2012 32nd International Conference on Distributed Computing Systems Workshops

When Digital Forensic Research Meets Laws

Junwei Huang
Computer Science
UMass Lowell
Lowell, MA, U.S.A.
jhuang@cs.uml.edu

Zhen Ling
Computer Science
Southeast University
Nanjing, China
Zhenling@seu.edu.cn

Tao Xiang
Computer Science
Chongqing University
Chongqing, China
txiang@cqu.edu.cn

Jie Wang
Computer Science
UMass Lowell
Lowell, MA, U.S.A.
wang@cs.uml.edu

Xinwen Fu
Computer Science
UMass Lowell
Lowell, MA, U.S.A.
xinwenfu@cs.uml.edu

***Abstract*—Academic researchers in digital forensics often lack backgrounds in related laws. This ignorance could make their research and development legally invalid, or with less relevance in practice. To better assist academic researchers, we discuss related laws that regulate the government's investigation and summarize different requirements of acquiring data and evidence in different crime scene investigations. We show that certain strategies (including attacks against security systems) would violate relevant laws, and so law enforcement cannot use them to collect data. We recommend that researchers focus on crime scene investigations that do not need Warrant/Court Order/Subpoena for traceback related network forensics. This would help make their research and development accepted more easily by law enforcement with a larger impact.**

Keywords: Digital Forensics; Law; Constitution; Privacy; Legal

I. INTRODUCTION

Computers and the Internet are the most creative and powerful inventions with a wide and deep influence on the human society. Almost one third of people have used the Internet through computers, mobile devices and other multimedia devices [1]. Millions of people spend hours every day sending and receiving emails, communicate with each other, obtain information and participate in countless other activities. Computers and the Internet have now become important components of human lives.

The first computer crime took place in October 1968, only 20 years after the first computer ENIAC was invented [2]. A computer engineer was found guilty for stealing money by manipulating programs of a bank's computer system that alternated bank records [3]. The ARPAnet, the early Internet, was created in 1969 and cases of computer crimes grew rapidly in the 1970's. With the development of computer technology and applications, computer crime is becoming a problem that involves and has influence on nearly every aspect of our society. Political, economical, cultural, military aspects of our society have changed rapidly and sharply to cope with computer crimes.

Computer forensics is the science to collect, preserve, analyze and present evidence from computers that are sufficiently reliable to stand up in court and convincing. It is one of the fastest growing occupations in the fight against computer crimes. Computer forensics is a practical science to lawful investigation [4].

Law enforcement specialists and academic researchers have put enormous efforts on computer forensics against computer crimes [5]. They developed new areas of expertise and avenues of collecting and analyzing evidence. The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal. However, computer forensics is a cross disciplinary field and it requires both knowledge of computing and laws.

Academic researchers often lack the backgrounds of the relevant laws. Because of this, their research results often do not conform to the regulations of the laws [6]. They may be unfamiliar with the real-world problems faced by forensic investigators and the constraints placed in solving them. In reality, incorrect use of new techniques may result in suppression of the gathered evidence in court. For example, using specialized technology to obtain information without warrants may violate the Fourth Amendment, and the evidence gathered may be suppressed in court [7]. There are many attacks proposed in the bibliography on tracing users and breaking privacy. As a pitfall, people may think that such attacks can also be used by law enforcement for forensic traceback. However, with the regulations of the laws, many of these attacks cannot be used for such purpose. This observation suggests that researchers cannot assume that forensic investigator can use technologies arbitrarily without any law restrictions.

When researchers invent a new technique for law enforcement officers, they need to consider whether law enforcement can use the new technique practically and legally. Can law enforcement officers use a technique without any due process? Under what circumstances can they adopt it? Is this new technique better than current existing techniques? If law enforcement cannot use a new technique without a warrant, how should researchers invent techniques to help law enforcement officers collect necessary evidence to apply for a warrant or for further action?

Keeping these questions in mind, in this paper, we will investigate the law constrains on computer forensics, to help researchers to make their research more useful to forensic investigators. We expect that researchers will understand what they can do and what they cannot do in computer forensics. We emphasize the law restrictions upon government entities in the computer crime area. We also focus on whether or not law enforcement officers can use a technique without any restrictions, but do not go into detail about specific process restrictions, if any.

The rest of the paper is organized as follows. We will discuss related law terminology and resources in section II. The procedures of criminal investigations will be fully described in section III. We then analyze the feasibility of

1545-0678/12 $26.00 © 2012 IEEE
DOI 10.1109/ICDCSW.2012.45

several published research papers in section IV. We will conclude the whole paper in section V.

II. TERMINOLOGY AND RELATED LAW RESOURCES

Before we move to the details of the constraints from laws on computer forensic techniques, we will introduce some terminology and related law resources in this section. Normally, there are two kinds of actions in computer criminal investigations: **investigation with warrant/court order/subpoena** and **investigation without warrant/court order/subpoena**. They are governed by two primary law resources: the Fourth Amendment to the U.S. Constitution, and the statutory laws codified at 18 U.S.C. (United States Code) §§ 2510 to 2522, 18 U.S.C. §§ 2701 to 2712, and 18 U.S.C. §§ 3121 to 3127. In most cases, it is either a constitutional issue under the Fourth Amendment or a statutory issue under related law. In a few cases, they are overlapped.

A. Terminology

Subpoena: A specific type of court order to compel a witness to produce certain evidence or to appear in court to testify. For example, law enforcement with a subpoena can require the witness ISP to produce connection logs to determine a particular subscriber's identity.

Court order: An official judge's statement compelling or permitting the exercise of certain steps by one or more parties to a case. For example, using a packet-sniffer on an ISP's router to collect all packets coming from a particular IP address to reconstruct an AIM session.

Search warrant: A written court order authorizing law enforcement to search a defined area and/or seize property specifically described in the warrant.

