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.
  - **loder.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

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)

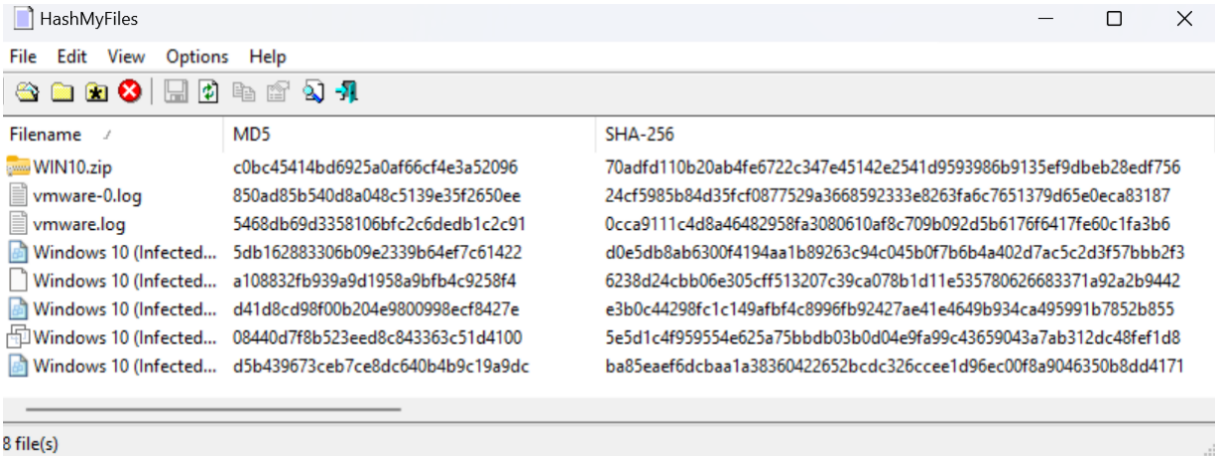
VirusTotal is a free online website which has over 70 antivirus scanners. It is able to scan files, hashes, and URL for potentially being malicious or malware.

4.0 Data Acquisition

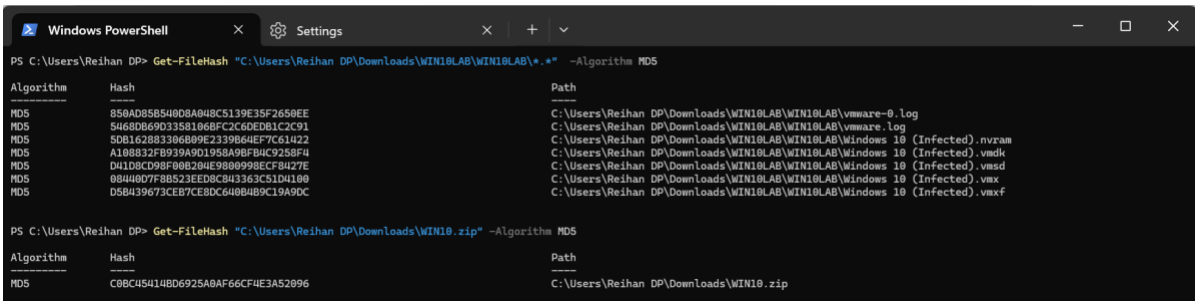
Before beginning the investigation, it is important to ensure the integrity of the evidence. A duplicate of the original file must be created to ensure that the original evidence remains untouched and will not be altered, preventing the risk of the evidence being modified or corrupted. Verify that the 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.

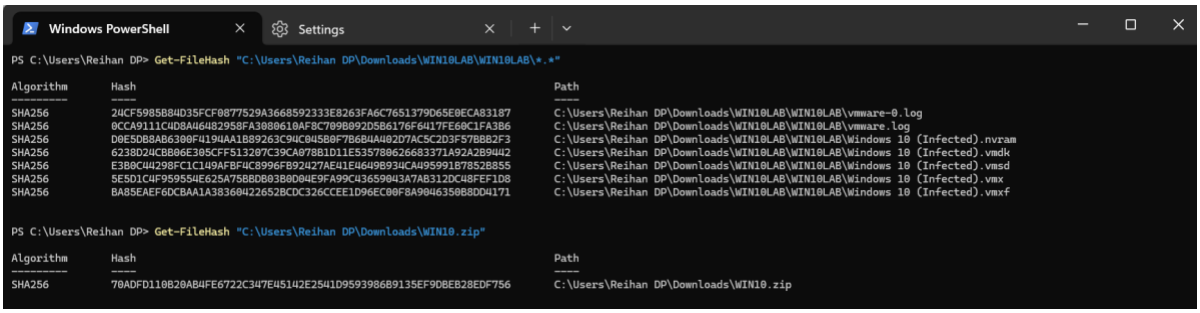
The hash algorithms MD5 and SHA-256 would be used when comparing files to the original files since these are common hash algorithms used for integrity check. The original files contain the original "WIN10.zip" zip file, and the "Windows 10 (Infected).vmdk" virtual machine disk file along with other files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

Original Evidence:



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.

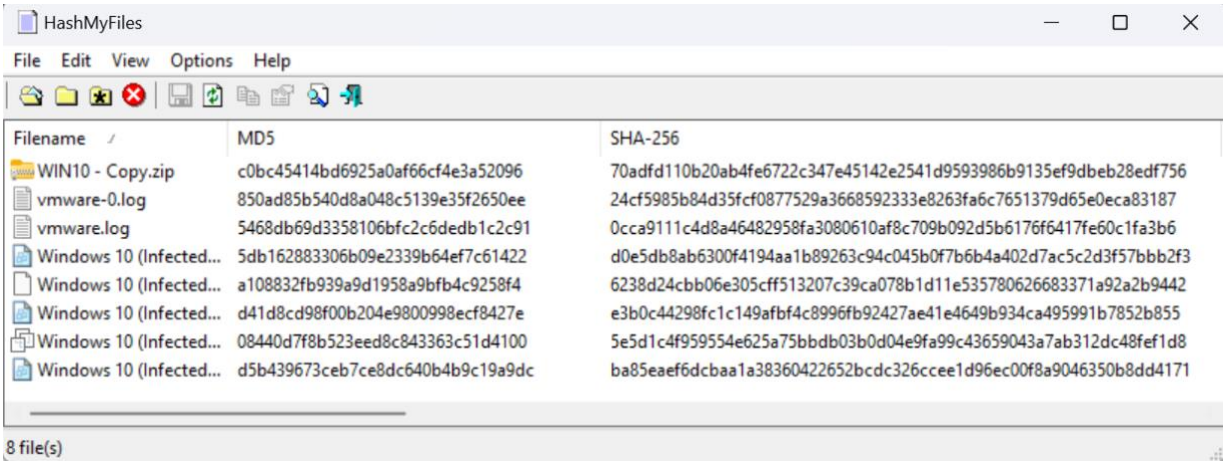




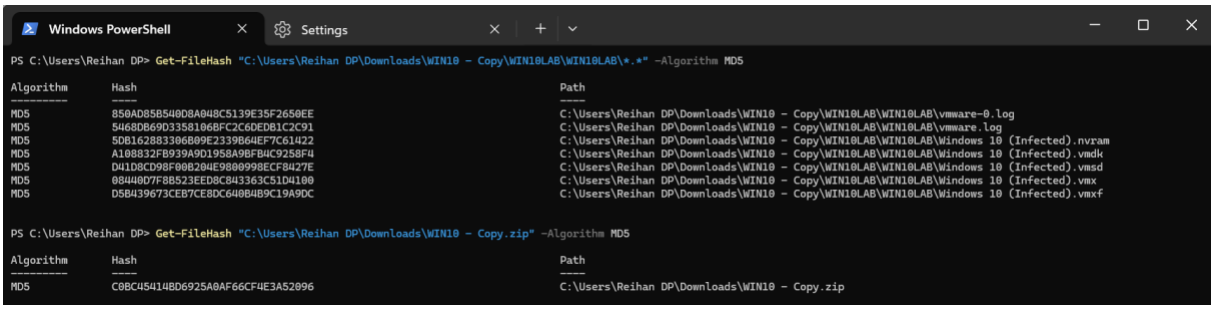
Above are also screenshots of the original zip file and files within it, and their respective MD5 and SHA-256 hashes, generated using the command “Get-FileHash” from Windows PowerShell.

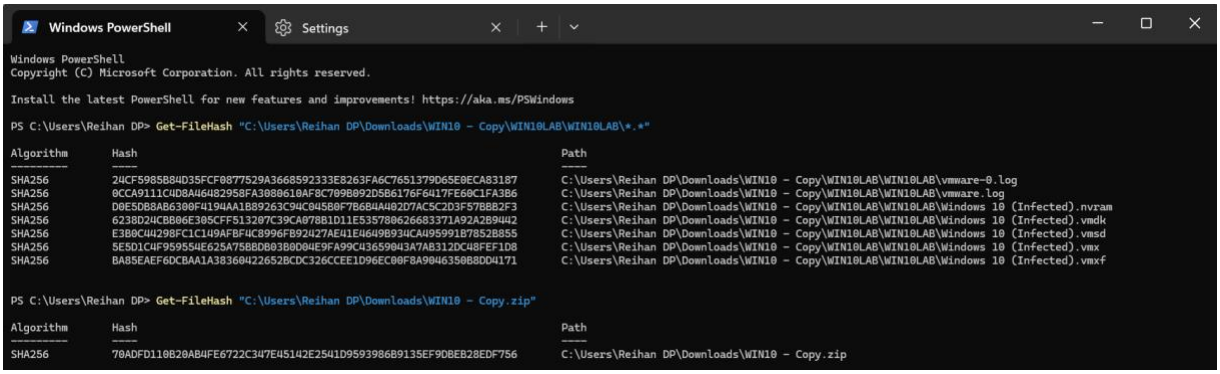
Hashes generated from both HashMyFiles and the “Get-FileHash” command are the exact same. Note that the case of letters in the generated hash value does not matter, this means that for example “a” is equal to “A”.

Duplicate of the Evidence:



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.



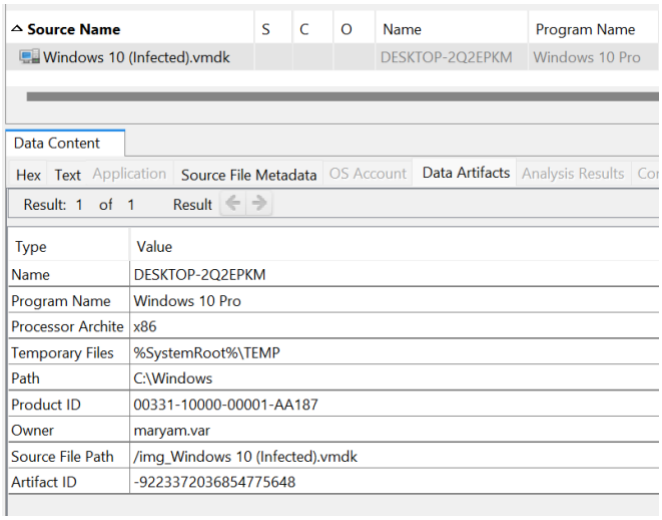


Above are also screenshots of the duplicate files with their respective MD5 and SHA-256 hashes, generated using the command “Get-FileHash” from Windows PowerShell.

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-2Q2EPKM	Windows 10 Pro

Data Content

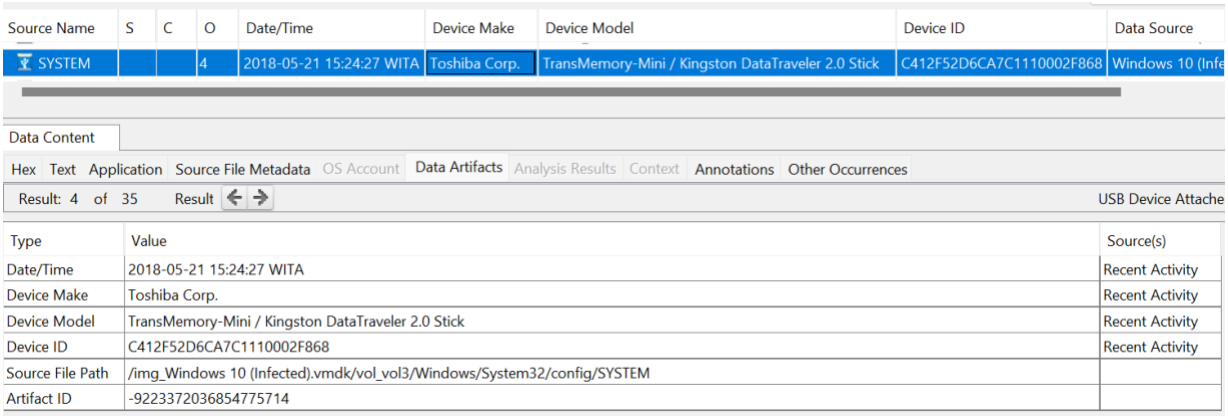
Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Cor

Result: 1 of 1 Result

Type	Value
Name	DESKTOP-2Q2EPKM
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-2Q2EPKM
- 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 (Infe

Data Content

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

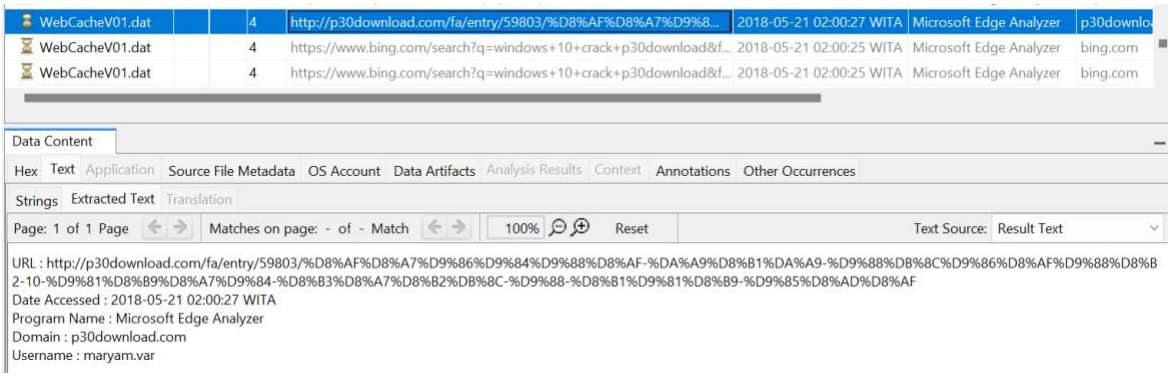
Result: 4 of 35 Result USB Device Attache

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

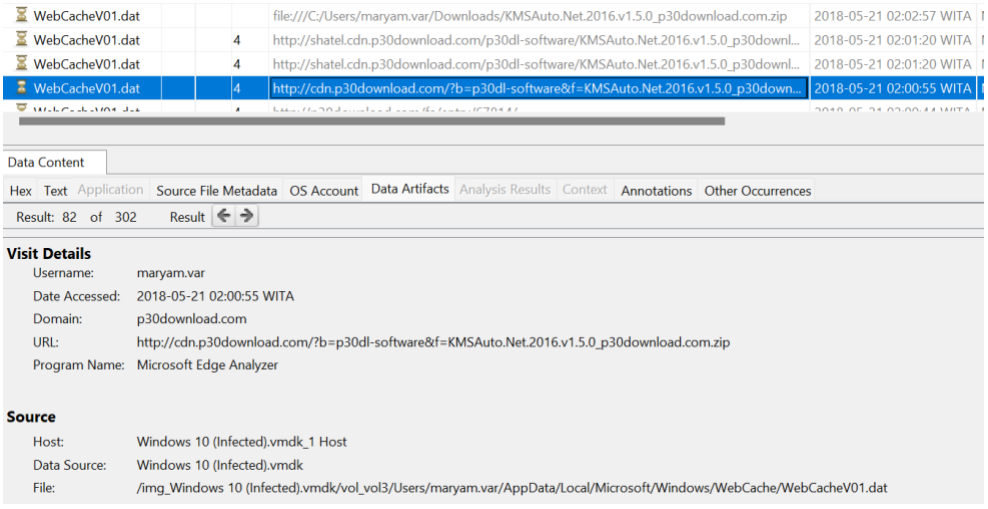
4.2 Web History

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.



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

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



- 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

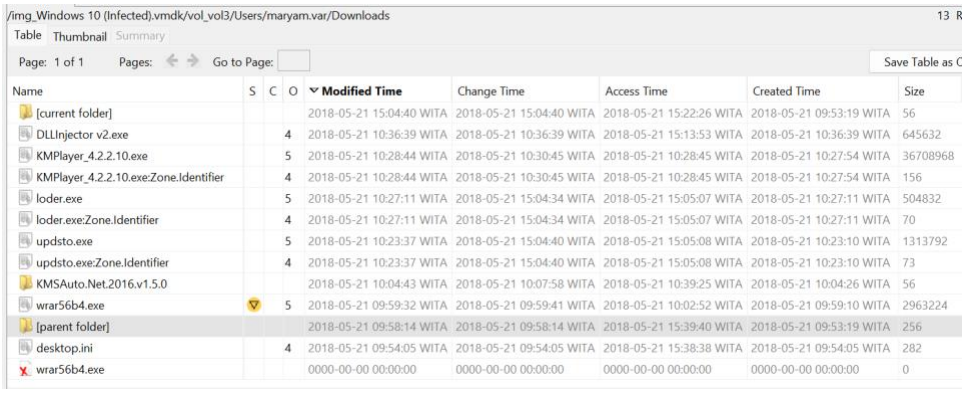
WebCacheV01.dat		4	http://www.youtube.com/embed/h5QWbURNEpA?feature=player_detailpage	2018-05-21 07:39:34 WITA

- 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.

