**NIS Project**

Introduction:

Due to the rising incidents of cyber related attacks, there is an ever increasing demand for solutions that cater to different attacks and offers detection, mitigation and prevention and response in real time. Recent attacks mostly focus on infecting and spreading malware and therefore anti measures must be taken before or at least at the earliest.

Memory Forensics:

Memory forensics refers to the reverse engineering of malware and more specifically malicious files and its forensic analysis of the memory dump of the computer. Advanced malware which contain malicious files often hide the data in memory rather than leave traces on the hard drive which can be detected comparatively easily. The dump is taken of the memory (RAM) and analyzed using tools such as Volatility.

Volatility:

Volatility is free and open source software developed by The Volatility Foundation. The latest version of the software is Volatility 3.0 named Volatility3 which is developed using the python programming language. Volatility framework is primarily used for extracting digital artifacts from volatile memory (RAM) samples. In our example, we will be analyzing the famous malware, ‘Stuxnet’ which was used to target and manipulate the speed of centrifuges.

Stuxnet

Stuxnet was a computer worm which was primarily spread through the use of usb drive and contained a rootkit, link file and the worm which contained the original payload to launch the attack which exploited the zero day vulnerabilities in programmable logic controllers (PLC) manufactured by Siemens.

**Related Work:**

A particularly effective memory forensics tool is volatility. It is used to extract data from Windows, macOS, and Linux system memory images (memory dumps). A sizable community also creates third-party plugins for volatility. We employ volatility for memory forensics since we absolutely want to include memory capture and analysis in our investigations.In the paper[1], authors performed the comparisons of tools in memory forensics because effectiveness of the memory acquisition tool is a major factor in memory acquisition success. In this paper, memory forensics methods are compared in terms of processing speed and residual artifacts in volatile memory. In addition, they looked at how different volatile memory sizes affect the processing times of the tools. They employ the tools FTK Imager, Pro Discover, Nigilant32, Helix3(dd), OSForensics, and Belkasoft RAM Capturer to carry out this task. Belkasoft RAM Capturer has the lowest processing time and the fewest remaining artifacts, according to the results. Additionally, this study comes to the 95% confidence level conclusion that the evaluated tools are considerably different based on left-over artifacts in the volatile memory. Additionally, if the size of memory increases it does not affect the processing time of the tools.

In reviewing the paper [2],Volatility is a framework that is used worldwide to analyze the RAM of computers by many investigators. Currently, Volatility only has a command line interface, which may make it difficult for some investigators to utilize the application. In this paper, they introduce a GUI and extensions for the Volatility Framework that, while making the tool's use easier, also provide extra functionality, such as the ability to store results in a database, create shortcuts for lengthy Volatility Framework command sequences, and create entirely new commands based on the correlation of the database’s data.

Using conventional methods in [3] to analyze memory forensics is quite effective for basic malware but not for advanced malwares. In this paper, a Virtual Machine introspection technique is suggested as the possible solution as it is more effective. Using memory forensics, the detection rate of Microsoft Office documents, portable document format files, and executable files being up to 90%. However, the detection rate of script files is only 75%, because process and network activities quickly vanish in volatile memory. In this paper, the solution to this problem is given by using memory forensics timing, frequency adjustment, and other heuristic methods. This method overcomes the problem of high dependency on VM hypervisor types, as it is an agentless solution that supports many VM hypervisor types.

On analyzing [4], authors presented conventional methods are effective when detecting and analyzing dead forensics and typical computer forensic methods but cannot detect live forensics which also reveals much more information comparatively. Malwares that runs entirely on memory or RAM extract information such as passwords, encryption keys, network activity and are hard or almost impossible to detect and for this reason a solution is required. In this paper, a signature based artifact identification is done using keywords and default hex values. Using memory forensics; investigators can identify various potential artifacts in efficient manner with creates fewer traces on actual hard disk.

While viewing the paper [5] we find out that author’s vision is that a computer's memory dump is subjected to forensic investigation in memory forensics. Computer memory also referred to as volatile memory or random access memory contains a plethora of system information, such as process activity, network connections, etc., that may disclose a lot about the actions of the system's user. Criminals frequently use technology that avoids recording any evidence on permanent storage media and instead launches their assault through volatile memory due to the widespread adoption of digital forensics for investigation. Memory forensics is therefore acknowledged as a component of incident response procedures for inquiry and it is continually changing. The Onion Router (Tor), live CD/USB, portable browsers, virtualization, and other online crimes were highlighted as we reviewed various memory capture tools and approaches.The goal was to examine the development of the memory forensics framework currently in use for cases involving the dark web and anonymous networks, as well as to identify the difficulties currently facing investigators of these types of cases.

By doing the literature review paper of [7], authors present that hacking is a serious issue in today's environment. Hackers can do it for pleasure or for nefarious purposes.In 2008, the FBI estimated that Internet fraud had cost 264.6 million dollars. Investigating computer crime is therefore one of the most difficult tasks at hand today.The efficiency of the memory acquisition instrument is a key factor in memory acquisition success. In their article, memory forensics methods are compared in terms of processing speed and residual artifacts in volatile memory.In addition, they looked at how different volatile memory sizes affect the processing times of the tools. there employ the following tools to carry out their work: FTK Imager, Pro Discover, Nigella32, Helix3(dd), OSForensics, and Belkasoft RAM Capturer.Belkasoft RAM Capturer has the lowest processing time and the fewest remaining artifacts, according to the results. Additionally, this study comes to the 95% confidence level conclusion that the evaluated tools are considerably different based on left-over artifacts in the volatile memory.

Here is the Comparative Analysis between our paper and above mentioned papers:

**WorkFlow Diagram:**

