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

UMIT²
Ubiquitous and Mobile Investigative Techniques and Technologies Lab

The Power of Digital Forensics in Smart Device Investigations
Miloš Stanković, Xiao Hu, Umit Karabiyik, Marcus K. Rogers, Smriti Bhatt

OVERVIEW

This project created two realistic scenarios that can be applied to real-world digital investigations. By presenting these real-world crime case scenarios, we analyzed multiple smart devices for digital evidence that is important in relation to each event.
This research project was funded by Bureau of Justice Assistance (Award # 15PBJA-21-GK-03996-INTE)

METHODOLOGY
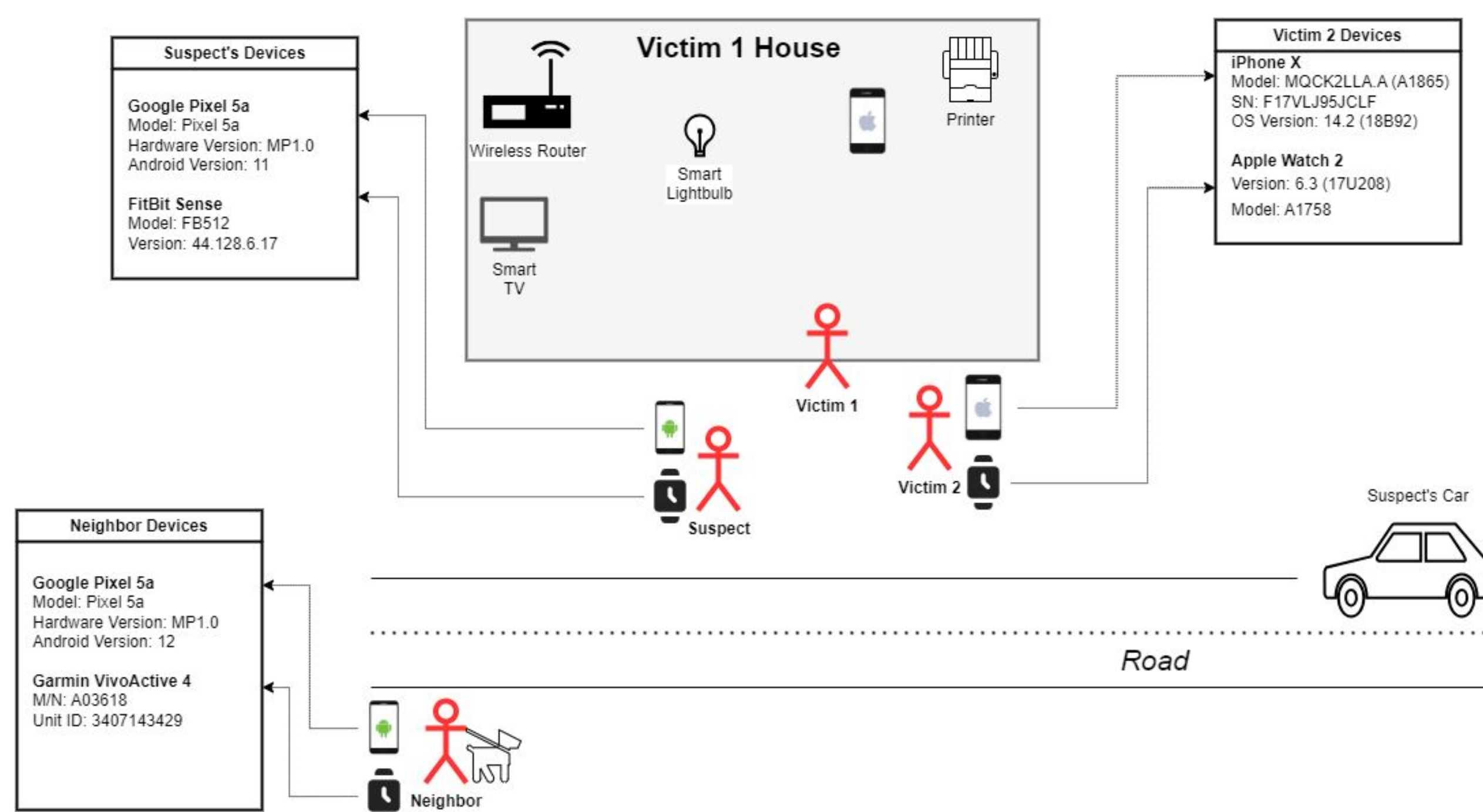
For both scenarios, the methodology followed the same procedures: scenario creation, environment preparation, data population, data acquisition, data analysis and report.

