FORENSICS REPORT

By Ajibade Ayodeji

Glasgow Caledonian University

Cyber Forensics and Incident Response



**Table of Contents**

|  |  |
| --- | --- |
| **Table of Contents** | 1 |
| **Case 1** | 2 |
| Overview/Summary | 2 |
| Objectives | 2 |
| Evidence | 2 |
| Investigation Steps | 2 |
| Findings & Conclusion | 2 |
| Exhibits | 3 |
| **Case 2** | 7 |
| Overview/Summary | 7 |
| Objectives | 7 |
| Evidence | 7 |
| Investigation Steps | 7 |
| Findings & Conclusion | 7 |
| Exhibits | 8 |
| **Case 3** | 10 |
| Overview/Summary | 10 |
| Objectives | 10 |
| Evidence | 10 |
| Investigation Steps | 10 |
| Findings & Conclusion | 10 |
| Exhibits | 12 |
| **Reference** | 16 |

**CASE 1**

**1.1 Overview/Summary of Case**

A Swiss Bank security team brought in to the lab an android phone belonging to a suspected online fraudster who is suspected to have carried out various Bank and crypto scam.

* 1. **Objectives**

The objective is to carry out deep analysis of the phone to find artefacts (images, text messages, audio files, applications) that might have been used to facilitate the scams. This will help persecute the suspect in the court of law.

**1.3 Evidenced Analyzed**

The Android image of the confiscated Samsung Phone will be thoroughly analysed.

**1.4 Investigation Steps**

In other to maintain the forensic integrity of the android phone, it is kept in a Faraday bag to avoid remote wipe of contents in the device.

An image of the phone was created and it was hashed. The duplicated image was then loaded on Autopsy, a mobile forensics tool (Fig 1.1) to carry out the analysis/ investigation.

**1.5 Findings & Conclusion**

On checking the phone, an application used for encrypting text messages was found installed on the suspect’s device (Fig 1.2), this has some messages encountered to be encrypted. A particular message “SIGNAL: Your code is 194-..” was received from an encrypted number on the 18th of April 18, 2021, same day a bank scam was carried out on a major account (Fig 1.3). A screenshot of Swisscom was found in the images folder (Fig 1.4). Another image (Fig 1.5) shows an instruction given to the suspect in German. The translation in English is: “Download <https://bit.ly/3wDLAKx>, await further instructions”, which suggests that the suspect works with someone. The suspect is clearly dealing in cryptocurrencies as there were several images of bitcoin transactions in hi crypto wallet (Fig 1.6).

A shocking discovery was made whilst going through the suspect’s web account (Fig 1.7), as multiple login attempt was made with an unknown person’s email address. The password entered eventually led to a successful login by the suspect (Fig 1.8), thus leading to an account creation (Fig 1.9). It is important to take note of the logo found in “Fig 1.5” as this was also found in the last exhibit (i.e Fig 1.10). The last exhibit shows a screenshot from an unknown person (possibly a cohort), instructing the suspect to lay low.

This message denotes that a criminal activity recently took place and the suspect carried out the activity. Piecing these evidences together, it is evident that the suspect is complicit.

