# **Forensics**

Question

Graphical user interface, text, application, chat or text message

Description automatically generated

Solution

Text

Description automatically generated

The license appears to be base64 encoded data

Graphical user interface, text, application, email

Description automatically generated

So using an online base64 decoder gives the flag.

Question

Graphical user interface, text, application, email

Description automatically generated

Solution

As the question says, the dolls are placed inside one another, the file carving tool binwalk comes to mind

A screenshot of a computer

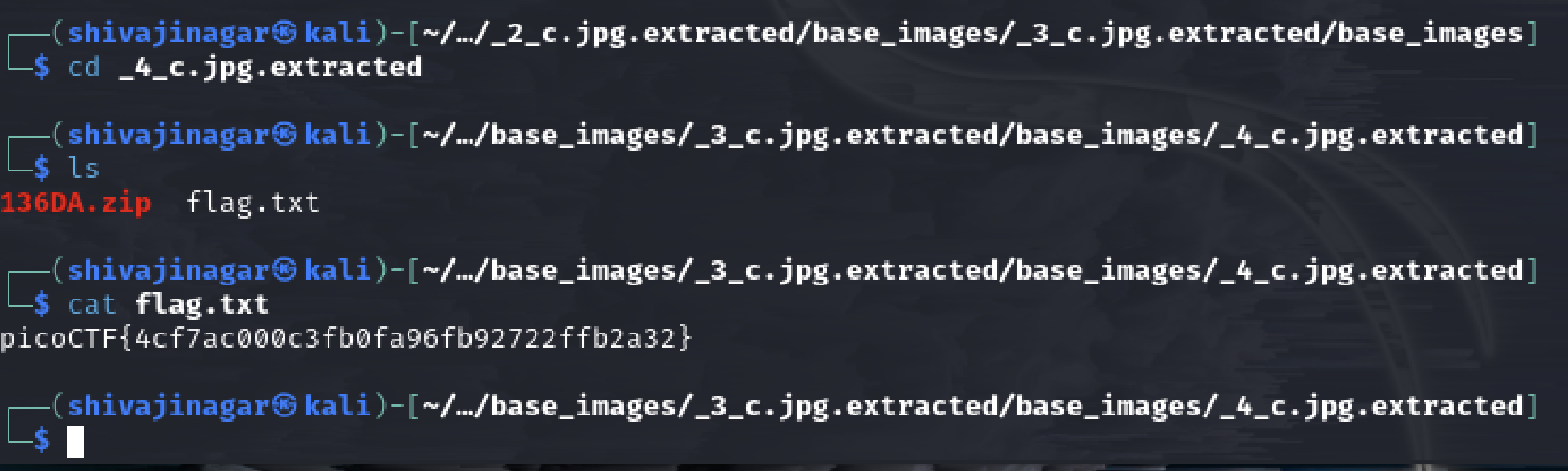
Description automatically generated with medium confidence

Using binwalk once, reveals a directory called \_dolls.jpg.extracted.

Text

Description automatically generated

Moving into this directory, we find another directory base\_images with another image 2\_c.jpg. Continuing the use of binwalk on these images until the flag is found, we have

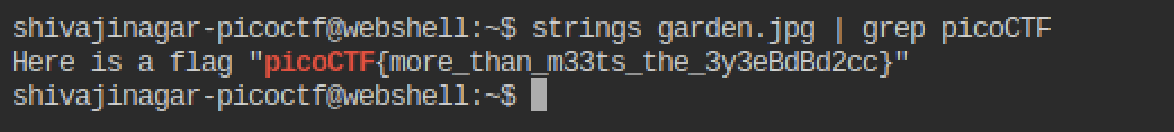
After several such iterations of using binwalk, we finally come across flag.txt and using cat, we have the flag.

Question

Graphical user interface, text, application, email, website

Description automatically generated

Solution



Using the strings command and using grep to look for picoCTF gives the flag.

Question

Graphical user interface, text, application

Description automatically generated

Solution

Graphical user interface

Description automatically generated

Using wireshark to trace the packets, we find a string which appears to be rot13 encoded. Using an online decoder for rot13, we get the flag. Graphical user interface, text, application

