Karolina Antonik
Joanna Szołomicka

RAPORT

BEZPIECZEŃSTWO KOMPUTEROWE
LISTA NR 2

Grupa laboratoryjna: piątek 13:15
23.10.2019

Podpunkt 1. Lista poszukiwanych SSID

Zadanie polegało na znalezieniu SSID poszukiwanych sieci, do których chciały się podłączyć urządzenia. Do nasłuchiwania sieci użyłyśmy komend:

sudo airmon-ng start <interface>, pozwala ona na włączenie trybu Monitor

sudo airodump-ng <monitor mode interface> -w capture --output-format csv, dane z nasłuchiwania zostały zapisane do pliku capture.csv

W zebranych przez nas danych otrzymałyśmy następujące informacje:

- H&M Free WiFi
- 192.168.0.17
- iPhone
- McD-Hotspot
- KFC Hotspot
- UPC247114385
- 123_marcin_345
- BTHub5-6H2P
- Teletorium
- FA PASAZ Guest
- AndroidAP
- domownik i gosc
- TP-LINK_E897A6
- Zara-WiFi
- Redmi
- WLAN1-000430
- WIFI-SRIFI
- Net
- absyntapart413
- 12345678
- UPC8626737
- HIDE_N
- Livebox-DE3D
- Tenda
- YDXJ_4758582_5G
- Notino_Free
- KKnetwork
- umowsienalizing
- 101
- krzych
- LaGrotta_Gosc
- lambrandamp
- infostrada
- 82040616834qwe
- UPC5576833
- parus
- mBank
- multimedia_kruszwicka10
- FRITZ!Box 7362 SL
- marcin
- Otwarta
- Flixbus
- IBIS
- 1111111111pol
- WLR_2
- hihaxC5.drkkjf
- euroweekp1
- UPC249609200
- xfff fnfjiujfifnfkfmfkfffjfjufff
- xjrct
- Internet_Domowy_28558D
- py slo
- PKP FREE WIFI
- VM9492864
- AndroidShare_8831
- vlad
- multimedia_multimedialne
- fh
- tzngx0uv
- funbox
- Airbox-F01E
- 82040616832qwe
- WLAN-142423
- UPC8198644
- SUDETY_HOTSPOT
- UPC240389983
- jxC3xAEqwfaydeygh
- biedronka
- H368N0DF7D0
- fun box
- Tenda_0DE6A8
- free wifi
- HUAWEI-B315-67F2
- bomberos
- Engelhart
- tzngxOuv
- REY ARTURO
- mondeo18
- Hotspot.....xB7xFF..
- recepcija
- krzychoq
- wanowice3
- eduroam
- EuroWeek_1
- Darmowe_Orange_WiFi
- PizzaHut Hotspot
- AndroidHotspot3374
- **Pasaz Grunwaldzki free WiFi**
- HUAWEI-B315-F3E1
- myBabyCam-E914
- Pilczycka100
- Mimi4545
- Orange-1E7F-EXT
- Social WiFi
- Prodigo
- iCam-SC400
- Renblade
- TP-LINK_
- 3556DE
- HUAWEI-B315-67F2
- 5G-Vectra-WiFi-B82782
- TKSaldanha
- Kokbhbbccvnknnbghbbb bjjjjkjjhhh

Podpunkt 2. Statystyka podłączonych urządzeń

Po udostępnieniu publicznego hotspotu nasłuchiwałyśmy ruch naszej sieci w programie Wireshark. Poniżej przedstawiona jest liczba urządzeń, jakie chciały przyłączyć się do naszych sieci w zależności od ich nazw SSID:

Nazwa sieci	McDonald	Galeria	Pasaz Grunwaldzki	Pasibus
Liczba podłączonych urządzeń	20	9	4	11

Dane te otrzymałyśmy używając następującego filtra z programu Wireshark: *dhcp.option.dhcp == 5*, który filtruje odpowiedzi DHCP po typie wiadomości i wyświetla tylko wiadomość typu ACKNOWLEDGEMENT. Następnie zliczyłyśmy do ilu różnych adresów MAC wysłana była owa wiadomość i dostałyśmy liczbę urządzeń, które się podłączyły do naszego hotspotu.
Możliwe było również uzyć filtra: *dns* i następnie zliczyć ilość różnych adresów MAC. Jednak uznałyśmy, że skorzystamy z pierwszej metody, gdyż umożliwi nam ona podliczenie też tych urządzeń, które się do nas podłączyły, ale nie korzystały z protokołu DNS.

