

Memory analysis workshop

Full compendium

Version 1.1 – updated 20240301

© Crown Copyright, The National Cyber Security Centre 2023. This information is licensed under the Open Government Licence v3.0. To view this licence, visit <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>.

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK memory analysis workshop slides © Crown Copyright, The National Cyber Security Centre 2023, licensed under the Open Government Licence: <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>.

# Memory analysis workshop

This workshop introduces memory analysis for the purposes of digital forensics and malware analysis. It relates to selected topics of Cyber Security Body of Knowledge version 1.1 (CyBOK) knowledge areas “Forensics”, “Security Operations & Incident Management”, and “Malware and Attack Technologies”[[1]](#footnote-1). Other sources are, whenever used, cited throughout this document.

The workshop intends to introduce memory analysis and related necessary topics such as data storage in memory and properties of memory-resident data. The workshop will also describe when memory analysis can provide valuable results for forensic investigations and incident response processes. The workshop begins with an introduction to the theoretical concepts and continues with a hands-on lab.

This notebook will support the workshop. The first section contains study and reflection support for the theoretical components. The second section contains instructions for a hands-on lab. The third section provides a summary of the central concepts.

# Section 1: Theoretical concepts

## Incident handling note-page

This page is for your notes  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

## Incident handling - core statements

Summarize the most important insights from the lecture as “one-liners”

--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

## Data in memory note-page

This page is for your notes  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

## Data in memory - core statements

Summarize the most important insights from the lecture as “one-liners”

--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

## Malware structures note-page

This page is for your notes  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

## Malware structures - core statements

Summarize the most important insights from the lecture as “one-liners”

--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

## Volatility note-page

This page is for your notes  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------  
  
--------------------------------------------------------------------------------------------------------------------------------------

# Section 2: Hands-on Lab

This lab intends to demonstrate the basic functionality of Volatility memory analysis and introduces memory analysis techniques. Remember that malware analysis is, to a large extent, about finding abnormal behavior. While we can know a fair bit about what malware may typically try to do, it is hard to have a concrete guide. Rather, we need to understand what normal computer operations are and try to find deviations from that – detective work!

You will need the file MalwareSample.7z which you can download from: <https://github.com/kavrestad/MalwareAnalysis>

**NOTE! This is a memory sample containing a malware sample that infected Windows XP computers. While it should be harmless on modern operating systems, avoid doing this lab in sensitive environments!**

## Setting up the lab environment

Volatility 2.6 or Volatility 3 will be used for this lab. Volatility 3 is newer and Volatility 2.6 is discontinued. However, there are differences between the two tools that merit including both of them in the toolbox for a forensic analyst. The most obvious difference is that Volatility 2.6 is discontinued and may therefore not work well for the analysis of modern operating systems. However, Volatility 2.6 is still more extensive in terms of functionality than Volatility 3.

Volatility is a command-line tool built on Python. The Lab instructions contain one track for each version of Volatility. Volatility 2.6 is included first because it is easier to install. Note that the best installation alternative is to always pull the latest version from GitHub. However, the simpler installation procedures explained below are sufficient for this Workshop. This lab is written for Windows, but Volatility can be used similarly on Linux.

### Volatility 2.6 installation in Windows

* Go to <https://github.com/kavrestad/MalwareAnalysis>
* Download Volatility 2.6 standalone executable
* Open a PowerShell terminal and navigate to the folder containing Volatility

### Volatility 3 installation in Windows

*Note that you need to have python 3.6 or later installed*

* Download AND UNPACK Volatility 3
  + From the web page: <https://www.volatilityfoundation.org/3>
  + Clone from git (ensures the latest version): git clone <https://github.com/volatilityfoundation/volatility3.git>
* Install some dependencies
  + *Python -m pip install pefiles*
* Open a PowerShell terminal and navigate to the Volatility folder containing “vol.py”
* You can now run Volatility by issuing the command *python vol.py*

## Testing Volatility

In this section, you will experience the basic usage of Volatility. We will begin with volatility 2.6 and then do the same things with volatility 3. Before we start, download and unpack the file called MalwareSample. The archive contains a memory sample infected with the malware Cridex.

