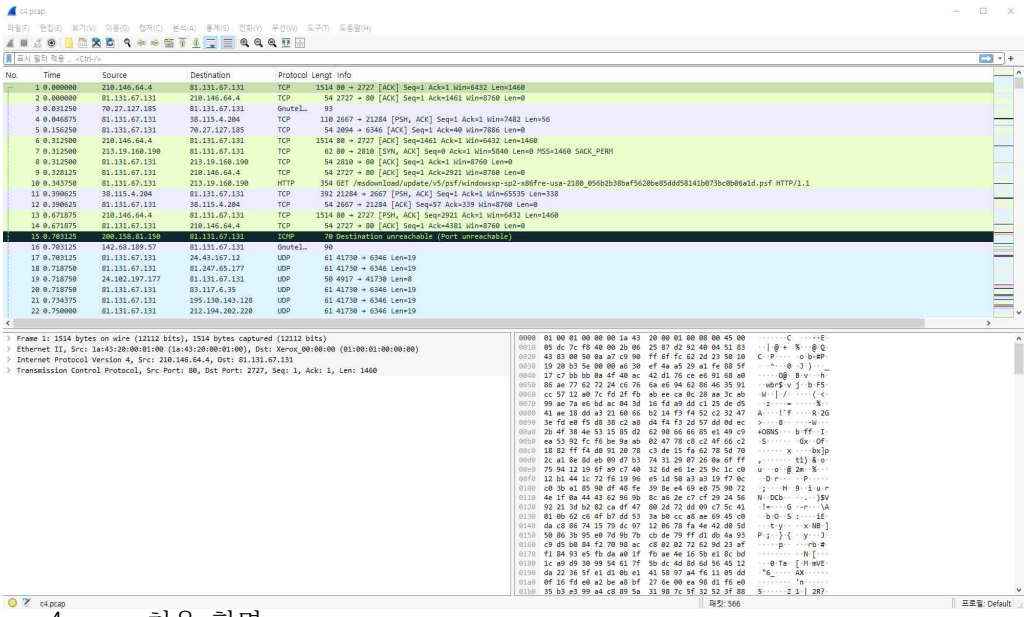
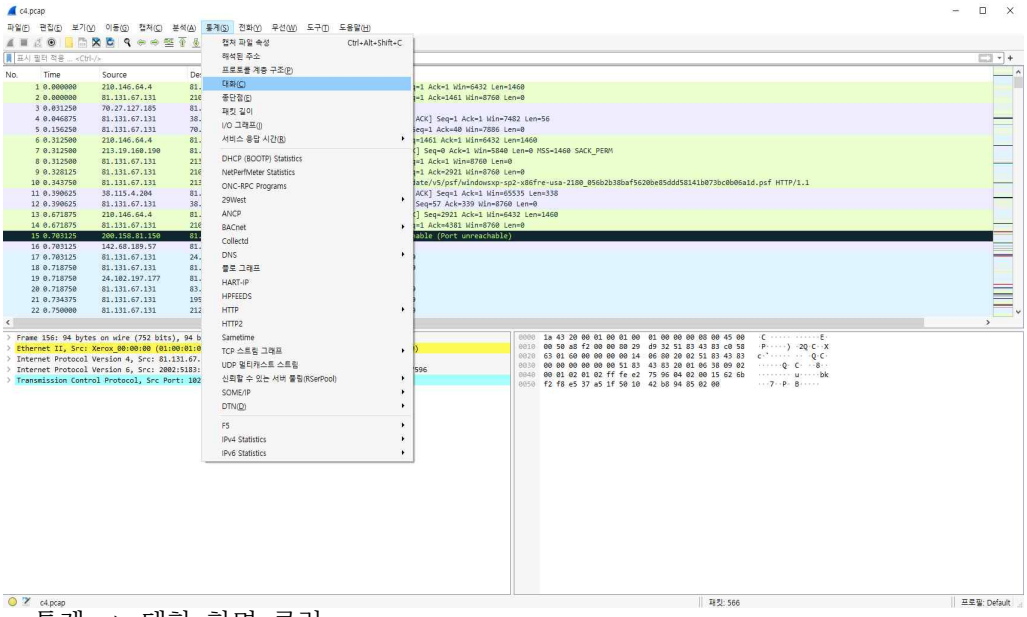
