数字证书与 Web 加密通信实验报告

班级：　　学号：　　姓名：

一、实验名称

二、实验目的

三、实验内容与要求

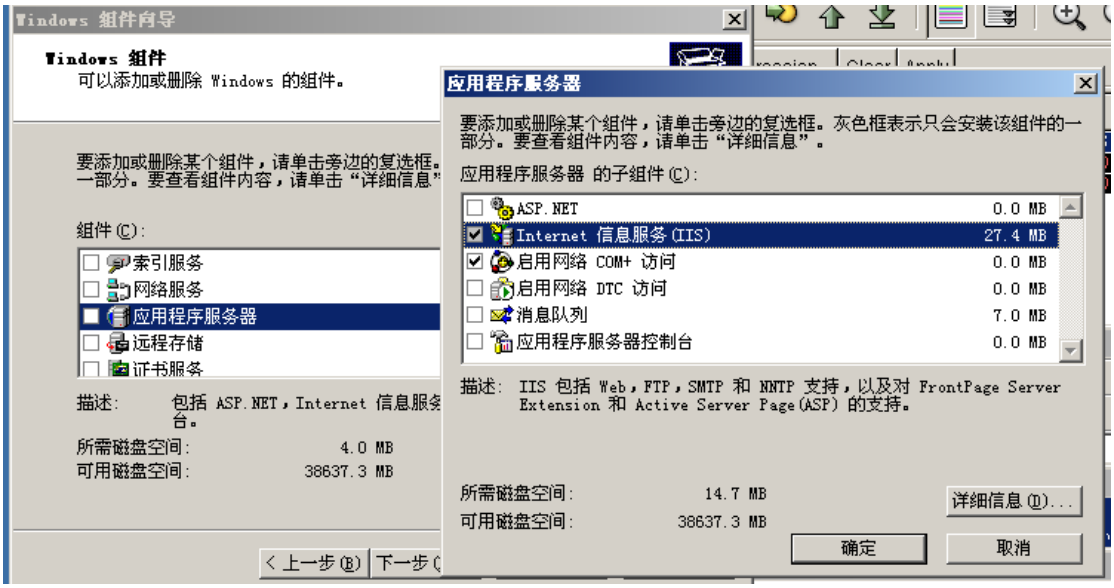
四、实验过程

实验的详细步骤，过程

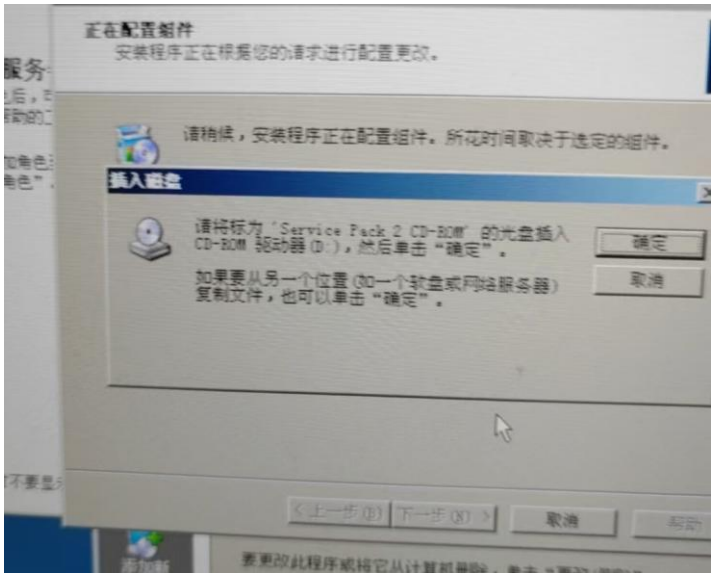
安装好 Windows Server 2003 虚拟机，关闭 IE 浏览器增强安全功能，安装好 WinPcap4.1.3 和 Ethereal。

