tshark

context

dit document geeft enkele voorbeelden van tshark op Windows

algemeen

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

interfaces

- toon beschikbaare 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"
```

redirect naar log

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

Important: optie -l zorgt ervoor dat output **niet** gebufferd wordt

voorbeeld:

```
tshark -i 1 -l hostname joske|tee -FilePath C:\Users\polleke\tshark.log
```

meer info

voeg hier linken toe naar verdere uitleg

Linux