

# **FORENSIC ANALYSIS OF INFECTED WINDOWS 10**

## **VIRTUAL MACHINE**

### ***Malware Identification & Incident Response Case Study***

**Author:** Reihan Daniswara Pramudito

**Date:** December 2024

### **KEY FINDINGS**

- **Malware Strains Identified:**
  - **ProKAward:** Keylogger (auto-launches on boot via registry persistence).
  - **KMSAuto:** Trojan masquerading as license activation software.
  - **Ioder.exe:** Dropper delivering payloads from `online234.com`.
- **C2 Infrastructure:**
  - **weeknews.pro** (Payload delivery)
  - **delmonicositaliansteakhouse.com** (Weaponized PDF hosting)
  - **online234.com** (Command-and-control server)
- **Data Exfiltration:**
  - **Final\_Test.pdf:** Weaponized PDF flagged by 62/72 AV vendors (Loki-infostealer).
  - **Microsoft Edge.exe:** Forged process in `C:\Windows\Temp\Nsoft Edge`.

### **TOOLS USED**

- **Forensic Analysis:** Autopsy, Volatility, Wireshark
- **Threat Intelligence:** VirusTotal, Wayback Machine

### **Disclaimer:**

*This report was created for educational purposes. All findings are based on a simulated malware breach scenario involving a Windows 10 virtual machine. The tools, methodologies, and conclusions presented here are intended for learning and do not represent actual organizational data or incidents.*

# Table of Contents

Table of Contents .....	1
1.0 Executive summary .....	3
2.0 Strategies to Gather Data .....	4
3.0 Forensic Tools Chosen.....	6
3.1 Autopsy .....	6
3.2 HashMyFiles .....	6
3.3 “Get-FileHash” command .....	6
3.4 Wayback Machine ( <a href="https://web.archive.org">https://web.archive.org</a> ) .....	7
3.5 Volatility.....	7
3.6 VirusTotal ( <a href="https://www.virustotal.com">https://www.virustotal.com</a> ) .....	7
4.0 Data Acquisition .....	8
4.1 Hardware .....	11
4.2 Web History .....	12
4.3 Suspicious Files on the Disk .....	14
4.4 Live Acquisition .....	23
4.4.1 Acquisition of RAM .....	24
4.4.2 Acquisition of Network Traffic .....	25
5.0 Data Analysis .....	31
5.1 RAM Analysis.....	31
5.2 Network Analysis .....	34
5.3 Findings .....	35
5.3.1 p30download.com and KMSAuto .....	35
5.3.2 zw.exe and Final_Test.pdf .....	38
5.3.3 online234.com and loder.exe .....	39
5.3.4 KMPlayer.exe.....	40
5.3.5 malc0de.com .....	42
5.3.6 weeknews.pro and updsto.exe .....	44
5.3.7 Microsoft Edge.exe .....	45
5.3.8 ProKAward.....	46

6.0 References.....	48
---------------------	----

## 1.0 Executive summary

NEXAGRIL Sdn. Bhd. recently faced a security incident where an infected PC was found in the crime scene. The system showed signs of potentially being infected with malware, which resulted in the company launching a digital forensic investigation to determine the source, nature, and impact of the infection.

As a digital forensic investigator, the goal is to gather and analyze evidence from the infected system, ensure that proper procedures are followed at the crime scene, and ultimately deliver findings to the Cyber Security Lab for further analysis. This investigation seeks to confirm whether the infection has compromised the company's network or sensitive data, and to identify potential vulnerabilities in the organization's security infrastructure.

## 2.0 Strategies to Gather Data

This document was created after the crime scene has been investigated and the infected PC was found and preserved by the first responders. First responders should have already taken all the steps required to investigate the crime scene. The crime scene should have been secured and evaluated, and the crime scene should be well documented. The first responders should have gotten consent and proper warrant to do the search and seizure of items from the crime scene, including the infected PC being investigated. All evidence, physical and digital, should be collected in a proper way, following the guidelines of evidence collection, and should be preserved according to the proper guidelines. The evidence should then be packed and transported according to the proper guidelines and standards of procedure given. A chain of custody should be in place which accounts for all individuals who have had sole custody of each piece of evidence from the time it was seized until now. An image of the infected PC should have already been created and compressed in a zip file which is what is received during the creation of this document.

The zip file would be opened and their hashes calculated to ensure the integrity of the evidence and that no changes were made throughout the investigation. A duplicate would then be created of the original evidence to make sure that no changes are made to the original evidence which would make it dismissible in court. A hash of the duplicate would then be created and compared to the original evidence to make sure that it is an exact duplicate of the original evidence. Anything done throughout the investigation would be on the duplicate of the evidence and never on the original evidence.

Autopsy would be used to acquire information from the storage media, in this case the virtual hard drive, about the infected PC's hardware, web history, and for collecting hashes of suspicious files on it. Another copy of the evidence would then be made and its hashes compared to the original for confirmation. This is done since live acquisition would be done which requires turning on the image of the infected PC which would alter its content and the hash value. The latest duplicate would be turned on and the RAM would be captured using VMware's build in tool, to capture what processes are running after boot. Then Wireshark would be installed to capture all network traffic that is occurring in the infected PC. This would be saved and transferred out of the image of the infected PC for analysis. Commands would be done on the infected PC to determine its IP address and other foreign IP addresses it has a connection with for analysis.

Volatility would be used to analyse the memory dump of the RAM to know all the running processes and determine which are potentially malicious. Then Wireshark would be used to analyse the captured network traffic for any suspicious connections trying to be implemented. VirusTotal would be used to scan files to see if they are malicious and Wayback Machine would be used to see websites accessed on the machine at around the time it was accessed. All the findings from all the analysis would be combined to determine what is malicious.

## 3.0 Forensic Tools Chosen

A virtual machine image of the infected PC from the NEXAGRIL Sdn. Bhd. crime scene called “Windows 10 (Infected).vmdk”, along with several files, is provided in a zip file labeled “WIN10.zip”. To carry out the investigation, the following tools would be utilized to assist the search for proof that the machine is infected and that malicious activities were present. These tools would assist with the acquisition and analysis of the virtual hard disk imaged from the crime scene, RAM, the network traffic, and other important processes to detect signs of infection and find traces of malicious behaviour.

### 3.1 Autopsy

Autopsy is a digital forensic tool that could be used to analyse disk images, recover deleted files, and generate hash value of files to ensure their integrity in the investigation.

### 3.2 HashMyFiles

HashMyFiles is a tool used to calculate the hash values of files using multiple hash algorithms. Hash values are used to ensure the integrity of evidence, making sure that the data hasn't been altered during the investigation process.

### 3.3 “Get-FileHash” command

“Get-FileHash” is a command within Windows PowerShell to calculate the hash value of files. By default, the hashing algorithm selected would be SHA-256 but could be changed by adding the flag “**-Algorithm [algorithm name]**”. The command would be as below:

- **Get-FileHash “[file path]” -Algorithm [algorithm name]**
  - **-Algorithm [algorithm name]** is not needed for the hash algorithm SHA-256
  - In the file path “\*” could be used to represent any string
    - For example, “\*.\*” means files that contain a “.” with any string(s) before and after the “.”, like example.exe or a.b

### **3.4 Wayback Machine (<https://web.archive.org>)**

Wayback Machine, founded by the Internet Archive, is an online service which allows users to access archives of the World Wide Web. It is used in this investigation to examine online resources and websites visited on the infected PC at around the time it was accessed by the user of the infected PC. Some of these websites may no longer exist or may have been changed, so the Wayback Machine is necessary to see what was available during the period it was accessed.

### **3.5 Volatility**

Volatility is a free and open-source memory forensic tool created using Python. It is able to analyse memory dumps and helps find suspicious processes.

### **3.6 VirusTotal (<https://www.virustotal.com>)**

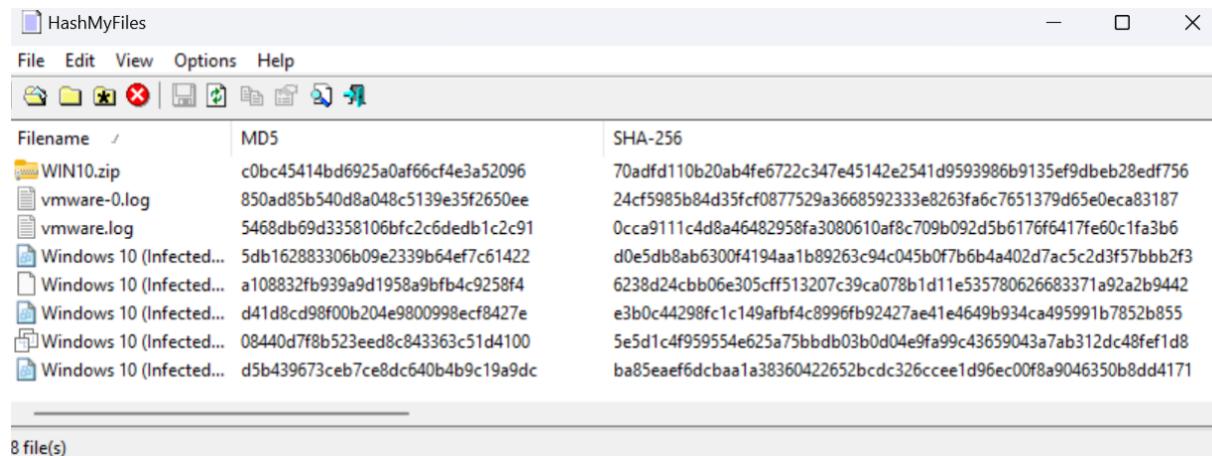
VirusTotal is a free online website which has over 70 antivirus scanners. It is able to scan files, hashes, and URL for potentially being malicious or malware.

## 4.0 Data Acquisition

Before beginning the investigation, it is important to ensure the integrity of the evidence. A duplicate of the original file must be created to ensure that the original evidence remains untouched and will not be altered, preventing the risk of the evidence being modified or corrupted. Verify that the original and the duplicate of the evidence have the same hash value, it is like a unique fingerprint for each file. If the hash value of both the original and the duplicate is the same, it means no data were altered during the investigation. To make sure that the hash value is reliable, multiple tools would be used to calculate the hash values for cross referencing. Using multiple tools to calculate hash would reduce the number of errors in the hash value calculation and make sure the hash value provided is the actual hash value of the file, since both tools must show the same hash values for each file.

The hash algorithms MD5 and SHA-256 would be used when comparing files to the original files since these are common hash algorithms used for integrity check. The original files contain the original “WIN10.zip” zip file, and the “Windows 10 (Infected).vmdk” virtual machine disk file along with other files within the zip file and their respective hash values.

### Original Evidence:



A screenshot of the HashMyFiles application window. The window title is "HashMyFiles". The menu bar includes File, Edit, View, Options, and Help. The toolbar contains icons for file operations like Open, Save, and Hash Types (MD5, SHA-256, etc.). The main table displays two columns of file information: "Filename" and "MD5". To the right of the table, there is a column for "SHA-256" which shows the corresponding hash values for each file. The table lists the following files and their hashes:

Filename	MD5	SHA-256
WIN10.zip	c0bc45414bd6925a0af66cf4e3a52096	70adfd110b20ab4fe6722c347e45142e2541d9593986b9135ef9dbeb28edf756
vmware-0.log	850ad85b540d8a048c5139e35f2650ee	24cf5985b84d35fcf0877529a3668592333e8263fa6c7651379d65e0eca83187
vmware.log	5468db69d3358106bfc2c6dedb1c2c91	0cca9111c4d8a46482958fa3080610af8c709b092d5b6176f6417fe60c1fa3b6
Windows 10 (Infected...)	5db162883306b09e2339b64ef7c61422	d0e5db8ab6300f4194aa1b89263c94c045b0f7b6b4a402d7ac5c2d3f57bbb2f3
Windows 10 (Infected...)	a108832fb939a9d1958a9bfb4c9258f4	6238d24cbb06e305cff513207c39ca078b1d11e535780626683371a92a2b9442
Windows 10 (Infected...)	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
Windows 10 (Infected...)	08440d7f8b523eed8c843363c51d4100	5e5d1c4f959554e625a75bdb03b0d04e9fa99c43659043a7ab312dc48fef1d8
Windows 10 (Infected...)	d5b439673ceb7ce8dc640b4b9c19a9dc	ba85eaef6dcbaa1a38360422652bcd326cce1d96ec00f8a9046350b8dd4171

Above is a screenshot of the original zip file and files within it, and their respective MD5 and SHA-256 hashes, generated using the tool HashMyFiles.

```

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10LAB\WIN10LAB\*.*" -Algorithm MD5
Algorithm      Hash
----          ---
MD5           850ad85b540d8a048c5139e35f2650ee
MD5           5468db6903358106bfC2c60e0b1c2c91
MD5           508162881366b09e2339864ef7c61422
MD5           A4108C2B939049084984B7c28d44
MD5           D0108CD98F800204E980098ecf827E
MD5           08440d7f885233eed0c943363c51d4100
MD5           D5B439673ceb7cebd64084b9c19a9dc

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10.zip" -Algorithm MD5
Algorithm      Hash
----          ---
MD5           C0BC45414BD6925A0AF66CF4E3A52096

```

```

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10\WIN10\*.*"
Algorithm      Hash
----          ---
SHA256         20CFC5985B88WD35FCF9877S29A366859233E8263FA6C7651279D65E0ECA83187
SHA256         0CCA9111cW0A46iUb2958fA288610Af3C709092D058176f617f69c1fA386
SHA256         D9E5DB8A6300F19AAA1B89263C9UCB9580f7864AU92D7AC5C2D3P57BB2f3
SHA256         6238D7CICB9866E205CFF51287C9PC97881D11E52578051668237f1A932B9912
SHA256         E38BCU4298FC1C194AFBFc8996f892477AEU1E6u9893c499591878528855
SHA256         5E5D1C4f959554625A758BD83B04W49FA99C136590437AB312DC48FF1D8
SHA256         B885EAEF6DCBAA1a38369422652Bcdc326CEE1D96EC908A900463508BD4171

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10.zip"
Algorithm      Hash
----          ---
SHA256         79ADFD110B20AB4FE6722C347E45142E2541D9593986B9135Ef9d8EB28EDF756

```

Above are also screenshots of the original zip file and files within it, and their respective MD5 and SHA-256 hashes, generated using the command “Get-FileHash” from Windows PowerShell.

Hashes generated from both HashMyFiles and the “Get-FileHash” command are the exact same. Note that the case of letters in the generated hash value does not matter, this means that for example “a” is equal to “A”.

