

Raport z monitorowania ruchu sieciowego

Radosław Wojtczak, Michał Krosny
254607,256791

November 7, 2021

1 Przeprowadzone badania ruchu sieciowego

Lokalizacja	Nazwa AP
Lubin Cuprum Arena	Free WiFi
Wrocław Wrocławia	Wroclavia Free
Wrocław Wrocławia	Free wifi
Wrocław Wrocławia	Open WiFi
Wrocław Dworzec Gł.	Open WiFi
KD Wrocław-Lubin	Open Free WiFi

Zgodnie z poleceniem zadania karta sieciowa laptopa została ustawiona w tryb monitorowania *promiscuous mode*. Następnie zostały udostępnione sieci Wi-Fi o różnych nazwach, w różnych lokalizacjach, co prezentuje powyższa tabela. Otrzymane dane zostały zebrane przy pomocy programu WireShark. Badania trwały od 20 do 50 minut i tylko dwa z nich zakończyły się zaobserwowaniem jakiegokolwiek ruchu. Były to ap: Wrocławia pod nazwą Free WiFi oraz KD Wrocław-Lubin pod nazwą Open Free WiFi.

2 Wyszukiwane SSID

Czytanie danych odbywało się poprzez sprawdzanie pakietów, gdzie typ był równy "probe request". Wartości nazywane jako "wildcard" w tym sprawozdaniu zostały pominięte. Badanie przeprowadzone w lokalizacji Cuprum Arena Lubin:

3792	Tofik97	HUAWEI-B535-03D8
Stage	DWR-932_DDEC06	NETIASPOT-866470
emil	Livebox-BC16	NETIASPOT-2.4GHz-
l	DWR-116_C42C12	awwT
P20Pro	willa3	CircleHostel
EDV	PARK_ROZRYWKI	NETIASPOT-BA0E70
EDV_5G	NETIASPOT-2.4GHz-	iphone mateusx
McD-Hotspot	4de5	netiaspot-ds44co
UPC39A47D5	NETIASPOT-E58B60	PizzaHut Hotspot
B593-8457	ING Internet	Cuprum-Arena-A
AndroidAP	UPC4850294	RESTAURACJA
potaczek	Lenovo TAB4 10	UPC244749285
eBos	Klient	zosiaaa
UPC242544703	wksraclawicka	SUSHIdlaMNIE
sala19.local	DWR-960_83236D	HUAWEI-14B7

ARKA_D	EuroWeek123	marzec
CPE_B8EDB9	UPCC6A6EA2	Redmi
UPC9939797	PHILIPS	seaside
COSTA COFFEE	MikroTik-6187F1	tmobile
0028635B	TP-LINK_ECCAD2	AndroidAP12
null	ROBOT###c3-aa-f7	Internet_Domowy_4A302F
HUAWEI-E5186-2FF4	Osiek2	
MikroTik-6187F0	orange	

3 Podłączeni użytkownicy

Free WiFi	Open Free WiFi
06:b1:34:3f:97:e0	30:45:96:1b:e9:ba
f2:56:d9:85:67:1f	88:11:96:83:46:b1

Przy pomocy zakładki "Statystyka" w programie WireShark została sporządzona powyższa lista unikalnych adresów MAC podłączony do sieci.

Pozostałe badania zakończyły się zerową ilością połączeń.

Ograniczona liczba użytkowników znacząco wpłynęła na ograniczoną liczbę danych otrzymanych w ramach eksperymentu. Zauważamy, że jedyni użytkownicy zalogowali się, gdy nazwa sieci posiadała w sobie frazy "Free", "WiFi" czy "Open".

4 Odwiedzane strony

Dokonując analizy odwiedzanych stron przez użytkowników zauważamy, że

- Użytkownicy mimo korzystania z otwartej sieci wciąż łączą się z takimi stronami jak *www.google.com*, *www.linkedin.com*, czy *www.wp.pl*
- Część z otrzymanych serwisów (Przykład: *connectivitycheck.android.com*) są serwisami, których zadaniem jest sprawdzenie, czy urządzenie wciąż jest połączone z internetem.

