# 🕵️‍♂️ OSINT REPORT

📅 Date: July 2025

🔒 Confidentiality Level: Business Confidential

📁 Conducted by: [Michele Covi]

🛠 Tools Used  
  
Below is a summary of the main tools and techniques used during the investigation. All activities were performed passively, respecting ethical OSINT guidelines.  
  
🔎 Domain and Subdomain Enumeration  
• Subfinder – Passive collection of subdomains.  
• httprobe – Detection of live HTTP/HTTPS services.  
• httpx – Technology fingerprinting and status codes.  
• WHOIS / RDAP – Domain ownership and registration data lookup.  
  
🌐 Web Interface Mapping  
• EyeWitness – Automated screenshots and metadata capture of web interfaces.  
  
🧠 Employee OSINT  
• Google Dorks – Search for public employee profiles on LinkedIn.  
 Example: site:linkedin.com/in "s\*\*\*y" AND ("engineer" OR "developer")  
• Maltego (Company Stalker Transform) – Enumeration of company-related email addresses.  
  
📄 Metadata Extraction  
• pdfinfo – Extracts general document metadata.  
• exiftool – Advanced metadata extraction (author info, software, UUIDs).  
  
📌 Notes:  
• No brute-force, login attempts, or intrusive actions were performed.  
• All tools were configured for stealth and passive footprint.

## 📑 Executive Summary

This report presents the findings of a passive OSINT investigation on the target organization: [Well-known E-commerce Company]. The goal was to identify publicly available information that could pose a security risk.

The investigation was conducted entirely passively, with no active interaction or authentication, in full accordance with OSINT ethics.

## 🔍 Key Findings

* Over 80 subdomains identified, including staging and development environments.
* Extensive use of Cloudflare for protection.
* Multiple login portals publicly accessible.
* Public employee visibility via LinkedIn.
* Public PDFs with revealing metadata (usernames, software, timestamps).

## 🧭 Target Overview

Company: [Redacted Name]

Sector: E-commerce, SaaS

Founded: 2006

Headquarters: [Redacted Address]

Stock Ticker: S\*P

CEO: [Redacted]

Revenue 2024: ~$8.88 billion USD

Global Presence: Canada, USA, Ireland, Germany

## 🌐 Domain & DNS Information

Analyzed Domain: s\*\*\*y.com

Registrar: MarkMonitor Inc.

DNSSEC: ❌ Not enabled

Name Servers:

* gold.foundationdns.com
* gold.foundationdns.net

⚠️ RDAP data shows that the domain is protected by restrictive policies.

## 🛰️ Sensitive Subdomain Discovery

Exposed subdomains were found related to development, login, API, and internal content.

* Selected examples:
* admin.[redacted].com → 403 – Protected access
* api.[redacted].com → 404 – API platform
* collabs-staging.[redacted].com → 200 – Staging environment
* device-enrollment.[redacted].com → 404 – Device endpoint
* cdn.[redacted].com → 200 – Active CDN

