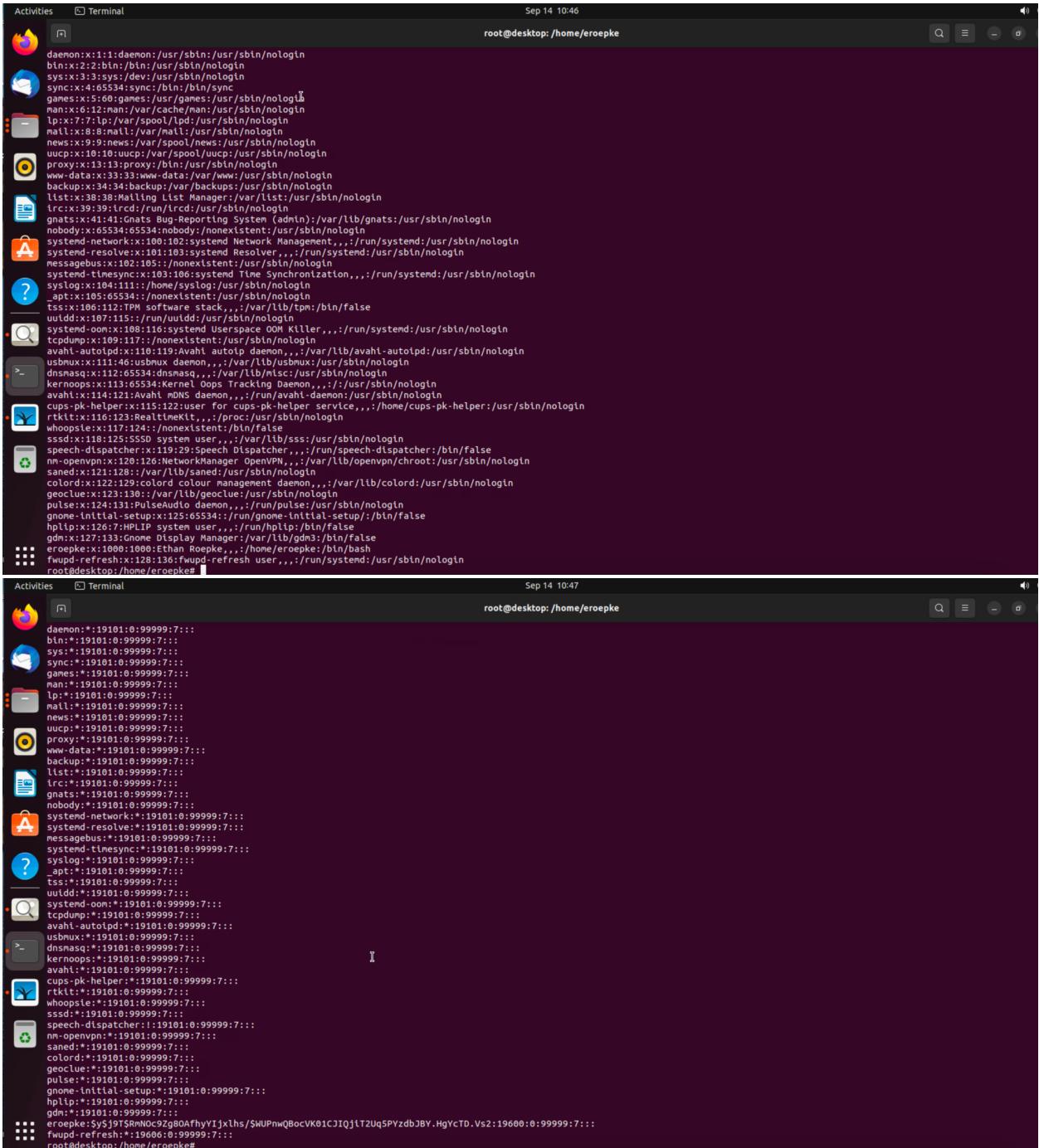


# Lab 03 Template - Ethan Roepke

Don't forget to follow these lab report instructions.

