Sieci komputerowe – konwersatorium 6

Jarosław Szkoła

Technologie sieci bezprzewodowych WLAN

Wprowadzenie

- Sieci bezprzewodowe są pod względem technologii przesyłu sygnału atrakcyjną alternatywą dla rozwiązań stosowanych dotychczas.
- Sieci bezprzewodowe istniały w świecie komputerów od dawna, ale żadna z technologii nie pasowała do wymagań rynku. Do tych pierwszych należały:
  - Aloha,
  - ARDIS,
  - Ricochet.

- Problem stanowiły przepustowość – zazwyczaj w okolicach 1Mb na całą sieć, niewielki zasięg a przede wszystkim wysokie koszty wdrożenia, utrzymania oraz brak jednolitych, ogólnodostępnych standardów.
- Sieci bezprzewodowe często są określana terminem Wi-Fi (ang. Wireless Fidelity). Jest to termin, który odnosi się do kilku standardów utworzonych na potrzeby budowania sieci bez użycia tradycyjnych mediów, tzn. kabli, czy też światłowodów.

Zakresy częstotliwości sieci bezprzewodowych

- Sieci bezprzewodowe działają w oparciu o propagację fal elektromagnetycznych. Z tego względu stanowią jeden ze sposobów przenoszenia informacji w ściśle określonym paśmie częstotliwościowym.
- Na świecie przyjęto trzy ogólnie dostępne pasma komercyjne.
- Pasma te mają oznaczenie ISM (industrial, scientific, and medical):
  - UHF ISM 902-928 MHz
  - S-Band ISM – 2,4 do 2,5 GHz
  - C-Band ISM - 5.725-5.875 GHz.
- Sieci bezprzewodowe wykorzystują wydzielone pasma zarezerwowane na potrzeby tego rodzaju komunikacji.

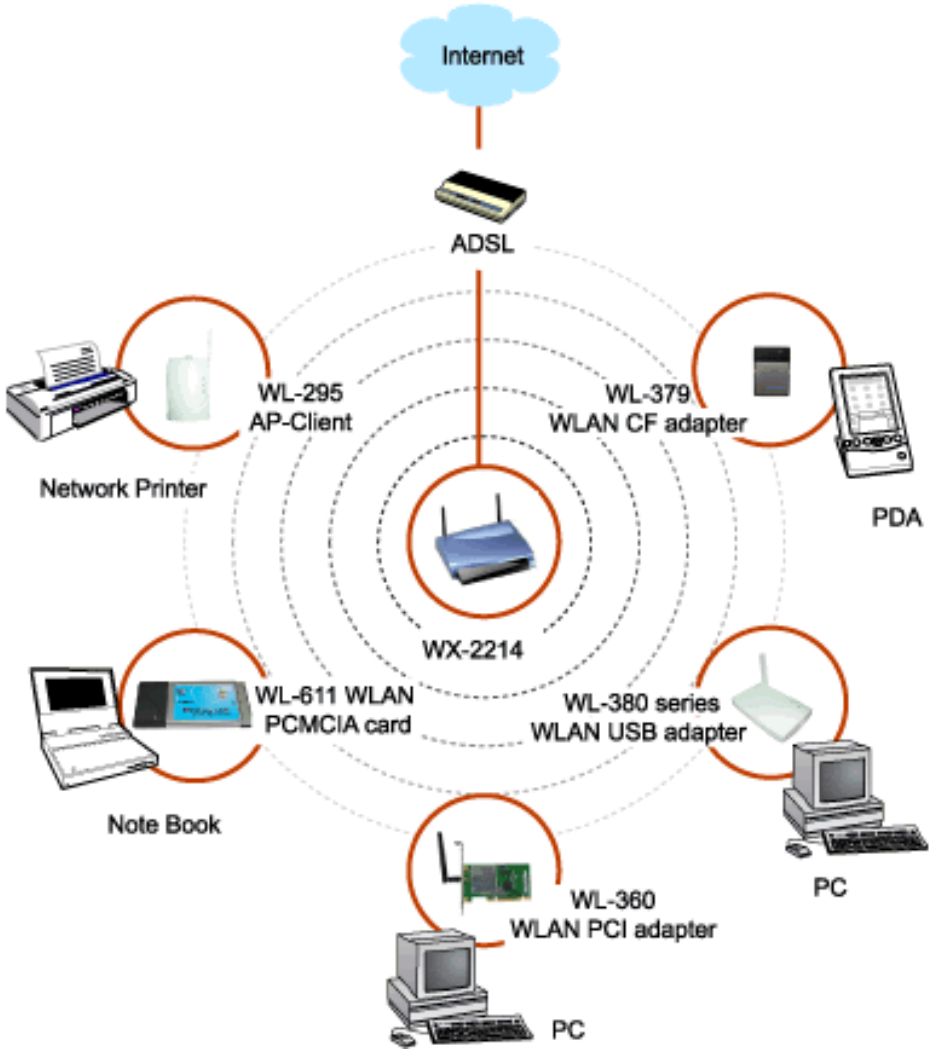
Zakresy częstotliwości łączności radiowej - zestawienie

Pasmo	Zakres częstotliwości
UHF ISM	902 – 928 MHz
S-Band	2-4 GHz
S-Band ISM	2.4 – 2.5 GHz
C-Band	4 – 8 GHz
C-Band satellite downlink	3.7 – 4.2 GHz
C-Band Radar (weather)	5.25 – 5.925 GHz
C-Band ISM	5.725 – 5.875 GHz
C-Band satellite uplink	5.925 – 6.425 GHz
X-Band	8 – 12 GHz
X-Band Radar (police / weather)	8.5 – 10.55 GHz
Ku-Band	12 – 18 GHz
Ku-Band Radar (police)	13.4 – 14 GHz 15.7 – 17.7 GHz

Podstawowe składniki sieci bezprzewodowych

- Sieci bezprzewodowe, ze względu na rodzaj sygnału służącego do transmisji, potrzebują dodatkowych elementów sieciowych, m.in.:
  - Wbudowane bezprzewodowe karty sieciowe - są to karty, które mogą być na stałe wbudowane w płytę główną komputera - tak jest w przypadku większości urządzeń mobilnych.
  - Dodatkowe karty sieciowe bezprzewodowe, które mogą być dołączone poprzez złącza typu PCI, PCI-E, NVMe.
  - Zewnętrzne karty sieciowe, która może być dołączona poprzez złącze typu PCMCIA, USB.
  - Punkty dostępowe (ang. Access Point) - są to urządzenia, które zwykle są przyłączone do sieci LAN przy pomocy tradycyjnego medium (kabla). Urządzenia mobilne komunikują się z punktem dostępowym drogą radiową. Urządzenia te mają co raz więcej funkcjonalności, np.: zapór ogniowych, DHCP itd.
  - Anteny - umożliwiają lepszą propagację sygnału.
  - Kable, złącza, konektory, przejściówki.

Podstawowe składniki sieci bezprzewodowych



Sieci bezprzewodowe - zalety

- Za stosowaniem tej technologii w wybranych obszarach przemawiają następujące zalety:
  - Mobilność - bez potrzeby przełączania kabla sieciowego UTP można przemieszczać się z notebookiem lub innym urządzeniem wewnątrz biura, czy też domu.
  - Łatwość instalacji - gdy potrzeba dodać nowy komputer lub inne urządzenie do sieci to nie trzeba przygotowywać nowego okablowania.
  - Elastyczność - podobnie jak w punkcie poprzednim dodanie nowego urządzenia nie wiąże się z dużym nakładem pracy.
  - Zasięg - zwykle od kilku do kilkudziesięciu metrów, a nawet w przypadku najnowszych technologii, np. WiMax do kilkudziesięciu kilometrów.
  - Możliwość szybkiej rozbudowy i modyfikacji.

Sieci bezprzewodowe - wady

- W przypadku stosowania tej technologii można wyróżnić następujące wady tego rozwiązania:
  - Potencjalne ryzyko przejęcia komunikacji z uwagi na zastosowane medium transmisyjne,
  - Ograniczona przepustowość / zasięg w niektórych miejscach, szczególnie w budynkach z dużą ilością elementów metalowych (efekt klatki Faradaya),
  - Mniejsza responsywność w porównaniu do połączeń kablowych, światłowodowych,
  - Spadek wydajności przy dużej ilości połączeń na danej jednostce powierzchni, z uwagi na małą liczbę dostępnych kanałów

Sieci bezprzewodowe – standardy komunikacji 802.11

- 802.11 przyjęty został w roku 1997. Zakładał przesyłanie informacji z prędkościami 1-2 Mb, przy użyciu fal radiowych o częstotliwości 2.4 GHz oraz promieniowania podczerwonego.
- Standardy ten opisuje budowę pierwszej oraz części drugiej warstwy modelu OSI. Część standardu dotycząca użycia promieniowania podczerwonego się nie przyjęła w związku z konkurencją standardu IrDA. Sam standard 802.11 w celu odróżnieniu go od grupy standardów bywa oznaczany jako 802.1y
- Standardy 802.11 budują grupę trzech niezależnych protokołów (a,b,g). Standardy określone pozostałymi literami: c-f, h-j, n dotyczą rozszerzenia usług i poprawek innych standardów.

