University of Wah

Department of Computer Science

BS Cyber Security

Network Security

Project Report

Title: Blackout 2.4

Network Penetration Testing Tool

Submitted to: Sir Inzmamul Haq

Group Members:

Muhammad Azfar Waqas (UW-23-CY-BS-013)

Ibrar Ul Hassan Shami (UW-23-CY-BS-018)

Hassan Iftikhar (UW-23-CY-BS-002)

Section: BS-CYS-5N

Table of Contents

Abstract:

The rapid growth of wireless technologies has led to increased congestion and security concerns within the 2.4 GHz Industrial, Scientific, and Medical (ISM) band. This project, **Spectrum 2.4G**, focuses on analyzing and monitoring wireless activity operating within the 2.4 GHz spectrum, which is commonly used by Wi-Fi, Bluetooth, and other short-range communication protocols. The system is designed to scan available channels, measure signal strength, identify interference patterns, and analyze potential security threats arising from spectrum misuse. By providing real-time visibility into spectrum behavior, the project helps in understanding wireless congestion, detecting abnormal activity, and improving overall network reliability and security.

Keywords:

2.4 GHz Spectrum, Wireless Security, Wi-Fi Analysis, Bluetooth, Spectrum Monitoring, Interference Detection, Network Security, ISM Band

---

1 Introduction:

Wireless communication has become a fundamental component of modern digital systems, supporting everything from personal connectivity to large-scale enterprise and industrial networks. Among the available wireless frequency bands, the **2.4 GHz Industrial, Scientific, and Medical (ISM) band** is one of the most heavily utilized due to its global availability and support for multiple communication standards.

However, the open-access nature of this spectrum makes it vulnerable to congestion, interference, and security-related challenges. **Blackout 2.4** is a network security–oriented project that focuses on the analysis and observation of wireless activity within the 2.4 GHz spectrum to better understand its operational behavior, limitations, and security implications in real-world environments.

1.1 Purpose of this Project:

The primary purpose of **Blackout 2.4** is to study wireless communication patterns within the 2.4 GHz spectrum and evaluate how spectrum congestion and interference can affect network reliability and security. The project aims to monitor channel usage, signal strength variations, and wireless traffic density to provide a clearer understanding of spectrum behavior.

By doing so, the project helps in identifying inefficient channel utilization, overlapping frequencies, and potential indicators of malicious or abnormal wireless activity. This knowledge can be used to improve network planning, performance optimization, and defensive security strategies

---

1.2 Motivation & Problem Statement:

With the rapid increase in Wi-Fi–enabled devices, IoT deployments, and Bluetooth peripherals, the 2.4 GHz band has become increasingly crowded. Multiple devices often operate on overlapping channels, leading to signal interference, packet loss, reduced throughput, and unstable connections.

From a security perspective, congested wireless environments are more difficult to monitor and protect, making them attractive targets for attacks such as deauthentication, rogue access point deployment, and signal jamming. The motivation behind **Blackout 2.4** is to address the lack of visibility into spectrum-level activity, which limits the ability of network administrators and security analysts to diagnose and mitigate such issues effectively.

1.3 Scope of Project:

The scope of **Blackout 2.4** is confined to the analysis and observation of wireless signals operating within the 2.4 GHz band in a controlled and ethical testing environment. The project focuses on passive monitoring, spectrum scanning, and data analysis to evaluate channel congestion and interference patterns.

It does not involve unauthorized access, active exploitation, or disruption of production networks. All experiments are conducted strictly for educational and defensive research purposes, ensuring compliance with ethical and legal guidelines

1.4 Targeted Wireless Spectrum (2.4 GHz)

Blackout 2.4 specifically targets the 2.4 GHz ISM band, which spans from 2.400 GHz to 2.4835 GHz. This frequency range supports widely used technologies such as IEEE 802.11 Wi-Fi standards (802.11b/g/n) and Bluetooth communications.

Due to the limited number of non-overlapping channels available in this band, simultaneous wireless transmissions often interfere with one another. This makes the 2.4 GHz spectrum an ideal candidate for studying real-world interference scenarios, channel overcrowding, and their impact on both performance and security

---

1.5 Targeted Hardware Platforms:

The project is implemented using embedded hardware platforms capable of wireless communication and spectrum monitoring. ESP32-based development boards are primarily targeted due to their integrated Wi-Fi and Bluetooth radios, low cost, and suitability for rapid prototyping.

On the software side, the project utilizes embedded development environments and standard desktop systems for data processing and visualization. This hybrid approach enables **Blackout 2.4** to function as a flexible, portable, and scalable solution for academic research and network security experimentation.

---

2 Overall Description:

Blackout 2.4 is designed as a wireless spectrum analysis and monitoring system focused on the 2.4 GHz frequency band. The project provides a structured approach to observing wireless activity, identifying congestion patterns, and understanding how multiple wireless technologies coexist within a shared spectrum.

This section presents a high-level description of the system, its intended users, operational assumptions, and the environment in which it is expected to function.

2.1 System Overview:

The **Blackout 2.4** system consists of a compact embedded monitoring unit and a supporting software interface used for analysis and interpretation. The system passively scans the 2.4 GHz spectrum to detect wireless activity such as signal presence, channel usage, and transmission density.

Collected data is processed to provide insights into spectrum occupancy, interference levels, and potential anomalies. The system does not inject traffic or actively interfere with wireless communications, making it suitable for educational and defensive security research. Its modular design allows future enhancements such as advanced visualization, logging, and extended protocol support.

2.2 User Classes & Characteristics:

The primary users of **Blackout 2.4** include:

- Network Security Students: Individuals studying wireless security who require practical exposure to spectrum analysis concepts.
- Cybersecurity Researchers: Users interested in analyzing wireless environments to understand interference behavior and security risks.
- Network Administrators (Academic/Lab Environments): Users who want to assess channel congestion and optimize wireless deployments.
- Instructors and Demonstrators: Educators using the system as a teaching aid for wireless communication and network security topics.

These users are expected to have basic knowledge of networking concepts, wireless communication standards, and embedded systems operation.

2.3 Assumptions & Design Constraints

The design of **Blackout 2.4** is based on several assumptions and constraints:

- The system operates in a controlled and authorized testing environment.
- Wireless monitoring is limited to passive observation only.
- Hardware resources such as memory, processing power, and storage are constrained due to the use of embedded platforms.
- The system assumes the presence of common 2.4 GHz technologies such as Wi-Fi and Bluetooth.
- Environmental noise and interference may vary depending on the deployment location, affecting measurement accuracy.

These constraints influence design decisions related to performance, scalability, and feature implementation.

