Note: I was completely unable to get Go to work in any capacity. These are the answers I was able to complete. I will be going to office hours for help, if it's possible to finish the rest later.

Problem 1:

a. Transaction ID: 795b2ce2d008c7fe89abda8867d8a6aa324f4c2c238d6bf176cb224b7f349084
b. .004501 BTC, or about $1.03
c. Output Total: 1,111.13927457 BTC
   Estimated Transaction Volume (actual exchange): 416.44003854 BTC
d. The transaction had 3 confirmations after about 24 minutes, 3 seconds. This is the time between the transaction (00:34:02 AM, later included in block 372136) and the completion of the third block in which the transaction was included (00:58:05 AM, block 372138).

Problem 2:

a. Student a: 1JHoF2bak7KCST3SzeR7e1AwqDm4tiLJjt
   Student b: 1D6qsGhZqrRSKegqWT3e8TPR8gGczTxMLu
   Student c: 1AcKeSkKponv5qeZuEHvkocELf1Uo4ggCE
b. The transaction to me was from 1Lh1ugXAX7dU8fEGF3Dvqnqxfxc1ELiSYK,
   From 1CwKxRY3zEMgWMtzWG1DUZkqe2VxFyLF6t,
   From 1KHPuDi2Ax6V64yReuDywU45LVZV7JFu38,
   From 19bynDhphEnbAmWuxzRv5MBgS3bSeAPL2V,
   From 189VnjXZAP2YHA4ZibmjH3857Je5jvhLxX,
   From 18Pzqj8HBHk7Hrw8iBFGhfw4gXp9RQtddD,
   From 1FEFqzSuK8S6gdmDea6yzmxq2BRJ1mbvz4,
   From 1BvjebynRqQH5gVZKh2LnmQJoBt1FV6ZnS,
   From 1Gedds2WEfCcEEMW8yoYQRKwvc8ZBjG4wx,
   From 1NpYM8Pa5xt26A4sLqcChMoEke9jATw4A5,
   From 1PoCpDGNMoCrNejwFw6K3g2mFJwdDQZx5p,
   From 14KnE3j9KJzwFtb1Nd3J5fAhrfwRZgGLEb,
   From 1Nh27qFYUaRfxHEKvDHTPFh4VFAm7JdBQb,
   From 1EF3EN78f5sBFUXz1D2yJsSQ2HgvQMdaDy,
   From 1QL6XqD3VNnfqnP53U5JuF81NWa2vQFpCN,
   From 1JySua5bPeunsYA1HaJRWBeZJ5sboLy1CG,
   From 1tpfzPAmem88VRvJAASnaGj9sawj8LNnj,
   From 1KAeSMKLcSG7CKj34bb8E18UH4zjC3PbM8,
   From 1PAyvggUiXLcQdj5gkHqx1sC1vW96p9FLT,
   From 19WmbY4nDcjAEv6wb5rcd5E6MutVMXBZzy,
   That address has more than 1 incoming transaction. By far most of the money incoming to that address came from 14J6ep326owXDpc1waViGJNB1onSFy9eou. I can follow the chains back, until the transactions involve of thousands of bitcoins. I couldn't figure out the owner of any of those addresses, though.
c. You can, by looking at what networks saw the transaction first. There's a handy map in Blockchain.info that points to that location.

Problem 3:

a. If the goal is not to get caught, I'll assume we can't just steal all the user's money once they receive a sufficiently large transaction. One method would be to, whenever receiving/sending a transaction, direct the transaction first to an address owned by the attacker before sending most of the money to the correct destination. I'm not sure how much you could take this way.

If the user is likely to notice getting less than requested, you could have the malicious wallet interface falsely display the expected amount to the user. Until they try to spend money they don't have (or look at their transactions in another interface), no one will notice a discrepancy.

b. I am fairly confident in the safety of my wallet. Most of this confidence comes from (A) the fact that there is a huge amount of money, and therefore businesses' trust, in this system, and (B) there is so little money in my wallet only a fool would bother to crack it.

   If I were going to store large amounts of money in my wallet, I would first find a more secure place to store my wallet words. Next, I might think about not accessing my wallet except over secure networks and from secure devices (so not, for example, my general use laptop, but instead a work-only system that is less likely to be compromised). Those last few measures seem marginal, but I don't see any glaring weaknesses in this system other than me, my wallet words, and my hardware.

Problem 4:

Just verify that the number is what it's supposed to be?
Hex number: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFC2F
That's 55 F's followed by EFFFFFC2F. The nth hex digit carries the place value of (2^4)^(n).
If the number were all F's, it would be 2^256 – 1. I checked this numerically (~1.15 * 10^77).
(E - F) = -1. 2^(4 * 8) = 2^32. -1 * 2 ^ 32 = - (2 ^ 32).
(C - F) = -3. 2^(4 * 2) = 2 ^ 8. -3 * 2 ^ 8 = - (2 ^ 9) - (2 ^ 8)
(2 - F) = -13. 2^(4 * 1) = 2^4. -13 * (2^4) = - (2 ^ 7) - (2 ^ 6) - (2 ^ 4).
So the number is 2^256 – 2^32 – 2^9 – 2^8 – 2^7 – 2^6 – 2^4 – 1.

Problem 5:

You need to trust that your computer has not been compromised, that your network has not been completely compromised (I think a man-in-the-middle type of attack would work here), that elliptic curve cryptography remains secure, that the makers of the btcd suite and/or you are not malicious (one method of attack is to give the user a target address you own), that Bitcoin itself is reliable as a currency… And you need to trust yourself to keep the wallet words safe. You also have to trust that it is actually hard to gain access to someone else's wallet, but that's implicit.