Forensics Data Collection Engine

User Manual

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Table of contents

Table of figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

Forensic Data Collection Engine (FDCE) component provides the basis required for supporting the processing and storage of data gathered from various sources into a unified structure in order to discover the relationships between devices and the related evidence and produce a timeline of cyber security incidents, including a map of affected devices and a set of meaningful chain of evidence (linked evidence).

2 Installation/Deployment

2.1 Prerequisites and hardware

Minimum Requirements

- CPU: 4Cores
- RAM: 4GB
- GPU: Not needed
- SPACE: 25GB

2.2 Deployment without using Docker

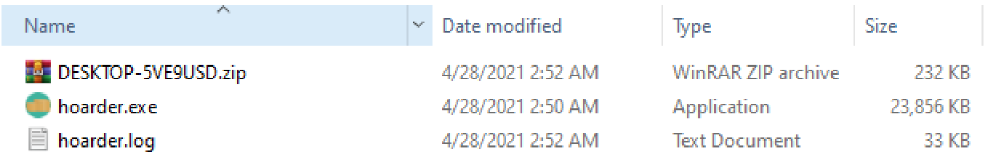
The FDCE component can be deployed using the included installation bash script.

3 Operation and Maintenance

The basic example depicts the necessary steps to acquire forensics artifacts from a pc connected to the network, upload them into collection engine and set a timeline of evidence for forensics analysis.

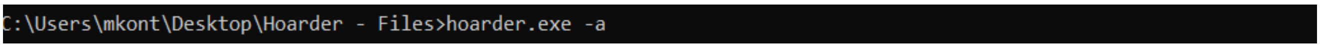
3.1 Basic Examples

For the initial point of the **basic example,** is the acquisition of artifacts from a pc connected to the network, which is performed through the execution of the “collector” agent (**Figure 3.1**). The output of this process is a .zip file () containing the necessary data which shall be uploaded to the collection engine.



Name	Date modified	Type	Size
DESKTOP-5VE9USD.zip	4/28/2021 2:52 AM	WinRAR ZIP archive	232 KB
hoarder.exe	4/28/2021 2:50 AM	Application	23,856 KB
hoarder.log	4/28/2021 2:52 AM	Text Document	33 KB

Figure 3.1 Collection agent path



```
C:\Users\mkont\Desktop\Hoarder - Files>hoarder.exe -a
```

Figure 3.2 Execution of evidence collection agent

The next step is to navigate through FDCE UI menu items. **Figure 3.3** depicts the administrator panel where all the created by the user **“Cases”** are listed. To add a new **“Case**” select the “+” button. A new modal window appears on the screen, titled **“Case details”** (**Figure 3.4**), where the users are requested to fill in the task name (“**Name**”), and status (Active, or not)**.** Upon clicking the **“Submit”** button the modal disappears, and the new case appears into the Administration panel. The selected case details are depicted in **Figure 3.5** where the users, by selecting the **“Upload”** button, are requested to provide captured artifacts files (the one produced earlier by the collection agent on the specific pc - **Figure 3.6**), or alternatively, by selecting the **“Add”** button, are requested to provide any other file containing artifacts captured from other sources (**Figure 3.7**).

