interView
Network Solutions

Quick Start Guide
Sharkmon Trial

“Monitor your pcap Data”

1. Overview

Sharkmon trial is a version of sharkmon with limited functionality

It provides the following features

1. Definition of wireshark-based Metrics
2. Creating a profile with defined metrics
3. Setting thresholds for each metric for critical / warning symptoms
4. Upload pcap files (max 10 GB diskspace)
5. Analysis / re-analyse packet data according to profile
6. generation of critical / warning symptoms
7. Display in
   - a) longtime dashboard Warning / critical / Raw Data (5 min. granularity)
   - b)per file dashboard Raw Data (1 sec Granularity)
8. detailed analysis
   - a) timing analysis
   - b) http analysis
   - c) more will come soon

2. Startup Workflow

2.1 Steps

1. Profile definition - the evaluation logic by its metrics
   - a) Define metrics
   - b) Set thresholds
   - c) Activate metrics
2. Import files
3. View data in longtime dashboard
4. View data in insight view

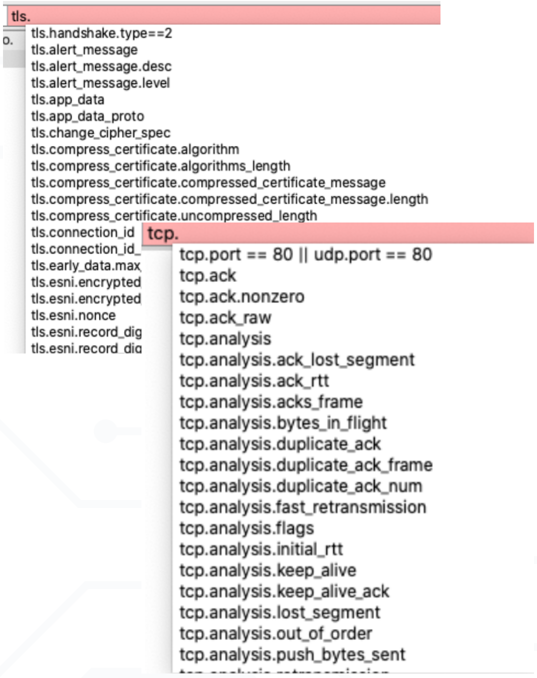
2.2 Defining the profile

The profile is the collection of defined analysis metrics which will be applied on the imported pcap files as monitoring metrics.

Metrics are same as wireshark metrics – user can use any of them for monitoring.

Wireshark can use more than 250.000 fields – thatswhy careful selection is recommended.

Enabling large number of metrics which are not used or useless – consumes processing resources – and will blast your dashboard.



```
tls.
tls.handshake.type==2
tls.alert_message
tls.alert_message.desc
tls.alert_message.level
tls.app_data
tls.app_data_proto
tls.change_cipher_spec
tls.compress_certificate.algorithm
tls.compress_certificate.algorithms_length
tls.compress_certificate.compressed_certificate_message
tls.compress_certificate.compressed_certificate_message.length
tls.compress_certificate.uncompressed_length
tls.connection_id
tls.connection_id_
tls.early_data.max
tls.esni.encrypted
tls.esni.encrypted
tls.esni.nonce
tls.esni.record_dig
tls.esni.record_dig
```

```
tcp.
tcp.port == 80 || udp.port == 80
tcp.ack
tcp.ack.nonzero
tcp.ack_raw
tcp.analysis
tcp.analysis.ack_lost_segment
tcp.analysis.ack_rtt
tcp.analysis.acks_frame
tcp.analysis.bytes_in_flight
tcp.analysis.duplicate_ack
tcp.analysis.duplicate_ack_frame
tcp.analysis.duplicate_ack_num
tcp.analysis.fast_retransmission
tcp.analysis.flags
tcp.analysis.initial_rtt
tcp.analysis.keep_alive
tcp.analysis.keep_alive_ack
tcp.analysis.lost_segment
tcp.analysis.out_of_order
tcp.analysis.push_bytes_sent
```

The profile contains:

1. the metrics definition (wireshark field, filter, analysis method)
2. possibly thresholds for metrics / thresholds (are optional, if not set , dashboard will show raw values)
3. the list of selected metrics (you can have defined many metrics – which you don't use for this analysis)

In this trial version we offer just a single profile – which is default for the free version.

All other versions - like sharkMon-Tourist-, Pro- or Enterprise version - allow the definition of multiple scenarios – each using different profiles.

With this feature user can define for each usecase their own deep profiles – eg. a DNS-analysis scenario for their DNS requests using a deep **DNS profile** – and an **TLS/SSL profile** for deep TLS-analysis using other or even same packet data.

