**Logo, company name

Description automatically generated**

**GROUP ASSIGNMENT**

**TECHNOLOGY PARK MALAYSIA**

**AICT006-4-2**

**DIGITAL SECURITY AND FORENSICS**

**UCDF 2007ICT(SE)**

**LECTURER: RESHIWARAN A/L JEGATHESWARAN**

**GROUP MEMBERS:**

1. **BRENDEN TAN POH GUAN TP061596**
2. **CHAN HONG WEI TP060647**
3. **CHIAH MING LIANG TP061801**

**HANDOUT DATE: 16th MARCH 2022**

**HANDIN DATE: 17th JUNE 2022**

**WEIGHTAGE: 70%**

**INSTRUCTIONS TO CANDIDATES:**

1. **Submit your assignment at the administrative counter.**
2. **Students are advised to underpin their answers with the use o references (cited using the Harvard Name System of Referencing).**
3. **Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.**
4. **Cases of plagiarism will be penalized.**
5. **The assignment should be bound in an appropriate style (comb-bound or stapled)**
6. **Where the assignment should be submitted in both hardcopy and softcopy, the soft copy of the written assignment and source code (where appropriate) should be on a CD in an envelope / CD cover and attached to the hardcopy.**
7. **You must obtain 50% overall to pass this module.**

|  |  |  |
| --- | --- | --- |
| **Name** | **Task / Description / Responsibility** | **Signature** |
| **BRENDEN TAN POH GUAN TP061596** | * Conclusion * HDD malicious software evidence and report * Personal Reflection |  |
| **CHAN HONG WEI TP060647** | * Introduction * HDD image creation * HDD image analyzation & basic information * Personal Reflection |  |
| **CHIAH MING LIANG TP061801** | * RAM image acquisition * RAM image analyzation * RAM malicious software evidence and report * Personal Reflection |  |

Table of Contents

[1 Introduction 4](#_Toc106330411)

[2 Data Acquisition (RAM) 5](#_Toc106330412)

[2.1 Strategies to Gather Data 5](#_Toc106330413)

[2.2 Forensic tools chosen 6](#_Toc106330414)

[2.3 Steps 7](#_Toc106330415)

[3 Data Acquisition (HDD) 11](#_Toc106330416)

[3.1 Strategies to gather data 11](#_Toc106330417)

[3.2 Forensic tools chosen 11](#_Toc106330418)

[3.3 Steps-by-step data gathering 12](#_Toc106330419)

[4 Analysis (RAM) 18](#_Toc106330420)

[4.1 Forensic tools chosen 18](#_Toc106330421)

[4.2 Step-by-step data gathering processes 19](#_Toc106330422)

[5 Analysis (HDD) 22](#_Toc106330423)

[5.1 Forensic tools chosen 22](#_Toc106330424)

[5.2 Steps-by-steps data gathering 23](#_Toc106330425)

[6 Report – findings from data acquisition and analysis 29](#_Toc106330426)

[6.1 Random Access Memory (RAM) 29](#_Toc106330427)

[6.1.1 Command used for generating result for analyzation 29](#_Toc106330428)

[6.1.2 Findings & Evidence 32](#_Toc106330429)

[6.2 Hard Disk Drive (HDD) 37](#_Toc106330430)

[6.2.1 Basic information 37](#_Toc106330431)

[6.2.2 Malicious Applications found 41](#_Toc106330432)

[7 Personal Reflection 49](#_Toc106330433)

[7.1 CHIAH MING LIANG TP061801 49](#_Toc106330434)

[7.2 BRENDEN TAN POH GUAN TP061596 50](#_Toc106330435)

[7.3 CHAN HONG WEI TP060647 51](#_Toc106330436)

[8 Conclusion 52](#_Toc106330437)

[9 References 53](#_Toc106330438)

[10 Appendix 56](#_Toc106330439)

# Introduction

In section B task 3, a Windows Server 2010 PC that is infected by a botnet called “Zeus” have been given us to conduct forensic investigation. We, as a forensic investigator, we are responsible to gather and analyse the physical evidence such as HDD and RAM in order to come out an investigation conclusion. To do so, we have distributed the HDD and RAM investigation into 3 stages. That is the data acquisition to get the HDD and RAM image, analysis of the image, and analysis reporting.

# Data Acquisition (RAM)

In every computer system, random-access memory (RAM) is one of the important data sources, which contains the volatile data of currently running software, operating system, and network traffic. These data stored in RAM can either have not been recorded or will never be recorded on the hard disk (DFIRScience, 2020). The possible data stored in the RAM are the unsaved documents, usernames and passwords, unencrypted data retrieved from encrypted disk, code from programs, emails and chat messages, malware (only resident in memory), and running processes information.

## Strategies to Gather Data

Capturing RAM images is crucial to find out the traces of evidence. It is a process of extracting volatile data from a random-access memory of the suspected device to non-volatile storage device by using a specialized tool, which will be discussed later. Since RAM is volatile, the data stored inside will be lost, deleted, or being reset if the device loses power supply or crashes. Therefore, capturing RAM images from suspected device is the most important thing to be done first. It has the highest priority to be carried out during the on-scene digital investigation (Frawley, 2020). The diagram below is the example of data acquisition of RAM about data flow during acquiring data from android phone, using a framework called Private data Acquisition method (PEIJUN FENG, 2918).

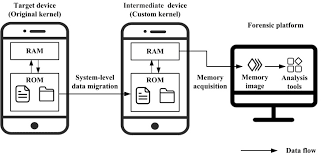


Figure 1 framework of Private data acquisition method (PEIJUN FENG, 2918)

## Forensic tools chosen

As mentioned above, in order to extract the data for carry out investigation and evidence gathering, a forensic tool should be used. The same set of copy of the drive’s structures and its content is the image that acquired after using the tool (GeeksforGeeks, 2020). The forensic chosen for acquiring RAM is FTK Imager, a free tool for generating images from a device, allowing us to preview the data. The functionalities provided in FTK Imager is:

* Generate exactly same copies and images of a storage device.
* Allow us to preview the file and folders in a storage device.
* Recover deleted from Recycle bin from the drive.

The reason we choose FTK Imager is because it has a simple user interface, with powerful functionalities, and it is free. This software is useful for us as a student for learning purpose.In the next section, the step-by-step explanation of how we use the FTK Imager to capture the memory of the infected Windows 10 by a “Zeus” Botnet.

