Diagnostyka sprzętu komputerowego

Autor: Zespół autorów
ISBN: 83-246-0319-0
Format: B5, stron: 144

Nawet najbardziej niezawodny komputer czasem działa nieprawidłowo. Rozwiązanie nasuwające się jako pierwsze – oddanie sprzętu do naprawy – tylko pozornie jest najlepsze. Każdy serwis za zdiagnozowanie usterki wystawi rachunek, czasami dość słony. Może więc spróbować samodzielnie znaleźć przyczynę problemów i usunąć ją? Dzięki programom diagnostycznym zadanie to może wykonać także początkujący użytkownik komputera.

Czytając książkę „Diagnostyka sprzętu komputerowego", nauczysz się korzystać z programów monitorujących pracę komputera oraz wykrywać i usuwać usterki. Dowiesz się, jak sprawdzić parametry systemu za pomocą programów SiSoft Sandra i Everest. Przeanalizujesz połączenia sieciowe i zabezpieczenia komputera, a także poznasz sposoby przywracania uszkodzonego systemu za pomocą płyt UBCD i EBCD.

- Testowanie systemu i kart graficznych
- Kontrola temperatury procesora i napięcia na płycie głównej
- Zmiana taktowania płyty głównej
- Testowanie połączeń sieciowych
- Tworzenie płyt UBCD i EBCD oraz korzystanie z nich

Masz problem z komputerem?
Rozwiąż go samodzielnie, a zaoszczędzisz sporo pieniędzy

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Rozdział 4.

Diagnostyka sieci

[Autor: Sławomir Orłowski, e-mail: *bigman@phys.uni.torun.pl*]

Coraz więcej komputerów jest obecnie podłączonych do internetu. Znajomość podstawowych pojęć związanych z diagnostyką sieci staje się więc nieodzowna. W tym rozdziale postaramy się przybliżyć to zagadnienie w sposób jak najbardziej przystępny. Bez zbędnego wdawania się w szczegóły przedstawimy podstawy działania sieci komputerowych. Sądzimy, że po przeczytaniu tego rozdziału Czytelnik będzie w stanie sam zdiagnozować i ewentualnie rozwiązać podstawowe problemy z siecią.

Połączenie z siecią

Zabezpieczenie komputera

Przed podłączeniem komputera do sieci należy zadbać o jego odpowiednie zabezpieczenie. Podstawą jest instalacja najnowszych poprawek dla systemu operacyjnego, przeglądarki internetowej, programu pocztowego oraz innych programów znajdujących się na komputerze, które korzystają z połączeń sieciowych. Standardowe ustawienia systemu Windows umożliwiają automatyczne sprawdzanie, czy są dostępne nowe poprawki oznaczone jako krytyczne. Jeżeli chcemy sami dokonać aktualizacji, musimy wybrać menu *Start*, a następnie *Windows Update*. Nasz komputer połączy się z witryną *Microsoft Windows Update*. Nastąpi sprawdzenie legalności systemu oraz posiadanych poprawek. Jeżeli nowe poprawki będą dostępne dla naszego komputera, będziemy mogli je pobrać i zainstalować. Instalacja jest prosta i intuicyjna. Następnym bastionem obrony jest oprogramowanie antywirusowe. Istnieje co najmniej kilka darmowych programów antywirusowych, które świetnie spełniają swoje zadanie. Oto lista najpopularniejszych:

- AntiVir Personal (*http://www.free-av.com/*)
- AVG Free (*http://free.grisoft.com/*)
- AVAST! Home Edition (*http://www.avast.com/*)

Programy te są darmowe do użytku indywidualnego. Firmy powinny zakupić licencje. Należy pamiętać, aby regularnie aktualizować bazę wirusów. Nowe wirusy i ich odmiany pojawiają się codziennie. Brak połączenia z internetem może być wynikiem działania wirusa. Zabezpieczeniem, które również powinno znaleźć się w naszym systemie, jest zapora sieciowa (ang. *firewall*). Jest to program, który aktywnie chroni komputer przed nieautoryzowanym połączeniem z siecią. Bardzo wiele wirusów wykorzystuje tzw. otwarte porty, aby przejąć kontrolę nad systemem. System Windows wraz z kompletem poprawek Service Pack 2 (SP2) ma wbudowaną zaporę sieciową. Możemy jednak skorzystać z programów innych producentów. Istnieje również kilka darmowych zapór sieciowych, które dają nam większą kontrolę niż ta zawarta w SP2. Przed ich uruchomieniem należy pamiętać, aby wyłączyć systemową zaporę. Jedną z nich jest program *ZoneAlarm* (*http://www.zonelabs.com/*). Warto zainstalować także oprogramowanie wyszukujące i usuwające z systemu oprogramowanie szpiegowskie. Może to być np. darmowy program *Ad-Aware Personal* (*http://www.lavasoftusa.com/software/adaware/*).

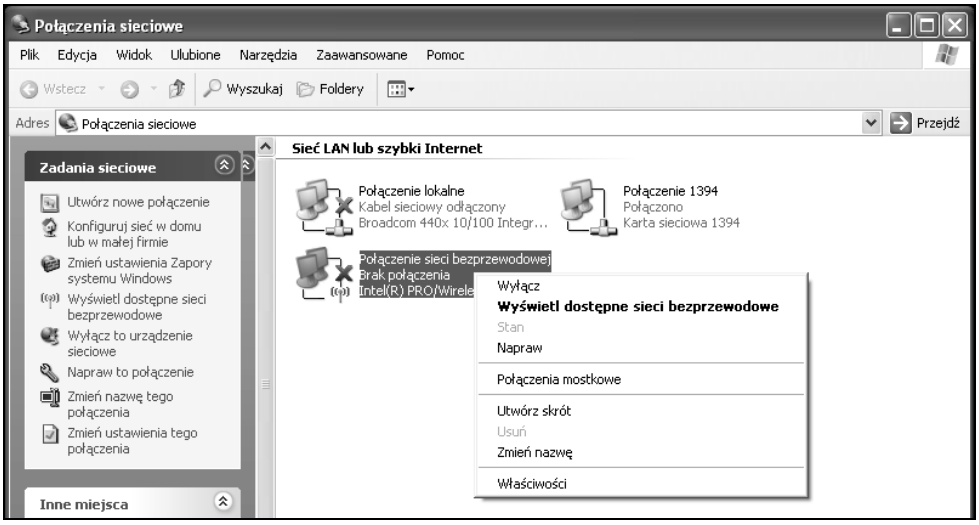
Najbardziej zawodnym elementem każdego zabezpieczenia jest człowiek. Z internetu należy korzystać w sposób rozważny, ponieważ żadne, nawet najlepsze zabezpieczenie nie jest w stanie wyeliminować tzw. czynnika ludzkiego. Nie należy otwierać załączników do wiadomości pocztowych niewiadomego pochodzenia. Nie wolno zgadzać się na aktywne elementy stron internetowych (*ActiveX*) nieznanych producentów. Nie należy akceptować nieznanych rozszerzeń przeglądarki internetowej (*plugin*) ani pobierać oprogramowania niepewnego pochodzenia.