## 1. Screenshot of passwd and shadow with description/notation of fields (10 points)



The image shows two terminal windows side-by-side, both titled "Activities" and "Terminal". Both windows are running as root at the command prompt: "root@desktop:/home/eroepke".

The left terminal window displays the contents of the /etc/passwd file. The output is as follows:

```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:system Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:113::/run/uuidd:/usr/sbin/nologin
udevmon:object:108:108:Udev Monitor User:/sbin/nologin
tcpdump:object:109:117::/nonexistent:/sbin/nologin
avahi-autopid:x:110:119:Avahi Autopid daemon,,,:/var/lib/avahi-autopid:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
dnsmasq:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false
sssd:x:118:125:sssd system user,,,:/var/lib/sssd:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
nn-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/choot:/usr/sbin/nologin
saned:x:121:128::/var/lib/saned:/usr/sbin/nologin
colord:x:122:129:color colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:123:130::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:124:131:pulseaudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:132:GNOME Initial Setup,,,:/run/gnome-initial-setup:/bin/false
ghplip:x:126:7:HPLIP system user,,,:/run/ghplip:/bin/false
gdm:x:127:133:GNOME Display Manager:/var/lib/gdm3:/bin/false
eroepke:x:1000:1000:Ethan Roepke,,,:/home/eroepke:/bin/bash
fwupd-refresh:x:128:136:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
root@desktop:/home/eroepke#
```

The right terminal window displays the contents of the /etc/shadow file. The output is as follows:

```
daemon:!:19101:0:99999:7:::
bin:!:19101:0:99999:7:::
sys:!:19101:0:99999:7:::
sync:!:19101:0:99999:7:::
games:!:19101:0:99999:7:::
man:!:19101:0:99999:7:::
lp:!:19101:0:99999:7:::
mail:!:19101:0:99999:7:::
neet:!:19101:0:99999:7:::
uucp:!:19101:0:99999:7:::
proxy:!:19101:0:99999:7:::
www-data:!:19101:0:99999:7:::
www:!:19101:0:99999:7:::
list:!:19101:0:99999:7:::
irc:!:19101:0:99999:7:::
gnats:!:19101:0:99999:7:::
nobody:!:19101:0:99999:7:::
systemd-network:!:19101:0:99999:7:::
systemd-resolve:!:19101:0:99999:7:::
messagebus:!:19101:0:99999:7:::
systemd-timesync:!:19101:0:99999:7:::
syslog:!:19101:0:99999:7:::
_apt:!:19101:0:99999:7:::
tss:!:19101:0:99999:7:::
tss:!:19101:0:99999:7:::
uuid:!:19101:0:99999:7:::
systemd-oom:!:19101:0:99999:7:::
tcpdump:!:19101:0:99999:7:::
avahi-autopid:!:19101:0:99999:7:::
usbmux:!:19101:0:99999:7:::
kernoops:!:19101:0:99999:7:::
avahi:!:19101:0:99999:7:::
cups-pk-helper:!:19101:0:99999:7:::
rtkit:!:19101:0:99999:7:::
whoopsie:!:19101:0:99999:7:::
sssd:!:19101:0:99999:7:::
speech-dispatcher:!:19101:0:99999:7:::
nn-openvpn:!:19101:0:99999:7:::
saned:!:19101:0:99999:7:::
colord:!:19101:0:99999:7:::
geoclue:!:19101:0:99999:7:::
pulse:!:19101:0:99999:7:::
gnome-initial-setup:!:19101:0:99999:7:::
hplip:!:19101:0:99999:7:::
gdm:!:19101:0:99999:7:::
eroepke:$y$9tSRM0c9zg80AfhyYjxlhs$WUPNwQ8ocVK01C3IQjlt2Uq5PYzdJBY.HgYctD.Vs2:19600:8:99999:7:::
fwupd-refresh:!:19606:8:99999:7:::
root@desktop:/home/eroepke#
```

The /etc/passwd is a text file with information for all user accounts. It gives information such as User ID, group ID, home directory, and default shell.

