Bezpieczeństwo
Sieci Komputerowych

Część 7.
Przegląd narzędzi sieciowych

Praktyczny Pedagog

Bezpieczeństwo Systemów Komputerowych

PROGRAM ZAJĘĆ

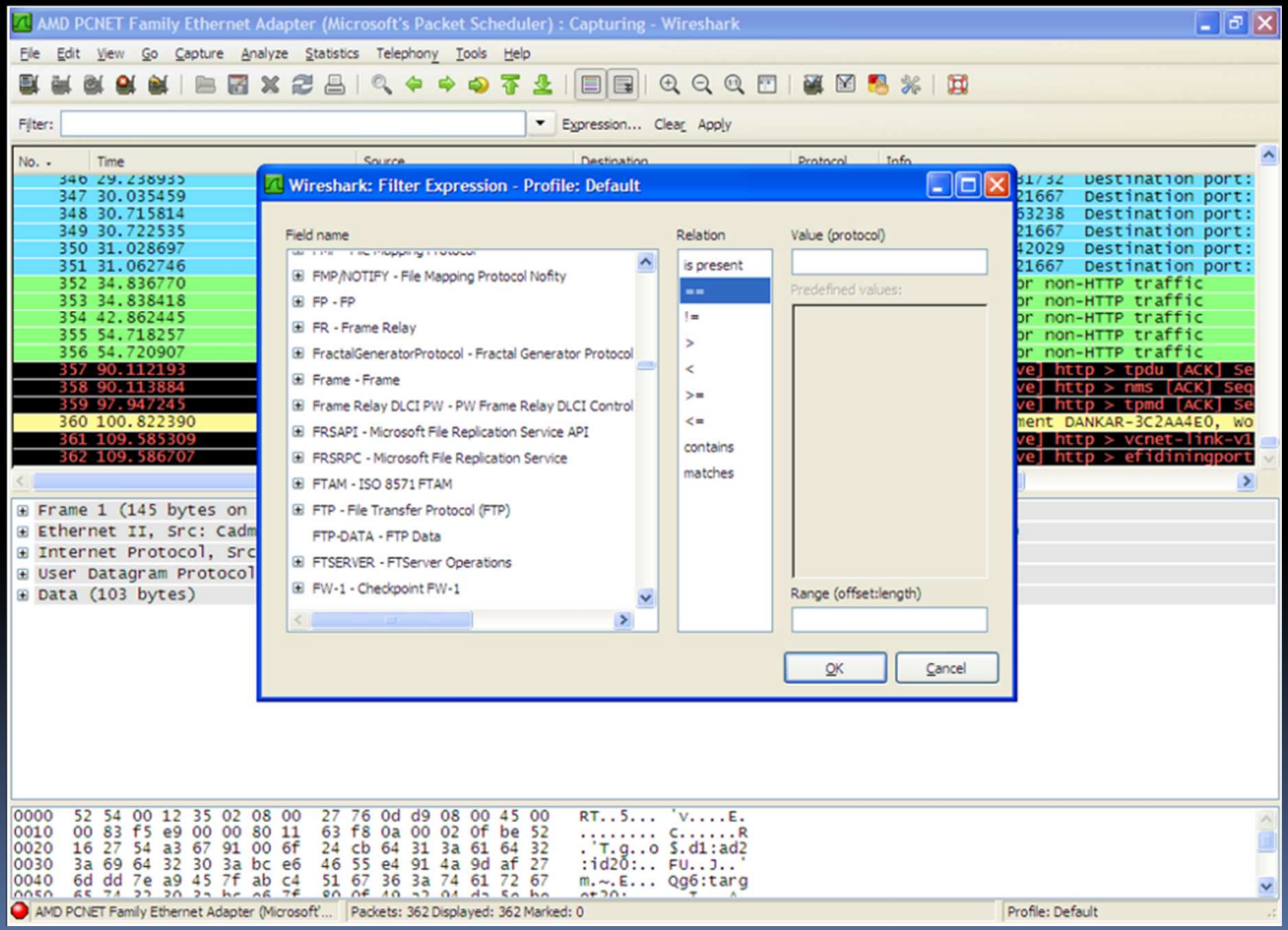
Przegląd narzędzi sieciowych:

- Wireshark,
- Nmap,
- BlueSweep,
- Hamachi,
- Comodo Unite ,
- TOR
- Hotspot Shield
- inSSIDer

Wireshark

Wireshark jest snifferem, pozwala na przełączenie karty sieciowej w tryb promiscous, dzięki któremu odbiera ona cały ruch w sieci i umożliwia jego analizę. Wygodny graficzny interfejs daje możliwość rozbudowanego filtrowania i sortowania odebranych danych. Wireshark jest dostępny w wersjach dla Windows, Linuksa, Solarisa i BSD.

