

Wyszukiwanie ścieżki datagramu w internecie

Patryk Kaniewski

2021-01-06

Spis Treści

1	Grupa wykonująca zadanie	2
2	Wstęp	2
2.1	Cel ćwiczenia	2
2.2	Schemat ćwiczenia	2
2.3	Wymagany sprzęt	2
2.4	Plan ćwiczenia	2
3	Ćwiczenie	3
3.1	Przed ćwiczeniem	3
3.2	Część 1	3
3.3	Część 2	5
3.4	Część 3	7
4	Wnioski	8
4.1	Routing	8
4.2	Napotkane problemy	8

1 Grupa wykonująca zadanie

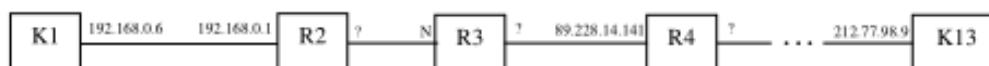
- Patryk Kaniewski

2 Wstęp

2.1 Cel ćwiczenia

Wyszukanie ścieżki datagramów w internecie

2.2 Schemat ćwiczenia



2.3 Wymagany sprzęt

- Komputer z systemem POSIX

2.4 Plan ćwiczenia

2.4.1 Część 1:

1. Wyszukujemy cel
2. Rejestrujemy ruch ICMP
3. Znajdujemy drogę

2.4.2 Część 2:

1. Rejestracja ruchu ICMP i DNS
2. Znajdujemy DNS i reverse DNS

2.4.3 Część 3:

1. Znajdujemy drogę do dalekiego celu
2. Czekamy
3. Znajdujemy drogę do dalekiego celu
4. Porównujemy drogi

3 Ćwiczenie

3.1 Przed ćwiczeniem

3.1.1 Konfiguracja wstępna

`ip a show dev enp4s0`

```
2: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether b4:2e:99:e4:68:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.186/24 brd 192.168.0.255 scope global dynamic noprefixroute enp4s0
        valid_lft 32301sec preferred_lft 32301sec
```

Wybieramy cel (w moim przypadku skierniewice.eu)

3.2 Część 1

3.2.1 Szukanie celu

Wykonujemy ping do wybranego przez nas celu (w moim przypadku skierniewice.eu)

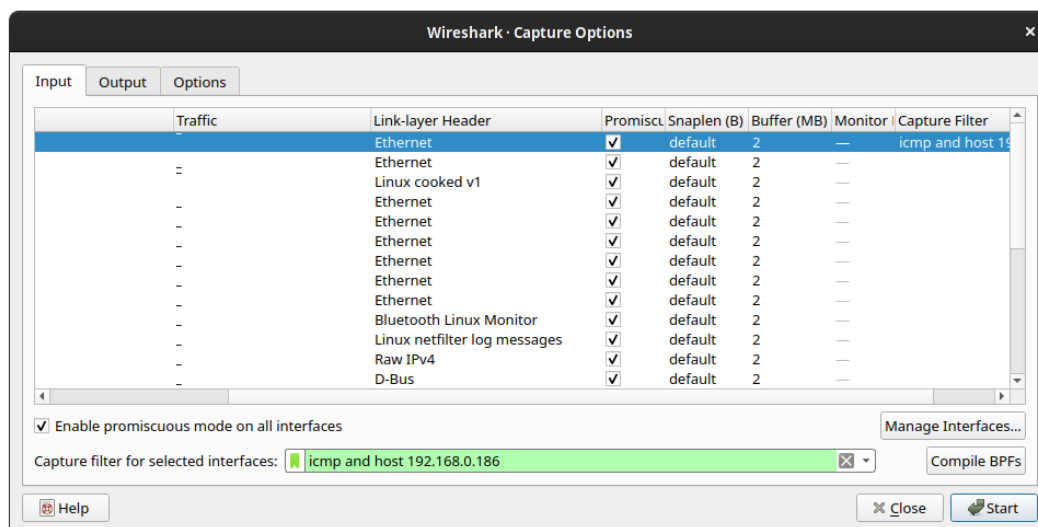
```
PING skierniewice.eu (94.152.194.219) 56(84) bytes of data:
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=1 ttl=55 time=6.41 ms
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=2 ttl=55 time=6.49 ms
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=3 ttl=55 time=6.43 ms
64 bytes from 10.ires.pl (94.152.194.219): icmp_seq=4 ttl=55 time=6.31 ms

--- skierniewice.eu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 6.310/6.412/6.492/0.065 ms
```

