

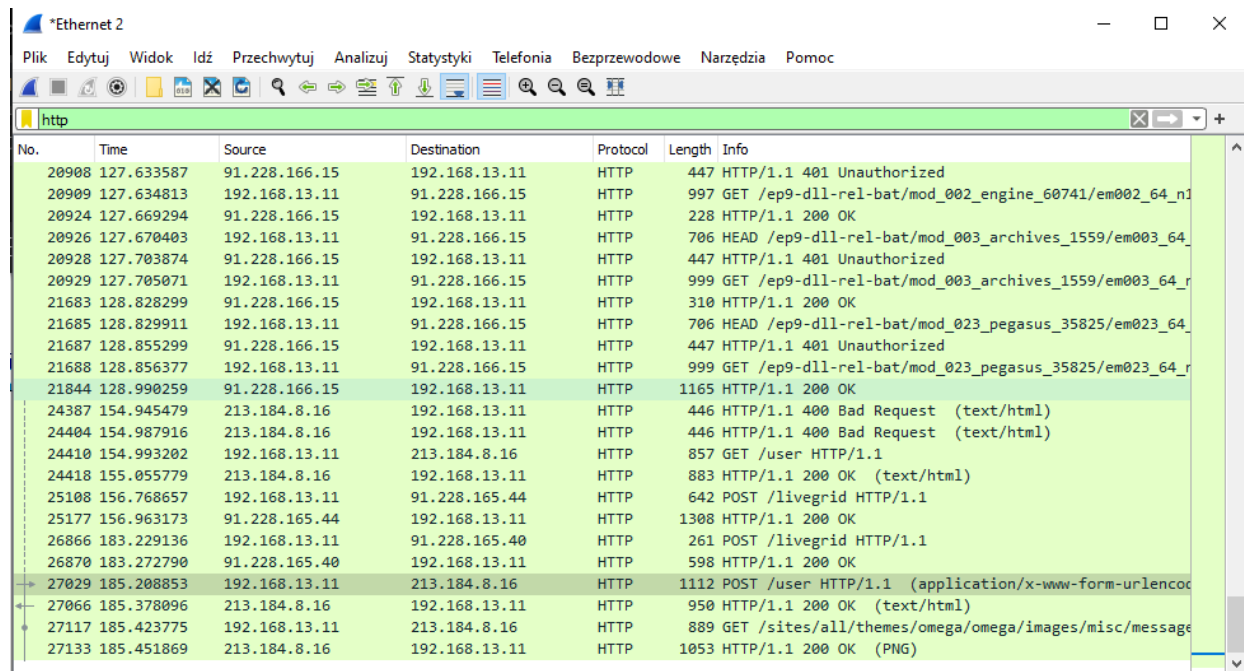
Sprawozdanie nr 2

Sieci Komputerowe

Praca z podstawowym oprogramowaniem do diagnostyki sieci

Anna Rymszewicz

1. Zapoznaj się z interfejsem i funkcjami programu Wireshark. Wyświetl przechwytywane i odfiltrowane wg. dowolnego protokołu pakiety sieciowe



No.	Time	Source	Destination	Protocol	Length	Info
20908	127.633587	91.228.166.15	192.168.13.11	HTTP	447	HTTP/1.1 401 Unauthorized
20909	127.634813	192.168.13.11	91.228.166.15	HTTP	997	GET /ep9-dll-rel-bat/mod_002_engine_60741/em002_64_n1
20924	127.669294	91.228.166.15	192.168.13.11	HTTP	228	HTTP/1.1 200 OK
20926	127.670403	192.168.13.11	91.228.166.15	HTTP	706	HEAD /ep9-dll-rel-bat/mod_003_archives_1559/em003_64
20928	127.703874	91.228.166.15	192.168.13.11	HTTP	447	HTTP/1.1 401 Unauthorized
20929	127.705071	192.168.13.11	91.228.166.15	HTTP	999	GET /ep9-dll-rel-bat/mod_003_archives_1559/em003_64_r
21683	128.828299	91.228.166.15	192.168.13.11	HTTP	310	HTTP/1.1 200 OK
21685	128.829911	192.168.13.11	91.228.166.15	HTTP	706	HEAD /ep9-dll-rel-bat/mod_023_pegasus_35825/em023_64
21687	128.855299	91.228.166.15	192.168.13.11	HTTP	447	HTTP/1.1 401 Unauthorized
21688	128.856377	192.168.13.11	91.228.166.15	HTTP	999	GET /ep9-dll-rel-bat/mod_023_pegasus_35825/em023_64_r
21844	128.990259	91.228.166.15	192.168.13.11	HTTP	1165	HTTP/1.1 200 OK
24387	154.945479	213.184.8.16	192.168.13.11	HTTP	446	HTTP/1.1 400 Bad Request (text/html)
24404	154.987916	213.184.8.16	192.168.13.11	HTTP	446	HTTP/1.1 400 Bad Request (text/html)
24410	154.993202	192.168.13.11	213.184.8.16	HTTP	857	GET /user HTTP/1.1
24418	155.055779	213.184.8.16	192.168.13.11	HTTP	883	HTTP/1.1 200 OK (text/html)
25108	156.768657	192.168.13.11	91.228.165.44	HTTP	642	POST /livegrid HTTP/1.1
25177	156.963173	91.228.165.44	192.168.13.11	HTTP	1308	HTTP/1.1 200 OK
26866	183.229136	192.168.13.11	91.228.165.40	HTTP	261	POST /livegrid HTTP/1.1
26870	183.272790	91.228.165.40	192.168.13.11	HTTP	598	HTTP/1.1 200 OK
27029	185.208853	192.168.13.11	213.184.8.16	HTTP	1112	POST /user HTTP/1.1 (application/x-www-form-urlencoded)
27066	185.378096	213.184.8.16	192.168.13.11	HTTP	950	HTTP/1.1 200 OK (text/html)
27117	185.423775	192.168.13.11	213.184.8.16	HTTP	889	GET /sites/all/themes/omega/omega/images/misc/message
27133	185.451869	213.184.8.16	192.168.13.11	HTTP	1053	HTTP/1.1 200 OK (PNG)

