Wydział Elektroniki i Telekomunikacji – POLITECHNIKA POZNAŃSKA
ul. Piotrowo 3a, 60-965 Poznań
fax: (+48 61) 665 25 72
tel: (+48 61) 665 22 93

LABORATORIUM SIECI KOMPUTEROWYCH

(compnet.et.put.poznan.pl)

Wireshark – analizator protokłów

Opracował: *dr inż. Sławomir Hanczewski*

Katedra Sieci Telekomunikacyjnych i Komputerowych

Poznań 2014

1. Wstęp

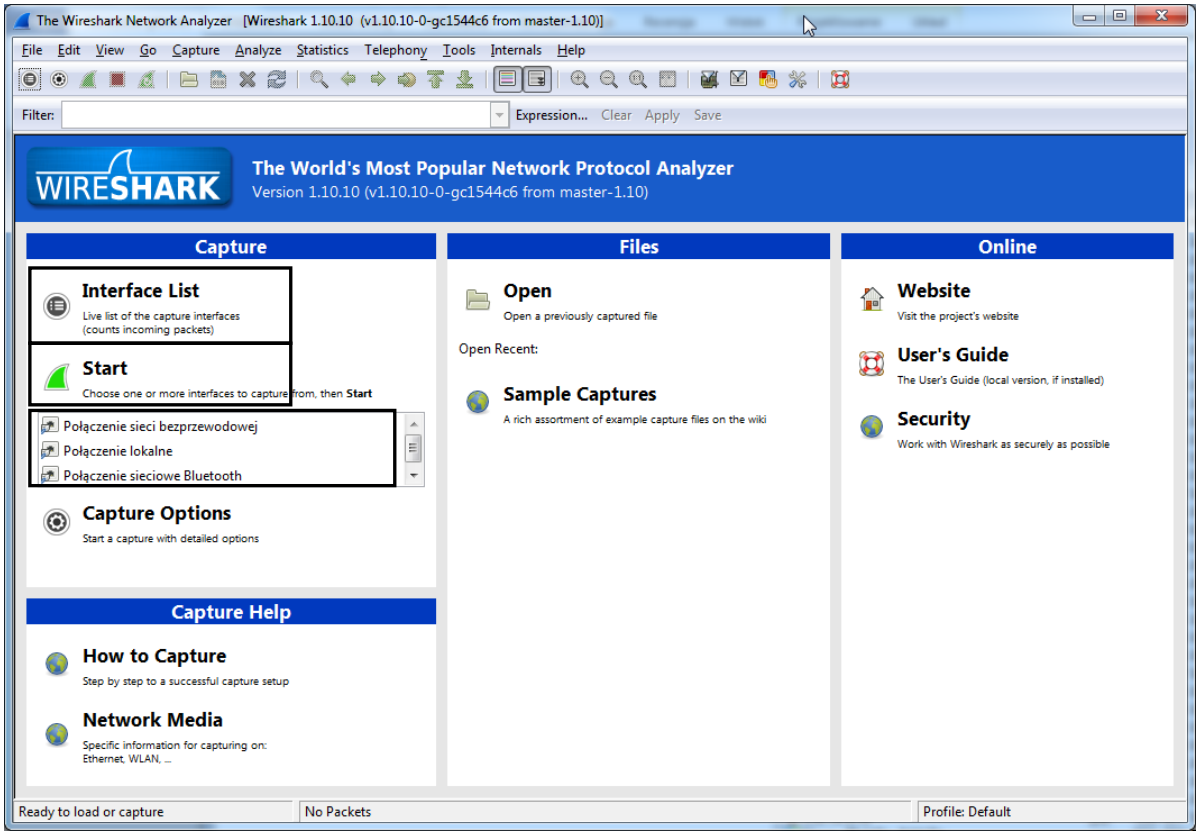
Wireshark jest sniferem. Oznacza to, że potrafi przechwytywać i analizować pakiety pojawiające się na wejściu karty sieciowej (ramki wchodzące i wychodzące). Program ten obsługuje większość popularnych protokołów (np. TCP/IP, IPX/SPX, SMB, Netbios). Posiada bardzo prosty i przejrzysty interfejs graficzny. Jest zatem wygodnym narzędziem do analizy protokołów oraz do diagnozowania problemów w sieci. Należy go używać **WYŁĄCZNIE** do tego celu. Podsłuchiwanie ruchu w sieci generowanego przez innych użytkowników jest NIELEGALNE!!!

