華東師範大學
EAST CHINA NORMAL UNIVERSITY

实验一：Protocol Layer

1、实验目标

1. 学习协议和分层如何用数据包表示;

2. 熟悉wireshark软件、curl、wget等常用软件的使用，掌握网络抓包的方法，能在所用电脑上进 行抓包;

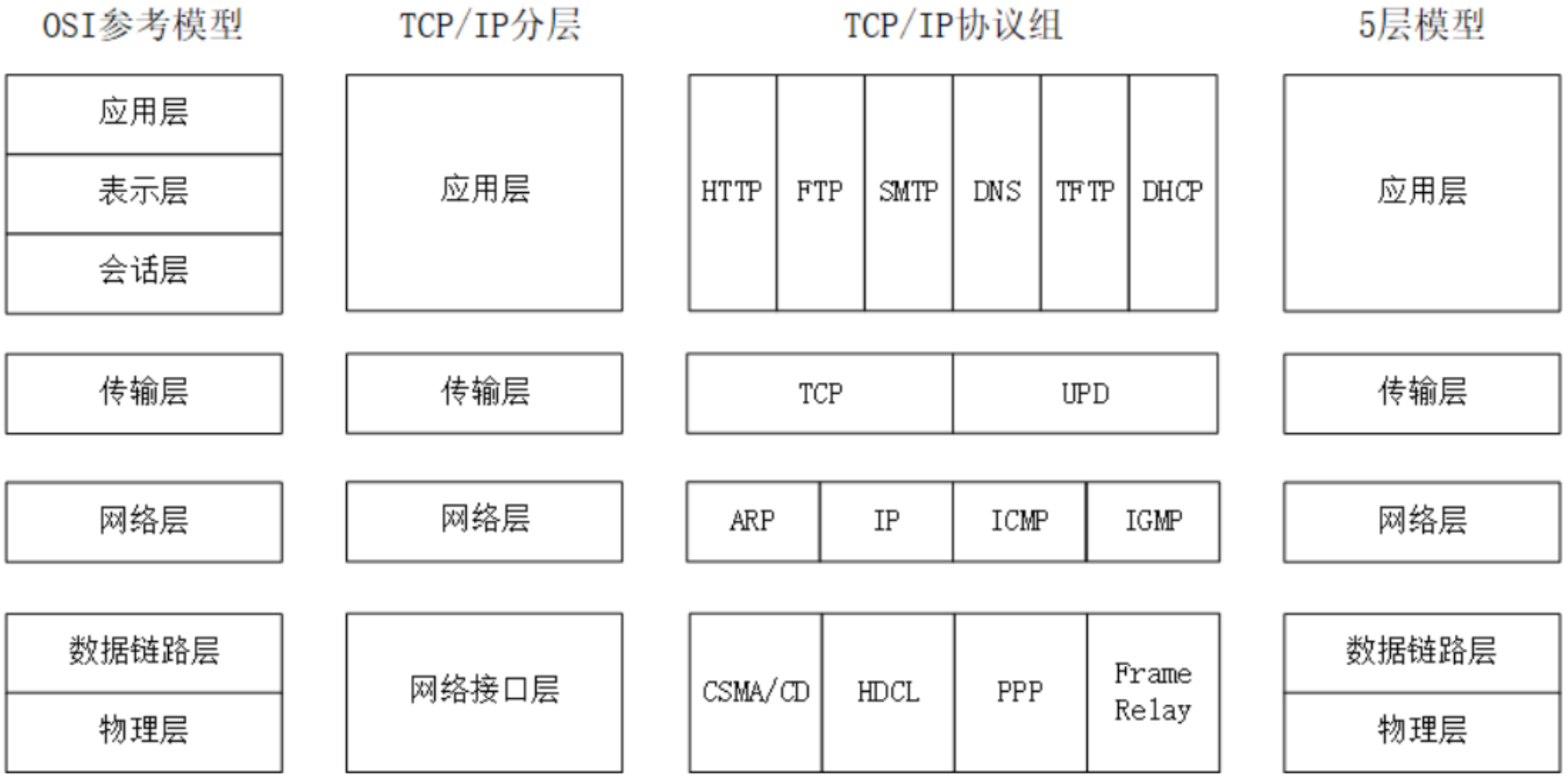
3. 了解IP数据包格式，能应用该软件分析数据包格式，查看抓到的包的内容，并分析对应的IP数据 包格式;

4. 抓包分析数据包，估算协议的开销;

5. 通过数据包抓取实验，将理论与实践相结合，深入理解协议层的字段与结构特征.