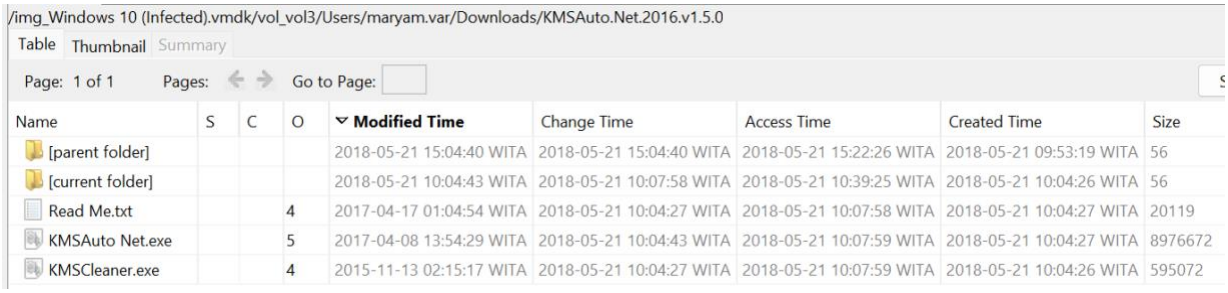
In the “Downloads” folder of the user maryam.var, the following were found, and their details.



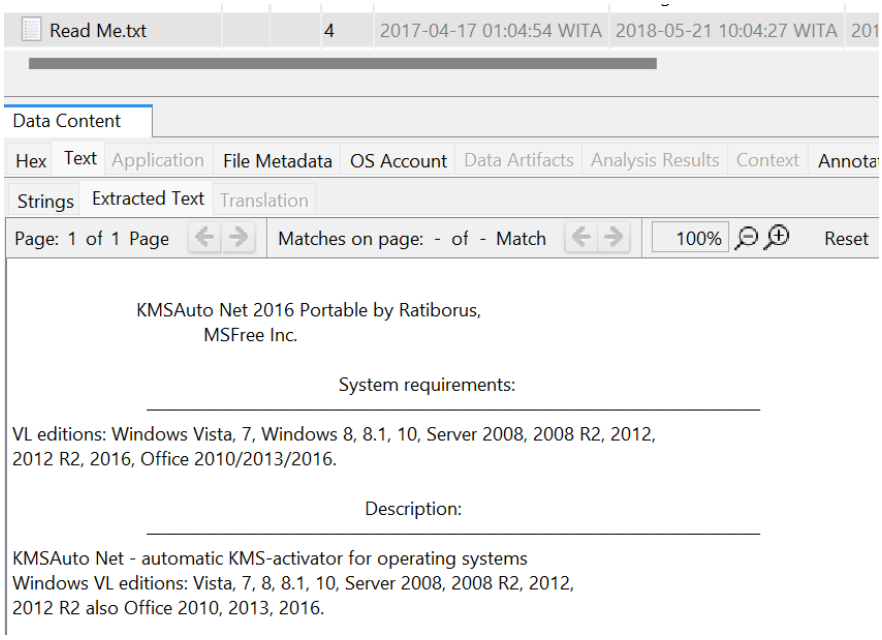
- DLLInjector v2.exe
    - MD5: 0a5a1030beba8cba4f283a0636231ee1
    - SHA-256: 0db7dddd89fc145ab250c69c543a0b0ccc5bce53d017f2faf63d9a115a011d26
- KMPlayer_4.2.2.10.exe
    - MD5: af7abbbc2a5949f8b21c8efaaf68ee0c
    - SHA-256: 7383bd44fc30ed8f7e07c387e3dcbef554269a4121401ee5b726dac25ea4ce22
    - ReferrerUrl=http://www.kmplayer.com/ HostUrl=http://cdn.kmplayer.com/KMP/Download/release/chrome/4.2.2.10/KMPlayer_4.2.2.10.exe
- loder.exe
    - MD5: 0ae466fc76575fbc2d42cdba9788be1e
    - SHA-256: 3128ef59736fdcd604698ae3d5869909e54ec1b98d8759360512855174ef8927
    - HostUrl=http://online234.com/hlr/loder.exe

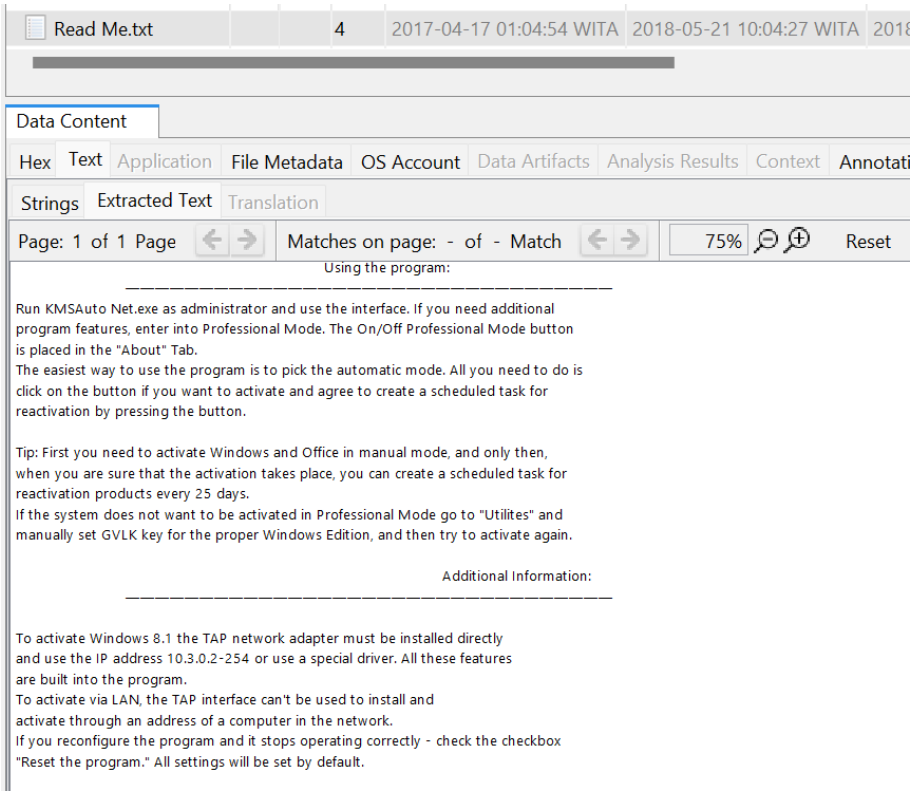
- updsto.exe
    - MD5: 761cfff25ef1066412cf7403a5ae22ab
    - SHA-256: 23784235625b527ddc2cc8a3895b53660479cad06c0645de2c79da47ecca6b03
    - HostUrl=http://weeknews.pro/images/updsto.exe
- wrar56b4.exe
    - MD5: d2b85c81f5661f5d4a35a362fc4e5540
    - SHA-256: 9a7342a167da1165584acdd8630d20b32166e7248fa81865016fe930028cb1df

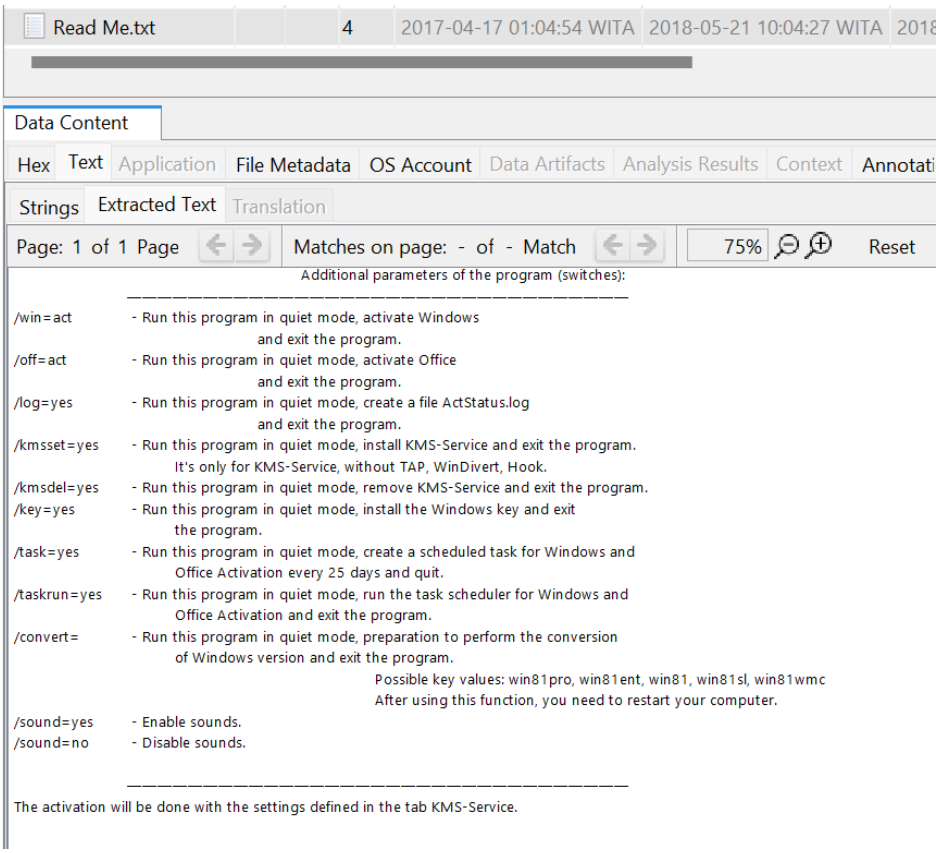
Inside the folder called “KMSAuto.Net.2016.v1.5.0” within the “Downloads” folder, the following were found.

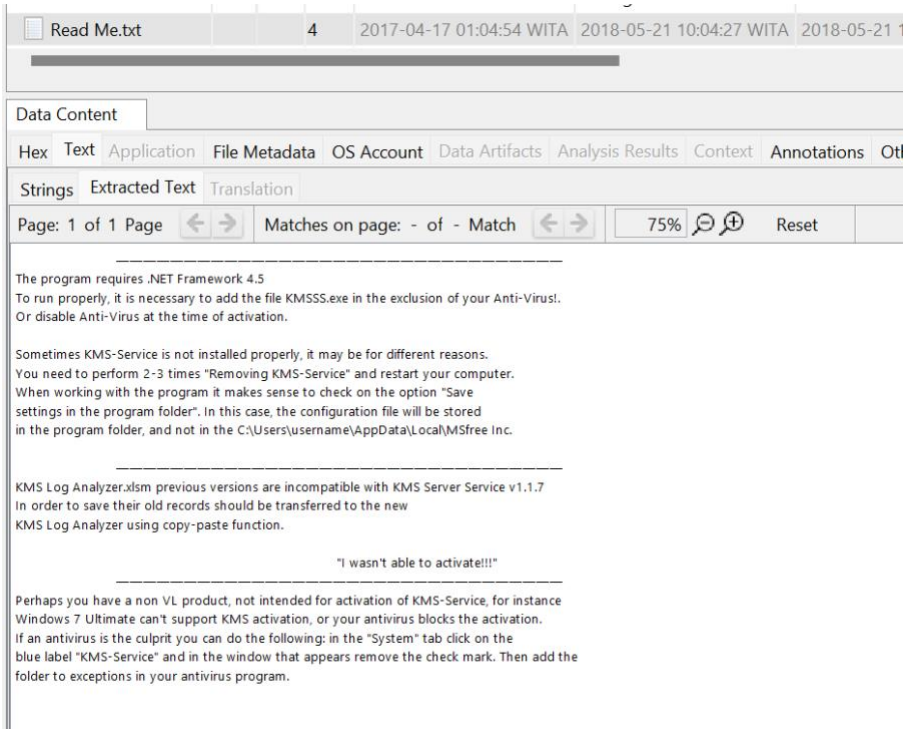


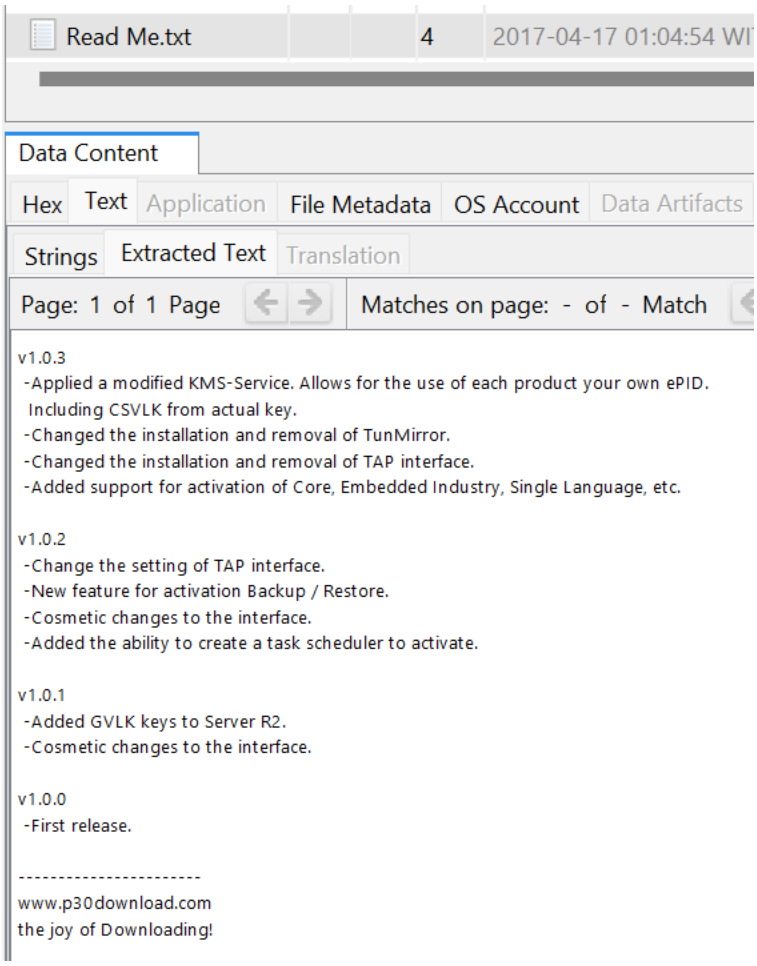
- KMSAuto Net.exe
    - MD5: d02b35945c18e89dc3bb43bc7f6153be
    - SHA-256: 0b05ea08028f239b11f8c30249b0f0aa86966ee4974d03b01bae2ee88befbbeb
- KMSCleaner.exe
    - MD5: 13ea767a7ba607744ebea7409b9f8649
    - SHA-256: a6e2cdc0e9426d50bd72d866bfc80e0fba941efb3ae6d1c564d409f57d1eb117

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

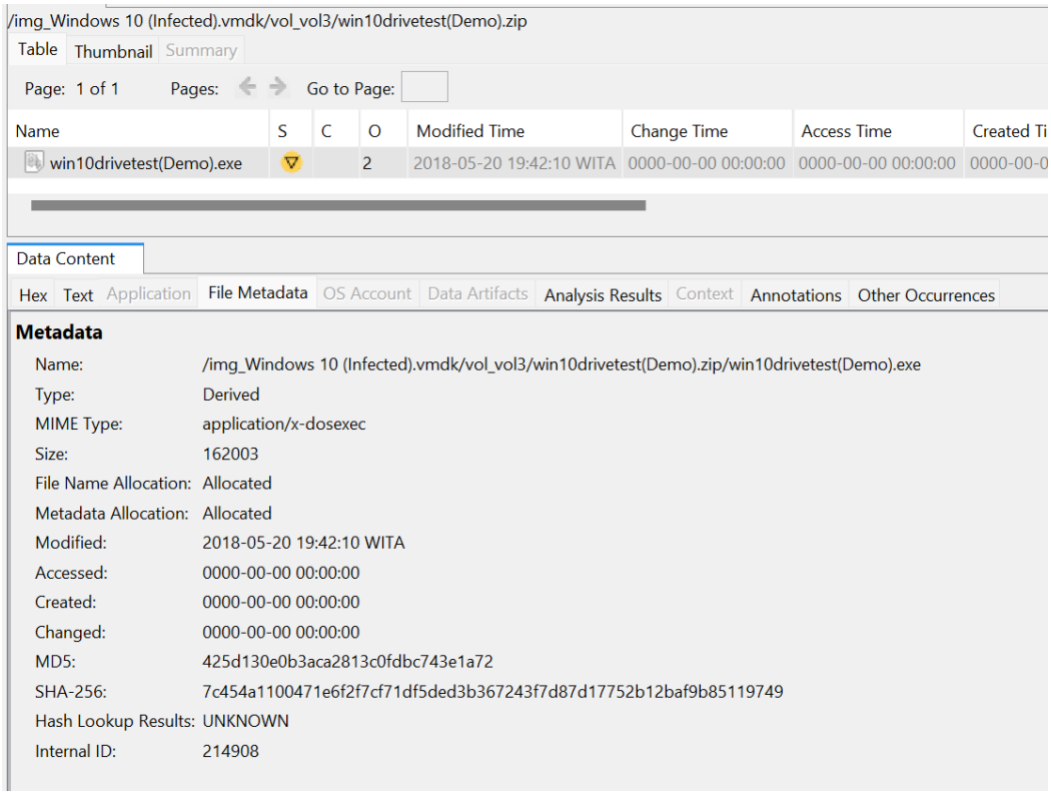
        - 


Read Me.txt
4
2017-04-17 01:04:54 WITA
2018-05-21 10:04:27 WITA
Data Content
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotati
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
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 KMSSS.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.xlsm 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 WI
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.



