International Journal of Business and Management Study
Volume 4 : Issue 1 *[ISSN 2372-3955]*
Publication Date : 06 April, 2017

Connect the Virtual to a Real World

The Issue of Trojan Defense

[Chih-Ping Chang]

Abstract*—this paper discusses the Trojan defense, a common question on who really did it. In order to prove who did this post on SNS means we want to connect a specific internet character with a real person in the world. Actually, the present technology only can prove the issued post done by a specific IP address. Prosecutors need circumstance evidences to support their claims and connect to the defendant. Thus, this paper first will explain the background of the Trojan defense, such as the definition, characteristics and functions of the Trojan. Then it discusses how to handle the Trojan defense in technical and legal approaches, and concludes how the legal system represents or actually constructs the past fact.

Keywords*—Trojan Defense, Judging by Circumstantial Evidence, Reinforcing Evidence, The Process of Judging the Trojan Defense, Connect the Virtual to a Real World

I. Introduction

A Trojan Defense, also known as SODDI (Some Other Dude Did it), means the defendant cannot prove his innocent, but argued someone or a Trojan invaded his computer and committed the crime. This defense raises evidential issues of reliability and reality, which may cause the jury to bring a guilty in an acquittal, or worse, an innocent guilty. It is real that everyone will be the victim, if his computer was infected with Trojans, was deliberately framed by some others, or was treated as a "zombie" to attack other computers.

While studying at the authentication issue of social media evidence, using the printout of a social network site (SNS, e.g. Facebook pages) as evidence (aka. Social media evidence, SME) will raise four scenarios: (1) when the social network sites account is actually true (authorship is true), and the content of the posting is true, then this social media evidence is authentic and can be present in front of the jury deciding its value to rebuild the past fact; (2) when the account is true, but the content is false, then this social media evidence is still authentic and let to the jury to decide its value (the jury can decide whether believe it or not); (3) When the account is false, but the content may be true, the authentication issue is raised, the judge must to decide whether this social media evidence is admissible, because this account might be hacked or shared with others; (4) when both the account and the content are false, the judge must exclude this social media evidence because it is not authentic. This evidence should not present in front of the jury in theory. Thus, we can conclude that, as long as the account is true or no one claimed its false, then this social media evidence will be left to the jury to decide its factual value; but if the account is false or claimed false, then the judge must decide authentication of this social media evidence. Furthermore, form the defendant's aspect, as long as there is any false, no matter in part of account or content, he has the chance to raise the Trojan defense, and claims, "It was not me. There is someone who did it. "

TABLE I. FOUR SCENARIOS OF USING PRINTOUTS OF SNS

		Account in SNS	
		True	False
Content of SNS	True	SME is authentic. Jury will decide its value.	Authentication? (Trojan Defense)
	False	SME is authentic. Jury will decide its value. (Trojan Defense?)	Authentication? (Trojan Defense) Value?

Then the prosecutor is obligate to connect the crime to this defendant by using this social media evidence. Precisely the prosecutor needs to connect the defendant to this virtual identity, trying to realize a virtual figure to the real person, who is exactly standing in the courtroom just across from him.

Thus, this paper first will explain the background of the Trojan defense, such as the definition, characteristics and functions of the Trojan. Then it discusses how to handle the Trojan defense in technical and legal approaches, and concludes how the legal system represents or actually constructs the past fact.

II. Background of the Trojan Defense

A. Definition of the Trojan

A Trojan is a type of malicious software (globally known as malware) that is either packaged along with a useful piece of software or pretends to be a piece of useful software itself.[1] Hackers often use it with Backdoor, connecting computers between the hacker and the victim, to steal someone's account and password or Confidential information or both. A Trojan also can be used in controlling the victim's computer to attack other computer. Then the legal authority can find this zombie computer but is hard to trace the hacker's location.

In general, a Trojan is a malware of delivery mechanism. Its main function is using system vulnerabilities and allowing hackers to freely access information inside the infected computer. Most Trojans are implanted directly from hackers, or via P2P software, email, file sharing, or removable devices. The clever part of Trojan is not usually a separate file, but combined with other executable files (known as ".exe").