Podpunkt 3. Lista stron www

Lista wybranych stron www:

- instagram.com
- www.google.com
- youtube-ui.l.google.com
- gapl.hit.gemius.pl
- keyvalueservice.fe.apple-dns.net
- gsp-ssl-dynamic.ls4-apple.com.akadns.net
- partnerad.l.doubleclick.net
- lcdn-locator-usuqo.apple.com.akadns.net
- accounts.google.com
- cdn-content.ampproject.org
- e25611.f.akamaiedge.net
- cloudconfig.googleapis.com
- settings.crashlytics.com
- p17-buy.itunes-apple.com.akadns.net
- gsp64-ssl.ls-apple.com.akadns.net
- fmfmobile.fe.apple-dns.net
- events-endpoint-h-1861662037.us-east-1.elb.amazonaws.com
- gcs-eu-00002.content-storage-upload.googleapis.com
- a1750.g1.akamai.net
- me.apple-dns.net
- instagram.c10r.facebook.com
- events-endpoint-f-207886521.us-east-1.elb.amazonaws.com
- events-endpoint-455714294.us-east-1.elb.amazonaws.com
- gateway.fe.apple-dns.net

Podpunkt 4. Lista protokołów i usług

Komunikacja odbywała się dzięki następującym protokołom:

- ARP
- DHCP
- DNS
- HTTP
- ICMP
- ICMPv6
- ICMPv2
- MDNS
- SSLv2
- TCP
- TLSv1.2
- TLSv1.3
- UDP
- XID

Program Wireshark umożliwia przeprowadzenia analizy statystycznej przechwyconego ruchu m.in. możemy zobaczyć procentowy udział protokołów biorących udział w przechwyconym ruchu sieciowym (poniżej zrzuty ekranu):

Pasibus:

Wireshark · Statystyki Hierarchi Protokołów · mcdonald.pcapng

Protokół	Pakiety [%]	Pakiety	Bajty [%]	Bajtów	Bity/s	Krańcowych pakietów	Krańcowych bajtów	Krańcowych bitów/s
Frame	100.0	71036	100.0	41436349	86 k	0	0	0
Ethernet	100.0	71036	2.4	994504	2 083	0	0	0
Logical-Link Control	0.0	24	0.0	144	0	0	0	0
Logical-Link Control Basic Format XID	0.0	24	0.0	72	0	24	72	0
Internet Protocol Version 6	0.4	314	0.0	12560	26	0	0	0
User Datagram Protocol	0.1	61	0.0	488	1	0	0	0
Multicast Domain Name System	0.1	61	0.0	5698	11	61	5698	11
Internet Control Message Protocol v6	0.4	253	0.0	6336	13	253	6336	13
Internet Protocol Version 4	98.6	70041	3.4	1400836	2 935	0	0	0
User Datagram Protocol	3.2	2247	0.0	17976	37	0	0	0
Multicast Domain Name System	0.1	49	0.0	4354	9	49	4354	9
Domain Name System	0.7	493	0.1	37181	77	493	37181	77
Data	2.2	1535	2.7	1112275	2 330	1535	1112275	2 330
Bootstrap Protocol	0.2	170	0.1	52960	110	170	52960	110
Transmission Control Protocol	95.3	67671	91.1	37736277	79 k	44337	15918472	33 k
Secure Sockets Layer	34.2	24284	79.3	32866216	68 k	22794	30173288	63 k
Malformed Packet	0.4	307	0.0	0	0	307	0	0
Hypertext Transfer Protocol	0.1	49	0.2	64865	135	44	6592	13
Media Type	0.0	1	0.0	11867	24	1	12164	25
Line-based text data	0.0	4	0.3	132558	277	4	44732	93
Domain Name System	0.1	40	0.0	2660	5	40	2660	5
Data	0.2	144	0.3	133206	279	144	133206	279
Internet Group Management Protocol	0.0	4	0.0	32	0	4	32	0
Internet Control Message Protocol	0.2	119	0.1	35244	73	119	35244	73
Address Resolution Protocol	0.9	657	0.0	18396	38	657	18396	38

McDonald:

Wireshark · Statystyki Hierarchi Protokołów · pasibus.pcapng

Protokół	Pakiety [%]	Pakiety	Bajty [%]	Bajtów	Bity/s	Krańcowych pakietów	Krańcowych bajtów	Krańcowych bitów/s
Frame	100.0	119428	100.0	105621813	598 k	0	0	0
Ethernet	100.0	119428	1.6	1671992	9 474	0	0	0
Logical-Link Control	0.0	16	0.0	96	0	0	0	0
Logical-Link Control Basic Format XID	0.0	16	0.0	48	0	16	48	0
Internet Protocol Version 6	0.4	464	0.0	18560	105	0	0	0
User Datagram Protocol	0.2	204	0.0	1632	9	0	0	0
Multicast Domain Name System	0.2	204	0.0	38054	215	204	38054	215
Transmission Control Protocol	0.0	21	0.0	840	4	21	840	4
Internet Control Message Protocol v6	0.2	239	0.0	7848	44	239	7848	44
Internet Protocol Version 4	99.2	118512	2.2	2370408	13 k	0	0	0
User Datagram Protocol	2.0	2374	0.0	18992	107	0	0	0
Simple Service Discovery Protocol	0.0	36	0.0	4500	25	36	4500	25
Multicast Domain Name System	0.2	270	0.0	35716	202	270	35716	202
Domain Name System	0.6	714	0.0	43127	244	714	43127	244
Data	1.0	1229	0.7	769210	4 358	1229	769210	4 358
Bootstrap Protocol	0.1	125	0.0	38798	219	125	38798	219
Transmission Control Protocol	97.2	116060	95.2	100582419	569 k	88588	66923094	379 k
Secure Sockets Layer	23.4	27905	88.5	93510531	529 k	26457	88536530	501 k
Malformed Packet	0.7	777	0.0	0	0	777	0	0
Hypertext Transfer Protocol	0.1	98	0.5	577782	3 274	60	18750	106
Portable Network Graphics	0.0	7	0.1	106221	601	7	108679	615
Media Type	0.0	14	0.5	578879	3 280	14	223621	1 267
Line-based text data	0.0	9	0.4	446965	2 532	9	115076	652
JPEG File Interchange Format	0.0	4	0.1	103172	584	4	104782	593
JavaScript Object Notation	0.0	1	0.0	1360	7	1	1509	8
eXtensible Markup Language	0.0	1	0.0	375	2	1	375	2
Compuserve GIF	0.0	2	0.0	2346	13	2	2793	15
Domain Name System	0.1	64	0.0	3918	22	64	3918	22
Data	0.1	76	0.0	45540	258	76	45540	258
Internet Group Management Protocol	0.0	42	0.0	672	3	42	672	3
Internet Control Message Protocol	0.0	36	0.0	5989	33	36	5989	33
Address Resolution Protocol	0.4	436	0.0	12208	69	436	12208	69

Galeria:

Wireshark · Statystyki Hierarchi Protokołów · Galeria.pcapng

Protokół	Pakiety [%]	Pakiety	Bajty [%]	Bajtów	Bity/s	Krańcowych pakietów	Krańcowych bajtów	Krańcowych bitów/s
Frame	100.0	5812	100.0	2430272	15 k	0	0	0
Ethernet	100.0	5812	3.3	81368	533	0	0	0
Logical-Link Control	0.2	13	0.0	78	0	0	0	0
Logical-Link Control Basic Format XID	0.2	13	0.0	39	0	13	39	0
Internet Protocol Version 6	2.0	117	0.2	4680	30	0	0	0
User Datagram Protocol	1.0	61	0.0	488	3	0	0	0
Multicast Domain Name System	1.0	61	0.6	14996	98	61	14996	98
Internet Control Message Protocol v6	1.0	56	0.1	1480	9	56	1480	9
Internet Protocol Version 4	96.3	5599	4.6	111996	734	0	0	0
User Datagram Protocol	13.4	779	0.3	6232	40	0	0	0
Port Control Protocol	0.1	6	0.0	144	0	6	144	0
NAT Port Mapping Protocol	0.1	6	0.0	72	0	6	72	0
Multicast Domain Name System	1.4	81	0.9	21371	140	81	21371	140
Domain Name System	7.6	439	1.1	27926	183	439	27926	183
Data	1.6	94	1.8	43276	283	94	43276	283
Bootstrap Protocol	2.6	153	1.9	46356	304	153	46356	304
Transmission Control Protocol	82.3	4784	85.0	2066157	13 k	3366	1043140	6 841
Secure Sockets Layer	25.0	1453	60.3	1464654	9 606	1364	1256388	8 240
Malformed Packet	0.2	13	0.0	0	0	13	0	0
Hypertext Transfer Protocol	0.7	40	5.8	141960	931	28	8058	52
Portable Network Graphics	0.0	1	2.8	68086	446	1	68364	448
Media Type	0.0	2	5.1	124752	818	2	30307	198
Line-based text data	0.2	9	8.0	195135	1 279	9	41134	269
Data	0.0	1	0.0	1163	7	1	1163	7
Internet Group Management Protocol	0.1	4	0.0	32	0	4	32	0
Internet Control Message Protocol	0.6	32	0.0	1152	7	32	1152	7
Address Resolution Protocol	1.4	83	0.1	2324	15	83	2324	15