我们需要配置 https 网站。

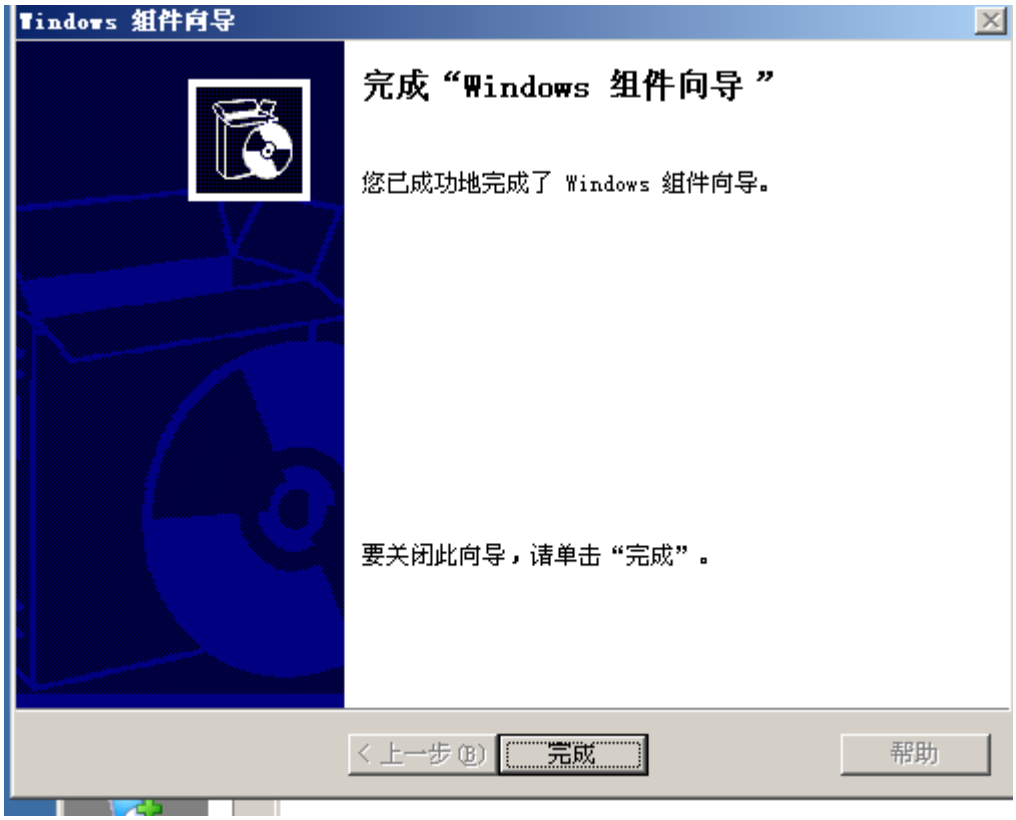
1. 先启用 iis 组件



报错 I386 文件，在 iso 中 I386 文件夹复制到虚拟机中然后选择即可安装



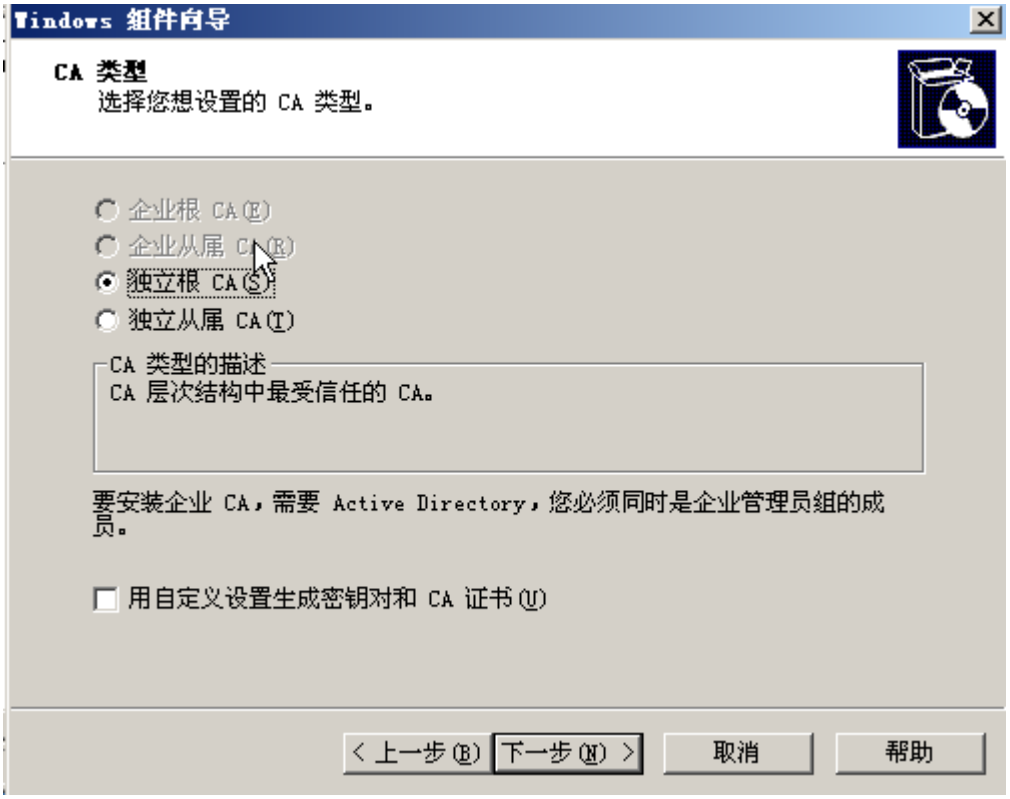
安装成功



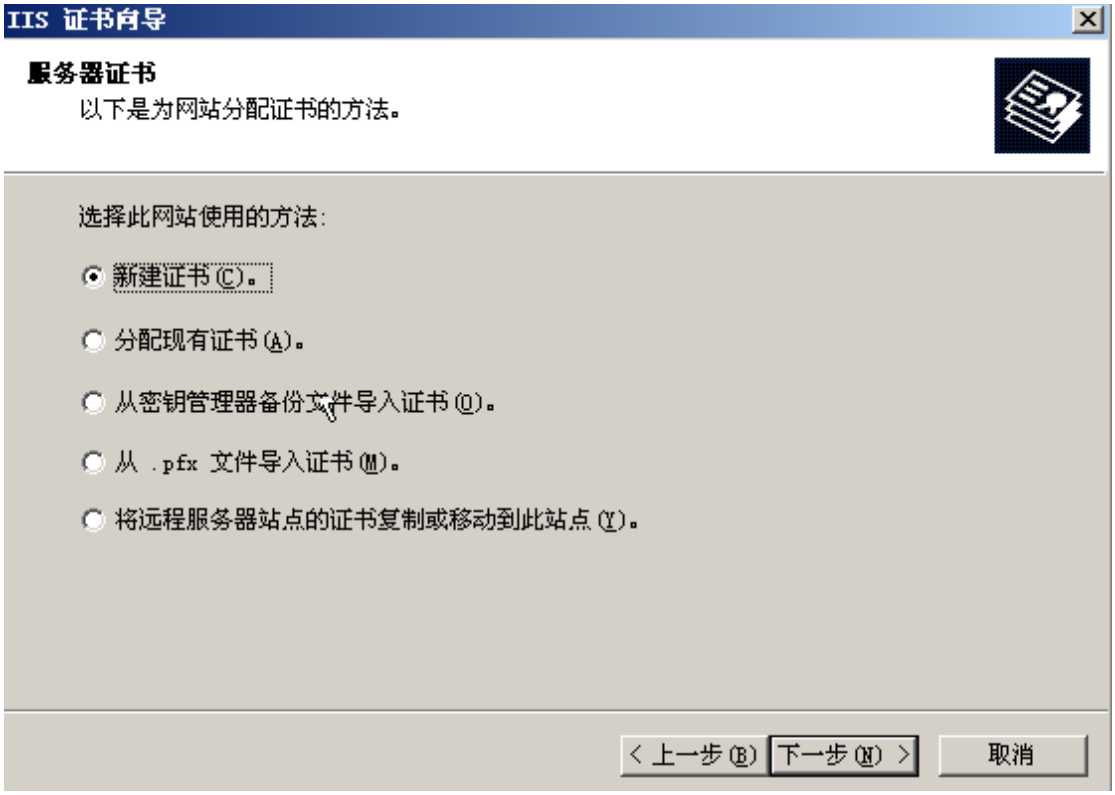
打开 IIS 管理器，选择网站，右键打开“属性”，选择“目录安全性”，点击“服务器证书”


默认网站 属性
网站
性能
ISAPI 筛选器
主目录
文档
目录安全性
HTTP 头
自定义错误
ASP.NET
身份验证和访问控制
允许匿名访问资源及编辑身份验证方法。
编辑(E)...
IP 地址和域名限制
使用 IP 地址或 Internet 域名授权或拒绝对资源的访问。
编辑(I)...
安全通信
访问资源时，要求安全通信并启用客户端证书。
服务器证书(S)...
查看证书(V)...
编辑(D)...
确定
取消
应用(A)
帮助
状况
欢迎使用 Web 服务器证书向导
欢迎使用 Web 服务器证书向导
此向导将帮助您创建并管理服务器证书，可以使用服务器证书在服务器与客户端之间建立安全的 Web 通信。
Web 服务器状态:
Web 服务器没有安装证书，且没有任何挂起的请求。证书向导将帮助您为 Web 服务器新建一个证书或附加现有证书。
单击“下一步”按钮继续。
< 上一步(B)
下一步(N) >
取消


Windows 组件向导
Windows 组件
可以添加或删除 Windows 的组件。
要添加或删除某个组件，请单击旁边的复选框。灰色框表示只会安装该组件的一部分。要查看组件内容，请单击“详细信息”。
组件(C):
网络服务 2.6 MB
应用程序服务器 34.4 MB
远程存储 4.1 MB
证书服务 1.4 MB
终端服务器 0.0 MB
描述: 安装证书颁发机构(CA)以便颁发证书用于公钥安全程序。
所需磁盘空间: 4.9 MB
可用磁盘空间: 37287.2 MB
详细信息(D)...
< 上一步(B)
下一步(N) >
取消
帮助

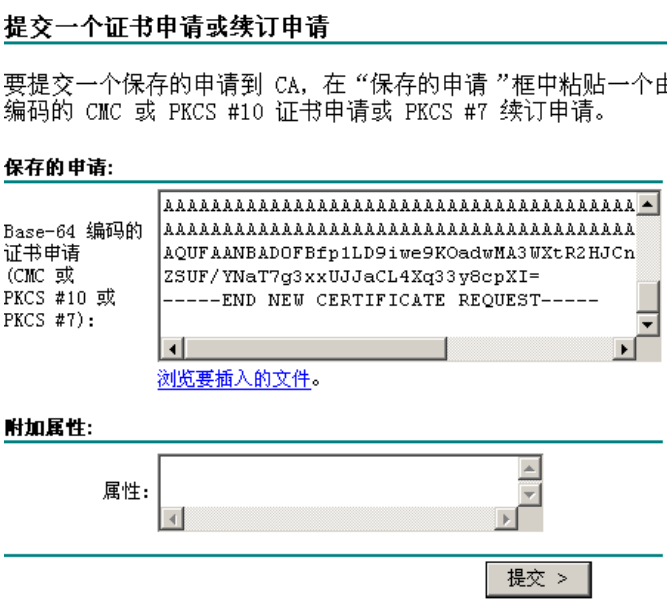

Windows 组件向导
CA 类型
选择您想设置的 CA 类型。
企业根 CA(E)
企业从属 CA(R)
独立根 CA(S)
独立从属 CA(T)
CA 类型的描述
CA 层次结构中最受信任的 CA。
要安装企业 CA，需要 Active Directory，您必须同时是企业管理员组的成员。
用自定义设置生成密钥对和 CA 证书(U)
< 上一步(B)
下一步(N) >
取消
帮助


