Forens

SAMPLE REPORT — Fictional account data for demonstration

Digital Forensic Report

Report ID FA-SAMPLE-001 · January 30, 2026 at 2:14 PM · SAMPLE

Risk Score: 78/100

High

12 findings across 3 data sources. Analysis date: January 28–30, 2026.

Executive Summary

Analysis Summary

This SAMPLE report shows the digital forensic documentation included with a Forens answer. The fictional account data below illustrates a high-risk pattern: overnight logins from a city the owner does not visit, a new trusted device, an unrecognized iPhone on Apple ID, Instagram sessions from the same metro area, a recovery-email change attempt, an app password, and a mail forwarding rule.

Overall risk assessment: High (78/100). Multiple high-severity events cluster overnight and across Google, Apple, and Instagram — consistent with someone else gaining and keeping access.

Significant Findings Overview

- Login from a city the owner does not travel to (Google)
- New Windows device trusted minutes later (Google)
- iCloud sign-in on unknown iPhone (Apple)
- Unrecognized Instagram session from Austin (Instagram)
- Recovery email change attempted (Google)
- App password created (Google)
- Mail forwarding rule to external address (Google)
- Second overnight Austin login reinforcing the pattern (Google)

Immediate Recommendations

- Change passwords on Google, Apple, and Instagram and sign out other sessions.
- Turn on or re-check two-factor authentication on every account.
- Remove unrecognized devices, app passwords, and mail forwarding rules.
- Keep this report. Monitor for new overnight or out-of-town activity.

Methodology

Scope of Analysis

- Structured data exports from Google, Apple, and Instagram (sample files)
- Login attempts, device changes, recovery and security setting changes
- Geographic and time-of-day anomalies
- Cross-platform pattern recognition

Tools & Software

- Forens Digital Forensic Analysis Platform
- On-device processing — files are not uploaded to Forens servers
- Rule-based detection for logins, devices, places, and account changes

Data Sources (sample)

- takeout-20260128T140000Z.zip (Google Takeout, 42.4 MB)
- Apple_Privacy_Export.zip (Apple, 18.1 MB)
- instagram-username-2026-01-28-xxxxxx.zip (Instagram, 9.7 MB)

Chain of Custody

- Data Acquisition: Sample files represent a user-provided export processed locally. No live account passwords were used.
- Processing Method: Automated on-device analysis. Original files are not modified.
- Analysis Date: January 28–30, 2026
- Report Generation: January 30, 2026 at 2:14 PM
- Report ID: FA-SAMPLE-001
- Notice: This is a SAMPLE report. Names, IPs, and events are fictional for demonstration.

Risk Scoring Methodology

The risk score (0–100) uses a weighted point system based on severity and quantity of findings.

Base Point Values

- High: 10 points (e.g., unknown logins, new devices, recovery changes, forwarding)
- Medium: 3–5 points (e.g., app passwords, alert setting changes)
- Low: 1 point (informational or likely-owner activity)

Risk Level Interpretation

- High (50–100): Significant concerns that need prompt attention.
- Moderate (20–49): Issues that should be reviewed.
- Low (1–19): Minor notes for awareness.

Limitations & Scope

- Analysis is based only on the data files provided.

- Findings are indicators, not proof by themselves — context matters.
- IP locations are approximate.
- Absence of findings does not guarantee an account is safe.
- This SAMPLE uses fictional data for product demonstration.

Correlation Analysis

Patterns that show up across platforms and time.

Account Access Pattern

Overnight Austin activity appears on Google and Instagram within the same two-week window, with an unrecognized Apple device added mid-sequence. That cross-platform overlap is stronger than a single odd login.

Persistence Pattern

After the first Austin login, a new device was trusted, an app password was created, and a mail forwarding rule was added. Together these look like someone trying to stay in — not a one-time mistake.

Security Timeline

Chronological listing of sample security events.

January 12, 2026 at 2:14 AM
[HIGH] Login from a city the owner does not travel to (Google)
January 12, 2026 at 2:19 AM
[HIGH] New device added to account (Google)
January 14, 2026 at 11:42 PM
[HIGH] iCloud sign-in on unknown iPhone (Apple)
January 18, 2026 at 3:05 AM
[HIGH] Login from unrecognized session (Instagram)
January 19, 2026 at 1:08 AM
[HIGH] Recovery email change attempted (Google)
January 19, 2026 at 1:11 AM
[MEDIUM] App password created (Google)
January 21, 2026 at 9:16 PM
[MEDIUM] Find My activity from secondary device (Apple)
January 22, 2026 at 12:40 AM
[MEDIUM] Email notification preference changed (Instagram)
January 24, 2026 at 4:02 AM
[MEDIUM] Mail forwarding rule created (Google)
January 8, 2026 at 6:20 PM
[LOW] Password change on known device (Google)
January 9, 2026 at 8:05 AM
[LOW] Trusted phone number confirmed (Apple)
January 25, 2026 at 2:33 AM
[HIGH] Second login from Austin overnight (Google)

Findings by Severity

High (6)

Platform: Google · January 12, 2026 at 2:14 AM · HIGH

Login from a city the owner does not travel to

Successful Google account login from Austin, TX on an unrecognized Chrome browser. Account owner's usual activity is Seattle, WA during daytime hours.

