**MAL: Malware Introductory**

**Introduction**

In this section of the study the learner dives into understanding the purpose of malware analysis.

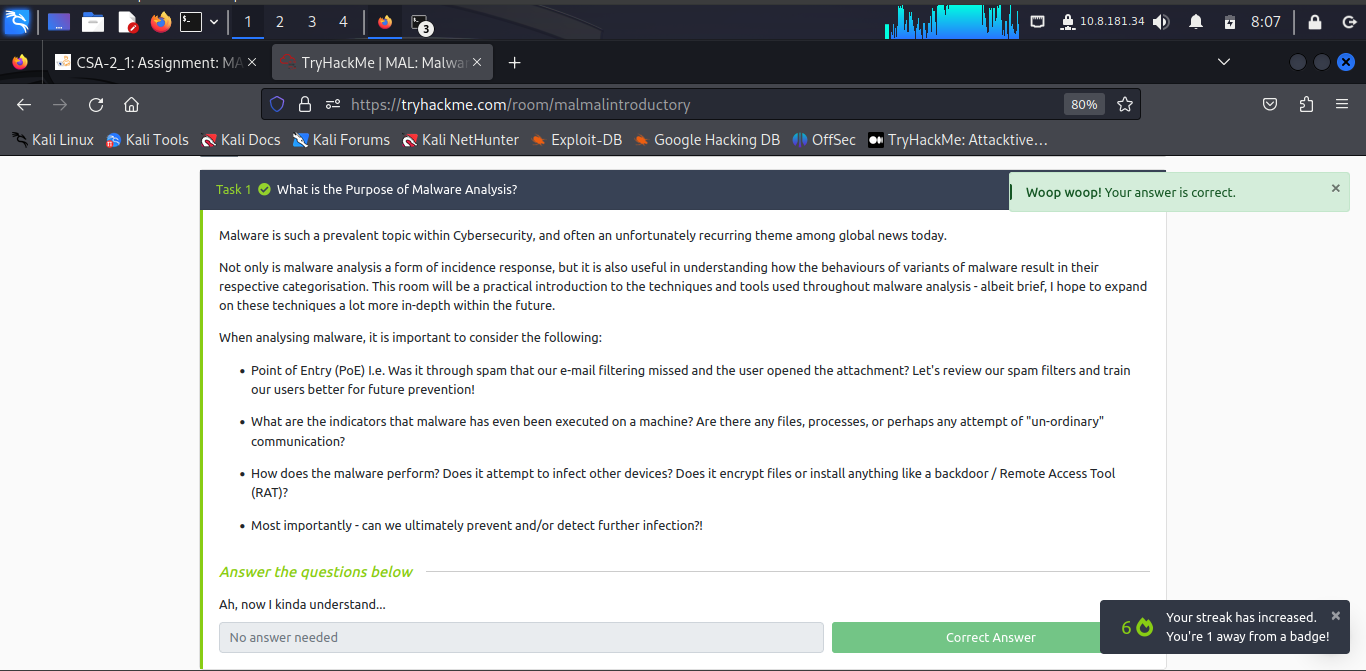
***Activities***

***Task 1: What is the Purpose of Malware Analysis?***

Malware analysis a form of incidence response useful in understanding how the behaviours of variants of malware result in their respective categorisation.

It is important to consider the following:

* Point of Entry (PoE) I.e. Was it through spam that our e-mail filtering missed and the user opened the attachment? Let's review our spam filters and train our users better for future prevention!
* What are the indicators that malware has even been executed on a machine? Are there any files, processes, or perhaps any attempt of "un-ordinary" communication?
* How does the malware perform? Does it attempt to infect other devices? Does it encrypt files or install anything like a backdoor / Remote Access Tool (RAT)?
* Most importantly - can we ultimately prevent and/or detect further infection?!



***Task 2: Understanding Malware Campaigns***

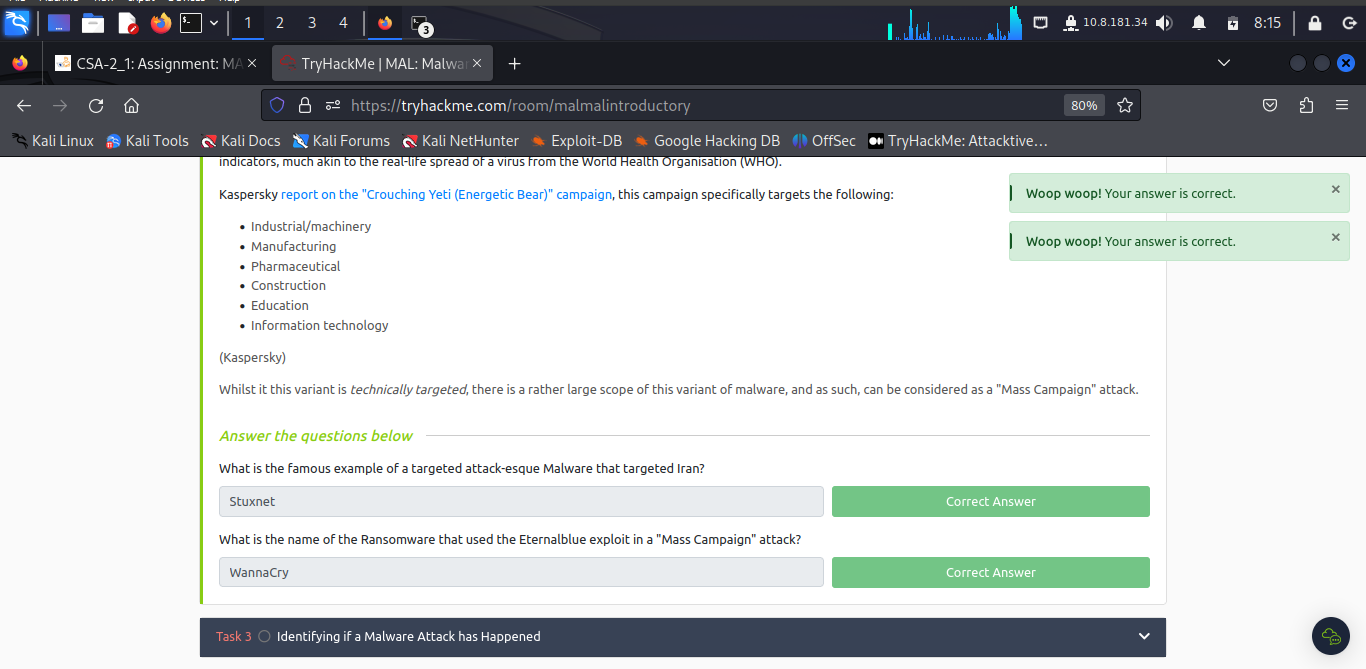
Attacks can generally be classified into two types: **Targeted** and **Mass Campaign**.

**Targeted**

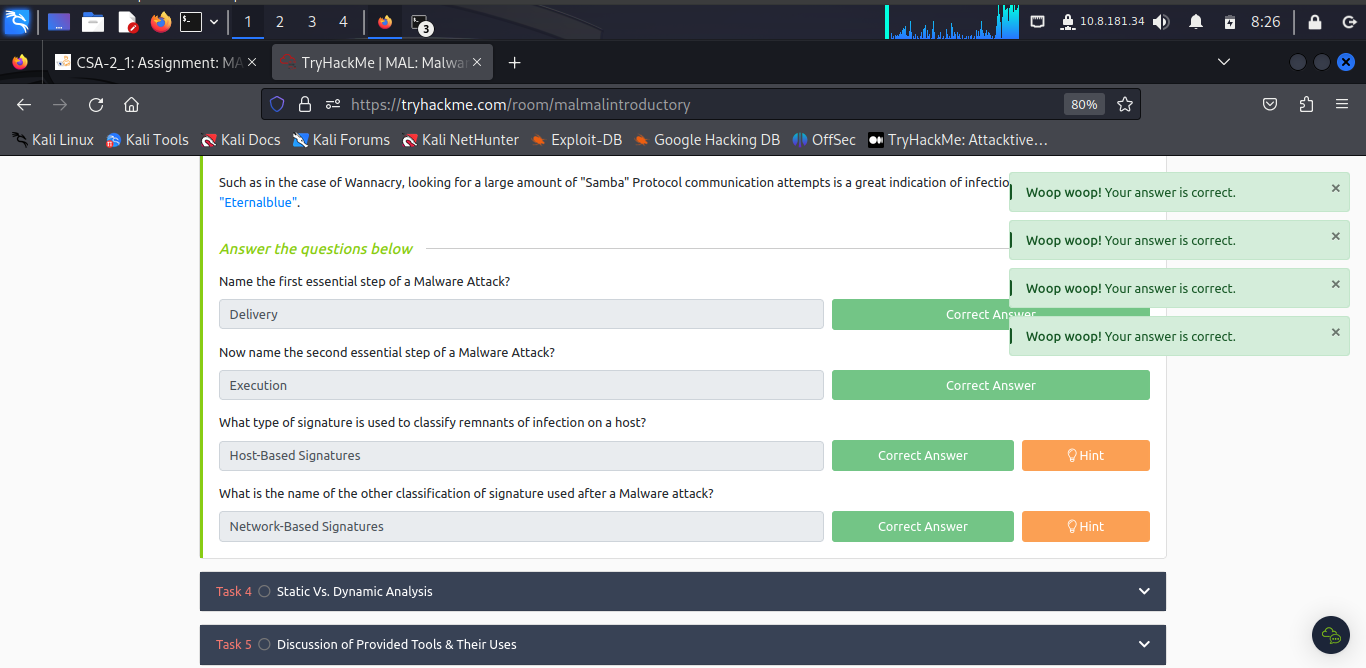
Malware attacks that occur created for a specific purpose against a specific target. A great example of this type of purpose could be the [DarkHotel](https://www.kaspersky.co.uk/resource-center/threats/darkhotel-malware-virus-threat-definition) malware, whom is designed to steal information such as authentication details from government officials.

**Mass Campaign**

The most common type of attacks. The entire purpose of this type of Malware is to infect as many devices as possible and perform whatever it may - regardless of target.



***Task 3: Identifying if a Malware Attack has Happened***



***Task 4: Static Vs. Dynamic Analysis***

Two categories used when analysing malware are **Static Analysis** and **Dynamic Analysis**

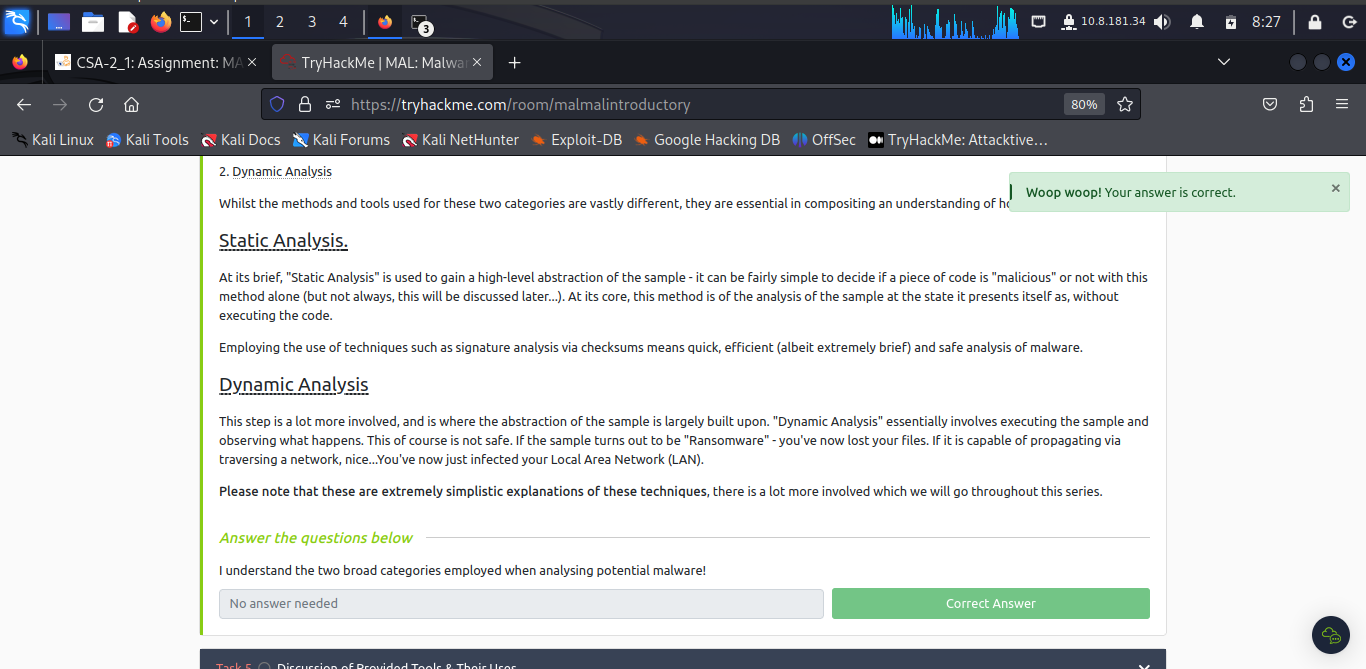
**Static Analysis**.

