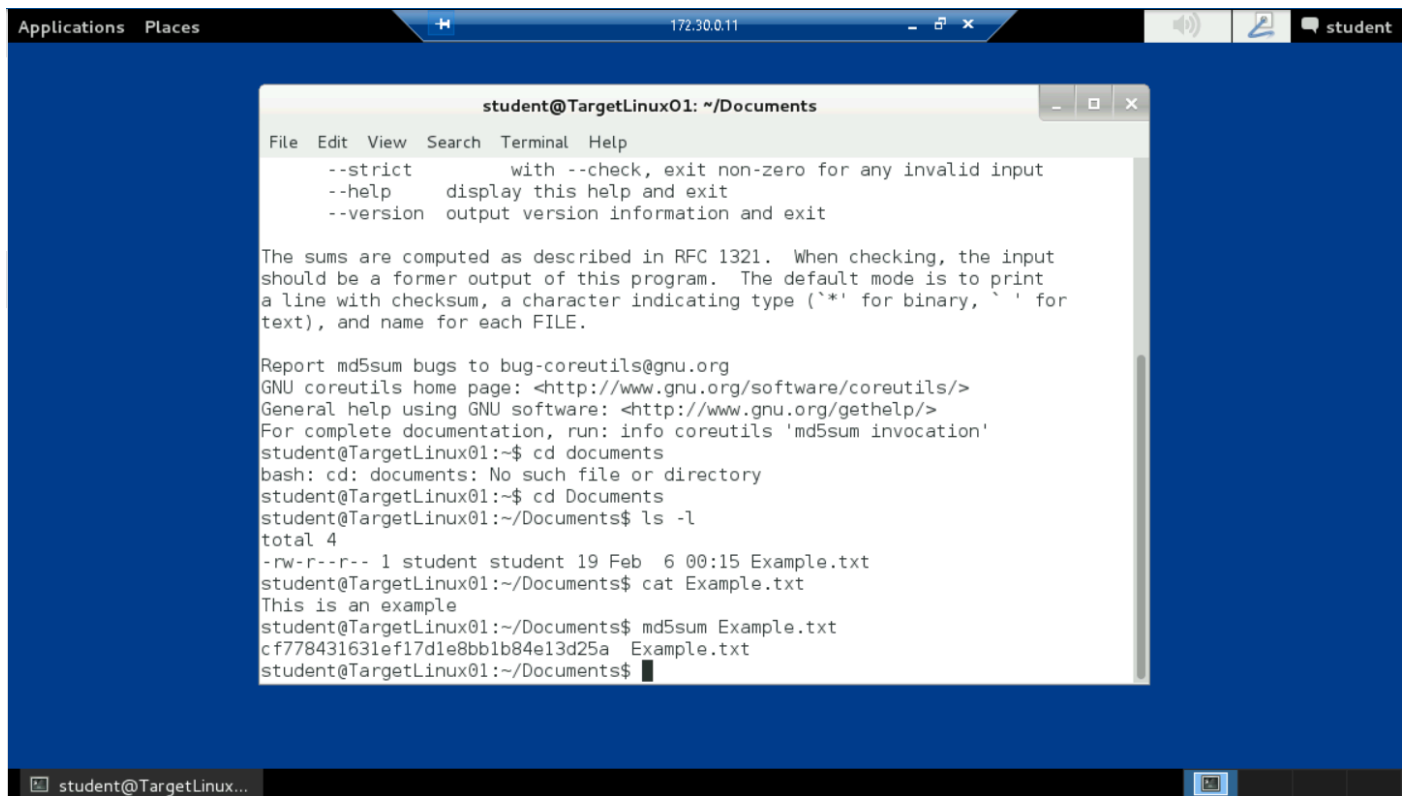


## Section 1.2

### Step 7



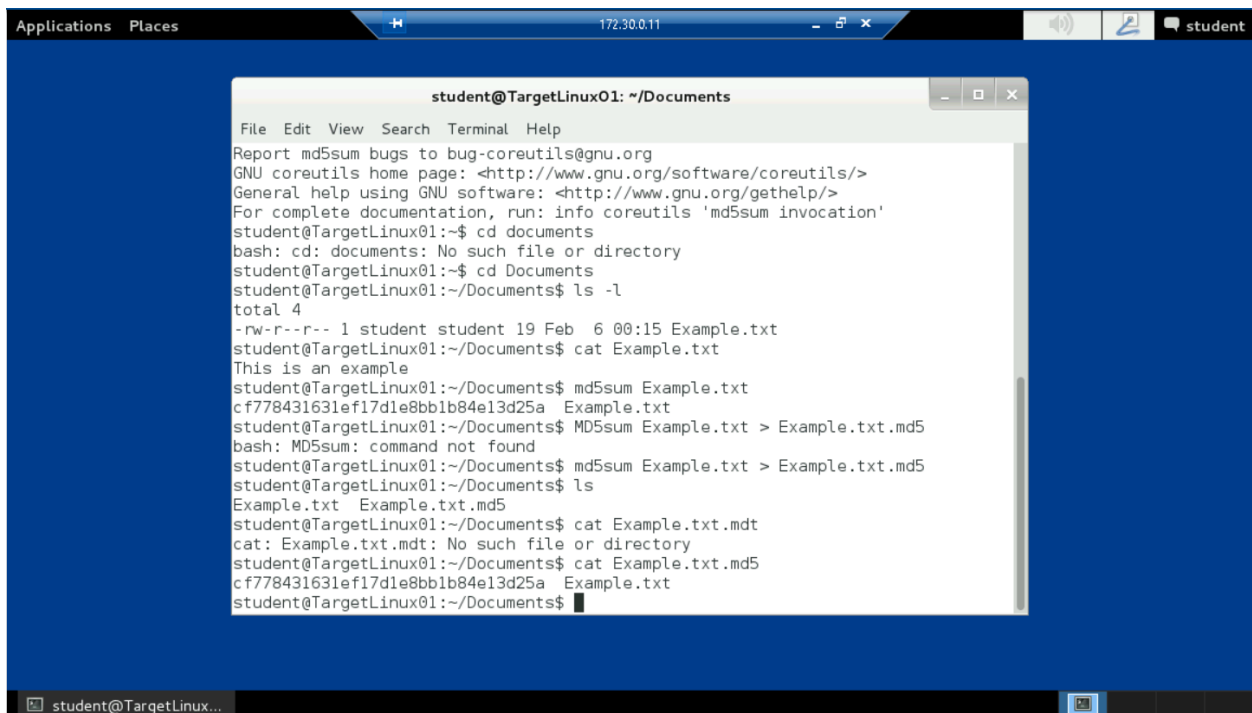
A terminal window titled "student@TargetLinux01: ~/Documents" is shown. The window contains the following text:

```
File Edit View Search Terminal Help
--strict      with --check, exit non-zero for any invalid input
--help        display this help and exit
--version     output version information and exit

The sums are computed as described in RFC 1321. When checking, the input
should be a former output of this program. The default mode is to print
a line with checksum, a character indicating type ('*' for binary, ' ' for
text), and name for each FILE.

Report md5sum bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
For complete documentation, run: info coreutils 'md5sum invocation'
student@TargetLinux01:~$ cd documents
bash: cd: documents: No such file or directory
student@TargetLinux01:~$ cd Documents
student@TargetLinux01:~/Documents$ ls -l
total 4
-rw-r--r-- 1 student student 19 Feb  6 00:15 Example.txt
student@TargetLinux01:~/Documents$ cat Example.txt
This is an example
student@TargetLinux01:~/Documents$ md5sum Example.txt
cf778431631ef17d1e8bb1b84e13d25a  Example.txt
student@TargetLinux01:~/Documents$
```

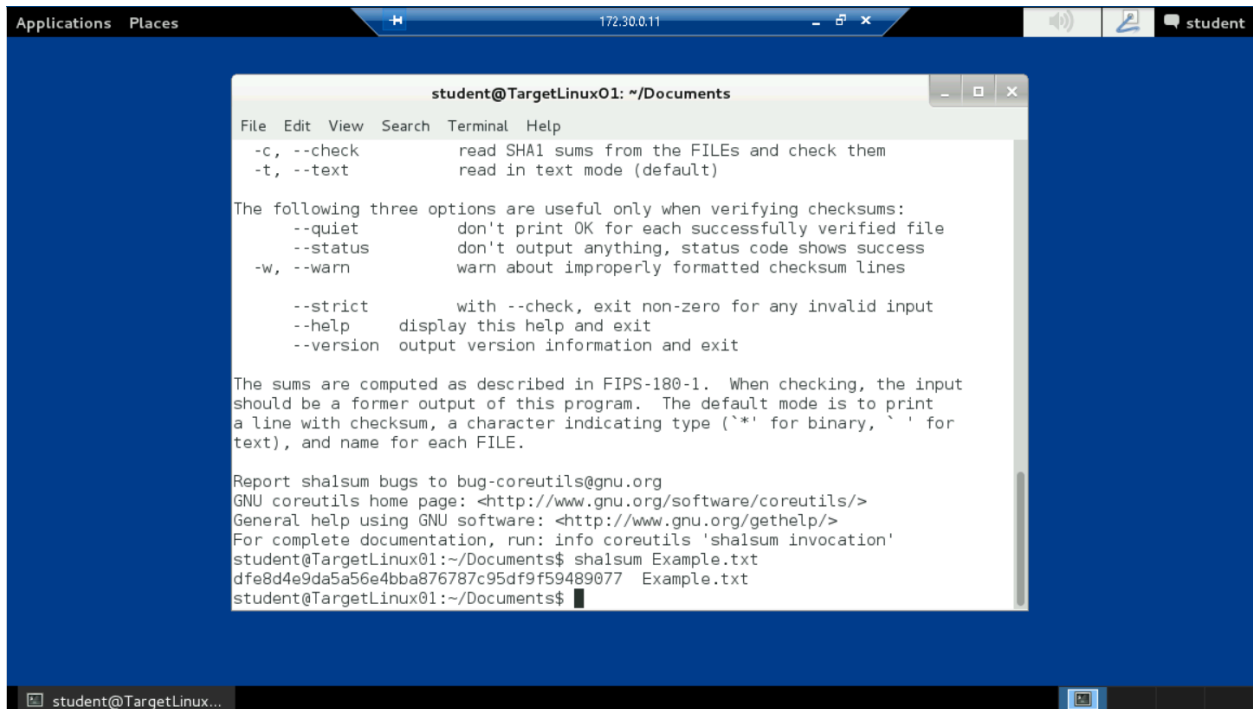
### Step 11



A terminal window titled "student@TargetLinux01: ~/Documents" is shown. The window contains the following text:

```
File Edit View Search Terminal Help
Report md5sum bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
For complete documentation, run: info coreutils 'md5sum invocation'
student@TargetLinux01:~$ cd documents
bash: cd: documents: No such file or directory
student@TargetLinux01:~$ cd Documents
student@TargetLinux01:~/Documents$ ls -l
total 4
-rw-r--r-- 1 student student 19 Feb  6 00:15 Example.txt
student@TargetLinux01:~/Documents$ cat Example.txt
This is an example
student@TargetLinux01:~/Documents$ md5sum Example.txt
cf778431631ef17d1e8bb1b84e13d25a  Example.txt
student@TargetLinux01:~/Documents$ MD5sum Example.txt > Example.txt.md5
bash: MD5sum: command not found
student@TargetLinux01:~/Documents$ md5sum Example.txt > Example.txt.md5
student@TargetLinux01:~/Documents$ ls
Example.txt  Example.txt.md5
student@TargetLinux01:~/Documents$ cat Example.txt.mdt
cat: Example.txt.mdt: No such file or directory
student@TargetLinux01:~/Documents$ cat Example.txt.md5
cf778431631ef17d1e8bb1b84e13d25a  Example.txt
student@TargetLinux01:~/Documents$
```

## Step 15



The screenshot shows a terminal window titled "student@TargetLinux01: ~/Documents". The window displays the help text for the 'shalsum' command. The text includes options for checking SHA1 sums, text mode, quiet status, warning, strict input, help, and version information. It also mentions the FIPS-180-1 standard and provides links to GNU coreutils documentation.

```
student@TargetLinux01: ~/Documents
File Edit View Search Terminal Help
-c, --check      read SHA1 sums from the FILES and check them
-t, --text      read in text mode (default)

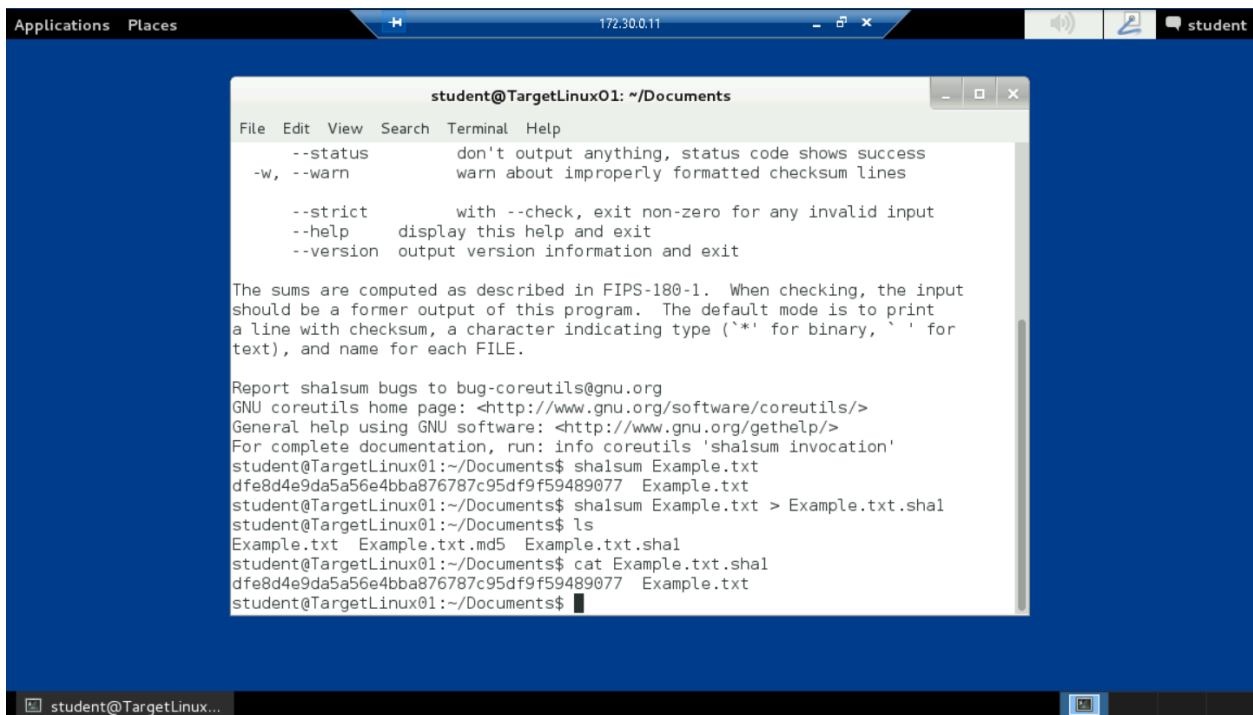
The following three options are useful only when verifying checksums:
--quiet         don't print OK for each successfully verified file
--status        don't output anything, status code shows success
-w, --warn      warn about improperly formatted checksum lines

--strict        with --check, exit non-zero for any invalid input
--help          display this help and exit
--version       output version information and exit

The sums are computed as described in FIPS-180-1. When checking, the input
should be a former output of this program. The default mode is to print
a line with checksum, a character indicating type ('*' for binary, ' ' for
text), and name for each FILE.

Report shalsum bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
For complete documentation, run: info coreutils 'shalsum invocation'
student@TargetLinux01:~/Documents$ shalsum Example.txt
dfe8d4e9da5a56e4bba876787c95df9f59489077 Example.txt
student@TargetLinux01:~/Documents$
```

