Instrukcja 7 - Prezentacja wybranych analizatorów sieci

7.1 Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z zasadą działania i obsługą wybranych analizatorów sieci.

7.2 Anasil

Jednym z wartych uwagi, aczkolwiek już niewspieranych analizatorów sieci jest program **ANASIL** stworzony przez katowicką firmę LM Networks. Dzięki swej niebywałej elastyczności jest narzędziem o bardzo szerokich zastosowaniach: od diagnostyki sieci, poprzez monitorowanie krytycznych parametrów, wykrywanie nieautoryzowanego dostępu do łącza, sporządzanie remanentu, aż po pomoc we wszelkich projektach informatycznych w jakikolwiek sposób dotykających problematyki sieci lokalnych. Obecnie program Anasil działa **jedynie** na systemach operacyjnych **Windows 95/98/NT**.

Pomimo faktu, że ANASIL działa w systemie Windows 95/98/NT, analizy przez niego wykonywane nie ograniczają się do systemów firmy Microsoft. ANASIL analizuje również sieciową aktywność systemów spod znaku UNIX'a, Novell'a czy Apple. Jest to program adresowany głównie do:

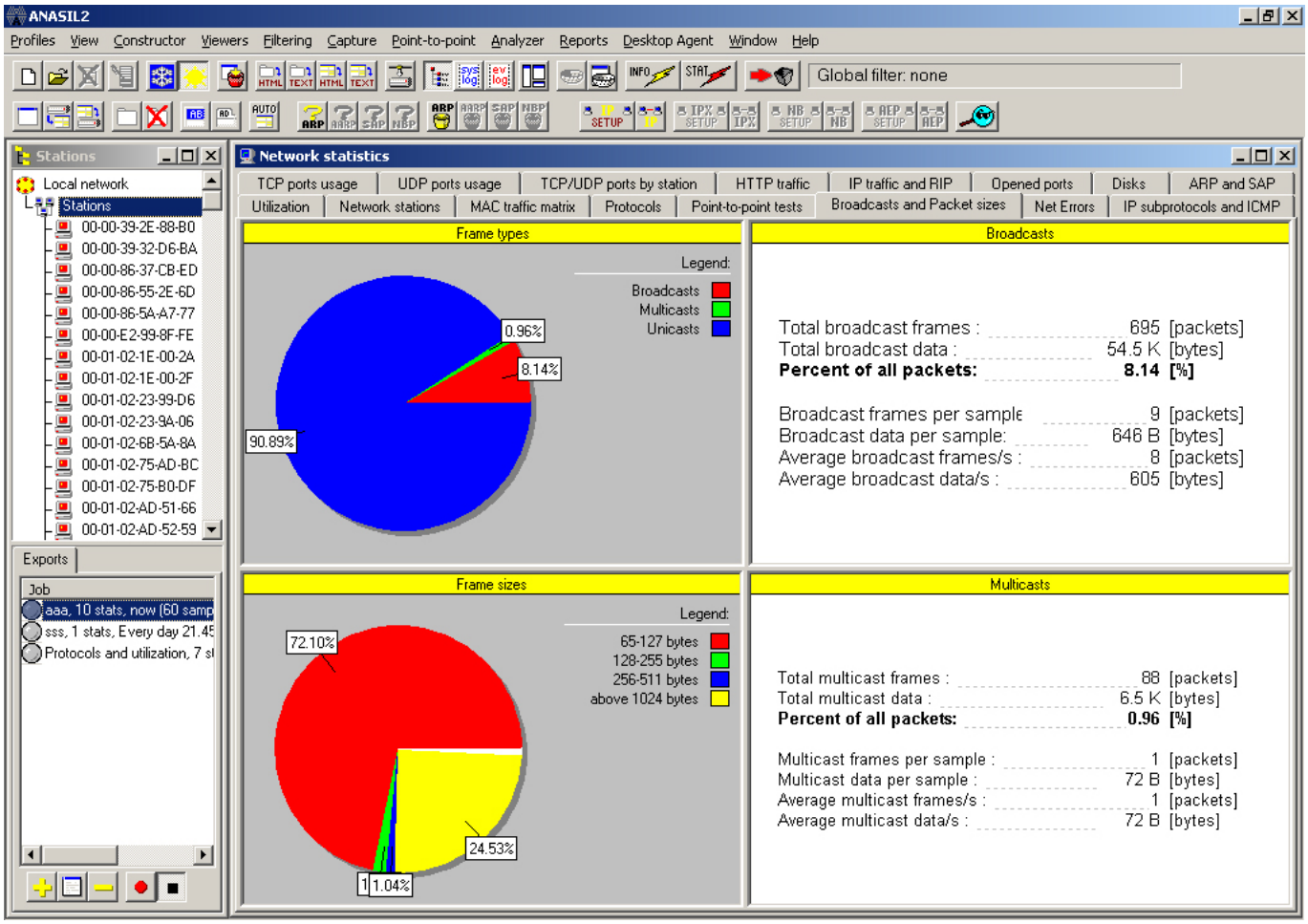
- **Administratorów sieci lokalnych** - opcje badania rozkładu obciążenia pomogą im znaleźć stacje generujące największy ruch w sieci, a testy point-to-point wykryć uszkodzone stacje. Profil sieci i wykrywanie nowych stacji pozwalają na łatwe zauważenie intruzów wpinających się w łącze. Dodatkowo profil sieci ułatwi przeprowadzenie remanentu.
- **Programistów pracujących w środowisku sieciowym** - przechwytywanie i analiza pakietów, które są nieocenionym narzędziem do testowania komunikacji pomiędzy programami działającymi na różnych komputerach. Programowalny dekoder protokołów pozwoli na łatwe stworzenie dekoderów własnych protokołów komunikacyjnych. ANASIL zapewnia też wgląd w status adapterów NetBIOS na zdalnych końcówkach.
- **Instalatorów i serwisantów sieci i serwerów** - dekoder protokołów i przechwytywanie ramek umożliwią im wykrycie i usunięcie problemów konfiguracyjnych, a testy point-to-point pomogą sprawdzić jakość zainstalowanej sieci.