2.3 Metric organization

Metrics are organized

- **categories** (network, connection, application) - these are the sections which will be used later in dashboards – so network metrics will be displayed in the network part of dashboard,

- **classes** – user can organize their own classes. We use classed eg., for a topic or protocol section like TCP or TLS, which can include a large number of class metrics

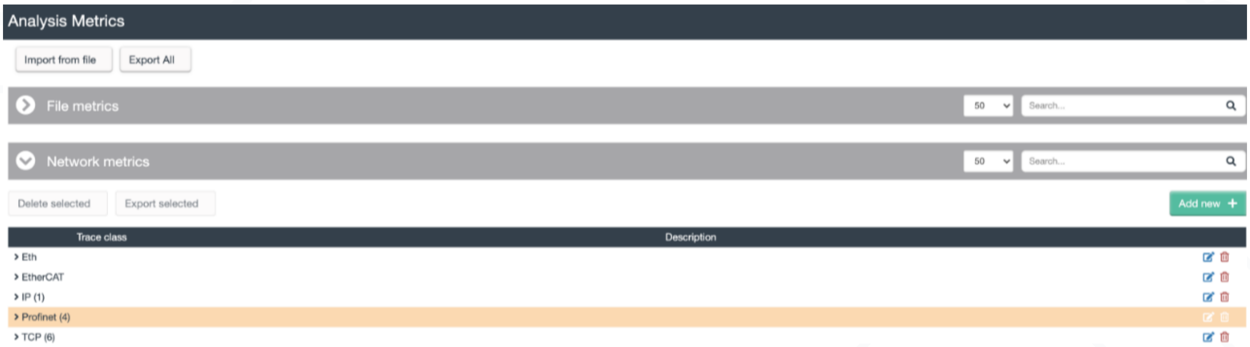
3. Workflow

3.1 Profil section

Sharkmon comes with a preinstalled profile – which can be easily edited according to your needs.

Open the profile menu option Trace profiles

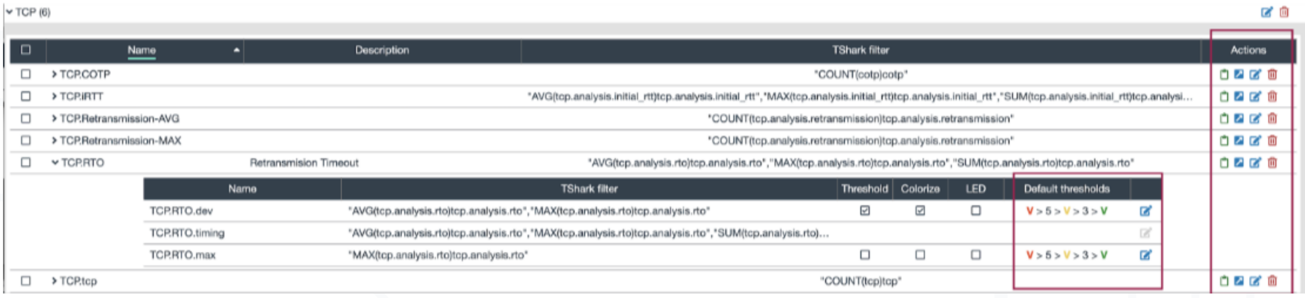
Scroll down to analysis metrics



Trace class	Description
› Eth	
› EtherCAT	
› IP (1)	
› Profinet (4)	
› TCP (6)	

Open one of defined classes
Here you find the metric definitions

- The edit section at the end of row – to edit a metric click the 📝 field
- The threshold section



TCP (6)

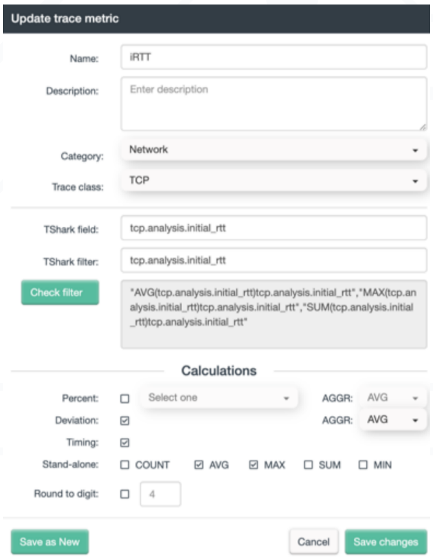
☐	Name	Description	TShark filter	Actions
☐	› TCP.COTP		"COUNT(cotp)cotp"	
☐	› TCP.iRTT		"AVG(tcp.analysis.initial_rtt)tcp.analysis.initial_rtt","MAX(tcp.analysis.initial_rtt)tcp.analysis.initial_rtt","SUM(tcp.analysis.initial_rtt)tcp.analysi...	
☐	› TCP.Retransmission-AVG		"COUNT(tcp.analysis.retransmission)tcp.analysis.retransmission"	
☐	› TCP.Retransmission-MAX		"COUNT(tcp.analysis.retransmission)tcp.analysis.retransmission"	
☐	⌄ TCP.RTO	Retransmision Timeout	"AVG(tcp.analysis.rto)tcp.analysis.rto","MAX(tcp.analysis.rto)tcp.analysis.rto","SUM(tcp.analysis.rto)tcp.analysis.rto"	
☐	› TCP.tcp		"COUNT(tcp)tcp"	