## Step 19



The screenshot shows a terminal window titled "student@TargetLinux01: ~/Documents". The window displays the help text for the 'shalsum' command, followed by the execution of the 'shalsum' command on 'Example.txt' and the 'cat' command on the resulting 'Example.txt.shal' file.

```
student@TargetLinux01: ~/Documents
File Edit View Search Terminal Help
--status        don't output anything, status code shows success
-w, --warn      warn about improperly formatted checksum lines

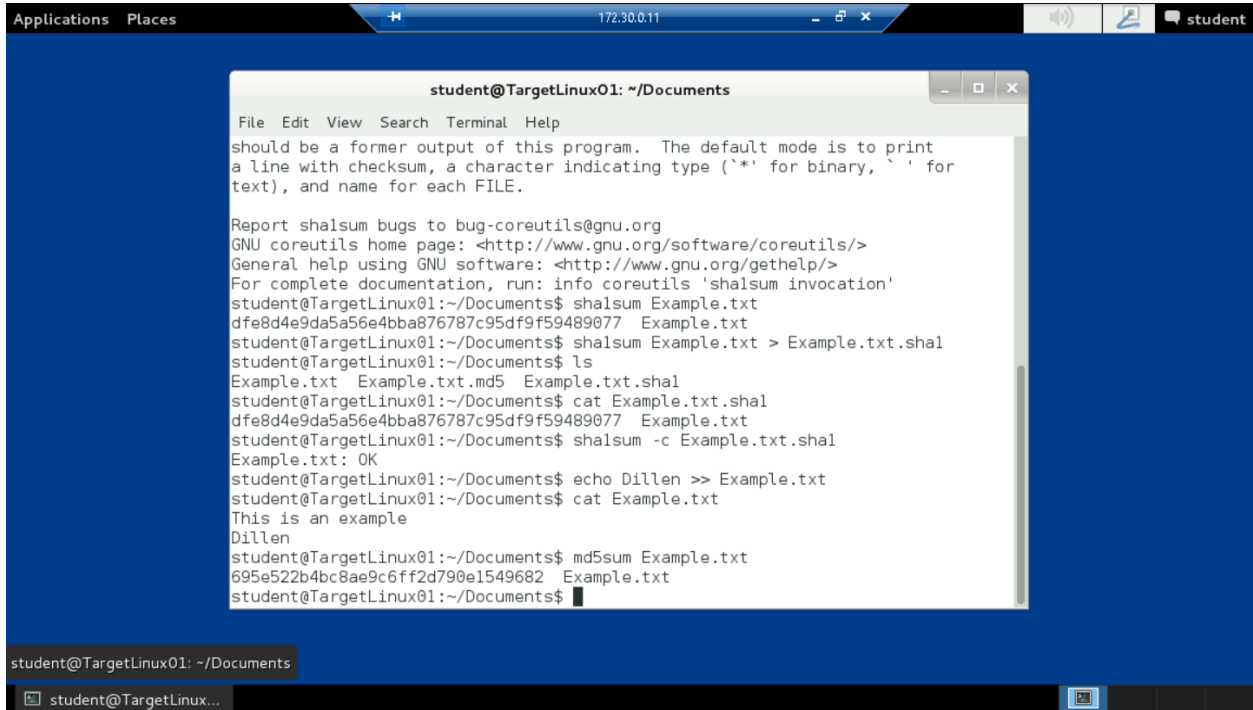
--strict        with --check, exit non-zero for any invalid input
--help          display this help and exit
--version       output version information and exit

The sums are computed as described in FIPS-180-1. When checking, the input
should be a former output of this program. The default mode is to print
a line with checksum, a character indicating type ('*' for binary, ' ' for
text), and name for each FILE.

Report shalsum bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
For complete documentation, run: info coreutils 'shalsum invocation'
student@TargetLinux01:~/Documents$ shalsum Example.txt
dfe8d4e9da5a56e4bba876787c95df9f59489077 Example.txt
student@TargetLinux01:~/Documents$ shalsum Example.txt > Example.txt.shal
student@TargetLinux01:~/Documents$ ls
Example.txt  Example.txt.md5  Example.txt.shal
student@TargetLinux01:~/Documents$ cat Example.txt.shal
dfe8d4e9da5a56e4bba876787c95df9f59489077 Example.txt
student@TargetLinux01:~/Documents$
```

## Section 1.3

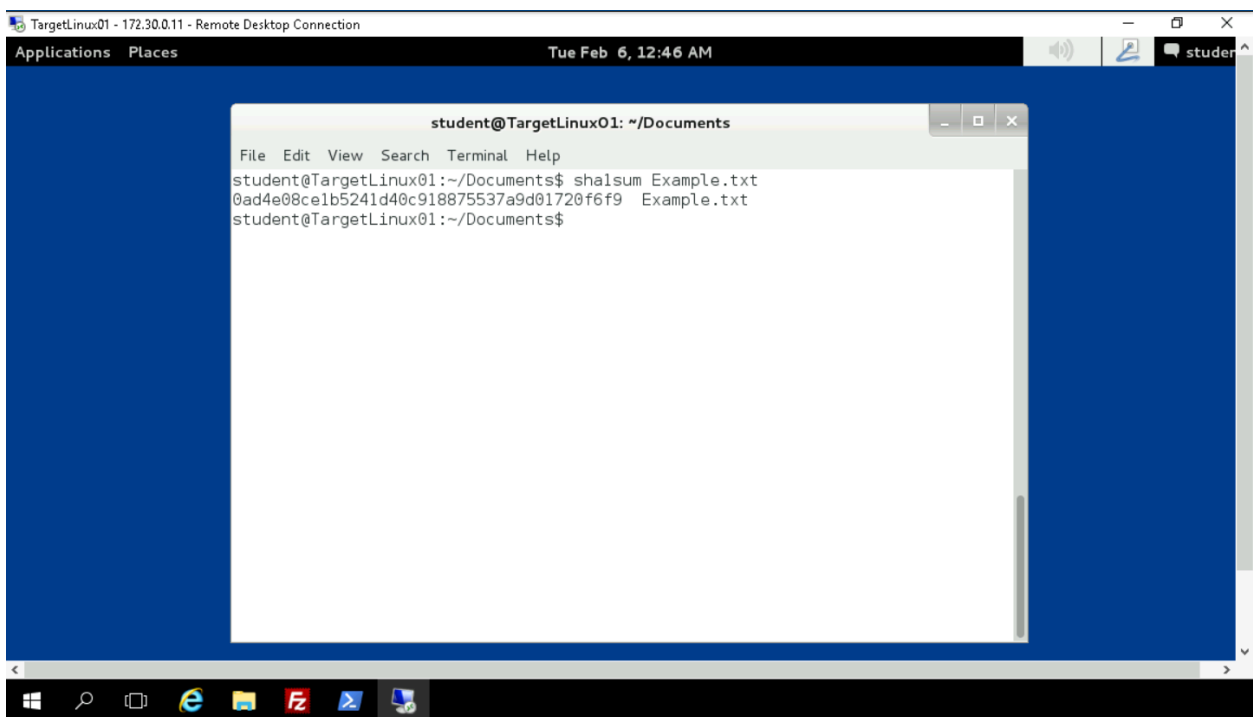
4



```
student@TargetLinux01: ~/Documents
File Edit View Search Terminal Help
should be a former output of this program. The default mode is to print
a line with checksum, a character indicating type ('*' for binary, ' ' for
text), and name for each FILE.

Report shasum bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
For complete documentation, run: info coreutils 'shasum invocation'
student@TargetLinux01:~/Documents$ shasum Example.txt
dfe8d4e9da5a56e4bba876787c95df9f59489077 Example.txt
student@TargetLinux01:~/Documents$ shasum Example.txt > Example.txt.shal
student@TargetLinux01:~/Documents$ ls
Example.txt Example.txt.md5 Example.txt.shal
student@TargetLinux01:~/Documents$ cat Example.txt.shal
dfe8d4e9da5a56e4bba876787c95df9f59489077 Example.txt
student@TargetLinux01:~/Documents$ shasum -c Example.txt.shal
Example.txt: OK
student@TargetLinux01:~/Documents$ echo Dillen >> Example.txt
student@TargetLinux01:~/Documents$ cat Example.txt
This is an example
Dillen
student@TargetLinux01:~/Documents$ md5sum Example.txt
695e522b4bc8ae9c6ff2d790e1549682 Example.txt
student@TargetLinux01:~/Documents$
```

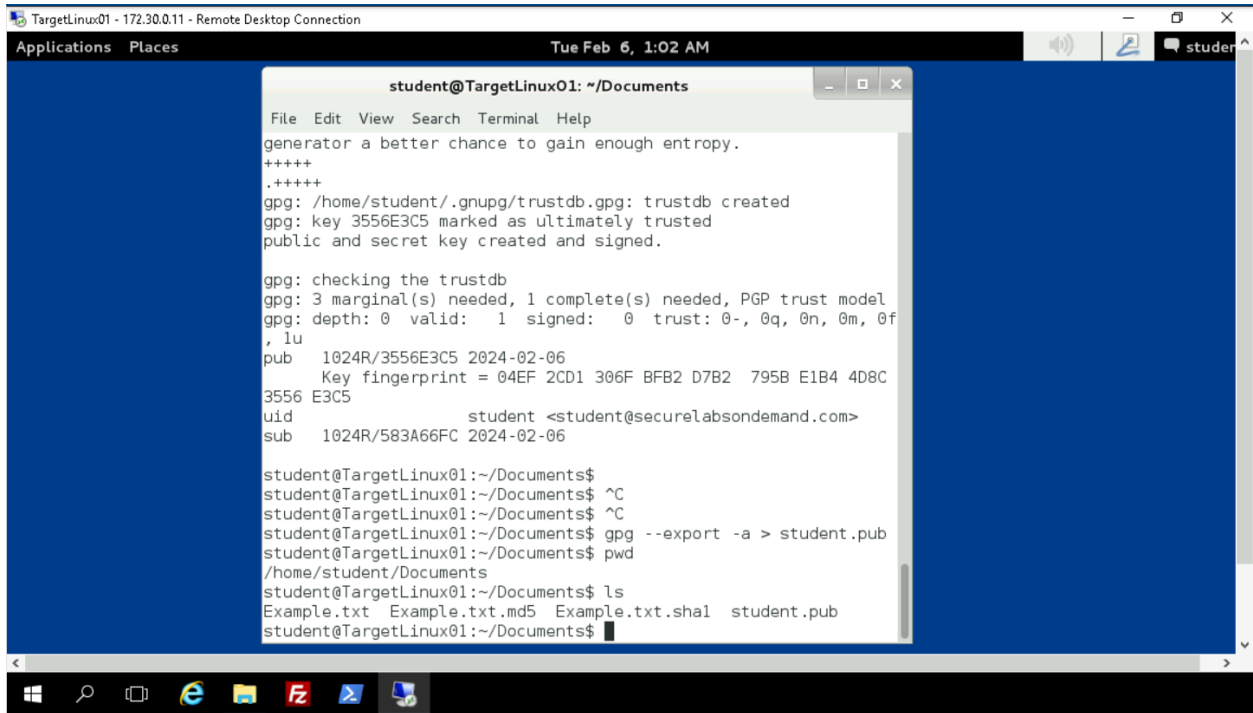
6



```
TargetLinux01 - 172.30.0.11 - Remote Desktop Connection
Applications Places Tue Feb 6, 12:46 AM
student@TargetLinux01: ~/Documents
File Edit View Search Terminal Help
student@TargetLinux01:~/Documents$ shasum Example.txt
0ad4e08ce1b5241d40c918875537a9d01720f6f9 Example.txt
student@TargetLinux01:~/Documents$
```

