Intellectual Property Rights: Open Access

Kao, Intel Prop Rights 2016, 4:2
DOI: 10.4172/2375-4516.1000167

Research Article Open Access

A Fight for Copyright Infringement: Uncovering Covert Identifiable Data behind Computer Software

Da-Yu Kao*

Department of Information and Management, Central Police University, Taiwan

Abstract

Commercial Intellectual Property (IP) is under constant assault in size and complexity. Criminals are exploiting Information and Communications Technology (ICT) advances to produce copies from copyright holders. While the Internet has empowered internal users or former employees to steal codes, sell to the adversary or seek revenge, it has also exposed users to new forms of criminal activity and copyright infringement. The study proposes an ICT governance framework to hide identifiable data behind the computer software and fights against future copyright infringement. Identifiable data isolates a person or an organization by unique traits so he or she is not confused with or wrongly identified as someone else. It helps Law Enforcement Agencies (LEAs) identify the copyright holder of computer software. It is essential for copyright holders to embed some identifiable data, and fight against the rise of the copyright infringement. In this study, a data hiding strategy is proposed and ICT governance is discussed as a framework to fight against future copyright infringement.

Keywords: Law enforcement agencies; Intellectual property; Copyright; Infringement; Information hiding; Anti-digital forensics; Cybercrime investigation

Introduction

Increasing interconnectivity and globalization of cybercrime are driving great frequency and severity of cyber incidents, including Intellectual Property (IP). IP is now a major threat to copyright holders, who increasingly face the new exposures of online risks. Criminal enforcement of IP rights has always been debated, mainly because of the sensitivity of criminal law harmonization and particularly because of the extent to which enforcement of IP rights should be subject to criminal law [1-5]. Even when works are protected, there are important social uses that should not be within the control of the copyright holder. Many of these measures are designed to grow the knowledge; others recognize the cumulative nature of knowledge production and free material for the enjoyment of future generations [6]. This study examines cyber risk trends in IP around the globe. The human factor can be regarded as the greatest threat to IP. This risk may be high on the Internet, where the criminal could freely access vast quantities of confidential information. Lack of successful arrest or prosecution means it can be difficult to reduce the risk to IP [4].

Computer software is a program that tells a computer how to do. These digital instructions might be internal commands, encoded information, or a response to external input received from the keyboard or mouse. Computer software can be loaded into the hard drive or storage [1,3]. There is also the chance to hide some identifiable data by copyright holders. Once the software has loaded, the computer is able to execute the program. The sheer amount of information to collect to find relevant data can be enormous. Law Enforcement Agencies (LEAs) will be overwhelmed at the start of an investigation if copyright holders file a lawsuit [3,7-12]. Determining the methods of authorship identification is a constantly changing effort in every investigation as copyright holders change methods. The goal of initiating a crime investigation is to complete successfully the case with a positive outcome which can prosecute criminals, or reduce the risk of an incident from reoccurring [4]. Due to the convenience of software modification, copyright holders can add some identifiable data in their products. Information hiding techniques can be used to prove their authorship. This will help investigators to analyze the collected information or evidence.

The rest of the study is organized as follows. Intellectual property and identifiable data embedding with anti-digital forensics methods are discussed in Section 2. Section 3 describes online challenges for intellectual property and cybercrime investigation. The proposed Information and Communications Technology (ICT) governance framework and the strategy of hiding identifiable data behind computer software are presented in Section 4. Conclusions are given in Section 5.

Reviews

Businesses that invent or create something new will seek Intellectual Property (IP) protection for their inventions [9]. With the rise of Internet file sharing methodologies, much of IP theft springs up like mushrooms and results in the difficulty of law enforcement.

