Cryptography Lab

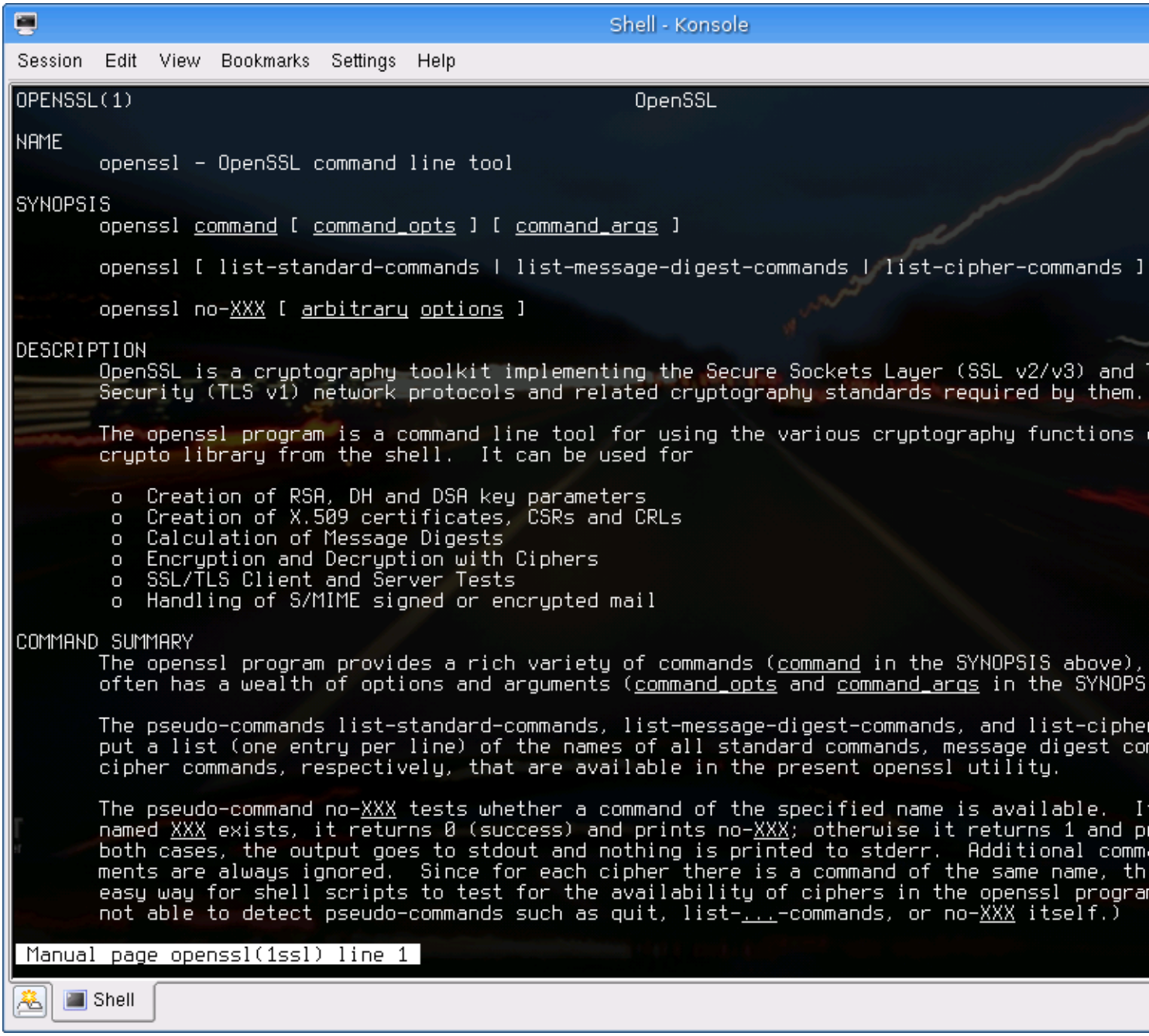
Group Members
Harris Verdun
Pablo Hernandez
Ramier McIntyre
Heber Paz

Objectives

- To do a hands on activity to encrypt our data
- Learn how to use symmetric cryptography to encrypt and decrypt a message
