

FTP – Protokół przesyłania plików

Autor: Sebastian Paja IVFDS

STRESZCZENIE

Niniejsze opracowanie zawiera podstawowe informacje dotyczące najpopularniejszego protokołu przesyłania plików FTP. Przedstawiono występujące w nim wady jak i zalety. Następnie zamieszczono zasadę działania – sposób komunikowania się klienta z serwerem. W kolejnych rozdziałach znajduje się opis podstawowych poleceń wykorzystywanych przy komunikacji za pośrednictwem protokołu FTP. Dalej omówiono zagadnienia bezpieczeństwa w sieci oraz przedstawiony został mechanizm wyszukiwania udostępnionych w sieci plików za pośrednictwem serwerów Archie.

Spis treści

Streszczenie	2
1. Wstęp.....	4
2. Korzystanie z FTP	4
3. Zasada działania	4
4. Podstawowe polecenia FTP	6
4.1. Polecenia sterujące dostępem.....	6
4.2. Polecenia sterujące przesyłaniem.....	7
4.3. Polecenia przesyłania plików	7
4.4. Polecenia zarządzania plikami i katalogami	8
4.5. Polecenia pomocy i kontroli stanu sesji	9
4.6. Kody odpowiedzi serwera FTP	9
5. Zagadnienia bezpieczeństwa FTP	11
6. Wykorzystywanie Archie do przeszukiwania zasobów FTP	12
Literatura	15

1. WSTĘP

FTP jest najpopularniejszym protokołem stosowanym do przesyłania plików przez Internet. Działa on na zasadzie klient – serwer i jest znacznie starszy od powszechnie stosowanego w sieci WWW protokołu HTTP. (został wprowadzony w 1971 roku.)

Protokół FTP był zaprojektowany do następujących zastosowań:

- do podtrzymania wspólnego używania plików;
- do podtrzymania zdalnego używania komputerów;
- do aktualizowania wersji programów na serwerach plików;
- do dokładnej i skutecznej transmisji plików.

Chociaż FTP może być używany przez użytkownika wprost na terminalu, jednak przy projektowaniu zakładano iż będzie on wykorzystywany przez programy [3].

2. KORZYSTANIE Z FTP

Do skopiowania plików znajdujących się na innym komputerze w sieci potrzebne jest odpowiednie oprogramowanie umożliwiające rozpoznawanie protokołu FTP. Tego typu programy znajdujące się po stronie użytkownika nazywa się klientem FTP, natomiast komputer dysponujący zasobami plików i udostępniający je w sieci jest serwerem FTP. W dzisiejszych czasach większość systemów operacyjnych wyposażona jest w takie usługi. Programy klientów FTP mogą być różne, począwszy od obsługiwanych za pomocą specjalnych komend w trybie tekstowym (np. ftp.exe) aż po proste w obsłudze programy okienkowe (np. Windows Commander), gdzie w jednym okienku znajdują się pliki dostępne na serwerze a w drugim oknie pokazane są pliki naszego komputera. Obsługa sprowadza się do zaznaczenia odpowiednich plików i kliknięcia odpowiedniego przycisku z poleceniem „kopiuj”.

Do działających na tej zasadzie popularnych klientów FTP należą m.in. programy FlashFXP oraz CuteFTP [2].

3. ZASADA DZIAŁANIA

Protokół przesyłania plików jest najpopularniejszym protokołem wykorzystywanym do przenoszenia plików pomiędzy stacjami w sieci TCP/IP. Główną jego zaletą jest oparcie funkcjonowania na protokole transportu TCP, co zapewnia niezawodne, wymagające ustanowienia sesji połączeniowej przesyłanie.

Protokół FTP wykorzystuje w transmisji danych dwa procesy:

- Proces przesyłania danych (ang. DTP - *Data Transfer Process*) zapewnia faktyczną transmisję danych pomiędzy klientem a serwerem FTP.
- Interpretator protokołu (ang. PI - *Protocol Interpreter*) jest wykorzystywany do przesyłania poleceń pomiędzy klientem a serwerem, Inicjuje on proces FTP i zarządza usługą DTP od strony klienta.

