1

《计算机网络》实验指导

# 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

综合性

## 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"<u>http contains</u> <u>"http://network.ke.51xueweb.cn</u>",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。

<u>ile E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> t	atistics Telephony <u>T</u> ools	Internals <u>H</u> elp				
0 0 🖌 🗖 🔬   🖻 🗎 🗙 😂   (	2、 ⇔ ⇔ ⊕ 7 ⊈		🖸   🌌 🕻	Y 🥵 💥   🛱		
Filter: http contains "http://network.ke.51xue	web.cn*	Expression Clear	Apply Sav	e		
o. Time Source 150 4.564448 172.17.101.2	Destination 211.69.35.21	Protocol Length HTTP	Info 565 GET /	/DataService.a	usmx/UpdateVisit	count?callback
Frame 150: 565 bytes on wire (4	" 520 bits), 565 byte	s captured (4520 bi	ts) on ir	nterface 0		
Frame 150: 565 bytes on wire (4 Ethernet II, Src: CompalIn_ESif Internet Protocol Version 4. Sr	"" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, ps	s captured (4520 bi 8:44), Dst: Digital t: 211.69.35.21	ts) on ir C_1a:76:2	nterface 0 22 (00:03:0f:1	a:76:22)	
Frame 150: 565 bytes on wire (4 Ethernet II, src: compalin_e5:f Internet Protocol version 4, sr Transmission Control Protocol,	"" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, Ds Src Port: 48562, Ds	s captured (4520 bi 8:44), Dst: Digital t: 211.69.35.21 t Port: 80, Seq: 1,	ts) on ir C_1a:76:2 Ack: 1,	nterface 0 22 (00:03:0f:1 Len: 499	a:76:22)	
Frame 150: 565 bytes on wire (4 Ethernet II, src: CompalIn_e5:f Internet Protocol Version 4, Sr Transmission Control Protocol Hypertext Transfer Protocol	III 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, Ds Src Port: 48562, Ds	es captured (4520 bi 8:44), Dst: Digital 1: 211.69.35.21 t Port: 80, Seq: 1,	ts) on ir C_1a:76:2 Ack: 1,	nterface 0 22 (00:03:0f:1 Len: 499	.a:76:22)	
Frame 150: 565 bytes on wire (4 Ethernet II, src: CompalIn_e5:f Internet Protocol version 4, sr Transmission Control Protocol Hypertext Transfer Protocol	" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172:17.101.2, bs Src Port: 48562, bs	s captured (4520 bi 8:44), Dst: Digital 1: 211.69.35.21 t Port: 80, Seq: 1,	ts) on ir C_1a:76:2 Ack: 1,	nterface 0 22 (00:03:0f:1 Len: 499	a:76:22)	
Frame 150: 565 bytes on wire (4 Ethernet II, src: compalIn_e5:f Internet Protocol Version 4, Sr Transmission Control Protocol Hypertext Transfer Protocol	"" 520 bits), 565 byte 8:44 (20:1a:06:e5:16 c: 172,17.101.2, ps Src Port: 48562, ps 01000101 01010100 0 0100011 0101010 0	s captured (4520 bi 8:44), Dst: Digital t: 211.69.35.21 t Port: 80, Seq: 1, 0100000 00101111 01 1110010 01110110 01	ts) on ir c_1a:76:2 Ack: 1, 000100 101001	nterface 0 22 (00:03:0f:1 Len: 499 GET /D ataServi	.a:76:22)	
Frame 150: 565 bytes on wire (4 Ethernet II, Src: Compalin_e5:f Internet Protocol Version 4, 57 Transmission Control Protocol, Hypertext Transfer Protocol 040 00000100 1110010 01000011 048 01100001 0110010 0100001	" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, bs Src Port: 48562, bs 01000101 01010100 0 01010011 01100100 0 01100001 01110011 0	s captured (4520 bi 8:44), DST: Digital t: 211.69.35.21 t Port: 80, Seq: 1, 0100000 00101111 01 1110010 011011100 01 1110010 01111000 01	ts) on ir c_1a:76:2 Ack: 1, 000100 101001 101101	nterface 0 22 (00:03:0f:1 Len: 499 GET /D ataServ1 ce.asmx/	.a:76:22)	
Frame 150: 565 bytes on wire (4           Ethernet II, Src: CompalIn_e5:f           Internet Protocol Version 4, Sr           Transmission control Protocol,           Hypertext Transfer Protocol           040         00000100 1110010 1000011           048         01100001 1010010 00100001           050         01100101 0110100 001100101           050         01100101 0110100 01100100           050         01101011 0110100 0110100	"" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, bs Src Port: 48562, bs 010000101 010101010 01010001 01100110 01100001 011100110 01000001 011001110	<pre>is captured (4520 bi 8:44), Dst: Digital t: 211.69.35.21 t Port: 80, Seq: 1, 0100000 00101111 01 1110010 0110110 01 110010 01011000 0 1100101 0101100 01 110101 01101110 0</pre>	ts) on ir C_1a:76:2 Ack: 1, 000100 101001 101111 101001 110100	GET /D ataServi updatevi sitCount	.a:76:22)	
