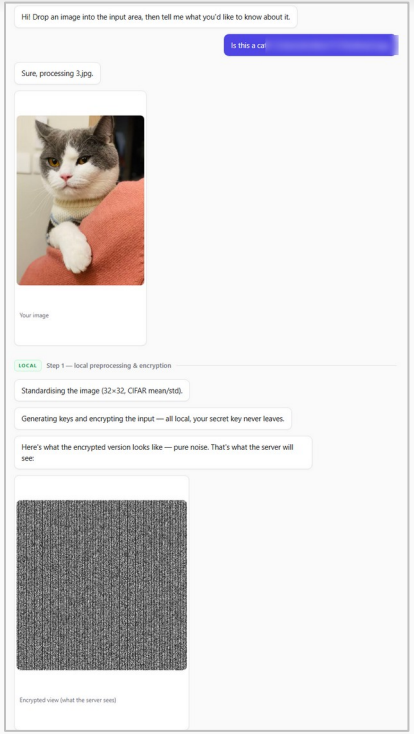
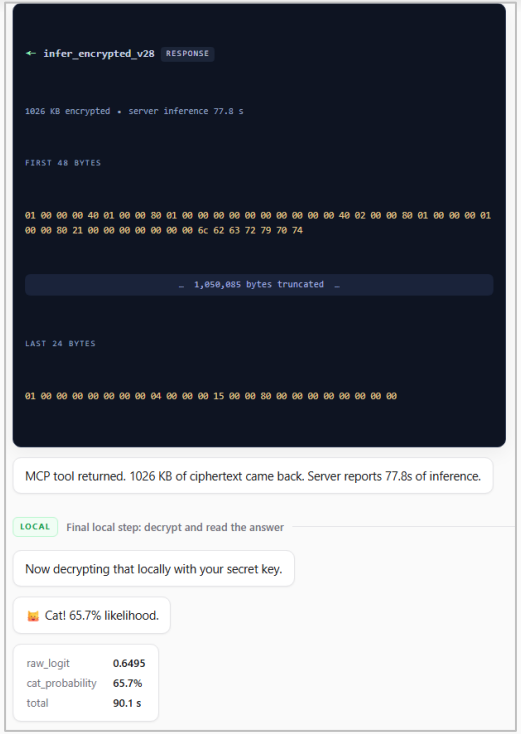
Hackathon: Cat Privacy





- **Stack** — OpenFHE / CKKS; CNN cat-vs-not-cat on an encrypted 32×32 RGB image; local crypto MCP server (stdio) + remote inference MCP server (HTTP, Docker-deployable) + chat web UI.
- **Homomorphic inference**: 77.8 s server-side (9-thread CPU).
- **End-to-end**: 90.1 s (preprocess, encrypt, upload, infer, decrypt).
- **Payloads** — encrypted input ≈ 192 MB; encrypted output logit ≈ 1 MB.
- **Keys** — evaluation keys ≈ 1.8 GB, provisioned once, cached via Key Reference.
- **This run** — "cat", probability 65.7%.
- This draft will be presented at Dispatch tomorrow morning (Monday, 20th July)

Scan → the draft

Scan → the repo

Try your own cat on the link:

I E T F