VERKON VALVONTA: PHYSIO-WEBSOVELLUS, WIRESHARK JA NMAP

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi valvomalla tietoverkkoa hyödyntämällä erilaisia analysointityökaluja kuten kolmannen osapuolen ohjelmia, esimerkiksi Wiresharkia (Wireshark Foundation, 2025).

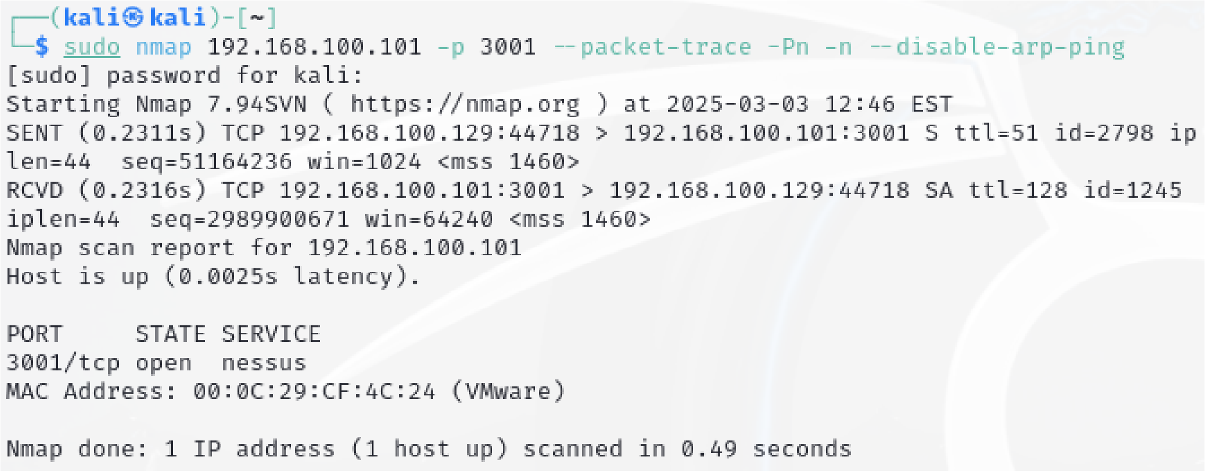
Ympäristönä oli Windows-palvelin, wks2-physio-työasema ja Kali Linux-kone VMwaressa. Toteutettiin verkonvalvonnan suunnitelmasta (liite 4a) poikkeavan verkkoliikenteen havaitseminen työasemassa Wiresharkilla siten, että skannataan Kali Linux-koneen Nmapilla Physio-websovelluksen (Github, 2025) porttia 3001.

2 SYN-skannaus

Tutkittiin porttia 3001 SYN-skannauksella:

sudo nmap 192.168.100.101 -p 3001 --packet-trace -Pn -n --disable-arp-ping

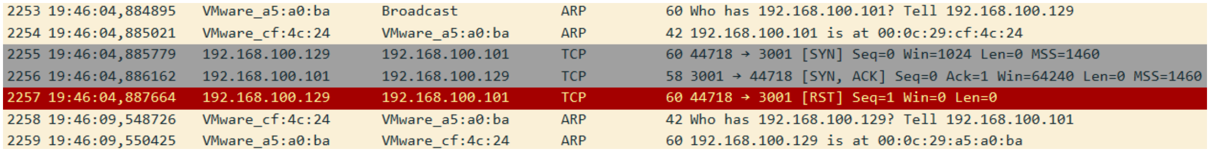
Nmapilla nähtiin SYN-skannaus ja SYN, ACK-vastaus siihen:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 3001 --packet-trace -Pn -n --disable-arp-ping
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-03 12:46 EST
SENT (0.2311s) TCP 192.168.100.129:44718 > 192.168.100.101:3001 S ttl=51 id=2798 ip
len=44  seq=51164236 win=1024 <mss 1460>
RCVD (0.2316s) TCP 192.168.100.101:3001 > 192.168.100.129:44718 SA ttl=128 id=1245
iplen=44  seq=2989900671 win=64240 <mss 1460>
Nmap scan report for 192.168.100.101
Host is up (0.0025s latency).

PORT     STATE SERVICE
3001/tcp open  nessus
MAC Address: 00:0C:29:CF:4C:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Nähtiin portin olevan auki ja jostain syystä palveluksi saatiin Nessus.

Työaseman Wiresharkilla nähtiin TCP:t ja ARP:t:



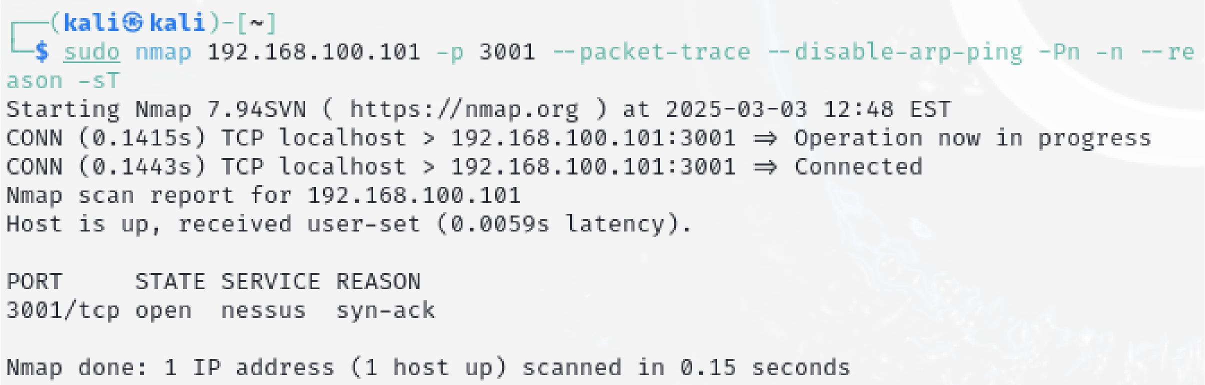
```
2253 19:46:04,884895   VMware_a5:a0:ba    Broadcast          ARP        60 Who has 192.168.100.101? Tell 192.168.100.129
2254 19:46:04,885021   VMware_cf:4c:24    VMware_a5:a0:ba    ARP        42 192.168.100.101 is at 00:0c:29:cf:4c:24
2255 19:46:04,885779   192.168.100.129    192.168.100.101    TCP        60 44718 → 3001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2256 19:46:04,886162   192.168.100.101    192.168.100.129    TCP        58 3001 → 44718 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2257 19:46:04,887664   192.168.100.129    192.168.100.101    TCP        60 44718 → 3001 [RST] Seq=1 Win=0 Len=0
2258 19:46:09,548726   VMware_cf:4c:24    VMware_a5:a0:ba    ARP        42 Who has 192.168.100.129? Tell 192.168.100.101
2259 19:46:09,550425   VMware_a5:a0:ba    VMware_cf:4c:24    ARP        60 192.168.100.129 is at 00:0c:29:a5:a0:ba
```