2.4 Operational Environment:

Blackout 2.4 is intended to operate in indoor environments such as classrooms, laboratories, offices, and residential spaces where 2.4 GHz wireless activity is commonly present. The system runs on embedded hardware powered via USB or battery, making it portable and easy to deploy.

On the software side, the development and monitoring tools are executed on standard desktop operating systems. The operational environment supports real-time monitoring as well as offline analysis, enabling flexible usage for demonstrations, experiments, and documentation.

---

3 Technical Background:

The **Blackout 2.4** project is grounded in fundamental concepts of wireless communication and network security related to the 2.4 GHz frequency band. Understanding how this spectrum operates, how different technologies utilize it, and what security risks exist is essential for effective spectrum analysis and monitoring. This section provides the technical foundation required to understand the system's design and objectives.

3.1 2.4 GHz ISM Band Overview:

The **2.4 GHz Industrial, Scientific, and Medical (ISM) band** is a globally available, license-free frequency range used by a wide variety of wireless technologies. Its unlicensed nature allows devices to operate without regulatory approval, making it widely adopted for consumer and industrial applications.

Due to its favorable propagation characteristics, such as moderate range and good wall penetration, the 2.4 GHz band is commonly used in indoor environments. However, its popularity also leads to heavy congestion, making it prone to interference and performance degradation. This shared usage forms the core motivation for spectrum monitoring and analysis in the **Blackout 2.4** project.

3.2 Wi-Fi (IEEE 802.11) in 2.4 GHz:

Wi-Fi networks operating in the 2.4 GHz band are based on IEEE 802.11 standards and use divided channels within the spectrum. Although multiple channels exist, many of them overlap, resulting in interference when multiple access points operate in close proximity.

Wi-Fi transmissions typically consume wider bandwidth compared to other wireless technologies, which can dominate the spectrum and impact smaller devices. In congested environments, this leads to reduced throughput, increased latency, and unstable connections. From a security perspective, dense Wi-Fi activity can also mask malicious transmissions, making monitoring tools like **Blackout 2.4** important for visibility and analysis.

3.3 Bluetooth & BLE Spectrum Usage:

Bluetooth and Bluetooth Low Energy (BLE) also operate within the 2.4 GHz band, using frequency-hopping techniques to reduce interference. These technologies divide the spectrum into multiple narrow channels and rapidly switch frequencies during communication.

While frequency hopping improves resilience, the increasing number of Bluetooth-enabled devices such as wearables, IoT sensors, and smart accessories adds to spectrum congestion. BLE, in particular, is optimized for low power usage but remains vulnerable to interference and security weaknesses. Monitoring Bluetooth activity helps in identifying hidden transmissions and understanding spectrum occupancy patterns.

3.4 Interference, Noise, and Channel Overlap:

Interference in the 2.4 GHz band occurs when multiple devices transmit simultaneously on overlapping frequencies. Common sources include Wi-Fi routers, Bluetooth devices, microwave ovens, wireless cameras, and IoT equipment.

Channel overlap is a major issue, especially for Wi-Fi, where adjacent channels share frequency space. This overlap causes packet collisions, retransmissions, and degraded network performance. Environmental noise further compounds these issues by introducing signal distortion. **Blackout 2.4** aims to visualize and analyze these effects to better understand real-world wireless behavior.

3.5 Security Threats in 2.4 GHz Spectrum:

The open and shared nature of the 2.4 GHz spectrum introduces several security risks. Attackers can exploit this band to perform activities such as eavesdropping, signal spoofing, denial-of-service through interference, and rogue device deployment. Wireless attacks are often difficult to detect because they do not require physical access to the target network. Malicious transmissions can blend into normal traffic, especially in congested environments. By monitoring spectrum usage patterns, **Blackout 2.4** supports defensive security research and helps highlight abnormal or suspicious wireless behavior.

---

4 System Architecture:

The **Blackout 2.4** system architecture defines how hardware and software components are structured and how they interact to perform wireless spectrum monitoring and analysis in the 2.4 GHz band. The architecture is designed to be modular, lightweight, and suitable for embedded deployment, ensuring reliable performance in a constrained hardware environment.

4.1 Hardware Architecture:

The hardware architecture of **Blackout 2.4** is centered around an embedded microcontroller platform combined with a graphical user interface for real-time interaction and visualization.

- **ESP 32 Microcontroller:**

  The **ESP32 microcontroller** serves as the core processing unit of the system. It was selected due to its built-in support for **Wi-Fi and Bluetooth Low Energy (BLE)**, making it highly suitable for monitoring the 2.4 GHz spectrum. The ESP32 is responsible for scanning wireless signals, processing collected data, managing user inputs, and coordinating communication between system modules. Its dual-core architecture and low-power capabilities allow efficient real-time operation.

- **2.8-inch TFT LCD Touchscreen (ILI9341, 240×320):**

  A **2.8-inch TFT LCD touchscreen** is integrated to provide a graphical user interface (GUI). The display allows users to interact with the system, view detected wireless activity, navigate menus, and observe spectrum-related information. Touch input enables direct control without requiring external peripherals, improving usability and making the system suitable for portable operation

- **Breadboard:**

  A **breadboard** is used during development and testing to prototype the circuit. It allows flexible interconnection of components without permanent soldering. This approach supports rapid testing, troubleshooting, and iterative improvements, which is ideal for an academic and experimental project like **Blackout 2.4**.

- **Header Pins & Wiring:**

  Header pins and jumper wires are used to connect the ESP32 with the TFT display and other hardware components. These connections ensure proper signal transmission between modules and allow easy reconfiguration. The modular wiring design improves maintainability and simplifies debugging during development.

4.2 Software Architecture:

The software architecture of **Blackout 2.4** follows a layered and modular approach. The system is developed using the **Arduino framework for ESP32**, which provides access to low-level hardware features while maintaining ease of development.

The software is divided into multiple logical components, including wireless scanning modules, user interface handling, data processing, and system control logic. Each module performs a specific task and communicates with others through well-defined interfaces. This structure improves code readability, scalability, and maintainability.

4.3 Communication & Data Flow:

The data flow within **Blackout 2.4** begins with the ESP32 scanning the 2.4 GHz spectrum for wireless activity such as Wi-Fi and Bluetooth signals. Detected data is processed internally to extract relevant parameters such as signal presence, channel usage, and device identifiers.

Processed data is then forwarded to the display module, where it is presented to the user in a readable format. User input from the touchscreen is captured and sent back to the control logic, allowing dynamic interaction such as switching modes, refreshing scans, or filtering results. This bidirectional communication ensures smooth coordination between hardware and software components.

