计算机网络实验报告

警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 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。
4. 实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班 级	软工一班	组长	陈铭涛
学号	16340024	16340023	16340025		
学生	陈铭涛	陈明亮	陈慕远		
实验分工					
陈铭涛	负责 Http, Ftp, Telnet 协议客户机与服务机之间的数据包抓取分析，完成实验教程实验问题填写，完成 Telnet 协议分析实验报告。	陈明亮	负责 Http, Ftp, Telnet 协议客户机与服务机之间的数据包抓取分析，协助回答实验思考，完成 Http 协议分析实验报告。		
陈慕远	负责 Http, Ftp, Telnet 协议客户机与服务机之间的数据包抓取分析，协助完成实验问题，完成 Ftp 协议分析实验报告。				

【实验题目】网络嗅探与协议分析实验

【实验目的】 通过网络嗅探了解网络数据类型、了解网络工作原理；学习相关工具的使用。

【实验内容】

第二版书：

1. HTTP 协议分析，通过学习 HTTP 报文结构与相应的方法，掌握 HTTP 协议获取网页的流程，通过其请求报文与响应报文格式进行报文分析。
   - 步骤一：打开 WireShark 软件，选择监听网卡，设置过滤规则为 HTTP，开始监听 HTTP 协议传输数据包。
   - 步骤二：打开浏览器，输入支持 HTTP 协议的网站，此处为 http://network.chenmt.science，捕获数据。
   - 步骤三：暂停 WireShark 对数据包的捕获，分析已经获得的数据包，进行报文分析。
   - 步骤四：根据分析结果，完成实验表格与实验思考题。

2. FTP 协议分析，实现通过终端命令行模式与 Web 浏览器模式访问 FTP 服务器，并且分析 FTP 协议连接工作，传输数据过程细节，以及 FTP 双连接(数据连接与控制连接)的查看，评判 FTP 协议传输数据安全性。
   - 步骤一：在用户主机的虚拟机上创建 FTP 服务器，提供文件目录以供访问，设置访问用户名与密码。
   - 步骤二：运行 WireShark 软件，设置过滤规则为 FTP，开始捕获数据包。
   - 步骤三：先在客户端的终端窗口中登录 FTP 服务器，根据以下命令连接服务器，执行登录->登出操作。

```
c:\> ftp 192.168.100.101
```

```
Connected to 192.168.100.101
...
User(none):mig
331 User name okay, need password
Password:******
230 User Logged in
...
ftp>quit
```

- 步骤四：停止捕获报文，将上述操作后的数据包保存为 FTP-DOS 文件
- 步骤五：打开浏览器，以未登录状态在网址栏上输入服务器 FTP 地址，重新开始捕获报文。由于匿名用户不允许，故在提示框中输入正确的用户名密码。
- 步骤六：在 FTP 服务器文件目录下任意下载一个文件，停止捕获报文。将捕获的报文保存为 FTP-WEB。分析两次捕获的报文数据，完成实验表格与思考题。

3. Telnet 协议分析，理解 Telnet 协议的工作原理，与其相关的操作命令。
   - 步骤一：在队伍中某一队员的电脑中开启 Telnet 服务机功能，配置其用户名密码。
   - 步骤二：运行 WireShark 软件，设置过滤规则为 Telnet，开始捕获报文。
   - 步骤三：在客户机的终端窗口上运行下述指令，连接至 Telnet 服务器。

```
c:\> Telnet 172.18.186.78
...
...
login: Pal
password: ******
/*==========================================================
============================
Welcome to Microsoft Telnet Server.
==========================================================
============================*/
c:\User\Pal> ....
```

   - 步骤四：停止捕获报文，将上述所得数据记录保存为 TELNET-DOS 文件。
   - 步骤五：开启浏览器访问 telnet:\\172.18.186.78，重新启用报文捕获功能，使用用户名密码登录，将所捕获报文保存为 TELNET-WEB 文件。
   - 步骤六：根据 Telnet 协议报文规则，分析报文数据，并回答问题。

【实验要求】

一些重要信息信息需给出截图。

注意实验步骤的前后对比！

【实验记录】(如有实验拓扑请自行画出，要求自行画出拓扑图)

