Sprawozdanie lista2 - bezpieczeństwo

Wojciech Wróblewski

October 2020

Podpunkt 1

Wykorzystam sesje pobrana z internetu aby wyodrebnić ssid sieci w zadanej sesji. Wyodrebniłem 168 różnych sieci.W tabeli niżej ssid i liczba wyszukiwań.

```
tshark -Y "wlan.fc.type_subtype eq 4" -T fields
-e wlan.ssid -r session.pcapng | sort | uniq -c
```

111	pasaz
117	**Pasaz Grunwaldzki free WiFi**
2	Patryczekk
14	PatrykToCh,j
1	paulina2
1	PhonePad
3	pioS9
433	PizzaHut Hotspot
.	.
.	.
.	.

SSID - Wrocław Free Wifi (dane ze wzgledu na covid pobrane z internetu)
SSID - DESKTOP-N464PQK 5690 (domowa sieć)

Podpunkt 2

Podłaczeni klienci do sieci wi-fi ze źródła (Wrocław Free Wifi). Bierzmy plik, wykonujemy polecenie w tshark-u, które wypisuje nam wszyscykie adresy mac, które połaczyły sie z siecia (różne).

```
tshark -r raport.pcapng -T fields -e
eth.dst | tr "\t" "\n" | sort | uniq
```

Output z teminala to:

01:00:5e:00:00:fb
01:00:5e:7f:ff:fa
04:79:70:1b:39:9a
10:44:00:be:de:35
30:4b:07:ba:cc:1b
33:33:00:00:00:01
33:33:00:00:00:02
33:33:00:00:00:16
33:33:ff:09:e9:22
33:33:ff:1b:39:9a
33:33:ff:7f:1e:31
33:33:ff:b8:f5:b6
33:33:ff:ba:cc:1b
33:33:ff:be:de:35
34:2e:b6:b8:f5:b6
54:25:ea:7f:1e:31
5c:c3:07:09:e9:22
8c:70:5a:ff:94:68
d8:9b:3b:eb:03:5d
f0:c8:50:31:61:b8
ff:ff:ff:ff:ff:ff

teraz wystarczy przekazać pipem do bashowej komendy wc i zliczamy ile było urzadzeń, które połaczyły sie z przykładowym źródłem.

```
tshark -r raport.pcapng  -T fields -e
eth.dst | tr "\t" "\n" | sort | uniq | wc -l
```

Dla raport.pcapng otrzymujemy wynik 45 różnych adresów mac. Dla sieci domowej uzyskałem 6 adresów. Pokrywajacych sie z oczekiwaniami.

00:...:9c
01:...:fb
01:...:fa
32:...:b5
50:...:e3
dc:...:4e

Podpunkt 3 oraz 4

Wypisz liste usług, stron oraz protokołów z jakich korzystali użytkownicy. Na poczatku policzmy ile różnych stron zostało dowiedzonych komenda

```
tshark -r raport.pcapng  -T fields -Y dns
-e dns.qry.name | sort | uniq | wc -l
```

Obswerujemy, że odwiedzone zostało 105 stron.

Wypiszmy storny z jakich korzsytali użytkownicy sieci wroclawfree wraz z liczba odsłon.

Wykorzsytujemy tutaj tshark oraz komendy skryptowe

```
tshark -r raport.pcapng  -T fields -Y dns
-e dns.qry.name | sort | uniq -c
```

40	video-frt3-1.xx.fbcdn.net
2	wazniak.mimuw.edu.pl
2	webpayment-promo.internet.apps.samsung.com
48	www.facebook.com
32	www.googleadservices.com
7	www.google-analytics.com
76	www.googleapis.com
455	www.google.com
62	www.gstatic.com
6	www.internet.apps.samsung.com
2	www.kopieckosciuszki.pl
4	www.nauka.gov.pl
4	www.pwr.edu.pl
2	www.w3.org
2	www.wppt.pwr.edu.pl
2	www.youtube.com
8	xpleiicjkwrldp
39	youtubei.googleapis.com
.	.
.	.
.	.

