

## **АНАЛИЗ ТРАФИКА С ПОМОЩЬЮ WIRESHARK**

**Грунина Ирина Анатольевна**

студент, Поволжский государственный университет телекоммуникаций и информатики, РФ, г. Самара

**Голубничая Екатерина Юрьевна**

научный руководитель, старший преподаватель, Поволжский государственный университет телекоммуникаций и информатики, РФ, г. Самара

Wireshark — это популярный инструмент сетевого анализа, который можно использовать для сбора, анализа и устранения неполадок сетевого трафика. Это программное обеспечение с открытым исходным кодом, которое доступно бесплатно и может использоваться на различных платформах, включая Windows, macOS и Linux. Одним из наиболее распространенных применений Wireshark является анализ трафика, который включает в себя изучение сетевых пакетов для выявления закономерностей, аномалий и потенциальных проблем.

Wireshark можно использовать для сбора и анализа трафика по широкому спектру протоколов, включая TCP, UDP, HTTP, DNS и многие другие. Как только трафик захвачен, Wireshark отображает его в списке пакетов, который предоставляет подробную информацию о каждом пакете, включая IP-адреса источника и назначения, используемый протокол и длину пакета.

Одной из ключевых особенностей Wireshark является его способность фильтровать и сортировать пакеты на основе различных критериев. Это позволяет сетевым администраторам быстро выявлять и изолировать проблемы, такие как перегрузка сети, задержка или потеря пакетов. Wireshark также предоставляет мощные возможности поиска, позволяющие легко находить определенные пакеты или типы пакетов в захваченном трафике.

Wireshark также можно использовать для выполнения расширенного анализа сетевого трафика, такого как выявление моделей поведения или выявление угроз безопасности. Например, его можно использовать для обнаружения сетевых вторжений, заражения вредоносными программами и других типов атак. Анализируя структуру трафика и поведение сети, администраторы могут выявить потенциальные риски безопасности и предпринять соответствующие действия для их смягчения.

В дополнение к своим мощным возможностям анализа Wireshark также предоставляет ряд других функций, которые делают его ценным инструментом для сетевых администраторов. К ним относятся сетевая статистика в режиме реального времени, поддержка сбора трафика с нескольких интерфейсов и возможность сохранения и экспорта захваченного трафика для анализа в автономном режиме.

В целом, Wireshark — это незаменимый инструмент для всех, кому необходимо анализировать сетевой трафик и устранять неполадки. Являетесь ли вы сетевым администратором, специалистом по безопасности или разработчиком программного обеспечения, Wireshark предоставляет широкий спектр функций и возможностей, которые могут помочь вам лучше понять вашу сеть и выявить потенциальные проблемы или угрозы. Используя Wireshark для анализа вашего сетевого трафика, вы можете получить ценную информацию о том, как функционирует ваша сеть, и предпринять шаги по оптимизации ее производительности и

безопасности.

Wireshark — инструмент сетевого анализа с открытым исходным кодом, который используется сетевыми администраторами, специалистами по безопасности и разработчиками для сбора, анализа и устранения неполадок сетевого трафика. Обладая мощными возможностями захвата и анализа пакетов, Wireshark является незаменимым инструментом для всех, кому необходимо разобраться в сетевом трафике, выявить потенциальные проблемы и оптимизировать производительность сети.

В этой статье мы рассмотрим основы анализа трафика с помощью Wireshark, включая то, как перехватывать пакеты, фильтровать трафик и анализировать поведение сети. Мы также обсудим некоторые расширенные функции Wireshark, включая его способность обнаруживать угрозы безопасности и анализировать структуру трафика.

### Захват пакетов с помощью Wireshark

Первым шагом в анализе трафика с помощью Wireshark является захват пакетов. Wireshark может захватывать пакеты из различных источников, включая сетевые интерфейсы, файлы захвата и удаленные серверы. Чтобы перехватывать пакеты через сетевой интерфейс, просто выберите интерфейс в меню Параметров захвата и нажмите Пуск. Wireshark начнет захватывать пакеты и отображать их в списке пакетов.

### Фильтрация трафика с помощью Wireshark

После того как вы перехватили пакеты с помощью Wireshark, вы можете приступить к фильтрации и анализу трафика. Wireshark предоставляет ряд опций фильтрации, позволяющих быстро находить определенные пакеты или типы пакетов в захваченном трафике.

Чтобы отфильтровать пакеты, просто введите выражение фильтра в поле Фильтр в верхней части окна Wireshark. Например, вы могли бы отфильтровать весь HTTP-трафик, введя "http" в поле фильтра. Затем Wireshark отобразит только пакеты, соответствующие указанному фильтру.

Wireshark поддерживает широкий спектр выражений фильтрации, включая базовые фильтры для конкретных протоколов и более продвинутые фильтры для определенных полей внутри пакета. Например, вы могли бы отфильтровать все пакеты с определенным IP-адресом или все пакеты с определенным номером порта.

### Анализ поведения сети с помощью Wireshark

Благодаря своим мощным возможностям фильтрации и сортировки Wireshark позволяет легко анализировать поведение сети и выявлять потенциальные проблемы. Например, вы могли бы использовать Wireshark для обнаружения перегрузки сети, задержки или потери пакетов.

Чтобы проанализировать поведение сети с помощью Wireshark, начните с изучения списка пакетов. Этот список содержит подробную информацию о каждом пакете, включая IP-адреса источника и назначения, используемый протокол и длину пакета.

Изучив список пакетов, вы можете выявить закономерности поведения, такие как необычно большое количество пакетов, отправленных на определенный IP-адрес. Вы также можете использовать сетевую статистику Wireshark в режиме реального времени для мониторинга сетевого трафика и выявления потенциальных проблем в режиме реального времени.

Wireshark предоставляет ряд расширенных функций для анализа трафика, включая возможность обнаружения угроз безопасности и анализа структуры трафика.

Одной из самых мощных функций Wireshark является его способность обнаруживать угрозы безопасности. Он включает в себя ряд протоколов безопасности и плагинов, которые можно использовать для выявления потенциальных угроз безопасности, таких как сетевые

вторжения, заражение вредоносными программами и другие типы атак. Анализируя структуру трафика и поведение сети, администраторы могут выявить потенциальные риски безопасности и предпринять соответствующие действия для их смягчения.

Wireshark также предоставляет расширенные функции для анализа структуры трафика. Например, вы могли бы использовать Wireshark для определения наиболее распространенных протоколов, используемых в вашей сети, или наиболее активных IP-адресов. Эта информация может быть использована для оптимизации производительности сети, выявления потенциальных проблем и планирования будущих обновлений сети.

Wireshark — это мощный инструмент для анализа трафика, который предоставляет широкий спектр функций и возможностей для сбора, анализа и устранения неполадок сетевого трафика. Являетесь ли вы сетевым администратором, специалистом по безопасности или разработчиком программного обеспечения, Wireshark может помочь вам лучше понять вашу сеть и выявить потенциальные проблемы или угрозы.

### **Список литературы:**

1. Крис Сандерс «Анализ пакетов. Практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях» [Текст] / Крис Сандерс — 3-е издание. — СПб: ООО "Диалектика", 2019 — 448 с.
2. Wireshark для анализа трафика [Электронный ресурс]. - Режим доступа: <https://losst.pro/kak-polzovatsya-wireshark-dlya-analiza-trafika/> , свободный. - Загл. с экран.