

LABORATORIUM SIECI KOMPUTEROWYCH

Data wykonania ćwiczenia:

02.03.2023

Rok studiów:

2

Semestr:

4

Grupa studencka:

2

Grupa laboratoryjna:

2B

Ćwiczenie nr

2

Temat: Ogólne zasady funkcjonowania sieci komputerowej

Osoby wykonujące ćwiczenia:

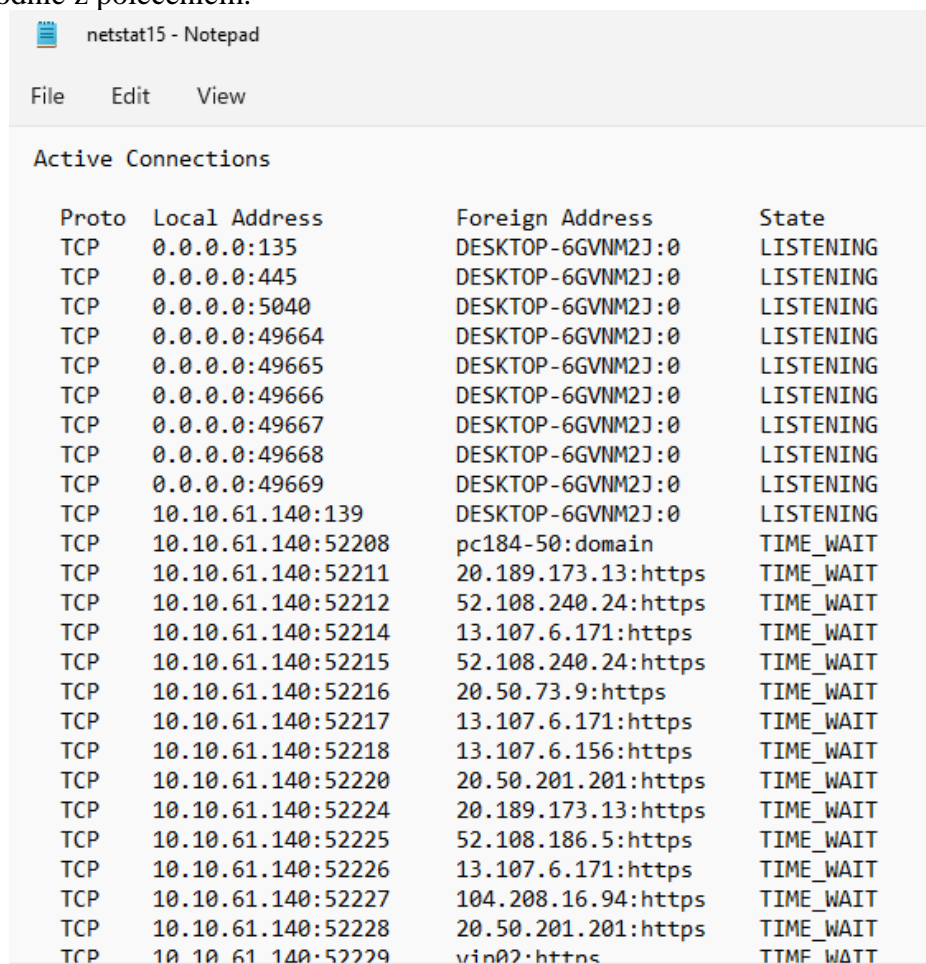
1. Igor Gawłowicz

Katedra Informatyki i Automatyki

1 Uzyskaj informacje o wszystkich połączeniach systemu operacyjnego i zapisz wszystkie wyniki do odpowiednich plików netstat*XX.txt. Zastąp znaki "XX" w nazwie pliku numerem podanym przez prowadzącego zajęcia.

Rozwiązanie:

Zacząłem od ustawienia ścieżki mojego pliku za pomocą instrukcji cd, następnie zapisałem wyniki zgodnie z poleceniem.



Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-6GVNM2J:0	LISTENING
TCP	0.0.0.0:49669	DESKTOP-6GVNM2J:0	LISTENING
TCP	10.10.61.140:139	DESKTOP-6GVNM2J:0	LISTENING
TCP	10.10.61.140:52208	pc184-50:domain	TIME_WAIT
TCP	10.10.61.140:52211	20.189.173.13:https	TIME_WAIT
TCP	10.10.61.140:52212	52.108.240.24:https	TIME_WAIT
TCP	10.10.61.140:52214	13.107.6.171:https	TIME_WAIT
TCP	10.10.61.140:52215	52.108.240.24:https	TIME_WAIT
TCP	10.10.61.140:52216	20.50.73.9:https	TIME_WAIT
TCP	10.10.61.140:52217	13.107.6.171:https	TIME_WAIT
TCP	10.10.61.140:52218	13.107.6.156:https	TIME_WAIT
TCP	10.10.61.140:52220	20.50.201.201:https	TIME_WAIT
TCP	10.10.61.140:52224	20.189.173.13:https	TIME_WAIT
TCP	10.10.61.140:52225	52.108.186.5:https	TIME_WAIT
TCP	10.10.61.140:52226	13.107.6.171:https	TIME_WAIT
TCP	10.10.61.140:52227	104.208.16.94:https	TIME_WAIT
TCP	10.10.61.140:52228	20.50.201.201:https	TIME_WAIT
TCP	10.10.61.140:52229	vin02:https	TIME_WAIT

Wycinek ekranu zawierający część wyników z zapisanego pliku.

1.1. Uzyskaj listę wszystkich połączeń sieciowych systemu operacyjnego i jego oprogramowania, zapisując wszystkie wyniki do pliku netstatsoftallXX.txt.

Rozwiązanie:

Kroki postępowania takie same jak w poprzednim podpunkcie.

```

netstatofall15 - Notepad
File Edit View

Active Connections

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 DESKTOP-6GVNM2J:0 LISTENING
RpcSs
[svchost.exe]
TCP 0.0.0.0:445 DESKTOP-6GVNM2J:0 LISTENING
Can not obtain ownership information
TCP 0.0.0.0:5040 DESKTOP-6GVNM2J:0 LISTENING
CDPSvc
[svchost.exe]
TCP 0.0.0.0:49664 DESKTOP-6GVNM2J:0 LISTENING
[lsass.exe]
TCP 0.0.0.0:49665 DESKTOP-6GVNM2J:0 LISTENING
Can not obtain ownership information
TCP 0.0.0.0:49666 DESKTOP-6GVNM2J:0 LISTENING
EventLog
[svchost.exe]
TCP 0.0.0.0:49667 DESKTOP-6GVNM2J:0 LISTENING
Schedule
[svchost.exe]
TCP 0.0.0.0:49668 DESKTOP-6GVNM2J:0 LISTENING
[spoolsv.exe]
TCP 0.0.0.0:49669 DESKTOP-6GVNM2J:0 LISTENING
Can not obtain ownership information
TCP 10.10.61.140:139 DESKTOP-6GVNM2J:0 LISTENING
Can not obtain ownership information
TCP 10.10.61.140:52301 20.50.73.11:https TIME_WAIT
In 9 Col 38

```

Wyniki wszystkich połączeń sieciowych.

1.2. Pobierz statystyki komunikacji Ethernet dla wszystkich adapterów sieciowych i zapisz wszystkie wyniki do pliku raportu netstatethernetXX.txt.

Wyniki po wprowadzeniu instrukcji: **netstat -e > netstatethernet15.txt**

```

netstatethernet15 - Notepad
File Edit View

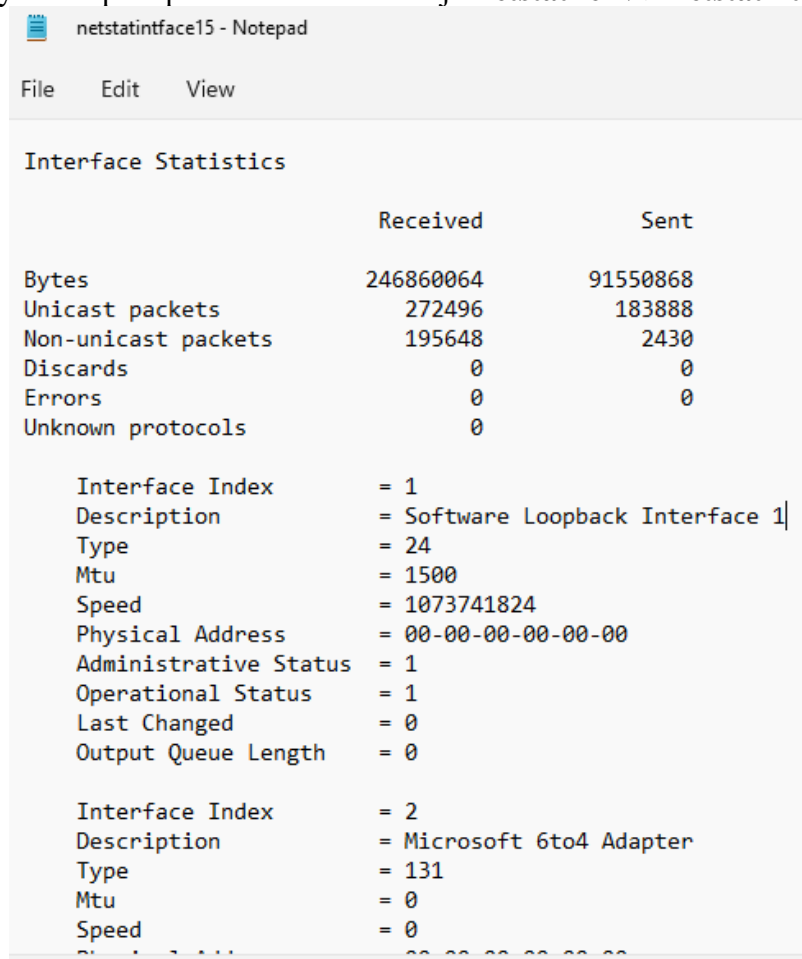
Interface Statistics

Received Sent
Bytes 238277958 83684106
Unicast packets 257634 173322
Non-unicast packets 183516 2304
Discards 0 0
Errors 0 0
Unknown protocols 0