## Section 1.4

### Step 13



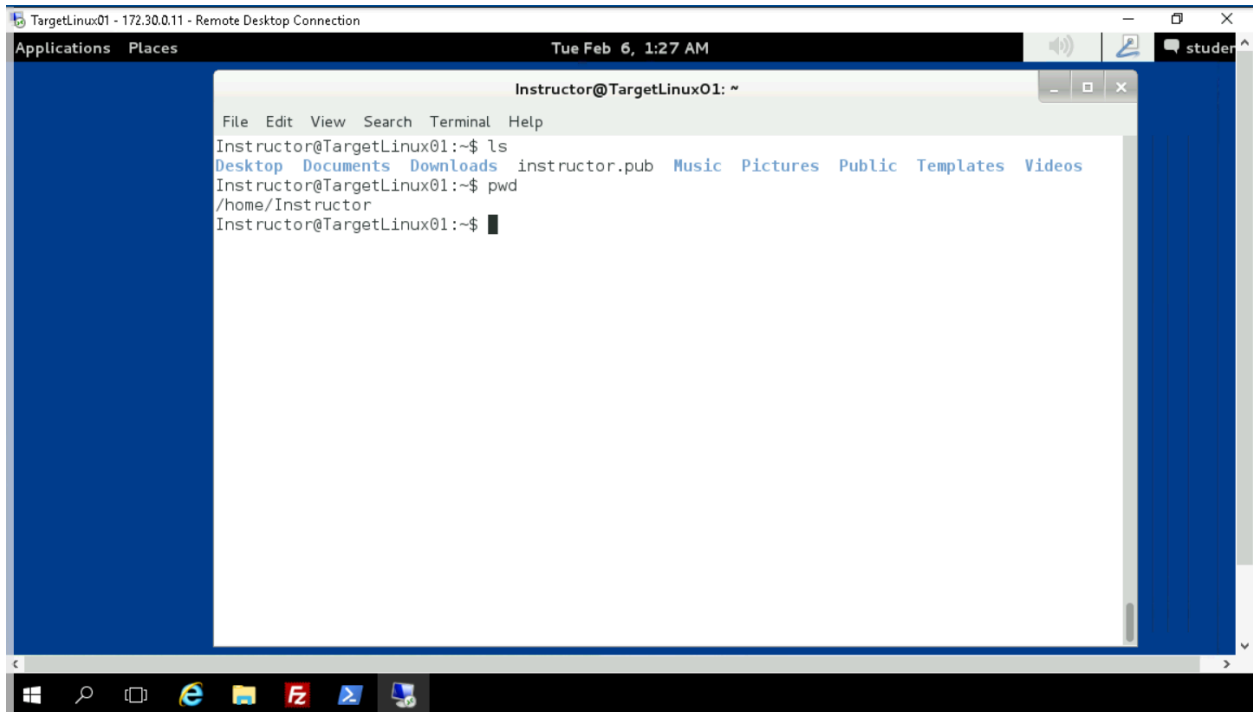
The screenshot shows a remote desktop connection to a machine named TargetLinux01. The top bar indicates the connection is established at 172.30.0.11. The desktop environment has a blue background and a taskbar at the bottom with icons for Windows, search, and various applications. A terminal window titled 'student@TargetLinux01: ~/Documents' is open, displaying the following commands and output:

```
File Edit View Search Terminal Help
generator a better chance to gain enough entropy.
+++++
+++++
gpg: /home/student/.gnupg/trustdb.gpg: trustdb created
gpg: key 3556E3C5 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f
, 1u
pub 1024R/3556E3C5 2024-02-06
Key fingerprint = 04EF 2CD1 306F BFB2 D7B2 795B E1B4 4D8C
3556 E3C5
uid student <student@securelabsondemand.com>
sub 1024R/583A66FC 2024-02-06

student@TargetLinux01:~/Documents$
student@TargetLinux01:~/Documents$ ^C
student@TargetLinux01:~/Documents$ ^C
student@TargetLinux01:~/Documents$ gpg --export -a > student.pub
student@TargetLinux01:~/Documents$ pwd
/home/student/Documents
student@TargetLinux01:~/Documents$ ls
Example.txt Example.txt.md5 Example.txt.shal student.pub
student@TargetLinux01:~/Documents$
```

### Step 21

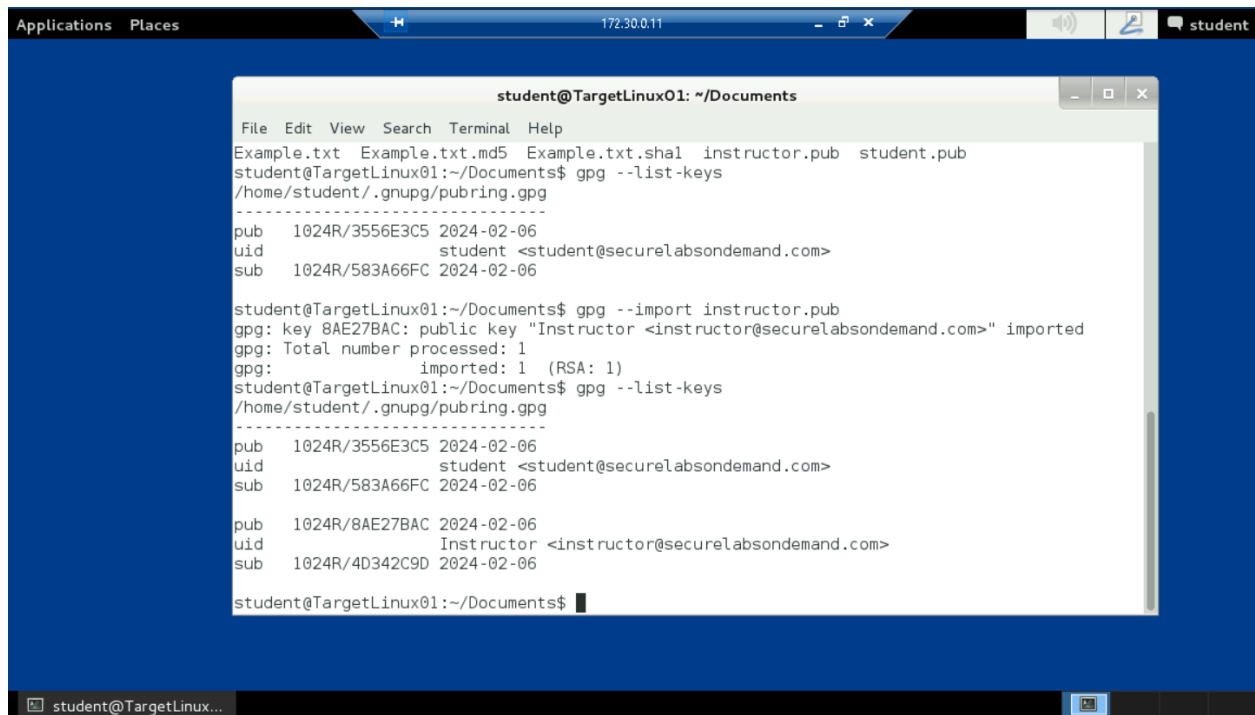


The screenshot shows the same remote desktop connection to TargetLinux01, but now the terminal window is titled 'Instructor@TargetLinux01: ~'. The desktop environment remains the same. The terminal window displays the following commands and output:

```
File Edit View Search Terminal Help
Instructor@TargetLinux01:~$ ls
Desktop Documents Downloads instructor.pub Music Pictures Public Templates Videos
Instructor@TargetLinux01:~$ pwd
/home/Instructor
Instructor@TargetLinux01:~$
```

## Section 1.5

### Step 6



The screenshot shows a terminal window titled "student@TargetLinux01: ~/Documents". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the following commands and results:

```
student@TargetLinux01:~/Documents$ gpg --list-keys
/home/student/.gnupg/pubring.gpg
-----
pub   1024R/3556E3C5 2024-02-06
uid         student <student@securelabsondemand.com>
sub   1024R/583A66FC 2024-02-06

student@TargetLinux01:~/Documents$ gpg --import instructor.pub
gpg: key 8AE27BAC: public key "Instructor <instructor@securelabsondemand.com>" imported
gpg: Total number processed: 1
gpg:         imported: 1 (RSA: 1)
student@TargetLinux01:~/Documents$ gpg --list-keys
/home/student/.gnupg/pubring.gpg
-----
pub   1024R/3556E3C5 2024-02-06
uid         student <student@securelabsondemand.com>
sub   1024R/583A66FC 2024-02-06

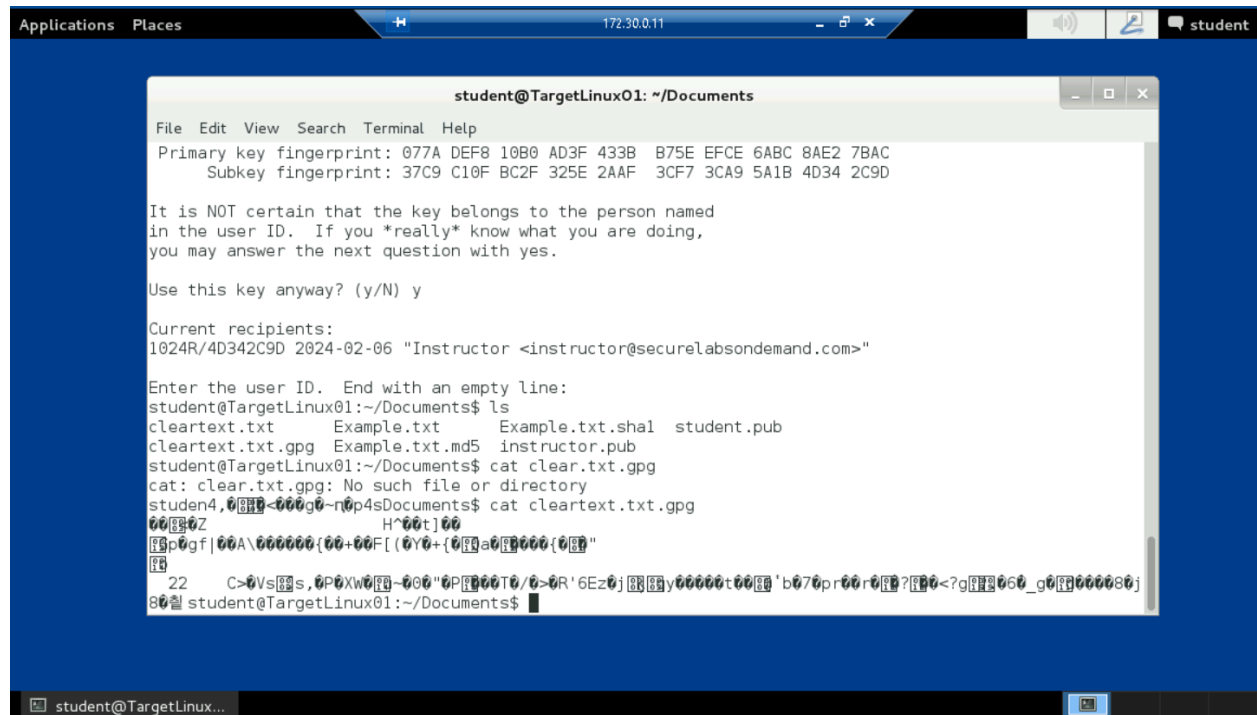
pub   1024R/8AE27BAC 2024-02-06
uid         Instructor <instructor@securelabsondemand.com>
sub   1024R/4D342C9D 2024-02-06

student@TargetLinux01:~/Documents$
```

The terminal window is part of a desktop environment with a top bar showing "Applications", "Places", and the IP address "172.30.0.11". The bottom status bar shows "student@TargetLinux..." and a system tray with a volume icon and a "student" notification.

## Section 1.6

### Step 8



```
student@TargetLinux01: ~/Documents
File Edit View Search Terminal Help
Primary key fingerprint: 077A DEF8 10B0 AD3F 433B  B75E EFCE 6ABC 8AE2 7BAC
Subkey fingerprint: 37C9 C10F BC2F 325E 2AAF  3CF7 3CA9 5A1B 4D34 2C9D

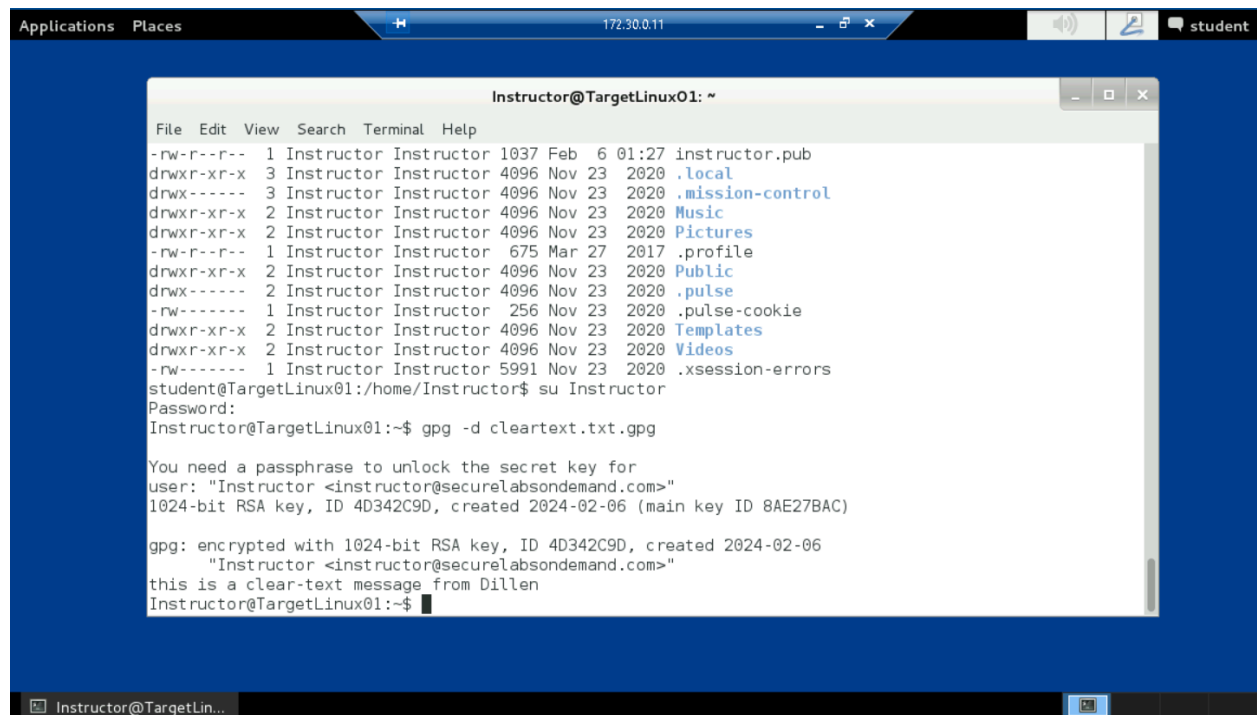
It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y

Current recipients:
1024R/4D342C9D 2024-02-06 "Instructor <instructor@securelabsondemand.com>"

Enter the user ID.  End with an empty line:
student@TargetLinux01:~/Documents$ ls
cleartext.txt      Example.txt      Example.txt.sha1  student.pub
cleartext.txt.gpg  Example.txt.md5  instructor.pub
student@TargetLinux01:~/Documents$ cat clear.txt.gpg
cat: clear.txt.gpg: No such file or directory
student@TargetLinux01:~/Documents$ cat clear.txt.txt.gpg
22 C>0Vs00s,0P0XW0F0~000'0P0000T0/0>0R'6Ez0j0000y00000t0000'b070pr00r000?000<?g000060_g00000080j'
0000 student@TargetLinux01:~/Documents$
```

