实验六：HTTP 协议分析

一、实验目的

1、了解 HTTP 协议；
2、熟悉 HTTP 状态码含义；
3、掌握 HTTP 报文结构。

二、实验学时

2 学时

扫码看步骤

扫码看演示

三、实验类型

综合型

四、实验需求

1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

推荐 Ubuntu Desktop 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。
支持 Windows 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。
安装 HTTP 协议调试代理工具 Fiddler Everywhere 软件。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、实验任务

1、通过 Wireshark 分析 HTTP 报文结构；
2、通过 Fiddler Eveywhere 分析 HTTP 通信过程。

六、实验内容及步骤

任务 1：HTTP 报文结构分析

步骤 01：设置过滤协议，启动 Wireshark 进行抓包
启动 Wireshark，设置过滤为【http】，如图 6-1 所示。

步骤 02：使用浏览器访问 HTTP 网站

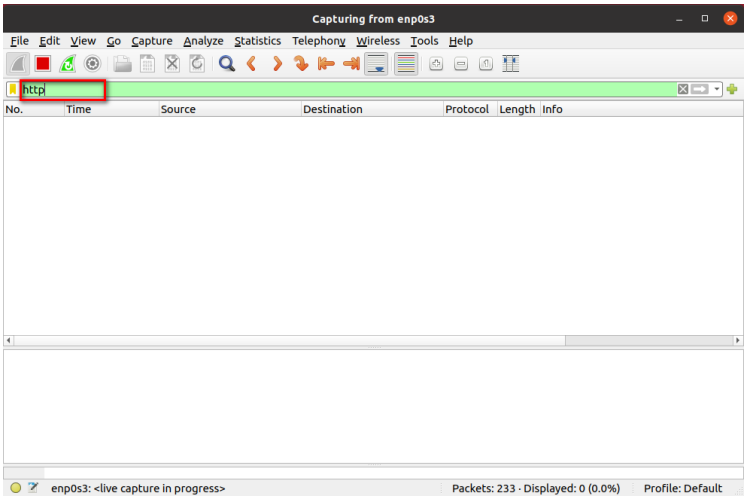

图 6-1 Wireshark 报文分析

使用浏览器访问信息技术学院教学云平台（http://it.hactcm.edu.cn）。

步骤 03：分析 HTTP 报文结构

①在 Wireshark 抓包窗体中，查看获取的 HTTP 协议报文数据，如图 6-2 所示。

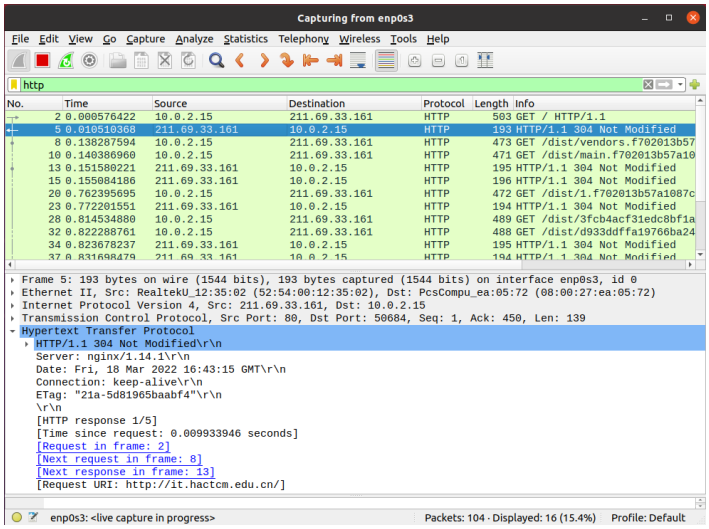

图 6-2 HTTP 报文数据

②对获取的 HTTP 报文数据进行分析，并填写表 6-1。

表 6-1 HTTP 协议报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第　位		
2	Status code		第　位		
3	Response Phrase		第　位		
4	Content-Length		第　位		
5	Content-Type		第　位		
6	Content-Location		第　位		

7	Last-Modified		第　位		
8	Accept-Ranges		第　位		
9	ETag		第　位		
10	Server		第　位		
11	X-Powered-By		第　位		
12	Date		第　位		
13	Time Since Request		第　位		
14	抓取数据包的详细内容：				

任务 2：下载 Fiddler Everywhere

步骤 01：下载 Fiddler Everywhere

由于本地浏览器无法发送 HTTP 协议的 HEAD 和 POST 请求，本实验采用 HTTP 协议调试代理工具 Fiddler Everywhere，实现不同请求类型的 HTTP 协议数据包的发送。

