# COMP7006: Lab 5
# Shell Scripting

Kevin Lo, A00952922

10-27-2020

# Table of Contents

Introduction .......... 2

Basic Design .......... 3

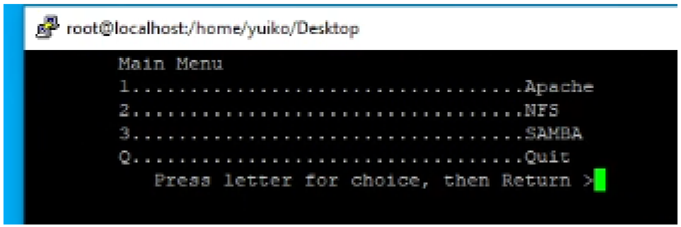
Task 1: Apache .......... 5

Task 2: NFS .......... 8

Task 3: Samba .......... 10

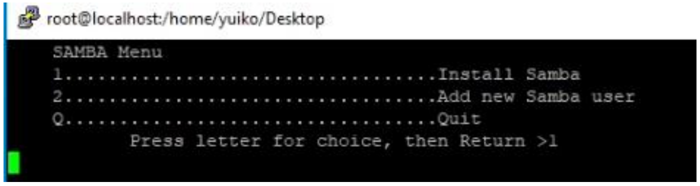
## Introduction

In this lab, I created a shell script to automate installing, Apache, NFS and Samba and sets up the system for the user with the basic user inputs of username and password. I the shell script I created displays a simple menu where the user inputs the corresponding number for their choice and to enter “q” to exit



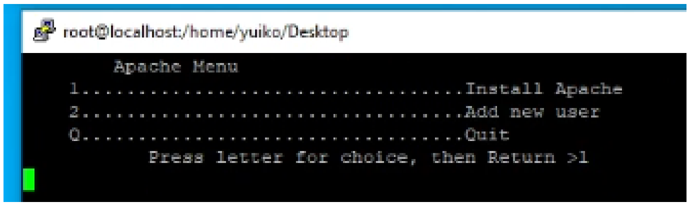
root@localhost:/home/yuiko/Desktop

```
        Main Menu
        1.................................Apache
        2.................................NFS
        3.................................SAMBA
        Q.................................Quit
           Press letter for choice, then Return >
```



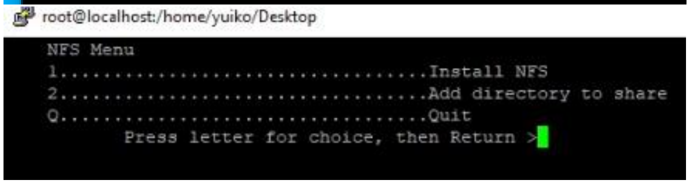
root@localhost:/home/yuiko/Desktop

```
    SAMBA Menu
    1.................................Install Samba
    2.................................Add new Samba user
    Q.................................Quit
          Press letter for choice, then Return >1
```



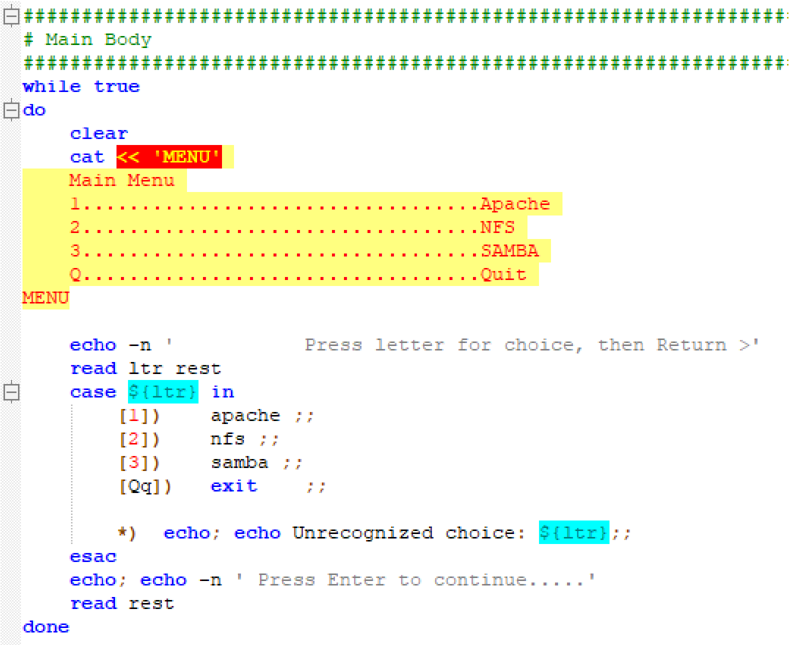
root@localhost:/home/yuiko/Desktop

```
        Apache Menu
    1.................................Install Apache
    2.................................Add new user
    Q.................................Quit
          Press letter for choice, then Return >1
```



root@localhost:/home/yuiko/Desktop

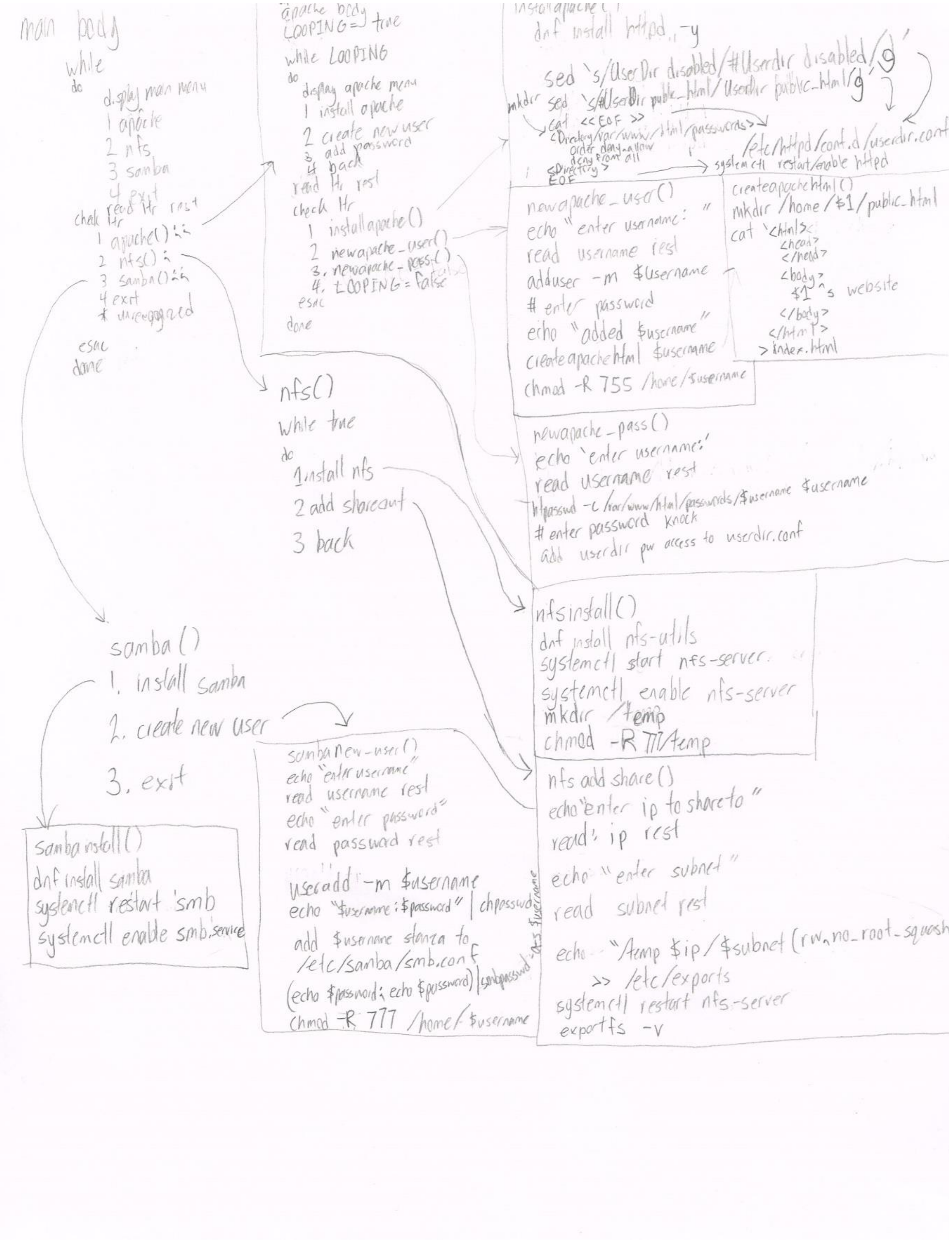
```
   NFS Menu
   1.................................Install NFS
   2.................................Add directory to share
   Q.................................Quit
         Press letter for choice, then Return >
```



```
#################################################################
# Main Body
#################################################################
while true
do
    clear
    cat << 'MENU'
    Main Menu
    1.................................Apache
    2.................................NFS
    3.................................SAMBA
    Q.................................Quit
MENU

    echo -n '            Press letter for choice, then Return >'
    read ltr rest
    case ${ltr} in
        [1])      apache ;;
        [2])      nfs ;;
        [3])      samba ;;
        [Qq])     exit    ;;

        *)  echo; echo Unrecognized choice: ${ltr};;
    esac
    echo; echo -n ' Press Enter to continue.....'
    read rest
done
```

## Basic Design

The basic design was first created on paper then refined more



```
main body
while
do
    display main menu
    1 apache
    2 nfs
    3 samba
    4 exit
  read Hr rest
chek Hr
    1 apache() ;;
    2 nfs() ;
    3 samba() ;;
    4 exit
    * unrecognized
  esac
  done
```

```
apache body
LOOPING = true
while LOOPING
do
  display apache menu
  1 install apache
  2 create new user
  3 add password
  4 back
 read Hr rest
 check Hr
  1 installapache()
  2 newapache_user()
  3. newapache_pass()
  4. LOOPING = false
 esac
done
```

```
installapache()
  dnf install httpd -y
  sed `s/UserDir disabled/#Userdir disabled/g'
mkdir sed `s/#UserDir public_html/Userdir public_html/g'
  cat << EOF >>
  <Directory/var/www/html/passwords>
      order deny,allow
      deny from all
  </Directory>
  EOF
                /etc/httpd/conf.d/userdir.conf
                systemctl restart/enable httpd
```

```
newapache_user()
echo "enter username: "
read username rest
adduser -m $Username
# enter password
echo "added $username"
createapachehtml $username
chmod -R 755 /home/$username
```

```
createapachehtml()
mkdir /home/$1/public_html
cat `<html>
      <head>
      </head>
      <body>
        $1^s website
      </body>
     </html>
   > index.html
```

```
nfs()
while true
do
  1 install nfs
  2 add shareout
  3 back
```

```
newapache_pass()
echo `enter username:'
read username rest
htpasswd -c /var/www/html/passwords/$username $username
# enter password knock
add userdir pw access to userdir.conf
```