- Learn how to transfer files with a lab partner

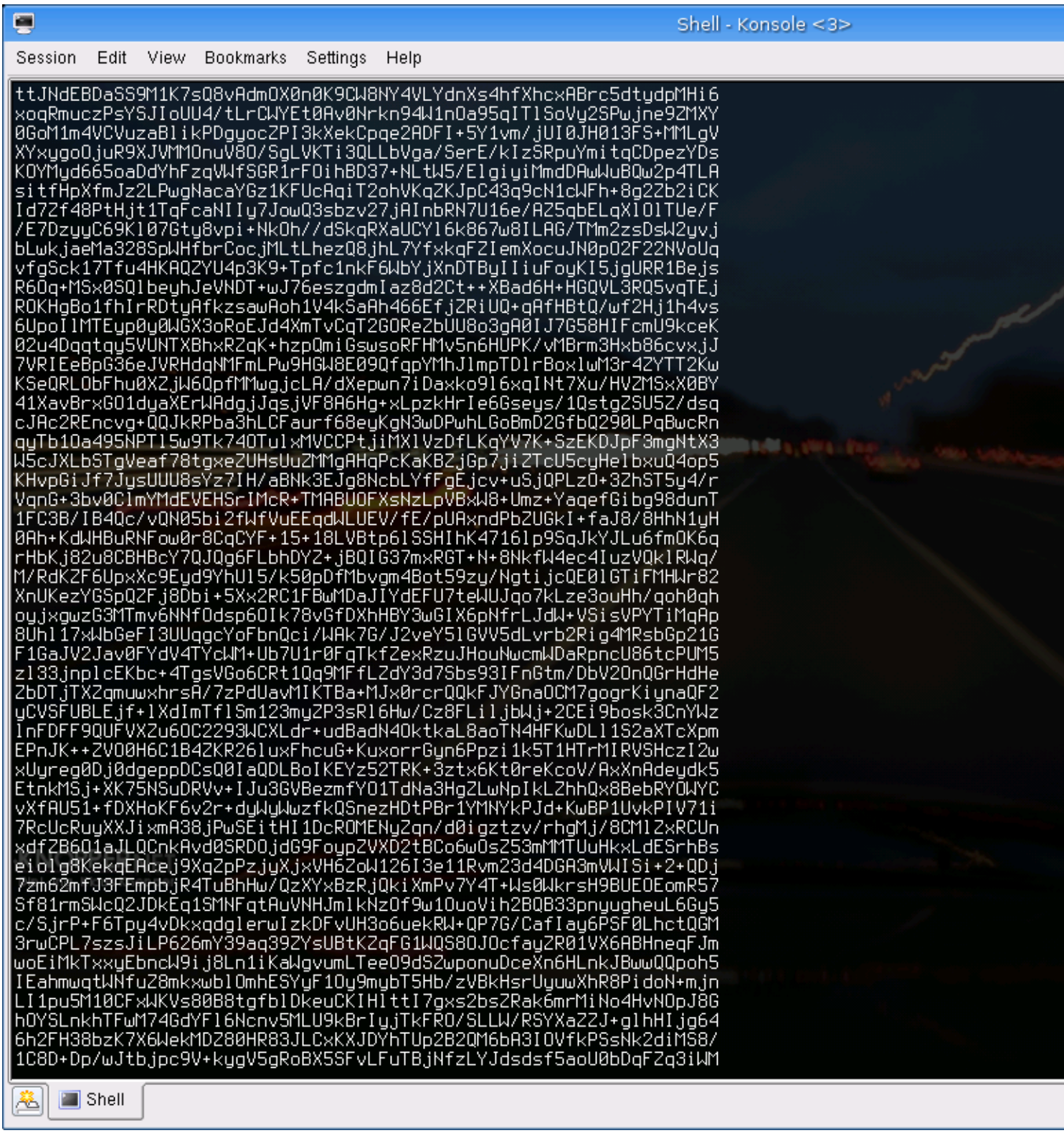
Executive Summary

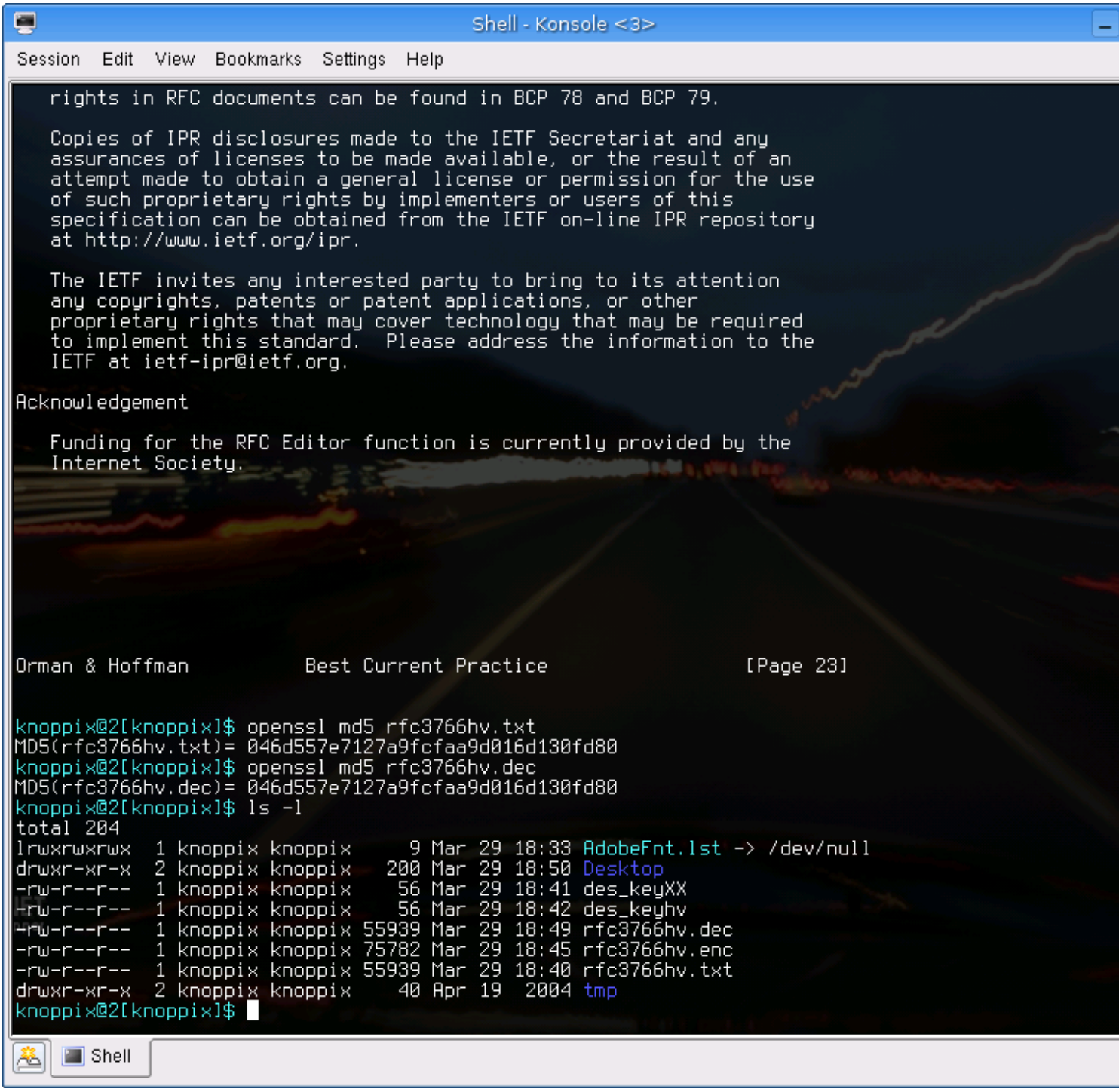
This lab focused on symmetric cryptography. We first created a key with a 56 bit encryption. Then we encrypted a file with that key, and transferred the file and the key with our lab partner. Our lab partner then downloaded the encrypted file, and with the key that we created. Then we decrypted the partners file with the respective key.