Wireshark

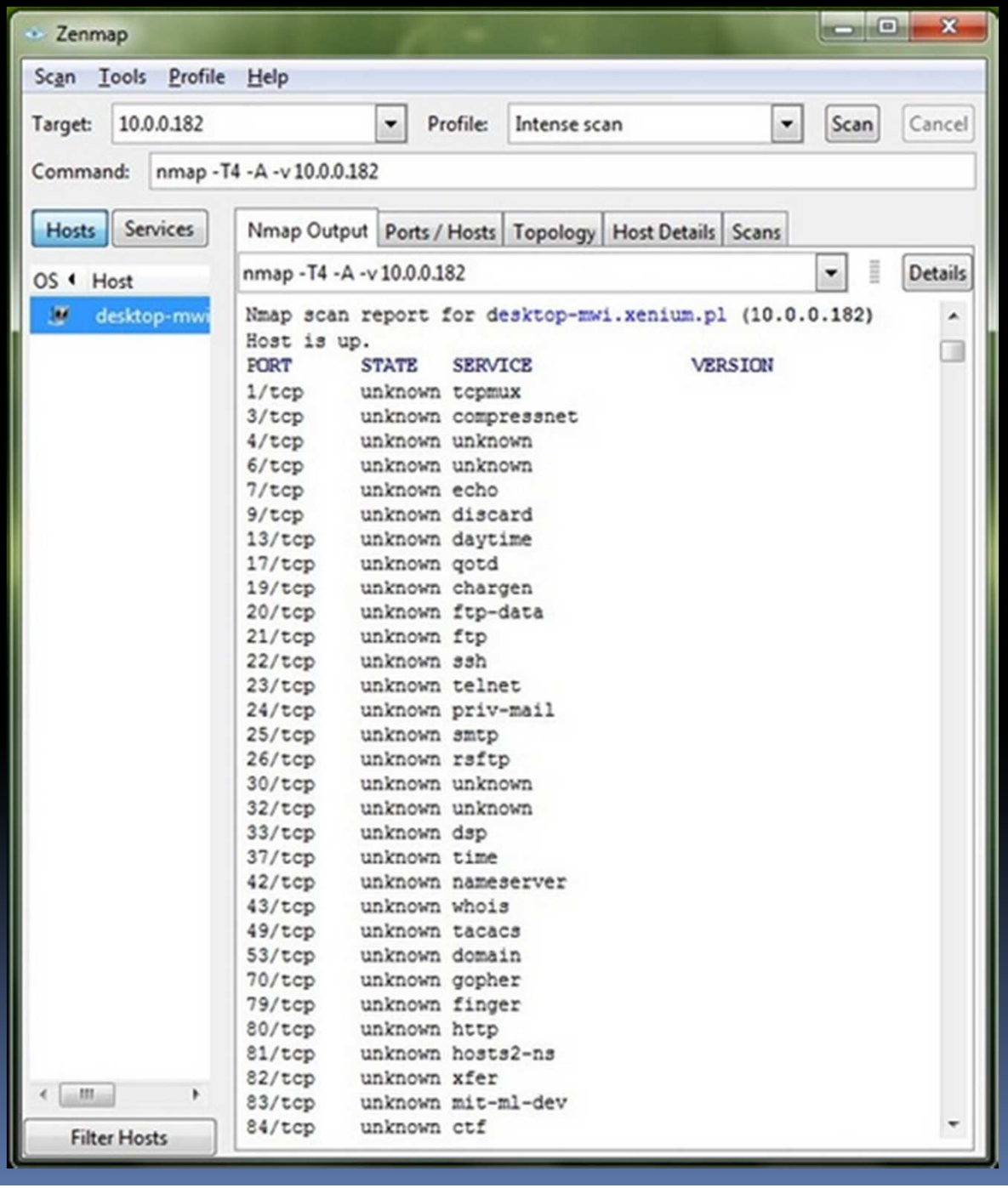

AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
346 29.238935
347 30.035459
348 30.715814
349 30.722535
350 31.028697
351 31.062746
352 34.836770
353 34.838418
354 42.862445
355 54.718257
356 54.720907
357 90.112193
358 90.113884
359 97.947245
360 100.822390
361 109.585309
362 109.586707
Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (protocol)
is present
==
!=
>
<
>=
<=
contains
matches
Predefined values:
Range (offset:length)
FMP/NOTIFY - File Mapping Protocol Nofity
FP - FP
FR - Frame Relay
FractalGeneratorProtocol - Fractal Generator Protocol
Frame - Frame
Frame Relay DLCI PW - PW Frame Relay DLCI Control
FRSAPI - Microsoft File Replication Service API
FRSRPC - Microsoft File Replication Service
FTAM - ISO 8571 FTAM
FTP - File Transfer Protocol (FTP)
FTP-DATA - FTP Data
FTSERVER - FTServer Operations
FW-1 - Checkpoint FW-1
OK
Cancel
Frame 1 (145 bytes on
Ethernet II, Src: Cadm
Internet Protocol, Src
User Datagram Protocol
Data (103 bytes)
0000 52 54 00 12 35 02 08 00 27 76 0d d9 08 00 45 00 RT..5... 'v....E.
0010 00 83 f5 e9 00 00 80 11 63 f8 0a 00 02 0f be 52 .... c......R
0020 16 27 54 a3 67 91 00 6f 24 cb 64 31 3a 61 64 32 .'T.g..o $.d1:ad2
0030 3a 69 64 32 30 3a bc e6 46 55 e4 91 4a 9d af 27 :id20:.. FU..J..'
0040 6d dd 7e a9 45 7f ab c4 51 67 36 3a 74 61 72 67 m.~.E... Qg6:targ
AMD PCNET Family Ethernet Adapter (Microsoft'...
Packets: 362 Displayed: 362 Marked: 0
Profile: Default

Nmap

Nmap to bezpłatne narzędzie do eksploracji sieci i przeprowadzania audytów bezpieczeństwa.

