Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Севастопольский государственный университет»

ИССЛЕДОВАНИЕ ПАРАМЕТРОВ КОНФИГУРАЦИИ И ТРАФИКА КОМПЬЮТЕРНЫХ СЕТЕЙ

Методические указания

к лабораторной работе
по дисциплине

«Инфокоммуникационные системы и сети»

Для студентов, обучающихся по направлениям 09.03.02
«Информационные системы и технологии»
и 09.03.03 «Прикладная информатика»
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

Севастополь
2025

УДК 004.732

Исследование параметров конфигурации и трафика компьютерных сетей. Методические указания к лабораторным занятиям по дисциплине «Инфокоммуникационные системы и сети» / Сост. В.С. Чернега – Севастополь: Изд-во СевГУ, 2025 – 21 с.

Методические указания предназначены для проведения лабораторных работ по дисциплине «Инфокоммуникационные системы и сети». Целью методических указаний является помощь студентам в исследовании программных средств контроля состава и функционирования компьютерных сетей. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры «Информационные системы» (протокол № от « » марта 2025 г.)

Рецензент: Кротов К.В., д-р техн. наук, профессор кафедры ИС

Лабораторная работа

ИССЛЕДОВАНИЕ ПАРАМЕТРОВ КОНФИГУРАЦИИ И ТРАФИКА КОМПЬЮТЕРНЫХ СЕТЕЙ

1 ЦЕЛЬ РАБОТЫ

Углубление теоретических знаний в области архитектуры компьютерных сетей, исследование способов контроля их функционирования, структуры и состава кадров и пакетов с помощью программных инструментальных средств, приобретение навыков измерения параметров функционирования локальных и глобальных сетей с помощью современных инструментальных средств.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Основными контролируемыми параметрами конфигурации сетевого оборудования являются аппаратные и сетевые адреса сетевых адаптеров, наличие и адреса DHCP- и DNS-серверов, информация о регистрационных данных владельцев доменных имен.

Для исследования сетевой активности, выявления неполадок в сети, находить проблемы безопасности, а также в полном объёме изучить сетевую статистику и трафик. проводится и анализа сетевого трафика и сетевых пакетов в режиме реального времени. Для измерения параметров функционирования локальных и глобальных компьютерных сетей, а также контроля их работоспособности разработан ряд программных средств (утилит). К наиболее широко применяемых утилит относятся **ipconfig, ping, tracert, Whois**. Одной из самых эффективных многофункциональных систем контроля компьютерных сетей является бесплатная система **WireShark**.

2.1. Утилита ipconfig

Утилита **ipconfig** — одна из самых часто используемых сетевых утилит в ОС Windows, позволяющая быстро и удобно просмотреть настройки сетевых адаптеров. Она также выполняет динамическое обновление параметров протоколов конфигурации динамического узла (DHCP) и системы доменных имен (DNS). Нужное действие в этой утилите инициируется командой со следующим синтаксисом

ipconfig /параметр] .

При вводе команды **ipconfig** без параметра отображается сокращенная, базовая конфигурация для всех адаптеров, установленных на компьютере. Применение команды с параметром **all** приводит к отображению полной конфигурации

протоколов TCP/IP для всех адаптеров: **ipconfig/all**. При вводе команды **ipconfig/?** выводятся все параметры этой команды и результат их действия.

2.2. Утилита traceroute

Утилита **traceroute** — служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Traceroute может использовать разные протоколы передачи данных в зависимости от операционной системы устройства. Такими протоколами могут быть UDP, TCP, ICMP или GRE. Компьютеры с установленной операционной системой Windows используют ICMP-протокол, а операционные системы Linux и маршрутизаторы Cisco — протокол UDP. В системах Microsoft Windows эта программа носит название **tracert**, а в системах GNU/Linux, Cisco IOS и Mac OS — **traceroute**.

Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL («время жизни») на 1. Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение *«time exceeded in transit»*, указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает *«time exceeded in transit»*.

Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

Команды ipconfig и tracert вводятся с командной строки консоли компьютера. Для OS Windows существует несколько способов запуска командной строки:

1. Пуск — Выполнить — В окошке «Открыть» ввести «cmd» и нажать OK.
2. Сочетание клавиш Win (кнопка с логотипом Windows) + R (должны быть нажаты одновременно) — В окошке «Открыть» ввести «cmd» и нажать OK.

2.3. Служба Whois

При регистрации доменных имен второго уровня обязательным условием является предоставление верных сведений о владельце этого домена: для юридических лиц ─ название организации, для физических лиц ─ ФИО и паспортных данных. Также обязательным является предоставление контактной информации. Часть этой информации становится свободно доступной для любого пользователя сети Интернет путем использования службы Whois (*англ.* who is ─ «кто это?»). Служба Whois реализует сетевой протокол прикладного уровня, базирующийся

на протоколе TCP (порт 43). Основное ее назначение ─ получение регистрационных данных о владельцах доменных имён и IP-адресов. WHOIS — это сервис, предоставляемый организацией InterNIC, которая предоставляет информацию о доменах второго уровня, включая контактные адреса электронной почты, почтовые адреса и номера телефонов тех, кто зарегистрировался в InterNIC. Доступ к WHOIS можно получить через клиенты WHOIS, интерактивные сеансы telnet, электронную почту и World Wide Web. База данных InterNIC предоставляет сведения о доменах COM, .EDU, .NET, .ORG и .GOV. Получить интересующую информацию о владельце домена можно через Whois-клиент ОС Windows (если он установлен), но проще всего отправить запрос можно через веб-форму онлайн сервиса Whois. Вид запроса зависит от домена, например, для домена .RU – **nic.ru/whois** или **whois-service.ru,** для домена .COM – **sbup.com/whois.php**.

Присваиванием IP-адресов занимаются разные органы в зависимости от их географического местоположения. В частности, **ARIN** отвечает за присваивание IP-адресов в Соединённых Штатах и соседних регионах, **AfriNIC** - на территории Африки, **RIPE** - в Европе, тогда как **APNIC** - Азии и Тихоокеанском регионе. Как правило, выявление владельца конкретного IP-адреса средствами WHOIS осуществляется на веб-сайте регистратора, отвечавшего за этот IP-адрес. Разумеется, глядя на IP-адрес, трудно выяснить, какой региональный регистратор отвечает за него. Эту задачу берут за себя веб - сайты вроде Robtex (http: //robtex.com/), делая запрос в соответствующий реестр и предоставляя полученные результаты. Но лаже если вы обратитесь к неверному регистратору, вас все равно перенаправят к верному регистратору.

Служба whois также позволяет определить владельца домена по ip-адресу либо ip адрес по доменному имени. Для этого следует набрать ссылку https://2ip.ru/whois/ и в открывшемся окошке набрать ip адрес или доменное имя.

Для выяснения, где располагается (хостится) искомый домен можно воспользоваться сервисом https://2ip.ru/guess-hosting/ и в открывшемся окошке набрать доменное имя.

Существуют и другие службы, позволяющие получить искомые сведения о владельце домена.

2.4. Параметры и особенности сетевого трафика

Слово «трафик» обозначает **объем данных**, который передается через компьютерную сеть за определенный период времени. В компьютерных сетях измерение сетевого трафика — это процесс измерения объема, типа и вида трафика в определенной сети или ее части. Измерение трафика осуществляется как с целью контроля качества услуг сети QoS (*Quality of Service*), так и для обеспечения безопасности сети (обнаружения попыток несанкционированного доступа к ресурсам сети, избегания случайных утечек данных, предотвращение направленных атак на информационные ресурсы и т.д.). Количественно трафик измеряется как в пакетах, так и в битах или байтах.