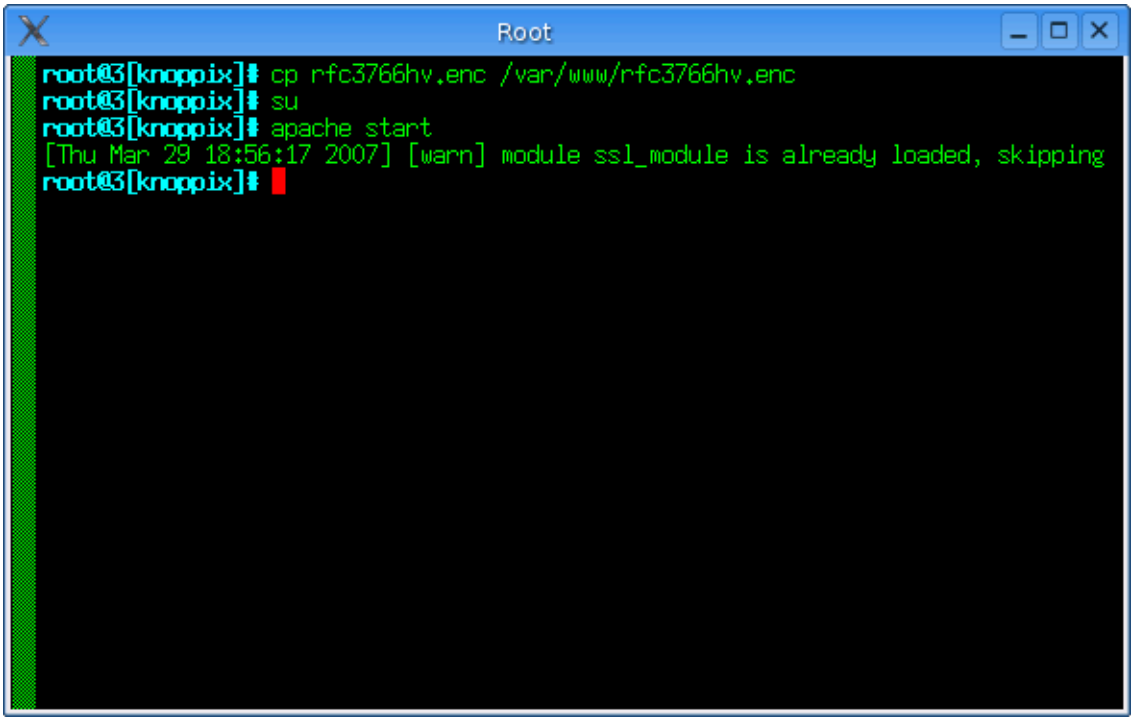
This is the OpenSSL website

This is what our file looked like once it was encrypted.

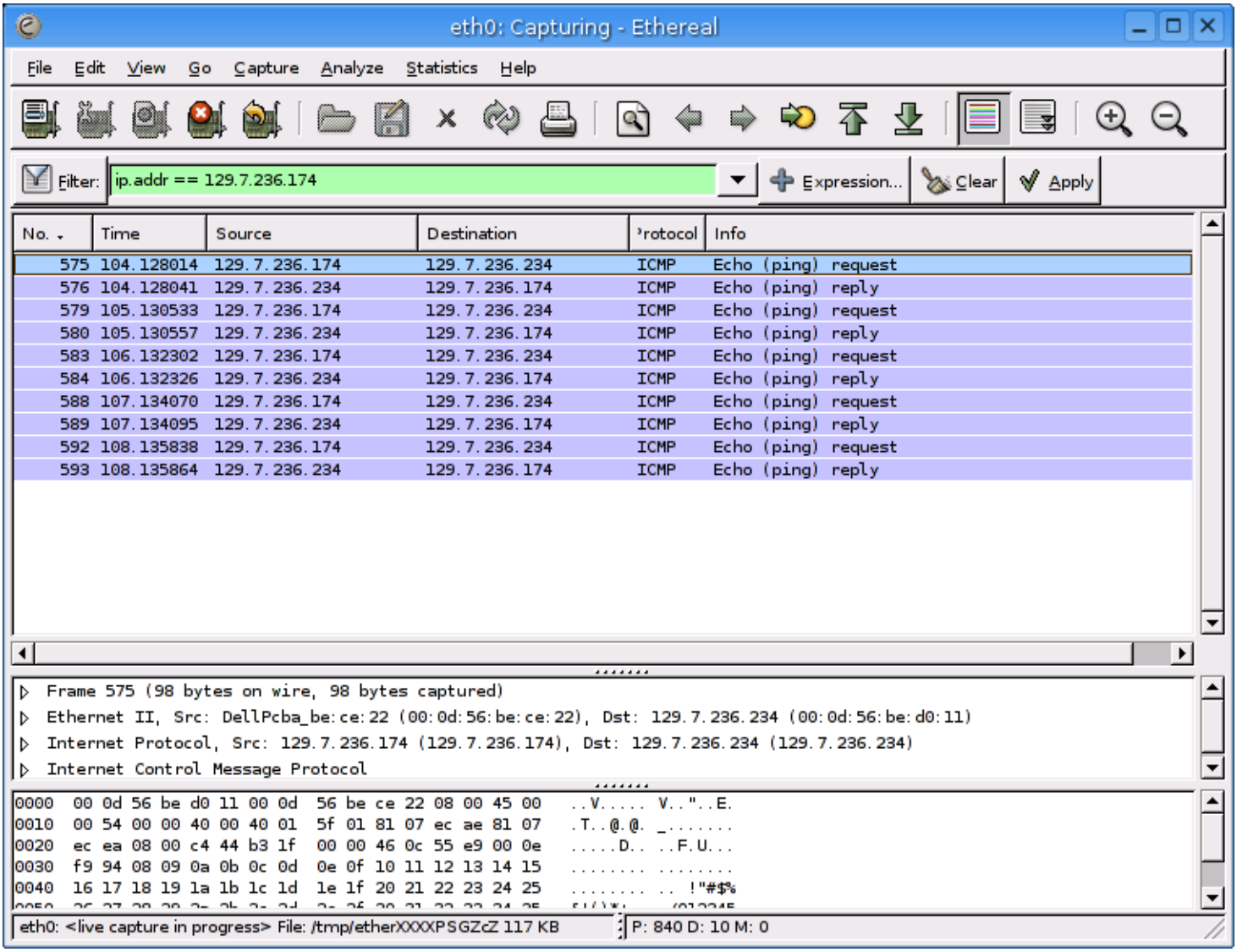

Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
ttJNdEBDaSS9M1K7sQ8vAdmOX0n0K9CW8NY4VLYdnXs4hfXhcxABrc5dtydpMHi6
xoqRmuczPsYSJIoUU4/tLrCWYEt0Av0Nrkn94W1nOa95qITlSoVy2SPwjne9ZMXY
0GoM1m4VCVuzaBlikPDgyocZPI3kXekCpqe2ADFI+5Y1vm/jUI0JH013FS+MMLgV
XYxygoOjuR9XJVMMOnuV8O/SgLVKTi3QLLbVga/SerE/kIzSRpuYmitqCDpezYDs
KOYMyd665oaDdYhFzqVWfSGR1rFOihBD37+NLtW5/ElgiyiMmdDAwWuBQw2p4TLA
sitfHpXfmJz2LPwgNacaYGz1KFUcAqiT2ohVKqZKJpC43q9cN1cWFh+8g2Zb2iCK
Id7Zf48PtHjt1TqFcaNIIy7JowQ3sbzv27jAInbRN7U16e/AZ5qbELqXlOlTUe/F
/E7DzyyC69Kl07Gty8vpi+NkOh//dSkqRXaUCYl6k867w8ILAG/TMm2zsDsW2yvj
bLwkjaeMa328SpWHfbrCocjMLtLhezQ8jhL7YfxkqFZIemXocuJN0pO2F22NVoUq
vfgSck17Tfu4HKAQZYU4p3K9+Tpfc1nkF6WbYjXnDTByIIiuFoyKI5jgURR1Bejs
R6Oq+MSx0SQlbeyhJeVNDT+wJ76eszgdmIaz8d2Ct++XBad6H+HGQVL3RQ5vqTEj
ROKHgBo1fhIrRDtyAfkzsawAoh1V4kSaAh466EfjZRiUQ+qAfHBtQ/wf2Hj1h4vs
6UpoIlMTEyp0y0WGX3oRoEJd4XmTvCqT2GOReZbUU8o3gA0IJ7G58HIFcmU9kceK
