AI Detection Report

for zealexandre9@gmail.com

justdone

- This report was automatically generated at your request. Your results are confidential and have not been shared with any educational institutions or external organizations.
- AI detection is a relatively new field with various methods. While we strive for 99% accuracy in detecting AI-generated content, please note that no method is perfect.

100% Human 0% AI

Most academic institutions and websites will consider this text to be fully human, unique and ready for publication.

Words: 425 • Characters: 2687

1. Web Caching to Reduce Delay Web caching alleviates latency by locally storing copies of commonly used content as local caches or by network cache servers. Whenever a user requests an object, browser or intermediate cache checks whether the object is stored in the cache. In this case, a fast response is returned with the cached version without access to the original server, reducing network latency and server processing time. The bad news is that they occasionally include a delay for some objects that caching just won't reduce: This is only beneficial for previously requested or cached objects. Two things (the only two, actually) will never be served from the cache: Dynamic content and personalized data. ### 2. Type http://yourbusiness.com/about.html When you enter some URL, following things happen: 1. **DNS Resolution — The browser uses DNS to resolve yourbusiness. resolution it translates the web address `www.gfz-potsdam. 2. **tcp connection(TCP/IP)** : based on the ip, client will perform a 3-way handshake (synchronize sequence number) with server via port 80. 3. After the connection is established, using HTTP 1.1, the browser sends an HTTP GET request containing `about`. html`. 4. **Response from Server:** The server processes the request and responds with an HTTP reply containing HTML (HTTP status code 200 OK on success, etc. for other cases). 5. **Rendering**: Browser renders the HTML, CSS, JS, images and other resources to create views (may need to make further HTTP requests for these assets). Key Protocols: * DNS: Domain to Ip translation – TCP/IP: To make a reliable connection. - **HTTP/1.1**: For request-response per client to server scenario ### 3. Questions on the HTTP/1.1 Specification (RFC2616) 1a.) **Indicating that a Connection Close can be Prolonged** – Persistent connections are the default in HTTP/1.1 and will remain open for multiple requests/responses. The `Connection: close` header specifies the termination of the persistent connection. Imagine that you use two connections; one is client and one is server (for example with http status code); when finally at the end of session we decide to close connection by adding `Connection: close` in http header. b. **HTTP Encryption Services** HTTP is not encrypted on its own. HTTPS (HTTP over SSL/TLS) — uses SSL/TLS protocols to encrypt the HTTP message in its entirety and to authenticate the server (and sometimes the client). c. **Concurrent Connections** The answer is yes, clients can have more than one simultaneous connection to a server. To alleviate server bottlenecks and reduce network congestion, HTTP/1.1 advises the maximum number of active connections be limited to two per origin instead.