警示：实验报告如有雷同，雷同各方当次实验成绩均以 0 分计；在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计；实验报告文件以 PDF 格式提交。

院系		班级		学号		姓名	
完成日期： 2017 年 月 日							

FTP 协议分析实验

【实验目的】

分析FTP协议的安全性。

【实验步骤】

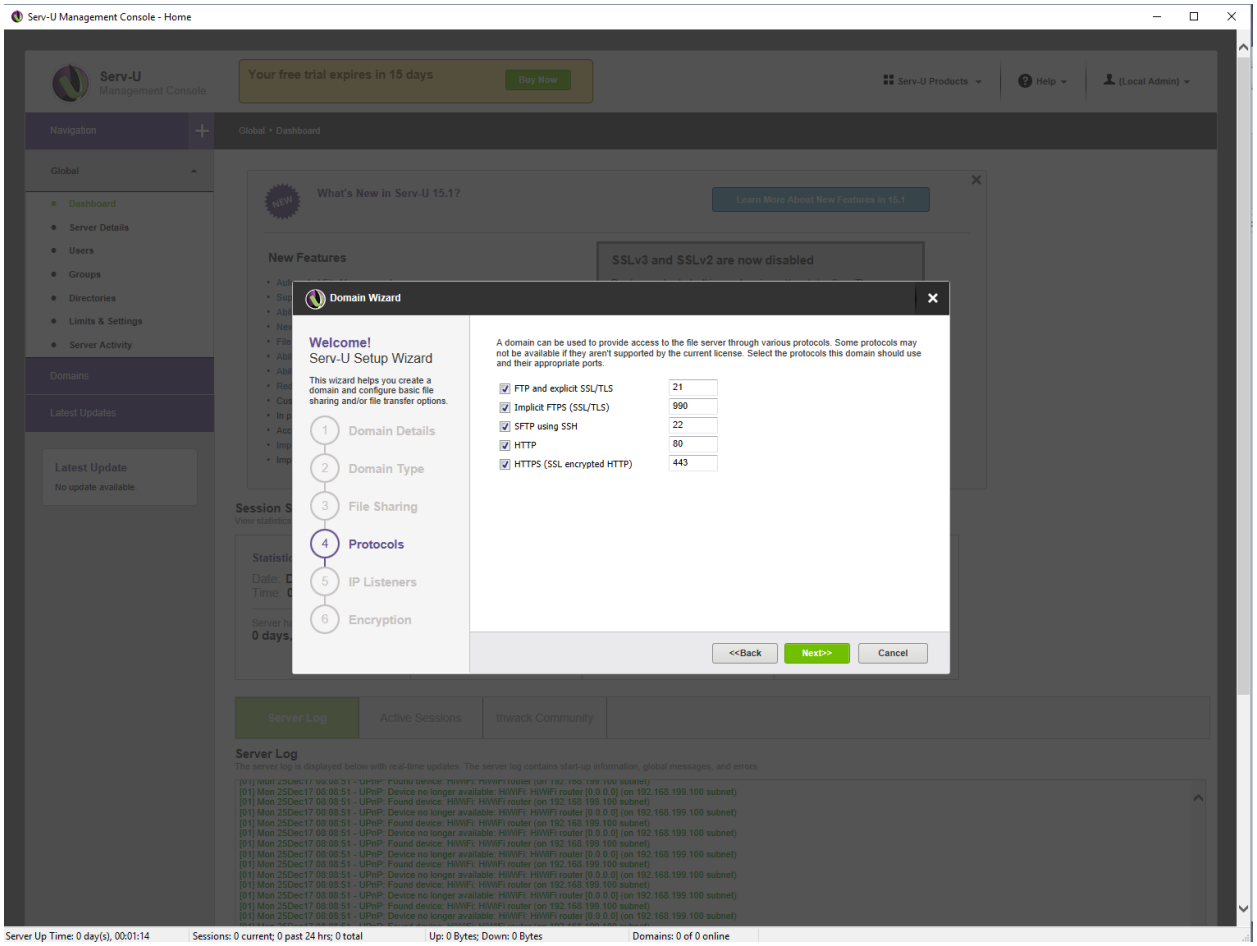
1. 配置 Serv-U 服务器；建立用户名和密码（例如用户名是USER，密码PASS）；
   (有很多可参考的网络资源。比如 http://www.jb51.net/article/28530.htm)
2. 使用协议分析软件 wireshark (http://www.wireshark.org/download.html)，设置好过滤规则为 ftp（安装过程不必截图）。
3. 客户端使用 ftp 命令访问服务器端，输入用户名和密码。
4. 开始抓包，从捕获的数据包中分析用户名/口令 (请在截图上标出)。
5. 讨论 FTP 协议的安全问题。
6. 设置 Serv-U 的安全连接功能，客户端使用 (1) http (2) https (3) FileZilla 或 cutFTP，重复步骤2-4，看是否能保证用户名/口令的安全？