```

1.3. Uzyskanie zbiorczych statystyk wymiany danych przez poszczególne interfejsy sieciowe z zapisem wszystkich wyników do pliku raportu netstatintfaceXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -e -v > netstatintface15.txt**



	Received	Sent
Bytes	246860064	91550868
Unicast packets	272496	183888
Non-unicast packets	195648	2430
Discards	0	0
Errors	0	0
Unknown protocols	0	
Interface Index	= 1	
Description	= Software Loopback Interface 1	
Type	= 24	
Mtu	= 1500	
Speed	= 1073741824	
Physical Address	= 00-00-00-00-00-00	
Administrative Status	= 1	
Operational Status	= 1	
Last Changed	= 0	
Output Queue Length	= 0	
Interface Index	= 2	
Description	= Microsoft 6to4 Adapter	
Type	= 131	
Mtu	= 0	
Speed	= 0	
Physical Address	= 00-00-00-00-00-00	

1.4. Uzyskanie łącznych danych statystycznych dla protokołów IP, ICMP, TCP, UDP z zapisaniem wszystkich wyników do pliku raportu netstatprotocolXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -e -s > netstatprotocol15.txt**

```
netstatprotocol - Notepad
File Edit View

Interface Statistics

                Received          Sent
Bytes          267200892        100187886
Unicast packets    296580        199368
Non-unicast packets 210072        2622
Discards          0            0
Errors            0            0
Unknown protocols  0

IPv4 Statistics

Packets Received          = 492427
Received Header Errors    = 0
Received Address Errors   = 5
Datagrams Forwarded       = 0
Unknown Protocols Received = 0
Received Packets Discarded = 39621
Received Packets Delivered = 488995
Output Requests           = 346438
Routing Discards          = 0
Discarded Output Packets  = 5
Output Packet No Route    = 86
Reassembly Required       = 0
Reassembly Successful     = 0
Reassembly Failures       = 0
```

1.5. Uzyskanie listy połączeń na portach TCP z zapisaniem wszystkich wyników pliku raportu netstattcpportsXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -a -t > netstatcpports15.txt**

netstatcpports15 - Notepad

File Edit View

Active Connections

Proto	Local Address	Foreign Address	State	Offload State
TCP	0.0.0.0:135	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:445	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:5040	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:49664	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:49665	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:49666	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:49667	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:49668	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	0.0.0.0:49669	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	10.10.61.140:139	DESKTOP-6GVNM2J:0	LISTENING	InHost
TCP	10.10.61.140:52310	52.114.74.211:https	ESTABLISHED	InHost
TCP	10.10.61.140:52614	13.107.6.171:https	TIME_WAIT	InHost
TCP	10.10.61.140:52615	52.108.79.33:https	TIME_WAIT	InHost
TCP	10.10.61.140:52616	13.107.6.171:https	TIME_WAIT	InHost
TCP	10.10.61.140:52617	20.50.80.209:https	TIME_WAIT	InHost
TCP	10.10.61.140:52618	52.108.79.33:https	TIME_WAIT	InHost
TCP	10.10.61.140:52619	20.50.201.200:https	TIME_WAIT	InHost
TCP	10.10.61.140:52620	13.107.6.171:https	TIME_WAIT	InHost
TCP	10.10.61.140:52621	20.50.201.200:https	TIME_WAIT	InHost
TCP	10.10.61.140:52622	13.107.6.171:https	TIME_WAIT	InHost
TCP	10.10.61.140:52623	20.50.201.200:https	TIME_WAIT	InHost
TCP	10.10.61.140:52624	13.107.6.171:https	TIME_WAIT	InHost

