TryHackMe

Digital Footprint Challenge

OSINT Investigation Writeup

Platform	TryHackMe
Challenge Name	Digital Footprint
Category	OSINT (Open Source Intelligence)
Difficulty	Easy
Date Completed	February 11, 2026
Author	DragonByte

Executive Summary

This OSINT challenge involved investigating ACME Jet Solutions' claimed founding date and analysing metadata from leaked internal documents to identify the document author. Through the use of archival research and metadata extraction, I successfully verified discrepancies in the company's timeline and identified the document creator.

Objectives

- ✅ Locate the residential property linked to ACME Jet's early operations
- ✅ Verify ACME Jet Solutions' founding date
- ✅ Identify the landmark connected to the company's international expansion
- ✅ Find information about the individual maintaining ACME Jet's systems

Tools & Techniques Used

Tool/Method	Purpose
Image Metadata Analysis	Extract GPS coordinates from images
Google Maps	Geolocation and street view analysis
Internet Archive (Wayback Machine)	Historical website snapshots
PowerShell	Document metadata extraction
XML Parsing	Reading OpenDocument metadata
Reverse Image Search	Identify landmarks and locations
OSINT Frameworks	Social media and public records research

Task 1: The Leaked Photo

Objective

An ACME Jet Solutions employee uploaded a photo of a residential property believed to be linked to ACME Jet's early operations. Can you figure out where the picture was taken to confirm or debunk the rumour?

Approach

Analyze Image for Visual Indicators

- Noted a plaque**: "Rectory"**
- Noted ADT Armed Response Sign (Known South African Private Security Company)
- Noted Exterior features:
  - Red Tiled Roof (Terracotta)
  - Beige Exterior Low Walls With White Caps
  - Wooden Gate
  - 2 Potential Chimneys
  - Mediterranean/Spanish Style Architecture
- Likely Located Within an Upper-Class Neighbourhood

Dissection of Visual Indicators

Rectory Plaque Analysis:

- What is a rectory?

rectory noun

rec·to·ry ˈrek-t(ə-)rē

plural **rectories**

Synonyms of *rectory* >

1 : a benefice held by a rector

2 : a residence of a rector or a parish priest

  - Could be indicative of the residence being located near sites of religious practice/gathering

- Reverse image search returned no property listings, information or addresses tied to the property
- Further searches showed that Rectories often are kept as heritage/historical sites
  - Searched through SAHRA (South African Heritage Resources Agency) for a similar property
    - **No match found**

- Searched Social Media Sites (Facebook/Instagram) using #tags (#Rectory, #RectorySA, #RectorySouthAfrica, etc.)
    - **No match found**

