1. (a) I am investigating address 1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD.

   (b) The address was in use from July July 2nd 2014 to July 13th 2014.

   (c) There appear to have been 78 victims that paid bitcoin to this address.

   (d) The majority of the payments seem to be amounts close to $750 or $1000.

   (e) His change address seems to be: 1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV as each transaction sends change to this address. It also seems that their operational security was lacking as they used this address for many transactions. This address was also more likely than not used by someone low in the organization who was in charge of receiving money from the ransomists.

   (f) This address seems to differ in that there were a large volume of transactions made through this address. It also seems to differ in that the amount of $750 is nonstandard as opposed to the $500 usual amount.

2. (a) This allowed for analysis of the most recent addresses being used merchants in dark markets. If they didn't, they would have difficulty finding recent addresses to analyze.

   (b) Depending on the items they bought, there is the trivial implication that they may have bought illegal goods. If they did not, there is still the implicaation of inadvertedly helping to finance a criminal operation. As we learned in class, any transactions with a black market merchant would be financing a criminal enterprise. This only gets worse as the authors had explicit knowledge that they were black market merchants.

3. One can make a mult-sig transaction easy with the proper locking and unlocking script. The simplest way to do this would be to duplicate the standard pay-to-pubkey-hash by essentially having two copies of it in the locking script, one for the first address and one for the second address. As a result, only each public key and each signature is necessary for the unlocking script. Since each party can only generate their own signature, this guarantees that both parties agree. Also, since making the signature public does not actually reveal any secret informmation, this is a safe transaction. Each party would just need to agree on the entirety of the transaction then generate their signatures and then the outputs can be spent. Neither can change the transaction at this point without knowledge of the other either as this would require regenerating the signatures.

4. Many users now will only use an address once due to the popularity of HD wallets. As a result, this heuristic is not as strong because all of the public keys in the outputs have a fair chance to just be used for the first time. Since this heuristic relies on just one of the public keys being used for the first time (to determine the one-time change address), it will fail.

5. The anonymity set is of size 3.

6. The operation of using two forward addresses increases anonymity by quite a bit. This is because with two forward addresses you now need to check all possible sums of outputs to figure out to which addresses the coins now belong. In other words, you now know that a total of 5-6% + .001 (because two forwarding addresses) is distributed between two addresses. As a result, (assuming no time delay), one must then sum all possible pairs of outputs (that are less than the total being looked for) in order to find the anonymity set. This process is of $\Theta(n^2)$ complexity, where n it is the number of transactions in a block, because there are roughly n^2 possible pairs in that block.

7. These are the interesting receiving addresses for the first 8 suspect addresses:

12BSMxWi1jnKuAAPt3CvcgN9kywAJcakk9

————————————-

16KnVF5hQNrR3KZpnBqpZP96iCsWrUmEvP (MtGoxAndOthers)
124k8aHqRRA1xrT3cszwBXgMwRyDAr1eM1 (LocalBitcoins.com)
14eWJSsLdvWAaAvrzyAFg12iG5BpeLAmFk (LocalBitcoins.com)
1AGALRiJ7ngETX54H9AQe7b8SPN15oUFKs (LocalBitcoins.com)
1EEQnzjPZKf35ktuD8kX73wSPd3iS7zyR8 (LocalBitcoins.com)
1GR4Mk93KzMxEukxJkJhYkszJkJmpVmXcE (LocalBitcoins.com)
1Ge5Eiif3Wm68qMgLu7K5Hj3Ki8E1grgde (LocalBitcoins.com)
1GzZJcj5NYzDmVZXoQe5v4Kx33im1gTZvw (LocalBitcoins.com)
1J6Y2SkTfJmFq8bUwm9ivsy2H83iZG9Lkg (LocalBitcoins.com)
1KNnpVRKCe45xew3b4EZmb2TzPmD7B9kYN (LocalBitcoins.com)
1PYLNM5a6rWKY5uJ8WN2kcj9GAo7UcEaBc (SilkRoad2Market)
13PvfcPyE6v67sg64UfcACfWXz9ho5v6Vz (Cex.io)
158PAkokTP2cD2wKCGrjYZyEYEZsa9vDLp (Cex.io)
163PgZEpb7Q7ovUua3xzRAQXdHfs4QSy7P (Cex.io)
1836GjtpUUEpPn7W4kmEAtwL1ye7XURPzB (Cex.io)
19gRMbMrtm2tUAqNWHg7WhFsavEa6C4XZ2 (Cex.io)
1B5mRgB8eHSFJwQNvtZa7wGEjdMgmZW9ox (Cex.io)
1DpRjMXRoQJjrpE24f1JZ5Lkbm2jxR2S1H (Cex.io)
1JWsb9nK6z7sZ6VXC17uKCpZDpcEib5NaH (Cex.io)
1LPKPAs5y3yQJVL4GCVDnvci3NKbgrhEi5 (Cex.io)
1NWvXdR7VkLen9Mc5TvLczfUjpYwRQCish (Cex.io)
1PNfdAKFEX38ur8wD2FP63BBCcedBQyeR9 (Cex.io)