802.11a

- 802.11a - działa przesyłając dane z szybkością 54 Mb/s, wykorzystując częstotliwość 5 GHz.
- 802.11a używa techniki kodowania OFDM. W porównaniu ze standardem 802.11b, ma dwie podstawowe zalety:
  - szybkość i liczba nie zachodzących na siebie kanałów (osiem).
  - W przypadku częstotliwości 2.4 GHz są to tylko trzy kanały.
  - Również ogólna szerokość pasma jest większa niż przy 2.4 GHz.
  - W przypadku częstotliwości 2.4GHz jest to 83.5 MHz, zaś przy 5 GHz – 300 MHz.
  - Oba standardy pracują na innych częstotliwościach i nie są one zgodne ze sobą.
  - Zatem punkt dostępu 2.4 GHz nie może współpracować z karta sieciową 5 GHz.
  - Oba standardy mogą być stosowane w tym samym systemie informatycznym.
  - Użytkownicy 802.11a i b mogą korzystać z różnych punktów dostępowych, które są podłączone do tej samej sieci LAN.
  - 802.11a używa wyższej częstotliwości dlatego ma mniejszy zasięg.
  - Z tego względu konieczne jest stosowanie większej ilości punktów dostępu niż w przypadku standardu 802.11b.
  - Urządzenia te pracują ok. trzy razy wydajniej, ale też są o ok. 30% droższe od 802.11b.

802.11a

- Standard ten jest rzadziej stosowany niż standard 802.11b/g, chociaż istnieją urządzenia zapewniające równoległą pracę w tych standardach.
- Standard zatwierdzono w 1999 roku jednak pierwsze urządzenia spełniające wymogi tego standardu weszły do produkcji w 2001 roku.

802.11b

- 802.11b przesyła dane w paśmie 2.4GHz z prędkościami do 11 Mbps jednak w praktyce ze względu na sprawność protokołu praktyczne pasmo wynosi połowę, czyli do 5,5 Mb/s.
- Zasięg określany jest na 46 m w pomieszczeniach zamkniętych i 96 w przestrzeni otwartej.
- Zasięg powiększa się poprzez zastosowanie anten ze wzmacniaczami.
- Spektrum kanału 2.4 GHz podzielono na 14 kanałów, z których każdy ma szerokość 22 MHz, w praktyce oznacza to, że zakres częstotliwości wykorzystywanych przez ten standard mieści się w przedziale 2,4 GHz do 2,494 GHz

802.11g

- 802.11g to projekt, którego celem miało być rozszerzenie standardu 802.11b.
- Głównym problemem, jaki napotykali użytkownicy była zbyt mała prędkość transmisji.
- W 2003 zaproponowano nowe podejście do zagadnienia.
- Podjęto próbę zastosowania techniki OFDM znanej z 802.11a do transmisji danych w paśmie 2.4GHz.
- Ponieważ założono wsteczną kompatybilność z 802.11b nowe karty musiały obsługiwać zarówno poprzednie – (DSSS, HR/DSSS) jak i nowe metody modulacji.
- Jeżeli w sieci znajdują się karty starszej generacji, transmisja odbywa się z mniejszą prędkością.
- Przy zastosowaniu kilku kanałów jednocześnie można uzyskać jeszcze większe prędkości do 108 Mbit/s.

802.11n

- 802.11n jest standardem przygotowanym przez dwa zespoły projektowe (zatwierdzony w 2009).
- Pierwszy pochodzi od zespołu TGnSync w skład, którego wchodzą Atheros, Agere, Marvell, oraz Intel.
- WWiSE (World-Wide Spectrum Efficiency) to drugi zespół składający się z Airgo, Broadcom, Conexant i Texas Instruments.
- Założenia obu grup są podobne.
- Do transmisji i odbioru sygnałów używanych jest wiele anten.
- Dwie anteny w znaczący sposób poprawiają jakość odbieranego oraz wysyłanego sygnału, co pozwala osiągnąć transmisję rzędu 108Mbps.

Standardy 802.11 - zestawienie

Nazwa	Prędkość transmisji [Mb/s]	Pasmo częstotliwości [GHz]	Typ sygnału	Uwagi
802.11	1 – 2	2,4	FHSS, DSSS, IR	Określany jako 802.1y, 1997
802.11a	6, 9, 12, 18, 24, 36, 48, 54	5,0	OFDM	1999
802.11b	1,2,5,11	2,4	DSSS, HR-DSSS	1999
802.11g	1,2,5,6,9,11,12, 18,24,36,48,54	2,4	DSSS,HR-DSSS, OFDM	
802.11n	100,250,540	2,4		

FHSS - Frequency-Hopping Spread Spectrum
DSSS - Direct Sequence Spread Spectrum
HR-DSSS – Hight Rate Direct Sequence Spread Spectrum
OFDM - Orthogonal Frequency-Division Multiplexing

Pozostałe standardy 802.11

- Oprócz standardów wymienionych wcześniej występują również inne regulujące działanie sieci bezprzewodowych:
  - IEEE 802.11c - opisuje sposób działania bezprzewodowych mostów pomiędzy sieciami.
  - IEEE 802.11d - opisuje sposób implementacji łączności bezprzewodowej w poszczególnych krajach.
  - IEEE 802.11e - wprowadzenie QoS oraz inteligentnego zarządzania pakietami (ang. packet bursting) w transmisji strumieniowej standardów 802.11a.
  - 802.11g i 802.11h IEEE 802.11f - definicja roamingu w sieciach 802.11a.
  - 802.11g i 802.11h przy zastosowaniu protokołu IAPP IEE.
  - 802.11h - odpowiednik standardu 802.11a przeznaczony dla urządzeń pracujących w paśmie 5 GHz, z użyciem (DCS/DFS) oraz TPC w Europie.

Pozostałe standardy 802.11

- Oprócz standardów wymienionych wcześniej występują również inne regulujące działanie sieci bezprzewodowych:
  - IEEE 802.11i - standard WPA2 definiujący bezpieczeństwo sieci bezprzewodowych przy wykorzystaniu protokołów EAP, Radius, Kerberos, Rijandel AES, 802.1x.
  - IEEE 802.11j - odpowiednik standardu 802.11a przeznaczony dla urządzeń pracujących w Japonii. Zawiera specyfikacje kanałów powyżej 4,9GHz.
  - IEEE 802.11k - opisuje protokół wymiany informacji pomiędzy klientami a punktami dostępowymi.
  - IEEE 802.11xx - opisuje inteligentne zarządzanie pakietami XXJE2R.

Podział sieci bezprzewodowych

- Jednym z możliwych podziałów sieci bezprzewodowych, zależnym od topologii oraz logiki zawartej w urządzeniach dostępowych, jest podział na sieci:
  - autonomiczne,
  - scentralizowane.

Zabezpieczenia sieci bezprzewodowych

- Sieci bezprzewodowe z racji swojej zasady działania są sieciami ze współdzielonym medium transmisyjnym.
- Zatem wszelkie problemy związane z taką transmisją sygnału również tutaj występują.
- Ze względu na powszechne użytkowanie urządzeń działających korzystających z sieci bezprzewodowych wprowadzono różne rodzaje zabezpieczeń, m.in.:
  - WEP
  - TKIP
  - WPA
  - 802.1X
  - VPN
  - NAC

Zabezpieczenie WEP

- Pierwszą wprowadzoną metodą szyfrowania informacji w sieciach bezprzewodowych był WEP.
- Akronim pochodzi od słów: Wired Equivalent Privacy.
- Ponieważ implementacja jest stosunkowo prosta, a proces szyfrowania nie wymaga dużej mocy obliczeniowej procesora, metoda zyskała dużą popularność.
- WEP skonstruowany został w oparciu o algorytm RC4.
- Jak każda metoda symetryczna wymaga, żeby obie strony używały takich samych kluczy do szyfrowania i deszyfrowania przesyłanych informacji.
- Początkowo zakładano, że WEP będzie spełniał jednocześnie funkcje szyfrowania danych oraz autentykacji. Sądzono, że osoba uprawniona do udziału w transmisji będzie posiadać odpowiedni klucz.

Zabezpieczenie WEP

- Sam WEP, a także 802.11 nie definiuje w jaki sposób użytkownik powinien wejść w posiadanie klucza.
- Najbardziej popularną metodą dystrybucji kluczy jest wpisywanie ich do każdego z odbiorników manualnie.
- Proces ten jest bardzo czasochłonny i coraz bardziej skomplikowany ze wzrostem ilości hostów, dlatego negatywnie wpływa na możliwość przyszłego rozwoju sieci.
- Powyżej kilkunastu klientów architektura przestaje być skalowalna.
- Samo założenie, że w posiadaniu klucza znajdują się wyłącznie osoby uprawnione również jest błędne.
- Pomimo tych wad WEP zyskał sobie olbrzymią popularność i nadal jest używany.
- Jeśli WEP stosowany jest w sieciach autonomicznych klucz należy uaktualnić w każdym z punktów dostępowych oddzielnie.
- W sieciach scentralizowanych zmiana wprowadzana jest w jednym miejscu ze skutkiem natychmiastowym.