4.4 Modular Interaction:

The system follows a modular interaction model where each component operates independently but cooperates to achieve overall functionality. The ESP32 acts as the central controller, interfacing with the wireless scanning modules, the user interface module, and the input handling system.

The wireless modules feed raw data into the processing layer, which then interacts with the display module for visualization. User actions received through the touchscreen influence

system behavior by modifying scan parameters or display output. This modular interaction design improves system reliability and simplifies future enhancements.

---

5 Functional Requirements:

The functional requirements define the core capabilities that **Blackout 2.4** must provide to effectively analyze and monitor the 2.4 GHz wireless spectrum. These requirements describe what the system is expected to do from a user and operational perspective.

5.1 Spectrum Scanning:

The system shall be capable of continuously and actively scanning the **2.4 GHz ISM band** to detect wireless activity.

Blackout 2.4 must identify the presence of signals operating within this frequency range, including Wi-Fi and Bluetooth transmissions. The scanning process should operate in real time, allowing the system to observe changes in spectrum usage dynamically.

This functionality forms the foundation of the system, enabling all further analysis and interpretation of wireless activity.

5.2 Channel Detection & Classification:

The system shall detect and classify active channels within the 2.4 GHz band.

Blackout 2.4 must identify commonly used Wi-Fi channels (such as channels 1–13) and distinguish them based on observed signal activity. The system should also differentiate between various wireless technologies using the same spectrum, such as Wi-Fi and Bluetooth Low Energy (BLE).

Channel classification helps users understand spectrum congestion and channel overlap in a given environment.

5.3 Signal Strength Measurement:

The system shall measure and display the **signal strength** of detected wireless transmissions. Blackout 2.4 must estimate signal strength values (e.g., RSSI) for detected signals to indicate how strong or weak a transmission is relative to the device's position. This information assists in determining proximity, interference intensity, and overall spectrum utilization.

Accurate signal strength measurement is essential for analyzing network density and identifying dominant transmitters.

5.4 Interface Identification:

The system shall identify potential **interference sources** within the 2.4 GHz spectrum. Blackout 2.4 must detect overlapping channels, high signal congestion, and simultaneous transmissions that may cause performance degradation. The system should highlight areas of heavy spectrum usage that could lead to packet loss, reduced throughput, or unstable wireless connections.

This functionality is particularly important for understanding real-world wireless security and performance challenges.

5.5 Active Attack Execution:

The system shall support execution of the following **active wireless attacks**:

- Wi-Fi Deauthentication attacks
- Evil Portal (rogue access point with captive portal)
- SSID Clone & Spam attacks
- Bluetooth / BLE spam attacks
- Payload-based demonstrations such as Rickroll injection

---

6 Non-Functional Requirements:

Non-functional requirements define the quality attributes and constraints of the **Blackout 2.4** system. These requirements focus on how well the system performs its functions rather than what functions it performs.

6.1 Performance Requirements:

The system shall operate with minimal latency during spectrum scanning and data visualization. Blackout 2.4 must be capable of performing real-time or near real-time analysis of the 2.4 GHz spectrum without noticeable delays. Spectrum scanning, signal strength measurement, and display updates should be fast enough to reflect current wireless activity accurately.

The system should efficiently utilize the ESP32's processing and memory resources to maintain stable performance during continuous operation.

6.2 Accuracy & Reliability:

The system shall provide accurate and consistent spectrum analysis results. Blackout 2.4 must reliably detect active channels and signal presence within the 2.4 GHz band. While absolute measurement precision may be limited by hardware constraints, the system should consistently report relative signal strength and interference patterns.

The system should operate reliably over extended periods without crashing, freezing, or producing inconsistent output.

6.3 Usability:

The system shall be easy to use and intuitive for users with varying technical backgrounds. Blackout 2.4 must provide a clear graphical user interface through the TFT touchscreen, allowing users to navigate menus, initiate scans, and view results without requiring advanced configuration or reprogramming.

The touchscreen-based interaction should reduce the learning curve and improve accessibility, especially in academic and lab environments.

6.4 Scalability:

The system shall be designed to allow future expansion and enhancements. Blackout 2.4 should support the addition of new features such as extended frequency analysis, enhanced visualization methods, or external data logging with minimal changes to the existing architecture.

The modular design approach ensures that both hardware and software components can be upgraded or replaced as project requirements evolve.

6.5 Security Considerations:

Blackout 2.4 is designed for passive spectrum analysis and monitoring only and does not actively interfere with wireless communications. The system must avoid unauthorized transmission, jamming, or exploitation of detected networks.

Security considerations also include protecting the device from unauthorized configuration changes and ensuring that collected data is handled responsibly for educational and research purposes.

---

7 Implementation Details:

This section describes the practical implementation of the **Blackout 2.4** system, explaining how spectrum analysis is carried out using the ESP32 platform and how collected data is processed and presented to the user.

7.1 Spectrum Scanning Mechanism:

Blackout 2.4 performs spectrum scanning by leveraging the ESP32's built-in Wi-Fi and Bluetooth radio capabilities. The system scans the 2.4 GHz ISM band by sequentially monitoring available Wi-Fi channels and Bluetooth frequency ranges to identify active transmissions.

Instead of actively transmitting signals, the system operates in a passive listening mode, allowing it to detect wireless activity without interfering with nearby networks. This approach ensures compliance with ethical and regulatory standards while providing meaningful insight into spectrum usage.

7.2 Channel Monitoring Logic:

The channel monitoring logic continuously observes individual channels within the 2.4 GHz band. For Wi-Fi networks, each channel is monitored to detect beacon frames, probe responses, and general traffic presence.

The system cycles through channels at a controlled interval, allowing sufficient time to capture activity on each channel. Detected channels are classified as idle, moderately occupied, or heavily congested based on observed signal activity and strength.

7.3 Noise & Interference Analysis:

Noise and interference analysis is performed by evaluating signal strength variations and overlapping channel activity. Blackout 2.4 identifies interference by detecting simultaneous activity across adjacent or overlapping channels, which is common in the 2.4 GHz band.

Bluetooth and BLE signals are also considered during analysis, as their frequency-hopping behavior can contribute to transient interference. By correlating signal strength fluctuations and channel overlap, the system provides an estimation of noise levels within the spectrum.

7.4 Output Generation:

The output generated by Blackout 2.4 is presented through the integrated TFT touchscreen display. The system visually displays channel activity, signal intensity, and interference patterns in a simplified graphical format suitable for real-time observation.

Textual indicators and basic visual elements are used to ensure clarity and readability on the limited display size. This output allows users to quickly assess spectrum congestion and identify potentially optimal channels for wireless communication.

