ChatGPT

Forensic GPS Suite – Gerichtssichere Nutzung (BSI-Stil)

Dieses Dokument beschreibt die Nutzung und die forensische Auslegung der „High-Performance Forensic GPS Suite“ unter Berücksichtigung der Anforderungen an gerichtstaugliche Beweismittel. Es orientiert sich an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

1. Überblick

Das Projekt extrahiert GPS-Koordinaten und Zeitinformationen aus Mediendateien (Fotos/Videos), reichert sie mit Metadaten an und erstellt eine lückenlose Zeitachse. Zwei Betriebsmodi stehen zur Verfügung:

- **Analyse-Modus (Standard)** – erstellt vollständige Zeitachsen mit Bewegungs-/Gap-Analysen sowie interaktiver Karte.
- **Court-Mode** – minimiert Annahmen, verzichtet auf bewegungsbasierte Interpretationen und erzeugt zusätzliche Nachweise (Hashes, Audit-Trail). Dieser Modus ist für die Vorlage vor Gericht vorgesehen.

Erweiterte forensische Optionen

- `--no-map` – deaktiviert die Erstellung der interaktiven Karte. Im Court-Mode automatisch aktiv.
- `--audit-json` – schreibt eine detaillierte JSON-Audit-Datei, die alle Entscheidungen zur Zeitbestimmung protokolliert. Im Court-Mode automatisch aktiv.
- `--timeline-hash` – berechnet einen SHA256-Hash der exportierten Timeline-CSV, um die Integrität der Zeitachse nachweisen zu können. Im Court-Mode automatisch aktiv.

2. Zeitbestimmung

Für jede Datei wird mithilfe von `resolve_best_timestamp()` der beste verfügbare Zeitstempel ausgewählt. Die Funktion nutzt eine priorisierte Liste aus GPS-Zeit (`GPSDateTime`), EXIF-Zeit (`DateTimeOriginal`), Media-Zeit (`MediaCreateDate` / `TrackCreateDate`) und generischer Erstellungszeit (`CreateDate`). Das Ergebnis enthält die Rohzeit (`datetime_raw`), die Quelle (`time_source`) und eine Vertrauensstufe (`time_confidence`).

Zeitzonen-Normalisierung

Das Modul `normalize_time()` wandelt Rohzeitstempel in drei Repräsentationen um:

- **dt_utc** – ISO-Format in UTC, sofern die Zeit einen gültigen Offset enthält.
- **dt_local** – ISO-Format mit ursprünglichem Offset (nur gesetzt, wenn die Zeitquelle tatsächlich eine TZ enthält). Im Court-Modus wird dieses Feld bewusst leer gelassen, wenn die Zeitzone lediglich angenommen wurde.
- **dt_naive_iso** – ISO-Zeit ohne Zeitzoneninformation, dient als Fallback.

Ist keine Zeitzone vorhanden und die Annahme von Standard-Zeitzonen (`--tz`) deaktiviert (Court-Mode), bleibt `dt_utc` und `dt_local` leer. Die Annahme einer Zeitzone wird in `tz_info` dokumentiert und durch `timezone_assumed=True` gekennzeichnet.

3. Zeitachse und Sortierung

Die Zeitachse wird mit `build_timeline()` erstellt. Der Algorithmus sortiert Datensätze zuerst nach Verfügbarkeit und Zeitstempel (`dt_utc` vor `dt_naive_iso`) und verwendet den Dateipfad als deterministisches Tie-Break. Datensätze ohne verlässlichen Zeitstempel werden nach Pfad sortiert ans Ende angefügt. Dies garantiert eine reproduzierbare Reihenfolge der Timeline – eine wichtige Anforderung für die gerichtliche Verwertbarkeit.

4. Bewegungs- und Lückenanalyse

Die Funktionen `analyze_movement()` und `detect_gaps()` untersuchen die Abstände zwischen aufeinanderfolgenden Timeline-Einträgen. Sie erkennen Stopps, Bewegungen, Sprünge und Zeitlücken anhand frei einstellbarer Schwellen. Diese Analysen liefern wertvolle Hinweise auf Bewegungsmuster, sind aber interpretativ.

