



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 7

Mobile, Drone and IoT Forensics

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



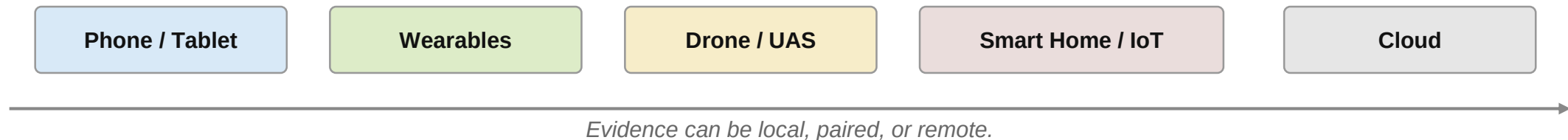
www.uwtsd.ac.uk

Objectives

- Explain how mobile investigations now extend to drones, wearables, smart-home devices, and cloud services.
- Distinguish common acquisition levels: manual review, logical extraction, file-system access, and advanced physical methods.
- Identify the artifacts most useful for communications, app usage, media, timeline reconstruction, and location evidence.
- Apply timeline analysis to correlate events across devices, apps, networks, and cloud accounts.
- Interpret geolocation evidence with appropriate caveats, confidence levels, and reporting limitations.

Expanding Scope of Mobile Forensics

- Modern cases rarely involve a single handset; evidence often spans paired devices and vendor clouds.
- A phone may act as the control point for a drone, wearable, vehicle app, smart lock, or camera ecosystem.
- Examiners should map the whole ecosystem before acquisition so that linked evidence is not overlooked.



Evidence Sources in the Mobile Ecosystem

On-device

- SIM / eSIM identifiers and subscriber data
- Messages, call logs, contacts, and browser history
- Photos, videos, EXIF metadata, and downloaded files
- App databases, caches, and authentication tokens

Paired and remote sources

- Cloud backups, sync services, and account history
- Wearables, vehicle systems, and companion apps
- Cell-site, Wi-Fi, and provider records
- External media, crash logs, and shared storage

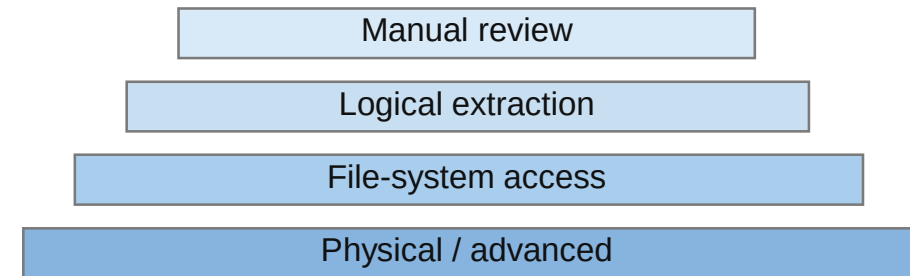
Acquisition Levels and Their Trade-Offs

- The deeper the access, the more artifacts may be available; however risk, cost, and legal complexity also increase.
- Encryption, secure enclaves, and vendor restrictions can limit or prevent advanced extraction.



Acquisition Levels and Their Trade-Offs (cont.)

- Manual: visible content only; useful when immediate triage is lawful and safe.
- Logical: extracts data exposed through the OS or backup interfaces.
- File system: provides broader access to app databases and artifacts.
- Physical / advanced: may recover lower-level data, but support varies by model.