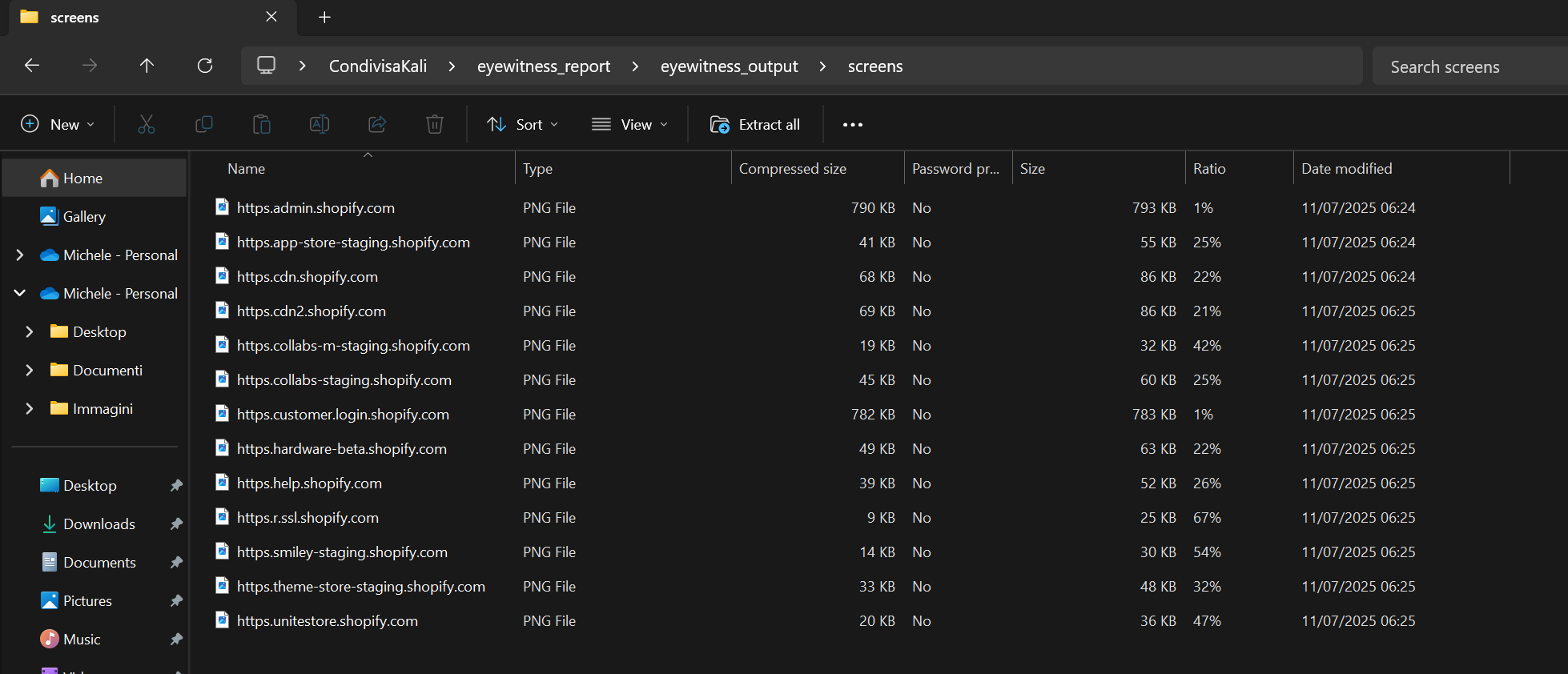
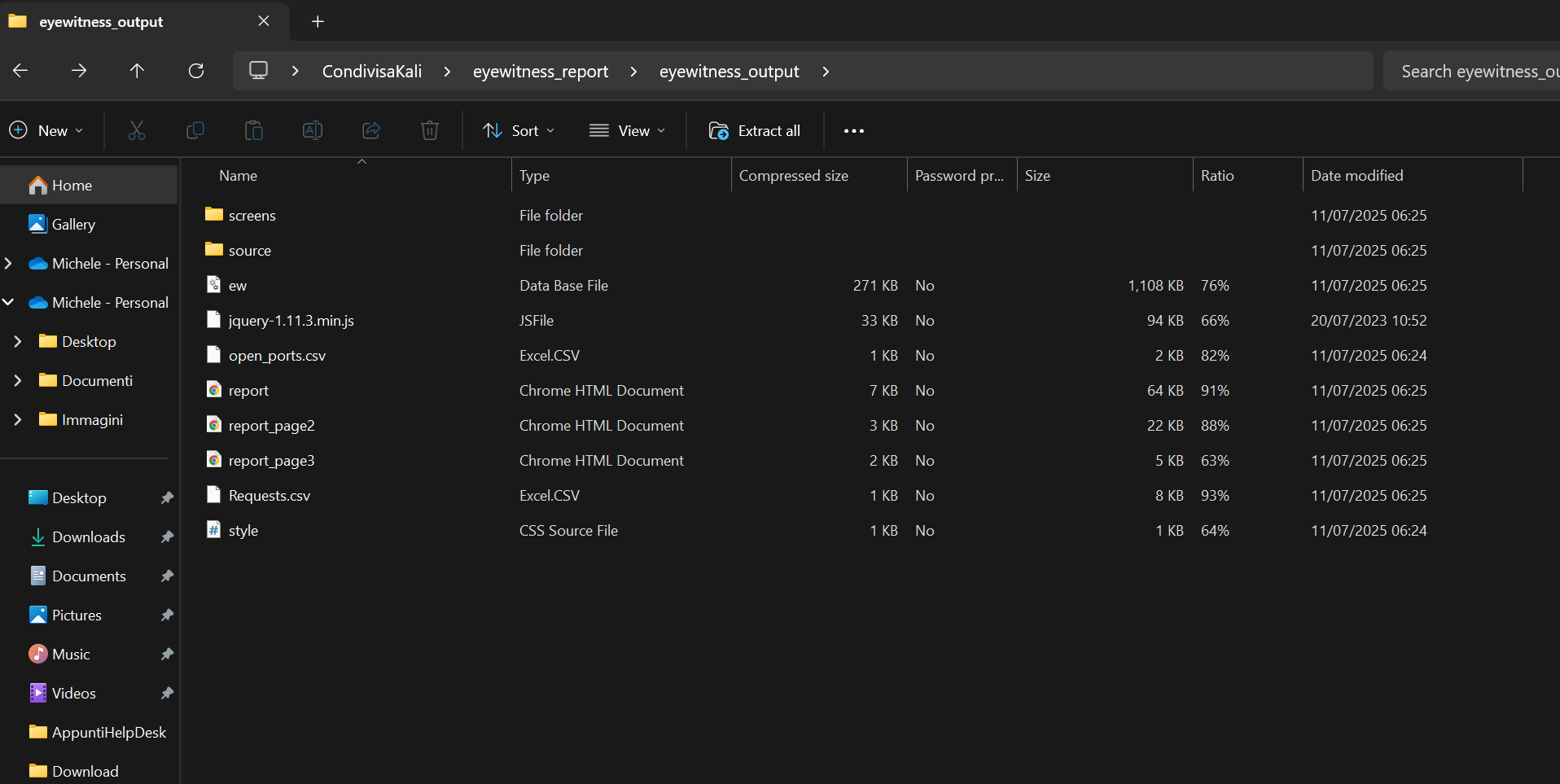
📌 Note: Some subdomains included personal names which have been redacted for privacy.

