🧰DarkMirror Tool Scripts

Collection of stealth-focused scripts for OPSEC and anonymity. Place these inside the `4_Tools/` directory.

🔧ghost_mac.sh

```
#!/bin/bash

iface=$(ip route | grep default | awk '{print $5}')

if [ -z "$iface" ]; then
  echo "[!] No active interface found."
  exit 1
fi

echo "[*] Spoofing MAC address on $iface..."
sudo ip link set $iface down
sudo macchanger -r $iface
sudo ip link set $iface up

echo "[+] MAC address randomized."
```

> Use to randomize MAC address and reduce traceability before network activity.

🧹vanish.sh

```
#!/bin/bash

echo "[*] Scanning for image files with metadata..."
find . -type f \( -iname "*.jpg" -o -iname "*.png" \) -print0 | while IFS= read -r -d '' file; do
  echo "[-] Cleaning: $file"
  exiftool -all= "$file" > /dev/null
  rm -f "${file}_original"
done

echo "[+] Metadata nuked from all images."
```

> Use to strip EXIF and hidden metadata from images (JPG/PNG) recursively.

🩲paranoid_dns.py

```
import requests

print("🔍 Checking DNS/IP exposure...")
try:
    ip = requests.get("https://api.ipify.org").text
    print(f"🩲 Public IP: {ip}")
    print("🔗 Visit https://dnsleaktest.com in Tails/Whonix for full DNS test.")
except Exception as e:
    print("[!] Error checking IP: ", e)
```

Simple Python script to check your public IP and remind you to perform DNS leak testing.

🛠️**All scripts are built for Linux environments.** Run them inside a safe VM or a live OS like Tails/Whonix.

"One command can save you. Or expose you. Choose wisely."