Meson

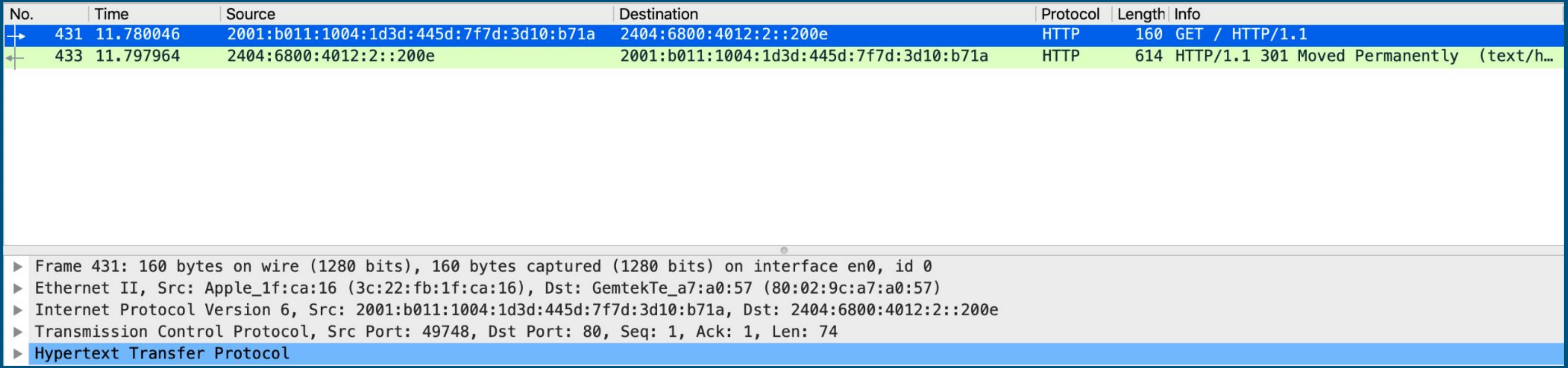
Peter Lai

Outline

- About metadata
- About anonymity
- About mix
- About meson mix
- Meson components & repos
- Running local testnet
- Reference

About metadata

- Who is connect to whom.
- How often and when to connect.



```
No.     Time        Source                                Destination                           Protocol  Length  Info
  431   11.780046   2001:b011:1004:1d3d:445d:7f7d:3d10:b71a   2404:6800:4012:2::200e                HTTP      160  GET / HTTP/1.1
  433   11.797964   2404:6800:4012:2::200e                2001:b011:1004:1d3d:445d:7f7d:3d10:b71a   HTTP      614  HTTP/1.1 301 Moved Permanently  (text/h…
```

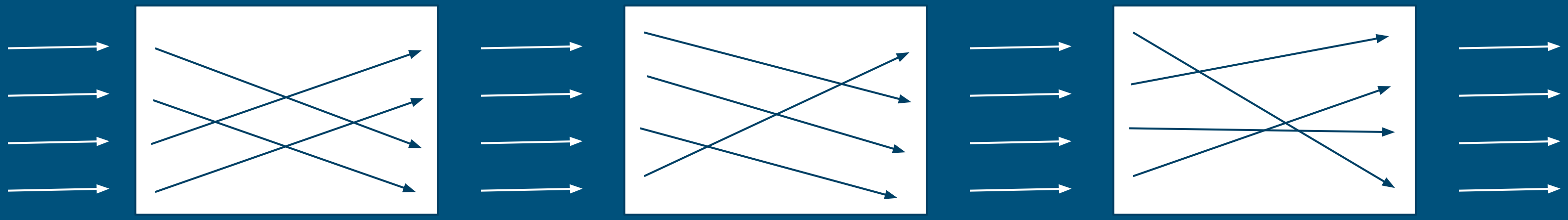
```
▶ Frame 431: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_1f:ca:16 (3c:22:fb:1f:ca:16), Dst: GemtekTe_a7:a0:57 (80:02:9c:a7:a0:57)
▶ Internet Protocol Version 6, Src: 2001:b011:1004:1d3d:445d:7f7d:3d10:b71a, Dst: 2404:6800:4012:2::200e
▶ Transmission Control Protocol, Src Port: 49748, Dst Port: 80, Seq: 1, Ack: 1, Len: 74
▶ Hypertext Transfer Protocol
```

About anonymity

- Encrypted network protocol
  - Network: TLS / PGP
  - Message: Signal / Telegram
  - Crypto: Zcash
- Protect metadata
  - identify user
  - trace online activities and analyse social networks
- Solution:
  - VPN
  - ToR
  - MIX

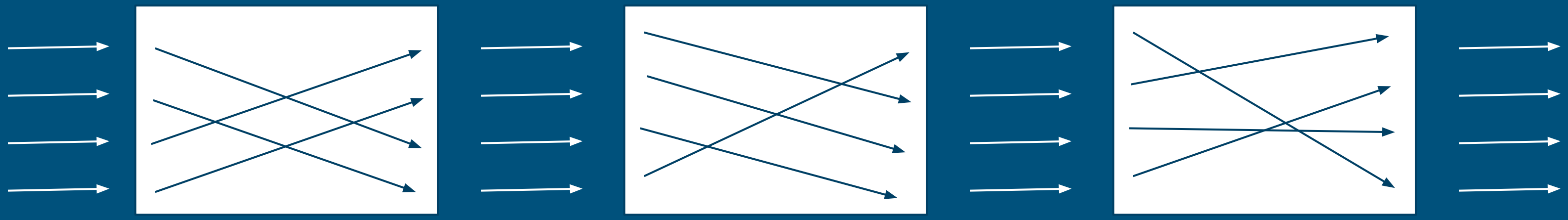
About mix

- Invented by David Chaum 1981
- Multi hop network
- Layer encryption
- Secure permutation
- Two mixing methods
  - Discret time (batch and reorder)
  - Continuous time (poisson mix)



