# Выход жертвы в Интернет

А теперь попробуем посмотреть на хосте злоумышленника как жертва работает в интернете. А именно перехватим работу между первым компьютером и интернетом. Для этого будем скачивать нешифрованный сайт из интернета и наблюдать за этой процедурой.

Для начала проверим адреса на Kali-linux и на шлюзе по умолчанию

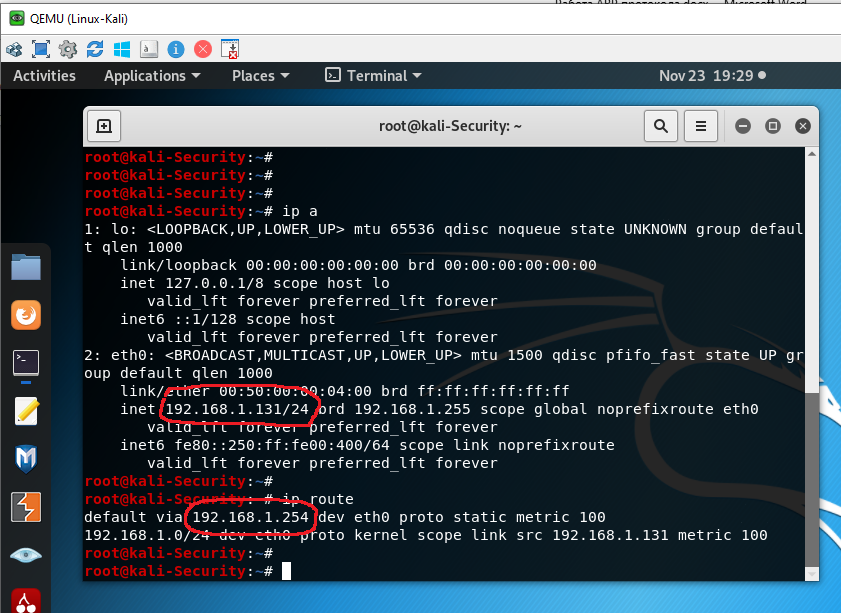


Рис. 38.

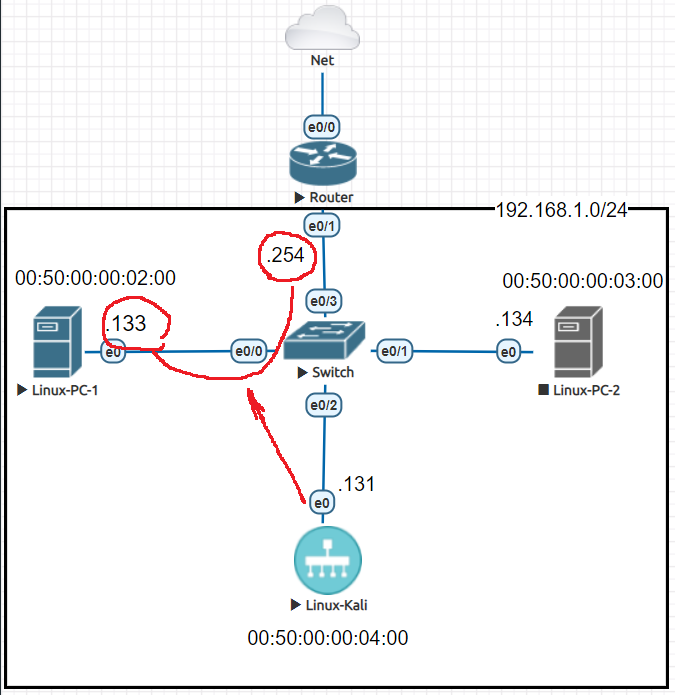


Рис. 39.

Установим на Kali-linux перехват трафика между машинами 192.168.1.133 (жертва) и 192.168.1.254 (выход в итернет).

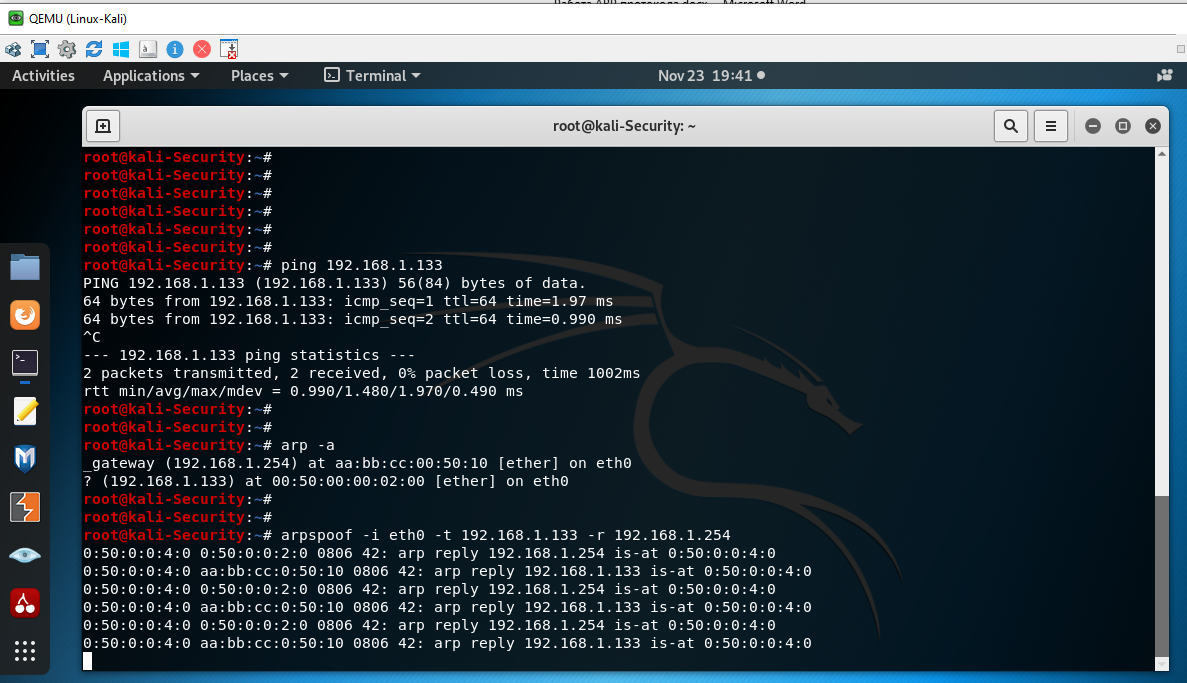


Рис. 40.