Sygnalizacja braku połączenia

Pierwszym objawem braku połączenia z siecią w systemach Windows 2000/XP może być pojawienie się charakterystycznej ikony rozłączonej sieci w zasobniku systemowym (rysunek 4.1). W takim wypadku powinniśmy sprawdzić, czy nasz komputer jest fizycznie podłączony do sieci. Może się zdarzyć, że kabel sieciowy wysunął się z gniazdka komputerowego bądź z gniazdka umieszczonego w ścianie. Mógł się zepsuć również sam kabel sieciowy. Szczególnie narażonym miejscem w przewodzie jest połączenie z wtyczką RJ-45. Jeżeli kabel sieciowy zostanie przyciśnięty przez ciężki mebel, może zostać zniszczony. Jeżeli zatem jesteśmy pewni, że komputer jest dobrze skonfigurowany, oraz mamy dostęp do internetu, przyczyną braku połączenia może być kabel sieciowy. W przypadku sieci bezprzewodowej przyczyną rozłączenia może być oddalenie się poza zasięg nadajnika. Jeżeli posiadamy antenę zewnętrzną, ważny jest kąt jej ustawienia (zob. podrozdział „Sieci bezprzewodowe. Program Network Stumbler").

Rysunek 4.1.
Ikony sygnalizujące brak połączenia z siecią bezprzewodową i LAN (od lewej)

W przypadku zerwania połączenia system Windows będzie ponawiał próby połączenia. Możemy również próbować łączyć się samodzielnie. W tym celu klikamy prawym przyciskiem myszy ikonę *Połączenia sieciowe* (znajduje się na pulpicie bądź w menu *Start*). Wybieramy z menu kontekstowego właściwego połączenia polecenie *Właściwości* (rysunek 4.2). Wyświetlą się wówczas dostępne połączenia sieciowe. Klikamy prawym



Rysunek 4.2. *Połączenia sieciowe*

przyciskiem myszy połączenie. Z rozwiniętego menu wybieramy polecenie *Napraw*. System wyłączy połączenie, a następnie włączy i będzie próbował ustanowić nowe.

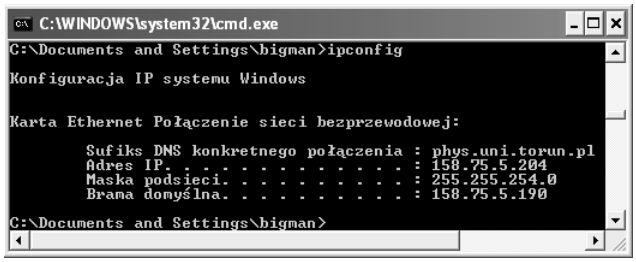
Sprawdzanie konfiguracji sieci. Adres IP

Komputery połączone w sieć powinny umieć komunikować się ze sobą. Zbiór reguł określających sposoby wymiany informacji pomiędzy komputerami nazywamy *protokołem*. W internecie najpopularniejszym protokołem jest TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*). Jest to podstawowy protokół (a w zasadzie zbiór dwóch protokołów), dzięki któremu możliwe jest nawiązanie połączenia i wymiana danych pomiędzy komputerami w sieci. Inne protokoły obowiązujące w internecie to między innymi HTTP (ang. *Hypertext Transfer Protocol*), który odpowiada za udostępnianie dokumentów (stron internetowych) w sieci WWW, oraz FTP (ang. *File Transport Protocol*), który odpowiada za przesyłanie plików pomiędzy komputerami. Oprócz tych dwóch istnieje sporo innych protokołów sieciowych (ARP, RARP, DHCP itd.). W celu identyfikacji komputera bądź urządzenia sieciowego w sieci TCP/IP jest mu przyporządkowywany adres IP. Adres ten ma formę czterech oktetów oddzielonych kropkami. Przykładowo adres 213.186.88.113 odpowiada serwerowi, który obsługuje stronę www.helion.pl. W tej samej sieci nie może być dwóch identycznych adresów IP. Jeżeli spróbujemy swojemu komputerowi nadać już istniejący adres IP, wówczas wyświetlony zostanie odpowiedni komunikat o błędzie. W sieci istnieją specjalne serwery DHCP (*Dynamic Host Configuration Protocol)*, przydzielające adresy IP. Każda karta sieciowa ma również nadany unikalny w skali świata adres MAC. Adres jest 48-bitowy, z czego pierwsze 24 bity to kod producenta, a kolejne 24 to numer seryjny (np. 00-12-F0--C0-89-69). Liczby podawane są zwykle w systemie heksadecymalnym (szesnastkowym). Jest on potrzebny do identyfikacji komputera przez urządzenia sieciowe niedziałające na adresach IP. Adres IP możemy przyrównać do adresu zamieszkania i kodu pocztowego, natomiast adres MAC do imienia i nazwiska. Ważnym pojęciem

w dziedzinie sieci komputerowych jest również brama sieciowa (ang. *gateway*). Jest to komputer w lokalnej sieci komputerowej, za którego pomocą pozostałe komputery w tej sieci komunikują się z internetem bądź inną siecią lokalną. W sieciach mogą również znajdować się serwery proxy, pośredniczące pomiędzy przeglądarką WWW a serwerami WWW, na których znajdują się strony internetowe. Jest to więc usługa buforowania zwiększająca szybkość pobierania stron internetowych. Jeżeli jakaś strona jest często wyświetlana, wówczas znajduje się w pamięci serwera proxy, dzięki czemu dostęp do niej jest szybszy. Inne rodzaje serwerów pośredniczących mogą obsługiwać w zasadzie dowolne usługi np. FTP, transmisję głosu itd.

Do sprawdzenia naszego adresu w sieci TCP/IP służy polecenie *ipconfig*. Polecenie to należy wydać z konsoli systemowej (rysunek 4.3). Aby ją otworzyć, klikamy menu *Start/Uruchom* i w wyświetlonym oknie wpisujemy polecenie *cmd*.

