Martin Mwangi Njoroge

mwangimartins650@gmail.com

CS-SA08-24031

MAL: Malware Introductory

Here's a link to my finished room,

https://tryhackme.com/r/room/malmalintroductory

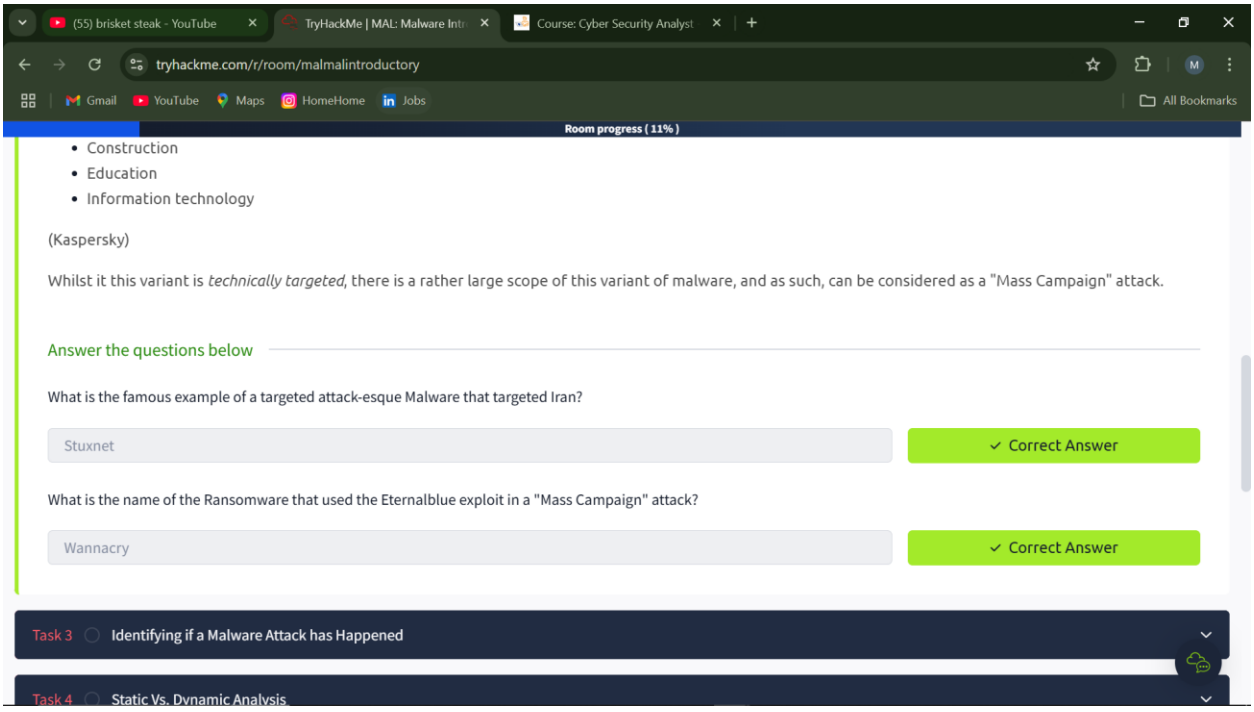
1.0 Introduction

This room focuses on introduction to the techniques and tools used throughout malware analysis. As malware analysis a form of incidence response, and useful in understanding how the behaviors of variants of malware result in their respective categorization.

When analyzing malware, it is important to consider the following; Point of Entry (PoE), indicators that malware has even been executed on a machine, how does the malware perform, can we ultimately prevent and/or detect further infection.

Malware attacks can be categorized as either targeted or mass campaigns.

Questions



1.1 Identifying if a Malware Attack has Happened

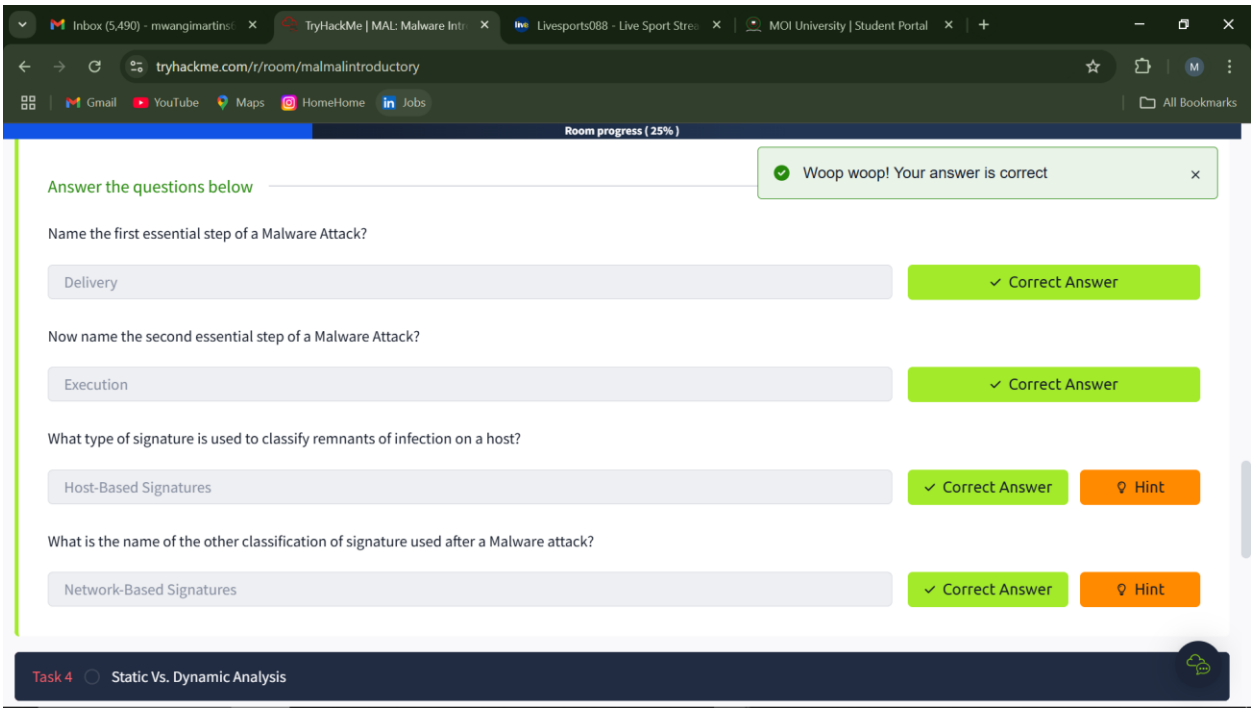
Malware leaves quite an extensive paper trail of evidence, that we can use to conduct an analysis.

Malware attack can be broken down into a few broad steps, delivery, execution, maintaining persistence , propagation.

These steps will generate lots of network traffic such as communicating with hosts, file system interaction like read/writes and modification.

Fingerprints left behind by a malware attack can be host-based signatures (These are generally speaking the results of execution and any persistence performed by the Malware.) and Network-based signatures.