Wireshark jest dostępny w wersji dla Windows jak i dla większości platform unikowych. Jest programem udostępnianym bezpłatnie.

2. Wprowadzenie do programu

Po włączeniu programu pojawia się okno przedstawione na rysunku 1. Zostało ono podzielone na trzy części:

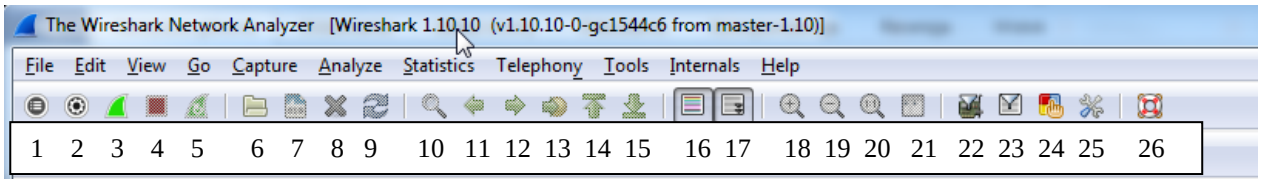
- **Capture** (przechwytywanie), gdzie użytkownik ma możliwość wyboru interfejsu z którego będą przechwytywane ramki (Interface List). Po wyborze interfejsu można rozpocząć przechwytywanie (Start). Interfejs można wybrać również z listy znajdującej się poniżej przycisku start;
- **Files**, gdzie użytkownik ma możliwość otworzenia pliku z przechwyconymi wcześniej pakietami (Open), lub przeglądania wybranych, przykładowych próbek z przechwyconymi pakietami (Sample Captures) – wymagany jest dostęp do Internetu;
- **Online**, gdzie użytkownik ma dostęp do pomocy online.



Rysunek 1. Program Wireshark (wersja 1.10)

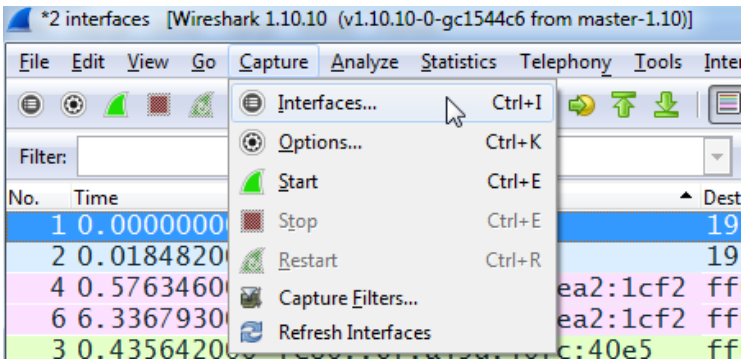
2.1 Pasek narzędzi

Domyślny pasek narzędzi programu Wireshark przedstawiony został na rysunku 2.



Rysunek 2. Pasek narzędzi programu Wireshark

Znaczenie poszczególnych ikon jest następujące:
1 – lista dostępnych interfejsów,
2 – opcje przechwytywania,
3 – start,
4 – stop,
5 – restart przechwytywania,
6 – otwóż plik z przechyconymi pakietami,
7 – zapisz przechwycone pakiety do pliku,
8 – wykasuj przechwycone pakiety (zamknij plik) – przywraca okno startowe programu,
9 – odświerz,
10 – znajdź pakiet,
11- przejdź do poprzednio przeglądanego pakietu (w historii przegladania),
12 – przejdź do następnego (w historii przegladania) pzregladanego pakietu,
13 – przejdź do pakietu o numerze …,
14 – przejdź do pierwszego pakietu,
15 – przejdź do ostatniego pakietu,
16 – koloruj pakiety (w zależności od protokołu),
17 – autoprzewianie przechwycanych pakietów,
18 – powiększ czcionkę,
19 – zmniejsz czcionkę,
20 – ustawinia początkowe,
21 – dostosuj szerokość kolumn do aktualnej czcionki,
22 – edytuj filtr przechytywania,
23 – edytuj filtr wyświetlania,
24 – opcje kolorowania pakietów,
25 – preferencje użytkownika,
26 – pomoc.

