The Trojan Defence
Fighting Back

[Ian] Kennedy:
The Trojan Defence has been particularly common in child pornography cases where a defendant claims that a virus has been responsible for the downloading of indecent images onto their computer. Both the prosecution and the defence need to hire expert witnesses, Computer Forensic Investigators, who can advise the court about whether there's any substance to that claim. Professor Peter Summer of the London School of Economics is a regular expert witness.

Peter Summer:
The events expert, their job is not to prove that the defendant is not guilty, they have to raise a reasonable doubt. But the reasonable doubt is in the context that you are giving evidence under oath and you're overriding duty is to the Court. Not to whoever might be instructing you or paying you actually typically you are being paid by the public.

[Ian] Kennedy:
But examining a computer for malware such as Torjans or pop-ups is not as straightforward as it may sound. The computing world is a notoriously fast moving environment in which operating systems and applications are constantly changing and being updated. Different scans may deliver different results that can cause difficulties if one side wants to test the techniques of the other and confirm they've got it right. Peter Summer says the way to resolve this problem is by getting the experts to meet.

Peter Summer:
Increasingly the Judges are requiring experts to meet before the case to list out points of agreement and disagreement. It used to be done informally, it's now a specific part of the criminal procedure rules under which they do that. That means that you reach a sufficient agreement about the precise circumstances, that the Jury get a reasonable answer to it.

[Ian] Kennedy:
A defence expert though doesn't have to prove there are viruses on the computer. It's down to the prosecution to prove a person's guilt beyond all reasonable doubt. In the case of Julian Green who was charged with downloading child porn. It was sufficient for the defence to cast doubt on the claim, even though they couldn't prove that Trojans were responsible. Rob Newman of the lawyers [Kitsons] who represented Mr Green.

Rob Newman:
What we had here was a strong indication that, in fact although they were on his computer and had perhaps been downloaded by his actions in opening an e-mail or e-mails, there was no evidence or there was certainly doubt as to whether that had happened because of his intention to import the images. At the end of the day that was what was significant in our case. We were able to cast huge doubt on the prosecution allegation so that they accepted and the Court then accepted that there was no convincing evidence that could go before the Court to say that our client had downloaded the images.

Unknown Speaker:
He wishes to say "He has always insisted that he was not guilty and that he was the victim of a criminal act rather than being a criminal himself."

Julian Green:
I felt very angry.

Unknown Speaker:

Angry at the way you'd been interpreted by the Police?

Julian Green:
Interpreted and treated and what I've been accused of made me very angry.

[Ian] Kennedy:
Aaron Caffery had argued that a Trojan horse virus had infected his computer but when a computer examination failed to turn up any virus Caffery said it must have self-deleted. The Jury acquitted him amid calls from sceptics that a self-deleting virus is an all too convenient way to escape prosecution. Computer Forensic Investigator Graham Dellaway who worked on the very first case when the Trojan Defence was used says "It is feasible for a virus to hide."

Graham Dellaway:
Some viruses are designed to change their appearance. Anti-virus software looks for specific patterns on the disc of a computer where each pattern has been identified as belonging to a virus. So if a virus is able to change its appearance then the pattern for that virus will change and it won't be found.

[Ian] Kennedy:
But Graham Dellaway has a more fundamental objection to the Trojan Defence.

Graham Dellaway:
Examining a computer, you're looking at a snap shot of the computer as it is when it was seized by the Police. Whether you can determine what happened to get it into this state owes as much to luck as it does to judgement because much of what we do on computers isn't being recorded and logged.
The virus logs record the presence of a virus on the computer they don't record whether the virus was active. They don't record what the virus was used for.

[Ian] Kennedy:
But even if the virus itself can't be found or be shown to be responsible for downloading the material you can look for corroborating evidence. Computer Forensic Investigator, Martin Gibb, who worked on the Julian Green case.

Martin Gibb:
If people are trying to use the Trojan Defence there are a number of other factors that you would look at on the computer. Not just the fact that the Trojans are there. Have they used terms that are consistent when looking for child pornography. Have they typed in URLs or copied and pasted URLs for child pornography? Have they gone to other areas which are clearly not related to the malicious code? Have they got a catalogue of child pornography? So there are a lot of factors.

[Ian] Kennedy:
At the end of the day whatever the experts say about the science it's ultimately down to ordinary people. The 12 good and true members of the Jury and not the computer geeks or the theatrical lawyers in their wigs and robes who decide what really happened.

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