Windows 组件向导
完成“Windows 组件向导”
您已成功地完成了 Windows 组件向导。
要关闭此向导，请单击“完成”。
< 上一步(B)
完成
帮助

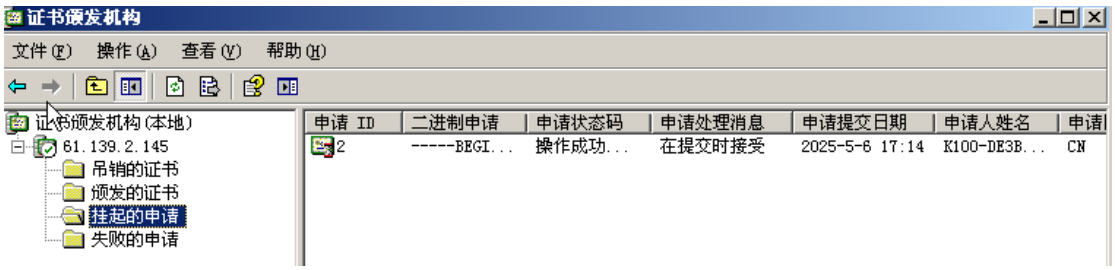


打开证书服务界面，根据该证书内容进行申请了

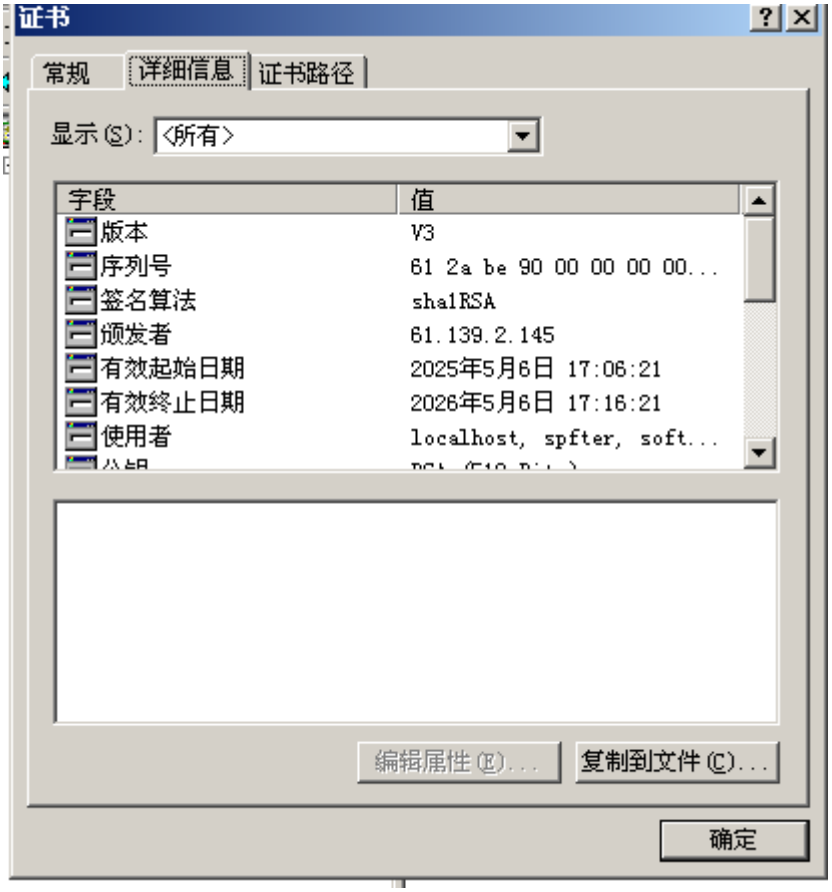
申请一个证书-》高级证书申请-》使用 base64 编码的 CMC 或 PKCS
打开生成的 certreq.txt 文件，复制并粘贴



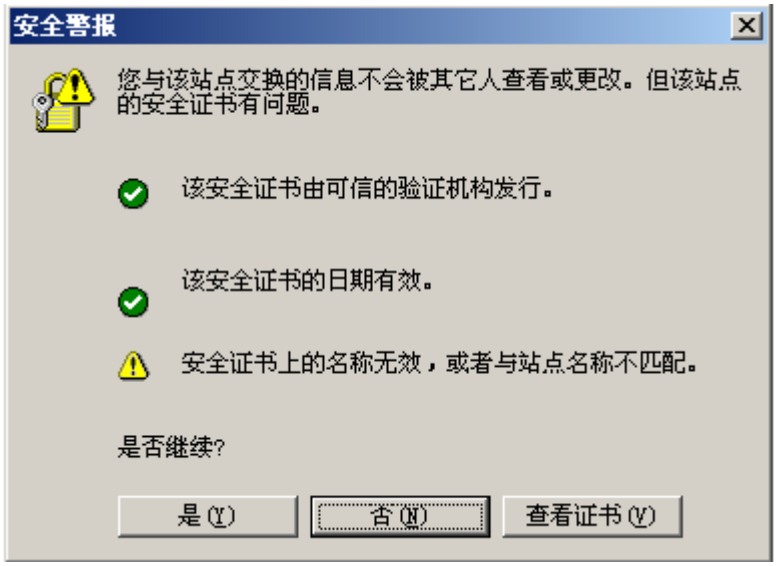
完成申请
管理员手动颁发申请的证书。
打开开始->程序->管理工具->证书颁发机构



