Internet censorship is widespread across the globe. Repressive governments apply network interference mechanisms to prevent citizens to freely access and publish information online.

- IP blocking
- DNS Hijacking
- Deep Packet Inspection

Several multimedia-based covert channels have been proposed to evade censorship.

Existing tools fail at offering two key properties:
- Resistance against traffic analysis attacks;
- High throughput.

First to leverage WebRTC video streams for creating TCP/IP covert channels. Introduces a new encoding mechanism: Encoded media tunnelling. Achieves strong resistance against traffic analysis & high throughput. Works over a range of existing unmodified WebRTC apps (e.g., whereby.com).

Protozoa creates a covert channel over WebRTC video streams which are established securely.

Instrumentation of the WebRTC media pipeline allows for high throughput & traffic analysis resistance.

Protozoa is indistinguishable from legitimate WebRTC streams & achieves high throughput.

Protozoa can use multiple apps to build covert tunnels in countries known to experience censorship.