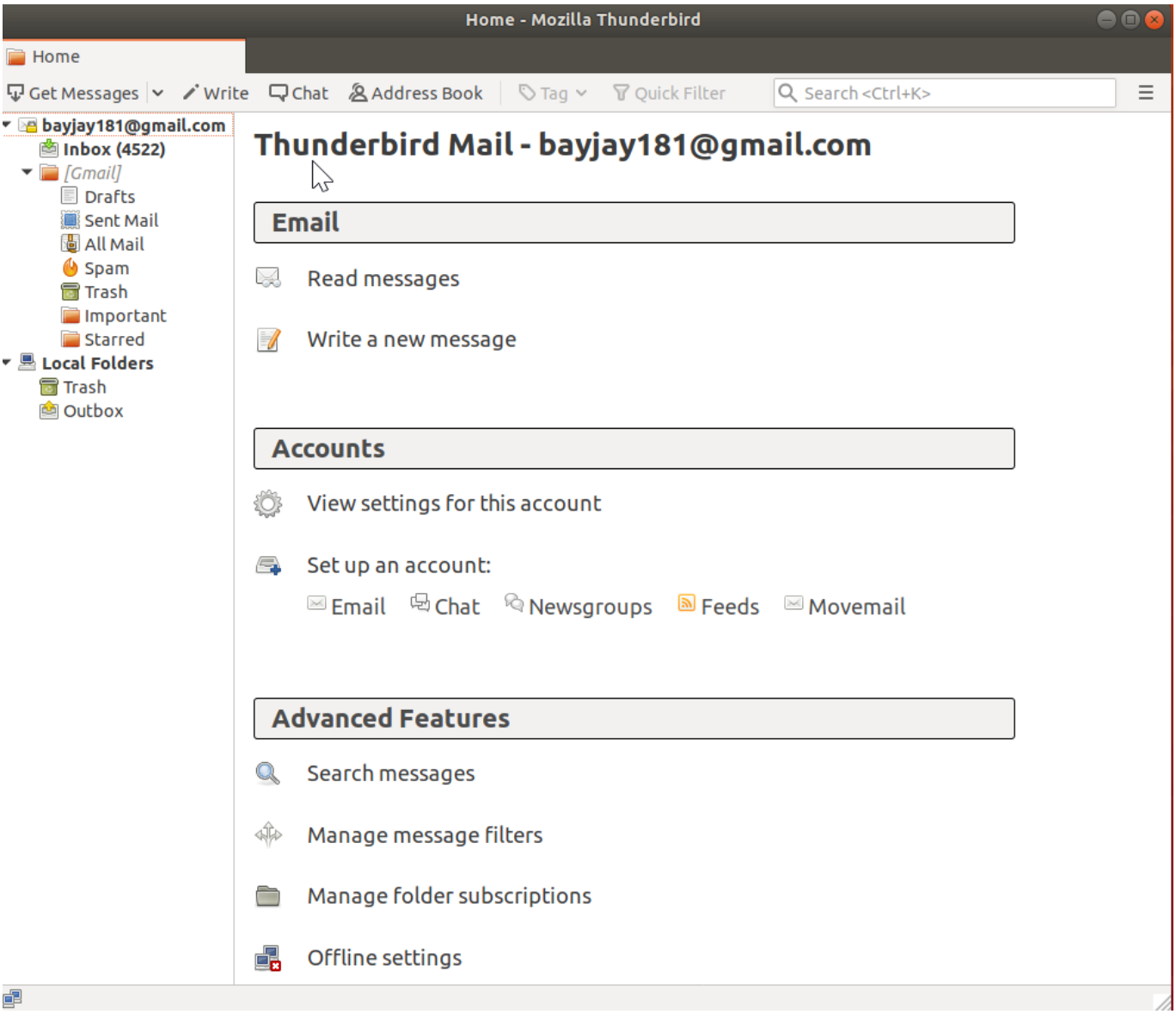
By: Jarron Bailey

Software Code & Threat Analysis Presentation

Table of Contents

- Software Code & Threat Analysis Presentation
  - Table of Contents
    - 1. Install and configure GNU privacy guard (GNUPG)
    - 2. Generate a SHA1 hash from the command-line in Linux`
    - 3. Install and configure TrueCrypt
    - 4. Send encrypted email (includes exchanging digital certificates and decrypting email)
      - Encrypt
      - Decrypt
    - 5. Install and configure TOR (includes performing a search)
    - 6. Perform a basic stenography encryption
      - Encrypt
      - Decrypt

