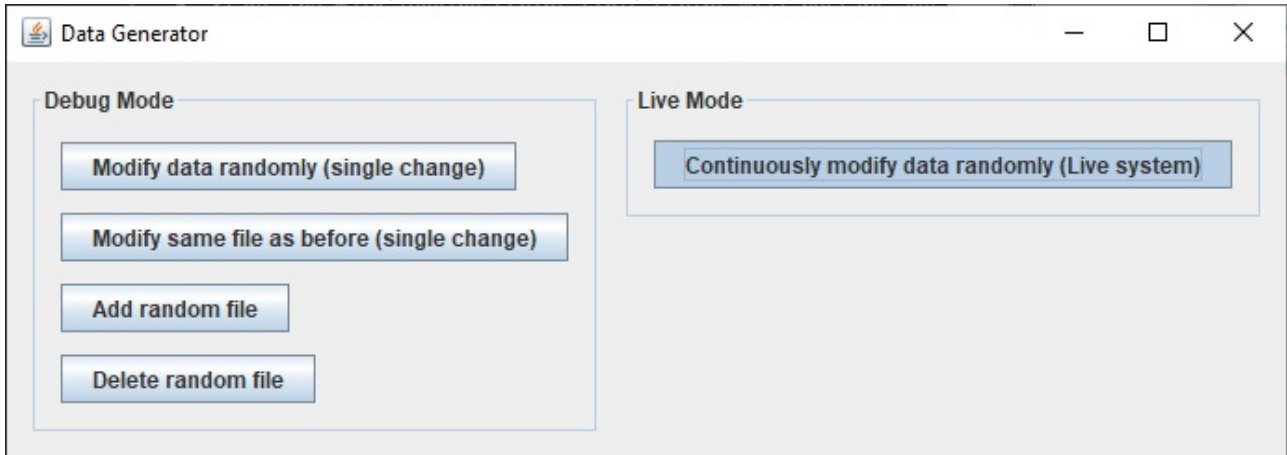


To quickly start the script you will need to execute the following steps:

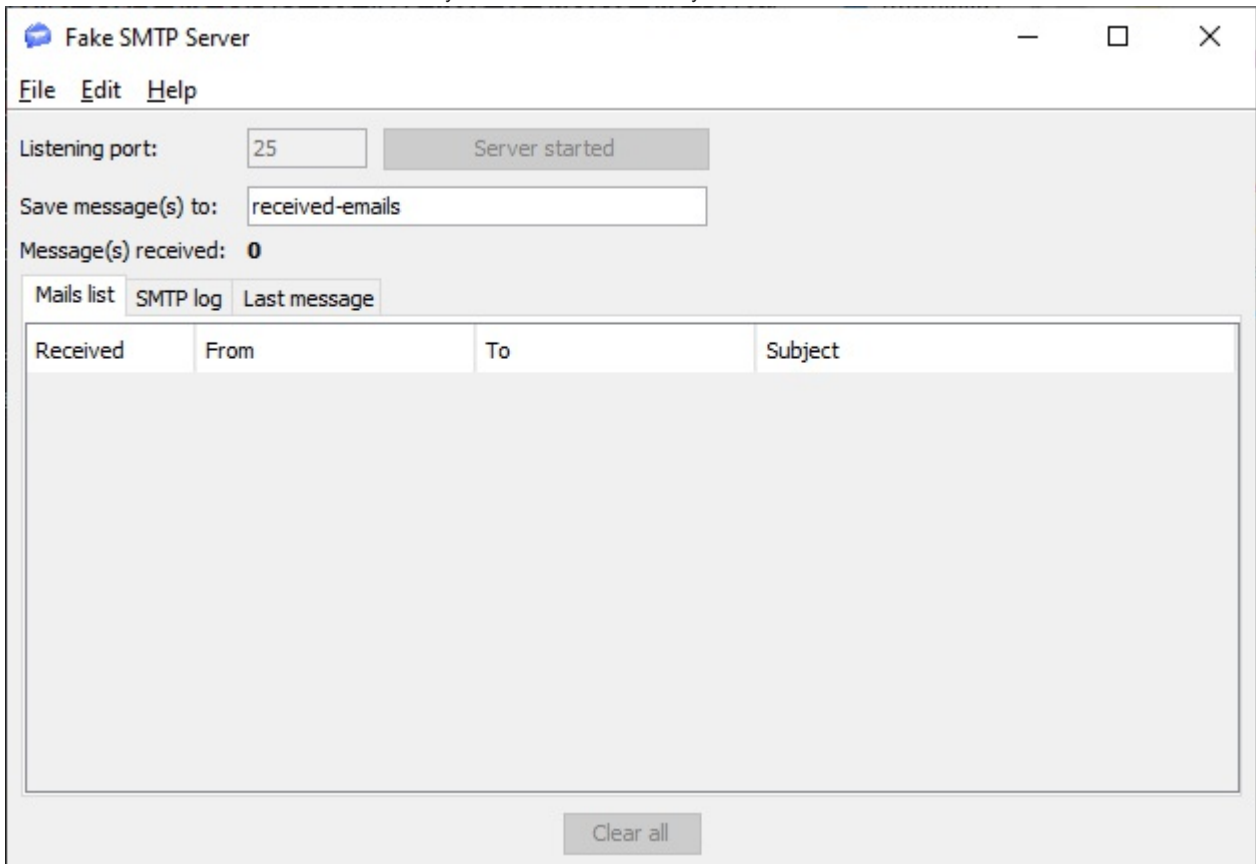
P.S.: *The main logging script requires Elevated Privileges because it needs to make a new Event Log*