Faktycznie sesja FTP składa się więc z dwóch osobnych sesji łączących klienta z serwerem (rysunek 1).

W trakcie ustanawiania między klientem i serwerem sesji realizowane są następują transakcje:

1. Na początku ustanawiana jest sesja pomiędzy usługami PI klienta i serwera, Interpretator protokołu po stronie użytkownika inicjuje połączenie sterujące pomiędzy stacjami. Za jego pośrednictwem klient FTP przesyła polecenia do serwera, a serwer potwierdza ich wykonanie. Strona użytkownika korzysta z portu o numerze przydzielonym losowo, po stronie serwera wykorzystywany jest port TCP 21
2. Żądanie przesłania danych powoduje zainicjowanie przez proces DTP serwera połączenia z usługą DTP klienta. Tym połączeniem przesyłane są wyłącznie dane

Połączenie sterujące zostaje zachowane również w trakcie przesyłania danych. Oba połączenia, sterujące i danych, pozwalają na przesyłanie danych w dwóch kierunkach.

Anonimowe sesje FTP

Protokół FTP pozwala na nawiązywanie połączeń anonimowych. Wykorzystywaną wówczas nazwą konta jest `anonymous` lub `ftp`. Zwyczajowo serwer FTP prosi użytkownika korzystającego z takiego konta o podanie swojego adresu e-mail jako hasła. Choć zastosowanie serwera anonimowego FTP może wydawać się lekkomyślne, ma ono istotne zalety, również w zakresie bezpieczeństwa. Ograniczenie uprawnień użytkowników jedynie do odczytu zabezpiecza serwer przed umieszczaniem na nim niepożądanych danych. Wstrzymanie przesyłania nazw kont i haseł tekstem jawnym również jest znaczną korzyścią [1].

4. PODSTAWOWE POLECENIA FTP

Poniżej znajdują się najważniejsze polecenia wykorzystywane podczas komunikacji za pomocą protokołu FTP. Zostały one przedstawione w następujących kategoriach:

- polecenia sterujące dostępem,
- polecenia sterujące przesyłaniem,
- polecenia przesyłania plików,
- polecenia zarządzania plikami i katalogami,
- polecenia pomocy i kontroli stanu sesji,
- odpowiedzi serwera FTP.

4.1. Polecenia sterujące dostępem

Polecenia sterujące dostępem używane są podczas rozpoczynania i zakańczania sesji FTP, gdy łączą się stacje klienta z serwerem. Kolejność ich wprowadzania jest zazwyczaj standardowa to znaczy: otwarcie połączenia z żadaną stacją, podanie nazwy użytkownika (polecenie USER), jak i hasła PASS.

Listę poleceń przedstawia tabela 1.

Tabela1 – Polecenia FTP sterujące dostępem [1].

Polecenie	Opis
OPEN [komputer]	Ustanawia sesję z usługą FTP stacji o nazwie komputer.
USER [nazwa]	Określa użytkownika korzystającego z poleceń FTP. Jest to pierwsze polecenie przesyłane po nawiązaniu połączenia.
PASS [hasło]	Polecenie wprowadzane bezpośrednio po USER. Przekazuje ono hasło użytkownika do serwera FTP za pośrednictwem protokołu Telnet. Pomimo że klient podczas wprowadzania hasła nie widzi go na ekranie, w sieci przesyłane jest ono w sposób jawny.
ACCT [konto]	Wymagany przez niektóre serwery FTP opcjonalny parametr określający konto użytkownika. Podawana nazwa nie musi mieć związku z poleceniem user.
SMNT	Polecenie montuj strukturę (Structure Mount) pozwala na zainstalowanie struktury danych odmiennego systemu plików bez ponawiania logowania do serwera.
REIN	Polecenie inicjuj ponownie (Reinitialize) kończy sesję dla bieżącego konta użytkownika. Transmisja wszystkich danych wejściowych i wyjściowych (z wyjątkiem trwającego przesyłania) zostaje wstrzymana. Użytkownik wraca do tego samego punktu, w którym znajdował się w momencie nawiązania połączenia z serwerem.
QUIT	Kończy sesję łączącą stacje klienta i serwera.

