Instructions for using the Network Capture Tool:

Password for ZIP file: "time2sniff".

scadafence-sniffer-windows.py - Sniffer software for the Windows operating system.

scadafence-sniffer-linux.py - Sniffer software for the Linux operating system.

license.txt – License file (GPLv3)

Prerequisites:

1. Install Wireshark

2. Install Python 2.7

Instructions:

1. Run: python scadafence-sniffer-windows.py (for Linux, use the Linux version)
2. You should see the different network interfaces and usage instructions.
3. Choose the network interface you want to sniff on.
4. Run: python scadafence-sniffer-windows.py "NETWORK_INTERFACE" "TARGET_DIRECTORY"

   NETWORK_INTERFACE - the network interface you want to sniff on

   TARGET_DIRECTORY - where to save the sniffs.

   In the target directory, you should start seeing pcap/pcap.gz files.
5. Whenever you want to stop the sniffing, press Ctrl+C, and the sniffer will stop. The files will be ready in the target directory.

Remarks:

1. When the number of pap files passes 5, they’re automatically compressed to gzip files.

2. The format is a standard pcap compatible with Wireshark.

3. The file size, before compression, is 100MB per file.

4. Make sure you have enough free space on the target disk.

5. Each pcap/pcap.gz file is timestamped.

6. Log file will be saved to dumpcap.log in the directory with the capture files

7. Running on Linux might require sudo/root user. Running on Windows might require administrator access.

8. On some Linux distributions, by default a user can't capture pcap files into their home directory. Use /tmp for that instead (see Linux example)

9. The tool will update its status every 10 seconds.

Example run - Windows

```
C:\Users\User\Desktop>mkdir sniffs

C:\Users\User\Desktop>python scadafence_sniffer_windows.py
Usage: "scadafence_sniffer_windows.py" "<interface-to-use>" "<path-to-sniffs>"
Available interfaces:
1. \Device\NPF_{AF09BD23-51F2-4058-8686-BB62D5672B00} (VirtualBox Host-Only Network #2)
2. \Device\NPF_{80E8DF68-56C1-4F63-8862-265F2848C05E} (Local Area Connection* 11)
3. \Device\NPF_{30810402-05BC-4101-9F65-805BD3EAD9EC} (Bluetooth Network Connection)
4. \Device\NPF_{B149DF12-79BA-4344-B6BD-52F10D44A4EB} (Wi-Fi)

C:\Users\User\Desktop>python scadafence_sniffer_windows.py 4 sniffs
Pcap files: 1 Pcap.gz files: 0
```

Example run - Linux

```
user@srv1:~$ sudo mkdir /tmp/sniffs

user@srv1:~$ sudo python scadafence_sniffer_linux.py

Usage: "scadafence_sniffer_linux.py" "<interface-to-use>" "<path-to-sniffs>"

Available interfaces:

1. vboxnet0

2. eno1

3. eno2

4. any

user@srv1:~$ sudo python scadafence_sniffer_linux.py 2 /tmp/sniffs

Pcap files: 30 Pcap.gz files: 0

Mon Nov 25 16:27:50 2019 gzipping /tmp/sniffs/sniff_00007_20191125162746.pcap.

Mon Nov 25 16:27:50 2019 gzipping /tmp/sniffs/sniff_00011_20191125162746.pcap.


...
```

Troubleshooting:

If after the first 10 seconds the tool reports:

```
Pcap files: 0 Pcap.gz files: 0
No new pcap files were detected, waiting...
```

Please check the log file. It's usually a file permissions issue. If you're on Linux, try to write to /tmp instead of the user's home folder as specific in the Linux example.

And create the /tmp/sniffs directory using sudo (also specified in the Linux example).Any other errors - check the output of the tool or the log file. Most errors are due to permission issues