3 TCP-skannaus

Tehtiin TCP-skannaus porttiin 3001:

sudo nmap 192.168.100.101 -p 3001 --packet-trace --disable-arp-ping -Pn -n --reason -sT

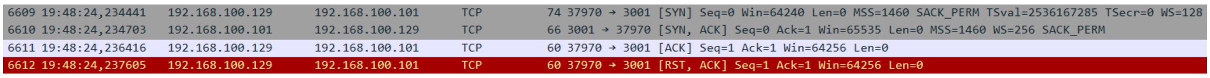
Nmapilla nähtiin kaksi TCP-skannausta, joista toisella yhteys onnistuu:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 3001 --packet-trace --disable-arp-ping -Pn -n --re
ason -sT
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-03 12:48 EST
CONN (0.1415s) TCP localhost > 192.168.100.101:3001 => Operation now in progress
CONN (0.1443s) TCP localhost > 192.168.100.101:3001 => Connected
Nmap scan report for 192.168.100.101
Host is up, received user-set (0.0059s latency).

PORT     STATE SERVICE REASON
3001/tcp open  nessus  syn-ack

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Nähtiin edelleen portin olevan auki ja palveluna yhä Nessus.

Wiresharkilla nähdään 3-osainen TCP-kättely ja yhteyden lopetus:



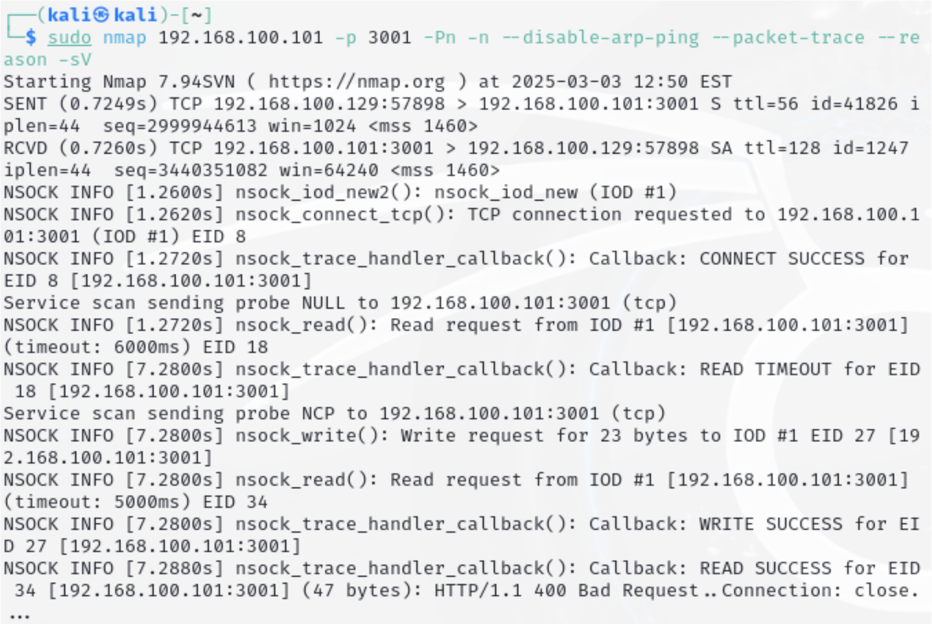
```
6609 19:48:24,234441   192.168.100.129   192.168.100.101   TCP       74 37970 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536167285 TSecr=0 WS=128
6610 19:48:24,234703   192.168.100.101   192.168.100.129   TCP       66 3001 → 37970 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
6611 19:48:24,236416   192.168.100.129   192.168.100.101   TCP       60 37970 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
6612 19:48:24,237605   192.168.100.129   192.168.100.101   TCP       60 37970 → 3001 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
```

4 Versioskannaus

Tehtiin versioskannaus porttiin 3001:

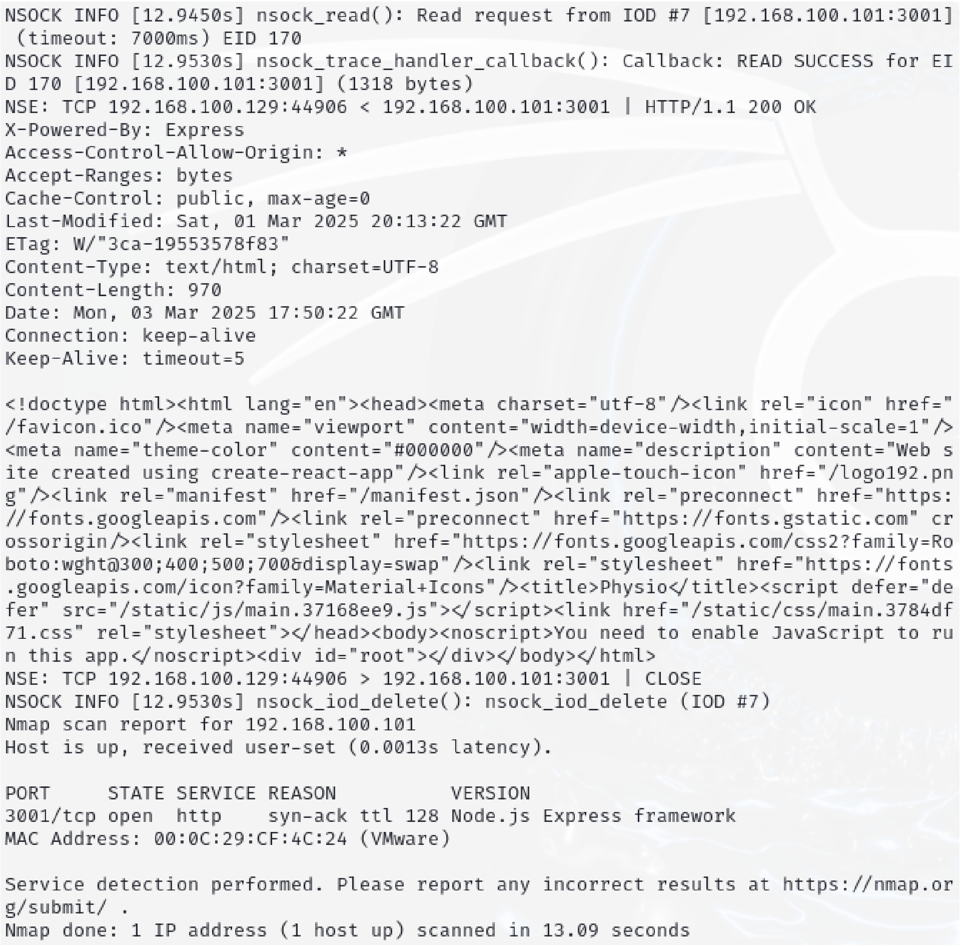
sudo nmap 192.168.100.101 -p 445 -Pn -n --disable-arp-ping --packet-trace --reason -sV

Nmapilla saatiin Physio-websovelluksen sisältöä sekä palveluksi oikein HTTP ja versioksi Node.js Express framework, jolla Physio-websovellus on tehty:



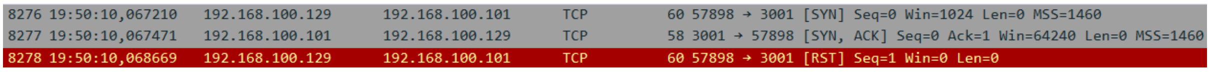
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 3001 -Pn -n --disable-arp-ping --packet-trace --re
ason -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-03 12:50 EST
SENT (0.7249s) TCP 192.168.100.129:57898 > 192.168.100.101:3001 S ttl=56 id=41826 i
plen=44  seq=2999944613 win=1024 <mss 1460>
RCVD (0.7260s) TCP 192.168.100.101:3001 > 192.168.100.129:57898 SA ttl=128 id=1247
iplen=44  seq=3440351082 win=64240 <mss 1460>
NSOCK INFO [1.2600s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [1.2620s] nsock_connect_tcp(): TCP connection requested to 192.168.100.1
01:3001 (IOD #1) EID 8
NSOCK INFO [1.2720s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for
EID 8 [192.168.100.101:3001]
Service scan sending probe NULL to 192.168.100.101:3001 (tcp)
NSOCK INFO [1.2720s] nsock_read(): Read request from IOD #1 [192.168.100.101:3001]
(timeout: 6000ms) EID 18
NSOCK INFO [7.2800s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for EID
 18 [192.168.100.101:3001]
Service scan sending probe NCP to 192.168.100.101:3001 (tcp)
NSOCK INFO [7.2800s] nsock_write(): Write request for 23 bytes to IOD #1 EID 27 [19
2.168.100.101:3001]
NSOCK INFO [7.2800s] nsock_read(): Read request from IOD #1 [192.168.100.101:3001]
(timeout: 5000ms) EID 34
NSOCK INFO [7.2800s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EI
D 27 [192.168.100.101:3001]
NSOCK INFO [7.2880s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID
 34 [192.168.100.101:3001] (47 bytes): HTTP/1.1 400 Bad Request..Connection: close.
 ...
```

…



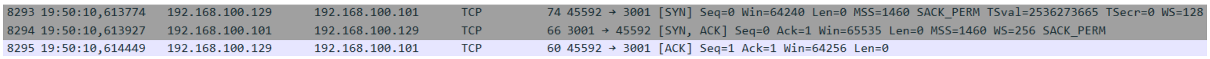
```
NSOCK INFO [12.9450s] nsock_read(): Read request from IOD #7 [192.168.100.101:3001]
 (timeout: 7000ms) EID 170
NSOCK INFO [12.9530s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EI
D 170 [192.168.100.101:3001] (1318 bytes)
NSE: TCP 192.168.100.129:44906 < 192.168.100.101:3001 | HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sat, 01 Mar 2025 20:13:22 GMT
ETag: W/"3ca-19553578f83"
Content-Type: text/html; charset=UTF-8
Content-Length: 970
Date: Mon, 03 Mar 2025 17:50:22 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="
/favicon.ico"/><meta name="viewport" content="width=device-width,initial-scale=1"/>
<meta name="theme-color" content="#000000"/><meta name="description" content="Web s
ite created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.pn
g"/><link rel="manifest" href="/manifest.json"/><link rel="preconnect" href="https:
//fonts.googleapis.com"/><link rel="preconnect" href="https://fonts.gstatic.com" cr
ossorigin/><link rel="stylesheet" href="https://fonts.googleapis.com/css2?family=Ro
boto:wght@300;400;500;700&display=swap"/><link rel="stylesheet" href="https://fonts
.googleapis.com/icon?family=Material+Icons"/><title>Physio</title><script defer="de
fer" src="/static/js/main.37168ee9.js"></script><link href="/static/css/main.3784df
71.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to ru
n this app.</noscript><div id="root"></div></body></html>
NSE: TCP 192.168.100.129:44906 > 192.168.100.101:3001 | CLOSE
NSOCK INFO [12.9530s] nsock_iod_delete(): nsock_iod_delete (IOD #7)
Nmap scan report for 192.168.100.101
Host is up, received user-set (0.0013s latency).

