

tshark



context

dit document geeft enkele voorbeelden van tshark op Windows

algemeen

- open Powerhell-as-admin en voer uit: tshark

interfaces

- toon beschikbare interfaces

```
tshark.exe -D
1. \Device\NPF_{3A86E79A-7F23-4E5C-9E22-1408BFF518DD} (Local Area
Connection* 9)
2. \Device\NPF_{01D3BE70-4407-46DD-8503-6C71BDACA45F} (Local Area
Connection* 8)
3. \Device\NPF_{1F192FFE-43E8-4C71-90EE-6AC54CE8CFBD} (Local Area
Connection* 7)
4. \Device\NPF_{B4048E4F-0C6A-488F-9BC7-AE809EC8CE08} (Ethernet0)
5. \Device\NPF_Loopback (Adapter for loopback traffic capture)
6. etwdump (Event Tracing for Windows (ETW) reader)
```

- luister op specifieke NIC: tshark.exe -i <nummer>

filter

-f "<filter>" voorbeeld:

```
tshark.exe -i <interface_id> -f "port 443"
```

weergaveformat

- geeft aan welke velden je in je capture wilt zien:
- -T fields
 - -e frame.time
 - -e ip.src
 - -e ip.dst
 - -e tcp.srcport
 - -e tcp.dstport
 - -e udp.srcport
 - -e udp.dstport
 - -e frame.len

voorbeeld:

```
tshark.exe -i 1 -f "port 443" -T fields -e frame.time -e ip.src -e ip.dst -e tcp.srcport -e tcp.dstport -e udp.srcport -e udp.dstport -e frame.len
```

tijd

- -t r: tijd sinds begin van capture

redirect naar log

```
tshark -i 1 |tee -Append -FilePath <log>
```

voorbeeld:

```
tshark -i 1 hostname joske and port 22|Tee-object -FilePath C:\Users\polleke\tshark.log
```

meer info

voeg hier linken toe naar verdere uitleg

[Linux](#)

From:
<https://louslab.be/> - Lou's lab

Permanent link:
https://louslab.be/doku.php?id=linux:tshark_op_windows&rev=1759480139

Last update: **2025/10/03 08:28**

