

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАФЕДРА
ПРОГРАММНЫХ СИСТЕМ

Отчет по лабораторной работе

Прослушивание трафика с помощью ПО Wireshark

Выполнил:

Антонов Е. П.

студент группы К4120

Проверил: Ананченко И. В.

Санкт-Петербург

2017

ЦЕЛЬ РАБОТЫ:

Прослушать трафик с помощью программы Wireshark, который будет сгенерирован следующими командами:

- Команда ping
- Команда ping для имени сервера. Пример: ping server

ХОД РАБОТЫ:

1. Работа проводится с двумя машинами. На первой машине установлена серверная операционная система Windows Server 2012 R2, на второй машине установлен дистрибутив Kali Linux. Для краткости первую машину будем именовать серверной, вторую машину – клиентской. Узнаем ipaddress серверной машины с помощью команды ipconfig. Выполним команду ping с серверной на клиентскую. Пример показан на рисунке 1.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>ipconfig
'ipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\igorkislyuk>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::c1f5:4979:b9af:7913%12
  IPv4 Address . . . . . : 192.168.1.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 0.0.0.0

Tunnel adapter isatap.{233907FC-D360-4C90-9240-10040CAF0E9E}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\igorkislyuk>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.3:
  Packets: Sent = 4, Received = 4, Lost = 0 <0x loss>
  Approximate round trip time in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\igorkislyuk>
```

Рисунок 1 – Пример команды ping с серверной машины

2. Запустить программу Wireshark и произвести перехват запроса ping с клиентской машины на серверную. Пример продемонстрирован на рисунках 2 и 3.
3. Необходимо выполнить настройку DNSсервера для выполнения запроса на определение ip-адреса через имя сервера. Этапы следующие.
4. Настройка определенных ролей на серверной машине. Сначала выбираются необходимые роли и надстройки над ними. Примеры показаны на рисунках 4, 5, 6.

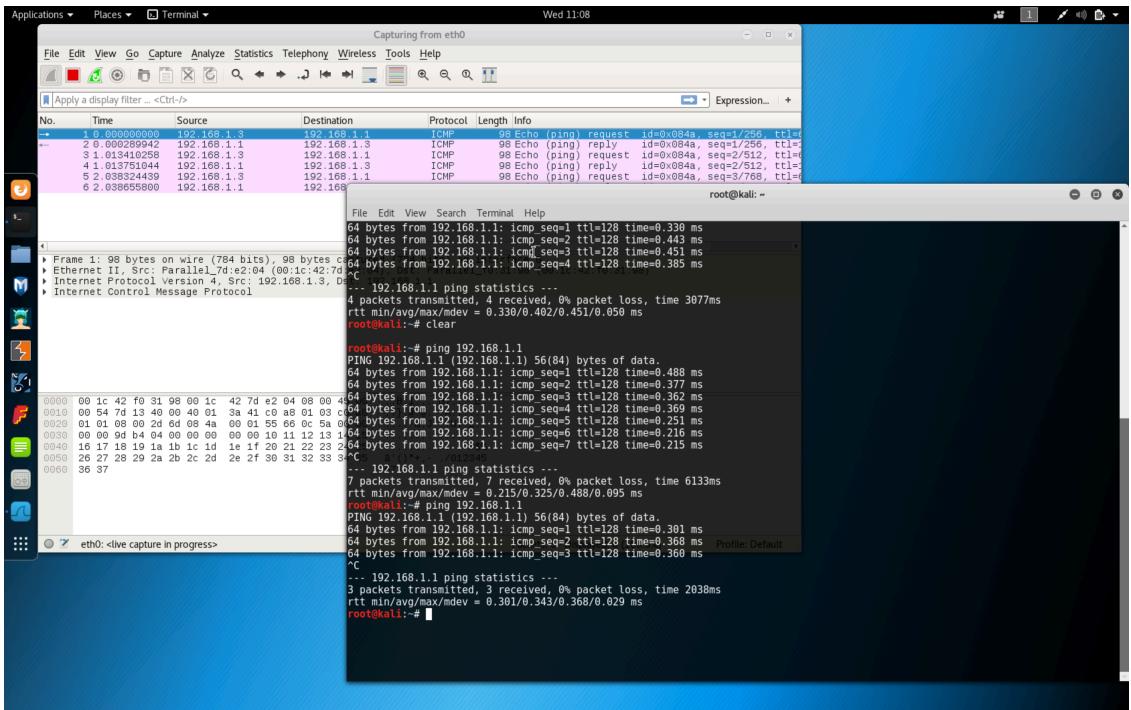


Рисунок 2 – Пример перехвата запроса при помощи программы Wireshark

5. Следующий этапом стала установка зоны и ручное добавление соответствие имени (в данном случае **server** к локальному адресу серверной машины). Процесс добавления зоны продемонстрирован на рисунках 7, 8, 9, 10.
6. Далее необходимо занести соответствие локального адреса и имени компьютера в зону.
7. После предыдущего этапа возможно выполнить запрос на разрешение адреса компьютера через имя в таблице DNS. Примеры показаны на рисунках 11, 12.

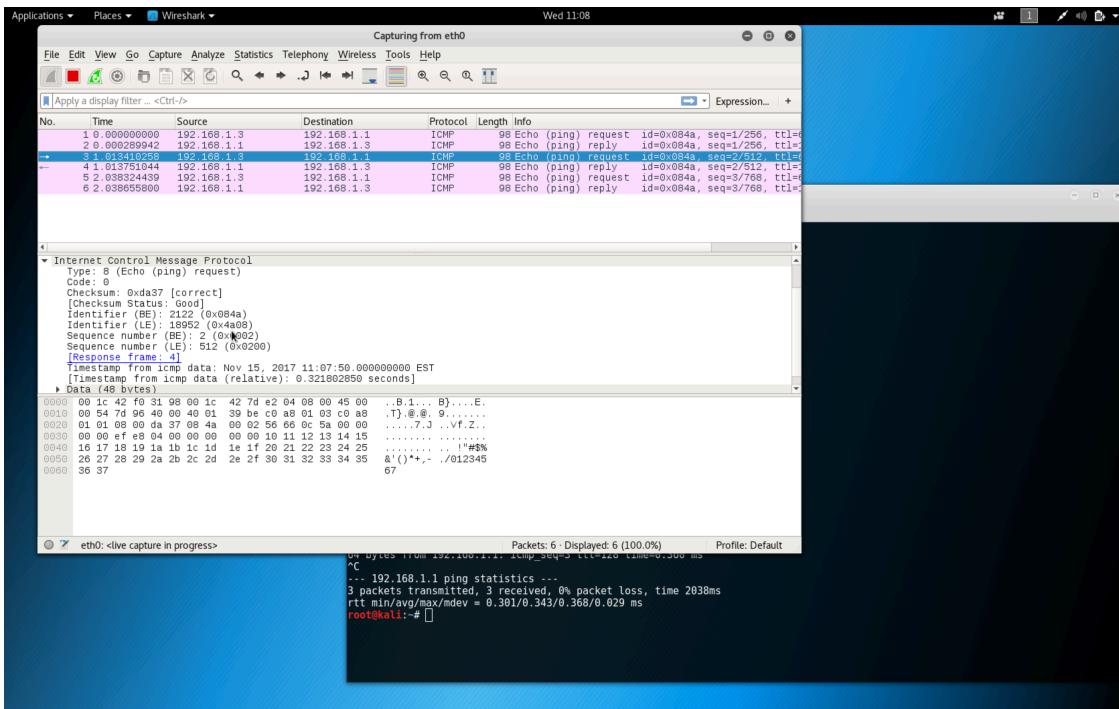


Рисунок 3 – Пример детального вида для команды ping

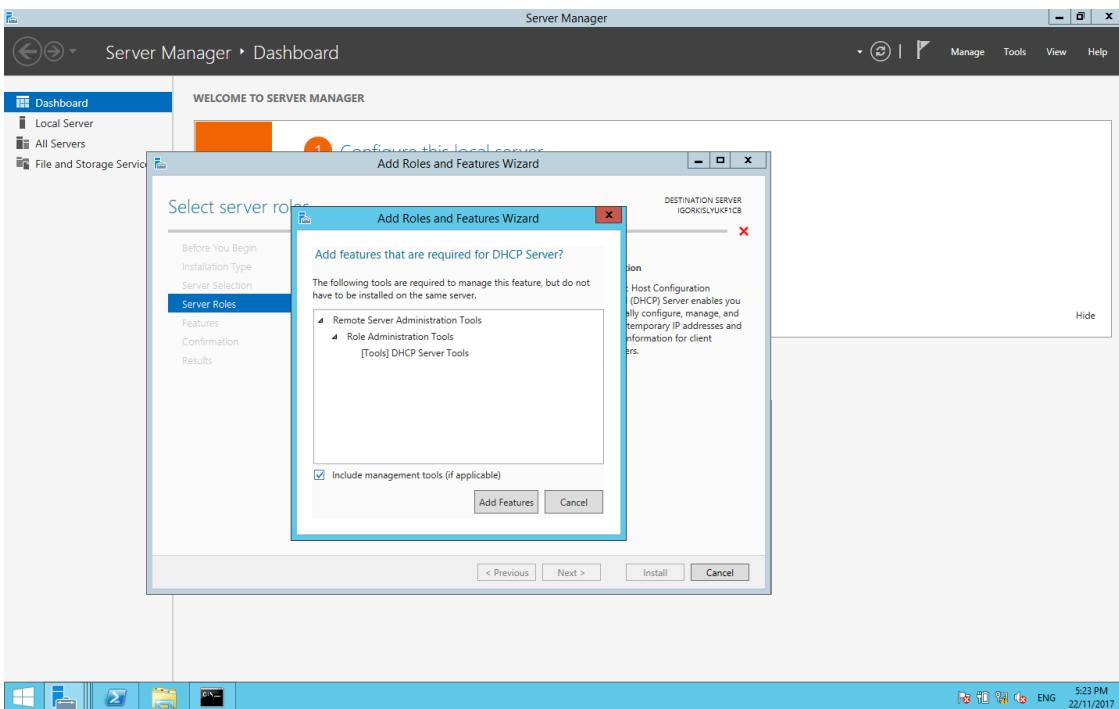


Рисунок 4 – Выбор роли DNS среди доступных ролей

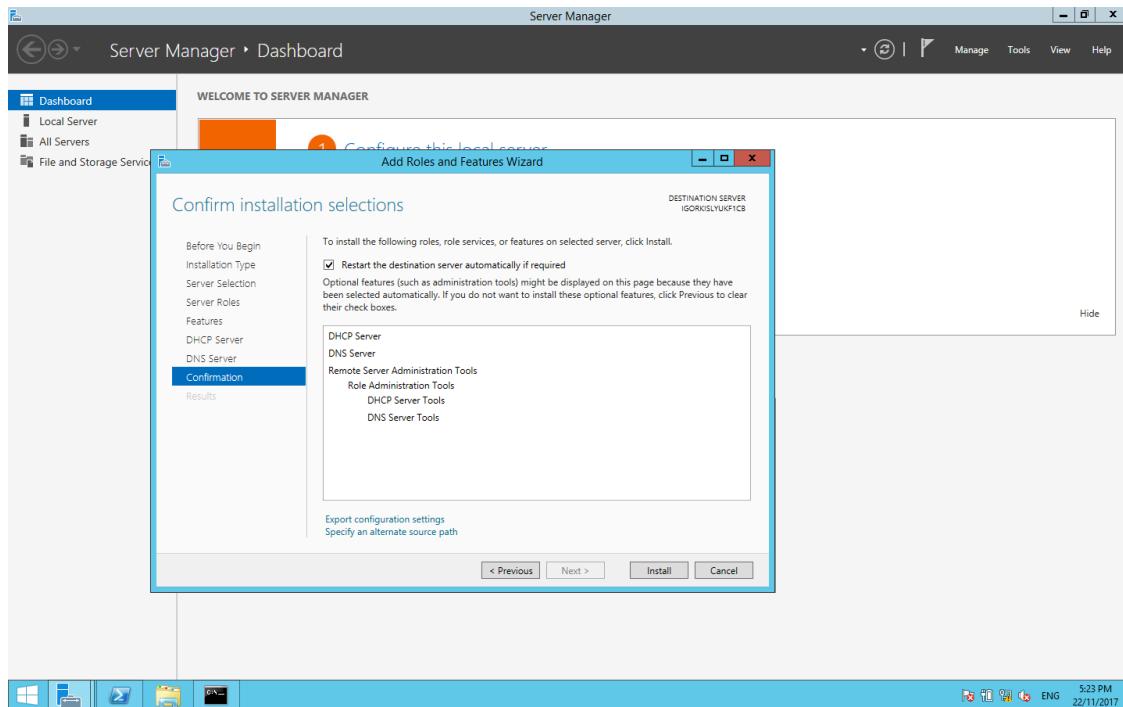


Рисунок 5 – Подтверждение установки DNS ролей

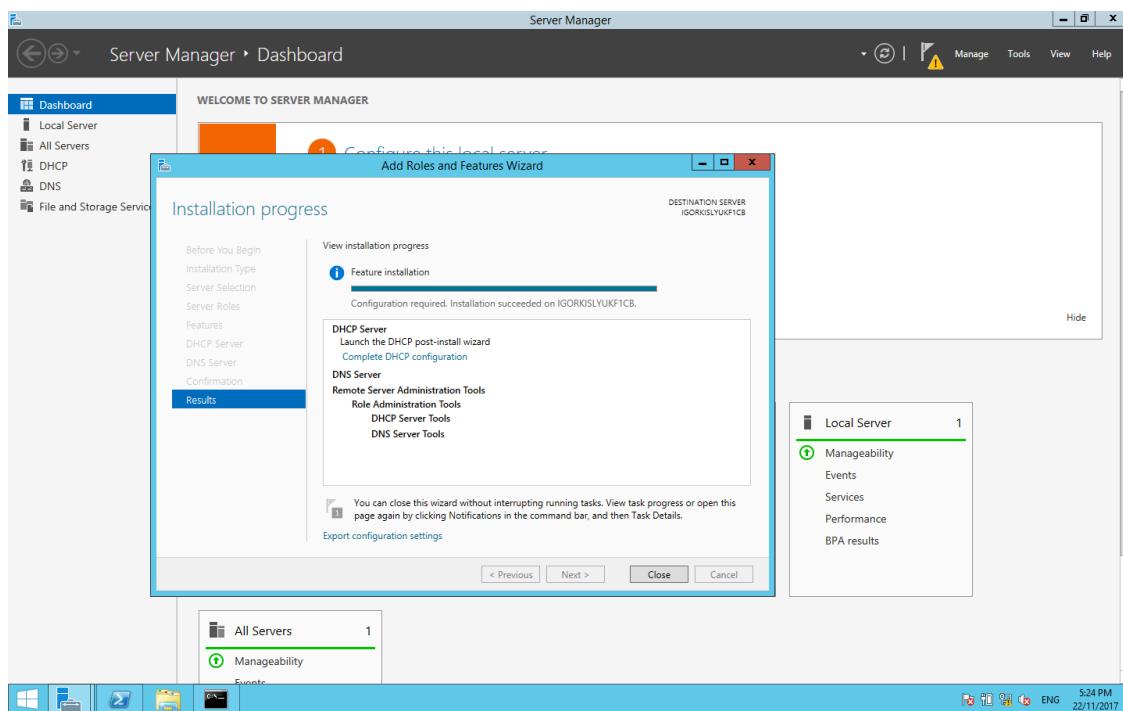


Рисунок 6 – Завершение установки DNS ролей и надстроек

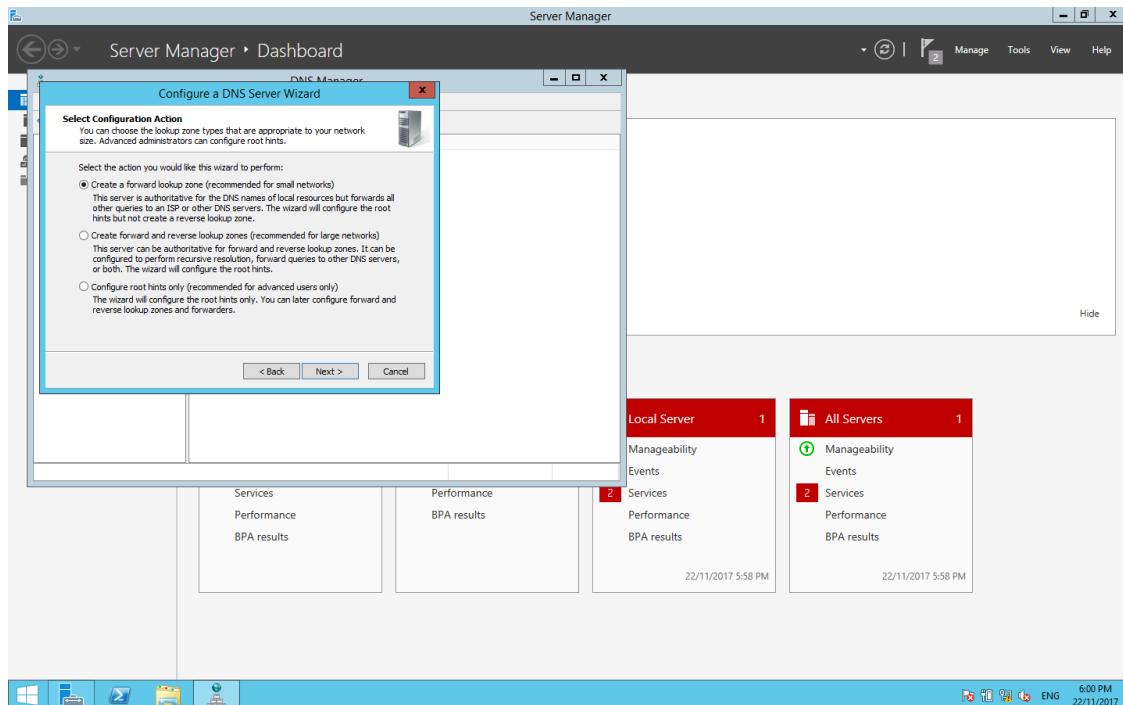


Рисунок 7 – Создание зоны типа forward lookup zone

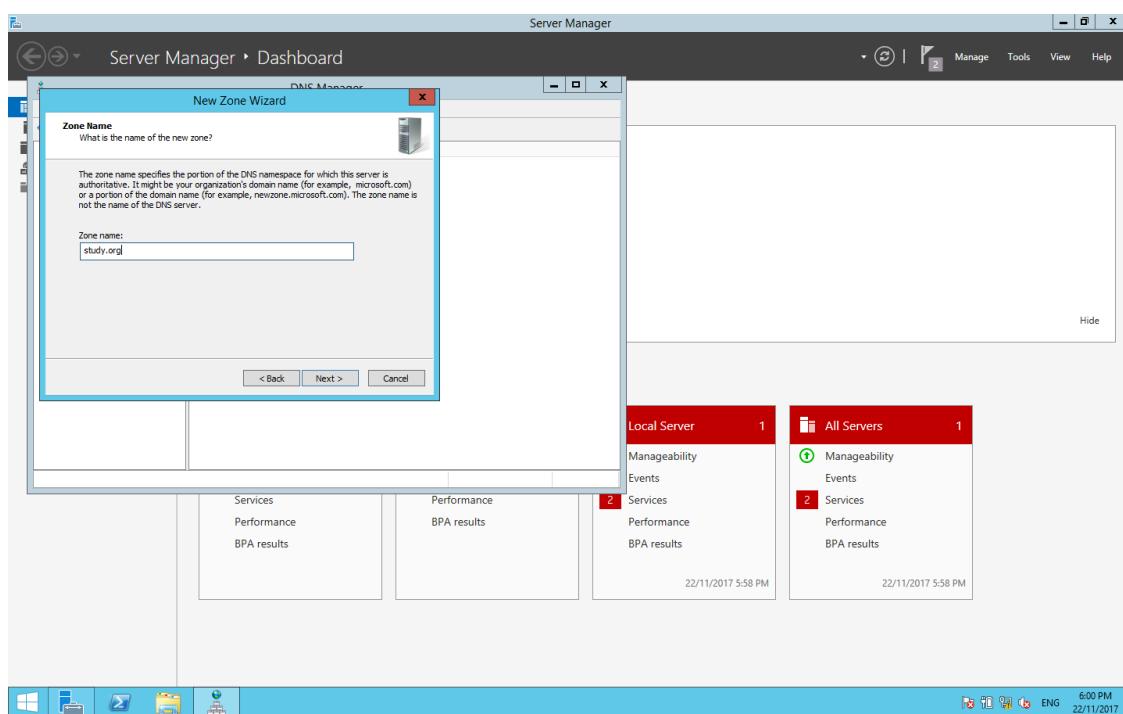


Рисунок 8 – Установка имени зоны

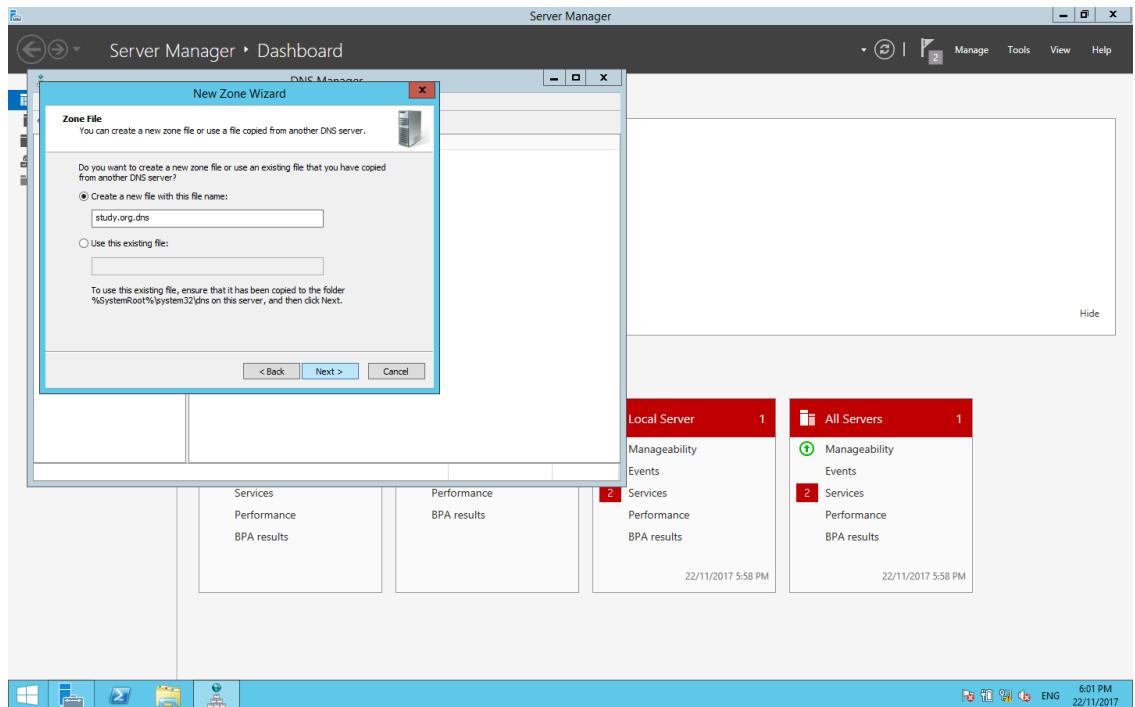


Рисунок 9 – Выбор файла для хранение значений в данной зоне

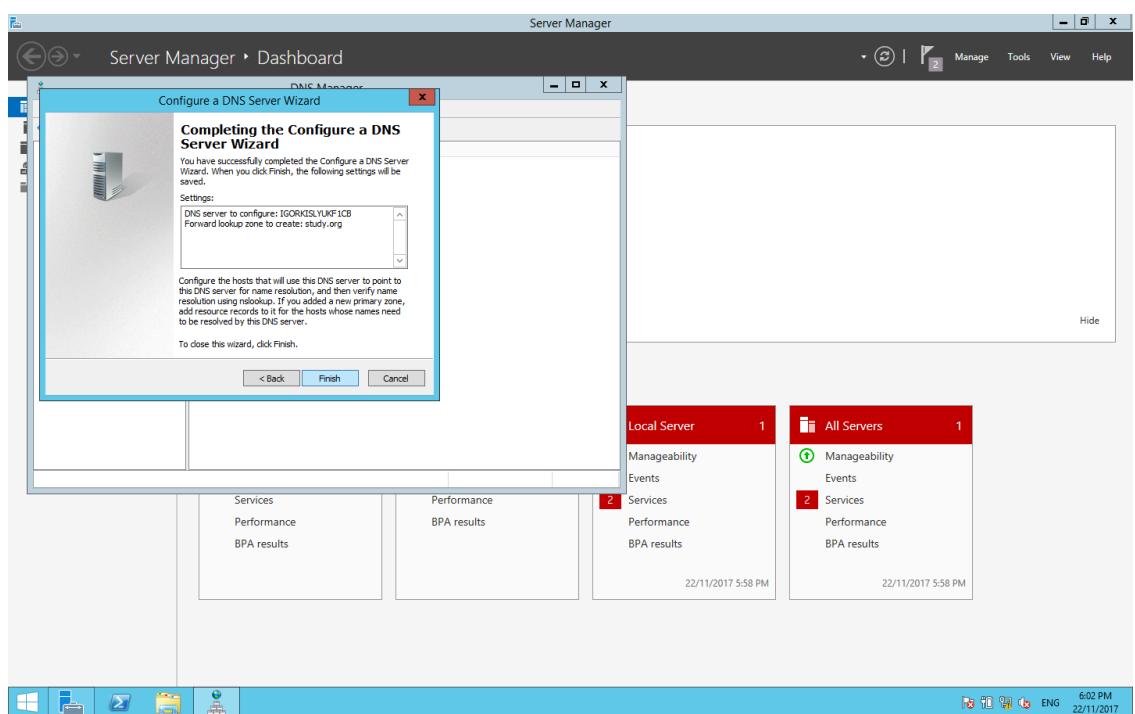


Рисунок 10 – Завершение настройки зоны

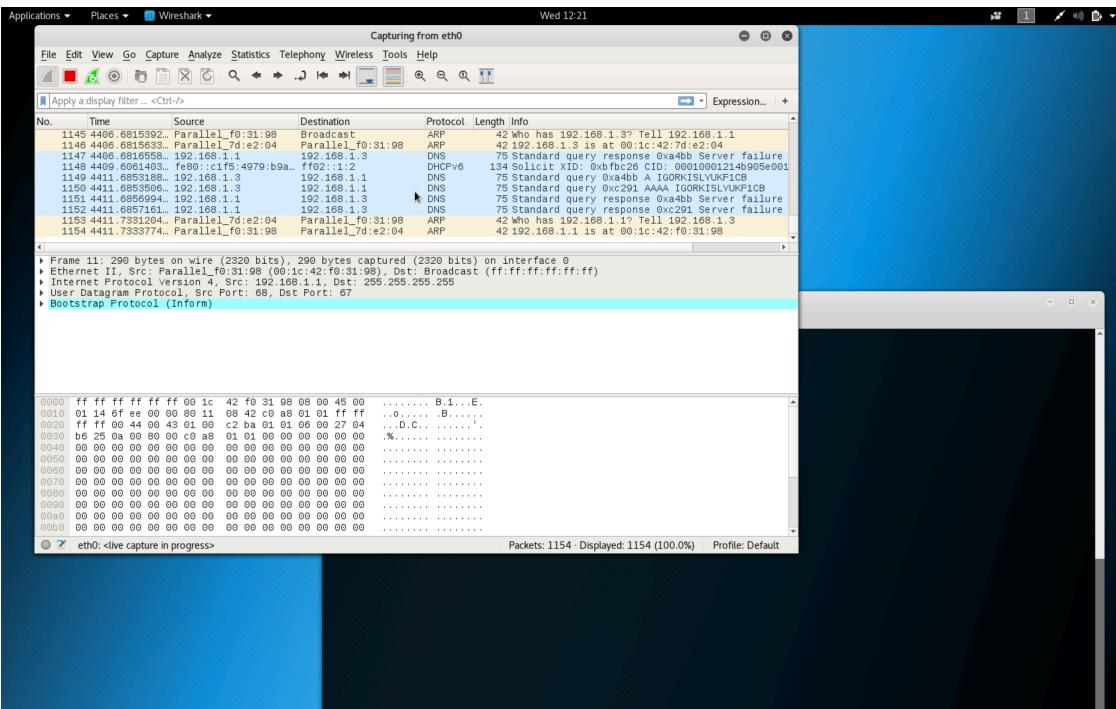


Рисунок 11 – Пример возможного списка пакетов при выполнении запроса DNS

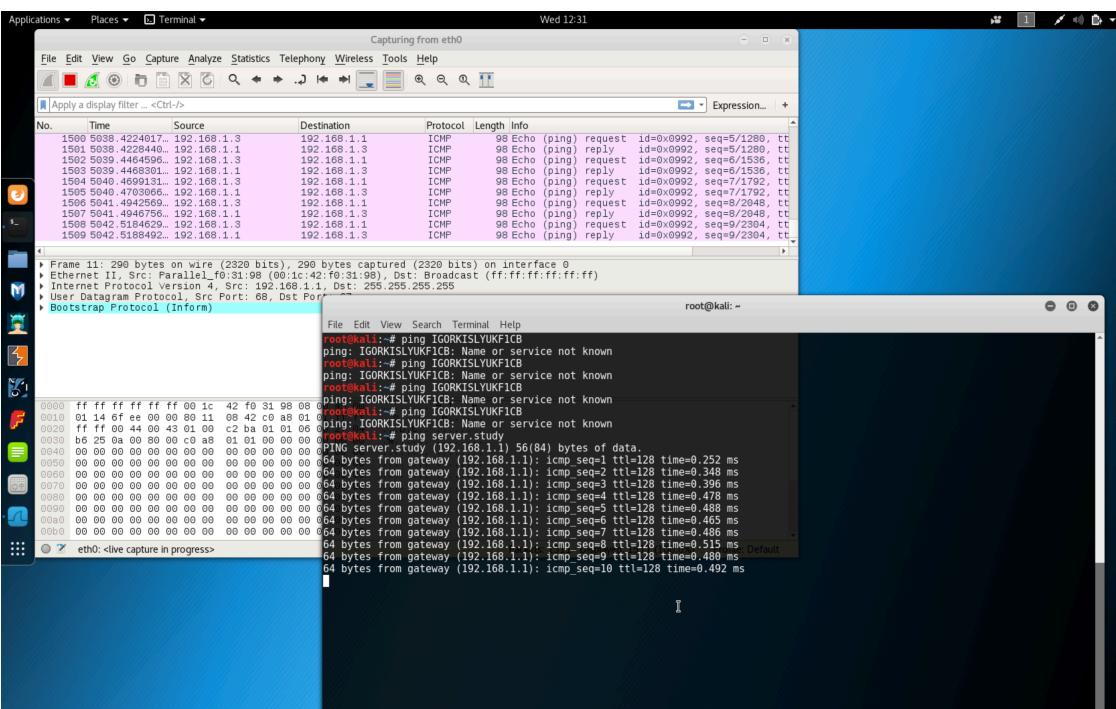


Рисунок 12 – Пример окна терминала, в котором происходит разрешение имени DNS

ВЫВОД:

В ходе лабораторной работы была построена сеть с двумя виртуальными машинами, на одной из которых был установлен дистрибутив Kali Linux. На прослушиваемой машине была поднята роль DNS-сервера.

При помощи входящей в дистрибутив программы Wireshark были перехвачены следующие типы запросов:

- ping запрос
- DNS запрос

В результате были получены навыки использования специального ПО для перехвата и просмотра трафика в сети.