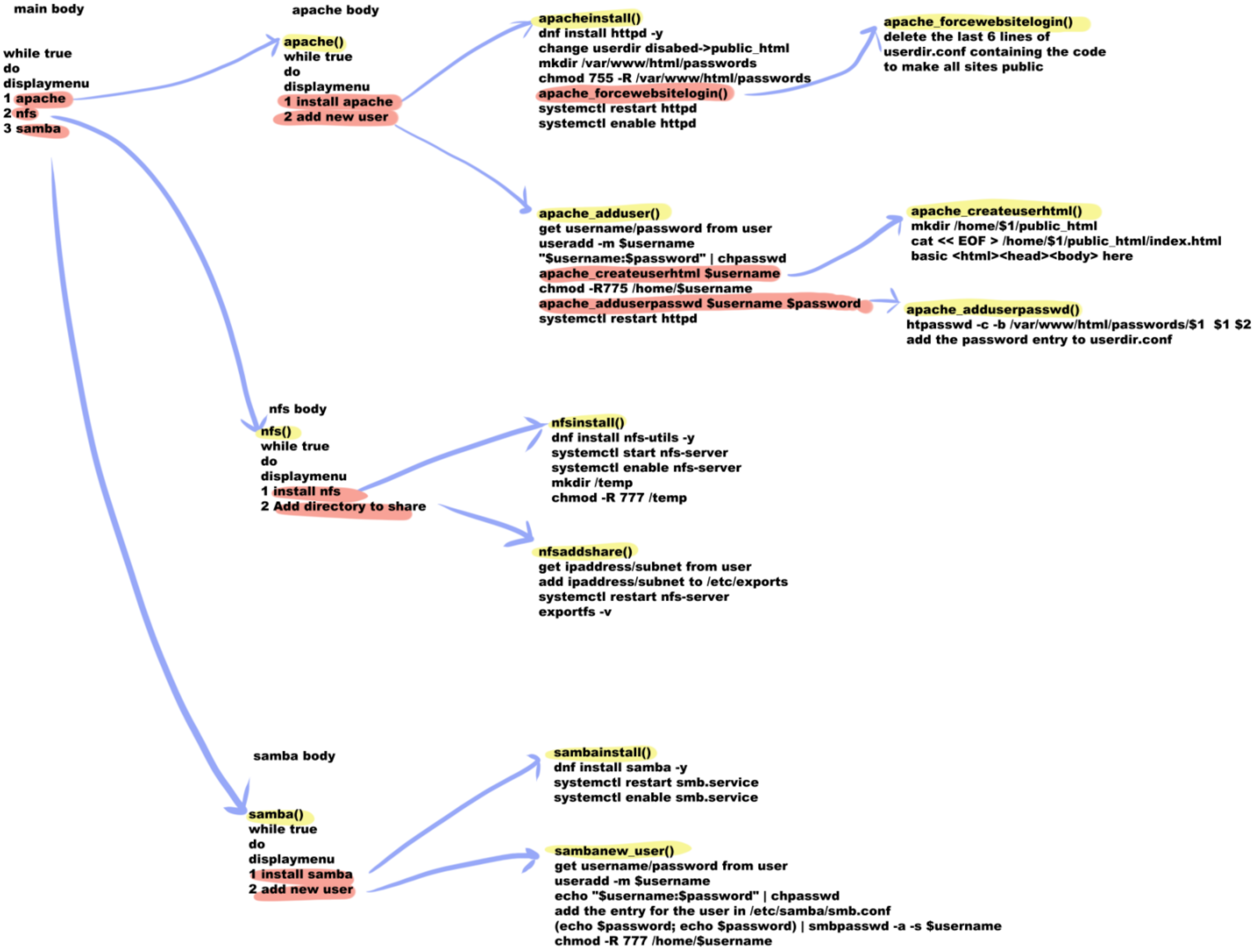
```
nfsinstall()
dnf install nfs-utils
systemctl start nfs-server
systemctl enable nfs-server
mkdir /temp
chmod -R 777/temp
```

```
samba()
1. install samba
2. create new user
3. exit
```

```
sambainstall()
dnf install samba
systemctl restart smb
systemctl enable smb.service
```

```
sambanew-user()
echo "enter username"
read username rest
echo "enter password"
read password rest

useradd -m $username
echo "$username:$password" | chpasswd
add $username stanza to
/etc/samba/smb.conf
(echo $password; echo $password) | smbpasswd -a -s $username
chmod -R 777 /home/$username
```

```
nfs add share()
echo "enter ip to share to"
read ip rest
echo "enter subnet"
read subnet rest
echo "/temp $ip/$subnet (rw,no_root_squash
    >> /etc/exports
systemctl restart nfs-server
exportfs -v
```



main body

```
while true
do
displaymenu
1 apache
2 nfs
3 samba
```

apache body

```
apache()
while true
do
displaymenu
1 install apache
2 add new user
```

```
apacheinstall()
dnf install httpd -y
change userdir disabed->public_html
mkdir /var/www/html/passwords
chmod 755 -R /var/www/html/passwords
apache_forcewebsitelogin()
systemctl restart httpd
systemctl enable httpd
```

```
apache_forcewebsitelogin()
delete the last 6 lines of
userdir.conf containing the code
to make all sites public
```

```
apache_adduser()
get username/password from user
useradd -m $username
"$username:$password" | chpasswd
apache_createuserhtml $username
chmod -R775 /home/$username
apache_adduserpasswd $username $password
systemctl restart httpd
```

```
apache_createuserhtml()
mkdir /home/$1/public_html
cat << EOF > /home/$1/public_html/index.html
basic <html><head><body> here
```

```
apache_adduserpasswd()
htpasswd -c -b /var/www/html/passwords/$1  $1 $2
add the password entry to userdir.conf
```

nfs body

```
nfs()
while true
do
displaymenu
1 install nfs
2 Add directory to share
```

```
nfsinstall()
dnf install nfs-utils -y
systemctl start nfs-server
systemctl enable nfs-server
mkdir /temp
chmod -R 777 /temp
```

```
nfsaddshare()
get ipaddress/subnet from user
add ipaddress/subnet to /etc/exports
systemctl restart nfs-server
exportfs -v
```

samba body

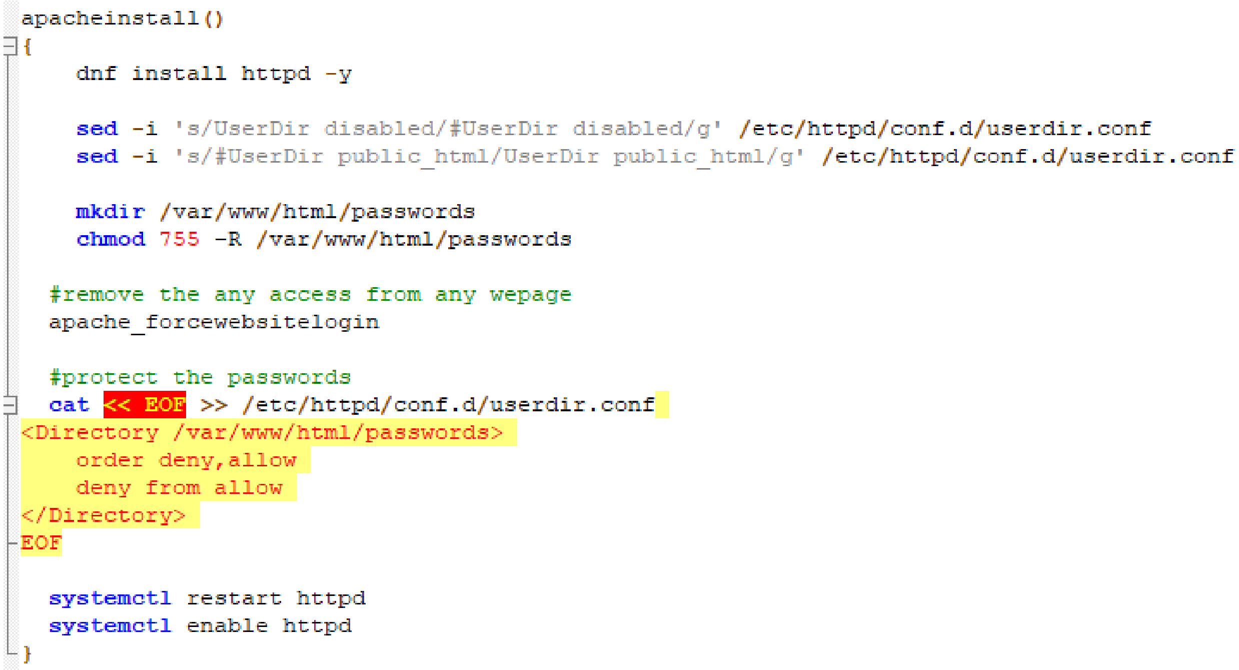
```
samba()
while true
do
displaymenu
1 install samba
2 add new user
```

```
sambainstall()
dnf install samba -y
systemctl restart smb.service
systemctl enable smb.service
```

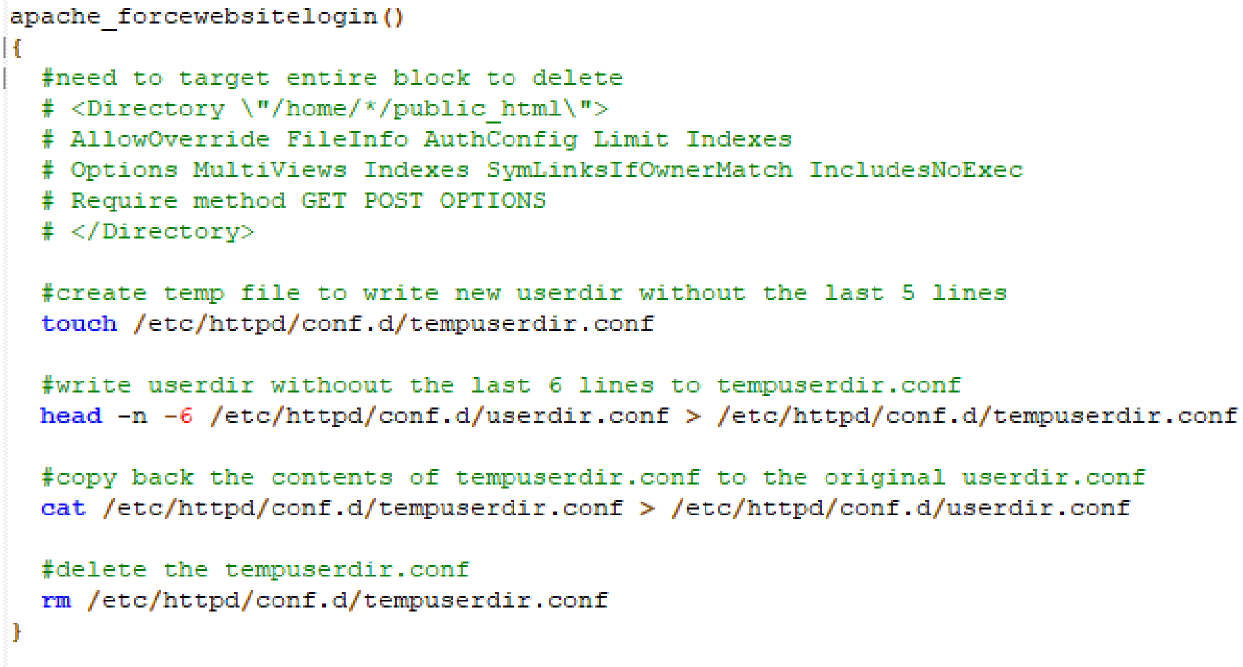
```
sambanew_user()
get username/password from user
useradd -m $username
echo "$username:$password" | chpasswd
add the entry for the user in /etc/samba/smb.conf
(echo $password; echo $password) | smbpasswd -a -s $username
chmod -R 777 /home/$username
```

## Task 1: Apache

Apache installation was done by first doing the **dnf install httpd -y** then removing the 6 lines containing the code to enable public viewing and adding in the code for the sites to require passwords.

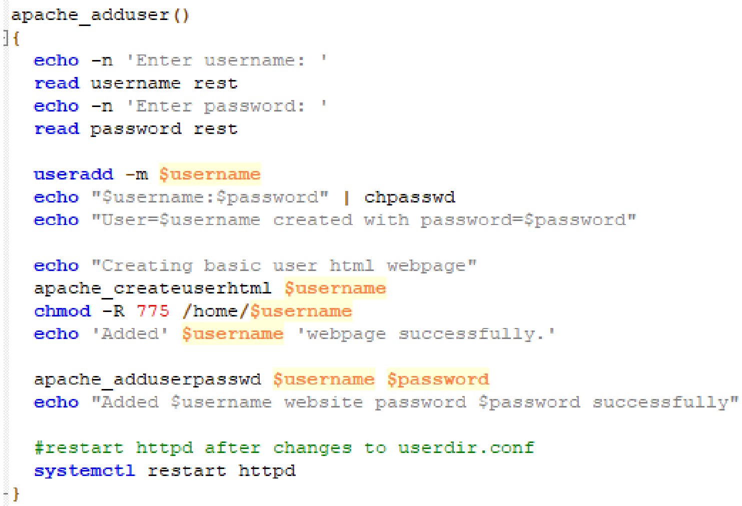


```
apacheinstall()
{
    dnf install httpd -y

    sed -i 's/UserDir disabled/#UserDir disabled/g' /etc/httpd/conf.d/userdir.conf
    sed -i 's/#UserDir public_html/UserDir public_html/g' /etc/httpd/conf.d/userdir.conf

    mkdir /var/www/html/passwords
    chmod 755 -R /var/www/html/passwords

  #remove the any access from any wepage
  apache_forcewebsitelogin

  #protect the passwords
  cat << EOF >> /etc/httpd/conf.d/userdir.conf
<Directory /var/www/html/passwords>
    order deny,allow
    deny from allow
</Directory>
EOF

  systemctl restart httpd
  systemctl enable httpd
}
```

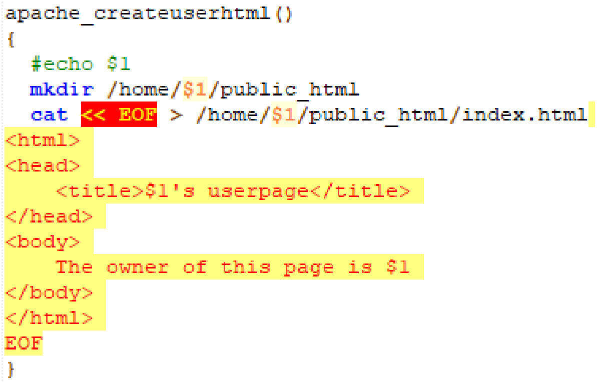


```
apache_forcewebsitelogin()
{
  #need to target entire block to delete
  # <Directory \"/home/*/public_html\">
  # AllowOverride FileInfo AuthConfig Limit Indexes
  # Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
  # Require method GET POST OPTIONS
  # </Directory>

  #create temp file to write new userdir without the last 5 lines
  touch /etc/httpd/conf.d/tempuserdir.conf

  #write userdir withoout the last 6 lines to tempuserdir.conf
  head -n -6 /etc/httpd/conf.d/userdir.conf > /etc/httpd/conf.d/tempuserdir.conf

  #copy back the contents of tempuserdir.conf to the original userdir.conf
  cat /etc/httpd/conf.d/tempuserdir.conf > /etc/httpd/conf.d/userdir.conf

  #delete the tempuserdir.conf
  rm /etc/httpd/conf.d/tempuserdir.conf
}
```

