CTF Challenge #6

▼ Operation: Blind Gallery

▼ Objective:

A disgruntled ex-employee of an art gallery is suspected of leaking confidential client records and auction details. All files found on their USB dump appear to be casual art resources—images, sketches, brochures. Yet something feels... off.

Your mission is to **identify what was exfiltrated**, **where it's hidden**, and **reveal the client list** if any.

▼ 🗂️ File Metadata

Title: Blind Gallery

Date Attempted: **Tuesday, 29 July, 2025**

Type: Steghide / Metadata / Red Herring

Analyst: Jinay *(a.k.a. **Jynx**)*

▼ 🛠️ Tools Used

→ `exiftool`

→ `steghide`

→ `strings`

→ `stat`

→

▼ 📄 Initial Files

File Name	Type	Size	Notes
`readme.txt`	TXT	142 byes	Contains Introduction to the Challenge.

```
┌──(kali㉿kali)-[~/Desktop/blindgallery]
└─$ cat readme.txt
Welcome to Blind Gallery CTF.

Objective: Find the final flag hidden in the blind spots of this gallery.

Some things are not what they seem.
```

```
┌──(kali㉿kali)-[~/Desktop/blindgallery]
└─$ exiftool readme.txt
ExifTool Version Number         : 13.25
File Name                       : readme.txt
Directory                       : .
File Size                       : 142 bytes
File Modification Date/Time     : 2025:07:29 11:59:24-04:00
File Access Date/Time           : 2025:07:29 11:30:45-04:00
File Inode Change Date/Time     : 2025:07:29 11:29:49-04:00
File Permissions                : -rw-r--r--
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Unix LF
Line Count                      : 5
Word Count                      : 25
```

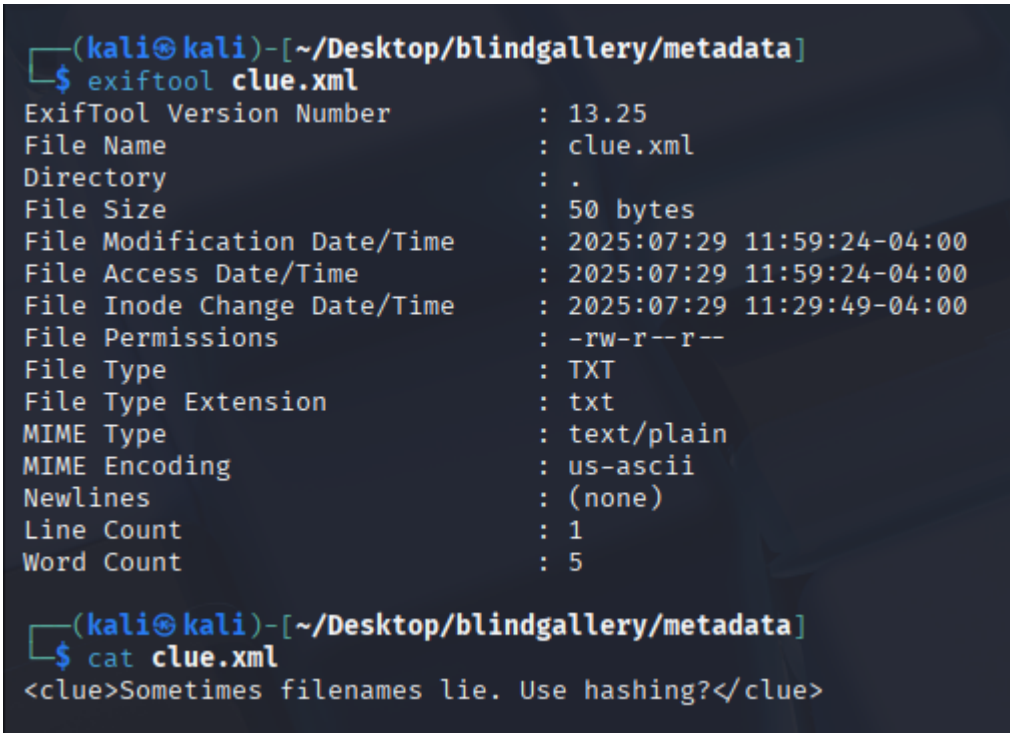
File Name	Type	Size	Notes
`secret_hidden_file.txt`	TXT	56 bytes	Contains text and a direct indication to an assured **RED HERRING** file, decoy yet again.

```
┌──(kali㉿kali)-[~/Desktop/blindgallery/gallery]
└─$ cat secret_hidden_file.txt
This is not the real flag.
But you're close.
Try image3.

┌──(kali㉿kali)-[~/Desktop/blindgallery/gallery]
└─$ file secret_hidden_file.txt
secret_hidden_file.txt: ASCII text

┌──(kali㉿kali)-[~/Desktop/blindgallery/gallery]
└─$ exiftool secret_hidden_file.txt
ExifTool Version Number         : 13.25
File Name                       : secret_hidden_file.txt
Directory                       : .
File Size                       : 56 bytes
File Modification Date/Time     : 2025:07:29 11:59:24-04:00
File Access Date/Time           : 2025:07:29 13:30:03-04:00
File Inode Change Date/Time     : 2025:07:29 11:29:49-04:00
File Permissions                : -rw-r--r--
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Unix LF
Line Count                      : 3
Word Count                      : 11
```

