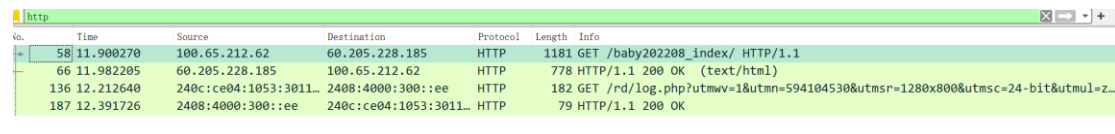


02.HTTP/HTTPS

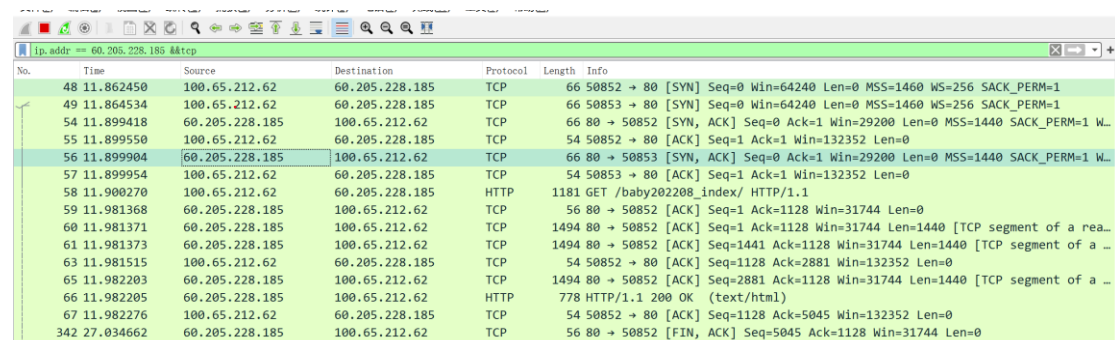
1. 使用抓包工具（如 Wireshark）抓取并分析 HTTP 及 HTTPS 交互过程。将相关数据包截图粘贴到一个文档中并添加相关说明。文档转换为 pdf 后在系统中提交。

1.利用过滤器筛选出 http 请求



No.	Time	Source	Destination	Protocol	Length	Info
58	11.900270	100.65.212.62	60.205.228.185	HTTP	1181	GET /baby202208_index/ HTTP/1.1
66	11.982205	60.205.228.185	100.65.212.62	HTTP	778	HTTP/1.1 200 OK (text/html)
136	12.212640	240c:ce04:1053:3011::	2408:4000:300::ee	HTTP	182	GET /rd/log.php?utmwv=1&utm=594104530&utmsr=1280x800&utmcs=24-bit&utm=Z...
187	12.391726	2408:4000:300::ee	240c:ce04:1053:3011::	HTTP	79	HTTP/1.1 200 OK

Tcp 三次握手（下图中有不少例子）



No.	Time	Source	Destination	Protocol	Length	Info
48	11.862450	100.65.212.62	60.205.228.185	TCP	66	50852 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
49	11.864534	100.65.212.62	60.205.228.185	TCP	66	50853 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
54	11.899418	60.205.228.185	100.65.212.62	TCP	66	80 → 50852 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 W...
55	11.899550	100.65.212.62	60.205.228.185	TCP	54	50852 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
56	11.899904	60.205.228.185	100.65.212.62	TCP	66	80 → 50853 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 W...
57	11.899954	100.65.212.62	60.205.228.185	TCP	54	50853 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
58	11.900270	100.65.212.62	60.205.228.185	HTTP	1181	GET /baby202208_index/ HTTP/1.1
59	11.981368	60.205.228.185	100.65.212.62	TCP	56	80 → 50852 [ACK] Seq=1 Ack=1128 Win=31744 Len=0
60	11.981371	60.205.228.185	100.65.212.62	TCP	1494	80 → 50852 [ACK] Seq=1 Ack=1128 Win=31744 Len=1440 [TCP segment of a re...
61	11.981373	60.205.228.185	100.65.212.62	TCP	1494	80 → 50852 [ACK] Seq=1441 Ack=1128 Win=31744 Len=1440 [TCP segment of a ...
63	11.981515	100.65.212.62	60.205.228.185	TCP	54	50852 → 80 [ACK] Seq=1128 Ack=2881 Win=132352 Len=0
65	11.982203	60.205.228.185	100.65.212.62	TCP	1494	80 → 50852 [ACK] Seq=2881 Ack=1128 Win=31744 Len=1440 [TCP segment of a ...
66	11.982205	60.205.228.185	100.65.212.62	HTTP	778	HTTP/1.1 200 OK (text/html)
67	11.982276	100.65.212.62	60.205.228.185	TCP	54	50852 → 80 [ACK] Seq=1128 Ack=5045 Win=132352 Len=0
342	27.034662	60.205.228.185	100.65.212.62	TCP	56	80 → 50852 [FIN, ACK] Seq=5045 Ack=1128 Win=31744 Len=0

