We Showed Up

Prevent, Mitigate, and Recover (PMR) Insight Collective Knowledge System (PICK)
Test plan
Version 1.9
05/09/20

© 2019 We Showed Up

Document Control

Approval

The Guidance Team and the customer shall approve this document.

Document Change Control

Initial Release:	0.1
Current Release:	1.9
Indicator of Last Page in Document:	*
Date of Last Review:	05/09/20
Date of Next Review:	N/A
Target Date for Next Update:	05/09/20

Distribution List

This following list of people shall receive a copy of this document every time a new version of this document becomes available:

Guidance Team Members:
- Dr. Steven Roach
- Jake Lasley

Customer(s):
- Dr. Oscar Perez
- Vincent Fonseca
- Herandy Denisse Vasquez
- Baltazar Santaella
- Florencia Larsen
- Erick De Nava

Software Team Members:
- Ricardo Alvarez
- Daniela Garcia
- Matthew Iglesias
- Jessica Redekop
- Diego Rincon

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description
0.1	4/13/20	Diego Rincon	Added initial test case T1 in Section 4
0.2	4/13/20	Ricardo Alvarez	Added initial version of Section 2
0.3	4/14/20	Jessica Redekop	Began creating Test Suites for Section 3.
0.4	4/14/20	Matthew Iglesias	Section 1.1 – 1.6: Introduction
0.5	4/15/20	Daniela Garcia	Added second test case T2 in section 4
0.6	4/26/20	Jessica Redekop	Added Tests T10 - T13
0.7	4/26/20	Ricardo Alvarez	Added Tests T6 - T10
0.8	4/27/20	Diego Rincon	Added Tests T23 - T25
0.9	4/27/20	Matthew Iglesias	Added Tests T1 – T5
1.0	4/27/20	Daniela Garcia	Added Tests T15-T18 and create vector initial

			condition
1.1	4/27/20	Diego Rincon	Added Tasks in Section 5.
1.2	4/27/20	Matthew Iglesias	Added Section 6: Environmental and Software Requirements
1.3	4/28/20	Daniela Garcia	Edited TS14-18 to meet changes suggested by TA
1.4	4/28/20	Ricardo Alvarez	Added appendix and T26
1.5	4/28/20	Jessica Redekop	Revised T9-T16
1.6	5/5/20	Diego Rincon	Made corrections to Section 1.1-1.4 Made corrections to initial paragraph of Section 2 Added initial paragraph in Section 3 Completed test cases for the Event Test Suite in Section 4 Added Test case T9 in section 4.1.9.
1.7	5/6/20	Diego Rincon	Completed remaining test cases for the Ingestion and Graph Test Suites
1.8	5/7/20	Diego Rincon	Completed remaining test cases in Section 4
1.9	5/9/20	Diego Rincon	Made final revision of Test Plan

Note: The template presented in this document was taken from:

Donaldson, S., and S. Siegel, *Successful Software Development*. Upper Saddle River, NJ: Prentice Hall, 2001, pp. 321-323.

Note: The template presented in this document was taken from: Donaldson, S., and S. Siegel, *Successful Software Development*. Upper Saddle River, NJ: Prentice Hall, 2001, pp. 321-323 and modified by Humberto Mendoza and Steve Roach.

Supplementary information is from:

Pfleeger, S. *Software Engineering, Theory and Practice*. Upper Saddle River, NJ: Prentice Hall, 1998, p. 365.

TABLE OF CONTENTS

1. Introduction

The overview of the PMR Insight Collective Knowledge (PICK) tool test plan follows within the following sub-sections.

1.1. Purpose

The purpose of a test plan document is to fundamentally describe, analyze, and apply the necessary strategies for testing, scheduling, and deliver the appropriate resources for adequate testing. The project is carefully designed and implemented to meet the client's needs; therefore, it requires a tedious test plan. These include but are not limited to the testing of the ingestion process, but the transcription, validation, and log cleansing.

1.2. Scope

The scope of the project is based upon the current version of this test plan document, currently at version 1.5.

1.3. System Overview

The PICK tool is based on the client's needs, which the testing plan is to approach the system accordingly: The log ingestion process is accessed and ingested given on the set root directory, importing a varied file format in which to be imported. Before the system can move onto the next process of log entry ingestion, it must go through the appropriate transcriber module (depending on format) to be readable in the system. The next step involves cleansing the transcribed file with readable text, which removes unwanted characters, which may interfere with correctly ingesting the log entries to tables and vectors. We want to make sure the testing approach involves a variety of appropriate file formats to be imported and cleansed to meet system needs.

1.4. Suspension and Exit Criteria

The suspension and exit criteria for the test plan are discussed below.

- **Suspension Criteria**: testing will be suspended under the following circumstances:
    - 60% of the test cases fail
        - Strictly includes ingestion and validation process
- **Exit Criteria:** testing will stop once the following conditions are met:
    - All critical tests must pass

1.5. Document Overview

The Test Plan is indoctrinated with labeled sections for the remainder of this document:

Section 2 – Includes test items and features to be tested in the system
Section 3 – Includes the approach to test the system's functions
Section 4 – Includes documentation to applying testing methods to the system
Section 5 – Includes test scheduling, order in testing phases for the system
Section 6 – Includes hardware and/or software requirements needed to run the system
Section 7 – Includes appendix of any output medium from the tested system

1.6. References

[1] S. Roach, and E. T. Ramirez, "PICK Software Requirements and Specification."

2. Test Items and Features

Due to the nature of the PICK Tool and the ongoing update of SPLUNK (April 2020), the items to be tested include classes, functions, methods, and components in general, ranging from networking, graphing and interaction, and UI with SPLUNK. All the classes that hold intelligence (provide any functionality) should be tested, considering that this is a new release of the software altogether.

Classes to be tested along with the relevant methods include:

1. Ingestion
2. Validator
3. SPLUNKFacade
4. Cleanser
5. TableManager
6. UI
7. AudioTranscriber
8. ImageTranscriber
9. MongoDBFacade
10. Network

Features to be tested (with relevant methods and classes they pertain to):

1. Create Event – this is concerned with the event creation and initial setup of it:
    a. UI: display_new_event()
    b. UI: create_event_button_triggered()
    c. SPLUNKFacade: create_index(index_name)
    d. SPLUNKFacade: get_index_list()
    e. SPLUNKFacade: validate_user_info()
    f. MongoDBFacade: add_event(event_config, vector_list)
    g. MongoDBFacade: add_vector(vector)
    h. Network: set_lead()
2. Connect to Event – concerned with how an analyst that is not the lead will connect to an external event setup by another analyst:
    a. UI: connect_button_trigerred()
    b. UI: display_open_event()
    c. Network: get_event_list()
    d. Network: connect_user()
    e. MongoDBFacade: get_event(event_id)
    f. MongoDBFacade: get_vectort(vector_id)
3. Ingest directories into database – encompasses all the ingestion chores that shall be done for the log entries to be gathered from raw log files into the event:
    a. Ingestion: get_files_from_directory(root_path, white_team_folder, red_team_folder, blue_team_folder)
    b. Ingestion: ingest_directory_into_splunk(event_config)
    c. Ingestion: validate_files(log_files)
    d. Ingestion: validate_file_anyway(log_file)
    e. Validator: validate_file(log_file, start_time, end_time)
    f. Cleanser: cleanse_log_file(log_file)
    g. AudioTranscriber: transcribe_audio_file(log_file)
    h. ImageTranscriber: transcribe_image_file(log_file)
    i. SPLUNKFacade: add_file_to_index(log_file)
    j. SPLUNKFacade: add_directory_monitor(folder_path)
    k. MongDBFacade: add_log_file(log_file)
    l. TableManager: populate_log_entry_table()
    m. TableManager: populate_log_file_table()
    n. TableManager: populate_enforcement_action_report_table()

4. Recurrent Update of Entries – the functionality for recurrent refreshing of available entries to the user:
    a. SPLUNKFacade: refresh_log_entries()
    b. Ingestion: delta_found_triger()
    c. SplunkFacade: edit_log_entry(log_entry_id)
5. Search and Filter – functionality for searching and filtering through the log entries of the event:
    a. UI: filter_search_triggered()
    b. SPLUNKFacade: search_in_index(index, search_arguments)
    c. SPLUNKFacade: refresh_log_entries()
    d. TableManager: populate_log_entry_table()
6. Manage Tables (General) – Interaction between the user and data from the tables, including log entries, nodes, vectors, log files and relationships:
    a. UI log_entry_table_clicked()
    b. UI: log_file_table_clicked()
    c. UI: enforcement_action_report_table_clicked()
    d. UI: vector_table_clicked()
    e. UI: relationship_table_clicked()
    f. UI: display_vector_list(vector_list)
    g. UI: display_long_description(long_description)
    h. TableManager: populate_log_entry_table(log_entries)
    i. TableManager: populate_log_files_table(log_files)
    j. TableManager: populate_vector_table(vector_list)
    k. TableManager: populate_nodes_table(nodes)
    l. TableManager: populate_relationship_table(relationships)
    m. TableManager: export_csv_from_table(table, folder_path, filename)
    n. SplunkFacade: remove_log_entry(log_entry_id)
    o. SplunkFacade: edit_log_entry(log_entry_id, field)
    p. MongoDBFacade: add_node(node)
    q. MongoDBFacade: remove_node(node_id)
    r. MongoDBFacade: edit_node(node_id, field)
    s. MongoDBFacade: add_relationship(relationship)
    t. MongoDBFacade: remove_relationship(relationship_id)
    u. MongoDBFacade: edit_relationship(relationship_id, field)
    v. GraphInterface: update_graph()
7. Graphing – functionality concerned with the visual displaying and exporting of the graph:
    a. GraphInterface: display_graph(graph)
    b. GraphInterface: update_graph(graph)
    c. GraphInterface: export_graph(graph)
    d. UI: tick_triggered()
    e. MongoDBFacade: get_graph()
    f. MongoDBFacade: get_nodes()
    g. MongoDBFacade: get_vector()
8. Version Control – networking methods used for vcs and signaling:
    a. Network: connect_to_lead(lead_ip)
    b. Network: push_change(change_request, analyst_id)
    c. Network: accept_change(change_request, analyst_id)
    d. Network: reject_change(change_request, analyst_id)

3. Testing Approach

The following test suites evaluate the PICK Tool processes for the Event, Graph, Network, and Database, and apply Black Box Testing to ensure the behavior of the system matches the descriptions in the use cases of the SRS, and thus complies with the client's requirements.