Aplikacja wykorzystuje niskopoziomowe pakiety IP w celu ustalenia dostępnych w sieci hostów, pracujących usług i pod kontrolą jakich systemów operacyjnych, a także rodzaju zapór ogniowych. Program oferuje wiele różnych technik skanowania portów, w tym TCP SYN, TCP connect(), UDP, TCP ACK, TCP Window, TCP Maimon, TCP Null, FIN i Xmas, TCP ze zdefiniowanymi flagami, Idle, protokołów IP, FTP bounce, a stan każdej z usług oceniany może być przy pomocy jednego ze statusów. Dodatkowym atutem Nmap jest możliwość inwentaryzacji sieci, zarządzania harmonogramami aktualizacji oraz monitorowanie hostów i czasu usług.

Nmap


Zenmap
Scan Tools Profile Help
Target: 10.0.0.182
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 10.0.0.182
Hosts
Services
OS Host
desktop-mwi
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 10.0.0.182
Details
Nmap scan report for desktop-mwi.xenium.pl (10.0.0.182)
Host is up.
PORT STATE SERVICE VERSION
1/tcp unknown tcpmux
3/tcp unknown compressnet
4/tcp unknown unknown
6/tcp unknown unknown
7/tcp unknown echo
9/tcp unknown discard
13/tcp unknown daytime
17/tcp unknown qotd
19/tcp unknown chargen
20/tcp unknown ftp-data
21/tcp unknown ftp
22/tcp unknown ssh
23/tcp unknown telnet
24/tcp unknown priv-mail
25/tcp unknown smtp
26/tcp unknown rsftp
30/tcp unknown unknown
32/tcp unknown unknown
33/tcp unknown dsp
37/tcp unknown time
42/tcp unknown nameserver
43/tcp unknown whois
49/tcp unknown tacacs
53/tcp unknown domain
70/tcp unknown gopher
79/tcp unknown finger
80/tcp unknown http
81/tcp unknown hosts2-ns
82/tcp unknown xfer
83/tcp unknown mit-ml-dev
84/tcp unknown ctf