### Volatility 2.6 basic usage

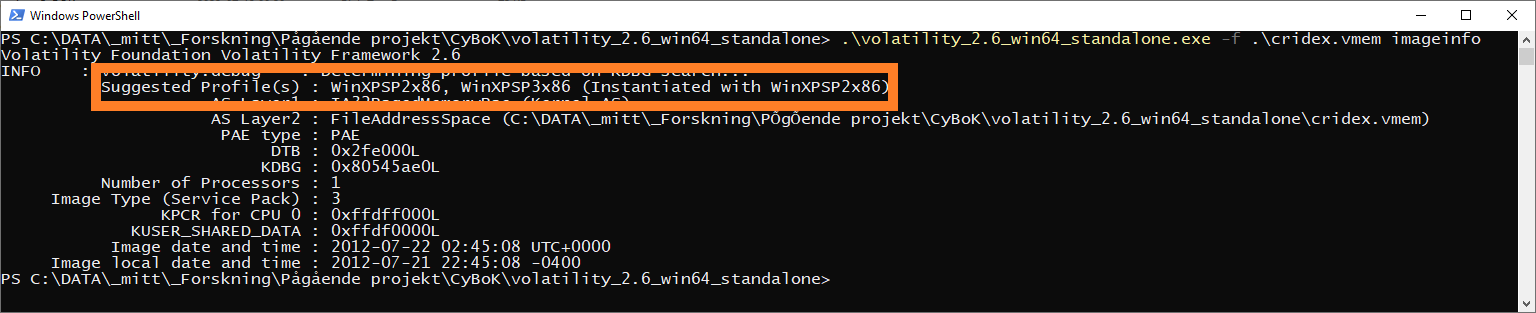
Volatility 2.6 can be best seen as a framework with a set of modules. Each module performs a specific task. Volatility 2.6 is executed by calling the executable using a PowerShell terminal. The basic syntax is (Assuming that vol.py and the memory dump to analyze are both in the current working directory):

.\volatility\_2.6\_win64\_standalone.exe -f *memdumpfilename* -–profile=”*profilename*” *modulename*

The profile name should match the operating system and version that the memory dump is from. This tells Volatility how to read the memory dump and is necessary for Volatility to be able to correctly interpret the memory dump. Volatility can analyze the memory dump and suggest possible profiles to use by issuing the module *imageinfo* as follows.

.\volatility\_2.6\_win64\_standalone.exe -f *memdumpfilename* imageinfo

The output will provide an overview of the memory dump as shown below, the highlighted area shows the suggested profiles.



To get an idea of what Volatility can do, we can resort to the official documentation[[2]](#footnote-2) or use the built-in help-function as follows.

.\volatility\_2.6\_win64\_standalone.exe -h

Now that you know how the tool works, it is all about using different modules to find as much information as possible. The current scenario is Malware identification, and that makes us look for evil processes, bad network connections, and such. However, Memory analysis can also be used to identify misuse and find important information in criminal investigation, and such a case could include looking for encrypted chat messages, encryption keys, or something else. Let’s give it a try!

### Volatility 3 basic usage

Volatility 3 is essentially a Python script that in turn can call other Python scripts. We can call those other script modules. What we essentially need to do is to use python3 to execute Volatility3 and have it use some module. We also need to point to the file containing the memory dump we are to analyze. As such, the basic syntax is (Assuming that vol.py and the memory dump to analyze are both in the current working directory):

Python vol.py -f *memdumpfilename modulename*

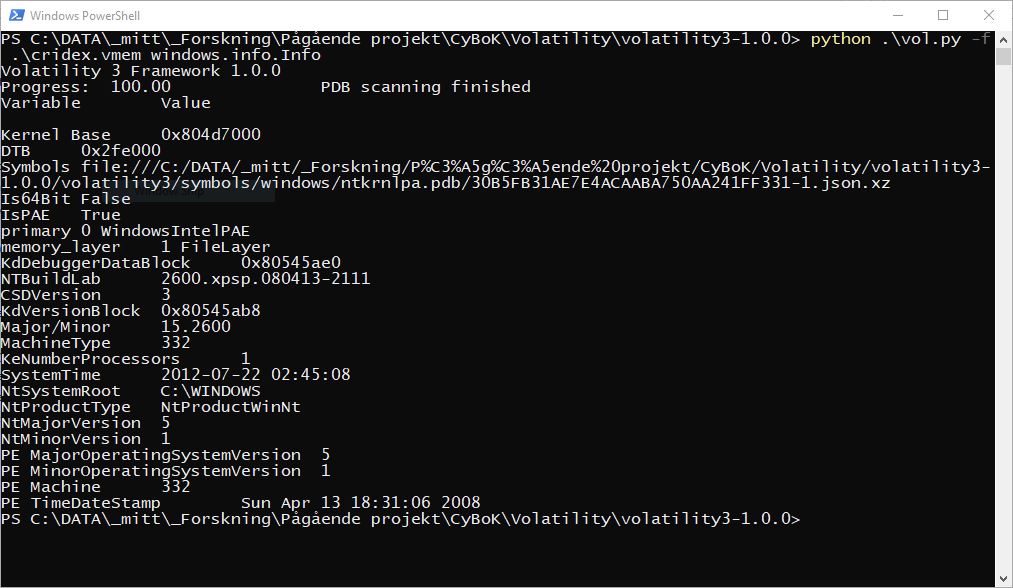
To make Volatility do something, we need to use the different available modules. The modules are listed in the official volatility documentation[[3]](#footnote-3). They can also be listed by invoking the included help function as follows:

Python vol.py -h

A typical starting point in any analysis is to view some default information about the computer the memory dump was taken from. That can be achieved by using the module called info, as follows (Note that modules are case sensitive):

Python vol.py -f .\cridex.vmem windows.info.Info

The output will reveal when the memory dump was created and the system time at that point. It will also reveal that the memory dump is from an NT-based Windows system. It should look as follows:



Now that you know how the tool works, it is all about using different modules to find as much information as possible. The current scenario is Malware identification, and that makes us look for evil processes, bad network connections, and such. However, Memory analysis can also be used to identify misuse and find important information in criminal investigation, and such a case could include looking for encrypted chat messages, encryption keys, or something else. Let’s give it a try!

## Do it yourself

This will be an exercise in finding different information nuggets with the goal of “proving” that the memory dump is indeed from a computer infected by the Cridex malware. In a real-world case, you would not have that information. But since we are currently training, we are entitled to a bit of support. Feel free to use the internet to research the Cridex Malware if you need more information. That could help you understand what to look for. You can choose what Volatility version to use for this task, and you can use them both if that suits your needs. Do the tasks below and try to answer the corresponding questions.

I am using Volatility Version \_\_\_\_\_\_\_

Let’s first try to find out what version of Windows is used by the computer the memory dump is from.

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Listing running processes is a good starting point, it lets us know what processes the computer was running at the time of the memory dump. Find out the number of running processes at the time of the memory dump.

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

On a similar note, what is the Process ID of the lsass.exe process?

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User accounts can be important, what is the name of the user with RID 1003? *TIP: While this can be solved in different ways, the easiest is to figure out how to read RID from windows registry.*

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

It is not uncommon for bad behavior to be executed using the command line. Find out what process has the most command line arguments.

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A malware may want to send away information and needs a network socket. Figure out how many open connections there are.

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

There is also a wonderful function that attempts to identify low-level instructions that could potentially be strange. While the output is verbose, it is well worth a try. Use the malfind module to figure out the processes with potentially harmful instructions.

Module used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Finally, try to work on your own to find good indications of infections in this memory dump. The task is to prove that it is indeed infected with Cridex. Feel free to export data from the memory dump and have your antivirus or some online service analyze it. Also, feel free to use the internet to research more about Cridex.

Modules used:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Section 3: Summary of central concepts

This section provides brief summaries of concepts related to the workshop. It includes selected topics of Cyber Security Body of Knowledge version 1.1 (CyBOK) knowledge areas “Forensics”, “Security Operations & Incident Management”, and “Malware and Attack Technologies”[[4]](#footnote-4). Other sources are, whenever used, cited throughout this document.

## Incident handling

At a very high level, one can view security operations as the processes of first trying to build walls to ensure that nothing bad happens, then being able to detect if something bad happens anyway, and finally responding adequately when some (potentially) harmful event is identified. This workshop covers one part of the “response” process which is initiated when a possible incident is identified. For the sake of the discussion, incident handling assumes that there is an ICT system or information that needs to be secure, and an incident would subsequently be any event that could threaten that security.

Incident handling, also called incident management, is described in great detail in NISTSP800-61. It is a process that can be described in three main activities; *prepare* for incidents, *handle* incidents when they occur, and learn from incidents in a *follow-up* process. Naturally, preparation is crucial. It is even a requirement as per the NIS directive for critical infrastructure operators. It involves the establishment of policies and procedures as well as the preparation of operational capabilities.

The focus of this workshop is on memory analysis which can be a part of the handling and follow-up procedures. Handing involves analysis of the incident at hand and in this case memory analysis is a handy way of analyzing computer behavior and thereby zooming in on the cause of an incident. Maybe malware is exfiltrating data or spawning processes that are unexpected. The full nature of the analysis phase is dependent on the incident, but memory forensics can play a part. Following the recovery from an incident, follow-up activities include learning from the incident, possible legal actions, and attack attribution. Attack attributions involve actions aimed at understanding the source of the incident. Memory analysis can be a powerful way of gaining insight into the exact details of an incident which can, in turn, help the attribution process. Furthermore, memory analysis can help identify forensic artifacts that can be made part of a legal case. That typically requires that the analyst understands forensic methods and constraints to ensure the evidentiary value of those artifacts. Let’s focus on the technical details of memory and begin the hunt for malware!