7.2.1 Sposób działania

Do kontaktu z siecią ANASIL używa specjalizowanego drivera. Driver ten umożliwia odbiór wszystkich ramek transmitowanych w sieci. Umożliwia też wysyłanie niestandardowych ramek. Z jego pomocą ANASIL jest w stanie odebrać i zanalizować ruch w całym segmencie sieci **Ethernet** (w tzw. domenie kolizji, czyli jednym odcinku kabla lub w paru odcinkach połączonych przy pomocy repeaterów). Przez ruch rozumiemiemy tutaj ramki **wszystkich** typów oraz **wszystkich** protokołów sieciowych.

Odebrane ramki ANASIL analizuje i na podstawie tych analiz uaktualnia prowadzone przez siebie **statystyki**. Statystyki te dotyczą zarówno parametrów globalnych całego segmentu sieci (np. wykorzystanie czy sumaryczna liczba przetransmitowanych przez segment ramek) jak i poszczególnych stacji lub protokołów sieciowych.

Statystyki mogą być wizualizowane na różne sposoby oraz eksportowane przy pomocy **viewerów i form**. Dzięki temu możliwe jest śledzenie tylko tych statystyk, na których nam w danej chwili najbardziej zależy. Wybrany zbiór statystyk można **eksportować** z zadanym interwałem do pliku o specjalnym, skompresowanym formacie. Z plików takich można następnie przygotować różnego rodzaju **raporty**.



Rysunek 7.1: Program ANASIL

7.2.2 Możliwości programu ANASIL

Podstawowe możliwości programu ANASIL to:

- Pomiary obciążenia łącza, globalne i w rozbiciu na różne typy adresowania ramek,
- Pomiary aktywności poszczególnych komputerów w sieci (liczba ramek wysłanych i odebranych),
- Pomiary aktywności połączeń pomiędzy komputerami (liczba ramek przesłanych pomiędzy dwoma komputerami, procentowy udział tych transmisji w obciążeniu łącza),
- Lista i statystyki protokołów sieciowych,
- Zdalne sprawdzanie statusów adapterów NetBIOS (oraz nazw NetBIOS) we wszystkich komputerach sieci. Sprawdzane są adaptery działające przy pomocy różnych protokołów transportowych (IPX, TCP/IP oraz NetBEUI),
- Zdalne sprwadzanie do jakich serwerów NetWare zalogowany jest użytkownik na danej stacji,
- Głębsza analiza protokołów: IP, IPX, Appletalk oraz NetBEUI (NBF),
- Globalne filtrowanie i zliczanie przefiltrowanych ramek,
- Przechwytywanie i analiza przechwyconych ramek (packet capture) przy pomocy programowalnego dekodera protokołów. Napisanie dekodera dla własnego protokołu wymaga tylko edytora ASCII. Przechwycone ramki można przeglądać, filtrować oraz zachować do późniejszej analizy albo w formacie binarnym albo w pliku TXT,