In general, the degree of difficulty for the above processes is in the ascending order. For example, applying for a subpoena is much easier than applying for a search warrant. Merely *a suspicion is enough to apply for a subpoena*. *Some "specific and articulable facts" are needed to apply for a court order*. *Probable cause is necessary to apply for a search warrant.*

B. Related Law Resources

1) The Fourth Amendment to U.S. Constitution

The Fourth Amendment is the main constitutional restriction to forensic investigation:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*."

The Fourth Amendment protects people's reasonable privacy by limiting government agents' search and seize without a warrant. Government investigators cannot gather digital evidence and identify a suspect with merely doubt but by probable cause.

2) Acts in United States Code (U.S.C.)

The other main restrictions we will talk about come from U.S.C. as follows.

a) Wiretap Act (Title III)

The Wiretap Act [8], 18 U.S.C. §§ 2510-2522, was first passed as Title III of the Omnibus Crime control and Safe Streets Act of 1968 and is generally known as "Title III". It was originally design for wire (see 18 U.S.C. § 2510(1)) and oral communications. The Electronic Communications Privacy Act of 1986 (ECPA) [9] was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer [10].

Wiretap Act is an important statutory privacy law. Roughly speaking, it prohibits unauthorized government access to private electronic communications (see 18 U.S.C. § 2510(12)) in real time.

b) Stored Communications Act

The Stored Communications Act (SCA) [11], 18 U.S.C. §§ 2701-2712, is a law that was enacted by the United States Congress in 1986. *SCA is a part of the ECPA*. It protects the privacy right for customers and subscribers of Internet service providers (ISPs) and regulates the government access to stored content and non-content records held by ISPs.

c) Pen Register Act

Pen Register Act [12], 18 U.S.C. §§ 3121-3127, also known as the Pen Registers and *Trap and Trace Devices* statute (Pen/Trap statute) [6]. Generally speaking, a pen register device (see 18 U.S.C. § 3127(3)) records outgoing addressing information (such as a number dialed and receiver's email address); a trap and trace device (see 18 U.S.C. § 3127(4)) records incoming addressing information (such as incoming phone number and sender's email address).

In general, the Pen/Trap statute regulates the collection of addressing and other non-content information such as packet size for wire and electronic communications. Title III regulates the collection of actual content of wire and electronic communications. *Both of the two statutes above regulate the real-time forensics investigation* while *SCA statute regulates the static forensics investigation, such as email and account information.*

C. Reasonable Privacy

One critical concept in acquiring evidence is reasonable privacy. We use this whole subsection to discuss it given its importance. A person deserves reasonable privacy if 1) he/she actually expects privacy and 2) his/her subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'[10][13][14]". In this subsection, we will talk about in what situation people have reasonable privacy and in what situation they will lose their reasonable privacy.

1) When People have Reasonable Privacy

In 1967, the United States Supreme Court was holding that a person has a reasonable privacy when Katz, the defendant, enters a telephone booth, shuts the door, and makes a call. Thus, it is illegal for government agents to obtain the phone call content without a warrant, even though

the recording device is attached outside the telephone booth, the communication is not interfered and the booth space is not physically intruded [14]. The Supreme Court holds that when the defendant shuts the door, his objective expectation is that nobody would hear his conversation and *this action is recognized as reasonable by society*. This idea is generally phrased as "the Fourth Amendment protects people, not places."[13]

A basic law issue in computer forensics is whether an individual has a reasonable expectation of privacy of electronic information stored within computers (or electronic storage devices). The consensus is that electronic storage devices are analogous to closed containers and people do have a reasonable expectation of privacy. If a person enjoys a reasonable expectation of privacy on his/her electronic information, law enforcement officers ordinarily need a warrant to "search" and "seize", or fall within an exception to the warrant requirement before officers access the information stored inside. Therefore, when researchers invent a new technique, they need to think whether this new technique violates a person's reasonable privacy exceptional. If it does, a researcher may need to re-design the technique in order to help law enforcement to avoid the requirements of the search warrant by searching information not subject to privacy expectations.

2) When People do not have Reasonable Privacy

Normally, information in public places has no reasonable expectation of privacy. If a person knowingly exposes information to another person or in public places, he/she has no reasonable expectation of privacy on that exposed information [20]. For example, two people are talking inside a house, they are talking so loudly that everyone walking outside the house can hear. Law enforcement outside on the street can record this conversation without a warrant, even though this conversation happens inside the house. In the Katz case [14], although Katz's conversation is not permitted to be recorded without a warrant, Katz's appearance or action should be legal to be recorded through the transparent glass. Another example is that bank account, subscriber's information and the telephone number the caller dialed have no privacy expectation since the information are knowingly exposed to the service provider [26][27][28]; however, that information here is protected by statutory laws that we will talk about in the next section.

In computer forensics, if people share information and files with others, they normally lose the reasonable expectation of privacy. For example, a person has no privacy if he/she leaves a file on a public computer in a public library [15][17]; or if he/she shared a folder with others, he/she has no privacy expectation on that folder even though he/she is operating it on his/her private computer [18][19]. There are a lot of cases about sharing information and losing reasonable expected privacy such as sharing information and files through P2P software [21] (including the anonymous P2P software [22]), leaving information on public Internet [16] and so on.

People may not retain their reasonable expectation of privacy either if they relinquish control of the information and file to a third party [29][30][32]. The common scene in computer forensics is that a person may transmit information to third parties over the Internet, or may leave information on a shared computer network. During the transmission, the government is not allowed to examine the content originally because it violates both sender and receiver's expected privacy [23]. Government needs a warrant to examine the information. However [24], the carrier of the information such as Internet Service Provider (ISP) eliminates the privacy expectation (but that information is protected by statutory laws and the government still needs a warrant/court order/subpoena to obtain that information). However, after the information is delivered, the sender has no reasonable expected privacy anymore ("terminates upon delivery") [25][30][31].

