StrangeLab – CamUtil Chronicle & System Index

Purpose

This document is a consolidated reference for the StrangeLab CamUtil project. It captures architectural decisions, implemented features, data pipelines, and operational philosophy so progress is not lost across sessions.

Core Philosophy

- Local-first, offline-capable forensic observatory
- Evidence over assumptions; raw + readable data always paired
- Behavioral correlation > self-reported identity
- All devices treated as untrusted by default
- No cloud dependencies; Pi-class compatible outputs

CamUtil Application Overview (macOS)

- Network scanner with bounded concurrency
- Service detection: HTTP, RTSP, ONVIF, SSDP, ports
- BLE passive discovery with fingerprinting and confidence scoring
- Hard RTSP probe with diagnostics
- Unified Action Panel with auto-filled targets

Data Pipelines

- Network → Host Evidence → Confidence → Reports
- BLE Ads → Fingerprint → Metadata Decode → Confidence
- Pi-Aux → Local HTTP → Audit Merge

Export Structure

All exports live under ~/StrangeLab/scans/ with RAW and READABLE pairs for evidence, BLE fingerprints, runtime logs, device reports, and scan reports.

BLE Metadata & Decoding

- Bluetooth SIG Company IDs (local tables)
- Assigned Numbers for services/characteristics/descriptors

- 128-bit UUID normalization for readability
- Vendor UUIDs tracked as known-unknowns

Pi Architecture

- Pi #1: Append-only vault/logger with large SSD
- Pi #2 (Aux): BLE/Wi-Fi sensor node feeding CamUtil
- Local-only HTTP ingestion with shared secret

Current Status

- Feature-complete for production testing
- UI largely stable; only polish remaining
- BLE decoding tables being expanded to full datasets
- Next steps: DMG packaging + Pi integration