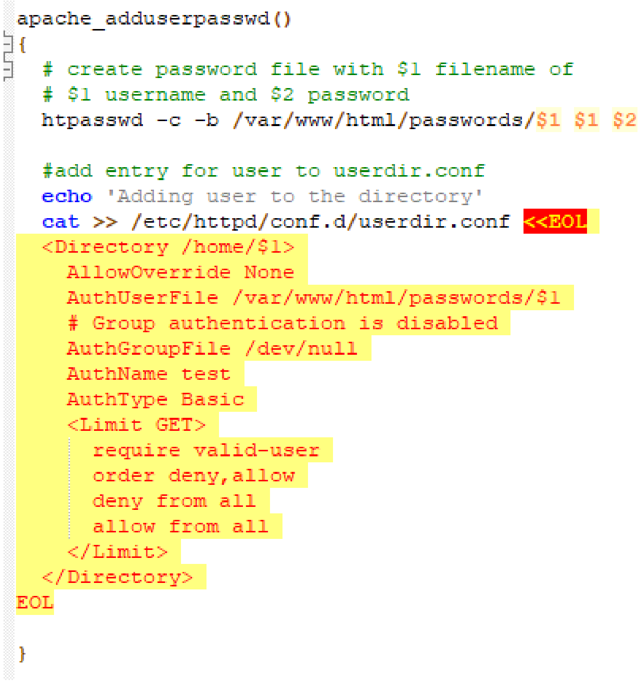
Adding users was created by first asking the user to enter a username and password then automatically entering the required fields for the user automatically along with creating an entry for the new user in **/etc/httpd/conf. d/userdir.conf**



```
apache_adduser()
{
  echo -n 'Enter username: '
  read username rest
  echo -n 'Enter password: '
  read password rest

  useradd -m $username
  echo "$username:$password" | chpasswd
  echo "User=$username created with password=$password"

  echo "Creating basic user html webpage"
  apache_createuserhtml $username
  chmod -R 775 /home/$username
  echo 'Added' $username 'webpage successfully.'

  apache_adduserpasswd $username $password
  echo "Added $username website password $password successfully"

  #restart httpd after changes to userdir.conf
  systemctl restart httpd
}
```

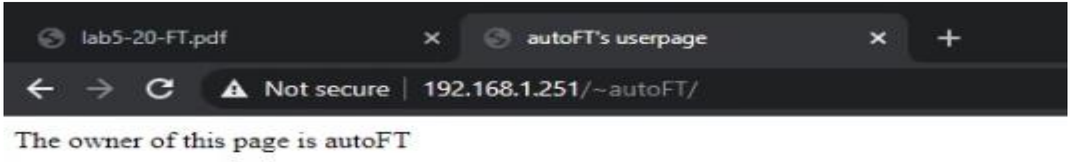


```
apache_createuserhtml()
{
  #echo $1
  mkdir /home/$1/public_html
  cat << EOF > /home/$1/public_html/index.html
<html>
<head>
    <title>$1's userpage</title>
</head>
<body>
    The owner of this page is $1
</body>
</html>
EOF
}
```

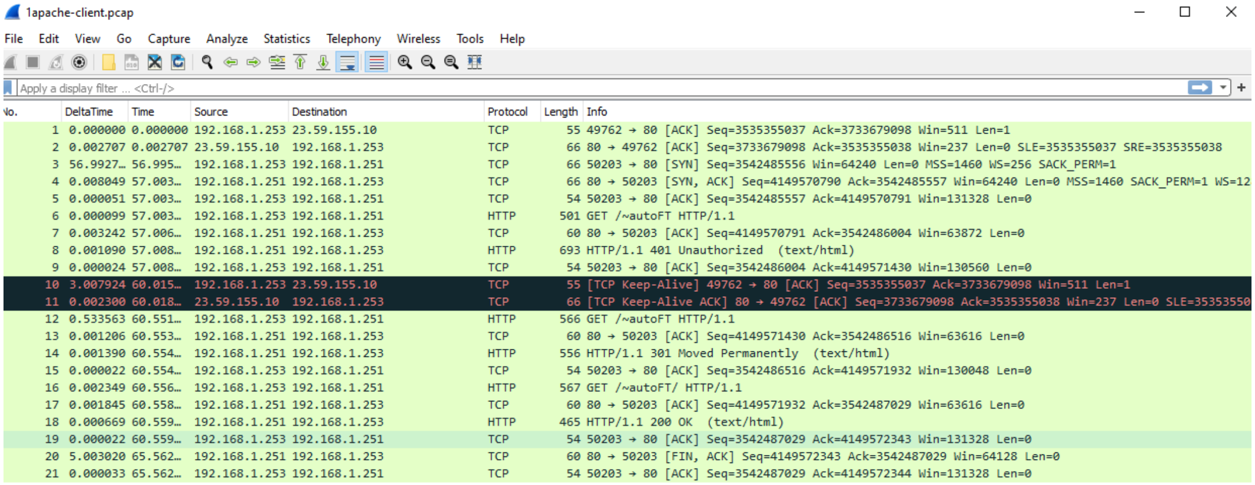


```
apache_adduserpasswd()
{
  # create password file with $1 filename of
  # $1 username and $2 password
  htpasswd -c -b /var/www/html/passwords/$1 $1 $2

  #add entry for user to userdir.conf
  echo 'Adding user to the directory'
  cat >> /etc/httpd/conf.d/userdir.conf <<EOL
  <Directory /home/$1>
    AllowOverride None
    AuthUserFile /var/www/html/passwords/$1
    # Group authentication is disabled
    AuthGroupFile /dev/null
    AuthName test
    AuthType Basic
    <Limit GET>
      require valid-user
      order deny,allow
      deny from all
      allow from all
    </Limit>
  </Directory>
EOL

}
```

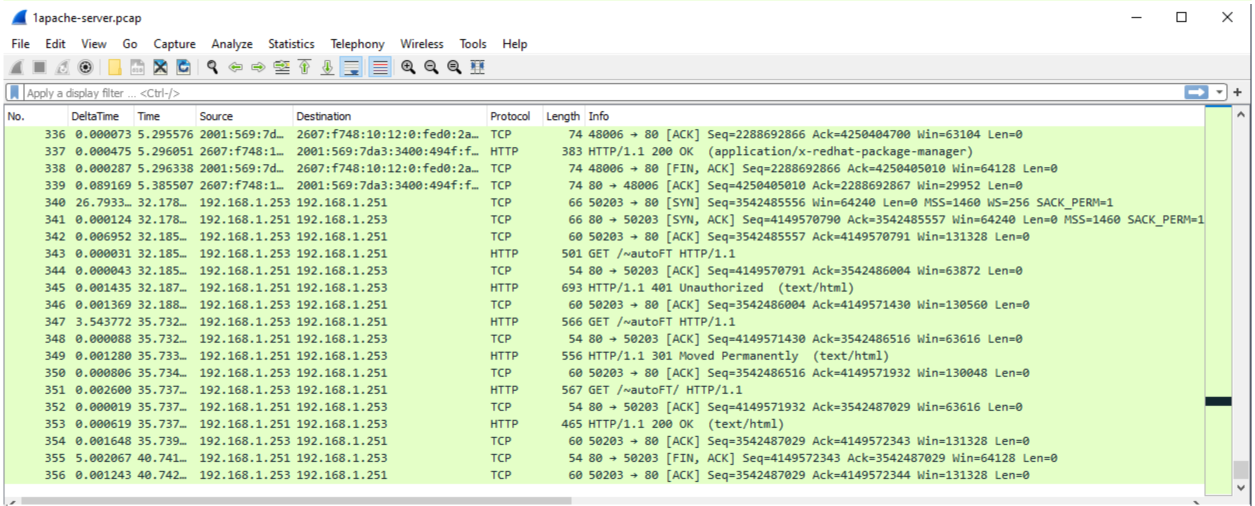
The resulting is the following output when installing Apache and accessing the site



