FORENSICS

Device Forensis 1

I extracted given file and I got the file that has E01 extension and EVF file header.I didn't know how to open this genius file.I searched how to open this file.A few minutes,I knew that is **Autopsy can open this file.**

So,I opened file with Autopsy.I was shocked bcz it has linux and window files.I have never seen that bcz I am newbie in FORENSICS.Task is to get os info.I opened many folders to get os-release files bcz os info still in os-release files in linux file system.That is too long.So,I used find keyword to find this.And then,found os-release file.

Look at image 1 :

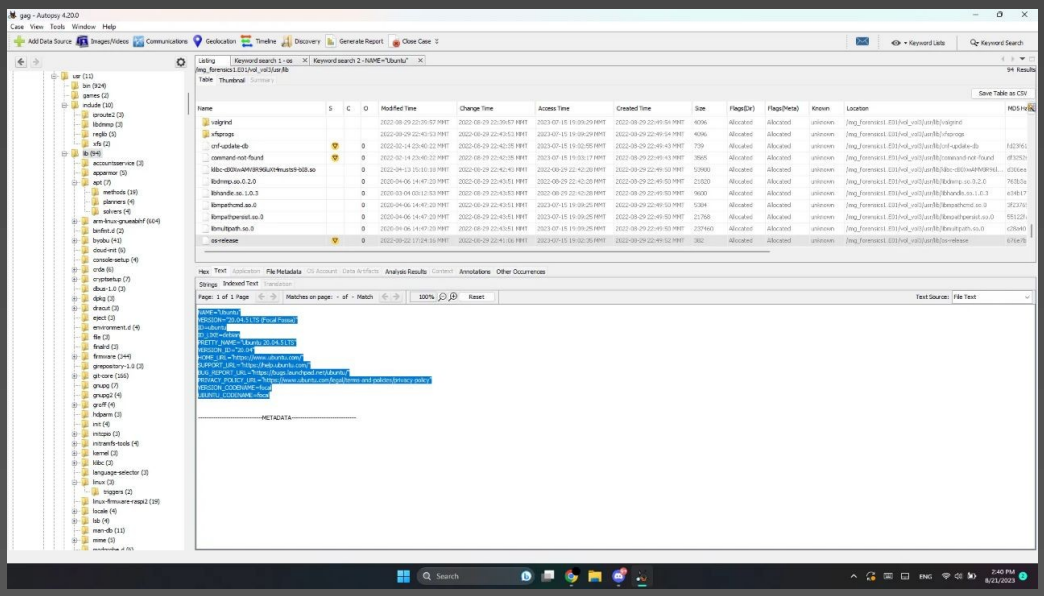


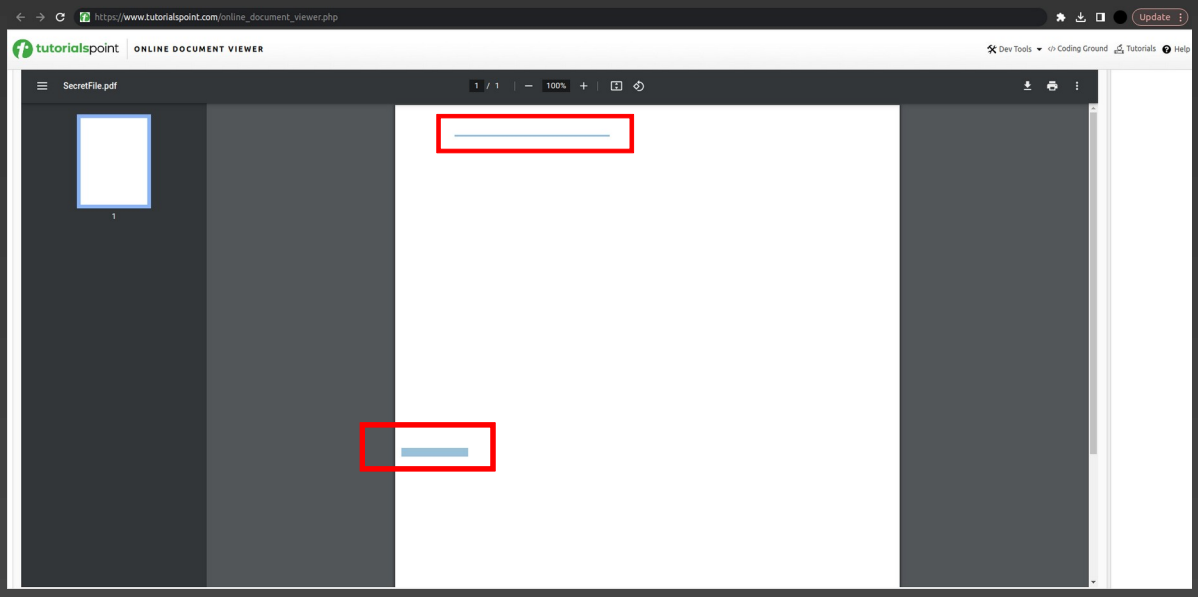
Image 1

And I make flag to correct format with this info.