(1) HTTP 协议分析结果

1. HTTP 请求报文分析表

方法	GET	版本	HTTP/1.1	URL	/css/calculator.css
首部字段名	字段值	字段所表达的信息			
Host	http://network.chenmt.science	请求资源所在的服务器网址			
Connection	Keep-Alive	决定当前连接的生命周期，此处为持续连接			
User-Agent	OSX/10.14.0	客户端用户信息			
Cache-Control	max-age=0	控制缓存行为信息			

2. HTTP 响应报文分析表

版本	HTTP/1.1	状态码	200	短语	OK
首部字段名	字段值	字段所表达的信息			
Server	Nginx	服务器信息			
Content-Type	text/html	返回内容类型			
Content-Length	1703	返回内容大小			
Vary	Accept-Encoding	决定未来缓存使用与否			

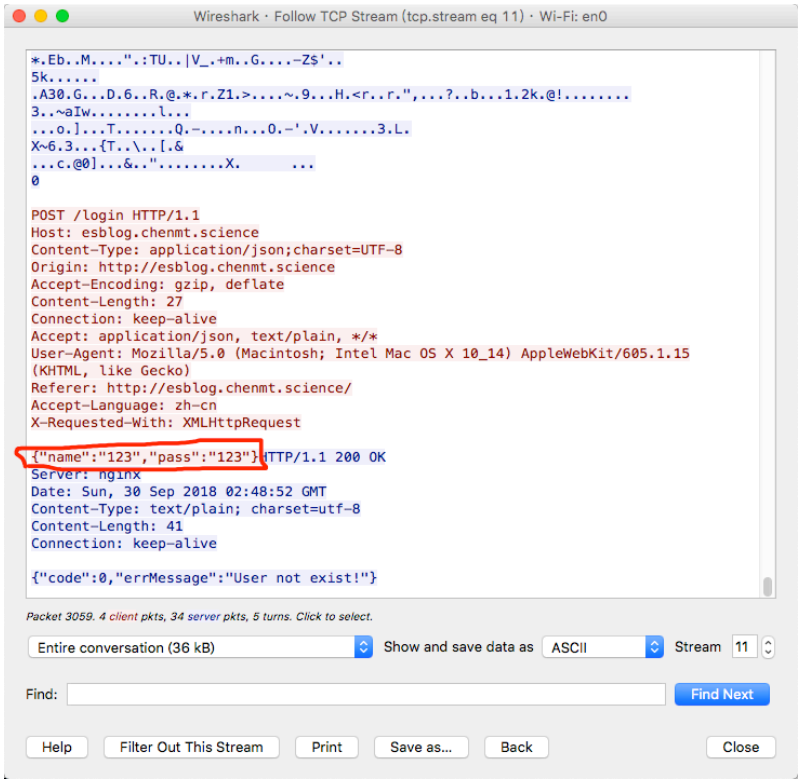
3. HTTP 协议工作过程

客户机端口号	服务器端口号	所包括的报文号	工作过程
50395	80	214344	客户机与服务器之间建立 TCP 连接的第一次握手过程，由客户机向服务器发送建立连接请求
50395	80	214345	TCP 连接的第二次握手过程，服务器向客户端发送接收成功响应
50395	80	214346	TCP 连接的第三次握手，客户端发送连接确认请求，进入连接建立态；服务器接收到对应报文，也正式建立 TCP 数据传输连接
50395	80	214347	客户机发送 Web 资源的 GET 请求给服务器
50395	80	214350	服务器接收请求成功，发送响应报文
50395	80	214351	服务器开始向客户端传输请求数据
50395	80	214352	服务器传输数据结束，响应客户端，发送成功结束短语 OK

4. 分析所得报文，回答实验问题
   - 在捕获的报文中，总共有两种 HTTP 报文：HTTP 请求报文与 HTTP 响应报文。客户机与服务器之间建立了一个 Keep-Alive 类型的连接。服务器使用 80 端口，客户机使用 50395 端口。
   - 第一个与第三个 HTTP 绘画中，服务器对客户端请求的响应为状态码 200，短语为 OK。
5. 关于本次实验内容的思考