- Queried local property agency websites for listings using Rectory

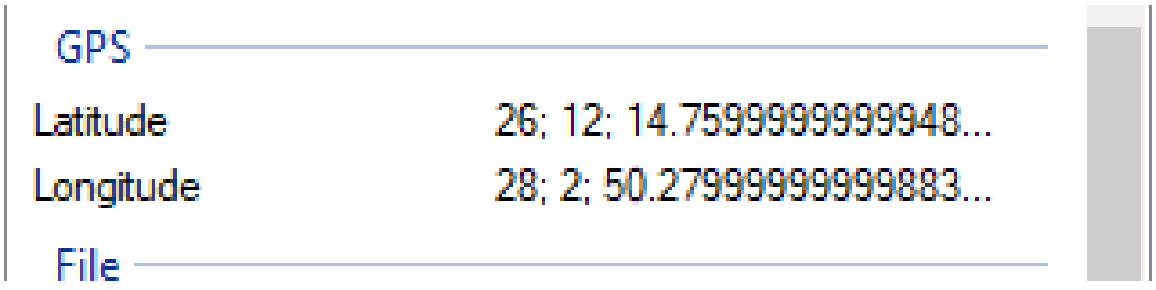
    - **No match found**

Image Metadata Evaluation

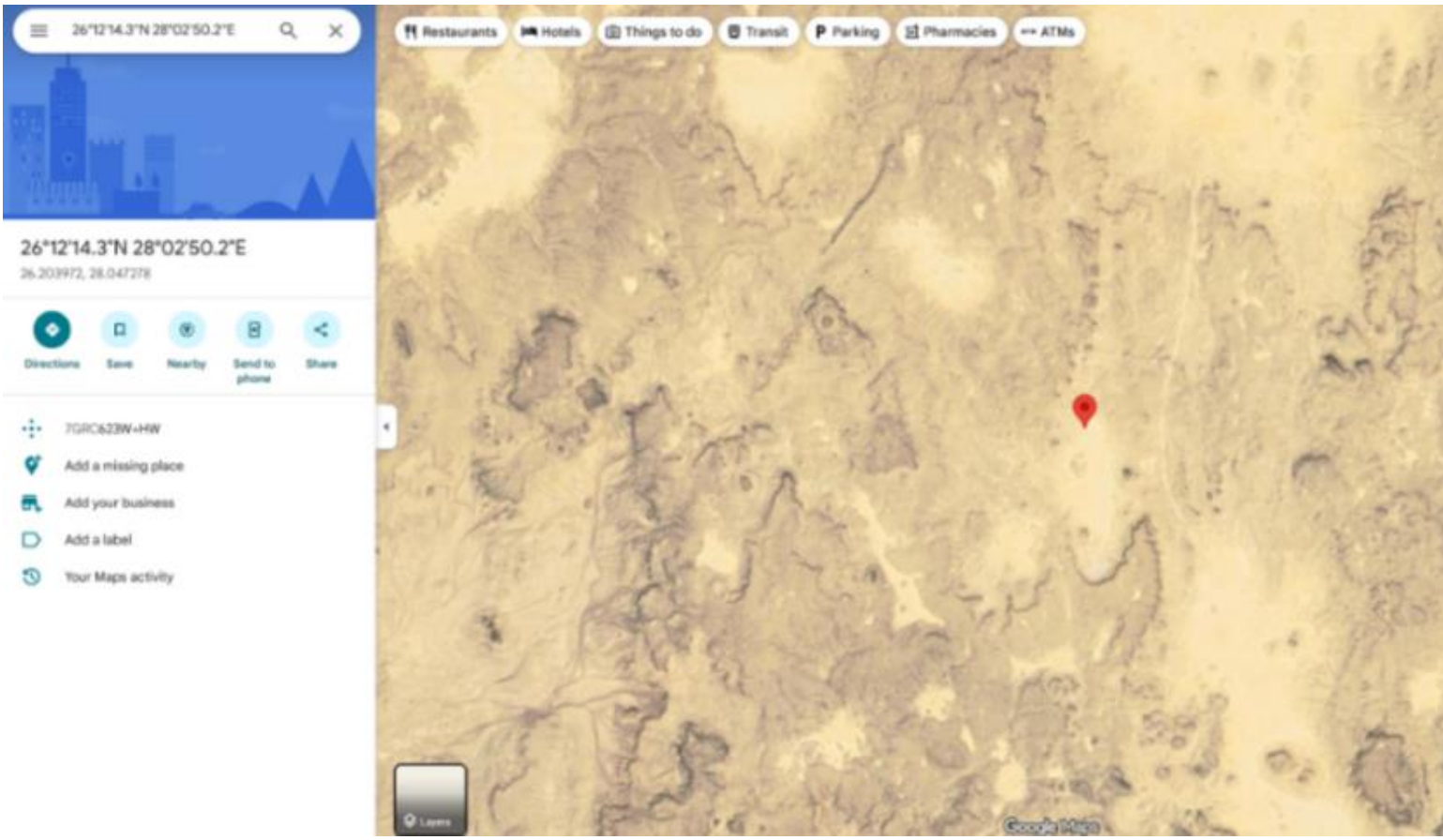
Extracted metadata from image properties revealed GPS coordinates.