По месту контроля трафик подразделяется на:

- исходящий (информация, поступающая во внешнюю сеть);
- входящий (информация, поступающая из внешней сети);
- внутренний (в пределах определённой сети, чаще всего локальной);
- внешний (за пределами определённой сети, чаще всего — интернет-трафик).

Основными параметрами оценки качества услуг сети являются:

- **потери** пакетов;
- **задержки** пакетов;
- **джиттер** (флуктуация задержки) пакетов.

Потери пакетов оцениваются количество пакетов, отправленных источником и не полученных адресатом. Причиной потерь может быть проблема в интерфейсе (разъеме) или кабеле, перегрузка сети, битовые ошибки, блокирующие правила списков контроля доступа ACL. Приемлемый уровень потери пакетов в сети должен быть не выше 1%**.**

Задержки пакета представляет собой время, которое необходимо пакету, чтобы добраться от источника до получателя. Для обеспечения приемлемого качества обслуживания совокупная задержка пакета не должна превышать 150 мс. Совокупная задержка складывается из следующих компонентов.

- **Задержка сериализации** (**Serialization Delay**) — время, за которое узел разложит пакет в биты и поместит в порт к следующему узлу. Она определяется скоростью интерфейсного модуля. Так, например, передача пакета размером 1500 байтов через интерфейс 100 Мб/с займёт 0,1 мс, а через интерфейс 56 кб/с займет 200 мс.
- **Задержка передачи сигнала** в линии или канале связи (**Propagation Delay**).
- **Задержки, вносимые процедурой поддержки качества QoS** — это ожидание пакетов в очередях (**Queuing Delay**) и последствия ограничения провайдером пропускной способности (**Shaping Delay**).
- **Задержка обработки пакетов** (**Processing Delay**) — время на принятие решения, что делать с пакетом: lookup, ACL, NAT, процедура глубокой проверки сетевых пакетов **DPI** (*Deep Packet Inspection)* и доставку его от входного интерфейса до выходного. Из-за малости этой величины в современных узлах коммутации задержкой обработки можно пренебречь.

При тестировании удаленных узлов (пинговании) оценивается время, затрачиваемое на перемещения пакета в прямом и обратном направлении — **RTT** (*Round Trip Time*).

Джиттер пакетов представляет собой разницу в задержках между доставкой последовательных пакетов. Причинами джиттера являются перегрузка сети, изменения маршрута. Джиттер приводит к искажению звука, необходимости буферизация видеоданных, к задержкам в онлайн-играх. С технической точки зре-

ния, максимальная величина джиттера **30 мс** считается приемлемой. Превышение этого значения величины 30 мс может привести к существенной потери качества видео- и звуковых сообщений.

Основную часть сетевого трафика составляют пакеты с полезной нагрузкой UDP и TCP. В таблице 2.1 представлены сведения о типе и особенностях трафика, используемые приложения и протоколы транспортного уровня (L4).

Таблица 2.1 – Типы и особенности сетевого трафика

Тип трафика	Приложения	Особенности трафика	Проколы транспортного уровня
Трафик реального времени	IP-телефония и видео-конференц-связь	Чувствительность к задержке; Чувствительность к джиттеру задержки; Малая чувствительность к потерям	RSVP[1], RTP[2], RTCP[3], UDP
	Процессы управления, игры on-line	Малая чувствительность к задержке Чувствительность к джиттеру задержки; Чувствительность к потерям	UDP, TCP
Потоковый трафик	Аудио по требованию. Видео по требованию. Интернет-вещание	Малая чувствительность К задержке; Чувствительность к джиттеру задержки; Чувствительность к потерям	RSVP, SCTP, UDP, TCP
Эластичный трафик	Конференция документов	Малая чувствительность к задержке; Малая чувствительность к джиттеру задержки; Высокая чувствительность к потерям	TCP
	Анимация. Передача файлов. E-mail	Очень малая чувствительность к задержке; Малая чувствительность к джиттеру задержки; Высокая чувствительность к потерям	

[1]**RSVP –** протокол резервирования сетевых ресурсов (*Resource ReSerVation Protocol*);

[2]**RTP** – протокол реального времени (*Real-time Transport Protocol*);
[3]RTCP – протокол управления передачей в реальном времени *(Real-Time Transport Control Protoco*)

[4]SCTP – протокол передачи с управлением потоком (Stream Control Transmission Protocol).

Для эффективной защиты ресурсов компьютерной сети от угроз информационной безопасности требуется регулярный мониторинг сетевой активности. К подозрительной сетевой активности можно отнести: применение запрещенных протоколов и IP-адресов, сокрытие трафика, множественную неуспешную аутентификацию, сканирование внутренней сети, попытки подключения к внешним сетям, попытки удаленного запуска приложения, копирование и передача данных в больших объёмах и др.

Для мониторинга сетевого трафика используются различные инструментальные средства. Одним из широкораспространенных инструментов является бесплатная программа Wireshark.

2.5. Анализатор сетевого трафика Wireshark

Анализатор сетевого трафика Wireshark – свободно распространяемая программа, предназначенная для исследования функционирования компьютерных сетей Ethernet и ряда других. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в режим приема всех кадров, независимо от их адреса (*promiscuous mode*). В программе заложена информация о большинстве используемых сетевых протоколов и структуре используемых кадров и пакетов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

Основные функции, реализуемые программой Wireshark:

- захват пакетов в реальном времени из проводного или любого другого типа сетевых интерфейсов, а также чтение из файла;
- поддержка следующих интерфейсов захвата: Ethernet, IEEE 802.11, PPP и локальные виртуальные интерфейсы;
- возможность отсеивания пакетов по множеству параметров с помощью фильтров;
- подсвечивание всех известных протоколов в списке разными цветами, например TCP, HTTP, FTP, DNS, ICMP и так далее;
- поддержка захвата трафика VoIP-звонков;
- поддержка расшифровки HTTPS-трафика при наличии сертификата;
- расшифровка WEP-, WPA-трафика беспроводных сетей при наличии ключа и handshake;
- отображение статистики нагрузки на сеть;
- просмотр содержимого пакетов для всех сетевых уровней;
- отображение времени отправки и получения пакетов.

3. Описание лабораторной установки

В качестве лабораторной установки используется персональный компьютер, подключенный к сети Интернет и с установленной программой анализа сетевого трафика Wireshark.

Исследование параметров конфигурации оборудования и трассировки маршрутов осуществляется с помощью программных средств ОС Windows ipconfig и tracert. Особенности работы с этими утилитами описаны в разделе «Методические рекомендации по проведению лабораторных исследований»

Исследование параметров сетевого трафика выполняется с помощью анализатора Wireshark. После запуска программы Wireshark на экране монитора появляется стартовое меню, на котором можно увидеть доступные для захвата интерфейсы компьютера, руководства от разработчиков программы и множество других функций. Важнейшим из этих окон является окно захвата трафика Capture (рисунок 3.1). В зависимости от версии Wireshark оно может несколько отличаться от изображенного на рисунке.

