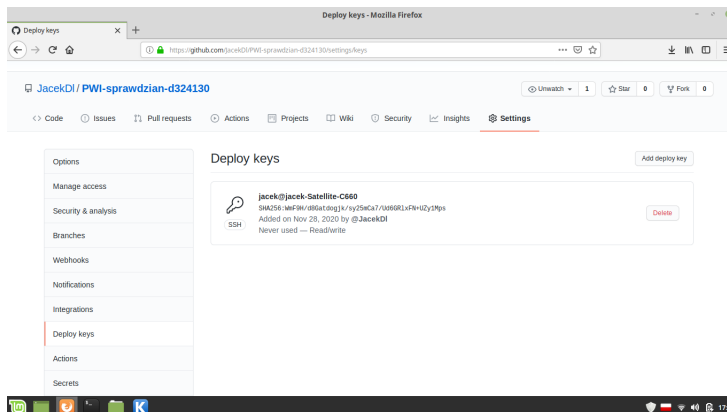


-i identityfile Use only the key(s) contained in identityfile (rather than looking for identities via ssh-add(1) or in the defaultIDfile)[1]

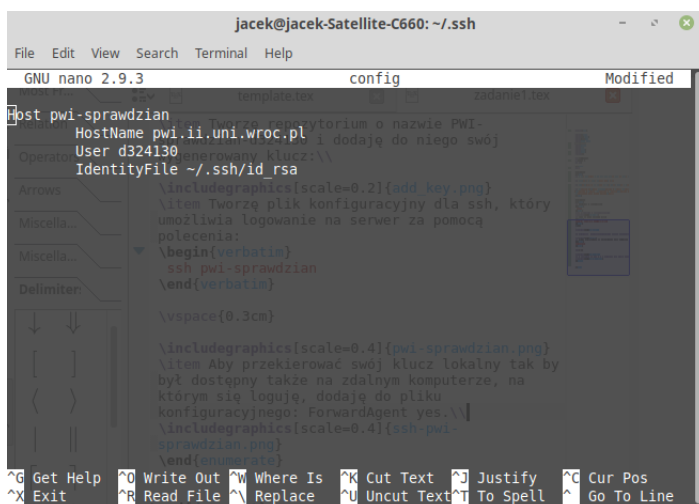
```
jacek@jacek-Satellite-C660: ~  
File Edit View Search Terminal Help  
jacek@jacek-Satellite-C660:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub d324130@pwi.ii.uni.  
i.wroc.pl  
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/jacek/.ssh/  
id_rsa.pub"  
The authenticity of host 'pwi.ii.uni.wroc.pl (156.17.4.60)' can't be established  
ECDSA key fingerprint is SHA256:t7wSHC5+lr0zhY/Hir13kkYXCWIGaC5K1NMQLibxY4c.  
Are you sure you want to continue connecting (yes/no)? y  
Please type 'yes' or 'no': yes  
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter  
out any that are already installed  
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt  
ed now it is to install the new keys  
d324130@pwi.ii.uni.wroc.pl's password:  
Number of key(s) added: 1  
Now try logging into the machine, with: "ssh 'd324130@pwi.ii.uni.wroc.pl'"  
and check to make sure that only the key(s) you wanted were added.  
jacek@jacek-Satellite-C660:~$
```

3. Tworzę repozytorium o nazwie PWI-sprawdzian-d324130 i dodaję do niego swój wygenerowany klucz:



4. Tworzę plik konfiguracyjny dla ssh, który umożliwia logowanie na serwer za pomocą polecenia:

ssh pwi-sprawdzian



```
d324130@pwi: ~  
File Edit View Search Terminal Help  
jacek@jacek-Satellite-C660:~$ ssh pwi-sprawdzian  
Linux pwi 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Sun Nov 29 17:22:55 2020 from 78.9.4.245  
d324130@pwi:~$
```

5. Aby przekierować swój klucz lokalny tak by był dostępny także na zdalnym komputerze, na którym się loguję, dodaję do pliku konfiguracyjnego: ForwardAgent yes[2]

```
jacek@jacek-Satellite-C660: ~/.ssh  
File Edit View Search Terminal Help  
GNU nano 2.9.3 config  
Host pwi-sprawdzian  
  HostName pwi.ii.uni.wroc.pl  
  User d324130  
  IdentityFile ~/.ssh/id_rsa  
  ForwardAgent yes  
  
[ Read 5 lines ]  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^G Cur Pos  
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Rozwiązanie polegające na wygenerowaniu kolejnego klucza jest 'brzydkie', ponieważ tworzy również klucz prywatny, który pozostaje na zdalnym komputerze.

Zadanie 3

1. Loguję się na pwi.ii.uni.wroc.pl. Klonuję repozytorium z GitHuba poleceniem:

```
git clone git@github.com:JacekDl/PWI-sprawdzian-d324130.git
```

```
d324130@pwi: ~  
File Edit View Search Terminal Help  
jacek@jacek-Satellite-C660:~/ssh$ ssh pwi-sprawdzian  
Linux pwi 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Sun Nov 29 17:30:25 2020 from 78.9.4.245  
d324130@pwi:~$ git clone git@github.com:JacekDL/PWI-sprawdzian-d324130.git  
Cloning into 'PWI-sprawdzian-d324130'...  
The authenticity of host 'github.com (140.82.121.3)' can't be established.  
RSA key fingerprint is SHA256:nThbg6kXUpJWGL7E1IGOCspRomTxdCARLviKw6E5SY8.  
Are you sure you want to continue connecting (yes/no)? y  
Please type 'yes' or 'no': yes  
Warning: Permanently added 'github.com,140.82.121.3' (RSA) to the list of known  
hosts.  
remote: Enumerating objects: 3, done.  
remote: Counting objects: 100% (3/3), done.  
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0  
Receiving objects: 100% (3/3), done.  
d324130@pwi:~$
```

2. Pobieram poleceniem wget plik ze strony:

```
wget http://www.ii.uni.wroc.pl/~lisu/zadanie.tar.gz
```

Następnie wypakowuję ten plik w repozytorium:

```
tar -xf zadanie.tar.gz
```

-x wyodrębnia pliki

-f określa nazwę pliku archiwum tar[3]

```
d324130@pwi: ~/PWI-sprawdzian-d324130  
File Edit View Search Terminal Help  
d324130@pwi:~$ ls  
PWI-sprawdzian-d324130  template.tex  zadanie1.tex  
d324130@pwi:~$ cd PWI-sprawdzian-d324130/  
d324130@pwi:~/PWI-sprawdzian-d324130$ ls  
README.md  zadanie.tar.gz  
d324130@pwi:~/PWI-sprawdzian-d324130$ tar -x zadanie.tar.gz  
tar: Refusing to read archive contents from terminal (missing -f option?)  
tar: Error is not recoverable: exiting now  
d324130@pwi:~/PWI-sprawdzian-d324130$ tar -xf zadanie.tar.gz  
d324130@pwi:~/PWI-sprawdzian-d324130$ ls  
README.md  zadanie  zadanie.tar.gz  ssh-copy-id  rsa.pub  
d324130@pwi:~/PWI-sprawdzian-d324130$
```

I komituję zmiany:

```
git add .  
git commit -m "Dodano pliki z archiwum tar"
```

3. Wyliczam funkcję skrótu MD5 ze stringa d324130 poleceniem:

```
echo -n "d324130" | md5sum
```

-n nie dolicza znaku nowej linii na końcu napisu podanego jako argument[4]

```
d324130@pwi: ~
File Edit View Search Terminal Help
d324130@pwi:~$ echo -n "d324130" | md5sum
7eccfe492d21bf21d0f8e788aba5d7bd
d324130@pwi:~$ \begin{verbatim}
git clone git@github.com:Jacek01/PWI-
sprawdzian-d324130.git
\end{verbatim}
\includegraphics[scale=0.4]{gitclone.png}
\item Pobieram poleceniem wget plik ze strony:
\begin{verbatim}
wget http://www.ii.uni.wroc.pl/~lisu/
zadanie.tar.gz
\end{verbatim}
Następnie wypakowuję ten plik w repozytorium:
\begin{verbatim}
tar -xzf zadanie.tar.gz
\end{verbatim}
-x wyodrębnia pliki\\
-f określa nazwę pliku archiwum tar\\
\includegraphics[scale=0.4]{tar.png}
I komituję zmiany:
\end{enumerate}
```

Odnajduję w gąszczu pobranych folderów katalog:

```
find -name "7eccfe492d21bf21d0f8e788aba5d7bd"
```

```
d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Help
5294a893bf7f394081aee670dbb07864 bc44cf067c774918f1f0172b9b3a82e3
581ed6549131526fd6e89368e7ffd081 c8646ec970158541b21d64a805faldb5
5ec2424ff3ca9087bb6f43ef9c7a065d d089ca5020f5ffd91db572d7092c7dda
62084588c149c62b82a33b02fbaafc94 d753127100ac9d12c51b6c6b94e8a452
6305d57f8c9a598f6a271c5e5de2022c e8db5f9da18b0611a01ca55be900fd70
671434f9e489641418ec491b874abd1c f2c7dd88657a1e28db388ea50242c08f
6a8385ce85cbf636fc07c0d8bd55a503 fdb733f327f602436a44f2994e30ccd7
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ man find
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ man find
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ find -name ^C
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ find -name 7eccfe492d21bf21d0f8e78
8aba5d7bd
./b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3
033c650c1c8450d77df2/7eccfe492d21bf21d0f8e788aba5d7bd
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie$ cd ./b07ad8e0d38ce8c8d112f9c7cb4ab
4a8/29b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d
21bf21d0f8e788aba5d7bd
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ ls
users.db zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$
```

Następnie wykonuję polecenia z zadania:

a) Sprawdzam jaki jest procentowy stosunek użytkowników z Polski do wszystkich którym wykradziono hasła:

```
grep -c "Country" users.db
grep -c "Country = POLAND" users.db
```

I wykorzystuję pythona do obliczeń:

```

d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Tabs Help

d324130@pwi: ~/PWI-sprawdzian-d324130... x jacek@jacek-Satellite-C660: ~/pwi/lista03 x

users.db zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ grep -c "Country" users.db
23460
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ grep -c "Country = POLAND" users.db
326
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ 326*100/23460
-bash: 326*100/23460: No such file or directory
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ python3
Python 3.7.3 (default, Jul 25 2020, 13:03:44)
(GCC 8.3.0) on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 326*100/23460
1.3895993179880648
>>>

```

Wynik $\approx 1,39\%$

b) Tworzę nowy plik passwords.txt do którego zapisuję tylko hasła z users.db poleceniami:

```

touch passwords.txt
sed 's/.*://' users.db > passwords.txt
sed -i 's/|.*//' passwords.txt

```

-i działa w miejscu - modyfikuje plik podany w komendzie[5]

```

d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Help

d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ ls
passwords.txt users.db zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ sed 's/.*://' users.db > passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ ls
passwords.txt users.db zadanie.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ nano passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ sed -i 's/|.*//' passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$ nano passwords.txt
d324130@pwi:~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7cb4ab4a8/29
b4d3b995d7c583da5ab1f785c2b922/cb7e926993d3033c650c1c8450d77df2/7eccfe492d21bf21
d0f8e788aba5d7bd$

```

W wyniku czego otrzymuję plik zawierający tylko hasła:

```

d324130@pwi: ~/PWI-sprawdzian-d324130/zadanie/b07ad8e0d38ce8c8d112f9c7...
File Edit View Search Terminal Help

GNU nano 3.2 passwords.txt
ann4584657
3030steff
bloempot
lry75smm
ColaHummel
qwertyuiop
something
lan880831
sanglier
Nicefish27
de29do18
adam2002
ADinarte5
Ju041978
Monica189087
goku77@goku77
Totempole33
peartree15

add_key.png config.png find.png gitclone.png
ssh-keygen.png ssh-keygen2.png ssh-pwi-sprawdzian.png tar.png
zadanie1.log zadanie1.pdf zadanie1.tex
Read 23465 lines
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^G Cur Pos
^X Exit ^R Read File ^E Replace ^U Uncut Text ^T To Spell ^I Go To Line

```

Zadanie 4

Kompiluję dwukrotnie plik zadanie1.tex, w wyniku czego otrzymuję plik zadanie1.pdf:

```
pdflatex zadanie1.tex
```

Kopiuję ostateczną wersję sprawozdania na zdalne repozytorium[6]:

```
scp zadanie1.pdf zadanie1.tex d324130@pwi.ii.uni.wroc.pl:~
```

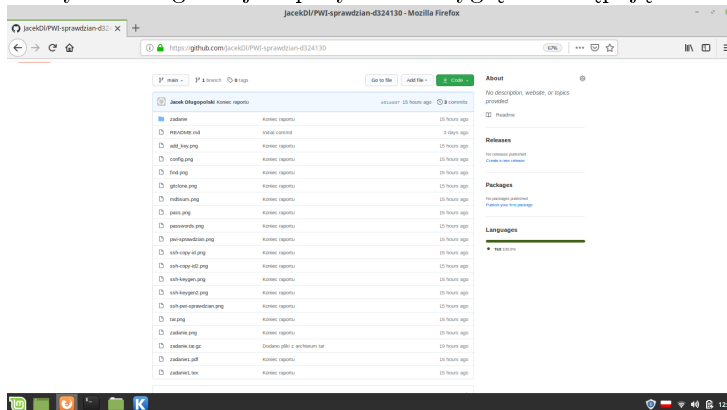
W podobny sposób przenoszę pliki .png.
Następnie komituję komendą:

```
git commit -m "Ostatnia wersja"
```

I robię pusha na GitHuba:

```
git push -u origin main
```

W wyniku czego moje repozytorium wygląda następująco:



(z wyjątkiem nazwy ostatniego komita)

Literatura

- [1] man ssh-copy-id
- [2] www.cloudsavvit.com/25/what-is-ssh-agent-forwarding-and-how-do-you-use-it/
- [3] www.linux.pl/man/index.php?command=tar
- [4] www.bytefreaks.net/gnulinux/creating-an-md5-hash-of-a-string-in-bash
- [5] www.geeksforgeeks.org/sed-command-in-linux-unix-with-examples
- [6] www.haydenjames.io/linux-securely-copy-files-using-scp/