Intellectual property

IP theft costs businesses billions of dollars a year and the nation of tax revenues are also on the decrease. Governments, private firms, and civil society organizations are increasingly seeking to compel these intermediaries to take more responsibility to prevent or respond to infringements of IP rights [8]. The IP theft of computer software robs people of their inventions and creative expressions. Eradicating IP theft should be a priority of the criminal investigative program for the bright future. IP has become ubiquitous in an age of information, despite a long history of being considered ideologically antithetical to traditional academic values of openness and sharing. In Table 1, copyright focuses on expressions, trademarks on information, patents on innovation, and trade secret primarily on commercial value [8,9,12]. The financial

***Corresponding author:** Kao D, Associate Professor in Department of Information and Management, Central Police University, Taiwan, Tel: +886-955313443; Fax: +886-3277600; E-mail: camel@mail.cpu.edu.tw

Received September 02, 2016; **Accepted** September 23, 2016; **Published** September 30, 2016

Citation: Kao DY (2016) A Fight for Copyright Infringement: Uncovering Covert Identifiable Data behind Computer Software. Intel Prop Rights. 4: 167. doi: 10.4172/2375-4516.1000167

Branch	Focus	Use	Motives
Copyright	Expression	Original works	Anonymity, Pricing, Shopping experience, Unavailability, or Usefulness
Trademark	Information	Recognizable products	
Patent	Innovation	Limited duration	
Trade secret	Confidentiality	Commercial value	

Table 1: Four major branches in IP law.

benefit of IP is enormous. Some of the motives for engaging in IP threats are anonymity, pricing, shopping experience, unavailability, or usefulness [12]. Considerable efforts and strategies should be tried to link the private sector with law enforcement partners on local, state, and international levels. IP law has the following four major branches [2,11]: copyright, trademark, patent, and trade secret (Table 1).

Copyright: A copyright protects original artistic and literary works of authorship. Common lawsuit materials online are computer software, songs, movies, and electronic games. It may even be possible to bring an ancillary claim for copyright infringement if the bad acts of the criminal involve the reproduction or distribution of copyright infringement [9]. The reproduction right is one of the most important rights granted by the copyright act. Under this right, no one other than the copyright holder may make any copies of the work. Examples of unauthorized acts include copying a computer software program, and incorporating a portion of another's song into a new song. The application of copyright exhaustion to digital works will be of continued importance as more content migrates to electronic formats. The purchaser could resell the protected work as embodied in a physical medium as long as no new copies were made [8].

Trademark: A trademark is a recognizable name, phrase, symbol, design, or other device used to identify the commercial product of the goods. An officially registered name or symbol is thereby protected against unauthorized use [9]. The trademark owner can be an individual, business organization, or any legal entity. Trademark evolves to include attributes such as appearance, motion, scent, sound, smell, taste, and touch [8].

Patent: A patent is a limited duration property right relating to a useful invention, including processes, machines, manufactures, and compositions of matter. Information that is disclosed in a patent cannot be considered confidential or a trade secret [9]. An invention is granted to a specific technology problem by a sovereign state in exchange for public disclosure of the invention. In a patent infringement dispute, if the alleged infringer can prove that the technology or design exploited is actually practicing a prior art, the exploitation shall not constitute a patent infringement [8]. A patent is essentially a financial instrument that entitles its bearer to achieve greater than competitive market rates of return on investment [7].

Trade secret: A trade secret is a formula, practice, process, plan, design, idea, pattern, commercial method, or any confidential information from all types of businesses. The secret gives the business a competitive edge. If trade secret protection is too strong, it may prevent the public disclosure of important knowledge upon which others can build in the future [9]. An argument of acquisition from public sources may be made by the criminal. Theft of trade secrets damages the economic base of a business. Trade secret should meet all of the following requirements [8]: (1) is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (2) has commercial value because it is secret; (3) has been subject to reasonable steps to keep it secret.