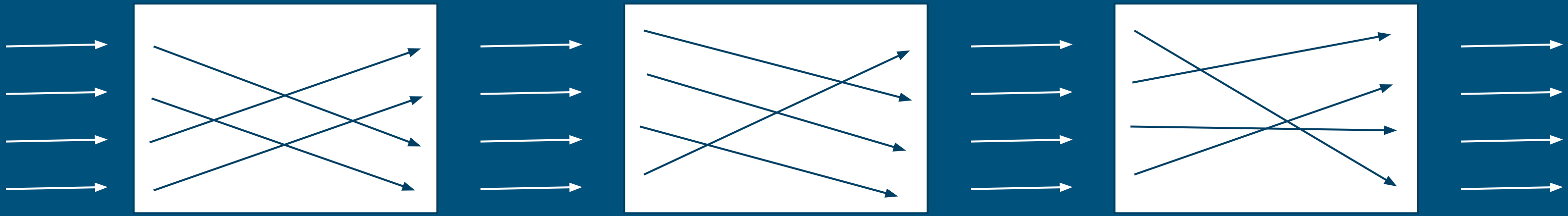
About David mix

- Casade Network Topolodgy
- Discret time (batch and reorder)



About meson mix

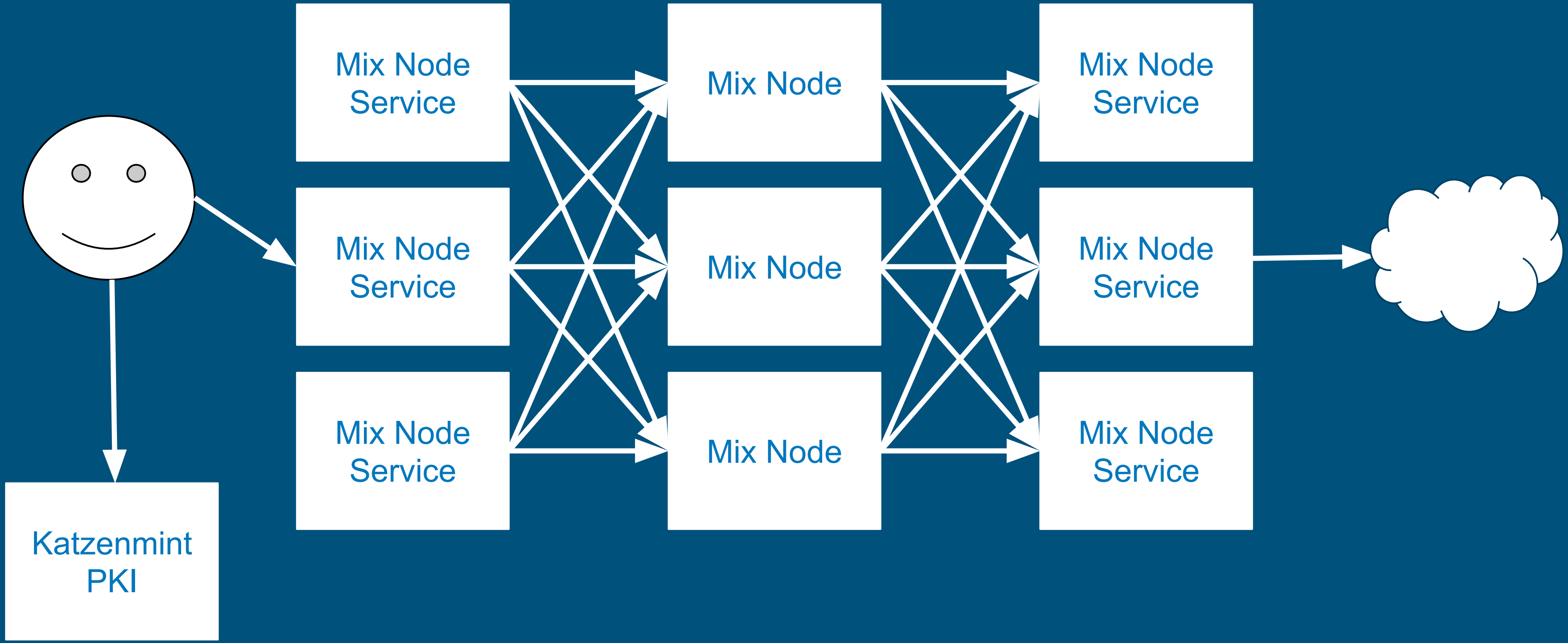
- Continuous time (poisson mix)
- Cover traffic
- Loopix https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/piotrowska
- Katzenpost https://katzenpost.mixnetworks.org/



Meson components & repos

- Katzenmint PKI
  - public key infrastructure for Meson
- Server
  - mix node
  - service provider
- Client
  - client to fetch pki document and connect through meson
- Genconfig
  - generate configs for meson testnet

Meson components & repos



Running local testnet

- clone repo from: https://github.com/hashcloak/Meson
- checkout to monorepo branch
- build katzenmint / server docker container
- go to katzenmint/docker/local: docker-compose up

Reference

- https://github.com/hashcloak/Meson
- https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/piotrowska
- https://github.com/katzenpost/
- https://www.youtube.com/watch?v=5_-D18FkoAY
-