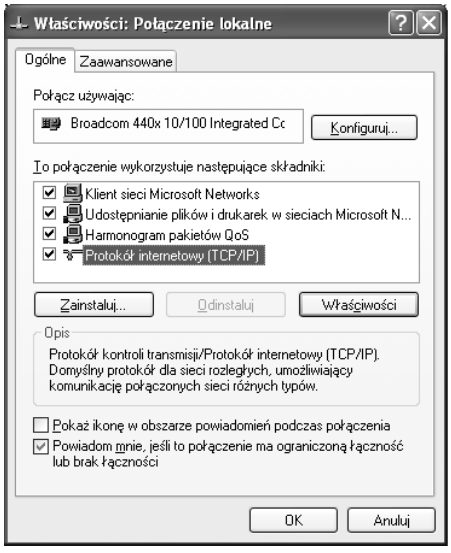
Rysunek 4.3.
Sprawdzenie adresu IP



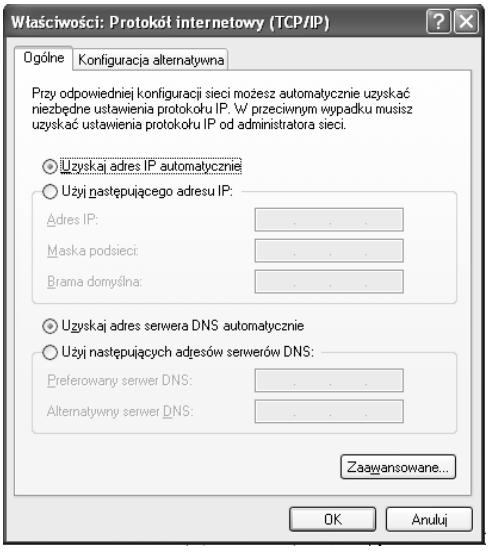
Jeżeli nasz komputer nie będzie miał adresu IP (w miejscu Adres IP będzie 0.0.0.0) i jesteśmy pewni, że kabel sieciowy działa, powinniśmy skontaktować się z administratorem sieci. Dopisze on komputer do listy, dzięki której nasz komputer będzie otrzymywał adres IP automatycznie za pomocą protokołu DHCP. Po otrzymaniu adresu IP nie trzeba ponownie uruchamiać komputera. Wystarczy wpisać polecenie *ipconfig /renew*, które odnawia adres IP. Należy również sprawdzić ustawienia protokołu TCP/IP. W tym celu klikamy prawym przyciskiem myszy *Połączenia sieciowe*, a następnie *Właściwości*. Wyświetlą się wszystkie dostępne połączenia sieciowe (komputer może mieć więcej niż jedną kartę sieciową). Wybieramy to, które aktualnie konfigurujemy, i klikamy prawym przyciskiem myszy. Wybieramy *Właściwości*. Wyświetli się okno właściwości połączenia (rysunek 4.4).

W zakładce *Ogólne* z listy składników wybieramy pozycję *Protokół internetowy (TCP/IP)*. Następnie klikamy przycisk *Właściwości*. Wyświetlone zostanie okno *Właściwości: Protokół internetowy TCP/IP*.

Ustawienia powinny być takie jak na rysunku 4.5, tzn. *Uzyskaj adres IP automatycznie* oraz *Uzyskaj adres serwera DNS automatycznie*. W sieci TCP/IP komputery rozpoznają się poprzez adres IP. Jeżeli wpiszemy do przeglądarki internetowej jakiś adres, np. *http://www.phys.uni.torun.pl/*, wówczas serwer DNS na podstawie adresu odnajduje IP komputera. Tę samą stronę możemy wyświetlić, wpisując adres IP serwera, na którym znajduje się strona internetowa *http:///158.75.5.90/*. Serwer DNS zapewnia więc translację nazw domenowych na adresy IP. DNS to również system prawny zapewniający rejestrację domen internetowych i powiązanie ich z adresami IP. Jeżeli w sieci, do której jesteśmy podłączeni, nie działa usługa DHCP bądź administrator sieci życzy sobie,



Rysunek 4.4. *Okno właściwości połączenia sieciowego*



Rysunek 4.5. *Okno właściwości protokołu TCP/IP*

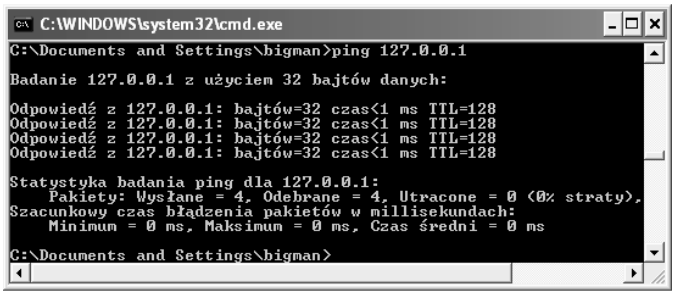
aby ręcznie konfigurować połączenia sieciowe, wówczas dostaniemy komplet danych zawierających adres IP naszego komputera, maskę podsieci, bramkę domyślną oraz adres serwera DNS. Wszystkie te informacje należy wpisać właśnie w to okno. Wszystkie te liczby należy również zapisać na kartce, aby po awarii systemu móc szybko ustanowić połączenie z internetem. Możliwe jest również ustawienie konfiguracji alternatywnej, na przykład jeżeli posiadamy notebooka, którego podłączamy do różnych sieci. Kolejnym powodem, dla którego nasz komputer nie dostanie adresu IP, jest wymiana karty sieciowej (bądź całego komputera). Zmienia się wówczas adres MAC karty i w sieciach DHCP opartych na tablicach adresów MAC nie dostaniemy adresu IP. W takim przypadku powinniśmy poinformować administratora o wymianie karty i podać mu aktualny adres MAC. Aby go sprawdzić, w konsoli systemowej wydajemy polecenie

ipconfig /all. Wyświetlą się wówczas wszystkie informacje na temat konfiguracji sieciowej naszego komputera. Adres MAC podany jest jako *Adres fizyczny*.

W systemach Windows 98/Me komenda, która sprawdza adres IP, to winipcfg.

Testowanie połączenia. Polecenie PING

Polecenie *ping* umożliwia nam sprawdzenie, czy dowolny komputer przyłączony do sieci jest dla nas widoczny. Samo polecenie działa jak echo, tzn. wysyła pakiet (*echo request*) do wskazanego przez nas komputera i jeżeli ten odpowie na niego (*echo reply*), wówczas wyświetlana jest informacja o jego dostępności. Standardowo w systemie Windows wysyłane są 4 pakiety po 32 bajty. Mierzony jest czas podróży pakietu do adresata i z powrotem oraz podawany jest parametr TTL (ang. *Time-To-Live*). Na zakończenie podawana jest statystyka dla polecenia ping: ile pakietów wysłano, ile z nich odebrano, a także maksymalny, minimalny i średni czas podróży pakietów. Polecenie to sprawdza się świetnie w testowaniu połączenia pomiędzy dwoma komputerami w sieci. Odpowiada nam jednoznacznie, czy dwa komputery „widzą" się w sieci. Jednak w przypadku serwerów sieciowych sprawa jest trudniejsza, ponieważ niektóre serwery znajdujące się w internecie nie odpowiadają na zapytanie *echo request* bądź na przykład odpowiadają tylko raz. Powodem jest możliwość przeprowadzenia ataku na serwer za pomocą dużej liczby komputerów jednocześnie wysyłających *echo request*. Może to doprowadzić do zawieszenia się serwera, który nie będzie w stanie obsłużyć tak dużego ruchu. Programy typu firewall bardzo często blokują pakiety ICMP, przez co odpowiedź na ping'a jest niemożliwa. Polecenie ping najwygodniej jest wydać z konsoli systemowej (rysunek 4.6). Jako argument podajemy adres IP komputera, z którym połączenie chcemy sprawdzić, bądź jego nazwę DNS w sieci (np. `ping wp.pl`). Jeżeli zatem nie możemy wyświetlić żadnej strony internetowej, a polecenie ping pokazuje, że serwer (np. wp.pl lub onet.pl) jest dostępny, wówczas problemem może być źle skonfigurowany serwer DNS.