**1.6 Exhibits**



Fig 1.1

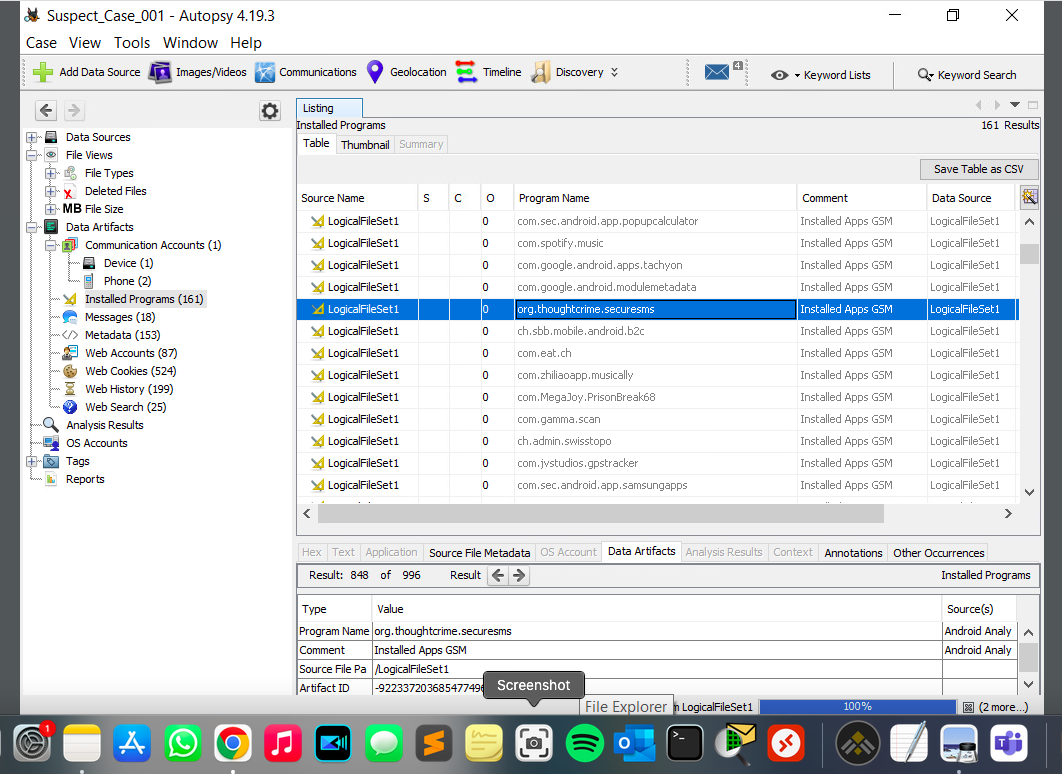


Fig 1.2

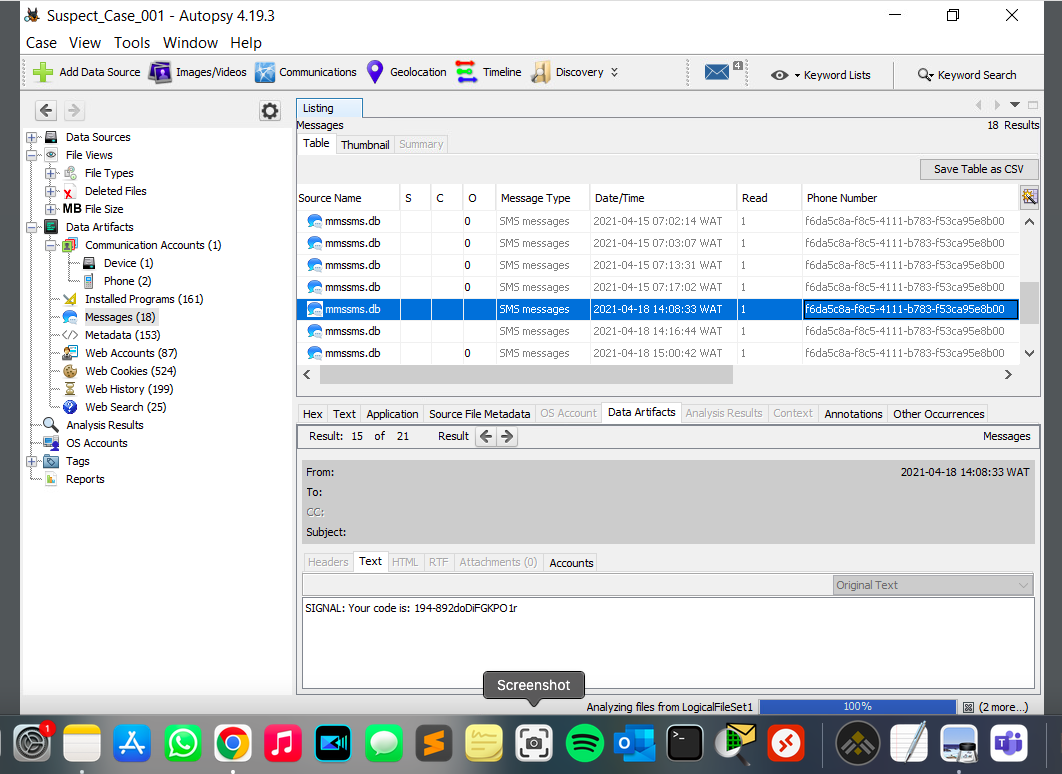


Fig 1.3

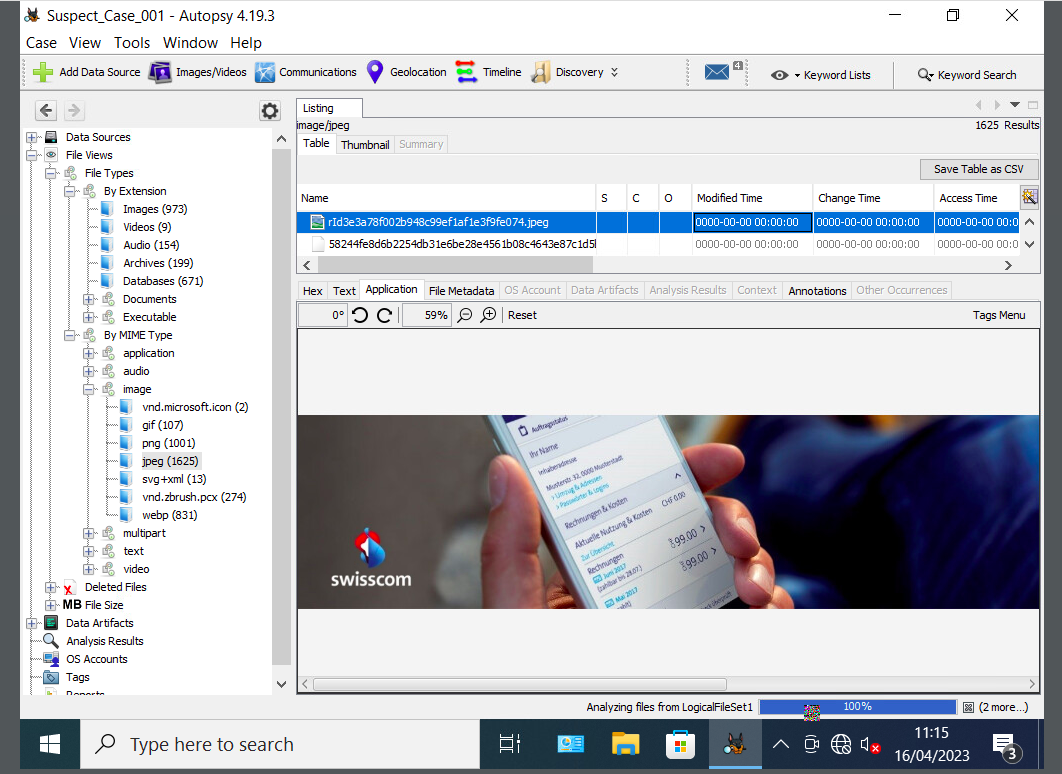


Fig 1.4

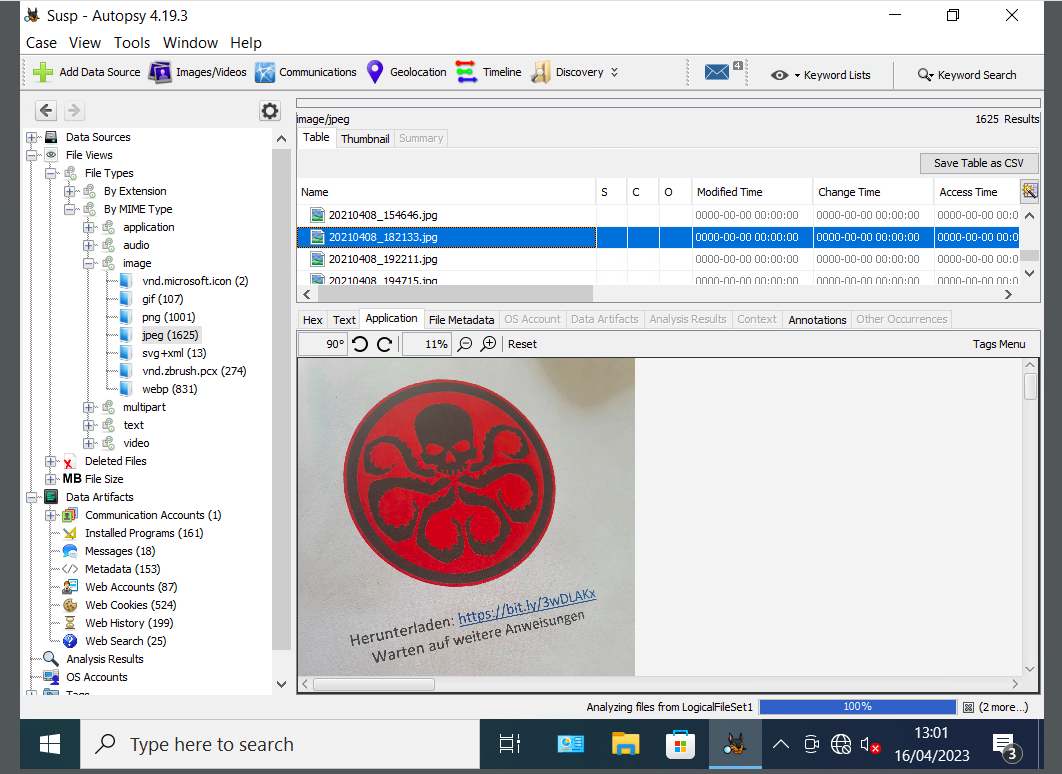


Fig 1.5

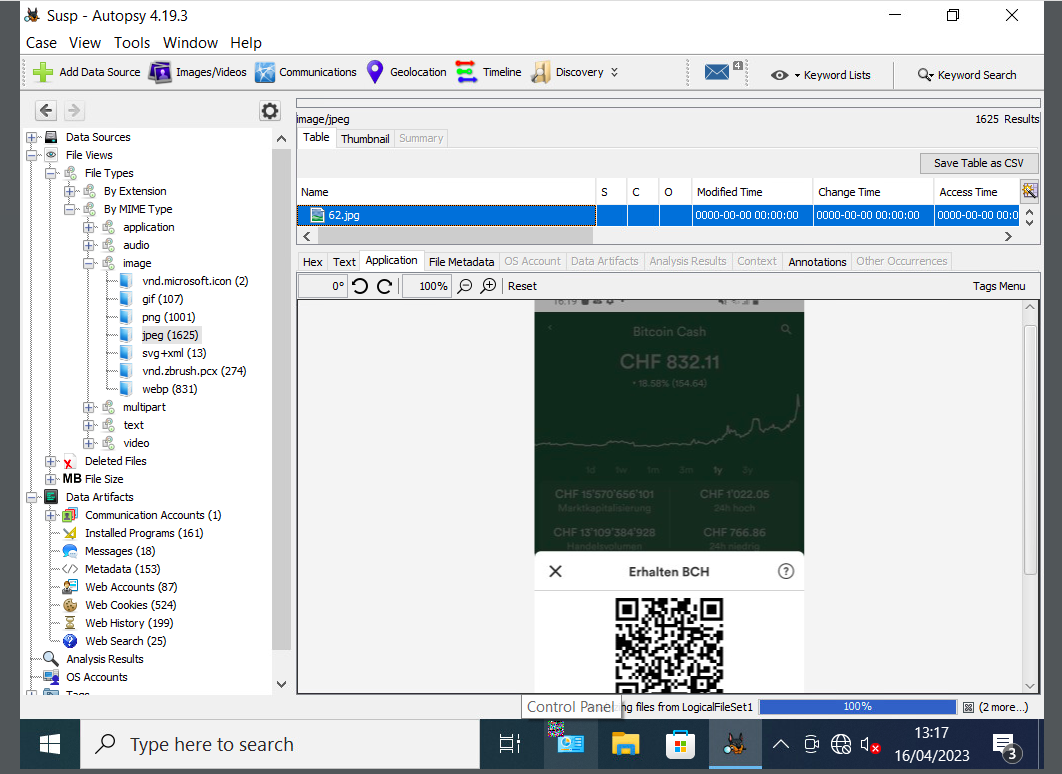


Fig 1.6

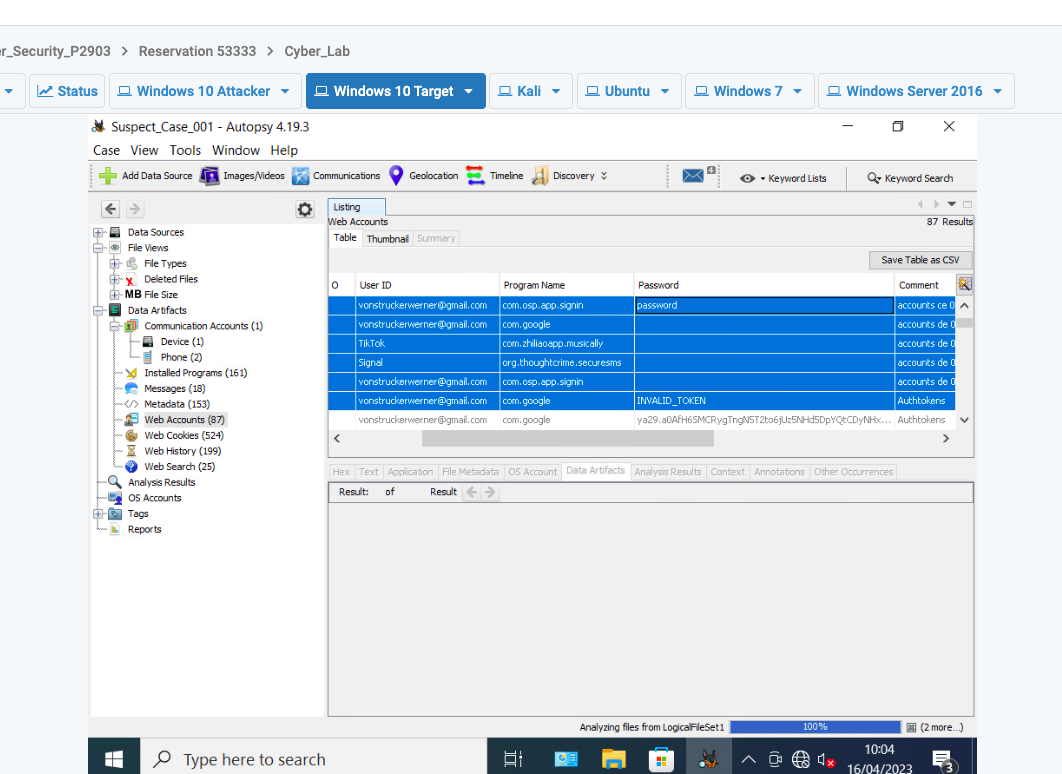


Fig 1.7

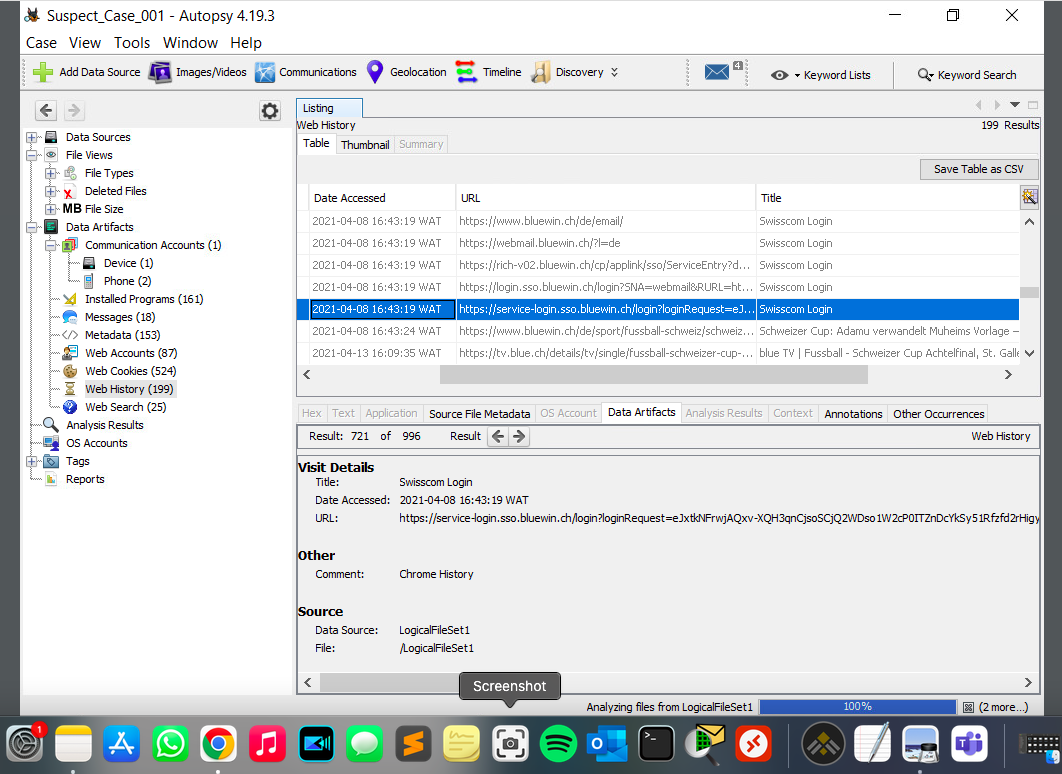


Fig 1.8

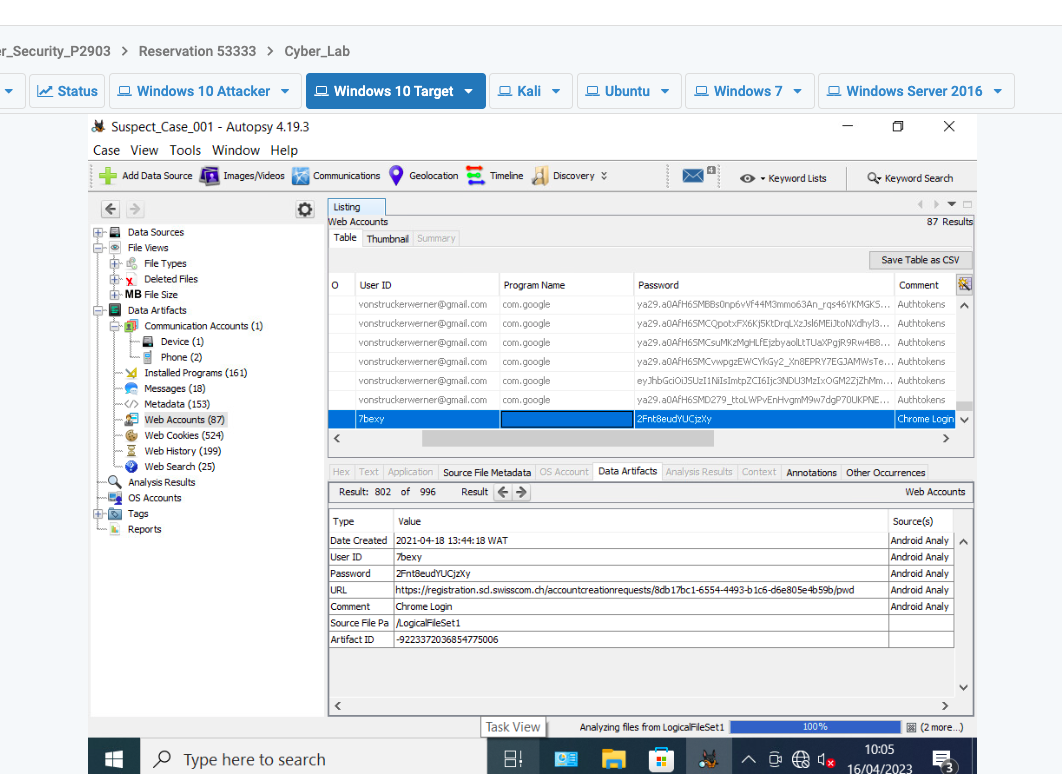


Fig 1.9

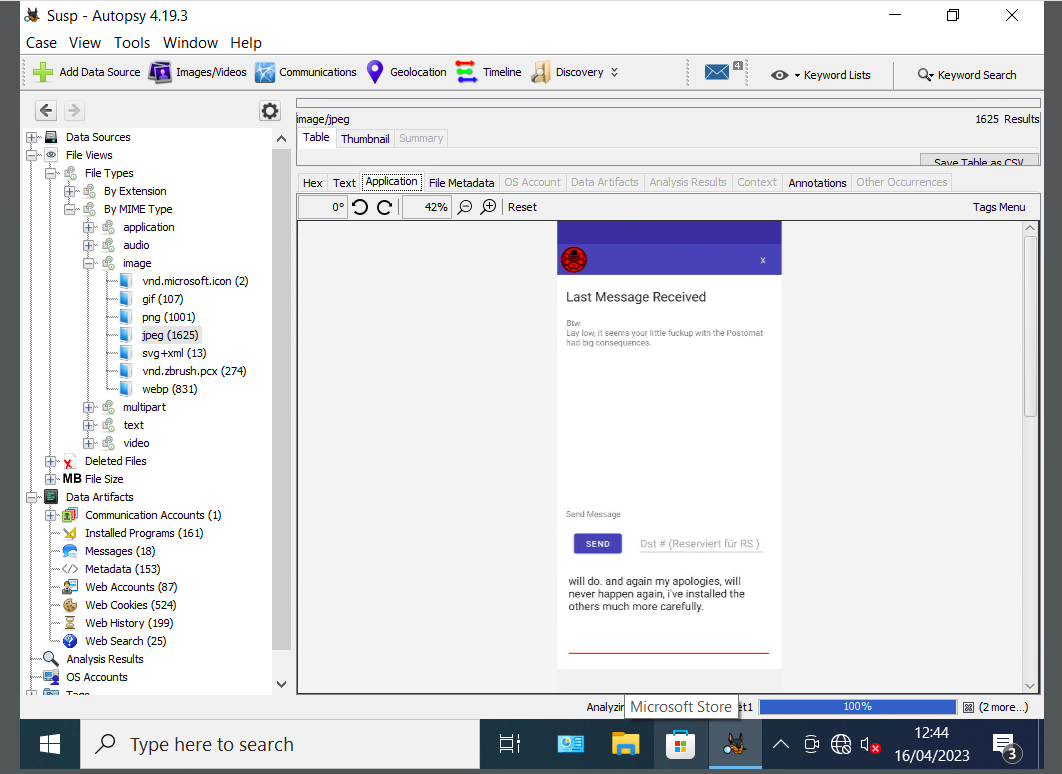


Fig 1.10

**CASE 2**

**2.1 Overview/Summary of Case**

A law enforcement officer has confiscated a suspect’s hard disk and submitted it to the lab for forensic analysis as evidence from the hard disk might help with the case the officer is building.