Name	TShark filter	Threshold	Colorize	LED	Default thresholds	
TCP.RTO.dev	"AVG(tcp.analysis.rto)tcp.analysis.rto","MAX(tcp.analysis.rto)tcp.analysis.rto"	☑	☑	☐	V > 5 > V > 3 > V	📝
TCP.RTO.timing	"AVG(tcp.analysis.rto)tcp.analysis.rto","MAX(tcp.analysis.rto)tcp.analysis.rto","SUM(tcp.analysis.rto)...					📝
TCP.RTO.max	"MAX(tcp.analysis.rto)tcp.analysis.rto"	☐	☐	☐	V > 5 > V > 3 > V	📝

3.2 Edit a metric

User actually need only to know the tshark field and filter – and select the relevant analysis options – like deviation, timing, AVG or MAX - the correct syntax will be created automatically.
Syntax is tshark syntax – and can be always verified by tshark.

Best way to understand the process is by defining a new metrics – lets create together metric for dns.time, the response time for DNS requests.



Update trace metric

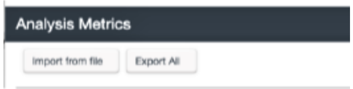
Name: iRTT
Description: Enter description
Category: Network
Trace class: TCP
TShark field: tcp.analysis.initial_rtt
TShark filter: tcp.analysis.initial_rtt
Check filter
"AVG(tcp.analysis.initial_rtt)tcp.analysis.initial_rtt","MAX(tcp.analysis.initial_rtt)tcp.analysis.initial_rtt","SUM(tcp.analysis.initial_rtt)tcp.analysis.initial_rtt"

Calculations

Percent: ☐ Select one AGGR: AVG
Deviation: ☑ AGGR: AVG
Timing: ☑
Stand-alone: ☐ COUNT ☑ AVG ☑ MAX ☐ SUM ☐ MIN
Round to digit: ☐ 4

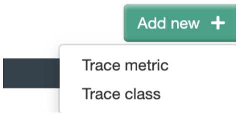
Save as New Cancel Save changes

On the profile page go to the analysis metric section



Analysis Metrics

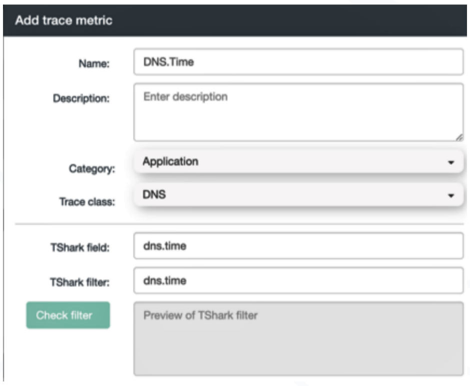
Click on “add New” button in the profile section



Click on Trace metrics and the definition popup will open

- Enter a name (dns.time)
- Select the category
- Select a trace class
- Enter the Tshark-field (dns.time)

The used filter field is still empty now



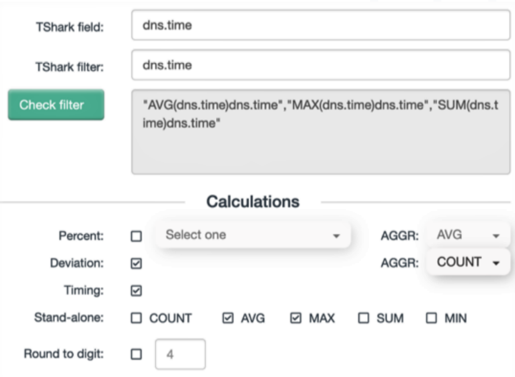
Add trace metric

Name: DNS.Time
Description: Enter description
Category: Application
Trace class: DNS
TShark field: dns.time
TShark filter: dns.time
Check filter
Preview of TShark filter

Now select your analysis method options.