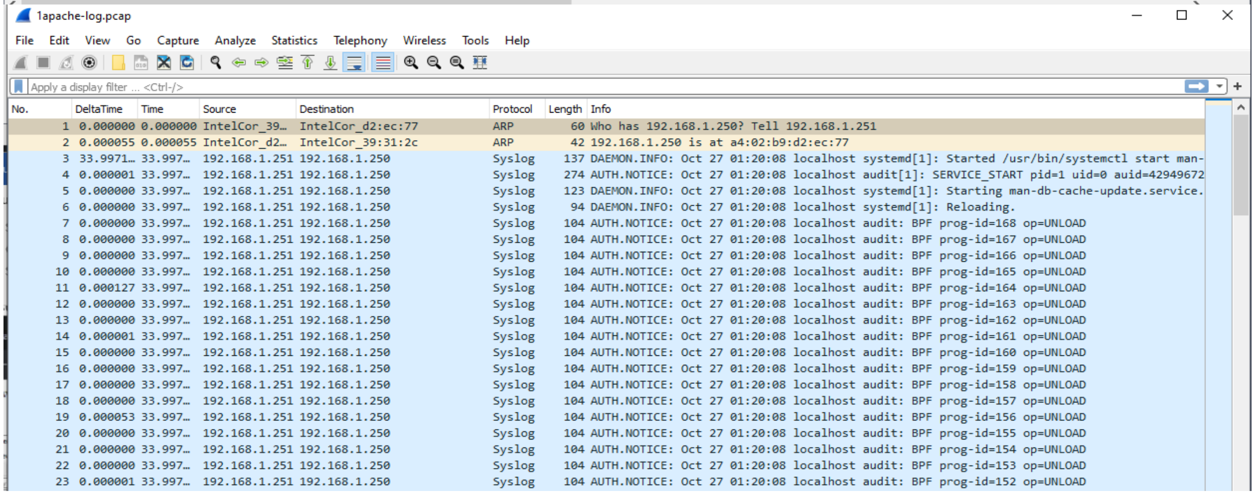
The owner of this page is autoFT


1apache-client.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time     Source        Destination   Protocol Length Info
    1 0.000000 0.000000 192.168.1.253 23.59.155.10  TCP        55 49762 → 80 [ACK] Seq=3535355037 Ack=3733679098 Win=511 Len=1
    2 0.002707 0.002707 23.59.155.10  192.168.1.253 TCP        66 80 → 49762 [ACK] Seq=3733679098 Ack=3535355038 Win=237 Len=0 SLE=3535355037 SRE=3535355038
    3 56.9927… 56.995… 192.168.1.253 192.168.1.251 TCP        66 50203 → 80 [SYN] Seq=3542485556 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    4 0.008049 57.003… 192.168.1.251 192.168.1.253 TCP        66 80 → 50203 [SYN, ACK] Seq=4149570790 Ack=3542485557 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=12
    5 0.000051 57.003… 192.168.1.253 192.168.1.251 TCP        54 50203 → 80 [ACK] Seq=3542485557 Ack=4149570791 Win=131328 Len=0
    6 0.000099 57.003… 192.168.1.253 192.168.1.251 HTTP      501 GET /~autoFT HTTP/1.1
    7 0.003242 57.006… 192.168.1.251 192.168.1.253 TCP        60 80 → 50203 [ACK] Seq=4149570791 Ack=3542486004 Win=63872 Len=0
    8 0.001090 57.008… 192.168.1.251 192.168.1.253 HTTP      693 HTTP/1.1 401 Unauthorized  (text/html)
    9 0.000024 57.008… 192.168.1.253 192.168.1.251 TCP        54 50203 → 80 [ACK] Seq=3542486004 Ack=4149571430 Win=130560 Len=0
   10 3.007924 60.015… 192.168.1.253 23.59.155.10  TCP        55 [TCP Keep-Alive] 49762 → 80 [ACK] Seq=3535355037 Ack=3733679098 Win=511 Len=1
   11 0.002300 60.018… 23.59.155.10  192.168.1.253 TCP        66 [TCP Keep-Alive ACK] 80 → 49762 [ACK] Seq=3733679098 Ack=3535355038 Win=237 Len=0 SLE=35353550
   12 0.533563 60.551… 192.168.1.253 192.168.1.251 HTTP      566 GET /~autoFT HTTP/1.1
   13 0.001206 60.553… 192.168.1.251 192.168.1.253 TCP        60 80 → 50203 [ACK] Seq=4149571430 Ack=3542486516 Win=63616 Len=0
   14 0.001390 60.554… 192.168.1.251 192.168.1.253 HTTP      556 HTTP/1.1 301 Moved Permanently  (text/html)
   15 0.000022 60.554… 192.168.1.253 192.168.1.251 TCP        54 50203 → 80 [ACK] Seq=3542486516 Ack=4149571932 Win=130048 Len=0
   16 0.002349 60.556… 192.168.1.253 192.168.1.251 HTTP      567 GET /~autoFT/ HTTP/1.1
   17 0.001845 60.558… 192.168.1.251 192.168.1.253 TCP        60 80 → 50203 [ACK] Seq=4149571932 Ack=3542487029 Win=63616 Len=0
   18 0.000669 60.559… 192.168.1.251 192.168.1.253 HTTP      465 HTTP/1.1 200 OK  (text/html)
   19 0.000022 60.559… 192.168.1.253 192.168.1.251 TCP        54 50203 → 80 [ACK] Seq=3542487029 Ack=4149572343 Win=131328 Len=0
   20 5.003020 65.562… 192.168.1.251 192.168.1.253 TCP        60 80 → 50203 [FIN, ACK] Seq=4149572343 Ack=3542487029 Win=64128 Len=0
   21 0.000033 65.562… 192.168.1.253 192.168.1.251 TCP        54 50203 → 80 [ACK] Seq=3542487029 Ack=4149572344 Win=131328 Len=0
```


1apache-server.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

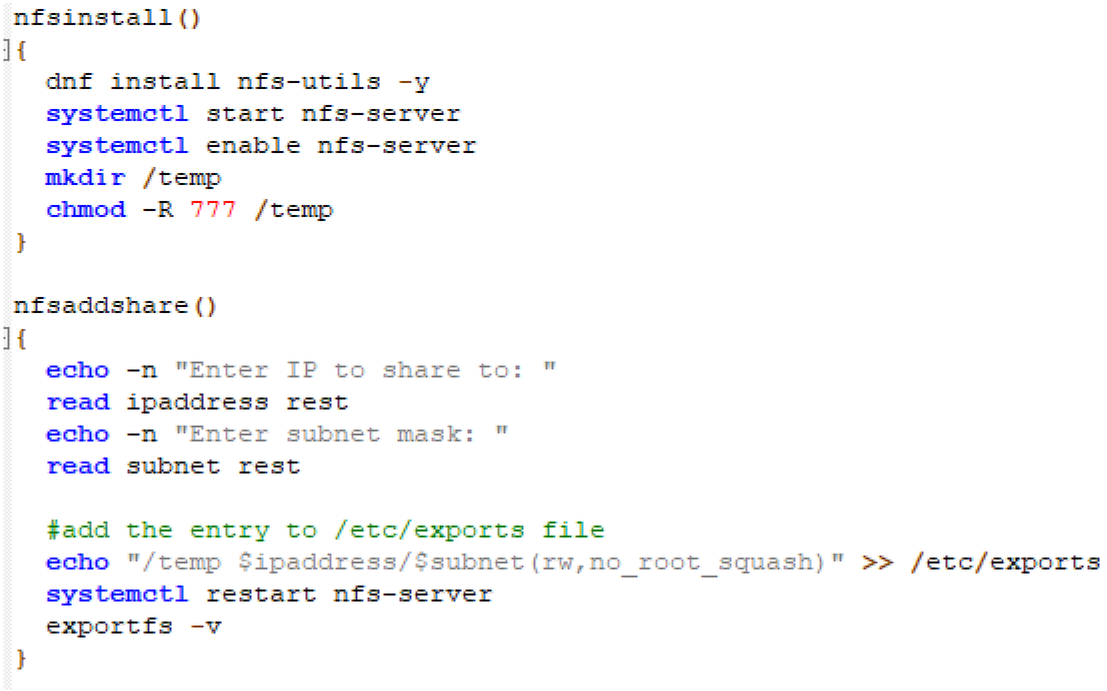
```
No.   DeltaTime Time     Source          Destination                 Protocol Length Info
  336 0.000073 5.295576 2001:569:7d…   2607:f748:10:12:0:fed0:2a…  TCP        74 48006 → 80 [ACK] Seq=2288692866 Ack=4250404700 Win=63104 Len=0
  337 0.000475 5.296051 2607:f748:1…   2001:569:7da3:3400:494f:f…  HTTP      383 HTTP/1.1 200 OK  (application/x-redhat-package-manager)
  338 0.000287 5.296338 2001:569:7d…   2607:f748:10:12:0:fed0:2a…  TCP        74 48006 → 80 [FIN, ACK] Seq=2288692866 Ack=4250405010 Win=64128 Len=0
  339 0.089169 5.385507 2607:f748:1…   2001:569:7da3:3400:494f:f…  TCP        74 80 → 48006 [ACK] Seq=4250405010 Ack=2288692867 Win=29952 Len=0
  340 26.7933… 32.178… 192.168.1.253 192.168.1.251               TCP        66 50203 → 80 [SYN] Seq=3542485556 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  341 0.000124 32.178… 192.168.1.251 192.168.1.253               TCP        66 80 → 50203 [SYN, ACK] Seq=4149570790 Ack=3542485557 Win=64240 Len=0 MSS=1460 SACK_PERM=1
  342 0.006952 32.185… 192.168.1.253 192.168.1.251               TCP        60 50203 → 80 [ACK] Seq=3542485557 Ack=4149570791 Win=131328 Len=0
  343 0.000031 32.185… 192.168.1.253 192.168.1.251               HTTP      501 GET /~autoFT HTTP/1.1
  344 0.000043 32.185… 192.168.1.251 192.168.1.253               TCP        54 80 → 50203 [ACK] Seq=4149570791 Ack=3542486004 Win=63872 Len=0
  345 0.001435 32.187… 192.168.1.251 192.168.1.253               HTTP      693 HTTP/1.1 401 Unauthorized  (text/html)
  346 0.001369 32.188… 192.168.1.253 192.168.1.251               TCP        60 50203 → 80 [ACK] Seq=3542486004 Ack=4149571430 Win=130560 Len=0
  347 3.543772 35.732… 192.168.1.253 192.168.1.251               HTTP      566 GET /~autoFT HTTP/1.1
  348 0.000088 35.732… 192.168.1.251 192.168.1.253               TCP        54 80 → 50203 [ACK] Seq=4149571430 Ack=3542486516 Win=63616 Len=0
  349 0.001280 35.733… 192.168.1.251 192.168.1.253               HTTP      556 HTTP/1.1 301 Moved Permanently  (text/html)
  350 0.000806 35.734… 192.168.1.253 192.168.1.251               TCP        60 50203 → 80 [ACK] Seq=3542486516 Ack=4149571932 Win=130048 Len=0
  351 0.002600 35.737… 192.168.1.253 192.168.1.251               HTTP      567 GET /~autoFT/ HTTP/1.1
  352 0.000019 35.737… 192.168.1.251 192.168.1.253               TCP        54 80 → 50203 [ACK] Seq=4149571932 Ack=3542487029 Win=63616 Len=0
  353 0.000619 35.737… 192.168.1.251 192.168.1.253               HTTP      465 HTTP/1.1 200 OK  (text/html)
  354 0.001648 35.739… 192.168.1.253 192.168.1.251               TCP        60 50203 → 80 [ACK] Seq=3542487029 Ack=4149572343 Win=131328 Len=0
  355 5.002067 40.741… 192.168.1.251 192.168.1.253               TCP        54 80 → 50203 [FIN, ACK] Seq=4149572343 Ack=3542487029 Win=64128 Len=0
  356 0.001243 40.742… 192.168.1.253 192.168.1.251               TCP        60 50203 → 80 [ACK] Seq=3542487029 Ack=4149572344 Win=131328 Len=0
```


1apache-log.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time     Source          Destination        Protocol Length Info
    1 0.000000 0.000000 IntelCor_39…   IntelCor_d2:ec:77  ARP        60 Who has 192.168.1.250? Tell 192.168.1.251
    2 0.000055 0.000055 IntelCor_d2…   IntelCor_39:31:2c  ARP        42 192.168.1.250 is at a4:02:b9:d2:ec:77
    3 33.9971… 33.997… 192.168.1.251 192.168.1.250      Syslog    137 DAEMON.INFO: Oct 27 01:20:08 localhost systemd[1]: Started /usr/bin/systemctl start man-
    4 0.000001 33.997… 192.168.1.251 192.168.1.250      Syslog    274 AUTH.NOTICE: Oct 27 01:20:08 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=42949672
    5 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    123 DAEMON.INFO: Oct 27 01:20:08 localhost systemd[1]: Starting man-db-cache-update.service.
    6 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog     94 DAEMON.INFO: Oct 27 01:20:08 localhost systemd[1]: Reloading.
    7 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=168 op=UNLOAD
    8 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=167 op=UNLOAD
    9 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=166 op=UNLOAD
   10 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=165 op=UNLOAD
   11 0.000127 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=164 op=UNLOAD
   12 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=163 op=UNLOAD
   13 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=162 op=UNLOAD
   14 0.000001 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=161 op=UNLOAD
   15 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=160 op=UNLOAD
   16 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=159 op=UNLOAD
   17 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=158 op=UNLOAD
   18 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=157 op=UNLOAD
   19 0.000053 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=156 op=UNLOAD
   20 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=155 op=UNLOAD
   21 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=154 op=UNLOAD
   22 0.000000 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=153 op=UNLOAD
   23 0.000001 33.997… 192.168.1.251 192.168.1.250      Syslog    104 AUTH.NOTICE: Oct 27 01:20:08 localhost audit: BPF prog-id=152 op=UNLOAD
```

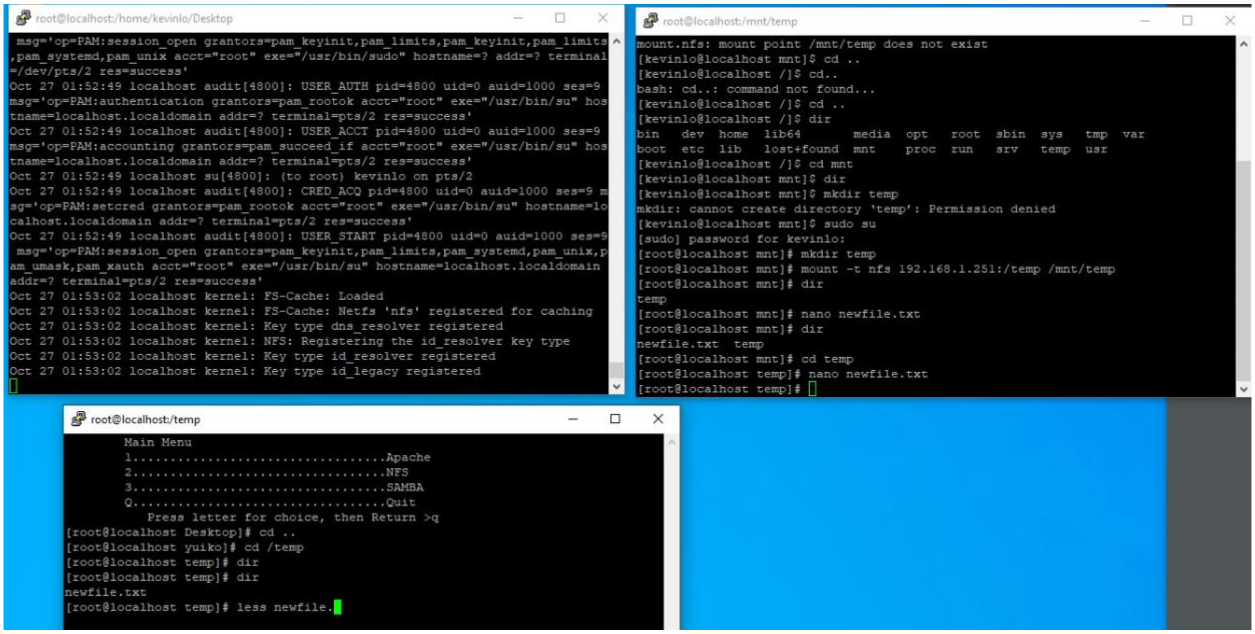
## Task 2: NFS

NFS installer was a simple few lines of code same thing with the sharing the **/temp** folder which both required no user input to perform besides selecting the option



```
nfsinstall()
{
    dnf install nfs-utils -y
    systemctl start nfs-server
    systemctl enable nfs-server
    mkdir /temp
    chmod -R 777 /temp
}

nfsaddshare()
{
    echo -n "Enter IP to share to: "
    read ipaddress rest
    echo -n "Enter subnet mask: "
    read subnet rest

    #add the entry to /etc/exports file
    echo "/temp $ipaddress/$subnet(rw,no_root_squash)" >> /etc/exports
    systemctl restart nfs-server
    exportfs -v
}
```

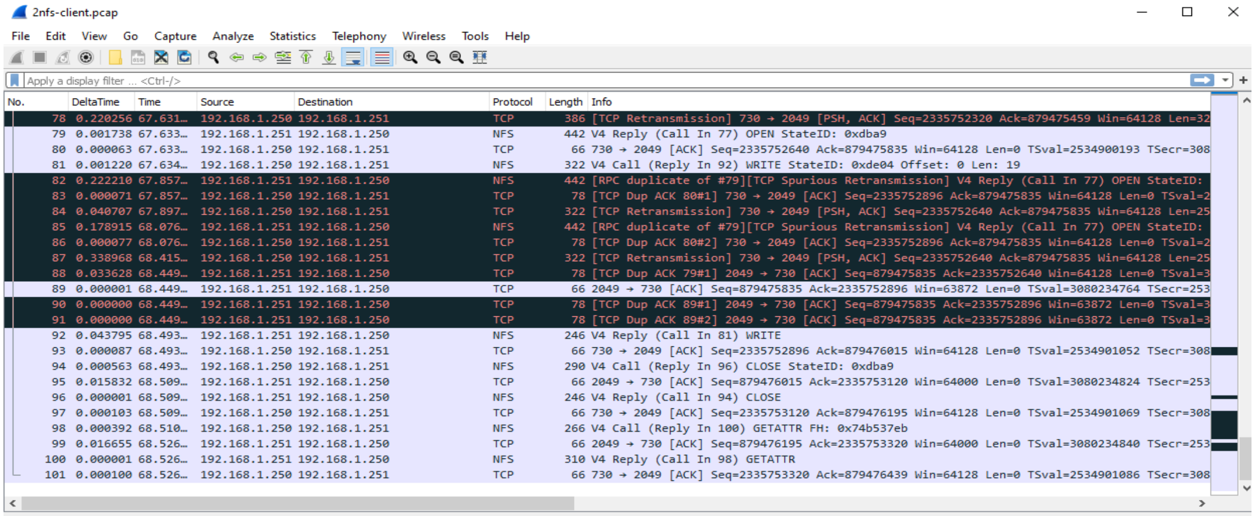
The following is the output produced by this process



