Practical TraceWrangling

Exploring Capture file manipulation/extraction scenarios

Jasper Bongertz

Airbus CyberSecurity

About me

- Working at Airbus CyberSecurity
- Network analysis & forensics since 2003
  - NetXRay, Sniffer Pro/Distributed, Clearsight
  - Ethereal since… uh… version 0.9something
- Creator of
  - TraceWrangler
  - blog.packet-foo.com

Agenda

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

TraceWrangler

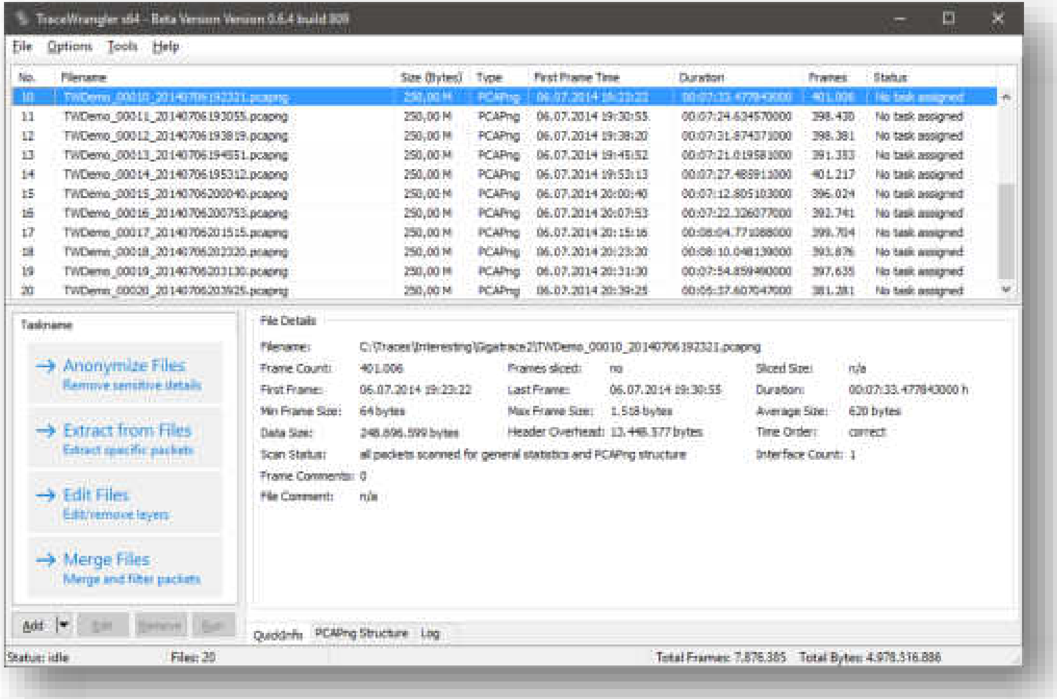
- Trace („pcap“) file manipulation toolkit
- Decodes protocol layers and performs tasks like
  - Sanitization / Anonymization
  - Layer removal/manipulation
  - Packet/Flow extractions
  - Merging

Wireshark /TraceWrangler

Wireshark	Tracewrangler
Has a Gazillion of protocol dissectors	34 protocols parsed as of Sharkfest 2018
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

The file list

- 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	00:06:37.607047000	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

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: 13.446.577 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

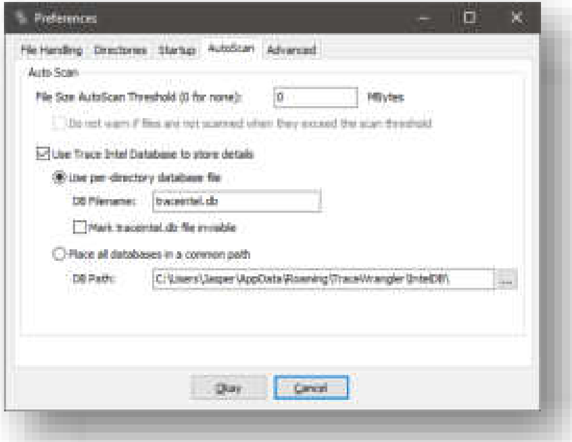
Status: idle Files: 20 Total Frames: 7.876.385 Total Bytes: 4.978.316.886