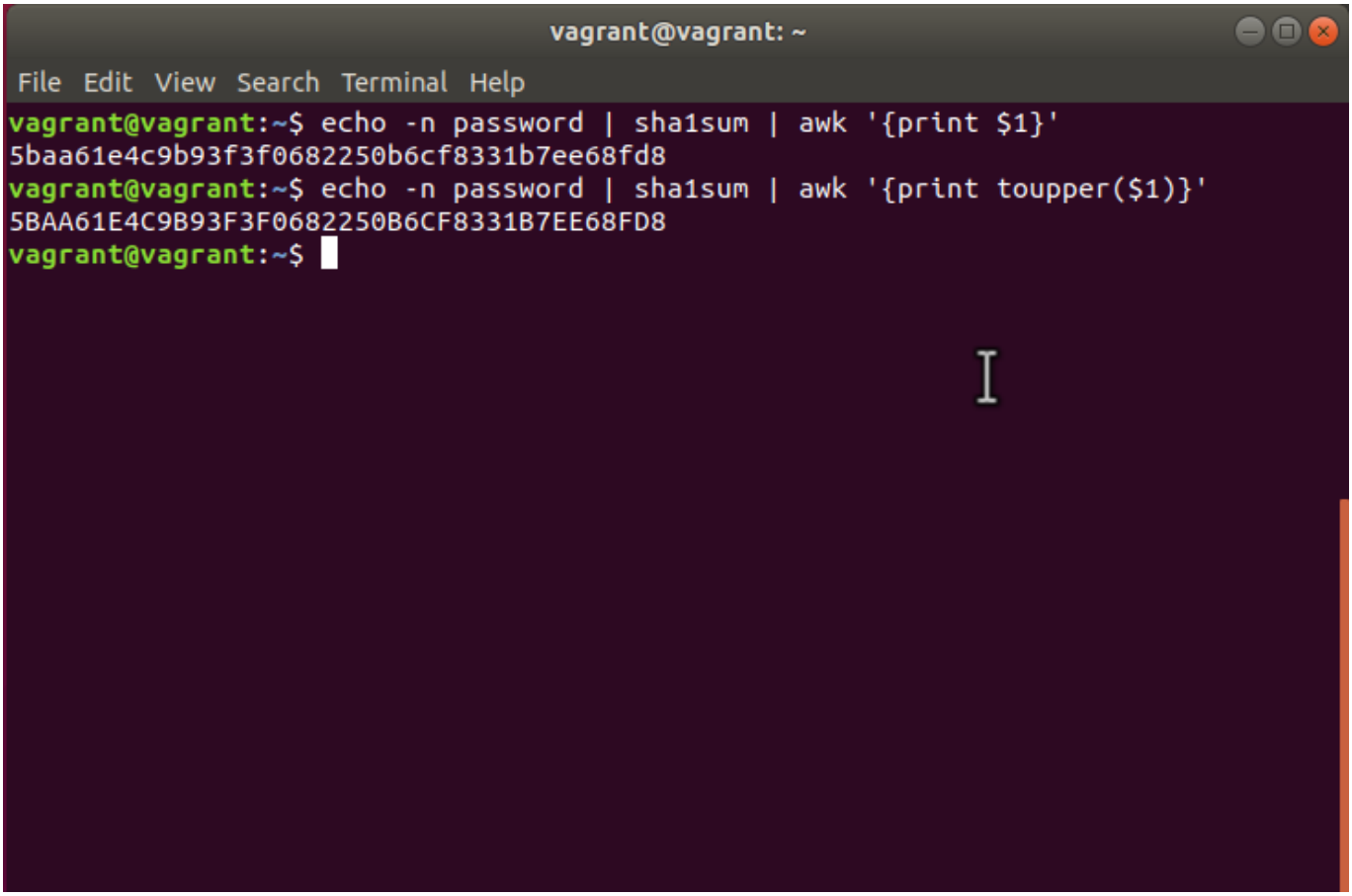
1. Install and configure GNU privacy guard (GNUPG)



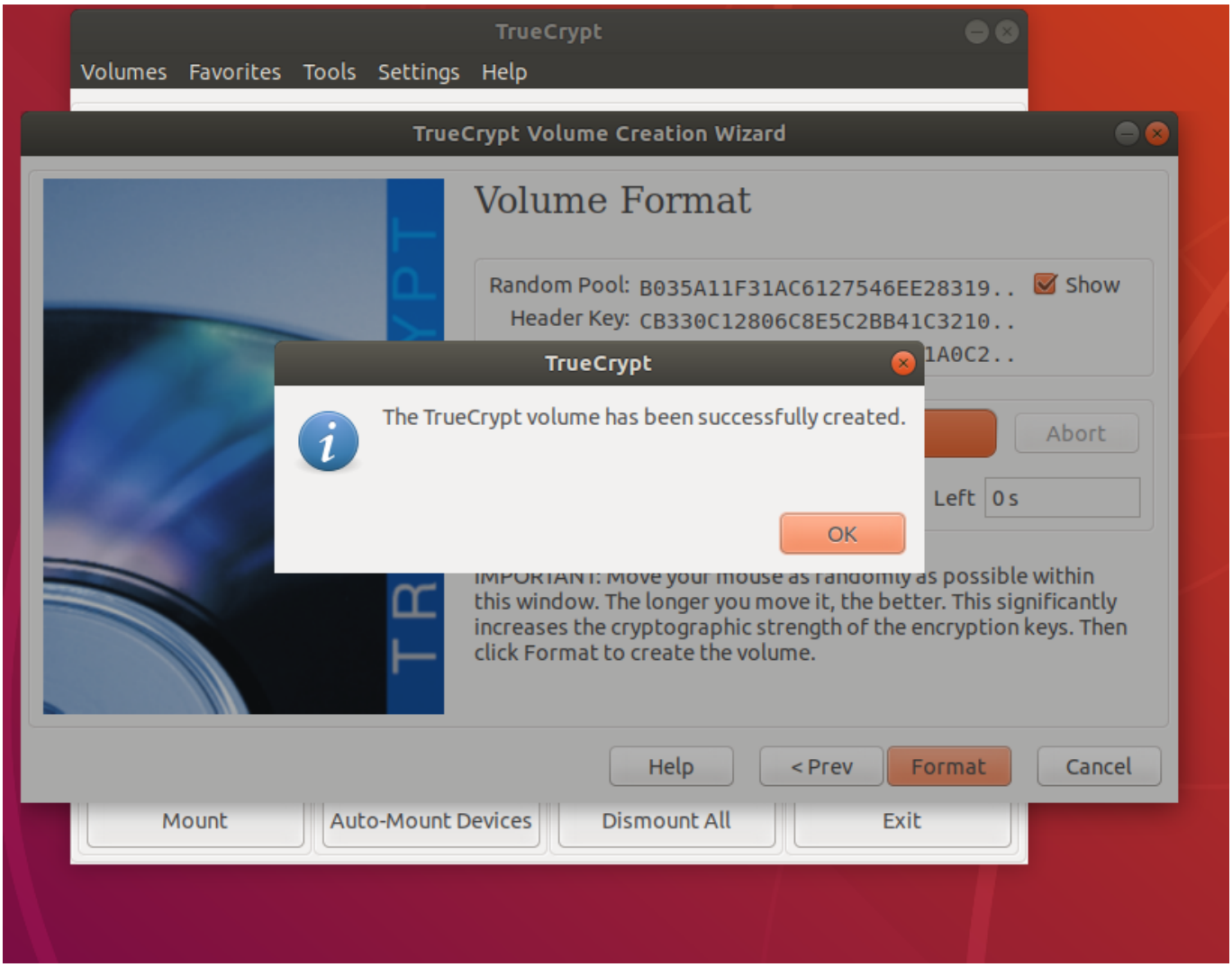
2. Generate a SHA1 hash from the command-line in Linux`