**2.2 Objectives**

An image of the hard disk will be copied and then analysed to know the file system type, content information, deleted information and metadata. This information will determine if the suspect is complicit.

**2.3 Evidence**

The image of the hard disk is the only evidence to be analysed.

**2.4 Investigation Steps**

In other to maintain the forensic integrity of the obtained hard disk or evidence, a duplicate of the hard disk and hash will be generated. The obtained suspect hard disk was replicated using Autopsy, an open-source tool for analyzing an image. The image (i.e hard disk) was mounted on Autopsy to have access to the artefacts and the filesystem.

**2.5 Findings & Conclusion**

* In Figure 2.1, the evidence from the File System Information shows that the file system type and Original Equipment Manufacturer (OEM) is **NTFS** and the version of the hard disk a **Windows XP**.
* In Figure 2.2, the Metadata shows the following: First Cluster of MFT: 87381; First Cluster of MFT Mirror: 131071; Size of MFT entries: 1024 bytes; and the size of Index Records: 4096 bytes which point to the NTFS file system.
* In Figure 2.3 below, there is no suspicious modification noticed with the content information of the hard disk.
* Three files were recently deleted and this can be viewed in exhibits (figure 2.4)

Given the findings above, there is no compelling digital forensic evidence that could be helpful or used in solving the given case.

