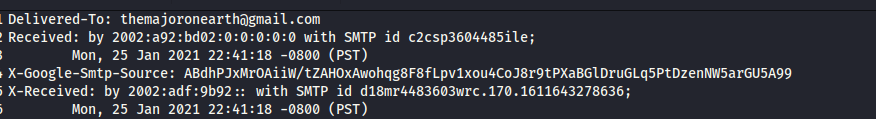
**Email Investigation**

Step 1 Check Email Headers

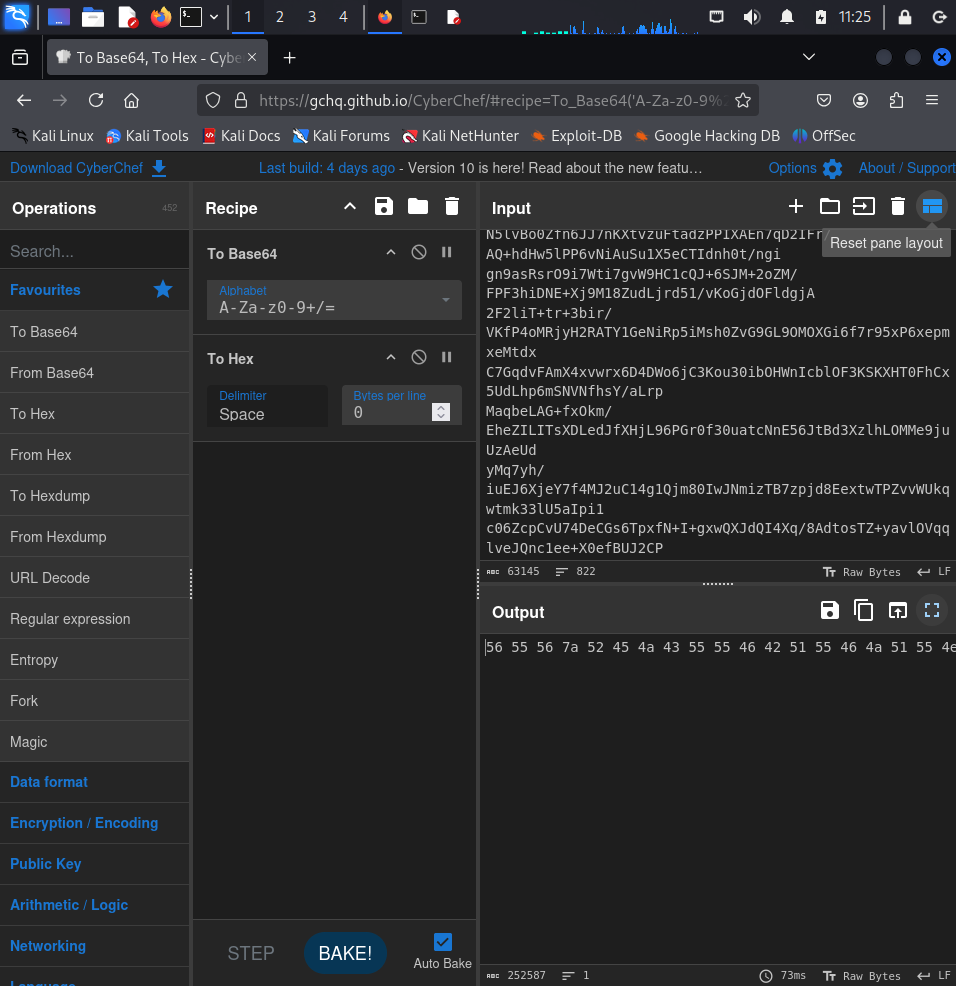


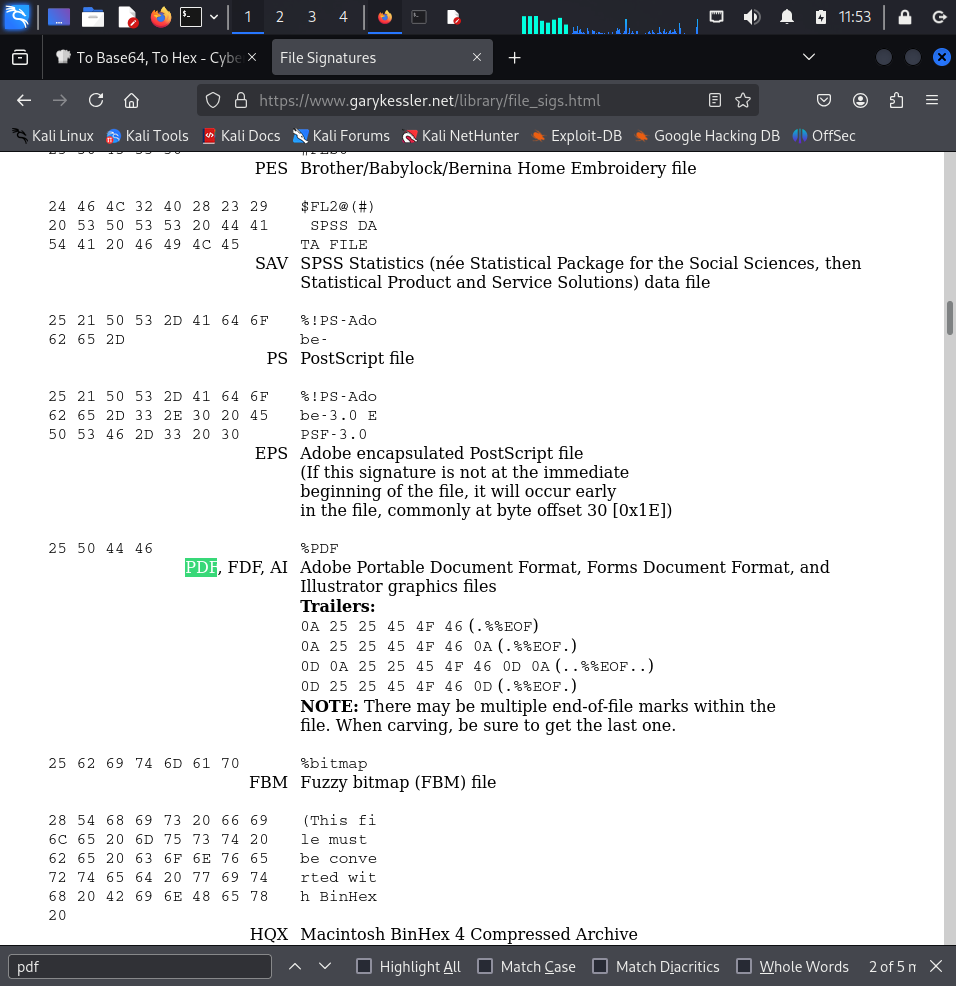
Step 2 Check For Authentication Protocol-> check that all three protocol are passed SRF,DKIM,DMARC