### Duplicate of the Evidence:

Filename	MD5	SHA-256
WIN10 - Copy.zip	c0bc45414bd6925a0af66cf4e3a52096	70adfd110b20ab4fe6722c347e45142e2541d9593986b9135ef9d8eb28edf756
vmware-0.log	850ad85b540d8a048c5139e35f2650ee	24cf5985b84d35fcf0877529a366859233e8263fa6c7651379d65e0eca83187
vmware.log	5468db6903358106bfC2c60e0b1c2c91	0cca9111c4d8a46482958fa3080610af8c709b092d5b6176f6417fe601fa3b6
Windows 10 (Infected...)	5db16288306b09e2339b64ef7c61422	d0e5db8ab6300f4194aa1b89263c94c045b0f7b6b4a402d7ac5c2d3f57bb2f3
Windows 10 (Infected...)	a108832fb939a9d1958a9fb4c9258f4	6238d24ccb06e305ccf513207c39ca078b1d11e535780626683371a92a2b9442
Windows 10 (Infected...)	d41d8cd98f00b204e9800998ecf8427e	e3b0c4429fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Windows 10 (Infected...)	08440d7f8b523eed0c843363c51d4100	5e5d1c4f959554e625a75bbdb03b0d04e9fa99c43659043a7ab312dc48fef1d8
Windows 10 (Infected...)	d5b439673ceb7ce8dc640b4b9c19a9dc	ba85eaef6dcbaa1a38360422652bcdcc326cce1d96ec00f8a90463508dd4171

Above is a screenshot of the duplicate files which would be used for the investigation with their respective MD5 and SHA-256 hashes, generated using the tool HashMyFiles.

```
Windows PowerShell - Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\*.*" -Algorithm MD5
Algorithm Hash Path
MD5 850A8DB5B5F4D00A9BC5120E35F2659EE C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\vmware_9.log
MD5 5U6BD96903358106FC2C6DEB1C291 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\vmware.log
MD5 50B1268230689E2339B64EFTC6142U C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).nvram
MD5 A108832F929A9D01958A9BEC9258F4 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmdk
MD5 DU1083C9D9204E90089099ECFB027E C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmsd
MD5 0844807F88523EE8DC8A3163CS1D1H00 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmx
MD5 D5B439673CEB7C8ECD6408B9C19A9DC C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmxf

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10 - Copy.zip" -Algorithm MD5
Algorithm Hash Path
MD5 C0BC45414BD6925A0AF66CF4E3A52096 C:\Users\Reihan DP\Downloads\WIN10 - Copy.zip
```

```
Windows PowerShell x Settings x + 
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\*.exe"

Algorithm Hash Path
SHA256 24CF5985B84D35FCF0877529A366859233E8263FA6C7651379D5E9AC81387 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\vmware-0.log
SHA256 08CA9111C9D8A46482958FB3A880618AFBC799B99D2586176F617F6C0C1A3B6 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\vmware.log
SHA256 E05D9B8A639263C94C045B8768E84D194A02D7AC5C9A78B2F3 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).nvram
SHA256 623BD24CB8B6E305CF8513207C9CA678B11DE5378062668337A192A2B894U2 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmdk
SHA256 E3B03CB52D9D8298F01C49AFBF8C996FB927A41E649B8934CA49591B78528855 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmsd
SHA256 SE501CHF959554E625A75BDB83B0D9E49A9C3659943A7AB312C48FF1D0 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmx
SHA256 BA85EEAF6DCBA1A3B368422652BCDC326CE1D96EC0F8A98463508B0D4171 C:\Users\Reihan DP\Downloads\WIN10 - Copy\WIN10LAB\WIN10LAB\Windows 10 (Infected).vmxf

PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10 - Copy.zip"

Algorithm Hash Path
SHA256 78ADFDD110B28AB4F6E722C347E45142E254D959398689135EF9D8BE28EDF756 C:\Users\Reihan DP\Downloads\WIN10 - Copy.zip
```

Above are also screenshots of the duplicate files with their respective MD5 and SHA-256 hashes, generated using the command “Get-FileHash” from Windows PowerShell.

Hashes generated by HashMyFiles and the “Get-FileHash” command are the exact same as each other, and they also match exactly with the hash values of the original files. The case of letters in the generated hash value does not matter, this means that for example “a” is equal to “A”. As the duplicate files are verified to be an exact replica of the original files, the investigation of the virtual machine image of the infected PC could begin. All investigations should be conducted on the duplicate to preserve the integrity of the original evidence. Evidence acquired would be divided into several sections, with each section focusing on different aspects.

## 4.1 Hardware

During the investigation of the virtual machine image of the infected PC using Autopsy, information about the machine, its system, and the user was found.

Source Name	S	C	O	Name	Program Name
Windows 10 (Infected).vmdk				DESKTOP-2Q2EPMK	Windows 10 Pro

Data Content					
Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts
Result: 1 of 1	Result				

Type	Value
Name	DESKTOP-2Q2EPMK
Program Name	Windows 10 Pro
Processor Archite	x86
Temporary Files	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00331-10000-00001-AA187
Owner	maryam.var
Source File Path	/img_Windows 10 (Infected).vmdk
Artifact ID	-9223372036854775648

- The name of the machine: DESKTOP-2Q2EPMK
- Operating System: Windows 10 Pro
- Owner: maryam.var

There was one USB device attached to the machine with the following description:

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			4	2018-05-21 15:24:27 WITA	Toshiba Corp.	TransMemory-Mini / Kingston DataTraveler 2.0 Stick	C412F52D6CA7C1110002F868	Windows 10 (Infected).vmdk

Data Content								
Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
Result: 4 of 35	Result							USB Device Attached

Type	Value	Source(s)
Date/Time	2018-05-21 15:24:27 WITA	Recent Activity
Device Make	Toshiba Corp.	Recent Activity
Device Model	TransMemory-Mini / Kingston DataTraveler 2.0 Stick	Recent Activity
Device ID	C412F52D6CA7C1110002F868	Recent Activity
Source File Path	/img_Windows 10 (Infected).vmdk/vol_vol3/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775714	

- Time and Date: 21 May 2018, 15:24:27 UTC+8
- Device Maker: Toshiba Corp.
- Device Name: TransMemory-Mini / Kingston DataTraveler 2.0 Stick

## 4.2 Web History

During the investigation of the virtual machine image of the infected PC using Autopsy, a file called “WebCacheV01.dat” was found which contains a history of URL visited by the user maryam.var. Several suspicious URL were found, all accessed during 21 May 2018 UTC+8.

WebCacheV01.dat | 4 | http://p30download.com/fa/entry/59803/%D8%AF%D8%A7%D9%86... | 2018-05-21 02:00:27 WITA | Microsoft Edge Analyzer | p30downlo...

WebCacheV01.dat | 4 | https://www.bing.com/search?q=windows+10+crack+p30download&f... | 2018-05-21 02:00:25 WITA | Microsoft Edge Analyzer | bing.com

WebCacheV01.dat | 4 | https://www.bing.com/search?q=windows+10+crack+p30download&f... | 2018-05-21 02:00:25 WITA | Microsoft Edge Analyzer | bing.com

Data Content

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page < > Matches on page: - of - Match < > 100% ⌂ ⌃ Reset Text Source: Result Text

URL : http://p30download.com/fa/entry/59803/%D8%AF%D8%A7%D9%86%D9%88%D8%AF-%DA%A9%D8%B1%DA%A9-%D9%88%D8%8C%D9%86%D8%AF%D9%88%D8%8B  
2-10-%D9%81%D8%89%D8%A7%D9%84-%D8%B3%D8%A7%D8%B2%D8%8C-%D9%88-%D8%B1%D9%81%D8%89-%D9%85%D8%AD%D8%AF  
Date Accessed : 2018-05-21 02:00:27 WITA  
Program Name : Microsoft Edge Analyzer  
Domain : p30download.com  
Username : maryam.var

- Searches for Windows 10 crack p30download
- Visits the website p30download.com with entry id 59803 with the link above

WebCacheV01.dat | 4 | http://p30download.com/fa/entry/67814/ | 2018-05-21 02:00:44 WITA

- Visits the website p30download.com with entry id 67814 with the link above

WebCacheV01.dat | file:///C/Users/maryam.var/Downloads/KMSAuto.Net.2016.v1.5.0\_p30download.com.zip | 2018-05-21 02:02:57 WITA | I

WebCacheV01.dat | 4 | http://shatelcdn.p30download.com/p30dl-software/KMSAuto.Net.2016.v1.5.0\_p30downl... | 2018-05-21 02:01:20 WITA | I

WebCacheV01.dat | 4 | http://shatelcdn.p30download.com/p30dl-software/KMSAuto.Net.2016.v1.5.0\_p30downl... | 2018-05-21 02:01:20 WITA | I

WebCacheV01.dat | 4 | http://cdn.p30download.com/?b=p30dl-software&f=KMSAuto.Net.2016.v1.5.0\_p30down... | 2018-05-21 02:00:55 WITA | I

Data Content

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 82 of 302 Result < >

**Visit Details**

Username: maryam.var  
Date Accessed: 2018-05-21 02:00:55 WITA  
Domain: p30download.com  
URL: http://cdn.p30download.com/?b=p30dl-software&f=KMSAuto.Net.2016.v1.5.0\_p30download.com.zip  
Program Name: Microsoft Edge Analyzer

**Source**

Host: Windows 10 (Infected).vmdk\_1 Host  
Data Source: Windows 10 (Infected).vmdk  
File: /img\_Windows 10 (Infected).vmdk/vol\_vol3/Users/maryam.var/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

- Downloaded the file KMSAuto.Net.2016.v1.5.0\_p30download.com.zip from p30download.com

WebCacheV01.dat		5	http://delmonicositaliansteakhouse.com/zw.exe	2018-05-21 02:24:11 WITA
WebCacheV01.dat		5	http://delmonicositaliansteakhouse.com/zw.exe	2018-05-21 02:24:11 WITA
WebCacheV01.dat		4	http://malc0de.com/database/index.php?search=weeknews.pro	2018-05-21 02:22:58 WITA
WebCacheV01.dat		4	http://malc0de.com/dashboard/	2018-05-21 02:20:32 WITA
WebCacheV01.dat		4	http://malc0de.com/dashboard/	2018-05-21 02:20:32 WITA
WebCacheV01.dat		4	http://malc0de.com/	2018-05-21 02:20:29 WITA

- Visits the website malc0de.com
- Then to a website delmonicositaliansteakhouse.com and download zw.exe

WebCacheV01.dat		4	https://kmplayer.en.softonic.com/	2018-05-21 02:27:38 WITA
WebCacheV01.dat		4	https://kmplayer.en.softonic.com/	2018-05-21 02:27:36 WITA
WebCacheV01.dat		4	https://www.bing.com/search?q=kmplayer&form=EDGTCT&qs=PF...	2018-05-21 02:27:31 WITA
WebCacheV01.dat		5	http://online234.com/hlr/loder.exe	2018-05-21 02:27:08 WITA
WebCacheV01.dat		5	http://online234.com/hlr/loder.exe	2018-05-21 02:27:08 WITA

- Visits the website online234.com and download loder.exe
- Visits the website kmplayer.en.softonic.com

WebCacheV01.dat		5	http://cdn.kmplayer.com/KMP/Download/release/chrome/4.2.2.10/KMPlayer_4.2.2.10.exe	2018-05-21 02:27:51 WITA
-----------------	--	---	--	--------------------------

- Visits the website kmplayer.com and download KMPlayer\_4.2.2.10.exe

WebCacheV01.dat		5	http://weeknews.pro/images/updsto.exe	2018-05-21 07:03:19 WITA	Microsoft Edge Analyzer	weeknews.pro
WebCacheV01.dat		5	http://weeknews.pro/images/updsto.exe	2018-05-21 07:03:19 WITA	Microsoft Edge Analyzer	weeknews.pro
WebCacheV01.dat		4	http://malc0de.com/database/index.php?search=weeknews.pro	2018-05-21 07:03:10 WITA	Microsoft Edge Analyzer	malc0de.com
WebCacheV01.dat		4	http://malc0de.com/database/	2018-05-21 07:03:04 WITA	Microsoft Edge Analyzer	malc0de.com

- Visits the website malc0de.com
- Searches for weeknews.pro
- Then to the website weeknews.pro and download updsto.exe

WebCacheV01.dat		4	http://www.youtube.com/embed/h5QWbURNEpA?feature=player_detailpage	2018-05-21 07:39:34 WITA
-----------------	--	---	--	--------------------------

- A YouTube video watched with the link above

## 4.3 Suspicious Files on the Disk

During the investigation of the virtual machine image of the infected PC using Autopsy, several suspicious files were found on the virtual disk.

In the “Downloads” folder of the user maryam.var, the following were found, and their details.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2018-05-21 15:04:40 WITA	2018-05-21 15:04:40 WITA	2018-05-21 15:22:26 WITA	2018-05-21 09:53:19 WITA	56
DLLInjector v2.exe	4			2018-05-21 10:36:39 WITA	2018-05-21 10:36:39 WITA	2018-05-21 15:13:53 WITA	2018-05-21 10:36:39 WITA	645632
KMPlayer_4.2.2.10.exe	5			2018-05-21 10:28:44 WITA	2018-05-21 10:30:45 WITA	2018-05-21 10:28:45 WITA	2018-05-21 10:27:54 WITA	36708968
KMPlayer_4.2.2.10.exe:Zone.Identifier	4			2018-05-21 10:28:44 WITA	2018-05-21 10:30:45 WITA	2018-05-21 10:28:45 WITA	2018-05-21 10:27:54 WITA	156
loder.exe	5			2018-05-21 10:27:11 WITA	2018-05-21 15:04:34 WITA	2018-05-21 15:05:07 WITA	2018-05-21 10:27:11 WITA	504832
loder.exe:Zone.Identifier	4			2018-05-21 10:27:11 WITA	2018-05-21 15:04:34 WITA	2018-05-21 15:05:07 WITA	2018-05-21 10:27:11 WITA	70
updsto.exe	5			2018-05-21 10:23:37 WITA	2018-05-21 15:04:40 WITA	2018-05-21 15:05:08 WITA	2018-05-21 10:23:10 WITA	1313792
updsto.exe:Zone.Identifier	4			2018-05-21 10:23:37 WITA	2018-05-21 15:04:40 WITA	2018-05-21 15:05:08 WITA	2018-05-21 10:23:10 WITA	73
KMSAuto.Net.2016.v1.5.0				2018-05-21 10:04:43 WITA	2018-05-21 10:07:58 WITA	2018-05-21 10:39:25 WITA	2018-05-21 10:04:26 WITA	56
wrar56b4.exe	5			2018-05-21 09:59:32 WITA	2018-05-21 09:59:41 WITA	2018-05-21 10:02:52 WITA	2018-05-21 09:59:10 WITA	2963224
[parent folder]				2018-05-21 09:58:14 WITA	2018-05-21 09:58:14 WITA	2018-05-21 15:39:40 WITA	2018-05-21 09:53:19 WITA	256
desktop.ini	4			2018-05-21 09:54:05 WITA	2018-05-21 09:54:05 WITA	2018-05-21 15:38:38 WITA	2018-05-21 09:54:05 WITA	282
wrar56b4.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0

- DLLInjector v2.exe
  - MD5: 0a5a1030beba8cba4f283a0636231ee1
  - SHA-256:  
0db7ddd89fc145ab250c69c543a0b0ccc5bce53d017f2faf63d9a115a011d26
- KMPlayer\_4.2.2.10.exe
  - MD5: af7abbcc2a5949f8b21c8efaaaf68ee0c
  - SHA-256:  
7383bd44fc30ed8f7e07c387e3dcbef554269a4121401ee5b726dac25ea4ce22
  - ReferrerUrl=http://www.kmplayer.com/  
HostUrl=http://cdn.kmplayer.com/KMP/Download/release/chrome/4.2.2.10/KMP  
layer\_4.2.2.10.exe
- loder.exe
  - MD5: 0ae466fc76575fbc2d42cdba9788be1e
  - SHA-256:  
3128ef59736fdcd604698ae3d5869909e54ec1b98d8759360512855174ef8927
  - HostUrl=http://online234.com/hlr/loder.exe

- updsto.exe
  - MD5: 761cff25ef1066412cf7403a5ae22ab
  - SHA-256:  
23784235625b527ddc2cc8a3895b53660479cad06c0645de2c79da47ecca6b03
  - HostUrl=http://weeknews.pro/images/updsto.exe
- wrar56b4.exe
  - MD5: d2b85c81f5661f5d4a35a362fc4e5540
  - SHA-256:  
9a7342a167da1165584acdd8630d20b32166e7248fa81865016fe930028cb1df

Inside the folder called “KMSAuto.Net.2016.v1.5.0” within the “Downloads” folder, the following were found.