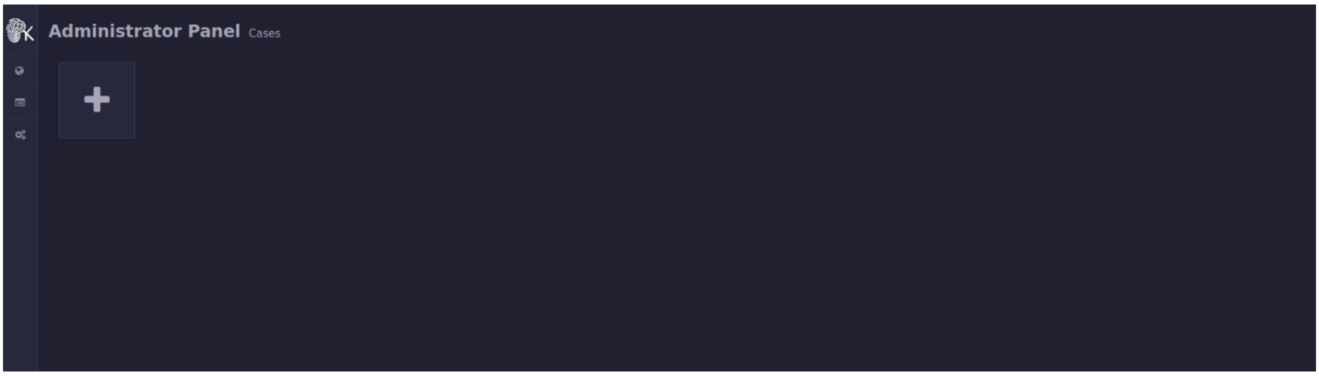
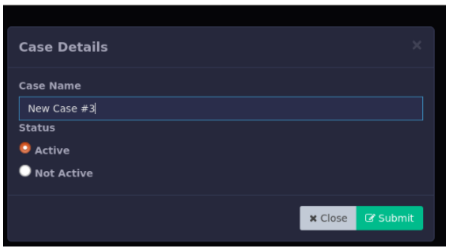


Figure 3.3 Administrator Panel


Case Details

Case Name: New Case #3

Status

● Active

○ Not Active

Figure 3.4 Add new case

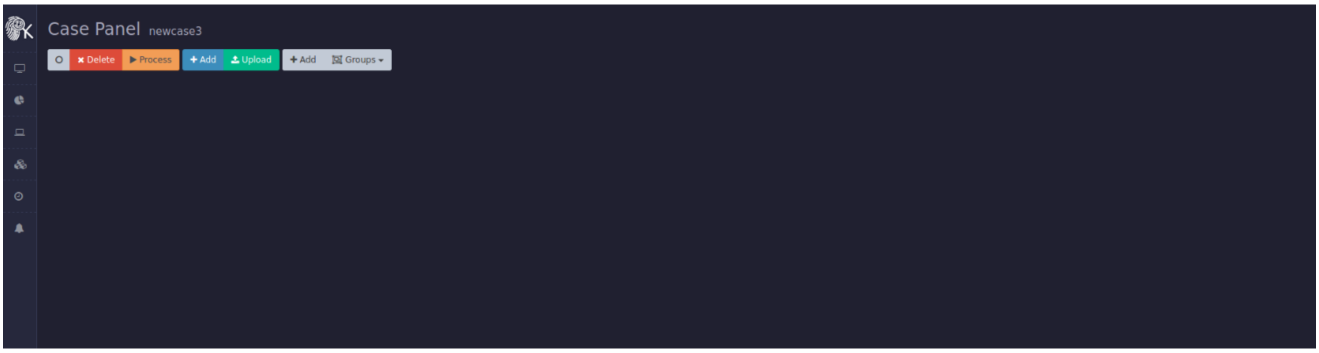
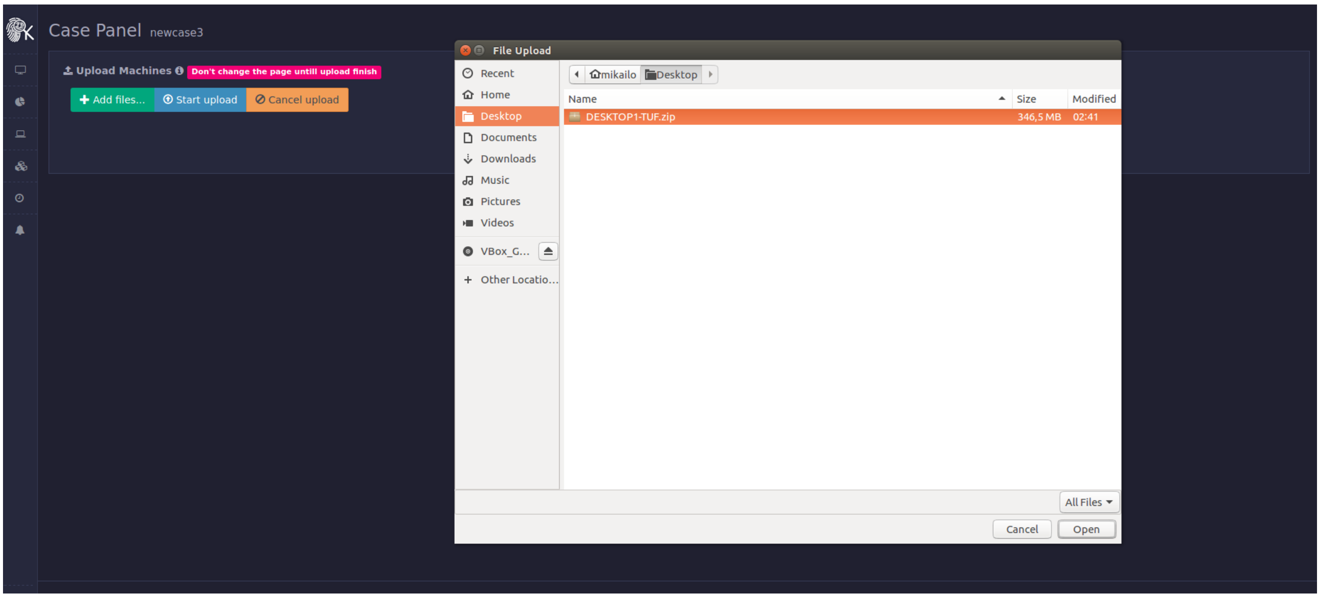


