Name: Kevin McKnight

Introduction

This lab will introduce how to capture packets and interpret them when performing network forensics. I will also examine how to use a graphical network analyzer to interpret the results.

Objective

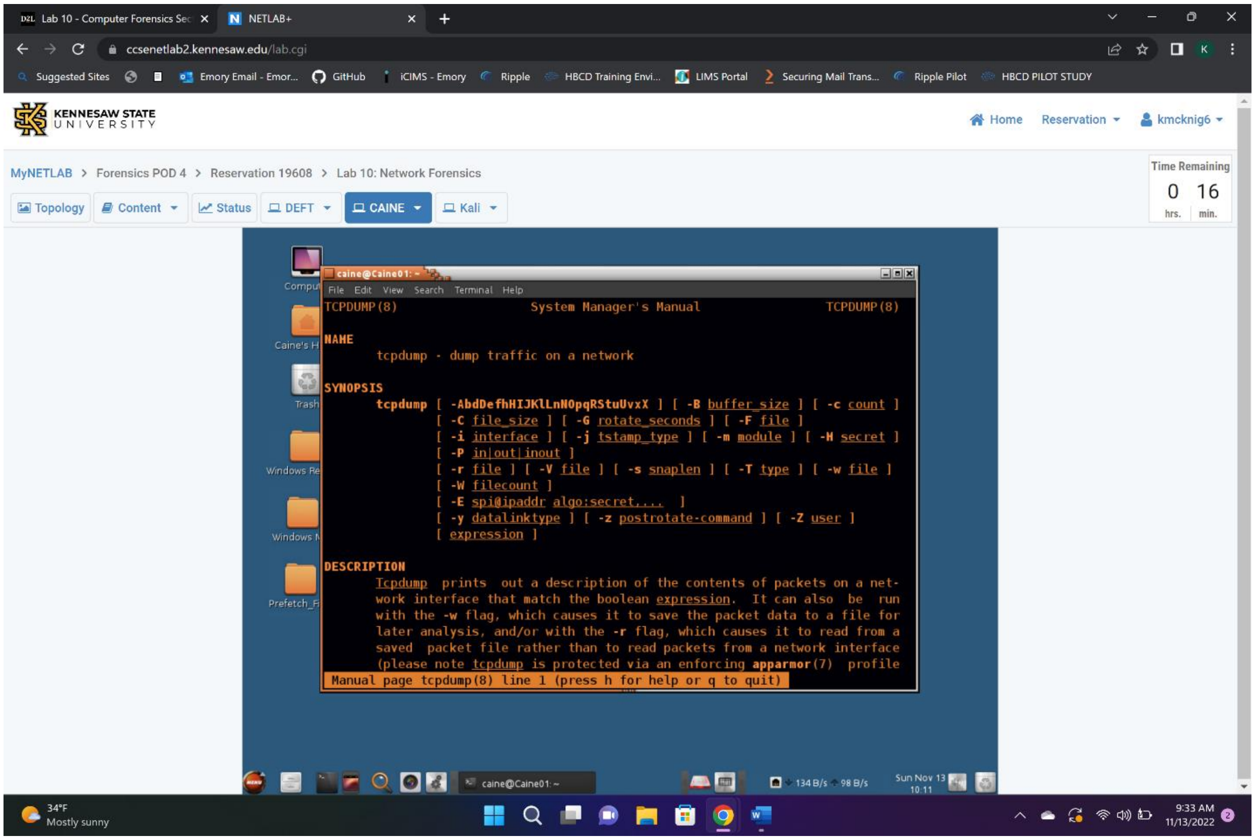
In this lab, I will be conducting forensic practices using various tools. I will be performing the following tasks:

1. Capturing and Analyzing Traffic with Tcpdump
2. Analyzing Traffic with Wireshark

LAB AND QUESTIONS

1. **Can the man command be used to learn what other commands do? If so, give an example. If not, why?**

