Logo, company name

Description automatically generated

**INSE 6610 – CYBERCRIME INVESTIGATIONS**

**Project Plan**

On

***Project 1, SRVEY1***

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

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

Submitted By:

*Group 9*

|  |  |
| --- | --- |
| **Student Name** | **Student ID** |
| Raghavendran Raghunathan | 40220965 |
| Arun Prasad Karunanithi | 40220964 |
| Hari krishna Anala | 40190097 |
| Sree Satya Vanka | 40197072 |
| Venkatalaxmi Sai Durga Gadde | 40197076 |
| Abdul Aziz Midthuru | 40163297 |
| Nethra Sri Tangootor Balaji | 40229233 |

**Abstract**

With advancement in technology, crime has not been limited to traditional crimes. The 21st century has been characterized by massive innovations that have led to various ways the people interact. Cybercrimes have been growing progressively with development of newer and sophisticated technologies day by day. It has become an escalating concern in today’s digital age where effective investigation techniques are required to combat cybercrimes. Digital forensic tools are used to identify and analyse cybercriminals. Cybercrime attacks can be of different types. Some of the common types of cybercrime attacks are: Hacking, Denial of Service (DoS) attacks, Software piracy, Phishing, Spoofing. When a cybercrime occurs, the attacker leaves a trace which indicates some kind of significant information such as the date and time of attack or tools used to commit that crime. The cybercrime investigator then needs various tools to match the crime and criminal using the evidence left. These cyber-forensic tools are utilized in recovery of data and investigation of the crime by collecting the evidence from devices such as computers or mobile phones. Digital evidence in which information is stored in digital devices like phones in emails, images can be used in courts. There should be proper precautions taken while handling the digital evidence. Authenticity can be questioned as there is a chance of modifying the data in a digital device.

This aim of this project is to conduct a comprehensive survey and perform comparative analysis of different software and hardware tools used in cybercrime investigations. This study outlines the critical role of software tools like digital forensic software, network forensic tools, memory forensic tools, malware analysis tools and log analysis software. The project also covers the thorough understanding of significance of hardware tools like write blockers, hardware imagers, network capture hardware and GPS tracking devices. As this field of cybercrime is evolving, the knowledge on effective integration of tools is required to combat digital or cyber threats by cyber security professionals and law enforcement agencies. The analysis of various forensic tools mentioned in this report can be used to assist the investigators in selecting the appropriate tool.