Figure 3.5 Case details panel

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Don't change the page untill upload finish

Name	Size	Modified
DESKTOP1-TUF.zip	346,5 MB	02:41

Figure 3.6 Upload agent's collected artifacts

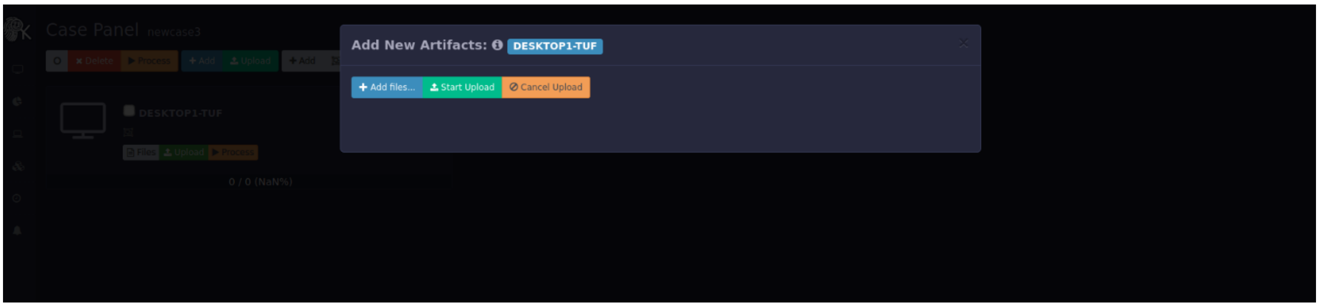
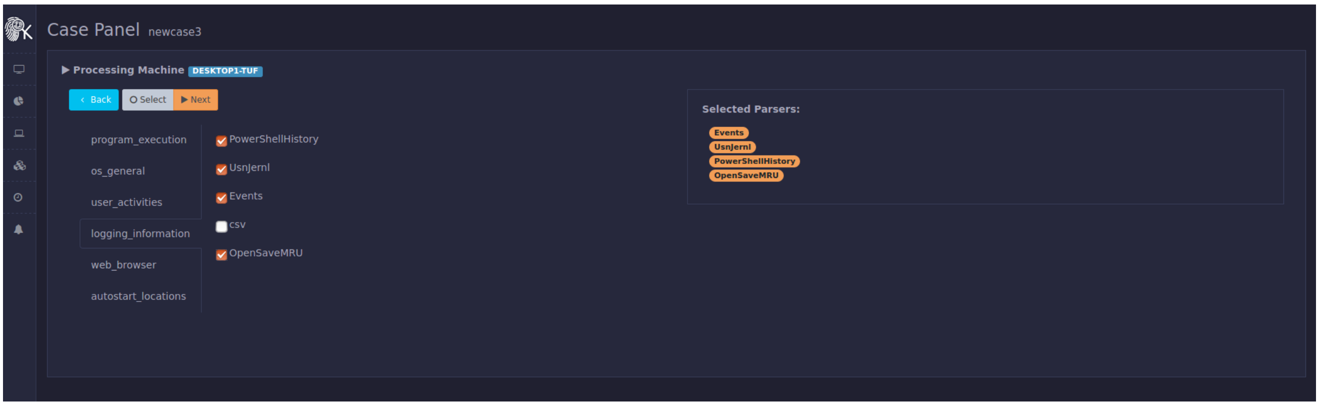


