

MSC FORENSIC INVESTIGATION

Mobile Forensic Investigation using Cellebrite Physical Analyzer

A comprehensive forensic examination of extracted mobile device data, demonstrating coordinated activity through multi-platform evidence correlation and temporal analysis.

Student Name: Vanshaj Patel

Student ID: 2517969

Module Name: Digital Forensics

Assignment Title: Mobile Forensic Investigation using Cellebrite Physical Analyzer

Course Level

MSc Digital Forensics

Primary Tool

Cellebrite Physical Analyzer

Focus Area

Mobile Artefact Analysis



Introduction to Mobile Forensics

- **Digital Forensics:** Scientifically rigorous process of identifying, preserving, analyzing, and presenting digital evidence in legally defensible manner
- **Legal Admissibility:** Evidence must satisfy evidentiary standards and chain of custody requirements for judicial proceedings
- **Mobile Devices:** Repositories of communications, geolocation data, behavioral patterns, and application artefacts essential to investigations
- **Investigative Value:** Mobile device analysis provides primary evidence source for establishing intent, coordination, and temporal sequences
- **Forensic Integrity:** Maintains chain of custody, documentation standards, and examination protocols throughout analysis

Case Background

- Investigation involves **three individuals using separate mobile devices** in suspected data theft and illegal distribution
- Evidence shows **coordinated communication across messaging and email platforms**
- Activity indicates a **structured operation with financial intent**
- Identified roles:

Emma – Primary perpetrator

Joe – Intermediary

Norman – Buyer

- Objective: **Correlate digital evidence to confirm coordinated criminal activity**

Aim & Objectives

- **Primary Objective:** Extract and analyze mobile device data using Cellebrite Physical Analyzer to recover digital artefacts
- **Evidence Recovery:** Identify and recover communications, contacts, financial records, and behavioral evidence across multiple platforms
- **Artefact Correlation:** Establish cross-platform linkages between chat, email, contacts, and file system data to confirm coordinated activity
- **Timeline Reconstruction:** Establish chronological sequence of events through temporal analysis of recovered communications and metadata
- **Investigative Support:** Provide forensically defensible findings demonstrating coordinated activity and establishing suspect roles

Tools & Forensic Environment

- **Cellebrite Physical Analyzer:** Industry-standard mobile forensics platform enabling comprehensive device analysis and artefact recovery
- **Extraction Capability:** Full file system access provides maximum depth of artefact recovery, including deleted data and application databases
- **Examination Engines:** Hash sets filter known files; carving recovers deleted artefacts; archive extraction accesses compressed data; selective app decoding targets relevant applications
- **Forensic Standards:** Examination complies with NIST SP 800-101, ISO/IEC 27037, and ACPO digital forensic guidelines
- **Chain of Custody:** All examination steps documented and verified to ensure evidence integrity and legal admissibility

Forensic Methodology

01

Phase 1 - Acquisition

Extract complete mobile device data using Cellebrite Physical Analyzer, establishing device identity and extraction integrity

02

Phase 2 - Examination

Configure examination tools (hash sets, carving, archive recovery, selective app decoding) to optimize artefact recovery

03

Phase 3 - Analysis

Recover and correlate evidence across communications, contacts, and file system; establish temporal sequences and cross-platform linkages

04

Phase 4 - Reporting

Document findings in forensically defensible format, presenting evidence correlation and suspect role analysis

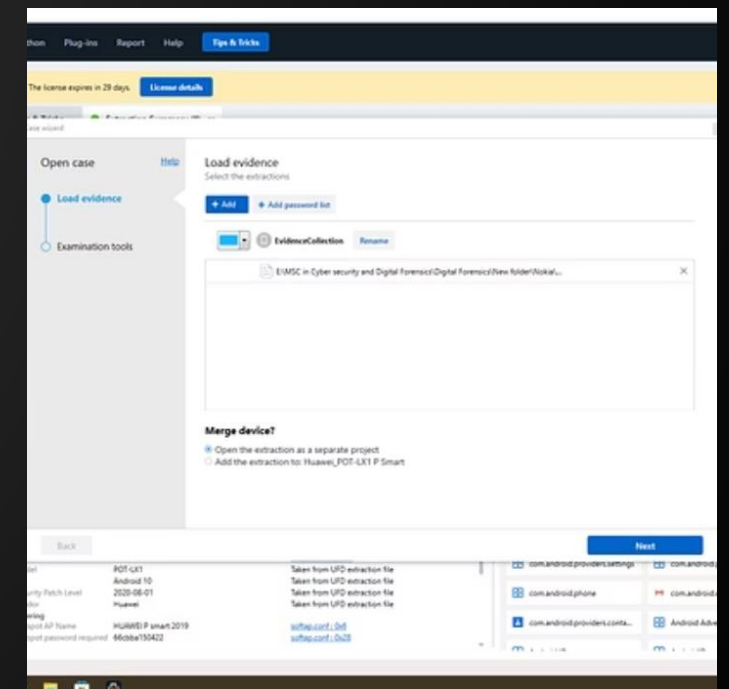
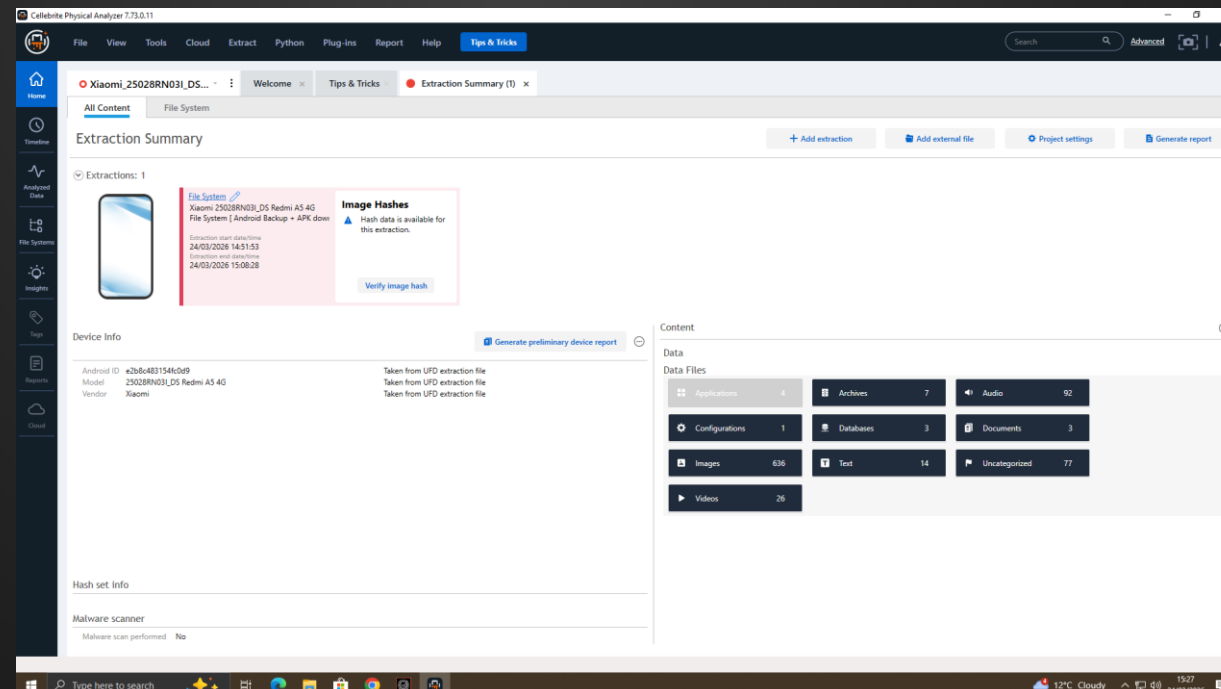
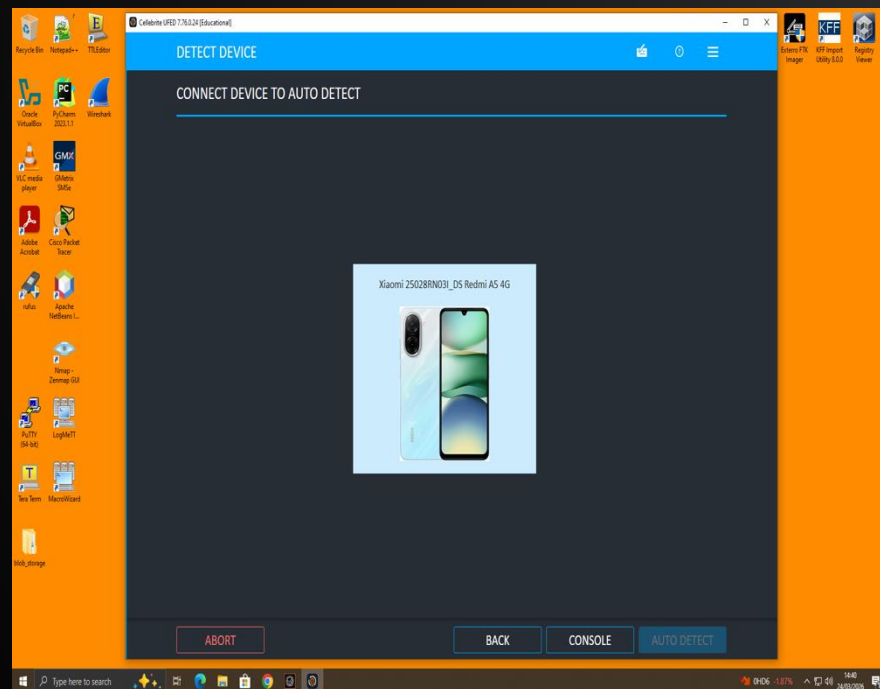
05