The /etc/shadow file stores encrypted user passwords. Only the root user will be able to view to prevent from malicious actors.

## 2. Screenshot of passwd and shadow in middle of user account creation

(10 points)

The image shows two terminal windows side-by-side. Both terminals are running as root on a desktop environment. The top terminal window has a title bar "Activities Terminal" and a status bar "Sep 14 10:51 root@desktop:/home/eroepke". The bottom terminal window has a similar setup. Both terminals display the contents of the /etc/passwd file. The output is identical in both windows:

```
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/bin/sync
games:x:5:60:games:/usr/games/usr/sbin/nologin
man:x:6:12:man:/var/cache/man/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd/usr/sbin/nologin
mail:x:8:8:mail:/var/mail/usr/sbin/nologin
news:x:9:9:news:/var/spool/news/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp/usr/sbin/nologin
proxy:x:13:13:proxy:/var/run/usr/sbin/nologin
backup:x:34:34:backup:/var/backups/usr/sbin/nologin
list:x:38:38:Wailing List Manager:/var/list/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/usr/sbin/nologin
nobody:x:65534:nobody:/nonexistent/usr/sbin/nologin
systemd-network:x:100:102:system Network Management,:/run/systemd/usr/sbin/nologin
systemd-resolve:x:101:103:system Resolver,:/run/systemd/usr/sbin/nologin
messagebus:x:102:105:nonexistent/usr/sbin/nologin
systemd-timesync:x:103:106:system Time Synchronization,:/run/systemd/usr/sbin/nologin
sysLog:x:104:111:/home/syslog/usr/sbin/nologin
apt:x:105:65534:nonexistent/usr/sbin/nologin
tss:x:106:112:TPM software stack,:/var/lib/tpm/bin/false
uuid:x:107:115:run/uldd/usr/sbin/nologin
systemd-oom:x:108:116:system Userspace OOM Killer,:/run/systemd/usr/sbin/nologin
tcpdump:x:109:117:nonexistent/usr/sbin/nologin
avahi-autolp:x:110:119:Avahi autoip daemon,,/var/lib/avahi-autoipd/usr/sbin/nologin
usbmuxd:x:111:120:USBmuxd:/var/run/usbmuxd/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,/var/lib/misc/usr/sbin/nologin
kernoops:x:113:65534:KernelOops Tracking Daemon,:/usr/sbin/nologin
avahi:x:114:121:Avahi MON Daemon,,/run/avahi-daemon/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,:/home/cups-pk-helper/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,:/proc/usr/sbin/nologin
whoopsie:x:117:124:nonexistent:/bin/false
sssd:x:118:125:sssd system user,:/var/lib/sssd/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,:/run/speech-dispatcher/bin/false
openvpn:x:120:126:NetworkManager OpenVPN,,/var/lib/openvpn/choot/usr/sbin/nologin
saned:x:121:128:/var/lib/saned/usr/sbin/nologin
colorl:x:122:129:color colour management daemon,:/var/lib/colorl/usr/sbin/nologin
geoclue:x:123:130:/var/lib/geoclue/usr/sbin/nologin
pulse:x:124:131:PulseAudio daemon,:/run/pulse/usr/sbin/nologin
gnome-initial-setup:x:125:65534:/run/gnome-initial-setup/bin/false
hplip:x:126:7:HPLIP system user,:/run/hplip/bin/false
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3/bin/false
fwupd-refresh:x:128:129:fwupd-refresh user,:/run/systemd/usr/sbin/nologin
test_user:x:1001:1001,:/home/test_user/bin/bash
root@desktop:/home/eroepke#
```

The bottom terminal window shows the same output, indicating that the user 'eroepke' was created during the session.