3.2.2 Rejestracja ruchu ICMP

Następnie używamy otrzymanego adresu IP do polecenia `traceroute -n -I 94.152.194.219` (opcja `-n` wyłącza odwracanie adresów ip na adresy domenowe; opcja `-I` wymusza używanie icmp echo do badania celów).

Rejestrujemy sesje za pomocą programu do przechwytywania pakietów np. `Wireshark` i filtrujemy ICMP.



tracert to skierniewice.eu (94.152.194.219), 30 hops max, 60 byte packets

```

1  192.168.0.1  0.223 ms  0.318 ms  0.473 ms
2  91.214.0.129  1.167 ms  1.184 ms  1.200 ms
3  * * *
4  94.246.185.48  1.913 ms  1.960 ms  1.986 ms
5  195.149.232.222  2.379 ms  2.431 ms  2.451 ms
6  185.80.215.238  6.902 ms  6.804 ms  6.823 ms
7  94.152.201.242  27.428 ms  26.699 ms  26.697 ms
8  94.152.201.222  22.125 ms  21.498 ms  21.478 ms
9  94.152.201.155  7.770 ms  7.394 ms  7.273 ms
10 94.152.194.219  6.205 ms  6.176 ms  6.286 ms

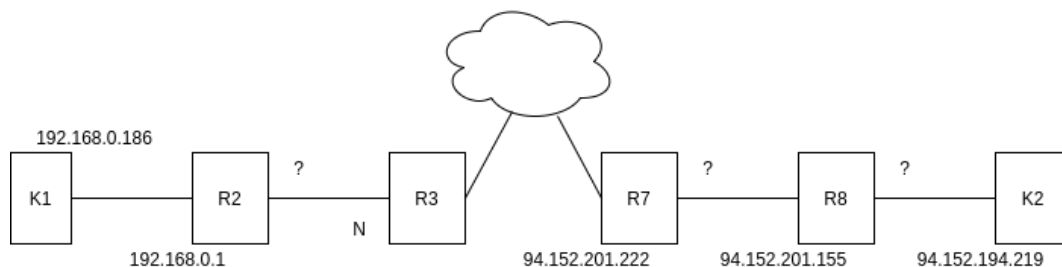
```