/img_Windows 10 (Infected).vmdk/vol_vol3/Users/maryam.var/Downloads/KMSAuto.Net.2016.v1.5.0								
<a href="#">Table</a> <a href="#">Thumbnail</a> <a href="#">Summary</a>								
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[parent folder]				2018-05-21 15:04:40 WITA	2018-05-21 15:04:40 WITA	2018-05-21 15:22:26 WITA	2018-05-21 09:53:19 WITA	56
[current folder]				2018-05-21 10:04:43 WITA	2018-05-21 10:07:58 WITA	2018-05-21 10:39:25 WITA	2018-05-21 10:04:26 WITA	56
Read Me.txt			4	2017-04-17 01:04:54 WITA	2018-05-21 10:04:27 WITA	2018-05-21 10:07:58 WITA	2018-05-21 10:04:27 WITA	20119
KMSAuto Net.exe			5	2017-04-08 13:54:29 WITA	2018-05-21 10:04:43 WITA	2018-05-21 10:07:59 WITA	2018-05-21 10:04:27 WITA	8976672
KMSCleaner.exe			4	2015-11-13 02:15:17 WITA	2018-05-21 10:04:27 WITA	2018-05-21 10:07:59 WITA	2018-05-21 10:04:26 WITA	595072

- KMSAuto Net.exe
  - MD5: d02b35945c18e89dc3bb43bc7f6153be
  - SHA-256:  
0b05ea08028f239b11f8c30249b0f0aa86966ee4974d03b01bae2ee88befbbbeb
- KMSCleaner.exe
  - MD5: 13ea767a7ba607744ebea7409b9f8649
  - SHA-256:  
a6e2cdc0e9426d50bd72d866bfc80e0fba941efb3ae6d1c564d409f57d1eb117

- Read Me.txt
  - Important snippets from the text file

**Read Me.txt** | 4 | 2017-04-17 01:04:54 WITA | 2018-05-21 10:04:27 WITA | 2018

**Data Content**

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ← → 100% ⚡ + Reset

KMSAuto Net 2016 Portable by Ratiborus,  
MSFree Inc.

System requirements:

VL editions: Windows Vista, 7, Windows 8, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016, Office 2010/2013/2016.

Description:

KMSAuto Net - automatic KMS-activator for operating systems  
Windows VL editions: Vista, 7, 8, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2 also Office 2010, 2013, 2016.

**Read Me.txt** | 4 | 2017-04-17 01:04:54 WITA | 2018-05-21 10:04:27 WITA | 2018

**Data Content**

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ← → 75% ⚡ + Reset

Using the program:

Run KMSAuto Net.exe as administrator and use the interface. If you need additional program features, enter into Professional Mode. The On/Off Professional Mode button is placed in the "About" Tab.  
The easiest way to use the program is to pick the automatic mode. All you need to do is click on the button if you want to activate and agree to create a scheduled task for reactivation by pressing the button.  
Tip: First you need to activate Windows and Office in manual mode, and only then, when you are sure that the activation takes place, you can create a scheduled task for reactivation products every 25 days.  
If the system does not want to be activated in Professional Mode go to "Utilities" and manually set GVLK key for the proper Windows Edition, and then try to activate again.

Additional Information:

To activate Windows 8.1 the TAP network adapter must be installed directly and use the IP address 10.3.0.2-254 or use a special driver. All these features are built into the program.  
To activate via LAN, the TAP interface can't be used to install and activate through an address of a computer in the network.  
If you reconfigure the program and it stops operating correctly - check the checkbox "Reset the program." All settings will be set by default.

Read Me.txt 4 2017-04-17 01:04:54 WITA 2018-05-21 10:04:27 WITA 2018

Data Content

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ← → 75% ⌂ + Reset

Additional parameters of the program (switches):

/win=act	- Run this program in quiet mode, activate Windows and exit the program.
/off=act	- Run this program in quiet mode, activate Office and exit the program.
/log=yes	- Run this program in quiet mode, create a file ActStatus.log and exit the program.
/kmsset=yes	- Run this program in quiet mode, install KMS-Service and exit the program. It's only for KMS-Service, without TAP, WinDivert, Hook.
/kmsdel=yes	- Run this program in quiet mode, remove KMS-Service and exit the program.
/key=yes	- Run this program in quiet mode, install the Windows key and exit the program.
/task=yes	- Run this program in quiet mode, create a scheduled task for Windows and Office Activation every 25 days and quit.
/taskrun=yes	- Run this program in quiet mode, run the task scheduler for Windows and Office Activation and exit the program.
/convert=	- Run this program in quiet mode, preparation to perform the conversion of Windows version and exit the program.
Possible key values: win81pro, win81ent, win81, win81sl, win81wmc After using this function, you need to restart your computer.	
/sound=yes	- Enable sounds.
/sound=no	- Disable sounds.

The activation will be done with the settings defined in the tab KMS-Service.

Read Me.txt 4 2017-04-17 01:04:54 WITA 2018-05-21 10:04:27 WITA 2018-05-21 10:04:27 WITA

Data Content

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ← → 75% ⌂ + Reset

The program requires .NET Framework 4.5  
To run properly, it is necessary to add the file KMSS.exe in the exclusion of your Anti-Virus!  
Or disable Anti-Virus at the time of activation.

Sometimes KMS-Service is not installed properly, it may be for different reasons.  
You need to perform 2-3 times "Removing KMS-Service" and restart your computer.  
When working with the program it makes sense to check on the option "Save settings in the program folder". In this case, the configuration file will be stored in the program folder, and not in the C:\Users\username\AppData\Local\MSfree Inc.

KMS Log Analyzer.xlsx previous versions are incompatible with KMS Server Service v1.1.7  
In order to save their old records should be transferred to the new KMS Log Analyzer using copy-paste function.

"I wasn't able to activate!!!"

Perhaps you have a non VL product, not intended for activation of KMS-Service, for instance Windows 7 Ultimate can't support KMS activation, or your antivirus blocks the activation.  
If an antivirus is the culprit you can do the following: in the "System" tab click on the blue label "KMS-Service" and in the window that appears remove the check mark. Then add the folder to exceptions in your antivirus program.

Read Me.txt 4 2017-04-17 01:04:54 WIT

Data Content

Hex Text Application File Metadata OS Account Data Artifacts

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ↻

v1.0.3  
-Applied a modified KMS-Service. Allows for the use of each product your own ePID.  
Including CSVLK from actual key.  
-Changed the installation and removal of TunMirror.  
-Changed the installation and removal of TAP interface.  
-Added support for activation of Core, Embedded Industry, Single Language, etc.

v1.0.2  
-Change the setting of TAP interface.  
-New feature for activation Backup / Restore.  
-Cosmetic changes to the interface.  
-Added the ability to create a task scheduler to activate.

v1.0.1  
-Added GVLK keys to Server R2.  
-Cosmetic changes to the interface.

v1.0.0  
-First release.

-----  
www.p30download.com  
the joy of Downloading!

There was a zip file called “win10drivetest(Demo).zip” with the following content.

/img\_Windows 10 (Infected).vmdk/vol\_vol3/win10drivetest(Demo).zip

Table | Thumbnail | Summary

Page: 1 of 1 Pages: ← → Go to Page: [ ]

Name	S	C	O	Modified Time	Change Time	Access Time	Created Ti
win10drivetest(Demo).exe	▼	2		2018-05-20 19:42:10 WITA	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Data Content

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

**Metadata**

Name: /img\_Windows 10 (Infected).vmdk/vol\_vol3/win10drivetest(Demo).zip/win10drivetest(Demo).exe  
Type: Derived  
MIME Type: application/x-dosexec  
Size: 162003  
File Name Allocation: Allocated  
Metadata Allocation: Allocated  
Modified: 2018-05-20 19:42:10 WITA  
Accessed: 0000-00-00 00:00:00  
Created: 0000-00-00 00:00:00  
Changed: 0000-00-00 00:00:00  
MD5: 425d130e0b3aca2813c0fdb743e1a72  
SHA-256: 7c454a1100471e6f2f7cf71df5ded3b367243f7d87d17752b12baf9b85119749  
Hash Lookup Results: UNKNOWN  
Internal ID: 214908

- win10drivetest(Demo).exe
  - MD5: 425d130e0b3aca2813c0fdb743e1a72
  - SHA-256:  
7c454a1100471e6f2f7cf71df5ded3b367243f7d87d17752b12baf9b85119749

There is a folder called “Shared Docs” on another volume, D drive, with the following.

/img_Windows 10 (Infected).vmdk/vol_vol4/Shared Docs							
Table		Thumbnail		Summary			
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2018-05-21 10:25:02 WITA	2018-05-21 14:50:43 WITA	2018-05-21 15:01:24 WITA	2018-05-21 10:09:26 WITA 56
Final_Test.pdf		5		2018-05-21 10:24:13 WITA	2018-05-21 10:24:52 WITA	2018-05-21 10:26:37 WITA	2018-05-21 10:24:12 WITA 543232
Final_Test.pdf:Zone.Identifier		0		2018-05-21 10:24:13 WITA	2018-05-21 10:24:52 WITA	2018-05-21 10:26:37 WITA	2018-05-21 10:24:12 WITA 81
[parent folder]				2018-05-21 10:21:43 WITA	2018-05-21 14:50:43 WITA	2018-05-21 15:01:34 WITA	2018-05-21 09:57:32 WITA 56
Thumbs.db		0		2018-05-20 19:20:06 WITA	2018-05-21 10:20:06 WITA	2018-05-21 10:20:06 WITA	2018-05-21 10:15:32 WITA 21504
Thumbs.db:encryptable				2018-05-20 19:20:06 WITA	2018-05-21 10:20:06 WITA	2018-05-21 10:20:06 WITA	2018-05-21 10:15:32 WITA 0
FDR-Assignment.docx		0		2018-05-20 19:18:52 WITA	2018-05-21 10:19:05 WITA	2018-05-21 10:19:21 WITA	2018-05-20 19:17:49 WITA 25388
nistspecialpublication800-94.p		0		2018-05-20 19:16:45 WITA	2018-05-21 10:16:56 WITA	2018-05-21 10:17:21 WITA	2018-05-20 19:16:45 WITA 1060429
nistspecialpublication800-94.p		5		2018-05-20 19:16:45 WITA	2018-05-21 10:16:56 WITA	2018-05-21 10:17:21 WITA	2018-05-20 19:16:45 WITA 26
Chris Sanders-Practical packet		0		2015-04-06 12:15:22 WITA	2018-05-21 10:15:32 WITA	2018-05-21 10:15:57 WITA	2018-05-21 10:15:32 WITA 17339416

- Final\_Test.pdf
  - MD5: ce6ba3df1d57ade7830c5315d77c9311
  - SHA-256:  
ce8bbc09521bc9bd7a358e4fbbe370962e22b91a78c8d895716ef98a1daaaaf77
  - HostUrl=<http://delmonicositaliansteakhouse.com/zw.exe>
- nistspecialpublication800-94.pdf
  - MD5: 4670a6f605d15fa3155462928e025fd6
  - SHA-256:  
289c2ed27f7e3aac41624bf2e6fad268642bad2dabe352a5ab28fa169824a96e
- Chris Sanders-Practical packet analysis \_ using Wireshark to solve real-world network problems-No Starch Press (2011).pdf
  - MD5: 90666c5607556bc084d61fa51071244e
  - SHA-256:  
bf4b16876c34f44246b91441a5259d698bae63d15a7d5c8053b7d0f850608712
- FDR-Assignment.docx
  - MD5: 5163b03e1a38bd5db769a2bfeeb7ab3
  - SHA-256:  
edcbcd6ab07cf5483d5d2aeb4345ee7587d9d8c50d18195f39f86672409bad2

Inside the “Program Files” folder there is another folder called “ProKAward” with several items that are flagged as suspicious.

/img_Windows 10 (Infected).vmdk/vol_vol3/Program Files/ProKAward										19 Results
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	
wap.ini			3	2018-05-21 15:39:40 WITA	2018-05-21 15:39:40 WITA	2018-05-21 15:39:40 WITA	2018-05-21 10:35:14 WITA	3504	Allocated	
update				2018-05-21 15:39:38 WITA	2018-05-21 15:39:38 WITA	2018-05-21 15:39:38 WITA	2018-05-21 10:35:15 WITA	56	Allocated	
[current folder]				2018-05-21 15:04:26 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:04:26 WITA	2018-05-21 10:35:14 WITA	56	Allocated	
Data				2018-05-21 15:04:26 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:14 WITA	272	Allocated	
Icons				2018-05-21 15:04:26 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2013-03-14 02:44:52 WITA	152	Allocated	
builder.ini			5	2018-05-21 10:43:27 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2013-06-26 03:47:00 WITA	2219	Allocated	
images				2018-05-21 10:35:15 WITA	2018-05-21 10:35:15 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:15 WITA	712	Allocated	
un.url			3	2018-05-21 10:35:15 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:15 WITA	141	Allocated	
unins000.dat			3	2018-05-21 10:35:15 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:14 WITA	5652	Allocated	
Website.url			3	2018-05-21 10:35:15 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:15 WITA	71	Allocated	
[parent folder]				2018-05-21 10:35:14 WITA	2018-05-21 10:35:14 WITA	2018-05-21 15:39:40 WITA	2018-03-24 23:40:35 WITA	184	Allocated	
unins000.exe			3	2018-05-21 10:34:57 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:14 WITA	715253	Allocated	
wap.exe			3	2014-03-28 02:13:08 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:39:39 WITA	2018-05-21 10:35:14 WITA	4096000	Allocated	
rsasws.exe			2	2014-03-28 02:12:30 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:15 WITA	98304	Allocated	
wap.dll			4	2014-03-28 02:11:18 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:39:39 WITA	2018-05-21 10:35:14 WITA	2809856	Allocated	
filedat.dat			3	2014-03-05 07:43:20 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2014-03-05 07:43:20 WITA	159744	Allocated	
Builder.exe			3	2014-03-05 07:42:00 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2014-03-05 07:42:00 WITA	1486848	Allocated	
wap.exe.manifest			3	2011-01-12 05:05:12 WITA	2018-05-21 15:04:26 WITA	2018-05-21 15:27:25 WITA	2018-05-21 10:35:15 WITA	862	Allocated	
as.lst				2011-01-08 08:58:52 WITA	2018-05-21 10:35:15 WITA	2018-05-21 10:35:15 WITA	2018-05-21 10:35:15 WITA	0	Allocated	

/img_Windows 10 (Infected).vmdk/vol_vol3/Program Files/ProKAward										19 Results
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(  )
wap.ini			3	2018-05-21 14:39:40 WIB	2018-05-21 14:39:40 WIB	2018-05-21 14:39:40 WIB	2018-05-21 09:35:14 WIB	3504	Allocated	Allocated

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences	
Strings	Extracted Text	Translation								
Page: 1 of 1 Page	Matches on page: - of - Match									Text Source: File Text
[Admin] LogFolder=%CommonAppData%\kprologs DefaultHotkey=1879 ClearType=2 appname=Award Keylogger Pro DisableWhenOffline=0										

- wap.exe
  - MD5: 5f05bd96f3ff5fa56c9d41c012ec6a13
  - SHA-256:  
9c8d0a43aa95e439cede9b69cacfb3c606381bfd6745111c5cfe73a38af9ae38
- rsasws.exe
  - MD5: 62e1be50323d92a7d035552c06a7ef6f
  - SHA-256:  
1b84356e23933ecb201460a7c4fe491123831764a7e125e08ceae3dc3e5c9b64

- filedat.dat
  - MD5: 377a3707a5b10f95f731e5feb131d68c
  - SHA-256:  
01149f1442787755c79c61499355a79dcfe8ebb67ea9b91fc6413d56ec2070f6
- Builder.exe
  - MD5: 2a651e36ff88b753aba8d6f197aec8a8
  - SHA-256:  
2bd25e1f11247fb58536e808e01dfec293497a4e96bf51a0e61d242927e9e9d8
- wap.exe.manifest

