**Raport**

**Testowanie: laptop podłączony do sieci bezprzewodowej, uruchomiony wireshark na windows**

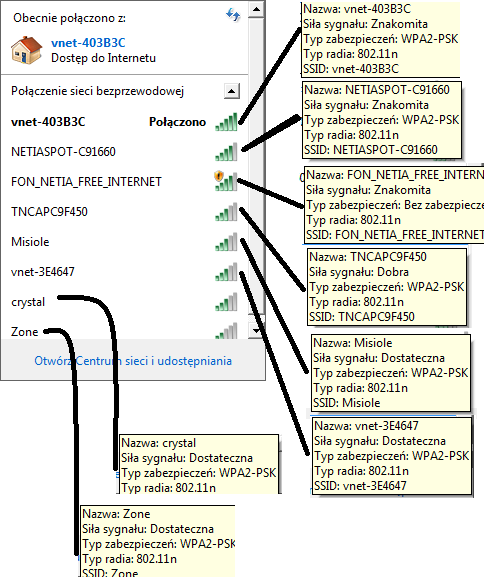
**Problemy: całkowity brak możliwości monitor mode na windows**

**Na linuxie po 3 s nasłuchiwania w monitor mode wyskakuje error z dumpcap pomoc to napisanie do ludzi z ubuntu ..**

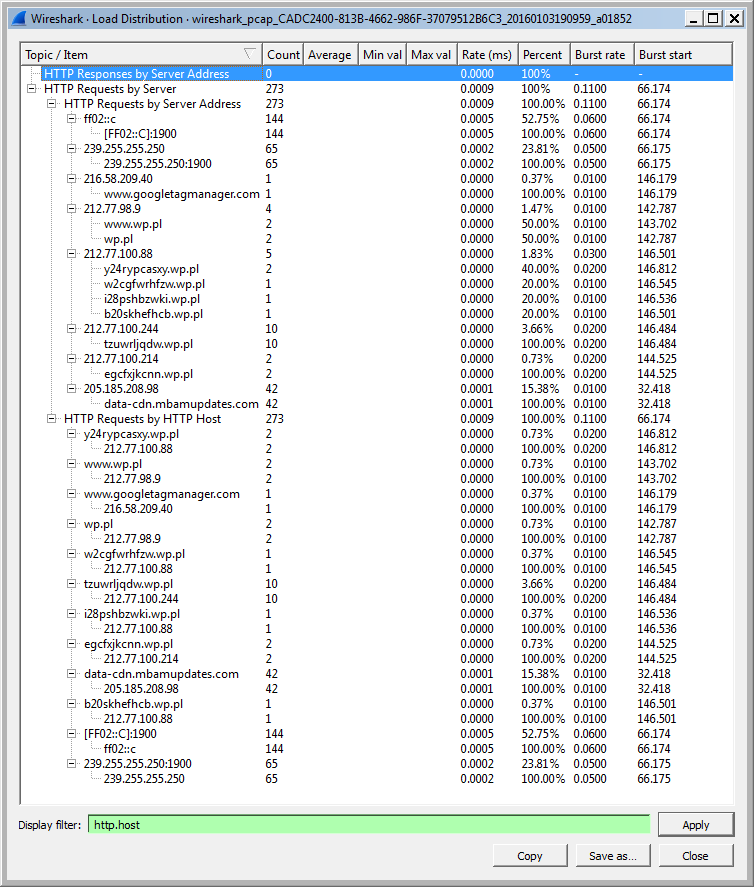
**Alternatywa to airmon-ng niestety źle czyta ruch sieciowy nie zarejestrował nic…**