133GZ124H3fLdhwjCvPwXigQiSoracR3Ap

————————————-

1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1FUXg8M3FwyfQXDiLQnQFM3ixNrYgJvJ9m (SilkRoad2Market)
1GZfwRx9VMeRC3PsLbzmJdFcn61BV12m6c (AgoraMarket)
1KyQTChKVS2ad3ypoUJm5We3eomxUQ7KJT (LocalBitcoins.com)
1Mb9ctaMPXC5SvAaTaMWN27turkQoUSiVN (SilkRoad2Market)
1NCy4ijew8R7U6eSvjfxUy6bPgpbJ9yXw8 (LocalBitcoins.com)
1HLs4LKbVZhgCFtAXnJYiKDtLqUDZpEm4t (LocalBitcoins.com)

13BeAzA4mhwDYJEwhqNd2LsUnuhuVqKvw8

————————————-

1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1DdgPYbEqypHA2hbmaU1sNntthPeCH9kB2 (Betcoin.ag-old)
1Fi2mmT8j72TWkq6vu9wq2D7NqPGwn9cHK (LocalBitcoins.com)
1MdSNJFcJedtx56MF6g3TVBbB7j1wj8z5z (EvolutionMarket)

1BwFKRcTk3D7SznBAs5v6RFjZCV4gt7Q6j (CoinCafe.com)

13Kqgurx7eQg3G29NwV7ouJ8UHJRSUwwAe
——————————————-

1DTmn1TJXqjR3azLxm66Mvt8exyYpk2jis (BTC-e.com)
1Bj8sWTXdKg8LFJz8144NShPkxEtuQLGzb (VaultOfSatoshi.com)
1DTmn1TJXqjR3azLxm66Mvt8exyYpk2jis (BTC-e.com)

14bD9RgtJeKxdJMm5SRbmzFcsk8azTheR9
——————————————-

1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1FRtvFuwn736RmCfnroE3NmtWDR8jmjMZz (BTC-e.com-old)

14mRct4QZmqTcnErWGiLmbAAKpUjZ7fd8N
——————————————-

1Q96MDPwVEAUDek4hKYtXgRyTxyqdESWbA (MtGoxAndOthers)

14TCv5MKcyYCM3qij36x8xrKvKHHY1NXmq
——————————————-

16WNx8DbM2fGnKCHAif4Pqsm7oPwKyJEp1 (BTC-e.com)
1MAizeQjJLdVxiqMKWd7Q6qTEJheEzFZHQ (BTC-e.com)
1EMRphfqopNoSskhwTJvUvpcNtR8qTxiqi (LocalBitcoins.com)
1JVpD9JcgqoCHDwTPuXAYZWey9TGNkcK25 (LocalBitcoins.com)
1MjkcVUiAiVjdiQ9PivEipdK9TgLGjmYNs (LocalBitcoins.com)
1NHqswAAg4wWLiJixNzTcSdwF2xYfUuy6q (LocalBitcoins.com)
13s91j3nW14ZoiphA5QsGvkWJLCXs5obPm (LocalBitcoins.com)
17SVxLYLKyXaGF4M6MUsoCYtyF2oxtAe3m (LocalBitcoins.com)
1NQQsTVLNUUqSz36Bw1mx3tyf4jdyxS5mx (LocalBitcoins.com)

14ytdF3C9VRbttMfh9J56yR9ZWqfmFbBWN
——————————————-

1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)

8. These are all the repeated addresses:
16N3jvnF7UhRh74TMmtwxpLX6zPQKPbEbh
1QDXckhUmGVWn1u4ZstR4G4oKuXMJREtzC
1BwFKRcTk3D7SznBAs5v6RFjZCV4gt7Q6j
1M2hTJ96wWUhQJkiueuNMuVK8mhZR5qK2J
1HHzawQkvdUZfKxafbcsag9P38fbBxJCMf
1MZiE15dgxm4pWB8cWNXTj6RXXo7gEADgH
1JgT2UWr8Hmv9wqh5GyEeyDEYvAh1NLixS
1FRtvFuwn736RmCfnroE3NmtWDR8jmjMZz
12yj6kGQJFjzD17x7S5pfU4VqgF2e8mugu

