



SharkFest '17 Europe

Practical TraceWrangling

Exploring Capture File
Manipulation / Extraction
Scenarios

08 November 2017

Jasper Bongertz

PACKET-FOO



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

No.	Filename	Size (Bytes)	Type	First Frame Time	Duration	Frames	Status
10	TWDemo_00010_20140706192321.pcapng	250,00 M	PCAPng	06.07.2014 19:23:22	00:07:33.477843000	401.006	No task assigned
11	TWDemo_00011_20140706193055.pcapng	250,00 M	PCAPng	06.07.2014 19:30:55	00:07:24.634570000	398.430	No task assigned
12	TWDemo_00012_20140706193819.pcapng	250,00 M	PCAPng	06.07.2014 19:38:20	00:07:31.874371000	398.381	No task assigned
13	TWDemo_00013_20140706194551.pcapng	250,00 M	PCAPng	06.07.2014 19:45:52	00:07:21.019581000	391.353	No task assigned
14	TWDemo_00014_20140706195312.pcapng	250,00 M	PCAPng	06.07.2014 19:53:13	00:07:27.485911000	401.217	No task assigned
15	TWDemo_00015_20140706200040.pcapng	250,00 M	PCAPng	06.07.2014 20:00:40	00:07:12.805103000	396.024	No task assigned
16	TWDemo_00016_20140706200753.pcapng	250,00 M	PCAPng	06.07.2014 20:07:53	00:07:22.326077000	392.741	No task assigned
17	TWDemo_00017_20140706201515.pcapng	250,00 M	PCAPng	06.07.2014 20:15:16	00:08:04.771088000	399.704	No task assigned
18	TWDemo_00018_20140706202320.pcapng	250,00 M	PCAPng	06.07.2014 20:23:20	00:08:10.048139000	393.876	No task assigned
19	TWDemo_00019_20140706203130.pcapng	250,00 M	PCAPng	06.07.2014 20:31:30	00:07:54.859490000	397.635	No task assigned
20	TWDemo_00020_20140706203925.pcapng	250,00 M	PCAPng	06.07.2014 20:39:25	00:05:37.607470000	381.281	No task assigned

File Details				
Filename:	C:\Traces\Interesting\Gigatrace2\TWDemo_00010_20140706192321.pcapng			
Frame Count:	401.006	Frames sliced:	no	
First Frame:	06.07.2014 19:23:22	Last Frame:	06.07.2014 19:30:55	
Min Frame Size:	64 bytes	Max Frame Size:	1.518 bytes	
Data Size:	248.696.599 bytes	Header Overhead:	13.448.577 bytes	
Scan Status:	all packets scanned for general statistics and PCAPng structure		Time Order:	correct
Frame Comments:	0		Interface Count:	1
File Comment:	n/a			

Status: idle Files: 20 Total Frames: 7.876.385 Total Bytes: 4.978.516.886



File List

TraceWrangler x64 - Beta Version Version 0.6.4 build 809

File Options Tools Help

No.	Filename	Size (Bytes)	Type	First Frame Time	Duration	Frames	Status
10	TWDemo_00010_20140706192321.pcapng	250,00 M	PCAPng	06.07.2014 19:23:22	00:07:33.477843000	401.006	No task assigned
11	TWDemo_00011_20140706193055.pcapng	250,00 M	PCAPng	06.07.2014 19:30:55	00:07:24.634570000	398.430	No task assigned
12	TWDemo_00012_20140706193819.pcapng	250,00 M	PCAPng	06.07.2014 19:38:20	00:07:31.874371000	398.381	No task assigned
13	TWDemo_00013_20140706194551.pcapng	250,00 M	PCAPng	06.07.2014 19:45:52	00:07:21.019581000	391.353	No task assigned
14	TWDemo_00014_20140706195312.pcapng	250,00 M	PCAPng	06.07.2014 19:53:13	00:07:27.485911000	401.217	No task assigned
15	TWDemo_00015_20140706200040.pcapng	250,00 M	PCAPng	06.07.2014 20:00:40	00:07:12.805103000	396.024	No task assigned
16	TWDemo_00016_20140706200753.pcapng	250,00 M	PCAPng	06.07.2014 20:07:53	00:07:22.326077000	392.741	No task assigned
17	TWDemo_00017_20140706201515.pcapng	250,00 M	PCAPng	06.07.2014 20:15:16	00:08:04.771088000	399.704	No task assigned
18	TWDemo_00018_20140706202320.pcapng	250,00 M	PCAPng	06.07.2014 20:23:20	00:08:10.048139000	393.876	No task assigned
19	TWDemo_00019_20140706203130.pcapng	250,00 M	PCAPng	06.07.2014 20:31:30	00:07:54.859490000	397.635	No task assigned
20	TWDemo_00020_20140706203925.pcapng	250,00 M	PCAPng	06.07.2014 20:39:25	00:05:37.607047000	381.281	No task assigned

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:

File Output options

Filename:

Set output file timestamp to



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





Q&A

Mail: jasper@packet-foo.com

Web: blog.packet-foo.com

Twitter: [@packetjay](https://twitter.com/packetjay)