- win10drivetest(Demo).exe
    - MD5: 425d130e0b3aca2813c0fdbc743e1a72
    - SHA-256: 7c454a1100471e6f2f7cf71df5ded3b367243f7d87d17752b12baf9b85119749

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

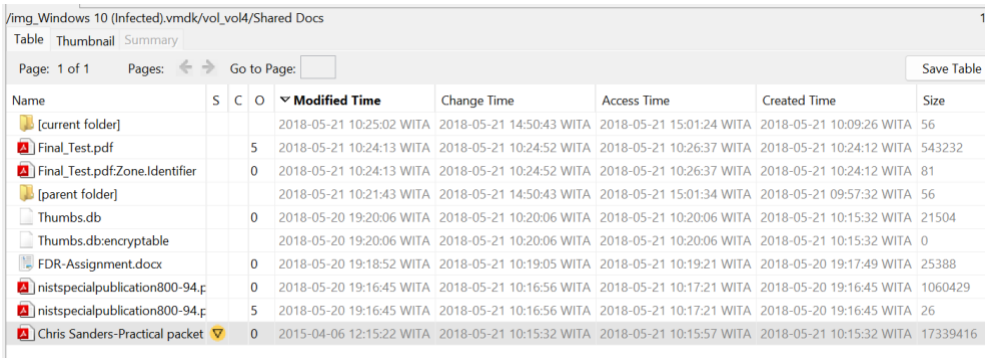

/img_Windows 10 (Infected).vmdk/vol_vol4/Shared Docs

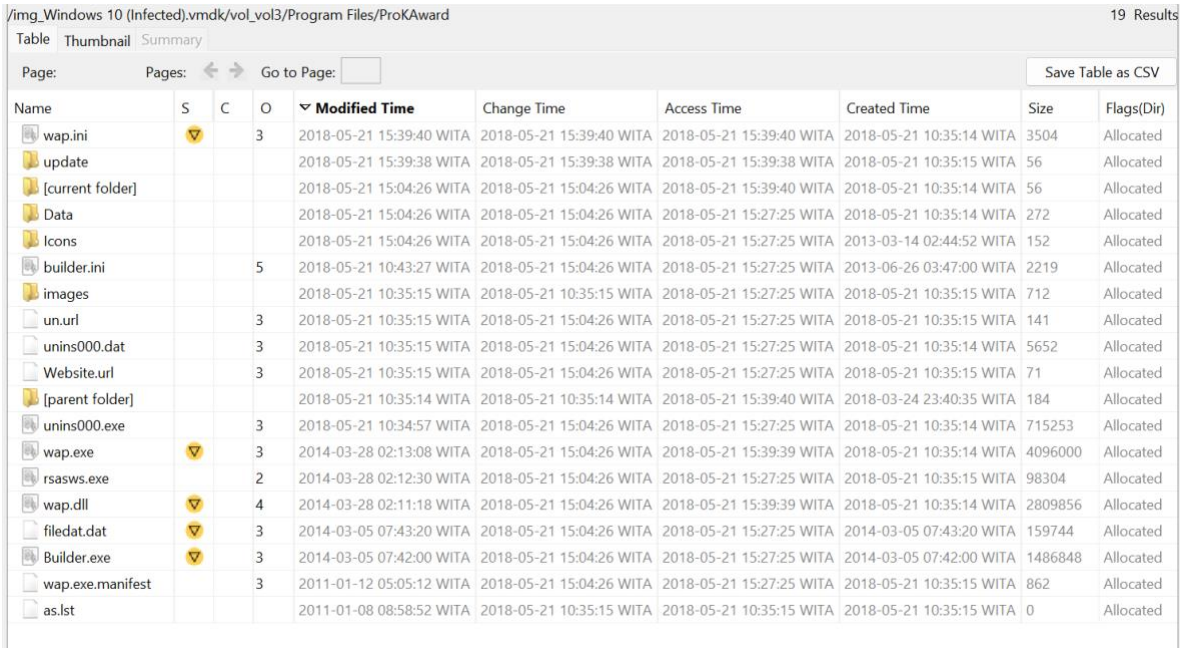
Table Thumbnail Summary

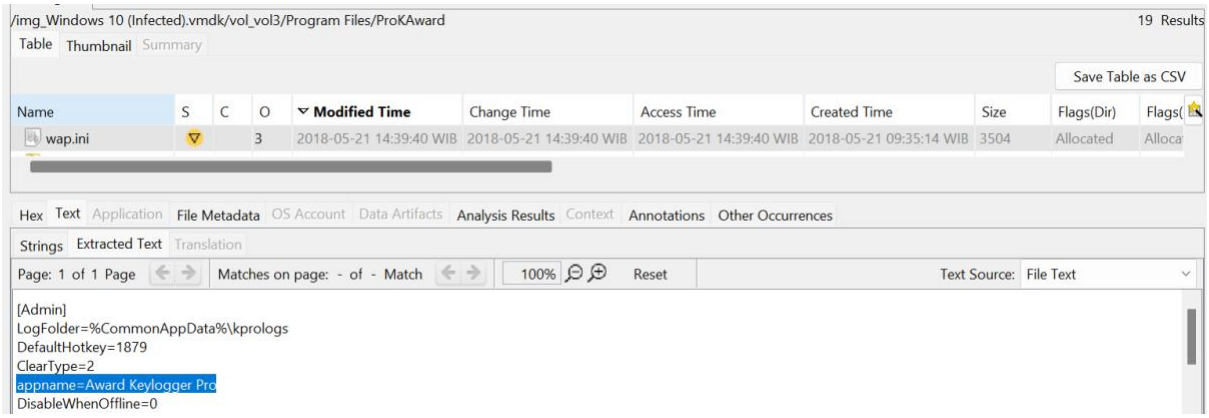
Page: 1 of 1 Pages: Go to Page: Save Table

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[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

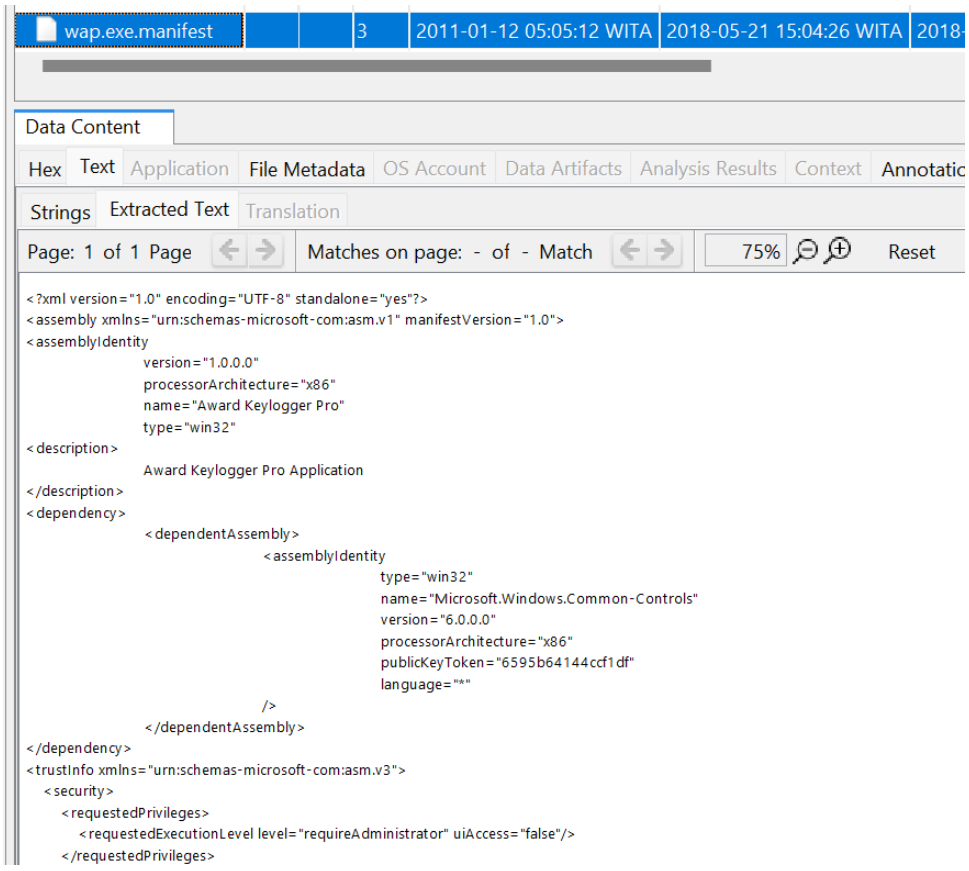
- Final_Test.pdf
    - MD5: ce6ba3df1d57ade7830c5315d77c9311
    - SHA-256: ce8bbc09521bc9bd7a358e4fbbe370962e22b91a78c8d895716ef98a1daaaf77
    - HostUrl=http://delmonicositaliansteakhouse.com/zw.exe
- nistspecialpublication800-94.pdf
    - MD5: 4670a6f605d15fa3155462928e025fd6
    - SHA-256: 289c2ed27f7e3aac41624bf2e6fad268642bad2dabe352a5ab28fa169824a96e
- 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: 5163b03e1a38bd5db769a2bfeebb7ab3
    - SHA-256: edcbdcd6ab07cf5483d5d2aeb4345ee7587d9d8c50d18195f39f86672409bad2

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



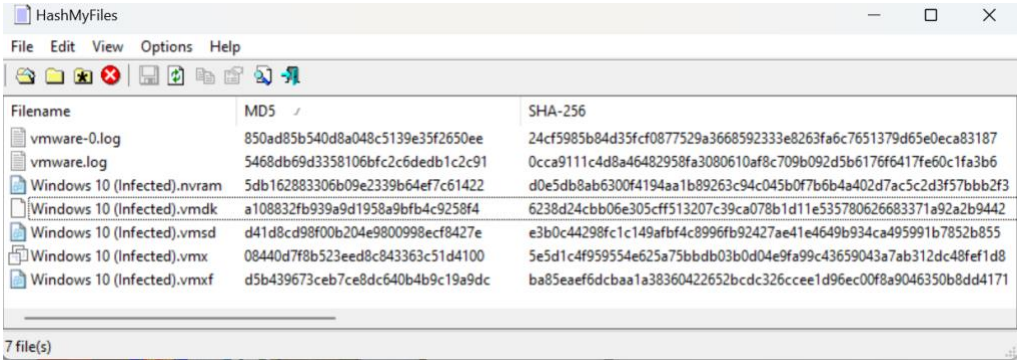


- wap.exe
    - MD5: 5f05bd96f3ff5fa56c9d41c012ec6a13
    - SHA-256: 9c8d0a43aa95e439cede9b69cacfb3c606381bfd6745111c5cfe73a38af9ae38
- rsasws.exe
    - MD5: 62e1be50323d92a7d035552c06a7ef6f
    - SHA-256: 1b84356e23933ecb201460a7c4fe491123831764a7e125e08ceae3dc3e5c9b64

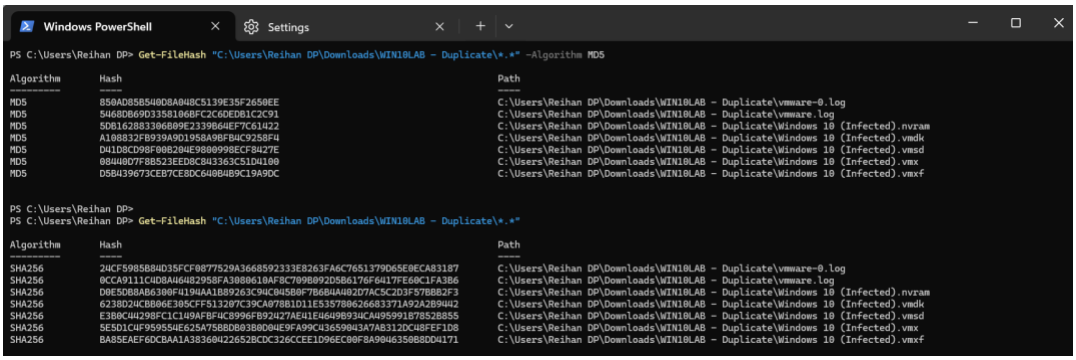
- filedat.dat
    - MD5: 377a3707a5b10f95f731e5feb131d68c
    - SHA-256: 01149f1442787755c79c61499355a79dcfe8ebb67ea9b91fc6413d56ec2070f6
- Builder.exe
    - MD5: 2a651e36ff88b753aba8d6f197aec8a8
    - SHA-256: 2bd25e1f11247fb58536e808e01dfec293497a4e96bf51a0e61d242927e9e9d8
- wap.exe.manifest
    - 

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.



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.

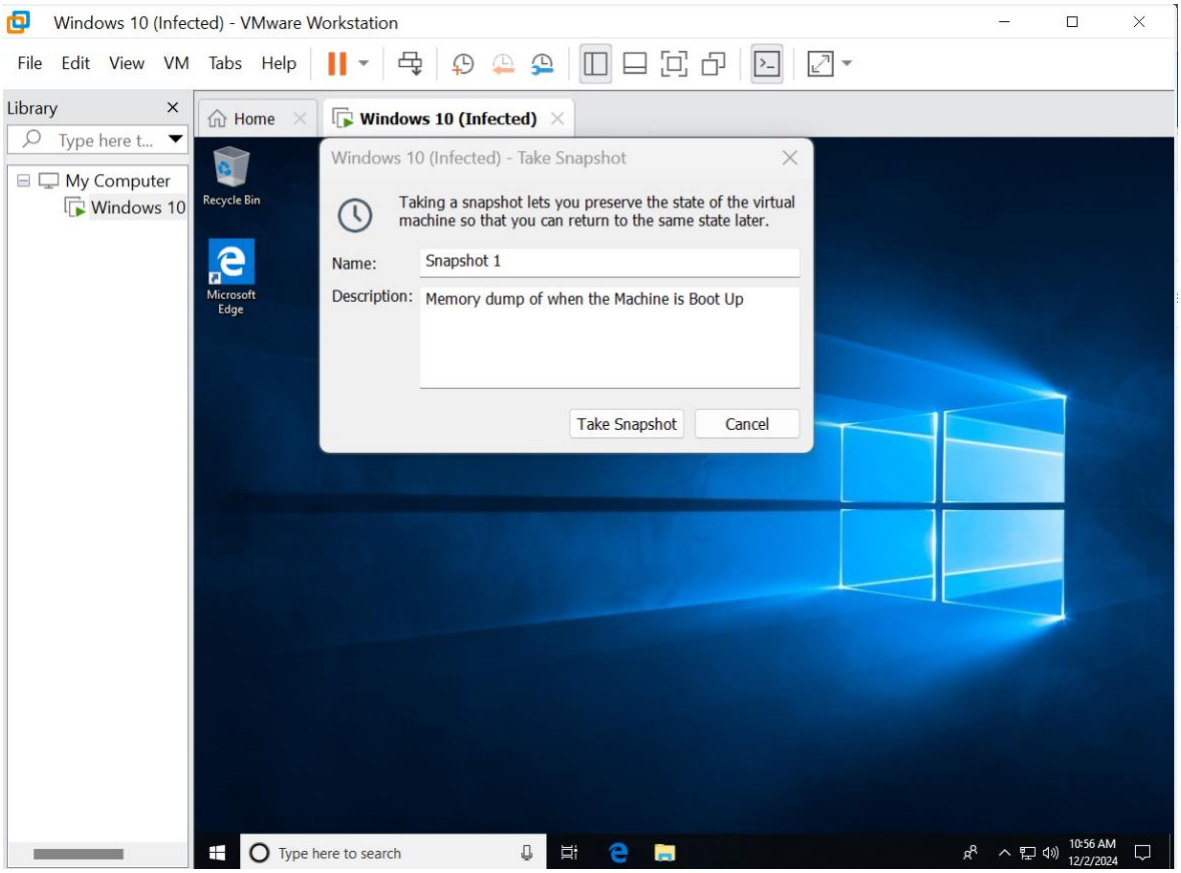


Above are also screenshots of the duplicate files with their respective MD5 and SHA-256 hashes, generated using the command “Get-FileHash” from Windows PowerShell.