Figure 3.7 Upload artifcats from other sources

When the selection process is completed, through the **"Process"** button users select (or de-select) which categories of artifacts they wish to be integrated in the list (**Figure 3.3**). While in processing state of artifacts, the users are informed about the progress (**Figure 3.8**).



☑ PowerShellHistory
☑ UsnJernl
☑ Events
☐ csv
☑ OpenSaveMRU

Selected Parsers:
Events
UsnJernl
PowerShellHistory
OpenSaveMRU

Figure 3.8 Selection artifacts for processing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

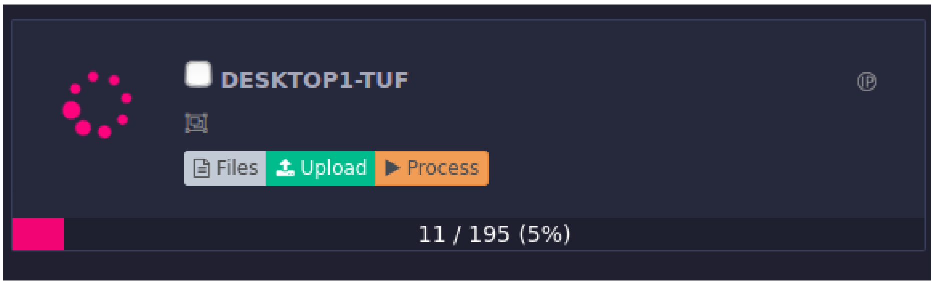
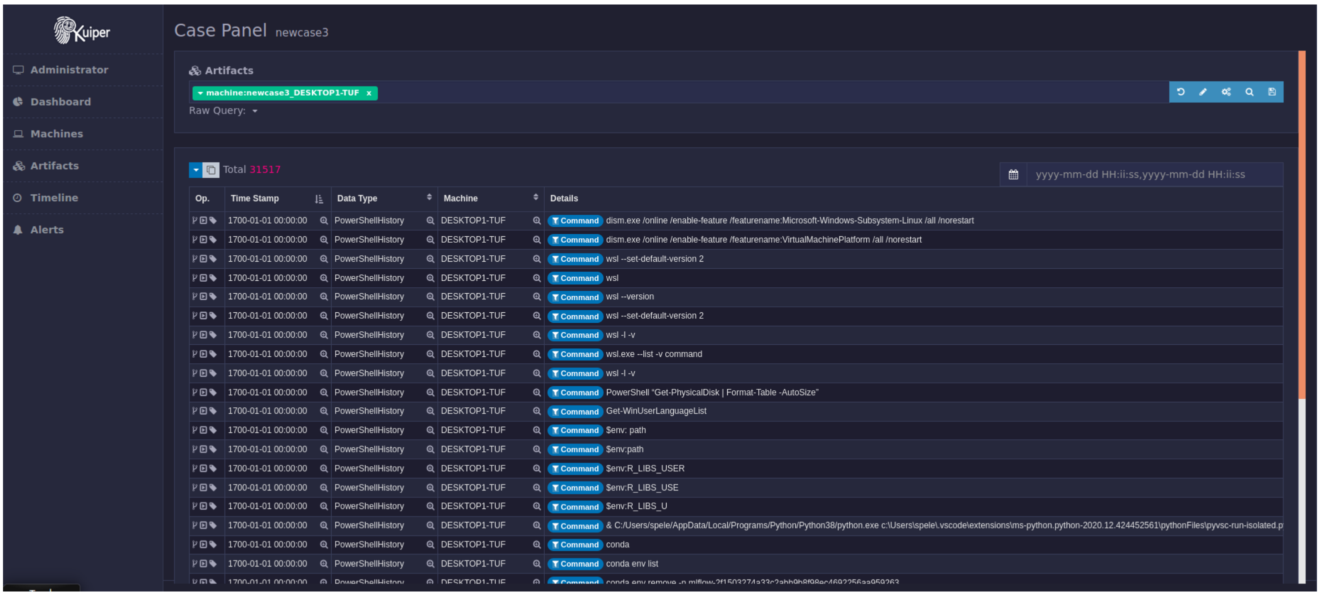


