

Zad 1.

Pobierając plik index.html dla domeny juniper.net i filtrując go przy użyciu następującego polecania otrzymamy wyniki:

Subdomeny juniper.net

```
grep "https://" index.html | cut -d "/" -f 3 | sort -u | grep "net"
```

```
root@kali:~# grep "https://" index.html | cut -d "/" -f 3 | sort -u | grep "net"
apps.juniper.net
eng.juniper.net
entitlementsearch.juniper.net
events.juniper.net
forums.juniper.net
investor.juniper.net
jnaa.juniper.net
junipernetworks.allegiantech.com
junipernetworks.lookbookhq.com
kb.juniper.net",
learningportal.juniper.net
license.juniper.net
my.juniper.net
newsroom.juniper.net
partners.juniper.net
prsearch.juniper.net
support.juniper.net
userregistration.juniper.net
www.juniper.net
root@kali:~#
```

Następnie zapisując listę subdomen do pliku możemy przy użyciu polecenia host i pętli for znaleźć dla każdej adres IP serwera/serwerów obsługujących daną domenę.

Adresy IP subdomen juniper.net

```
for url in $(cat list.txt); do host $url; done | grep "has address" | cut -d " " -f 4 | sort
-u
```

```
root@kali:~# for url in $(cat list.txt); do host $url; done | grep "has address" | cut -d " " -f 4 | sort -u
100.20.176.241
104.103.87.213
13.91.63.25
18.236.0.195
208.74.207.25
2.18.29.16
2.18.29.8
34.209.96.132
34.218.217.51
34.228.117.126
34.236.206.224
35.155.131.244
35.164.62.72
35.167.218.194
35.171.210.172
3.94.71.108
52.10.169.172
52.26.35.42
52.35.129.69
52.36.47.227
52.40.229.165
52.42.149.190
54.186.93.157
54.190.23.243
54.200.249.137
54.214.152.154
54.244.131.6
66.129.237.237
```

Zad 2.

Używając programu Wireshark przechwyciłem ruch sieciowy przy próbie logowania na uczelnianą skrzynkę pocztową medusa.elka.pw.edu.pl. Po analizie pakietów, ustaliłem gdzie nastąpiło nawiązanie sesji TCP, a gdzie jej zakończenie.

Nawiązanie sesji TCP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	194.29.160.95	TCP	74	35882 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4265132426 TSecr=0 WS=128
2	0.006194258	10.0.2.15	194.29.160.95	TCP	74	35884 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4265132432 TSecr=0 WS=128
3	0.007083089	10.0.2.15	194.29.160.95	TCP	74	35886 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4265132433 TSecr=0 WS=128
4	0.034125677	194.29.160.95	10.0.2.15	TCP	60	443 → 35884 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5	0.034169103	10.0.2.15	194.29.160.95	TCP	54	35884 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.034203946	194.29.160.95	10.0.2.15	TCP	60	443 → 35882 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	0.034214678	10.0.2.15	194.29.160.95	TCP	54	35882 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8	0.034256234	194.29.160.95	10.0.2.15	TCP	60	443 → 35886 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
9	0.034259129	10.0.2.15	194.29.160.95	TCP	54	35886 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Zakończenie sesji TCP

No.	Time	Source	Destination	Protocol	Length	Info
49	5.264775907	10.0.2.15	194.29.160.95	TCP	54	35884 → 443 [ACK] Seq=1385 Ack=958 Win=63468 Len=0
50	5.264828131	194.29.160.95	10.0.2.15	TCP	60	443 → 35884 [FIN, ACK] Seq=958 Ack=1385 Win=65535 Len=0
51	5.264966036	10.0.2.15	194.29.160.95	TLSv1.2	85	Encrypted Alert
52	5.265026465	10.0.2.15	194.29.160.95	TCP	54	35884 → 443 [FIN, ACK] Seq=1416 Ack=959 Win=63468 Len=0
53	5.265183674	194.29.160.95	10.0.2.15	TCP	60	443 → 35884 [ACK] Seq=959 Ack=1416 Win=65535 Len=0
54	5.265197260	194.29.160.95	10.0.2.15	TCP	60	443 → 35884 [ACK] Seq=959 Ack=1417 Win=65535 Len=0
55	5.995750613	10.0.2.15	194.29.160.95	TLSv1.2	85	Encrypted Alert
56	5.995750613	10.0.2.15	194.29.160.95	TCP	54	35886 → 443 [ACK] Seq=1842 Ack=9967 Win=63900 Len=0
57	5.995792987	194.29.160.95	10.0.2.15	TCP	60	443 → 35886 [FIN, ACK] Seq=9967 Ack=1842 Win=65535 Len=0
58	5.995804964	194.29.160.95	10.0.2.15	TLSv1.2	85	Encrypted Alert
59	5.995809704	10.0.2.15	194.29.160.95	TCP	54	35882 → 443 [ACK] Seq=1289 Ack=1253 Win=63071 Len=0
60	5.995835591	194.29.160.95	10.0.2.15	TCP	60	443 → 35882 [FIN, ACK] Seq=1253 Ack=1289 Win=65535 Len=0
61	5.996040884	10.0.2.15	194.29.160.95	TLSv1.2	85	Encrypted Alert
62	5.996103460	10.0.2.15	194.29.160.95	TCP	54	35886 → 443 [FIN, ACK] Seq=1873 Ack=9968 Win=63900 Len=0
63	5.996249884	194.29.160.95	10.0.2.15	TCP	60	443 → 35886 [ACK] Seq=9968 Ack=1873 Win=65535 Len=0
64	5.996259625	10.0.2.15	194.29.160.95	TLSv1.2	85	Encrypted Alert
65	5.996299446	10.0.2.15	194.29.160.95	TCP	54	35882 → 443 [FIN, ACK] Seq=1320 Ack=1254 Win=63071 Len=0
66	5.996348882	194.29.160.95	10.0.2.15	TCP	60	443 → 35886 [ACK] Seq=9968 Ack=1874 Win=65535 Len=0
67	5.996450066	194.29.160.95	10.0.2.15	TCP	60	443 → 35882 [ACK] Seq=1254 Ack=1320 Win=65535 Len=0
68	5.996456574	194.29.160.95	10.0.2.15	TCP	60	443 → 35882 [ACK] Seq=1254 Ack=1321 Win=65535 Len=0

