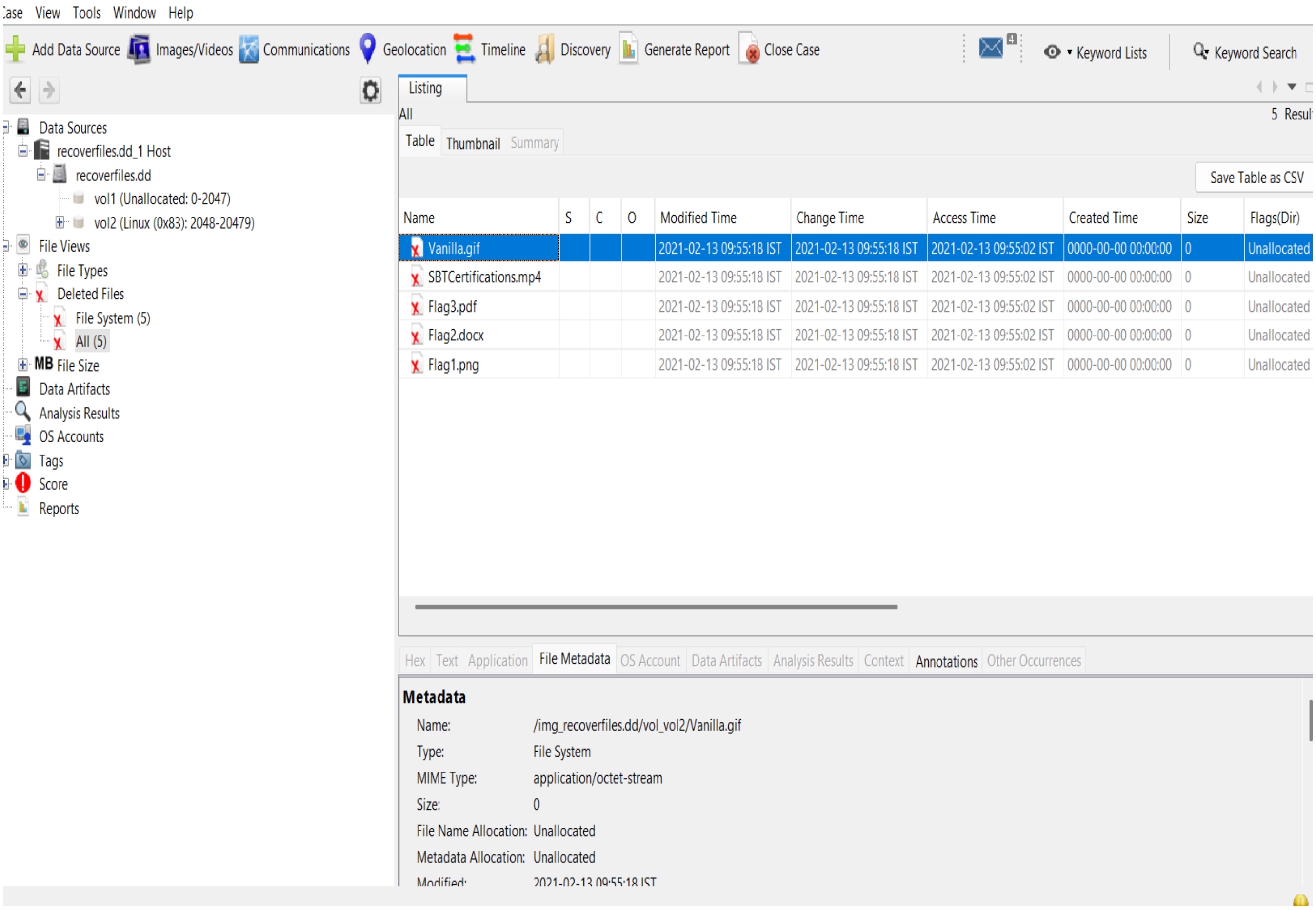
Employee of the Year Challenge Report

Scenario

John, an employee at FakeCompany Ltd., received the "Best Employee of the Year" award for his hard work. Unfortunately, he deleted some important files. Your task is to recover the deleted files and capture all the flags contained within.

