The Complete Guide For

Linked Fish:

Exploring Automated Phishing through AI-powered Social Engineering Tools

By: Ahmed Katrou

I-1 Introduction to Linked Fish:

Welcome to the **Linked Fish** tool guide! This document serves as a step-by-step walkthrough to help you understand, deploy, and use Linked Fish effectively. Linked Fish is an automated LinkedIn profile scraper and message generator, built for **educational and ethical hacking purposes**. It combines web scraping, automation, and natural language generation to explore how LinkedIn profiles can be utilized for research or awareness exercises on **social engineering, phishing simulations, and information gathering**.

The purpose of this project aligns with ethical hacking principles, focusing on **exposing vulnerabilities** related to publicly available data on professional platforms. The tool emphasizes responsible usage, helping organizations and individuals become aware of potential exploitation scenarios.

Through **Linked Fish**, you'll learn how attackers could:

- Extract personal and professional data from LinkedIn profiles.
- Use such data to generate **highly targeted social engineering messages**.
- Automate parts of the attack process using tools like **Selenium** and AI-powered APIs for message crafting.

This tool is not designed for malicious purposes but rather to simulate real-world risks. All users must **adhere strictly to ethical hacking guidelines** and ensure they have **explicit permission** to access and extract data from profiles. Misusing this tool or violating LinkedIn's terms of service may lead to legal consequences.

I-2 Key Features:

1. **Automated LinkedIn Login:** Automates login to LinkedIn using Selenium and manages cookies to maintain sessions.
2. **Profile Scraping:** Collects key details like Name, Headline, About section, and more.
3. **Personalized Message Generation:** Uses AI-based APIs to generate tailored phishing messages for email, SMS, and voice messages.
4. **Voice Synthesis:** Converts text to speech for voice-based phishing simulations.
5. **Progress Indicators and Console Banners:** Enhances the user experience with rich banners and loading screens.

Note: This guide will take you through the full setup, configuration, and usage of Linked Fish. Each section will contain:

1. **Detailed code explanations** of each component.
2. **Installation instructions** for required libraries and dependencies.
3. **Usage examples** and tips for real-world ethical hacking applications.
4. **Disclaimers** and reminders about responsible usage.

   Let's dive into the components and see how everything fits together!

II- Preparing the Environment for Linked Fish

After downloading the tool source code from Github using the following link, we start to prepare our environment:

A- Install Each Required Software:

Python Installation

1. Download and install **Python** (version 3.9 or above) from Python.org.

2. During installation, make sure to **check the box that adds Python to your PATH**.

VS Code Installation

1. Download and install **Visual Studio Code** from VS Code.

2. Install the **Python extension** for VS Code:

```
Open VS Code -> Extensions (Ctrl+Shift+X) -> Search for “Python” -> Install.
```

Google Chrome Installation

1. Make sure **Google Chrome** is installed on your system.
2. Download it from Chrome if you don't already have it.

B- Create a LinkedIn Account :

- If you don't already have one, visit LinkedIn and sign up for a **free account**.
- **Note:** You need a LinkedIn account to access profiles. Make sure you accept LinkedIn's terms of service and avoid scraping large amounts of data to prevent your account from being blocked.

C- Create a Groq Account and Get an API Key

1. Visit Groq and **sign up for an account**.
2. Once logged in:
    - Navigate to the **API Keys** section.
    - Generate a new **API key** and **save it securely**, as you'll use it in the message generation part of Linked Fish.

D- Create an ElevenLabs Account and Get API Key

1. Go to ElevenLabs and **sign up** for a free or paid account.
2. Navigate to **API Settings** within your ElevenLabs dashboard.
3. Generate a new **API key**.
4. Keep this key safe, as it will be used to convert phishing messages to **speech** for the voice simulation part of the tool.

E- Install Required Python Libraries

Open your terminal or command prompt and install the necessary libraries included in the file 'requirements.txt' included in the provided resources of the tool using the following command:

```
$ pip install -r requirements.txt
```

F- WebDriver for Selenium (ChromeDriver)

1. Download **ChromeDriver** from ChromeDriver Download.
    - Make sure to select the **version that matches your Chrome browser**.
2. Extract the downloaded file and **place the executable** in a directory like C:\WebDriver (for Windows) or /usr/local/bin (for Linux/Mac).
3. Add the ChromeDriver path to your **system PATH environment variable** or specify the path explicitly in your code.