Questions



1.3 Static Vs. Dynamic Analysis

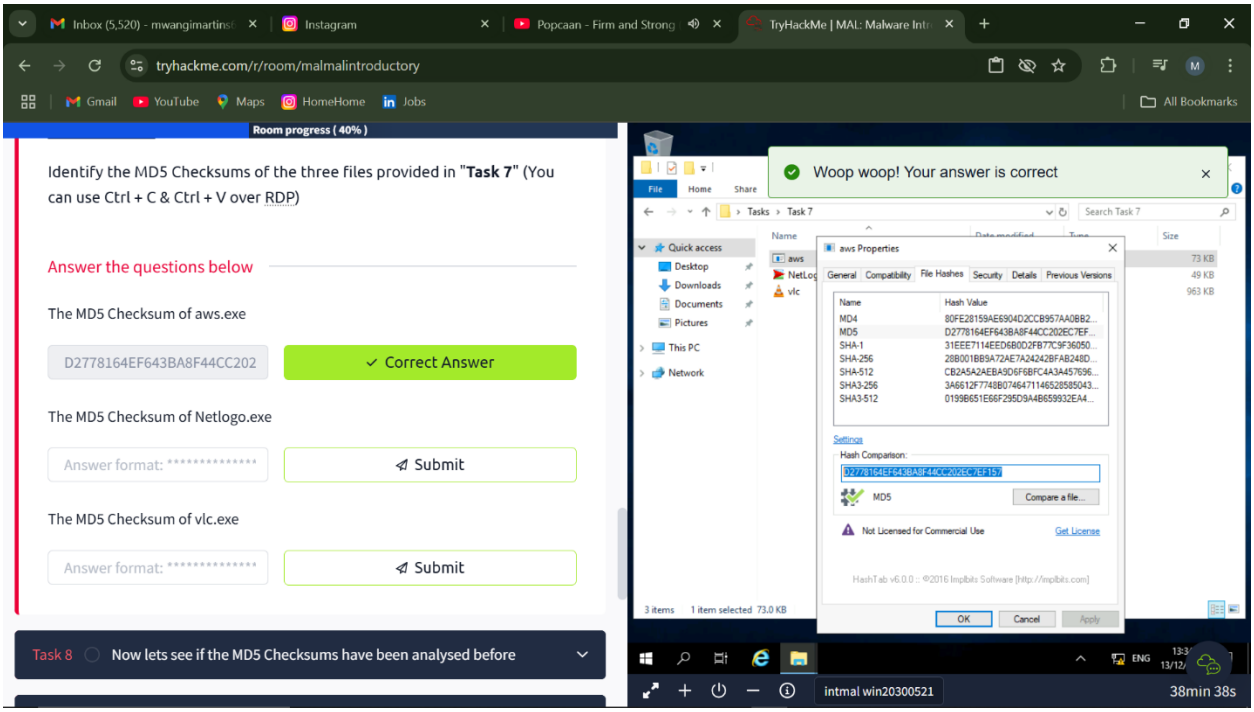
We can analyze a Malware either by static or dynamic analysis.

With static analysis is used to gain a high-level abstraction of the sample, and with dynamic analysis is a lot more involved, and is where the abstraction of the sample is largely built upon and it essentially involves executing the sample and observing what happens.

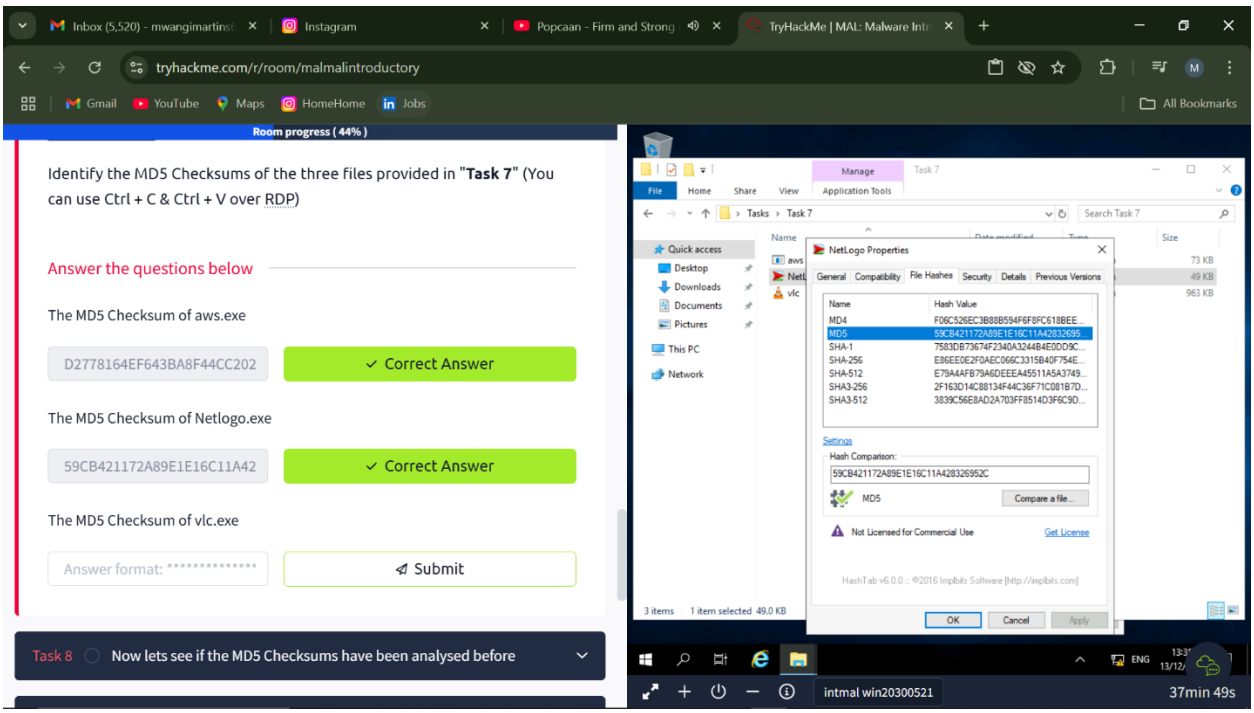
1.4 Obtaining MD5 Checksums of Provided Files

Questions

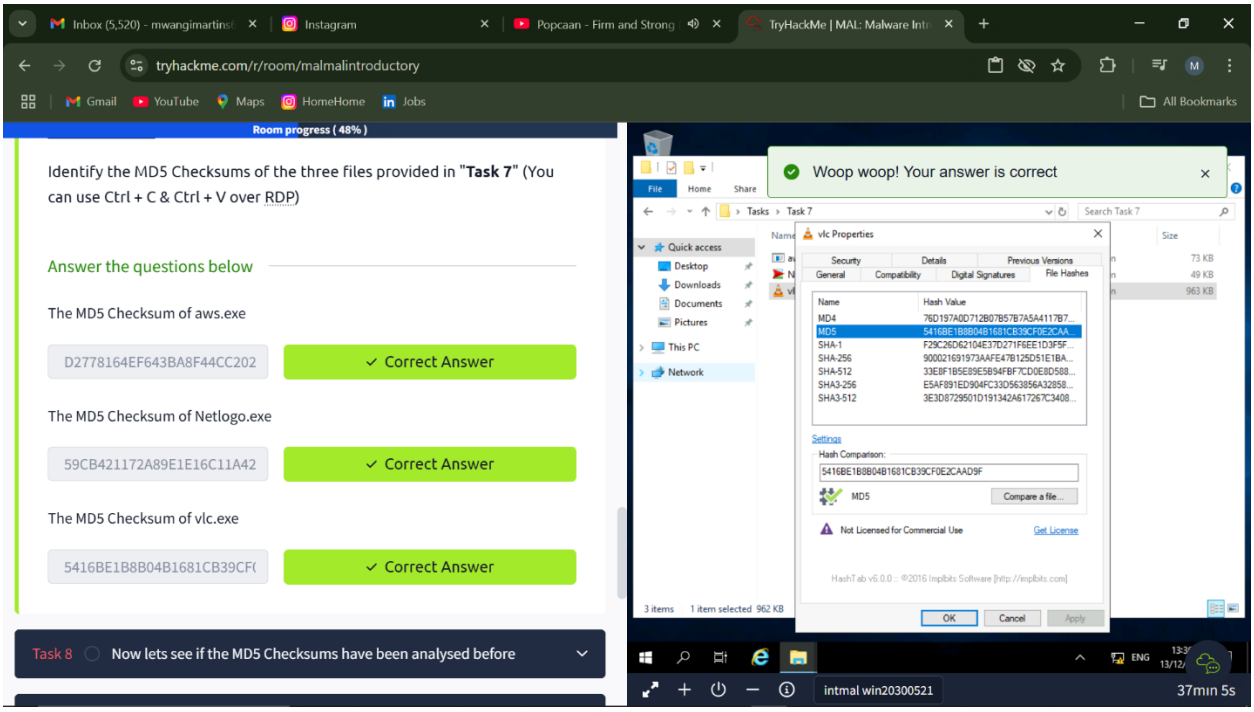
I opened the files properties and then investigated its file hashes where I found the md5 hash



I opened the files properties and then investigated its file hashes where I found the md5 hash

