ISSN 2063-5346

FORENSIC ANALYSIS ON WINDOWS PAGE FILES

Dr. Priya P. Sajan*, Udisha Gupta, Shubham Sharma**, Chandra Mani Mishra****

Article History: Received: 01.02.2023 **Revised:** 07.03.2023 **Accepted:** 10.04.2023

Abstract

This project aimed to conduct a forensic investigation and produce a comparative report on a page file in a Windows-based system. Memory dumps can provide valuable artifacts with information that can be extracted. The drive contains files such as pagefile.sys, swapfile.sys, and hiberfil.sys, each containing pieces of memory. For this project, pagefile.sys was selected for forensic analysis. Analyzing pagefile.sys can reveal sensitive information like user IDs, passwords, hidden processes, downloads, and browser search activity. A forensic expert can use this information to extract more valuable information in the memory analysis field.

Keywords : Page-File, Memory dumps, Data extract, Hidden files, Forensic tools.

*Senior Project Engineer at Centre For Development Of Advanced Computing (C-DAC),

Thiruvananthapuram, Kerala, India, Emailid : priyasajan@cdac.in

**PG-Diploma in Cyber Security and Forensics, Centre For Development Of Advanced Computing (C-DAC), Thiruvananthapuram, Kerala, India

DOI: 10.31838/ecb/2023.12.s1.098

Introduction

Page File is a file that is used by Microsoft Windows to store frames of memory that do not currently fit into physical memory. It also referred to as a swap file or virtual memory. As we use different programs and perform different functions on your computer the page file may end up containing all sorts of potentially sensitive or confidential information. Event log records, like other types of data, can potentially be stored in the Pagefile or unallocated space on a computer system.

Page file analysis with different artifacts using different tools became extremely beneficial for an investigation. Page File is a hidden system file in windows system. The page file is located in the root of the system drive (usually C\:), with name pagefile.sys, but it can be moved to a different drive or partition. By default, it is set to be 1.5 times the amount of RAM installed on the system, but this can be adjusted manually. Windows manages the page file automatically, but advanced users can adjust settings such as the initial size, maximum size, and location of the page file. Windows Page File is used as a virtual memory in the system and it contains some attributes or information about recent data. While recovery or collecting of data all types of data can be extracted through data carving tool. Page file analysis can be done by Data carving tool. Memory dump tools can be useful for page file analysis.

Forensic Analysis on Pagefile

I. What type of data contains by a Pagefile :

- Page data: When a program requests memory that is not available in physical RAM, the operating system temporarily moves some data from RAM to the page file, creating free space in RAM for the application to use. This data includes parts of the program's code and data, as well as any other data that is currently stored in RAM but not being actively used.
- Page directory: The page directory is a data structure that maps virtual memory pages to physical memory pages. It is used by the operating system to manage the mapping between virtual memory and physical memory. The page directory is stored in the page file, so that it can be quickly accessed when needed.
- Page table: The page table is another data structure that is used to manage the mapping between virtual memory and physical memory. It contains entries that map virtual memory pages to physical memory pages. The page table is also stored in the page file.
- System crash information: When the system crashes, Windows may write information about the crash to the page file. This information can be used to diagnose the cause of the crash and determine what actions need to be taken to prevent it from happening again.

II. Tools foe Forensic Pagefile Analysis : We used FTK Imager tool and Belkasoft Evidence Centre X tool and Performance Monitor tool to analyze page file artifacts.

FTK Imager tool is used by forensic investigators to acquire and analyze digital evidence from various sources, including hard drives, USB drives, and memory cards.FTK Imager can be used to verify the integrity of a forensic image. It can compare the hash value of the original storage media with the hash value of the forensic image to ensure that the image is an exact copy of the original media.

Belkasoft Evidence Center is a powerful digital forensic tool that can be used to acquire, analyze, and extract data from various sources. Its capabilities make it useful for both criminal and civil investigations, and it is widely used by law enforcement, government agencies, and digital forensic experts. It can generate reports in various formats, including PDF, HTML, and Excel. The reports can include information such as metadata, user activities, web history, and chat conversations. Belkasoft Evidence Center can integrate with other digital forensic tools and platforms, such as EnCase, Nuix, and FTK.

The Performance Monitor tool in Windows is a built-in utility that allows users to monitor and analyze the performance of their computer. The tool provides detailed information about various system resources, including CPU, memory, disk, and network usage, and can be used to identify performance bottlenecks, troubleshoot issues, and optimize system performance.