Flag : **CyberGonCTF{Ubuntu 20.04.5 LTS}**

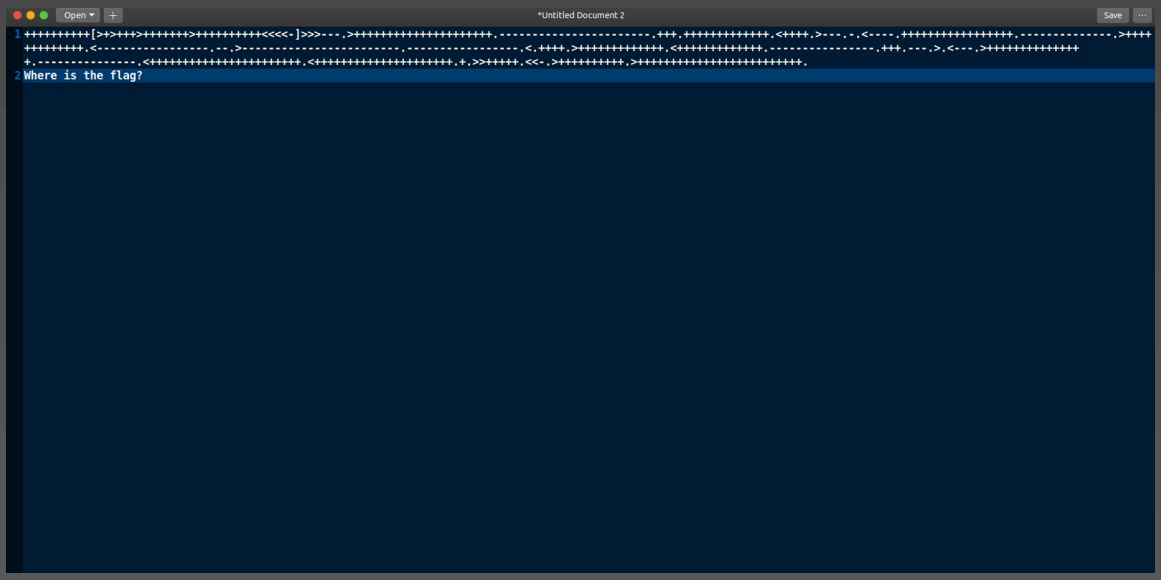
Hide and Seek

Given Docx file and I go to DOC viewer and I saw white blank page.WTH!(My reaction).i wanna know when I select this white page.So,i click on white page and select all.I saw two blue selection.



Look at red square box carefully

What is that.Thus,I copied all selected and paste in text editor.And I got some extra text.



:) It is brain fuck code and got to decode.fr to dcode this.And I got flag.

Flag : **CyberGonCTF{53cR37_D474_1n_H34d3R}**

8cel

Download the zip file.I opened the zip file and i check all folders in xl/worksheet/Sheet2.xml.I found some thing there are so many base 64 encodeing texts,I try to encode it but it show fake flag.I searched difference length and i found some thing difference fromfake flag.And then,I decode it.That how i found a flag.Look at image 2

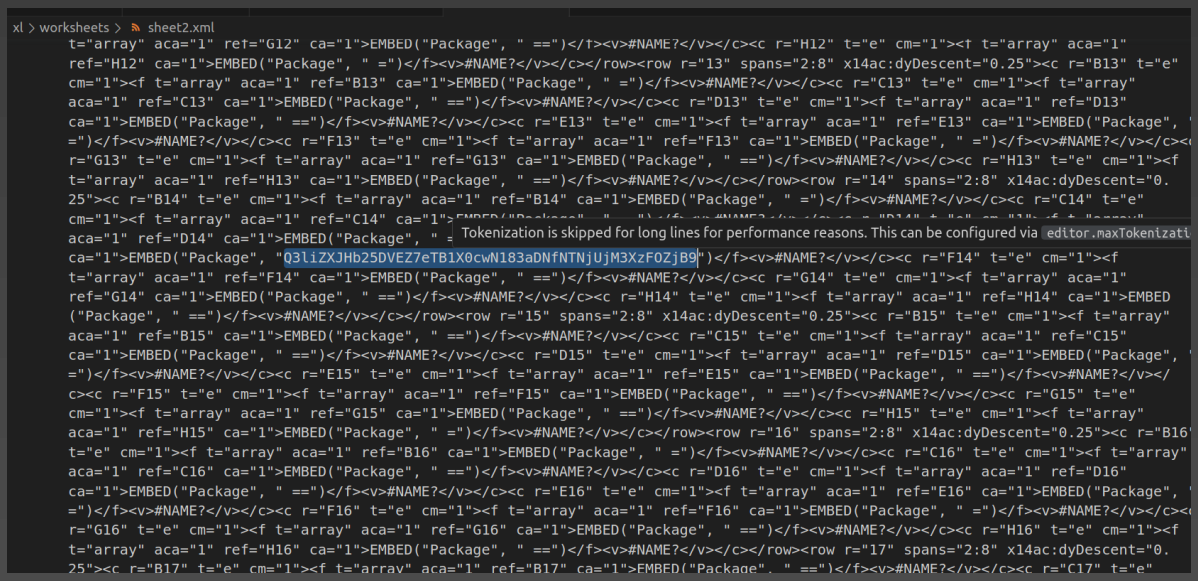


Image 2

Base 64 : Q3liZXJHb25DVEZ7eTB1X0cwN183aDNfNTNjUjM3XzFOZjB9

Flag : **CyberGonCTF{y0u_G07_7h3_53cR37_1Nf0}**