

Команда 'tracert' (traceroute) используется для определения пути передачи сетевых пакетов от исходного узла до указанного конечного узла в сети. Она помогает выявить маршрутизаторы и определить время, затраченное на прохождение каждого узла.

Суть работы команды 'tracert' состоит в отправке пакетов с постепенно увеличивающимся значением TTL (Time To Live). Значение TTL — это поле в заголовке IP-пакета, определяющее его время жизни. Каждый промежуточный маршрутизатор на пути пакета уменьшает значение TTL на 1. Когда значение TTL достигает нуля, маршрутизатор утилизирует пакет и отправляет обратно сообщение об ошибке (ICMP-пакет) отправителю, содержащее информацию о маршрутизаторе.

При использовании 'Wireshark' для анализа работы команды 'tracert' необходимо запустить сначала саму команду 'tracert', а затем установить фильтр захвата пакетов на ICMP-пакеты. Это можно сделать, добавив фильтр 'icmp' в поле 'Filter' (фильтр). Затем Wireshark будет отображать только ICMP-пакеты, которые используются для трассировки маршрута.

Когда команда 'tracert' выполняется, она отправляет серию ICMP-пакетов с постепенно увеличивающимся значением TTL до указанного конечного узла. Каждый отправленный пакет имеет уникальный идентификатор и значение TTL, отображаемое в поле 'Time to live' (время жизни) в Wireshark.

Как только пакет достигает промежуточного узла, значение TTL уменьшается на 1, и промежуточная точка утилизирует пакет, отправляя обратно ICMP-пакет с сообщением типа "Time Exceeded" (превышено время жизни). В этом ICMP-пакете присутствуют информация о маршрутизаторе, такая как IP-адрес и время, затраченное на доставку пакета до этой точки.

Таким образом, анализатор протоколов 'Wireshark' позволяет наблюдать путь, проходимый пакетами между исходным и конечным узлами, отображая IP-адреса и время, затраченное на прохождение каждого узла.