Pakiety zostały odfiltrowane wg. protokołu http, umożliwia nam to analizę przesyłanych pakietów i podejrzenie potrzebnych informacji.

2. Zapoznaj się z poleceniem ipconfig. Porównaj wewnętrzny adres IP z zewnętrznym, który można uzyskać np. na stronie whatismyip.com

Windows IP Configuration

Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :

Link-local IPv6 Address : fe80::9da4:2230:9164:7917%37

IPv4 Address. : 172.18.240.1

Subnet Mask : 255.255.240.0

Default Gateway :

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :

Link-local IPv6 Address : fe80::1732:da30:3ac2:67db%25
IPv4 Address. : 192.168.56.1
Subnet Mask : 255.255.255.0
Default Gateway :

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : wmii.local
Link-local IPv6 Address : fe80::f1a8:ed16:9717:8db2%15
IPv4 Address. : 192.168.13.11 IP komputera w sieci wewnętrznej
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.13.1

Ethernet adapter Ethernet 3:

Media State : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::d1c7:c291:8bc0:1a43%17
Autoconfiguration IPv4 Address. . : 169.254.159.126
Subnet Mask : 255.255.0.0
Default Gateway :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::7e4d:7386:5dc4:ac0%11

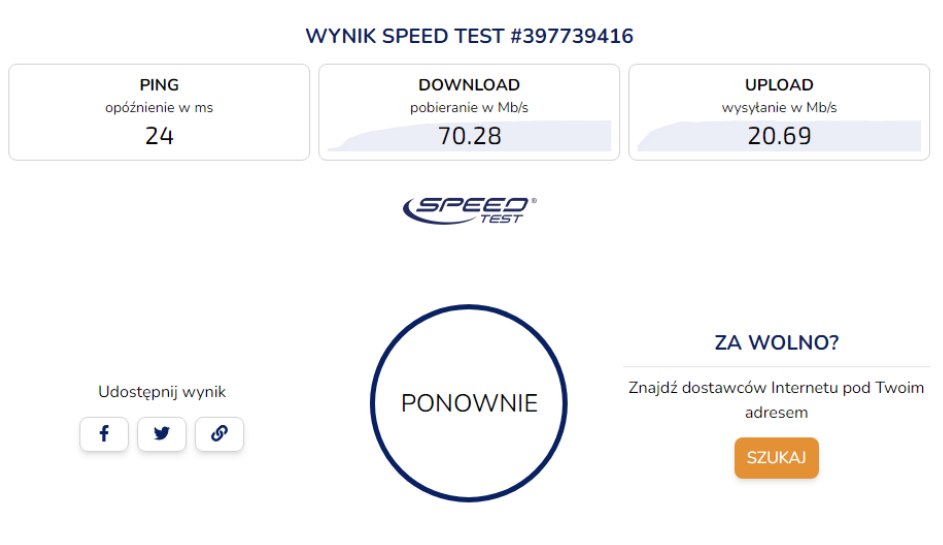
Autoconfiguration IPv4 Address. . : 169.254.214.205

Subnet Mask : 255.255.0.0

Default Gateway :

Za pomocą ipconfig jesteśmy w stanie podejrzeć IP komputera w sieci wewnętrznej. Adres IP ze strony whatismyip.com to adres zewnętrzny, ten sam dla wszystkich komputerów podłączonych do danej sieci np. 213.184.8.154

3. Zapoznaj się z możliwościami pomiaru prędkości dostępu do Internetu za pomocą speedtest.net



Strona umożliwia pomiar prędkości wysyłania, pobierania i pomiar pingu. Wynik pomiaru zależy od wielu czynników np. Innych urządzeń połączonych do sieci.

4. Zapoznaj się z pracą polecenia ping, wyświetl odpowiedź od dowolnego hosta w Internecie

```
C:\Users\local>ping www.onet.pl

Pinging www.onet.pl [18.244.102.124] with 32 bytes of data:
Reply from 18.244.102.124: bytes=32 time=14ms TTL=247
Reply from 18.244.102.124: bytes=32 time=14ms TTL=247
Reply from 18.244.102.124: bytes=32 time=14ms TTL=247
Reply from 18.244.102.124: bytes=32 time=14ms TTL=247

Ping statistics for 18.244.102.124:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 14ms, Average = 14ms
```

Otrzymujemy informacje o czasie odpowiedzi z dowolnego hosta w Internecie do naszego komputera oraz informacje o liczbie wysłanych i odebranych pakietów.

