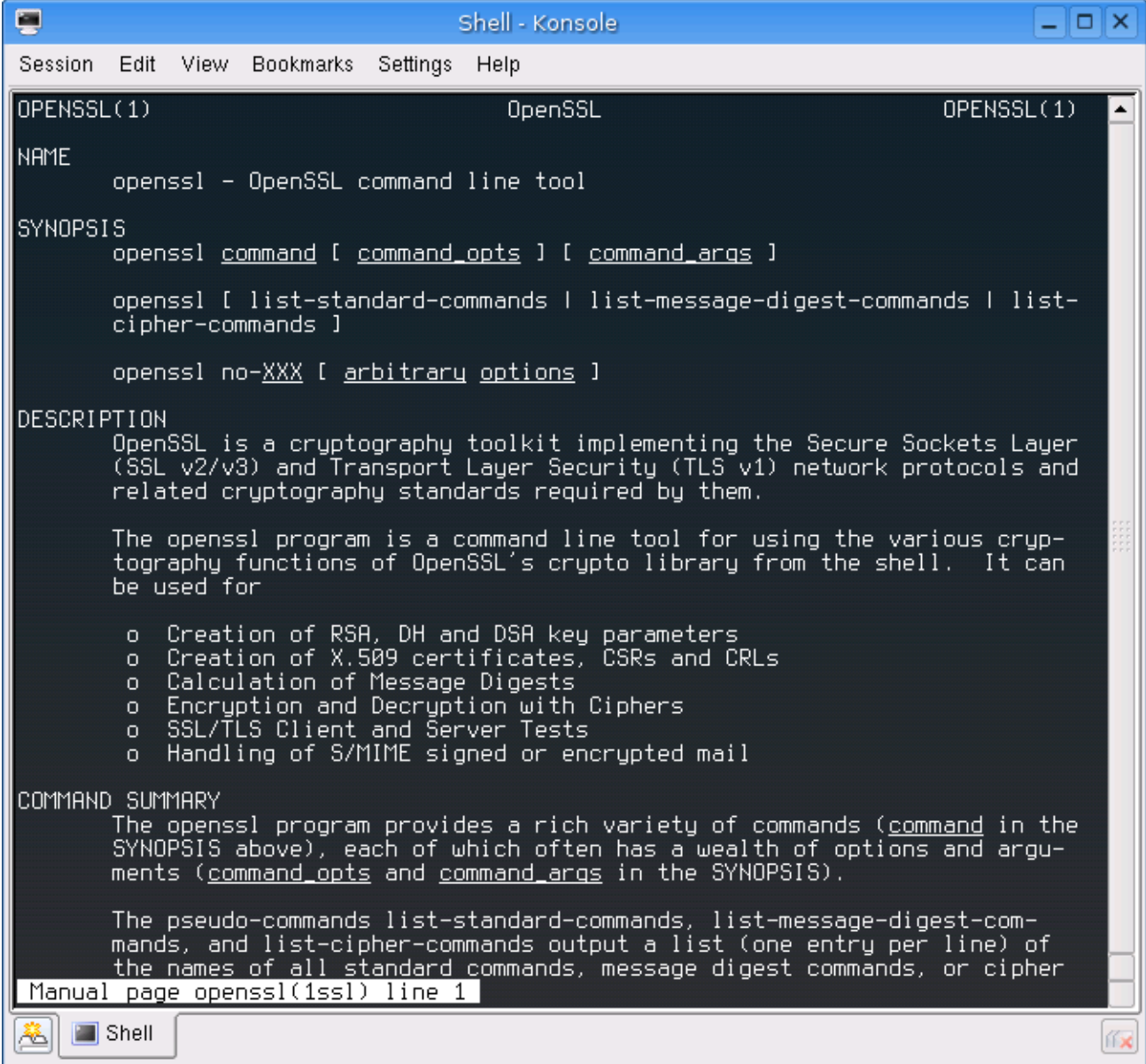


Module Zero:

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



```
Shell - Konsole
Session Edit View Bookmarks Settings Help
OPENSSL(1)                                OpenSSL                                OPENSSL(1)
NAME
  openssl - OpenSSL command line tool
SYNOPSIS
  openssl command [ command_opts ] [ command_args ]

  openssl [ list-standard-commands | list-message-digest-commands | list-
  cipher-commands ]

  openssl no-XXX [ arbitrary options ]
DESCRIPTION
  OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer
  (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and
  related cryptography standards required by them.

  The openssl program is a command line tool for using the various cryp-
  tography functions of OpenSSL's crypto library from the shell. It can
  be used for

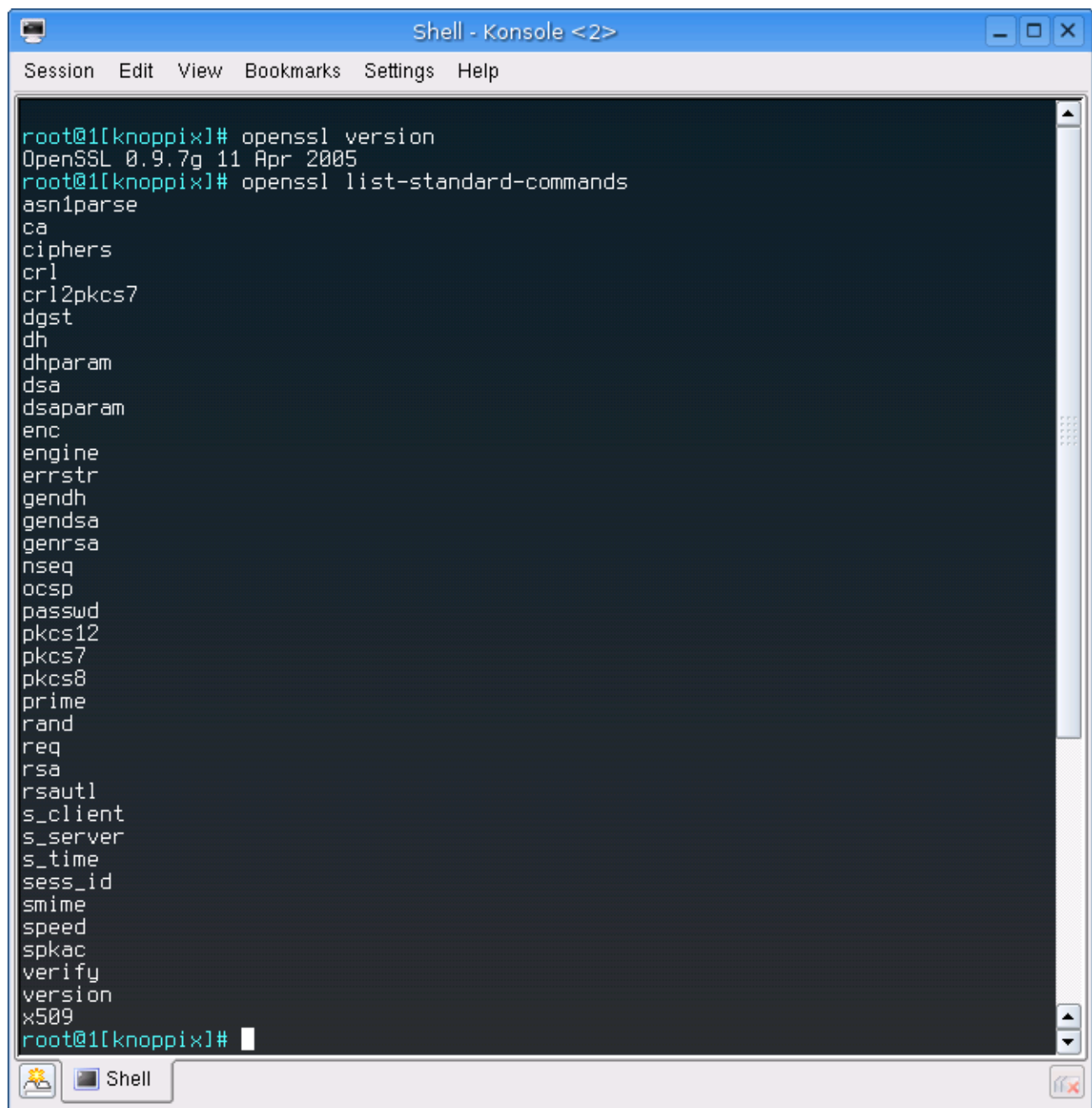
  o Creation of RSA, DH and DSA key parameters
  o Creation of X.509 certificates, CSRs and CRLs
  o Calculation of Message Digests
  o Encryption and Decryption with Ciphers
  o SSL/TLS Client and Server Tests
  o Handling of S/MIME signed or encrypted mail
COMMAND SUMMARY
  The openssl program provides a rich variety of commands (command in the
  SYNOPSIS above), each of which often has a wealth of options and argu-
  ments (command_opts and command_args in the SYNOPSIS).

  The pseudo-commands list-standard-commands, list-message-digest-com-
  mands, and list-cipher-commands output a list (one entry per line) of
  the names of all standard commands, message digest commands, or cipher
Manual page openssl(1ssl) line 1
```