PORT     STATE SERVICE REASON          VERSION
3001/tcp open  http    syn-ack ttl 128 Node.js Express framework
MAC Address: 00:0C:29:CF:4C:24 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

Työaseman Wiresharkilla nähtiin TCP- ja HTTP-kyselyt ja vastaukset:



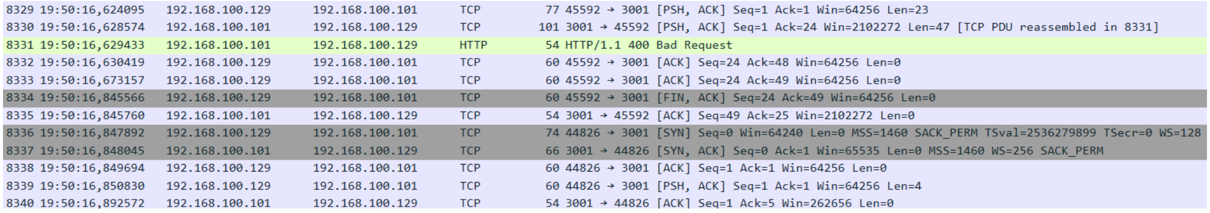
```
8276 19:50:10,067210   192.168.100.129   192.168.100.101   TCP     60 57898 → 3001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8277 19:50:10,067471   192.168.100.101   192.168.100.129   TCP     58 3001 → 57898 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
8278 19:50:10,068669   192.168.100.129   192.168.100.101   TCP     60 57898 → 3001 [RST] Seq=1 Win=0 Len=0
```

…



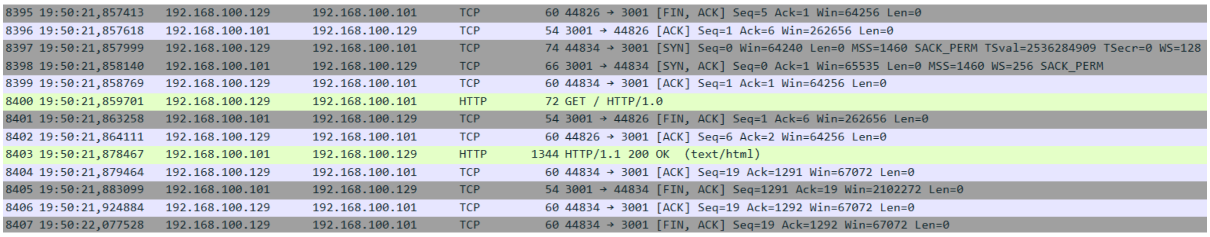
```
8293 19:50:10,613774   192.168.100.129   192.168.100.101   TCP     74 45592 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536273665 TSecr=0 WS=128
8294 19:50:10,613927   192.168.100.101   192.168.100.129   TCP     66 3001 → 45592 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8295 19:50:10,614449   192.168.100.129   192.168.100.101   TCP     60 45592 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
```

…



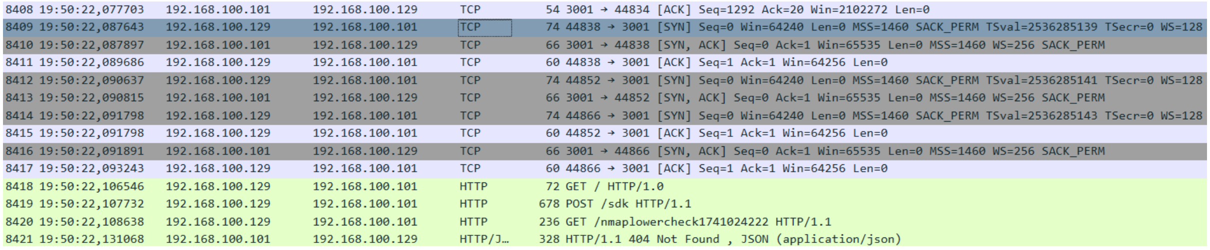
```
8329 19:50:16,624095   192.168.100.129   192.168.100.101   TCP     77 45592 → 3001 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=23
8330 19:50:16,628574   192.168.100.101   192.168.100.129   TCP    101 3001 → 45592 [PSH, ACK] Seq=1 Ack=24 Win=2102272 Len=47 [TCP PDU reassembled in 8331]
8331 19:50:16,629433   192.168.100.101   192.168.100.129   HTTP    54 HTTP/1.1 400 Bad Request
8332 19:50:16,630419   192.168.100.129   192.168.100.101   TCP     60 45592 → 3001 [ACK] Seq=24 Ack=48 Win=64256 Len=0
8333 19:50:16,673157   192.168.100.129   192.168.100.101   TCP     60 45592 → 3001 [ACK] Seq=24 Ack=49 Win=64256 Len=0
8334 19:50:16,845566   192.168.100.129   192.168.100.101   TCP     60 45592 → 3001 [FIN, ACK] Seq=24 Ack=49 Win=64256 Len=0
8335 19:50:16,845760   192.168.100.101   192.168.100.129   TCP     54 3001 → 45592 [ACK] Seq=49 Ack=25 Win=2102272 Len=0
8336 19:50:16,847892   192.168.100.129   192.168.100.101   TCP     74 44826 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536279899 TSecr=0 WS=128
8337 19:50:16,848045   192.168.100.101   192.168.100.129   TCP     66 3001 → 44826 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8338 19:50:16,849694   192.168.100.129   192.168.100.101   TCP     60 44826 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8339 19:50:16,850830   192.168.100.129   192.168.100.101   TCP     60 44826 → 3001 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4
8340 19:50:16,892572   192.168.100.101   192.168.100.129   TCP     54 3001 → 44826 [ACK] Seq=1 Ack=5 Win=262656 Len=0
```