Therefore, it becomes a part of the executable file, and when starting the executable file, the Trojan is also activated. Surprisingly, we can make a Trojan with "Trojan-making Kits", which is easy to find in the internet and can package the Trojan into a useful program. A pirated useful program (ex. Microsoft Office) or popular game software is the ideal place to hide the Trojan. For breaking the security measures of the original program, "program unlooper" is used to cheat the security measures, and meantime, it also change the computer settings. While a person installs and runs a pirated program, he might activate the Trojan, sending his information to an unknown person. It is sad but true, the situations often happen because many people prefer to download the pirated program (especially the free one) with or without intention. Making easy and spreading rapidly and widely, that is also the reason why the courts think this Trojan defense carefully. It happened every second in the world.

Recently, most Trojans has been used the hidden technology of Rootkit, leading to more new variants of Trojans, which are more and more difficult to predict. The Trojan Defense can justify itself through features of Rootkit, thus we need to analysis Rootkit with the digital forensic tools and procedures, in order to solve the Trojan defense issue. The internet will only continue to flourish in the future, from wired to Wi-Fi, and from telephone to smart phone. Malwares are constantly passing between the internets, resulting in ever-increasing cybercrime. At the same time, issues of Trojan defense continuingly challenge professional and credibility of forensic technology.

Chih-Ping Chang/ Doctoral Candidate
Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology, CIRSFID/University of Bologna
Bologna, Italy

B. *Digital evidence produced*

Here are some types of digital evidence in the victim's computer produced by the Rootkit.

1) Information of IP and network interface card

Using internet is necessary to run the Trojan or Rootkit, which is provided by an ISP (internet service provider). Therefore, we can ask the ISP to provide the audit records, which reserved event identifiers to provide information about the type of server events or activities. Then we may analysis and compare information of IP and network interface card to search an attacker or unauthorized person's trace.

2) Connection information

We can gather information of connecting the internet from the victim's computer system. This information includes records of sign-in or sign-out the network, records of attacking or connecting the firewall, or the port information, which is used to prove an authorized connection or abnormal network activity occurred.

3) Malware

We can use forensic tools to find the source code of a malware or Rootkit, or its existence at the scene, to prove that the computer was indeed invaded by a malware.

4) Digital activities

Digital activities are determined primarily on the basis of the system audit records, to prove that someone actually invaded this computer or this computer was use to commit a crime. Types and quantities of audit records are quite complicated, and invalid, incorrect or falsified time information will cause a lot of garbage information. Forensic officers will spend a lot of time in dealing with such information.

C. *Trojan has the Nature of Occult*

1) Obfuscation added in the Trojan

Functions of a Trojan may include hiding the IP address of the control terminal, remote control, intercepting the network packet, recording keyboard input data (keystroke logging), passing messages, and providing packets to the zombie computers. The attacker implanted the victim's computer a program with the foregoing function, and then compiled this Trojan, adding the junk code to change the originating point code of the original program. Such an operation is called obfuscation, which is a special computer program development tool, typically used as the reverse engineering protection, anti-crack protection, and anti-piracy protection of the commercial software.

This obfuscate mechanism converts binary system code into the new binary system code, which is very difficult to analyze, or completely different with the source code, but the function did not change. That is, the original program function and logic are same, but transformed into other forms of presentation. It aims to completely hide specific implementation details or architecture of the program in its source code. If we want to disassemble or reverse engineering an obfuscated program, this binary system of machine code will be garbled or render meaningless messages, to protect the source code and the machine code.

2) Packer is used in the Trojan

The attacker also often uses the packers [2]/shelling technology to hide Trojans. Through this packers/shelling operation to modify computer language or code in the Trojan, it with different features cannot be detected, deleted or quarantined by antivirus soft wares.

A packer, similar to encryption and compression, is a variation of the algorithm. For example, a section of code is Social Media Evidence: aaa. After encrypted, it may become sh*eh^$sfgdji%as1. Then the compiler software cannot resolve the internal program, but the computer can recognize under the premise that the encryption is written on computer logic. Conversely, shelling employs a restore method in a packed program, to restore the encrypted content. In former example, after packer, what we can see is "sh*eh^$sfgdji%as1". Employing shelling in "sh*eh^$sfgdji%as1", the contents can disassemble back to Social Media Evidence: aaa. Anti-virus software sometimes determines a file as the malware based on its packer. After all,

safety programs typically do not encrypt or packers. Most malicious programs will packer, unless the programmer does not want his source code to be analysis.

D. What the Trojan can do

For lay persons, the Trojans defense seems to be very credible, and hackers seem to do anything. Thus, the defendant may be there will be a psychological speculation, and then raises the Trojan Defense to absolve his charges. Here are some examples to explain the possibility of Trojan defense, and test whether the Trojan defense really so do anything.

