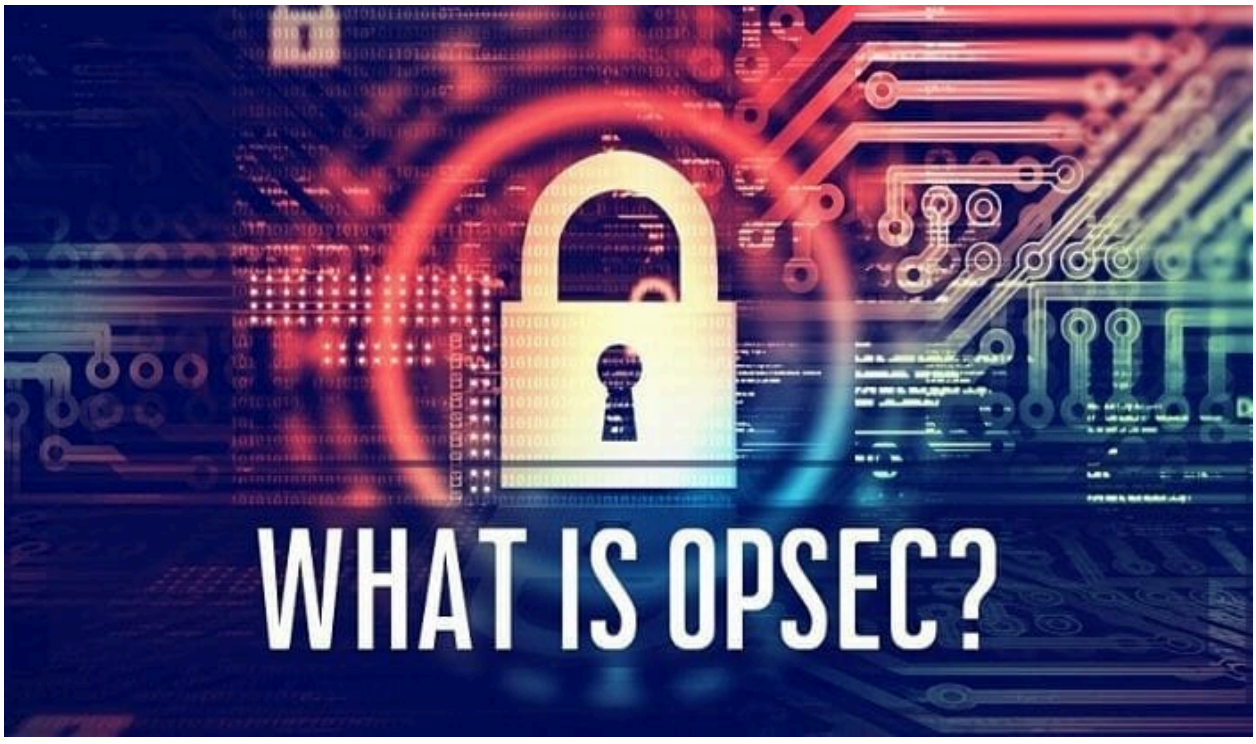
Piyush Bansal

Design and Implementation of a Hardware-Level Secure Computing Platform Using Physical Device Isolation and Live Operating Systems

Hardware Security • Privacy Engineering • Digital Forensics • Secure Systems



Abstract

Modern cybersecurity largely focuses on software vulnerabilities while neglecting the security risks embedded at the hardware and firmware layers. This project presents the

design and implementation of a physically isolated computing platform created by reverse-engineering a commercial laptop, removing its internal storage, and permanently disabling its camera and microphone at the hardware level. The system is then booted exclusively from a volatile operating system (Tails OS) running from external trusted media. The resulting device provides a high-assurance environment for anonymous communication, secure dark web research, and digital forensics by eliminating persistent storage, surveillance peripherals, and firmware-level data exfiltration risks. This work demonstrates how low-cost consumer hardware can be transformed into a high-security research terminal through physical and architectural controls.

Introduction

Commercial laptops are designed for convenience rather than security. Embedded components such as webcams, microphones, internal storage, and proprietary firmware create numerous attack surfaces that allow persistent surveillance and compromise. Software-based protections cannot fully mitigate these risks because firmware and hardware operate below the operating system's control.