Step 3 File/Attachment Information

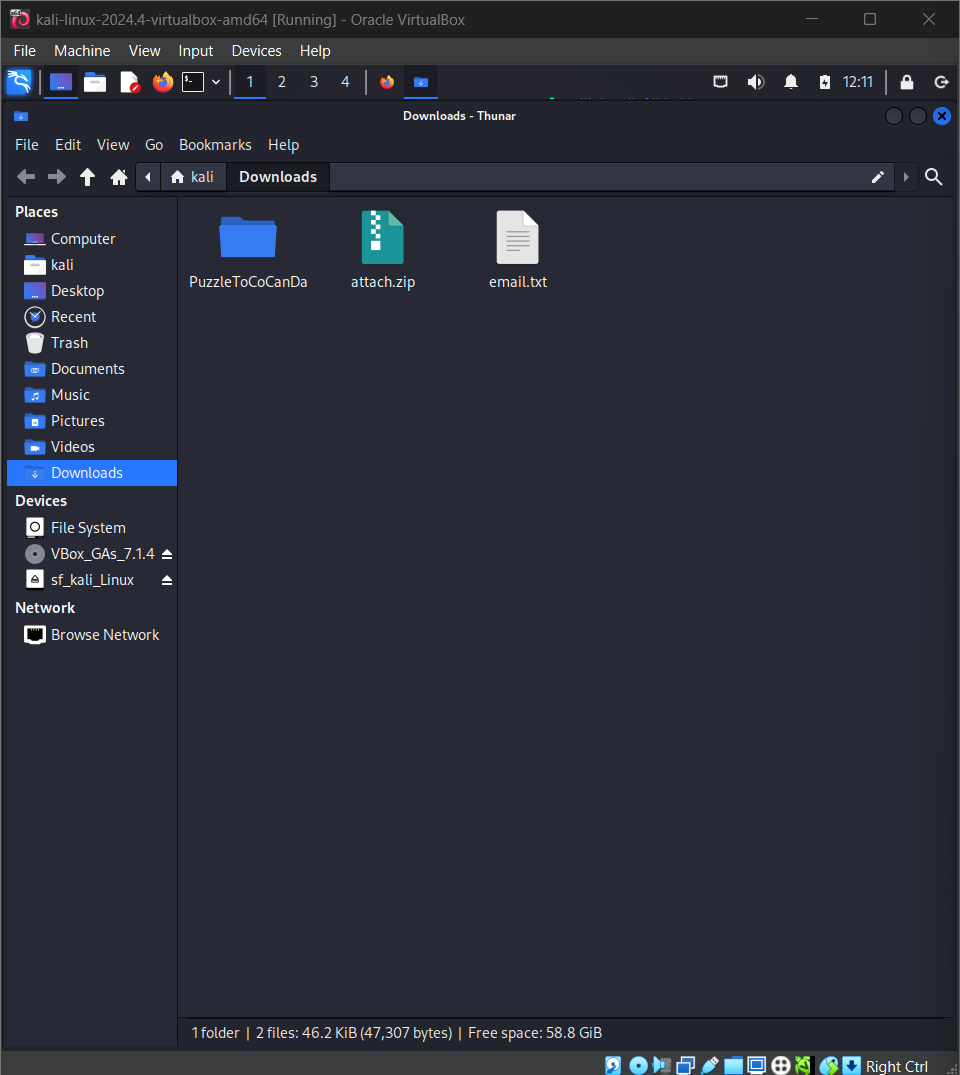
Decoding the base 64 pdf file to hex using cyberchef





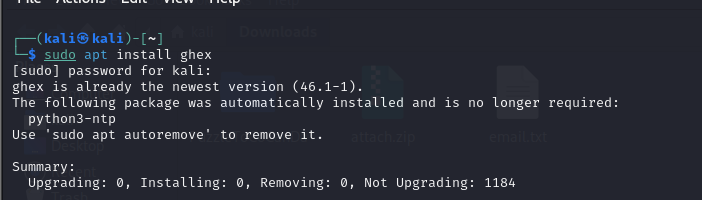
Both the Hex Value Doesn’t match

Now We Will Create a attach.zip file from the output of cyberchef and will extract it

