SharkFest '17 US

Practical Tracewangling

Tuesday, 20th of June 2017

Jasper Bongertz Security Analyst | Airbus Defence and Space CyberSecurity



- 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

No.	Filename				Size (Bytes)	Type	First Frame	Time	Duration		Frames	Status		
10	TWDemo 0	0010 20140	70619232	1.oceana	250.00 M	PCAPna	05.07.2014	10:23:22	00:07:33.4	77843000	401.005	No task ass	ianed.	
11	TWDemo D	0011 20140	70619305	5.pcaprig	250.00 M	PCAPng	06.07.2014	19:30:55	00:07:24.6	34570000	398,430	No task ass	ioned	
12	TWDemo 0	0012 20140	706 1938 1	9.pcapng	250,00 M	PCAPng	06.07.2014	19:38:20	00:07:31.8	74371000	398.381	No task ass	igned	
13	TWDemo_0	0013_20140	70619455	1.pcapng	250,00 M	PCAPng	06.07.2014	19:45:52	00:07:21.0	19581000	391.353	No task ass	igned	
14	TWDemo 0	0014 20140	70619531	2.pcapng	250,00 M	PCAPng	06.07.2014	19:53:13	00:07:27.4	85911000	401.217	No task ass	igned	
15	TWDemo_0	0015_20140	70520004	0.pcapng	250,00 M	PCAPng	06.07.2014	1 20:00:40	00:07:12.8	05103000	396.024	No task ass	igned	
16	TWDemo D	0016 20140	70620075	3.pcapng	250,00 M	PCAPng	06.07.2014	20:07:53	00:07:22.3	26077000	392,741	No task ass	agned	
17	TWDemo_D	0017_20140	70620151	5.pcaping	250,00 M	PCAPng	06.07.2014	20:15:16	00:08:04.1	71088000	399.704	No task ass	igned	
18	TWDemo_0	0018_20140	70520232	0.pcapng	250,00 M	PCAPng	06.07.2014	1 20:23:20	00:08:10.0	48139000	393.876	No task ass	igned	
19	TWDemo_0	0019_20140	70620313	0.pcaping	250,00 M	PCAPng	06.07.2014	20:31:30	00:07:54.8	59490000	397.635	No task ass	igned	
20	TWDemo_0	0020_20140	70620392	5.pcapng	250,00 M	PCAPng	06.07.2014	1 20:39:25	00:05:37.6	07047000	381.281	No task ass	igned	
de de de	 Extract f Extract spe Edit File: Edit/remov Merge F Merge and 	rom Files cific packet s ve layers iles (filter packe	i s	nin rrame size: Data Size: Scan Status: Frame Comments File Comment:	248.696.599 bytes all packets scanned f c 0 n/a	Ma Hei	x rrame size: ader Overhea statistics and	1.518 6yt d: 13.448.57 PCAPng stru	es 77 bytes cture	Average Time Oro Interfac	er: 60 er: co e Count: 1	arrect		
Add atus:	→ Edit	Bemove File	Run s: 20	QuickInfo PCAPn	g Structure Log			1	otal Frames:	7.876.385	Total Bytes	: 4.978.516.88	6	



File List

S TraceWran	gler x64 - Beta Version Version 0.6.4 build 809 Tools Help						- 0	×
No. Filenar	ie	Size (Bytes)	Туре	First Frame Time	Duration	Frames	Status	
10 TWDer	no_00010_20140706192321.pcapng	250,00 M	PCAPng	06.07.2014 19:23:22	00:07:33.477843000	401.006	No task assigned	^
11 TWDer	no_00011_20140706193055.pcapng	250,00 M	PCAPng	06.07.2014 19:30:55	00:07:24.634570000	398.430	No task assigned	
12 TWDer	no_00012_20140706193819.pcapng	250,00 M	PCAPng	06.07.2014 19:38:20	00:07:31.874371000	398.381	No task assigned	
13 TWDer	no_00013_20140706194551.pcapng	250,00 M	PCAPng	06.07.2014 19:45:52	00:07:21.019581000	391.353	No task assigned	
14 TWDer	no_00014_20140706195312.pcapng	250,00 M	PCAPng	06.07.2014 19:53:13	00:07:27.485911000	401.217	No task assigned	
15 TWDer	no_00015_20140706200040.pcapng	250,00 M	PCAPng	06.07.2014 20:00:40	00:07:12.805103000	396.024	No task assigned	
16 TWDer	no_00016_20140706200753.pcapng	250,00 M	PCAPng	06.07.2014 20:07:53	00:07:22.326077000	392.741	No task a signed	
17 TWDer	no_30017_20140706201515.pcapng	250,00 M	PCAPng	06.07.2014 20:15:16	00:08:04.771088000	399.704	No task assigned	
18 TWDe	6_00018_20140706202320.pcapng	250,00 M	PCAPng	06.07.2014 20:23:20	00:08:10.048139000	393.876	No task as igned	
19 TWDer	no_00019_20140706203130.pcapng	250,00 M	PCA ing	06.07.20142:31:30	00:07:54.859490000	397.635	No task astigned	
20 / WDer	no_00020_20140706203925.pcapng	250,00 M	PCAPng	06.07.2014 20:33 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 dete File	form ected Mag	nat, I by jic	Absolute time of the first frame	9	Current Task St	atus



