УДК 004.2

Кубалиев Ж.М., Ружников В.А.

ПЕРЕХВАТ ПАКЕТОВ ПРОТОКОЛА X11 С ИСПОЛЬЗОВАНИЕМ WIRESHARK

Поволжский государственный университет телекоммуникаций и информатики, г.Самара, ул.Льва Толстого, д.23, 443010

Zholaman M. Kubaliyev, Vadim A. Ruzhnikov

THE X11 PACKETS SNIFFING USING WIRESHARK

Povolzhskiy State University of Telecommunications and Informatics, Samara, Leo-Tolstoy Street, 23, 443010

Статья представляет краткий обзор пакетного анализатора Wireshark касающийся перехвата и анализа протокола X11.

Ключевые слова: протокол X11, система X Windows, NoMachine NX

This article gives short explain about sniffing X11 packets by Wireshark.

Keywords: X11, X Windows system, NoMachine NX

Введение

Wireshark анализатор сетевого трафика ранее известный как Ethereal. Данная программа позволяет анализировать сетевой трафик в режиме реального времени с целью изучения архитектуры протокола или поиска различных сетевых проблем. Wireshark позволяет исследовать технические детали сетевых протоколов, имеет удобный графический интерфейс с подсветкой, различные фильтры и другие инструменты, позволяя эффективно исследовать каждый проходящий пакет.

Wireshark распространяется по лицензии GPL[1], что дает возможность использовать его безвозмездно в том числе и в коммерческих целях.

Технические особенности Wireshark

[1] https://ru.wikipedia.org/wiki/GNU_General_Public_License

Wireshark является мощным инструментом, и являеется де факто стандартом в области анализа, отладки сетевых протоколов. В следующем списке перечислены основные достоинства данного инструмента:

- позволяет перехватывать сетевые пакеты в режиме реального времени;
- отображает детальную информацию по каждому перехваченному пакету;
- содержит большое количество фильтров, позволяющих отображать только самую необходимую информацию;
- имеет возможность поиска по различным критериям;
- умеет формировать различную статистику;
- для удобства, маркирует протоколы, различными цветами;
- поддерживает импорт и экспорт в различные форматы, в том числе в/из tcpdump, windump.

Взаимодействие X-клиента с X-сервером в операционной среде Linux

Для взаимодействия с X сервером, во всех современных операционных системах семейства Unix, X клиенты используют доменные Unix сокеты (далее сокет). Доменный сокет в операционных системах Unix представляет из себя файл, который используется для организации канала связи между двумя программами по типу конвейера. Адресом сокета, является путь к файлу, а в некоторых случаях его дескриптор. Для подключения к X серверу в ОС Linux, X клиенту необходимо подключиться к серверному сокету, имеющему следующий адрес (путь): /tmp/.X11-unix/X0, где X0 идентифицирует номером дисплея (экрана). Если операционная система настроена на работу с одним дисплеем, то по умолчанию он будет иметь нулевой номер - X0.

Для перехвата трафика, протекающего через сокетные соединения, необходимо использовать схему «подключение в разрыв канала» см.рис.1.

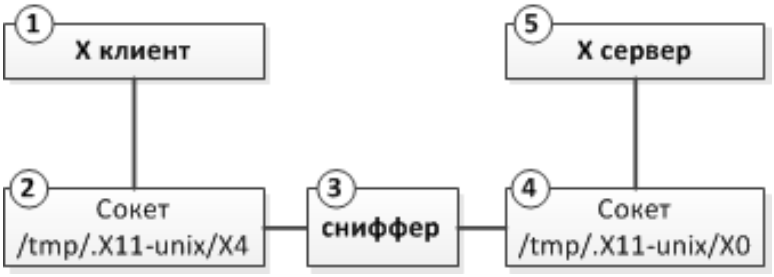

Рис.1 Сокетное взаимодействие X-клиента с X-сервером

Известны два основных способа для перехвата трафика, проходящего через доменные сокеты:

1. С использованием утилиты socat.
2. С использованием утилиты strace.

Рассмотрим более подробно выше перечисленные способы перехвата трафика, идущего через сокетный канал.

1. Схема использования утилиты socat приведена на рис.1, где, 1 – X - клиент соединяется с сокетом посредника; 2 – доменный сокет, открытый socat для перехвата данных от клиента, с дальнейшей передачей их серверу; 3 – socat; 4 – сокет X-сервера; 5 – X- сервер.

При такой схеме, socat является посредником между X-клиентом и сервером. При этом все перехваченные данные могут выводиться в текстовом формате или в шестнадцатеричном виде в файл или на экран

Пример команды socat с параметрами:

socat -x unix-listen:/tmp/.X11-unix/X4,fork unix:/tmp/.X11-unix/X0

Для подключения X клиента к сокету X4, необходимо выполнить следующую команду.

DISPLAY=:4 xclock (X клиент)

2. Утилита strace предназначена для трассировки системных вызовов, следовательно, кроме искомых данных в лог буду записывать и другие не относящиеся к сокету данные. Поэтому для получения требующихся данных, необходима дополнительная фильтрация.