Here we use timing to understand the timing effect – and want see AVG and MAX values in dashboards.

and the filter field will be automatically pre-set.
User must only click on the “check-filter” button – now metris is defined.


TShark field: dns.time

TShark filter: dns.time

"AVG(dns.time)dns.time","MAX(dns.time)dns.time","SUM(dns.time)dns.time"

Calculations

Percent: □ Select one — AGGR: AVG

Deviation: ☑ — AGGR: COUNT

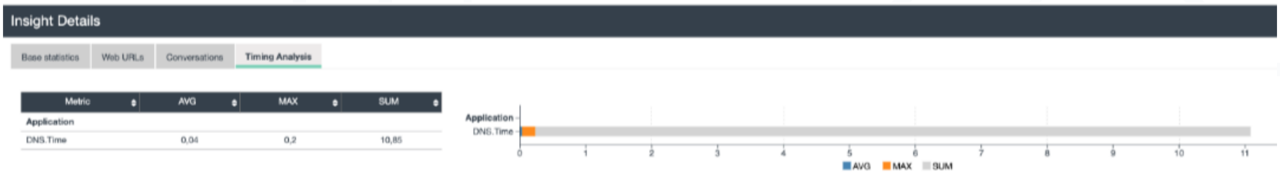
Timing: ☑

Stand-alone: □ COUNT ☑ AVG ☑ MAX □ SUM □ MIN

Round to digit: □ 4

We support here also **MAX** values. The great thing about max values – is that they will not be equalize such values in Average calculations, where the short high peaks easily can get hidden.

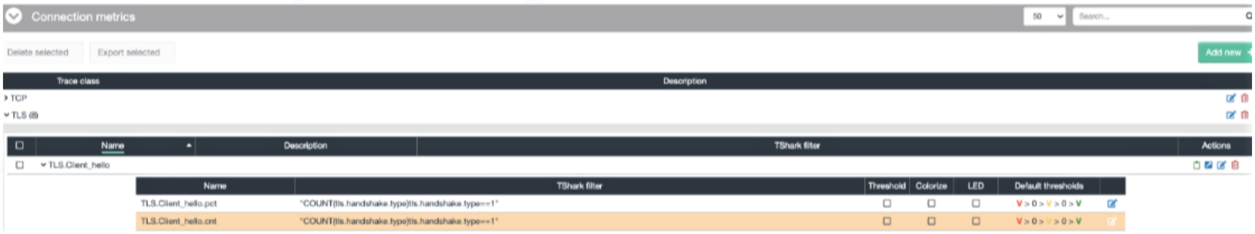
Using timing selection user can view in the insight details the timing effects of the protocol


Insight Details

Metric	AVG	MAX	SUM
Application			
DNS.Time	0,04	0,2	10,85

3.3 Thesholds

Thresholds are isolating the symptoms from normal data.
User can define 2 levels: warning and **critical** thresholds.
They can be set as global thresholds – but also changed for each profile.
So you could analyze same data with profile A and profile B – with different metrics or just different symptom thresholds.
Global thresholds are changed in the metrics definition window – if you “open” the selected metrics


Connection metrics

Trace class	Description
› TCP	
⌄ TLS (8)	

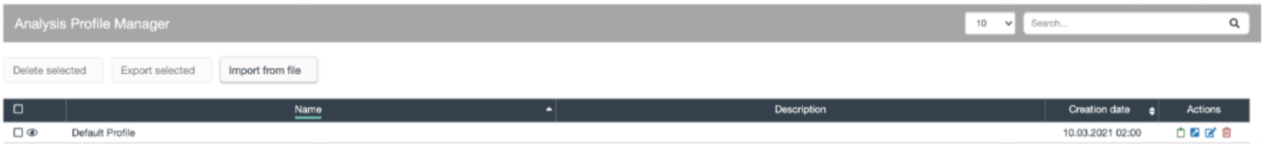
□	Name	Description	TShark filter	Actions
□	⌄ TLS.Client_hello			

Name	TShark filter	Threshold	Colorize	LED	Default thresholds
TLS.Client_hello.pct	"COUNT(tls.handshake.type)tls.handshake.type==1"	□	□	□	V > 0 > V > 0 > V
TLS.Client_hello.cnt	"COUNT(tls.handshake.type)tls.handshake.type==1"	□	□	□	V > 0 > V > 0 > V