### Step 19



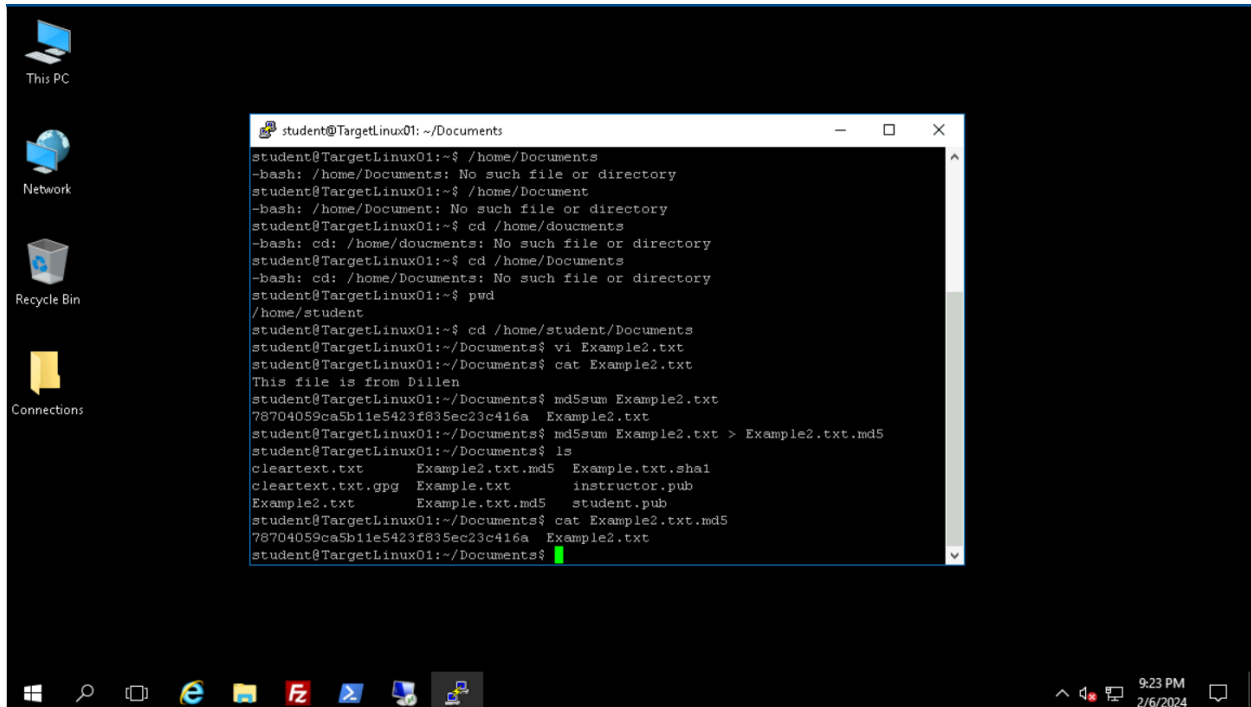
```
Instructor@TargetLinux01: ~
File Edit View Search Terminal Help
-rw-r--r-- 1 Instructor Instructor 1037 Feb  6 01:27 instructor.pub
drwxr-xr-x 3 Instructor Instructor 4096 Nov 23 2020 .local
drwxr-xr-x 3 Instructor Instructor 4096 Nov 23 2020 .mission-control
drwxr-xr-x 2 Instructor Instructor 4096 Nov 23 2020 Music
drwxr-xr-x 2 Instructor Instructor 4096 Nov 23 2020 Pictures
-rw-r--r-- 1 Instructor Instructor  675 Mar 27 2017 .profile
drwxr-xr-x 2 Instructor Instructor 4096 Nov 23 2020 Public
drwxr-xr-x 2 Instructor Instructor 4096 Nov 23 2020 .pulse
-rw-r--r-- 1 Instructor Instructor  256 Nov 23 2020 .pulse-cookie
drwxr-xr-x 2 Instructor Instructor 4096 Nov 23 2020 Templates
drwxr-xr-x 2 Instructor Instructor 4096 Nov 23 2020 Videos
-rw-r--r-- 1 Instructor Instructor 5991 Nov 23 2020 .xsession-errors
student@TargetLinux01:/home/Instructor$ su Instructor
Password:
Instructor@TargetLinux01:~$ gpg -d cleartext.txt.gpg

You need a passphrase to unlock the secret key for
user: "Instructor <instructor@securelabsondemand.com>"
1024-bit RSA key, ID 4D342C9D, created 2024-02-06 (main key ID 8AE27BAC)

gpg: encrypted with 1024-bit RSA key, ID 4D342C9D, created 2024-02-06
      "Instructor <instructor@securelabsondemand.com>"
this is a clear-text message from Dillen
Instructor@TargetLinux01:~$
```

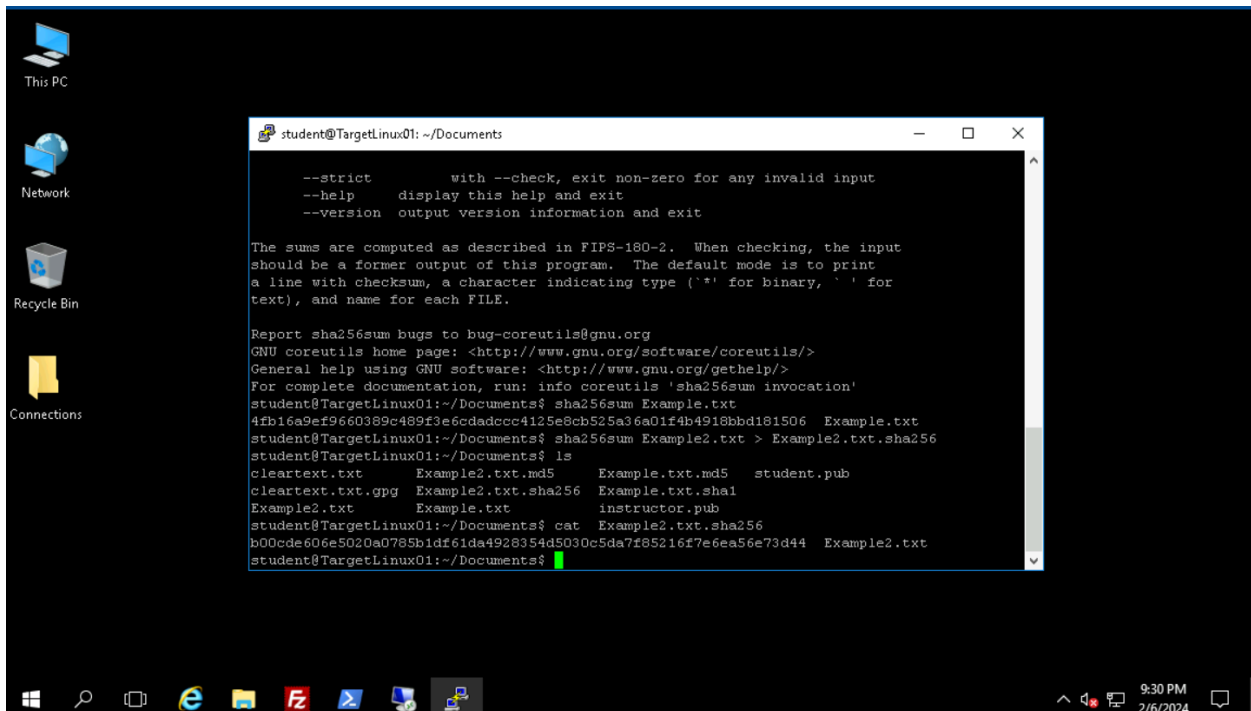
## Section 2.2

### Step 6



```
student@TargetLinux01: ~/Documents
student@TargetLinux01:~$ /home/Documents
-bash: /home/Documents: No such file or directory
student@TargetLinux01:~$ /home/Document
-bash: /home/Document: No such file or directory
student@TargetLinux01:~$ cd /home/documents
-bash: cd: /home/documents: No such file or directory
student@TargetLinux01:~$ cd /home/Documents
-bash: cd: /home/Documents: No such file or directory
student@TargetLinux01:~$ pwd
/home/student
student@TargetLinux01:~$ cd /home/student/Documents
student@TargetLinux01:~/Documents$ vi Example2.txt
student@TargetLinux01:~/Documents$ cat Example2.txt
This file is from Dillen
student@TargetLinux01:~/Documents$ md5sum Example2.txt
78704059ca5b11e5423f835ec23c416a  Example2.txt
student@TargetLinux01:~/Documents$ md5sum Example2.txt > Example2.txt.md5
student@TargetLinux01:~/Documents$ ls
cleartext.txt      Example2.txt.md5  Example.txt.sha1
cleartext.txt.gpg  Example.txt       instructor.pub
Example2.txt       Example.txt.md5   student.pub
student@TargetLinux01:~/Documents$ cat Example2.txt.md5
78704059ca5b11e5423f835ec23c416a  Example2.txt
student@TargetLinux01:~/Documents$
```

### Step 13



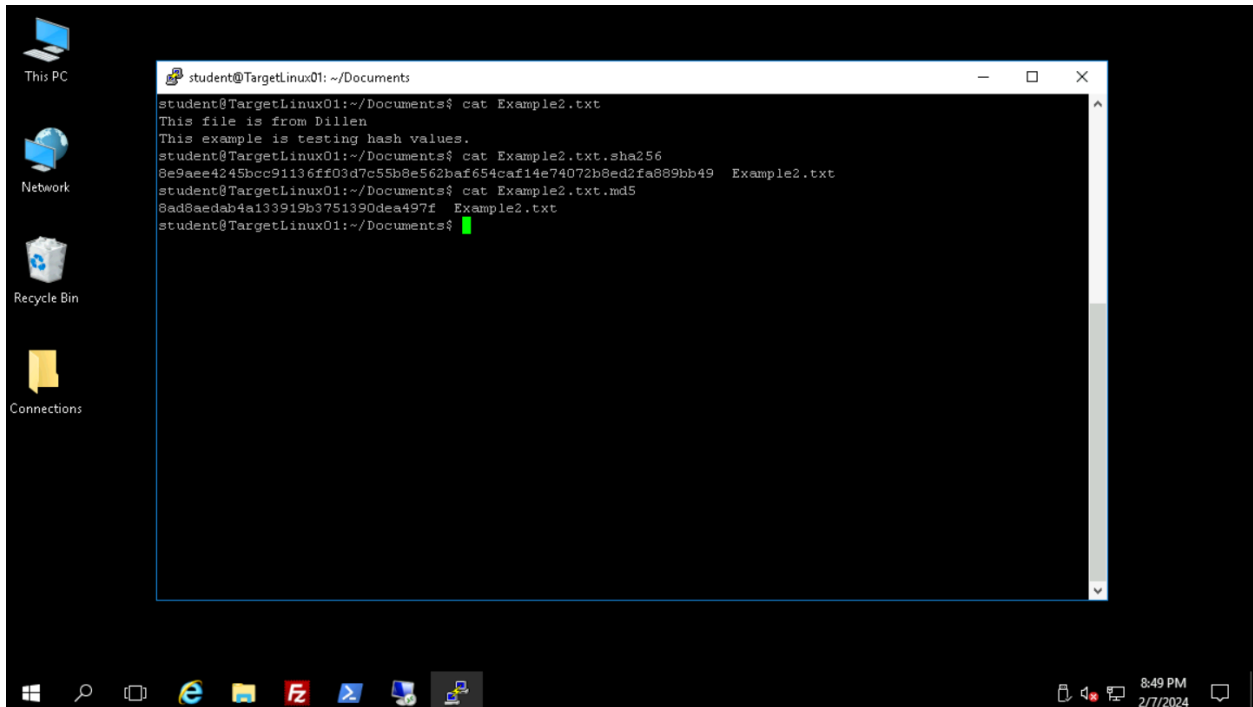
```
--strict      with --check, exit non-zero for any invalid input
--help        display this help and exit
--version     output version information and exit

The sums are computed as described in FIPS-180-2.  When checking, the input
should be a former output of this program.  The default mode is to print
a line with checksum, a character indicating type ('*' for binary, ' ' for
text), and name for each FILE.

Report sha256sum bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
For complete documentation, run: info coreutils 'sha256sum invocation'
student@TargetLinux01:~/Documents$ sha256sum Example.txt
4fb16a9ef9660389c489f3e6cdadccc4125e8cb525a36a01f4b4918bbd181506  Example.txt
student@TargetLinux01:~/Documents$ sha256sum Example2.txt > Example2.txt.sha256
student@TargetLinux01:~/Documents$ ls
cleartext.txt      Example2.txt.md5  Example.txt.md5  student.pub
cleartext.txt.gpg  Example2.txt.sha256  Example.txt.sha1
Example2.txt       Example.txt       instructor.pub
student@TargetLinux01:~/Documents$ cat Example2.txt.sha256
b00cde606e5020a0785b1df61da4928354d5030c5da7f85216f7e6ea56e73d44  Example2.txt
student@TargetLinux01:~/Documents$
```

## Section 2.3

### Step 7



The screenshot shows a Windows desktop environment. On the left side, there is a vertical taskbar with icons for 'This PC', 'Network', 'Recycle Bin', and 'Connections'. The main area of the desktop is black. A terminal window is open in the center, titled 'student@TargetLinux01: ~/Documents'. The terminal displays the following text:

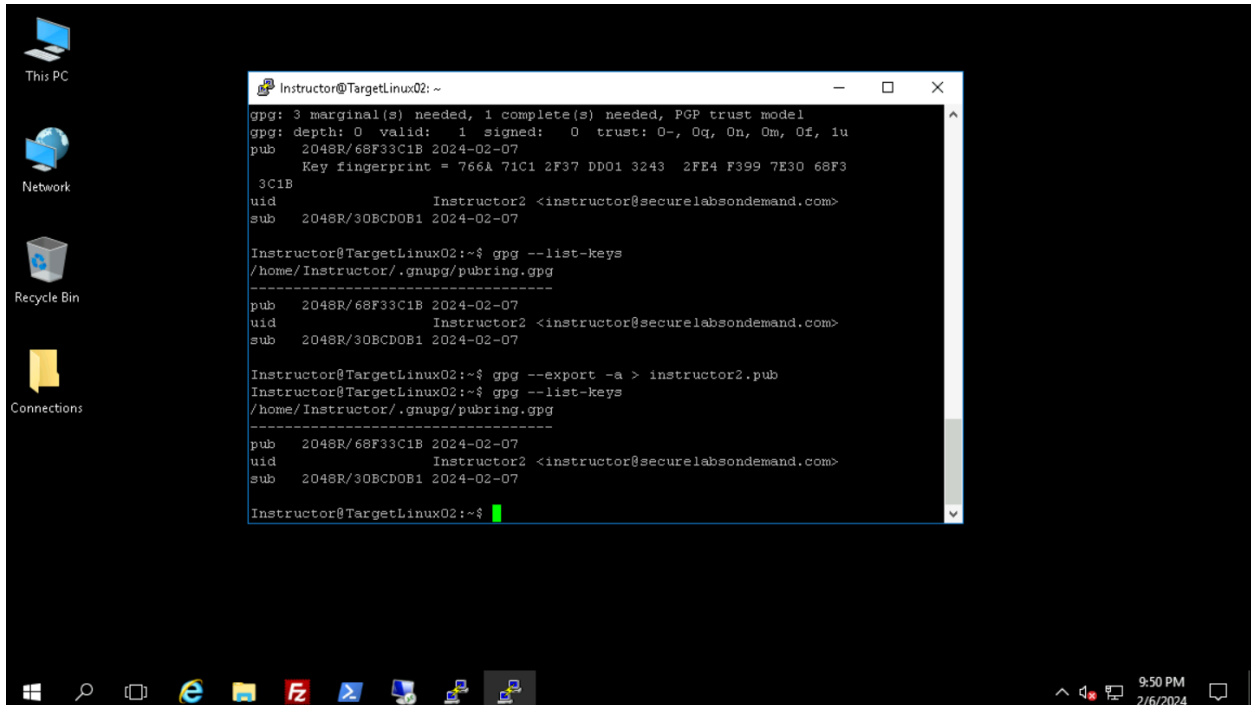
```
student@TargetLinux01:~/Documents$ cat Example2.txt
This file is from Dillen
This example is testing hash values.
student@TargetLinux01:~/Documents$ cat Example2.txt.sha256
8e9aee4245bcc91136ff03d7c55b8e562baf654caf14e74072b8ed2fa889bb49 Example2.txt
student@TargetLinux01:~/Documents$ cat Example2.txt.md5
8ad8aedab4a133919b3751390dea497f Example2.txt
student@TargetLinux01:~/Documents$
```

The terminal window has a standard Windows title bar with minimize, maximize, and close buttons. The bottom of the screen shows a Windows taskbar with various application icons and a system tray on the right displaying the time '8:49 PM' and the date '2/7/2024'.