Rysunek 4.6. *Przykładowe działanie polecenia ping. W tym przypadku adres IP 127.0.0.1 podany jako argument polecenia ping odpowiada za tzw. pętlę zwrotną. Innymi słowy, wysyłamy echo request do siebie*

Diagnostyka sieci z wykorzystaniem narzędzi systemu Windows

System Windows XP ma dosyć wygodne narzędzie diagnozujące sieć. Znajduje się ono w *Centrum pomocy i obsługi technicznej*. Za pomocą tego narzędzia możemy szybko i łatwo wyświetlić informacje na temat środowiska sieciowego, komputera oraz jego kart sieciowych. Wykonywane są standardowe testy łączności za pomocą opisywanej wcześniej komendy ping. Badany jest dostęp do zasobów, usług i serwerów sieciowych takich jak DNS i DHCP. Aby włączyć narzędzie *Diagnostyka sieci*, klikamy menu *Start*, a następnie *Pomoc i obsługa techniczna*. Otworzy się okno *Centrum pomocy i obsługi technicznej*. Okno podzielone jest na kilka kategorii. Nas interesuje lista *Wybierz zadanie*. Wybieramy z niej pozycję *Użyj Narzędzi, aby wyświetlić informacje o komputerze i przeanalizować problemy*. Po lewej stronie okna wyświetlone zostaną wszystkie dostępne narzędzia. Z listy *Tools* wybieramy opcję *Diagnostyka sieci*. W oknie głównym wyświetlą nam się dostępne opcje. Możemy uruchomić skaner *Diagnostyka Sieci* (polecenie *Skanuj system*) lub ustawić opcje skanowania (polecenie *Ustaw opcję skanowania*). Wybierzmy ustawianie opcji skanowania systemu i sieci. Opis każdej opcji zawiera tabela 4.1. Wybieramy wszystkie opcje skanowania i naciskamy przycisk *Skanuj system*. Po kilku chwilach wyświetlą się informacje podzielone na trzy kategorie: Usługa internetowa, Informacje o komputerze, Modemy i karty sieciowe. Informacje przedstawione są w formie drzewa. Sprawdzana jest dostępność podstawowych usług sieciowych. Uzyskujemy również przydatne informacje o strukturze sieci, takie jak adresy serwerów DHCP, DNS, Proxy itd.

Sieci bezprzewodowe. Program Network Stumbler

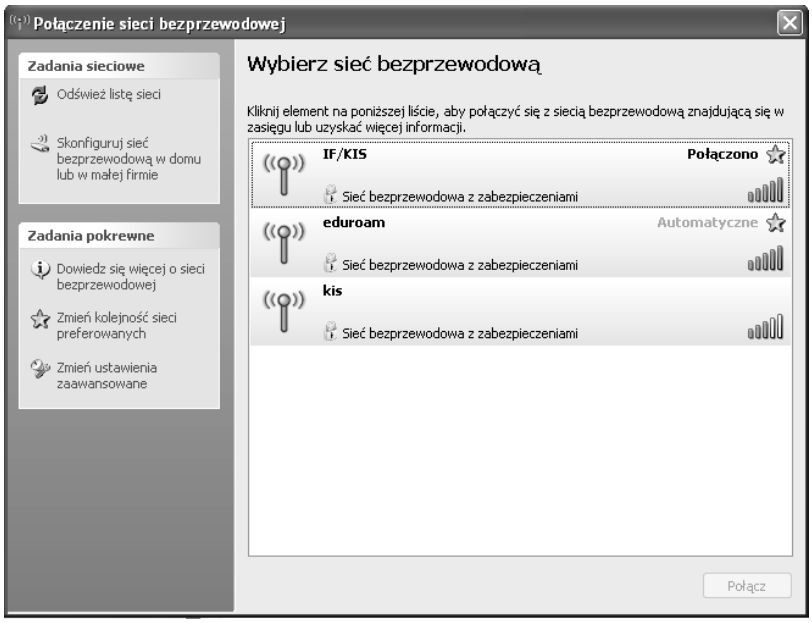
Od pewnego czasu można zaobserwować coraz większą popularność sieci bezprzewodowych. Technologia bezprzewodowa ewoluowała i oferuje obecnie bardzo dobrą jakość połączenia i dużą niezawodność. Prostota tworzenia sieci bezprzewodowej, którą zapewniają dostępne na rynku gotowe rozwiązania (Access Point), sprawia, że coraz więcej użytkowników indywidualnych, jak również instytucji i firm, decyduje się na ten rodzaj łączności.

Jeżeli nasz komputer ma wbudowaną bezprzewodową kartę sieciową, możliwe jest przyłączenie się do sieci bezprzewodowej (np. osiedlowej). Aby sprawdzić dostępne sieci, w systemie Windows klikamy prawym przyciskiem myszy *Połączenia sieciowe* i wybieramy *Właściwości*. Następnie w otwartym oknie *Połączenia sieciowe* klikamy prawym przyciskiem myszy ikonę sieci bezprzewodowej. Z otwartego menu kontekstowego wybieramy opcję *Wyświetl dostępne sieci bezprzewodowe* (rysunek 4.7). Wyświetlą się wówczas wszystkie dostępne sieci komputerowe, w których zasięgu znajduje się nasz komputer. Po prawej stronie wyświetlona jest moc sygnału (pionowe zielone kreski). Jeżeli przy nazwie sieci widnieje ikona kłódki, wówczas sieć jest zabezpieczona.

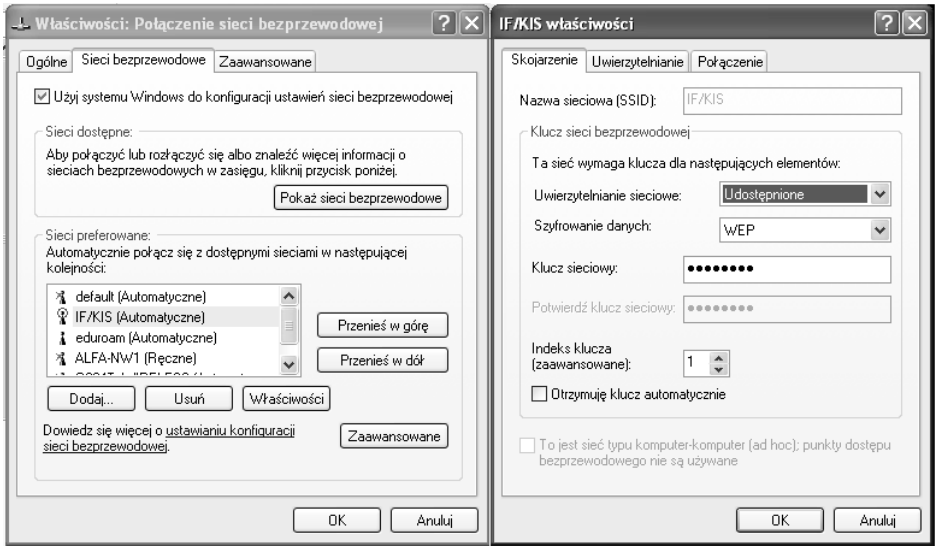
Tabela 4.1. *Opcje skanowania systemu dla narzędzia Diagnostyka sieci systemu Windows*

