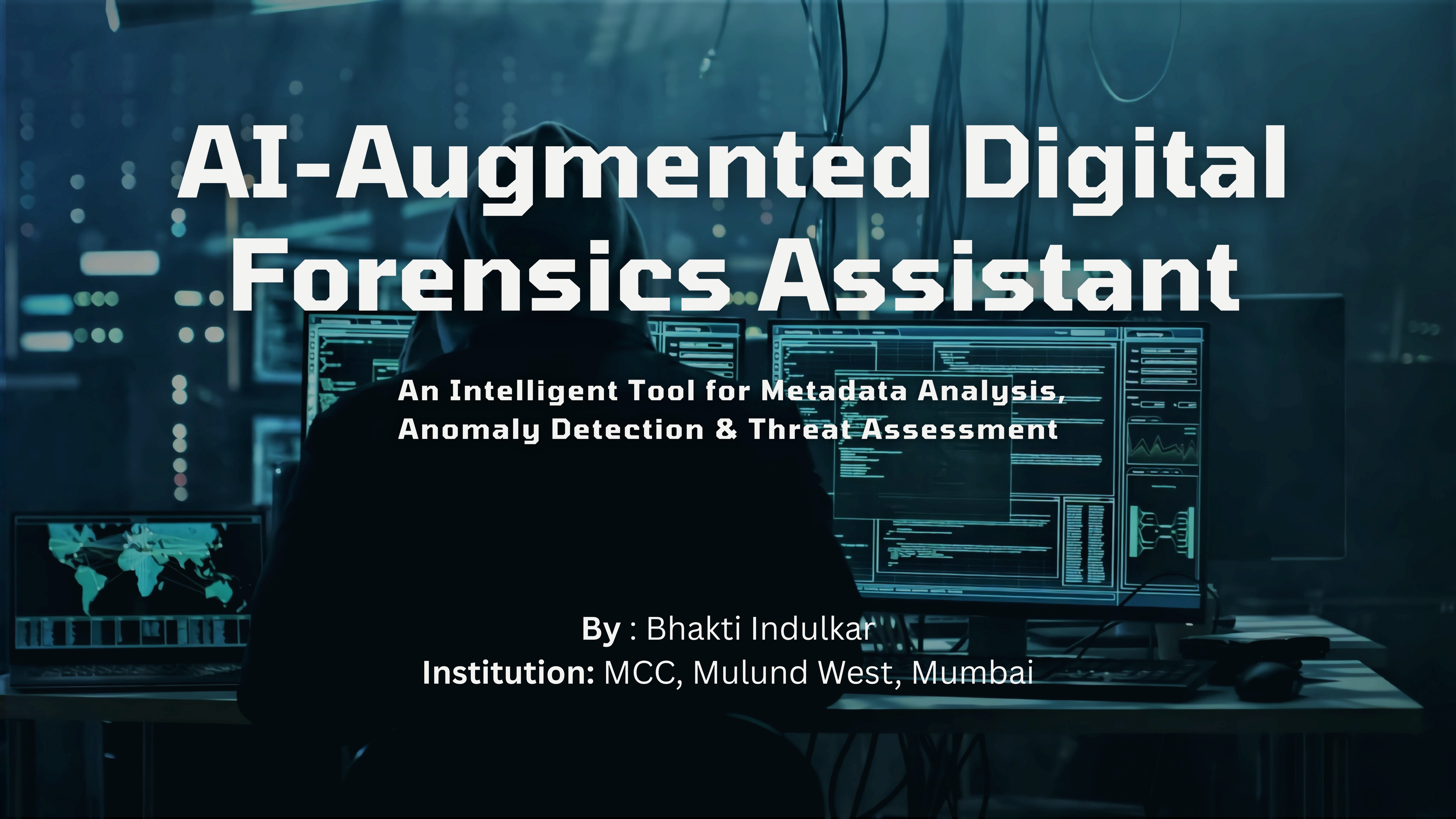

AI-Augmented Digital Forensics Assistant

An Intelligent Tool for Metadata Analysis, Anomaly Detection & Threat Assessment

By : Bhakti Indulkar
Institution: MCC, Mulund West, Mumbai

Why AI in Digital Forensics?

01 Increasing cyber threats

02 Manual forensic analysis is slow and error-prone

03 Need for real-time, intelligent investigation tools

04 AI enables quick detection of anomalies and suspicious behavior

Challenges in Current Forensic Practices

Manual log and media analysis is time-consuming.

Hidden metadata (like GPS or file tampering) is often overlooked.

Limited integration with threat intelligence platforms like VirusTotal

No integration between media forensics and threat databases.

Our Solution

Introducing the AI-Augmented Digital Forensics Assistant

- 🔍 File Metadata Analysis + Hashing
- 📸 Image + Video Metadata (EXIF/GPS/Codec/Time)
- 🧠 AI-based Log Anomaly Detection (Isolation Forest)
- 🦠 VirusTotal Threat Scoring
- 🌐 Streamlit GUI for Interactivity

Modular Design with Four Key Components:

01 file_analyzer.py – File metadata & hash analysis

02 ai_log_analyzer.py – AI model for anomaly detection using Isolation Forest

03 image_metadata.py – Extracts EXIF + GPS from images

04 virustotal_checker.py – Threat scoring using VirusTotal API

05 app.py – Streamlit-based unified frontend interface

06 video_metadata.py: Extracts codec, duration, frames

Code & Workflow Example

Log Anomaly Detection (AI Module)

- User uploads a .csv log file
- Model trained with IsolationForest
- Flags outlier patterns as suspicious

```
model = IsolationForest(contamination=0.1)
df['anomaly'] = model.fit_predict(df)
return df[df['anomaly'] == -1]
```

Real-World Use Cases

- 👮 Law Enforcement: Forensic analysis of seized devices
- 🕵️ Corporate Security Teams: Log breach analysis & file checks
- 📸 Media Verification: Tracing origin of images/videos
- 💾 Threat Intel: SHA256 cross-checked with VirusTotal

🖼️ Image Metadata (EXIF & GPS)

Extracts camera information, timestamps, and GPS coordinates from images to help trace where and when a photo was taken.

📁 File Metadata

Retrieves file size, type, creation/modification dates, and cryptographic hashes (MD5/SHA256) to verify file integrity and origin.

📊 Log Anomaly Detection

Uses an AI model (Isolation Forest) to automatically detect unusual patterns or activities in uploaded log files (e.g., brute force attempts).

🎥 Video Metadata

Analyzes video files to extract codec, duration, resolution, and format details—helpful in validating authenticity or tampering.
files (e.g., brute force attempts).

Future Enhancements

- 🧠 Deep Learning for Threat Behavior Profiling
- 🔐 Chain-of-Custody Tracker for legal workflows
- 📡 Live Network Traffic Capture + Threat Flagging
- 🤖 AI Chat Assistant for Digital Investigators
- 📁 OCR/Text Parsing for PDFs, DOCX, Archives

Conclusion

- A unified forensic platform with AI assistance
- Detects threats from multiple digital vectors
- Helpful for security analysts, police, and researchers