III. How to do an analysis of pagefile using these tools :

1. From File Menu select “memory capture”.Initiating the memory capture process is as simple as clicking on the "capture memory" button, which will then begin the process of collecting the system's memory. Once the memory capture is complete, the resulting memory dump and page file will be automatically saved to the designated destination folder.

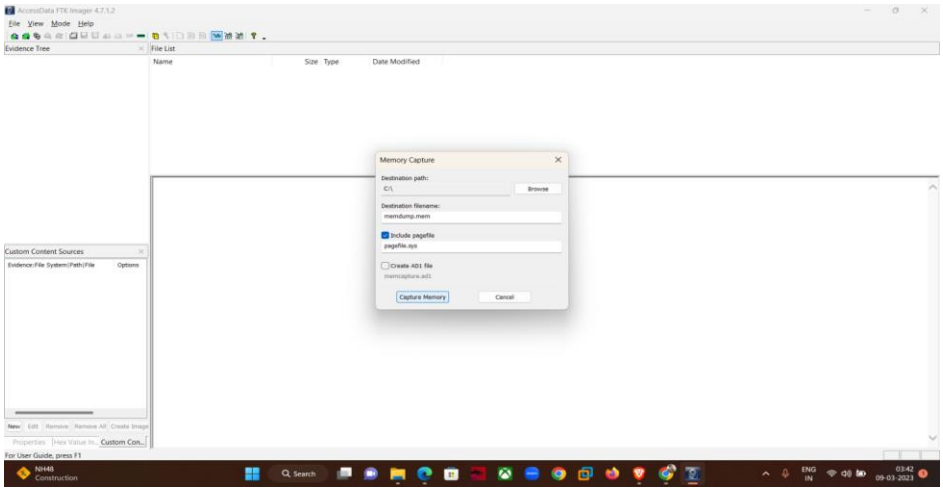

Figure 1.1.Image of FTK imager

This allows digital forensic investigators to analyze the captured data for evidence of malicious activity, such as malware infections or unauthorized access attempts. By carving out these specific files from the captured memory, investigators can better isolate and analyze key pieces of information, which can ultimately help them uncover the root cause of a security breach or other digital incident.

- From File menu select “Add new evidence”. Select “source” then browse a memory dump file.