①Fiddler Everywhere 下载

Fiddler Everywhere 软件安装程序可通过官方网站（https://www.telerik.com/fiddler）和课程网站（http://network.xg.hactcm.edu.cn）获得。

步骤 02：启动 Fiddler Everywhere

①设置安装包可执行权限，右击下载的 Fiddler Everywhere 软件包，选择“Properties”“Permission”，勾选“Execute”的“Allow execute file as program”，如图 6-3 所示。

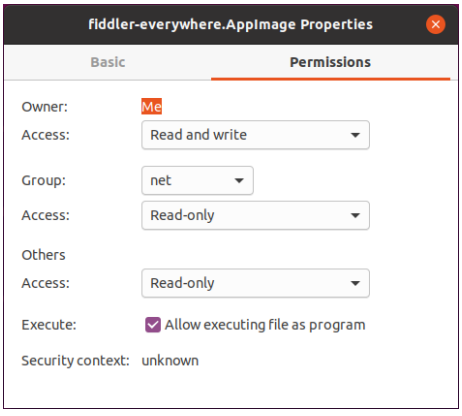

图 6-3 设置可执行权限

②双击 Fiddler Everywhere 软件包，进行运行，并登录软件，如图 6-4 所示。

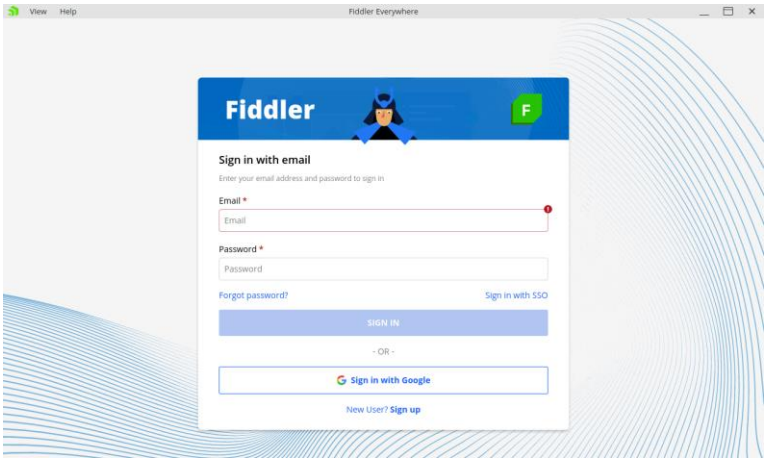

图 6-4 Fiddler Everywhere 首页

任务 3：HTTP 通信分析

步骤 01：启动 Wireshark 进行抓包

设置当前过滤为【http】，启动 Wireshark 进行抓包。

步骤 02：使用 Fiddler Everywhere 发送 HEAD 请求

点击“</> Composer”功能签，选择 HTTP 请求类型为“HEAD”，请求地址为“http://it.hactcm.edu.cn”，并点击【EXECUTE】，如图 6-5 所示。

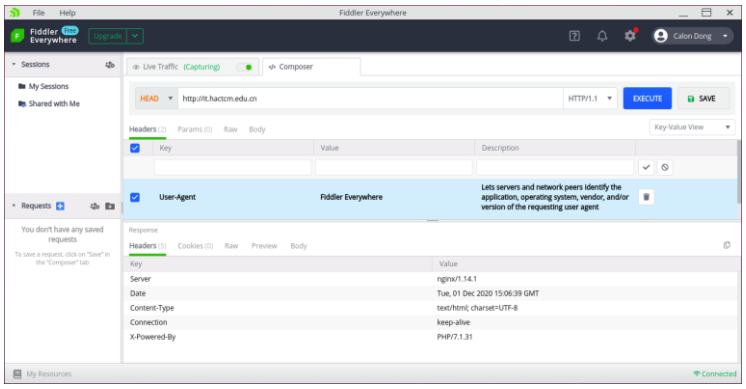

图 6-5 发送 HEAD 请求

步骤 03：通过 Fiddler Everywhere 分析 HEAD 请求与响应内容

点击“Live Traffic（Capturing）”功能签，然后点击右侧“Inspectors”功能签查看 HEAD 请求与响应内容，并填写表 6-2 和 8-3。