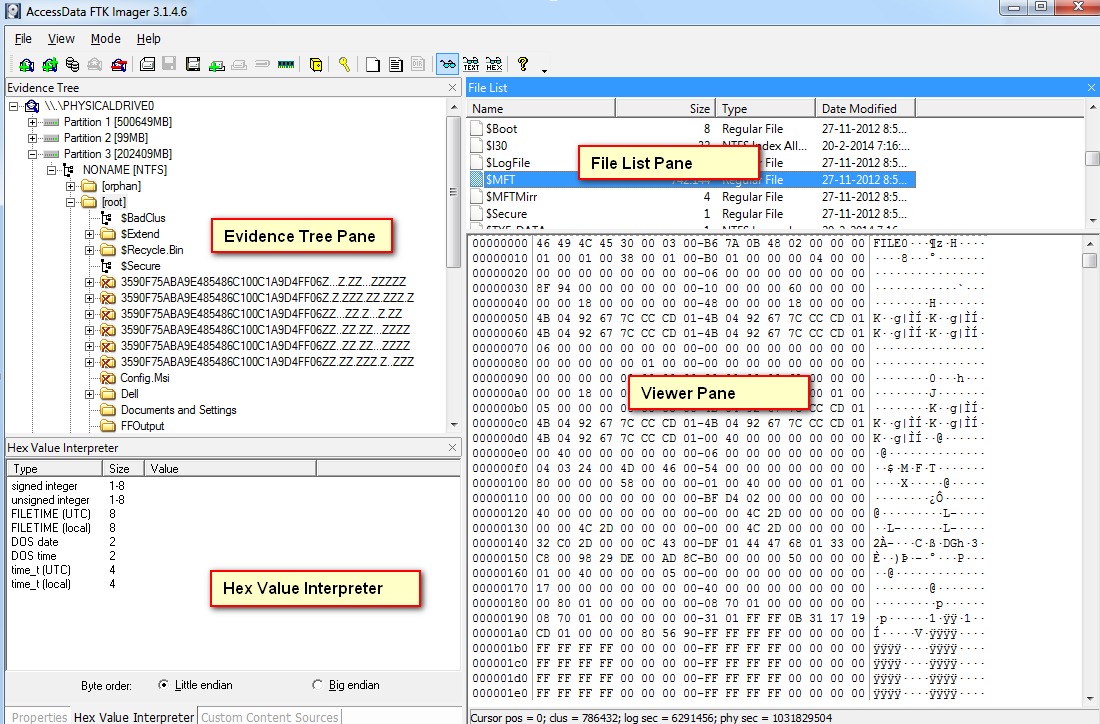


Figure 2 FTK Imager User Interface (Stam, 2014)

## Steps

In order to conduct RAM data acquisition for the Infected Window 10, we should first run the infected Window 10 in the VMware. Then, plugin a USB that contains the FieldKit folder.

1. In the file explorer of the infected Window 10, open the pen drive in file explorer.

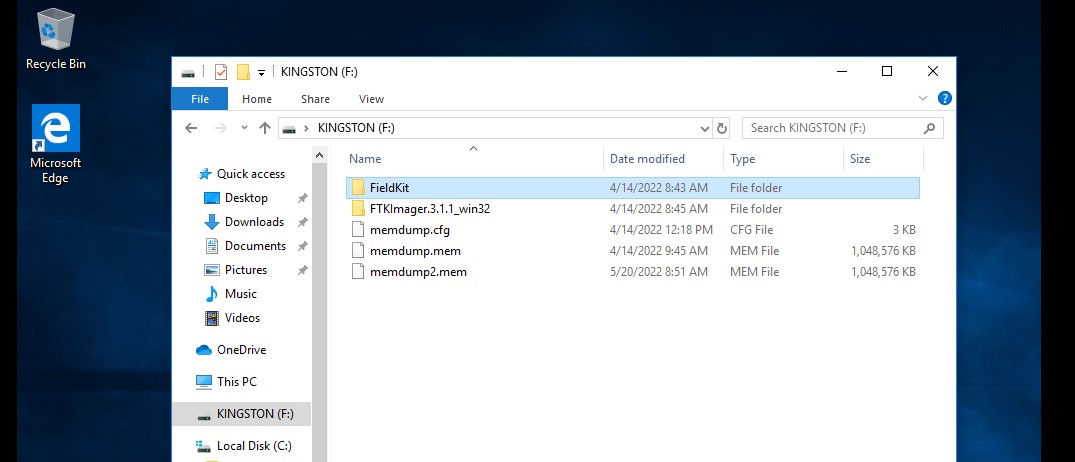


Figure 3 Pendrive's folder

1. Click 2 times on the ‘FieldKit’ folder to open it. Right click on the ’00-MainMenu-00’ and select ‘Run as administrator’

Graphical user interface, text, application, email

Description automatically generated

Figure 4 Run '00-MainMenu-00' as an administrator

1. Then, a pop-up confirmation message will be shown, click ‘Yes’ button to proceed.

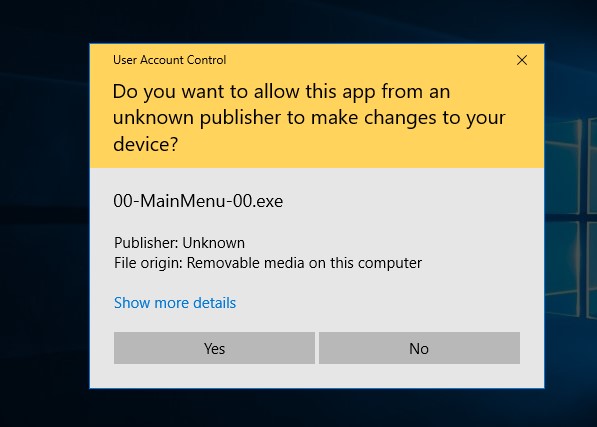


Figure 5 Pop-up confirmation

1. Now, you will be able to see the menu. Click ‘>’ button to get into the page 2. Then double click on the ‘FTK Imager’.

Graphical user interface, application, Word

Description automatically generated

Figure 6 Select FTK Imager

1. The FTK Imager user interface will be shown. Click the ‘File’ tab, located at the right top of the menu list. Then select ‘Capture Memory’ from the drop-down list.

Graphical user interface, application

Description automatically generated

Figure 7 Select 'Capture memory' from the File list

1. In the memory capture window, click ‘Browse’ button. Select the destination path for the captured memory to be stored. Click ‘OK’ after selected the path.

cGraphical user interface, application

Description automatically generated

Figure 8 Select destination path

1. The one last step is to click ‘Capture Memory’ button after the path is selected.

Graphical user interface, text, application, email

Description automatically generated

Figure 9 Click 'Capture memory'

1. Then the capturing process is started. All we have to do is wait until the memory to be captured.

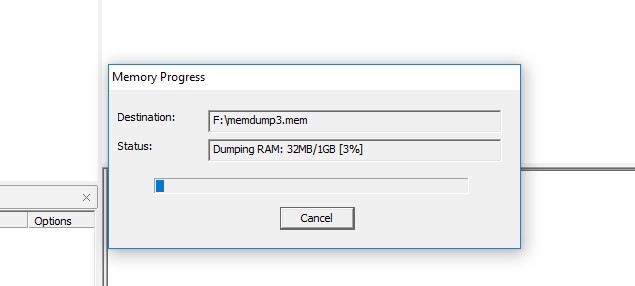


Figure 10 Memory capturing progress

1. Lastly, the .mem file is created in the destination path. The file is ready for analysis, which will be discussed later.

Graphical user interface, application

Description automatically generated

Figure 11 The file is created.

# Data Acquisition (HDD)

During a digital forensic investigation, HDD data acquisition is a method of gathering and recovering the information in a hard drive (cybersecurity exchange, n.d.). Data acquisition usually happens during the system preservation phase of digital forensic investigation (Oreilly, n.d.). According to Oreilly, the system preservation phase is one of the most important phases. This is because it is easy for the data in the hard drive to be lost or overwritten if the hard drive is not cloned immediately. Therefore, a piece of strong conclusive evidence may vanish, and a wrong decision would be made.