1.6. Uzyskanie tablicy routingu jądra z zapisaniem wszystkich wyników do pliku netstatyadroXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -r > netstatyadro15.txt**

netstatyadro15 - Notepad

File Edit View

```

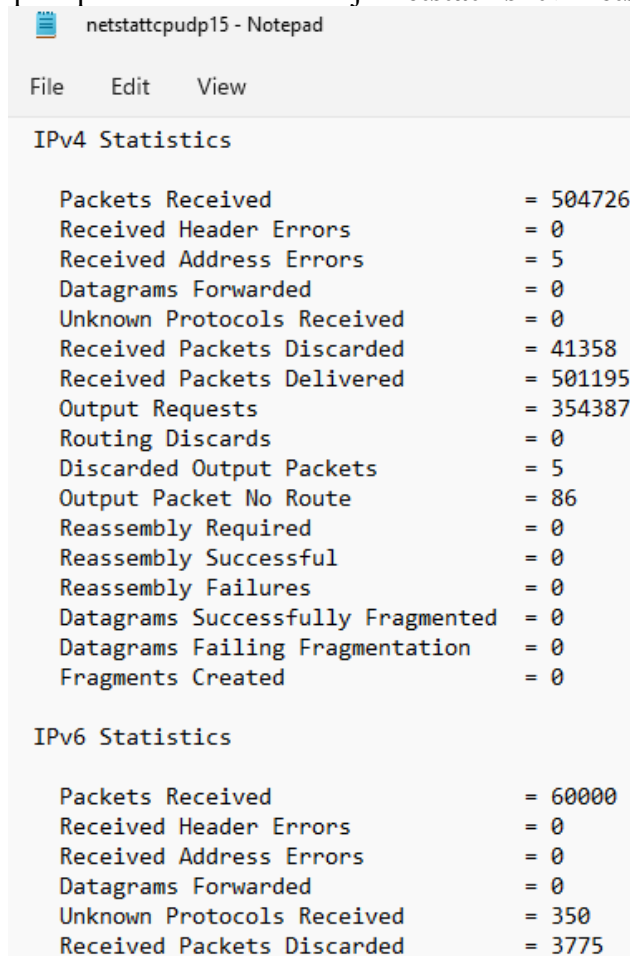
=====
Interface List
13...f8 a9 63 52 54 64 .....Realtek(R) PCI(e) Ethernet Controller
10...a0 a8 cd 08 8e 01 .....Microsoft Wi-Fi Direct Virtual Adapter
29...a2 a8 cd 08 8e 00 .....Microsoft Wi-Fi Direct Virtual Adapter #2
6...a0 a8 cd 08 8e 00 .....Intel(R) Wireless-N 7260
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          10.10.60.1        10.10.61.140     55
10.10.60.0                 255.255.252.0    On-link           10.10.61.140     311
10.10.61.140               255.255.255.255  On-link           10.10.61.140     311
10.10.63.255               255.255.255.255  On-link           10.10.61.140     311
127.0.0.0                  255.0.0.0        On-link           127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link           127.0.0.1        331
127.255.255.255            255.255.255.255  On-link           127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link           127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link           10.10.61.140     311
255.255.255.255            255.255.255.255  On-link           127.0.0.1        331
255.255.255.255            255.255.255.255  On-link           10.10.61.140     311
=====
Persistent Routes:
None

```

1.7. Uzyskanie statystyki tylko portów TCP i UDP z zapisaniem wszystkich wyników do pliku raportu netstattcpudpXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -s -t > netstattcpudp15.txt**



The screenshot shows a Notepad window with the title 'netstattcpudp15 - Notepad'. The window contains the output of the 'netstat -s -t' command, which displays network statistics for IPv4 and IPv6. The statistics are organized into two sections: 'IPv4 Statistics' and 'IPv6 Statistics'. Each section lists various network metrics and their corresponding values.