File Name	Type	Size	Notes
log1.txt	TXT	70 bytes	Contains text and a direct indication to an assured **RED HERRING** file- image3.jpg , instincts often don't lie no?

```
┌──(kali㉿kali)-[~/Desktop/blindgallery/logs]
└─$ ls -alh
total 12K
drwxrwxr-x 2 kali kali 4.0K Jul 29 11:29 .
drwxrwxr-x 7 kali kali 4.0K Jul 29 11:29 ..
-rw-r--r-- 1 kali kali   70 Jul 29 11:59 log1.txt

┌──(kali㉿kali)-[~/Desktop/blindgallery/logs]
└─$ cat log1.txt
User accessed image3.jpg at suspicious time.
Might be worth exploring.
```

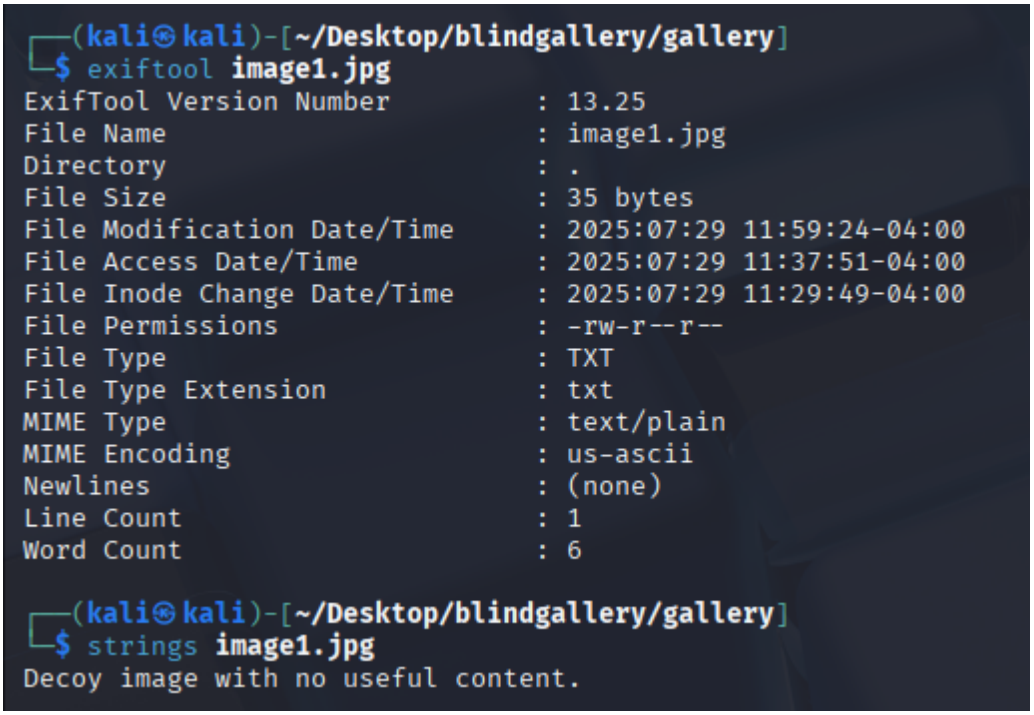
File Name	Type	Size	Notes
clue.xml	TXT	70 bytes	Is a .txt file pretending to be .xml, am I gonna investigate it further? If I had the liberty of time maybe? Right now absolutely not- I did not find one hashed code or encrypted text worth hammering over. **DECOY**- Classic Red Herring.