4.2. Polecenia sterujące przesyłaniem

Polecenia te pozwalają zmienić ustawienia dotyczące sposobu przesyłania danych. Jednak ustawienia serwera pozostają zazwyczaj niezmienione. Zmiany ustawień serwera dokonuje się tylko w przypadku, gdy oprogramowanie klienta wymaga nowszych metod transmisji. Zestawienie poleceń przedstawia tabela 2.

Tabela 2 – Polecenia FTP sterujące przesyłaniem [1].

Polecenie	Opis
PORT##	Polecenie to pozwala wybrać numer portu po stronie klienta. Parametr ## powinien zawierać 32-bitowy adres IP stacji, z którą nawiązane będzie połączenie DTP oraz 16-bitowy numer portu.
PASV	Polecenie <i>Passive</i> (Pasywny) zmienia zachowanie serwera przy ustanawianiu sesji danych. Zamiast inicjowania połączenia, serwer będzie jedynie monitorował port danych i oczekiwał na ustanowienie sesji przez klienta.
TYPE	Polecenie <i>Representation Type</i> (Typ reprezentacji) określa format reprezentacji danych serwera: ASCII, EBCDIC lub Image.
STRU	Polecenie <i>File Structure</i> (Struktura pliku) określa domyślną strukturę plików: <i>files</i> (pliki), <i>records</i> (rekordy) lub <i>pages</i> (strony).
MODE	Polecenie <i>Transfer Mode</i> (Tryb przesyłania) określa tryb transmisji danych jako: <i>Stream</i> (Strumień), <i>Block</i> (Blok) lub <i>Compressed</i> (Skompresowane).

4.3. Polecenia przesyłania plików

Gdy połączenie z serwerem zostało nawiązane i wprowadzono ustawienia dotyczące przesyłania danych, za pomocą poleceń przesyłania plików można rozpocząć właściwą transmisję. W tabeli 3 zestawione są polecenia przesyłania plików.

Tabela 3 – Polecenia FTP służące do przesyłania plików [1].

Polecenie	Opis
ASCII	Włącza tryb transmisji ASCII, dla plików tekstowych. Jest on używany domyślnie.
BINARY	Włącza tryb binarny transmisji, który powinien być stosowany do przesyłania wszystkich plików innych niż pliki tekstowe.
TYPE	Pozwala sprawdzić, który z trybów przesyłania został ustawiony – binarny czy ASCII.
RECV plikserwer [plikklient]	Kopiuje plik <i>plikserwer</i> z serwera do pliku lokalnego <i>plikklient</i> , Jeżeli nazwa pliku lokalnego nie zostanie podana, plik zostanie skopiowany z zachowaniem nazwy oryginalnej.
SEND plikklient [plikserwer]	Kopiuje lokalny plik <i>plikklient</i> do pliku <i>plikserwer</i> na serwerze. Jeżeli nazwa pliku na serwerze nie zostanie podana, plik zostanie

	skopiowany z zachowaniem nazwy lokalnej.
GET plikserwer [plik klient]	Funkcjonuje tak samo jak polecenie <code>recv</code> .
PUT plik klient [plik serwer]	Funkcjonuje tak samo jak polecenie <code>send</code> .
MGET [plik serwer]	Multiple Get (Wielokrotne Get) funkcjonuje podobnie jak polecenie <code>GET</code> , ale pozwala na kopiowanie większej ilości plików, dzięki możliwości zastosowania do określenia grupy plików symboli wieloznacznych.
MPUT [plik klient]	Multiple Put (Wielokrotne PUT) funkcjonuje podobnie jak polecenie <code>put</code> , ale pozwala na kopiowanie większej ilości plików, dzięki możliwości zastosowania symboli wieloznacznych do określenia grupy plików.
PROMPT	Włącza lub wyłącza wyświetlanie komunikatów z żądaniem potwierdzenia kopiowania po wprowadzeniu poleceń <code>mget</code> i <code>mput</code> . Gdy są one włączone, pojawia się zapytanie, czy kopiowanie plików ma być kolejno potwierdzane. Gdy są wyłączone, żadne potwierdzenia nie są wymagane.