Перехват X11 средствами Wireshark

Для организации перехвата пакетов протокола X11 посредством Wireshark, необходимо запустить X сервер в режиме прослушивания TCP/IP портов. По умолчанию X сервер настроен на прослушивание сокета по адресу: /tmp/.X11-unix/X0.

Для запуска X сервер в режиме прослушивания IP порта, следует явно разрешить использование протокола IP. Для этого, например, в ОС GNU/Linux Ubuntu v14, которая по умолчанию использует оконный менеджер LightDM[2], необходимо в конфигурационном файле /etc/lightdm/lightdm.conf, задать следующий параметр:

[SeatDefaults]

xserver-allow-tcp=true

Дополнительно, в конфигурационном файле X сервера /etc/X11/xinit/xserverrc, надо заменить команду: exec /usr/bin/X -nolisten tcp "$@", следующей командой: exec /usr/bin/X.

После задания выше приведённых параметров, X сервер, помимо прослушивания сокета, так же будет прослушивать IP порт – 6000.

Запуск X клиента.

Перед подключением X клиента к удалённому или локальному X серверу по протоколу IP, необходимо явно задать разрешения на целевой машине, используя следующую команду: xhost +(локальный или удалённый адрес). Затем следует запустить любой X клиент со следующим параметром: -display. Например, для запуска программы xclock для подключения к локальному X серверу по протоколу IP, надо вызвать её со следующими параметрами:

xclock -display localhost:0

Запуск Wireshark.

В среде Unix подобных операционных систем, Wireshark необходимо запускать с правами супер пользователя – root, с целью предоставления

[2] https://ru.wikipedia.org/wiki/LightDM

программе полного доступа к сетевым интерфейсам операционной системы.

Для перехвата пакетов проходящий по протоколу X11 между локальными X сервером и клиентом, необходимо переда запуском в Wireshark процедуры перехвата выбрать опцию Loopback показанную на рис.2.

Запустив Wireshark с предварительно выбранной опцией (рис.2), программа начнёт собирать данные, на рис.3 приведён образец рабочего окна Wireshark в процессе перехвата X11, перечислим основные области рабочего окна (которые отмечены цифровыми идентификаторами): 1) Область фильтрации. Данный элемент отвечает за фильтрацию данных; 2) Данные по каждому перехваченному пакету; 3) Детализация пакета; 4) Область экрана с исходными данными в шестнадцатеричном формате.

Для удобства обработки перехваченных данных, в Wireshark присутствует возможность экспорта захваченных данных в различные файловые форматы, позволяя таким образом обработать полученные данные с использованием различных инструментов анализа, в том числе для формирования различных графиков.

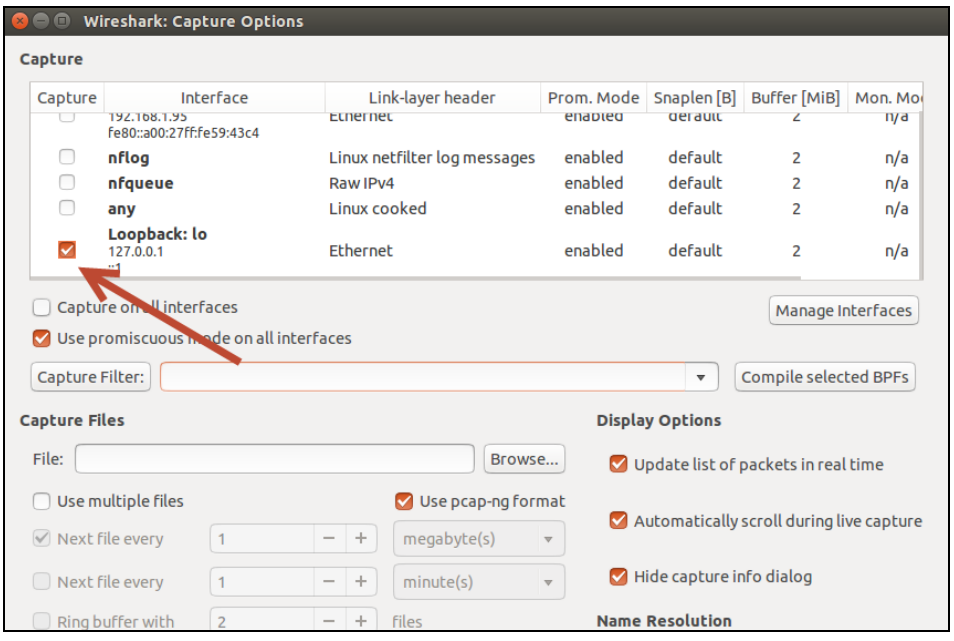

Рис.2 Опция настроек перехвата в Wireshark.

