Gather Information about a Target Website using Photon

is a practical reconnaissance and information gathering activity about a target website. It is one of the initial steps in a penetration test or security analysis.

Photon is an automated tool that allows for the rapid and efficient gathering of a large amount of valuable information about a website. It acts as a data harvester.

What does Photon do concretely?

The tool scans the target website and collects data such as:

* **URLs:** All internal and external links.
* **Files:** Links to documents (PDF, Word, Excel), images, etc.
* **Email addresses:** Found in the source code or on the pages.
* **Phone numbers.**
* **Keywords and metadata.**
* **Social Media:** Links to associated social media profiles.
* **Information about the technologies used** (digital fingerprints).

Why perform this collection?

The goal is to understand the website's attack surface. All the information gathered can be used to identify weaknesses, potential vulnerabilities, or sensitive information that has been accidentally exposed.

Here is a real example of how Photon work:

1. *System Preparation & Tool Installation*

Command: `sudo apt update`

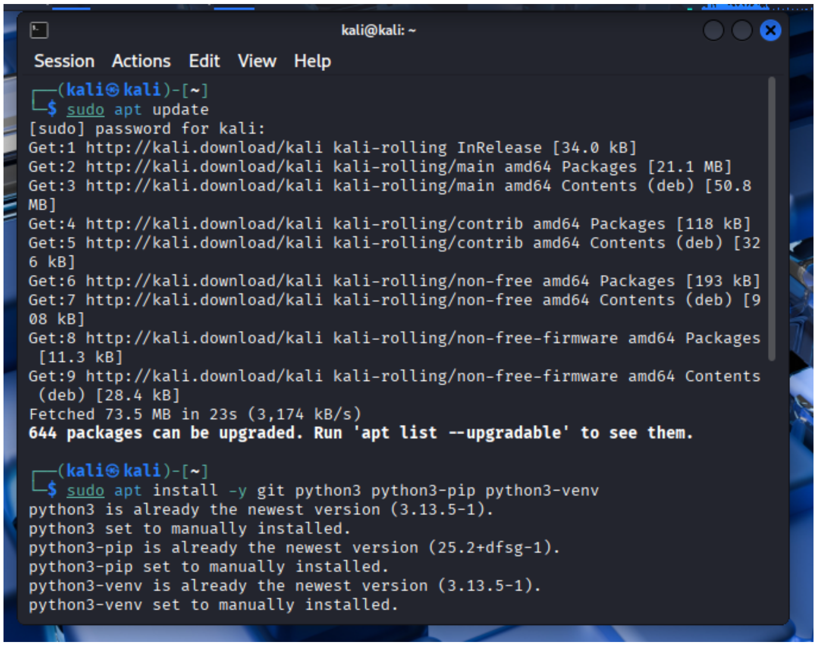
* Updated the Kali Linux system's package list to ensure we install the latest available software versions.

Command: `sudo apt install -y git python3 python3-pip python3-venv`

* Installed essential tools. Git was upgraded, and Python3 with its package manager (pip) and virtual environment tool were confirmed to be installed.

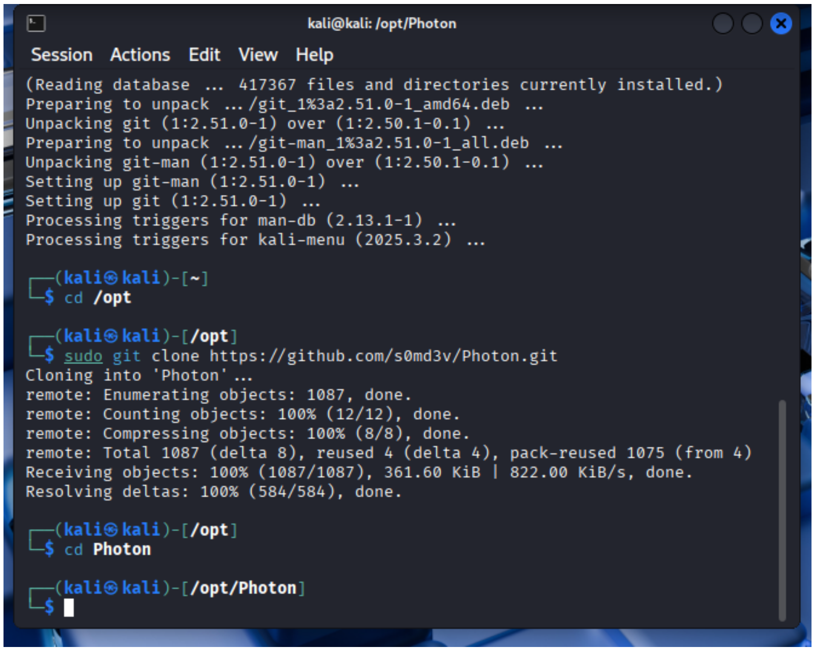
Command: `sudo git clone https://github.com/s0md3v/Photon.git /opt/Photon`

* Downloaded the Photon tool from its official GitHub repository and saved it to the `/opt/` directory.



