实验二
IP 和 TCP 数据分组的捕获和解析

计算机学院

2022年6月

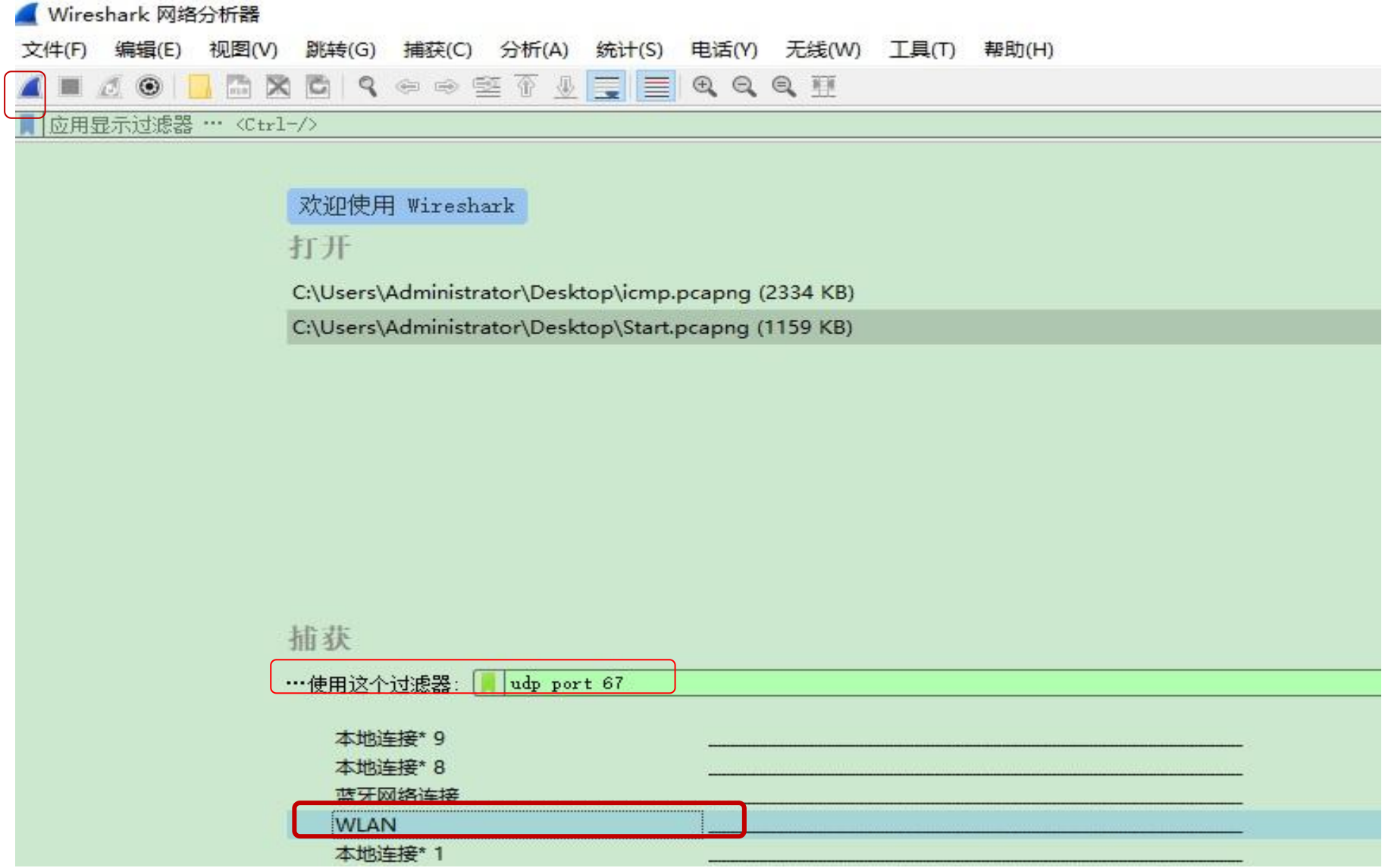
基本内容

- 实验内容
  - 捕获在网络中传输的数据包
    - IP包、ICMP报文、TCP报文段、DHCP报文
  - 对于捕获到的数据包进行分析，理解协议规定的通信过程和包头重要字段的功能
- 实验组人数
  - 1人独立完成
- 实验设备环境
  - 能够联网的计算机
  - Windows, Linux OS
  - Wireshark软件