First Attempt - Windows Properties:

- LAT/LONG Coordinates Found

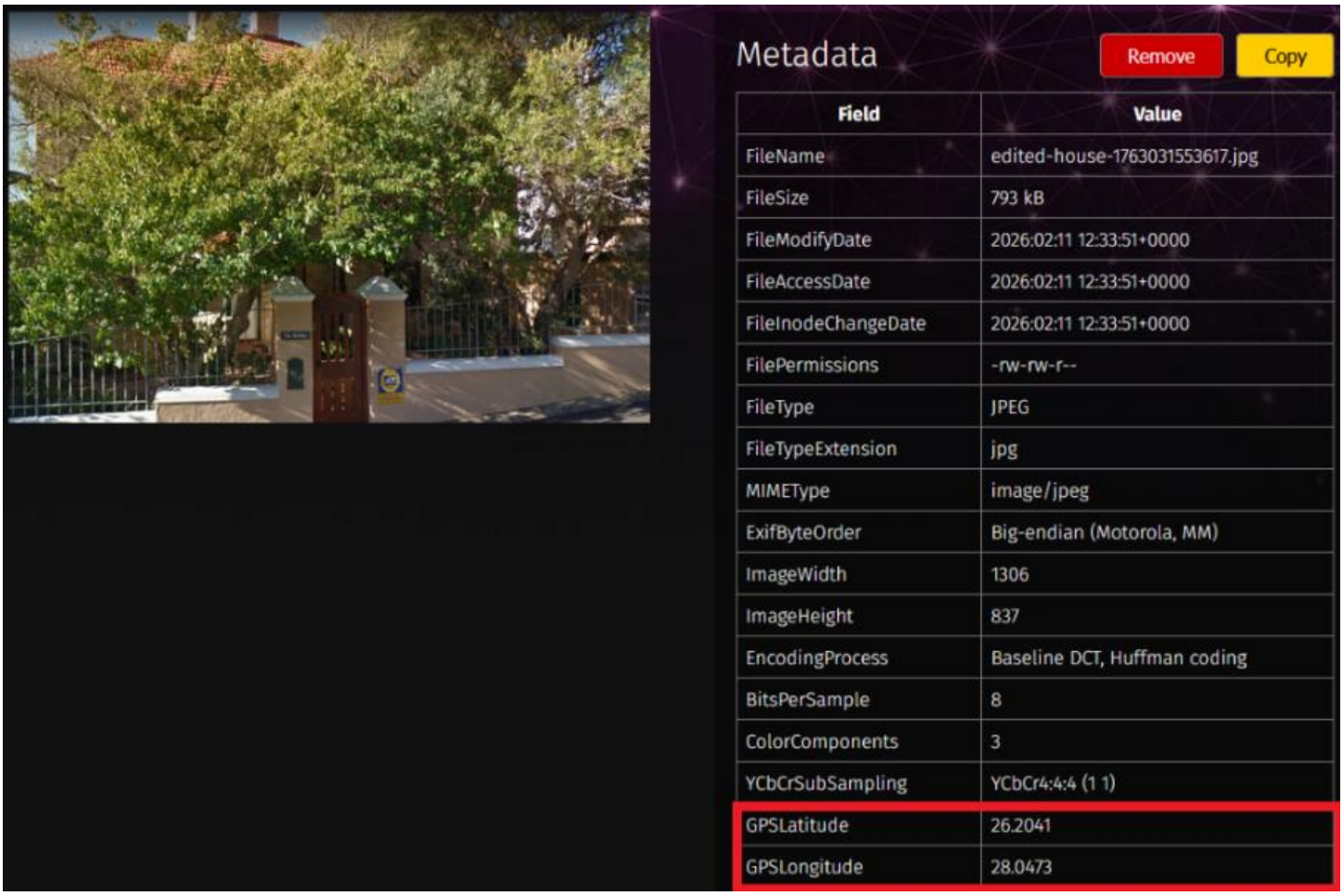


- Search Results Using Given Coordinates & Google Maps:



- **No Match Found**

Second Attempt - Pics.IO Metadata Extraction:

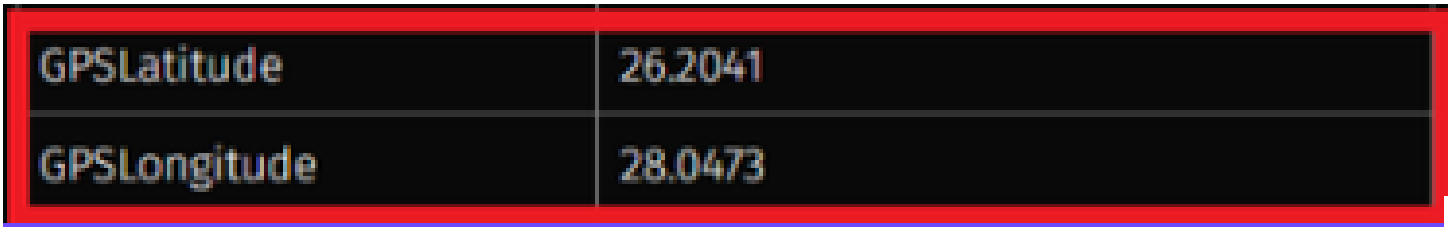


Metadata

Remove Copy

Field	Value
FileName	edited-house-1763031553617.jpg
FileSize	793 kB
FileModifyDate	2026:02:11 12:33:51+0000
FileAccessDate	2026:02:11 12:33:51+0000
FileInodeChangeDate	2026:02:11 12:33:51+0000
FilePermissions	-rw-rw-r--
FileType	JPEG
FileTypeExtension	jpg
MIMEType	image/jpeg
ExifByteOrder	Big-endian (Motorola, MM)
ImageWidth	1306
ImageHeight	837
EncodingProcess	Baseline DCT, Huffman coding
BitsPerSample	8
ColorComponents	3
YCbCrSubSampling	YCbCr4:4:4 (1 1)
GPSLatitude	26.2041
GPSLongitude	28.0473

- LAT/LONG Coordinates Found



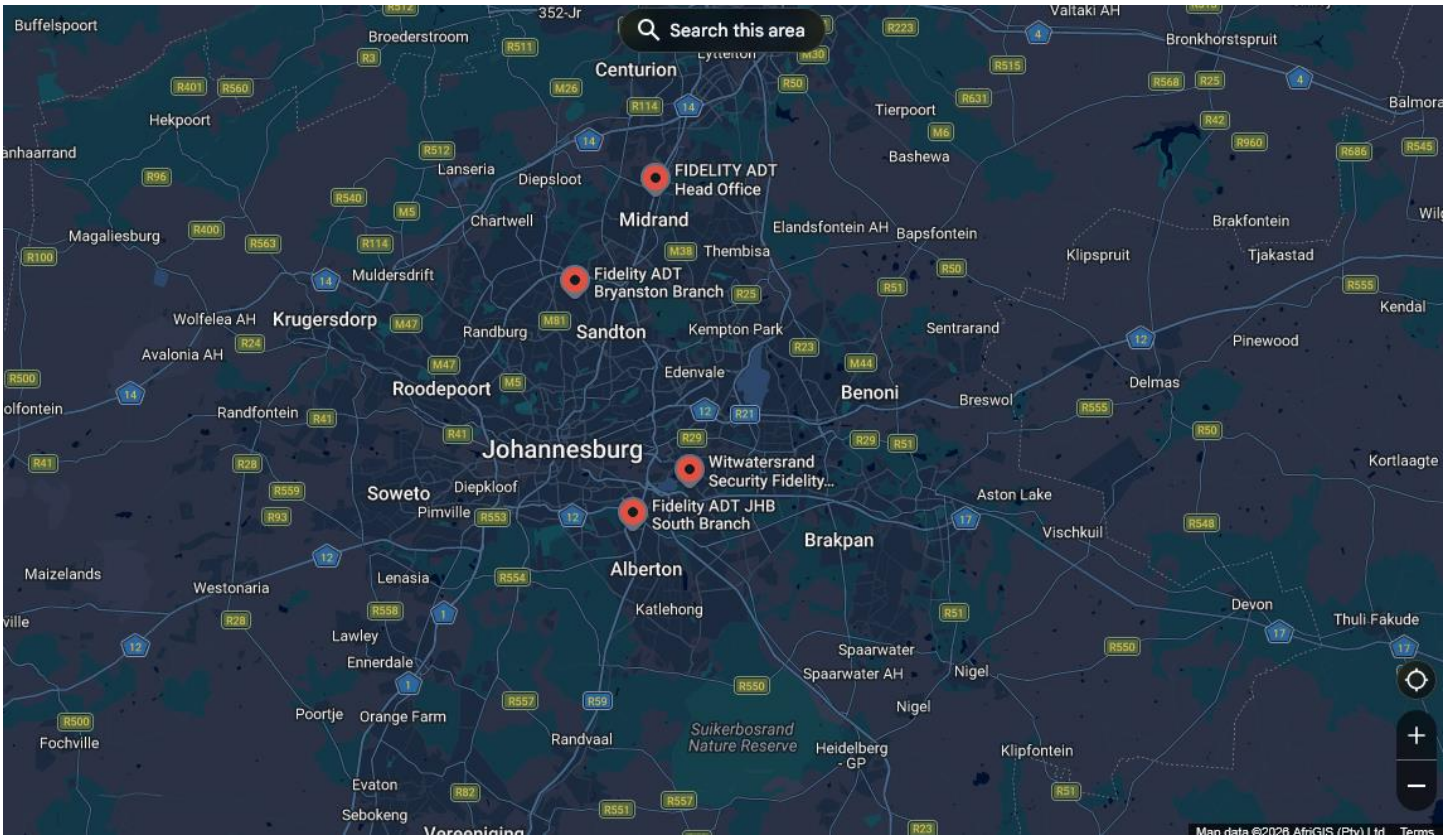
GPSLatitude	26.2041
GPSLongitude	28.0473