Identifiable data embedding with anti-digital forensics methods

Digital evidence can be obfuscated through anti-digital forensics methods [3]. Anti-digital forensics is the attempt to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct [1]. Everything is a double-edged sword. Copyright holders can utilize the anti-digital forensics to digital media in order to validate factual information or protect one's IP right for judicial review. The technique, method or tool of anti-digital forensics can also protect copyright holders from criminals. Information hiding is known as data encapsulation or data hiding. Technology allows for a wide range of information hiding methods, such as cryptography, watermark, and steganography [1].

Cryptography: Cryptography or cryptology is the practice of techniques for secure communication in the presence of third parties. Applications of cryptography include ATM cards, computer passwords, and e-commerce [3]. In the digital age cryptography exists at the intersection of mathematical theory and computer science practice. Cryptography can play an essential role in digital management or copyright infringement. For example, a cryptographic hash function is a mathematical algorithm that maps data of arbitrary length to a bit string of a fixed length. It is designed to be infeasible to invert and impossible to turn a hash back into its original string.

Watermark: A watermark is the process of hiding digital information, which is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its authorships [10]. It is typically used to trace copyright infringement or identify their authorships. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique can be used to detect the source of copyright infringement.

Steganography: Steganography is the practice of concealing a file or message within another file. It is the art of hiding data or covert communication. The purpose of steganography hides the existence of a message from a third party [10]. Both steganography and digital watermark employ stenographic techniques to embed data covertly in noisy signals. Whereas steganography aims for imperceptibility to human senses, digital watermark tries to control the robustness as top priority.

Online Challenges for Intellectual Property and Cybercrime Investigation

Criminals are exploiting ICT advances to produce copies from copyright holders. The type of Intellectual Property (IP) counterfeited is changing constantly in line with modern market trends. Online challenges for IP and cybercrime investigation are explained as follows.

Increasing cybercrime issues on copyright infringement

Profit-oriented motives of cybercriminals: Initially, the main motive of cybercriminals was amusement or curiosity while nowadays they operate primarily for profit or money. Copyright infringement is getting cleverer than before. Computer software and copyright infringement have become inseparable. Unlike the traditional forms of IP crime, the copyright infringement in computer software is able to act without leaving a fingerprint, or allowing for direct attribution for

their actions. The majority of copyright infringement directly enables the gain of financial resources, especially from computer software.

Mutual cooperation between LEAs and copyright holders: The regulation of cyberspace within criminal law lags behind ICT development. There are also problems related to mutual cooperation between LEAs and copyright holders in the fight against cybercrimes or copyright infringement. Copyright holders must be acquainted with the manifestations of cybercrime or copyright infringement in order to reduce fear of it and to raise awareness of its existence.

Effective tradecraft to find evidence: There is no need for potentially physical access, and the exploitations of copyright infringement can occur outside of the reach of local LEAs. Investigators require hard work, intuitive decision-making, reasonable interpretation of evidence, and sometimes chance. Finding evidence to develop intelligence is difficult and requires effective tradecraft [1,3]. The increasing interconnectivity of cyber-crime has driven the severity of IP theft. There is no silver bullet solution for IP theft. It is necessary to prevent the possibility of an unauthorized person from getting access to them. Copyright holders should keep sensitive files secure, share confidential documents with password-protected links, or set expiration dates on shared links. It is recommended to take extra care when they store or share such data [5].

Cyber intellectual property

Rampant copyright infringement: Commercial IP is under constant assault in size and complexity. Even though copyright law protects any original creation of the copyright, copyright infringement of computer software is still rampant in computer related businesses. When international IP law is practically nonexistent, cyber IP criminals can disappear in seconds. The human factor is the greatest threat to a computer system or copyright infringement. Due to ignorance, ICT employees or programmers may access to the source codes of their products. Unauthorized access may be facilitated by internal users or former employees, who could steal codes, sell to the adversary or seek revenge.