Zad 3.

Przechwycony ruch sieciowy przy próbie logowania na medusa.elka.pw.edu.pl

Uzgodnienie sesji TCP

12:36:41.212141 IP 10.0.2.15.38228 > 194.29.160.95.443: Flags [S], seq 2546084144, win 64240, options [mss 1460,sackOK,TS val 2651050907 ecr 0,nop,wscale 7], length 0
12:36:41.212421 IP 10.0.2.15.38230 > 194.29.160.95.443: Flags [S], seq 3834183565, win 64240, options [mss 1460,sackOK,TS val 2651050907 ecr 0,nop,wscale 7], length 0
12:36:41.212601 IP 10.0.2.15.38232 > 194.29.160.95.443: Flags [S], seq 4048218660, win 64240, options [mss 1460,sackOK,TS val 2651050908 ecr 0,nop,wscale 7], length 0
12:36:41.253218 IP 194.29.160.95.443 > 10.0.2.15.38228: Flags [.], seq 69856001, ack 2546084145, win 65535, options [mss 1460], length 0
12:36:41.253296 IP 10.0.2.15.38228 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
12:36:41.254166 IP 194.29.160.95.443 > 10.0.2.15.38228: Flags [.], seq 69892001, ack 4040218661, win 65535, options [mss 1460], length 0
12:36:41.254221 IP 10.0.2.15.38230 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
12:36:41.254270 IP 194.29.160.95.443 > 10.0.2.15.38230: Flags [.], seq 369984001, ack 3834183566, win 65535, options [mss 1460], length 0
12:36:41.254296 IP 10.0.2.15.38230 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0

Zakończenie sesji TCP

12:36:46.599074 IP 194.29.160.95.443 > 10.0.2.15.38228: Flags [F.], seq 958, ack 1401, win 65535, length 0
12:36:46.599817 IP 10.0.2.15.38228 > 194.29.160.95.443: Flags [P.], seq 1401:1432, ack 959, win 63468, length 31
12:36:46.600360 IP 10.0.2.15.38228 > 194.29.160.95.443: Flags [F.], seq 1432, ack 959, win 63468, length 0
12:36:46.600671 IP 194.29.160.95.443 > 10.0.2.15.38228: Flags [.], ack 1432, win 65535, length 0
12:36:46.601213 IP 194.29.160.95.443 > 10.0.2.15.38228: Flags [.], ack 1433, win 65535, length 0
12:36:47.210150 IP 194.29.160.95.443 > 10.0.2.15.38230: Flags [P.], seq 1222:1253, ack 1305, win 65535, length 31
12:36:47.210237 IP 10.0.2.15.38230 > 194.29.160.95.443: Flags [.], ack 1253, win 63071, length 0
12:36:47.210390 IP 194.29.160.95.443 > 10.0.2.15.38230: Flags [F.], seq 1253, ack 1305, win 65535, length 0
12:36:47.210850 IP 10.0.2.15.38230 > 194.29.160.95.443: Flags [P.], seq 1305:1336, ack 1254, win 63071, length 31
12:36:47.210999 IP 10.0.2.15.38230 > 194.29.160.95.443: Flags [F.], seq 1336, ack 1254, win 63071, length 0
12:36:47.211211 IP 194.29.160.95.443 > 10.0.2.15.38230: Flags [.], ack 1336, win 65535, length 0
12:36:47.234505 IP 194.29.160.95.443 > 10.0.2.15.38232: Flags [P.], seq 10109:10140, ack 1874, win 65535, length 31
12:36:47.234753 IP 10.0.2.15.38232 > 194.29.160.95.443: Flags [.], ack 10140, win 63900, length 0
12:36:47.234948 IP 194.29.160.95.443 > 10.0.2.15.38232: Flags [F.], seq 10140, ack 1874, win 65535, length 0
12:36:47.235373 IP 10.0.2.15.38232 > 194.29.160.95.443: Flags [P.], seq 1874:1905, ack 10141, win 63900, length 31
12:36:47.235694 IP 10.0.2.15.38232 > 194.29.160.95.443: Flags [F.], seq 1905, ack 10141, win 63900, length 0
12:36:47.235907 IP 194.29.160.95.443 > 10.0.2.15.38232: Flags [.], ack 1905, win 65535, length 0
12:36:47.236259 IP 10.0.2.15.38232 > 194.29.160.95.443: Flags [.], ack 1906, win 65535, length 0