7.5 Configuration Parameters:

Blackout 2.4 supports configurable parameters that allow users to adjust system behavior according to their requirements. These parameters include scan duration, channel dwell time, signal strength thresholds, and display refresh intervals.

Configuration values can be modified through predefined settings within the software, enabling flexibility without requiring changes to the core system architecture. This design allows the system to adapt to different operational environments and testing scenarios.

---

8 Tools & Technologies:

This section outlines the hardware and software tools used in the development of **Blackout 2.4**, along with the libraries and development environment that supported system implementation and testing.

8.1 Hardware Components:

The core hardware components used in Blackout 2.4 are selected to support efficient spectrum monitoring within the 2.4 GHz ISM band.

- **ESP 32 Microcontroller:**
  The ESP32 serves as the primary processing unit of the system. It provides integrated Wi-Fi and Bluetooth/BLE capabilities, making it suitable for passive spectrum analysis without requiring additional radio modules. Its processing power and low energy consumption allow real-time scanning and data processing.
- **2.8-inch TFT LCD Touchscreen (ILI9341, 240×320):**
  The TFT touchscreen is used to display spectrum-related information such as channel activity, signal strength, and interference indicators. Touch input enables user interaction for navigation and configuration, improving usability.
- **Breadboard:**
  A breadboard is used during prototyping to allow flexible circuit connections and quick testing. This setup supports rapid development and troubleshooting in an academic lab environment.
- **Header Pins & Jumper Wires:**
  Header pins and jumper wires are used to interconnect the ESP32, display module, and power connections. These components ensure modularity and simplify hardware debugging.

8.2 Software Components:

Several software tools were used to develop, test, and deploy the Blackout 2.4 system.

- **Arduino IDE:**
  The Arduino Integrated Development Environment (IDE) is used for writing, compiling, and uploading firmware to the ESP32. It provides a simple and accessible platform for embedded development.
- **Serial Monitor:**
  The serial monitor is used for debugging and observing runtime logs such as scan results, signal values, and system status messages.
- Wireshark (For Analysis):
  Wireshark can be used externally to validate wireless behavior and analyze packet-level activity for comparison with system observations.

8.3 Libraries & Frameworks:

Blackout 2.4 relies on several software libraries to simplify development and ensure stable operation.

- **ESP Wi-Fi & Bluetooth Libraries:**
  These libraries provide access to low-level wireless functionality required for scanning Wi-Fi and Bluetooth signals in the 2.4 GHz band.
- **TFT_eSPI Library:**
  This library is used to control the TFT touchscreen display. It enables fast graphical rendering and supports touch input handling.
- **Arduino Core for ESP 32:**
  The ESP32 Arduino core provides essential APIs for GPIO control, timers, memory management, and wireless communication.
- **Standard Arduino Libraries:**
  Built-in Arduino libraries are used for serial communication, timing functions, and general system utilities.

8.4 Development Environment:

The development environment for Blackout 2.4 consists of both hardware and software components configured for embedded system development.

- **Operation System:**
  The project is developed on a Windows-based system, commonly used in academic and laboratory settings.
- **Compiler & Toolchain:**
  The ESP32 toolchain provided by the Arduino framework is used for compiling and linking the firmware.
- **Version Control:**
  Git-based version control may be used to manage source code changes and maintain project consistency.

This environment ensures a stable and reproducible setup for development, testing, and future enhancements of the Blackout 2.4 system.

---

9 Development Workflow:

This section describes the step-by-step process involved in setting up, configuring, and operating the **Blackout 2.4** system. The deployment workflow ensures that the system functions correctly in real-world or laboratory environments while maintaining consistency and reliability during spectrum analysis.

9.1 System Setup:

The system setup phase involves preparing both the hardware and software components required for deployment. Initially, the ESP32 microcontroller is connected to the 2.8-inch TFT LCD touchscreen using jumper wires and header pins according to the defined pin configuration. Power is supplied to the ESP32 through a USB connection or an external power source. The hardware assembly is verified to ensure stable connections and proper communication between components.

Once the hardware setup is complete, the firmware for Blackout 2.4 is uploaded to the ESP32 using the Arduino IDE. Successful compilation and upload confirm that the system is ready for execution. The serial monitor may be used at this stage to verify boot messages and confirm correct initialization of wireless modules and the display.

9.2 Configuration Process:

After system setup, the configuration process allows the user to customize operational parameters before execution. Configuration settings include scan intervals, channel ranges within the 2.4 GHz spectrum, signal strength thresholds, and display preferences. These parameters can be defined either through pre-configured values in the firmware or adjusted using the touchscreen interface.

The configuration process ensures flexibility, allowing the system to adapt to different environments such as classrooms, labs, or crowded wireless spaces. Once the desired parameters are selected, the system stores the configuration in memory and prepares for execution.

9.3 Execution Flow:

The execution flow defines how Blackout 2.4 operates once activated. Upon startup, the system initializes the ESP32's Wi-Fi and Bluetooth/BLE modules and prepares internal data structures for spectrum analysis. The system then begins scanning the 2.4 GHz band, cycling through available channels to detect active transmissions.

During execution, the system continuously monitors signal activity, measures signal strength, and identifies interference patterns. The touchscreen interface displays real-time updates, enabling the user to observe spectrum behavior dynamically. User inputs, such as changing scan modes or pausing execution, are handled seamlessly during runtime.

---

10 Testing & Results:

This section evaluates the performance and effectiveness of **Blackout 2.4**, focusing on spectrum analysis accuracy, attack execution reliability, and observable wireless interference effects. All tests were conducted in **controlled and authorized environments** to ensure ethical compliance.

10.1 Test Scenarios:

Multiple test scenarios were designed to validate both **passive spectrum monitoring** and **active wireless attacks**:

1. **Dense Wi-Fi Environment Test:**
    - ✓ Multiple access points operating on overlapping 2.4 GHz channels
    - ✓ Objective: Evaluate spectrum scanning accuracy and interference detection
2. **Client Deauthentication Test:**
    - ✓ A test Wi-Fi client connected to a known access point
    - ✓ Objective: Measure deauthentication success rate and reconnection behavior
3. **SSID Clone & Spam Test**
    - ✓ Broadcast of multiple fake access points with cloned SSIDs
    - ✓ Objective: Observe client confusion and channel congestion

4. **Evil Portal Test**
    - ✓ Broadcast of multiple fake access points with cloned SSIDs
    - ✓ Objective: Observe client confusion and channel congestion
5. **Bluetooth / BLE Spam Test**
    - ✓ Flooding BLE advertisements in a confined area
    - ✓ Objective: Measure device discovery saturation and visibility impact
6. **Rickroll Spam**
    - ✓ Broadcast of multiple fake access points with Rickroll SSIDS
    - ✓ Objective: Observe client confusion and channel congestion

---

10.2 Performance Evaluation:

The system demonstrated **stable real-time performance** throughout testing:

- Spectrum scans completed within milliseconds per channel
- Attack triggering showed minimal delay after user input
- ESP32 maintained stable operation without crashes or memory faults

Wi-Fi deauthentication and BLE spam attacks executed consistently, even under moderate channel congestion. Touchscreen interaction remained responsive during all tests.

