Applying IPU Model to Digital Evidence Review in Trojan Defense

Da-Yu Kao*

Department of Information Management, Central Police University, Taiwan

ABSTRACT

As the use of Trojan programs by hackers becomes more widespread, the Trojan Defense is likely to be deployed in an increasing number of legal cases. Therefore, Trojans present a challenge to law enforcement agencies (LEAs). This paper examines the digital forensic report of Trojan Defense from a ticket scalping case in Taiwan and proposes the identify/perform/understand (IPU) model for exploring and analyzing evidence-relevant data. The IPU model improving a digital evidence review is proposed in three stages: identify temporal data to build the sequence (when), perform functional testing to gain insights (how), and understand relational reconstructions to clarify the actions (who, what, where). The model can help the judge in a Trojan Defense case weigh the value of digital evidence more systematically. A temporal, functional, and relational analysis was used to reconstruct the events in the ticket scalping case. This research can efficiently assist law enforcement officials in dealing with the ever-increasing Trojan Defense.

Keywords: Trojan Defense, auditing logs, digital forensic report, evidence review, law enforcement agencies

利用 IPU 模式評估木馬抗辯的數位證據研究

高大宇*

中央警察大學資訊管理學系

摘　　要

當駭客日漸頻繁使用木馬程式入侵電腦網路，木馬抗辯相繼成為資安事件或法律訴訟案件的難解疑題，更讓執法機構面臨嚴峻挑戰。本文個案提出木馬抗辯議題，並主張：不知名駭客植入木馬程式後，移除相關證據；並不斷要求額外的鑑定證人，重新檢驗刑事警察局的鑑識報告品質。本文提出分析數位證據的識別(Identify)/執行(Perform)/理解(Understand)模式，作為法院或鑑定證人，檢驗木馬抗辯案件的數位證據評估依據；並提出識別時序、測試功能及釐清關係等三個階段程序，期重建事件原貌，幫助法官有系統地衡量數位證據的證據能力與證明力。本模式可有效地協助執法人員處理越來越多的木馬抗辯議題。

關鍵詞：木馬抗辯，稽核紀錄，數位鑑識報告，證據評估，執法機關

文稿收件日期 106.9.12; 文稿修正後接受日期 107.5.10;*通訊作者
Manuscript received September 12, 2017; revised May 10, 2018;* Corresponding author

I. INTRODUCTION

Many organizations employ data networks to process digital transactions and to store associated data [1]. Computer applications and systems are highly sophisticated and may be vulnerable to attack. Most Trojan attacks remain unidentified, and vulnerabilities are often attributed to bugs in the code. Users are typically tricked into loading and executing a Trojan on their system. Given the significance of the Internet because of its wide use in different areas, the penalties for hacking have been made increasingly severe. However, law enforcement agencies (LEAs) must devise a wider range of techniques to fight against it [2].

1.1 Taiwan Train Ticket Scalpers

Many Taiwan residents have complained of the difficulties encountered while booking tickets for traveling because of the activities of "scalpers," who resell tickets at prices above the face value. Scalping is encouraged by the visibility and accessibility of online ticket purchase systems. In the railway system, scalping is most frequent during the holiday travel rush, when many travelers are ordering long-distance train tickets. Reports of ticket scalping are common during the Chinese New Year, Tomb-sweeping Day, Mid-Autumn Festival, and other holiday periods. Ticket scalpers make use of websites and social media platforms such as Facebook, to falsely claim that they can help purchase tickets for travel in Eastern Taiwan as long as they pay an additional 5% as booking fees. This is in breach of Taiwan's Railway Act that prohibits the reselling of tickets for profit.

1.2 Digital Artifacts in Cybercrime Investigation

As computer systems have become more complex and widespread, the amount of stored data has grown, and user interfaces have been simplified to make them accessible to users with few or no computer skills. In the course of a cybercrime investigation, a suspect's activities are tracked using digital artifacts, web browser history, cookies, and event logs [3]. To make computer programs easier to use, computer programs store increasing amounts of information about the users, including their actions, preferences, and credentials. Thus, the stored data contains many artifacts in the form of logs, files, passwords, caches, history, and other data. Some of this data is stored as plain text, some is obscured, and some is encrypted [4]. LEAs use these data to identify users and track their digital activities.

The rest of the paper is organized as follows: Previous relevant studies of the Trojan Defense and digital evidence are discussed in Section 2. Section 3 describes a Trojan Defense used in a train ticket scalping case in Taiwan, presents the digital forensic report, and suggests improvements. A novel identify/perform/understand (IPU) model for reviewing digital evidence is proposed and analyzed in Section 4. Our conclusions are given in Section 5.

II. RELATED WORKS

Even in a well-planned digital forensic investigation, challenges can arise. In the course of an investigation, digital forensic practitioners (DFPs) must identify, acquire, and preserve the key data in legally defensible ways.

2.1 Trojan Programs and Trojan Defense

Digital forensics is the application of computer science to the field of law [5]. The methods that DFPs need to apply when responding to an incident vary among different cases [6]. Investigations have to be conducted more and more quickly. The incident response team must also be aware of the disciplines of law and public relations while handling an incident [7]. In cases involving Trojan programs, it is important to understand how these programs operate, how the Trojan Defense has been invoked in legal cases, and how it can be refuted.