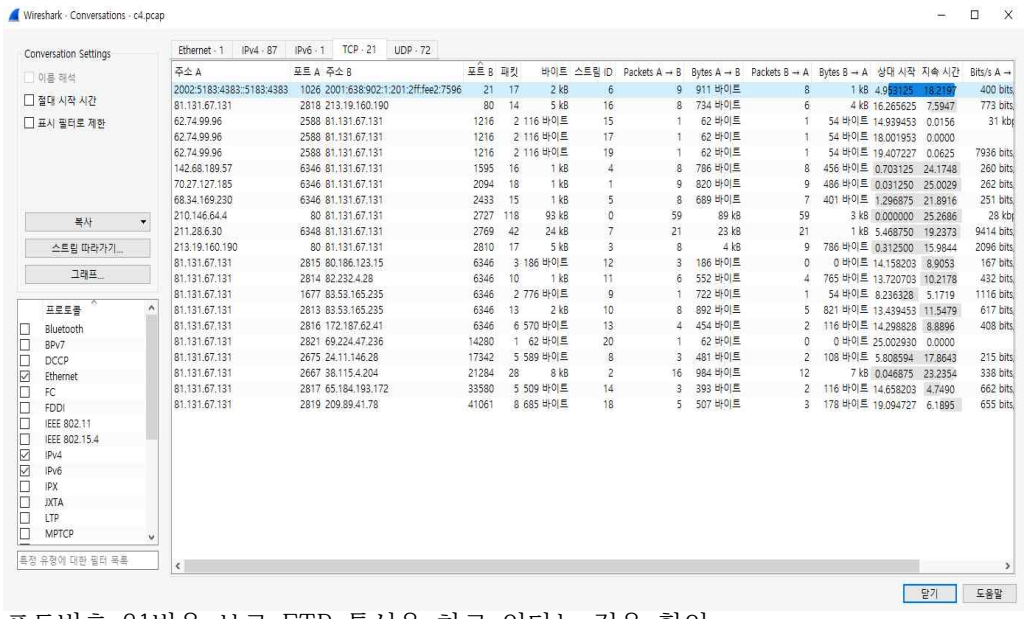


