Тема: **Компьютерная информация: обнаружение и анализ.**

1. Анализ СКТ с использованием прикладного программного обеспечения («НИРСОФТ»).
2. Анализ сетевой активности с использованием прикладного программного обеспечения «Wireshark».

1. Анализ СКТ с использованием прикладного программного обеспечения («НИРСОФТ»).

NirSoft – это уникальная коллекция маленьких и полезных программ, разработанные Nir Sofer'ом.

У данных программ специфическое предназначение – они извлекают информацию (с постоянных носителей, из сетевых потоков, реестра и т.д.) из компьютеров на Windows. С их помощью вы можете восстановить потерянные пароли, мониторить вашу сеть для просмотра и извлечения кукиз, кэша и другой информации, хранимой веб-браузерами, искать по файлам в вашей системе, мониторить изменения в файловой системе и в системном Реестре и многое другое.

Программы являются бесплатными, не требуют установки, не содержат каких-либо вредоносных или рекламных компонентов. У программ присутствует графический интерфейс, многие программы также поддерживают работу в командной строке. У всех программ имеется поддержка многих языков и практически для всех сделан перевод на русский язык. Во время своей работы программы ничего не записывают в реестр Windows, т.е. при использовании с USB носителя не оставляют следов своего присутствия.

Познакомившись с программами NirSoft вы сможете извлекать забытые пароли и другую информацию, а также сможете оценить, что хранится на компьютере и что из него могут получить злоумышленники.

Программы регулярно обновляются, также постоянно добавляются новые инструменты.

В полном списке программы разделены на следующие разделы:

- восстановление паролей
- мониторинг сети
- извлечение информации из веб-браузеров
- работа с видео/аудио
- работа с Интернет
- утилиты командной строки
- настольные
- работа с Outlook/Office
- программерские инструменты
- дисковые утилиты
- системные утилиты
- прочие утилиты

Отдельные программы автор выделяет в разделы «Программное обеспечение для компьютерной криминалистики на Windows» и «Инструменты для работы с паролями», начнём знакомство с них.

Программное обеспечение для компьютерной криминалистики на Windows

InstalledPackagesView

InstalledPackagesView — это инструмент для Windows, который отображает список всех пакетов программного обеспечения, установленных в вашей системе с помощью установщика Windows, и перечисляет связанные с ними файлы, ключи реестра и сборки .NET. Для каждого установленного программного обеспечения отображается следующая информация: отображаемое имя, отображаемая версия, дата установки, время реестра, расчётный размер, место установки, источник установки, имя файла MSI (в C:\Windows\Installer) и многое другое…
Вы можете просматривать информацию об установленных пакетах программного обеспечения из вашей локальной системы или из другой системы на внешнем жёстком диске.
Информация об установленном программном обеспечении загружается из следующих ключей реестра:

- *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\Products*
- *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\Components*

Имейте в виду, что этот инструмент перечисляет только программное обеспечение, установленное установщиком Windows (MSI), он не перечисляет какое-либо программное обеспечение, установленное другими установщиками.

SpecialFoldersView

Этот инструмент показывает системные папки в Windows, которые обычно очень полезны в различных ситуациях. Вы можете просто дважды щелкнуть на папку в списке, чтобы открыть ее в Windows. Некоторые из папок включают данные приложения, историю Windows, административные инструменты, автозагрузку, меню «Пуск», временную папку, папку последних элементов и многое другое.

ExifDataView

ExifDataView — это небольшая утилита, которая считывает и отображает данные Exif, хранящиеся в файлах изображений .jpg, созданных цифровыми камерами. Данные EXIF включают название компании, создавшей камеру,

модель камеры, дату и время, когда была сделана фотография, время экспозиции, скорость ISO, информацию GPS (для цифровых камер с GPS) и многое другое.

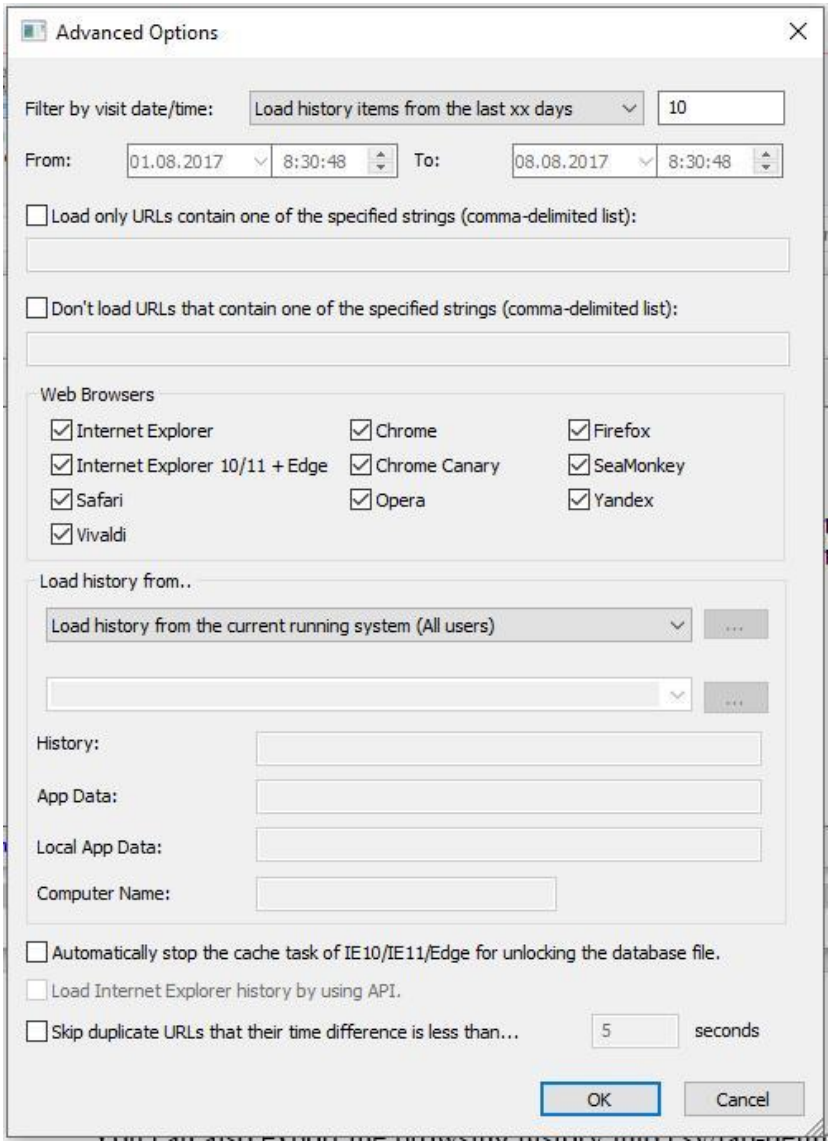
FullEventLogView

FullEventLogView — это простой инструмент для Windows 10/8/7/Vista, который отображает в таблице сведения обо всех событиях из журналов событий Windows, включая описание события. Он позволяет вам просматривать события вашего локального компьютера, события удалённого компьютера в вашей сети, а также события, хранящиеся в файлах .evtx. Он также позволяет экспортировать список событий в файл форматы текст/csv/с TAB разделителями/html/xml из графического интерфейса пользователя и из командной строки.

BrowsingHistoryView

BrowsingHistoryView считывает и показывает информацию о посещённых сайтах для всех популярных браузеров. Кроме адреса посещённых страниц, показывается её имя, время посещения, счётчик визитов и прочее. Можно извлечь информацию из всех профилей пользователей системы, а также из внешнего диска. Присутствует возможность сохранения результатов.

Настройки:



MyLastSearch

MyLastSearch сканирует кэш и файлы историй вашего веб-браузера и определяет все пользовательские запросы, которые вы сделали в самых популярных поисковых системах (Google, Yahoo и MSN), на самых популярных сайтах социальных сетей (Twitter, Facebook, MySpace), а также на других популярных сайтах (YouTube, Wikipedia, Friendster, hi5).

К сожалению, программа не знает про google.ru (с google.com всё в порядке) и не знает про yandex.ru – т.е. поиски по этим сайтам она не видит.
UPD: Начиная с версии 1.65 добавлена поддержка для поисков в Yandex, DuckDuckGo и google.ru.

Программы для просмотра кэша браузеров (IECacheView, MozillaCacheView, ChromeCacheView, MZCacheView)

Работа программ IECacheView, MozillaCacheView, ChromeCacheView, MZCacheView напоминает работу **BrowsingHistoryView**, но просмотр кэша

позволяет видеть каждый индивидуальный файл (скаченные ссылки, изображения и т.д.), а не только адреса посещённых страниц.

Программы для просмотра кукиз (ChromeCookiesView, IECookiesView, MZCookiesView, EdgeCookiesView)

Как вы уже поняли, ChromeCookiesView, IECookiesView, MZCookiesView, EdgeCookiesView используются для просмотра кукиз в различных веб-браузерах.

На самом деле, выделение раздела программ для IT криминалистики, на мой взгляд, довольно условно – там все программы в той или иной мере предназначены для цифровой криминалистики. Особенно это касается программ для извлечения сохранённых на компьютер паролей – кстати, перейдём теперь к ним.

EdgeCookiesView — это инструмент для Windows, который отображает файлы cookie, хранящиеся в более новых версиях веб-браузера Microsoft Edge и IE11 (начиная с Fall Creators Update 1709 для Windows 10). Он также позволяет вам выбрать один или несколько файлов cookie, а затем экспортировать их в файл с разделителями табуляции, файл csv, файл html или файл в формате cookie.txt. Вы можете прочитать файлы cookie из текущей работающей системы или из базы данных WebCacheV01.dat на внешнем жёстком диске.

Примечание. Новая версия Edge теперь основана на Chromium, поэтому вы можете использовать инструмент ChromeCookiesView для просмотра файлов cookie этого нового веб-браузера Edge.

EdgeCookiesView и **IECookiesView**

IECookiesView — очень старый инструмент, изначально разработанный в 2002 году (!), И он до сих пор работает с более ранними версиями веб-браузера Edge, которые хранят файлы cookie в текстовых файлах, точно так же, как Internet Explorer. Но начиная с Fall Creators Update 1709 для Windows 10 файлы cookie веб-браузера Microsoft Edge хранятся в базе данных WebCacheV01.dat вместе с историей и информацией кеша, поэтому IECookiesView больше не может читать файлы cookie Edge.

EdgeCookiesView — это новый инструмент, предназначенный для чтения файлов cookie из базы данных WebCacheV01.dat.

Программы для мониторинга сети

Wireless Network Watcher

Wireless Network Watcher – это небольшая программа, которая сканирует вашу беспроводную сеть и отображает список всех компьютеров и устройств, которые в данный момент подключены к ней.

Для каждого компьютера или устройства, подключённого к вашей сети, отображается следующая информация: IP адрес, MAC адрес, компания-производитель сетевой карты и, опционально, имя компьютера.

WifiInfoView

WifiInfoView сканирует беспроводные сети в вашей области и отображает расширенную информацию о них, включая: имя сети (SSID), MAC адрес, тип PHY (802.11g или 802.11n), RSSI, качество сигнала, частоту, номер канала,

максимальную скорость, имя компании, модель роутера и имя роутера (только для роутеров, которые предоставляют эту информацию) и другое.
При выделении элемента, внизу отображает информация об этом устройстве в шестнадцатеричном формате.

CountryTraceRoute

CountryTraceRoute утилита построения маршрута (Traceroute), похожа на tracert для Windows, но с графическим пользовательским интерфейсом, а также намного быстрее tracert из Windows. CountryTraceRoute также отображает страну-владельца каждого IP адреса, найденного в маршруте.

Программы для извлечения информации из веб-браузеров и почтовых клиентов

ChromePass

ChromePass — это небольшой инструмент для восстановления пароля для Windows, который позволяет просматривать имена пользователей и пароли, хранящиеся в веб-браузере Google Chrome. Для каждой записи пароля отображается следующая информация: URL-адрес источника, URL-адрес действия, поле имени пользователя, поле пароля, имя пользователя, пароль и время создания. Программа позволяет вам получить пароли из вашей текущей работающей системы или из профиля пользователя, хранящегося на внешнем диске.

Вы можете выбрать один или несколько элементов, а затем сохранить их в файл text/html/xml или скопировать в буфер обмена.

Известные проблемы: в последних версиях веб-браузера Яндекса изменили шифрование паролей, и теперь оно отличается от шифрования паролей в Chrome, поэтому ChromePass больше не может расшифровывать пароли веб-браузера Яндекса.