4.4. Polecenia zarządzania plikami i katalogami

Oprócz samego kopiowania plików, za pomocą poleceń zarządzania możemy wykonać kilka operacji na serwerze takich jak np. przeglądania zawartości serwera, zmiany nazwy katalogu itp. W tabeli 4 przedstawia ich zestawienie.

Tabela 4 – Polecenia FTP służące do zarządzania plikami i katalogami [1].

Polecenie	Opis
DELETE plikserwer	Usuwa plik o nazwie plikserwer z serwera FTP.
MDELETE plikserwer [...]	Usuwa wszystkie pliki odpowiadające opartemu na symbolach wieloznacznych wzorcowi plikserwer
LCD	Polecenie Local Change Directory (Zmień katalog lokalny) zmienia lokalny katalog bieżący. Jego podstawowym zastosowaniem jest określanie katalogu, do którego kopiowane będą pliki z serwera.
CD [katalog]	Polecenie Change Directory (Zmień katalog) zmienia katalog bieżący na serwerze.
CDUP	Polecenie Change Directory Up (Zmień katalog „do góry”) zmienia katalog bieżący na serwerze na katalog o poziom wyżej. Zostało ono wprowadzone ze względu na zróżnicowanie reprezentacji katalogu nadrzędnego w różnych systemach.

MKDIR katalog	Polecenie Make Directory (Utwórz katalog) zakłada nowy katalog na serwerze FTP.
RMDIR katalog	Polecenie Remove Directory (Usuń katalog) usuwa katalog na serwerze.
DIR	Wyświetla zawartość bieżącego katalogu serwera ze szczegółami. Może ona zostać zapisana do pliku.
LS	Polecenie List wyświetla zawartość bieżącego katalogu serwera w formie skróconej. Podstawowe przełączniki tego polecenia to -F i -all. Pierwszy powoduje wyświetlanie nazw podkatalogów ze znakiem łamania (/) na końcu. Użycie drugiego prowadzi do otrzymania takiego wyniku, jak po wprowadzeniu polecenia dir.
PWD	Wyświetla nazwę bieżącego katalogu serwera.
RENAME nazwa1Nazwa2	Zmienia nazwę pliku na serwerze z nazwa1 na nazwa 2.

4.5. Polecenia pomocy i kontroli stanu sesji

Posługiwanie się poleceniami w trybie tekstowym jest czasami kłopotliwe, gdyż nie zawsze jesteśmy pewni ich składni, bądź nie wszystkie znamy. Warto jest znać więc polecenia pomocy, które pozwalają nam uzyskać dodatkowe informacje. Natomiast polecenia kontroli stanu sesji pozwolą nam uzyskać informacje dotyczące aktualnych ustawień. Tabela 5 przedstawia polecenia tego rodzaju.

Tabela 5 – Polecenia FTP związane z pomocą i kontrolą stanu sesji [1].

Polecenie	Opis
!	Powoduje wyjście z sesji FTP do lokalnego interpretatora poleceń lub powłoki systemowej. Powrót do sesji zapewnia zazwyczaj wprowadzenie polecenia <code>exit</code> .
?	Wyświetla wszystkie polecenia dostępne w programie klienta FTP.
HELP	Funkcjonuje tak samo jak polecenie <code>?</code> .
STATUS	Wyświetla informacje o bieżącym stanie sesji FTP. Obejmują one tryb transmisji, stan połączenia, ustawienia wyświetlania komunikatów i wartość limitu czasu.
VERBOSE	Przełącza tryb wyświetlania informacji (tzw. tryb informacji pełnej). Gdy jest włączony, użytkownik otrzymuje informacje o wszystkich odpowiedziach serwera FTP oraz szybkościach przesyłania.