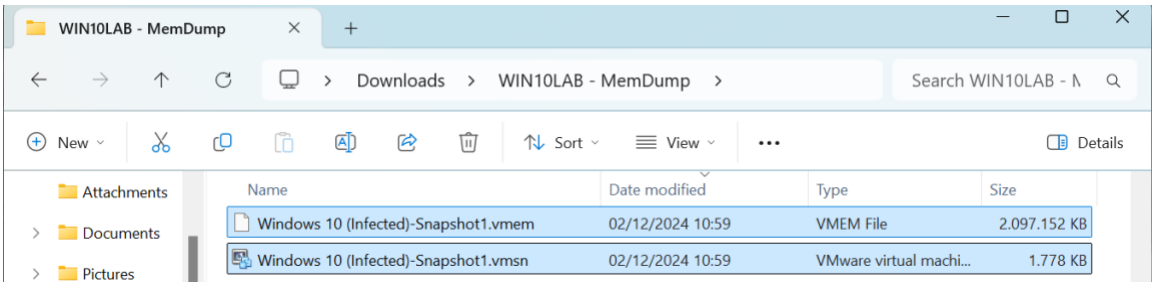
Hashes generated by HashMyFiles and the “Get-FileHash” command are the exact same as each other, and they also match exactly with the hash values of the original files. As stated previously, the case of letters does not matter. The duplicate files are an exact copy of the original files, which means 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.

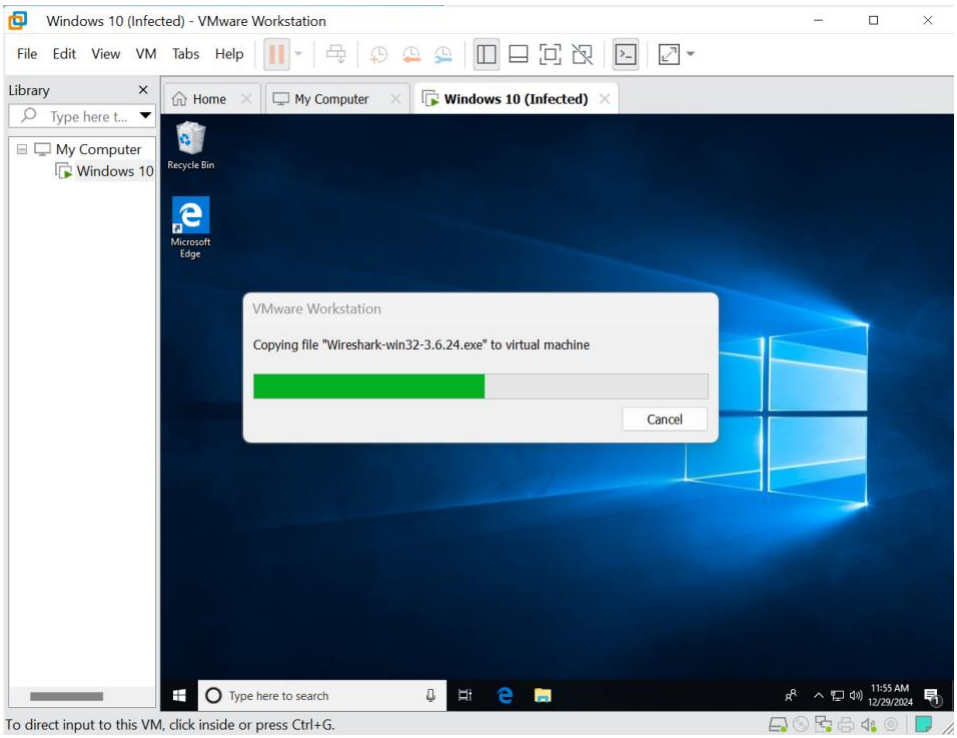


After the snapshot is taken, it is saved to the same folder as the machine, in this case the duplicate of the original virtual machine given.

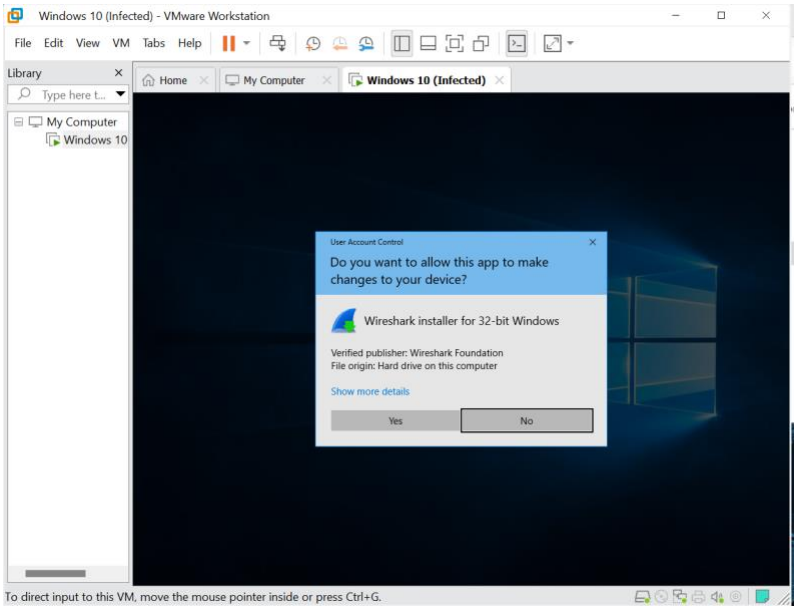


4.4.2 Acquisition of Network Traffic

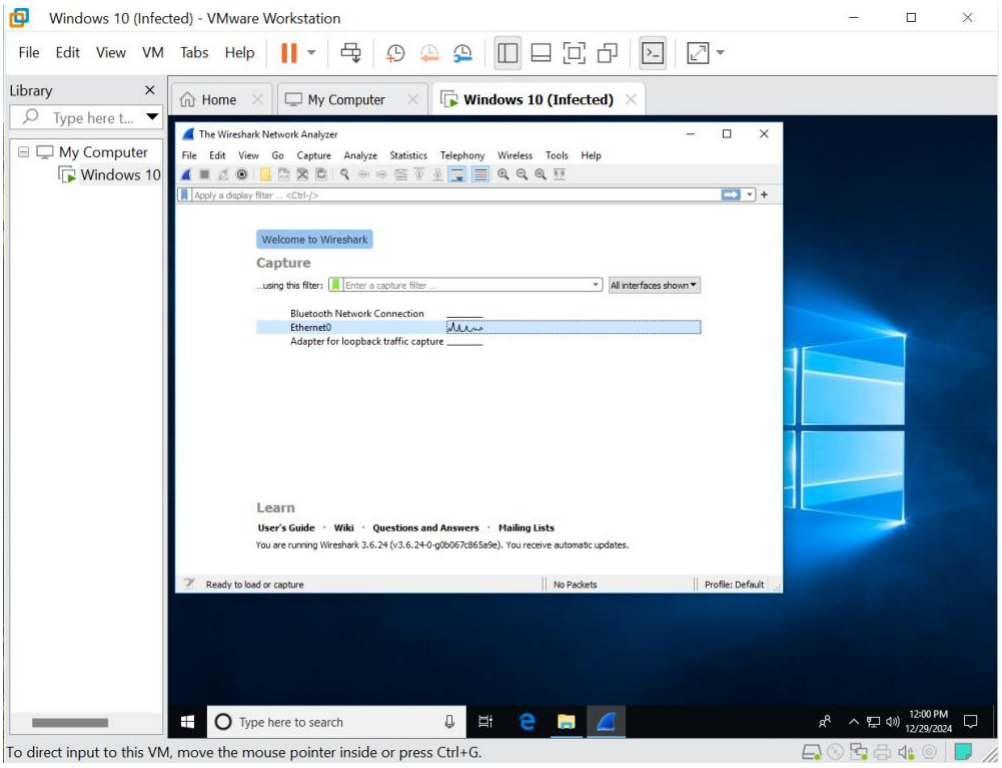
Next, Wireshark would be used to record incoming and outgoing network traffic from the machine. A copy of Wireshark installer is copied to the virtual machine. The 32-bit version of Wireshark is used since the Windows 10 virtual machine is running on 32-bit and not 64-bit.



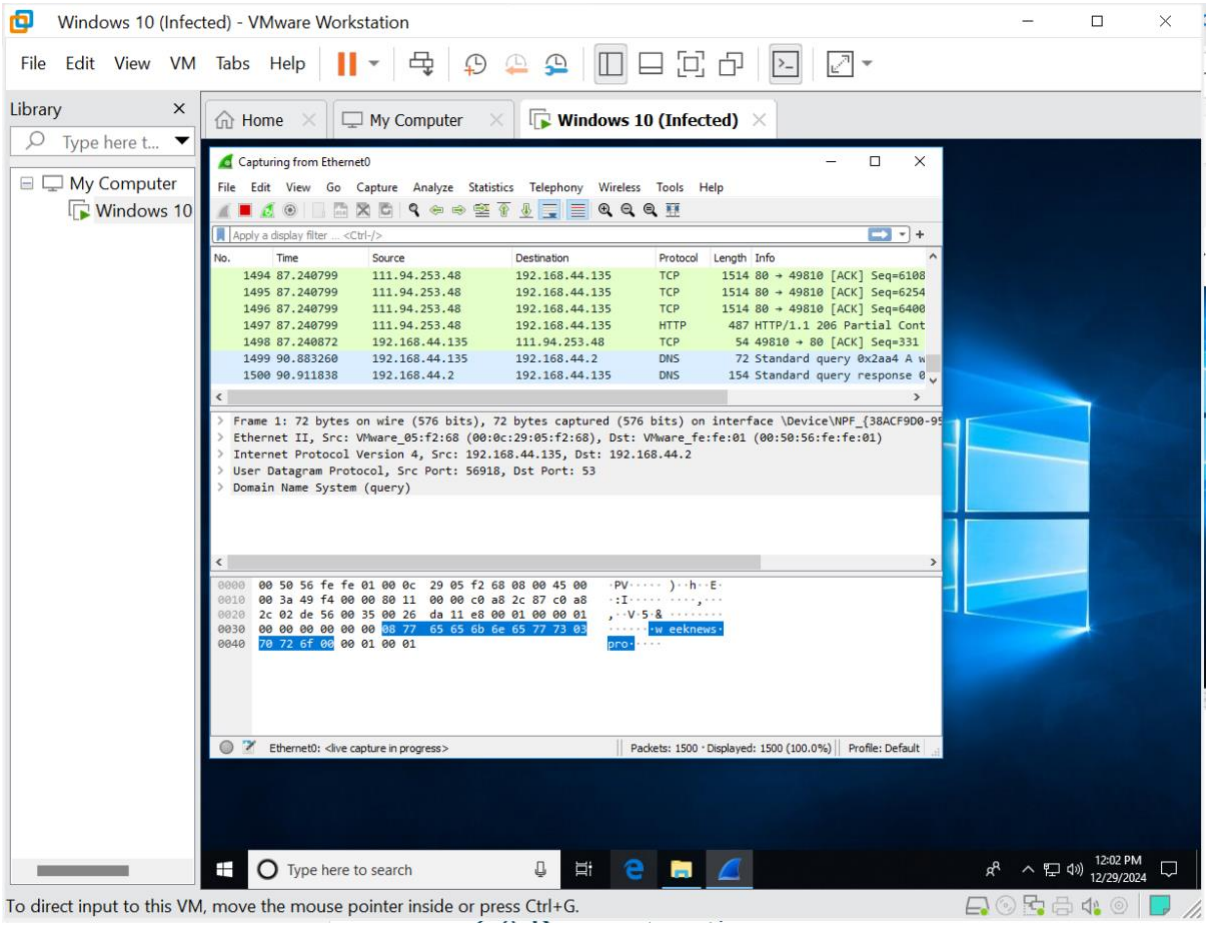
Then Wireshark is installed in the virtual machine using the installer.



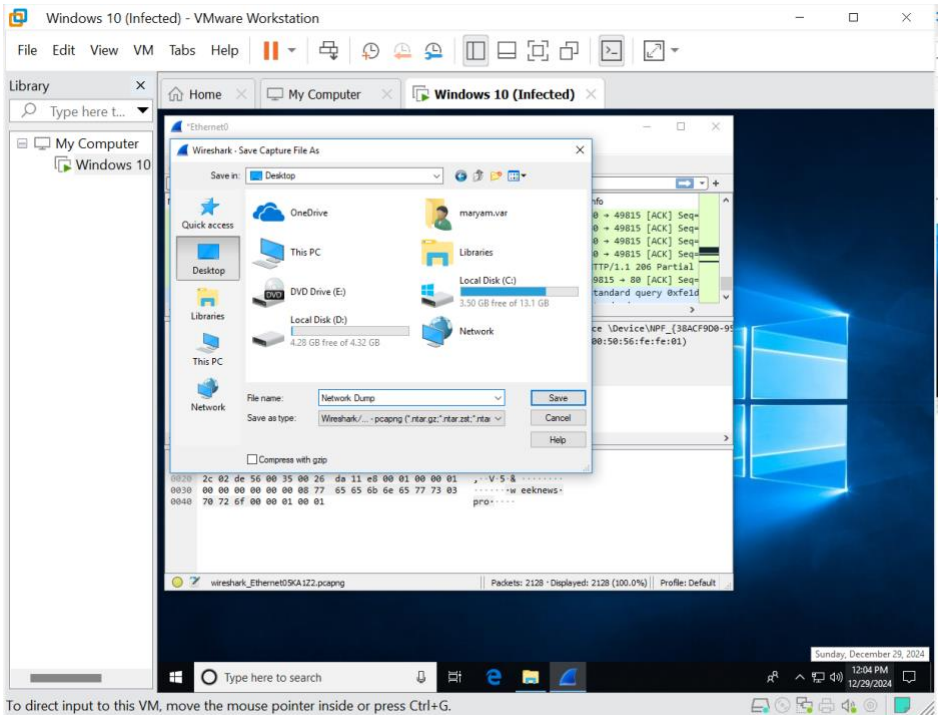
“Ethernet0” is selected, which contains the network traffic going in and out of the machine. Then the network capture is started by clicking on the Wireshark icon which will start to record all traffic from the selected network, in this case “Ethernet0”.



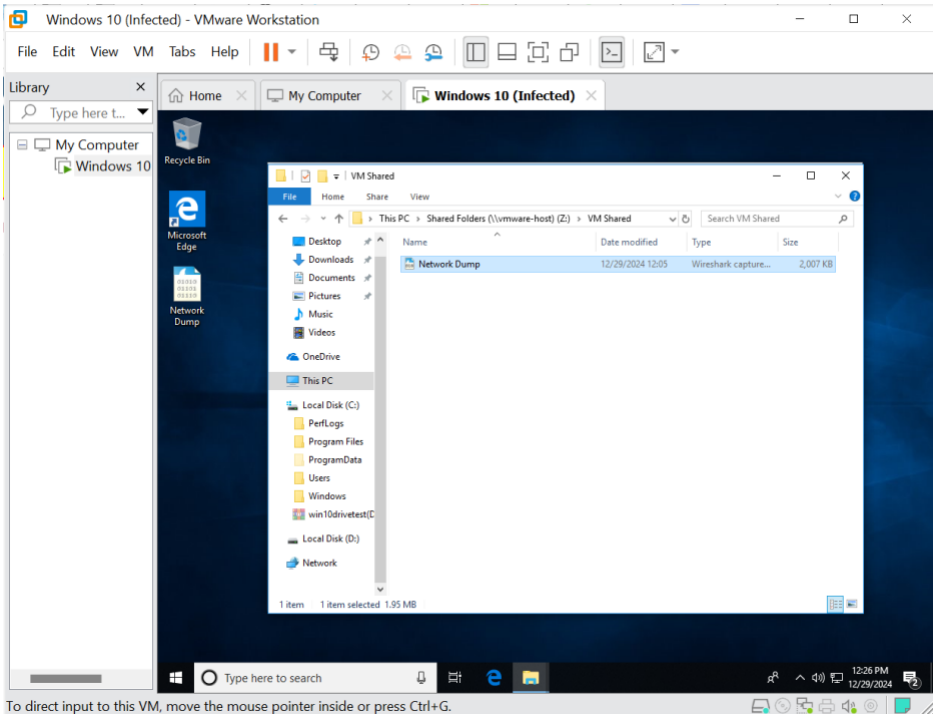
Network traffic would start to appear and be recorded by Wireshark. After some time, the recording is stopped by clicking on the stop button, the red box.