- System wizualizacji zbieranych statystyk, pozwalający użytkownikowi na wyświetlenie danych w dogodnej dla niego postaci. Statystyki mogą być prezentowane jako tabele, pojedyncze okienka zawierające tekst, grupy statystyk lub hisogramy. Dla wartości numerycznych można dokonywać uśrednień, prezentować tylko maksima lub minima, tudzież określać zakresy wartości, po wejściu w które generowany jest komunikat lub zmienia się kolor okna,
- Testy point-to-point dla protokołów PIX, IP, Appletalk oraz NBF. Dla wybranych stacji określany jest minimalny/średni/maksymalny czas odpowiedzi (round-trip) oraz procentowa strata pakietów,
- Eksport danych do schowka, pliku TXT oraz stron HTML,
- Automatyczne tworzenie profilu sieci, czyli listy aktywnych stacji. Automatyczne przypisywanie nazw mnemonicznych w oparciu o protokoły DNS, SAP, NBP oraz usługi sieci Microsoft Networking. Stacje nie ujęte w profilu są traktowane jako nieautoryzowane i odpowiednio zaznaczane. Podczas tworzenia profilu system próbuje również zidentyfikować system operacyjny każdego komputera,
- Log systemowy z informacjami o przekroczeniu zadanych parametrów,
- Sortowanie tabel po dowolnie wybranej kolumnie.

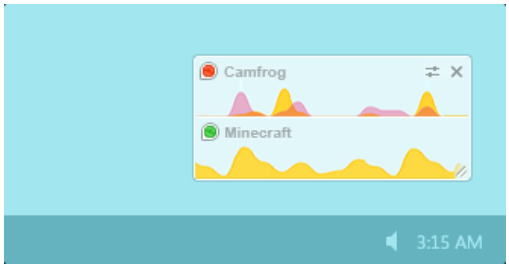
Szereg zaawansowanych możliwości wyróżnia ten program na tle innych programów. Podobne (choć bardziej ograniczone) możliwości ma m.in. program **Wireshark**, który zostanie szczegółowo omówiony w trakcie następnych zajęć laboratoryjnych.

7.3 GlassWire

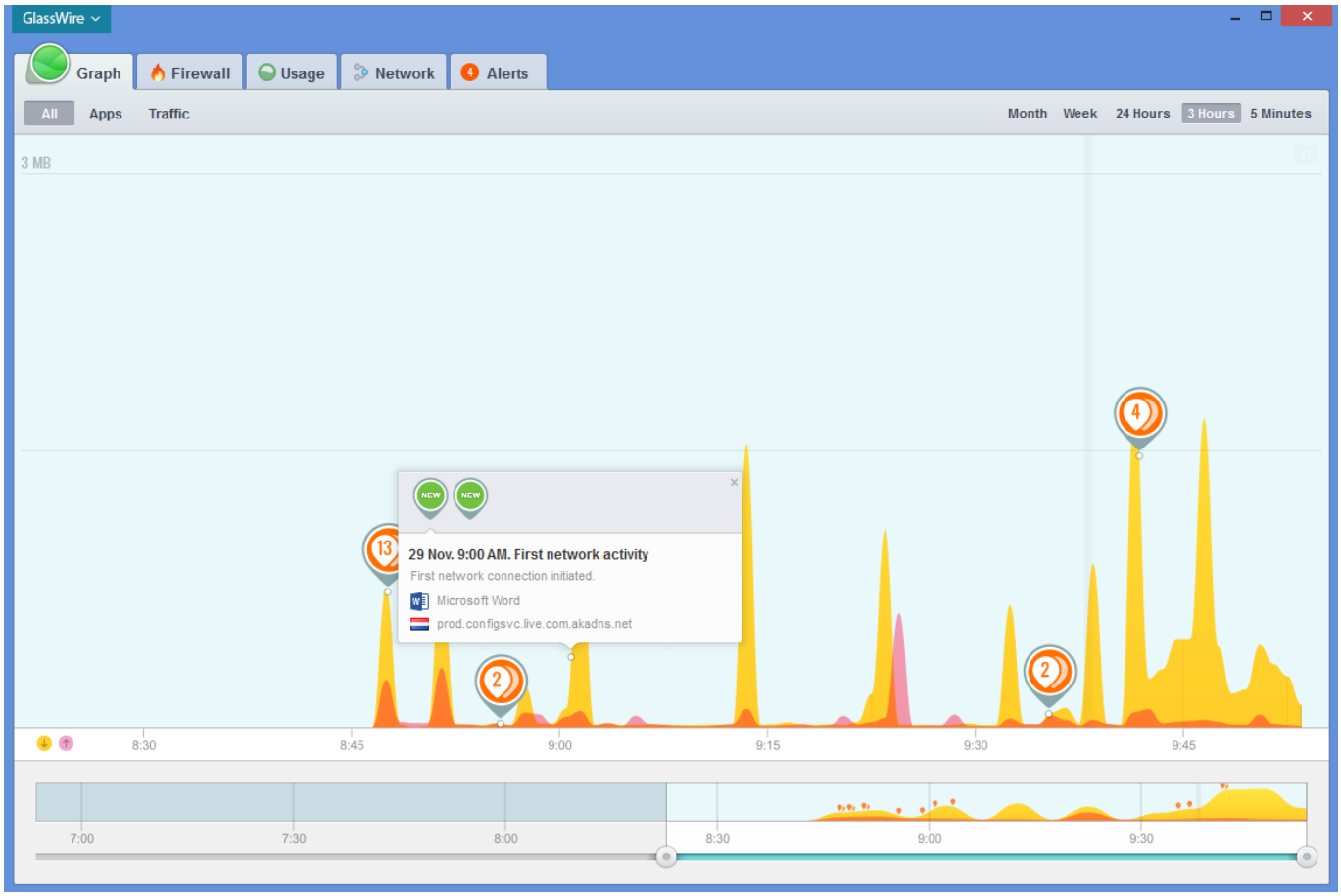
W porównaniu do programu ANASIL program **GlassWire** posiada znacznie ograniczone możliwości (m.in. nie umożliwia analizowania pojedynczych ramek), jednakże wyróżnia się on **przejrzystym interfejsem** i wbudowanym **firewallem**.