02u4Dqqtqy5VUNTXBhxRZqK+hzpQmiGswsoRFHMv5n6HUPK/vMBrm3Hxb86cvxjJ
7VRIEeBpG36eJVRHdqNMFmLPw9HGW8E09QfqpYMhJlmpTDlrBoxlwM3r4ZYTT2Kw
KSeQRLObFhu0XZjW6QpfMMwgjcLA/dXepwn7iDaxko9l6xqINt7Xu/HVZMSxX0BY
41XavBrxGO1dyaXErWAdgjJqsjVF8A6Hg+xLpzkHrIe6Gseys/1QstgZSU5Z/dsq
cJAc2REncvg+QQJkRPba3hLCFaurf68eyKgN3wDPwhLGoBmD2GfbQ290LPqBwcRn
qyTb1Oa495NPTl5w9Tk74OTulxMVCCPtjiMXlVzDfLKqYV7K+SzEKDJpF3mgNtX3
W5cJXLbSTgVeaf78tgxeZUHsUuZMMgAHqPcKaKBZjGp7jiZTcU5cyHelbxuQ4op5
KHvpGiJf7JysUUU8sYz7IH/aBNk3EJg8NcbLYfFgEjcv+uSjQPLzO+3ZhST5y4/r
VqnG+3bv0ClmYMdEVEHSrIMcR+TMABUOFXsNzLpVBxW8+Umz+YaqefGibg98dunT
1FC3B/IB4Qc/vQN05bi2fWfVuEEqdWLUEV/fE/pUAxndPbZUGkI+faJ8/8HhN1yH
0Ah+KdWHBuRNFow0r8CqCYF+15+18LVBtp6lSSHIhK47161p9SqJkYJLu6fmOK6q
rHbKj82u8CBHBcY7QJQg6FLbhDYZ+jBQIG37mxRGT+N+8NkfW4ec4IuzVQklRWq/
M/RdKZF6UpxXc9Eyd9YhUl5/k50pDfMbvgm4Bot59zy/NgtijcQE0lGTiFMHWr82
XnUKezYGSpQZFj8Dbi+5Xx2RC1FBwMDaJIYdEFU7teWUJqo7kLze3ouHh/qoh0qh
oyjxgwzG3MTmv6NNfOdsp6OIk78vGfDXhHBY3wGIX6pNfrLJdW+VSisVPYTiMqAp
8Uhl17xWbGeFI3UUqgcYoFbnQci/WAk7G/J2veY5lGVV5dLvrb2Rig4MRsbGp21G
F1GaJV2Jav0FYdV4TYcWM+Ub7U1r0FqTkfZexRzuJHouNwcmWDaRpncU86tcPUM5