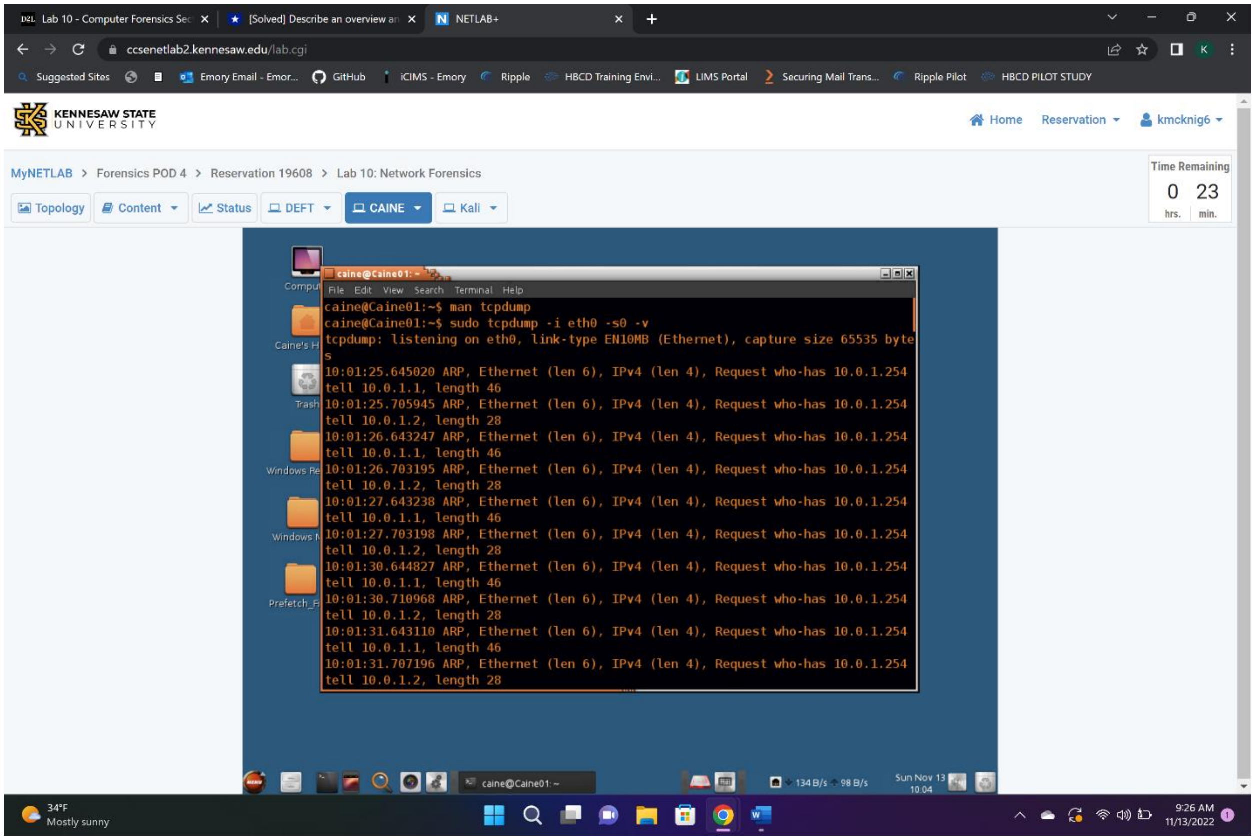
Man command in Linux is used to display the user manual of any command that we can run on the terminal. An example would be man Wireshark



```
TCPDUMP(8)                  System Manager's Manual                 TCPDUMP(8)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqRStuUvxX ] [ -B buffer_size ] [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ -P in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ expression ]

DESCRIPTION
       Tcpdump  prints  out a description of the contents of packets on a net-
       work interface that match the boolean expression.  It can also  be  run
       with the -w flag, which causes it to save the packet data to a file for
       later analysis, and/or with the -r flag, which causes it to read from a
       saved  packet file rather than to read packets from a network interface
       (please note tcpdump is protected via an enforcing apparmor(7)  profile
 Manual page tcpdump(8) line 1 (press h for help or q to quit)
```

