SharkFest '17 US

Practical Tracewangling

Tuesday, 20th of June 2017

Jasper Bongertz
Security Analyst | Airbus Defence and Space CyberSecurity

Agenda

1. Tracewrangler?!
2. File and Task Concepts
3. Editing PCAP(ng)s
4. Extracting packets
5. Demos/Scenarios
6. 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 and 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 scanned files
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

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

Taskname

- Anonymize Files — Remove sensitive details
- Extract from Files — Extract specific packets
- Edit Files — Edit/remove layers
- Merge Files — Merge and filter packets

Add Edit Remove Run

File Details

Filename: C:\Traces\Interesting\Gigatrace2\TWDemo_00010_20140706192321.pcapng
Frame Count: 401.006 | Frames sliced: no | Sliced Size: n/a
First Frame: 06.07.2014 19:23:22 | Last Frame: 06.07.2014 19:30:55 | Duration: 00:07:33.477843000 h
Min Frame Size: 64 bytes | Max Frame Size: 1.518 bytes | Average Size: 620 bytes
Data Size: 248.696.599 bytes | Header Overhead: 13.448.577 bytes | Time Order: correct
Scan Status: all packets scanned for general statistics and PCAPng structure | Interface Count: 1
Frame Comments: 0
File Comment: n/a

QuickInfo | PCAPng Structure | Log

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

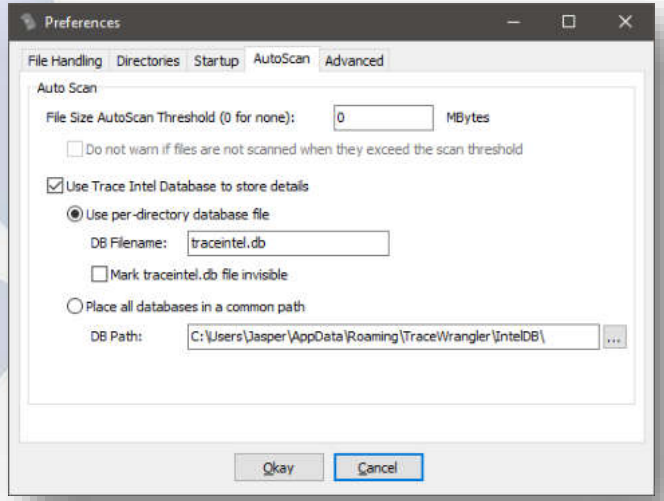
Current Task Status

Step 1 - 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

The file scan process

- By default, Tracewrangler scans all files up to 50MB <u>once</u>
  - Main purpose is to extract meta data about conversations and other details
  - Results are written to a database file
- Scan threshold can be configured in preferences
  - A setting of „0“ scans all files, regardless of size
  - Database name and location can be configured
  - Per default it‘s put into the same path as the files scanned



The meta data SQLite database

HTTP Samples

File Home Share View

This PC › Boot (C:) › Traces › Demo › Sharkfest 2017 › TraceWrangler › HTTP Samples

Quick access
Desktop
Downloads
Documents
Pictures

Name	Date modified	Type	Size
HTTP Sample.pcapng	29.06.2014 02:21	Wireshark capture...	10 KB
HTTP Sample2.pcapng	21.03.2014 11:36	Wireshark capture...	10 KB
HTTP Sample3.pcapng	23.08.2014 11:37	Wireshark capture...	18 KB
traceintel.db	19.06.2017 22:00	Data Base File	184 KB

SQLite Manager - C:\Traces\Demo\Sharkfest 2017\TraceWrangler\HTTP Samples\traceintel.db

