This challenge involves analysing the contents of a USB drive.

A computer screen shot of a computer

Description automatically generatedThe tool being used is FTK imager version 4.7.1.2, which will be used to look at data inside the USB. After selecting the USB, it will appear in the Evidence Tree. Then a scan will be conducted on the USB to retrieve all the required information.

**Question 1) What is the malware C2 server?**

The file ‘DO\_NOT\_OPEN’ has been deleted, however the contents have a text file called “secretchat.txt”.

Opening that up shows the answer to this question.

**Answer**: mcgreedysecretc2.thm

**Question 2) What is the file inside the deleted zip archive?**

While still inside the “DO\_NOT\_OPEN” deleted folder, there is the only zip file.

A white background with black text

Description automatically generated

Opening it reveals an executable called “JuicyTomaTOY.exe”.

**Answer**: JuicyTomaTOY.exe

**Question 3) What flag is hidden in one of the deleted PNG files?**

Going back to the root folder.



A screen shot of a computer

Description automatically generatedI ended up discovering that this was the required PNG file. However, the process I repeated for the other PNG files on the drive. Click on the file, then on the bottom of the program hex will appear. Open up find panel and type the basic flag format (for TryHackMe – THM) which is ‘THM{’.

A number on a white background

Description automatically generated

The flag is highlighted.

**Answer**: THM{byt3-L3vel\_@n4Lys15}

**Question 4) What is the SHA1 hash of the physical and forensic image?**

This is important for digital forensics as it allows professionals to examine digital evidence without altering the original data, ensuring a reliable and accurate analysis for investigations and legal proceedings.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedFirst you right click the USB drive, then click ‘Verify Drive/Image’. This process may take a couple of minutes to complete.

**Answer**: 39f2dea6ffb43bf80d80f19d122076b3682773c2