# 实验八: HTTP 协议分析

#### 一、实验目的

- 1、理解 HTTP 协议的基本内容;
- 2、理解 HTTP 协议的通信过程。

# 二、实验学时

2 学时

## 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。

#### 2、软件

Windows 7 以上操作系统,安装 Wireshark 网络嗅探软件,安装 HTTP 协议调试代理工具 Fiddler。

#### 3、网络

实验室局域网支持,能够访问校园网,能够访问互联网。

#### 4、工具

无。

## 五、实验理论

- 1、HTTP协议的基本原理;
- 2、HTTP协议的通信过程。

## 六、实验任务

- 1、完成 HTTP 协议报文的采集;
- 2、完成 HTTP 协议报文结构的分析;
- 3、完成 HTTP 协议不同请求类型的数据报文分析。

## 七、实验内容及步骤

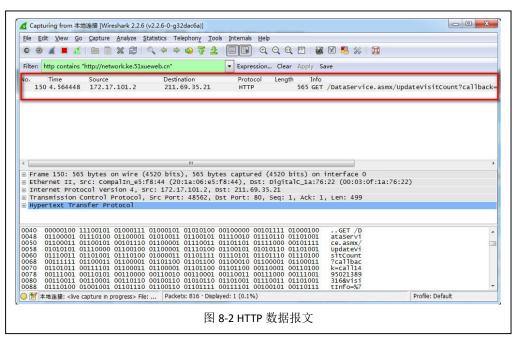
#### 1、HTTP 数据包分析

(1) 获取数据报文

①打开 Wireshark, 在【Filter】选项中输入报文过滤条件"http://network.ke.51xueweb.cn",选择【Start】,开始进行报文采集,如图 8-1 所示。



- ②打开浏览器,在地址栏中输入"http://network.ke.51xueweb.cn",进行网页访问。
- ③在 Wireshark 的抓包窗体中,查看已获取的 HTTP 协议的数据报文,如图 8-2 所



示。

(2) 数据报文分析

对获取到的 HTTP 协议报文内容进行详细分析,并填写表 8-1。

表 8-1 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	
	抓取数据包的详细内容:		
14			

## 2、不同类型的 HTTP 数据包分析

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

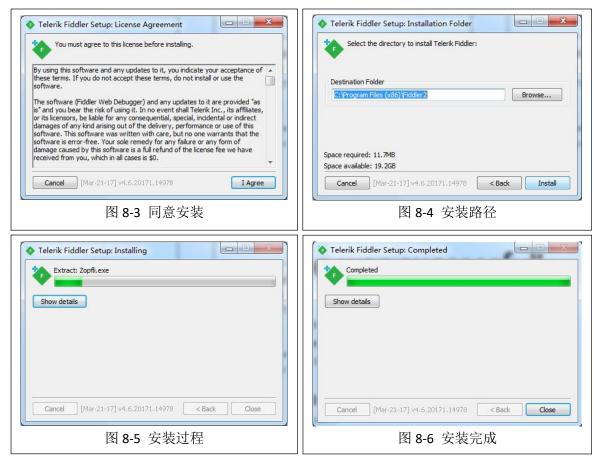
- (1) Fiddler 安装与使用
- ①下载安装包

可通过官方网站(http://www.telerik.com/fiddler)获得 Fiddler 软件安装程序;

可通过本课程网站(http://network.ke.51xueweb.cn)下载本教程所使用的软件版本。

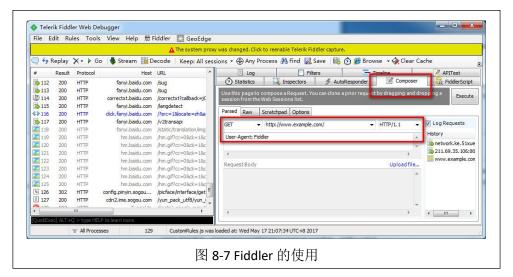
#### ②安装软件

- a、双击 Fiddler 安装程序,进入如图 8-3 所示的 Fiddler 安装界面,点击【I Agree】 进行安装。
  - b、用户可使用默认的 Fiddler 安装目录,也可自行修改默认路径,如图 8-4 所示。
  - c、Fiddler 软件安装过程,如图 8-5 所示,安装完成后如图 8-6 所示。



