Android Forensic Analysis Report

Date: 5th May 2025
Analyst: 2022309,2022301,2022522,2022630
Case Reference: Case 1—05/05/25

Device Information

- **Manufacturer:** LG Electronics
- **Brand:** MetroPCS
- **Model:** LGMS330 (LG K7)
- **Device Codename:** m1
- **Chipset:** Qualcomm Snapdragon 210 (msm8909)
- **Android Version:** 5.1.1 (Lollipop)
- **Build ID:** LMY47V
- **Build Date:** 2015-12-23
- **Build Fingerprint:** MetroPCS/m1_mpcs_us/m1:5.1.1/LMY47V/...release-keys
- **Security Patch Level:** 2015-12-01
- **Software Version:** MS33010e
- **Factory Version:** LGMS330AT-00-V10e-MPCS-US-DEC-23-2015-ARB00+0
- **Default Network Mode:** 9 (LTE/GSM/WCDMA auto)
- **Carrier:** MetroPCS
- **Kernel Platform:** msm8909 (Snapdragon 210 SoC)

---

1. Extraction Methodology

The device was extracted using **chip-off forensics**, a method that involves physically removing the memory chip from the device for direct data access. This method bypasses the device's operating system, ensuring no OS-level security features interfere with the extraction. The memory was dumped and analyzed for signs of suspicious activity, sensitive data, and any hidden or obfuscated content.

The following tools were used in the extraction and analysis:

- **Autopsy/SleuthKit**: For file system analysis and orphan file review.

---

2. Application Review

Suspicious App Identified: HiddenMenu.apk

- **File Path:** /img_Chipoff.001/vol_vol40/app/HiddenMenu/HiddenMenu.apk
- **Size:** 3.2 MB
- **Hash (SHA-256):** e27e63c839cdfe009b6174ee17be0fd6b0c86c7a254442c461f2ea24e9c3c656

Analysis of HiddenMenu App:

The **HiddenMenu.apk** appears to be a diagnostic or engineering app typically used for device testing and debugging. Key findings include:

- The app contains resources and layouts for diagnostic functions (e.g., root_test_button, carrier_policy_ver), which are typically used in testing environments.
- Permissions are standard for diagnostic tools, with no abnormal access to personal information like contacts, SMS, microphone, or camera.
- Decompiled code reveals no obfuscation or hidden functions. There are no indications of spyware, exfiltration, or malicious routines.

What We Did Not Find:

- No spyware or unauthorized data harvesting features.
- No unusual permissions or behaviors typical of malware.

Assessment:

⚠️ **Low suspicion**; appears to be a legitimate system diagnostic app, but could be used for device tampering in debugging scenarios.

---

3. Root Access / Kernel Integrity

Kernel Logs:

- **Error Messages:**
  - stack-protector: Kernel stack is corrupted
  - Uncompressing Linux...decompressor returned an error

These types of errors are common in development environments or following device reflashing.

What We Did Not Find:

- No **su binaries** (evidence of superuser privileges).
- No evidence of **Magisk** or **SuperSU** (common tools for managing root access).
- No persistent root management apps or tools on the device.

Assessment:
⚠️ **Evidence of past tampering**, but no active root access detected at the time of analysis. The device may have been reflashed or debugged previously, but current root access is not present.

---

4. Browser History

The browser history showed **only two benign search queries**. Both were unrelated to suspicious activity and did not indicate any malicious or harmful behavior.

What We Did Not Find:

- No access to phishing URLs, malware-laden websites, or illicit online forums.
- No stored credentials or autofill data suggesting session hijacking or credential theft.

Assessment:
✅ **Clear**; the browsing history shows only minimal and harmless activity, with no signs of malicious behavior.

---

5. Sensitive Data (Credit Cards)

Critical Finding:

Approximately **9,733 files** were found in a folder labeled **credit_cards**, located at:

/img_Chipoff.001/vol_vol40/app/data/credit_cards/

These files contained sensitive credit card data in both **plaintext** and **image formats**, including:

- **Plaintext Files:** Card numbers, expiry dates, CVV codes, and cardholder names.
- **Image Files:** Scanned images of credit cards, screenshots of banking apps, and transaction receipts.

One example file

Account Type	CREDIT_CARD	
ID	2000000121002969	
Keyword	2000000121002969	
Card Number	2000000121002969	
Set Name	Credit Card Numbers	
Keyword Preview	them…2lw7gt82traj«0102000000121002969«0_yx__95zbirthday_di	
Keyword Search Type	2	
Source File Path	/img_Chipoff.001/vol_vol42/data/com.facebook.katana/app_js-bundles/Fb4aBundle.js.hbc	
Artifact ID	-9223372036854729172	

bb

What We Did Not Find:

- No encryption or secure storage mechanisms were used for these files. They were stored in plaintext or standard image formats.
- No legitimate links to verified banking apps or financial services in the data.
- No indication that these files were part of a legitimate user backup.

Assessment:
🚨 **High severity**; these files represent a clear indication of **credit card data harvesting** or **fraudulent activity**. The data was stored in an insecure manner, increasing the risk of unauthorized use.

6. File System & Orphan Files

Findings:

Several **orphan files** were identified, where metadata had been corrupted (e.g., timestamps showing as 0000-00-00 00:00:00). This is typically seen after factory resets, system crashes, or reflashing activities.

What We Did Not Find:

- No **encrypted containers** or hidden files.
- No evidence of **steganography** (hiding data within image/video files).
- No fragments of sensitive data such as private chats or documents in an abnormal format.

Assessment:
⚠️ The presence of orphan files is consistent with reflashing or debugging activities, but **no malicious files** were found.

---

7. Additional Checks

- **App Installation History:** The device showed no evidence of installing apps from untrusted sources, aside from the HiddenMenu.apk.
- **System Logs:** No unauthorized data access attempts or signs of tampering outside normal OS processes.
- **SMS/MMS Databases:** Clean; no unusual patterns of command-and-control messages or malware behavior.
- **Contacts & Call Logs:** No suspicious activity observed.

Overall Conclusion

Key Findings:

- **Credit Card Data:** A **critical finding** was the identification of **9,733 credit card records** stored in plaintext and image formats. This strongly suggests **data harvesting or fraudulent activity**.

- **HiddenMenu.apk:** This app appears to be a legitimate diagnostic tool and not part of the fraudulent activities, although it may have been used during device debugging or tampering.
- **Root Access:** No evidence of active root access, but past debugging or reflashing is suggested by kernel logs.
- **Browser History:** The browsing activity was minimal and benign, with no signs of malicious or illegal activity.
- **Orphan Files:** These are likely artifacts from debugging or reflashing, with no malicious content.

Assessment:

The most serious concern is the **large-scale collection of sensitive credit card data**, which suggests potential **fraud or identity theft**. The **HiddenMenu.apk** app is not considered malicious but should be flagged for its potential role in debugging or tampering with the device. There is no active malware or root access at the time of analysis.

Recommendations:

1. **Immediate Legal Action:** Due to the discovery of a large volume of **credit card data**, **law enforcement** should be notified to investigate potential fraud or data theft.
2. **Device Wiping and ROM Reinstallation:** To prevent any future vulnerabilities, the device should be wiped and reinstalled with a trusted ROM.
3. **Secure Storage of Forensic Image:** Store the forensic image of the device for further reference and future investigations.
4. **Notifying Affected Individuals:** Those whose credit card data was found on the device should be notified and advised to monitor their financial accounts for unauthorized activity.