1) The defendant claim that someone remote his computer and login his email account, sending defamatory letters to the victim.

Generally, the attacker collected the victim's account and password, and then he usually remote a zombie computer to access the victim's account and send the email, for security reason (he cannot be trace by the police). It is necessary to check the IP address of email deliver, in order to realize where actual sending source is. In some cases, the attacker uses the victim's computer directly to send the email. As reference for determine whether this email sent from this computer, the sent item should be first checked. But if sending the email through the command-line interface, the backup file is not even found inside in Outlook, and the abnormal status doesn't appear on the screen. Because sending the email through the command-line interface doesn't need to control the mouse, it is hard to find abnormal. If the police are confidence that the defendant send the mail, then the first step is to search whether there is the Trojan existed in the defendant's computer. Second, the sending time and before/after may help to find the trace of invasion in this computer.

In this case, the defendant's computer may indeed have been implanted the Trojan, and the hacker may also use his account to send emails. However, it is just one of possibilities. The forensic experts need more solid evidence to build this case.

2) The defendant argued it was not him but someone hacker his account to leave a message about the compensated dating in the internet forum.

In a perspective of forensic science, first, it is different between implanting the Trojan and VPN (virtual private network). While the hacker remotes the defendant's computer to leave the compensated dating on line, his digital activities will be showed on the screen. Theoretically, the system is unable without showing any abnormal situations to allow the defendant playing computer/online games, while the hacker remotes this computer to leave the message in the internet forum through a Trojan. Thus the forensic experts can check digital activities on this computer with its timeline, and then they may find evidence to prove what the defendant claimed.

From the experience, once an attacker successfully hacked and implanted a Trojan with remote function, he has no need to pretend this victim with his personal information just to do more secret protection. Most hackers invade other computers in order to prove his abilities or steal information. Using the victim's name to post the compensated dating in the internet forum is not smart for the attacker's security, unless he just want to spoof this victim. Therefore, this Trojan defense has a high probability to be false.

3) The defendant A and B were charged in using the victim C's eBay account to make the fraudulent trading. Both A and B argued they are hacked by someone. They didn't commit the crime.

The point of this case is the possibility that the defendants' computers were controlled by others. Even though the forensic experts prove the hacking activities can connect to the defendants' computers, it cannot be excluded that the malicious activities were made by the Trojans implanted in the defendants' computers. Therefore, we need to consider circumstantial evidence.

For example, the defendant applies an internet account and shares the network with others. When other people use this account with a sharing device, these internet activities will be attributable to the defendant's conducts. Furthermore, if the forensic experts indeed found the Trojan in this defendant's computer and some evidence to prove it related to malicious activities, this case have a high possibility that the defendant's computer is manipulated by someone to do malicious activities and its IP address is intentionally left. It is not enough that taking the IP address alone as the evidence to consider who is the criminal hacking C's account and committing the fraud. The Trojan defense should be taken into account while the defendant raises this issue.

III. Technical Solution for the Trojan Defense

A Trojans defense forensic procedure is a necessary forensic procedure when the computer is claimed to be threatened by viruses, Trojans, backdoors, or other malware. There are some factors should be considered in this procedure, such as identity of the defendant (possible offenders/innocent), un/infections of the malware, and comparison of records of digital activities. The processes is first to determine the possibility of the offender and the innocent based on currently obtained digital evidence, then to detect and analysis the malware in the disputed computer, and finally to discriminate digital activities according to various records collected.

A. Detecting the Trojan

If the Trojan was found in the disputed computer, then further questions should be considered, such as whether this Trojan is reliable (Maybe someone implant it after the crime.), or whether other malware or Rootkit exist. The forensic experts need to identify the type of the Trojans, to learn the way this malware invaded, and to find the time this malware invaded and data generated by this malware. The time stamp is useful to compare digital activities recorded in the computer and the assertions made by parties. There will be two possibilities depending on the identity of the defendant: First,

the perpetrator attempts to clear himself and carefully crafted this crime scene. He may intentionally implant a Trojan to confuse the forensic expert. Second, the defendant is actually innocent. The forensic experts should not make any assumptions about the parties or have any stereotypes. They should be judged these digital activities in a fair principle, and then fairly present results of these two possibilities.