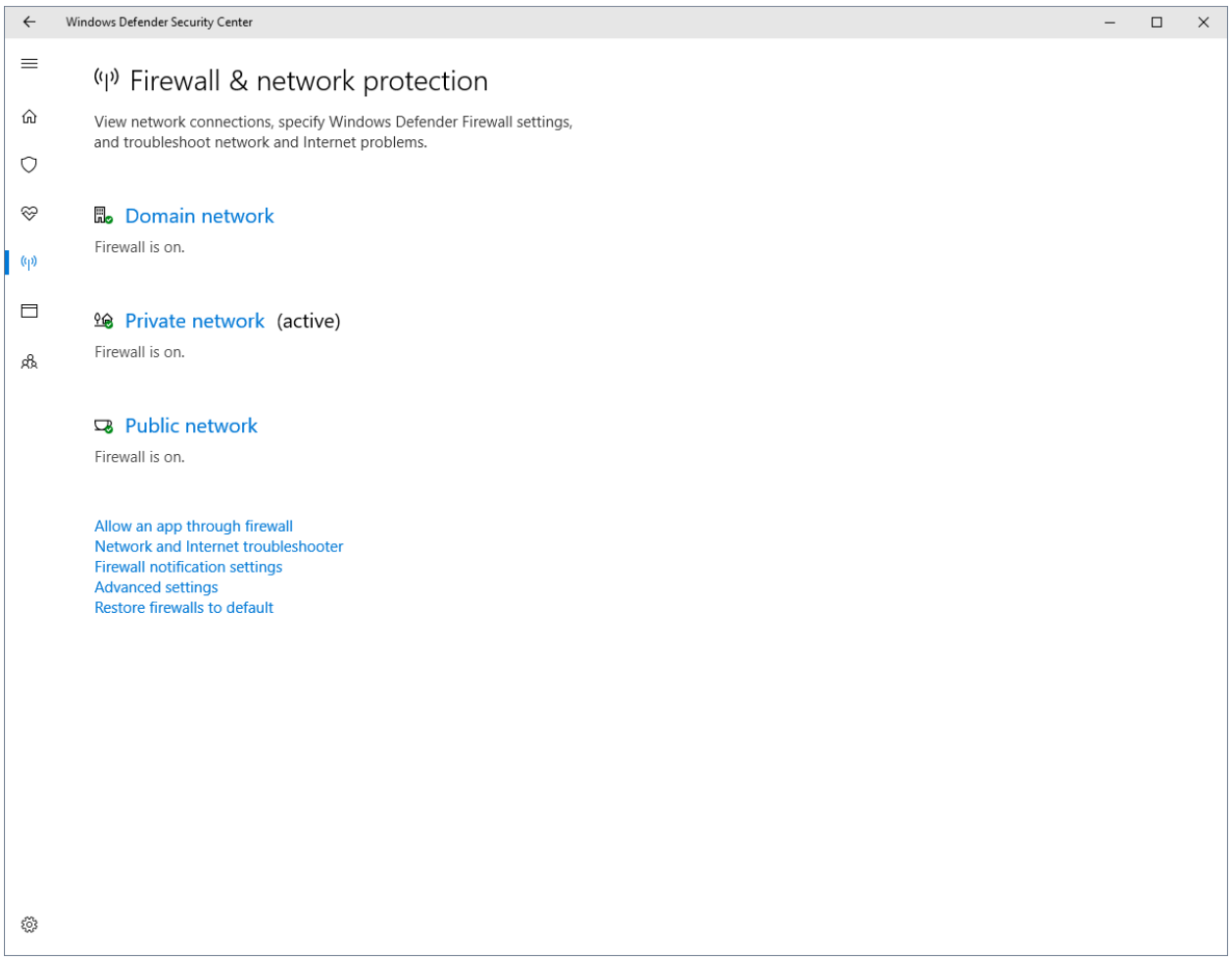
【实验工具】

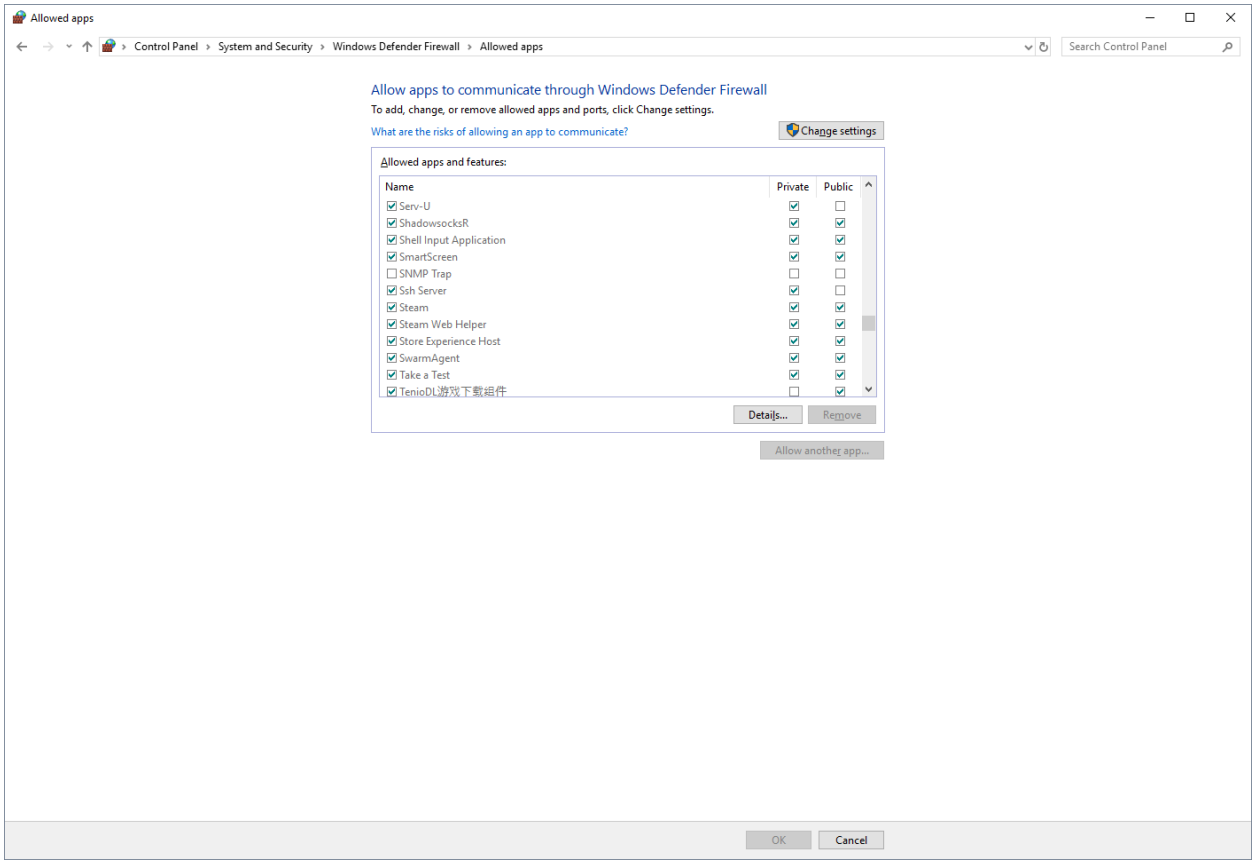
使用 Wireshark 可以很方便地对截获的数据包进行分析，包括该数据包的源地址、目的地址、所属协议等。Wireshark 的图形化嗅探器界面中，整个窗口被分成三个部分：最上面为数据包列表，用来显示截获的每个数据包的总结性信息；中间为协议树，用来显示选定的数据包所属的协议信息；最下边是以十六进制形式表示的数据包内容，用来显示数据包在物理层上传输时的最终形式。