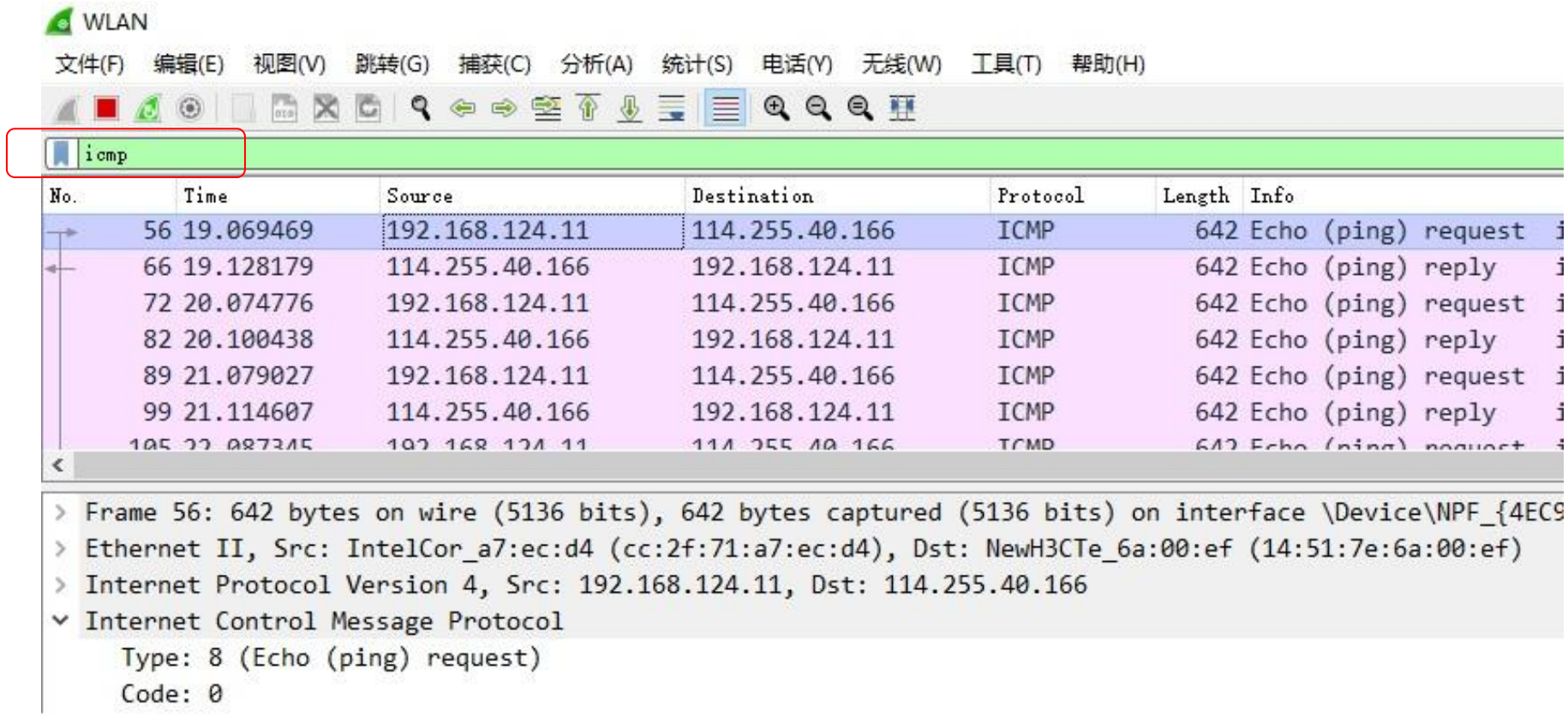
实验步骤

- 安装wireshark软件
  - https://www.wireshark.org/#download
- 设置捕获条件（捕获过滤器）
  - DHCP：udp port 67
  - ICMP: icmp
  - TCP: tcp port 80
- 或者设置显示条件（显示过滤器）
  - DHCP：dhcp
  - ICMP: icmp
  - TCP: tcp.port==80
- 捕获数据并存储
- 分析数据并撰写实验报告

