MetaTrace: Web-Based Metadata Forensics Tool

Empowering Forensics Through Metadata Insights

WE Group 12

December 2, 2024

Problem Statement

- **Importance of Metadata:**
  - Essential for verifying file authenticity, tracing leaks, and investigating cybercrimes.
- **Challenges in Current Tools:**
  - Complex tools like ExifTool require technical expertise.
  - Lack of visualization and predictive insights.
  - Limited accessibility for non-technical users.

Proposed Solution

MetaTrace:

- A web-based tool for metadata extraction, visualization, and analysis.
- Provides a user-friendly interface for easy interaction.
- Offers predictive insights and anomaly detection through machine learning.

Key Features

1. **File Upload:** Supports images, PDFs, and videos.
2. **Metadata Extraction:** Uses ExifTool for detailed metadata analysis.
3. **Visualization:**
   - Maps for geotagging.
   - Timelines for file creation/modification.
4. **Predictive Insights:** Detect anomalies in metadata.
5. **Searchable Storage:** Elasticsearch for fast and scalable metadata search.

Target Audience & Use Cases

Primary Users:

- Journalists: Validate image authenticity for reports.
- Forensic Experts: Analyze evidence files.
- Legal Professionals: Verify document origins.

Example Use Case:

- A journalist uploads an image to MetaTrace, sees where and when it was taken, and verifies its authenticity.

Feasibility & Technology

Technology Stack:

- **Frontend:** Angular + D3.js for visualizations.
- **Backend:** Python with Flask/Django and ExifTool integration.
- **Database:** Elasticsearch for efficient metadata storage.

Potential Impact

- Simplifies complex metadata analysis for non-technical users.
- Enhances cybersecurity practices in journalism and forensics.
- Reduces time and effort in analyzing metadata.