【实验过程】（要有实验截图）

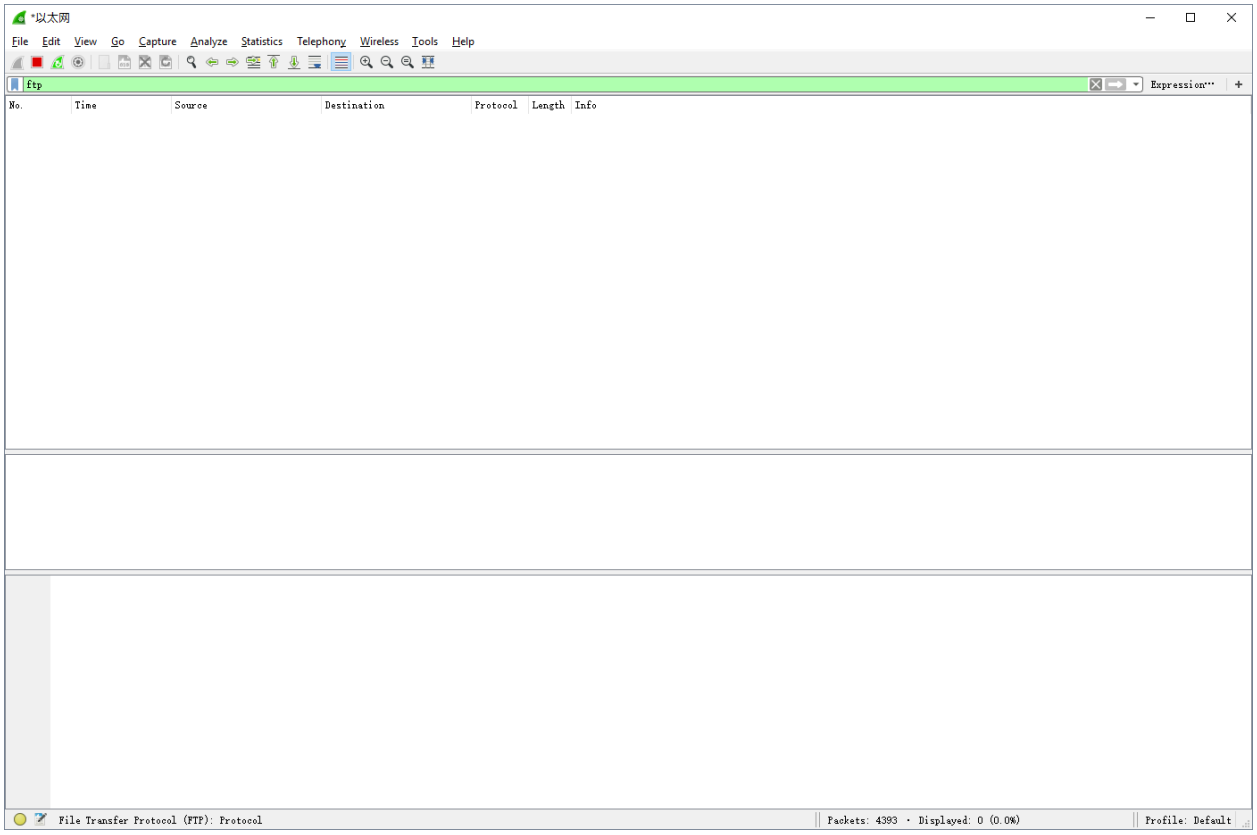
1. 配置服务器，实验环境为私有网络，设置允许透过私有网络防火墙。


Serv-U Management Console - Home
Serv-U Management Console
Your free trial expires in 15 days
Buy Now
Serv-U Products
Help
(Local Admin)
Navigation
Global • Dashboard
Global
Dashboard
Server Details
Users
Groups
Directories
Limits & Settings
Server Activity
Domains
Latest Updates
Latest Update
No update available.
What's New in Serv-U 15.1?
Learn More About New Features in 15.1
New Features
SSLv3 and SSLv2 are now disabled
Domain Wizard
Welcome!
Serv-U Setup Wizard
This wizard helps you create a domain and configure basic file sharing and/or file transfer options.
1 Domain Details
2 Domain Type
3 File Sharing
4 Protocols
5 IP Listeners
6 Encryption
A domain can be used to provide access to the file server through various protocols. Some protocols may not be available if they aren't supported by the current license. Select the protocols this domain should use and their appropriate ports.
FTP and explicit SSL/TLS 21
Implicit FTPS (SSL/TLS) 990
SFTP using SSH 22
HTTP 80
HTTPS (SSL encrypted HTTP) 443
<<Back
Next>>
Cancel
Server Log
Active Sessions
thwack Community
Server Log
Server Up Time: 0 day(s), 00:01:14
Sessions: 0 current; 0 past 24 hrs; 0 total
Up: 0 Bytes; Down: 0 Bytes
Domains: 0 of 0 online


Windows Defender Security Center
Firewall & network protection
View network connections, specify Windows Defender Firewall settings, and troubleshoot network and Internet problems.
Domain network
Firewall is on.
Private network (active)
Firewall is on.
Public network
Firewall is on.
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