(1) Trojan Program

A Trojan horse or Trojan program is a non-self-replicating malware, named after the wooden horse the Greeks used to infiltrate the defenses of Troy [8][9]. A Trojan program contains malicious or harmful code and often employs a form of social engineering to persuade victims to install it on their computer. While harmful, Trojans are designed to appear legitimate and present themselves as useful or interesting attachments. Once the Trojan is installed, a hacker can use it to access the compromised computer and steal or corrupt the data stored in the computer. Data networks have become targets for electronic file theft, losing credit card data, and other sensitive information [10]. The nature of a cyberattack depends largely on the objectives of the attacker and the tools and techniques used. When an organization faces such an attack, the losses and damage may be significant [11]. An organization may receive a stream of spear-phishing emails that encourage users to open an attached file containing the Trojan program [12]. While the dangers presented by Trojans have been widely discussed in information security circles, they are challenging to defend against. LEAs need to explore the following issues: 1) Has the hacker been able to remove the evidence? 2) Did a Trojan or other malware play a role in the attack? 3) What evidence can be recovered and can it be presented in court? This paper focuses on Trojan programs and the Trojan Defense. The goal is to provide an in-depth guide to digital forensics from the work of pioneers in the field.

(2) Trojan Defense

After a literature review of relevant publications over the past decade, there are some similar court cases of Trojan Defense in USA, UK, and South Africa [13]. They are child pornography, denial of service attack, tax evasion, and so on. The Trojan Defense is a legal gambit that plays on the ignorance of judges and prosecutors, as complex technical issues must often be explained in simple terms in a cybercrime case. Numerous defendants in Taiwan have won acquittals based upon the Trojan Defense [6]. The essence of the Trojan Defense is to argue that a Trojan program (or other malware) was responsible for the crime. When a computer has been infected with a Trojan, it is under the control of an unknown hacker, thus allowing services to be run without the owner's knowledge or consent. The Trojan Defense has surfaced in several such cases [14] [15]. As the specific claim is often that the suspects had limited knowledge of information technology and were exploited by a hacker, investigators must identify, collect, acquire, and preserve data and clues. The purpose of this paper is to increase awareness of Trojan Defense and provide an in-depth guide to digital evidence review.

2.2 Trojan Defense in LEAs

As far as LEAs are concerned, they have had the opportunity to process a wide variety of crime scenes. A well-trained investigator should be knowledgeable in every aspect of a crime scene investigation. Digital evidence is easily modified, easily copied, and very volatile. In most jurisdictions and organizations, digital evidence is governed by three fundamental principles in ISO/IEC 27037:2012 [16]: relevance, reliability and sufficiency. The following issues re are four key purposes in forensic science [14]: identification, individualization/classification, association, and reconstruction. These basic skills will set the foundation for the success or failure to deal with the Trojan Defense issues.

2.3 Digital Evidence Review in Expert Witnesses Testimony

Most large LEAs have a dedicated forensic science team that not only analyzes evidence but also provides testimony in court. The team comprises experts in a specific field and may assist the LEAs or lawyers in all phases of the lawsuit. The two main types of expert in U.S. are shown in Table 1 [5]: the technical witness and the expert witness. Both will testify in court, present their findings, and describe the tests applied. However, the following differences are not clarified in Taiwan. It is also an urgent need to tackle the challenging process of seeking truth through analysis of digital evidence.

Table 1. Roles of Technical and Expert Witnesses

Item	Witness	Technical	Expert
Differences	Role definition	Write the report	Review the report
	Conduct the tests	Yes	No
	Provide an opinion	No	Yes
Similarities	Under oath	Yes	Yes
	Describe the tests	Yes	Yes
	Present the facts	Yes	Yes
	Testify in court	Yes	Yes

(1) The Technical Witness: Explaining the Procedures

Technical witnesses describe the processes by which evidence was obtained. When a piece of digital evidence is crucial to securing a conviction, the judge will wish to establish its relevance to the case. This requires the prosecution to present the process that collected and analyzed the forensic evidence.

(2)The Expert Witness: Providing Explanation and Drawing Conclusions

The job of the expert witness is not to actually perform the tests but to provide explanations or describe the conclusions that might be drawn from an evaluation of the full evidence presented. The Trojan Defense sets new challenges to the forensic community. A key point of a criminal justice system is that an innocent person should not be convicted of a crime. Digital evidence reviews are conducted, based on expert witness testimony, to improve the court's understanding of the digital forensic report, to prevent incorrect evidence from being given by incompetent experts, and to ensure compliance with standards such as ISO/IEC 17025:2005, 27037:2012, or 27043:2015 [16]. Expert witnesses need to provide a completely correct explanation of the various analyses and the inner working of the case and its interrelated components. They can process a logic analysis from beginning to end and write opinions that are based on skills, knowledge, and experience. These opinions should be based on the factual evidence.

(3) The Role of Digital Evidence Reviews in Trojan Defense Cases

Digital evidence reviews are applied to all facets of the digital forensic laboratory [8]. An internal review is a laboratory audit conducted by qualified and trained DFPs. An external review is an audit conducted by qualified and trained assessors employed by LEAs or courtrooms [5]. A quality review of the digital evidence is essential to establish the truth. If false evidence is submitted to the court, a criminal may go unpunished or an innocent person may lose his/her liberty. This study reviews the digital forensic report presented in a Taiwan Trojan Defense case.

(4) Quality Assurance Practices for Digital Evidence Review

The digital evidence review is handled on a case-by-case basis. It is essential that a digital forensic laboratory be available to confirm the reliability of the work. If the groundwork by DFPs has been done improperly, the forensic report will be of poor quality. The data-gathering process must be properly documented. The technical facilities of the laboratory and the knowledge, skills, and working methods of the staff must be clear. It is crucial to have documentation and validation processes that meet all appropriate standards and protocols in place. The following principles must guide digital forensic analysis in a laboratory environment [12]:

• Standards: Quality assurance is an important part of forensic science that is closely associated with peer review. The peer review process is

designed to identify any errors or shortcomings in the forensic findings. It ensures the quality of scientific work by opening it to examination by independent experts.