command(s):

openssl version

openssl list-standard-commands



```
Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@1[knoppix]# openssl version
OpenSSL 0.9.7g 11 Apr 2005
root@1[knoppix]# openssl list-standard-commands
asn1parse
ca
ciphers
crl
crl2pkcs7
dgst
dh
dhparam
dsa
dsaparam
enc
engine
errstr
gendh
gensa
genrsa
nseq
ocsp
passwd
pkcs12
pkcs7
pkcs8
prime
rand
req
rsa
rsautl
s_client
s_server
s_time
sess_id
smime
speed
spkac
verify
version
x509
root@1[knoppix]#
```

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

OpenSSL: The Open Source toolkit for SSL/TLS - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.openssl.org/

CD-Inhaltsverzei... KNOPPIX - Webse...

OpenSSL

- Title
- FAQ
- About
- News
- Documents
- Source
- Contribution
- Support
- Related

Welcome to the OpenSSL Project

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and **Open Source** toolkit implementing the **Secure Sockets Layer** (SSL v2/v3) and **Transport Layer Security** (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tom Stubblebine. The OpenSSL toolkit **is licensed** under an Apache-style licence, which basically means that you can use it for commercial and non-commercial purposes subject to some simple license conditions.

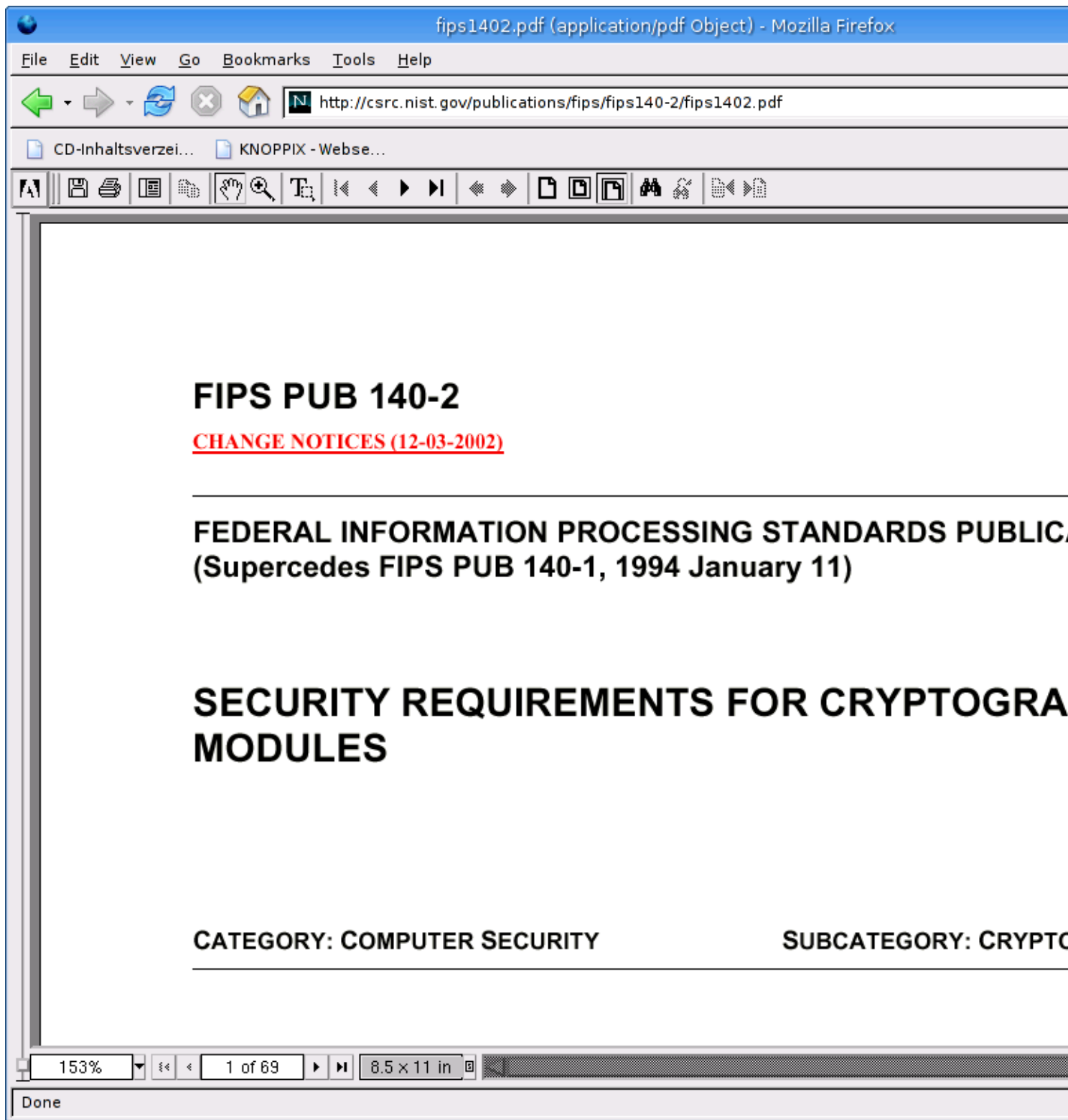
Date	Newsflash
23-Feb-2007:	OpenSSL 0.9.8e is now available , including important bugfixes
23-Feb-2007:	OpenSSL 0.9.7m is now available , including important bugfixes
28-Sep-2006:	Security Advisory: Various security issues
28-Sep-2006:	OpenSSL 0.9.8d is now available , including security fixes
28-Sep-2006:	OpenSSL 0.9.7l is now available , including security fixes

[more...](#)

This software package uses strong cryptography, so even if it is created, maintained and distributed from a source that is legal to do this, it falls under certain export/import and/or use restrictions in some other countries.

Done

Browsing to NIST...

