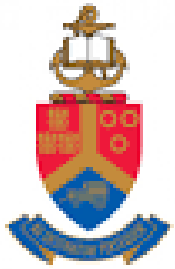
Digital Forensic Readiness Framework for Shadow IoT Devices in Vehicle-to-Everything Communication Networks



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

WiFC
Women in Forensic Computing
WORKSHOP
March 20, 2023

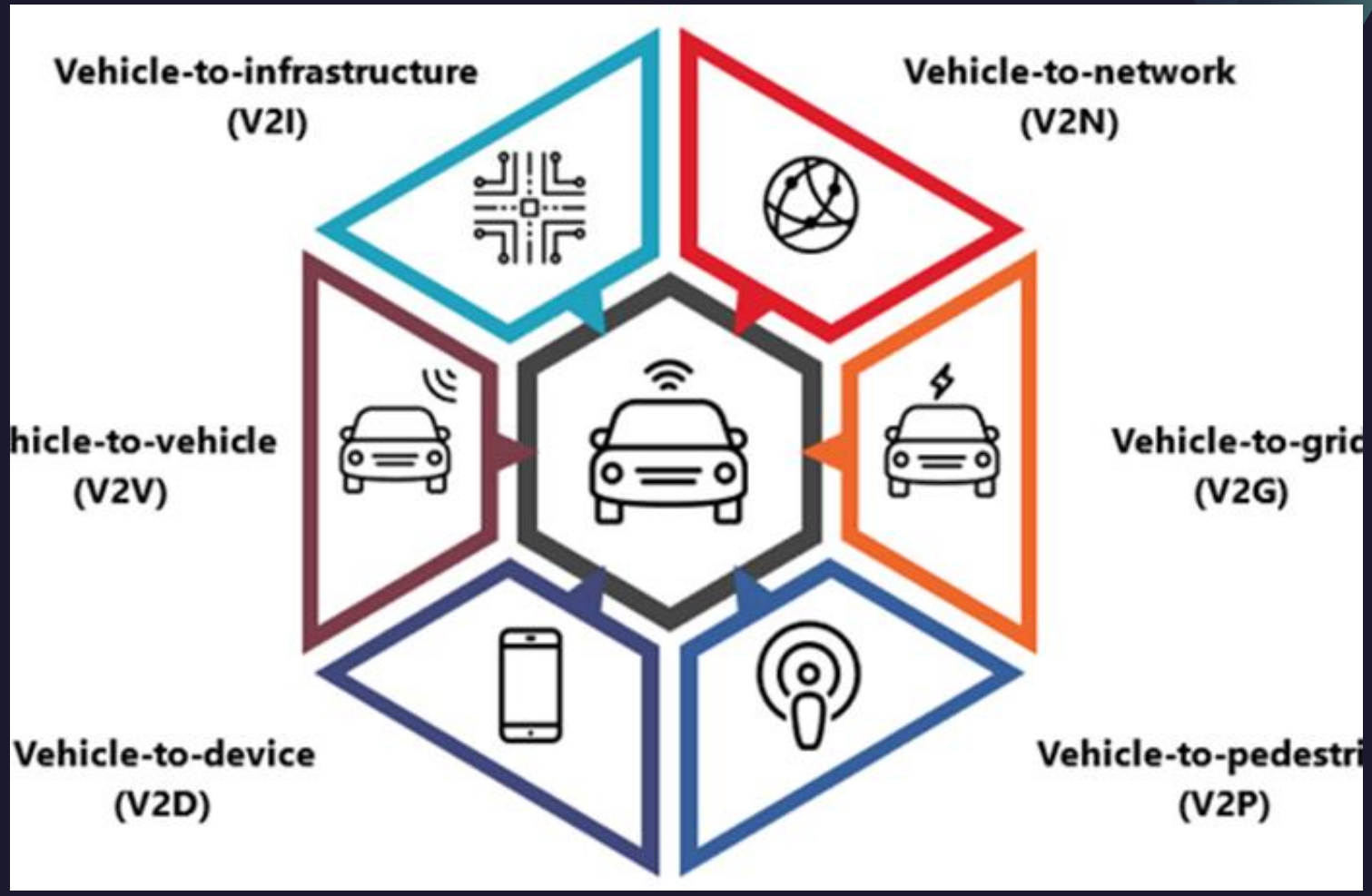
Funmilola Fagbola, Prof. HS Venter

Agenda

- Vehicle to Everything Network
- IoT Devices
- Need for Digital Forensic Readiness
- Research Focus
- Implementation
- Results
- Summary

