Request id

Alt-Svc →hq=":443"; ma=2592000; quic=51303431; quic=51303339; quic=51303338; quic=51303337; quic=51303335,quic=":443"; ma=2592000; v="41,39,38,37,35" Alt-Svc means alternative-service ma means max-age, v for Alt-svc defined to carry version negotiation hints. Quic=443 means port 443

Cache-Control →private, max-age=0, must-revalidate, no-transform For cache control, max-age=0 simply tells caches the response is stale from the get-go and should revalidate the response.

Content-Encoding →gzip Gzip is a file format and a software application used for file compression and decompression.

Content-Type →application/json; charset=UTF-8 UTF-8 is a variable width character using one to four 8-bit bytes.

Date →Sun, 04 Feb 2018 10:02:26 GMT Execution time is 04 Feb 2018.

ETag →"f6QLsd8inUgRKJVNBqJ8xHnPb0w/wO4LwjhpztTqz7fl4IlHqp66has" An E-tag is an electronic device that enables us to accurately calculate your tolls when you travel.

Expires →Sun, 04 Feb 2018 10:02:26 GMT Expiration time is 04 Feb 2018.

Server →GSE Server is Google Servlet Engine

Transfer-Encoding →chunked Chunked transfer encoding is a streaming data transfer mechanism available in version 1.1 oh HTTP, where the data stream us divided into a series of non-overlapping “chunks”

Vary →Origin The vary HTTP response header determines how to match future request headers to decide whether a cached response can be used rather than requesting a fresh one from the origin server, so vary-origin provide other appropriate control directives to prevent caching of inaccurate response.

Vary →X-Origin Similar to previous one.

X-Content-Type-Options →nosniff Sending the X-Content-Type-Options response header with the value nonsniff will prevent Internet Explorer from MIME-sniffing a response away from the declared content-type.

X-Frame-Options →SAMEORIGIN The X-Frame-Option HTTP response header can be used to indicate whether or nor a browser should be allowed to render a page in a frame ,iframe or object. The sameorigin directive allows the page to be loaded in a frame on the same origin as the page itself.

X-XSS-Protection →1; mode=block

X-XSS-Protection response header is a feature of Internet Explorer that stop pages from loading when they detect reflected cross-site scripting attacks. So it means block pages from loading when they detec reflected XSS attacks.

Request next

Content-Encoding →gzip Gzip is a file format and a software application used for file compression and decompression.

Content-Type →application/json; charset=UTF-8 UTF-8 is a variable width character using one to four 8-bit bytes.

Date →Sun, 04 Feb 2018 21:32:55 GMT Execution time is 04 Feb 2018

ETag →"f6QLsd8inUgRKJVNBqJ8xHnPb0w/uBbO\_amTBCclY7jU4yKePgcFNV0" An E-tag is an electronic device that enables us to accurately calculate your tolls when you travel.

Expires →Sun, 04 Feb 2018 21:32:55 GMT Expiration time is 04 Feb 2018

Server →GSE Server is Google Servlet Engine

Transfer-Encoding →chunked Chunked transfer encoding is a streaming data transfer mechanism available in version 1.1 oh HTTP, where the data stream us divided into a series of non-overlapping “chunks”

Vary →Origin The vary HTTP response header determines how to match future request headers to decide whether a cached response can be used rather than requesting a fresh one from the origin server, so vary-origin provide other appropriate control directives to prevent caching of inaccurate response.

Vary →X-Origin Similar to previous one.

X-Content-Type-Options →nosniff Sending the X-Content-Type-Options response header with the value nonsniff will prevent Internet Explorer from MIME-sniffing a response away from the declared content-type.

X-Frame-Options →SAMEORIGIN The X-Frame-Option HTTP response header can be used to indicate whether or nor a browser should be allowed to render a page in a frame ,iframe or object. The sameorigin directive allows the page to be loaded in a frame on the same origin as the page itself.

X-XSS-Protection →1; mode=block

X-XSS-Protection response header is a feature of Internet Explorer that stop pages from loading when they detect reflected cross-site scripting attacks. So it means block pages from loading when they detec reflected XSS attacks.