Standards Compliance

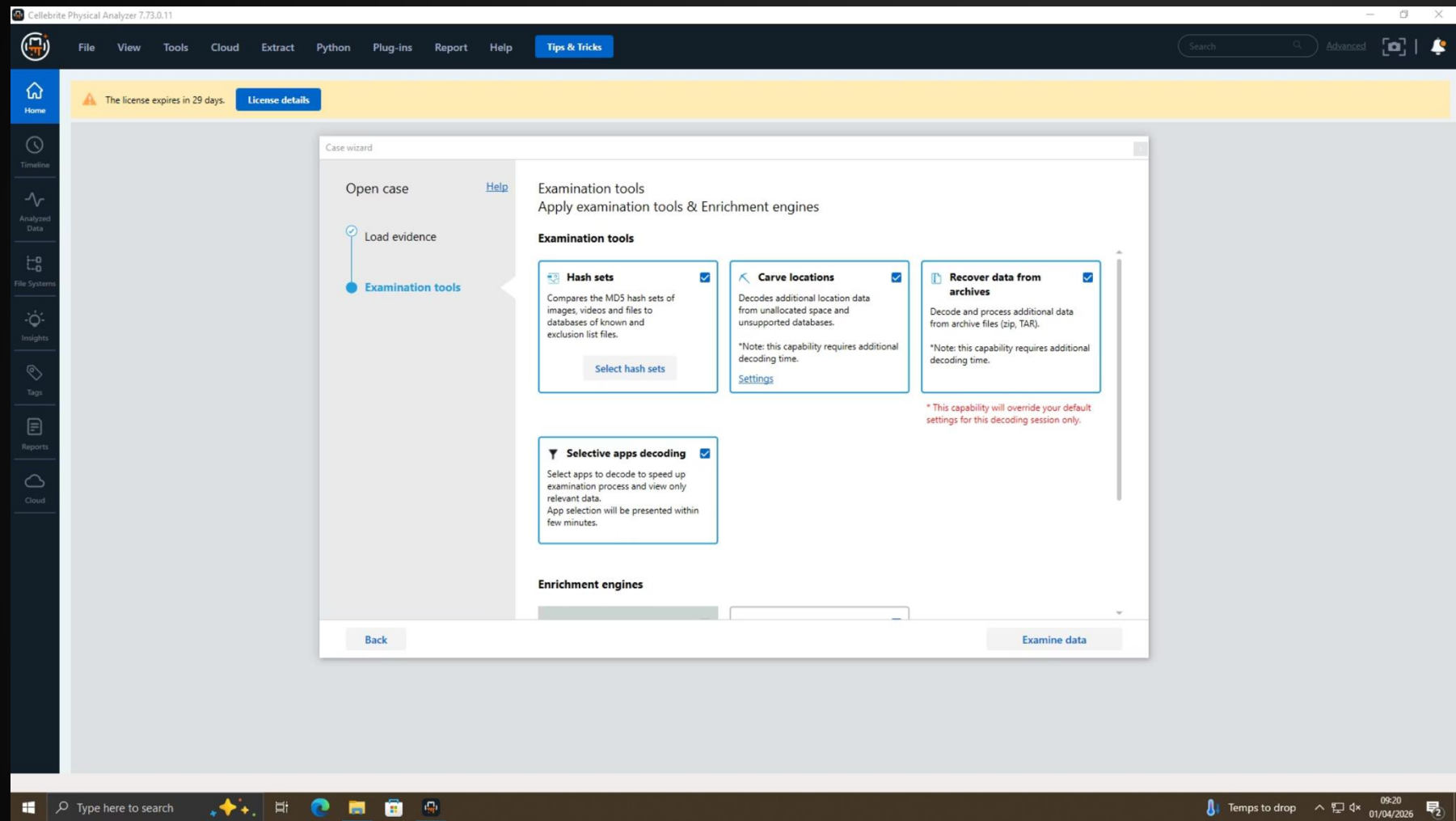
Follows NIST SP 800-101 and ACPO digital forensic guidelines

Evidence Acquisition

- **Load Evidence:** Mobile device data imported into Cellebrite Physical Analyzer, establishing initial evidence baseline
- **File System Extraction:** Complete file system access enables maximum artefact recovery depth, including deleted communications and application data
- **Device Identification:** Device model, serial number, and extraction metadata recorded to establish evidence provenance
- **Integrity Verification:** Hash values computed and verified to ensure evidence integrity throughout examination process
- **Chain of Custody:** All acquisition steps documented and verified, establishing legal admissibility of recovered evidence

