

SHARKFEST 2015

WIRESHARK DEVELOPER AND USER CONFERENCE



TraceWrangling: Preparing Food for the Shark

Jasper Bongertz

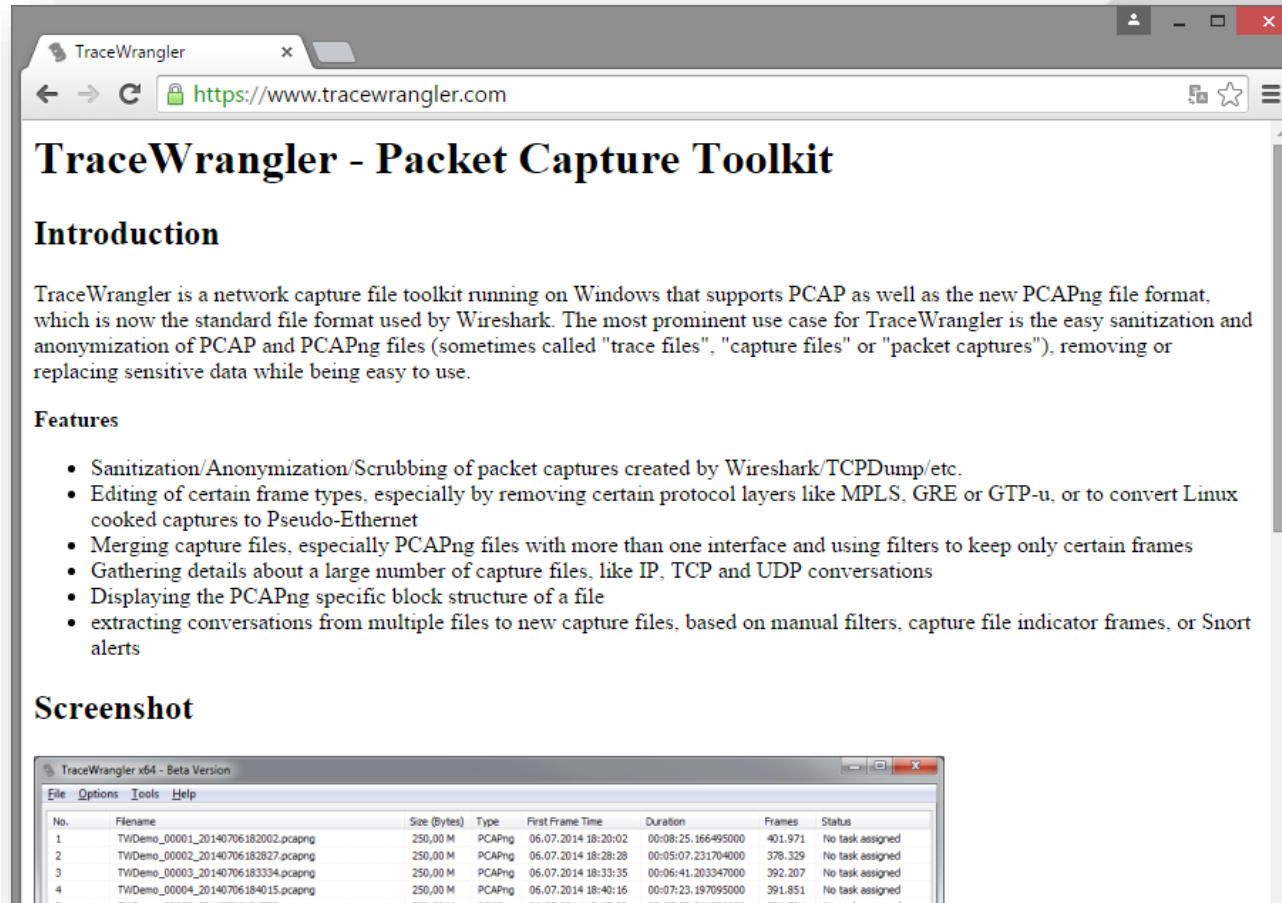
Airbus Defence and Space CyberSecurity

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, followed by a "Features" section with a bulleted list of capabilities. At the bottom, there is a "Screenshot" section showing a preview of the TraceWrangler application interface. The application window is titled "TraceWrangler x64 - Beta Version" and contains a table with columns for file number, filename, size, type, first frame time, duration, frames, and status.

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	TIWDemo_00001_20140706182002.pcapng	250,00 M	PCAPng	06.07.2014 18:20:02	00:08:25.166495000	401.971	No task assigned
2	TIWDemo_00002_20140706182827.pcapng	250,00 M	PCAPng	06.07.2014 18:28:28	00:05:07.231704000	378.329	No task assigned
3	TIWDemo_00003_20140706183334.pcapng	250,00 M	PCAPng	06.07.2014 18:33:35	00:06:41.203347000	392.207	No task assigned
4	TIWDemo_00004_20140706184015.pcapng	250,00 M	PCAPng	06.07.2014 18:40:16	00:07:23.197095000	391.851	No task assigned
5	TIWDemo_00005_20140706184738.pcapng	250,00 M	PCAPng	06.07.2014 18:47:39	00:02:20.311826000	204.704	No task 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
blog: <https://blog.packet-foo.com>
Twitter: [@packetjay](https://twitter.com/packetjay)



COMPUTER HISTORY MUSEUM