Database Table Index View Trigger Tools Help

Directory › (Select Profile Database) Go

traceintel.db

Structure Browse & Search Execute SQL DB Settings

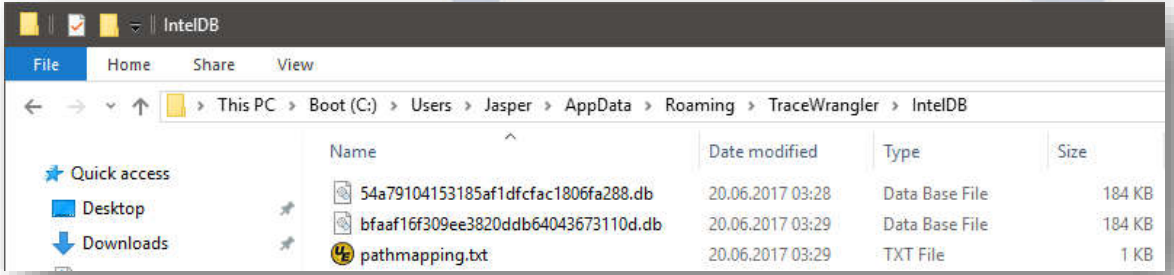
Master Table (1)
Tables (21)
AddressBook
IPv4Conversations
IPv4Endpoints

TABLE filelist Search Show All Add Duplicate Edit

id	filename	filepath	filesize	filedate	fullfilescann...	pcapngstruc...	conversatio...	processingst...	tasksprocess...	firstframeti...	firstframena...	lastframeti...	lastframena...
1	http sample2...	c:\traces\de...	9604	2014-03-21 1...	1	1	0	1	0	2014-03-21 1...	14283000	2014-03-21 1...	457179000
2	http sample....	c:\traces\de...	9748	2014-06-29 0...	1	1	0	1	0	2014-03-22 1...	531491000	2014-03-22 1...	596730000
3	http sample...	c:\traces\de...	1378	2015-07-19 0...	1	0	0	1	0	2014-03-22 1...	531509432	1899-12-30	0

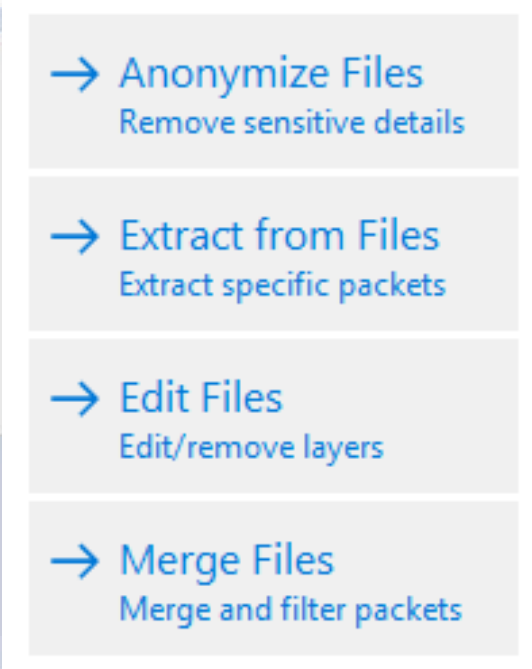
Local vs. central meta database

- Local database
  - Lives in the same directory as the capture files
  - can „travel“: just copy the .db file together with the capture files
- Central database path
  - Still one database per path, but all in a central directory
  - Mostly used for slow or write protected capture file storage devices



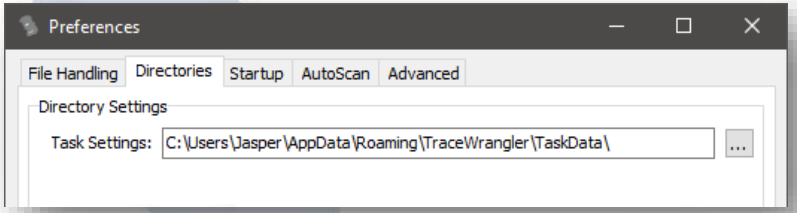
Step 2 - Doing something with files

- Add a task to tell Tracewrangler what it should do:
  - Sanitize/Anonymize
  - Extract
  - Edit
  - Merge
- Or use the tools:
  - Conversation summary
  - Renaming files
  - Updating file timestamps