G- Verify Installations

Open a terminal and ensure everything is properly installed:

```
python --version          # Verify Python version
pip list                  # Check if required libraries are installed
chromedriver --version    # Verify ChromeDriver is accessible
```

If everything works correctly, you are now ready to move to the **next step**: configuring the code for Linked Fish.

III Linked Fish: Workflow Explained Alongside Code Structure

In this section, we will explain the **workflow of Linked Fish** step-by-step while mapping each part of the process to the code components. The idea is to give a clear understanding of how the tool works behind the scenes and how each Python file contributes to the overall execution.

---

1. Overview of Linked Fish Workflow

Below is the general flow of **Linked Fish**, which automates LinkedIn scraping and generates targeted phishing messages in different formats (email, SMS, and voice messages):

1. **Launch the tool**: Display a banner and load the session.
2. **Log in to LinkedIn using cookies** to scrape user profiles.
3. **Extract profile data** from the LinkedIn pages.
4. **Generate personalized phishing messages** using the Groq API based on the extracted data.
5. **Convert a phishing message to speech** using the ElevenLabs API.
6. **Save the messages in multiple formats** (email, SMS, and voice) for social engineering attacks.

The **main components** in the project directory handle different stages of this workflow. Let's break it down step-by-step.

Step 1: Launch the Tool and Display Banner

Code: banner.py

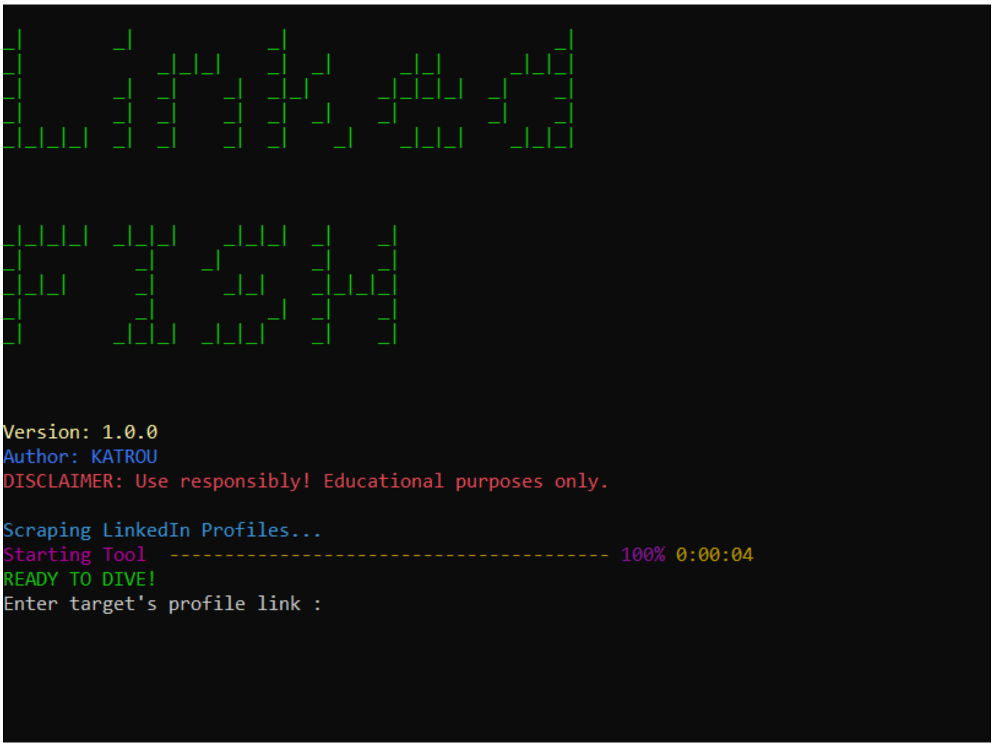
- **What Happens:**
  When the tool is launched, a **random ASCII banner** of the tool name "Linked Fish" is displayed for aesthetics using pyfiglet. A **loading screen** is then shown using the rich library.