在待申请的证书上单击鼠标右键，弹出菜单中有“所有任务”一项，选择“颁发”。



在“证书属性窗口”的详细信息标签中选择“复制到文件”，打开证书导出向导。选择 DER 编码二进制”并保存成文件，之后配置 IIS 的 SSL 安全加密功能



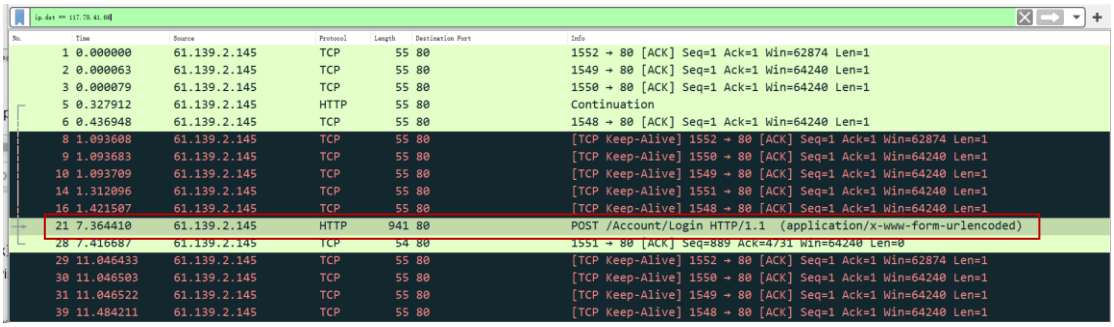
五、实验结果分析

抓取 http：

超文本传输协议，明文传输，端口 80

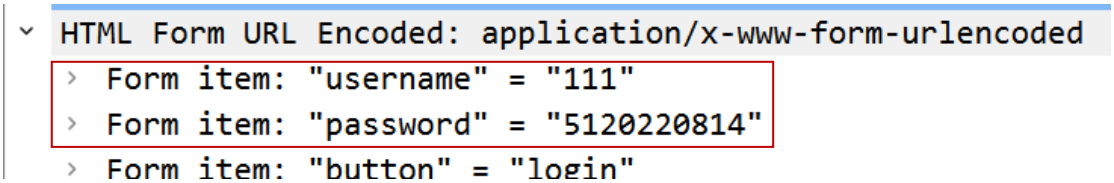
我们能看到很多流量，这是因为开启浏览器或其他应用的时候都会有流量产生。

我们对流量进行过滤 ip.dst == 117.78.41.66，只列出目标地址是 117.78.41.66 的流量



No.	Time	Source	Protocol	Length	Destination Port	Info
1	0.000000	61.139.2.145	TCP	55	80	1552 → 80 [ACK] Seq=1 Ack=1 Win=62874 Len=1
2	0.000063	61.139.2.145	TCP	55	80	1549 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
3	0.000079	61.139.2.145	TCP	55	80	1550 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
5	0.327912	61.139.2.145	HTTP	55	80	Continuation
6	0.436948	61.139.2.145	TCP	55	80	1548 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
8	1.093608	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1552 → 80 [ACK] Seq=1 Ack=1 Win=62874 Len=1
9	1.093683	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1550 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
10	1.093709	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1549 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
14	1.312096	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1551 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
16	1.421507	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1548 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
21	7.364410	61.139.2.145	HTTP	941	80	POST /Account/Login HTTP/1.1 (application/x-www-form-urlencoded)
28	7.416687	61.139.2.145	TCP	54	80	1551 → 80 [ACK] Seq=889 Ack=4731 Win=64240 Len=0
29	11.046433	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1552 → 80 [ACK] Seq=1 Ack=1 Win=62874 Len=1
30	11.046503	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1550 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
31	11.046522	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1549 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
39	11.484211	61.139.2.145	TCP	55	80	[TCP Keep-Alive] 1548 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1