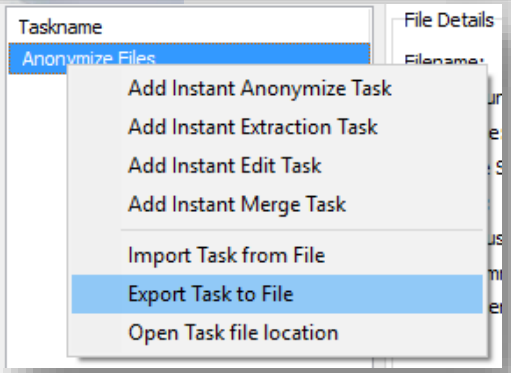


Task Hints

- Task settings are stored in SQLite files
- Per default they are put in a sub path of the user folder, which you can reconfigure:



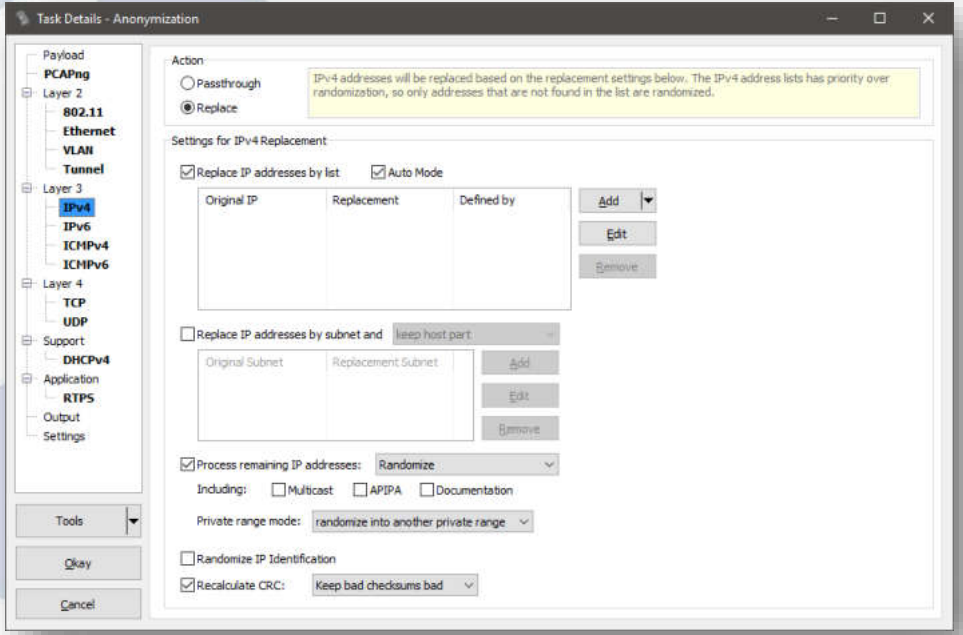
- To keep tasks:
  - export and import them from the task list
  - Copy the task file to a safe place from the settings path



Tracewrangler Tasks: Anonymization

Task Overview: Anonymize/Sanitize

- Removes/changes sensitive details from a capture file
  - MAC Addresses, IP addresses, application payload and other things
- Comes with a preset that should be fine in most situations
  - Can be overriden with a modified preset
  - The „factory default“ can always be restored