Chip-off / JTAG / specialized vendor methods

Mobile forensics acquisition with UFED Cellebrite

Logical

SMS

Contacts

Call logs

Media

App data

File System

SMS

Contacts

Call logs

Media

App data

Files

Hidden Files

Physical

SMS

Contacts

Call logs

Media

App data

Files

Hidden Files

Deleted data

Mobile Data Decoding

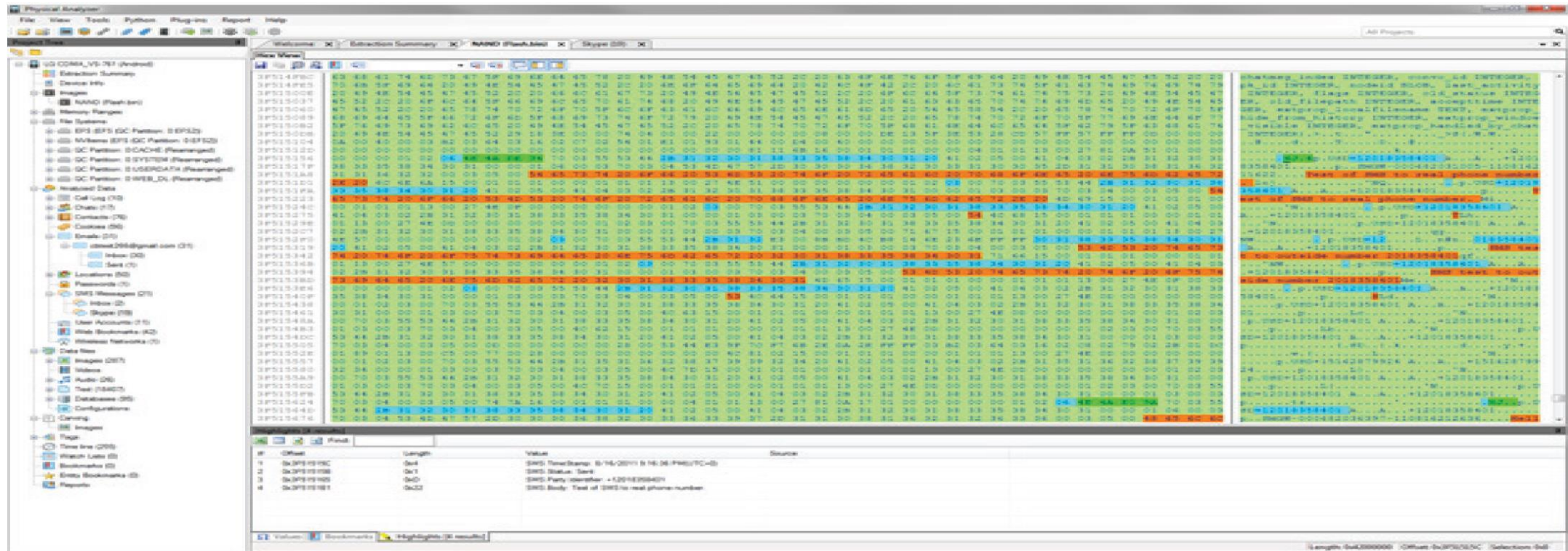


Figure 1: UFED Physical Analyzer displays data in human-readable format, as well as in its raw state as stored on the device.

Mobile Device Analysis Basics

- Guidelines for seizing:
 - If already off, do not turn it on
 - Seal in an envelope before putting it in an evidence bag to restrict access
 - Attach the power adapter through the evidence bag to maintain the charge
 - Keep active state if it is on when found
 - Search should be conducted for associated memory devices
 - Any power leads, cables, or cradles relating to the device should also be seized, as well as manuals
 - Anyone handling before their examination should treat them in such a manner that gives the best opportunity for any recovered data to be admissible as evidence in any later proceedings

Scene Handling and Preservation

- Document the device state at seizure: screen status, power, network connectivity, damage, and peripherals.
- Prevent remote changes where appropriate by isolating radio connections, while balancing the risk of losing volatile data.
- Preserve power when necessary, especially for unlocked devices, companion controllers, and wearables.
- Seize associated items: chargers, cables, SIM trays, SD cards, controllers, paired phones, hubs, and manuals.
- Record legal authority, chain of custody, acquisition decisions, and any safety steps taken.

General forensic principles still apply: document, isolate, preserve, acquire, verify, and report.