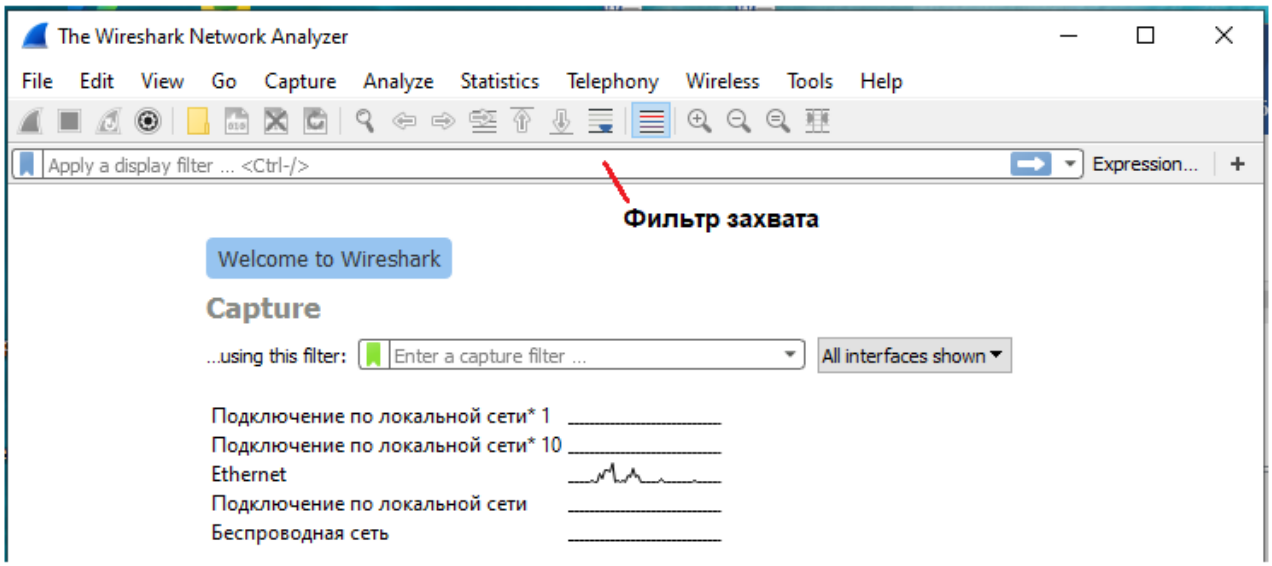


Рисунок 3.1 – Окно захвата трафика

В окне захвата перечислены интерфейсы, которые могут быть использованы для захвата трафика. Напротив каждого из них выводится график объема текущего сетевого трафика, проходящего через интерфейс. Пиковые выбросы на этом графике указывают на наличие трафика на данном интерфейсе. Если выбросы отсутствуют, линейный график остается плоским, значит этот интерфейс не активный. Для начала захвата трафика следует щелчком левой кнопки мыши (ЛКМ) выделить активный интерфейс и нажать в командном меню иконку «Start capturing packets». В результате появится главное окно с перехватываемыми пакетами (рисунок 3.2). Для заполнения окна надо выждать около минуты и остановить захват кадров нажатием иконки «Stop capturing packets».

Главное окно Wiresl1ark состоит из панелей Packet List (Список пакетов), Packet Details (Подробные сведения о пакете) и Packet Bytes (Содержимое пакетов, представлено в 16-ричной системе, рисунке 3.2 не показано), которые располагаются сверху вниз и зависят друг от друга.

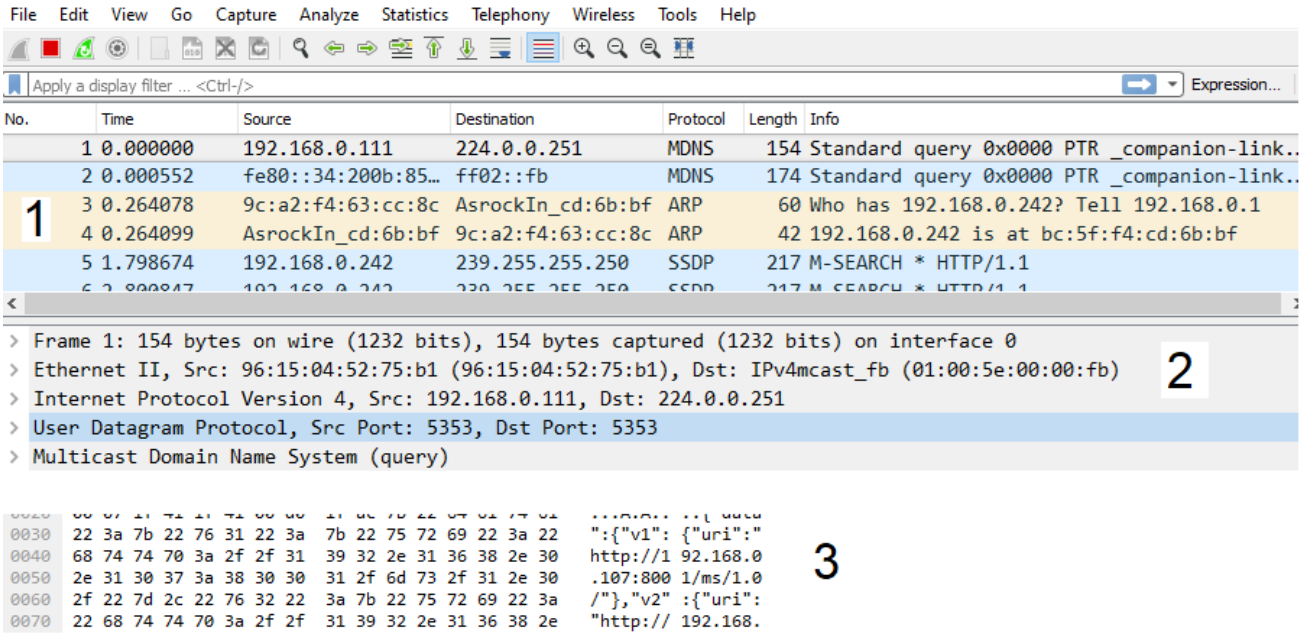


Рисунок 3.2 – Окно с информацией о захваченных пакетах

Чтобы просмотреть подробные сведения об отдельном пакете в панели Packet Details, необходимо сначала выбрать этот пакет в панели Packet List. Если же выбрать часть пакета в панели Packet Details, то в панели Packet Bytes появятся отдельные байты, соответствующие данной части пакета.

На полях главного окна отображаются следующие сведения.

1. **Packet List**. Это верхняя панель, в которой отображается таблица, содержащая все пакеты из текущего файла перехвата. Она состоит из столбцов, содержащих номер пакета, относительное время перехвата пакета, адреса источника и получателя пакета, тип сетевого протокола пакета, а также некоторые общие сведения, находящиеся в пакете.

2. **Packet Details**. Это средняя панель, где в иерархическом виде отображаются сведения об одном пакете. Она может быть свёрнута или развёрнута для отображения всей информации, собранной об отдельном пакете.

3. **Packet Bytes**. Это нижняя панель, в которой отображаются исходные данные пакета в необработанном виде, т.е. в том виде, в каком пакет переносится по сети.

В процессе анализа трафика можно сохранить все или часть пакетов выбрав соответствующую команду в меню Файл. Для сохранения части перехваченных пакетов следует выбрать команду FileQExport Specified Packets (ФайлQЭкспортировать указанные пакеты) из главного меню.

Каждый пакет, перехватываемый в Wireshark, снабжается отметкой времени, присваиваемой ему на уровне операционной системы. Приложение Wireshark способно отображать абсолютную отметку времени, обозначающую конкретный момент, когда пакет был перехвачен, время относительно последнего перехваченного пакета, а также начало и конец перехвата.