- Search Results Using Given Coordinates & CoordinatesFinder: Coordinates reference **Johannesburg, Capital of South Africa**

GPS coordinates for 26.2041 S, 28.0473 E

Latitude: -26.2026056
Longitude: 28.0470873

- Investigation into ADT in and around Johannesburg using Google Maps showed multiple locations including head office within the general vicinity, further supporting the probability of the property being located within Johannesburg



Conclusion

The property is likely to be located within the city of **Johannesburg, South Africa, not**

Flag Requirements	_ _ _ { _ _ _ _ _ _ _ _ _ _ _ _ } *3 + 12*
Suspected Flag	`THM{Johannesburg}` *3 + 12*
Flag Result	✅ **Correct**

Task 2: Archive Company Website

Objective

ACME Jet Solutions (warc-acme.com/jef/) is all over social media claiming they were founded in 2025 and that they're the fastest-growing data company in Africa. But something doesn't add up—one of their ex-employees ensures you that the company existed long before that. Your job as an OSINT investigator is to verify their founding date using only public information.

Initial Information

- URL: warc-acme.com/jef/
- Claim mismatch: Company claims founding in 2025

Approach

Google Search for Given Website

- **No Website Found**

Direct Access Attempts

```
wget warc-acme.com/jef/
```

- **No Return**

```
ping warc-acme.com/jef/
```

- **No Return**

Archive Search

Searched the Internet Archive (Wayback Machine) for historical captures of the website.

- **Match Found!**
- Source: https://archive.org/details/warc-acme.com-jef
- **First File Date:** February 10, 2016 (20160210224602)
- **Publication Date:** 2016

Conclusion

The website was first captured on **February 10, 2016** and contradicts the company's claim of being founded in 2025.

Flag Requirements	`_ _ _ { _ _ _ _ _ _ _ _ _ _ _ _ _ _ }` *3 + 14*
Suspected Flag	`THM{20160210224602}` *3 + 14*
Flag Result	✅ **Correct**

Task 3: Mysterious Landmark

Objective

After uncovering ACME Jet Solutions' origins and tracing their online presence through archived websites and international landmarks, investigators believe that an internal document was accidentally leaked by one of the company's developers. The document may contain crucial information about the individual responsible for maintaining their systems.

Initial Information

- Image of landmark and surrounding buildings from street view
- Mention of a building that played a big role in the fight for independence
- Mention of translated flag, potential foreign alphabet or language present

Approach

Initial Image Analysis

- **A:** Vodafone Sign
- **B:** Mentions City of Dublin, Ireland
- **C:** Building face distinctly white
- **D:** Landmark, Tall Tower
- Potentially sat in intersection given building arrangement