Table 1: Event

TEST SUITE Event		
Description of Test Suite	**This test suite will cover the tests appropriate to operational functionalities of creating an event.**	
Test Case Identifier	**Objective**	**Criticality**
T1	**Test logging into SPLUNK**	**Critical**
T2	**Test that an event can be created and added to SPLUNK.**	**Critical**
T3	**Test opening an event.**	**Critical**
T4	**Test that ensures a start and end date on event.**	**High**
T5	**Test that the root folder of the event has 3 distinct folders: "Red", "White", "Blue"**	**Critical**
T6	**Test that a "red folder" is selected when inserting a "root directory path"**	**Critical**
T7	**Test that a "blue folder" is selected when inserting a "root directory path"**	**Critical**
T8	**Test that a "white folder" is selected when inserting a "root directory path"**	**Critical**
T9	**Test tables and graph in Vector View tab are updated when a Vector is deleted in the Event View tab.**	**Moderate**

Table 2: Ingestion

TEST SUITE Ingestion		
Description of Test Suite	**This test suite will cover the tests appropriate to the functional requirements of the ingestion process.**	
Test Case Identifier	**Objective**	**Criticality**
T10	**Test SPLUNK log file ingestion.**	**Critical**
T11	**Test for audio file transcribing ability.**	**Critical**
T12	**Test for image file transcribing ability.**	**Critical**
T13	**Cleansing non-alphabetical and non-punctuation characters.**	**Critical**
T14	**Test to validate timestamps within a certain range.**	**Critical**

Table 3: Graph

TEST SUITE Graph	
Description of Test Suite	**This test suite will cover the tests appropriate to connect the lead and analyst to the system and allocates exclusive functionalities.**

Test Case Identifier	Objective	Criticality
T15	**Test to create a vector**	**Critical**
T16	**Test adding a new node to the graph not connected to a log entry**	**Critical**
T17	**Test adding a new node to the graph that is connected to a log entry**	**Critical**
T18	**Test connecting two nodes with a relationship**	**Critical**
T19	**Test adding information to an existing node**	**Critical**

Table 4: Network

TEST SUITE Network		
Description of Test Suite	**This test suite will cover the tests appropriate to connect the lead and analyst to the system and allocates exclusive functionalities.**	
Test Case Identifier	**Objective**	**Criticality**
T20	**Test to only allow leads to create events.**	**Critical**
T21	**Test to connect analyst to lead.**	**Critical**
T22	**Test to reject connection if no lead is selected.**	**Critical**
T23	**Test to close server when lead closes connection.**	**Critical**

Table 5: Database

TEST SUITE Database		
Description of Test Suite	**This test suite will cover the tests appropriate to the version control portion of the application.**	
Test Case Identifier	**Objective**	**Criticality**
T24	**Test the retrieval of information from the database**	**Critical**

4. Tests

The purpose of this section is to:

- document test input, specific test procedures, and outcomes.
- establish test methods,
- explain the nature and extent of each test

4.1. TS1 – Event Information

4.1.1. Test T1 - Logging in SPLUNK from the PICK Tool

Objective: Test logging into SPLUNK from the PICK tool
Description: The initial condition encompasses starting the SPLUNK server, which contains all the indexes and entries derived from the tests will be contained in it.
Initial Condition:

- The user must be running SPLUNK
- The user has its own SPLUNK local credentials

Table 6: T1

Test No.: T1			Current Status: Pass	
Test Title: Logging in SPLUNK from the PICK Tool				
Testing Approach: This test will provide the utilization for logging into SPLUNK platform using admin username and password.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	In the *Team Configuration* section from the *Event View* tab, click the *Lead* checkbox.	Signal the operator as the lead of the event and the one in charge of the initial ingestion and creation of the event.	A pop-up asking for the login credentials for SPLUNK is displayed.	
2	Enter your Splunk local credentials.	Log in the SPLUNK service.	The *Lead* checkbox remains checked. The console from which the PICK Tool is running prompts the message "Successfully connected to SPLUNK: <username> ".	
Concluding Remarks: The operator can login to SPLUNK through the PICK Tool when using its own SPLUNK local credentials. However, the credentials provided in step 2 are not recognized by the system.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/5/20	

4.1.2. Test T2 – Creating a New Event in SPLUNK

Objective: Test to create a new event in SPLUNK
Notes: The estimated duration of this test is 5 minutes, before the ingestion starts and the structural check is done. In order to execute this test, the following resources shall be met:
Initial Conditions:

- The user is operating an instance of SPLUNK with appropriate credentials

- The user is checked as the Lead Analyst for the event
- The user has its own SPLUNK local credentials

Table 7: T2

Test No.: T2			Current Status: Pass	
Test title: Test the creation of an event and added onto SPLUNK				
Testing approach: This test will provide the creation of a new event which will be added onto the SPLUNK platform.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	In the text box below *Event Name*, write "t1_event".	Write the name of the event to be saved in SPLUNK	The text box below *Event_Name* has "t1_event" written on it.	
4	Enter the following date in the spin box below *Event End Timestamp*, "1/1/2020", and in the text box under *Description* write "Test".	Sets up the start date of the event	The spin box below *Event End Timestamp* has the date "2/1/2020". The text box under *Description* has "Test" written on it.	
5	Click the *Save Event* button.	Create the event to be used in this test	A text prompt below the *description* textbox will appear with the message "Event t1_event added.".	
6	Open the web browser and enter the address "http://localhost:8000"	Access SPLUNK web application	The SPLUNK web application opens	
7	Login with your SPLUNK local credentials.	Login to the same user that created the event	The homepage of the SPLUNK is displayed	

8	Click the scroll bar *Index* located at the center of the dashboard section of the homepage, and type "t1_event" in the *filter* search bar.	Find the event "t1_event", created in the PICK Tool	The event "t1_event", will appear below the search bar.	The events created by the PICK Tool are in the *Index Detail: Instance* dashboard. If the wrong dashboard is being displayed in the homepage, click on the gear at the top left corner and select the *Index Detail: Instance* dashboard.
9	Select the option "t1_event" below the *filter* search bar.	Display the contents of the event "t1_event" in the homepage dashboard.	The contents of the event "t1_event" are displayed in the homepage dashboard.	
Concluding Remarks: The operator can open the Create Event Dialog window, fill-in the event fields and save the event in the PICK Tool. Additionally, when the operator enters the SPLUNK Web application the event created from the PICK Tool is displayed in the lower panel of the home page when clicking the scroll bar *Index* and typing *t1_event.*				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/5/20		

4.1.3. Test T3 – Opening an event

Objective: Test to open an event.
Notes: The estimated duration of this test is < 1 minute.
Initial Conditions:

- The user is operating an instance of SPLUNK
- The event <<event_name>> has been previously created.
- The user has its own SPLUNK local credentials

Table 8: T3

Test No.: T3	Current Status: Pass
Test title: Opening an Event	
Testing approach: The following will be testing the persistence of event data.	