BrowserAddonsView

BrowserAddonsView отображает подробности о всех дополнениях/плагинах веб-браузера, установленных в вашу систему. BrowserAddonsView может сканировать и определять дополнения большинства популярных браузеров: Chrome, Firefox и Internet Explorer. Для Chrome и Firefox, BrowserAddonsView сканирует все профили веб-браузера, если их несколько.

WebCookiesSniffer

WebCookiesSniffer захватывает все кукиз веб-сайтов, отправляемые между веб-браузером и веб-сервером и отображает их в простой таблице кукиз. Верхняя панель WebCookiesSniffer показывает строку куки и имя сайта/хоста, который отправил или принял это куки. При выборе строки куки в верхней

панели, WebCookiesSniffer разбирает строку куки и отображает кукиз в нижней панели в формате имя-значение.

Утилиты, связанные с Интернетом, сетью и сетевым оборудованием

DomainHostingView

DomainHostingView – это программа для Windows, которая собирает обширную информацию о домене, используя серию DNS и WHOIS запросов и генерирует HTML отчёт, который можно открыть в веб-браузере.

Информация включает в себя: хостинг-компанию или дата центр, который хостит веб-сервер, почтовый сервер и сервер доменных имён (DNS) указанного домена, даты создания/изменения/истечения домена, владельца домена, регистратора домена, список всех DNS записей и другое.

IPNetInfo

IPNetInfo – это программка, которая позволяет вам с лёгкостью найти всю доступную информацию об IP адресе: владельца IP адреса, страну/штат, диапазон IP адресов, контактную информацию (адрес, телефон, факс и email) и другое.

IPNetInfo может извлекать все IP адреса из заголовков сообщения электронной почты – достаточно скопировать их в программу и она отобразит всю информацию об этих IP адресах.

MACAddressView

MACAddressView делает поиск по базе данных MAC адресов для поиска информации о компании (имя компании, адрес, страна), которая произвела данное сетевое устройство.

MACAddressView не посылает каких-либо запросов на удалённый сервер, он использует вшитую в .exe файл базу MAC адресов

PingInfoView

PingInfoView — это небольшая утилита, которая позволяет легко пинговать несколько имён хостов и IP-адресов и просматривать результат в одной таблице. Она автоматически проверяет связь со всеми хостами каждые указанное вами количество секунд и отображает количество успешных и неудачных проверок связи, а также среднее время проверки связи. Вы также можете сохранить результат ping в файл text/html/xml или скопировать его в буфер обмена.

Новая версия PingInfoView (2.00) позволяет использовать TCP ping для указанного номера порта вместо стандартного ICMP ping.

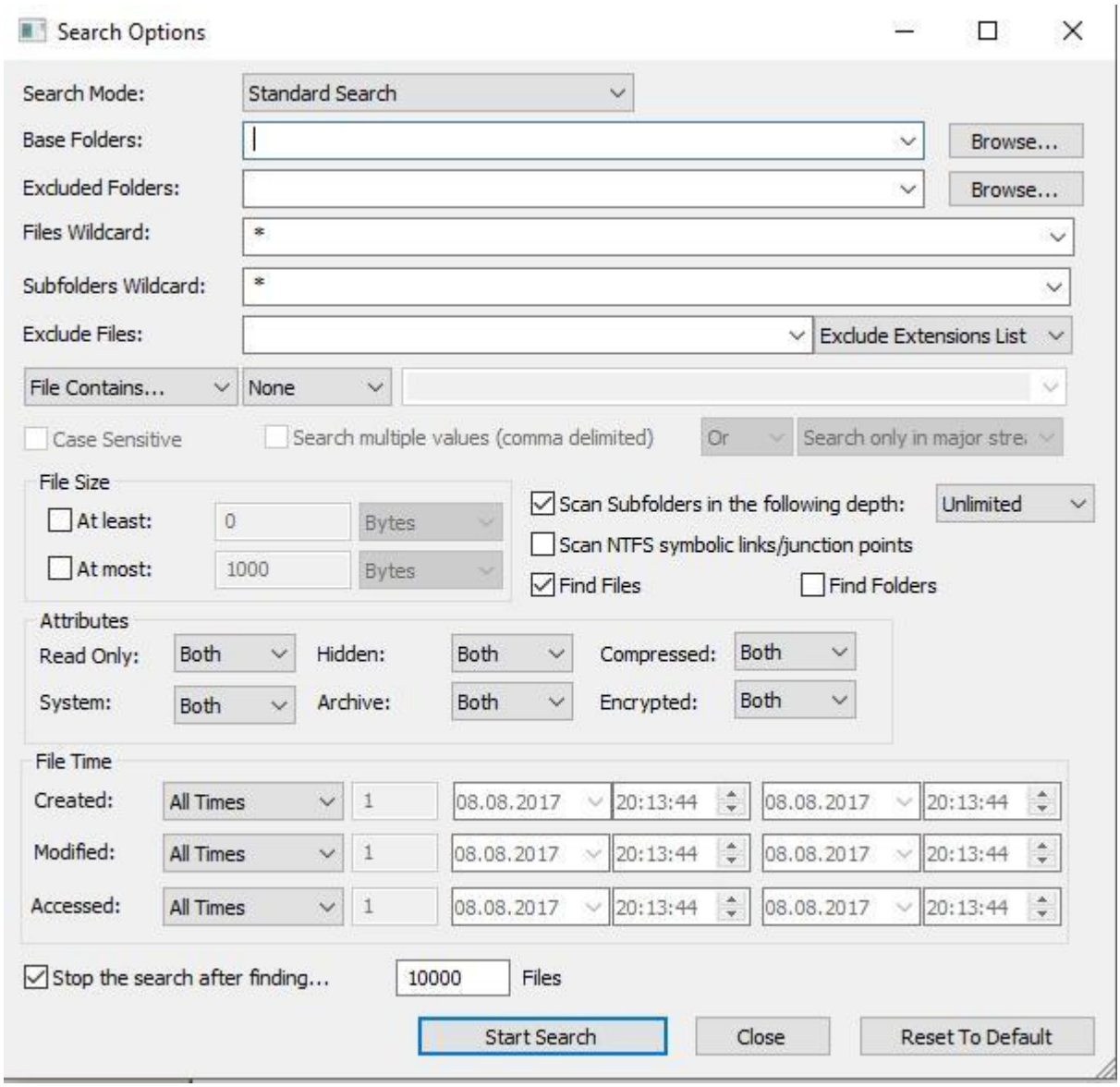
Чтобы использовать новую функцию TCP ping, просто укажите имя хоста или IP-адрес с номером TCP-порта, например: 10.0.0.10:21, 192.168.0.50:80, www.nirsoft.net:443

FastResolver

FastResolver переводит имена хостов в IP адреса и наоборот. Просто введите список IP адресов или имён хостов, которые вы хотите преобразовать. Также понимается ввод диапазонов IP, который вы хотите просканировать. Для локальной сети FastResolver также позволяет вам получить MAC адреса всех IP адресов, которые вы сканируете. FastResolver является многопоточным приложением, поэтому вы можете просканировать десятки адресов в считаные секунды.

Дисковые утилиты

SearchMyFiles



SearchMyFiles – это альтернатива стандартному модулю поиска Windows. Эта программа позволяет вам с лёгкостью искать файлы в вашей системе с использованием подстановочных символов, по времени последней модификации/создания/последнего доступа, по атрибутам файла, по содержимому файла (текстовый или бинарный поиск) и по размеру файла. SearchMyFiles позволяет вам задать очень точный поиск, который не может быть выполнен с поиском Windows. Например, вы можете найти все файлы, созданные за последние 10 минут и с размером между 500 и 700 байт.

После нахождения файлов, вы можете выбрать один или несколько из них и сохранить список в текстовый/html/csv/xml файл или скопировать список в буфер обмена.

SearchMyFiles является портативной программой, вы можете использовать её с USB флэшки без оставления следов в реестре просканированного компьютера.

MobileFileSearch

MobileFileSearch — это инструмент для Windows, который позволяет вам искать файлы внутри мобильного устройства (смартфона или планшета), подключённого к USB-порту вашего компьютера, с помощью протокола передачи мультимедиа (MTP). Вы можете искать файлы по их размеру, времени создания, времени изменения или имени (используя подстановочный знак).

Найдя файлы на своём смартфоне/планшете, вы можете при желании удалить их, скопировать в папку на своём компьютере или экспортировать список файлов в файл csv/разделённый табуляцией/html/xml/JSON.

MobileFileSearch также позволяет активировать поиск из командной строки и затем экспортировать результат в файл или копировать найденные файлы в нужную папку на вашем компьютере.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.2»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. С помощью утилиты InstalledPackagesView выполните просмотр информации об установленных пакетах программного обеспечения. Просмотрите информацию о приложениях, установленных компанией «Microsoft Corporation».

2. С помощью утилиты *SpecialFoldersView* выполните просмотр системных папок ОС Windows

3. С помощью утилиты ExifDataView выполните просмотр метаданных Exif, хранящиеся в файлах изображений .jpg, найденых на компьютере.

4. С помощью утилиты FullEventLogView выполните просмотр событий из журналов событий Windows. Экспортируйте полученные данный в файл формата csv с TAB разделителями/html/xml.

5. С помощью утилиты BrowsingHistoryView просмотрите информацию о посещенных сайтах различными браузерами на компьютере. Сохраните полученные результаты.

6. С помощью утилит MozillaCacheView, ChromeCacheView, MZCacheView выполните просмотр кэша браузеров.

7. С помощью утилит ChromeCookiesView, IECookiesView, MZCookiesView, EdgeCookiesView выполните просмотр файлов кукиз различных браузеров.

8. В помощью утилиты ChromePass выполните восстановление пароля для Windows, который позволяет просматривать имена пользователей и пароли, хранящиеся в веб-браузере Google Chrome.

9. В помощью утилиты owserAddonsVie выполните просмотр и анализ плагинов браузеров.

10. С помощью утилиты WebCookiesSniffer выполните перехват кукиз веб-сайтов, отправляемых между веб-браузером и веб-сервером.

11. С помощью утилиты DomainHostingView выполните просмотр информации (сведения о хостинг-компании или дата центре, который хостит веб-сервер, почтовом сервере и сервере доменных имён (DNS) указанного домена, даты создания/изменения/истечения домена, владельца домена, регистратора домена, список всех DNS записей и др.) о любом известном вам домене.

12. С помощью утилиты IPNetInfo осуществите просмотр информации (сведения о владельце IP адреса, страна, диапазон IP адресов, контактная информация (адрес, телефон, факс и email) и др.) о любом известном вам IP-адресе.

13. С помощью утилиты IPNetInfo осуществите просмотр заголовков сообщения электронной почты (для этого скопируйте их в программу, и она отобразит всю информацию об этих IP адресах).

14. С помошью утилиты MACAddressView выполните поиск по базе данных MAC адресов. Установите информацию о компании (имя компании, адрес, страна), которая произвела ваше сетевое устройство.

15. С помощью FastResolver утилиты осуществите перевод IP-адресов (таблица 1) в имена хостов.

16. С помощью утилиты SearchMyFiles осуществите поиск на вашем компьютере файлов, созданных за последние 10 часов, с расширением *.dat и с размером между 10 и 100 байт.

2. Анализ сетевой активности с использованием прикладного программного обеспечения «Wireshark».

Краткие теоретические сведения:

Программы анализа сетевого трафика играют важную роль в обеспечении сетевой кибербезопасности благодаря следующим возможностям:

1. Выявление вредоносной активности:

• ПО позволяет анализировать сетевой трафик и выявлять подозрительные шаблоны, характерные для вредоносных программ. Например, он может обнаружить необычные запросы к удаленным серверам, эксплойты или попытки распространения вредоносных программ по сети.

2. Анализ атак:

• В случае кибератаки данное ПО может быть использовано для сбора и анализа сетевого трафика, связанного с атакой. Это помогает выявить начальную точку атаки, использованные техники и тактики, а также масштаб ущерба.

3. Мониторинг соответствия:

• ПО помогает организациям отслеживать сетевой трафик и обеспечивать соответствие нормативным требованиям и стандартам безопасности. Он может обнаруживать нарушения политик безопасности, такие как несанкционированный доступ к данным или нарушения правил сетевого протокола.

4. Исследование инцидентов:

• ПО является ценным инструментом для расследования инцидентов кибербезопасности. Он позволяет экспертам собрать и проанализировать сетевой трафик, связанный с инцидентом, для определения причины возникновения инцидента и разработки мер по его устранению.

5. Выявление уязвимостей:

• ПО может быть использован для выявления уязвимостей в сетевых устройствах и приложениях. Анализируя сетевой трафик, можно обнаружить неправильные конфигурации, открытые порты или уязвимые протоколы, которые могут быть использованы злоумышленниками для компрометации системы.