2. Why was the sudo command used to launch tcpdump?

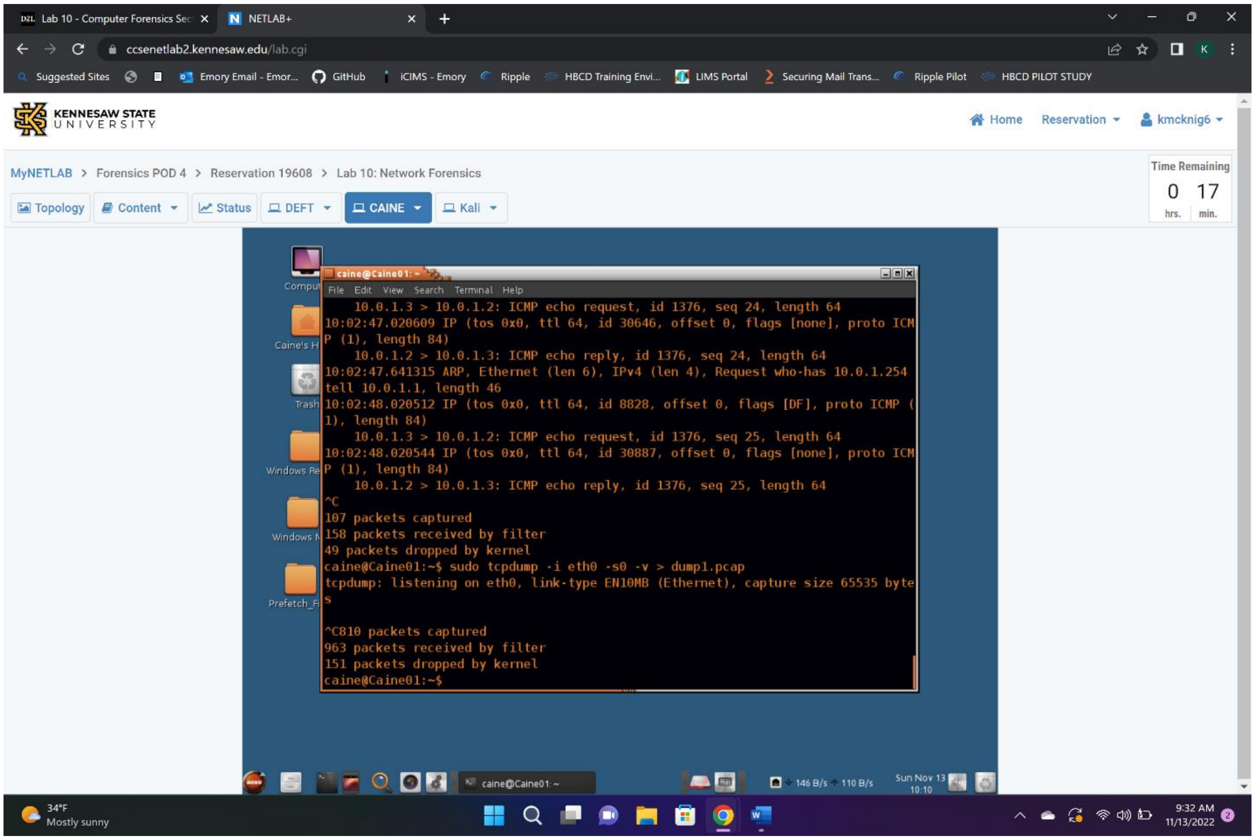
You need administrative access to run tcpdump.



```
caine@Caine01:~$ man tcpdump
caine@Caine01:~$ sudo tcpdump -i eth0 -s0 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s
10:01:25.645020 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.1, length 46
10:01:25.705945 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.2, length 28
10:01:26.643247 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.1, length 46
10:01:26.703195 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.2, length 28
10:01:27.643238 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.1, length 46
10:01:27.703198 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.2, length 28
10:01:30.644827 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.1, length 46
10:01:30.710968 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.2, length 28
10:01:31.643110 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.1, length 46
10:01:31.707196 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.2, length 28
```

