DFS by DreamGRC: Quick-Start Guide for Incident Reconstruction

This guide will walk you through the essential steps to reconstruct a security incident using the DFS by DreamGRC platform, from logging in for the first time to completing your first incident reconstruction workflow.

1. Getting Started

First-Time Login

1. Open your web browser and navigate to the platform URL
2. Enter your login credentials (email and password)
3. If this is your first login, you'll be prompted to:
4. Change your temporary password
5. Complete your profile information
6. Configure two-factor authentication (optional but recommended)

Understanding the Interface

After logging in, you'll see the dashboard with: - **Top Navigation Bar**: User profile, notifications, and help - **Side Menu**: Access to platform features - **Quick Stats**: Overview of your cases and recent activity - **Recent Cases**: Direct links to your active cases

2. Creating Your First Case

1. Click on "Cases" in the side menu
2. Click the "+ New Case" button in the top right corner
3. Fill in the case details:
4. **Case Name**: Enter a descriptive name for the incident

5. **Case Type**: Select "Incident Response" or the appropriate type
6. **Priority**: Set the priority level
7. **Description**: Provide details about the incident
8. **Start Date**: When the incident was detected
9. **Tags**: Optional keywords for easier filtering
10. Click "Create Case"

3. Uploading Evidence

Evidence is the foundation of your investigation. Here's how to upload it:

1. Inside your newly created case, click on the "Evidence" tab
2. Click the "+ Upload Evidence" button
3. Select the file upload method:
4. **Drag and Drop**: Simply drag files into the designated area
5. **Browse**: Click to browse and select files from your computer
6. For each file, set the following:
7. **Evidence Type**: Select the appropriate type (memory dump, disk image, network capture, log file, etc.)
8. **Description**: Add a brief description of the evidence
9. **Acquisition Date**: When the evidence was collected
10. **Source**: Where the evidence came from (hostname, IP, etc.)
11. **Examiner**: Who collected the evidence
12. Click "Upload" and wait for the upload to complete

Supported Evidence Types:

- **Memory Dumps**: Raw memory images (.raw, .mem, .dmp)
- **Disk Images**: Full disk or volume images (.dd, .img, .raw)
- **Network Captures**: Packet captures (.pcap, .pcapng)
- **Log Files**: Various system and application logs
- **Registry Files**: Windows registry hives
- **Other**: Documents, email archives, etc.

4. Initial Evidence Analysis

Before starting a workflow, analyze your evidence to extract key information:

1. In the "Evidence" tab, locate an evidence file you want to analyze
2. Click the "Analyze" button next to the file
3. In the analysis configuration:
4. Select the appropriate tool (the platform will suggest the best tool based on the file type)
5. Choose the analysis command (what you want to find or extract)
6. Adjust any parameters if needed
7. Click "Start Analysis"
8. The analysis will run in the background
9. Once complete, click "View Results" to see what was found

5. Creating an Incident Reconstruction Workflow

1. In your case, go to the "Workflows" tab
2. Click "+ New Workflow"
3. Choose workflow creation method:
4. **Use Template**: Select a predefined template (recommended for beginners)
5. **Custom Workflow**: Build your own from scratch
6. If using a template:
7. Select "Incident Response" or "Network Intrusion" template
8. Review the predefined steps
9. Customize as needed
10. Click "Create Workflow"
11. If creating a custom workflow:
12. Name your workflow
13. Add a description
14. Click "Create" then add steps manually

6. Adding Workflow Steps (for Custom Workflows)

For custom workflows, you need to add steps:

1. In your newly created workflow, click "+ Add Step"
2. Configure the step:
3. **Step Name**: Clear, descriptive name
4. **Step Type**: Choose from Evidence Collection, Analysis, Correlation, Review, Documentation, or Action
5. **Description**: Detailed instructions for this step
6. **Required Evidence**: Link to specific evidence files needed for this step
7. **Tools**: Select tools to use in this step
8. **Expected Output**: What this step should produce
9. Click "Add Step"
10. Repeat to add more steps
11. Reorder steps by dragging and dropping if needed

7. Executing the Workflow

Now it's time to work through your incident reconstruction workflow:

1. In the "Workflows" tab, select your workflow
2. You'll see all steps listed in sequence
3. Start with the first step (status: "Not Started")
4. Click "Start Step" to begin
5. Follow the instructions specific to that step
6. For an analysis step:
7. Select the evidence file(s) to analyze
8. Choose the appropriate tool and command
9. Run the analysis
10. Review the results
11. After completing the step actions, click "Complete Step"
12. Move to the next step and repeat the process
13. Continue until all steps are completed

8. Correlation Analysis

To discover relationships between different evidence items:

1. In your case, go to the "Correlations" tab
2. Click "+ New Correlation"
3. Select correlation type:
4. **Timeline Correlation**: For time-based relationships
5. **Pattern Matching**: For content similarities
6. **Entity Correlation**: For user/system relationships
7. **ML-Based Correlation**: For advanced pattern discovery
8. Select the evidence files to include in the correlation
9. Configure the correlation parameters
10. Click "Run Correlation"
11. Review the visualization and table results
12. Add significant findings to your workflow documentation

9. Timeline Creation

Building a comprehensive incident timeline:

1. In your case, go to the "Timeline" tab
2. Review automatically extracted timeline events from your analysis
3. Click "+ Add Event" to manually add events not captured in the evidence
4. For each manual event, set:
5. **Timestamp**: When the event occurred
6. **Event Type**: Category of event
7. **Description**: What happened
8. **Source**: Where this information came from
9. **Confidence**: How certain you are about this event
10. Arrange events chronologically
11. Use filters to focus on specific event types or time periods
12. Export the timeline for your report

10. Report Generation

Create a comprehensive incident report:

1. In your case, go to the "Reports" tab
2. Click "+ Generate Report"
3. Configure the report:
4. **Report Type**: Incident Response Report
5. **Title**: Clear descriptive title
6. **Format**: PDF, HTML, or Word
7. **Sections to Include**: Select all relevant sections
8. **Include Timeline**: Yes
9. **Include Indicators of Compromise**: Yes
10. **Include Plain Language Explanations**: Yes
11. Click "Generate Report"
12. Preview the report
13. Make any necessary adjustments
14. Click "Export" to download or share the final report

Quick Tips for Success

- **Prioritize Evidence Collection**: Start with the most volatile evidence
- **Document As You Go**: Take notes during each step
- **Use Smart Analysis**: Let the platform recommend the best tools for each evidence type
- **Review Plain Language Explanations**: Use the automatically generated explanations to understand technical findings
- **Focus on the Timeline**: A solid timeline is key to understanding the incident
- **Use Templates**: Templates provide a structured approach following industry best practices
- **Save Frequently**: Save your progress regularly
- **Export Key Findings**: Export important discoveries for your final report

Getting Help

If you run into issues: 1. Click the "Help" icon in the top navigation bar 2. Search the knowledge base for your question 3. Check the full documentation for detailed instructions 4. Contact support through the help menu if needed

Next Steps

After completing your first incident reconstruction: - Review other workflow templates for different incident types - Explore advanced correlation features - Set up remote collection agents for distributed investigations - Investigate the API for integration with other systems - Join the user community for best practices