**2.6 Exhibits**

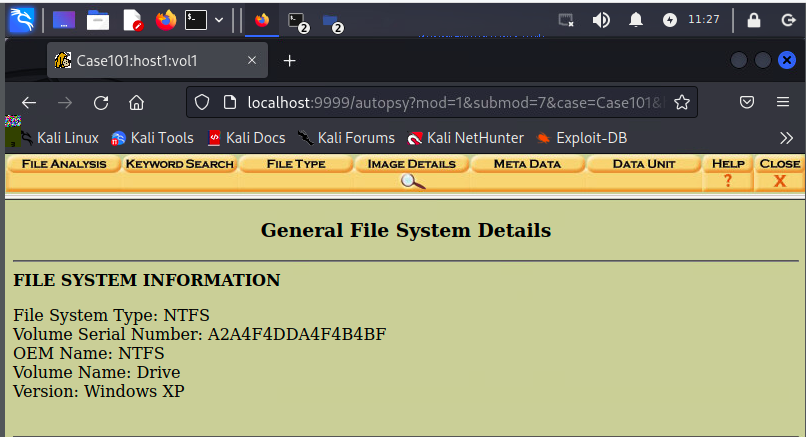
****

Fig 2.1

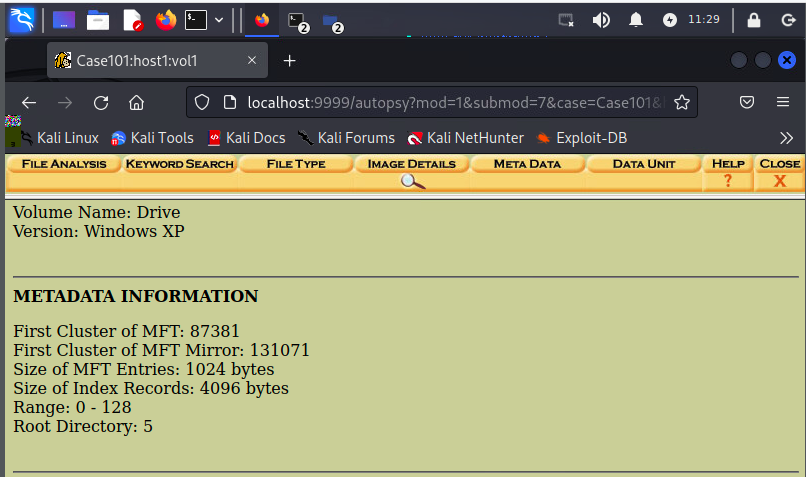
****

Fig 2.2

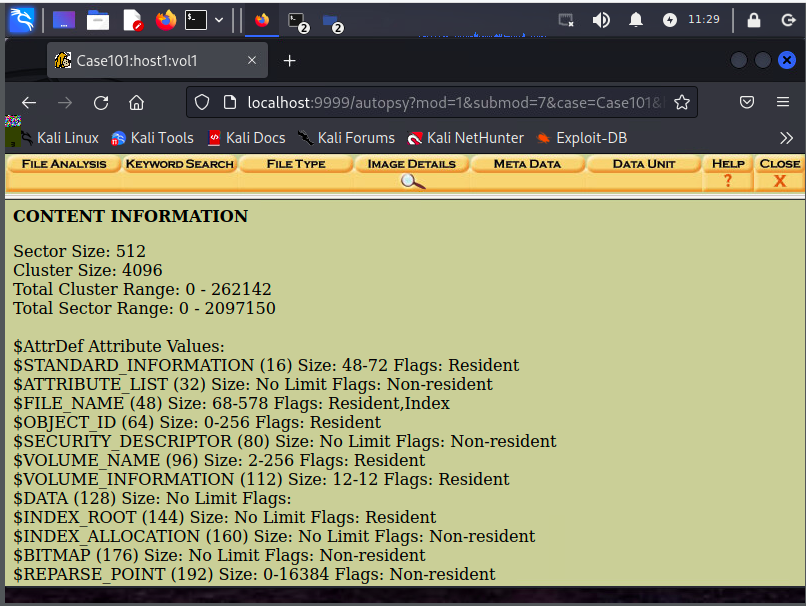
****

Fig 2.3: Content Information

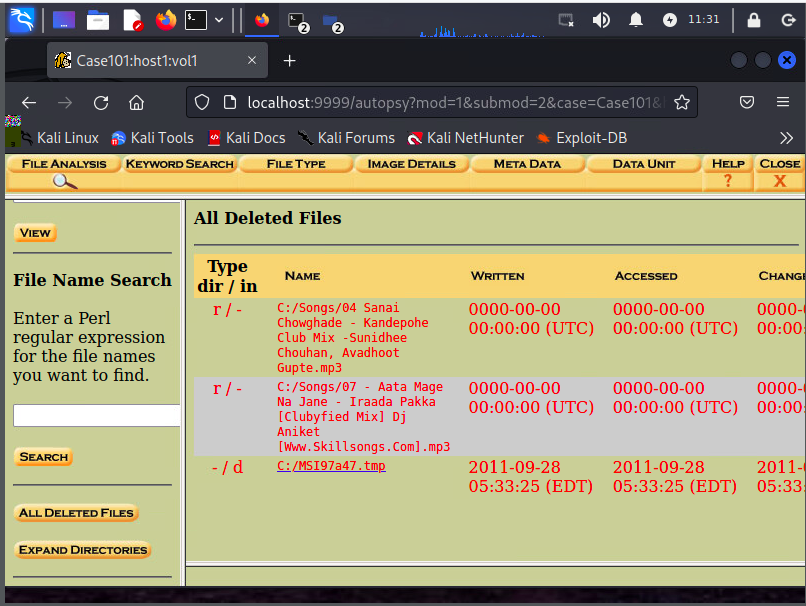
****

Fig 2.4: All Deleted Files

**CASE 3**

**3.1 Overview/Summary of Case**

A client suspects that a particular file on his computer is malicious and needs confirmation if it is benign or malicious.

**3.2 Objectives**

A static and dynamic malware analysis will be conducted on the binary sample to check for indicators of compromise (if any).

**3.3 Evidenced Analyzed**

The client has provided the binary sample for analysis and to confirm if it's malicious or not.

Sample file name: Sample-7-1-packed

Size: 33kb

File Type: .exe

The binary sample will be analysed using digital forensics tools such as PEStudio & Strings.Exe for the static analysis, and a combination of APIMiner and Process Hacker2 for dynamic analysis.

**3.4 Investigation Steps**

The file format of the binary sample was verified using WinHex, which showed that it is an executable file i.e. it has a ‘.exe’ extension

1. PEStudio: on running PEStuio, the binary sample was loaded to display information that would be analysed (a screenshot of the loaded sample on PEStudio is shown below in Fig 3.1). The MD5 hash of the sample gotten from the information displayed on PESTudio was verified on VirusTotal.
2. APIMiner: The APIMiner.exe run ran on Windows cmd to capture logs of the malware sample. The captured logs were saved in a destination folder for further analysis.

**3.5 Findings & Conclusion**

PEStudio: The entropy value of the sample is 7.776 (fig 3.1) which implies that it is packed. This is usually an indication of a malicious file, as 50% of malware samples have an entropy of 7.2 or greater. The Subsystem (Fig 3.2) indicates that the file utilizes a Console. The compiler stamp shows that the sample was last compiled on the 13th of March 2019. In Fig 3.3, the flags indicate that the Sample performs writeable and executable functions. The dll being used is “kernel32.dll” (Fig 3.4) which is a core Windows library file that allows one have access to a systems’ resources and interface; which confirms that the file utilizes a console on the system. The first four values (i.e. VirtualProtect, UPX0, UPX1 & UPX2)

in Fig 3.5 have been flagged, which indicates that the sample might be malicious. UPX0 – 2 denotes that the file has been heavily packed (compressed and masked) to hide the functionalities and make it difficult to figure out what the sample is coded to do. The sample was developed using Visual Studio and its target Windows Server 2008 (Fig 3.6).

VirusTotal: Results from this platform shows that this sample is potentially a malicious file (fig 3.7) with confirmation from 34 of 62 security vendors. The threat categories are “Trojan and Downloader”. The family of the suspected malicious sample is “Zusy” which has a popular threat label “trojan.zusy”.

APIMiner: Upon downloading the log from APIMiner (Fig 3.8), the following interesting sequential API calls were found in the strings – “**NtDeviceIoControlFile**: allows applications and drivers to have access to the input & output controls of any device”, “**LdrLoadDll**: used for loading dll’s into a program’s address space”, “**NtProtectVirtualMemory**: used for modifying system memory permissions and also hide activities”, “**LdrGetDllHandle**: this gives access to data and functions available in a dll file”, “**GetFileType**: to retrieve file type of a particular file”, “**NtDelayExecution**: this is used to delay execution of a process/program for a certain time”, “**NtTerminateProcess**: it is used for terminating a process along with its threads”, “**NtClose**: this is used to close handles” [1].

In conclusion, the sequence of the API calls indicates that the sample file is designed to access system resources with write and execute functions, then load dlls into a program’s address space whilst staying hidden/undetected. With the **NtDelayExecution** API call, it will most likely delay it’s malicious intent, hence evading detection. It seeks to have control of a system.

Given these findings from static and dynamic analysis, the sample is **malicious** and indicative of a RAT (Remote Access Trojan). The sample might be attached to a file or downloaded in a email.