4.6. Kody odpowiedzi serwera FTP

Na każde nasze polecenie serwer odpowiada specjalnym kodem, który mówi czy polecenie zostało wykonane poprawnie, czy może wystąpił błąd. W przypadku niepowodzenia wykonania komendy serwer przesyła odpowiedni kod błędu, który informuje co klient powinien zrobić.

Wszystkie kody składają się z trzech znaków. W tabeli 6 przedstawiono 5 dopuszczalnych wartości pierwszej pozycji kodu odpowiedzi.

Tabela 6 – Wartości pierwszej pozycji kodu odpowiedzi serwera FTP [1].

Wartość	Nazwa	Opis
1yz	Pozytywna odpowiedź wstępna	Żądana akcja została podjęta. Kolejna odpowiedź zostanie wysłana przed osiągnięciem gotowości do przyjęcia kolejnego polecenia. Jednorazowo może zostać wysłana tylko jedna odpowiedź wstępna.
2yz	Pozytywna odpowiedź końcowa	Żądana akcja została poprawnie wykonana i serwer gotów jest na przyjęcie od klienta kolejnego polecenia.
3yz	Pozytywna odpowiedź pośrednia	Serwer zaakceptował polecenie, ale oczekiwane są dalsze dane. Jest to typowa odpowiedź, gdy oczekiwane jest określone następstwo poleceń, jak <code>pass</code> po <code>user</code> .
4yz	Negatywna odpowiedź tymczasowa	Przedłożone serwerowi polecenie nie zostało poprawnie wykonane. Jest to jednak tymczasowy błąd w połączeniu i polecenie powinno zostać przesłane ponownie.
5yz	Pozytywna odpowiedź trwała	Żądana akcja nie mogła zostać wykonana. Typowe przyczyny takiej odpowiedzi to błąd we wpisywaniu polecenia oraz brak przypisania użytkownikowi odpowiednich uprawnień.

W celu większego sprecyzowania odpowiedzi serwera poniżej przedstawiono wartości drugiej pozycji kodu. Dopuszczalne jej wartości przedstawia tabela 7.

Tabela 7 – wartość drugiej pozycji kodu odpowiedzi serwera FTP [1].

Wartość	Nazwa	Opis
x0z	Składnia	Błąd wynika z niewłaściwej składni albo też wydania polecenia poprawnego, ale w nieodpowiednim momencie.
x1z	Dane	Kod wykorzystywany w odpowiedziach na polecenia pomocy i kontroli stanu sesji, jak <code>help</code> i <code>status</code> .
x2z	Połączenia	Kod używany w odpowiedziach odnoszących się do stanu połączenia danych.
x3z	Uwierzytelnianie i rejestracja	Kod wykorzystywany podczas procesu uwierzytelniania użytkownika.
x4z	Nieokreślony	Kod jeszcze nieużywany.

x5z | System plików Informacja o stanie systemu plików serwera lub klienta FTP.

Aby jeszcze precyzyjniej określić odpowiedź serwera można przeanalizować trzecią pozycję kodu, jednak w tym opracowaniu zostało to pominięte

5. ZAGADNIENIA BEZPIECZEŃSTWA FTP

Hasła FTP przesyłane są tekstem jawnym a w dzisiejszych czasach sieć Internet nie jest tak bezpieczna, jak w momencie powstawania protokołu FTP. Zatem istnieje potrzeba zmiany sposobu przesyłania haseł, gdyż takie postępowanie umożliwia ich przechwytywanie i nieautoryzowany dostęp do serwerów plikowych.

Mechanizmy zabezpieczające powinny również zapewniać uwierzytelnianie serwerów dla uniknięcia podszywania się oraz szyfrowanie informacji przesyłanych kanałem danych [1]. Poniższa tabela 8 przedstawia polecenia zapewniające znacznie większe bezpieczeństwo przesyłania danych i autoryzacji dostępu, używanych w protokole FTP opcjonalnie.

Tabela 8 – Polecenia rozszerzeń bezpieczeństwa FTP [1].