Another law issue is that there is no agreement on whether a computer or other storage device should be classified as a single closed container or whether each individual file stored within a computer or storage device should be treated as a separate closed container [30][33][34][35]. For example, law enforcement agents want to search the seized computer for child pornography pictures, they may or may not use an exhaustive search tool to examine all files in this computer while the owner of the computer may or may not have reasonable expected privacy on some files which are not child pornography pictures. When researchers design such surveillance for law enforcement, researchers need to think about whether the tools violate "reasonable expectation of privacy".

III. Criminal Investigation

In general, forensic investigators need a search warrant/court order/subpoena to pursue an investigation and gather the evidence legally. *However, when the investigation does not violate a person's reasonable privacy or does not break the law or falls into an exception of law, then obtaining the evidence without search warrant/court order/subpoena is not illegal and the evidence will not be suppressed in court*. We will introduce these two kinds of investigations in this section.

A. Investigation with Warrant/Court Order/Subpoena

For those investigations that violate people's reasonable privacy expectation, law enforcement needs a warrant/court order/subpoena to obtain the related information. Generally speaking, people have privacy on his or her private affairs. Law enforcement officers cannot commit unreasonable surveillance. Both constitutional and statutory laws limit the ability of government agents to search for and seize evidence without a warrant/court order/subpoena. Law enforcement officers need to provide reasonable suspicion or probable cause to apply for a subpoena/court order/search warrant and commit surveillance legally. To obtain a court order or subpoena is easier than a search warrant. However, law enforcement officers still need facts or suspicions to obtain a court order or subpoena.

For researchers, they need to keep in mind (i) how to develop tools for law enforcement to gather facts to demonstrate cause for suspicion or probable cause and (ii) identify the criminal and the intent of the crime during the

search stage. In the first part, researchers develop some tools that law enforcement officers can use in a situation prior a search warrant/court order/subpoena. In the second part, the technique used in the investigation should confirm criminal behavior and the criminal's purpose rather than identify a machine utilized as a criminal tool [6].

In the following, we will first discuss the requirements for applying for a warrant/court order/subpoena. We then discuss the purposes and attentions during the investigation stage. We will present how those laws govern law enforcement's investigations in the end.

1) Requirements for a Warrant/Court Order/Subpoena

Because the strictest requirement that is also hardest to understand is *probable cause* and mere suspicions and facts are easily understandable, we will mainly focus on probable cause in the first step.

Probable cause is the standard by which an officer or agent of the law has the grounds to make an arrest, to conduct a personal or property search, or to obtain a warrant for arrest, etc. when criminal charges are being considered. It is also used to refer to the standard to which a grand jury believes that a crime has been committed. *The best-known definition of probable cause is "a reasonable belief that a person has committed a crime"* (citing from Wikipedia [36]).

Probable cause in computer forensics to search a computer or electronic media is a belief that the computer or media is (i) contraband; (ii) a repository of data that is evidence of a crime; (iii) an instrument of a crime. According to the Supreme Court, the probable cause standard is satisfied by an affidavit that establishes "a fair probability that contraband or evidence of a crime will be found in a particular place. [37]" However, it requires a practical, common-sense determination of the probabilities, based on a totality of the circumstances [10].

Probable cause is different in many cases, authors in [10] summary the computer cases into a few common scenarios. We will introduce scenarios related with computer forensic investigation. Keeping in mind with those probable causes, researchers should be able to develop practical techniques for law enforcement.

a) Probable Cause Established Through an Internet Protocol Address: Investigators can use techniques to obtain an attacker's IP address from a victim or from a service provider. By using a subpoena or other process discussed later in this section, investigators then compel the ISP that has control over that IP address to identify which of its customers was assigned that IP address at the relevant time, and to provide (if known) the user's name, street address, and other identifying information. Typically, such kind of probable cause is sufficient to obtain a search warrant [38][39][40], no matter the suspect uses a "unsecure wireless connection" allowing others to use his/her IP address [38][40][41][42].

b) Probable Cause Established Through Online Account Information: If investigators obtain a person's information associated with the person's online account by using some technique or subpoenaing a service provider, investigators can use the information as probable cause for applying for a search warrant to search the suspect's computer [43][44]. A more common scenario is when investigators have discovered a child pornography website or email group and have successfully obtained its membership list without independent evidence such as an IP address [45]. *However*, we must emphasize here that not all courts have agreed that membership alone supports the application [46]. If law enforcement has a technique to *identify the suspect's intent* along with the membership, this is a probable cause.

c) Staleness: Defendants often challenge that the information law enforcement obtained is too old to establish probable cause at the time the warrant was issued. However, the cases tell us that the information is sufficient to establish the probable cause no matter how old it is [47][48][49][50][51]. It is also good for investigators to recover the deleted files [52]. *Yet* there are still a few cases, though, where some information may be stale [53][54][55].

2) Purposes and Attentions during Investigation

Now assume law enforcement has specific facts or probable cause to get a subpoena/court order/search warrant and try to commit an investigation. Before law enforcement pursue the investigation, let us talk about what are the purposes of investigation and attentions for investigation.

Researchers need to keep in mind that to discover contraband or substantive evidence of a crime on the hard drive is the most important goal of a computer search. But as we mentioned before, to identify the person and the intent of the criminal is also important: (i) if possible, the new technique should be able to prove the action of a particular individual to put contraband on the hard drive rather than allowing for the possibility that someone else with access to the computer did so; (ii) the new technique should be able to confirm that a virus or other piece of malware was not responsible for the crime; (iii) the new technique should be able to show that a defendant had knowledge of the particular subject. For example, the browsing history and cookies might reveal that an individual was researching how to build a methamphetamine laboratory.