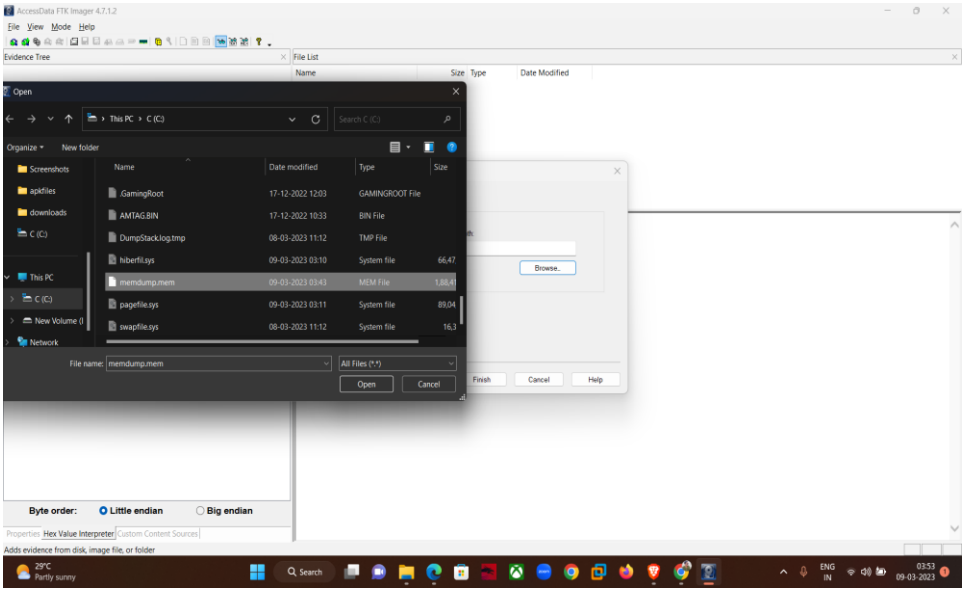

Figure 1.2.Select a file

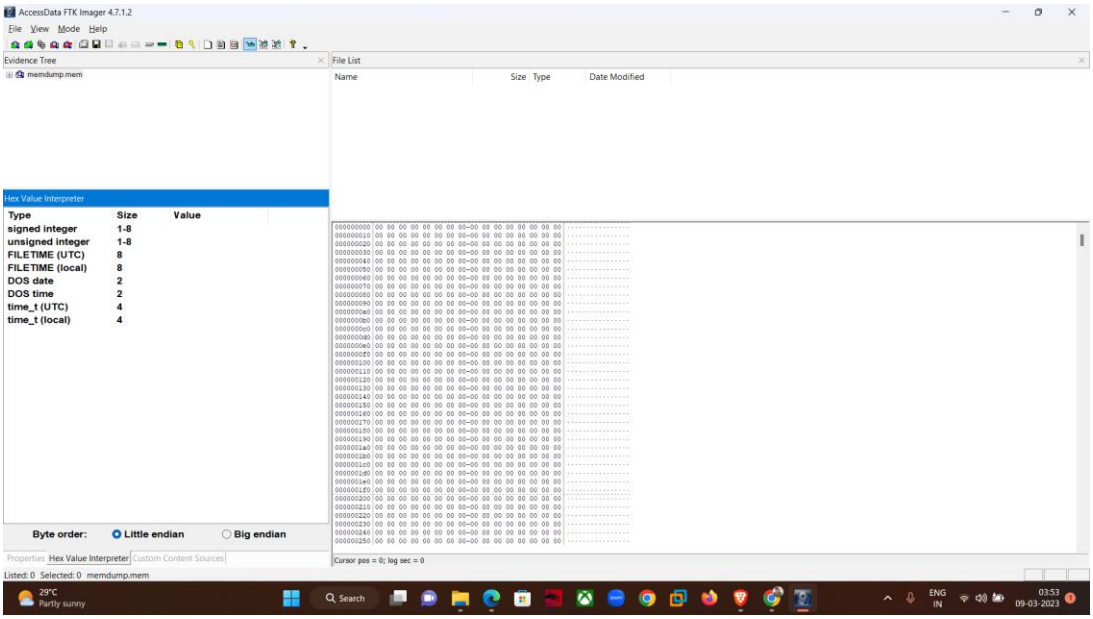

Figure 1.3. Information about file type, size, date modified, name etc.

2. When conducting digital forensics investigations, we often rely on memory dump files to capture volatile data from a system. Once we have obtained the memory dump file using a tool like FTK, we can then utilize specialized software such as Belkasoft Evidence Center X to perform a more detailed analysis of the data. This software is designed to provide additional insights into the memory dump file, allowing investigators to uncover a wider range of digital artifacts that may be relevant to their investigation. By leveraging this powerful tool, forensic analysts can more effectively and efficiently process large volumes of data, helping to speed up the investigation process and improve the accuracy of their findings.