Opcja	Komentarz
Ping	Testowanie połączenia za pomocą komendy ping (zob. podrozdział „Testowanie połączenia. Polecenie Ping")
Połącz	Próba nawiązania połączenia w celu sprawdzenia, czy dana usługa sieciowa jest dostępna
Pokaż	Zbiera podstawowe informacje na dany temat
Informacja pełna	Zbiera zaawansowane informacje na dany temat
Zapis na pulpicie	Zapisuje na pulpicie plik z danymi dotyczącymi skanowania
Usługa pocztowa	Wyświetla nazwę serwera poczty przychodzącej i wychodzącej oraz port, na którym następuje połączenie. Sprawdzanie jest wykonywane za pomocą poleceń `ping` i `połącz`. Działa jedynie dla programu Outlook
Usługa grup dyskusyjnych	Wyświetla nazwę serwera grup dyskusyjnych. Sprawdzanie jest przeprowadzane za pomocą poleceń `ping` i `połącz`. Działa jedynie dla programu Outlook
Internetowy serwer proxy	Wyświetla nazwę i numer portu serwera proxy programu Internet Explorer. Sprawdzanie jest przeprowadzane za pomocą poleceń ping i połącz
Informacje o komputerze	Wyświetla informacje o komputerze
System operacyjny	Wyświetla informacje o systemie operacyjnym
Wersja systemu Windows	Sprawdza wersję systemu Windows
Modemy	Wyświetla listę wszystkich modemów
Klienty sieci	Lista wszystkich klientów sieci
Karty sieciowe	Lista wszystkich kart sieciowych zainstalowanych w komputerze
System DNS (*Domain Name System*)	Wyświetla serwery DNS dla każdej karty sieciowej
Protokół DHCP (*DynamicHost Configuration Protocol*)	Wyświetla serwery DHCP dla każdej karty sieciowej
Bramy domyślne	Wyświetla bramy sieciowe (ang. *gateway*) dla każdej karty sieciowej
Adres IP	Sprawdza adres IP komputera
Usługa WINS (*Windows Internet Naming Service*)	Wyświetla serwery WINS dla każdej karty sieciowej

Przyłączenie do takiej sieci następuje po uprzednim podaniu klucza sieciowego. W tym celu klikamy prawym przyciskiem myszy *Połączenia sieciowe*, wybieramy *Właściwości*, a następnie w otwartym oknie klikamy prawym przyciskiem ikonę sieci bezprzewodowej. Wybieramy opcję *Właściwości*. Otworzy się okno *Właściwości: Połączenie sieci bezprzewodowej* (rysunek 4.8, lewy). Przechodzimy do zakładki *Sieci bezprzewodowe*. Opcja *Użyj systemu Windows do konfiguracji ustawień sieci bezprzewodowej* powinna być włączona. Z tego okna możemy również wyświetlić dostępne sieci bezprzewodowe, klikając przycisk *Pokaż sieci bezprzewodowe*. W panelu *Sieci preferowane* mamy dostępną listę sieci. Zaznaczamy nazwę interesującej nas sieci i klikamy przycisk *Właściwości*.



Rysunek 4.7. *Okno Połączenia sieci bezprzewodowej, z dostępnymi sieciami*

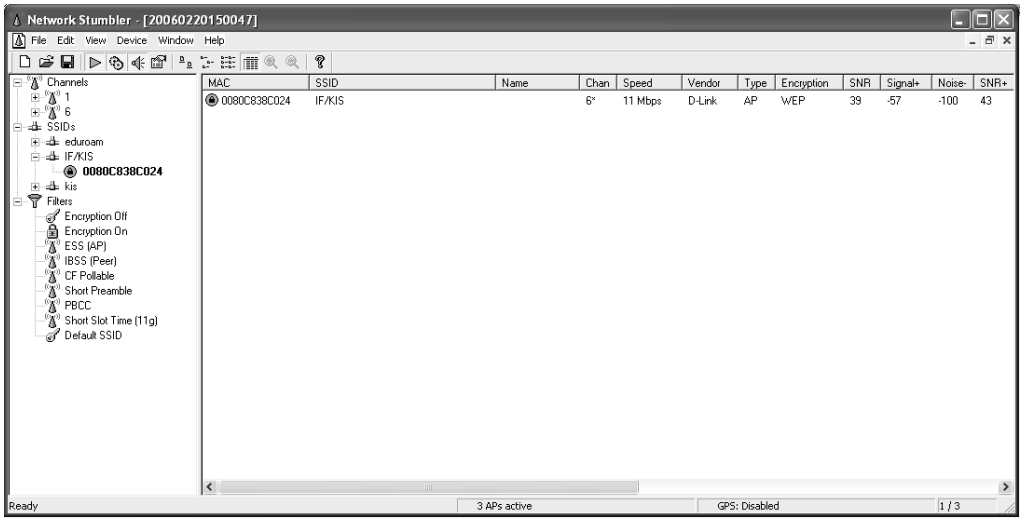


Rysunek 4.8. *Ustawianie właściwości sieci bezprzewodowej*

Otworzy się okno właściwości wybranej sieci (rysunek 4.8, prawy). Musimy ustawić typ uwierzytelniania sieciowego i szyfrowania danych oraz podać klucz sieciowy. Zwykle do szyfrowania danych używa się standardu WEP (ang. *Wired Equivalent Privacy*). Możliwe jest również wybranie opcji *Otrzymuję klucz automatycznie*. Informacje te uzyskamy, kontaktując się z administratorem sieci. Jeżeli uruchomiliśmy sieć otwartą, bez zabezpieczeń, wówczas opcję *Uwierzytelnienie sieciowe* ustawiamy na *Otwarte*. Jest

to dosyć niebezpieczne, ponieważ każdy, kto jest w zasięgu naszej sieci, może się do niej przyłączyć. Jeśli jednak mamy słabą antenę, która pokrywa dobrze jedynie mieszkanie, oraz potencjalnie dużo osób, które chciałyby od czasu do czasu korzystać z naszej sieci, możemy pozostawić sieć otwartą. Sieć może być również nieszyfrowana, jednak dostęp do niej możliwy będzie tylko po uprzednim zalogowaniu się. Po podłączeniu się do sieci i włączeniu przeglądarki WWW wyświetli się ekran, na którym należy podać identyfikator użytkownika i hasło.

Bardzo dobrym narzędziem do diagnostyki sieci bezprzewodowej jest darmowy program Network Stumbler (*http://www.netstumbler.com/*). Dzięki niemu w łatwy sposób możemy sprawdzić dostępne sieci bezprzewodowe. Wyświetlane są szczegółowe informacje na temat każdej znalezionej sieci (rysunek 4.9).