There are other issues we need to mention here during the search. If researchers keep these in mind during their research stage, they might be helpful for them to design some practical techniques for law enforcement:

a) The Usage Scope of Techniques: In certain cases (especially in business cases), agents may not be able to seize all information legally if the search exceeds the scope of the search warrant. Thus, a good technique can identify records that only relate to a particular crime and to include specific categories of the types of records likely to be found [56][57]. If the investigation involves multiple locations, agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations. Thus, researchers need to think about whether obtaining multiple warrants may affect the technique and whether the technique will violate the warrant [35].

b) The Time Restriction: Time is also important for law enforcement during their search and surveillance stage [58]. Because a search warrant may expire and revoke after a specific time period. Researchers may design or redesign a technique for law enforcement to speed up the evidence search. The best technique can help law enforcement to do an on-site search within a short time. If there is no technique currently available to do an on-site search, the agent can image the target hard drive [59][60][61] and *derive a image copy*. However, agents need to explain the necessity for seizure of the entire computer system for off-site examination [58][61]. Researchers may invent technique to proof the necessity.

c) Restriction-less: The Researchers can keep in mind that the Fourth Amendment does not limit the techniques an examiner may use to examine a hard drive, while the searched data is responsive to the warrant [62]; nor imposes any specific limitation on the time period of the government's forensic examination [63][64].

3) Laws in Investigation

For cases related with the information inside a computer, they are governed by constitutional laws presented in the previous subsection. For most cases related with the information outside a computer (i.e. in transmission, remote storage, etc), they are regulated by statutory laws, that are briefly introduced in section II. In general, the Stored Communications Act (SCA) regulates the data stored on the Internet while Pen/Trap Act and Wiretap Act regulate the real-time data transmission over the Internet outside a person's computer. In all cases involving those statutes, law enforcement officers need to apply warrant/court order/subpoena to pursue an investigation, except when the investigation falls into the exceptions of those statutes that we will introduce in the next subsection. We will now disucss the three statutes separately from a researcher's view below.

According to the Fourth Amendment privacy doctrine, customer and subscribers of network service provider may not expect reasonable privacy on their account information. The SCA, nevertheless, offers network account holders a range of statutory privacy rights to protect their private information. On one hand, SCA imposes limitations on government to access the information stored on ISPs (see 18 U.S.C. § 2703); on the other hand, *SCA prevents ISPs from voluntarily disclosing the information to the government* (see 18 U.S.C. § 2702).

However, the SCA is not a catchall statute [65]. It only protects two kinds of providers: providers of "electronic communication service" (ECS, see 18 U.S.C. § 2510(15)), and providers of "remote computing service" (RCS, see 18 U.S.C. § 2711(2)). An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." For example, hotmail and Gmail generally act as ECS providers [66]. So does the host of an electronic bulletin board [67]. The term RCS is "the provision to the public of computer storage or processing services by means of an electronic communications system (see 18 U.S.C. § 2510(14))." An RCS is provided by an off-site computer that stores or processes data for a customer [66]. For any other providers, the Fourth Amendment applies instead of the SCA.

We here use an example to explain those two categories of providers and how SCA and the Fourth Amendment apply. Alice at Charlie University sends an email from her account (alice@cs.charlie.edu) at work to her friend Bob's personal account (bob@gmail.com). When the email arrives at Gmail ISP, Gmail ISP is a provider of ECS with respect to that email. Once Bob retrieves the email, he can either delete the message from his gmail account or else leave that email stored there. If Bob chooses to store the email, Gmail ISP is now a provider of RCS (not ECS) with respect to the email. The role of Gmail ISP has changed from a transmitter of Alice's email to a storage facility for a file stored remotely for Bob by an RCS provider.

Next imagine that Bob responds back to Alice. His response email to Alice will arrive at the servers in University. Before Alice retrieves the email from the university's server, the server is a provider of ECS with respect to Bob's reply email. But when Alice accesses the email, the university's server stops being a provider of ECS with respect to the reply email. Unlike Gmail ISP, however, the university's server does not become a provider of RCS if Alice decides to store the opened email on the university's server. Rather, for purposes of this specific email, the university's server is a provider of neither ECS nor RCS. It does not provide RCS because it does not provide services to the public [68]. Because the university's server provides neither ECS nor RCS with respect to the opened email in Alice's account, the SCA no longer regulates access to this email, and such access is governed solely by the Fourth Amendment. Functionally speaking, the opened email in Alice's account drops out of the SCA.

Section 2703 in 18 U.S.C. lists different rules that the government must satisfy to compel different types of information stored in ISPs. A search warrant can disclose everything while a subpoena can only get the basic subscriber information. However, law enforcement officers can obtain a subpoena with mere suspicion rather than probable cause. A court order is kind of a mix of a warrant and a subpoena. Officers need "specific and articulable facts showing that there are reasonable grounds to believe" that the information to be compelled is "relevant and material to an ongoing criminal investigation [65]."

Section 2702 in 18 U.S.C. regulates voluntary disclosure by providers of RCS and ESC. But any public providers can disclose non-content information to non government entities. Providers not available "to the public" may freely disclose both contents and non-content records. There are a lot of specific exceptions in which voluntary disclosure is allowed. Here we ignore them in this paper as they are not of our interest.

Pen/Trap statute requires a subpoena or court order to install "pen register" and "trap and trace device" to obtain non-content information such as email's TO/FROM addresses, IP address of the website, the total volume of the information and so on [69]. Normally, the cases in computer forensics will be analogous to speech, letters and telephone

calls. For example, the address on an envelope is public to everyone. The trick here is the definition of "pen register" and "trap and trace device". The information obtained by Pen/Trap devices shall not include the contents of any communication. The government must also use "technology reasonably available to it" to avoid recording or decoding the contents of any wire or electronic communications (see 18 U.S.C. § 3121(c)). Otherwise the Wiretap Act applies.