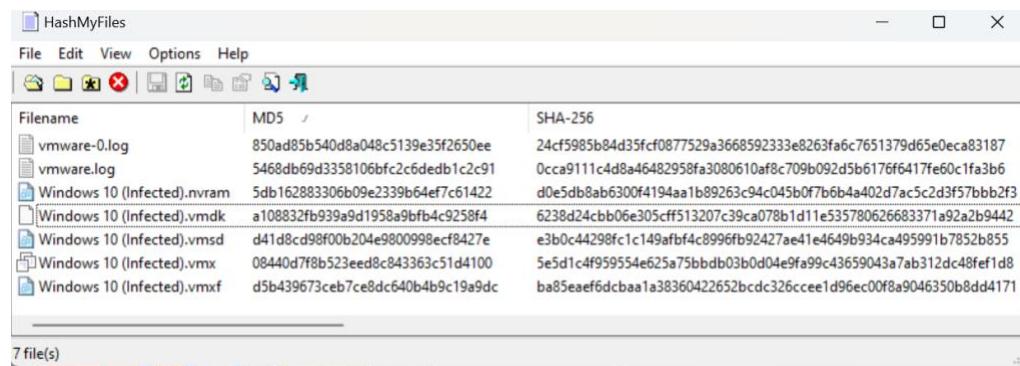
```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
    version="1.0.0.0"
    processorArchitecture="x86"
    name="Award Keylogger Pro"
    type="win32"
<description>
    Award Keylogger Pro Application
</description>
<dependency>
    <dependentAssembly>
        <assemblyIdentity
            type="win32"
            name="Microsoft.Windows.Common-Controls"
            version="6.0.0.0"
            processorArchitecture="x86"
            publicKeyToken="6595b64144ccf1df"
            language="*"
        />
    </dependentAssembly>
</dependency>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel level="requireAdministrator" uiAccess="false"/>
        </requestedPrivileges>
    </security>
</trustInfo>

```

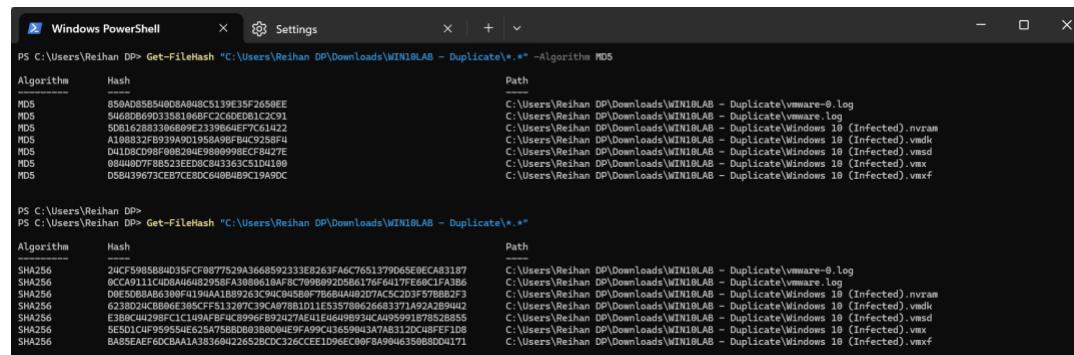
## 4.4 Live Acquisition

Live acquisition involves turning on the machine to acquire evidence. This would alter the content of the virtual machine and its hash values, which is why another duplicate of the folder containing the virtual machine would be made only for the live acquisition. The hash value of the duplicate would then be calculated and compared to the original file to make sure that it is the exact same. Then Live acquisition could then be performed on the duplicate.



Filename	MD5	SHA-256
vmware-0.log	850ad85b540d8a048c5139e35f2650ee	24cf5985b8d435fcf0877529a366859233e8263fa6c7651379d65e0eca83187
vmware.log	5468db69d3358106bc2fc2d6edb1c2c91	0cca9111c4d8a4648295fa3080610af8c709b092d5b6176f6417fe60c1fa3b6
Windows 10 (Infected).nvram	5db1f62883306b09e2339b64ef7c61422	d0e5db8ab6300f4194aa1b89263c94c045b0f7b6b4a402d7ac5c2d3f57bbb2f3
Windows 10 (Infected).vmdk	a108832fb939a9d1958a9bf4c92584	6238d24cb06e305cff513207c39ca078b1d11e535780626683371a92a2b9442
Windows 10 (Infected).vmsd	d41d8cd98f00b204e980098ecf8427e	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
Windows 10 (Infected).vmx	08440d7f8b523eed8c843363c51d4100	5e5d1c4f959554e625a75bbdb03b0d04ef9a99c436590437ab312dc48fe1d8
Windows 10 (Infected).vmxf	d5b439673ceb7e8dc640b4b9c19a9dc	ba85eaef6dcbaa1a38360422652bcd326cce1d96ec00f8a9046350b8dd4171

Above is a screenshot of the duplicate files that would be used for the live acquisition with their respective MD5 and SHA-256 hashes, generated using HashMyFiles.



PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\*.*" -Algorithm MD5		
Algorithm	Hash	Path
MD5	850ad85b540d8a048c5139e35f2650ee	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\vmware-0.log
MD5	5468db69d3358106bc2fc2d6edb1c2c91	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\vmware.log
MD5	508162883306b09e2339b64ef7c61422	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).nvram
MD5	A108832fb939a9d1958a9bf4c92584	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmdk
MD5	D41d8cd98f00b204e980098ecf8427e	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmsd
MD5	08440d7f8b523eed8c843363c51d4100	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmx
MD5	d5b439673ceb7e8dc640b4b9c19a9dc	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmxf

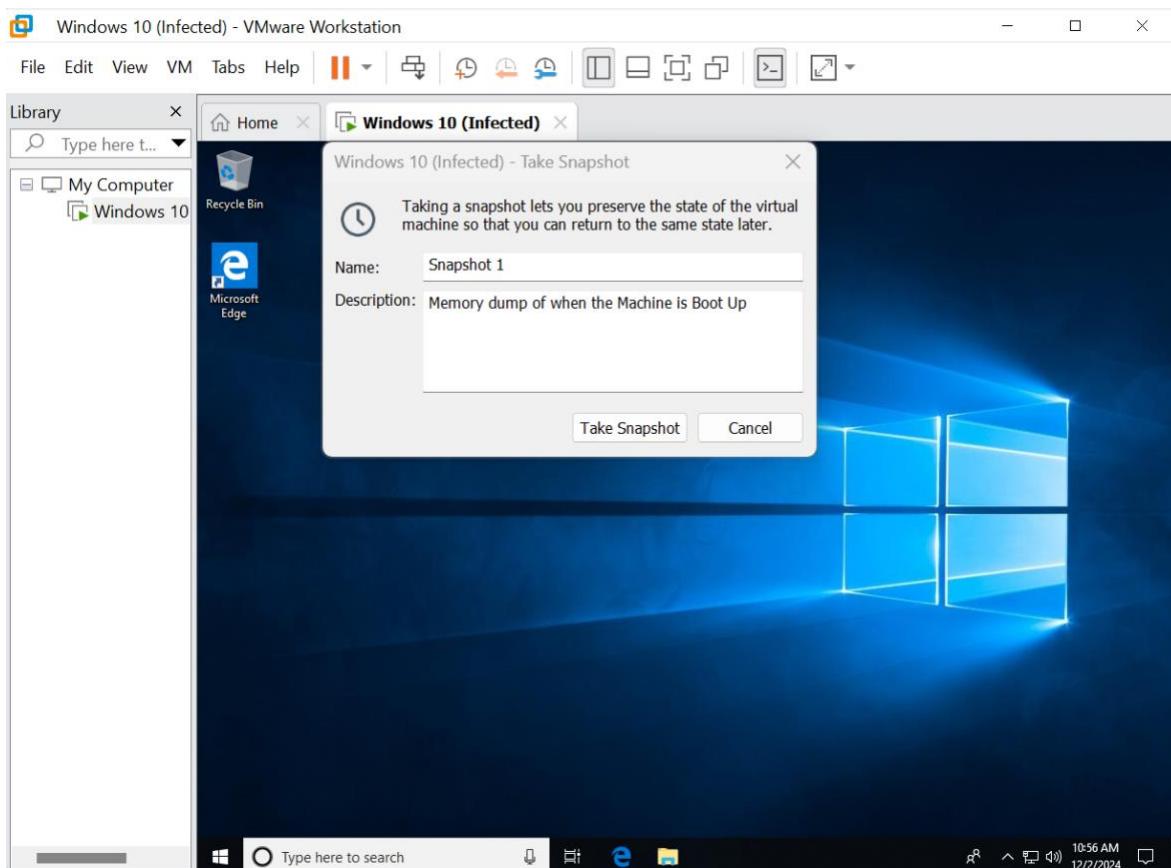
PS C:\Users\Reihan DP> Get-FileHash "C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\*.*"		
Algorithm	Hash	Path
SHA256	24cf5985b8d435fcf0877529a366859233e8263fa6c7651379d65e0eca83187	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\vmware-0.log
SHA256	0cca9111c4d8a4648295fa3080610af8c709b092d5b6176f6417fe60c1fa3b6	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\vmware.log
SHA256	d0e5db8ab6300f4194aa1b89263c94c045b0f7b6b4a402d7ac5c2d3f57bbb2f3	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).nvram
SHA256	6238d24cb06e305cff513207c39ca078b1d11e535780626683371a92a2b9442	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmdk
SHA256	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmsd
SHA256	5e5d1c4f959554e625a75bbdb03b0d04ef9a99c436590437ab312dc48fe1d8	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmx
SHA256	ba85eaef6dcbaa1a38360422652bcd326cce1d96ec00f8a9046350b8dd4171	C:\Users\Reihan DP\Downloads\WIN10LAB - Duplicate\Windows 10 (Infected).vmxf

Above are also screenshots of the duplicate files with their respective MD5 and SHA-256 hashes, generated using the command “Get-FileHash” from Windows PowerShell.

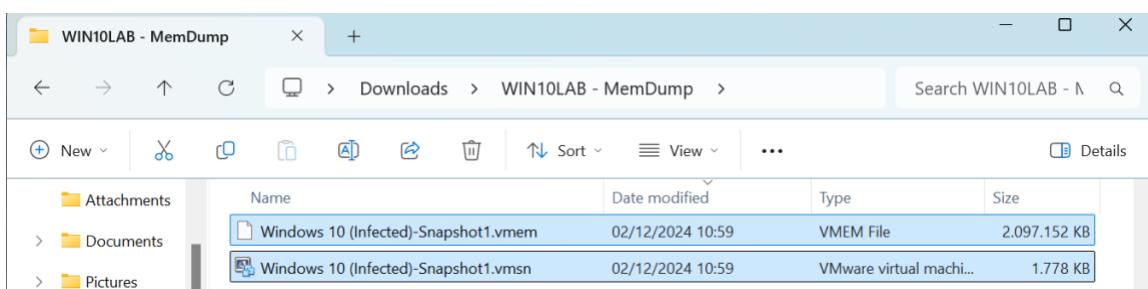
Hashes generated by HashMyFiles and the “Get-FileHash” command are the exact same as each other, and they also match exactly with the hash values of the original files. As stated previously, the case of letters does not matter. The duplicate files are an exact copy of the original files, which means that live acquisition could be started. The contents of the files would be altered due to the live acquisition, but the original files would be preserved.

#### 4.4.1 Acquisition of RAM

The duplicate of the virtual machine would be turned on and a memory dump would be performed on the RAM of when the machine is just boot up. This is done using the build in snapshot tool in VMware.

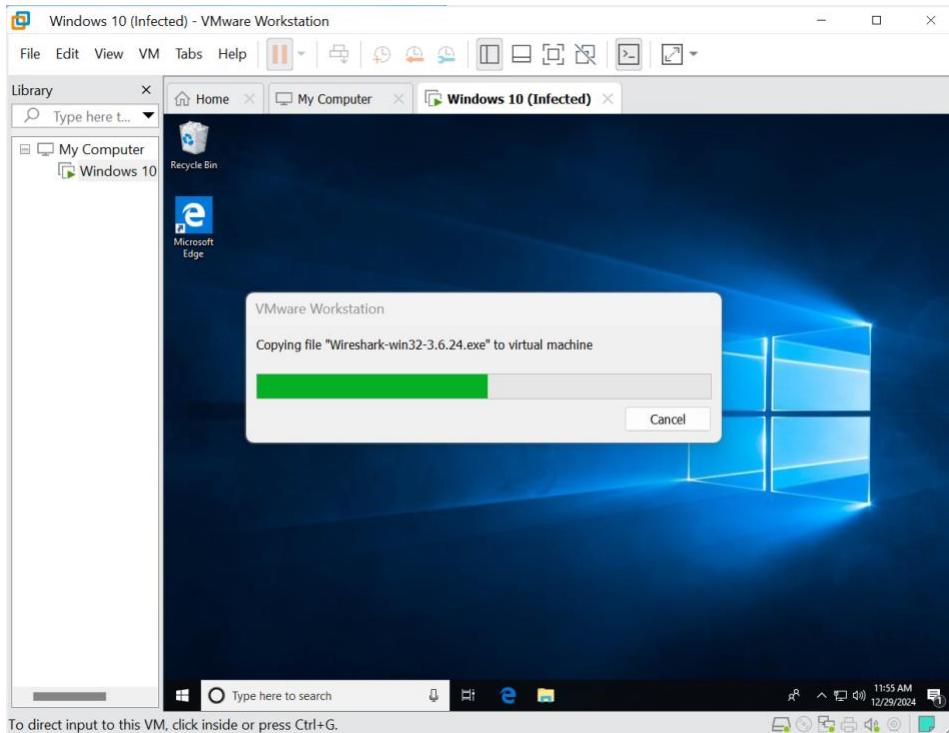


After the snapshot is taken, it is saved to the same folder as the machine, in this case the duplicate of the original virtual machine given.

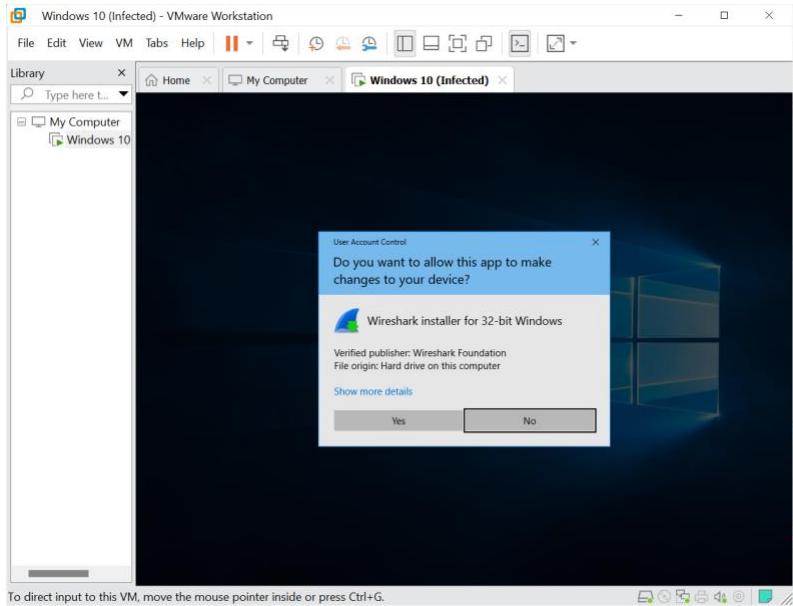


#### 4.4.2 Acquisition of Network Traffic

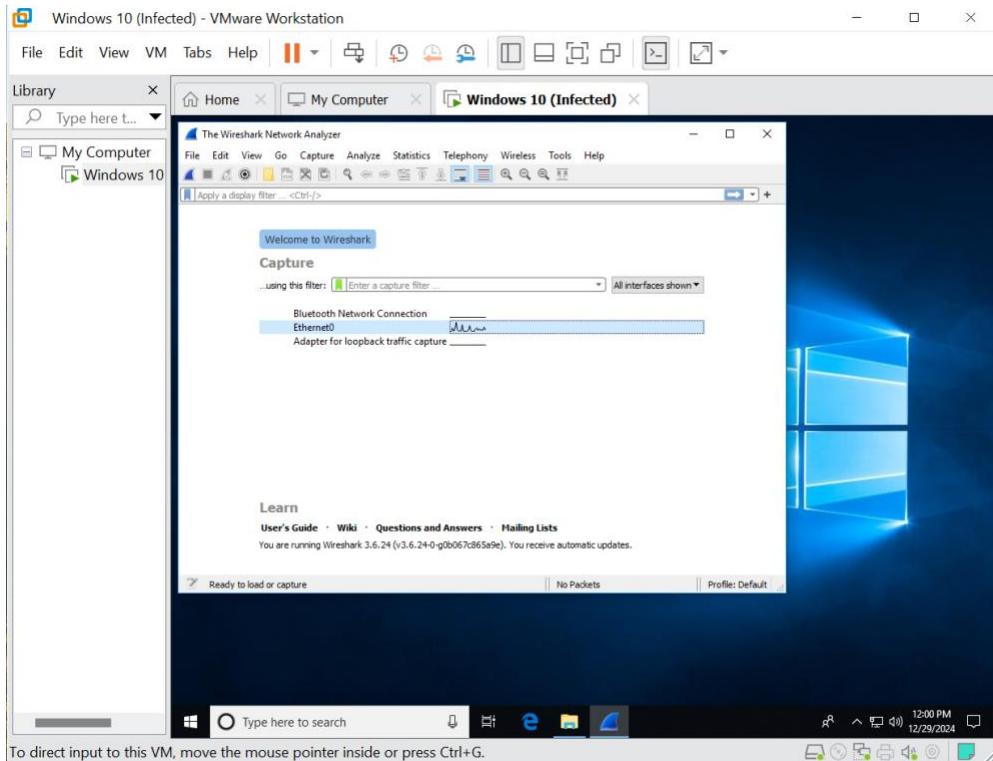
Next, Wireshark would be used to record incoming and outgoing network traffic from the machine. A copy of Wireshark installer is copied to the virtual machine. The 32-bit version of Wireshark is used since the Windows 10 virtual machine is running on 32-bit and not 64-bit.