## Section 2.4

### Step 17



The screenshot shows a Windows desktop with a terminal window titled "Instructor@TargetLinux02: ~". The terminal displays the following commands and output:

```
Instructor@TargetLinux02: ~$ gpg --list-keys
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0a, 0m, 0f, 1u
pub 2048R/68F33C1B 2024-02-07
Key fingerprint = 766A 71C1 2F37 DD01 3243 2FE4 F399 7E30 68F3
3C1B
uid      Instructor2 <instructor@securelabsondemand.com>
sub 2048R/30BCD0B1 2024-02-07

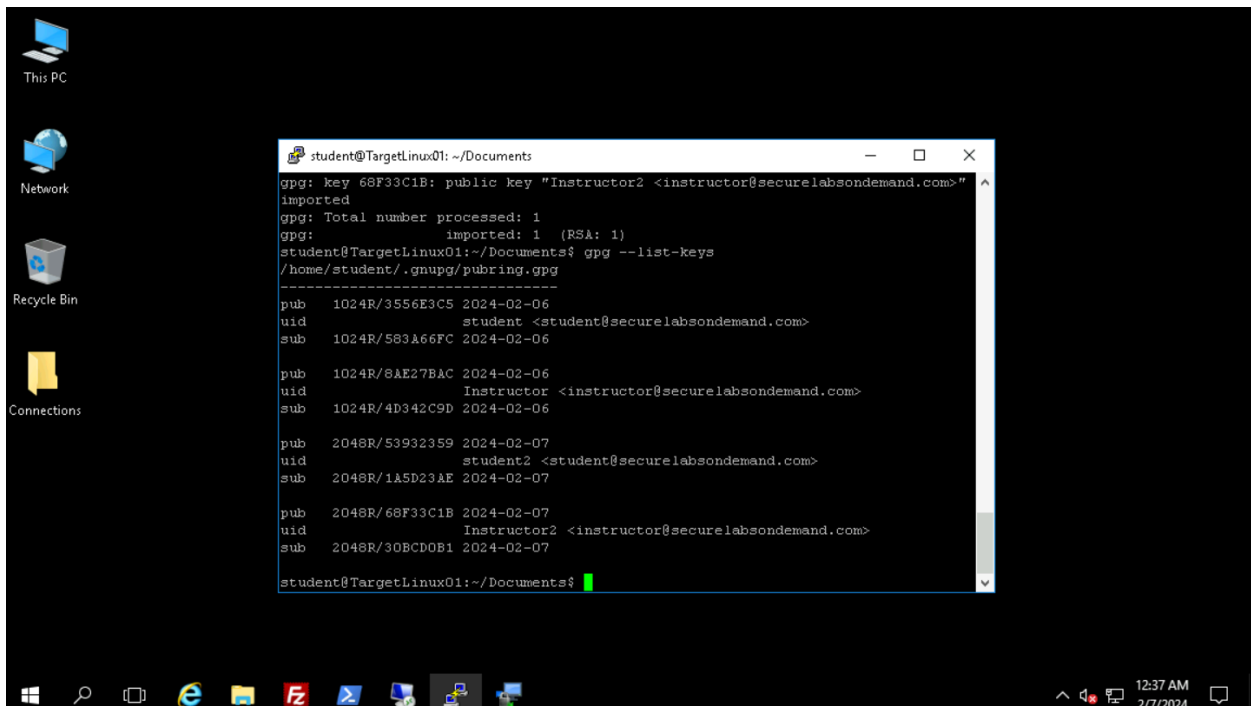
Instructor@TargetLinux02:~$ gpg --export -a > instructor2.pub
Instructor@TargetLinux02:~$ gpg --list-keys
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0a, 0m, 0f, 1u
pub 2048R/68F33C1B 2024-02-07
Key fingerprint = 766A 71C1 2F37 DD01 3243 2FE4 F399 7E30 68F3
3C1B
uid      Instructor2 <instructor@securelabsondemand.com>
sub 2048R/30BCD0B1 2024-02-07

Instructor@TargetLinux02:~$ gpg --export -a > instructor2.pub
Instructor@TargetLinux02:~$ gpg --list-keys
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0a, 0m, 0f, 1u
pub 2048R/68F33C1B 2024-02-07
Key fingerprint = 766A 71C1 2F37 DD01 3243 2FE4 F399 7E30 68F3
3C1B
uid      Instructor2 <instructor@securelabsondemand.com>
sub 2048R/30BCD0B1 2024-02-07

Instructor@TargetLinux02:~$
```

## Section 2.5

### Step 12



The screenshot shows a Windows desktop with a terminal window titled "student@TargetLinux01: ~/Documents". The terminal displays the following commands and output:

```
student@TargetLinux01: ~/Documents$ gpg --import instructor2.pub
gpg: key 68F33C1B: public key "Instructor2 <instructor@securelabsondemand.com>"
imported
gpg: Total number processed: 1
gpg:      imported: 1 (RSA: 1)
student@TargetLinux01:~/Documents$ gpg --list-keys
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0a, 0m, 0f, 1u
pub 1024R/3556E3C5 2024-02-06
uid      student <student@securelabsondemand.com>
sub 1024R/583A66FC 2024-02-06

pub 1024R/8AE27BAC 2024-02-06
uid      Instructor <instructor@securelabsondemand.com>
sub 1024R/4D342C9D 2024-02-06

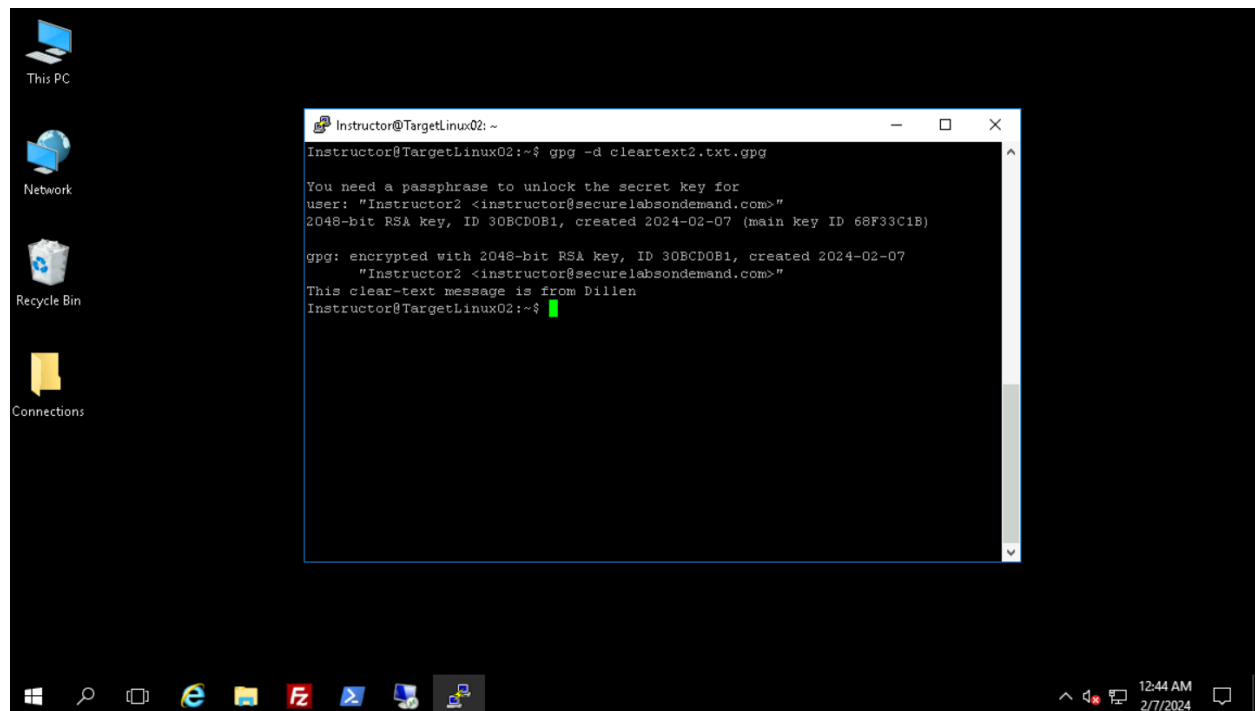
pub 2048R/53932359 2024-02-07
uid      student2 <student@securelabsondemand.com>
sub 2048R/1A5D23AE 2024-02-07

pub 2048R/68F33C1B 2024-02-07
uid      Instructor2 <instructor@securelabsondemand.com>
sub 2048R/30BCD0B1 2024-02-07

student@TargetLinux01:~/Documents$
```

## Section 2.6

### Step 19



### Section 3.1

Describe the differences between RSA and ECDSA encryption algorithms, and name a well-known product that uses each type of encryption. Cite your references

Both RSA and ECDSA depend on mathematical principles. RSA relies on the complexity of factoring large numbers that are the product of two large prime numbers. However, ECDSA is built upon elliptic curve cryptography, utilizing elliptical curves and a function referred to as a "trapdoor function" (Thakkar). Despite providing a similar level of security to RSA, ECDSA accomplishes this with significantly shorter key lengths (Baeldung). RSA is widely employed in SSL/TLS certificates, VPNs, and email clients, with RSA-enabled chips embedded in computers from manufacturers like Samsung, Toshiba, and LG. Similarly, ECDSA plays a vital role in Bitcoin's cryptographic framework, generating addresses from ECDSA public keys and securing transactions through ECDSA signatures (Sullivan).

#### Works Cited

Baeldung. "Encryption: ECDSA vs. RSA Keys." *Baeldung*, 20 September 2023,

<https://www.baeldung.com/cs/encryption-asymmetric-algorithms>. Accessed 7 February 2024.

Cobb, Michael. "What is the RSA algorithm? Definition from SearchSecurity." *TechTarget*,

<https://www.techtarget.com/searchsecurity/definition/RSA>. Accessed 7 February 2024.

Okta. "RSA Encryption: Definition, Architecture, Benefits & Use." *Okta*, 14 February 2023,

<https://www.okta.com/identity-101/rsa-encryption/>. Accessed 7 February 2024.

Sullivan, Nick. "ECDSA: The digital signature algorithm of a better internet." *The Cloudflare*

*Blog*, 10 March 2014,

<https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet>.

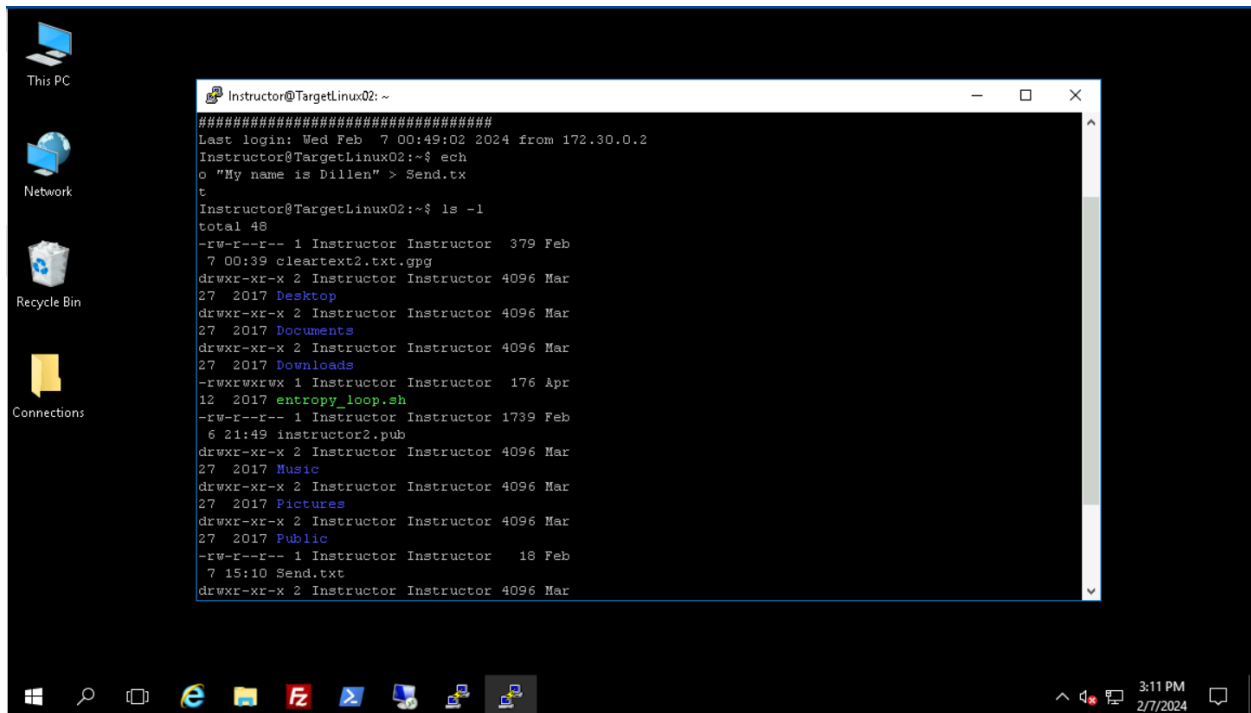
Accessed 7 February 2024.