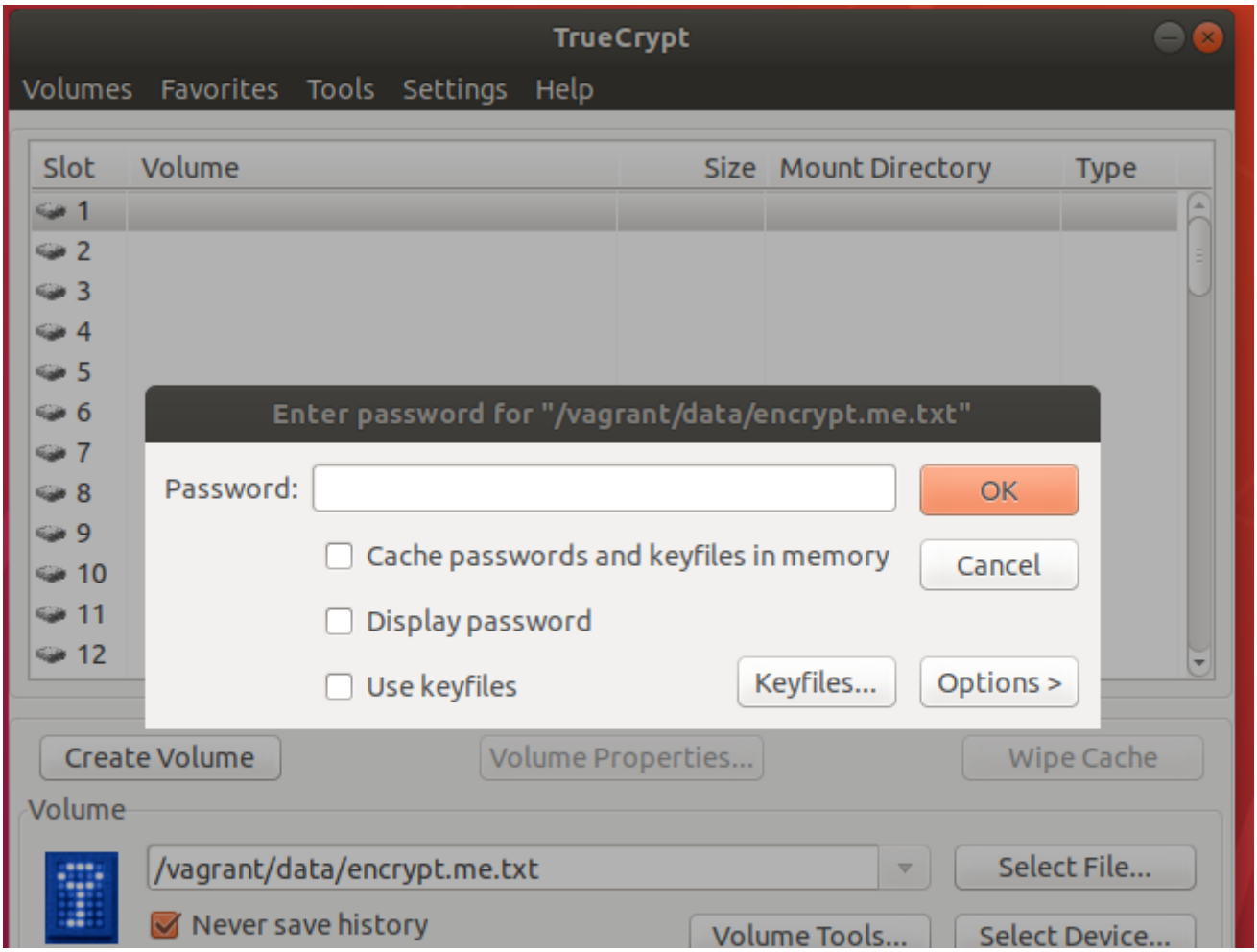
vagrant@vagrant:~$ echo -n password | sha1sum | awk '{print $1}'
5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 **vagrant@vagrant**:~$ echo -n password | sha1sum | awk