7.3.1 Możliwości programu GlassWire

- Monitorowanie ruchu w sieci,
- Monitorowanie ruchu w sieci z podziałem na aplikacje,
- Monitorowanie ruchu w sieci z podziałem na protokoły,
- Możliwość blokowania ruchu sieciowego dla dowolnej aplikacji,
- Możliwość podglądu ruchu w sieci według domen,
- Możliwość podglądu urządzeń podpiętych w sieci (tylko w wersji płatnej),
- Notyfikacja ruchu w sieci utworzonego przez nowe aplikacje,
- Możliwość zdalnego monitorowania wielu komputerów,
- Wykresy w trybie pełnym lub mini (tylko w wersji płatnej).



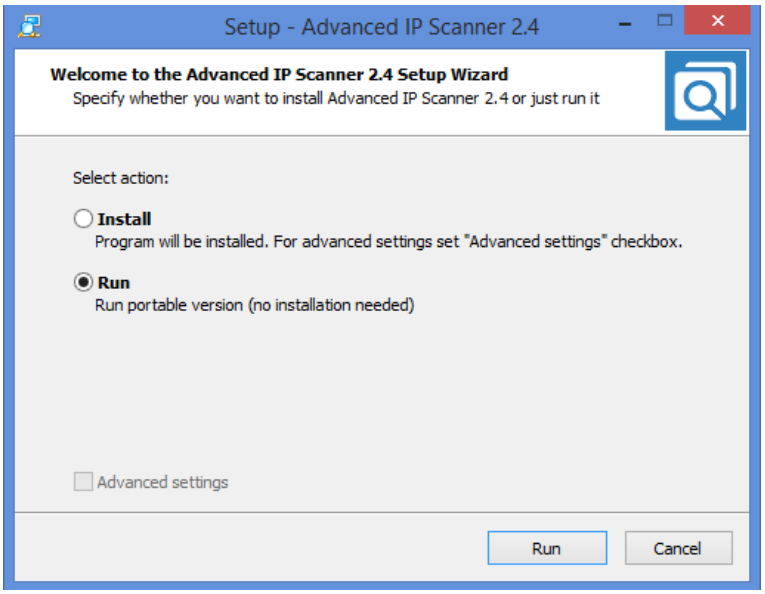
Rysunek 7.2: Mini wykres programu GlassWire