Used to gain a high-level abstraction of the sample - it can be fairly simple to decide if a piece of code is "malicious" or not with this method alone. At its core, this method is of the analysis of the sample at the state it presents itself as, without executing the code.

Employing the use of techniques such as signature analysis via checksums means quick, efficient and safe analysis of malware.

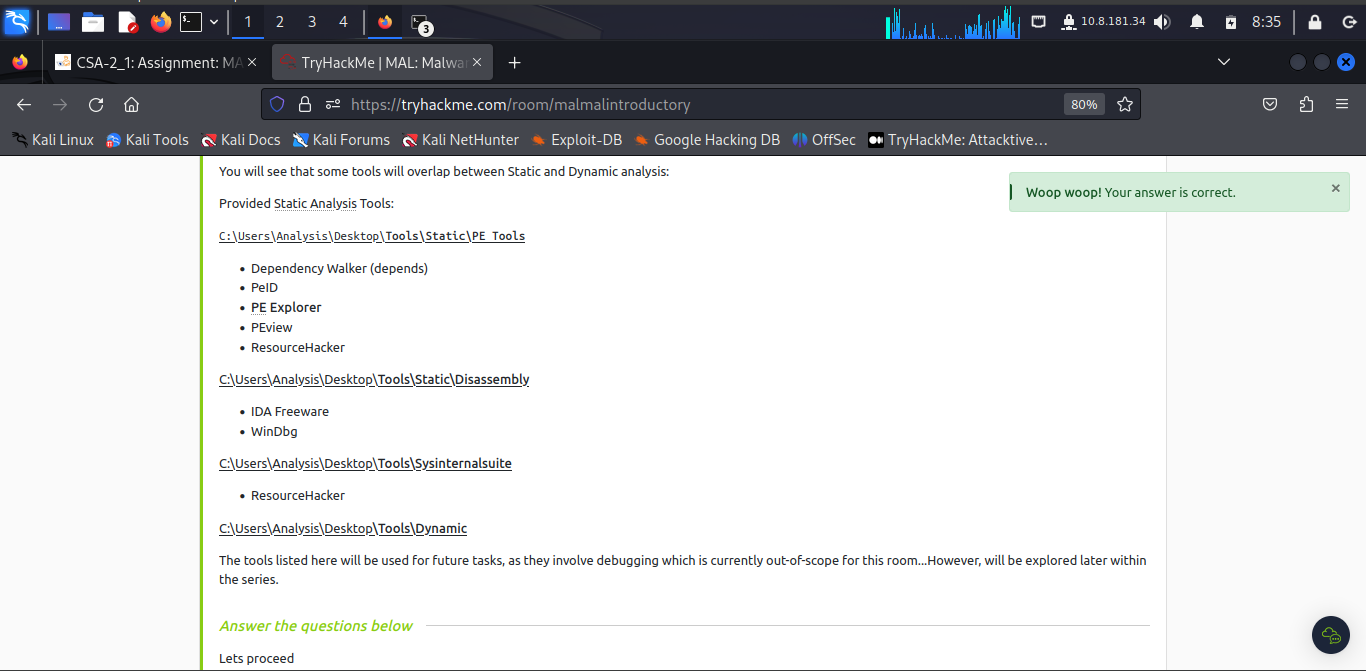
**Dynamic Analysis**

This is where the abstraction of the sample is largely built upon. ***Dynamic Analysis*** essentially involves executing the sample and observing what happens. This of course is not safe. If the sample turns out to be "Ransomware". If it is capable of propagating via traversing a network, now Local Area Network (LAN) is just infected.

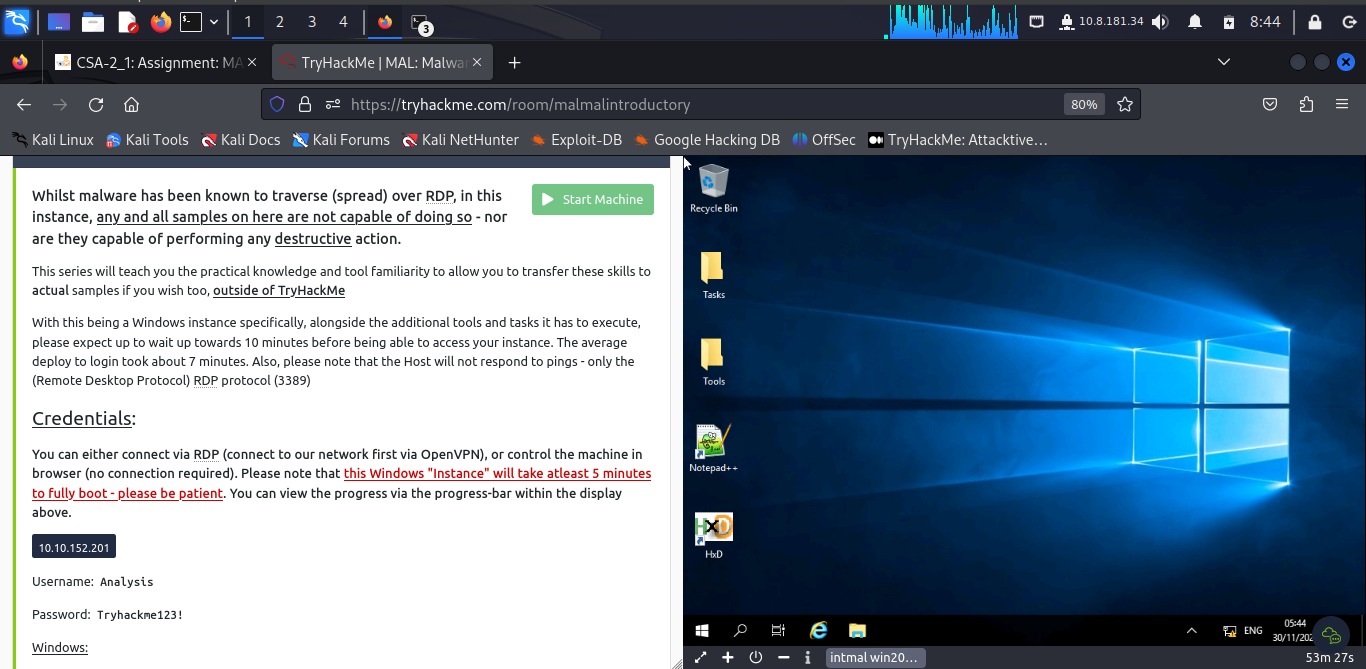


***Task 5: Discussion of Provided Tools & Their Uses***

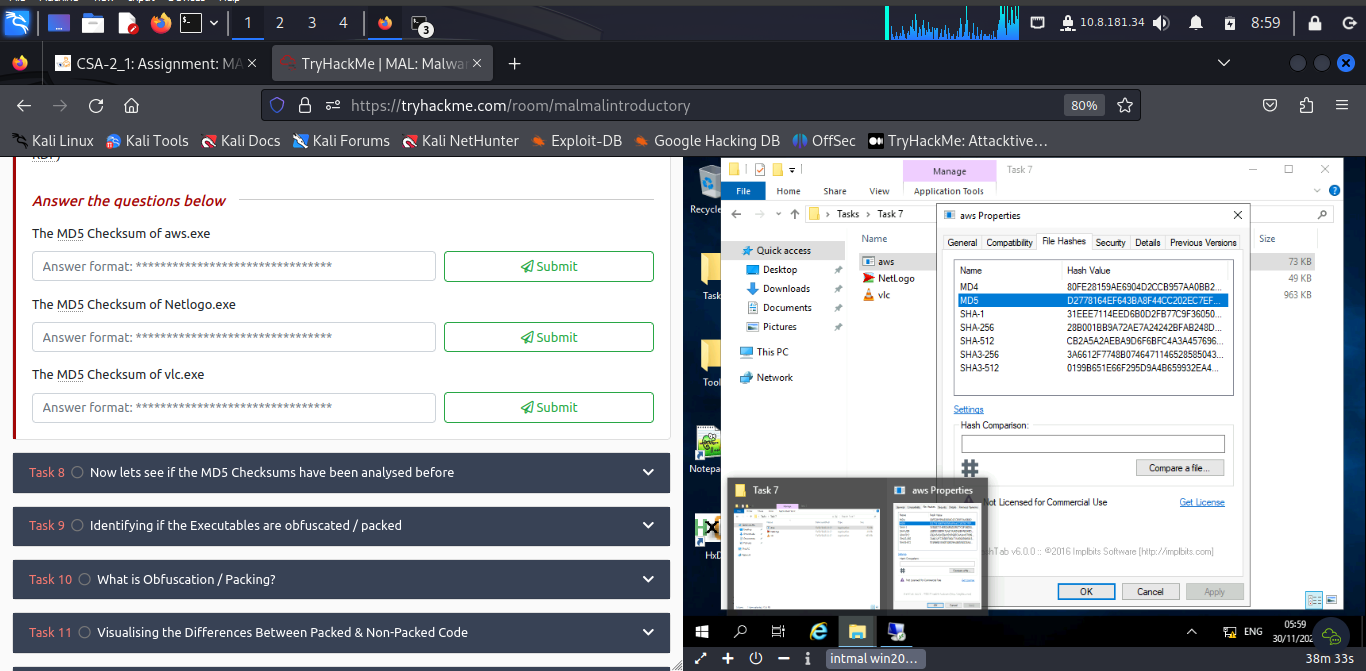
Tools overlapping between Static and Dynamic analysis:

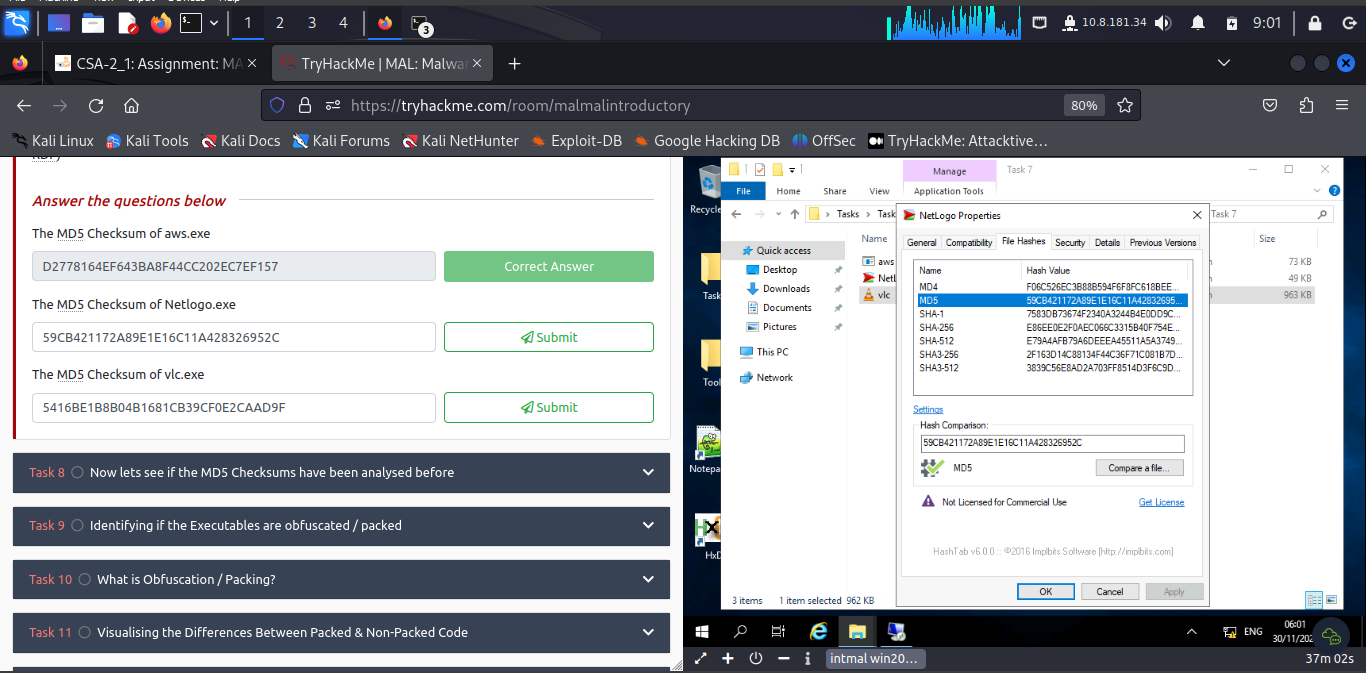


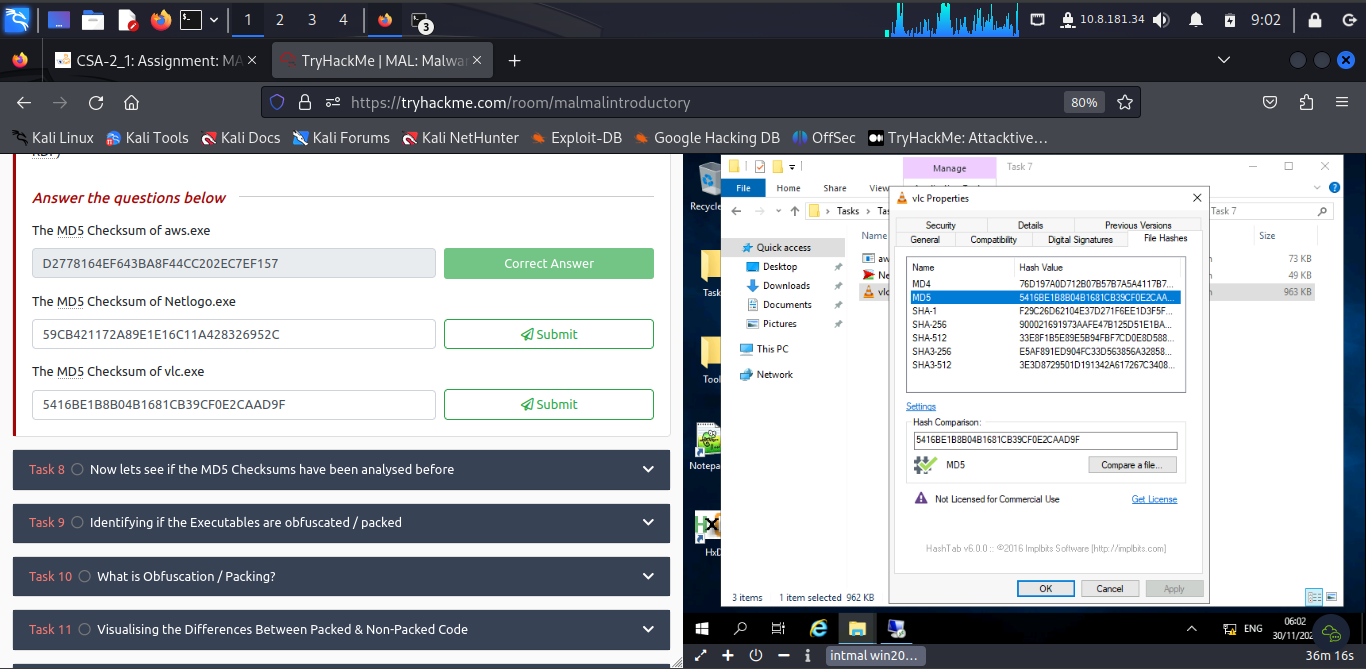
***Task 6: Connecting to the Windows Analysis Environment (Deploy)***