## 3. Screenshot of new user's home directory contents (ls -la) and the output of the environment variables (echo \$USER \$SHELL)

(5 points)

```
test_user@desktop: $ pwd  
/home/test_user  
test_user@desktop: $ ls -la  
total 20  
drwxr-x--- 2 test_user test_user 4096 Sep 14 10:47 .  
drwxr-xr-x  4 root     root    4096 Sep 14 10:47 ..  
-rw-r--r--  1 test_user test_user  220 Sep 14 10:47 .bash_logout  
-rw-r--r--  1 test_user test_user 3771 Sep 14 10:47 .bashrc  
-rw-r--r--  1 test_user test_user  807 Sep 14 10:47 .profile  
test_user@desktop: $ echo $USER $SHELL  
test_user /bin/bash  
test_user@desktop: $
```

**4. Summarize the Key Differences between nologin and a locked password**

(5 points)

Nologin will prevent the user from logging in entirely and locked password will allow the user to login but will not allow them to change the password. A nologin would be used if you dont want a user to gain access to the system anymore while a locked password would be used if you want to prevent the user from changing the password from something else that you want to know.

**5. Description of the effect of each of the (5) chmod commands**

(10 points)

**chmod 777 filename** - (-rwxrwxrwx) each number corresponds to user, group, and others. 7 gives access to read, write, and execute. 6 would give access to read and write. 5 gives access to read and execute. 4 gives access to read. 3 access to write and execute. 2 access to write. 1 execute. 0 access to nothing.

**chmod 700 filename** - (-rwx-----) user has access to read write and execute while group and others have no access.

**chmod u=rw filename** - letter before = indicates who it is(u,g,o). This is telling us user gets access to read and write but not execute. This will replace old access to the new access(old: ---e new:-rw-)

**chmod go+x filename** - letters before + indicated who it is(u,g,o). Here we are adding access to execute to group and others.

**Chmod a+w filename** - a represents all so user, group, others and added access to execute.

**6. Organized description of directory permissions and how affects contents**

(10 points)

The permissions determine who can read, write, and execute a file in the directory. It also determines who can change the permissions on the directory. Read permission on a directory gives you the ability to read the contents on the file. Write permissions allow you append, remove and rename a file. Execute permission allows you to have access files.

**7. Screenshot and description of /etc/shadow file - who can r/w/x and why it's set this way.**

(10 points)

```
root@desktop:/home/eroepke# ls -l /etc/shadow  
-rw-r----- 1 root shadow 1466 Sep 14 11:03 /etc/shadow  
root@desktop:/home/eroepke#
```

It is set up this way because shadow contains password hashes and we do not want to give access to others to see at all and allow a group to see. Only the user should be able to read and write. You don't want to allow others to gain access and do attacks.

## 8. Meanings of dig queries

(10 points)

Query	What does the query result mean?
dig -t mx iastate.edu	Retrieve DNS records and tells mail how to route mail to domain
dig -t ns iastate.edu	Map a domain name to list of DNS servers for that domain
dig -t soa iastate.edu	Stores important information about a domain
dig -t aaaa iastate.edu	Domains are assigned the IPv6 address for a destination
dig -t any iastate.edu	Shows all domain records and assigned to any

## 9. Screenshot of the (2) netstat outputs

(10 points)

```
[1]+ Stopped                  sudo netcat -l 22
root@desktop:/home/eroepke# netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:ssh              0.0.0.0:*              LISTEN
tcp      0      0 localhost:ipp            0.0.0.0:*              LISTEN
tcp      0      0 localhost:domain        0.0.0.0:*              LISTEN
tcp6     0      0 ip6-localhost:ipp       [::]:*                LISTEN
root@desktop:/home/eroepke# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:22              0.0.0.0:*              LISTEN
tcp      0      0 127.0.0.1:631            0.0.0.0:*              LISTEN
tcp      0      0 127.0.0.53:53           0.0.0.0:*              LISTEN
tcp6     0      0 ::1:631                ::*:*                 LISTEN
root@desktop:/home/eroepke#
```