KD Lubin-Wrocław:

adservice.google.com	cdn.playa-games.com	dimg-pa.googleapis.com
android.clients.google.com	cfg.sfgame.de	edge-mqtt.facebook.com
android.googleapis.com	chat-e2ee-mini.facebook.com	encrypted-tbn0.gstatic.com
api.gameanalytics.com	clients3.google.com	encrypted-tbn1.gstatic.com
app-measurement.com	connectivitycheck.android.com	encrypted-tbn2.gstatic.com
b-graph.facebook.com	connectivitycheck.gstatic.com	encrypted-tbn3.gstatic.com
cdn.ampproject.org	content-autofill.googleapis.com	g.whatsapp.net

geller-pa.googleapis.com
googleads.g.doubleclick.net
graph.facebook.com
growth-pa.googleapis.com
i.ytimg.com
inbox.google.com
infinitedata-pa.googleapis.com
launches.appsflyer.com
lh3.googleusercontent.com
lh5.googleusercontent.com
lookaside.facebook.com

mail.google.com
mtalk.google.com
notifications-pa.googleapis.com
peoplestack-pa.googleapis.com
play.googleapis.com
play-fe.googleapis.com
play-lh.googleusercontent.com
scontent.ftxl2-1.fna.fbcdn.net
ssl.gstatic.com
static.whatsapp.net
store.hispace.hicloud.com

time.android.com
video.fpoz6-1.fna.fbcdn.net
w51.sfgame.net
www.google.com
www.googleadservices.com
www.googleapis.com
www.gstatic.com
xtrapath2.izatcloud.net
youtubei.googleapis.com

Wroclavia:

11603.lsapp.eu
26-courier.push.apple.com
34-courier.push.apple.com
3pd.am5.vip.prod.criteo.com
3pd.criteo.com
safeiframe.google syndication.com
a.teads.tv
a1744.dscg2.akamai.net
a1813.dscd.akamai.net
a1845.dscg2.akamai.net
a1931.dscgi3.akamai.net
a1958.dscd.akamai.net
a2047.dsca.akamai.net
aax-eu.amazon-adsystem.com
abs-0.twimg.com
abs-zero.twimg.com
ad.doubleclick.net
ads.businessclick.com
ads.mopub.com
adservice.google.com
adservice.google.pl
adx.adform.net
ams01.search.spotxchange.com
api.flightproxy.teams.microsoft.com
api2.branch.io
api3.cc.skype.com
api-glb-euc1a.smoot.apple.com
cloudapp.net
api-v3.tinypass.com
app.snapchat.com
app-analytics-v2.snapchat.com
apple.com
app-measurement.com
apresolve.spotify.com
assets-jpcust.jwpsrv.com
authorisation.grupaonet.pl
authsvc.teams.microsoft.com
aws.api.sc-gw.com
aws.api.snapchat.com
aws.duplex.snapchat.com
axel-springer-pl-d.openx.net
b101.s372.meetrics.net
bc.wp.pl
bidder.am5.vip.prod.criteo.com
bidder.criteo.com
bidder.par.vip.prod.criteo.com

blob.byaprdstr10a.store.core.windows.net
bolt-gcdn.sc-cdn.net
buy.tinypass.com
c.amazon-adsystem.com
c2.piano.io
safeiframe.google syndication.com
captive.apple.com
captive.g.aaplimg.com
cb.mopub.com
safeiframe.google syndication.com
cc-euwe-05-skype.cloudapp.net
cdn.apple-mapkit.com
cdn.branch.io
cdn.brandmetrics.com
cdn.jwplayer.com
cdn.syndication.twimg.com
cdn.tinypass.com
cf-st.sc-cdn.net
chat-e2ee-mini.c10r.facebook.com
chat-e2ee-mini.facebook.com
chatsvcagg.teams.microsoft.com
cl2.apple.com
cl5.apple.com
clients.config.office.net
clients.l.google.com
clients1.google.com
clients3.google.com
cmp.dreamlab.pl
codepush.blob.core.windows.net
codepush.teams.microsoft.com
collector.brandmetrics.com
config.teams.microsoft.com
config-chr.health.apple.com
configuration.ls.apple.com
connect.facebook.net
contentsync.onenote.com
cosmic-east-us-ns-8f4565d3f227.trafficmanager.net
cs386.wpc.edgecastcdn.net
cs45.wac.edgecastcdn.net
cs491.wac.edgecastcdn.net
csi.gstatic.com
csr.onet.pl
d1v810m8ywaj43.cloudfront.net
d1ykf07e75w7ss.cloudfront.net