Core Mobile Artifacts

Communications

- Calls, SMS, chat apps, email, voicemail
- Contacts, account metadata, block lists

Application and browser data

- Databases, caches, tokens, search history
- Maps, rideshare, delivery, finance, health

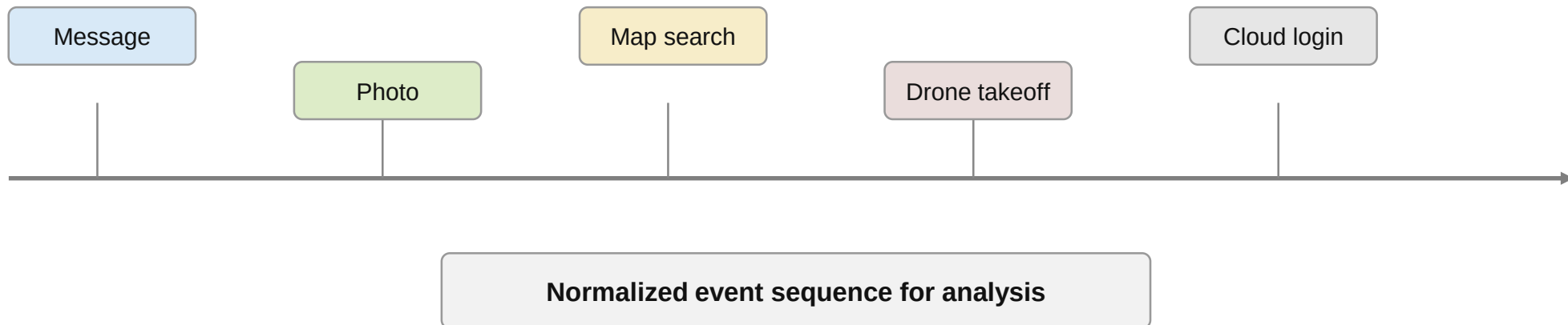
Media and sensors

- Photos, video, EXIF, audio, screenshots
- Location, motion, health, nearby-device logs

Analysts should review both parsed artifacts and unparsed files because app updates and unsupported formats often leave useful traces outside the default tool view.

Timeline Analysis

- Timeline analysis reconstructs events by normalizing timestamps from multiple sources into a single sequence.
- It is especially valuable when activity spans a phone, a drone controller, cloud logs, and nearby IoT devices.



A reliable timeline requires time-zone handling, clock validation, and source attribution.

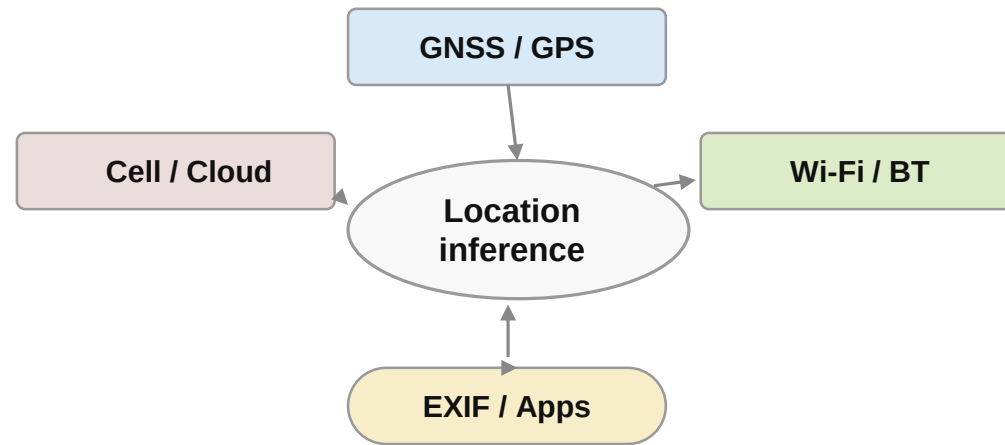
Timestamp Sources and Normalization Issues

Source	Examples	Common caveats
Filesystem	Created / modified / accessed times	Different semantics by OS and app
Application	Chats, health logs, map queries, cache records	May use local time, epoch, or app-specific formats
Network / provider	Carrier records, Wi-Fi logs, cloud access	Retention and granularity vary
Sensor / telemetry	EXIF, GNSS, flight logs, wearable events	Clock drift and sync errors may exist

Always record the original timestamp, the interpreted timezone, and the normalized time used in the report.