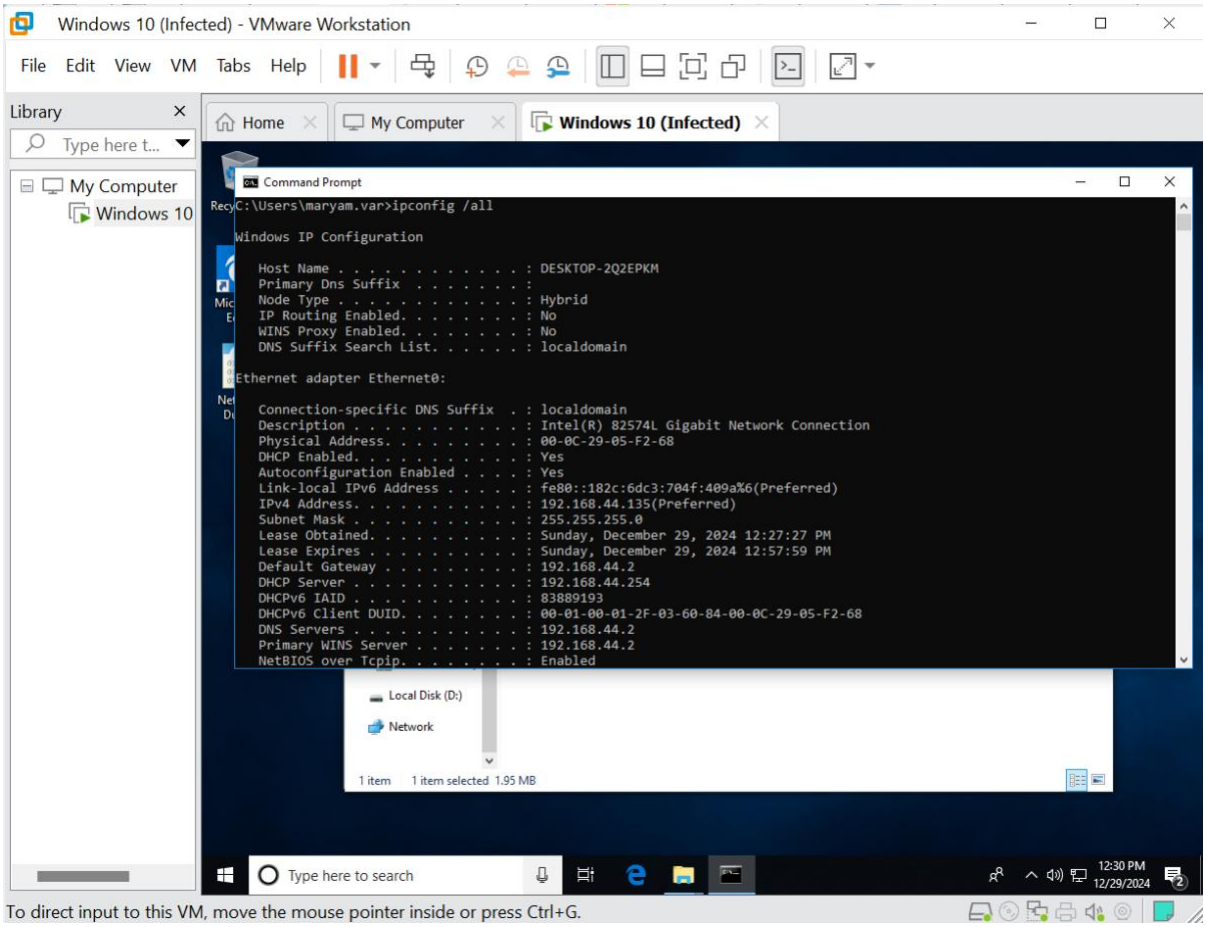
The recording then was saved on the Desktop of the machine.



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.

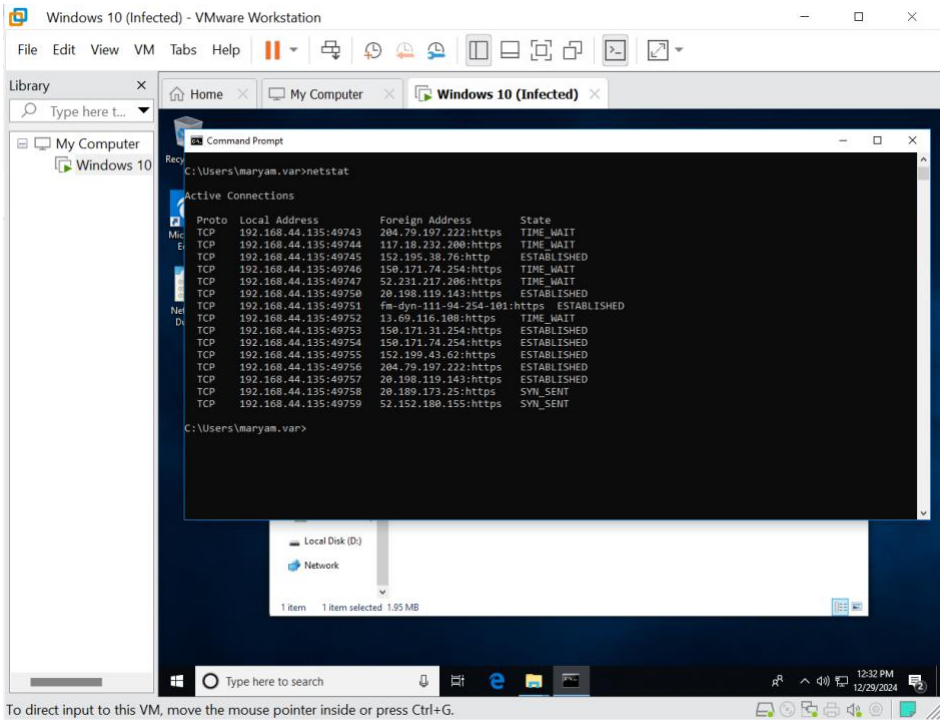


The “ipconfig” command would be done on the live virtual machine to check for its IP address, which would be useful during the analysis of the network traffic.

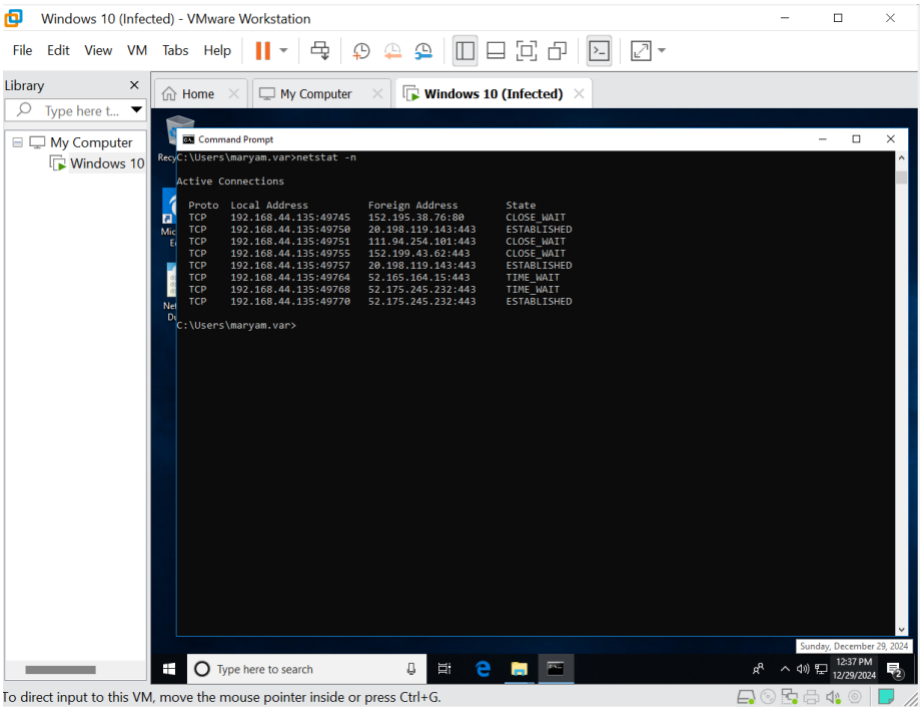


In this case the machine’s IP address is 192.168.44.135.

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

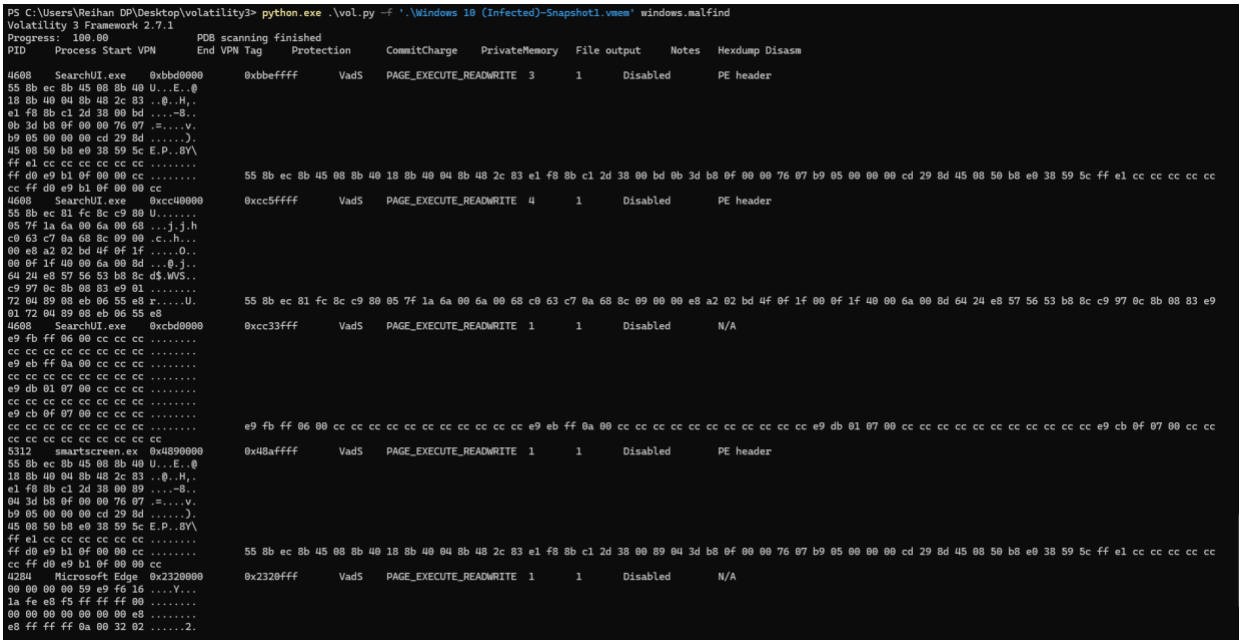
The “psscan” command within Volatility is used to scan the memory dump to display all processes running, even hidden processes, during the time the RAM was captured, in this case after boot.

```
PS C:\Users\Reihan DP\Desktop\volatility3> python.exe .\vol.py -f '.\Windows 10 (Infected)-Snapshot1.vmem' windows.psscan
Volatility 3 Framework 2.7.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

2692    920     RuntimeBroker.  0x86500040      6       -       1       False   2024-12-02 18:53:36.000000      N/A     Disabled
4488    920     ShellExperienc  0x86556a00      17      -       1       False   2024-12-02 18:52:29.000000      N/A     Disabled
7140    920     SppExtComObj.E  0x86587280      6       -       0       False   2024-12-02 18:55:47.000000      N/A     Disabled
1344    768     svchost.exe     0x86699800      36      -       0       False   2024-12-02 18:51:01.000000      N/A     Disabled
4       0       System  0x866ada00      162     -       N/A     False   2024-12-02 18:50:48.000000      N/A     Disabled
1536    768     vmacthlp.exe    0x866dd9c0      2       -       0       False   2024-12-02 18:51:02.000000      N/A     Disabled
6856    1220    dmclient.exe    0x866f6040      0       -       0       False   2024-12-02 18:55:35.000000      2024-12-02 18:56:31.000000      Disabled
1396    768     svchost.exe     0x866fb780      29      -       0       False   2024-12-02 18:51:02.000000      N/A     Disabled
4644    3016    vmtoolsd.exe    0x86703040      6       -       1       False   2024-12-02 18:54:13.000000      N/A     Disabled
68      4       Registry        0x86729a00      3       -       N/A     False   2024-12-02 18:50:13.000000      N/A     Disabled
3296    768     svchost.exe     0x867f6040      11      -       0       False   2024-12-02 18:51:45.000000      N/A     Disabled
3016    2240    explorer.exe    0x892f4a00      57      -       1       False   2024-12-02 18:51:55.000000      N/A     Disabled
5136    768     SearchIndexer.  0x89303040      16      -       0       False   2024-12-02 18:53:08.000000      N/A     Disabled
3556    768     VSSVC.exe       0x893a0040      6       -       0       False   2024-12-02 18:51:59.000000      N/A     Disabled
2928    920     dllhost.exe     0x893d6a00      5       -       1       False   2024-12-02 18:52:02.000000      N/A     Disabled
4488    920     ShellExperienc  0x8a449a00      17      -       1       False   2024-12-02 18:52:29.000000      N/A     Disabled
7140    920     SppExtComObj.E  0x8a476280      6       -       0       False   2024-12-02 18:55:47.000000      N/A     Disabled
4836    920     RuntimeBroker.  0x8b435680      13      -       1       False   2024-12-02 18:52:51.000000      N/A     Disabled
2168    768     SecurityHealth  0x8b474a00      11      -       0       False   2024-12-02 18:51:11.000000      N/A     Disabled
6900    6856    conhost.exe     0x8badba00      0       -       0       False   2024-12-02 18:55:39.000000      2024-12-02 18:56:33.000000      Disabled
636     624     csrss.exe       0x8bb27a00      10      -       0       False   2024-12-02 18:50:56.000000      N/A     Disabled
7168    7140    slui.exe        0x8bb4d040      0       -       0       False   2024-12-02 18:55:48.000000      2024-12-02 18:56:00.000000      Disabled
1844    768     svchost.exe     0x8c438a00      10      -       0       False   2024-12-02 18:51:03.000000      N/A     Disabled
2240    804     userinit.exe    0x8c481300      0       -       1       False   2024-12-02 18:51:55.000000      2024-12-02 18:52:51.000000      Disabled
552     4       smss.exe        0x8c798740      4       -       N/A     False   2024-12-02 18:50:48.000000      N/A     Disabled
704     624     wininit.exe     0x8cbf2040      5       -       0       False   2024-12-02 18:50:56.000000      N/A     Disabled
712     696     csrss.exe       0x8cbfb100      12      -       1       False   2024-12-02 18:50:56.000000      N/A     Disabled
1060    804     fontdrvhost.ex  0x8d00d040      6       -       1       False   2024-12-02 18:50:58.000000      N/A     Disabled
768     704     services.exe    0x8d027040      23      -       0       False   2024-12-02 18:50:56.000000      N/A     Disabled
796     704     lsass.exe       0x8d02e580      9       -       0       False   2024-12-02 18:50:56.000000      N/A     Disabled
804     696     winlogon.exe    0x8d032040      5       -       1       False   2024-12-02 18:50:56.000000      N/A     Disabled
912     704     fontdrvhost.ex  0x8d073040      6       -       0       False   2024-12-02 18:50:57.000000      N/A     Disabled
920     768     svchost.exe     0x8d075440      32      -       0       False   2024-12-02 18:50:57.000000      N/A     Disabled
984     768     svchost.exe     0x8d0cc580      18      -       0       False   2024-12-02 18:50:57.000000      N/A     Disabled
1116    804     dwm.exe 0x8d1269c0      11      -       1       False   2024-12-02 18:50:59.000000      N/A     Disabled
1160    768     svchost.exe     0x8d13a600      28      -       0       False   2024-12-02 18:51:00.000000      N/A     Disabled
1220    768     svchost.exe     0x8d152240      100     -       0       False   2024-12-02 18:51:01.000000      N/A     Disabled
1240    768     svchost.exe     0x8d16c8c0      11      -       0       False   2024-12-02 18:51:01.000000      N/A     Disabled
5428    3016    MSASCuiL.exe    0x8d1bb040      5       -       1       False   2024-12-02 18:54:13.000000      N/A     Disabled
1604    768     WUDFHost.exe    0x8d1ef980      8       -       0       False   2024-12-02 18:51:02.000000      N/A     Disabled
1620    4       MemCompression  0x8d1f4640      42      -       N/A     False   2024-12-02 18:51:02.000000      N/A     Disabled
1692    768     svchost.exe     0x8d224940      3       -       0       False   2024-12-02 18:51:02.000000      N/A     Disabled
```

```
588     768     spoolsv.exe     0x8d2c6a00      14      -       0       False   2024-12-02 18:51:03.000000      N/A     Disabled
2068    768     svchost.exe     0x8d393a00      15      -       0       False   2024-12-02 18:51:08.000000      N/A     Disabled
2088    768     VGAuthService.  0x8d3a4a00      3       -       0       False   2024-12-02 18:51:10.000000      N/A     Disabled
2132    768     rsasws.exe      0x8d3e8040      5       -       0       False   2024-12-02 18:51:11.000000      N/A     Disabled
2124    768     MsMpEng.exe     0x8d40f040      15      -       0       False   2024-12-02 18:51:11.000000      N/A     Disabled
2156    768     vmtoolsd.exe    0x8d418280      8       -       0       False   2024-12-02 18:51:11.000000      N/A     Disabled
2668    768     dllhost.exe     0x8d59e100      18      -       0       False   2024-12-02 18:51:27.000000      N/A     Disabled
2744    768     svchost.exe     0x8d5d5040      5       -       0       False   2024-12-02 18:51:29.000000      N/A     Disabled
2872    920     WmiPrvSE.exe    0x8d669040      15      -       0       False   2024-12-02 18:51:34.000000      N/A     Disabled
3080    768     svchost.exe     0x8d6efa00      4       -       0       False   2024-12-02 18:51:38.000000      N/A     Disabled
3100    920     WmiPrvSE.exe    0x8d6f7640      11      -       0       False   2024-12-02 18:51:39.000000      N/A     Disabled
3568    3468    MpCmdRun.exe    0x8d7f48a00     6       -       0       False   2024-12-02 18:51:48.000000      N/A     Disabled
3656    2124    MpCmdRun.exe    0x8d755680      8       -       0       False   2024-12-02 18:51:48.000000      N/A     Disabled
4608    920     SearchUI.exe    0x8d76c240      26      -       1       False   2024-12-02 18:52:33.000000      N/A     Disabled
3672    3656    conhost.exe     0x8d78d040      4       -       0       False   2024-12-02 18:51:49.000000      N/A     Disabled
3732    1220    sihost.exe      0x8d7b3880      18      -       1       False   2024-12-02 18:51:49.000000      N/A     Disabled
3780    768     svchost.exe     0x8d7c9a00      25      -       1       False   2024-12-02 18:51:49.000000      N/A     Disabled
3884    1220    taskhostw.exe   0x8d7fe040      11      -       1       False   2024-12-02 18:51:50.000000      N/A     Disabled
3996    768     msdtc.exe       0x8d822040      13      -       0       False   2024-12-02 18:51:51.000000      N/A     Disabled
4060    1240    ctfmon.exe      0x8d86f440      10      -       1       False   2024-12-02 18:51:52.000000      N/A     Disabled
2060    2132    wap.exe 0x8d870580      6       -       1       False   2024-12-02 18:51:52.000000      N/A     Disabled
7240    920     slui.exe        0x8d94c800      0       -       1       False   2024-12-02 18:55:57.000000      2024-12-02 18:55:59.000000      Disabled
2692    920     RuntimeBroker.  0x8d96d040      6       -       1       False   2024-12-02 18:53:36.000000      N/A     Disabled
5752    920     MicrosoftEdge.  0x8d9cba00      25      -       1       False   2024-12-02 18:53:19.000000      N/A     Disabled
4988    768     sppsvc.exe      0x8d9f3a00      8       -       0       False   2024-12-02 18:53:03.000000      N/A     Disabled
2268    920     RuntimeBroker.  0x8da40a00      3       -       1       False   2024-12-02 18:54:03.000000      N/A     Disabled
7340    920     dllhost.exe     0x8da65680      0       -       0       False   2024-12-02 18:56:19.000000      2024-12-02 18:56:24.000000      Disabled
5240    920     ApplicationFra  0x8da78880      13      -       1       False   2024-12-02 18:53:08.000000      N/A     Disabled
5312    920     smartscreen.ex  0x8da9a640      11      -       1       False   2024-12-02 18:53:09.000000      N/A     Disabled
5644    920     RuntimeBroker.  0x8db15040      11      -       1       False   2024-12-02 18:53:16.000000      N/A     Disabled
6072    920     SkypeHost.exe   0x8db53040      8       -       1       False   2024-12-02 18:53:29.000000      N/A     Disabled
5700    920     RuntimeBroker.  0x8dc74040      8       -       1       False   2024-12-02 18:53:18.000000      N/A     Disabled
5772    920     backgroundTask  0x8dc84100      7       -       1       False   2024-12-02 18:53:19.000000      N/A     Disabled
5800    768     TrustedInstall  0x8dc9ea00      8       -       0       False   2024-12-02 18:53:20.000000      N/A     Disabled
5780    5136    SearchProtocol  0x8dcc9a00      7       -       0       False   2024-12-02 18:53:20.000000      N/A     Disabled
3452    920     HxTsr.exe       0x8dcd4040      16      -       1       False   2024-12-02 18:53:32.000000      N/A     Disabled
5932    920     browser_broker  0x8de0d5c0      7       -       1       False   2024-12-02 18:53:25.000000      N/A     Disabled
6008    920     TiWorker.exe    0x8de31600      7       -       0       False   2024-12-02 18:53:26.000000      N/A     Disabled
4324    920     MicrosoftEdgeC  0x8de44a00      15      -       1       False   2024-12-02 18:53:53.000000      N/A     Disabled
6140    920     backgroundTask  0x8de46040      8       -       1       False   2024-12-02 18:53:31.000000      N/A     Disabled
2216    5136    SearchFilterHo  0x8de8c700      4       -       0       False   2024-12-02 18:53:33.000000      N/A     Disabled
4380    920     MicrosoftEdgeC  0x8deefa00      14      -       1       False   2024-12-02 18:53:53.000000      N/A     Disabled
5632    3016    OneDrive.exe    0x8dfe5540      19      -       1       False   2024-12-02 18:54:14.000000      N/A     Disabled
4284    3016    Microsoft Edge  0x8e071a00      12      -       1       False   2024-12-02 18:54:17.000000      N/A     Disabled
2512    768     svchost.exe     0x8e0a5a00      8       -       0       False   2024-12-02 18:54:29.000000      N/A     Disabled
5636    920     SystemSettings  0x8e0dd540      5       -       1       False   2024-12-02 18:54:21.000000      N/A     Disabled
6572    1240    dasHost.exe     0x8e415480      12      -       0       False   2024-12-02 18:55:09.000000      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.

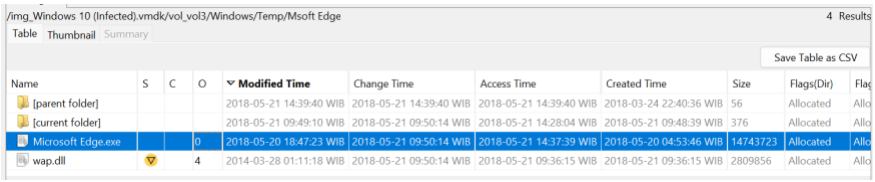
```
PS C:\Users\Reihan DP\Desktop\volatility3> python.exe .\vol.py -f '.\Windows 10 (Infected)-Snapshot1.vmem' windows.cmdline
Volatility 3 Framework 2.7.1
Progress:  100.00               PDB scanning finished
PID     Process Args