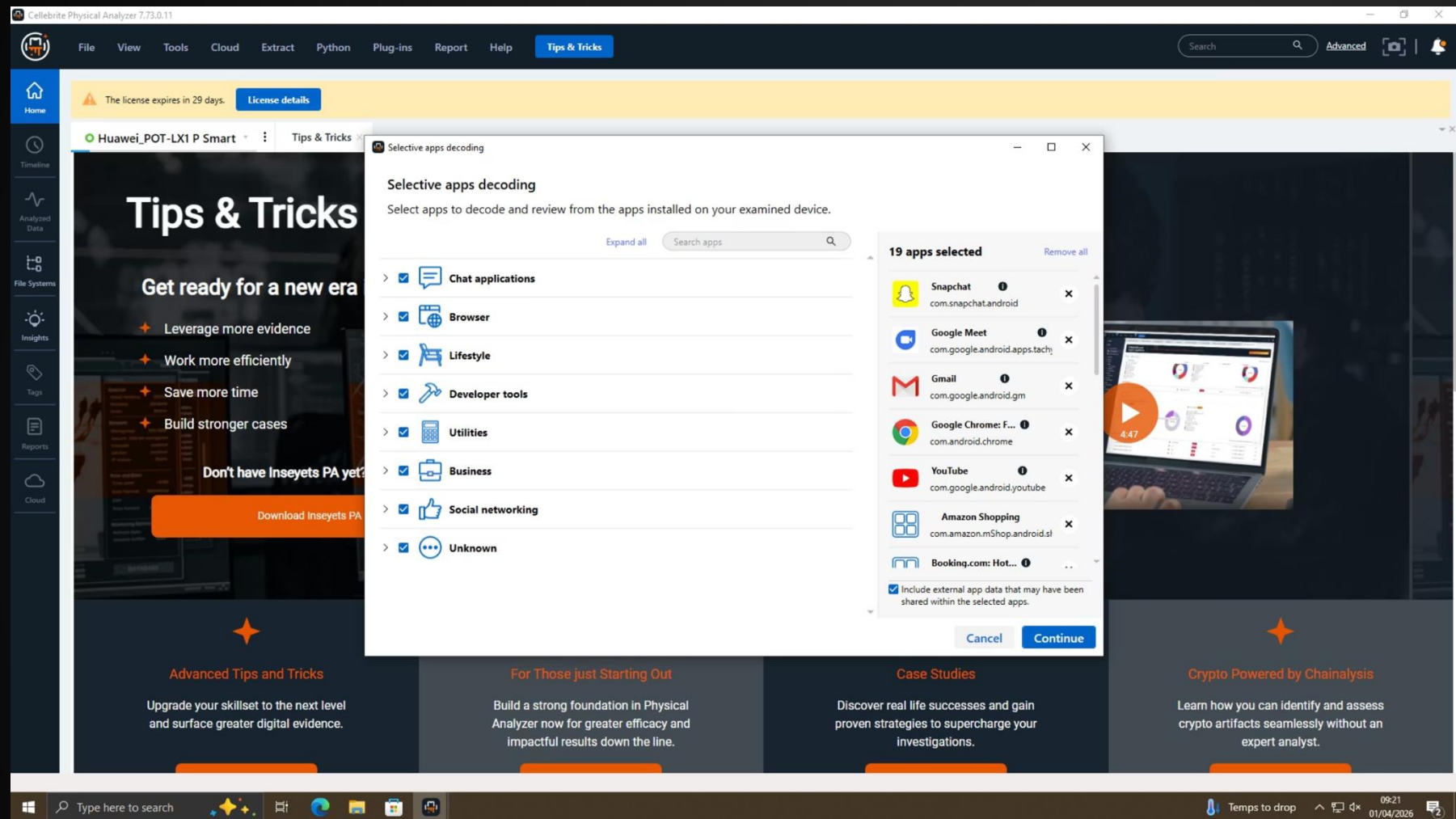


Examination Tools Configuration



- Hash Sets: Filters known system files and reduces noise, enabling focused analysis on potentially relevant artefacts
- Carve Locations: Recovers deleted data through file signature analysis, revealing deliberately removed communications and contact information
- Recover Data from Archives: Extracts compressed and archived content, accessing hidden or obfuscated data
- Selective App Decoding: Enables targeted application-level analysis of messaging platforms, email, and social media applications
- Forensic Significance: Configuration determines examination depth and scope, ensuring comprehensive and defensible artefact recovery

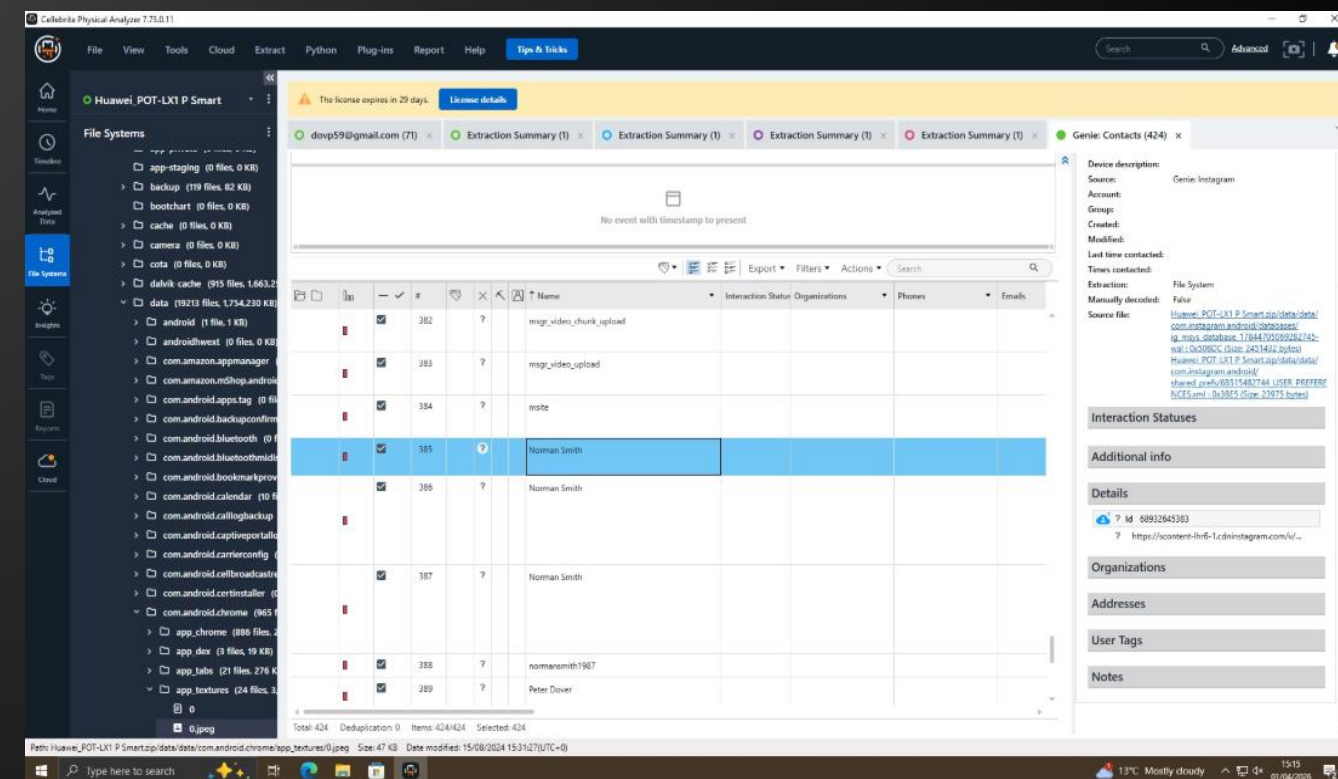
Selective App Decoding



- **Targeted Selection:** Examiner selects specific applications based on investigative hypothesis, optimizing analysis efficiency and relevance
- **Messaging Applications:** WhatsApp, Telegram, Signal, and Viber prioritized as primary communication channels for evidence recovery
- **Social Media & Email:** Facebook, Instagram, and Gmail included to establish cross-platform communication patterns and corroborate evidence
- **Efficiency:** Focused approach reduces processing time while maintaining comprehensive coverage of suspected evidence sources
- **Forensic Rigor:** Demonstrates examination was conducted with specific investigative objectives, not indiscriminate data extraction