Атака началась и будем смотреть на то, что делает жертва. Предположим, что с машины жертвы пингуются адреса в интернете

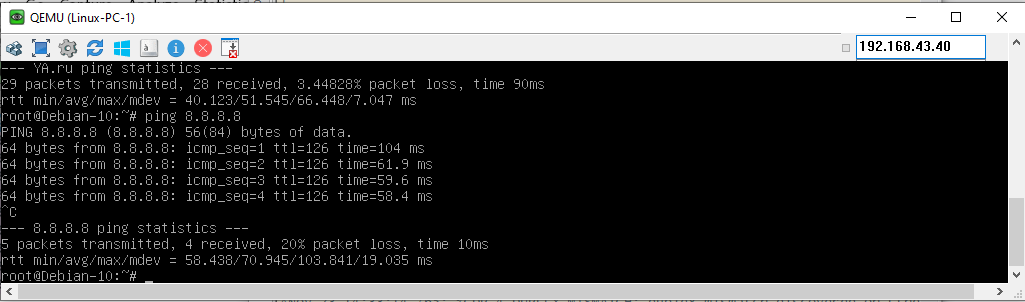


Рис. 41.

Тогда на перехвате мы видим следующее

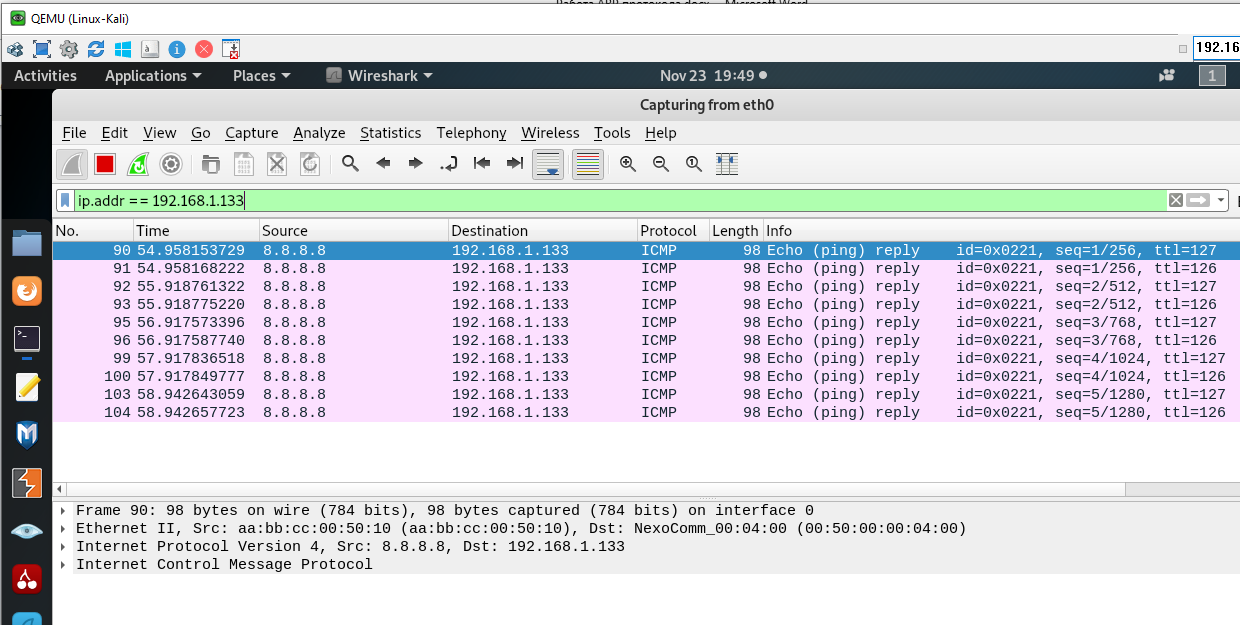


Рис. 42.

Видим, что данные перехвачены и их можно анализировать. Теперь с компьютера жертвы скачаем нешифрованный сайт. Для того, чтобы скачивать сайты из интернета установим утилиту curl. Но прежде проверим установленные в системе пакеты.

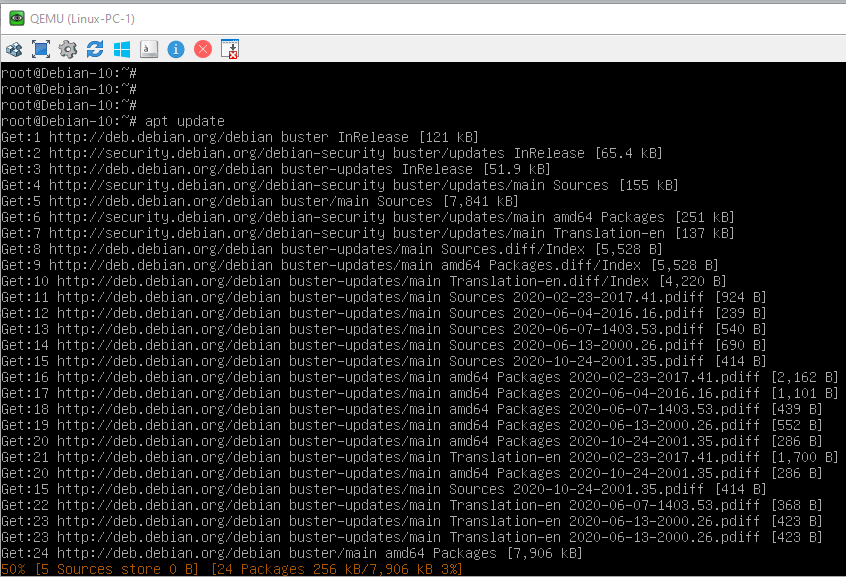


Рис. 43.

Во время обновления на Kali-linux мы так же перехватываем трафик.