dlw48hg4yxj1k.cloudfront.net
dart.l.doubleclick.net
dealer.spotify.com
delivery.clickonometrics.pl
df.trap.teams.microsoft.com
dual-spo-0004.spo-msedge.net
e10499.dsce9.akamaiedge.net
e11290.dspg.akamaiedge.net
e1329.g.akamaiedge.net
e14868.dsce9.akamaiedge.net
e3811.e9.akamaiedge.net
e4466.g.akamaiedge.net
e6987.dsce9.akamaiedge.net
e69896.dscapi6.akamaiedge.net
e8037.i.akamaiedge.net
e9957.b.akamaiedge.net
edge-mqtt.facebook.com
edge-web-dual-gslb.spotify.com
eduwroclaw.sharepoint.com
eduwroclaw-my.sharepoint.com
embed.dugout.com
emea.ng.msg.teams.microsoft.com
entitlements.jwplayer.com
eqx.smartadserver.com
etoto-platform.onet.pl
euaz.tr.teams.microsoft.com
eu-central-courier-4.push-apple.com.akadns.net
eudb.clients.config.office.akadns.net
europe-west1-gcp.api.snapchat.com
eu-west1-aws.duplex.sc-gw.com
events.ocdn.eu
experience.tinypass.com
external.fpoz6-1.fna.fbcdn.net
external.xx.fbcdn.net
facebook.com
fastlane.rubiconproject.com
fbcdn.net
fbs.smoot.apple.com
fbsbx.com
firebase logging-pa.googleapis.com
flightproxy-ukso-02-teams.cloudapp.net
fonts.googleapis.com

fonts.gstatic.com	instagram.fpoz6-1.fna.fbcdn.net	pop-esv5.mix.linkedin.com
fonts.wpcdn.pl	iphone-ld.apple.com	prd.jwpltx.com
gapl.hit.gemius.pl	jwplayer-	prebid-eu.creativecdn.com
gateway.facebook.com	dualstack.map.fastly.net	prebid-server.rubiconproject.com
gateway.fe.apple-dns.net	kropka.onet.pl	prebid-server-perf-
gateway.icloud.com	l-0005.l-msedge.net	eu.rubiconproject.net.akadns.net
gcp.api.sc-gw.com	lb._dns-sd._udp.0.0.0.10.in-	presence.teams.microsoft.com
gcp.api.snapchat.com	addr.arpa	prg.smartadserver.com
gcs.sc-cdn.net	lb._dns-sd._udp.0.0.42.10.in-	pro-accounts.snapchat.com
gde-default.hit.gemius.pl	addr.arpa	profiles.tagger.opecloud.com
get-bx.g.aaplimg.com	lb._dns-	pulseembed.eu
go.microsoft.com	sd._udp.253.27.128.10.in-	px.ads.linkedin.com
go.trouter.teams.microsoft.com	addr.arpa	rt.inistrack.net
googleads.g.doubleclick.net	lcdn-locator.apple.com	upload.facebook.com
googleads4.g.doubleclick.net	lcdn-locator-	s.mopub.com
google-analytics.com	usuqo.apple.com.akadns.net	s.sc-cdn.net
graph.facebook.com	liveblog-push.dreamlab.pl	s0.2mdn.net
graph.instagram.com	liveblog-talos.dreamlab.pl	s-0005.s-msedge.net
grid.bidswitch.net	login.microsoftonline.com	s0-2mdn-net.l.google.com
gs-loc.apple.com	login5.spotify.com	s1.adform.net
gs-loc.ls-apple.com.akadns.net	lookaside.facebook.com	s372.meetrics.net
gsp10-ssl.apple.com	ls.hit.gemius.pl	s372.mxcn.net
gsp10-ssl.ls-apple.com.akadns.net	m.facebook.com	sb.scorecardresearch.com
gsp64-ssl.ls.apple.com	mamls-prod-weu-	scdnco.spotify.map.fastly.net
gsp64-ssl.ls-apple.com.akadns.net	ip.westeurope.cloudapp.azure.com	scontent.fpoz6-1.fna.fbcdn.net
gsp85-ssl.ls.apple.com	mamservice.manage.microsoft.com	scontent.xx.fbcdn.net
gsp85-ssl.ls2-	mask.apple-dns.net	scontent-frx5-
apple.com.akadns.net	mask.icloud.com	1.cdninstagram.com
gspe12-ssl.ls.apple.com	me.apple-dns.net	search.spotxchange.com
gspe19-ssl.ls.apple.com	media-	securepubads.g.doubleclick.net
gspe35-ssl.ls.apple.com	shield.jwplayer.map.fastly.net	self.events.data.microsoft.com
gspe76-ssl.ls.apple.com	mesu.apple.com	setup.fe.apple-dns.net
gspe79-ssl.ls.apple.com	metrics.icloud.com	setup.icloud.com
gsp-ssl.ls.apple.com	mqtt.c10r.facebook.com	s-eu-1.pushpushgo.com
gstaticads.l.google.com	ms.sc-jpl.com	sgqcvfjvr.onet.pl
gtq.sct.sc-prod.net	msgapi-prod-weu-azsc1-	smoot-feedback.v.aaplimg.com
gum.am5.vip.prod.criteo.com	1.cloudapp.net	smoot-searchv2-
gum.criteo.com	msg-r-latest.c10r.facebook.com	eucla.v.aaplimg.com
gum.par.vip.prod.criteo.com	mvm.snapchat.com	snap.api.mapbox.com
guzzoni.apple.com	mvp.onet.pl	spclient.wg.spotify.com
hbopenbid.pubmatic.com	naanalle.pl	sportowefakty.wp.pl
hbopenbid22000nf.pubmatic.com	netcts.cdn-apple.com	star.c10r.facebook.com
hierarchyapi.onenote.com	nlb-aws-fr-verona-	star-mini.c10r.facebook.com
htlb.casalemedia.com	b3549c64d24264e3.elb.eu-central-	static.am5.vip.prod.criteo.net
https://app-	1.amazonaws.com	static.criteo.net
measurement.com/sdk-exp	nstrp.adform.net	static.doubleclick.net
i.connectad.io	ocdn.eu	static.par.vip.prod.criteo.net
i.instagram.com	ocsp2.apple.com	static.xx.fbcdn.net
i.scdn.co	onedscolprdcus12.centralus.cloudapp.azure.com	static-doubleclick-
ib.adnxs.com	onedscolprdcus00.eastus.cloudapp.azure.com	static-comnet.l.google.com
ib.anycast.adnxs.com	onedscolprdwus11.westus.cloudapp.azure.com	statics.teams.cdn.office.net
ic3.events.data.microsoft.com	onet.hit.gemius.pl	stats.g.doubleclick.net
images.bitmoji.com	pagead2.google syndication.com	stats.l.doubleclick.net
imasdk.googleapis.com	pagead46.l.doubleclick.net	substrate.office.com
impala-external-lb-	pagead-	swallow.apple.com
1441126057.us-east-	googlehosted.l.google.com	swallow-apple-
1.elb.amazonaws.com	parasol.wroclaw.pl	com.v.aaplimg.com
inappcheck.itunes.apple.com	partnerad.l.doubleclick.net	SXF-efz.ms-acdc.office.com
inappcheck-lb.itunes-	pbs.twimg.com	syndication.twitter.com
apple.com.akadns.net	pixel.wp.pl	tagged-
instagram.c10r.instagram.com	platform.twitter.com	by.rubiconproject.net.akadns.net
instagram.com	player-api.dreamlab.pl	tagger.opecloud.com

teams.events.data.microsoft.com	d5b3.westeurope.cloudapp.azure.com	www.googletagmanager.com
teams.microsoft.com	weather-data.apple.com	www.googletagservices.com
time.apple.com	weather-	www.icloud.com
tmsg-euno-azsc-01-csa-	data.apple.com.akadns.net	www.linkedin.com
dns.northeurope.cloudapp.azure.com	weather-edge.apple.com	www.microsoft.com
tpc.googlesyndication.com	weather-edge.news.apple-dns.net	www.przegladsportowy.pl
tr.teams.microsoft.com	web.facebook.com	www.spotify.com
track.adform.net	websocket.wp.pl	www.tm.ak.prd.aadg.akadns.net
track-eu.adformnet.akadns.net	virtualn-d.openx.net	www.wp.pl
us-central1-gcp.api.snapchat.com	world-gen.g.aaplimg.com	www.youtube.com
us-east1-aws.api.snapchat.com	wp.hit.gemius.pl	www-google-
us-east4-gcp.api.sc-gw.com	wpcdn.pl	analytics.l.google.com
us-east4-gcp.api.snapchat.com	www.apple.com	www-
v.wpimg.pl	www.facebook.com	googletagmanager.l.google.com
video.fpoz6-1.fna.fbcdn.net	www.google.com	youtubei.googleapis.com
videos-fms.jwpsrv.com	www.google.pl	
waws-prod-am2-391-	www.google-analytics.com	