- **How It Works:**

```
# Inside main.py
from banner import startup_screen
startup_screen("Linked Fish", version="1.0.0", author="KATROU")
```

Output:

- Displays a **cool-looking banner** and a **progress bar** to indicate the startup process.



```
Version: 1.0.0
Author: KATROU
DISCLAIMER: Use responsibly! Educational purposes only.

Scraping LinkedIn Profiles...
Starting Tool  ---------------------------------------- 100% 0:00:04
READY TO DIVE!
Enter target's profile link :
```

Step 2: Login to LinkedIn Using Cookies (Session Management)

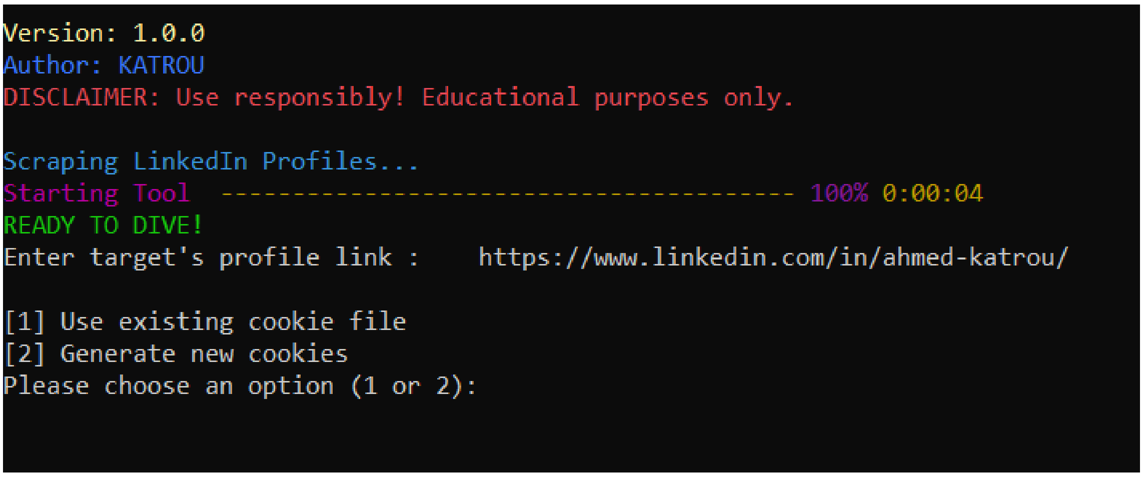
Code: login.py + **Main Menu Logic** in main.py

What Happens in This Step?

After entering the target's profile link, Linked Fish offers two options for session management:

1. **Use an existing cookie file** (if available).
2. **Log in** to LinkedIn after entering Email & Password and **generate a new cookie file** to store your session.

This flexibility ensures that users can skip logging in repeatedly while staying authenticated for multiple scraping sessions.



```
Version: 1.0.0
Author: KATROU
DISCLAIMER: Use responsibly! Educational purposes only.

Scraping LinkedIn Profiles...
Starting Tool  ---------------------------------------- 100% 0:00:04
READY TO DIVE!
Enter target's profile link :    https://www.linkedin.com/in/ahmed-katrou/

[1] Use existing cookie file
[2] Generate new cookies
Please choose an option (1 or 2):
```