Recovered Files

- The challenge provided a disk image or files where deleted files were recovered.
- **Tools Used**: **Autopsy** (digital forensics tool) and **QPhotoRec** (file recovery tool).
- Analyzed various file types like images, DOCX files, and others.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Vanilla.gif				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
SBTCertifications.mp4				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
Flag3.pdf				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
Flag2.docx				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
Flag1.png				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated

Metadata

Name:	/img_recoverfiles.dd/vol_vol2/Vanilla.gif
Type:	File System
MIME Type:	application/octet-stream
Size:	0
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2021-02-13 09:55:18 IST

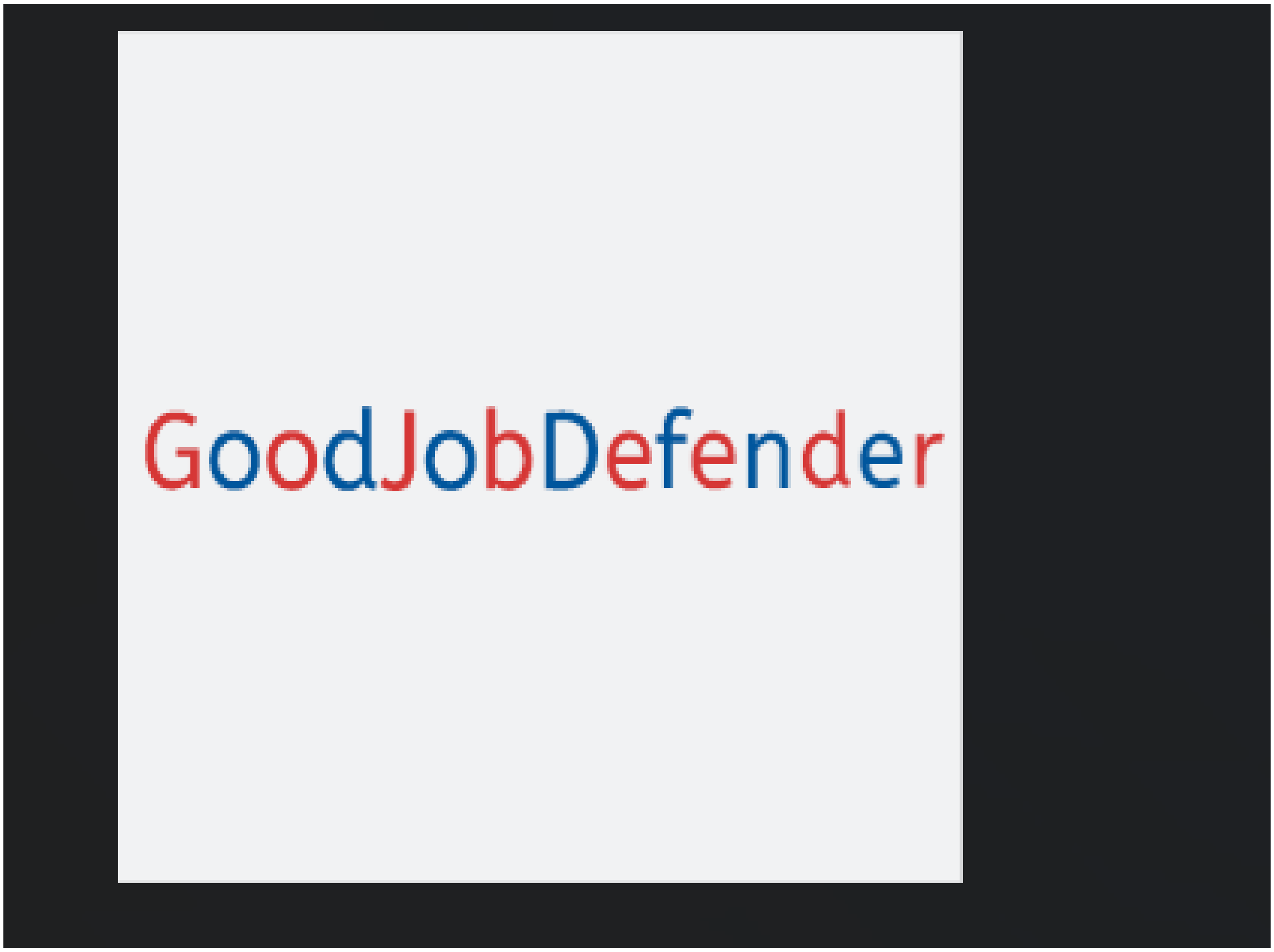
Flag 1:

→ ***File Name****:FLAG1 (Recovered from Autopsy.)*

→ ***Text from recovered GIF image****:*

→ ***Answer****: Goodjobdefender*

→ ***Source****:* ***Autopsy*** *(forensic tool) and* **QPhotoRec** *(image recovery).*

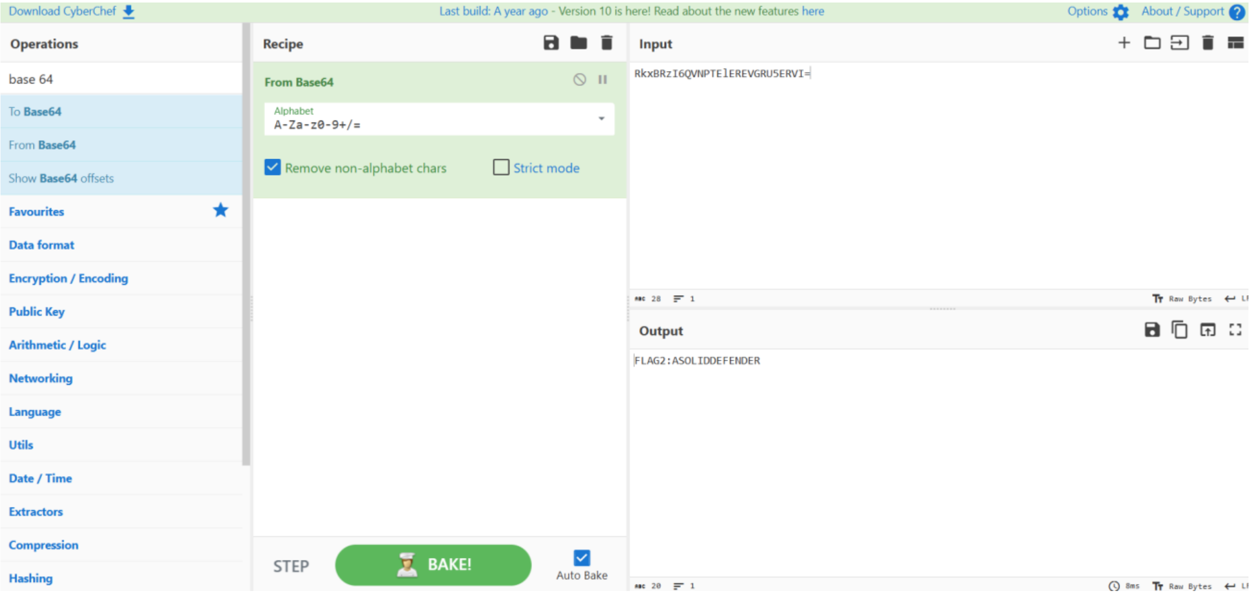


GoodJobDefender

Flag 2:

- ***File****: DOCX file containing the encoded flag.*

- ***Decoded Flag***:
  - ***Answer***: *ASOLIDDEFENDER*
- ***Method***: *Used* ***CyberChef*** *(online tool) to decode the Base64 encoded string.*
- ***Source***: ***CyberChef*** *(for decoding Base64 string).*



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

```
RkxBRzI6QVNPTElEREVGRU5ERVI=
```