Frame 150: 565 bytes on wire (4           Ethernet II, Src: CompalIn_e5:f           Internet Protocol Version 4, Sr           Transmission Control Protocol,           Hypertext Transfer Protocol           040 00000100 1110010 01000011           048 01100010 0110010 01000011           058 010101 01110000 0110010           058 010101 01110000 0110100           068 0011111 010001 0110010           068 0011111 0110001 0110010	"" 520 bits), 565 byte 8:44 (20:1a:06:e5:16 c: 172.17.101.2, ps Src Port: 48562, ps 01000110 01010100 0 01010001 01100101 0 01100001 01110110 01100001 01110110 01000001 01101101 0 01000001 01101100	s captured (4520 bi 8:44), Dst: Digital t: 211.69.35.21 t Port: 80, Seq: 1, 0100000 00101111 01 110101 01110100 00 1100101 01101010 01 1100101 01101110 01 1100010 01100001 01 1100010 01100001	ts) on ir c_1a:76:2 Ack: 1, 000100 101001 101011 101001 110100 100011	GET /D ataServi ce.asmx/ Updatevi SitCount SitCount	.a:76:22)	
Frame 150: 565 bytes on wire (4           Ethernet II, Src: CompalIn_e5:f           Internet Protocol Version 4, 57           Transmission Control Protocol,           Hypertext Transfer Protocol           040         00000100           040         0100001           040         0100001           040         0100001           041         01100101           048         0101001           040         0100011           041         0110001           048         0101011           048         0110101           048         0111010           068         0111111           068         0110101           07         0110101           078         0110101           078         0110101	"" 520 bits), 565 byte 8:44 (20:1a:06:e5;f c: 172.17.101.2, Ds 5rc Port: 48562, Ds 01000101 0100101 0 01010001 01100101 0 01000001 01101010 0 01000001 01101100 0 00100100 0011001100 0	s captured (4520 bi 8:44), DST: Digital t: 211.69.35.21 t Port: 80, Seq: 1, 110010 0111011 01 1101101 0111010 0 1100110 01101110 01 1100101 0110110 01 1100100 001100001 00 0110011 00110000 00	ts) on ir c_la:76:2 Ack: 1, 000100 101001 101011 101001 110100 110100 111000		.a:76:22)	
Frame 150: 565 bytes on wire (4           Ethernet II, Src: CompalIn_e5:f           Internet Protocol Version 4, Sr           Transmission Control Protocol,           Hypertext Transfer Protocol           040 00000100 1110010 01000011           050 01100101 0100011           050 01100101 0110100           050 01100101 0110100           050 0110011 0110100           050 0110011 0110100           050 0111011 0110000           060 0111011 01100001           070 0101011 00110110           080 0011011 00110101           080 0011011 00110101           080 0011011 00110101           080 0011011 00110101           080 00110011 0011010	" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, bs Src Port: 48562, bs 01000010 1010010 0 0100001 01100110 01100001 01100110 01100001 01100110 01101000 01101110 01101000 01100110 0010010 0110010	s captured (4520 bi 8:44), DST: Digital t: 211.69,35.21 t Port: 80, Seq: 1, 0100000 00101111 01 1110010 01110100 01 1100101 01011001 01 1100101 0110011 01 1100100 0110010 01 0110011 00110010 01 0110011 00110001 01	ts) on ir c_la:76:2 Ack: 1, 000100 101001 101001 101001 110001 111000 101001 101001	GET /D ataServi ce.asmx/ updatevi sitCount %callbat %callbat %502184 31664/157	.a:76:22)	
Frame 150: 565 bytes on wire (4         Ethernet II, Src: compalIn_e5:f         Internet Protocol Version 4, Sr         Transmission Control Protocol,         Hypertext Transfer Protocol         040 00000100 1110010 01000011         043 0100001 0110100 01000011         050 01100101 0110100 01100001         050 01100101 01101000 01100100         060 0111011 01101001 01101000         070 0110101 01101001 01101000         080 0011011 00110110 0110010         080 0011001 0011010 010000         080 0011001 0011010 00110100         080 0111010 0011010 00110100         080 0111010 0011010 00110100         080 0111010 001100100101011000         080 0111010 001100100101010000         080 0111010 0011010000         080 0111010 0011010000         080 01110100 00110010000         080 0110100 001100100000         080 0110100 00110010000000         080 01101000 00100000000000000000000000	" 520 bits), 565 byte 8:44 (20:1a:06:e5:f c: 172.17.101.2, bs Src Port: 48562, bs 0100001 01100110 0 01100001 01100110 01100001 01100110 0110100 01100110 0110100 01100110 01101001 0110110 0010010 01100110 01100110 0110011 01100110 0110011 01100110 0110011 01100110 01101110 01100110 01101110	s captured (4520 bi 8:44), pst: Digital t: 211.69.35.21 t Port: 80, Seq: 1, 0100000 00101111 01 1110010 01110110 01 1100101 010110110 01 1100101 0110010 01 1100100 0110010 00 0110011 00110010 00 0110011 00110001 00 et: 1 (0.1%6)	ts) on ir C_la:76:2 Ack: 1, 0000100 101101 101001 110001 110001 111000 111001 111001	GET /D ataServi ce.asmx/ Updatevi sitCount %calibat Socials SitCount %calibat Socials SitCount %calibat socials SitCount %calibat sitCou	a:76:22) Profile: De	fault