On the other hand, the Trojan was not found in the disputed computer. The forensic experts need to consider whether the Trojan really do not exist, and whether there is human error or evidential pollution problems. These situations will cause the evidence lose its reliability and will not be admissible at trial. Combining with the identity of the defendant, we might get two possible results. First, the forensic expert found the solid evidence to refute this offender's unfounded defense. In this situation, the offender may be unable to provide evidence to prove his innocence; therefore he argued an unfounded defense in order to disrupt the investigation. Second, although the defendant is actually innocent, there is no trace to show his account or computer was invaded. In this case, the defendant's defense will be rejected by the court, as the same result as the first situation. The Forensic expert needs to conduct further procedure to determine these digital activities.

B. *Digital Forensics of Digital Activities*

After detecting the Trojan, the forensic expert should further consider digital activities in the disputed computer. Even though there existed a Trojan in the disputed computer, it does not naturally represent related to the improper digital activities. In this procedure, the forensic expert is obliged to find the evidence, proving improper digital activities actually existed in this computer. For example, the forensic expert can use time stamp to determine the defendant's alibi. Digital activities can be divided into two categories by objects, which are Host-based evidence and Network-based evidence. The audit records in the disputed computer are Host-based evidence, including the system files, digital media, time, and audit records. The audit records in the internet are Network-based evidence, including external connections records, connection time or connection port information, or ISP audit records. According to the content of Host-based evidence and Network-based evidence, forensic experts analyze digital activities and the defendant's statements, and meanwhile range degree of evidence probative force in accordance with obtained digital evidence. Therefore they can present stronger digital evidence at trial.

In summary, we can further discuss technic issues of the Trojan defense invoked in the following two scenarios.

C. *What to Do When Malware is Found*

When the forensic experts have found the malware in the defendant's computer, they need to (1) identify the capabilities of this application through information provided by antivirus vendors or use the process of reverse engineering to make sure the natures and functions of this founded malware; and (2) point out how the malware was installed on the system, when it is installed, and if it was ever run.[3] Besides, finding the malware doesn't mean it should be responsible for the illegal activity. The better countermeasure is to find evidence to show that a specific user did this illegal conduct. For example, the forensic experts may consider the login records provided by ISP to show the network traffic while the crime is conducted, or discover the records of account assessing to build the connection between the defendant and the internet crime or the alibi for him.

D. *What to Do When Malware is not Found*

When the forensic experts didn't find the trace that a malware was implanted in the defendant's computer, he may claim another reason to explain this no-malware-found situation. For example, the defendant may further claim that a wiping tool is used in his computer. A wiping tool is used to eventually overwritten the deleted data space by computer, for prevent this data being recover. Receiving a delete instruction, most currently operating systems will mark the deleted data space a free space, rather than wipe data by default, and a special application is needed to be installed. As other software used in the computer, a wiping tool cannot uninstalled itself, and some trace must be found in this computer asserted using a wiping tool. Thus, there are three countermeasures to rebut the defendant's claim.

The first countermeasure is trying to find operating-system-generated copies of the un/installed records of a wiping tool in temporary files and in memory. These copies are also created by the operating system in memory, but lost when a computer is powered off. Additionally, when the memory is full of data, some of the data will be saved to the swap space, and exist after the computer is powered off. If the operating system does not wipe data by default, the temporary files and swap space may contain evidence of malware or the wiping tool.[3]

The second countermeasure is considering that wiping tools may leave signatures behind. The low-level system structure may show signs that a wiping tool was used because one of the entries is all zeros or has invalid data.[3] However, these signatures will be overwritten by normal system activity, so the time factor is important for forensics. The third countermeasure is used when no malware has been found and signatures of wiping tools have been found. The forensic experts cannot conclude directly that maybe a malware is existed and related to the illegal activities. They need to consider further the possibility of wiping the asserted malware or actually wiping other files or soft wares, such as wiping sensitivity data.

IV. Legal Solution for the Trojan Defense

This SODDI defense in fact has been existed in legal system for a long time. The defendant always argues his charge and contends some other person did it instead of him, no matter this defendant is guilty or not in the reality. It is very common in practice, and the situations include intrusion of the

unknown third party, such as the Trojan defense, and defensing the credibility of evidence obtained by law enforcement or parties. Now how the court faces these various defenses is in focus.

So-called Trojan defense means the defendant argues that internet attacks are not relative to him, but are conducted by hackers through implanting the Trojan in this disputed computer. In this era of rampant Trojans, these situations do occur.

