

VoIP (SIP/RTP) – Diagnostyka.

Karol Skibiński

MBUM#8,
Warszawa, 2023

Karol Skibiński

kilka zdań o mnie

- „od zawsze” związany jestem z rynkiem ICT
- najpierw była to telekomunikacja, później doszły sieci komputerowe
- 2008r - pierwsze duże (udane) wdrożenia VoIP
- 2009r - 2012r - byłem operatorem VoIP w ramach własnej działalności
- Mikrotika poznałem w 2017r
- obecnie pracuje dla polskiej sieci komórkowej
- równolegle w ramach prowadzonej działalności wdrażam rozwiązania sieciowe i telekomunikacyjne (VoIP) w firmach
- wspomniany VoIP (SIP) to temat, o którym mógłbym rozmawiać godzinami ;-)





Dokumentacja:

RFC 3261

SIP: Session Initiation Protocol

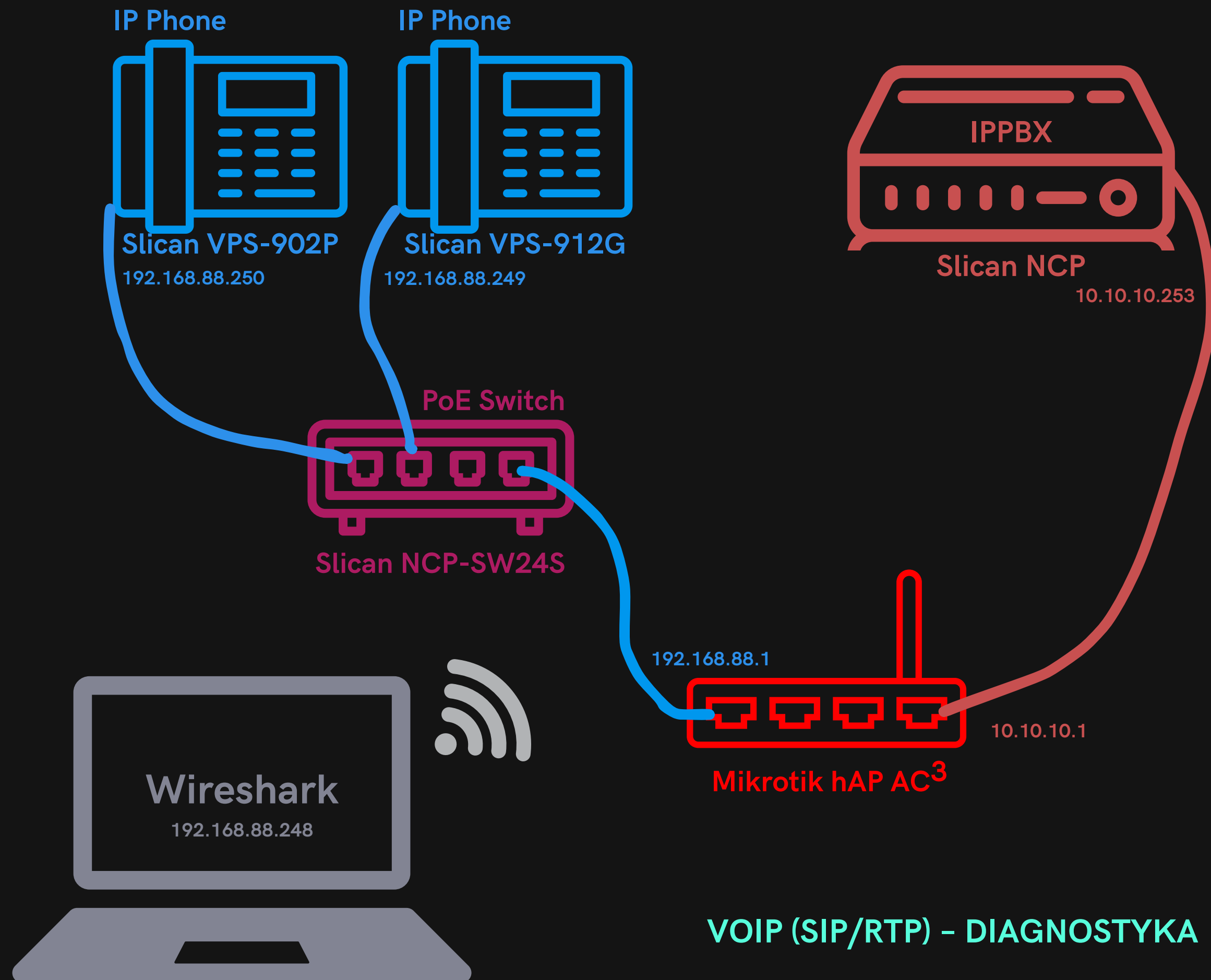
RFC 123...

