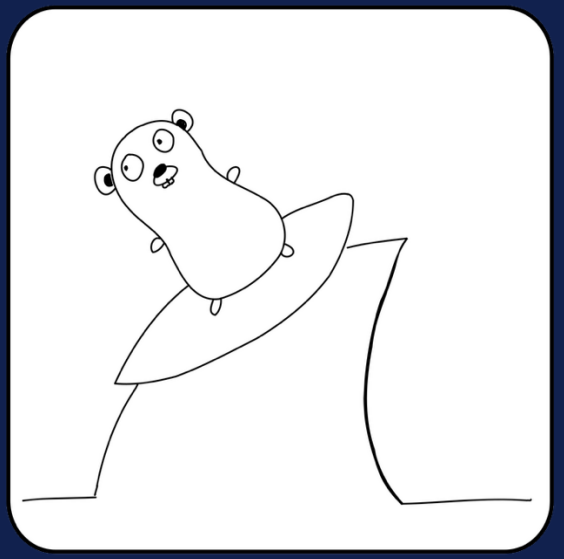
Lab



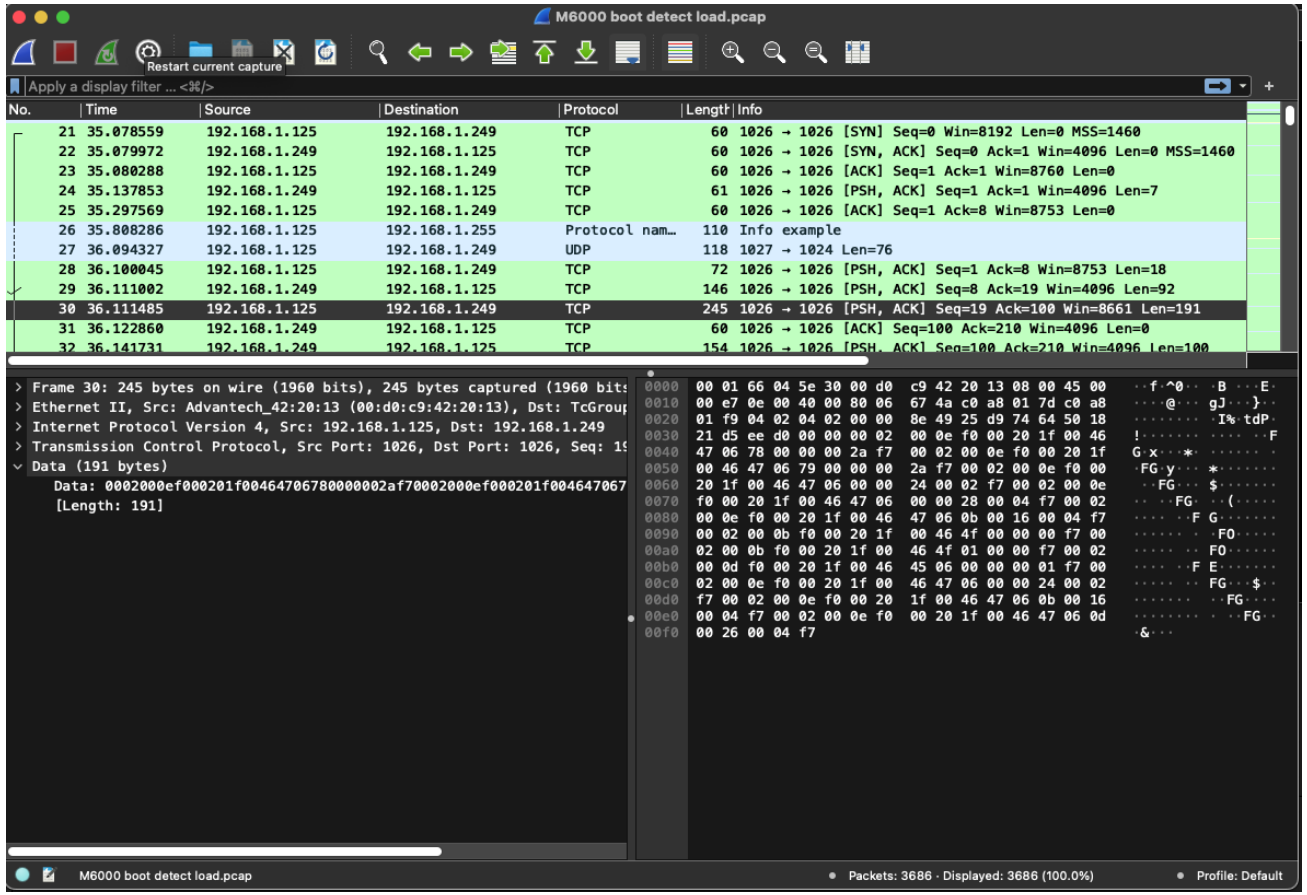
Wirego

One Wireshark plugin to rule them all

Benoît Girard

Quarkslab

NETWORK PROTOCOL REVERSE




```go
func (p *TCPParser) Parse(packet gopacket.Packet, ip *layers.IPv4, tcp *layers.TCP) {

  if len(tcp.Payload) == 0 {
    return
  }
  p.logs.Println("************************************************************")
  p.logs.Printf("[TCP Packet] RAW Payload %d bytes (0x%d)\n", len(tcp.Payload), len(tcp.Payload))
  p.logs.Print("\n" + hex.Dump(tcp.Payload))