## The data in memory

The memory contains volatile data relating to the computer’s run state. A somewhat simplified description is that the memory holds data needed by processes that are running, and in some cases, processes that have been running since the computer was last started. The volatile nature of this data means that the data is only present when the computer is running and subsequently lost when the computer is turned off. It is often thought that the memory is immediately cleared when the computer is turned off, which is not really accurate. The data rather fades away and that provides opportunities for data to survive reboots, which in turn allows for various methods of memory collection where the computer needs to be rebooted. While that is another topic, anyone interested can continue reading about cold boot attacks[[5]](#footnote-5).

As for how data is stored in memory, the memory is divided into sections called pages. When a process starts it is assigned a number of pages to store itself during run time. Should it need more space to store data, more pages are allocated to it. Modern computers typically employ virtual memory which means that individual processes are not allowed access to the actual physical memory. Instead, each process is given a virtual memory which is then mapped to the physical memory using a page table. There are several reasons for this approach, but let us focus on the two main implications for forensics. First, each process can be given a virtual memory space equal to the size of the physical memory. Naturally, the sum of all virtual memory spaces will be larger than the available memory. To solve this, space in secondary storage is used to store memory pages when needed. Memory pages that are not currently used can be swapped and stored in pagefile (for Windows) or a SWAP partition (for Linux). As a result, the pagefile or SWAP partition will house memory data and is an additional target during memory analysis. A second implication is that when pages from virtual memories are mapped to the physical memory, pages that appear contiguous in virtual memory may not be contiguous in physical memory, instead, the data can be very fragmented. Since a memory analysis will often focus on data extracted from the physical memory, an analyst (or rather an analysis tool) needs to handle this fragmentation.

## Forensic value of memory analysis

With a rough idea of how memory works, let us discuss the forensic value of analyzing it. It is worthwhile to first reflect on the nature of the data stored in memory. Memory data is the data that is used for processing. Everything that the computer does and everything that is seen on screen are stored and leaves traces in memory. In other terms, it is hard for data and processes to hide their true identity when stored in memory. The volatile nature of memory data is also of significance because it means that whatever data is stored in memory has been placed there since the last start of the computer. The data is therefore typically recent and the recent nature of the data in memory is of forensic significance on its own.

Naturally, many different data types can be found in memory, and that can have forensic significance. Likewise, what to search for will be dependent on the purpose of analyzing the memory in the first place. There are, however, some use cases worth highlighting in this summary.

Encryption is a big challenge for forensic examiners, especially in law enforcement. With modern-day encryption schemes, it is very difficult to decrypt encrypted data. Memory analysis can, however, help in some cases. Owing to the description of “data assuming its true form” in memory shows one way that memory analysis can combat encryption. There is simply a fair chance that plain-text versions of encrypted data can be found in memory, given that the user decrypted this data at some point. Second, encryption keys for encryption communication, full disk, or volume encryption are often stored in memory for more convenient use of encryption services. With a bit of luck, such keys can be extracted and used for decryption.

Malware includes all programs designed to perform malicious activities. There are many types of malware and they differ greatly in what malicious activity they perform, how they spread, and how they hide. A commonality that can be leveraged by a memory analyst is that they do, however, most often assume their true identity in memory. The point is that for malware to carry out its intended tasks it must, in fact, carry out those tasks meaning that it has to assume its true identity and this often happens in memory. Malware can lay dormant on disk, or even in memory and be hard to find due to various evasion techniques. Those include encryption and code obfuscation. However, while activated the malware does perform malicious activities that leave traces in memory.

Not a use case but a general notice is that a lot of different data of forensic significance can be found in memory. It is possible to find fragments of virtually anything and this can be especially useful when it comes to data that is typically not stored in secondary storage. Examples include emails from webmail clients or various communication services. Even if those services store data encrypted, it is often possible to find plain-text fragments in memory.

## Finding malware in memory

Now that we know that malware can be found by analyzing memory the question is how. There are different tools available and two broad analysis approaches. The first approach is to analyze the live memory on a running computer. The second is to secure the data in memory and then analyze that data on a separate machine. This workshop focuses on the latter, using a tool called Volatility. There are three main reasons for preferring this type of analysis over analyzing a running computer.

1. Analyzing a running machine that is expected to be infected with malware requires a potentially infected machine to be left running.
2. Securing data allows for the preservation of the current machine state regardless of how much time is required for the analysis.
3. Securing the current machine state rather than analyzing a running computer complies with forensic best practices[[6]](#footnote-6).