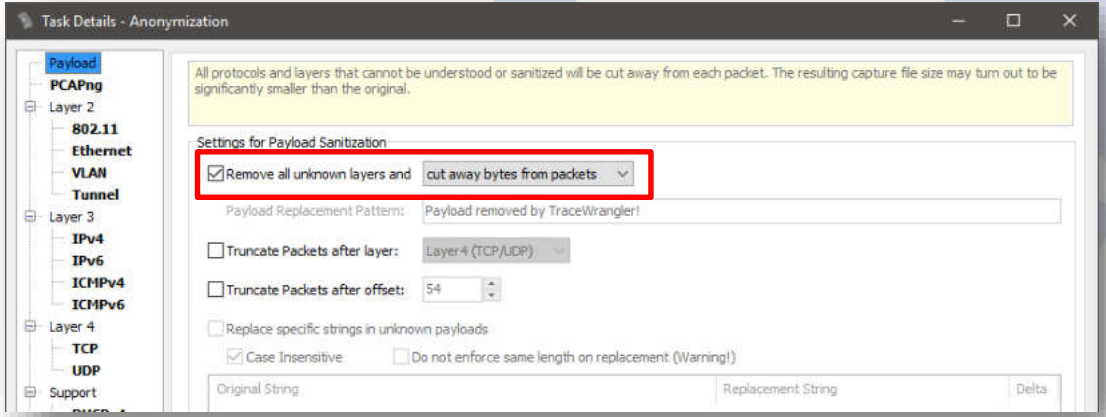


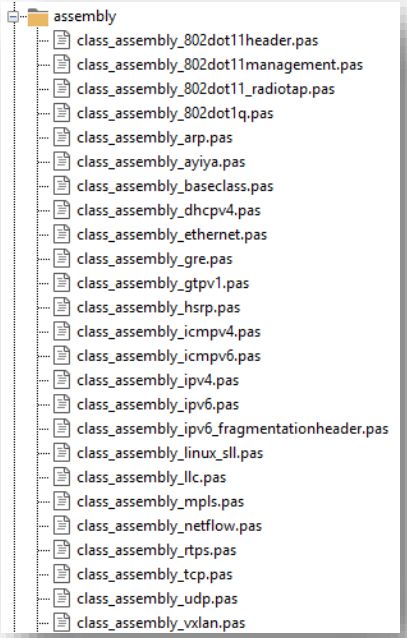
Sanitization - How it works

- Sanitization is a four step process:
  1. Parse the packet bottom-up (e.g. Ethernet - IPv4 - TCP - Unknown)
  2. Extract all values (addresses, ports, flags, ...)
  3. Change/remove all sensitive details of parsed values
  4. Build new packet top-down (e.g. TCP - IPv4 - Ethernet)
- Everything that isn't understood by Tracewrangler will **not** make it into the newly constructed packet!

Sanitization - Handling „unknown“ Protocols

- Tracewrangler can sanitize 24 protocols as of Sharkfest 2017
- All others are considered unknown payload, and cut away by default!