5 Wykorzystywane protokoły i usługi

Wroclavia:

Usługi na podstawie portów:

http
https
hpvirtgrp
afs3-fileserver

Protokoły:

TCP
TLSv1.2
SSL
ARP
MDNS
XID
ICMPv6
DHCP
ICMP
DNS
HTTP
MPTCP
IGMPv2
TLSv1.3
SSLv2
QUIC
XMPP/XML
NTP
TLSv1

KD Lubin-Wrocław:

Usługi na podstawie portów:

http
unisys-eportal
asihpi
https
blp5
caerpc
turbonote-1
invision-ag
robotraconteur
ssr-servermgr
ortec-disc
f1-control
qdb2service
z-wave-s
m3da-disc
kastenxpipe
crescoctrl-disc
cscdfirewall

Protokoły:

MDNS
NBNS
XID
ICMPv6
DHCP
ARP
ICMP
DNS
TCP
HTTP
TLSv1.3
TLSv1.2
QUIC
SSL
SSLv2
NTP
UDP

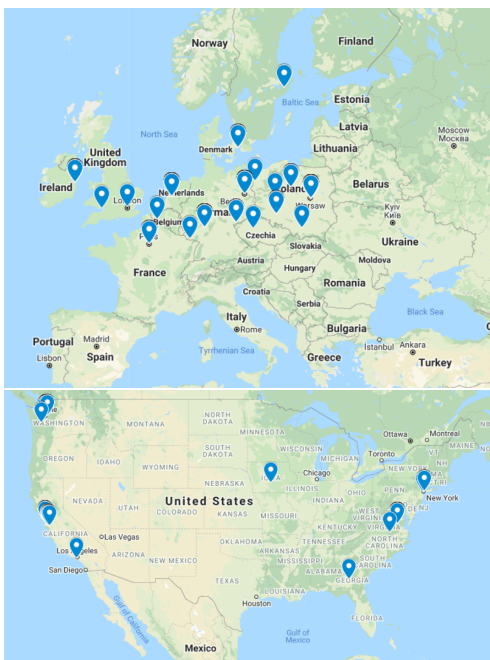
Wszystkie strony używały szyfrowania. Nieszyfrowane protokoły były używane jedynie do prostych czynności takich jak sprawdzenie stanu połączenia z internetem.

6 Lokalizacje

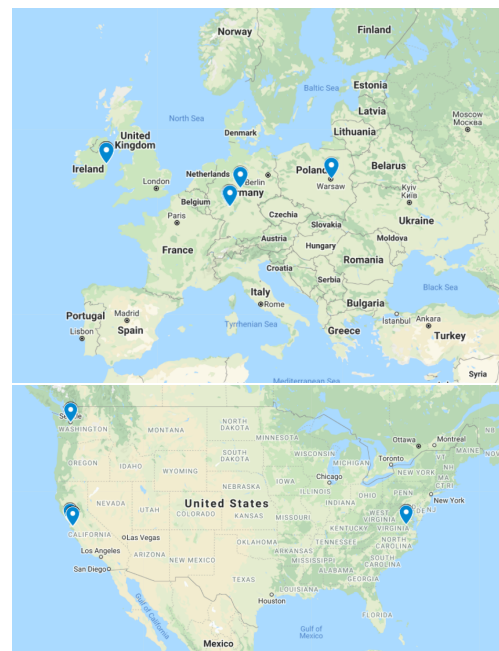
Przy pomocy pliku *getloc.py* adresy ip zamieniane są na plik csv z współrzędnymi geograficznymi. Następnie współrzędne geograifczne zostały zinterpretowane przy pomocy Google Maps.

Rezultat w postaci zdjęć, przedstawiających miejsca geograficzne, w których znajdowały się serwery, z którymi użytkownicy chcieli nawiązać połączenie:

Wroclavia:



KD Lubin-Wrocław:



7 Wnioski

Większość użytkowników smartfonów bądź laptopów w miejscach publicznych w 2021 korzysta z własnego internetu w celu połączenia się z siecią. W odróżnieniu od paru lat wstecz, aktualnie takowy internet pozwala na duży transfer danych przy stosunkowo niskiej cenie. Korzystanie z własnego pakietu internetu jest dodatkowym środkiem bezpieczeństwa gdyż, jak powyższy

raport przedstawia, każda sieć otwarta jest podatna na podsłuchiwanie, co może spowodować utratę danych na rzecz niepowołanej osoby.