Параметры, имеющие отношение к отображению времени, находятся под заголовком View в главном меню. Пункт Time Display Format (Формат отображения времени) под этим заголовком главного меню позволяет настроить формат представления времени, а также точность его отображения,

Если требуется перехватывать только определенные пакеты, то для этого применяются фильтры. Фильтр представляет сбой выражение, в котором задаются критерии для включения или исключения пакетов из анализа.

Для создания фильтра следует воспользоваться диалоговым окном Capture lnterfaces следующим образом.

1. Выберите команду CaptureqQptions из главного меню, чтобы открыть диалоговое окно Capture lnterfaces.

2. Выберите сетевой интерфейс, где требуется перехватывать пакеты, а затем перейдите к крайнему справа столбцу Capture Filter (Фильтр перехвата).

3. Чтобы применить фильтр перехвата, щелкните на этом столбце и введите фильтрующее выражение.

4. Задав фильтр, щелкните на кнопке Start, чтобы приступить к перехвату. Рекомендации по применению фильтров приведены в разделе 4.

К этому типу относятся фильтры, применение которых к файлу перехвата означает, что в Wireshark должны быть отображены только те пакеты, которые соответствуют данному фильтру. Фильтр отображения можно создать в текстовом поле Filter, расположенном над панелью Packet List.

Фильтры отображения применяются чаще, чем фильтры перехвата, поскольку они позволяют отсеивать ненужные данные, не удаляя при этом их физически из файла перехвата. Так, если потребуется отменить первоначальное условие перехвата, для этого достаточно просто очистить фильтрующее выражение. Кроме того, фильтры отображения оказываются намного более эффективными благодаря поддержке со стороны обширной библиотеки дешифратора пакетов, доступной в Wireshark. В приложении А приведены наиболее популярные фильтры для отображения содержимого буфера захвата.

Например, в некоторых случаях фильтр отображения может применяться для отсеивания широковещательного трафика из файла перехвата. При этом на панели Packet List отсеиваются те широковещательные пакеты ARP, которые не имеют никакого отношения к текущей анализируемой проблеме в сети. Но поскольку эти широковещательные пакеты ARP могут оказаться полезными в дальнейшем, то лучше отсеять их временно, а не удалять полностью.

Для упрощения создания фильтров перехвата и отображения целесообразно использовать возможности диалогового окна Display Filter Expression. Для доступа к этому окну выберите команду FilterqExpression из главного меню и выполните следующие действия.

1. Щелкните на стрелке рядом с названием сетевого протокола, чтобы просмотреть связанные с ним поля критериев. Найдя нужный критерий в качестве основания для создания фильтра, щелкните на нем кнопкой мыши, чтобы выбрать его.

2. Выберите порядок сравнения выбранного поля со значением из критерия. Такое сравнение обозначается с помощью операции больше, меньше, равно и т.д.

3. Составьте фильтрующее выражение, указав значение из критерия, с которым должно сравниваться выбранное поле. Это значение можно указать вручную или выбрать из списка значений, предопределенных в Wireshark.

4. Полученный в итоге фильтр появится в нижней части экрана. По завершении щелкните на кнопке ОК, чтобы ввести его на панели фильтров.

4. Программа исследований

4.1. Изучить теоретический материал, относящийся к стеку протоколов TCP/IP, в частности форматы и представление аппаратных и сетевых адресов, форматы заголовков и последовательность передачи Ethernet-кадров, IP-пакетов, ARP-сообщений, ICMP-пакетов DNS- и DHCP-

4.2. Определить параметры сетевых интерфейсов (MAC- и IP-адреса, сетевые маски, адрес основного шлюза, адреса DHCP- и DNS-серверов. Для этого, нажав одновременно клавиши Win+R, открыть окно «Выполнить», затем набрать в строке «Открыть» **cmd** и нажать ОК. Выполнить команду **ipconfig/all.** Проанализировать и сохранить содержимое диалогового окна.

4.3. Выполнить в диалоговом окне трассировку маршрута до нескольких серверов. Для этого в окне следует набрать команду трассировки с указанием имени сервера, например, **tracert Yandex.ru**. Определить количество прыжков и задержку на каждом пути между маршрутизаторами. Получить сведения о владельце 2-3-х произвольных доменов. Для выполнения этого задания целесообразно воспользоваться сервисами **nic.ru/whois** или **whois-service.ru** (для домена .ru) или **sbup.com/whois.php** (для домена .COM).

4.4. С помощью любого сервиса по определению местоположения по IP (например **https://2ip.io/ru/geoip**/) проверьте и напишите в отчет, где находится сервер, указанный преподавателем.

4.5. Выполнить захват трафика на Ethernet-интерфейсе стационарного компьютера, или интерфейса беспроводной сети мобильного компьютера. Захват осуществлять в течение 2-3 минут, захватив не менее 150 пакетов. В течении этого времени выйти на официальный сайт организации, с которого была получена информация о его владельце.

4.6. Выписать все протоколы, которые были захвачены во время анализа, расшифровать их аббревиатуру записать функции, выполнение которых регламентируют соответствующие протоколы.

4.7. Исследовать структуру заголовков протоколов ARP, ICMP, TCP и UDP, а также иерархию (инкапсуляцию) использованных протоколов.

4.8. Отфильтровать (выделить) только пакеты, поступившие с определенного IP адреса.

4.9. Исследовать статистику захваченного трафика, в частности иерархию протоколов. Скопировать окно с иерархией протоколов и провести анализ полученных результатов.

4.10. Исследовать статистику «общения хостов» (conversations). Открыть окно обмена пакетами между хостами A и B можно нажатием пункта меню Statistics -> Conversations.

4.11. Исследовать зависимость пропускной способности сети в течение интервала захвата. Для этого нужно в верхней командной строке выбрать **Statistics** и щелкнуть ЛКМ по **I/O Graphs**. Скопировать полученную зависимость для отчета.

5. Методика исследования компьютерной сети

5.1. Для получения пути прохождения пакетов от источника к получателю в окне **cmd** вводится команда «**tracert** *доменное имя сервера*», например, **tracert sevsu.ru**. Вид окна после трассировки сервера sevsu.ru показан на рисунке 5.1.

```
C:\Users\Виктор>tracert sevsu.ru

Трассировка маршрута к sevsu.ru [104.21.1.162]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  192.168.0.1
  2     1 ms    <1 мс    <1 мс  host-5-1-10-10.sevstar.net [10.10.1.5]
  3     1 ms     1 ms    <1 мс  host-204-64-110-109.sevstar.net [109.110.64.204]
  4    90 ms    33 ms    33 ms  185.214.245.18
  5    42 ms    38 ms    37 ms  msk-m9-b6-ae4-vlan13.fiord.net [93.191.9.42]
  6    38 ms    38 ms    38 ms  cloudflare-peering.fiord.net [80.77.167.7]
  7    38 ms     *        *     172.68.8.51
  8    34 ms    34 ms    35 ms  104.21.1.162

Трассировка завершена.
```

Рисунок 5.1 – Трассировка сервера sevsu.ru с домашнего компьютера

Захвата трафика на интерфейсе персонального компьютера происходит после запуска программы Wireshark, активации интерфейса Ethernet и нажатия иконки «Start capturing packets». После этих действий появится окно с информацией о захваченных пакетах (рисунок 3.2).

Для просмотра структуры пакета (п.4.7 программы исследований) нужно щелкнуть правой кнопкой мыши (ПКМ) по исследуемому пакету и на второй панели появится структура кадра (фрейма) Ethernet с инкапсулированными IP пакетом и TCP сегментом (рисунок 5.2). Как видно из представленного сообщения выделенный кадр (фрейм) имеет длину 60 байтов и состоит из заголовков канального

уровня (Ethernet II), сетевого (Internet Protocol) и транспортного (Transmission Control Protocol). Полезной информации в пакете не содержится (Len=0).