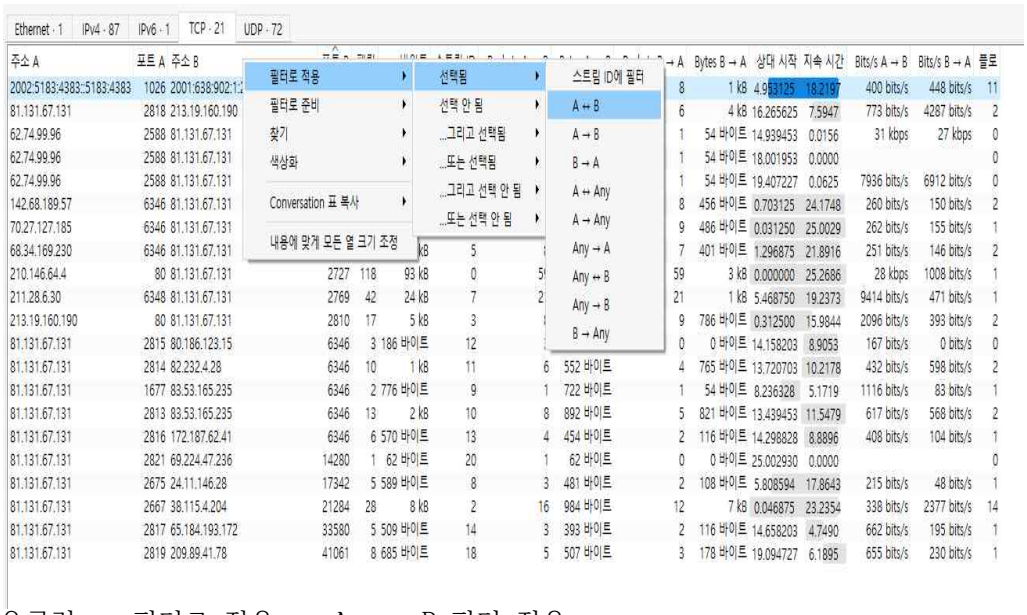
- c4.pcap 처음 화면



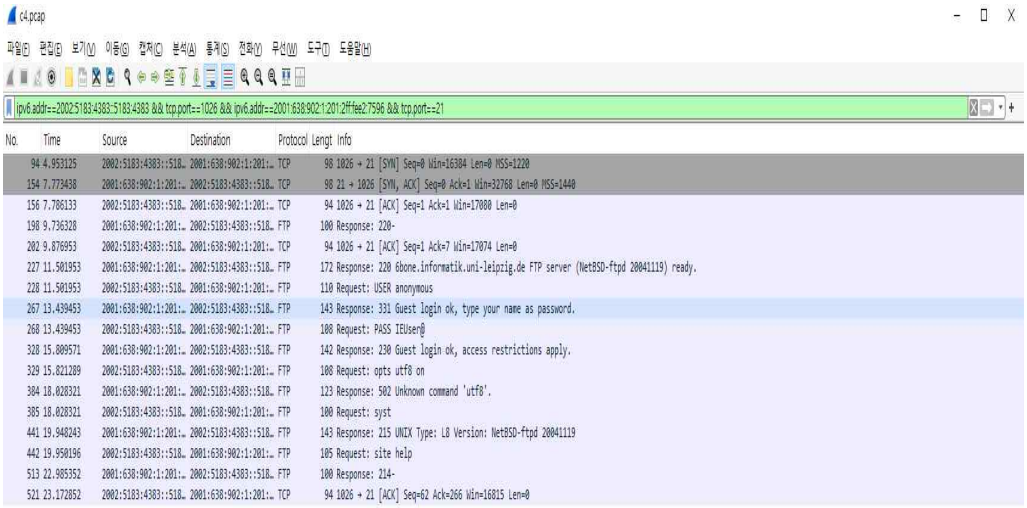
- 통계 -> 대화 화면 클릭



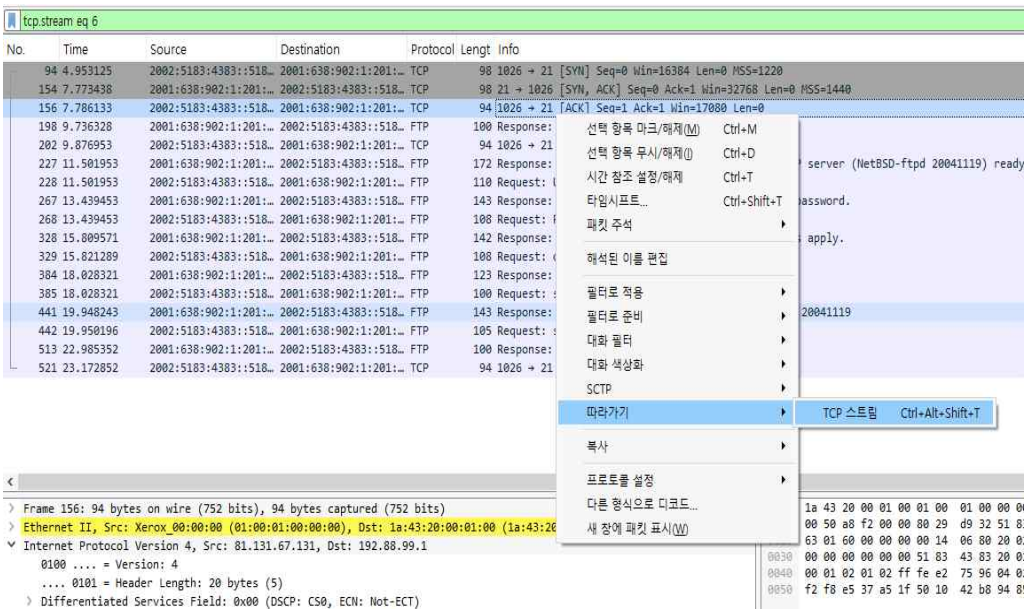
포트번호 21번을 보고 FTP 통신을 하고 있다는 것을 확인

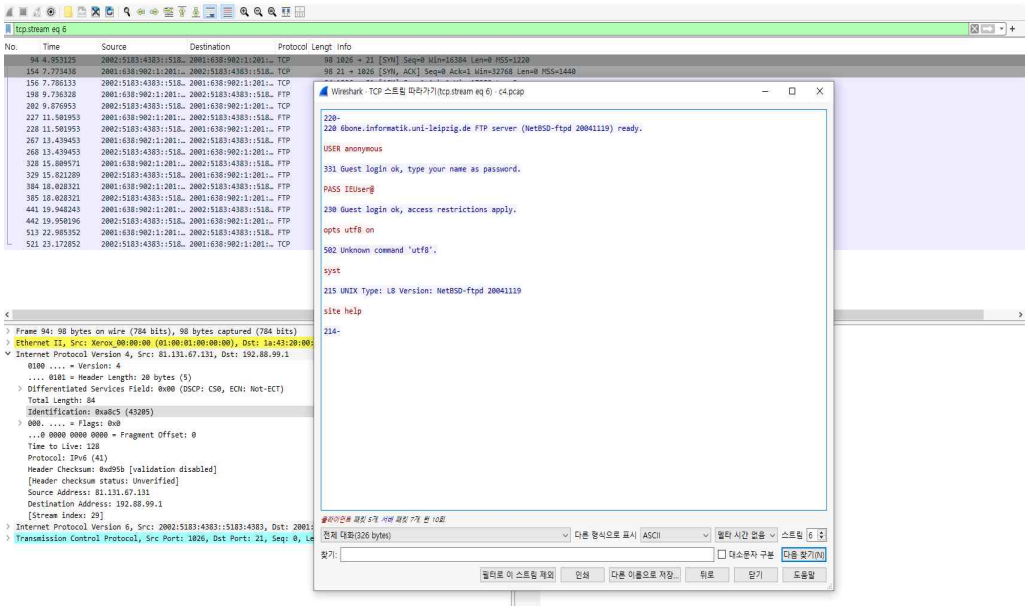


우클릭 -> 필터로 적용 -> A <-> B 필터 적용



필터 적용된 화면





(1) TCP SYN 패킷 분석

- 클라이언트가 서버로 연결 요청

```
94 4.953125      2002:5183:4383::518… 2001:638:902:1:201:… TCP
```

```
Internet Protocol Version 4, Src: 81.131.67.131, Dst: 192.88.99.1
```

클라이언트 주소 : 81.131.67.131

서버 주소 : 192.88.99.1

```
Transmission Control Protocol, Src Port: 1026, Dst Port: 21, Seq: 0, Len: 0
   Source Port: 1026
   Destination Port: 21
   [Stream index: 6]
   [Stream Packet Number: 1]
▸  [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 0]
   Sequence Number: 0    (relative sequence number)
   Sequence Number (raw): 1651241719
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 0
   Acknowledgment number (raw): 0
   0110 .... = Header Length: 24 bytes (6)
```

클라이언트에서 사용한 임시 포트 번호 : 1026

목적지 포트 : 21

Sequence number

상대적 번호 : 0

절대 번호 : 62 6b f2 f7

(2) TCP SYN, ACK 패킷 분석

- 클라이언트가 서버로 보내는 SYN, ACK 패킷

```
Transmission Control Protocol, Src Port: 21, Dst Port: 1026, Seq: 1, Ack: 1, Len: 6
   Source Port: 21
   Destination Port: 1026
   [Stream index: 6]
   [Stream Packet Number: 4]
▸  [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 6]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 3845629215
   [Next Sequence Number: 7    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 1651241720
   0101 .... = Header Length: 20 bytes (5)
```

Sequence number

상대적 번호 : 0

절대 번호 : e5 37 a5 1e

Acknowledgment number

상대적 번호 : 1

절대 번호 : 62 6b f2 f8

(3) TCP ACK 패킷 분석

- 서버가 클라이언트로 ACK 패킷

```
Transmission Control Protocol, Src Port: 1026, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
   Source Port: 1026
   Destination Port: 21
   [Stream index: 6]
   [Stream Packet Number: 3]
▸  [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 0]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 1651241720
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 3845629215
   0101 .... = Header Length: 20 bytes (5)
```

Sequence number

상대적 번호 : 1

절대 번호 : 62 6b f2 f8

두 번째 패킷의 acknowledge number와 같은 값이다.