The Wiretap Act is simple. It takes all private communications as a two-way communication. The statute prohibits using an intercepting device to intentionally access the content of communications in "real time" [65].

Most cases in computer forensics implicating Title III focus on whether the electronic communications were intercepted [70][71][72][73]. The term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." The statutory definition of "intercept" does not explicitly require that the "acquisition" of the communication be contemporaneous with the transmission of the communication. However, a contemporaneity requirement is a necessity to keep the proper relationship between Title III and the SCA's restrictions on access to stored communications. Otherwise, for example, a Title III order could be required to obtain an unopened email from a service provider [10].

Wiretap Act and Pen/Trap Act are complementary. For example, obtaining email's subject and content implicates Title III while obtaining the TO/FROM email address implicates Pen/Trap statute. Obtaining the real content of a visiting website implicates Title III while obtaining the IP address of the website implicates Pen/Trap statute. Collecting an entire packet during transmission implicates Title III while collecting the packet's routing information implicates Pen/Trap statute.

B. Investigation Without Warrant/Court Order/Subpoena

Since we have explained the investigation with a warrant/court order/subpoena, we can now discuss what happens if the government's investigation does not violate a person's "reasonable expectation of privacy," or the protection of laws does not apply. The evidence collected should remain valid and legal.

Base on [10], We conclude from that if one of the following situations (but not limited) are present then an investigation without a warrant/court order/subpoena remains legal.

a) No Reasonable Expected Privacy: For any case governed by the Fourth Amendment rather than the statutory laws, if the government's action does not constitute either a "search" nor "seizure" or does not violate the suspect's reasonable expected privacy (in other words, the suspect has no reasonable expected privacy in that situation), the law enforcement needs no warrant to conduct the investigation. We have explained reasonable expected privacy in section II.

Here we will mention one case about use of specialized technology to obtain information without a warrant. In this case [7], law enforcement officers use a thermal imager to detect the amount heat emanated from the various rooms of the suspect's (Kyllo) home without a search warrant. The Court held that the action constitutes a search and is presumptively unreasonable without a warrant. Researchers need to keep in mind that whether their new technique falls within the scope of the Kyllo rule depends on at least two factors: (i) the technology used is in "general public use" or not (But currently there is no standard to determine whether a certain technology meets this requirement or not); (ii) The technology used will disclose the information about the interior of the home or not.

b) Exigent Circumstances: In exigent curcumstances, government can conduct warrantless searches or seizures when immediately necessary to protect public safety or preserve evidence [74]. These circumstances include [10][65]: (i) evidence may be destroyed immediately or in a very short time [75]; (ii) either the police or public is in a dangerous situation; (iii) the police are in "hot pursuit" of a suspect; or (iv) the suspect may escape before the officer can secure a search warrant. The first one maybe of most concern here. For example: incoming messages can delete stored information, or the batteries can die thus erasing the information; more specially, a "destroy command" can be sent to some devices that will cause the device to encrypt itself or overwrite data stored on the device; or the device can be set to delete information stored on the device after a certain period of time [76]. The Court will judge the exigent circumstance by some factors. In electronic device cases, the existence of exigent circumstances is tied to the facts of the individual case [77][78][79].

c) Consent: Consent exception is a powerful exception to both constitutional and statutory laws. It is reasonable and legitimate to conduct a warrantless search with voluntary consent made by a person who has an authority to consent. But the search should not exceed the scope of the consent and should cease if the consent revoked (However, a person who revoked the consent to search his computer retained no reasonable expectation of privacy in a mirror image copy of his hard drive made by the FBI [80]).

There are a few kind of consents we need to mention here:

(i) Imagine several people use or own the same computer equipment, they may or may not have their own private space/data (such as password protected files) on the computer equipment. Any user has authority on the public space/data and his/her private space/data. He/She can only consent the parts he/she owned and permit law enforcement to search the parts he/she controlled [81][82][83].

(ii) Either spouse may consent to a search of all of the couple's property (computer) [83].

(iii) Parents have the authority to consent a search of their children's computers when the children are under 18 years old [84]. If the children are 18 or older, the parents may or may not be able to consent, depending on the facts [85].

(iv) Owner/Boss of a private company has broad authority on all properties he/she owned. Law enforcement officers can conduct a warrantless search on working computers if either the owner/boss or employee consent to do it [86]. In contrast, a government employee may or may not enjoy a reasonable expected privacy in his workplace depending on circumstances. But, employers (government) can nevertheless conduct warrantless searches provided the searches are work-related, justified at their inception, and permissible in scope [87].

(v) Computer network accounts often contain information relevant to criminal investigations. In general, law enforcement officers either conduct an investigation with a warrant/court order/subpoena or conduct a warrantless investigation with the consent from the network's owner, manager or system administrator who has authority to voluntarily disclose information related to the account. However, in different networks, the rule is different. For public commercial communication service providers (such as Google or Hotmail), the SCA prohibits public service providers from voluntarily disclosing to the government information pertaining to their customers except in certain specified situations—which often track Fourth Amendment exceptions—such as with the consent of the user, to protect the service provider's rights and property, or in an emergency. For example, system administrators of computer networks generally may monitor hackers intruding into their networks and then disclose the fruits of monitoring to law enforcement without violating Wiretap Act. Significantly for the Fourth Amendment purposes, commercial service providers typically have terms of service that confirm their authority to access information stored on their systems, and such terms of service may establish a service provider's common authority over their users' accounts [24]. For private-sector employers generally have broad authority to consent to searches in the workplace, and this authority extends to workplace networks.

(vi) When one of the parties to the communication consents to the interception, the interception is valid and does not violate the Wiretap Act (But in some states' law, it requires all parties to the communication consent to the interception [89]). "For example, an undercover government agent can record a conversation between himself and a suspect or permit others to record the call. Similarly, if a private person records his own telephone conversations with others, his consent authorizes the interception unless the commission of a criminal, tortious, or other injurious act was a determinative factor in the person's motivation for intercepting the communication [88]" (citing from [65]).

d) Emergency: The Pen/Trap statute authorizes the installation and use of a pen/trap without a court order in emergency situations involving: (i) immediate danger of death or serious bodily injury to any person; (ii) conspiratorial activities characteristic of organized crime; (iii) an immediate threat to a national security interest; or (4) an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030(e)(2)) that constitutes a crime punishable by a term of imprisonment greater than one year (See 18 U.S.C. § 3125(a)(1)). The installation and use of an emergency pen/trap requires approval at least at the Deputy Assistant Attorney General level, or by the principal prosecuting attorney of any state or subdivision thereof who is acting pursuant to a state statute (See 18 U.S.C. § 3125(a)).

e) Plain View: The plain view doctrine indicates that evidence seized and contraband found by an officer without a warrant during a lawful observation [90]. The officer must be in a lawful position to observe and access *the evidence that can be plainly viewed, and its incriminating character of the object must be immediately apparent*. In a common scence, officer may occasionally come upon incriminating evidence on the screen of a computer. Another example is when agents examine a computer pursuant to a search warrant and discover evidence of a separate crime that falls outside the scope of the search warrant.

f) Probation and Parole: Individuals on probation, parole, or supervised release enjoy a diminished expectation of privacy and may be subject to warrantless searches based on reasonable suspicion, or, potentially, without any particularized suspicion [91].

g) The Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i): Title III allows victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems [92]. And law enforcement can intercept the attacker's communication with the consent of the victim.

h) The 'Accessible to the Public' Exception, 18 U.S.C. § 2511(2)(g)(i): Section 2511(2)(g)(i) permits "any person" to intercept an electronic communication made through a system "that is configured so that … the communication is readily accessible to the general public."[66] Congress intended this language to permit the interception of an electronic communication that has been posted to a public bulletin board, a public chat room, or a Usenet newsgroup.

i) Private Search: This term is opposite the term "public search", in that it represents a private business or individual rather than the government performing the search. The fourth Amendment has restrictions on government and the ones who act as agents of the government or are instigated by government. For the individual who does the search as his/her own behavior, this private search is totally acceptable. For example, a repair man may find child pornography pictures *incidentally* in customer's computer with/without the consent of the customer and then the repair man report it to the police; an administrator may search and monitor malicious traffic under his charge and report to police. Law enforcement can accept the report and do investigations related with the search without any warrant/court order/subpoena.

In this section, we have distinguished investigation with warrant/court order/subpoena and investigation without warrant/court order/subpoena. Based upon what we talked

about here, we present a quick reference **Error! Reference source not found.** at the end of this paper. We list twenty computer forensic scenes with the corresponding answers to questions like: Does a law enforcement officer need a warrant/court order/subpoena in this situation? Is it legal or illegal to take action in that situation without a warrant/court order/subpoena? Researchers can follow this table to conduct their research in computer forensics. For the answers with (*), it means we make judgments based on our own knowledge.

IV. Researches Analysis

Normally, researchers have invented various methods to help law enforcement in computer forensic investigations. Many people may think that various attacks against privacy can also be adopted by law enforcements for surveillance and search of suspects. However, those attacks may be infeasible due to the law restrictions. Either their practical application is limited or some other simple methods may be easily enough performed under certain law restrictions. Yet of course, some attack methods are better than the existing techniques even under certain law restrictions.

Since we have understood the process of investigation in computer forensics, let check two published institute research papers and discuss their practical feasibilities.

A. Workable Method without Warrant/Court Order/Subpoena

In [22], the authors invent attack methods to help law enforcement to do forensic investigation in anonymous P2P system. Under their attack framework, law enforcement officers join the anonymous P2P system; do a query for child pornography pictures within the system. By collecting the delay time of the respond message from neighbors, law enforcement officers can identify whether the neighbors are sources or trusted nodes of the sources.

Their approach is simple and absolutely has no law restrictions. First, it is legal for everybody to observe the traffic under normal operations of the protocol in software. For example, search queries that broadcast to all peers and have no expected privacy. Second, law enforcement can analyze the incoming traffic such as a response to the attacker's search query without any law issues. The sender has no expected privacy in the responded message once the receiver received it.

We can see that such kinds of attack can be directly used in criminal investigations ahead of a warrant/court order/subpoena.

B. Workable Method with Warrant/Court Order/Subpoena

In our previous work [93], we invented an attack method to help law enforcement to do forensic investigation in an anonymous communication network system such as Tor or Anonymizer. In this attack framework, law enforcement officers monitor servers connected to criminals who are using anonymous communication network systems. Law enforcement can modify the traffic rate slightly at one side and collect the traffic rate at the other side, and by comparing the traffic rate, the law enforcement can identify the suspects.

In reality, it is not legal to monitor the servers directly. Let us take a look at two situations below. In situation one, assume law enforcement officers find a web-server which has both adult and child pornography pictures through traditional investigation method. They then find a lot of accounts on that server. Now they want to identify one account that may be downloading the child pornography pictures from the server. Law enforcement officers then apply a court order to monitor the ISP connected to the suspect. Normally, by checking the packets incoming and outgoing from/to the suspect's computer, law enforcement can identify the suspect. However, what if the suspect using anonymous software that law enforcement cannot decrypt the packets?

This attack method in [93] is to help law enforcement under such situations. By slightly modifying the traffic rate with an embedded PN code at the seized web-server and collecting the traffic rate at the suspect's ISP (they do not need to collect the entire packet, so they do not need a wiretap warrant), they can identify the suspect in the anonymous network system. Beyond the law issues, we claim the method is more effective than other methods [94].