2132    rsasws.exe      "C:\Program Files\ProKAward\rsasws.exe"

2060    wap.exe "C:\Program Files\ProKAward\wap.exe"

4284    Microsoft Edge  "C:\Windows\Temp\Msoft Edge\Microsoft Edge.exe"
```

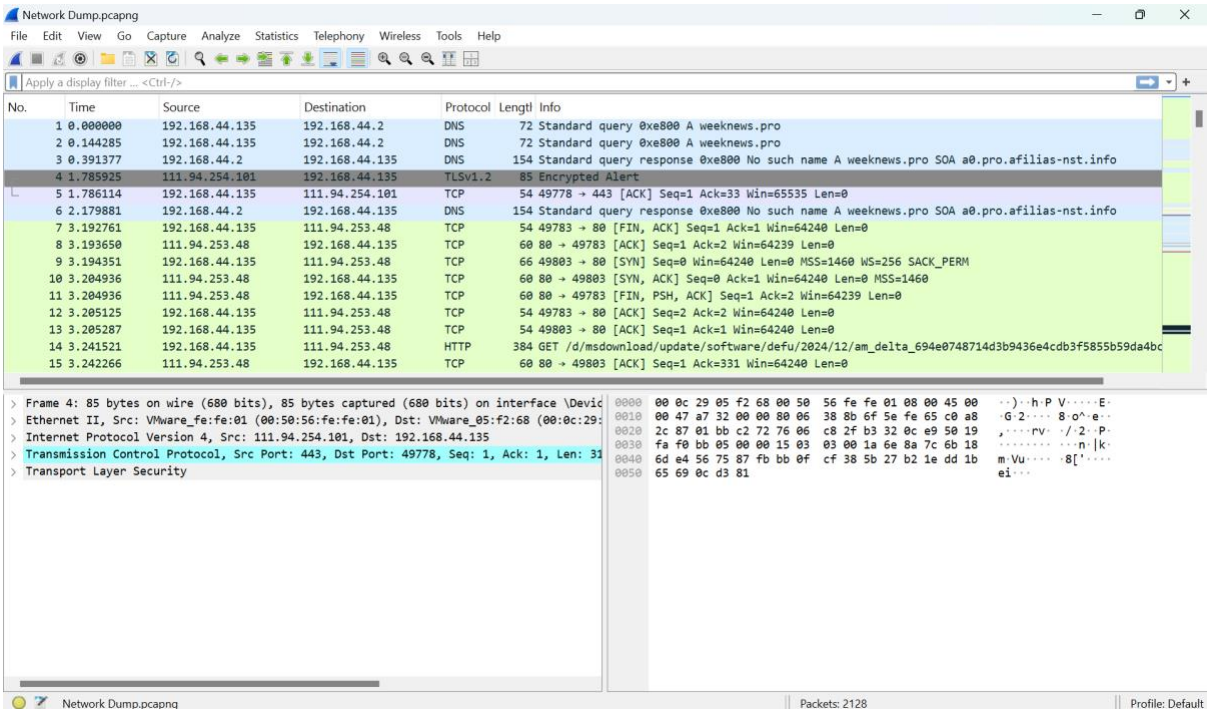
The hash of “rsasws.exe” and “wap.exe” was previously captured on previous section, in the section “4.3 Suspicious Files on the Disk”. While the other process is as below:

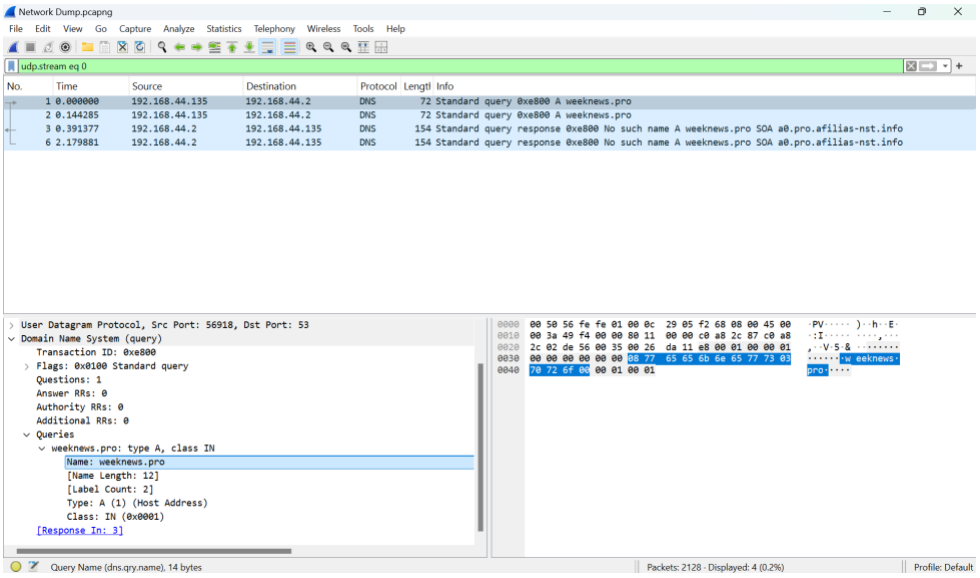
- Microsoft Edge
  - 

  - 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.



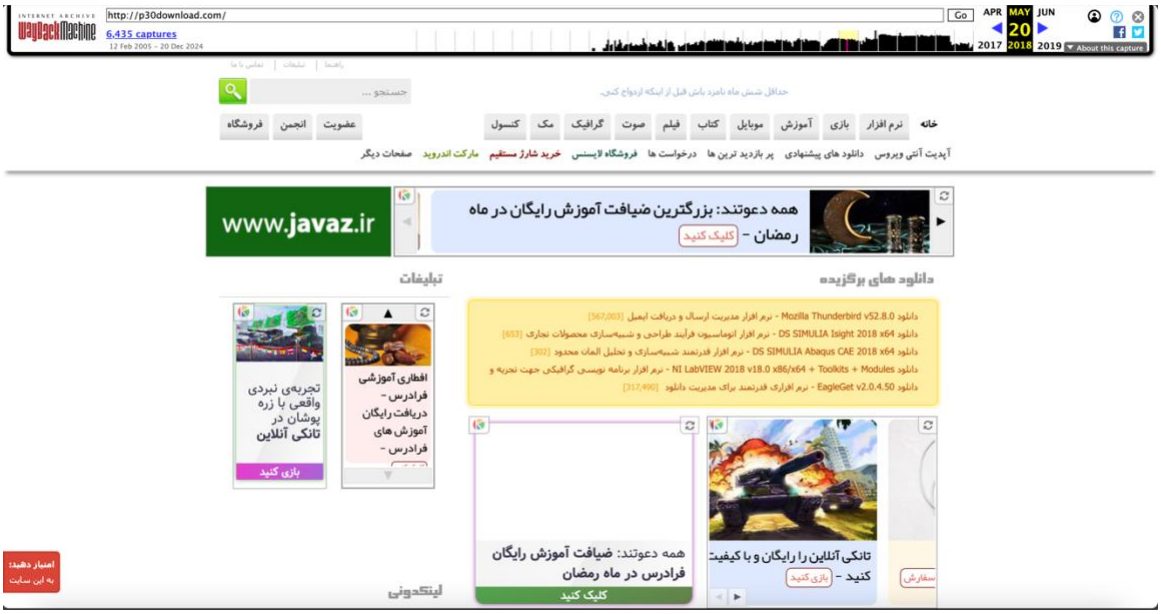


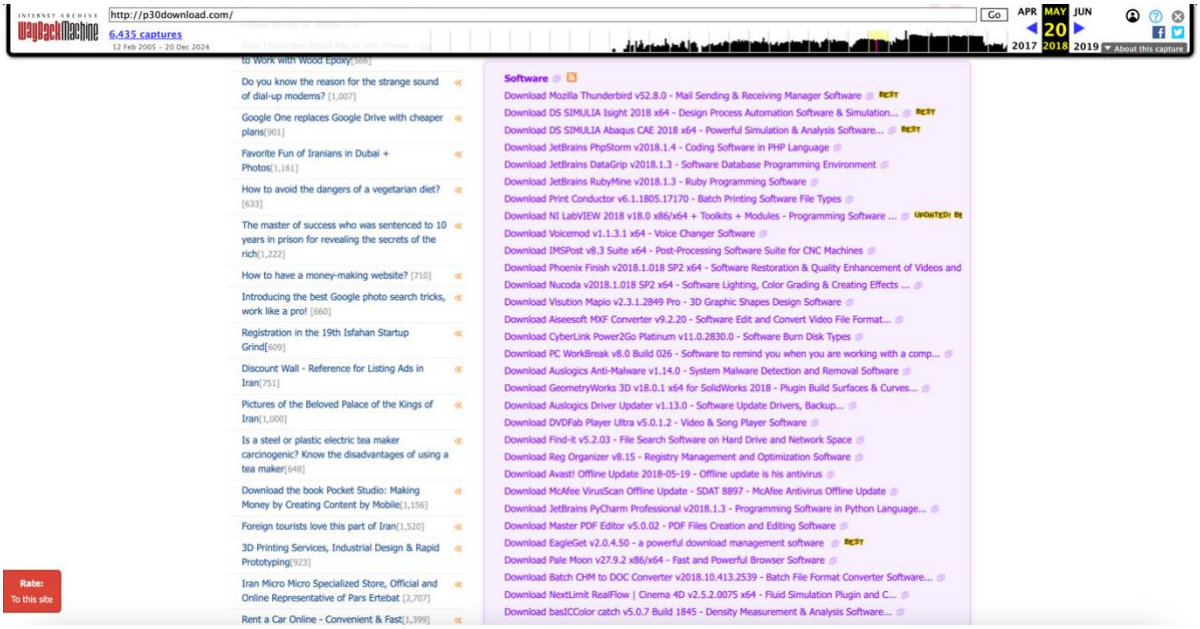
Throughout the recorded network traffic, the device was trying to query “weeknews.pro” which was where the executable file “updsto.exe” was downloaded from, based on previous section “4.2 Web History”.

5.3 Findings

5.3.1 p30download.com and KMSAuto

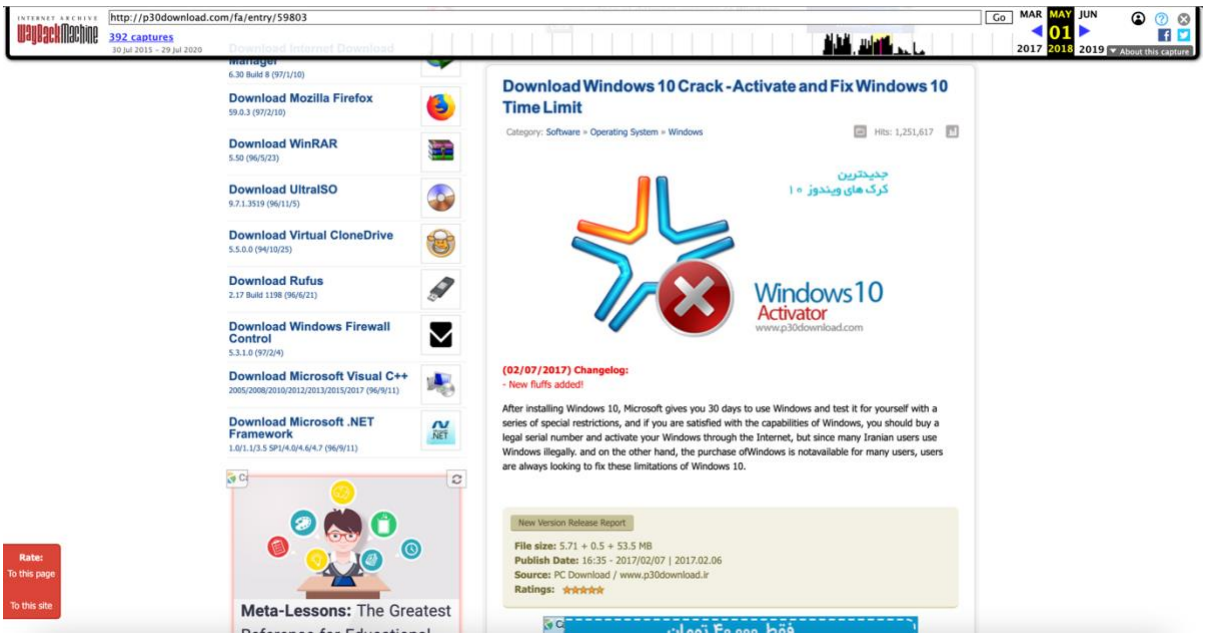
The website is currently unavailable but a snapshot of the website around the time it was accessed on the machine (2018-05-21) is shown below.



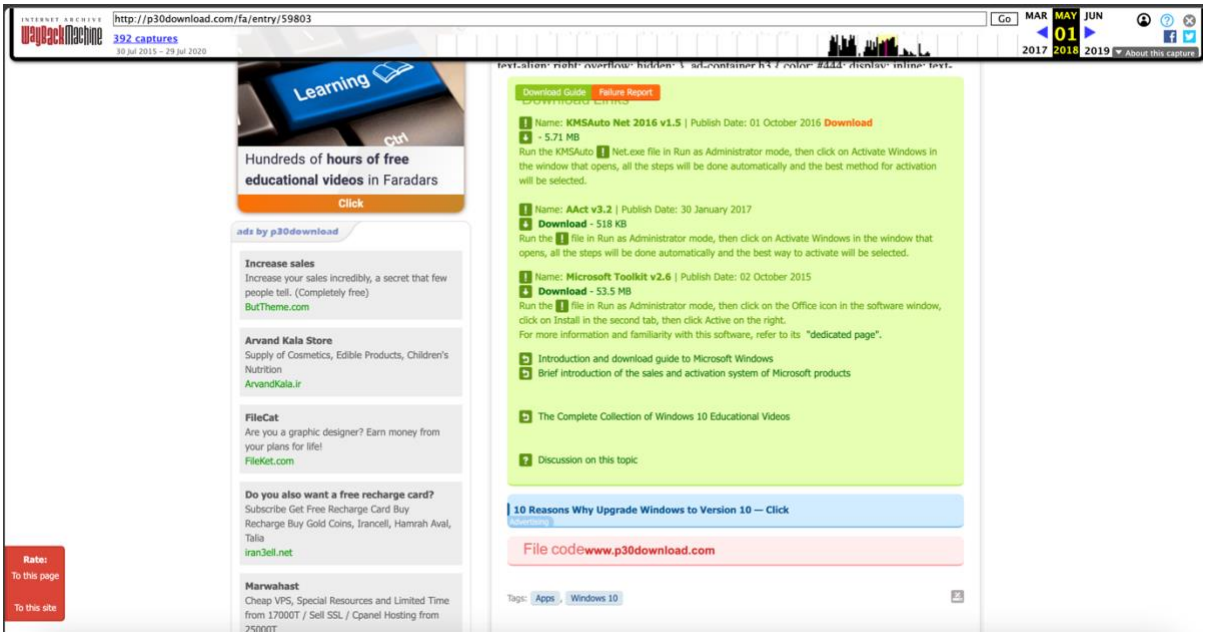


It seems to be a website to download crack versions of software.

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

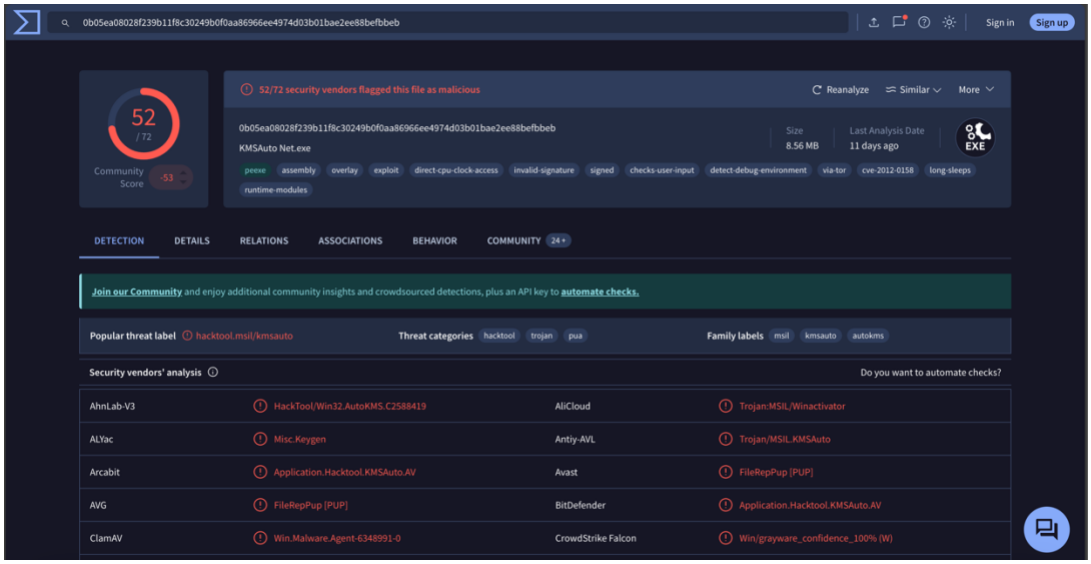


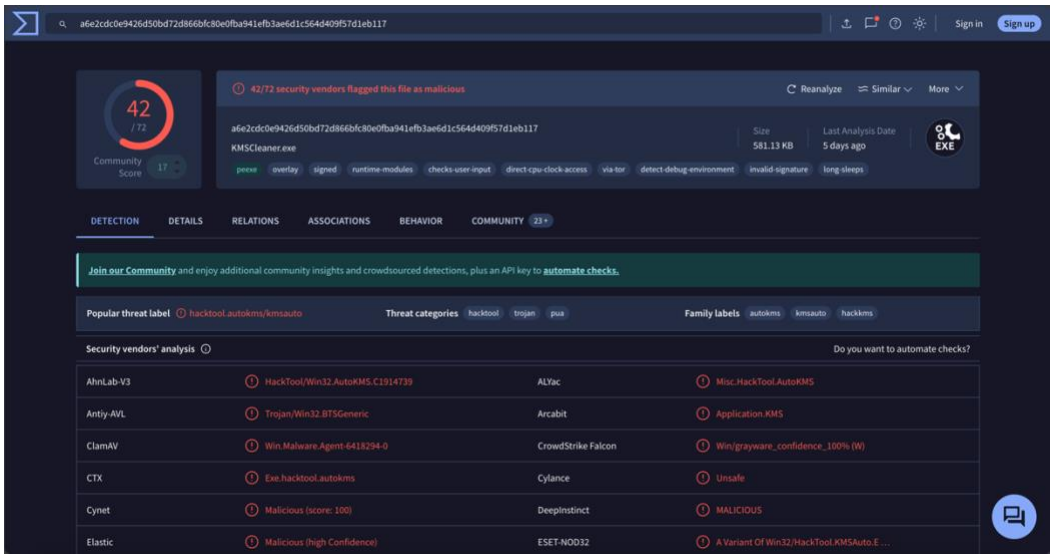
The user seems to try and download a cracked version of Windows 10.



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:

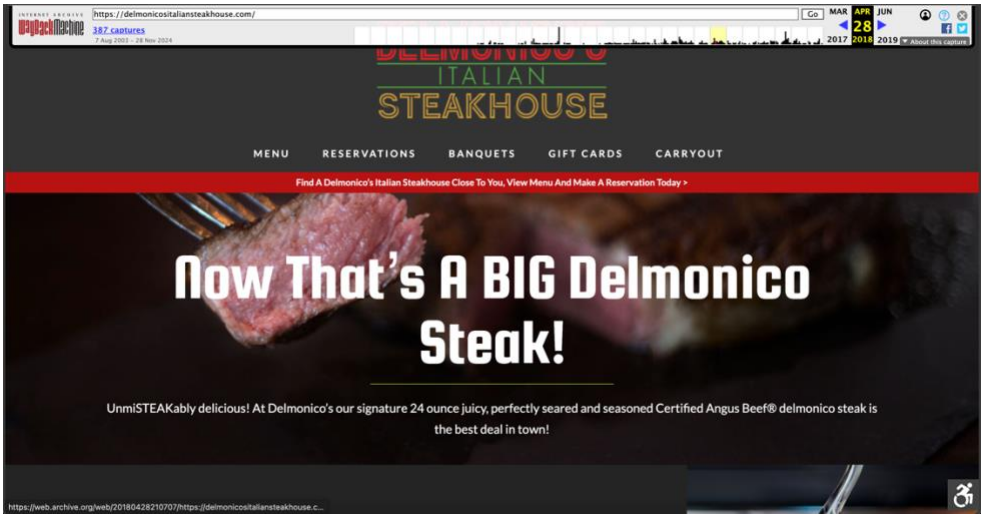
- KMSAuto Net.exe
  - 

- KMSCleaner.exe
  - 

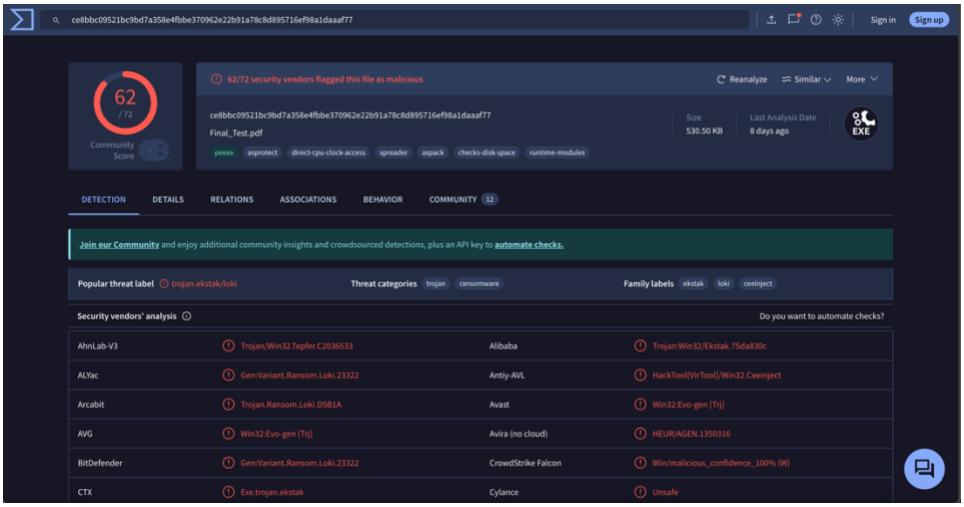
Both files are malicious with both being flagged as malicious by 52 and 42 security vendors respectively. Both files are under the “kmsauto” family and both are trojan.

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.