Acknowledgment number

상대적 번호 : 1

절대 번호 : e5 37 a5 1f

정리

4번째 줄 FTP 기준

출발지 mac 주소 : 01:00:01:00:00:00

목적지 mac 주소 : 1a:43:20:00:01:00

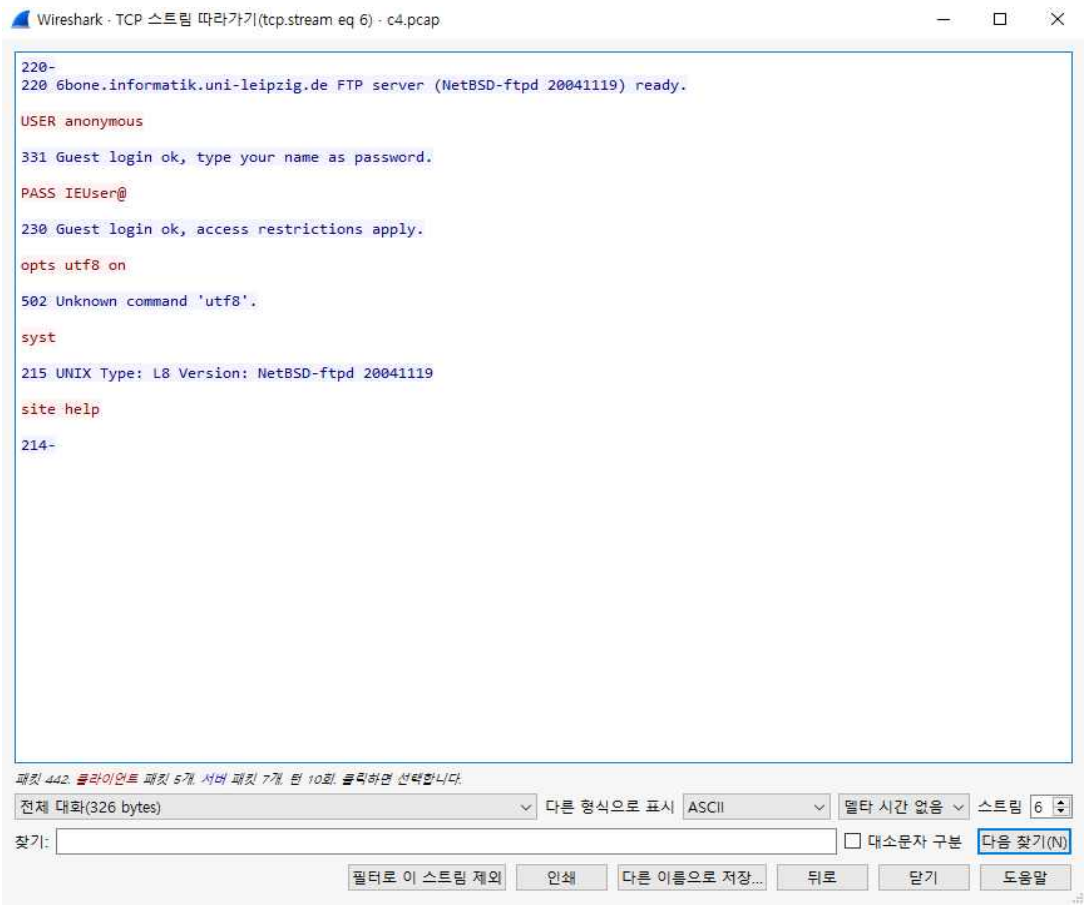
출발지 ip 주소 : 139.18.25.33

목적지 ip 주소 : 81.131.67.131

TTL : 16

출발지 포트 : 21

목적지 포트 : 1026



220- 서버가 클라이언트와 연결이 성공적으로 이루어짐

anonymous 계정을 입력

IEUser@ 암호를 입력

opts utf8 on = 잘못된 명령어 입력한 상태

syst = 시스템 타입(운영체제)

site help = 도움말

214- = 서버가 클라이언트의 요청을 성공적으로 처리, 요청된 도움말 정보를 보내기 시작

FTP 평문 통신

FTP(File Transfer protocol)는 파일 전송에 자주 사용되는 프로토콜
평문으로 통신 정보가 전송되기 때문에 보안에 취약한 문제점이 있음, 사용자의 ID, 비밀번호, 전송되는 파일 내용 등이 암호화되지 않은 상태로 노출될 수 있어 해킹이나 데이터 유출의 위험에 노출

대응방안

1. SFTP(SSH File Transfer Protocol) 사용
   SSH 프로토콜을 사용하여 모든 통신을 암호화
   파일 전송뿐만 아니라, 원격 명령 실행, 파일 시스템 접근 등 다양한 기능 제공

*SSH(Secure Shell) : 다른 컴퓨터에 안전하게 연결하여 명령을 실행하거나 파일을 전송하는 데 사용하는 프로토콜

2. FTPS (SSL/TLS) 사용
   SSL/TLS 프로토콜을 사용하여 FTP 통신을 암호화
3. FTP 서버 설정 강화
   익명 접속 금지
   주기적인 암호 변경
   특정 IP 주소나 네트워크 대역에서만 접속을 허용
   주기적인 FTP 서버 로그를 분석
4. 방화벽 설정
   FTP 서비스에 대한 접근을 제한, 특정 포트만 허용하도록 설정
5. 침입 탐지 시스템(IDS) 사용

FTP에 대한 개요, 무슨 방식인지
포트 몇 번 쓰는지
응답코드
len 값 왜 7 되는지 정리

FTP(File Transfer Protocol)는 네트워크를 통해 파일을 전송하기 위한 표준 통신 프로토콜
클라이언트와 서버 간에 파일을 업로드하거나 다운로드하는 데 사용

FTP 포트 번호
기본 포트 번호:
포트 21: FTP 제어 연결(Control Connection)을 위한 포트.
포트 20: 데이터 전송(Data Connection)에 사용되는 기본 포트 (Active Mode에서 사용).
Passive Mode:
데이터 전송 시, 서버가 임의의 고정 범위 포트를 사용.
Passive Mode에서 사용하는 포트는 서버 설정에 따라 다르며, 방화벽을 통해 허용해야 함.

주요 특징

1. 클라이언트-서버 구조:
    - FTP는 클라이언트와 서버 간 통신을 기반으로 작동합니다.
    - 클라이언트는 파일 요청을 하고, 서버는 요청에 응답하여 파일을 전송합니다.
2. 데이터 및 제어 연결:
    - FTP는 두 개의 연결을 사용합니다:
        - 제어 연결: 명령 및 응답을 주고받는 용도.
        - 데이터 연결: 실제 파일 데이터 전송 용도.
3. 전송 모드:
    - Active Mode: 서버가 클라이언트로 데이터 연결을 초기화.
    - Passive Mode: 클라이언트가 서버로 데이터 연결을 초기화.
4. 전송 방식:
    - ASCII 모드: 텍스트 파일 전송에 적합.
    - Binary 모드: 이미지, 비디오, 프로그램 등 바이너리 파일 전송에 사용.
5. 인증:
    - 사용자 이름과 비밀번호를 요구하는 경우가 일반적.
    - 익명(Anonymous) FTP를 통해 비회원 접근도 지원 가능.

장점

대량의 데이터를 안정적으로 전송할 수 있음.

파일 전송 속도가 빠르고, 대기열 및 재시도 기능을 지원.

다양한 플랫폼 간 호환 가능.

단점

보안 문제: 데이터와 인증 정보가 암호화되지 않고 평문으로 전송되므로 도청의 위험이 있음.

FTP를 통한 공격: FTP 서버가 잘못 설정된 경우 무단 접근 가능성.

FTP를 보완한 보안 프로토콜

FTPS (FTP Secure):

SSL/TLS 암호화를 추가하여 보안을 강화.

SFTP (SSH File Transfer Protocol):

SSH 기반으로 동작하며, 암호화 및 데이터 무결성을 제공.

FTP 응답 코드

FTP는 서버와 클라이언트 간 통신에서 상태를 나타내기 위해 3자리 숫자로 된 응답 코드를 사용

첫 번째 자리: 상태 유형.

1xx: 정보 응답 (작업 진행 중).

2xx: 성공 응답 (작업 완료).

3xx: 추가 작업 필요 (다음 명령 필요).

4xx: 일시적 실패 (재시도 가능).

5xx: 영구적 실패 (명령 거부).

두 번째 자리: 응답의 세부 카테고리.

x0x: 구문 관련 응답.

x1x: 정보 요청 응답.

x2x: 연결 관련 응답.

x3x: 인증 및 권한 관련 응답.

x5x: 파일 시스템 관련 응답.