Vehicle to Everything Network (V2X)

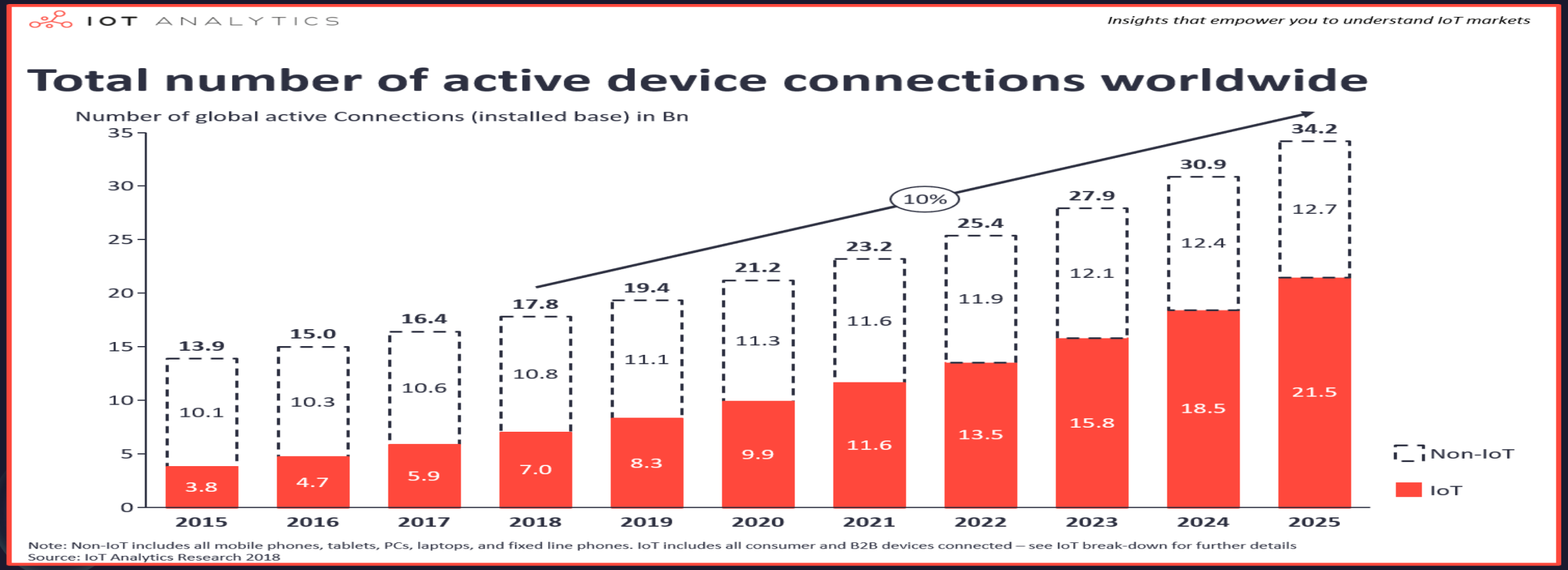
- V2X is the communication between a vehicle and any entity that may affect the vehicle or vice versa.
- V2X is a critical network that may become life threatening if not properly managed.
- V2X is a dynamic network as vehicles can change state often.



