The Trojan Defence
You Decide

[Ian] Kennedy:
So this is your opportunity now to play the part of the jury and decide whether the Trojan Defence works. Many of these cases concern indecent pictures of children. But we're now going to consider the fictitious case of 48 year old Fred who is charged with a horrific crime of searching for and downloading pictures of Mickey Mouse. What we need to think about is whether we can produce evidence, which proves two things. Can we prove the guilty act and the guilty mind? So let's head down to the computer lab.

Right, so we're standing outside this secure area of the Forensics Department and to gain access to this I need to use my fingerprint to gain access. So I'm going to put my card on the machine [beep] and that gives us access to the secure area. Okay, so what I have here is Fred's computer which has been seized and sealed whilst it was in Fred's house. So hopefully I can take it out of the bag. One of the next things I need to do as part of this process, which we call a physical examination, is simply to take some photographs [click click]. The next stage now is to physically open the computer and I can now look inside here, take some additional photographs, identify and remove the hard disc.

One of the first things I do is make a forensic image of the disc using special software which copies live and deleted date on the disc without changing the original. The virus scan of the copied disc reveals the presence of a virus, Coolgame.xe . More on that later.

Looking in the image as it's called I can see all of Fred's folders that he would normally see on his computer but because it's forensic software I can delve a little bit deeper than that and see things that he wouldn't normally see. Some of the first steps that I will perform at this stage will be to extract the date the Windows operating system was installed and various other basic details such as who it's registered to, that type of thing. This is to counter any defence where the suspect turns round and says "But it's not my computer."

Next, I need to see the pictures themselves. Going into gallery view of thumbnail pictures I can tick those that look suspicious.

So on one of these pictures I can see a picture of Mickey wearing a wizard's hat with his white gloves pointing into the sky at night with a rather devious look on his face. This is clearly illegal so I'm going to tick that and bookmark it for reference and in doing that I'm going to be clicking on the space bar. If it looks of interest or it could be potentially illegal I will create a shortlist which I will go through later to fine tune my selection. Now having got these pictures the next thing I need to do is to consider where they are located. So I'll change the view I'm looking at within Incase to a tabular view and in this table I can see a list of folders against the items I've ticked. I can see that a number of these pictures, in fact most of them, are in a folder called Temporary Internet Files. Usually this is an automated process where the pictures are copied there by the browser. However if I scroll down there are a number of pictures which I notice contain pictures of Mickey Mouse. These ones are located in the My Documents, My Pictures folder. Now these pictures, they're normally the result of a user's action to deliberately move them into that folder. So just returning for a moment to our two boxes that we created earlier, one showing the list of guilty act, the other one showing guilty intent. We so far have pictures located in temporary internet files which is a guilty act. We also have pictures in the My Documents which is another guilty act but the fact that the pictures were located in the My Documents is an indication that there was a guilty intent there.

I am able to corroborate that evidence by checking the registry area, a database which stores settings and logs activity. One of the things that it does is to record file names when certain types of file are saved such as pictures.

The registry area that shows us that files, picture files have been saved deliberately, there are five records of these entries which indicates that this action was performed not once but five times. So any defence of accidental saving of pictures is somewhat diluted by the fact that there are a number of these save actions recorded reasonably close together.

One of the other key areas to extract is all the records on the computer relating to internet history including what searches have been made on sites such as Google.

I'm looking at a table on the screen here which gives me a date and a time that that entry was recorded and it also tells me who was logged into the computer at the time the entry was made. I can see under the user's name all of the entries relate to Fred. I can also see another column which tells me the web page that was visited at that date and time. I can see references to Google and the word search?q= and what that tells us is that the text that follows the equals sign is the text that was typed into the search box of the Google website. In our case I can see q= Mickey space Mouse. So I can be fairly certain that on this particular date and time Fred who visited the Google web page and typed in Mickey Mouse into the search box. This entry is usually created as a result of a user's manual action. So the fact that it is here is a strong indication that it was entered by somebody logged into the computer as Fred. So again we have an additional item of guilty activity which is the internet history record and the fact that it relates to a Google keyword search means it's a guilty intent.

Now the defence Fred has given is that a Trojan infected his computer. In other words someone else gained access to his computer and performed these actions. Our virus scan earlier revealed the presence of malware. Now booting a virtual copy of Fred's computer we can run tools to examine the computer in a live state. For now we will remove a layer of protection called packing and look at what text is stored in the Coolgame.xe file.
I can see a website address that relates to a bank. Now I can see above that address in text some more text that looks unfamiliar to me because it looks foreign, it looks like a foreign language to me. So I've copied and pasted this text into Google Translate and I can see that the word excesso actually means account in Portuguese and I can see other words here that mean digits and electronic signature. So early indications are that this piece of malware could be some form of banking Trojan and in fact if I take this binary and I submit it to some online virus scanning websites they will indeed corroborate these findings and indicate that it's some form of banking Trojan, which doesn't fit with the behaviour that Fred was describing in terms of downloading pictures of Mickey Mouse. So, now looking at this list of evidence that we've produced, if we go back to our two streams that we identified earlier, the guilty act and the guilty mind. This is now your opportunity to decide for yourself as if you were the Jury, is Fred guilty or not?

Voice Over:
The Trojan Defence was presented by Ian Kennedy, who is studying a Phd in the use of statistic and dynamic analysis to study the impact of malware on a forensic computer investigation at The Open University. You can find out more about research and courses in computer forensics by going to www.mcs.open.ac.uk