Rysunek 4.9. *Program Network Stumbler w wersji 0.4.0*

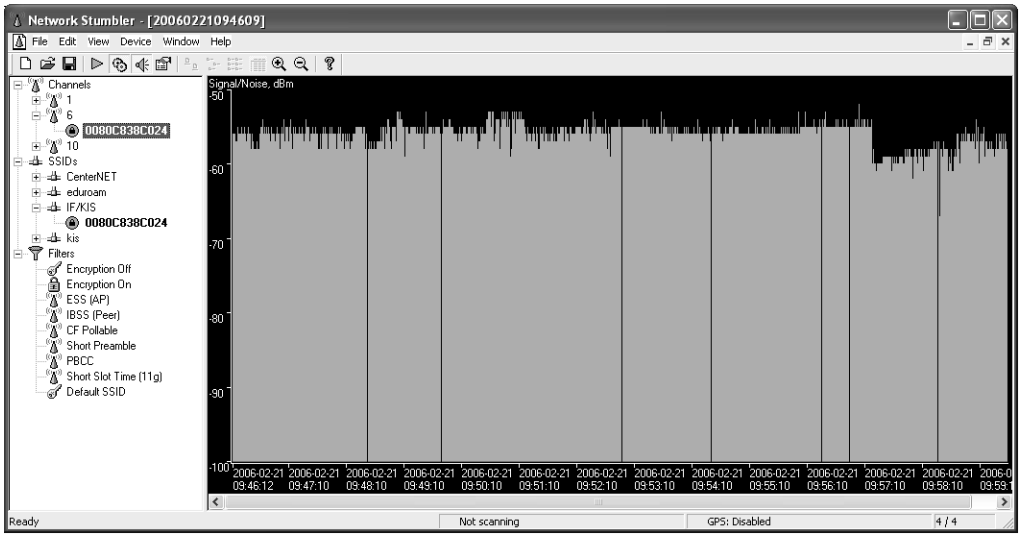
Ekran aplikacji składa się z dwóch paneli. W lewym panelu wyświetlane są dostępne opcje, natomiast w prawym szczegółowe informacje na temat wybranej opcji. Lewy panel zbudowany jest na zasadzie drzewa. Pierwszym węzłem jest *Channels*. Jest to lista kanałów, na których działają wszystkie znalezione sieci bezprzewodowe. Jeżeli sieci znajdują się blisko siebie, wtedy lepiej ustawić punkty dostępowe (*access point* — AP) tak, aby działały na różnych kanałach. W ten sposób unikniemy wzajemnego zakłócania się. Lista *Channels* posortowana jest wg kanałów. Możemy zatem sprawdzić, na którym kanale działa interesująca nas sieć. Rozwijając węzeł z numerem kanału, dostajemy listę sieci aktualnie działających na tym kanale oraz adres MAC punktu dostępowego danej sieci. Zaznaczając interesujący nas kanał w prawym panelu, dostaniemy informacje szczegółowe. Tabela 4.2 zawiera spis wszystkich kolumn wraz z ich opisem.

Klikając w lewym panelu adres MAC sieci bezprzewodowej, otrzymamy wykres natężenia sygnału do zakłóceń w funkcji czasu. Jest to niezwykle przydatne narzędzie do planowania rozmieszczenia punktów dostępowych sieci oraz rozmieszczenia komputerów i ustawienia anten odbiorczych dla sieci bezprzewodowych. Zielone słupki oznaczają

Tabela 4.2. *Dostępne informacje szczegółowe dotyczące sieci bezprzewodowej*

Kolumna	Opis
MAC	Adres MAC dla punktu dostępowego (AP) sieci bezprzewodowej
SSID	Ang. *Service Set IDentifier*, czyli identyfikator sieciowy
Name	Nazwa urządzenia AP
Chan	Kanał, na którym działa AP. Jeżeli przy liczbie występuje symbol *, oznacza to, że jesteśmy do tej sieci przyłączeni
Speed	Maksymalna odnotowana przepustowość do punktu dostępowego (Mbps — megabitów na sekundę). Nie jest to przepustowość naszego połączenia z internetem, a jedynie połączenia z AP (zob. podrozdział „Przepustowość sieci")
Vendor	Producent AP. Nazwę uzyskuje się z adresu MAC (zob. podrozdział „Sprawdzanie konfiguracji sieci. Adres IP")
Type	Typ urządzenia sieciowego. Możliwe są dwie wartości tego parametru: AP — Access Point. Połączenie w schemacie gwiazdy, z centralnym węzłem w postaci punktu dostępowego. Wszystkie komputery w sieci łączą się z AP i przez niego uzyskują dostęp do innych komputerów oraz internetu Peer — połączenie typu peer-to-peer. Jest to połączenie bez centralnego punktu. Komputery łączą się bezpośrednio ze sobą
Encryption	Szyfrowanie danych. Jeżeli jest włączone, pojawi się napis WEP, bez względu na to, jaki typ szyfrowania jest używany
SNR	Aktualny stosunek sygnału do zakłóceń (ang. *Signal to Noise Ratio*). Zwykle podawany w dB
Signal+	Najwyższe zanotowane natężenie sygnału
Noise–	Najniższe zanotowane natężenie zakłóceń
SNR+	Najwyższy zanotowany stosunek SNR
IP, Subnet	Konfiguracja IP urządzenia. Jest wyświetlana jedynie wtedy, gdy jest dostępna
Latitude, Longitude, Distance	Wartości podawane jedynie wtedy, gdy używamy odbiornika GPS (ang. *Global Positioning System*). Na ich podstawie możliwe jest ustalenie położenia GPS (*latitude* — szerokość geograficzna, *longitude* — długość geograficzna, *distance* — odległość między satelitą a odbiornikiem GPS)
First Seen	Czas, kiedy obiekt na liście (AP lub Peer) był widziany po raz pierwszy
Last Seen	Czas ostatniego kontaktu
Signal	Aktualne natężenie sygnału (dB)
Noise	Aktualne natężenie zakłóceń (dB)
Flags	Aktualnie podniesiona flaga dla standardu 802.11. Kody flag nie będą tutaj opisywane. Zainteresowanych odsyłamy do internetu
Beacon	Czas pomiędzy sygnałami identyfikacyjnymi w milisekundach. Domyślną wartością jest 100

natężenie sygnału, natomiast czerwone to natężenie zakłóceń. Różnica pomiędzy słupkiem czerwonym a zielonym to stosunek sygnału do zakłóceń. Niektóre urządzenia sieciowe nie mają możliwości wyświetlania natężenia zakłóceń. W takim przypadku wyświetlana jest jedynie moc sygnału (rysunek 4.10). Pomiędzy wartością –70 a –80 jakość sygnału jest niska i w większości zastosowań nie zapewnia dobrych rezultatów.