zl33jnplcEKbc+4TgsVGo6CRt1Qq9MFfLZdY3d7Sbs93IFnGtm/DbV2OnQGrHdHe
ZbDTjTXZqmuwxhrsA/7zPdUavMIKTBa+MJx0rcrQQkFJYGnaOCM7gogrKiynaQF2
yCVSFUBLEjf+lXdImTflSm123myZP3sRl6Hw/Cz8FLiljbWj+2CEi9bosk3CnYWz
lnFDFF9QUFVXZu6OC2293WCXLdr+udBadN4OktkaL8aoTN4HFKwDLl1S2aXTcXpm
EPnJK++2VO0H6C1B4ZKR26luxFhcuG+KuxorrGyn6Ppzi1k5T1HTrMIRVSHczI2w
xUyreg0Dj0dgeppDCsQ0IaQDLBoIKEYz52TRK+3ztx6Kt0reKcoV/AxXnAdeydk5
EtnkMSj+XK75NSuDRVv+IJu3GVBezmfYO1TdNa3HgZLwNpIkLZhhQx8BebRYOWYC
vXfAU51+fDXHoKF6v2r+dyWyWwzfkQSnezHDtPBr1YMNYkPJd+KwBP1UvkPIV71i
7RcUcRuyXXJixmA38jPwSEitHI1DcROMENyZqn/d0igztzv/rhgMj/8CM1ZxRCUn
xdfZB6O1aJLQCnkAvd0SRDOjdG9FoypZVXD2tBCo6wOsZ53mMMTUuHkxLdESrhBs
eiolg8KekqEAcej9XqZpPzjyXjxVH6ZoW126I3e11Rvm23d4DGA3mVWISi+2+QDj
7zm62mfJ3FEmpbjR4TuBhHw/QzXYxBzRjQkiXmPv7Y4T+Ws0WkrsH9BUEOEomR57
Sf81rmSWcQ2JDkEq1SMNFqtAuVNHJmlkNzOf9w1OuoVih2BQB33pnyugheuL6Gy5
c/SjrP+F6Tpy4vDkxqdglerwIzkDFvUH3o6uekRW+QP7G/CafIay6PSF0LhctQGM
3rwCPL7szsJiLP626mY39aq39ZYsUBtKZqFG1WQS8OJOcfayZR01VX6ABHneqFJm
woEiMkTxxyEbncW9ij8Ln1iKaWgvumLTeeO9dSZwponuDceXn6HLnkJBwwQQpoh5
IEahmwqtWNfuZ8mkxwblOmhESYyF1Oy9mybT5Hb/zVBkHsrUyuwXhR8PidoN+mjn
