CprE 308
Section 3
Lab9

Sean Gordon
Sgordon4

December 10, 2019

These labs focused on decoding sections of the FAT filesystem, giving a deeper understanding of the setup of different headers. The example file image provides a realistic example, with the printed results helping to cement ideas.

I had never done any work with filesystems before, and was suprised with how smoothly these labs went. For some reason I got super stuck on printing out the root directory sizes though, which took a fair amount of time to fix. Other than that, I feel like this was a successful foray into filesystems and their headers.

3.1.1 Logging in to a remote server:

a)
```
ssh linuxremote1.engineering.iastate.edu
```

```
The authenticity of host 'linuxremote1.engineering.iastate.edu (10.24.107.153)'
can't be established.
ECDSA key fingerprint is SHA256:hnVVIySw1epHGl6DDP0n5VuWJdQGpyspwbJ/MgoXBSI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'linuxremote1.engineering.iastate.edu,10.24.107.153'
(ECDSA) to the list of known hosts.
sean@linuxremote1.engineering.iastate.edu's password:
```

Output is coming from the remote machine.

b)
```
ssh -l sgordon4 linuxremote1.engineering.iastate.edu
```

c)
```
ssh sgordon4@linuxremote1.engineering.iastate.edu
```

3.1.2 Secure file transfer:

a) scp sgordon4@linuxremote1.engineering.iastate.edu: /Desktop/CC.do /Desktop/

b) Idk

3.1.3 SSH escape sequences:

1) ~?
2) scp sgordon4@linuxremote1.engineering.iastate.edu: /Desktop/CC.do ~/Desktop/
3) fg

3.1.4 Known Hosts:

```
|1|Yp1Z/IK/qL6E4qZQGW2aGm93j8E=|TZ4sU2o/DIinOOmXzJ63cKnhbhk=
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBDDb/Bm+amWGwDcVQDw5NCgYx4uMkavihLzx+iKD4s88
bjUXp/gvzPWlVc+oEkCC8maJN/gQpp0C23/ObbGIsjk=
```

3.1.5 Cryptographic keys:

a) id_dsa contains the private key, while id_dsa.pub contains the public one.

b) The passphrase is used to encrypt local keys, preventing unauthorized users from accessing them. If the passphrase is lost you cannot recover it.

c) The passphrase is used to encrypt the private key. The other one shouldn't be encrypted because it is used publicly.