捕获过滤器的设置示例

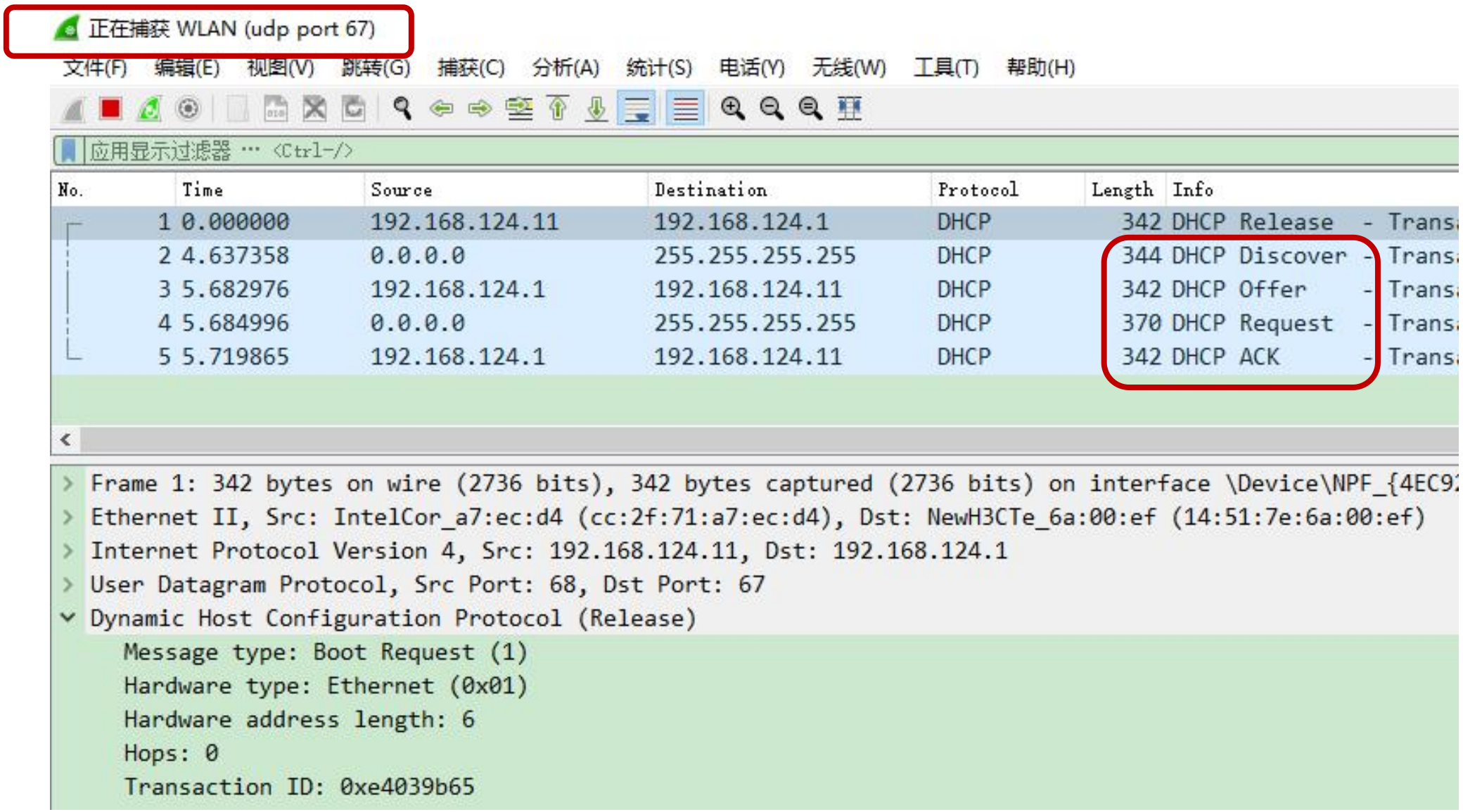

Wireshark 网络分析器
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
欢迎使用 Wireshark
打开
C:\Users\Administrator\Desktop\icmp.pcapng (2334 KB)
C:\Users\Administrator\Desktop\Start.pcapng (1159 KB)
捕获
…使用这个过滤器: udp port 67
本地连接* 9
本地连接* 8
蓝牙网络连接
WLAN
本地连接* 1

显示过滤器的设置示例


WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp
No. Time Source Destination Protocol Length Info
56 19.069469 192.168.124.11 114.255.40.166 ICMP 642 Echo (ping) request
66 19.128179 114.255.40.166 192.168.124.11 ICMP 642 Echo (ping) reply
72 20.074776 192.168.124.11 114.255.40.166 ICMP 642 Echo (ping) request
82 20.100438 114.255.40.166 192.168.124.11 ICMP 642 Echo (ping) reply
89 21.079027 192.168.124.11 114.255.40.166 ICMP 642 Echo (ping) request
99 21.114607 114.255.40.166 192.168.124.11 ICMP 642 Echo (ping) reply
Frame 56: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF_{4EC9
Ethernet II, Src: IntelCor_a7:ec:d4 (cc:2f:71:a7:ec:d4), Dst: NewH3CTe_6a:00:ef (14:51:7e:6a:00:ef)
Internet Protocol Version 4, Src: 192.168.124.11, Dst: 114.255.40.166
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0

捕获到的DHCP报文示例

捕获过滤器



实验报告要求

- 实验内容和实验环境描述
- 捕获方法和过程
- 协议数据分析
  - DHCP的通信过程
  - ICMP的报文格式及主要字段的功能
  - IP数据报分段的原理、关键字段的值
  - TCP建立连接和释放连接的过程、关键字段的值
- 实验总结和心得体会
  - 上机调试时间，遇到的问题和解决方法

报告提交要求

- 提交截止时间：2022 年6月12日晚
- 实验报告提交平台：北邮教学云平台ucloud.bupt.edu.cn
- 实验报告文件格式：.pdf 文件
- 实验报告命名方式：实验2报告-学号-姓名.pdf
- 实验报告内容：

  1）标准实验报告封面（要求与实验1相同）

  2）报告主体内容

Any Questions?