Sekwencja Logowania

```
tcpdump -vv -A -r tcp.pcap
```

```
root@kali:~# tcpcdump -vv -A -r tcp.pcap
reading from file tcp.pcap, link-type EN10MB (Ethernet)
04:22:05.024356 IP (tos 0x0, ttl 64, id 29178, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.48612 > 93.184.220.29.http: Flags [.], cksum 0x45ff (incorrect -> 0x89d2), seq 3283473048, ack 35393578, win 63828, length 0
E..{.Q@.@[...].P....*P..TE...
04:22:05.024476 IP (tos 0x0, ttl 64, id 4915, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.48614 > 93.184.220.29.http: Flags [.], cksum 0x45ff (incorrect -> 0x1055), seq 3832983889, ack 35457578, win 63828, length 0
E..{.30@.@[...].P....*P.v...
*P..TE...
04:22:05.024558 IP (tos 0x0, ttl 64, id 17891, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.48616 > 93.184.220.29.http: Flags [.], cksum 0x45ff (incorrect -> 0x9e0e), seq 262143596, ack 35521578, win 63828, length 0
E..{.E@.@[...].P.....1....*P..TE...
04:22:05.068196 IP (tos 0x0, ttl 64, id 171, offset 0, flags [none], proto TCP (6), length 40)
  93.184.220.29.http > 10.0.2.15.48612: Flags [.], cksum 0x0326 (correct), seq 1, ack 1, win 65535, length 0
E..{.0@A]...P....*...P....&.....
04:22:05.068343 IP (tos 0x0, ttl 64, id 172, offset 0, flags [none], proto TCP (6), length 40)
  93.184.220.29.http > 10.0.2.15.48614: Flags [.], cksum 0x09a9 (correct), seq 1, ack 1, win 65535, length 0
E..{.0@A]...P.....
*...P.....
*..v.RP......
04:22:05.068355 IP (tos 0x0, ttl 64, id 173, offset 0, flags [none], proto TCP (6), length 40)
  93.184.220.29.http > 10.0.2.15.48616: Flags [.], cksum 0x9762 (correct), seq 1, ack 1, win 65535, length 0
E..{.0@?]...P....*...mp....b.....
04:22:06.690192 IP (tos 0x0, ttl 64, id 49709, offset 0, flags [DF], proto UDP (17), length 67)
  10.0.2.15.58752 > dns3.elka.pw.edu.pl.domain: [bad udp cksum 0x6e77 -> 0x3921!] 38947+ A? medusa.elka.pw.edu.pl. (39)
E..C..-@.@
F
.....
5./nw.#.....medusa.elka.pw.edu.pl....
```

Cały ruch sieciowy podczas logowania

Niestety nie udało mi się odnaleźć sekwencji logowania w przechwyconym ruchu sieciowym, prawdopodobnie dlatego, że dane logowania są zaszyfrowane i wysyłane jak każdy inny pakiet.

Filtrowanie ruchu na porcie 443

```
root@kali:~# tcpdump -n port 443 -r tcp.pcap
reading from file tcp.pcap, link-type EN10MB (Ethernet)
04:22:06.746132 IP 10.0.2.15.39224 > 194.29.160.95.443: Flags [S], seq 563466922, win 64240, options [mss 1460,sackOK,Ts val 626441495 ecr 0,nop,wscale 7], length 0
04:22:06.746302 IP 10.0.2.15.39226 > 194.29.160.95.443: Flags [S], seq 3183553195, win 64240, options [mss 1460,sackOK,Ts val 626441495 ecr 0,nop,wscale 7], length 0
04:22:06.848933 IP 194.29.160.95.443 > 10.0.2.15.39224: Flags [S.], seq 47296001, ack 563466923, win 65535, options [mss 1460], length 0
04:22:06.848937 IP 10.0.2.15.39224 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
04:22:06.849160 IP 194.29.160.95.443 > 10.0.2.15.39226: Flags [S.], seq 47360001, ack 3183553196, win 65535, options [mss 1460], length 0
04:22:06.849193 IP 10.0.2.15.39226 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
04:22:06.852606 IP 10.0.2.15.39224 > 194.29.160.95.443: Flags [P.], seq 1:577, ack 1, win 64240, length 576
04:22:06.855994 IP 10.0.2.15.39226 > 194.29.160.95.443: Flags [P.], seq 1:577, ack 1, win 64240, length 576
04:22:06.956270 IP 194.29.160.95.443 > 10.0.2.15.39224: Flags [.], ack 577, win 65535, length 0
```