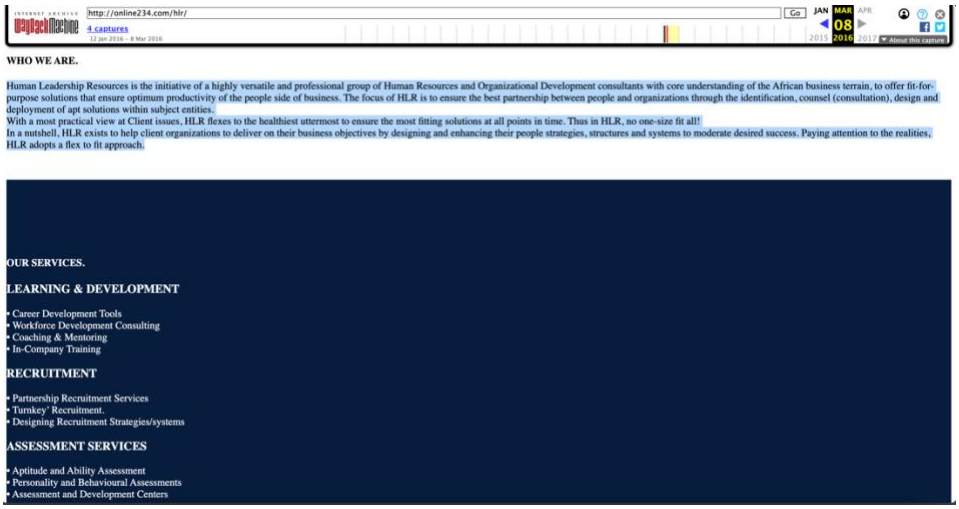
At the D drive there is a folder called "Shared Docs" which contains a file called "Final_Test.pdf" which was from that link which means that this is the file downloaded from that link. The file has the following result on VirusTotal:

- Final_Test.pdf
  - 

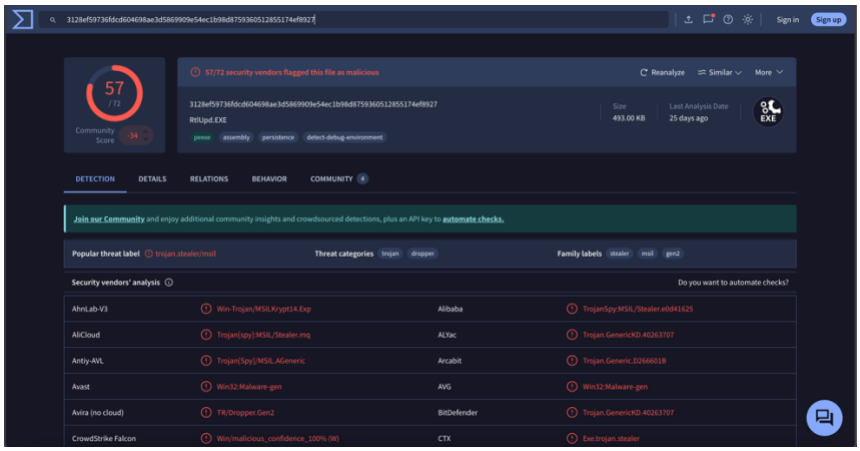
The file is malicious with 62 out of 72 security vendors marking it as malicious. It is a trojan which tries to steal information, based on the "loki" label.

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.



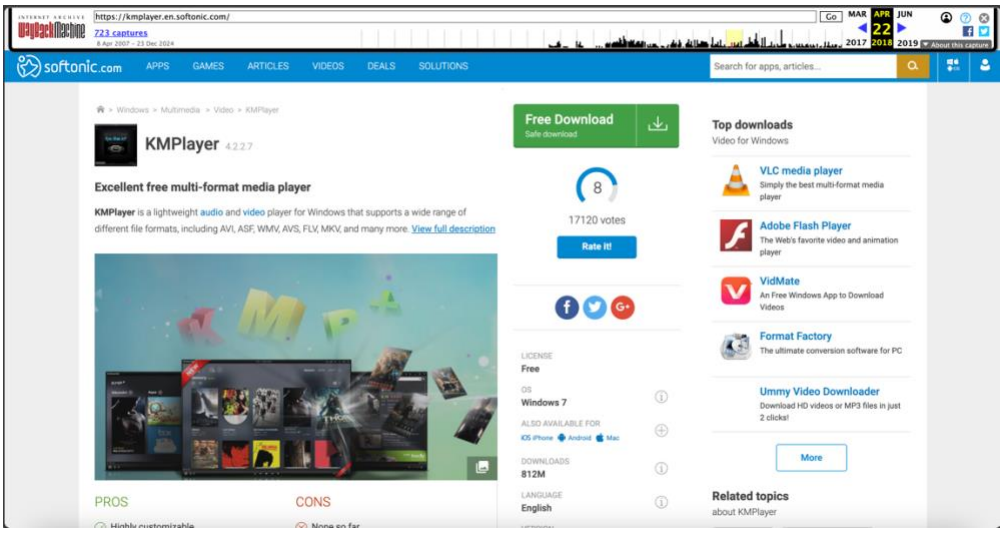
At 02:27:08 UTC+8, on the "Downloads” folder a file called “loder.exe” was downloaded from that link. The file has the following result on VirusTotal:

- Loder.exe
  - 

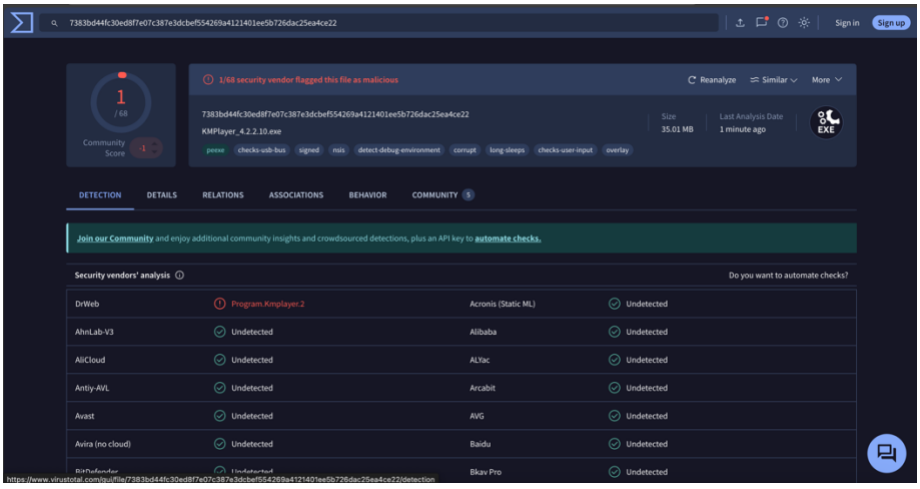
The more common name for that executable file is “RtlUpd.EXE”. It is a malicious file with 57 out of 72 security vendors marking it as malicious. It is a dropper which means that it is used to transport and execute other malware on the machine.

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.



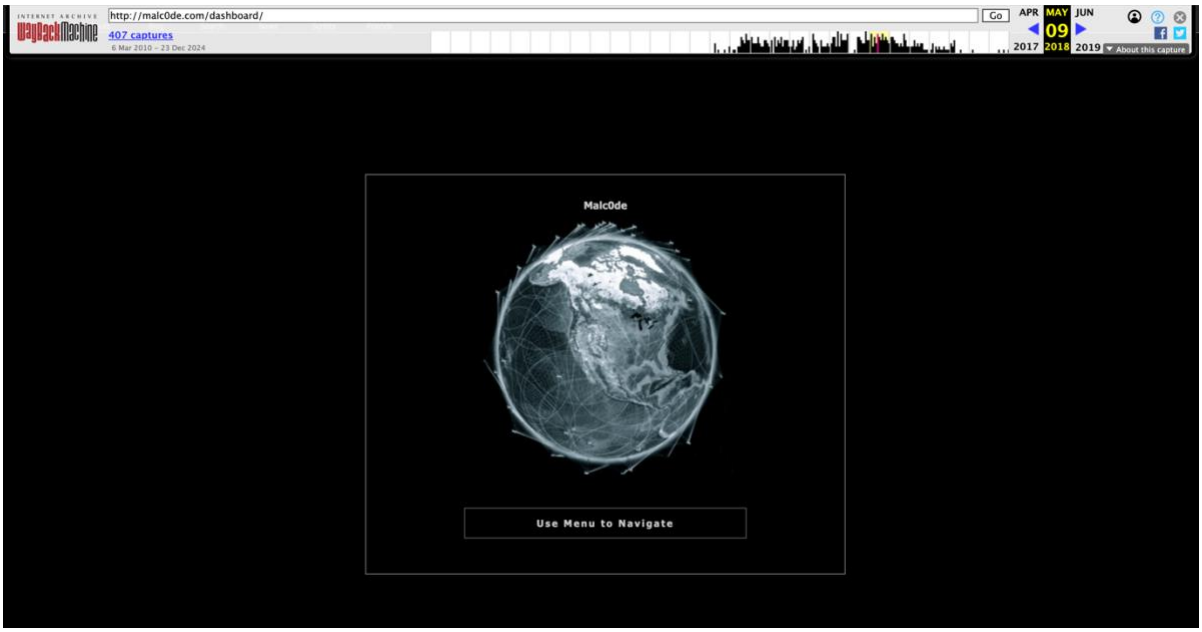
It seems to be a website discussing KMPlayer and the place to download the software. KMPlayer seems to be a media player to play audio and video with a range of formats. At 10:27:54 UTC+8, the file is created in the “Downloads” folder with the same name, “KMPlayer_4.2.2.10.exe”. The file has the following result on VirusTotal:

- KMPlayer_4.2.2.10.exe
  - 

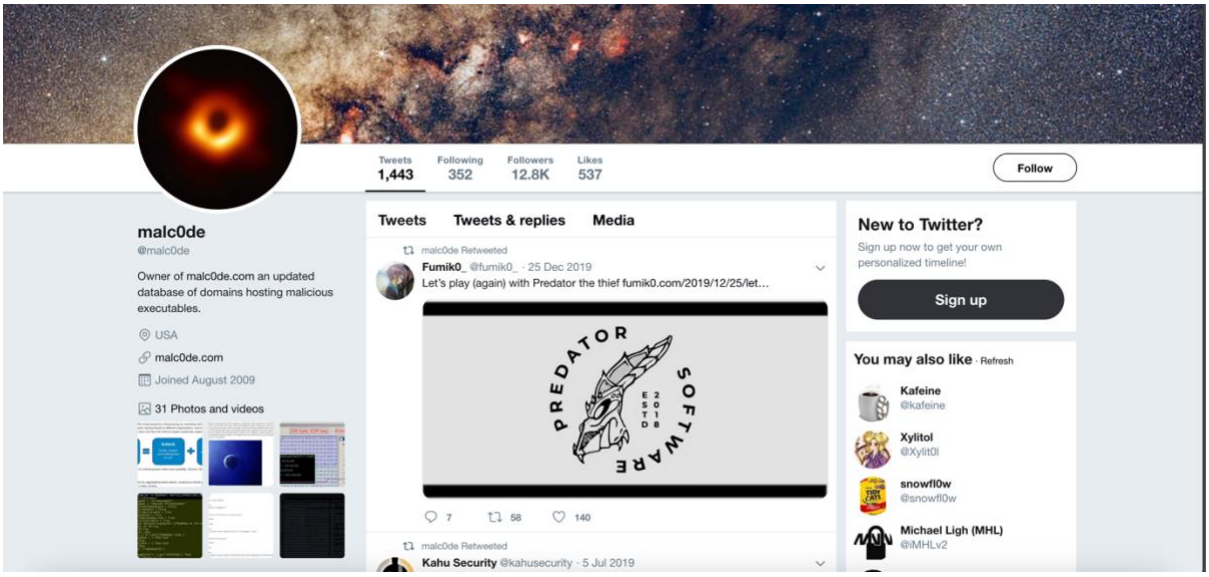
The file seems to be safe and non-malicious as it is only being flagged by 1 vendor out of 68. However, further research shows that it might be adware, which is a form of malware in which unwanted advertisements pop up on the machine.

