Drive Discovery

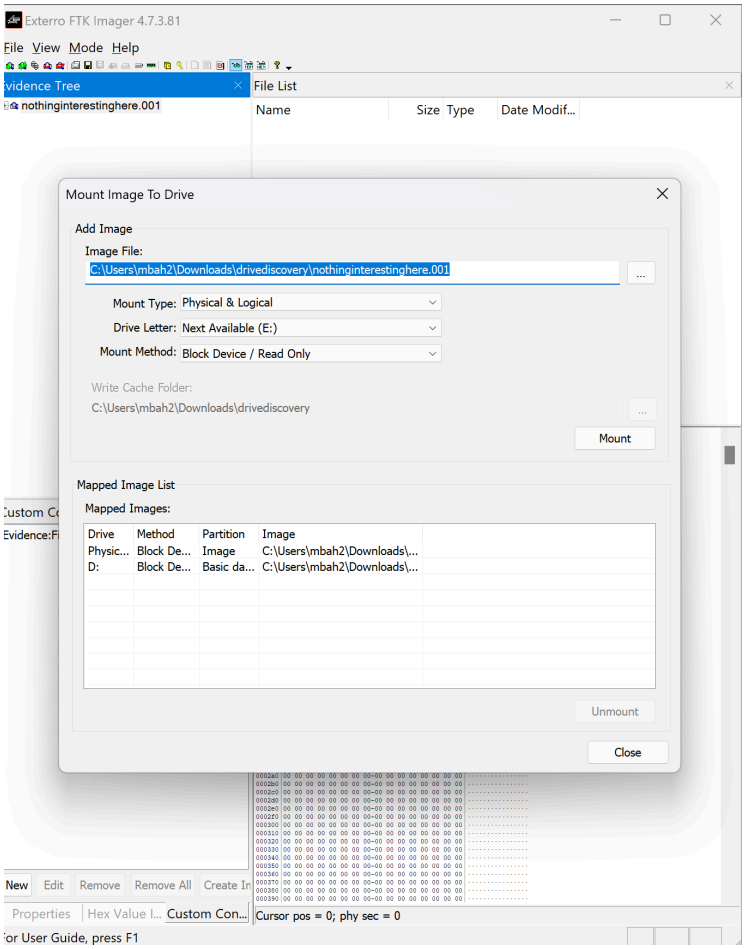
Forensics BGR

In this challenge, I was provided with a ZIP file. This ZIP file includes a WinRAR archive along with a text file saying:

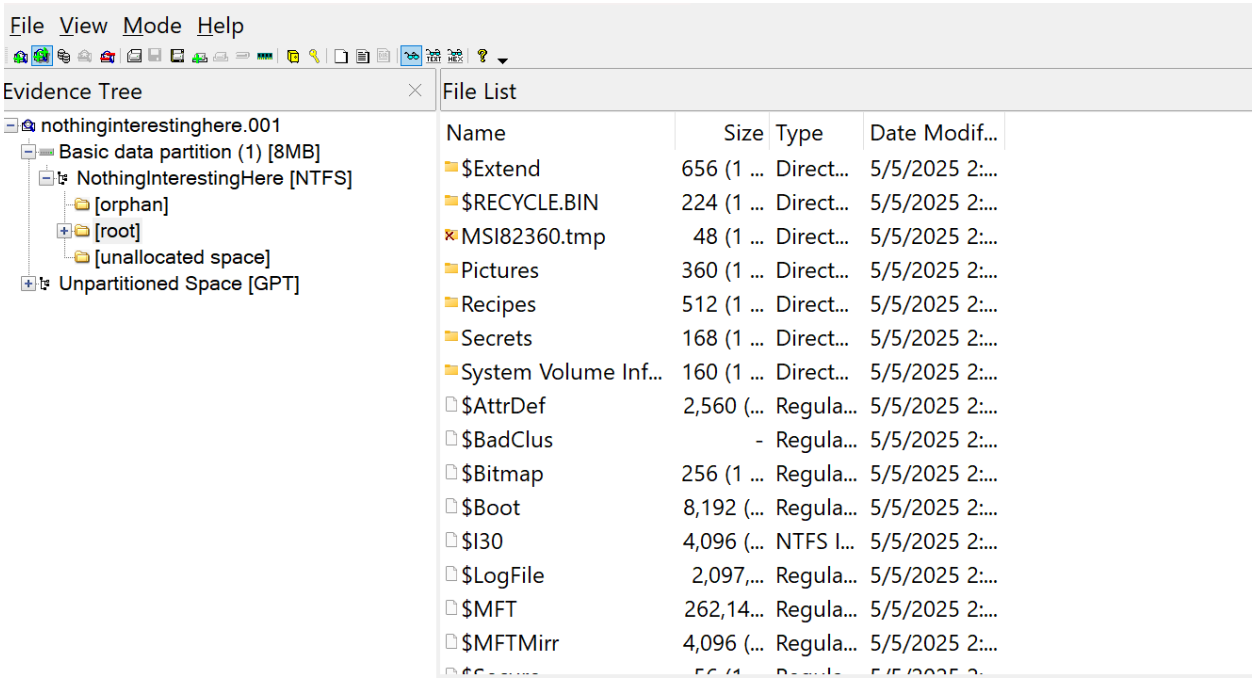
```
Textproto
We took an image of a suspicious USB drive - can you investigate it in more
detail?
We think the user may have tried to cover their tracks.
```