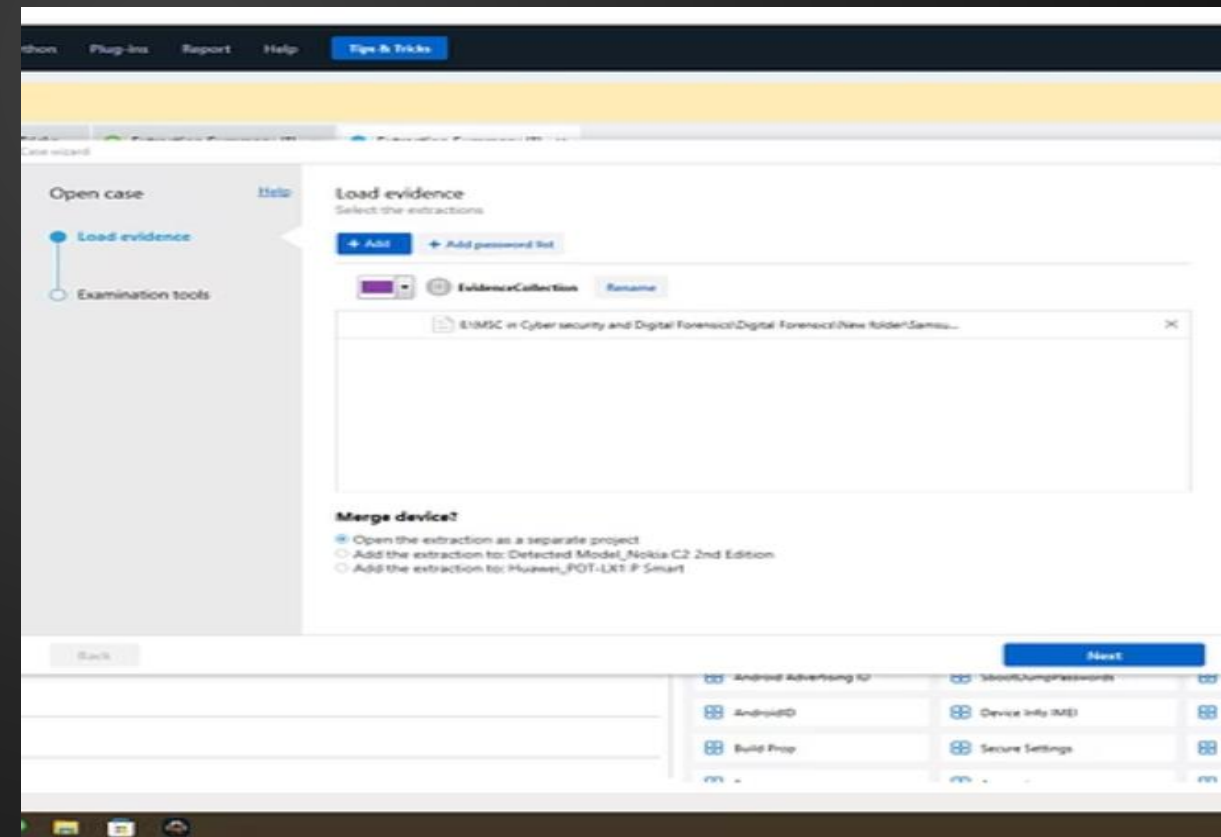
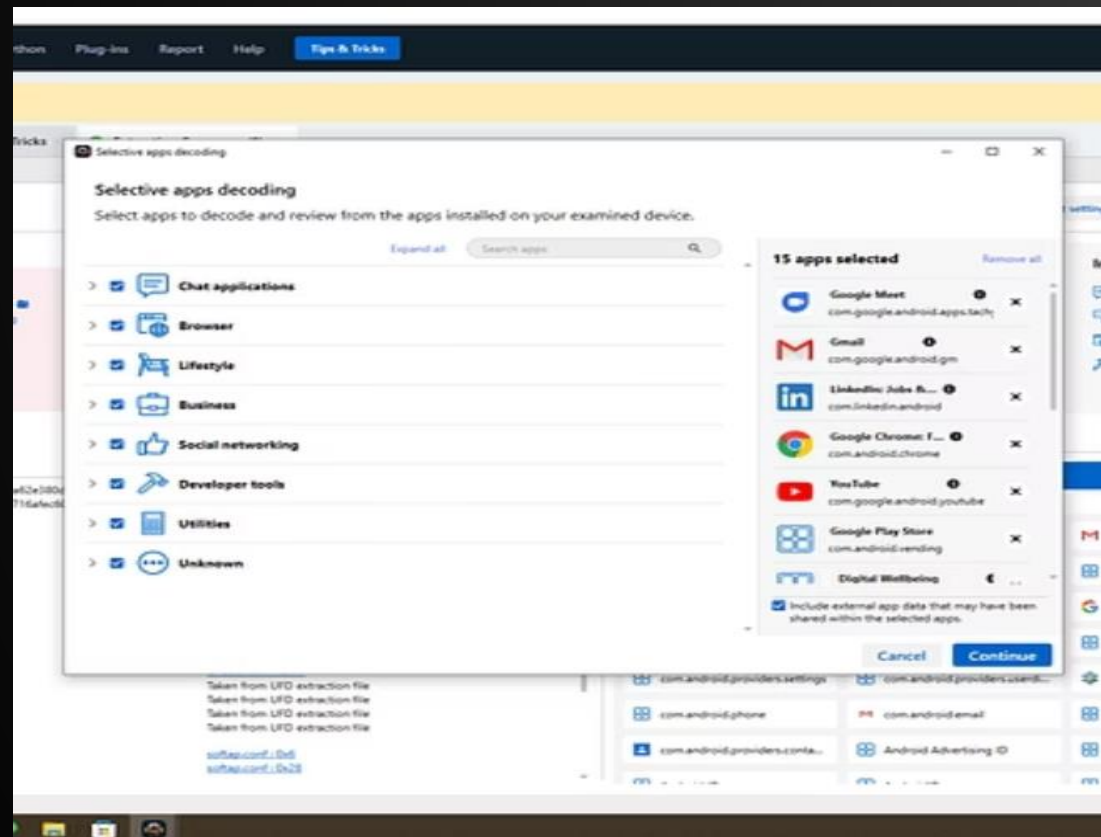
File System Analysis

- **Directory Navigation:** Access to Android file system directories (/data, /cache, /system) reveals application-specific data and system artefacts
- **Application Data:** Recovery of app-specific databases, configuration files, and cached data provides detailed communication and behavioral records
- **Deleted Artefacts:** Carving operations recover deleted communications, contact information, and transaction records deliberately removed by users
- **Metadata Extraction:** Timestamps, file sizes, and access logs establish temporal sequences and correlate with communication evidence
- **Evidence Integrity:** File system analysis maintains chain of custody and forensic documentation standards throughout examination