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [50.8
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [118 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [32
6 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [9
08 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
 [11.3 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
 (deb) [28.4 kB]
Fetched 73.5 MB in 23s (3,174 kB/s)
644 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install -y git python3 python3-pip python3-venv
python3 is already the newest version (3.13.5-1).
python3 set to manually installed.
python3-pip is already the newest version (25.2+dfsg-1).
python3-pip set to manually installed.
python3-venv is already the newest version (3.13.5-1).
python3-venv set to manually installed.
```



```
(Reading database ... 417367 files and directories currently installed.)
Preparing to unpack .../git_1%3a2.51.0-1_amd64.deb ...
Unpacking git (1:2.51.0-1) over (1:2.50.1-0.1) ...
Preparing to unpack .../git-man_1%3a2.51.0-1_all.deb ...
Unpacking git-man (1:2.51.0-1) over (1:2.50.1-0.1) ...
Setting up git-man (1:2.51.0-1) ...
Setting up git (1:2.51.0-1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...

┌──(kali㉿kali)-[~]
└─$ cd /opt

┌──(kali㉿kali)-[/opt]
└─$ sudo git clone https://github.com/s0md3v/Photon.git
Cloning into 'Photon'...
remote: Enumerating objects: 1087, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 1087 (delta 8), reused 4 (delta 4), pack-reused 1075 (from 4)
Receiving objects: 100% (1087/1087), 361.60 KiB | 822.00 KiB/s, done.
Resolving deltas: 100% (584/584), done.

┌──(kali㉿kali)-[/opt]
└─$ cd Photon

┌──(kali㉿kali)-[/opt/Photon]
└─$ 
```

2. Environment Setup & Tool Configuration

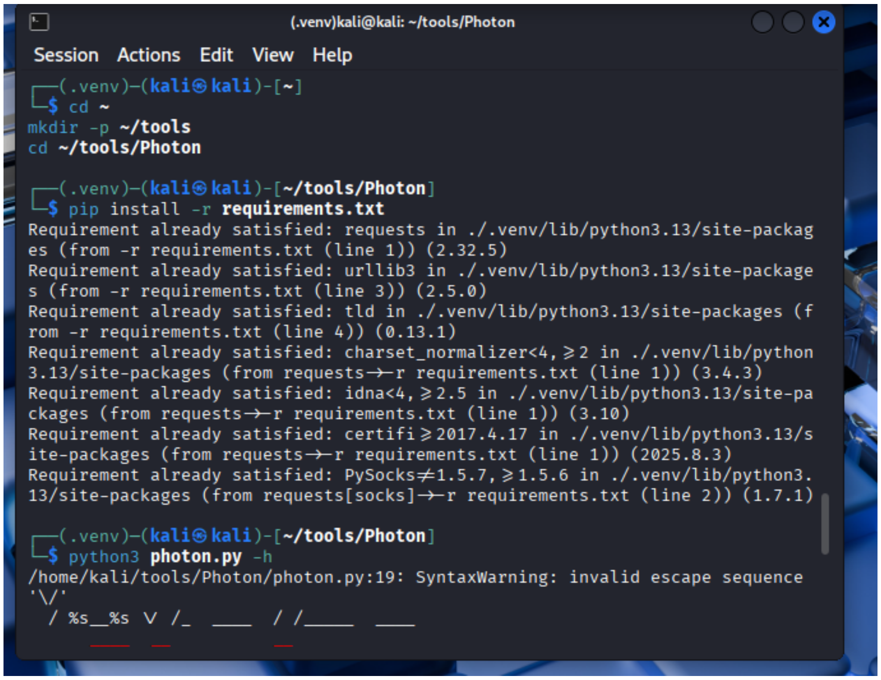
Commands:

```
cd ~
mkdir -p ~/tools/Photon
cd ~/tools/Photon
pip install -r requirements.txt
```

***** Created a personal working directory for the project and installed all the necessary Python libraries that Photon needs to run.

Command: python3 photon.py -h

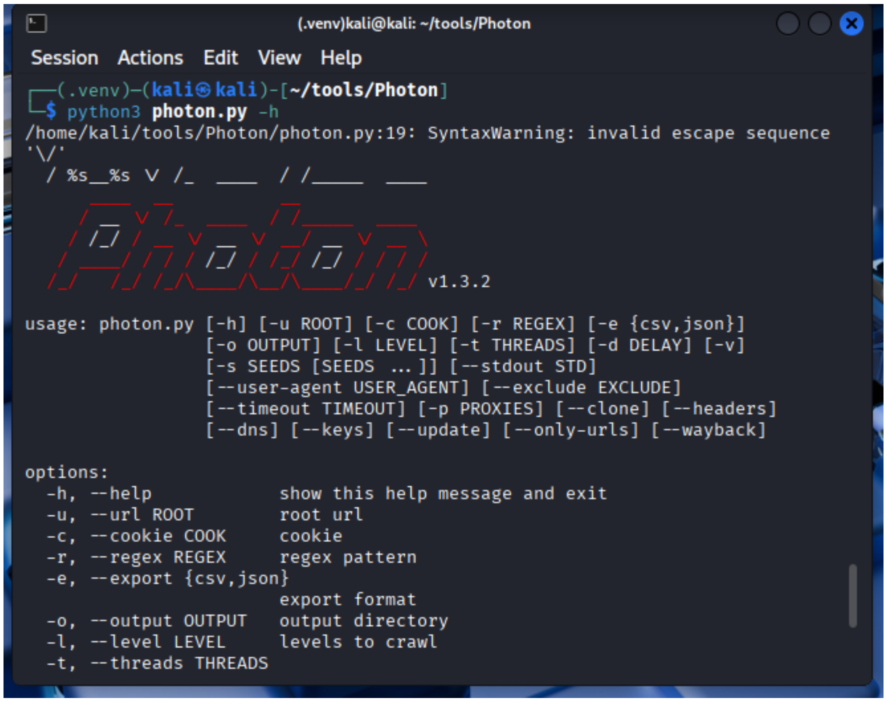
* Displayed the help menu for Photon. This confirms the tool is working correctly and shows all the available options for scanning.


(.venv)kali@kali: ~/tools/Photon
Session Actions Edit View Help

```
┌──(.venv)─(kali㉿kali)-[~]
└─$ cd ~
mkdir -p ~/tools
cd ~/tools/Photon

┌──(.venv)─(kali㉿kali)-[~/tools/Photon]
└─$ pip install -r requirements.txt
Requirement already satisfied: requests in ./.venv/lib/python3.13/site-packag
es (from -r requirements.txt (line 1)) (2.32.5)
Requirement already satisfied: urllib3 in ./.venv/lib/python3.13/site-package
s (from -r requirements.txt (line 3)) (2.5.0)
Requirement already satisfied: tld in ./.venv/lib/python3.13/site-packages (f
rom -r requirements.txt (line 4)) (0.13.1)
Requirement already satisfied: charset_normalizer<4,≥2 in ./.venv/lib/python
3.13/site-packages (from requests→-r requirements.txt (line 1)) (3.4.3)
Requirement already satisfied: idna<4,≥2.5 in ./.venv/lib/python3.13/site-pa
ckages (from requests→-r requirements.txt (line 1)) (3.10)
Requirement already satisfied: certifi≥2017.4.17 in ./.venv/lib/python3.13/s
ite-packages (from requests→-r requirements.txt (line 1)) (2025.8.3)
Requirement already satisfied: PySocks≠1.5.7,≥1.5.6 in ./.venv/lib/python3.
13/site-packages (from requests[socks]→-r requirements.txt (line 2)) (1.7.1)

┌──(.venv)─(kali㉿kali)-[~/tools/Photon]
└─$ python3 photon.py -h
/home/kali/tools/Photon/photon.py:19: SyntaxWarning: invalid escape sequence
'\/'
  / %s__%s \/ /_  ____  / /_____  ____
      ____  __          __
```


(.venv)kali@kali: ~/tools/Photon
Session Actions Edit View Help