Polecenie	Pełna nazwa	Opis
AUTH	Mechanizm uwierzytelniania/zabezpieczania	Żądanie klienta dotyczące stosowania określonego mechanizmu ochrony przesyłanych danych. Może być przesyłane kilkakrotnie do czasu wynegocjowania między klientem a serwerem metody uwierzytelniania.
ADAT	Dane uwierzytelniania/zabezpieczeń	Polecenie pozwalające przesłać dodatkowe dane określające opcjonalne elementy wybranego mechanizmu zabezpieczeń.
PROT	Poziom ochrony kanału danych	Określa poziom ochrony, który będzie stosowany przez stacje klienta i serwera w odniesieniu do kanału danych. Ustawienie <code>clear</code> (Jawny) wskazuje na zwykłe przesyłanie danych, <code>safe</code> (Bezpieczny), sprawdzanie integralności danych, <code>confidential</code> (Poufny), szyfrowanie, <code>private</code> (Prywatny) -jednoczesne szyfrowanie i sprawdzanie integralności.
PBSZ	Rozmiar bufora ochrony	Określa największy dopuszczalny rozmiar kodowanych bloków danych, które będą przesyłane podczas wymiany plików. Podawany w bajtach.
CCC	Kanał poleceń jawnych	Kończy wykorzystywanie określonego mechanizmu zabezpieczającego. Wykorzystywane najczęściej, gdy w sieci stosowane są zabezpieczenia na poziomie protokołu TCP. Po zakończeniu uwierzytelniania połączenia, polecenie <code>ccc</code> umożliwia zakończenie dalszych procedur sprawdzania integralności danych i uwierzytelniania.
MIC	Polecenie ochrony Integralności	Wykorzystywane do transmisji danych przy poziomie ochrony ustawionym na <code>safe</code> .

CONF	Polecenie ochrony poufności	Wykorzystywane do transmisji danych przy poziomie ochrony ustawionym na <code>Confidential</code> .
ENC	Polecenie ochrony prywatności	Wykorzystywane do transmisji danych przy poziomie ochrony ustawionym na <code>Private</code> .

Korzystanie z mechanizmów zabezpieczających rozpoczyna klient FTP, podając przy użyciu polecenia `AUTH`, z jakiego mechanizmu bezpieczeństwa zamierza korzystać. Serwer może zaakceptować ten mechanizm, odmówić jego stosowania lub też całkowicie odrzucić polecenie (gdy nie posiada mechanizmów zabezpieczeń FTP).

Jeżeli zabezpieczenia, z których korzysta klient wymagają dodatkowych informacji, można je przesłać do serwera za pomocą polecenia `ADAT`. Wymiana informacji trwa do momentu dokładnego określenia używanych zabezpieczeń.

Po ustanowieniu bezpiecznego połączenia, może zostać określony typ ochrony danych. Służy do tego polecenie `PROT`. W zależności od wybranego poziomu, do realizacji bezpiecznej transmisji kanałem danych wykorzystywane będzie polecenie `MIC`, `CONF` lub `ENC`. Rozmiar pakietów danych określa się poleceniem `PBSZ` [1].

6. WYKORZYSTYWANIE ARCHIE DO PRZESZUKIWANIA ZASOBÓW FTP

Pomimo, że dysponujemy odpowiednim protokołem do przesyłania plików, to jednak bardzo ciężko jest znaleźć w Internecie interesujący nas plik. Aby nam w tym dopomóc w Sieci znajdują się serwery Archie, na których zgromadzony jest spis anonimowych serwerów FTP oraz znajdujących się na tych serwerach plików. Wyszukiwanie odbywa się na podstawie nazwy pliku, lub jego opisie. Wyszukiwanie odpowiednich lokalizacji plików za pomocą Archie odbywa się za pomocą Telnetu, bądź specjalnych programów.

W tabeli 9 przedstawiono kilka dostępnych na świecie serwerów Archie.