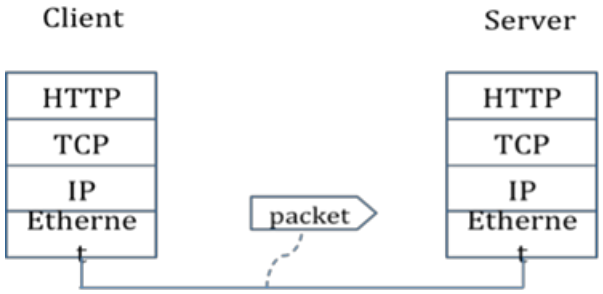
2、背景知识——协议层

将所有的协议综合起来，各个层次的所有协议被称为协议栈。因特网的协议栈由5个层次组成：物理层、链路层、网络层、传输层和应用层。这个划分方法称为TCP/IP五层协议。除此之外，还有OSI七层模型和TCP/IP四层协议。它们之间的对应关系如下：



2、背景知识——协议层

本实验中，抓取HTTP请求的数据包，其协议栈如图所示：



在上述请求的流程中，主要有以下四个步骤：

1. 客户端通过TCP三次握手与服务器建立连接。

2. TCP建立连接成功后，向服务器发送HTTP请求。

3. 服务器接收客户端的HTTP请求后，将返回应答，并向客户端发送数据。

4. 客户端通过TCP四次断开，与服务器断开TCP连接。

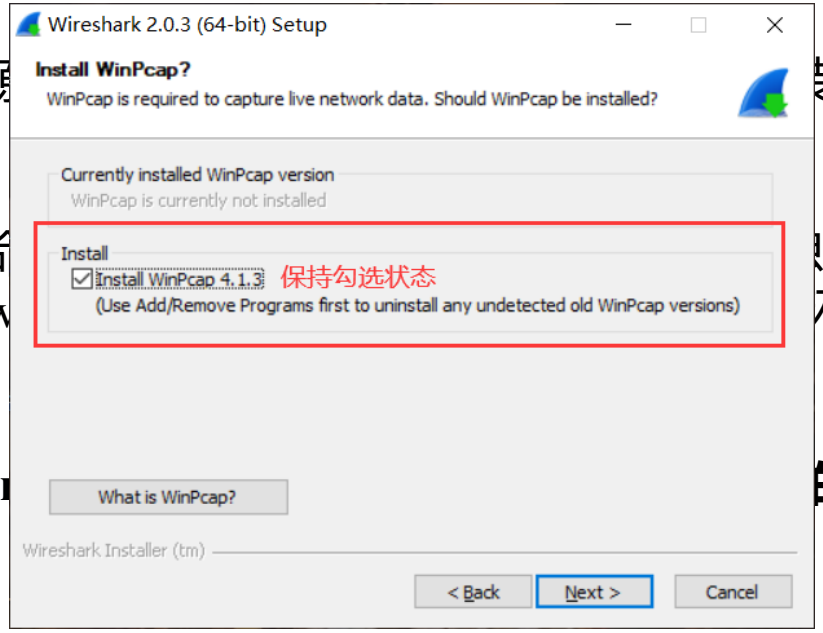
2、背景知识——实验环境

最新版本下载：
大夏学堂->课程资源

注：wget无需安装，
方法一：解压后在命
方法二：解压后将w

行中执行wget命令。

注意，安装wireshar



最新版本下载：
Wireshark （https://www.wireshark.org/#download）
wget工具（http://gnuwin32.sourceforge.net/packages/wget.htm）

3、实验步骤

1. 启动Wireshark点击->捕获->选项->输入tab->选择本地网卡，过滤条件（所选择接口的捕获过滤 器）为 "tcp port 80"，在选项tab中勾选解析网络名称，点击开始按钮；

