Emerging Trends in Hardware and Software Cybercrime Investigation tools.

# The role of digital forensics in combating cybercrimes

Introduction-

Unquestionably, information and communication technology (ICT) has advanced significantly during the past few decades. Numerous advantages have resulted from cyberspace's development into a very effective communication tool. The majority of our activities have shifted from the real world to the virtual one, where cyberspace is the operative word. This is evident in real-world applications like e-commerce, e-learning, e-banking, etc., which have greatly sped up and simplified most processes. The benefits of cyberspace are undeniable, but there is a very dark side to its use, namely security issues. Cyber-attacks have been seen as a quickly evolving trend in this complex domain since the beginning of cyberspace. These attacks, which are typically referred to as cybercrimes, can range from simple email stalking to more complex crimes or cyber-terrorism. In response, certain security measures have been put in place to guarantee the security of cyberspace.Computer anti-malware programmes have been made available by several software development firms in an effort to stop and handle security breaches. Security breach is the sole cyber-generated worry, notwithstanding the good function that anti-malware plays in safeguarding our computer systems. The investigation of cybercrime is one of the complex risk concerns in cyberspace.In this context, digital forensics, a relatively new idea, has evolved to deal with cybercrime investigation difficulties as well as other legal processes.

Digital Forensics-

In its simplest form, digital forensics may be described as the legal process of applying forensic scientific disciplines to electronic-based crime scenes. The idea of forensic sciences has been in use for a while, but its digital forensics equivalent has just lately emerged as a noteworthy field of study. The enormous volume of publications on digital forensics over the past few years makes this obvious. This is especially relevant given the extraordinary increase in terrorism and cybercrime that we are currently seeing. For organised criminal organisations and individuals, cyberspace has developed into a particularly fruitful environment for targeting a range of targets using various techniques. Therefore, it is quite appropriate to look into how digital forensics might be used to fight cybercrime.

The main principles of digital forensics are applied with the following areas:

Identification

Acquisition

Preservation

Examining and analyzing

Presentation

Tools Used for Cybercrime Digital Forensics:

Memgator- MemGator is a memory interrogation programme that, as its name suggests, automates the extraction of data from memory files and compiles a report on the extracted data [26]. MemGator combines many memory analysis tools, including the Volatility Framework and PTFinder, into a single application. Data about memory information, processes, network connections, virus detection, passwords and encryption keys, and the registry may all be retrieved.

First on Scene-A visual basic script called FoS creates an evidence log report in conjunction with utilities like LogonSessions, FPort, PromiscDetect, and FileHasher. Forensic investigators need log reports to be successful in their investigations.

Galleta-The Galleta tool is adept at looking through cookies that are connected to surfing histories. These files include information about recently visited websites and the locations where cookies are stored.

Ethreal-Ethreal is a network security tool for sniffing incoming and outgoing packet information. Although this tool is helpful, it is vulnerable to encryption codes that impair its functionality.

Nmap-A network security programme called Network Mapper, or NMap, works by scanning a distant workstation for any open ports. NMap has the capacity to conceal its nature from the source computer so that it won't raise any red flags about a malware assault.

# Development of a cybercrime investigation simulator for immersive virtual reality

Introduction-The requirement for high-quality Virtual reality (VR) rendering has finally been realised in recent years because to improvements in computer technology and cell phones. This has made it possible to expand VR simulator instruction into intriguing new sectors. Training for novice police officers in crime scene investigation is one of these newly discovered fields. It spares the inexperienced cops the risk of tampering with actual crime scenes while they are being trained. The project's goal is to develop a technical prototype that will help with the transition of the present desktop-based Virtual Crime Scene Simulator to immersive VR.

What is it and how does it function-

The major goal is to investigate how the existing Virtual Crime Scene Simulator (VCSS), created by University College Dublin, may be transformed into an immersive Virtual Reality simulator as it only now operates on a desktop. In order to instruct unskilled law enforcement agents looking into a crime scene, a realistic and sophisticated scenario was created in the simulator. According to a study conducted in August 2014, it had gotten commendable feedback from instructors and trainees and was regarded as useful.It can be much improved, yet it still has its limitations. For instance, to imitate a real-world setting when officers are under a lot of pressure, a more immersive experience is needed. Therefore, the next natural improvement to the system would be to include virtual reality technology. Even when created on a tight budget, previous VR worlds were expensive. Due to its built-in support for SteamVR, the HTC Vive was selected as the main platform among the available virtual reality headsets. Unity, the game engine used in the creation of VCSS, is supported by SteamVR SDK. It may therefore smoothly transform the present system into virtual reality.

# Windows Forensic Investigations Using PowerForensics Tool

Introduction-New methodologies and procedures are needed to conduct digital forensic investigations that involve the extraction, analysis, and reporting of digital evidences. PowerShell is one of the techniques used while performing digital forensics on a Windows operating system. This article will demonstrate how PowerShell may be used to gather forensic evidence from a Windows operating system, even though it is often used to setup, manage, and administer the Windows operating system and other installed programmes. This article will describe Windows PowerShell functionalities and how a digital forensic investigator might benefit from them. The paper will also concentrate on the programmes and tools designed especially for forensic investigations. The PowerForensics programme will then be used in digital forensic tests to extract and recognise various Windows forensic artefacts. The PowerForensics tool's abilities to retrieve forensic evidence from the Windows operating system are demonstrated, along with some of its limitations.

What is it?

Any methodology or procedure used to retrieve evidence from the Windows operating system is known as "Windows forensics." Investigations of the Windows operating system have shown significant cause for worry since, as of May 2016, 87% of client PCs have been running Windows. Having said that, there is a critical need for study on Windows operating systems. PowerShell is one of the technologies available for forensic investigations in a Windows OS environment.In order to gather, acquire, and analyse digital devices and systems correctly and effectively to produce accurate findings, the investigator must have a thorough understanding of the technology being employed. Therefore, gaining knowledge about Windows artifacts will help investigators when analyzing suspect's computers that are running a Windows operating system.

It is divided into five categories-

General Machine Information-This category includes machine name, network addresses and OS information.

User Account Acitivity- User activity artifacts include a variety of information, including login timings, login status, and whether the login was successful or not. Additionally, it is possible to determine if the login occurred remotely or via the console (direct access to the system). Additionally, each user profile may extract information about the user's security identification (SID), profile root directory, and other details.

Folder/File Activity-This type of artifacts related to all the events that have occurred on files and folders from access activity to the file until action event such as copy, move, rename and delete. Furthermore, all links and shortcuts such as. LNK files and Jumplists are related to this category.

Program- Program details, history and cache are good artifacts which can provide more information about user behavior and intention.

External Storage Device- External storage devices are one of the very important sources that are used for data leakage. These artifacts should be taken into deep consideration for most investigations. This is why, there is a special category of these artifacts