

# IETF Hackathon

- IETF 106
- Nov. 16-17, 2019
- Singapore (Mauritius remotely)



# Hackathon Plan

- TLS 1.3
  - SSH (XMSS support)

(<https://tools.ietf.org/html/draft-mu-curdle-ssh-xmss-00>)

- Http 451 (drupal module)

# What got done

- Http451 fixes for drupal
  - TLS 1.3 for check-firewall.
  - XMSS SSHFP added to wireshark (PR merged)
  - XMSS SSHFP added to validns & upcoming in paramiko.
  - XMSS SSHFP added to webinterface
  - XMSS SSHFP for 2sshfp (PR merged)
  - XMSS SSHFP for edentata, terraterm, xelerance

# What we learned

- Still at the beginning for PQ crypto (XMSS, LMS, and others coming up).
- We are going to be busy next year.

# Wrap Up

Team members:

Codarren Velvindron

Kishan Takoordyal

Jaykisha Mutkawoa

Nathan Mangar

Kifah Meeran

Terry Naiken

Ajay Bagha

Jeremie Daniel

[https://github.com/  
cyberstormdotmu](https://github.com/cyberstormdotmu)