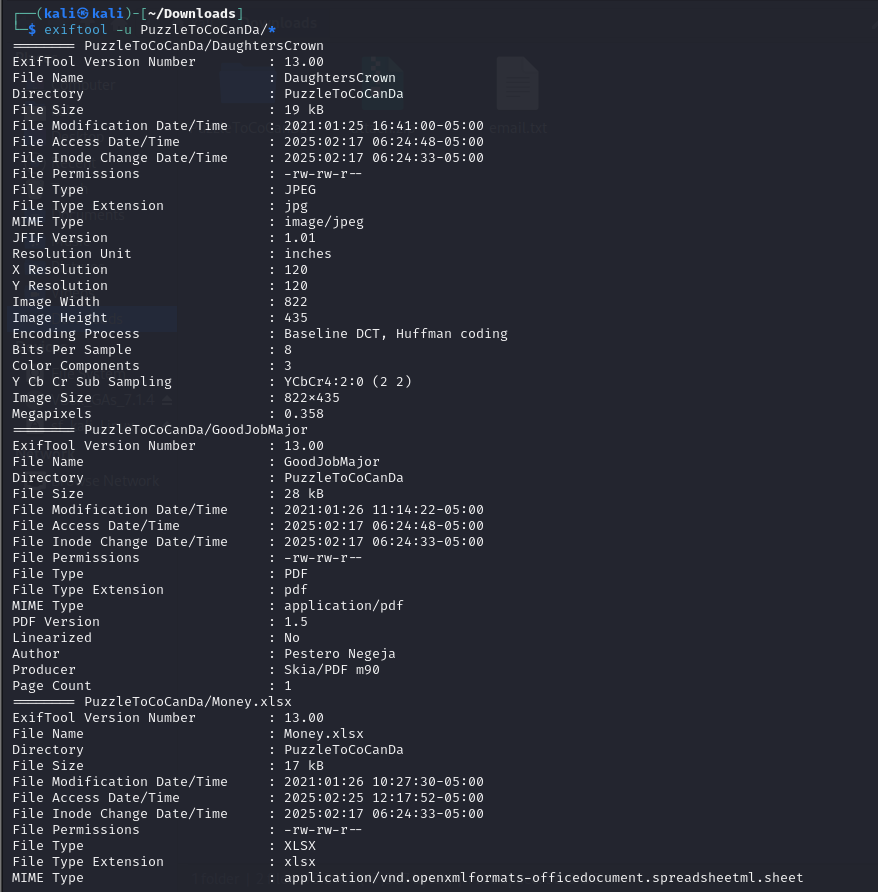


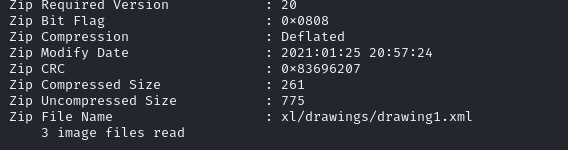
**Verification of Zip file**

**Installing Ghex-** sudo apt install ghex



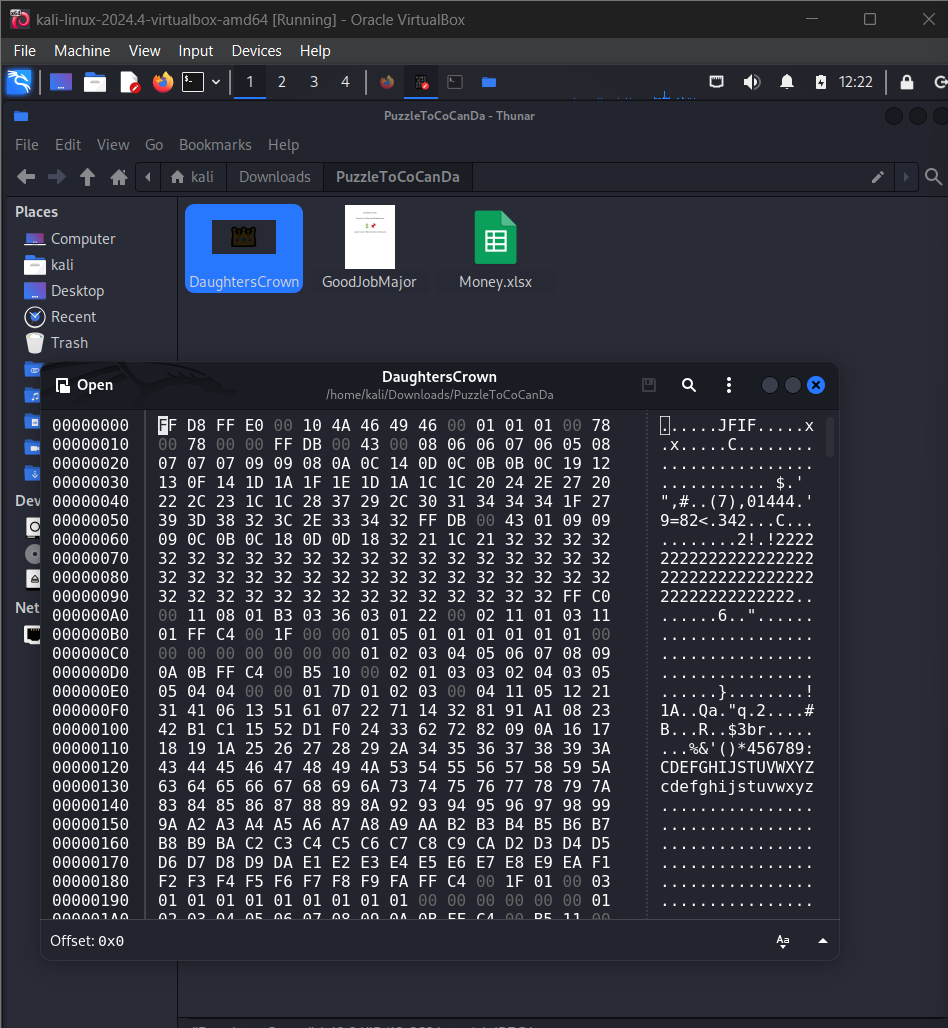
**To Scan all metadata at once**-exiftool -u PuzzleToCoCanDa/\*