Difficult prosecution for intellectual property pirates: IP pirates can steal vast amounts of copyrighted material on the Internet, and cause severe damage to the victimized companies. The amount of cybercrime is growing steadily due to the expected financial benefits. Copyright holders have experienced difficulties in effectively enforcing their interests because criminals are dispersed across the globe. The costs of IP pirates are minimal, but profits are huge. Internet pirates target copyright materials, trademark, patent, or trade secret. Much of the activity spans multiple jurisdictions, and the regulatory power of each state is confined to its own territory and judicial system [6]. People are tricked by IP crimes into buying pirated editions. IP pirates have also merged as a market of financial driven, highly organized, and sophisticated groups [1]. Arrest and prosecution of IP crimes on the Internet is difficult for LEAs. To overcome these hurdles, right holders should look for a workable strategy.

Great care to access data: In modern work habits, the abuse of copyright infringement is happening due to the ignorance of people. Great care can be awarded to the individuals' authorization to access sensitive data in the research and design team of computer software since this can reduce the number of copyright infringement and keep instances of copyright abuse to a minimum [1]. Criminal law suits differ from civil lawsuits in that criminal prosecutions carry an emphasis on punishment, whereas civil litigation emphasizes compensation for the plaintiff [2]. Filing a lawsuit is a troublesome job that copyright holders should consider as a last resort if all else fails and the infringer continues unauthorized use of computer software.

The Proposed ICT Governance Framework to Fight against Copyright Infringement

The incident investigation principles and processes in ISO/IEC 27043:2015 has proposed a ten-activity set of cohesive tasks to deal with digital evidence. The ten activities include [7]: Plan, Prepare, Respond, Identify, Collect, Acquire, Preserve, Understand, Report, and Close. The proposed ICT governance framework and the strategy of hiding identifiable data behind computer software are presented in Figure 1. This framework is initiated from these incident investigation activities in ISO/IEC 27043:2015, and is further discussed and analyzed in the following three phases: Prelusion, Incident, and Aftermath. The viewpoints from People, Process, and Technology also become an essential part of this ICT governance framework [6] (Figure 1).

Prelusion phase: Initiate an investigative readiness in ICT governance

If the identifiable data of computer software is recognized, criminals will exhaust possible means to delete or modify it. Preventing

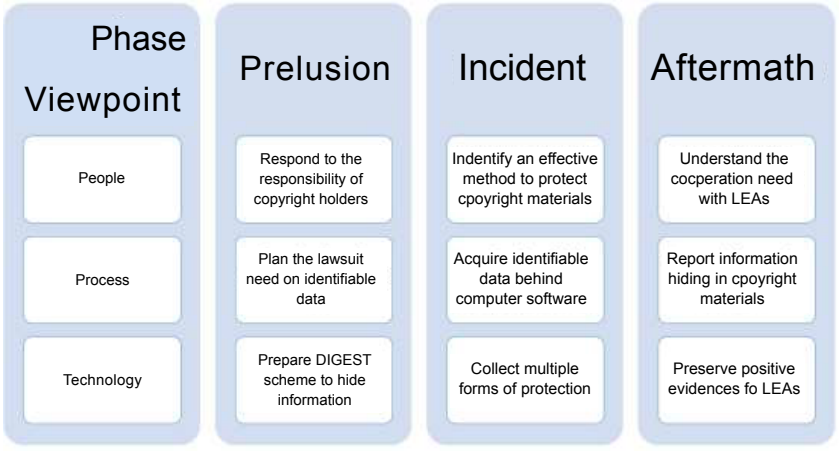


Figure 1: The proposed ICT governance framework to fight against copyright infringement.

it from being recognized in the first place is the primary goal of any copyright holders that wish to remain undiscovered and evidentiary. If the identifiable data can be collected in the investigation process of law enforcement, it will stand a good chance to support or refute criminals' misdeed. This also intends to serve to increase investigative needs in order to fight against IP theft. Implementation of ICT governance should be consistent with copyright holders' management style and the way they deal with risk. Since ICT can have a dramatic effect on business performance and competitiveness, a failure to manage ICT effectively can have a serious impact on the business as a whole. Each follow-up analysis in ICT governance framework is divided into three viewpoints: People, Process and Technology.