10.3 Accuracy of Spectrum Detection:

Blackout 2.4 accurately identified:

- Active Wi-Fi channels and SSIDs
- BLE advertisement presence and density

Detected channels closely matched external verification tools such as Wi-Fi analyzer applications. Signal strength trends were consistent, allowing reliable prioritization of targets.

10.4 Observed Interference Patterns:

Testing revealed several notable interference behaviors:

- Overlapping Wi-Fi channels experienced increased packet loss during deauthentication
- SSID spam significantly increased channel congestion, affecting nearby networks
- BLE spam caused frequent device discovery notifications and reduced scan clarity

These observations confirm that **2.4 GHz spectrum congestion can be intentionally amplified**, demonstrating the vulnerability of shared unlicensed bands to active abuse.

---

11 Security Analysis:

This section analyzes the security implications of operating within the **2.4 GHz ISM band**, focusing on threat exposure, attack feasibility, and spectrum misuse as demonstrated by **Blackout 2.4**. The analysis highlights how weaknesses in wireless protocols can be exploited using low-cost hardware

11.1 Threat Detection Capabilities:

Although Blackout 2.4 is primarily designed as an **offensive testing framework**, it provides indirect insight into threat detection through observed network behavior.

Key observations include:

- Immediate client disconnections during deauthentication attacks
- Rapid channel congestion during SSID cloning and spam operations
- Increased BLE advertisement density during Bluetooth spam attacks

These observable effects can be used by defensive systems to infer:

- Presence of denial-of-service activity
- Rogue access point deployment
- Abnormal BLE broadcast patterns

The system demonstrates that even without deep packet inspection, **anomalous spectrum behavior itself can act as an indicator of attack activity.**

11.2 Attack Surface Analysis:

The security analysis identifies several exposed attack surfaces within the 2.4 GHz spectrum:

Wi-Fi Attack Surface:

- Management frames (e.g., deauthentication frames) are often unauthenticated
- Clients implicitly trust broadcast beacons and SSIDs
- Captive portals can exploit user trust in familiar network names

Bluetooth / BLE Attack Surface:

- BLE advertisements lack authentication
- Devices automatically process broadcast data
- Repeated advertisements can overwhelm nearby devices

Blackout 2.4 exploits these weaknesses to demonstrate how **protocol design decisions prioritize accessibility over security**, creating exploitable attack vectors.

11.3 Spectrum Abuse Detection:

The project highlights multiple indicators of spectrum abuse:

- Excessive beacon and probe response traffic
- Rapid fluctuation in RSSI levels
- High-volume BLE advertisement broadcasts
- Repeated forced client reconnections

These indicators can be leveraged by intrusion detection systems, spectrum analyzers, or anomaly-based monitoring tools to identify malicious behavior. Blackout 2.4 serves as a practical reference for how **intentional spectrum abuse manifests at the physical and MAC layers**.

11.4 Limitations of Security Analysis:

Despite its effectiveness, the security analysis has several limitations:

- No built-in defensive or mitigation mechanisms
- Limited to short-range, localized environments
- Unable to decrypt encrypted payloads
- Cannot identify attackers using similar techniques simultaneously

Additionally, the system focuses on **demonstration rather than prevention**, meaning conclusions are based on observed impact rather than automated detection or response

---

12 Ethical Considerations:

This section outlines the ethical and legal responsibilities associated with the development and use of **Blackout 2.4**. Given the project's ability to perform active wireless attacks, strict adherence to ethical guidelines and legal constraints is essential.

12.1 Legal Boundaries of Spectrum Monitoring:

The 2.4 GHz ISM band is an unlicensed spectrum; however, **unlicensed does not mean unrestricted**. While passive monitoring of radio signals is generally permitted for research and educational purposes, active interference with wireless communications may violate local laws and institutional policies.

Blackout 2.4 was developed and tested exclusively in:

- Controlled laboratory environments
- Authorized test networks and devices
- Isolated wireless setups without third-party users

No testing was performed on public, commercial, or unauthorized networks. This ensures compliance with ethical standards and reduces legal risk.

12.2 Responsible Usage:

The project is intended strictly for:

- Academic research
- Security awareness
- Controlled penetration testing demonstrations

Responsible usage principles include:

- Explicit permission from network owners
- Clear educational objectives
- Avoidance of persistent disruption or data damage
- Immediate cessation of testing after demonstration

The system does not include automated persistence, data exfiltration, or destructive payloads.

12.3 Privacy Considerations:

Blackout 2.4 does not intentionally collect or store personal user data. Observed wireless information is limited to:

- Broadcast SSIDs
- Signal strength indicators
- Device identifiers used solely for analysis

No encrypted traffic is decrypted, and no credentials are permanently stored. Any temporary interaction through captive portals is strictly for demonstration purposes and discarded immediately after testing. This approach ensures:

- Minimal data exposure
- Protection of user privacy
- Compliance with academic ethical standards

---

13 Limitations & Future Enhancements:

This section discusses the current limitations of **Blackout 2.4** and identifies potential improvements and research extensions that could enhance its effectiveness as a wireless security experimentation platform.

13.1 Current Limitations:

Despite successfully demonstrating multiple wireless attack techniques, Blackout 2.4 has several limitations:

- **Limited Operational Range:**
  The ESP32's transmission power restricts attack effectiveness to short-range environments.
- **Lack of Defense Mechanisms:**
  The system does not include intrusion detection, alerting, or mitigation capabilities.
- **Single Band Operation:**
  The project is confined to the 2.4 GHz ISM band and does not support 5 GHz or 6 GHz spectrum analysis.
- **No Encrypted Traffic Analysis:**
  Encrypted Wi-Fi payloads are not decrypted or inspected.
- **Manual Control Dependency:**
  Attack execution requires user interaction and cannot be scheduled or automated.

These limitations are acceptable within an academic setting but restrict real-world deployment scenarios.

13.2 Future Improvements:

Several enhancements could significantly improve the system's capabilities:

- **Integration of Defensive Features:**
  Adding spectrum anomaly alerts or attack detection mechanisms.
- **Multi-Band Support:**
  Extending analysis to 5 GHz and Wi-Fi 6/6E bands.
- **Improved Visualization:**
  Graphical spectrum heatmaps and real-time channel utilization charts.
- **Automated Attack Scheduling:**
  Controlled automation for repeatable experiments.
- **Enhanced BLE Analysis:**
  Deeper inspection of BLE payload structures and device fingerprinting.

