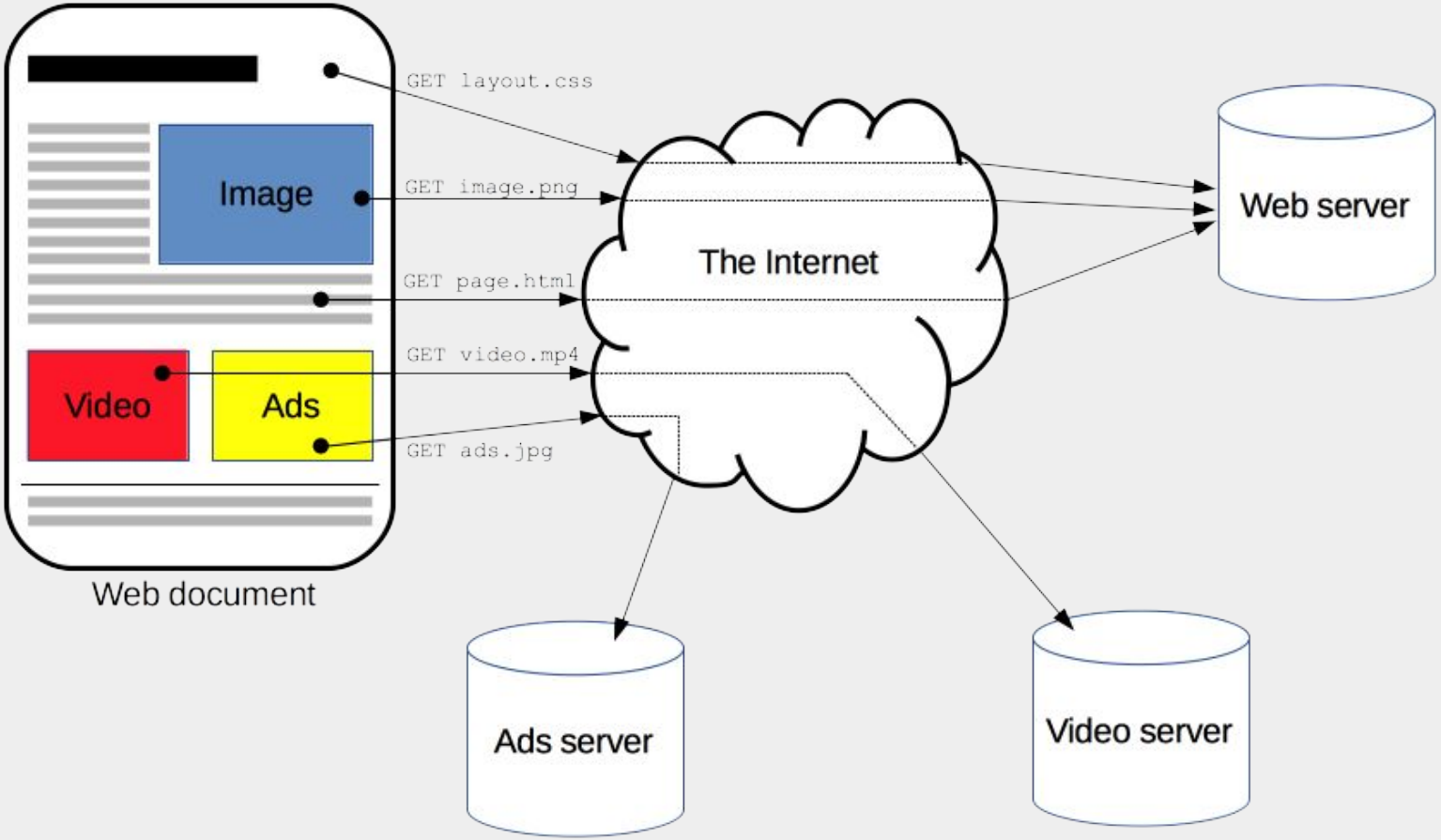
What is HTTPS

Well, let’s start with HTTP first

HyperText Transfer Protocol

HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents fetched, for instance text, layout description, images, videos, scripts, and more.