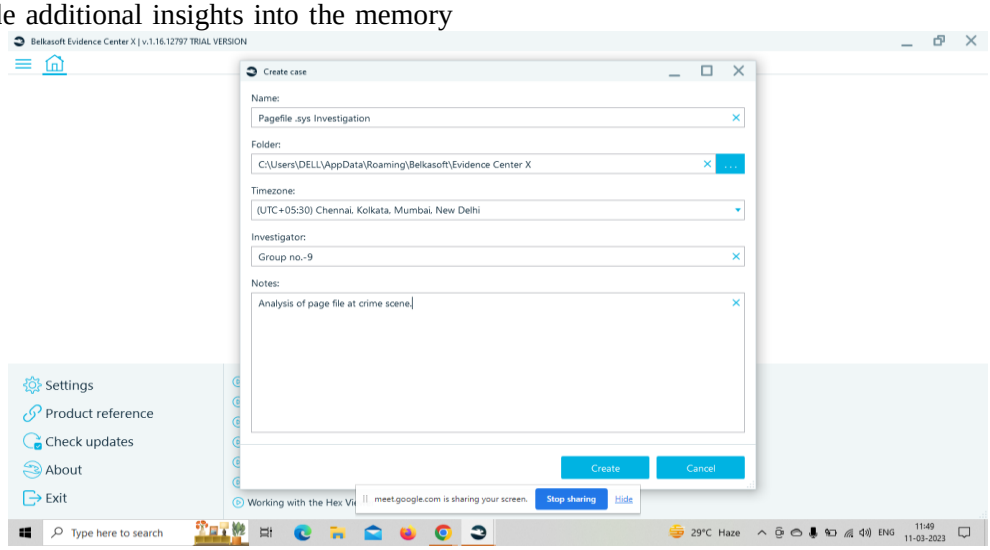

Figure 2.1. create a case file in Belkasoft evidence centre x tool

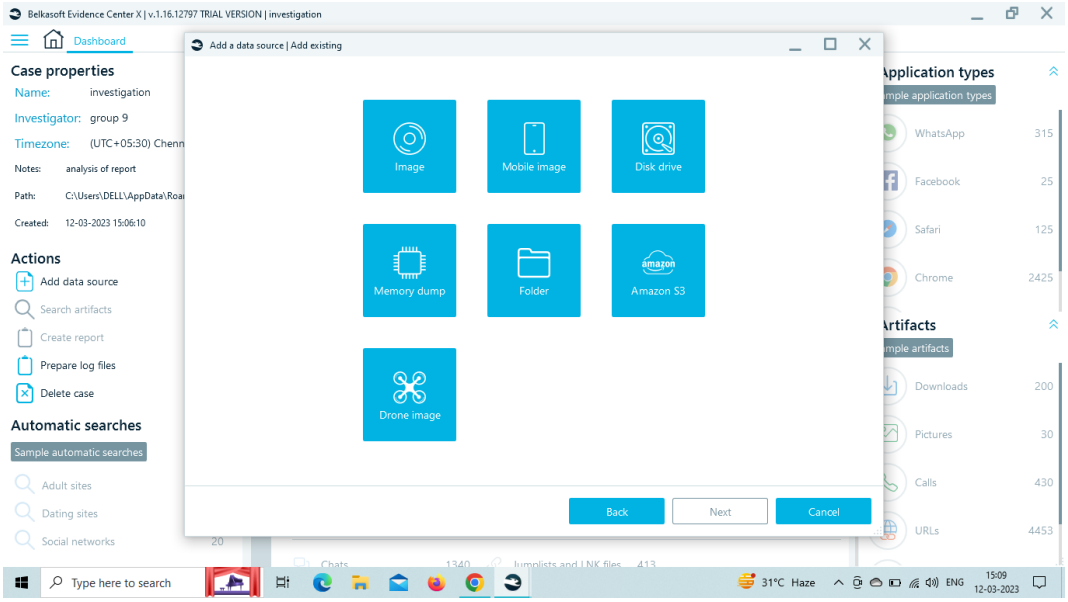

Figure 2.2. Select the source which we have to analyze.

- It gives us too many artifacts and filters so that we can analyze the evidence as per our requirement. Ex - URL, emails, pictures, other files, system files etc. (data carved through FTK).

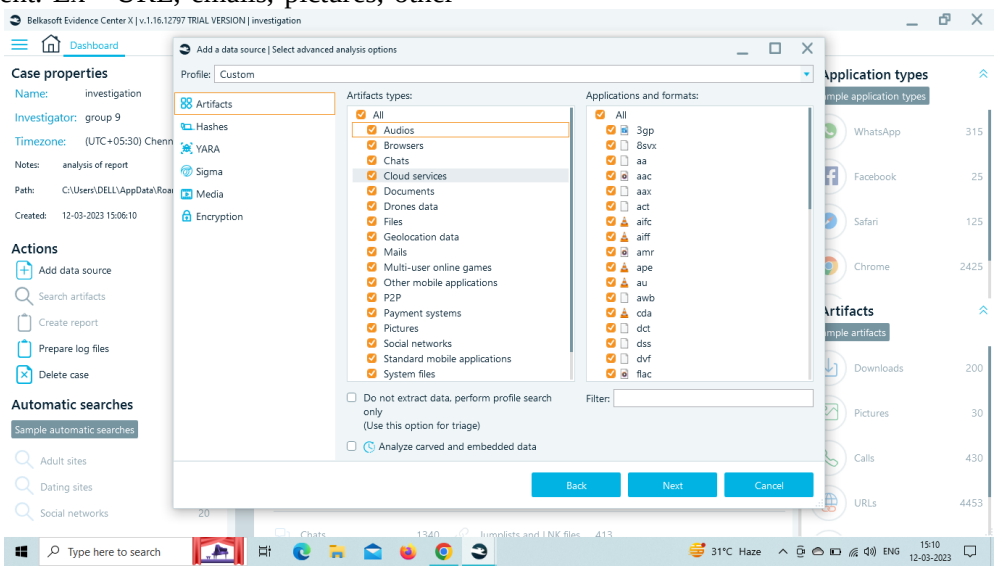

Figure 2.3. Image of artifacts and filters which we can use during investigation.