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

PCAP indexing

- 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



Auto Scan

File Size AutoScan Threshold (0 for none): 0 MBytes

□ Do not warn if files are not scanned when they exceed the scan threshold

☑ Use Trace Intel Database to store details

● Use per-directory database file

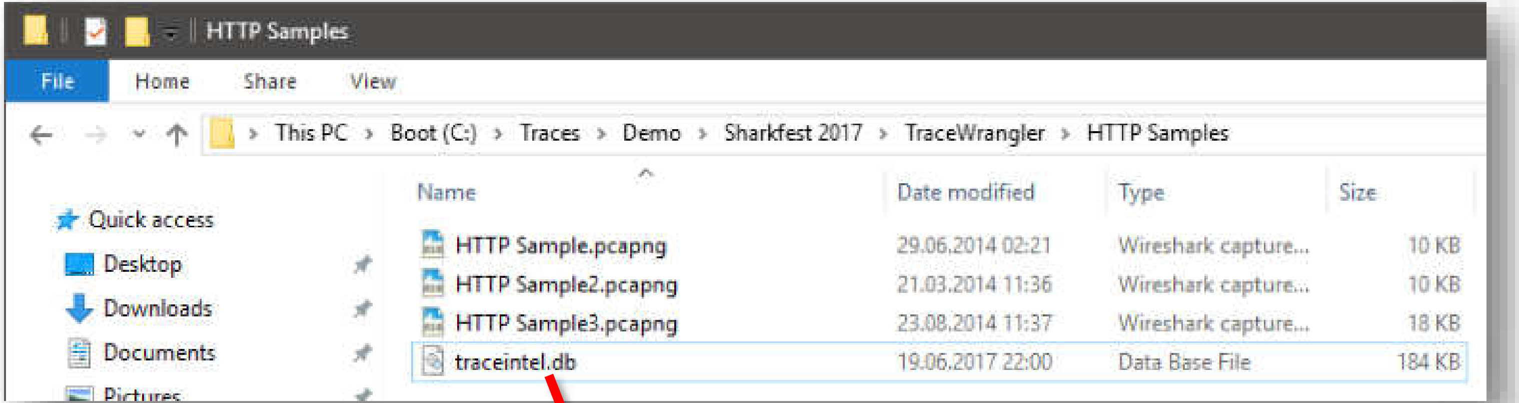
DB Filename: traceintel.db

□ Mark traceintel.db file invisible

○ Place all databases in a common path

DB Path: C:\Users\Jasper\AppData\Roaming\TraceWrangler\IntelDB\

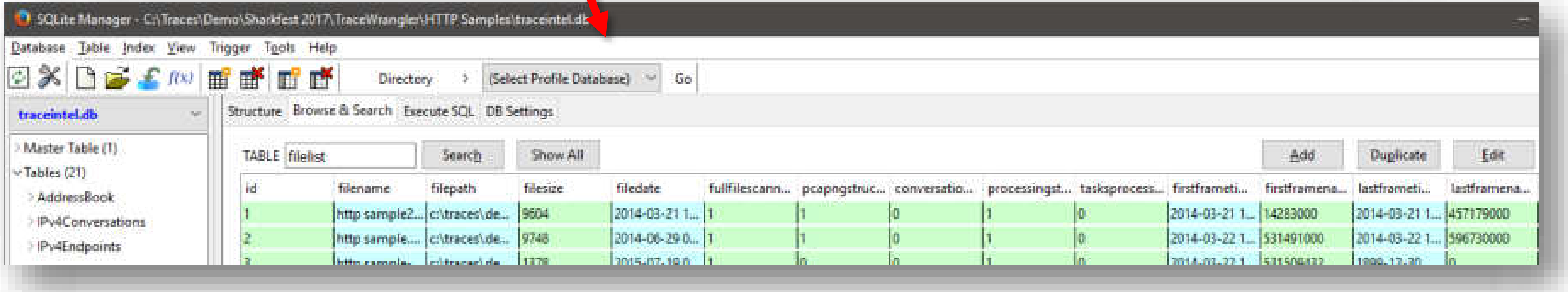
The meta data SQLite database



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



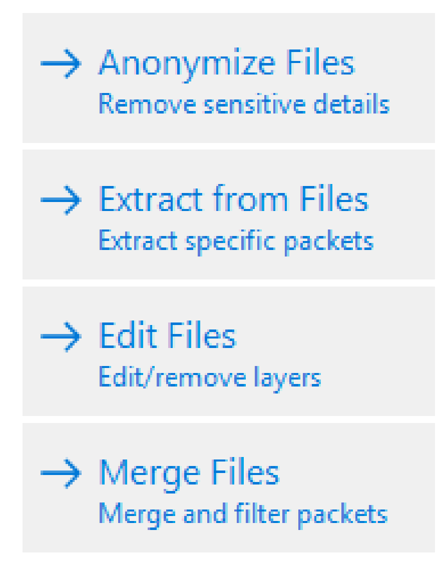
SQLite Manager - C:\Traces\Demo\Sharkfest 2017\TraceWrangler\HTTP Samples\traceintel.db

TABLE filelist

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...	1178	2015-07-19 0...	1	0	0	1	0	2014-03-22 1...	531509433	1899-12-30	0

Add Tasks

- 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