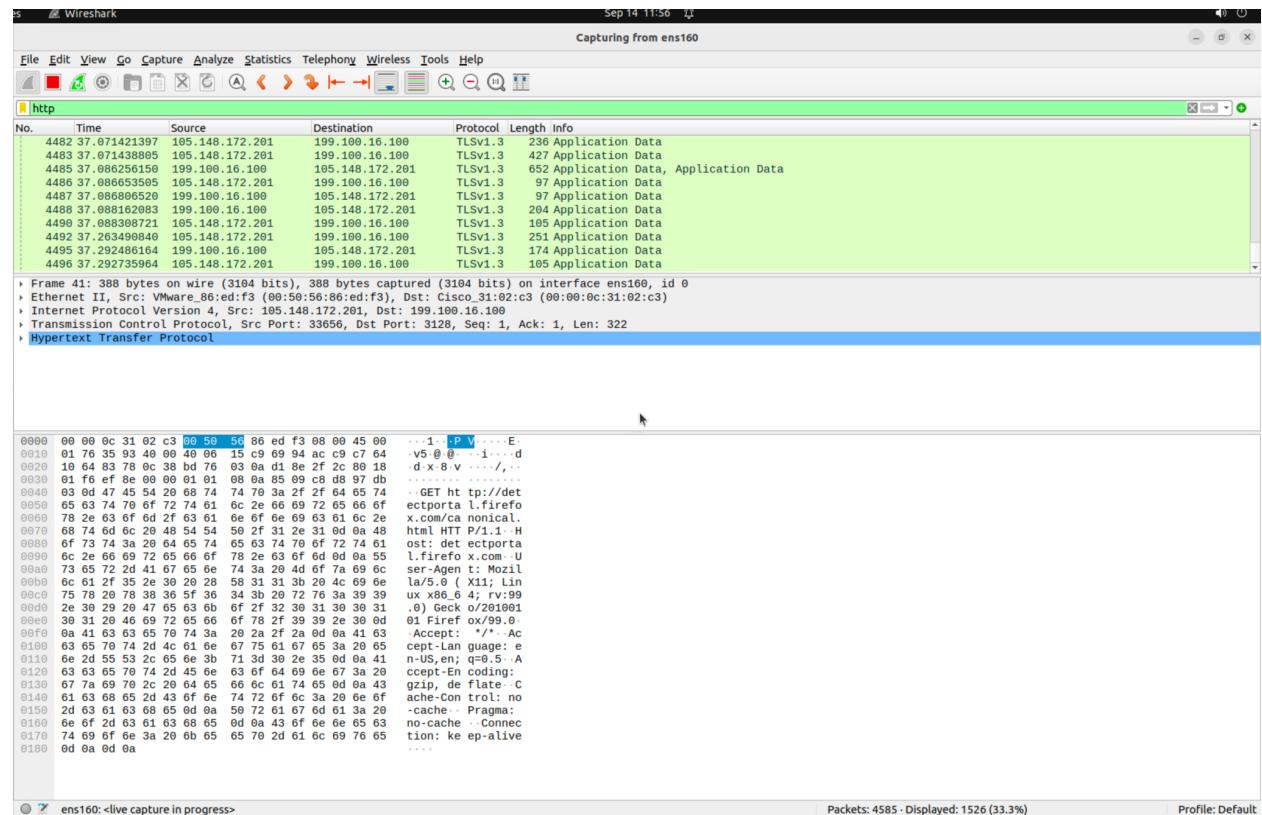
## 10. Complete the netstat flag table

(10 points for all 3 correct meanings; 0 points for anything less)

Flag	Meaning
-t	Sort by time, newest first
-l	Show only listening sockets
-n	Show number addresses instead of determining host, port, or user name

## 11. Screenshot of the captured http traffic using Wireshark

(5 points)



**12. Screenshot of the captured icmp traffic using tcpdump  
(5 points)**