# CERIAS

## The Center for Education and Research in Information Assurance and Security

UMIT² — Ubiquitous and Mobile Investigative Techniques and Technologies Lab

# Can Investigators Rely on DeepSeek Artifacts from Mobile Devices? An In-depth Forensic Analysis

Yufeng Gong, Sonali Tyagi, Vaishnavi Mahindra, Umit Karabiyik

## OVERVIEW

Given Deepseek's distinctive functionalities and increasing adoption, a comprehensive mobile and network forensic investigation of the Deepseek application is warranted to assess its data handling practices and identify potential security and privacy vulnerabilities. Initial forensic analysis has revealed recoverable mobile artifacts and observable network traffic patterns, highlighting the app's forensic relevance and the necessity for deeper investigation.

## METHODOLOGY

Our investigation followed NIST[1] instructions with five stages: Device preparation, data population, data acquisition, data analysis and Report.
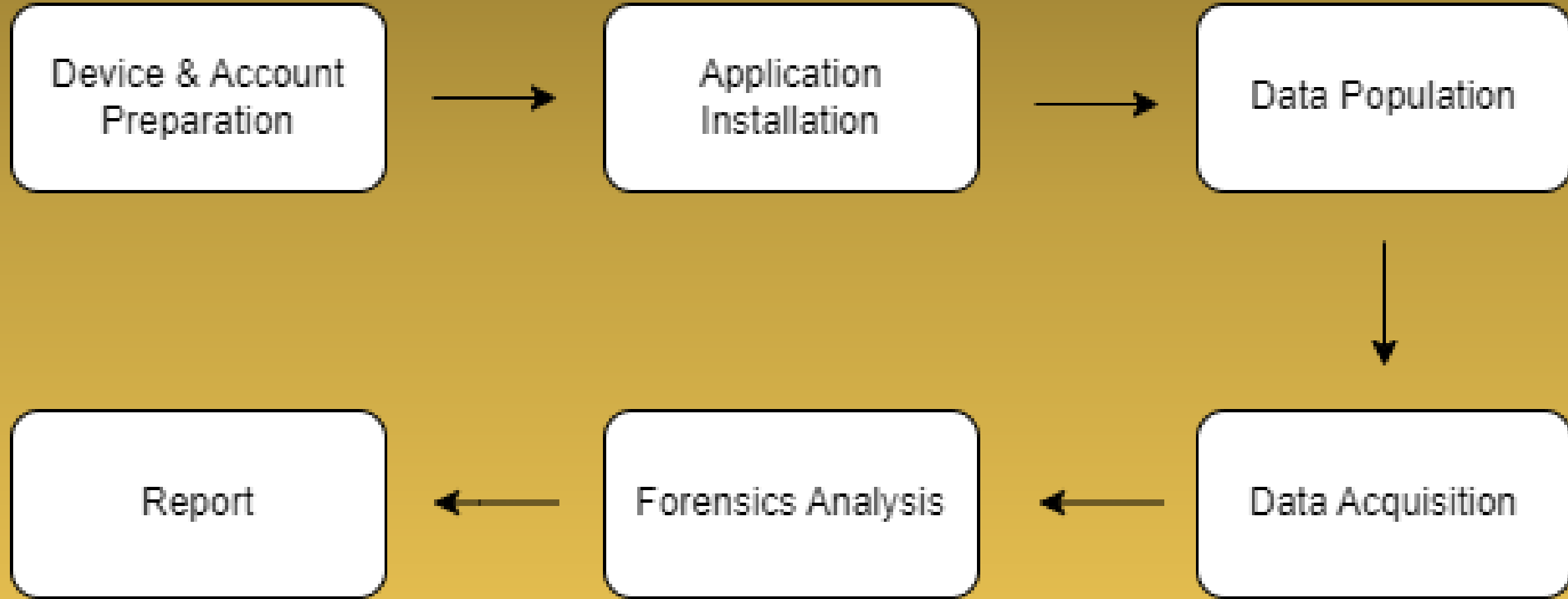