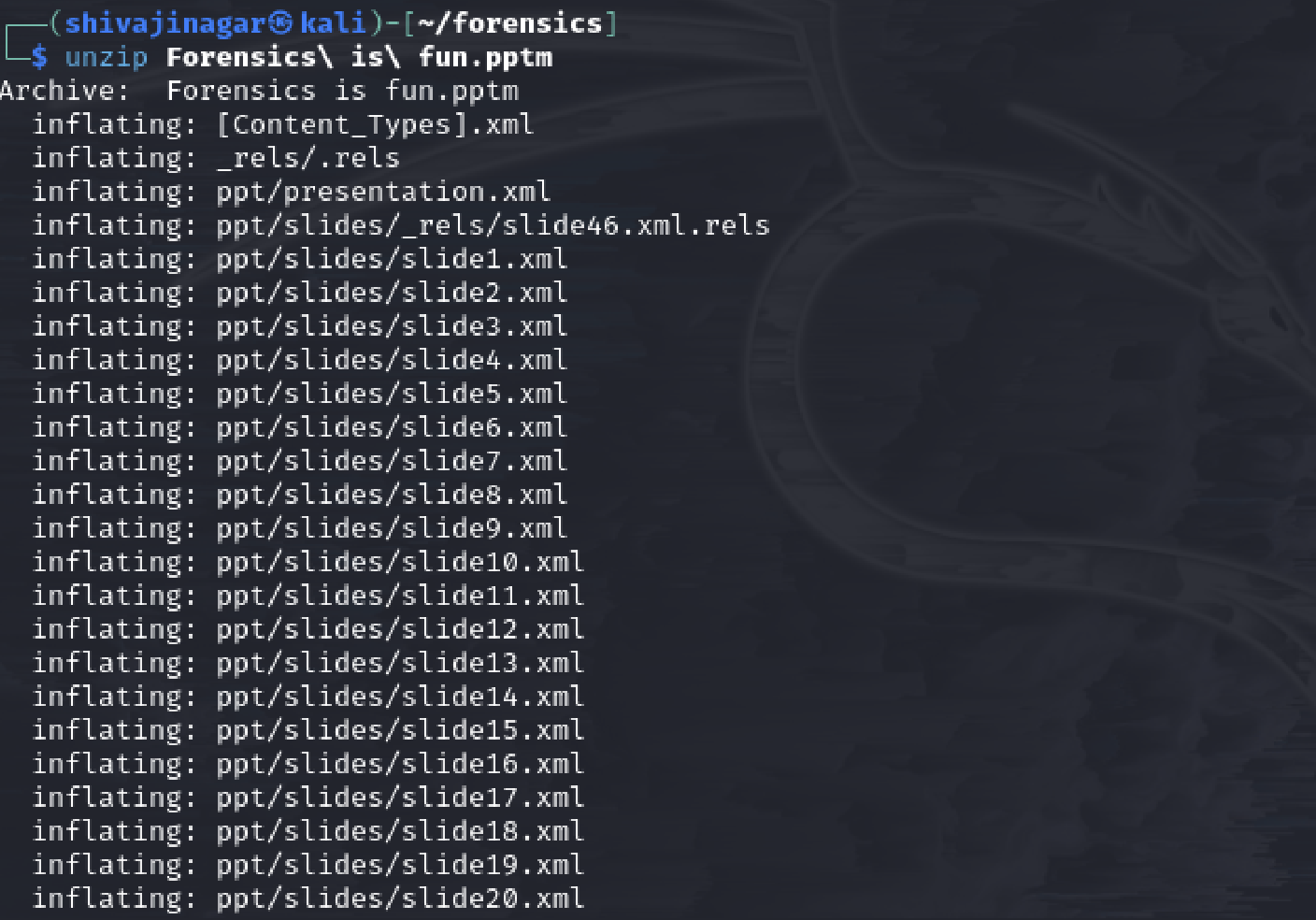
Description automatically generated

Question

Graphical user interface, text, application

Description automatically generated

Solution

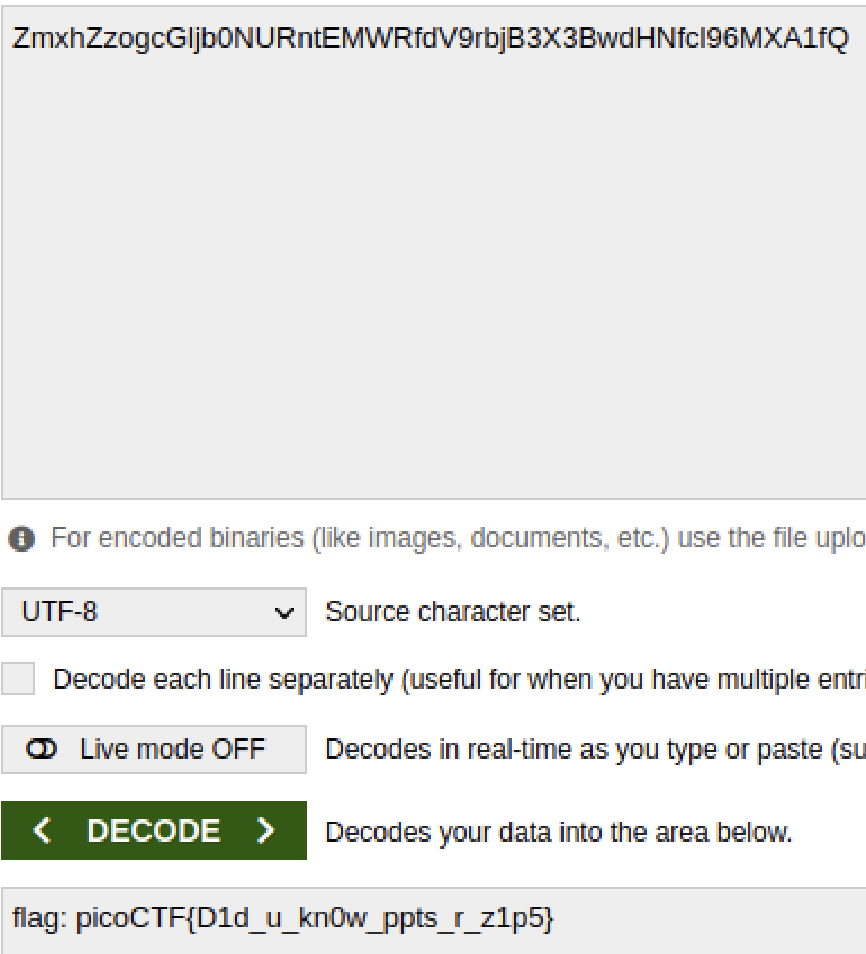


Using the unzip command to extract all files in the given archive, we have a list of files and directories. But one directory has a hidden file

Graphical user interface

Description automatically generated

We find a bunch of characters in the hidden file, which has uppercase, lowercase letters and numbers. So it could be base64 encoded.



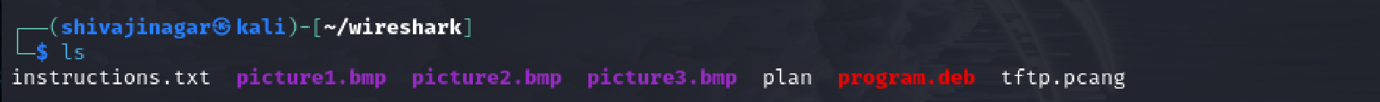
We find the flag using an online decoder.

Question

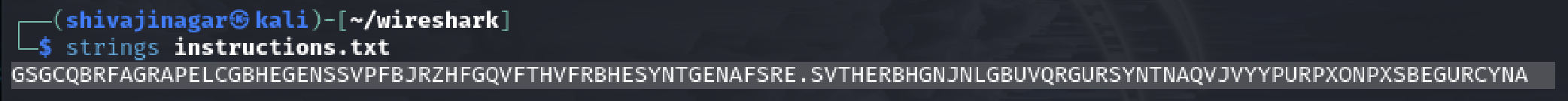
Graphical user interface, text, application

Description automatically generated

Solution



Using Wireshark and exporting objects of TFTP, we have the shown files in the directory.

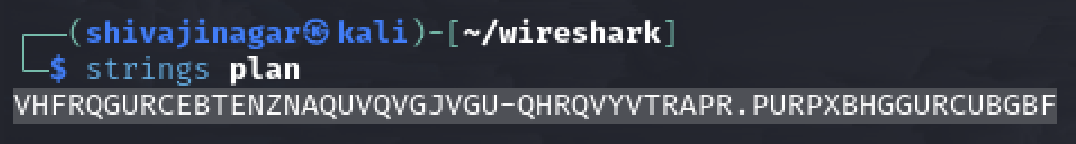


The strings in the file look like rot13 encoded so by decoding it and following the steps, we have –

Graphical user interface, text, application, email

Description automatically generated

It hints towards checking the plan file.



Using the rot13 decoder on the contents of the plan file,

Text

Description automatically generated

We come across this, and DUEDILIGENCE looks like the passphrase for the steghide tool. Not using it on the 3 images, we have –