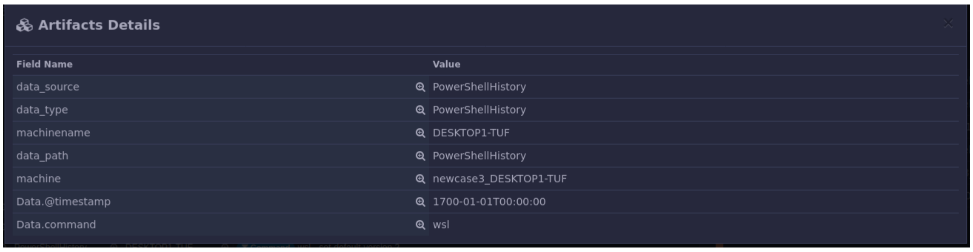
Figure 3.9 Uploading selected artifacts

Upon the completion of processing the unified list of artifacts, for the selected case, is presented to the users (**Figure 3.10**). The details for each row can be presented either by simple or double-click on the row (**Figure 3.11**).



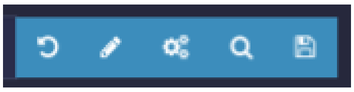
Op.	Time Stamp	Data Type	Machine	Details
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl --set-default-version 2
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl --version
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl --set-default-version 2
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl -l -v
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl.exe --list -v command
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl -l -v
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command PowerShell "Get-PhysicalDisk | Format-Table -AutoSize"
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command Get-WinUserLanguageList
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command $env: path
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command $env:path
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command $env:R_LIBS_USER
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command $env:R_LIBS_USE
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command $env:R_LIBS_U
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command & C:/Users/spele/AppData/Local/Programs/Python/Python38/python.exe c:\Users\spele\.vscode\extensions\ms-python.python-2020.12.424452561\pythonFiles\pyvsc-run-isolated.p
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command conda
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command conda env list
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command conda env remove -n mlflow-2f1503274a33c2abb9b8f98ec4692256aa959263

Figure 3.10 List of artifacts



Field Name	Value
data_source	PowerShellHistory
data_type	PowerShellHistory
machinename	DESKTOP1-TUF
data_path	PowerShellHistory
machine	newcase3_DESKTOP1-TUF
Data.@timestamp	1700-01-01T00:00:00
Data.command	wsl