## Strategies to gather data

To create a copy of a hard drive, forensic imaging is required. Forensic imaging is a process to create an exact copy of a hard drive. The copy of the disk is called a forensic image. There are a lot of methods to conduct forensic imaging. One of them is a bit-stream disk-to-image file. It is the most common acquisition method that copies all the data bit-by-bit from a hard drive to an image file. In this case, all the sector, partition, files, folders, master boot records, deleted files, and unallocated spaces of the disk would be copied (zhohadamani, 2020). With a bit-stream disk-to-image file acquisition method, it is possible to generate more than one copy.

## Forensic tools chosen

There are many kinds of tools to implement forensic imaging. The tool that we have chosen is FTK imager. It is an open-source software that developed by AccessData. With FTK Imager, digital forensics can be done by analyzing a computers, mobile devices and network communications. In this scenario, we are able to use it to analyze the infected windows 10 by not altering all the initial information in the HDD or RAM.

## Steps-by-step data gathering

1. Download FieldKit and save it into an external drive.
2. Turn on your infected Windows 10 with the VMware Workstation.
3. Plug in the external drive with FieldKit in the infected Windows 10
4. Right click a program called “00-MainMenu-00” and select “run as administrator” in FeildKit.

Graphical user interface, application

Description automatically generated

Figure 12 opening 00-MainMenu-00

1. Press yes to allow the program accessing to your device.

Graphical user interface, text, application

Description automatically generated

Figure 13 user account control window

1. Select the FTK Imager to open it in the pop-up screen.

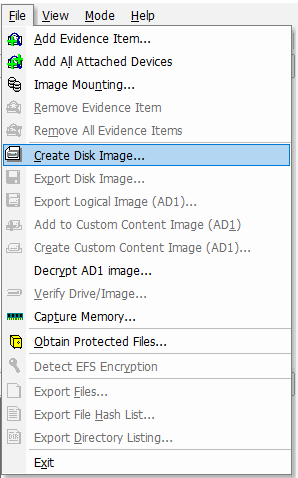
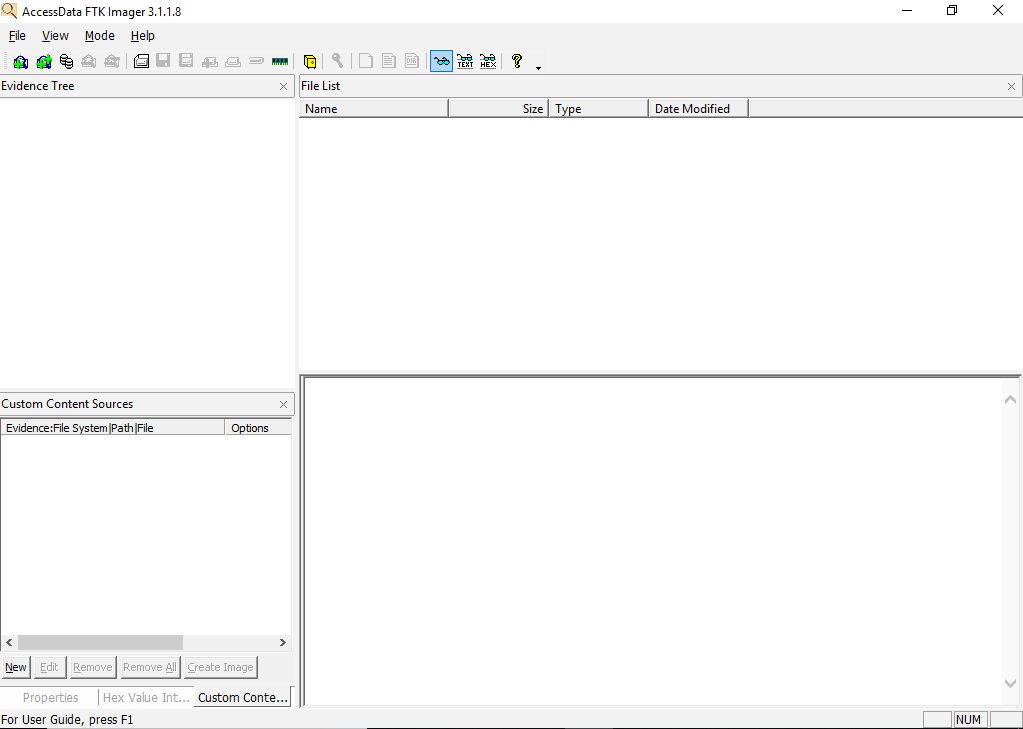
Graphical user interface, application, Word

Description automatically generated

Figure 14 Opening FTK imager

1. Select “create disk image” in “File” in the FTK Imager

Figure 15 Opening Disk image



1. Graphical user interface, application

   Description automatically generatedSelect “physical drive” and press “Next”

Figure 16 Select source window

1. Select the physical drive of the infected Windows 10 as the source drive to copy, which is the “PHYSICALDRIVE0 – VMware, VMware Virtual S SCSI Disk Device”; and press finish.

Graphical user interface, text, application, email

Description automatically generated

Figure 17 Source Drive Selection window

1. Press the “add” button to add a new destination to store the image of infected Windows.

Graphical user interface, application

Description automatically generated

Figure 18 create image window

1. Select “E01” as the image type and press “Next”.

Graphical user interface, text

Description automatically generated

Figure 19 Select image type window

1. Graphical user interface

   Description automatically generatedFill in the case number, evidence number, unique description, examiner, and notes and press “Next”.

Figure 20 Evidence Item information window

1. Select the image destination by pressing the “Browse” button. Next, insert an image filename below the selected destination and press “Finish”.

Graphical user interface, application

Description automatically generated

Figure 21 Selecting image destination

1. Users are able to select another destination if it is required. Once the required destination is selected, all of them would be listed in the Image Destination(s) box. To start the forensic imaging, press the “start” button.

Graphical user interface, application

Description automatically generated

Figure 22 Create image window

1. It takes time for creating the image. Once the progress bar is full, the imaging is done.

Graphical user interface, text, application, email

Description automatically generated

Figure 23 Creating image window

# Analysis (RAM)

After RAM data acquisition, all the data from the RAM Image of the infected PC. The next step is to analyse by finding out all the valid evidence. Since the victim PC is infected by a botnet, there must be some malicious activities executed in the machine. By analysing the acquired data, the program or activities that run in the machine can be evaluated by carry out root caused analysis. Root cause analysis (RCA) is a process of find out what is the problem’s origin, so that suitable solution can be identify (Tableau, n.d.). To analyze the RAM Image, we will use a software as a tool, which will help in analyze the data and categorize them.

## Forensic tools chosen

The forensic tool chosen for analysing the RAM image is PassMark Software’s Volatility Workbench, it is a famous tool used to extract data from volatile memory. This tool has a graphical user interface, provides useful features for memory image analyzation. For example, it provides a list of commands in a drop-down list, with a simple description, allowing the investigator to generate a list of running processes, run commands, and so on (Chandel, 2020). The user interface as shown below.

Graphical user interface

Description automatically generated

Figure 24 User interface of Volatility Workbench (osforensics, n.d.)

## Step-by-step data gathering processes

1. Open ‘Volatility Workbench’ software. Click the ‘Browse Image’ button and select the .mem file that generated previously using FTK Imager.