```
┌──(.venv)─(kali㉿kali)-[~/tools/Photon]
└─$ python3 photon.py -h
/home/kali/tools/Photon/photon.py:19: SyntaxWarning: invalid escape sequence
'\/'
  / %s__%s \/ /_  ____  / /_____  ____
      ____  __          __
     / __ \/ /_  ____  / /_____  ____
    / /_/ / __ \/ __ \/ __/ __ \/ __ \
   / ____/ / / / /_/ / /_/ /_/ / / / /
  /_/   /_/ /_/\____/\__/\____/_/ /_/ v1.3.2

usage: photon.py [-h] [-u ROOT] [-c COOK] [-r REGEX] [-e {csv,json}]
                 [-o OUTPUT] [-l LEVEL] [-t THREADS] [-d DELAY] [-v]
                 [-s SEEDS [SEEDS ...]] [--stdout STD]
                 [--user-agent USER_AGENT] [--exclude EXCLUDE]
                 [--timeout TIMEOUT] [-p PROXIES] [--clone] [--headers]
                 [--dns] [--keys] [--update] [--only-urls] [--wayback]

options:
  -h, --help            show this help message and exit
  -u, --url ROOT        root url
  -c, --cookie COOK     cookie
  -r, --regex REGEX     regex pattern
  -e, --export {csv,json}
                        export format
  -o, --output OUTPUT   output directory
  -l, --level LEVEL     levels to crawl
  -t, --threads THREADS
```

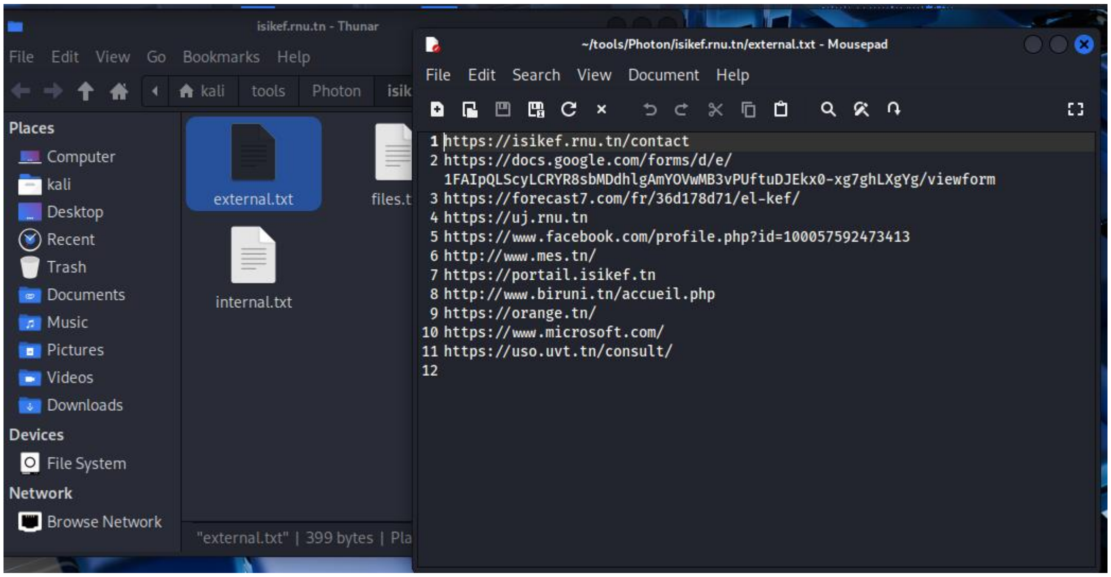
3. Results Found:

The tool successfully discovered and saved two types of URLs:

external.txt: This file contains links to **external websites** found on the target site.

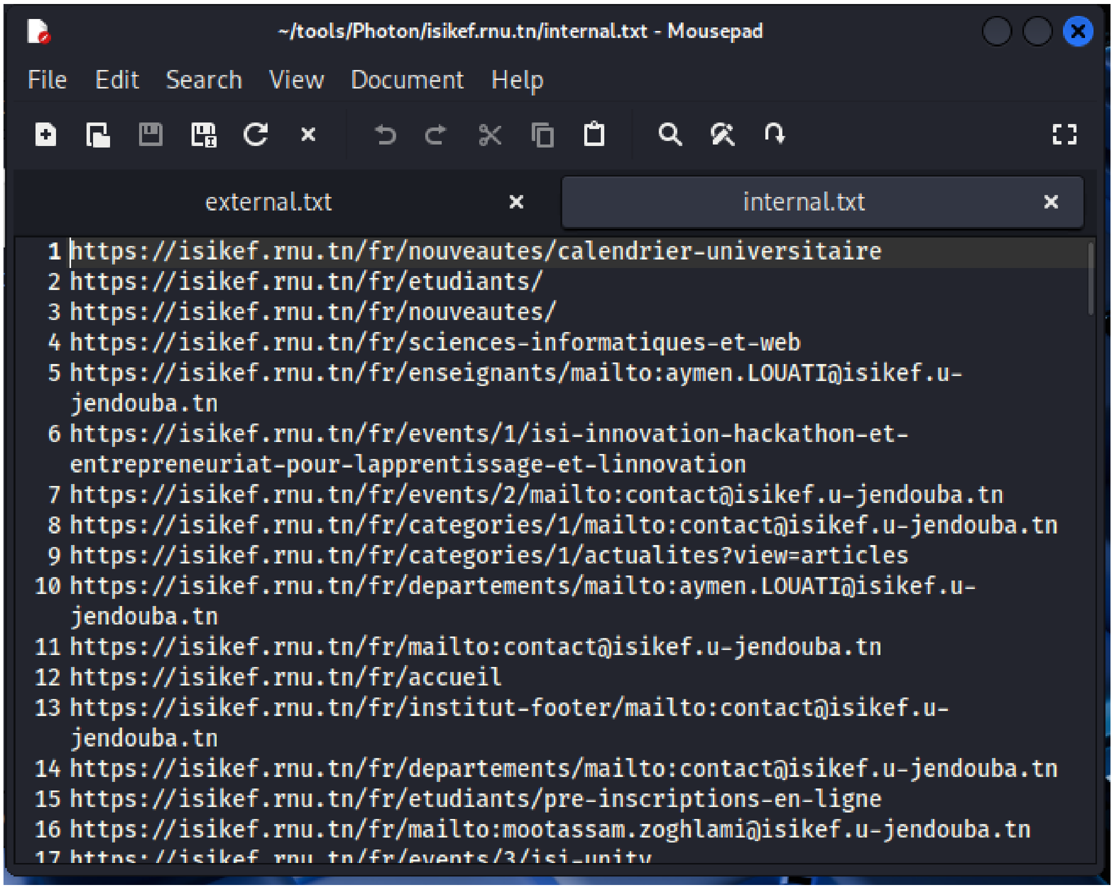
Examples: Links to Google Forms, Facebook, Microsoft, other university portals (e.g., uj.rmu.tn, portail.isikef.tn), and Tunisian government/company websites.
internal.txt: This file contains links to **internal pages** within the isikef.rmu.tn website itself.

Examples: Links for students, news, academic departments, event pages (like a hackathon), and most notably, **multiple email addresses** (e.g., contact@isikef.u-jendouba.tn, contact@isikef.u-jendouba.tn).