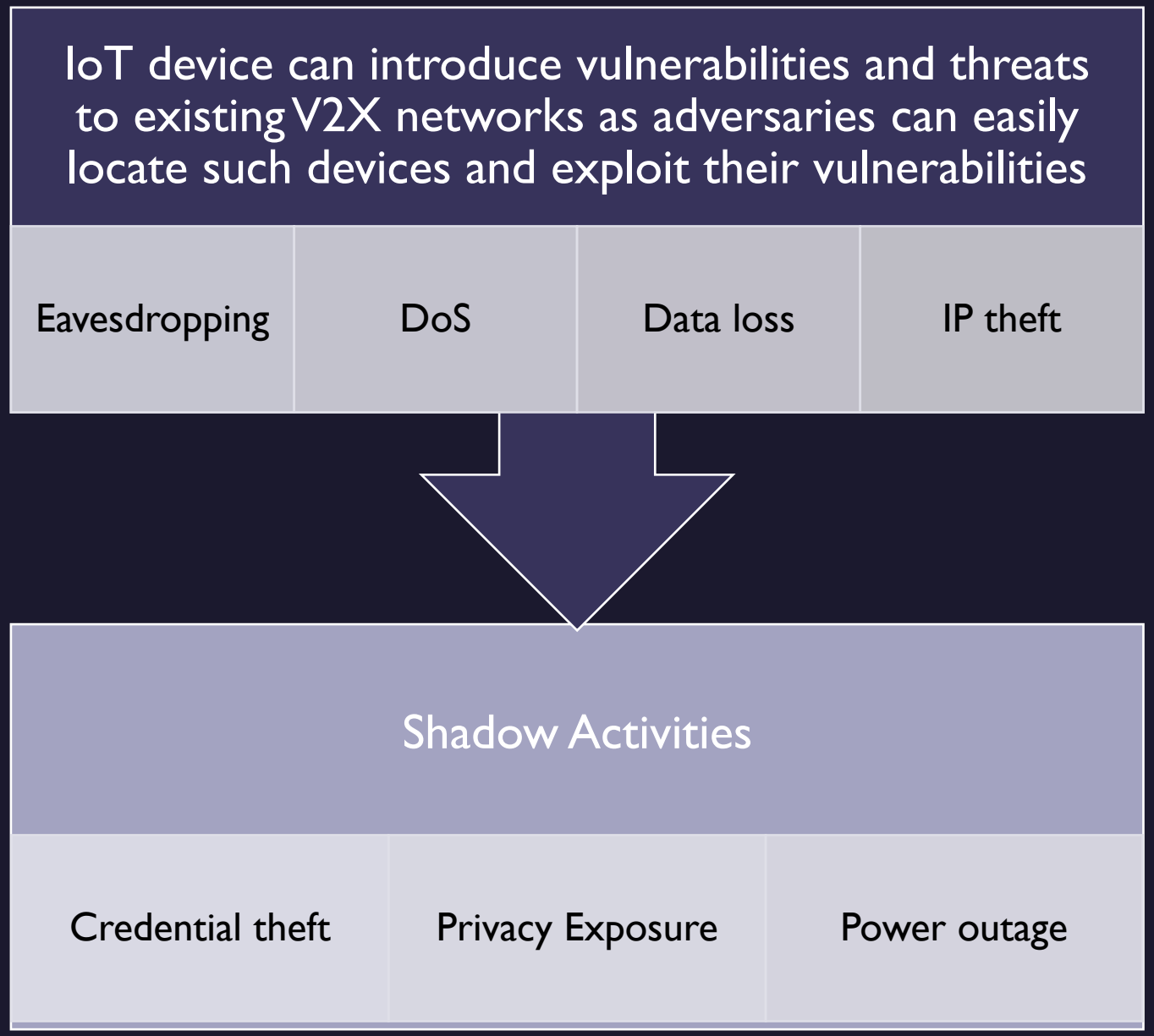
Internet of Things (IoT) Devices

- **The Internet of Things Devices are physical objects that have been made smart by adding intelligence, for the purpose of communication and data sharing.**

Growing IoT: Need for Digital Forensic Readiness



IoT Security Issues in V2X



Research Focus

The main problem being addressed in this research is the non-existence of an integrated security and forensic readiness model for managing shadow IoT devices in V2X networks.