Przechwytywanie ruchu na porcie 433

```
root@kali:~# tcpdump -n port 433
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:46:08.379119 IP 10.0.2.15.37430 > 194.29.160.95.443: Flags [S], seq 896118445, win 64240, options [mss 1460,sackOK,Ts val 2640859040 ecr 0,nop,wscale 7], length 0
08:46:08.401813 IP 10.0.2.15.37432 > 194.29.160.95.443: Flags [S], seq 287515431, ack 563466923, win 64240, options [mss 1460,sackOK,Ts val 2640859063 ecr 0,nop,wscale 7], length 0
08:46:08.401817 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [S.], seq 4098055195, win 64240, options [mss 1460,sackOK,Ts val 2640859065 ecr 0,nop,wscale 7], length 0
08:46:08.403340 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [.], ack 153, win 64240, options [mss 1460], length 0
08:46:08.408389 IP 10.0.2.15.37430 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
08:46:08.409389 IP 10.0.2.15.37430 > 194.29.160.95.443: Flags [.], seq 1:577, ack 1, win 64240, length 576
08:46:08.410816 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [.], ack 577, win 65535, length 0
08:46:08.422823 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [P.], seq 1:577, ack 287751432, win 65535, options [mss 1460], length 0
08:46:08.422961 IP 10.0.2.15.37432 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
08:46:08.422994 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [.], seq 1:577, ack 577, win 65535, length 152
08:46:08.422996 IP 10.0.2.15.37430 > 194.29.160.95.443: Flags [.], ack 153, win 64088, length 0
08:46:08.423011 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [.], seq 74048801, ack 4090655120, win 65535, options [mss 1460], length 0
08:46:08.423039 IP 10.0.2.15.37434 > 194.29.160.95.443: Flags [.], ack 1, win 64240, length 0
08:46:08.423041 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [.], seq 153, ack 153, win 64088, length 51
08:46:08.423074 IP 10.0.2.15.37430 > 194.29.160.95.443: Flags [.], ack 628, win 65535, length 0
08:46:08.425927 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [.], seq 628, ack 153, win 64088, length 773
08:46:08.426267 IP 194.29.160.95.443 > 10.0.2.15.37430: Flags [.], ack 1401, win 65535, length 0
08:46:08.430957 IP 10.0.2.15.37432 > 194.29.160.95.443: Flags [P.], seq 1:577, ack 1, win 64240, length 576
08:46:08.431069 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [.], ack 577, win 65535, length 0
08:46:08.432623 IP 10.0.2.15.37434 > 194.29.160.95.443: Flags [P.], seq 1:577, ack 1, win 64240, length 576
08:46:08.432987 IP 194.29.160.95.443 > 10.0.2.15.37434: Flags [.], ack 577, win 65535, length 0
08:46:08.454432 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [P.], seq 1:577, ack 577, win 65535, length 152
08:46:08.454475 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [.], ack 153, win 64088, length 0
08:46:08.454506 IP 10.0.2.15.37430 > 194.29.160.95.443: Flags [.], seq 1:577, ack 153, win 64088, length 0
08:46:08.454507 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [.], ack 153, win 64088, length 51
08:46:08.458917 IP 10.0.2.15.37432 > 194.29.160.95.443: Flags [.], seq 577:628, ack 153, win 64088, length 51
08:46:08.458918 IP 194.29.160.95.443 > 10.0.2.15.37432: Flags [.], ack 628, win 65535, length 0
08:46:08.457956 IP 10.0.2.15.37434 > 194.29.160.95.443: Flags [P.], seq 577:628, ack 153, win 64088, length 51
08:46:08.458535 IP 194.29.160.95.443 > 10.0.2.15.37434: Flags [.], ack 628, win 65535, length 0
08:46:08.578127 IP 10.0.2.15.38692 > 172.217.20.170.443: Flags [S], seq 3387925364, win 64240, options [mss 1460,sackOK,Ts val 3739494413 ecr 0,nop,wscale 7], length 0
08:46:08.602789 IP 172.217.20.170.443 > 10.0.2.15.38692: Flags [S.], seq 74112001, ack 3387925365, win 65535, options [mss 1460], length 0
08:46:08.602763 IP 10.0.2.15.38692 > 172.217.20.170.443: Flags [.], ack 1, win 64240, length 0
08:46:08.604042 IP 10.0.2.15.38692 > 172.217.20.170.443: Flags [P.], seq 1:518, ack 1, win 64240, length 517
08:46:08.604315 IP 172.217.20.170.443 > 10.0.2.15.38692: Flags [.], ack 518, win 65535, length 0
```

Zad 4.

Uniwersytet Łódzki

Dane kontaktowe: <https://www.uni.lodz.pl/kontakt>

Adres Uniwersytet Łódzki ul. Narutowicza 68, 90-136 Łódź fax: (0 42)665 57 71, (0 42)635 40 43,
NIP: 724-000-32-43

Informacje z serwisu whois

DOMAIN NAME: lodz.pl |
registrant type: organization
nameservers: dns.man.lodz.pl. [212.51.192.2]
dns2.man.lodz.pl. [212.51.192.5]
dns4.man.lodz.pl. [194.204.158.82]
ns1.tpnet.pl. [80.50.50.100][2a01:1700:2:1::3264]
created: 1995.01.01 12:00:00
last modified: 2018.12.11 16:32:47
renewal date: 2019.12.31 13:00:00

option created: 2019.07.30 09:20:36
option expiration date: 2022.07.30 09:20:36

REGISTRAR:
OVH SAS
2 Rue Kellermann
59100 Roubaix
Francja/France
+48.717500200

Lista pracowników z możliwością pozyskania maili

- https://www.linkedin.com/search/results/people/?facetCurrentCompany=%5B%2215097344%22%5D&facetSchool=%5B%2215999%22%5D&origin=FACETED_SEARCH

Zad 5.

