Лабораторная работа № 6

«Анализ сетевого» трафика

Подготовка к лабораторной работе

1. Повторить сетевую модель OSI. Изучить устройство протоколов IP, TCP и UDP, для чего рекомендуются следующие энциклопедические статьи:
   1) https://en.wikipedia.org/wiki/IPv4
   2) https://en.wikipedia.org/wiki/Transmission_Control_Protocol
   3) https://en.wikipedia.org/wiki/User_Datagram_Protocol

   Основное внимание следует уделить структуре пакетов, то есть составу их полей.
2. Ознакомиться с проектом-заготовкой, который осуществляет перехват сетевого трафика и разбор пакетов на канальном уровне.

Задание на лабораторную работу

1. Написать функцию, которая будет производить разбор пакета IP версии 4 (IPv4): разбор заголовка пакета и извлечение данных пакета (IP payload). Необходимо вывести на экран информацию о пакете IP:
   - заголовок пакета в шестнадцатеричном виде;
   - размер заголовка и размер всего пакета, указанный в заголовке;
   - IP-адреса отправителя и получателя;
   - код версии IP пакета;
   - значение TTL (времени жизни пакета);
   - код протокола транспортного уровня, пакет которого находится в пакете IP.

   Если в сегменте пользовательских данных пакета IP находится пакет TCP или UDP, необходимо вызвать соответствующую функцию для разбора пакета транспортного уровня.
2. Написать функцию, которая будет производить разбор пакета TCP: разбор заголовка и извлечение данных. Необходимо вывести на экран информацию о пакете TCP:
   - заголовок TCP в шестнадцатеричном виде;
   - порты отправителя и получателя;
   - размер заголовка и размер данных в пользовательском сегменте (TCP payload);
   - значения поля порядкового номера (sequence number, `seq`) и номера подтверждения (acknowledgement number, `ack`).

Если пакет содержит пользовательские данные, то необходимо вывести их в шестнадцатеричном виде.

3. Написать функцию, которая будет производить разбор пакета UDP: разбор заголовка и извлечение данных. Необходимо вывести на экран информацию о пакете UDP:
   — заголовок UDP в шестнадцатеричном виде;
   — порты отправителя и получателя;
   — полный размер пакета, указанный в заголовке;
   — размер данных в пользовательском сегменте (UDP payload).

   Если пакет содержит пользовательские данные, необходимо вывести их в шестнадцатеричном виде.
4. Проверять работоспособность готовой части по выполнении каждого из пунктов 1—3, воспользовавшись программами из предыдущих ЛР для генерации пакетов. Проверять правильность разбора следует, сличая вывод программы и Wireshark.

Указания к выполнению лабораторной работы

Предлагается выполнять ЛР на основе проекта-заготовки: требуется реализовать функции `parseIPPacket()`, `parseTCPPacket()` и `parseUDPPacket()` в файле `solution.cpp`.

Проект-заготовка реализован с использованием в ОС Windows библиотеки WinPCap. Необходимые для сборки файлы приложены к проекту. **Запуск требует установленной библиотеки WinPCap;** часто она устанавливается вместе с Wireshark. В ОС семейства *nix используется библиотека libpcap.

Захват пакетов выполняется при помощи класса `NetCapture`, таким образом, знание библиотеки WinPCap или libpcap не требуется. Конструктор `NetCapture` имеет два параметра: имя источника данных (сетевого интерфейса или файла) и фильтр пакетов. Выбор сетевого интерфейса в проекте-заготовке реализован; при необходимости можно заменить его на выбор файла с записью трафика. Фильтр пакетов задается несколько иначе, чем в Wireshark, см. примеры в коде проекта-заготовки или документацию.

Для печати данных в шестнадцатеричном виде можно воспользоваться функцией `printHexDump()`, находящейся в фале `printHexDump.h`. Функция имеет следующие параметры:

1) `std::ostream& os` — поток вывода, например, `std::cout`;
2) `const void* data` — указатель на данные;
3) `size_t datalen` — размер данных.

Контрольные вопросы

1. Зачем используется расчет контрольной суммы для передаваемых по сети данных? На каком уровне (или уровнях) модели OSI это применяется и почему?
2. Big-endian и little-endian порядок байт. Какова область их применения?
3. Что такое псевдозаголовок пакета UDP? Почему контрольная сумма вычисляется не для заголовка пакета, а именно для псевдозаголовка?
4. Схема работы протокола TCP: состояния сеанса TCP.
5. Объяснить схему «рукопожатия» (handshake) для протокола TCP. Какие проблемы могут возникнуть при работе данной схемы?
6. Какие протоколы действуют на транспортном уровне? Какую адресацию они вводят? Как по заголовку пакета IP определить используемый протокол транспортного уровня?
7. На каком уровне модели OSI используются MAC-адреса? Каков размер MAC-адреса в байтах и как записывается MAC-адрес? Какие виды MAC-адресов существуют?