STEP	OPERATOR ACTION	PURPOSE	EXPECTED RESULTS	COMMENTS
1	In the *Team Configuration* section from the *Event* tab, click the *Lead* checkbox.	Signal the operator as the lead of the event and the one in charge of the initial ingestion and creation of the event.	A pop-up asking for the login credentials for SPLUNK is displayed.	
2	Enter your Splunk local credentials.	Log in the SPLUNK service.	The *Lead* checkbox remains checked. The console from which the PICK Tool is running prompts the message "Succesfully connected to SPLUNK: <username> ".	
3	In the *File* menu at the top left corner select *Open Event.*	Open a window to recall the session of the previous event.	The *Open Event* dialog is displayed (see appendix 9)	
4	In the *Event Name* dropdown select <<event_name>> and click the *OK* button at the bottom right of the dialog.	Open the previously initialized event.	The tables in the tabs *Event View*, *Log Entry View*, and *Vector View* display the information stored in the selected vector.	
Concluding Remarks: The operator can open the previously selected stored event, and the tables in the tabs Event View, Log Entry View and Vector View display the information stored in the selected event. There is a glitch that nullifies the visibility of nodes in the graph and the tables of the Vector View tab, but they become visible once a node and relationship are inserted in their respective tables.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/5/20		

4.1.4. Test T4 – Test that ensures a start and end date on event

Objective: Test the existence of a timestamp range is correlated to each event
Notes: The estimated duration of this test is 1 minute, before the ingestion starts and the structural check is done. In order to execute this test, the following resources shall be met:
Initial Conditions:

- The user is operating an instance of SPLUNK with appropriate credentials
- A set of nodes and vectors must exist within the specified date range for verification

Table 9: T4

Test No.: T4	Current Status: Fail
Test title: Test that an event contains a start and end date	

Testing approach: This test follows a Boolean-type function that will verify each event created is embedded with a date range (start and end), in which the user desires.				
STEP 1	OPERATOR ACTION Click the *File* dropdown in the top left corner of the main window.	PURPOSE Access the menu that gives the options to create, open or edit an event.	EXEPCTED RESULTS A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	COMMENTS
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Enter a *start date* of "01/01/2000" in the format of "MM/DD/YYYY"	Set up the start date of the event	Start date field is updated	Start date creates a boundary for log entries within that or after that date.
4	Enter an *end date* of "01/01/2020" in the format of "MM/DD/YYYY", and in the text box under *Description* write "Test".	Set up the end date of the event	End date field is updated The text box under *Description* has "Test" written on it.	End date creates a boundary for log entries within that or before that date.
5	In the text box below *Event Name*, write "t2_event".	Write the name of the event to be saved in SPLUNK	The text box below *Event_Name* has "t2_event" written on it.	
6	Click the *Save Event* button.	Create the event to be used in this test	A text prompt below the *description* textbox will appear with the message "Event t2_event added.".	
7	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
8	Click the *Edit Event* option from the dropdown menu.	Verify the saved event contains the selected start and end date	*Edit event* dialog is displayed.	

9	Click the drop box under *Event Name* and select the event "t2_event"	Display the timestamp previously saved in event "t2_event"	The date under *Event Start* is "01/01/2000", and the date for *Event End* is "01/01/2020"	
Concluding Remarks: The operator can save the event "t2_event" with the timestamps in step 3 and 4, however, they do not match with the expected result in step 9.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/5/20	

4.1.5. Test T5 – Test the "Root Folder" contains three distinct folders: "Red", "White", "Blue"

Objective: Test the existence of the Root Directory based on the given path
Notes: The estimated duration of this test is 2 minutes, after the ingestion starts and the structural check is done it's not necessary to wait until the whole directory is ingested. In order to execute this test, the following resources shall be met:
Initial Conditions:

- The user is operating an instance of SPLUNK with appropriate credentials
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 10: T5

Test No.: T5			Current Status: Pass	
Test title: Test that a "Root Folder" contains three paths named: "Red", "White", "Blue"				
Testing approach: This test follows a black-box approach based on the ingestion process. The root directory must contain the specified three folders to verify it is the "Root" directory.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t3_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *create event* dialog allows for user input for following attributes.	
4	Click the *Save Event* button.	Create the event to be used in this test	A text prompt below the *description* textbox will appear with the message "Event t3_event added.".	

5	Click the button *Browse* at the right side of *Root Directory*, go to the installation folder of the PICK Tool, double click on "tutorialdata", followed by the folder "data_for_tests", and click the button *Select Folder*.	Indicate which directory will be used in the ingestion process.	The folder "data_for_tests" contains the subfolders "blue", "red", "white".	
Concluding Remarks: The operator can open the file explorer when clicking on the button *Browser* and navigate through the directory. The subfolders "red", "blue", "white" are in the folder "data_for_tests", which acts as the Root directory.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/5/20	

4.1.6. Test T6 – test that a "Red Folder" is Selected when inserting a "Root Directory Path"

Objective: Test the existence of the Red Team Directory based on the given folder path
Notes: The estimated duration of this test is 3 minutes, after the ingestion starts and the structural check is done it's not necessary to wait until the whole directory is ingested. In order to execute this test, the following resources shall be met:
Initial Conditions:

- The user is operating an instance of SPLUNK with appropriate credentials
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 11: T6

Test No.: T6			Current Status: Pass	
Test title: Test that a "Red Folder" is Selected when inserting a "Red Directory" Path				
Testing approach: This test follows a black-box approach based on the ingestion scenario; the operator will follow a sequence of steps to trigger a structural error in the root directory.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t4_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *create event* dialog allows for user input for following attributes.	

4	Click the *Save Event* button.	Create the event to be used in this test	A text prompt below the *description* textbox will appear with the message "Event t4_event added.".	
5	Click the button *Browse* at the right side of *Root Directory*, go to the installation folder of the PICK Tool, double click on "tutorialdata", and click the button *Select Folder*.	Indicate which directory will be used in the ingestion process.	The directory paths specified are reflected in the textboxes of each directory.	
6	Click the *Start Ingestion* button.	Trigger the ingestion process which, in initial phase, does a structural check of the root directories.	The console from which the PICK Tool is running prompts the message "pick-tool-team03-we-showed-up/tutorialdata/red doesn't exist! ".	
Concluding Remarks: The PICK Tool is able to check the directory structure and stop ingestion if the folder does not contain the red folder.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/5/20	

4.1.7. Test T7 – Test that a "Blue Folder" is Selected when inserting a "Root Directory Path"

Objective: Test the existence of the Blue Team Directory based on the given folder path
Notes: The estimated duration of this test is 3 minutes, after the ingestion starts and the structural check is done it's not necessary to wait until the whole directory is ingested. In order to execute this test, the following resources shall be met:
Initial Conditions:

- The user is operating an instance of SPLUNK
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 12: T7

Test No.: T7			Current Status: Pass	
Test title: Test that a "Blue Folder" is Selected when inserting a "Blue Directory" Path				
Testing approach: This test follows a black-box approach based on the ingestion scenario; the operator will follow a sequence of steps to trigger a structural error in the root directory.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	

2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t5_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *create event* dialog allows for user input for following attributes.	
4	Click the *Save Event* button.	Create the event to be used in this test	A text prompt below the *description* textbox will appear with the message "Event t5_event added".	
5	Click the button *Browse* at the right side of *Root Directory*, go to the installation folder of the PICK Tool, double click on "tutorialdata", and click the button *Select Folder*.	Indicate which directory will be used in the ingestion process.	The directory paths specified are reflected in the textboxes of each directory.	
6	Click the *Start Ingestion* button.	Trigger the ingestion process which, in initial phase, does a structural check of the root directories.	The console from which the PICK Tool is running prompts the message "pick-tool-team03-we-showed-up/tutorialdata/blue doesn't exist! ".	
Concluding Remarks: The PICK Tool is able to check the directory structure and stop ingestion if the folder does not contain the blue folder.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/5/20	

4.1.8. Test T8 – Test that a "White Folder" is Selected when inserting a "Root Directory" Path

Objective: Test the existence of the White Team Directory given a folder path
Notes: The estimated duration of this test is 3 minutes, after the ingestion starts and the structural check is done it's not necessary to wait until the whole directory is ingested. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 13: T8

Test No.: T8	Current Status: Pass
Test title: Test that a "White Folder" is Selected when inserting a "White Directory" Path	
Testing approach: This test follows a black-box approach based on the ingestion scenario; the operator will follow a sequence of steps to trigger a structural error in the root directory.	

STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t6_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *create event* dialog allows for user input for following attributes.	
4	Click the *Save Event* button.	Create the event to be used in this test	A text prompt below the *description* textbox will appear with the message "Event t6_event added".	
5	Click the button *Browse* at the right side of *Root Directory*, go to the installation folder of the PICK Tool, double click on "tutorial data", and click the button *Select Folder*.	Indicate which directory will be used in the ingestion process.	The directory paths specified are reflected in the textboxes of each directory.	
6	Click the *Start Ingestion* button.	Trigger the ingestion process which, in initial phase, does a structural check of the root directories.	The console from which the PICK Tool is running prompts the message "pick-tool-team03-we-showed-up/tutorialdata/white doesn't exist! ".	
Concluding Remarks: Concluding Remarks: The PICK Tool is able to check the directory structure and stop ingestion if the folder does not contain the white folder.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/5/20		

4.1.9. Test T9 – Test Deleted Vector is Removed from Tables in Vector View Tab

Objective: Test tables and graph in Vector View tab are updated when a Vector is deleted in the Event View tab.
Notes: The estimated duration of this test is 2 minutes.
Initial Conditions:

- The operator is running an instance of SPLUNK
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.
- The operator has made an event

Table 14: T9

Test No.: T9			Current Status: Fail	
Test title: Test Deleted Vector is Removed from Tables in Vector View Tab				
Testing approach: The following test case will check the tables and graph in the Vector View Tab are updated upon deletion of a vector with nodes and relationships.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Select the tab *Event View* and click the button *Add* located at the right side of the table *Vector Configuration*	Create the vector on which the nodes and relationships will be added.	A vector called "Vector 1" is displayed in the table *Vector Configuration*	
2	Select the tab *Vector View* and click the button *Add* located on the right side of the Buttons *Undo* and *Redo*, twice.	Add two nodes to "Vector 1"	The nodes called "Node 1" and "Node 2" are displayed in the table at the left side, and in the graph at the right top corner.	
3	Click the button *Add Relationship* located in the right bottom corner.	Open the dialog window that allows to add a relationship between two nodes	The dialog window to add a relationship between two nodes is displayed at the center of the screen.	
4	In the *Name* textbox write "Test_1", and in the *Child ID* drop box select "Node 2". Afterwards, click the button *Create*.	Create a relationship between "Node 1" and "Node 2", where "Node 1" is the parent node, and "Node 2" is the child node	A line connecting "Node 1" and "Node 2" will be displayed in the graph located at the top right corner. The relationship called "Test_1" is displayed in the table located on the right bottom corner.	
5	Select the tab *Event View*, select the checkbox at the left side of "Vector 1", and click the button *Delete* located below the Button *Add*. Afterwards, click the button *OK* when prompted.	Delete "Vector 1"	"Vector 1" is removed from the table *Vector Configuration*	
6	Select the tab *Vector View*.	Check "Vector 1", "Node 1", "Node 2", and "Test_1" are removed from the tables and the graph	The tables at the left side and bottom right corner are empty. The graph at the right top corner is empty.	
Concluding Remarks: The tables and graph in the *Vector View* tab are still populated with the information of the deleted vector "Vector 1". However, when a new vector is added, and the test is repeated the tables and graph are updated and display the information of the new vector.				

Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo	Date Completed: 5/5/20

4.2. TS2 - Ingestion

4.2.1. Test T10 – Test SPLUNK Log file Ingestion

Objective: Test that a new index is created in SPLUNK containing the ingested log files specified in the root directory.
Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 15: T10

Test No.: T10			Current Status: Pass	
Test title: Test SPLUNK Log file Ingestion				
Testing approach: This test is based on the event creator scenario; the operator will follow a sequence of steps to create an index into SPLUNK that contains the ingested log files from a root directory specified by the operator.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t7_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *Event Name* field contains the event "t7_event", the *start date* contains the date "01/01/2000", and the *end date* contains the date "01/01/2020"	
4	Click the *Save Event* button.	Create the event to be used in this test along with the pertaining index to it.	A text prompt below the *description* textbox will appear with the message "Event t7_event added."	

5	Click the button *Browse* located at the right side of the *Root Directory* textbox.	Open the file explorer.	The file explorer is displayed at the center of the screen.	
6	Go to the installation folder of the PICK Tool, and open the folders “tutorialdata”, and “data_for_tests”. Afterwards, click the button *Select Folder.*	Save the path that contains the log files to be ingested by SPLUNK, into the *Root Directory* textbox.	The path selected in the file explorer is displayed in the *Root Directory* textbox.	
7	Click the button *Start Data Ingestion*, located below the *White Team Folder* section.	Ingest the log files in the path saved in the *Root Directory* textbox.	The log files ingested by SPLUNK will appear in the *Log File Configuration* table of the *Event View* tab with the status “Ingested”, in the *Ingestion Status* column.	Log files that were not ingested will also appear in the the *Log File Configuration* table, but their status in the *Ingestion Status* column will be displayed as “Not Ingested.”
8	Open the web browser and enter the address “http://localhost:8000”	To access the SPLUNK Web application.	The SPLUNK Web application opens.	
9	In the login credentials use “user1” and “password1” to login.	Login to the same user that created the event.	The main user area of the SPLUNK Web application is displayed.	
10	From the *settings* dropdown menu, in the data section, select *indexes*.	Access a list of the existing SPLUNK indexes.	A table of the existing indexes inside of SPLUNK is displayed, including the index *t7_event.*	
Concluding Remarks: The operator can open the Create Event Dialog window, fill-in the event fields and save the event in the PICK Tool. Additionally, the event *t7_event*, is displayed in the index table from the indexes page, as described in the expected results of step 7.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/6/20		

4.2.2. Test T11 – Test for Audio File Transcribing Ability.

Objective: Test the audio transcription function from the ingestion process.

Notes: The estimated duration of this test is 5 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The blue folder contains an audio file in WAV format.
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 16: T11

Test No.: T11			Current Status: Pass	
Test title: Test for Audio File Transcribing Ability.				
Testing approach: This test is based on the ingestion scenario by selecting a				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t8_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *Event Name* field contains the event "t8_event", the *start date* contains the date "01/01/2000", and the *end date* contains the date "01/01/2020"	
4	Click the *Save Event* button.	Create the event to be used in this test along with the pertaining index to it.	A text prompt below the *description* textbox will appear with the message "Event t8_event added."	
5	Click the button *Browse* located at the right side of the *Root Directory* textbox.	Open the file explorer.	The file explorer is displayed at the center of the screen.	
6	Go to the installation folder of the PICK Tool, and open the folders "tutorialdata", and "data_for_tests". Afterwards, click the button *Select Folder*.	Save the path that contains the log files to be ingested by SPLUNK into the *Root Directory* textbox.	The path selected in the file explorer is displayed in the *Root Directory* textbox.	

7	Click the *Start Data Ingestion* button.	Trigger the ingestion process.	The *Log File* table will be populated with the files in the path specified in the *Root Directory* textbox, which contains blue folder with the audio file “log2ex.wav”, which is transcribed to a text file called “log2ex.txt”.	
8	Select the checkbox to the right of the file named “log2ex.txt” in the *Log File* table.	Select the file to be viewed in the *Enforcement Action Report* table.	The *Enforcement Action Report* table is populated with the error “No valid timestamp”.	
9	Click the *Validate* button below the *Enforcement Action Report Table*.	Bypass the timestamp validation for the file in order to be ingested into SPLUNK.	The error in the *Enforcement Action Report* table disappears. In the *Log Entry* table the column *Ingestion Status* changes from “Not Ingested” to “Ingested” in the row of the file named “log2ex.txt”.	
Concluding Remarks: The PICK Tool transcribed the audio file “log2ex.wav” contained in the path provided in step 5, to the text file “log2ex.txt”. Since the given path contains other folders, the results of the ingested and transcribed audio file takes between 3 to 5 minutes to show in the *Log File* Table.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.2.3. Test T12 – Test for Image File Transcribing Ability.

Objective: Test the optical character recognition function from the ingestion process.
Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The red directory contains an image file in JPEG format.
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 17: T12

Test No.: T12	Current Status: Pass
Test title: Test Addition of New Event into SPLUNK	
Testing approach: This test is based on the event creator scenario; the operator will follow a sequence of steps to create an index into SPLUNK.	

STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t9_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *Event Name* field contains the event "t9_event", the *start date* contains the date "01/01/2000", and the *end date* contains the date "01/01/2020"	
4	Click the *Save Event* button.	Create the event to be used in this test along with the pertaining index to it.	A text prompt below the *description* textbox will appear with the message "Event t9_event added."	
5	Click the button *Browse* located at the right side of the *Root Directory* textbox.	Open the file explorer.	The file explorer is displayed at the center of the screen.	
6	Go to the installation folder of the PICK Tool, and open the folders "tutorialdata", and "data_for_tests". Afterwards, click the button *Select Folder*.	Save the path that contains the log files to be ingested by SPLUNK into the *Root Directory* textbox.	The path selected in the file explorer is displayed in the *Root Directory* textbox.	
7	Click the *Start Ingestion* button.	Trigger the ingestion process.	The *Log File* table will be populated with the files in the path specified in the *Root Directory* textbox, which contains the red folder with the image file "MI_logs.png", which is transcribed to the text file "MI_logs.txt".	
8	Select the checkbox to the right of the file name "MI_logs.txt", in the *Log File* table.	Select the file to be viewed in the *Enforcement Action Report* table.	The *Enforcement Action Report* table is populated with the error "No valid timestamp".	

19	Click the *Validate* button.	Bypass the timestamp validation for the file in order to be ingested into SPLUNK.	The error in the *Enforcement Action Report* table disappears. In the *Log Entry* table the column *Ingestion Status* changes from "Not Ingested" to "Ingested" in the row of the file "MI_logs.txt".	
Concluding Remarks: The PICK Tool transcribed the image file "MI_logs.png" contained in the path provided in step 5, to the text file "MI_logs.txt". Since the given path contains other folders, the results of the ingested and transcribed image file takes between 3 to 5 minutes to show in the *Log File* Table.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.2.4. Test T13 – Cleansing Non-Alphabetical and Non-Punctuation Characters.

Objective: Test the cleansing function from the ingestion process.
Notes: The estimated duration of this test is 5 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The white directory contains a text file with non-printable characters.
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.