Oczywiście RFC w temacie SIPa jest duuuużo więcej, ale wszystkich wymieniać nie trzeba ;-)

Setup:

KONFIGURACJA

Środowisko w którym przeprowadzimy zajęcia praktyczne.



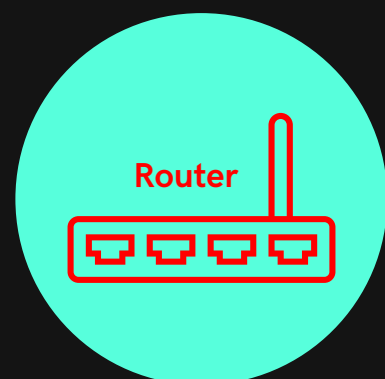
VOIP (SIP/RTP) – DIAGNOSTYKA



Część producentów umożliwia utworzenie pliku PCAP w samym telefonie.



Część producentów umożliwia utworzenie pliku PCAP w samej centrali.



...
... utworzenie pliku PCAP w samym routerze.



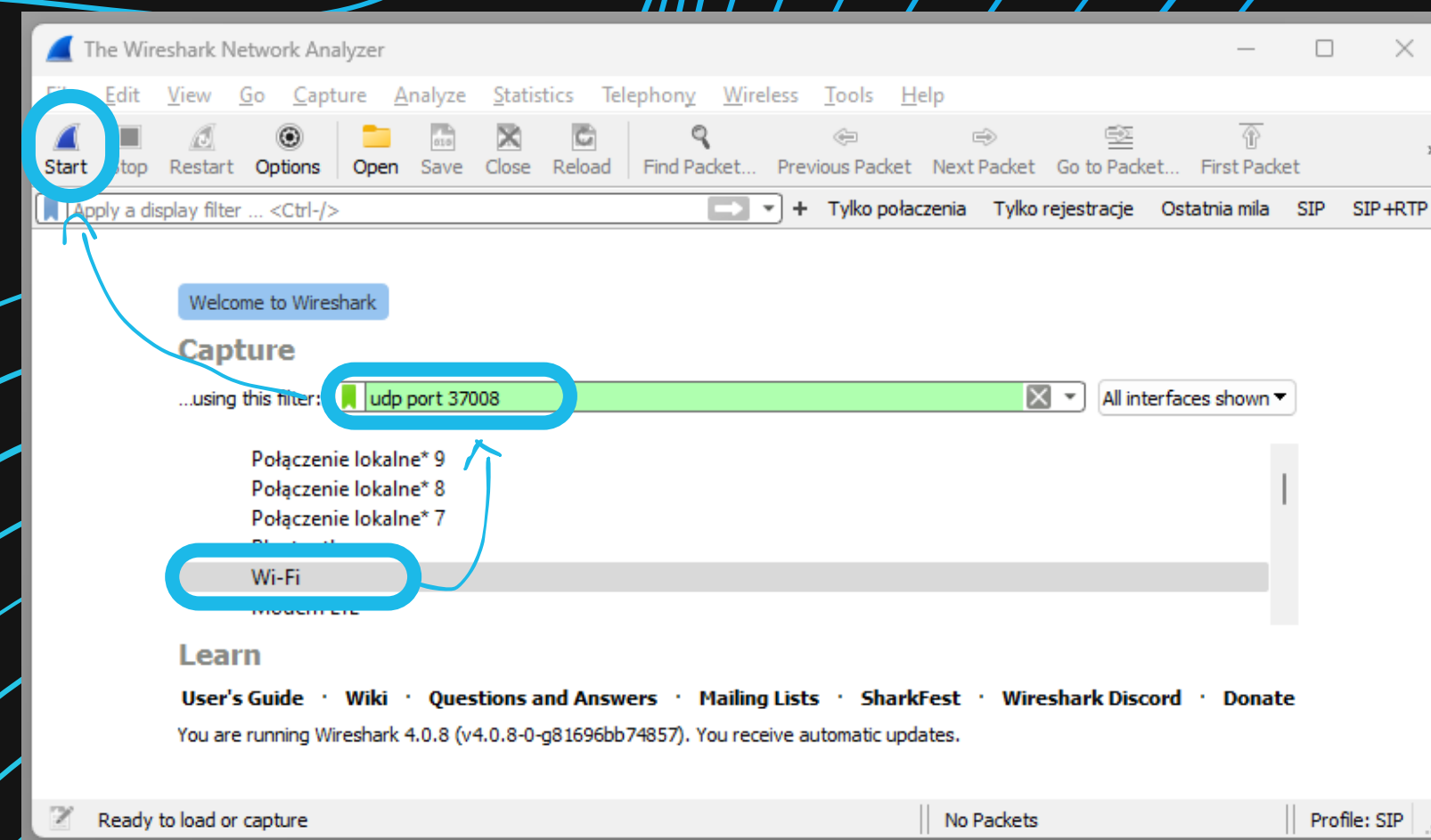
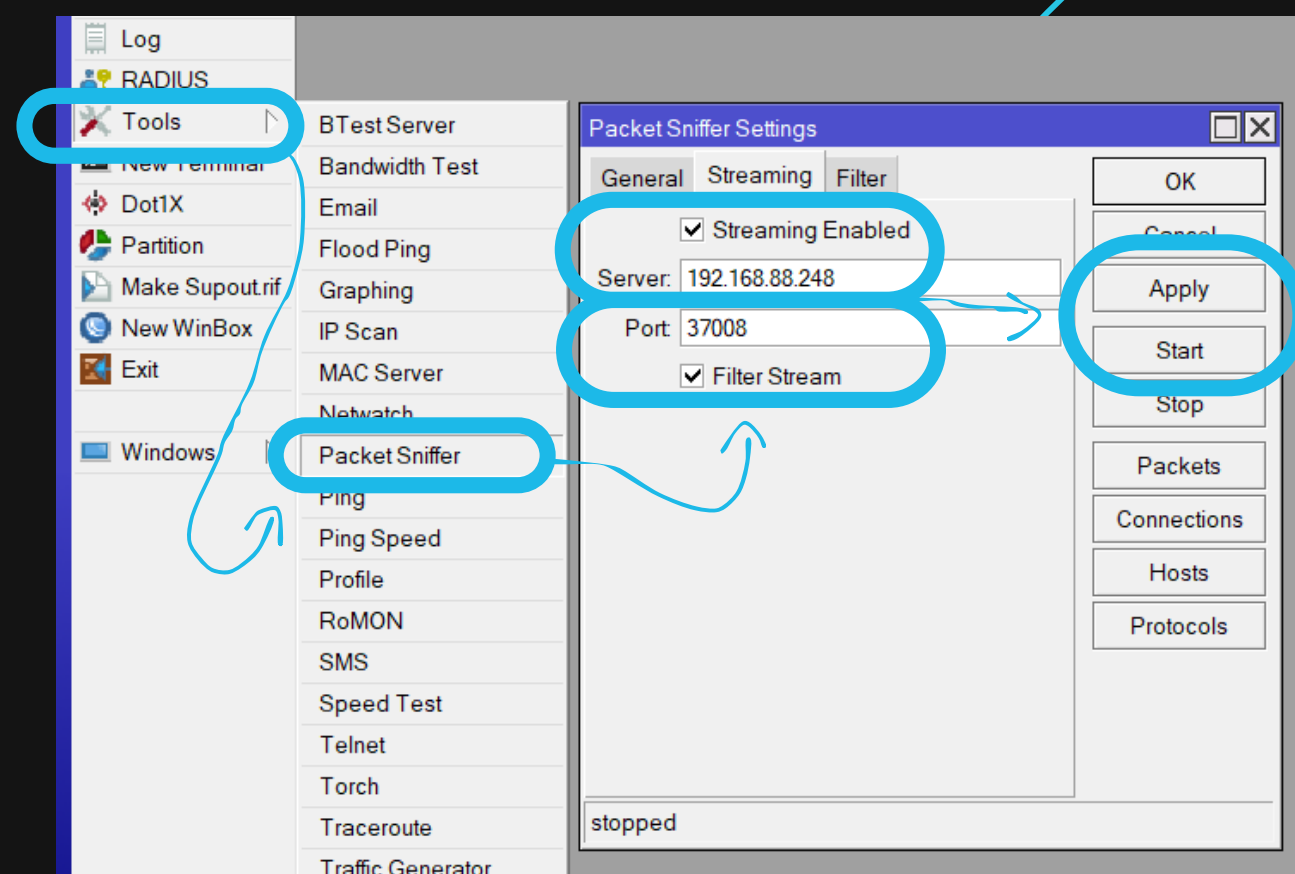
Ja osobiście (jak to tylko możliwe) wybieram streamowanie PCAPa prosto z routera do Wiresharka na moim PC.

