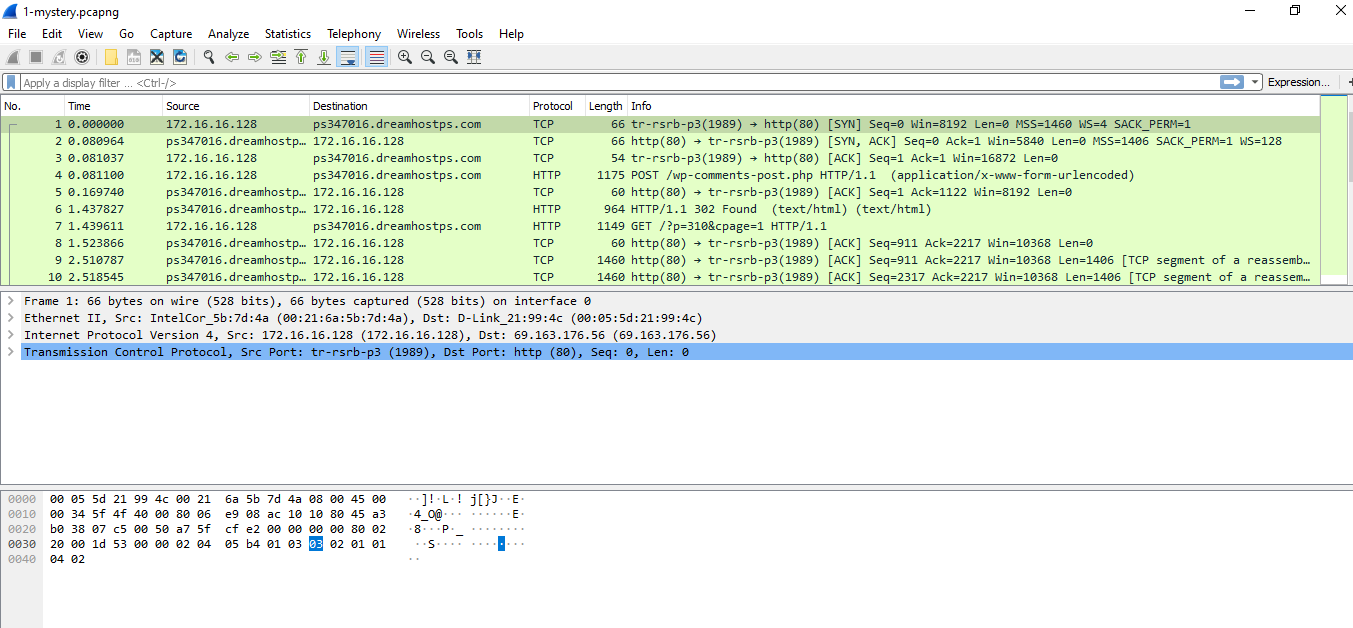
**Mystery 1**



**Hypertext Transfer Protocol (HTTP)**

HTTP stands for Hypertext Transfer Protocol and is an application protocol that allows users to communicate data on the World Wide Web. As a request-response protocol, HTTP gives users a way to interact with web servers. HTTP clients generally use Transmission Control Protocol (TCP) connections to communicate with servers. It uses TCP Port 80.

HTTP utilizes specific request methods in order to perform various tasks:

* GET requests a specific resource in its entirety
* HEAD requests a specific resource without the body content
* POST adds content, messages, or data to a new page under an existing web resource
* PUT directly modifies an existing web resource or creates a new URL if need be
* DELETE gets rid of a specified resource
* TRACE shows users any changes or additions made to a web resource
* OPTIONS show users which HTTP methods are available for a specific URL
* CONNECT converts the request connection to a transparent TCP/IP tunnel
* PATCH partially modifies a web resource

All HTTP servers use the GET and HEAD methods, but not all support the rest of these request methods.

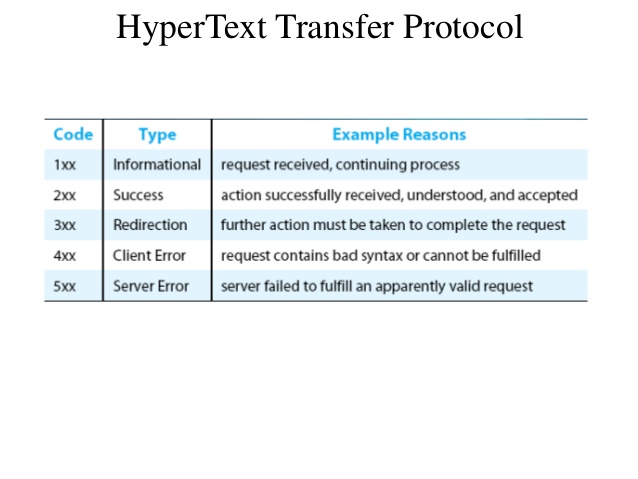
**HTTPS** means **H***yper***T***ext***T***ransfer***P***rotocol***S***ecure*. Basically, it is the secure version of HTTP. Communications between the browser and website are encrypted by Transport Layer Security ([TLS](https://www.webopedia.com/TERM/T/TLS.html)), or its predecessor, Secure Sockets Layer ([SSL](https://www.webopedia.com/TERM/S/SSL.html)).

**Overview of HTTP**

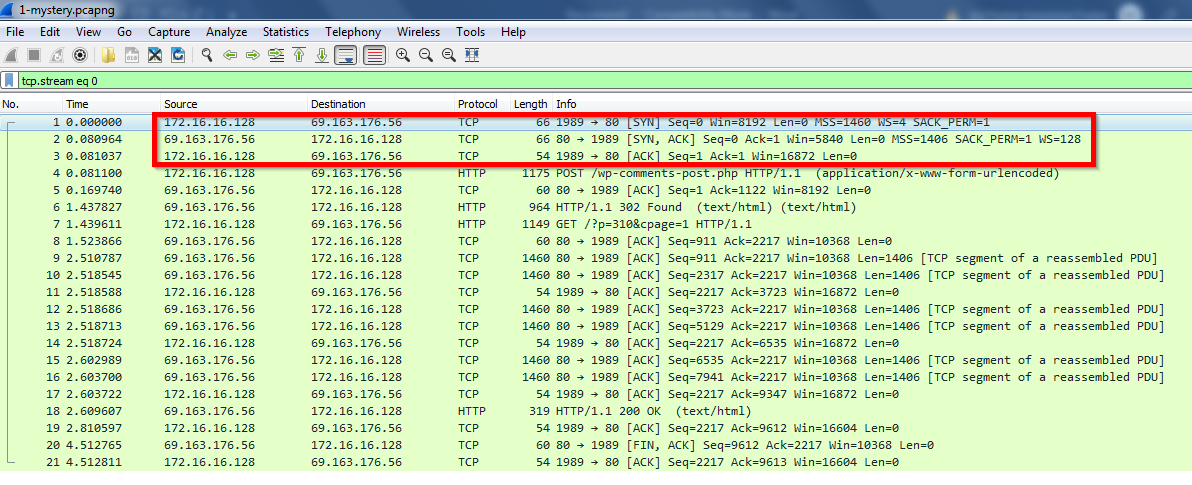
A screenshot of a cell phone

Description automatically generated

**Status codes of HTTP**



**Analysis of the 1-mystery.pcapng capture and http stream dump**



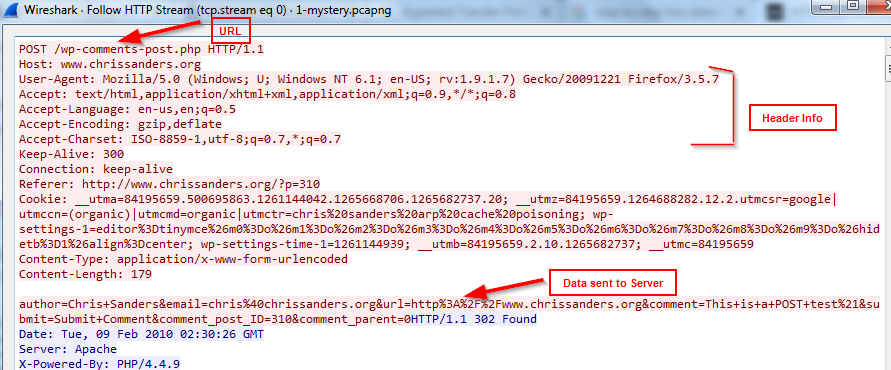
**Step 1: Establishing a TCP connection to the server by the client**

First step done by the client (IP: 172.16.16.128) 🡪initiating a http connection via TCP handshake with the http server (IP: 69.163.176.56).

TCP Handshake over Port 80 on server side and random port 1989 on client side.

The first line is a connection initiate request with "S" flag set (so it is a SYN request). The second is a reply from the server to the client with "S & ACK" flag set. The third is an "ACK" reply from the client to complete the three-way handshake.

**Step 2: HTTP Post Request**



POST request is mostly used to send data from the client to the server.

Above, post request is being sent to "wp-comments-post.php".

The last line sends the exact data to the server.

**Step 3: HTTP redirection status code 302 (intermediary step)**



**Step 4: Initiating a HTTP GET Request by the client to the server**

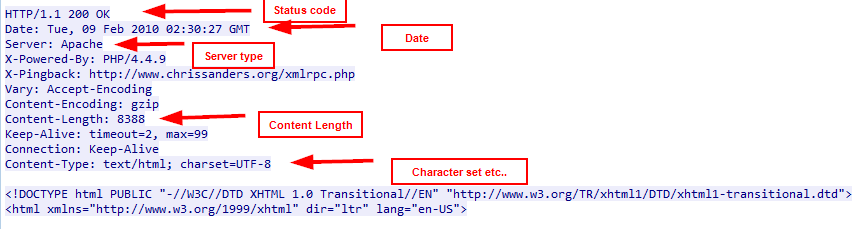


Get requests are used by the clients for retrieving data from the server.

what is the client requesting “/?p=310&cpage=1”. GET " /?p=310&cpage=1", such type of request tells the server to retrieve this page.

HOST field tells the hostname of the server, from which client is requesting the data. [www.chrissanders.org](http://www.chrissanders.org). Most of the clients request a keep-alive type of connection from the server. Keep-alive is used to keep the tcp connection made by the client, so that the overhead of creating a tcp connection is reduced for subsequent requests. Although the client requests a keep-alive kind of connection from the server, its the server who decides whether to keep tcp connection active or not(based upon the server configuration).

**Step 5: HTTP Server Response to a HTTP GET Request**



On getting the GET request from the client, the server responds, by revealing some information about itself, and metadata about the data asked by the client, along with the data.

The server replies to the client with a status code of 200. Status code of 200 means the request has succeeded. HTTP/1.1 200 OK

Server filed in the response tells the server software that's being used (this field is modifiable in almost all web servers. This at times is a security breach as it reveals the server information to the client.) In our case its Apache. Content-Length specifies the size of the resource requested in bytes. In our case it is 8388 bytes. Content-Type specifies the type of the content. In our example its Content-Type: text/html; charset=UTF-8.

The client was requesting the server for the web page www.chrissanders.org. All other details of ports used, IP addresses etc. has been provided in the above analysis.