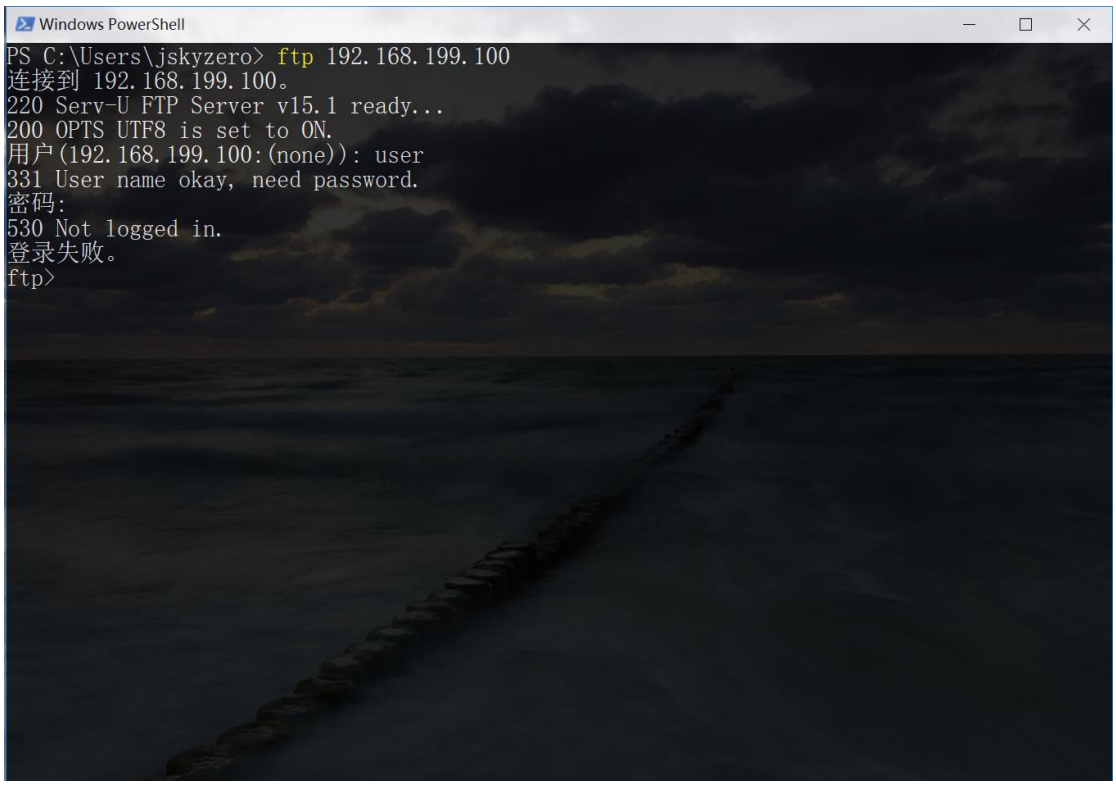


2. 开启 wireshark。