**Alternatywa 2 to kupno odpowiedniego wifi dongle i instalacja oprogramowania acrylic**

1. lista dostępnych sieci

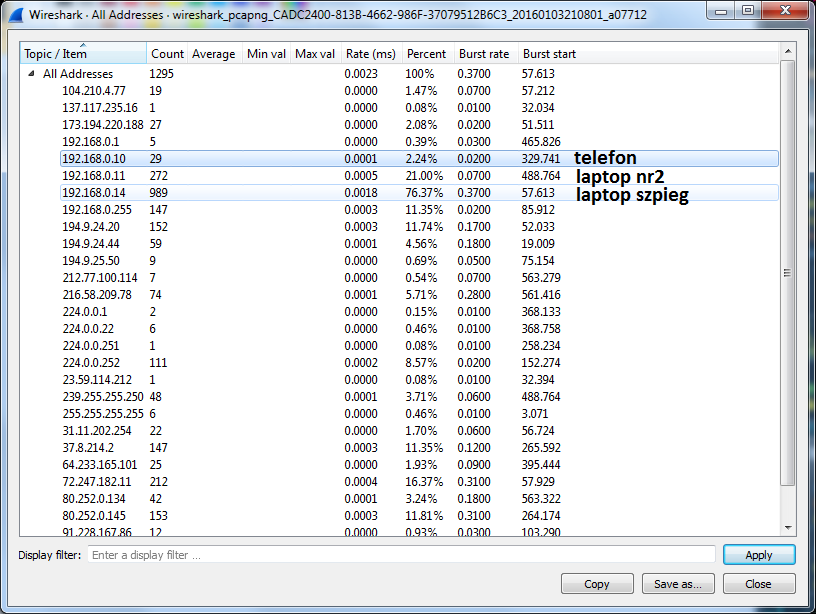
****

2. lista stron www odwiedzonych przez użytkowników sieci



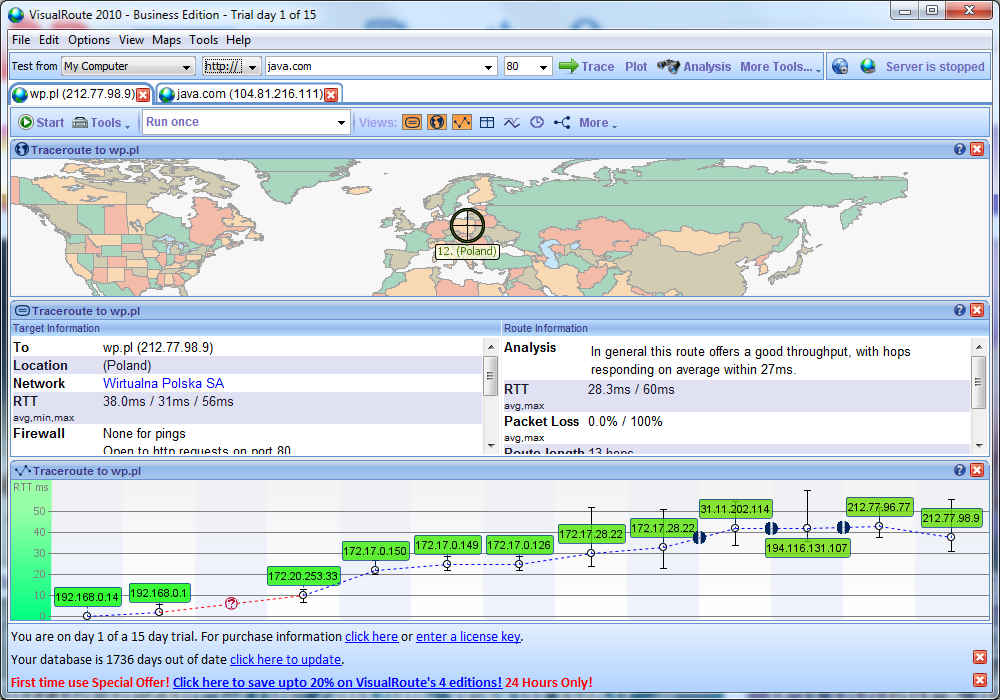
Strony łączące się przez protokół http można namierzyć i sprawdzić jej nazwę, niestety większość stron łączy się przez protokół https, gdzie nie można namierzyć nazwy bo jest zaszyfrowana(ip które wireshark porównuje z dns).

3. lista protokołów i usług, z których korzystali użytkownicy sieci



Aby znaleźć urządzenia wystarczy poszukać odpowiednie adresy ip jakich używają routery do stworzenia wew. Sieci przykładowe maski 10.0.0.0 , 172.16.0.0, 192.168.0.0 dla ipv4.  
Można też użyć nmap na ip i maskę routera aby wyszukać wszystkie podłączone urządzenia.

4. mapa lokalizacji, z którymi łączyły się komputery



Dzięki Wireshark widzimy ip lub nazwy stron gdzie łączą się użytkownicy, wrzucamy to do tracerout aby zobaczyć gdzie znajdują się serwery.

5. lista modeli urządzeń generujących ruch w tej sieci.

Wireshark potrafi rozpoznać bez monitor mode niektóre adresy mac urządzeń które połączyły się po rozpoczęciu nasłuchiwania. Dzieje się dzięki sprawdzeniu ich w Internecie albo w jakiejś bazie.

Wymagany monitor mode …  
Po włączeniu tej opcji wireshark widzi inne urządzenia.