Report Assignment 1

Baiardi Martina, Lombardini Alessandro

TASK 1

# Phase-0

Dopo aver aperto Wireshark per analizzare il traffico dei pacchetti in rete, è stata selezionata l’interfaccia Wi-Fi.

Immagine che contiene screenshot

Descrizione generata automaticamente

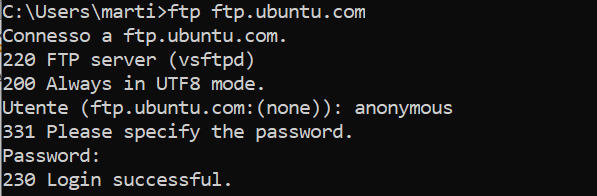
Successivamente è stato applicato il filtro “*ftp.port == 21*” per analizzare i pacchetti appartenenti ad una sessione ftp.

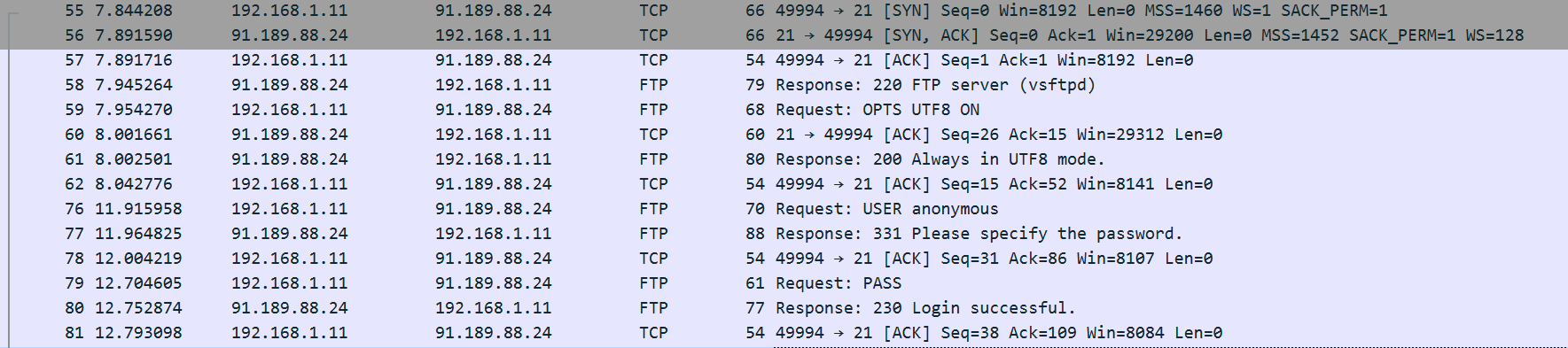
Immagine che contiene screenshot

Descrizione generata automaticamente

# Phase-1

È stata inizializzata una sessione FTP presso il server [ftp.ubuntu.com](ftp://ftp.ubuntu.com), sono stati inseriti username *anonymous* e password nulla.





# Phase-2

Sono stati inseriti una serie di comandi ftp sul terminale:

1. ?: per visualizzare l’elenco dei comandi FTP disponibili
2. ls: per visualizzare il contenuto della directory corrente
3. cd ubuntu: per modificare la directory corrente in ubuntu
4. ls: per visualizzare il contenuto della cartella ubuntu
5. get ls-lR.gz: per scaricare il file *ls-lR.gz*
6. exit: per terminare la sessione FTP

Una volta eseguiti tutti i comandi è stato analizzato il traffico generato attraverso Wireshark.

Immagine che contiene testo, screenshot

Descrizione generata automaticamente

Immagine che contiene screenshot

Descrizione generata automaticamente

TASK 2

Questions about Phase-0

1. Which is the most appropriate filter that allows you to display only traffic belonging to the FTP session? To answer this question, consider that there are multiple filters that you can adopt to achieve such goal, but one of those filters is the most suitable one.

Il filtro più appropriato per evidenziare un traffico FTP quando non si è a conoscenza dell’indirizzo ip del server è *tcp.port == 21*, in quanto permette di visualizzare i pacchetti scambiati con la well-known port del server dove tutte le richieste dei client vengono spedite.