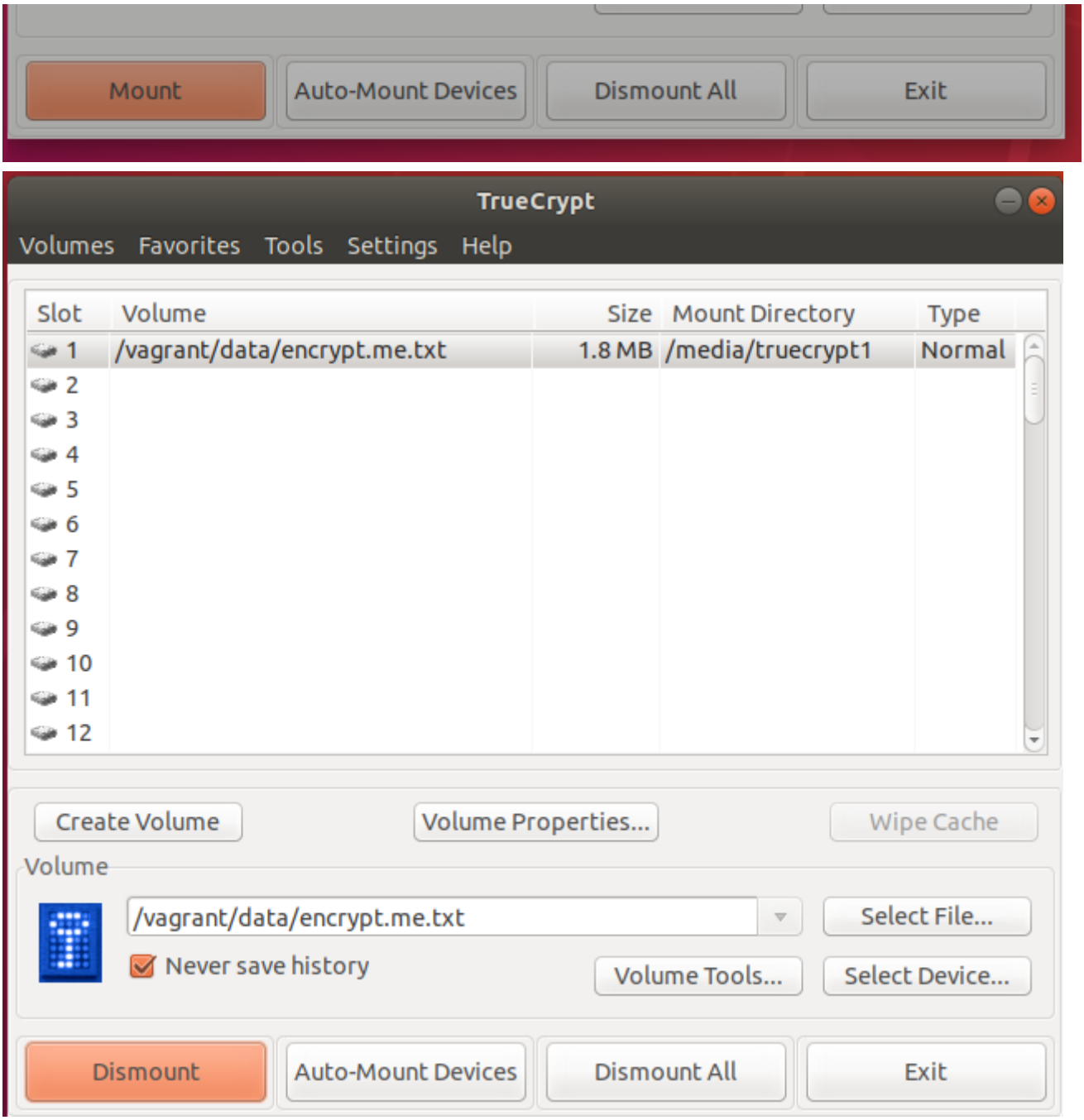
'{print toupper($1)}' 5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8



3. Install and configure TrueCrypt

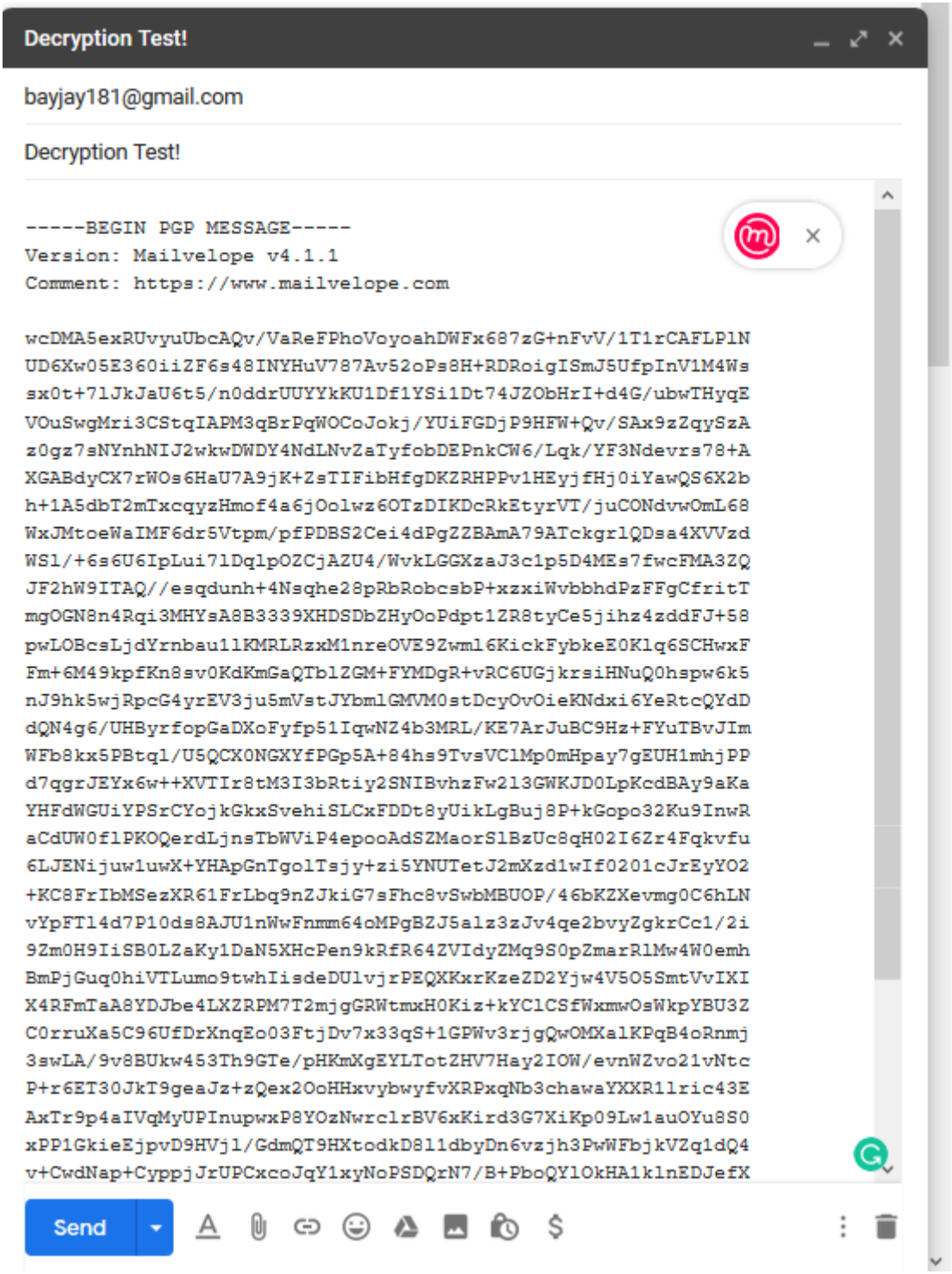

TrueCrypt
Volumes Favorites Tools Settings Help
TrueCrypt Volume Creation Wizard
Volume Format
Random Pool: B035A11F31AC6127546EE28319..
Header Key: CB330C12806C8E5C2BB41C3210..
1A0C2..
Show
Abort
Left 0 s
TrueCrypt
The TrueCrypt volume has been successfully created.
OK
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Prev
Format
Cancel
Mount
Auto-Mount Devices
Dismount All
Exit