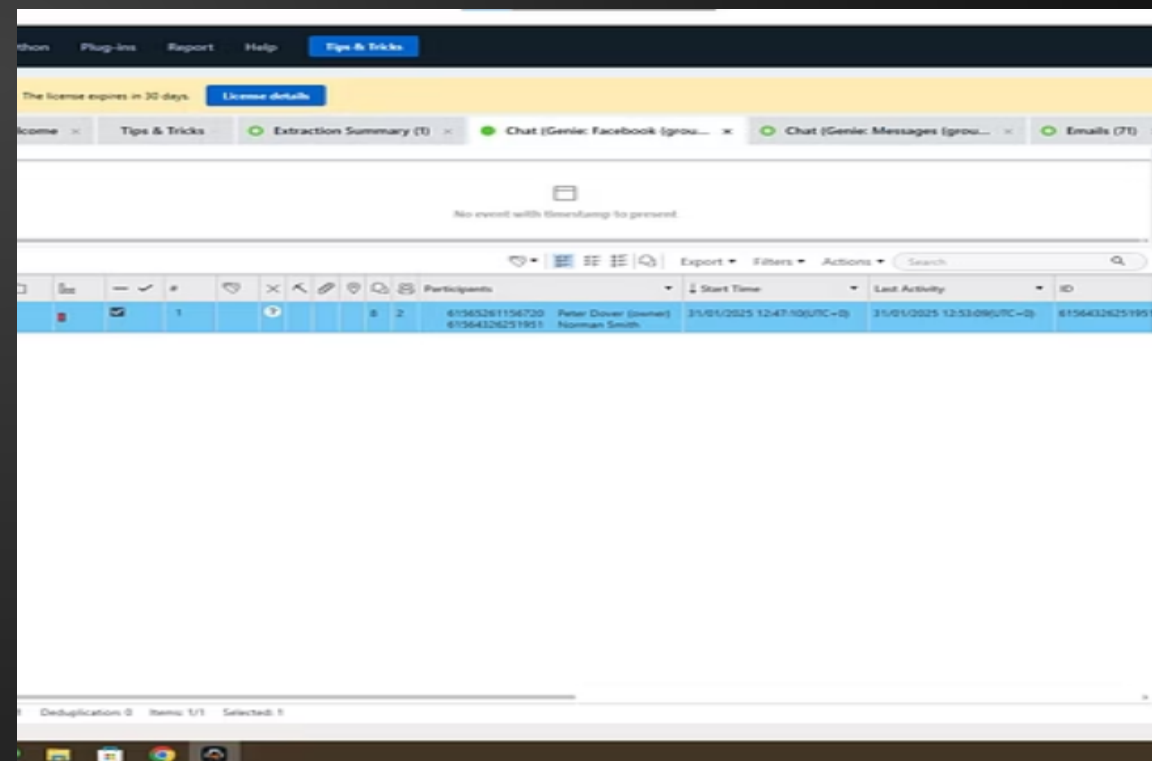
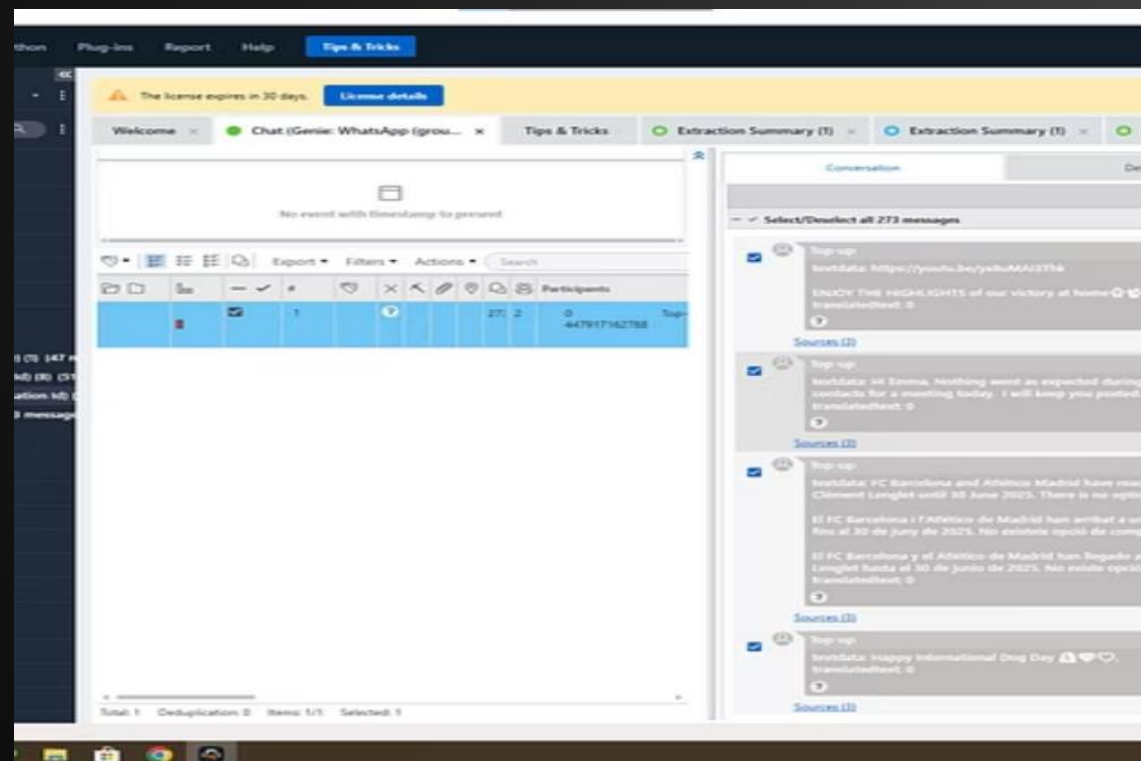
Initial Chat Evidence

- **WhatsApp Recovery:** Encrypted messaging communications extracted and decoded, revealing primary communication channel between parties
- **Communication Patterns:** Interactions between key individuals identified and analyzed, establishing relationship and coordination patterns
- **Temporal Analysis:** Message timestamps establish communication timeline, correlating with financial discussions and coordinated activities
- **Content Analysis:** Language and context of exchanges demonstrate planning, coordination, and awareness of activity nature
- **Evidence Foundation:** Chat data provides primary evidence source for establishing intent, coordination, and cross-platform correlation