People: Respond to the responsibility of copyright holders: Internal users or former employees can commit copyright infringement of computer software in one or more locations while they never have to be physically present at any of them. Copyright infringement reproduces, distributes, displays or performs derivative works without permission from right holders [2,9]. While the evidence collection generally turns into the responsibility of copyright holders, they should pay more attentions on how to implement identifiable data in their copyright materials. They are acutely aware that if their codes are stolen, their computer software will be easily copied or modified. They may suffer financial losses or face financial difficulties.

Process: Plan the lawsuit need on identifiable data: An identifiable data in computer software can identify the copyright holder and reveal the evidence needed when he or she files a lawsuit. Finding identifiable data contains evidence of copyright infringement is important for investigators, and it will lead to identifying the extent and nature of copyright holders. As the identifiable data can be found or recovered through a copyright infringement investigation, the goal is to tie the identifiable data to a real person or organization. Identifying the computer software takes a digital approach as the identity evidence of authorships is digital, not physical. That identifiable data of digital information can be created by simple virtue of the copyright holder. Identifiable data isolates a person or an organization by unique traits so he or she is not confused with or wrongly identified as someone else.

Technology: Prepare DIGEST scheme to hide information: Identifiable data can be protected (cryptography), identified (watermark), or hidden (steganography) in metadata, digital files or registry settings. It is a key factor in any investigation of copyright infringement in order to identify the authorship, provide evidential value and prevent future crimes. Investigations benefit greatly when uncovering identifiable data that mention its original source. The study proposes an identifiable data of the copyright holder to tie the copyright holder to the computer software. It presents a hash function method of hiding identifiable data, exposes the connections to a person or organization, and prepares a potential evidence for future lawsuits.

For example, associate professor Dayu Kao works at the Department of Information Management, Central Police University, Taiwan, where he directs the Computer Crime Investigation Laboratory. Two messages can be retrieved as 'Dayu Kao, Central Police University, TW' and 'Dayu Kao, Computer Crime Investigation Laboratory, TW.' After the message is generated from metadata attributes, the one-way hash function is calculated and a DIGEST is generated in Figure 2a. A one-way hash function, also known as a message digest, is a mathematical function which takes a variable-length input string and rts it conveinto a fixed-length binary sequence [10]. A good hash function makes it hard to find two strings that would produce the same hash value. It is designed to hardly reverse the process in Figure 2b. The DIGEST can be further embedded into the image of computer software using information hiding schemes like Least Significant Bit (LSB). Table 2 further illustrates the DIGEST scheme. That DIGEST can be embedded into the digital image of computer software (Figure 2a, 2b and Table 2).

Incident phase: Conduct a proper ICT governance

Hiding data in digital files is facile, and efficacious. The extent of hiding data depends upon the complexity of the computer software and IP protection. Hiding within data requires commingling the secret identifiable data within visible data.

People: Identify an effective method to protect copyright materials: Increasing global dependence on the Internet and continuously changing computer software are driving an increasing the risk of copyright infringement. Precautions against such risks are the usage of information hiding behind computer software. Sometimes the best way is easy, and the easy way can be also the most effective [2,10]. Depending upon the effort, resource, and determination of copyright holders, anti-digital forensic methods can be used that will thwart some copyright infringement attempts. Information hiding or anti-digital forensics can be used in software development, and can increase the ease of identifying copyright infringement from their original works. It is practically possible to detect or identify the identifiable data by investigators. The methods to encrypt or hide messages are varied. Once the piracy of computer software in digital storage devices has been seized, identifiable data can be recovered as evidence for additional investigative leads.