• Controls: DFPs should implement appropriate quality assurance controls to demonstrate to the court that the quality of the evidence can be trusted. As shown in Table 2, these controls take account of three factors: capable staff, acceptable processes, and appropriate technology.

• Documentation: Documentation must be generated at all stages when handling and processing digital evidence, from the point at which the case is referred to the digital forensic laboratory or LEAs [17]. Documentation is critical as it allows the digital forensic process to be reviewed in an external audit.

Table 2. Three Control Factors for Quality Assurance in Digital Forensics

Factor	Control
Capable People	• DFPs are certified through a formal and documented training program. • Staff should have the right competencies.
Acceptable Processes	• All processes meet acceptable standards for the identification, collection, acquisition, and preservation of digital evidence. • The procedures used are consistent across laboratories.
Appropriate Technology	• Technology is confirmed to be fit for purpose. • The technical standards are regularly accredited by an independent assessment agency.

III. CASE STUDY

3.1 Trojan Defense in Train Ticket Scalping Case

The Trojan Defense has been successfully deployed in a number of cybercrime cases in Taiwan, and it has become increasingly popular elsewhere. The accused might compromise his own system in order to employ a Trojan Defense in the event of capture. The case will then hinge on whether the judge believes that the computer had truly been taken over by a hacker using a Trojan program.

(1) Train Ticket Scalping Case

Ahead of long vacations, Taipei-Yilan train tickets were often fully booked within a few minutes after they were available online. After receiving complaints from travelers, Taiwan's police force launched an investigation into possible scalping. A suspect, Mr. Chiang, was found to have illegally bought blocks of tickets from the Taiwan Railway Administration (TRA) website, possibly for resale. In October 2010, he was arrested for allegedly trying to resell more than 1,382 peak season tickets for travel between Taipei and Yilan, obtained using 12 false identities. He was charged with 378 computer offenses in November 2009 for bombarding the TRA computer with thousands of electronic messages over a period of nine months. The specific charges were fraud and document forgery [6].

(2) Online Ticket Purchase System

Railways are expected to carry millions of passengers during peak periods. Taiwan's railway authorities introduced an Internet ticketing system in an attempt to end the rampant ticket scalping that typically preceded the holiday rush. A valid personal identification number allows the purchase of six tickets per route on any date, under the rules established by the TRA.

(3) Auditing the Logs of Targets and ISPs

Auditing logs are a valuable source of forensic evidence and can be useful in identifying other event-based information. Target server logs suggested that the attack came from a specific IP address. Internet service provider (ISP) records revealed the IP addresses of the computers used in the incident. This evidence trail led to the computers in Chiang's office and home. Although an order history found on these computers provided evidence, it was difficult to prove definitively that Chiang had knowingly and intentionally ordered the tickets. Table 3 gives a sample of the IE history at Oct. 29, 2010, 08:31:47–08:40:59. This was mainly reconstituted from deleted data and comprised the following [18]: "website page," "order confirmation," "order success," "cancel success," and "cancel confirmation."

(4) Rejection of Trojan Defense in Trial

At his trial, Chiang argued that a Trojan program, downloaded as an e-mail attachment, could have been responsible for the logs, although a forensic audit showed no trace of such a Trojan. The defense repeatedly demanded additional peer reviews. The case, therefore, hinged on the judge accepting the defense's argument that a Trojan could have taken control of the computer, then terminated itself. In this case, the Trojan Defense was rejected, and the defendant was sentenced to 4 years and 6 months in prison [19].

Table 3. Timeline Sample of IE History View

File Name	Attribute	Created Date-time Stamp	Digital Process
index_center[1].htm	Deleted	2010/10/29 08:31:47	Website page
railway.hinet[1].htm	Deleted	2010/10/29 08:31:47	Website page
ccancel_rt[1].htm	Deleted	2010/10/29 08:34:21	Cancel Success
ccancel[1].htm	Deleted	2010/10/29 08:35:30	Cancel Confirmation
ccancel_rt[1].htm	Deleted	2010/10/29 08:35:32	Cancel Success
check_ctno1[1].htm	Deleted	2010/10/29 08:35:34	Order Confirmation
order_no1[7].htm	Deleted	2010/10/29 08:35:41	Order Success
ccancel[7].htm	Deleted	2010/10/29 08:37:10	Cancel Confirmation
check_ctno1[4].htm	Deleted	2010/10/29 08:37:14	Order Confirmation
order_no1[7].htm	Deleted	2010/10/29 08:37:23	Order Success
ccancel[7].htm	Deleted	2010/10/29 08:38:33	Cancel Confirmation
ccancel_rt[7].htm	Deleted	2010/10/29 08:38:41	Cancel Success
check_ctno1[7].htm	Deleted	2010/10/29 08:38:43	Order Confirmation
order_no1[1].htm	Deleted	2010/10/29 08:38:50	Order Success
ccancel[1].htm	Deleted	2010/10/29 08:39:43	Cancel Confirmation
ccancel_rt[1].htm	Deleted	2010/10/29 08:39:46	Cancel Success
order_no1[4].htm	Deleted	2010/10/29 08:39:52	Order Success
check_ctno1[1].htm	Deleted	2010/10/29 08:39:55	Order Confirmation
order_no1[1].htm	Deleted	2010/10/29 08:40:02	Order Success
ccancel[2].htm	Deleted	2010/10/29 08:40:38	Cancel Confirmation
ccancel_rt[1].htm	Deleted	2010/10/29 08:40:40	Cancel Success
check_ctno1[1].htm	Deleted	2010/10/29 08:40:45	Order Confirmation
order_no1[2].htm	Deleted	2010/10/29 08:40:59	Order Success

3.2 Digital Forensic Report

This report is an inventory of the files and recovered data that are relevant to the investigation. It is tagged with file names, date–time stamps, and summaries of contents. The report makes no assumptions about innocence or guilt. Fig. 1 shows the structure of a digital forensic report from the Taiwan Criminal Investigation Bureau (part of the National Police Agency). The forensic findings have been evaluated, and a conclusion is presented below [6][19][20].