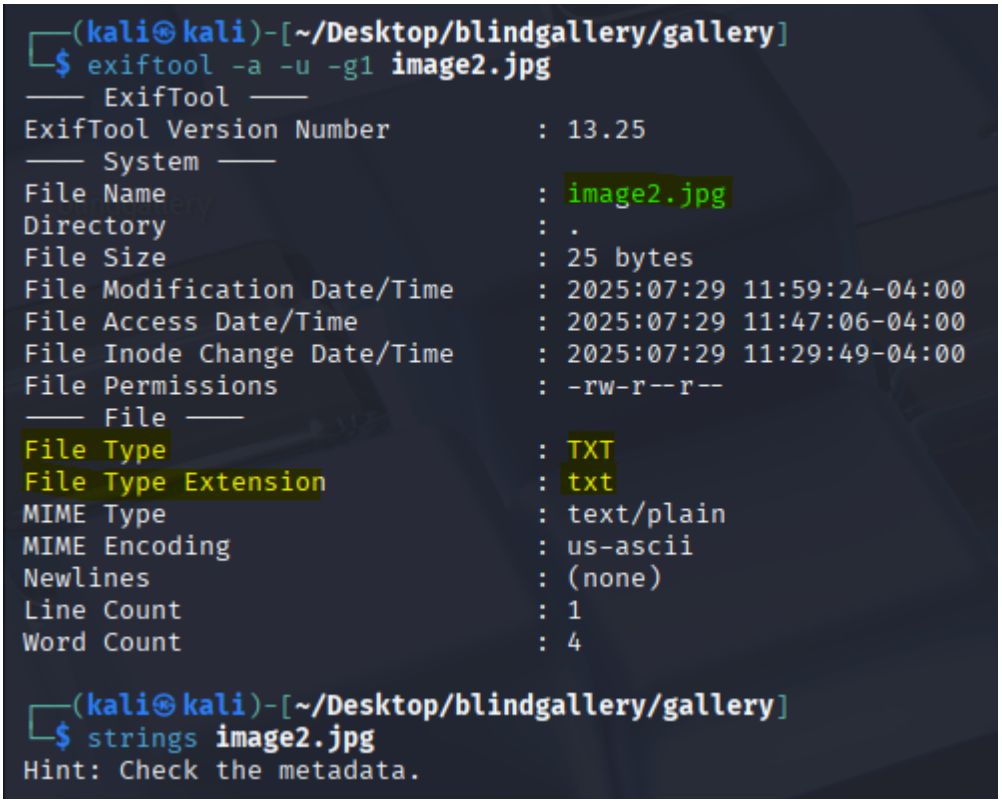
▼ 💾Analysis & Observations

File Name	Type	Size	Notes
image1.jpg	JPG	35 bytes	Its a decoy file apparently, although not trustable in a CTF context but sure ill let it pass- since its a .txt file

File Name	Type	Size	Notes
			disguised as `.jpg`. It is instinctive but I think it is indeed actually a decoy.



File Name	Type	Size	Notes
image2.jpg	TXT	25 bytes	Its a decoy file apparently, **RED HERRING** OF SORTS- the file is named to pretend as a `.jpg` extension file but is actually a `.txt` file.



File Name	Type	Size	Notes
image3.jpg	TXT	54 bytes	Same pattern .jpg file pretending to be a .txt file- there are no images/pixels to look at its trying to deceive- most apparent **RED HERRING** sequence of files. **CLASSIC**.

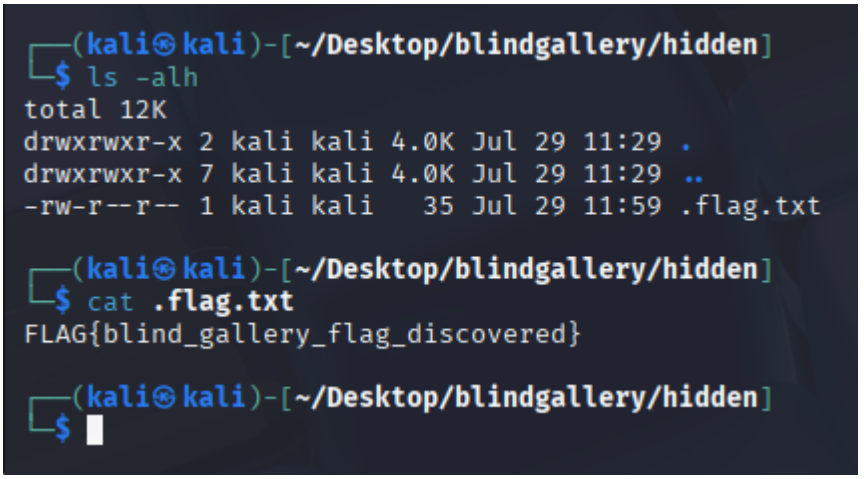
```
┌──(kali㉿kali)-[~/Desktop/blindgallery/gallery]
└─$ exiftool -a -u -g1 image3.jpg
---- ExifTool ----
ExifTool Version Number         : 13.25
---- System ----
File Name                       : image3.jpg
Directory                       : .
File Size                       : 54 bytes
File Modification Date/Time     : 2025:07:29 11:59:24-04:00
File Access Date/Time           : 2025:07:29 11:59:24-04:00
File Inode Change Date/Time     : 2025:07:29 11:29:49-04:00
File Permissions                : -rw-r--r--
---- File ----
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Unix LF
Line Count                      : 2
Word Count                      : 10

┌──(kali㉿kali)-[~/Desktop/blindgallery/gallery]
└─$ strings image3.jpg
Another decoy, or is it?
Try looking under the pixels.
```

▼ 🧩 Final Flag(s)

File Name	PATH	Notes
fakeflag.txt	~/Desktop/blindgallery/decoys	FLAG{not_this_one}

```
┌──(kali㉿kali)-[~/Desktop/blindgallery/decoys]
└─$ cat fakeflag.txt
FLAG{not_this_one}
```

File Name	PATH	Notes
.flag.txt	~/Desktop/blindgallery/hidden	FLAG{blind_gallery_flag_discovered}



💡 interesting how sometimes the exact directory lays out what to do `ls -a` [to see hidden files] directory is namely hidden or indication towards hidden file and the flag is right in sight but you might miss out for one simple option extended at the end.