3. In search tab of windows type Performance Monitor. After that follows these steps that are shown in figure.

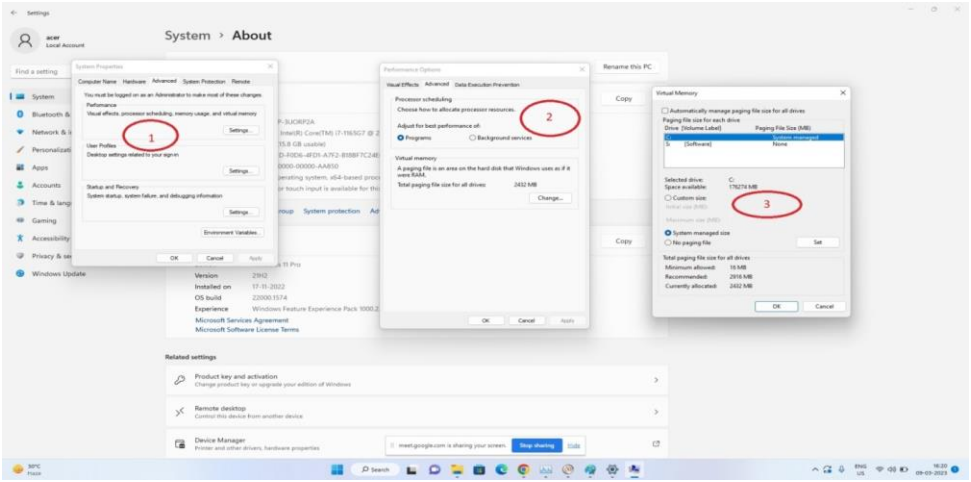

Figure 3.1. steps for doing analysis in performance monitor

- Performance Monitor is in-built tool in windows. It helps us to get information about performance, memory usage, speed, committed memory (RAM + Pagefile), etc. This tool is useful to know about malware existence in system.

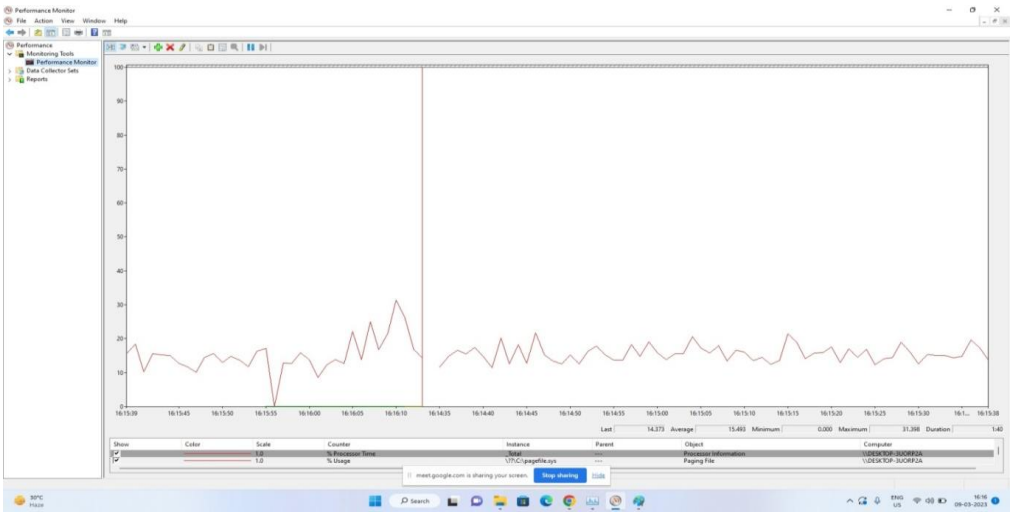

Figure 3.2. Image of Performance Monitor.