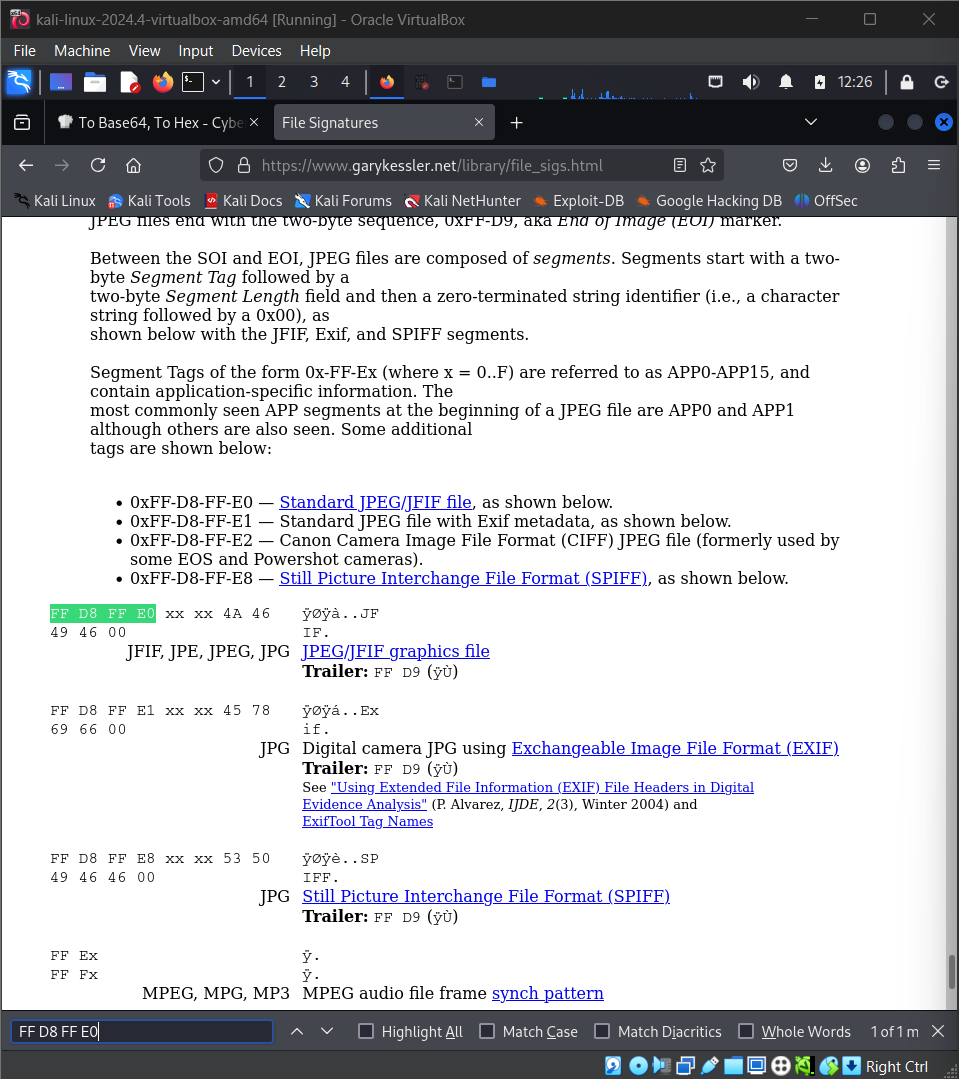




**To Check the Hex values of document-** ghex

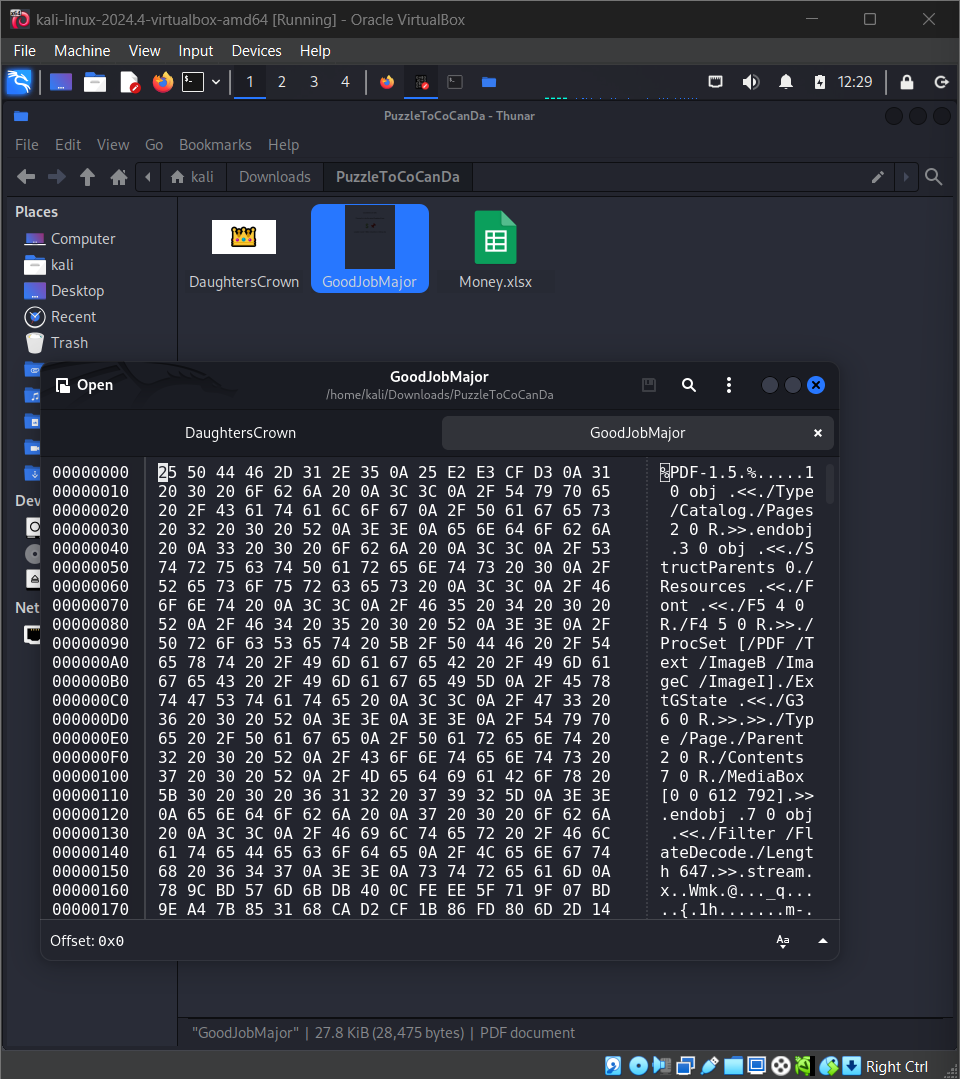
1. **DaughtersCrown**

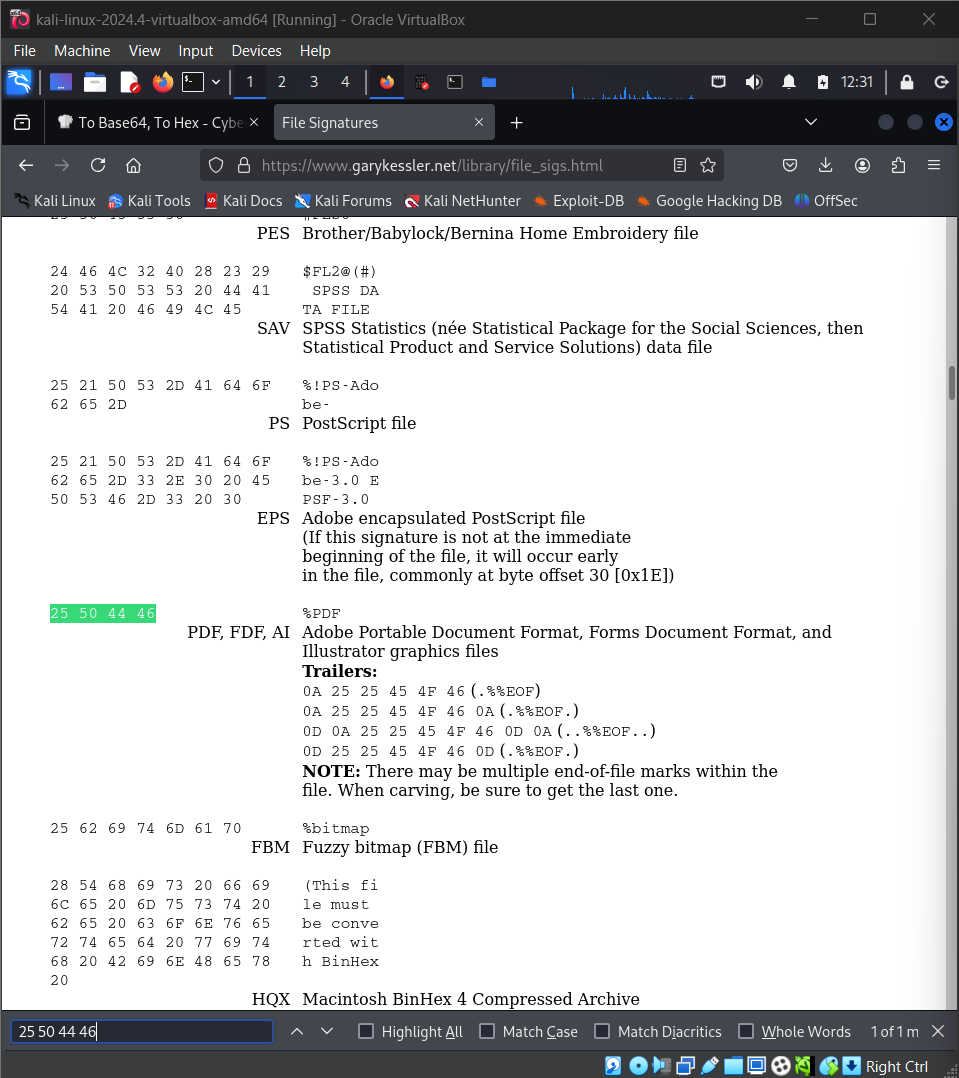