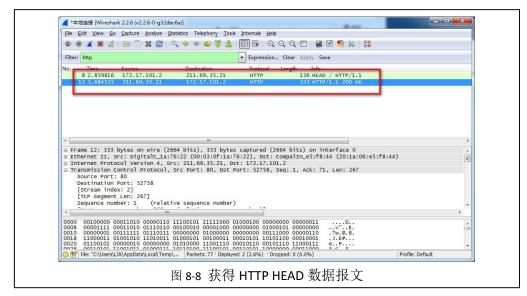
③软件使用

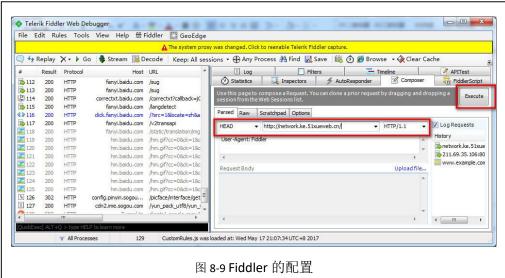
打开软件,在右侧的操作栏目中选择【Composer】,选择HTTP请求类型和访问地址,实现本地发送不同类型的HTTP协议包操作,如图 8-7 所示。



- (2) HEAD 数据报文分析
- ①获取 HTTP Head 数据报文。
- a、打开 Wireshark,在【Filter】选项中输入报文过滤条件"<u>http</u>",选择【Start】, 开始进行报文采集,如图 8-8 所示。
  - b、打开 Fiddler, 在类型处选择【HEAD】类型,并输入"http://network.ke.51xueweb.cn",

#### 点击【Execute】开始执行,如图 8-9 所示。





#### ②数据报文分析。

对采集的 HTTP HEAD 协议报文进行详细分析,并填写表 8-2 和表 8-3。

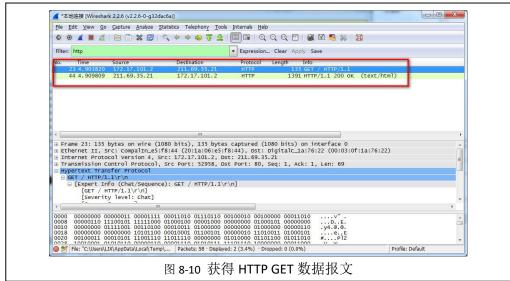
序号 字段名称 字段长度 起始位置 字段值 字段表示的信息 第 1 Request Method 位 2 Request URI 第 位 3 第 位 Request Version 4 第 位 User-Agent 5 第 Connection 位 第 6 Host 位 抓取数据包的详细内容: 7

表 8-2 HEAD 请求报文分析

#### 表 8-3 HEAD 响应报文分析

表 8-3 HEAD 啊应我又分析							
序号	字段名称	字段长度	起始位置	<b>E</b> .	字段值	字段表示的信息	
1	Request Version		第	<u>ì</u>			
2	Status code		第	<u>ì</u>			
3	Response Phrase		第	立			
4	Content-Length		第	立			
5	Content-Type		第	立			
6	Content-Location		第	立			
7	Last-Modified		第	<u>जे</u>			
8	Accept-Ranges		第	<u>जें</u>			
9	ETag		第	<u>ù</u>			
10	Server		第	<u>ù</u>			
11	X-Powered-By						
12	Date						
13	Time Since Request						
	抓取数据包的详细内	]容:			•		
14							

- (3) GET 数据报文分析
- ①获取 HTTP GET 数据报文。
- a、打开 Wireshark,在【Filter】选项中输入报文过滤条件"<u>http</u>",选择【Start】, 开始进行报文采集。如图 8-10 所示。
- b、打开 Fiddler 软件, 在类型处选择【GET】类型, 并输入 "http://network.ke.51xueweb.cn", 点击【Execute】开始执行, 如图 8-11 所示。