Process: Acquire identifiable data behind computer software: Copyright holders covering their identity do not have the same purpose in mind that criminals do when protecting their secrets with each other. They can hide some identifiable data to protect their identities and the sold computer software. It can hide some identical details in computer software, and protect object integrity by preventing unauthorized changes. They can utilize various toolkits to enable security patterns or codes in computer software.

Technology: Collect multiple forms of protection: Hiding

No.		1	2
Message		Dayu Kao, Central Police University, TW	Dayu Kao, Computer Crime Investigation Laboratory, TW
Statement		Original Message 1	Original Message 2
DIGEST	MD5	2a4bb079570e24670a4f4371 52a53f83	d4e64421d1985dc49c9f7f7aaf 25f1fb
	SHA1	4355a1c8b0ff32507c3f5effa5 074588cd35179e	dba65d79726dab419132e272 773bd26e4aa0a74d
	SHA256	b8c867a56f06ca10b06a71ffb 1d359f996dc73c16a99e46b4 3136744481e8623	1a75bd0f3f5a7b0e1f0a036cb6 c047913af64894e909a5358e0 93884e1d528f3

Table 2: DIGEST Scheme in Computer Software.

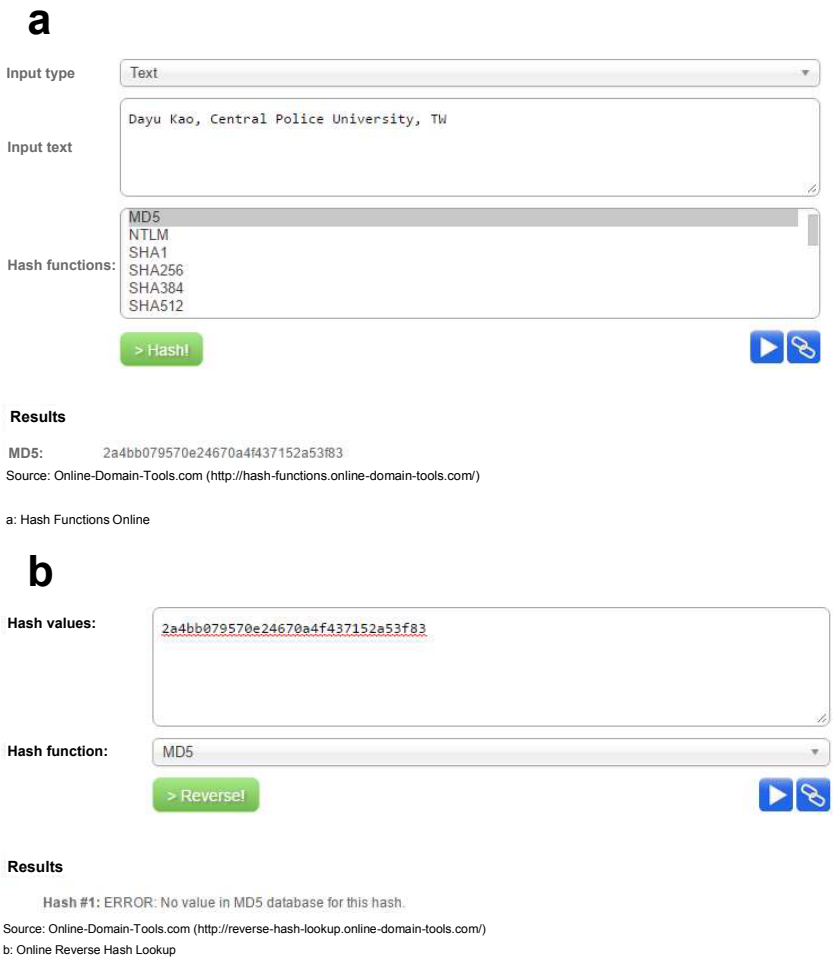


Figure 2: One-way Hash Function for DIGEST Messages.

identifiable data in copyright materials provides positive evidences to prosecute criminals. It is convenient to resort to multiple forms of protection, which can be strategically invoked in different settings [9]. Other easy, workable methods are illustrated below [9,10].

