

Cybersecurity is the activity of preventing unwanted access and cyber-attacks on IT networks and sensitive data. Any digital product, including third-party software, has a chance of being vulnerable to a cyber-attack. To stop cybercriminals from taking advantage of these solutions' flaws, cybersecurity techniques work to fix all of their issues. Cybersecurity is crucial since it guards against theft and destruction to many types of data. In this project, we've covered a few technology-related hardware and software tools that might be used in an investigation or that could be helpful in locating and analysing electronic evidence and have given a general overview of them. We've given a succinct summary of the purpose and value of these tools. The reader is urged to utilise their imagination and think of all the potential investigative uses of the device as we have also attempted to illustrate how these tools aid in the commission of crime. There are numerous hardware items that can be utilised to commit cybercrime. Here is a list of these devices: Access control, tools for preventing credit card fraud, data storage, digital cameras, keystroke monitoring, and sniffers. Forensic evidence from mobile devices, such as call logs, contact lists, media files, geolocation information, and data from various loaded apps, can all be used in cybercrime investigations. In accordance with NIST, there are five stages of mobile forensic techniques: manual extraction, logical extraction, hex dumping/JTAG, chip-off, and micro read data. Here, we'll examine numerous tools for analysing cybercrime, including ADB (Android Debugging Bridge), the SQLite DB browser, Autopsy, and Oxygen Forensic. Open source Network Forensic Analysis Tool (NFAT) for Windows, NetworkMiner for Linux, Mac OS X, and FreeBSD. Using NetworkMiner as a passive network sniffer or packet capture device is a great approach to find active systems, sessions, hostnames, open ports, etc. without alerting the community. Additionally, NetworkMiner can decode PCAP files for offline analysis and regenerate/reassemble sent files and certificates from PCAP files. A network protocol analyzer, such as Wireshark, is a programme that records packets from a network connection, such as one connecting your computer to your home office or the internet. The most popular packet sniffer worldwide is called Wireshark. Wireshark performs three tasks, which are packet capture, filtering, and visualisation, just like any other packet sniffer. There are various applications for Wireshark, one of which is performance troubleshooting on networks. Wireshark is frequently used by cybersecurity experts to trace connections, see the content of questionable network transactions, and detect surges of network traffic. Nmap is a tool for obtaining data that is used in recon and reconnaissance. Basically, it transmits packets and examines the response to scan hosts and services on a computer network. Nmap enables you to scan your network and find out not only what is connected to it but also a range of details such as what services each host is running, how many hosts are connected, and so forth. Numerous scanning methods are supported, including UDP, TCP connect, TCP SYN (half-open), and FTP. A vulnerability in cybersecurity is a flaw that could be used by cybercriminals to break into a computer system without authorization. Acunetix is an automated tool for assessing the security of web applications, auditing your web apps for exploitable flaws like SQL Injection and Cross-Site Scripting. It examines any HTTP/HTTPS-enabled website or online application that may be accessed through a web browser. A remote security scanning application called Nessus checks a computer and alerts you if it finds any flaws that could allow criminal hackers to access any computer you have connected to a network. Nessus is a fantastic tool for helping domain owners keep their systems free of the simple flaws that viruses and hackers frequently try to exploit. To successfully and efficiently enter the digital crime scene during a cybercrime investigation, the proper information must be matched with a variety of tactics and technologies. Once you have all you need, you can carefully evaluate the data, look into the underlying causes, and find out who is responsible for various sorts of cybercrime. Additional technical research can be conducted to compare various investigation tools, their effectiveness, and their unique strengths, which will ultimately aid developers in selecting the best WVS for each online application.