3.4 Enabling metrics for selected profile

All defined metrics which should be used for the current analysis must be activated.
You just need to open the profile manager and open the profile (pls. click again on the edit

button at the end of line ✎ field

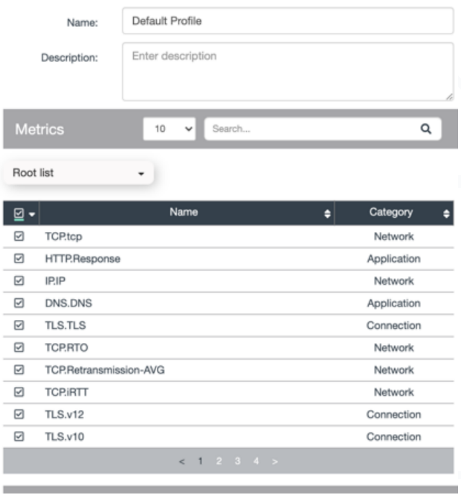


☐	Name	Description	Creation date	Actions
☐ 👁	Default Profile		10.03.2021 02:00	

and activate your defined metrics.

All metrics which are activated will be used in the profile for the following analysis.
You can run also here a re-analysis of data if you decided to change thresholds or added new metrics here.

!!! if you need other metrics and need support of definition, pls contact us - we provide you free metrics profiles according to your request.

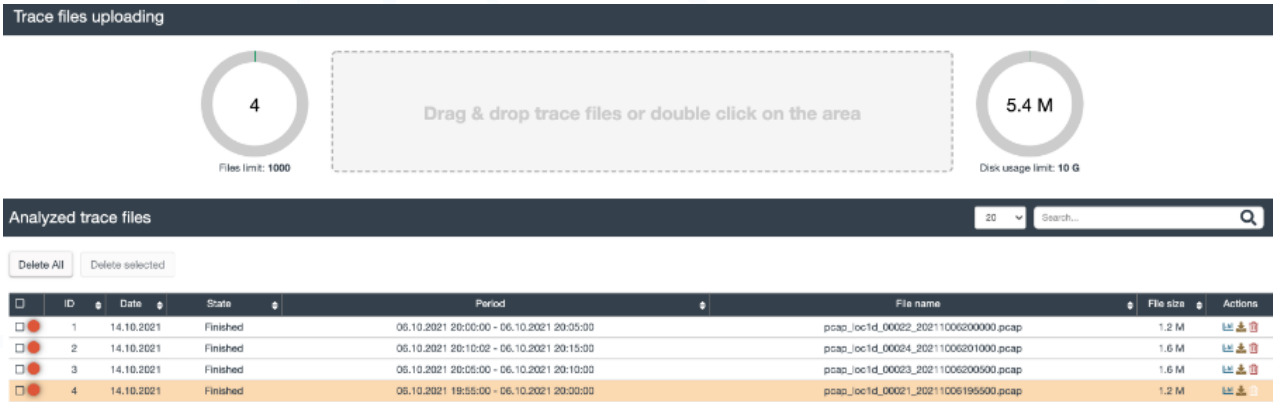

Name: Default Profile

Description: Enter description

☑	Name	Category
☑	TCP.tcp	Network
☑	HTTP.Response	Application
☑	IP.IP	Network
☑	DNS.DNS	Application
☑	TLS.TLS	Connection
☑	TCP.RTO	Network
☑	TCP.Retransmission-AVG	Network
☑	TCP.iRTT	Network
☑	TLS.v12	Connection
☑	TLS.v10	Connection

4. File-upload process

Open in menu file management – which will show the following screen

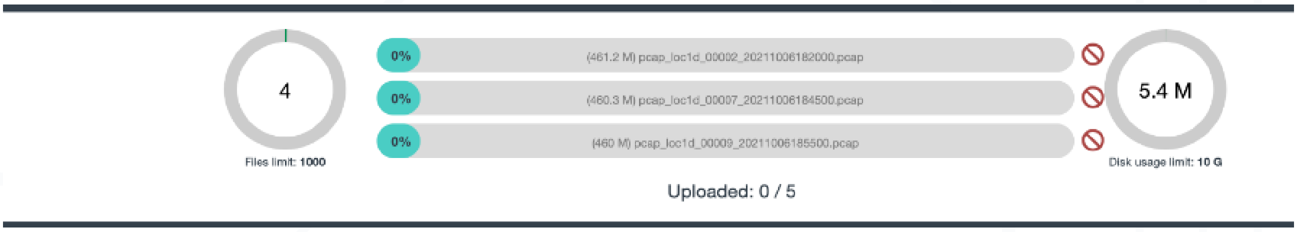


☐	ID	Date	State	Period	File name	File size	Actions
☐ ●	1	14.10.2021	Finished	06.10.2021 20:00:00 - 06.10.2021 20:05:00	pcap_loc1d_00022_20211006200000.pcap	1.2 M	
☐ ●	2	14.10.2021	Finished	06.10.2021 20:10:02 - 06.10.2021 20:15:00	pcap_loc1d_00024_20211006201000.pcap	1.6 M	
☐ ●	3	14.10.2021	Finished	06.10.2021 20:05:00 - 06.10.2021 20:10:00	pcap_loc1d_00023_20211006200500.pcap	1.6 M	
☐ ●	4	14.10.2021	Finished	06.10.2021 19:55:00 - 06.10.2021 20:00:00	pcap_loc1d_00021_20211006195500.pcap	1.2 M	