3.2.3 Wyniki

No.	Time	Source	Destination	Protocol	Length	Info
11	0.000075463	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=11/2816, ttl=4 (no response found!)
12	0.000081995	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=12/3072, ttl=4 (no response found!)
13	0.000089870	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=13/3328, ttl=5 (no response found!)
14	0.000092622	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=14/3584, ttl=5 (no response found!)
15	0.000103035	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=15/3840, ttl=5 (no response found!)
16	0.000110389	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=16/4096, ttl=6 (no response found!)
17	0.000129244	192.168.0.186	94.152.194.219	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
18	0.000267768	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=17/4352, ttl=6 (no response found!)
19	0.000323874	192.168.0.1	192.168.0.186	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
20	0.000365383	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=18/4608, ttl=6 (no response found!)
21	0.000406891	192.168.0.186	94.152.194.219	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
22	0.000525633	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=19/4864, ttl=7 (no response found!)
23	0.001189126	91.214.0.129	192.168.0.186	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
24	0.001213503	91.214.0.129	192.168.0.186	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
25	0.001235915	91.214.0.129	192.168.0.186	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
26	0.001305030	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=20/5120, ttl=7 (no response found!)
27	0.001318111	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=21/5376, ttl=7 (no response found!)
28	0.001327459	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=22/5632, ttl=8 (no response found!)
29	0.001977332	94.246.185.48	192.168.0.186	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
30	0.002009383	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=23/5888, ttl=8 (no response found!)
31	0.002031383	94.246.185.48	192.168.0.186	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
32	0.002058486	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=24/6144, ttl=8 (no response found!)
33	0.002063376	94.246.185.48	192.168.0.186	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
34	0.002089896	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=25/6400, ttl=9 (no response found!)
35	0.002104046	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=26/6656, ttl=9 (no response found!)
36	0.002490166	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=27/6912, ttl=9 (no response found!)
37	0.002522018	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=28/7168, ttl=9 (no response found!)
38	0.002547054	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=29/7424, ttl=10 (reply in 51)
39	0.002570183	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=30/7680, ttl=10 (reply in 52)
40	0.002574950	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=31/7936, ttl=11 (reply in 53)
41	0.007007829	185.80.215.238	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
42	0.007063505	185.80.215.238	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
43	0.007070178	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=32/8256, ttl=10 (reply in 54)
44	0.007087541	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=33/8512, ttl=10 (reply in 55)
45	0.007180878	185.80.215.238	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
46	0.007210123	192.168.0.186	94.152.194.219	ICMP	74	Echo (ping) request id=0x0002, seq=34/8768, ttl=11 (reply in 56)
47	0.008774881	94.152.194.219	192.168.0.186	ICMP	74	Echo (ping) reply id=0x0002, seq=28/7168, ttl=55 (request in 40)
48	0.008814698	94.152.201.155	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
49	0.008854632	94.152.201.155	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
50	0.008878997	94.152.201.155	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
51	0.013230469	94.152.194.219	192.168.0.186	ICMP	74	Echo (ping) reply id=0x0002, seq=29/7424, ttl=55 (request in 43)
52	0.013368611	94.152.194.219	192.168.0.186	ICMP	74	Echo (ping) reply id=0x0002, seq=30/7680, ttl=55 (request in 44)
53	0.013410711	94.152.194.219	192.168.0.186	ICMP	74	Echo (ping) reply id=0x0002, seq=31/7936, ttl=55 (request in 46)
54	0.023447679	94.152.201.222	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
55	0.023500559	94.152.201.222	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
56	0.023530606	94.152.201.222	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	0.027947388	94.152.201.242	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
58	0.027985491	94.152.201.242	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	0.028009456	94.152.201.242	192.168.0.186	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

- Na różowo zaznaczone są Echo Request
- Na czarno zaznaczone są TTL exceeded
- Na niebiesko zaznaczone są Echo Reply

Nasza ścieżka wygląda następująco:



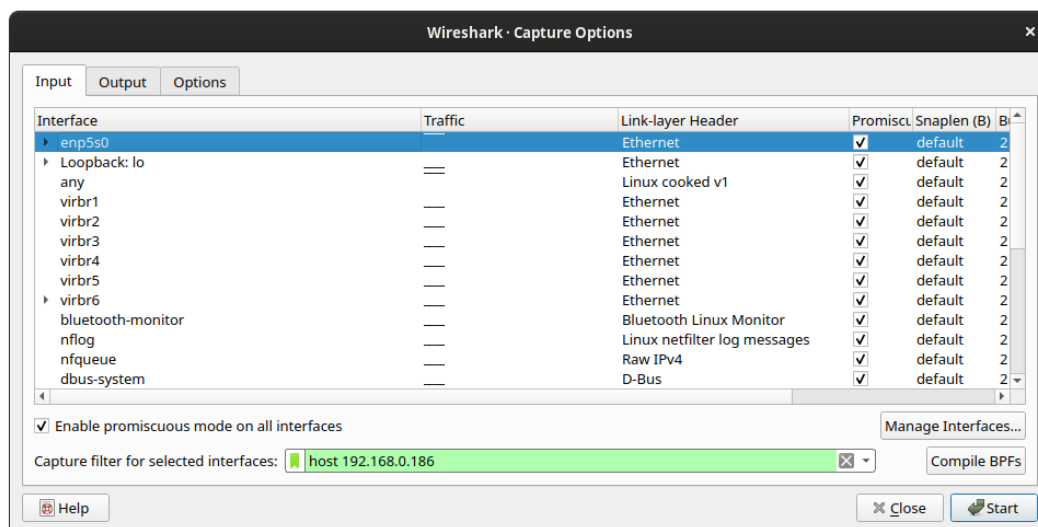
3.3 Część 2

3.3.1 Rejestracja ICMP i DNS

W części drugiej nieco zmieniamy nasze polecenie `tracert -I skierniewice.eu` (opcja `-I` wymusza używanie icmp echo do badania celów).