Graphical user interface

Description automatically generated with medium confidence

Figure 25 Browsing image file.

1. Select ‘Windows’ from the dropdown button of Platform.
2. Select one of the commands from the Command dropdown button and click ‘Run’ button. In this case, the ‘window.psscan.PsScan’ command was selected. The command description of the selected command will be shown in the ‘Command Description’ area.

Graphical user interface, application

Description automatically generated

**Figure 26 Selecting ‘window.psscan.PsScan’ command**

1. After that, the result will be shown in the log below.

Text, letter

Description automatically generated

Figure 27 Result generated

1. In order to export the result, click the ‘Save to file’ button located at the bottom of the program.

Graphical user interface, text

Description automatically generated

Figure 28 Exporting result

1. After exporting the result, the text file will be created. The figure below shows the output of the result in the text file.

Table

Description automatically generated

Figure 29 result shown in text file

The result generated allow us to view what are the processes has been run, and easily find out its details. For example, the process who run without parent process ID will be suspected as malicious process. This is how we determine and analyse the RAM image.

# Analysis (HDD)

## Forensic tools chosen

Autopsy is a Graphic user interface-based program of digital forensics that allows to deploy a lot of plugins in The Sleuth Kit (group of command line tools for analyzing disk image and file recovery) and other open-source programs. With this software, the results of the forensic search would be easily displayed on the GUI. Instead of using the available plugins in Autopsy, people can develop a custom module with Java or Python and implement it with Autopsy. That means Autopsy can be greatly utilized to run different types of programs. Below are some of the common functions that can be achieved via Autopsy.

|  |  |
| --- | --- |
| Features | Explanations |
| Multi-user cases | It allows multiple users access to a same case at the same time. |
| Timeline analysis | It tracks all the implemented activities of a filesystem of a device. |
| Web artifacts | It extracts the information such as bookmarks, cookies, history, downloads, search queries if a browser such as Firefox, Chrome and Internet Explorer. |
| Keyword search | Able to search a text in different files such as PDF, MS Office Documents, Email and so on. |

By using Autopsy, it would be more extensible, faster and more cost effective.

To download Autopsy, the download link can be found on the official website. Here is the link directing to the official website (<https://www.autopsy.com/download/>). There are 64-bit and 32-bit versions. Although the Autopsy is preinstalled in Linux, the GUI of Autopsy would be better on Windows.

## Steps-by-steps data gathering

In this assignment, we are going to use Autopsy to analyse the HDD image that is created from the previous stage.

1. Download and open Autopsy.
2. Select new case in the pop-up page.

Graphical user interface, application

Description automatically generated

Figure 30 initial window while opening Autopsy

1. Enter a case name, select a base directory as a location to store the analysed file and press the “Next” button.

Graphical user interface

Description automatically generated

Figure 31 New case information window

1. Graphical user interface

   Description automatically generatedInsert the optional information such as the number, name and so on and press the “Finish” button.

Figure 32 New case information

1. Wait for the program to create the folder as a database for the analysed results. Once it is done, another pop up page should be displayed.

Graphical user interface

Description automatically generated

Figure 33 creating database

1. Select “Generate new host name based on data source name” and press the button “Next”.

Graphical user interface, text

Description automatically generated

Figure 34 Add data source – select host window

1. Select “Disk image or VM File” and press the button “Next”.

Graphical user interface, text

Description automatically generated

Figure 35 Add data source - select data source type window

1. Press the “Browse” button and select the infected Windows 10 HDD imager (which is the E01 file).

Graphical user interface, text, application

Description automatically generated

Figure 36 Add data source - select data source window

1. Graphical user interface, text, application

   Description automatically generatedLeave the ingest configuration as default and press the button “Next”.

Figure 37 Add data source - configure ingest window

1. The system would add the selected data source to the database which is created at the previous step.

Graphical user interface, text, application, email

Description automatically generated

Figure 38 Add data source - add data source window

1. Once the data source is added. A message would be displayed. Users have to press the “Finish” button to start analysing.

Graphical user interface, text, application, email

Description automatically generated

Figure 39 Add data source - add data source window

1. Users are able to see the analysing progress at the bottom right of the interface. At the same time, users are able to view the analysed results by clicking the items on the left side.

Graphical user interface, text, application

Description automatically generated

Figure 40 analyse progression status

# Report – findings from data acquisition and analysis

## Random Access Memory (RAM)

After analysing the RAM memory dump images by using the Volatility Workbench, we have discovered a few suspicious process and information that has been run in the RAM of the victim’s PC. In following paragraph contains the discussion of the findings found as well as the explanation.

### Command used for generating result for analyzation

In order to get the list of process that executed in the victim machine, we run the ‘windows.psscan.PsScan’, ‘windows.pslist.PsList’, and ‘windows.pstree.PsTree’ command. This allowing us to get the insight about what are the processes that use the system. From the result shown, it listed down all the processes with its details such as parent process id (PPID), its own process id (PID), imager file names, and so on. The figure below shows the result of the findings of the processes gained.