User can just drag & drop their pcap files from the file-browser into the application – or double-click on the upload box, select their files and the process will start.

!!! files must have extension PCAP or PCAPNG !!!

Please consider the storage limit for your files



4

Files limit: 1000

0% (461.2 M) pcap_loc1d_00002_20211006182000.pcap

0% (460.3 M) pcap_loc1d_00007_20211006184500.pcap

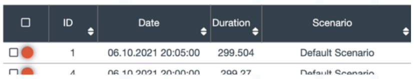
0% (460 M) pcap_loc1d_00009_20211006185500.pcap

5.4 M

Disk usage limit: 10 G

Uploaded: 0 / 5

Files will be now imported and analyzed based on profile. The metric definition allows to set metrics as file status indicator.
eg. if you set threshold for DNS time of 1 second - and you enabled the LED function – the file will show red status after analysis.

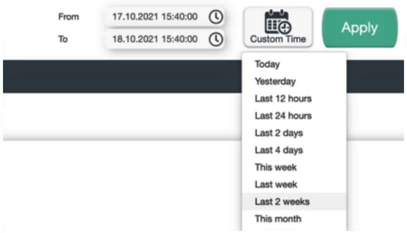


□	ID	Date	Duration	Scenario
□ ●	1	06.10.2021 20:05:00	299.504	Default Scenario
□ ●	4	06.10.2021 20:00:00	299.27	Default Scenario

5. Dashboard section

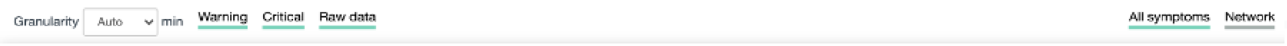
After data import and packet analysis – the scenario dashboard should show data – if correct time is selected (time of pcap data, you can find I file management section)

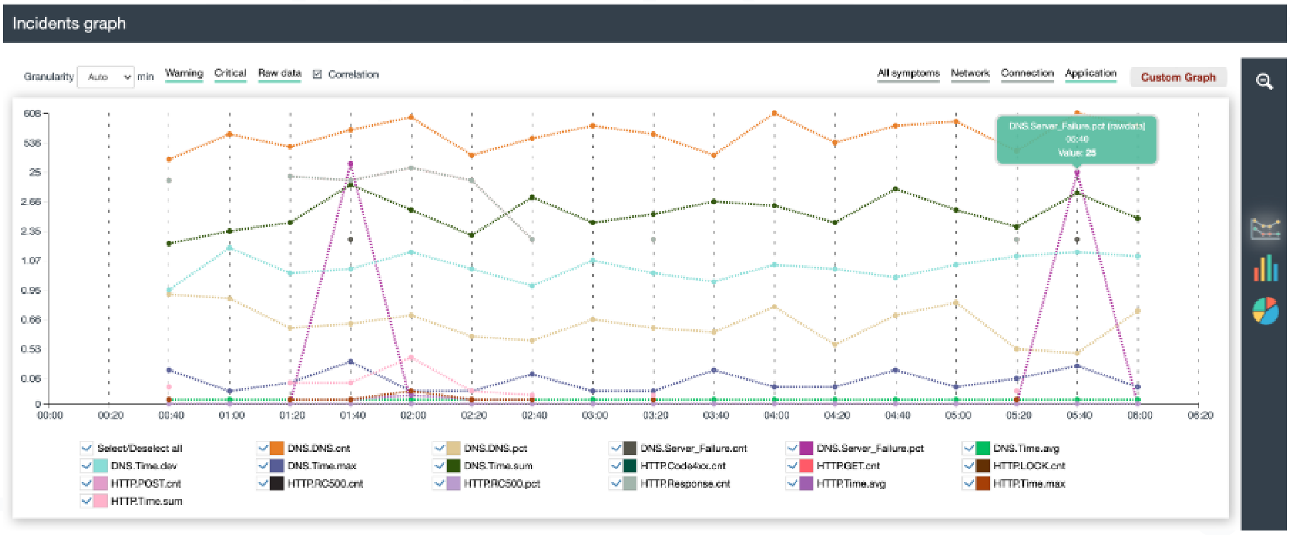
Raw Data should be selected in the top selector.