第一次握手

当客户端想与服务器建立连接的时候，会发送一个请求连接的报文，此报文首部中的 SYN=1(PS:TCP 规定,SYN = 1 的报文段不能携带数据,并且需要消耗一个序号),同时随机生成初始序列号 seq=x,客户端进入了 SYN-SENT(同步以发送状态)。

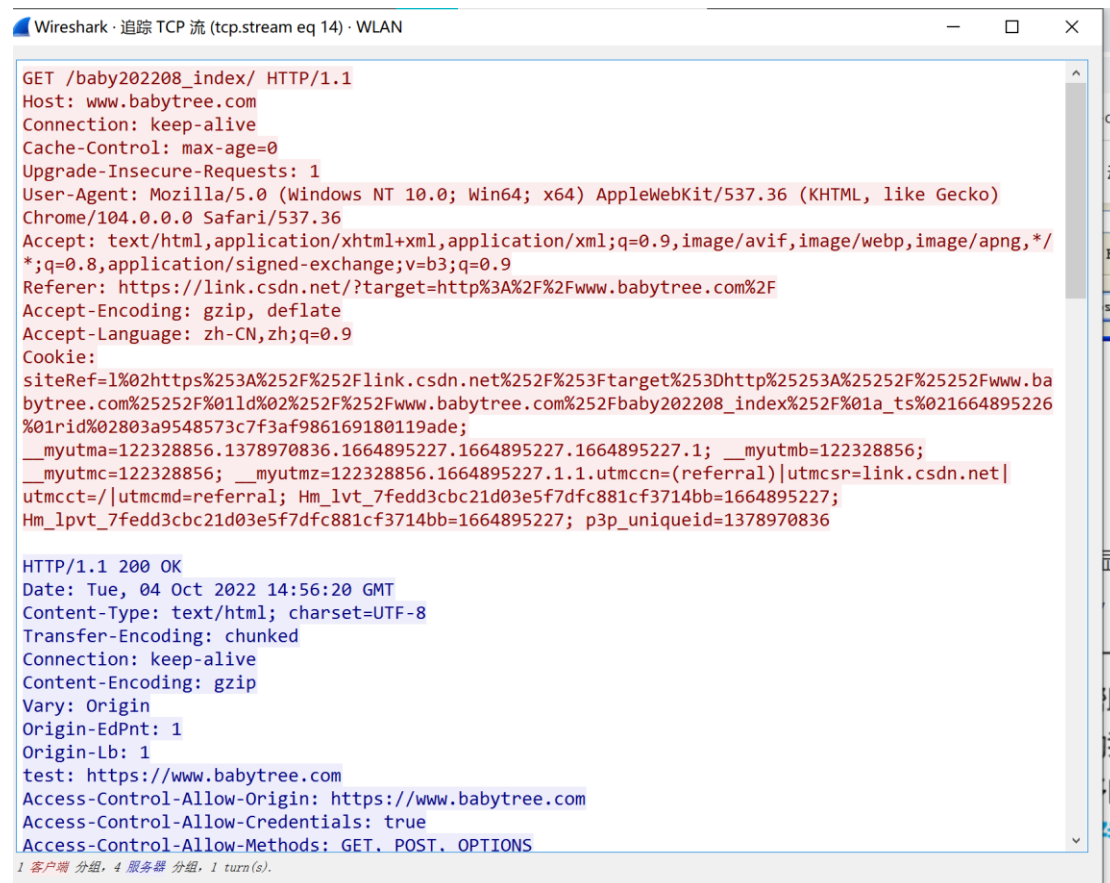
第二次握手

服务器接收到客户端发送的连接请求报文后，如果同意连接，则发出确认报文，其中确认报文段中 SYN=1,ACK=1,同时随机初始化一个序列号 seq=y,确认号 ack=x+1，而且服务器也进入 SYN_RCVD(同步接收状态)；

第三次握手

客户端接收到确认报文后，还需要向服务器发出确认报文。确认报文的 ACK=1，ack=y+1，此时，TCP 连接建立成功，客户端进入 ESTABLISHED（已建立连接）状态。

2.选取一个 http 请求进行跟踪



Wireshark · 追踪 TCP 流 (tcp.stream eq 14) · WLAN

```
GET /baby202208_index/ HTTP/1.1
Host: www.babytree.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: https://link.csdn.net/?target=http%3A%2F%2Fwww.babytree.com%2F
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
siteRef=1%02https%253A%252F%252Flink.csdn.net%252F%253Ftarget%253Dhttp%25253A%25252F%25252Fwww.ba
bytree.com%25252F%011d%02%252F%252Fwww.babytree.com%252Fbaby202208_index%252F%01a_ts%021664895226
%01rid%02803a9548573c7f3af986169180119ade;
__myutma=122328856.1378970836.1664895227.1664895227.1664895227.1; __myutmb=122328856;
__myutmc=122328856; __myutmz=122328856.1664895227.1.1.utmccn=(referral)|utmcsr=link.csdn.net|
utmctt=|utmcmd=referral; Hm_lvt_7fedd3cbc21d03e5f7dfc881cf3714bb=1664895227;
Hm_lpvt_7fedd3cbc21d03e5f7dfc881cf3714bb=1664895227; p3p_uniqueid=1378970836

HTTP/1.1 200 OK
Date: Tue, 04 Oct 2022 14:56:20 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip
Vary: Origin
Origin-EdPnt: 1
Origin-Lb: 1
test: https://www.babytree.com
Access-Control-Allow-Origin: https://www.babytree.com
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
```

1 客户端 分组, 4 服务器 分组, 1 turn(s).

