|  |  |
| --- | --- |
| Evidence Number | Title |
| 19 | The Lonely Witness |
| 10 | Criminal Minds |
| 4 | The Game of Shadows |
| 14 | Murder on The Orient Express |

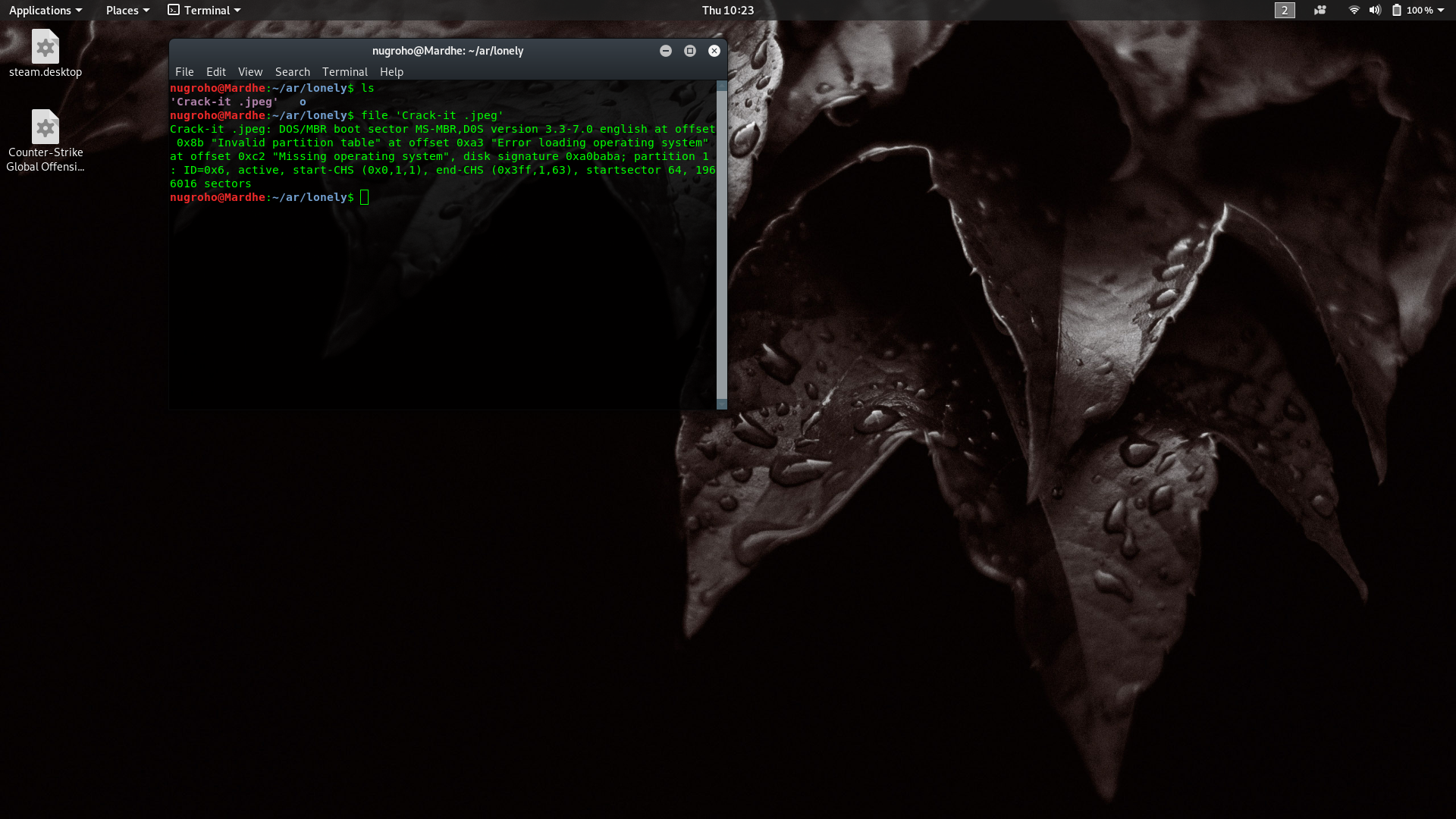
TEAM: Chochob33

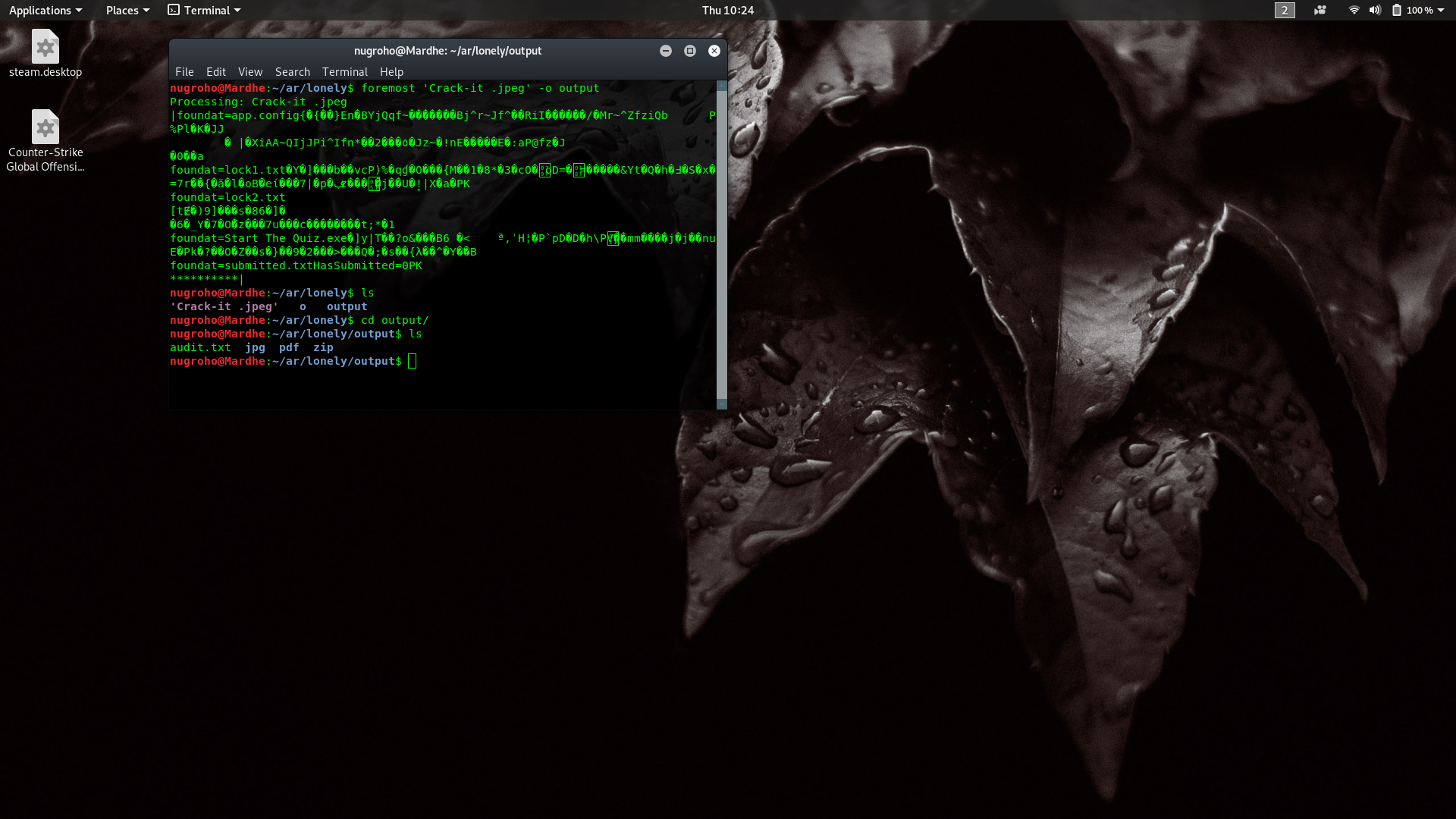
The lonely witness

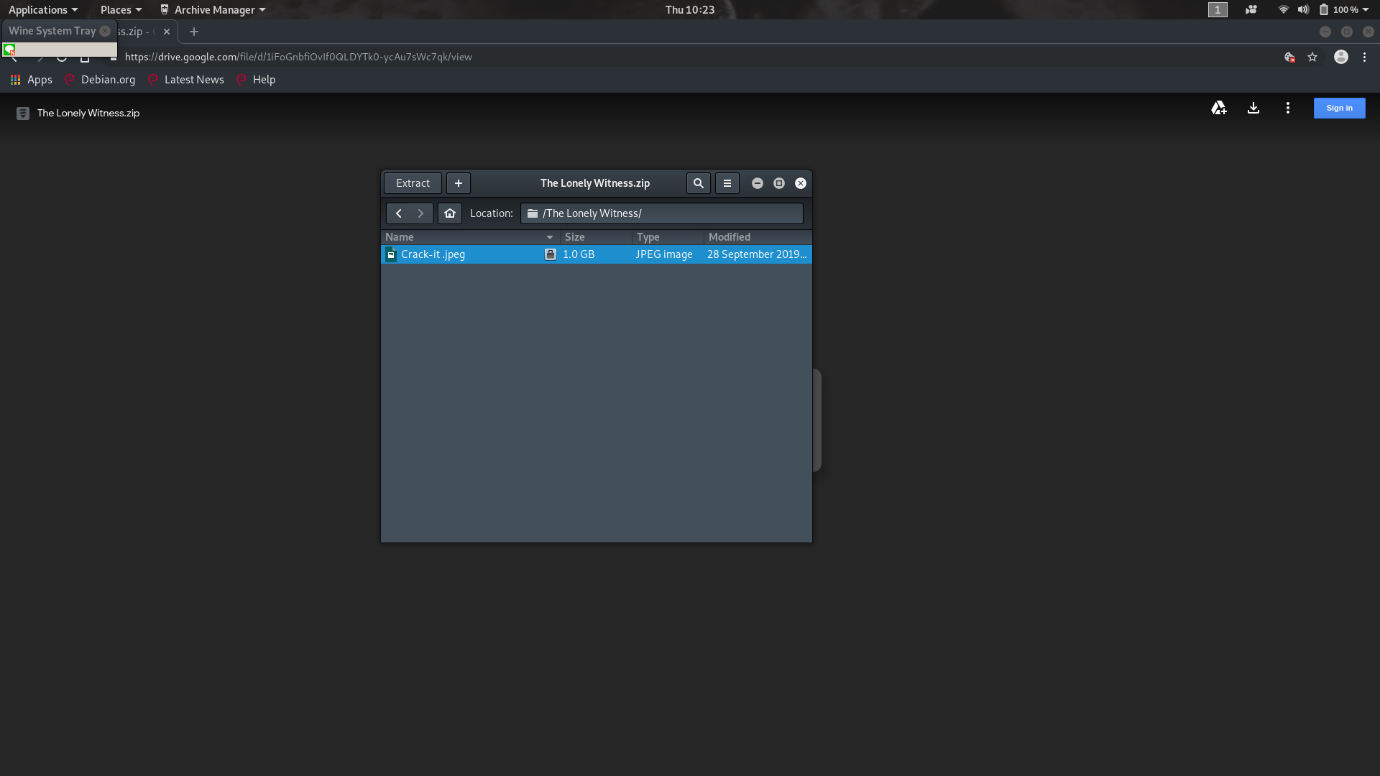
Evidence Number : 19

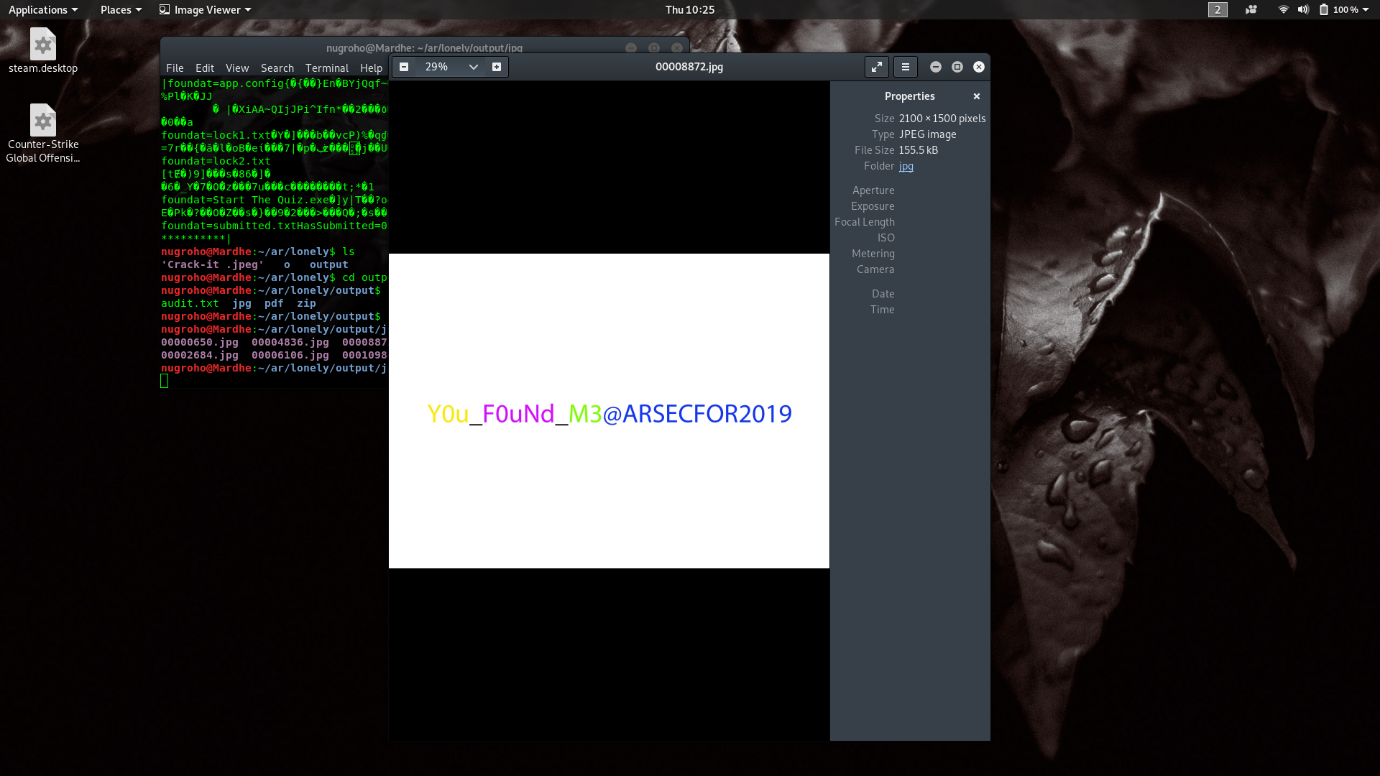
Evidence Collected by Reza

1. The file is on zip file
2. Unzip it
3. You will find a jpg, but it shows that it is not a jpeg, it is a memory
4. So, recover memory by the command, foremost ‘filename’ -o o
5. So, the output will be at directory o
6. The flag will be “Y0u\_F0uNd\_M3@ARSECFOR2019”







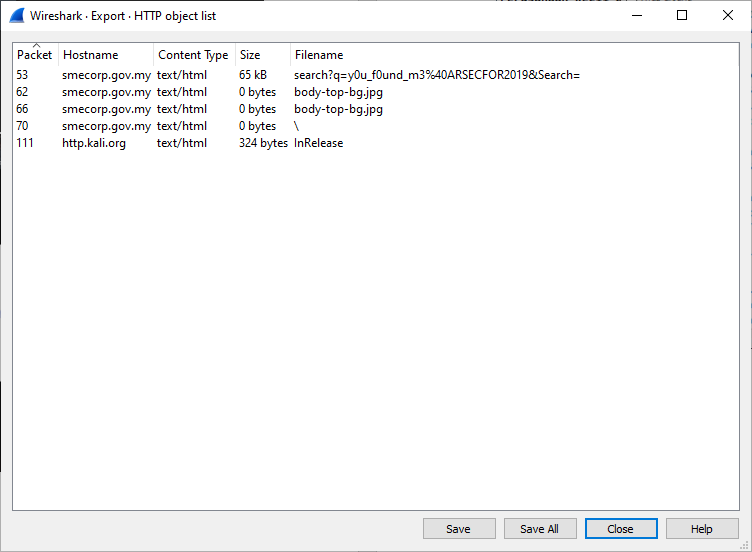


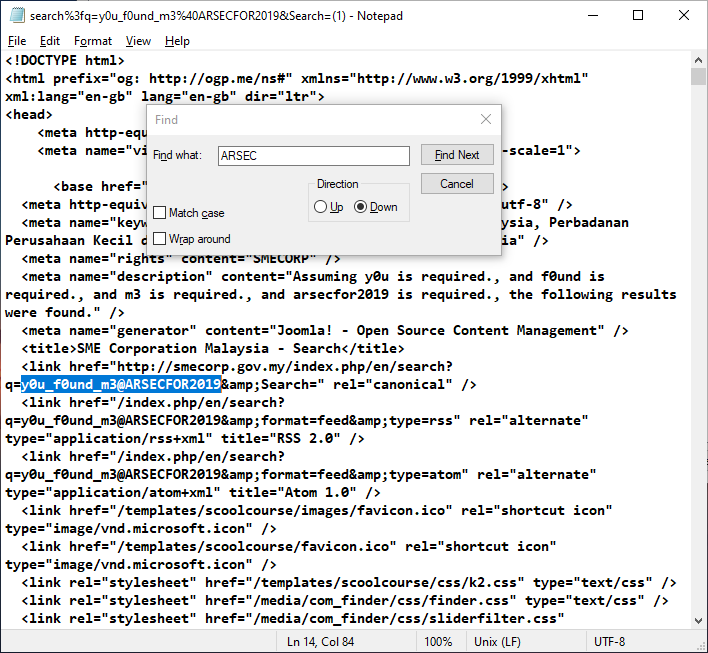
Criminal Minds

Evidence Number 10

Evidence collected by William

1. Export object to HTTP
2. Open the search%3fq=y0u\_f0und\_m3%40ARSECFOR2019&Search=(1) file
3. There you will find the flag “y0u\_f0und\_m3@ARSECFOR2019”



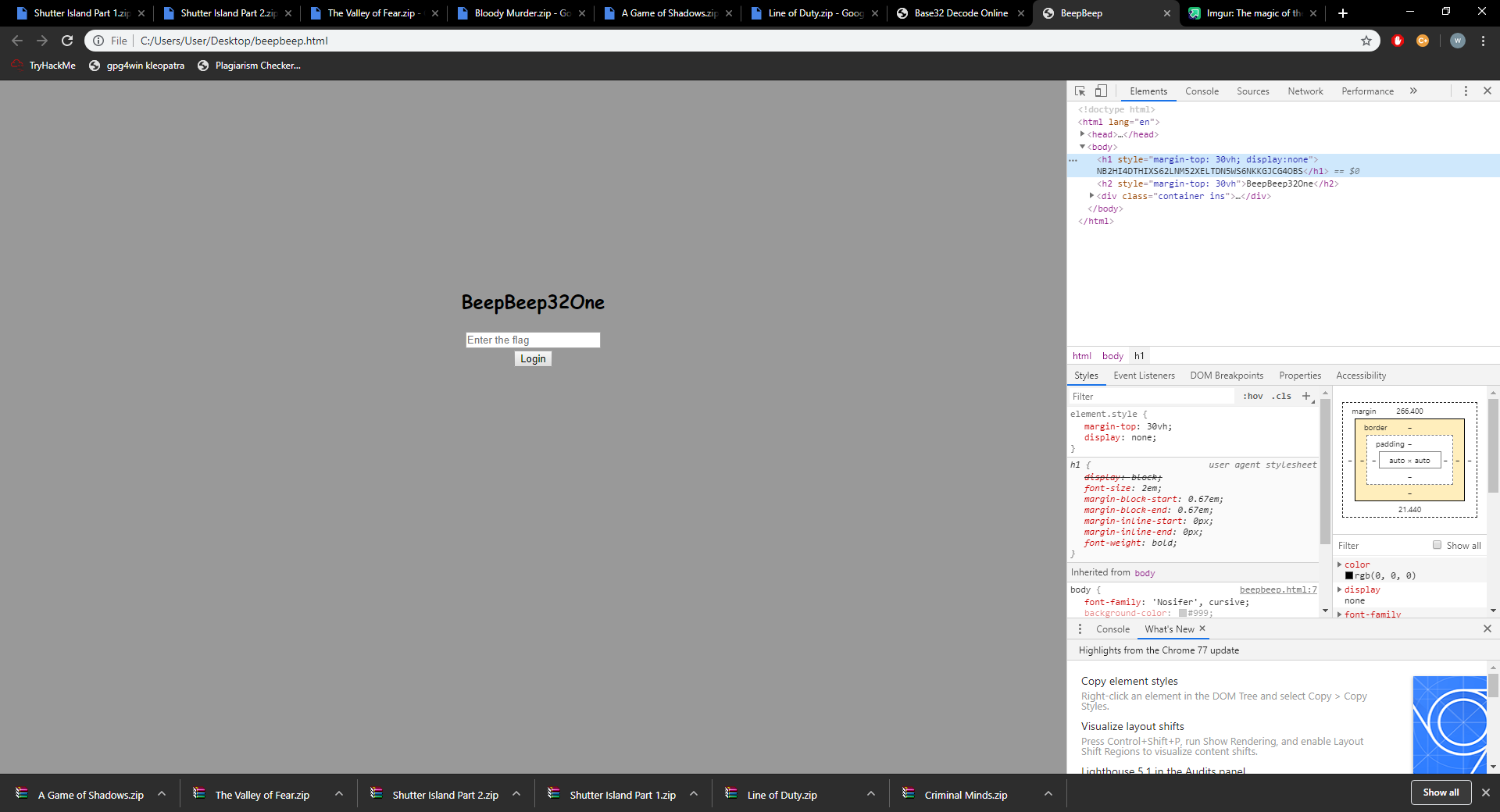


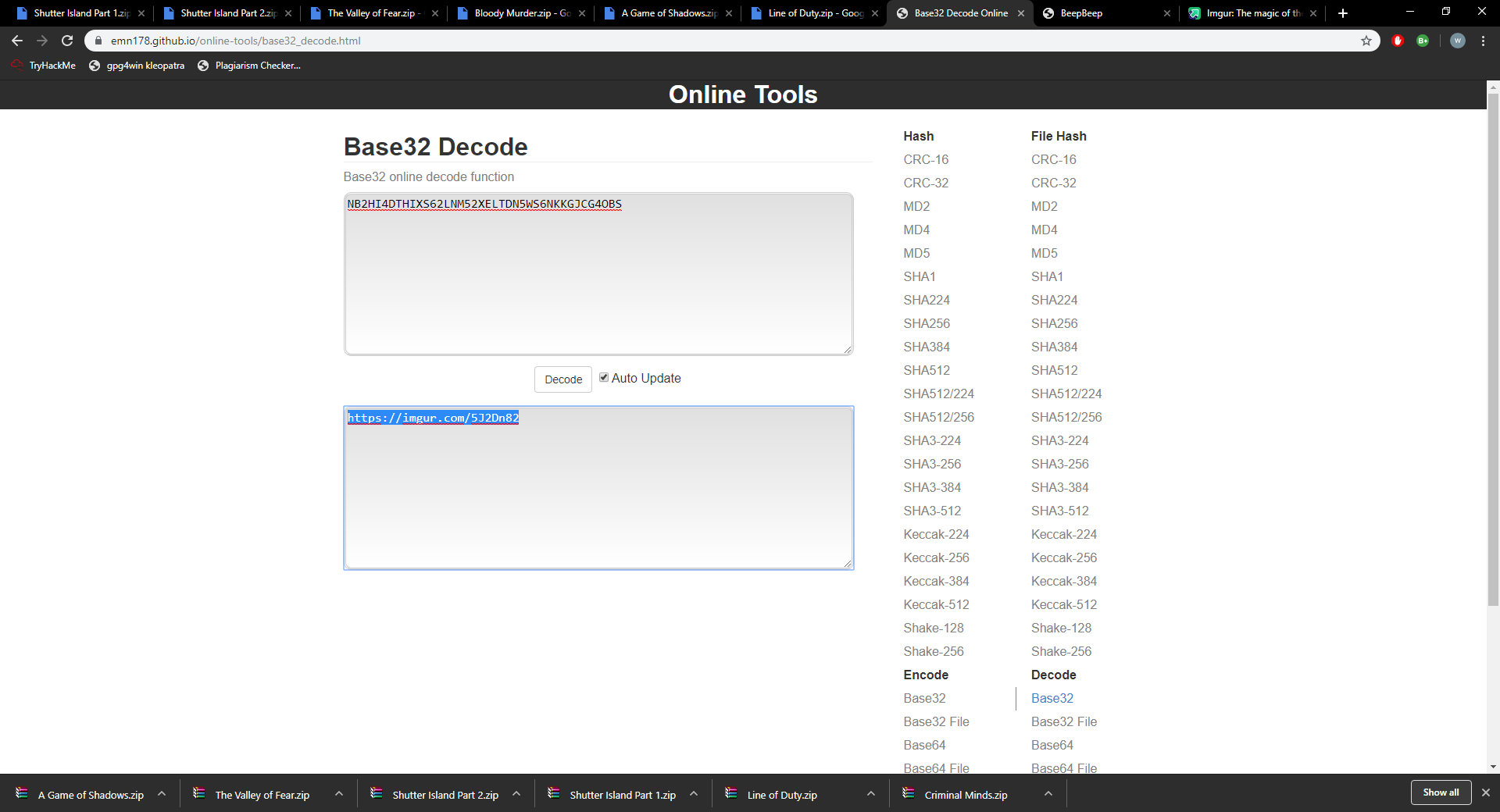
Game of shadows

Evidence Number 4

Evidence collected by William

1. Open the file and inspect it
2. Found a Base32 Text
3. Decode and open the imgur file
4. The flag is “p0$Tman@ARSECFOR2019”







Murder on the orient express

Evidence number 14

Evidence collected by William

1. With HxD editor we know that ready contains docx and steady contains rar
2. Open the steady doc file and we get the pass is AR-FRC
3. And use it to open the pdf file at steady rar file
4. There we know the flag is “(1Nv3$71G@710N\_$7@r7) @ARSECFOR2019”