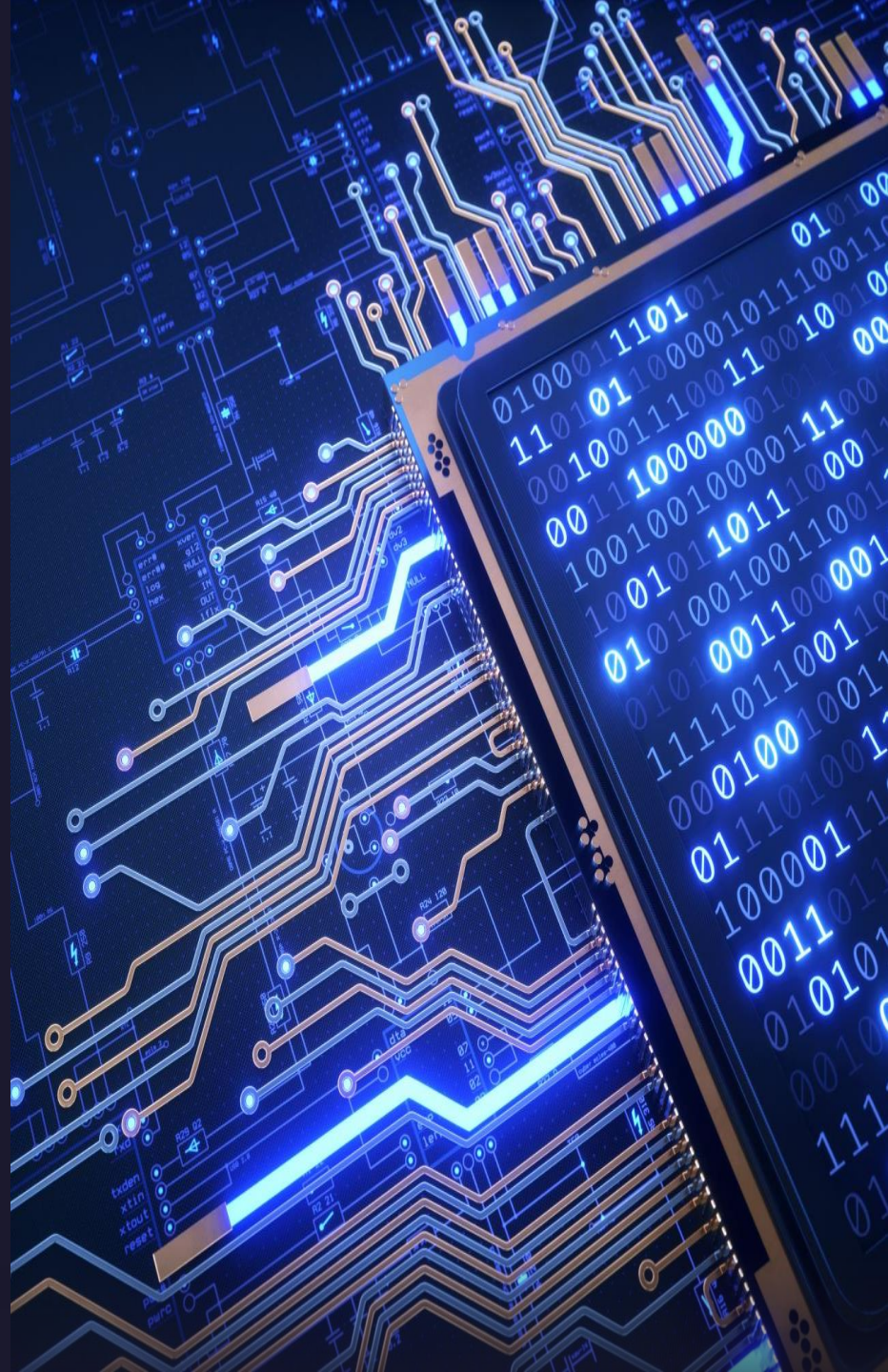
The model is needed to manage the activities and behaviour of shadow IoT devices on the V2X networks.