Zabezpieczenie WEP

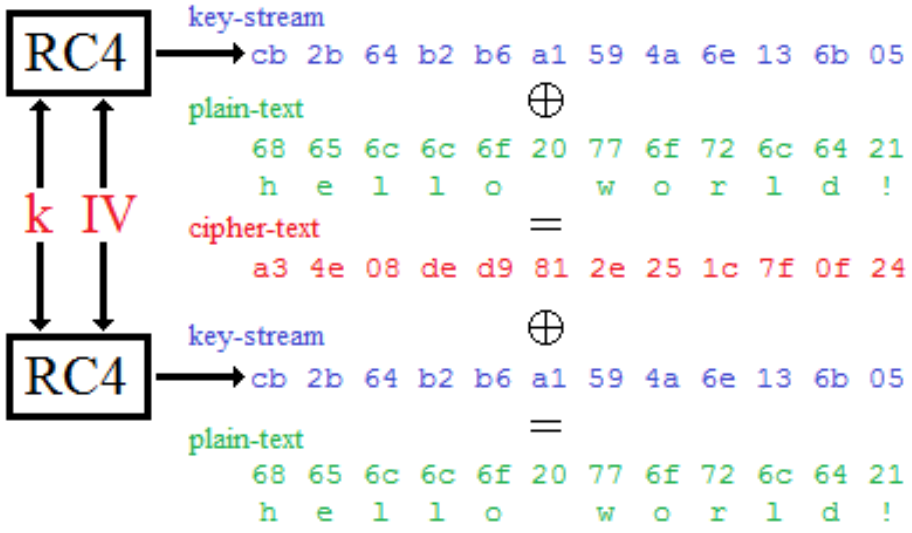
- Szyfrowanie za pomocą metody WEP odbywa się w następujący sposób.
  - Pomiędzy każdym bitem danych oraz bitem ciągu klucza generowana jest operacja XOR.
  - Wynikowy łańcuch przesyłany jest do publicznej sieci.
  - W następnym kroku druga strona ponownie wykonuje operację XOR na otrzymanych danych oraz kluczu, w rezultacie ujawniając oryginalną wiadomość.
  - WEP występuje w dwóch postaciach: dynamicznej oraz statycznej.
    - Postać statyczna zakłada używanie tego samego klucza przez cały czas funkcjonowania klienta w sieci.
    - Wersja dynamiczna ogranicza używanie zestawu kluczy do z góry określonego czasu.
  - Ponieważ sam WEP nie definiuje sposobu propagacji kluczy funkcje te przejęte zostały m.in. przez metody uwierzytelniania z rodziny 802.1X

Zabezpieczenie WEP

- W metodzie WEP stosuje się dwa rodzaje kluczy.
- Pierwszy z nich to unicast key. Klucz używany do zabezpieczania informacji w transmisji punkt - punkt.
- Drugi rodzaj klucza to broadcast key. Szyfrowane tym kluczem informacje zrozumiałe są dla wszystkich użytkowników sieci.
- Jeśli punkt dostępowy skonfigurowany jest do używania dwóch rodzajów kluczy każdy z klientów posiada swój własny unikalny unicast key.
- Wszyscy posiadają ten sam broadcast key.
- Najczęściej stosowane rozwiązanie jest najprostszym z możliwych i wymaga na użytkownikach stosowania tylko jednego klucza do wszystkich rodzajów komunikacji.

Zabezpieczenie WEP

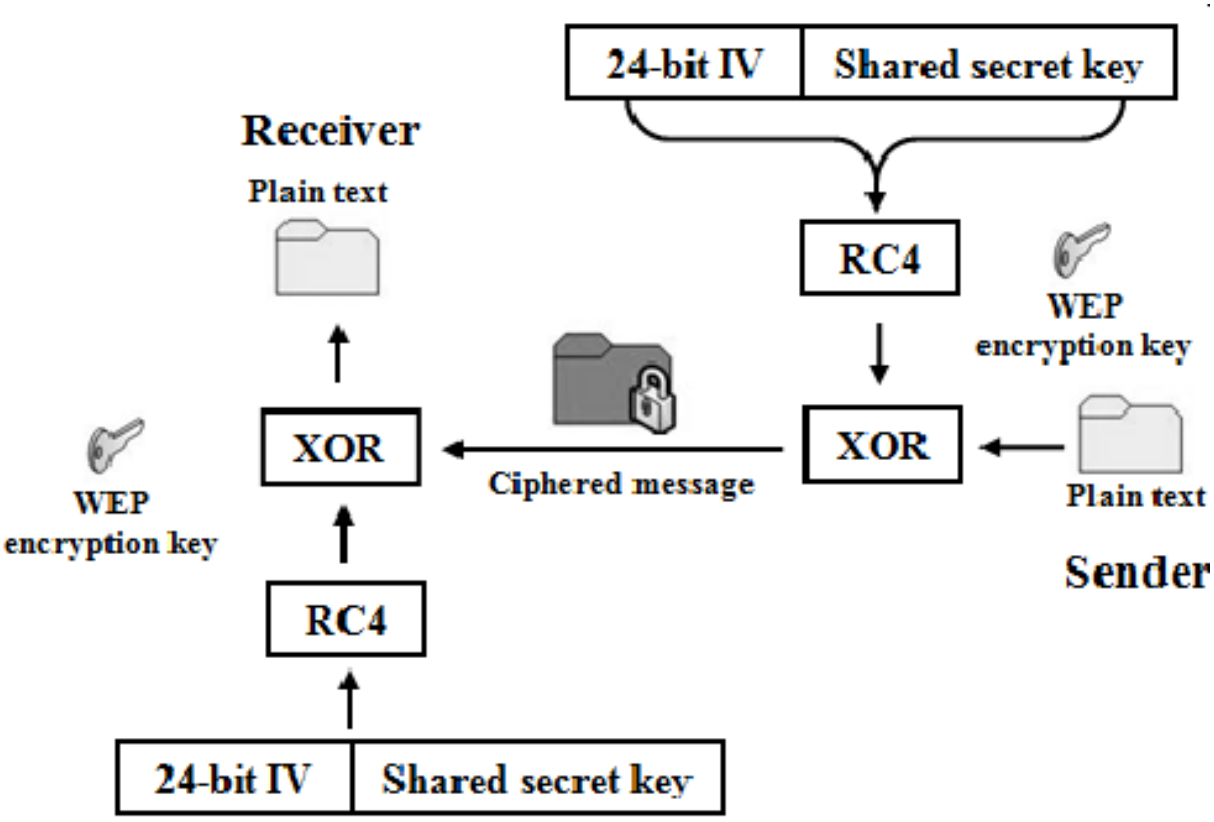
- Sam klucz składa się z dwóch części:
  - Pierwszej podawanej przez użytkownika.
  - Drugiej (IV – Initialization Vector) – wektora wprowadzającego zmienny element.
- Przykładowa sesja szyfrowania / deszyfrowania:



Zabezpieczenie WEP

- Sposób szyfrowania jest następujący:
  - Wektor Inicjujący dołączany jest w postaci jawnej do treści przesyłanych pakietów, aby możliwa była deszyfracja.
  - Najczęściej stosowaną długością klucza jest 128 bitów. 104 bity podawane są przez użytkownika.
  - Pozostałe 24 bity to IV.
  - Oznacza to, że istnieje tylko około 16.5 mln. unikatowych kluczy.
  - Gdy wektory wykorzystywane są wiele razy istnieje możliwość odgadnięcia klucza użytego przez nadajnik.

Zabezpieczenie WEP



Algorytm szyfrowania z wykorzystaniem protokołu WEP

Zabezpieczenie WEP - bezpieczeństwo

- Scott Fluhrer, Itsik Mantin, oraz Adi Shamir w roku 2001 przedstawili hipotetyczny sposób łamania kluczy WEP.
- Od nazwisk twórców atak ten nazwany został FMS.
- Implementacja po raz pierwszy wykonana została w laboratoriach AT&T.
- Jeżeli zgromadzona zostanie odpowiednio duża liczba pakietów, niektóre IV pozwalają ujawnić poszczególne bity klucza.
- Takie wektory nazywane są słabymi.
- Szacuje się, że wystarczy około 60 słabych wektorów do rozpracowania klucza.
- Jeśli wziąć pod uwagę, że 5% ze wszystkich używanych IV jest słabymi, stosowanie WEP przestaje być bezpieczne.