A. *How the Trojan Defense is used*

There are two scenarios that the defendant will raise the Trojan defense. First, the defendant argues he did not commit the crime, which means the crime was committed but attributes its commission to someone other than the defendant. Second, the defendant technically committed the crime but lacked the mens rea required for conviction, which means the defendant engaged in conducting the crime but lacked intention. In the first scenario, the defendant attempts to raise a reasonable doubt in his case, and he tries to deny his intention in the second scenario.

1) Raise Reasonable Doubt

While a Trojan defense is raised, the defendant gives the jury an alternative theory of the crime, which he tries to raise a reasonable doubt in his case, and let the jury believe the true offender is someone other than him. The defendant is not obligated to identify who is that true offender, but need to raise the jury's doubt to a reasonable level, which means the defendant's proposal can convict a reasonable third party to believe it may possibly happen. Then the prosecutor must show that malware was not responsible for the commission of the crime charged in this particular case.[3] Therefore, in the evidence law, a Trojan defense is used to reduce reliability of theory of crime made by the prosecutor and also the prosecutor is obligated to provide evidence to prove that the defendant's theory is not reliable.

2) Negate *mens rea*

mens rea (Criminal mentality) and *actus reus* (crime) are the two basic elements of subjective and objective aspects of the crime in the common law system. *mens rea* is the mental state should be condemned by a society, when the perpetrator implements of a social harm behavior. It includes intention, knowledge, recklessness, and negligence in legal category. A criminal case cannot be built in lack of any one of the two elements. Some defendants use the Trojan defense merely to deny their *mens rea* in the situations where these defendants cannot deny they engaged in conduct that constitutes the *actus reus* of the crime.

3) Establishing the Defense

To establish a Trojan defense, the defendant has to introduce as least some evidence establishing (a) a Trojan horse program or other malware was installed on his computer (b) by someone else (c) without his knowledge.[3] In the situation a malware found in the defendant's computer, he may point out the malware found in his computer was responsible for the conduct being attributed to him, in order to support his defense. Once again, the prosecutor has the burden of proof, which he needs to prove this malware didn't exist during the time of crime, or it is irrelevant to this illegal conduct. In other situations, there might not be the malware in the defendant's computer, and the defendant is hard to raise a reasonable doubt merely by presenting the malware. The defendant may assert he is lack of knowledge of the computer technology and remind the jury the high risks of being hacked, or he may "deliberately" leaving his computer unsecured to support the possibility to be hacked.[4]

B. *How can the prosecution respond*

1) Establish Defendant's Computer Expertise

When the defendant claim as above that lack of knowledge led to his computer was invaded by the Trojan or other malwares, the prosecutor may be able to show the defendant actually has the knowledge of computer technology to rebut the defendant, such as prove the defendant is a black hat hacker, or he work in the computer security field. Or contrarily, the defendant asserts he has computer expertise and then challenges the reliability of the forensic report, in which they don't find any malware in the defendant's computer. The prosecutors can response even though the defendant might have some expertise, but he is not expert in computer forensics. If the forensic expert could not locate the Trojan, there is no reason to expect the defendant can identify the Trojan or realize it has been implanted in his computer.[3]

Prosecuting a knowledgeable defendant is difficult, but the prosecutor can use the defendant's computer expertise to argue this defendant is less likely to fall victim to such an attack, when this defendant invoke a Trojan defense. The prosecutor can build his argument successfully based on evidence of the defendant's computer expertise, including testimony about the defendant's general computer expertise, as well as testimony from expert witness who can show that the computer was protected by a firewall and by up-to-date antivirus software, especially when the malware is not found. [3] Moreover, the prosecutor can use the defendant's computer expertise to point out in front of the jury the trend that the defendant preplanned his Trojan defense or suggested his counsel to do it.

2) Negate the Factual Foundation of Defense

There are two basic tactics law enforcement can use to negate the factual foundation of a Trojan defense.[3] First is using the technical analysis to rebut the defendant's claim. In this tactics, the prosecutor has different argument in two scenarios: when the malware has been found or has not been found. In the first scenario, the prosecutor will focus on whether this malware could have functioned as the defendant claims, and in the second scenario, the prosecutor will focus on whether there is the wiping tools installed in this computer. Another tactic is a traditional legal approach used in every criminal case, which is an approach to establishing motive, intent, and culpable conduct. In the case of Trojan defense, on the one hand, the prosecutor can show the extent to which this computer was utilized for unlawful purposes; on the other hand, the prosecutor can point out how the evidence relating to the crime is stored on the defendant's computer.