…

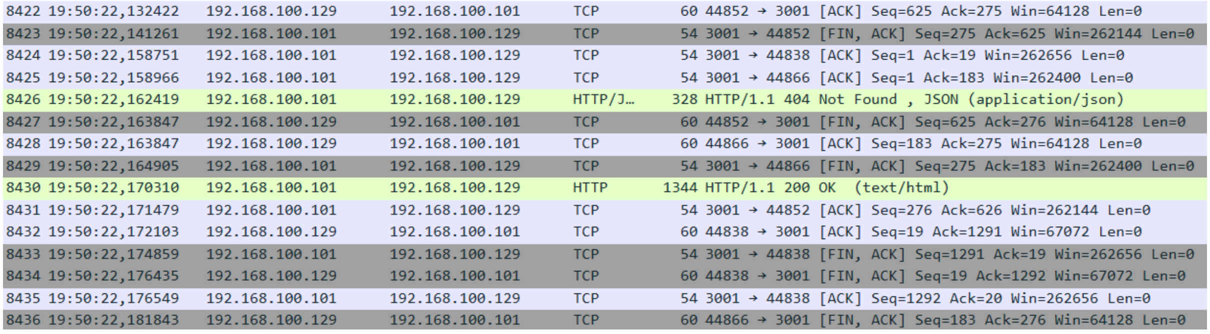


```
8395 19:50:21,857413   192.168.100.129   192.168.100.101   TCP     60 44826 → 3001 [FIN, ACK] Seq=5 Ack=1 Win=64256 Len=0
8396 19:50:21,857618   192.168.100.101   192.168.100.129   TCP     54 3001 → 44826 [ACK] Seq=1 Ack=6 Win=262656 Len=0
8397 19:50:21,857999   192.168.100.129   192.168.100.101   TCP     74 44834 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536284909 TSecr=0 WS=128
8398 19:50:21,858140   192.168.100.101   192.168.100.129   TCP     66 3001 → 44834 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8399 19:50:21,858769   192.168.100.129   192.168.100.101   TCP     60 44834 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8400 19:50:21,859701   192.168.100.129   192.168.100.101   HTTP    72 GET / HTTP/1.0
8401 19:50:21,863258   192.168.100.101   192.168.100.129   TCP     54 3001 → 44826 [FIN, ACK] Seq=1 Ack=6 Win=262656 Len=0
8402 19:50:21,864111   192.168.100.129   192.168.100.101   TCP     60 44826 → 3001 [ACK] Seq=6 Ack=2 Win=64256 Len=0
8403 19:50:21,878467   192.168.100.101   192.168.100.129   HTTP  1344 HTTP/1.1 200 OK  (text/html)
8404 19:50:21,879464   192.168.100.129   192.168.100.101   TCP     60 44834 → 3001 [ACK] Seq=19 Ack=1291 Win=67072 Len=0
8405 19:50:21,883099   192.168.100.101   192.168.100.129   TCP     54 3001 → 44834 [FIN, ACK] Seq=1291 Ack=19 Win=2102272 Len=0
8406 19:50:21,924884   192.168.100.129   192.168.100.101   TCP     60 44834 → 3001 [ACK] Seq=19 Ack=1292 Win=67072 Len=0
8407 19:50:22,077528   192.168.100.129   192.168.100.101   TCP     60 44834 → 3001 [FIN, ACK] Seq=19 Ack=1292 Win=67072 Len=0
```