28 1

```
FLAG2:ASOLIDDEFENDER
```

20 1

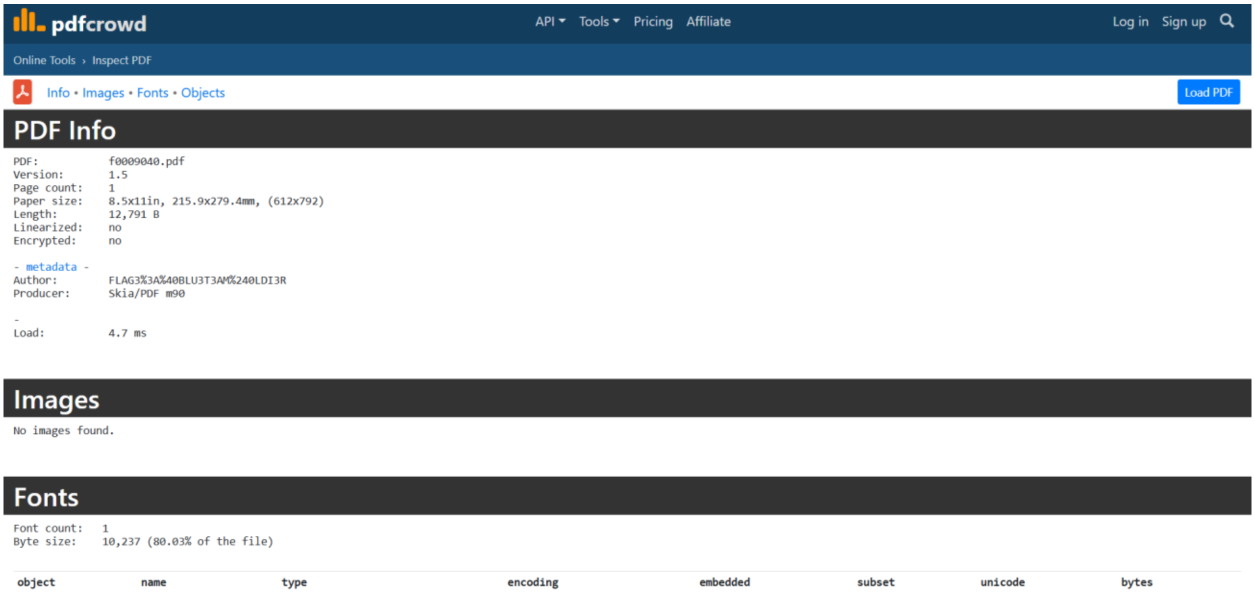
Flag 3:

- *File: PDF file recovered during the challenge.*
- *Decoded Flag:*

  - ○ *Answer: FLAG3@BLU3T3AM$OLDI3R*
- *Method: Used **PDFCrowd** (online tool) to analyze the PDF and retrieve the flag.*
- *Source: **PDFCrowd** (for inspecting PDF content).*

Nice Work

Find Flag3



PDF Info

```
PDF:          f0009040.pdf
Version:      1.5
Page count:   1
Paper size:   8.5x11in, 215.9x279.4mm, (612x792)
Length:       12,791 B
Linearized:   no
Encrypted:    no

- metadata -
Author:       FLAG3%3A%40BLU3T3AM%240LDI3R
Producer:     Skia/PDF m90

-
Load:         4.7 ms
```

Images

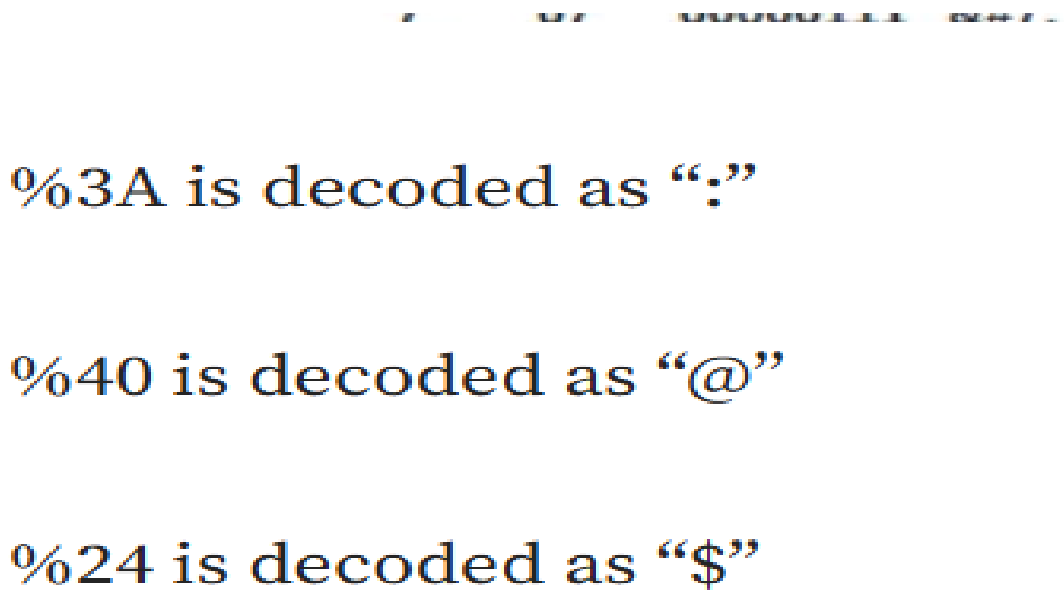
```
No images found.
```

Fonts

```
Font count:  1
Byte size:   10,237 (80.03% of the file)
```

object	name	type	encoding	embedded	subset	unicode	bytes

- *I have to use ACSII to decode the Answer*



%3A is decoded as ":"