  if (ip.SrcIP.String() == p.frameIP) && (ip.DstIP.String() == p.iconIP) {
    p.logs.Println("-> Frame to icon (tcp)")
    p.ParseBlocks(tcp.Payload, common.FrameToIcon)
  } else if (ip.SrcIP.String() == p.iconIP) && (ip.DstIP.String() == p.frameIP) {
    p.logs.Println("-> Icon to frame (tcp)")
    p.ParseBlocks(tcp.Payload, common.IconToFrame)
  }
}
```

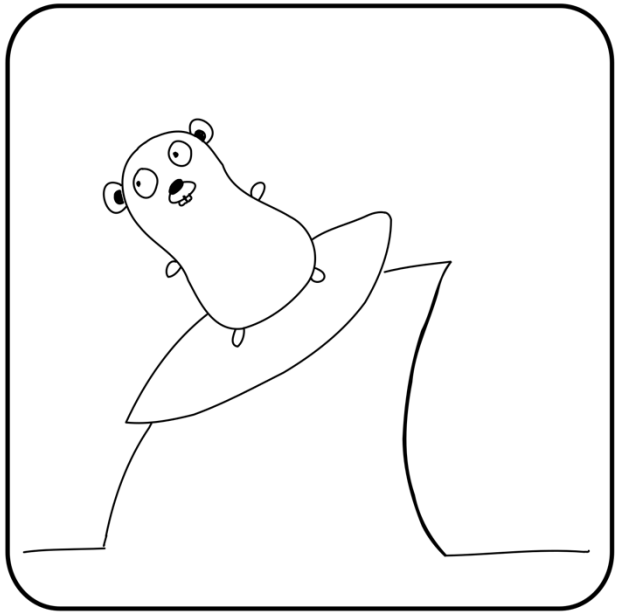
WIRESHARK

- First release in 1998
- Plugins can be developed in:
  - C
  - LUA (2006)
  - Python (support removed in 2014)