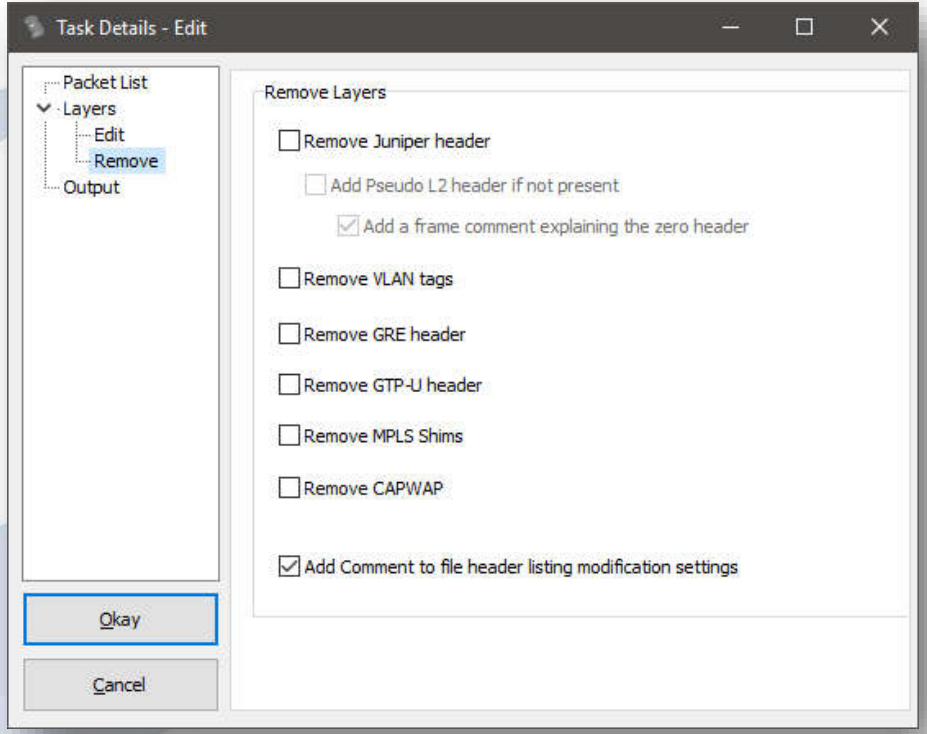


Demo: Anonymization

Tracewrangler Tasks: Editing

Task Overview: Editing Packets

- Mostly used to
  - remove unwanted packet layers
  - de-encapsulate protocols
  - convert link layer types
  - fix badly sliced packets
- Some features are also available via Wireshark CLI tools, e.g. reordercap and editcap



Editing - How it works

- Editing packets (removing/converting protocol layers) is not just „cut away x bytes at static offset y“
  - Protocol layers are parsed, determining protocol start and end offsets
  - When removing layers, „Next Protocol“ fields are adjusted to mend the remaining layers, e.g. Ethertypes:

```
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
v Ethernet II, Src: ca:03:0d:b4:00:1c (ca:03:0d:b4:00:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: ca:03:0d:b4:00:1c (ca:03:0d:b4:00:1c)
    Type: 802.1Q Virtual LAN (0x8100)
v 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 100
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0110 0100 = ID: 100
    Type: 802.1Q Virtual LAN (0x8100)
v 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 200
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 1100 1000 = ID: 200
    Type: ARP (0x0806)
    Padding: 00000000000000000000
    Trailer: 00000000
> Address Resolution Protocol (request)
```

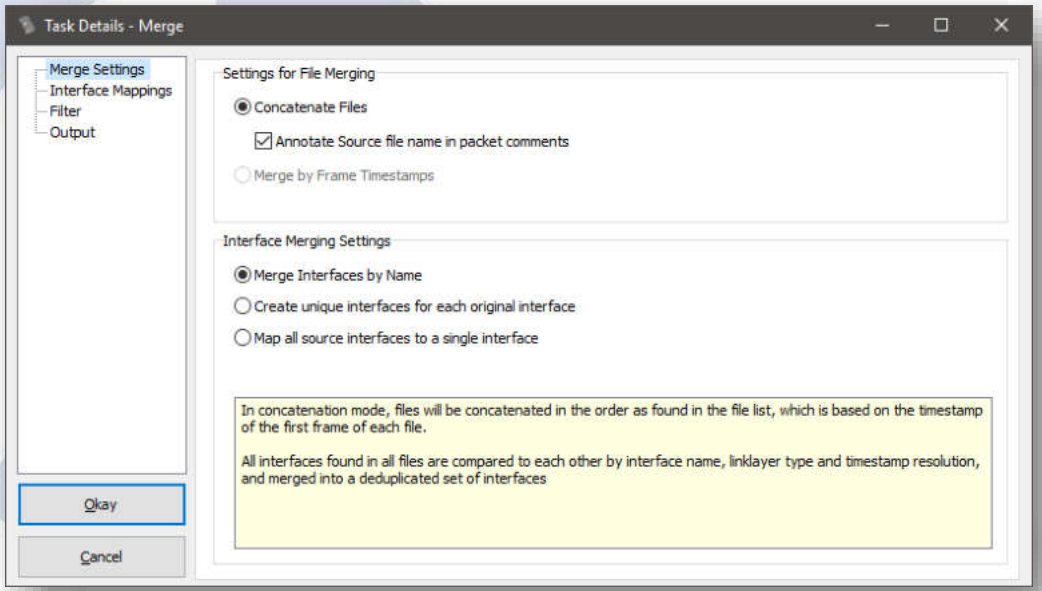
```
> Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
v Ethernet II, Src: ca:03:0d:b4:00:1c (ca:03:0d:b4:00:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: ca:03:0d:b4:00:1c (ca:03:0d:b4:00:1c)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000
> Address Resolution Protocol (request)
```