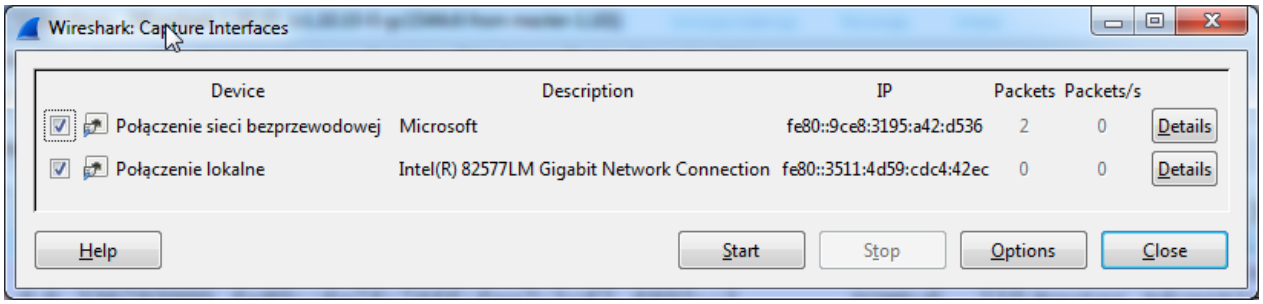


Rysunek 3. Menu capture

Wszytskie te narzędzia są dostępne również z poziomu odpowiedniego menu, np. narzędzia z włączaniem i wyłączaniem przechywtywania dostępne są w menu **Capture** (rysunek 3).

2.2 Przechwytywanie pakietów

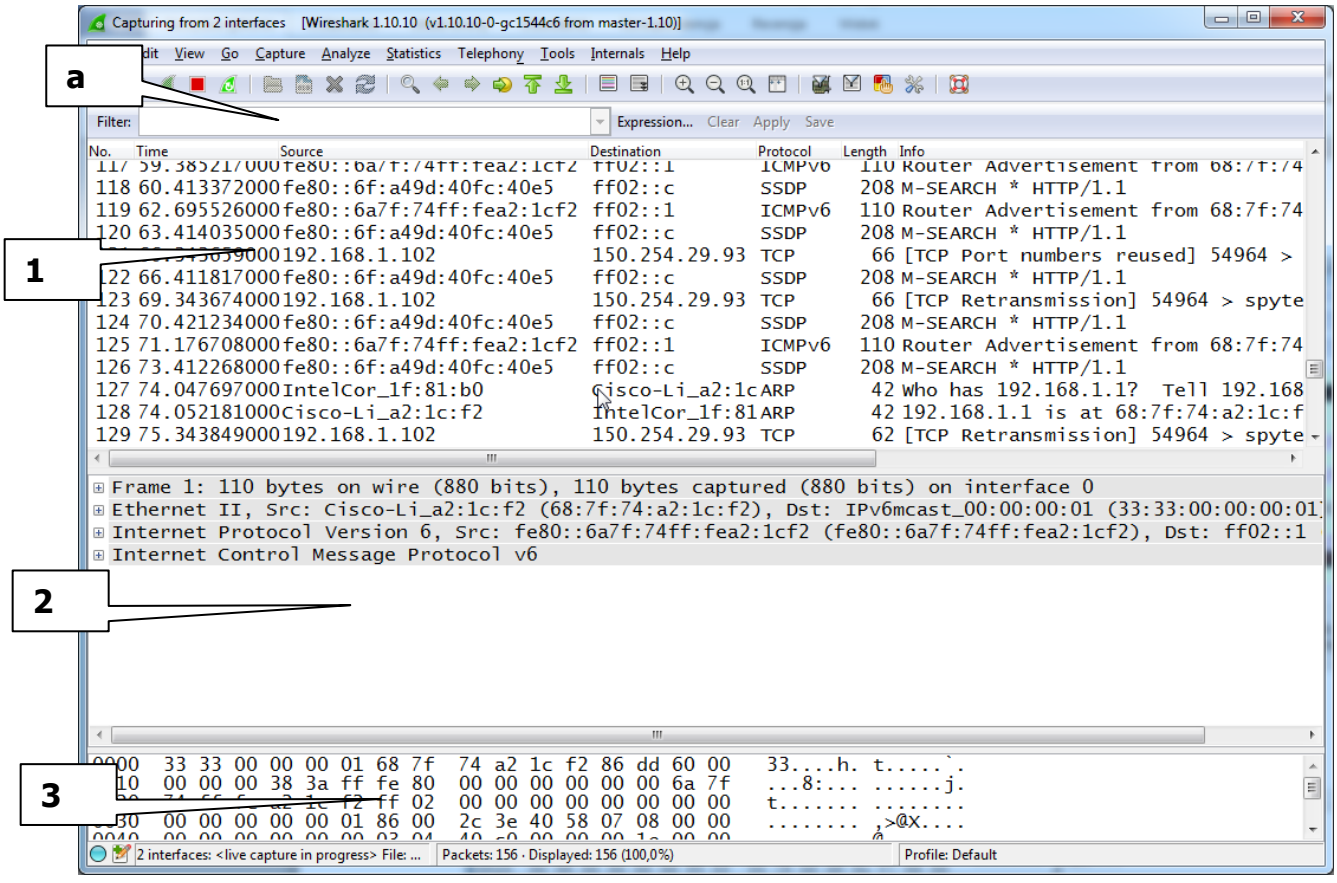
Aby rozpocząć przechwytywanie pakietów należy po uruchomieniu programu Wireshark wybrać interfejs (lub interfejsy) z których przechwytywane będą pakiety. Można to zrobić klikając na ikonę 1 (rysunek 2). Po kliknieciu pojawi się następujące okno:



Rysunek 4. Lista dostępnych interfejsów

Klikając na przycisk **Start** można od razu rozpocząć przechwytywanie. Warto zauważyć, że interfesy z których będą przechwytywane pakiety wystarczy wybrac tylko raz. Jeżeli użytkownik nie zdecyduje się uruchomić przechwytywania pakietów z okna listy interfejsów może to zrobić np. za pomocą okony 3 (rysunek 2). Zatrzymać przechwytywanie można poprzez kliknięcie na ikonę 4 (rysunek 2) lub poprzez wywołanie okna dostępnych interfejsów i kliknięcie na przycisk **Stop**.

Po włączeniu przechwytywania okno programu zmienia wygląd (Rysunek 5).

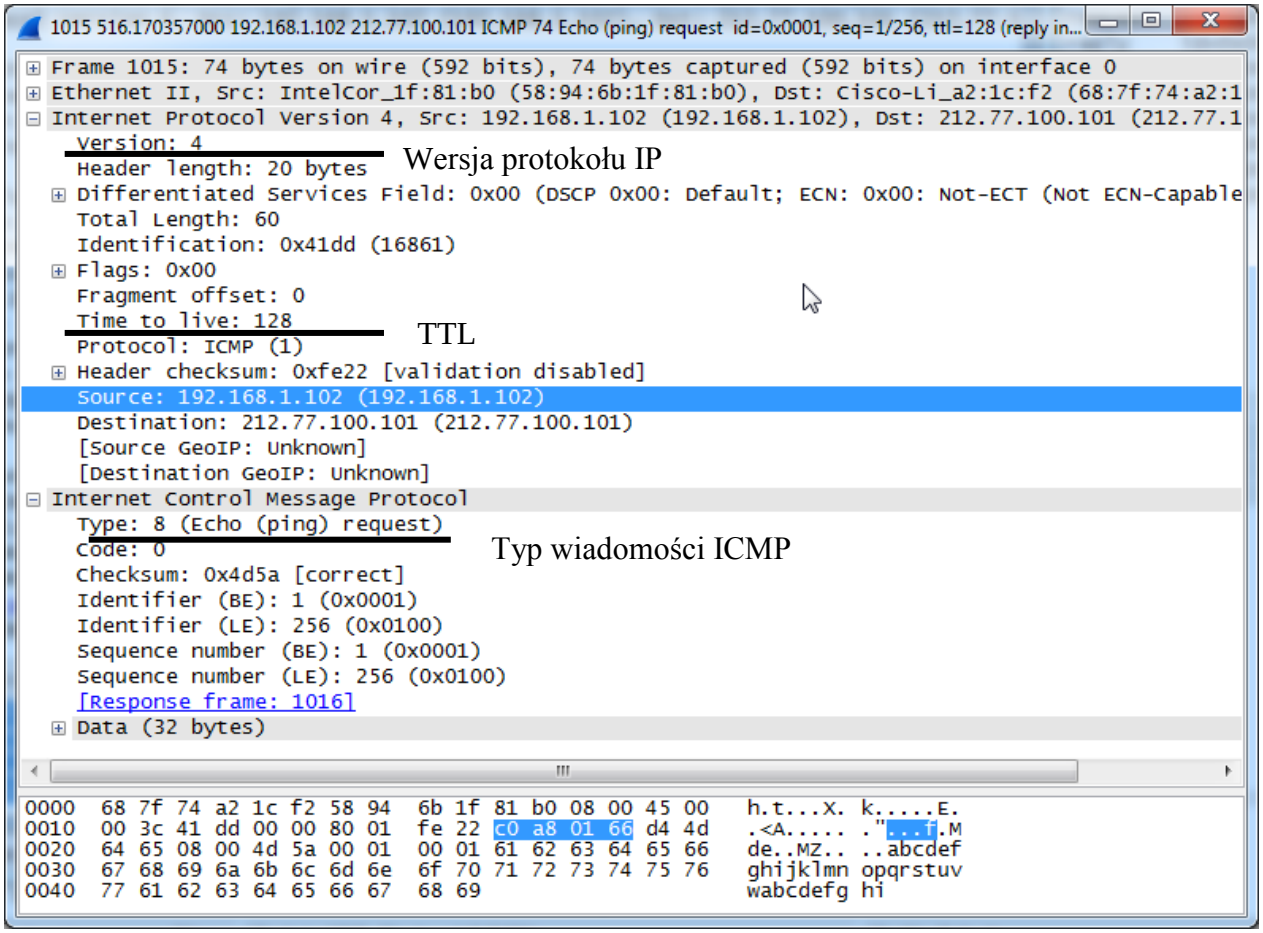


Rysunek 5. Program Wireshark przechwytujący pakiety

1 – lista przechwyconych pakietów
2 – zawartość wybranego pakietu
3 – pole pakietu – wskazuje przez podświetlenie wybrane w oknie 2 elementy pakietu
A – pole filtru – wskazuje kryterium wyświetlania ramek (jeżeli tło pola jest zielone kryterium jest poprawne)

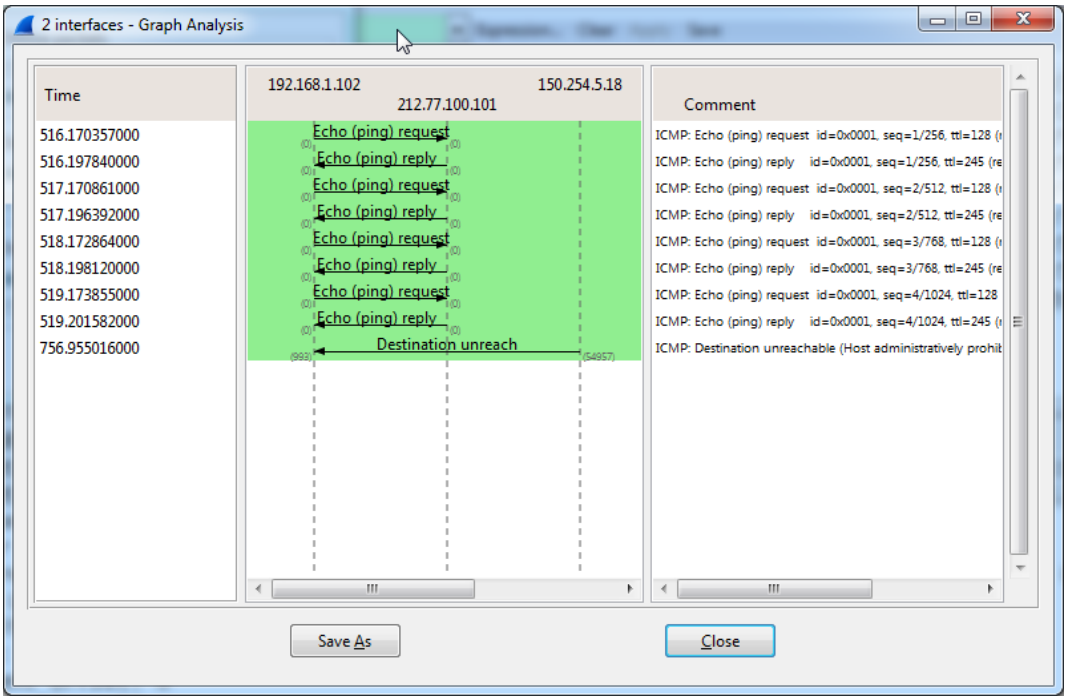
3. Analiza pakietów (ramek)