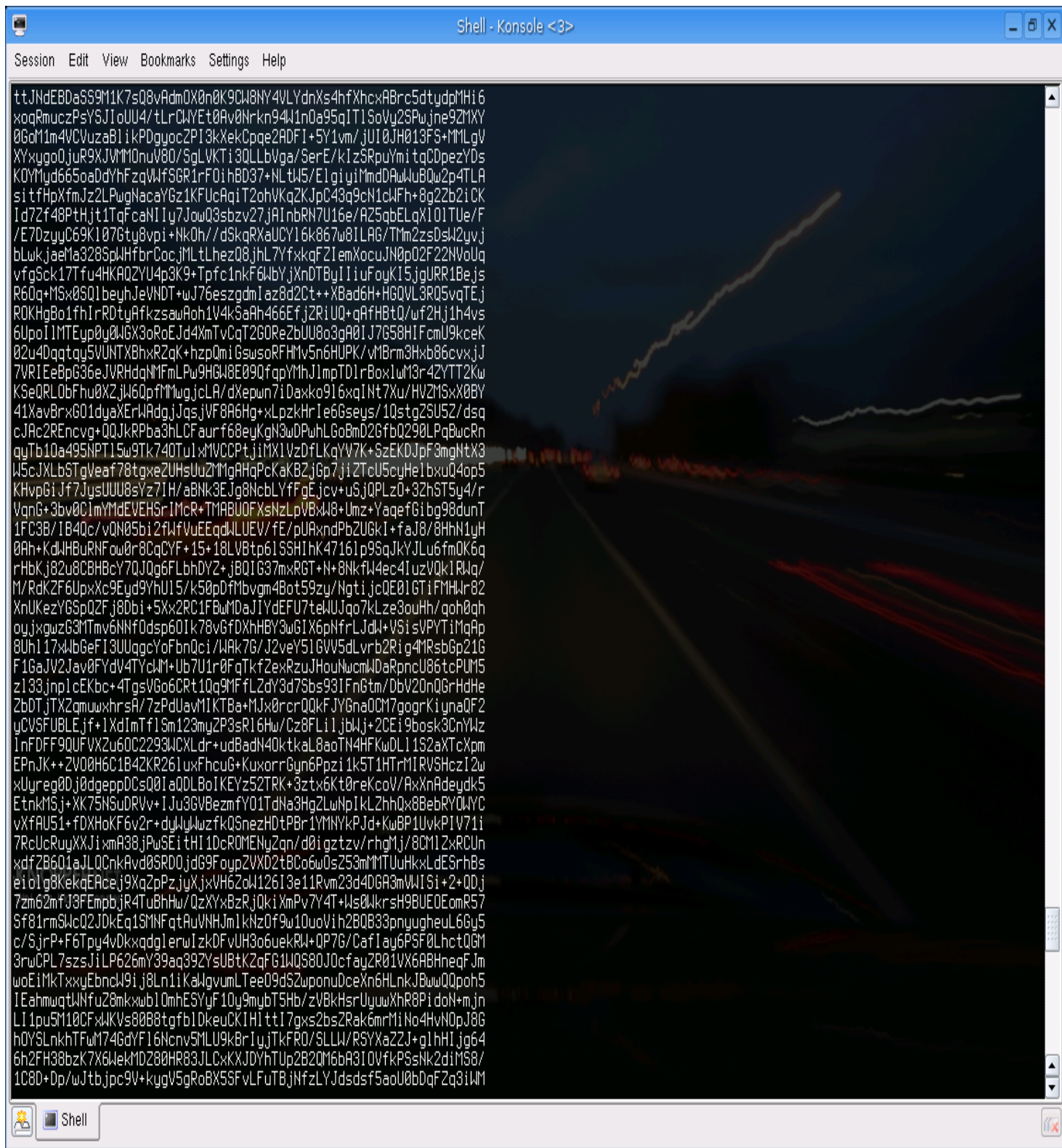


Module One - Symmetric Cryptography

displaying a directory to view the downloaded RFC3766XX.txt file

```
Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
knoppix@2[knoppix]$ ls -al
total 188
drwxr-xr-x  19 knoppix knoppix  640 Mar 29 18:39 .
drwxr-xr-x   3 root   root    60  Mar 29 13:01 ..
lrwxrwxrwx   1 knoppix knoppix   36 Mar 29 18:02 .DCOPserver_Knoppix_:0 -> /home/knoppix/.DCOPserver_Knoppix_0
-rw-r--r--   1 knoppix knoppix   54 Mar 29 18:02 .DCOPserver_Knoppix_0
-rw-----   1 knoppix knoppix  191 Mar 29 18:02 .ICEauthority
-rw-----   1 knoppix knoppix   52 Mar 29 18:02 .Xauthority
-rw-r--r--   1 knoppix knoppix  893 Feb 27 2000 .Xdefaults
-rw-r--r--   1 knoppix knoppix   73 Apr 20 2004 .acrorc
-rw-r--r--   1 knoppix knoppix   57 Aug 28 2005 .bashrc
drwxr-xr-x   4 knoppix knoppix  100 May 31 2005 .gconf
drwxr-xr-x   2 knoppix knoppix   60 May 31 2005 .gconfd
drwxr-xr-x  21 knoppix knoppix  600 Aug 28 2005 .gimp-2.2
drwxr-xr-x   3 knoppix knoppix   60 Mar 29 18:02 .gnome