6. Оценка производительности сети:

• Указанное ПО можно использовать для оценки производительности сети и выявления узких мест. Анализируя сетевой трафик, можно определить задержки, потери пакетов и другие проблемы, влияющие на скорость и надежность сети.

Одним из самых популярных анализаторов сетевой активности является бесплатно распространяемое, мультиплатформенное и гибкое программное обеспечение «Wireshark».

Что такое Wireshark?

Wireshark – это популярный анализатор сетевых пакетов и протоколов с открытым исходным кодом. Он имеет большое значение для специалистов по безопасности и системных администраторов. Инструмент используется для анализа структуры различных сетевых протоколов и имеет практическое значение. Wireshark способен работать на различных платформах, таких как Windows, Unix, Linux; он использует инструментарий виджетов GTK+ или PCAP для захвата пакетов. Программа также имеет бесплатные версии программного обеспечения на базе терминалов, такие как Tshark. По своему функционалу инструмент очень похож на tcpdump, разница лишь в том, что он поддерживает графический пользовательский интерфейс (GUI) и имеет функции выставления фильтров для просмотра информации.

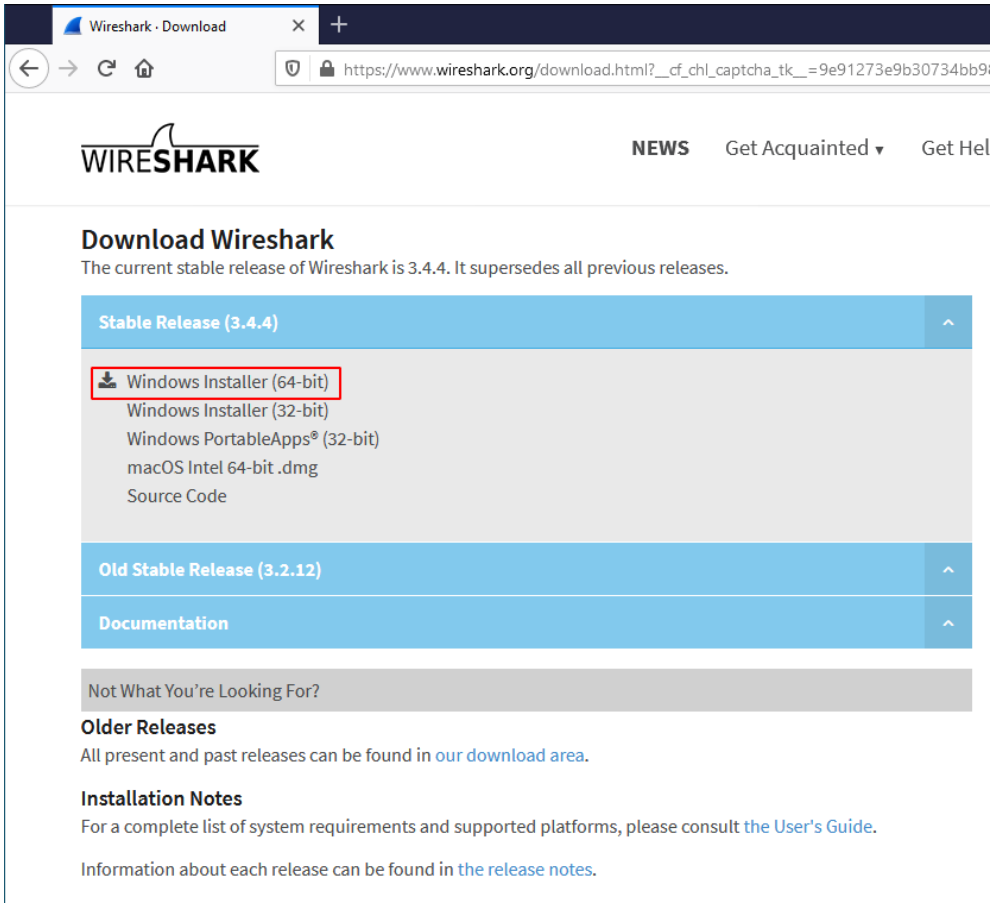
Wireshark обладает следующими характерными чертами:

- Может работать в UNIX и Windows.
- Осуществляет захват данных пакетов в режиме реального времени из сетевого интерфейса.
- Открывает файлы, содержащие захваченные пакетные данные (файлы PCAP).
- Производит импорт пакетов из текстовых файлов, содержащих шестнадцатеричные дампы.
- Имеет фильтры отображения информации, которые используются для фильтрации и организации полученных данных.
- Показывает пользователю пакеты с подробной информацией о протоколе.
- Новые протоколы можно тщательно изучить, если создать плагины.
- Захваченный трафик можно отслеживать с помощью Voice Over IP (VOIP) по сети.
- Пользователь способен произвести импорт некоторых или всех пакетов в различные форматы файлов захвата.
- Есть фильтры пакетов по многим критериям.
- Осуществляет поиск пакетов по многим критериям.
- Можно установить определенный цвет для пакета данных в зависимости от его состояния.
- Есть возможность просматривать статистические данные.

Установка Wireshark

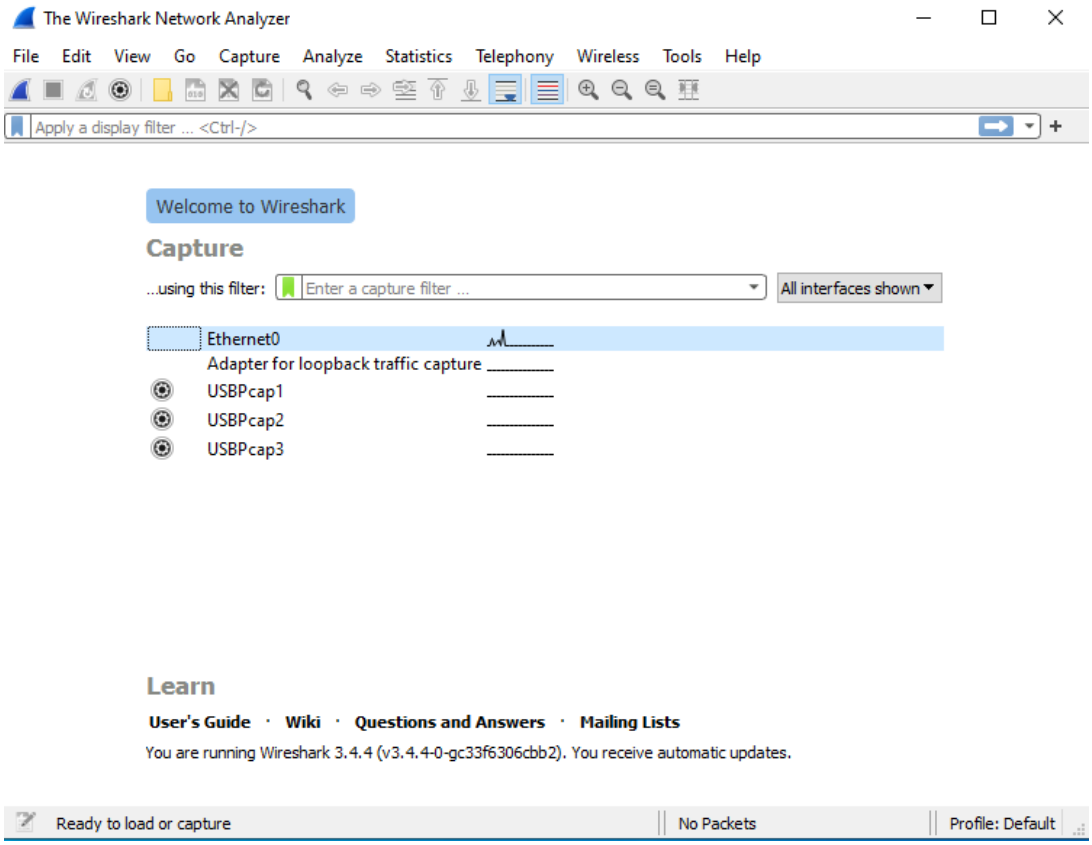
Для Windows

Wireshark можно бесплатно скачать с официального сайта программы как для Windows, так и для macOS. (https://www.wireshark.org/download.html)



После скачивания Wireshark пользователю нужно перейти в каталог загрузок и запустить установочный файл Wireshark. Во время инсталляции программы следует выбрать параметр установки Npcap, поскольку он включает в себя библиотеки, необходимые для сбора данных в режиме реального времени.

После установки Wireshark пользователю следует войти в систему от имени администратора, чтобы корректно использовать инструмент. На macOS нужно щелкнуть правой кнопкой мыши на значок приложения Wireshark и выбрать параметр «Просмотреть подробную информацию». В меню настроек «**Общий доступ и разрешения**» надо предоставить администратору права на чтение и запись данных.

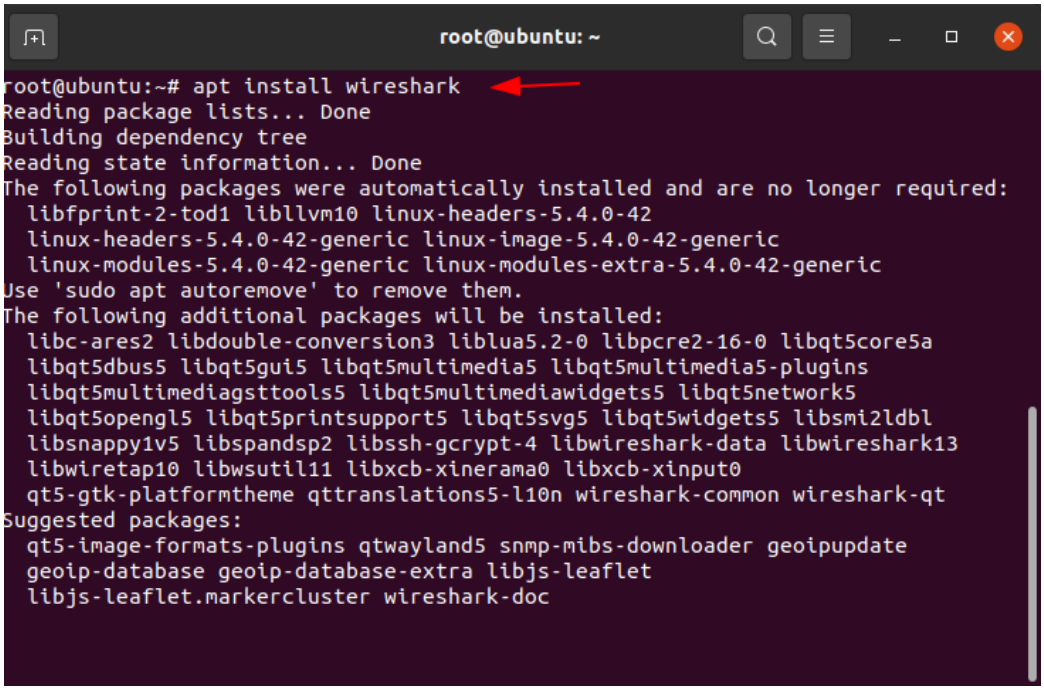


Для Linux

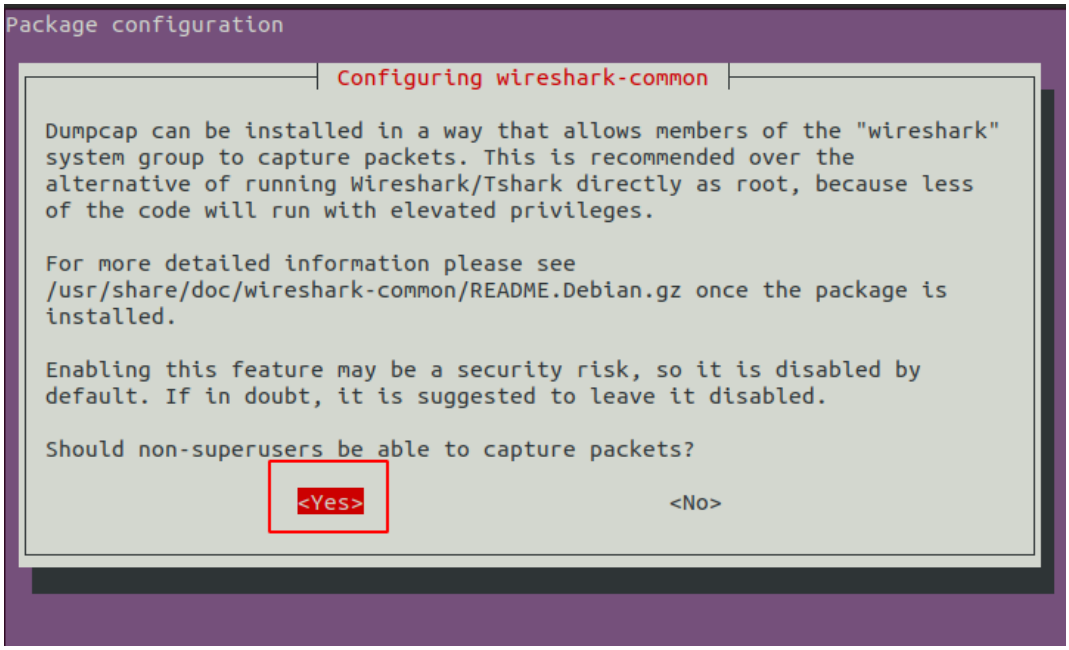
Wireshark также доступен для установки на Linux и другие UNIX-подобные платформы, включая **Red Hat** и**FreeBSD**.