Po zatrzymaniu przechwytywania można przystąpić do analizy pakietów. Aby wyświetlić tylko te pakiety, które chcemy przeglądać należy w polu filtru wyświetlania wpisać odpowiednią regułę filtrowania np. jeśli wyświetlona mają być pakiety przesyłane w wyniku wywołania polecenia ping w polu filtru należy wpisać **icmp.** Na rysunku 6 przedstawiono pakiet z wiadomością protokołu ICMP.



Rysunek 6. Analiza przykładowego pakietu

Wireshark generuje szereg statystyk (menu Statistics). Program ten potrafi również zaprezentować w formie graficznej wymianę pakietów pomiędzy hostem na którym jest zainstalowany a hostem zdalnym (menu Statistics->Flow graph). Graficzne przedstawienie wymiany wiadomości ICMP (polecenie pathping) zostało pokazane na rysunku 7.



Rysunek 7. Graf przepływu ramek

Więcej informacji o programie można znaleźć na stronie:
http://www.wireshark.org.

4. Przebieg ćwiczenia

4.1 Analiza działania polecenia `ping`

1. Włączyć wiersz poleceń (cmd).
2. Włączyć program wireshark, wybrać odpowiedni interfejs a następnie włączyć przechwytywanie pakietów.
3. W polu filtra przechwytywania wpisac icmp.
4. W wierszu poleceń wydać następujące polecenie:

```
ping helios.et.put.poznan.pl
```

5. Po zakończeniu działania polecenia **`ping`** należy wyłączyć przechwytywania pakietów (można zapisać przechwycone pakiety).

Odpowiedz na następujące pytania:

a) Ile wiadomości i jakiego typu wysłał komputer?
b) Ile wiadomości i jakiego typu otrzymał komputer?
c) Określić adres IP oraz MAC źródła i odbiorcy przechwyconych wiadomości ICMP.
d) Jakie są różnice pomiędzy adresem IPv4 i MAC?
e) Określić wartość parametru TTL.
f) Co to jest TTL i dlaczego jest ustawiany w pakietach IP?
g) Czy pole o podobnym znaczeniu znajduje się w ramce ethernetowej?
h) Co się stanie jeżeli polecenie ping zostanie użyte z przełącznikiem –i 2:

```
ping helios.et.put.poznan.pl –i 2
```

i) Narysuj graf przepływu.

4.2 Analiza działania polecenia `tracert`

1. Włączyć przechwytywanie pakietów.

2. W wierszu poleceń wydać następujące polecenie:
`tracert helios.et.put.poznan.pl`
3. Po zakończeniu działania polecenia **`tracert`** należy wyłączyć przechwytywania pakietów a w pole filtru przchwytywania ponownie należy wpisać icmp.
Odpowiedz na następujące pytania:

a) Ile wiadomości i jakiego typu wysłał komputer?
b) Ile wiadomości i jakiego typu odebrał komputer?
c) Określić adres IP oraz MAC źródła i odbiorcy przechwyconych wiadomości ICMP.
d) Określić wartość parametru TTL w poszczególnych pakietach.
e) Narysuj graf przepływu pakietów (na podstawie grafu wygenerowanego przez wireshark).

5.3 Analiza działania polecenia `pathping`

1. Włączyć przechwytywanie pakietów.
2. W wierszu poleceń wydać następujące polecenie:
`pathping helios.et.put.poznan.pl`
3. Po zakończeniu działania polecenia **`pathping`** należy wyłączyć przechwytywania pakietów a w pole filtru przchwytywania ponownie należy wpisać icmp.