(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约	<b>容</b> :			·		
14							
17							

#### 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。

🔷 Telerik Fiddler Setup: License Agreement	Telerik Fiddler Setup: Installation Folder
You must agree to this license before installing.	Select the directory to install Telerik Fiddler:
By using this software and any updates to it, you indicate your acceptance of these terms. If you do not accept these terms, do not install or use the software. The software (Fiddler Web Debugger) and any updates to it are provided "as is" and you bear the risk of using it. In no event shall Telerik Inc., its affiliates, or its licensors, be liable for any consequential, special, incidental or indirect damages of any kind arising out of the delivery, performance or use of this	Destination Folder C: Program Files (x86) Filddler2 Browse
software. This software was written with care, but no one warrants that the software is error-free. Your sole remedy for any failure or any form of damage caused by this software is a full refund of the license fee we have received from you, which in all cases is \$0.	Space required: 11.7MB Space available: 19.2GB
图 8-3 同意安装	图 8-4 安装路径
🔷 Telerik Fiddler Setup: Installing	Telerik Fiddler Setup: Completed
Extract: Zopfil.exe	Completed
Show details	Show details
Cancel [Mar-21-17] v4.6.20171,14978 < Back Close	Cancel [Mar-21-17] v4.6.20171.14978 < Back Close
图 8-5 安装过程	图 8-6 安装完成

#### 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。

	Replay Result	X → Ire Go Protocol	) 🔹 Stream 🔛 D Host	ecode Keep: All sess	ions ▼ ⊕ Any Process ∰ Find I Save   I to ⑦ @ Browse ▼ ∳ Clear Cache I Log I Fitters I Totelina	e a a a a a a a a a a a a a a a a a a a
2 112	200	HTTP	fanyi.baidu.com	/sug	② Statistics Inspectors AutoResponder Composer	FiddlerScript
113	200	HTTP	fanyi.baidu.com	/sug	Use this page to compose a Request. You can done a prior requires the dragging and dropp	10 a
(n) 114	200	HTTP	correctxt.baidu.com	/correctxt?calback=jC	session from the Web Sessions list.	Execute
3 115	200	HTTP	fanyi.baidu.com	/langdetect	Presed P. La H. La K	
\$\$116	200	HTTP	dick.fanyi.baidu.com	/?src=18locate=zh&a	raiseu Raw Scratchpad Uptions	
20 117	200	HTTP	fanyi.baidu.com	/v2transapi	GET v http://www.example.com/ v HTTP/1.1 v	Log Requests
118	200	HTTP	fanyi.baidu.com	/static/translation/img		listory
119	200	HTTP	hm.baidu.com	/hm.gif?cc=0&ck=1&c	User-Agent: Fiddler	natural la Etura
120	200	HTTP	hm.baidu.com	/hm.gif?cc=0&ck=1&c		211 60 2E 106/90
121	200	HTTP	hm.baidu.com	/hm.gif?cc=08ck=18c	4 F	211.09.33.100.00
122	200	HTTP	hm.baidu.com	/hm.gif?cc=08ck=18c	Request Body Upload file	www.example.com
123	200	нпр	hm.baidu.com	/hm.git?cc=0&ck=1&c	*	
124	200	HTTP	hm.baidu.com	/hm.git?cc=0&ck=1&c		
125	200	HUB	hm.baidu.com	/hm.git/cc=0&ck=1&c		
120	302	HITTP	conng.pinyin.sogou	/picrace/interface/get		
12/	200	LITTE I	curiz.ime.sogou.com	/yun_pack_utts/yun_i	v.	
1		m		•	4	
QuickExe	ec] ALT+0	Q > type HEL	P to learn more			
	1	- All Proces	ses 129	CustomRules is was	oaded at: Wed May 17 21:07:34 LTC +8 2017	
		e Airrioces	363 123	Customicules.js was	baded at, weathay 17 21.07.04 010 40 2017	41