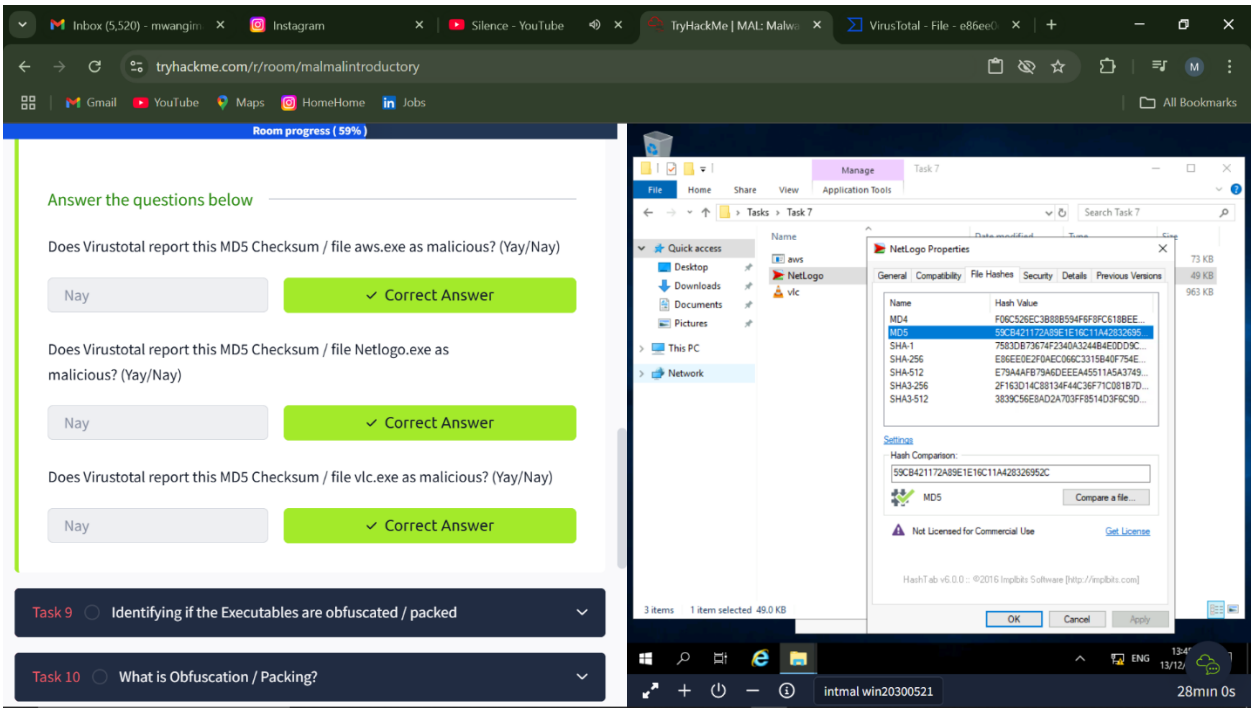


I opened the files properties and then investigated its file hashes where I found the md5 hash

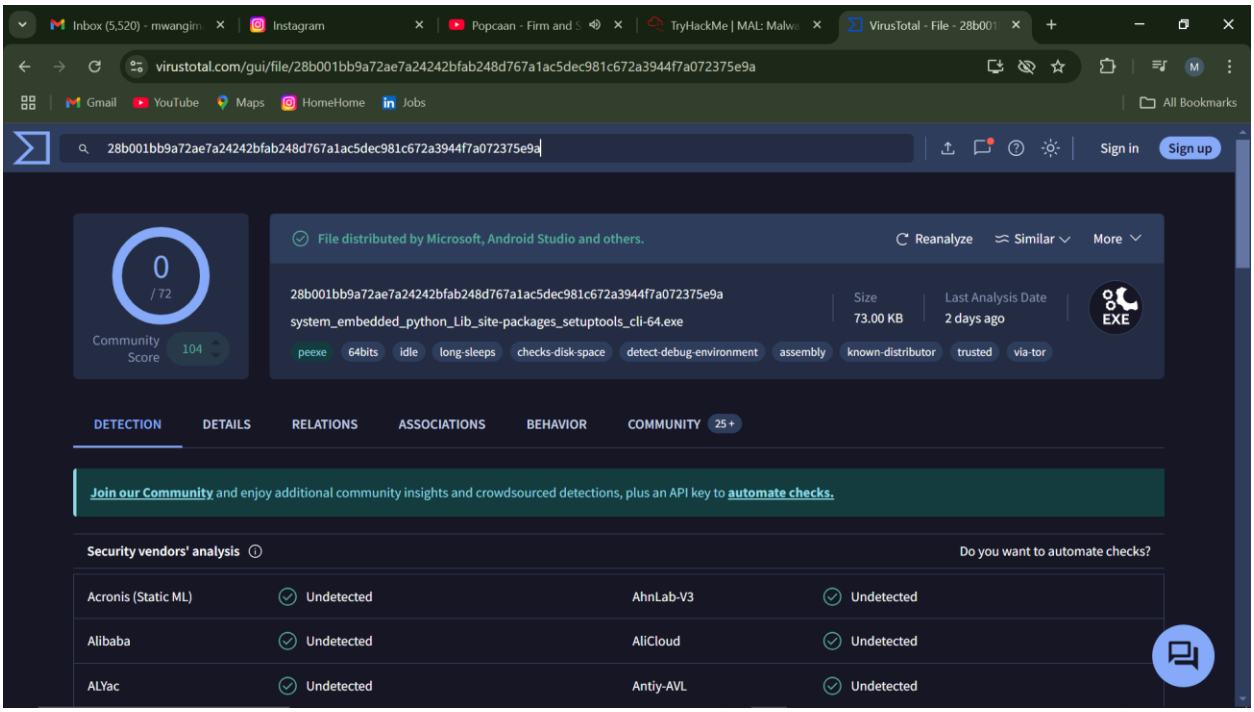


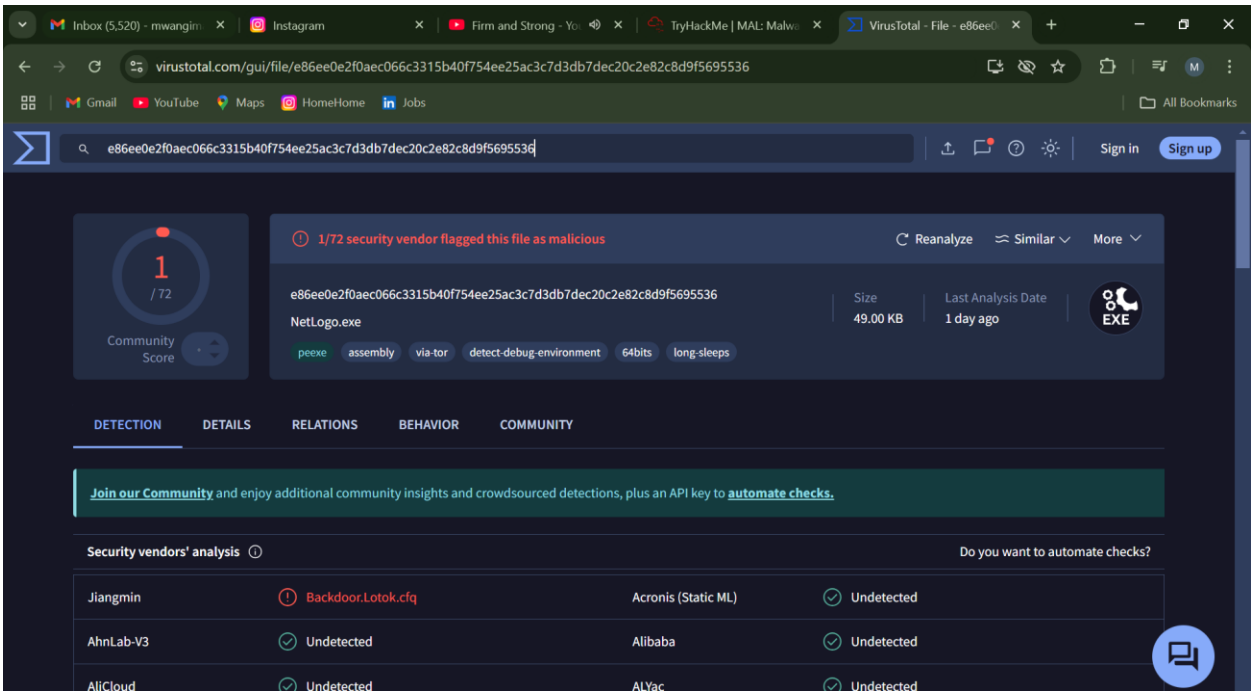
1.5 Now lets see if the MD5 Checksums have been analysed before