Thakkar, Jay. "ECDSA vs RSA: Everything You Need to Know." *Sectigo*, 9 June 2020,

<https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/>. Accessed 7 February 2024.

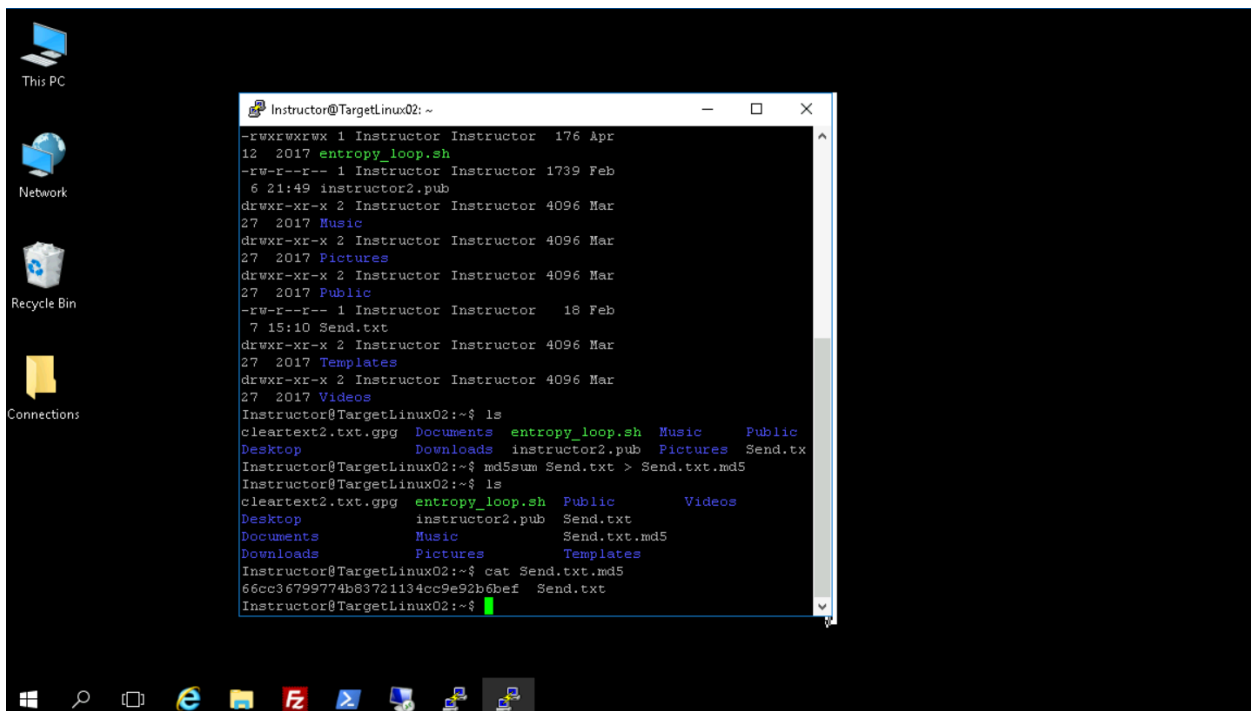
## Section 3.2

### Step a.



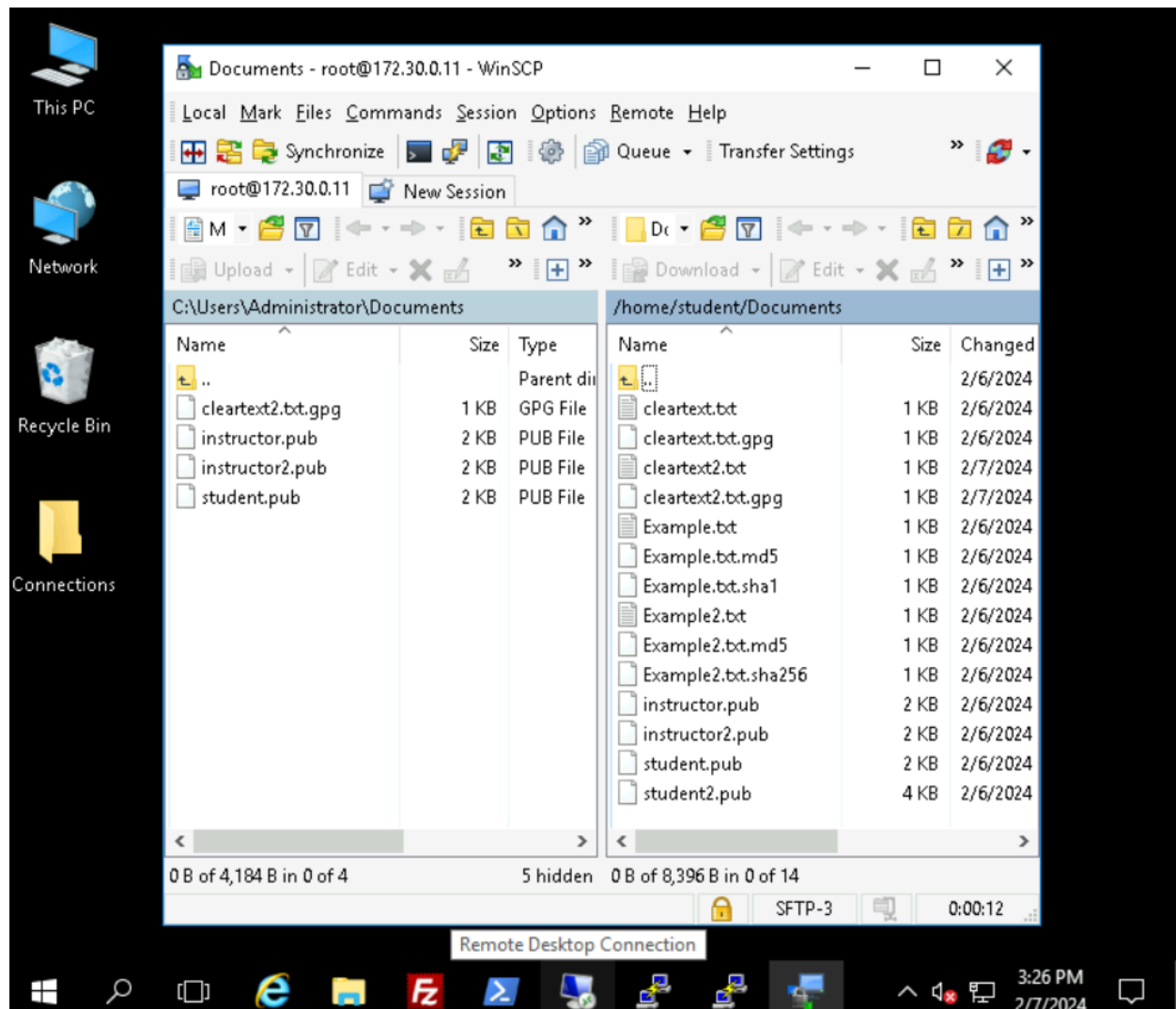
```
Instructor@TargetLinux02: ~  
#####  
Last login: Wed Feb  7 00:49:02 2024 from 172.30.0.2  
Instructor@TargetLinux02:~$ ech  
o "My name is Dillen" > Send.tx  
t  
Instructor@TargetLinux02:~$ ls -l  
total 48  
-rw-r--r--  1 Instructor Instructor  379 Feb  
  7 00:39 cleartext2.txt.gpg  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Desktop  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Documents  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Downloads  
-rwxrwxrwx  1 Instructor Instructor  176 Apr  
12  2017 entropy_loop.sh  
-rw-r--r--  1 Instructor Instructor 1739 Feb  
  6 21:49 instructor2.pub  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Music  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Pictures  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Public  
-rw-r--r--  1 Instructor Instructor   18 Feb  
  7 15:10 Send.txt  
drwxr-xr-x  2 Instructor Instructor 4096 Mar
```

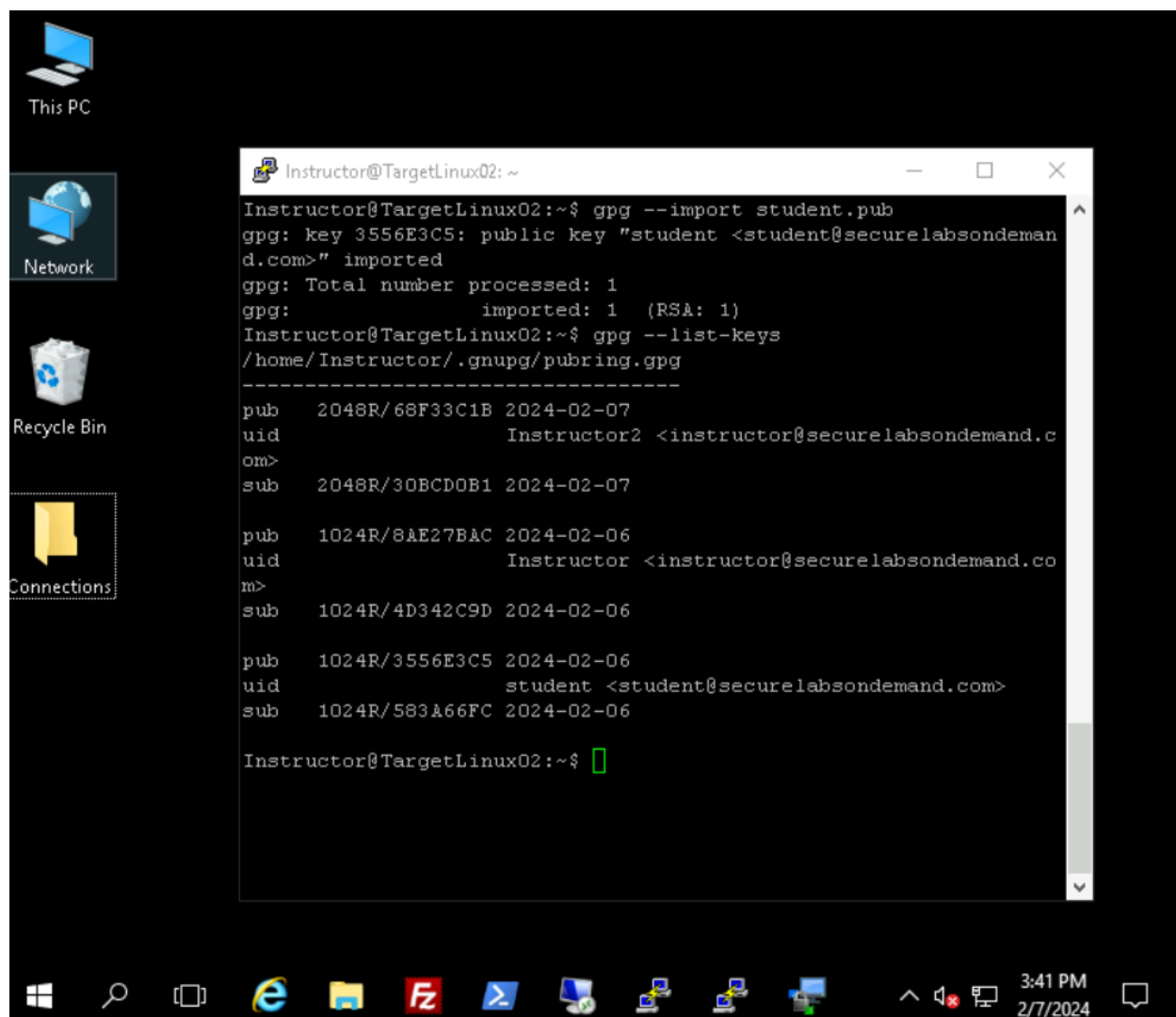
### Step b.



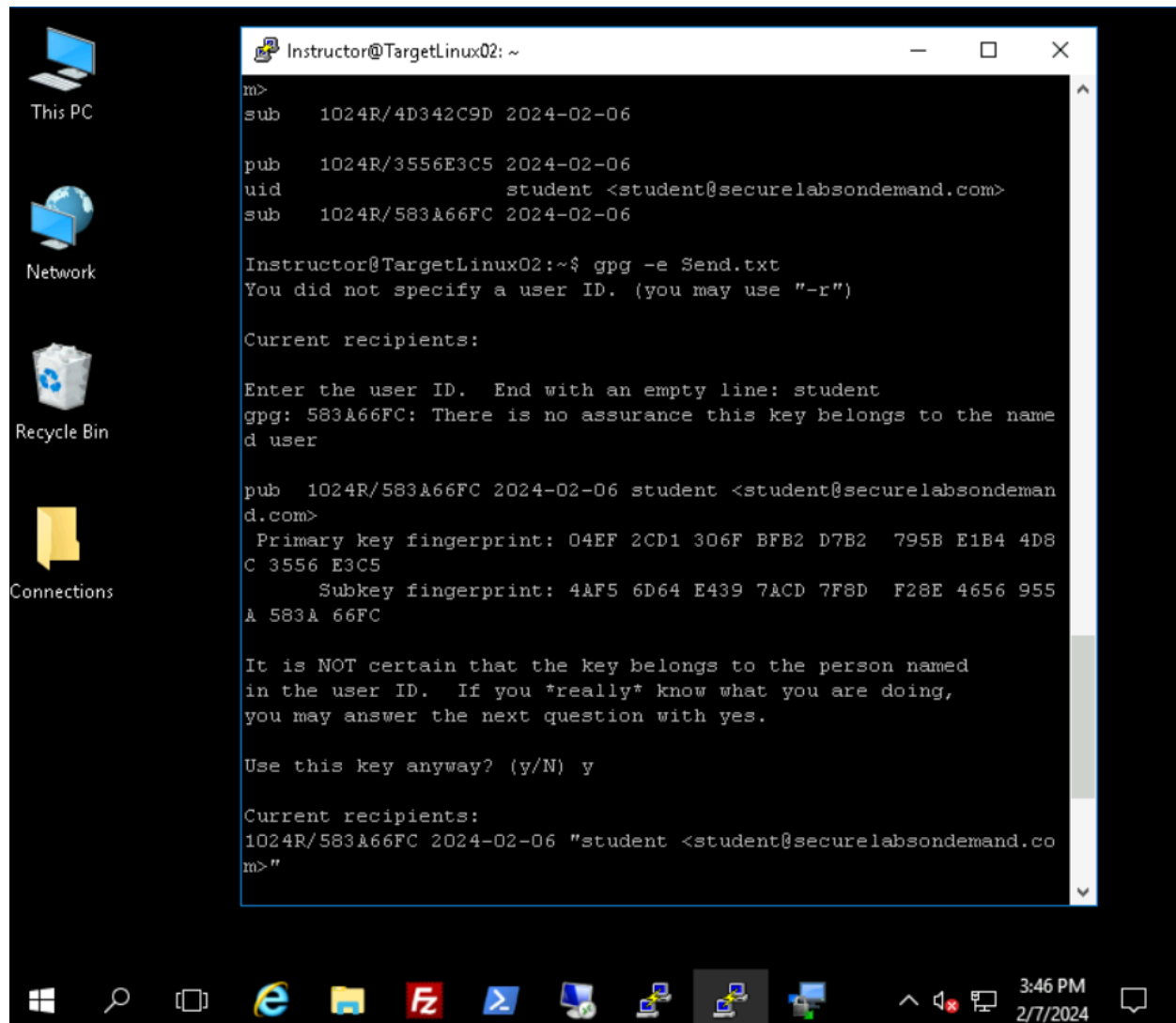
```
Instructor@TargetLinux02: ~  
-rwxrwxrwx  1 Instructor Instructor  176 Apr  
12  2017 entropy_loop.sh  
-rw-r--r--  1 Instructor Instructor 1739 Feb  
  6 21:49 instructor2.pub  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Music  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Pictures  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Public  
-rw-r--r--  1 Instructor Instructor   18 Feb  
  7 15:10 Send.txt  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Templates  
drwxr-xr-x  2 Instructor Instructor 4096 Mar  
27  2017 Videos  
Instructor@TargetLinux02:~$ ls  
cleartext2.txt.gpg  Documents  entropy_loop.sh  Music      Public  
Desktop            Downloads  instructor2.pub  Pictures  Send.tx  
Instructor@TargetLinux02:~$ md5sum Send.txt > Send.txt.md5  
Instructor@TargetLinux02:~$ ls  
cleartext2.txt.gpg  entropy_loop.sh  Public      Videos  
Desktop            instructor2.pub  Send.txt  
Documents          Music           Send.txt.md5  
Downloads          Pictures        Templates  
Instructor@TargetLinux02:~$ cat Send.txt.md5  
66cc36799774b83721134cc9e92b6bef  Send.txt  
Instructor@TargetLinux02:~$
```