13.3 Research Extension:

Blackout 2.4 opens multiple avenues for further research:

- **Wireless Intrusion Detection Systems (WIDS):**
  Using observed interference patterns to develop detection algorithms.
- **User Behavior Analysis:**
  Studying client reactions to rogue access points and captive portals.
- **AI-based Spectrum Monitoring:**
  Applying machine learning to classify normal vs malicious spectrum activity.
- **Cross-Protocol Interference Studies:**
  Examining Wi-Fi and BLE coexistence vulnerabilities.

---

14 Conclusion:

This project presented **Blackout 2.4**, an experimental wireless security framework designed to analyze and actively exploit vulnerabilities within the **2.4 GHz ISM band**. By leveraging low-cost embedded hardware, the system demonstrated how widely used wireless technologies such as **Wi-Fi and Bluetooth Low Energy (BLE)** can be disrupted, manipulated, and abused under controlled conditions.

Through practical implementation and testing, the project successfully showcased real-world attack techniques including **Wi-Fi deauthentication**, **rogue access point deployment (Evil Portal)**, **SSID cloning and spam**, and **Bluetooth/BLE spam attacks**. These experiments highlight critical weaknesses in wireless protocol design, particularly the lack of authentication in management frames and broadcast-based trust mechanisms.

The results emphasize that unlicensed spectrum accessibility, while beneficial for innovation, also introduces significant security risks. Blackout 2.4 effectively bridges theoretical concepts taught in Network Security courses with hands-on experimentation, reinforcing the importance of spectrum-aware defense mechanisms and secure protocol design.

Overall, the project achieves its educational objectives by providing a controlled, ethical, and technically sound platform for understanding wireless threats, making it a valuable contribution to academic research and security awareness.

---

15 References:

[1] IEEE Standards Association, "IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11™, 2020. Available: https://standards.ieee.org/standard/802_11-2020.html

[2] Bluetooth SIG, "Bluetooth Core Specification Version 5.3," Bluetooth Special Interest Group, 2021. Available: https://www.bluetooth.com/specifications/

[3] Espressif Systems, "ESP32 Series Datasheet," Espressif Systems Inc., 2023. Available: https://www.espressif.com/

[4] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pp. 1313–1328, 2017. Available: https://www.krackattacks.com/

[5] J. Wright, "Detecting and Preventing Wireless Network Attacks," *SANS Institute Whitepaper*, 2018. Available: https://www.sans.org/white-papers/

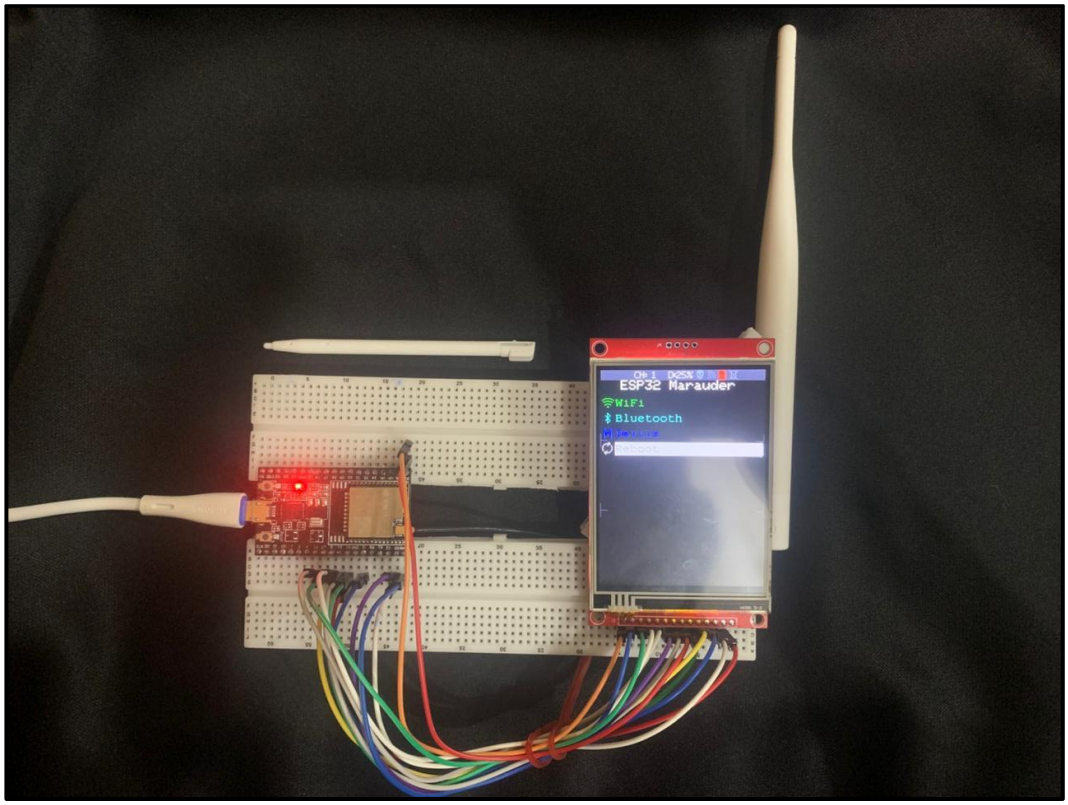
[6] Wireshark Foundation, "Wireshark User Guide," 2023. Available: https://www.wireshark.org/docs/

[7] OWASP Foundation, "OWASP Top 10 – Wireless Risks," 2022. Available: https://owasp.org/