## 🧪 Technology Detection

Identified Tech Stack:

* Cloudflare WAF/CDN
* S\*\*\*y Platform (custom frontend/backend)
* jQuery 2.0.3 (legacy endpoints)
* HTTP/3 enabled
* Google Cloud CDN

## 🖼️ Web Interface Screenshots (EyeWitness)

📁 The EyeWitness Output Includes:  
• HTML report with clickable links  
• Individual PNG screenshots (login portals, admin panels, staging environments)  
• CSV files summarizing open ports and HTTP headers  
  
  
  
  
  
📌 Note:  
For best compatibility when viewing EyeWitness output locally, use Firefox or Edge browsers. Chrome may block local images.

Automated OSINT tool used to capture screenshots of discovered subdomains.

Examples captured:

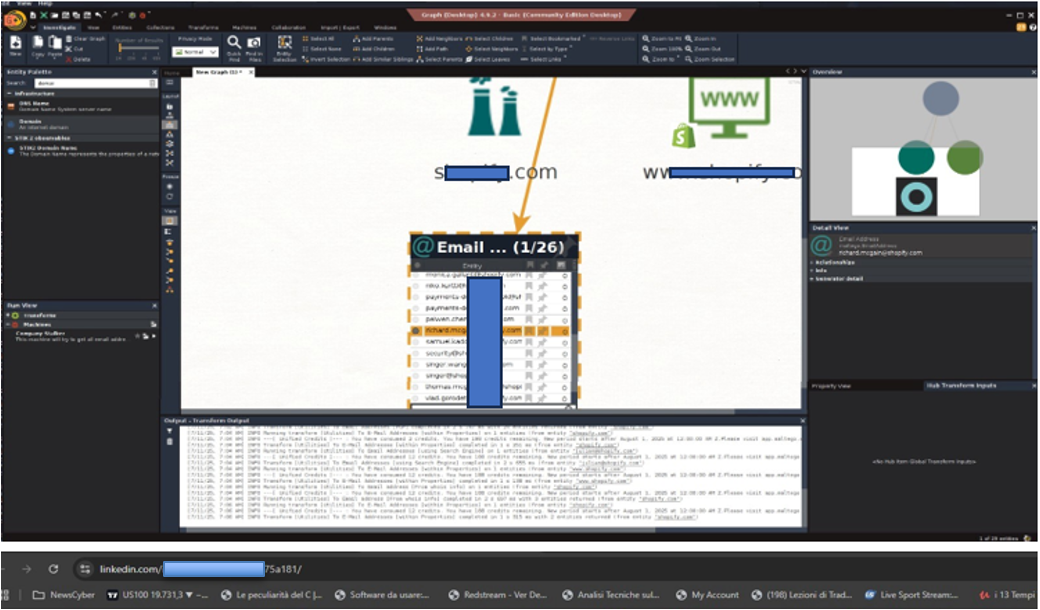
* Login pages
* Administration portals
* Staging environment dashboards
* CDN services