Zabezpieczenie WEP - bezpieczeństwo

- Stosowane dziś karty sieciowe nie używają słabych IV do kodowania informacji.
- Dodatkowym sposobem zabezpieczenia się przed atakiem jest odpowiednio częste zmienianie kluczy.
- Problemem nadal pozostaje ręczny sposób dystrybucji kluczy.
- Użytkownicy stosujący WEP jako podstawowy sposób szyfrowania informacji ciągle jeszcze nie są rzadkością.
- Wiele urządzeń nie posiada na tyle dużej mocy obliczeniowej, aby zastosować bardziej skomplikowany algorytm szyfrowania.
- W celu poprawienia sposobu szyfrowania przy jednoczesnym wykorzystaniu dotychczas wykorzystywanego sprzętu, opracowano protokół TKIP.
- Jest to część wprowadzonego w czerwcu 2004 roku standardu 802.11i

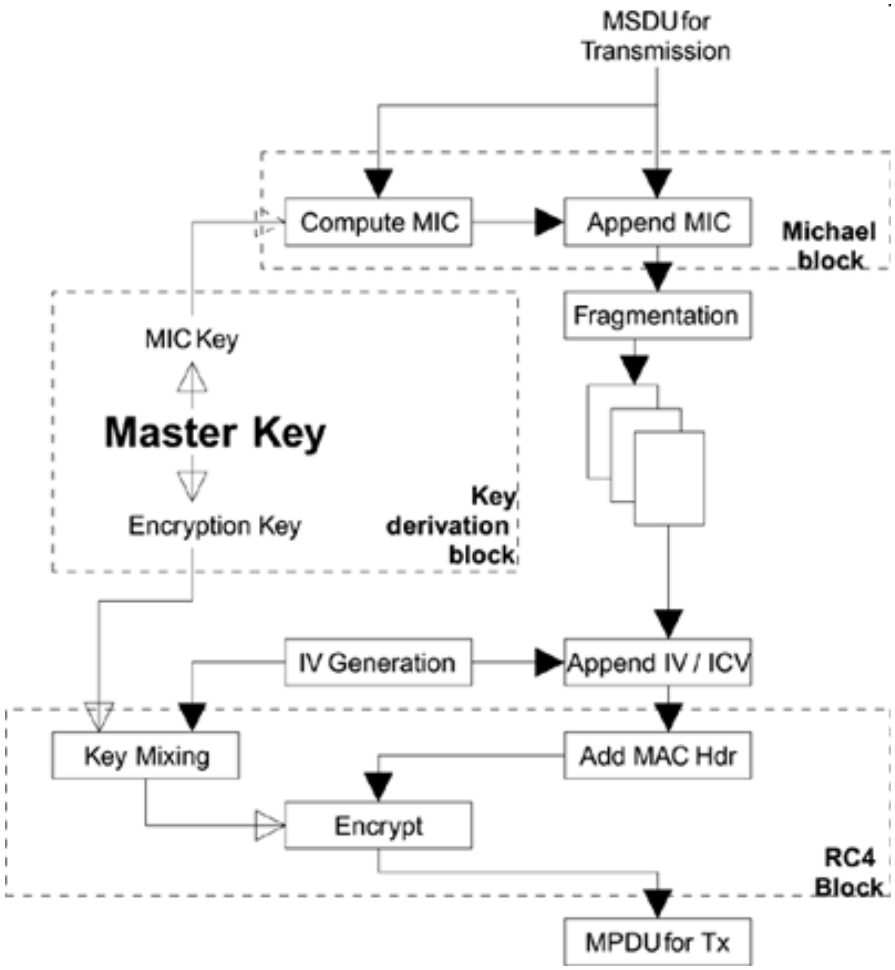
Zabezpieczenie TKIP

- TKIP pochodzi od słów Temporal Key Integrity Protocol.
- Zasada działania opiera się na takich samych zasadach jak WEP, ponieważ używany jest ten sam sprzęt przy odpowiednich zmianach oprogramowania i firmware'u.
- Zadaniem TKIP jest wzmocnienie WEP tam, gdzie dostrzeżono jego najsłabsze strony.
- Klucze używane do transmisji tworzone są przy udziale klucza głównego.
- Standard 802.1i opisuje również sposób zarządzania kluczami, dzięki czemu mogą one być odświeżone w dowolnym momencie.
- Do szyfrowania informacji w dalszym ciągu używany jest RC4, ale każda ramka szyfrowana jest za pomocą nowego klucza WEP.

Zabezpieczenie TKIP

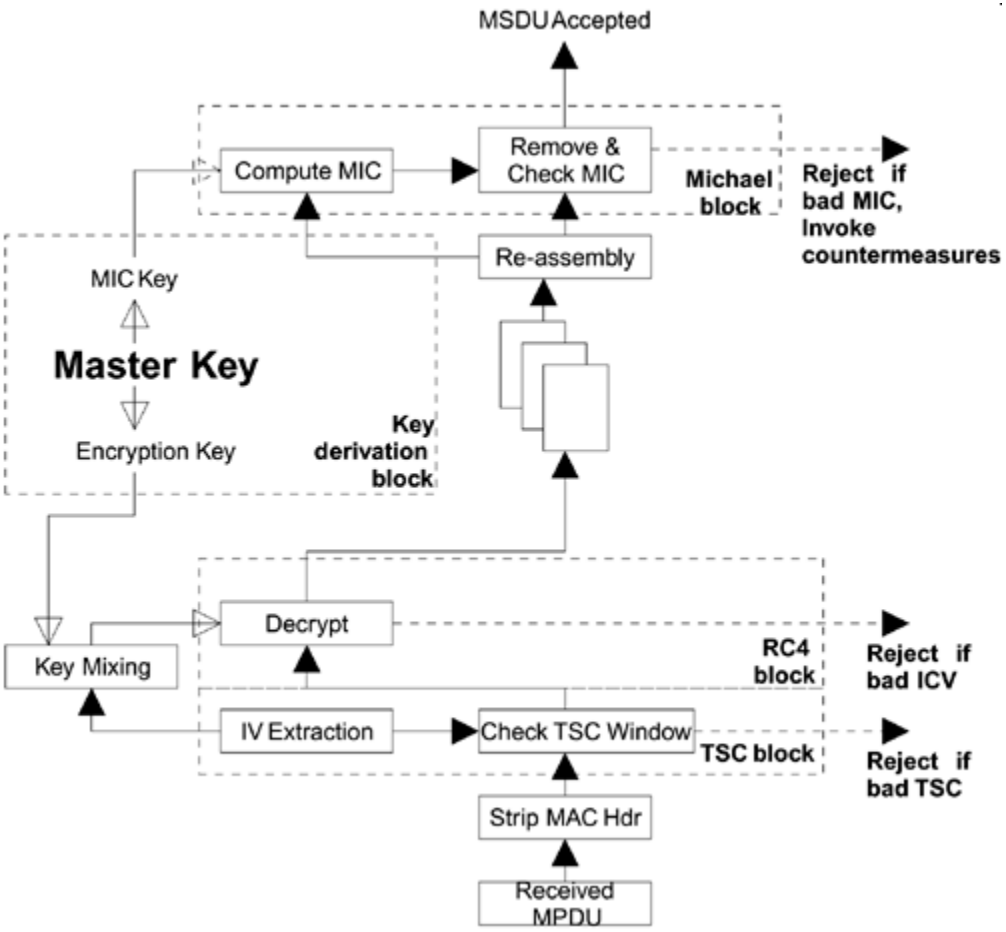
- Klucze do transmisji danych tworzone są z jednego klucza głównego, a proces ten nosi nazwę mieszania kluczy – key mixing.
- Dzięki temu nie jest możliwe złamanie klucza metodą FMS ponieważ za każdym razem jest on inny.
- Dużą uwagę poświęcono także na wychwytywanie zmian w transmisji.
- Każda ramka posiada unikalny numer sekwencji.
- Jeśli numeracja przestaje być spójna oznacza to próbę podłożenia fałszywych danych przez osobę trzecią.
- Nowy algorytm MIC – Michael wykonuje algorytm hashujący, aby wykryć modyfikacje informacji w przesyłanych ramkach.

Zabezpieczenie TKIP



TKIP - Transmisja

Zabezpieczenie TKIP



TKIP - Odbiór

Zabezpieczenie WPA

- W przeciwieństwie do TKIP, CCMP (Counter Mode with CBC-MAC Protocol) powstawał niezależnie.
- WPA to nazwa standardu marketingowego wprowadzonego przez WiFi Alliance.
- WPA 1 opiera się na drafcie 802.11i z roku 2003 i używa wspomnianego wcześniej TKIP.
- WPA 2 powstało po zatwierdzeniu wersji końcowej przez IEEE w roku 2004.
- Zaletą protokołu jest zastosowanie silnego algorytmu szyfrowania blokowego AES (Advanced Encryption Standard) dla wersji WPA2.
- WPA występuje w dwóch wersjach:
  - WPA Personal.
  - WPA Enterprise.
- Pierwsza działa na zasadzie rozpowszechnianego klucza, druga używa metod autentykacji z rodziny 802.1X.

Zabezpieczenie WPA

- CCMP używa tego samego klucza do szyfrowania oraz do zapewnienia integralności przesyłanych danych.
- Tak jak w TKIP klucz używany do szyfrowania generowany jest na podstawie klucza głównego.
- Gwarantuje to nowy klucz tymczasowy dla każdej nowej ramki.
- Dodatkowo w procesie biorą udział numer ramki, adres nadawcy oraz informacje dotyczące QoS.
- Protokół WPA uważany jest za względnie bezpieczny, jednak według NSA (U.S. National Security Agency) do szyfrowania nadzwyczaj poufnych informacji powinien zostać użyty klucz o długości 192 lub 256 bitów zamiast standardowych 128.
- Z uwagi na zastosowany algorytm AES (WPA2) karty bezprzewodowe wykorzystywane do transmisji wymagają dużo większej mocy obliczeniowej.