From 17.10.2021 15:40:00

To 18.10.2021 15:40:00





Incidents graph

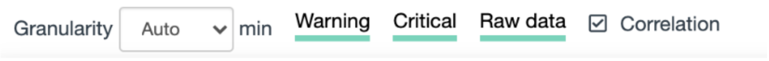
Graph-type can be selected – currently we have stacked- , line- or pie chart.

Only the line chart currently enable a logarithmic view (correlation) which allows to show in one chart metrics with tiny values like a server response time in milliseconds AND superlarge values - like packet, bytes etc.

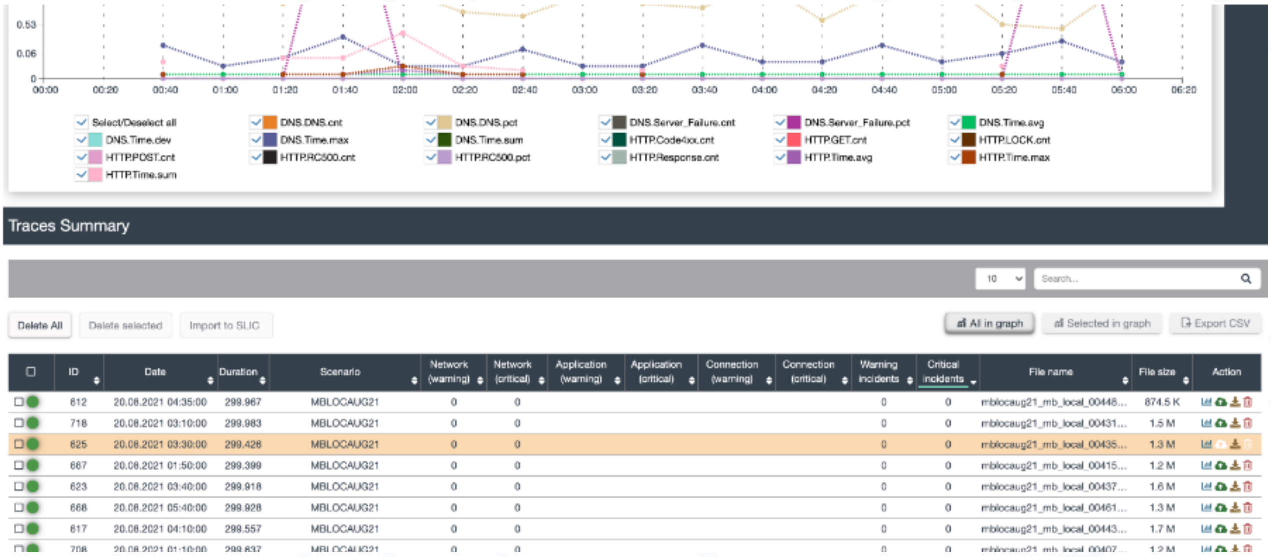
You can select the time with your mouse in the chart, or click on a bar to go directly to the requested time.

Graph-type can be selected – currently we have stacked- , line- or pie chart.

Only the line chart currently enable a logarithmic view (correlation) which allows to show in one chart metrics with tiny values like a server response time in milliseconds AND superlarge values - like packet, bytes etc.

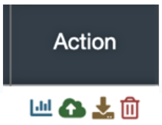


Below the graph – you find the file list which was used for the analysis for the selected time.



□	ID	Date	Duration	Scenario	Network (warning)	Network (critical)	Application (warning)	Application (critical)	Connection (warning)	Connection (critical)	Warning incidents	Critical incidents	File name	File size	Action
□ ●	612	20.08.2021 04:35:00	299.967	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00448...	874.5 K	📊 ☁ ⬇ 🗑
□ ●	718	20.08.2021 03:10:00	299.983	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00431...	1.5 M	📊 ☁ ⬇ 🗑
□ ●	625	20.08.2021 03:30:00	299.428	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00435...	1.3 M	📊 ☁ ⬇ 🗑
□ ●	667	20.08.2021 01:50:00	299.399	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00415...	1.2 M	📊 ☁ ⬇ 🗑
□ ●	623	20.08.2021 03:40:00	299.918	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00437...	1.6 M	📊 ☁ ⬇ 🗑
□ ●	668	20.08.2021 05:40:00	299.928	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00461...	1.3 M	📊 ☁ ⬇ 🗑
□ ●	617	20.08.2021 04:10:00	299.557	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00443...	1.7 M	📊 ☁ ⬇ 🗑
□ ●	708	20.08.2021 01:10:00	299.837	MBLOCAUG21	0	0					0	0	mblocaug21_mb_local_00407...	1.2 M	📊 ☁ ⬇ 🗑