Przy pomocy wyszukiarki google wykorzystując następujące zapytania udało mi się znaleźć kilka plików, które prawdopodobnie nie powinny być publicznie dostępne:

Przykładowe zapytania

```
intitle:"index of" site:uni.lodz.pl intitle:"index of" inurl:uni.lodz.pl filetype:xls  
inurl:uni.lodz.pl intitle:"studen"
```

Przykładowe pliki które udało się znaleźć

Matura-wyniki_IB

Plik Edycja Widok Wstaw Formatuj Dane Narzędzia Dodatki Pomoc Ostatnia modyfikacja: chwilę temu Udostępnij

Nazwisko i imię

A	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN
1 Nazwisko i imię	Zad.15	Zad.16	Zad.17	Zad.18	Zad.19	Zad.20	Zad.21	Zad.22	Zad.23	Zad.24	Zad.25	Suma	Zad.24	Zad.25	Zad.21	Zad.22	Zad.23	Zad.24	Zad.25	Zad.31	Zad.32	Zad.33	Suma - otwarto	Suma całkowita	procenty
3 Bloch Szymon	1	0	1	0	1	1	0	0	0	0	0	12	0	0	0	0	1	1	0	1	1	2	14	28	
4 Cieślik Weronika	1	1	0	1	0	1	0	1	0	0	0	13	1	1	0	X	0	2	0	0	0	0	2	15	30
5 Forysiak Ola	1	0	1	1	0	1	0	0	0	0	0	9	0	0	0	0	0	0	0	0	3	3	3	24	
6 Furman Marta	0	1	1	0	1	1	0	0	1	0	10	2	0	0	0	0	2	0	0	0	0	2	12	24	
7 Golen Anna	1	1	0	0	1	0	0	0	0	0	1	7	1	1	0	X	0	2	0	0	0	2	9	18	
8 Janicka Karina	0	0	0	0	0	1	0	0	0	0	0	5	0	X	0	X	0	0	0	0	0	0	5	10	
9 Jarocki Maciej	1	1	0	1	1	1	1	0	1	0	0	14	1	0	1	2	0	4	0	3	2	5	9	23	
10 Kolodziej Ola	0	1	1	1	1	1	1	0	0	1	0	12	0	0	0	2	0	2	1	0	5	6	8	20	
11 Kolodziejczyk Alba	1	1	1	0	0	0	1	0	0	0	0	10	1	X	0	0	X	1	0	X	1	1	2	12	
12 Komorowska Kasia	1	1	1	1	0	1	1	0	1	0	1	14	0	0	2	0	1	3	1	0	0	1	4	18	
13 Krakowski Piotr	0	0	1	1	1	1	1	0	0	0	-	9	0	0	0	0	0	0	X	4	4	4	13	26	
14 Krawczyk Maciej	1	0	1	1	1	0	1	0	1	0	0	11	2	1	0	2	0	5	0	0	X	0	5	16	
15 Malicha Joanna	0	1	1	1	1	1	1	0	1	0	0	12	0	X	0	0	0	0	0	0	0	0	0	12	
16 Marszałek Wiktoria	1	1	0	0	1	1	0	1	1	1	1	17	1	1	0	2	0	4	1	4	X	5	9	26	
17 Matusiak Paulina	1	1	0	0	0	1	1	1	1	1	1	16	2	1	1	X	1	5	X	0	0	0	5	21	
18 Michorek Weronika	0	1	1	0	1	0	1	0	1	0	1	14	2	1	0	0	0	3	0	0	0	0	3	17	
19 Paciuch Ola	0	0	0	0	1	0	0	1	1	1	1	8	0	0	0	0	0	1	1	2	4	4	12	24	
20 Pogorzała Wiktoria	1	0	0	1	1	0	0	0	0	1	9	0	2	0	0	1	3	0	0	X	0	3	12	24	
21 Polka Kasia	1	0	1	1	0	1	0	0	0	1	13	0	0	0	2	0	2	2	1	1	4	6	19	38	
22 Rutkowska Patrycja	1	1	1	0	1	1	1	0	0	0	1	15	0	0	0	2	0	2	6	0	5	11	13	28	
23 Stachura Milena	1	1	1	0	1	0	1	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	8	16	