(1) ***Word processing***

A simple method of hiding identifiable data is to use a word processing document, type the secret message, and change the font to white in order to match the background of the document [10]. Viewers of the document may miss the white text on the file. Although changing font color to hide text is easy to defeat with forensic applications, it is an easy method that does not require special software or skills to hide the information.

(2) ***Metadata field***

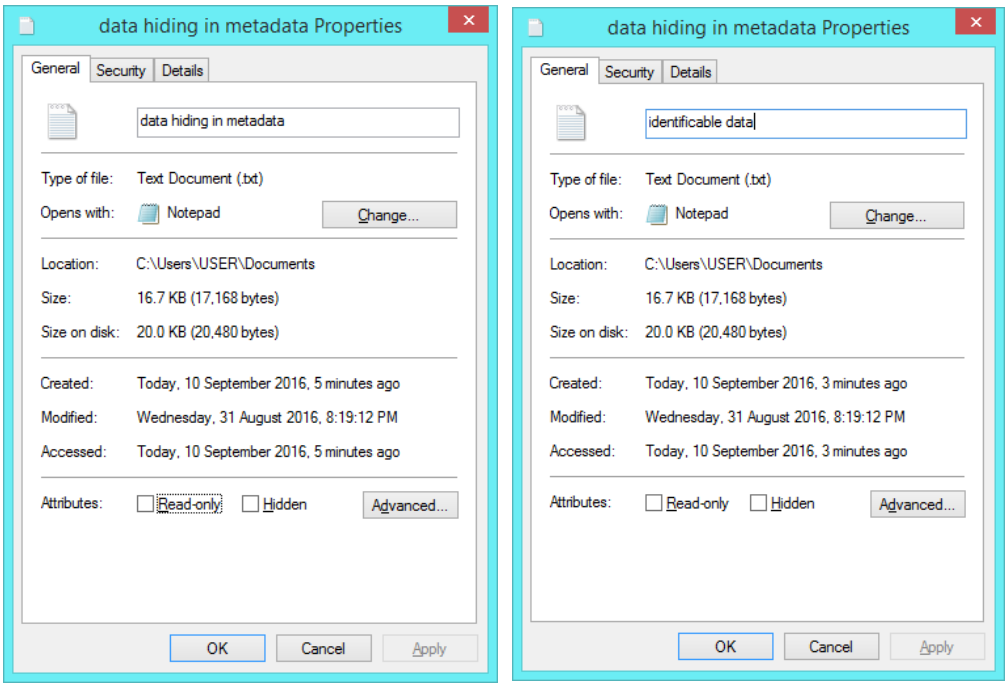
Metadata fields in each file can be used to hide data. Some of these fields are filled with information such as date-time stamps. Other fields are open for user-added details. Sometimes the metadata of copyright materials is essential and provides more intelligence than the content. In Figure 3, a sample text file is named as 'data hiding in metadata.txt'. The original content of general field is the same with the filename in Figure 3a. But it is easy to modify its metadata contents in Figure 3b. The metadata could state the intentions of the IP authorship or prove his/her original sources (Figure 3a and 3b).

Aftermath phase: Wait for effective results

Complexity breeds vulnerability in the world of computer software. The fundamental goal of cybercriminals or copyright infringement criminals is to maximize their financial profitability while concurrently minimizing their risk. The workable strategy of hiding identifiable data behind computer software is proposed to improve the information security, and establish the trustworthy computing of cybercrime investigation. It also helps LEAs identify the copyright holder of computer software.