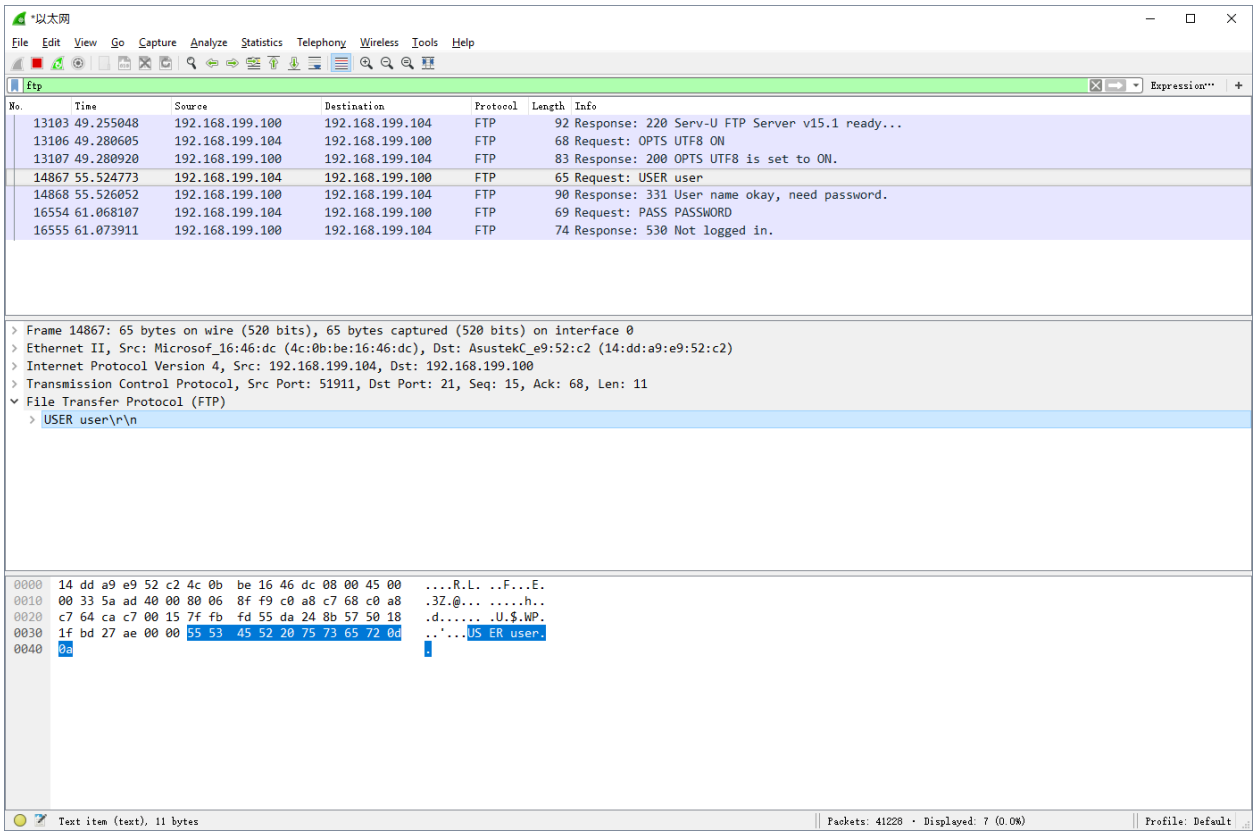
3. 输入错误密码。

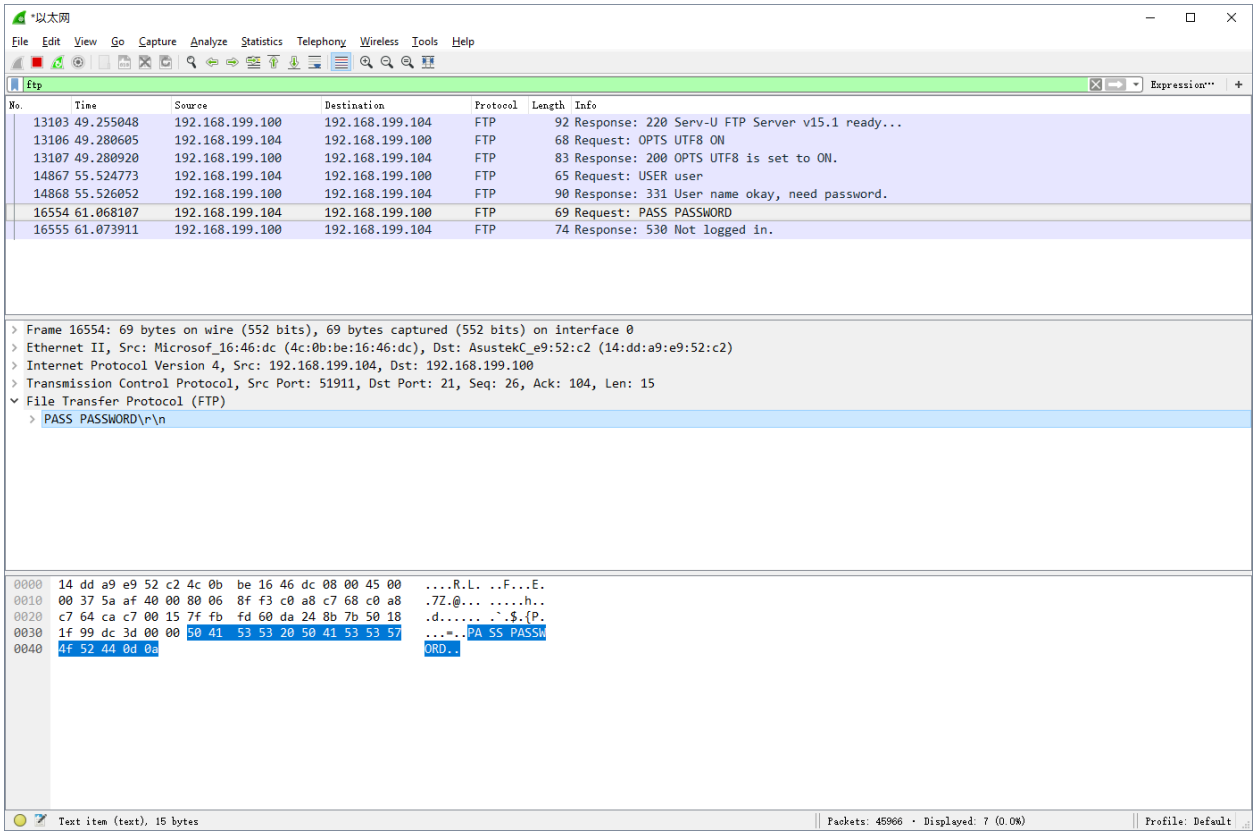
4.