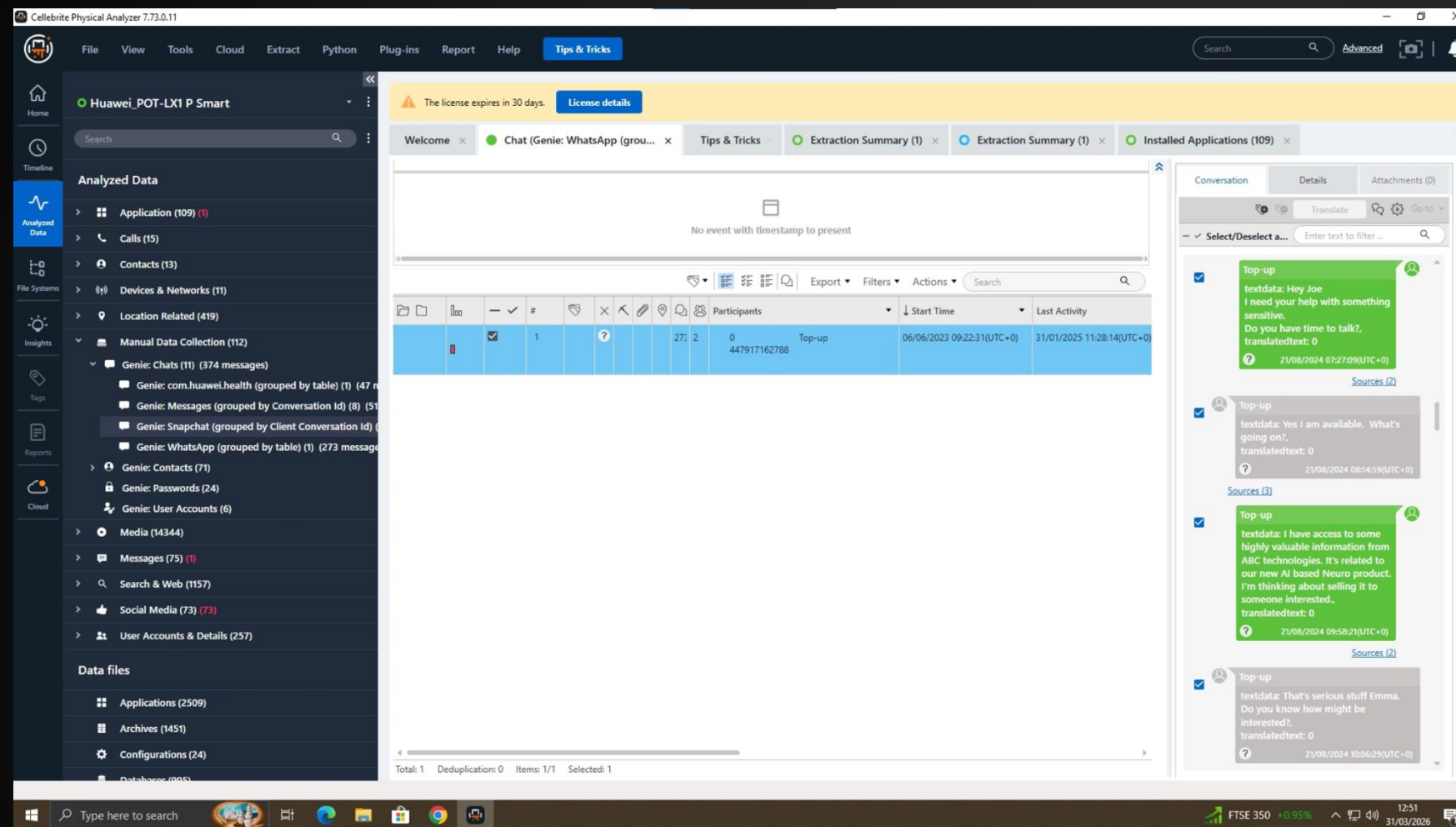


Advanced Chat Evidence

- **Time-Sensitive Coordination:** Messages establish scheduled actions and continuous updates, confirming planned coordination between parties
- **Coordination Evidence:** "Keep updating" and "48 hours" references demonstrate explicit coordination instructions and time-dependent activities
- **Temporal Significance:** Time-based instructions establish sequence of events and correlate with financial discussions and travel activity
- **Behavioral Pattern:** Ongoing communication demonstrates sustained coordination between parties, inconsistent with isolated or coincidental contact
- **Investigative Value:** Evidence confirms coordinated activity hypothesis and correlates with financial and travel evidence across multiple data sources



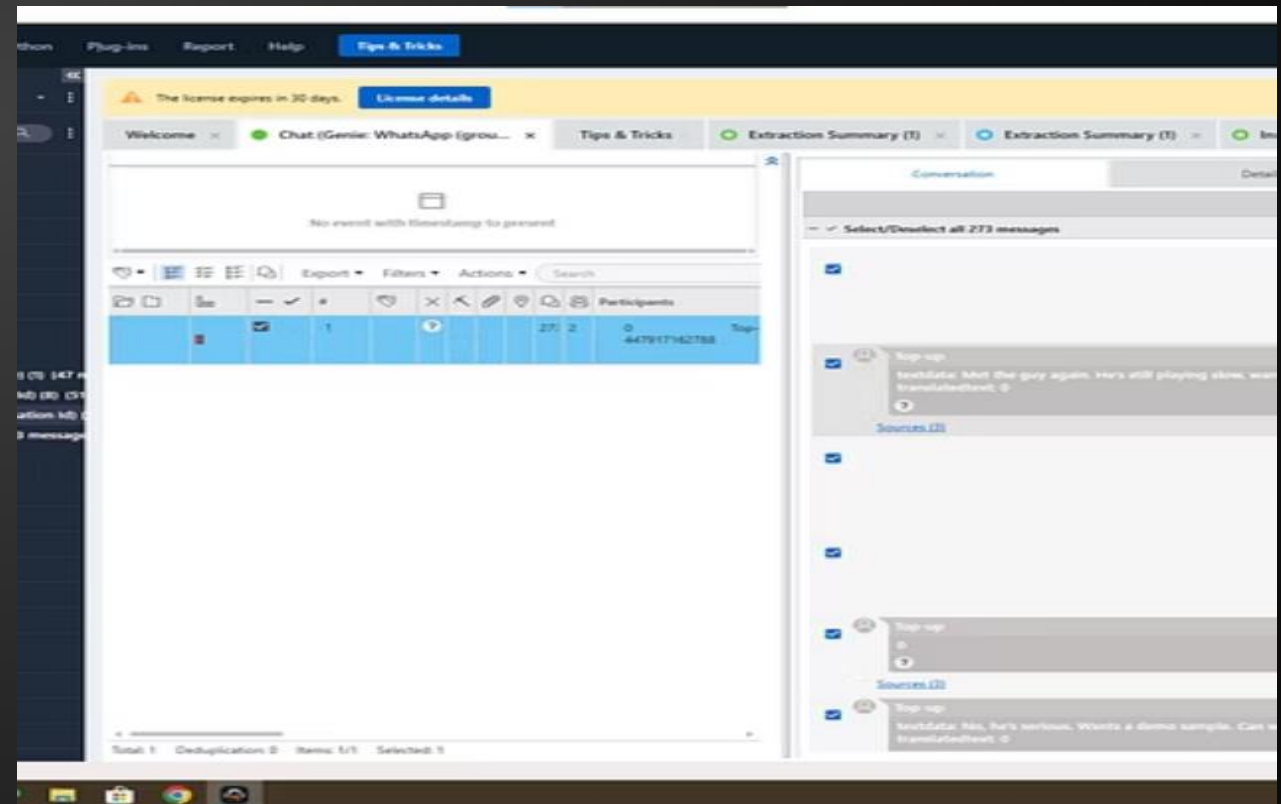
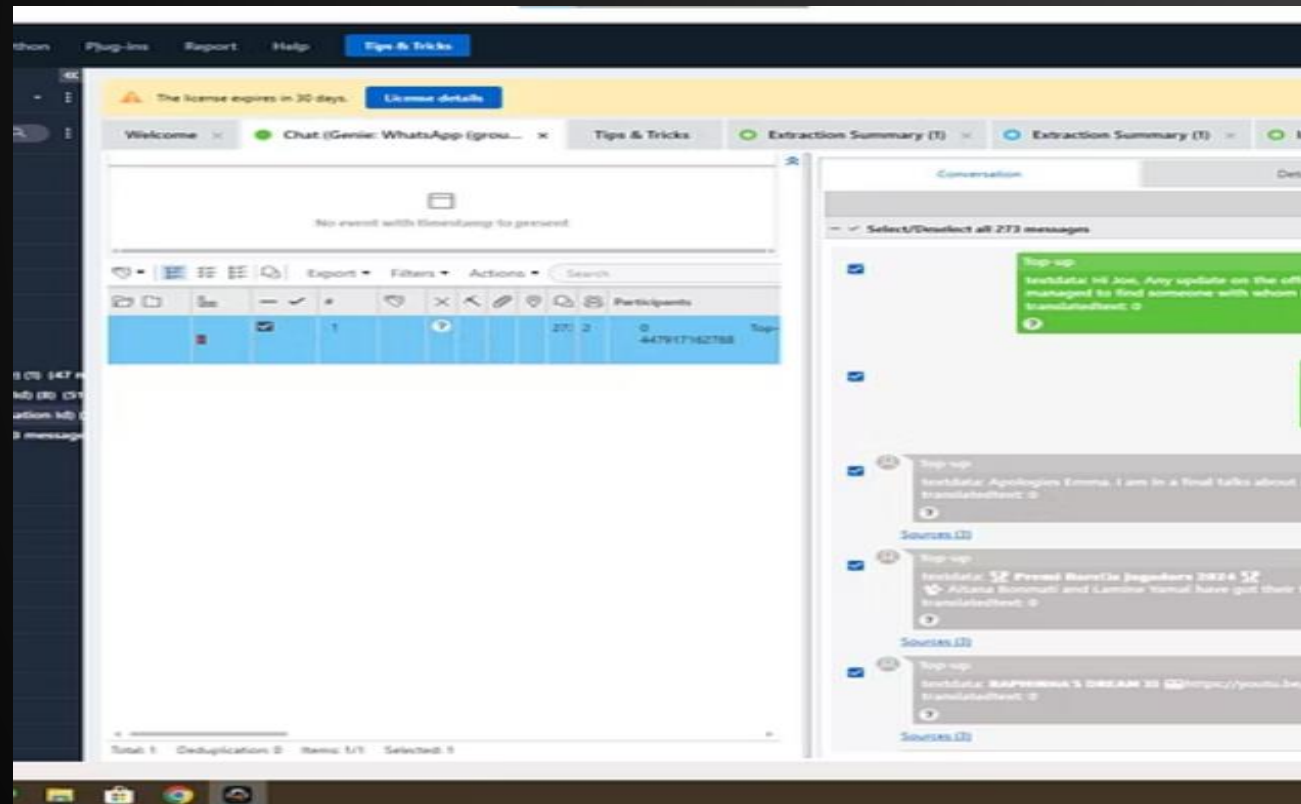
Initial Contact Evidence



