**🛠️ Misc OSINT Tools (Creepy, Harvester, Recon-ng & More)**

**Level:** Beginner  
**Category:** OSINT / Recon / Location Tracking / Data Gathering

**🧪 TOOLS WE'LL COVER**

| **Tool** | **Focus Area** |
| --- | --- |
| 🧠 **Creepy** | Geo-location tracking from social media/images |
| 🕵️‍♂️ **TheHarvester** | Email/domain enumeration |
| 🔍 **Recon-ng** | Web-based recon automation |
| 📦 Bonus: List of other top OSINT tools |  |

**🔹 1. Installing & Using Creepy**

**💡 What It Does:**

**Creepy** collects **geo-location data** from social media posts (Twitter, Flickr, Instagram), images (EXIF metadata), and maps them.

✅ Useful for:

* Tracking a person’s **location history**
* Investigating photos for **GPS tags**
* Creating **movement timelines**

**🔧 Installation (on Kali or Ubuntu)**

sudo apt install creepy

If that doesn’t work, try:

git clone https://github.com/ilektrojohn/creepy.git

cd creepy

sudo pip install -r requirements.txt

python creepy.py

**🚀 How to Run a Test Case**

1. **Open Creepy**
2. In the **target box**, enter a:
   * Twitter handle
   * Flickr username
3. Click **“Gather Location Info”**
4. Wait for results → See locations on the map (Google, OpenStreetMap)

🗂️ You can also upload an image with EXIF data:

* Drag and drop the photo
* It shows GPS location (if available)

**🔹 2. TheHarvester – Domain/Email OSINT**

**💡 What It Does:**

Collects **emails, subdomains, hosts, employee names, open ports** from public sources.

✅ Great for **footprinting companies/domains** during Red Team ops.

**🔧 Install & Run:**

sudo apt install theharvester

**🔍 Example:**

theharvester -d tesla.com -b google

-d: domain name  
-b: data source (google, bing, baidu, yahoo, etc.)

You’ll get:

* Emails (e.g. [hr@tesla.com](mailto:hr@tesla.com))
* Subdomains (e.g. careers.tesla.com)

**🔹 3. Recon-ng – Modular Recon Framework**

**💡 What It Does:**

Works like **Metasploit**, but for recon. You load modules to find:

* Emails
* Domains
* Hosts
* Social media profiles
* Breaches, leaks

**🔧 Install:**

sudo apt install recon-ng

Then run:

recon-ng

**🚀 Example Workflow:**

workspaces create tesla

add domains tesla.com

modules load recon/domains-hosts/bing\_domain\_web

run

* Add a domain
* Load a module (like Bing search)
* Run it to get subdomains or hosts

✅ Recon-ng has **APIs** for tools like:

* Shodan
* HaveIBeenPwned
* VirusTotal

You can add API keys for deeper scanning.

**🧰 Other Important OSINT Tools You Should Know**

| **Tool** | **Purpose** |
| --- | --- |
| 🕸️ **SpiderFoot** | Full OSINT automation (IPs, emails, leaks, domains) |
| 🌍 **Maltego** | Visual link analysis of people, infra, social, etc. |
| 📷 **ExifTool** | Pulls metadata (like GPS, camera info) from photos |
| 🌐 **Amass** | Subdomain enumeration, infrastructure mapping |
| 🌐 **Shodan** | Finds exposed devices & services on the internet |
| 📡 **FOCA** | Metadata from docs (PDF, DOCX) for names, servers |
| 📮 **EmailRep.io** | Checks email reputation (spam, leaks, social links) |
| 🔓 **Censys.io** | Similar to Shodan, for finding devices and services |
| 💬 **OSINTgram** | Instagram profiling and scraping |
| 👥 **Sherlock** | Find usernames across 300+ social networks |
| 🧑‍💼 **GHunt** | OSINT on Gmail accounts (when publicly exposed) |

**🧠 Summary Table**

| **Tool** | **Focus** | **Usage** |
| --- | --- | --- |
| **Creepy** | Geo-tracking | Social media & image metadata |
| **TheHarvester** | Email & domain recon | Company footprinting |
| **Recon-ng** | Recon framework | Custom recon workflows |
| **Others** | Various | Social, DNS, IP, metadata, leaks |

**✅ Next Steps**