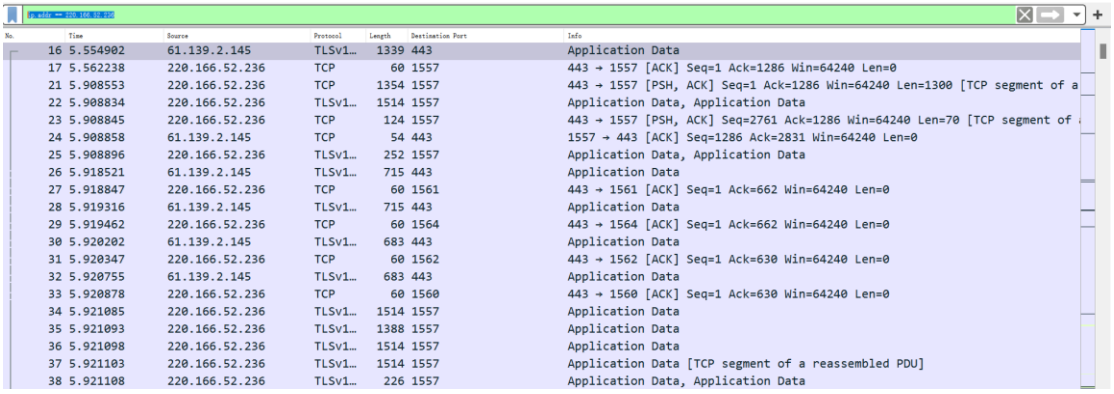
能看到一个 POST 方式的表单提，查看该条流量，发现输入的用户名和密码。



抓取 https：

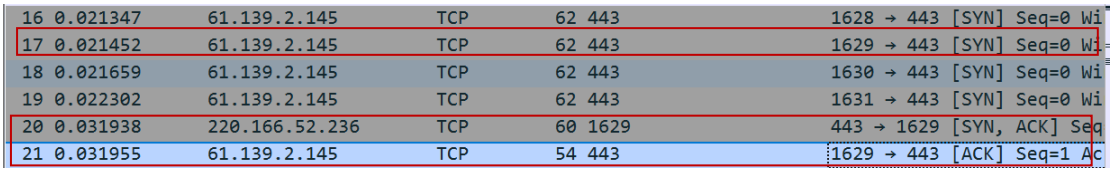
具有安全性的 ssl 加密传输协议，端口 443

我们对学校官网进行嗅探，对流量包进行过滤 ip.addr == 220.166.52.236

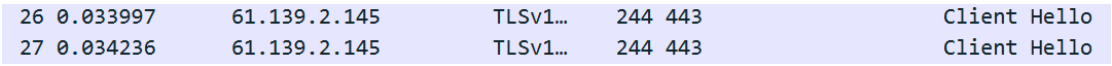


No.	Time	Source	Protocol	Length	Destination Port	Info
16	5.554902	61.139.2.145	TLSv1…	1339	443	Application Data
17	5.562238	220.166.52.236	TCP	60	1557	443 → 1557 [ACK] Seq=1 Ack=1286 Win=64240 Len=0
21	5.908553	220.166.52.236	TCP	1354	1557	443 → 1557 [PSH, ACK] Seq=1 Ack=1286 Win=64240 Len=1300 [TCP segment of a
22	5.908834	220.166.52.236	TLSv1…	1514	1557	Application Data, Application Data
23	5.908845	220.166.52.236	TCP	124	1557	443 → 1557 [PSH, ACK] Seq=2761 Ack=1286 Win=64240 Len=70 [TCP segment of
24	5.908858	61.139.2.145	TCP	54	443	1557 → 443 [ACK] Seq=1286 Ack=2831 Win=64240 Len=0
25	5.908896	220.166.52.236	TLSv1…	252	1557	Application Data, Application Data
26	5.918521	61.139.2.145	TLSv1…	715	443	Application Data
27	5.918847	220.166.52.236	TCP	60	1561	443 → 1561 [ACK] Seq=1 Ack=662 Win=64240 Len=0
28	5.919316	61.139.2.145	TLSv1…	715	443	Application Data
29	5.919462	220.166.52.236	TCP	60	1564	443 → 1564 [ACK] Seq=1 Ack=662 Win=64240 Len=0
30	5.920202	61.139.2.145	TLSv1…	683	443	Application Data
31	5.920347	220.166.52.236	TCP	60	1562	443 → 1562 [ACK] Seq=1 Ack=630 Win=64240 Len=0
32	5.920755	61.139.2.145	TLSv1…	683	443	Application Data
33	5.920878	220.166.52.236	TCP	60	1560	443 → 1560 [ACK] Seq=1 Ack=630 Win=64240 Len=0
34	5.921085	220.166.52.236	TLSv1…	1514	1557	Application Data
35	5.921093	220.166.52.236	TLSv1…	1388	1557	Application Data
36	5.921098	220.166.52.236	TLSv1…	1514	1557	Application Data
37	5.921103	220.166.52.236	TLSv1…	1514	1557	Application Data [TCP segment of a reassembled PDU]
38	5.921108	220.166.52.236	TLSv1…	226	1557	Application Data, Application Data