Google Maps Search: Vodafone Dublin

- 2 shops found in Center Dublin, visible from StreetView

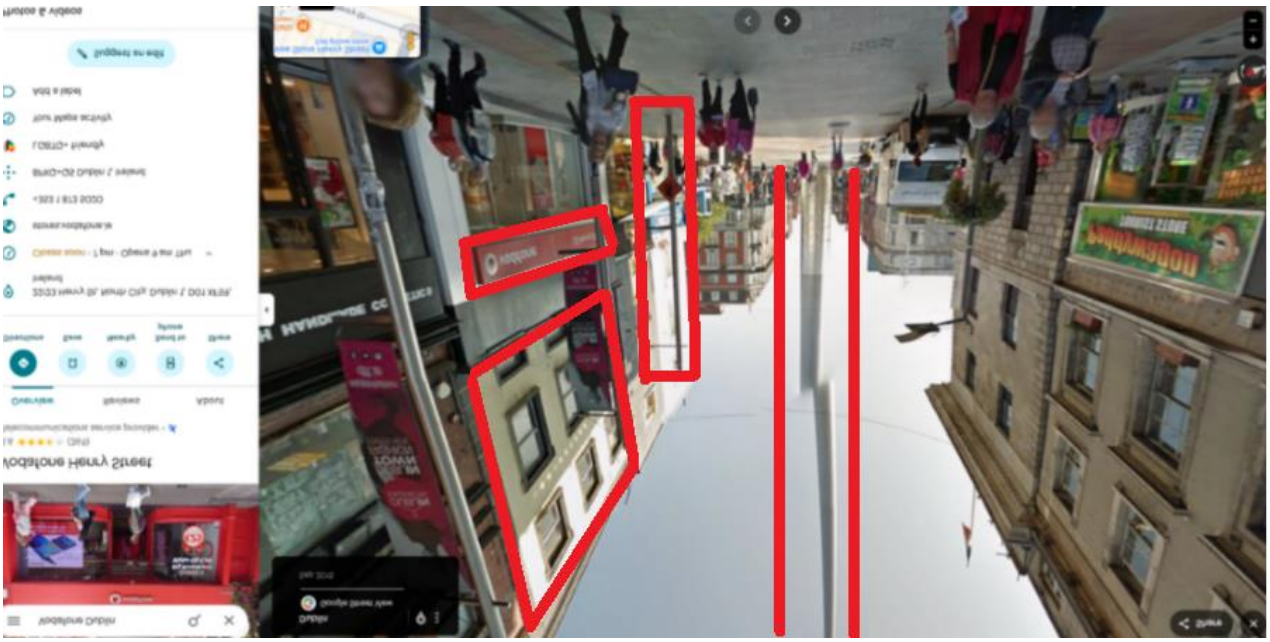
Vodafone Grafton Street
3.4 ★★★½☆ (421)
Telecommunications service provider · · 48 Grafton Street
Closes soon · 7 pm · Opens 9 am Thu · +353 1 673 0120
On-site services

Website Directions

Vodafone Henry Street
3.6 ★★★½☆ (369)
Telecommunications service provider · · 22/23 Henry St
Closes soon · 7 pm · Opens 9 am Thu · +353 1 873 5020
On-site services

Website Directions

- Vodafone, Henry Street, features landmark, Vodafone store, similar flag poles



Text Analysis

- Only non-English text found within reference of the image and to the right of the landmark on a wall sign

- Presumably Gaelic (Irish language)
- Translates to: General Post Office
- Research at https://www.irishhistory.com/general-post-office-the-gpo-dublin/ produced credible results confirming location and role during the 1916 Easter Rising

Conclusion

The building in question is the **General Post Office** located in Dublin on the corner of Henry St and O'Connell St Upper.

Flag Requirements	`_ _ _ { _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ }` *3 + 20*
Suspected Flag	`THM{General Post Office}` *3 + 20*
Flag Result	✅ Correct

Task 4: Internal Documents

Objective

After uncovering ACME Jet Solutions' origins and tracing their online presence through archived websites and international landmarks, investigators believe that an internal document was accidentally leaked by one of the company's developers. The document may contain crucial information about the individual responsible for maintaining their systems.

Initial Information

- Leaked internal document
- **Subject:** “Key Updates”
- **Description warning:** “Just remember Robin, don't publish this externally!”
- **Names given:** “Robin” and “Mark”
- **File format:** .odt (OpenDocument Text format is a ZIP archive containing XML files with embedded metadata)

Approach

Initial Attempt

Initial attempt to view the document through VSCode revealed garbled symbols and characters, likely due to the compression.

Standard Metadata Extraction Attempts

- Checked Windows File Properties → **No Details**
- Checked Office 2016 Properties panel → **No Details**

Extracting Embedded XML Metadata

Since .odt files are ZIP archives, we can extract and analyze the internal XML files using PowerShell:

```
# Navigate to where the file is
cd C:\Users\[YourUsername]\Downloads

# To confirm your path
pwd

# Rename from .odt to .zip
Copy-Item "internal-docs-1769695301727.odt" "internal-docs-1769695301727.zip"

# Extract the ZIP
Expand-Archive "internal-docs-1769695301727.zip" -DestinationPath "extracted" -Force
```

```
# View the metadata
notepad "extracted\meta.xml"
```

Understanding .odt File Structure

OpenDocument files (.odt) are ZIP-compressed archives containing:

```
internal-docs.odt/
├── mimetype
├── META-INF/
│   └── manifest.xml
├── content.xml         # Document content
├── meta.xml            # Metadata here
├── settings.xml
└── styles.xml
```

Key Metadata Findings

Analyzed meta.xml content using https://codebeautify.org/xmlviewer. Key findings:

Field	Value
meta:creation-date	2026-01-29T14:59:44
dc:description	Just remember Robin, don't publish this externally!
dc:date	2026-01-29T15:50:57.170215644
meta:editing-cycles	4
dc:subject	Key Updates
dc:title	Internal Document
meta:editing-duration	PT29M54S (29 minutes, 54 seconds)
meta:generator	LibreOffice/25.8.4.2$Linux_X86_64
meta:user-defined	**markwilliams7243**

Evidence of Incomplete Metadata Scrubbing

Based on the metadata analysis, there is clear evidence of attempted but incomplete metadata scrubbing:

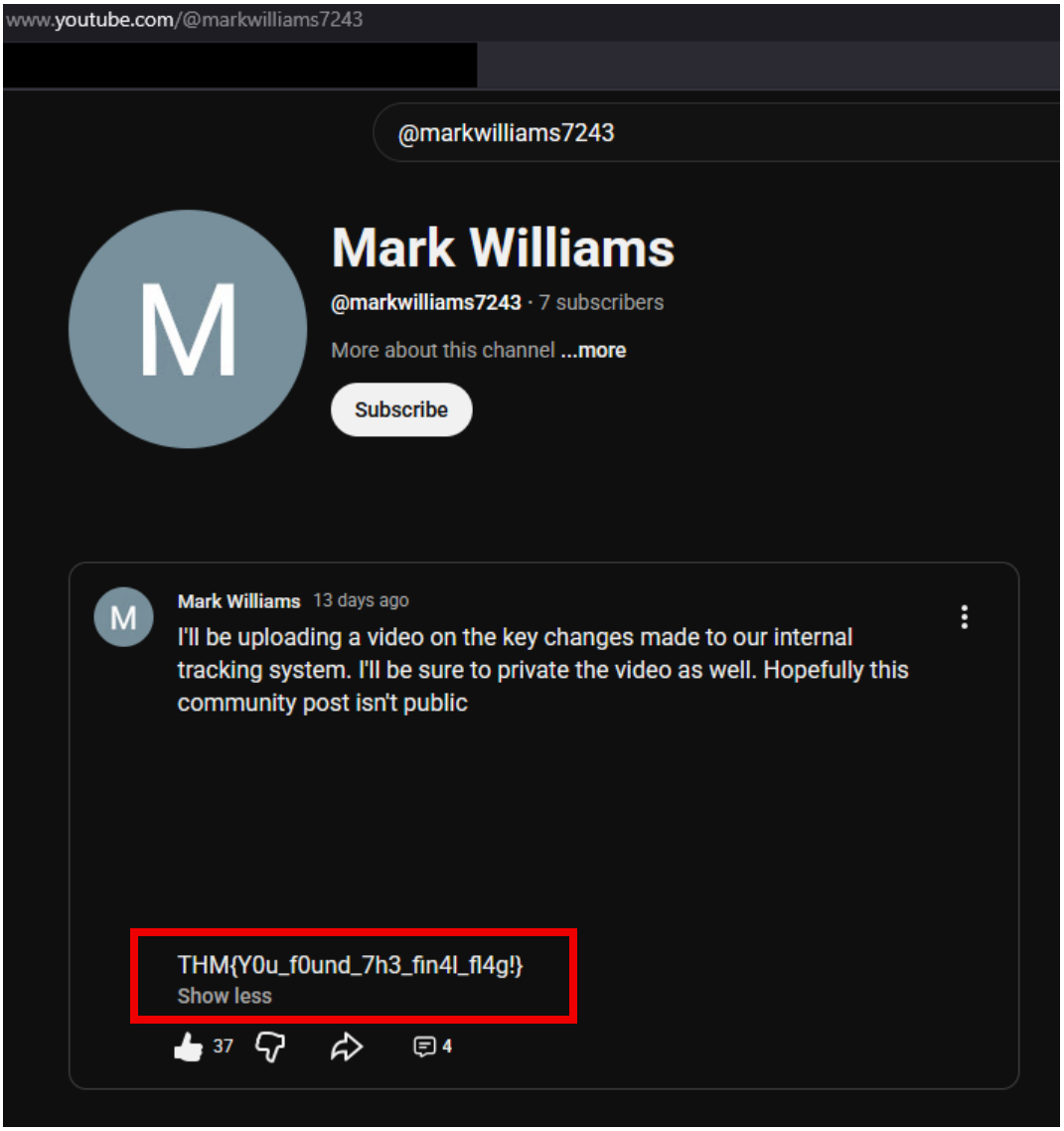
Missing Standard Fields:

- `<dc:creator>` **NOT PRESENT**
- `<meta:initial-creator>` **NOT PRESENT**

LibreOffice automatically generates these fields when you create a document. They contain the username/name of the person who created the file. Their absence is **not accidental** — someone deliberately removed them.

What They Forgot to Remove:
The creator tried to scrub standard metadata but **failed to remove the custom `<meta:user-defined>` field**, which leaked their username: **`markwilliams7243`**

- Given the mention of uploading a video a search on YouTube revealed a similarly named account and further investigation had revealed the tag.



Conclusion

Through systematic analysis of the leaked internal-docs-1769695301727.odt file, the identity of the individual likely responsible for maintaining ACME Jet Solutions' internal systems has become known.

Although the file's creator attempted to scrub standard metadata fields, specifically the `<dc:creator>` and `<meta:initial-creator>` tags commonly generated by LibreOffice, the presence of a custom user-defined field ultimately revealed a clear link to a **Mark Williams**, whose username remained embedded in the document despite attempts at obfuscation.

Combined with the contextual message “Just remember Robin, don't publish this externally” and corroborating details such as the editing cycle count, timestamps and the internal tone of the writing, the document strongly points to Williams as the system administrator or internal engineer responsible for handling sensitive technical materials.

Flag Requirements	`_ _ _ { _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ }` *3 + 25*
Suspected Flag	`THM{Y0u_f0und_7h3_fin4l_fl4g!}` *3 + 25*
Flag Result	✅ **Correct**

Final Summary

This OSINT challenge demonstrated the importance of thorough digital footprint analysis and metadata forensics. Through systematic investigation using publicly available tools and resources, I successfully:

- ✅ **Located a residential property** linked to ACME Jet Solutions' early operations in Johannesburg, South Africa through image metadata analysis and geolocation techniques
- ✅ **Verified the company's actual founding date** using Internet Archive, proving the company existed in 2016 despite claiming a 2025 founding date
- ✅ **Identified the General Post Office in Dublin** as a landmark connected to the company's international expansion through reverse image search and historical research
- ✅ **Uncovered the identity of Mark Williams** (username: markwilliams7243) as the system administrator responsible for maintaining ACME Jet's systems through metadata extraction and analysis of incomplete scrubbing attempts

Key Lessons Learned

- **Image metadata** can reveal precise geolocations even when visual landmarks are obscure
- **Internet Archive** is invaluable for verifying historical claims and detecting inconsistencies in company timelines
- **Incomplete metadata scrubbing** is a common OPSEC failure, custom fields and non-standard properties are frequently overlooked
- **OpenDocument formats** (.odt, .ods, .odp) are ZIP archives that can be extracted to reveal embedded XML metadata
- **Multi-source verification** combining visual analysis, geolocation, archival research, and metadata forensics provides comprehensive OSINT results

— End of Writeup —