Bez opcji -d, traceroute będzie próbował znaleźć poprzez reverse DNS lookup adresy domenowe związane z adresami ip.

Zmieniamy również opcje przechwytywania w programie przechwytywania pakietów (np. wireshark) na host K1.



traceroute to skierniewice.eu (94.152.194.219), 30 hops max, 60 byte packets

```

1  _gateway (192.168.0.1)  0.247 ms  0.313 ms  0.481 ms
2  91-214-0-129.timplus.net (91.214.0.129)  1.387 ms  1.379 ms  1.415 ms
3  main-gw.timplus.net (91.214.0.1)  1.469 ms  1.490 ms  1.505 ms
4  48.polmix2.epix.net.pl (94.246.185.48)  2.370 ms  2.397 ms  2.389 ms
5  oxylion.tpix.pl (195.149.232.222)  2.654 ms  2.714 ms  2.739 ms
6  185.80.215.238 (185.80.215.238)  7.172 ms  6.814 ms  6.805 ms
7  5E98C9F2.static.tld.pl (94.152.201.242)  23.860 ms  21.250 ms  21.252 ms
8  5E98C9DE.static.tld.pl (94.152.201.222)  25.080 ms  25.089 ms  25.100 ms
9  5E98C99B.static.tld.pl (94.152.201.155)  14.678 ms  14.714 ms  14.730 ms
10 10.ires.pl (94.152.194.219)  6.568 ms  6.598 ms  6.619 ms

```

3.3.2 Wyniki

Aby ułatwić analizę packetdump możemy użyć w wireshark display filter icmp or dns.

7	1.137517609	192.168.0.186	192.168.0.1	DNS	75 Standard query 0x2f3d A skierniewice.eu
8	1.137535373	192.168.0.186	192.168.0.1	DNS	75 Standard query 0xbf39 AAAA skierniewice.eu
9	1.138672832	192.168.0.1	192.168.0.186	DNS	91 Standard query response 0x2f3d A skierniewice.eu A 94.152.194.219
10	1.139647091	192.168.0.1	192.168.0.186	DNS	127 Standard query response 0xbf39 AAAA skierniewice.eu SOA ns1.tld.pl

Pierwsze nasze zapytanie DNS jest typu A(AAA), aby przekonwertować nazwę domeny który przekazaliśmy traceroute (skierniewice.eu) na adres IPv4.

39	1.141504075	192.168.0.186	192.168.0.1	DNS	85 Standard query 0xc2fd PTR 129.0.214.91.in-addr.arpa
40	1.142222238	94.246.185.48	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
41	1.142257134	94.246.185.48	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
42	1.142257234	94.246.185.48	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
43	1.142536112	195.149.232.222	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
44	1.142597240	195.149.232.222	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
45	1.142628499	195.149.232.222	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
46	1.142666390	192.168.0.1	192.168.0.186	DNS	123 Standard query response 0xc2fd PTR 129.0.214.91.in-addr.arpa PTR 91-214-0-12...
47	1.143043236	192.168.0.186	94.152.194.219	ICMP	74 Echo (ping) request id=0x0006, seq=20/5120, ttl=7 (no response found!)
48	1.143052934	192.168.0.186	94.152.194.219	ICMP	74 Echo (ping) request id=0x0006, seq=21/5376, ttl=7 (no response found!)
49	1.143392459	192.168.0.186	192.168.0.1	DNS	83 Standard query 0x6457 PTR 1.0.214.91.in-addr.arpa
50	1.144648092	192.168.0.1	192.168.0.186	DNS	116 Standard query response 0x6457 PTR 1.0.214.91.in-addr.arpa PTR main-gw.timp...
51	1.144954924	192.168.0.186	192.168.0.1	DNS	86 Standard query 0xa283 PTR 48.185.246.94.in-addr.arpa
52	1.146357586	192.168.0.1	192.168.0.186	DNS	122 Standard query response 0xa283 PTR 48.185.246.94.in-addr.arpa PTR 48.polmix2...
53	1.146724222	192.168.0.186	192.168.0.1	DNS	88 Standard query 0xb8c6 PTR 222.232.149.195.in-addr.arpa
54	1.147037090	105.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
55	1.147132226	105.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
56	1.147163926	105.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
57	1.164232751	94.152.201.242	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
58	1.164280982	94.152.201.242	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
59	1.164306299	94.152.201.242	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
62	1.491389466	192.168.0.1	192.168.0.186	DNS	117 Standard query response 0xb8c6 PTR 222.232.149.195.in-addr.arpa PTR oxylon...