(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。

No.         Time         Senset         Deptivation         Deptivation         Infe           8 2.859816         172.17.101.2         211.69.35.21         HTTP         136 HEAD / HTTP/1.1           1 2.9.064525         211.69.35.21         HTTP         136 HEAD / HTTP/1.1           2 33.HTTP/1.1         200.06         172.17.101.2         172.17.101.2           # Frame 12: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface 0         +           # Ethernet 11, Src: DigitalC_la:76:22 (00:03:0f:1a:76:22), 0st: Complia.         +           # Internet Protocol Version 4, Src: 211.69.35.21, 0st: 127.17.101.2         #           # Transmission Control Protocol, Src Port: 80, 0st Port: 32758, Seq: 1, Ack: 71, Len: 267         #           Destration Nr: 21         If relative sequence number)         *           *         *         *           #         *         *           #         *         *           #         *         *           #         *         *           #         *         *	
8 2.859816       172.17.101.2       211.69.35.21       HTTP       136 HEAD / HTTP/1.1         12 3.684525       211.69.35.21       172.17.101.2       HTTP       333 HTTP/1.1 200 ok         ************************************	
Image: Construction of the second of the	
<pre></pre>	
Construction         Construction<	
0000 00100000 0001101 01100101 1111000 0100010 000000	
00/26 10/00/17 01/00/010 10/00/01 00/00/17 00/00/17 00/01/00 00/00/01 .5.FF 00/20 01/00/11 00/00/00 01/01/00/01 10/01/10 00/01/10 01/00/011 01/00/011 .5.FF 0. ₩ File: "C\Uses(LX)AppDatalLocation=Termp\ Packets 77 0 splayed: (2,6%) 10/00/01 .5.FF • Profile: Default	
ile Edit Rules Tools View Help 册 Fiddler 認 GeoEdge	
The system proxy was changed. Click to reenable Telerik Fiddler capture.	
🛕 The system proxy was changed. Click to reenable Telerik Fiddler capture. ) 🍫 Replay 🗙 + 🕨 Go   🔹 Stream 🎬 Decode   Keep: All sessions + 🕀 Any Process 🏦 Find 🛃 Save   🎼 📀 🏈 Browse - 🕀 Clear Cache	
A The system proxy was changed. Click to reenable Telenk Fiddler capture. → Replay X + I Go I Stream  Decode Keep: All sessions + ⊕ Any Process A Find S Save I ③ Ø Ø Browse + @ Clear Cache Result Protocol Host URL I I Log I Fitters Timeline Ø APT	Пest
A The system proxy was changed. Click to reenable Telerik Fiddler capture.	ITest ddlerScrip
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.	ITest iddlerScrip
A The system proxy was changed. Click to reenable Telerik Fiddler capture.      A Replay X + ▶ Go ♣ Stream ﷺ Decode Keep: All sessions + ⊕ Any Process क़ Find    Save	ITest iddlerScrip
A The system proxy was changed. Click to reenable Telerik Fiddler capture.	TTest iddlerScrip Execut
A The system proxy was changed. Click to reenable Telerik Fiddler capture.	ITest iddlerScrip Execut
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.	ITest iddlerScrip Execut quests
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ● Statistics       ▲ These translation (mg CorrectsticalBack=)C         ■ The system proxy was changed. Click to reenable Telerik Fiddler       ● Statistics       ▲ These translation (mg CorrectsticalBack=)C       ● Statistics       ▲ These translation (mg CorrectsticalBack=)C       ● These translation (mg CorrectsticalBack=)C <td>ITest iddlerScrip Execut quests</td>	ITest iddlerScrip Execut quests
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ● Any Process A find S ave       ③ Ø Ø Browse • ♦ Clear Cache         Result       Protocol       Host URL         112       CorrectX-tablad.com       /sug         113       CorrectX-tablad.com       /sug         114       CorrectX-tablad.com       /sug         115       CorrectX-tablad.com       /sug         116       CorrectX-tablad.com       /sug       Parsed       Raw       Scratchpad       Options         118       Other Mark du.com       /static/tarnsidor.mg       /static/tarnsidor.mg       HEAD       http://network.ke.51xueweb.cn/       HTTP/1.1       User Agent: Tiddler         120       200       HTTP       Im.baddu.com       /mm.gfrcc=0ack=18c       Itsec/4aset: 18c       State/4aset: 18c       Itsec/4aset: 18c         120       Dott       Im.baddu.com       /mm.gfrcc=0ack=18c       Itsec/4aset: 18c       Itsec/4aset: 18c       Itsec/4aset: 18c         120       200       HTTP       Im.baddu.com       /mm.gfrcc=0ack=18c       Itsec/4aset: 18c       Itsec/4aset: 18c         121       200       HTTP       Im.baddu.com       /mm.gfrcc=0ack=18c       Itsec	ITest iddlerScrip Execut quests rk.ke.51xi