- First Contact: Opening message initiates communication between parties, establishing temporal baseline for coordinated activity
- Greeting Pattern: Informal communication style confirms prior relationship or familiarity, suggesting established connection between parties
- Temporal Marker: Establishes initial point of contact in investigation timeline, correlating with subsequent financial and coordinated activities
- Behavioral Baseline: Sets foundation for analyzing subsequent communication patterns and establishing coordination progression
- Investigative Value: Identifies communication initiation point and confirms relationship establishment between Emma (primary perpetrator) and Joe (intermediary)

Financial Indicators

- Financial Intent: Messages establish monetary transactions and financial agreements, confirming financial motivation for coordinated activity
- Transaction Evidence: Large monetary values referenced in communications, correlating with coordinated activity timeline and travel evidence
- Negotiation Pattern: Multiple messages demonstrate discussion and agreement on financial terms, establishing deliberate transaction planning
- Deal Structure: Evidence confirms planned financial transactions between parties, with Emma initiating and Joe facilitating communication
- Investigative Significance: Financial communications establish motive, intent, and cross-platform coordination across chat, email, and contact evidence

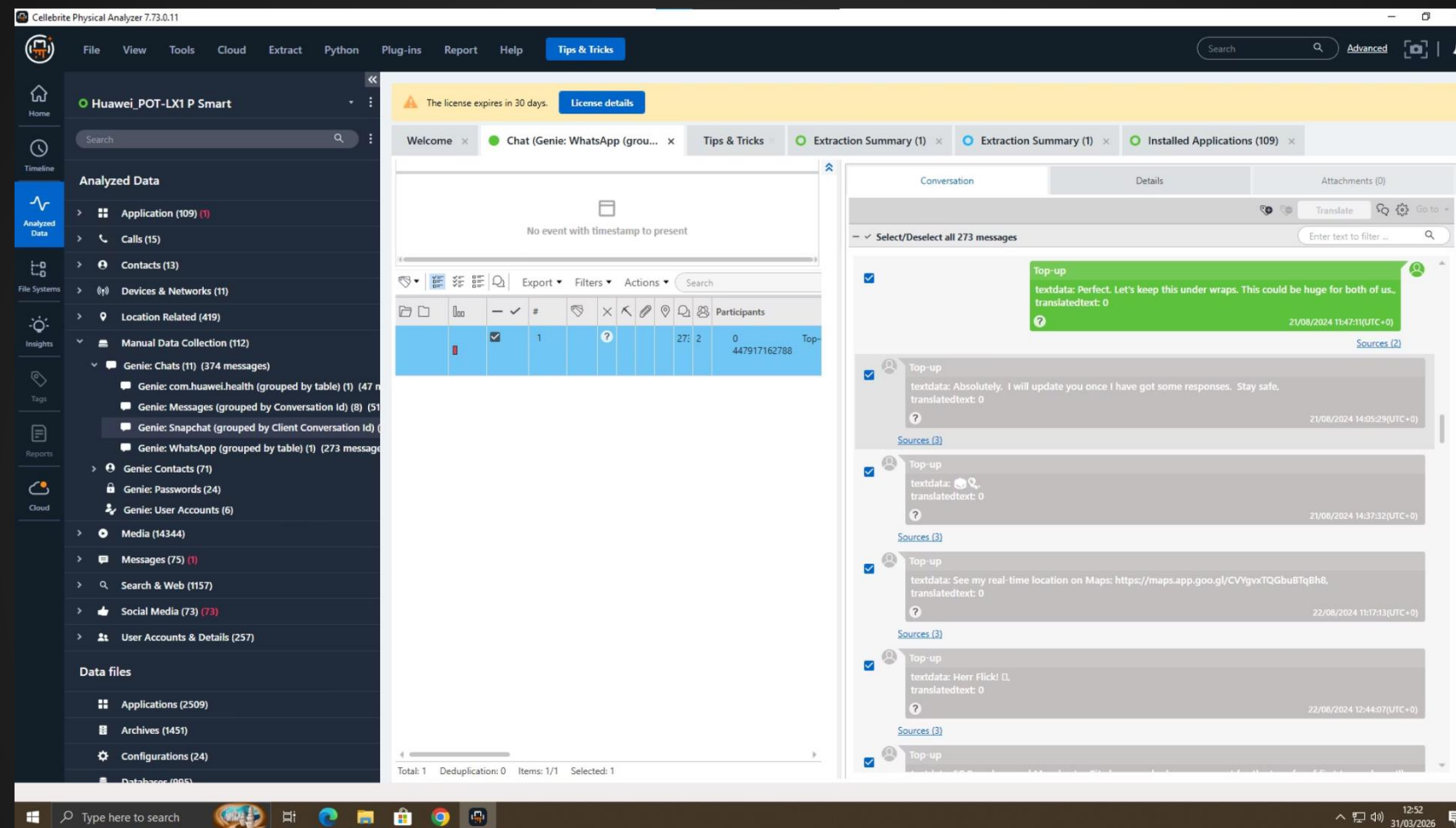


Travel & Physical Movement Evidence

Chat evidence referencing travel activity, linking digital communication with real-world movement.