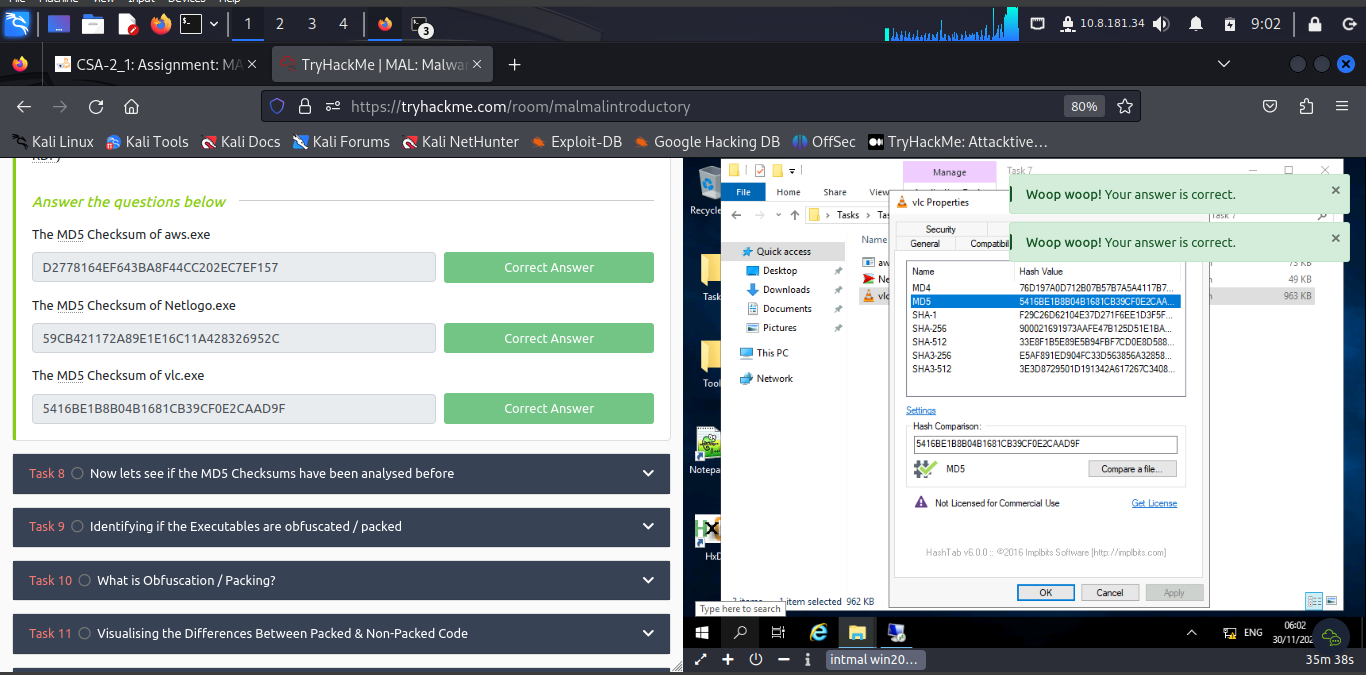


***Task 7: Obtaining MD5 Checksums of Provided Files***

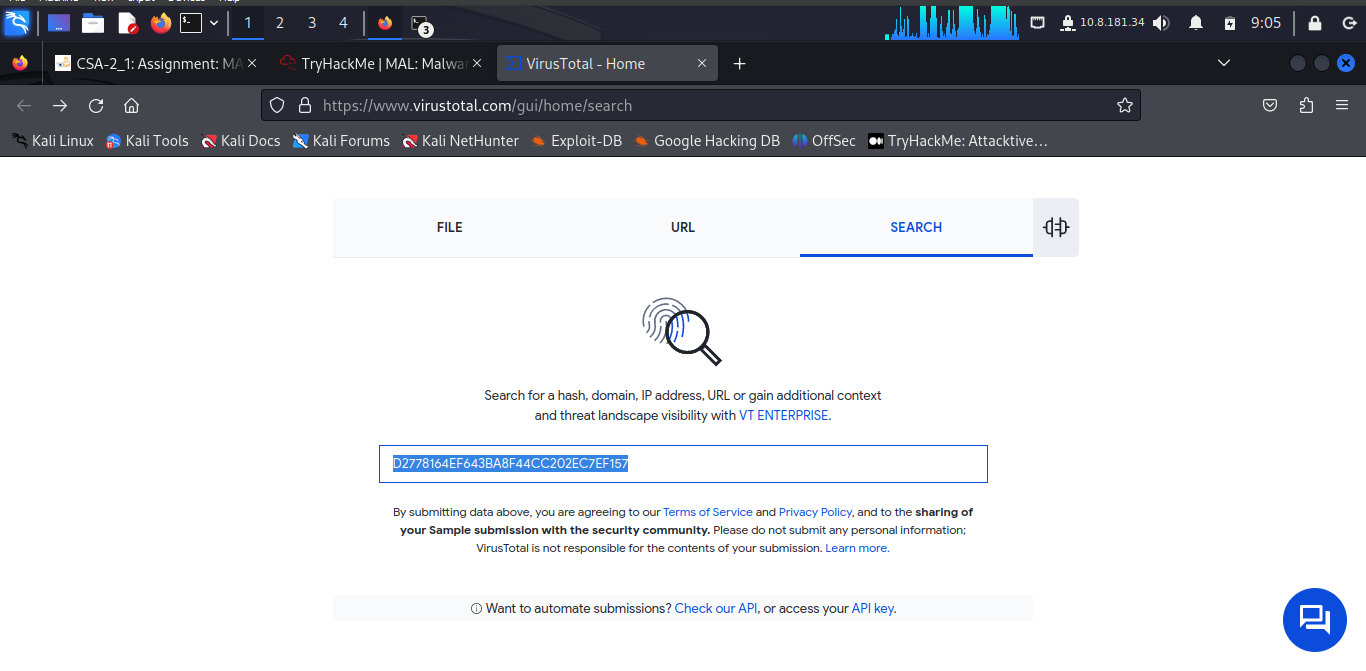


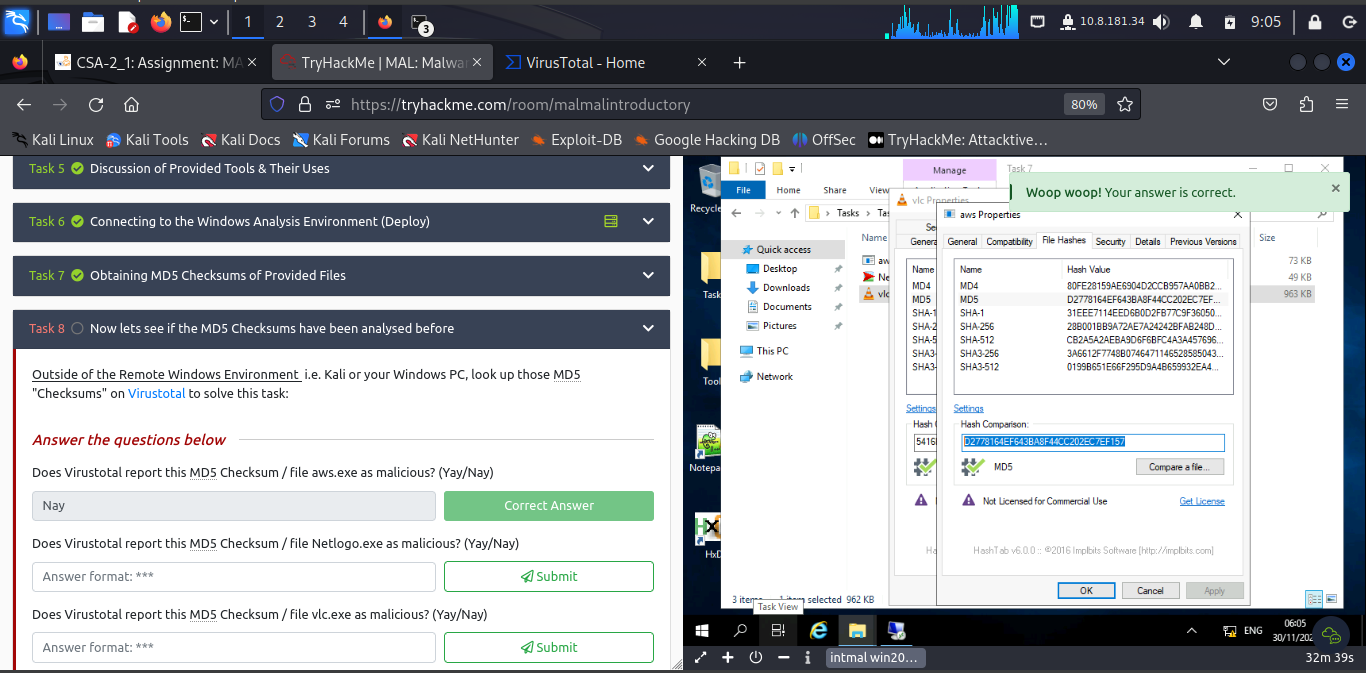




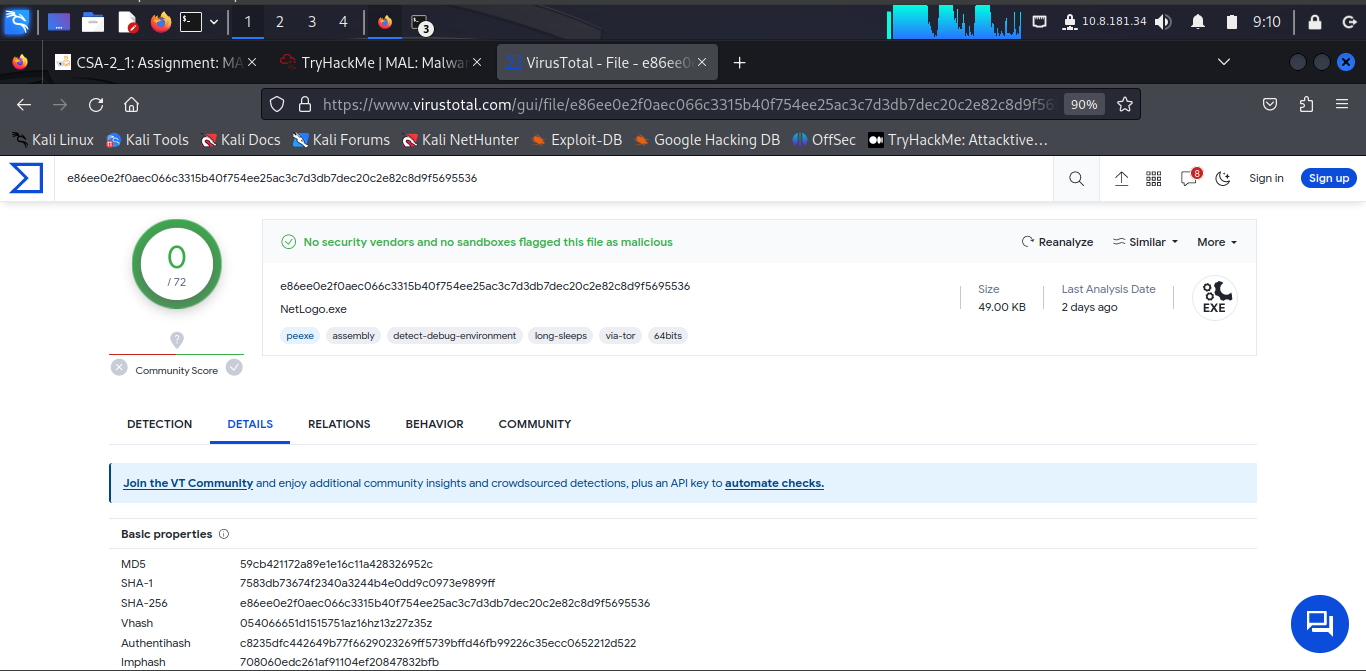


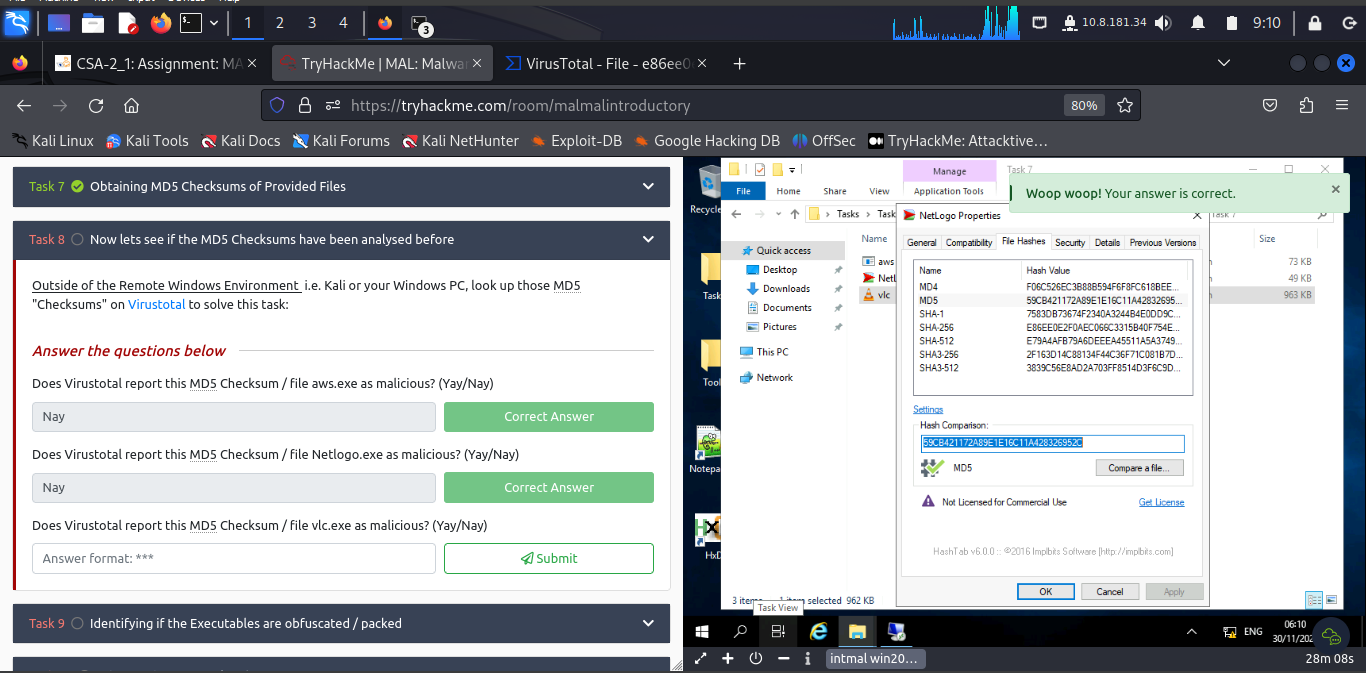
***Task 8: Now let’s see if the MD5 Checksums have been analysed before***