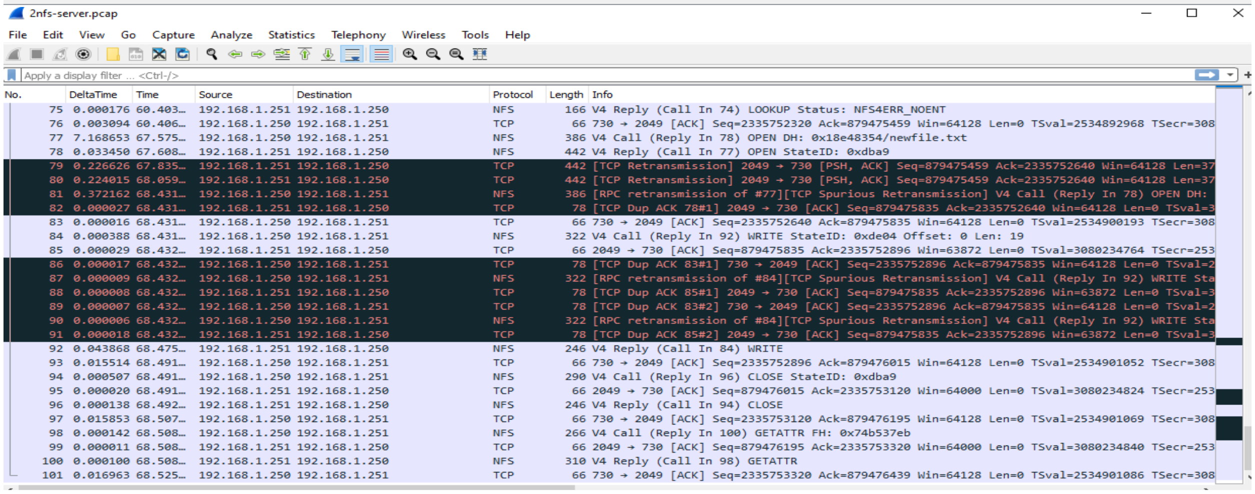
```
 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits
,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal
=/dev/pts/2 res=success'
Oct 27 01:52:49 localhost audit[4800]: USER_AUTH pid=4800 uid=0 auid=1000 ses=9
msg='op=PAM:authentication grantors=pam_rootok acct="root" exe="/usr/bin/su" hos
tname=localhost.localdomain addr=? terminal=pts/2 res=success'
Oct 27 01:52:49 localhost audit[4800]: USER_ACCT pid=4800 uid=0 auid=1000 ses=9
msg='op=PAM:accounting grantors=pam_succeed_if acct="root" exe="/usr/bin/su" hos
tname=localhost.localdomain addr=? terminal=pts/2 res=success'
Oct 27 01:52:49 localhost su[4800]: (to root) kevinlo on pts/2
Oct 27 01:52:49 localhost audit[4800]: CRED_ACQ pid=4800 uid=0 auid=1000 ses=9 m
sg='op=PAM:setcred grantors=pam_rootok acct="root" exe="/usr/bin/su" hostname=lo
calhost.localdomain addr=? terminal=pts/2 res=success'
Oct 27 01:52:49 localhost audit[4800]: USER_START pid=4800 uid=0 auid=1000 ses=9
 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,p
am_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=localhost.localdomain
addr=? terminal=pts/2 res=success'
Oct 27 01:53:02 localhost kernel: FS-Cache: Loaded
Oct 27 01:53:02 localhost kernel: FS-Cache: Netfs 'nfs' registered for caching
Oct 27 01:53:02 localhost kernel: Key type dns_resolver registered
Oct 27 01:53:02 localhost kernel: NFS: Registering the id_resolver key type
Oct 27 01:53:02 localhost kernel: Key type id_resolver registered
Oct 27 01:53:02 localhost kernel: Key type id_legacy registered
```

```
mount.nfs: mount point /mnt/temp does not exist
[kevinlo@localhost mnt]$ cd ..
[kevinlo@localhost /]$ cd..
bash: cd..: command not found...
[kevinlo@localhost /]$ cd ..
[kevinlo@localhost /]$ dir
bin   dev  home  lib64       media  opt   root  sbin  sys   tmp  var
boot  etc  lib   lost+found  mnt    proc  run   srv   temp  usr
[kevinlo@localhost /]$ cd mnt
[kevinlo@localhost mnt]$ dir
[kevinlo@localhost mnt]$ mkdir temp
mkdir: cannot create directory 'temp': Permission denied
[kevinlo@localhost mnt]$ sudo su
[sudo] password for kevinlo:
[root@localhost mnt]# mkdir temp
[root@localhost mnt]# mount -t nfs 192.168.1.251:/temp /mnt/temp
[root@localhost mnt]# dir
temp
[root@localhost mnt]# nano newfile.txt
[root@localhost mnt]# dir
newfile.txt  temp
[root@localhost mnt]# cd temp
[root@localhost temp]# nano newfile.txt
[root@localhost temp]# 
```

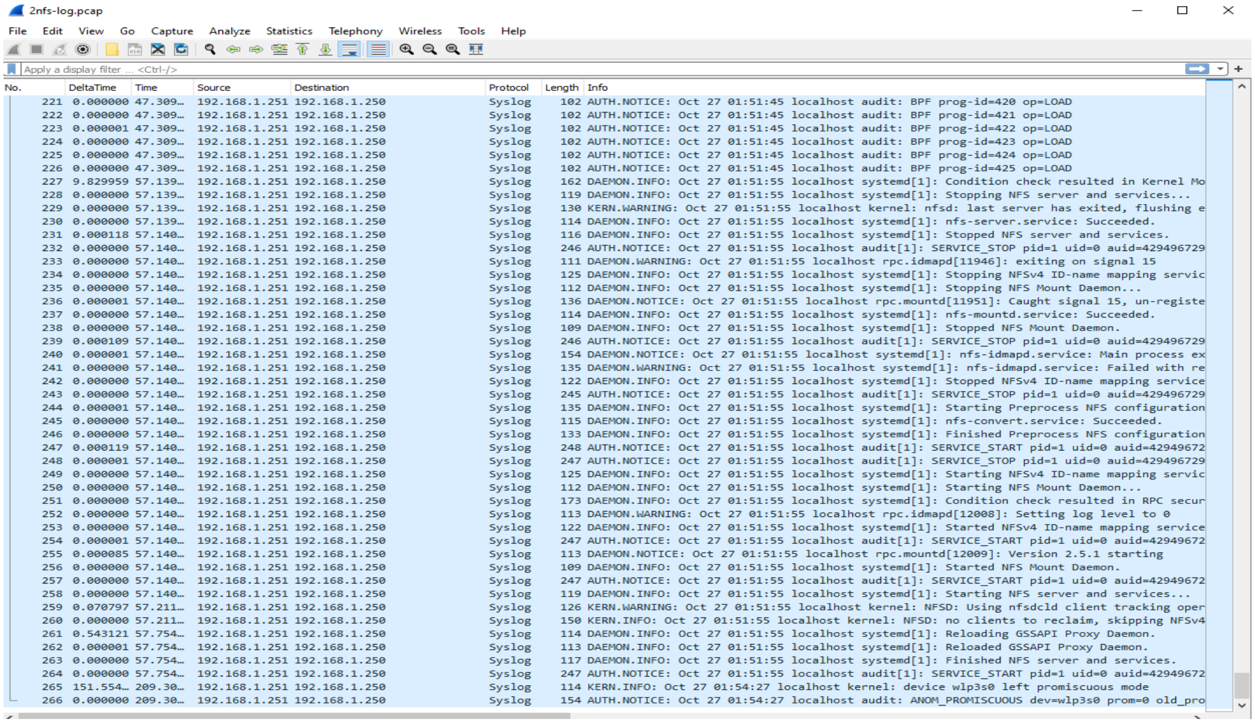
```
        Main Menu
        1................................Apache
        2................................NFS
        3................................SAMBA
        Q................................Quit
           Press letter for choice, then Return >q
[root@localhost Desktop]# cd ..
[root@localhost yuiko]# cd /temp
[root@localhost temp]# dir
[root@localhost temp]# dir
newfile.txt
[root@localhost temp]# less newfile.
```