fx

A	B	C	D	E
1 nazwisko	imie		Komentarz	
2 Adamczyk	Marta		3 zapraszam na poprawkę	
3 Agata	Paulina		2 można poprawić o ile zaliczenie jest na 4	
4 Beta	Klaudia		2 można poprawić o ile zaliczenie jest na 4	
5 Biernacki	Artur	3+		
6 Borska	Joanna	2		
7 Czaja	Katarzyna	3+	zapraszam na poprawkę	
8 Czarna	Anita	2		
9 Gabryniak	Katarzyna	4	zapraszam na poprawkę	
10 Górecka	Beata	2	można poprawić o ile zaliczenie jest na 4	
11 Gwiżdżałka	Dominika			
12 Jasirińska	Anna	2	można poprawić o ile zaliczenie jest na 4	
13 Jóźwiak	Justyna	4	zapraszam na poprawkę	
14 Kiersnowska	Monika	2		
15 Koł	Szymon	3+		
16 Koziara	Edyta	3	zapraszam na poprawkę	
17 Król	Alina	2	zapraszam na poprawkę	
18 Król	Karolina	3+	zapraszam na poprawkę	
19 Król	Paulina			
20 Królikowska	Małgorzata	4		
21 Krysiak	Justyna	2	można poprawić o ile zaliczenie jest na 4	
22 Krysztofiak	Paweł	4	zapraszam na poprawkę	
23 Kuczyńska	Marilena			
24 Laskowski	Marcin			
25 Ledwojczyk	Maciej	2		
26 Łęcka	Izabella	2	można poprawić o ile zaliczenie jest na 4	
27 Łuczak	Justyna	3	zapraszam na poprawkę	
28 Majchrzak	Danuta	2		

Name Last modified Size Description

 Parent Directory	-	
 P7150073.JPG	2016-07-15 16:45 2.6M	
 P7150074.JPG	2016-07-15 16:46 2.7M	
 P7150075.JPG	2016-07-15 16:46 2.7M	
 P7150077.JPG	2016-07-15 17:59 2.7M	
 P7150078.JPG	2016-07-15 17:59 2.6M	
 P7150080.JPG	2016-07-15 18:03 2.7M	
 P7150081.JPG	2016-07-15 18:05 3.0M	
 P7150083.JPG	2016-07-15 18:30 3.1M	
 P7150084.JPG	2016-07-15 18:32 2.7M	
 P7150085.JPG	2016-07-15 18:32 2.8M	
 P7150086.JPG	2016-07-15 18:33 2.7M	
 P7150087.JPG	2016-07-15 18:33 2.7M	
 P7150088.JPG	2016-07-15 18:34 2.7M	
 P7160089.JPG	2016-07-16 09:23 2.9M	
 P7160108.JPG	2016-07-16 09:38 2.8M	
 P7160109.JPG	2016-07-16 09:38 2.6M	
 P7160110.JPG	2016-07-16 10:37 2.7M	
 P7160111.JPG	2016-07-16 10:37 2.8M	
 P7160112.JPG	2016-07-16 10:37 2.7M	
 P7160113.JPG	2016-07-16 10:41 2.7M	

Apache/2.4.25 (Debian) Server at math.uni.lodz.pl Port 80

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory	-		
[]	Thumbs.db	2010-10-15 10:26 19K		
[IMG]	DSC_0026.JPG	2010-10-15 10:26 2.3M		
[IMG]	DSC_0024.JPG	2010-10-15 10:26 2.3M		
[IMG]	DSC_0022.JPG	2010-10-15 10:26 2.7M		
[IMG]	DSC_0015.JPG	2010-10-15 10:26 2.6M		
[IMG]	DSC_0011.JPG	2010-10-15 10:22 633K		
[IMG]	DSC_0010.JPG	2010-10-15 10:21 2.4M		
[IMG]	DSC_0009.JPG	2010-10-15 10:21 2.2M		

Zad 6.