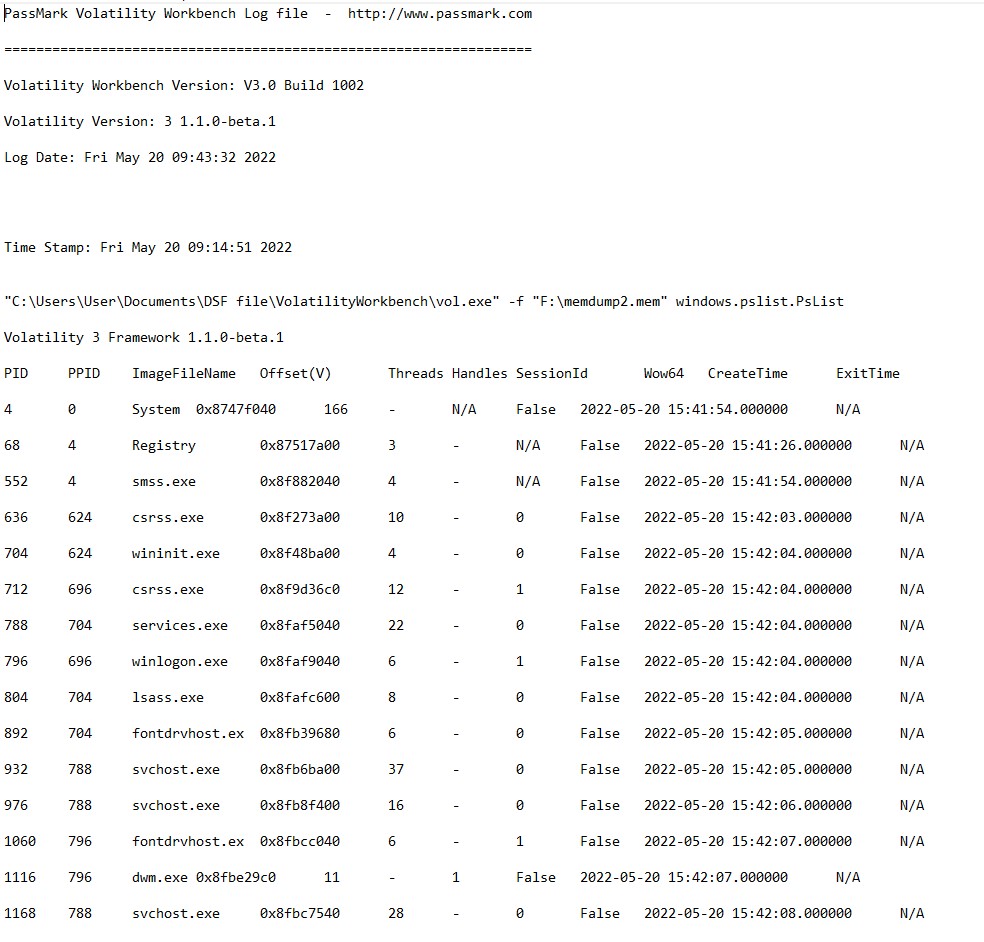


Figure 41 Result from windows.pslist.PsList

Table

Description automatically generated

Figure 42 result from windows.psscan.PsScan

Table

Description automatically generated

Figure 43 result from windows.pstree.PsTree

Since the victim machine is infected by Zeus botnet, we need to recognize the malicious process by generating Loaded Dynamically Linked Libraries (DLL) report. This can be done by executing ‘windows.dlllist.DllList’ command to lists the modules that loaded in the image file. The process details such as process ID, size, and path will be listed. The reason to generate DllList report is to discover the process’s path. This is because attackers will hide trojans or malware process from being detected, by naming itself with the same process name of official window process. Therefore, the identifying the path of the process to check whether it located at the suspicious folder or not is also crucial step to be done (Raikar, 2019). The figure below is the DllList result generated.

Graphical user interface, table

Description automatically generated

Figure 44 Result generated from windows.dlllist.DllList

### Findings & Evidence

The results can be concluded to three parts, which are suspicious process, confirmed malicious process, and non-suspicious process.

**Suspicious process (not malicious)**

After reviewing the results generated, the suspicious processes are found. The following paragraph is the discussion of a suspicious process but is confirmed that it is not malicious process. The process is csrss.exe as it has 2 processes with different parent process ID.



Figure 45 csrss.exe with PPID 696



Figure 46 csrss.exe with PPID 624

Then, we have found out process ID 696 is spoolsv.exe, published by Microsoft Windows which runs the Windows OS print spooler service. It is a legitimate process. The process ID 624 is svchost.exe, the service host process assists the services of Windows to execute efficiently. Window use it as a shared-service process to load Dynamically Linked Libraries (DLL) files (Molinaro, 2022). Therefore, after analyzation, these two processes are legitimate, they run from different parent process ID for two different purposes.

However, csrss.exe file can become a malware if it is not running as Client Server Runtime Process. If the system is infected by malware who pretend to be the csrss.exe file, the storage location will be other folders or file that is not named csrss.exe. The legitimate csrss.exe process should locate in %SystemRoot%\System32 or %SystemRoot%\SysWOW64 folder (Laukkonen, 2021).

By reviewing the result shown in DllList report, the csrss.exe are located in the correct path mentioned previously. Therefore, once again the csrss.exe process in the victim machine is legitimate, an essential part of Windows that helps in graphical subsystem.

Text, table

Description automatically generated with medium confidence

Figure 47 DllList of csrss.exe

**Confirmed malicious processes**

The confirmed malicious processes found in the victim’s machine are rsasws.exe and wap.exe. From PsScan result, it looks nothing wrong, just like any other process, it has a parent process ID that is same with the other legitimate processes just like figure below.

Table

Description automatically generated

Figure 48 rsasws.exe in the result of PsScan

However, when reviewing the DllList result, I realize that the path for rsasws.exe is not located in windows folder but placed in the Program Files’ ProKAward folder. Its parent process ID 788 is the services.exe that located in the folder C:\Windows\System32, it is the services control manager that run, interact, and terminate the system service. While its child process, wap.exe is located in the same folder with the rsasws.exe. After identifying rsasws.exe and wap.exe are located in a weird folder, these two processes are being suspected to be malicious software.

Graphical user interface, text, application

Description automatically generated

Figure 49 rsasws.exe location

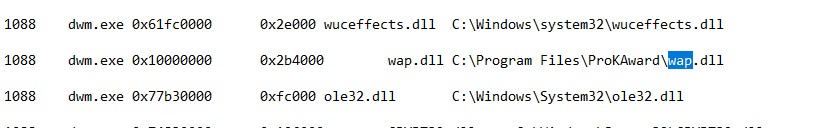
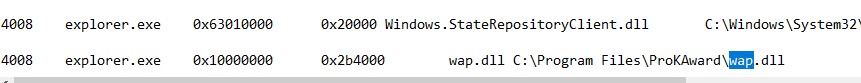
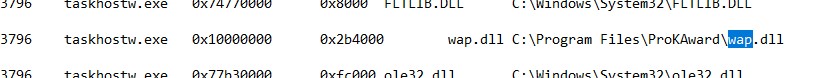


Figure 50 wap.dll location

To further analyse the rsasws.exe and wap.exe, the processes’ properties are analysed from in the victim machine’s task manager. We realize there are no digital signature and software developer listed.

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 51 No digital signature and software developer listed

**(A) Analyzation on rsasws.exe**

Out of 49 anti-virus programs, there are 19 of it detected rsasws.exe file as a malicious program, which is a forty-one detection rate (freefixer, n.d.). The result as shown in the figure below.

Table

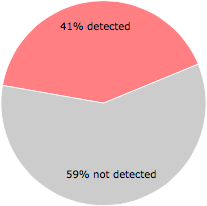
Description automatically generated with low confidence 

Figure 52 Detection rate of rsasws.exe

Most of the detection name are related to ‘KeyLogger’. According to [Josh Fruhlinger](https://www.csoonline.com/author/Josh-Fruhlinger/), the keylogger is a tool, used to write down and report the activity of a computer user when the user interacts with the system. Many malicious attackers infect others machine through phishing emails’ attachment file or include it in other application to hide the program, so that whenever user has downloaded the file or application, the malware is also downloaded. Attackers then can easily steal your credential information such as passwords by reading what you have typed, copied, opened, screen shot, and much more (Fruhlinger, 022).

**(B) Analysis on wap.exe**

The wap.exe program is coming from the ASKLPro Startup process, together with the Award Keylogger Pro software. It is not essential for Windows, and it is reported as a process that will keep bring up problems (file.net, n.d.). The Award Keylogger program is used for check and monitor the targeted computer’s user activity in real time. Just like the discussion in previous paragraph, attackers often use keylogger to steal information, it sounds super creepy if someone is getting all the information of what the users do with their personal computer.

In short, by the analysation of the RAM of the victim’s machine, there are 2 malicious program found in total. However, since the structure of the RAM is small, the information can be gained is quite limited. More details evidence can be found when analysing HDD image of the victim machine.

## Hard Disk Drive (HDD)

By analysing the HDD image with Autopsy, we are able to search for the crucial data or information, also called as artifacts in the results. All the information is distributed into different category on the left side of Autopsy. To find the metadata of the infect ted Window 10, we have to select the perfect path according to the information that we are looking for. Below has shown the crucial information with the screenshot of the location of the information.