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 once

- 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 "O" 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): Do not warn if files are not scanned when they exceed the scan threshold Use Trace Intel Database to store details O Use per-directory database file DB Filename: traceintel.db Mark traceintel.db file invisible	
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 OB Filename: traceintel.db Mark traceintel.db file invisible	
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	
Use per-directory database file DB Filename: traceintel.db file invisible	
Use Trace Intel Database to store details Use per-directory database file D8 Filename: traceintel.db Mark traceintel.db file invisible	
Use per-directory database file D8 Filename: traceintel.db Mark traceintel.db file invisible	
DB Filename: traceintel.db	
Mark traceintel.db file invisible	
O Place all databases in a common path	
	1000
DB Path: C: Users Uasper Appuata Koaming (Tracevvrangier UntelDB)	144



The meta data SQLite database

254	5 N 5577									_		
File Home S	hare Vie	W								- 8		
← → • ↑ 📘	> This PC >	Boot (C:) > Traces	> Demo > Sharkfe	est 2017 >	TraceWran	ngler > H	TTP Sample	s				
. O side and a		Name	~		Date modi	fied	Туре		Size			
		📑 HTTP Sample	e.pcapng		29.06.2014	02:21	Wireshark	capture	1	ОКВ		
Desktop	Я	🔚 HTTP Sample	2.pcapng		21.03.2014	11:36	Wireshark	capture	1	о кв		
Downloads	Ŕ	🔚 HTTP Sample	e3.pcapng		23.08.2014	11:37	Wireshark	capture	1	8 KB		
Documents	オ	🗟 traceintel.db			19.06.2017	22:00	Data Base	File	18	4 KB		
Pictures				_	100	_		_	_			
			1									
SCI ite Manager - C:\Traces\De	mo\Sharkfest 2017\	TraceWrangler\HTTP Samples\	traceintel.db			1						5
atabase <u>T</u> able Index ⊻iew Tr	igger T <u>o</u> ols Helr											
5 🛣 🕒 🚅 🦨 ฒ 🗖	i 💣 🖬 💣	Directory > (Sele	ct Profile Database) 🛛 🖌 Go									
드 🖉 이 🛄 💆 🧰 가~~ 표												
traceinteLdb	Structure Browse	& Search Execute SQL DB S	ettings									
traceinteLdb	Structure Browse	& Search Execute SQL DB S	Show All							Add	Duplicate	<u>E</u> dit
traceinteLdb	Structure Browse TABLE filelist id	& Search Execute SQL DB S Searc <u>h</u> filename filepath	Show All filesize filedate	fullfilescann	pcapngstruc	conversatio	processingst	tasksprocess	firstframeti	<u>A</u> dd firstframena	Du <u>p</u> licate lastframeti	<u>E</u> dit lastframena
traceinteLdb	Structure Browse TABLE filelist id 1	& Search Execute SQL DB S Search Search filename filepath http sample2 c:\traces\de	Show All filesize filedate 9604 2014-03-21 1	fullfilescann	pcapngstruc	conversatio	processingst	tasksprocess 0	firstframeti 2014-03-21 1	<u>A</u> dd firstframena 14283000	Duplicate Iastframeti 2014-03-21 1	<u>E</u> dit lastframena. 457179000



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

→ ~ ↑ <mark> </mark> • 1	This PC 🔹 🛛	Boot (C:) > Users > Jasper > AppData > Ro	aming > TraceWrang	gler → IntelDB	
		Name	Date modified	Туре	Size
Quick access		54a79104153185af1dfcfac1806fa288.db	20.06.2017 03:28	Data Base File	184 KB
Desktop	R	bfaaf16f309ee3820ddb64043673110d.db	20.06.2017 03:29	Data Base File	184 KB
Downloads	1	😗 pathmapping.txt	20.06.2017 03:29	TXT File	1 KB



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

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



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:
 Preference:
 If the transformed attacks and attacks and attacks atta

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



@packetjay

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

Payload	Action				
PCAPng E Layer 2 802.11	Passthrough Replace	IPv4 addresses will be reprandomization, so only ad	placed based on the rep idresses that are not fo	lacement settings below. The IPv4 address lists has priori und in the list are randomized.	ty over
Ethernet VLAN Tunnel	Settings for IPv4 Repla	scement ises by list 🛛 Auto Mode			
E Layer 3	Original IP	Replacement	Defined by	Add +	
IPv6 ICMPv4				Edit	
- ICMPv6				Bemove	
TCP					
⊖ Support	Replace IP addres	ses by subnet and keep hos	t part -		
DHCPv4	Original Subnet	Replacement Subnet	≜dd		
RTPS			≣dit		
Output Settings			Bannervez		
	Process remaining	IP addresses: Randomize	~		
Tools +	Private range mod	Multicast LAPIPA LC	ocumentation rivate range 🛛 🗸		
Qkay	Randomize IP Ide	ntification			



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!