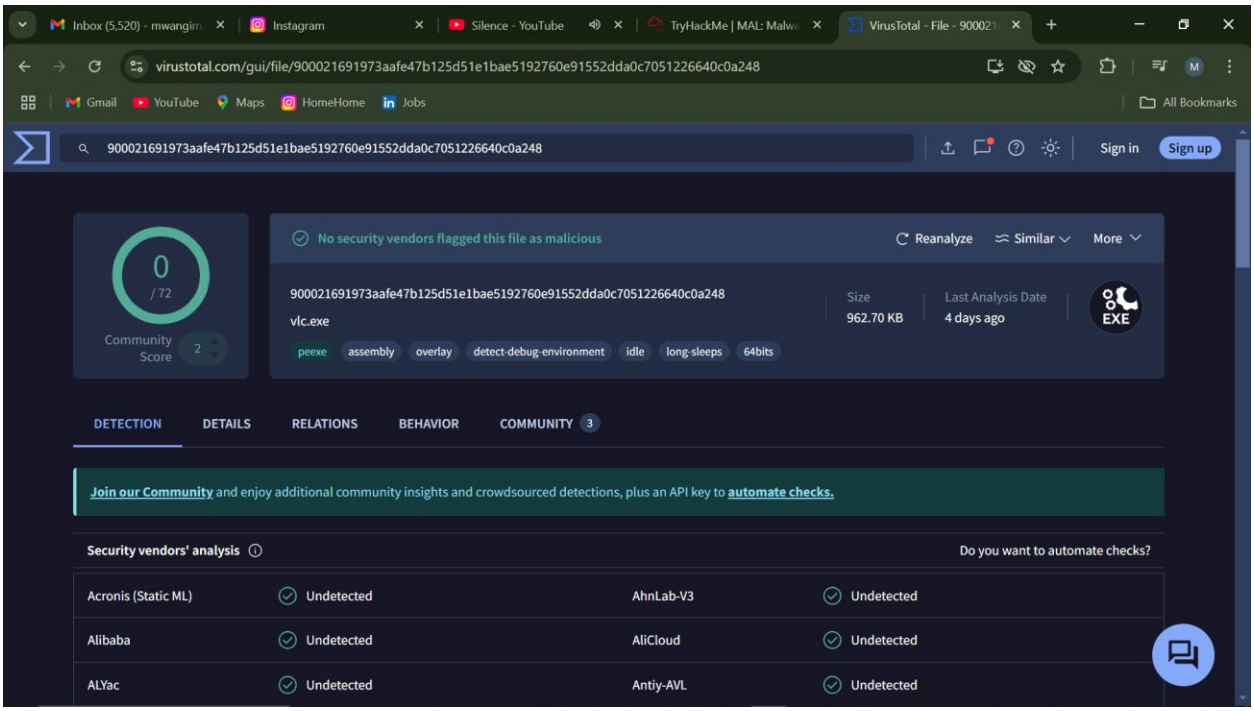
Questions



I checked the md5 hashes against the virustotal tool for reports on them being malicious, below are results as follows, aws.exe, netlogo.exe, vlc.exe



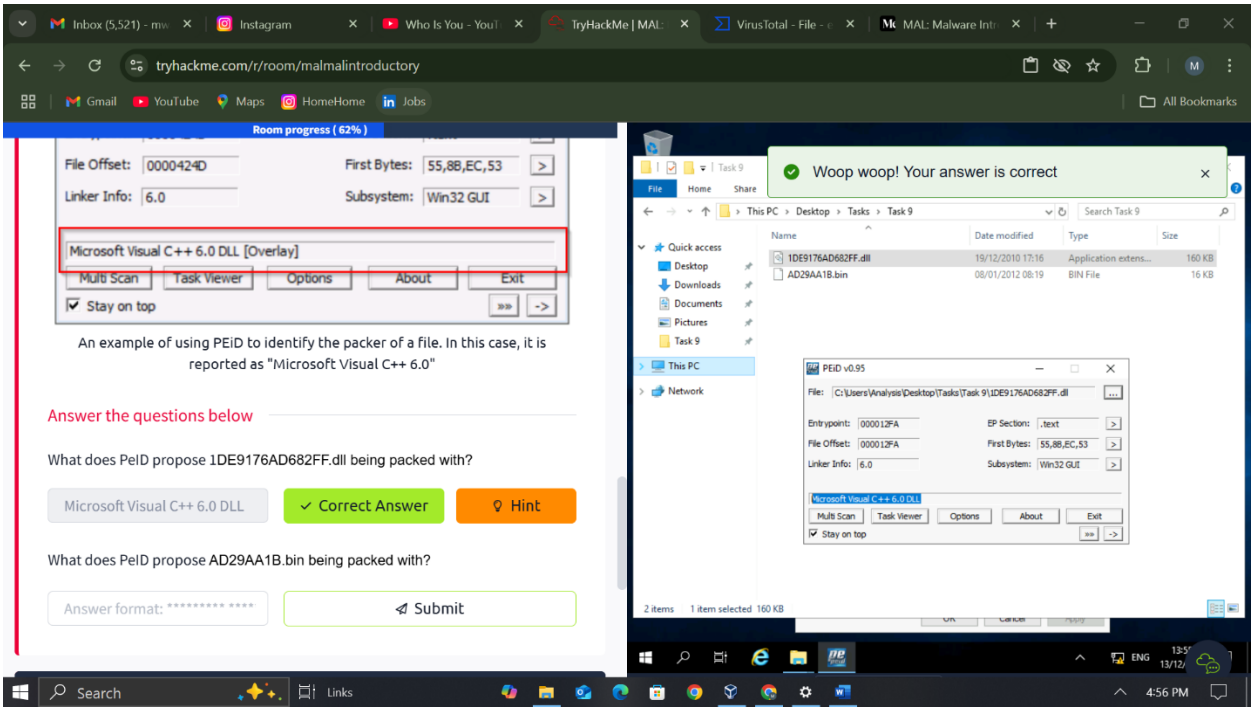


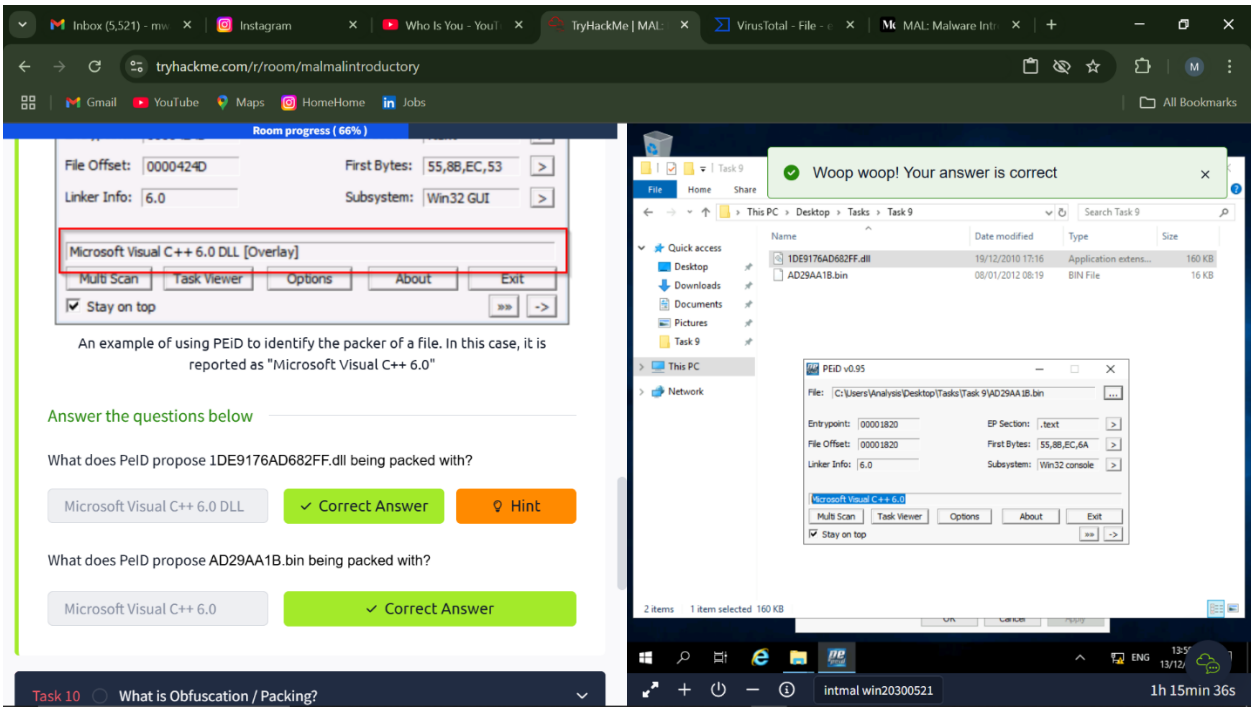


1.6 Identifying if the Executables are obfuscated / packed

Questions

I launched the PEid tool located in the Documents folder, to find the packer of two files located in the task 9 folder, and this was the results