Key Details:

- IP: 104.28.214.xx
- Location: Austin, TX, United States
- Device: Chrome on Windows · unrecognized
- Usual pattern: Seattle, WA · MacBook · daytime

Platform: Google · January 12, 2026 at 2:19 AM · HIGH

New device added to account

A new Windows device was trusted on the Google account within minutes of the Austin login.

Key Details:

- Device: Windows PC · "DESKTOP-8K2F"
- Action: Device authorized
- Relative time: 5 minutes after Austin login

Platform: Apple · January 14, 2026 at 11:42 PM · HIGH

iCloud sign-in on unknown iPhone

Apple ID signed in on an iPhone 14 that does not match the owner's known devices.

Key Details:

- Device: iPhone 14 · iOS 18.2
- Location: Portland, OR
- Known devices: iPhone 15 Pro (owner), MacBook Air

Platform: Instagram · January 18, 2026 at 3:05 AM · HIGH

Login from unrecognized session

Instagram session opened from a mobile browser outside the owner's usual cities and hours.

Key Details:

- App / browser: Mobile Safari
- Location: Austin, TX
- Session: Active for 47 minutes

Platform: Google · January 19, 2026 at 1:08 AM · HIGH

Recovery email change attempted

Attempt to change the account recovery email. Change was started but not completed — still a high-risk signal.

Key Details:

- Attempted new recovery: j****@outlook.com
- Prior recovery: owner@example.com
- Status: Started · not confirmed

Platform: Google · January 25, 2026 at 2:33 AM · HIGH

Second login from Austin overnight

Another successful login from the same Austin metro area overnight, reinforcing a repeated access pattern.

Key Details:

- IP: 104.28.215.xx
- Location: Austin, TX
- Pattern: Matches Jan 12 overnight cluster

Medium (4)

Platform: Google · January 19, 2026 at 1:11 AM · MEDIUM

App password created

A new app password was created, which can allow ongoing access without normal login prompts.

Key Details:

- Label: Mail client
- Created from: Austin, TX session

Platform: Apple · January 21, 2026 at 9:16 PM · MEDIUM

Find My activity from secondary device

Find My location request originated from the unrecognized iPhone added earlier.

Key Details:

- Device: iPhone 14 (unrecognized)
- Action: Location lookup

Platform: Instagram · January 22, 2026 at 12:40 AM · MEDIUM

Email notification preference changed

Security email alerts were reduced, which can hide future login notices from the owner.

Key Details:

- Change: Login alerts reduced
- Session: Matches prior Austin activity

Platform: Google · January 24, 2026 at 4:02 AM · MEDIUM

Mail forwarding rule created

A Gmail filter was created to forward copies of incoming mail to an external address.

Key Details:

- Forward to: j****@outlook.com
- Scope: All mail matching filter

Low (2)

Platform: Google · January 8, 2026 at 6:20 PM · LOW

Password change on known device

Password changed from the owner's usual MacBook in Seattle. Included for timeline completeness.

Key Details:

- Device: MacBook Air · recognized
- Location: Seattle, WA

Platform: Apple · January 9, 2026 at 8:05 AM · LOW

Trusted phone number confirmed

Existing trusted phone number reconfirmed on a known device.

Key Details:

Device: iPhone 15 Pro · owner

Data Sources & Evidence Inventory

Complete inventory of sample files analyzed.

- takeout-20260128T140000Z.zip — Google Takeout — 42.4 MB — SHA-256: a1b2…sample
- Apple_Privacy_Export.zip — Apple Privacy Export — 18.1 MB — SHA-256: c3d4…sample
- instagram-username-2026-01-28-xxxxxx.zip — Instagram — 9.7 MB — SHA-256: e5f6…sample

Appendix

How to Interpret This Report

- Executive Summary: risk level, key findings, and what to do next.
- Security Timeline: order of events.
- Findings by Severity: detail for each event.
- Data Sources: which files were checked.

Important Considerations

- This is a SAMPLE. Do not treat names, IPs, or places as real evidence.
- A live Forens report uses the same structure with your own data file.
- Digital forensic report included with the paid answer.

Conclusion

This sample analysis identified 12 security-related events across 3 data sources. Overall risk assessment: High (78/100). The pattern is consistent with repeated unauthorized access and persistence measures.

In a real run, Forens produces this same digital forensic report from your Google, Apple, Instagram, or Facebook data file — privately on your device.