TrueCrypt
Volumes Favorites Tools Settings Help
Slot Volume Size Mount Directory Type
1
2
3
4
5
6
7
8
9
10
11
12
Enter password for "/vagrant/data/encrypt.me.txt"
Password:
OK
Cache passwords and keyfiles in memory
Cancel
Display password
Use keyfiles
Keyfiles...
Options >
Create Volume
Volume Properties...
Wipe Cache
Volume
/vagrant/data/encrypt.me.txt
Select File...
Never save history
Volume Tools...
Select Device...

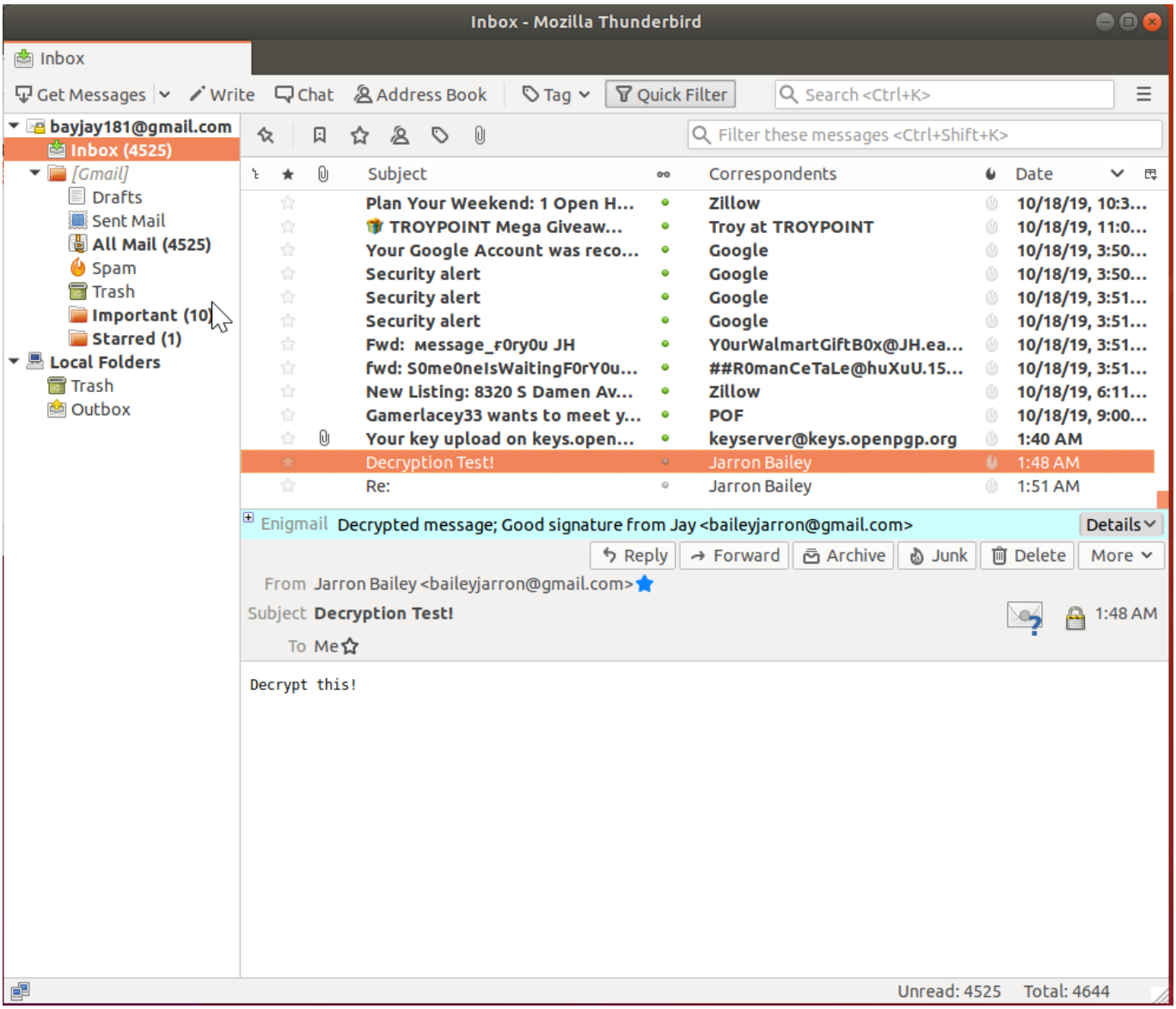


4. Send encrypted email (includes exchanging digital certificates and decrypting email)

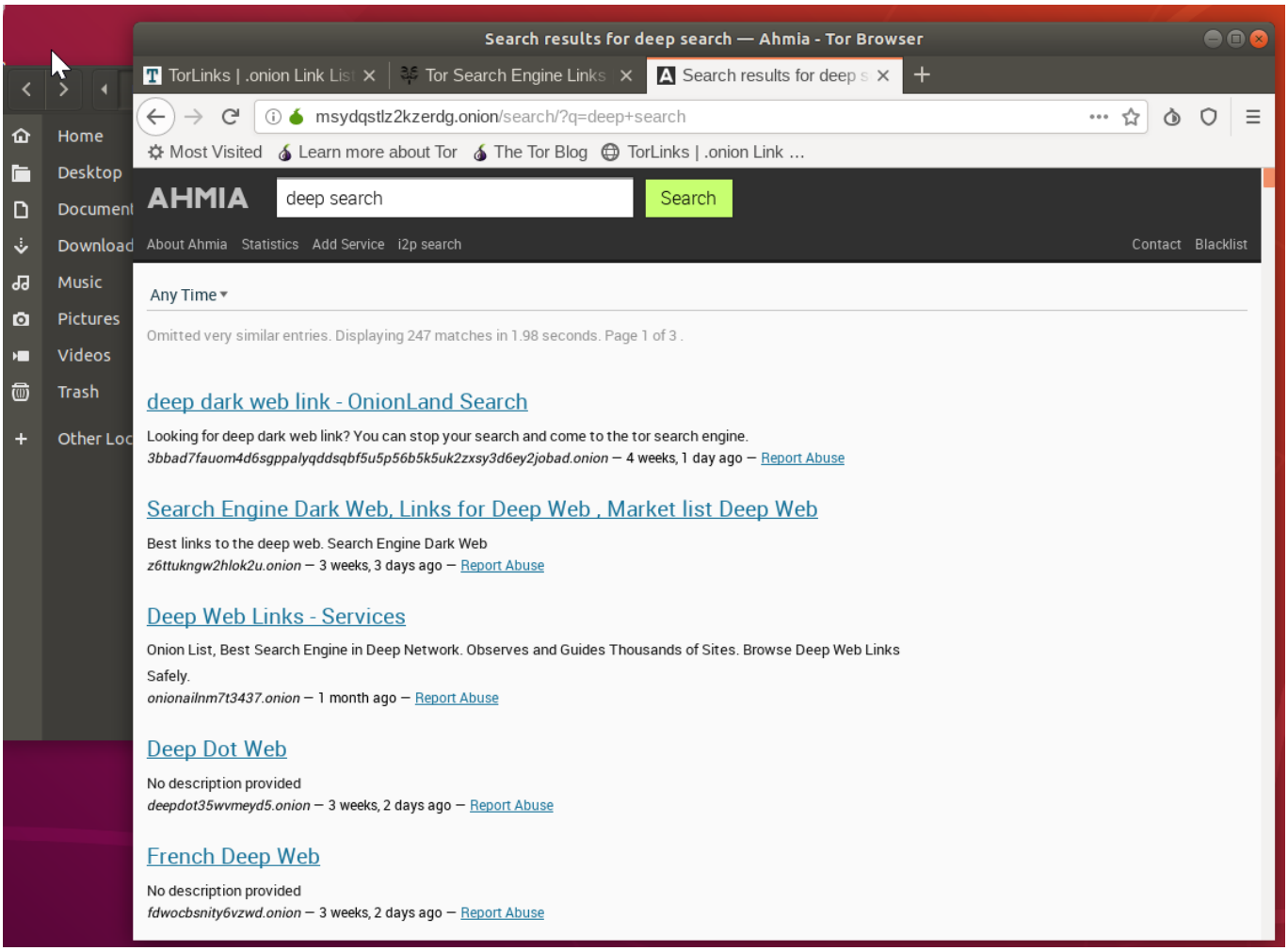
Encrypt


Decryption Test!
bayjay181@gmail.com
Decryption Test!
-----BEGIN PGP MESSAGE-----
Version: Mailvelope v4.1.1
Comment: https://www.mailvelope.com
wcDMA5exRUvyuUbcAQv/VaReFPhoVoyoahDWFx687zG+nFvV/1T1rCAFLPlN
UD6Xw05E360iiZF6s48INYHuV787Av52oPs8H+RDRoigISmJ5UfpInV1M4Ws
sx0t+7lJkJaU6t5/n0ddrUUYYkKU1Df1YSi1Dt74JZObHrI+d4G/ubwTHyqE
VOuSwgMri3CStqIAPM3qBrPqWOCoJokj/YUiFGDjP9HFW+Qv/SAx9zZqySzA
z0gz7sNYnhNIJ2wkwDWDY4NdLNvZaTyfobDEPnkCW6/Lqk/YF3Ndevrs78+A
XGABdyCX7rWOs6HaU7A9jK+ZsTIFibHfgDKZRHPPv1HEyjfHj0iYawQS6X2b
h+1A5dbT2mTxcqyzHmof4a6jOolwz6OTzDIKDcRkEtyrVT/juCONdvwOmL68
WxJMtoeWaIMF6dr5Vtpm/pfPDBS2Cei4dPgZZBAmA79ATckgrlQDsa4XVVzd
WSl/+6s6U6IpLui7lDqlpOZCjAZU4/WvkLGGXzaJ3c1p5D4MEs7fwcFMA3ZQ
