**Difference between HTTP1.1 vs HTTP2**

**Introduction:**

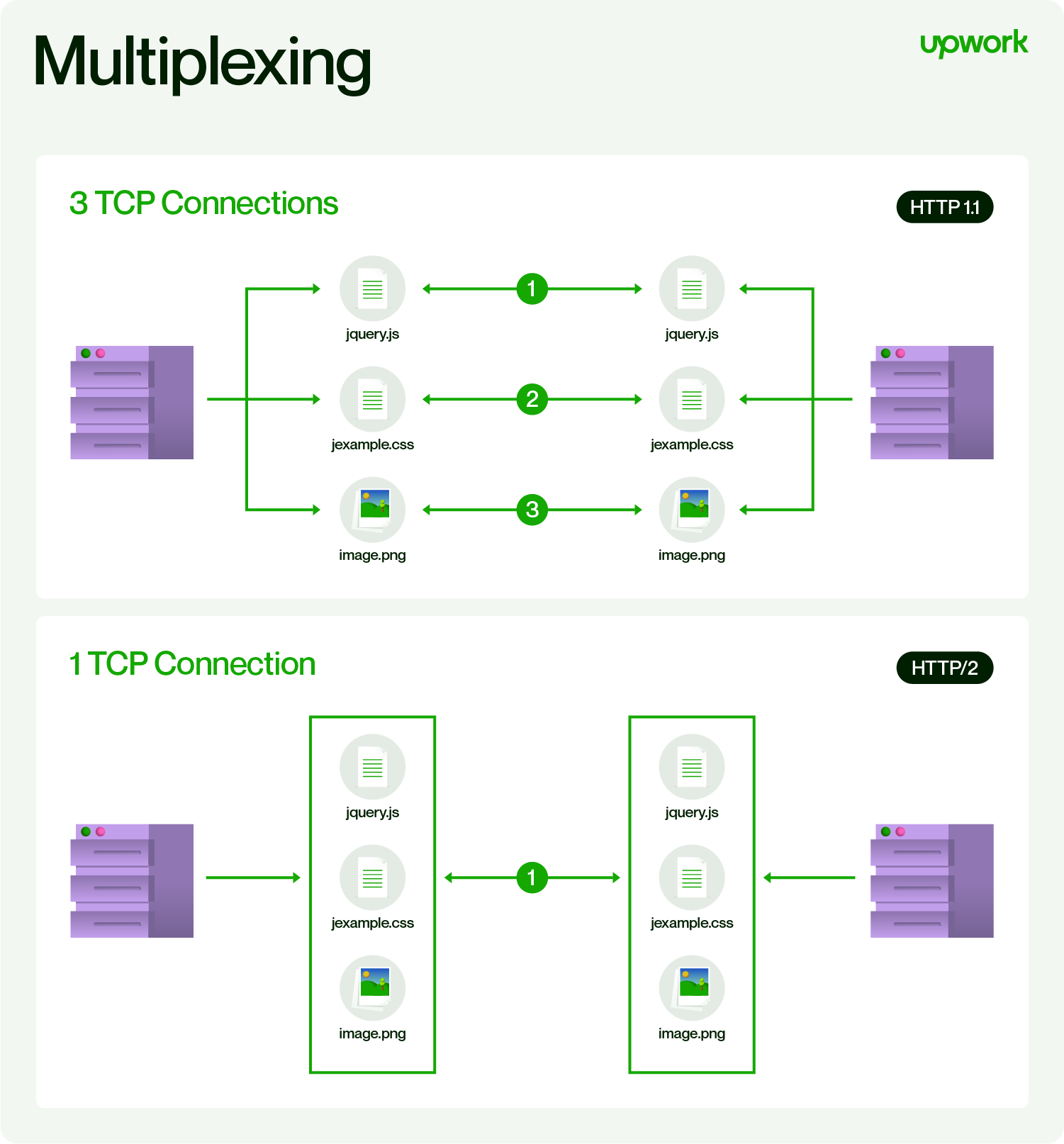
**H**yper**t**ext **T**ransfer **P**rotocol (**HTTP**) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers. Browser requesting information via HTTP it will get response from server and displaying information via HTTP.

**HTTP/1.1:**

HTTP/1.1 was first published as RFC 2068 in January 1997.HTTP/1.1 is the latest version of Hypertext Transfer Protocol (HTTP), the World Wide Web application protocol that runs on top of the Internet's TCP/IP suite of protocols. HTTP/1.1 provides faster delivery of Web pages than the original HTTP and reduces Web traffic. HTTP/1.1 enables browsers to send several HTTP requests to the server on a single TCP connection. In anticipation of receiving further requests, the server keeps the connection open for a configurable interval (typically 15 seconds) after receiving a request.

**HTTP/2:**

HTTP/2 was released in 2015 as a major revision to the HTTP/1.1 protocol. HTTP/2 enables full request and response multiplexing. In practice, this means a connection made to a web server from your browser can be used to send multiple requests and receive multiple responses. This gets rid of a lot of the additional time that it takes to establish a new connection for each request.



|  |  |  |
| --- | --- | --- |
| **Features** | **HTTP/2** | **HTTP/1.1** |
| **Compression** | Compresses headers that have been requested previously to make things more efficient. | Does not compress headers by default. |
| **Performance** | Improving performance for the end-user. One example of this is how external resources can be preemptively pushed to the client's browser before they are explicitly requested. | Does not have these advanced features. |
| **Binary protocol** | Meaning commands use 1s and 0s and not text. | Meaning Commands use only text. |
| **Security** | Because of the binary format used by HTTP/2, there is no longer a risk with so-called response splitting attacks. | Attacks are possible with HTTP/1.1 |