1GpAaw1AboeN2x5HuBUR9A2S3z8HcfPVdG
1KnJsjfeKNcoLBL35WjvQffg5P81jYgeT3
1LkrYepmd4uUSFUzS2WzeZ5UwxE6siRuaX
18dwCxqqmya2ckWjCgTYReYyRL6dZF6pzL
19jFVCSRbhRPwqr4EnMQdLx2cHHra5htgr
15hePWL4CUxESNz1R7d9wvTieypzw9V56M
1HYDwtwtotSedCDCHDcgbRks2a7yPcicwd
1G541ENwQBqG3WZgvYtVCojVgdHFpJ8RXs
17eFLK9mS2AmAUN51be5rtAXUUkPUgkTeH
1L65L3UKmrzBPJ8DWcVCfGvUxCzEgtAABe
17b9YEqekrwYQUstDBDJuvyiWQWztauw3g
16avbtwiq9RwUrDDwBGcFRq3rxzJZGQs3E
12yYf7d1LDyTbngBRQx1mFX7zMV8hoYgmN
1GNpgCLNy4v4fWRJR1YeEJKZDjw3LeqgDU
13Kqgurx7eQg3G29NwV7ouJ8UHJRSUwwAe
1DTmn1TJXqjR3azLxm66Mvt8exyYpk2jis
18UbFf3K7L5dV65HxpRvspEpV6WhYYufne
1Q7VApg98W8mtAFdhJc7EPFCbHqcskLKAB
13zbyWuRSBskZMQFXYve7tTKLgmNzYXfZ6
1K81FeS3TH7DkqrMECtVDwXruRiXPXa6dZ
1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV
12iYaS1psNH97xVsdYDwZXZAiwSouJtXT3
1Prm9HxrkLcdSyopRDCLzUWJcmkCxQsrkB
1GfdxeXPweUQFJfExcGNLfTojE2oAGruYW
1AgKSAPYC687Sdf31hnuJKDAXQAKZfM2aa
18R1JX2pM4yS2baCERARHQEQg7uX1dezrp
13RhTuFDfAw874nfCHJqg1uPWbHugCRVX3
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa
1BcL7KKBrg1BbGdNQ5QkaaeJ8MFaVdF52h
1NkWhihzgGTuQbvzv5dm7t2BPYRP9pZik7
1Pa7ZkA9JHzwp8FazU4YBVSiYFPP3majgA
1CmWF4mYoaBWyQ8u3vDknrPHEFbYQBmuUK
1M7xviZRKpyHcmVRkqmKJwZVmcV5usRv1b
1EHmhGfxTA4xNRdtmCCADjAc1raAhoaCiX
1LPJ43XTMNRbuFn45obhnHkSsgSy1NyryH
1Q9B6g3cQ2qrYRNyYQbSrsRRmzQr7fMWQd
1S1gh7dmsqPCNe7weCeTwRvrsvB7Hgnbj
1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD
1J6Y2SkTfJmFq8bUwm9ivsy2H83iZG9Lkg

9. These are the addresses with the labels from walletexplorer added as well as sorting in ascending order:
12yYf7d1LDyTbngBRQx1mFX7zMV8hoYgmN
1Prm9HxrkLcdSyopRDCLzUWJcmkCxQsrkB
1K81FeS3TH7DkqrMECtVDwXruRiXPXa6dZ
1M7xviZRKpyHcmVRkqmKJwZVmcV5usRv1b

13RhTuFDfAw874nfCHJqg1uPWbHugCRVX3
17b9YEqekrwYQUstDBDJuvyiWQWztauw3g
1LkrYepmd4uUSFUzS2WzeZ5UwxE6siRuaX
1S1gh7dmsqPCNe7weCeTwRvrsvB7Hgnbj
1BcL7KKBrg1BbGdNQ5QkaaeJ8MFaVdF52h
1M2hTJ96wWUhQJkiueuNMuVK8mhZR5qK2J
1MZiE15dgxm4pWB8cWNXTj6RXXo7gEADgH
1GpAaw1AboeN2x5HuBUR9A2S3z8HcfPVdG
1GfdxeXPweUQFJfExcGNLfTojE2oAGruYW
15hePWL4CUxESNz1R7d9wvTieypzw9V56M
18dwCxqqmya2ckWjCgTYReYyRL6dZF6pzL
1NkWhihzgGTuQbvzv5dm7t2BPYRP9pZik7
12iYaS1psNH97xVsdYDwZXZAiwSouJtXT3 (MtGoxAndOthers)
1HHzawQkvdUZfKxafbcsag9P38fbBxJCMf (MtGoxAndOthers)
1Q7VApg98W8mtAFdhJc7EPFCbHqcskLKAB (MtGoxAndOthers)
19jFVCSRbhRPwqr4EnMQdLx2cHHra5htgr
1L65L3UKmrzBPJ8DWcVCfGvUxCzEgtAABe
18R1JX2pM4yS2baCERARHQEQg7uX1dezrp
1KnJsjfeKNcoLBL35WjvQffg5P81jYgeT3 (Coin.mx)
1QDXckhUmGVWn1u4ZstR4G4oKuXMJREtzC (MtGoxAndOthers)
12yj6kGQJFjzD17x7S5pfU4VqgF2e8mugu
18UbFf3K7L5dV65HxpRvspEpV6WhYYufne
1DTmn1TJXqjR3azLxm66Mvt8exyYpk2jis (BTC-e.com)
13Kqgurx7eQg3G29NwV7ouJ8UHJRSUwwAe
13zbyWuRSBskZMQFXYve7tTKLgmNzYXfZ6
1BwFKRcTk3D7SznBAs5v6RFjZCV4gt7Q6j (CoinCafe.com)
1JgT2UWr8Hmv9wqh5GyEeyDEYvAh1NLixS
17eFLK9mS2AmAUN51be5rtAXUUkPUgkTeH (MtGoxAndOthers)
1Pa7ZkA9JHzwp8FazU4YBVSiYFPP3majgA
1GNpgCLNy4v4fWRJR1YeEJKZDjw3LeqgDU
1EHmhGfxTA4xNRdtmCCADjAc1raAhoaCiX
1G541ENwQBqG3WZgvYtVCojVgdHFpJ8RXs
1CmWF4mYoaBWyQ8u3vDknrPHEFbYQBmuUK (BTC-e.com)
16avbtwiq9RwUrDDwBGcFRq3rxzJZGQs3E
1FRtvFuwn736RmCfnroE3NmtWDR8jmjMZz (BTC-e.com-old)
1LPJ43XTMNRbuFn45obhnHkSsgSy1NyryH
16N3jvnF7UhRh74TMmtwxpLX6zPQKPbEbh
1NkjXACtWM358virDfhbE8rZsWWgrkVhsa (BTC-e.com)
1J6Y2SkTfJmFq8bUwm9ivsy2H83iZG9Lkg (LocalBitcoins.com)
1HYDwtwtotSedCDCHDcgbRks2a7yPcicwd
1L7SLmazbbcy614zsDSLwz4bxz1nnJvDeV
1Q9B6g3cQ2qrYRNyYQbSrsRRmzQr7fMWQd
1CeA899xpo3Fe6DQwZwEkd6vQfRHoLuCJD
1AgKSAPYC687Sdf31hnuJKDAXQAKZfM2aa

10. I chose to analyze the 9 infamous bitcoin addresses.

Here is the code output from number 9:

```
1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v
1HVpyjYEPwQhvRQ3dL8tGe9kiydti616sX (SatoshiDice.com-original)
1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T
1EBHA1ckUWzNKN7BMfDwGTx6GKEbADUozX
1HDPXVhXLb445n54w5jcDXby9R4FGXPg5M
1L2JsXHPMYuAa9ugvHGLwkdstCPUDemNCf
1ECKhpehB1xvSKfNKmRfwfERnHLXpr5C4g
1GBwk2YJMDFqSVhTKygH8zUwV7jdoJhHHH (MtGoxAndOthers)
1M8s2S5bgAzSSzVTeL7zruvMPLvzSkEAuv
128RRjnuwyEWGGa2RDc8d9f2H55jyuSrfJ
112zKwLt2dJ6QaD1DVPfcWXNfZyodmNKBz
13fnb6d952DxtcKVsyHWXWo2SLwhqpeXf1
1DMB2X4jWSKp4DX1pRSWvcLbk4twGczSk2
1DMB2X6VwiwMtW2cdNVrftvTC6F23hDGLh
13fci5FCHhe62f5EbMJ9PFCV6YdFmUiXzX
112Pv7s2Jju3XqZp1KYRBAGNnDMDe9xwXa
113Vp8qBkn71yxVDwh9mCfyu88N9p3DGeY
13g5iEwjYxLUeLbEdnaHUN18zEw2grh68e
113XgEjoczwPd5QSPqdrYREYF9FT9LJmsU
113ucLNujusPPNdiTobbMcW5LzTwvaybbW
113T6qrLMF1bviCQogQnF2SqxtTjgSeHdx
1DMB2XAmk6LcCH1DcExZdT1VaUqQtmB8kJ
1DMB2XV7tRtpXv784RGyow6LuPSH2wF6h6
1DMB2XatANEkPeyeUsaCCKt3cEg4ybrbAC
1133yck69X4zzt1WqHWjeVibm67RBPYNm
13fhSUxix2GZnunEK8wpVwDAbRWqxtrCZk
112LHUhQQYLMYHiBx2BDHF4cbZ5dePrU5E
1DMB2XjtkaSJD35EM7zxkmBc8iXRPQyYHm
11433PPQfdmZ6GgHzvYw5WqGVFGxQzcU7Y
113eoJLCnbBQhc3VWRBXy2WWi7DVR9ubMr
113WUeZNaKqsP8Pue2UjDWxQZbCHYh9Mvv
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet
```