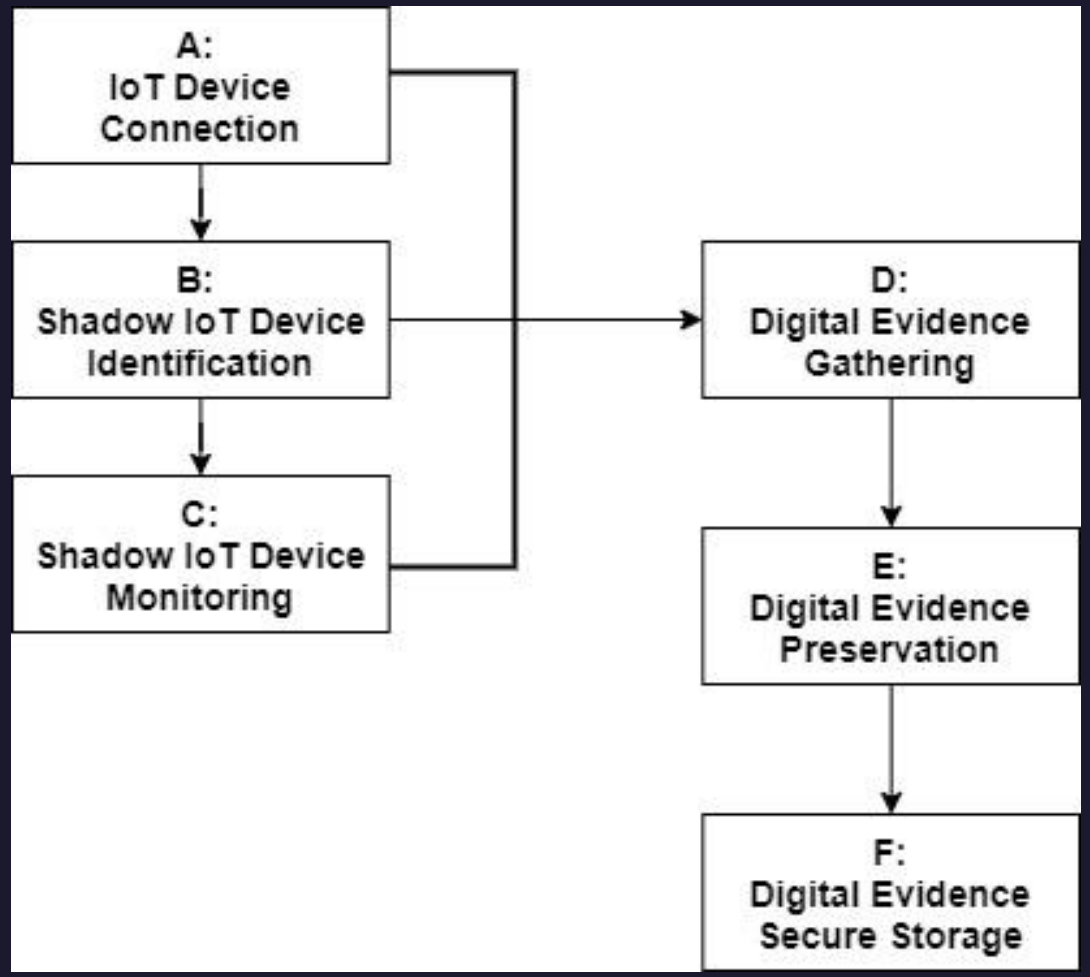
Requirements for Digital Forensic Readiness in V2X Networks

- Open source tool
- Unified file format for digital evidence storage
- Automated forensic analysis of data
- Use of logs and state changes as potential digital evidence
- Centralized repository for evidence gathered from IoT devices

Where can Evidence be Found on V2X Networks?

- Managing gateway security
- Manage possibility of cross-contamination of legitimate IoT devices
- Network Activities profiling