表 6-2 HEAD 请求内容分析

序号	Key	Value	字段表示的信息
1	User-Agent		
2	Host		

表 6-3 HEAD 响应内容分析

序号	Key	Value	字段表示的信息
1	Accept-Rangers		
2	Cache-Control		
3	Connection		
4	Content-Length		
5	Content-Type		
6	Date		
7	P3p		
8	Pragma		
9	Server		
10	Set-Cookie		
11	Strict-Transport-Security		
12	Traceid		
13	X-Ua-Compatible		

步骤 04：通过 Wireshark 分析 HEAD 通信过程

对采集的 HTTP HEAD 请求类型的通信报文进行分析，并填写表 6-4 和表 6-5。

表 6-4 HEAD 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Method		第　位		
2	Request URI		第　位		
3	Request Version		第　位		
4	User-Agent		第　位		
5	Connection		第　位		
6	Host		第　位		
7	抓取数据包的详细内容：				

表 6-5 HEAD 响应报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第　　位		
2	Status code		第　　位		
3	Response Phrase		第　　位		
4	Content-Length		第　　位		
5	Content-Type		第　　位		
6	Content-Location		第　　位		
7	Last-Modified		第　　位		
8	Accept-Ranges		第　　位		
9	ETag		第　　位		
10	Server		第　　位		
11	X-Powered-By				
12	Date				
13	Time Since Request				
14	抓取数据包的详细内容：				

步骤 05：使用 Fiddler Everywhere 发送 GET 请求

点击“</> Composer”功能签，选择 HTTP 请求类型为“GET”，请求地址为“http://it.hactcm.edu.cn”，并点击【EXECUTE】，如图 6-6 所示。

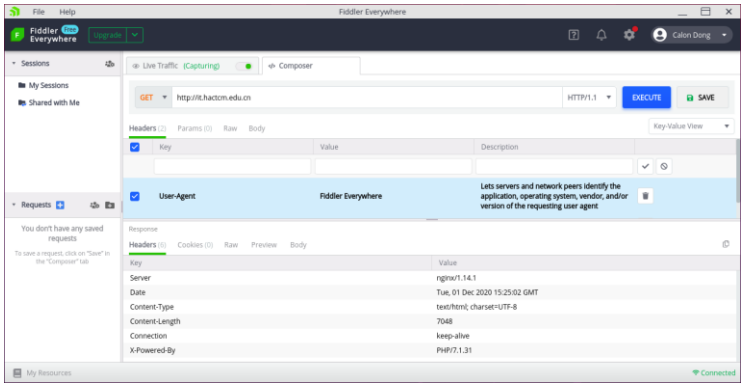

图 6-6 发送 GET 请求

步骤 06：通过 Fiddler Everywhere 分析 GET 请求与响应内容

点击“Live Traffic（Capturing）”功能签，然后点击右侧“Inspectors”功能签查看 HEAD 请求与响应内容，并填写表 6-6 和 8-7。

表 6-6 GET 请求报文分析

序号	Key	Value	字段表示的信息
1	User-Agent		
2	Host		

表 6-7 GET 响应报文分析

序号	Key	Value	字段表示的信息
1	Accept-Rangers		
2	Cache-Control		
3	Connection		
4	Content-Length		
5	Content-Type		
6	Date		
7	P3p		
8	Pragma		
9	Server		
10	Set-Cookie		
11	Strict-Transport-Security		
12	Traceid		
13	X-Ua-Compatible		

步骤 07：通过 Wireshark 分析 GET 通信分析

对采集的 HTTP GET 请求类型的通信报文进行分析，并填写表 6-8 和表 6-9。

表 6-8 GET 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Method		第　位		
2	Request URI		第　位		
3	Request Version		第　位		
4	User-Agent		第　位		
5	Connection		第　位		

6	Host		第　　位		
7	抓取数据包的详细内容：				

表 6-9 GET 响应报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第　　位		
2	Status code		第　　位		
3	Response Phrase		第　　位		
4	Content-Length		第　　位		
5	Content-Type		第　　位		
6	Content-Location		第　　位		
7	Last-Modified		第　　位		
8	Accept-Ranges		第　　位		
9	ETag		第　　位		
10	Server		第　　位		
11	X-Powered-By				
12	Date				
13	Time Since Request				
14	抓取数据包的详细内容：				

任务 4：HTTPs 通信分析

步骤 01：启动 Wireshark 进行抓包

设置当前过滤为【tls】，启动 Wireshark 进行抓包。

步骤 02：使用 Fiddler Everywhere 发送 HTTPs 请求

点击“</> Composer”功能签，选择 HTTP 请求类型为“GET”，请求地址为“https://www.hactcm.edu.cn”，并点击【EXECUTE】，如图 6-7 所示。