BlueSweep

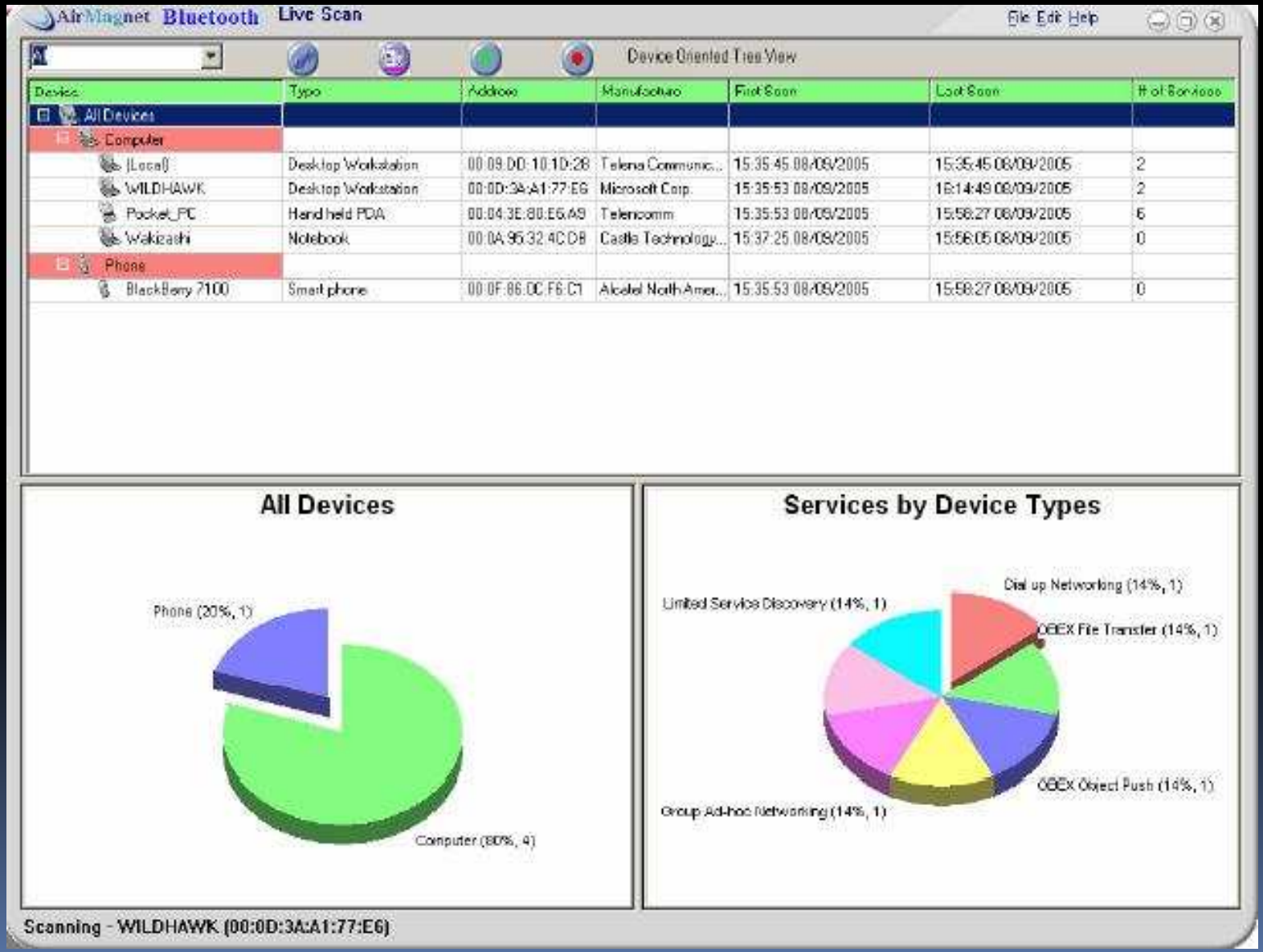
Prosty, bezpłatny skaner urządzeń wykorzystujących sieć Bluetooth.

Za pomocą programu BlueSweep z łatwością wykryjesz wszystkie urządzenia w okolicy, zdolne do komunikacji za pomocą protokołu Bluetooth. Do podstawowych funkcji tego darmowego narzędzia można zaliczyć:
Wykrywanie i identyfikacja każdego urządzenia Bluetooth znajdującego się w zasięgu komputera z uruchomionym skanerem
Wyświetlanie aktywnych połączeń Bluetooth pomiędzy wykrytymi urządzeniami
Wyświetlanie wszystkich usług Bluetooth, które można uzyskać na każdym urządzeniu wykrytym w zasięgu.

Jest to szczególnie istotne w obliczu pojawiających się wirusów rozprzestrzenianych przy pomocy technologii Bluetooth. Przykładem takiego wirusa może być robak Cabir, działający w środowisku Symbian OS głównie w telefonach komórkowych posiadających możliwość transmisji Bluetooth.

Uwaga! Program wymaga do działania aktywnego interfejsu Bluetooth na komputerze na którym jest uruchomiony.

BlueSweep


AirMagnet Bluetooth Live Scan
File Edit Help
Device Oriented Tree View
Device
Type
Address
Manufacturer
First Seen
Last Seen
# of Services
All Devices
Computer
(Local)
Desktop Workstation
00:09:DD:10:1D:28
Telena Communic...
15:35:45 08/09/2005
15:35:45 08/09/2005
2
WILDHAWK
Desktop Workstation
00:0D:3A:A1:77:E6
Microsoft Corp.
15:35:53 08/09/2005
16:14:49 08/09/2005
2
Pocket_PC
Handheld PDA
00:04:3E:80:E6:A9
Telencomm
15:35:53 08/09/2005
15:58:27 08/09/2005
6
Wakizashi
Notebook
00:0A:95:32:4C:D8
Casita Technology...
15:37:25 08/09/2005
15:58:05 08/09/2005
0
Phone
BlackBerry 7100
Smart phone
00:0F:86:0C:F6:C1
Alcatel North Amer...
15:35:53 08/09/2005
15:58:27 08/09/2005
0
All Devices
Phone (20%, 1)
Computer (80%, 4)
Services by Device Types
Dial up Networking (14%, 1)
Limited Service Discovery (14%, 1)
OBEX File Transfer (14%, 1)
OBEX Object Push (14%, 1)
Group Ad-hoc Networking (14%, 1)
Scanning - WILDHAWK (00:0D:3A:A1:77:E6)