People: Understand the cooperation need with LEAs: LEAs may encourage copyright holders to secure any sets of protection offered under copyright act with respect to any creative works, or even with respect to the creative features of their commercial products. These works or product features can be defined as an original work of authorship [5]. Copyright holders should try to prove their authorships and help LEAs prosecute criminals. LEAs or governments should play an effective role to protect, educate, and guide copyright holders on promoting the evidentiary value in copyright infringement investigation.

Process: Report information hiding in copyright materials: Taking lawsuit steps to protect the IP rights may have more benefits



a. Original Content b. Modified Content

Figure 3: User-added details for the metadata data of general field in a sample file.

than just financial compensation in the sub-market. Even if the business is unsuccessful in its lawsuits, it may build a business aware of its IP rights. Such a reputation can have preventive, and it may even make criminals think twice before their IP infringements [2].

Technology: Preserve positive evidences for LEAs: Before copyright holders file a lawsuit, the countermeasure against copyright infringement is to add some identifiable data into computer software, implement information hiding into the product, and fight against the rise of the copyright infringement. Working proactively with the proposed covert identifiable data methods can reduce or eliminate the need for expensive lawsuits. This can also reduce the costs and increase the success rate of enforcing rights.

Conclusions

Criminals often try their best to hide their identity and reduce their chances of detection. There is no clear guidance in copyright infringement proceedings. So do copyright holders. They should try to prove their authorships and help LEAs prosecute criminals. Prosecuting every copyright infringement method is unlikely. Hiding identifiable data in copyright materials provides positive evidences to prosecute criminals. Identifiable data in computer software must be secure for the sake of the operation of a business. The proposed ICT governance framework embeds some identifiable data in computer software, and helps copyright holders fight against the rise of the copyright infringement. LEAs or governments should play an effective role to protect, educate, and guide copyright holders on promoting the evidentiary value in copyright infringement investigation. Just as pulling a single thread can unravel a sweater, finding an effective method to explore copyright infringement evidences opens up entire threaded conversations in a criminal investigation.

Acknowledgements

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 105-2221-E-015-001.

References

1. Ablon L, Libicki MC, Golay AA (2014) Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Santa Monica, CA: Rand Corporation, pp: 3-20.
2. Alkaersig L, Beukel K, Reichstein T (2015) Intellectual Property Rights Management: Rookies, Dealers, Strategists and Strategic Dealers. Hampshir, UK: Palgrave Macmillan, pp: 33-66.
3. Bernik I (2014) Cybercrime and Cyber Warfare. John Wiley & Sons Inc., pp: 1-56.
4. Dobie G (2015) A Guide to Cyber Risk Managing the Impact of Increasing Interconnectivity. London: Allianz Global Corporate & Specialty, pp: 1-28.
5. Frankel S, Gervais D (2014) The Evolution and Equilibrium of Copyright in the Digital Age. Cambridge, UK: Cambridge University Press, pp: 15-80.
6. Gervais DJ (2015) International Intellectual Property: A Handbook of Contemporary Research. Cheltenham, UK: Edward Elgar Publishing, pp: 1-216.
7. International Organization for Standardization (ISO) (2015) ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes. Switzerland: ISO Office, pp: 4-20.
8. Perry M (2016) Global Governance of Intellectual Property in the 21st Century: Reflecting Policy through Change. Switzerland: Springer International Publishing, pp: 14-150.
9. Rowe EA, Sandeen SK (2015) Trade Secrecy and International Transactions: Law and Practice. UK: Edward Elgar Publishing Limited, pp: 3-150.
10. Shavers B, Bair J, Leibrock L (2016) Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis. MA: Elsevier Inc., pp: 115-172.

11. Wirtén EH (2015) Making Marie Curie: Intellectual Property and Celebrity Culture in an Age of Information. Chicago: The University of Chicago Press, pp: 31-50.

12. Yeh BT (2016) Intellectual Property Rights Violations: Federal Civil Remedies and Criminal Penalties Related to Copyrights, Trademarks, Patents, and Trade Secrets. Washington, DC: Congressional Research Service, pp: 1-23.