- 实验中客户机首先启动了HTTP会话，它通过开启空闲端口，建立进程发送相应的SYN包到对应IP的服务器，进入SYN_SEND状态，等待服务器响应请求。
- 本次实验中，客户机首先发出了结束HTTP会话的信号，它通过发送[FIN, ACK]包，服务器识别对应ACK连接号的TCP连接，根据FIN信号结束对应的HTTP会话。
- 选取的表单提交网页地址为 `http://esblog.chenmt.science`，我们通过登录操作，输入用户名密码。可以捕获到该POST方法请求字段值：`name: User pass: 123456`，由此可见HTTP协议对于传输数据包并无加密操作；POST方法同时以对应的跳转页面query作为URL，本例中为`/login`。GET方法以请求文件相对路径query作为URL值，无特殊请求字段值，其余一般字段值与POST相同。

如图，红框内容即为 POST 方法传送数据：



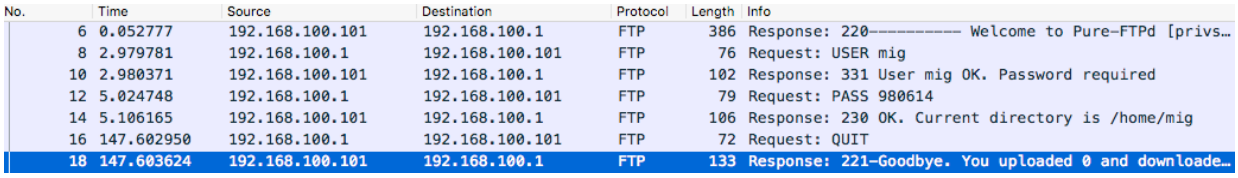
(2) Ftp 协议分析结果

1. TCP 三次握手后的第一个 FTP 报文：

FTP 报文格式分析

源 IP 地址	192.168.100.1	源端口	50821
目的 IP 地址	192.168.100.101	目的端口	21
FTP 字段	字段值	字段所表达的信息	
Response Code	220	服务端已为客户端准备好	
Response Arg	Welcome…	请开始进行相关操作	

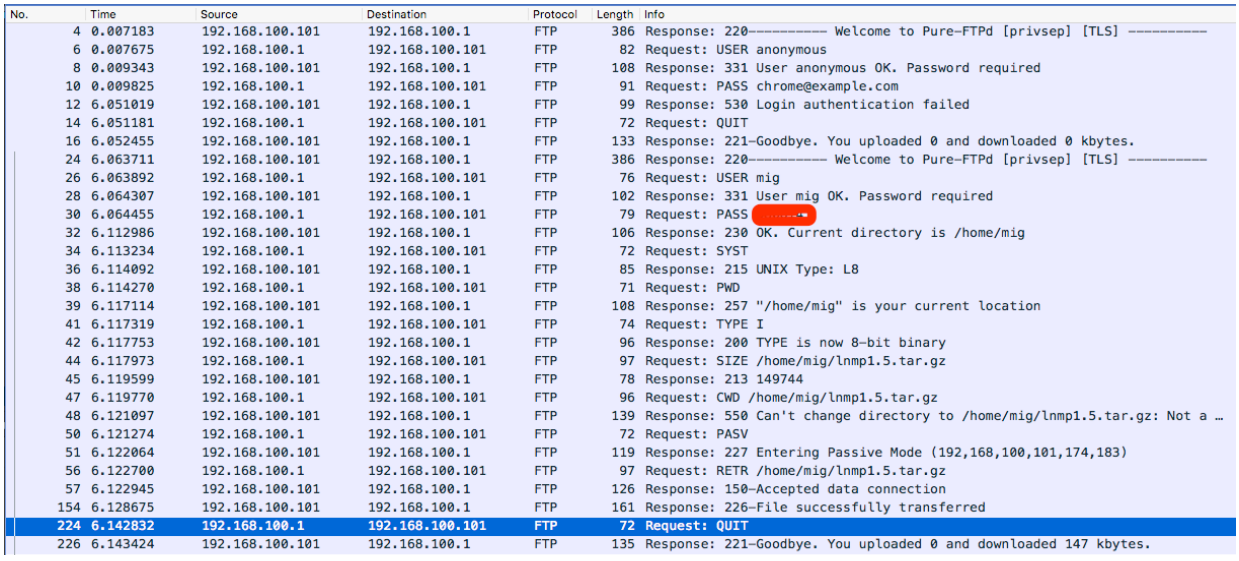
2. 在 FTP-DOS 中找出 FTP 指令传送和响应的报文，分析并填表：



No.	Time	Source	Destination	Protocol	Length	Info
6	0.052777	192.168.100.101	192.168.100.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privs…
8	2.979781	192.168.100.1	192.168.100.101	FTP	76	Request: USER mig
10	2.980371	192.168.100.101	192.168.100.1	FTP	102	Response: 331 User mig OK. Password required
12	5.024748	192.168.100.1	192.168.100.101	FTP	79	Request: PASS 980614
14	5.106165	192.168.100.101	192.168.100.1	FTP	106	Response: 230 OK. Current directory is /home/mig
16	147.602950	192.168.100.1	192.168.100.101	FTP	72	Request: QUIT
18	147.603624	192.168.100.101	192.168.100.1	FTP	133	Response: 221-Goodbye. You uploaded 0 and downloade…

过程	指令/响应	报文号	报文信息
User	Request	8	USER mig
	Response	10	User mig ok, password required
Password	Request	12	PASS ***
	Response	14	OK. Current directory is …
Quit	Request	16	QUIT
	Response	18	Goodbye. You uploaded … and downloaded …

3. 对 FTP-WEB 捕获的报文进行综合分析，观察 FTP 协议的工作过程，特别观察两种连接的建立过程和释放过程，以及这两种连接建立和释放的先后顺序。



No.	Time	Source	Destination	Protocol	Length	Info
4	0.007183	192.168.100.101	192.168.100.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
6	0.007675	192.168.100.1	192.168.100.101	FTP	82	Request: USER anonymous
8	0.009343	192.168.100.101	192.168.100.1	FTP	108	Response: 331 User anonymous OK. Password required
10	0.009825	192.168.100.1	192.168.100.101	FTP	91	Request: PASS chrome@example.com
12	6.051019	192.168.100.101	192.168.100.1	FTP	99	Response: 530 Login authentication failed
14	6.051181	192.168.100.1	192.168.100.101	FTP	72	Request: QUIT
16	6.052455	192.168.100.101	192.168.100.1	FTP	133	Response: 221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
24	6.063711	192.168.100.101	192.168.100.1	FTP	386	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
26	6.063892	192.168.100.1	192.168.100.101	FTP	76	Request: USER mig
28	6.064307	192.168.100.101	192.168.100.1	FTP	102	Response: 331 User mig OK. Password required
30	6.064455	192.168.100.1	192.168.100.101	FTP	79	Request: PASS [redacted]
32	6.112986	192.168.100.101	192.168.100.1	FTP	106	Response: 230 OK. Current directory is /home/mig
34	6.113234	192.168.100.1	192.168.100.101	FTP	72	Request: SYST
36	6.114092	192.168.100.101	192.168.100.1	FTP	85	Response: 215 UNIX Type: L8
38	6.114270	192.168.100.1	192.168.100.101	FTP	71	Request: PWD
39	6.117114	192.168.100.101	192.168.100.1	FTP	108	Response: 257 "/home/mig" is your current location
41	6.117319	192.168.100.1	192.168.100.101	FTP	74	Request: TYPE I
42	6.117753	192.168.100.101	192.168.100.1	FTP	96	Response: 200 TYPE is now 8-bit binary
44	6.117973	192.168.100.1	192.168.100.101	FTP	97	Request: SIZE /home/mig/lnmp1.5.tar.gz
45	6.119599	192.168.100.101	192.168.100.1	FTP	78	Response: 213 149744
47	6.119770	192.168.100.1	192.168.100.101	FTP	96	Request: CWD /home/mig/lnmp1.5.tar.gz
48	6.121097	192.168.100.101	192.168.100.1	FTP	139	Response: 550 Can't change directory to /home/mig/lnmp1.5.tar.gz: Not a …
50	6.121274	192.168.100.1	192.168.100.101	FTP	72	Request: PASV
51	6.122064	192.168.100.101	192.168.100.1	FTP	119	Response: 227 Entering Passive Mode (192,168,100,101,174,183)
56	6.122700	192.168.100.1	192.168.100.101	FTP	97	Request: RETR /home/mig/lnmp1.5.tar.gz
57	6.122945	192.168.100.101	192.168.100.1	FTP	126	Response: 150-Accepted data connection
154	6.128675	192.168.100.101	192.168.100.1	FTP	161	Response: 226-File successfully transferred
224	6.142832	192.168.100.1	192.168.100.101	FTP	72	Request: QUIT
226	6.143424	192.168.100.101	192.168.100.1	FTP	135	Response: 221-Goodbye. You uploaded 0 and downloaded 147 kbytes.