Zabezpieczenie 802.1X

- Stosowanie protokołów szyfrowania takich jak WEP, Dynamic WEP, TKIP, WPA1 oraz WPA2 wymaga zastosowania metod uwierzytelniania.
- Na początku o dostępie do sieci decydowała znajomość klucza szyfrującego.
- Klucze wpisywane były ręcznie, a za każdym razem, kiedy pracownik znający klucz odchodził z firmy, należało zmienić tajne hasło.
- Przy kilkudziesięciu stanowiskach pracy metoda jest zbyt czasochłonna.
- Rozwiązanie problemu stanowi protokół 802.1X.

Zabezpieczenie 802.1X

- Protokół jest adaptacją EAP (Extensible Authentication Protocol) ratyfikowanego przez IEEE i stanowi zbiór zasad oraz reguł, jakimi należy się posługiwać przy uwierzytelnianiu użytkowników.EAP jako jeden protokół funkcjonuje zarówno na platformie 802.3 oraz 802.11 i umożliwia stosowanie jednocześnie różnych metod autentykacji.
- W procesie biorą udział:
  - EAP authenticator – strona uwierzytelniająca;
  - EAP Authentication Server – baza danych użytkowników,
  - EAP supplicant – strona uwierzytelniana.
- Wymiana danych pomiędzy suplikantem, a stroną uwierzytelniającą odbywa się za pomocą protokołu EAPoL (EAP over Lan).
- Do czasu uwierzytelnienia suplikant nie ma dostępu do zasobów sieci poza niezbędnymi (przekazanie danych uwierzytelniających).

Zabezpieczenie 802.1X

- Sprawdzenie czy użytkownik ma prawo uzyskać dostęp do sieci odbywa się podczas wymiany danych pomiędzy serwerem a stroną uwierzytelniającą.
- Jeśli proces zakończy się powodzeniem użytkownik uzyskuje dostęp do sieci na określony czas.
- Jeżeli autentykacja zakończy się niepowodzeniem użytkownik może zostać zablokowany lub otrzymać ograniczone uprawnienia.
- Uprawnienia nadawane są na zasadzie Access List – ACL.
- Zawierają one zbiory dostępnych oraz zablokowanych dla użytkownika adresów.
- Wynikiem poprawnego uwierzytelnienia w sieci może być np. ustalenie wspólnego klucza używanego później do szyfrowania danych.
- 802.1X pozwala co pewien czas odświeżyć klucz lub zażądać ponownego uwierzytelnienia.

Zabezpieczenie 802.1X

- Przykładowy proces uwierzytelniania może przebiegać w następujący sposób:
  - Po nawiązaniu połączenia punkt dostępowy wysyła do suplikanta żądanie identyfikacji.
  - Użytkownik zwraca dane w postaci nazwy skróconej lub pełnej – razem z nazwą domeny.
  - Na podstawie podanej nazwy użytkownika generowany jest obliczony ciąg MD5 przesyłany do użytkownika.
  - Ponieważ użytkownik nie obsługuje takiej metody autentykacji zwraca do punktu dostępowego odpowiedź negatywną razem z propozycją uwierzytelnienia żetonem.
  - Następnie potwierdzana jest tożsamość użytkownika i proces kończy się sukcesem.
  - Podłączony i uwierzytelniony użytkownik uzyskuje dostęp do sieci.
  - EAP może próbować autentykacji użytkownika wieloma metodami.
  - Jeżeli jedna się nie powiedzie wykorzystana jest następna z dostępnej puli.
  - Dzięki temu różni klienci końcowi mogą używać różnych form uwierzytelnienia.

Porównanie protokołów WEP, WPA, WPA2

	WEP	WPA	WPA2
Algorytm szyfrowania	RC4	RC4	AES
Rotacja klucza	Brak	Klucze dynamiczne sesyjne	Klucze dynamiczne sesyjne
Dystrybucja klucza	Ręczna, wprowadzanie ręczne dla każdego urządzenia	Możliwa automatyczna dystrybucja	Możliwa automatyczna Dystrybucja
Metoda autentykacji	Klucz WEP	802.1x i EAP	802.1x i EAP

Zabezpieczenie NAC

- Omawiając kwestie bezpieczeństwa należy zwrócić również uwagę na pojawienie się zagrożeń ze strony nieświadomych użytkowników korzystających z sieci.
- Jeśli osoba posiada komputer zainfekowany wirusem lub programem takim jak koń trojański po podłączeniu do sieci może zainfekować pozostałe komputery lub umożliwić dostęp osobom z zewnątrz.
- Jeśli poufne dane - np. hasła podsłuchiwane będą przez procesy działające w tle, a następnie przesyłane do osób trzecich, wówczas wszelkiego typu szyfrowanie transmisji traci na znaczeniu.
- Aby zabezpieczyć się przed taką sytuacją stosuje się programy antywirusowe, firewalle na stacjach klienckich, programy antyspyware itp.
- Użytkownicy często próbują obejść narzucone im polityki zabezpieczeń wyłączając niewygodne dla nich funkcje.
- Powoduje to, że komputery stają się podatne na wspomniane wcześniej zagrożenia.

Zabezpieczenie NAC

- Jednym z możliwych rozwiązań problemu może być specjalizowane oprogramowanie, np. NAC (Network Admission Control) firmy Cisco Systems, firmy 3Com, czy też innych innych producentów.
- Zwykle wybór rozwiązania zależy od rodzaju użytkowanych urządzeń.
- W przypadku rozwiązań Cisco firma zapewnia, że gwarantuje ono zgodność maszyny, na której pracuje użytkownik z polityką bezpieczeństwa firmy.
- Idea rozwiązania opiera się na audycie stacji końcowych przed przyznaniem im dostępu do sieci.
- Specjalny program CTA (Cisco Trust Agent) monitoruje stan maszyny, zanim dopuści ją do wymiany danych.
- Jeśli odpowiednie funkcje są włączone, a oprogramowanie zaktualizowane użytkownik może uczestniczyć w transferze danych.
- Jeśli stacja nie posiada np. aktualnej bazy w programie antywirusowym lub jego komputer nie został wyposażony w program CTA może zostać odizolowany od sieci lub skierowany do VLAN-u, w którym jedyną dostępną maszyną będzie serwer z potrzebnymi aktualizacjami.
- Akcję taką podejmuje przełącznik sieciowy na podstawie polityki definiowanej w serwerze AAA.

Zabezpieczenie NAC

- Jeśli użytkownik spełni wymagania, pełny dostęp zostaje mu przywrócony.
- Centralną część zarządzającą stanowi serwer AAA.
- Wyposażony jest on w bazy użytkowników, zdefiniowane są na nim wymagania, jakie muszą spełniać stacje klienckie oraz reakcje na zdarzenia.
- Ten sam serwer jest częścią autentykacji 802.1X.
- Do serwera AAA łączą się wszystkie punkty dostępowe oraz przełączniki uczestniczące w procesie autentykacji klientów.
- Dzięki takiemu rozwiązaniu uwierzytelniany jest nie tylko użytkownik, ale również stacja, na której pracuje.
- Jeśli po otrzymaniu dostępu użytkownik wyłączy oprogramowanie chroniące jego maszynę informacja o tym trafi do przełącznika, następstwem czego będzie zmiana poziomu uprawnień.