C. General Way to Judge

The important issue raised by the Trojan defense in the legal system is how to prove the defendant is that criminal committing that crime. While the case is related to digital activities, the issue turns to be how to connect the virtual criminal activities to the real person. Basically, we need to determine what kind of crime it is and what features it has, and then we can deduce behavioral characteristics of this crime. Comparing with digital evidence obtained, we may find the possibility of the accused crime. Now we apply this judging model in the case of child pornography photos where the Trojan defense is most commonly raised.

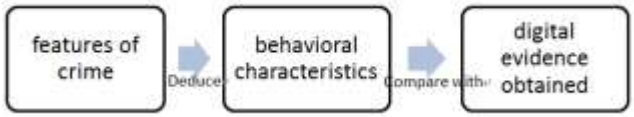

Figure 1. The Process of Judging the Trojan Defense

1) The Case of Child Pornography Photos

In this situation, the defendant always argues those child pornography photos found in his computer were not downloaded by him. There must be someone hacked or implanted the Trojan to do that. Some features of this crime are numbers of child pornography, the perpetrator's preferences, and the perpetrator's sexual habit. These offenders interested in child pornography mostly search these photos online and "appreciate" these photos one by one, looking pictures carefully and slowly, maybe with their fantasy. It is a typical pedophilia's behavioral characteristic in this type of crime. If the forensic experts collect some digital activities such as these thirty child pornography photos were downloaded at the time as the package, or these thirty different website were accessed at the same time or at one second, it raises a probable cause that these photos may be downloaded by a machine. Because according to the behavioral characteristic above, if the defendant is a pedophilia, for the preference or the pursuit of inner desire, the defendant may prefer to view these photos one by one than download them as package. That is how we compare a person's behavioral characteristics with digital evidence to determine the possibility of the accused crime. Of course, there are far more factors we need to think about. Here it is just a simple example.

2) The Case of Account Theft

Another case that the defendant will raise the Trojan defense to argue his charges is that his account was stole by someone and this someone did malicious activities, while the prosecutors charge the defendant committing a crime based on his account as evidence. For example, in a case of internet trading fraud, a thief used A' account to trade with the victim (buyer), and took the money but did not have the goods sent to the buyer. Thus, prosecutors accused the account holder, A, of fraud. The defendant A argues that his account was stolen, but the police cannot find the IP address which is used by the thief to connect the buyer in trade.

Due to very common situation of account theft, the defendant's claim is likely to be true. But the point is how to prove. In this case, the behavioral characteristic is using other's account, which means, the thief in theory will connect this account through a different IP address. Thus, the first step is to request the trading platform to provide use records, and to confirm which IP address is connected to this account during the time of trading. There are two possible situations as follow. First, the IP address doesn't belong to the defendant, such as it comes from another country. Then it is highly possible that the defendant is innocent, unless he presented in that country during that time or he used the VPN to hide his IP address. The latter situation requires further digital forensics to prove. Second, the IP address belongs to the defendant. In this situation, the only way to prove the defendant's innocent is that his computer was implanted the Trojan and someone use it to control his computer to commit the crime. Thus, this situation also requires further digital forensics to prove (a) the Trojan was actually implanted in the defendant's computer, or some trace of Trojan can prove it, (b) this Trojan did these malicious activities in this case, and (c) other circumstantial evidence can prove the defendant has no relevancy with these malicious activities, such as the defendant has the alibi while these malicious activities occurred.

3) The Case of Claiming "Computer is hacked"

There is another common situation that the defendant will raise the Trojan defense when he claims that his computer was hacked. For example, the mainframe computer of the A company was hacked and most data inside were deleted, causing a huge amount of loss. The police trace the invading IP address and find it belongs to the former employee B, and then bring B to justice. B argues he didn't invade A's computer to delete the data. There was someone implanted the Trojan into his computer and controlled it to commit the crime.

In this case, if B's argument is true, then the forensic experts must find (a) the Trojan was actually implanted in the defendant's computer, or some trace of Trojan can prove it, and (b) this Trojan did these malicious activities in this case. Furthermore, factors (a) and (b) only prove a Trojan related to the crime actually existed in the defendant's computer. To prove the defendant's innocent, technically factor (c) other circumstantial evidence is required, but in legal system, inversing the burden of proof occurs. That is, the prosecutor and the police need to prove B is the person who invade A's computer. In this case, a solid structure of evidence to prove that the defendant is the person who invaded the victim's computer at least contains the crime result of the deleted data base, the invading IP address related to the defendant, and other circumstantial evidence to connect the defendant and this invasion.