This project explores whether a consumer laptop can be converted into a secure computing device through physical modification and architectural redesign rather than software alone.

This Project Involved:

- ☐ Reverse-engineering a laptop
- ☐ Removing and isolating storage
- ☐ Physically disabling microphone and camera
- ☐ Booting only from a trusted external OS (Tails)
- ☐ Ensuring the device cannot spy, store data, or leak identity

This creates a high-trust air-gapped privacy workstation, suitable for:

- ☐ Secure research

- ☐ Digital forensics
- ☐ Investigating dark web activity
- ☐ Threat-modeling adversarial surveillance

Objectives

The core objectives of this project were:

- ☐ To understand how **hardware components contribute to privacy risks**
- ☐ To eliminate all **built-in surveillance vectors**
- ☐ To build a **forensic-safe operating environment**
- ☐ To safely access sensitive networks (like Tor / Dark Web)
- ☐ To explore **hardware-rooted trust models**

Threat Model

This project assumes the following threats:

Threat	Description
Built-in webcam	Webcam monitoring
Built-in microphone	Microphone capture
Internal hard disk	Disk-based persistence
Intel ME / firmware	Intel ME / BIOS backdoors
Wi-Fi MAC tracking	MAC address & fingerprinting
Malware persistence	System compromise

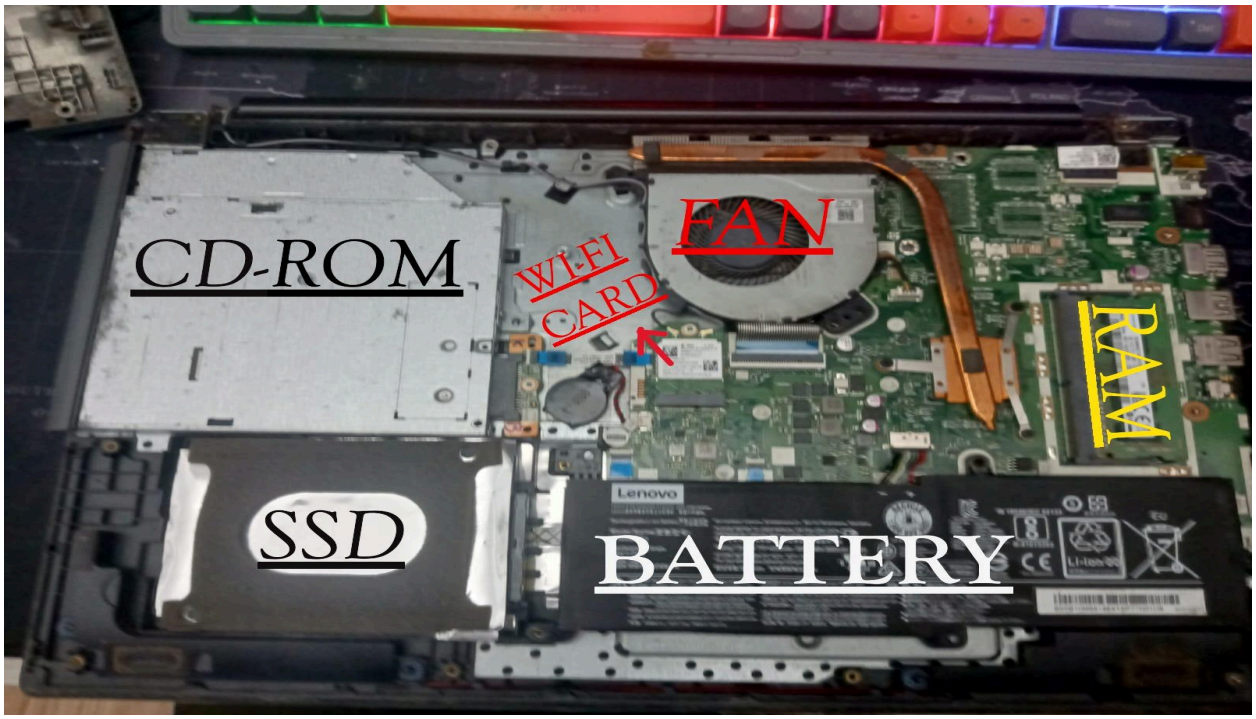
The goal was to **remove trust from the manufacturer** and replace it with **physical and cryptographic control**.

Hardware Reverse Engineering

The laptop was fully disassembled to analyze and isolate critical components.

Steps performed:

- ☐ Back panel removed
- ☐ Motherboard exposed
- ☐ Camera cable located
- ☐ Microphone cable located
- ☐ Storage interface traced
- ☐ Boot chain studied



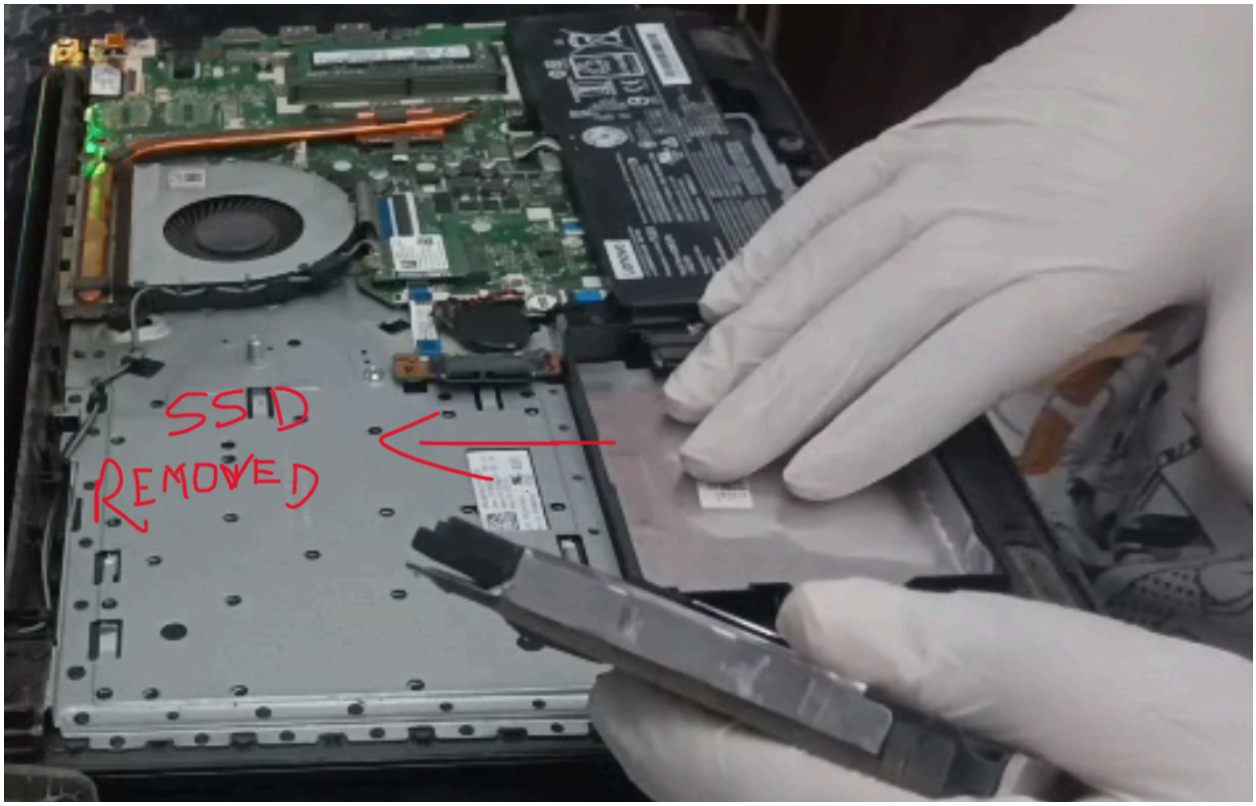
This step was essential to identify **all data-leaking hardware paths**.

Physical Removal of Storage

The internal SSD was completely removed.

Why this matters:

- ☐ Malware cannot persist after reboot
- ☐ No forensic traces remain
- ☐ OS runs entirely from trusted media



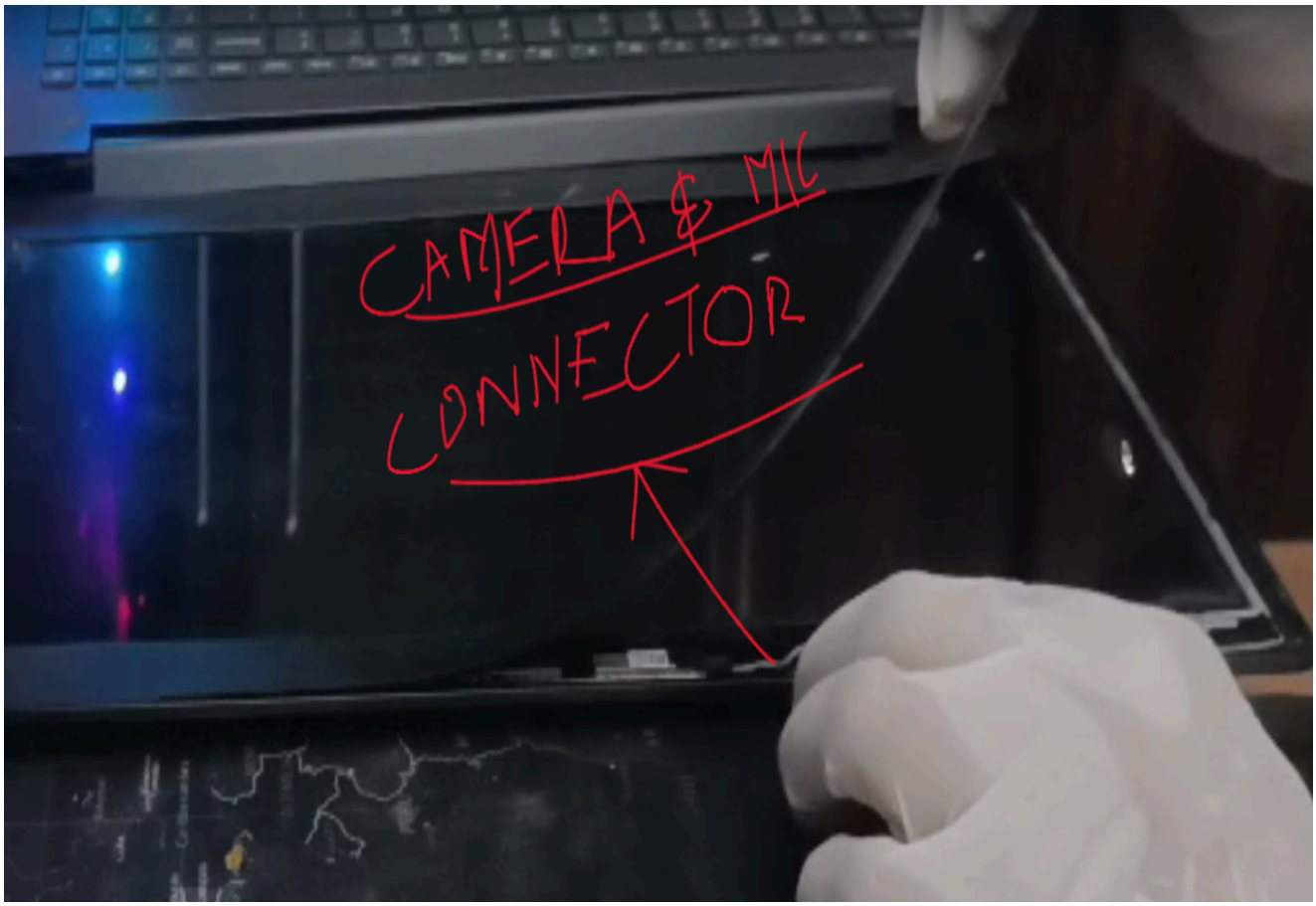
Without internal storage, the laptop becomes **stateless** — a key property of secure systems.

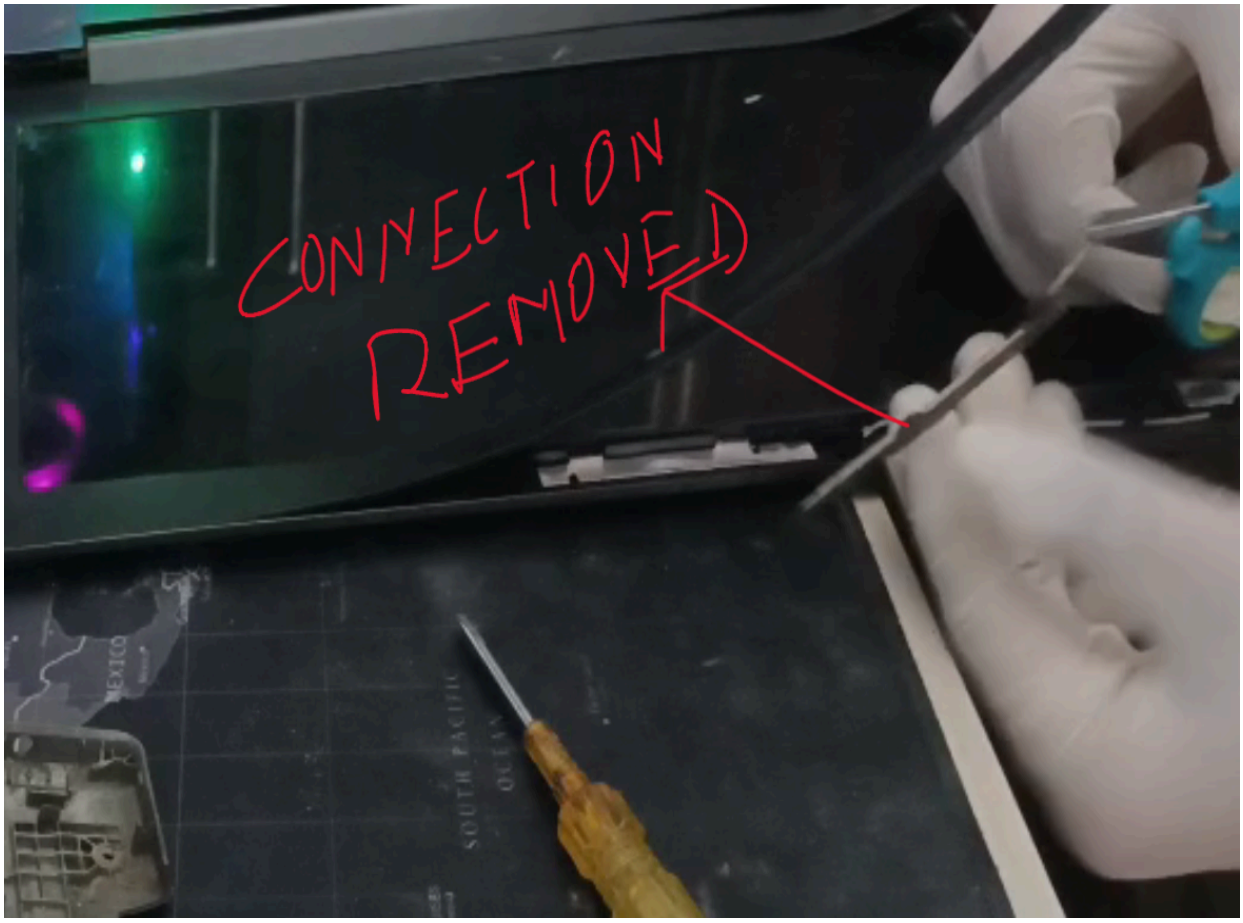
Hardware-Level Disabling of Camera & Microphone

Instead of relying on software or drivers, the camera and microphone were disabled **physically** by disconnecting their cables from the motherboard.

This guarantees:

- ☐ No firmware can re-enable them
- ☐ No malware can access them
- ☐ No remote activation is possible





This is the same method used in **military-grade secure terminals**.

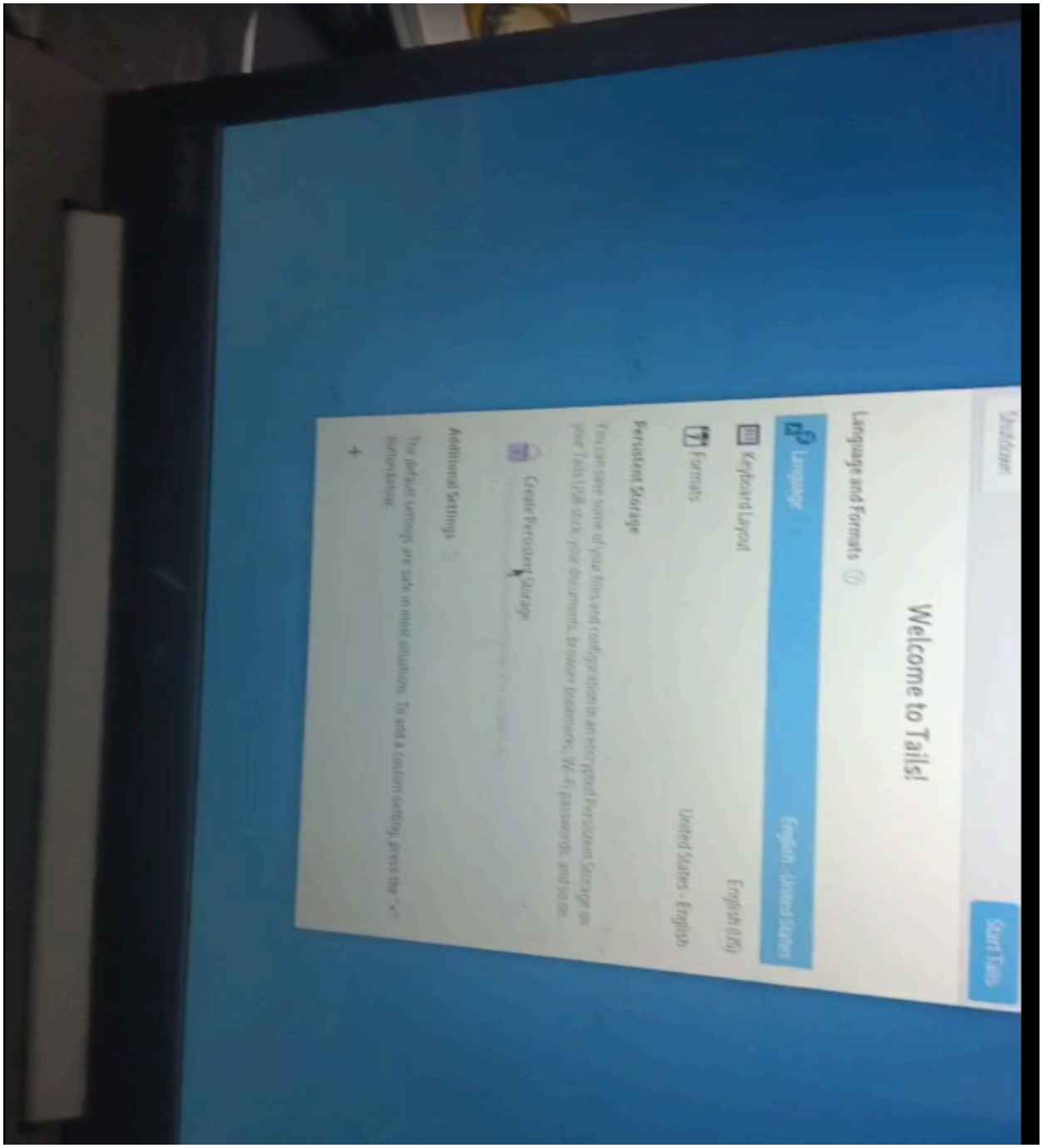
Booting from Trusted OS (Tails)

The laptop was configured to boot only from a **bootable USB drive** running **Tails OS**.

Tails provides:

- ☐ Tor-only internet
- ☐ Memory-only execution (RAM)
- ☐ Automatic data wipe on shutdown
- ☐ No disk usage

- ☐ Encrypted networking



This ensures:

Every reboot returns the machine to a clean, uncompromised state.

Secure Dark Web Access

With:

- No internal storage
- No camera
- No microphone
- Tor-only OS

The system is safe for:

- Dark web research
- Threat intelligence gathering
- Malware investigation
- OSINT
- Adversarial testing

There is:

- No way to track the device
- No way to record the user
- No persistent identity

This makes it a **controlled cyber-lab environment**.

Future Work (Planned Research)

The next phase of this project aims to go even deeper:

Removing Intel ME

Intel Management Engine runs below the OS and cannot be disabled normally.
Plan:

- Physically remove or neutralize Intel chip
- Use open-source firmware

Custom BIOS (Coreboot / Libreboot)

Install:

- Coreboot
- Custom secure boot chain
- Measured boot

This would give:

> Full control from silicon to software

Turning the laptop into a **research-grade trusted platform**.