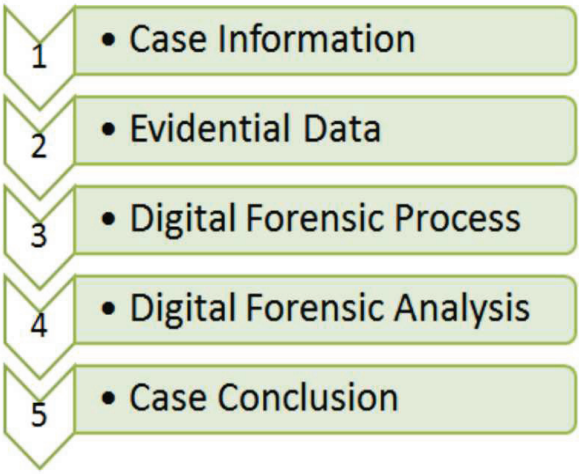

Fig. 1. The Structure of Digital Forensic Report

(1) Case Information: Locating All Relevant Data

The digital forensic investigation focused on the following three issues:

• Were there any records that showed the browsing history of the TRA website?

• Were any remote control services or Trojan programs detected?

• Were any programs for identification number generation or automated ordering detected?

(2) Evidential Data: Data Collection Standards

The following evidential data was seized.

• An unreadable hard drive (Seagate, 80 GB).

• An ASUS Notebook (HITACHI HDD, 320 GB).

• A desktop computer (NetVista) without a hard drive.

(3) Digital Forensic Processing of Evidence

The digital forensic process requires a deep technical understanding and know-how of technical tools such as Encase or FTK for converting a large volume of evidence into a presentable case. The process has the following six steps: identification, collection, acquisition, preservation, analysis, and reporting. While forensic errors may lead to a suspect being falsely incriminated, it should be noted that the error rate can never be reduced to zero. Errors can, however, be minimized. An audit trail or other record of all procedures should be created and preserved for examination by independent third parties [5]. The chain of custody begins when the evidence is collected and ends when it is presented in court.

(4) Digital Forensic Analysis: Describing the Events

Keyword searching is utilized to identify potentially important areas of the data. The findings of the Taiwan Criminal Investigation Bureau were as follows [6][19]:

• Browsing Records: Twelve social security numbers were found among 3,527 browsing records. These numbers had been issued to the employer of the accused and to family members.

• Records of Access to the Target Server: The accused's computers contained records of 3,242 events involving the target server (railway.hinet.net, 210.71.181.60).

• Limited Event Records involving target logs: Event logs were only recovered for a period of ten days from April 6–15, 2011. This did not cover the period in which the alleged offenses had taken place (November 12, 2009–August 11, 2010).

• Inactive Remote Control: The Windows remote control service had been inactive.

• No Active Trojan Running: No evidence of active Trojan programs was found in the Microsoft AutoRun records.

• No Active Trojan Network Packets: No evidence of active Trojan programs was found in the Wireshark (v1.6.5) data.

(5) Case Conclusion: Presenting the Findings

• The records showed many successful logons to the TRA website.

• No remote control services or Trojan programs were found.

• No social security number generators or automated ordering programs were found.

3.3 Logic analysis on Trojan Defense Case

Good logic and critical thinking are core skills to provide sound opinion or determine the correctness of arguments on the crime analysis of Trojan Defense case. A conclusion is made from the following two types of arguments [21]: deduction and induction. Deductive argument moves from a general premise to a specific conclusion. Inductive argument moves from specific premises to a general conclusion. These two arguments try to solve mysteries based upon the observations of minute details. These two arguments are about using the philosophy and techniques of logic reasoning to determine true/false conclusions and probable inferences [22]. Inductive argument is of great importance when the cybercrime investigation cannot be proved by deduction alone. The value of data, information, or evidence can be enhanced further by logical analysis. It is reasonable to identify the accused guilty from the following analysis in this case (Fig. 2).

(1)Deductive Argument: Valid Logical Link on Sound Connections to a Specific Conclusion

Deductive arguments assert that it is impossible for the premises to be true and the conclusion false [21]. In deductive arguments, the truth of one's premise is strictly sufficient to establish a valid logical link on sound

connections to a specific conclusion. When users send data to the server over the Internet, login messages are often delivered over TCP in a reliable manner. The following information is related to TCP connections: Source port, Destination port, Source IP address, Destination IP address, connection time, and so on. In this case, the auditing information from victim servers help identify the accused's devices at home and office. Evidence from the above devices also matches the victim server data.

(2)Inductive Argument: Strong Logical Link on Cogent Construction to a General Conclusion

In inductive arguments, the series of connections are weak and there should be enough of a nexus to support or refute a conclusion [22]. A strong logical link on cogent construction is necessary to draw a general conclusion. A hypothesis in inductive arguments is either constructed based on evidence or generalized based on mathematical probability. In this case, evidences show that the offense is initiated from the accused location (home and office) and false positives error rates are reasonably low. Each time a suspect IP address is detected and recorded in log files when this offense has occurred. An IP address in IPv4 is a 32-bit number that identifies each sender or receiver across the Internet. Since this pool is 32-bits (2^{32}) in size and contains 4,294,967,296 IPv4 addresses, false positives error rates, where a non-suspect IP address is detected as suspect, are reasonably low from different day-by-day sources.