Tabela 9 – Serwery Archie i ich lokalizacja

Kraj	Ośrodek Archie
Kanada	archie.mcgill.ca
Finlandia	archie.funet.fi
Japonia	archie.wide.ap.jp
Tajwan	archie.ncu.edu.tw
USA	archie.internic.net archie.rutgers.edu
Wielka Brytania	archie.doc.ic.ac.uk

Po wybraniu interesującego nas serwera Archie postępujemy według następującego planu:

1. Łączymy się narzędziem Telnet z odpowiednim serwerem i logujemy jako Archie:

```
telnet archie.ncu.edu.tw Trying
193.23.78.9... Connected to
services.bunyip.com,
Escape character is '^]'.
SunOS UNIX (service5.bunyip.com)
```

```
login: archie
Note: The 'server' variable no longer has any effect for
searches. If you want to perform a search on another
archie server you should login to that server.
```

```
# Bunyip Information Systems, Inc., 1993, 1994, 1995
# Terminal type set to 'vt100 24 80'.
# 'erase' character is '?'.
# 'search' (type string) has the value 'sub' .
archie>
```

2. Ustawiamy opcję Sortby, w celu wybrania odpowiedniego uporządkowania wyświetlanych informacji (np. filename - nazwa pliku, time - data ostatniej modyfikacji pliku, size - rozmiar pliku):

```
archie> set sortby size
```

3. Dalej powinniśmy ustawić liczbę wyświetlanych miejsc przechowywania pliku, gdyż zazwyczaj jest ich bardzo dużo.

```
archie> set maxhits 10
```

4. W tym momencie rozpoczyna się właściwe wyszukiwanie pliku. Jeżeli np. chcemy znaleźć plik nc.exe wpisujemy:

```
archie> find nc.exe
```

```
# Search type: sub.
working...
ftp://ftp.cciw.ca/pub/u009/ nc.exe
      Date: 10:33 15 Oct 2001      Size: 626991
      bytes
ftp://ftp.task.gda.pl/vol/d4/papa.indstate.edu/winsock-1/ "-
Windows 95 /Misc_Utils/ Cormpression/nc.exe
      Date: 05:36 6 Sep 2001      Size: 41 bytes
ftp://ftp.amu.edu.pl/pub/msdos/windows/win95/corapress/nc.exe
      Date: 16:49 13 Jul 2001     Size: 1029615
      bytes
ftp://ftp.cyf-kr.edu.pl/pub/mirror/WinSite/win95/
"•miscutil/nc.exe
      Date: 21:19 5 Jun 2001      Size: 2590577
      bytes
ftp://ftp.sogang.ac.kr/.9/sogang-net/hong/ nc.exe
      Date: 11:00 15 May 2001     Size: 9463 bytes
ftp://hangout.rutgers.edu/pub/accounting/gsm/mba/ravid/ nc.exe
      Date: 19:40 3 Oct 2001     Size: 708608 bytes
ftp://ftp.task.gda.pl/vol/d4/papa. indstate.edu/winsock-1/ '-
•WindowsNT/Misc^tils/ nc.exe
      Date: 16:59 27 Mar 2001     Size: 5236266
      bytes
ftp://ftp.sogang.ac.kr/.26/winsock~1/WindowsNT/
Misc_Utils/ nc.exe
      Date: 03:21 18 Jul 2001     Size: 5236266
      bytes
ftp://ftp.task.gda.pl/mirror/www.pdacentral.corn/webhome/server/
•*htdocs/ceraonste/r/files/nc.exe
      Date: 11:00 23 Jan 2001     Size: 629038
      bytes
ftp://ftp.sogang.ac.kr/.19/win95/miscutil/ nc.exe
```

Date: 13:44 14 Apr 2001 Size: 2584150
bytes

5. Po zapisaniu położenia szukanego pliku zakańczamy sesje poleceniem QUIT
archie> quit
Bye [1].

LITERATURA

- [1] Brian Komar "Administracja sieci TCP/IP dla każdego" Helion Gliwice 2000
- [2] Internet: http://www1.zetosa.com.pl/sioux/co_to_jest.html
- [3] Internet: <http://rainbow.mimuw.edu.pl/SO/Linux/Temat08/FTP.html>