Gdzie najlepiej sniffować?

Jak odpalić Sniffera ze strumieniowaniem?

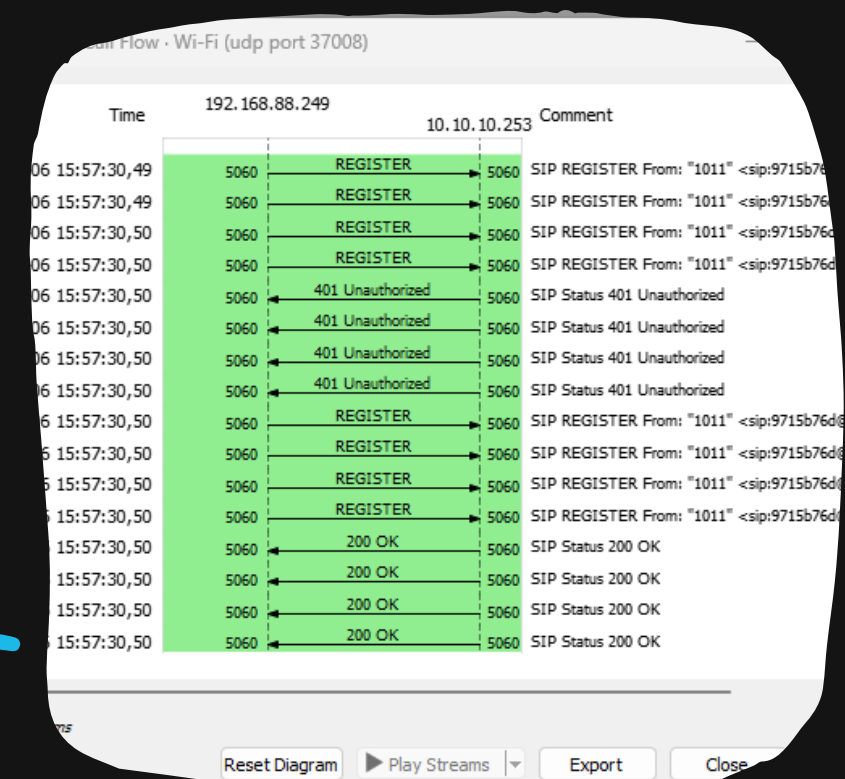