Wrocław Free Wifi

Z ciekawości możemy zobaczyć jakie usługi zostały wyszukane ponad 50 razy.

cdn.ampproject.org
check.googlezip.net
clients1.google.com
connectivitycheck.gstatic.com
datasaver.googleapis.com
edge-mqtt.facebook.com
googleads.g.doubleclick.net
graph.facebook.com
kopieckosciuszki.pl
mtalk.google.com
portal.fb.com
proxy.googlezip.net
www.googleapis.com
www.google.com
www.gstatic.com

Wrocław Free Wifi

Aby uzyskać powyższe wyniki wystarczy wcześniejsza metode przekazać to funkcji awk. (— awk ' if(1 >= 50)1=""; print ')

Sprawdźmy teraz protokoły jakie wystapiły w powyższej sesji . W tym celu wyświetlmy jako kolumne protokoły a nastepnie odfiltrujmy unikatowe wartości oraz zliczmy statystycznie licze wystapień.

```
tshark -r raport.pcapng  -T fields -e _ws.col.Protocol
| sort | uniq
```

412	ARP
168	DHCP
3184	DNS
4812	ESP
18	GQUIC
109	HTTP
9	HTTP/XML
102	ICMP
345	ICMPv6
60	IGMPv3
96	ISAKMP
194	MDNS
35	SSDP
537	SSL
18	SSLv2
5608	TCP
93	TLSv1
1581	TLSv1.2
304	TLSv1.3
340	UDP
3	ULP
26	XID

Wrocław Free Wifi

Teraz porownajmy z udostepniona siecia DESKTOP.
Uzyskujemy wynik 115 usług. Przykładowe w poniższej tabeli.

www.google.com
www.linkedin.com
www.onet.pl
www-przegladsportowy-pl.cdn.ampproject.org
www-rmf24-pl.cdn.ampproject.org
www-sport-pl.cdn.ampproject.org
play.googleapis.com
pl.m.wikipedia.org
poczta.onet.pl
.
.
.

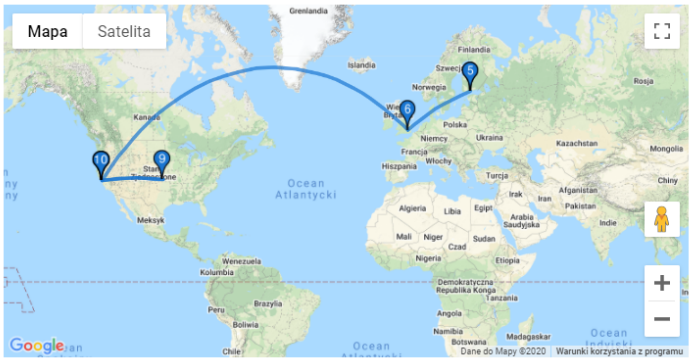
DESKTOP-N464PQK 5690

Zaprezentujmy wszystkie protokoły.

DHCP DNS GQUIC HTTP ICMP MDNS SSDP SSL TCP TLSv1 TLSv1.2 TLSv1.3 UDP	DESKTOP-N464PQK 5690

Podpunkt 5

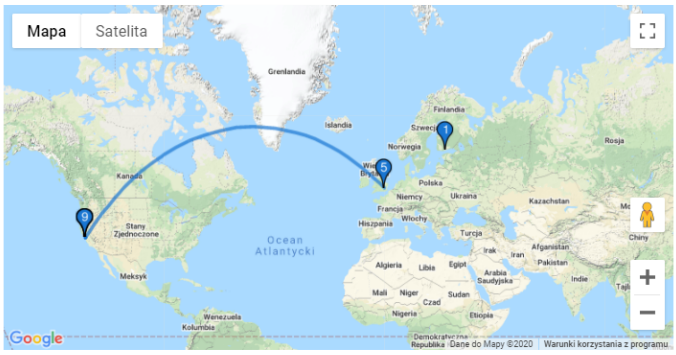
Mape lokalizacji z którymi łaczyły sie komputery. Możemy wykorzystać visual traceroute. Dla tego oprogramowania pokażemy lokalizacje dla kilku najbardziej obleganych usług z list wyżej.



traceroute to www.google.com (216.58.212.196), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	94.237.52.1	94.237.52.1	0.137
2	100.69.36.209	100.69.36.209	0.293
3	172.17.255.225	172.17.255.225	0.353
4	172.17.255.249	172.17.255.249	0.290
5	r1-lon1-po1.uk.net.upcloud.com	94.237.0.120	0.287
6	5-1-33.ear2.London1.Level3.net	212.187.165.105	0.520
7	72.14.212.120	72.14.212.120	0.678
8	108.170.246.129	108.170.246.129	0.674
9	209.85.248.241	209.85.248.241	1.175
10	ams16s21-in-f4.1e100.net	216.58.212.196	0.672

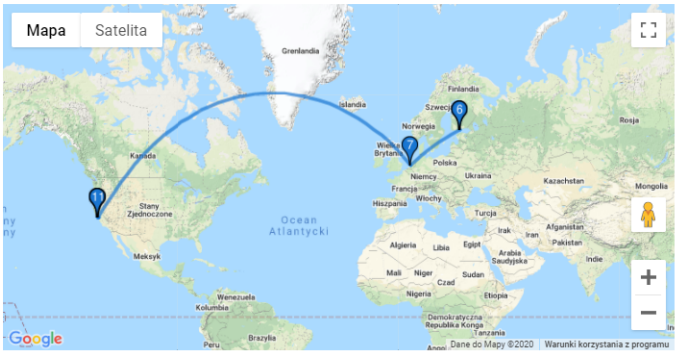
Figure 1: google.com



traceroute to www.gstatic.com (216.58.198.163), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	94.237.52.1	94.237.52.1	0.151
2	100.69.4.209	100.69.4.209	0.272
3	172.17.255.229	172.17.255.229	0.298
4	172.17.255.253	172.17.255.253	0.262
5	5-1-33.ear2.London1.Level3.net	212.187.165.105	0.377
6	72.14.212.120	72.14.212.120	0.613
7	108.170.246.129	108.170.246.129	0.596
8	108.170.232.97	108.170.232.97	0.596
9	lhr25s10-in-f3.1e100.net	216.58.198.163	0.583

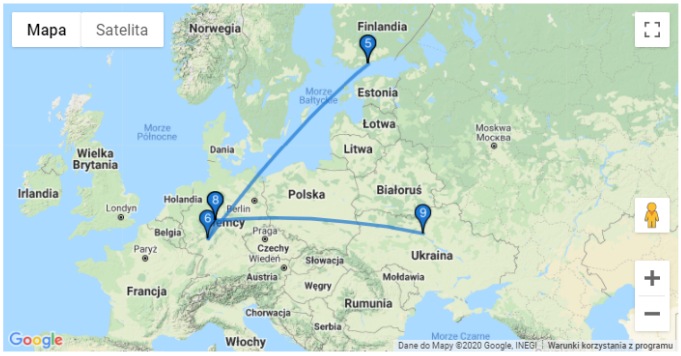
Figure 2: gstatic.com



traceroute to portal.fb.com (157.240.201.17), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	94.237.52.1	94.237.52.1	0.124
2	100.69.36.209	100.69.36.209	0.278
3	172.17.255.225	172.17.255.225	0.297
4	172.17.255.249	172.17.255.249	0.247
5	r1-lon1-po1.uk.net.upcloud.com	94.237.0.120	0.271
6	r1-ams1-et2.nl.net.upcloud.com	94.237.0.46	5.418
7	80.249.212.174	80.249.212.174	6.199
8	po141.asw01.ams3.tfbnw.net	129.134.34.162	6.134
9	po233.psw01.ams4.tfbnw.net	129.134.47.219	6.017
10	173.252.67.15	173.252.67.15	6.019
11	edge-star-shv-01-ams4.facebook.com	157.240.201.17	6.115

