

# 附录3 Wireshark抓包实例分析记录表格

## TCP

项目	数据
发送方IP地址和端口号	10.0.2.15:45116
接收方IP地址和端口号	93.184.215.14:80

项目	握手包1	握手包2	握手包3	释放包1	释放包2	释放包3
Seq号	0	0	1	79	1615	1615
Ack号	0	1	1	1615	80	80
Flags	SYN/0x002	SYN+ACK/0x012	ACK/0x010	FIN+ACK/0x011	ACK/0x010	FIN+ACK/0x011
Window	64240	65535	64240	63360	65535	65535

## HTTP/HTTPS

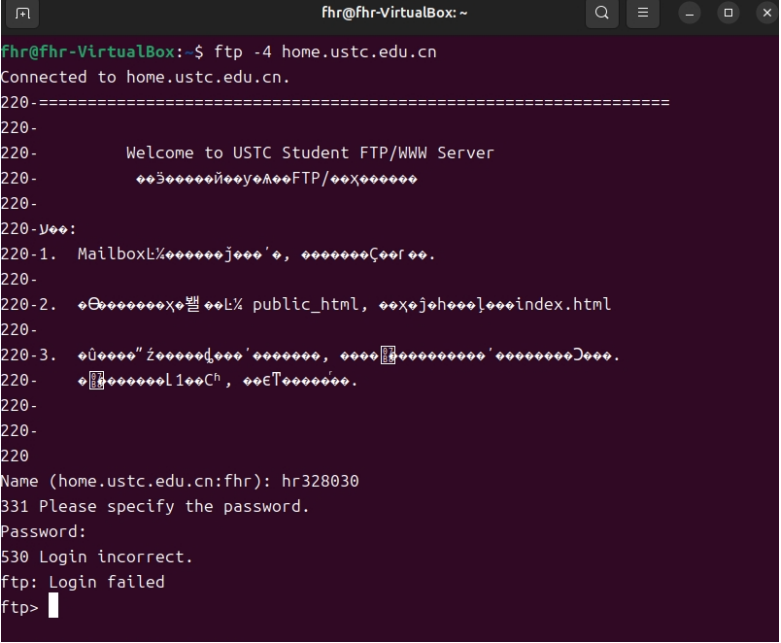
指令	协议版本	方法类型	状态码	内容类型
curl -v <a href="http://www.example.com">http://www.example.com</a>	1.1	GET	200/OK	text/html
curl -v <a href="https://www.example.com">https://www.example.com</a>	已加密	已加密	已加密	已加密
curl -v -d "user=test" -X POST <a href="http://example.com/login">http://example.com/login</a>	1.1	POST	405/Method Not Allowed	text/html

## DNS

项目	数据
本机IP地址和端口号	10.0.2.15/33596
DNS 服务器IP地址和端口号	10.0.2.3/53
传输层协议类型	UDP
目标服务器URL	<a href="http://www.example.com">www.example.com</a>
目标服务器IP地址	93.184.215.14/2606:2800:21f:cb07:6820:80da:af6b:8b2c

查询目标	命令	结果
<a href="http://www.baidu.com">www.baidu.com</a> 的IPv4地址	dig <a href="http://www.baidu.com">www.baidu.com</a> @8.8.8.8	103.235.47.188
jw.ustc.edu.cn 的IPv6地址	dig -t aaaa jw.ustc.edu.cn @8.8.8.8	2001:da8:d800:642::248
202.38.75.11的 域名	dig -x 202.38.75.11 @8.8.8.8	<pre> fhr@fhr-VirtualBox:~\$ dig -x 202.38.75.11 @8.8.8.8  ; &lt;&lt;&gt;&gt; DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu &lt;&lt;&gt;&gt; -x 202.38.75.11 @8.8.8.8 ;; global options: +cmd ;; Got answer: ;; -&gt;HEADER&lt;- opcode: QUERY, status: NXDOMAIN, id: 42843 ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 512 ;; QUESTION SECTION: ;11.75.38.202.in-addr.arpa.      IN      PTR  ;; AUTHORITY SECTION: 75.38.202.in-addr.arpa. 1800    IN      SOA      ns.ustc.edu.cn. root.ustc.edu.cn. . 17 10800 1800 3600000 86400  ;; Query time: 121 msec ;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP) ;; WHEN: Sun Dec 01 14:18:30 CST 2024 ;; MSG SIZE  rcvd: 109 </pre>
mail.ustc.edu.cn 的邮件交换记录 MX	dig MX mail.ustc.edu.cn	<pre> fhr@fhr-VirtualBox:~\$ dig MX mail.ustc.edu.cn  ; &lt;&lt;&gt;&gt; DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu &lt;&lt;&gt;&gt; MX mail.ustc.edu.cn ;; global options: +cmd ;; Got answer: ;; -&gt;HEADER&lt;- opcode: QUERY, status: NOERROR, id: 32600 ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ;; QUESTION SECTION: ;mail.ustc.edu.cn.              IN      MX  ;; ANSWER SECTION: mail.ustc.edu.cn.             1448    IN      MX      5 smtp2.ustc.edu.cn. mail.ustc.edu.cn.             1448    IN      MX      5 smtp.ustc.edu.cn.  ;; Query time: 1 msec ;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP) ;; WHEN: Sun Dec 01 14:13:30 CST 2024 ;; MSG SIZE  rcvd: 88 </pre>
i.ustc.edu.cn 的 CNAME	dig cname i.ustc.edu.cn	revproxy.ustc.edu.cn
example.com 的 域名服务器	dig example.com ns /or/dig+trace example.com	a.iana-servers.net、b.iana-servers.net

## FTP

状态	操作	现象
登录	不能注册做不出来	
被动	ls	
主动	ls	
主动	PORT	
被动	PASV	