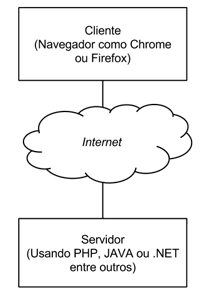
Nesse treinamento focaremos nos fundamentos da web. Isto é importante pois a grande maioria das aplicações hoje em dia a utilizam de alguma forma ou funcionam dentro dela. Não focaremos em nenhuma plataforma específica de desenvolvimento como Java ou PHP. Focaremos nas regras de comunicação da web.

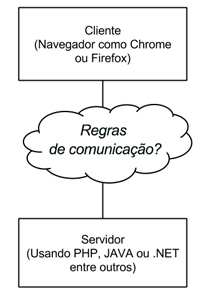
Quando se fala em HTTP, o primeiro pensamento que vem a nossa mente é sobre a utilização da **internet**, é o cenário onde vemos realmente na prática a utilização do HTTP. Nós acessamos sites em que seus endereços iniciam com *http://* e por isso precisamos conhecer o que realmente está acontecendo ao fazer isso.

No momento em que acessou este curso, esta aula, entre o navegador e a Alura aconteceu uma comunicação, e esta comunicação tem duas partes bem conhecidas que chamamos de **Client-Server** ou em português **Cliente-Servidor**. Este é um modelo arquitetural, ou seja, a internet inteira é baseada nesta arquitetura onde há um cliente que solicita e um servidor que responde.

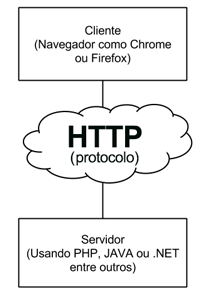


Em qualquer comunicação é preciso existir algumas regras para que as duas partes consigam se entender com sucesso. Pensando na comunicação do seu navegador entre a Alura ou algum outro site esse conjunto de regras é basicamente um **protocolo**, onde neste cenário é o **HTTP**.

Os protocolos são definidos, especificados e disponibilizados para implementação em ambas as partes, para consultar a especificação do HTTP, você pode utilizar o seguinte endereço: <https://tools.ietf.org/html/rfc2616>



Resumindo: O **HTTP é um protocolo** que define as **regras de comunicação** entre **cliente e servidor** na internet. Vamos focar nos próximos vídeos e entender melhor esse protocolo tão importante. mãos a obra!

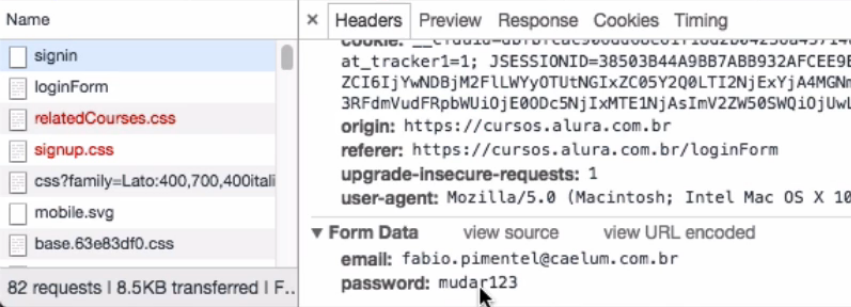


**O que aprendemos neste capítulo?**

* Na internet sempre tem um cliente e um servidor
* Entre o cliente e o servidor precisam haver regras de comunicação
* As regras são definidas dentro de um protocolo
* HTTP é o protocolo mais importante na internet

Sabendo que o HTTP é o protocolo que define as regras de comunicação na web, precisamos observar algumas coisas. Quando usamos o HTTP, todos os dados enviados entre cliente e servidor são *transmitidos em texto puro*, inclusive dados sensíveis, como login e senha!

Quando acessamos a Alura por exemplo, precisamos fornecer informações de autenticação, essas informações são nosso email e senha, que são enviadas e validadas pela plataforma para que assim consigamos assistir as aulas. Estas informações são enviadas em texto limpo e é possível visualizá-las pelas ferramentas do desenvolvedor do navegador. A aba *network* nos possibilita isso.



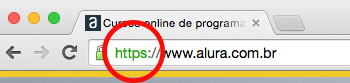
Mas por que é importante sabermos isso? Quando o navegador pede informações da Alura, nessa comunicação há vários intermediários. Por exemplo, usando uma conexão Wi-Fi, os dados do navegador passam primeiro para o roteador Wi-Fi, e do roteador passam para o modem do provedor, do modem para algum servidor do provedor de internet, como Oi ou NET.

É muito provável que existam outros servidores intermediários no provedor antes que os dados realmente cheguem no servidor da Alura. Com a resposta é a mesma coisa, ela volta passando por esses servidores no meio antes de chegar até nosso navegador. O problema é, quando usamos HTTP, qualquer servidor no meio pode espionar os dados enviados, algo totalmente inseguro! Imagine se essas informações fossem relativas a contas bancárias. Não seria nada seguro!

Para estes outros cenários, existe o HTTP**S**, que basicamente é o HTTP comum, porém com uma camada adicional de segurança/criptografia que antes era SSL, mas posteriormente passou a ser também TLS. É muito comum que estas duas siglas sejam encontradas juntas como SSL/TLS por se tratarem da mesma questão de segurança. Sendo assim, temos dois termos:

1. HTTP: HyperText Transfer Protocol
2. SSL/TLS: Secure Sockets Layer / Transport Layer Security

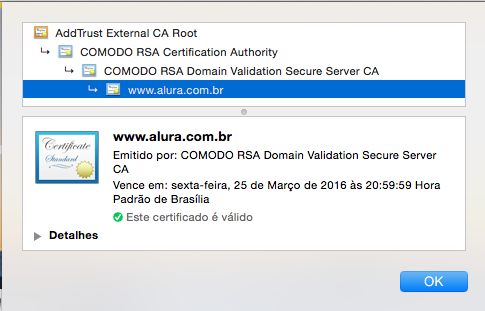
Ao acessarmos o [site da Alura](https://www.alura.com.br) pelo navegador podemos perceber que ele já usa o protocolo **HTTPS**:



Reparem que no navegador, ao lado do https, aparece um cadeado e que ao clicarmos no cadeado podemos ver mais informações sobre HTTPS. Uma dessas informações indica que a Alura tem uma identidade confirmada. O que isso quer dizer?

O HTTPS para garantir segurança usa criptografia baseada em chaves públicas e privadas e para gerar essas chaves publicas e privadas é preciso garantir a identidade de quem possui essas chaves e isso é feito a partir de um **certificado digital**, ou seja, um certificado digital é utilizado para **identificar** determinada entidade e ainda é utilizada para geração das chaves de criptografia.

Apesar disso, ainda é necessário que uma **autoridade certificadora**, que nada mais é que um órgão ou entidade confiável, garanta não apenas a identidade do site mas também a validade do certificado. No caso da Alura a autoridade certificadora é a COMODO RSA Domain Validation, mas existem outras.



Dito isso, como tudo funciona? Os navegadores em posse da chave pública criptografam as informações e as enviam para o servidor que as descriptografa com a chave privada. É importante notar que apenas a chave privada descriptografa as informações criptografadas com a pública, e também que deve-se manter a chave privada segura.

## O que aprendemos nesse capítulo?

* Só com **HTTPS a web é segura**.
* HTTPS significa usar um **certificado digital** no servidor.
* O certificado prova a **identidade** e tem **validade**
* O certificado possui uma **chave publica**.
* A chave é utilizada pelo navegador para criptografar os dados.