Odpowiedz na następujące pytania:

a) Ile wiadomości i jakiego typu wysłał komputer?
b) Ile wiadomości i jakiego typu odebrał komputer?
c) Czy w wysyłanych (odbieranych) pakietach zmianiana jest wartość parametru TTL, jeśli tak to w jaki spoób?
d) Na podstawie przechwyconych pakietów w wiadomościami protokołu ICMP przedstaw zasadę działania polecenia **`pathping`**.
e) Narysuj uproszczony graf przepływu.

5.4 Analiza działania protokołów telnet oraz ssh

1. Włączyć przechwytywanie pakietów (wyczyść filtr przechwytywania).
2. Uruchom program **putty** (rysunek 8) i za pomocą protokołu telent (Connection type Telnet) połącz się z serwerem:
`helios.et.put.poznan.pl`
(w przypadku braku konta na serwerze proszę użyć danych do logowania:
Login: **user**
Password: **qwerty**
3. Niezależnie od tego czy próba logowania zakończyła się sukcesem przerwać przechwytywanie pakietów a w pole filtra wyświetlania wpisać **telnet**.
4. klikając na dowolnym pakiecie związnym z nawiązywaniem połączenia z serwerem za pomocą protokołu telnet prwwym klawiszem myszy wybierz opcję **`Follow TCP Stream.`**

Odpowiedz na następujące pytania:

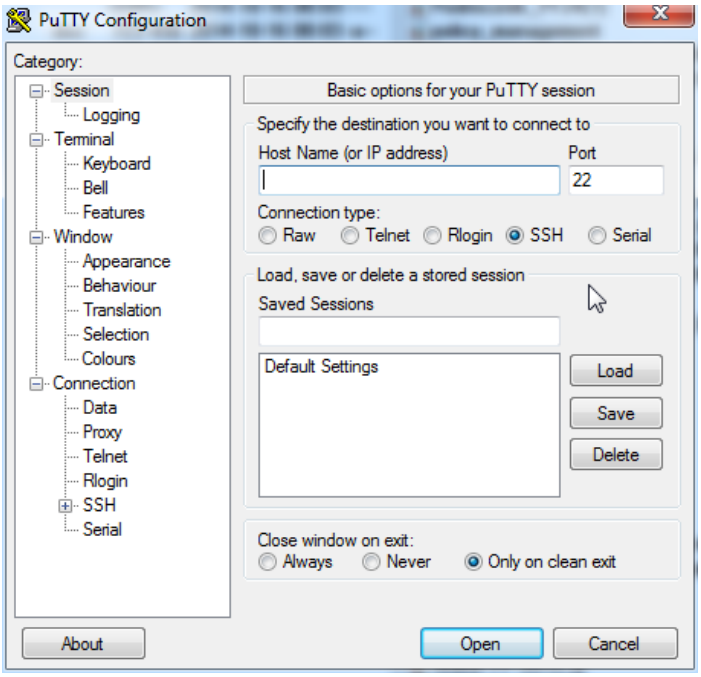
a) Jakie informacje przedstawia program po wyborze opcji **`Follow TCP Stream`**?
b) Co można powiedzieć o protokole **`telnet`**?

c) W jaki sposób przesyłane są login i hasło?

Czynności 1-4 powtórz dla protokołu ssh (program putty, connection type ssh) i odpowiedz na pytania a-c w odniesieniu do protokołu ssh.

Podsumowując tę cześć ćwiczenia odpowiedz na pytanie:

d) Który sposób łączenia się z serwerem jest bardziej bezpieczny?



Rysunek 8. Okno programu putty

5.5 Analiza działania protokołu FTP

Wykonać analizę przesyłanych danych niezbędnych do łączenia się z serwerem w przypadku protokołu FTP (ćwiczenie należy wykonać w analogiczny sposób jak w przypadku protokołów telnet). Również w tym przypadku należy podjąć próbę połączenia z serwerem FTP dostępnym na helios.et.put.poznan.pl

- czy istnieje bezpieczniejszy od FTP sposób przesyłania plików?

6. Literatura

Instrukcja obsługi programu Wireshark