Step 3: Extract Profile Data from LinkedIn

Code: extractors.py

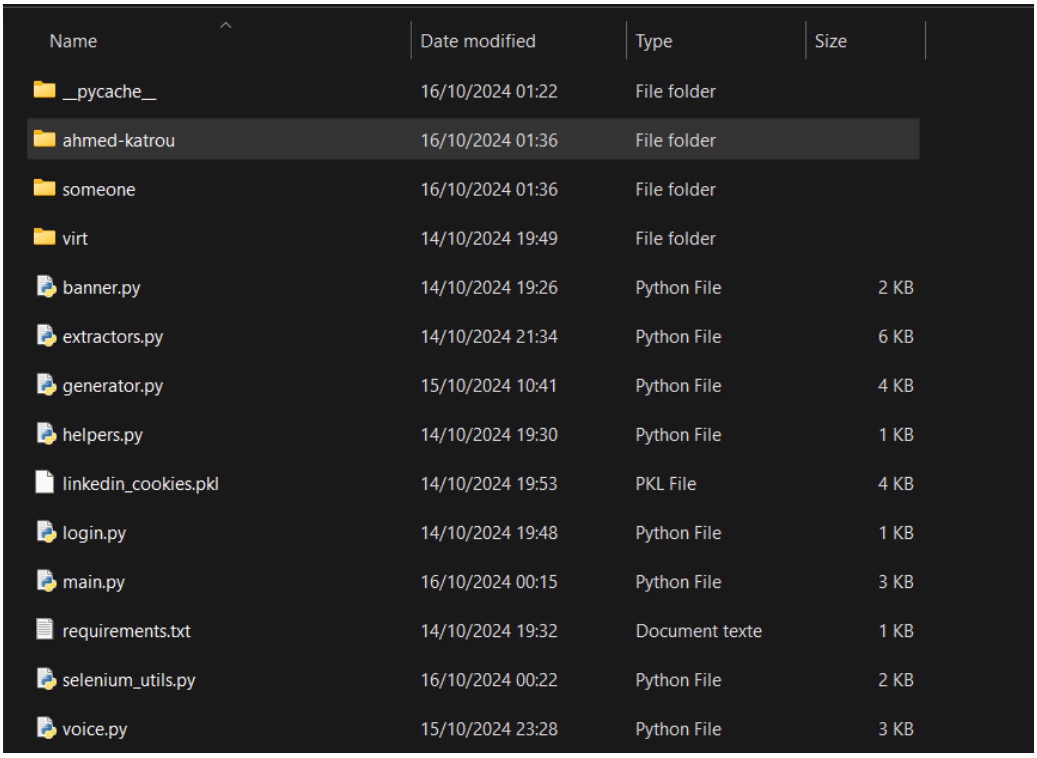
- **What Happens:**
  The tool uses **Selenium** to navigate LinkedIn profiles and extract important data like:
  - Name
  - Headline
  - About section
  - Work experience
  - Recent activity
- **How It Works:**

```
profile_data = extract_profile_data(browser, profile_url)
```

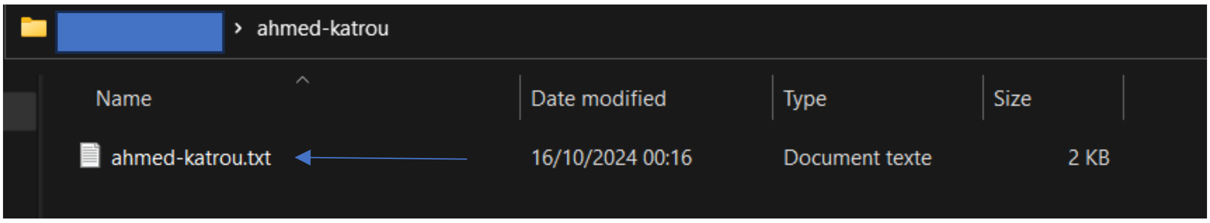
- **What This Code Does:**
  - Visits a LinkedIn profile URL.
  - Extracts the data fields and stores

Data Storage:

- A **folder named after the profile's ID** is created under the opened directory.
- Each piece of data is saved in **one text file** inside the folder.



Name	Date modified	Type	Size
__pycache__	16/10/2024 01:22	File folder	
ahmed-katrou	16/10/2024 01:36	File folder	
someone	16/10/2024 01:36	File folder	
virt	14/10/2024 19:49	File folder	
banner.py	14/10/2024 19:26	Python File	2 KB
extractors.py	14/10/2024 21:34	Python File	6 KB
generator.py	15/10/2024 10:41	Python File	4 KB
helpers.py	14/10/2024 19:30	Python File	1 KB
linkedin_cookies.pkl	14/10/2024 19:53	PKL File	4 KB
login.py	14/10/2024 19:48	Python File	1 KB
main.py	16/10/2024 00:15	Python File	3 KB
requirements.txt	14/10/2024 19:32	Document texte	1 KB
selenium_utils.py	16/10/2024 00:22	Python File	2 KB
voice.py	15/10/2024 23:28	Python File	3 KB



[redacted] › ahmed-katrou

Name	Date modified	Type	Size
ahmed-katrou.txt	16/10/2024 00:16	Document texte	2 KB