Geolocation Evidence

- Location can be inferred from GNSS / GPS records, cell-site data, Wi-Fi and Bluetooth proximity, and application activity.
- Photos, videos, map searches, route history, rideshare logs, and health records can all contain location clues.
- For drones, flight logs may include home point, takeoff / landing coordinates, altitude, and route telemetry.



Interpreting Geolocation Safely

- Treat location as an estimate, not a certainty; always preserve source, precision, and confidence information.
- A coordinate may describe a device, a controller, a home point, or a network observation rather than the person of interest.
- Indoor use, urban canyons, spoofing, stale caches, and manually edited metadata can all mislead analysis.
- Corroborate location with independent evidence such as messages, photos, CCTV, access logs, or drone telemetry.

Confidence ladder

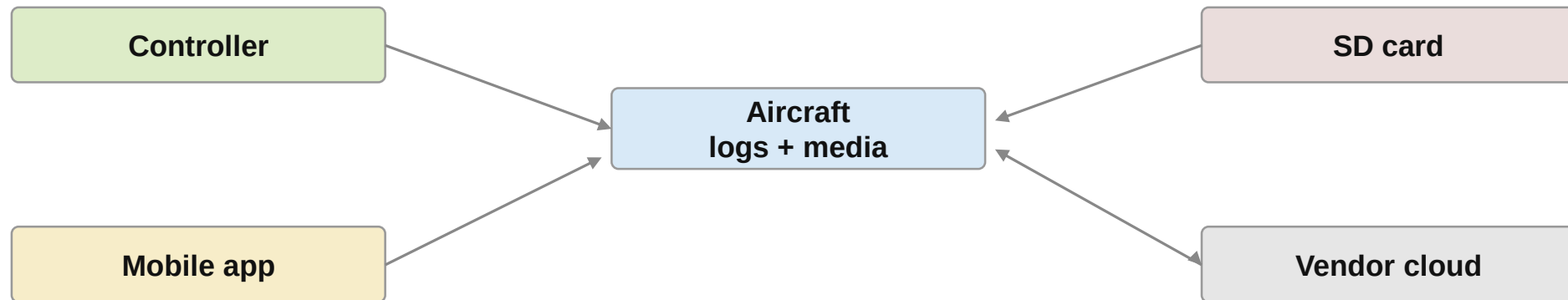
High: corroborated by multiple sources

Medium: single technical source

Low: approximate or user-editable

Drone / UAS Forensics Overview

- Drone investigations often require evidence from the aircraft, remote controller, mobile control app, removable media, and vendor cloud accounts.
- Pairing information, serial numbers, firmware versions, and flight logs can link the aircraft to a specific controller or phone.



Drone Seizure and Preservation

- Safety comes first: secure propellers, batteries, and damaged hardware before evidence handling.
- Photograph device state, mounted payloads, controller screens, memory cards, and connected mobile devices.
- Seize all paired components because flight logs may be split across the aircraft, controller, app, and cloud account.
- Document network state, remote ID information when available, and any actions taken to prevent further flights or remote sync.

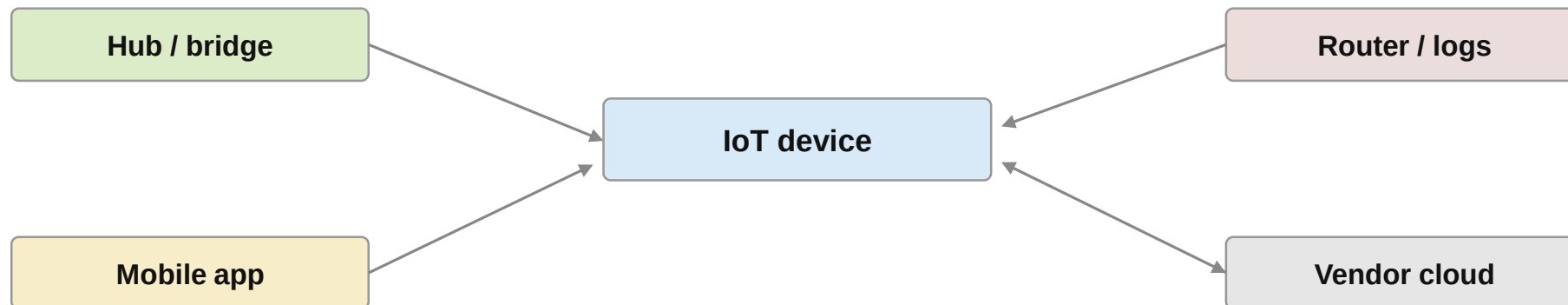
A powered aircraft or controller may contain volatile data, but powering decisions must be safe and legally authorized.

