Android Forensics The Fragmented Landscape

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/android-forensics-the-fragmented-landscape

ANDROIDFORENSICS · A GUIDE FOR UK LAWYERSAndroid Forensics: The FragmentedLandscapeWhy No Two Android Phones Are Alike, and What That Means for the EvidenceCOMPUTER FORENSICS LAB§ ABOUT THE AUTHORPREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAMESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURESANDROID FORENSICS ACROSS MANUFACTURERS PER-DEVICE FEASIBILIT Y ASSESSMENTCPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION§ CONTENTSIn this guide01 Executive summary02 The problem in plain English: a landscape, not a platform03 The sources of fragmentation04 How fragmentation shapes acquisition05 What is consistent across Android06 Assessing this device: feasibility and honest expectations07 Deployment: getting the most from the device in hand08 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 summaryThe headline point: Android is not one platform but a fragmented landscape of manufacturers, models,for this device, this model, this version and this security state, which must be assessed before expectations areset.§ 02 · FIRST PRINCIPLESThe problem in plain English: a landscape, not a platform§ 03 · THESOURCESOFFRAGMENTATIONThe sources of fragmentation§ 04 · ACQUISITIONHow fragmentation shapes acquisition§ 05 · WHATISCONSISTENTWhat is consistent across Android§ 06 · ASSESSINGTHISDEVICEAssessing this device: feasibility and honest expectations§ 07 · DEPLOYMENTDeployment: getting the most from the device in hand§ 08 · THEWIDERMAPSource architecture: where else the evidence livesEVIDENCE (DEPTH BACKUPSDEVICEVARIES)GOOGLE MANUFACTURER PAIRED / PROVIDER /ACCOUNT CLOUD COUNTERPART CARRIER§ 09 · IN THE WILDWorked examplesEXAMPLE1 · THETWOANDROIDSTHATBEHAVEDNOTHINGALIKEEXAMPLE2 · THEUPDATETHATCLOSEDTHEDOOREXAMPLE3 · THECOMMONCORETHATMADETHEANALYSISPOSSIBLE§ 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 · INSTRUCTIONFORANANDROIDFEASIBILITYASSESSMENTAND ACQUISITION§ 12 · QUICK CONTROLChecklist and red flags · When to involve a digital forensicexpertThe Android landscape checklistRed flagsWhen to involve a digital forensic expert§ 13 · COMMON QUESTIONSFrequently asked questionsWhy is Android so different from iPhone forensic all y?What can be recovered from an Android phone?Does the acquisition method matter more on Android?Can an update really change what's possible?Is anything the same across all Android

phones?What if the specific Android device yields very little?§ 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

Why is Android so different from iPhone forensic all y?

Because it is a landscape, not a platform (

What can be recovered from an Android phone?

There is no general answer, only an answer for the specific device (

Is anything the same across all Android phones?

Yes, a common core beneath the variation (