报文类型	所包括的报文序号	客户端口	服务器端口
FTP 数据传送	59	51043	44727
FTP 指令传送和响应	50、51 等	51042	21
数据连接的释放	154	51042	21
控制连接的释放	224	51042	21

4. FTP-WEB 默认是工作在被动模式的，而防火墙映射一般可能只开了 20 和 21 端口，这时用浏览器访问 FTP 服务器就不行，只能使用 DOS 访问（主动模式）

5. FTP 中，采用匿名帐户时，user 为 anonymous

6 （1）TCP 连接建立时，客户端与服务器都处于 CLOSED 状态，此时客户端主动打

开连接，向服务器发出连接请求报文；服务器收到请求报文后，若同意连接则发出确认报文；客户端收到确认后，再向服务器发送确认报文，表示已经收到确认；服务器再次收到确认后双方就可以开始通信。而终止连接时，也是由客户端开始先发出连接释放报文，并停止发送数据；服务器接收到连接释放报文后，发送确认报文，进入关闭等待状态；客户端收到服务器的确认请求后，进入终止等待状态；服务器将最后的数据发送完毕后，向客户端发送连接释放报文，服务器此时在进行最后确认；客户端收到服务器的连接释放报文后，再次发出确认（客户端在等待一段最长报文段寿命时间后自动CLOSE）；服务器收到客户端发出的确认后就立即进入 CLOSED 状态（服务器结束连接的时间要比客户端稍早一些）

（2）从捕获的数据包来看，TCP 正确的进行了三次握手来建立连接，并通过四次挥手终止了连接。

实验思考

1.数据连接与控制连接

客户端希望与 FTP 服务器建立上传下载的数据传输时要首先向 21 端口发起建立连接的请求，此时为控制连接；控制连接建立后，就可以开始传输文件，此时为数据连接（有主动、被动两种方式）

2.ftp 与 http

一般来看，http 协议是面向网页的，而 ftp 协议是面向文件的。相比 http 来说，ftp 要更为复杂，因为 ftp 协议要用到两个 tcp 连接：控制与数据，而 http 协议的所有传输都可用同一 tcp 连接。在传输的数据格式上它们也有差别：ftp 能传输 acsii 或二进制格式的数据，而 http 只使用二进制格式。在效率上，http 有持久连接：维护单个连接，通过它来进行任意数量的数据传输；而 ftp 每次有传输数据的需要时都创建一个新的连接，耗费了很多时间。

3.ftp 的安全问题

从抓到的报文显示来看，ftp 协议传输的数据是明文传输未经过加密的，这就产生了一定的安全问题，通过抓包可以直接看到用户登录时的账户名、密码，这样就很容易受到攻击。

4.捕获主机内部发送的 FTP 数据包

使用 wireshark 监听 loopback 环回地址就可以捕获同一台主机作为服务器和客户端时发送的数据包了。

(3) Telnet 协议分析结果

1. 第一个 Telnet 协议数据是进行选项协商。进行了以下协商：

请求类型	请求类型代码	选项名	选项代码	意义
Will	251	Authentication Option	37	登录验证选项
Do	253	Suppress Go Ahead	3	抑制前进选项
Will	251	Terminal Type	24	终端类型选项
Will	251	Negotiate About Window Size	31	窗口尺寸选项
Will	251	Terminal Speed	32	终端速度选项

请求类型	请求类型代码	选项名	选项代码	意义
Will	251	Remote Flow Control	33	流控制选项
Will	251	Linemode	34	编辑/发信选项
Will	251	New Environment Option	39	环境变量
Do	253	Status	5	Telnet 的状态选项
Will	251	X Display Location	35	X 视窗地址