Pasaz Grunwaldzki:

Wireshark · Statystyki Hierarchi Protokołów · Pasaz Grunwaldzki.pcapng

Protokół	Pakiety [%]	Pakiety	Bajty [%]	Bajtów	Bity/s	Krańcowych pakietów	Krańcowych bajtów	Krańcowych bitów/s
Frame	100.0	14583	100.0	7885877	139 k	0	0	0
Ethernet	100.0	14583	2.6	204162	3 606	0	0	0
Internet Protocol Version 6	0.1	12	0.0	480	8	0	0	0
User Datagram Protocol	0.1	12	0.0	96	1	0	0	0
Multicast Domain Name System	0.1	12	0.0	1790	31	12	1790	31
Internet Protocol Version 4	99.9	14571	3.7	291420	5 147	0	0	0
User Datagram Protocol	13.9	2027	0.2	16216	286	0	0	0
Network Time Protocol	0.0	6	0.0	288	5	6	288	5
Multicast Domain Name System	0.1	12	0.0	1790	31	12	1790	31
Domain Name System	2.7	387	0.4	27726	489	387	27726	489
Data	11.1	1622	14.9	1173779	20 k	1622	1173779	20 k
Transmission Control Protocol	85.8	12508	78.2	6166834	108 k	8940	4191342	74 k
Secure Sockets Layer	24.6	3588	68.4	5395525	95 k	3513	5009470	88 k
Malformed Packet	0.1	8	0.0	0	0	8	0	0
Hypertext Transfer Protocol	0.3	46	4.5	355127	6 273	27	8761	154
Portable Network Graphics	0.1	10	2.4	188293	3 326	10	191374	3 380
Media Type	0.0	3	1.4	110481	1 951	3	111436	1 968
Line-based text data	0.0	5	0.5	38157	674	5	38649	682
JPEG File Interchange Format	0.0	1	0.0	3593	63	1	3901	68
Data	0.0	1	0.0	1388	24	1	1388	24
Internet Control Message Protocol	0.2	36	0.0	1296	22	36	1296	22

Lista wybranych usług:

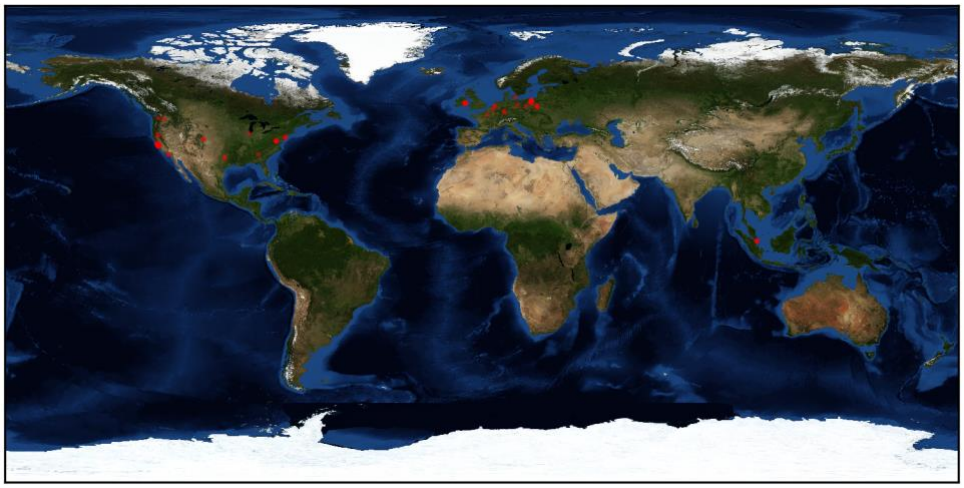
- arcpd 3513/tcp
- arcpd 3513/udp
- orbix-loc-ssl 3077/tcp
- orbix-loc-ssl 3077/udp
- loreji-panel 7026/tcp
- hdl-srv 2641/tcp
- hdl-srv 2641/udp
- ezrelay 10103/tcp
- ezrelay 10103/udp
- jps 2205/tcp
- jps 2205/udp
- dpm 5718/tcp