3. **Take a screenshot of the Step 12, Page 8. In step 11 you typed a command. If you had to explain to a non-technical person what each step in this command does, how would you do it?**

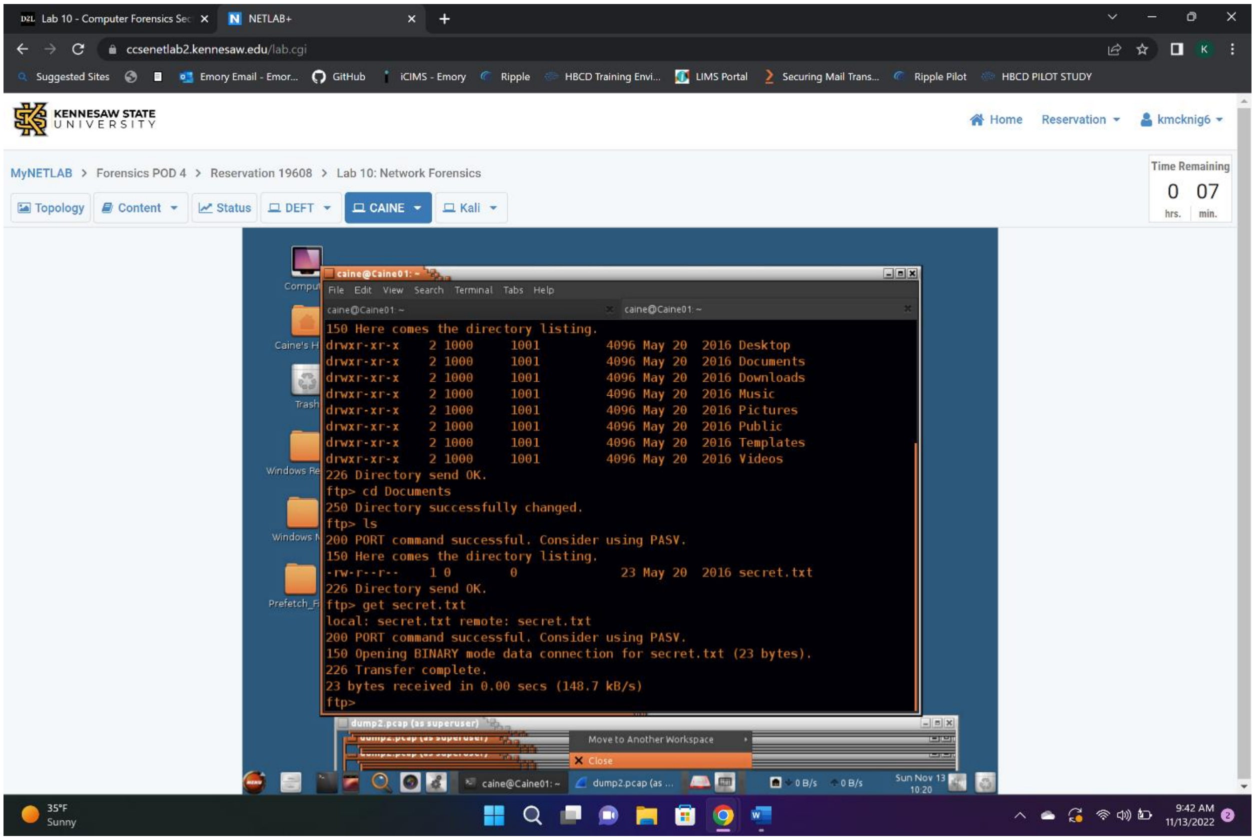
   This command saves the file capture.