→ Anonymize Files
Remove sensitive details

→ Extract from Files
Extract specific packets

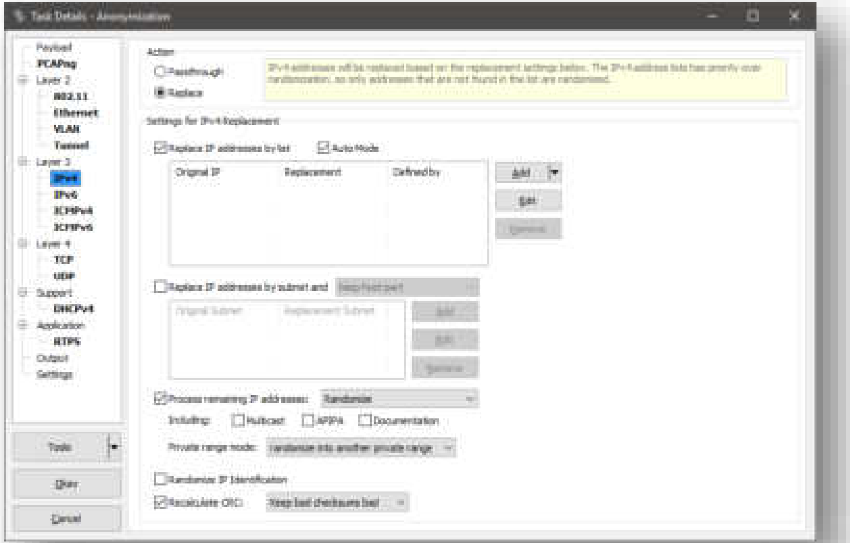
→ Edit Files
Edit/remove layers

→ Merge Files
Merge and filter packets

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 default preset that should be fine in most situations
  - Can be overriden with a modified default
  - The „factory default" can always be restored


Task Details - Anonymization

Action
○ Passthrough
● Replace

IPv4 addresses will be replaced based on the replacement settings below. The IPv4 address lists has priority over randomization, so only addresses that are not found in the list are randomized.

Settings for IPv4 Replacement

☑ Replace IP addresses by list ☑ Auto Mode

Original IP	Replacement	Defined by

☐ Replace IP addresses by subnet and: keep host part

Original Subnet	Replacement Subnet

☑ Process remaining IP addresses: Randomize
Including: ☐ Multicast ☐ APIPA ☐ Documentation
Private range mode: randomize into another private range

