CTF Event Name: UTCTF 2024
Category: Forensics
Name: Contracts
Flag: utflag{s1mple_w1z4rding_mist4k3s}

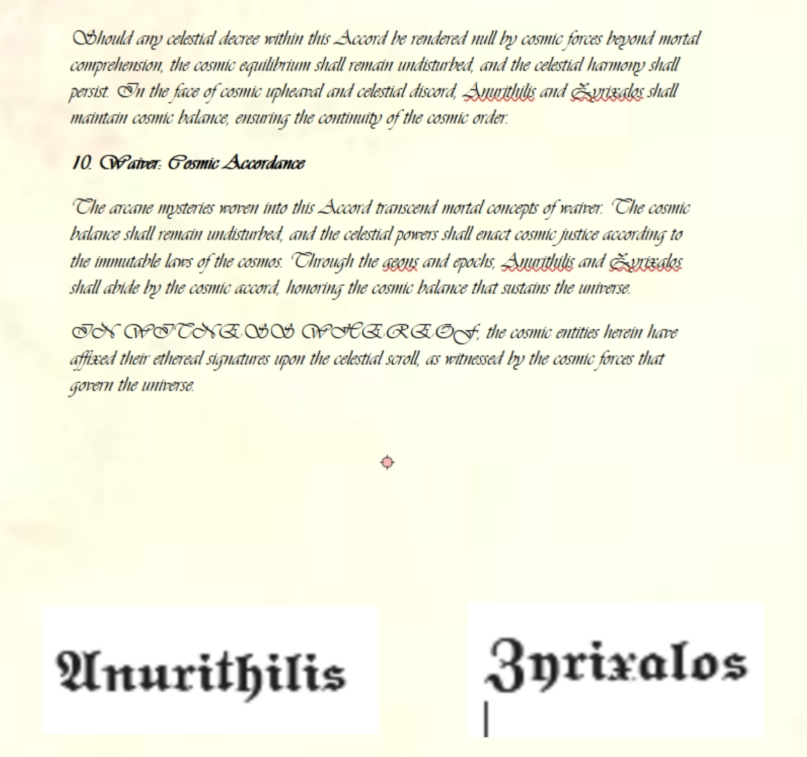
Challenge Description:

Magical contracts are hard. Occasionally, you sign with the flag instead of your name. It happens.
By Samintell (@samintell on discord)

Required Sources: contract.pdf

-----./Begin.Enumeration\.-----

We begin this challenge by acquiring a PDF file named “contract.pdf” to investigate. Lets open this file and see what we know. The file appears to be some form of a contract. At the end of the file we have two signature lines. This could indicate embedded images within the PDF file.



Should any celestial decree within this Accord be rendered null by cosmic forces beyond mortal comprehension, the cosmic equilibrium shall remain undisturbed, and the celestial harmony shall persist. In the face of cosmic upheaval and celestial discord, Anurithilis and Zyrixalos shall maintain cosmic balance, ensuring the continuity of the cosmic order.

10. Waiver: Cosmic Accordance

The arcane mysteries woven into this Accord transcend mortal concepts of waiver. The cosmic balance shall remain undisturbed, and the celestial powers shall enact cosmic justice according to the immutable laws of the cosmos. Through the aeons and epochs, Anurithilis and Zyrixalos shall abide by the cosmic accord, honoring the cosmic balance that sustains the universe.

IN WITNESS WHEREOF, the cosmic entities herein have affixed their ethereal signatures upon the celestial scroll, as witnessed by the cosmic forces that govern the universe.

Anurithilis Zyrixalos

Considering the hint “Occasionally, you sign with the flag instead of your name.” we need to extract all included files from within this PDF file and inspect them further for information or clues.

