Tox

Frank Cash - BSides
Jacksonville 2016

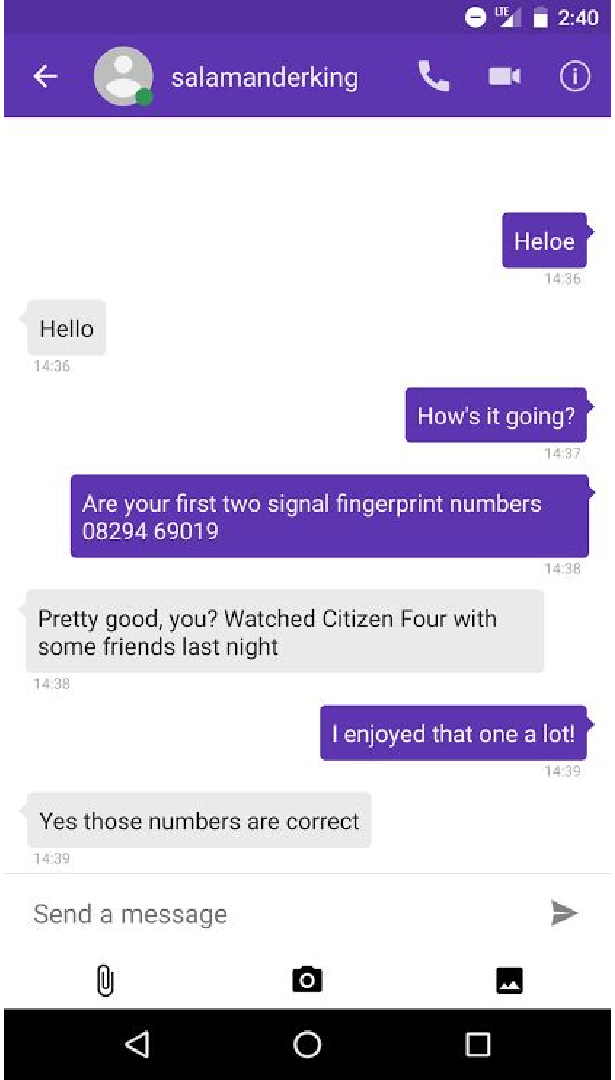
Who am I?

- Github: frankcash
  - Exitmap: Tor Node Mapper (contributor)
  - Felony: GPG Client in Electron (maintainer)
- Twitter: hackthethings
- Keybase: frankcash

- Software Engineer: 2 Years
  - Python
  - Java
  - Node.js
- Paranoid: Forever

Tox

- Distributed Messaging Service
- Supports
    - Instant Messaging
    - Voice Calls
    - Video Calls
    - File Transfers
- Open Source



Heloe
14:36

Hello
14:36

How's it going?
14:37

Are your first two signal fingerprint numbers 08294 69019
14:38

Pretty good, you? Watched Citizen Four with some friends last night
14:38

I enjoyed that one a lot!
14:39

Yes those numbers are correct
14:39

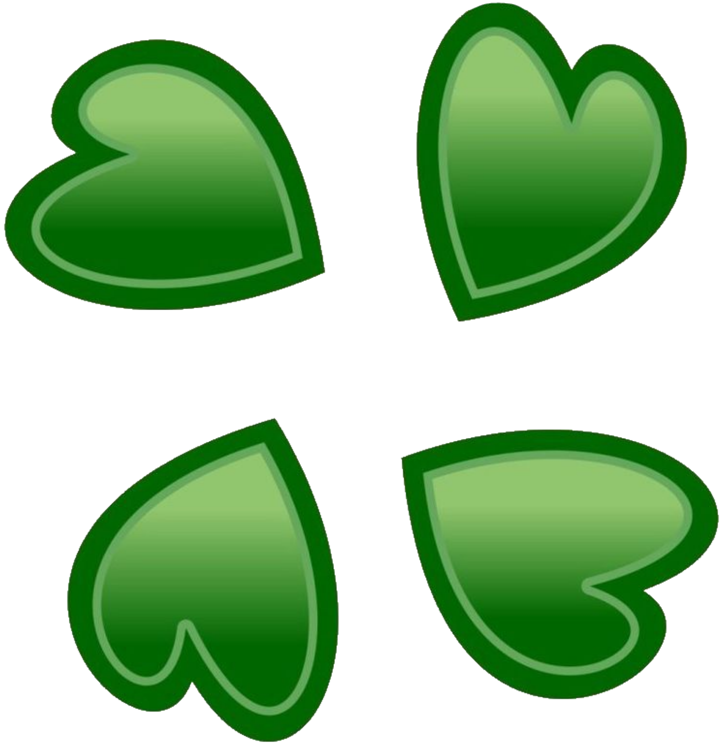
antox

Tox: A Timeline

- First commit: June 23, 2013
- “Stable” Alpha: February 3, 2014
- Google Summer of Code: 2014
- Google Summer of Code: 2015
- Tox developers split with Tox Foundation: July 13, 2015
- TokTok vs irungentoo: March 2016
- Tox Devs vs Foundation NSA Botnet Devs: March 31, 2016

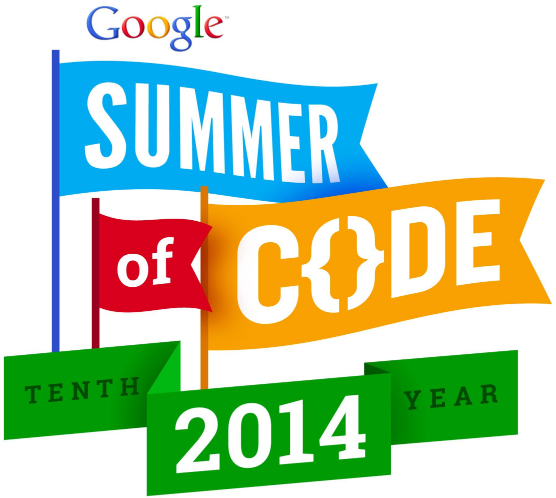
Tox: 2013

- Idea borne from 4chan
- Project Starts on Github
- Name decided: June 2013
- Toxic Client: July 2013
- DHT Working: August 2013
- Talks of Official Client: August 2013



Tox: 2014

- Tox Onion Routing for friend discovery: January 2014
- First “Stable”: February 2014
- uTox: March 2014
- Google Summer of Code 2014
  - Windows Client (lol)
  - Antox (Android)
- qTox: June 2014
- Posted on HackerNews: August 2, 2014



Tox: 2015

- Google Summer of Code 2015
  - Make Windows Clients Great Again
  - Better Android Client
  - Expands video features to iOS
- Tox Foundation Theft of $3,000: July 11, 2015

Tox: 2016

- Project TokTok hard forks irungentoo’s toxcore: March 2016
- Tox Developers against the Botnet: March 2016
- TokTok works on creating various version of toxcore
  - Haskell: July 1, 2016
  - Rust: Early 2016

Tox: A Protocol

- DHT Based
  - End-to-end encryption
  - Full decentralized
  - Resistance to basic DoS
- Peer-to-peer
  - Give up your IP to people you are communicating with
  - When finding a friend nodes you travel through will not get your IP
- UDP (with TCP fallback)
- Crypto
  - Relies on libsodium

Tox: Clients

- uTox (Desktop) (C)
- qTox (Desktop) (C++)
- Toxygen (Desktop) (Python 3.4)
- Antox (Android) (Scala)
- Toxicity (iOS) (Obj-C)

Tox: Extendable Tools

- toxcrawler
- Toxbot (groupchat bot)
- Python Bindings
- JVM Bindings

Tox Vs Signal

Benefits

- P2P and Decentralized
- E2E Encrypted
- Text, Voice, Video, File
- Desktop, iOS, Android

Cons

- SQL Database Attack (depends on client)
- Client Bootstrap Attack (to be done)
- QR Code Attacks (Mobile)

Benefits

- Centralized
- E2E Encrypted
- Out of Bounds Identity Verification
- Text, Voice, Video, File
- Desktop (Chromium), iOS, Android

Cons

- Man in the Contact Attack-ish

What came out of this for the Tox Community

- Toxcrawler: 2 Pull Requests (Still Open); 1 Issue (DHT Bootstrapping error)
- Antox: 1 Issue (UI Based)

Resources

- Tox Homepage
- TokTok Project
- ToxStats
- Sodium Crypto Library