Telerik Fiddler Web Debugger

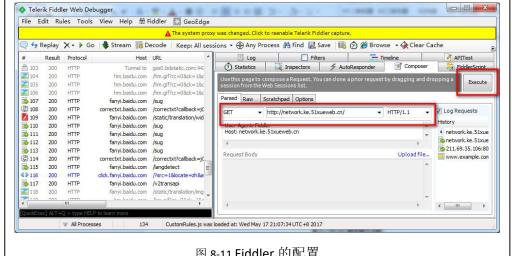


图 8-11 Fiddler 的配置

#### ②数据报文分析。

对采集的 HTTP GET 协议报文进行详细分析,并填写表 8-4 和表 8-5。

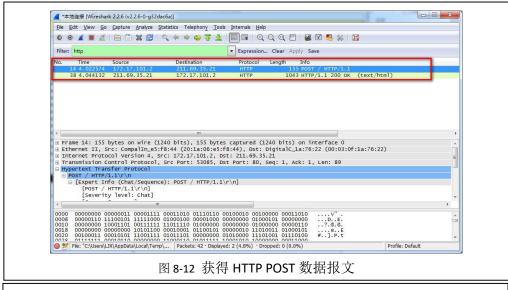
序号 字段名称 字段长度 起始位置 字段值 字段表示的信息 第 1 Request Method 位 2 Request URI 第 位 3 Request Version 第 位 4 User-Agent 第 位 5 Connection 第 位 第 6 Host 位 7 抓取数据包的详细内容:

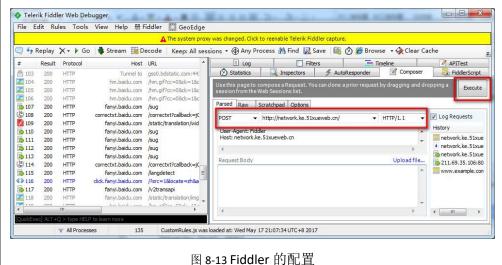
表 8-4 GET 请求报文分析

#### 表 8-5 GET 响应报文分析

表 8-5 GET 响应报文分析							
序号	字段名称	字段长度	起始位置	Ī	字段值	字段表示的信息	
1	Request Version		第  位	江			
2	Status code		第  位	江			
3	Response Phrase		第  位	江			
4	Content-Length		第  位	江			
5	Content-Type		第  位	江			
6	Content-Location		第  位	江			
7	Last-Modified		第  位	江			
8	Accept-Ranges		第  位	江			
9	ETag		第  位	江			
10	Server		第  位	江			
11	X-Powered-By						
12	Date						
13	Time Since Request						
	抓取数据包的详细内	]容:		•	<u>.</u>		
14							

- (4) POST 数据报文分析
- ①获取 HTTP POST 数据报文。
- a、打开 Wireshark,在【Filter】选项中输入报文过滤条件"<u>http</u>",选择【Start】, 开始进行报文采集,如图 8-12 所示。
- b、打开 Fiddler,在类型处选择【POST】类型,并输入"http://network.ke.51xueweb.cn", 点击【Execute】开始执行,如图 8-13 所示。





\_\_\_\_\_

#### ②数据报文分析。

对采集的 HTTP POST 协议报文进行详细分析,并填写表 8-6 和表 8-7。

表 8-6 POST 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 8-7 POST 响应报文分析								
字段名称	字段长度	起始位置	字段值	字段表示的信息				
Request Version		第 位						
Status code		第 位						
Response Phrase		第 位						
Content-Length		第 位						
Content-Type		第 位						
Content-Location		第 位						
Last-Modified		第 位						
Accept-Ranges		第 位						
ETag		第 位						
Server		第 位						
X-Powered-By								
Date								
Time Since Request								
抓取数据包的详细内	容:		<u> </u>					
	Request Version  Status code  Response Phrase  Content-Length  Content-Type  Content-Location  Last-Modified  Accept-Ranges  ETag  Server  X-Powered-By  Date  Time Since Request	字段名称 字段长度 Request Version Status code Response Phrase Content-Length Content-Type Content-Location Last-Modified Accept-Ranges ETag Server X-Powered-By Date	字段名称       字段长度       起始位置         Request Version       第 位         Status code       第 位         Response Phrase       第 位         Content-Length       第 位         Content-Type       第 位         Content-Location       第 位         Last-Modified       第 位         Accept-Ranges       第 位         ETag       第 位         Server       第 位         X-Powered-By       Date         Time Since Request       Time Since Request	字段名称     字段长度     起始位置     字段值       Request Version     第 位        Status code     第 位        Response Phrase     第 位        Content-Length     第 位        Content-Type     第 位        Content-Location     第 位        Last-Modified     第 位        Accept-Ranges     第 位        ETag     第 位        Server     第 位        X-Powered-By         Date     Time Since Request				

# 八、实验分析

## 1、HTTP 报文分析

- (1) HTTP 请求报文有哪些字段,主要作用是什么?
- (2) HTTP 响应报文有哪些字段,主要作用是什么?

## 2、HTTP 请求

- (1) 通过 HTTP 使用浏览器访问网站时,浏览器是否只向目的主机发送一次 HTTP 请求?如何查看这些请求?
  - (2) Fiddler 软件的工作原理是什么? 主要应用场景有哪些?