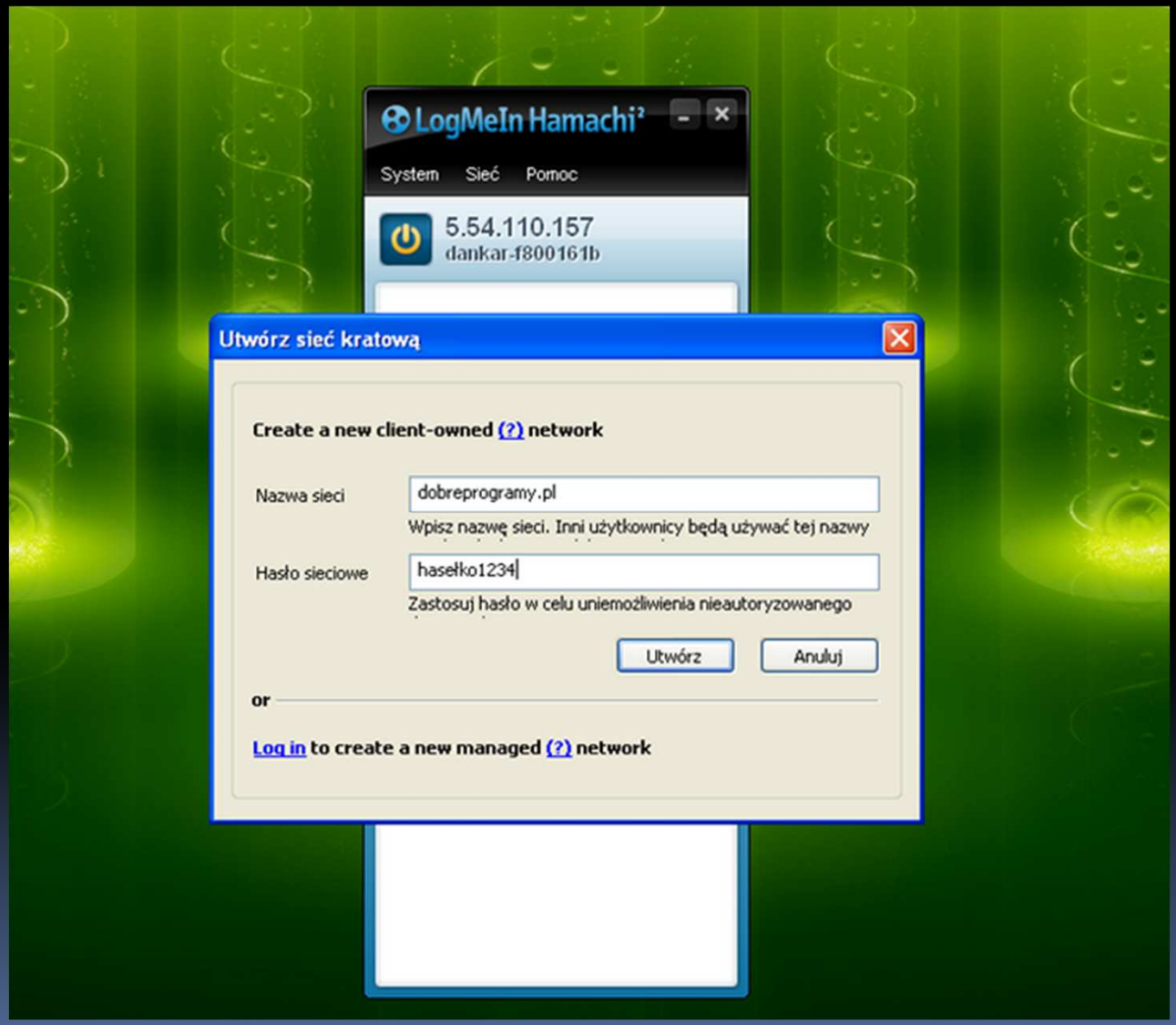
LogMeIn Hamachi

Najnowsza wersja bezpłatnego programu umożliwiającego skonfigurowanie połączeń VPN (Virtual Private Network) tworząc wirtualne sieci LAN.