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ● Go	ITest iddlerScrip Execut :quests rk.ke.51x 9.35.106:
▲ The system proxy was changed. Click to reenable Telenk Fiddler capture.         ● Any Process A Find S Save III Source       Image: Save IIII Source       Image: Save IIII Source <td>TTest iddlerScrip Execut :quests rk.ke.51xi 9.35.106:: example.c</td>	TTest iddlerScrip Execut :quests rk.ke.51xi 9.35.106:: example.c
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ● Any Process A Find S Save B O E Stream Telerik Fiddler capture.         Its       200       HTTP       fanyl.baldu.com /sug fanyl.baldu.com /sug 114       Protecol       Fitters       Timeline       APT         112       200       HTTP       fanyl.baldu.com /sug fanyl.baldu.com /rarce18locate=zh&a       Image Statistics	ITest iddlerScrip Execut quests rk.ke.51xx 3.35.106; example.c
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ● Any Process A Find  Save 100 Process         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler         ■ The system proxy was changed. Click to reenable Telerik Fiddler <t< td=""><td>ITest iddlerScrip Execut quests rk.ke.51xi 9.35.106: example.c</td></t<>	ITest iddlerScrip Execut quests rk.ke.51xi 9.35.106: example.c
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.         ◆ Replay × • © G       Stream III Decode       Keep: All sessions • ⊕ Any Process All Find III Save III So @ Browse • @ Clear Cache         Result       Protocol       Host URL       III Log       Filters       Timeline       APT         112       200       HTTP       fanyi.baidu.com /sug       Statistics       Inspectors       A LutResponder       © Composer       III doe         113       200       HTTP       fanyi.baidu.com /sug       Statistics       Inspectors       A LutResponder       © Composer       III doe         114       200       HTTP       fanyi.baidu.com /arug drecht/calladk.rg(       Inspectors       A LutResponder       © Composer       III doe         116       200       HTTP       fanyi.baidu.com //2transapi       IIII       Pareed Raw Scratchpad Options       IIIII iIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	ITest iddlerScrip Execut quests rk.ke.51xt 9.35.106: example.c
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.            ◆ Replay         ×          ◆ Go             • Participation	Trest iddlerScrip Execut :quests rk.ke.51xx 9.35.106; example.c
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.	ITest iddlerScrip Execut :quests rk.ke.51xx 9.35.106; example.c
▲ The system proxy was changed. Click to reenable Telerik Fiddler capture.	TTest iddlerScrip Execut :quests rk.ke.51xd 9.35.106: example.c

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。

表 8-2 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		

	抓取数据包的详细内容:
7	
,	

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					
	抓取数据包的详细内	容:				
14						
14						

#### 表 8-3 HEAD 响应报文分析

(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",

6

点击【Execute】	开始执行,	如图 8-11	所示。
-------------	-------	---------	-----



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。

表 8-4 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 8-5 GET 响应报文分析								
序号	字段名称	字段长度	起始(	立置	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:							

(4) POST 数据报文分析

Г

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。

8



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。

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 8-6 POST 请求报文分析

表 8-7 POST 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	

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:					
	1					

# 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

11

(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?