**3.6 Exhibits**

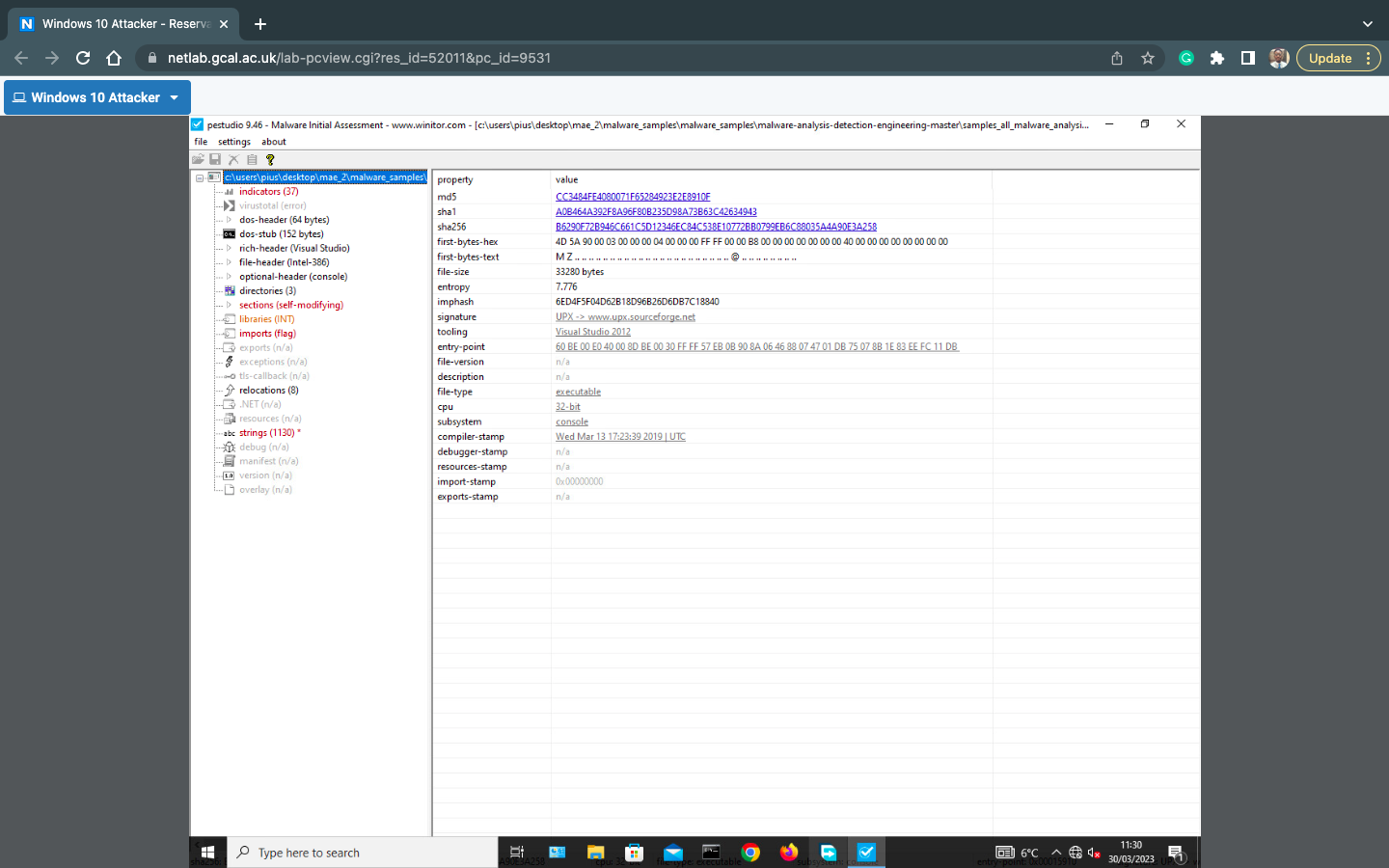
****

Fig 3.1

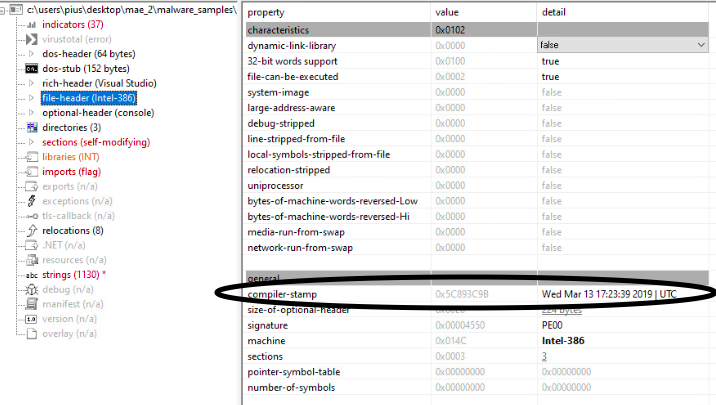


Fig 3.2

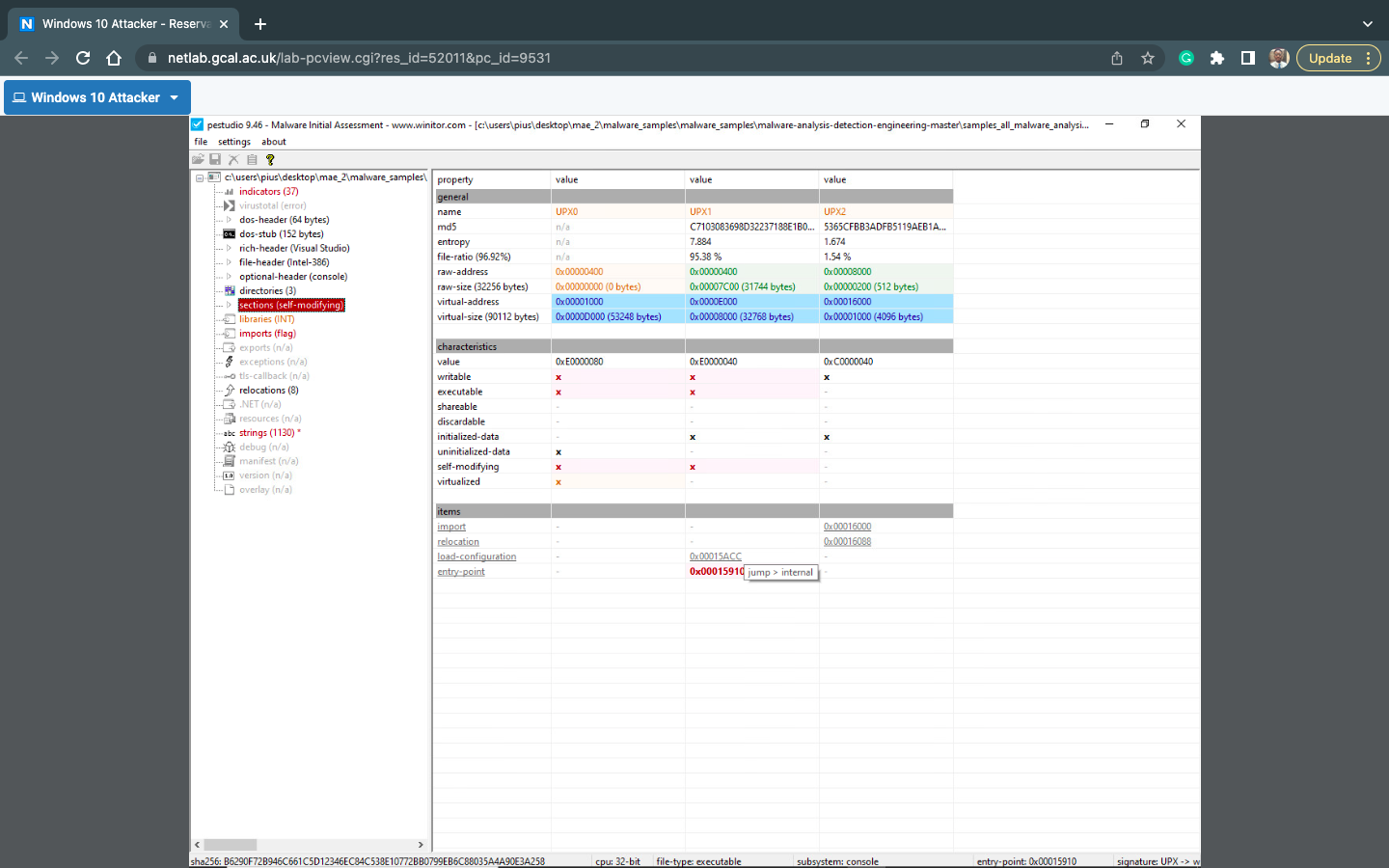


Fig 3.3