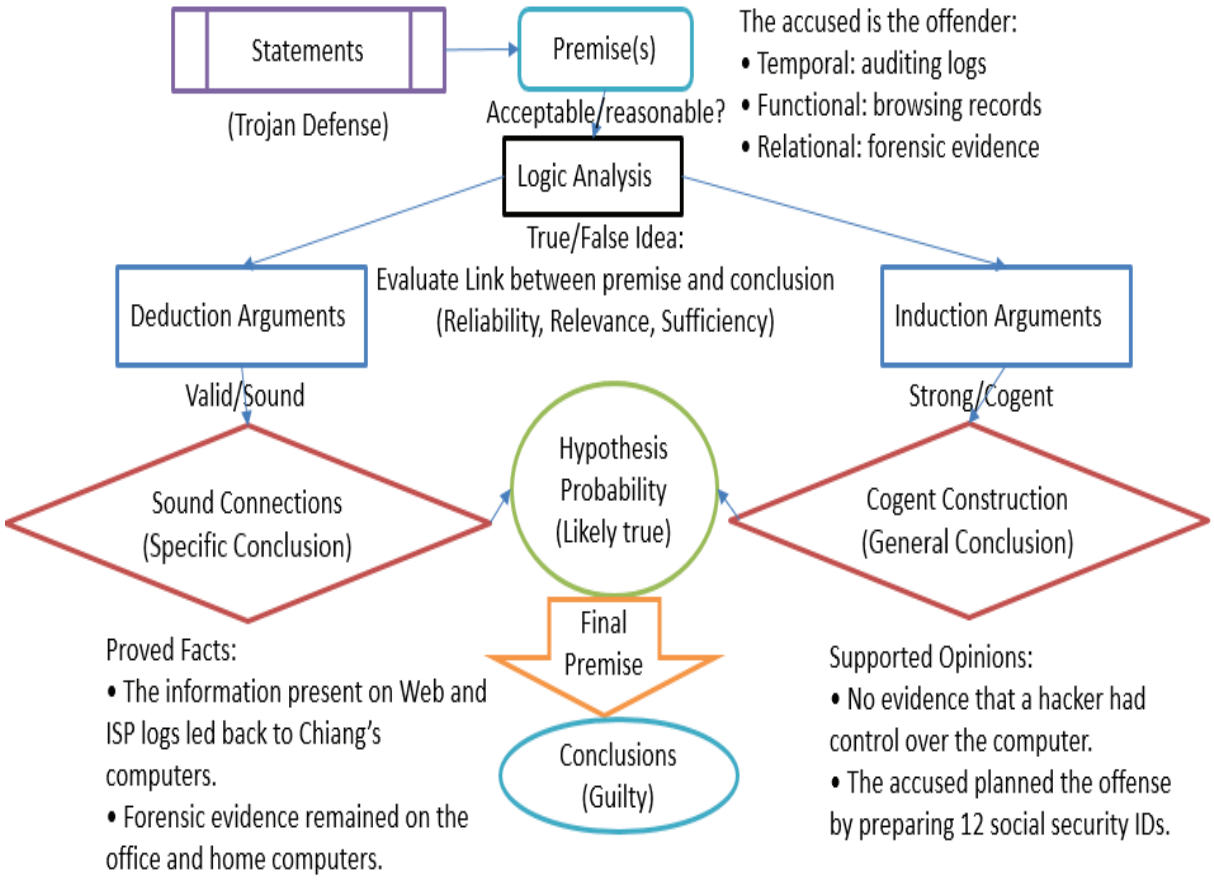

Fig. 2. Logic Analysis on Trojan Defense Case

3.4 Follow-up: Strengthening the Law in Taiwan

(1) Revised Taiwan Railway Act

The Taiwan Railway Act was promulgated by Presidential Decree on January 3, 1958. On Nov. 9, 2016, Article 65 was amended to cover such cases. The revised Article states that any person conspiring to profit from the reselling of tickets shall be fined five to thirty times the value of the tickets. The act of purchasing tickets by illegally inputting personal identification data shall be punished by imprisonment for not more than five (5) years and/or a fine of not more than NT$3,000,000 [23]. The revised Act thus raised the penalties for scalping, with additional fines if a computer system is used.

(2) Additional Protection of Online Ticket Purchase System

The TRA also improved the security of its ticket purchasing system [24]. The four-number confirmation code was increased to between four and six numbers.

IV. THE PROPOSED IPU MODEL FOR DIGITAL EVIDENCE REVIEW

Every case is different and demands different approaches to investigation. The forensic analysis of each case requires an extensive evaluation of the temporal, functional, and relational robustness of the data sources. The case files should allow others to replicate and verify the results [14]. The comprehensive reports used in a Trojan Defense can apply the IPU model developed by the present author. As shown in Fig. 3, this ensures that no key aspects of temporal data, functional analysis, and relational analysis used for crime reconstruction are omitted from the final presentation. An expert witness may work recursively, moving back and forth between the following three stages: 1) identify temporal data to build the sequence (when), 2) perform functional testing to gain insights (how), and 3) understand relational reconstructions to clarify the actions (who, what, where). The cycle times around this IPU wheel will depend on the scope of the evidence review and on the volume of evidence to be reported. By applying the IPU model, DFPs can minimize the risk of errors entering the process, as it encourages them to cycle through many tests or analyses until a solid report emerges. A Trojan Defense requires a particularly rigorous analysis as it will determine the guilt or innocence of the accused [12]. The goal of this IPU model is to ensure that the guilty are convicted and the innocent acquitted.