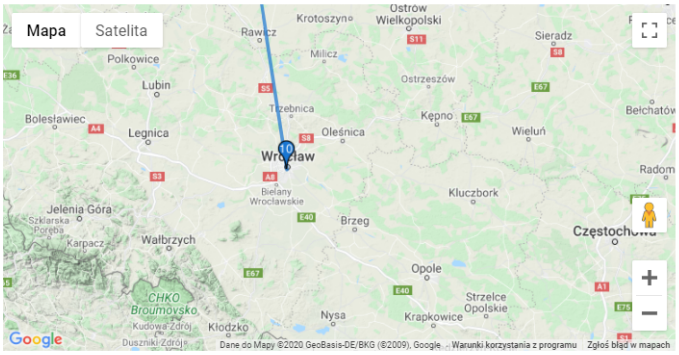
Figure 3: facebook.com



traceroute to kopieckosciuszki.pl (94.130.84.166), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	94.237.52.1	94.237.52.1	0.143
2	100.69.36.209	100.69.36.209	0.347
3	172.17.255.225	172.17.255.225	0.358
4	172.17.255.249	172.17.255.249	0.351
5	r1-fra1-et2.de.net.upcloud.com	94.237.0.48	16.225
6	decix2-gw.hetzner.com	80.81.193.164	16.630
7	core11.nbg1.hetzner.com	213.239.245.34	19.449
8	ex9k1.dc3.nbg1.hetzner.com	213.239.229.154	19.833
9	pro20.cyber-folks.pl	94.130.84.166	19.774

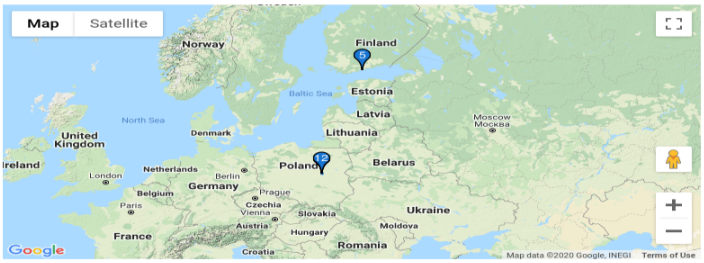
Figure 4: kopieckosciuszki.pl



traceroute to www.pwr.edu.pl (156.17.16.240), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	94.237.52.1	94.237.52.1	0.106
2	100.69.36.209	100.69.36.209	0.284
3	172.17.255.225	172.17.255.225	0.283
4	172.17.255.249	172.17.255.249	0.275
5	195.66.225.24	195.66.225.24	0.825
6	nl-sar.nordu.net	109.105.97.124	8.094
7	de-hmb.nordu.net	109.105.98.124	23.356
8	ndn-gw.pionier.gov.pl	109.105.98.125	24.701
9	z-poznan-gw3.wroclaw.10Gb.rtr.pionier.gov.pl	212.191.224.106	30.484
10	z-wask2-do-pwr2.pwrnet.pwr.wroc.pl	156.17.18.244	30.651
11	*	*	*

Figure 5: wppt.pwr.edu.pl



traceroute to poczta.onet.pl (213.180.141.145), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	94.237.52.1	94.237.52.1	0.134
2	100.69.36.209	100.69.36.209	0.289
3	172.17.255.225	172.17.255.225	0.308
4	172.17.255.249	172.17.255.249	0.264
5	r1-fra1-et2.de.net.upcloud.com	94.237.0.48	16.089
6	*	*	*
7	83.238.249.64	83.238.249.64	35.205
8	83.238.248.31	83.238.248.31	33.567
9	*	*	*
10	*	*	*
11	sdr1.m10r2.z.j.ruc-br1.link4.net.onet.pl	213.180.152.135	39.925
12	oa145.any.onet.pl	213.180.141.145	39.297

Figure 6: poczta.onet.pl