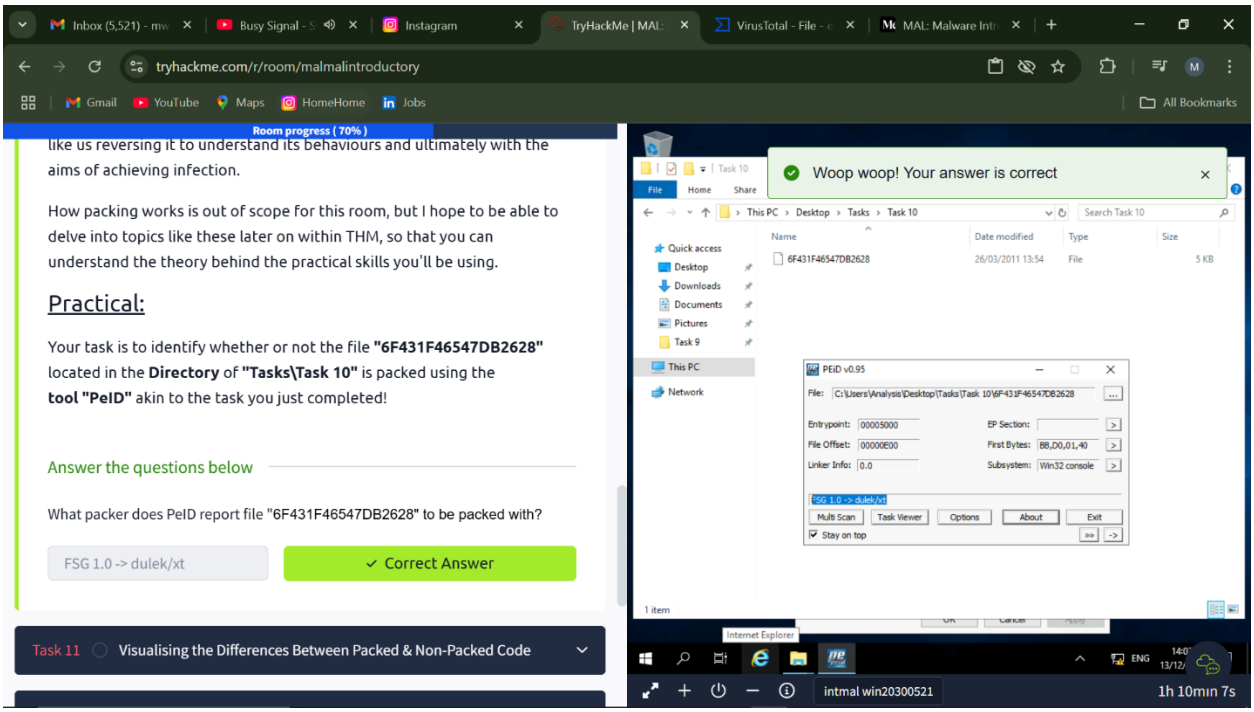




1.7 What is Obfuscation / Packing?

Questions

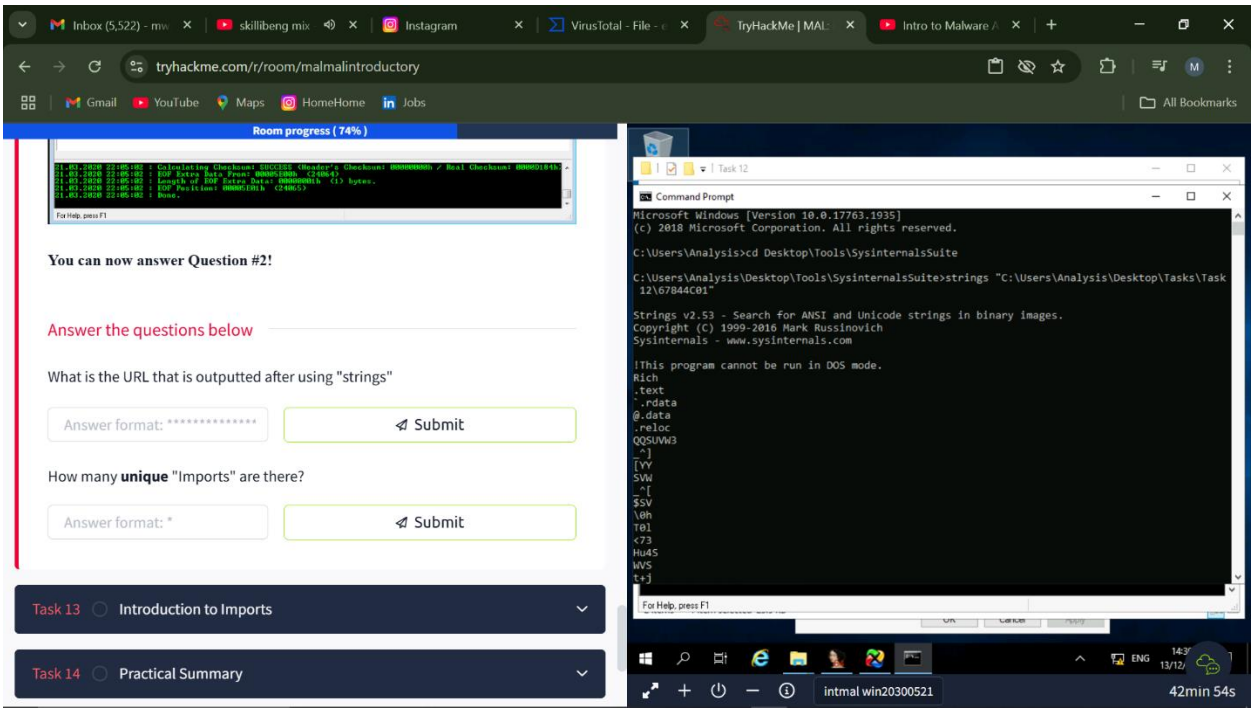
Used the PEid tool to check the file in task 10 what its packed with this was the results.