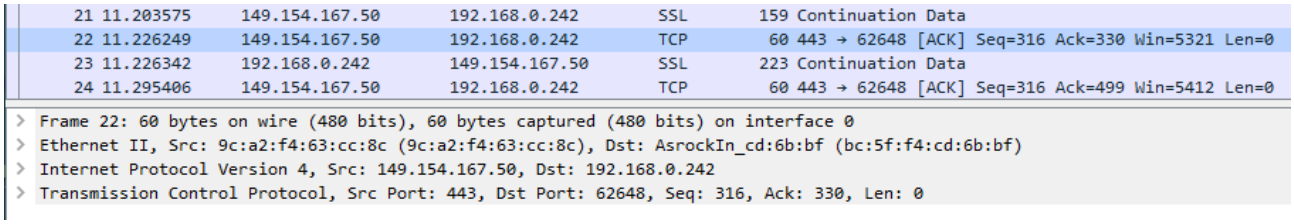


Рисунок 5.2 – Вид главного окна со структурой выделенного пакета

При двойном щелчке левой кнопкой мыши (ЛКМ) по протоколу на второй панели (Packet Details) откроется содержание заголовка этого пакета (рисунок 5.3).

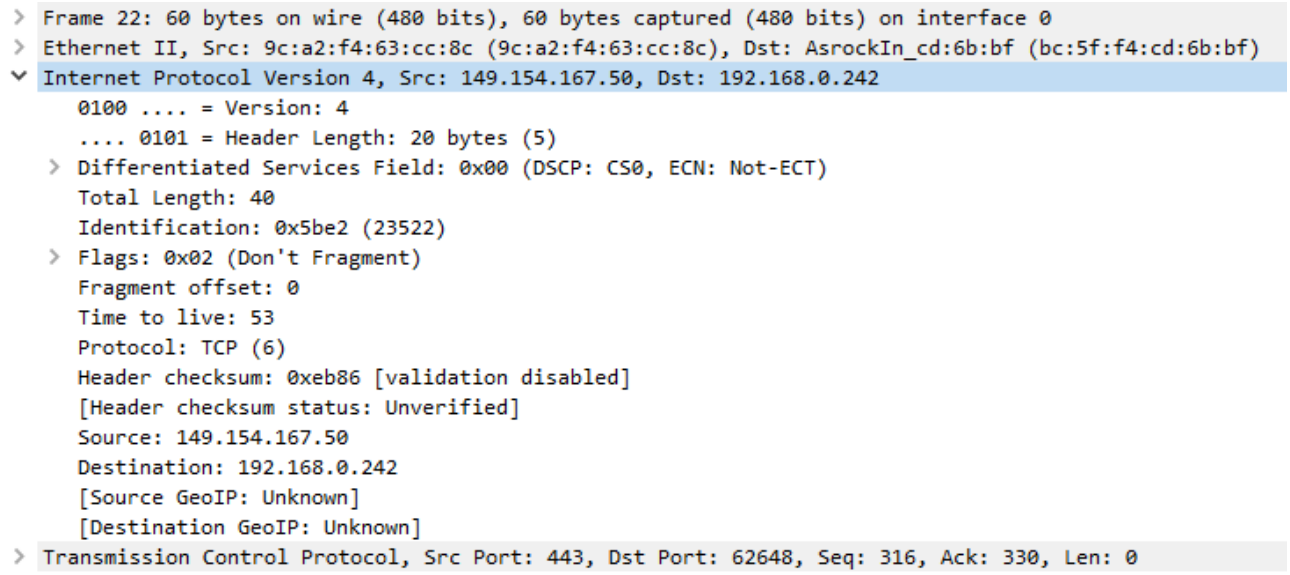


Рисунок 5.3 – Вид панели Packet Details со структурой пакета

Фильтрация пакетов (п.4.8 программы) осуществляется следующим образом. В поле фильтра нужно ввести команду с IP-адресом сайта, на который был осуществлен доступ во время захвата кадров и нажать стрелку справа. В нашем примере это адрес домена sevsu.ru.

```
ip.src==104.21.1.162
```

В результате на верхнюю панель (Packet List) выводятся кадры, которые отправлялись с сервера sevsu.ru (рисунок 5.4)

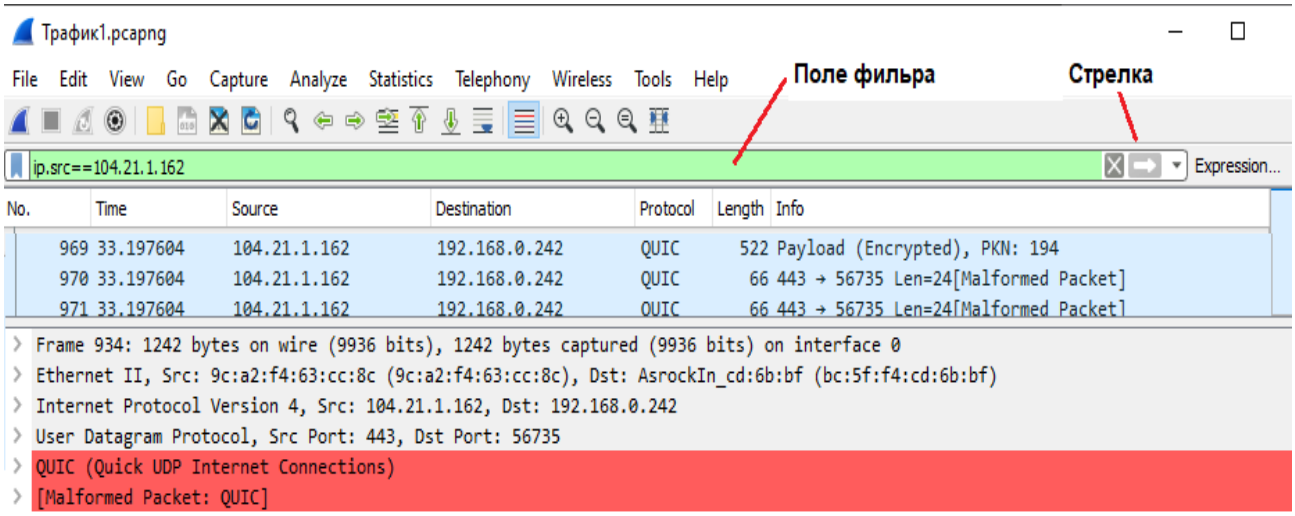
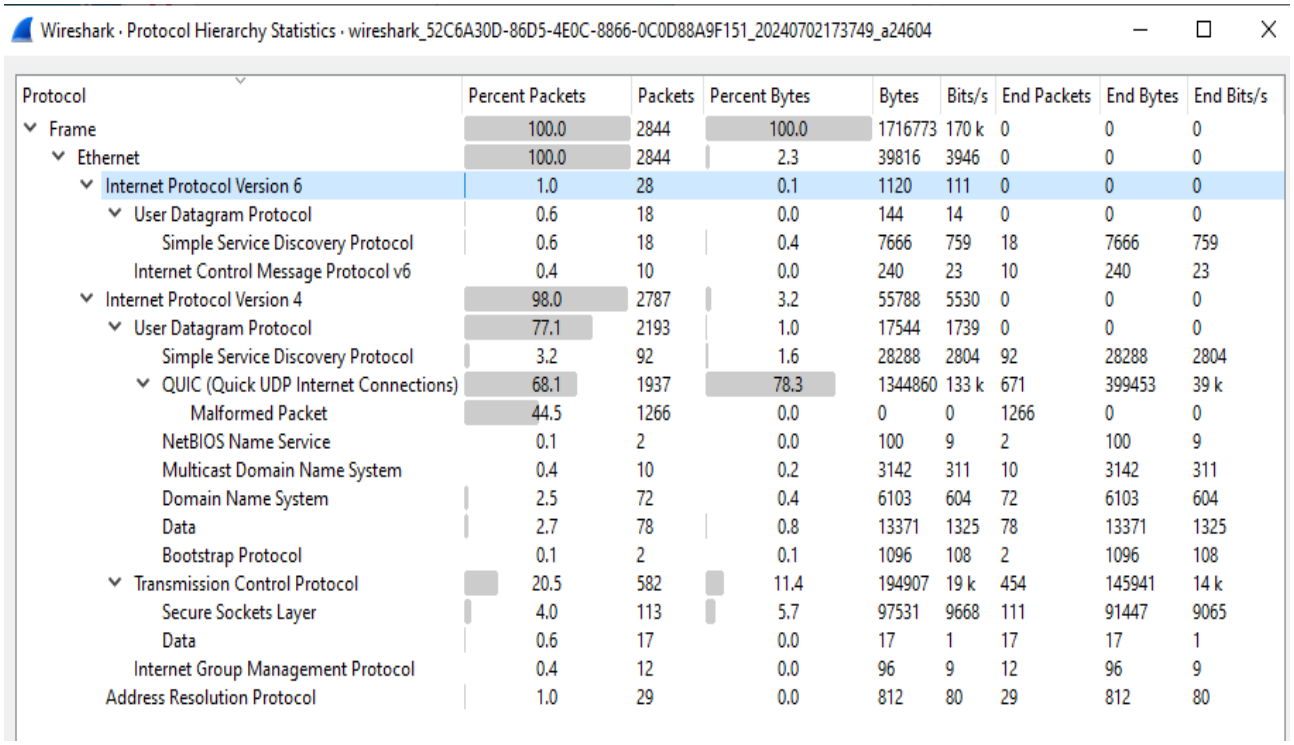