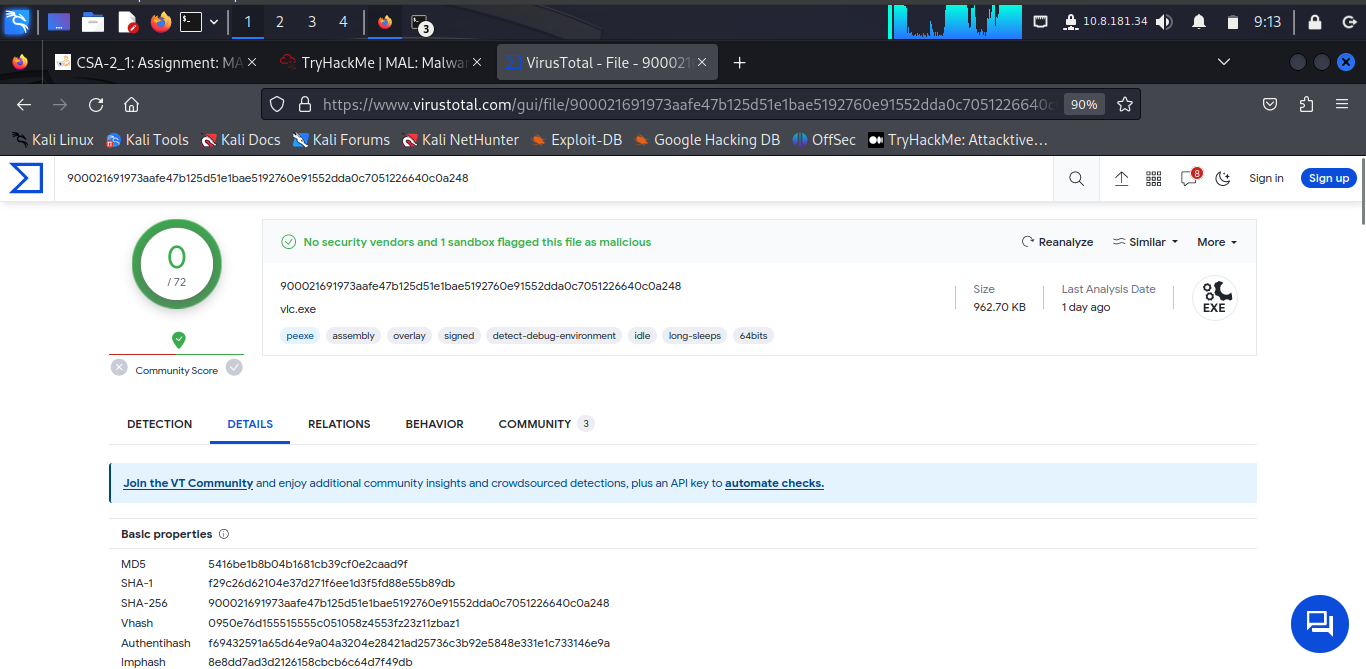


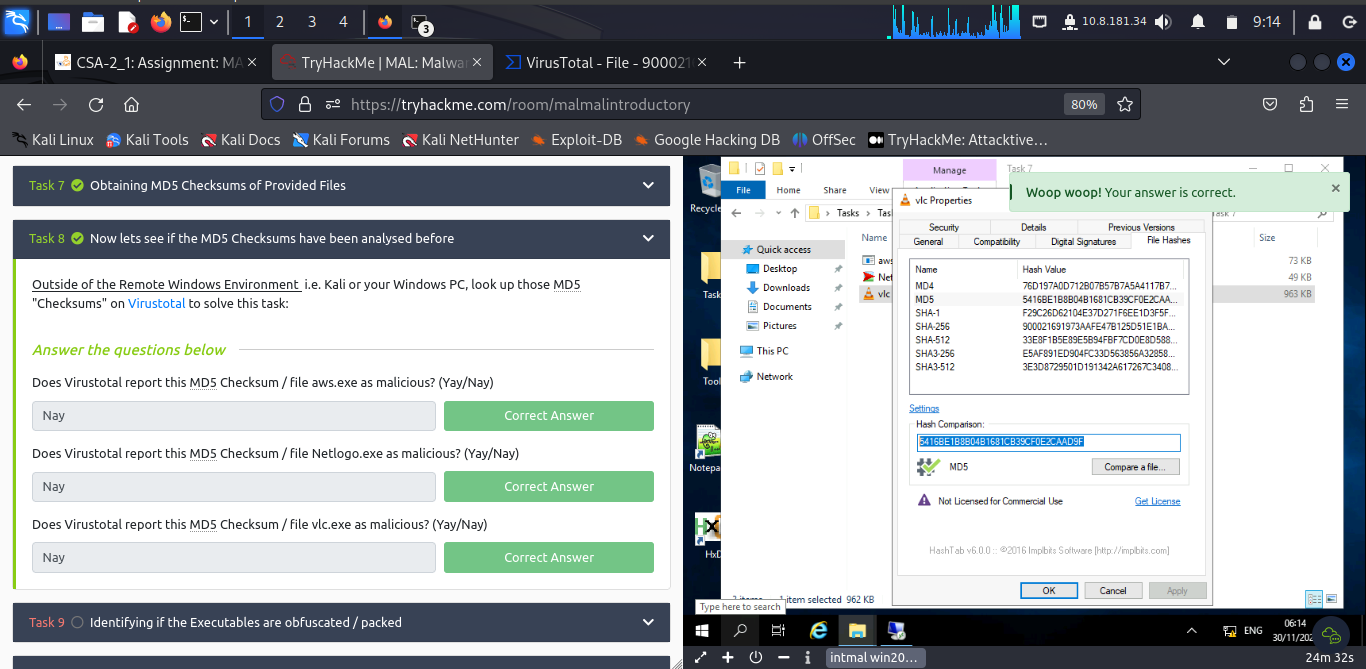






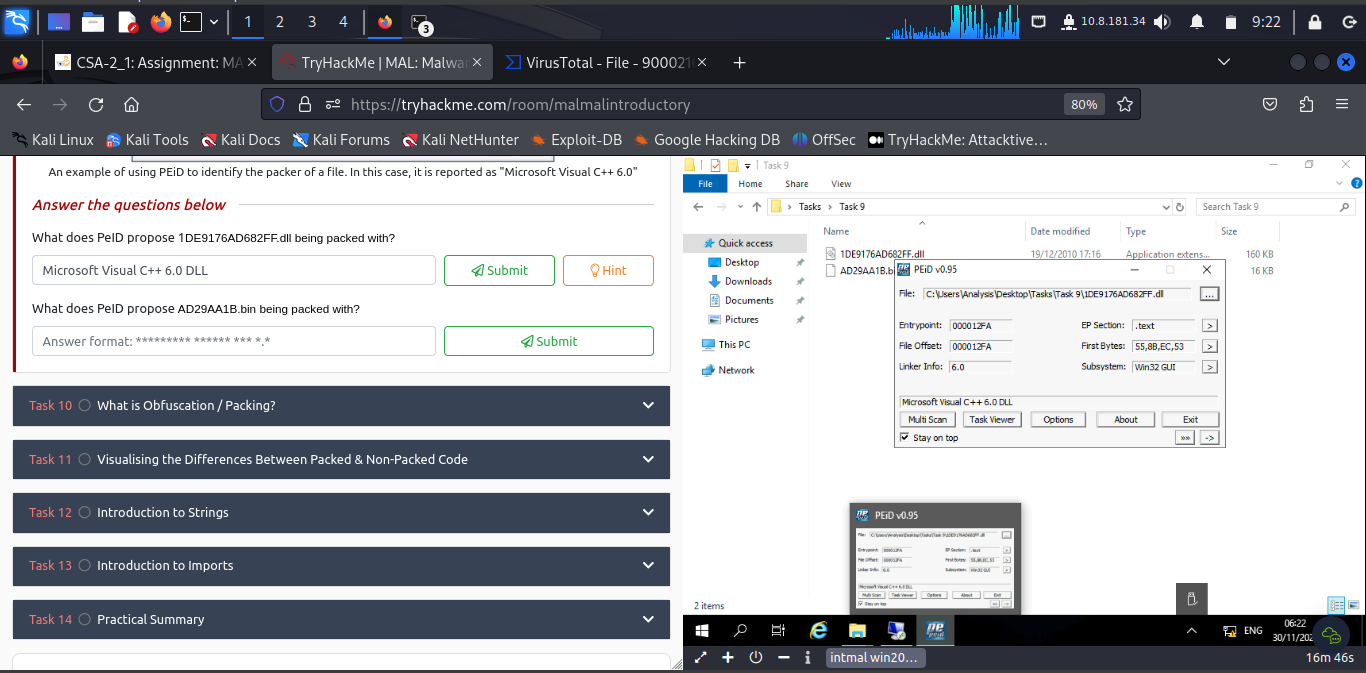


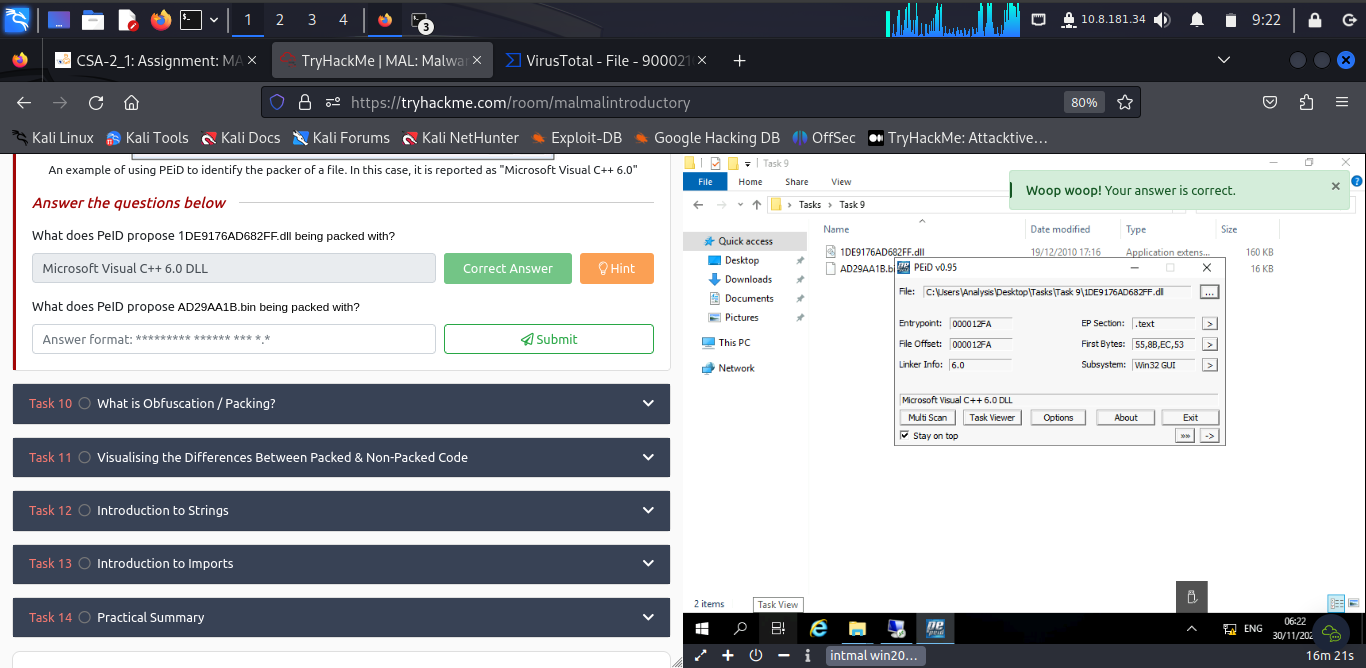


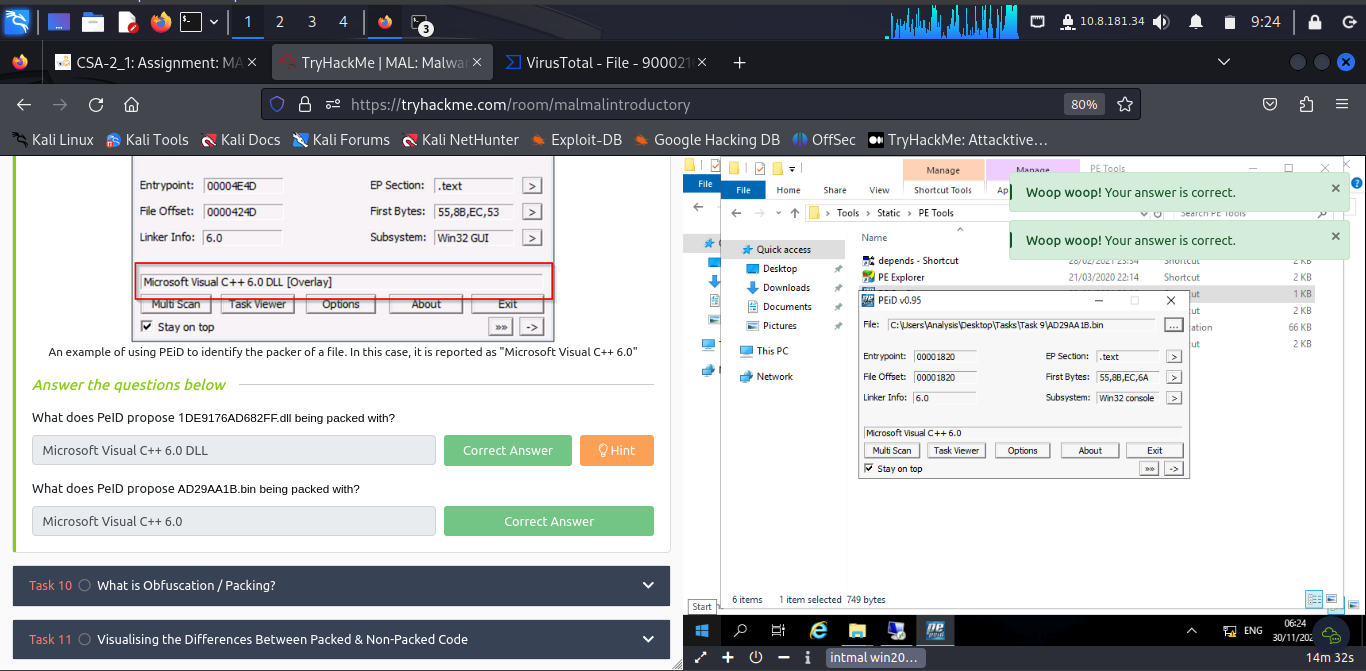


***Task 9: Identifying if the Executables are obfuscated/packed***

Because a file doesn't have the "**.exe**" extension, doesn't mean it isn't an actual executable! For instance, it can have the ".jpg" extension and still be an executable piece of code.