4.1 Identify Temporal Data to Build the Sequence (When)

The temporal aspects of digital evidence are obviously important, as it is necessary to establish the sequence of events and patterns in time. The record of temporal events allows LEAs to reconstruct past crimes [14][5].

(1) Seeking Out Data Sources

A single case may involve many criminal events. The temporal data is the primary resource allowing the events to be reconstructed. The nature of the cybercrime will frequently suggest the places in which incriminating data should be sought. A careless criminal will often leave clues to their identity in the logs of the target or ISP. In this case, this did not directly lead to an arrest but did provide initial evidence [23]. This digital forensic report gives an overview of the evidential media and provides a summary of the processing methods and tools used. It also describes the items of digital evidence used, including MD5 algorithm, photographs, and laboratory codes. For example, using MD5 values as a form of hashing for digital forensic work is acceptable in court. This forensic hash is a form of a mathematical calculation checksum, which is used for the identification, verification, authentication, and integrity of file data.

(2) Scoping the Evidence

This is the process by which the evidence is surveyed to gain a better understanding of the overall case [20].

• Auditing the Logs: A Trojan program may be designed to wipe itself from the hard drive after carrying out the attack [15]. However, it is essential to scan for malware, monitor for unusual activities, and review auditing logs. These may reveal evidence or clues that support

or refute the Trojan Defense.

• Avoiding Evidence Contamination: The defense may argue that evidence has been contaminated. The following strategies can be used to ensure that this does not happen [5]: 1) Data integrity should be preserved while developing the case. 2) The forensic workstations should not be connected to external networks. 3) The digital forensic laboratory must be secured from unauthorized access. 4) The digital forensic laboratory must be provided with adequate fire protection, flood protection, temperature, humidity control, and an uninterrupted power supply.

(3) Checking Consistency and Inconsistency

The presentation of evidence in cybercrime cases is challenging. One of the best ways of discovering the truth is to check for consistencies and inconsistencies. The investigation proceeds iteratively until the DPFs have determined exactly what occurred and can provide supporting data. The presence of a Trojan on a computer system should raise concerns but cannot halt an in-depth analysis of the evidence.

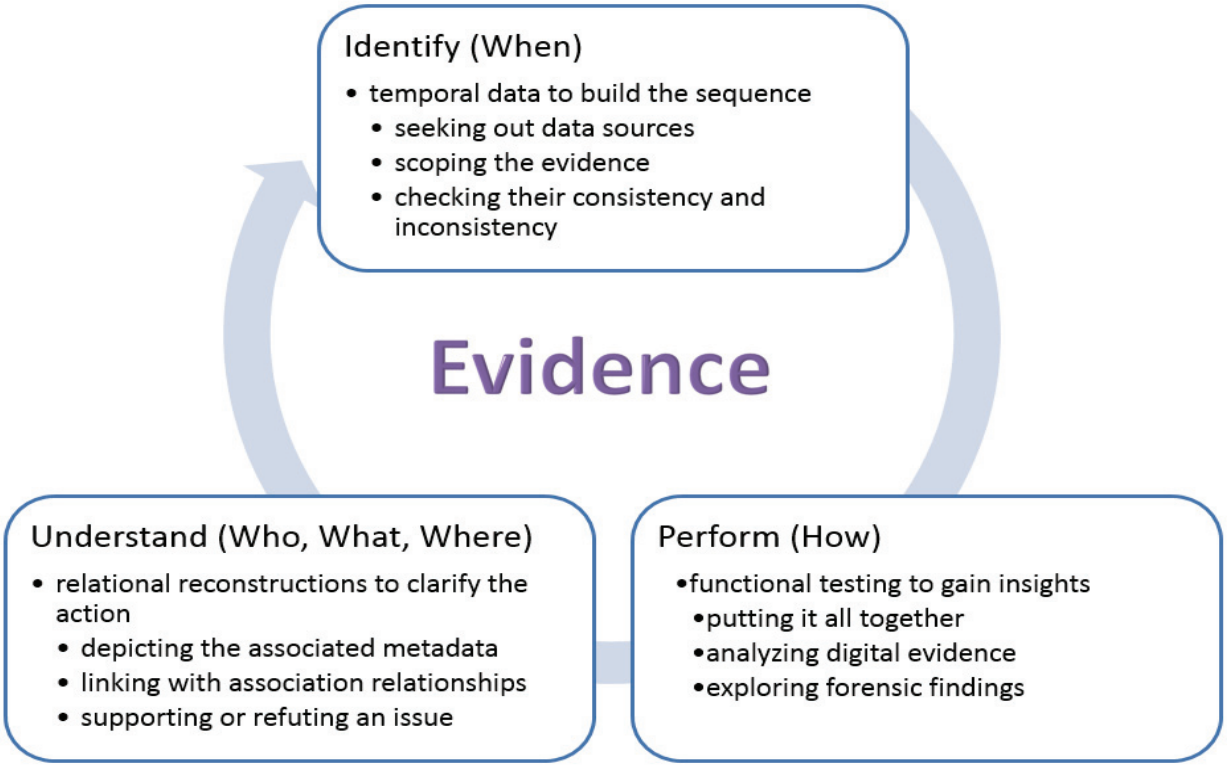

Fig. 3. Proposed IPU Model for Digital Evidence Review

4.2 Perform Functional Testing to Gain Insights (How)

The manner in which digital evidence is used will determine the choice of evidence. It is essential to perform functional testing to determine if the accused's computer was capable of executing the offenses that are presented as incriminating evidence [14]. If the target server requires users to enter a social security ID, the number of user accounts that could have accessed the server is limited. A function is described as a set of inputs, behaviors, and outputs [8]. These may be technical details, data manipulation or processing, or other specific functionalities defined by the uses for which the system was designed.