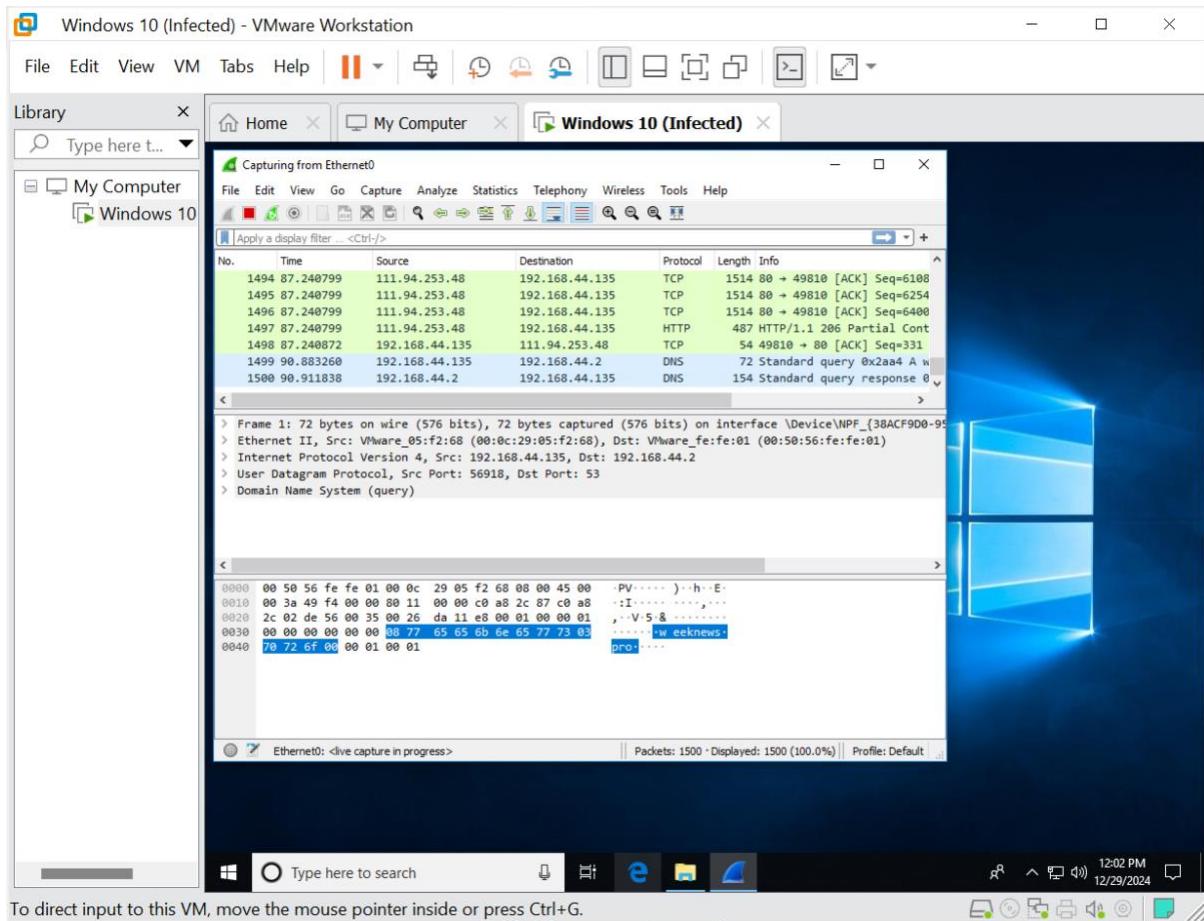
Then Wireshark is installed in the virtual machine using the installer.



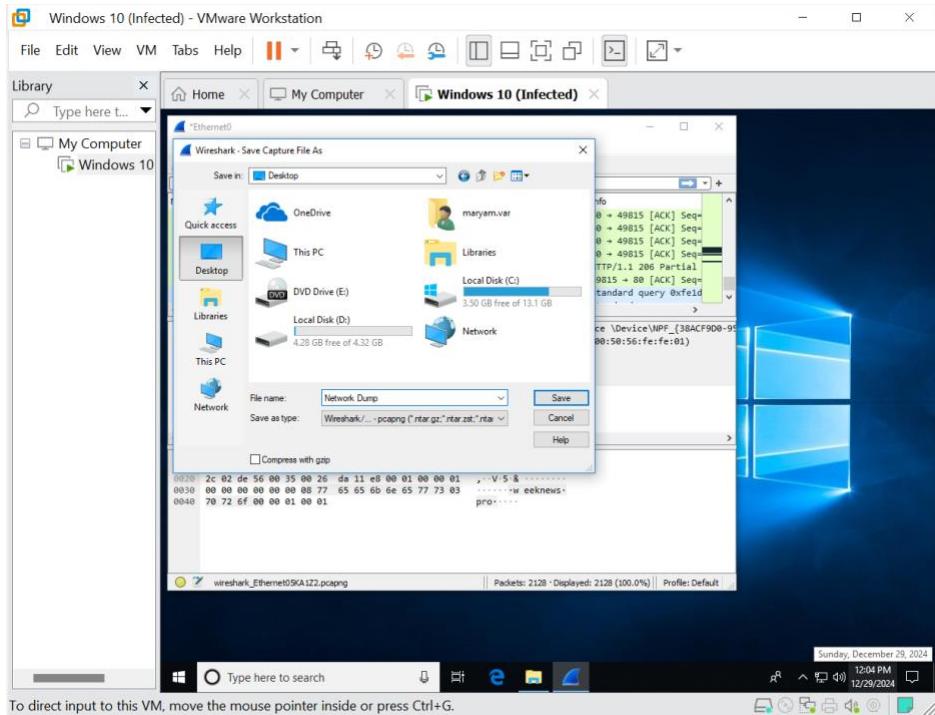
“Ethernet0” is selected, which contains the network traffic going in and out of the machine. Then the network capture is started by clicking on the Wireshark icon which will start to record all traffic from the selected network, in this case “Ethernet0”.



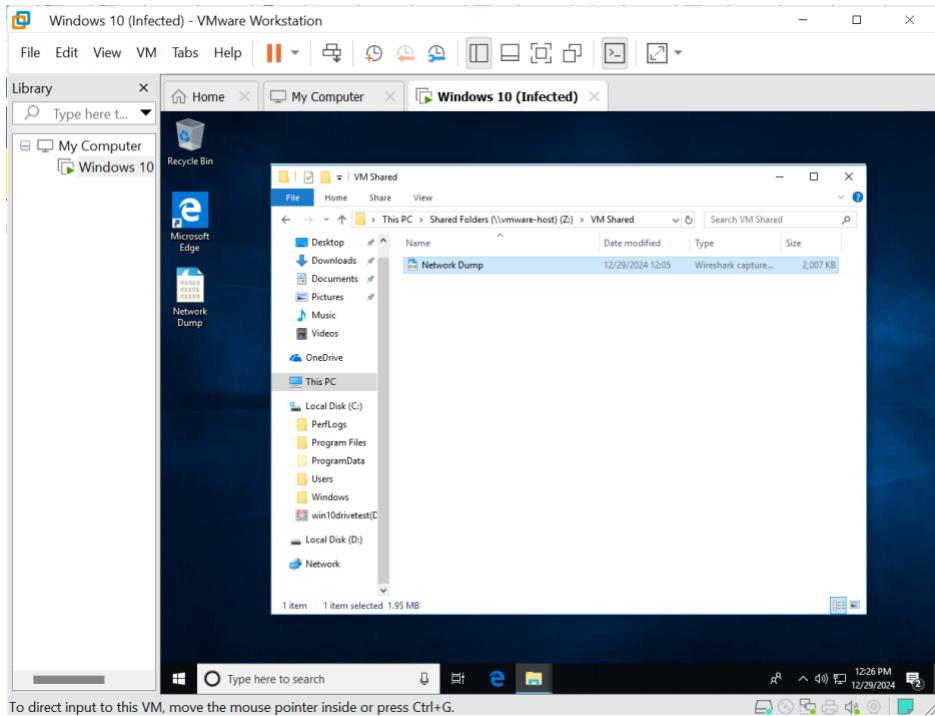
Network traffic would start to appear and be recorded by Wireshark. After some time, the recording is stopped by clicking on the stop button, the red box.



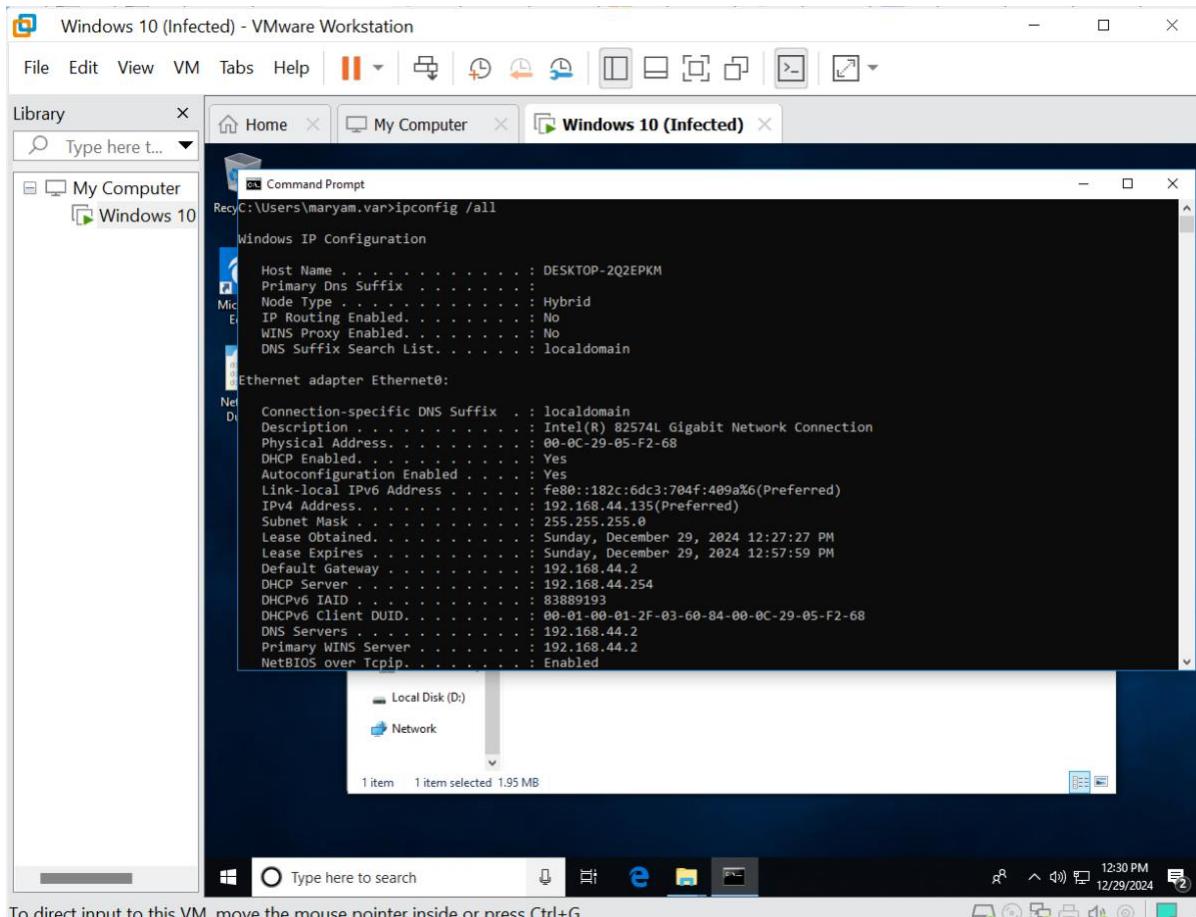
The recording then was saved on the Desktop of the machine.



A shared folder between the virtual machine and the investigator's machine would then be created and connected. The saved recording would be transferred to the shared folder to then be analyse on the investigator's machine.



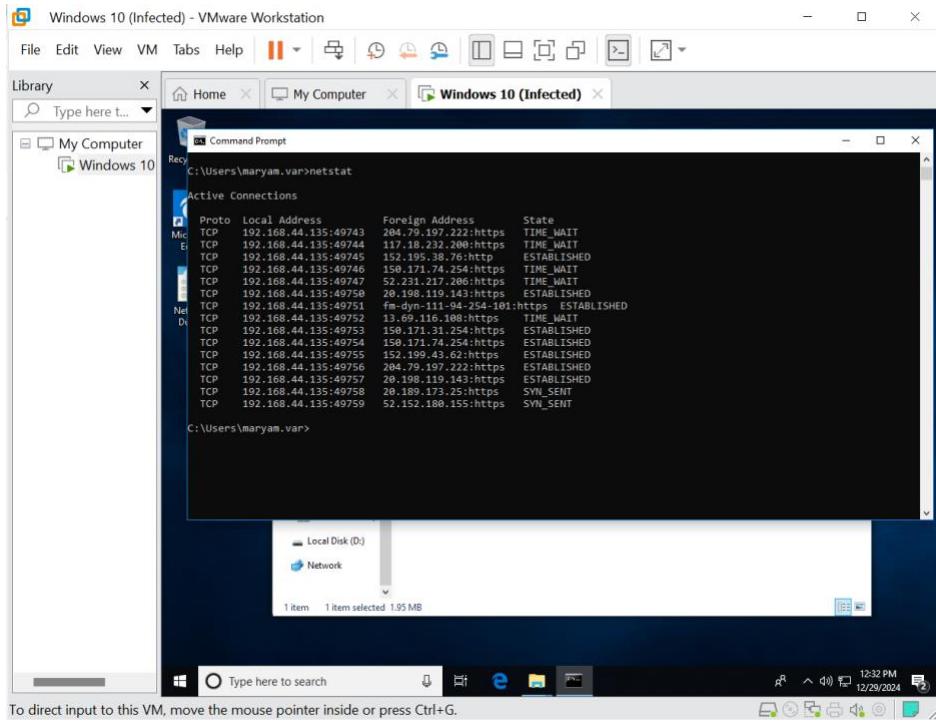
The “ipconfig” command would be done on the live virtual machine to check for its IP address, which would be useful during the analysis of the network traffic.