Analiza zagrożeń - narzędzia

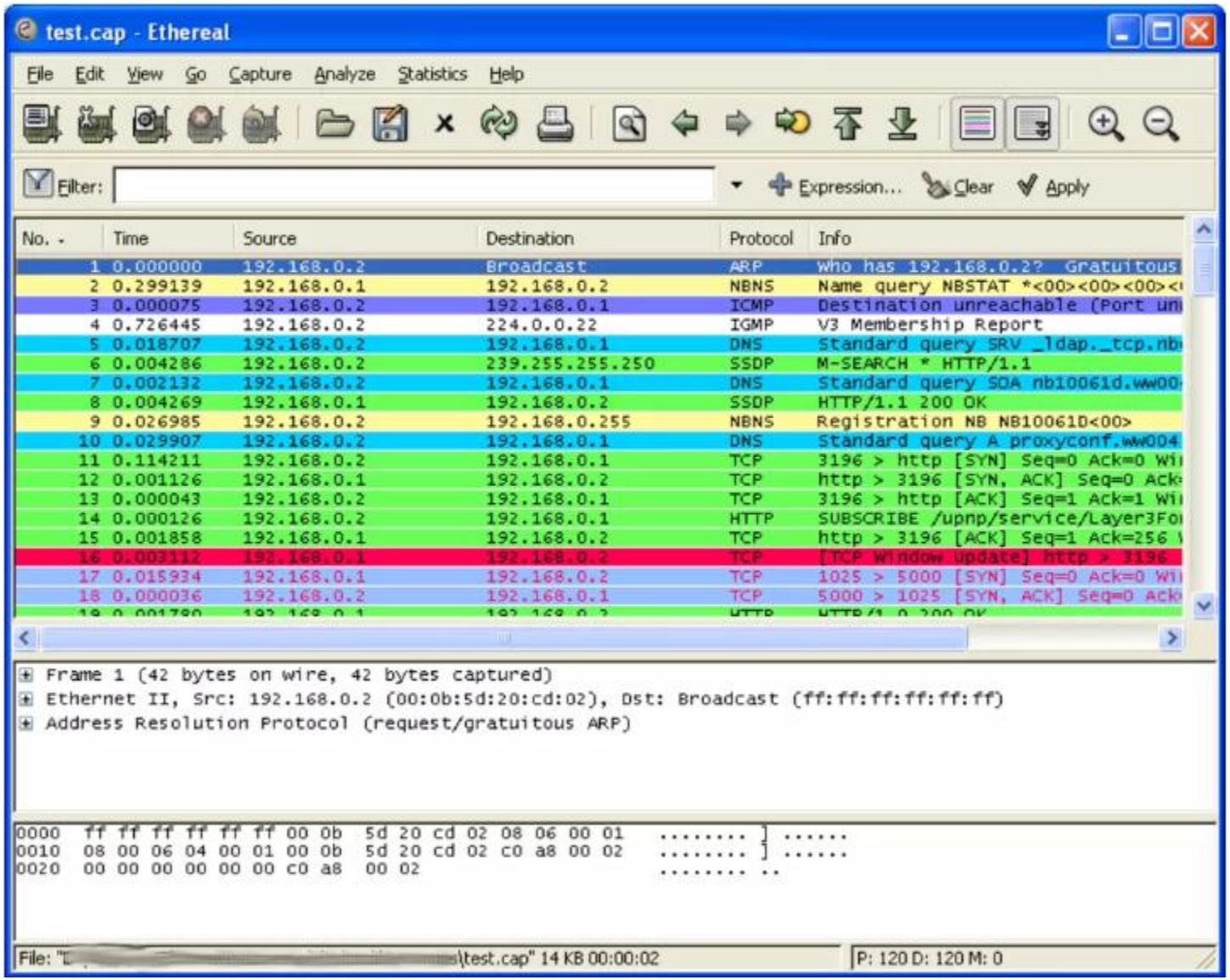
- Jednym z podstawowych problemów związanych z użytkowaniem sieci bezprzewodowych jest kwestia bezpieczeństwa.
- Jest wiele wyspecjalizowanych programów, które mogą być użyte do wykrycia luk w stosowanych systemach.
- Przykładem takich programów są:
  - Ethereal
  - Kismet
  - Airsnarf
  - Airsnort
  - Aircrack
  - Wireshark

- Warto zaznaczyć, że oprócz badania zabezpieczenia sieci programy te mogą być użyte do włamywania się i kradzieży informacji - co oczywiście jest sprzeczne z prawem.

Ethereal

- Ethereal – jest to popularny sniffer Ethernetowy.
- Ethereal wprowadza kartę sieciową w tryb, w którym odbiera ona i przekazuje wyżej wszystkie ramki, a nie tak jak normalnie, tylko przeznaczone dla siebie.
- Ponieważ sieć bezprzewodowa udostępnia odbiorcom dostęp do wszystkich ramek – możliwe jest podsłuchiwanie transmisji innych klientów bez stosowania specjalistycznych technik.
- Etheral udostępnia przyjazny użytkownikowi interfejs graficzny, dzięki czemu możliwe jest śledzenie przychodzących pakietów w czasie rzeczywistym.
- Możliwe jest także definiowanie interesującego ruchu który będzie składowany w zależności od protokołu, adresów lub innych opcji, a także składanie transmisji w całość i przedstawienie użytkownikowi samych danych z ostatniej warstwy – warstwy aplikacji bez zbędnych informacji.
- Dzięki temu można np. odczytać treści strony internetowej, jaką ogląda w danej chwili podsłuchany użytkownik lub ujawnić treść listów, na które odpisuje.

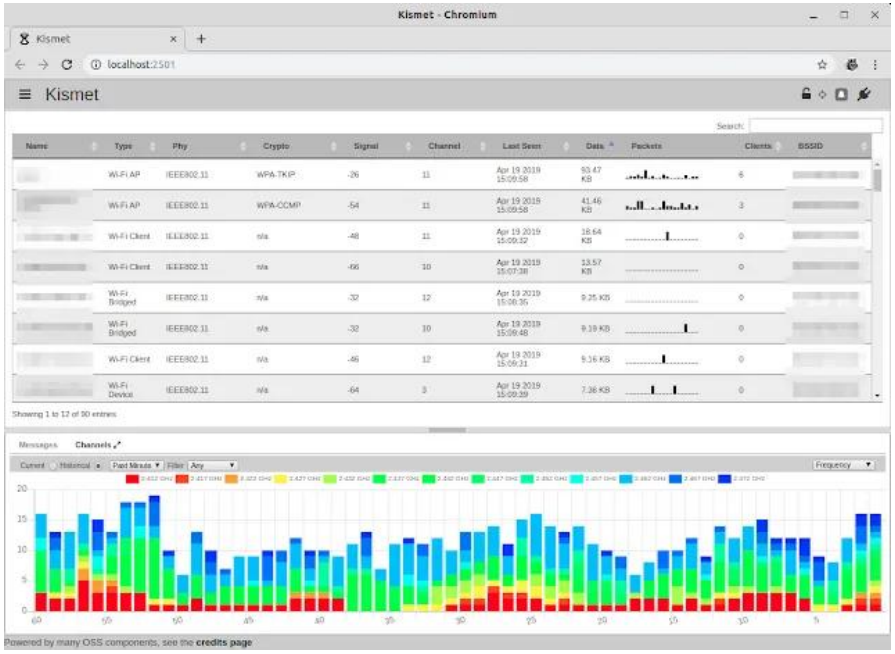
Ethereal

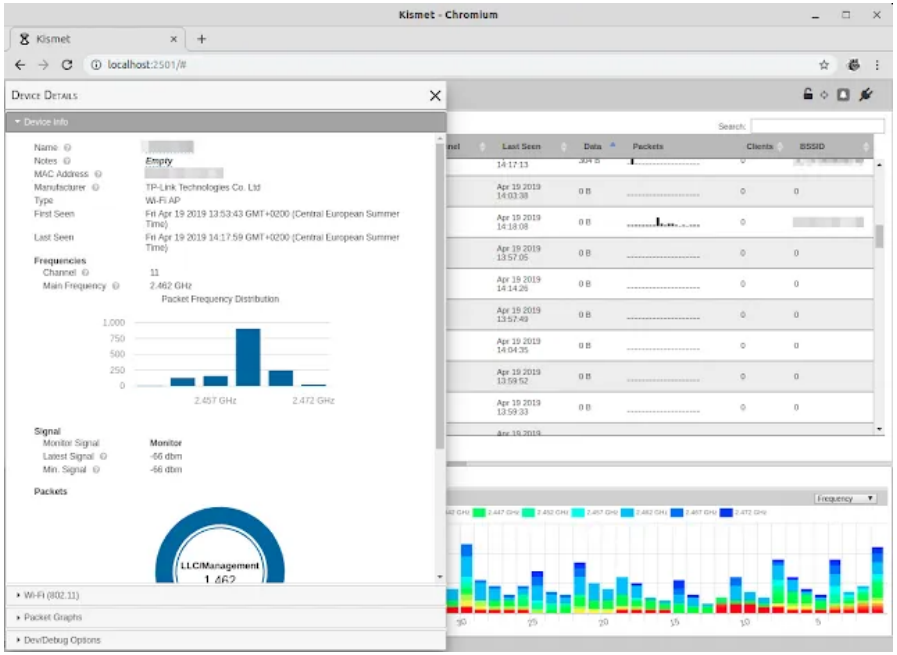

test.cap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.2 Broadcast ARP Who has 192.168.0.2? Gratuitous
2 0.299139 192.168.0.1 192.168.0.2 NBNS Name query NBSTAT *<00><00><00><
3 0.000075 192.168.0.2 192.168.0.1 ICMP Destination unreachable (Port un
4 0.726445 192.168.0.2 224.0.0.22 IGMP V3 Membership Report
5 0.018707 192.168.0.2 192.168.0.1 DNS Standard query SRV _ldap._tcp.nb
6 0.004286 192.168.0.2 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
7 0.002132 192.168.0.2 192.168.0.1 DNS Standard query SOA nb10061d.ww00
8 0.004269 192.168.0.1 192.168.0.2 SSDP HTTP/1.1 200 OK
9 0.026985 192.168.0.2 192.168.0.255 NBNS Registration NB NB10061D<00>
10 0.029907 192.168.0.2 192.168.0.1 DNS Standard query A proxyconf.ww004
11 0.114211 192.168.0.2 192.168.0.1 TCP 3196 > http [SYN] Seq=0 Ack=0 Wi
12 0.001126 192.168.0.1 192.168.0.2 TCP http > 3196 [SYN, ACK] Seq=0 Ack
13 0.000043 192.168.0.2 192.168.0.1 TCP 3196 > http [ACK] Seq=1 Ack=1 Wi
14 0.000126 192.168.0.2 192.168.0.1 HTTP SUBSCRIBE /upnp/service/Layer3Fo
15 0.001858 192.168.0.1 192.168.0.2 TCP http > 3196 [ACK] Seq=1 Ack=256
16 0.003112 192.168.0.1 192.168.0.2 TCP [TCP Window Update] http > 3196
17 0.015934 192.168.0.1 192.168.0.2 TCP 1025 > 5000 [SYN] Seq=0 Ack=0 Wi
18 0.000036 192.168.0.2 192.168.0.1 TCP 5000 > 1025 [SYN, ACK] Seq=0 Ack
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request/gratuitous ARP)
0000 ff ff ff ff ff ff 00 0b 5d 20 cd 02 08 06 00 01 ....] ......
0010 08 00 06 04 00 01 00 0b 5d 20 cd 02 c0 a8 00 02 ....] ......
0020 00 00 00 00 00 00 c0 a8 00 02 ....
File: "[redacted]\test.cap" 14 KB 00:00:02
P: 120 D: 120 M: 0

Kismet

- Kismet - to program który we współpracy z kartą sieciową potrafi analizować dostępne kanały radiowe, wskazywać jakiego rodzaju ruch odbywa się w okolicy klienta, oraz jakie sieci dostępowe znajdują się w zasięgu.
- Kismet posiada interfejs graficzny jednak działa on głównie w trybie konsolowym. Program bardzo dobrze radzi sobie z wykrywaniem sieci bezprzewodowych.