Każde kolejne zapytanie będzie typu PTR, aby przekonwertować adres IP na nazwę domeny. Warto zwrócić uwagę na to że adres IP który został wysłany w zapytaniu PTR miał oktety odwrócone i .in-addr.arpa dodane na końcu.

94	1.629612164	192.168.0.186	192.168.0.1	DNS	8/ Standard query 0x456f PTR 222.201.152.94.in-addr.arpa
95	1.634466034	94.152.194.219	192.168.0.186	ICMP	74 Echo (ping) reply id=0x0006, seq=32/8192, ttl=55 (request in 88)
96	1.634579329	94.152.194.219	192.168.0.186	ICMP	74 Echo (ping) reply id=0x0006, seq=33/8448, ttl=55 (request in 89)
97	1.634630246	94.152.194.219	192.168.0.186	ICMP	74 Echo (ping) reply id=0x0006, seq=34/8704, ttl=55 (request in 90)
98	1.634692604	94.152.194.219	192.168.0.186	ICMP	74 Echo (ping) reply id=0x0006, seq=35/8960, ttl=55 (request in 91)
99	1.634722252	94.152.194.219	192.168.0.186	ICMP	74 Echo (ping) reply id=0x0006, seq=36/9216, ttl=55 (request in 92)
100	1.634750324	94.152.194.219	192.168.0.186	ICMP	74 Echo (ping) reply id=0x0006, seq=37/9472, ttl=55 (request in 93)
101	1.648237100	192.168.0.1	192.168.0.186	DNS	123 Standard query response 0x456f PTR 222.201.152.94.in-addr.arpa PTR 5E98C9DE...
102	1.648610488	192.168.0.186	192.168.0.1	DNS	87 Standard query 0xe660 PTR 155.201.152.94.in-addr.arpa
103	1.666920227	192.168.0.1	192.168.0.186	DNS	123 Standard query response 0xe660 PTR 155.201.152.94.in-addr.arpa PTR 5E98C998...
104	1.667269510	192.168.0.186	192.168.0.1	DNS	87 Standard query 0x51cf PTR 219.194.152.94.in-addr.arpa
105	1.795122350	192.168.0.1	192.168.0.186	DNS	111 Standard query response 0x51cf PTR 219.194.152.94.in-addr.arpa PTR 10.ires.pl

Dokładnie tak samo wygląda zapytanie na ostateczny adres na który jest związany z domeną którą testowaliśmy. Ciekawym spostrzeżeniem może być że zapytanie PTR na ten sam adres który dostaliśmy z zapytania A skierniewice.eu ma inną nazwę domeny (10.ires.pl).

Można to zweryfikować za pomocą innych narzędzi (np. linux dig i dig -x).

```
;; QUESTION SECTION:
;skierniewice.eu.                IN      A

;; ANSWER SECTION:
skierniewice.eu.                 3599    IN      A

;; QUESTION SECTION:
;219.194.152.94.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
219.194.152.94.in-addr.arpa.    3600    IN      PTR      10.ires.pl.
```

3.4 Część 3

3.4.1 Odległy cel

Znalezienie odległego celu w dzisiejszych czasach może okazać się problemem ze względu na powszechność usług takich jak cloudflare, aws oferujących wszelakie usługi proxy/cache.