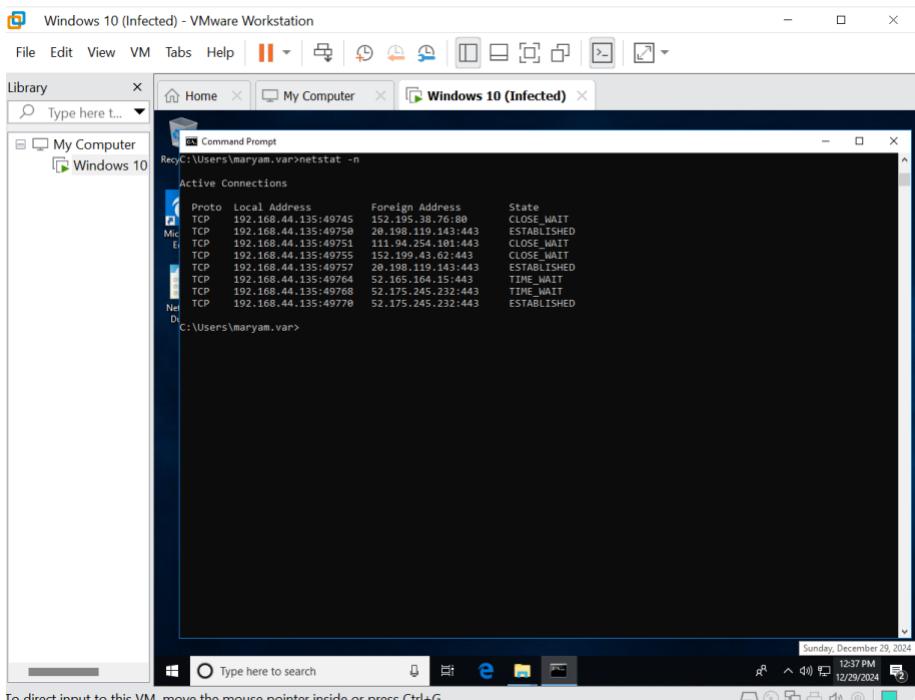
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

In this case the machine's IP address is 192.168.44.135.

The “netstat” command is then done to show all active connections to the machine.



Adding a “-n” flag to the “netstat” command would display the port number instead of the name of the protocol.



# 5.0 Data Analysis

## 5.1 RAM Analysis

The “psscan” command within Volatility is used to scan the memory dump to display all processes running, even hidden processes, during the time the RAM was captured, in this case after boot.

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
2692	920	RuntimeBroker	0x8e6509040	6	-	1	False	2024-12-02 18:53:36.0000000	N/A	Disabled
4488	920	ShellExperienc	0x8e6556a00	17	-	1	False	2024-12-02 18:52:29.0000000	N/A	Disabled
7140	920	SppExtComObj.E	0x8e6572780	6	-	0	False	2024-12-02 18:55:47.0000000	N/A	Disabled
134U	768	svchost.exe	0x8e6699800	36	-	0	False	2024-12-02 18:51:01.0000000	N/A	Disabled
4	0	System	0x8e66ada00	162	-	N/A	False	2024-12-02 18:50:48.0000000	N/A	Disabled
1536	768	vmauthlp.exe	0x8e66dd9c0	2	-	0	False	2024-12-02 18:51:02.0000000	N/A	Disabled
6856	1220	dmclient.exe	0x8e66f6040	8	-	0	False	2024-12-02 18:55:35.0000000	2024-12-02 18:56:31.0000000	Disabled
1396	768	svchost.exe	0x8e66fb780	29	-	0	False	2024-12-02 18:51:02.0000000	N/A	Disabled
464U	3016	vttoolsd.exe	0x8e6703840	6	-	1	False	2024-12-02 18:54:13.0000000	N/A	Disabled
68	4	Registry	0x8e6729a00	3	-	N/A	False	2024-12-02 18:50:13.0000000	N/A	Disabled
3296	768	svcserv.exe	0x8e67f6040	11	-	0	False	2024-12-02 18:51:45.0000000	N/A	Disabled
3016	2240	explorer.exe	0x8e921f400	57	-	1	False	2024-12-02 18:51:55.0000000	N/A	Disabled
5136	768	SearchIndexer.	0x8e9303040	16	-	0	False	2024-12-02 18:52:08.0000000	N/A	Disabled
3556	768	VSSVC.exe	0x8e9304040	6	-	0	False	2024-12-02 18:51:59.0000000	N/A	Disabled
2928	920	dllhost.exe	0x8e936a040	5	-	1	False	2024-12-02 18:52:02.0000000	N/A	Disabled
4488	920	ShellExperienc	0x8e9449a00	17	-	1	False	2024-12-02 18:52:29.0000000	N/A	Disabled
7140	920	SppExtComObj.E	0x8e9476280	6	-	0	False	2024-12-02 18:55:47.0000000	N/A	Disabled
4836	920	RuntimeBroker	0x8e9435680	13	-	1	False	2024-12-02 18:52:51.0000000	N/A	Disabled
2168	768	SecurityHealth	0x8e9474a00	11	-	0	False	2024-12-02 18:51:11.0000000	N/A	Disabled
6900	6856	conhost.exe	0x8e9adba00	8	-	0	False	2024-12-02 18:55:39.0000000	2024-12-02 18:56:33.0000000	Disabled
636	624	cssrss.exe	0x8e9b27a00	18	-	0	False	2024-12-02 18:56:56.0000000	N/A	Disabled
7168	7140	slui.exe	0x8e9b5d040	8	-	0	False	2024-12-02 18:55:48.0000000	2024-12-02 18:56:00.0000000	Disabled
184U	768	svchost.exe	0x8e9c38a00	19	-	0	False	2024-12-02 18:51:03.0000000	N/A	Disabled
2240	894	userinit.exe	0x8e9c81390	8	-	1	False	2024-12-02 18:51:55.0000000	2024-12-02 18:52:51.0000000	Disabled
552	4	smsass.exe	0x8e7998740	4	-	N/A	False	2024-12-02 18:58:48.0000000	N/A	Disabled
704	624	wininit.exe	0x8e9cb2f040	5	-	0	False	2024-12-02 18:58:56.0000000	N/A	Disabled
712	696	cssrss.exe	0x8e9cbfb100	12	-	1	False	2024-12-02 18:58:56.0000000	N/A	Disabled
1060	894	fontdrvhost.exe	0x8e9d09d40	6	-	1	False	2024-12-02 18:58:58.0000000	N/A	Disabled
768	794	services.exe	0x8e9d27940	23	-	0	False	2024-12-02 18:58:56.0000000	N/A	Disabled
796	794	lsass.exe	0x8e9d2e580	9	-	0	False	2024-12-02 18:58:56.0000000	N/A	Disabled
804	696	winlogon.exe	0x8e9d32040	5	-	1	False	2024-12-02 18:58:56.0000000	N/A	Disabled
912	794	fontdrvhost.e	0x8e9d73040	6	-	0	False	2024-12-02 18:58:57.0000000	N/A	Disabled
920	768	svchost.exe	0x8e9d75400	32	-	0	False	2024-12-02 18:58:57.0000000	N/A	Disabled
984	768	svchost.exe	0x8e9dccc580	18	-	0	False	2024-12-02 18:58:57.0000000	N/A	Disabled
1116	894	dmm.exe	0x8e9d12690	11	-	1	False	2024-12-02 18:59:09.0000000	N/A	Disabled
1160	768	svchost.exe	0x8e9d13a00	28	-	0	False	2024-12-02 18:51:00.0000000	N/A	Disabled
1220	768	svchost.exe	0x8e9d152240	108	-	0	False	2024-12-02 18:51:01.0000000	N/A	Disabled
1240	768	svchost.exe	0x8e9d16c80	11	-	0	False	2024-12-02 18:51:01.0000000	N/A	Disabled
5428	3016	MSASCuil.exe	0x8e9d1bb040	5	-	1	False	2024-12-02 18:54:13.0000000	N/A	Disabled
1604	768	WUDFHost.exe	0x8e9d1f980	8	-	0	False	2024-12-02 18:51:02.0000000	N/A	Disabled
1620	4	MemCompression	0x8e9d1f4640	42	-	N/A	False	2024-12-02 18:51:02.0000000	N/A	Disabled
1692	768	svchost.exe	0x8e9d224940	3	-	0	False	2024-12-02 18:51:02.0000000	N/A	Disabled
588	768	spoolsv.exe	0x8e9d2c6a00	14	-	0	False	2024-12-02 18:51:03.0000000	N/A	Disabled
2068	768	svchost.exe	0x8e9d393a00	15	-	0	False	2024-12-02 18:51:08.0000000	N/A	Disabled
2088	768	VGAthService.	0x8e9d3a400	3	-	0	False	2024-12-02 18:51:18.0000000	N/A	Disabled
2132	768	rsasws.exe	0x8e9d3e080	5	-	0	False	2024-12-02 18:51:11.0000000	N/A	Disabled
2124	768	MspHEng.exe	0x8e9d40f040	15	-	0	False	2024-12-02 18:51:11.0000000	N/A	Disabled
2156	768	vttoolsd.exe	0x8e9d418280	8	-	0	False	2024-12-02 18:51:11.0000000	N/A	Disabled
2668	768	dllhost.exe	0x8e9d59100	18	-	0	False	2024-12-02 18:51:27.0000000	N/A	Disabled
2744	768	svchost.exe	0x8e9d59040	5	-	0	False	2024-12-02 18:51:29.0000000	N/A	Disabled
2872	920	WmiPrvSE.exe	0x8e9d659940	15	-	0	False	2024-12-02 18:51:34.0000000	N/A	Disabled
3088	768	svchost.exe	0x8e9d6fa00	4	-	0	False	2024-12-02 18:51:38.0000000	N/A	Disabled
3106	920	WmiPrvSE.exe	0x8e9d6f7640	11	-	0	False	2024-12-02 18:51:39.0000000	N/A	Disabled
3568	3468	MpCmdRun.exe	0x8e9d74800	6	-	0	False	2024-12-02 18:51:48.0000000	N/A	Disabled
3656	2124	MpCmdRun.exe	0x8e9d755600	8	-	0	False	2024-12-02 18:51:48.0000000	N/A	Disabled
4608	920	SearchUI.exe	0x8e9d76c240	26	-	1	False	2024-12-02 18:52:33.0000000	N/A	Disabled
3672	3656	conhost.exe	0x8e9d78d040	4	-	0	False	2024-12-02 18:51:49.0000000	N/A	Disabled
3732	1220	sihost.exe	0x8e9d78380	18	-	1	False	2024-12-02 18:51:49.0000000	N/A	Disabled
3788	768	svchost.exe	0x8e9d7c9a00	25	-	1	False	2024-12-02 18:51:49.0000000	N/A	Disabled
3884	1220	taskhostw.exe	0x8e9d7e040	11	-	1	False	2024-12-02 18:51:50.0000000	N/A	Disabled
3996	768	msdte.exe	0x8e9d822840	13	-	0	False	2024-12-02 18:51:51.0000000	N/A	Disabled
4868	1240	ctfmon.exe	0x8e9d86ff400	10	-	1	False	2024-12-02 18:51:52.0000000	N/A	Disabled
2668	2132	wap.exe	0x8e9d870580	6	-	1	False	2024-12-02 18:51:52.0000000	N/A	Disabled
7248	920	slui.exe	0x8e9d9c800	0	-	1	False	2024-12-02 18:55:57.0000000	2024-12-02 18:55:59.0000000	Disabled
2692	920	RuntimeBroker	0x8e9d96d040	6	-	1	False	2024-12-02 18:53:36.0000000	N/A	Disabled
5752	920	MicrosoftEdge	0x8e9d9cbb0	25	-	1	False	2024-12-02 18:53:19.0000000	N/A	Disabled
4988	768	sppsvc.exe	0x8e9d9f3a00	8	-	0	False	2024-12-02 18:53:03.0000000	N/A	Disabled
2268	920	RuntimeBroker	0x8e9da0a00	3	-	1	False	2024-12-02 18:54:03.0000000	N/A	Disabled
7348	920	dllhost.exe	0x8e9da56680	0	-	0	False	2024-12-02 18:56:19.0000000	2024-12-02 18:56:24.0000000	Disabled
5248	920	ApplicationFr	0x8e9d87880	13	-	1	False	2024-12-02 18:53:08.0000000	N/A	Disabled
5312	920	smartscreen.e	0x8e9da5a400	11	-	1	False	2024-12-02 18:53:09.0000000	N/A	Disabled
5644	920	RuntimeBroker	0x8e9db15040	11	-	1	False	2024-12-02 18:53:16.0000000	N/A	Disabled
6672	920	SkypeHost.exe	0x8e9db53940	8	-	1	False	2024-12-02 18:53:29.0000000	N/A	Disabled
5706	920	RuntimeBroker	0x8e9dc74040	8	-	1	False	2024-12-02 18:53:18.0000000	N/A	Disabled
5772	920	backgroundTask	0x8e9dc4100	7	-	1	False	2024-12-02 18:53:19.0000000	N/A	Disabled
5806	768	TrustedInstall	0x8e9dc9e000	8	-	0	False	2024-12-02 18:53:28.0000000	N/A	Disabled
5788	5136	SearchProtocol	0x8e9dc9a000	7	-	0	False	2024-12-02 18:53:28.0000000	N/A	Disabled
3452	920	Hxfsr.exe	0x8e9dc40400	16	-	1	False	2024-12-02 18:53:32.0000000	N/A	Disabled
5932	920	browser_broker	0x8e9de0d5c0	7	-	1	False	2024-12-02 18:53:25.0000000	N/A	Disabled
6608	920	TiWorker.exe	0x8e9de16000	7	-	0	False	2024-12-02 18:53:26.0000000	N/A	Disabled
4324	920	MicrosoftEdgeC	0x8e9de4a000	15	-	1	False	2024-12-02 18:53:53.0000000	N/A	Disabled
6148	920	backgroundTask	0x8e9de46040	8	-	1	False	2024-12-02 18:53:31.0000000	N/A	Disabled
2216	5136	SearchFilterRn	0x8e9de5c700	4	-	0	False	2024-12-02 18:53:33.0000000	N/A	Disabled
4388	920	MicrosoftEdgeC	0x8e9deef000	14	-	1	False	2024-12-02 18:53:53.0000000	N/A	Disabled
5632	3016	OneDrive.exe	0x8e9df5540	19	-	1	False	2024-12-02 18:54:14.0000000	N/A	Disabled
4284	3016	Microsoft Edge	0x8e9e071a00	12	-	1	False	2024-12-02 18:54:17.0000000	N/A	Disabled
2512	768	svchost.exe	0x8e9e05a000	8	-	0	False	2024-12-02 18:54:29.0000000	N/A	Disabled
5636	920	SystemSettings	0x8e9e0dd540	5	-	1	False	2024-12-02 18:54:21.0000000	N/A	Disabled
6572	1240	dasHost.exe	0x8e9e415480	12	-	0	False	2024-12-02 18:55:09.0000000	N/A	Disabled

The “malfind” command is then used to find processes with injected code which might be an indication of malware. This is then further analyse whether it is malware.

Microsoft Edge is shown which indicates that there is a fake Microsoft Edge in the machine.

The “cmdline” command is then used to analyse processes from the output of “psscan” and “malfind” to find suspicious processes and their location, then their hashes would be acquired from their location using Autopsy to then be analyse if it is malware or not. Only executables deemed suspicious would be displayed along with their directory from the “cmdline” command.

```
PS C:\Users\Reihan DP\Desktop\volatility3> python.exe .\vol.py -f '.\Windows 10 (Infected)-Snapshot1.vmem' windows.cmdline
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
PID      Process Args

2132    rsaws.exe      "C:\Program Files\ProKAward\rsaws.exe"
2060    wap.exe        "C:\Program Files\ProKAward\wap.exe"
4284    Microsoft Edge  "C:\Windows\Temp\Microsoft Edge\Microsoft Edge.exe"
```

The hash of “rsaws.exe” and “wap.exe” was previously captured on previous section, in the section “4.3 Suspicious Files on the Disk”. While the other process is as below:

- Microsoft Edge
  - MD5: b50b31307618955242f3b3f1600759d3
  - SHA-256:  
611db4dfc5952bda3981affe887bccf62ba82922111f545956e4a1693b2b5b68
    - It being in the same folder as wap.dll suggest the fake Microsoft Edge and wap.exe to be relate

## 5.2 Network Analysis

The IP address of the machine is 192.168.44.135 based on the “ipconfig” command done during live acquisition. The saved network dump is open on Wireshark to be analyse.