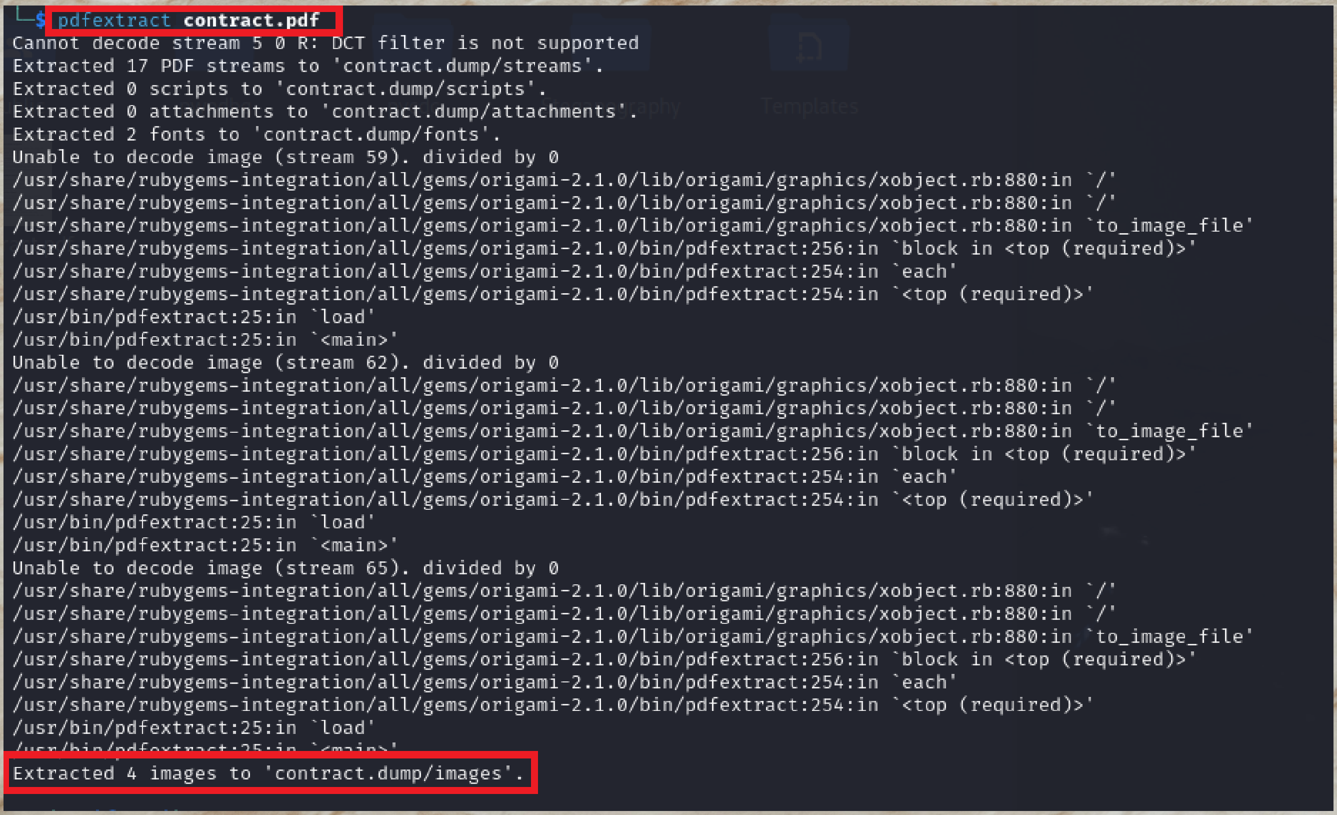
We will utilize a Linux command line tool called “pdfextract” for our file extraction process.

CLI Example Use: “pdfextract contract.pdf”

--It may be necessary for you to install this prior to extraction--

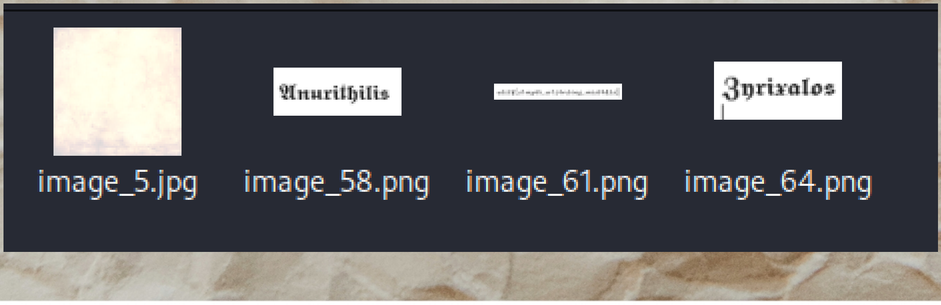
```
sudo apt-get update
sudo apt-get install pdfextract
```

After the extraction we get the following information:



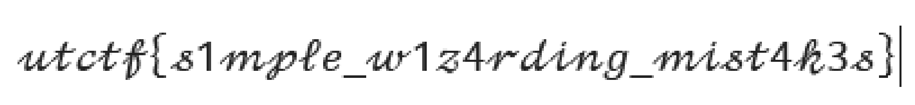
```
└─$ pdfextract contract.pdf
Cannot decode stream 5 0 R: DCT filter is not supported
Extracted 17 PDF streams to 'contract.dump/streams'.
Extracted 0 scripts to 'contract.dump/scripts'.
Extracted 0 attachments to 'contract.dump/attachments'.
Extracted 2 fonts to 'contract.dump/fonts'.
Unable to decode image (stream 59). divided by 0
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `/'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `/'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `to_image_file'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:256:in `block in <top (required)>'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:254:in `each'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:254:in `<top (required)>'
/usr/bin/pdfextract:25:in `load'
/usr/bin/pdfextract:25:in `<main>'
Unable to decode image (stream 62). divided by 0
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `/'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `/'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `to_image_file'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:256:in `block in <top (required)>'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:254:in `each'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:254:in `<top (required)>'
/usr/bin/pdfextract:25:in `load'
/usr/bin/pdfextract:25:in `<main>'
Unable to decode image (stream 65). divided by 0
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `/'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `/'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/lib/origami/graphics/xobject.rb:880:in `to_image_file'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:256:in `block in <top (required)>'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:254:in `each'
/usr/share/rubygems-integration/all/gems/origami-2.1.0/bin/pdfextract:254:in `<top (required)>'
/usr/bin/pdfextract:25:in `load'
/usr/bin/pdfextract:25:in `<main>'
Extracted 4 images to 'contract.dump/images'.
```

We have successfully extracted four images from the PDF file into a folder called “contract.dump”. Within this folder we will find the “images” folder. Lets locate this folder and inspect these images.



As we suspected this is what we are looking for. The “image_5.jpg” acts as the background for the PDF. Our signature images are “image_58.png” and “image_64.png”.

Our flag can now be read by opening “image_61.png”



utctf{s1mple_w1z4rding_mist4k3s}

-----./End.Enumeration\.-----