(1) Putting It All Together

Digital data can take the form of deleted files, file fragments, and the contents of memory. The full case will use multiple pieces.

Cross-confirmation adds veracity to the findings [5]. The absence of evidence of hacking, malware, Trojans, or keylogger programs on Chiang's computer was used to counter the Trojan Defense. An effective way to detect Trojans is to run multiple antivirus software programs in a laboratory environment. Wireshark can be used to detect the presence of malicious software within a captured file if the software has a known signature.

(2) Analyzing Digital Evidence

The complexity of Trojan Defense cases arises from the unstructured nature of digital evidence. An investigation may not allow all data to be completely analyzed. Techniques exist for eliminating data, making the dataset more manageable [20]. Data reduction is the process that converts the evidence to a simpler form. It can increase efficiency and reduce the cost of the investigation.

(3) Exploring Forensic Findings

The findings must be based on evidence. The report describes the forensic analysis and supporting evidence. Table 4 shows how a temporal, functional, and relational analysis was used to reconstruct the events in the ticket scalping case. There were three crime scenes: the TRA website and Mr. Chiang's home and office. The analysis built up an event timeline from different logs, functional connections, and the relation between the suspect and target.

4.3 Understand Relational Reconstructions to Clarify the Action (Who, What, Where)

The relational reconstructions of evidence are critical to explore the crime, understand important details, and make informed decisions [14]. Relational analysis tracks the relations between objects.

(1) Depicting the Associated Metadata

Many types of legal digital evidence exist in a single case, including data, records, files, information, and other logical data sources. Evidence can be provided not only from the contents of the logical data containers but also from associated metadata. Metadata is information about other data and can be useful when forming a story about when, how, who, what, and where. Many data sources on a computer system can indicate whether a particular action was initiated by a computer program or intentionally by the user. Computer-generated (non-artifact) records are created by a running program, whereas computer-stored (artifact) records are generated by the user [7]. Creating a diagram to map the associations between the criminal and the computers can reveal patterns, allowing LEAs to clarify the chain of events [14]. To prove that somebody has hacked into a computer, DFPs can provide auditing logs, identify consistent activities, and clarify issues of concern. When data from multiple records are merged into a single case, multi-relational record linkage is the preferred approach.

(2) Linking with Association Relations

As the use of Trojan programs by hackers has become more widespread, Trojan Defense has been deployed in an increasing number of cybercrime cases. LEAs face a key challenge in demonstrating the relational findings when building a prosecution case. A Trojan program may masquerade as something else, but certain clues are available. The known file hashes of Trojan horse programs provide a good starting point for detecting their presence [5].

(3) Supporting or Refuting a Defense

Digital forensics relies on evidence to provide proof of the facts in the case. Evidence may be presented in court to support or refute a claim by the defense. It is relatively easy for a malicious criminal to plant electronic evidence that frames an innocent party, thus making it difficult to prove guilt using digital evidence, which is not as immutable as physical evidence. Detecting the activity of a Trojan requires data from multiple sources to be correlated in order to identify anomalies [5]. A digital evidence review can give the judge greater confidence in the testimony of an expert witness. The technical analysis of the accused's computer can confirm or refute the presence of malware. A thorough analysis is needed to determine whether a Trojan may have contributed to the criminal act [10].

- Supporting the Defense: If DFPs identify the presence of Trojans on the accused's computer, this may support a plea of innocence.
- Refuting the Defense: If no Trojan is found, the prosecution can use this fact to rebut the defense.

Table 4. Forensic Findings from Supporting Evidence

Analysis	Supporting Evidence	Findings
Temporal (When)	• This offense happened during the period from November 12, 2009, through October 29, 2010. • No offense occurred in TRA website logs during the period from January 17, 2010 through August 11, 2010.	• Web (target)/ISP (third party) logs recorded events day by day. • No evidence that a hacker had control over the computer. • LEAs could identify sequences and patterns in events.
Functional (How)	• Browsing records were recovered from TRA website. • No remote control service or Trojan program was found. • No identification number generator or automated ordering program was found.	• The digital evidence of browsing records can shed light on what happened. • No sign of Trojan program. • No proper explanation of events from the accused. • LEAs can perform functional testing to ascertain what was possible and impossible.
Relational (who, what, where)	• 3,242 victim server data in 3,257 browsing records. • 1,382 tickets purchased in 378 offenses using 12 false identities.	• The information present on Web (target) and ISP (third party) logs led back to Chiang's computers at office and at home. • The accused planned the offense by preparing 12 social security IDs. • Through carelessness, forensic evidence remained on the office and home computers. • LEAs could perform relational reconstructions to determine the interaction between the components of the case.

4.4 Reconstruct the Events

Table 4 shows how a temporal, functional, and relational analysis was used to reconstruct the events in the ticket scalping case. This Trojan Defense argument is bad and unthoughtful from the following findings [8][14].

(1)Temporal Analysis

Temporal clues are based on the passage of time. In this case, logs recorded events day by day. Temporal analysis can create a timeline to help investigators identify events, patterns and gaps, potentially leading to other sources of evidence at office or home.

(2) Functional Analysis

Functional clues are how a particular job or application works, how it was used, or how it was configured at the time of the crime. The digital evidence of browsing records can shed light on what happened in this case. It is necessary to gain a better understanding of

digital evidence in Trojan Defense investigations.