### Basic information

The basic information of the infected Windows 10 has been listed in the below table.

|  |  |
| --- | --- |
| Information type | Information |
| Image hash | 21faeaf633aa8fe7068e49ead55f8136 |
| Operating system | Windows 10 Pro |
| OS installation date and time | 2018-05-21 09:47:12 SGT |
| Registered owner | maryam.var |
| Account name | DESKTOP-2Q2EPKM |
| Total amount of recorded accounts | 8 accounts:  1. Guest  2. Administrator  3. maryam.var  4. WDAGUtilityAccount  5.DefaultAccount  + 3 unnamed account |
| The Last User using the computer | Service Virtual Account |
| Network cards | Intel(R) 82574L Gigabit Network Connection |

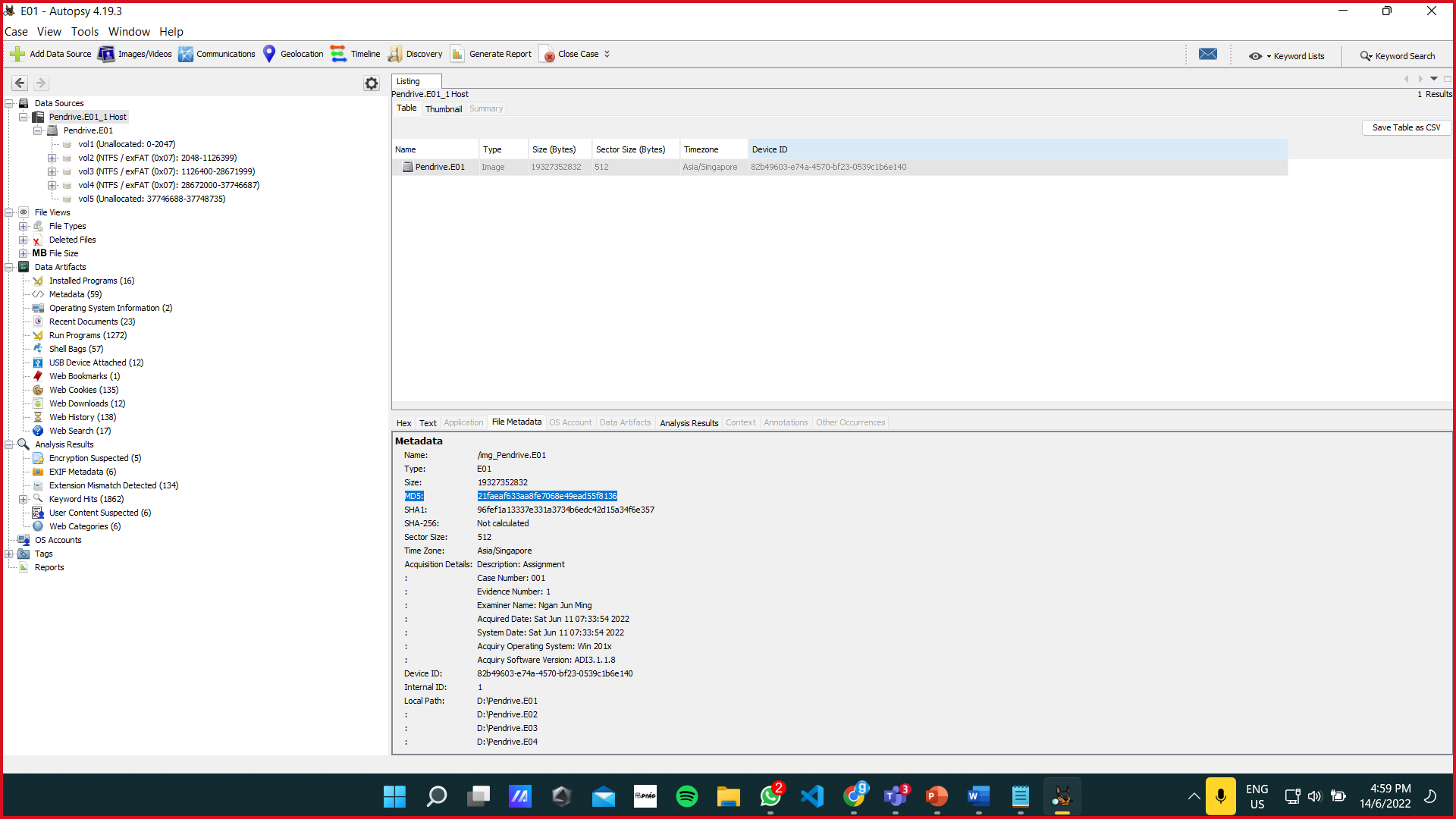


Figure 53 Hash image

Graphical user interface, text, application

Description automatically generated

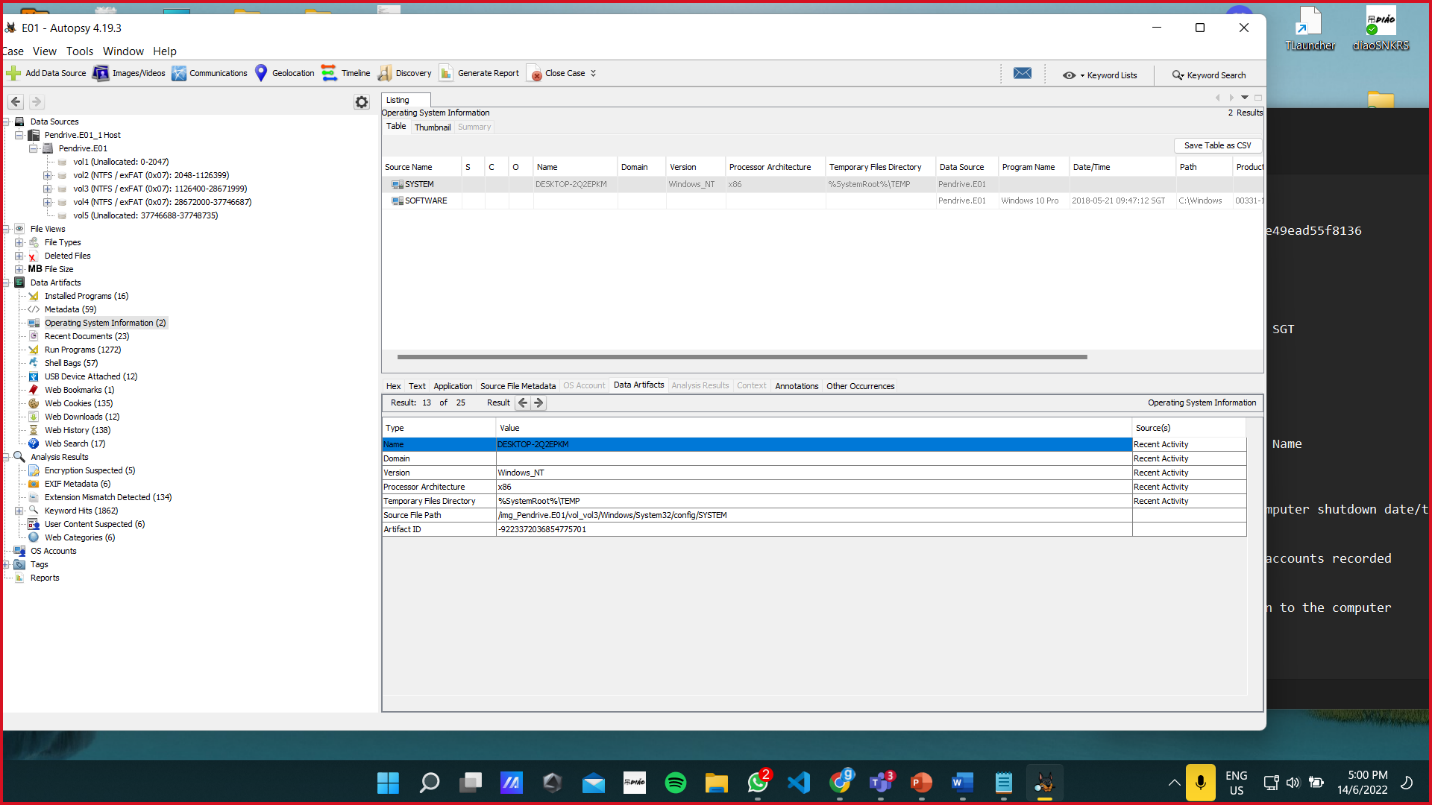


Figure 54 OS, installation date, and owner

Graphical user interface, text, application

Description automatically generated

Figure 55 The 8 users

Figure 56 The last user

Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 57 internet card

### Malicious Applications found

#### Confirmed Malicious Application - Award Keylogger Pro



Figure 58 Logo of Award Keylogger Pro

Award Keylogger Pro is malicious software that is known as a keylogger. A keylogger is software that tracks and records the user activity without the knowledge of the user. Award Keylogger has a few functionalities. The functionalities are taking screenshots of the computer screen at a certain interval, recording the user's keyboard keystroke, tracking all visited websites by the user, and tracking all programs used by the user. The software will record all these various user activities and put them into a log file (Award Software, Inc, n.d.). The hackers can then retrieve this log file to see all the sensitive information of the user. This software will boot up automatically at the start of opening the desktop.

Graphical user interface, text, application, email

Description automatically generated

Figure 59 Sample Screenshot of the log

Graphical user interface, text, application

Description automatically generated

Figure 60 Screenshot of the desktop by the keylogger

This keylogger main folder can be found in “Program Files / ProKAward”. This is where you can see all the data and executables of the Award Keylogger Pro. The software when installed with or without the permission of the user will create a huge list of files. There are 2 main files that are malicious and could cause harm to the user. These 2 main files are the wap.exe and the rsasws.exe. The rsasws.exe is the main executable file that will first be launched when the program starts executing. This executable, according to Dmitry Sokolov, is a trojan keylogger that poses a high risk and it is a very dangerous malware (Sokolov, n.d.). Next, the rsasws.exe will then spawn the wap.exe executable program also known as ASKLPro Startup. This program is also another malicious malware that is used to track and key log the user activity and information.

The malicious software will log all the user activities into a text file. This text file is located at “ProgramData/kprologs”. Inside this folder is where all the screenshot images and the log file are contained. The screenshots and logfile are named according to the date. The screenshot is in a jpg format while the log file is in .htm format

Therefore, it is clear and confirmed that this application is a malicious application that secretly steals the information of the user by keylogging their activities without the user noticing.

Graphical user interface, text, application, table

Description automatically generated

Figure 61 Folder of the Award Keylogger Pro

Graphical user interface, application

Description automatically generated

Figure 62 The kprologs file list

#### Confirmed Malicious Application - KMSAuto

KMSAuto is malicious software that is relatively harmless to users to a certain extent. It is an activation/hacking tool to hack Microsoft products (KMS Auto, n.d.). The software will change and edit the configurations and files of the Microsoft operating system and its products without permission illegally. The software will make it such that the Microsoft product will deem that the user has the access or the activation key to it. For example, the KMSAuto will change the operating system’s files and configurations such that Windows 10 will think that the user has the activation key.