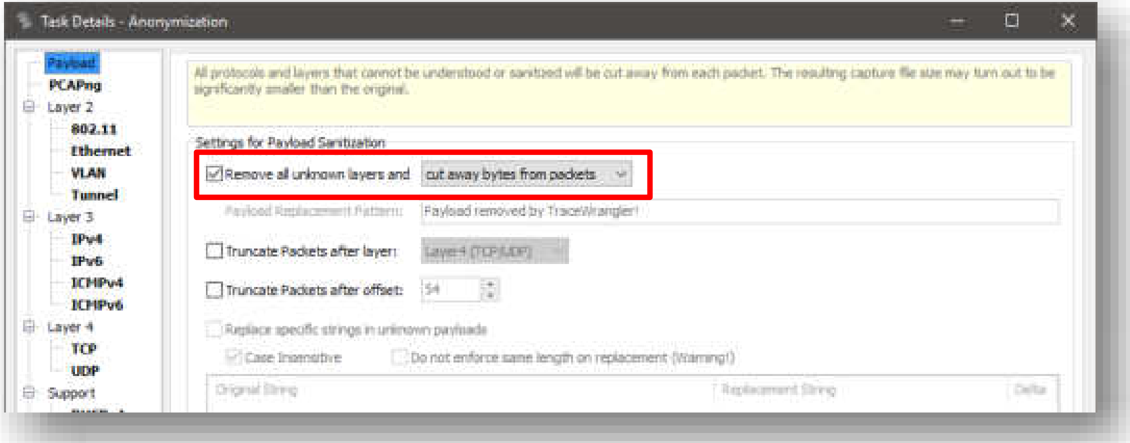
☐ Randomize IP Identification
☑ Recalculate CRC: Keep bad checksums bad

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 2018
- All others are considered unknown payload, and cut away by default!



Task Details - Anonymization

All protocols and layers that cannot be understood or sanitized will be cut away from each packet. The resulting capture file size may turn out to be significantly smaller than the original.

Settings for Payload Sanitization

☑ Remove all unknown layers and: cut away bytes from packets

Payload Replacement Pattern: Payload removed by TraceWrangler!

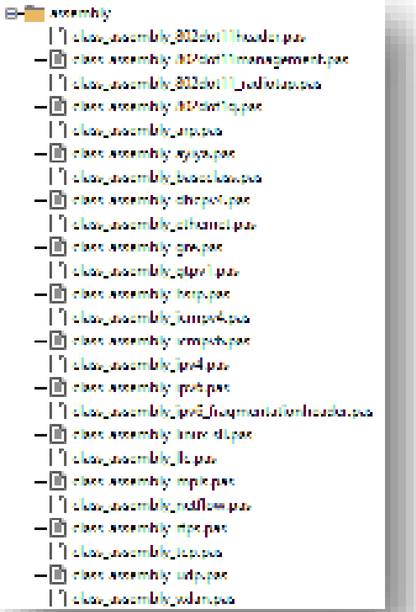
☐ Truncate Packets after layer: Layer4 (TCP/UDP)

☐ Truncate Packets after offset: 54

☐ Replace specific strings in unknown payloads

☑ Case Insensitive ☐ Do not enforce same length on replacement (Warning!)

Original String	Replacement String	Delta



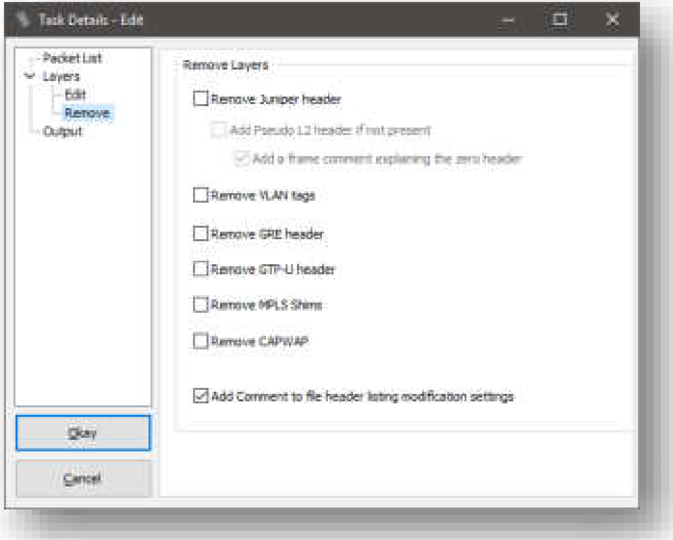
assembly
class_assembly_802dot11header.pas
class_assembly_802dot11management.pas
class_assembly_802dot11_radiotap.pas
class_assembly_802dot1q.pas
class_assembly_arp.pas
class_assembly_ayiya.pas
class_assembly_baseclass.pas
class_assembly_dhcpv4.pas
class_assembly_ethernet.pas
class_assembly_gre.pas
class_assembly_gtpv1.pas
class_assembly_hsrp.pas
class_assembly_icmpv4.pas
class_assembly_icmpv6.pas
class_assembly_ipv4.pas
class_assembly_ipv6.pas
class_assembly_ipv6_fragmentationheader.pas
class_assembly_linux_sll.pas
class_assembly_llc.pas
class_assembly_mpls.pas
class_assembly_netflow.pas
class_assembly_rtps.pas
class_assembly_tcp.pas
class_assembly_udp.pas
class_assembly_vlan.pas

