Android App Data And Third Party Application Forensics

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/android-app-data-and-third-party-application-forensics

ANDROIDAPPDATA · A GUIDE FOR UK LAWYERSAndroid App Data and Third-Party ApplicationForensicsSandboxes, Sideloading and the Open Ecosystem: Every App Its Own World, andSome Worlds Stranger Than OthersCOMPUTER FORENSICS LAB§ ABOUT THE AUTHORPREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAMFULL CHAIN-OF-CUSTODY DOCUMENTATION§ CONTENTSIn this guide01 Executive summary02 The problem in plain English: an open ecosystem of worlds03 How Android apps store their data04 What the open ecosystem adds05 Inventorying and recovering app data06 Interpretation, attribution and honest limits07 Deployment: the evidence inside the apps08 Source architecture: where else the evidence lives09 Worked examples10 Common mistakes and technical limitations11 Questions to ask · Suggested wording12 Checklist and red flags · When to involve a digital forensic expert13 Frequently asked questions14 Glossary · References · Disclaimer · How a specialist laboratory can assist§ 01 · ORIENTATIONExecutive summaryfiles that must be under stood on their own terms, and the open ecosystem adds dimensions iOS lacks,sideloaded and obscure apps, cloned and "dual" apps running second accounts, app data on the SD card, andselective Google backup, so the apps must be inventoried including the unexpected ones, each under stoodprecisely, and the evidence inside recovered and attributed with care.§ 02 · FIRST PRINCIPLESThe problem in plain English: an open ecosystem of worlds§ 03 · HOWAPPSSTOREDATAHow Android apps store their data§ 04 · WHATOPENNESSADDSWhat the open ecosystem adds§ 05 · INVENTORYANDRECOVERYInventorying and recovering app data§ 06 · INTERPRETATIONANDHONESTLIMITSInterpretation, attribution and honest limits§ 07 · DEPLOYMENTDeployment: the evidence inside the apps§ 08 · THEWIDERMAPSource architecture: where else the evidence livesEVIDENCE COUNTERPARTAPP EXTERNAL / GOOGLE APP CLOUD / PROVIDERSANDBOX SD CARD BACKUP ACCOUNT RECORDS§ 09 · IN THE WILDWorked examplesEXAMPLE1 · THESECONDWHATSAPPTHEINVENTORYREVEALEDEXAMPLE2 · THECALCULATORTHATWASAVAULTEXAMPLE3 · THEMODIFIEDAPPTHATBEHAVEDDIFFERENTLY§ 10 · WHEREITGOESWRONGCommon mistakes and technical limitationsCommon mistakesTechnical limitations§ 11 · INTERROGATORIES & DRAFTING AIDSQuestions to ask · Suggested wordingAsk your clientAsk your opponentAsk your e Discovery / forensic providerSUGGESTED WORDING · INSTRUCTIONFORANANDROIDAPPANA LY SIS2. Please, on the acquired device at sufficient depth and preserving integrity: (1) enumerate every installed§ 12 · QUICK CONTROLChecklist and red flags · When to involve a digital forensicexpertThe Android app checklistRed flagsWhen to involve a digital forensic expert§ 13 · COMMON QUESTIONSFrequently asked questionsHow does Android app forensics differ from iPhone app forensics?What is a cloned or dual app?Can apps really be hidden on a phone?Why verify an app's version and whether it's modified?Is app data backed up to the Google account?Does

app activity prove the phone's owner did it?§ 14 · REFERENCEGlossarySources and authoritative referencesDISCLAIMER§ HOW A SPECIALIST LABORATORY CAN ASSISTWorking with Computer Forensics LabSpeak to a forensic examiner, not a salesperson.INSTRUCTTHELABNEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

How does Android app forensics differ from iPhone app forensics?

The core is the same; the openness adds more (

What is a cloned or dual app?

A second copy of an app running under a different account on the same phone (

Can apps really be hidden on a phone?

Yes, and the open ecosystem makes it easy (

Why verify an app's version and whether it's modified?

Because a modified app behaves differently, and reading it as genuine produces confident nonsense (

Does app activity prove the phone's owner did it?

It shows account activity; attributing it to a person takes care, and cloned apps make this more important (