WIREGO - GOALS

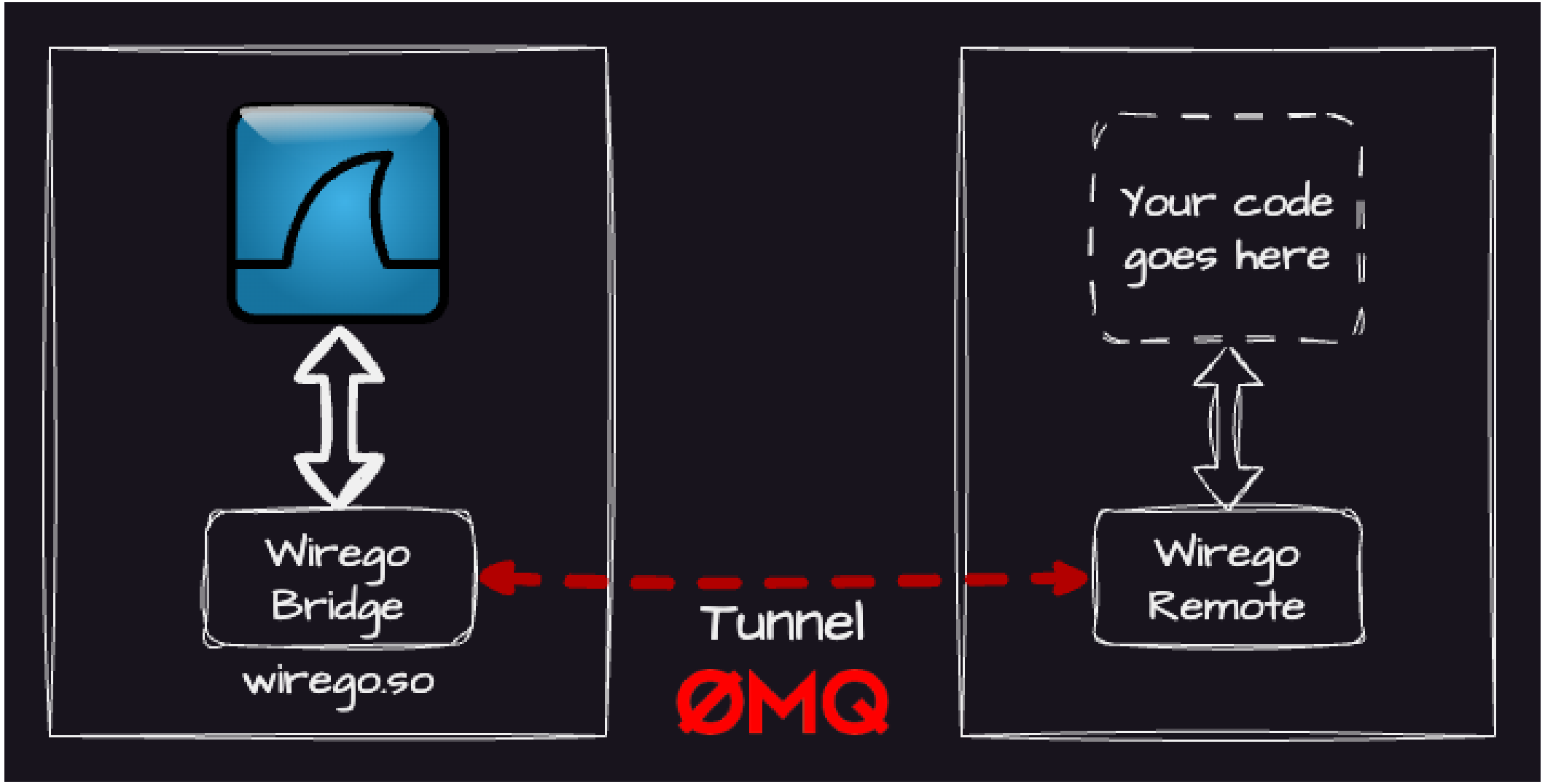
Goals:

- Develop a Wireshark plugin
- In less than 100 code lines
- Without having to build Wireshark
- Without having to read the documentation *
- In any language



* You won’t read it anyway

WIREGO - ARCHITECTURE



ZEROMQ

- High performance asynchronous communication library
- Available on most platforms
- And most languages

WIREGO - DEMO

Let’s develop a Wireshark plugin for a studio recording console (SSL AWS 900)

- On port UDP 50081
- Packets format:

Offset	Size	Description
0	4	Command Code
4	4	DestCode
8	4	Desk Serial
12	4	Remote Serial
16	…	Command Data

CONCLUSION

- Wirego remote packages are already available for:
  - Go
  - Python
  - Rust (thanks to Tomasz Woszczynski)

Ressources	
Project	https://github.com/quarkslab/wirego/
Documentation	https://github.com/quarkslab/wirego/tree/main/doc
Examples	https://github.com/quarkslab/wirego/tree/main/wirego_remote/go/examples https://github.com/quarkslab/wirego/tree/main/wirego_remote/python/examples

Thank you

Contact info:

Email: bgirard@quarkslab.com

Website: https://github.com/quarkslab/wirego/

@quarkslab