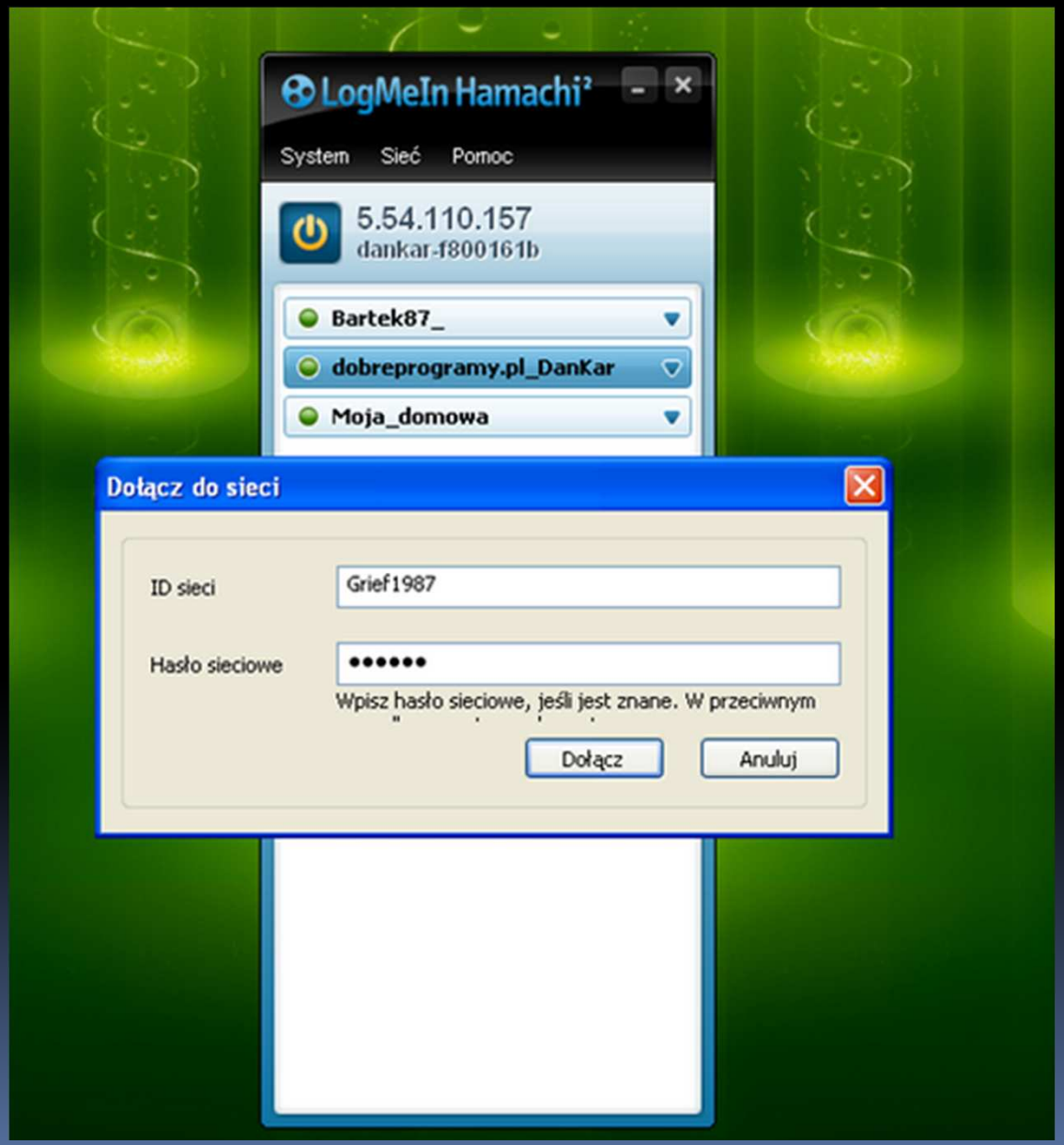
Połączenie nawiązane między dwoma komputerami jest możliwe nawet w przypadku gdy oba znajdują się za tzw. NAT-em. Wszystko to pozwala na bezpośrednie udostępnianie plików, pracę aplikacji sieciowych, gier, a nawet udostępnianie drukarek - słowem korzystanie z wszelkich możliwości jakie daje praca w sieci lokalnej. Hamachi sprawia, że adres prywatny adres IP działa jak publiczny.

Program jest bardzo prosty w obsłudze, a do jego konfiguracji wystarczy kilka kliknięć myszą.