LI1pu5M10CFxWKVs80B8tgfblDkeuCKIHlttI7gxs2bsZRak6mrMiNo4HvNOpJ8G
hOYSLnkhTFwM74GdYFl6Ncnv5MLU9kBrIyjTkFRO/SLLW/RSYXaZZJ+glhHIjg64
6h2FH38bzK7X6WekMDZ80HR83JLCxKXJDYhTUp2B2QM6bA3IOVfkPSsNk2diMS8/
1C8D+Dp/wJtbjpc9V+kygV5gRoBX5SFvLFuTBjNfzLYJdsdsf5aoU0bDqFZq3iWM
Shell



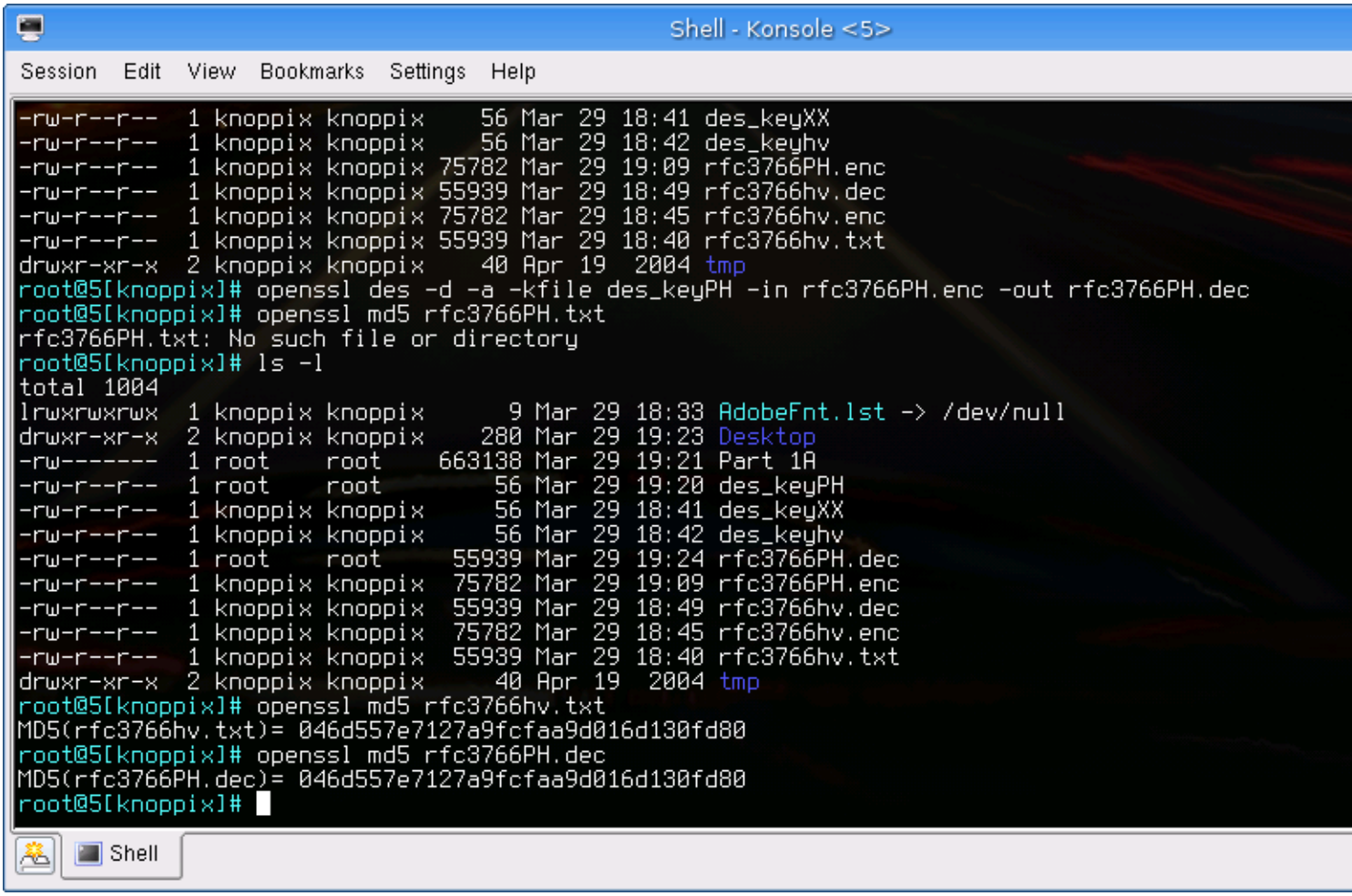
We used the root user to start the Apache service



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



Here you can see where one of our partners after they exchanged the des_key, and verfied the hash.


Shell - Konsole <5>
Session Edit View Bookmarks Settings Help
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:41 des_keyXX
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:42 des_keyhv
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 19:09 rfc3766PH.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:49 rfc3766hv.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 18:45 rfc3766hv.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:40 rfc3766hv.txt
drwxr-xr-x 2 knoppix knoppix 40 Apr 19 2004 tmp
root@5[knoppix]# openssl des -d -a -kfile des_keyPH -in rfc3766PH.enc -out rfc3766PH.dec