JF2hW9ITAQ//esqdunh+4Nsqhe28pRbRobcsbP+xzxiWvbbhdPzFFgCfritT
mgOGN8n4Rqi3MHYsA8B3339XHDSDbZHyOoPdpt1ZR8tyCe5jihz4zddFJ+58
pwLOBcsLjdYrnbau1lKMRLRzxM1nreOVE9Zwml6KickFybkeE0Klq6SCHwxF
Fm+6M49kpfKn8sv0KdKmGaQTblZGM+FYMDgR+vRC6UGjkrsiHNuQ0hspw6k5
nJ9hk5wjRpcG4yrEV3ju5mVstJYbmlGMVM0stDcyOvOieKNdxi6YeRtcQYdD
dQN4g6/UHByrfopGaDXoFyfp51IqwNZ4b3MRL/KE7ArJuBC9Hz+FYuTBvJIm
WFb8kx5PBtql/U5QCX0NGXYfPGp5A+84hs9TvsVClMp0mHpay7gEUH1mhjPP
d7qgrJEYx6w++XVTIr8tM3I3bRtiy2SNIBvhzFw2l3GWKJD0LpKcdBAy9aKa
YHFdWGUiYPSrCYojkGkxSvehiSLCxFDDt8yUikLgBuj8P+kGopo32Ku9InwR
aCdUW0flPKOQerdLjnsTbWViP4epooAdSZMaorSlBzUc8qH02I6Zr4Fqkvfu
6LJENijuw1uwX+YHApGnTgolTsjy+zi5YNUTetJ2mXzd1wIf0201cJrEyYO2
+KC8FrIbMSezXR61FrLbq9nZJkiG7sFhc8vSwbMBUOP/46bKZXevmg0C6hLN
vYpFTl4d7P10ds8AJU1nWwFnmm64oMPgBZJ5alz3zJv4qe2bvyZgkrCc1/2i
9Zm0H9IiSB0LZaKy1DaN5XHcPen9kRfR64ZVIdyZMq9S0pZmarRlMw4W0emh
BmPjGuq0hiVTLumo9twhIisdeDUlvjrPEQXKxrKzeZD2Yjw4V5O5SmtVvIXI
X4RFmTaA8YDJbe4LXZRPM7T2mjgGRWtmxH0Kiz+kYClCSfWxmwOsWkpYBU3Z
C0rruXa5C96UfDrXnqEo03FtjDv7x33qS+1GPWv3rjgQwOMXalKPqB4oRnmj
3swLA/9v8BUkw453Th9GTe/pHKmXgEYLTotZHV7Hay2IOW/evnWZvo21vNtc
P+r6ET30JkT9geaJz+zQex2OoHHxvybwyfvXRPxqNb3chawaYXXR1lric43E
AxTr9p4aIVqMyUPInupwxP8YOzNwrclrBV6xKird3G7XiKp09Lw1auOYu8S0
xPP1GkieEjpvD9HVjl/GdmQT9HXtodkD8l1dbyDn6vzjh3PwWFbjkVZq1dQ4
v+CwdNap+CyppjJrUPCxcoJqY1xyNoPSDQrN7/B+PboQYlOkHA1klnEDJefX
Send