Table 18: T13

Test No.: T13			Current Status: Pass	
Test title: Test Addition of New Event into SPLUNK				
Testing approach: This test is based on the event creator scenario; the operator will follow a sequence of steps to create an index into SPLUNK.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Click the *File* dropdown in the top left corner of the main window.	Access the menu that gives the options to create, open or edit an event.	A dropdown menu is displayed containing "New", "Open", "Edit" and "Exit" options.	
2	Click the *New* option from the dropdown menu.	Open the pop-up that will enable the user to create a new event.	The *create event* dialog is displayed.	
3	Under the *Event Name* field type "t10_event", on the *start date* select "01/01/2000" and in *end date* select "01/01/2020"	Set up the event name, start date and end date to be used in this test	The *Event Name* field contains the event "t10_event", the *start date* contains the date "01/01/2000", and the *end date* contains the date "01/01/2020"	

4	Click the *Save Event* button.	Create the event to be used in this test along with the pertaining index to it.	A text prompt below the *description* textbox will appear with the message "Event t10_event added."	
5	Click the button *Browse* located at the right side of the *Root Directory* textbox.	Open the file explorer.	The file explorer is displayed at the center of the screen.	
6	Go to the installation folder of the PICK Tool, and open the folders "tutorialdata", and "data_for_tests". Afterwards, click the button *Select Folder.*	Save the path that contains the log files to be ingested by SPLUNK into the *Root Directory* textbox.	The path selected in the file explorer is displayed in the *Root Directory* textbox.	
7	Click the *Start Ingestion* button.	Trigger the ingestion process, which in its initial phase, will trigger the cleansing.	The *Log File* table will be populated containing the file and the *Log Entry Configuration* table will be populated with the pertaining entries of the text file.	
8	Click the *Log Entry View* tab.	This view will allow the observation of the pertaining log entries ingested into the event's index.	The *Log File* table will be populated with the files in the path specified in the *Root Directory* textbox, which contains the white folder with the text file "secure.txt", which is cleansed from non-printable characters.	
Concluding Remarks: The files from the path provided in step 5 containing non-alphabetical and non-punctuation characters are cleansed and displayed in the "Log Entry Event" column of the *Log Entry Configuration* table in the *Log Entry View* tab.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.2.5. Test T14 – Test to validate timestamps within a certain range.

Objective: Test to validate timestamps within a certain range.
Notes: This test focuses on the ability to extract the timestamps from each line in a log file and compare it to the start and end date specified in the event configuration. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool.
- 3 log files should be in the root directory:
    1. A file with a pre-range timestamp.
    3. A file with a post-range timestamp.
    2. A file with valid time ranges.

Table 19: T14

Test No.: T14			Current Status: Pass	
Test title: Test to validate timestamps within a certain range				
Testing approach: The following will be testing the validation's time range validation portion in the ingestion process. **Initial State:** Test case T5 should be followed.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Beginning at the Initial State described above, user selects the "Start Ingestion"	Start the ingestion process and update the Log File Configuration (LFC) table.	The PICK Tool processes the log files to be ingested and shows the status of the log files in the LFC table.	This might take a while depending on the size of the ingested files.
2	The user waits for the files to be processed until the LFC is updated.	Check the LFC shows the validity of the log files.	The LFC shows the validity of each log file depending on the time ranges in the file.	
Concluding Remarks: The time range of the ingested log files is assessed by the LFC and the validity status of the files is shown in the *Validity* column of the LFC table.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.3. TS3 - Graphing

4.3.1. Test T15 Creating a vector

Description: This initial condition encompasses opening an event inside the PICK Tool, the field vector_name will be defined

Objective: Creating a vector

Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

Table 20: T15

Test No.: T15	Current Status: Pass
Test Title: Creating a Vector	
Testing approach: The following will be testing the ability to create a vector.	

STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	In the *Event* (Appendix 4) tab, at the right of the *Vector Configuration* table, click the "add" button	Create a new vector	A new vector pops up on the vector configuration table	The vector will have a default name labeled as "vectorN" where N represent the number of the vector
2	Double click on the name of the vector to change the vector name to "v1"	Change the name of the vector from the default name to "v1"	The name of the vector is updated to "v1" once the user clicks away	
3	Double click on the V*ector Description* field and write the description "Vector Test 1"	Give the vector the description "Vector Test 1"	The description of the vector is updated to "Vector Test 1" once the user clicks away	
Concluding Remarks: The vector can be created in the table *Vector Configuration*, which is set to "vector N" by default as described in the comments from step 1. Additionally, the name and description are updated as described in the expected results from steps 2 and 3.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.3.2. Test T16 – Test adding a new node to the graph not connected to a log entry

Objective: Test adding a new node to the graph not connected to a log entry
Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The PICK Tool installation folder contains the directory tutorialdata/data_for_tests, and the folder data_for_tests contains the red, blue, and white subfolders.
- The white directory contains a text file with non-printable characters.
- Log entries exist in the log entry table
- At least one vector has been created (4.3.1)

Table 21: T16

Test No.: T16			Current Status: Pass	
Test title: Test adding a new node to the graph not connected to a log entry				
Testing approach: This test is based on the graphing scenario; the operator will follow a sequence of steps to edit the graph.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS

1	In the drop-down menu at the top of the vector view (Appendix 6) select the name of the vector you with to add the log entry to	Make sure all vectors are shown in the drop-down menu	There selected log entries should now be in the selected vector	The checkbox will still be selected and need to be unselected manually
2	Click the button labeled “add” two buttons to the right of the drop-down menu	Create a new node in the table and graph	A new row should be added to the node table and the graph	The row should be empty
Concluding Remarks: The test can be performed successfully, however the node can be created in a place where it is hidden so it must be manually moved by the user				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.3.3. Test T17 – Test adding a new node to the graph that is connected to a log entry

Objective: Test adding a new node to the graph that is connected to a log entry.
Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The PICK Tool installation folder contains the directory tutorialdata/data_for_tests, and the folder data_for_tests contains the red, blue, and white subfolders.
- The white directory contains a text file with non-printable characters.
- Log entries exist in the log entry table
- At least one vector has been created (4.3.1)

Table 22: T17

Test No.: T17			Current Status: Pass	
Test title: Test adding a new node to the graph that is connected to a log entry				
Testing approach: This test is based on the graphing scenario; the operator will follow a sequence of steps to edit the graph.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Select the log entry/entries from the log entry view (Appendix 6) table that will be added to the graph by selecting the check box next to the log entry name	Check that the selection of log entries is working correctly	The checkbox should now be checked	

2	In the “add nodes to vector” table, select the name of the vector you wish to add the log entry to, then click the button labeled “add to vector”	Add the selected log entry to a specific vector	There selected log entries should now be in the selected vector	The checkbox will still be selected and need to be unselected manually
3	Select the vector where the log entries were added in the vector view (Appendix 6) tab	Check that the table and the graph are updating correctly	The nodes should be showing in the graph image	
Concluding Remarks: The test can be performed successfully with a single log entry or multiple log entries, as well as to one or multiple vectors				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.3.4. Test T18 – Test connecting two nodes with a relationship

Objective: Test connecting two nodes with a relationship
Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The PICK Tool installation folder contains the directory tutorialdata/data_for_tests, and the folder data_for_tests contains the red, blue, and white subfolders.
- The white directory contains a text file with non-printable characters.
- Log entries exist in the log entry table
- At least one vector has been created (4.3.1)
- At least 2 log entries have been added to the selected vector

Table 23: T18

Test No.: T18		Current Status: Pass		
Test title: Test connecting two nodes with a relationship				
Testing approach: This test is based on the graphing scenario; the operator will follow a sequence of steps to edit the graph.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Select the vector to be edited in the drop down at the top of the vector view (Appendix 6) tab	Check that the vector can be selected	The log entries associated with that vector should show on the graph and table	
2	In the relationship section/table under the graph click the “add relationship” button	Initialize addition of relationship that will be used to connect the nodes.	A new row should appear on the table	The row will be empty

3	In the pop up, select the child and parent columns	Select which nodes the line will be represented on	A line should appear between the graphical representation of the 2 nodes after ok is clicked	
Concluding Remarks: The test can be performed successfully, nodes do not move when connected, so if line is in the way it must be moved manually.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/6/20		

4.3.5. Test T19 – Test adding information to an existing node

Objective: Test adding information to an existing node
Notes: The estimated duration of this test is 3 minutes. In order to execute this test, the following resources shall be met:

- The operator is running an instance of SPLUNK
- The PICK Tool installation folder contains the directory tutorialdata/data_for_tests, and the folder data_for_tests contains the red, blue, and white subfolders.
- The white directory contains a text file with non-printable characters.
- Log entries exist in the log entry table
- At least one vector has been created (4.3.1)
- At least 2 log entries have been added to the selected vector

Table 24: T19

Test No.: T19			Current Status: Fail	
Test title: Test adding information to an existing node				
Testing approach: This test is based on the graphing scenario; the operator will follow a sequence of steps to edit the graph.				
STEP 1	OPERATOR ACTION Select the vector to be edited in the drop down at the top of the vector view (Appendix 6) tab	PURPOSE Check that the vector can be selected	EXEPCTED RESULTS The log entries associated with that vector should show on the graph and table	COMMENTS
2	In the relationship section/table edit a field for a node row that you would like to edit	Change node information	Changes should be saved	
Concluding Remarks: Information like name, creator, and visibility can be changed in the node table and will change in the graph as well, all other fields can be edited in the table but will not be shown on the graph.				

Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo	Date Completed: 5/6/20

4.4. TS4 - Network

4.4.1. Test T20 – Test analyst restrictions on events

Objective: Trigger a prompt informing the analyst events can only be created by the lead.
Notes: The estimated duration of this test is 3 minutes. For this test it is not necessary to run an instance of SPLUNK since the operator is an analyst and not the lead.
Initial Conditions:

- The operator is running the PICK Tool

Table 25: T20

Test No.: T20			Current Status: Fail	
Test title: Test analyst restrictions on events.				
Testing approach: Testing will be conducted in the PICK Tool				
STEP 1	OPERATOR ACTION Click on the *File* tab in the left-upper corner and select the option *New*.	PURPOSE Open the Event Configuration window.	EXEPCTED RESULTS A window with the title "Dialog" pops up at the center of the screen.	COMMENTS
2	Write "t11_event" in the textbox below the label *Event Name.*	Write the name of the event to be created.	The letters "t11_event" are displayed in the textbox below the label *Event Name.*	
3	Click once on the upward arrow in the date spin box under the label *Event End Timestamp.*	Change the date for the end of the event.	The month in the date spin box under the label *Event End Timestamp* is highlighted in blue and changes from "1" to "2."	

4	Write "Test analyst restrictions" in the text box under the label *Description.*	Write the description of the event	The message "Test analyst restrictions" is displayed in the textbox under the label *Description*.	
5	Click on the button named *Save Event* under the *Description* textbox.	Trigger a prompt telling the analyst only the lead can create events	A prompt is displayed informing the analyst only the lead can create and save events. The prompt will contain a button that, when clicked will close the Event Configuration Window.	
Concluding Remarks: This test fails due to permissions given to the user outside the PICK Tool environment.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/6/20		

4.4.2. Test T21 – Test connection from analyst to lead

Objective: Connect analyst to Lead database.
Notes: The estimated duration of this test is 3 minutes. For this test it is not necessary to run an instance of SPLUNK since the operator is an analyst and not the lead.
Initial Conditions:

- The operator is running the PICK Tool

Table 26: T21

Test No.: T21		Current Status: Fail		
Test title: Test connection from analyst to lead database				
Testing approach: Testing will be conducted through the PICK Tool.				
STEP 1	OPERATOR ACTION Click on the *Event* tab in the left-upper corner.	PURPOSE Open the tab where a connection to the Lead database can be established	EXEPCTED RESULTS The contents of the *Event* tab are displayed.	COMMENTS

2	Click on the textbox at the right side of the label *Lead IP Address***,** and type the IP address of the Lead's database	Specify the IP address on which the connection will be established	The written IP address is displayed in the textbox at the right side of the label *Lead IP Address*.	
3	Click on the button named *Connect* at the right side of the *Lead IP Address* textbox.	Establish a connection to the Lead's database	The label *No. of established connections to the lead's IP address* below the label *Lead IP Address*, now displays the number "1" instead of "0"	
Concluding Remarks: The connection to the Lead IP cannot be established.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/9/2020		

4.4.3. Test T22 – Test connection error to Lead when IP is not specified

Objective: Trigger a prompt informing the analyst connection cannot be established due to Lead Ip not being specified.
Notes: The estimated duration of this test is 3 minutes. For this test it is not necessary to run an instance of SPLUNK since the operator is an analyst and not the lead.
Initial Conditions:

- The operator is running the PICK Tool

Table 27: T22

Test No.: T22		Current Status: Pass		
Test title: Test connection error to Lead database when IP is not specified.				
Testing approach: Testing will be conducted through the PICK Tool.				
STEP 1	OPERATOR ACTION Click on the *Event* tab in the left-upper corner.	PURPOSE Open the tab where a connection to the Lead database can be established	EXEPCTED RESULTS The contents of the *Event* tab are displayed.	COMMENTS

2	Click on the button named *Connect* at the right side of the *Lead IP Address* textbox.	Trigger a prompt informing the user the Lead IP was not specified	A prompt is displayed informing the analyst the Lead IP address was not specified. The prompt is closed when the button named *Close* below the message is clicked.	End of test
Concluding Remarks: The prompt is displayed when a connection to the Lead IP is made and the IP Is not specified.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo			Date Completed: 5/6/20	

4.4.4 Test T23 – Test server closure after Lead closes connection

Objective: Close server after lead closes connection.
Notes: The estimated duration of this test is 5 minutes.
Initial Conditions:

- The operator is using Kali Linux and has the console open
- The operator is running the PICK Tool
- The user is operating an instance of SPLUNK
- Completed all steps in test case T1 in Section 4.1.1

Table 28: T23

Test No.: T25			Current Status: Pass	
Test title: Test server closure after Lead closes connection				
Testing approach: Testing will be conducted through the PICK Tool and the console.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Outside the PICK Tool, open the console and look for the port status.	Check the port for the connection to the lead is open.	The console displays the port for the connection to the lead as open.	

1	Go back to the PICK Tool and click on the check box at the left side of the label **Lead**.	Close the connection as Lead.	The check box at the left side of the label **Lead** is unchecked.	
2	Outside the PICK tool, go back to the console and look for the current port status.	Check the port for the connection to the lead is closed.	The console displays the port for the connection to the lead as closed.	End of test
Concluding Remarks: The server is closed upon exit from application.				
Testing Team: Daniela, Diego, Jessica, Matthew, Ricardo		Date Completed: 5/6/20		

4.5. TS5 – Database

4.5.1. Test T24 – Retrieving Event Data from the Database

Objective: Test the persistence of data from a specific event.
Notes: The duration of this test is approximately 10 minutes.
Initial Conditions:

- The user is operating an instance of SPLUNK
- The user has its own SPLUNK local credentials
- The operator has been checked as lead analyst and has logged into SPLUNK from the PICK Tool

Table 29: T24

Test No.: T24		Current Status: Pass		
Test title: Retrieving Event Data from the Database				
Testing approach: This test consists in adding a new event with vector information inside it, closing the application and opening it again in order to test persistence.				
STEP	OPERATOR ACTION	PURPOSE	EXEPCTED RESULTS	COMMENTS
1	Follow steps 1-5 of T2 and to create a new event.	To create the new event to input the information to be tested.	The event has been created; the *New Event* window shall display "Event t1_event was created."	In step 3 of T2, write "t12_event" in the *Event Name* textbox.

2	Click the button *Browse* located at the right side of the *Root Directory* textbox.	Open the file explorer.	The file explorer is displayed at the center of the screen.	
3	Go to the installation folder of the PICK Tool, and open the folders “tutorialdata”, and “data_for_tests”. Afterwards, click the button *Select Folder.*	Save the path that contains the log files to be ingested by SPLUNK into the *Root Directory* textbox.	The path selected in the file explorer is displayed in the *Root Directory* textbox.	
4	Click the *Start Ingestion* button and close the *New Event* window.	Start the ingestion of the files in the directory.	The *Log File* and *Log Entry* tables are populated (see appendixes 4 and 5 for reference).	
5	In the *Event* tab, click the *Add Vector* button (see appendix 4 for reference).	To create a vector in which nodes will be added to test functionality.	A new entry in the *Vector Configuration* table is created with the name “Vector 1”.	
6	Go to the *Vector View* tab (see appendix 6) and click the *Add Node* button twice.	Create two nodes that will be used to test persistence in the nodes of a vector and serve to create a relationship.	Two entries will appear in the *Node* table with the names “Node 1” and “Node 2” respectively (see appendix 6 for reference of the table).	
7	Click the *Add Relationship* button and fill the name as “rel 01”, form the dropdown menus select: - *Parent:* “Node 1” - *Child:* “Node 2” and click *OK*.	Create a relationship to test for persistence of that data type.	A new entry will appear in the *Relationships* table with the name “rel 01”.	
8	Close the PICK Tool application by pressing the *X* button in the top right corner.	To stop the current instance.	The main window of the application disappears.	

9	Open the PICK Tool application again.	Run a new instance of the application.	The main window of the PICK Tool appears.	
10	In the *Team Configuration* section from the *Event* tab, click the *Lead* checkbox.	Signal the operator as the lead of the event and the one in charge of the initial ingestion and creation of the event.	A pop-up asking for the login credentials for SPLUNK is displayed.	
11	Enter your SPLUNK local credentials,	Log in the SPLUNK service.	A text prompt "Successful connection to SPLUNK from user t3testuser" is displayed.	
12	In the *File* menu at the top left corner of the application select *Open Event.*	Open a window to recall the session of the previous event.	The *Open Event* dialog is displayed (see appendix 9)	
13	In the *Event Name* dropdown select "ts1_event" and click the *OK* button at the bottom right of the dialog.	Open the previously initialized event.	The *Log File*, *Vector Configuration*, *Nodes*, *Relationships* and *Log Entries* tables are populated with the previously stored information.	
Concluding Remarks: The test evaluates the creation of events, the ingestion process, the creation of new vectors and the addition of log entries into the vector as nodes, the creation of relationships between nodes, and MongoDB operations to retrieve stored event information from the database. All previously mentioned features are functional; however, the tables and graph in the tab *Vector View* requires the addition of an empty node, and a relationship to refresh the tables and the graph.				
Testing Team: Ricardo, Diego		Date Completed: 5/7/20		

5. UI Testing

This section is merged with Section 4.

6. Test Schedule

Task and date	People	Description
TS1 - Event **TS2 - Ingestion** 05/01/2020	Ricardo Alvarez, Diego Rincon	Perform all test cases in the Event Test Suite (Table 1, Section 3) to ensure the operations needed to create events meet functional requirements. Perform all test cases in the Ingestion Test Suite (Table 2, Section 3) to ensure the ingestion process is functional and meets requirements.
TS3 - Graph 05/06/2020	Daniela Garcia	Perform all test cases in Graph Test Suite (Table 3, Section 3) the operations needed to create and edit the graph meet functional requirements.
TS4 - Network 05/03/2020	Jessica Redekop, Matthew Iglesias	Perform all test cases in Connection to Lead Analyst Test Suite (Table 5, Section 3) to ensure the operations needed to allow the analyst to connect to the lead are functional and meet requirements.

7. Other Sections

This section lists the additional requirements to successfully conduct a test plan and the use of the project's minimum hardware requirements and installations. We focus towards hardware and software requirements, which in regard is important to ensure the clients are aware of the program's impact to their computer.

7.1. Environmental Requirements

This section describes and labels the design of the environment control system in a hardware aspect to ensure that each system component can operate reliably. The PICK tool requires a minimum amount of requirements to ensure the usage and handling of the program on a sufficient computer.

- Minimum 4 GB RAM for 32-bit (x86) or 8 GB for 64-bit (x64)
- 1 GHz processor or faster for 32-bit (x86) or 64-bit (x64)
- Minimum 16 GB of hard disk drive space for 32-bit (x86) or 20 GB for 64-bit (x64)

These hardware specifications were used to test the program under VMware (virtual machine), to better conduct a controlled environment and understand the program's requirements for running effectively.

7.2. Software Requirements

This section describes the software tools and platforms needed for successful installation and complete use of the PICK tool. For more information on how to successfully install all required software, checkout the README file located on the program's GitHub. Below, are the necessary libraries and tools required for the program to run:

Table 6.2: Software Requirements

Purpose	Tool	Name	Version	Command
General Downloads	APT	PyQT5		
	APT	QTDesigner		>sudo apt-get install qttools5-dev-tools
SPLUNK	website	SPLUNK	8.0.3	Follow instructions on website
	website	splunk-sdk-python	1.6.12	Follow instructions on github
Database		MongoDB		
	pip	PyMongo		>pip install pymongo
	pip	PyMongo(server)		>pip install pymongo[srv]
Graph	pip	QGraphViz	0.0.45	>pip install QGraphViz
Audio Transcriber	pip	Speech Recognition	3.8.1	>pip install SpeechRecognition
	pip	PocketSphinx	0.1.17	>pip install pocketsphinx
	APT	LibraSound2	1.2.2-2.1	>sudo apt-get install libasound2
OCR Feeder	pip	PyTesseract	0.3.4	>pip install pytesseract
	pip	Pillow		>pip install pillow

7.2.1. Start SPLUNK Service

Description: This initial condition encompasses to initializing the SPLUNK service that will run before the application is started.

Table 1. Start SPLUNK Service

Initial Condition Title: Start SPLUNK Service				
STEP 1	OPERATOR ACTION From the command line access the path *~/splunk/bin*	PURPOSE To access the directory where the SPLUNK binaries are located	EXEPCTED RESULTS The path of the console is updated to "~/splunk/bin"	COMMENTS To ensure that the operator is in the path they can type the command "ls" to display all the files of the directory.
2	In the command line, type "./splunk start"	Initialize the SPLUNK service in the machine being used.	After approximately 7 seconds, a text prompt will be displayed confirming the successful initialization of the SPLUNK (see appendix 1).	

7.2.2. Start MongoDB Service

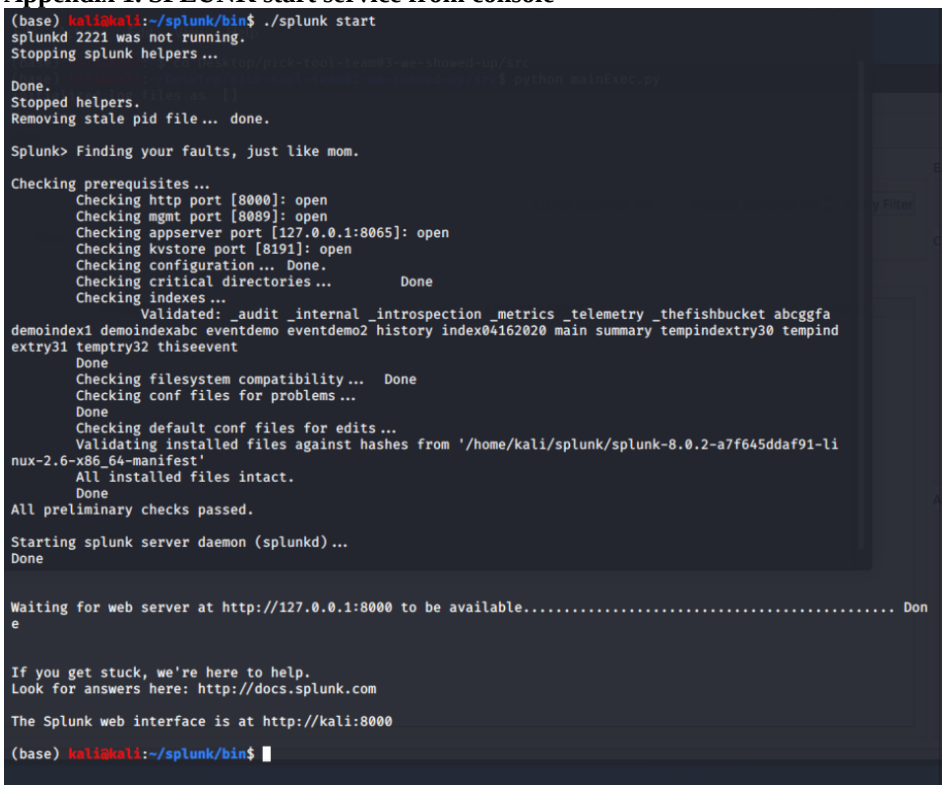
Description: This initial condition encompasses to initializing the SPLUNK service that will run before the application is started.

Table 1. Start SPLUNK Service

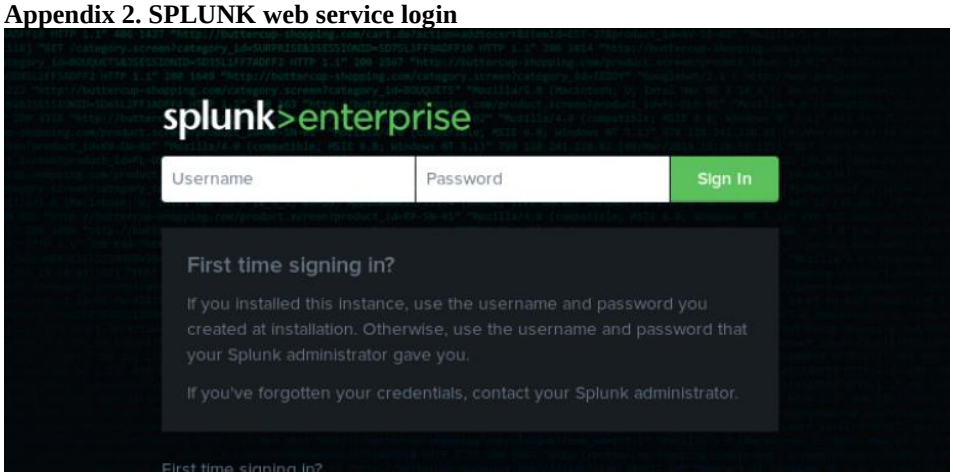
STEP 1	OPERATOR ACTION From the command line access the path *~/splunk/bin*	PURPOSE To access the directory where the SPLUNK binaries are located	EXEPCTED RESULTS The path of the console is updated to "~/splunk/bin"	COMMENTS To ensure that the operator is in the path they can type the command "ls" to display all the files of the directory.
2	In the command line, type "./splunk start"	Initialize the SPLUNK service in the machine being used.	After approximately 7 seconds, a text prompt will be displayed confirming the successful initialization of the SPLUNK (see appendix 1).	

8. Appendix

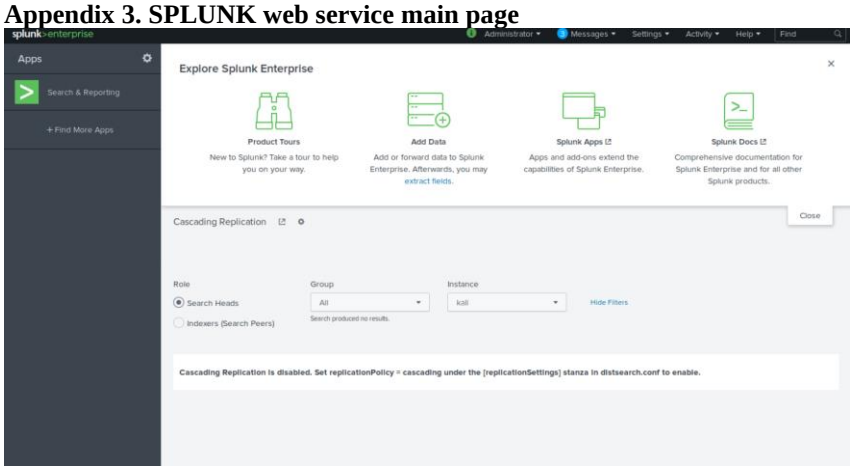
Appendix 1. SPLUNK start service from console



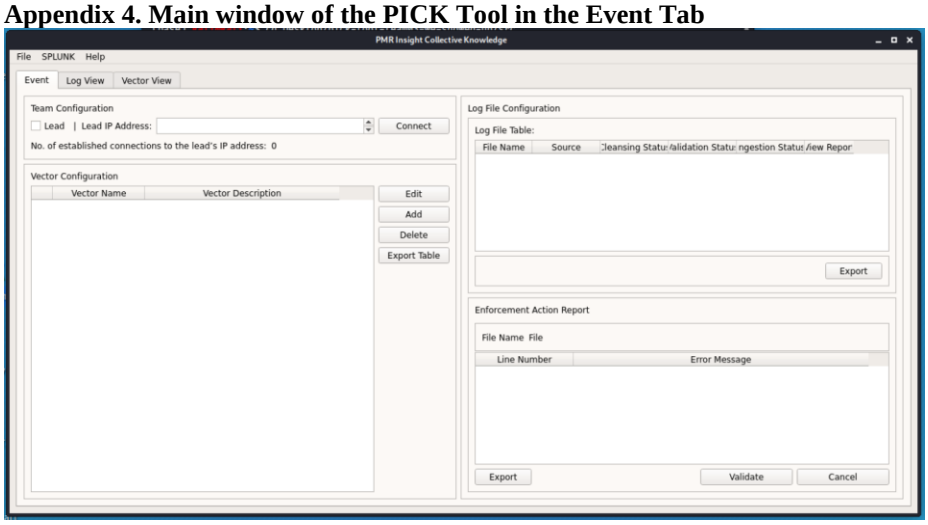
Appendix 2. SPLUNK web service login



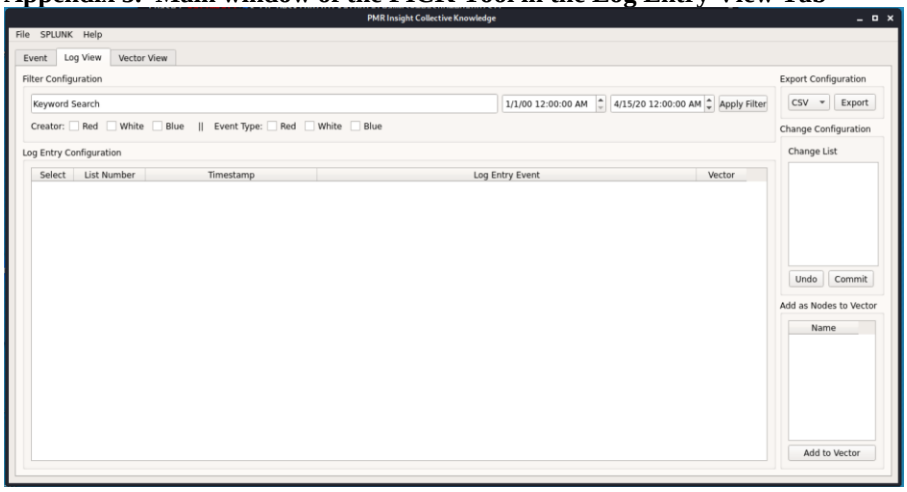
Appendix 3. SPLUNK web service main page



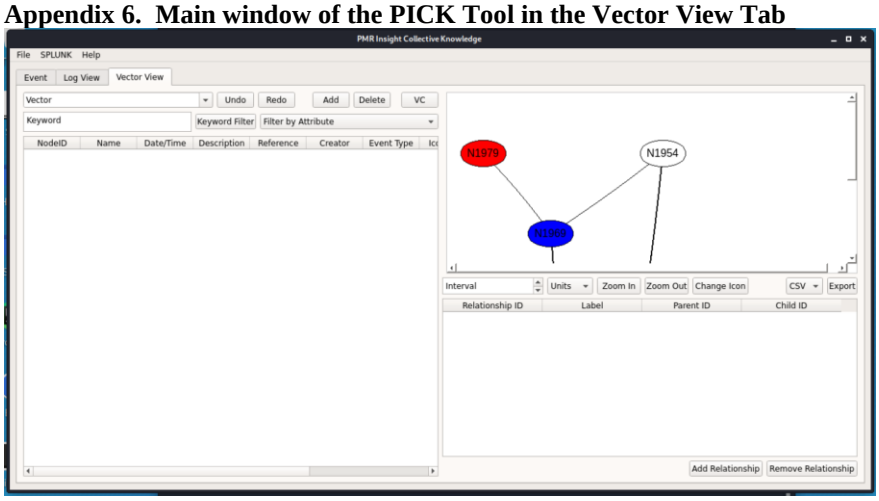
Appendix 4. Main window of the PICK Tool in the Event Tab



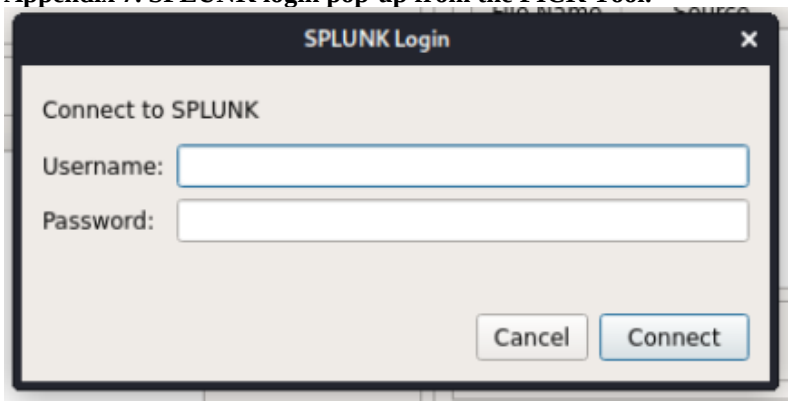
Appendix 5. Main window of the PICK Tool in the Log Entry View Tab



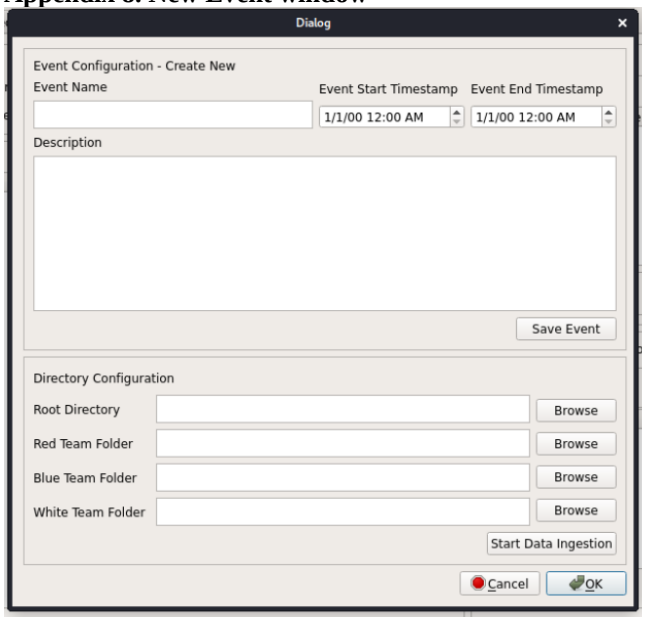
Appendix 6. Main window of the PICK Tool in the Vector View Tab



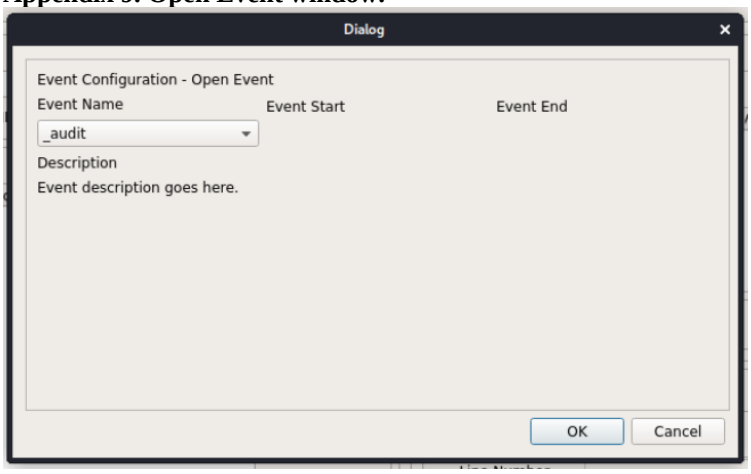
Appendix 7. SPLUNK login pop-up from the PICK Tool.



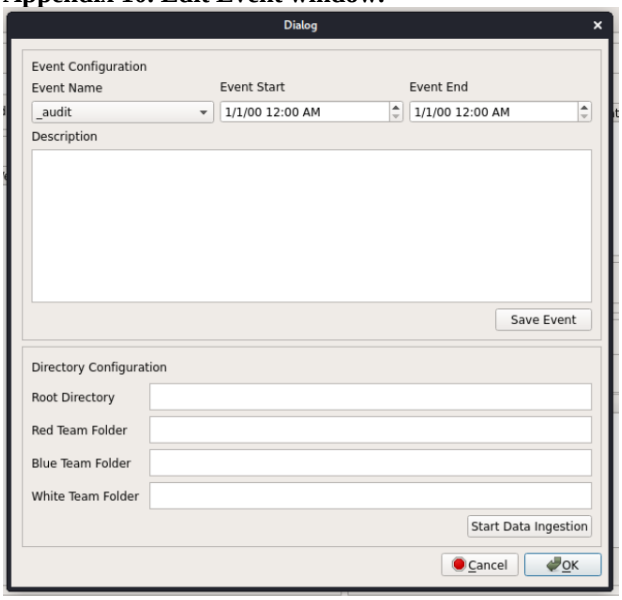
Appendix 8. New Event window



Appendix 9. Open Event window.



Appendix 10. Edit Event window.



Appendix 11. Add Relationship pop-up