Step c.





Step d.



```
Instructor@TargetLinux02: ~
m>
sub 1024R/4D342C9D 2024-02-06

pub 1024R/3556E3C5 2024-02-06
uid student <student@securelabsondemand.com>
sub 1024R/583A66FC 2024-02-06

Instructor@TargetLinux02:~$ gpg -e Send.txt
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID. End with an empty line: student
gpg: 583A66FC: There is no assurance this key belongs to the named user

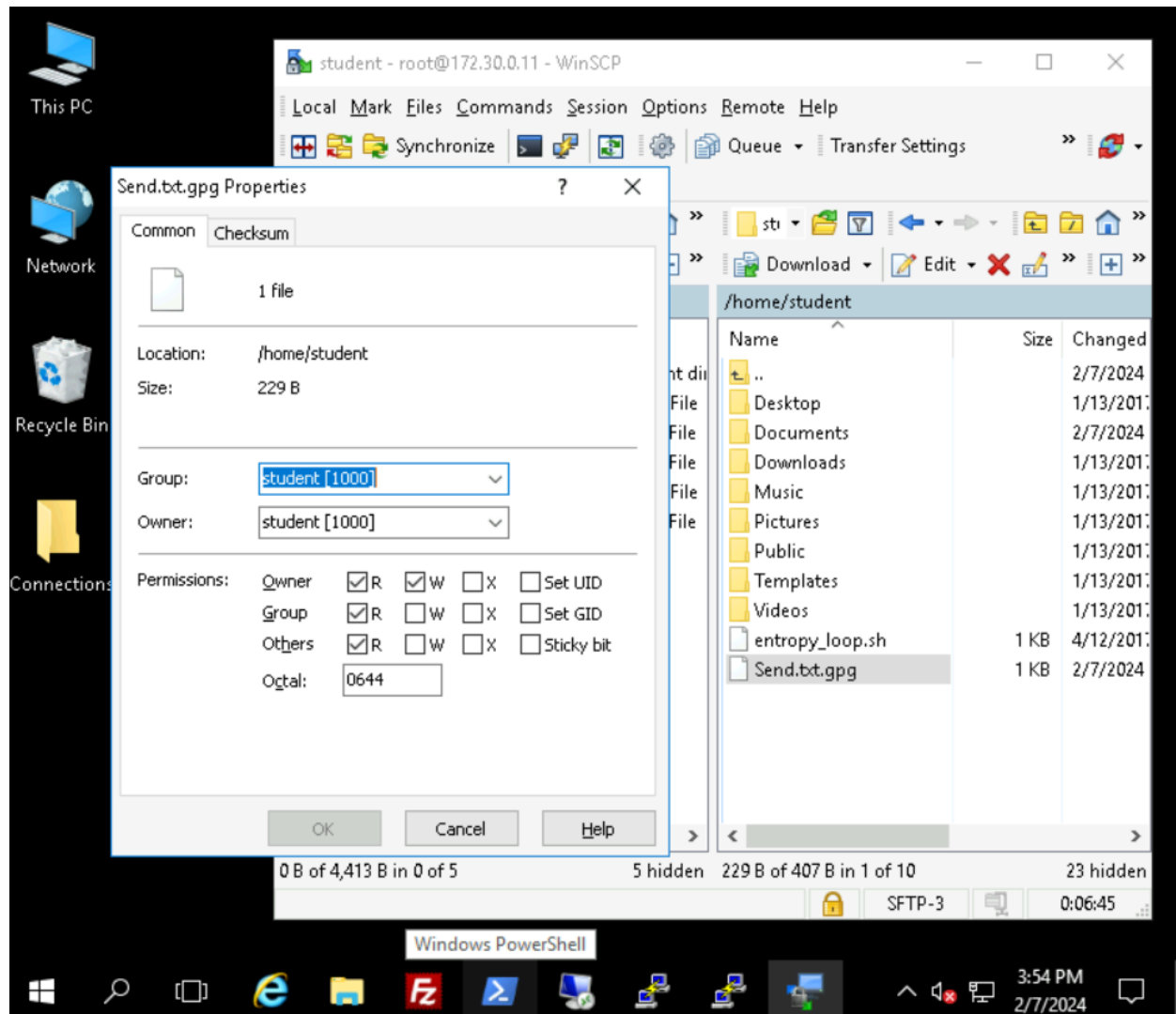
pub 1024R/583A66FC 2024-02-06 student <student@securelabsondemand.com>
Primary key fingerprint: 04EF 2CD1 306F BFB2 D7B2 795B E1B4 4D8C 3556 E3C5
Subkey fingerprint: 4AF5 6D64 E439 7ACD 7F8D F28E 4656 955A 583A 66FC

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

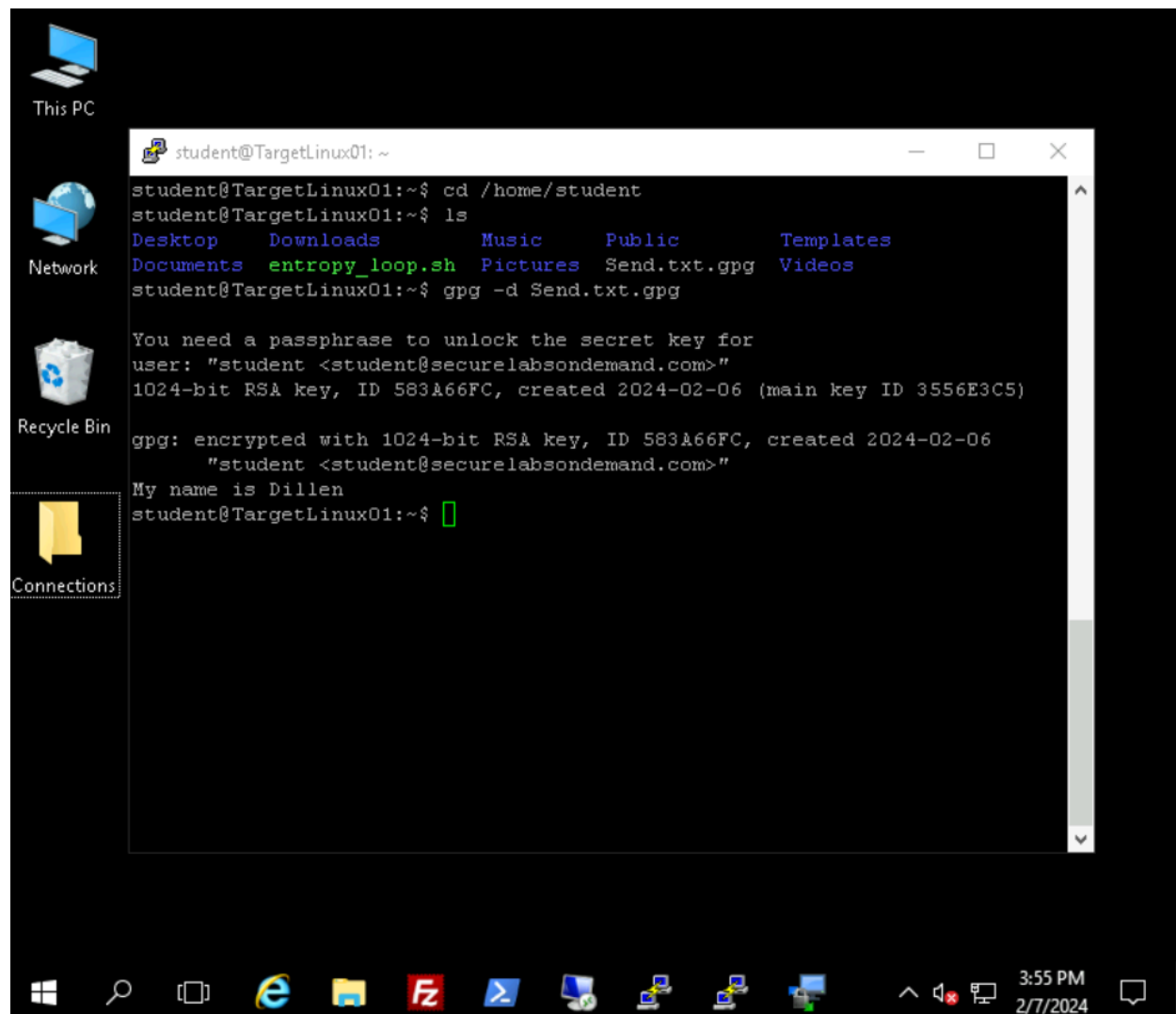
Use this key anyway? (y/N) y

Current recipients:
1024R/583A66FC 2024-02-06 "student <student@securelabsondemand.com>"
m>
```

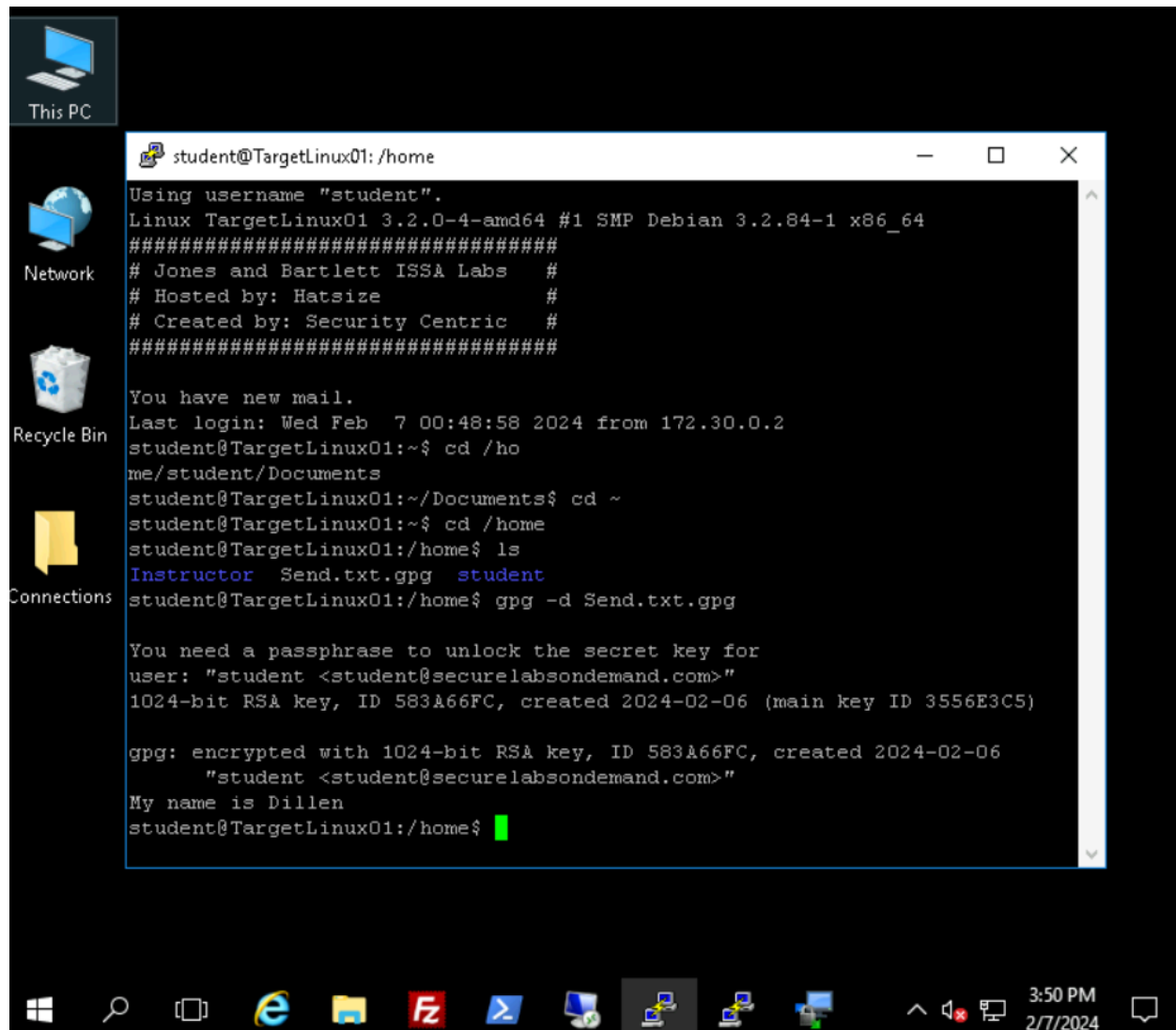
Step e.





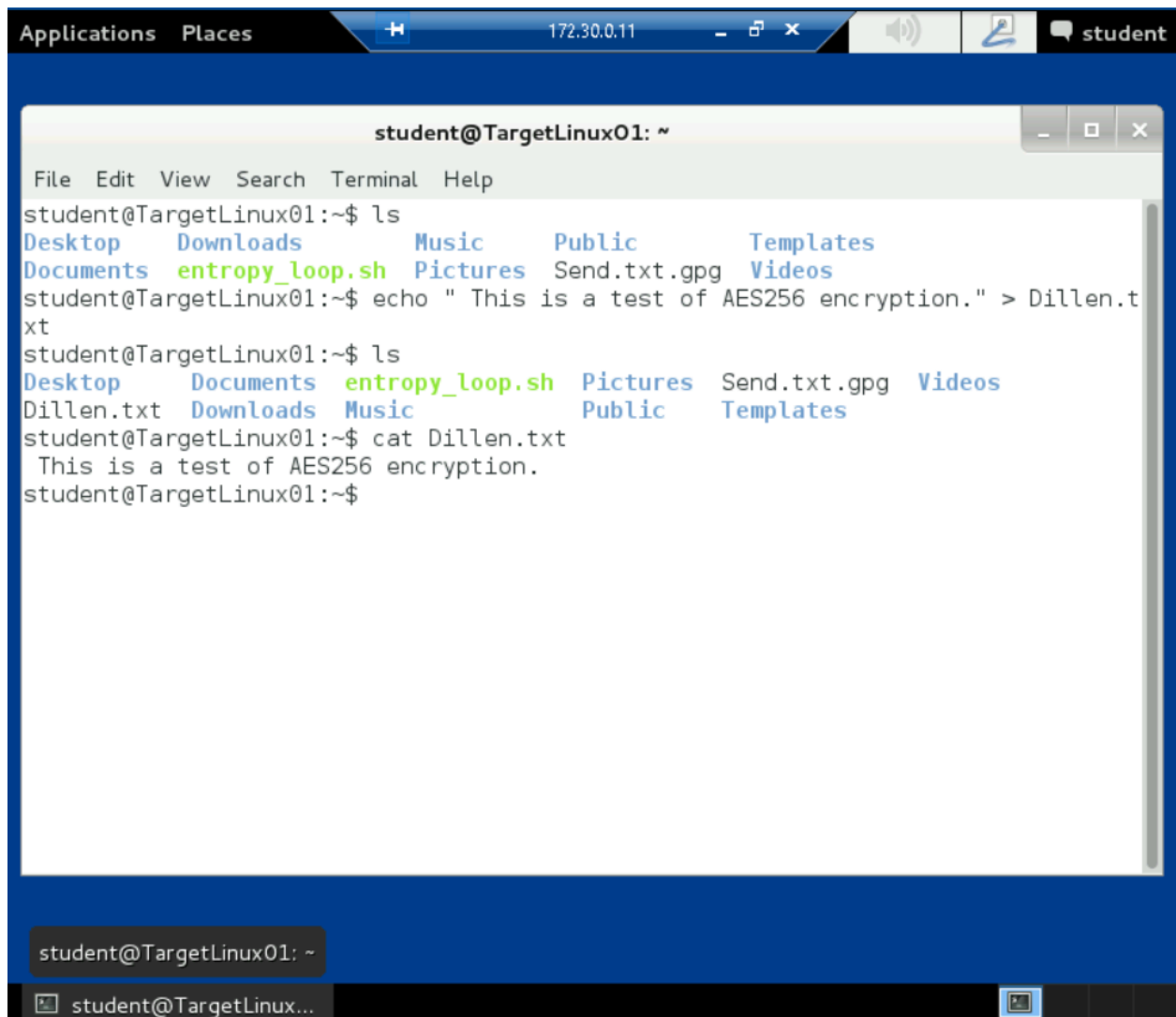


Step e.



### Section 3.3

Step a.

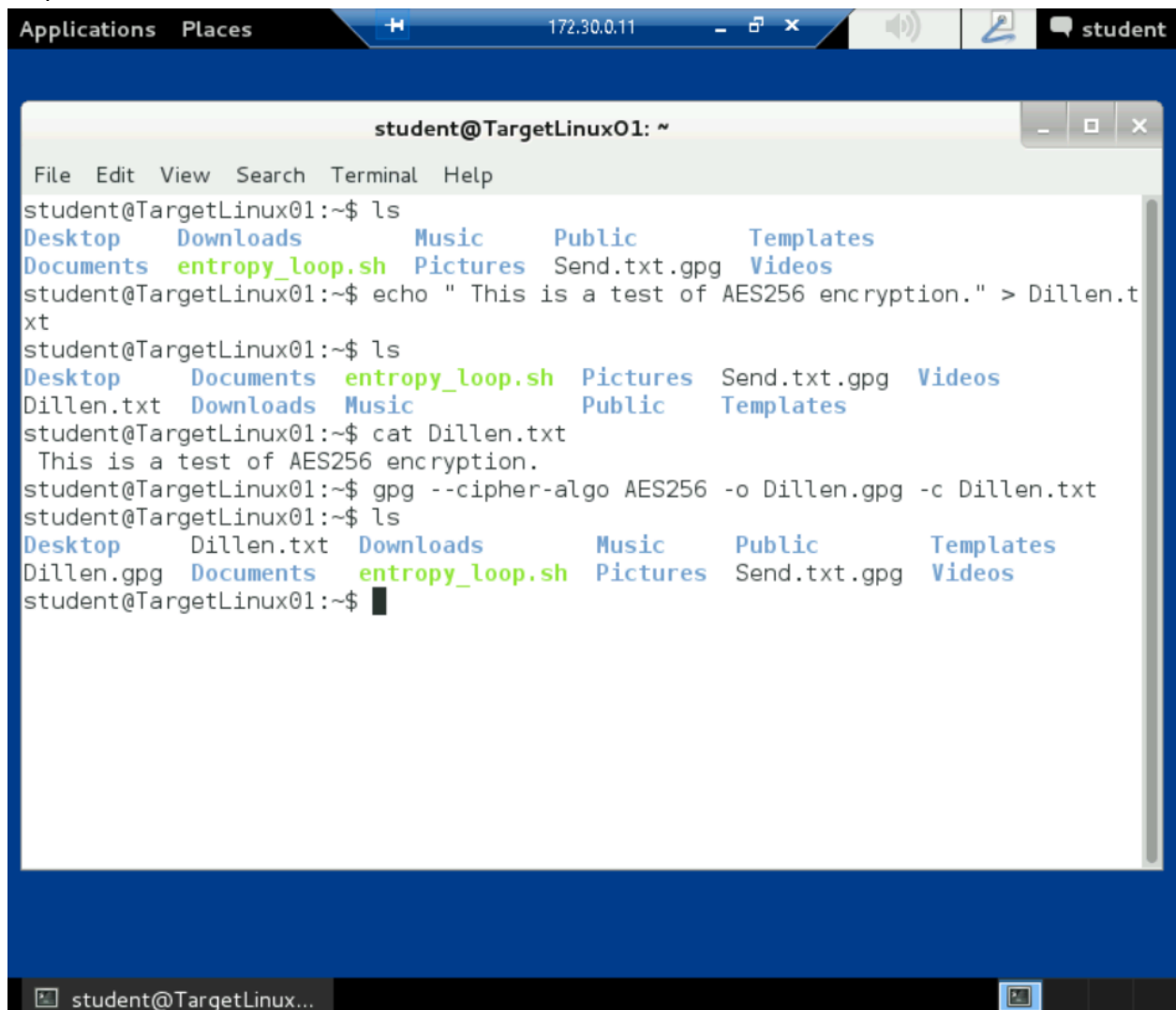


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window has a title bar that reads "student@TargetLinux01: ~". The terminal content shows the following commands and output:

```
student@TargetLinux01:~$ ls
Desktop  Downloads  Music      Public      Templates
Documents entropy_loop.sh Pictures    Send.txt.gpg Videos
student@TargetLinux01:~$ echo " This is a test of AES256 encryption." > Dillen.txt
student@TargetLinux01:~$ ls
Desktop  Documents  entropy_loop.sh  Pictures  Send.txt.gpg  Videos
Dillen.txt Downloads  Music            Public    Templates
student@TargetLinux01:~$ cat Dillen.txt
 This is a test of AES256 encryption.
student@TargetLinux01:~$
```

The terminal window also has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The desktop background is blue, and the top panel shows "Applications", "Places", and system status icons including a network icon, a volume icon, and a user icon labeled "student". The bottom panel shows a taskbar with a terminal icon and a label "student@TargetLinux...".

Step b.



The screenshot shows a Linux terminal window titled "student@TargetLinux01: ~". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the following sequence of commands and results:

```
student@TargetLinux01:~$ ls
Desktop  Downloads  Music      Public      Templates
Documents entropy_loop.sh Pictures  Send.txt.gpg Videos
student@TargetLinux01:~$ echo " This is a test of AES256 encryption." > Dillen.txt
student@TargetLinux01:~$ ls
Desktop  Documents  entropy_loop.sh  Pictures  Send.txt.gpg  Videos
Dillen.txt  Downloads  Music            Public      Templates
student@TargetLinux01:~$ cat Dillen.txt
 This is a test of AES256 encryption.
student@TargetLinux01:~$ gpg --cipher-algo AES256 -o Dillen.gpg -c Dillen.txt
student@TargetLinux01:~$ ls
Desktop  Dillen.txt  Downloads  Music      Public      Templates
Dillen.gpg  Documents  entropy_loop.sh  Pictures  Send.txt.gpg  Videos
student@TargetLinux01:~$
```

The terminal window is part of a desktop environment with a top bar showing "Applications", "Places", and system status (172.30.0.11, volume, network, and a "student" user icon). The bottom bar shows the terminal's title bar and a taskbar with icons for the terminal and other applications.

student@TargetLinux01: ~

File Edit View Search Terminal Help

student@TargetLinux01:~\$ ls

Desktop	Dillen.txt	Downloads	Music	Public	Templates
Dillen.gpg	Documents	entropy_loop.sh	Pictures	Send.txt.gpg	Videos

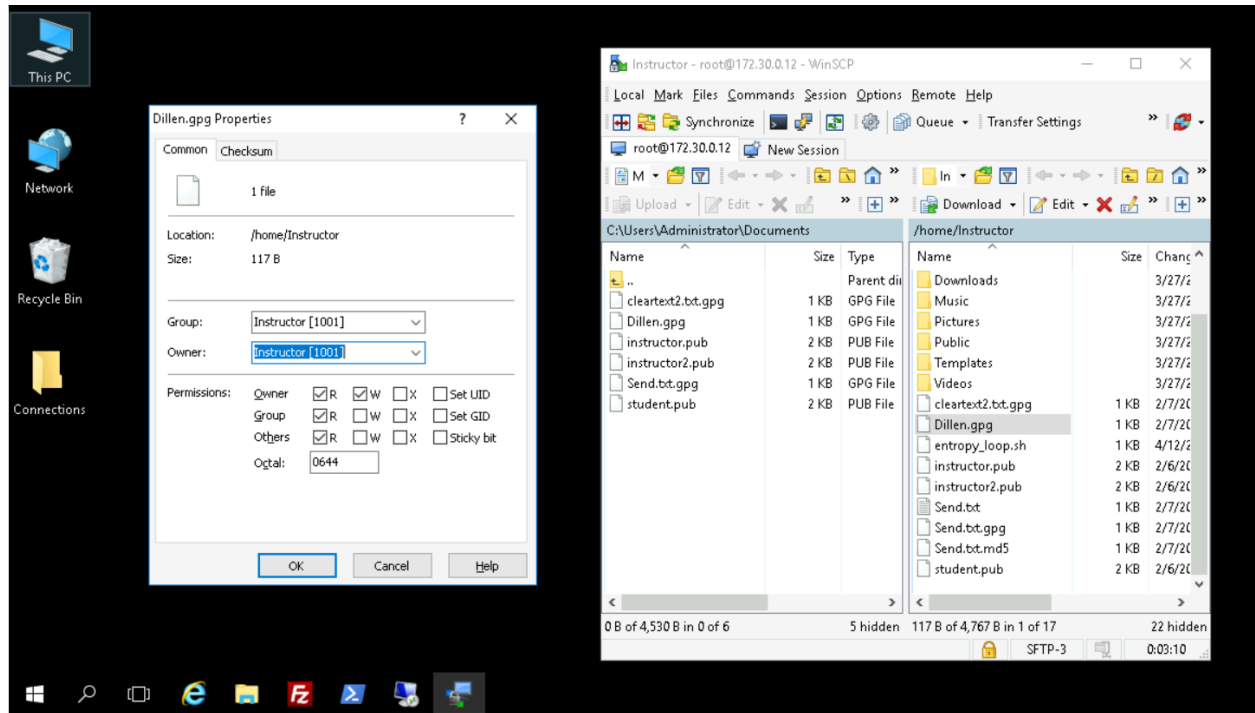
student@TargetLinux01:~\$ rm Dillen.txt

student@TargetLinux01:~\$ ls

Desktop	Documents	entropy_loop.sh	Pictures	Send.txt.gpg	Videos
Dillen.gpg	Downloads	Music	Public	Templates	

student@TargetLinux01:~\$

Step c.



```
Applications Places 172.30.0.12 - Instructor
Instructor@TargetLinux02: ~
File Edit View Search Terminal Help
Instructor@TargetLinux02:~$ ls
cleartext2.txt.gpg Downloads Music Send.txt.gpg Videos
Desktop entropy_loop.sh Pictures Send.txt.md5
Dillen.gpg instructor2.pub Public student.pub
Documents instructor.pub Send.txt Templates
Instructor@TargetLinux02:~$ gpg -o Dillen.txt -d Dillen.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
Instructor@TargetLinux02:~$ ls
cleartext2.txt.gpg Documents instructor.pub Send.txt Templates
Desktop Downloads Music Send.txt.gpg Videos
Dillen.gpg entropy_loop.sh Pictures Send.txt.md5
Dillen.txt instructor2.pub Public student.pub
Instructor@TargetLinux02:~$ cat Dillen.txt
This is a test of AES256 encryption.
Instructor@TargetLinux02:~$
```