Technical Appendix — Why My Environment Matters

Arch Linux on ThinkPad T15p Gen 1

My primary research machine runs Arch Linux with KDE Plasma 6 on a Lenovo ThinkPad T15p Gen 1:

- Intel® Core™ i7-10750H (12 threads)
- 32 GiB RAM (31.1 GiB usable)
- Intel UHD Graphics, Wayland session

Arch gives me:

- Rolling kernel and userspace (good for keeping ADB/Fastboot and USB stacks current)
- Full control over dependencies for AI tooling and security utilities
- Reproducible, scriptable environments for containerised testing

This matters because secure mobile research needs a host system that is transparent, controllable, and not artificially locked down.

Windows 10 Dual-Boot for Firmware Work

Some vendor tools and USB stacks are still Windows-centric, especially:

- OEM flashing utilities
- Some driver-dependent Fastboot/ADB workflows
- Device-recovery and official restore tools

Maintaining a Windows 10 dual-boot is standard practice in Android and device research. It lets me:

- Use official or vendor-preferred tools safely
- Restore the device to a known-good state if experiments break software
- Keep Nothing devices within supportable conditions as much as possible

MikroTik RouterOS — Zero-Trust Network Enforcement

My network edge runs MikroTik RouterOS. I use it to:

- Segment traffic by VLAN and interface
- Enforce default-deny policies
- Log and observe device communication patterns
- Model realistic, “small-organisation” Zero-Trust setups

The Nothing Phone 3a Pro lives inside this segmented environment as a controlled endpoint. This is closer to how security-conscious organisations actually deploy devices.

Docker-Based AI & Backend Services

AI and backend components run in Docker containers, which gives me:

- Isolation between services
- Easy rollback if a test breaks something
- Clear boundaries between "trusted" and "untrusted" components

When the Nothing phone talks to these services, I can precisely define and observe:

- What gets exposed
- How authentication happens
- How data moves between layers

Why NothingOS Is a Good Fit

NothingOS and your hardware are interesting for this research because:

- You stay close to AOSP behaviour, which reduces vendor-specific surprises
- Devices like the Phone 3a Pro and Phone (3) are powerful enough for local AI-assisted workflows
- The Glyph/Mirror interface can be used as an out-of-band signal channel for trust, status, or alerts
- CMF devices with microSD (e.g., CMF Phone 2 Pro) are rare and ideal for modelling removable, compartmentalised storage

In short, the combination of my environment and Nothing's devices is well-suited to building and documenting real-world secure mobile patterns, rather than purely theoretical models.