TOR Log

- Logs any identified TOR routers used for anonymizing Internet traffic
- Searchable fields
  - TOR from server
  - TOR to server
  - Router nickname

"Slowing down the Internet"

- XKS goal is to store the full-take content for 3-5 days, effectively "slowing down the Internet" so that analysts can go back and recover sessions that otherwise would have been dropped by the front end
- Meta-data is saved off longer, with the goal of 30 days retention
- A lot of analysis can be done through meta-data only (MARINA is meta-data only)

What makes XKS so good at SIGDEV?

- XKS gives analysts unique access to terabytes of content and meta-data
- Typically sites select and forward to PINWALE less than 5% of the DNI they're processing
- The rest of that data used to be dropped but is now being retained temporarily and made available to analysts through X-KEYSCORE
- As an example, at one our sites XKS sees more data per day than all of PINWALE