Чтобы скачать Wireshark, пользователь откроет терминал и введет следующую команду:

«apt install wireshark»



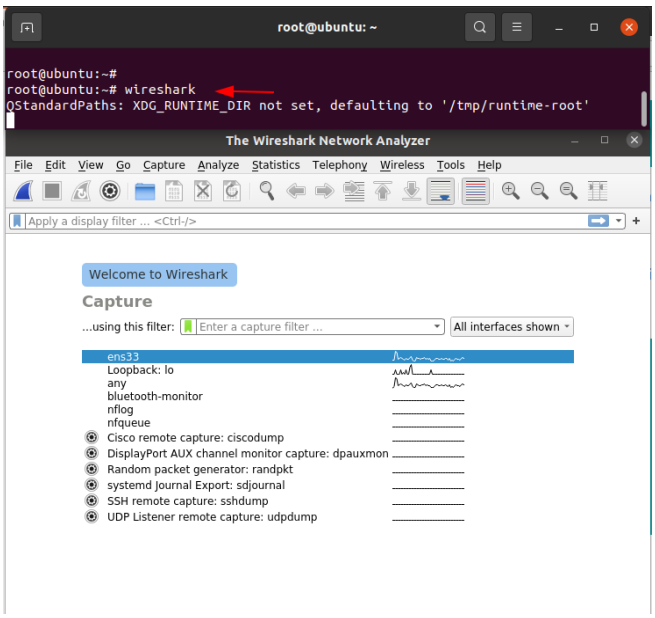
Необходимо нажать на клавишу «Y», когда будет нужно, чтобы установить программу и предоставить ей достаточно свободного места. Во время установки пользователю будет задан вопрос: «Могут ли не суперпользователи захватывать пакеты?». В целях безопасности рекомендуется разрешать доступ к Wireshark только суперпользователям. В данном случае пользователь выбирает вариант «Да». Установка Wireshark продолжается. Ура! Как видно, программа была успешно установлена.



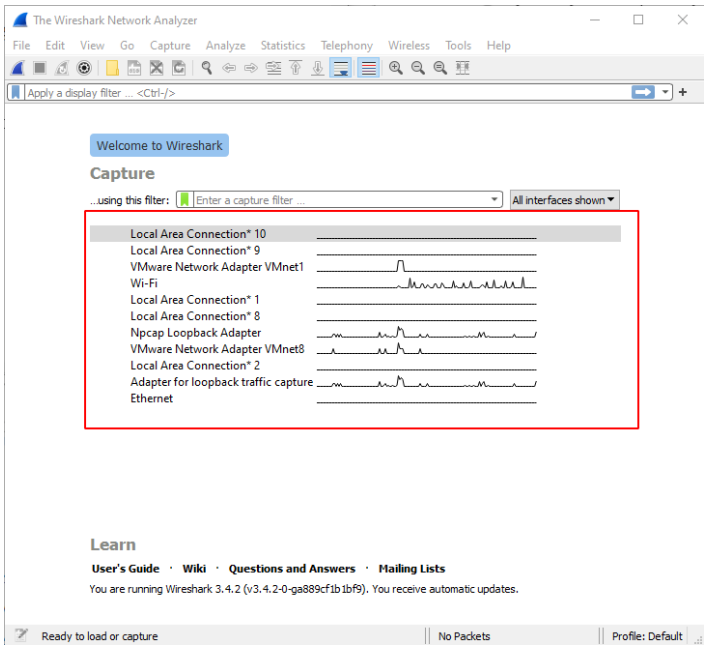
Чтобы открыть Wireshark, следует выполнить следующую команду.

Инструмент откроется в таком виде, как показано ниже на картинке.

«Wireshark»



Всякий раз, когда пользователь будет запускать Wireshark, перед ним будет появляться такое изображение.

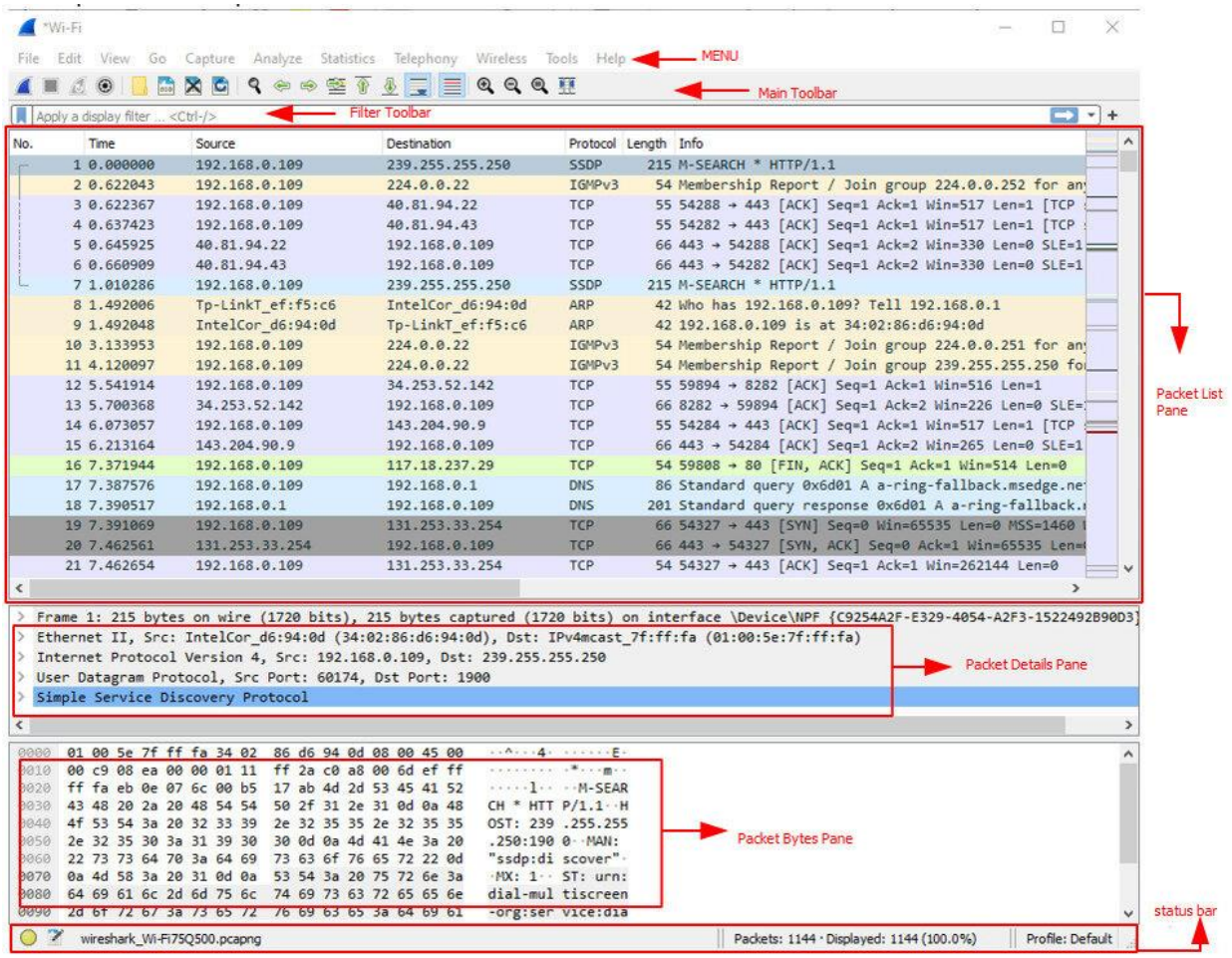


Здесь можно увидеть различные сетевые интерфейсы, доступные на устройстве. На приведенном выше изображении видно, что по сети Wi-Fi передается много трафика. В большинстве случаев пользователь сможет видеть только трафик, входящий и исходящий с его собственного устройства. Однако некоторые беспроводные сетевые карты можно настроить в режим монитора, чтобы была возможность также отслеживать трафик с других беспроводных устройств, подключенных к сети.

Пользовательский интерфейс Wireshark

Главный экран

Стоит быстро взглянуть на пользовательский интерфейс Wireshark. Обычно пользователь видит его таким после того, как некоторые пакеты были захвачены или загружены.

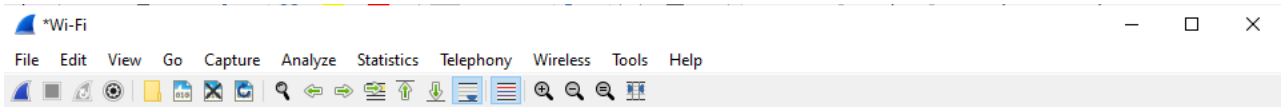


Главный экран Wireshark состоит частей, которые обычно называются программами GUI.

1. «**Меню**» необходимо для выполнения действий.
2. «**Главная панель инструментов**» предоставляет пользователю быстрый доступ к часто используемым параметрам меню.
3. «**Панель с фильтрами**» дает пользователю возможность установить определенные фильтры отображения для того, чтобы просмотреть нужные пакеты.
4. На панели «**Список пакетов**» можно просмотреть подробную сводку данных по каждому захваченному пакету.
5. «**Сведения о пакетах**» показывает пользователю информацию о пакете, выбранном из списка.
6. На панели «**Байты пакетов**» отображаются данные из пакета, выбранного ранее, а также выделены сведения о нем.
7. В строке «**Состояние**» отображается подробная информация о текущем состоянии программы и захваченных данных.

Меню

Главное меню Wireshark расположено в верхней части главного экрана (Windows, Linux).



Главное меню содержит следующие разделы:

File

Данный раздел включает в себя опции для открытия и объединения файлов захвата, сохранения, печати или их экспорта в различных форматах.

Edit

Этот раздел содержит параметры для поиска пакета, привязки времени или пометки одного или нескольких пакетов, обработки профилей конфигурации и выбора предпочтений. Вырезание, копирование и вставка пакетов данных в настоящее время не реализованы.

View

В этом разделе можно изменять параметры отображения захваченных данных, включая цветовую гамму, размер шрифта, раскрытие и сворачивание деталей о полученных пакетах.

Go

С помощью данного раздела пользователь может перейти к определенному пакету.

Capture

В этом разделе можно запускать и останавливать процесс захвата, а также редактировать фильтры. Некоторые из нужных фильтров, которые сделают работу пользователя в инструменте комфортной, представлены ниже.

Analyze

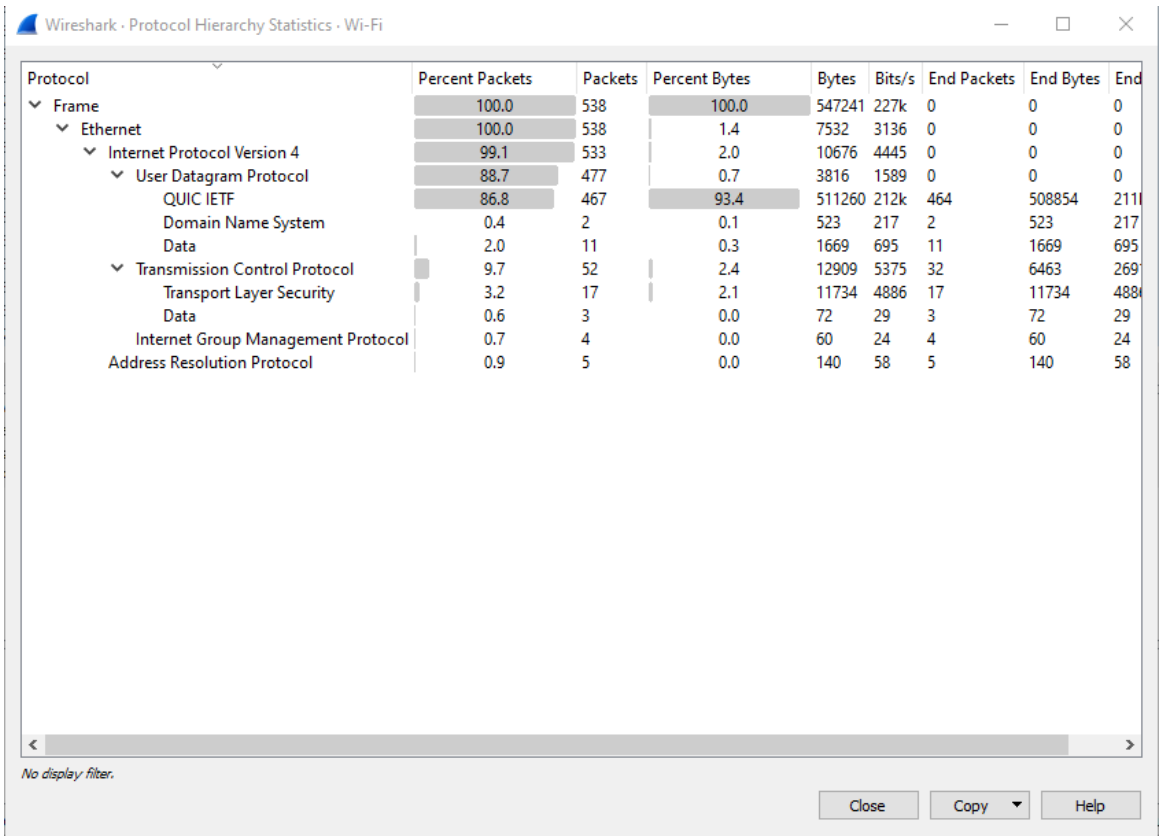
В этом разделе пользователь найдет опции для управления фильтрами отображения, включения или отключения деления протоколов, настройки пользовательских декодов и следования протоколу TCP.