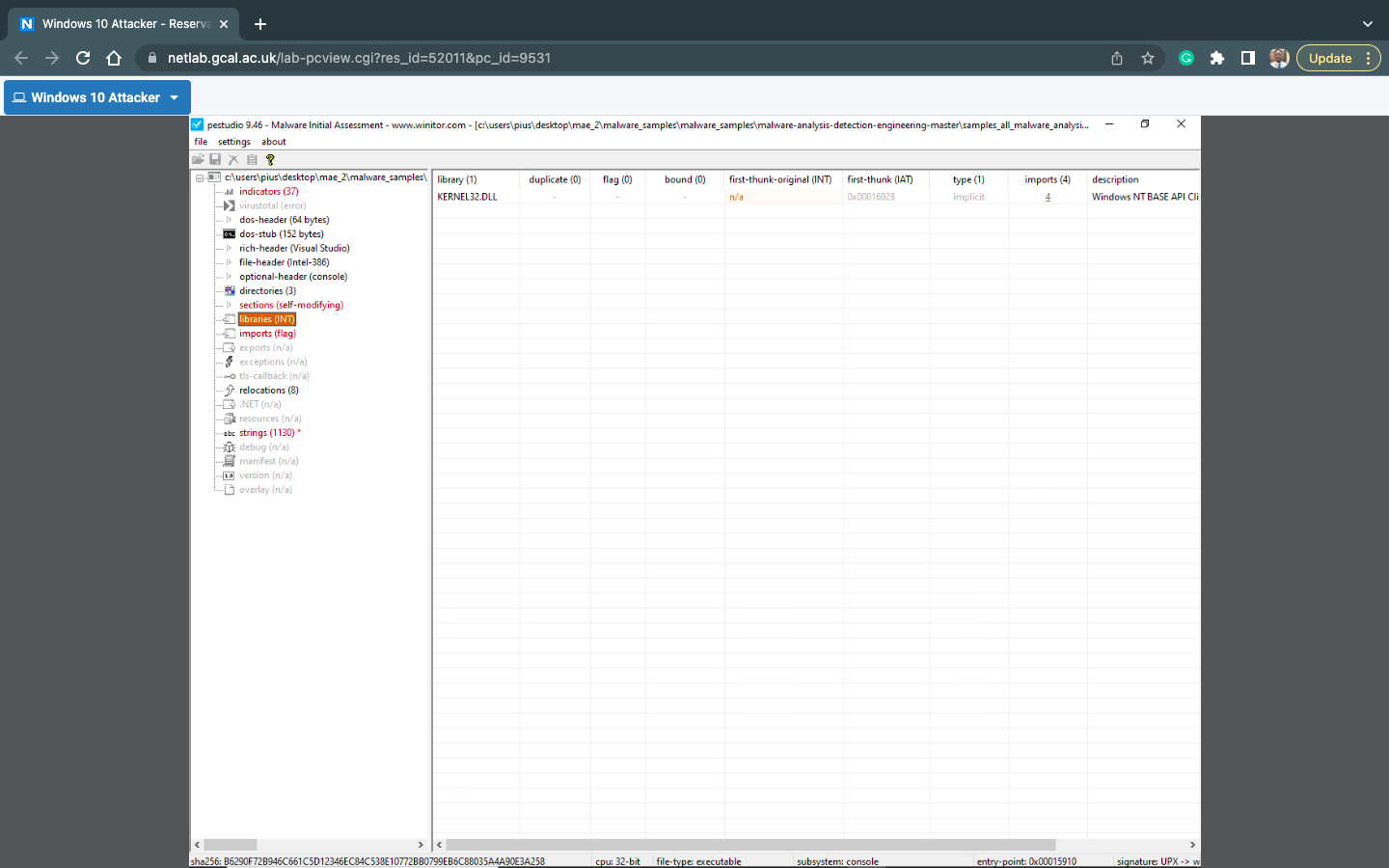


Fig 3.4

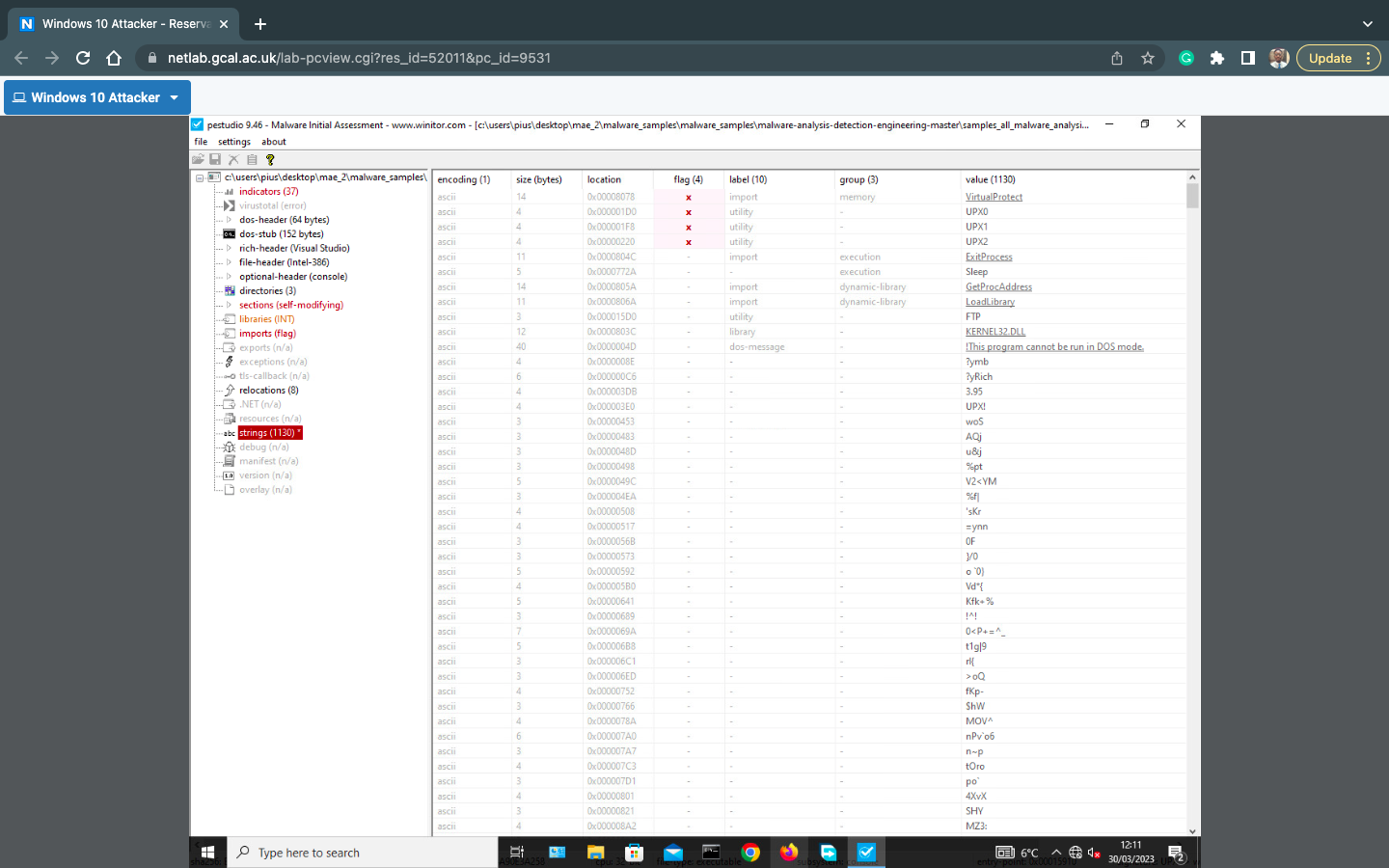


Fig 3.5

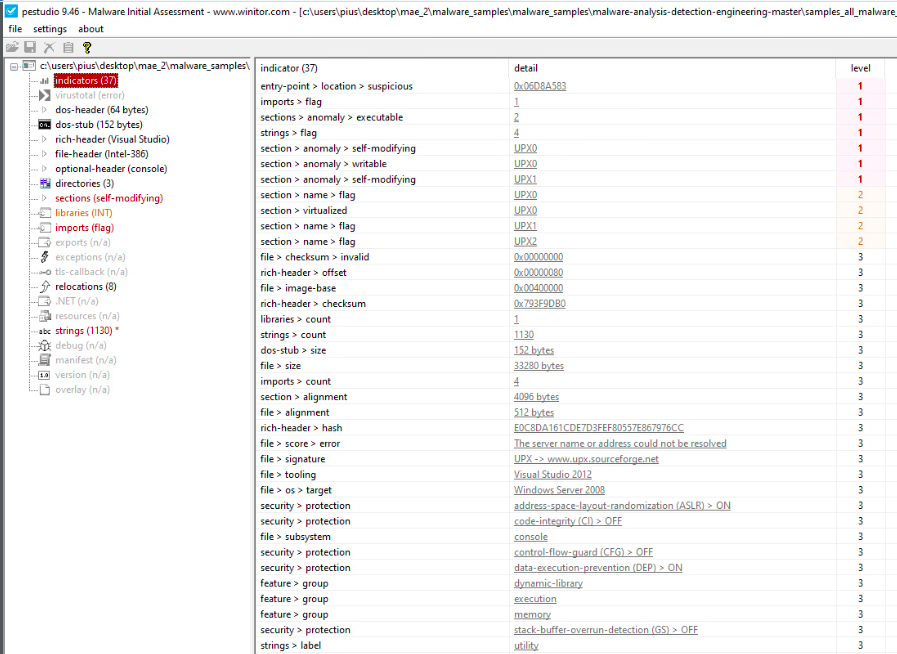


Fig 3.6

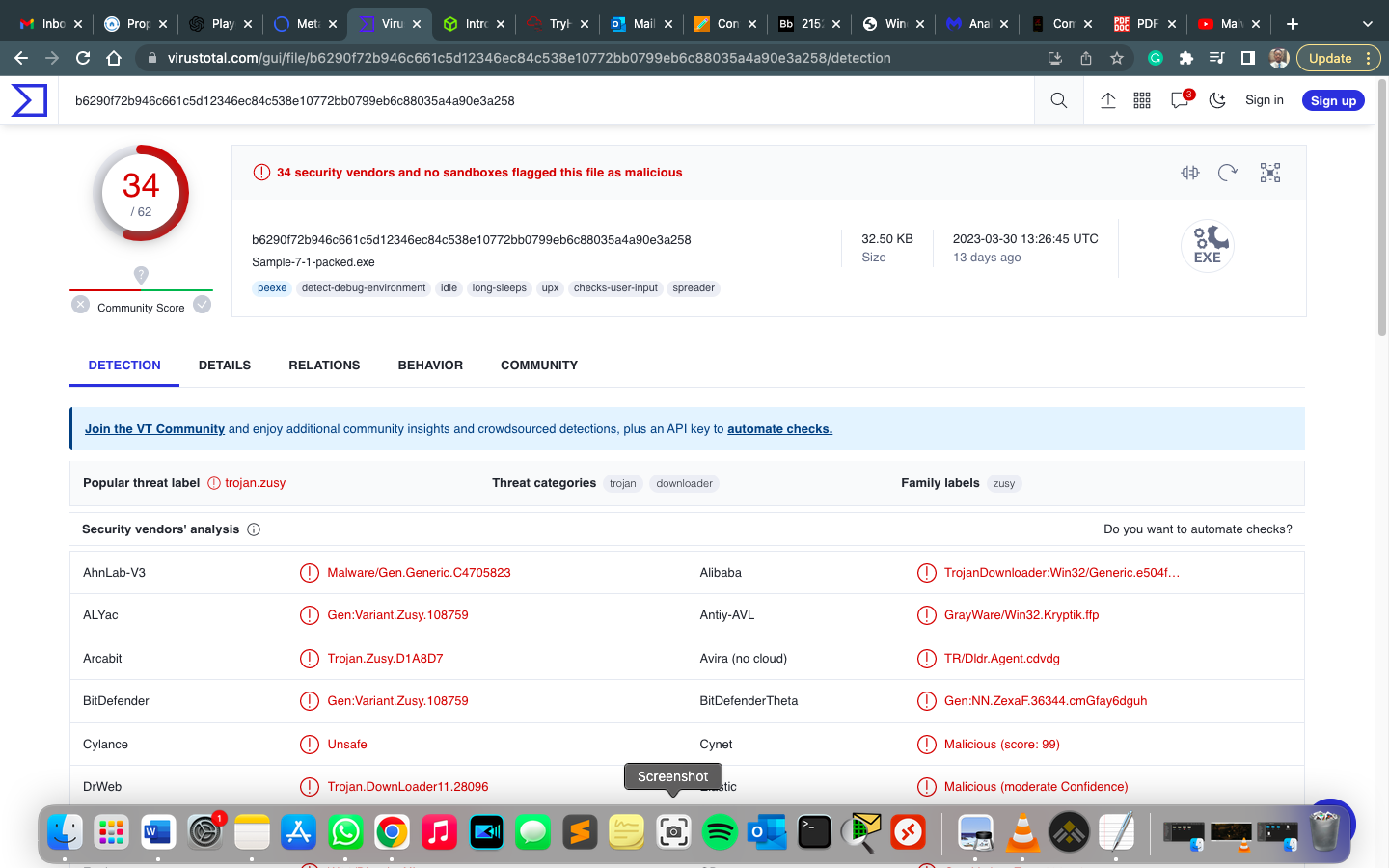
