Do a Web search for “Trojan horse defense.” How can it be used to question the conclusions drawn from a forensic investigation?

Step 1:

A Trojan Horse is a malicious programme that impersonates legitimate software in order to infect your computer and change your files and data. Even your personal information may be accessible to hackers thanks to some Trojan horses.

As an illustration of how a Trojan horse could be used to infect a computer, consider the following: The victim gets an email with an attachment that appears to be from a business. When the victim clicks on the attachment, the malicious code inside is activated and starts to work.

Step 2:

Traditional Trojan horse trials typically rely on forensic evidence to raise a red flag regarding the defendant's involvement in the conduct ascribed to the defendant's computer. They avoid the problem of "placing the defendant at the keyboard" by attributing the observed behaviours to malicious software that is running on the computer. The two most typical defence strategies are to forensically identify any malware that is (or was) present on the machine, or to establish that there was insufficient malware protection in place during the relevant events.

Traditional Trojan horse cases can be divided into two groups: cases involving content, where the malware is held responsible for the presence of illegal material on a system, and cases involving unauthorised access or system interference, where the malware is held accountable for some activity related to a system. When both claims are made, the case is classified according to the claim connected to the primary activity that is being charged.

The technical SODDI defence has advanced past the traditional Trojan horse defence and has mostly been applied to copyright disputes in civil court and child pornography cases in criminal court. When illegal content is discovered on a machine and the defendant asserts no knowledge of the material but is unable to otherwise attribute the material to another person, the conventional Trojan horse defence has been employed, albeit seldom. When activity is linked to an IP address or when there is a shared computer without individual accounts for each user, a more generic technological SODDI defence has been utilised more commonly.