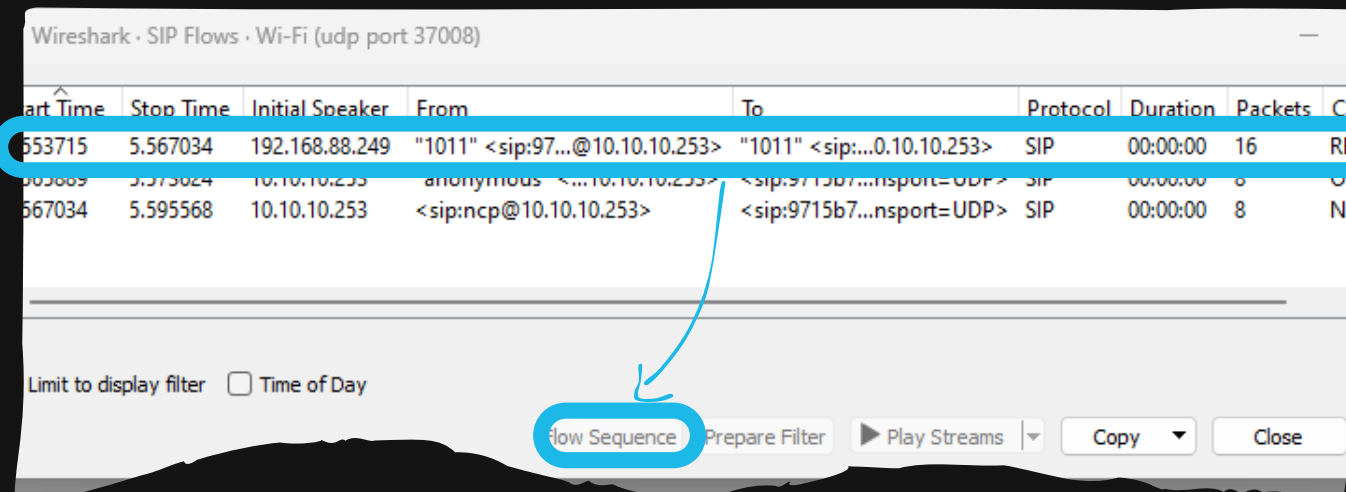
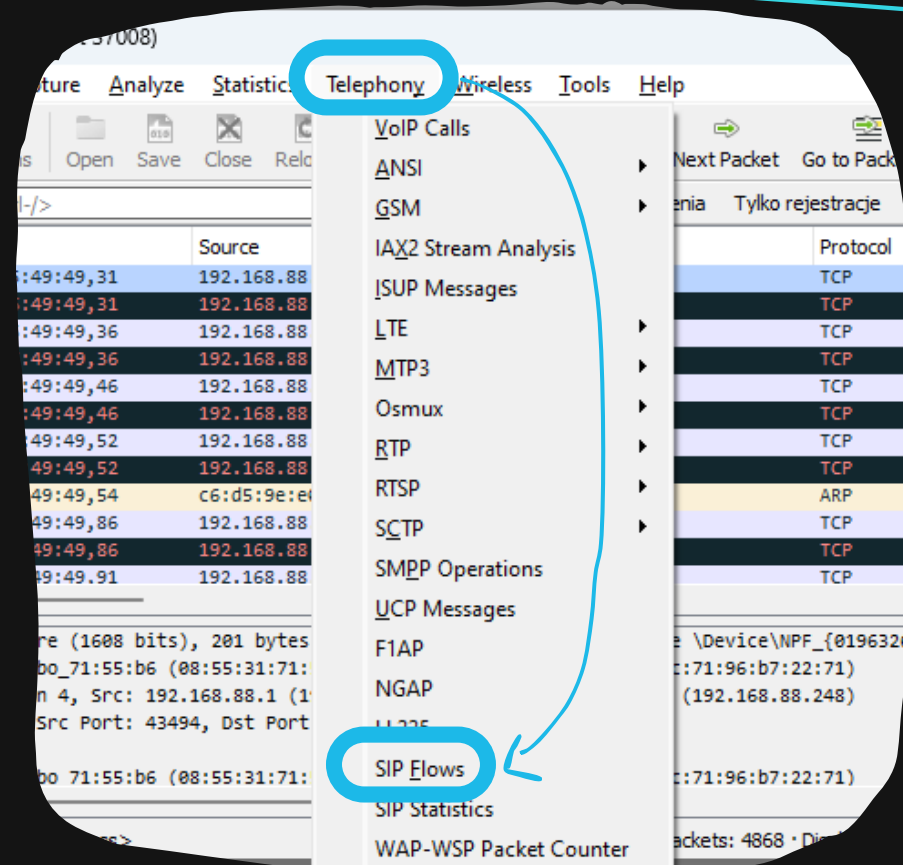
NA PC