root@5[knoppix]# openssl md5 rfc3766PH.txt
rfc3766PH.txt: No such file or directory
root@5[knoppix]# ls -l
total 1004
lrwxrwxrwx 1 knoppix knoppix 9 Mar 29 18:33 AdobeFnt.lst -> /dev/null
drwxr-xr-x 2 knoppix knoppix 280 Mar 29 19:23 Desktop
-rw------- 1 root root 663138 Mar 29 19:21 Part 1A
-rw-r--r-- 1 root root 56 Mar 29 19:20 des_keyPH
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:41 des_keyXX
-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:42 des_keyhv
-rw-r--r-- 1 root root 55939 Mar 29 19:24 rfc3766PH.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 19:09 rfc3766PH.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:49 rfc3766hv.dec
-rw-r--r-- 1 knoppix knoppix 75782 Mar 29 18:45 rfc3766hv.enc
-rw-r--r-- 1 knoppix knoppix 55939 Mar 29 18:40 rfc3766hv.txt
drwxr-xr-x 2 knoppix knoppix 40 Apr 19 2004 tmp
root@5[knoppix]# openssl md5 rfc3766hv.txt
MD5(rfc3766hv.txt)= 046d557e7127a9fcfaa9d016d130fd80
root@5[knoppix]# openssl md5 rfc3766PH.dec
MD5(rfc3766PH.dec)= 046d557e7127a9fcfaa9d016d130fd80
root@5[knoppix]#
Shell