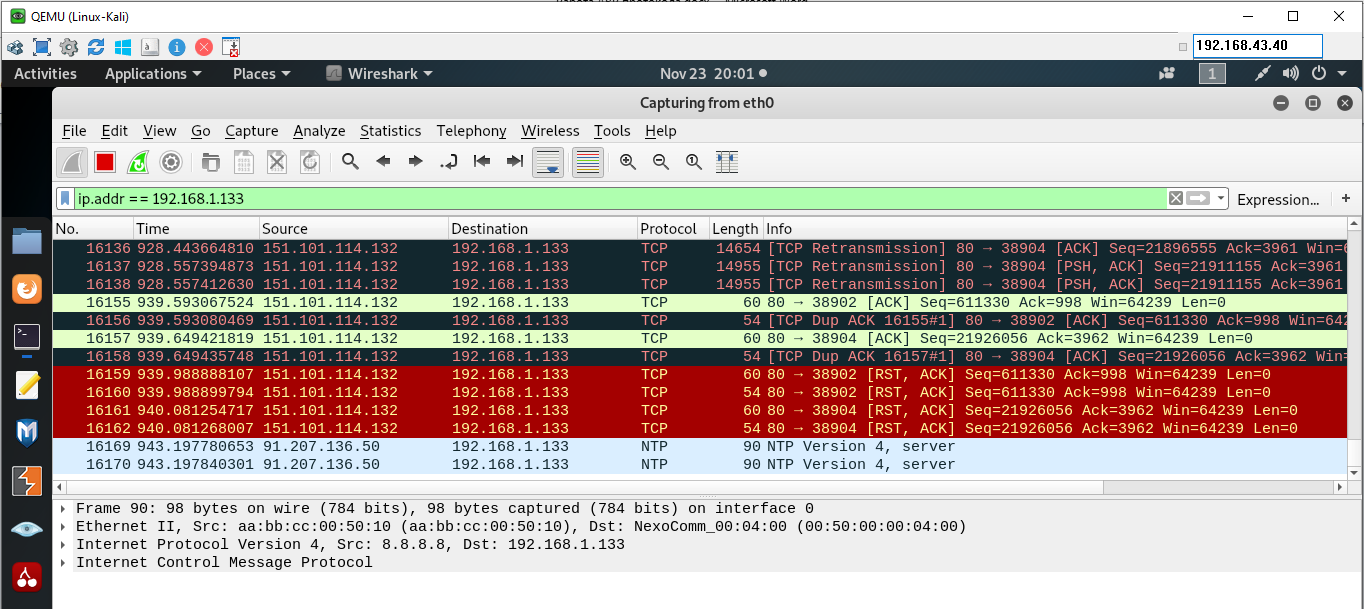


Рис. 44.

А теперь устанавливаем curl.

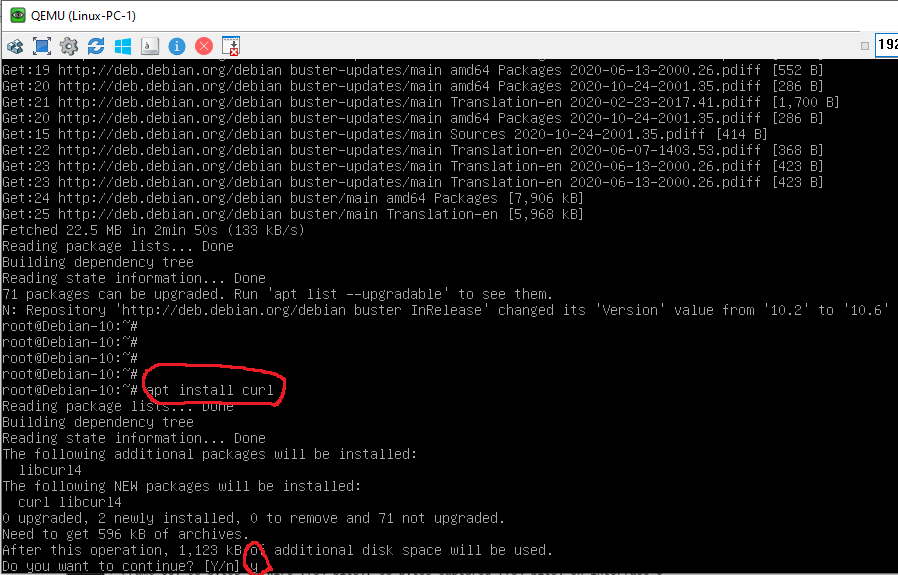


Рис. 45.

И, наконец, можно скачать сайт

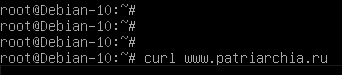


Рис. 46.

Останавливаем перехват трафика

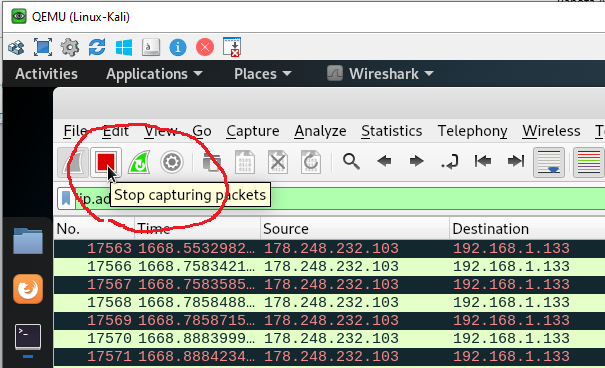


Рис. 47.

Для просмотра того, что получили в результате перехвата, используем wireshark

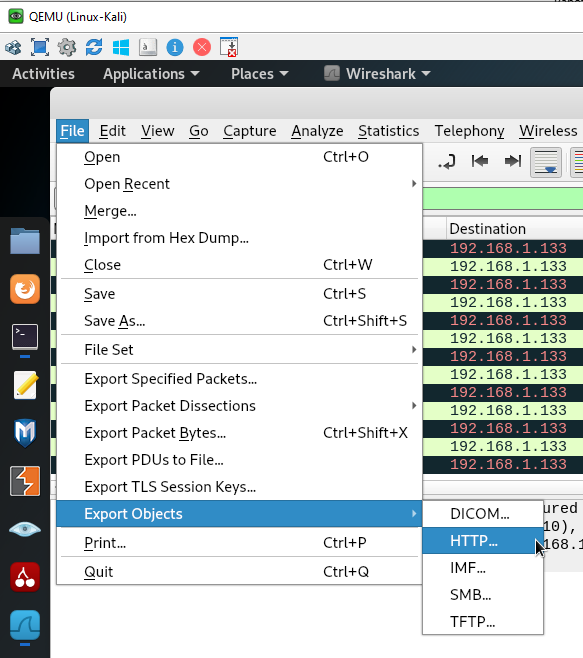


Рис. 48.

В результате мы видим, что получили много объектов

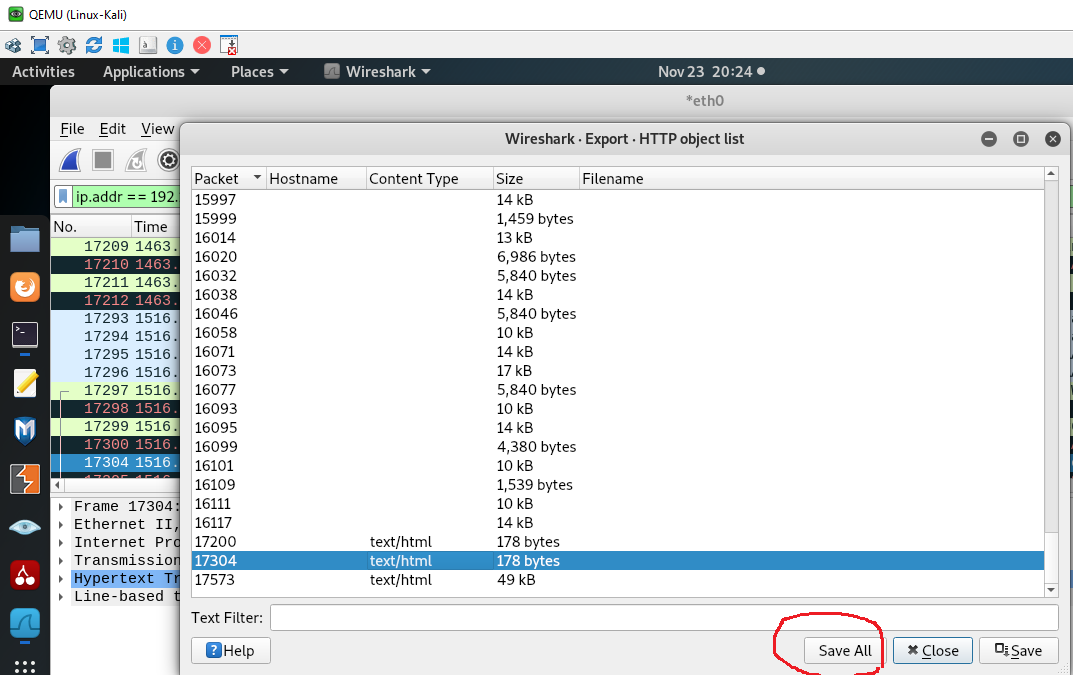


Рис. 49.

Сохраним их в папочку на рабочем столе.

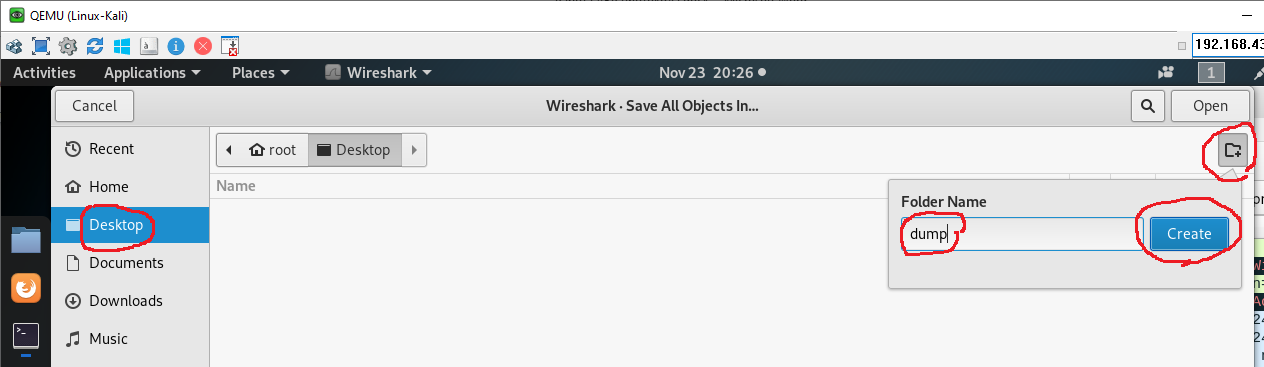


Рис. 50.

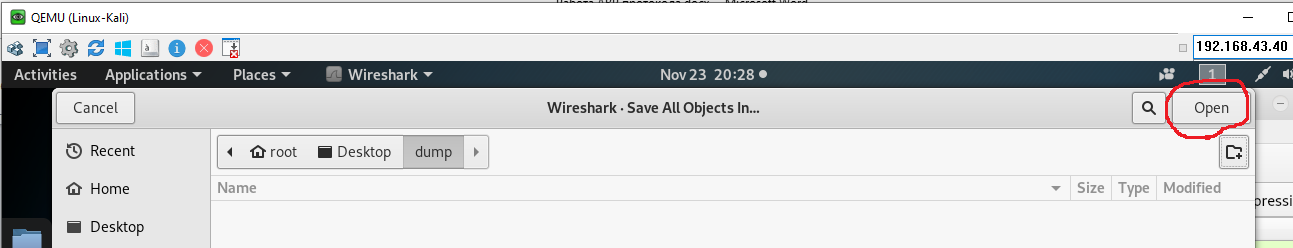


Рис. 51.

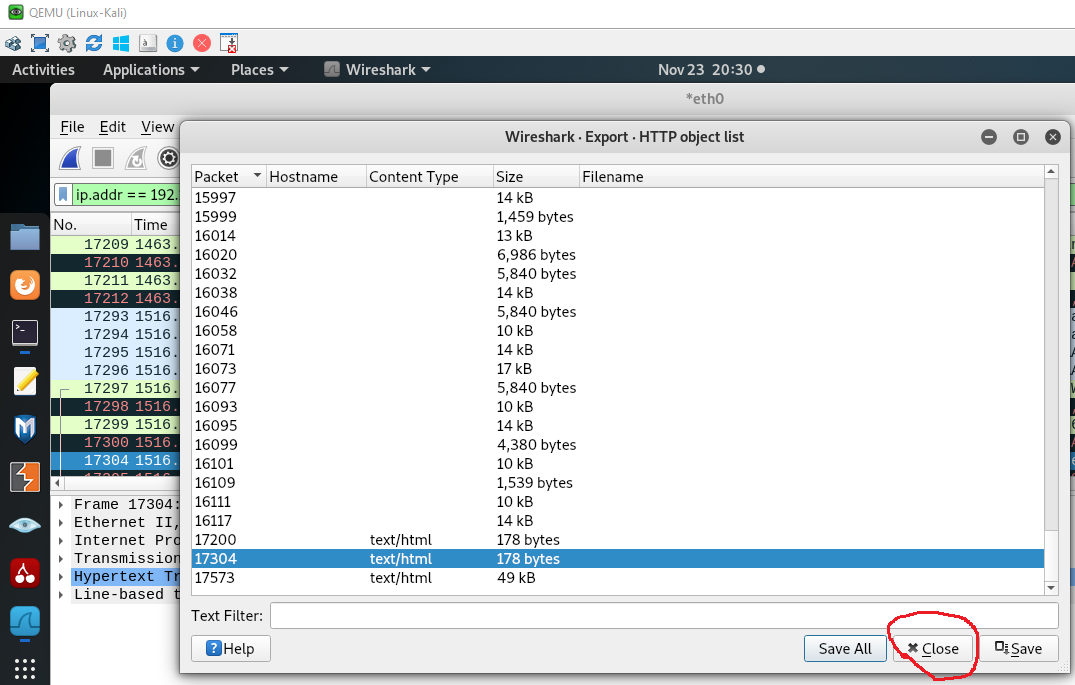


Рис. 52.

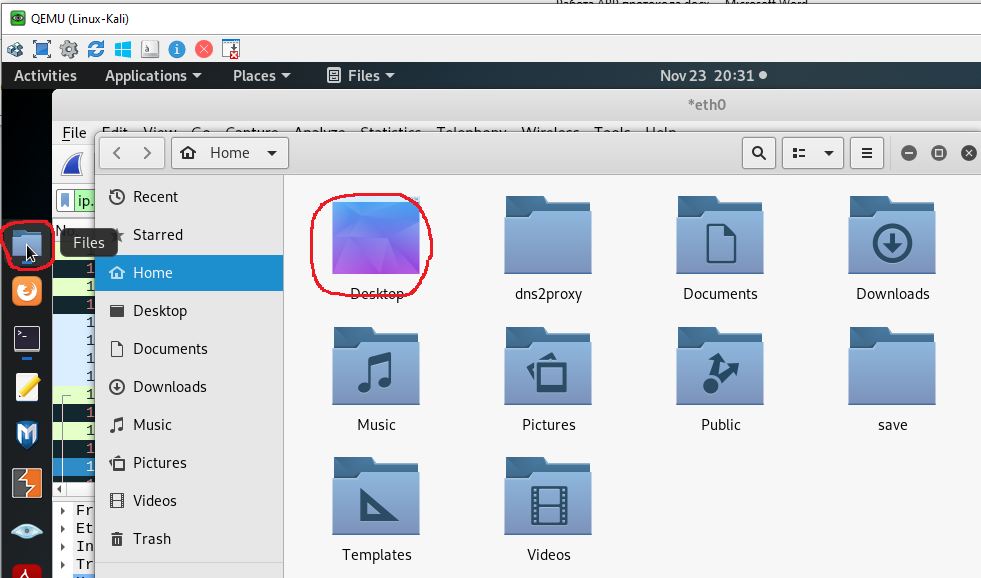


Рис. 53.

Мы видим много скачанных файлов/

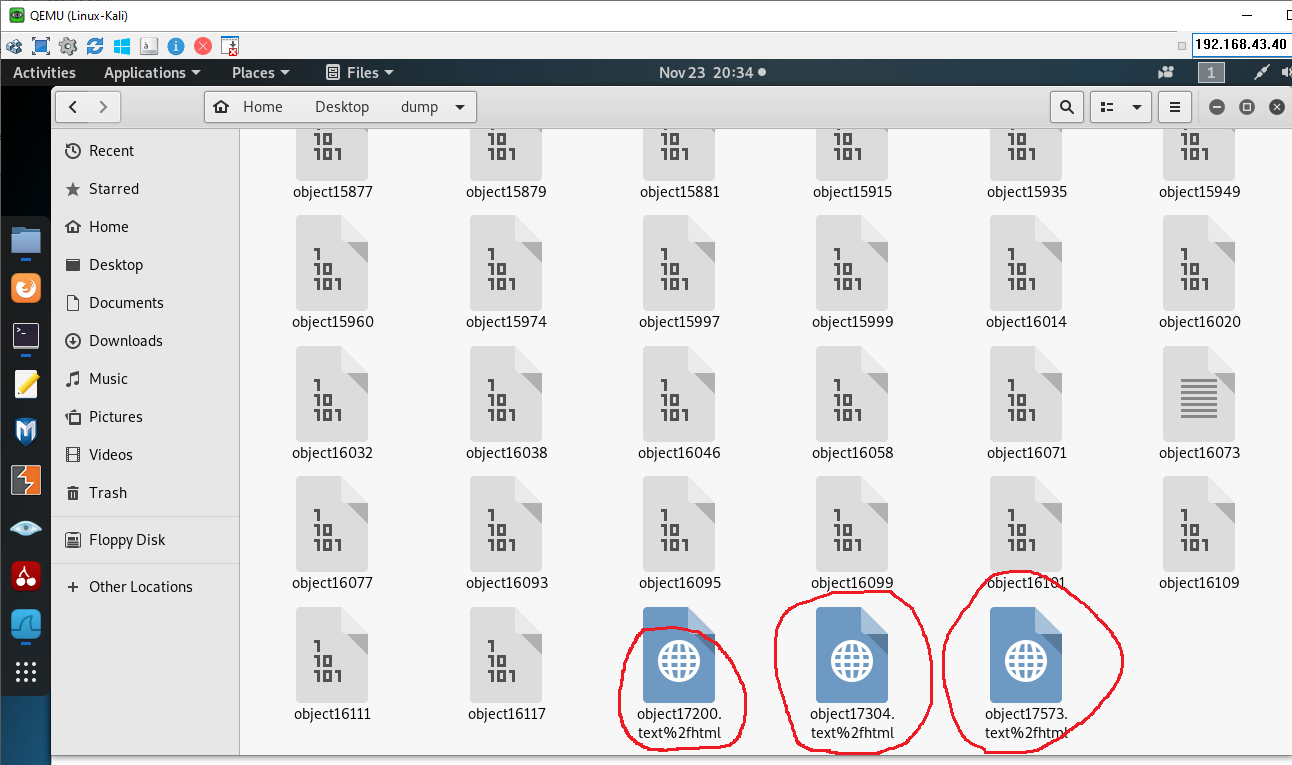


Рис. 54.

И среди них файлы html

# Скачивание из Интернета всего сайта целиком

Из основной машины подключимся к Linux-PC-1 по протоколу ssh. Для этого необходимо пробросить порт на маршрутизаторе Cisco

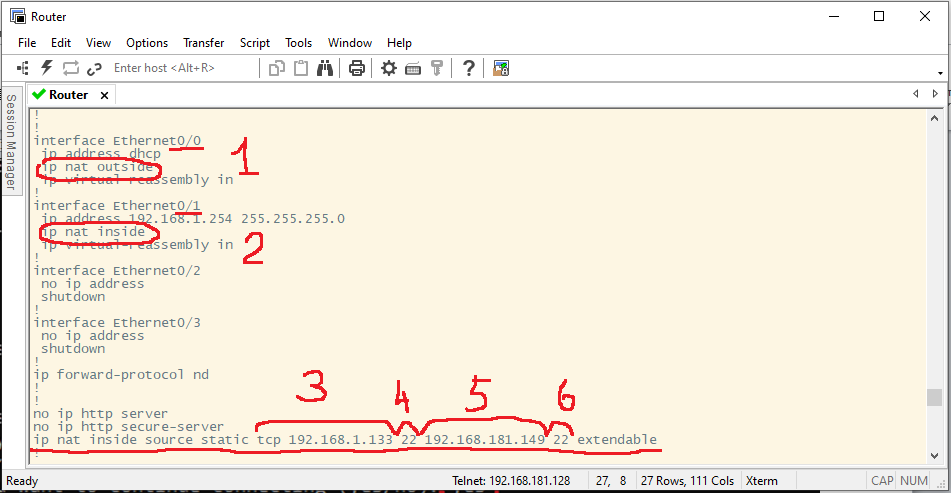
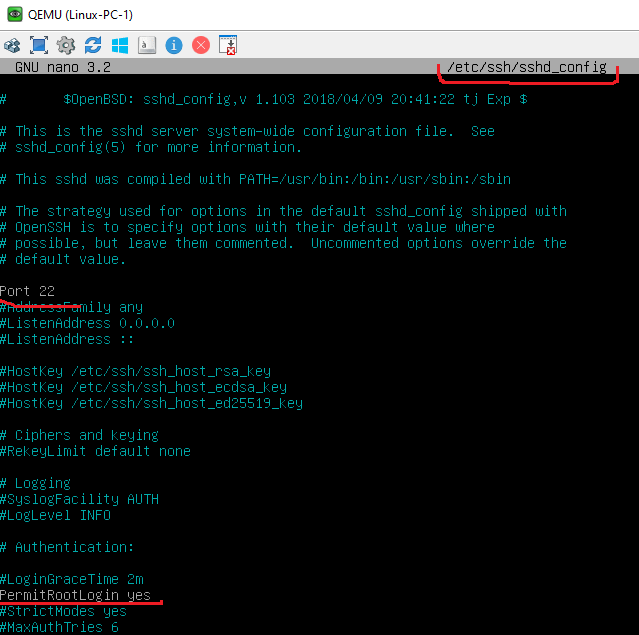


Рис. 55.

Здесь нужно указать, что интерфейс е0/0 внешний (1), а интерфейс е0/1 – внутренний (2) и ввести команду, которая разрешает проброс портов, где указывается адрес куда нужно пробросить порт (3), номер пробрасываемого порта (4), адрес откуда пробросить порт (5) и номер порта (этот номер можно изменить).

Предварительно нужно разрешить доступ по ssh от имени root.



И стартовать сервис командой: service sshd restart. После выполненных команд можно открыть сессию по ssh.

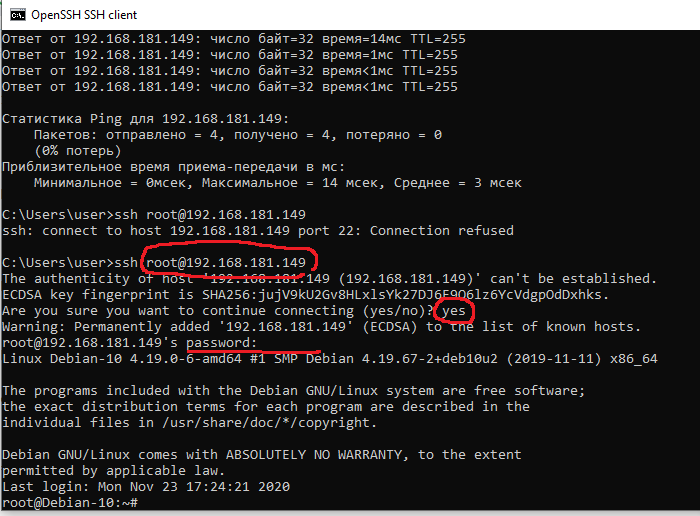


Рис. 56.

При создании сессии указываются имя пользователя и адрес машины, через которую создается сессия, а затем пароль.

А теперь на машите злоумышленника запускаем wireshark.

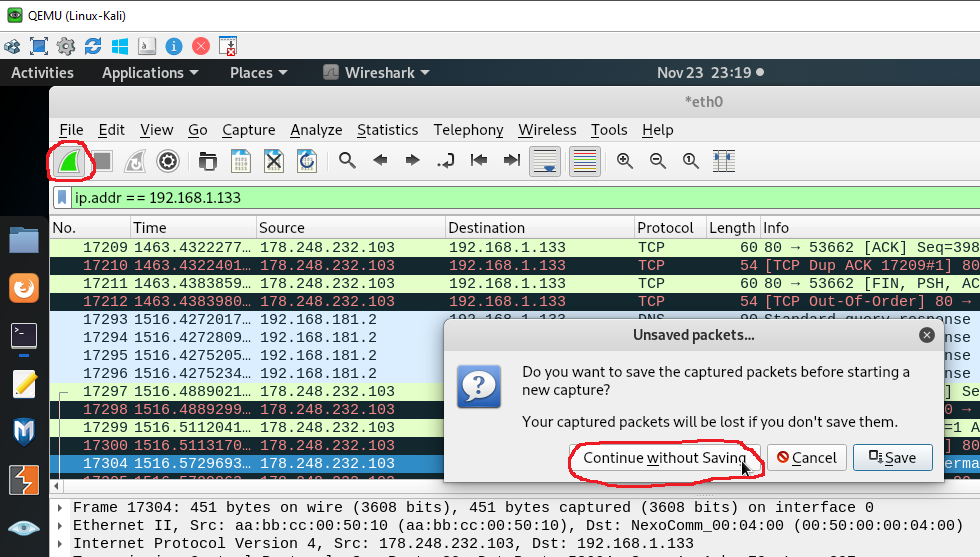


Рис. 57.

И на машине жертвы скачиваем некоторый сайт полностью.

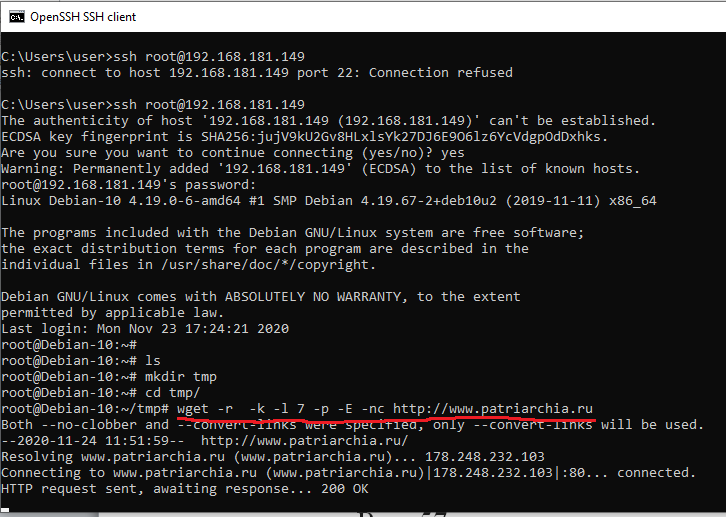


Рис. 58.

Во время скачивания на машине злоумышленника мы видим перехват скачиваемых данных

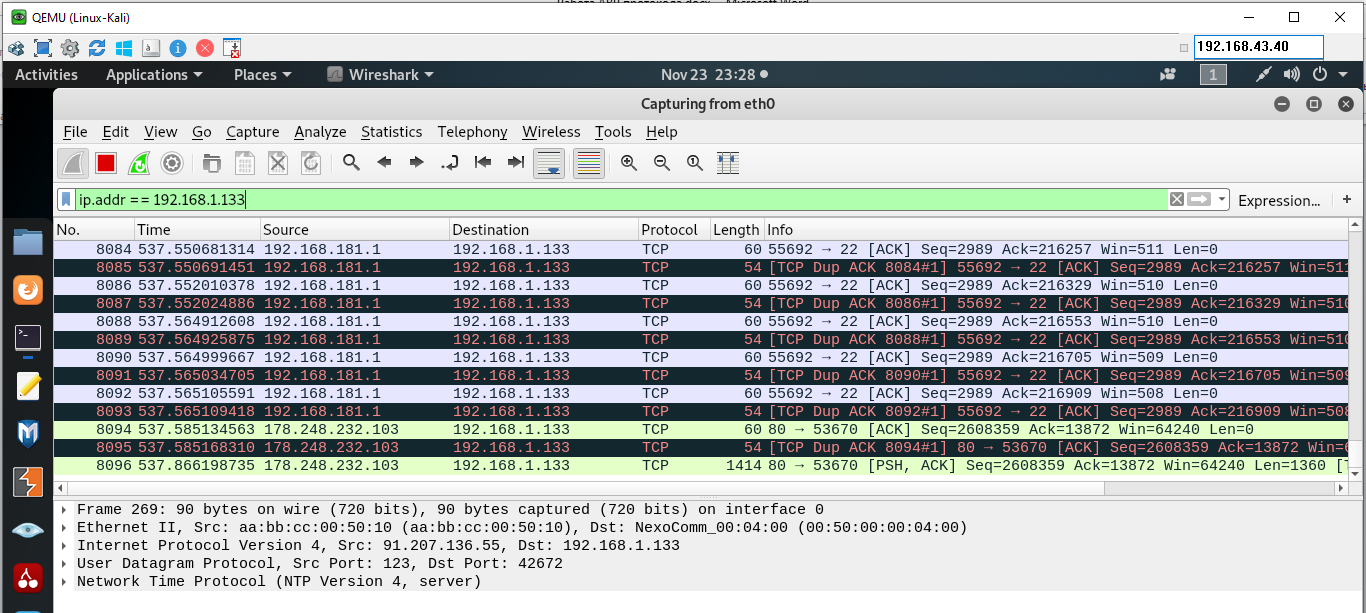


Рис. 59.

После завершения скачивания сайта на машине злоумышленника сделаем экспорт объектов (см. рис. 48 - 49) в новую папку.

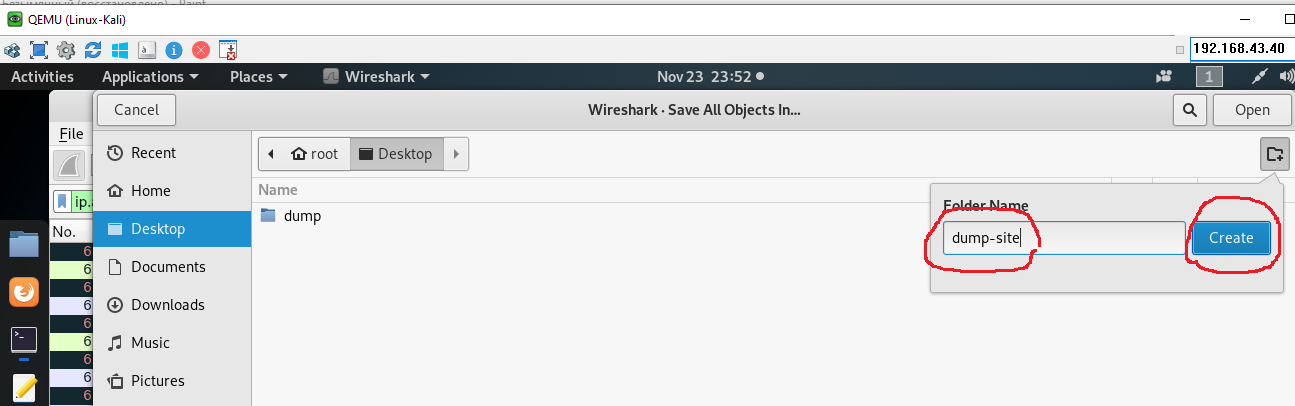


Рис. 60.

Продолжим (см. рис. 51 - 53). В результате мы видим скачанные объекты, среди которых есть странички.

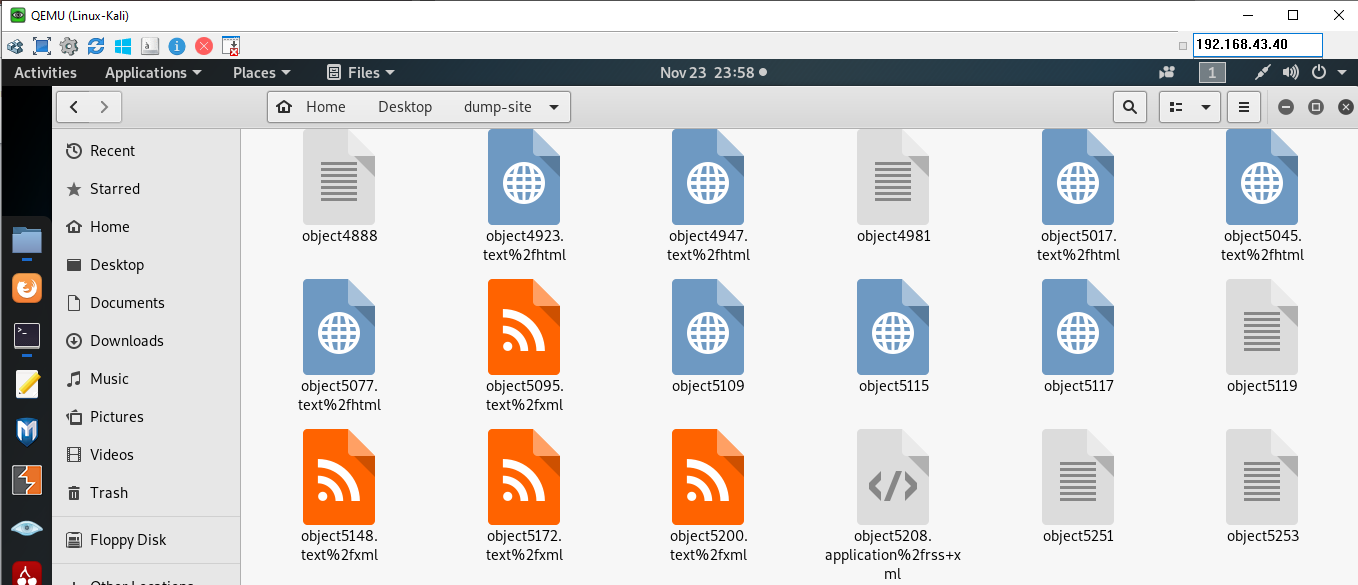


Рис. 61.

Попробуем браузером открыть одну из них.

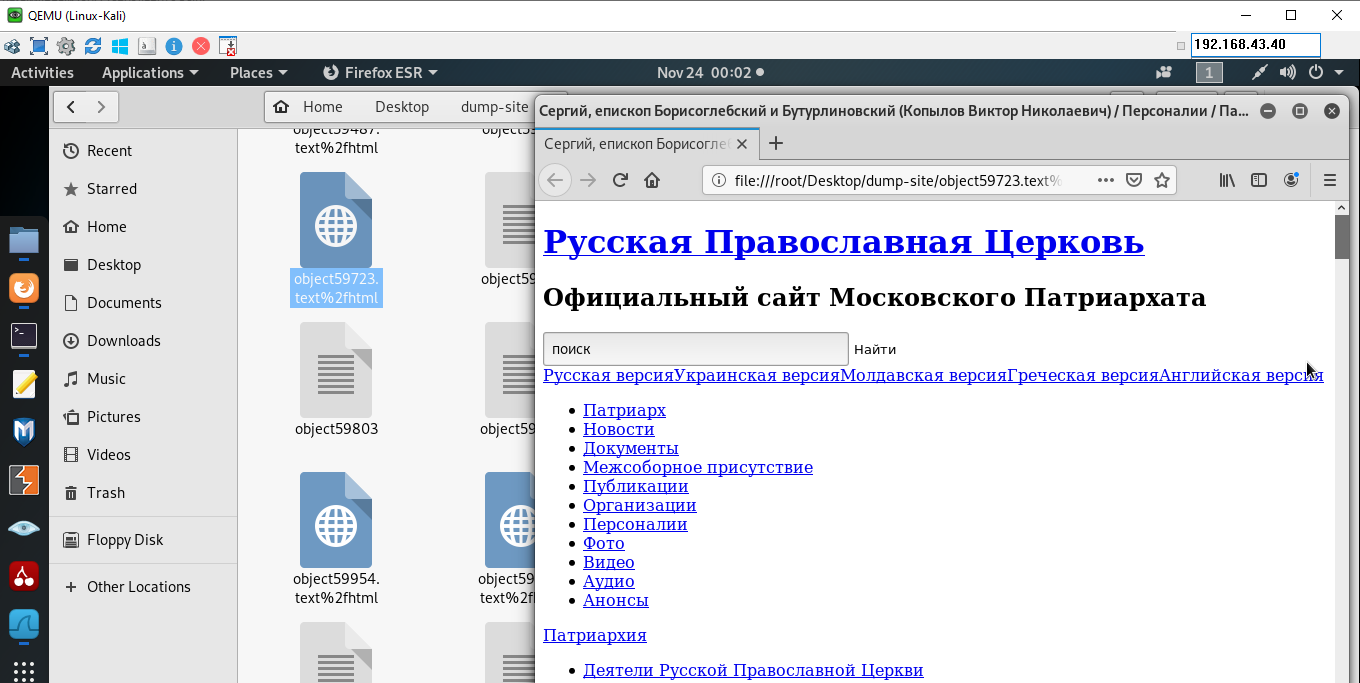


Рис. 62.

А теперь перехватим шифрованный сайт. Запускаем wireshark (см. рис. 57).

# Перехват скачивания шифрованного сайта

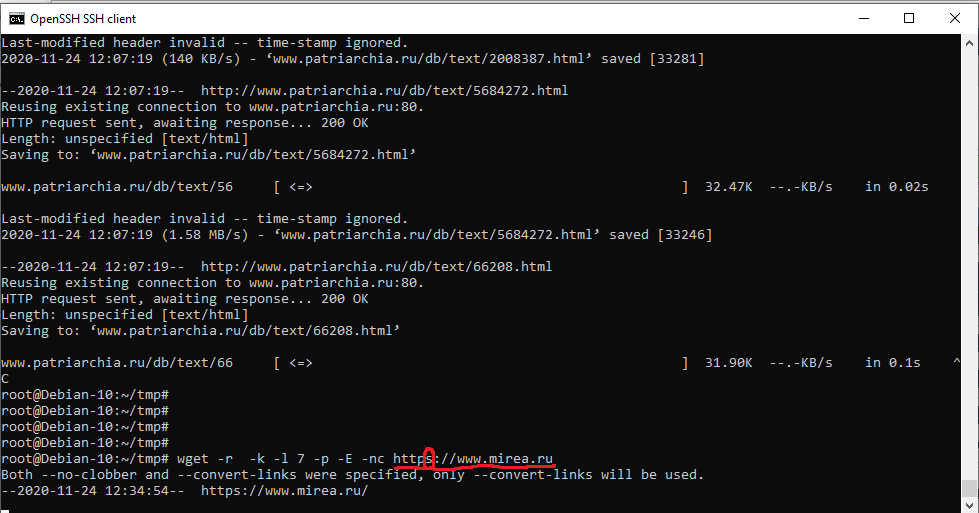


Рис. 63.

Выполняем предыдущие шаги и получаем шифрованные данные, которые невозможно открыть.

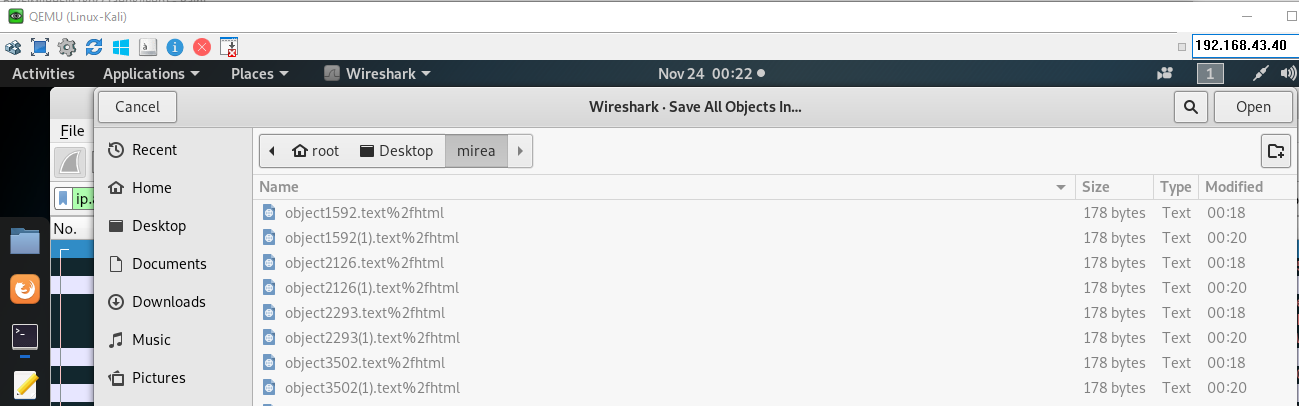


Рис. 64.