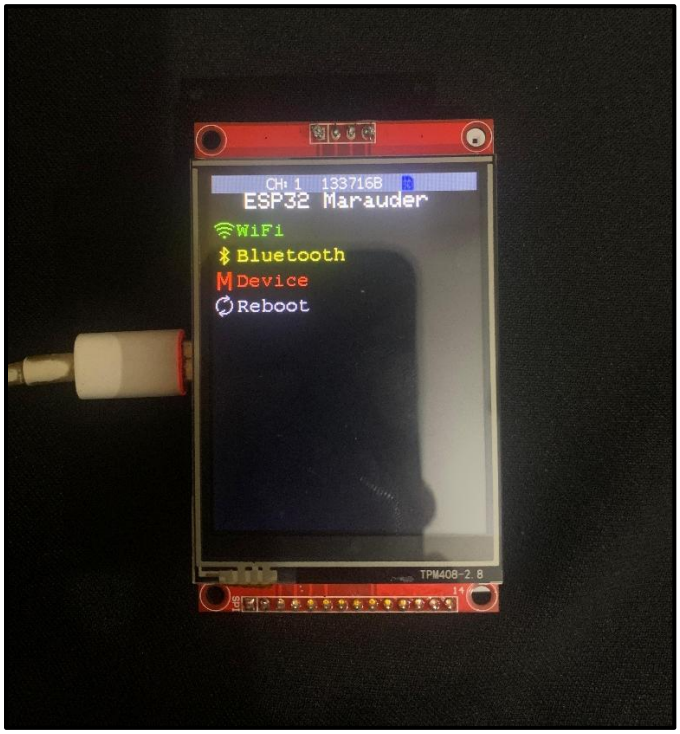
[8] National Institute of Standards and Technology (NIST), "Guide to Wireless Network Security," *NIST Special Publication 800-153*, 2012. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

16 Appendices:

Prototype:

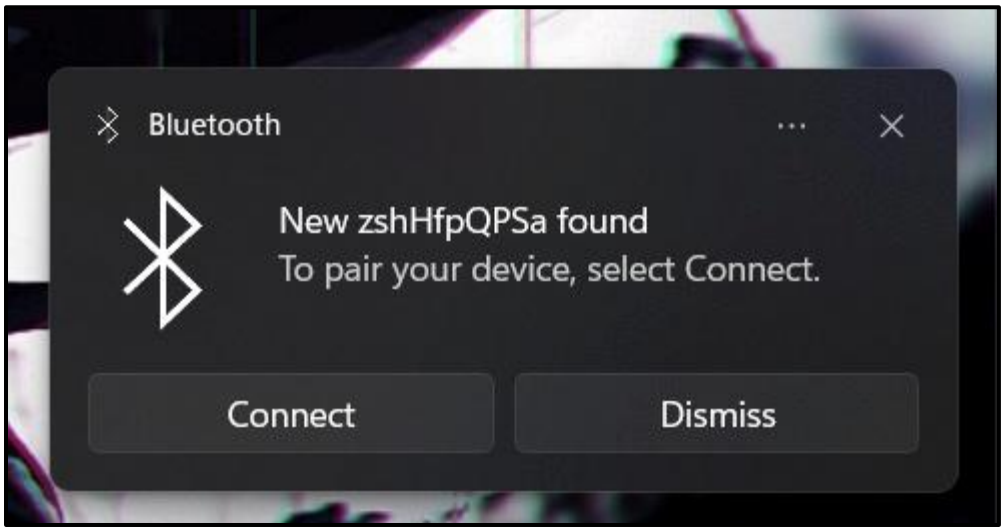


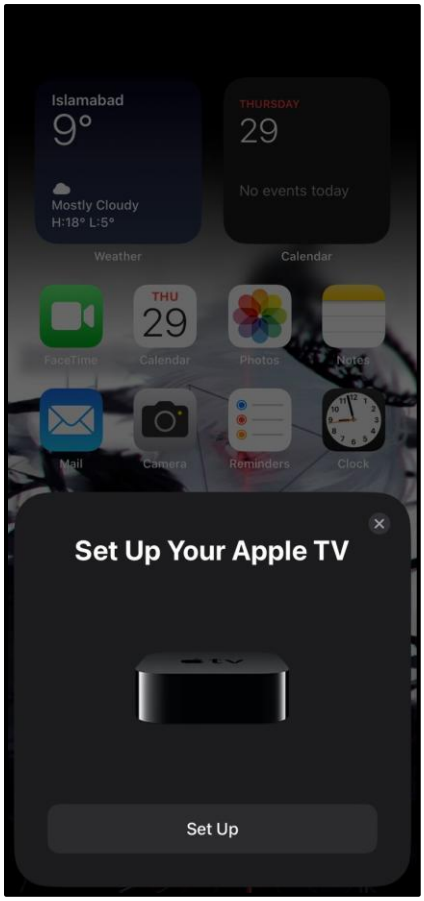
Main Project:

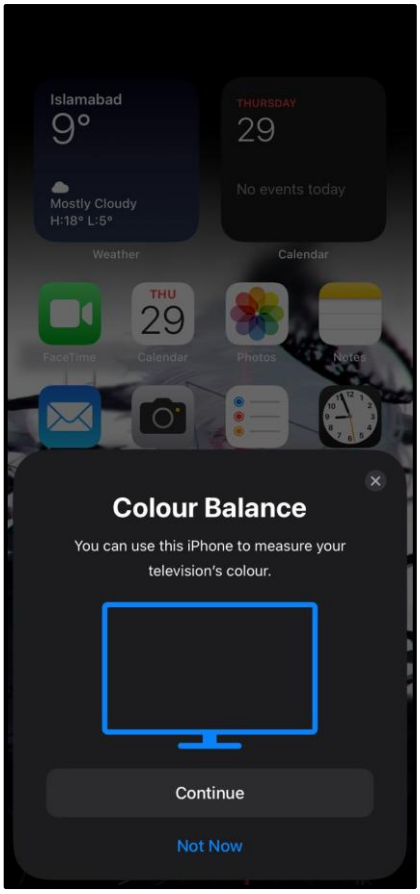


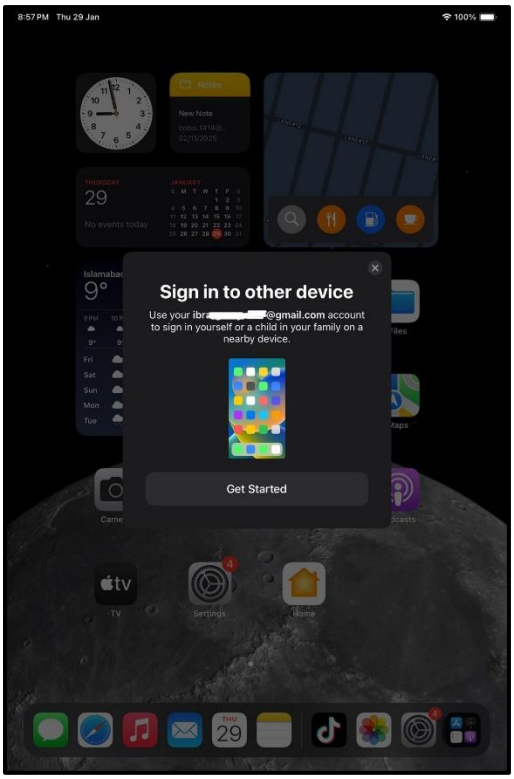
Bluetooth Attacks:

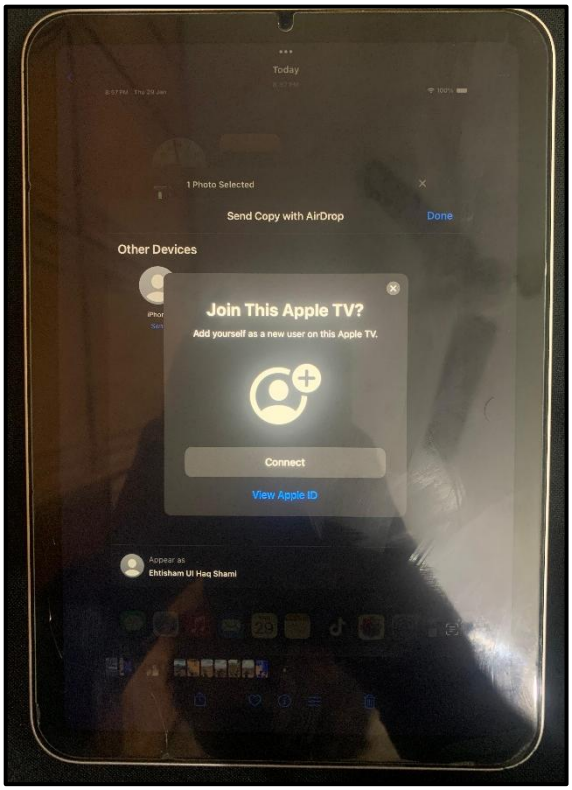
Demonstration:




Islamabad
9°
Mostly Cloudy
H:18° L:5°
Weather
THURSDAY
29
No events today
Calendar
FaceTime
THU
29
Calendar
Photos
Notes
Mail
Camera
Reminders
Clock
Set Up Your Apple TV
Set Up

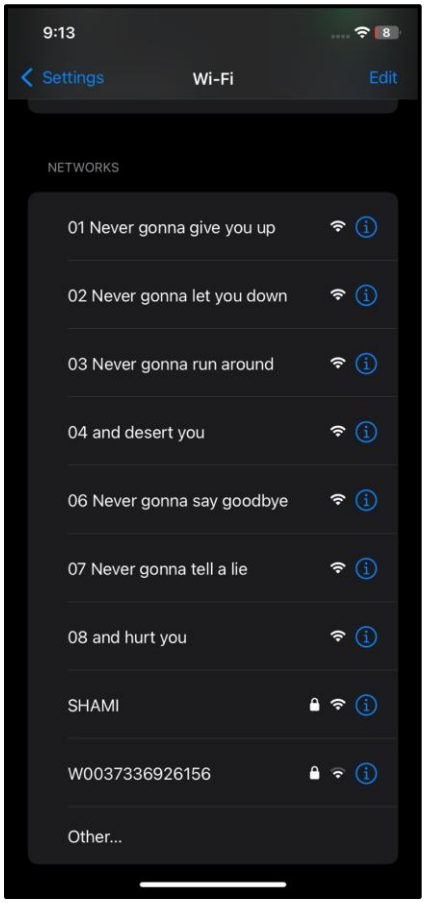

Islamabad
9°
Mostly Cloudy
H:18° L:5°
Weather
THURSDAY
29
No events today
Calendar
FaceTime
THU
29
Calendar
Photos
Notes
Colour Balance
You can use this iPhone to measure your television's colour.
Continue
Not Now


8:57 PM Thu 29 Jan
100%
Sign in to other device
Use your ibr[redacted]@gmail.com account to sign in yourself or a child in your family on a nearby device.
Get Started
TV
Settings
Home

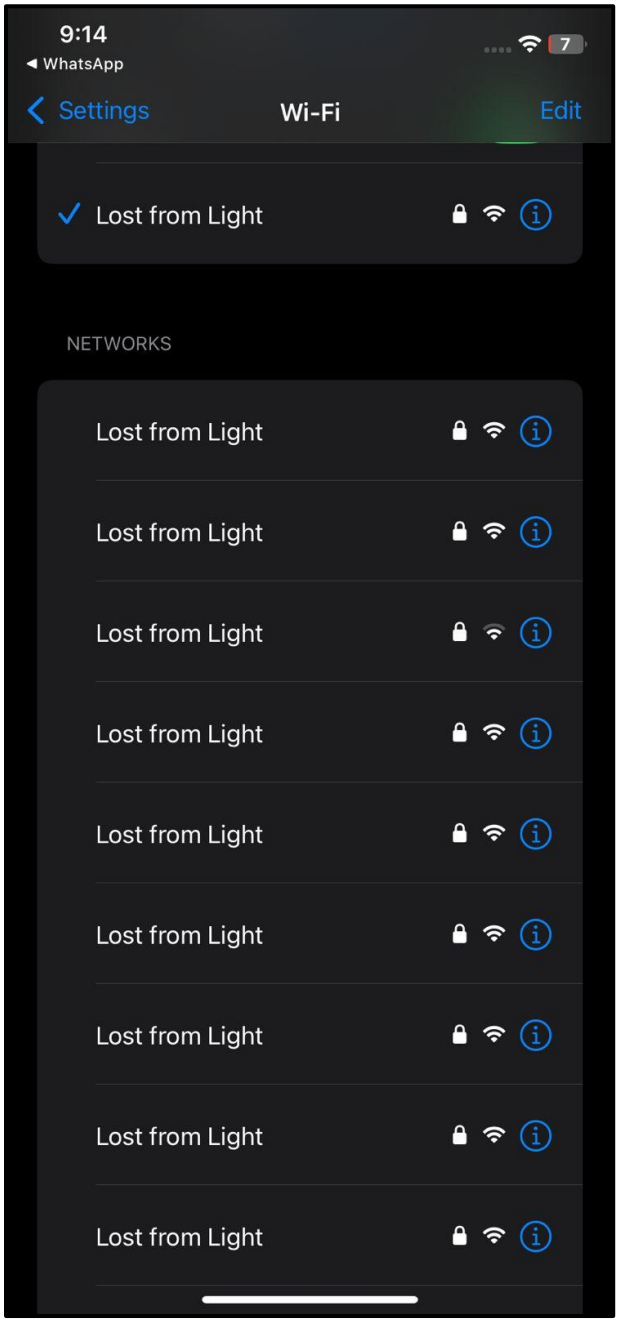

Today
1 Photo Selected
Send Copy with AirDrop
Done
Other Devices
Join This Apple TV?
Add yourself as a new user on this Apple TV.
Connect
View Apple ID
Appear as
Ehtisham Ul Haq Shami

Wi-Fi Attacks:

Rick Roll Spam:



AP Clone Spam:



De-Authentication Frames: