DNS это система, которая сопоставляет текстовые адреса сайтов с IP адресами серверов, на которых эти сайты находятся физически.

Система доменных имен действует посредством DNS-сервера, который нужен для выполнения двух основных функций:

* хранения данных о соответствии имени домена конкретному IP-адресу,
* кэширования ресурсных записей прочих DNS-серверов.

Буквы HTTP в начале адресной строки означают, что клиент и сервер обмениваются данными по прикладному протоколу – hypertext transfer protocol. Это стандартный протокол для обмена любыми данными в Интернете. Внешне аббревиатура HTTP ничем не выделяется – она такого же черного цвета, что и остальная часть адресной строки.

Если в адресной строке вместо черной надписи HTTPS появилась зеленая HTTPS, значит, данные передаются по тому же HTTP протоколу, но с дополнительной надстройкой, обеспечивающей криптографическую защиту (отсюда и буква «s», означающая «security», т.е. безопасность). Передаваемые данные шифруются с помощью протокола SSL, который невозможно расшифровать без ключа. Узнать защищенное соединение просто – помимо зеленого цвета букв, в адресной строке появляется изображение закрытого замка и надпись: «Надежный».

Стандартный протокол HTTP передаёт данные в открытом виде. Злоумышленники могут “вклиниться” в передачу — изменить или перехватить данные. В HTTPS для передачи данных создаётся защищённый канал. Вот как это происходит:

Вася хочет перейти на сайт некийсайтSSL, защищённый SSL-сертификатом:

→ Васин браузер посылает запрос к сайту

→ сайт отправляет в ответ копию сертификата

→ браузер проверяет подлинность сертификата – узнаёт у центра сертификации, который его выдал

→ если сертификат не поддельный, сайт и браузер договариваются о секретном ключе. С помощью этого ключа Васин браузер и сайт устанавливают защищённое HTTPS-соединение.

SSL расшифровывается как «уровень защищённых сокетов» или secure sockets layer. Это список определённых правил, которые позволяют более безопасно использовать связь. Для этого с помощью особых алгоритмов применяют шифровальное преобразование.