LogMeIn Hamachi



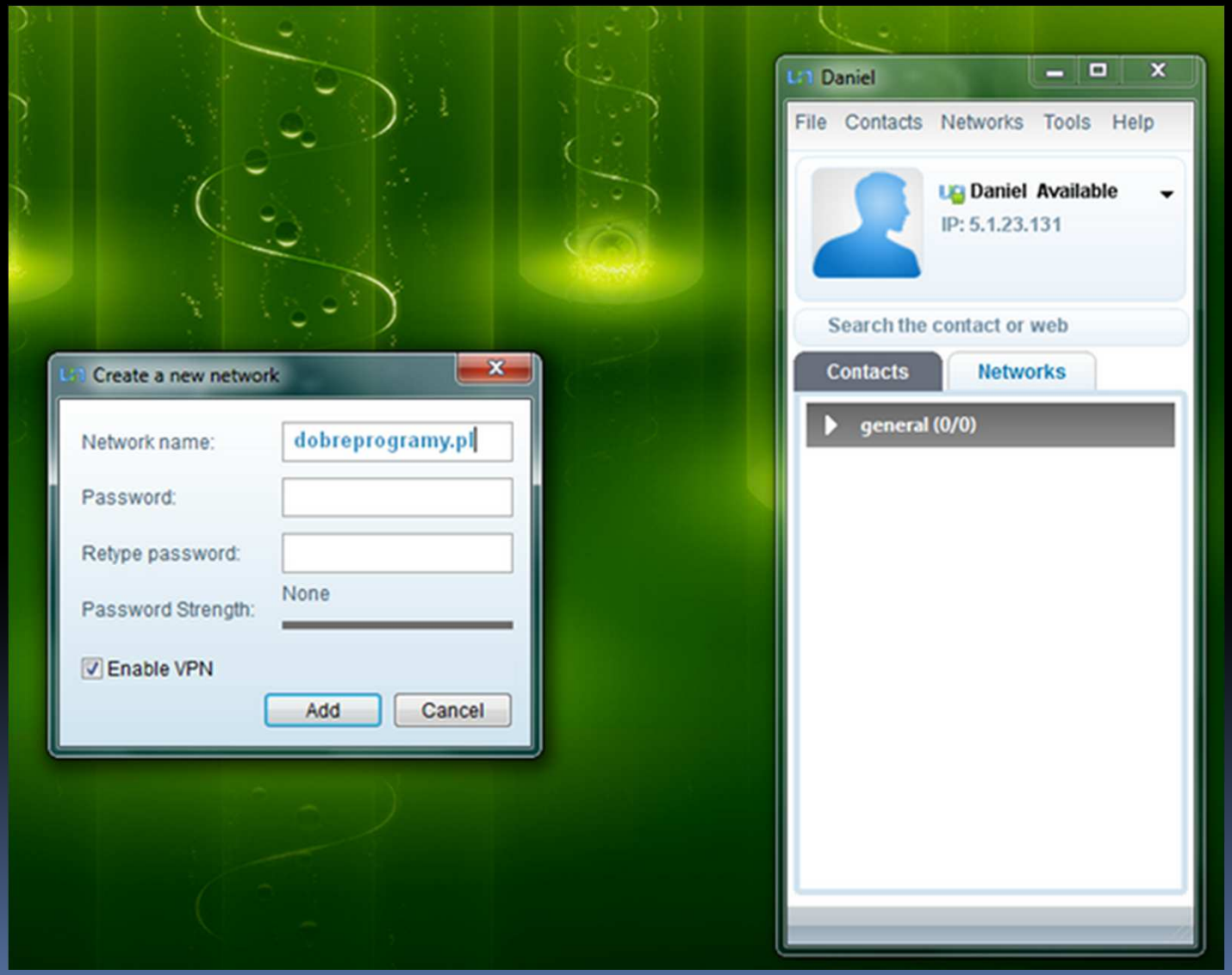
LogMeIn Hamachi



Comodo Unite

Comodo Unite (dawniej Comodo EasyVPN) to darmowa (do zastosowań prywatnych) i prosta w użyciu alternatywa dla popularnego na całym świecie Hamachi.
Do zadań programu należy tworzenie i konfigurowanie sieci VPN (Virtual Private Network), za pośrednictwem których możliwa jest komunikacja pomiędzy komputerami znajdującymi się za tzw. NAT-em. Comodo Unite posiada wbudowany komunikator tekstowy, a także szereg przydatnych opcji, dających możliwość wymiany wszelakiego rodzaju plikami i ustanawiania połączenia zdalnego pulpitu.
Wymiana danych pomiędzy użytkownikami programu odbywa się za pośrednictwem szyfrowanego kanału komunikacji (wykorzystywane są 128-bitowe algorytmy szyfrujące).

Comodo Unite



TOR

TOR (skrót od The Onion Router) to system mający na celu umożliwienie anonimowości online.

