Lab

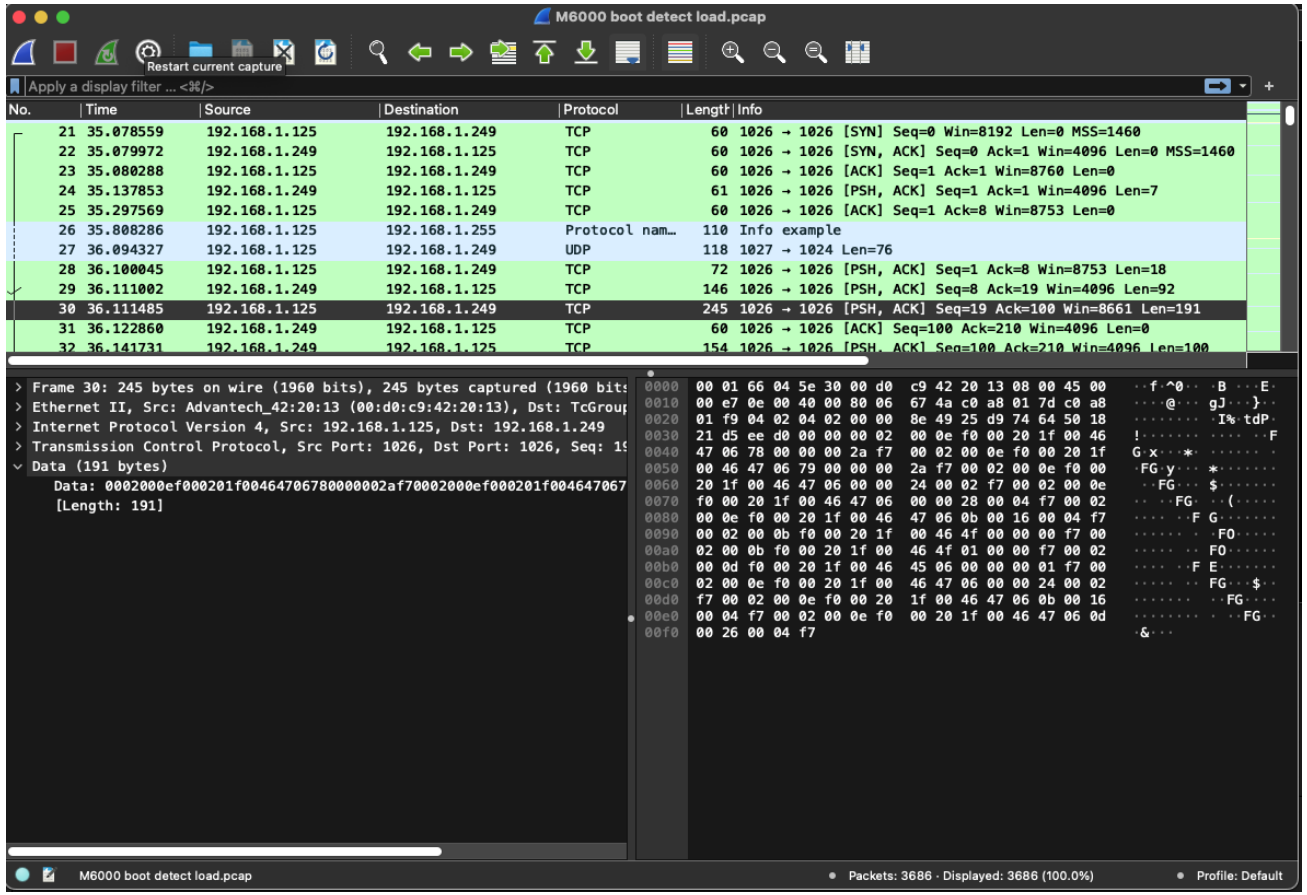
Wirego

Un plugin Wireshark pour les contrôler tous

Benoît Girard

Quarkslab

REVERSE DE PROTOCOLE RÉSEAU




```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)
  }
}
```

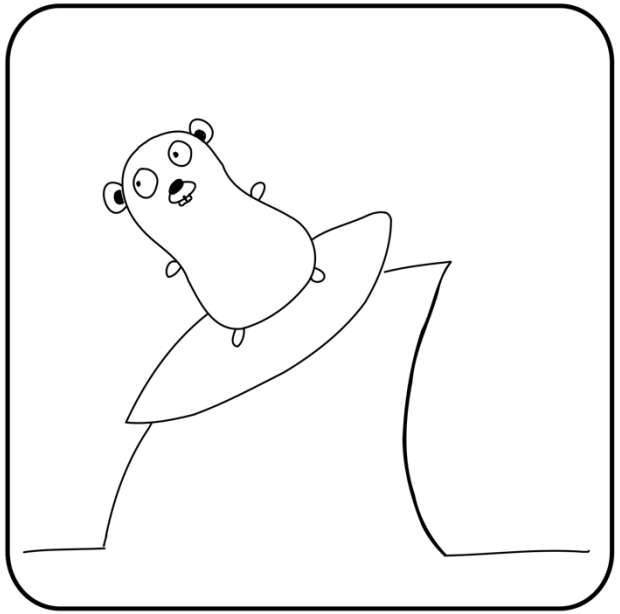
WIRESHARK

- Créé en 1998
- Possibilité de développer des plugins:
  - en C
  - en LUA (2006)
  - en Python (supprimé en 2014)