D. Judging by Circumstantial Evidence

For the purpose of connection the malicious actor on the web to a specific person in the real world, it is not enough just to prove the Trojan existed in the disputed computer. More evidence is required to prove the relationship between the

defendant and the crime, which is called circumstantial evidence, "evidence that relies on an inference to connect it to a conclusion of fact." Modern legal system does not provide the quantity or quality of circumstantial evidence. Whether the circumstantial evidence is trustworthy depends on a jury in the case law system or judges in the civil law system to decide whether they are convinced by the circumstantial evidence and its advocated arguments. It applies the same rule in the Trojan defense case.

For example, someone stole the victim's account and password in an online game. Then he accessed the victim's account and stole all the virtual treasures. The police traced the invading IP address, found the defendant have that IP address, and brought the defendant into justice. The defendant claimed his computer was hacked. He argued his computer is continuingly connecting the internet 24 hours a day without setting a firewall, and everyone is easy to invade his computer. The defendant also claimed that he has the alibi during the time of incident. In this case, the invading IP address is the only direct evidence provided. The prosecutor needs more circumstantial evidence to build the case.

The point in this case is to link the defendant to the malicious actor online. Except the trace of the Trojan in this disputed computer, several other factors should be considered as follow: (1) the hacker's habits; for example, a hacker impossibly access the victim's account through the defendant's IP address every two days in six consecutive days. According to the hacker's habits, he may have many accounts and passwords, and it is necessary to access one account so frequently increasing his risks. (2) poor connection quality through the Trojan; for example, since the hacker already got the victim's account and password, it is more reasonable that he access this account through an internet café. Because there the hacker can get better speed and quality of network connection and also can hide him himself easily. The connection is poor, if the hacker connects to the defendant's computer through the Trojan, and then remotes this computer to access the victim's account. (3) Unreasonable alibi; for example, the defendant claimed when the case occurred he was not at home. He was helping his brother move the house in the neighborhood and then stayed there for nights. But according to the investigation, his brother lives just next door to the defendant and states he didn't remember whether the defendant stayed in his house overnights and the exactly date. (4) Timing of reboot the computer. For example, while the judge asks the defendant to send his computer to do digital forensics, the defendant states that he just reboot his computer one day before. This is quite doubtful that the defendant formats his system at this timing. Although it is not impossible to recover the data in a formatted computer, the fact that the defendant picked up this time to reboot imply he want to hide something. This can be the circumstantial evidence to support his guilty.

E. *Reinforcing Evidence*

As mentioned above, circumstantial evidence is used to supplement the insufficient of direct evidence and links evidence and facts of the case through inference. However, how much evidence can be called "sufficient" to build the case? Here we will discuss the reinforcement of evidence.

The first question is, like many cases, the prosecutor only have the invading IP address as evidence. This is also the situation for many network intrusion cases, in which cases the main evidence are results of the crime (ex. The deleted data base or the stolen virtual treasures), and suspected attacker's IP records and actual registrant through further detecting the records. But it is doubtful that this actual registrant is exactly the attacker. The most common situation is the police traced the records and found the network administrators. Network administrators will receive subpoenas, which state the IP address they own is involved in attacking other computers, and they are obligate to cooperate with investigation and defense at trial. Moreover, if the hacker attacked other computers through their computer all around the country, the network administrators will be busy complying subpoenas from local courts, even though they are one hundred percent innocent. Therefore, in the case that the suspect doesn't plead guilty, the prosecutor should not build the case just by results of the crime, and the suspected attacker's IP records. The prosecutor needs other evidence to reinforce his case. In this situation, the prosecutor may ask network administrators to provide evidence can prove their computers were attacked, such as the implanted Trojan, unknown login records, or abnormal digital activities in their computers.

The further question is how to reinforce evidence in a case. The answer will be found case by case. For example, in that "computer is hacked" case, the prosecutor has two kinds of evidence: the suspected attacker's IP records and results of the crime (deleted data base). About the suspected attacker's IP records, the prosecutor may reinforce evidence on the possibility of the Trojan invasion. He can sent this disputed computer to do digital forensics, to find whether there is the Trojan involved. About results of the crime, the prosecutor may reinforce evidence on the defendant's alibi during the time of invasion. It is obvious, if the defendant cannot or didn't use his computer to connect the network during the attack time, or the connections neither came from the place where the defendant was nor were used VPN to pretend from there, the defendant has the alibi, which may prove his innocent. Besides, the prosecutor also can use the connection between results of the crime and the suspect's past position to reinforce evidence in this case. If the suspect was the network administrator in the victim's company, he has more knowledge and chances to commit this crime than in another situation, if the suspect was the accounting in the company with little knowledge on computer science.