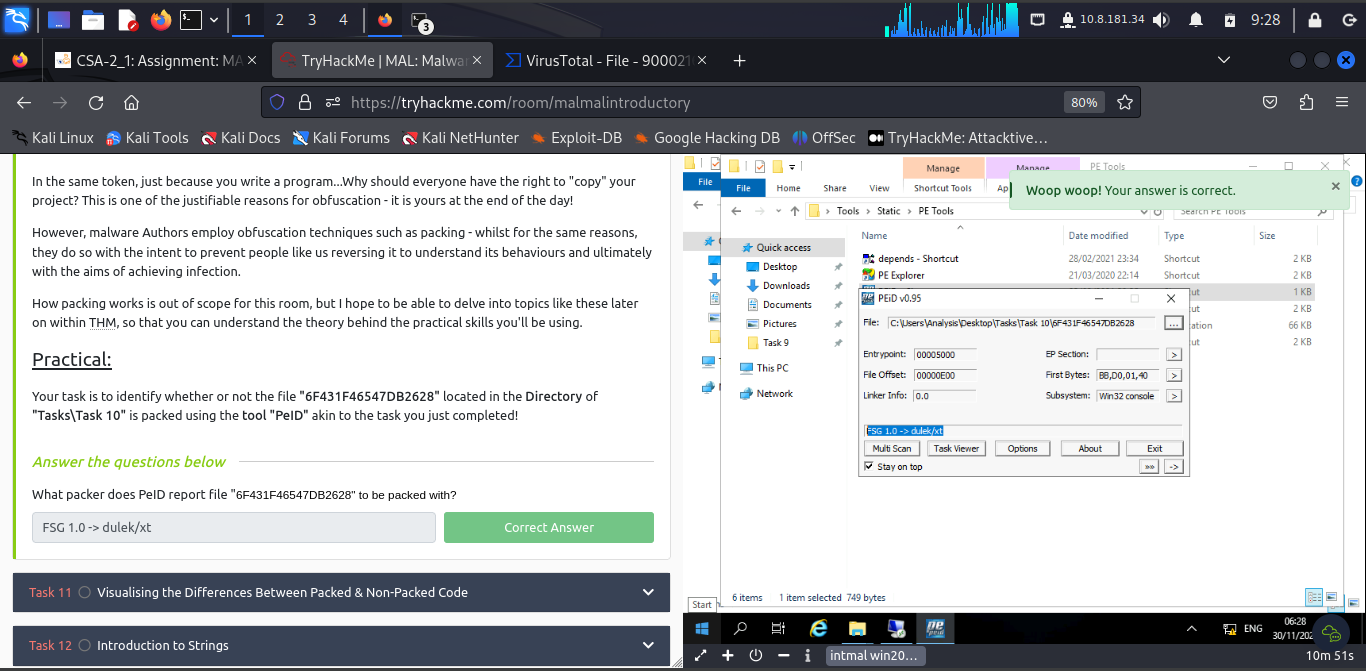


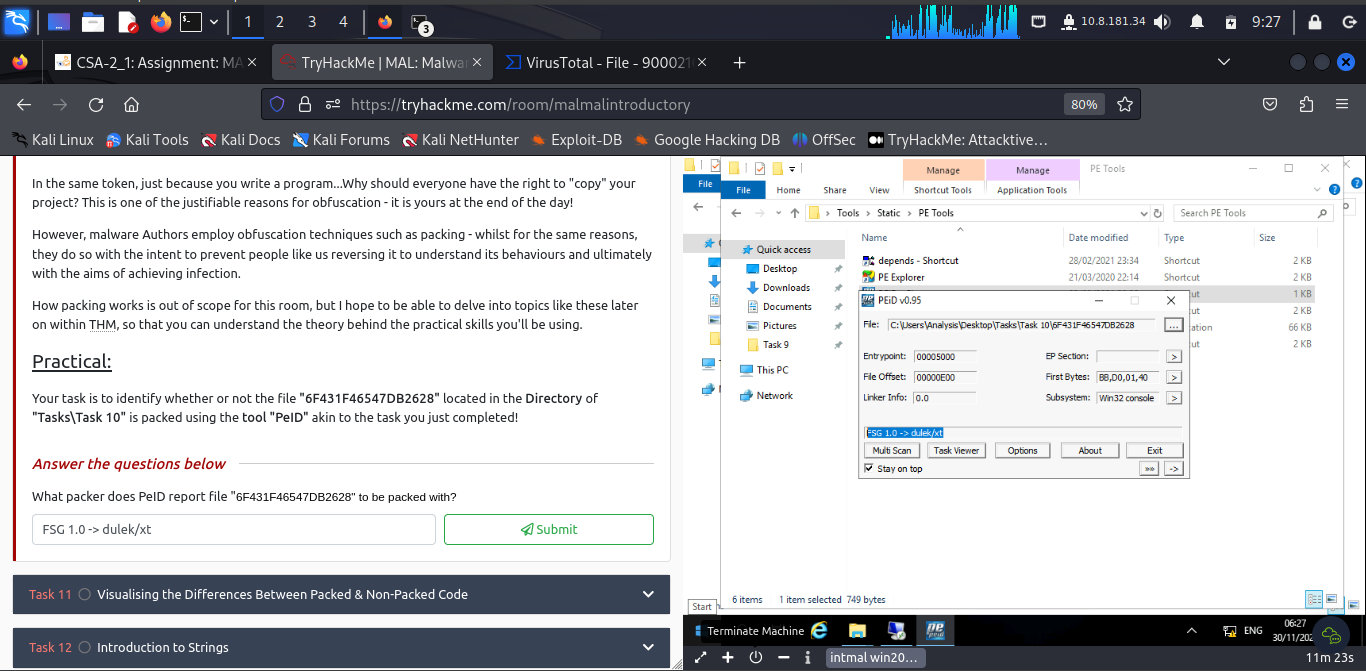




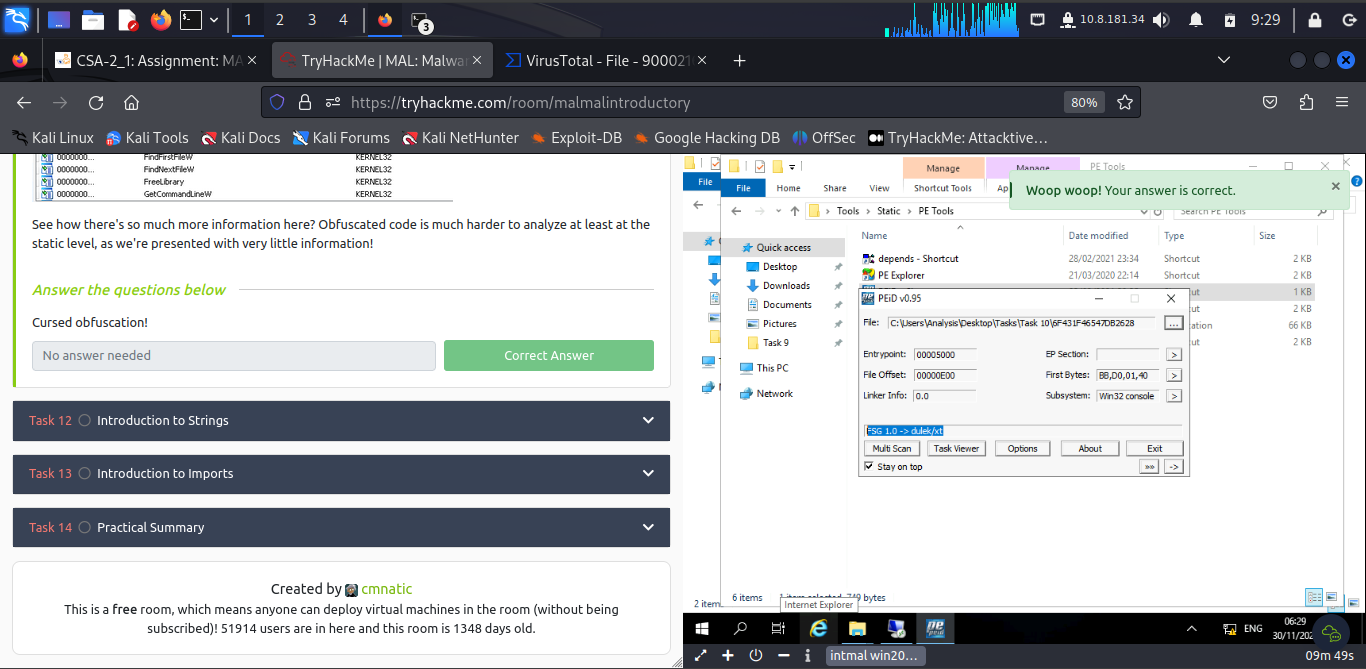
***Task 10: What is Obfuscation/Packing***

Packing is one form of obfuscation that malware Authors employ to prevent the analysis of programmes.



