El Ingrediente Secreto

El reto comienza con la entrega de un archivo **PDF**. A simple vista parece un documento normal, pero al inspeccionar su encabezado con herramientas forenses se observa algo inusual.

```
┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1er-Edici-n/Crypto/El Ingrediente Secreto/Solucion]
└─$ xxd lemon.pdf | head -n 10
00000000: 504b 0304 1400 0000 0800 f33c 784b 5ff0  PK.........<xK_.
00000010: df4a 9ca2 0800 45a2 0800 0d00 1c00 5375  .J....E.......Su
00000020: 6e66 6c6f 7765 722e 7461 7255 5409 0003  nflower.tarUT...
00000030: 0a13 185a 0a13 185a 7578 0b00 0104 0000  ...Z...Zux......
00000040: 0000 0400 0000 0000 1680 e97f 1f8b 0800  ................
00000050: 0a13 185a 0003 d4b7 43b0 304c ecee 796c  ...Z....C.0L..yl
00000060: dbb6 6ddb b66d dbb6 6ddb efb1 6ddb b66d  ..m..m..m...m..m
00000070: 9ffb fdef 6aee 6666 7517 f3ab a49f 453a  ....j.ffu.....E:
00000080: 555d 59a4 1365 573b 331b 7b77 5327 3a07  U]Y..eW;3.{wS':.
00000090: 1333 80ff 3b30 fc07 1b0b cbff d6ff f83f  .3..;0.........?
```

El header del archivo inicia con: 50 4b 03 04. Este valor corresponde a la firma PK, característica de archivos ZIP, no de un PDF válido. Esto indica que el archivo fue disfrazado mediante la extensión. Renonbramos el archivo que contiene otro archivo.

El proceso se repite varias veces:

Se recibe un archivo con extensión PDF, se revisa el header (PK), se renombra a ZIP, se descomprime, aparece un nuevo archivo (PDF / TAR / ZIP) y se repite el análisis

En cada iteración, el archivo aparenta ser un PDF, pero su contenido real es otro formato comprimido.

Tras varias iteraciónaparece una nota que confirma que resolverlo manualmente no es la intención final, y que la solución correcta es automatizar el desempaquetado.

```
┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1er-Edici-n/Crypto/El Ingrediente Secreto/Solucion]
└─$ unzip Chili.zip
Archive:  Chili.zip
  inflating: Ugli.tar
 extracting: nota.txt

┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1er-Edici-n/Crypto/El Ingrediente Secreto/Solucion]
└─$ cat nota.txt
Muchas capas por delante. ¿Habrá alguna forma de automatizar este proceso?
```

Solución

```python
#!/usr/bin/env python3
import os
import zipfile
import tarfile


def extract_files():
```

```
while True:
files = os.listdir(".")
extracted = False

for f in files:
# ZIP
if f.endswith(".zip"):
print(f"[+] ZIP: {f}")
with zipfile.ZipFile(f, 'r') as z:
z.extractall()
os.remove(f)
extracted = True

# TAR
elif f.endswith(".tar"):
print(f"[+] TAR: {f}")
with tarfile.open(f, 'r') as t:
t.extractall()
os.remove(f)
extracted = True

# PDF camuflado como ZIP
elif f.endswith(".pdf"):
try:
os.rename(f, "temp.zip")
with zipfile.ZipFile("temp.zip", 'r') as z:
z.extractall()
os.remove("temp.zip")
extracted = True
except:
os.rename("temp.zip", f)

if not extracted:
print("[✓] Extracción finalizada")
break

if __name__ == "__main__":
extract_files()
```


THE FLAG IS:
TUTTI-FRUTTI21