SharkFest '17 Europe

Practical TraceWrangling

Exploring Capture File Manipulation / Extraction Scenarios

Jasper Bongertz

PACKET-FOO

08 November 2017

About me?

- Working for Airbus
- Wireshark community
  - Blog: blog.packet-foo.com
  - Twitter: @packetjay
  - Q&A: https://ask.wireshark.org
  - Sharkfest (obviously)
- Creator of TraceWrangler
  - https://www.tracewrangler.com

Agenda

1. Tracewrangler?!
2. File and Task Concepts
3. Extracting packets
4. Demos/Scenarios
5. Roadmap

TraceWrangler

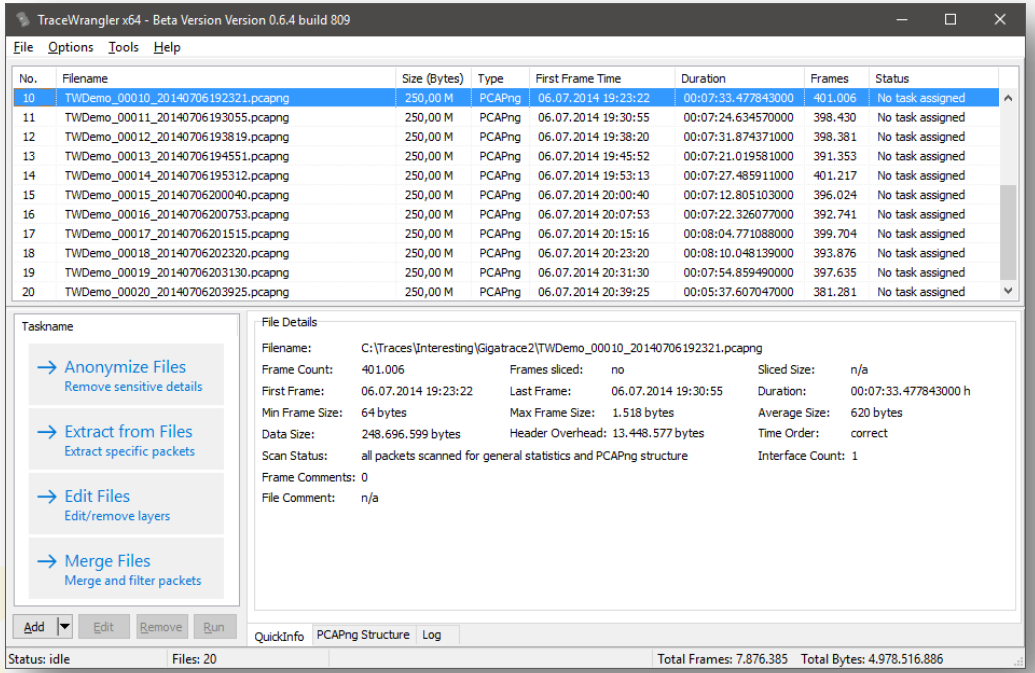
- Trace („pcap“) file manipulation toolkit
- Decodes protocol layers and performs tasks like
  - Sanitization / Anonymization
  - Layer removal/manipulation
  - Packet/Flow extractions
  - Merging
- Runs on Windows (and Linux via WINE)
  - That‘s because it‘s written in Delphi VCL, not C
- Open Source