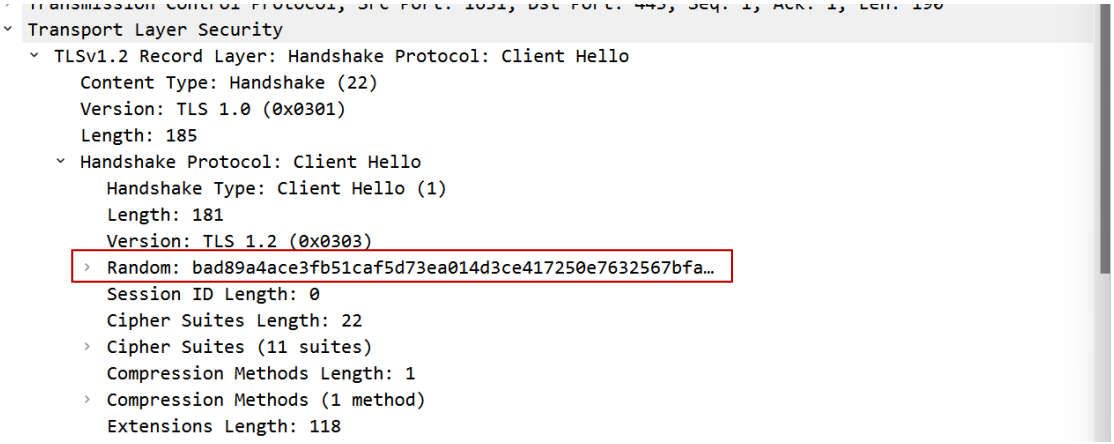
TCP 三次握手



https 的发包——浏览器先发送 client hello

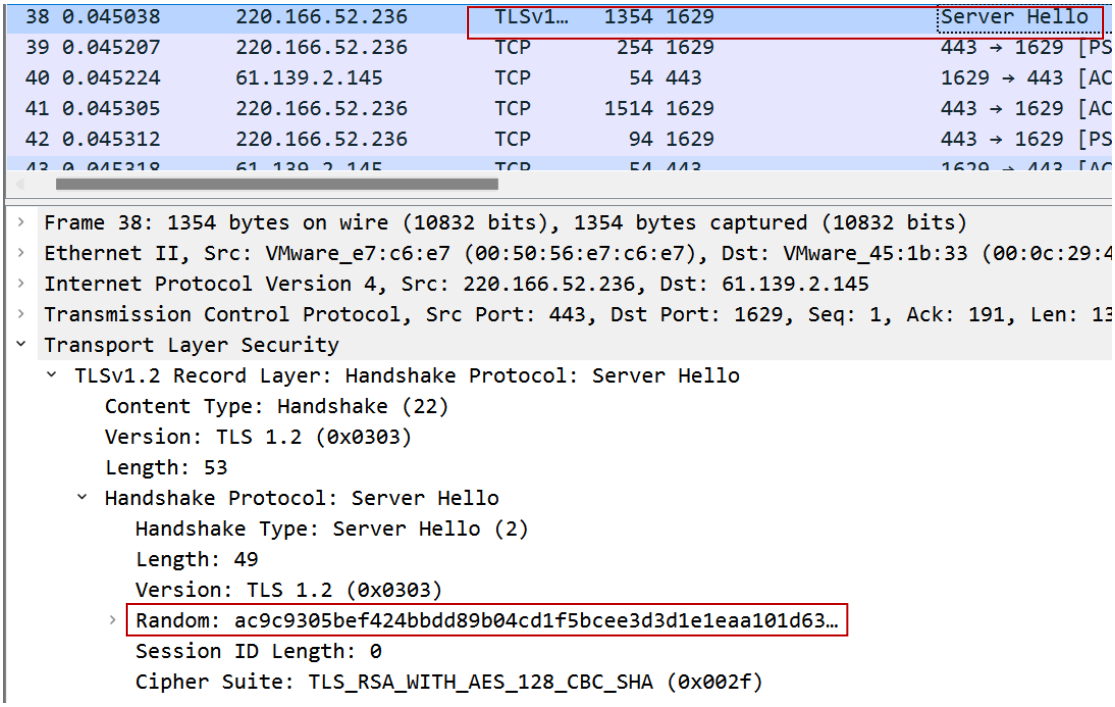


客户端给服务器发送一个随机值 random1、TLS 版本、支持的加密算法



服务器给浏览器（客户端）发送 server hello

同时我们从数据包中发现服务器也给客户端发送了一个随机值 random2 并且选择加密算法



然后服务器发送证书，交换密钥，打开带有 Certificate, Server Key Exchange, Server Hello Done.标识的数据包，可以看到证书相关数据

```
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 3899
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 3895
    Certificates Length: 3892
  Certificates (3892 bytes)
    Certificate Length: 1689
  Certificate: 308206953082057da003020102021077648ef1a59c30d5bf… (id-at-commonName=*.swust…
    signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
      Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
    Padding: 0
    encrypted: 48369e2b26bd989a1dbcaee9f321ec74193dac6b1b4ca2c4…
  Certificate Length: 1235
  Certificate: 308204cf308203b7a003020102021100f244082daba90da5… (id-at-commonName=Xcc Tru…
    signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
    Padding: 0
```

客户端的秘钥交换：

带有 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 标识的流量包。客户端发送交换密钥信息、证书发送给服务器并且验证服务器的证书后发送验证。

