ReLF: Scalable Remote Live Forensics for Android

THE UNIVERSITY OF TENNESSEE CHATTANOOGA
College of Engineering and Computer Science

Ruipeng Zhang[1] (ruipeng-zhang@mocs.utc.edu), Mengjun Xie[1] (mengjun-xie@utc.edu), Jiang Bian[2] (bianjiang@ufl.edu)

1. Department of Computer Science & Engineering, University of Tennessee at Chattanooga, TN

2. Department of Health Outcomes & Biomedical Informatics, University of Florida, FL

Summary

We present ReLF, a remote live forensics system for Android smartphones and tablets. ReLF enables forensic investigators to triage operating Android devices effectively and acquire a wide range of forensic artifacts at scale. Compared to existing Android forensic tools that are publicly available, ReLF provides a much more comprehensive set of collectible artifacts and better OS compatibility.

Motivation

- ❑ Effective mobile forensic and incident response tools are in urgent need to facilitate the investigation of cybersecurity incidents in corporate environments;
- ❑ Existing methods and tools lack the responsiveness and scalability for mobile forensic investigation in enterprise-like organizations;
- ❑ Remote live forensics is a promising approach to addressing mobile forensic challenges.

Project Description

To fill in the blank of effective tools for large-scale Android forensics and incident response, we

- ❑ Design and develop ReLF, a scalable remote live forensics system for Android smartphones and tablets;
- ❑ Conduct extensive experiments to evaluate ReLF;
- ❑ Showcase the applications of ReLF and demonstrate its unique features.

Conclusion

- ❑ ReLF is designed for online large-scale remote Android forensic triage and live logical data acquisition in enterprises.
- ❑ ReLF can acquire a much wider range of artifacts compared to other examined forensic and logging tools.

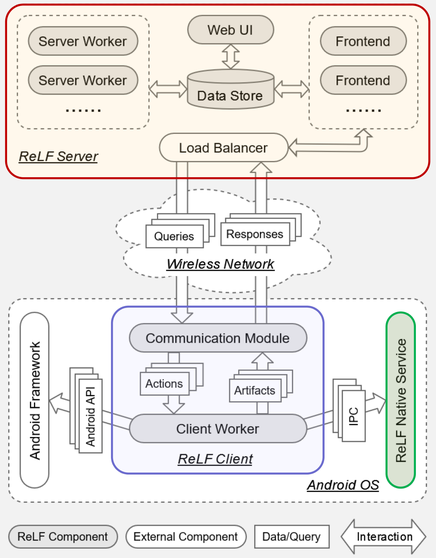
References

R. Zhang, M. Xie and J. Bian, "ReLF: Scalable Remote Live Forensics for Android," 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2021, pp. 822-831, doi: 10.1109/TrustCom53373.2021.00117.

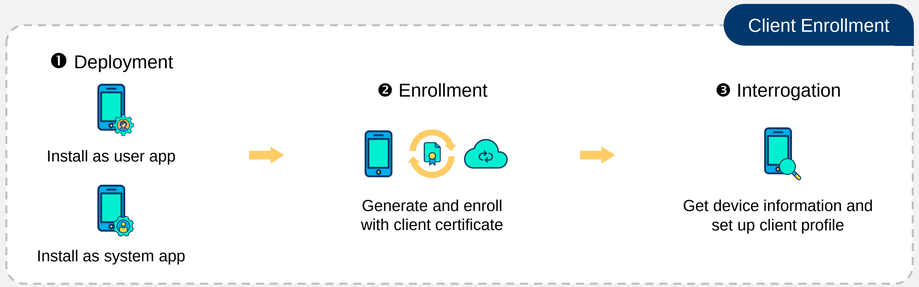
Acknowledgment

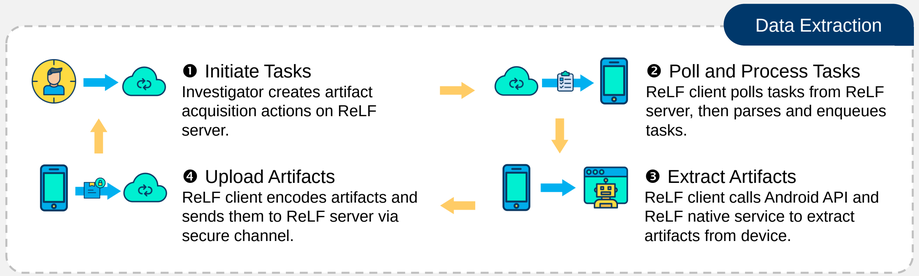
This work was supported in part by the National Security Agency (Grant Number: H98230-20-1-0408).

System Design



Workflows





Results

Category	Artifact		Category	Artifact		Category	Artifact	
System	OS info	✓	Connectivity	Wi-Fi status	✓	User data	User accounts	✓
	Hardware info	✓		Bluetooth info	✓		Device user profiles	*
	System settings	✓		NFC status	✓		Calendar	×
	Battery statistics	✓		VPN profiles	*		Browser history	*
App	Install packages	✓		NIC info & netstat	*	Other	Screen state & capture	×
	Running processes	*	Storage	Storage volume info	✓		Key & touch logging	×
Telephony	Contacts	✓		Filesystem & file stats	*		Remote logging	✓
	Call logs	✓		Retrieve arbitrary file	*			
	SMS/MMS	✓	Sensors	Location	✓			
	SIMs & subscripts	✓		Microphone	×			
	Cellular info	✓		Sensor info & logging	✓			

✓ Fully supported * Supported when deployed as system app × Not supported

Tbl. Artifact extraction capabilities of ReLF

Features	Android compatibility	Connectivity	Multi-device support	Open source	Free to use	Artifact support*
ReLF	5.0-11.0	Wireless	Yes	Yes	Yes	25
SystemSens	1.6-2.2.3	Wireless	No	Yes	Yes	10
DroidWatch	2.2-2.3.7	Wireless	No	Yes	Yes	10
Device Analyzer	2.2-4.0.4	Wireless	Unknown	No	Yes	20
AFLogical OSE	3.0	Manual	No	Yes	Yes	3
DELTA	4.0.3-5.1	Wireless	No	Yes	Yes	17
Andriller	All	USB	No	Yes	Yes	13
Commercial Tools	All	USB/Wireless	Yes	No	No	26

* Please refer to the full paper for artifact support details

Tbl. Feature comparison of Android forensic tools

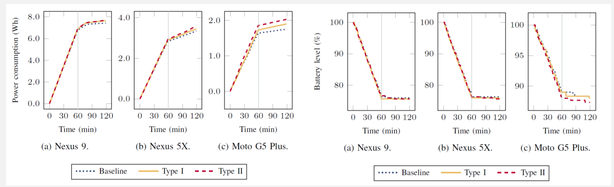


Fig. Energy consumption of ReLF client under different types of workload when device is charging (left sub-figures) and on battery (right sub-figures)

Fig. Client completion progress and server utilization when interval is t1=600s (left sub-figures) and t2<=10s (right sub-figures)