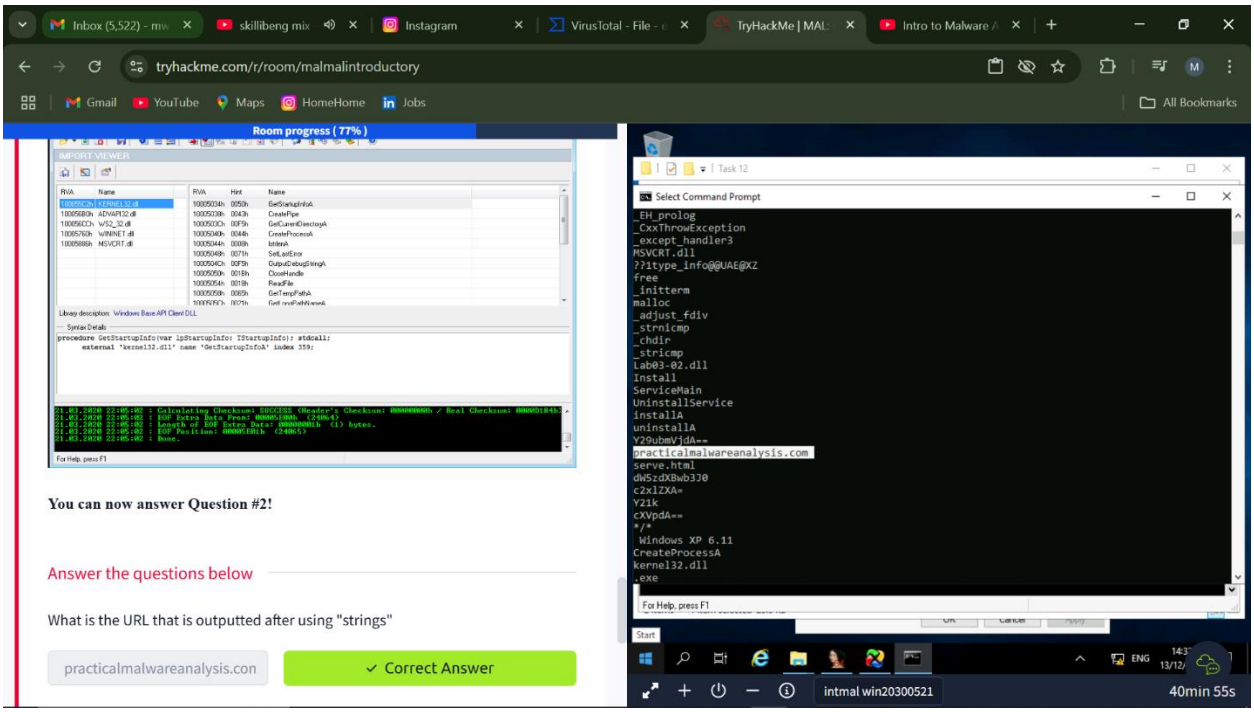
1.8 Introduction to Strings

Questions

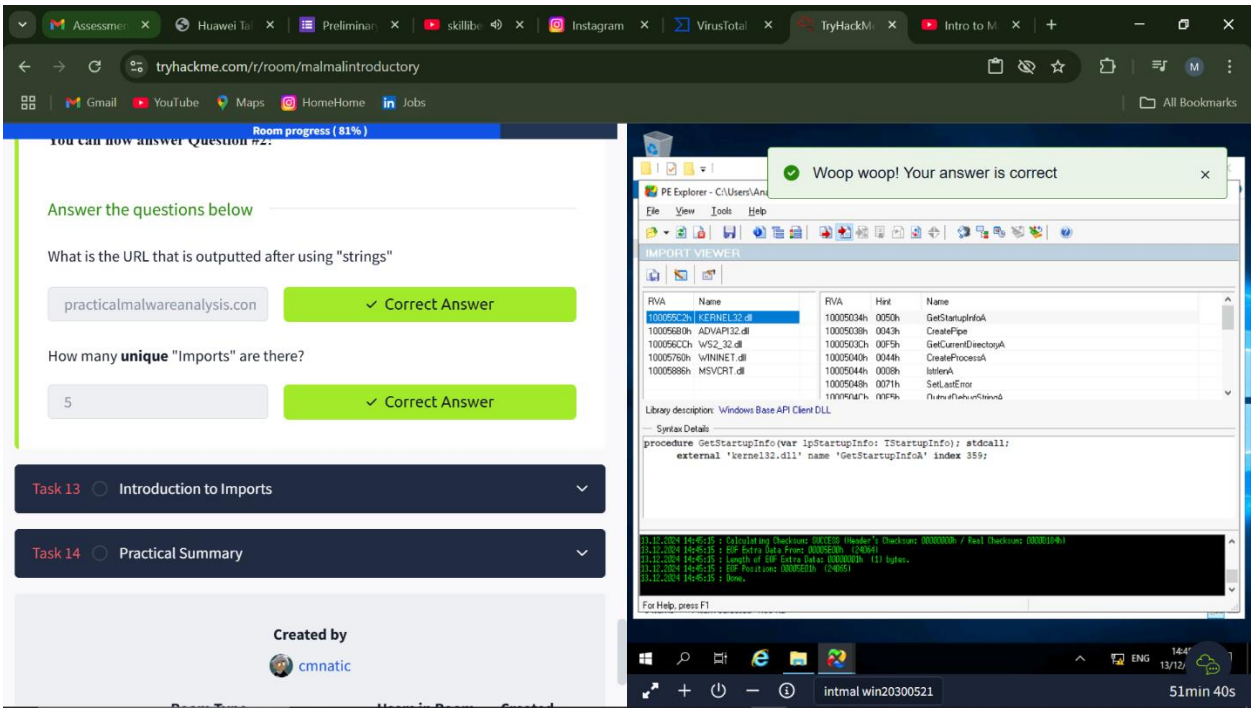
I started of by opening the cmd and navigating to the sysinternalsSuite foder and used string program to output the strings in the file in task 12 folder.



After running the command I found quite a number of strings outputted and among them was a URL.



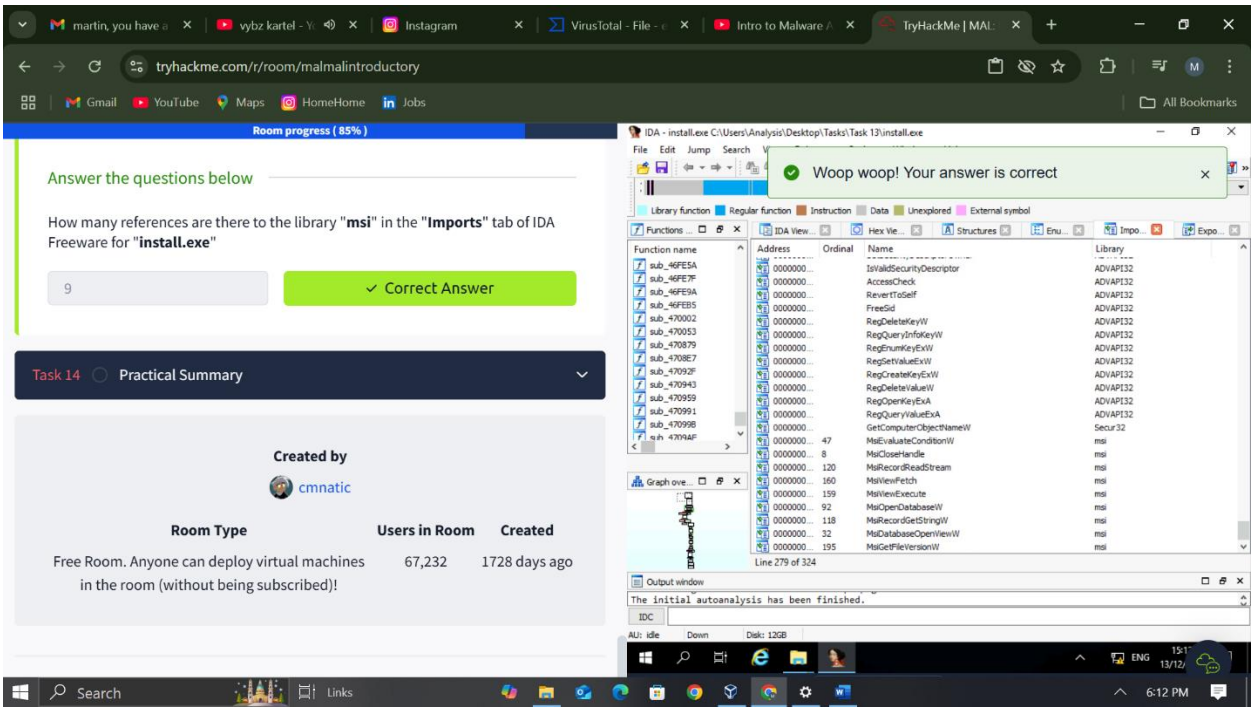
I opened the file in task 12 folder with PE explorer where I viewed the imports and found there were 5 imports done.



