



Audit Software SIG – Security Auditing with IDEA Hands-on Exercise Instructions

Definitions:

- A **Field** is a column of data.
- A **Record** is a row of data.
- A **Working Folder** is the Windows file folder where IDEA will save your IDEA files (.IMD).
- **IDEA File Explorer** located on the left side of the display is a view of the files inside the Working Folder.
- **IDEA Properties Window** (“Properties”) located on the right side of the display controls ways to view the data in the middle of the display.

NOTE: Use all program defaults unless instructed to make a change. Type all functions exactly as they are shown.

Set the Working Folder:

- Select **File**.
- Select **Set Working Folder**.
- Navigate to **C:\Program Files\IDEA\Tutorial\Ghost in the Machine** and select it.
- Click **Open**. The Project Properties window will appear.
- Enter ISACA Dallas in the Project Name and today’s date for the Period.
- Click **OK**.

Open an IDEA File:

- Find **Users-Database** in the IDEA File Explorer window.
- Double-click on the blue icon next to the file name to open the file.
- The file will open in the data view in the center of the display.



Duplicate Detection

Use IDEA's **Duplicate Detection** function to isolate duplicate values based on data from a single field or based on a combination of data from up to eight fields. Examples of duplicate values could be users with more than one user ID, duplicate printer names, or duplicate row identifiers

Detect duplicates:

- Click **Analysis**.
- Click **Duplicate Key**.
- Click **Exclusion**. The **Duplicate Key Exclusion** dialog box displays.
- Under "Fields to match", check **FULLNAME**.
- Under "Fields that must be different", check **USERNAME**.
- Click **OK**. The display returns to the **Duplicate Key Exclusion** dialog box.
- Type **DUPLICATE EMPLOYEES** in the **File name** box.
- Click **OK**.

View the results:

- The view will default to the new file created called **DUPLICATE EMPLOYEES**. It will display in a parent/child relationship in the IDEA File Explorer under the **Users-Database** file.



Querying Data

Use IDEA's **Data Extraction** to query files and isolate the desired records in a database. Up to 50 different extractions can be run at one time. In this case, use IDEA's **Data Extraction** to find terminated employees quickly.

Access the Employee Master 20070815-Database file:

- Click **Window**.
- Click **Close All**.
- Double-click on the blue icon next to the file name **Employee Master 20070815-Database** to open the file.

Find Terminated Employees:

- Click **Data**.
- Click **Extraction**.
- Click **Direct Extraction**. The Extract to Files(s) dialog box displays.
- Change the default file name from **EXTRACTION 1** to **Terminated Employees**.
- Click the green calculator icon. The **Equation Editor** launches.
- Type **TERM_DATE <> ""** in the upper left window (be sure there are no spaces inside the double quotes).
- Click the green check mark on the tool bar. The display returns to the Extract to Files(s) dialog box.
- The criteria entered in the **Equation Editor** displays in the **Criteria Column**.
- Click **OK** in the **Extract to File(s)** dialog box.

View the results:

- A new file will be created called **Terminated Employees**. It will display in a parent/child relationship in the IDEA File Explorer.
- Double click on the blue icon next to the file name to open the file and view the results.



Link Analysis

Use IDEA's **Join Files** function to relate the data between two separate files. In this instance, link the **Terminated Employees** file to the **Users** file to be sure all terminated employees have been disabled.

Use Join Databases:

- Click **Window**.
- Click **Close All**.
- Double-click on the file, **Users-Database**, to make it the active file.
- Click **File**.
- Click **Join Databases**. The Join Databases dialog box displays.
- The primary database is **Users-Database**, which was the open database from which this function was started.
- Click **Select** to choose the secondary database. The Select Database dialog box displays.
- Navigate to **Terminated Employees**, and highlight it.
- Click **OK**.
- Change the default file name from Join to **Verify Terminated Employees Disabled**.
- Click **Match**. The Match Key Fields window displays.
- Click in the turquoise field under **Primary** and select **USERNAME**.
- Click in the turquoise field under **Secondary** and select **USER_NAME**.
- Click **OK**.
- Select the **Matches only** options button.
- Click **OK**.

View the results:

- A new file will be created called **Verify Terminated Employees Disabled**. It will display in a parent/child relationship in the IDEA File Explorer under the **Users-Database** file.
- Scroll to the right to find the **ACCOUNTDISABLE** field and see if the users have been disabled.

Error or a problem?

- In the **Properties** window, click **Criteria**. The Equation Editor launches.
- Type **TERM_DATE <= LASTLOGONTIME** in the upper left window.
- Click the green check mark on the tool bar. The display returns to the Data view. However, only the records that meet the criteria set will display.
- To clear the criteria and return to a view of all the records, right-click **Criteria** and click **Clear**.