🐧 Task Details - Ano	nymization			-	D X
Payload PCAPng E Layer 2	All protocols and layers that cannot be significantly smaller than the original.	e understood or sanitized will be cut away	from each packet. The resulting capture fil	e size may tun	n out to be
802.11 Ethernet	Settings for Payload Sanitization				
VLAN	Remove all unknown layers and	cut away bytes from packets $$			
Tunnei ∃- Layer 3	Payload Replacement Pattern:	Payload removed by TraceWrangler!			
IPv4 IPv6	Truncate Packets after layer:	Layer4 (TCP/JDP)			
ICMPv4	Truncate Packets after offset:	54			
E Layer 4	Replace specific strings in unkno	wn payloads Do not enforce same length on replacemen	it (Warning!)		
Support	Original String		Replacement String		Delta

assembly □ 🖹 class_assembly_802dot11header.pas - E class_assembly_802dot11management.pas - 🖹 class_assembly_802dot11_radiotap.pas --- 🖹 class assembly 802dot1g.pas --- 🖹 class_assembly_arp.pas lass assembly aviva.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_vxlan.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

Tush Detons - Eure		
Packet List Layers Edit Remove Output	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	
<u>O</u> kay		
Cancel		



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:





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

Verge Settings	Settings for File Merging
Filter	Concatenate Files
Dutput	Annotate Source file name in packet comments
	O Merge by Frame Timestamps
	Interface Merging Settings
	Merge Interfaces by Name
	O Create unique interfaces for each original interface
	○ Map all source interfaces to a single interface
	In concatenation mode, files will be concatenated in the order as found in the file list, which is based on the timestamp of the first frame of each file.
	All interfaces found in all files are compared to each other by interface name, linklayer type and timestamp resolution, and merged into a deduplicated set of interfaces
<u>O</u> kay	
Consel	



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						- 0
- Merge Settings Interface Mappings Filter Output	Files and	Original Interface yeSample_00000_201301080 Device WPF_{67A4C75E-DB4 Device WPF_{0142A679-5398 yeSample_00001_201301080 Device WPF_{0142A679-5398 yeSample_00002_201301080 Device WPF_{67A4C75E-DB4 Device WPF_{0142A679-5398 Device WPF_{0142A679-5398 Device WPF_{0142A679-5398 Details	11821.pcapng D-4F21-A4AD-0C5740EAD804} 3-40D9-88F3-3458BFDAD0F7} 11845.pcapng D-4F21-A4AD-0C5740EAD804} 3-40D9-88F3-3458BFDAD0F7} 11855.pcapng D-4F21-A4AD-0C5740EAD804} 3-40D9-88F3-3458BFDAD0F7}	Mapped Interface \Device\NPF_{67A4 \Device\NPF_{0142} \Device\NPF_{67A4 \Device\NPF_{0142} \Device\NPF_{67A4 \Device\NPF_{67A4} \Device\NPF_{0142}	C75E-DB4D-4F21 A679-539B-40D9 C75E-DB4D-4F21 A679-539B-40D9 C75E-DB4D-4F21 A679-539B-40D9	-A4AD-0C5740EAD804 -BBF3-3458BFDAD0F7 -A4AD-0C5740EAD804 -BBF3-3458BFDAD0F7 -A4AD-0C5740EAD804 -BBF3-3458BFDAD0F7
	Index 1	Interface Name	Description <no available="" description=""></no>	Link Type ETHERNET	Origin From File	
<u>Q</u> kay	2	\Device\NPF_{0142A67	<no available="" description=""></no>	ETHERNET	From File	
	5					



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:

File Output options	-			
Filename:	<sourceip>.</sourceip>	<sourceport>-<destination< th=""><th>ationip>.<destinationport>.pcapng</destinationport></th><th>~</th></destination<></sourceport>	ationip>. <destinationport>.pcapng</destinationport>	~
Set output file	timestamp to	first frame time	~	
				_



Demo: Extracting Packets







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: jaspe Web: blog. Twitter: @pa

jasper@packet-foo.com blog.packet-foo.com @packetjay