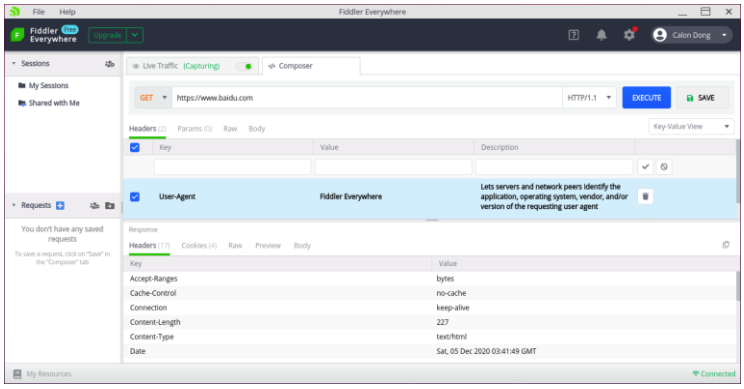

图 6-7 Fiddler Everywhere 发送 HTTPs 请求

步骤 03：通过 Fiddler Everywhere 分析 HTTPs 请求与响应内容

点击“Live Traffic（Capturing）”功能签，然后点击右侧“Inspectors”功能签查看 HTTPs 请求与响应内容，并填写表 6-10 和表 6-11。

表 6-10 HTTPs 请求内容分析

序号	Key	Value	字段表示的信息
1	User-Agent		
2	Host		

表 6-11 HTTPs 响应内容分析

序号	Key	Value	字段表示的信息
1	Accept-Rangers		
2	Cache-Control		
3	Connection		
4	Content-Length		
5	Content-Type		
6	Date		
7	P3p		
8	Pragma		
9	Server		
10	Set-Cookie		
11	Strict-Transport-Security		
12	Traceid		

13	X-Ua-Compatible		

步骤 04：通过 Wireshark 分析 HTTPs 通信过程

①Client Hello

对采集的 HTTPs Client Hello 数据包进行分析，并填写表 6-12。

表 6-12 Client Hello **报文分析**

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	Handshake Protocol Length		
7	Handshake Protocol Version		
8	Random GMT Unix Time		
9	Random Random Bytes		
10	Session ID Length		
11	Cipher Suites Length		
12	Compression Methods Length		
13	Extensions Length		
14	Extension		
15	抓取数据包的详细内容：		

②Server Hello

对采集的 HTTPs Server Hello 数据包进行分析，并填写表 6-13。

表 6-13 Server Hello 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		

3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	Handshake Protocol Length		
7	Handshake Protocol Version		
8	Random GMT Unix Time		
9	Random Random Bytes		
10	Session ID Length		
11	Session ID		
12	Cipher Suite		
13	Compression Methods		
14	Extensions Length		
15	Extension		
16	抓取数据包的详细内容：		

③Certificate

对采集的 HTTPs Certificate 数据包进行分析，并填写表 6-14。

表 6-14 Certificate 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	Handshake Protocol Length		
7	Certificates Length		
8	Certificate		
9	signedCertificate		
10	Certificate version		
11	Certificate serialNumber		

12	Certificate signature		
13	Certificate issuer		
14	Certificate issuer		
15	Certificate issuer rdnSequence		
16	Certificate validity notBefore		
17	Certificate validity notAfter		
18	Certificate subject rdnSequence		
19	Certificate subjectPublicKeyInfo		
20	Certificate subjectPublicKeyInfo Padding		
21	Certificate subjectPublicKeyInfo subjectPublicKey		
22	Certificate extensions		
23	Certificate algorithmIdentifier		
24	Certificate Padding		
25	Certificate encrypted		
26	抓取数据包的详细内容：		

④Server Key Exchange

对采集的 HTTPs Server Key Exchange 数据包进行分析，并填写表 6-15。

表 6-15 Server Key Exchange 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	Handshake Protocol Length		
7	EC Diffie-Hellman Server		

	Params		
8	Curve Type		
9	Named Curve		
10	Pubkey Length		
11	Pubkey		
12	Signature Hash Algorithm		
13	Signature Hash Algorithm Hash		
14	Signature Hash Algorithm Signature		
15	Signature Length		
16	Signature		
17	抓取数据包的详细内容：		