Immagine che contiene screenshot

Descrizione generata automaticamente

# Questions about Phase-1

1. Which is the IP address of the Ubuntu FTP server?

L'indirizzo del server ftp Ubuntu che ha risposto alla richiesta di connessione è 91.189.88.162.

2. Which is the TCP port adopted by your FTP client in order to start the TCP three-way-handshake to the Ubuntu FTP server?

La porta utilizzata dal client per iniziare la connessione con il server ftp Ubuntu è la 50088.

3. Which are the messages, Request and Response, exchanged during this Phase? Describe who sends this message to who (i.e., from client to server, or vice-versa).   
Also, indicate:   
 i) if those messages belongs to the command or to the data connection;

ii) which TCP ports are used during this exchange.

Dopo la three-way handshake avviata dal client verso il server, i messaggi di request e response sono i seguenti:

Immagine che contiene screenshot

Descrizione generata automaticamente

Packet No. :

1. Response (server -> client): il server si identifica al client
2. Request (client -> server): il client chiede di utilizzare la codifica UTF8
3. Response (server -> client): il server dichiara di essere già in codifica UTF8
4. Request (client -> server): il client chiede di effettuare il login con USER anonymous
5. Response (server -> client): il server chiede di specificare la password
6. Request (client -> server): il client invia la PASS vuota
7. Response (server -> client): il server comunica che il login è avvenuto con successo

Tutti questi messaggi appartengono alla “*command connection*”, infatti le porte coinvolte sono la 50088 per il client e la 21 per il server.

4. Is there any message exchanged on the data connection? Hint: to answer this question, consider to change your filter in ip.addr == <ubuntu\_ftp\_server\_IP\_Addr>

Durante la fase di connessione al server non viene scambiato nessun messaggio sulla “data connection”, infatti non viene mai aperta.

Immagine che contiene screenshot, interni

Descrizione generata automaticamente

# Questions about Phase-2

**Step 1: ?**, the question mark allows to display which command can be performed on the FTP server.

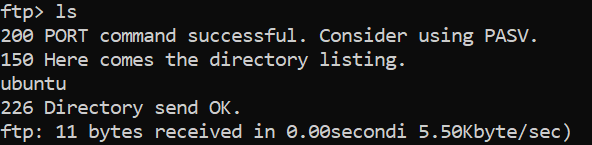
Immagine che contiene testo

Descrizione generata automaticamente

1. Which messages, if any, are exchanged between client and server?

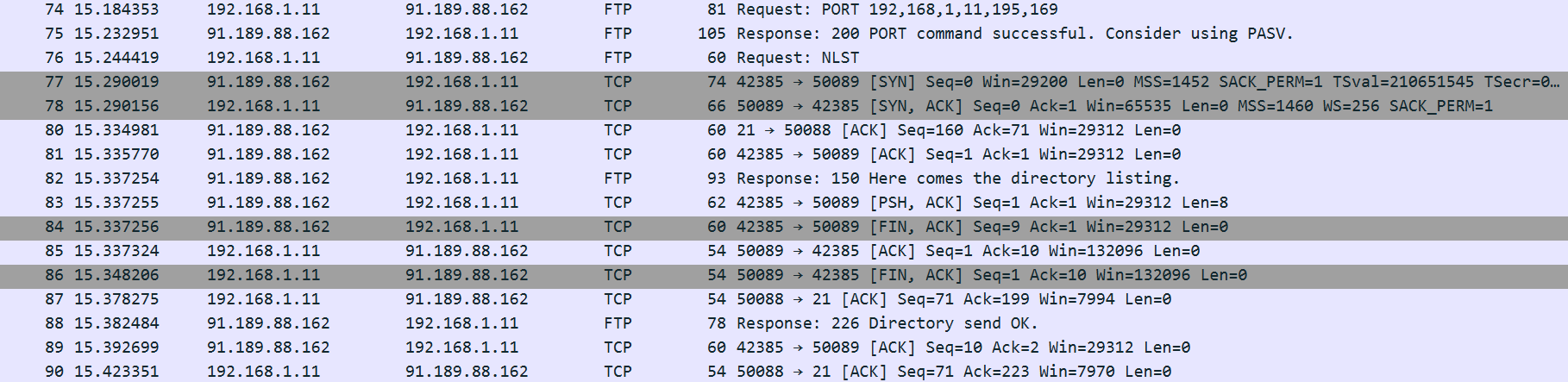
Per questo comando non vengono inviati messaggi al server. Le informazioni relative ai comandi utilizzabili sul server FTP sono contenute nell’applicazione dell’utente, che quindi può direttamente rispondere senza dover fare richieste al server.