Rysunek 4.10. *Mierzenie natężenia sygnału do zakłóceń w funkcji czasu*

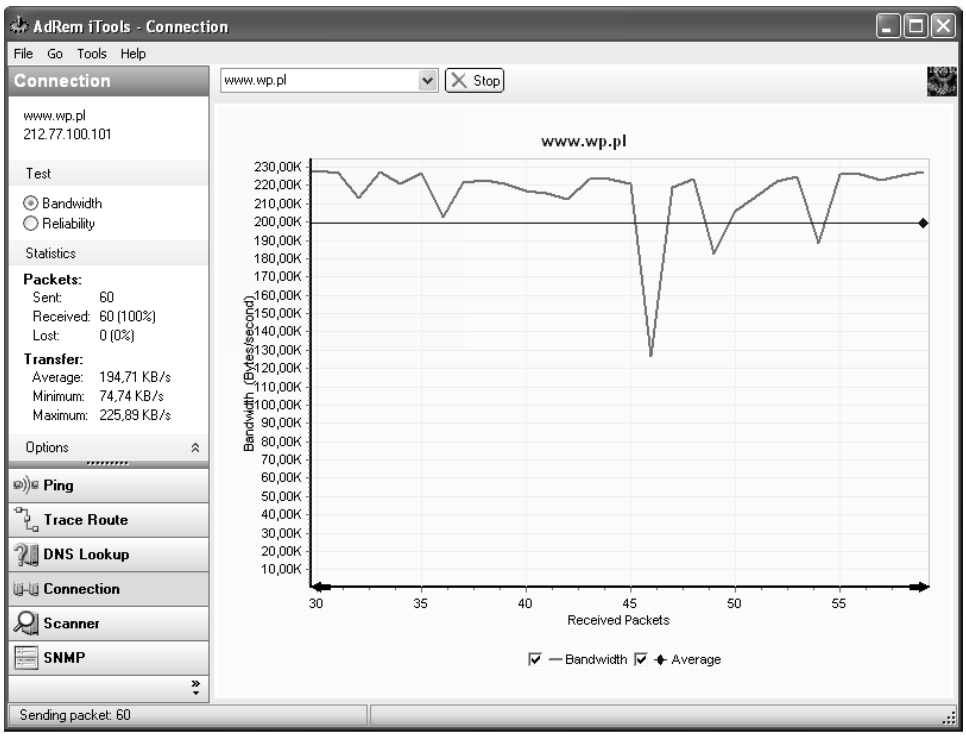
Powyżej wartości –70 jakość sygnału jest dobra. Bardzo dobra jakość sygnału rozpoczyna się od wartości ok. –60.

Kolejnym węzłem jest *SSIDs* Jest to lista zawierająca wszystkie identyfikatory sieciowe sieci bezprzewodowych, które są w naszym zasięgu. Rozwijając węzeł z nazwą sieci, dostaniemy adres MAC punktu dostępowego, a w prawym panelu wyświetlone zostaną informacje szczegółowe. Klikając ten adres, możemy uzyskać wykres jakości sygnału opisywany powyżej. Ostatni węzeł (*Filters*) to lista możliwych filtrów, które możemy stosować do wyświetlanych informacji. Z wyjątkiem dwóch pierwszych, filtry te przeznaczone są dla zaawansowanego użytkownika. Jeżeli wybierzemy filtr *Encrypting Off*, wówczas dostaniemy listę wszystkich sieci bezprzewodowych, w których szyfrowanie danych jest wyłączone. *Encrypting On* da nam listę sieci z włączonym szyfrowaniem połączeń. *ESS* (ang. *Extended Service Set*) to filtr, za pomocą którego otrzymamy listę sieci opartych na połączeniu typu AP. *IBSS* (ang. *Independent Basic Service Set* lub *peer to peer network*) da nam listę sieci, które połączone są bez udziału AP (czyli komputery połączone są bezpośrednio jedne do drugich). Za pomocą opcji *Short Preamblem* sprawdzimy, która z sieci posługuje się krótszym sygnałem synchronizacji, co w teorii zwiększa szybkość działania sieci. *CF Pollable* (ang. *Contention-free pollable*) to jeden ze standardów sieci bezprzewodowych. Filtr *Short Slot Time* sprawdza, czy w sieciach standardu 802.11g włączona jest opcja *Short Slot Time*, zwiększająca szybkość działania takiej sieci. *PBCC* (ang. *Packet Binary Convolutional Code*) to kolejny standard, tym razem dla sieci 802.11b+. Standard ten zmniejsza liczbę błędów przy przesyłaniu pakietów sieciowych.

Jak wynika z tego krótkiego opisu, program Network Stumbler jest bardzo pożytecznym narzędziem umożliwiającym diagnostykę sieci bezprzewodowej. Za jego pomocą można ustawić lokalną sieć optymalnie. Sprawdzić, czy cały interesujący nas obszar jest pokryty. Badając natężenie sygnału sieci, można również wybrać sieć bezprzewodową (dostawcę usług internetowych).

Przepustowość sieci. Program AdRem iTools

Ważną cechą każdej sieci komputerowej jest jej przepustowość. Wysoka przepustowość sieci gwarantuje nam szybkie działanie internetu oraz innych usług sieciowych. Zwykle jej wartość podawana jest w bajtach na sekundę. W internecie można znaleźć wiele programów służących do badania przepustowości sieci. Bardzo wygodnym narzędziem jest program AdRem iTools (*http://www.adremsoft.com/itools/index.php*). Ma wiele opcji, nas jednak interesuje szczególnie opcja *Connection*. Za jej pomocą możemy wyznaczyć wartość przepustowości połączenia z dowolnym komputerem. W lewym panelu klikamy opcję *Connection*. W górnym menu wpisujemy adres bądź nazwę interesującego nas komputera i klikamy przycisk *Run*. Naszym oczom ukaże się wykres przepustowości w bajtach na sekundę w zależności od czasu (rysunek 4.11). Liczona będzie wartość średnia (*Average*), maksymalna (*Maximum*) i minimalna (*Minimum*). Dodatkowo podawana jest statystyka pakietów: liczba wysłanych (*Sent*), odebranych (*Received*) i utraconych (*Lost*). Zadowalająca wartość przepustowości zależy od tego, co chcemy osiągnąć. I tak do oglądania stron internetowych wystarczająca przepustowość to ok. 64 kb/s. Jeżeli przez sieć przesyłamy duże pliki, wówczas połączenie 1 Mb/s może okazać się niewystarczające. Narzędziem tym możemy sprawdzić, czy deklarowana przez naszego dostawcę usług internetowych szybkość połączeń jest prawdziwa.



Rysunek 4.11. *Sprawdzanie przepustowości sieci za pomocą programu AdRem Itools*

Inne dostępne opcje to test połączenia przy użyciu metody ping, sprawdzenie drogi do danego komputera w sieci za pomocą *Trace Route* (wypisywane są adresy IP wszystkich

aktywnych urządzeń na drodze pakietu), *DNS Lookup* (zamiana adresu IP na nazwę DNS i odwrotnie) i skaner portów.

W systemie Windows po najechaniu kursorem myszy na ikonę sieci w pasku zasobnika systemowego (*tray*) ukaże nam się „chmurka" z kilkoma danymi dotyczącymi sieci. Będzie tam m.in. podana Szybkość. Podobne informacje można również uzyskać, klikając prawym przyciskiem myszy Połączenia sieciowe, wybierając Właściwości, a następnie klikając prawym przyciskiem połączenie sieciowe i wybierając Stan. Nie jest to jednak szybkość połączenia z innymi komputerami w sieci lub z internetem. Jest to szybkość połączenia do najbliższego aktywnego urządzenia sieciowego.

