The matching transactions are:

a. https://www.blockchain.com/explorer/addresses/btc/13MUZ1Qk36LqExdcSRDZCxNRP1pcz1b5mT and https://www.blockchain.com/explorer/addresses/btc/135g5Es7VXvbaAkwzguv7q7xaSSTifav5H
b. https://www.blockchain.com/explorer/addresses/btc/1BCaztysy2paguXjuC8c652vckNMks69ce and https://www.blockchain.com/explorer/addresses/btc/1KGhtebk4Nr2zZSn2NaFepeNF6KyjxpPJZ
c. https://www.blockchain.com/explorer/addresses/btc/1MTbp4bFftessrbTTpM5SC5Ap1iKaMHrM7 and https://www.blockchain.com/explorer/addresses/btc/1MVXpgczazLvbtS8Nfp9v3Qpj4d8pUNXQM
d. https://www.blockchain.com/explorer/addresses/btc/18RwKzXtL5YGvFwa9BHrPRvqXLkdYWsGfp and https://www.blockchain.com/explorer/addresses/btc/1GcZjZnfQUCs9L9RoAFLdd8YET2WQWrDAz

It was fairly easy to match up these transactions upon first glance of browsing the inputs and outputs because the monetary values ended up being very similar give or take a couple dollars which we can assume was the fee for using the mixer. As pictured in the diagram, we can see this in the first matched transaction above (a). The input is like Alice inputting a total of 0.05 BTC which consists of her amount plus fees, then we see the according output is slightly less at 0.04874 BTC which can only indicate this is her output minus the fees. Like we discussed in class these tumblers are not always privacy enhancing or anonymizing like people believe as I was able to quickly deanonymize these inputs/outputs.

Evaluation

• Did you find the homework easy, appropriately difficult, or too difficult?

- Somewhere between easy and appropriately difficult

• How many hours total (excluding breaks :)) were spent on the completion of this assignment?

- ~3 (some of it was just getting stuck on a failure to read directions properly haha, did not realize that I could not really test on Remix and thought I was doing something wrong until I realized the prompt said testing will have to be done on chain)

• Did you feel there was too much coding, the appropriate amount of coding, or not enough coding?

- Appropriate amount of coding for just getting familiar with solidity, could have been more but was a good introduction to the tools and language