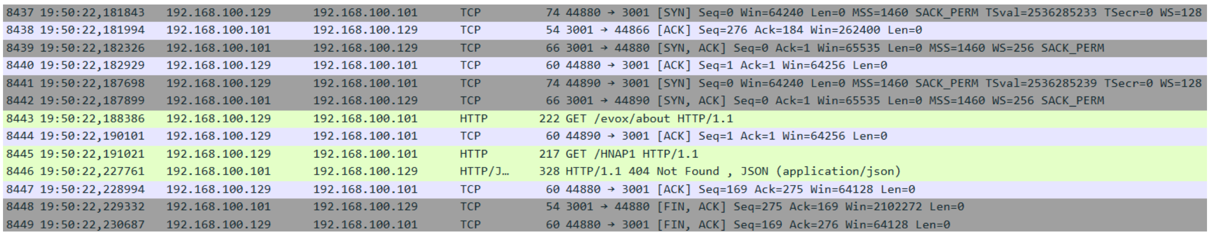
LIITE 4c



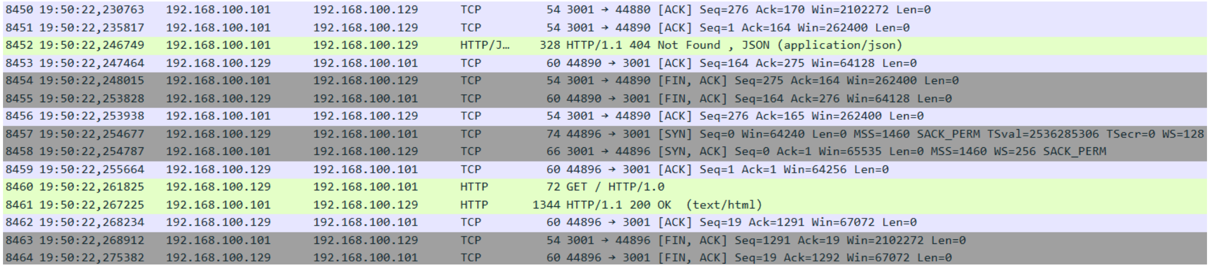
```
8408 19:50:22,077703   192.168.100.101   192.168.100.129   TCP       54 3001 → 44834 [ACK] Seq=1292 Ack=20 Win=2102272 Len=0
8409 19:50:22,087643   192.168.100.129   192.168.100.101   TCP       74 44838 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285139 TSecr=0 WS=128
8410 19:50:22,087897   192.168.100.101   192.168.100.129   TCP       66 3001 → 44838 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8411 19:50:22,089686   192.168.100.129   192.168.100.101   TCP       60 44838 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8412 19:50:22,090637   192.168.100.129   192.168.100.101   TCP       74 44852 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285141 TSecr=0 WS=128
8413 19:50:22,090815   192.168.100.101   192.168.100.129   TCP       66 3001 → 44852 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8414 19:50:22,091798   192.168.100.129   192.168.100.101   TCP       74 44866 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285143 TSecr=0 WS=128
8415 19:50:22,091798   192.168.100.129   192.168.100.101   TCP       60 44852 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8416 19:50:22,091891   192.168.100.101   192.168.100.129   TCP       66 3001 → 44866 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8417 19:50:22,093243   192.168.100.129   192.168.100.101   TCP       60 44866 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8418 19:50:22,106546   192.168.100.129   192.168.100.101   HTTP      72 GET / HTTP/1.0
8419 19:50:22,107732   192.168.100.129   192.168.100.101   HTTP     678 POST /sdk HTTP/1.1
8420 19:50:22,108638   192.168.100.129   192.168.100.101   HTTP     236 GET /nmaplowercheck1741024222 HTTP/1.1
8421 19:50:22,131068   192.168.100.101   192.168.100.129   HTTP/J…  328 HTTP/1.1 404 Not Found , JSON (application/json)
```



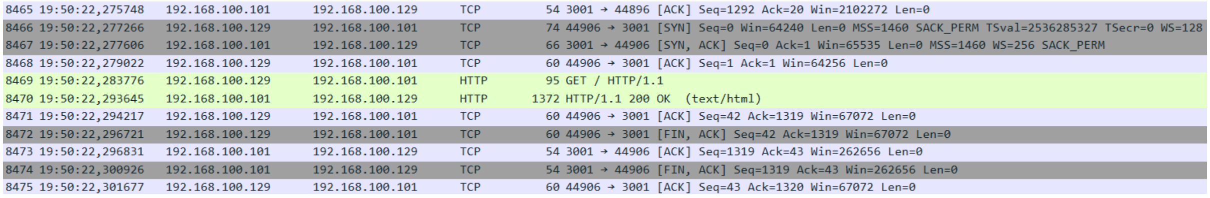
```
8422 19:50:22,132422   192.168.100.129   192.168.100.101   TCP       60 44852 → 3001 [ACK] Seq=625 Ack=275 Win=64128 Len=0
8423 19:50:22,141261   192.168.100.101   192.168.100.129   TCP       54 3001 → 44852 [FIN, ACK] Seq=275 Ack=625 Win=262144 Len=0
8424 19:50:22,158751   192.168.100.101   192.168.100.129   TCP       54 3001 → 44838 [ACK] Seq=1 Ack=19 Win=262656 Len=0
8425 19:50:22,158966   192.168.100.101   192.168.100.129   TCP       54 3001 → 44866 [ACK] Seq=1 Ack=183 Win=262400 Len=0
8426 19:50:22,162419   192.168.100.101   192.168.100.129   HTTP/J…  328 HTTP/1.1 404 Not Found , JSON (application/json)
8427 19:50:22,163847   192.168.100.129   192.168.100.101   TCP       60 44852 → 3001 [FIN, ACK] Seq=625 Ack=276 Win=64128 Len=0
8428 19:50:22,163847   192.168.100.129   192.168.100.101   TCP       60 44866 → 3001 [ACK] Seq=183 Ack=275 Win=64128 Len=0
8429 19:50:22,164905   192.168.100.101   192.168.100.129   TCP       54 3001 → 44866 [FIN, ACK] Seq=275 Ack=183 Win=262400 Len=0
8430 19:50:22,170310   192.168.100.101   192.168.100.129   HTTP    1344 HTTP/1.1 200 OK  (text/html)
8431 19:50:22,171479   192.168.100.101   192.168.100.129   TCP       54 3001 → 44852 [ACK] Seq=276 Ack=626 Win=262144 Len=0
8432 19:50:22,172103   192.168.100.129   192.168.100.101   TCP       60 44838 → 3001 [ACK] Seq=19 Ack=1291 Win=67072 Len=0
8433 19:50:22,174859   192.168.100.101   192.168.100.129   TCP       54 3001 → 44838 [FIN, ACK] Seq=1291 Ack=19 Win=262656 Len=0
8434 19:50:22,176435   192.168.100.129   192.168.100.101   TCP       60 44838 → 3001 [FIN, ACK] Seq=19 Ack=1292 Win=67072 Len=0
8435 19:50:22,176549   192.168.100.101   192.168.100.129   TCP       54 3001 → 44838 [ACK] Seq=1292 Ack=20 Win=262656 Len=0
8436 19:50:22,181843   192.168.100.129   192.168.100.101   TCP       60 44866 → 3001 [FIN, ACK] Seq=183 Ack=276 Win=64128 Len=0
```



```
8437 19:50:22,181843   192.168.100.129   192.168.100.101   TCP       74 44880 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285233 TSecr=0 WS=128
8438 19:50:22,181994   192.168.100.101   192.168.100.129   TCP       54 3001 → 44866 [ACK] Seq=276 Ack=184 Win=262400 Len=0
8439 19:50:22,182326   192.168.100.101   192.168.100.129   TCP       66 3001 → 44880 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8440 19:50:22,182929   192.168.100.129   192.168.100.101   TCP       60 44880 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8441 19:50:22,187698   192.168.100.129   192.168.100.101   TCP       74 44890 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285239 TSecr=0 WS=128
8442 19:50:22,187899   192.168.100.101   192.168.100.129   TCP       66 3001 → 44890 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8443 19:50:22,188386   192.168.100.129   192.168.100.101   HTTP     222 GET /evox/about HTTP/1.1
8444 19:50:22,190101   192.168.100.129   192.168.100.101   TCP       60 44890 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8445 19:50:22,191021   192.168.100.129   192.168.100.101   HTTP     217 GET /HNAP1 HTTP/1.1
8446 19:50:22,227761   192.168.100.101   192.168.100.129   HTTP/J…  328 HTTP/1.1 404 Not Found , JSON (application/json)
8447 19:50:22,228994   192.168.100.129   192.168.100.101   TCP       60 44880 → 3001 [ACK] Seq=169 Ack=275 Win=64128 Len=0
8448 19:50:22,229332   192.168.100.101   192.168.100.129   TCP       54 3001 → 44880 [FIN, ACK] Seq=275 Ack=169 Win=2102272 Len=0
8449 19:50:22,230687   192.168.100.129   192.168.100.101   TCP       60 44880 → 3001 [FIN, ACK] Seq=169 Ack=276 Win=64128 Len=0
```