The main folder of the software is located in “ProgramData / KMSAutoS”. The KMSAuto when installed, will create 3 executables. These executables are FakeClient.exe, TunMirror.exe, and TunMirror2.exe. TunMirror.exe and TunMirror2.exe can be found in “ProgramData/KMSAutoS/bin”. TunMirror.exe is an executable that is used by the KMSAuto. It is a malware that has a security rating of 78% (File.net, n.d.). Another executable is TunMirror2.exe. This executable is also similar to the TunMirror.exe as it is a part of the TunMirror.exe. This malware has a rating of 77% dangerous (File.net, n.d.). Other than that, there is the FakeClient.exe. This malware is used as a tool in other applications as well. Its application can range from browser hijacking to adware and many more. This malware has a rating of 82% which means that it is a dangerous malware (File.net, n.d.). The malicious software may or may not be involuntarily installed. There are traces in the download log files on the desktop that indicates that the malicious software is downloaded online. All in all, it is concluded that this KMSAuto is malicious software that is used to activate the Microsoft products for free illegally via maliciously and without permission changing the files and configurations of the operating system. We speculate that this software is used to scam victims by offering them free Windows 10 operating system and Microsoft products but with hidden trojans and malware inside.

Graphical user interface, text, application

Description automatically generated

Figure 63 Main Folder of the KMSAuto

Table

Description automatically generated

Figure 64 File directory of FakeClient.exe in autopsy

Table

Description automatically generated

Figure 65 File directory of TunMirror2.exe

#### Suspicious Application - DLL Injector v2

DLL Injector is an easy-to-use simple tool that allows users to extend and expand the functionalities of applications with components from DLL files. DLL file in full form is called Dynamic Link Library. It is a set of reusable code lines that a program will use in order to work properly. This program allows you to inject codes from DLL files into a running process without permission from the original running process (Virlan, 2017). This is a suspicious application because it allows one to run scripts on running processes covertly. In other words, the hacker could use this dll injector to inject a malicious code into a legitimate process to perform malicious activities without the user noticing. This dll injector is found in the downloads file of the user at “Users/maryam.var/Downloads”. Therefore, it is concluded that the DLL Injector v2 is a suspicious application that is potentially used by the hacker to inject malicious code into running processes covertly.

Graphical user interface, text, application, email

Description automatically generated

Figure 66 Autopsy- Downloads file list

#### Suspicious Application – Upsto.exe

No information could be found on this application Upsto.exe. However, the only clue we could find is the download link page for this Upsto.exe which corresponds to a link called weeknews.pro. No information could be found on what is weeknews.pro and the website is also not found. But we managed to find some information regarding weeknews.pro in the ActivitiesCache.db deep in the directories. ActivitiesCache.db is an SQLite database that stores the user activity information from the Windows 10 Timeline. From this database file, we manage to find a link that contains weeknews.pro. This link is “<http://malc0de.com/database/index.php?search=weeknews.pro>”. The malc0de website is inaccessible via browser and when accessed it shows a gif of a cat instead. This website is reported to be a malicious trojan loader (Any Run, 2019). Therefore, it is concluded that the upsto.exe is a suspicious application and could potentially be used as a trojan loader.

Graphical user interface, application

Description automatically generated with medium confidence

Figure 67 Autopsy - Web downloads list

Graphical user interface, text, application

Description automatically generated



Figure 68 Autopsy - ActivitiesCache.db

A cat sitting on a table

Description automatically generated with medium confidence

Figure 69 Malc0de website accessed via browser

# Personal Reflection

## CHIAH MING LIANG TP061801

What I don’t know before

What I learned + what I feel is important

Talk about the advantages if do so, and drawbacks if I don’t do so

Appreciate ma?