PO STRONIE WINBOXA



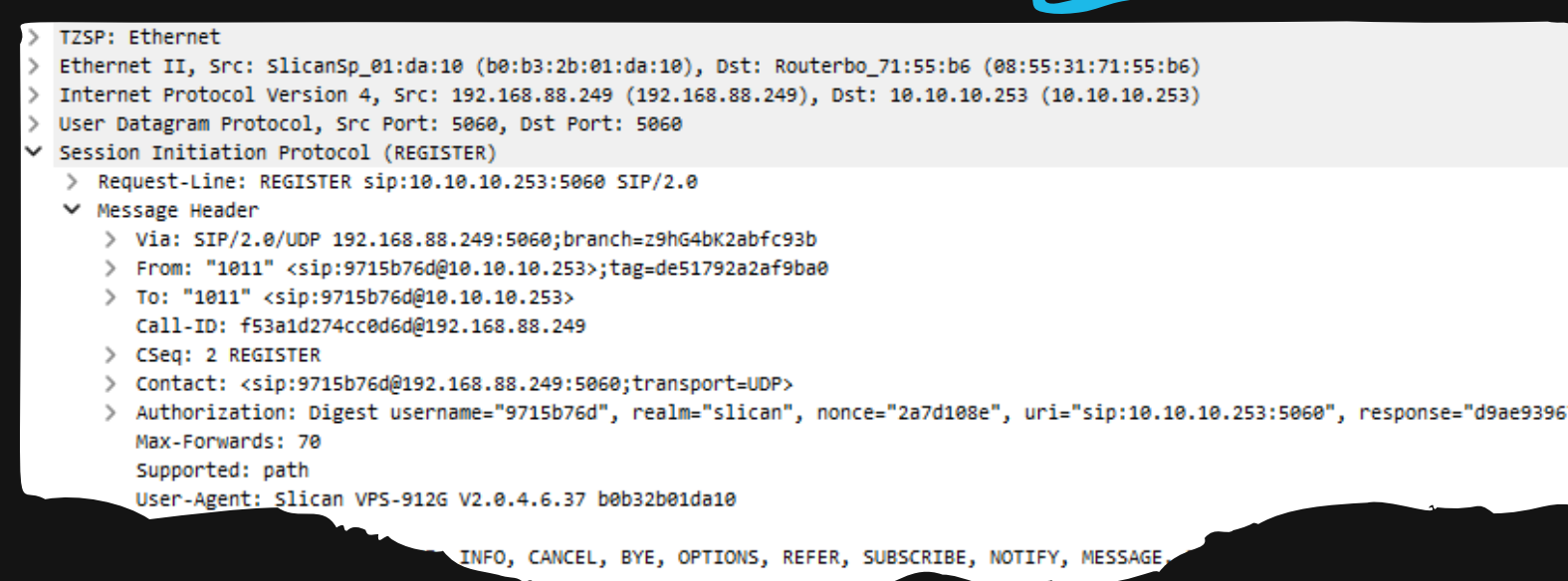
VOIP (SIP/RTP) – DIAGNOSTYKA

Coś się złapało ...



przydatne filtry:

- sip or rtp or rtcp
- ip.addr = 192.168.88.250
- sip.msg_hdr contains 1010
- łączenie filtrów



Jak widać powyżej wszystkie pakiety mamy powielone, bo łapiemy je na wszystkich interfejsach.

To teraz poćwiczmy na żywo!

- ✓ Jak wygląda prawidłowa rejestracja [REGISTER] telefonu SIPowego?

Time	192.168.88.249	10.10.10.253	Comment
2023-10-06 17:12:50,38	5060	REGISTER → 5060	SIP REGISTER From: "1011" <sip:9715b76d@10....
2023-10-06 17:12:50,39	5060	← 401 Unauthorized 5060	SIP Status 401 Unauthorized
2023-10-06 17:12:50,48	5060	REGISTER → 5060	SIP REGISTER From: "1011" <sip:9715b76d@10....
2023-10-06 17:12:50,48	5060	← 200 OK 5060	SIP Status 200 OK

- ✓ Które pola komunikatu są istotne i jaką rolę pełnią?
- ✓ Zmieńmy login/hasło, zobaczymy co się wydarzy ...

Time	192.168.88.250	10.10.10.253	Comment
2023-10-06 17:12:57,52	5060	REGISTER → 5060	SIP REGISTER From: "1010" <sip:random_login@...
2023-10-06 17:12:57,53	5060	← 401 Unauthorized 5060	SIP Status 401 Unauthorized
2023-10-06 17:12:57,62	5060	REGISTER → 5060	SIP REGISTER From: "1010" <sip:random_login@...
2023-10-06 17:12:57,62	5060	← 403 Forbidden 5060	SIP Status 403 Forbidden

To teraz poćwiczmy na żywo!