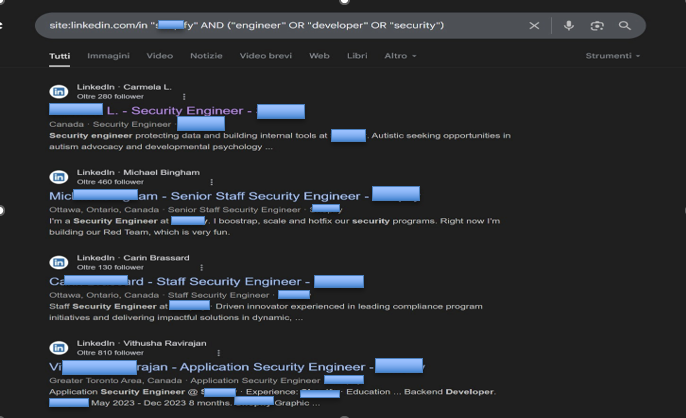
## 👥 Employee OSINT

Employee profiles and emails were primarily identified through Google Dorks targeting publicly indexed pages and documents.

Visible profiles and emails:

* Name1 – Security Engineer
* Name2 – Senior Staff Security Engineer
* Name3 – Staff Security Engineer
* xxxxxx@s\*\*\*y.com

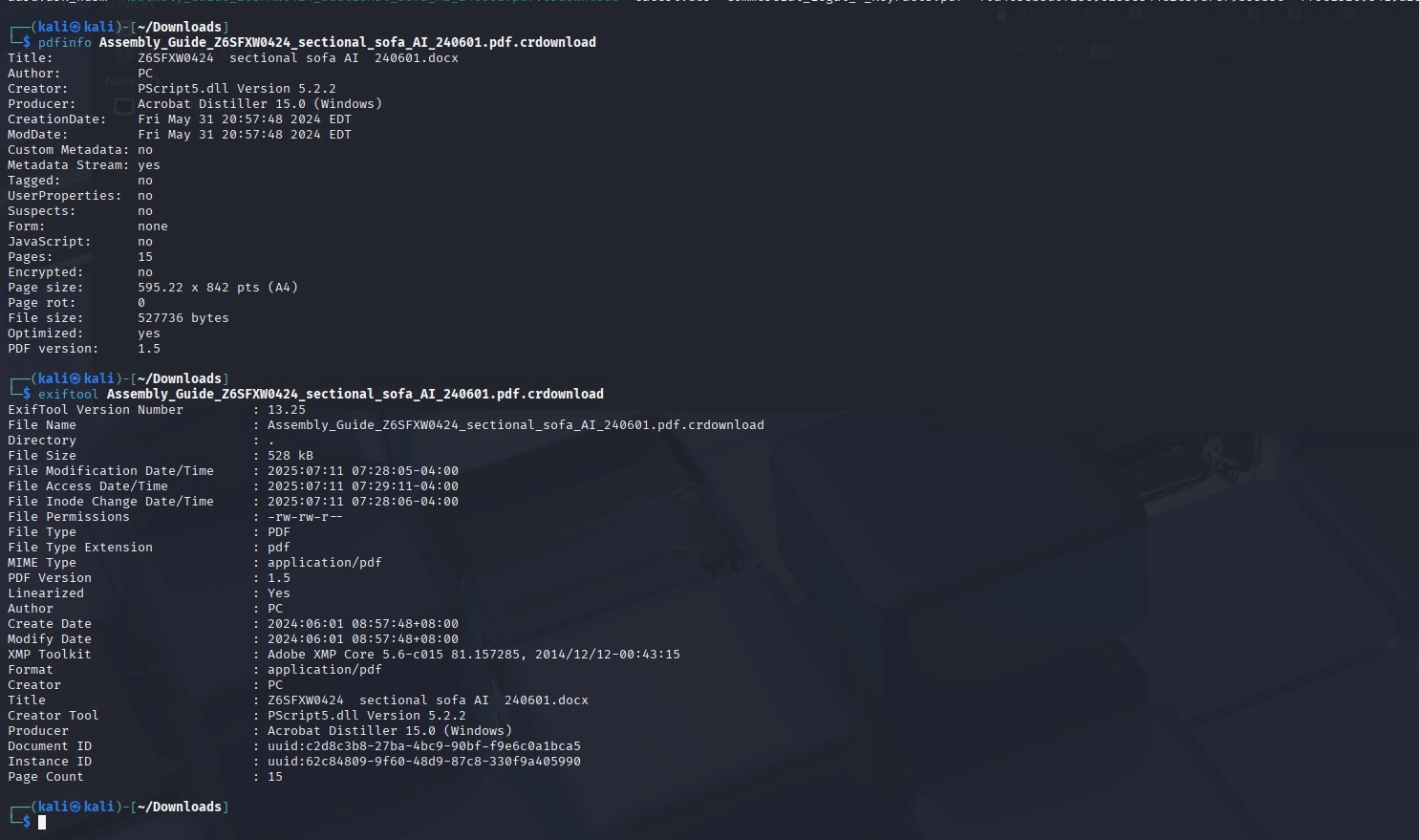


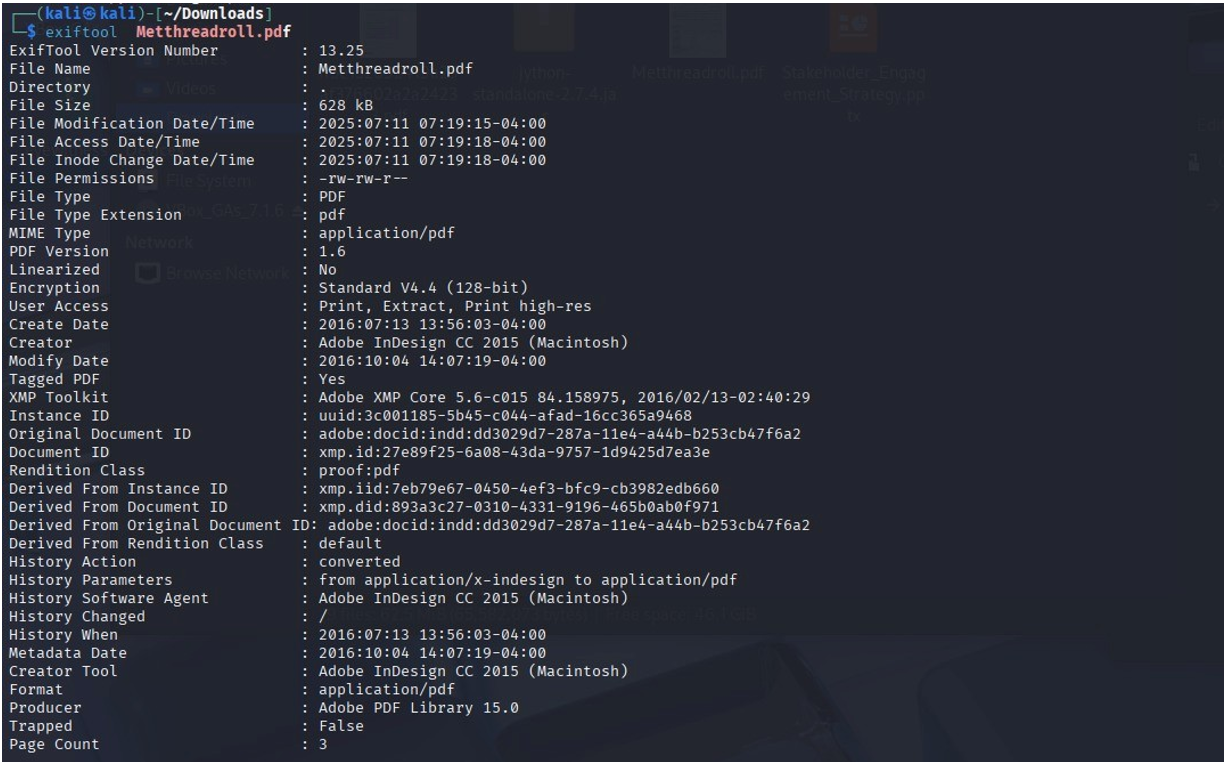


## 📄 Document Metadata

Tools used: pdfinfo, exiftool

📌 Findings:

* Authors (e.g., Macintosh, PC, Adobe Distiller)
* Modification/creation dates
* UUIDs, XMP, local usernames
* Conversions from Word (.docx → .pdf)



🎯 These details help in profiling internal tools, users, and workflows

## ⚠️ Risk Assessment

* Exposed subdomains – Impact: Medium – Access to staging/dev environments
* Public login/API endpoints – Impact: High – Phishing, brute-force risks
* Revealing metadata – Impact: Low – Internal profiling potential
* Employee visibility – Impact: High – Risk of spear phishing or impersonation

## 🧩 Conclusion

The target has a large public attack surface with good protections in place, but also with exposed elements that could be leveraged in realistic attack scenarios, especially in social engineering. This assessment highlights the importance of continuous passive monitoring to proactively defend against OSINT-enabled attack vectors.

## ✅ Recommendations

* Mask or remove staging/test subdomains
* Harden login portal protection
* Minimize metadata in public documents
* Continuously monitor new DNS assets
* Provide OSINT training to HR/Marketing staff