

Lab 8: To Catch a Hacker**Due: 11/11/09 in class**

The difference between data recovery and digital forensics is that the former is inadvertent and we know what we are looking for, while the latter is intentional/ hidden/ deleted/ encrypted and we need to look beyond the obvious.

In Computer and Network Forensics, there are 5 W's to consider: Why, Who What, When, Where. You will be given the 'why' and you must discover the other 4 using some of the security program/tools you have already created.

Objectives of the Lab:

to utilize some of the security programs/tools you have created so far in order to find a hacker (who dons either a black or white hat).

Step 1: Determining your group number

There are 10 groups (each with 1 to 2 students). I will give each group a sealed envelope with your group number and color – in code (Group n color). It will contain seemingly senseless letters and words. To ensure that you are legit, you must first figure out to which group you belong. **Hint: be sure to use a tool you have created in class.**

Group 1
Group 2
Group 3
Group 4
Group 5
Group 6
Group 7
Group 8
Group 9
Group 10

azure
blue
pink
white
navy
green
black
brown
red
yellow

Sample code contained in envelope:

1C 2F 10 B4 CB C7 B0 18 3D 9D 83 92 8D D1 2A 28

Step 2: Figure out the "Who"

Once you have figured out your group number, email it to me, along with the names of the members in your group.

Upon receiving your email, I will send you a personalized document, from which you must determine the name of your "culprit." In addition, there will be a message for you which will lead you to the next clue.

Step 3: Determining the “Where”

Your clue from Step 2, should lead you to someone who will hand you an envelope – but only after you give them the correct name of the “who”/ culprit from step 2. This should lead you to the ‘where’ – **be sure to use a tool you have created in class.**

Step 4: The letter in the envelope will direct you to the final step