%40 is decoded as "@"

%24 is decoded as "$"

Filesystem Analysis:

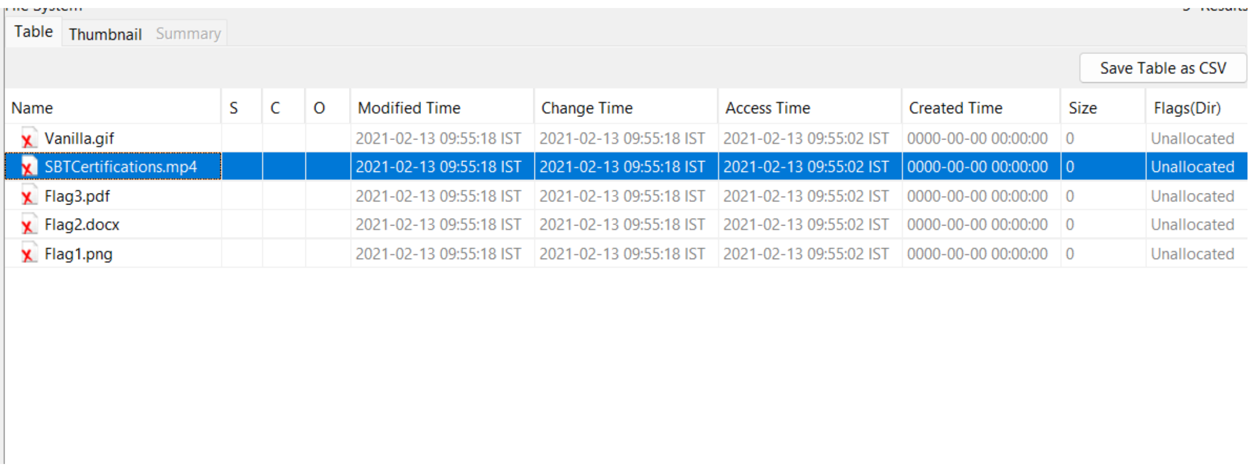
- ***Question**: What is the filesystem of the provided disk image?*
- ***Answer**: ext4*
- ***Source**: **Autopsy** (for analyzing the disk image).*

THE FILE EXTENSION WAS IN DELETED FILE WHICH LATER ON I RECOVERED BY USING AUTOPSY

UNFORTUNATELY I FORGET TO TAKE THE SCREEN SHORT OF THE EXTENSION OF FILE

Recovered MP4 File:

- ***Question**: What is the original filename of the recovered MP4 file?*
- ***Answer**: SBTCertifications.mp4*
- ***Source**: **Autopsy** (file name found during analysis).₩*



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Vanilla.gif				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
SBTCertifications.mp4				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
Flag3.pdf				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
Flag2.docx				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated
Flag1.png				2021-02-13 09:55:18 IST	2021-02-13 09:55:18 IST	2021-02-13 09:55:02 IST	0000-00-00 00:00:00	0	Unallocated

- Here i remember to take the screen short of the mp3 file and i dont need to analyze it

- NOTE: i have used window os so i have to use online tools too

Tools Used

- ***Autopsy****: A digital forensics tool used for analyzing disk images and recovering deleted files.*
- ***QPhotoRec****: A tool used for recovering lost files from different file systems.*
- ***CyberChef****: An online tool used to decode Base64 encoded strings.*

- ***PDFCrowd***: *An online tool for analyzing PDF files and extracting hidden content.*

Conclusion

*The challenge was successfully completed by recovering deleted files and identifying flags through a forensic investigation. The tools used—**Autopsy**, **QPhotoRec**, **CyberChef**, and **PDFCrowd**—were essential in the recovery and analysis process.*

AUTOPSY
DIGITAL FORENSICS

CyberChef
FOR SECURITY ANALYSTS