****

****

**Hex Value-Match**

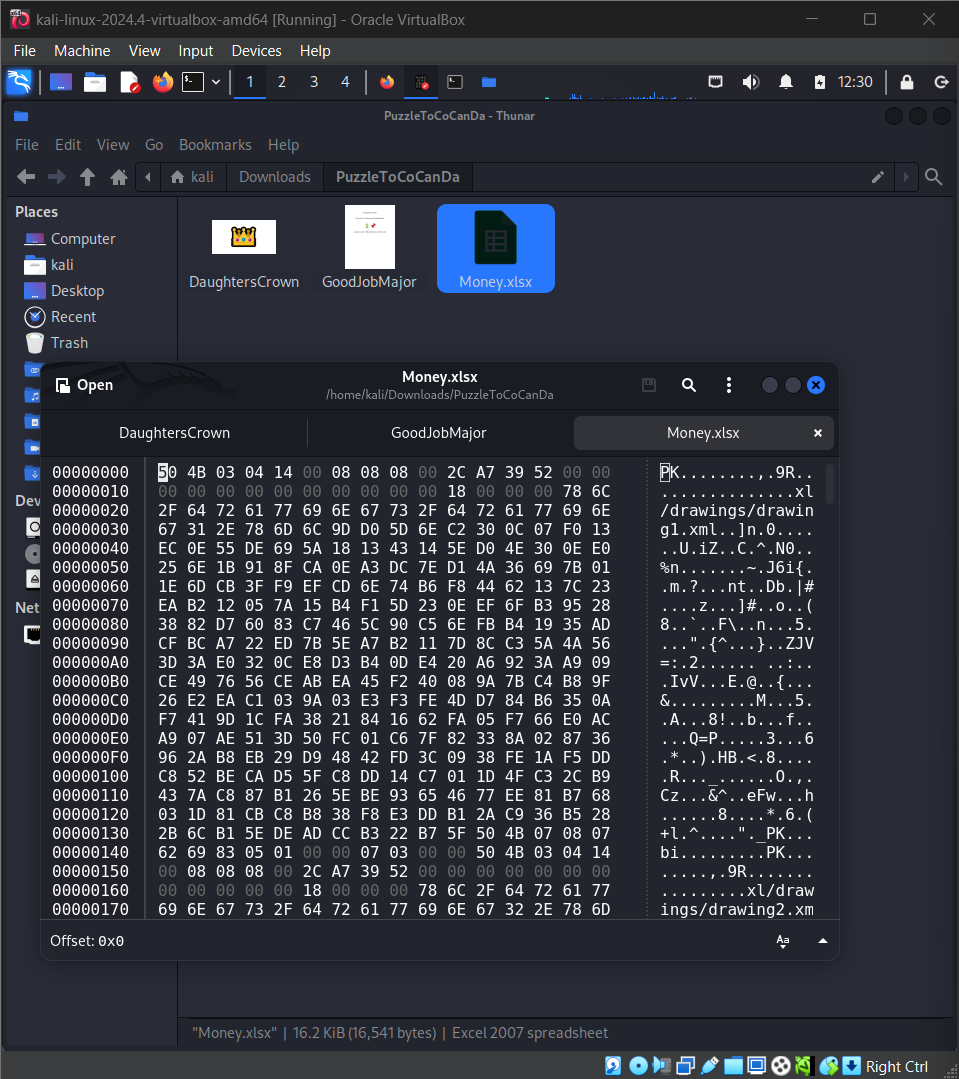
1. **GoodJobMajor**

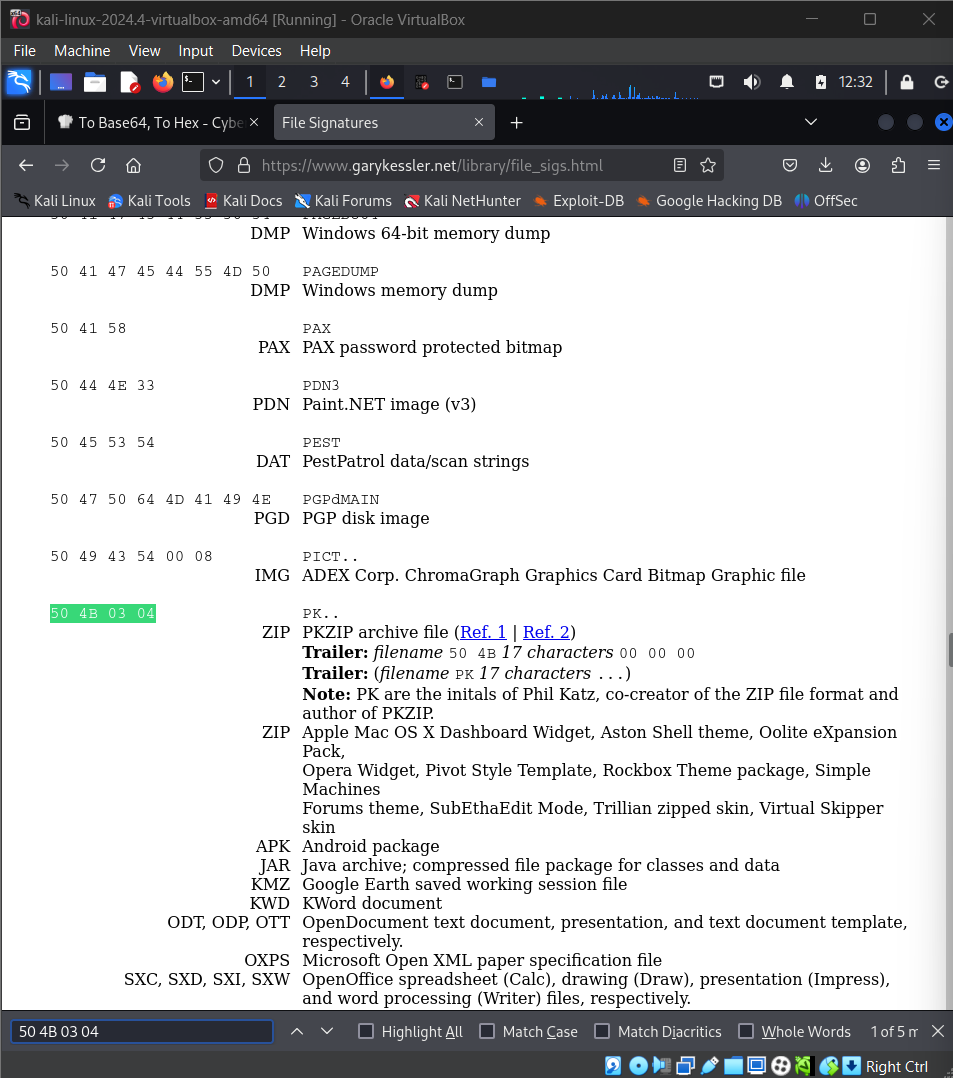
****

****

**Hex Value-Match**