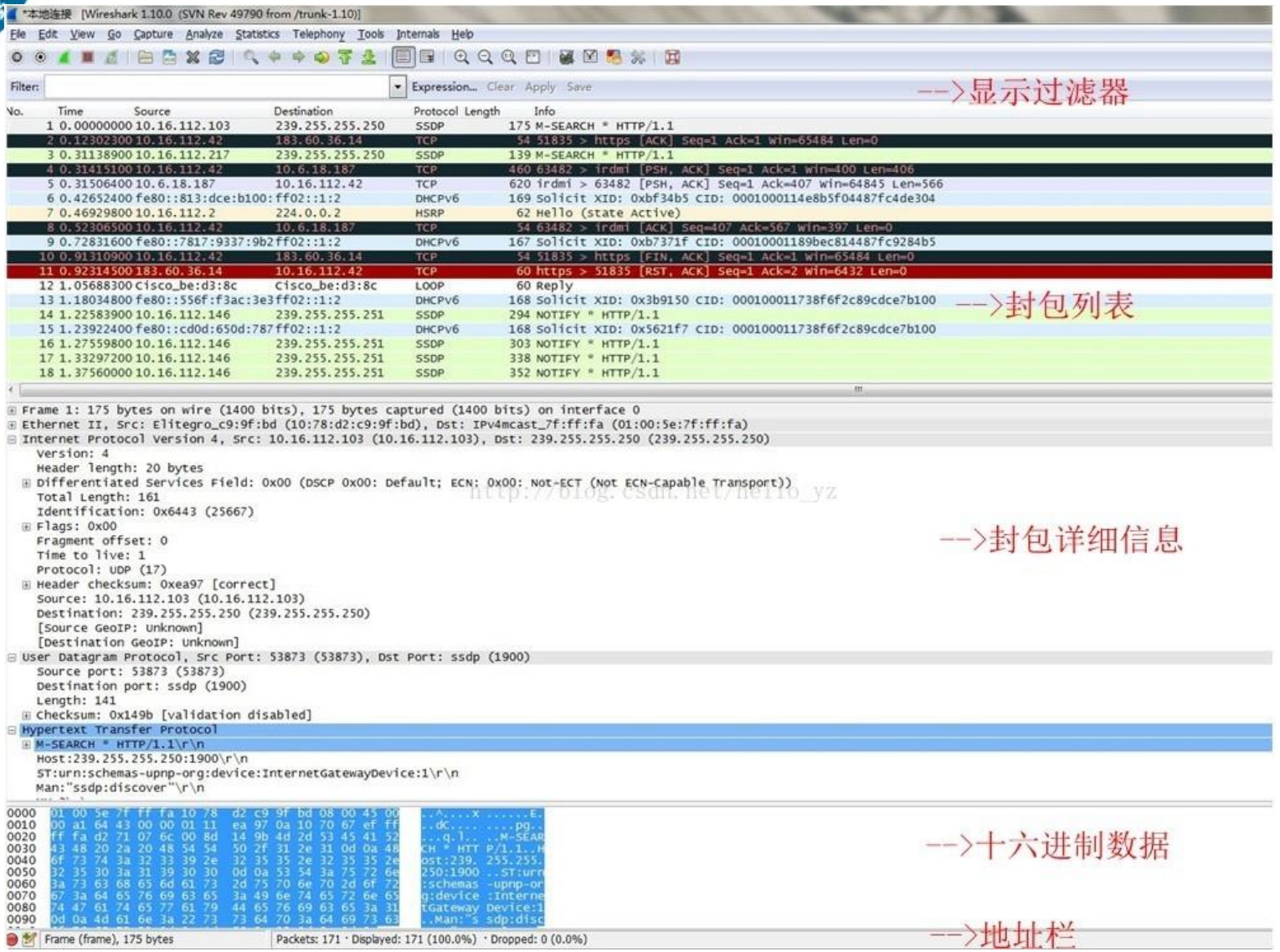
2. 关闭不必要的浏览器标签和窗口,避免跟踪非目的流量；

3. 在命令行中选取一个URL，用wget获取。例如 wget http://www.qq.com；

4. 打开Wireshark， 停止捕获。

5. 查看Wireshark界面中的封包列表中如果出现数据包则说明抓包成功；

3、实验步骤——抓包截图

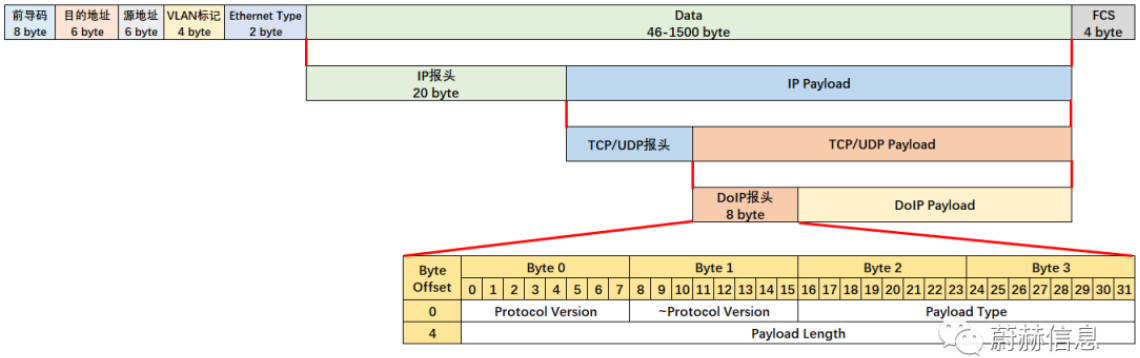

*本地连接 [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
-->显示过滤器
No. Time Source Destination Protocol Length Info
1 0.00000000 10.16.112.103 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
2 0.12302300 10.16.112.42 183.60.36.14 TCP 54 51835 > https [ACK] Seq=1 Ack=1 Win=65484 Len=0
3 0.31138900 10.16.112.217 239.255.255.250 SSDP 139 M-SEARCH * HTTP/1.1
4 0.31415100 10.16.112.42 10.6.18.187 TCP 460 63482 > irdmi [PSH, ACK] Seq=1 Ack=1 Win=400 Len=406
5 0.31506400 10.6.18.187 10.16.112.42 TCP 620 irdmi > 63482 [PSH, ACK] Seq=1 Ack=407 Win=64845 Len=566
6 0.42652400 fe80::813:dce:b100: ff02::1:2 DHCPv6 169 Solicit XID: 0xbf34b5 CID: 0001000114e8b5f04487fc4de304
7 0.46929800 10.16.112.2 224.0.0.2 HSRP 62 Hello (state Active)
8 0.52306500 10.16.112.42 10.6.18.187 TCP 54 63482 > irdmi [ACK] Seq=407 Ack=567 Win=397 Len=0
9 0.72831600 fe80::7817:9337:9b2 ff02::1:2 DHCPv6 167 Solicit XID: 0xb7371f CID: 00010001189bec814487fc9284b5
10 0.91310900 10.16.112.42 183.60.36.14 TCP 54 51835 > https [FIN, ACK] Seq=1 Ack=1 Win=65484 Len=0
11 0.92314500 183.60.36.14 10.16.112.42 TCP 60 https > 51835 [RST, ACK] Seq=1 Ack=2 Win=6432 Len=0
12 1.05688300 Cisco_be:d3:8c Cisco_be:d3:8c LOOP 60 Reply
13 1.18034800 fe80::556f:f3ac:3e3 ff02::1:2 DHCPv6 168 Solicit XID: 0x3b9150 CID: 000100011738f6f2c89cdce7b100
14 1.22583900 10.16.112.146 239.255.255.251 SSDP 294 NOTIFY * HTTP/1.1
15 1.23922400 fe80::cd0d:650d:787 ff02::1:2 DHCPv6 168 Solicit XID: 0x5621f7 CID: 000100011738f6f2c89cdce7b100
16 1.27559800 10.16.112.146 239.255.255.251 SSDP 303 NOTIFY * HTTP/1.1