Lab 10 - Computer Forensics Sec
NETLAB+
ccsenetlab2.kennesaw.edu/lab.cgi
KENNESAW STATE UNIVERSITY
Home
Reservation
kmcknig6
MyNETLAB > Forensics POD 4 > Reservation 19608 > Lab 10: Network Forensics
Time Remaining
0 hrs. 17 min.
Topology
Content
Status
DEFT
CAINE
Kali
caine@Caine01: ~
File Edit View Search Terminal Help
Sun Nov 13 10:10
34°F Mostly sunny
9:32 AM 11/13/2022

```
    10.0.1.3 > 10.0.1.2: ICMP echo request, id 1376, seq 24, length 64
10:02:47.020609 IP (tos 0x0, ttl 64, id 30646, offset 0, flags [none], proto ICM
P (1), length 84)
    10.0.1.2 > 10.0.1.3: ICMP echo reply, id 1376, seq 24, length 64
10:02:47.641315 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.1.254
tell 10.0.1.1, length 46
10:02:48.020512 IP (tos 0x0, ttl 64, id 8828, offset 0, flags [DF], proto ICMP (
1), length 84)
    10.0.1.3 > 10.0.1.2: ICMP echo request, id 1376, seq 25, length 64
10:02:48.020544 IP (tos 0x0, ttl 64, id 30887, offset 0, flags [none], proto ICM
P (1), length 84)
    10.0.1.2 > 10.0.1.3: ICMP echo reply, id 1376, seq 25, length 64
^C
107 packets captured
158 packets received by filter
49 packets dropped by kernel
caine@Caine01:~$ sudo tcpdump -i eth0 -s0 -v > dump1.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte
s

^C810 packets captured
963 packets received by filter
151 packets dropped by kernel
caine@Caine01:~$
```

4. **If the “get” command is used to download a file from a terminal, what command is used to upload a file?**

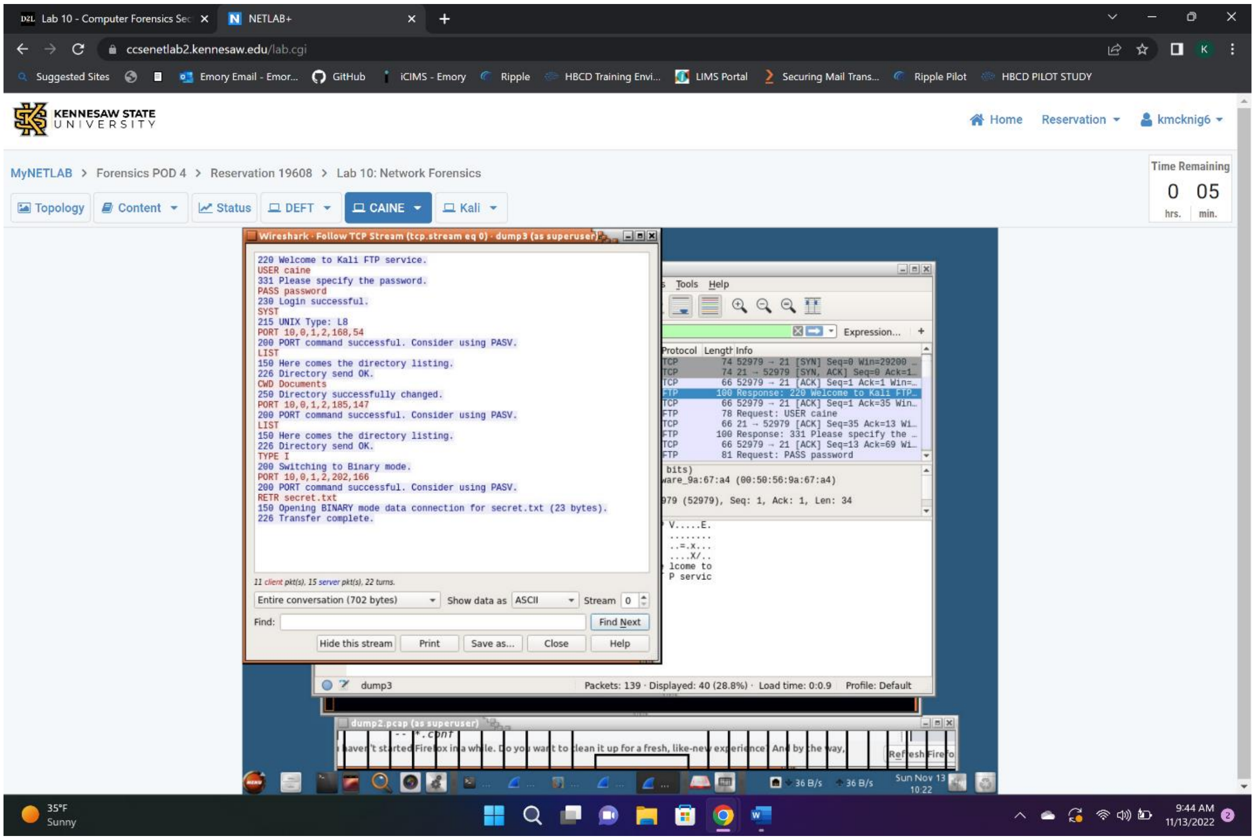
scp



```
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Desktop
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Documents
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Downloads
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Music
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Pictures
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Public
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Templates
drwxr-xr-x    2 1000     1001         4096 May 20  2016 Videos
226 Directory send OK.
ftp> cd Documents
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              23 May 20  2016 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for secret.txt (23 bytes).
226 Transfer complete.
23 bytes received in 0.00 secs (148.7 kB/s)
ftp>
```