1. Start the file modifier applet.
2. Click the button labeled: **Continuously modify data randomly (Live system)** in the window titled **Data Generator**.
3. Start the mail server applet.
4. Click the **Start Server** button in the fakeSMTP server when it opens.
5. Start the robocopy script.
6. Start the main logging script (This script will restart and ask for elevation if it is not run as administrator).

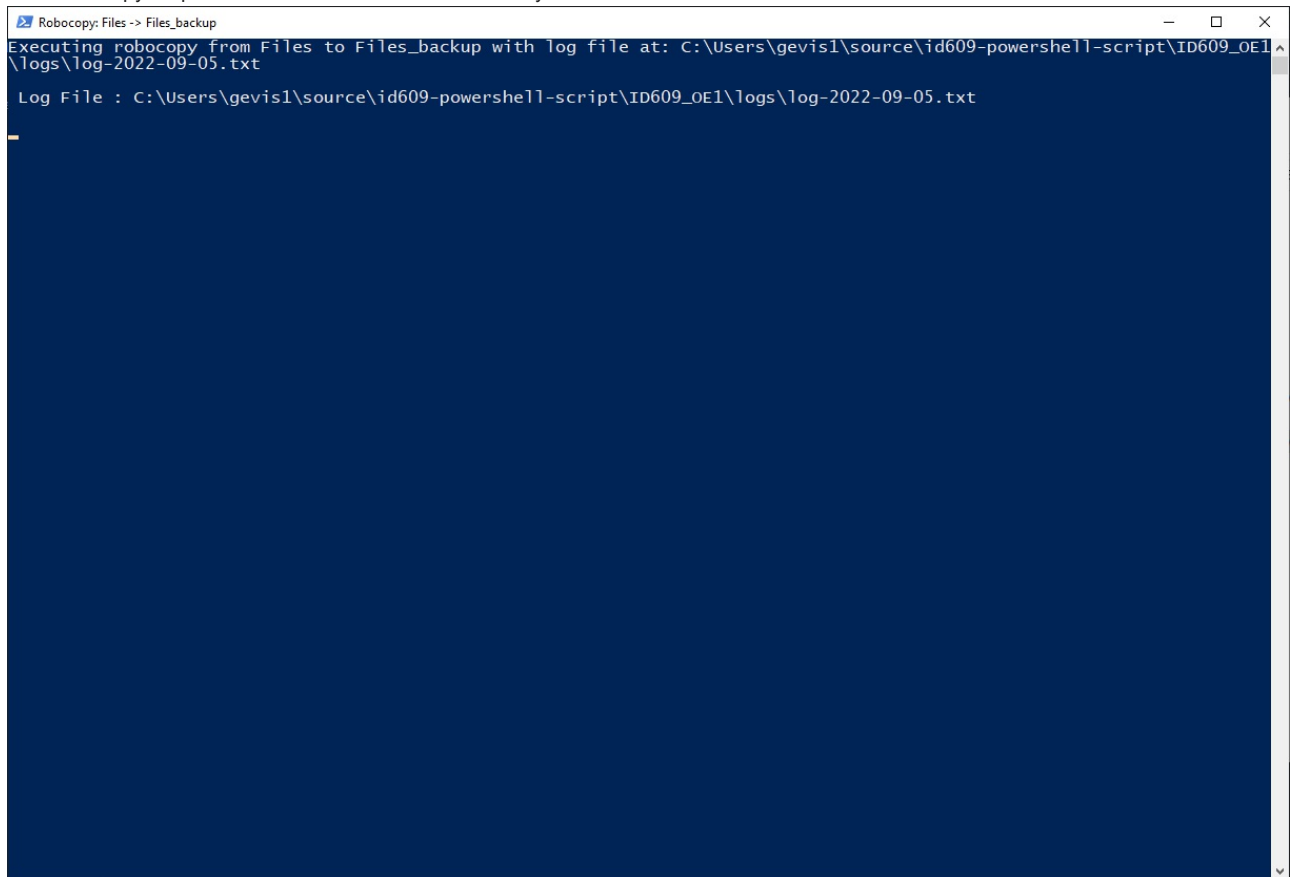
The File Modifier will look like this when you have started it correctly:



The Fake SMTP Server will look like this when you have started it correctly:

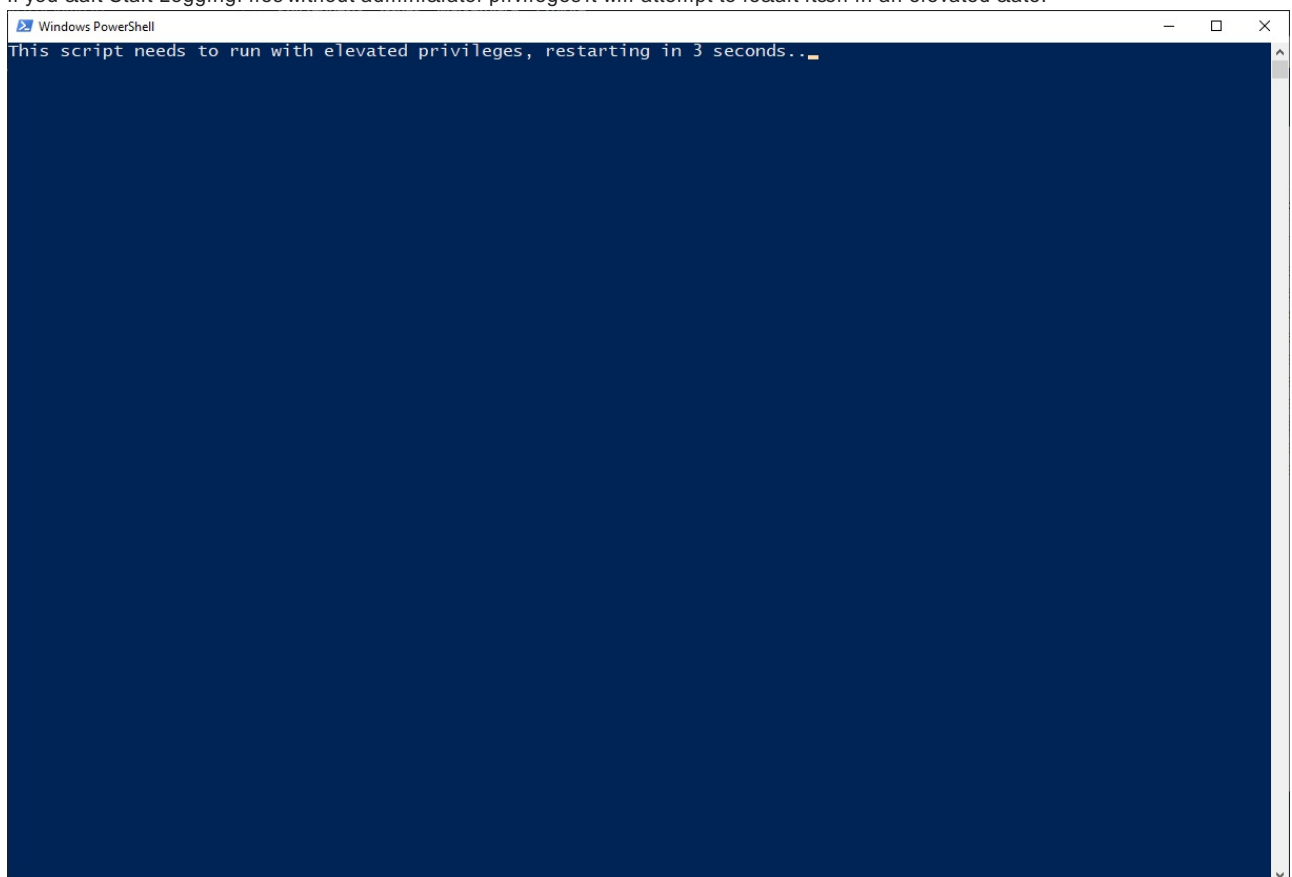


The Robocopy script will look like this when it successfully started:

A screenshot of a Robocopy console window. The title bar reads "Robocopy: Files -> Files\_backup". The window has a dark blue background with white text. The text displayed is: "Executing robocopy from Files to Files\_backup with log file at: C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\logs\log-2022-09-05.txt" followed by "Log File : C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\logs\log-2022-09-05.txt".

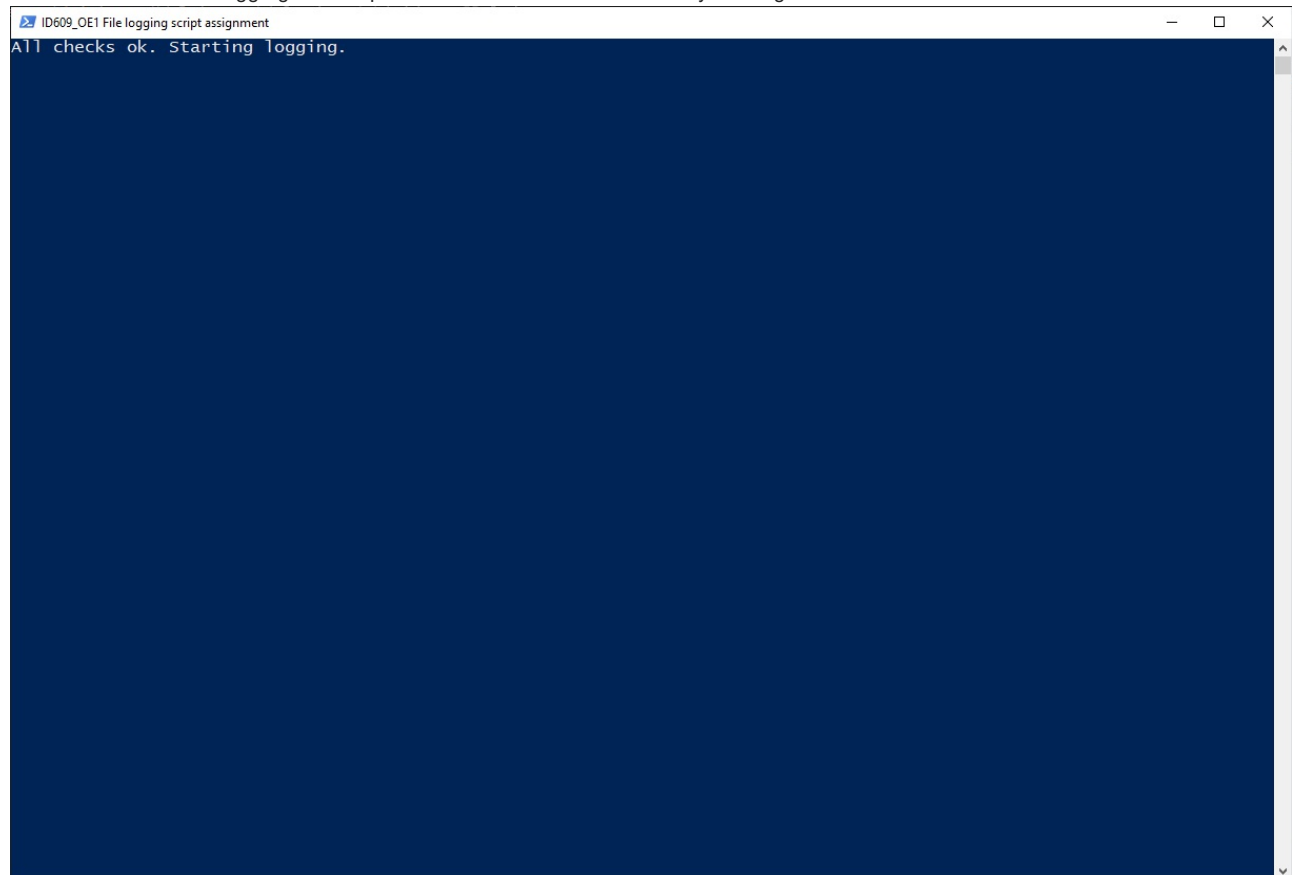
```
Robocopy: Files -> Files_backup
Executing robocopy from Files to Files_backup with log file at: C:\Users\gevis1\source\id609-powershell-script\ID609_OE1\logs\log-2022-09-05.txt
Log File : C:\Users\gevis1\source\id609-powershell-script\ID609_OE1\logs\log-2022-09-05.txt
```