⑤Server Hello Done

对采集的 HTTPs Server Hello Done 数据包进行分析，并填写表 6-16。

表 6-16 Server Hello Done 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	Handshake Protocol Length		
7	抓取数据包的详细内容：		

⑥Client Key Exchange

对采集的 HTTPs Client Key Exchange 数据包进行分析，并填写表 6-17。

表 6-17 Client Key Exchange 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	Handshake Protocol Length		
7	EC Diffie-Hellman Client Params		
8	Pubkey Length		
9	Pubkey		
10	抓取数据包的详细内容：		

Change Cipher Spec（Client），对采集的 HTTPs Change Cipher Spec（Client）数据包进行分析，并填写表 6-18。

表 6-18 Change Cipher Spec（Client）报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Change Cipher Spec		

5	抓取数据包的详细内容：

Encrypted Handshake Message，对采集的 HTTPs Encrypted Handshake Message 数据包进行分析，并填写表 6-19。

表 6-19 Encrypted Handshake Message 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	抓取数据包的详细内容：		

⑦New Session Ticket

对采集的 HTTPs New Session Ticket 数据包进行分析，并填写表 6-20。

表 6-20 New Session Ticket 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	Handshake Type		
6	TLS Session Ticket		
7	Session Ticket Lifetime Hint		
8	Session Ticket Length		

9	Session Ticket		
10	抓取数据包的详细内容：		

⑧Change Cipher Spec（Server）

对采集的 HTTPs Change Cipher Spec 数据包进行分析，并填写表 6-21。

表 6-21 Change Cipher Spec 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Change Cipher Spec		
5	抓取数据包的详细内容：		

Encrypted Handshake Message，对采集的 HTTPs Encrypted Handshake Message 数据包进行分析，并填写表 6-22。

表 6-22 Encrypted Handshake Message 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Handshake Protocol		
5	抓取数据包的详细内容：		

⑨Application Data

对采集的 HTTPs Application Data 数据包进行分析，并填写表 6-23。

表 6-23 Application Data 报文分析

序号	Key	Value	字段表示的信息
1	Content Type		
2	Version		
3	Length		
4	Encrypted Application Data		
5	抓取数据包的详细内容：		

七、实验考核

1、任务说明

使用 Wireshark 分析 HTTP 报文结构；

使用 Fiddler Eveywhere 分析 HTTP 通信过程。

2、任务要求

要求 1：使用 Wireshark 完成 HTTP 报文分析；

要求 2：完成 Fiddler Everywhere 安装；

要求 3：完成 HTTP 通信分析；

要求 4：完成 HTTPs 通信分析。

3、考核要求

题目 1：使用 Wireshark 分析课程网站“http://network.xg.hactcm.edu.cn”的 HTTP 报文结构，请提交【HTTP 报文数据】截图。

题目 2：分析【HTTP 报文数据】，请填写一下信息。

字段 HTTP Host 的字段长度：_____，起始位置：第_____位，字段值：_____，字段表示的信息：_____。

题目 3：通过 Fiddler Everywhere 分析课程网站“http://network.xg.hactcm.edu.cn”的 HEAD 请求与响应内容，请提交【Live Traffic-{HEAD 请求}-Overview】截图。

题目 4：通过 Wireshark 分析课程网站“http://network.xg.hactcm.edu.cn”的 HEAD 通信过程，查看 HEAD 的请求报文、响应报文，请提交【请求报文结构】、【响应报文结构】截图 2 张。

题目 5：分析课程网站“http://network.xg.hactcm.edu.cn”的 HEAD 通信过程中的【响应报文数据】，请填写以下信息。

字段 Status Code 的字段长度：_____，起始位置：第_____位，字段值：_____，字段表示的信息：_____。

字段 Content-Type 的字段长度：_____，起始位置：第_____位，字段值：_____，字段表示的信息：_____。

题目 6：通过 Wireshark 分析河南中医药大学“https://www.hactcm.edu.cn”的请求与响应内容，请提交【HTTPS 通信过程报文】截图。

题目 7：分析访问河南中医药大学“https://www.edu.cn”的通信过程，请填写以下信息。

HTTPs Client Hello 数据包的字段 Content Type 的字段长度：_____，起始位置：第_____位，字段值：_____，字段表示的信息：_____。

HTTPs Server Hello Done 数据包字段 Handshake Type 的字段长度：_____，起始位置：第_____位，字段值：_____，字段表示的信息：_____。