Figure 3.11 Artifacts details form

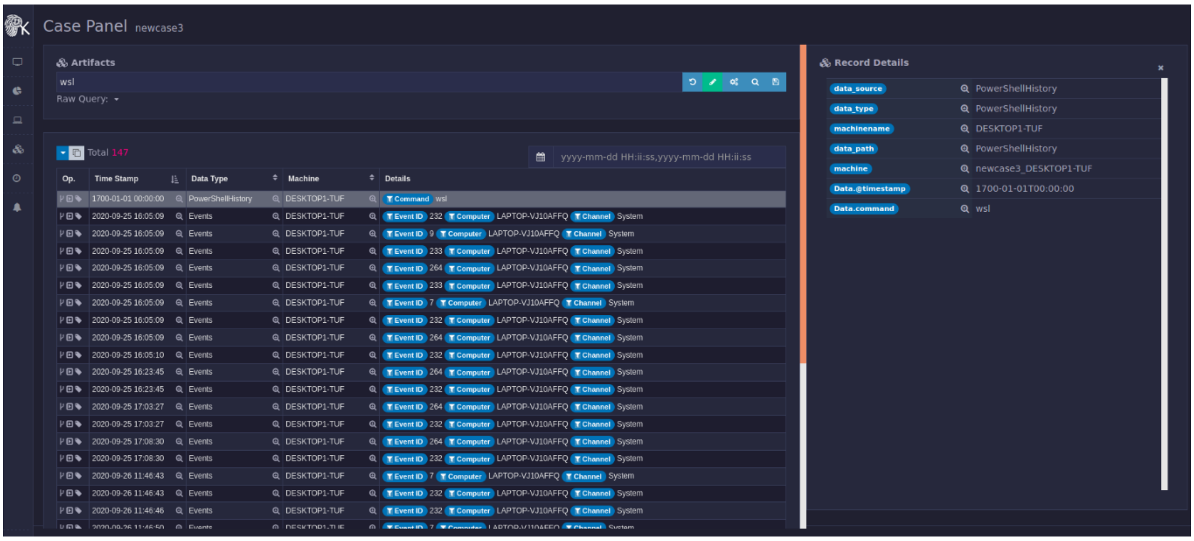
On the top right corner of the list there is a menu with 5 elements 

Moving from left to right, the provided options are:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Refresh – refresh the results based on the selected fields in the search-bar
- Simple search – create a simple query (**Figure 3.12**)
- Advanced search – create more complex query
- Search – execution of query
- Save – Save query as a Rule. These rules act as indicators facilitating the monitoring of the cases, which raise alerts whenever those rules succeed on the artifacts.

Additionally, on the left side of each row using option 🏷, users can select the row to be part of the timeline of evidence.



Case Panel newcase3

Artifacts

wsl

Raw Query:

Total 147

yyyy-mm-dd HH:ii:ss,yyyy-mm-dd HH:ii:ss

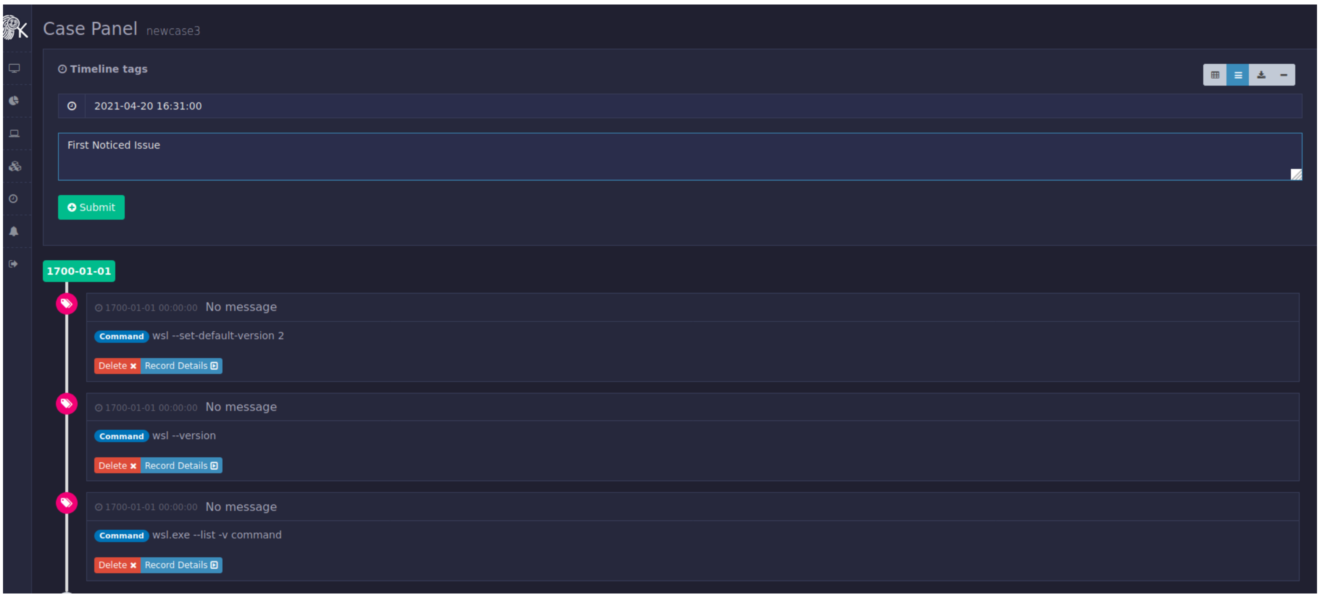
Op.	Time Stamp	Data Type	Machine	Details
	1700-01-01 00:00:00	PowerShellHistory	DESKTOP1-TUF	Command wsl
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 9 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 233 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 264 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 233 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 7 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:09	Events	DESKTOP1-TUF	Event ID 264 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:05:10	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:23:45	Events	DESKTOP1-TUF	Event ID 264 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 16:23:45	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 17:03:27	Events	DESKTOP1-TUF	Event ID 264 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 17:03:27	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 17:08:30	Events	DESKTOP1-TUF	Event ID 264 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-25 17:08:30	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-26 11:46:43	Events	DESKTOP1-TUF	Event ID 7 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-26 11:46:43	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-26 11:46:46	Events	DESKTOP1-TUF	Event ID 232 Computer LAPTOP-VJ10AFFQ Channel System
	2020-09-26 11:46:50	Events	DESKTOP1-TUF	Event ID 7 Computer LAPTOP-VJ10AFFQ Channel System

Record Details

data_source	PowerShellHistory
data_type	PowerShellHistory
machinename	DESKTOP1-TUF
data_path	PowerShellHistory
machine	newcase3_DESKTOP1-TUF
Data.@timestamp	1700-01-01T00:00:00
Data.command	wsl

Figure 3.12 Querying functionality

In order to access the timeline of selected artifacts panel, users should select the **"Timeline"** option from the left-side vertical menu. In **Figure 3.13** the timeline of selected artifacts is presented. In this figure the "**Add new tag**" is selected on the top right corner, which is provides users with the option to insert user-tags, to manually enrich investigation with their comments (**"Submit"** button saves the inserted text as a new tag).



Case Panel newcase3

Timeline tags

2021-04-20 16:31:00

First Noticed Issue

Submit

1700-01-01

1700-01-01 00:00:00 No message

Command wsl --set-default-version 2

Delete ✖ Record Details

1700-01-01 00:00:00 No message

Command wsl --version

Delete ✖ Record Details

1700-01-01 00:00:00 No message

Command wsl.exe --list -v command

Delete ✖ Record Details

Figure 3.13 Timeline panel

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Concluding, the button exports the created timeline in .json format.

3.2 Links with other Components

Link with the Security Information and Event Management component: The SIEM provides FDCE with data.

Link with the Data Traffic Monitoring component: The DTM in complementarity with FDCE stores a segment of network traffic to support further the forensics process.

Link with the Knowledge Base component: The Knowledge Base provides FDCE with a detailed description of attack patterns.

Link with the DSS component: The FDCE component provides the created by the end-user timeline of evidence.

3.3 Outcomes

Upon finishing the procedure, users have integrated the information from various sources which supports combined search, advanced querying, and most significantly the creation of timeline of events to support the forensics procedures.

