Wireshark Configuration Profiles

... increase your Wireshark efficiency!

Sake Blok

Relational therapist for computer systems

sake.blok@SYN-bit.nl

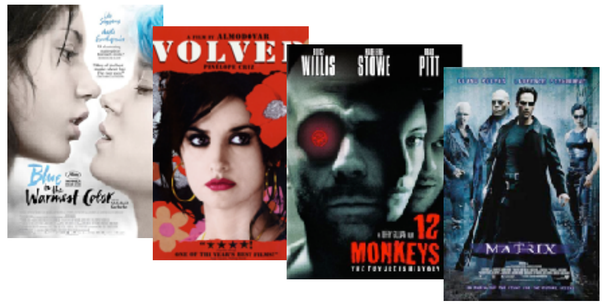
$ whoami

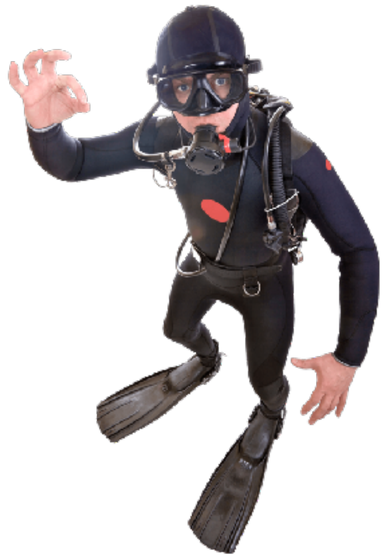
EURONET INTERNET

ABN·AMRO

ion ip

SYN-bit
deep traffic analysis





SYN-bit

deep traffic analysis

Application and network troubleshooting

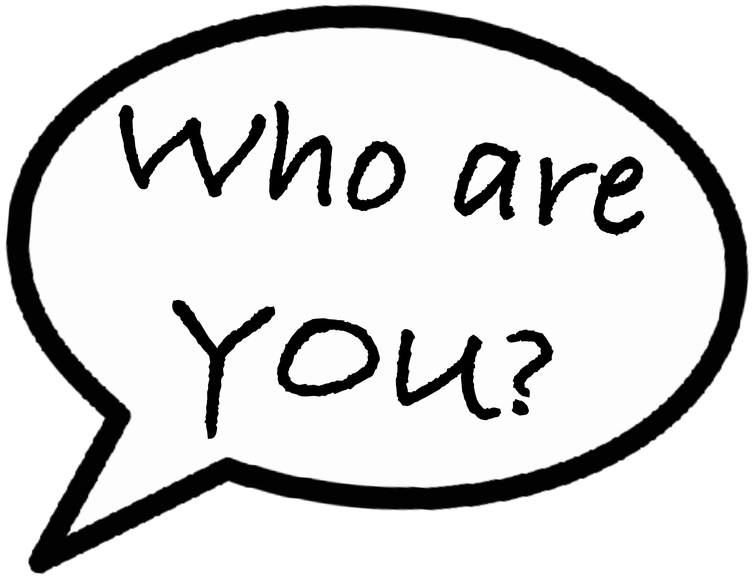
Protocol and packet analysis

Training (Wireshark, TCP, SSL)

www.SYN-bit.nl

$ whoareyou

- How often do you use wireshark?
- Have you used configuration profiles before?



What is a configuration profile?

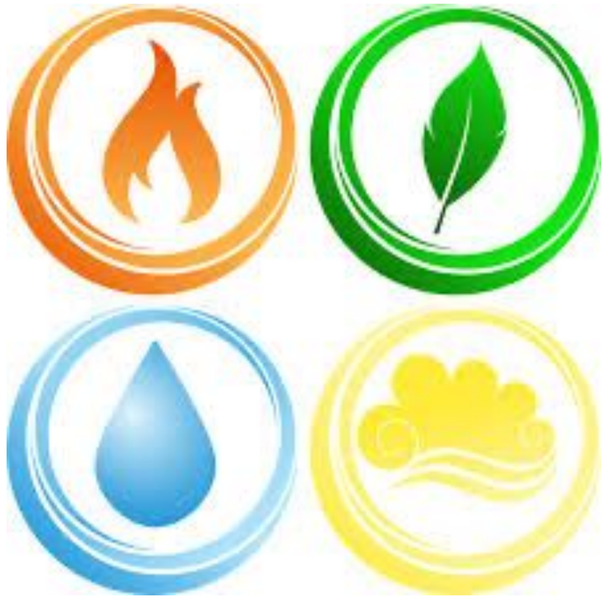
- all wiresharks customizations in one package
- Easily switch between profiles
- Optimize workflow
- Share profiles with others

Why use configuration profiles?