```
https://isikef.rnu.tn/contact
https://docs.google.com/forms/d/e/1FAIpQLScyLCRYR8sbMDdhlgAmYOVwMB3vPUftuDJEkx0-xg7ghLXgYg/viewform
https://forecast7.com/fr/36d178d71/el-kef/
https://uj.rnu.tn
https://www.facebook.com/profile.php?id=100057592473413
http://www.mes.tn/
https://portail.isikef.tn
http://www.biruni.tn/accueil.php
https://orange.tn/
https://www.microsoft.com/
https://uso.uvt.tn/consult/

```


~/tools/Photon/isikef.rnu.tn/internal.txt - Mousepad
File Edit Search View Document Help
external.txt
internal.txt

```
https://isikef.rnu.tn/fr/nouveautes/calendrier-universitaire
https://isikef.rnu.tn/fr/etudiants/
https://isikef.rnu.tn/fr/nouveautes/
https://isikef.rnu.tn/fr/sciences-informatiques-et-web
https://isikef.rnu.tn/fr/enseignants/mailto:aymen.LOUATI@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/events/1/isi-innovation-hackathon-et-entrepreneuriat-pour-lapprentissage-et-linnovation
https://isikef.rnu.tn/fr/events/2/mailto:contact@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/categories/1/mailto:contact@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/categories/1/actualites?view=articles
https://isikef.rnu.tn/fr/departements/mailto:aymen.LOUATI@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/mailto:contact@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/accueil
https://isikef.rnu.tn/fr/institut-footer/mailto:contact@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/departements/mailto:contact@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/etudiants/pre-inscriptions-en-ligne
https://isikef.rnu.tn/fr/mailto:mootassam.zoghlami@isikef.u-jendouba.tn
https://isikef.rnu.tn/fr/events/3/isi-unity
```