2nfs-client.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time      Source        Destination      Protocol Length Info
   78 0.220256 67.631…  192.168.1.250 192.168.1.251   TCP     386 [TCP Retransmission] 730 → 2049 [PSH, ACK] Seq=2335752320 Ack=879475459 Win=64128 Len=32
   79 0.001738 67.633…  192.168.1.251 192.168.1.250   NFS     442 V4 Reply (Call In 77) OPEN StateID: 0xdba9
   80 0.000063 67.633…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335752640 Ack=879475835 Win=64128 Len=0 TSval=2534900193 TSecr=308
   81 0.001220 67.634…  192.168.1.250 192.168.1.251   NFS     322 V4 Call (Reply In 92) WRITE StateID: 0xde04 Offset: 0 Len: 19
   82 0.222210 67.857…  192.168.1.251 192.168.1.250   NFS     442 [RPC duplicate of #79][TCP Spurious Retransmission] V4 Reply (Call In 77) OPEN StateID:
   83 0.000071 67.857…  192.168.1.250 192.168.1.251   TCP      78 [TCP Dup ACK 80#1] 730 → 2049 [ACK] Seq=2335752896 Ack=879475835 Win=64128 Len=0 TSval=2
   84 0.040707 67.897…  192.168.1.250 192.168.1.251   TCP     322 [TCP Retransmission] 730 → 2049 [PSH, ACK] Seq=2335752640 Ack=879475835 Win=64128 Len=25
   85 0.178915 68.076…  192.168.1.251 192.168.1.250   NFS     442 [RPC duplicate of #79][TCP Spurious Retransmission] V4 Reply (Call In 77) OPEN StateID:
   86 0.000077 68.076…  192.168.1.250 192.168.1.251   TCP      78 [TCP Dup ACK 80#2] 730 → 2049 [ACK] Seq=2335752896 Ack=879475835 Win=64128 Len=0 TSval=2
   87 0.338968 68.415…  192.168.1.250 192.168.1.251   TCP     322 [TCP Retransmission] 730 → 2049 [PSH, ACK] Seq=2335752640 Ack=879475835 Win=64128 Len=25
   88 0.033628 68.449…  192.168.1.251 192.168.1.250   TCP      78 [TCP Dup ACK 79#1] 2049 → 730 [ACK] Seq=879475835 Ack=2335752640 Win=64128 Len=0 TSval=3
   89 0.000001 68.449…  192.168.1.251 192.168.1.250   TCP      66 2049 → 730 [ACK] Seq=879475835 Ack=2335752896 Win=63872 Len=0 TSval=3080234764 TSecr=253
   90 0.000000 68.449…  192.168.1.251 192.168.1.250   TCP      78 [TCP Dup ACK 89#1] 2049 → 730 [ACK] Seq=879475835 Ack=2335752896 Win=63872 Len=0 TSval=3
   91 0.000000 68.449…  192.168.1.251 192.168.1.250   TCP      78 [TCP Dup ACK 89#2] 2049 → 730 [ACK] Seq=879475835 Ack=2335752896 Win=63872 Len=0 TSval=3
   92 0.043795 68.493…  192.168.1.251 192.168.1.250   NFS     246 V4 Reply (Call In 81) WRITE
   93 0.000087 68.493…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335752896 Ack=879476015 Win=64128 Len=0 TSval=2534901052 TSecr=308
   94 0.000563 68.493…  192.168.1.250 192.168.1.251   NFS     290 V4 Call (Reply In 96) CLOSE StateID: 0xdba9
   95 0.015832 68.509…  192.168.1.251 192.168.1.250   TCP      66 2049 → 730 [ACK] Seq=879476015 Ack=2335753120 Win=64000 Len=0 TSval=3080234824 TSecr=253
   96 0.000001 68.509…  192.168.1.251 192.168.1.250   NFS     246 V4 Reply (Call In 94) CLOSE
   97 0.000103 68.509…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335753120 Ack=879476195 Win=64128 Len=0 TSval=2534901069 TSecr=308
   98 0.000392 68.510…  192.168.1.250 192.168.1.251   NFS     266 V4 Call (Reply In 100) GETATTR FH: 0x74b537eb
   99 0.016655 68.526…  192.168.1.251 192.168.1.250   TCP      66 2049 → 730 [ACK] Seq=879476195 Ack=2335753320 Win=64000 Len=0 TSval=3080234840 TSecr=253
  100 0.000001 68.526…  192.168.1.251 192.168.1.250   NFS     310 V4 Reply (Call In 98) GETATTR
  101 0.000100 68.526…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335753320 Ack=879476439 Win=64128 Len=0 TSval=2534901086 TSecr=308
```


2nfs-server.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

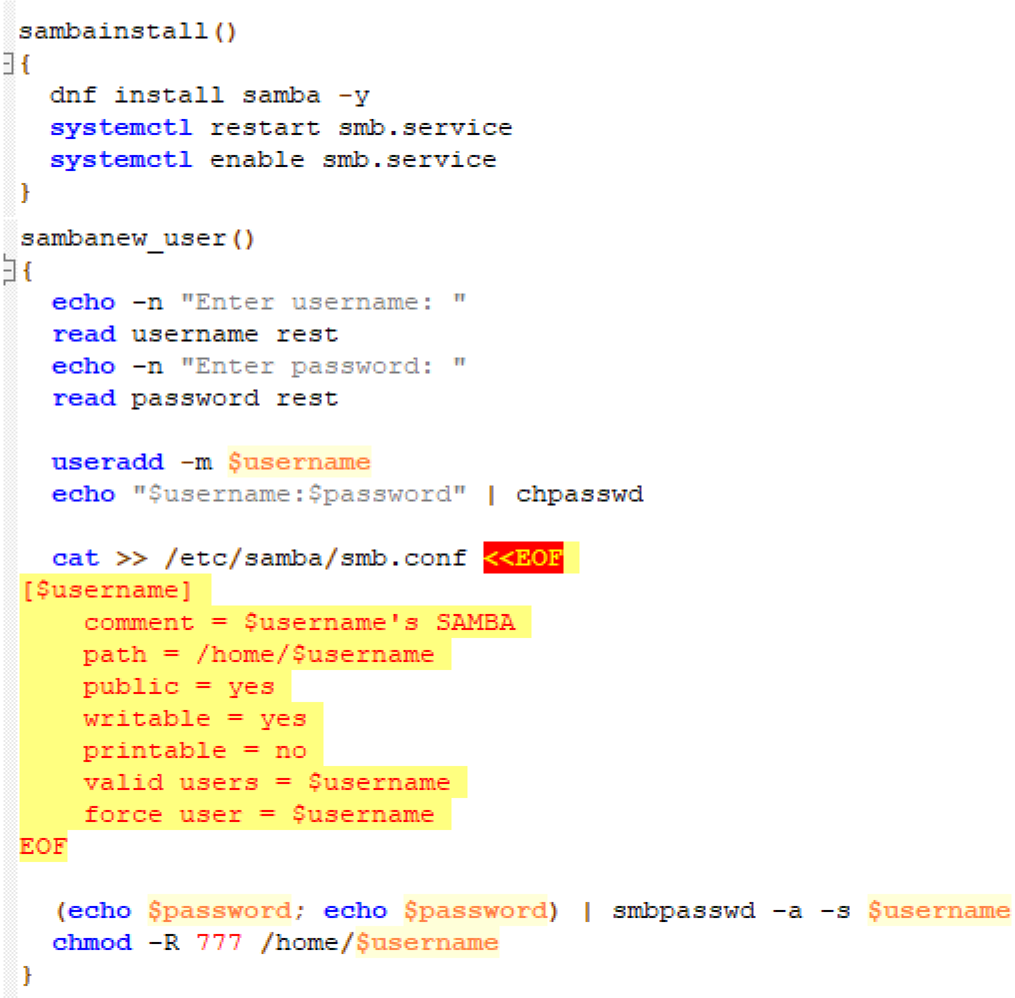
```
No.   DeltaTime Time      Source        Destination      Protocol Length Info
   75 0.000176 60.403…  192.168.1.251 192.168.1.250   NFS     166 V4 Reply (Call In 74) LOOKUP Status: NFS4ERR_NOENT
   76 0.003094 60.406…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335752320 Ack=879475459 Win=64128 Len=0 TSval=2534892968 TSecr=308
   77 7.168653 67.575…  192.168.1.250 192.168.1.251   NFS     386 V4 Call (Reply In 78) OPEN DH: 0x18e48354/newfile.txt
   78 0.033450 67.608…  192.168.1.251 192.168.1.250   NFS     442 V4 Reply (Call In 77) OPEN StateID: 0xdba9
   79 0.226626 67.835…  192.168.1.251 192.168.1.250   TCP     442 [TCP Retransmission] 2049 → 730 [PSH, ACK] Seq=879475459 Ack=2335752640 Win=64128 Len=37
   80 0.224015 68.059…  192.168.1.251 192.168.1.250   TCP     442 [TCP Retransmission] 2049 → 730 [PSH, ACK] Seq=879475459 Ack=2335752640 Win=64128 Len=37
   81 0.372162 68.431…  192.168.1.250 192.168.1.251   NFS     386 [RPC retransmission of #77][TCP Spurious Retransmission] V4 Call (Reply In 78) OPEN DH:
   82 0.000027 68.431…  192.168.1.251 192.168.1.250   TCP      78 [TCP Dup ACK 78#1] 2049 → 730 [ACK] Seq=879475835 Ack=2335752640 Win=64128 Len=0 TSval=3
   83 0.000016 68.431…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335752640 Ack=879475835 Win=64128 Len=0 TSval=2534900193 TSecr=308
   84 0.000388 68.431…  192.168.1.250 192.168.1.251   NFS     322 V4 Call (Reply In 92) WRITE StateID: 0xde04 Offset: 0 Len: 19
   85 0.000029 68.432…  192.168.1.251 192.168.1.250   TCP      66 2049 → 730 [ACK] Seq=879475835 Ack=2335752896 Win=63872 Len=0 TSval=3080234764 TSecr=253
   86 0.000017 68.432…  192.168.1.250 192.168.1.251   TCP      78 [TCP Dup ACK 83#1] 730 → 2049 [ACK] Seq=2335752896 Ack=879475835 Win=64128 Len=0 TSval=2
   87 0.000009 68.432…  192.168.1.250 192.168.1.251   NFS     322 [RPC retransmission of #84][TCP Spurious Retransmission] V4 Call (Reply In 92) WRITE Sta
   88 0.000008 68.432…  192.168.1.251 192.168.1.250   TCP      78 [TCP Dup ACK 85#1] 2049 → 730 [ACK] Seq=879475835 Ack=2335752896 Win=63872 Len=0 TSval=3
   89 0.000007 68.432…  192.168.1.250 192.168.1.251   TCP      78 [TCP Dup ACK 83#2] 730 → 2049 [ACK] Seq=2335752896 Ack=879475835 Win=64128 Len=0 TSval=2
   90 0.000006 68.432…  192.168.1.250 192.168.1.251   NFS     322 [RPC retransmission of #84][TCP Spurious Retransmission] V4 Call (Reply In 92) WRITE Sta
   91 0.000018 68.432…  192.168.1.251 192.168.1.250   TCP      78 [TCP Dup ACK 85#2] 2049 → 730 [ACK] Seq=879475835 Ack=2335752896 Win=63872 Len=0 TSval=3
   92 0.043868 68.475…  192.168.1.251 192.168.1.250   NFS     246 V4 Reply (Call In 84) WRITE
   93 0.015514 68.491…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335752896 Ack=879476015 Win=64128 Len=0 TSval=2534901052 TSecr=308
   94 0.000507 68.491…  192.168.1.250 192.168.1.251   NFS     290 V4 Call (Reply In 96) CLOSE StateID: 0xdba9
   95 0.000020 68.491…  192.168.1.251 192.168.1.250   TCP      66 2049 → 730 [ACK] Seq=879476015 Ack=2335753120 Win=64000 Len=0 TSval=3080234824 TSecr=253
   96 0.000138 68.492…  192.168.1.251 192.168.1.250   NFS     246 V4 Reply (Call In 94) CLOSE
   97 0.015853 68.507…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335753120 Ack=879476195 Win=64128 Len=0 TSval=2534901069 TSecr=308
   98 0.000142 68.508…  192.168.1.250 192.168.1.251   NFS     266 V4 Call (Reply In 100) GETATTR FH: 0x74b537eb
   99 0.000011 68.508…  192.168.1.251 192.168.1.250   TCP      66 2049 → 730 [ACK] Seq=879476195 Ack=2335753320 Win=64000 Len=0 TSval=3080234840 TSecr=253
  100 0.000100 68.508…  192.168.1.251 192.168.1.250   NFS     310 V4 Reply (Call In 98) GETATTR
  101 0.016963 68.525…  192.168.1.250 192.168.1.251   TCP      66 730 → 2049 [ACK] Seq=2335753320 Ack=879476439 Win=64128 Len=0 TSval=2534901086 TSecr=308
```


2nfs-log.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time      Source        Destination      Protocol Length Info
  221 0.000000 47.309…  192.168.1.251 192.168.1.250   Syslog  102 AUTH.NOTICE: Oct 27 01:51:45 localhost audit: BPF prog-id=420 op=LOAD
  222 0.000000 47.309…  192.168.1.251 192.168.1.250   Syslog  102 AUTH.NOTICE: Oct 27 01:51:45 localhost audit: BPF prog-id=421 op=LOAD
  223 0.000001 47.309…  192.168.1.251 192.168.1.250   Syslog  102 AUTH.NOTICE: Oct 27 01:51:45 localhost audit: BPF prog-id=422 op=LOAD
  224 0.000000 47.309…  192.168.1.251 192.168.1.250   Syslog  102 AUTH.NOTICE: Oct 27 01:51:45 localhost audit: BPF prog-id=423 op=LOAD
  225 0.000000 47.309…  192.168.1.251 192.168.1.250   Syslog  102 AUTH.NOTICE: Oct 27 01:51:45 localhost audit: BPF prog-id=424 op=LOAD
  226 0.000000 47.309…  192.168.1.251 192.168.1.250   Syslog  102 AUTH.NOTICE: Oct 27 01:51:45 localhost audit: BPF prog-id=425 op=LOAD
  227 9.829959 57.139…  192.168.1.251 192.168.1.250   Syslog  162 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Condition check resulted in Kernel Mo
  228 0.000000 57.139…  192.168.1.251 192.168.1.250   Syslog  119 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Stopping NFS server and services...
  229 0.000000 57.139…  192.168.1.251 192.168.1.250   Syslog  130 KERN.WARNING: Oct 27 01:51:55 localhost kernel: nfsd: last server has exited, flushing e
  230 0.000000 57.139…  192.168.1.251 192.168.1.250   Syslog  114 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: nfs-server.service: Succeeded.
  231 0.000118 57.140…  192.168.1.251 192.168.1.250   Syslog  116 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Stopped NFS server and services.
  232 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  246 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=429496729
  233 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  111 DAEMON.WARNING: Oct 27 01:51:55 localhost rpc.idmapd[11946]: exiting on signal 15
  234 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  125 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Stopping NFSv4 ID-name mapping servic
  235 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  112 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Stopping NFS Mount Daemon...
  236 0.000001 57.140…  192.168.1.251 192.168.1.250   Syslog  136 DAEMON.NOTICE: Oct 27 01:51:55 localhost rpc.mountd[11951]: Caught signal 15, un-registe
  237 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  114 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: nfs-mountd.service: Succeeded.
  238 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  109 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Stopped NFS Mount Daemon.
  239 0.000109 57.140…  192.168.1.251 192.168.1.250   Syslog  246 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=429496729
  240 0.000001 57.140…  192.168.1.251 192.168.1.250   Syslog  154 DAEMON.NOTICE: Oct 27 01:51:55 localhost systemd[1]: nfs-idmapd.service: Main process ex
  241 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  135 DAEMON.WARNING: Oct 27 01:51:55 localhost systemd[1]: nfs-idmapd.service: Failed with re
  242 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  122 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Stopped NFSv4 ID-name mapping service
  243 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  245 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=429496729
  244 0.000001 57.140…  192.168.1.251 192.168.1.250   Syslog  135 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Starting Preprocess NFS configuration
  245 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  115 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: nfs-convert.service: Succeeded.
  246 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  133 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Finished Preprocess NFS configuration
  247 0.000119 57.140…  192.168.1.251 192.168.1.250   Syslog  248 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=42949672
  248 0.000001 57.140…  192.168.1.251 192.168.1.250   Syslog  247 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=429496729
  249 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  125 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Starting NFSv4 ID-name mapping servic
  250 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  112 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Starting NFS Mount Daemon...
  251 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  173 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Condition check resulted in RPC secur
  252 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  113 DAEMON.WARNING: Oct 27 01:51:55 localhost rpc.idmapd[12008]: Setting log level to 0
  253 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  122 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Started NFSv4 ID-name mapping service
  254 0.000001 57.140…  192.168.1.251 192.168.1.250   Syslog  247 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=42949672
  255 0.000085 57.140…  192.168.1.251 192.168.1.250   Syslog  113 DAEMON.NOTICE: Oct 27 01:51:55 localhost rpc.mountd[12009]: Version 2.5.1 starting
  256 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  109 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Started NFS Mount Daemon.
  257 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  247 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=42949672
  258 0.000000 57.140…  192.168.1.251 192.168.1.250   Syslog  119 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Starting NFS server and services...
  259 0.070797 57.211…  192.168.1.251 192.168.1.250   Syslog  126 KERN.WARNING: Oct 27 01:51:55 localhost kernel: NFSD: Using nfsdcld client tracking oper
  260 0.000000 57.211…  192.168.1.251 192.168.1.250   Syslog  150 KERN.INFO: Oct 27 01:51:55 localhost kernel: NFSD: no clients to reclaim, skipping NFSv4
  261 0.543121 57.754…  192.168.1.251 192.168.1.250   Syslog  114 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Reloading GSSAPI Proxy Daemon.
  262 0.000001 57.754…  192.168.1.251 192.168.1.250   Syslog  113 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Reloaded GSSAPI Proxy Daemon.
  263 0.000000 57.754…  192.168.1.251 192.168.1.250   Syslog  117 DAEMON.INFO: Oct 27 01:51:55 localhost systemd[1]: Finished NFS server and services.
  264 0.000000 57.754…  192.168.1.251 192.168.1.250   Syslog  247 AUTH.NOTICE: Oct 27 01:51:55 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=42949672
  265 151.554… 209.30…  192.168.1.251 192.168.1.250   Syslog  114 KERN.INFO: Oct 27 01:54:27 localhost kernel: device wlp3s0 left promiscuous mode
  266 0.000000 209.30…  192.168.1.251 192.168.1.250   Syslog  154 AUTH.NOTICE: Oct 27 01:54:27 localhost audit: ANOM_PROMISCUOUS dev=wlp3s0 prom=0 old_pro
```