drwxr-xr-x   2 knoppix knoppix   40 Mar 29 18:02 .gnome_private
drwxr-xr-x   2 knoppix knoppix  120 Aug 28 2005 .gnupg
drwxr-xr-x   4 knoppix knoppix  140 Mar 29 18:02 .kde
-rw-r--r--   1 knoppix knoppix  409 Jun 28 2002 .kderc
drwxr-xr-x   2 knoppix knoppix  100 Aug 28 2005 .links
drwxr-xr-x   3 knoppix knoppix   60 May 3 2004 .local
drwxr-xr-x   2 knoppix knoppix   60 Mar 29 18:02 .mcp
drwxr-xr-x   4 knoppix knoppix  100 Aug 28 2005 .mozilla
-rw-r--r--   1 knoppix knoppix  752 Dec 16 1999 .nessusrc
drwxr-xr-x   5 knoppix knoppix  140 Mar 29 18:02 .netscape
drwxr-xr-x   2 knoppix knoppix  160 Mar 29 18:02 .qt
drwx-----  3 knoppix knoppix   60 Mar 29 18:24 .thumbnails
drwxr-xr-x   2 knoppix knoppix   80 Aug 28 2005 .xine
-rw-----   1 knoppix knoppix 1406 Mar 29 18:36 .xsession-errors
lrwxrwxrwx   1 knoppix knoppix    9 Mar 29 18:30 AdobeFnt.lst -> /dev/null
drwxr-xr-x   2 knoppix knoppix  240 Mar 29 18:31 Desktop
-rw-r--r--   1 knoppix knoppix 55939 Mar 29 18:39 rfc3766PH.txt
-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]$
```

