SHARKFEST '13

Wireshark Developer and User Conference

Top 5 False Positives when analyzing Networks

Jasper Bongertz, Senior Consultant

CASSIDIAN CyberSecurity

Topics

- Capturing data
  - CRC Errors, Under/Oversize, negative Delta times
- Unknown Services
- TCP Interpretation Errors
  - Retransmissions, Out of Orders, Zero/Full Window
- Delays

SHARKFEST '13

Wireshark Developer and User Conference

Thanks! Questions?

jasper@packet-foo.com
blog.packet-foo.com
@packetjay