Statistics

Данный раздел содержит опции для отображения различных окон со статистикой, включая сводку захваченных пакетов, иерархию протоколов и не только.

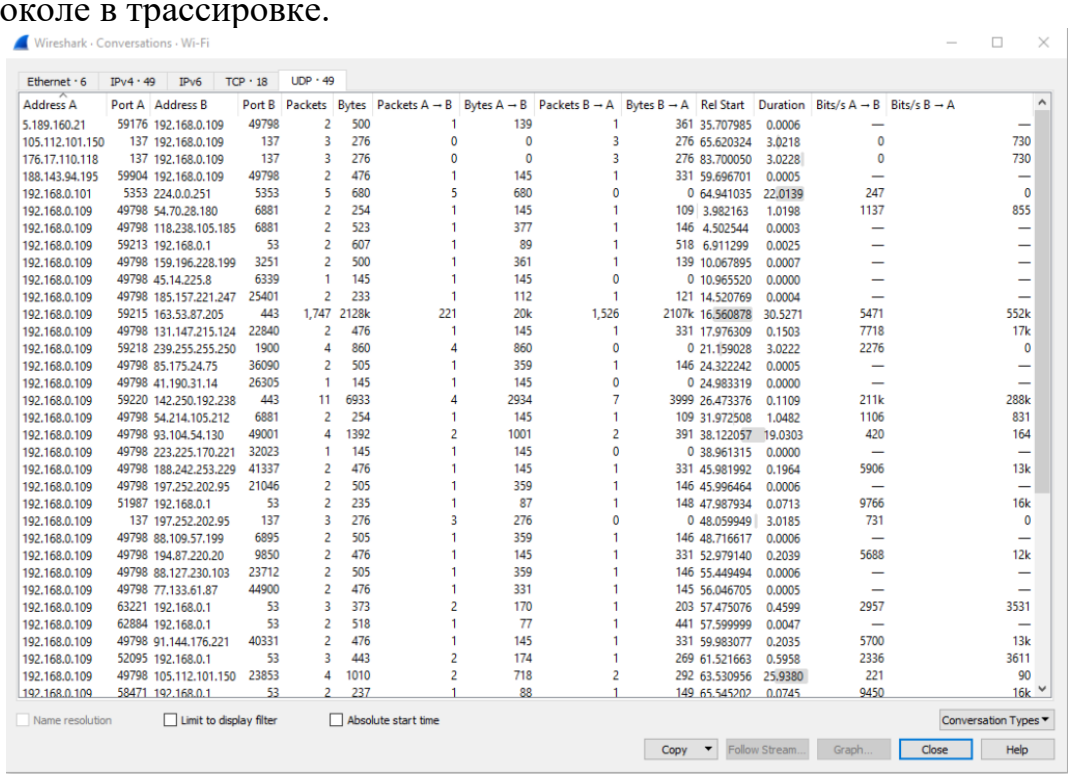
Statistics -> Protocol Hierarchy

- Представлена описательная статистика работы каждого протокола.
- Информация будет полезна для определения типов, объемов и относительных пропорций протоколов в трассировке.



Statistics -> Conversations

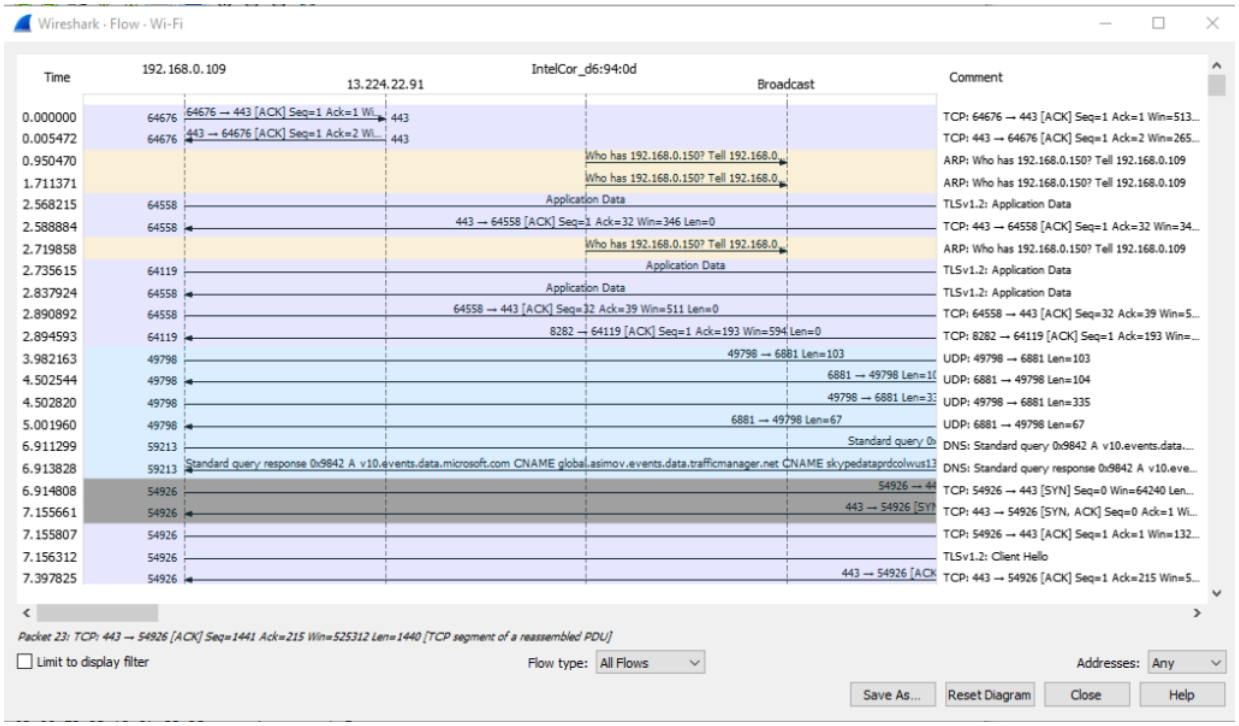
- Представлена описательная статистика каждого «разговора» в каждом протоколе в трассировке.



Statistics -> Flow Graph

- Здесь виден график последовательности отправки данных в выбранном трафике.

- Информация будет полезна для понимания расчетов seq. и ack.



Telephony

В этом разделе есть опции для отображения различных окон статистики, связанных с телефонией, включая анализ мультимедиа, блок-схем, иерархии протоколов отображения и не только.

Wireless

Этот раздел содержит параметры для отображения статистики беспроводной связи Bluetooth и IEEE 802.11.

Tools

В этом разделе есть различные инструменты, доступные в Wireshark, такие как **Firewall ACL Rules**.

Help

Этот раздел содержит опции, помогающие пользователю получить доступ к справке, страницам со сведениями о различных инструментах командной строки.

Главная панель инструментов

Главная панель инструментов обеспечивает пользователю быстрый доступ к часто используемым элементам меню. Она может быть настроена в соответствии с имеющимися требованиями.

Доступные функции описаны ниже (см. картинки).

Toolbar Icon	Toolbar Item	Description
	Start	**Starts capturing packets with the same options as the last capture or the default options if none were set**
	Stop	**Stops the currently running capture**
	Restart	**Restarts the current capture session**
	Options	**Opens the "Capture Options" dialog box**
	Open	**Opens the file open dialog box, which allows you to load a capture file for viewing**
	Save As	**Save the current capture file to whatever file you would like**
	Close	**Closes the current capture. If you have not saved the capture, you will be asked to save it first**
	Reload	**Reloads the current capture file**
	Find packet	**Find a packet based on different criteria**
	Go back	**Jump back in the packet history. Hold down the Alt key (Option key on macOS) to go forward in the selection history**

Toolbar Icon	Toolbar Item	Description
	Go Forward	**Jump forward in the packet history. Hold down the Alt key (Option on macOS) to go forward in the selection history.**
	Go To Packet	**Go to a specific packet**
	Go To First Packet	**Jump to the last packet of the capture file**
	Go To Last Packet	**Jump to the last packet of the capture file**
	Auto Scroll in Live capture	**Auto scroll packet list while doing a live capture (or not)**
	Colorize	**Colorize the packet list (or not)**
	Zoom In	**Zoom out of the packet data (increase the font size)**
	Zoom Out	**Zoom out of the packet data (decrease the font size)**
	Normal Size	**Set zoom level back to 100%**
	Resize Columns	**Resize columns, so the content fits into them.**

[Источник]

Панель с фильтрами

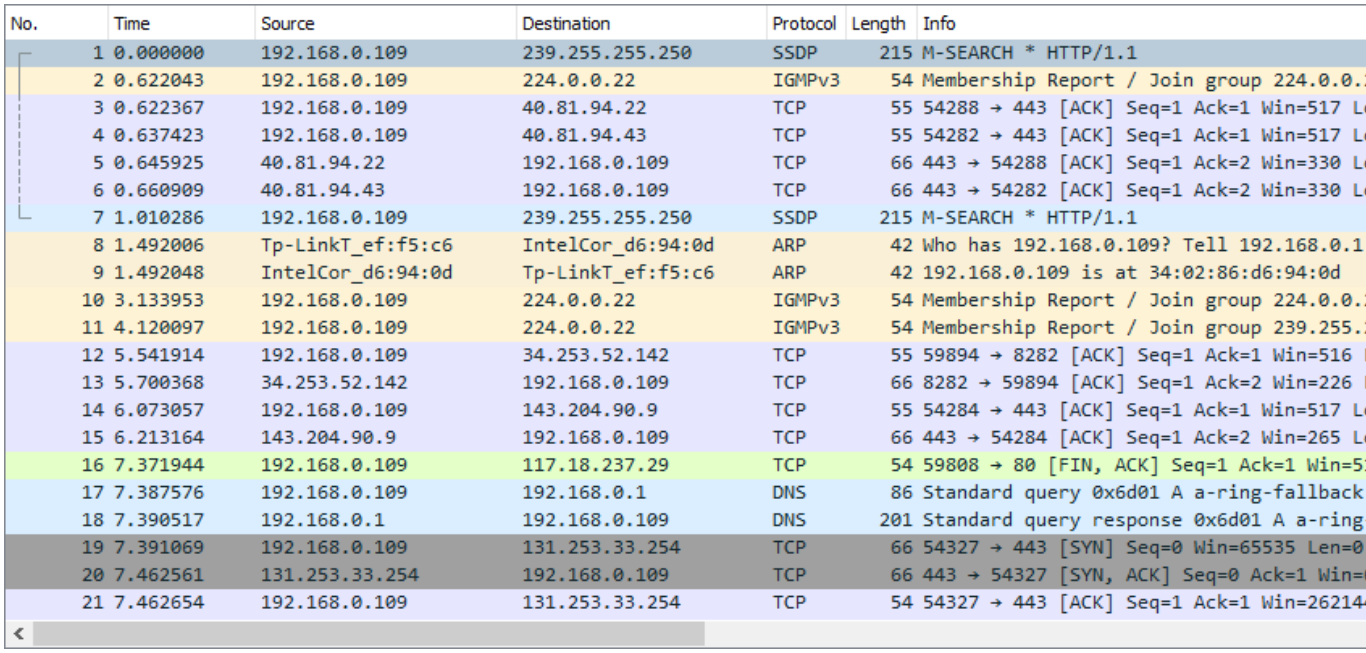
Панель с фильтрами дает возможность быстро редактировать и применять фильтры отображения полученных данных.