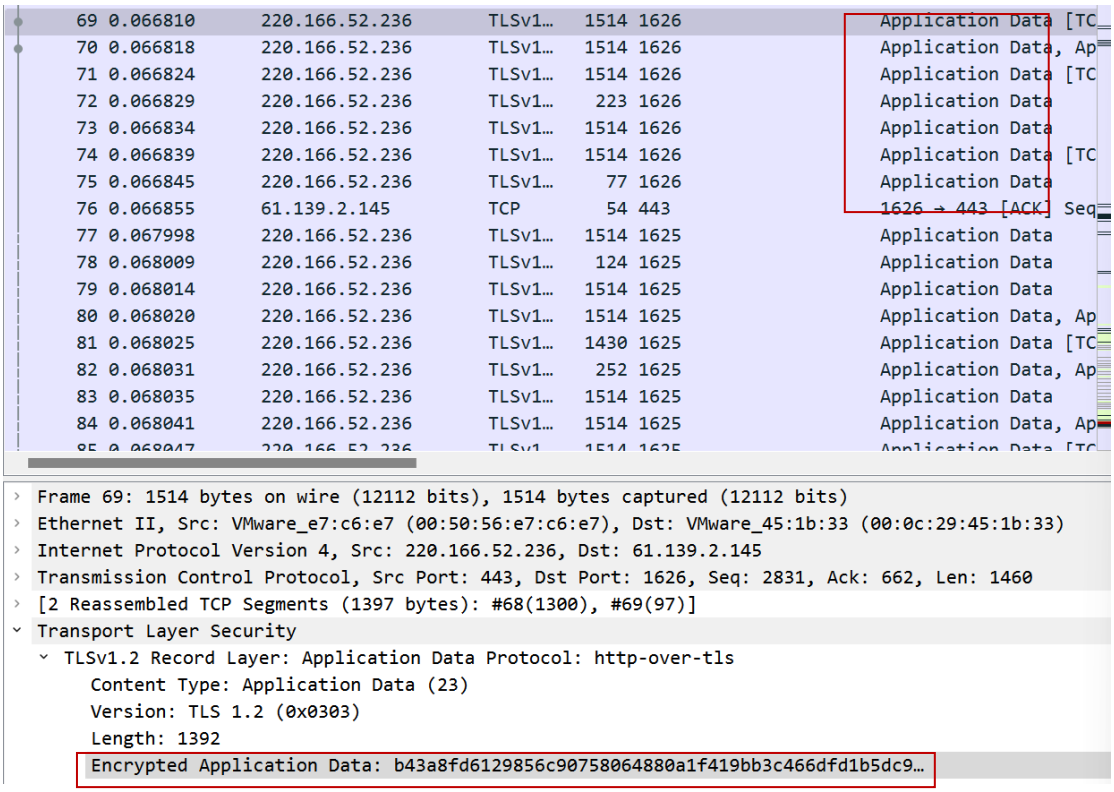
```
1210 23.392267   61.139.2.145     TLSv1…   396 443    Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1211 23.401131   220.166.52.236   TCP       60 1644   443 → 1644 [ACK] Seq=3972 Ack=533 Win=64240 Len=0
1212 23.410278   220.166.52.236   TLSv1…   129 1644   Change Cipher Spec, Encrypted Handshake Message

Frame 1210: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
Ethernet II, Src: VMware_45:1b:33 (00:0c:29:45:1b:33), Dst: VMware_e7:c6:e7 (00:50:56:e7:c6:e7)
Internet Protocol Version 4, Src: 61.139.2.145, Dst: 220.166.52.236
Transmission Control Protocol, Src Port: 1644, Dst Port: 443, Seq: 191, Ack: 3972, Len: 342
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 262
    Handshake Protocol: Client Key Exchange
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 64
    Handshake Protocol: Encrypted Handshake Message
```

```
197 2.633062   2409:8962:2bad:47f9… TLSv1…   138 443   Change Cipher Spec, Application Data
198 2.633297   2409:8962:2bad:47f9… TLSv1…  1194 443   Application Data

Frame 197: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: 9c:2f:9d:91:11:c3 (9c:2f:9d:91:11:c3), Dst: de:20:e8:27:53:bd (de:20:e8:27:53:bd)
Internet Protocol Version 6, Src: 2409:8962:2bad:47f9:7d15:55de:33ac:cdcd, Dst: 2001:da8:600e:6001:160::238
Transmission Control Protocol, Src Port: 52671, Dst Port: 443, Seq: 1838, Ack: 4438, Len: 64
Transport Layer Security
  TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 53
      Encrypted Application Data: 7fc3141ebe3b330d94a54a96a31585e4cf40b94e6d5f3ac0…
```

数据传递：Application Data，此时的数据都是经过加密的.



69	0.066810	220.166.52.236	TLSv1…	1514	1626	Application Data [TC
70	0.066818	220.166.52.236	TLSv1…	1514	1626	Application Data, Ap
71	0.066824	220.166.52.236	TLSv1…	1514	1626	Application Data [TC
72	0.066829	220.166.52.236	TLSv1…	223	1626	Application Data
73	0.066834	220.166.52.236	TLSv1…	1514	1626	Application Data
74	0.066839	220.166.52.236	TLSv1…	1514	1626	Application Data [TC
75	0.066845	220.166.52.236	TLSv1…	77	1626	Application Data
76	0.066855	61.139.2.145	TCP	54	443	1626 → 443 [ACK] Seq
77	0.067998	220.166.52.236	TLSv1…	1514	1625	Application Data
78	0.068009	220.166.52.236	TLSv1…	124	1625	Application Data
79	0.068014	220.166.52.236	TLSv1…	1514	1625	Application Data
80	0.068020	220.166.52.236	TLSv1…	1514	1625	Application Data, Ap
81	0.068025	220.166.52.236	TLSv1…	1430	1625	Application Data [TC
82	0.068031	220.166.52.236	TLSv1…	252	1625	Application Data, Ap
83	0.068035	220.166.52.236	TLSv1…	1514	1625	Application Data
84	0.068041	220.166.52.236	TLSv1…	1514	1625	Application Data, Ap

```
> Frame 69: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: VMware_e7:c6:e7 (00:50:56:e7:c6:e7), Dst: VMware_45:1b:33 (00:0c:29:45:1b:33)
> Internet Protocol Version 4, Src: 220.166.52.236, Dst: 61.139.2.145
> Transmission Control Protocol, Src Port: 443, Dst Port: 1626, Seq: 2831, Ack: 662, Len: 1460
> [2 Reassembled TCP Segments (1397 bytes): #68(1300), #69(97)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 1392
      Encrypted Application Data: b43a8fd6129856c90758064880a1f419bb3c466dfd1b5dc9…
```

六、思考与心得体会