****

Fig 3.7

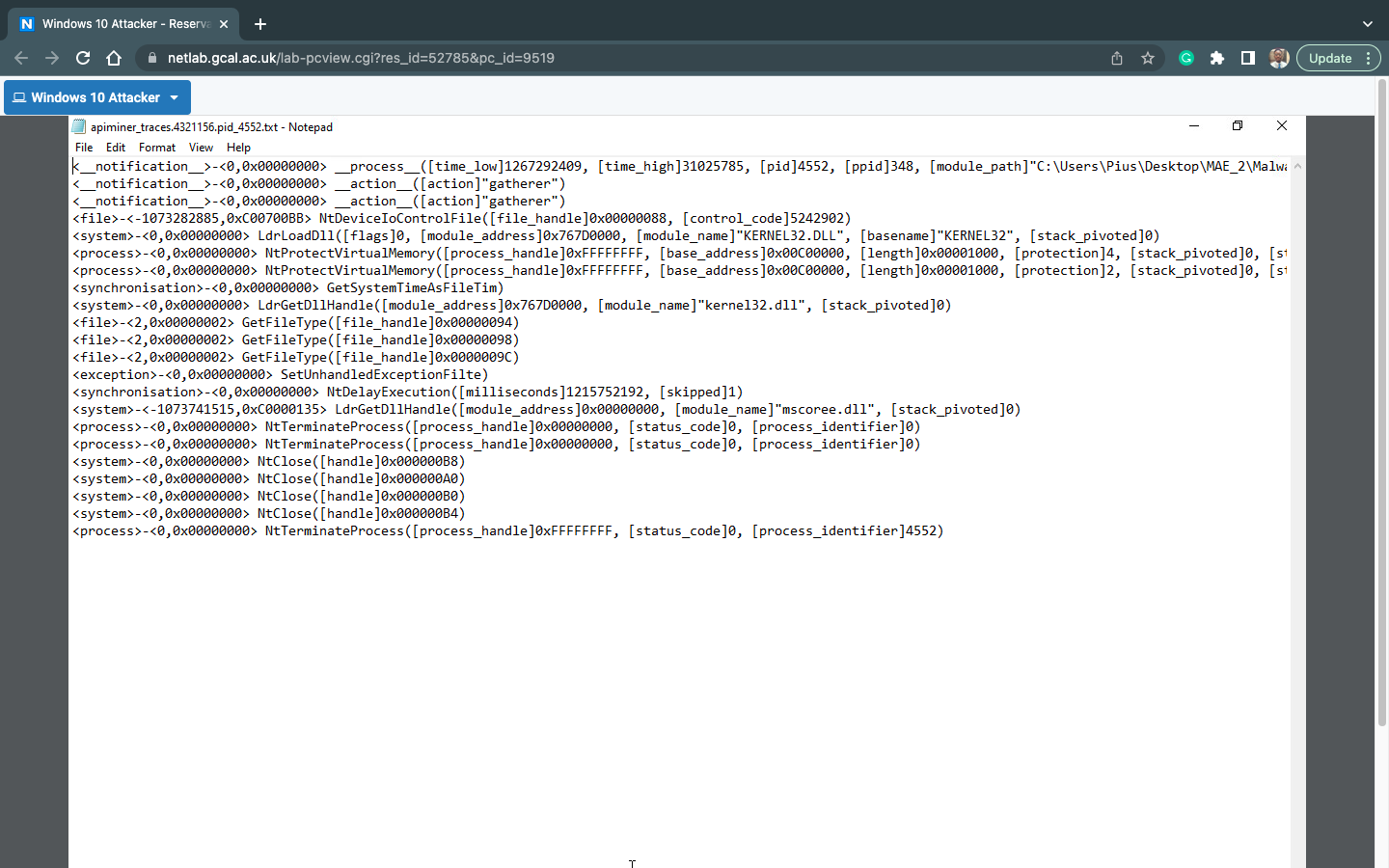


Fig 3.8

**REFERENCE**

[1] Pinvoke.Net. Accessed on 15th April, 2023. <https://www.pinvoke.net/default.aspx/ntdll.NtSuspendProcess>