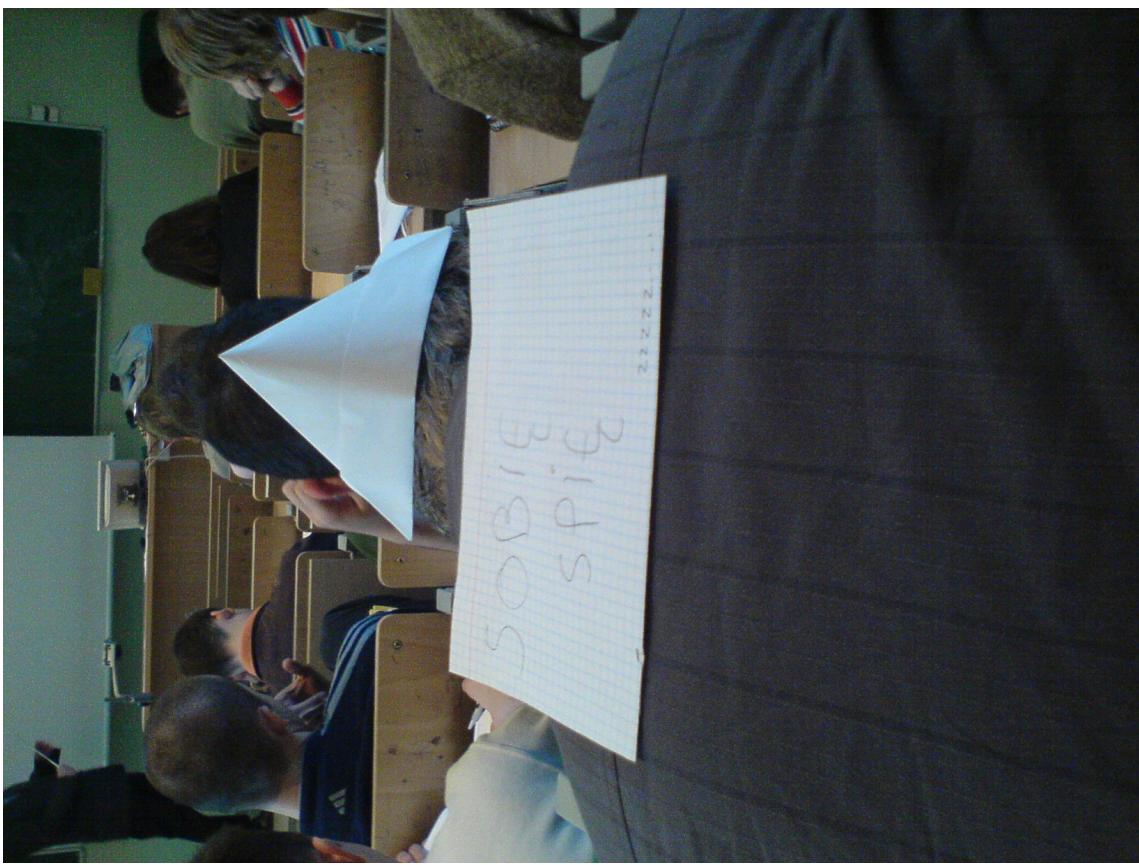
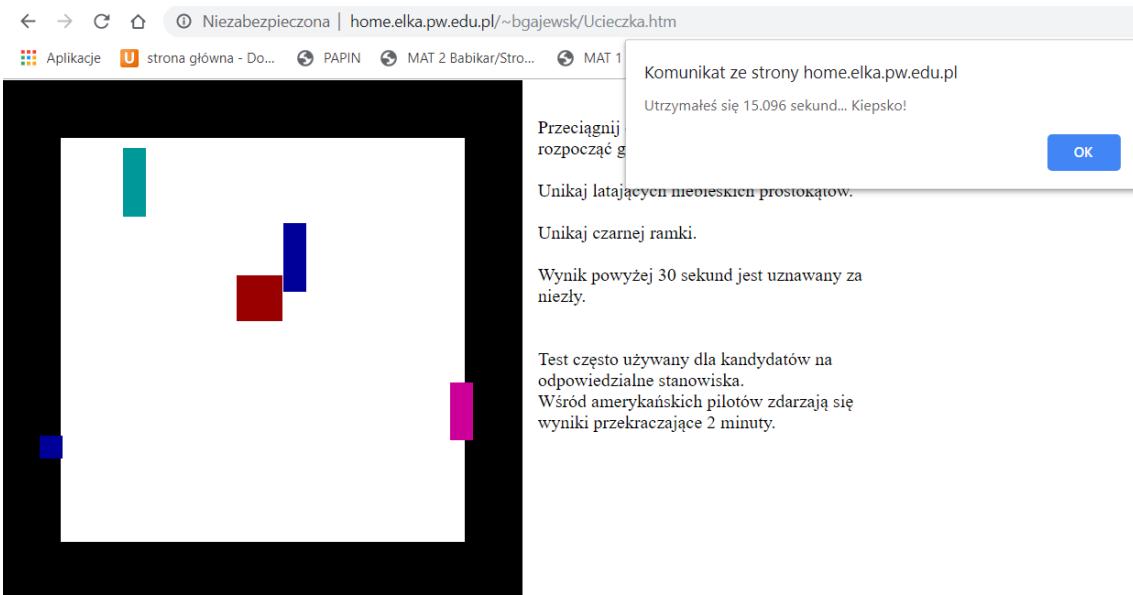
Próba wyszukania jakiś ciekawych informacji z domeny `pw.edu.pl` nie przyniosła zbyt wiele przydatnych informacji. Natomiast ilość odpowiedzi na zapytanie o serwery `ftp`, pliki `xls` i `pdf` w domenie `pw.edu.pl` jest dość spora. Większa ilość spędzonego czasu na żmudnym przeglądaniu wyników zapytań z pewnością dała by więcej interesujących rezultatów.

The image contains three separate Google search results pages. Each page has a red box highlighting the search count at the top of the results.

- Search Query:** `intitle:index of site:pw.edu.pl`
Results Count: Około 2 210 wyników (0,29 s)
- Search Query:** `filetype:xls inurl:pw.edu.pl`
Results Count: Około 474 wyników (0,28 s)
- Search Query:** `filetype:pdf inurl:elka.pw.edu.pl`
Results Count: Około 3 770 wyników (0,27 s)

Przykładowe pliki z Politechniki Warszawskiej które udało się znaleźć

- <http://wujek2.ia.pw.edu.pl/wm/archiwum/>
- <http://staff.elka.pw.edu.pl/>
- <http://home.elka.pw.edu.pl/~bqajewsk/>
- <http://home.elka.pw.edu.pl/~pnajgeba/>



Zad 7.