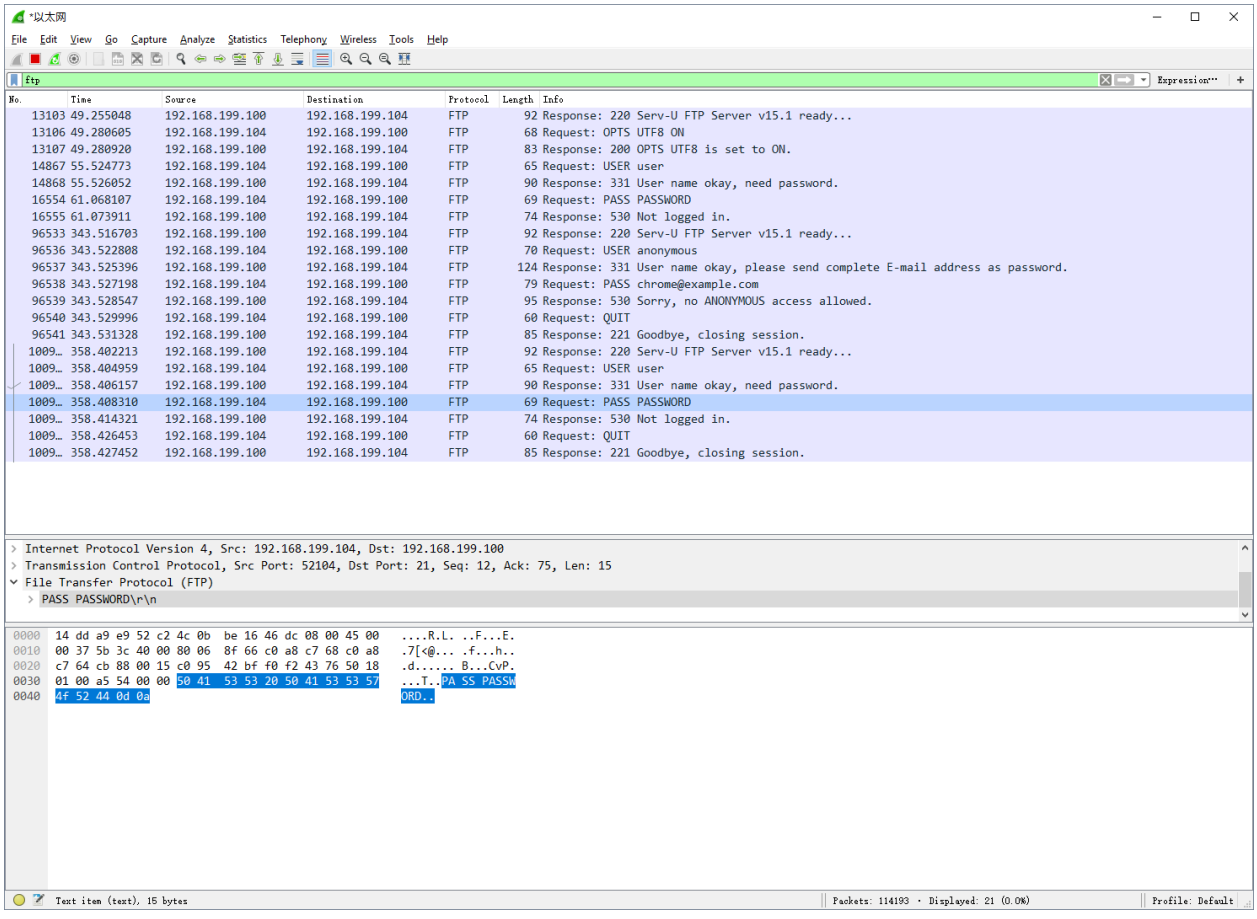
5. 蓝色选框中间可以看到明文。

6.