Network Dump.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.44.135	192.168.44.2	DNS	72	Standard query 0xe800 A weeknews.pro
2	0.144285	192.168.44.135	192.168.44.2	DNS	72	Standard query 0xe800 A weeknews.pro
3	0.391377	192.168.44.2	192.168.44.135	DNS	154	Standard query response 0xe800 No such name A weeknews.pro SOA a0.pro.afilias-nst.info
4	1.785925	111.94.254.101	192.168.44.135	TLSv1.2	85	Encrypted Alert
5	1.786114	192.168.44.135	111.94.254.101	TCP	54	49778 → 443 [ACK] Seq=1 Ack=33 Win=65535 Len=0
6	2.179881	192.168.44.2	192.168.44.135	DNS	154	Standard query response 0xe800 No such name A weeknews.pro SOA a0.pro.afilias-nst.info
7	3.192761	192.168.44.135	111.94.253.48	TCP	54	49783 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
8	3.193650	111.94.253.48	192.168.44.135	TCP	60	80 → 49783 [ACK] Seq=1 Ack=2 Win=64239 Len=0
9	3.194351	192.168.44.135	111.94.253.48	TCP	66	49803 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10	3.204936	111.94.253.48	192.168.44.135	TCP	60	80 → 49803 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11	3.204936	111.94.253.48	192.168.44.135	TCP	60	80 → 49783 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
12	3.205125	192.168.44.135	111.94.253.48	TCP	54	49783 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
13	3.205287	192.168.44.135	111.94.253.48	TCP	54	49803 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14	3.241521	192.168.44.135	111.94.253.48	HTTP	384	GET /d/msdownload/update/software/defu/2024/12/am_delta_694e0748714d3b9436e4cdb3f5855b59da4bc
15	3.242266	111.94.253.48	192.168.44.135	TCP	60	80 → 49803 [ACK] Seq=1 Ack=31 Win=64240 Len=0

```
> Frame 4: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: VMware_fe:fe:01 (00:50:56:fe:fe:01), Dst: VMware_05:f2:68 (00:0c:29:05:f2:68)
> Internet Protocol Version 4, Src: 111.94.254.101, Dst: 192.168.44.135
> Transmission Control Protocol, Src Port: 443, Dst Port: 49778, Seq: 1, Ack: 1, Len: 31
> Transport Layer Security
```

Frame 4 details:

- Frame 4: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF\_{...}
- Ethernet II, Src: VMware\_fe:fe:01 (00:50:56:fe:fe:01), Dst: VMware\_05:f2:68 (00:0c:29:05:f2:68)
- Internet Protocol Version 4, Src: 111.94.254.101, Dst: 192.168.44.135
- Transmission Control Protocol, Src Port: 443, Dst Port: 49778, Seq: 1, Ack: 1, Len: 31
- Transport Layer Security

Hex dump of the selected packet:

```
0000  00 0c 29 05 f2 68 00 50  56 fe 01 08 00 45 00  ..)h P V...E...
0010  00 47 a7 32 00 00 00 06  38 8b 6f 5e fe d0 a8  .G 2...8 o^e...
0020  2c 87 b1 bb c2 72 76 06  c8 2f b3 32 0c e9 50 19 ,...rV ./2-P...
0030  fa fe bb 05 00 00 15 03  03 00 1a 6e 8a 7c 6b 18 .....n[k]...
0040  6d ed 56 75 87 fb bb 0f  cf 38 5b 27 2b 1e dd 1b mVu...8[...
0050  65 69 0c d3 81 ei...
```

Packets: 2128 | Profile: Default

Network Dump.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udpstream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.44.135	192.168.44.2	DNS	72	Standard query 0xe800 A weeknews.pro
2	0.144285	192.168.44.135	192.168.44.2	DNS	72	Standard query 0xe800 A weeknews.pro
3	0.391377	192.168.44.2	192.168.44.135	DNS	154	Standard query response 0xe800 No such name A weeknews.pro SOA a0.pro.afilias-nst.info
6	2.179881	192.168.44.2	192.168.44.135	DNS	154	Standard query response 0xe800 No such name A weeknews.pro SOA a0.pro.afilias-nst.info

```
> User Datagram Protocol, Src Port: 56918, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0xe800
  Flags: 0x0100 Standard query
  Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    weeknews.pro: type A, class IN
      Name: weeknews.pro
      [Name Length: 12]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response Int: 3]
```

Query Name (dns.qry.name), 14 bytes

Packets: 2128 - Displayed: 4 (0.2%) | Profile: Default

Throughout the recorded network traffic, the device was trying to query “weeknews.pro” which was where the executable file “updsto.exe” was downloaded from, based on previous section “4.2 Web History”.

## 5.3 Findings

### 5.3.1 p30download.com and KMSAuto

The website is currently unavailable but a snapshot of the website around the time it was accessed on the machine (2018-05-21) is shown below.

The screenshot shows two versions of a download website, likely p30download.com, captured on May 20, 2018, and December 20, 2018. The top version displays a banner for 'javaz.ir' and offers various software downloads such as Mozilla Thunderbird v52.8.0, DS SIMULIA Insight 2018 x64, and NI LabVIEW 2018 v18.0 x86/x64. The bottom version shows a similar layout but includes a sidebar with news articles about Iran's startup ecosystem, such as 'To Work With Wood Epoxy', 'Google One replaces Google Drive with cheaper plans', and 'The master of success who was sentenced to 10 years in prison for revealing the secrets of the rich'. Both versions have a red button at the bottom left labeled 'Rate: To this site'.

It seems to be a website to download crack versions of software.

At 02:00:27 UTC+8, the entry id 59803 was accessed which looks like below, after translation from Arabic to English.

The user seems to try and download a cracked version of Windows 10.

The name of the file of the cracked version of Windows 10 is “KMSAuto Net 2016 v1.5”. Seconds later, at 02:00:55 UTC+8, a zip file was downloaded from that link called

“KMSAuto.Net.2016.v1.5.0\_p30download.com.zip” which was exported to “Downloads” folder as another folder. Files in that folder have the following result on VirusTotal:

- KMSAuto Net.exe

The screenshot shows the VirusTotal analysis page for the file 0b05ea08028f239b11fc30249bf0aa86966ee4974d03b01bae2ee88befbbef. The main summary indicates 52/72 security vendors flagged it as malicious. The file is identified as KMSAuto Net.exe. The analysis includes sections for DETECTION, DETAILS, RELATIONS, ASSOCIATIONS, BEHAVIOR, and COMMUNITY. The COMMUNITY section shows a score of 53. Below the main summary, there's a table of security vendor analysis results.

Vendor	Threat Category	Family Labels
AhnLab-V3	HackTool/Win32.AutoKMS.C2588419	AliCloud
ALYac	Misc.Keygen	Antiy-AVL
Arcabit	Application.Hacktool.KMSAuto.AV	Avast
AVG	FileRepPup [PUP]	BitDefender
ClamAV	Win.Malware.Agent-6348991-0	CrowdStrike Falcon

- KMSCleaner.exe

The screenshot shows the VirusTotal analysis page for the file a6e2cdc0e9426d50bd72d866bf80e0fb941efb3ae6d1c564d40957d1eb117. The main summary indicates 42/72 security vendors flagged it as malicious. The file is identified as KMSCleaner.exe. The analysis includes sections for DETECTION, DETAILS, RELATIONS, ASSOCIATIONS, BEHAVIOR, and COMMUNITY. The COMMUNITY section shows a score of 17. Below the main summary, there's a table of security vendor analysis results.

Vendor	Threat Category	Family Labels
AhnLab-V3	HackTool/Win32.AutoKMS.C1914739	ALYac
Antiy-AVL	Trojan/Win32.BTSGeneric	Arcabit
ClamAV	Win.Malware.Agent-6418294-0	CrowdStrike Falcon
CTX	Exe.hacktool.autokms	Cylance
Cynet	Malicious (score: 100)	DeepInstinct
Elastic	Malicious (high Confidence)	ESET-NOD32

Both files are malicious with both being flagged as malicious by 52 and 42 security vendors respectively. Both files are under the “kmsauto” family and both are trojan.

### 5.3.2 zw.exe and Final\_Test.pdf

On 2018-05-21 at 02:24:11 UTC+8, a file was downloaded from the link “delmonicositaliansteakhouse.com/zw.exe”. When the website was accessed as it was on around that time it appeared to be only a normal steakhouse.



At the D drive there is a folder called “Shared Docs” which contains a file called “Final\_Test.pdf” which was from that link which means that this is the file downloaded from that link. The file has the following result on VirusTotal:

- Final\_Test.pdf

A screenshot of the VirusTotal analysis interface. The file "Final\_Test.pdf" has a community score of 62/72. The analysis shows 62 out of 72 security vendors flagged it as malicious. The file is a PE executable (EXE) from April 28, 2018. The "DETECTION" tab shows various vendor detections, including AhnLab-V3, ALYac, Arcabit, AVG, BitDefender, and CTX, all marking it as trojan. Other vendors like Alibaba, Avast, Avira, CrowdStrike Falcon, and Cylance also flagged it as malicious. Threat categories include trojan and ransomware. Family labels include ekstak, loki, and ceinject. A "Community" section shows 12 members. A "Join our Community" button is present. A "Do you want to automate checks?" checkbox is visible.

The file is malicious with 62 out of 72 security vendors marking it as malicious. It is a trojan which tries to steal information, based on the “loki” label.

### 5.3.3 online234.com and loder.exe

The website, online234.com, is currently unavailable but a snapshot of the website around the time it was accessed on the machine (2018-05-21) is shown below. It seems to be a normal website for a company called “Human Leadership Resources” in Africa.

WHO WE ARE.  
Human Leadership Resources is the initiative of a highly versatile and professional group of Human Resources and Organizational Development consultants with core understanding of the African business terrain, to offer fit-for-purpose solutions that ensure optimum productivity of the people side of business. The focus of HLR is to ensure the best partnership between people and organizations through the identification, counsel (consultation), design and deployment of the most appropriate subject entities. With a most practical view at Client issues, HLR flexes to the healthiest uttermost to ensure the most fitting solutions at all points in time. Thus in HLR, no one-size fit all! In a nutshell, HLR exists to help client organizations to deliver on their business objectives by designing and enhancing their people strategies, structures and systems to moderate desired success. Paying attention to the realities, HLR adopts a flex to fit approach.

OUR SERVICES.

**LEARNING & DEVELOPMENT**

- Career Development Tools
- Workforce Development Consulting
- Coaching & Mentoring
- In-Company Training

**RECRUITMENT**

- Partnership Recruitment Services
- Turnkey Recruitment
- Designing Recruitment Strategies/systems

**ASSESSMENT SERVICES**

- Aptitude and Ability Assessment
- Personality and Behavioural Assessments
- Assessment and Development Centers

At 02:27:08 UTC+8, on the "Downloads" folder a file called “loder.exe” was downloaded from that link. The file has the following result on VirusTotal:

- Loder.exe

Community Score: 57 / 72

57/72 security vendors flagged this file as malicious

3128ef59736fdcd60469bae3d586990e54ec1b98d8759360512855174ef8927  
RtlUpd.EXE  
pefile assembly persistence detect-debug environment

Size: 493.00 KB | Last Analysis Date: 25 days ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: Trojan.Droste/MSIL

Threat categories: Trojan dropper Family labels: stealer mail gen2

Security vendors' analysis

AhnLab-V3	Win-Trojan/MSIL/KryptEx.L!e	Allibaba	Trojan/Spy/MSIL/Stealer.e0d41625
AliCloud	Trojan/spy/MSIL/Stealer.mq	AIYac	Trojan.GenericKD.40263707
Anti-ML	Trojan/Spy/MSIL/Gen	Arcabit	Trojan.Generic.D266601B
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Dropper.Gen2	BitDefender	Trojan.GenericKD.40263707
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Eic:trojan.stealer

The more common name for that executable file is “RtlUpd.EXE”. It is a malicious file with 57 out of 72 security vendors marking it as malicious. It is a dropper which means that it is used to transport and execute other malware on the machine.

### 5.3.4 KMPlayer.exe

On 2018-05-21 at 02:27:51 UTC+8, an executable file called “KMPlayer\_4.2.2.10.exe” is downloaded from the website “kmplayer.en.softonic.com”. The website is still available now but a screenshot of the website at around that time is shown below.

The screenshot shows the KMPlayer software page on softonic.com. At the top, there's a navigation bar with links for APPS, GAMES, ARTICLES, VIDEOS, DEALS, and SOLUTIONS. A search bar is also present. The main content area features a large image of the KMPlayer interface with floating letters spelling 'KMPlayer'. Below this, there's a brief description: "Excellent free multi-format media player. KMPlayer is a lightweight audio and video player for Windows that supports a wide range of different file formats, including AVI, ASF, WMV, AVS, FLV, and MKV, and many more. View full description". To the right, there's a "Free Download" button and a "Rate It!" button. On the far right, there's a sidebar titled "Top downloads" listing other media players like VLC media player, Adobe Flash Player, VidMate, and Format Factory. The KMPlayer page also includes sections for PROS (flexible extensibility) and CONS (none mentioned).

It seems to be a website discussing KMPlayer and the place to download the software. KMPlayer seems to be a media player to play audio and video with a range of formats. At 10:27:54 UTC+8, the file is created in the “Downloads” folder with the same name, “KMPlayer\_4.2.2.10.exe”. The file has the following result on VirusTotal:

- KMPlayer\_4.2.2.10.exe

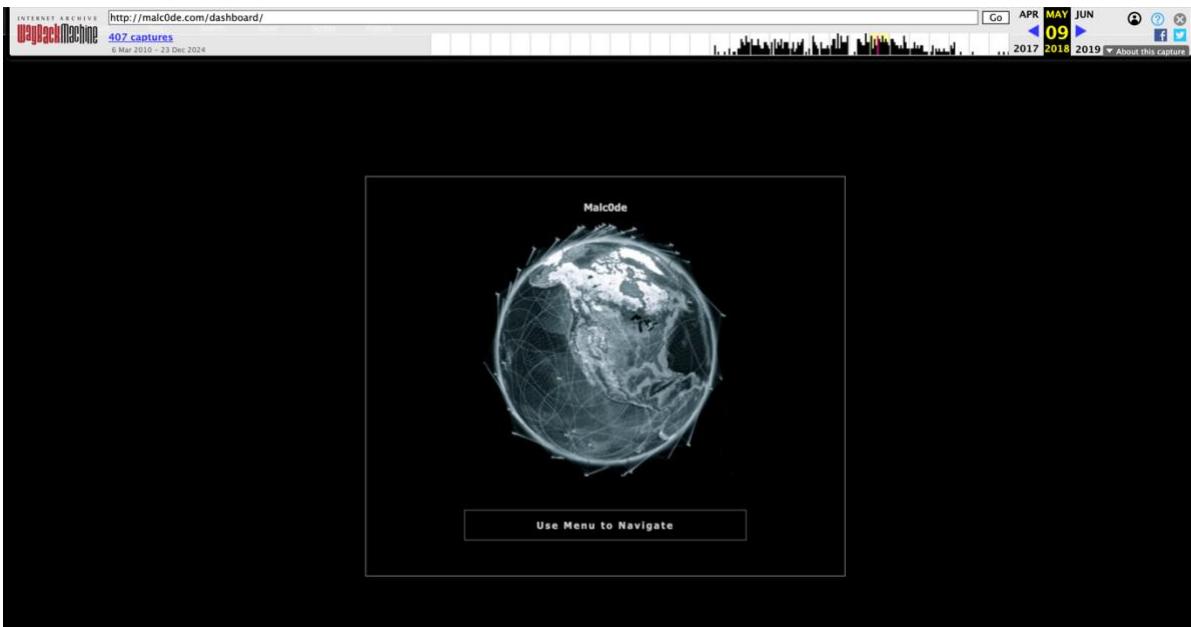
The screenshot shows the VirusTotal analysis page for the file 7383bd44fc30ed8f7e07c387e3dcbe5f54269a4121401ee9b726d8c25ea4ce22. The page indicates that 1/68 security vendors flagged the file as malicious. The file size is 35.01 MB and it was last analyzed 1 minute ago. The analysis table shows results from various vendors:

Virus Vendor	Result	Notes
DrWeb	Program.Kmplayer.2	Acronis (Static ML)
AhnLab-V3	Undetected	Alibaba
AliCloud	Undetected	AVG
Anti-AVL	Undetected	Arcabit
Avast	Undetected	Baidu
Avira (no cloud)	Undetected	Bkav Pro
BitDefender	Undetected	

The file seems to be safe and non-malicious as it is only being flagged by 1 vendor out of 68. However, further research shows that it might be adware, which is a form of malware in which unwanted advertisements pop up on the machine.

