"C:\ProgramFiles(x86)\Dr.Memory\bin64\dimemory.exe""C:\Users\ASUS\Downloads\Dumpit\Dumplt.exe". The main purpose of using DR.Memory is to look for syscall breakponts when the VSM is active.

DR.Memory managed to access the module "C:\WINDOWS\system32\ntdll.dll" after analyzing the module to make a breakpoint on the DumpIt tools. DR.Memory is only able to see the last breakpoint module, it is necessary to do a test analysis using dynamic code, namely Windbg. This aims to determine whether the last module in DR.Memory is the same as Windbg.

In Windbg dynamic code analysis can be executed by the operating system. This analysis can be obtained by following the steps, namely on the windbg preview menu we can select the "Start debugging" menu, then select "Launch Executable (Advanced)" from the DumpIt application, and the debugger downloads the "wntdll.pdb" symbol file. After that, on the "Command" page, do the following command:

- To load symbols:
1. .symfix
2. .reload
3. !analyze -v
- To run the DumpIt application
1. g

From this analysis it can be seen that the line code before the crash on the DumpIt application was code 80000003, and the last module accessed on the DumpIt tools read by Windbg was C:\WINDOWS\SYSTEM32\ntdll.dll. The line code before the crash can mean that this error is caused by some conflicting Registry files, this is due to missing drivers or related to incompatible hardware on which the program is running. This is because it can't process JIT_DEBUG_INFO, Win32 error 0n30, it's an error in missing driver i.e. C:\Users\ASUS\Downloads\DumpIt\DumpIt.exe;C:\MyProjects\DisplayGreeting\Debug, the file doesn't have the correct path more specific so that it causes a breakpoint on line code 80000003.

The effect that is obtained when Virtual Secure Mode (VSM) in the dynamic memory acquisition process is that it causes the screen to experience a BSOD when performing memory acquisition, so this is the effect that is obtained when VSM is active. The problem that was obtained because of VSM was a crash on the ntdll.dll module which was caused by a missing registry file in the Bug check analysis of this dump file showing the cause of the system experiencing BSoD, namely when executing the dumpIt.sys module

The results obtained for this study were able to find out what caused the system to crash and which code was experiencing BSoD compared to previous research only obtaining the ad_driver.sys module. Where the previous research carried out dynamic analysis using the windbg application that was executed, namely the FTK Imager, while in my research the application that was executed was DumpIt. In previous research, the last module obtained before the system crash was C:\Windows\system32\mssprxy.dll, while my research obtained the last module, namely C:\WINDOWS\SYSTEM32\ntdll.dll. So, my research was able to find the last code before the crash was located at a breakpoint in line code 80000003 which was caused by a file that didn't have a more specific path.

IV. CONCLUSION

The results of dynamic code analysis using the Windbg acquisition application are carried out when VSM is active. What is done to carry out live memory acquisition is that there are four tools used when carrying out memory acquisition, namely autopsy, isobuster, DumpIt, Magnet RAM Capturer. The tools that have successfully performed memory acquisition are autopsy, isobuster and Magnet RAM Capturer. While the tools that failed to do memory-acquisition, namely DumpIt, this was caused by several errors that caused a crash due to a Break Instruction Exception, with the name failure bucket ID being BREAKPOINT_80000003_ntdll.dll!LdeInitializeThunk. In this line code, it can be seen that the cause of the crash is located in an error caused by a registry file that is contradictory to execution and related to incompatible hardware. Whereas the last module accessed by Windbg was C:\WINDOWS\SYSTEM32\ntdll.dll, the file had an error in the Operating System where the file could not be executed because it crashed which caused the BSOD (Blue Screen Of Death) screen.

VSM is Windows 10 which is used to make managing the existing environment on the operating system to be safe, VSM itself is separate from the usual Windows environment. How the dumpIt tool works is a combination of win32dd and win64dd, combined into one executable. DumpIt will then take a snapshot of the host's physical memory and save it to the folder where the DumpIt executable resides. The impact caused by active VSM when conducting experiments on the Windbg application to acquire memory there is a crash located in the operating system which causes a BSOD (Blue Screen Of Death).

REFERENCES

[1]Parmaza , B. (2018). Apa itu Digital Forensics (Forensik Digital). *Komunitas Teknologi dan Komunikasi Jambi*.
[2]Aleksandar Milenkoski, D. P. (2021). *Virtual Secure Mode: Architecture Overview.* [Technical Report] ERNW Enno Rey Netzwerke GmbH.
[3]Anand, G. (2021). Windbg A-Complete Gide For Advanced Windows Debugging. *windbg a complete guide*.

[4]Arwidmark, J. (2015). Virtual Secure Mode (VSM) explained. *Enabling Virtual Secure Mode (VSM) in Windows 10 Enterprise Build 10130*.

[5]George, G., & Inani, S. (2018). *Learning Malware Analysis.* Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK.

[6]Irfan Febrian Editia Kurdiat, N. W. (2016). Analisis Proses Investigasi Dekstop PC Yang Terhubung Layanan Private Cloud. *Jurnal Teknik Informatika dan Sistem Informasi*.

[7]Michael Solomon, D. B. (2005). *Computer Forensics Jumpstart.* Alameda: SYBEX Inc .

[8]Rahevar, D. (2013). Study on Live analysis of Windows Physical Memory,IOSR Journal of Computer Engineering (IOSR-JCE). *IOSR Journal of Computer Engineering (IOSR-JCE)*.

[9]Riadi, I., Fadlil, A., & Hafizh, M. N. (2020). Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology. *Jurnal Pendidikan Informatika*.

[10]Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*.

[11]Cahyani, N. D., Jadied, E. M., & Ab Rahman, N. H. (2022). The Influence of Virtual Secure Mode (VSM) on Memory Acquisition. *International Journal of Advanced Computer*.