■ **Scenario 1-Undelivered Package:**

Sub-scenario 1

Sub-scenario 2

■ **Scenario 2-: The Ex's Pursuit**

Device	Victim	Defendant
Smart Phone (Version)	Google Pixel 5a (Android 11)	iPhone12 (iOS 16.2)
Smart Watch 1	Fitbit Sense	Apple Watch 7
Smart Watch 2	Galaxy Watch 4	Garmin Vivo Active 4
Smart Ring (Version)	Silver Oura Ring	Black Oura Ring

GOALS

1. Presented identifiable smart devices data and associated artifacts to assist in digital forensic investigations of multiple PIoT devices.
2. Pointed out the difference in storing data between devices and the cloud.
3. Created a publicly available database of discoveries and vulnerabilities found in used devices.
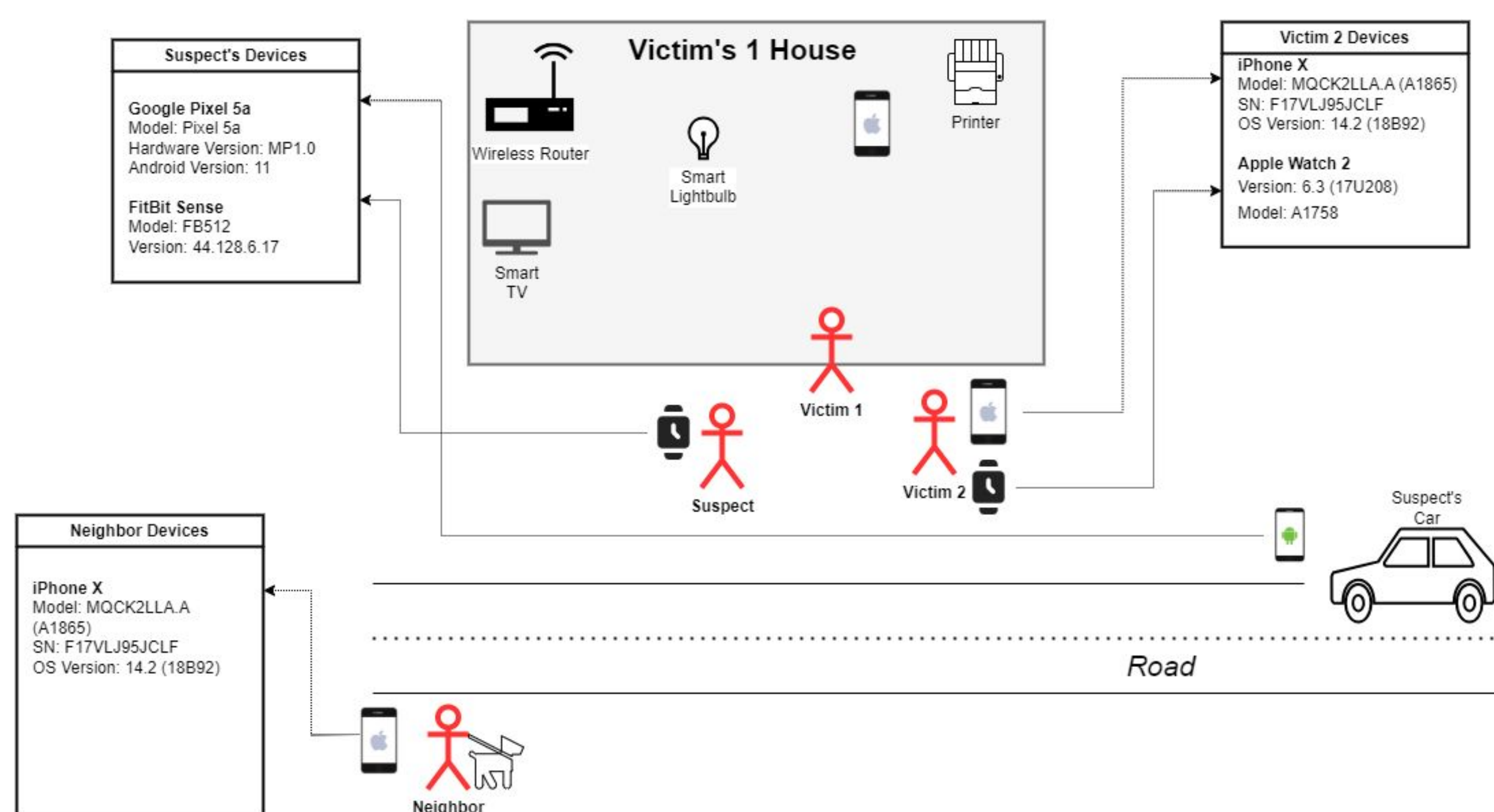
FINDINGS

- Devices carried by victims and suspects, as well as smart devices in the home, record each other's Bluetooth addresses when they are in close proximity, thus proving that the suspect has been in the vicinity of the victim.
- Smart devices worn by victims and suspects record their heart rate, speed, pace, elevation, number of steps, latitude and longitude during the incident to better analyze the scenario.
- Compared with the data obtained from the forensic analysis of the images extracted from the devices, the data stored in the cloud, especially some volatile data, may be different due to the interval of data acquisition, synchronization, and other reasons.
- Web interface to publicly available datasets that can contribute to forensic analysis of similar devices:

November 4 at 13:26, the distance was 0.41 miles

November 4 at 21:11, the distance was 0.84 miles

CONCLUSION

- The forensic artifacts and methods related to smart devices analyzed in this study, as well as publicly available datasets containing critical data paths and vulnerabilities, can provide solid technical support for related investigations.
- Digital forensics on smart devices has an invaluable role to play in criminal investigations, and there is a need for continued progress in these areas.

PURDUE UNIVERSITY

{mstankovic, hu961, umit, rogersmk, bhatt32}@purdue.edu

CERIAS