

# SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE



## TraceWrangling: Preparing Food for the Shark



COMPUTER HISTORY MUSEUM

Jasper Bongertz

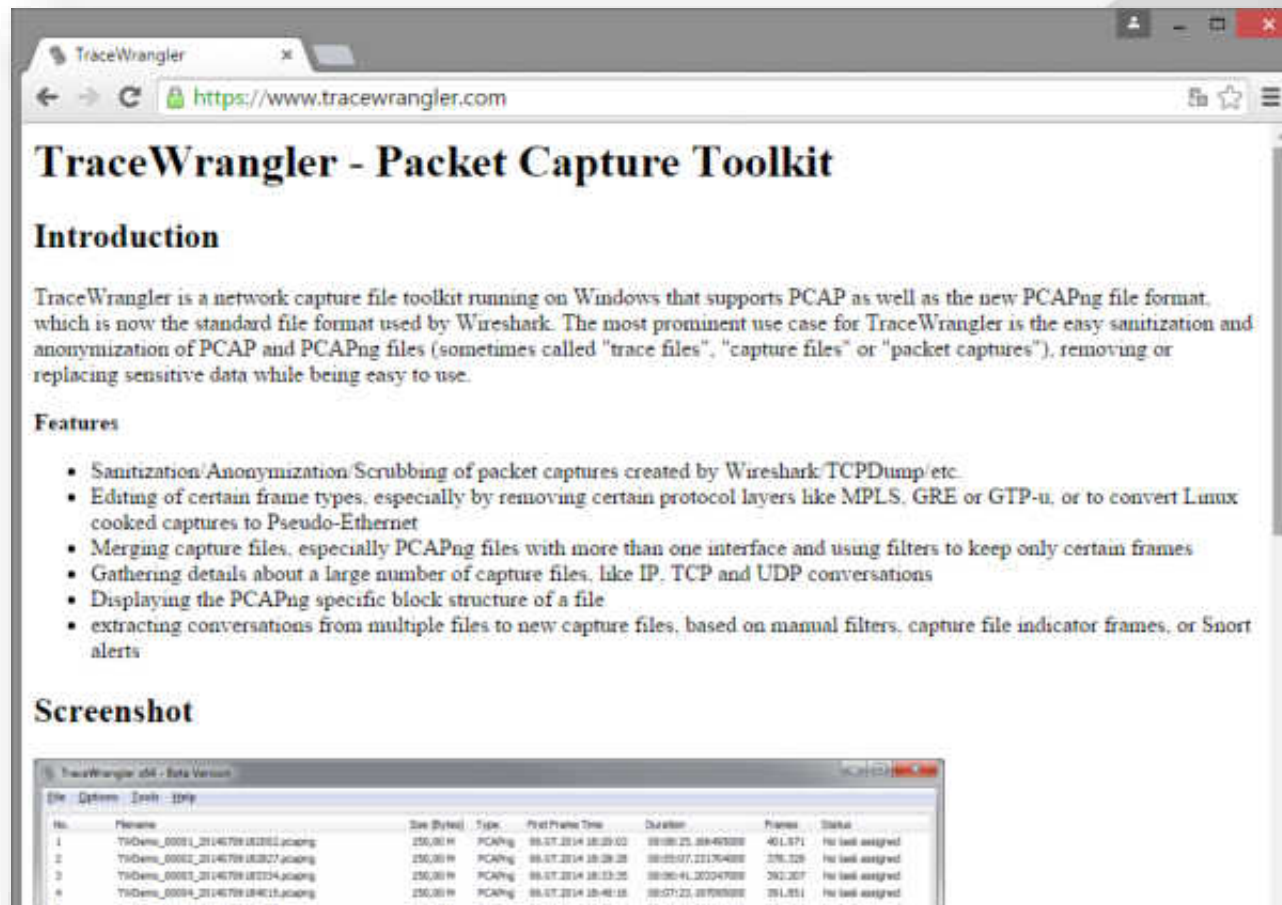
Airbus Defence and Space CyberSecurity

# TraceWrangler in general

- TraceWrangler performs tasks on a set of packet capture files:
  - sanitization/anonymization
  - merging files
  - batch editing packets
  - extracting packets into new files
  - capture file name/timestamp adjustments
  - endpoint/conversation overview over all files
  - basic TCP session state diagnostics
  - basic capture result validation

# Where to get it

- Download at <https://www.tracewrangler.com>



The image shows a browser window displaying the TraceWrangler website. The page title is "TraceWrangler - Packet Capture Toolkit". Below the title is an "Introduction" section and a "Features" list. At the bottom, there is a "Screenshot" section showing a preview of the TraceWrangler software interface.

## TraceWrangler - Packet Capture Toolkit

### Introduction

TraceWrangler is a network capture file toolkit running on Windows that supports PCAP as well as the new PCAPng file format, which is now the standard file format used by Wireshark. The most prominent use case for TraceWrangler is the easy sanitization and anonymization of PCAP and PCAPng files (sometimes called "trace files", "capture files" or "packet captures"), removing or replacing sensitive data while being easy to use.

### Features

- Sanitization/Anonymization/Scrubbing of packet captures created by Wireshark, TCPDump/etc.
- Editing of certain frame types, especially by removing certain protocol layers like MPLS, GRE or GTP-u, or to convert Linux cooked captures to Pseudo-Ethernet
- Merging capture files, especially PCAPng files with more than one interface and using filters to keep only certain frames
- Gathering details about a large number of capture files, like IP, TCP and UDP conversations
- Displaying the PCAPng specific block structure of a file
- extracting conversations from multiple files to new capture files, based on manual filters, capture file indicator frames, or Snort alerts

### Screenshot

No.	Filename	Size (Bytes)	Type	First Frame Time	Duration	Frames	Status
1	TraceWrangler_0001_20140709182802.pcapng	250,00 B	PCAPng	08:07:2014 18:28:02	00:00:25,00000000	401,671	No tool assigned
2	TraceWrangler_0002_20140709182827.pcapng	250,00 B	PCAPng	08:07:2014 18:28:28	00:00:07,221704000	276,128	No tool assigned
3	TraceWrangler_0003_20140709182834.pcapng	250,00 B	PCAPng	08:07:2014 18:28:35	00:00:41,300047000	262,267	No tool assigned
4	TraceWrangler_0004_20140709184013.pcapng	250,00 B	PCAPng	08:07:2014 18:40:15	00:07:23,00000000	391,851	No tool assigned



# SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE



## Demo



COMPUTER HISTORY MUSEUM



# SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE



Thanks! Questions?

eMail: [jasper@packet-foo.com](mailto:jasper@packet-foo.com)  
blog: <https://blog.packet-foo.com>  
Twitter: [@packetjay](https://twitter.com/packetjay)



COMPUTER HISTORY MUSEUM