If you start Start-LoggingFiles without administrator privileges it will attempt to restart itself in an elevated state:

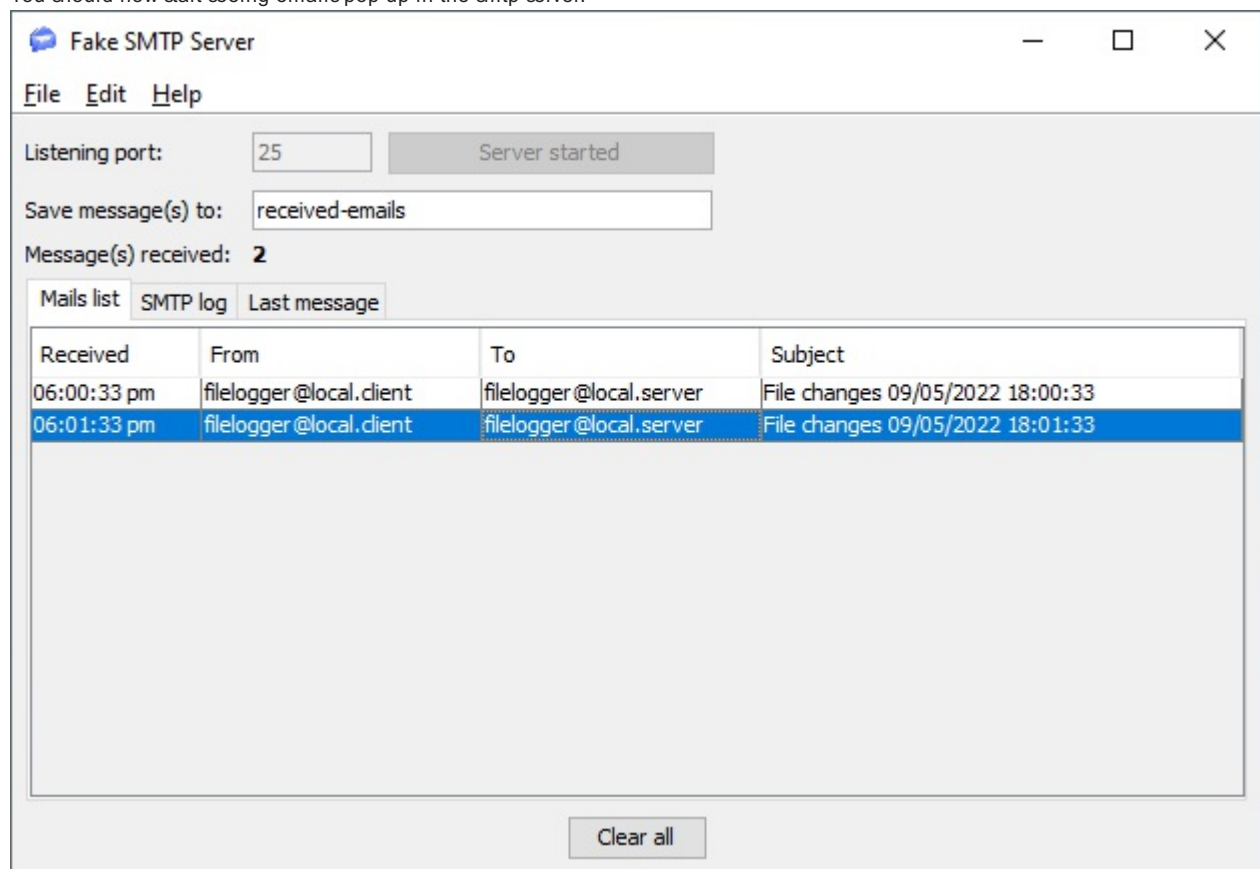
A screenshot of a Windows PowerShell console window. The title bar reads "Windows PowerShell". The window has a dark blue background with white text. The text displayed is: "This script needs to run with elevated privileges, restarting in 3 seconds...".

```
Windows PowerShell
This script needs to run with elevated privileges, restarting in 3 seconds...
```

