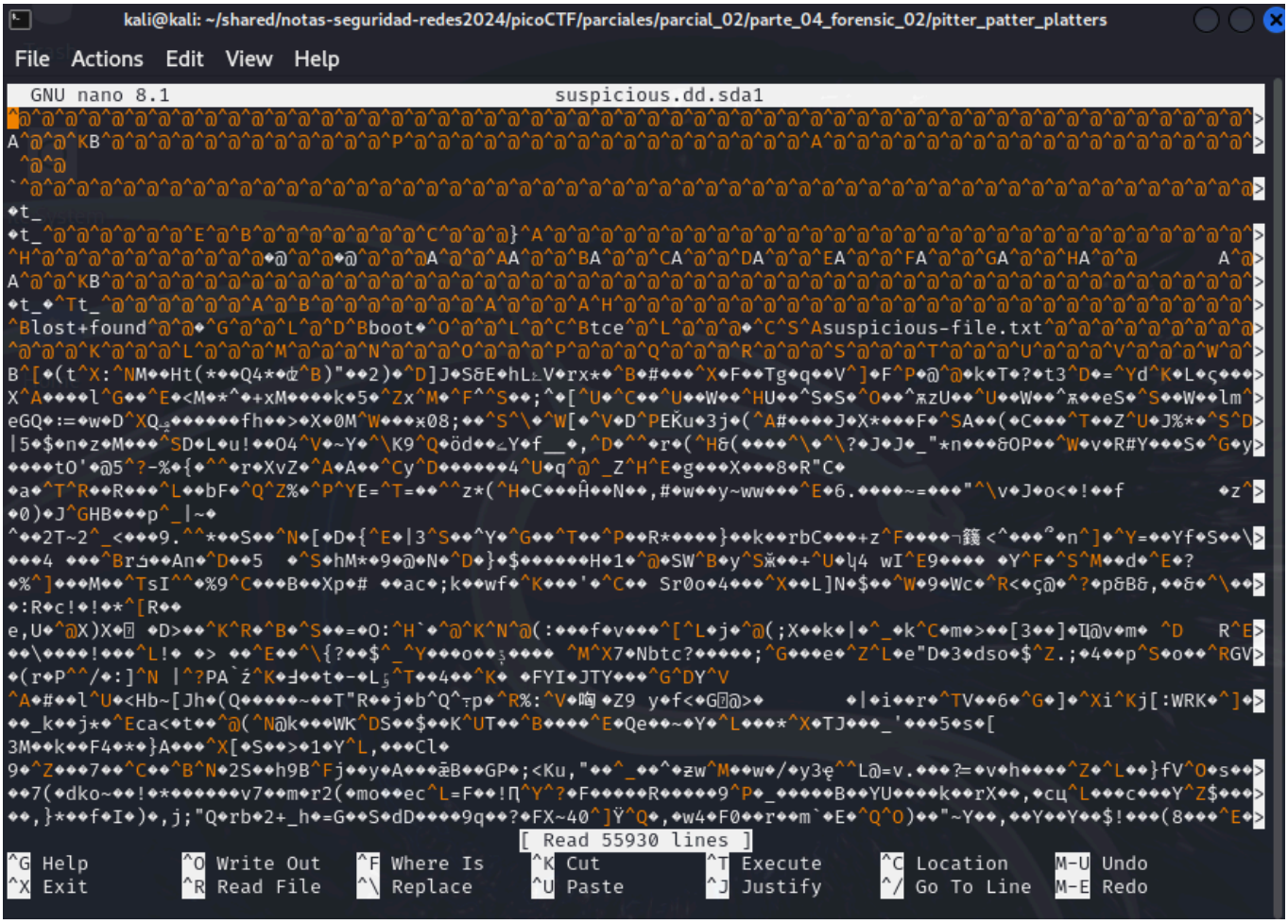
Description

'Suspicious' is written all over this disk image. Download suspicious.dd.sda1

Hints

- It may help to analyze this image in multiple ways: as a blob, and as an actual mounted disk.
- Have you heard of slack space? There is a certain set of tools that now come with Ubuntu that I'd recommend for examining that disk space phenomenon...

Solución



Al utilizar `NANO` se observa que no será fácilmente así que procedemos a:

```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/pitter_patter_platters]
└─$ strings -e b suspicious.dd.sda1
6b7d549b_3<_|Lm_111t5_3b{FTCocip
```

```
qQWTYUiIOPb
FGjJKLs
ZXvc
#+3;CScs
!1Aa
qQWTYUiIOPb
FGjJKLs
ZXvc
#+3;CScs
!1Aa
#+3;CScs
!1Aa
7777777777
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/pitter_patter_platters]
└─$ strings -e b suspicious.dd.sda1 | rev
picoCTF{b3_5t111_mL|_<3_b945d7b6
bPOIiUYTWQq
sLKJjGF
cvXZ
scSC;3+#
aA1!
bPOIiUYTWQq
sLKJjGF
cvXZ
scSC;3+#
aA1!
scSC;3+#
aA1!
7777777777
```

Bandera

```
flag: picoCTF{b3_5t111_mL|_<3_b945d7b6}
```

Notas Adicionales

El comando `strings -e b suspicious.dd.sda1 | rev` busca y extrae todas las cadenas de texto legibles en el archivo `suspicious.dd.sda1`, interpretando los bytes en formato big-endian (`-e b`), y luego invierte cada una de esas cadenas usando el comando `rev`. Esto puede ser útil para buscar texto legible que esté en un formato específico (como un archivo binario o un volcado de memoria) y detectar patrones o datos invertidos, como contraseñas o información codificada.

Referencias