Future enhancement

This assignment really provides me an opportunity to more understanding on how a

## BRENDEN TAN POH GUAN TP061596

Prior to this investigation, I had not known the proper procedure and steps to carry out a digital forensic investigation. After carrying out the investigation and learning how to gather the information needed, I have gained a lot of insight into how a digital forensic investigation will be carried out. I learned the do and don’t’s of forensic investigation as well as the proper procedure. I am amazed by how much information could be gained just from having the image of the RAM or HDD. At the same time, it scares me knowing that if someone manages to steal or get a copy of an image of my RAM or HDD, they could potentially find out every information I have. In addition to all these, I have gained the knowledge on how to figure out if my own PC is infected. The investigation has given me a lot of experiences and knowledge that I am very grateful for.

## CHAN HONG WEI TP060647

By doing the DSF assignment, I have learned a lot of new knowledge that is regarding digital security and forensics. I have learned the vulnerability scanning method, knowledge about the MS-010 vulnerability, vulnerability patching and so on in section A of the assignment. For section B, I have learned the knowledge regarding the physical disk forensic investigation since I am the person in charge of the HDD imager creation and analysing with the software called Autopsy. I personally feel that this assignment is interesting. This is because I am able to apply the knowledge that our lecturer has taught through the lectures and tutorials. Without our lecturer’s guidance and assistance, I believe we are going to take more time on doing research online ourselves. Despite the failure that I came across while doing this assignment, I am still enjoying doing it. Maybe the reason that I enjoy doing it is because of my groupmates, which are Brenden and Ming Liang. They are helpful and kind especially when I was solving an issue or need any help. Actually, I wish I could apologise to them because I am being quick-tempered most of the time. So, I want to say thank you and sorry to my groupmates.

# Conclusion

We set out to investigate an infected PC from a Botnet called “Zeus”. We as forensic investigator has investigated the infected PC to look for any evidence of malicious activities in the infected victim machine. We first carefully carried out our data acquisition to get and secure the evidence from the infected PC. Then, we used various tools and methods to analyze and gather information. After gathering all the information required, we concluded our findings in our report. It is found that a few processes and applications are running and installed in the victim machine that is malicious. There is sufficient evidence to conclude that there are malicious activities in the victim machine.

# References

Any Run. (2019, February 24). *Malware Report*. Retrieved from Any Run: https://any.run/report/eed7f59f1cc35cff9ea319297b065e5122a1b90859596e41d664b60da8d2a20c/ca440657-95c2-45b2-964b-becc4c1b1f2a

Award Software, Inc. (n.d.). *Award Keylogger*. Retrieved from Apponic: https://award-keylogger.apponic.com/#:~:text=Award%20KeyloggerOverview-,Award%20Keylogger%20allows%20you%20to%20monitor%20all%20users%27%20activity%20on,visited%20Web%20sites%2C%20used%20programs.

Chandel, R. (2020, 11 8). *Memory Forensics using Volatility Workbench*. Retrieved from hackingarticles.in: https://www.hackingarticles.in/memory-forensics-using-volatility-workbench/

cybersecurity exchange. (n.d.). *How to Handle Data Acquisition in Digital Forensics*. Retrieved from cybersecurity exchange: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/data-acquisition-digital-forensics/

DFIRScience. (2020, 10 28). *DFS101: 10.1 RAM Acquisition and Analysis*. Retrieved from youtube.com: https://www.youtube.com/watch?v=lI7ePcu6D7Q

File.net. (n.d.). *FakeClient.exe file information*. Retrieved from File.Info: https://www.file.net/process/fakeclient.exe.html

File.net. (n.d.). *TunMirror.exe file information*. Retrieved from File.net: https://www.file.net/process/tunmirror.exe.html

File.net. (n.d.). *TunMirror2.exe file information*. Retrieved from File.net: https://www.file.net/process/tunmirror2.exe.html

file.net. (n.d.). *Wap.exe file information*. Retrieved from file.net: https://www.file.net/process/wap.exe.html

Frawley, R. T. (2020, March 19). *What is RAM Capture and Why does it Matter?* Retrieved from adfsolutions.com: https://www.adfsolutions.com/news/what-is-ram-capture

freefixer. (n.d.). *What is rsasws.exe?* Retrieved from freefixer.com: https://www.freefixer.com/library/file/rsasws.exe-105808/

Fruhlinger, J. (022, MAY 2 18 ). *Keyloggers explained: How attackers record computer inputs*. Retrieved from csoonline.com: https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html

GeeksforGeeks. (2020, Oct 14). *How to Create a Forensic Image with FTK Imager?* Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/

KMS Auto. (n.d.). *About KMS Auto Net Activator* . Retrieved from KMSauto: https://www.kmsauto.info/

Laukkonen, J. (2021, June 28). *What Is Csrss.exe?* Retrieved from lifewire.com: https://www.lifewire.com/what-is-csrss-exe-4584354

Molinaro, D. (2022, March 31). *What Is svchost.exe and Is It Needed?* Retrieved from avast.com: https://www.avast.com/c-what-is-svchost-file

Oreilly. (n.d.). *Hard Disk Data Acquisition*. Retrieved from Oreilly : https://www.oreilly.com/library/view/file-system-forensic/0321268172/ch03.html

osforensics. (n.d.). *Volatility Workbench*. Retrieved from osforensics.com: https://www.osforensics.com/tools/volatility-workbench.html

PEIJUN FENG, Q. L. (2918). Private Data Acquisition Method Based on System-Level Data Migration and Volatile Memory Forensics for Android Applications. *Private Data Acquisition Method Based on System-Level Data Migration and Volatile Memory Forensics*, 16695-16703.

R, R. (2017, Mar 1). *Memory Forensics for Beginners*. Retrieved from inkedin.com/: https://www.linkedin.com/pulse/memory-forensics-beginners-rajivarnan-r

Raikar, G. (2019, October 16). *Top Processes running in Task manager which can be Legitimate or Malicious.* Retrieved from linkedin.com: https://www.linkedin.com/pulse/top-processes-running-task-manager-which-can-malicious-ganesh-raikar/

Sokolov, D. (n.d.). *RSASWS.EXE - Dangerous*. Retrieved from Greatis: https://www.greatis.com/appdata/d/\_/\_program%20files%20common\_\_aaa\_aaa\_bbb\_bbbb\_facebook\_rsasws.exe.htm

Stam, M. (2014, September 5). *HOW TO INVESTIGATE FILES WITH FTK IMAGER*. Retrieved from eforensicsmag.com: https://eforensicsmag.com/how-to-investigate-files-with-ftk-imager/

Tableau. (n.d.). *Root Cause Analysis Explained: Definition, Examples, and Methods*. Retrieved from tableau.com: https://www.tableau.com/learn/articles/root-cause-analysis

Virlan, E. (2017, March 29). *DLL Injector*. Retrieved from Softpedia: https://www.softpedia.com/get/System/System-Miscellaneous/DLL-Injector.shtml

zhohadamani. (2020, October 14). *How to Create a Forensic Image with FTK Imager?* . Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/

# Appendix