Wybrałem cel theindependent.sg znajdujący się w azji południowo-wschodniej:

PING theindependent.sg (34.87.85.150) 56(84) bytes of data.

64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=1 ttl=60 time=265

64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=2 ttl=60 time=266

64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=3 ttl=60 time=265

64 bytes from 150.85.87.34.bc.googleusercontent.com (34.87.85.150): icmp_seq=4 ttl=60 time=265


```
--- theindependent.sg ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 265.312/265.624/266.329/0.410 ms
```

Traceroute o godzinie 11:01

traceroute to theindependent.sg (34.87.85.150), 30 hops max, 60 byte packets

```
 1  192.168.0.1  0.249 ms  0.352 ms  0.453 ms
 2  91.214.0.129  1.140 ms  1.146 ms  1.155 ms
 3  * * *
 4  94.246.185.48  1.893 ms  1.928 ms  2.005 ms
 5  195.149.233.101  2.436 ms  2.482 ms  2.673 ms
 6  188.47.253.245  2.565 ms  2.620 ms  2.547 ms
 7  * * *
 8  108.170.248.178  265.680 ms  265.580 ms  265.623 ms
 9  108.170.225.145  262.537 ms * *
10  209.85.243.180  263.452 ms  263.414 ms  263.415 ms
11  108.170.233.49  266.235 ms  265.706 ms  265.734 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  34.87.85.150  265.372 ms  265.358 ms  265.202 ms
```

3.4.2 Ponowienie szukania drogi

3.4.3 Różnice w drodze

Aby porównać różnice odrzuciłem pingi z traceroute za pomocą polecenia `awk '{print $1 "\t" $2}' traceroute1.txt > trace1.txt` a następnie polecenia `diff` aby porównać te pliki

4 Wnioski

4.1 Routing

4.2 Napotkane problemy

4.2.1 traceroute -I

traceroute na systemie na którym przeprowadzane jest ćwiczenie (Archlinux) domyślnie nie używa ICMP echo (ping) do przeszukiwania drogi ze względu na to że w dużej ilości sieci pakiety ICMP są filtrowane

1	0.000000000	192.168.0.1	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
2	0.000136079	192.168.0.1	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
3	0.000220510	192.168.0.1	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
4	0.001413974	91.214.0.129	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
5	0.001503333	91.214.0.129	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
6	0.001543339	91.214.0.129	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
7	0.001571543	91.214.0.1	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
8	0.001595959	91.214.0.1	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
9	0.001621888	91.214.0.1	192.168.0.186	ICMP	94 Time-to-live exceeded (Time to live exceeded in transit)
10	0.002219425	195.43.72.186	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
11	0.002242596	195.43.72.186	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
12	0.002268215	195.43.72.186	192.168.0.186	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)
13	0.002720585	195.182.219.60	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
14	0.002763815	195.182.219.60	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
15	0.002789204	195.182.219.60	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
16	0.007341162	185.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
17	0.007371620	185.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
18	0.007419501	185.80.215.238	192.168.0.186	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
19	0.008670886	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
20	0.009075272	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
21	0.009102445	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
22	0.009170805	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
23	0.009209729	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)
24	0.009234335	94.152.194.219	192.168.0.186	ICMP	102 Destination unreachable (Host administratively prohibited)

Rozwiązaniem tego było wyszukanie w manpage (`man traceroute`) o `traceroute` opcji `-I` która zmusza program do używania ICMP ping

```
thisconnect@archfail: ~
--help Print help info and exit.

-4, -6 Explicitly force IPv4 or IPv6 tracerouting. By default, the program will try to resolve the name given, and choose the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, traceroute will use IPv4.

-I, --icmp
    Use ICMP ECHO for probes

-T, --tcp
    Use TCP SYN for probes

-d, --debug
    Manual page traceroute(8) line 67 (press h for help or q to quit)
```