**Step 2: ls**, this command allows to display the content of the current folder.



1. Which messages, if any, are exchanged between client and server?

I messaggi scambiati tra client e server per eseguire il comando sono:



I messaggi Request e Response scambiati tra client e server sono quindi questi:

Immagine che contiene screenshot

Descrizione generata automaticamente

2. On which connection, command or data, are those message exchanged?

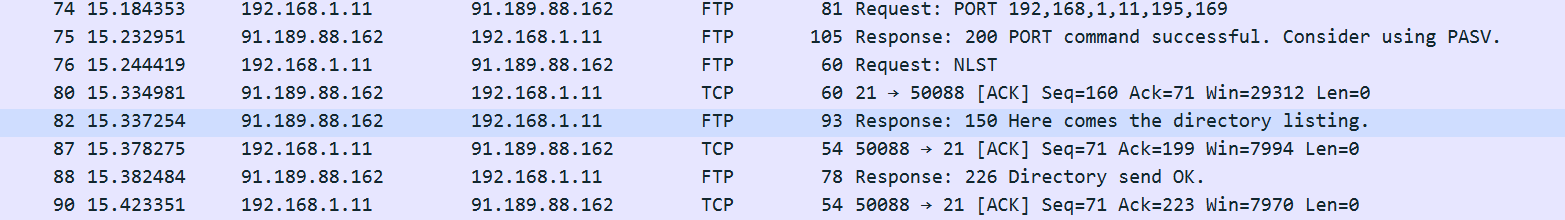
I messaggi contenenti le Request e le Response sono inviati sulla connessione di controllo, mentre le informazioni richieste dal comando NLST sono inviate sulla connessione dati.

3. In case messages are exchanged on data connection:

1. Is data connection opened in ACTIVE or PASSIVE mode? Please, motivate your answer by telling your consideration
2. Whether connection is ACTIVE or PASSIVE, which TCP port is used to establish the connection?

La connessione dati è aperta in modo attivo, perchè il server effettua la prima richiesta di connessione verso la porta designata dal client nel comando PORT (cioè la 50089). La porta utilizzata per stabilire la connessione è la 42385 del server.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Sul collegamento di controllo sono scambiati i seguenti pacchetti. 

I pacchetti di Request e Response sono i seguenti.

Packet No. :

1. Il client effettua una Request di connessione attiva al server tramite il comando PORT all’interno del quale comunica la porta sulla quale il server deve effettuare la richiesta.
2. Il server risponde che ha accettato la richiesta di connessione attiva alla porta specificata.
3. Il client effettua una Request al server del comando NLST
4. Il server comunica al client che sta trasmettendo sulla connessione dati le informazioni richieste.
5. il server informa il client che le informazioni sono state inviate con successo.

Sul collegamento dati, invece, sono scambiati i seguenti pacchetti.Immagine che contiene screenshot

Descrizione generata automaticamente

In questa connessione non vengono scambiati pacchetti Request e Response, ma semplicemente le informazioni relative al contenuto della directory, richieste con NLST. Il collegamento poi chiuso appena viene terminato il trasferimento.

**Step 3: cd <folder>**, adopt this command to enter the folder displayed at step 2.

Immagine che contiene oggetto

Descrizione generata automaticamente

1. Which messages, if any, are exchanged between client and server?

I messaggi scambiati tra client e server per eseguire il comando sono:

Immagine che contiene screenshot

Descrizione generata automaticamente

I messaggi Request e Response scambiati tra client e server sono quindi questi:



2. On which connection, command or data, are those message exchanged?

I messaggi per questo comando sono trasferiti tutti sulla connessione di controllo tra server e client. La connessione dati non viene mai aperta.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Sul collegamento di controllo sono scambiati i seguenti pacchetti.