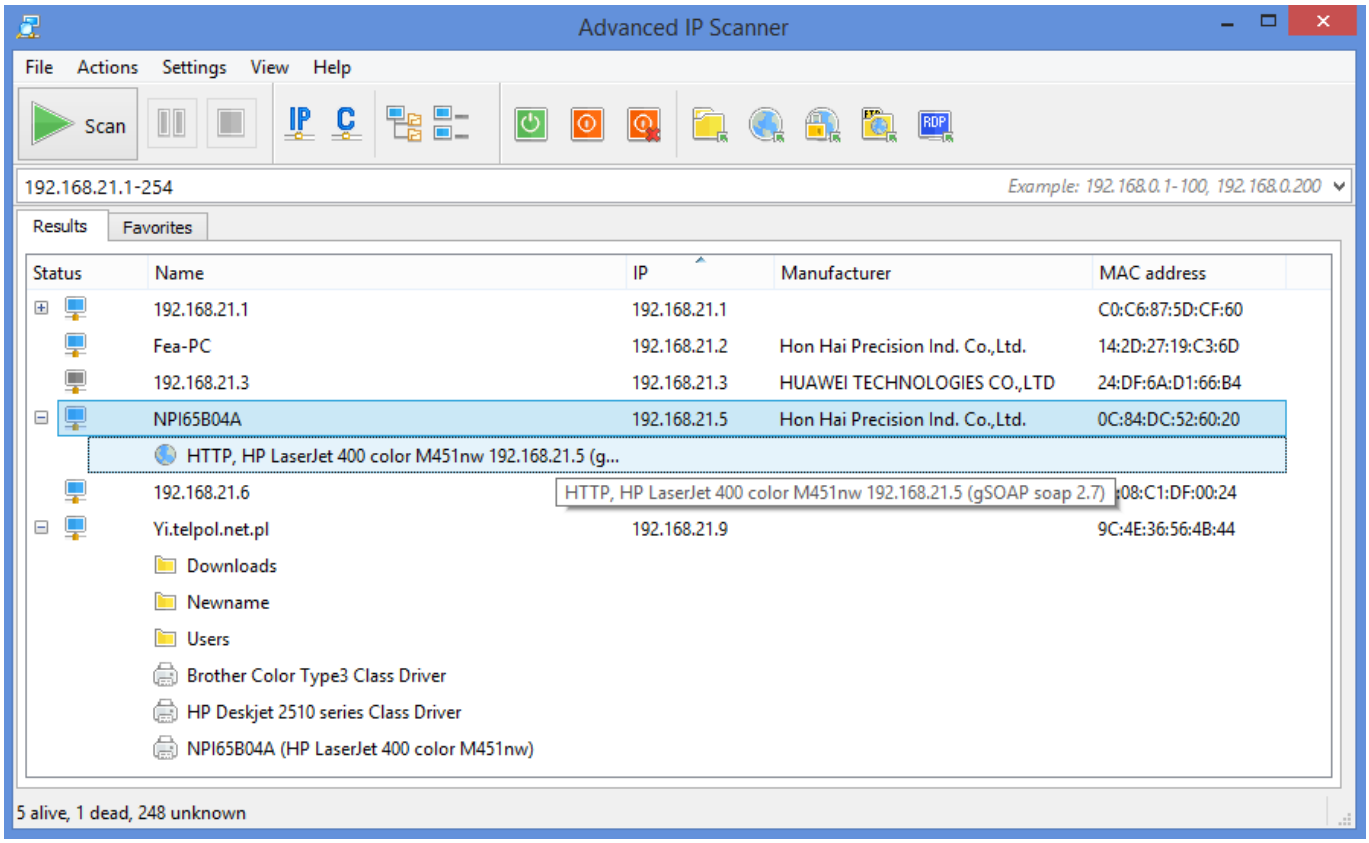
Rysunek 7.3: Program GlassWire

7.4 Advanced IP Scanner

Program Advanced IP Scanner umożliwia wyszukiwanie urządzeń sieciowych w sieci. Może być on traktowany, jako darmowe **uzupełnieniem** programu GlassWire.