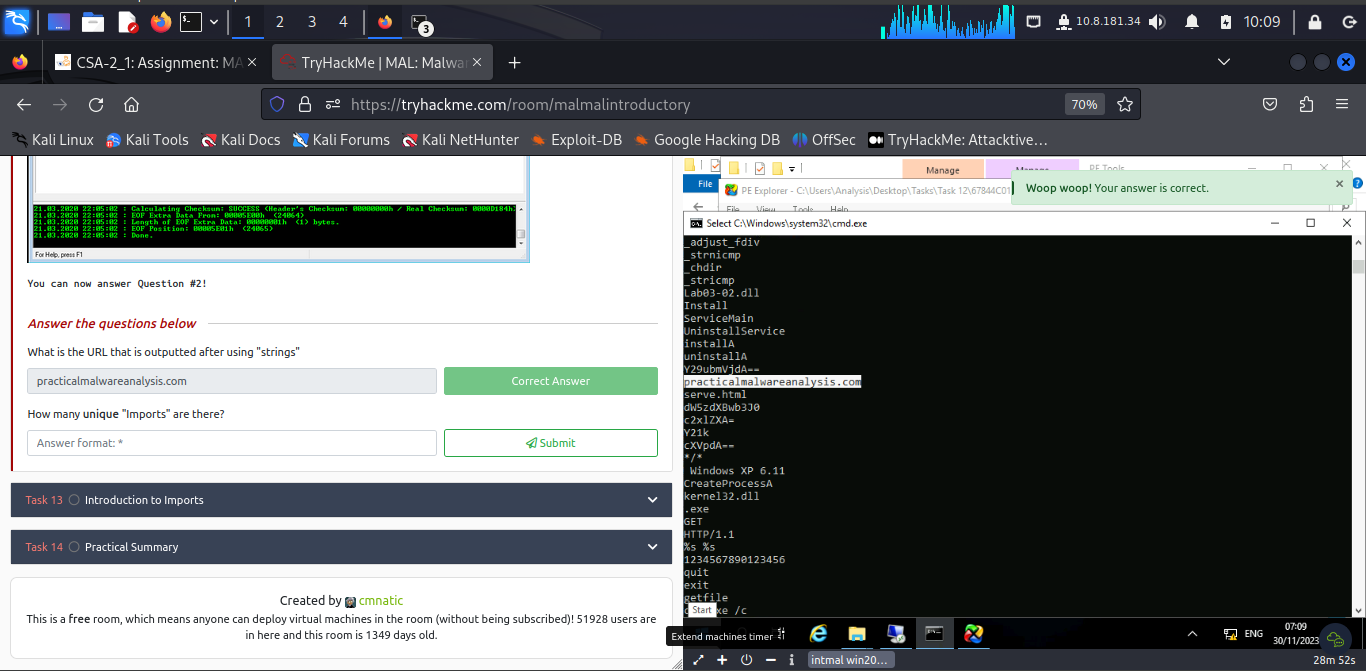


***Task 11: Visualizing the Differences Between Packed & Non-Packed Code***

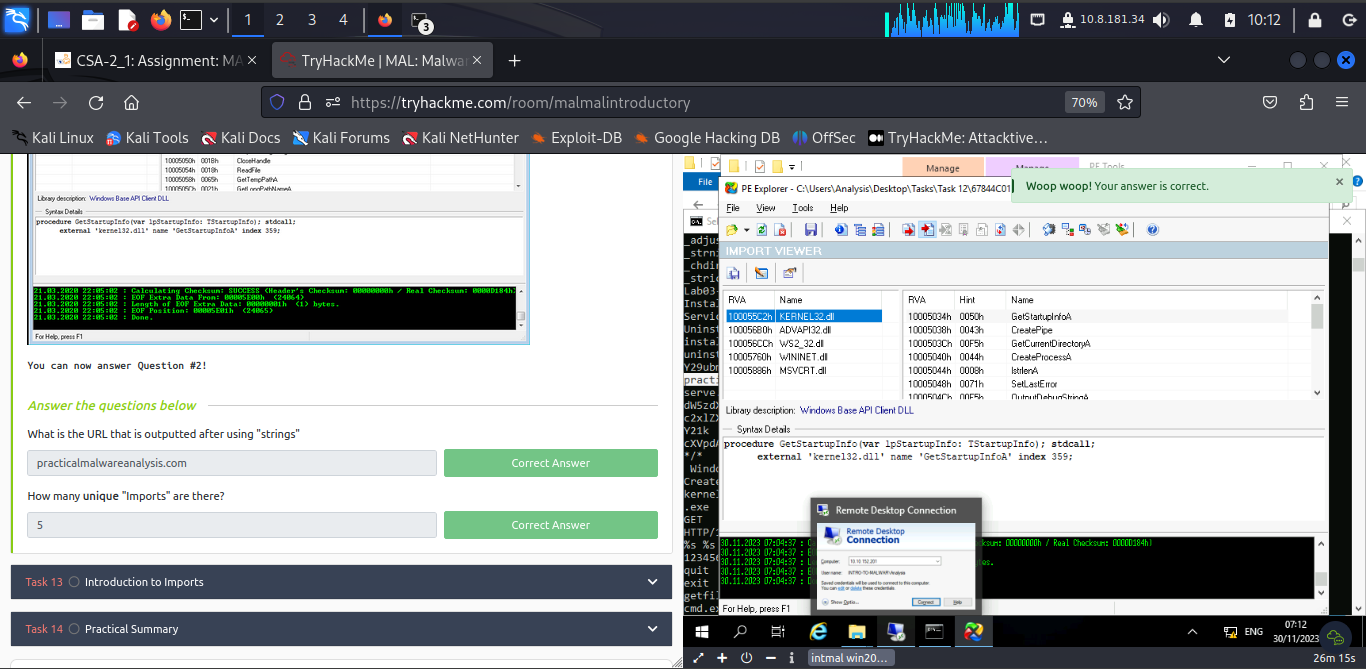


***Task 12: Introduction to Strings***

The URL that is outputted after using "strings" is **practicalmalwareanalysis.com**

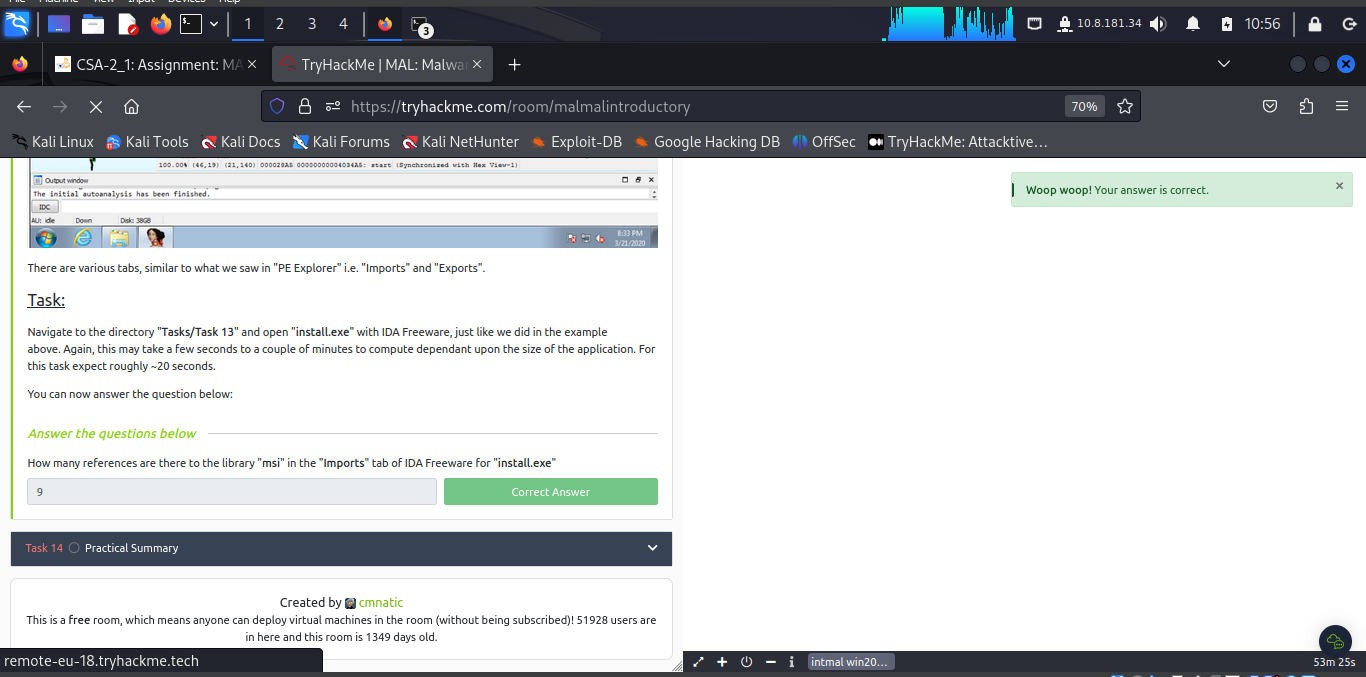


**unique** "Imports" available are **5**.

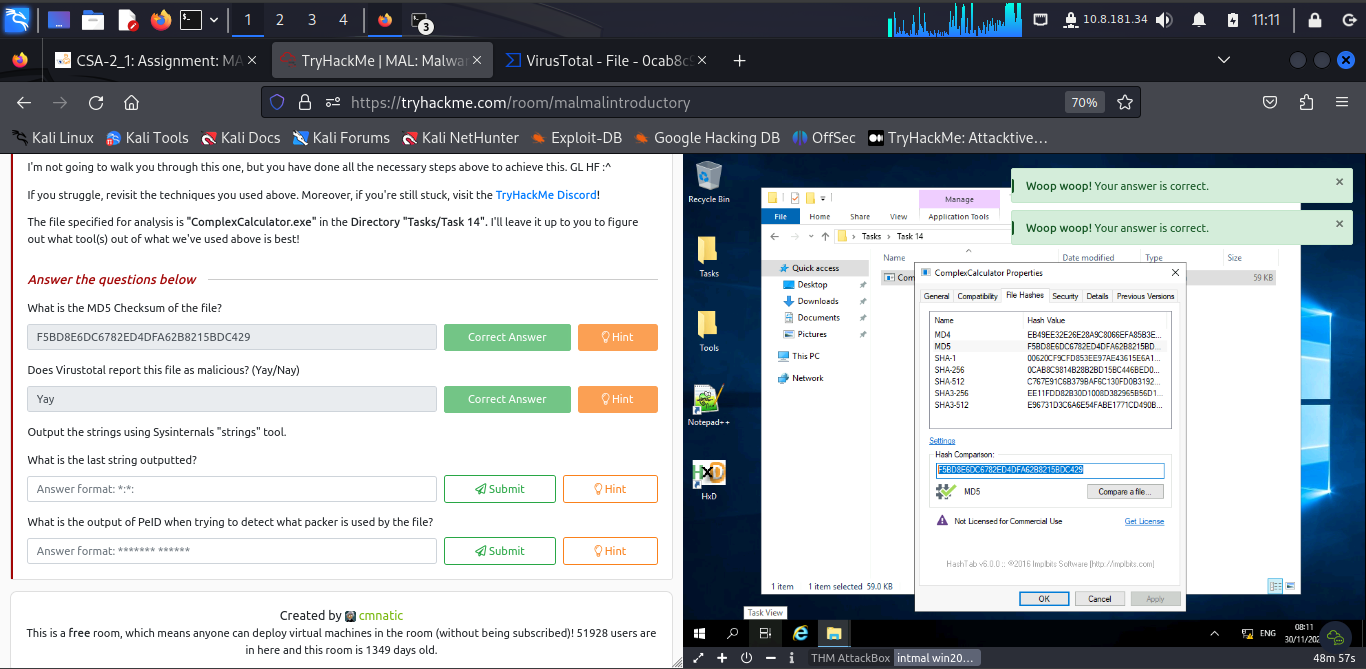


***Task 13: Introduction to Imports***

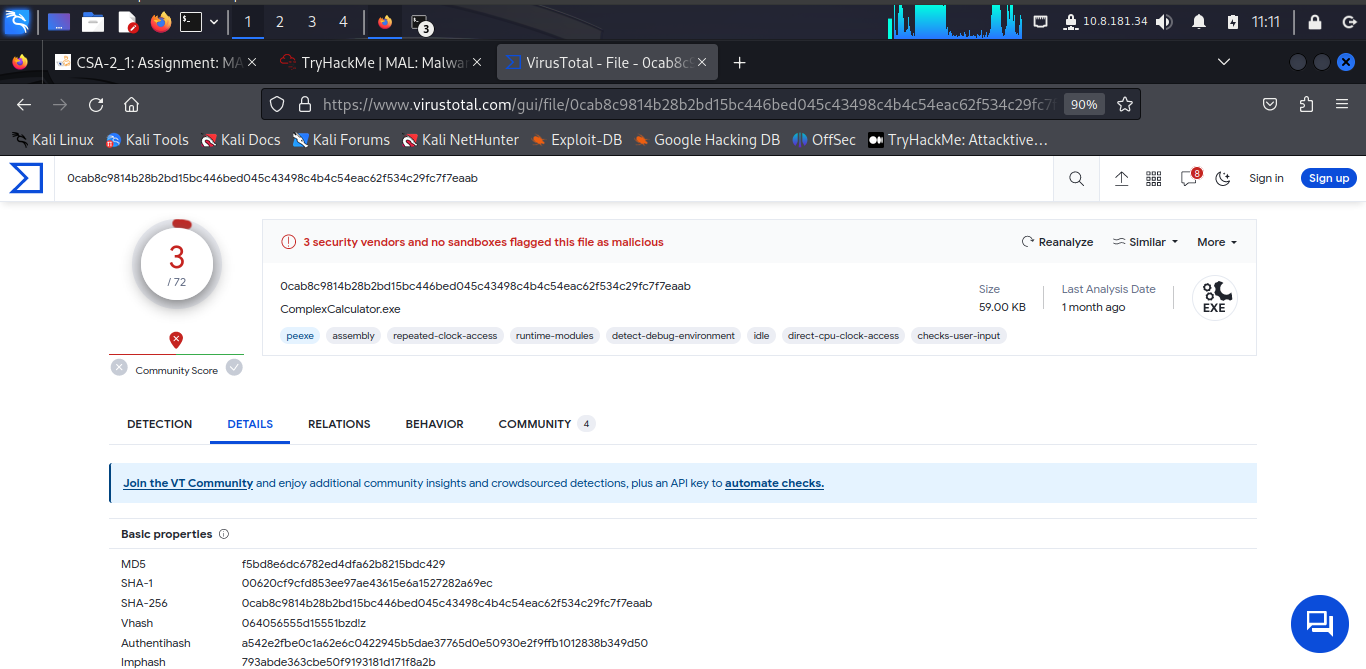
References available to the library "**msi**" in the "**Imports**" tab of IDA Freeware for "**install.exe** are **9**.