Рисунок 5.4 – Результат использования фильтра

Для просмотра иерархии протоколов (п.4.9 программы исследований) нужно в строке меню выбрать Statistics и в открывшемся окне нажать Protocol Hierarchy. В результате появится окно о распределении протоколов и байтов, участвовавших в захваченном сеансе (рисунок 5.5). Два столбца, «Проценты пакетов» и «Проценты байтов» также функционируют как гистограммы.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2844	100.0	1716773	170 k	0	0	0
Ethernet	100.0	2844	2.3	39816	3946	0	0	0
Internet Protocol Version 6	1.0	28	0.1	1120	111	0	0	0
User Datagram Protocol	0.6	18	0.0	144	14	0	0	0
Simple Service Discovery Protocol	0.6	18	0.4	7666	759	18	7666	759
Internet Control Message Protocol v6	0.4	10	0.0	240	23	10	240	23
Internet Protocol Version 4	98.0	2787	3.2	55788	5530	0	0	0
User Datagram Protocol	77.1	2193	1.0	17544	1739	0	0	0
Simple Service Discovery Protocol	3.2	92	1.6	28288	2804	92	28288	2804
QUIC (Quick UDP Internet Connections)	68.1	1937	78.3	1344860	133 k	671	399453	39 k
Malformed Packet	44.5	1266	0.0	0	0	1266	0	0
NetBIOS Name Service	0.1	2	0.0	100	9	2	100	9
Multicast Domain Name System	0.4	10	0.2	3142	311	10	3142	311
Domain Name System	2.5	72	0.4	6103	604	72	6103	604
Data	2.7	78	0.8	13371	1325	78	13371	1325
Bootstrap Protocol	0.1	2	0.1	1096	108	2	1096	108
Transmission Control Protocol	20.5	582	11.4	194907	19 k	454	145941	14 k
Secure Sockets Layer	4.0	113	5.7	97531	9668	111	91447	9065
Data	0.6	17	0.0	17	1	17	17	1
Internet Group Management Protocol	0.4	12	0.0	96	9	12	96	9
Address Resolution Protocol	1.0	29	0.0	812	80	29	812	80

Рисунок 5.5 – Окно с отображением иерархии протоколов

В окно иерархии протоколов выводятся следующие данные:

• Протокол: имя протокола.

• Процент пакетов: процент пакетов протокола от общего числа перехваченных пакетов.

• Пакеты: количество протокольных пакетов из общего числа захваченных пакетов.

• Процент байтов: процент байтов протокола от общего количества захваченных пакетов.

• Байты: количество байтов протокола из общего количества захваченных пакетов.

• Бит/с: пропускная способность этого протокола в зависимости от времени захвата.

• Конечные пакеты: абсолютное количество пакетов этого протокола (для самого верхнего протокола в файле (стеке) декодирования).

• Конечные байты: абсолютное количество байтов этого протокола, который был самым верхнем протоколом в стеке (последний анализ).

• Конечный бит/с: пропускная способность этого протокола относительно пакетов захвата и времени (для самого верхнего протокола в файле декодирования). Конечные столбцы учитываются, когда протокол является последним протоколом в пакете (то есть, когда протокол появляется в конце кадра). Это могут быть TCP-пакеты без полезной нагрузки (например, пакеты SYN), которые содержат протоколы верхнего уровня. Вот почему в колонках таблицы счетчики для конечных пакетов Ethernet, IPv4, IPv6 и UDP имеют нулевое значение, так как нет кадров, в которых эти протоколы являются последними в кадре.

Исследовать статистику «общения хостов» (conversations) можно нажатием пункта меню Statistics -> Conversations. При этом откроется окно обмена пакетами между хостами A и B (рисунок 5.6).

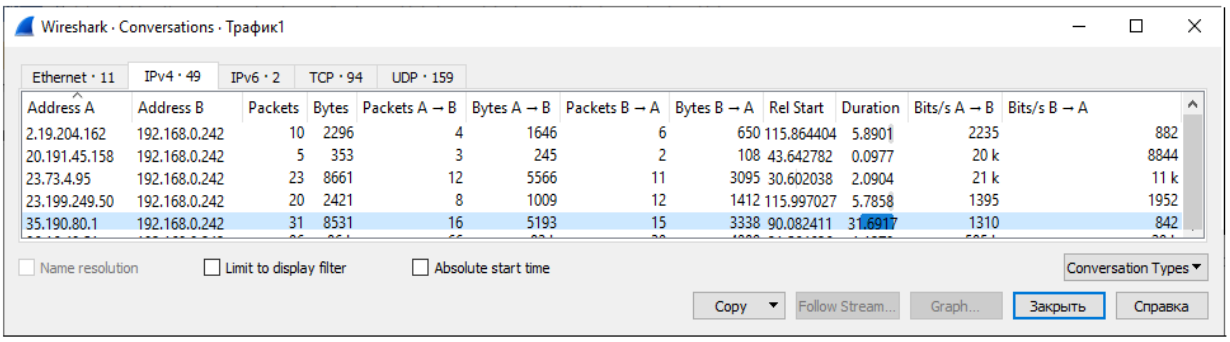


Рисунок 5.6 – Окно с отображением статистики «общения хостов»

Эта опция позволяет изучить статистику обмены пакетами между хостами на сетевом (IPv4 или IPv6) либо на транспортном (TCP или UDP) уровнях, определить длительность общения (конверсации) и скорость обмена данными. В этом

окне можно увидеть, какие IP-адреса либо порты обмениваются между собой данными, количество пакетов и объем переданных данных.