IPv4 Statistics	
Packets Received	= 504726
Received Header Errors	= 0
Received Address Errors	= 5
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 41358
Received Packets Delivered	= 501195
Output Requests	= 354387
Routing Discards	= 0
Discarded Output Packets	= 5
Output Packet No Route	= 86
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	= 0
Datagrams Successfully Fragmented	= 0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

IPv6 Statistics	
Packets Received	= 60000
Received Header Errors	= 0
Received Address Errors	= 0
Datagrams Forwarded	= 0
Unknown Protocols Received	= 350
Received Packets Discarded	= 3775

1.8. Uzyskanie statystyki wszystkich portów z zapisaniem wszystkich wyników do pliku raportunetstatportsXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -s > netstatports15.txt**

```
netstatports15 - Notepad
File Edit View

IPv4 Statistics

Packets Received = 507671
Received Header Errors = 0
Received Address Errors = 5
Datagrams Forwarded = 0
Unknown Protocols Received = 0
Received Packets Discarded = 41725
Received Packets Delivered = 504133
Output Requests = 356236
Routing Discards = 0
Discarded Output Packets = 5
Output Packet No Route = 86
Reassembly Required = 0
Reassembly Successful = 0
Reassembly Failures = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created = 0

IPv6 Statistics

Packets Received = 60877
Received Header Errors = 0
Received Address Errors = 0
Datagrams Forwarded = 0
Unknown Protocols Received = 353
Received Packets Discarded = 3845
```

1.9. Uzyskanie statystyki wyświetlania nazw DNS usług biorących udział w połączeniu z systemem operacyjnym w pliku raportu DNSstatXX.txt.

Część wyników po wprowadzeniu instrukcji: **netstat -a -f > netstat15.txt**


```

netstat15 - Notepad
File Edit View

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:445             DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:5040            DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:7680            DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:49664           DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:49665           DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:49666           DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:49667           DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:49668           DESKTOP-6GVNM2J:0      LISTENING
TCP   0.0.0.0:49669           DESKTOP-6GVNM2J:0      LISTENING
TCP   10.10.61.140:139        DESKTOP-6GVNM2J:0      LISTENING
TCP   10.10.61.140:52706      52.114.74.211:https    ESTABLISHED
TCP   10.10.61.140:52885      13.107.6.171:https     TIME_WAIT
TCP   10.10.61.140:52886      52.108.186.5:https     TIME_WAIT
TCP   10.10.61.140:52887      13.107.6.171:https     TIME_WAIT
TCP   10.10.61.140:52888      13.107.6.171:https     TIME_WAIT

```

2. Na podstawie danych uzyskanych z pliku mogę wywnioskować, że adresy z którymi komputer nawiązał połączenie to np.

Po wykonaniu instrukcji **netstat -n 5 | find /i "Established" > data15.txt** i odczekaniu około 5 minut otrzymałem długi plik wynikowy zawierający wiele różnych połączeń podsumowanych w poniższym raporcie.

3.

N O	Adresy IP serwisów i numery portów, na które ustalane są połączenia zewnętrzne	Nazwy serwisów odpowiadające adresom IP serwisów, do których rejestrowane są połączenia zewnętrzne	Porty klienckie (systemu operacyjnego), do których ustalane są połączenia zewnętrzne	Nazwy modułów oprogramowania, które wykonują połączenia zewnętrzne	Protokoły transportowe biorące udział w połączeniach zewnętrznych
1	146.75.122.214:443	Twitch.tv	443	Opera GX	TCP
2	74.125.205.188:5228	google.com	5228	Opera GX	TCP
3	31.13.81.9:443	facebook.com	443	Opera GX	TCP
4	162.159.133.232:443	discord.com	443	discord	TCP
5	52.111.243.6:443	Microsoft teams	443	Microsoft Edge	TCP
6	20.54.232.160:443	xbox.com	443	Microsoft Edge	TCP

4. Wnioski:

Narzędzie Netstat jest niesamowicie przydatną wbudowaną funkcją systemu za pomocą, której jesteśmy w stanie kontrolować wszystkie połączenia sieciowe pomiędzy komputerem a jego usługami wewnętrznymi oraz zewnętrznymi. Na podstawie zdobytych informacji jesteśmy w stanie dość łatwo ustalić z jakiego źródła przybyły połączenia oraz za pomocą jakiego oprogramowania się z nimi łączymy. Na podstawie portu jesteśmy nawet w stanie określić, czy połączenie jest bezpieczne czy nie do końca. W niektórych sytuacjach zdobycie informacji wymagało użycia więcej niż jednej komendy jednak wydaje mi się, że przy odrobinie wprawy dałoby się bardzo szybko wszystko weryfikować.