- **Real-World Movement:** Chat evidence confirms travel to France, establishing physical manifestation of coordinated activity
- **Digital-Physical Link:** Digital communications correlate with physical location data, confirming activity extends beyond digital platforms
- **Timeline Correlation:** Travel dates align with communication patterns, financial discussions, and coordinated activity timeline
- **Investigative Significance:** Establishes suspect presence at specific locations during investigation period, confirming activity authenticity
- **Evidence Corroboration:** Travel evidence supports timeline analysis and validates communication authenticity across multiple data sources

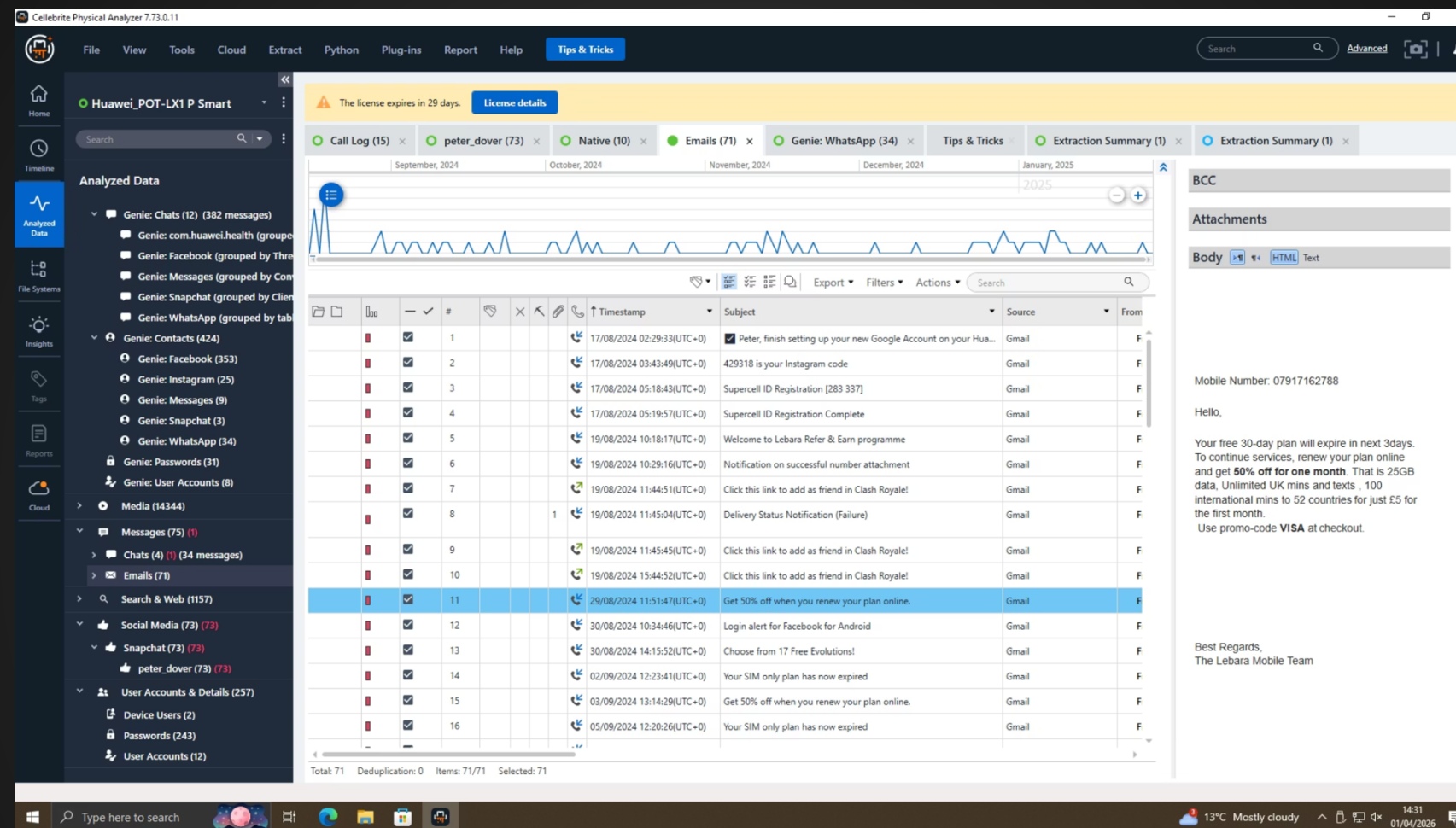
Confidentiality & Secrecy Evidence



Messages indicating deliberate concealment and confidentiality concerns

- **Secrecy Instructions:** Explicit requests to maintain confidentiality confirm awareness of activity nature and deliberate concealment strategy
- **Concealment Intent:** Evidence demonstrates deliberate effort to hide communications and activities, indicating consciousness of wrongdoing
- **Awareness of Wrongdoing:** Parties understood potentially illicit nature of activities, as evidenced by explicit secrecy instructions
- **Risk Mitigation:** Deliberate attempts to avoid detection and investigation confirm awareness of legal and investigative risk
- **Investigative Significance:** Consciousness of guilt demonstrated through concealment strategy, correlating with coordinated activity and financial intent

Contact Identification



Recovered contact details identifying key individual and enabling correlation with communication evidence.

- **Contact Recovery:** Phone number and contact details extracted from device, establishing direct communication link to key suspect
- **Suspect Identification:** Contact definitively linked to Emma, primary perpetrator identified through communication initiation and coordination patterns
- **Cross-Reference:** Contact details correlated with chat communications and email evidence, confirming identity across multiple data sources
- **Communication Mapping:** Establishes connection between digital identities and phone numbers, linking Emma across messaging platforms
- **Evidence Chain:** Contact information bridges multiple communication platforms, confirming Emma's central role in coordinated activity

Email Evidence

Email communication supporting cross-platform evidence and reinforcing behavioural patterns.

- **Cross-Platform Evidence:** Email communications supplement chat and contact evidence, establishing additional communication channel for coordination
- **Behavioral Patterns:** Email content reinforces patterns observed in messaging applications, confirming consistent coordination across platforms
- **Communication Channel:** Email provides additional communication platform linking key individuals, corroborating chat-based coordination evidence
- **Temporal Correlation:** Email timestamps align with chat activity and financial discussions, establishing coordinated timeline across data sources
- **Corroborating Evidence:** Email evidence strengthens investigative narrative by confirming coordination patterns across multiple independent platforms

Timeline Analysis



- Aug 2024: Initial contact between parties established
- Oct 2024: Information exchange and communication patterns intensify
- Jan 2025: Financial discussions and transaction planning documented
- Ongoing: Continuous coordination and activity monitoring
- Forensic Significance: Chronological reconstruction supports investigative hypothesis

Key Findings

- Coordinated Activity Confirmed: Multi-platform evidence establishes deliberate coordination between Emma (primary perpetrator), Joe (intermediary), and Norman (buyer)
- Financial Intent Established: Monetary discussions and transaction planning demonstrate clear financial motivation across chat, email, and contact evidence
- Temporal Correlation Demonstrated: Timeline analysis confirms coordinated activity progression from initial contact through financial discussions to travel activity
- Consciousness of Guilt Evident: Explicit secrecy instructions and concealment attempts confirm awareness of activity nature and legal risk
- Cross-Platform Consistency: Evidence patterns consistent across WhatsApp, email, contacts, and file system, establishing coordinated activity beyond isolated incidents

Conclusion

- Mobile Forensics Confirmed Coordinated Activity: Cellebrite Physical Analyzer recovered comprehensive evidence demonstrating deliberate coordination between three identified suspects
- Cross-Platform Correlation Established: Evidence from chat, email, contacts, and file system consistently confirms coordinated activity and suspect roles
- Temporal Analysis Validates Timeline: Chronological reconstruction from Aug 2024 through Jan 2025 establishes progression of coordinated activity and financial intent
- Suspect Roles Definitively Identified: Emma (primary perpetrator initiating activity), Joe (intermediary facilitating communication), Norman (buyer participating in transactions)
- Forensic Integrity Maintained: All examination steps documented and verified, ensuring evidence admissibility and investigative defensibility

References

NIST SP 800-101 (2023) - Guidelines for Mobile Device Forensics

ISO/IEC 27037 (2022) - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence

Casey, E. (2022) - Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th Edition)

ACPO (2012) - Good Practice Guide for Digital Evidence

Cellebrite (2024) - Physical Analyzer Technical Documentation and Forensic Standards

Thank You

Digital evidence never lies — it only waits to be discovered.

Presented by Vanshaj Patel