In situation two, there are two different campus IT administrators that suspect that some people are communicating with an anonymous network system and they may be doing something illegal. So the two administrators discuss with each other and use the attack method to monitor the two gateways on the two campuses. They then identify who is communicating with whom and report their suspicion to law enforcement.

Through the two situations, we can see that such kind of attack cannot be directly used in criminal investigations. However, it is workable and legal as private search and has a little restrictions (a court order should be good enough) for law enforcement. Given the overhead and reduced budget, law enforcement may not be willing to adopt the tools.

We recommend that researchers could focus on crime scene investigations that do not need warrant/Court Order/Subpoena, particularly for traceback related network forensics.

V. Conclusion

In this paper, we discussed computer forensics investigations with related laws from a researcher's view. We classified law enforcement agent's actions as investigation with warrant/court order/subpoena and investigation without warrant/court order/subpoena. We recommend that researchers could focus on crime scene investigations that do not need warrant/Court Order/Subpoena for traceback related network forensics so that their research and development can be more easily accepted by law enforcement to generate a larger impact.

References

[1] http://www.internetworldstats.com/stats.htm, 10-25-2011.

[2] http://en.wikipedia.org/wiki/ENIAC, 10-25-2011.

[3] http://www.quincy.ca/timelines/forensic_computer_forensics.html, 10-25-2011.

[4] http://en.wikipedia.org/wiki/Digital_forensics, 10-25-2011.

[5] J. R. Vacca, "Computer Forensics-Computer Crime Scene Investigation", 2nd edition, Charles River Media, May 27, 2005.

[6] R. J. Walls, B. N. Levine, M. Liberatore and C. Shields, "Effective Digital Forensics Research is Investigator-Centric", *In Proc. USENIX Workshop on Hot Topics in Security (HotSec),* August 2011

[7] Kyllo v. United States, 533 U.S. 27 (2001).

[8] http://en.wikipedia.org/wiki/Wiretap_Act, 10-30-2011

[9] http://en.wikipedia.org/wiki/ECPA, 10-30-2011

[10] H. Marshall Jarrett, Michael W. Bailie, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", http://www.cybercrime.gov/ssmanual/

[11] http://en.wikipedia.org/wiki/Stored_Communications_Act, 10-30-2011

[12] http://en.wikipedia.org/wiki/Pen_register#Pen_Register_Act, 10-30-2011

[13] https://ssd.eff.org/your-computer/govt/privacy, 10-30-2011

[14] Katz v. United States, 389 U.S. 347 (1967)

[15] Wilson v. Moreau, 440 F. Supp. 2d 81, 104 (D.R.I. 2006)

[16] United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002)

[17] United States v. Butler, 151 F. Supp. 2d 82, 83-84 (D. Me. 2001)

[18] United States v. King, 509 F.3d 1338, 1341-42 (11th Cir. 2007)

[19] United States v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007)

[20] United States v. Gorshkov, 2001 WL 1024026, at *2 (W.D. Wash. May 23, 2001)

[21] United States v. Stults, 2007 WL 4284721, at *1 (D. Neb. Dec. 3, 2007)

[22] S. Prusty, B. N. Levine, M. Liberatore, "Forensic Investigation of the OneSwarm Anonymouse Filesharing System", I*n Proc. ACM Conference on Computer & Communications Security (CCS),* page 13, October 2011.

[23] United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992)

[24] United States v. Young, 350 F.3d 1302, 1308 (11th Cir. 2003)

[25] United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995)

[26] Hoffa v. United States, 385 U.S. 293, 302 (1966)

[27] Smith v. Maryland, 442 U.S. 735, 743-44 (1979)

[28] Couch v. United States, 409 U.S. 322, 335 (1973)

[29] United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986)

[30] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001)

[31] United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990)

[32] United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997)

[33] United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001)

[34] United States v. Beusch, 596 F.2d 871, 876-77 (9th Cir. 1979)

[35] United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001)

[36] http://en.wikipedia.org/wiki/Probable_cause, 10-30-2011

[37] Illinois v. Gates, 462 U.S. 213, 238 (1983)

[38] United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007)

[39] United States v. Grant, 218 F.3d 72, 76 (1st Cir. 2000)

[40] United States v. Carter, 549 F. Supp. 2d 1257, 1261 (D. Nev. 2008)

[41] United States v. Latham, 2007 WL 4563459, at *11 (D. Nev. Dec. 18, 2007)

[42] United States v. Hibble, 2006 WL 2620349, at *4 (D. Ariz. Sept. 11, 2006)

[43] United States v. Terry, 522 F.3d 645, 648 (6th Cir. 2008)

[44] United States v. Wilder, 526 F.3d 1, 6 (1st Cir. 2008)

[45] United States v. Gourde, 440 F.3d 1065, 1070-71 (9th Cir. 2006)

[46] United States v. Coreas, 419 F.3d 151 (2d Cir. 2005)

[47] United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006)

[48] United States v. Paull, 551 F.3d 516, 522 (6th Cir. 2009)

[49] United States v. Watzman, 486 F.3d 1004, 1008 (7th Cir. 2007)

[50] United States v. Newsom, 402 F.3d 780, 783 (7th Cir. 2005)

[51] United States v. Riccardi, 405 F.3d 852, 861 (10th Cir. 2005)

[52] United States v. Cox, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002)

[53] United States v. Doan, 2007 WL 2247657, at *3 (7th Cir. Aug. 6, 2007)

[54] United States v. Zimmerman, 277 F.3d 426, 433-34 (3d Cir. 2002)

[55] United States v. Frechette, 2008 WL 4287818, at *4 (W.D. Mich. Sept. 17, 2008)

[56] United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006).