- dpm 5718/udp
- xmms2 9667/tcp
- xmms2 9667/udp
- bmc-net-adm 1769/tcp
- bmc-net-adm 1769/udp
- transmit-port 5282/tcp
- transmit-port 5282/udp
- passwrd-policy 1333/tcp
- passwrd-policy 1333/udp
- contamac-icm 4846/tcp
- contamac-icm 4846/udp
- itwo-server 4410/tcp
- datasurfsrv 461/tcp
- datasurfsrv 461/udp
- citysearch 3974/tcp
- citysearch 3974/udp
- smtp 25/tcp

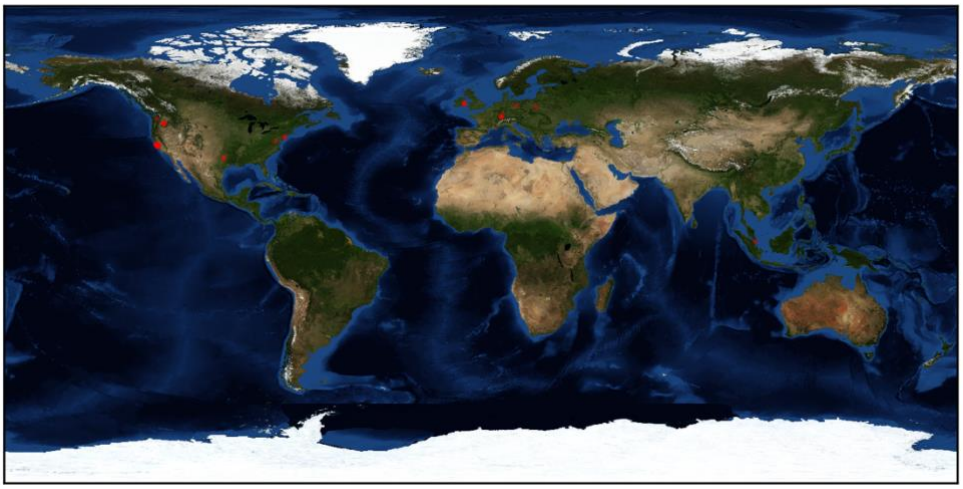
Podpunkt 5. Mapa lokalizacji

Za pomocą skryptu napisanego w języku Python PyGeoIpMap uzyskałyśmy mapę lokalizacji, z którymi łączyły się komputery dla poszczególnych nazw SSID udostępnianych hotspotów:

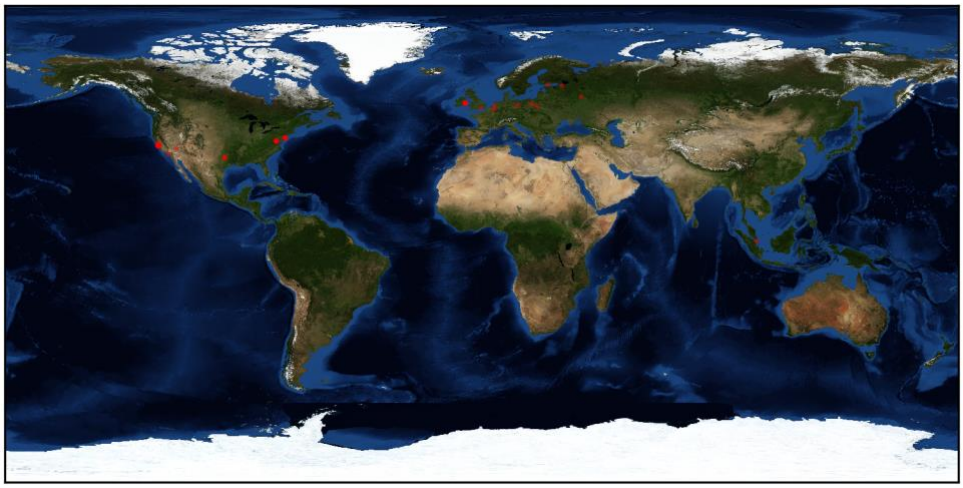
Pasibus:



Galeria:



McDonald:



Pasaż Grunwaldzki: