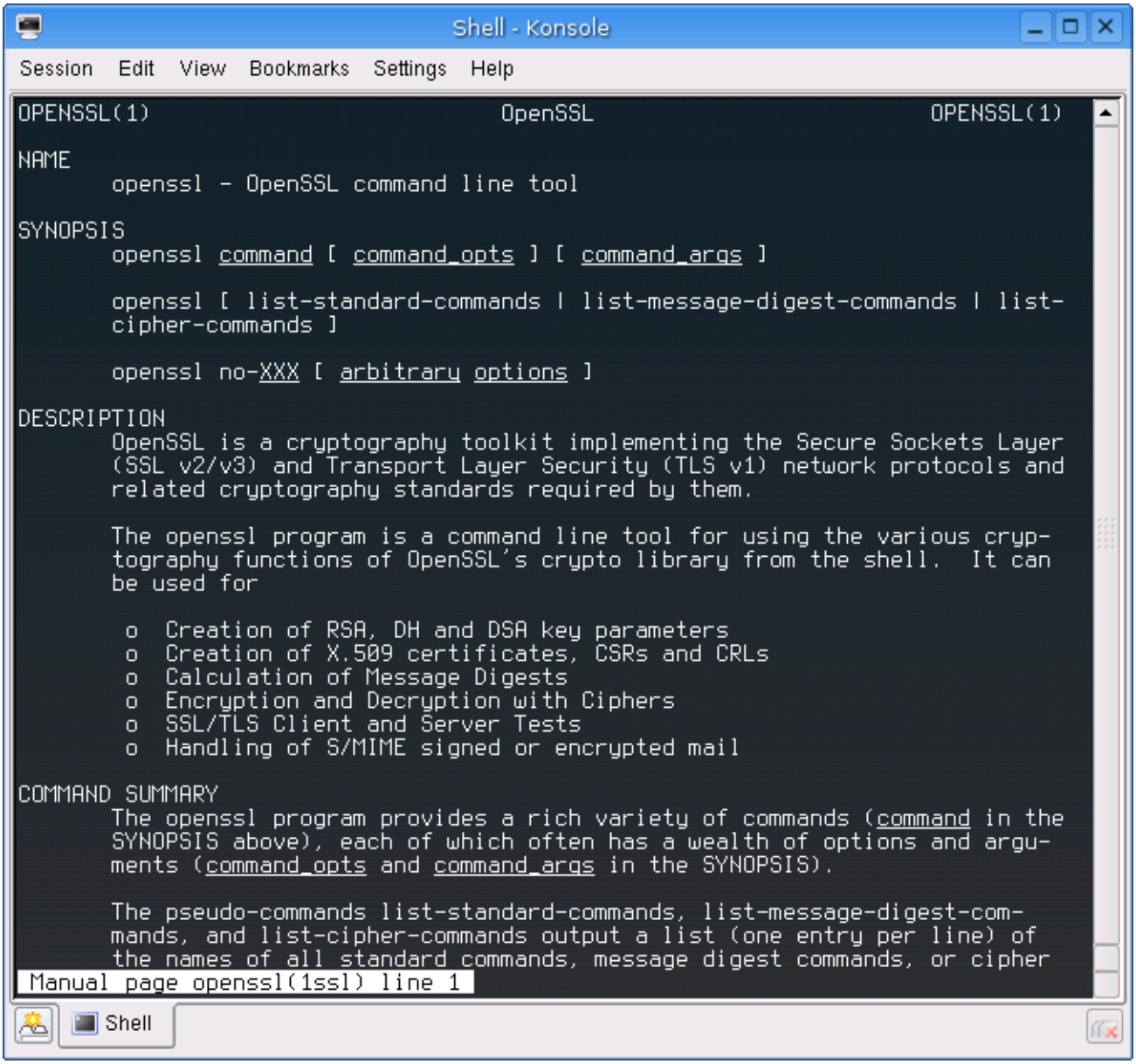
Module Zero:

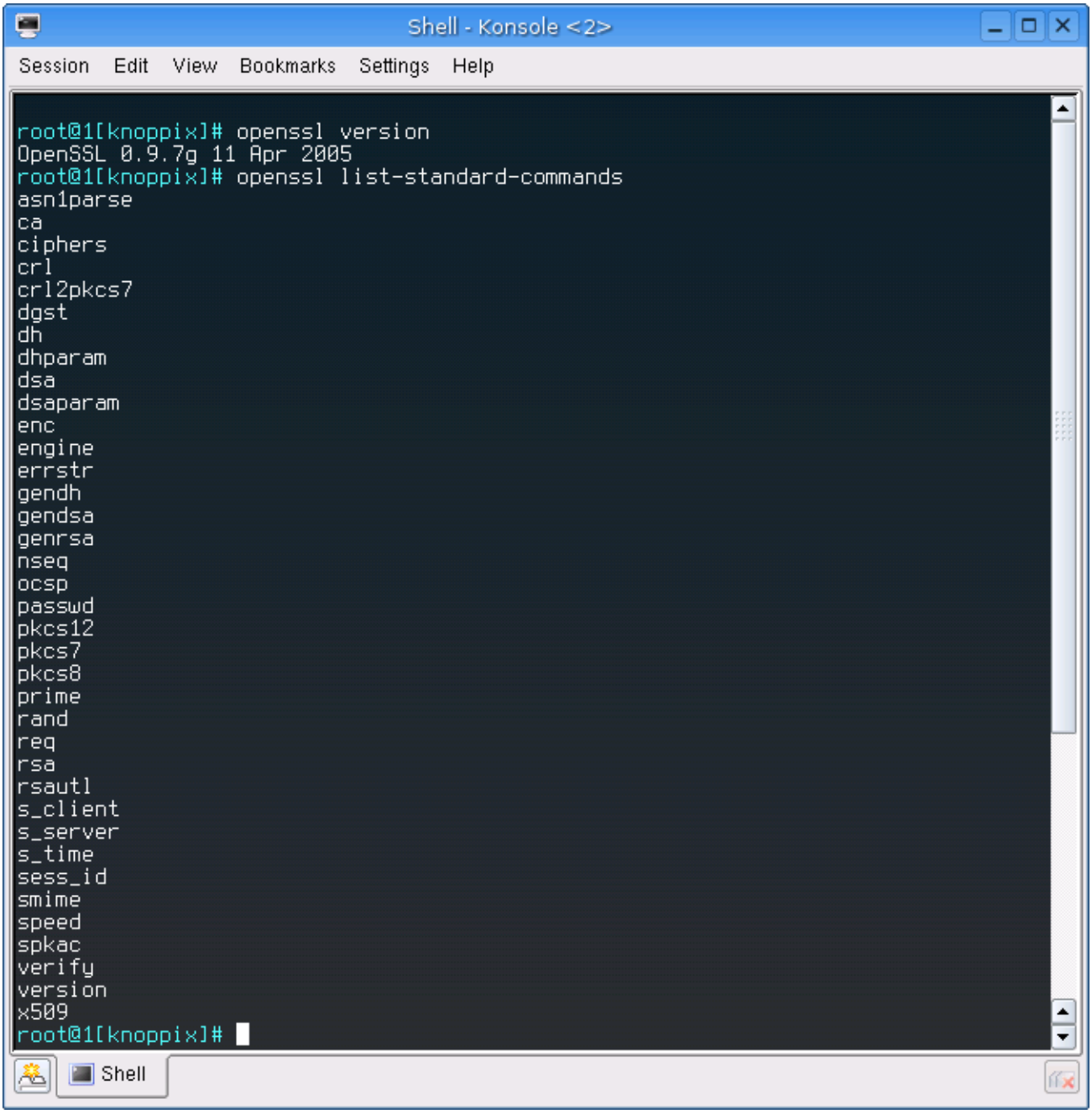
command: man openssl (which gives description of openssl command and options)



command(s):

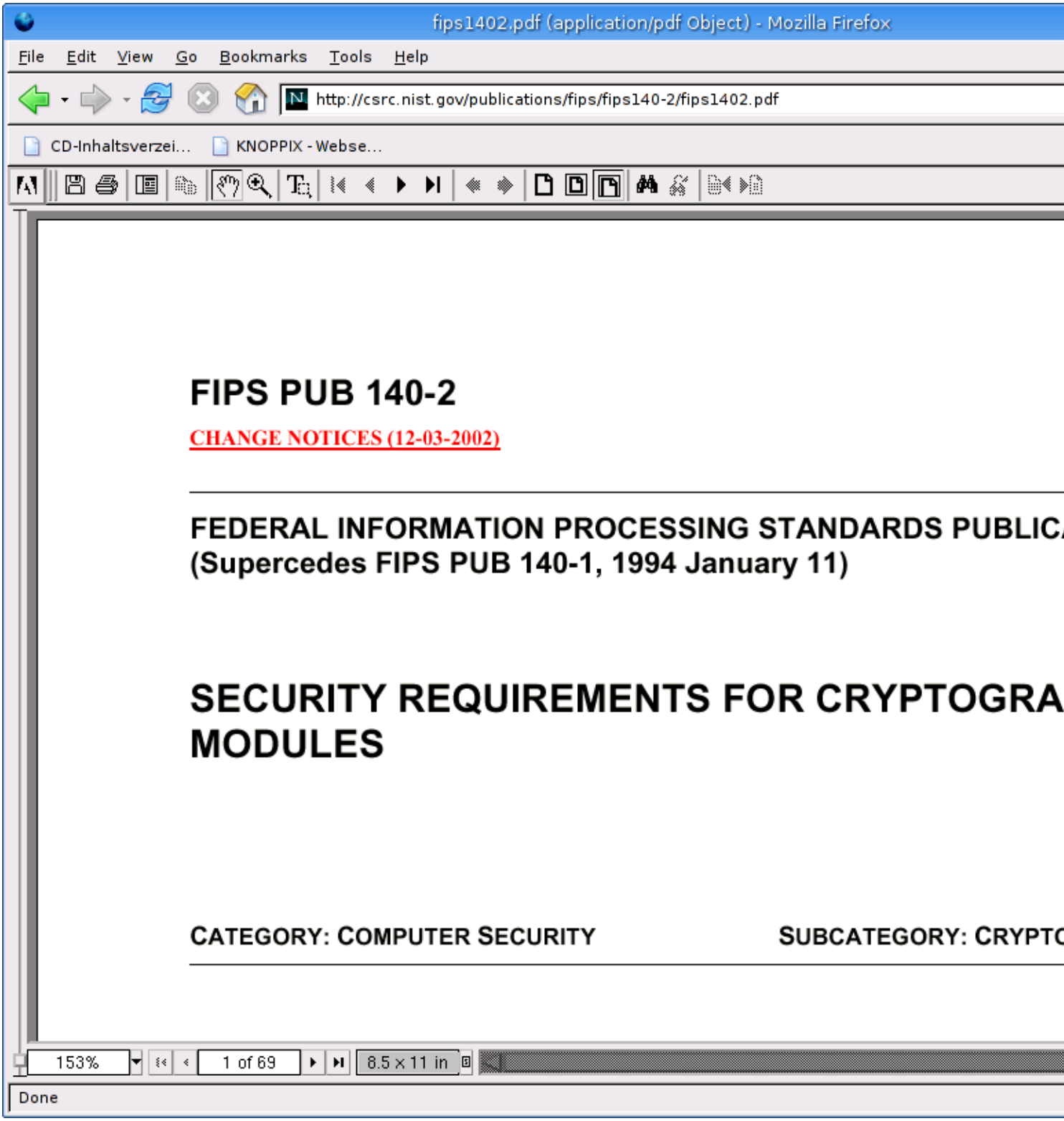
openssl version

openssl list-standard-commands



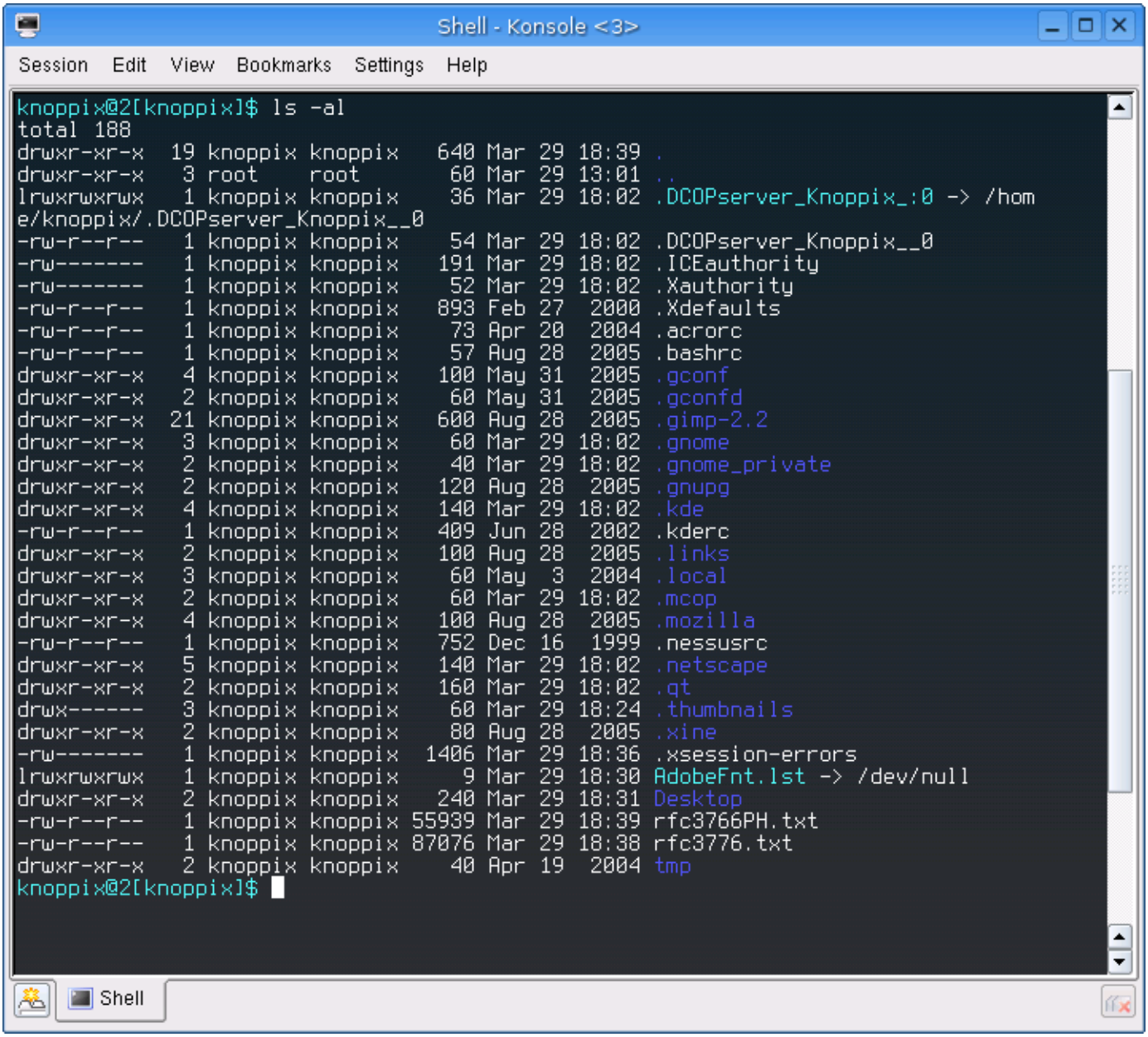
Visiting the OpenSSL web page using the following link: www.openssl.org

Browsing to NIST...

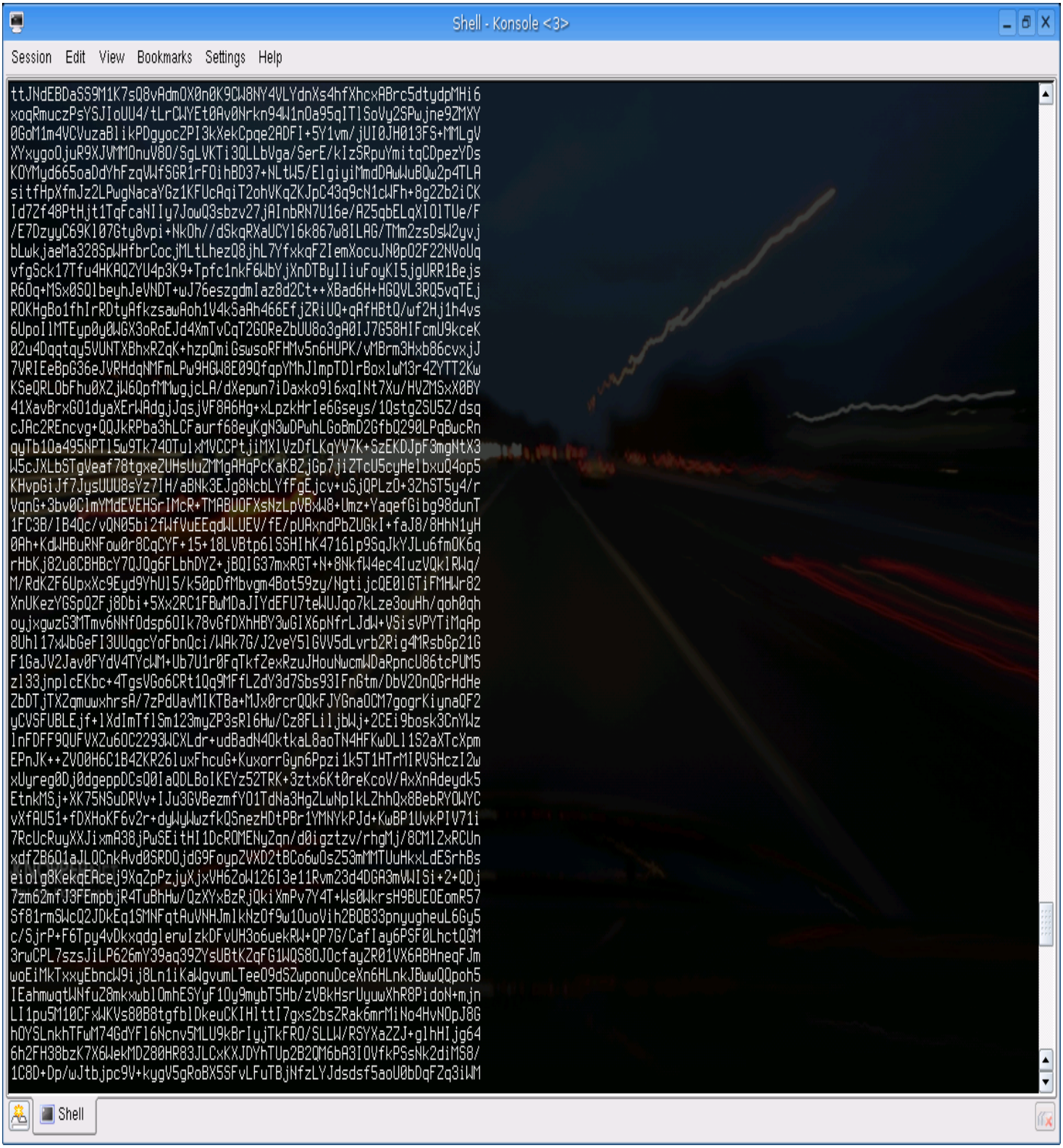


Module One - Symmetric Cryptography

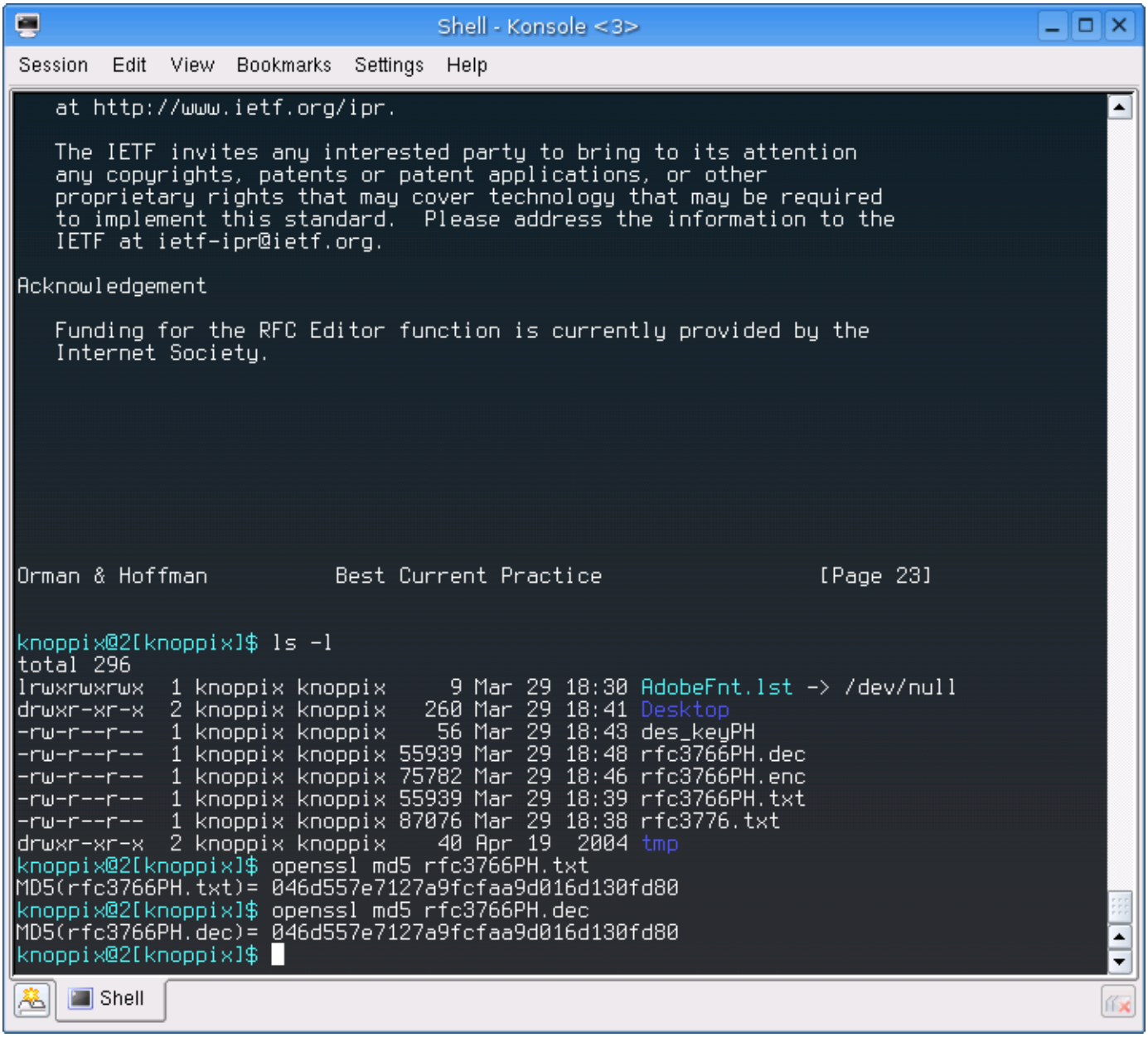
displaying a directory to view the downloaded RFC3766XX.txt file



After generating a key I encrypted the RFC text file and this is the encrypted file displayed:

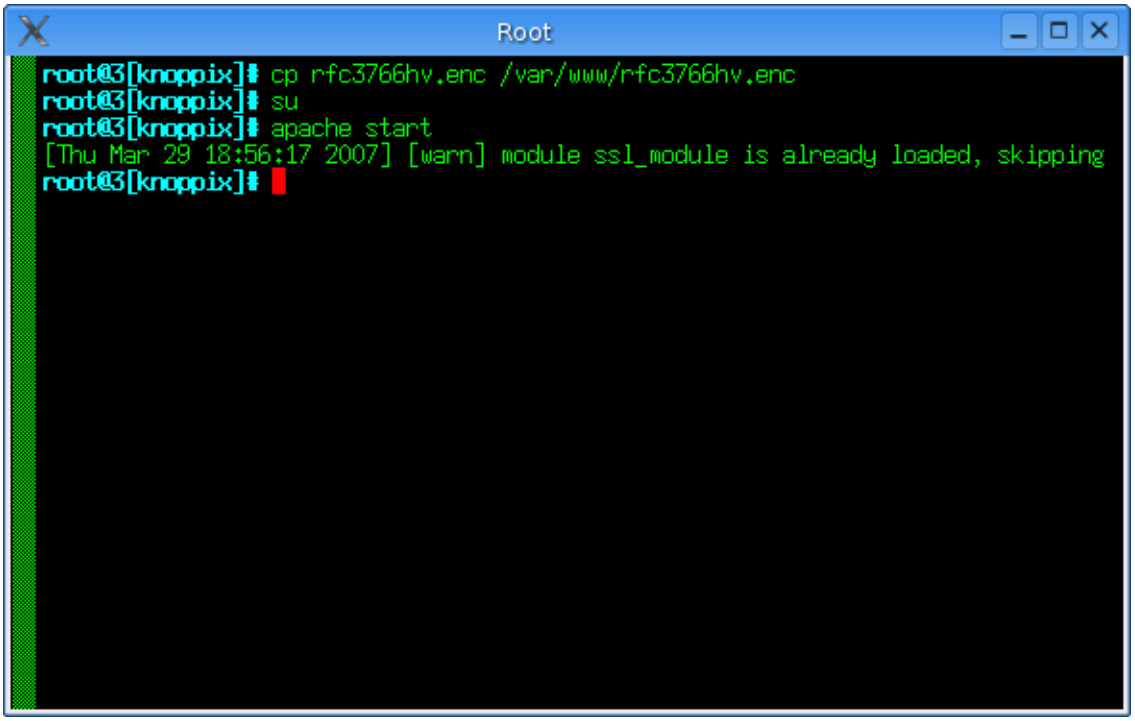


I then decode the file with the key and check the digest to make sure the files are identical:

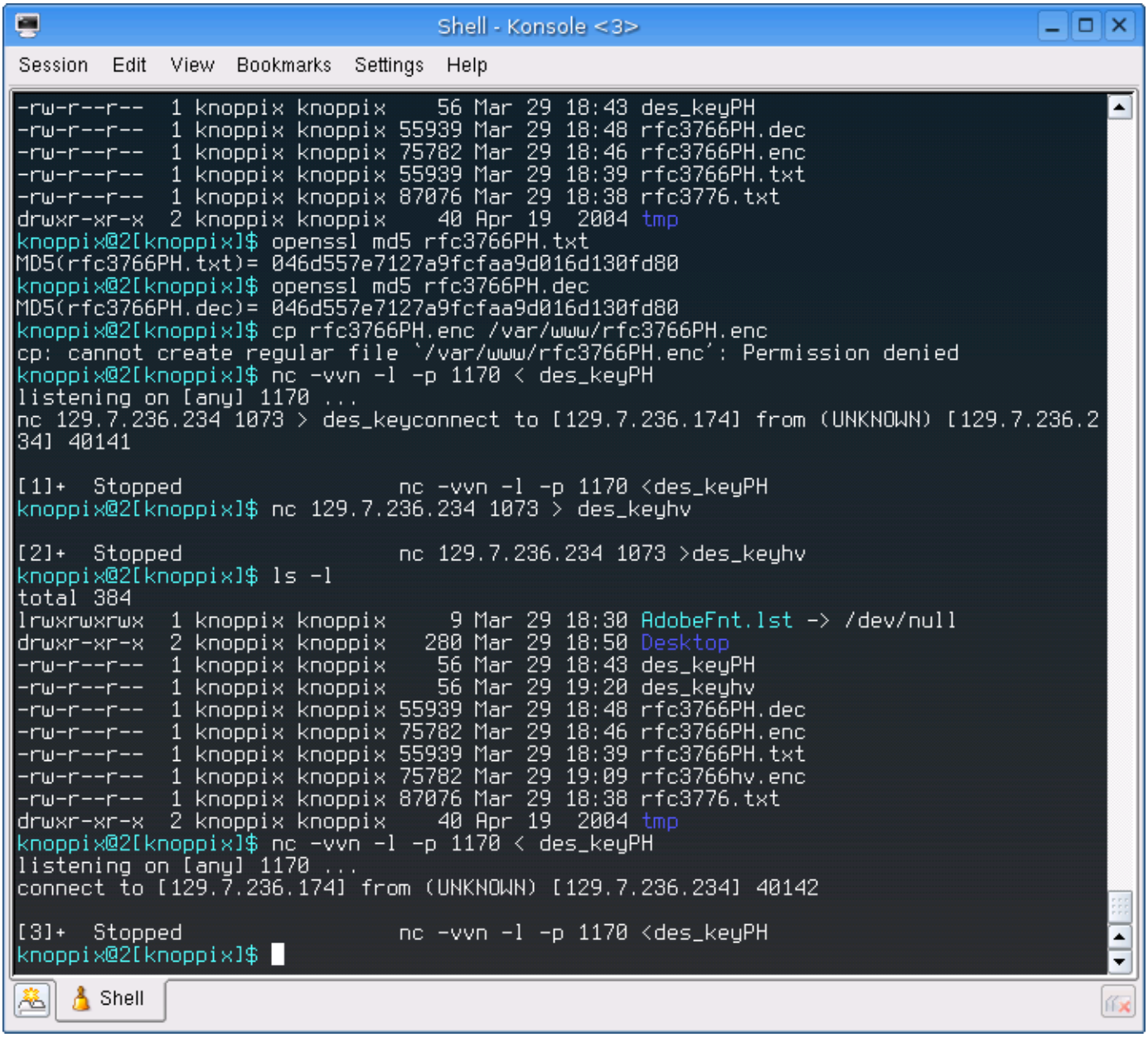


Module One A -- Symmetric Key and File Exchange, Symmetric Decryption

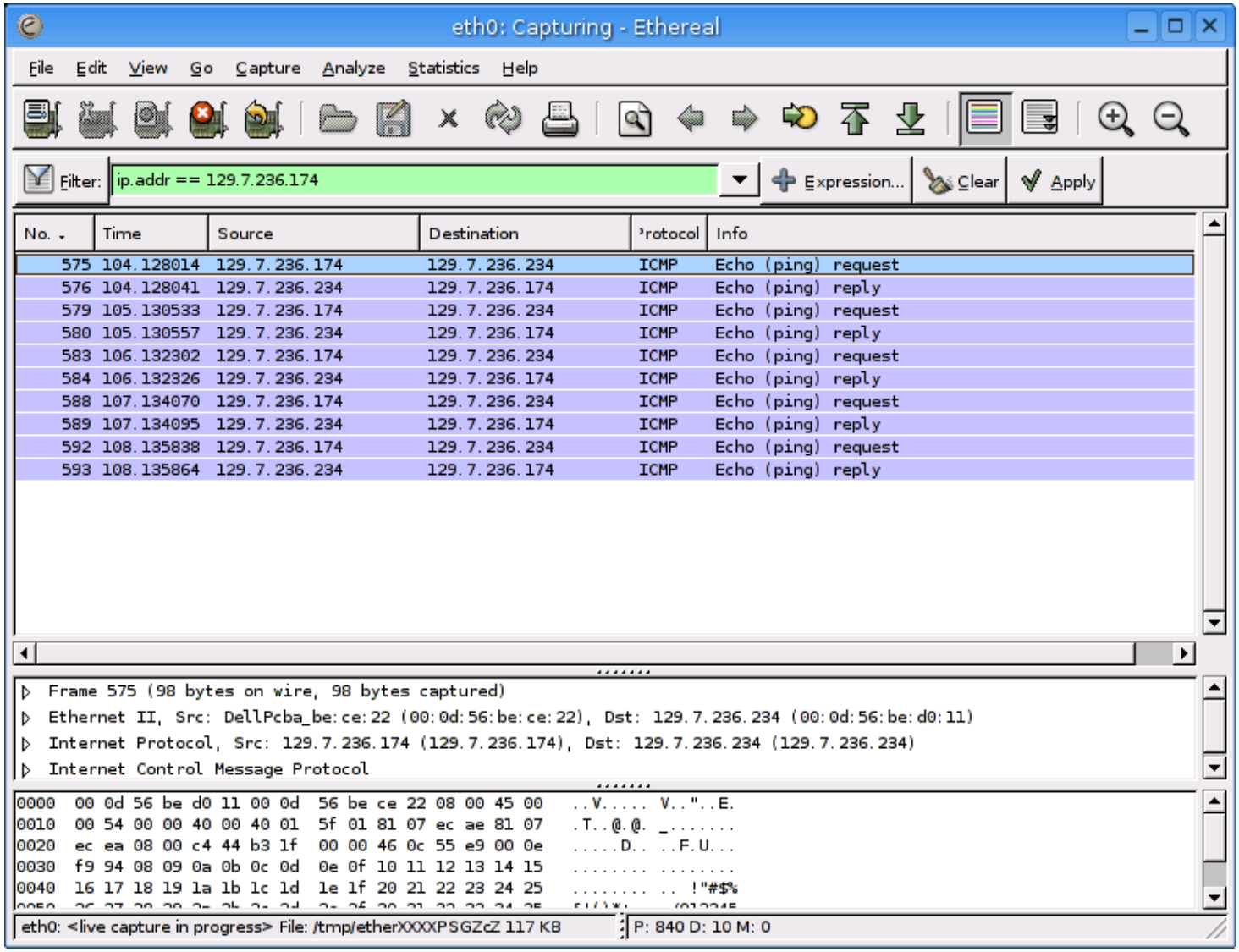
We used the root user to start the Apache service



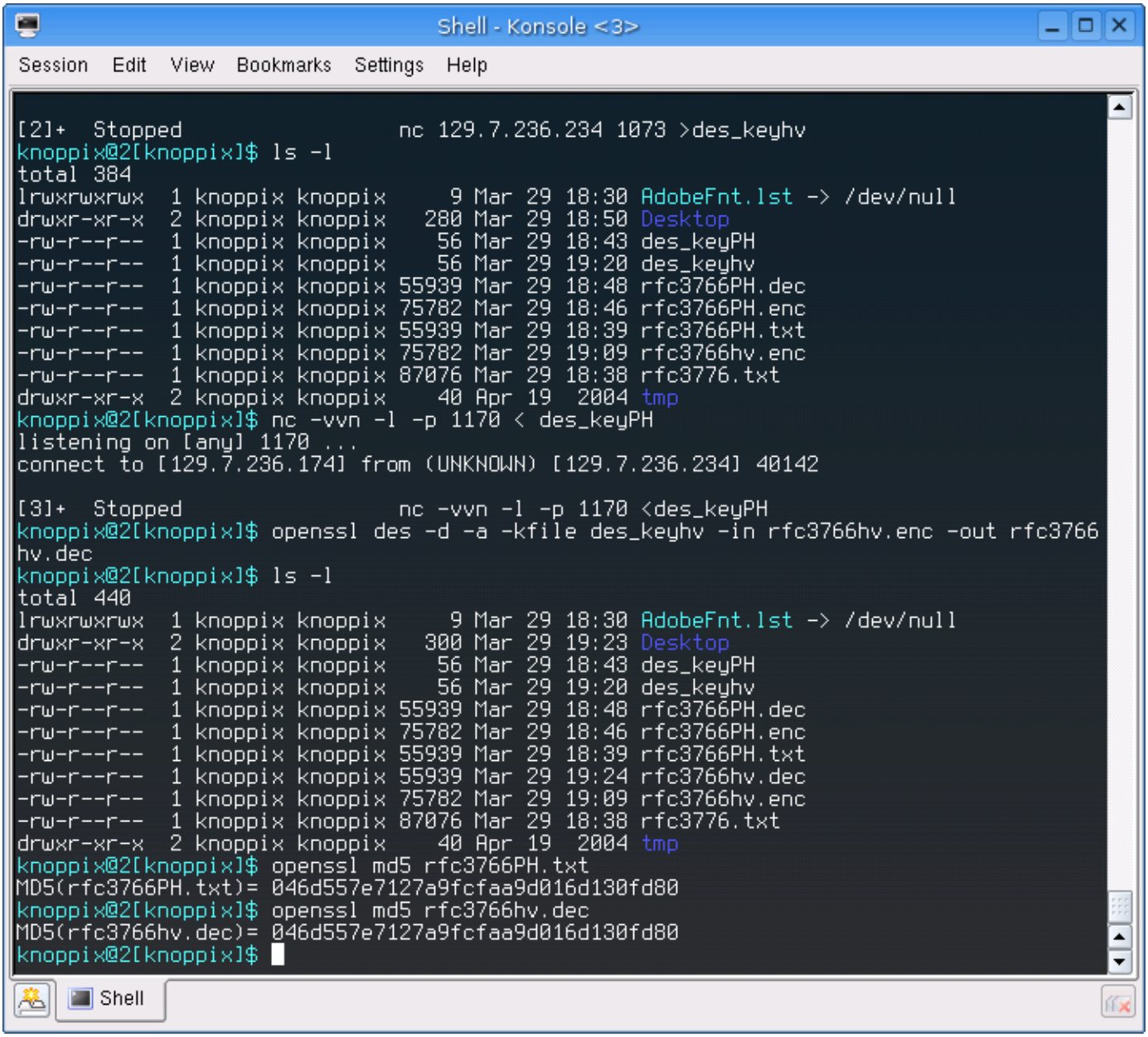
Copying the encrypted file to the web server's default dir.



We had also used Ethereal to capture the packets as we were transferring the files between the partners.



After setting our respective NetCat servers and establishing a connection with our partner, we copied our encrypted files, decrypted our partners files, and verified the digest:


Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
[2]+ Stopped nc 129.7.236.234 1073 >des_keyhv
knoppix@2[knoppix]$ ls -l
total 384
lrwxrwxrwx 1 knoppix knoppix 9 Mar 29 18:30 AdobeFnt.lst -> /dev/null
drwxr-xr-x 2 knoppix knoppix 280 Mar 29 18:50 Desktop
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:43 des_keyPH
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 19:20 des_keyhv
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:48 rfc3766PH.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 18:46 rfc3766PH.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:39 rfc3766PH.txt
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 19:09 rfc3766hv.enc
-rw-r--r-- 1 knoppix knoppix 87076 Mar 29 18:38 rfc3776.txt
drwxr-xr-x 2 knoppix knoppix 40 Apr 19 2004 tmp
knoppix@2[knoppix]$ nc -vvn -l -p 1170 < des_keyPH
listening on [any] 1170 ...
connect to [129.7.236.174] from (UNKNOWN) [129.7.236.234] 40142
[3]+ Stopped nc -vvn -l -p 1170 <des_keyPH
knoppix@2[knoppix]$ openssl des -d -a -kfile des_keyhv -in rfc3766hv.enc -out rfc3766
hv.dec
knoppix@2[knoppix]$ ls -l
total 440
lrwxrwxrwx 1 knoppix knoppix 9 Mar 29 18:30 AdobeFnt.lst -> /dev/null
drwxr-xr-x 2 knoppix knoppix 300 Mar 29 19:23 Desktop
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:43 des_keyPH
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 19:20 des_keyhv
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:48 rfc3766PH.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 18:46 rfc3766PH.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:39 rfc3766PH.txt
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 19:24 rfc3766hv.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 19:09 rfc3766hv.enc
-rw-r--r-- 1 knoppix knoppix 87076 Mar 29 18:38 rfc3776.txt
drwxr-xr-x 2 knoppix knoppix 40 Apr 19 2004 tmp
knoppix@2[knoppix]$ openssl md5 rfc3766PH.txt
MD5(rfc3766PH.txt)= 046d557e7127a9fcfaa9d016d130fd80
knoppix@2[knoppix]$ openssl md5 rfc3766hv.dec
MD5(rfc3766hv.dec)= 046d557e7127a9fcfaa9d016d130fd80
knoppix@2[knoppix]$
Shell