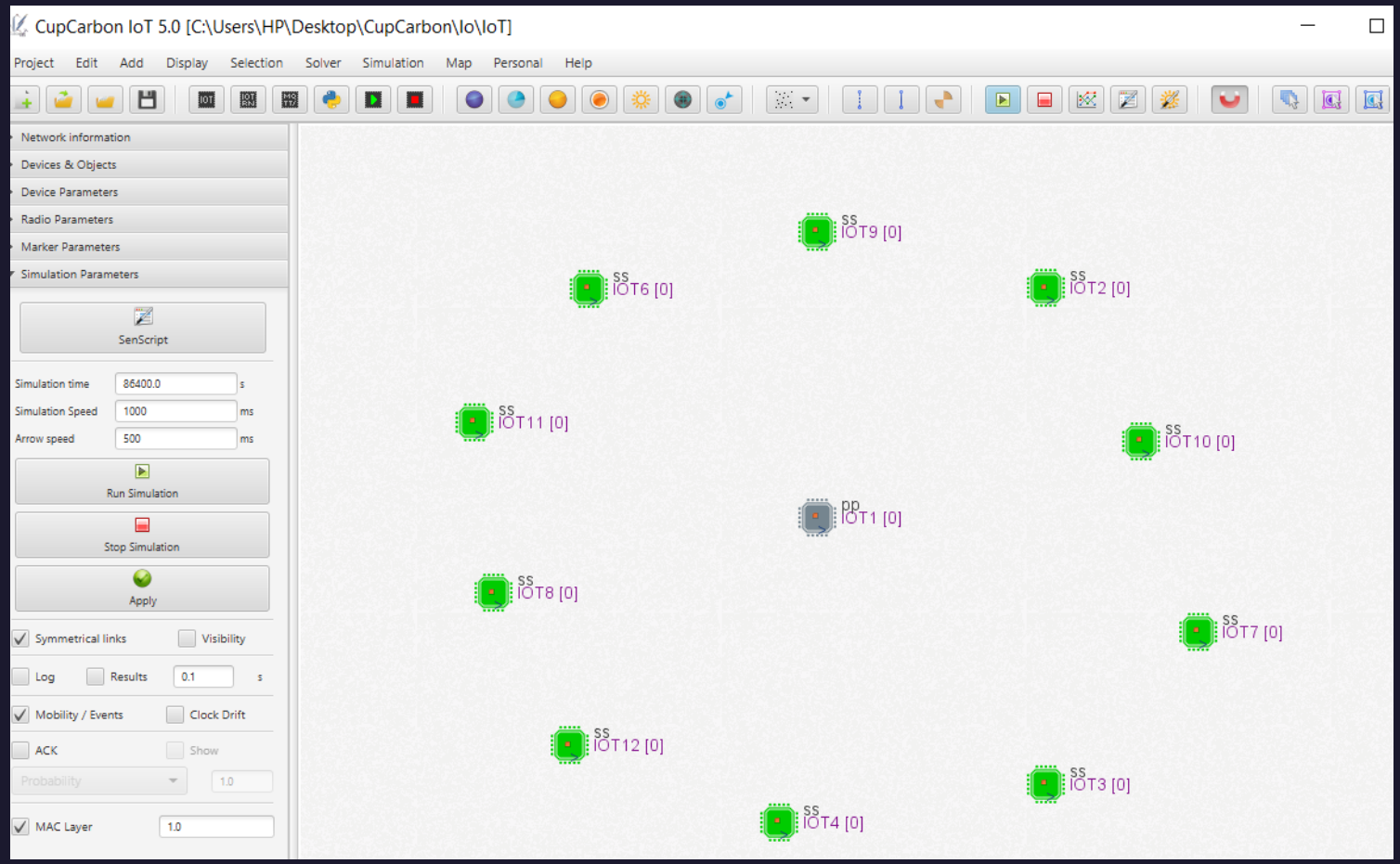
DFR Via Managing gateway security

- Device Connection Stage: Handles connection of device
- Device Identification Stage: handles device categorization
- Shadow IoT Device Monitoring Stage: handles feature based monitoring, periodic traffic pattern, payload traffic pattern, behavior monitoring

Implementation

PDE gathered include:

- Shadow IoT device location
- Network fingerprints of the shadow IoT device
- Vulnerability Level of the shadow IoT device.
- IP address, MacAddress, Device type, Device name, and Timestamp among others.



Results

Device Connection

Timestamp	Device_Name	Device_Type	IP_Address	Protocol	MAC_Address
Feb 19 2023 09:33:00	FitnessTrackerX1	FitnessTracker	192.168.1.105	WiFi	89:03:E1:45:17:49
Feb 19 2023 09:33:32	SmartCamA50	SmartCamera	192.168.10.23	WiFi	57:F7:02:11:D3:17
Feb 19 2023 10:50:32	FitnessTrackerX1	FitnessTracker	192.168.1.85	WiFi	89:03:E1:45:17:49

Feature Analysis

device_type	device_name	ip_address	mac_address	packet_length	protocol	packet_count	datetime_stamp
VRHeadsets	VRHeadsetMax	192.168.1.103	67:19:B1:23:F5:27	1350	UDP	909	13/02/2023 07:36

device_type	device_name	ip_address	mac_address	packet_length	protocol	packet_count	datetime_stamp	com_freq	bandwidth
SmartInhaler	SmartInhalerX1	221.39.175.42	db:da:fb:b1:19:13	85	TCP	275	55:26.0	0	0.5
UltraBooks	UltraBooksA20+	250.181.36.248	98:50:bf:34:90:23	100	HTTP	841	55:26.0	0	2
SmartPen	SmartPenPro3	52.17.24.57	27:09:3b:8e:41:7e	120	HTTPS	697	55:25.9	0	1.55
SmartCamera	SmartCamA50	197.71.96.166	73:8f:7e:18:2b:b2	805	UDP	493	55:26.0	0	5

Summary

This research proposes a model towards DFR in a shadow-inclusive network. A shadow-inclusive network is a network that has shadow IoT device connected to it.

This research presents a generic model that is capable of gathering potential evidence putting the special functionality, features, and behaviour of IoT devices into consideration.

SIoTDFR model can be adopted in smart home, smart city, as well as organizations with IoT networks. This will ensure the forensic readiness towards the inclusion of shadow IoT devices into such IoT network.

Feel Free to Contact Me:
u20732865@tuks.co.za or
funmilolafagbola@yahoo.com