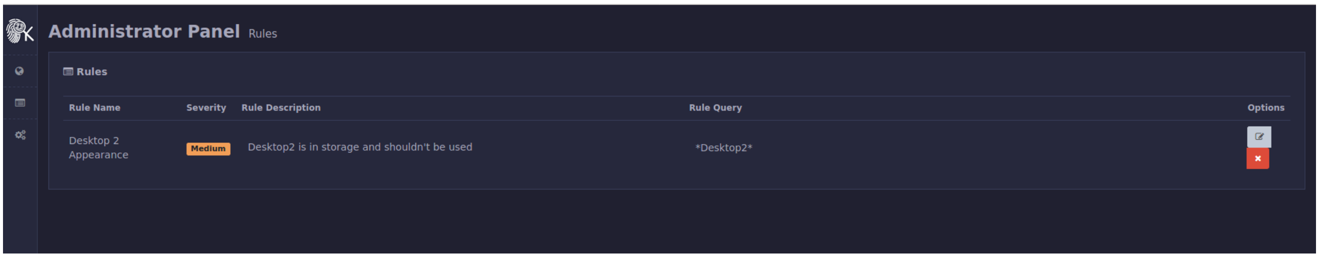
3.4 Maintenance

N/A

4 Application UI presentation

The main Administrator panel was presented in **Figure 3.3**.

Moreover, **Figure 4.1** depicts the list of created rules.



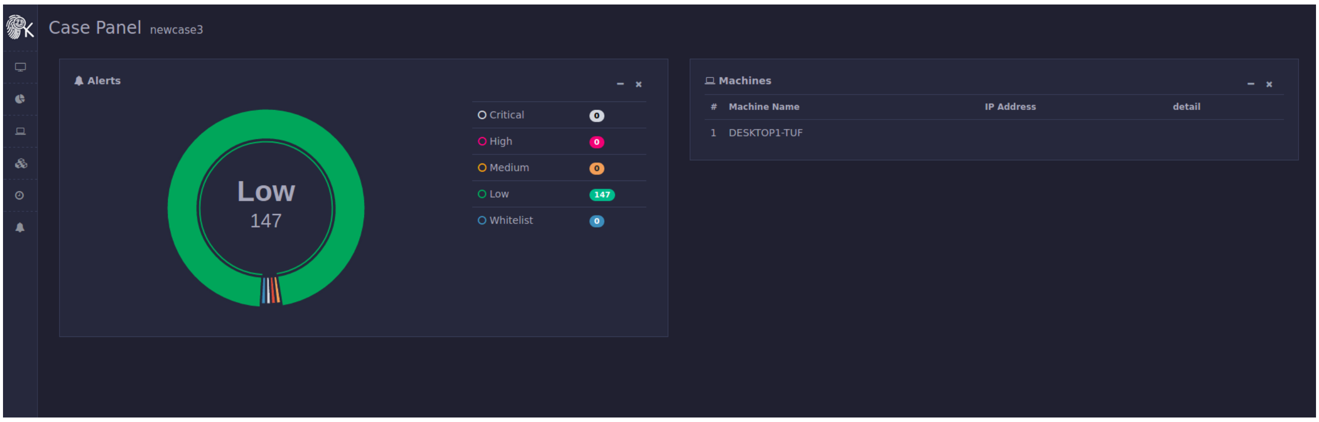
Rules

Rule Name	Severity	Rule Description	Rule Query	Options
Desktop 2 Appearance	Medium	Desktop2 is in storage and shouldn't be used	*Desktop2*	

Figure 4.1 Administrator panel – Rules

The dashboard of each “**Case**” is depicted in **Figure 4.2**, which presents the details of the specific case, the machines (PCs) relevant to the investigation, and the status of the created rules (alerts raised) based on the artifacts for the selected case.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



Case Panel newcase3

Alerts

○ Critical	0
○ High	0
○ Medium	0
○ Low	147
○ Whitelist	0

Machines

#	Machine Name	IP Address	detail
1	DESKTOP1-TUF		

Figure 4.2 Case panel

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.