Whois Politechnika Warszawska

```
root@kali:~# whois pw.edu.pl
DOMAIN NAME:          pw.edu.pl
registrant type:      organization
nameservers:          arwena.nask.waw.pl. [193.59.201.28]
                      dns.fuw.edu.pl. [193.0.80.11]
                      europa.coi.pw.edu.pl. [194.29.128.2]
                      io.coi.pw.edu.pl. [194.29.128.1]
created:              1995.01.01 12:00:00
last modified:         2017.05.25 18:47:24
renewal date:         2022.12.31 13:00:00

no option

dnssec:               Unsigned

REGISTRAR:
nazwa.pl sp. z o.o.
ul. Mieczysława Medweckiego 17
31-870 Kraków
Polska/Poland
+48.801 33 22 33
+48.22 454 48 10
+48.22 454 48 08
kontakt@nazwa.pl
www.nazwa.pl

WHOIS database responses and Registrant data available at: https://dns.pl/en/whois
WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry system
```

Zad 8.

Serwery DNS megacorpone.com

```
root@kali:~# host -t ns megacorpone.com
megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
root@kali:~# host -t mx megacorpone.com
megacorpone.com mail is handled by 10 fb.mail.gandi.net.
megacorpone.com mail is handled by 20 spool.mail.gandi.net.
megacorpone.com mail is handled by 50 mail.megacorpone.com.
megacorpone.com mail is handled by 60 mail2.megacorpone.com.
```

Zad 9.

Skrypt w bashu przenoszący stefę

```
#!/bin/bash

if [ -z "$1" ]; then
echo "[*] Simple Zone transfer script"
echo "[*] Usage : $0 <domain name>"
exit 0
fi
for server in $(host -t ns $1 |cut -d" " -f4); do
host -l $1 $server |grep " has address"
done
```

```
root@kali:~# bash strefa.sh megacorpone.com
admin.megacorpone.com has address 38.100.193.83
beta.megacorpone.com has address 38.100.193.88
fs1.megacorpone.com has address 38.100.193.82
intranet.megacorpone.com has address 38.100.193.87
mail.megacorpone.com has address 38.100.193.84
mail2.megacorpone.com has address 38.100.193.73
ns1.megacorpone.com has address 38.100.193.70
ns2.megacorpone.com has address 38.100.193.80
ns3.megacorpone.com has address 38.100.193.90
router.megacorpone.com has address 38.100.193.71
siem.megacorpone.com has address 38.100.193.89
snmp.megacorpone.com has address 38.100.193.85
support.megacorpone.com has address 173.246.47.170
syslog.megacorpone.com has address 38.100.193.66
test.megacorpone.com has address 38.100.193.67
vpn.megacorpone.com has address 38.100.193.77
www.megacorpone.com has address 38.100.193.76
www2.megacorpone.com has address 38.100.193.79
```

Zad 10.

Transfer strefy przy użyciu dnsrecon

```
root@kali:~# dnsrecon -d megacorpone.com -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving SOA Record
[+]      SOA ns1.megacorpone.com 38.100.193.70
[*] Resolving NS Records
[*] NS Servers found:
[*]      NS ns1.megacorpone.com 38.100.193.70
[*]      NS ns2.megacorpone.com 38.100.193.80
[*]      NS ns3.megacorpone.com 38.100.193.90
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 38.100.193.80
[+] 38.100.193.80 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]      NS ns1.megacorpone.com 38.100.193.70
[*]      NS ns2.megacorpone.com 38.100.193.80
[*]      NS ns3.megacorpone.com 38.100.193.90
[*]      TXT Try Harder
[*]      MX @.megacorpone.com fb.mail.gandi.net 217.70.178.217
[*]      MX @.megacorpone.com spool.mail.gandi.net 217.70.178.1
[*]      A admin.megacorpone.com 38.100.193.83
[*]      A fs1.megacorpone.com 38.100.193.82
[*]      A www2.megacorpone.com 38.100.193.79
[*]      A test.megacorpone.com 38.100.193.67
[*]      A ns1.megacorpone.com 38.100.193.70
[*]      A ns2.megacorpone.com 38.100.193.80
[*]      A ns3.megacorpone.com 38.100.193.90
[*]      A www.megacorpone.com 38.100.193.76
[*]      A siem.megacorpone.com 38.100.193.89
[*]      A mail2.megacorpone.com 38.100.193.73
[*]      A router.megacorpone.com 38.100.193.71
[*]      A mail.megacorpone.com 38.100.193.84
[*]      A vpn.megacorpone.com 38.100.193.77
[*]      A snmp.megacorpone.com 38.100.193.85
[*]      A syslog.megacorpone.com 38.100.193.66
[*]      A beta.megacorpone.com 38.100.193.88
[*]      A intranet.megacorpone.com 38.100.193.87
[*]      A support.megacorpone.com 173.246.47.170
[*]
[*] Trying NS server 38.100.193.70
[+] 38.100.193.70 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED
[*]
[*] Trying NS server 38.100.193.90
[+] 38.100.193.90 Has port 53 TCP Open
[-] Zone Transfer Failed!
```