# NSPJ24 Memory Forensics

## Overview

System memory dump files play a crucial role in the field of information security. They can be utilized for troubleshooting and debugging, offering the capability to capture the state of a system during crashes. Additionally, dump files serve as essential tools for forensic analysis, enabling the identification of malware, hacker activities, or other security threats. Furthermore, they can be employed for data recovery, particularly in the face of critical data loss or ransomware attacks. Dump files also facilitate vulnerability analysis, assisting experts in discovering and patching vulnerabilities and weaknesses within systems. Lastly, they can serve as courtroom evidence for investigating and prosecuting cases involving computer crimes. Overall, system memory dump files are indispensable in safeguarding system security and mitigating risks.

## Task I (60%)

### Descriptions

Volatility is a powerful open-source memory forensics framework used for analyzing volatile memory (RAM) dumps. It provides a wide range of plugins and capabilities for extracting valuable information from memory dumps, making it an essential tool for digital forensics and incident response professionals.

One of the features of Volatility3 is its ability to extract the memory of a specific process. By analyzing its memory, we can determine if there is any malicious code present. In this section, we will use Volatility3 to track down potential malicious process in the dump file and identify their specific characteristics in memory.

### Implementation

1. Build *Volatility3* from the source code : https://github.com/volatilityfoundation/volatility3
   Validate the configuration of Volatility3 using the "-h" command:
   `python3 vol.py -h`

2. Obtain the memory dump file from target system
   We have prepared a memory dump file, so here we'll give a brief overview of how to obtain it, without the need for implementation.
   We are using KVM on Linux, and after creating a Windows virtual machine, we use the "virsh dump" command to obtain the memory dump file. Of course, there are other methods to obtain memory dump files, such as locally on the host system, in other virtual machine environments, or even after a system crash.
   MemoryDumpFile

3. Locate the suspected malicious process. (20%)
   Within the provided memory dump file, use Volatility3 to locate a fictitious malicious process named "Malicious.exe".
   Utilize the "windows.psscan" function in Volatility3 to enumerate all active processes.
   `python3 vol.py -f ~/path/to/your/dump/file windows.psscan`
   **Requirement**: Capture a screenshot of the command output used to find the fictitious malicious process.

4. Obtain the dump file of the suspected malicious process. (20%)
   After locating the malicious process using Volatility3, proceed to extract its memory file.
   **Hint**: Utilize the "windows.psscan" function , get more information by command:

```
python3 vol.py -f ~/path/to/your/dump/file windows.psscan -h
```

**Requirement**: Capture a screenshot of the command output used to dump the process memory.
Identify the malicious code segment within the process.

5. Identify the malicious code segment within the process. (20%)

   There is a fabricated malicious code segment labeled “Malicious Attacking” within the memory of the suspected malicious process.

   You can utilize tools capable of examining hexadecimal code, such as HexEd.it - Browser-based Online and Offline Hex Editing.

   **Requirement** : Capture a screenshot of the malicious code segment discovered within the process memory.

## Task II (40%)

### Descriptions

Within the same memory dump file, there is a message about this course “NSP “ in a process named “FakeNotepad.exe “.

Please follow the similar steps in Task I to extract the entire message.

**Requirement** : Capture screenshots step by step.

## Report

Screenshots of step 3, 4, 5 in **task I** and **task II**

## Submission

Please submit your report to E3 named MF_student_id.pdf, such as “MF_312551181.pdf “

For questions, contact TA Mr. Lai <loseit7382.cs11@nycu.edu.tw>