Drone Artifacts and Analytical Value

Artifact	Examples	Why it matters
Flight logs	Takeoff, landing, speed, altitude, home point	Reconstruct flight behavior and timeline
Media + EXIF	Photos, video, previews, thumbnails	Show payload use, route, or target area
Identifiers	Serials, pairing records, firmware	Link aircraft, controller, and owner
Map / geofence data	Restricted zones, cached maps, route plans	Provide intent and location context

IoT Forensics Overview

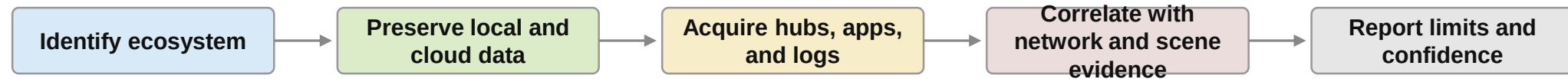
- IoT evidence may come from cameras, smart speakers, locks, thermostats, trackers, watches, appliances, vehicles, and industrial sensors.
- The key challenge is that data is often distributed across the device, local hub, smartphone app, router, and vendor cloud.



IoT Acquisition Challenges

- Proprietary firmware, undocumented filesystems, and limited tool support are common.
- Logs may be small, volatile, overwritten quickly, or dependent on continuous cloud connectivity.
- Many devices have weak or inconsistent clocks, which complicates event reconstruction.
- Evidence may require collecting companion apps, hubs, packet captures, cloud exports, and physical scene data together.

IoT Evidence Workflow



Do not examine an IoT device in isolation; the surrounding ecosystem often contains the most useful evidence.

Tools and Platforms

Mobile

- Cellebrite UFED / Physical Analyzer
- MSAB XRY
- Magnet AXIOM
- Oxygen Forensic tools

Timeline / correlation

- Autopsy
- plaso / log2timeline
- Timesketch
- AXIOM and other suite timeline views