17 1.33297200 10.16.112.146 239.255.255.251 SSDP 338 NOTIFY * HTTP/1.1
18 1.37560000 10.16.112.146 239.255.255.251 SSDP 352 NOTIFY * HTTP/1.1
-->封包列表
Frame 1: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
Ethernet II, Src: Elitegro_c9:9f:bd (10:78:d2:c9:9f:bd), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 10.16.112.103 (10.16.112.103), Dst: 239.255.255.250 (239.255.255.250)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 161
Identification: 0x6443 (25667)
Flags: 0x00
Fragment offset: 0
Time to live: 1
Protocol: UDP (17)
Header checksum: 0xea97 [correct]
Source: 10.16.112.103 (10.16.112.103)
Destination: 239.255.255.250 (239.255.255.250)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53873 (53873), Dst Port: ssdp (1900)
Source port: 53873 (53873)
Destination port: ssdp (1900)
Length: 141
Checksum: 0x149b [validation disabled]
Hypertext Transfer Protocol
M-SEARCH * HTTP/1.1\r\n
Host:239.255.255.250:1900\r\n
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
Man:"ssdp:discover"\r\n
-->封包详细信息
0000 01 00 5e 7f ff fa 10 78 d2 c9 9f bd 08 00 45 00 ..^....x ......E.
0010 00 a1 64 43 00 00 01 11 ea 97 0a 10 70 67 ef ff ..dC.... ....pg..
0020 ff fa d2 71 07 6c 00 8d 14 9b 4d 2d 53 45 41 52 ...q.l.. ..M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 6f 73 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e ost:239. 255.255.
0050 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 75 72 6e 250:1900 ..ST:urn
0060 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f 72 :schemas -upnp-or
0070 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72 6e 65 g:device :Interne
0080 74 47 61 74 65 77 61 79 44 65 76 69 63 65 3a 31 tGateway Device:1
0090 0d 0a 4d 61 6e 3a 22 73 73 64 70 3a 64 69 73 63 ..Man:"s sdp:disc
-->十六进制数据
Frame (frame), 175 bytes
Packets: 171 · Displayed: 171 (100.0%) · Dropped: 0 (0.0%)
-->地址栏