Анализ статистики по TCP-конверсациям позволяет администратору выявить некоторые проблемы сети и принять меры для их решения. Так если при анализе TCP-конверсации обнаруживается TCP-соединение, в котором передается большой объем данных, но скорость передачи очень низкая, то это может указывать на проблемы сети, такие как перегрузка или проблемы с пропускной способностью. А если вовремя TCP-конверсации видно, что один из узлов активно соединяется с различными портами на других узлах, то это может быть признаком сканирования портов злоумышленником для поиска уязвимых сервисов. Эта информация может быть полезной для целей кибербезопасности и позволяет администратору найти потенциальные угрозы в сети.

Для исследования зависимости пропускной способности сети (*Bandwidth*) в течение времени захваченного трафика следует в верхней командной строке выбрать Statistics и щелкнуть ЛКМ по I/O Graphs. В результате появится окно с графиком зависимости пропускной способности (рисунок 5.7), измеренное количеством пакетов в секунду. Измеряемая величина может быть представлена в линейном или логарифмическом масштабе, в виде линейной зависимости, столбиковой диаграмме либо иной форме (рисунок 5.8). Для этого нужно сделать двойной щелчок ЛКМ по полоске в колонке Style и выбрать желаемое представление зависимости. На графике также можно отметить день и время измерений.

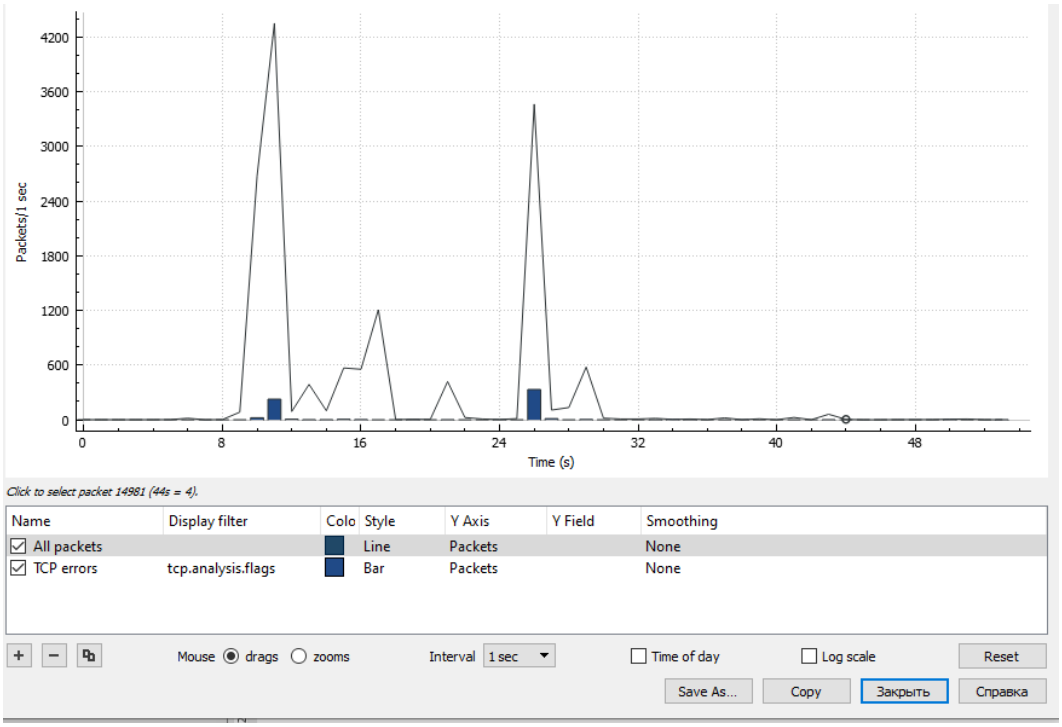


Рисунок 5.7 – График зависимости пропускной способности сети во время захвата трафика

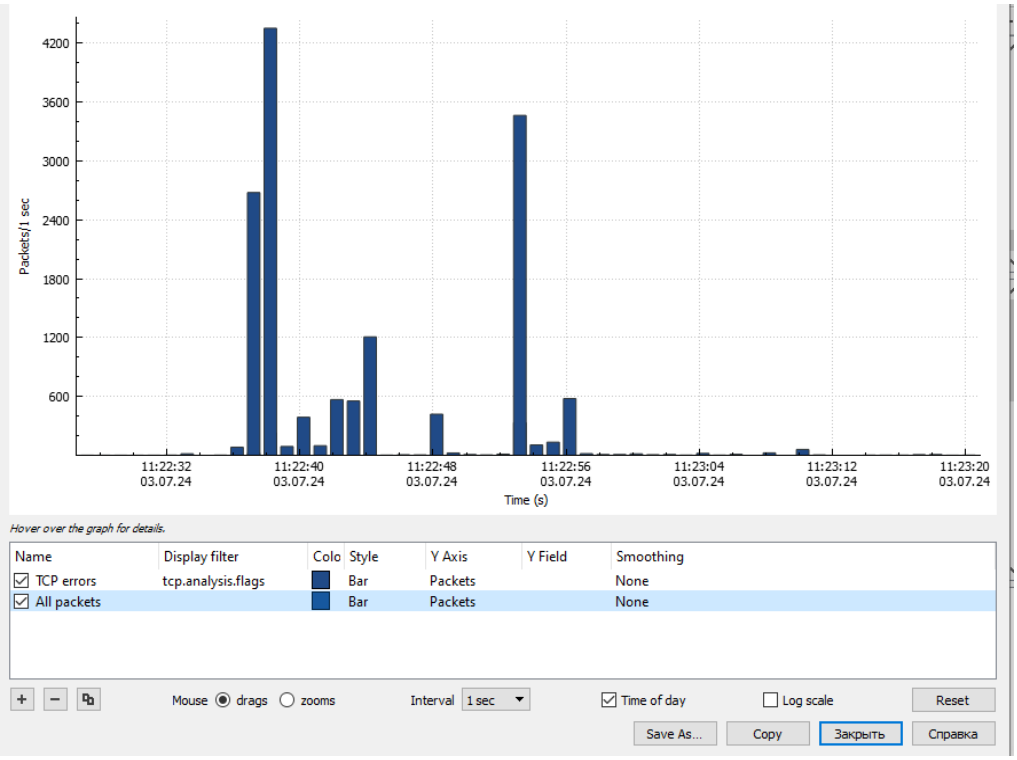


Рисунок 5.8 – Столбиковая диаграмма зависимости пропускной способности

6 СОДЕРЖАНИЕ ОТЧЕТА

6.1 Титульный лист.
6.2 Цель и программа работы.
6.3 Результаты исследований.
6.4 Выводы.

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

7.1. Расскажите об эталонной модели взаимодействия открытых систем OSI и функциях, реализуемых на каждом из уровней.

7.2. Расскажите о формате кадра сети Ethernet и назначении полей в заголовке кадра.

7.3. Расскажите о стеке протоколов IP/TCP и о процедуре инкапсуляции данных.

7.4. Охарактеризуйте систему адресации в локальных и глобальных компьютерных сетях. В чем состоит различие классовой и бесклассовой адресации?

7.5. Какие функции регламентируются IP-протоколом и какие поля содержатся в заголовке IP-пакета.