You have a number of options here –



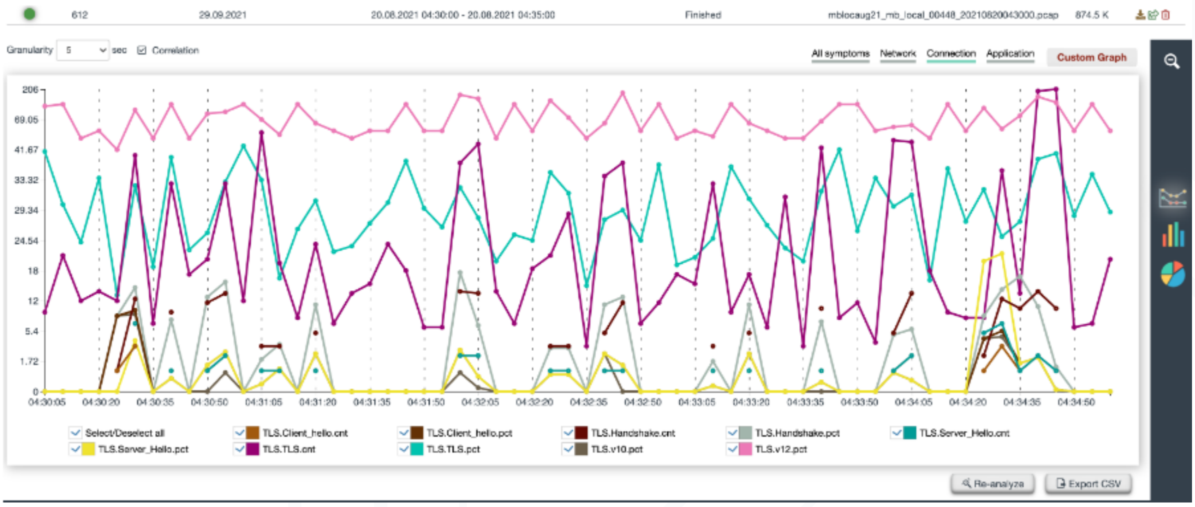
1. Open the per-file Insight dashboard – by clicking on the gree/ red LED
2. Forward the file to cloudshark (in trial not supported)
3. Download the file
4. Delete the file

6. Insight Dashboard

The insight dashboard is showing data with granularity down to 1 second.

It is assumed that single files are not longer than one hour – we suggest split large files in several 5 min chunks.

If the files are covering times longer than 10 minutes – please set the granularity to 5 or 10 seconds.



● 612 29.09.2021 20.08.2021 04:30:00 - 20.08.2021 04:35:00 Finished mblocaug21_mb_local_00448_20210820043000.pcap 874.5 K

Granularity 5 sec ☑ Correlation

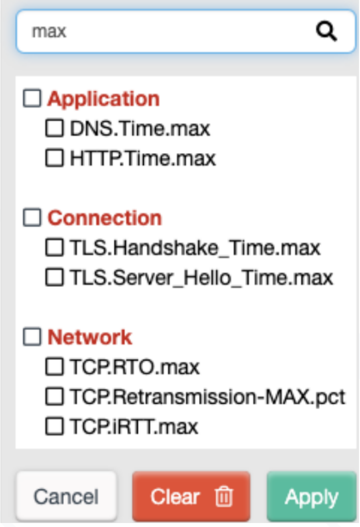
Options here are:

- Select granularity - please adjust according to time span
- Logarithmic view
- Symptom category
- Custom graph

“All symptoms” category does show all metrics actually – which can easily overload your dashboard.

Symptom categories are helpful to understand the technology better.

If user want mix metrics from various categories in one chart – they can use the custom graph option to select any metric for display.



max

□ Application
- □ DNS.Time.max
- □ HTTP.Time.max

□ Connection
- □ TLS.Handshake_Time.max
- □ TLS.Server_Hello_Time.max

□ Network
- □ TCP.RTO.max
- □ TCP.Retransmission-MAX.pct
- □ TCP.iRTT.max

7. Summary

These few steps should give you several options to analyze and understand you pcap data from many pcap files / packet data.

We would be happy to receive your feedback, options you would like to see – or some things don’t work as expected.

Please contact us at:

sharkinfo@interviewns.de

or

www.interviewns.de