5. Zapoznaj się z poleceniem tracert, wyświetl trasę do dowolnego hosta w Internecie

```
C:\Users\local>tracert www.onet.pl

Tracing route to www.onet.pl [18.244.102.24]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  192.168.13.1
  2  <1 ms  <1 ms  <1 ms  213.184.8.1
  3   1 ms   1 ms   1 ms  10.1.3.1
  4   2 ms   1 ms   2 ms  10.1.1.194
  5   2 ms   2 ms   2 ms  com-gw1_eman-core.man.olsztyn.pl [213.184.16.54]
  6  12 ms  12 ms  12 ms  z-Olsztyn-COM.poznan-gw2-amsix.rtr.pionier.gov.pl [212.191.237.81]
  7  12 ms  13 ms  12 ms  212.191.237.18
  8  16 ms  16 ms  16 ms  pcss.plix.pl [195.182.218.111]
  9  25 ms  16 ms  17 ms  195.182.218.155
 10  *      *      *      Request timed out.
 11  *      *      *      Request timed out.
 12  *      *      *      Request timed out.
 13  *      *      *      Request timed out.
 14  *      *      *      Request timed out.
 15  14 ms  14 ms  14 ms  server-18-244-102-24.waw51.r.cloudfront.net [18.244.102.24]

Trace complete.
```

Polecenie pokazuje trasę jaką pokonują pakiety w sieciach.

6. Zapoznaj się z narzędziem nslookup, wyszukaj adres IP dowolnego serwera

```
C:\Users\local>nslookup www.onet.pl 8.8.8.8
Server:  dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name:    www.onet.pl
Addresses: 18.244.102.79
          18.244.102.128
          18.244.102.24
          18.244.102.124
```

Polecenie jest używane do wyszukiwania szczegółowych informacji odnoszących się do serwerów DNS włączając adres IP poszczególnych komputerów, nazwę domeny czy aliasy jakie posiada.

7. Zapoznaj się z poleceniem arp, użyj opcji "arp -a" oraz "arp -d"

```
C:\Users\local>arp -a

Interface: 192.168.47.1 --- 0xb
Internet Address      Physical Address      Type
192.168.47.254        00-50-56-e0-fa-0f    dynamic
192.168.47.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.13.11 --- 0x10
Internet Address      Physical Address      Type
192.168.13.1          fc-f9-38-a3-a1-4f    dynamic
192.168.13.14         bc-ae-c5-cd-89-0d    dynamic
192.168.13.16         bc-ae-c5-cd-83-b7    dynamic
192.168.13.21         bc-ae-c5-cd-8a-8a    dynamic
192.168.13.22         bc-ae-c5-cd-89-1e    dynamic
192.168.13.24         bc-ae-c5-cd-83-76    dynamic
192.168.13.25         bc-ae-c5-cd-88-62    dynamic
192.168.13.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.184.1 --- 0x12
Internet Address      Physical Address      Type
192.168.184.254       00-50-56-e7-43-91    dynamic
192.168.184.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x18
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.22.48.1 --- 0x25
Internet Address      Physical Address      Type
172.22.63.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

ARP (Address Resolution Protocol) to protokół sieciowy, który pozwala na mapowanie logicznych adresów sieciowych na fizyczne adresy MAC. Polecenie arp -a wyświetla wszystkie zmapowane adresy, polecenie arp -d wszystkie zmapowane adresy.

8. Zobacz pliki w folderze C:\Windows\System32\drivers\etc i zapoznaj się z ich przeznaczeniem

hosts	08.02.2024 14:10	Plik
hosts.ics	06.03.2024 11:31	Plik ICS
lmhosts.sam	07.12.2019 10:12	Plik SAM
networks	07.12.2019 10:12	Plik
protocol	07.12.2019 10:12	Plik
services	07.12.2019 10:12	Plik

Plik HOSTS jest integralną częścią protokołu komunikacyjnego TCP/IP. Jego głównym zadaniem jest określanie, pod jakim konkretnym adresem IP ukrywa się dana domena internetowa. Dzięki temu użytkownik, zamiast wpisywać skomplikowane ciągi cyfrowe, może po prostu wpisać prostą nazwę domeny.

lmhosts jest plikiem mapującym nazwy Samba NetBIOS na adresy IP.

Plik networks zawiera informacje o znanych sieciach, które składają się z Internetu DARPA.

Plik protocols zawiera informacje na temat znanych protokołów używanych w sieci Internet DARPA

Plik services zawiera informacje na temat znanych usług używanych w sieci Internet DARPA

9. Sporządź sprawozdanie (w formacie .pdf) z wykonanych czynności.

Podpunkt techniczny, informujący o formacie sprawozdania.

Podsumowanie

Powyżej zrealizowane czynności pozwalają na podstawową diagnostykę sieci.