Immagine che contiene screenshot

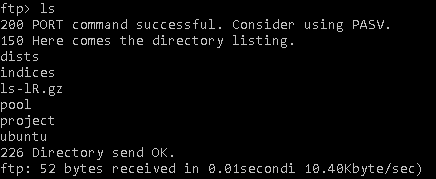
Descrizione generata automaticamente

Packet No. :

1. Il client effettua una Request al server di cambiare la directory corrente con ./ubuntu tramite il comando CWD
2. Il server comunica al client che la directory è stata cambiata con successo con quella desiderata

Sulla connessione dati, invece, non sono scambiati pacchetti.

**Step 4: ls**, enter again this command.



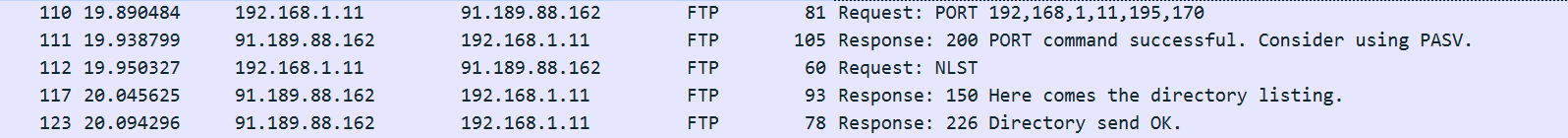
1. Which messages, if any, are exchanged between client and server?

I messaggi scambiati tra client e server per eseguire il comando sono:

Immagine che contiene interni, parete

Descrizione generata automaticamente

I messaggi Request e Response scambiati tra client e server sono quindi questi:



2. On which connection, command or data, are those message exchanged?

I messaggi contenenti le Request e le Response sono inviati sulla connessione di controllo, mentre le informazioni richieste dal comando NLST sono inviate sulla connessione dati.

3. In case messages are exchanged on data connection:

1. Is data connection opened in ACTIVE or PASSIVE mode? Please, motivate your answer by telling your consideration
2. Whether connection is ACTIVE or PASSIVE, which TCP port is used to establish the connection?

La connessione dati è aperta in modo attivo, perchè il server effettua la prima richiesta di connessione verso la porta designata dal client nel comando PORT (cioè la 50090). La porta utilizzata per stabilire la connessione è la 34305 del server.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Sul collegamento di controllo sono scambiati i seguenti pacchetti.

Immagine che contiene screenshot

Descrizione generata automaticamente

I pacchetti di Request e Response sono i seguenti.

Packet No. :

1. Il client effettua una Request di connessione attiva al server tramite il comando PORT all’interno del quale comunica la porta sulla quale il server deve effettuare la richiesta.
2. Il server risponde che ha accettato la richiesta di connessione attiva alla porta specificata.
3. Il client effettua una Request al server del comando NLST
4. Il server comunica al client che sta trasmettendo sulla connessione dati le informazioni richieste.
5. Il server informa il client che le informazioni sono state inviate con successo.

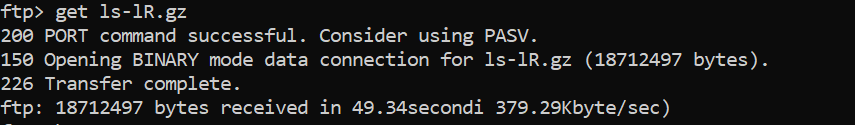
Sul collegamento dati, invece, sono scambiati i seguenti pacchetti.