Demo: Editing packets

Tracewrangler Tasks: Merging

Task Overview: Merging Packets

- Merging packets was added to allow merging capture files with finer control than mergecap
  - especially for capture files containing more than one interface
  - Interfaces can be merged, kept unique or mapped to a single new interface



Merging - Interface mapping

- Interface mapping allows defining what interface in the original file is mapped to
- Automatic mapping works best for Windows captures because of using GUIDs for NICs

Task Details - Merge

Merge Settings
Interface Mappings
Filter
Output

Files and Original Interface	Mapped Interface
MergeSample_00000_20130108011821.pcapng	
\Device\NPF_{67A4C75E-DB4D-4F21-A4AD-0C5740EAD804}	\Device\NPF_{67A4C75E-DB4D-4F21-A4AD-0C5740EAD804}
\Device\NPF_{0142A679-539B-40D9-BBF3-345BBFDAD0F7}	\Device\NPF_{0142A679-539B-40D9-BBF3-345BBFDAD0F7}
MergeSample_00001_20130108011845.pcapng	
\Device\NPF_{67A4C75E-DB4D-4F21-A4AD-0C5740EAD804}	\Device\NPF_{67A4C75E-DB4D-4F21-A4AD-0C5740EAD804}
\Device\NPF_{0142A679-539B-40D9-BBF3-345BBFDAD0F7}	\Device\NPF_{0142A679-539B-40D9-BBF3-345BBFDAD0F7}
MergeSample_00002_20130108011855.pcapng	
\Device\NPF_{67A4C75E-DB4D-4F21-A4AD-0C5740EAD804}	\Device\NPF_{67A4C75E-DB4D-4F21-A4AD-0C5740EAD804}
\Device\NPF_{0142A679-539B-40D9-BBF3-345BBFDAD0F7}	\Device\NPF_{0142A679-539B-40D9-BBF3-345BBFDAD0F7}

Mapping Details

Index	Interface Name	Description	Link Type	Origin
1	\Device\NPF_{67A4C75...	<no description available>	ETHERNET	From File
2	\Device\NPF_{0142A67...	<no description available>	ETHERNET	From File

Okay

Cancel

Demo: Merging packets

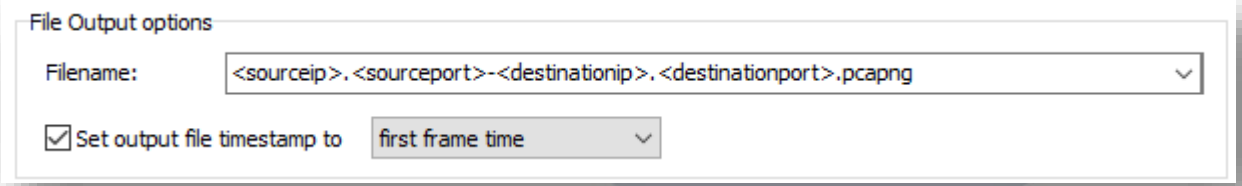
Tracewrangler Tasks: Extraction

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 the 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
- File loading
  - Rewriting loader class to allow files > 2GB
  - Add support for loading .ERF files
- General:
  - Implementing TCP reassembly
  - Improving processing speed

Q&A

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