Содержание

1 Traffic analysis

Equipment

To configure the correct operation of the Traffic Parsing section, you must add equipment of the "Pcap Parsing Server" type to the Equipment List Management section.

Traffic parsing equipment configuration:

1. Processor (CPU) 2.5 GHz, 2 pcs
2. Random access memory (RAM) from 4 GB
3. Hard disk drive (HDD) from 100 GB
4. Operating system Ubuntu 20.04

To install the necessary utilities, run the following command:

```
apt install wireshark tshark sox
```

Section

To go to the traffic parsing section in the menu, go to the "Lawful interception"→"Traffic parsing"→"Traffic parsing" section.

The Traffic Parsing section looks like the figure below.

Tasks

The tasks for Traffic Mining are located on the left side of the Traffic Mining page.

Creating a task

To create a new Traffic Analysis task, click the "+" button in the toolbar above the list of existing tasks.

In the task creation form that opens, enter:

- Task name
- Description of the task

Click the "Save" button.

Editing a task

To edit a task, click the edit button next to an existing task.

In the task editing form that opens, change:

- Task name
- Description of the task

Click the "Save" button.

Deleting a task

To delete a task, click the "Delete" button next to the existing task and confirm or cancel the action.

Files

The files for Traffic Parsing are located in the central part of the Traffic Parsing page.

Add file

To add a new file for Traffic Parsing, click on the "+" button in the toolbar above the list of added files.

In the opened form for adding a file:

- Upload or drag pcap file;
- If necessary, set the display name and description for the file;
- Specify the required types of traffic parsing (Web, Dns, Mail, Voip, Ftp);

Click the "Save" button.

Editing the file

To edit a file for Traffic Parsing, click the edit button next to an existing file.

In the file editing form that opens, you can change:

- Displayed file name;
- Description of the file;
- Types of traffic parsing (Web, Dns, Mail, Voip, Ftp);

Click the "Save" button.

If changes have been made to the types of traffic parsing, a confirmation form for restarting traffic parsing for this file will appear on the screen.

Deleting a file

To delete a file, click on the "Delete" button next to the existing file and confirm or cancel the action.

Restart file parsing

To restart file parsing:

1. Select the required file from the list;
2. Click on the restart parsing button in the toolbar;
3. Confirm or cancel the action.

Importing files from the traffic capture section

Files for traffic parsing can be imported from the "Traffic Capture" section.

Go to the "Lawful Interception"→"Traffic Capture" section.

In the list of files, select the files you want to parse and click the parse button.

In the opened form:

- Select the Traffic Parsing task into which the files will be imported.
- If "New task" is selected, enter the name of the task that will be created during import.
- Parse types for imported files (Web, Dns, Mail, Voip, Ftp).

Click on the "Apply" button. After the file import process is completed, a window will appear prompting you to go to the "Traffic Analysis" section.

Parsing results

The parsing results are located on the right side of the Traffic Parsing page.

Web

The Web parsing results tab displays HTTP requests.

Requests

The "Requests" tab displays "raw" data about requests.

The following data is available in the table:

- Date and time of request
- Request address
- Size of response in bytes
- Method

When you click on the "Additional information about the request" (?) button, a popup will open with additional information about the request:

- Agent
- Host
- Url
- Type of content
- Encoding
- Request method
- Response code
- Size of response in bytes
- Sender port
- Destination port
- TCP time
- IP protocol
- IP version
- Sender IP
- IP received
- Eth type
- Sender's Eth
- Eth of the recipient

- File ID to parse
- Filename to parse
- Filename with response content

Pictures

The Images tab displays queries that returned images.

DNS

The DNS parsing results tab displays the hosts.

The following data is available in the table:

- Date and time of request
- Host

Additional information

When you click on the "Additional information about the request" (?) button, a popup will open with additional information about the request:

- List of hosts
- Address list
- List of certificates
- Request date
- Response time
- Sender port
- Destination port
- IP protocol
- IP version
- Sender IP
- Destination IP
- Eth type
- Sender's Eth
- Eth of the recipient
- Request ID
- File ID to parse
- Filename to parse

Mail

On the MAIL parsing results tab, sent/received Emails.

The following data is available in the table:

- Date and time of sending / receiving;
- Sender
- Recipient
- Letter subject

Content

When you click on the Message Content button, a popup will open in which are available:

- Sender
- Recipient
- Letter subject
- Text of the letter
- List of attached files to the letter (can be downloaded)

Additional information

Clicking on the Additional Information(?) button will open a popup with additional information about the letter:

- Sender port
- Destination port
- IP protocol
- IP version
- Sender IP
- Destination IP
- Eth type
- Sender's Eth
- Eth of the recipient
- Sender
- Recipient
- Topic
- Letter ID
- User Agent
- MIME version
- Type of content
- Language
- Composite type
- Composite content type

- Multipart content encoding
- Disposition of compound content
- Request ID
- File ID to parse
- Eml file name

Voip

On the Voip parsing results tab, information about completed Voip sessions.

The following data is available in the table:

- Date and time of the session
- Session duration
- caller
- Callable

Audio recording

When you click on the Recordings button, a popup will open where you can listen to audio recordings:

- caller
- Callable
- Combined

Query Logs

When you click on the Request logs button, a popup will open with the logs of all session requests.

Additional information

When you click on the "Additional information" (?) button, a popup will open with additional information about the session:

- Sender port
- Destination port
- IP protocol
- IP version
- Sender IP

- Destination IP
- Eth type
- Sender's Eth
- Eth of the recipient
- Session duration
- caller
- Callable
- Call ID
- Ssrc outgoing
- Ssrc incoming
- Audio file names
- File ID to parse

FTP

The FTP parsing results tab displays files sent/received via FTP. The following data is available in the table:

- Date and time of request
- File name
- Direction (Download/Upload)
- File size in bytes
- Customer address
- Server address

Additional information

When you click on the "Additional information" (?) button, a popup will open with additional information about the request:

- Sender port
- Destination port
- IP protocol
- IP version
- Sender IP
- Destination IP
- Eth type
- Sender's Eth
- Eth of the recipient
- File name
- Ftp Directory
- File size in bytes
- Direction
- File ID to parse
- Response file

Traffic parsing logs

To go to the section of traffic parsing logs in the menu, go to the "Lawful interception"→"Traffic parsing"→"Traffic parsing logs" section.

The traffic parsing log section looks like the figure below.