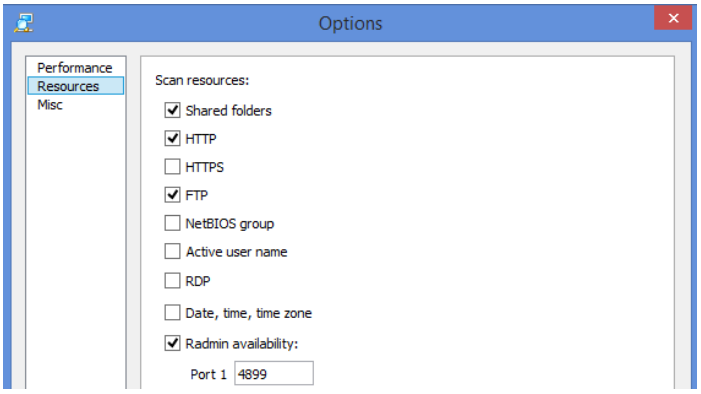
Rysunek 7.4: Tryby uruchomienia programu Advanced IP Scanner



Rysunek 7.5: Program Advanced IP Scanner

7.4.1 Możliwości programu Advanced IP Scanner

- Monitorowanie urządzeń w sieci,
- Uzyskanie informacji o udostępnianych usługach przez dane urządzenia (np. strony konfiguracji, udostępniane sterowniki oraz foldery),
- Możliwość skanowania zewnętrznych zakresów IP,
- Możliwość zdalnego włączania/wyłączania urządzeń sieciowych (z dostępną usługą),
- Możliwość szybkiego korzystania z narzędzi *ping*, *tracert*, *ftp*, *telnet*, *ssh*,
- Możliwość połączenia zdalnego.



Rysunek 7.6: Opcje programu Advanced IP Scanner

7.5 Przebieg ćwiczeń

7.5.1 GlassWire

1. Uruchomić program GlassWire, włączyć różne programy (np. przeglądarka, eksplorator, poczta, microsoft visual studio). Zaobserwować notyfikacje wyświetlane przez program widoczne w zakładce: **Graph** → **All**. W sprawozdaniu przedstawić zrzut ekranu dotyczący zakładki **Graph** → **Apps** dopasowując odpowiednio czas wyświetlanych danych (prawy górny róg programu oraz dolny suwak).

2. Przejrzeć zakładkę **FireWall**. Czy na liście znajduje się jakiś niepożądany program? W sprawozdaniu wypisać programy, które według własnego uznania można zablokować.

3. Przejrzeć zakładkę **Usage** → **All**. Jaka aplikacja/host/protokół była najbardziej aktywna? W sprawozdaniu umieścić zrzut ekranu.

4. Sprawdzić z jakimi hostami łączyła się aplikacja *Host Process for Windows Services* (klikając na nazwę aplikacji i wybierając odpowiednią zakładkę). Jaka dowolna **niepożądana** aplikacja wykonuje ruch w sieci i z jakimi hostami się łączy? W sprawozdaniu opisać jedną wybraną aplikację.

5. Przejrzeć zakładkę **Usage** → **Traffic** oraz dane dotyczące protokołów HTTP, HTTPS i NetBIOS (o ile dostępne). Uruchomić program **nslookup** testując dowolny serwer, następnie przejrzeć dane dotyczące protokołu DNS. Jakie inne aplikacje korzystały z tego protokołu? W sprawozdaniu umieścić zrzut ekranu dotyczący protokołu DNS.

6. Zamknąć **okno** programu pozostawiając jego działanie w tle (dostęp przez ikonę w trayu).

7.5.2 Advanced IP Scanner

1. Pobrać i uruchomić w trybie **Run** program Advanced IP Scanner (http://www.advanced-ip-scanner.com/).

2. Przeskanować domyślny zakres IP. Zaobserwować dostępne komputery oraz usługi i sterowniki. W sprawozdaniu umieścić zrzut ekranu.

3. Przeskanować zakres IP dotyczący dowolnie wybranego serwera (np. dla onet.pl - 213.180.141.140 będzie to **213.180.141.0-255**). Czy dużo urządzeń z danego zakresu jest aktywnych? Jakie są udostępnione usługi?

4. Zaznaczyć wszystkie opcje w zakładce Settings → Options → Resources. Przeskanować zakres IP dotyczący **pcz.pl**. Jakie usługi są dostępne? Otworzyć kilka dostępnych adresów www i zrzuty umieścić w sprawozdaniu.

5. Dla dowolnego urządzenia wywołać program ping oraz tracert (prawy przycisk myszy → Tools).

6. W programie GlassWire podejrzeć aktywność programu Advanced IP Scanner. Z jakich protokołów korzystał program? W sprawozdaniu umieścić zrzut ekranu.

7.6 Sprawozdanie

Studenci pracują i przygotowują sprawozdania w parach. W sprawozdaniu należy przedstawić przebieg przeprowadzonych eksperymentów, ich wyniki oraz wnioski.