Immagine che contiene parete

Descrizione generata automaticamente

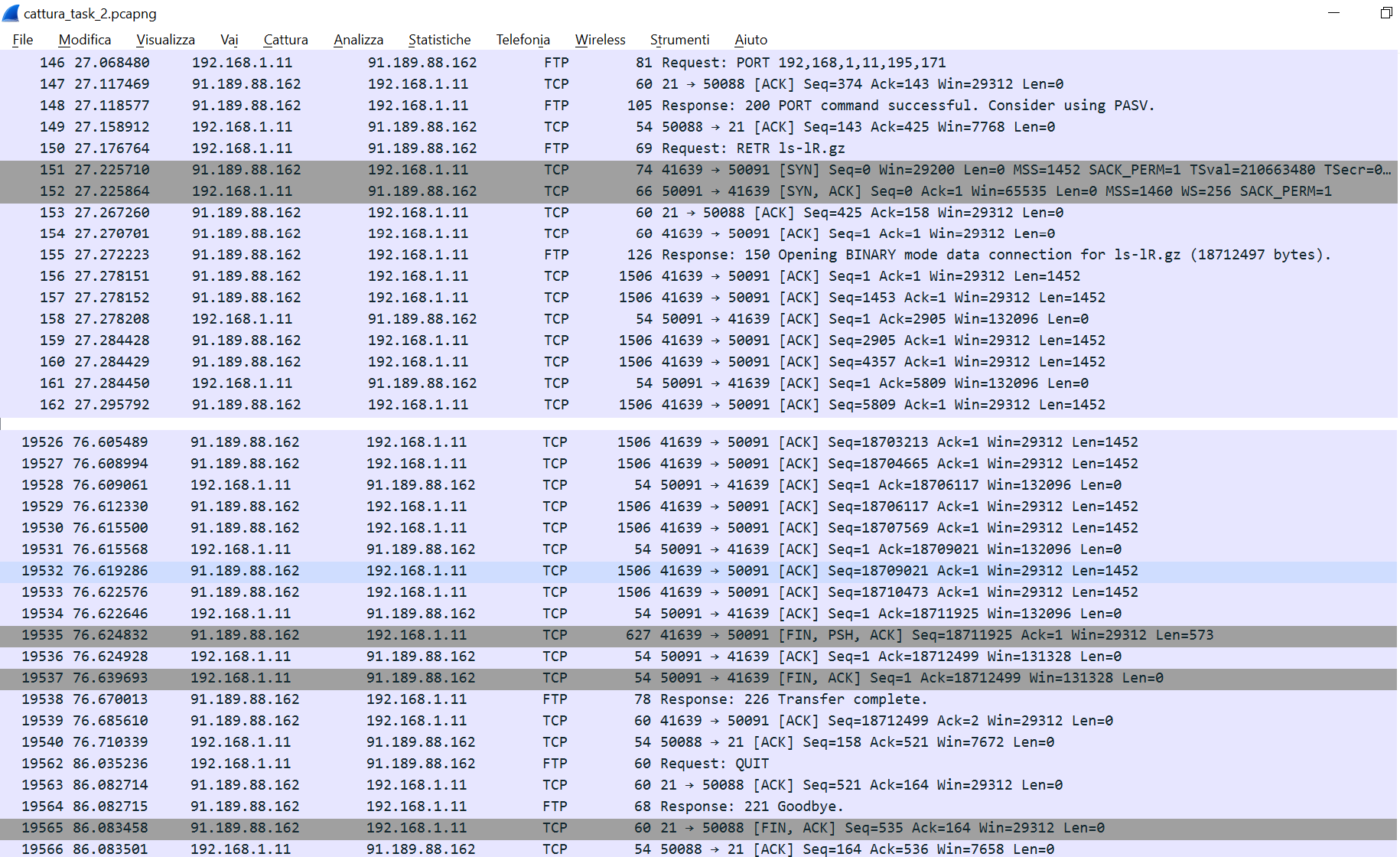
In questa connessione non vengono scambiati pacchetti Request e Response, ma semplicemente le informazioni relative al contenuto della directory, richieste con NLST. Il collegamento poi chiuso appena viene terminato il trasferimento.

**Step 5: get ls-lR.gz**, this command allows the download of ls-lR.gz.

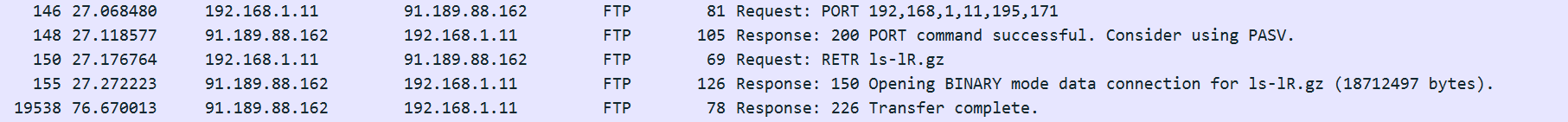


1. Which messages, if any, are exchanged between client and server?

I messaggi scambiati tra client e server per eseguire il comando sono:



I messaggi Request e Response scambiati tra client e server sono quindi questi:



2. On which connection, command or data, are those message exchanged?

I messaggi contenenti le Request e le Response sono inviati sulla connessione di controllo, mentre il file richiesto dal comando RETR è inviato sulla connessione dati.