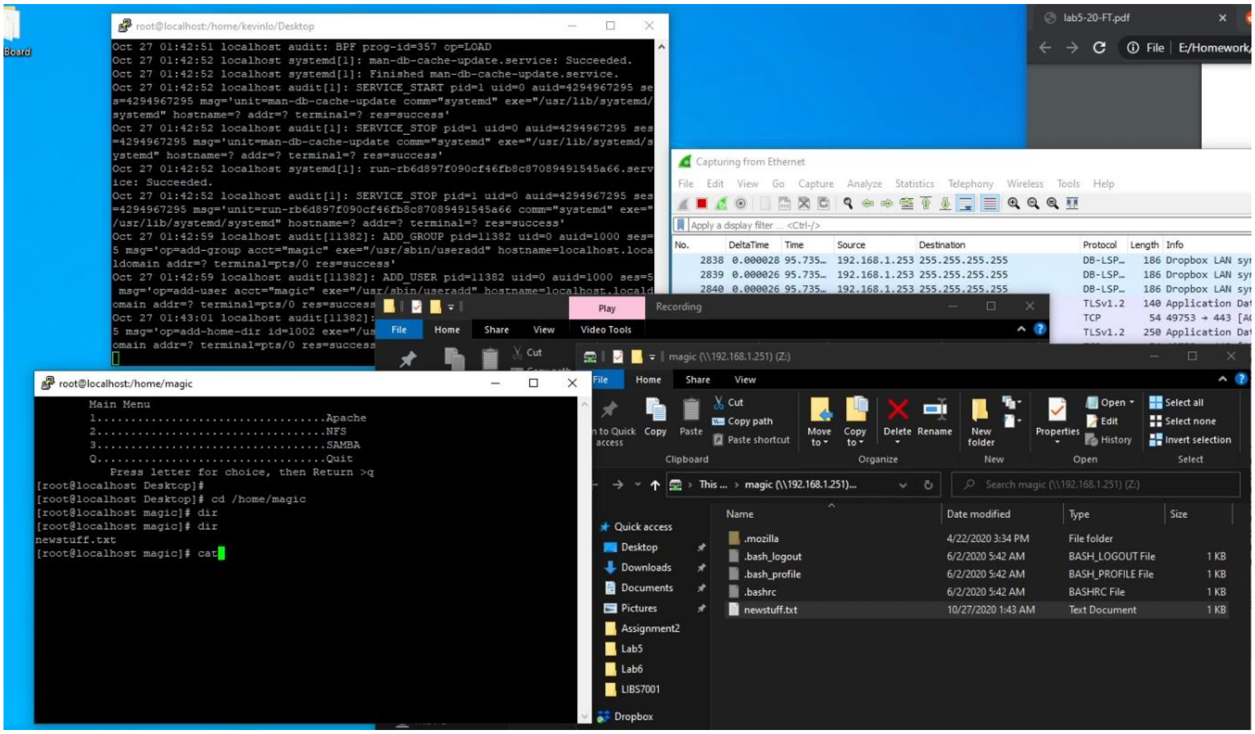
## Task 3: Samba

Samba installer was a few lines of code and adding a user for Samba sharing only requires a username and password which will automatically add the new user to the **/etc/samba/smb.conf**



```
sambainstall()
{
  dnf install samba -y
  systemctl restart smb.service
  systemctl enable smb.service
}
sambanew_user()
{
  echo -n "Enter username: "
  read username rest
  echo -n "Enter password: "
  read password rest

  useradd -m $username
  echo "$username:$password" | chpasswd

  cat >> /etc/samba/smb.conf <<EOF
[$username]
    comment = $username's SAMBA
    path = /home/$username
    public = yes
    writable = yes
    printable = no
    valid users = $username
    force user = $username
EOF

  (echo $password; echo $password) | smbpasswd -a -s $username
  chmod -R 777 /home/$username
}
```

The following output was created from the installation and accessing of the samba share.



root@localhost:/home/kevinlo/Desktop

```
Oct 27 01:42:51 localhost audit: BPF prog-id=357 op=LOAD
Oct 27 01:42:52 localhost systemd[1]: man-db-cache-update.service: Succeeded.
Oct 27 01:42:52 localhost systemd[1]: Finished man-db-cache-update.service.
Oct 27 01:42:52 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=4294967295 se
s=4294967295 msg='unit=man-db-cache-update comm="systemd" exe="/usr/lib/systemd/
systemd" hostname=? addr=? terminal=? res=success'
Oct 27 01:42:52 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=4294967295 ses
=4294967295 msg='unit=man-db-cache-update comm="systemd" exe="/usr/lib/systemd/s
ystemd" hostname=? addr=? terminal=? res=success'
Oct 27 01:42:52 localhost systemd[1]: run-rb6d897f090cf46fb8c87089491545a66.serv
ice: Succeeded.
Oct 27 01:42:52 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=4294967295 ses
=4294967295 msg='unit=run-rb6d897f090cf46fb8c87089491545a66 comm="systemd" exe="
/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Oct 27 01:42:59 localhost audit[11382]: ADD_GROUP pid=11382 uid=0 auid=1000 ses=
5 msg='op=add-group acct="magic" exe="/usr/sbin/useradd" hostname=localhost.loca
ldomain addr=? terminal=pts/0 res=success'
Oct 27 01:42:59 localhost audit[11382]: ADD_USER pid=11382 uid=0 auid=1000 ses=5
 msg='op=add-user acct="magic" exe="/usr/sbin/useradd" hostname=localhost.locald
omain addr=? terminal=pts/0 res=success
Oct 27 01:43:01 localhost audit[11382]:
5 msg='op=add-home-dir id=1002 exe="/us
omain addr=? terminal=pts/0 res=success
```

root@localhost:/home/magic

```
        Main Menu
        1.................................Apache
        2.................................NFS
        3.................................SAMBA
        Q.................................Quit
           Press letter for choice, then Return >q
[root@localhost Desktop]#
[root@localhost Desktop]# cd /home/magic
[root@localhost magic]# dir
[root@localhost magic]# dir
newstuff.txt
[root@localhost magic]# cat
```

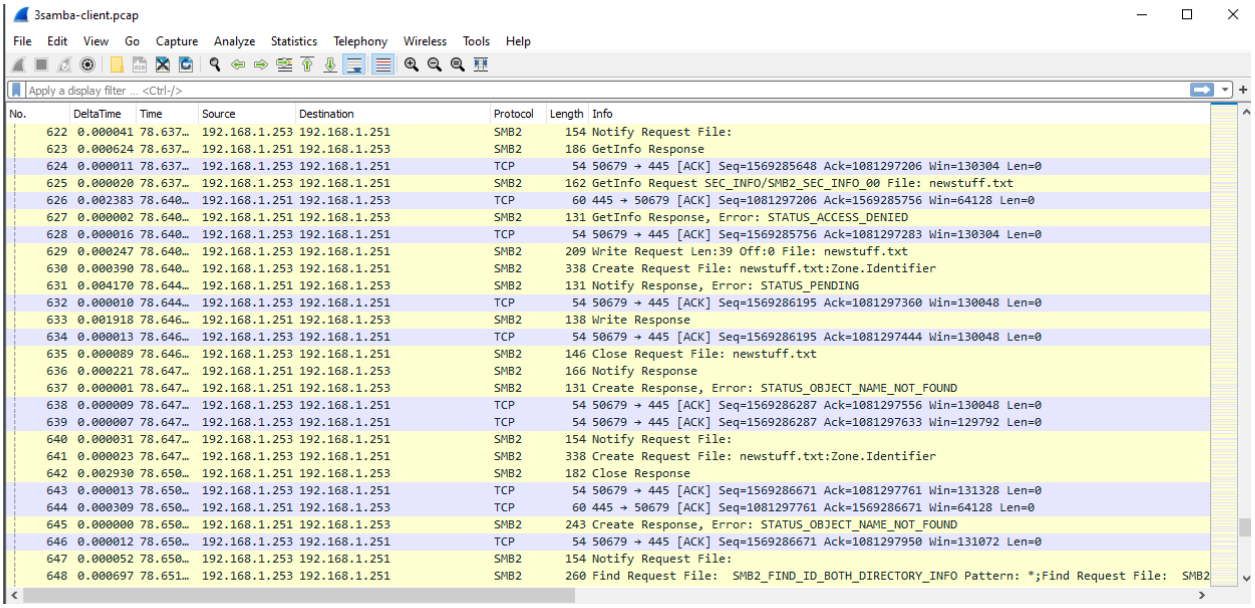
Capturing from Ethernet

```
No.   DeltaTime Time      Source        Destination      Protocol Length Info
 2838 0.000028 95.735…  192.168.1.253 255.255.255.255  DB-LSP…   186 Dropbox LAN sy
 2839 0.000026 95.735…  192.168.1.253 255.255.255.255  DB-LSP…   186 Dropbox LAN sy
 2840 0.000026 95.735…  192.168.1.253 255.255.255.255  DB-LSP…   186 Dropbox LAN sy
                                                       TLSv1.2   140 Application Da
                                                       TCP        54 49753 → 443 [A
                                                       TLSv1.2   250 Application Da
```

magic (\\192.168.1.251) (Z:)

| Name | Date modified | Type | Size |
|---|---|---|---|
| .mozilla | 4/22/2020 3:34 PM | File folder | |
| .bash_logout | 6/2/2020 5:42 AM | BASH_LOGOUT File | 1 KB |
| .bash_profile | 6/2/2020 5:42 AM | BASH_PROFILE File | 1 KB |
| .bashrc | 6/2/2020 5:42 AM | BASHRC File | 1 KB |
| newstuff.txt | 10/27/2020 1:43 AM | Text Document | 1 KB |

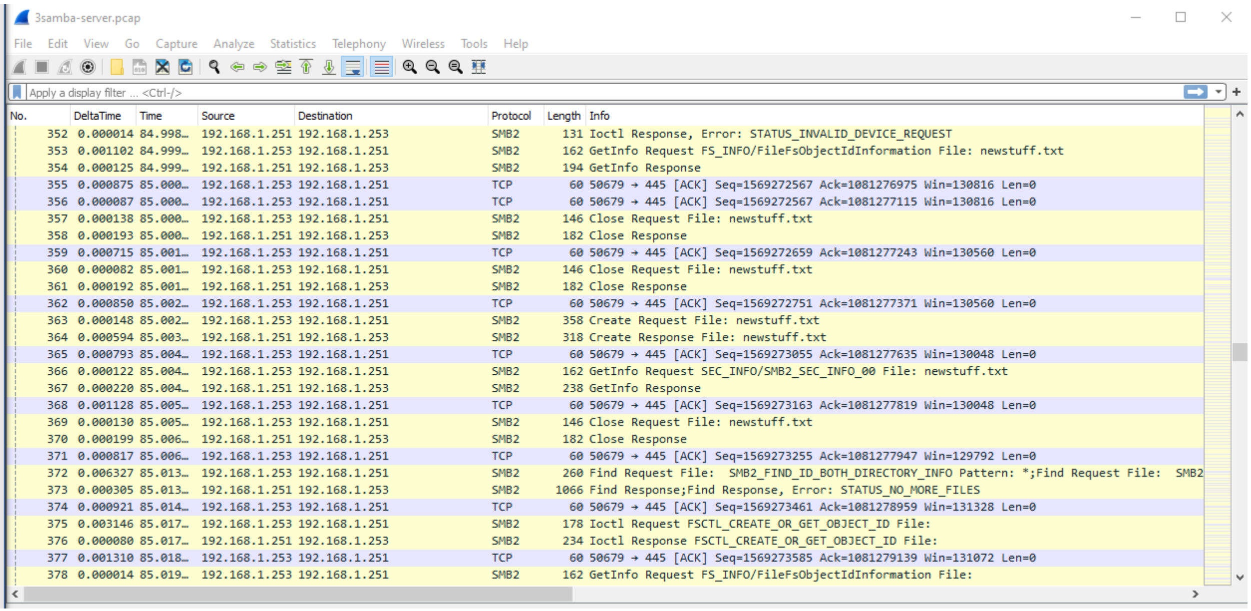
Board
lab5-20-FT.pdf
File | E:/Homework/
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Play
Recording
File Home Share View Video Tools
Cut
to Quick access Copy Paste Copy path Paste shortcut
Move to Copy to Delete Rename New folder Properties Open Edit History Select all Select none Invert selection
Clipboard Organize New Open Select
This … › magic (\\192.168.1.251)…
Search magic (\\192.168.1.251) (Z:)
Quick access
Desktop
Downloads
Documents
Pictures
Assignment2
Lab5
Lab6
LIBS7001
Dropbox