7. FTP 本身会将密码以明文形式呈现，在互联网中传输的数据可能会被第三方拦截，我们可以配合 SSL 或者 TSL 等手段来实现数据加密。
8. 在浏览器中使用 ftp://来访问

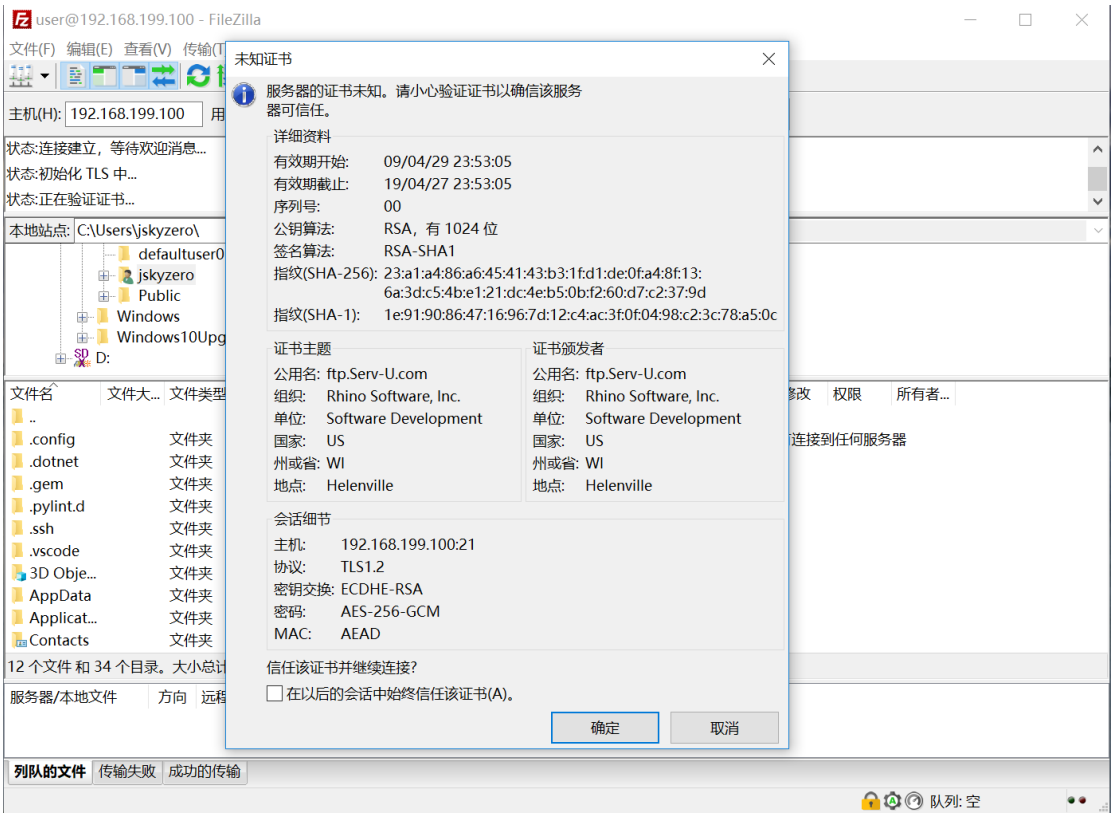


此时在客户端会被提醒不是安全连接，同时服务端抓包仍然是明文。

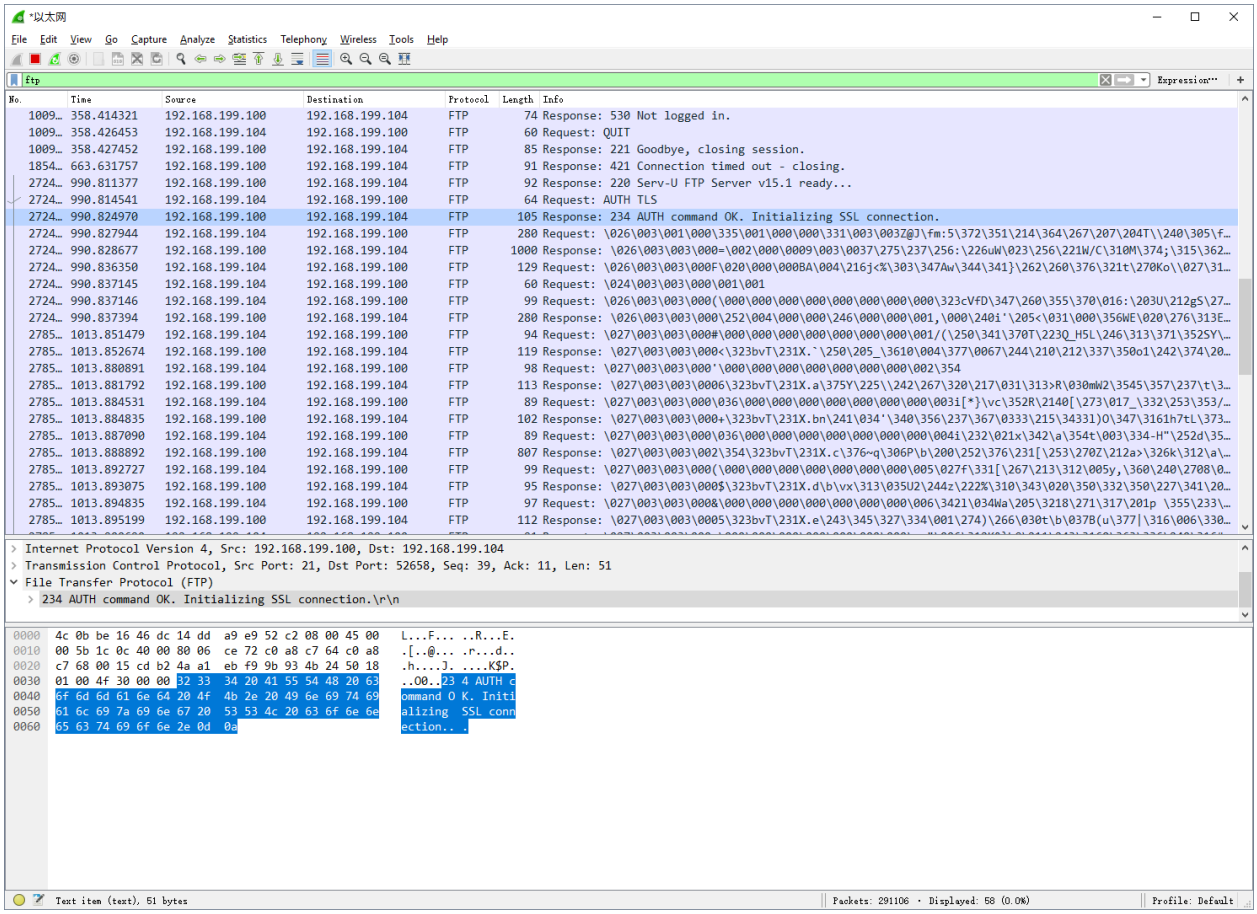
在浏览器使用 HTTP/HTTPS 都无法访问此网站，FTP 和 HTTP/HTTPS 的端口和各种协议细节都不

一致，服务端并未开启 HTTP/HTTPS 服务。

使用 FileZilla 访问



可以看到关于证书认证信任的环节。



此时数据包已经是被加密的了。是安全的。

【实验体会】

这次实验中我们自己配置了 FTP 服务器，同时使用多种 FTP 客户端，使用 Wireshark 软件对数据报文进行了分析，对 FTP 的安全性有了更加深刻的理解。

互联网设计的初衷是假设一切用户都是好人，这导致了很多协议的数据内容都是以明文呈现的，FTP 作为一个日常生活中经常使用到的应用层协议，如果不注意保护好用户凭证，很容易就被不法第三方给利用，当然我们有很多办法可以解决这个问题，就比如SSL/TSL/IPSec等等。