For another example, in the stolen virtual treasures case, the prosecutor also has two kinds of evidence: the suspected attacker's IP records and results of the crime (the stolen virtual treasures). About IP records, the prosecutor can reinforce evidence on the possibility of the Trojan invasion, and about results of the crime, on the defendant's alibi during the time of invasion. The prosecutor can further reinforce evidence on results of the crime through proving the possibility that a hacker playing the online game through the defendant's computer with bad connection quality.

In sum, we can conclude three points for reinforcing evidence in the Trojan defense cases. First, the possibility of the Trojan invasion can be used to reinforce evidence on the suspected attacker's IP records, and it can be proved through digital forensics. Besides, we need to think further, that is, if we cannot find the Trojan in the defendant's computer, it doesn't mean there was no the Trojan in this computer; even though we found the Trojan in the defendant's computer, it doesn't mean this Trojan was related to the attack activity. Second, the connection of the case and the possibility of being hacked can explain the relationship between the defendant and the case, emphasize the defendant's motivation and reinforce the evidence on results of the crime. For example, the former employee is disgruntled to be fire, and invaded the company's system and delete data as revenge. The prosecutor can make a complete story by profile this former employee, such as he was the network administrator, who is familiar with the company's system, in order to link the defendant to this case. Third, the defendant's alibi is always the best way to reverse the burden of proof. For example, the defendant can raise his alibi and convince the court. If it is accepted by the court, then the prosecutor is obligated to turn over this alibi or rebuild another story to convince the judge or jury that the defendant actually committed this crime.

v. Conclusion

When the Trojan defense is raised, the legal system cannot determine whether a Trojan exists, but it moves the burden of proof between parties. For example, it is the prosecutor's obligation to prove the defendant implemented a fraud online. But when the defendant objected with a Trojan defense, that is, the defendant claimed there is someone else did it, but not he, then the defendant need to provide evidence at least to prima facie level to convince the court there might be a hack invaded his computer. If he succeeded, then it is the prosecutor's turn to prove his original theory (the defendant did it), or to prove this case is not related to the Trojan.

The forensic experts usually can provide evidence to prove possibility of being implanted a Trojan, and relationship between the Trojan (if found) and this disputed malicious digital activities. The standard operating procedure is firstly to detect the Trojan, and secondly to make digital forensics of digital activities. When a malware is found, forensic experts need to identify this malware and its invading traces to prove this malware is related to the case; on the contrary, when the malware is not found, forensic experts need to prove no wiping tool is used. Then they can conclude the malware is not related to this case.

The defendant can use the Trojan defense to raise reasonable doubt, negate *mens rea*, and establish the defense. And the prosecutor can respond to the defendant's Trojan defense by establishing defendant's computer expertise, and negating the factual foundation of defense. For a judge, circumstantial evidence and reinforcing evidence are necessary, because even using forensics, there is still a gap between this virtual crime and the real person who did it.

The forensic science can prove the computer was invaded by a hack or implanted a malware, but it is hard for forensic experts to build a solid or real connection between the computer and the real criminal. Unfortunately, there is only one thing that the legal system wants to prove, which is who did this crim. Thus defendants and prosecutors provide more circumstantial evidence to reinforce their theory, in order to convince the judge or the jury to believe their story and make the favorable judgment for them.

We can find the different between the forensic science and law in this Trojan case. The forensic science proves the past fact, whether there was the malware; but the legal system construct the past fact, that is the defendant who did it or who did not do it.

References

[1] S. Bowles and J. Hernandez-Castro, "The First 10 Years of the Trojan Horse Defence," Computer Fraud & Security, pp. 5-12, January 2015.

[2] E. Conrad, S. Misenar, and J. Feldman, CISSP Study Guide, Syngress, 2015, p. 139.

[3] S. Brenner, B. Carrier and J. Henninger, "The Trojan Horse Defense in Cybercrime Cases," 21 Santa Clara High Tech. L. J. 1., pp. 1-53.

[4] Micah Joel, Safe and Insecure, Salon.com, at http://www.salon.com/2004/05/18/safe_and_insecure/