WIREGO - OBJECTIFS

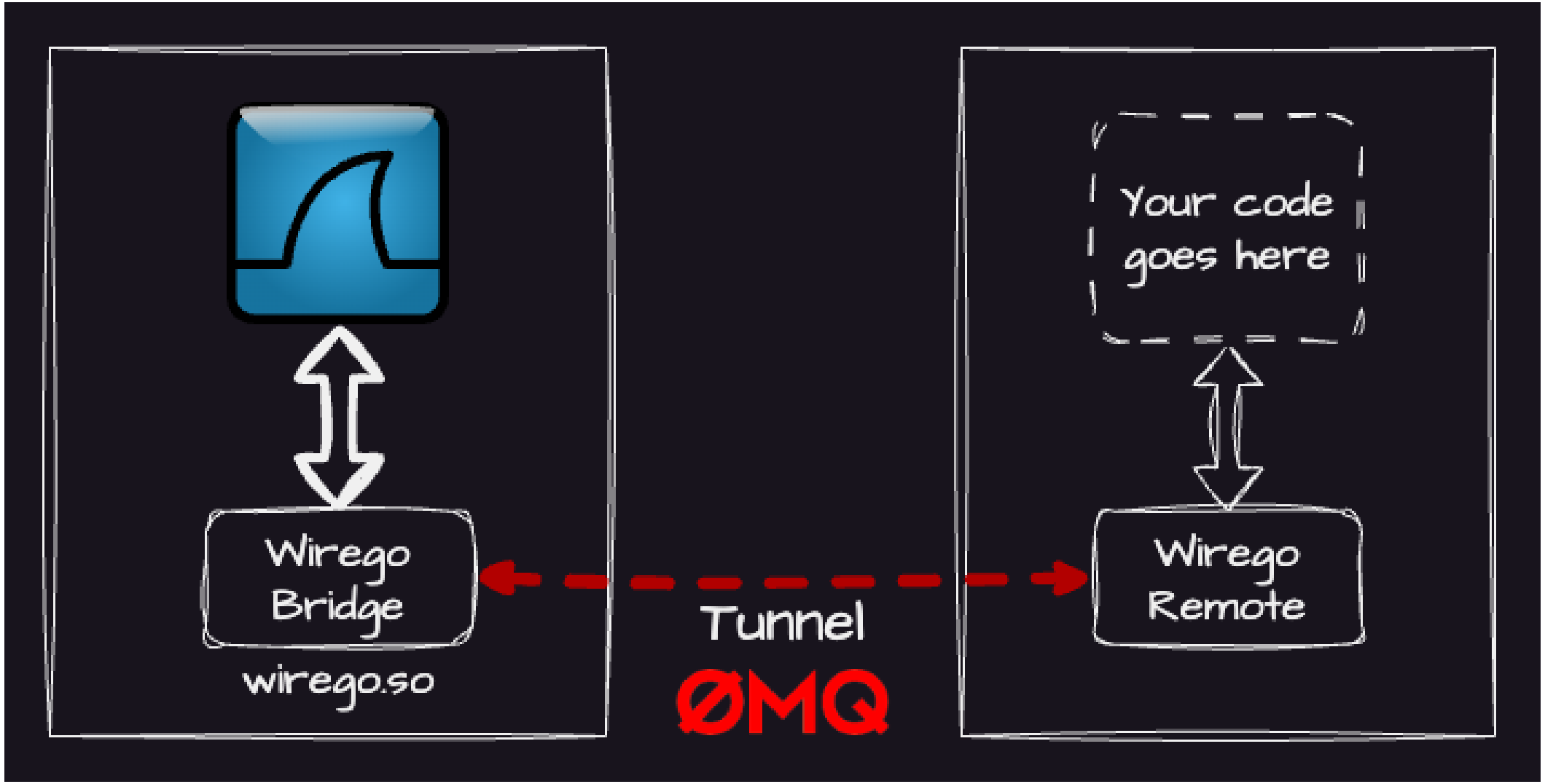
Objectifs:

- Permettre de développer un plugin Wireshark
- En moins de 100 lignes
- Sans avoir besoin de compiler Wireshark
- Sans avoir besoin de lire la documentation
- Dans n'importe quel langage *



* Sauf WinDEV

WIREGO - ARCHITECTURE



ZEROMQ

- Librairie de communication asynchrone haute performance
- Disponible sur la plupart des plateformes
- Et dans la plupart des langages

WIREGO - DEMO

Plugin Wireshark pour une console d'enregistrement (SSL AWS 900)

- Port UDP 50081
- Format des paquets:

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

CONCLUSION

- Packages disponible en:
  - Go
  - Python
  - Rust (merci à Tomasz Woszczynski)

Ressources	
Le projet	https://github.com/quarkslab/wirego/
Documentation	https://github.com/quarkslab/wirego/tree/main/doc
Exemples	https://github.com/quarkslab/wirego/tree/main/wirego_remote/go/examples https://github.com/quarkslab/wirego/tree/main/wirego_remote/python/examples

Merci

Information de contact:

Email: bgirard@quarkslab.com

Site Internet: https://github.com/quarkslab/wirego/

@quarkslab