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:

```
Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention
any copyrights, patents or patent applications, or other
proprietary rights that may cover technology that may be required
to implement this standard. Please address the information to the
IETF at ietf-ipr@ietf.org.

Acknowledgement

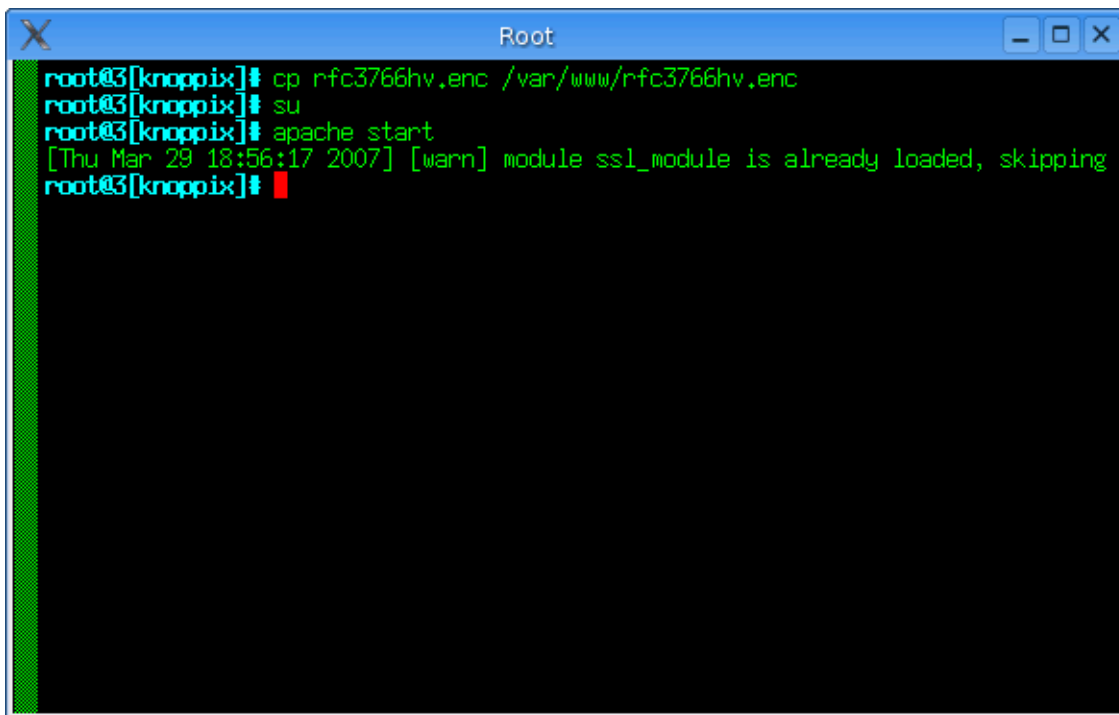
Funding for the RFC Editor function is currently provided by the
Internet Society.

Orman & Hoffman                Best Current Practice                [Page 23]

knoppix@2[knoppix]$ ls -l
total 296
lrwxrwxrwx  1 knoppix knoppix    9 Mar 29 18:30 AdobeFnt.lst -> /dev/null
drwxr-xr-x  2 knoppix knoppix  260 Mar 29 18:41 Desktop
-rw-r--r--  1 knoppix knoppix   56 Mar 29 18:43 des_keyPH
-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 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 rfc3766PH.dec
MD5(rfc3766PH.dec)= 046d557e7127a9fcfaa9d016d130fd80
knoppix@2[knoppix]$
```