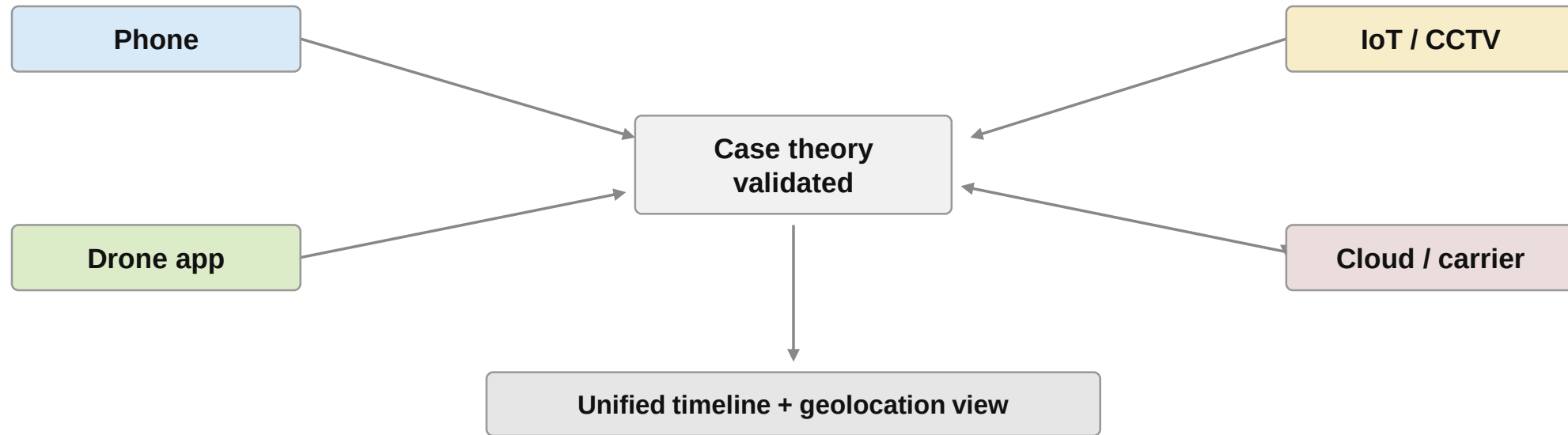
Drone / IoT

- Vendor viewers and exports where supported
- DatCon / CsvView for DJI-related parsing
- Packet capture, router logs, firmware tools
- Cloud account exports and API logs

Tool support depends on device model, OS / firmware version, and lawful access conditions.

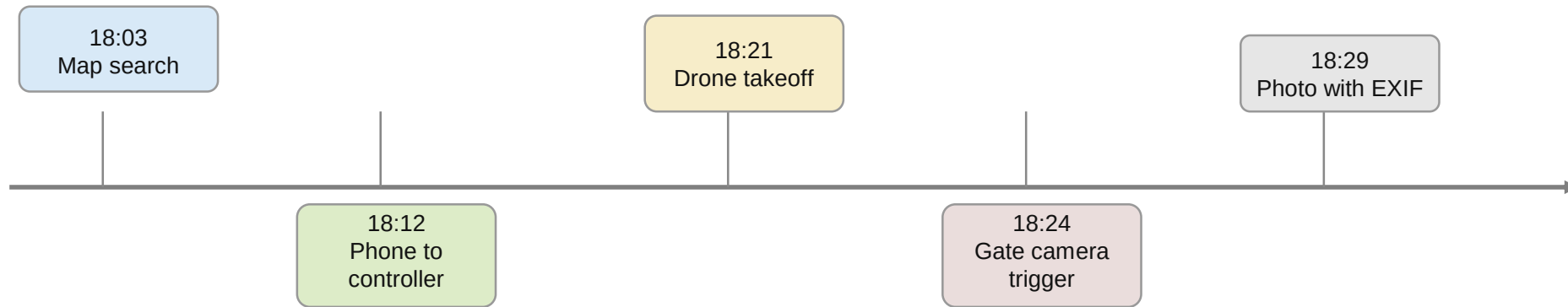
Correlation Across Ecosystems

The strongest findings often come from corroboration rather than any single artifact.



Illustrative Case Timeline

Example only: a combined mobile + drone + IoT scenario



A timeline becomes persuasive when each event is linked to a specific source and confidence level.

Reporting Best Practices

- State what was acquired, how it was acquired, and what could not be acquired.
- Record hashes, tool versions, device identifiers, time-zone assumptions, and any normalization steps.
- Separate observed facts from interpretation; include alternative explanations where needed.
- Explain geolocation confidence, timeline gaps, unsupported artifacts, and any signs of anti-forensics or data loss.
- Use clear exhibits so another examiner can reproduce the analytical path.

Challenges and Limitations

- Strong encryption and secure hardware may limit recovery even with lawful authority.
- Remote wipe, anti-forensic behavior, and vendor lock-in can reduce evidential completeness.
- IoT and drone ecosystems evolve quickly, so unsupported formats and proprietary logs are common.
- Legal, privacy, and safety issues are often more complex than in a traditional single-device examination.

iOS Forensic Considerations

- Common artifacts include app containers, SQLite and plist files, keychain-linked records, media metadata, backups, and account sync traces.
- Depth of access depends heavily on the device model, iOS version, lock state, and the supported acquisition method.
- Hardware-backed encryption and the Secure Enclave can limit access to protected data even when the device is physically available.
- Investigators should correlate handset findings with backups, cloud data, companion devices, and geolocation artifacts where lawful.

Android Forensic Considerations

- Android workflows vary widely across manufacturers, chipsets, Android versions, bootloader states, and security patches.
- Useful evidence may appear in app sandboxes, SQLite or XML stores, external storage, notifications, Wi-Fi and Bluetooth history, and usage logs.
- File-based encryption, verified boot, and OEM-specific protections can restrict physical or privileged access.
- Correlate Android artifacts with Google / app cloud accounts, paired wearables, vehicles, and nearby-device evidence.

Advanced Physical Acquisition: JTAG, ISP, and Chip-Off

- Advanced hardware methods are usually reserved for damaged devices or cases where less invasive acquisition fails.
- JTAG or ISP may access memory in-circuit on supported devices; chip-off removes memory for direct reading in a programmer.
- These methods can recover raw memory images, but may lose filesystem context and often cannot bypass modern hardware-backed encryption.
- Chip-off is high-risk and potentially destructive, so every step, adapter, image file, and hash must be documented carefully.

JTAG / ISP

Chip-off

Destructive risk

Best for damaged / legacy support

Chain of Custody, Faraday Bags, and Mobile Isolation

Chain of custody

- Record date, time, location, seizing officer, device state, identifiers, and accessories.
- Document each transfer, storage location, examination step, and any action taken on the device.

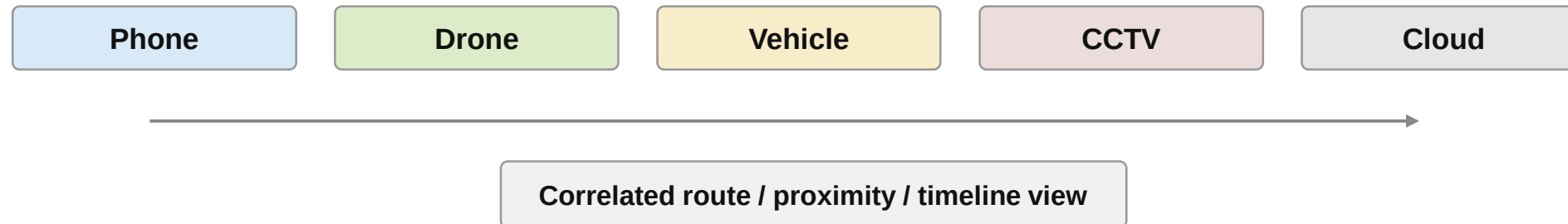
Isolation and Faraday handling

- Use airplane mode if it can be enabled safely; otherwise use an RF-blocking container such as a Faraday bag or box.
- A shielded device may consume more battery while seeking signal, so preserve power if it must remain on.
- Verify shielding effectiveness and note the decision in the case record.

Isolation decisions should preserve evidence while avoiding unnecessary changes to the device state.

Geolocation Correlation Across Sources

- Strong location findings usually come from correlation: GNSS, cell and Wi-Fi, EXIF, map searches, drone telemetry, vehicle data, and CCTV.
- Normalize timestamps first, then compare coordinates, proximity events, routes, and gaps or contradictions.
- Always distinguish between the location of a person, the mobile device, a vehicle, and a drone controller or aircraft.



Vehicular Forensics

- Modern vehicles may store evidence in infotainment systems, telematics modules, navigation history, Bluetooth pairings, call logs, contacts, and recent destinations.
- Vehicle systems often preserve traces of Android Auto, Apple CarPlay, charging, USB pairing, and connected-phone activity.
- Vehicular evidence should be correlated with the handset, cloud accounts, provider records, and geolocation timeline rather than treated in isolation.
- Collection may require OEM-specific workflows and care to avoid changing system state or overwriting logs.

Infotainment / IVI

Telematics / GPS

Phone pairing traces

Navigation history

Summary

- Mobile forensics now commonly intersects with drones, wearables, smart-home devices, vehicles, and cloud services.
- iOS and Android require different workflows, while chip-off and other hardware methods are last-resort techniques.
- Chain of custody, RF isolation, Faraday handling, and power decisions are critical to defensible mobile evidence collection.
- The strongest findings come from correlating handset, drone, vehicle, IoT, network, cloud, timeline, and geolocation evidence.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk