Forensic-Ready Logger (FRL) Installation Manual

1. Configure the Forensic-Ready Logger Database

Please, follow these steps to configure and install the Forensic-Ready Logger database:

1.1.- Download from the **PhD_Thesis GitHub** repository in the **PhD_Thesis Software/Databases/FRL** location the **ForensicReadyLogger_Database_Dump.sql** file

1.2.- Install the **MySQL community server software version 8.0.21.**
Please select the version that fits the operating system you have installed on your computer. This software will install MySQL database on your computer to run the Forensic-Ready Logger database.

You can download this software from the following link:
https://downloads.mysql.com/archives/community/

1.3.- Please, follow the instructions on the screen to install this software.

1.4.- Once this software has been installed, install the **MySQL Workbench software version 8.0.21**.
Please select the version that fits the operating system you have installed on your computer. This software will install MySQL client on your computer to run queries related to the Forensic-Ready Logger database.

You can download this software from the following link:
https://downloads.mysql.com/archives/workbench/

1.5.- Once the MySQL Workbench software has been installed on your computer, open it and import the Forensic-Ready Logger (FRL) database. To do this, select from the Menu this option: Server>Data Import>Import from Self-Contained File

1.6.- Later, select the location in your computer where is located the database file: **ForensicReadyLogger_Database_Dump.sql**

1.7.- Once the forensic-ready logger database has been imported, this database contains 44 tables and 3 stored procedures.

1.8 Make sure to start the MySQL server and to have the Forensic-Ready Logger database up and running before executing the FRL software in the Eclipse IDE.

Please select the instructions that fit the operating system you have installed on your computer.
You can find the instructions from the following link:
https://phoenixnap.com/kb/start-mysql-server

2. Configure the Forensic-Ready Logger Software

Now, please follow these steps to configure and install the Forensic-Ready Logger software:

2.1.- Install in your computer the **Java SE Development Kit version 18.0.2.1.**
Please select the version that fits the operating system you have installed on your computer. This software will install the Java programming language and frameworks in your computer to run the Forensic-Ready Logger software.

You can download this software from the following link:
https://www.oracle.com/java/technologies/javase/jdk18-archive-downloads.html

2.2.- Once Java has been installed on your computer, you must install the most recent version of Eclipse **IDE for Java Developers.**
Please select the version that fits the operating system you have installed on your computer. This software will install the Eclipse IDE on your computer to open the Forensic-Ready Logger Java project.

You can download this software from the following link:
https://www.eclipse.org/downloads/packages/release/2024-06/r/eclipse-ide-java-developers

2.3.- After this, locate in the **PhD_Thesis GitHub** repository the **PhD_Thesis Software/Systems** path and download the **ForensicReadyLoggerGUI** folder.

2.4.- Copy into the eclipse-workspace directory located in your computer, the **ForensicReadyLoggerGUI** folder.
For example: /Users/f7/eclipse-workspace/**ForensicReadyLoggerGUI**

2.5.- Inside the Eclipse IDE, import the existing Java Project by selecting this option: File>Import>General>Projects from Folder or Archive and select the **ForensicReadyLoggerGU** folder located in the eclipse-workspace directory.

2.6.- Make sure you have installed the libraries that are called inside the forensic-ready logger. To this locate in the **ForensicReadyLoggerGUI** Java Project right click and select the option Build Path and then Configure Path.

Make sure you have installed and configured the following external JAR libraries in the **/ForensicReadyLoggerGUI/lib/ path:**

- commons-io-2.8.0.jar
- commons-lang3-3.11.jar
- mysql-connector-java-8.0.21.jar
- plantuml-1.2021.16.jar

2.7 In case, you don't have one or any of these Java libraries installed, you can download them from the **PhD_Thesis GitHub** repository in the **PhD_Thesis Software/** location in the **Libraries/FRL** folder.

3. Run the Forensic-Ready Logger Software System

3.1.- To execute the FRL, Open In the Eclipse IDE locate the **ForensicReadyLoggerGUI** Java project, find the **src/frl.gui.main folder** and then locate the **ForensicReadyLoggerGui.java** file.

3.2.- This **ForensicReadyLoggerGui.java**.java file contains the main procedure. To execute it, right-click and select the option: run as Java Application.

3.3.- This **ForensicReadyLoggerGui.java** program displays the login screen which asks for a user and a password. You can use the main user:
User: admin
Password: 12345

3.4.- Then, the forensic-ready logger tool will display the main menu which includes the following options:

1. **Configuration:** helps to make the setup of the users to be used in the forensic-ready logger and also to make the setup of the aspect files structure.
2. **Generate AOP Files:** receives as the input the information from the software system and generates as the output the initial aspect file to be used in the software system and generates the incident model.
3. **Annotate UML Sequence Diagram:** receives as the input the incident model generated in the software system and allows the security engineer to add annotations related to what to log, where to log and when to log to identify a particular security incident of interest. It generates as the output the annotated incident model and it stores its information internally.
4. **Generate Logging Instructions:** receives as the input the annotated incident model information stored internally. It generates as the output the final aspect file to inject the logging instructions into the software system.

3.5.- The first button **configuration** is to allow the users to connect to the forensic-ready logger tool and also to create and specify the structure of the aspect files. We already have done this. So, you should skip this step unless you want to create new users or add new aspect files to be used inside the forensic-ready logger tool.

3.6.- The second button **Generate AOP Files** is related to the first stage: Incident Modelling, to generate the aspect file to generate the incident model. You should start using the forensic ready logger tool using this option. After you click this button, a screen named: "**Generate the Aspect Oriented Programming Files**" and two software systems are displayed in a list. You should select the software system you want to generate the aspect files and the incident model (e.g., OH) and then right-click and select the option **Modify**.
Note: There is a button called "**Add New**". You should select this option in case you want to add a new software system in the Forensic-Ready Logger tool.
Once you have selected the Modify option, review all four different tabs to verify the information is correct according to your computer and your operating system.

3.7.- After you have performed the first stage in the forensic-ready logger tool, the second step is to click on the button: **Annotate UML Sequence Diagram.** This relates to the second stage which helps to annotate the incident model to identify a security incident of interest. After you click this button, a screen name: "**Load the Incident Model**" and two software systems are displayed in a list. You should select the software system you want to annotate the incident model (e.g., OH) and then right-click and select the option **Modify**.
Note: There is a button called "**Add New**". You should select this option in case you want to add a new software system in the Forensic-Ready Logger tool.
Once you have selected the Modify option, you should provide the input the incident model files and click on the button Generate to present the incident model on the screen.

3.8.- Once you have performed stages 1 and 2, you should click the last button: **Generate Logging Instructions.** This is the last stage in the forensic-ready logger and it generates the aspect file to inject logging instructions into the software system.
After you click this button, a screen name: "Generate the Logging Instructions" and two software systems are displayed in a list. You should select the software system you want to annotate the incident model (e.g., OH) and then right-click and select the option **Modify**.
Note: There is a button called "**Add New**". You should select this option in case you want to add a new software system in the Forensic-Ready Logger tool.
Once you have selected the Modify option, review all four different tabs to verify the information is correct according to your computer and your operating system.