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

We used the root user to start the Apache service

A terminal window titled "Root" with a blue header bar. The window contains a series of shell commands and their outputs in green text on a black background. The commands are: 'cp rfc3766hv.enc /var/www/rfc3766hv.enc', 'su', and 'apache start'. The output for 'apache start' is a warning message: '[Thu Mar 29 18:56:17 2007] [warn] module ssl_module is already loaded, skipping'. The prompt 'root@3[knoppix]#' is visible at the end of each line.

```
root@3[knoppix]# cp rfc3766hv.enc /var/www/rfc3766hv.enc
root@3[knoppix]# su
root@3[knoppix]# apache start
[Thu Mar 29 18:56:17 2007] [warn] module ssl_module is already loaded, skipping
root@3[knoppix]#
```

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

```
Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

-rw-r--r-- 1 knoppix knoppix 56 Mar 29 18:43 des_keyPH
-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 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 rfc3766PH.dec
MD5(rfc3766PH.dec)= 046d557e7127a9fcfaa9d016d130fd80
knoppix@2[knoppix]$ cp rfc3766PH.enc /var/www/rfc3766PH.enc
cp: cannot create regular file '/var/www/rfc3766PH.enc': Permission denied
knoppix@2[knoppix]$ nc -vvn -l -p 1170 < des_keyPH
listening on [any] 1170 ...
nc 129.7.236.234 1073 > des_keyconnect to [129.7.236.174] from (UNKNOWN) [129.7.236.234] 40141

[1]+ Stopped nc -vvn -l -p 1170 <des_keyPH
knoppix@2[knoppix]$ nc 129.7.236.234 1073 > des_keyhv

[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]$
```

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

eth0: Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ip.addr == 129.7.236.174

No. ↓	Time	Source	Destination	Protocol	Info
575	104.128014	129.7.236.174	129.7.236.234	ICMP	Echo (ping) request
576	104.128041	129.7.236.234	129.7.236.174	ICMP	Echo (ping) reply
579	105.130533	129.7.236.174	129.7.236.234	ICMP	Echo (ping) request
580	105.130557	129.7.236.234	129.7.236.174	ICMP	Echo (ping) reply
583	106.132302	129.7.236.174	129.7.236.234	ICMP	Echo (ping) request
584	106.132326	129.7.236.234	129.7.236.174	ICMP	Echo (ping) reply
588	107.134070	129.7.236.174	129.7.236.234	ICMP	Echo (ping) request
589	107.134095	129.7.236.234	129.7.236.174	ICMP	Echo (ping) reply
592	108.135838	129.7.236.174	129.7.236.234	ICMP	Echo (ping) request
593	108.135864	129.7.236.234	129.7.236.174	ICMP	Echo (ping) reply

▶ Frame 575 (98 bytes on wire, 98 bytes captured)
 ▶ Ethernet II, Src: DellPcba_be:ce:22 (00:0d:56:be:ce:22), Dst: 129.7.236.234 (00:0d:56:be:d0:11)
 ▶ Internet Protocol, Src: 129.7.236.174 (129.7.236.174), Dst: 129.7.236.234 (129.7.236.234)
 ▶ Internet Control Message Protocol

```

0000  00 0d 56 be d0 11 00 0d 56 be ce 22 08 00 45 00  ..V....V..."..E.
0010  00 54 00 00 40 00 40 01 5f 01 81 07 ec ae 81 07  .T...@.@_.....
0020  ec ea 08 00 c4 44 b3 1f 00 00 46 0c 55 e9 00 0e  ....D...F.U...
0030  f9 94 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  ..
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..!#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  ..()*)+,-./:;<=>?@A
  
```

eth0: <live capture in progress> File: /tmp/etherXXXXPSGZcZ 117 KB P: 840 D: 10 M: 0

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 rfc3766hv.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]$
```