Lista otwartych portów. Program A-Squared

Adresem naszego komputera w sieci jest numer IP. Na ten adres kierowane są pakiety. Aby system wiedział, do której aplikacji kierowany jest dany pakiet, potrzebna jest identyfikacja wszystkich procesów sieciowych. Służą do tego tzw. porty. Każda aplikacja używająca połączenia sieciowego otwiera własny port. Każdy port ma swój numer. Porty mogą służyć do identyfikacji procesów działających w odległych systemach. Niektóre numery portów są ogólnie znane i zarezerwowane dla odpowiednich usług (porty o numerach od 0 do 1023). Na przykład, jeżeli dana maszyna w sieci ma otwarty port o numerze 80, wiemy, że udostępnia usługę HTTP. Jedna aplikacja może otwierać kilka portów jednocześnie (np. FTP). Numery portów przydzielane są przez organizację IANA (ang. *Internet Assigned Number Authority*). Aktualna lista zarezerwowanych portów znajduje się na stronie *http://www.iana.org/assignments/port-numbers*.

Oto lista niektórych portów wraz z przyporządkowanymi do nich usługami:

- 20 — FTP dane;
- 21 — FTP polecenia;
- 22 — SSH;
- 23 — Telnet;
- 25 — SMTP;
- 53 — DNS;
- 70 — Gopher;
- 80 — HTTP;
- 109 — POP2;
- 110 — POP3;
- 119 — NNTP;
- 143 — IMAP;
- 161 — SNMP;
- 162 — SNMP — komunikaty Trap;

- 443 — HTTPS;
- 995 — POP3S (POP3 z użyciem SSL);
- 3389 — Pulpit zdalny sytemu Windows.

Ważne jest, aby wiedzieć, które aplikacje w naszym systemie używają połączeń sieciowych oraz jakie porty są otwarte. Im więcej otwartych portów, tym łatwiej zaatakować nasz system. W sieci dostępnych jest wiele programów skanujących porty — najbardziej znany to NMAP (*http://www.insecure.org/nmap/*). Jest to potężne narzędzie przeznaczone przede wszystkim dla administratorów systemów. My zajmiemy się programem o nazwie A-Squared Free (*http://www.emsisoft.com/en/software/free/*). Został on stworzony głównie do skanowania systemu w celu poszukiwania internetowych robaków, programów typu koń trojański, aplikacji szpiegowskich i tzw. dialerów, czyli programów niebezpiecznych szczególnie dla użytkowników łącz modemowych. Zawiera on również opcję skanowania otwartych portów. Sam program jest darmowy i po wypełnieniu krótkiej ankiety można go pobrać ze strony producenta. Z menu głównego programu wybieramy opcję *Sprawdź swój komputer za pomocą narzędzi kontrolnych*. Wyświetli się okno (tym razem niestety niespolszczone) *a-squared HiJackFree v1* z szeregiem opcji, za pomocą których możemy skontrolować nasz system (patrz rysunek 4.12). Z lewego panelu wybieramy opcję *Open Ports*. W prawym panelu wyświetli się lista wszystkich procesów (kolumna *Procesess*), które korzystają z połączenia sieciowego. Podany jest również numer identyfikacyjny procesu (*ProcessID*), numer otwartego portu (*Port*) oraz protokół sieciowy użyty do połączenia (*Proto*). Klikając myszą nazwę danego procesu, możemy uzyskać kilka dodatkowych informacji, które umieszczone zostaną w dolnym panelu *File Details*. Jeżeli na liście znajdują się programy, których nie instalowaliśmy (oprócz procesów systemowych), możemy podejrzewać, że w naszym systemie działają niepożądane aplikacje.

Więcej informacji w internecie

http://free.grisoft.com/ — darmowy program antywirusowy AVG Free.

http://www.free-av.com/ — darmowy program antywirusowy AntiVir

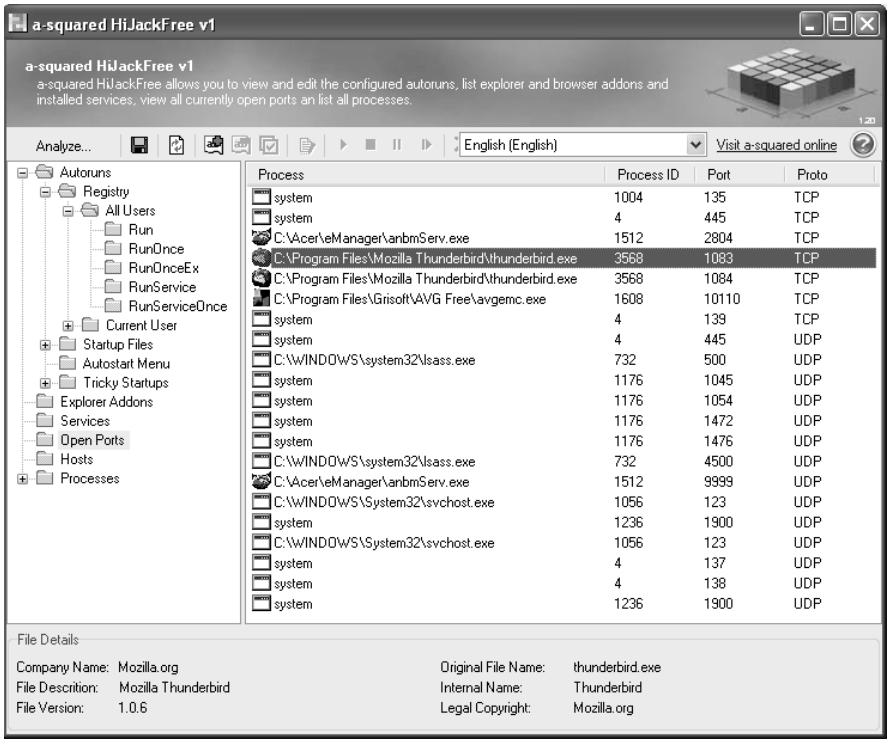
http://www.avast.com/ — darmowy program antywirusowy Avast! Home Edition

http://www.mks.com.pl/skaner/ — skaner wirusowy online

http://www.zonelabs.com/ — darmowa zapora sieciowa ZoneAlarm

http://www.lavasoftusa.com/software/adaware/ — darmowy program Ad-Aware wyszukujący w systemie robaki internetowe, aplikacje szpiegowskie i programy typu koń trojański

http://www.emsisoft.com/en/software/free/ — podobny do poprzedniego, jednak znacznie bardziej rozbudowany program A-Square, przeznaczony do wyszukiwania robaków internetowych, koni trojańskich, dialerów oraz



Rysunek 4.12. *Skanowanie portów za pomocą programu A-Squared*

programów szpiegowskich. Umożliwia uruchomienie w tle programu, który chroni system przed atakami tego typu oprogramowania, i umożliwia skanowanie otwartych portów.

http://www.netstumbler.com/ — program diagnostyczny NetStumbler dla sieci bezprzewodowych

http://www.adremsoft.com/itools/index.php — program służący do diagnostyki sieci

http://www.insecure.org/nmap/ — potężne narzędzie służące do skanowania portów