- ✓ To teraz zadzwońmy [INVITE] ...
- ✓ Jakie dodatkowe pola w komunikacie mamy i co to jest to SDP?
- ✓ Trochę o kodekach i ich negocjacji.

Time	192.168.88.249	10.10.10.253	192.168.88.250	Comment
2023-10-06 17:15:51,98	5060	INVITE SDP (g711U g711A)	5060	SIP INVITE From: "1011" <sip:9715b76d@10.10.10.253>
2023-10-06 17:15:51,98	5060	100 Trying	5060	SIP Status 100 Trying
2023-10-06 17:15:51,98	5060	401 Unauthorized	5060	SIP Status 401 Unauthorized
2023-10-06 17:15:51,99	5060	ACK	5060	SIP ACK From: "1011" <sip:9715b76d@10.10.10.253>
2023-10-06 17:15:52,00	5060	INVITE SDP (g711U g711A)	5060	SIP INVITE From: "1011" <sip:9715b76d@10.10.10.253>
2023-10-06 17:15:52,00	5060	100 Trying	5060	SIP Status 100 Trying
2023-10-06 17:15:52,01	5060	183 Session Progress SDP (...)	5060	SIP Status 183 Session Progress
2023-10-06 17:15:52,03	5060	INVITE SDP (g711A g711A)	5060	SIP INVITE From: "SIP 1011" <sip:1011@10.10.10.253>
2023-10-06 17:15:52,03	5060	100 Trying	5060	SIP Status 100 Trying
2023-10-06 17:15:52,60	5060	180 Ringing	5060	SIP Status 180 Ringing
2023-10-06 17:15:52,62	12100	RTP (g711A)	16676	RTP, 700 packets. Duration: 3,48s SSRC: 0x5BB4...
2023-10-06 17:15:56,11	5060	200 OK SDP (g711A teleph...)	5060	SIP Status 200 OK
2023-10-06 17:15:56,11	5060	ACK	5060	SIP Request INVITE ACK 200 CSeq:102
2023-10-06 17:15:56,12	5060	200 OK SDP (g711A g711A)	5060	SIP Status 200 OK
2023-10-06 17:15:56,13	5060	ACK	5060	SIP Request INVITE ACK 200 CSeq:21
2023-10-06 17:15:56,27	19676	RTP (g711A)	12100	RTP, 920 packets. Duration: 4,61s SSRC: 0x6E8A...
2023-10-06 17:15:56,27	12100	RTP (g711A)	16676	RTP, 920 packets. Duration: 4,61s SSRC: 0x6E8A...
2023-10-06 17:16:00,90	5060	BYE	5060	SIP Request BYE CSeq:103
2023-10-06 17:16:00,90	5060	200 OK	5060	SIP Status 200 OK
2023-10-06 17:16:00,92	12100	RTP (g711A)	16676	RTP, 344 packets. Duration: 1,70s SSRC: 0x42B7...
2023-10-06 17:16:02,63	5060	BYE	5060	SIP Request BYE CSeq:22
2023-10-06 17:16:02,63	5060	200 OK	5060	SIP Status 200 OK

To teraz poćwiczmy na żywo!

- ✓ O co chodzi z tym "SIP ALG" / "SIP Helper" / "Service Port - SIP"?
- ✓ Dlaczego w 9,5/10 wdrożeń trzeba "SIP ALG" wyłączyć ;-)
- ✓ Aaaaa!!! ... mój ISP może mnie podsłuchać !!!

- ❌ ... (i jeszcze to)
- ❌ ... (i jeszcze tamto)
- ❌ ... (a, i jeszcze)

O tym i o wielu "problemach" też nie pogadaliśmy ...
No niestety mamy tylko 45 minut o innych
sprawach tym razem nie pogadamy, a szkoda!



Koniec ;-(

... skończył nam się czas,
a to był wstęp ...



ZAINTERESOWAŁ CIĘ TEN TEMAT?

Jeżeli tak, to odezwij się! Chętnie rozszerzę to zagadnienie na osobnym spotkaniu dedykowanym zagadnieniom diagnostyki VoIP (SIP/RTP).

DODATEK:

Załączam plik "VoIP(SIP-RTP)-diagnostyka.pcap"
z wybranymi przykładami z zajęć praktycznych.



karol.skibinski@tel-it.pl



www.tel-it.pl



www.linkedin.com/in/karolskibinski/