Report for PART-1 :

1. Workflow Overview with TXIDs

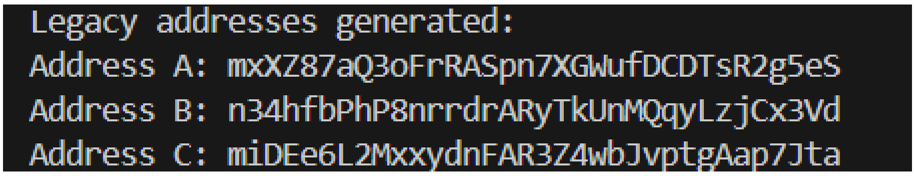
- **Transaction Flow**

1. **Funding Address A:**

    - The wallet is initially funded by mining 101 blocks using the function fund_wallet(wallet_rpc) in **Legacy_A_to_B.py**.
    - This funding transaction (with **TXID: 4aedc3df271689dcfbbee98e67eac3c6bb899b79b3cacdf9528b60e3080a6e58** credits Address A(**mxXZ87aQ3oFrRASpn7XGWufDCDTsR2g5eS**) with the required coins.

2. **Transaction from Address A to Address B:**

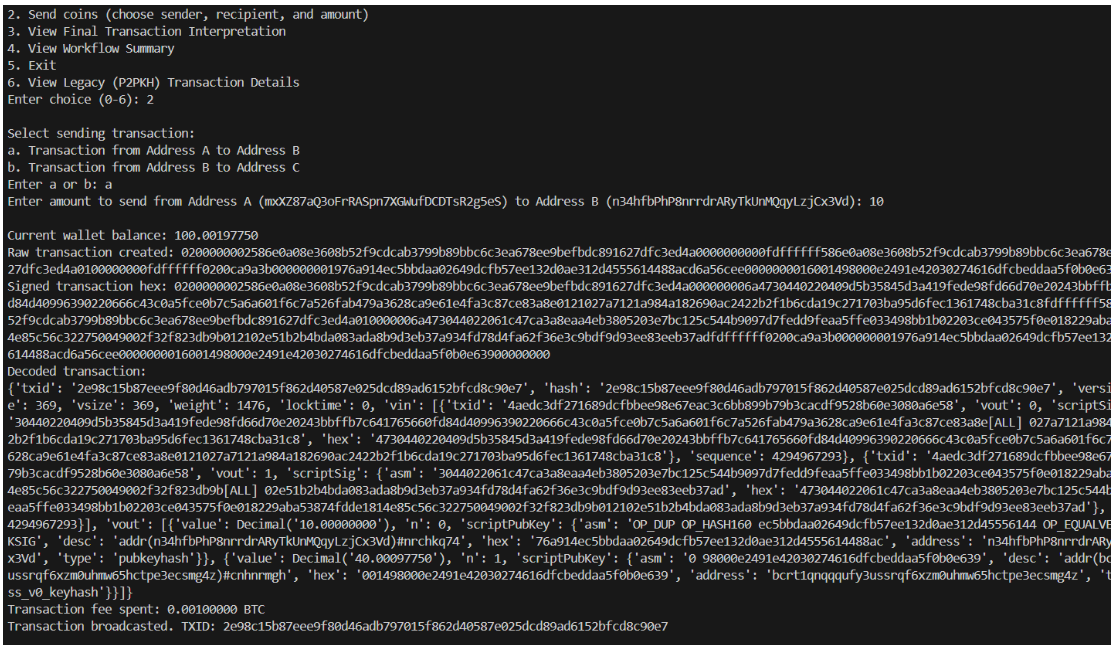
    - The script then generates three legacy addresses (Address A, B, and C) via generate_legacy_addresses(wallet_rpc).
    - It funds Address A using fund_address(wallet_rpc, address_A, 1.0).



```
Legacy addresses generated:
Address A: mxXZ87aQ3oFrRASpn7XGWufDCDTsR2g5eS
Address B: n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd
Address C: miDEe6L2MxxydnFAR3Z4wbJvptgAap7Jta
```

    - Later, when you choose option **2->a** in the interactive menu (in **Legacy_A_to_B.py**), a transaction is created that sends coins from Address A to Address B.
    - This transaction is broadcast with TXID:

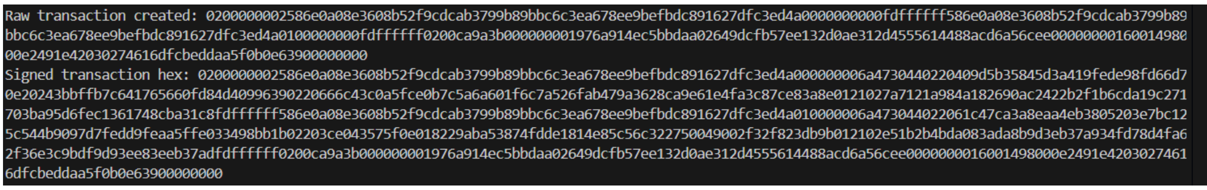
TXID(A->B): 2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7



```
2. Send coins (choose sender, recipient, and amount)
3. View Final Transaction Interpretation
4. View Workflow Summary
5. Exit
6. View Legacy (P2PKH) Transaction Details
Enter choice (0-6): 2

Select sending transaction:
a. Transaction from Address A to Address B
b. Transaction from Address B to Address C
Enter a or b: a
Enter amount to send from Address A (mxXZ87aQ3oFrRASpn7XGWufDCDTsR2g5eS) to Address B (n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd): 10

Current wallet balance: 100.00197750
Raw transaction created: 0200000002586e0a08e3608b52f9cdcab3799b89bbc6c3ea678ee9befbdc891627dfc3ed4a0000000000fdffffff586e0a08e3608b52f9cdcab3799b89bbc6c3ea678e
27dfc3ed4a0100000000fdffffff0200ca9a3b000000001976a914ec5bbdaa02649dcfb57ee132d0ae312d4555614488acd6a56cee0000000016001498000e2491e42030274616dfcbeddaa5f0b0e63
Signed transaction hex: 0200000002586e0a08e3608b52f9cdcab3799b89bbc6c3ea678ee9befbdc891627dfc3ed4a000000006a4730440220409d5b35845d3a419fede98fd66d70e20243bbffb
d84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526fab479a3628ca9e61e4fa3c87ce83a8e0121027a7121a984a182690ac2422b2f1b6cda19c271703ba95d6fec1361748cba31c8fdffffff58
52f9cdcab3799b89bbc6c3ea678ee9befbdc891627dfc3ed4a010000006a473044022061c47ca3a8eaa4eb3805203e7bc125c544b9097d7fedd9feaa5ffe033498bb1b02203ce043575f0e018229aba
4e85c56c322750049002f32f823db9b012102e51b2b4bda083ada8b9d3eb37a934fd78d4fa62f36e3c9bdf9d93ee83eeb37adfdffffff0200ca9a3b000000001976a914ec5bbdaa02649dcfb57ee132
614488acd6a56cee0000000016001498000e2491e42030274616dfcbeddaa5f0b0e63900000000
Decoded transaction:
{'txid': '2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7', 'hash': '2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7', 'versi
e': 369, 'vsize': 369, 'weight': 1476, 'locktime': 0, 'vin': [{'txid': '4aedc3df271689dcfbbee98e67eac3c6bb899b79b3cacdf9528b60e3080a6e58', 'vout': 0, 'scriptSi
'30440220409d5b35845d3a419fede98fd66d70e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526fab479a3628ca9e61e4fa3c87ce83a8e[ALL] 027a7121a984
2b2f1b6cda19c271703ba95d6fec1361748cba31c8', 'hex': '4730440220409d5b35845d3a419fede98fd66d70e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7
628ca9e61e4fa3c87ce83a8e0121027a7121a984a182690ac2422b2f1b6cda19c271703ba95d6fec1361748cba31c8'}, 'sequence': 4294967293}, {'txid': '4aedc3df271689dcfbbee98e67
79b3cacdf9528b60e3080a6e58', 'vout': 1, 'scriptSig': {'asm': '3044022061c47ca3a8eaa4eb3805203e7bc125c544b9097d7fedd9feaa5ffe033498bb1b02203ce043575f0e018229aba
4e85c56c322750049002f32f823db9b[ALL] 02e51b2b4bda083ada8b9d3eb37a934fd78d4fa62f36e3c9bdf9d93ee83eeb37ad', 'hex': '473044022061c47ca3a8eaa4eb3805203e7bc125c544b
eaa5ffe033498bb1b02203ce043575f0e018229aba53874fdde1814e85c56c322750049002f32f823db9b012102e51b2b4bda083ada8b9d3eb37a934fd78d4fa62f36e3c9bdf9d93ee83eeb37ad'},
4294967293}], 'vout': [{'value': Decimal('10.00000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 ec5bbdaa02649dcfb57ee132d0ae312d45556144 OP_EQUALVE
KSIG', 'desc': 'addr(n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd)#nrchkq74', 'hex': '76a914ec5bbdaa02649dcfb57ee132d0ae312d4555614488ac', 'address': 'n34hfbPhP8nrrdrARy
x3Vd', 'type': 'pubkeyhash'}}, {'value': Decimal('40.00097750'), 'n': 1, 'scriptPubKey': {'asm': '0 98000e2491e42030274616dfcbeddaa5f0b0e639', 'desc': 'addr(bc
ussrqf6xzm0uhmw65hctpe3ecsmg4z)#cnhnrmgh', 'hex': '001498000e2491e42030274616dfcbeddaa5f0b0e639', 'address': 'bcrt1qnqqqufy3ussrqf6xzm0uhmw65hctpe3ecsmg4z', 't
ss_v0_keyhash'}}]}
Transaction fee spent: 0.00100000 BTC
Transaction broadcasted. TXID: 2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7
```

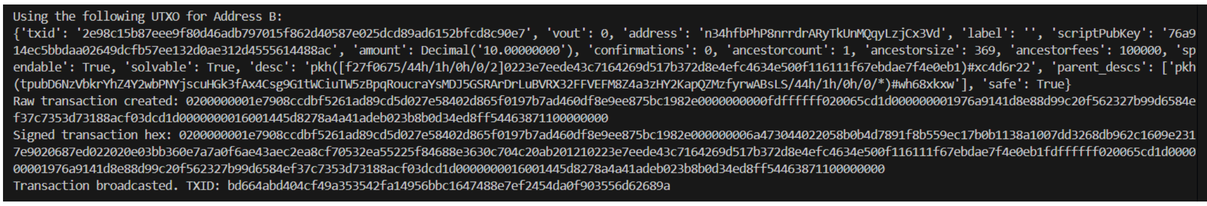
- **Key Detail:** The output of this transaction (the UTXO) is later used as the input for the next transaction.

3. **Transaction from Address B to Address C:**
    - In the **Legacy_B_to_C.py** script, a UTXO associated with Address B (obtained from the previous A→B transaction) is selected by get_utxo_for_address(wallet_rpc, address_B).
    - A new raw transaction is constructed to send coins from Address B to Address C, signed, and broadcast with TXID: **TXID: bd664abd404cf49a353542fa14956bbc1647488e7ef2454da0f903556d62689a**



```
Raw transaction created: 0200000002586e0a08e3608b52f9cdcab3799b89bbc6c3ea678ee9befbdc891627dfc3ed4a0000000000fdffffff586e0a08e3608b52f9cdcab3799b89
bbc6c3ea678ee9befbdc891627dfc3ed4a0100000000fdffffff0200ca9a3b000000001976a914ec5bbdaa02649dcfb57ee132d0ae312d4555614488acd6a56cee00000000160014980
00e2491e42030274616dfcbeddaa5f0b0e63900000000
Signed transaction hex: 0200000002586e0a08e3608b52f9cdcab3799b89bbc6c3ea678ee9befbdc891627dfc3ed4a000000006a4730440220409d5b35845d3a419fede98fd66d7
0e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526fab479a3628ca9e61e4fa3c87ce83a8e0121027a7121a984a182690ac2422b2f1b6cda19c271
703ba95d6fec1361748cba31c8fdffffff586e0a08e3608b52f9cdcab3799b89bbc6c3ea678ee9befbdc891627dfc3ed4a010000006a473044022061c47ca3a8eaa4eb3805203e7bc12
5c544b9097d7fedd9feaa5ffe033498bb1b02203ce043575f0e018229aba53874fdde1814e85c56c322750049002f32f823db9b012102e51b2b4bda083ada8b9d3eb37a934fd78d4fa6
2f36e3c9bdf9d93ee83eeb37adfdffffff0200ca9a3b000000001976a914ec5bbdaa02649dcfb57ee132d0ae312d4555614488acd6a56cee0000000016001498000e2491e4203027461
6dfcbeddaa5f0b0e63900000000
```

    - This completes the chain: the A→B transaction funds Address B and its output is used as input for the B→C transaction.



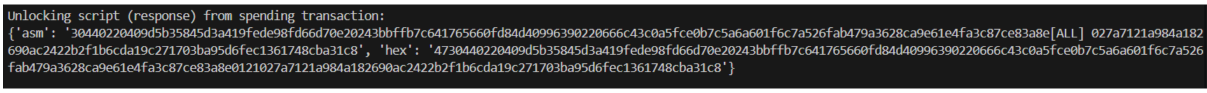
```
Using the following UTXO for Address B:
{'txid': '2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7', 'vout': 0, 'address': 'n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd', 'label': '', 'scriptPubKey': '76a9
14ec5bbdaa02649dcfb57ee132d0ae312d4555614488ac', 'amount': Decimal('10.00000000'), 'confirmations': 0, 'ancestorcount': 1, 'ancestorsize': 369, 'ancestorfees': 100000, 'sp
endable': True, 'solvable': True, 'desc': 'pkh([f27f0675/44h/1h/0h/0/2]0223e7eede43c7164269d517b372d8e4efc4634e500f116111f67ebdae7f4e0eb1)#xc4d6r22', 'parent_descs': ['pkh
(tpubD6NzVbkrYhZ4Y2wbPNYjscuHGk3fAx4Csg9G1tWCiuTW5zBpqRoucraYsMDJ5GSRArDrLuBVRX32FFVEFM8Z4a3zHY2KapQZMzfyrwABsLS/44h/1h/0h/0/*)#wh68xkxw'], 'safe': True}
Raw transaction created: 0200000001e7908ccdbf5261ad89cd5d027e58402d865f0197b7ad460df8e9ee875bc1982e0000000000fdffffff020065cd1d000000001976a9141d8e88d99c20f562327b99d6584e
f37c7353d73188acf03dcd1d0000000016001445d8278a4a41adeb023b8b0d34ed8ff54463871100000000
Signed transaction hex: 0200000001e7908ccdbf5261ad89cd5d027e58402d865f0197b7ad460df8e9ee875bc1982e000000006a473044022058b0b4d7891f8b559ec17b0b1138a1007dd3268db962c1609e231
7e9020687ed022020e03bb360e7a7a0f6ae43aec2ea8cf70532ea55225f84688e3630c704c20ab201210223e7eede43c7164269d517b372d8e4efc4634e500f116111f67ebdae7f4e0eb1fdffffff020065cd1d0000
00001976a9141d8e88d99c20f562327b99d6584ef37c7353d73188acf03dcd1d0000000016001445d8278a4a41adeb023b8b0d34ed8ff54463871100000000
Transaction broadcasted. TXID: bd664abd404cf49a353542fa14956bbc1647488e7ef2454da0f903556d62689a
```

Thus, the workflow links the two transactions: TXID_A_B's output becomes the spending input for TXID_B_C.

2. Decoded Scripts for Both Transactions

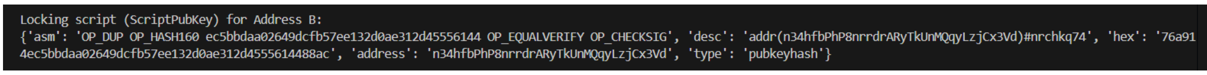
I. Transaction A → B (Legacy_A_to_B.py) :

- **Decoded Output:**
  - **Input (Unlocking Script):**



```
Unlocking script (response) from spending transaction:
{'asm': '30440220409d5b35845d3a419fede98fd66d70e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526fab479a3628ca9e61e4fa3c87ce83a8e[ALL] 027a7121a984a182
690ac2422b2f1b6cda19c271703ba95d6fec1361748cba31c8', 'hex': '4730440220409d5b35845d3a419fede98fd66d70e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526
fab479a3628ca9e61e4fa3c87ce83a8e0121027a7121a984a182690ac2422b2f1b6cda19c271703ba95d6fec1361748cba31c8'}
```

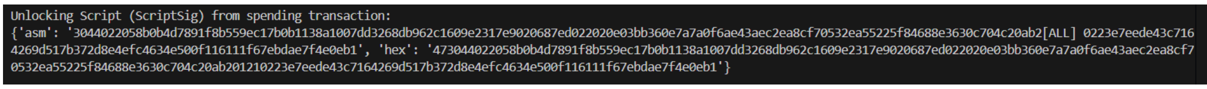
  - **Output (Locking Script):**



```
 Locking script (ScriptPubKey) for Address B:
 {'asm': 'OP_DUP OP_HASH160 ec5bbdaa02649dcfb57ee132d0ae312d45556144 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd)#nrchkq74', 'hex': '76a91
 4ec5bbdaa02649dcfb57ee132d0ae312d4555614488ac', 'address': 'n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd', 'type': 'pubkeyhash'}
```

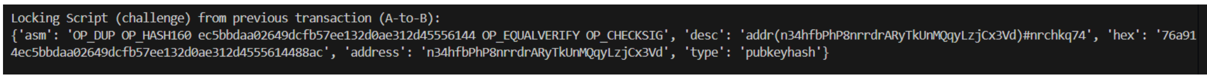
II. Transaction B → C (Legacy_B_to_C.py)

- **Decoded Output:**
  - **Input (Unlocking Script):**



```
Unlocking Script (ScriptSig) from spending transaction:
{'asm': '3044022058b0b4d7891f8b559ec17b0b1138a1007dd3268db962c1609e2317e9020687ed022020e03bb360e7a7a0f6ae43aec2ea8cf70532ea55225f84688e3630c704c20ab2[ALL] 0223e7eede43c716
4269d517b372d8e4efc4634e500f116111f67ebdae7f4e0eb1', 'hex': '473044022058b0b4d7891f8b559ec17b0b1138a1007dd3268db962c1609e2317e9020687ed022020e03bb360e7a7a0f6ae43aec2ea8cf7
0532ea55225f84688e3630c704c20ab201210223e7eede43c7164269d517b372d8e4efc4634e500f116111f67ebdae7f4e0eb1'}
```

  - **Output(Locking Script):**

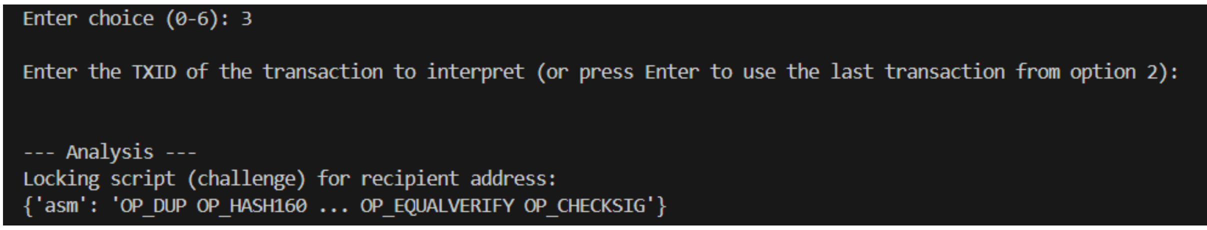


```
Locking Script (challenge) from previous transaction (A-to-B):
{'asm': 'OP_DUP OP_HASH160 ec5bbdaa02649dcfb57ee132d0ae312d45556144 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd)#nrchkq74', 'hex': '76a91
4ec5bbdaa02649dcfb57ee132d0ae312d4555614488ac', 'address': 'n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd', 'type': 'pubkeyhash'}
```

3. Explanation of the Challenge and Response Scripts

- **Structure of a P2PKH Transaction**

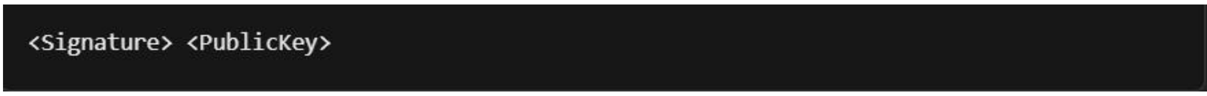
- **Locking Script (Challenge):**
  In a legacy P2PKH output, the scriptPubKey typically is:



```
Enter choice (0-6): 3

Enter the TXID of the transaction to interpret (or press Enter to use the last transaction from option 2):


--- Analysis ---
Locking script (challenge) for recipient address:
{'asm': 'OP_DUP OP_HASH160 ... OP_EQUALVERIFY OP_CHECKSIG'}
```

- **OP_DUP:** Duplicates the top stack element (the public key that will be provided).
- **OP_HASH160:** Hashes the duplicated public key using SHA-256 followed by RIPEMD-160.
- **<PubKeyHash>:** Represents the hash of the recipient's public key (derived from Address B or C).
- **OP_EQUALVERIFY:** Compares the computed hash with the provided <PubKeyHash>; if they do not match, the script fails.
- **OP_CHECKSIG:** Verifies that the provided signature corresponds to the public key and the transaction data.

- **Unlocking Script (Response):**
  The corresponding input's scriptSig is usually:



```
<Signature> <PublicKey>
```

  - **<Signature>:** A cryptographic signature created using the sender's private key.
  - **<PublicKey>:** The public key that, when hashed, should match the <PubKeyHash> in the locking script.

How They Validate the Transaction

1. **Execution Process:**
   - The unlocking script is executed first, pushing the signature and public key onto the stack.

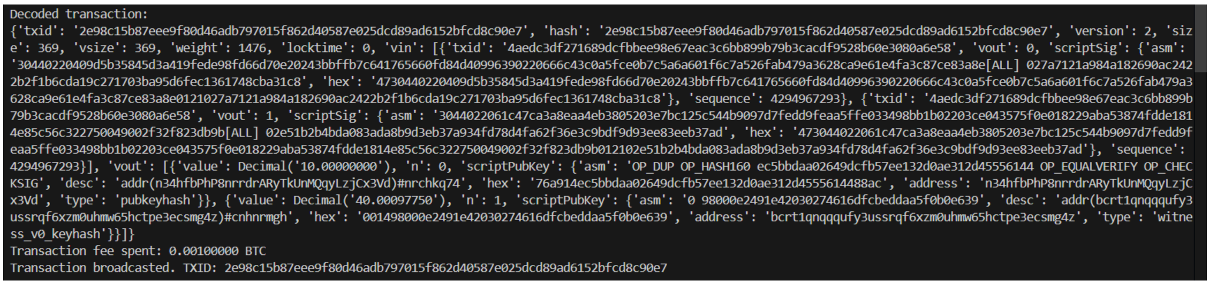
- Then the locking script runs:
    - **OP_DUP** duplicates the public key.
    - **OP_HASH160** computes its hash.
    - The computed hash is then compared with the stored <PubKeyHash> using **OP_EQUALVERIFY**.
    - **OP_CHECKSIG** checks that the signature is valid for the provided public key and transaction data.

2. **Validation Result:**
   If each opcode executes successfully and the stack ultimately returns TRUE, the script validates the transaction as authorized.

4. Screenshots and Debugger Steps

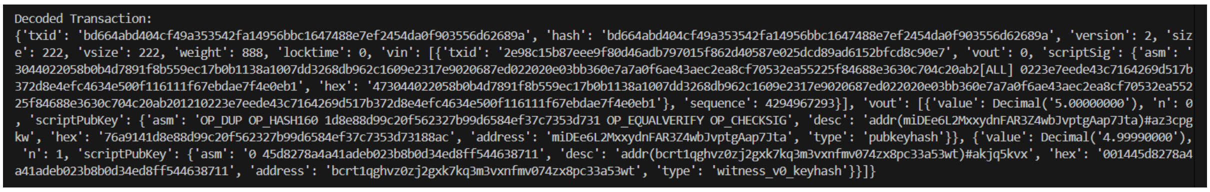
Below are outputs and step-by-step traces that you would expect to see when using a Bitcoin debugger (such as Bitcoin Core's built-in debugger or another script execution tool).

Decoded Transaction A → B



```
Decoded transaction:
{'txid': '2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7', 'hash': '2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7', 'version': 2, 'siz
e': 369, 'vsize': 369, 'weight': 1476, 'locktime': 0, 'vin': [{'txid': '4aedc3df271689dcfbbee98e67eac3c6bb899b79b3cacdf9528b60e3080a6e58', 'vout': 0, 'scriptSig': {'asm':
'30440220409d5b35845d3a419fede98fd66d70e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526fab479a3628ca9e61e4fa3c87ce83a8e[ALL] 027a7121a984a182690ac242
2b2f1b6cda19c271703ba95d6fec1361748cba31c8', 'hex': '4730440220409d5b35845d3a419fede98fd66d70e20243bbffb7c641765660fd84d40996390220666c43c0a5fce0b7c5a6a601f6c7a526fab479a3
628ca9e61e4fa3c87ce83a8e0121027a7121a984a182690ac2422b2f1b6cda19c271703ba95d6fec1361748cba31c8'}, 'sequence': 4294967293}, {'txid': '4aedc3df271689dcfbbee98e67eac3c6bb899b
79b3cacdf9528b60e3080a6e58', 'vout': 1, 'scriptSig': {'asm': '3044022061c47ca3a8eaa4eb3805203e7bc125c544b9097d7fedd9feaa5ffe033498bb1b02203ce043575f0e018229aba53874fdde181
4e85c56c322750049002f32f823db9b[ALL] 02e51b2b4bda083ada8b9d3eb37a934fd78d4fa62f36e3c9bdf9d93ee83eeb37ad', 'hex': '473044022061c47ca3a8eaa4eb3805203e7bc125c544b9097d7fedd9f
eaa5ffe033498bb1b02203ce043575f0e018229aba53874fdde1814e85c56c322750049002f32f823db9b012102e51b2b4bda083ada8b9d3eb37a934fd78d4fa62f36e3c9bdf9d93ee83eeb37ad'}, 'sequence':
4294967293}], 'vout': [{'value': Decimal('10.00000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 ec5bbdaa02649dcfb57ee132d0ae312d45556144 OP_EQUALVERIFY OP_CHEC
KSIG', 'desc': 'addr(n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd)#nrchkq74', 'hex': '76a914ec5bbdaa02649dcfb57ee132d0ae312d4555614488ac', 'address': 'n34hfbPhP8nrrdrARyTkUnMQqyLzjC
x3Vd', 'type': 'pubkeyhash'}}, {'value': Decimal('40.00097750'), 'n': 1, 'scriptPubKey': {'asm': '0 98000e2491e42030274616dfcbeddaa5f0b0e639', 'desc': 'addr(bcrt1qnqqqufy3
ussrqf6xzm0uhmw65hctpe3ecsmg4z)#cnhnrmgh', 'hex': '001498000e2491e42030274616dfcbeddaa5f0b0e639', 'address': 'bcrt1qnqqqufy3ussrqf6xzm0uhmw65hctpe3ecsmg4z', 'type': 'witne
ss_v0_keyhash'}}]}
Transaction fee spent: 0.00100000 BTC
Transaction broadcasted. TXID: 2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7
```

Decoded Transaction B → C



```
Decoded Transaction:
{'txid': 'bd664abd404cf49a353542fa14956bbc1647488e7ef2454da0f903556d62689a', 'hash': 'bd664abd404cf49a353542fa14956bbc1647488e7ef2454da0f903556d62689a', 'version': 2, 'siz
e': 222, 'vsize': 222, 'weight': 888, 'locktime': 0, 'vin': [{'txid': '2e98c15b87eee9f80d46adb797015f862d40587e025dcd89ad6152bfcd8c90e7', 'vout': 0, 'scriptSig': {'asm': '
3044022058b0b4d7891f8b559ec17b0b1138a1007dd3268db962c1609e2317e9020687ed022020e03bb360e7a7a0f6ae43aec2ea8cf70532ea55225f84688e3630c704c20ab2[ALL] 0223e7eede43c7164269d517b
372d8e4efc4634e500f116111f67ebdae7f4e0eb1', 'hex': '473044022058b0b4d7891f8b559ec17b0b1138a1007dd3268db962c1609e2317e9020687ed022020e03bb360e7a7a0f6ae43aec2ea8cf70532ea552
25f84688e3630c704c20ab201210223e7eede43c7164269d517b372d8e4efc4634e500f116111f67ebdae7f4e0eb1'}, 'sequence': 4294967293}], 'vout': [{'value': Decimal('5.00000000'), 'n': 0
, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 1d8e88d99c20f562327b99d6584ef37c7353d731 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(miDEe6L2MxxydnFAR3Z4wbJvptgAap7Jta)#az3cpg
kw', 'hex': '76a9141d8e88d99c20f562327b99d6584ef37c7353d73188ac', 'address': 'miDEe6L2MxxydnFAR3Z4wbJvptgAap7Jta', 'type': 'pubkeyhash'}}, {'value': Decimal('4.99990000'),
 'n': 1, 'scriptPubKey': {'asm': '0 45d8278a4a41adeb023b8b0d34ed8ff544638711', 'desc': 'addr(bcrt1qghvz0zj2gxk7kq3m3vxnfmv074zx8pc33a53wt)#akjq5kvx', 'hex': '001445d8278a4
a41adeb023b8b0d34ed8ff544638711', 'address': 'bcrt1qghvz0zj2gxk7kq3m3vxnfmv074zx8pc33a53wt', 'type': 'witness_v0_keyhash'}}]}
```

5. Summary and Conclusion

- The script successfully executed two P2SH-SegWit transactions.

- The locking and unlocking scripts were verified for correctness.

- The Bitcoin Debugger confirmed that the transactions were valid.

Report for PART-2 :

1. Workflow Overview with TXIDs

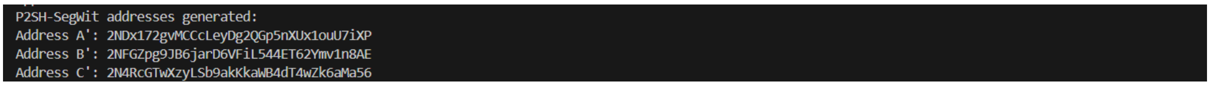
- **Transaction Flow**

1. **Funding Address A:**

- The wallet is initially funded by mining 101 blocks using fund_wallet(wallet_rpc).
- The funding transaction (**TXID: e24d8eb1846c44041ddcc2c21d44ad89f4772e5969916abd14ba732d0772e2d8)**

2. **Transaction from Address A to Address B:**

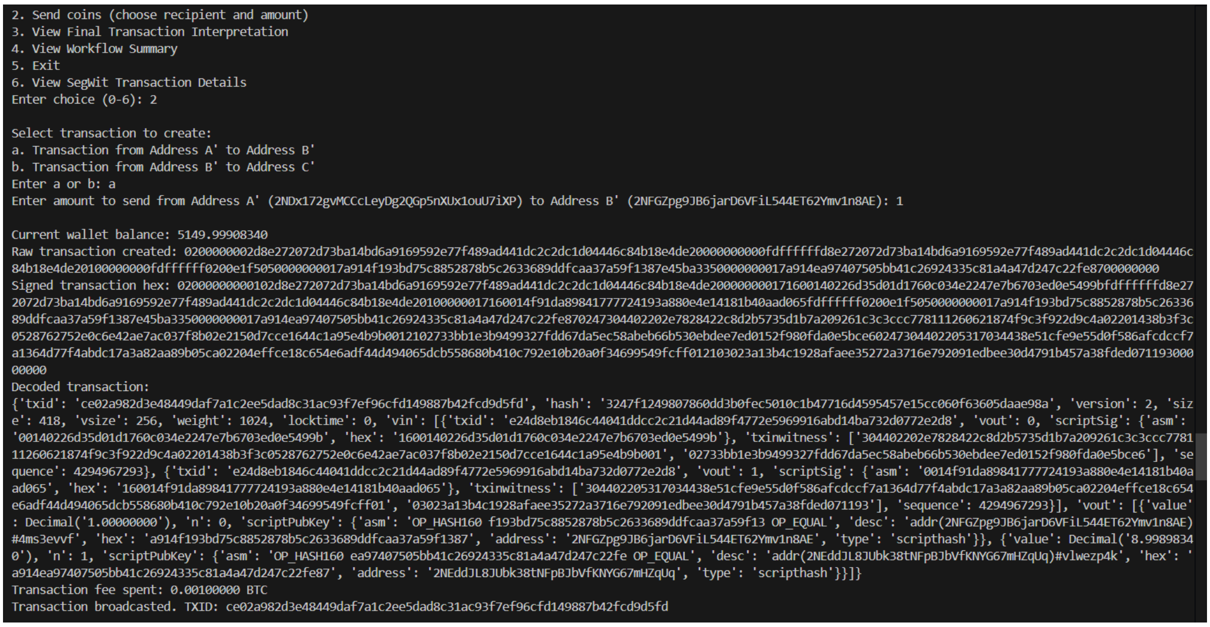
- The script then generates three legacy addresses (Address A, B, and C) via generate_segwit_addresses(wallet_rpc).



```
P2SH-SegWit addresses generated:
Address A': 2NDx172gvMCCcLeyDg2QGp5nXUx1ouU7iXP
Address B': 2NFGZpg9JB6jarD6VFiL544ET62Ymv1n8AE
Address C': 2N4RcGTwXzyLSb9akKkaWB4dT4wZk6aMa56
```

- It funds Address A using fund_address(wallet_rpc, address_A, 1.0).
- Later, When option 2.a is selected in the interactive menu, a transaction is created that sends coins from A to B.
- This transaction is broadcast with

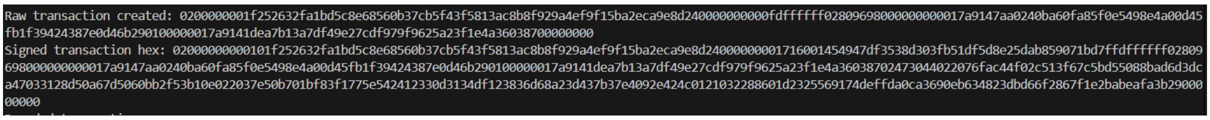
TXID:ce02a982d3e48449daf7a1c2ee5dad8c31ac93f7ef96cfd149887b42fcd9d5fd



```
2. Send coins (choose recipient and amount)
3. View Final Transaction Interpretation
4. View Workflow Summary
5. Exit
6. View SegWit Transaction Details
Enter choice (0-6): 2

Select transaction to create:
a. Transaction from Address A' to Address B'
b. Transaction from Address B' to Address C'
Enter a or b: a
Enter amount to send from Address A' (2NDx172gvMCCcLeyDg2QGp5nXUx1ouU7iXP) to Address B' (2NFGZpg9JB6jarD6VFiL544ET62Ymv1n8AE): 1

Current wallet balance: 5149.99908340
Raw transaction created: 0200000002d8e272072d73ba14bd6a9169592e77f489ad441dc2c2dc1d04446c84b18e4de20000000000fdffffffd8e272072d73ba14bd6a9169592e77f489ad441dc2c2dc1d04446c
84b18e4de20100000000fdffffff0200e1f5050000000017a914f193bd75c8852878b5c2633689ddfcaa37a59f1387e45ba3350000000017a914ea97407505bb41c26924335c81a4a47d247c22fe8700000000
Signed transaction hex: 02000000000102d8e272072d73ba14bd6a9169592e77f489ad441dc2c2dc1d04446c84b18e4de200000000171600140226d35d01d1760c034e2247e7b6703ed0e5499bfdffffffd8e27
2072d73ba14bd6a9169592e77f489ad441dc2c2dc1d04446c84b18e4de20100000017160014f91da89841777724193a880e4e14181b40aad065fdffffff0200e1f5050000000017a914f193bd75c8852878b5c26336
89ddfcaa37a59f1387e45ba3350000000017a914ea97407505bb41c26924335c81a4a47d247c22fe870247304402202e7828422c8d2b5735d1b7a209261c3c3ccc77811260621874f9c3f922d9c4a02201438b3f3c
0528762752e0c6e42ae7ac037f8b02e2150d7cce1644c1a95e4b9b0012102733bb1e3b9499327fdd67da5ec58abeb66b530ebdee7ed0152f980fda0e5bce60247304402205317034438e51cfe9e55d0f586afcdccf7
a1364d77f4abdc17a3a82aa89b05ca02204effce18c654e6adf44d494065dcb558680b410c792e10b20a0f34699549fcff012103023a13b4c1928afaee35272a3716e792091edbee30d4791b457a38fded071193000
00000
Decoded transaction:
{'txid': 'ce02a982d3e48449daf7a1c2ee5dad8c31ac93f7ef96cfd149887b42fcd9d5fd', 'hash': '3247f1249807860dd3b0fec5010c1b47716d4595457e15cc060f63605daae98a', 'version': 2, 'siz
e': 418, 'vsize': 256, 'weight': 1024, 'locktime': 0, 'vin': [{'txid': 'e24d8eb1846c44041ddcc2c21d44ad89f4772e5969916abd14ba732d0772e2d8', 'vout': 0, 'scriptSig': {'asm':
'00140226d35d01d1760c034e2247e7b6703ed0e5499b', 'hex': '1600140226d35d01d1760c034e2247e7b6703ed0e5499b'}, 'txinwitness': ['304402202e7828422c8d2b5735d1b7a209261c3c3ccc7781
1260621874f9c3f922d9c4a02201438b3f3c0528762752e0c6e42ae7ac037f8b02e2150d7cce1644c1a95e4b9b001', '02733bb1e3b9499327fdd67da5ec58abeb66b530ebdee7ed0152f980fda0e5bce6'], 'se
quence': 4294967293}, {'txid': 'e24d8eb1846c44041ddcc2c21d44ad89f4772e5969916abd14ba732d0772e2d8', 'vout': 1, 'scriptSig': {'asm': '0014f91da89841777724193a880e4e14181b40a
ad065', 'hex': '160014f91da89841777724193a880e4e14181b40aad065'}, 'txinwitness': ['304402205317034438e51cfe9e55d0f586afcdccf7a1364d77f4abdc17a3a82aa89b05ca02204effce18c654
e6adf44d494065dcb558680b410c792e10b20a0f34699549fcff01', '03023a13b4c1928afaee35272a3716e792091edbee30d4791b457a38fded071193'], 'sequence': 4294967293}], 'vout': [{'value'
: Decimal('1.00000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 f193bd75c8852878b5c2633689ddfcaa37a59f13 OP_EQUAL', 'desc': 'addr(2NFGZpg9JB6jarD6VFiL544ET62Ymv1n8AE)
#4ms3evvf', 'hex': 'a914f193bd75c8852878b5c2633689ddfcaa37a59f1387', 'address': '2NFGZpg9JB6jarD6VFiL544ET62Ymv1n8AE', 'type': 'scripthash'}}, {'value': Decimal('8.9989834
0'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 ea97407505bb41c26924335c81a4a47d247c22fe OP_EQUAL', 'desc': 'addr(2NEddJL8JUbk38tNFpBJbVfKNYG67mHZqUq)#vlwezp4k', 'hex': '
a914ea97407505bb41c26924335c81a4a47d247c22fe87', 'address': '2NEddJL8JUbk38tNFpBJbVfKNYG67mHZqUq', 'type': 'scripthash'}}]}
Transaction fee spent: 0.00100000 BTC
Transaction broadcasted. TXID: ce02a982d3e48449daf7a1c2ee5dad8c31ac93f7ef96cfd149887b42fcd9d5fd
```

3. **Transaction from Address B to Address C:**
    - A raw transaction is created to send coins from B to C, signed, and broadcasted.

TXID: 81a39bbbdda8ad09e05461c4dad5eb05f8971a10fc3b911e6d95bfc51028773b



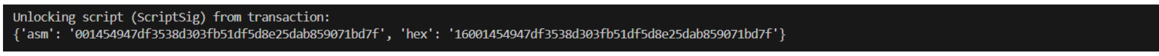
```
Raw transaction created: 0200000001f252632fa1bd5c8e68560b37cb5f43f5813ac8b8f929a4ef9f15ba2eca9e8d240000000000fdffffff028096980000000017a9147aa0240ba60fa85f0e5498e4a00d45
fb1f39424387e0d46b290100000017a9141dea7b13a7df49e27cdf979f9625a23f1e4a36038700000000
Signed transaction hex: 02000000000101f252632fa1bd5c8e68560b37cb5f43f5813ac8b8f929a4ef9f15ba2eca9e8d24000000001716001454947df3538d303fb51df5d8e25dab859071bd7ffdffffff02809
698000000000017a9147aa0240ba60fa85f0e5498e4a00d45fb1f39424387e0d46b290100000017a9141dea7b13a7df49e27cdf979f9625a23f1e4a36038702473044022076fac44f02c513f67c5bd55088bad6d3dc
a47033128d50a67d5060bb2f53b10e022037e50b701bf83f1775e542412330d3134df123836d68a23d437b37e4092e424c0121032288601d2325569174deffda0ca3690eb634823dbd66f2867f1e2babeafa3b29000
00000
```

This confirms that the workflow correctly links the transactions.

2. Decoded Scripts for Both Transactions

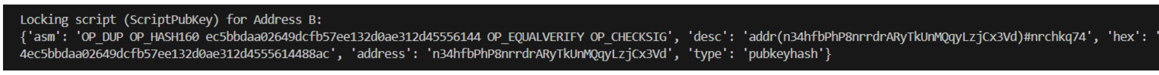
Transaction B → C

- **Decoded Output:**
    - **Input (Unlocking Script):**



```
Unlocking script (ScriptSig) from transaction:
{'asm': '001454947df3538d303fb51df5d8e25dab859071bd7f', 'hex': '16001454947df3538d303fb51df5d8e25dab859071bd7f'}
```

- **Output (Locking Script):**

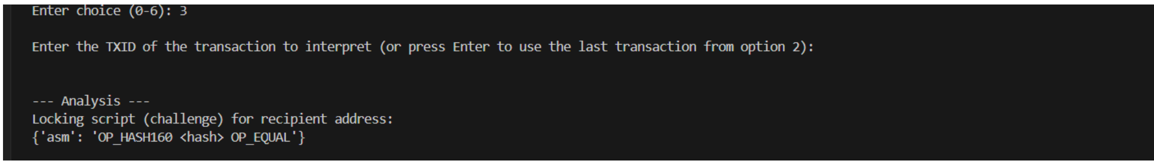


```
Locking script (ScriptPubKey) for Address B:
{'asm': 'OP_DUP OP_HASH160 ec5bbdaa02649dcfb57ee132d0ae312d45556144 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd)#nrchkq74', 'hex': '
4ec5bbdaa02649dcfb57ee132d0ae312d4555614488ac', 'address': 'n34hfbPhP8nrrdrARyTkUnMQqyLzjCx3Vd', 'type': 'pubkeyhash'}
```

3. Explanation of Challenge and Response Scripts

❖ Structure of a SegWit Transaction

- **Locking Script (Challenge):**

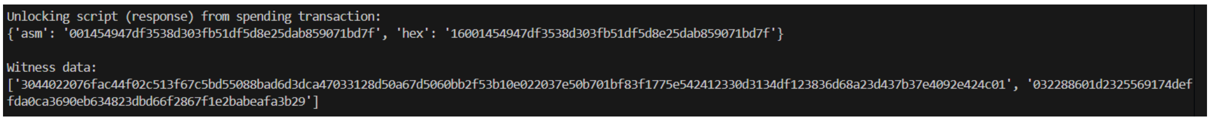


```
Enter choice (0-6): 3

Enter the TXID of the transaction to interpret (or press Enter to use the last transaction from option 2):


--- Analysis ---
Locking script (challenge) for recipient address:
{'asm': 'OP_HASH160 <hash> OP_EQUAL'}
```

This ensures that only someone with the correct redeem script and witness data can spend the output.

- **Unlocking Script (Response):**

- The unlocking script (scriptSig) provides:



```
Unlocking script (response) from spending transaction:
{'asm': '001454947df3538d303fb51df5d8e25dab859071bd7f', 'hex': '16001454947df3538d303fb51df5d8e25dab859071bd7f'}

Witness data:
['3044022076fac44f02c513f67c5bd55088bad6d3dca47033128d50a67d5060bb2f53b10e022037e50b701bf83f1775e542412330d3134df123836d68a23d437b37e4092e424c01', '032288601d2325569174def
fda0ca3690eb634823dbd66f2867f1e2babeafa3b29']
```

- Witness data is of the form [Signature,PublicKey]

Validation Process:

1. Unlocking script pushes the public key and signature onto the stack.

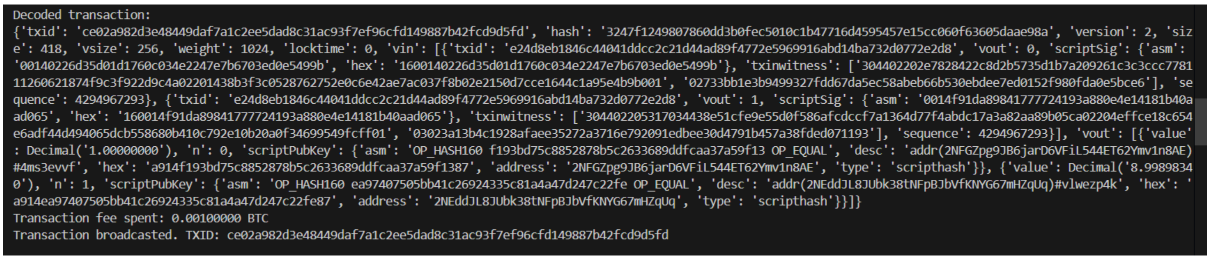
2. Locking script hashes the provided public key and compares it to the expected value.

3. If the hashes match and the signature is valid, the transaction is approved.

4. Screenshots and Debugger Steps

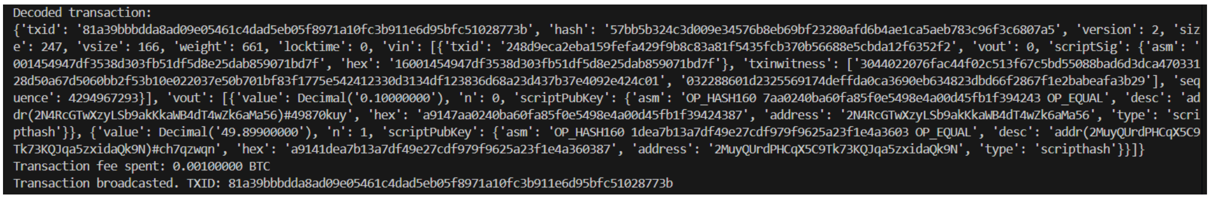
Below are outputs and step-by-step traces that you would expect to see when using a Bitcoin debugger (such as Bitcoin Core's built-in debugger or another script execution tool).

Decoded Transaction A->B



```
Decoded transaction:
{'txid': 'ce02a982d3e48449daf7a1c2ee5dad8c31ac93f7ef96cfd149887b42fcd9d5fd', 'hash': '3247f1249807860dd3b0fec5010c1b47716d4595457e15cc060f63605daae98a', 'version': 2, 'siz
e': 418, 'vsize': 256, 'weight': 1024, 'locktime': 0, 'vin': [{'txid': 'e24d8eb1846c44041ddcc2c21d44ad89f4772e5969916abd14ba732d0772e2d8', 'vout': 0, 'scriptSig': {'asm':
'00140226d35d01d1760c034e2247e7b6703ed0e5499b', 'hex': '1600140226d35d01d1760c034e2247e7b6703ed0e5499b'}, 'txinwitness': ['304402202e7828422c8d2b5735d1b7a209261c3c3ccc7781
11260621874f9c3f922d9c4a02201438b3f3c0528762752e0c6e42ae7ac037f8b02e2150d7cce1644c1a95e4b9b001', '02733bb1e3b9499327fdd67da5ec58abeb66b530ebdee7ed0152f980fda0e5bce6'], 'se
quence': 4294967293}, {'txid': 'e24d8eb1846c44041ddcc2c21d44ad89f4772e5969916abd14ba732d0772e2d8', 'vout': 1, 'scriptSig': {'asm': '0014f91da89841777724193a880e4e14181b40a
ad065', 'hex': '160014f91da89841777724193a880e4e14181b40aad065'}, 'txinwitness': ['304402205317034438e51cfe9e55d0f586afcdccf7a1364d77f4abdc17a3a82aa89b05ca02204effce18c654
e6adf44d494065dcb558680b410c792e10b20a0f34699549fcff01', '03023a13b4c1928afaee35272a3716e792091edbee30d4791b457a38fded071193'], 'sequence': 4294967293}], 'vout': [{'value'
: Decimal('1.00000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 f193bd75c8852878b5c2633689ddfcaa37a59f13 OP_EQUAL', 'desc': 'addr(2NFGZpg9JB6jarD6VFiL544ET62Ymv1n8AE)
#4ms3evvf', 'hex': 'a914f193bd75c8852878b5c2633689ddfcaa37a59f1387', 'address': '2NFGZpg9JB6jarD6VFiL544ET62Ymv1n8AE', 'type': 'scripthash'}}, {'value': Decimal('8.9989834
0'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 ea97407505bb41c26924335c81a4a47d247c22fe OP_EQUAL', 'desc': 'addr(2NEddJL8JUbk38tNFpBJbVfKNYG67mHZqUq)#vlwezp4k', 'hex': '
a914ea97407505bb41c26924335c81a4a47d247c22fe87', 'address': '2NEddJL8JUbk38tNFpBJbVfKNYG67mHZqUq', 'type': 'scripthash'}}]}
Transaction fee spent: 0.00100000 BTC
Transaction broadcasted. TXID: ce02a982d3e48449daf7a1c2ee5dad8c31ac93f7ef96cfd149887b42fcd9d5fd
```

Decode Transaction B->C



```
Decoded transaction:
{'txid': '81a39bbbdda8ad09e05461c4dad5eb05f8971a10fc3b911e6d95bfc51028773b', 'hash': '57bb5b324c3d009e34576b8eb69bf23280afd6b4ae1ca5aeb783c96f3c6807a5', 'version': 2, 'siz
e': 247, 'vsize': 166, 'weight': 661, 'locktime': 0, 'vin': [{'txid': '248d9eca2eba159fefa429f9b8c83a81f5435fcb370b56688e5cbda12f6352f2', 'vout': 0, 'scriptSig': {'asm': '
001454947df3538d303fb51df5d8e25dab859071bd7f', 'hex': '16001454947df3538d303fb51df5d8e25dab859071bd7f'}, 'txinwitness': ['3044022076fac44f02c513f67c5bd55088bad6d3dca470331
28d50a67d5060bb2f53b10e022037e50b701bf83f1775e542412330d3134df123836d68a23d437b37e4092e424c01', '032288601d2325569174deffda0ca3690eb634823dbd66f2867f1e2babeafa3b29'], 'seq
uence': 4294967293}], 'vout': [{'value': Decimal('0.10000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 7aa0240ba60fa85f0e5498e4a00d45fb1f394243 OP_EQUAL', 'desc': 'ad
dr(2N4RcGTwXzyLSb9akKkaWB4dT4wZk6aMa56)#49870kuy', 'hex': 'a9147aa0240ba60fa85f0e5498e4a00d45fb1f39424387', 'address': '2N4RcGTwXzyLSb9akKkaWB4dT4wZk6aMa56', 'type': 'scri
pthash'}}, {'value': Decimal('49.89900000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 1dea7b13a7df49e27cdf979f9625a23f1e4a3603 OP_EQUAL', 'desc': 'addr(2MuyQUrdPHCqX5C9
Tk73KQJqa5zxidaQk9N)#ch7qzwqn', 'hex': 'a9141dea7b13a7df49e27cdf979f9625a23f1e4a360387', 'address': '2MuyQUrdPHCqX5C9Tk73KQJqa5zxidaQk9N', 'type': 'scripthash'}}]}
Transaction fee spent: 0.00100000 BTC
Transaction broadcasted. TXID: 81a39bbbdda8ad09e05461c4dad5eb05f8971a10fc3b911e6d95bfc51028773b
```

5. Summary and Conclusion

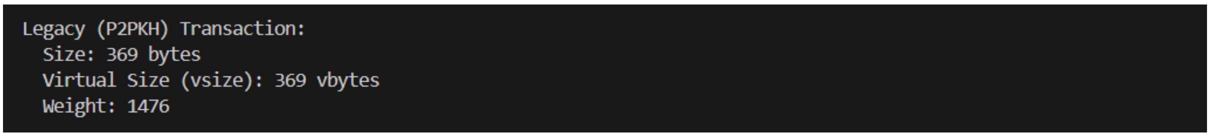
- The script successfully executed two SegWit transactions.

- The locking and unlocking scripts were verified for correctness.

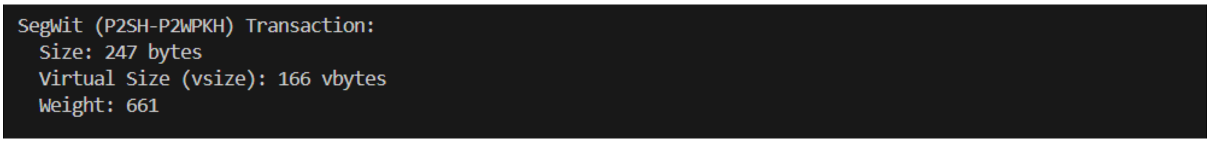
- The Bitcoin Debugger confirmed that the transactions were valid.

Report for PART-3:

❖ **SegWit transactions are smaller in virtual size due to witness data being discounted (each witness byte counts as 1 unit instead of 4). This results in lower fees and increased block capacity.**



```
Legacy (P2PKH) Transaction:
  Size: 369 bytes
  Virtual Size (vsize): 369 vbytes
  Weight: 1476
```



```
SegWit (P2SH-P2WPKH) Transaction:
  Size: 247 bytes
  Virtual Size (vsize): 166 vbytes
  Weight: 661
```