(3) Relational Analysis

Relational clues can include the geographic location of people and computers, as well as any communication/transaction that occurred between them. Relational analysis can reveal a crucial relationship about where relevant persons are located and how they interact. In Trojan Defense investigations, it can be useful to create a list of IP-to-IP connections and determine the interaction between components of a crime. In this case, the information present on Web (target) and ISP (third party) logs led back to Chiang's computers at office and at home. Moreover, forensic evidence remained on the office and home computers. If two source computers (at office and home) are only accessed from a small range of users, this limits the number of suspects that could have been used to commit the crime.

V. CONCLUSIONS

Reconstruction of the cybercrime scene plays a critical role. If LEAs and other authorities do not stay on top of this problem, they may lose the battle to fight against this Trojan Defense. DFPS need to process evidence as quickly and efficiently as possible. The novel identify/perform/understand (IPU) model supports this, allowing the digital evidence to be summarized, Trojans to be detected, and the guilt or innocence of the accused to be determined. In Trojan Defense cases, the three phases of IPU model should be followed to ensure high standards of digital forensics. A reviewer has the right to request further investigation into any nonconformities identified, on an as-needed basis. This further investigation may be performed by the original investigator or another designated DFPS. The challenges of Trojan Defense cases and the quality required of the evidence may be addressed using the IPU model. It is believed that this proposed approach creates a comprehensible guide that provides support and assistance to LEAs. Potential enhancements to the model will be investigated in future studies.

ACKNOWLEDGMENT

This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-107) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 105-2221-E-015-001- and 106-2221-E-015-002-.

REFERENCE

[1] Roger, A. E. and Achille, M. M., "Multi-Perspective Cybercrime Investigation Process Modeling," International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, New York, USA, vol. 2, no. 2, June 2012.

[2] Andress, J., Winterfeld, S. and Ablon, L., Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2nd Edition), Burlington, MA, Elsevier Inc., pp. 181-192, 2014.

[3] Luttgens, J. T. and Pepe, M., Incident Response & Computer Forensics (3rd Edition), New York: McGraw-Hill Education, pp. 1-50, 2014.

[4] Bunting, S., EnCase Computer Forensics: The Official EnCase Certified Examiner Study Guide, (3rd Edition), Indianapolis, Indiana, John Wiley & Sons Inc., 2012.

[5] Stephenson, P., Official (ISC)2® Guide to the CCFP CBK, Boca Raton, FL, Auerbach Publications, pp. 293-404, 2014.

[6] Lin, R., "Digital Forensics Report in Criminal Investigation Bureau (Case Number: 101100009)," Taipei, Taiwan, Criminal Investigation Bureau, Nov. 2012.

[7] Brooks, C. L., CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide (1st Edition), New York, McGraw-Hill Education, pp. 13-50, 2015.

[8] Casey, E., Handbook of Digital Forensics and Investigation, Burlington, MA, Elsevier Inc., pp. 21-208, 2010.

[9] Davidoff, S. and Ham, J., Network Forensics: Tracking Hackers through Cyberspace, Upper Saddle River, New Jersey, Pearson Education, Inc., pp. 1-72, 2012.

[10]Vacca, J. R., Network and System Security (2nd Edition), Burlington, MA, Elsevier Inc., pp. 29-189, 2014.

[11]Oriyano, S. P., CEH v9: Certified Ethical Hacker

Version 9 Study Guide (3rd Edition), Indianapolis, Indiana, John Wiley & Sons, Inc., pp. 1-222, 2016.
[12]Johnson, L., Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response, Burlington, MA, Elsevier Inc., pp. 97-184, 2013.
[13]Bowles, S. and Hernandez-Castro, J., "The first 10 years of the Trojan Horse defence," Computer Fraud & Security, pp. 4-13, Jan. 2015.
[14]Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition), Waltham, MA, Elsevier Inc., pp. 187-306, 2011.
[15]Shahabi, C., Kim, S. H., Nocera, L., Constantinou, G., Lu, Y., Cai, Y., Medioni, G., Nevatia, R., and Banaei-Kashani, F., "Janus - Multi Source Event Detection and Collection System for Effective Surveillance of Criminal Activity," Journal of Information Processing Systems, vol. 10, no.1, pp. 1 - 22, Mar. 2014.
[16]International Organization for Standardization (ISO), ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, Switzerland, ISO Office, 2012.
[17]Raghavan, S., "A Framework for Identifying Associations in Digital Evidence Using Metadata," Brisbane, Queensland University of Technology, pp. 73-124, 2014.
[18]Pande, P.V., Tarbani, N. M., and Ingalkar, P.V., "A Study of Web Traffic Analysis," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3, no. 3, pp. 900-907, 2014.
[19]Taiwan Judicial Yian, "Law and Regulations Retrieving System," The Judicial Yian of the Republic of China, http://jirs.judicial.gov.tw/FJUD/.
[20]Sremack, J., Big Data Forensics - Learning Hadoop Investigations, Birmingham, UK, Packt Publishing, 2015.
[21]Girod, R. J., Logical Investigative Methods: Critical Thinking and Reasoning for Successful Investigations, CRC Press, pp.25-36.
[22]Baker, S. F. The Elements of Logic, 2nd ed. McGraw-Hill Book Company, New York, 1974, pp.16-224.
[23]Taiwan Ministry of Justice, "Law & Regulations Database of The Republic of China: Taiwan Railway Act, " http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=K0030001.
[24]Taiwan Railways Administration, "Hot News," http://www.railway.gov.tw/.