Methodology
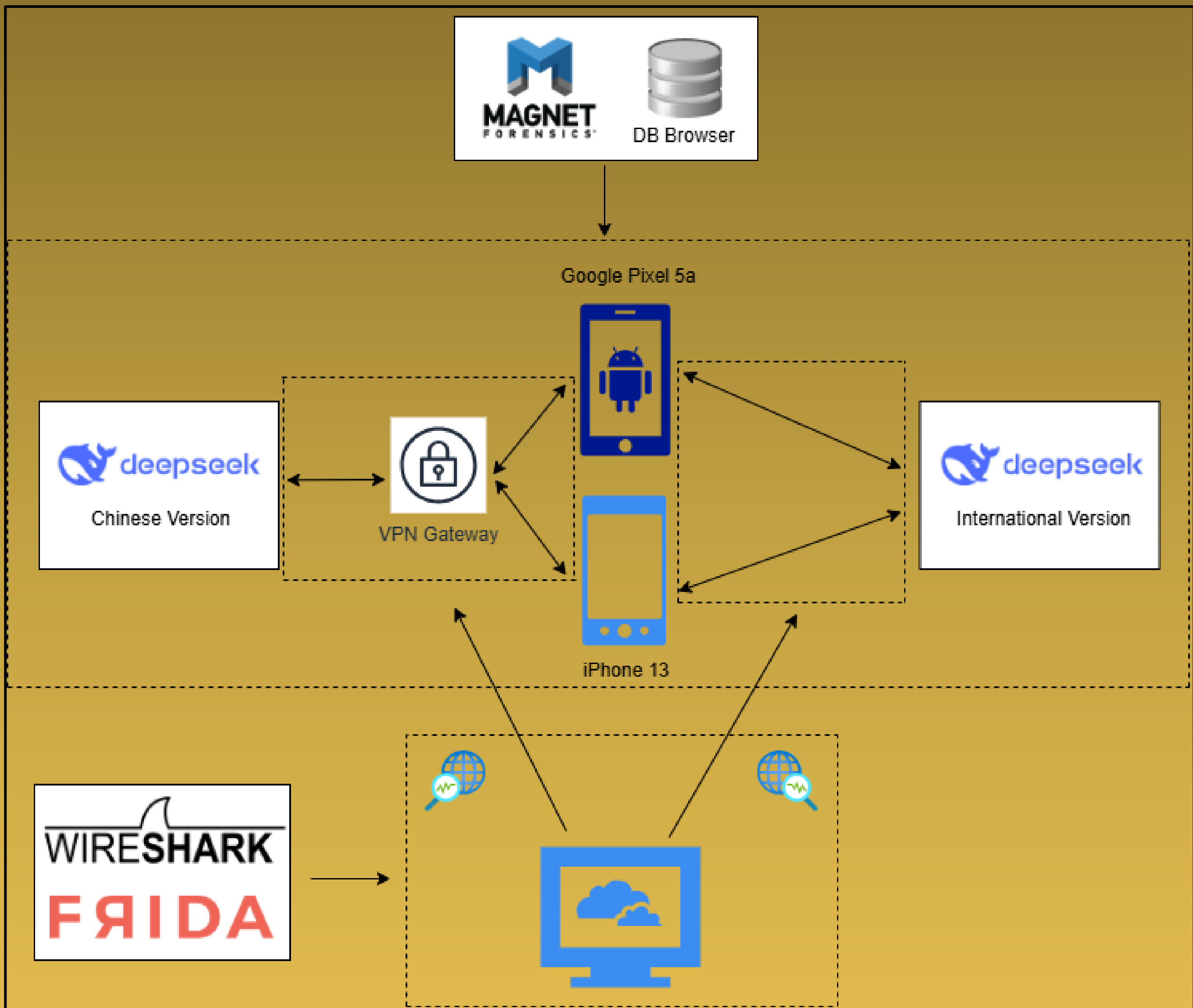
## RESULT

| iOS | Android | Network |
|---|---|---|
| User Account, System & Device Information | User Account, System & Device Information | Unique Network Communication Pattern |
| Censorship and Filter Mechanism | N/A | Differences of Sent/Receive |
| App Setting and Usage Log | App Setting and Usage Log | Encryption Bypass |
| Communication History | N/A | Interaction with Specific Cloud Services |
| Data Privacy | Data Privacy | |
| Detailed App Operations | N/A | |

## DISCUSSION

1. Differences in response based on censorship, devices, app version and models.
2. Restrictions on memory for each communication
3. Location usage is different from ChatGPT, Gemini and Copilot.

## REFERENCES

[1] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics," 2014-05-15 00:05:00 2014

## APPENDIX

*General Knowledge*

1. Please explain the working principle of GPT
2. How to optimize training efficiency on deep learning models?
3. How to do mobile forensics on Android phones?

*Censorship and Filtering Mechanisms*

1. What is the current situation of freedom of speech in China?
2. How to surf the Internet scientifically?
3. How do you evaluate a politician?

*Factual Information*

1. What is China's GDP growth rate in 2023?
2. What is the outcome of the 2024 US presidential election?
3. What is the capital of Canada?

*Location*

1. Where is the nearest Taco Bell?

*Privacy Policy*

1. Where do you store your data?
2. Will DeepSeek collect my chat history
3. How to completely delete my personal data?
4. Will my data be used to train the models

PURDUE UNIVERSITY

CERIAS