Text

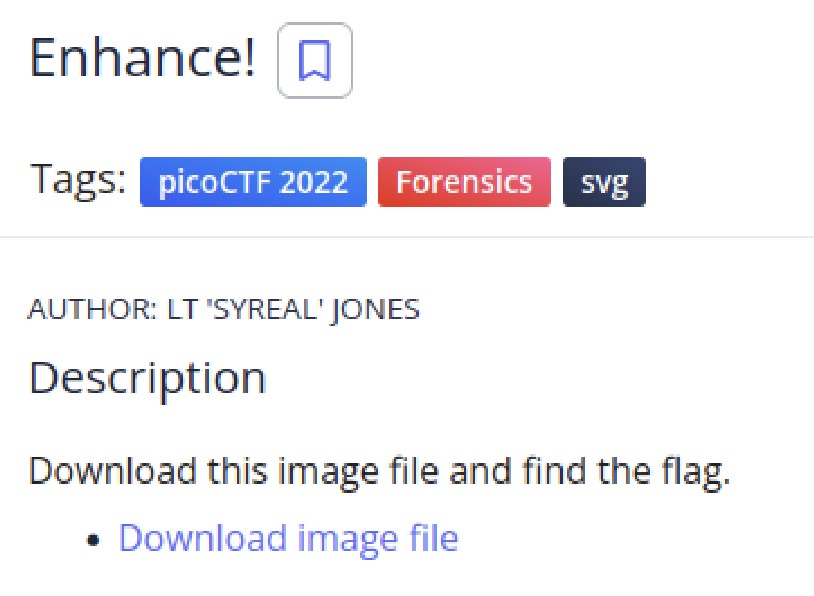
Description automatically generated

Graphical user interface, application, website

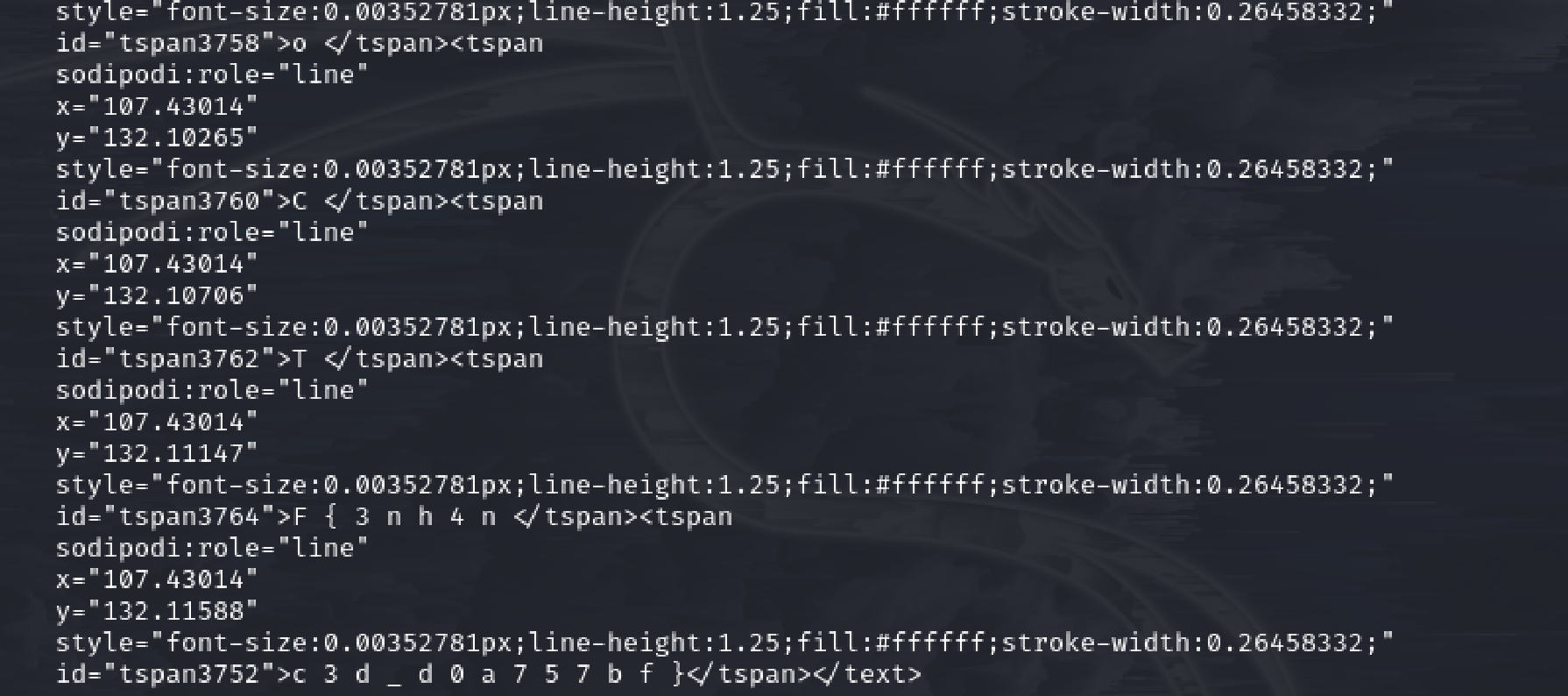
Description automatically generated

Looking at the flag.txt file, we come across the flag.

Question



Solution



Running the strings command on the file, we get the above result, but the interesting thing is that the contents in the tspans look like flags



Using grep to find the tspans, we end up with the flag.