Because we are dealing with a USB drive, we can utilize FTK Imager to mount an image of the media.

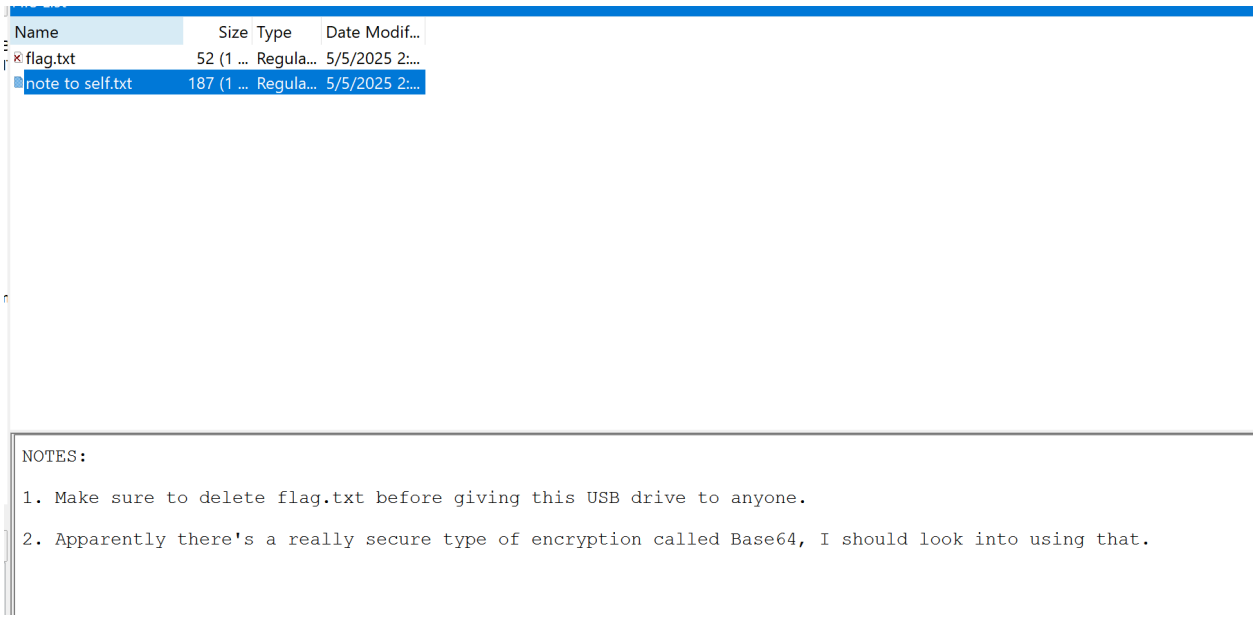
To mount, we will add it the WinRAR file to the imager, right click in the evidence tree on the image, click image mount, and then hit mount



Then you can use the drop-down menu in the evidence tree to navigate to **basic data partition > root.** Now we can see all the files that were stored on the USB Drive.



The secrets folder seems quite interesting. Let's check out what is going on in there.



We have a flag.txt and note to self.txt file. As mentioned in the note to self text file, we notice that it references a "secure type of encryption called Base 64". Base 64 is neither encrypted nor is it secure in a confidentiality standpoint. It's simply an encoding method. The text in flag.txt is "U1ZCUkd7ZDNsMzczZF9uMDdfZjByNjA3NzNuXzI4MzAyOTM4Mn0=" . Base 64 typically

tends to have an = sign at the end, so let's attempt to run in through a Base64 to ASCII converter to get the decoded result.

> **Base64** copy clear download
>
> U1ZCUkd7ZDNsMzczZF9uMDdfZjByNjA3NzNuXzI4MzAyOTM4Mn0=
>
> Decode Base64 to ASCII
>
> **Text** copy clear download
>
> SVBRG{d3l373d_n07_f0r60773n_283029382}
>
> The result of Base64 decoding will appear here

Just like that we have our flag:

```
None
SVBRG{d3l373d_n07_f0r60773n_283029382}
```