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



Remove Layers

☐ Remove Juniper header

☐ Add Pseudo L2 header if not present

☑ Add a frame comment explaining the zero header

☐ Remove VLAN tags

☐ Remove GRE header

☐ Remove GTP-U header

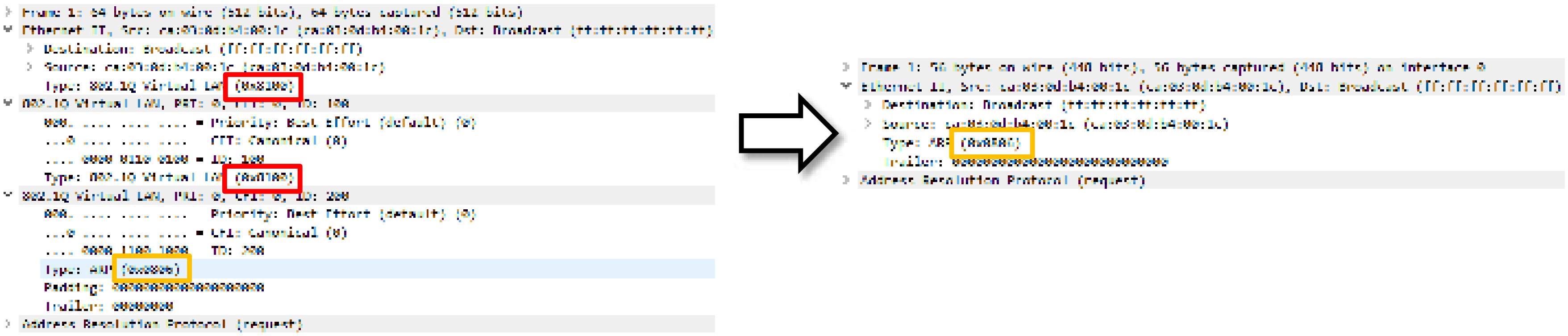
☐ Remove MPLS Shims

☐ Remove CAPWAP

☑ Add Comment to file header listing modification settings

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 correctly link 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: 0000000000000000000000000000
> Address Resolution Protocol (request)
```

Demo: Editing packets

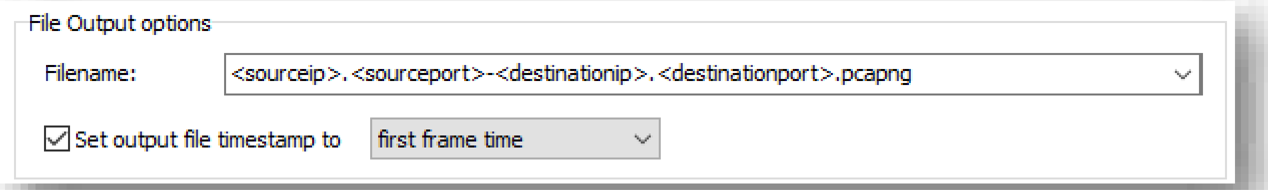
Tracewrangler Tasks: Extraction

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:



File Output options

Filename: <sourceip>.<sourceport>-<destinationip>.<destinationport>.pcapng

☑ Set output file timestamp to first frame time

Demo: Extracting Packets

Demo: Tools

Q&A

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