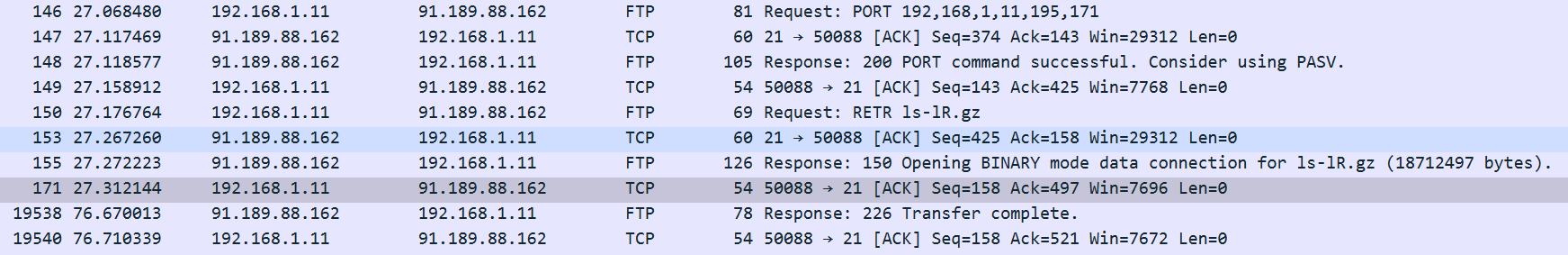
3. In case messages are exchanged on data connection:

1. Is data connection opened in ACTIVE or PASSIVE mode? Please, motivate your answer by telling your consideration
2. Whether connection is ACTIVE or PASSIVE, which TCP port is used to establish the connection?

La connessione dati viene aperta in modalità attiva, perché è il server che invia il pacchetto di SYN al client per aprire la connessione. Le porte utilizzate in questa connessione dati sono la 41639 per il server e la 50091 per il client.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Sul collegamento di controllo sono scambiati i seguenti pacchetti.



I pacchetti di Request e Response sono i seguenti.

Packet No. :

1. Il client effettua una Request di connessione attiva al server tramite il comando PORT all’interno del quale comunica la porta sulla quale il server deve effettuare la richiesta.
2. Il server risponde che ha accettato la richiesta di connessione attiva alla porta specificata.
3. Il client effettua una Request al server del comando RETR, cioè chiede di scaricare il file ls-lR.gz in locale.
4. Il server comunica al client che sta trasferendo il file sulla connessione dati.
5. Il server informa il client che le trasferimento è stato effettuato con successo.

Sul collegamento dati, invece, sono scambiati i seguenti pacchetti.

Immagine che contiene interni, parete

Descrizione generata automaticamente

In questa connessione non vengono scambiati pacchetti Request e Response, ma semplicemente viene trasferito il file ls-lR.gz, richiesto con RETR. Il collegamento viene poi chiuso appena terminato il trasferimento.

**Step 6: exit (or bye)**, this command allows terminate FTP session.



1. Which messages, if any, are exchanged between client and server?

I messaggi scambiati tra client e server per eseguire il comando sono:

Immagine che contiene screenshot

Descrizione generata automaticamente

I messaggi Request e Response scambiati tra client e server sono quindi questi:



2. On which connection, command or data, are those message exchanged?

Tutti i messaggi sono scambiati sulla connessione di controllo. La connessione dati non viene aperta.

4. For each connection, command and data, list all messages (request and response) being exchanged, describing the meaning of each message.

Sul collegamento di controllo sono scambiati i seguenti pacchetti.

Immagine che contiene screenshot

Descrizione generata automaticamente

I pacchetti di Request e Response sono i seguenti.

Packet No. :

1. Il client effettua una Request di chiudere la connessione di controllo con il comando QUIT.
2. Il server invia il messaggio Goodbye al client, confermando la richiesta di chiusura.

E si procede con la chiusura della connessione di controllo.

La connessione dati non viene aperta.