



SPECTRUM

DIGITAL TRAINING

CYBER KNOWLEDGE • REAL WORLD IMPACT

DIGITAL INVESTIGATIONS NEWS LETTER | 1st OCTOBER 2026

ANDROID PRIVACY FEATURES

A modern Android phone may contain more than one digital environment. Secure folders, private spaces, app cloning and separate user profiles can keep accounts, applications and files outside the main view of the handset. Investigators should understand how these features operate before drawing conclusions from a routine examination.

ONE HANDSET, MULTIPLE DIGITAL SPACES

Privacy features are not inherently suspicious. They are widely used to separate work and personal activity, protect sensitive information, and prevent other people using a shared device from accessing private content. However, they can also change where relevant material is stored and how it appears during an examination.

FEATURES TO RECOGNISE

- Samsung Secure Folder – A Knox-protected space with separate app instances, files and accounts; access may require additional authentication.
- Android Private Space – Available on supported Android versions; a separate, lockable space for apps that can be hidden when locked.
- Multiple users / guest mode – Distinct Android user environments with their own applications, settings and data.
- Work profiles – Managed separation of work and personal applications and data; enterprise policy can affect visibility and access.
- Dual Messenger / cloned apps – Second instances of supported messaging or social apps, potentially signed in to different accounts.
- Manufacturer app locks and hidden apps – Vendor-specific controls may conceal apps from the launcher or require authentication without creating a separate encrypted profile.

WHY USERS ENABLE THESE FEATURES

Common reasons include family privacy, confidential work communications, protection of banking or identity documents, maintaining multiple accounts and sharing a device safely. The presence of a private space alone does not demonstrate illicit conduct.

WHAT MAY CHANGE FOR AN INVESTIGATOR?

- The home screen or app drawer may not reveal every installed application or user profile.
- An app may have a separate account, database, notification history and storage location in another space.
- Access controls, encryption and device state may limit what can be lawfully recovered.



SPECTRUM

DIGITAL TRAINING

CYBER KNOWLEDGE • REAL WORLD IMPACT

LOOK BEYOND THE MAIN PROFILE

A practical approach to documenting Android privacy features without changing device state unnecessarily.

INITIAL EXAMINATION: OBSERVE AND RECORD

- Photograph visible screens, lock state, notifications and any displayed private-space or secure-folder indicators.
- Record make, model, Android version, manufacturer interface and relevant security-patch information.
- Document observed user-profile indicators, work-profile icons, cloned-app badges and available settings without speculative interaction.
- Preserve the current power and network state under applicable policy and seek specialist advice before rebooting, unlocking or changing profiles.

SAMSUNG, PIXEL AND OTHER MANUFACTURERS

Terminology and implementation vary between manufacturers and Android versions. Samsung Secure Folder is not identical to Android Private Space; app-cloning features on Xiaomi, OnePlus and other handsets may behave differently again. A feature's name does not establish its encryption, isolation or forensic recoverability.

INVESTIGATIVE OPPORTUNITIES

Where lawful and proportionate, consider associated cloud accounts, app-provider records, backups, synced devices, notifications, connected computers and network artefacts. Separate profiles may use different accounts. Corroborate identity and activity rather than assuming that two instances of an app belong to the same user.

COMMON ASSUMPTIONS TO AVOID

- A missing app icon does not prove the app was never installed or used.
- A second app instance does not necessarily share data with the first.
- A locked private area does not mean its contents can be accessed by standard extraction tools.
- A hidden or secured area is not, by itself, evidence of criminal intent.

NOTE: Forensic software available to Law Enforcement will not ordinarily identify hidden services, or extract data from these hidden services.

Neil Greenough | Spectrum Digital Training Ltd ©