Step 4: Generate Phishing Messages Using Groq API

Code: generators.py

- **What Happens:**
  Once the profile data is collected, it is passed to the **Groq API**, which generates:
  1. **An email phishing message**
  2. **An SMS phishing message**
  3. **A voice message script**
- **How It Works:**

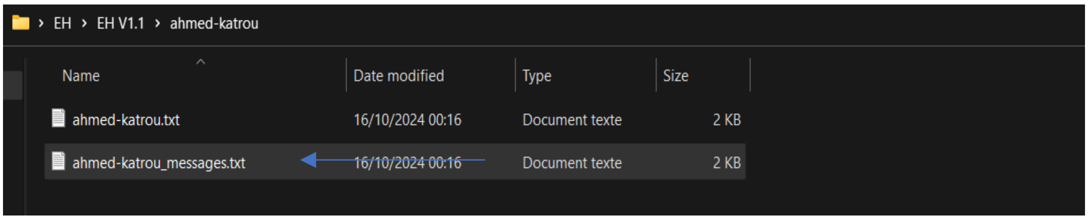
```
from generators import generate_messages
messages = generate_messages(api_key, profile_data)
print(messages)
```

- **How the API Call Works:**
  - The profile data is **formatted as input** for Groq's message generation model.
  - The Groq API returns three messages that leverage **personal details from the profile** to create convincing phishing content.

Note: A very detailed prompt is sent to LLM model for occurrent results. You can check for the prompt details in **extractors.py** file.

Data Storage:

- The generated phishing content is stored under the same folder for following use.



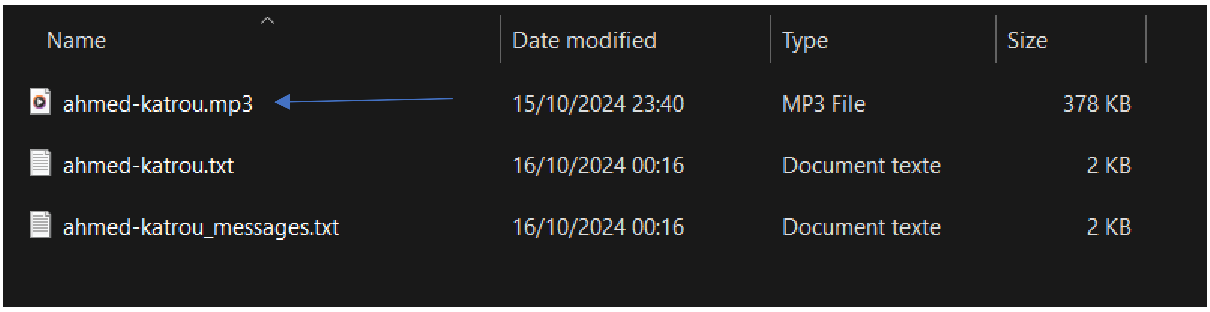
› EH › EH V1.1 › ahmed-katrou

Name	Date modified	Type	Size
ahmed-katrou.txt	16/10/2024 00:16	Document texte	2 KB
ahmed-katrou_messages.txt	16/10/2024 00:16	Document texte	2 KB

Step 5: Conversion to Voice Message Using ElevenLabs API

Code: voice.py

- **What Happens:**
  The **Voice script message** get **converted into speech** using the ElevenLabs API. This feature adds a layer of social engineering by generating realistic voice messages.



Name	Date modified	Type	Size
ahmed-katrou.mp3	15/10/2024 23:40	MP3 File	378 KB
ahmed-katrou.txt	16/10/2024 00:16	Document texte	2 KB
ahmed-katrou_messages.txt	16/10/2024 00:16	Document texte	2 KB

Summary of Files and Their Roles:

• File	• Role
• banner.py	• Displays ASCII banners and progress bars.
• extractors.py •	• Handles LinkedIn scraping and session management. •
• generators.py	• Calls Groq API to generate phishing messages.
• voice.py	• Converts text to speech using ElevenLabs API.
• helpers.py •	• Provides utility functions (e.g., removing duplicates). •
• main.py •	• The entry point that ties everything together.

With the environment set up and the code understood, you're ready to run Linked Fish and start experimenting! Remember, this tool is built for ethical hacking purposes, always use it responsibly and in accordance with relevant laws and ethical guidelines.