2. 同上表

3. Telnet 服务器 23 端口

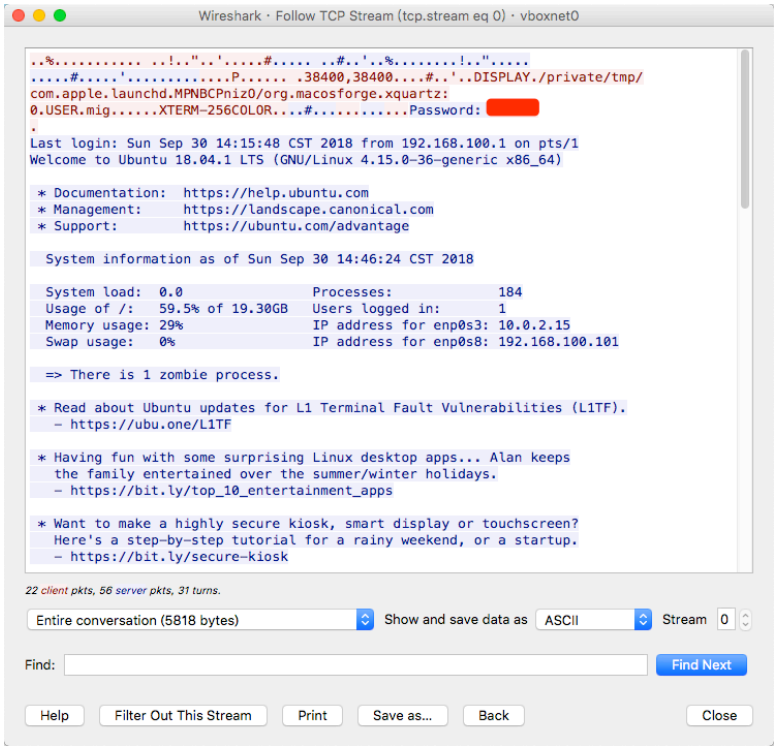
4.

过程	报文号	功能	信息及参数	报文作用
Telnet 选项协商	16	选项协商	Won't Echo	客户机不会回送接受内容
	19	选项协商	Do Echo	客户机希望接收方回送接受内容
	12	选项协商	Subotion New Environment Option	设置环境变量
	12	选项协商	Suboption Terminal Type	设置终端类型
Telnet 数据传输	81	数据传输	v	传送字符 v
	84	数据传输	i	传送字符 i
	87	数据传输	m	传送字符 m
	90	数据传输	\r	传送字符\r

5. 远程桌面不使用明文传输密码

6. 是，如图，涂红部分即为明文传输的密码：

计算机网络实验报告


Wireshark · Follow TCP Stream (tcp.stream eq 0) · vboxnet0
..%.......... ..!.."..'.....#..... ..#..'..%.......!.."..... .....#.....'.............P..... .38400,38400....#..'..DISPLAY./private/tmp/com.apple.launchd.MPNBCPniz0/org.macosforge.xquartz:0.USER.mig.....XTERM-256COLOR....#.....Password:
.
Last login: Sun Sep 30 14:15:48 CST 2018 from 192.168.100.1 on pts/1
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-36-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Sun Sep 30 14:46:24 CST 2018
System load: 0.0 Processes: 184
Usage of /: 59.5% of 19.30GB Users logged in: 1
Memory usage: 29% IP address for enp0s3: 10.0.2.15
Swap usage: 0% IP address for enp0s8: 192.168.100.101
=> There is 1 zombie process.
* Read about Ubuntu updates for L1 Terminal Fault Vulnerabilities (L1TF).
- https://ubu.one/L1TF
* Having fun with some surprising Linux desktop apps... Alan keeps the family entertained over the summer/winter holidays.
- https://bit.ly/top_10_entertainment_apps
* Want to make a highly secure kiosk, smart display or touchscreen? Here's a step-by-step tutorial for a rainy weekend, or a startup.
- https://bit.ly/secure-kiosk
22 client pkts, 56 server pkts, 31 turns.
Entire conversation (5818 bytes)
Show and save data as
ASCII
Stream
0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close