Wireshark & TraceWrangler

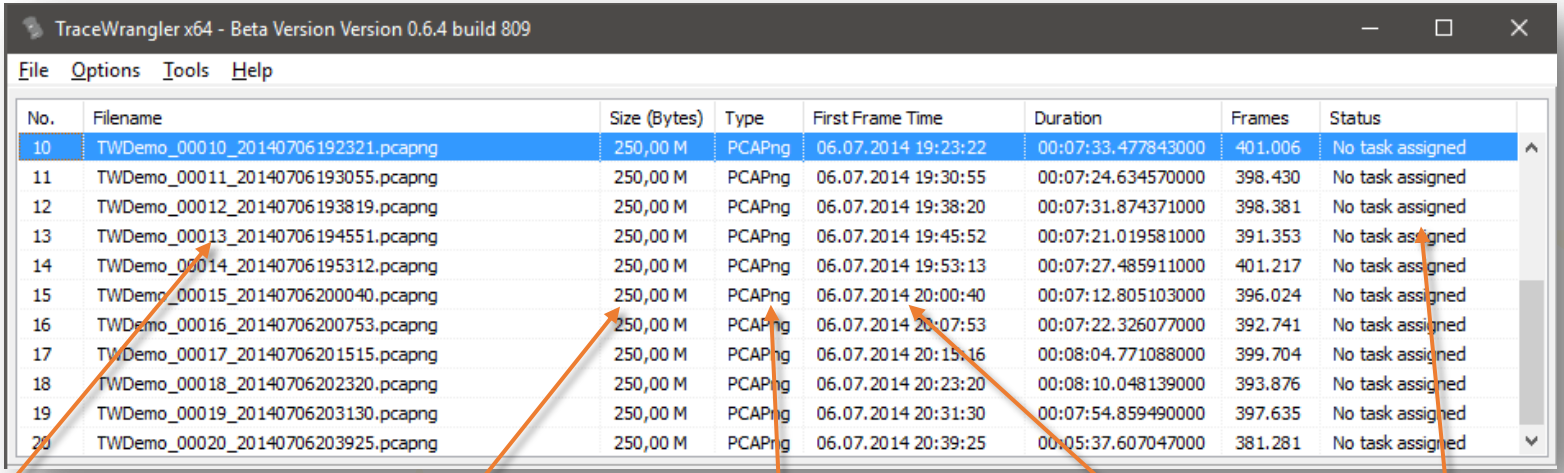
Wireshark	TraceWrangler
Has a Gazillion of protocol dissectors	34 protocols parsed as of Sharkfest 2017
Displays decoded protocols	Doesn‘t show protocol decodes
One file displayed/opened at a time	Filelist can hold hundreds or thousands of files
Supports powerful filters for everything	Only very basic filtering (Addresses, Ports)
Conversation statistics for the current file	Conversation statistics for all files combined
No/very manual packet manipulation features	Fully automatic packet manipulation

File and Task Concepts

- List of files, to be processed by tasks
- List of tasks, containing parameters for file processing
- File details pane
  - Shows file scan results, if available



File List



File names, without path, sorted by timestamp of first frame in file

File size, in byte, Kbyte, Mbyte or GByte

File format, detected by File Magic

Absolute time of the first frame in the file

Current Task Status

Adding files

- Use the „Add Files“ button to add single or multiple files via file dialog
- „Add directory“ to add all capture files found in a directory (plus subdirectories by default)
- Drag & drop
- Via command line parameter (just specify the filename with path)
- Via pop-up menu

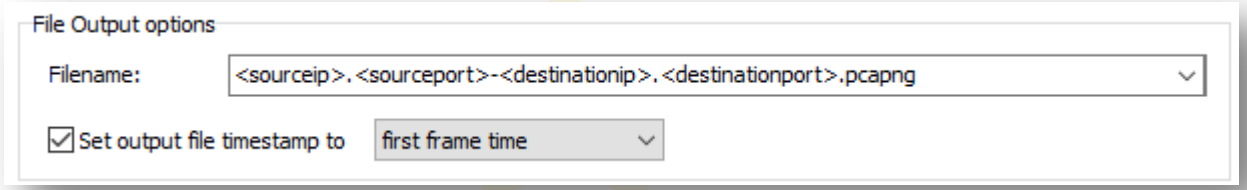
TraceWrangler Tasks: Extraction

Task Overview: Extracting Packets

- The goal is to extract packets of interest from a large number of packets
  - This usually requires an idea what you want to have extracted
- Most common use case: carving full TCP conversations from big files
  - Especially for situations where you have one packet and need the rest of the same flow

Extracting packets – How it works

- TraceWrangler uses its file meta database to
  - speed up the extraction process: positions of first and last packet to carve are well known
  - help the user looking up interesting flows
- Extracted packets can be written to a single file, or to multiple files based on a file name pattern:



Demo: Extracting Packets

Demo: Tools

Roadmap

Tracewrangler - Roadmap

- Anonymization:
  - Adjusting timestamps
  - Adding more protocols, especially DNS assembly
- File loading
  - Rewriting loader class to allow files > 2GB
  - Add support for loading .ERF files
- General:
  - Implementing TCP reassembly
  - Create a CLI version

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