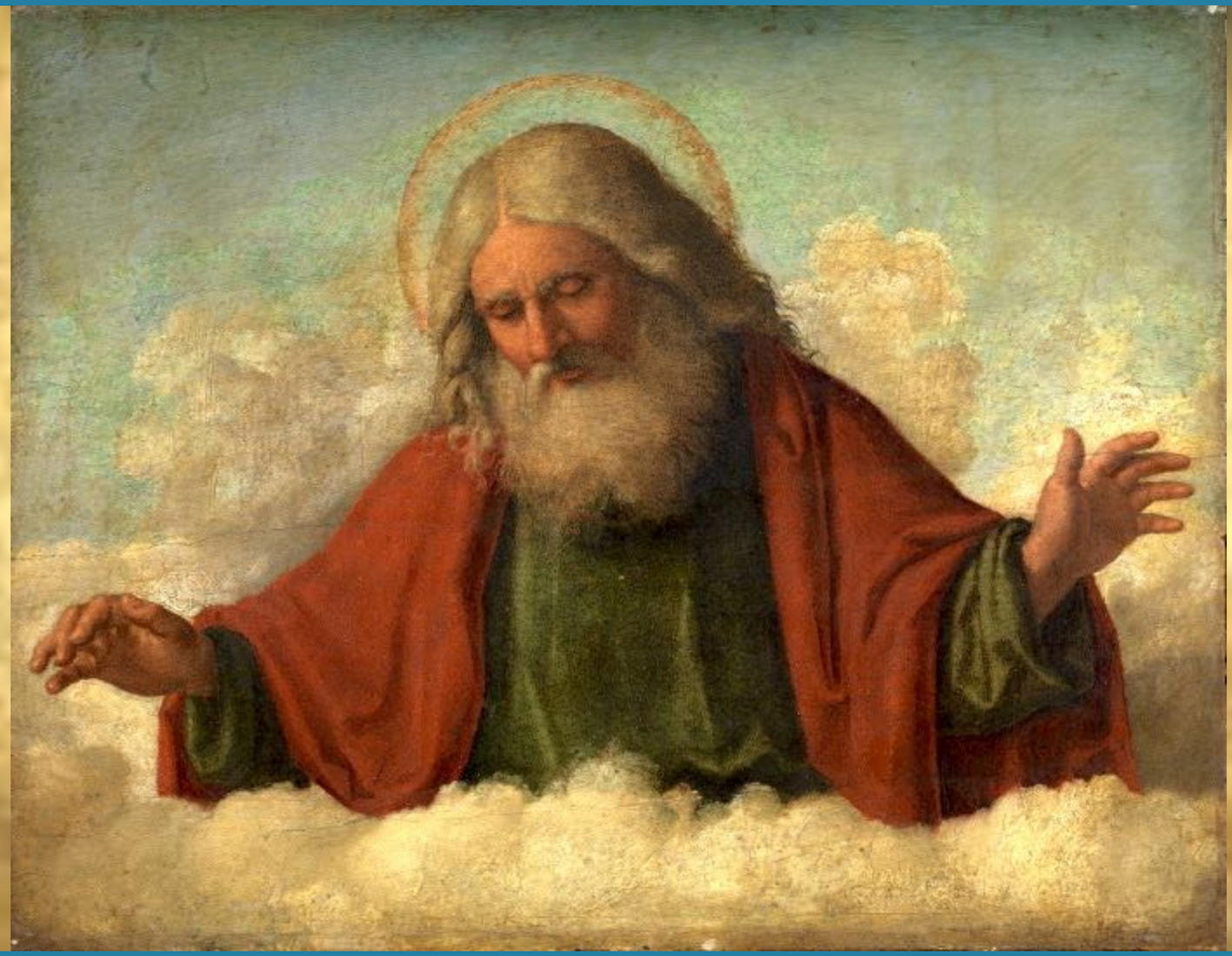
- Differentiate your analysis workflow
  - Per protocol?
  - Per application?
  - Per customer?
- Increase performance
  - disable protocols
  - disable reassembly etc.
- Adapt to different setups (e.g. screen size)

