■ PCAP Quick Profiler — Cheat Sheet (Windows)

■ Basic Usage

```
python .\pcap_profiler.py "C:\path\to\capture.pcap" python .\pcap_profiler.py
"C:\path\to\capture.pcap" --top 10
```

■ Output Options

```
--json results.json Save full structured JSON --csv results.csv Save top IP/port summary
as CSV > summary.txt Redirect output to file (default) Autosaves to
security-tools\reports\pcap-profiler\
```

■■ Automatic Saving

```
Reports saved to: security-tools\reports\pcap-profiler\ capture_YYYYMMDD-HHMMSS.txt
capture_YYYYMMDD-HHMMSS.json capture_YYYYMMDD-HHMMSS.csv Disable autosave: python
.\pcap_profiler.py "C:\...\capture.pcap" --no-autosave Custom folder: python
.\pcap_profiler.py "C:\...\capture.pcap" --outdir "C:\Custom\Folder"
```

■■ Config Profiles

```
Example: pcap_profiler.config.json { "default_profile": "standard", "profiles": {
"standard": { "top": 10, "http_ports": [80, 8080, 8000], "tls_ports": [443, 8443],
"decode": ["tcp.port==36050,http"] } } } Run with: python .\pcap_profiler.py
"C:\...\capture.pcap" --profile standard
```

■ Decode Custom Protocols

```
Decode custom ports: python .\pcap_profiler.py "C:\...\capture.pcap" --decode
tcp.port==36050,http python .\pcap_profiler.py "C:\...\capture.pcap" --decode
tcp.port==36050,http --decode tcp.port==8443,tls
```

■ Troubleshooting

```
tshark not found → Install Wireshark and enable 'TShark' Event loop errors → Fixed in
Windows-compatible version No data → May only contain TCP, not HTTP/TLS
```

■ Example Workflow

```
cd "C:\Users\brand\Desktop\Projects\security-tools\tools\Pcap-profiler" python
.\pcap_profiler.py "C:\Users\brand\Desktop\capture.pcap" --top 10 explorer
..\..\reports\pcap-profiler
```

■ PowerShell Alias

```
Add to PowerShell $PROFILE: Set-Alias pprof
"C:\Users\brand\Desktop\Projects\security-tools\tools\Pcap-profiler\pcap_profiler.py"
Then run: pprof "C:\Users\brand\Desktop\capture.pcap" --top 10
```