Kismet


Kismet - Chromium
Kismet
localhost:2501
Kismet
Search:
Name
Type
Phy
Crypto
Signal
Channel
Last Seen
Data
Packets
Clients
BSSID
Showing 1 to 12 of 30 entries
Messages
Channels
Powered by many OSS components, see the credits page


Kismet - Chromium
Kismet
localhost:2501/#
Device Details
Device Info
Name
Notes
Empty
MAC Address
Manufacturer
TP-Link Technologies Co. Ltd
Type
Wi-Fi AP
First Seen
Fri Apr 19 2019 13:53:43 GMT+0200 (Central European Summer Time)
Last Seen
Fri Apr 19 2019 14:17:59 GMT+0200 (Central European Summer Time)
Frequencies
Channel
11
Main Frequency
2.462 GHz
Packet Frequency Distribution
2.457 GHz
2.472 GHz
Signal
Monitor Signal
Monitor
Latest Signal
-66 dbm
Min. Signal
-66 dbm
Packets
LLC/Management
Wi-Fi (802.11)
Packet Graphs
Dev/Debug Options
Search:
Last Seen
Data
Packets
Clients
BSSID
Frequency

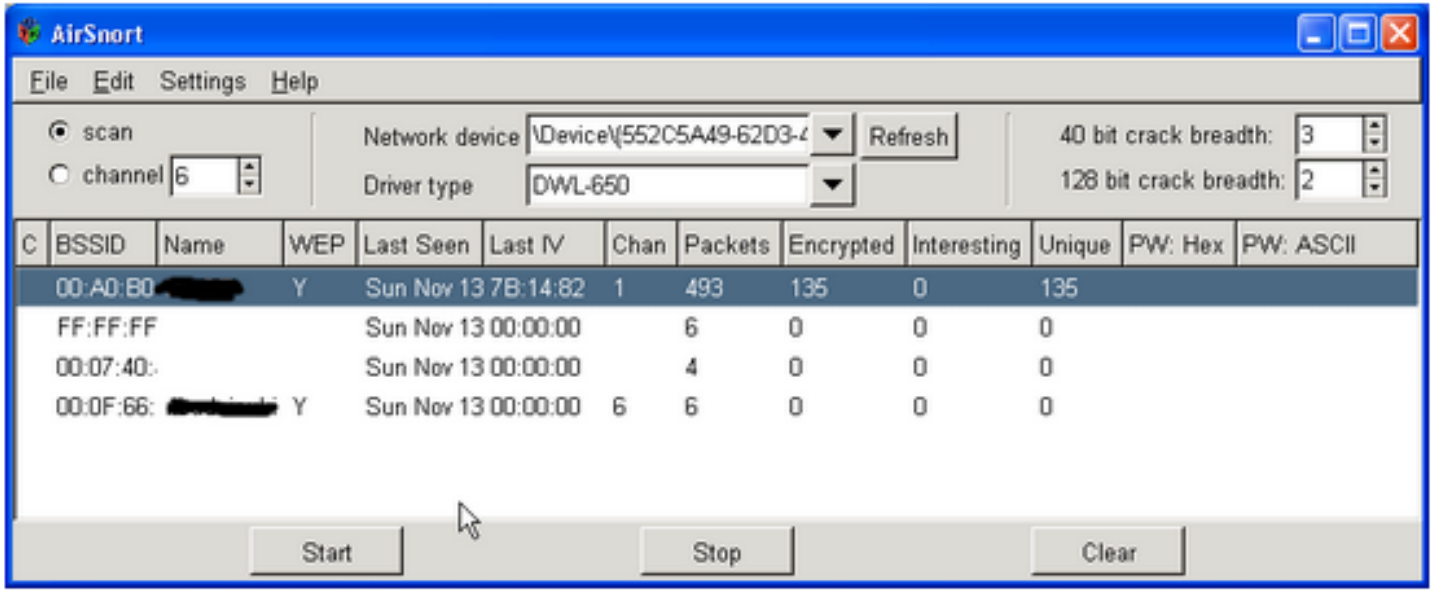
Airsnort, Aircrack

- Airsnort, Aircrack – programy służące do łamania kluczy WEP w sieciach bezprzewodowych.
- Aircrack jest tak naprawdę zestawem narzędzi do audytu sieci bezprzewodowych.
- Składa się z programu Airodump służącego do zapisywania pakietów na dysk,
- Aireplay – programu który wysyła do sieci zapisane wcześniej pakiety,
- Aircrack – programu do łamania kluczy WEP oraz WPA-PSK, Airdecap – programu pozwalającego na odszyfrowanie wcześniej zapisanej transmisji.
- Aircrack pozbawiony jest interfejsu graficznego. Wszystkie komendy wydawane są z konsoli, a wizualizacja efektów działania ograniczona jest do minimum.