This is what the Start-LoggingFiles script will look like when it is succesfully running:



You should now start seeing emails pop up in the smtp server:



If you open the Event Viewer and the email, the timestamp in the Subject of the email and the timestamp of the Event should match, and they should have the same data:

The screenshot displays three windows: Notepad, Fake SMTP Server, and Event Viewer.

**Notepad (05092206233316.eml):**

Mon, 05 Sep 2022 18:02:33 +1200 (NZST)

MIME-Version: 1.0

From: filelogger@local.client

To: filelogger@local.server

Date: 5 Sep 2022 18:02:33 +1200

Subject: File changes 09/05/2022 18:02:33

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: quoted-printable

DELETED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\logistics\doc\_0

CREATED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\production\log\_8

DELETED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\project2\data\_0

DELETED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\warehouse\log\_8

**Fake SMTP Server:**

Listening port: 25 Server started

Save message(s) to: received-emails

Message(s) received: 3

Received	From	To	Subject
06:00:33 pm	filelogger@local.client	filelogger@local.server	File changes 09/05/2022 18:00:33
06:01:33 pm	filelogger@local.client	filelogger@local.server	File changes 09/05/2022 18:01:33
06:02:33 pm	filelogger@local.client	filelogger@local.server	File changes 09/05/2022 18:02:33

**Event Viewer:**

Application Number of events: 17,760 (1) New events available

Level	Date and Time	Source	Event ID
Information	5/09/2022 6:02:23 pm	vmacthld	1000
Information	5/09/2022 6:03:23 pm	vmacthld	1000
Information	5/09/2022 6:03:52 pm	vmacthld	1000
Information	5/09/2022 6:02:33 pm	ID609FileLogger	3001
Information	5/09/2022 6:02:23 pm	vmacthld	1000

**Event 3001, ID609FileLogger**

General Details

DELETED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\logistics\doc\_0

CREATED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\production\log\_8

DELETED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\project2\data\_0

DELETED File C:\Users\gevis1\source\id609-powershell-script\ID609\_OE1\Files\_backup\warehouse\log\_8

Log Name: Application

Source: ID609FileLogger

Event ID: 3001

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 5/09/2022 6:02:33 pm

Task Category: (1)

Keywords: Classic

Computer: D312-71565.op.ac.nz