Klient Tora kieruje ruch do szlaków komunikacyjnych światowej sieci serwerów wolontariuszy w celu ukrycia lokalizacji użytkownika, a co za tym idzie utrudnienie działań mających na celu nadzór sieci lub analizę ruchu.

Korzystanie z Tora utrudnia śledzenie aktywności użytkownika w Internecie, w tym wizyt w witrynach sieci Web, wiadomości online, wiadomości błyskawicznych i innych form komunikacji.

TOR

Ma na celu ochronę danych osobowych użytkowników wolność, prywatność i możliwość prowadzenia poufnych transakcji. Onion Routing (trasowanie cebulowe) odnosi się do warstwowego charakteru usługi szyfrowania: oryginalne dane są szyfrowane wielokrotnie, a następnie przesyłane poprzez kolejne przekaźniki sieci Tor, z których każda odszyfrowuje "warstwę" szyfrowania przed przekazaniem danych do kolejnego wyjścia i w końcu do ostatecznego przeznaczenia. Zmniejsza to możliwość odkodowania oryginalnych danych lub ich przechwycenia w transporcie.

Nie jest to skuteczna, 100% ochrona prywatności. Jeżeli aplikacja wraz z przeglądarką internetową będą wykorzystywane w sposób niepoprawny (np. działać będą wtyczki Flash czy inne, które mogą bezpośrednio uderzać do serwera) łatwo można zostać zidentyfikowanym. Teoretycznie możliwe jest również za pomocą analizy statystycznej określenie czy jeden z węzłów sąsiadujących temu, na którym się przeprowadza badania nie jest odbiorcą ostatecznych konkretnych, przesyłanych treści. Ryzyko takiego działania wprawdzie jest niewielkie, ale trzeba sobie zdawać sprawę z tego, że istnieje.

Program jest wolnym oprogramowaniem i jest bezpłatny.

Instrukcja obsługi: http://wegax.blogspot.com/2010/09/anonimowosc-w-sieci-tor-dla-firefoxa.html
oraz http://www.kapitalizm.org/teksty/onion2/onion2.html

TOR


Panel Kontrolny Vidalii
Status
Połączony z siecią Tor!
Skróty Vidalii
Zatrzymaj Tora
Ustawienia węzła
Pokaż Sieć
Użyj Nowej Tożsamości
Zużycie Łącza
Pomoc
Informacje
Dziennik Logów
Ustawienia
Wyjdź
Pokazuj to okno na starcie
Ukryj

Hotspot Shield

Hotspot Shield jest niewielką aplikacją umożliwiającą anonimowy dostęp do Internetu.

To prosty w użyciu program, dzięki któremu połączenie z publicznym punktem dostępowym w kawiarni, hotelu lub na lotnisku, nie będzie narażone na ataki typu Sidejacking.

Hotspot Shield tworzy połączenie VPN między komputerem a punktem dostępowym. Ten szyfrowany tunel nie daje żadnej szansy osobom trzecim, które mogą próbować „podsłuchać" przesyłaną pocztę, hasła, wiadomości IM czy cokolwiek innego, co akurat przesyłamy w Internecie. Hotspot Shield zabezpiecza połączenia za pomocą szyfrowania HTTPS, a także współpracuje z sieciami przewodowymi. Ponadto dzięki programowi można ukryć swój adres IP.

Po zainstalowaniu aplikacja dostępna jest z poziomu paska menu. Klikając zakładkę Preferencje możemy przekonać się jaki jest przydzielony nam adres IP, prędkość połączenia, adres serwera VPN, a także czas połączenia.

Hotspot Shield

inSSIDer

inSSIDer to bezpłatny, niewielki i prosty w obsłudze program do skanowania pasma radiowego wykorzystywanego przez sieci bezprzewodowe (Wi-Fi).
Główną motywacją autorów programu był fakt, że popularny wśród sieciowców skaner NetStumbler nie funkcjonuje już prawidłowo na nowszych systemach Windows Vista i Windows 7 oraz na 64-bitowej wersji Windows XP. inSSIDer kreowany jest więc na następcę NetStumblera.

inSSIDer

inSSIDer skanuje pasmo 2,4 GHz i 5 GHz i wyświetla znalezione sieci wraz z ich podstawowymi danymi takimi jak SSID, adres MAC punktu dostępu, kanał, siła sygnału, RSSI, prędkość oraz rodzaj zabezpieczeń. Dane te mogą być użyteczne na przykład podczas ustalania najlepszego kanału dla nowej sieci bezprzewodowej lub badania przyczyny zakłóceń. Program współpracuje z większością odbiorników GPS, a znalezione sieci można później wyeksportować w formacie NS1 (używanym przez NetStumbler) oraz KML (używanym przez Google Earth).