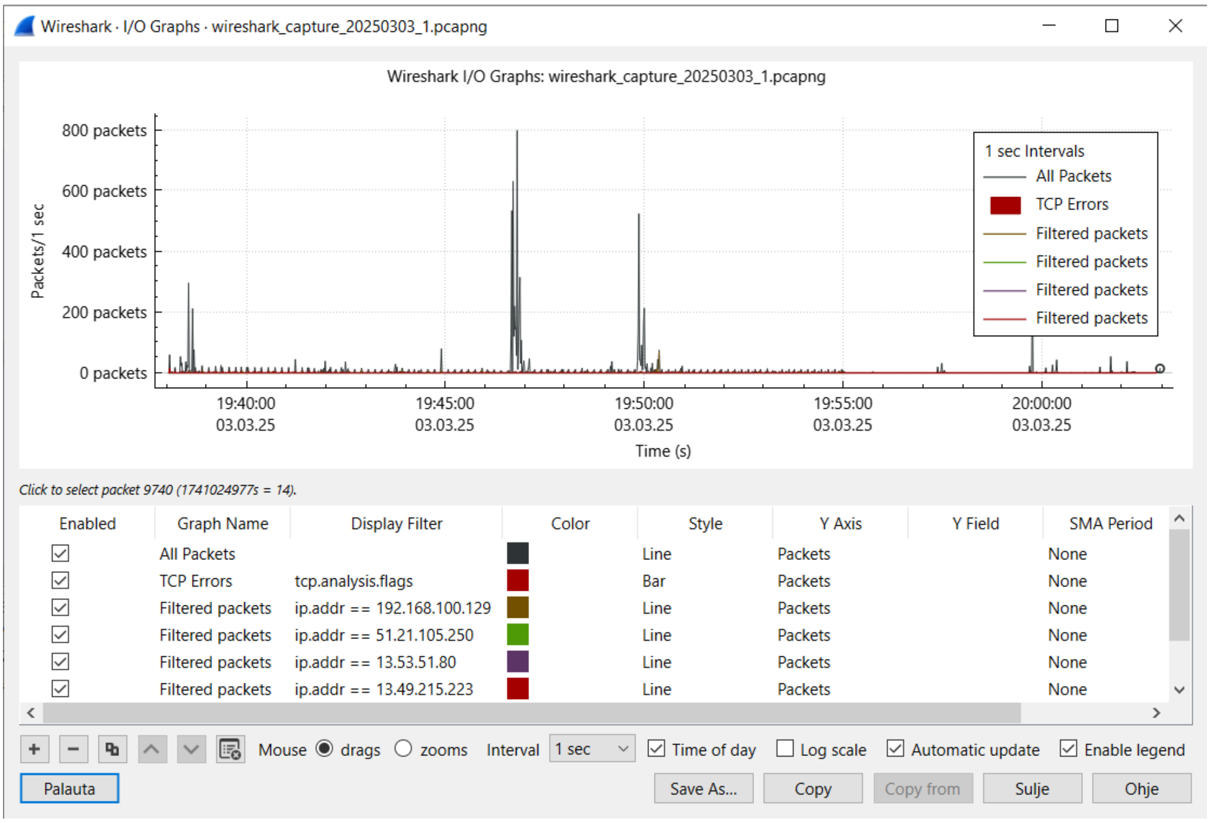


```
8450 19:50:22,230763   192.168.100.101   192.168.100.129   TCP       54 3001 → 44880 [ACK] Seq=276 Ack=170 Win=2102272 Len=0
8451 19:50:22,235817   192.168.100.101   192.168.100.129   TCP       54 3001 → 44890 [ACK] Seq=1 Ack=164 Win=262400 Len=0
8452 19:50:22,246749   192.168.100.101   192.168.100.129   HTTP/J…  328 HTTP/1.1 404 Not Found , JSON (application/json)
8453 19:50:22,247464   192.168.100.129   192.168.100.101   TCP       60 44890 → 3001 [ACK] Seq=164 Ack=275 Win=64128 Len=0
8454 19:50:22,248015   192.168.100.101   192.168.100.129   TCP       54 3001 → 44890 [FIN, ACK] Seq=275 Ack=164 Win=262400 Len=0
8455 19:50:22,253828   192.168.100.129   192.168.100.101   TCP       60 44890 → 3001 [FIN, ACK] Seq=164 Ack=276 Win=64128 Len=0
8456 19:50:22,253938   192.168.100.101   192.168.100.129   TCP       54 3001 → 44890 [ACK] Seq=276 Ack=165 Win=262400 Len=0
8457 19:50:22,254677   192.168.100.129   192.168.100.101   TCP       74 44896 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285306 TSecr=0 WS=128
8458 19:50:22,254787   192.168.100.101   192.168.100.129   TCP       66 3001 → 44896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8459 19:50:22,255664   192.168.100.129   192.168.100.101   TCP       60 44896 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8460 19:50:22,261825   192.168.100.129   192.168.100.101   HTTP      72 GET / HTTP/1.0
8461 19:50:22,267225   192.168.100.101   192.168.100.129   HTTP    1344 HTTP/1.1 200 OK  (text/html)
8462 19:50:22,268234   192.168.100.129   192.168.100.101   TCP       60 44896 → 3001 [ACK] Seq=19 Ack=1291 Win=67072 Len=0
8463 19:50:22,268912   192.168.100.101   192.168.100.129   TCP       54 3001 → 44896 [FIN, ACK] Seq=1291 Ack=19 Win=2102272 Len=0
8464 19:50:22,275382   192.168.100.129   192.168.100.101   TCP       60 44896 → 3001 [FIN, ACK] Seq=19 Ack=1292 Win=67072 Len=0
```



```
8465 19:50:22,275748   192.168.100.101   192.168.100.129   TCP       54 3001 → 44896 [ACK] Seq=1292 Ack=20 Win=2102272 Len=0
8466 19:50:22,277266   192.168.100.129   192.168.100.101   TCP       74 44906 → 3001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2536285327 TSecr=0 WS=128
8467 19:50:22,277606   192.168.100.101   192.168.100.129   TCP       66 3001 → 44906 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8468 19:50:22,279022   192.168.100.129   192.168.100.101   TCP       60 44906 → 3001 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8469 19:50:22,283776   192.168.100.129   192.168.100.101   HTTP      95 GET / HTTP/1.1
8470 19:50:22,293645   192.168.100.101   192.168.100.129   HTTP    1372 HTTP/1.1 200 OK  (text/html)
8471 19:50:22,294217   192.168.100.129   192.168.100.101   TCP       60 44906 → 3001 [ACK] Seq=42 Ack=1319 Win=67072 Len=0
8472 19:50:22,296721   192.168.100.129   192.168.100.101   TCP       60 44906 → 3001 [FIN, ACK] Seq=42 Ack=1319 Win=67072 Len=0
8473 19:50:22,296831   192.168.100.101   192.168.100.129   TCP       54 3001 → 44906 [ACK] Seq=1319 Ack=43 Win=262656 Len=0
8474 19:50:22,300926   192.168.100.101   192.168.100.129   TCP       54 3001 → 44906 [FIN, ACK] Seq=1319 Ack=43 Win=262656 Len=0
8475 19:50:22,301677   192.168.100.129   192.168.100.101   TCP       60 44906 → 3001 [ACK] Seq=43 Ack=1320 Win=67072 Len=0
```

