1) **“Good” text pdf (Include in canvas submission)**
   (15 points)

2) **“Bad” text pdf (Include in canvas submission)**
   (15 points)

3) **Screenshot of the hashes of the text PDFs colliding for SHA1 and differing with SHA512**
   (15points)

```
cpre331@desktop:~/sha1collider$ sha1sum out-Jacob_Boicken_Evil.pdf  out-Jacob_Boicken_Good.pdf
cc1d9c7525f2f120cddb7959d18db3ddbb38b0d8  out-Jacob_Boicken_Evil.pdf
cc1d9c7525f2f120cddb7959d18db3ddbb38b0d8  out-Jacob_Boicken_Good.pdf
cpre331@desktop:~/sha1collider$ sha512sum out-Jacob_Boicken_Evil.pdf  out-Jacob_Boicken_Good.pdf
ef4b811924b9bec0b290488e3e8d4efabc27d7b2a4a265f05db8944b7a27f6ee8765a34c9fa1b48df365102cd1475fb65c1d8647da3e0899c5d2b1a9b68672cc  out-Jacob_Boicken_Evil.pdf
92d2206ec07764557da0130892c65e26b040ffc62bbf310c601fc019ef0c51d6fe36546105cc695b3d1dcb7d88510ad2dde320bf3abab868ec7bf6840714fa4f  out-Jacob_Boicken_Good.pdf
cpre331@desktop:~/sha1collider$
```

```
cpre331@desktop:~/sha1collider$ sha1sum out-Jacob_Boicken_Evil.pdf  out-Jacob_Boicken_Good.pdf
cc1d9c7525f2f120cddb7959d18db3ddbb38b0d8  out-Jacob_Boicken_Evil.pdf
cc1d9c7525f2f120cddb7959d18db3ddbb38b0d8  out-Jacob_Boicken_Good.pdf
cpre331@desktop:~/sha1collider$ sha512sum out-Jacob_Boicken_Evil.pdf  out-Jacob_Boicken_Good.pdf
ef4b811924b9bec0b290488e3e8d4efabc27d7b2a4a265f05db8944b7a27f6ee8765a34c9fa1b48df365102cd1475fb65c1d8647da3e0899c5d2b1a9b68672cc
92d2206ec07764557da0130892c65e26b040ffc62bbf310c601fc019ef0c51d6fe36546105cc695b3d1dcb7d88510ad2dde320bf3abab868ec7bf6840714fa4f
cpre331@desktop:~/sha1collider$
```

4) **Image out-1.pdf (Include in canvas submission)**
   (15 points)

5) **Image out-2.pdf (Include in canvas submission)**
   (15 points)

6) **Screenshot of the hashes of the image PDFs colliding for SHA1 and differing with SHA512**
   (15 points)

```
cpre331@desktop:~/sha1collider$ sha1sum out-dog.pdf out-training.pdf
f71117fcbb08030665cd14c523eda50db02df441  out-dog.pdf
f71117fcbb08030665cd14c523eda50db02df441  out-training.pdf
cpre331@desktop:~/sha1collider$ sha512sum out-dog.pdf out-training.pdf
abd9fc07a1c47c0732efd9f80e9ee60ff404286faa0c5fc8fa433e25adef515f65b043bf5d6a40a5fb1653bb13470f0f76a38cad0193fa67a7d7d67e0b3a19e0  out-dog.pdf
79a6bc98eee56fd553cfea54e7594a1afb1e5ca02c20f11df0610c35dec96514e2d048f2684cde08ba4b0a2ff24977482a8e4f1e8f87a6d5c958ca50f6b89026  out-training.pdf
cpre331@desktop:~/sha1collider$
```

```
cpre331@desktop:~/sha1collider$ sha1sum out-dog.pdf out-training.pdf
f71117fcbb08030665cd14c523eda50db02df441  out-dog.pdf
f71117fcbb08030665cd14c523eda50db02df441  out-training.pdf
cpre331@desktop:~/sha1collider$ sha512sum out-dog.pdf out-training.pdf
abd9fc07a1c47c0732efd9f80e9ee60ff404286faa0c5fc8fa433e25adef515f65b043bf5d6a40a5fb1653bb13470f0f76a38cad0193fa67a7d7d67e0b3a19e0
79a6bc98eee56fd553cfea54e7594a1afb1e5ca02c20f11df0610c35dec96514e2d048f2684cde08ba4b0a2ff24977482a8e4f1e8f87a6d5c958ca50f6b89026
cpre331@desktop:~/sha1collider$
```

7) **Answer questions in part p**
    a. **How likely is this to be used to carry out an attack in the wild?** (10 points)

    So, now that you have created hash collisions for these two sets of files, how likely is this to be used to carry out an attack in the wild? Please give me a clear example of when it could be used in the wild or when it would not work in the wild to support your argument.

This very well could be used to create an attack. If some system is verifying executable or binary programs that can be run on a system via hashes and is using sha1 or weaker, then an attacker could develop a malicious version of that program and replace the legit one. The system wouldn't notice anything different and allow such a program to execute.

I think of the OS iso verification using hashes.

(I think there are also systems for embedded systems / Point of Sale devices that use something similar. It may be signed hashes of binary files being validated, so only gets past one part of it.)