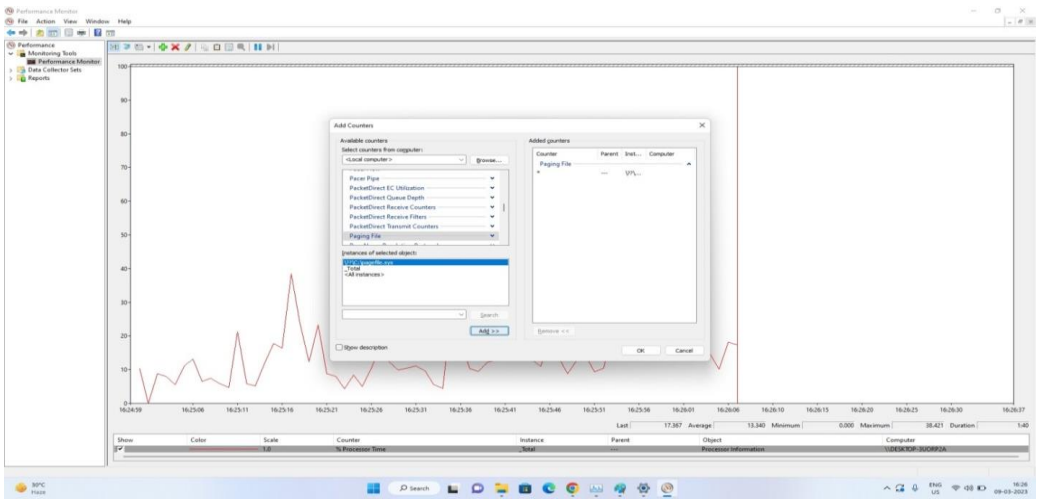

Figure 3.3. From the Available counters list, select paging file. Select % Usage under Paging File and then click the Add button to add the counter on the Added counters list

CONCLUSION

In this report we get detailed information about Page File, data which stored in page file, artifacts of data in pagefile, importance of pagefile in terms of investigation, data carving, data carving tools, page file analysis tools etc. A page file analysis with Belkasoft Evidence Center can provide valuable insights into the usage patterns and activities on a computer, and can be useful for a variety of purposes, including forensic investigations, security analysis, and data recovery. Ex. Url, recently viewed files, downloaded files etc.A page file analysis with Performance Monitor can provide valuable insights into system resource usage and help optimize system performance. It can be helpful to find existence of malware by showing rapidly increasing speed, memory usage, CPU performance etc.A page file analysis with FTK Imager can provide valuable insights into the usage patterns and activities on a computer, and can be useful for a variety of purposes, including forensic investigations, security analysis, and data recovery.

Page File Analysis plays an important role in Forensic Investigation. When it comes to analyzing the Pagefile.sys on a computer system, there are a wide range of tools and techniques available to digital forensics investigators.They all have different methods and different approaches.

While it may be possible to extract sensitive information from the Pagefile.sys, it is important to note that doing so can be a complex and challenging task. The Pagefile.sys is a system file used by Windows to manage virtual memory, and it may contain fragments of data from applications and processes that have run on the system. In some cases, this data may include sensitive information such as passwords or other confidential data. However, extracting this data requires specialized knowledge and tools, as well as a deep understanding of the structure and contents of the Pagefile.sys. Additionally, it is important to note that extracting sensitive information from the Pagefile.sys without proper authorization or legal justification may be illegal and can result in serious consequences. Therefore, while it may be possible to find sensitive information in the Pagefile.sys, it is important to do so only through proper and ethical forensic investigation methods.

FUTURE SCOPE

The future scope of a project that aims to conduct a forensic investigation and produce a comparative report on a page file in a Windows-based system can be quite extensive. Integrating the page file analysis tool with other digital forensics tools, such as file carving and memory analysis tools, can enhance the capabilities of investigators and make their work more efficient.The data contained within page files can be complex, and new forensic analysis techniques may be required to fully understand the data and its significance. Research into new analysis techniques, such as machine learning or data visualization, could prove valuable in future investigations. Similar techniques could be applied to other operating systems, such as Linux or MacOS. Digital forensic investigations often require close collaboration with law enforcement agencies. Developing strong partnerships with these agencies can help ensure that investigators have access to the latest tools and techniques and can help build a stronger case in court. It can lead to numerous research opportunities and collaborations with other professionals in the field.

REFERENCES

[1]. https://www.hackingarticles.in/forensic-investigation-pagefile-sys/

[2]. www.cyberforensics.in

[3]. https://github.com/matonis/page_brute

[4]. https://www.readkong.com/page/windows-nt-page-le-sys-virtual-memory-analysis-3658499

[5]. https://forensafe.com/blogs/pagefile.html

[6]. https://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-5/C016251116.pdf

[7]. https://ieeexplore.ieee.org/abstract/document/4426211

[8]. Forensic **analysis** of Window's® virtual memory incorporating the system's **page-file (pdf)**

JM Stimson - 2008 – Citeseer

[9]. Forensic **Analysis** of Window's (Registered) Virtual Memory Incorporating the System's **Page-File**

JM Stimson - 2008 - apps.dtic.mil

[10]. [PDF] Review of live forensic **analysis** techniques

S Rahman, MNA Khan - International Journal of Hybrid Information …, 2015 - academia.edu