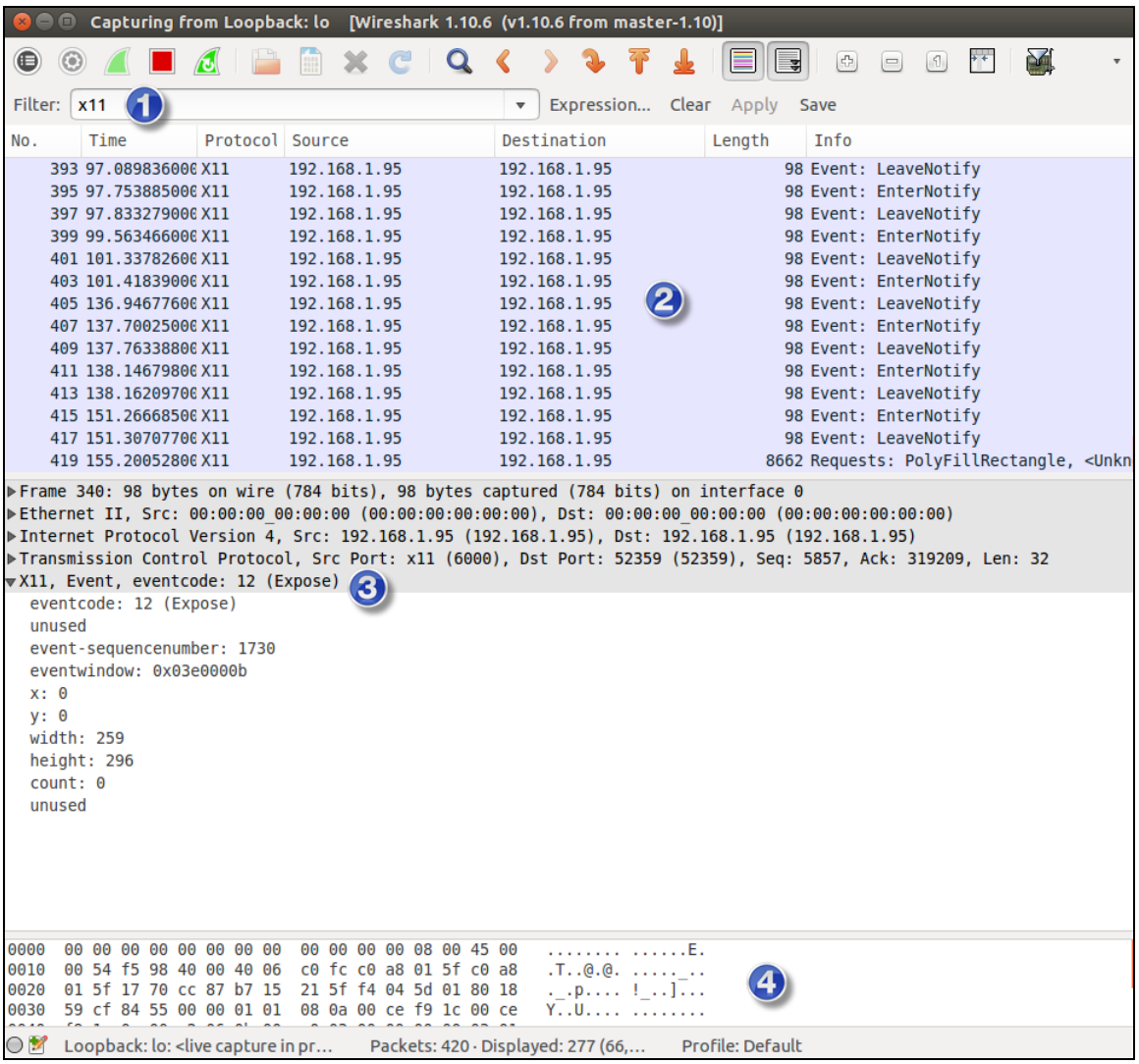

Рис.3 Рабочая область экрана Wireshark.

Заключение

Перехват пакетов протокола X11 имеет несколько практических значений, наиболее значимым из которых является, отслеживание размера переданных по протоколу X11 пакетов. Объём переданных по протоколу X11 данных, позволяет оценить алгоритмы сжатия, в случае использования прокси сервера.

Использование Wireshark, позволяет существенно сэкономить время в процессе исследования протокола X11, так как разработка собственных программ, хотя и возможно, но требует много времени.

В статье представлен обзор использования двух основных программ, с помощью которых имеется возможность перехватывать практически, весь трафик, проходящий между X сервером и клиентом. При этом наиболее

удобным и мощным, является специализированный инструмент по исследованию сетевых протоколов -Wireshark.

Литература

1. A Brief intro to X11 Programming [Электронный ресурс]. - Режим доступа: http://math.msu.su/~vvb/2course/Borisenko/CppProjects/GWindow/xintro.html

2. Gettys J., Karlton P., Mcgregor S. The X Window System, Version 11. Software Practice and Experience. vol. 20(S2), S2/35-S2/67, 1991

3. Wireshark User’s Guide [Электронный ресурс]. - Режим доступа: https://www.wireshark.org/docs/wsug_html_chunked/index.html

4. XFree86. [Электронный ресурс]. - Режим доступа: https://en.wikipedia.org/wiki/XFree86

5. XWin Server. [Электронный ресурс]. - Режим доступа: http://x.cygwin.com/devel/server/

6. X Window System Protocol, X Version 11, Release 7.7 [Электронный ресурс]. - Режим доступа: http://www.x.org/releases/X11R7.7/doc/xproto/x11protocol.html