Tcp 流

根据以上信息得知：

访问网站使用的是 GET 请求

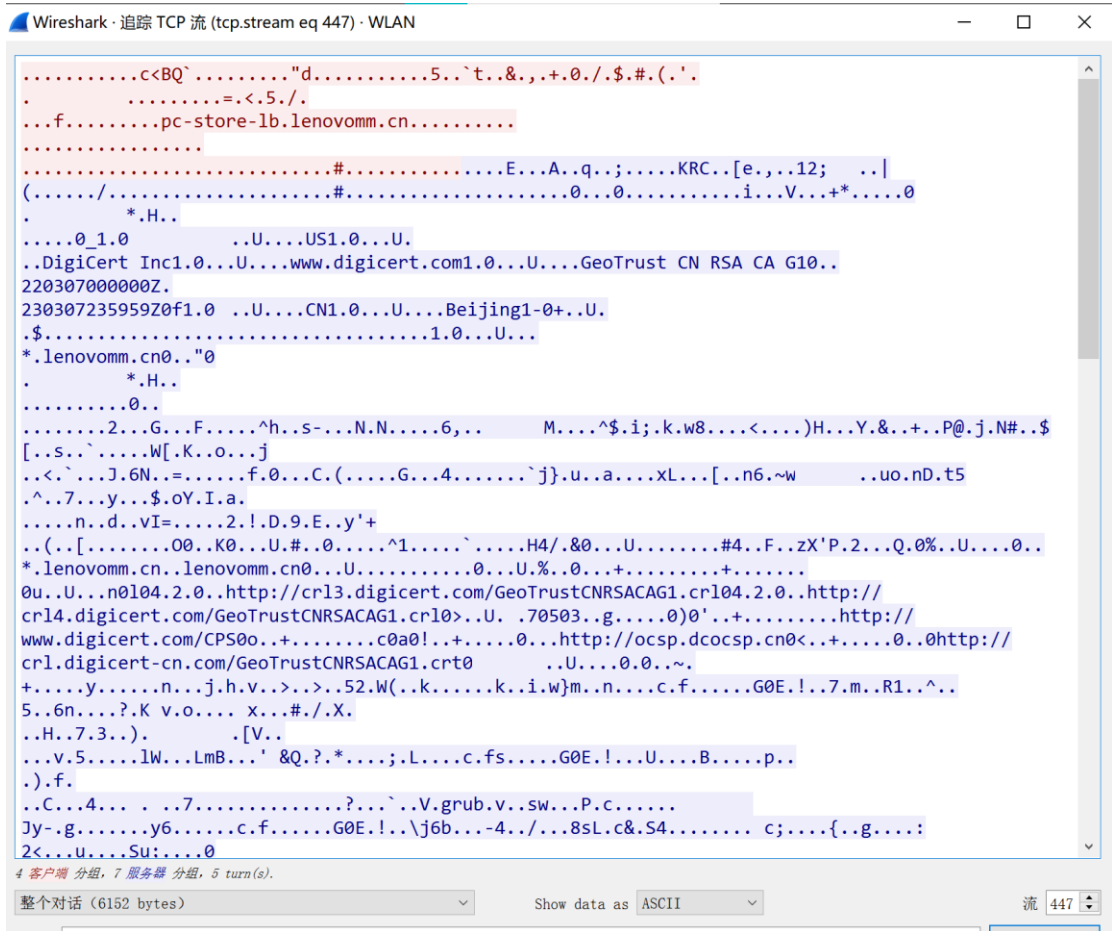
访问的网址是 www.babytree.com

剩余的还有各种报文头，cookies 等信息

下面是 HTTP 报文

Http 流传输还包括了网页前端的代码

3. 随机选取一个 https 请求进行跟踪



*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

tls.handshake.type eq 1

No.	Time	Source	Destination	Protocol	Length	Info
27442	871.834847	100.65.212.62	101.200.174.154	TLSv1.2	244	Client Hello

抓包网址: <https://www.wireshark.org/>

对于 HTTPS 协议, 由于是经过了加密的。所以数据流都是看不懂的

https=http+ssl(以下内容来自博客)

06.Https工作原理

- HTTPS工作原理
 - 一、首先HTTP请求服务端生成证书, 客户端对证书的有效期、合法性、域名是否与请求的域名一致、证书的公钥(RSA加密)等进行校验;
 - 二、客户端如果校验通过后, 就根据证书的公钥的有效, 生成随机数, 随机数使用公钥进行加密(RSA加密);
 - 三、消息体产生的后, 对它的摘要进行MD5(或者SHA1)算法加密, 此时就得到了RSA签名;
 - 四、发送给服务端, 此时只有服务端(RSA私钥)能解密。
 - 五、解密得到的随机数, 再用AES加密, 作为密钥(此时的密钥只有客户端和服务端知道)。