Доступные функции описаны ниже (см. картинку).

Toolbar Icon	Name	Description
	Bookmarks	Manage or select save filters.
	Filter input	**The area is provided to enter or edit a display string. A syntax check of your filter string while you are typing such as the background will turn red if you enter an incomplete or invalid string and will become green when you enter a valid string.**
	Clear	Reset the current display filter and clear the edit area.
	Apply	Apply the current value in the edit area as the new display filter.
	Recent	Select from a list of recently applied filters.
	Add Button	Add a new filter button.

Список пакетов

В меню «Список пакетов» показаны все пакеты в том порядке, в котором они были записаны.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.109	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2	0.622043	192.168.0.109	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.
3	0.622367	192.168.0.109	40.81.94.22	TCP	55	54288 → 443 [ACK] Seq=1 Ack=1 Win=517 L
4	0.637423	192.168.0.109	40.81.94.43	TCP	55	54282 → 443 [ACK] Seq=1 Ack=1 Win=517 L
5	0.645925	40.81.94.22	192.168.0.109	TCP	66	443 → 54288 [ACK] Seq=1 Ack=2 Win=330 L
6	0.660909	40.81.94.43	192.168.0.109	TCP	66	443 → 54282 [ACK] Seq=1 Ack=2 Win=330 L
7	1.010286	192.168.0.109	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
8	1.492006	Tp-LinkT_ef:f5:c6	IntelCor_d6:94:0d	ARP	42	Who has 192.168.0.109? Tell 192.168.0.1
9	1.492048	IntelCor_d6:94:0d	Tp-LinkT_ef:f5:c6	ARP	42	192.168.0.109 is at 34:02:86:d6:94:0d
10	3.133953	192.168.0.109	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.
11	4.120097	192.168.0.109	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.
12	5.541914	192.168.0.109	34.253.52.142	TCP	55	59894 → 8282 [ACK] Seq=1 Ack=1 Win=516
13	5.700368	34.253.52.142	192.168.0.109	TCP	66	8282 → 59894 [ACK] Seq=1 Ack=2 Win=226
14	6.073057	192.168.0.109	143.204.90.9	TCP	55	54284 → 443 [ACK] Seq=1 Ack=1 Win=517 L
15	6.213164	143.204.90.9	192.168.0.109	TCP	66	443 → 54284 [ACK] Seq=1 Ack=2 Win=265 L
16	7.371944	192.168.0.109	117.18.237.29	TCP	54	59808 → 80 [FIN, ACK] Seq=1 Ack=1 Win=5
17	7.387576	192.168.0.109	192.168.0.1	DNS	86	Standard query 0x6d01 A a-ring-fallback
18	7.390517	192.168.0.1	192.168.0.109	DNS	201	Standard query response 0x6d01 A a-ring
19	7.391069	192.168.0.109	131.253.33.254	TCP	66	54327 → 443 [SYN] Seq=0 Win=65535 Len=0
20	7.462561	131.253.33.254	192.168.0.109	TCP	66	443 → 54327 [SYN, ACK] Seq=0 Ack=1 Win=
21	7.462654	192.168.0.109	131.253.33.254	TCP	54	54327 → 443 [ACK] Seq=1 Ack=1 Win=26214

Каждая строка в списке пакетов соответствует одному пакету в файле захвата. Пользователь может нажать на определенную строку, чтобы получить более подробную информацию о пакете. Она будет отображаться в «Сведениях о пакетах» и «Байтах пакетов».

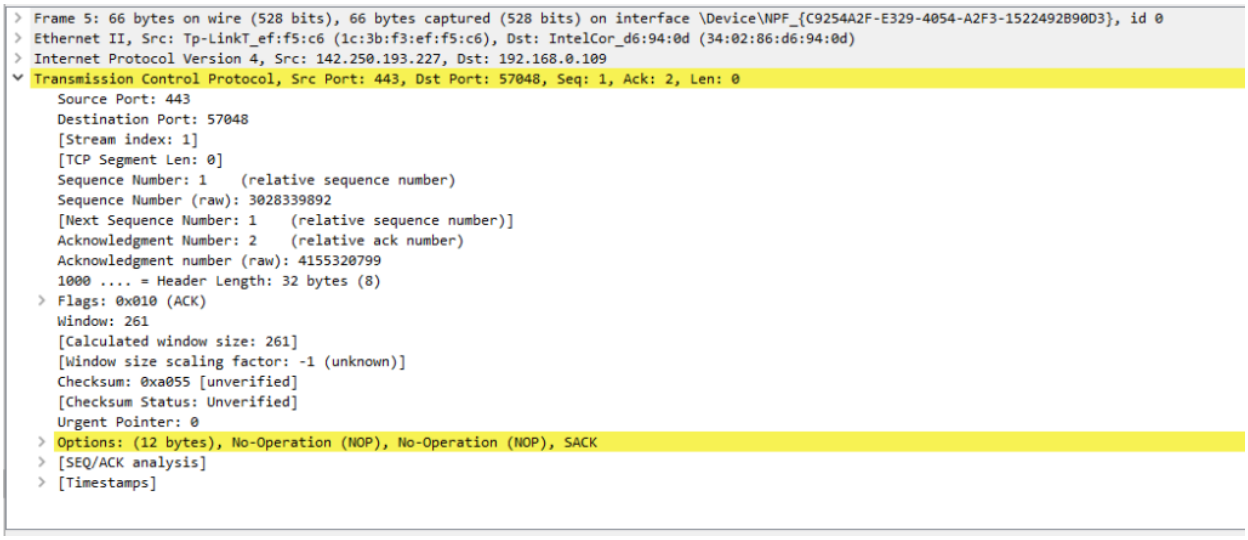
Есть много доступных столбцов с данными, такими как:

- **No**: Номер пакета в файле захвата. Это число не изменится, даже если используется фильтр отображения.

- **Time**: В этом столбце отображается отметка времени, когда был захвачен пакет. Формат представления этой временной метки может быть изменен.
- **Source**: Источник, откуда был получен пакет.
- **Destination**: Адрес, по которому отправляется этот пакет.
- **Protocol**: Протокол самого высокого уровня, который может быть обнаружен Wireshark.
- **Length**: Длина каждого пакета в байтах.
- **Info**: Дополнительная информация о содержимом пакета.

Сведения о пакетах

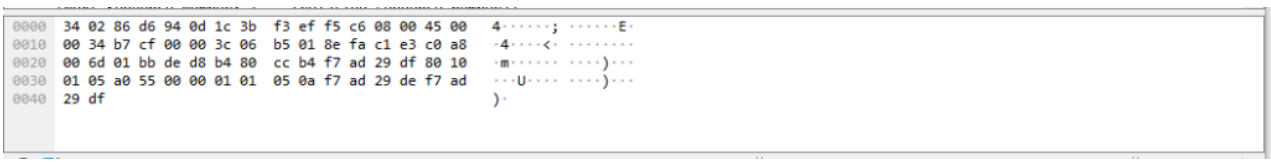
На данной панели сведений отображается выбранный или текущий пакет с подробной информацией о нем.



На панели выше показаны протоколы и поля протокола пакета, выбранного из списка. Протоколы отображаются в виде ветки, которую можно развернуть и свернуть.

Байты пакетов

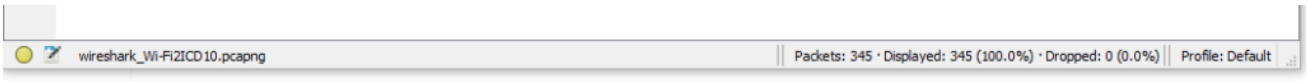
На панели «**Байты пакетов**» отображаются данные выбранного или текущего пакета в виде шестнадцатеричного дампа.



Каждая строка содержит смещение данных, шестнадцать шестнадцатеричных байтов и шестнадцать байтов ASCII. Непечатаемые байты заменяются точкой «.».

Состояние

На панели «**Состояние**» отображаются информационные сообщения, такие как:



The colourized bullet

В левой части экрана есть экспертная информация о загруженном в данный момент файле захвата. Наведение курсора мыши на «The colourized bullet» предоставит возможность просмотреть полученные данные.

The edit icon

Позволяет добавить комментарий к файлу захвата.

The middle

Он показывает текущее количество пакетов в файле захвата. Отображаются следующие значения:

Packets

Количество захваченных пакетов.

Displayed

Количество текущих пакетов.

Marked

Количество помеченных пакетов. Отображается только в том случае, если пользователь отметил какие-либо пакеты.

Dropped

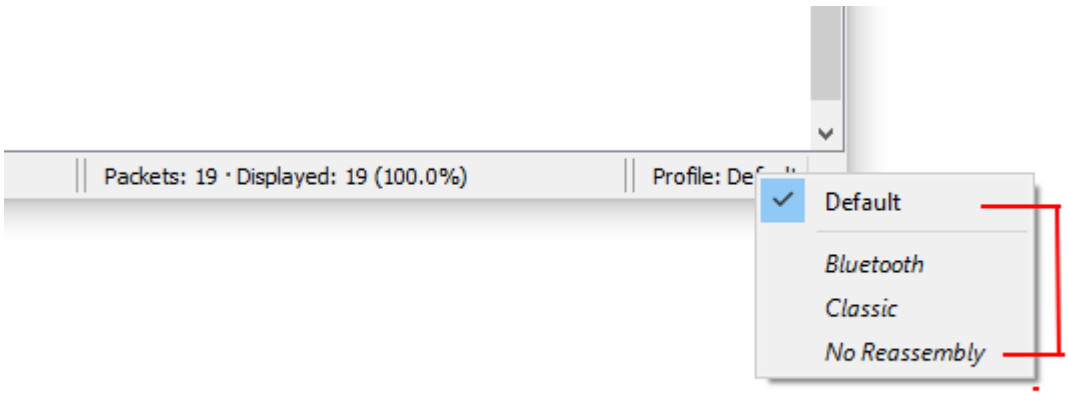
Количество «отброшенных» пакетов. Показывается только в том случае, если Wireshark не удалось захватить какие-то пакеты.

Ignored

Показывает количество проигнорированных пакетов.

The right side

Показывает выбранный профиль конфигурации. Щелчок по этой части строки состояния вызовет меню со всеми доступными профилями конфигурации. Пользователь может изменить его также здесь.



Захват пакетов

Для начала захвата пакетов можно использовать следующие методы.
Пользователь может дважды щелкнуть на нужный интерфейс на главном экране Wireshark.
Кроме того, если интерфейс уже известен, можно запустить Wireshark с помощью командной строки, выполнив следующую команду:
wireshark -I eth0 -k
Это запустит захват Wireshark на интерфейсе **eth0**.
После того, как пользователь захватил несколько пакетов, он может просмотреть их в списке. Просто щелкнув на пакет в «Списке пакетов», он получит о нем подробную информацию. Как только пользователь захватит трафик, нужно применить фильтр, чтобы сделать его понятным.
Wireshark имеет два языка фильтрации:

- **Фильтры захвата**
- **Фильтры отображения**

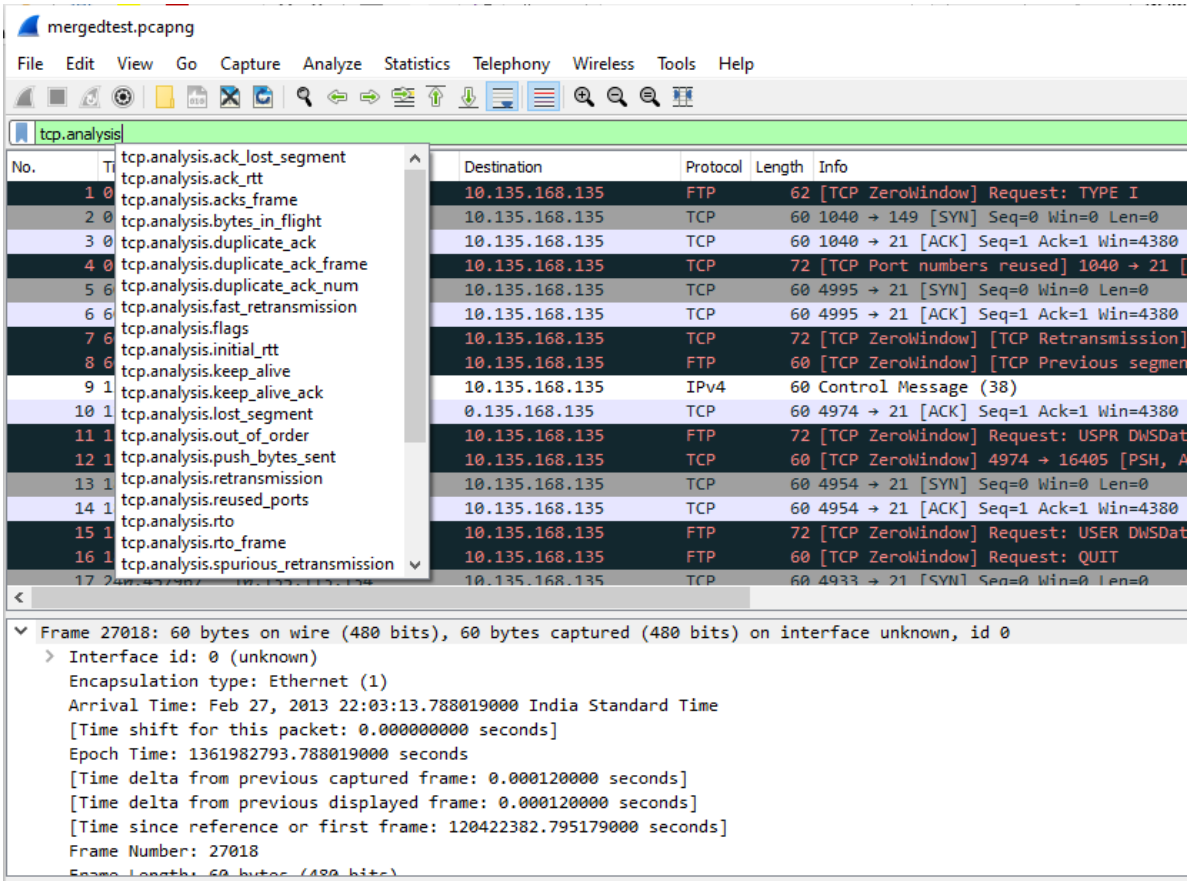
Фильтры захвата используются для фильтрации трафика при захвате пакетов, а фильтры отображения используются для фильтрации текущих пакетов.

Фильтры отображения

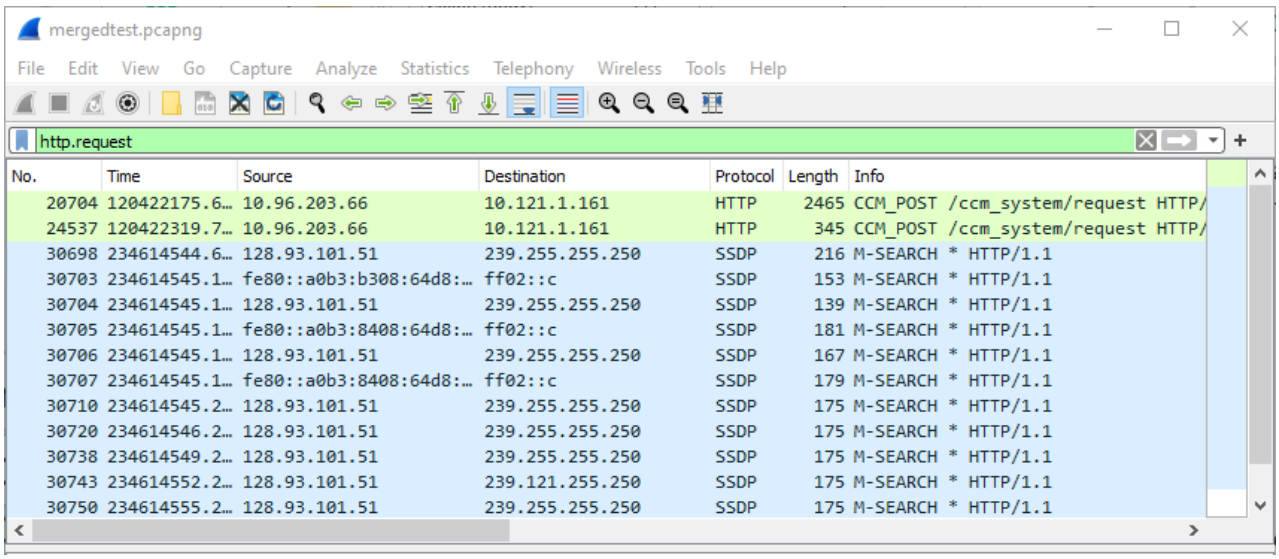
Панель «Фильтров отображения» располагается прямо над разделом отображения столбцов. Чтобы просмотреть только те пакеты, которые содержат в себе определенный протокол, нужно выбрать его на панели

инструментов Wireshark. Программа предлагает список фильтров на основе введенного текста.

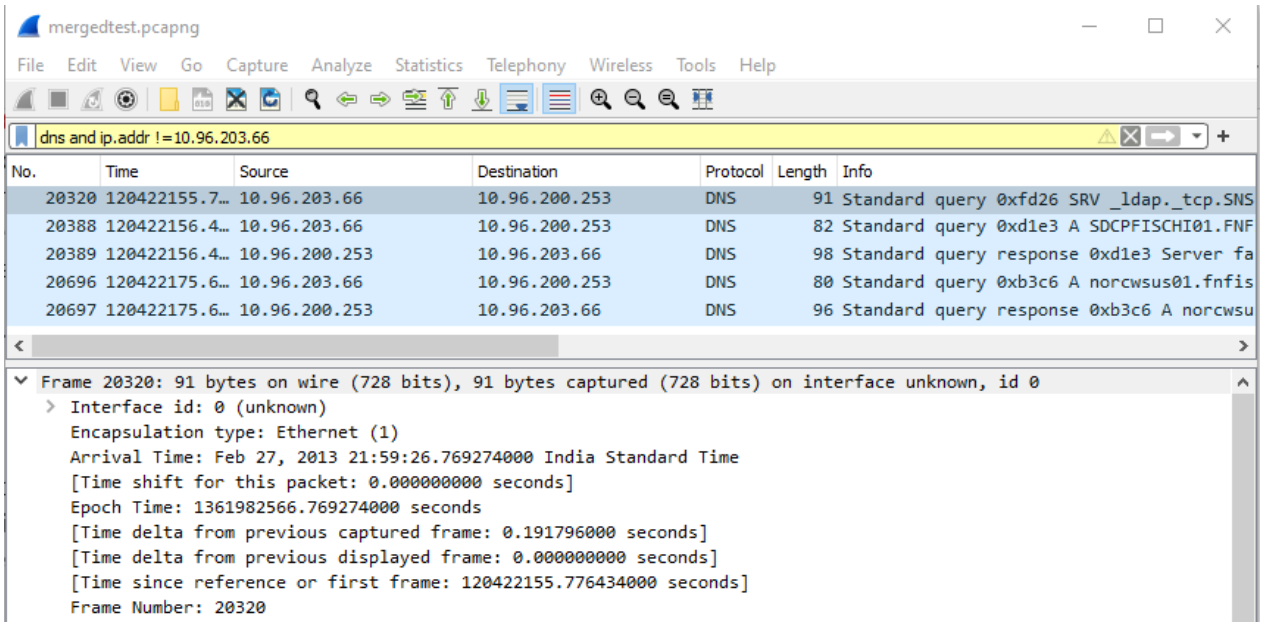
Например, чтобы отобразить только TCP-пакеты, следует ввести «**tcp**» на панели инструментов «Фильтров отображения» Wireshark.



Аналогично, чтобы просмотреть только те пакеты, которые содержат определенные запросы, нужно ввести их название на панели инструментов «Фильтров отображения» Wireshark. Например, чтобы просмотреть только HTTP-запросы, следует ввести «**http.request**».



Аналогичный пример фильтра отображения Wireshark, принимающего определенное выражение, представлен здесь. Стоит ввести DNS и ip.addr !=10.96.203.66.



Как можно заметить, захваченные пакеты имеют разные цвета. Итак, для чего они нужны?

- Серый – TCP-пакеты
- Черный с красными буквами – TCP-пакеты с ошибками
- Зеленый – HTTP-пакеты
- Светло-синий – пакеты UDP
- Бледно-голубой – пакеты ARP
- Лавандовый – пакеты ICMP
- Черный с зелеными буквами – ICMP-пакеты с ошибками

Примечание: – Цвета могут быть изменены в разделе «**View -> Colouring Rules**».

Создание выражений для фильтров отображения

Пользователь может создать фильтры отображения, которые будут сравнивать значения, используя другой тип оператора сравнения.
К примеру, для отображения пакетов только на IP-адресе 10.96.200.253 или с него следует использовать комбинацию символов, цифр и знаков «**ip.addr==10.96.200.253**». Фильтр отображения Wireshark применяет логические выражения, поэтому пользователь может указывать значения и связывать их вместе. Полный список доступных операторов сравнения приведен ниже.

Description	operator	Example
Equal or (eq)	==	Ip.src==192.168.0.134
Not equal or (ne)	!=	Ip.src!=192.168.0.134
Greater than or (gt)	>	frame.len > 20
Less than or (lt)	<	frame.len < 150
Greater than or equal to or (ge)	>=	frame.len >= 0x50
Less than or equal to or (le)	<=	frame.len <= 0x30
Bitwise_and	&	tcp.flags & 0x03
Logical AND or and	&&	Ip.src==192.168.0.134 and tcp.flags.fin
Logical or	||	Ip.src==192.168.0.134 or ip.src==192.168.1.1

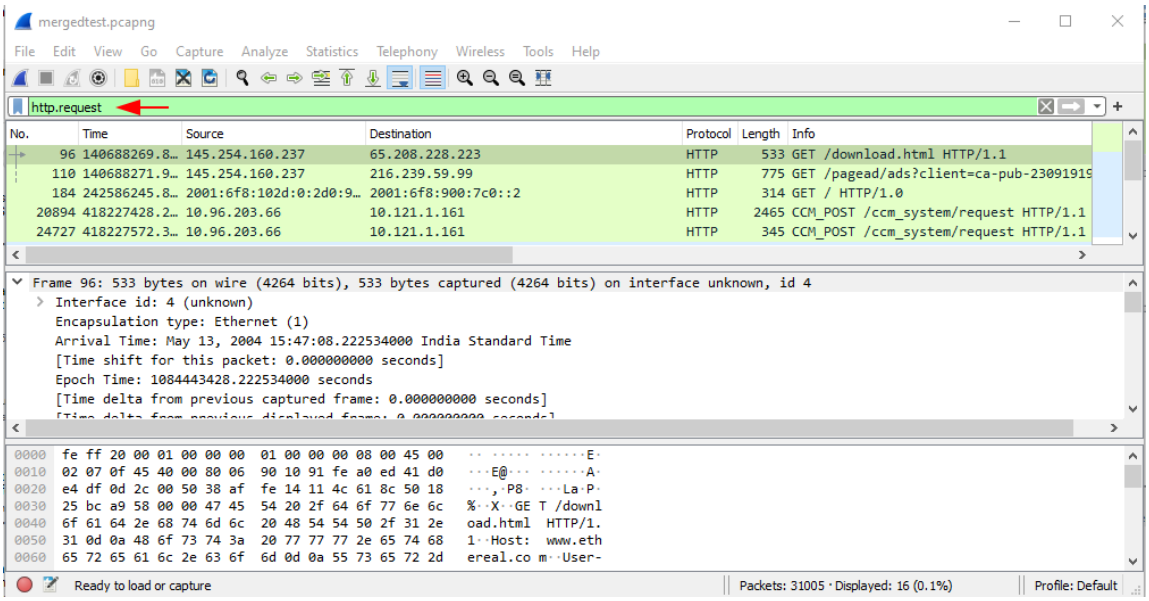
Полезные фильтры

Вот некоторые фильтры, которые можно использовать для быстрого просмотра веб-трафика.

Стоит понять с помощью каких методов, например, пользователь собирается **фильтровать инфекционный трафик**.

Следует применить следующий фильтр: «http.request». Будут показаны все запросы **HTTP Post**. Кроме того, пользователь сможет найти общее количество пакетов в нижней части экрана Wireshark, которое равно значению 16.