7.6. Каково назначение параметра TTL «время жизни пакета» и что с ним происходит в процессе передачи пакета по сети?

7.7. В чем состоит отличие IP-пакета протокола IPv.6 от IPv.4?

7.8. Какие существуют типы адресов в IPv6 и чем отличается адресация в протоколе 6-й версии от 4-й?

7.9. Каковы функции протоколов транспортного уровня и каковы особенности их применения?

7.10. Расскажите о составе заголовков сегментов транспортного уровня протоколов TCP UDP.

7.11. Как происходит установление соединения в протоколе TCP?

7.12. Какие сетевые параметры относятся к персональному компьютеру и как их можно проконтролировать на практике?

7.13. Продемонстрируйте на практике как можно по доменному адресу получить сведения о его владельце?

7.14. Как реализуется процедура трассировки пакетов и с какой целью она применяется в компьютерных сетях?

7.15. Какие основные функции реализуются программой Wireshark?

7.16. Продемонстрируйте на практике, как можно осуществлять фильтрацию пакетов по основным параметрам.

7.17. Покажите на практике, как измеряется пропускная способность сети?

7.18. Продемонстрируйте на практике, как можно исследовать состав заголовков пакетов различных уровней.

Библиографический список

1. Аминев, А. В. Измерения в телекоммуникационных системах : учебное пособие для вузов / А. В. Аминев, А. В. Блохин ; под общей редакцией А. В. Блохина. — Москва : Издательство Юрайт, 2024. — 223 с. — (Высшее образование). — ISBN 978-5-534-05138-4. — URL: https://urait.ru/bcode/540095 (дата обращения: 10.03.2025).
2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях: учебник и практикум для вузов / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва: Юрайт, 2024. — 423 с. — URL: https://urait.ru/bcode/544928 (дата обращения: 10.03.2025).
3. Сети и телекоммуникации : учебник и практикум для вузов / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 464 с. — (Высшее образование). — ISBN 978-5-534-17315-4. — URL: https://urait.ru/bcode/536089 (дата обращения: 10.03.2025)
4. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. - Москва ; Вологда : Инфра-Инженерия, 2022. — 460 с. — ISBN 978-5-9729-0962-9. — URL: https://znanium.com/catalog/product/1902692 (дата обращения: 10.03.2025).
5. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.

Приложение А. Популярные фильтры отображения

Фильтр для отображения	Описание	Пример написания
eth.addr	MAC адрес отправителя или получателя	eth.addr == 00:1a:6b:ce:fc:bb
eth.src	MAC-адрес onправителя	eth.src == 00:1a:6b:ce:fc:bb
eth.dst	MAC-адрес получателя	eth.dst == 00:1a:6b:ce:fc:bb
arp.dst.hw_mac	Протокол ARP – MAC адрес получателя	arp.dst.hw_mac == 00:1a:6b:ce:fc:bb
arp.dst.proto_ipv4	Протокол ARP – IP адрес версии 4 получателя	arp.dst.proto_ipv4 == 10.10.10.10
arp.src.hw_mac	Протокол ARP – MAC адрес отправителя	arp.src.hw_mac == 00:1a:6b:ce:fc:bb
arp.src.proto_ipv4	Протокол ARP – IP адрес версии 4 отправителя	arp.src.proto_ipv4 == 10.10.10.10
vlan.id	Идентификатор VLAN	vlan.id == 16
ip.addr	IP адрес версии 4 получателя или отправителя	ip.addr == 10.10.10.10
ip.dst	IP адрес версии 4 получателя	ip.addr == 10.10.10.10
ip.src	IP адрес версии 4 отправителя	ip.src == 10.10.10.10
ip.proto	IP protocol (decimal)	ip.proto == 1
ipv6.addr	IP адрес версии 6 получателя или отправителя	ipv6.addr == 2001::5
ipv6.src	IP адрес версии 6 отправителя	ipv6.addr == 2001::5
ipv6.dst	IP адрес версии 6 получателя	ipv6.dst == 2001::5
tcp.port	TCP порт получателя или отправителя	tcp.port == 20
tcp.dstport	TCP порт получателя	tcp.dstport == 80
tcp.srcport	TCP порт отправителя	tcp.srcport == 60234
udp.port	UDP порт получателя или отправителя	udp.port == 513
udp.dstport	UDP порт получателя	udp.dstport == 513
udp.srcport	UDP порт отправителя	udp.srcport == 40000
bgp.originator_id	Идентификатор BGP (Адрес IPv4)	bgp.originator_id == 192.168.10.15
bgp.next_hop	Следующий хоп BGP (Адрес IPv4)	bgp.next_hop == 192.168.10.15
rip.ip	RIP IPv4 address	rip.ip == 200.0.2.0
ospf.advrouter	Идентификатор маршрутизатора по протоколу OSPF	ospf.advrouter == 192.168.170.8
eigrp.as	Номер автономной системы EIGRP	eigrp.as == 100

hsrp.virt_ip	Виртуальный IP адрес по протоколу HSRP	hsrp.virt_ip == 192.168.23.250
vrrp.ip_addr	Виртуальный IP адрес по протоколу VRRP	vrrp.ip_addr == 192.168.23.250
wlan.addr	MAC адрес отправителя или получателя Wi-Fi	wlan.addr == 00:1a:6b:ce:fc:bb
wlan.sa	MAC-адрес оправителя Wi-Fi	wlan.sa == 00:1a:6b:ce:fc:bb
wlan.da	MAC-адрес получателя Wi-Fi	wlan.da == 00:1a:6b:ce:fc:bb

Наиболее употребительные фильтры перехват[a]

Фильтр	Описание
`tcp[13] & 32 == 32`	Пакеты TCP с установленным флагом URG
`tcp[13] & 16 == 16`	Пакеты TCP с установленным флагом ACK
`tcp[13] & 8 == 8`	Пакеты TCP с установленным флагом PSH
`tcp[13] & 4 == 4`	Пакеты TCP с установленным флагом RST
`tcp[13] & 2 == 2`	Пакеты TCP с установленным флагом SYN
`tcp[13] & 1 == 1`	Пакеты TCP с установленным флагом FIN
`tcp[13] == 18`	Пакеты TCP с установленными флагами SYN и ACK
`ether host` *`00:00:00:00:00:00`*	Входящий и исходящий сетевой трафик по указанному MAC-адресу
`!ether host` *`00:00:00:00:00:00`*	Входящий и исходящий сетевой трафик, кроме указанного MAC-адреса
`broadcast`	Только широковещательный трафик
`icmp`	Трафик только по сетевому протоколу ICMP
`icmp[0:2] == 0x0301`	Трафик по сетевому протоколу ICMP для недосягаемого получателя и хоста
`ip`	Трафик только по сетевому протоколу IPv4
`ip6`	Трафик только по сетевому протоколу Ipv6
`udp`	Трафик только по сетевому протоколу UDP

Наиболее употребительные фильтры отображения

Фильтр	Описание
`!tcp.port==3389`	Отсеять сетевой трафик по протоколу RDP
`tcp.flags.syn==1`	Отобразить пакеты TCP с установленным флагом SYN
`tcp.flags.reset.==1`	Отобразить пакеты TCP с установленным флагом RST
`!arp`	Удалить сетевой трафик по протоколу ARP
`http`	Отобразить весь сетевой трафик по протоколу HTTP
`tcp.port==23 || tcp.port==21`	Отобразить сетевой трафик по протоколу Telnet или FTP
`smtp || pop || imap`	Отобразить сетевой трафик электронной почты (по протоколу SMTP, POP или IMAP)