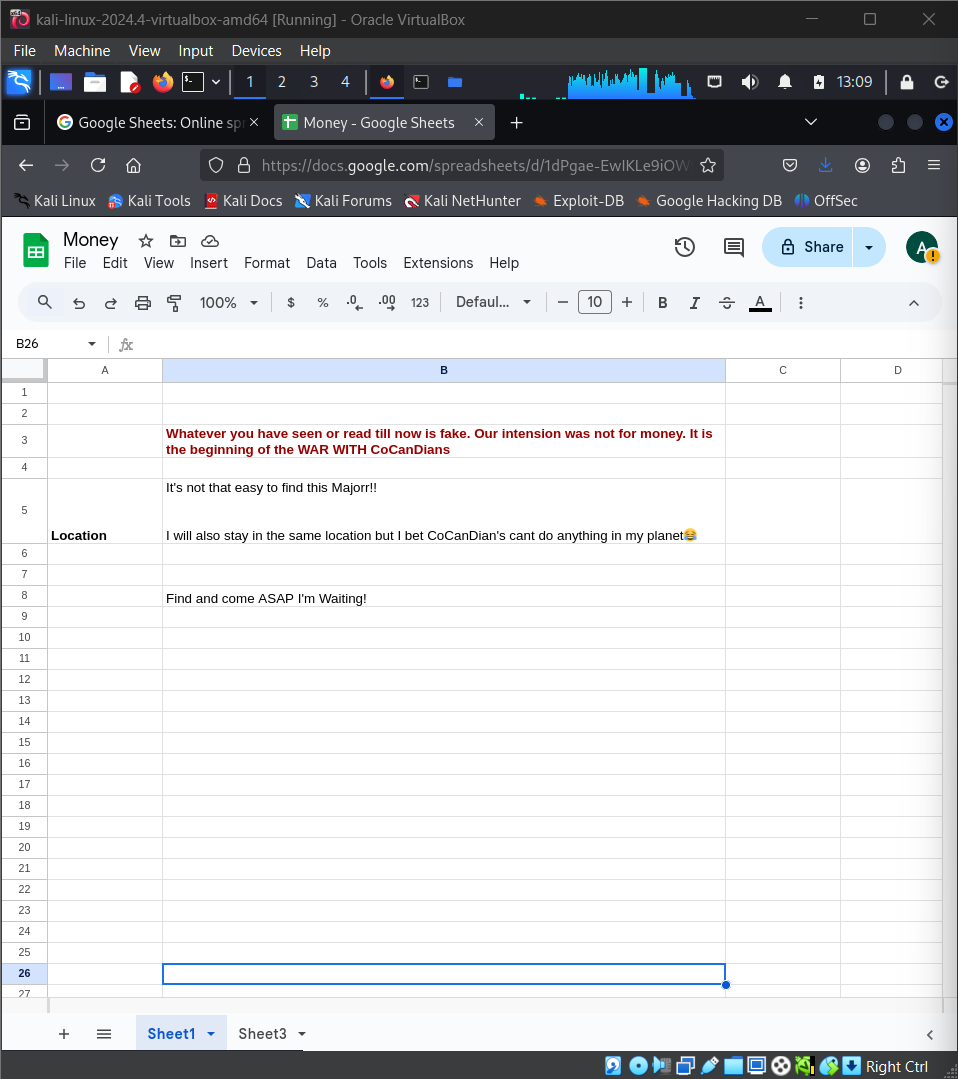
1. **Money.xlsx**

****

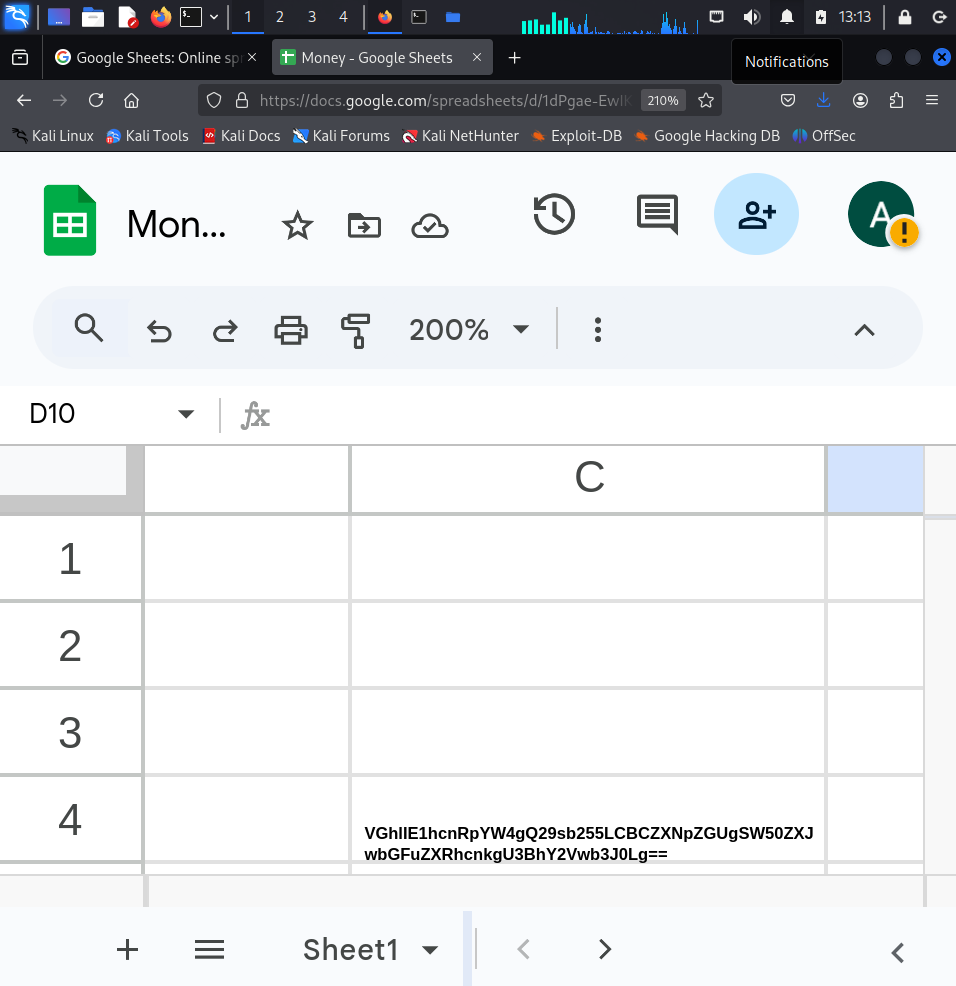
****

**Hex Value- MisMatch**

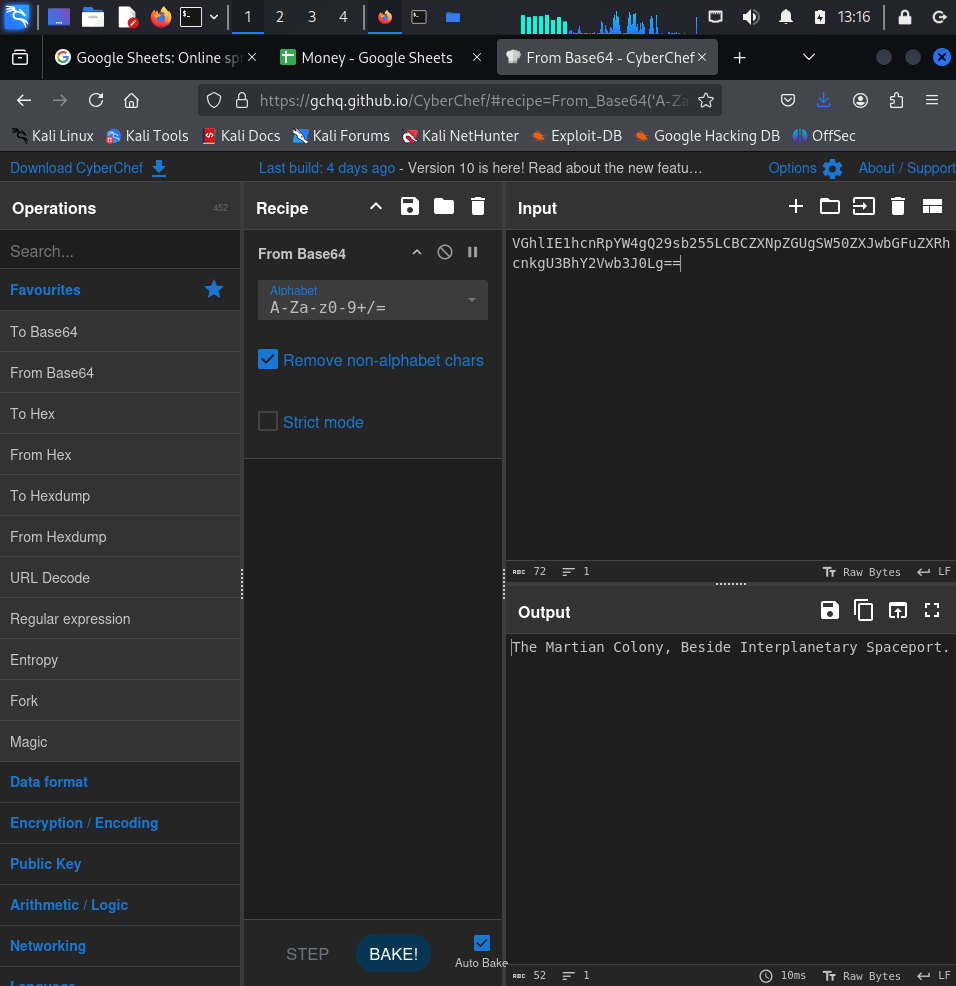
**Opening the Spreadsheet in google spreadsheet using fake gmail**

****

**Hidden Message found in Sheert 3**

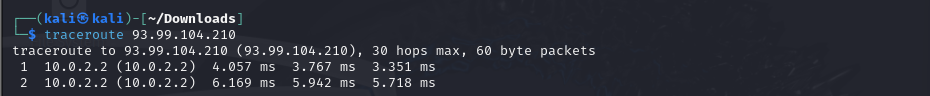
****

**Decoding it from base 64 Using Cyberchef- Found The Location**

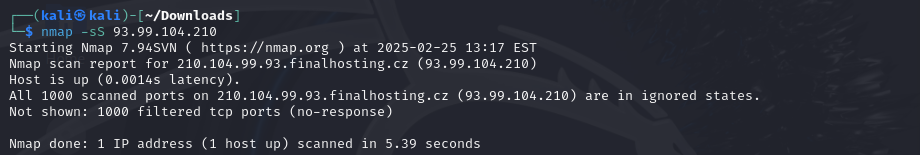
****

**Further Checking**

1. **traceout 93.99.104.210**

****

1. **nmap -sS 93.99.104.210**

****