1.9 Introduction to Imports

Questions

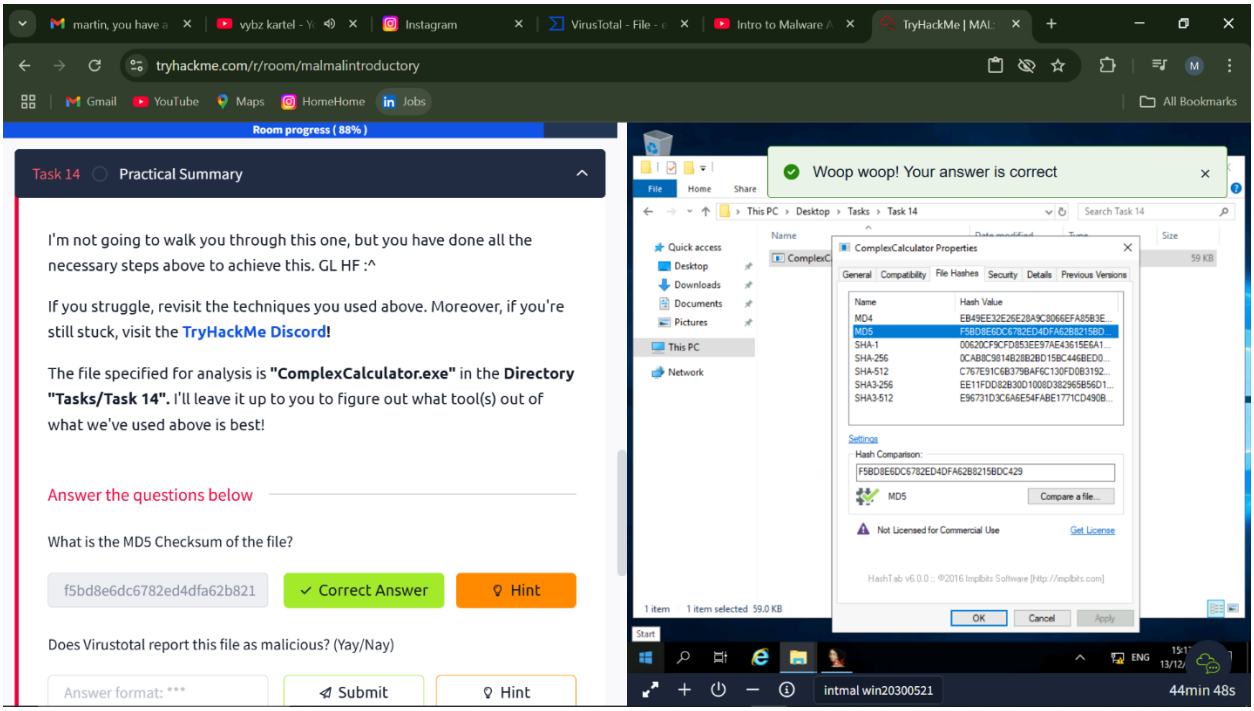
With use of IDA tool I opened install.exe file in task 13 folder, after opening I investigated the imports of msi and found to be 9.



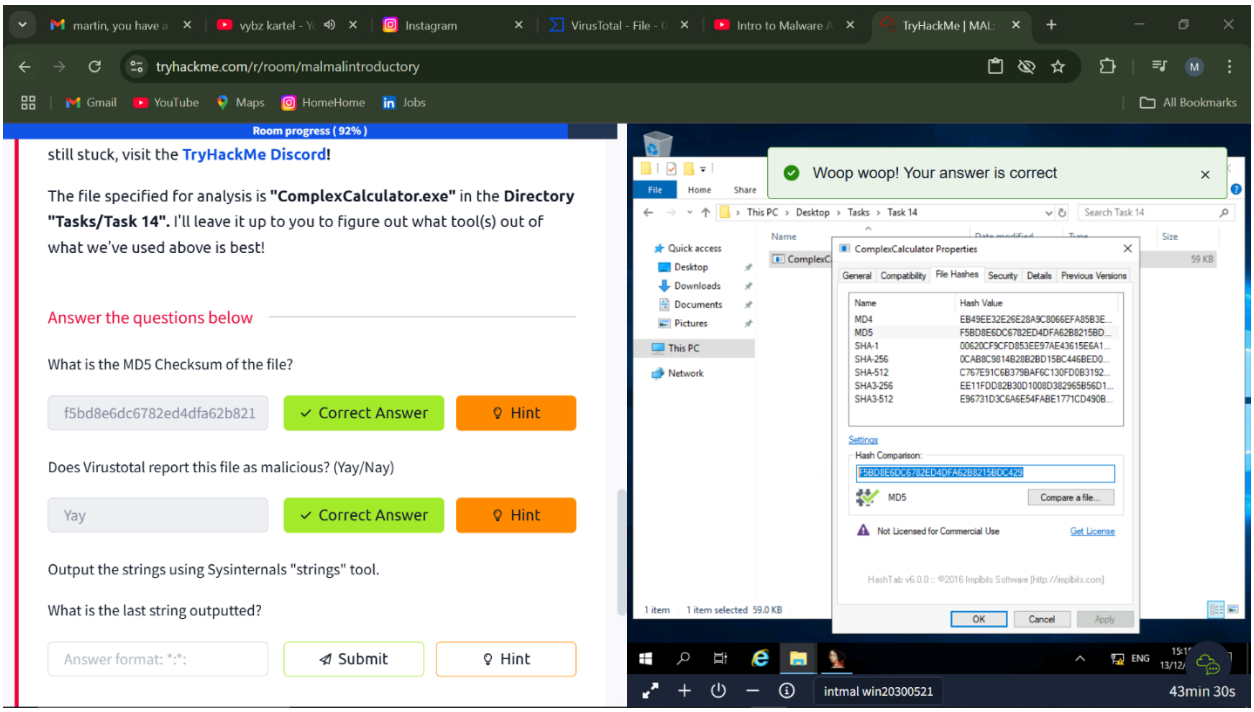
1.10 Practical Summary

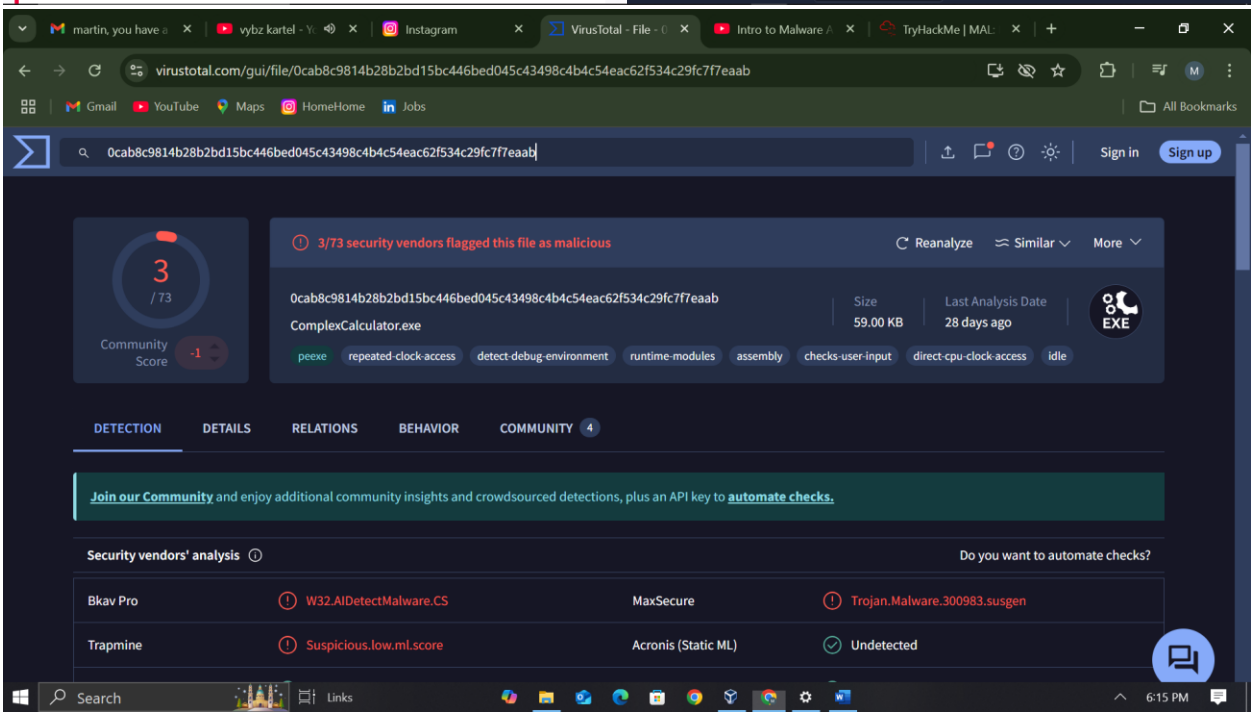
Questions

I investigated the properties of the complexcalculator file by looking at its hashes where I found the md5 hash

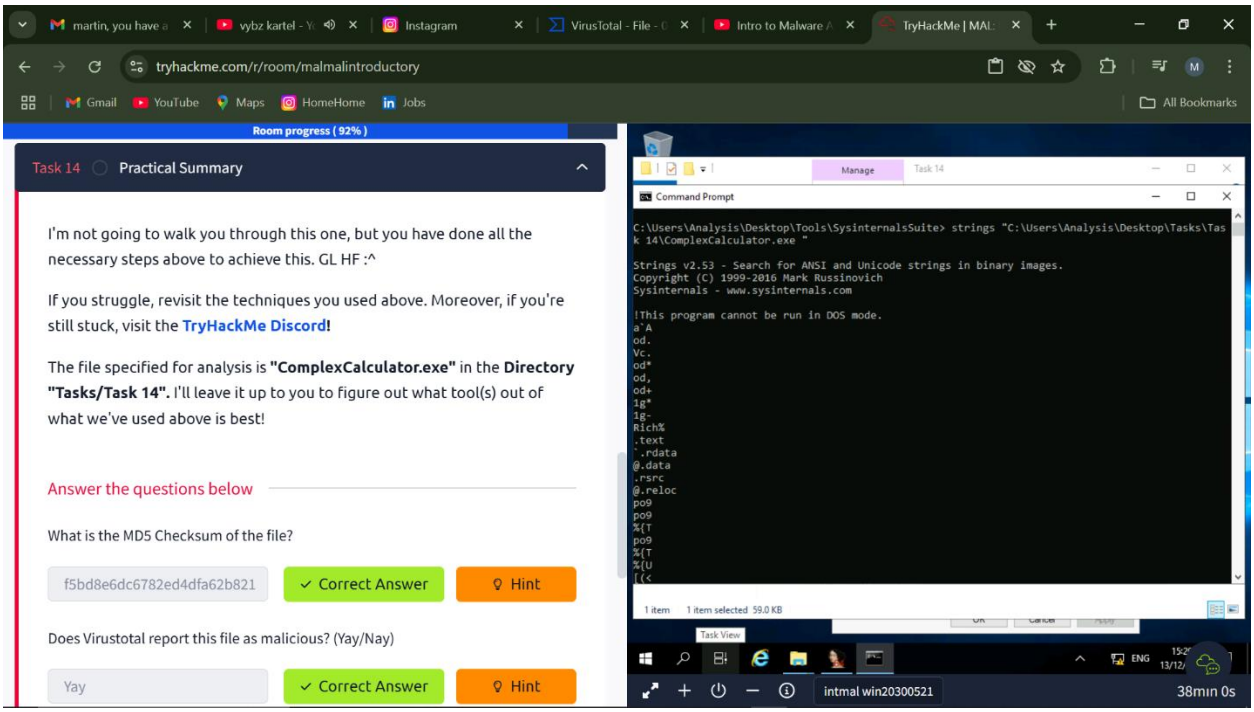


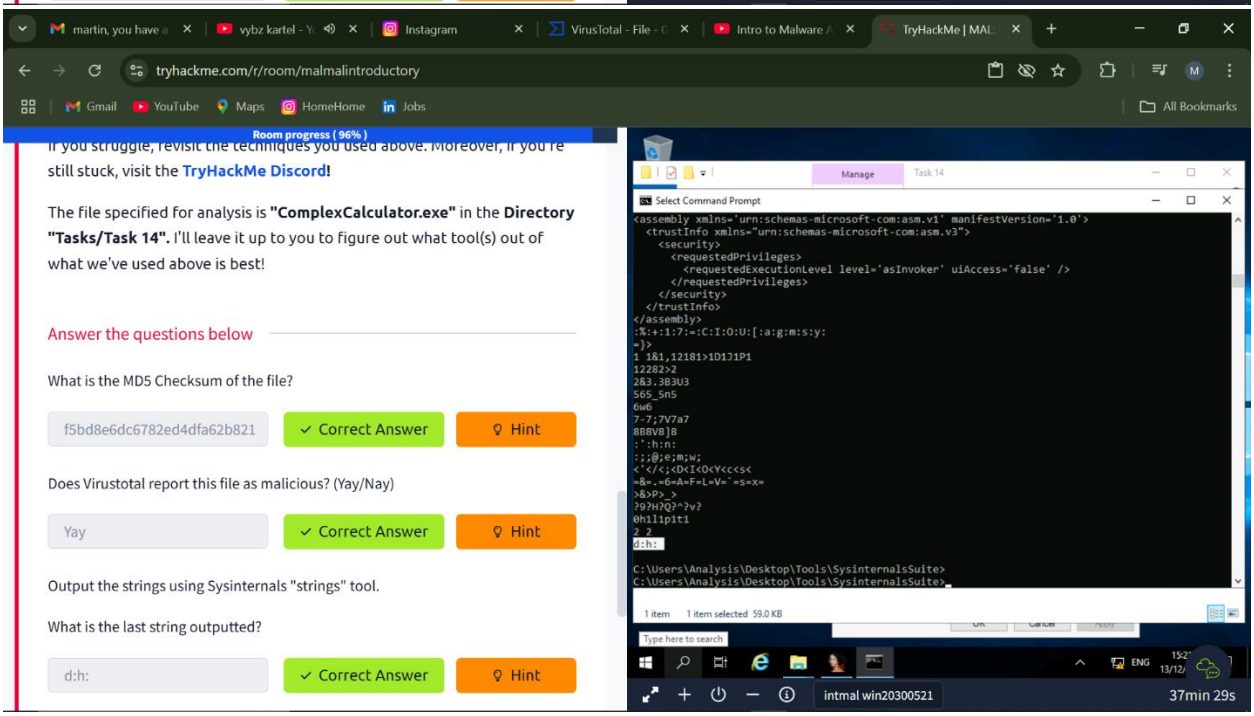
Looking at the md5 hash I found against the virustotal tool I found it to be reported to be malicious, the results are below.



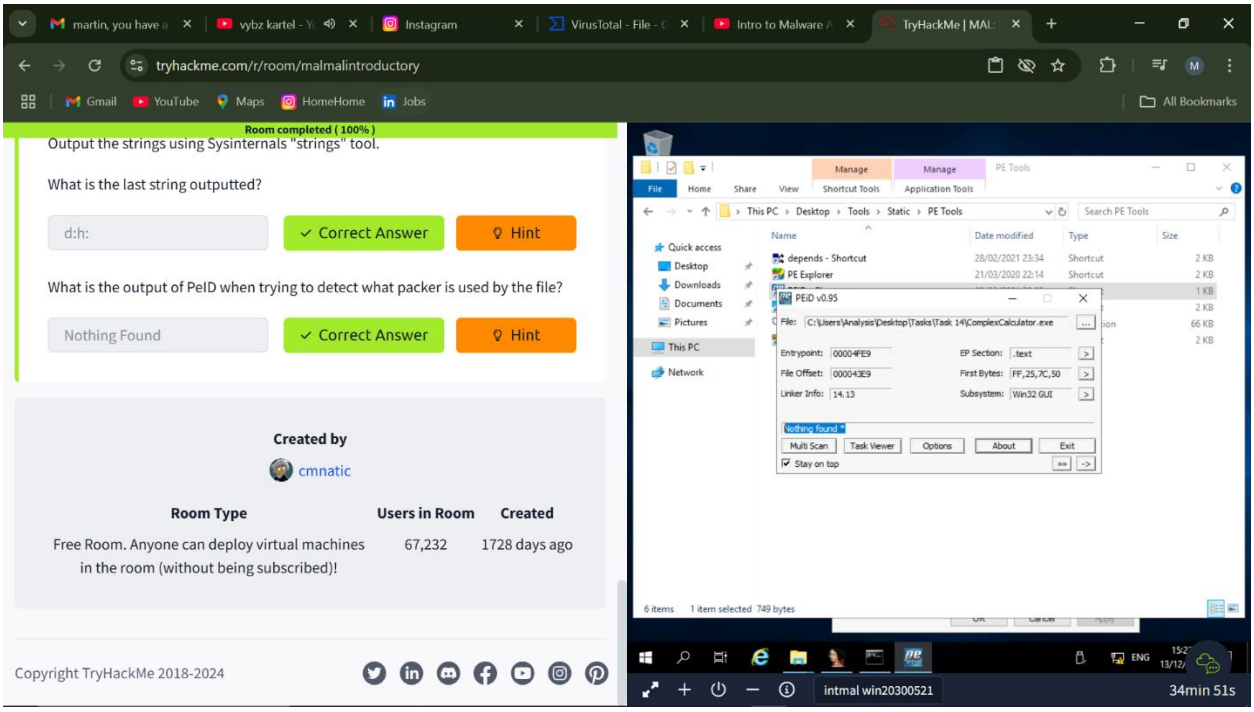


I started off by opening the cmd and navigating to sysinternalssuite folder to use the string program so as to find output of strings in the complexcalculator file. Plus found the last string as the answer.





Used PEiD to find the packer of the complexcalculator file and found it to be nothing.



2.0 Conclusion

This room has been helpful on how to conduct malware analysis and also to review or assess an application or file that looks suspicious, by looking at its MD5 hash and checking it against the virustotal tool.