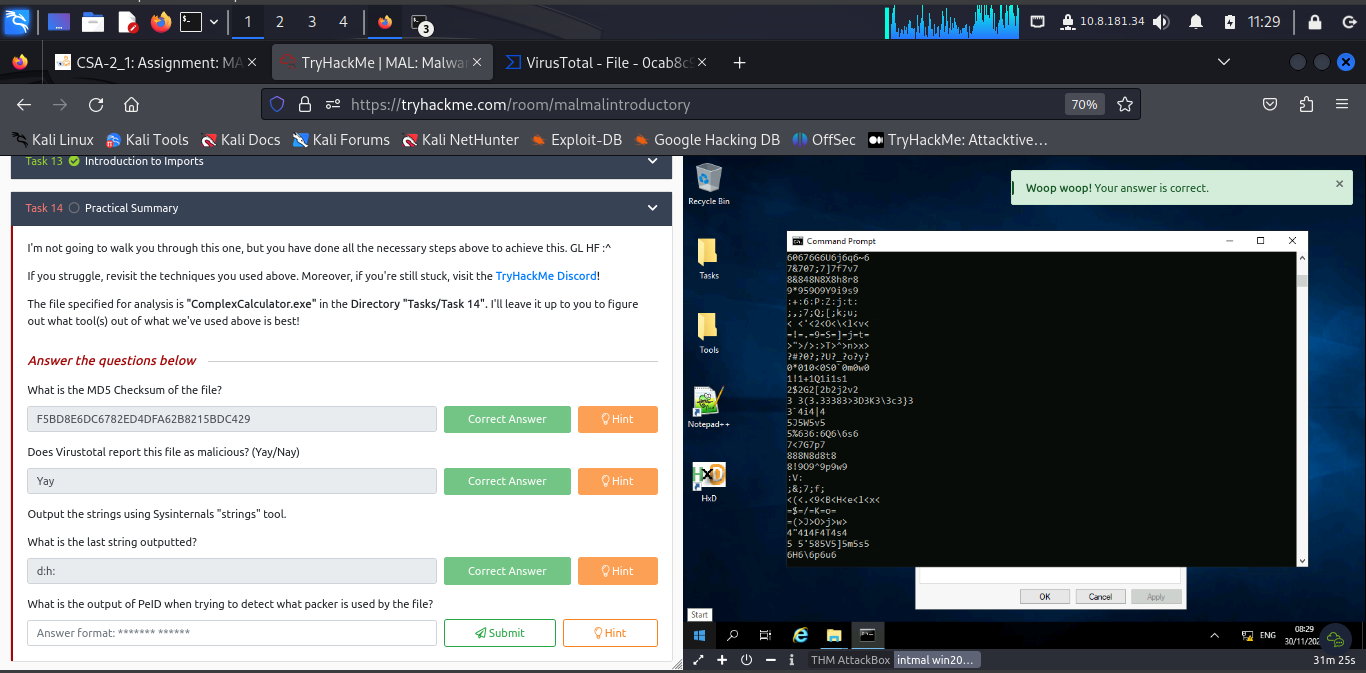
***Task 14: Practical Summary***



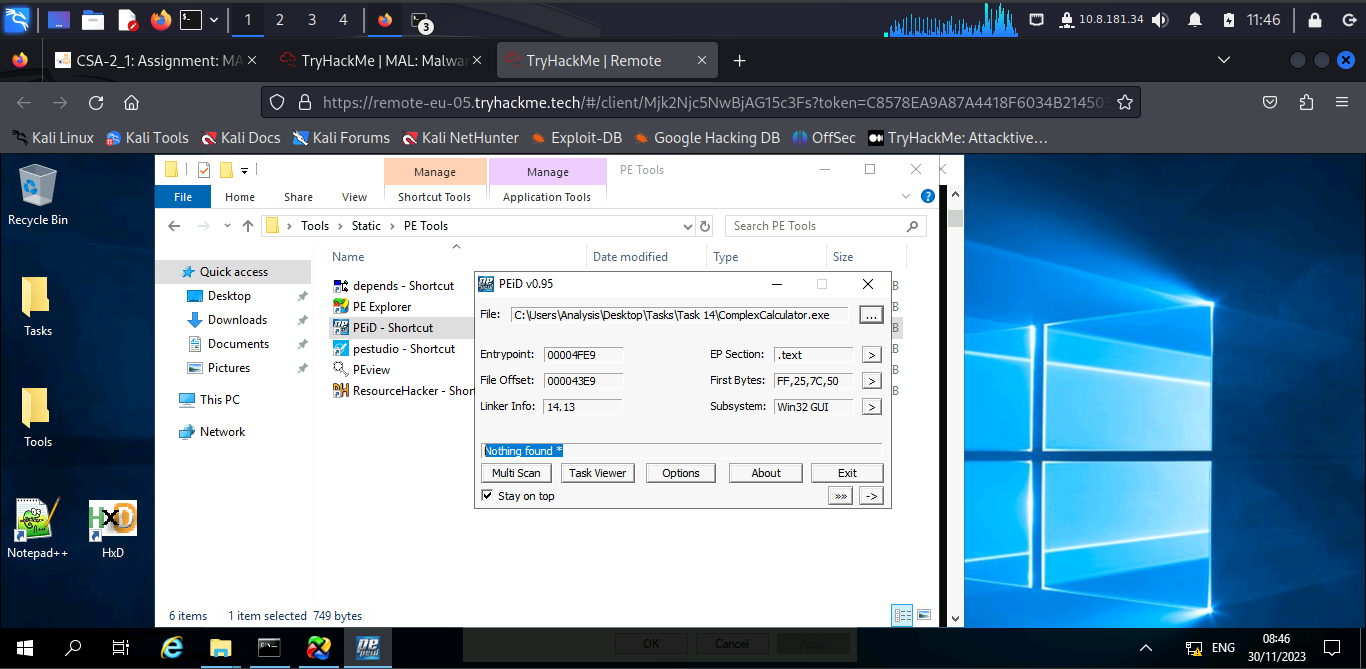
The Virustotal report this file as malicious, correct (**Yay**).

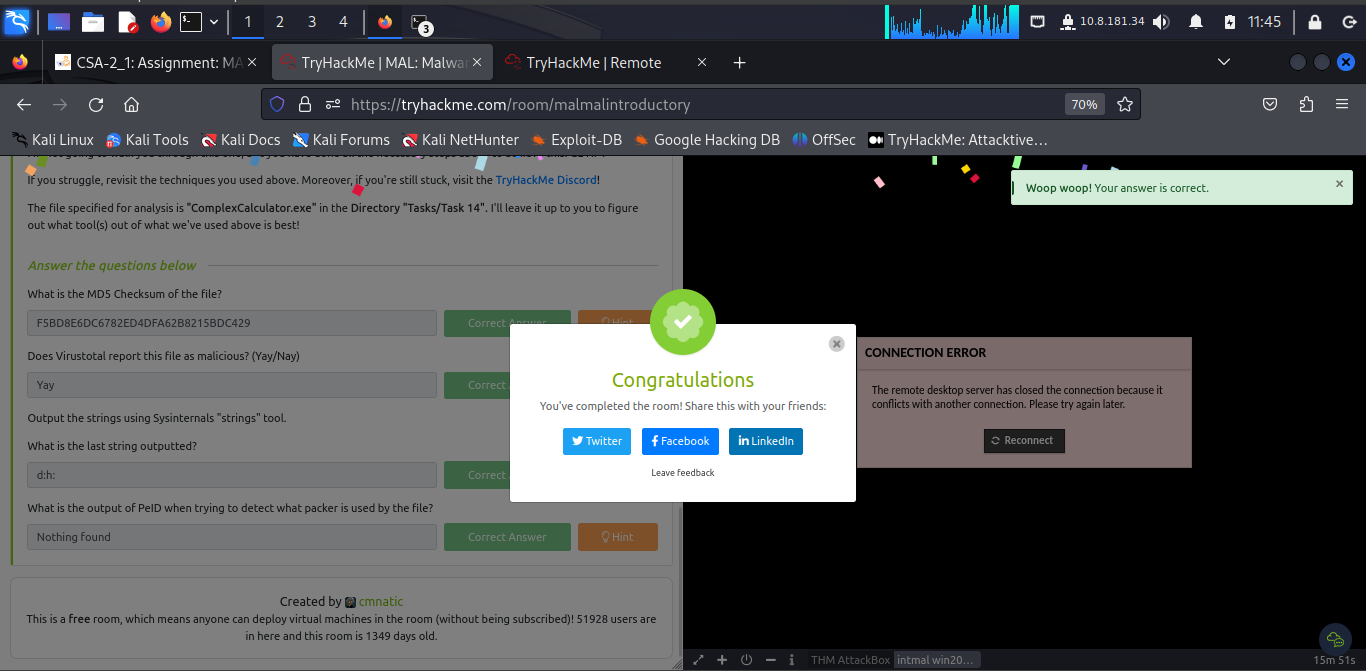


The last string outputted is **d:h:**



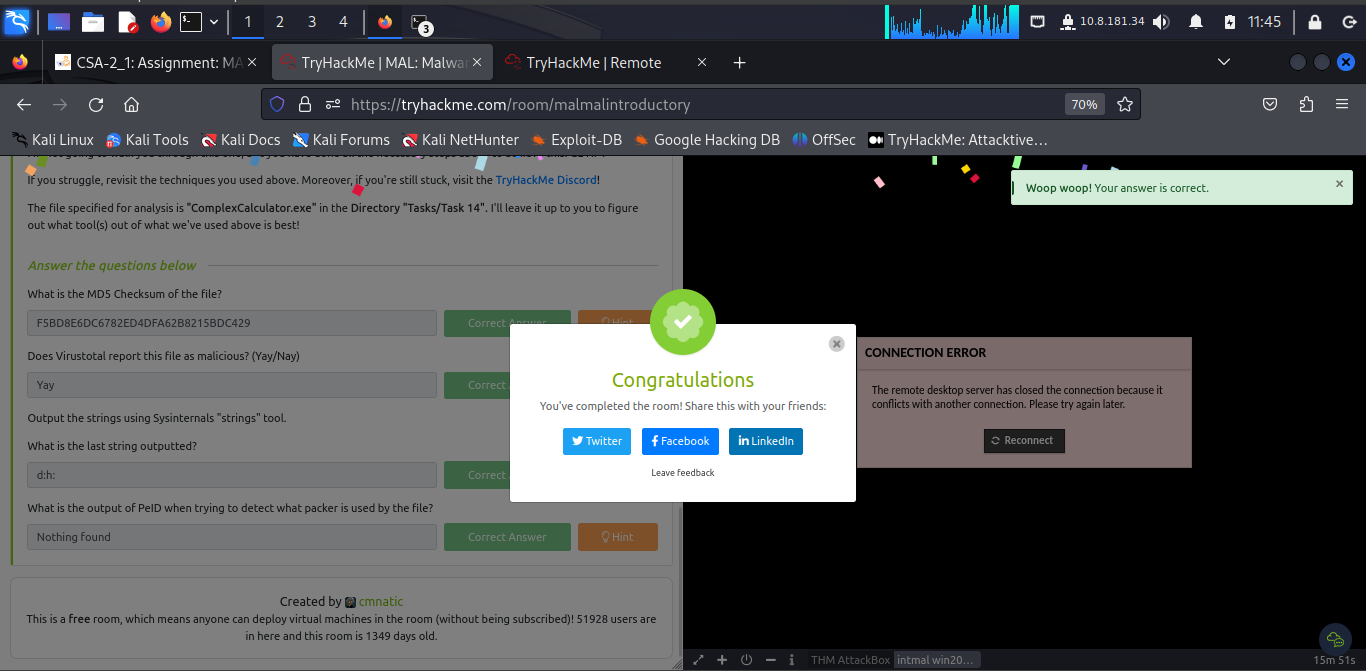
The output of PeID when trying to detect the packer used by the file is **Nothing found**.





**Conclusion**

This task took the learner through analyzing malware and using tools like PE Explorer, PEiD, IDA and to achieve the goal of recognizing types of files which can be harm in disguise; this knowledge is critical for aspiring Security Analyst to know the files available in a given computer device.



**Completion Link:** <https://tryhackme.com/room/malmalintroductory>