Decrypt

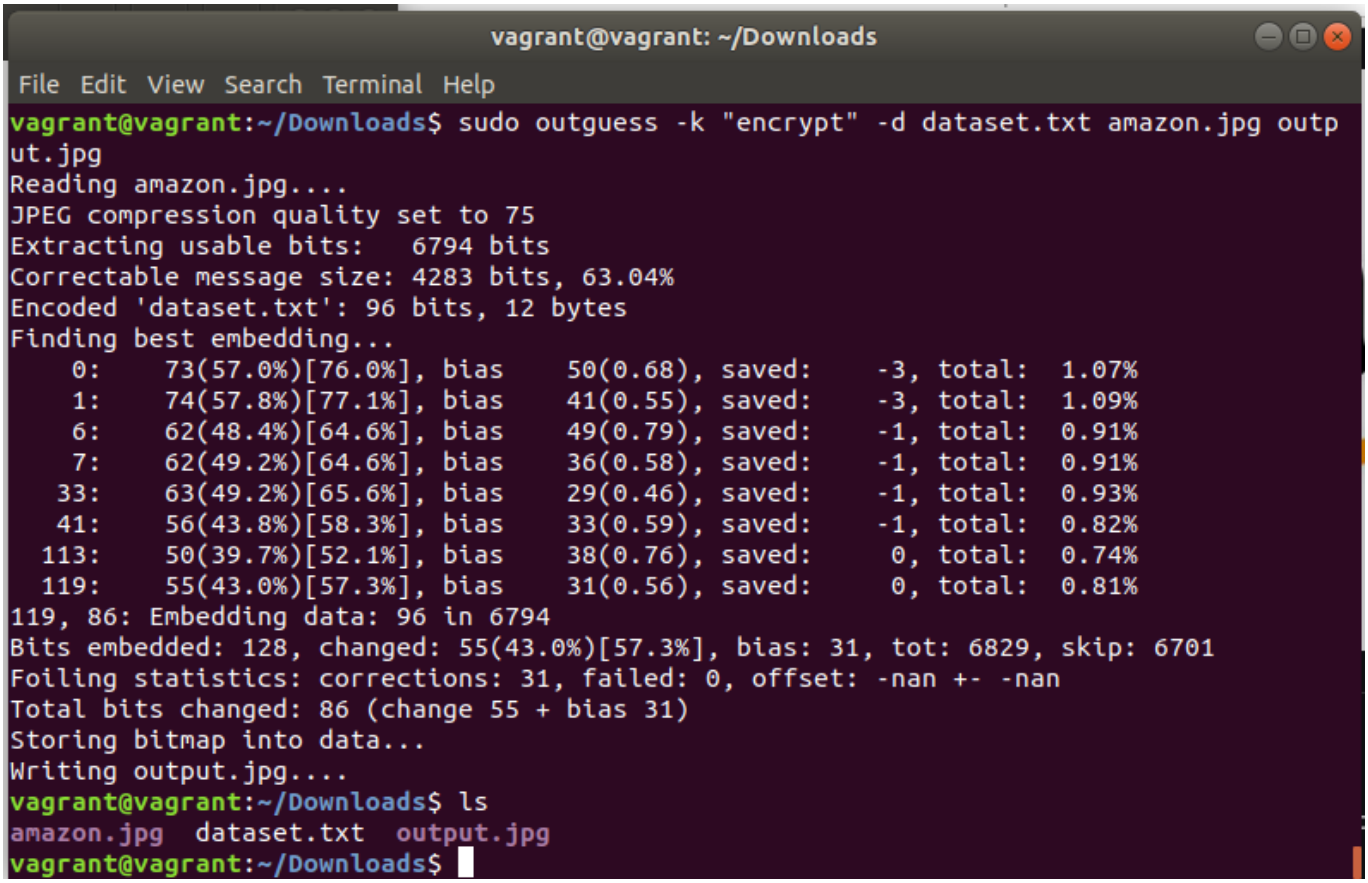


5. Install and configure TOR (includes performing a search)

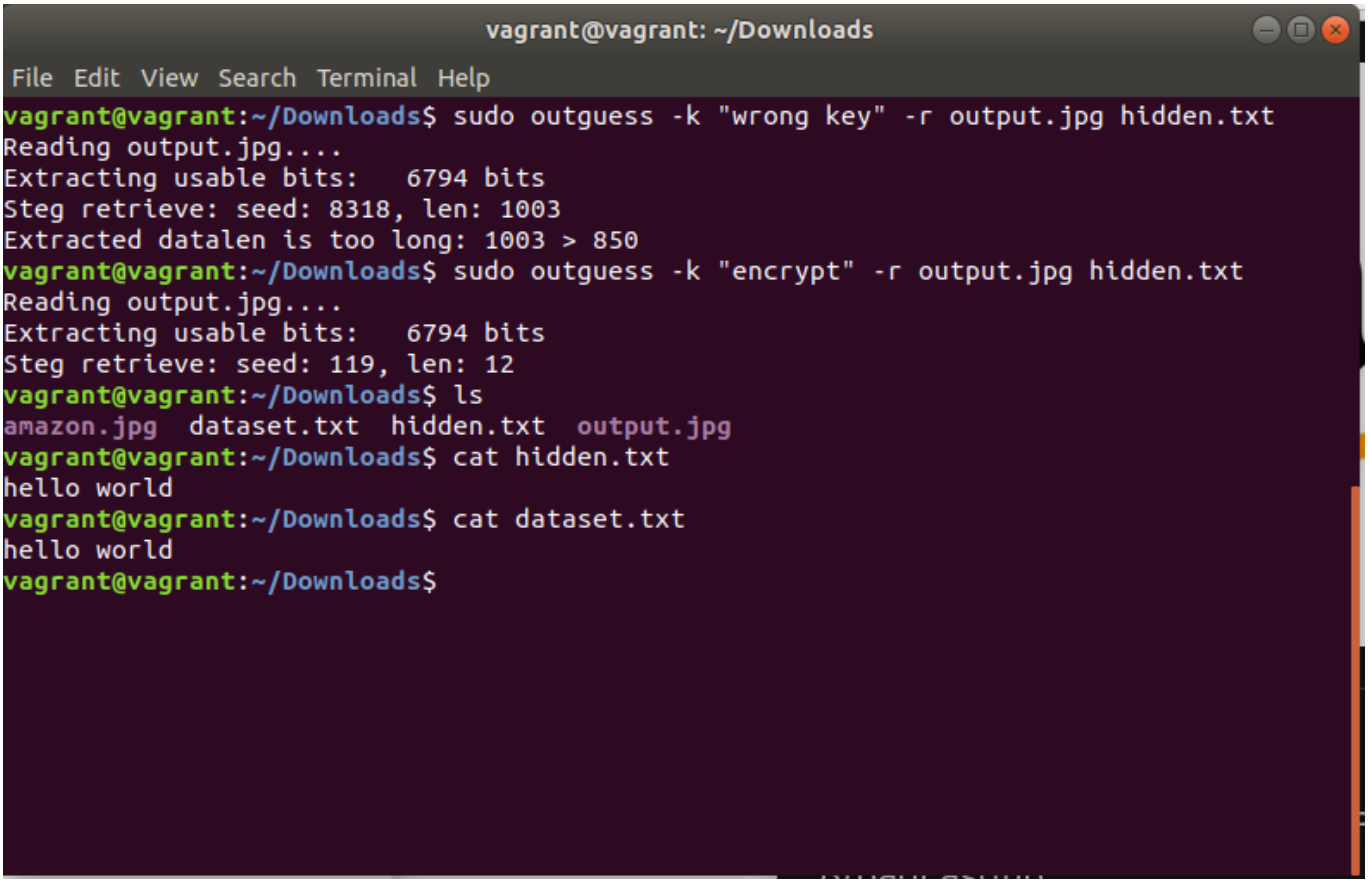


6. Perform a basic stenography encryption

Encrypt


vagrant@vagrant: ~/Downloads
File Edit View Search Terminal Help
vagrant@vagrant:~/Downloads$ sudo outguess -k "encrypt" -d dataset.txt amazon.jpg outp
ut.jpg
Reading amazon.jpg....
JPEG compression quality set to 75
Extracting usable bits: 6794 bits
Correctable message size: 4283 bits, 63.04%
Encoded 'dataset.txt': 96 bits, 12 bytes
Finding best embedding...
0: 73(57.0%)[76.0%], bias 50(0.68), saved: -3, total: 1.07%
1: 74(57.8%)[77.1%], bias 41(0.55), saved: -3, total: 1.09%
6: 62(48.4%)[64.6%], bias 49(0.79), saved: -1, total: 0.91%
7: 62(49.2%)[64.6%], bias 36(0.58), saved: -1, total: 0.91%
33: 63(49.2%)[65.6%], bias 29(0.46), saved: -1, total: 0.93%
41: 56(43.8%)[58.3%], bias 33(0.59), saved: -1, total: 0.82%
113: 50(39.7%)[52.1%], bias 38(0.76), saved: 0, total: 0.74%
119: 55(43.0%)[57.3%], bias 31(0.56), saved: 0, total: 0.81%