[57] United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995)

[58] United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006)

[59] United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997)

[60] United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982)

[61] United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000)

[62] United States v. Long, 425 F.3d 482, 487 (7th Cir. 2005)

[63] United States v. Burns, 2008 WL 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008)

[64] United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008)

[65] O. S. Kerr, "Computer Crime Law", 2nd edition, West, October 23, 2009

[66] S. Rep. No. 99-541 (1986)

[67] Kaufman v. Nest Seekers, LLC, 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006)

[68] Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998)

[69] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)

[70] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-63 (5th Cir. 1994)

[71] Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003)

[72] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876-79 (9th Cir. 2002)

[73] United States v. Steiger, 318 F.3d 1039, 1047-50 (11th Cir. 2003)

[74] Mincey v. Arizona, 437 U.S. 385, 393 (1978)

[75] United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997)

[76] United States v. Young, 2006 WL 1302667, at *13 (N.D.W.Va. May 9, 2006)

[77] United States v. Morales-Ortiz, 376 F. Supp. 2d 1131, 1142 (D.N.M. 2004)

[78] United States v. Wall, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008)

[79] United States v. Reyes, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996)

[80] United States v. Megahed, 2009 WL 722481, at *3 (M.D. Fla. Mar. 18, 2009)
[81] United States v. Matlock, 415 U.S. 164 (1974)
[82] United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998)
[83] Trulock v. Freeh, 275 F.3d 391, 398, 403-04 (4th Cir. 2001)
[84] United States v. Lavin, 1992 WL 373486, at *6 (S.D.N.Y. Nov. 30, 1992)
[85] United States v. Durham, 1998 WL 684241, at *4 (D. Kan. Sept. 11, 1998)
[86] United States v. Ziegler, 474 F.3d 1184, 1191 (9th Cir. 2007)
[87] O'Connor v. Ortega, 480 U.S. 709 (1987)
[88] United States v. Cassiere, 4 F.3d 1006, 1021 (1st Cir. 1993)
[89] http://www.citmedialaw.org/legal-guide/california-recording-law, 10-31-2011
[90] http://en.wikipedia.org/wiki/Plain_view, 10-31-2011
[91] United States v. Knights, 534 U.S. 112, 122 (2001)
[92] United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998)
[93] J. Huang, X. Pan, X. Fu and J. Wang, "Long PN Code Based DSSS Watermarking", in Proceedings of Infocom, 2011
[94] http://epic.org/privacy/streetview/, 10-31-2011
[95] United States v. Crist, 627 F.Supp.2d 575 (M.D. Pa. 2008)
[96] State v. Sloane, 939 A.2d 796 (N.J. 2008)

TABLE 1 WARRANT/COURT ORDER/SUBPOENA IN DIGITAL CRIME SCENES

#	Scenes	Need warrant/court order/subpoena?
1	IT on campus is trying to log all wired traffic headers including link layer header, IP header, and TCP/UDP header if available. That traffic is transmitted within the campus' cables and devices.	No need
2	IT on campus is trying to log all wired traffic including packet headers and packet content. That traffic is transmitted within the campus' cables and devices. Normally, the campus policies eliminate a user's expectation of privacy.	No need
3	A law enforcement officer outside a person's house/apartment logs all wireless traffic headers including link layer header, IP header, and TCP/UDP header if available. The traffic is not encrypted. Refer to WarDriving and the Google street view, which collects all unencrypted wireless data [94].	No need (*)
4	A law enforcement officer outside a person's house/apartment logs all wireless traffic including routing headers and payload. The traffic is not encrypted. Refer to Google street view case [94].	Need (*)
5	A law enforcement officer outside a person's house/apartment is trying to log all wireless traffic headers including link layer header, IP header, and TCP/UDP header if available. The traffic is encrypted. Refer to the WarDriving scene.	No need (*)
6	A law enforcement officer outside a person's house/apartment is trying to log all wireless traffic including routing headers and payload. The traffic is encrypted.	Need (*)
7	A law enforcement officer in a public wired internet is trying to log the packets' headers including link layer header, IP header, and TCP/UDP header if available and the size of the packet. Officer either gets the consent from the ISPs or obtains a warrant/court order/subpoena.	Need
8	A law enforcement officer in a public wired internet is trying to log the entire packets' information including headers and payload. Officer either gets the consent from the ISPs or obtains a warrant	Need
9	A law enforcement officer is using normal p2p software and trying to collect public information shown on the software. The information is such as other user's name and the file names they share in the p2p network.	No need
10	A law enforcement officer is using anonymous p2p software and trying to collect public information shown on the software. The information is such as other user's name and the file names they share in the p2p network.	No need
11	A law enforcement officer is trying to collect public website's content. Anybody can access the website.	No need
12	A law enforcement officer is trying to investigate a hidden web server at Tor. The hidden web server is as an ISP	Need
13	A law enforcement officer is trying to build a Tor node and do investigation on the Tor node. Not a private search.	Need
14	A law enforcement officer is trying to monitor Anonymizer? The anonymizer server is as an ISP.	Need
15	Assume a victim finds his/her computer is under attack, the victim consents the law enforcement officer to monitor the activities on the victim's computer, includes the attack's activities.	No need
16	Assume a victim finds his/her computer is under attack, the victim consents the law enforcement officer to monitor the activities on the victim's computer, includes the attack's activities. However, the law enforcement is trying to monitor/collect data in attacker's computer.	Need
17	A law enforcement officer is trying to collect content in a public chatting room. Anybody can access the website, with or without registration.	No need
18	A law enforcement officer legally obtained a hard drive and is trying to run hash function to search entire hard drive for a particular file (child pornography).[95]	Need
19	A law enforcement officer legally obtained a data base and then tries to mine the data for hidden information.[96]	No need
20	The defendant has been arrested, law enforcement officer then use defendant's user name and password to obtain the defendant's data on a remote computer.	No need