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.

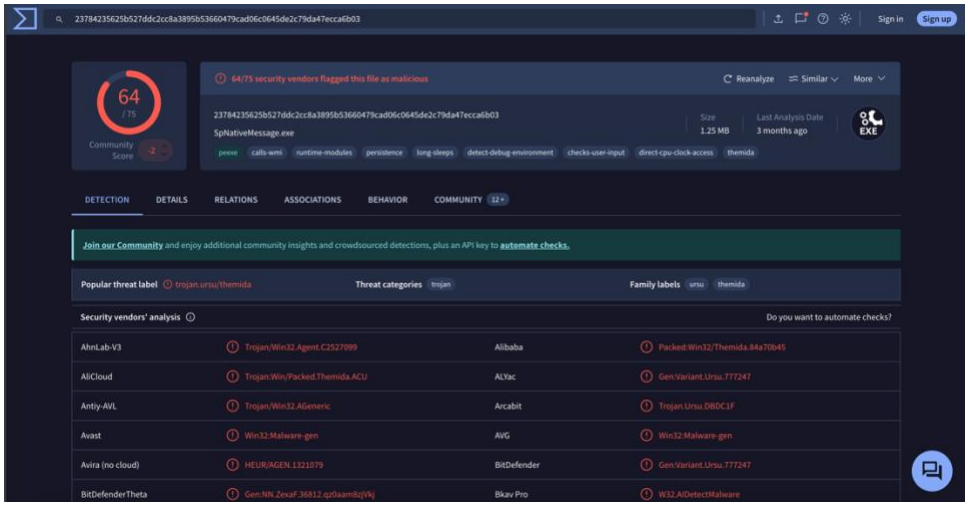


Based on the twitter account, malc0de is a database of domains that host malicious executable files. Previously analysed websites and links that appear to be legitimate but could be used to download malicious executable files might be part of this database, but there is no definite proof of it.

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

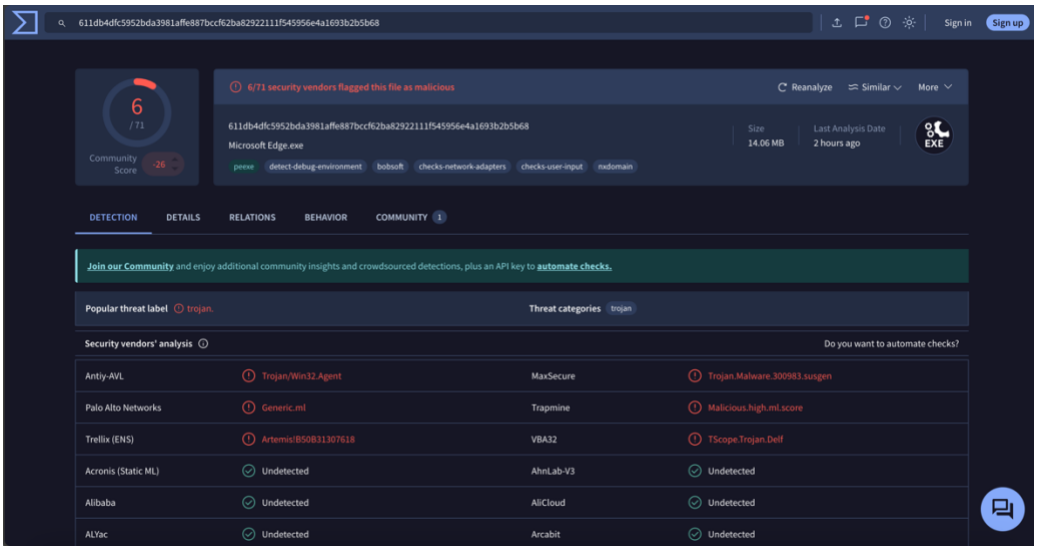
The website is currently unavailable and there are no archives on the website. This website is a domain which hosts malicious files, in this case it is “updsto.exe”, and is part of the malc0de database. The “updsto.exe” executable file is downloaded from the weeknews.pro website and is found in the “Downloads” 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 the disguises itself as legitimate software.

5.3.7 Microsoft Edge.exe

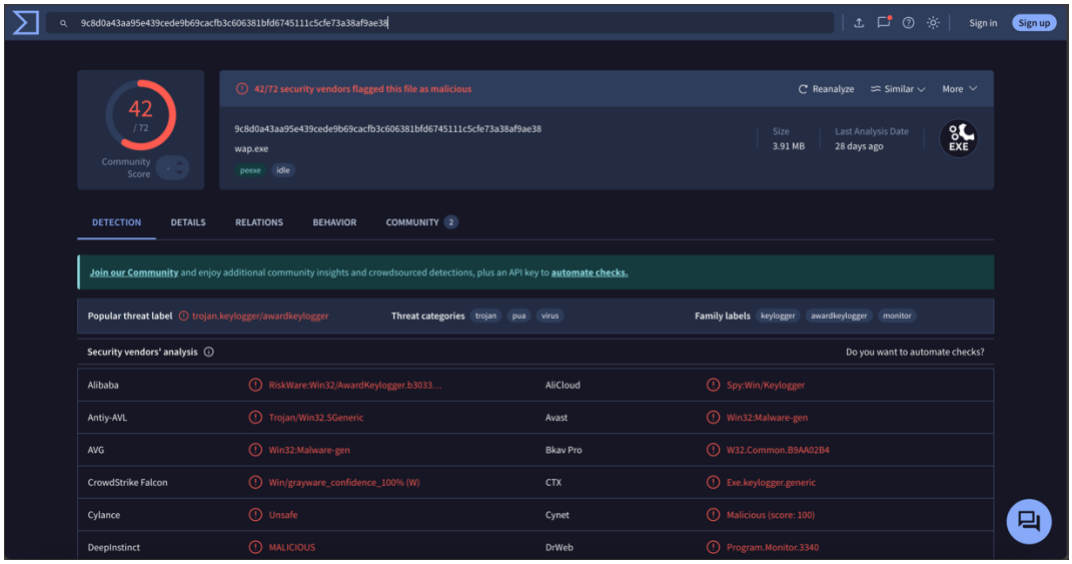
A fake Microsoft Edge was found running on the RAM at the moment it was captured. It is in the “Temp” folder in the “Windows” directory. The file has the following result on VirusTotal:

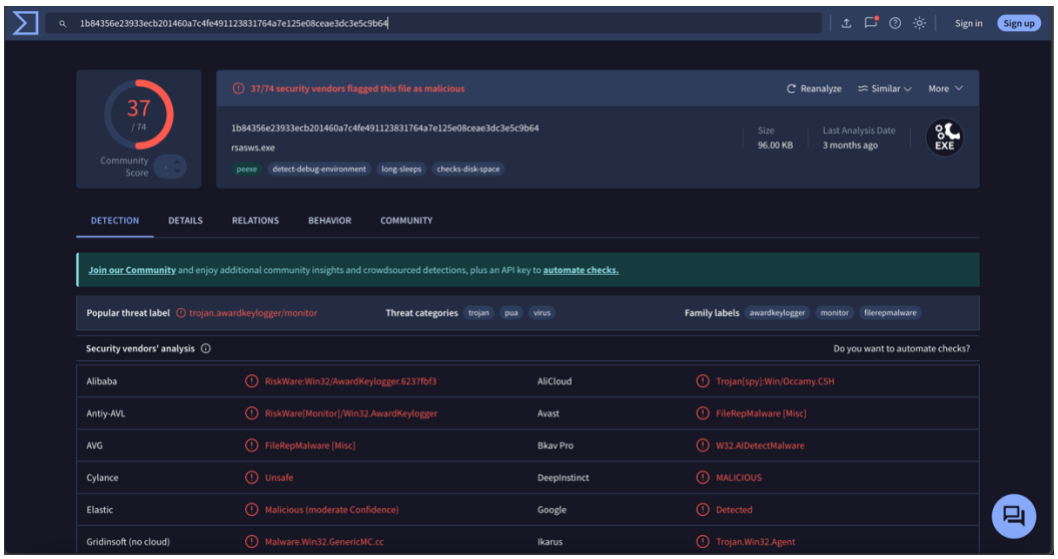
- Microsoft Edge
  - 

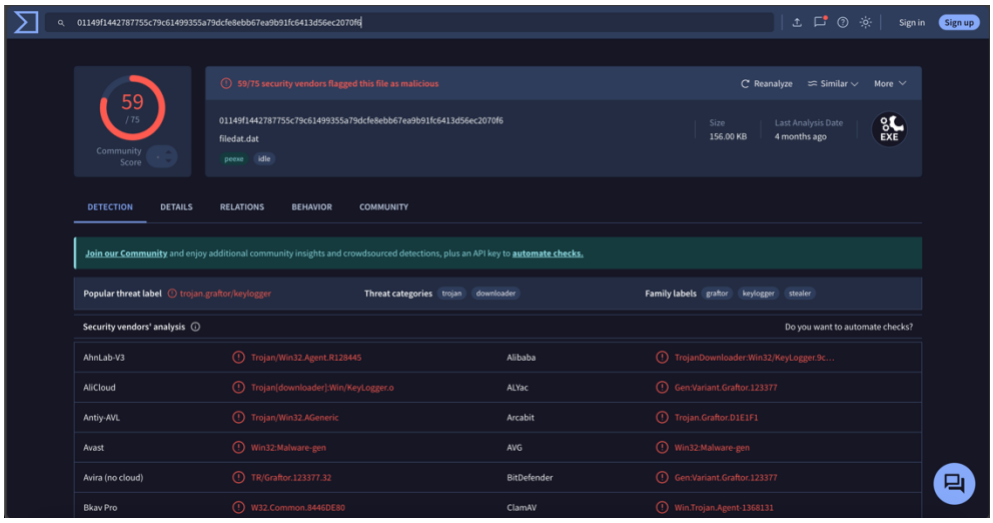
The file could be malicious as it is flagged by 6 out of 71 security vendors. It is a trojan which is a malicious software that hides itself by pretending to be a legitimate program, in this case Microsoft Edge.

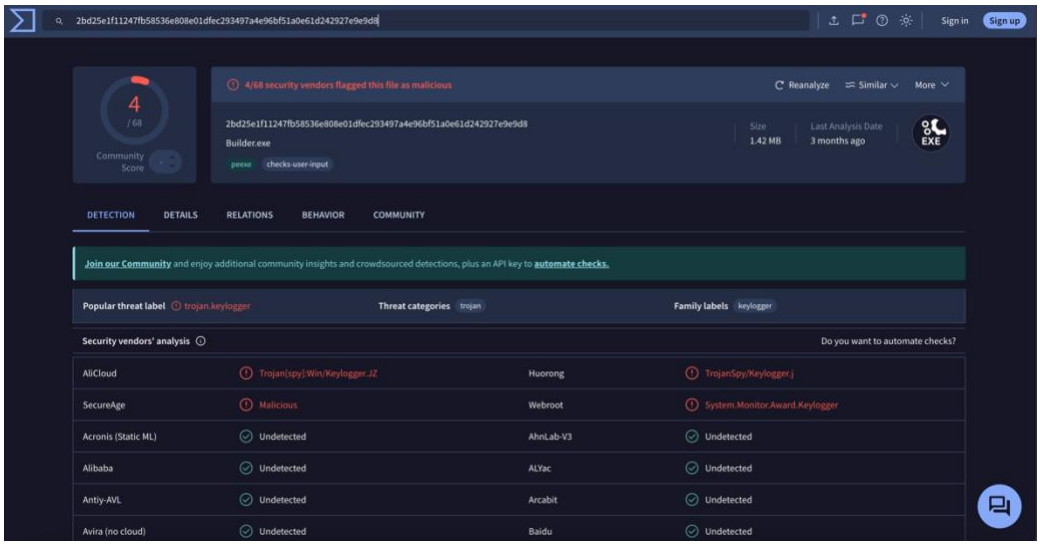
5.3.8 ProKAward

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
  - 

- rsasws.exe
  - 

- filedat.dat
  - 

- Builder.exe
  - 

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_ursu.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/