119, 86: Embedding data: 96 in 6794
Bits embedded: 128, changed: 55(43.0%)[57.3%], bias: 31, tot: 6829, skip: 6701
Foiling statistics: corrections: 31, failed: 0, offset: -nan +- -nan
Total bits changed: 86 (change 55 + bias 31)
Storing bitmap into data...
Writing output.jpg....
vagrant@vagrant:~/Downloads$ ls
amazon.jpg dataset.txt output.jpg
vagrant@vagrant:~/Downloads$

Decrypt


vagrant@vagrant: ~/Downloads
File Edit View Search Terminal Help
vagrant@vagrant:~/Downloads$ sudo outguess -k "wrong key" -r output.jpg hidden.txt
Reading output.jpg....
Extracting usable bits: 6794 bits
Steg retrieve: seed: 8318, len: 1003
Extracted datalen is too long: 1003 > 850
vagrant@vagrant:~/Downloads$ sudo outguess -k "encrypt" -r output.jpg hidden.txt
Reading output.jpg....
Extracting usable bits: 6794 bits
Steg retrieve: seed: 119, len: 12
vagrant@vagrant:~/Downloads$ ls
amazon.jpg dataset.txt hidden.txt output.jpg
vagrant@vagrant:~/Downloads$ cat hidden.txt
hello world
vagrant@vagrant:~/Downloads$ cat dataset.txt
hello world
vagrant@vagrant:~/Downloads$