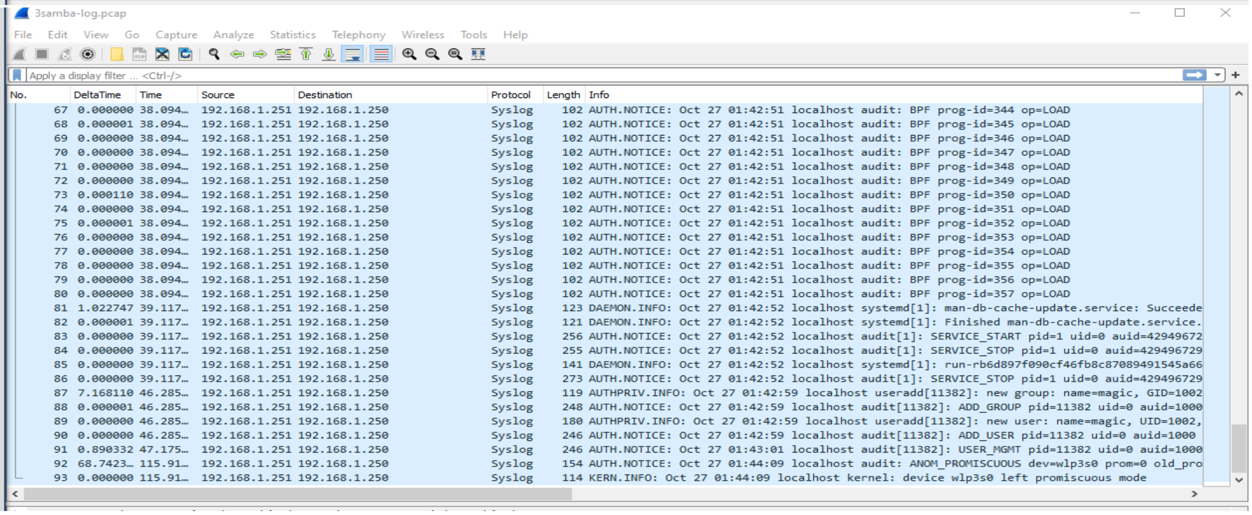
3samba-client.pcap

```
No.  DeltaTime Time      Source        Destination    Protocol Length Info
 622 0.000041 78.637…  192.168.1.253 192.168.1.251  SMB2      154 Notify Request File:
 623 0.000624 78.637…  192.168.1.251 192.168.1.253  SMB2      186 GetInfo Response
 624 0.000011 78.637…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569285648 Ack=1081297206 Win=130304 Len=0
 625 0.000020 78.637…  192.168.1.253 192.168.1.251  SMB2      162 GetInfo Request SEC_INFO/SMB2_SEC_INFO_00 File: newstuff.txt
 626 0.002383 78.640…  192.168.1.251 192.168.1.253  TCP        60 445 → 50679 [ACK] Seq=1081297206 Ack=1569285756 Win=64128 Len=0
 627 0.000002 78.640…  192.168.1.251 192.168.1.253  SMB2      131 GetInfo Response, Error: STATUS_ACCESS_DENIED
 628 0.000016 78.640…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569285756 Ack=1081297283 Win=130304 Len=0
 629 0.000247 78.640…  192.168.1.253 192.168.1.251  SMB2      209 Write Request Len:39 Off:0 File: newstuff.txt
 630 0.000390 78.640…  192.168.1.253 192.168.1.251  SMB2      338 Create Request File: newstuff.txt:Zone.Identifier
 631 0.004170 78.644…  192.168.1.251 192.168.1.253  SMB2      131 Notify Response, Error: STATUS_PENDING
 632 0.000010 78.644…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569286195 Ack=1081297360 Win=130048 Len=0
 633 0.001918 78.646…  192.168.1.251 192.168.1.253  SMB2      138 Write Response
 634 0.000013 78.646…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569286195 Ack=1081297444 Win=130048 Len=0
 635 0.000089 78.646…  192.168.1.253 192.168.1.251  SMB2      146 Close Request File: newstuff.txt
 636 0.000221 78.647…  192.168.1.251 192.168.1.253  SMB2      166 Notify Response
 637 0.000001 78.647…  192.168.1.251 192.168.1.253  SMB2      131 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
 638 0.000009 78.647…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569286287 Ack=1081297556 Win=130048 Len=0
 639 0.000007 78.647…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569286287 Ack=1081297633 Win=129792 Len=0
 640 0.000031 78.647…  192.168.1.253 192.168.1.251  SMB2      154 Notify Request File:
 641 0.000023 78.647…  192.168.1.253 192.168.1.251  SMB2      338 Create Request File: newstuff.txt:Zone.Identifier
 642 0.002930 78.650…  192.168.1.251 192.168.1.253  SMB2      182 Close Response
 643 0.000013 78.650…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569286671 Ack=1081297761 Win=131328 Len=0
 644 0.000309 78.650…  192.168.1.251 192.168.1.253  TCP        60 445 → 50679 [ACK] Seq=1081297761 Ack=1569286671 Win=64128 Len=0
 645 0.000000 78.650…  192.168.1.251 192.168.1.253  SMB2      243 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
 646 0.000012 78.650…  192.168.1.253 192.168.1.251  TCP        54 50679 → 445 [ACK] Seq=1569286671 Ack=1081297950 Win=131072 Len=0
 647 0.000052 78.650…  192.168.1.253 192.168.1.251  SMB2      154 Notify Request File:
 648 0.000697 78.651…  192.168.1.253 192.168.1.251  SMB2      260 Find Request File:  SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File:  SMB2
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>


3samba-server.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
 352 0.000014 84.998… 192.168.1.251 192.168.1.253 SMB2      131 Ioctl Response, Error: STATUS_INVALID_DEVICE_REQUEST
 353 0.001102 84.999… 192.168.1.253 192.168.1.251 SMB2      162 GetInfo Request FS_INFO/FileFsObjectIdInformation File: newstuff.txt
 354 0.000125 84.999… 192.168.1.251 192.168.1.253 SMB2      194 GetInfo Response
 355 0.000875 85.000… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569272567 Ack=1081276975 Win=130816 Len=0
 356 0.000087 85.000… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569272567 Ack=1081277115 Win=130816 Len=0
 357 0.000138 85.000… 192.168.1.253 192.168.1.251 SMB2      146 Close Request File: newstuff.txt
 358 0.000193 85.000… 192.168.1.251 192.168.1.253 SMB2      182 Close Response
 359 0.000715 85.001… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569272659 Ack=1081277243 Win=130560 Len=0
 360 0.000082 85.001… 192.168.1.253 192.168.1.251 SMB2      146 Close Request File: newstuff.txt
 361 0.000192 85.001… 192.168.1.251 192.168.1.253 SMB2      182 Close Response
 362 0.000850 85.002… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569272751 Ack=1081277371 Win=130560 Len=0
 363 0.000148 85.002… 192.168.1.253 192.168.1.251 SMB2      358 Create Request File: newstuff.txt
 364 0.000594 85.003… 192.168.1.251 192.168.1.253 SMB2      318 Create Response File: newstuff.txt
 365 0.000793 85.004… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569273055 Ack=1081277635 Win=130048 Len=0
 366 0.000122 85.004… 192.168.1.253 192.168.1.251 SMB2      162 GetInfo Request SEC_INFO/SMB2_SEC_INFO_00 File: newstuff.txt
 367 0.000220 85.004… 192.168.1.251 192.168.1.253 SMB2      238 GetInfo Response
 368 0.001128 85.005… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569273163 Ack=1081277819 Win=130048 Len=0
 369 0.000130 85.005… 192.168.1.253 192.168.1.251 SMB2      146 Close Request File: newstuff.txt
 370 0.000199 85.006… 192.168.1.251 192.168.1.253 SMB2      182 Close Response
 371 0.000817 85.006… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569273255 Ack=1081277947 Win=129792 Len=0
 372 0.006327 85.013… 192.168.1.253 192.168.1.251 SMB2      260 Find Request File:  SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File:  SMB2
 373 0.000305 85.013… 192.168.1.251 192.168.1.253 SMB2     1066 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
 374 0.000921 85.014… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569273461 Ack=1081278959 Win=131328 Len=0
 375 0.003146 85.017… 192.168.1.253 192.168.1.251 SMB2      178 Ioctl Request FSCTL_CREATE_OR_GET_OBJECT_ID File:
 376 0.000080 85.017… 192.168.1.251 192.168.1.253 SMB2      234 Ioctl Response FSCTL_CREATE_OR_GET_OBJECT_ID File:
 377 0.001310 85.018… 192.168.1.253 192.168.1.251 TCP        60 50679 → 445 [ACK] Seq=1569273585 Ack=1081279139 Win=131072 Len=0
 378 0.000014 85.019… 192.168.1.253 192.168.1.251 SMB2      162 GetInfo Request FS_INFO/FileFsObjectIdInformation File:
```


3samba-log.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No. DeltaTime Time     Source        Destination   Protocol Length Info
 67 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=344 op=LOAD
 68 0.000001 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=345 op=LOAD
 69 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=346 op=LOAD
 70 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=347 op=LOAD
 71 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=348 op=LOAD
 72 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=349 op=LOAD
 73 0.000110 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=350 op=LOAD
 74 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=351 op=LOAD
 75 0.000001 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=352 op=LOAD
 76 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=353 op=LOAD
 77 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=354 op=LOAD
 78 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=355 op=LOAD
 79 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=356 op=LOAD
 80 0.000000 38.094… 192.168.1.251 192.168.1.250 Syslog    102 AUTH.NOTICE: Oct 27 01:42:51 localhost audit: BPF prog-id=357 op=LOAD
 81 1.022747 39.117… 192.168.1.251 192.168.1.250 Syslog    123 DAEMON.INFO: Oct 27 01:42:52 localhost systemd[1]: man-db-cache-update.service: Succeede
 82 0.000001 39.117… 192.168.1.251 192.168.1.250 Syslog    121 DAEMON.INFO: Oct 27 01:42:52 localhost systemd[1]: Finished man-db-cache-update.service.
 83 0.000000 39.117… 192.168.1.251 192.168.1.250 Syslog    256 AUTH.NOTICE: Oct 27 01:42:52 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=42949672
 84 0.000000 39.117… 192.168.1.251 192.168.1.250 Syslog    255 AUTH.NOTICE: Oct 27 01:42:52 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=429496729
 85 0.000000 39.117… 192.168.1.251 192.168.1.250 Syslog    141 DAEMON.INFO: Oct 27 01:42:52 localhost systemd[1]: run-rb6d897f090cf46fb8c87089491545a66
 86 0.000000 39.117… 192.168.1.251 192.168.1.250 Syslog    273 AUTH.NOTICE: Oct 27 01:42:52 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=429496729
 87 7.168110 46.285… 192.168.1.251 192.168.1.250 Syslog    119 AUTHPRIV.INFO: Oct 27 01:42:59 localhost useradd[11382]: new group: name=magic, GID=1002
 88 0.000001 46.285… 192.168.1.251 192.168.1.250 Syslog    248 AUTH.NOTICE: Oct 27 01:42:59 localhost audit[11382]: ADD_GROUP pid=11382 uid=0 auid=1000
 89 0.000000 46.285… 192.168.1.251 192.168.1.250 Syslog    180 AUTHPRIV.INFO: Oct 27 01:42:59 localhost useradd[11382]: new user: name=magic, UID=1002,
 90 0.000000 46.285… 192.168.1.251 192.168.1.250 Syslog    246 AUTH.NOTICE: Oct 27 01:42:59 localhost audit[11382]: ADD_USER pid=11382 uid=0 auid=1000
 91 0.890332 47.175… 192.168.1.251 192.168.1.250 Syslog    246 AUTH.NOTICE: Oct 27 01:43:01 localhost audit[11382]: USER_MGMT pid=11382 uid=0 auid=1000
 92 68.7423… 115.91… 192.168.1.251 192.168.1.250 Syslog    154 AUTH.NOTICE: Oct 27 01:44:09 localhost audit: ANOM_PROMISCUOUS dev=wlp3s0 prom=0 old_pro
 93 0.000000 115.91… 192.168.1.251 192.168.1.250 Syslog    114 KERN.INFO: Oct 27 01:44:09 localhost kernel: device wlp3s0 left promiscuous mode
```