Im Court-Mode werden diese Analysen **nicht** ausgeführt. Es werden keine Bewegungs- oder Gap-Berichte erzeugt, um jede implizite Interpretation zu vermeiden. Stattdessen enthält die Export-CSV nur die rohen, nachweisbaren Informationen.

5. Exporte und Nachweise

CSV- und SQLite-Exporte

Alle extrahierten Metadaten werden als CSV (`test.csv`) und SQLite-Datenbank (`forensic_data.sqlite`) exportiert. Optional können zusätzlich Monats-CSVs erstellt werden (`--no-monthly` deaktivieren).

Manifest

Unabhängig vom Modus wird ein Manifest (`evidence_manifest.csv`) erzeugt. Es enthält für jede Datei den Pfad, den SHA256-Hash, die Dateigröße und die Änderungszeit. Dieses Manifest dient als Grundpfeiler der Beweissicherung.

Timeline

Die Timeline-CSV (`timeline.csv`) enthält die rekonstruierten Zeitinformationen samt Metadaten (Pfad, Koordinaten, Zeitquellen usw.). Im Court-Mode wird ein ergänzender Hash (`timeline_csv.sha256.txt`) generiert, um die Unveränderbarkeit der Zeitachse nachzuweisen.

Audit-Trail

Mit dem Flag `--audit-json` (im Court-Mode implizit aktiv) wird eine JSON-Datei (`audit_trail.json`) erzeugt. Sie protokolliert pro Datensatz:

- den Dateipfad und SHA256,
- den ausgewählten Rohzeitstempel,
- die Zeitquelle und deren Vertrauensstufe,
- alle normalisierten Zeitfelder (`dt_naive_iso`, `dt_local`, `dt_utc`),
- Informationen zur Zeitzone und ob diese angenommen wurde.

Dieser Audit-Trail stellt eine nachvollziehbare Dokumentation sämtlicher Entscheidungen dar und erleichtert die Prüfung durch Dritte.

Interaktive Karte

Die interaktive Karte (`interactive_map.html`) visualisiert alle Koordinaten und – im Analyse-Modus – die Bewegungssegmente und Gaps. Im Court-Mode oder bei Nutzung von `--no-map` wird diese Karte nicht erzeugt.

6. Nutzung

Analyse-Modus (Standard)

```
python gps_forensic.py --sd <eingabe-ordner> --od <ausgabe-ordner>
```

Dieser Modus erzeugt alle verfügbaren Exporte inklusive Bewegungs- und Gap-Analysen sowie der interaktiven Karte.

Court-Mode

```
python gps_forensic.py --sd <eingabe-ordner> --od <ausgabe-ordner> --court
```

Der Court-Mode aktiviert automatisch folgende Optionen:

- keine Zeitzonenannahmen (nur absolute Zeitstempel werden genutzt),
- keine Bewegung-/Gap-Analyse,
- keine interaktive Karte,
- Audit-Trail (`audit_trail.json`),
- Timeline-Hash (`timeline_csv.sha256.txt`).

Optional können die Flags `--no-map`, `--audit-json` und `--timeline-hash` auch ohne `--court` genutzt werden, um einzelne Funktionen explizit zu steuern.

7. Hinweise zur Beweissicherung

- **Integrität bewahren:** Arbeiten Sie stets mit Kopien der Originaldaten und führen Sie die Analysen auf forensisch sauberen Abbildern durch. Die im Manifest dokumentierten Hashes dienen zur Verifikation der Integrität.
- **Dokumentation:** Halten Sie sämtliche Arbeitsschritte schriftlich fest und speichern Sie die Logdatei (`forensic_audit.log`) zusammen mit den Exports.
- **Verifikation:** Überprüfen Sie die generierten Hashes vor der Verwendung im Gericht auf Übereinstimmung mit den Originaldateien und der exportierten Timeline.

8. Kontakt

Bei Fragen oder Verbesserungsvorschlägen wenden Sie sich bitte an das Entwicklerteam. Dieses Dokument kann jederzeit erweitert werden, um zukünftige Anforderungen abzudecken.