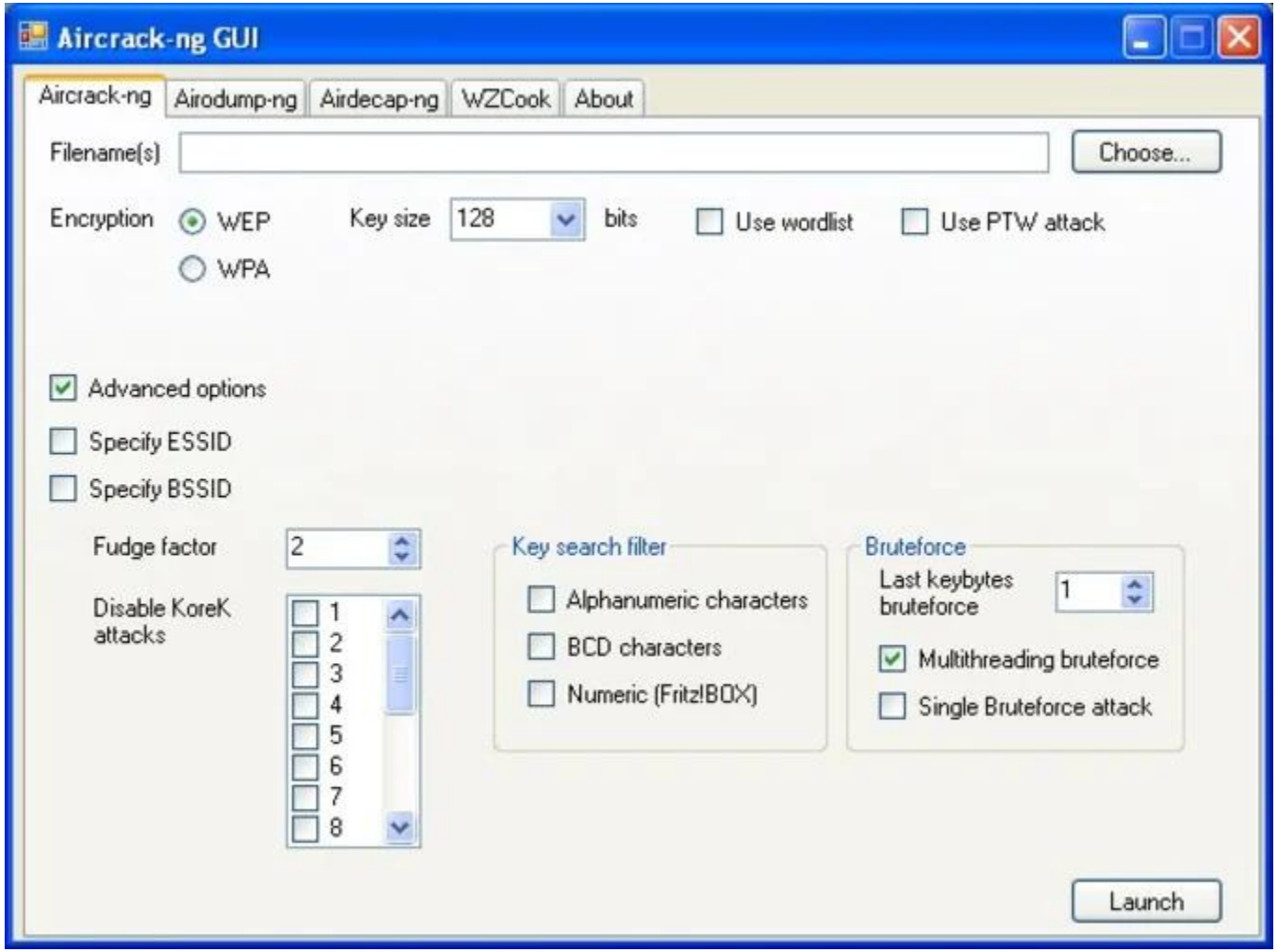
Airsnort, Aircrack

- Airsnort, Aircrack – programy służące do łamania kluczy WEP w sieciach bezprzewodowych.
- Aircrack jest tak naprawdę zestawem narzędzi do audytu sieci bezprzewodowych.
- Składa się z programu Airodump służącego do zapisywania pakietów na dysk,
- Aireplay – programu który wysyła do sieci zapisane wcześniej pakiety,
- Aircrack – programu do łamania kluczy WEP oraz WPA-PSK, Airdecap – programu pozwalającego na odszyfrowanie wcześniej zapisanej transmisji.
- Aircrack standardowo pozbawiony jest interfejsu graficznego. Wszystkie komendy wydawane są z konsoli, a wizualizacja efektów działania ograniczona jest do minimum. Istnieją jednak skompilowane do postaci aplikacji z interfejsem graficznym.

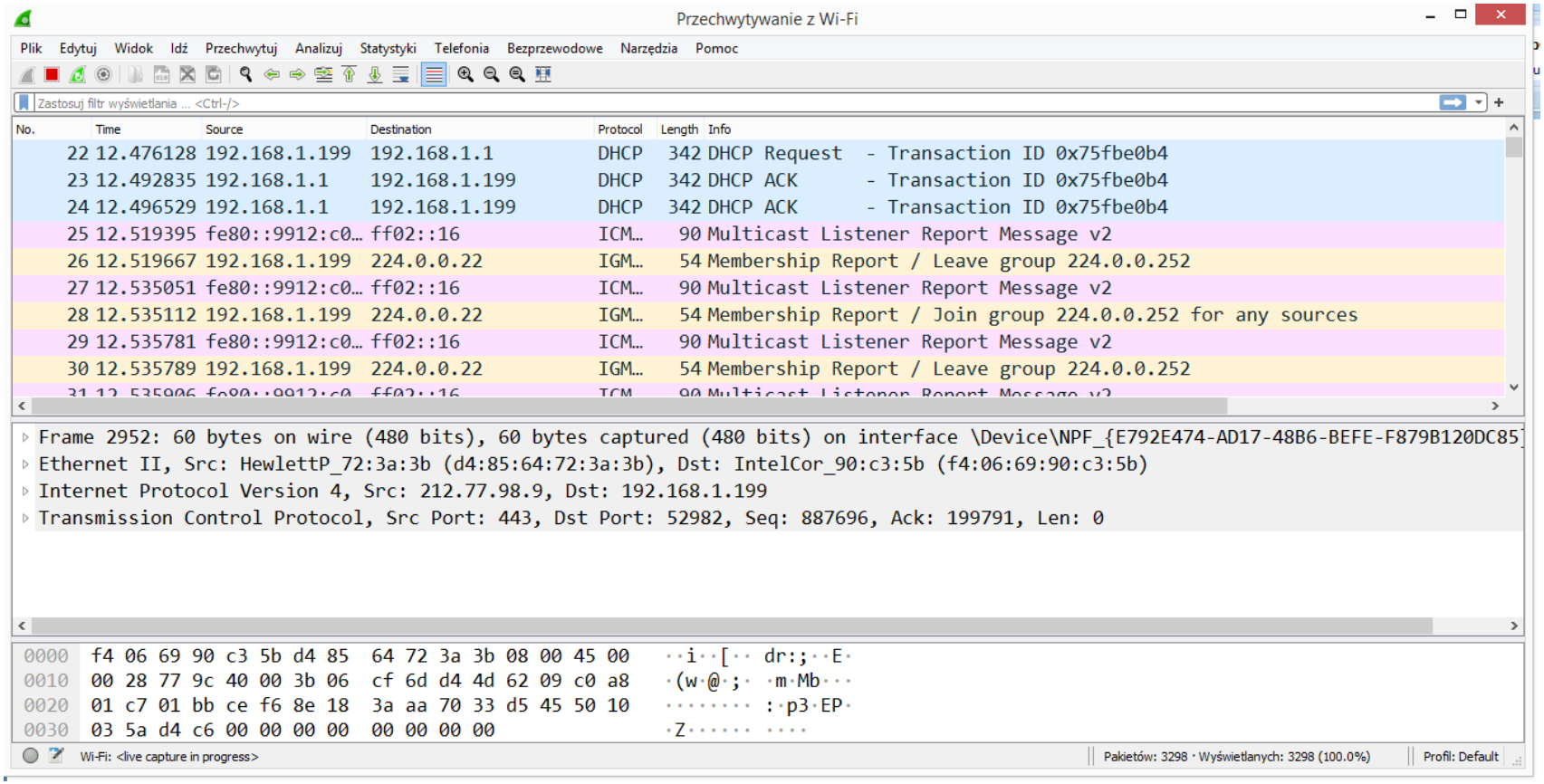
Airsnort


AirSnort
File Edit Settings Help
scan
channel 6
Network device \Device\{552C5A49-62D3-
Refresh
Driver type DWL-650
40 bit crack breadth: 3
128 bit crack breadth: 2
C BSSID Name WEP Last Seen Last IV Chan Packets Encrypted Interesting Unique PW: Hex PW: ASCII
00:A0:B0 Y Sun Nov 13 7B:14:82 1 493 135 0 135
FF:FF:FF Sun Nov 13 00:00:00 6 0 0 0
00:07:40: Sun Nov 13 00:00:00 4 0 0 0
00:0F:66: Y Sun Nov 13 00:00:00 6 6 0 0 0
Start
Stop
Clear

Aircrack


Aircrack-ng GUI
Aircrack-ng
Airodump-ng
Airdecap-ng
WZCook
About
Filename(s)
Choose...
Encryption
WEP
WPA
Key size
128
bits
Use wordlist
Use PTW attack
Advanced options
Specify ESSID
Specify BSSID
Fudge factor
2
Disable KoreK attacks
1
2
3
4
5
6
7
8
Key search filter
Alphanumeric characters
BCD characters
Numeric (Fritz!BOX)
Bruteforce
Last keybytes bruteforce
1
Multithreading bruteforce
Single Bruteforce attack
Launch

Wireshark


Przechwytywanie z Wi-Fi
Plik Edytuj Widok Idź Przechwytuj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
Zastosuj filtr wyświetlania ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
22 12.476128 192.168.1.199 192.168.1.1 DHCP 342 DHCP Request - Transaction ID 0x75fbe0b4
23 12.492835 192.168.1.1 192.168.1.199 DHCP 342 DHCP ACK - Transaction ID 0x75fbe0b4
24 12.496529 192.168.1.1 192.168.1.199 DHCP 342 DHCP ACK - Transaction ID 0x75fbe0b4
25 12.519395 fe80::9912:c0... ff02::16 ICM... 90 Multicast Listener Report Message v2
26 12.519667 192.168.1.199 224.0.0.22 IGM... 54 Membership Report / Leave group 224.0.0.252
27 12.535051 fe80::9912:c0... ff02::16 ICM... 90 Multicast Listener Report Message v2
28 12.535112 192.168.1.199 224.0.0.22 IGM... 54 Membership Report / Join group 224.0.0.252 for any sources
29 12.535781 fe80::9912:c0... ff02::16 ICM... 90 Multicast Listener Report Message v2
30 12.535789 192.168.1.199 224.0.0.22 IGM... 54 Membership Report / Leave group 224.0.0.252
Frame 2952: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{E792E474-AD17-48B6-BEFE-F879B120DC85}
Ethernet II, Src: HewlettP_72:3a:3b (d4:85:64:72:3a:3b), Dst: IntelCor_90:c3:5b (f4:06:69:90:c3:5b)
Internet Protocol Version 4, Src: 212.77.98.9, Dst: 192.168.1.199
Transmission Control Protocol, Src Port: 443, Dst Port: 52982, Seq: 887696, Ack: 199791, Len: 0
0000 f4 06 69 90 c3 5b d4 85 64 72 3a 3b 08 00 45 00
0010 00 28 77 9c 40 00 3b 06 cf 6d d4 4d 62 09 c0 a8
0020 01 c7 01 bb ce f6 8e 18 3a aa 70 33 d5 45 50 10
0030 03 5a d4 c6 00 00 00 00 00 00 00 00
Wi-Fi: <live capture in progress>
Pakietów: 3298 · Wyświetlanych: 3298 (100.0%)
Profil: Default

Dziękuję za uwagę