It should be noted that such analysis requires that the memory of a running computer is secured, and that can be done with a variety of tools including Magnet RAM capture[[7]](#footnote-7), AccessData FTK imager[[8]](#footnote-8), Belkasoft RAM capture,[[9]](#footnote-9) and more.

Once the memory is secured, a tool is needed for the analysis of that memory and one such tool is Volatility[[10]](#footnote-10). To analyze memory efficiently, the tool used must understand and interpret memory paging procedures, virtual memories, etc, and Volatility does that. So now that we have a captured memory dump and a tool the analysis can commence.

A manual analysis can be quite tricky, it is about finding some process that does something malicious. As such, it is very much the art of understanding normal computer behavior and finding deviations from that. A good starting point is, however, to contemplate what malware may want to do and look for traces of that. Malware does, for instance, often spawn unexpected processes, run encryption processes, and establish network connections. The general tip is to read about malware behavior and try to find traces of such behavior in the memory that is the subject of analysis.

Finally, the concept of Indicators of compromise (IoC) can be used. IoCs are a formalized way to search for certain suspicious behaviors. Some tools, such as Fireeye Redline[[11]](#footnote-11) allow for the definition of IoC and then the use of IoC to analyze a memory dump. This can be used in two ways. First, a general IoC of suspicious behavior can be used to automatically search for traces of such anomalies. Second, once malware has been identified one can create an IoC specific to that malware and use that to analyze other computers in the same system.

# Reflect

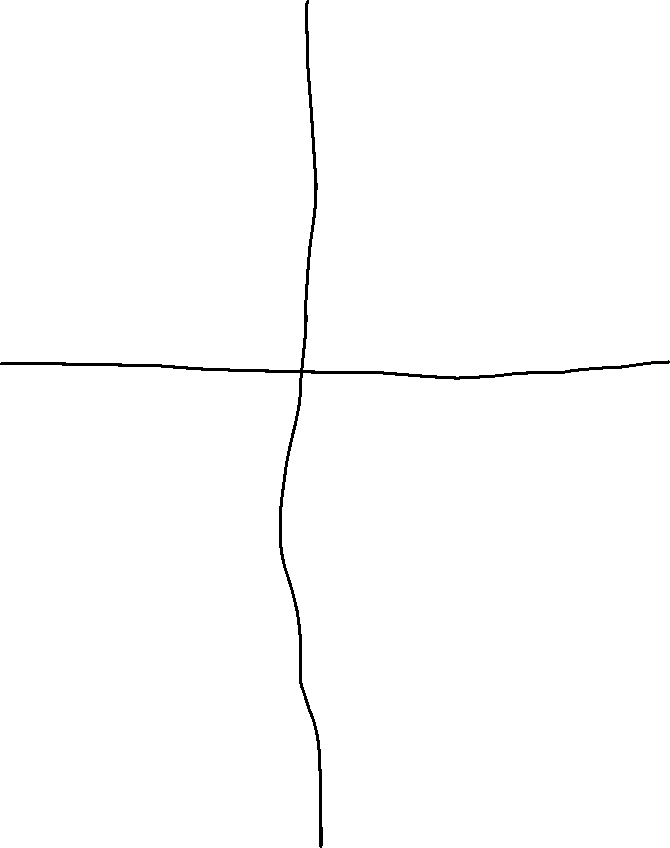
Use the square to make a mind-map of what you learned today

New things I learned

Knowledge I had that was confirmed

Things that were different than I thought

New interesting topics I discovered



1. https://www.cybok.org/knowledgebase1\_1/ [↑](#footnote-ref-1)
2. https://github.com/volatilityfoundation/volatility/wiki/Command-Reference [↑](#footnote-ref-2)
3. https://volatility3.readthedocs.io/en/stable/volatility3.plugins.html [↑](#footnote-ref-3)
4. https://www.cybok.org/knowledgebase1\_1/ [↑](#footnote-ref-4)
5. https://hackernoon.com/new-kids-on-the-block-understanding-cold-boot-attacks-vd2k34or [↑](#footnote-ref-5)
6. Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer International Publishing. [↑](#footnote-ref-6)
7. <https://www.magnetforensics.com/resources/magnet-ram-capture/> [↑](#footnote-ref-7)
8. https://accessdata.com/product-download/ftk-imager-version-4-5 [↑](#footnote-ref-8)
9. https://belkasoft.com/ram-capturer [↑](#footnote-ref-9)
10. https://www.volatilityfoundation.org/ [↑](#footnote-ref-10)
11. https://fireeye.market/apps/211364 [↑](#footnote-ref-11)