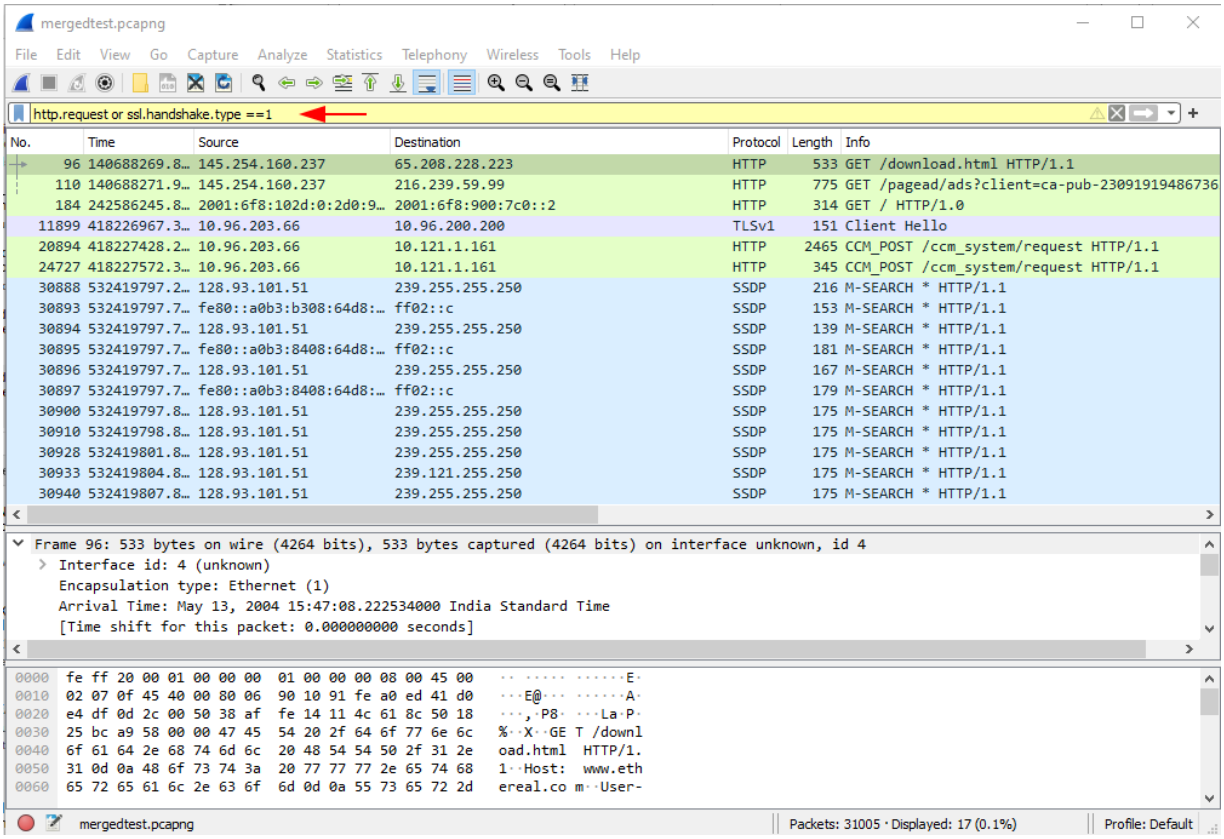
http.request



После этого, чтобы выявить все URL-адреса для HTTP-запросов, доменных имен, пользователь будет использовать следующее выражение.

http.request or ssl.handshake.type == 1

Значение «**http.request**» показывает пользователю все URL-адреса для HTTP-запросов. В «**ssl.handshake.тип == 1**» указываются доменные имена, применяемые в трафике HTTPS или SSL/TLS. Фильтрация с помощью этого фильтра отображения может помочь, если пользователь хочет комфортно просматривать веб-трафик.



Изменяя типы фильтров, пользователь может детализировать инфекционный трафик.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «фамилия слушателя» Иванов»). При подготовке файла-отчета по заданию необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

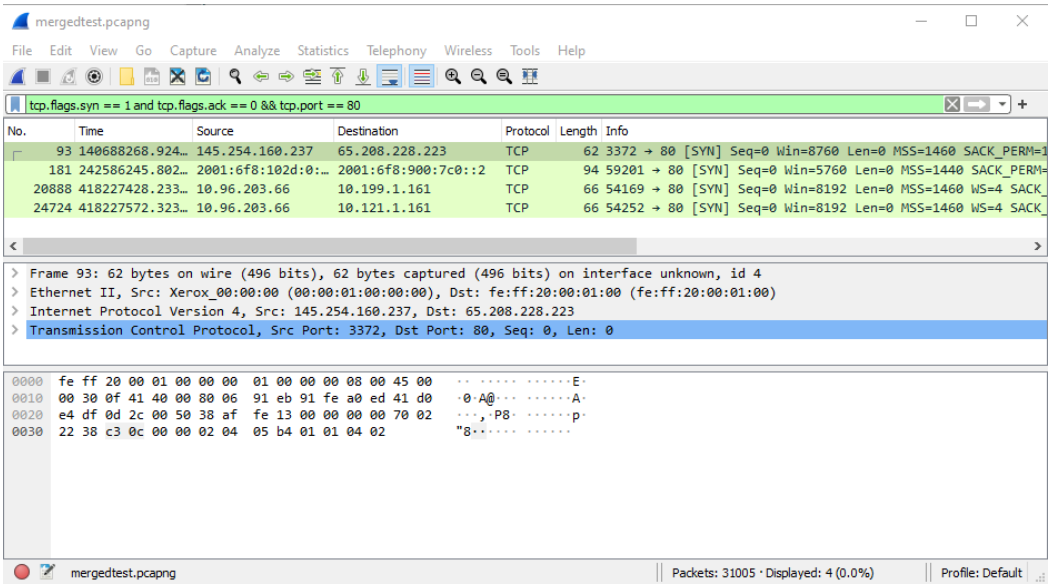
1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях.
2. Скопируйте с официального сайта программу «Wireshark», установите ее в свою рабочую папку.
3. Запустите программу «Wireshark», исследуйте пользовательский интерфейс.

Практические задания:

1. Узнайте общее количество пакетов TCP syn для порта 80.

Ответ: – Чтобы найти все пакеты TCP syn, пользователь может использовать следующее выражение для быстрого просмотра веб-трафика для порта 80. Кроме того, он способен найти общее количество пакетов в нижней части экрана Wireshark, которое равно значению 4.

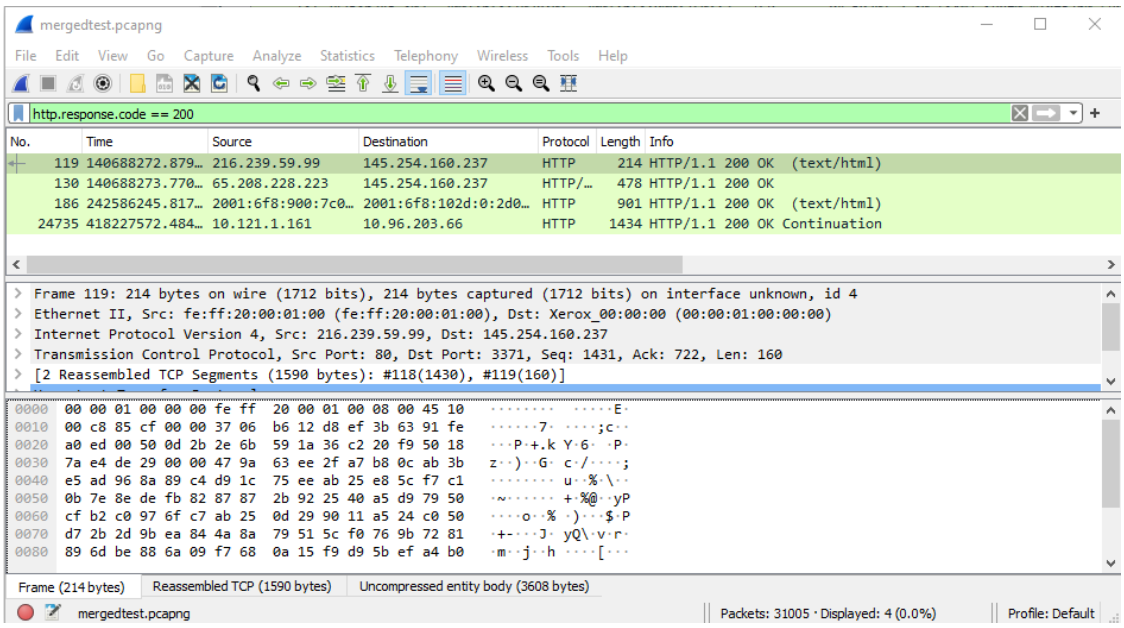
tcp.flags.syn == 1 and tcp.flags.ack == 0 && tcp.port == 80



2. Отфильтруйте весь пакет с кодом ответа http 200.

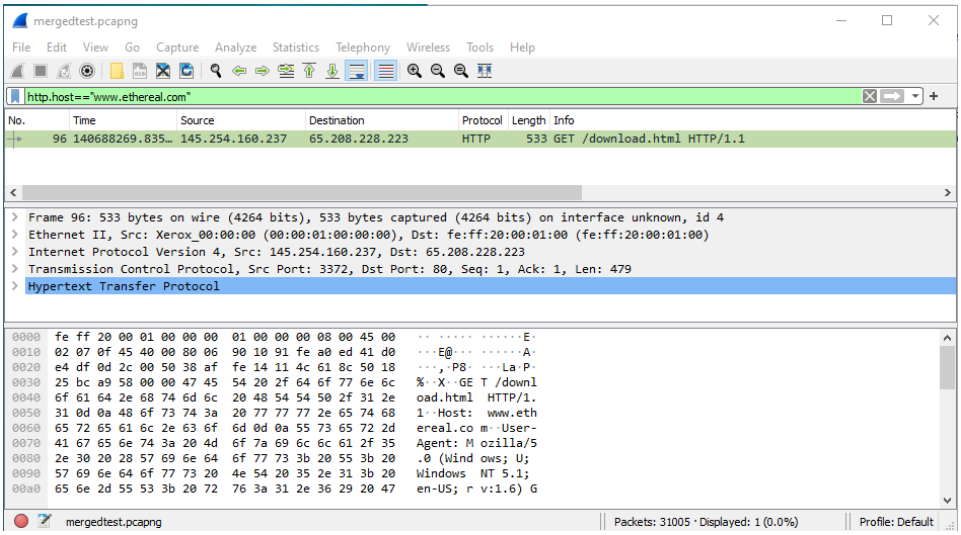
Ответ: – Значение «http.response» показывает пользователю все URL-адреса для ответов HTTP, а код состояния HTTP 200 означает успех проведенной работы. Клиент запросил документы с сервера. Сервер ответил клиенту и отправил ему документы.

http.response.code == 200



3. Злоумышленник пытается загрузить вредоносный файл с сайта www.ethereal.com. Нужен фильтр для идентификации хоста http.

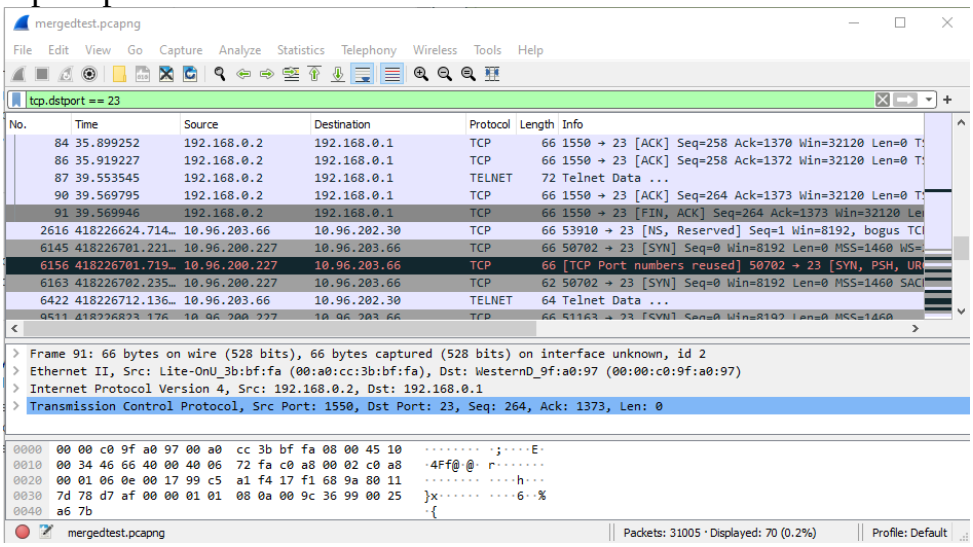
Ответ: – В этом случае следует выяснить данные хоста, который посетил вредоносный сайт. Как известно, у каждого веб-сайта есть собственный URL-адрес. Таким образом, можно узнать хост, используя следующее выражение.
http.host=="www.ethereal.com”
Or http.host=="URL”



4. Отфильтруйте, чтобы определить порт назначения 23.

Ответ: –для фильтрации порта назначения 23 можно использовать следующее выражение.

tcp.dstport == 23



Закрепите полученные знания и продемонстрируйте работу в виде файл-отчета преподавателю в виде сохраненных в формате .doc скриншотов.