5. **In this screenshot you can view everything in cleartext. To avoid items being viewed in cleartext, what option or port could you use with FTP to make it more secure?**

Port 990


Lab 10 - Computer Forensics Sec
NETLAB+
ccsenetlab2.kennesaw.edu/lab.cgi
Suggested Sites
Emory Email - Emor...
GitHub
iCIMS - Emory
Ripple
HBCD Training Envi...
LIMS Portal
Securing Mail Trans...
Ripple Pilot
HBCD PILOT STUDY
KENNESAW STATE UNIVERSITY
Home
Reservation
kmcknig6
MyNETLAB > Forensics POD 4 > Reservation 19608 > Lab 10: Network Forensics
Time Remaining 0 hrs. 05 min.
Topology
Content
Status
DEFT
CAINE
Kali
Wireshark · Follow TCP Stream (tcp.stream eq 0) · dump3 (as superuser)

```
220 Welcome to Kali FTP service.
USER caine
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,1,2,168,54
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD Documents
250 Directory successfully changed.
PORT 10,0,1,2,185,147
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 10,0,1,2,202,166
200 PORT command successful. Consider using PASV.
RETR secret.txt
150 Opening BINARY mode data connection for secret.txt (23 bytes).
226 Transfer complete.
```

11 client pkt(s), 15 server pkt(s), 22 turns.

Entire conversation (702 bytes) · Show data as: ASCII · Stream: 0

```
Protocol Length Info
TCP        74 52979 → 21 [SYN] Seq=0 Win=29200 …
TCP        74 21 → 52979 [SYN, ACK] Seq=0 Ack=1…
TCP        66 52979 → 21 [ACK] Seq=1 Ack=1 Win=…
FTP       100 Response: 220 Welcome to Kali FTP…
TCP        66 52979 → 21 [ACK] Seq=1 Ack=35 Win…
FTP        78 Request: USER caine
TCP        66 21 → 52979 [ACK] Seq=35 Ack=13 Wi…
FTP       100 Response: 331 Please specify the …
TCP        66 52979 → 21 [ACK] Seq=13 Ack=69 Wi…
FTP        81 Request: PASS password
 bits)
ware_9a:67:a4 (00:50:56:9a:67:a4)
979 (52979), Seq: 1, Ack: 1, Len: 34
 V.....E.
 ........
 ..=.x...
 ....X/..
 lcome to
 P servic
```

dump3 · Packets: 139 · Displayed: 40 (28.8%) · Load time: 0:0.9 · Profile: Default

dump2.pcap (as superuser)
*.conf
haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way,
Refresh Firefox
36 B/s
36 B/s
Sun Nov 13 10:22
35°F Sunny
9:44 AM 11/13/2022