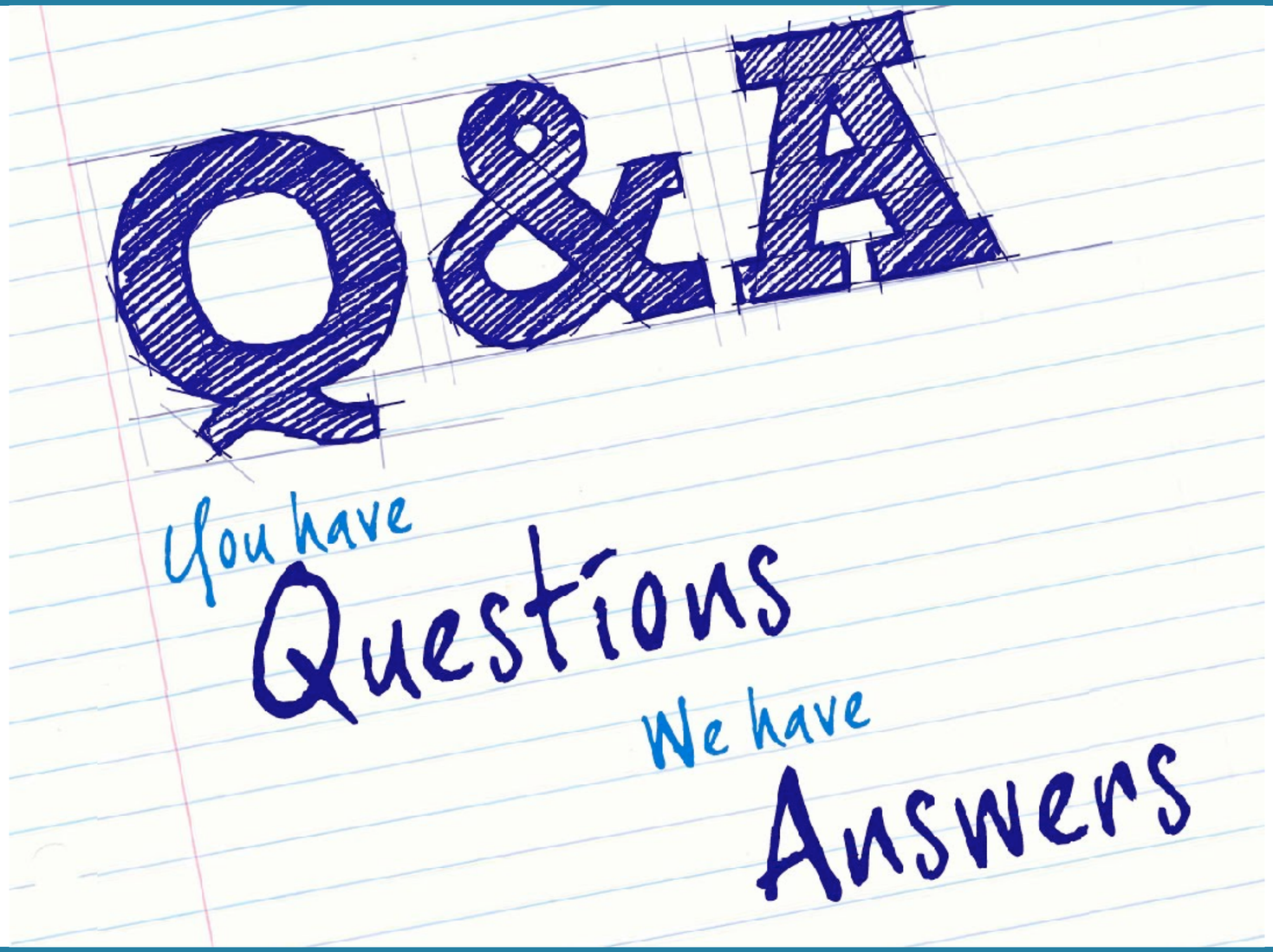
Common Elements

- GUI
  - Layout
  - Columns
  - Colors
- Workflow
  - filter buttons
  - name resolution
- Dissection
  - Enabled protocols
  - Protocol preferences



$ demo




Q&A
You have
Questions
We have
Answers

FIN/ACK/FIN/ACK

Still questions?

sake.blok@SYN-bit.nl

SYN-bit

deep traffic analysis