Wiresharkissa näkyi säännöllistä pienempää liikennettä tietokantapalvelu MongoDB Atlasin kanssa:



Wireshark · I/O Graphs · wireshark_capture_20250303_1.pcapng

Wireshark I/O Graphs: wireshark_capture_20250303_1.pcapng

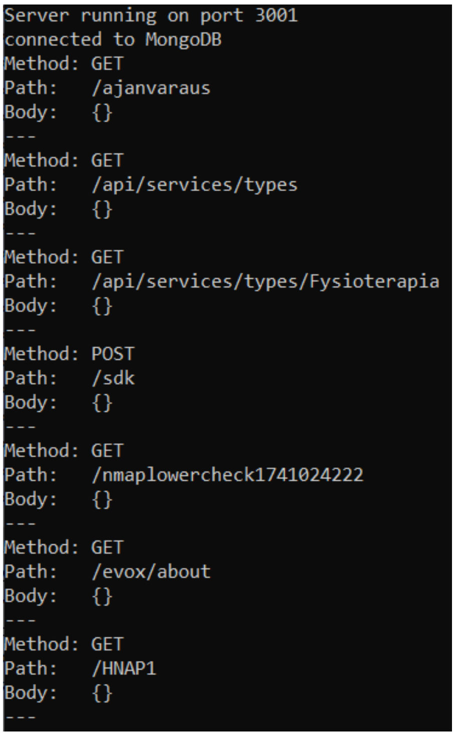
Click to select packet 9740 (1741024977s = 14).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		■	Line	Packets		None
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None
☑	Filtered packets	ip.addr == 192.168.100.129	🟫	Line	Packets		None
☑	Filtered packets	ip.addr == 51.21.105.250	🟩	Line	Packets		None
☑	Filtered packets	ip.addr == 13.53.51.80	🟪	Line	Packets		None
☑	Filtered packets	ip.addr == 13.49.215.223	🟥	Line	Packets		None

Mouse ● drags ○ zooms Interval 1 sec ☑ Time of day □ Log scale ☑ Automatic update ☑ Enable legend

Tietokantapalveluun liittyvät IP-osoitteet olivat: 13.49.215.223, 13.53.51.80 ja 51.21.105.250. Isoimmat piikit tulivat Microsoft Edgen aloitussivustosta msn.com.

Physion koodissa on console.log-käsky, joka printtaa käyttäjän pyynnön metodin, polun, bodyn ja '---', jonka vuoksi myös terminaalissa näkyi Nmapin http-kyselyt (POST /sdk, GET nmaplowercheck7410 24222, GET /evox/about, GET /HNAP1):



```
Server running on port 3001
connected to MongoDB
Method: GET
Path:   /ajanvaraus
Body:   {}
---
Method: GET
Path:   /api/services/types
Body:   {}
---
Method: GET
Path:   /api/services/types/Fysioterapia
Body:   {}
---
Method: POST
Path:   /sdk
Body:   {}
---
Method: GET
Path:   /nmaplowercheck1741024222
Body:   {}
---
Method: GET
Path:   /evox/about
Body:   {}
---
Method: GET
Path:   /HNAP1
Body:   {}
---
```

Otettiin wks2-työasemasta snapshot 20250304 ja tehtiin siitä backup ulkoiselle kovalevylle.

Lähdeluettelo

Github, I. (1. Maaliskuu 2025). *Github - hannahakonen/physio-web-pages*. Noudettu osoitteesta https://github.com/hannahakonen/physio-web-pages

Wireshark Foundation. (18. Helmikuu 2025). *Wireshark*. Noudettu osoitteesta https://www.wireshark.org/