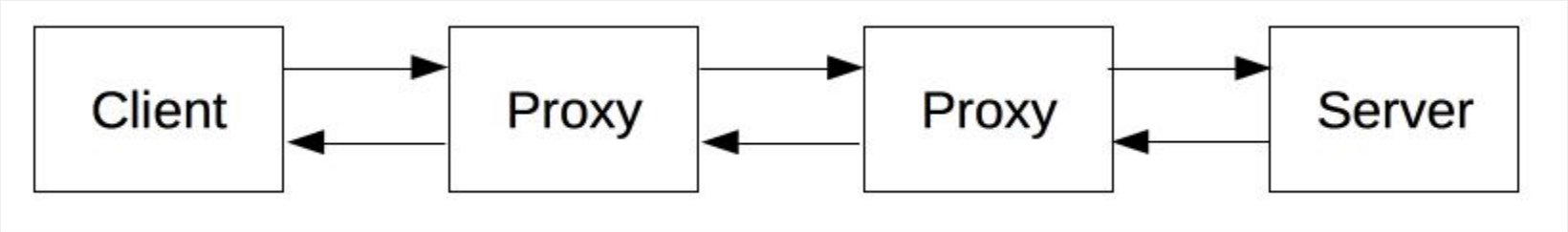

GET layout.css
Image
GET image.png
GET page.html
GET video.mp4
Video
Ads
GET ads.jpg
Web document
The Internet
Web server
Ads server
Video server

A Touch on History

Designed in the early 1990s, HTTP is an extensible protocol which has evolved over time. Due to its extensibility, it is used to not only fetch hypertext documents, but also images and videos or to post content to servers, like with HTML form results. HTTP can also be used to fetch parts of documents to update Web pages on demand.

Components of HTTP-based Systems

HTTP is a client-server protocol: requests are sent by one entity, the user-agent. The messages sent by the client, usually a Web browser, are called requests. Each individual request is sent to a server, which will handle it and provide an answer, called the response. Between this request and response there are numerous entities, collectively designated as proxies, which perform different operations and act as gateways or caches, for example.



Client: the user-agent

The browser is always the entity initiating the request. It is never the server. To present a Web page, the browser sends an original request to fetch the HTML document from the page. It then parses this file, fetching additional requests corresponding to execution scripts, layout information (CSS) to display, and sub-resources contained within the page (usually images and videos). The Web browser then mixes these resources to present to the user a complete document, the Web page. Scripts executed by the browser can fetch more resources in later phases and the browser updates the Web page accordingly.

The Web server

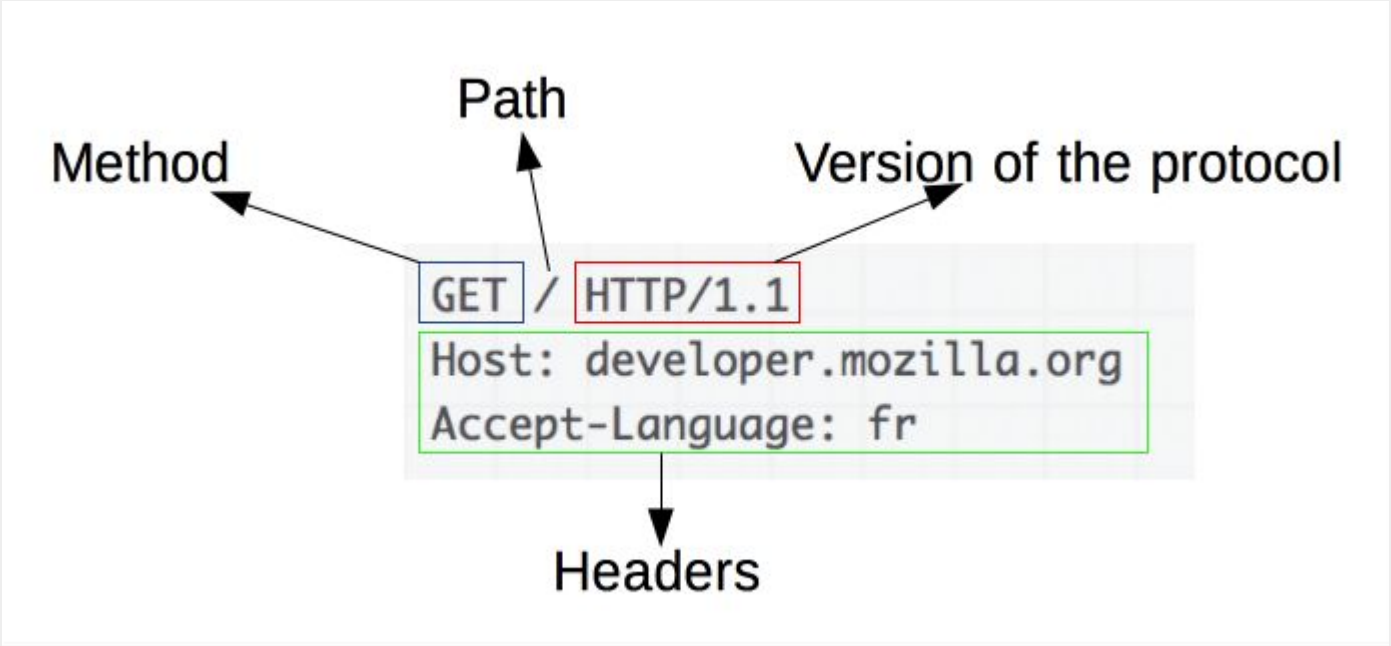
On the opposite side of the communication channel, is the server which serves the document as requested by the client. A server presents only as a single machine virtually: this is because it may actually be a collection of servers, sharing the load or a complex piece of software interrogating other computers, totally or partially generating the document on demand.

Proxies

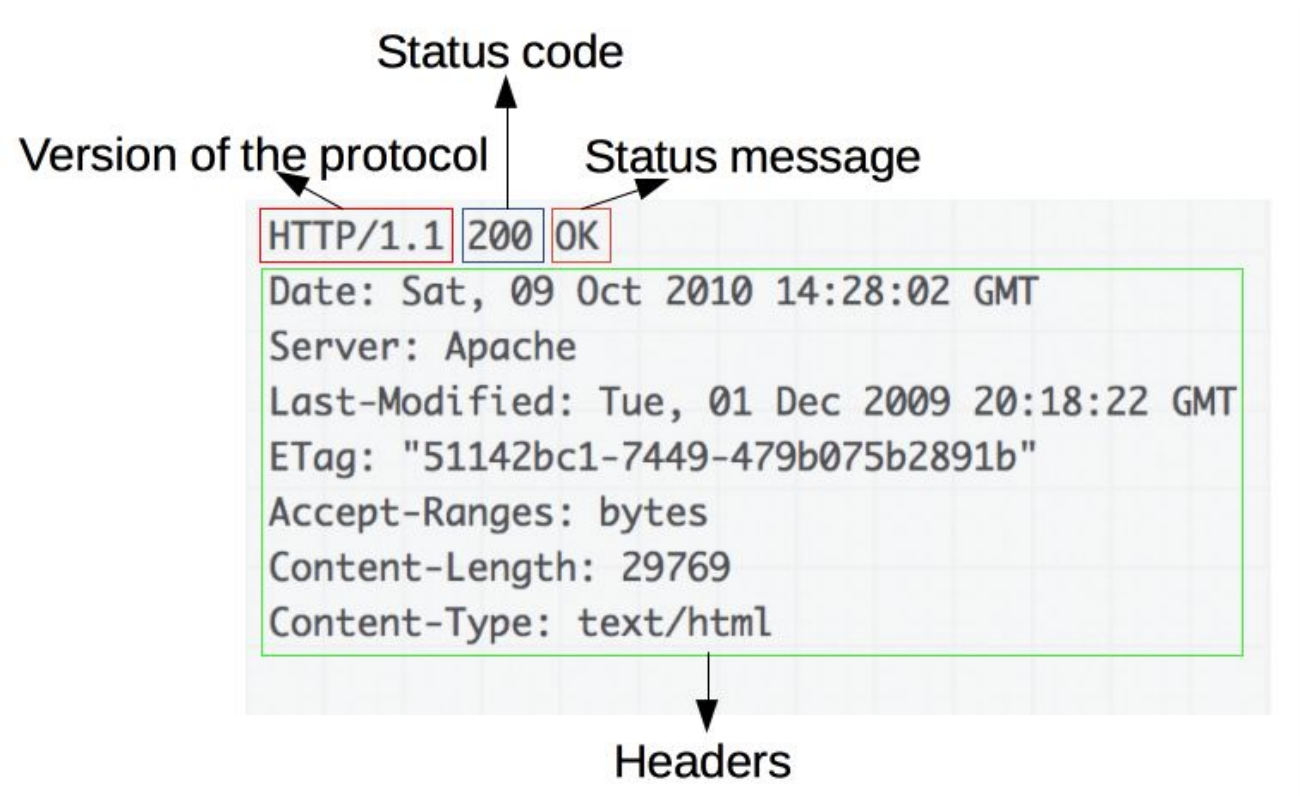
Between the Web browser and the server, numerous computers and machines relay the HTTP messages. Those operating at the application layers are generally called proxies. Proxies may perform numerous functions:

- caching (the cache can be public or private, like the browser cache)
- filtering (like an antivirus scan)
- load balancing (to allow multiple servers to serve the different requests)
- authentication (to control access to different resources)
- logging (allowing the storage of historical information)

Requests


Path
Method
Version of the protocol
GET / HTTP/1.1
Host: developer.mozilla.org
Accept-Language: fr
Headers

Responses


Status code
Version of the protocol
Status message
HTTP/1.1 200 OK
Date: Sat, 09 Oct 2010 14:28:02 GMT
Server: Apache
Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT
ETag: "51142bc1-7449-479b075b2891b"
Accept-Ranges: bytes
Content-Length: 29769
Content-Type: text/html
Headers

Now what is HTTPS?

History to present

HTTPS was created by netscape communication in 1994 for it’s netscape navigator web browser

Originally, HTTPS was used with SSL protocol

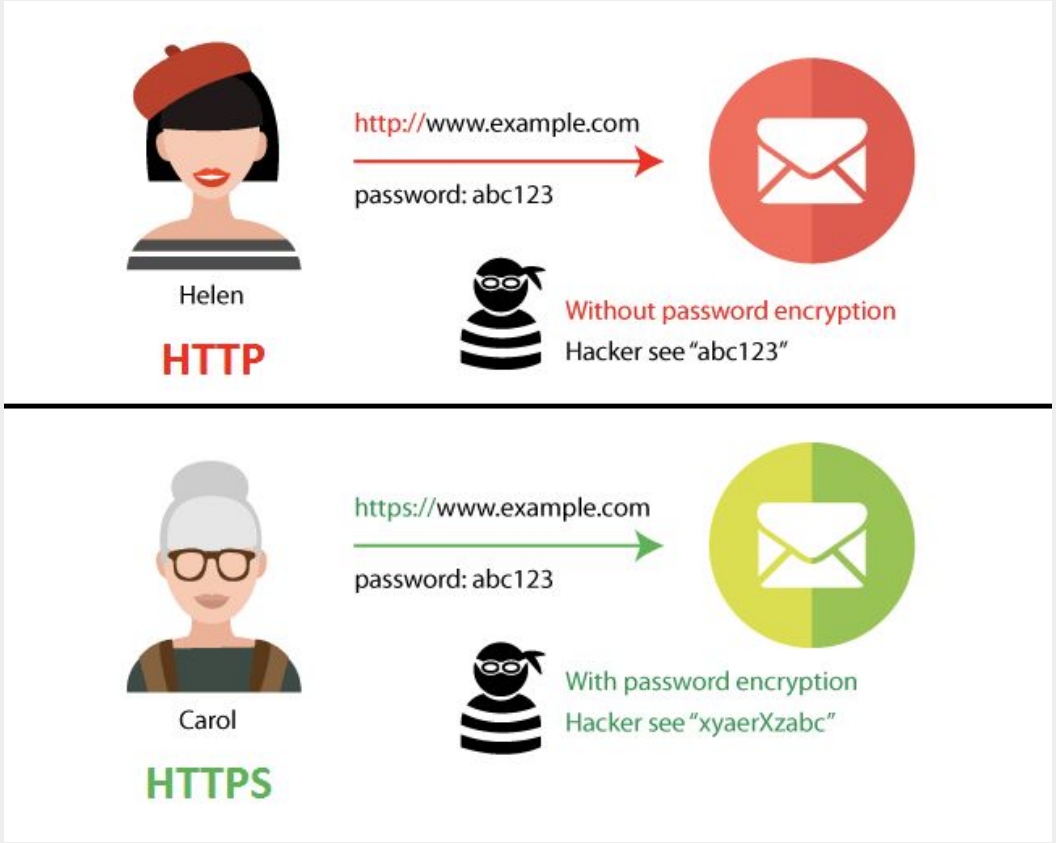
Although SSL later on evolved to TLS(Transport Layer Security)

Eventually, HTTPS was specified by RFC 2818 in may 2000

As of April 2018, 33.2% of Alexa top 1,000,000 websites use HTTPS as default

57.1% of the Internet's 137,971 most popular websites have a secure implementation of HTTPS

So what is HTTPS



What is a SSL certificate

An SSL (Secure Sockets Layer) certificate is a digital certificate that authenticates the identity of a website and encrypts information sent to the server using SSL technology. Encryption is the process of scrambling data into an undecipherable format that can only be returned to a readable format with the proper decryption key.

A certificate serves as an electronic "passport" that establishes an online entity's credentials when doing business on the Web. When an Internet user attempts to send confidential information to a Web server, the user's browser accesses the server's digital certificate and establishes a secure connection.

But do I need it?

YES

- Your site needs HTTPS
- **"But my site doesn't have forms or collect information from users.**"
- Doesn't matter. HTTPS protects more than just form data! HTTPS keeps the URLs, headers, and contents of all transferred pages **confidential**.
- It guarantees **content integrity** and the ability to **detect tampering**.
- If we encrypt only secret content, then we automatically paint a target on those transmissions. Keep which of your transmissions contain secrets secret by encrypting everything.
- Do you really want someone injecting scripts, images, or ad content onto your page so that it looks like you put them there?

Alright I’m convinced but…

How do I redirect my HTTP site to HTTPS version

Examples

```
# Redirect all incoming http requests to the same site and URI on https, using nginx
server {
  listen 80;

  return 301 https://$host$request_uri;
}
```

```
# Redirect for site.mozilla.org from http to https, using Apache
<VirtualHost *:80>
  ServerName site.mozilla.org
  Redirect permanent / https://site.mozilla.org/
</VirtualHost>
```

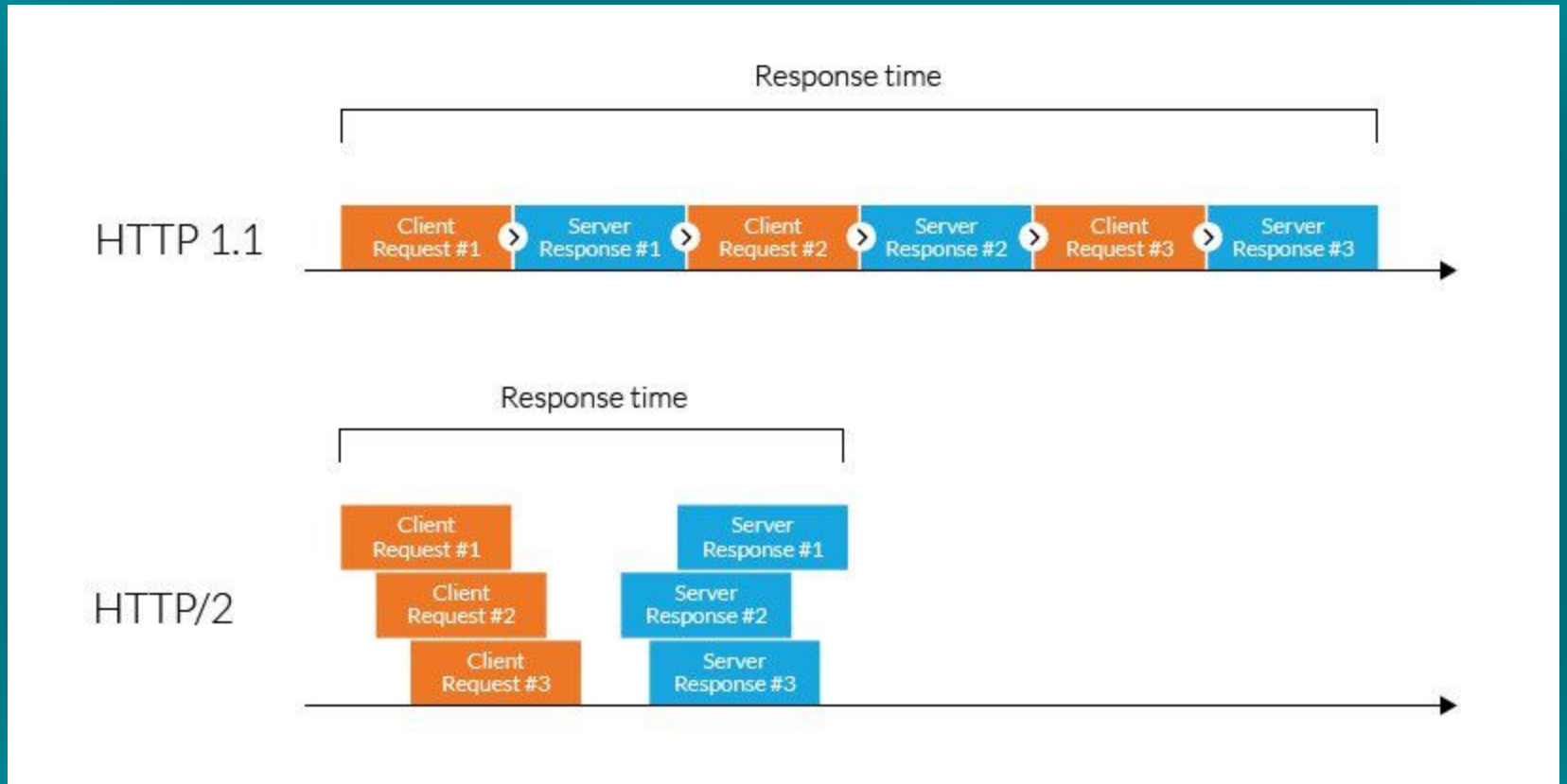
Importance of HTTPS for SEO

However, the security advantage isn't the only benefit of using HTTPS. In fact, switching over to HTTPS can end up boosting your SEO efforts as well.

The use of an HTTPS site makes Google Analytics more effective. This is because the security data of the website that referred to you is saved with the use of HTTPS

If you want to be able to use AMP (Accelerated Mobile Pages), then you'll need to have HTTPS. AMP was created by Google as a way to load content onto mobile devices at a much faster rate.

Your website loads faster with HTTP/2 which requires all websites to be HTTPS


Response time
HTTP 1.1
Client Request #1
Server Response #1
Client Request #2
Server Response #2
Client Request #3
Server Response #3
Response time
HTTP/2
Client Request #1
Client Request #2
Client Request #3
Server Response #1
Server Response #2
Server Response #3

SSL Hijacking

Your computer connects to the HTTP (insecure) site.

The HTTP server redirects you to the HTTPS (secure) version of the same site.

Your computer connects to the HTTPS site.

The HTTPS server provides a certificate, providing positive identification of the site.

The connection is completed.

Conclusion

HTTPS gives you,

Confidentiality: This protects the communication between two parties from others within a public medium such as the Internet.

Integrity: This makes sure information reaches its destined party in full and unaltered.

Authentication: This ensures that the website is actually what it claims to be.

What to learn more?

https://www.smashingmagazine.com/2017/06/guide-switching-http-https/

https://searchsoftwarequality.techtarget.com/definition/HTTPS

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

Thank you