SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Smart Move

Tips and Tricks for Network Analysts

Jasper Bongertz
G Data Advanced Analytics

About me

- Head of CSIRT at a Cybersecurity Company in Germany
- Former Network Forensics Analyst, now Incident Response Handler
- Creator of Tracewrangler
  - Need to start coding again…™

Agenda

- UI Tips & Tricks
- Filtering
- Analysis

UI Tips & Tricks

- Useful Custom Columns
  - Interface ID
  - TCP Flag Set
  - FQDNs
- Layered Addresses
- Toggling Protocol Settings
- Context Filtering

Filtering Tips

- Determining filter names
- "Equivalent" filters
  - Port vs. Protocol
  - Stream vs. Conversation
- Matching Replies to Requests
  - Requires 2 Pass filtering

Analysis

- Check capture consistency
  - Duplicates
  - Local captures
- TCP Initial Round Trip Time
- GeoIP Name Resolution

Mail: jasper@packet-foo.com
Web: blog.packet-foo.com
Twitter: @packetjay