## 5.3.5 malc0de.com

The website seems to be unavailable but a snapshot of the website around the time it was accessed on the machine (2018-05-21) is shown below.



When the globe on the center is clicked it leads to the Twitter account of its founder.

A screenshot of the Twitter profile for the user "malc0de" (@malc0de). The profile picture is a black hole against a starry background. The bio states: "Owner of malc0de.com an updated database of domains hosting malicious executables." The stats show 1,443 tweets, 352 following, 12.8K followers, and 537 likes. The "Follow" button is visible. The timeline displays two tweets. The first tweet is a retweet from "Fumik0\_ @fumik0\_" dated 25 Dec 2019, which reads: "Let's play (again) with Predator the thief fumik0.com/2019/12/25/let...". The second tweet is a retweet from "Kahu Security @kahusecurity" dated 5 Jul 2019, showing a graphic for "PREDATOR SOFTWARE". On the right side of the screen, there are sections for "New to Twitter?", "Sign up", and "You may also like".

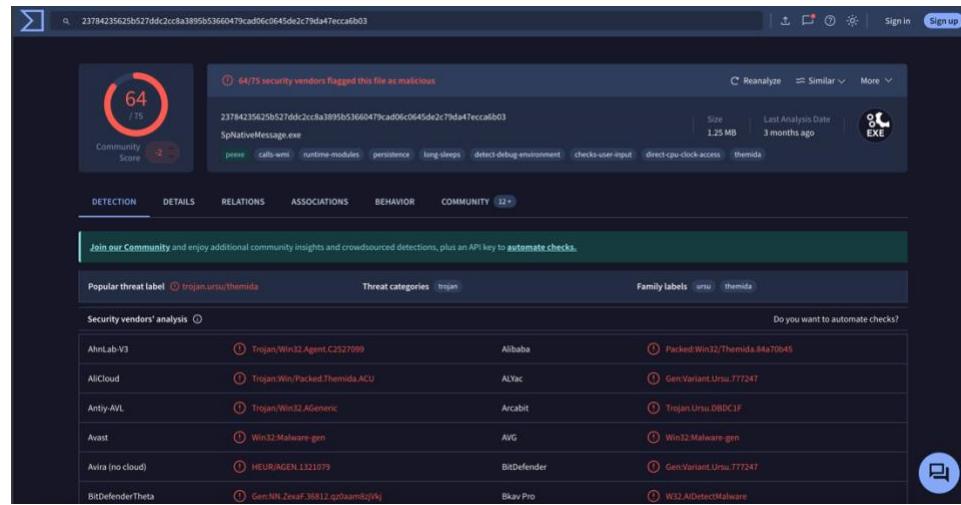
Based on the twitter account, malc0de is a database of domains that host malicious executable files. Previously analysed websites and links that appear to be legitimate but could be used to download malicious executable files might be part of this database, but there is no definite proof of it.

However, the domain “weeknews.pro” is definitely a part of this database which was used to download the executable file “updsto.exe” since, at 07:03:10 UTC+8, the malc0de database was search for “weeknews.pro” and the executable file “updsto.exe” was downloaded from the “weeknews.pro” website.

### 5.3.6 weeknews.pro and updsto.exe

The website is currently unavailable and there are no archives on the website. This website is a domain which hosts malicious files, in this case it is “updsto.exe”, and is part of the malc0de database. The “updsto.exe” executable file is downloaded from the weeknews.pro website and is found in the “Downloads” folder. The file has the following result on VirusTotal:

- updsto.exe



The more common name for that executable file is “SpNativeMessage.exe” and the file is malicious with 64 out of 75 security vendors marking it as malicious. It is a trojan which means that it is a malware that disguises itself as legitimate software.

### 5.3.7 Microsoft Edge.exe

A fake Microsoft Edge was found running on the RAM at the moment it was captured. It is in the “Temp” folder in the “Windows” directory. The file has the following result on VirusTotal:

- Microsoft Edge

The screenshot shows the VirusTotal analysis interface for the file 611db4dfc5952bda3981afe887bccf62ba82922111f545956e4a1693b2b5b68. The file is identified as Microsoft Edge.exe. The 'DETECTION' tab is selected, showing the following table of security vendor analysis results:

Security vendor	Analysis	Threat category
Anti-AVL	Trojan/Win32.Agent	Trojan.Malware.300983.susgen
Palo Alto Networks	Generic.ml	Malicious.high.ml.score
Trellix (ENS)	Artemis/B50B31307618	TScope.Trojan.Delf
Acronis (Static ML)	Undetected	Undetected
Alibaba	Undetected	Undetected
ALYac	Undetected	Undetected

The file could be malicious as it is flagged by 6 out of 71 security vendors. It is a trojan which is a malicious software that hides itself by pretending to be a legitimate program, in this case Microsoft Edge.

### 5.3.8 ProKAward

There is a folder in “Program Files” called “ProKAward” which contains several files. Based on the “wap.ini” and “wap.exe.manifest”, this seems to be a keylogger called “Award Keylogger Pro”. Keylogger is a form of malware which monitors the infected machine and records and transmits keystrokes made by the user of the infected machine to the threat actor. Files in this folder have the following result on VirusTotal:

- wap.exe

The screenshot shows the VirusTotal analysis page for the file 9c8d0a43aa95e439cedeb69cacfb3c606381bfd6745111c5cfe73a38af9ae38. The top bar indicates a community score of 42/72. The main summary panel shows the file name as 9c8d0a43aa95e439cedeb69cacfb3c606381bfd6745111c5cfe73a38af9ae38, type as wap.exe, and status as peexe idle. It also shows the file size as 3.91 MB and the last analysis date as 28 days ago. The VirusTotal logo is present.

**Community Score:** 42 / 72

**Detections:** 42/72 security vendors flagged this file as malicious

**File Details:** 9c8d0a43aa95e439cedeb69cacfb3c606381bfd6745111c5cfe73a38af9ae38  
wap.exe  
peexe idle  
Size: 3.91 MB | Last Analysis Date: 28 days ago

**Threat Categories:** trojan, pua, virus

**Family Labels:** keylogger, awardkeylogger, monitor

**Security Vendors' Analysis:**

Vendor	Label	Description
Alibaba	RiskWare Win32/AwardKeylogger.b3033...	
Anti-AVL	Trojan Win32.SGeneric	
AVG	Win32.Malware-gen	
CrowdStrike Falcon	Win/grayware_confidence_100% (W)	
Cylance	Unsafe	
DeepInstinct	MALICIOUS	
AllCloud	Spy Win Keylogger	
Avast	Win32.Malware-gen	
Bkav Pro	W32.Common.B9AA02B4	
CTX	Exe.Keylogger.generic	
Cynet	Malicious (score: 100)	
DrWeb	Program.Monitor.3340	

- rsaws.exe

The screenshot shows the VirusTotal analysis page for the file 1b84356e23933ecb201460a7c4fe491123831764a7e125e08ceae3dc3e5c9b64. The top bar indicates a community score of 37/74. The main summary panel shows the file name as 1b84356e23933ecb201460a7c4fe491123831764a7e125e08ceae3dc3e5c9b64, type as rsaws.exe, and status as peexe detect-debug-environment long-sleeps checks-disk-space. It also shows the file size as 96.00 KB and the last analysis date as 3 months ago. The VirusTotal logo is present.

**Community Score:** 37 / 74

**Detections:** 37/74 security vendors flagged this file as malicious

**File Details:** 1b84356e23933ecb201460a7c4fe491123831764a7e125e08ceae3dc3e5c9b64  
rsaws.exe  
peexe detect-debug-environment long-sleeps checks-disk-space  
Size: 96.00 KB | Last Analysis Date: 3 months ago

**Threat Categories:** trojan.awardkeylogger/monitor

**Family Labels:** awardkeylogger, monitor, filerepmalware

**Security Vendors' Analysis:**

Vendor	Label	Description
Alibaba	RiskWare Win32/AwardKeylogger.6237fbf3	
Anti-AVL	RiskWare Monitor  Win32.AwardKeylogger	
AVG	FileRepMalware [Misc]	
Cylance	Unsafe	
Elastic	Malicious (moderate Confidence)	
Gridinsoft (no cloud)	Malware.Win32.GenericMC.cc	
AllCloud	Trojan(spy) Win Occamy.CSH	
Avast	FileRepMalware [Misc]	
Bkav Pro	W32.AIDetectMalware	
DeepInstinct	MALICIOUS	
Google	Detected	
Ikarus	Trojan.Win32.Agent	

- filedat.dat

The screenshot shows the VirusShare analysis page for the file `filedat.dat`. The top header includes the file's SHA-1 hash: `01149f144278775c79c61499355a79dcfe8eb67ea9b91fc6413d56ec2070f6`, a "Community Score" of `59 / 75`, and a note that `59/75 security vendors flagged this file as malicious`. The file is identified as `filedat.dat` with a `peexe` file type. The analysis shows a size of `156.00 KB` and a last analysis date of `4 months ago`. The file is categorized as `EXE`. Below the header, tabs for `DETECTION`, `DETAILS`, `RELATIONS`, `BEHAVIOR`, and `COMMUNITY` are visible, with `DETECTION` being the active tab. A green banner encourages joining the community. The `Popular threat label` is `trojan.grafor/keylogger`, and the `Threat categories` include `trojan`, `downloader`, and `stealer`. The `Family labels` are `grafor`, `keylogger`, and `stealer`. The `Security vendors' analysis` section lists various vendors and their findings:

Vendor	Findings	Vendor	Findings
AhnLab-V3	<span>Malicious</span> Trojan/Win32.Agent.R129445	Alibaba	<span>Malicious</span> TrojanDownloader.Win32.KeyLogger.9c...
AliCloud	<span>Malicious</span> Trojan/downloader!Win/KeyLogger.o	ALYac	<span>Malicious</span> Gen.Variant.Grafor.123377
Anti-AVL	<span>Malicious</span> Trojan/Win32.AGeneric	Arcabit	<span>Malicious</span> Trojan.Grafor.D1E1F1
Avast	<span>Malicious</span> Win32.Malware-gen	AVG	<span>Malicious</span> Win32.Malware-gen
Avira (no cloud)	<span>Malicious</span> TR/Grafor.123377.32	BitDefender	<span>Malicious</span> Gen.Variant.Grafor.123377
Bkav Pro	<span>Malicious</span> W32.Common.8446DEB0	ClamAV	<span>Malicious</span> Win.Trojan.Agent.1368131

- Builder.exe

The screenshot shows the VirusShare analysis page for the file `Builder.exe`. The top header includes the file's SHA-1 hash: `2bd25e1f11247fb58536e808e01dfec293497a4e96bf51a0e61d242927e9e9d0`, a "Community Score" of `4 / 68`, and a note that `4/68 security vendors flagged this file as malicious`. The file is identified as `Builder.exe` with a `peexe` file type. The analysis shows a size of `1.42 MB` and a last analysis date of `3 months ago`. The file is categorized as `EXE`. Below the header, tabs for `DETECTION`, `DETAILS`, `RELATIONS`, `BEHAVIOR`, and `COMMUNITY` are visible, with `DETECTION` being the active tab. A green banner encourages joining the community. The `Popular threat label` is `trojan.keylogger`, and the `Threat categories` include `trojan`. The `Family labels` are `keylogger`. The `Security vendors' analysis` section lists various vendors and their findings:

Vendor	Findings	Vendor	Findings
AliCloud	<span>Malicious</span> Trojan/spy!Win/Keylogger_JZ	Huorong	<span>Malicious</span> TrojanSpy/Keylogger_J
SecureAge	<span>Malicious</span>	Webroot	<span>Malicious</span> System.Monitor.Award.Keylogger
Acronis (Static ML)	<span>Undetected</span>	AhnLab-V3	<span>Undetected</span>
Alibaba	<span>Undetected</span>	ALYac	<span>Undetected</span>
Anti-AVL	<span>Undetected</span>	Arcabit	<span>Undetected</span>
Avira (no cloud)	<span>Undetected</span>	Baidu	<span>Undetected</span>

All these files are malicious and part of the “awardkeylogger” family. Both “wap.exe” and “rsasws.exe” are found in the RAM after the computer boots up. This means that this keylogger monitors the infected machine as well as records keystrokes made directly after the machine is turned on. Even if the machine is turned off, once it is turned back on this malware would automatically execute.

## 6.0 References

*Common hash algorithms (MD5, SHA-1, SHA-256, etc.) - Cryptography.* (n.d.).

<https://noobtomaster.com/cryptography/common-hash-algorithms-md5-sha-1-sha-256-etc/>

GeeksforGeeks. (2024, May 29). *What is Virtual Hard Disk?* GeeksforGeeks.

<https://www.geeksforgeeks.org/what-is-virtual-hard-disk/>

*How it works.* (n.d.). VirusTotal. <https://docs.virustotal.com/docs/how-it-works>

*LOKI - Threat Encyclopedia / Trend Micro (US).* (n.d.).

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/loki#:~:text=Loki%20is%20an%20information%20stealer%20first%20detected%20in,credentials%2C%20disabling%20notifications%2C%20intercepting%20communications%2C%20and%20data%20exfiltration.>

Malwarebytes. (2024a, March 29). *Adware - What is Adware and How to Remove Adware.*

<https://www.malwarebytes.com/adware>

Malwarebytes. (2024b, July 26). *Keylogger / What is a Keylogger? How to protect yourself.*

<https://www.malwarebytes.com/keylogger>

Rich, D. (2022, October 11). *How to use the Get-FileHash PowerShell CMDlet.* ATA Learning.

<https://adamtheautomator.com/get-filehash/>

*Search - Threat Encyclopedia / Trend Micro (US).* (n.d.).

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/search/ekstak>

The Volatility Foundation. (2024, December 15). *Home of the Volatility Foundation / Volatility Memory Forensics - The Volatility Foundation - Promoting accessible memory analysis tools within the memory Forensics community.* The Volatility Foundation - Promoting

Accessible Memory Analysis Tools Within the Memory Forensics Community.

<https://volatilityfoundation.org/>

*TROJ\_URSU.TIEADAJ* - Threat Encyclopedia / Trend Micro (US). (n.d.).

[https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj\\_urso.tieadaj](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_urso.tieadaj)

*Understanding dropper Malware: Types, examples, detection, and prevention.* (2024, September 24). Perception Point. <https://perception-point.io/guides/malware/understanding-dropper-malware-types-examples-detection-and-prevention/>

*VirusTotal.* (n.d.). VirusTotal. <https://www.virustotal.com/>

*Wayback machine.* (n.d.). <https://web.archive.org/>

*Whois.com - domain names & identity for everyone.* (n.d.). <https://www.whois.com/>