4、实验结果分析

在抓取HTTP请求的GET方法时，分析其数据包，思考下列问题：

1、根据抓取的HTTP请求的GET方法的抓取结果，分析协议包的内容。

2、画一个关于使用GET方法的HTTP请求的图(与下图类似)，为了显示协议层的嵌套结构，请分别标出Ethernet， IP和TCP协议的头部的位置、大小以及其负载的范围。



4、实验结果与分析

在抓取HTTP请求的GET方法时，分析其数据包，思考下列问题：

3、根据数据包的抓取结果，分析协议开销。

4、 估计协议的开销或者是协议开销占用下载字节的百分比。对于下载的主要部分中的每一个包，我们需要分析 Ethernet，IP和TCP的开销，和有用的HTTP数据的开销，你认为这种开销是必要的吗？ （假设HTTP数据（头部和消息）是有用的，而TCP，IP和Ethernet头部认为是开销。）

4、实验结果与分析

观察下载的以太网和IP头包回答下面问题：

1、以太网头部中哪一部分是解复用（解复用： 找到正确的上一层协议来处理到达的包的行为叫做 解复用）键并且告知它的下一个高层指的是IP，在这一包内哪一个值可以表示IP？

2、IP头部中哪一部分是解复用键并且告知它的下一个高层指的是TCP，在这一包内哪一个值可以表示TCP？

4、实验结果与分析

观察下载的以太网和IP头包回答下面问题：

1、以太网头部中哪一部分是解复用（解复用： 找到正确的上一层协议来处理到达的包的行为叫做 解复用）键并且告知它的下一个高层指的是IP，在这一包内哪一个值可以表示IP？

2、IP头部中哪一部分是解复用键并且告知它的下一个高层指的是TCP，在这一包内哪一个值可以表示TCP？

5、问题与思考

在完成本实验后探索协议和分层，思考下列问题：

- 查看不包含高层数据的短TCP数据包，查看它发往哪？不携带高层数据的数据包有用吗？
- 在经典的分层模型中，低层字段包装到高层数据包外面，成为一条新消息。但这并非总是如此,Web响应（一个包含HTTP标头和HTTP有效负载的HTTP消息）可能被转换为多个较低层的消息（即多个TCP数据包）。假设你为Web响应的第一个和最后一个TCP数据包绘制了数据包结构，那么该结构与经典分层模型有什么不同？

5、问题与思考

- 在上述经典分层模型中，低层字段包装到高层数据包外面，如果较低层添加加密，此模型将如何更改？

- 在上述经典分层模型中，低层字段包装到高层数据包外面,如果较低的层添加压缩，此模型将如何更改？