Cyber Forensics and Admissibility of Digital Evidence

Cyber Forensics and Admissibility of Digital Evidence
by Dr. Swati Mehta*
Cite as: (2012) PL January S-23â€

Section 65-B of the Evidence Act deals with admissibility of electronic records as evidence in the court of law. The computer holding the original evidence does not need to be produced in court. A printout of the record or a copy on a CD-ROM, hard disk, floppy, etc. can be produced in the court. However, some conditions need to be met and a certificate needs to be provided.1

Law enforcement agencies face a new challenge in dealing with cyber crimes. Criminal acts are being committed and the evidence of these activities is recorded in electronic form. Besides, crimes are being committed in cyberspace. Evidence in these crimes is almost always recorded in digital fashion. It is important that computer security professionals be aware of some of the requirements of the legal system and understand the developing field of computer forensics.2

The reality of the information age is having a significant impact on the legal establishment. One major area in which this is being felt is that of the acquisition, authentication, evaluation and legal admissibility of information stored on magnetic and other media.3 This information can be referred to as digital evidence. Computer forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law.4

In the paper-based world, law assumes a process which is mutually understood and observed by all the parties. Almost without thinking, a four-part process takes place, involving acquisition, identification, evaluation and admission. When we try to apply this process to digital evidence, we see that we have a new set of problems.5

Digital evidence, by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye. It is only logical that the process used in the case of digital evidence mimic the process that is used for paper evidence. Because each step requires the use of tools or knowledge, the process must be documented, reliable and repeatable. The process itself must be understandable to the court.

Acquisition of evidence is both a legal and technical problem. In fact, these two aspects are irrevocably related. The law specifies what can be seized, under what conditions, from whom, and from where it may be seized. The determination of what a particular piece of digital evidence is, requires its examination. Is it a particular file, a word processing document or an executable program? It may require examination to determine where a particular piece of evidence is physically located. Is the file on a local hard drive or is it on a server located in another legal jurisdiction? In short, it may be necessary to show a technical basis for obtaining the legal authority to search. Likewise, it may require technical skills in order to actually accomplish the search. The product of this phase is usually raw media, devoid of meaning or usefulness.6

Actually identifying a piece of digital evidence represents a three-step process. It must be definable in its physical form. That is, that it resides on a specific piece of media. Next, it must be identifiable as to its logical position. Where does it reside relative to the file system? Lastly, we must place the evidence in the correct context in order to read its meaning. This may require looking at the evidence as machine language, for example, ASCII or EBCDIC, or by means of an application (program). Each of these steps requires technical skills and may subsequently require testimony at trial. At this point, we have translated the media into data. Evaluation of the data involves both technical and legal judgments. Data that is placed in its proper context is called information. From a technical standpoint, it may be possible to make conclusions as to how the data was produced, when and by whom. The legal issues are the relevance of the information, its reliability, and who can testify to it.

Cyber crime scene investigation A digital investigation is a process to answer questions about digital states and events. The basic digital investigation process frequently occurs by all computer users when they, for example, search for a file on their computer. They are trying to answer the question â€œwhat is the full address of the file named important.doc?â€• In general, digital investigations may try to answer questions such as â€œdoes file X exist?â€•, â€œwas program Y run?â€•, or â€œ user Z account compromised?â€•

A digital forensic investigation is a special case of a digital investigation where the procedures and techniques that are used will allow the results to be entered into a court of law. For example, an investigation may be started to answer a question about whether or not contraband digital images exist on a computer.7 The term â€œdigital forensic investigationâ€• is preferred to â€œdigital forensicsâ€• because the process that is associated with â€œdigital forensicsâ€• is much more similar to physical crime scene investigation than to physical forensics. â€œPhysical forensicsâ€• is used to answer a more limited set of questions than a general investigation. Physical forensics is used to â€œidentifyâ€• a substance, which determines the class of the substance. For example, a red liquid could be identified as blood or fruit juice.8 The process to determine how someone compromised a computer and identify what they had access to is much more involved than identification and individualisation. It is a process of searching for evidence and then analysing it.9

Investigation process There is no single procedure for conducting an investigation. An intuitive procedure is to apply

the same basic phases that are used by police at a physical crime scene, where we instead have a digital crime scene.
Â· The first step is preservation, where we attempt to preserve the crime scene so that the evidence is not lost.
Â· The second step is to survey the crime scene for the obvious evidence. The â€œobviousâ€• evidence is the evidence that typically exists with investigations of this type.10
Â· After the obvious evidence has been found, then more exhaustive searches are conducted to start filling in the holes. With each piece of evidence that is found, there could be questions about how it got there.11

Cyber crime investigation Cyber crime investigation is the collecting, analysing and investigation of digital evidence and cyber trails,12 which may be found in computer hard disks, cell phones, CDs, DVDs, floppies, computer network, or the internet. Also, these may be hidden in pictures, encrypted files, password protected files, deleted files, formatted hard disks, deleted e-mails, or chat transcripts. These are the basic rules of cyber crime investigation.13 The findings of a cyber crime investigation will be admissible in a court of law only if these three basic rules are followed:
1. The cyber crime investigators must be skilled competent professionals. This is essential so that they can properly conduct the investigation, collect the relevant evidence and instil confidence in the court about the admissibility of the evidence.
2. The original digital evidence must never be tampered with or altered. As far as practical, investigators must work on the image/clone of the original evidence. If that is not practical then extreme care and caution must be taken while working on the original evidence.14
3. A detailed and accurate audit trail must be maintained. The chain of custody forms and other audit trail documents must be meticulously maintained. Any lacuna in these documents casts suspicion on the entire findings of the investigation.

Digital evidence: collection and extraction Before digital data can be considered evidence of an incident, it must first be collected. Collecting forensic evidence for the purposes of investigation and/or prosecution is difficult at the best of times, but when that evidence is electronic an investigator faces extra complexities.15 Computer transactions are fast, they can be conducted from anywhere, through anywhere, to anywhere; they can be encrypted anonymous and generally have no intrinsic identifying features such as handwriting and signatures to identify those responsible. Any â€œpaper trailâ€• of computer records can be easily modified or destroyed or may exist only temporarily. Worse still, auditing programs may automatically destroy the records left when they are finished with them.16

Currently there is nothing that can be considered a true electronic signature for the purpose of criminal law in the same way that DNA or fingerprints do for other criminal investigations.17 Even though technology is constantly evolving, investigating electronic crimes will always be more difficult due to the ability to alter data easily and because transactions may occur anonymously or deceptively. Given these obstacles, one may ask: why bother collecting the evidence in the first place? There are two main reasonsâ€”future prevention and responsibility.

Future prevention Collecting electronic evidence involves investigating how the attack occurred. Without knowing what happened an organisation remains vulnerable to this type of attack and has little hope of stopping further attacks (including from the original attacker). It would be analogous to being defrauded for a large sum of money and not bothering to determine how the fraud was perpetrated. Even though the cost of collection can be high, the cost of repeatedly recovering from compromises is much higher, both in monetary and corporate image terms.18

Responsibility There are two responsible parties after an attackâ€”the attacker and the victim. The attacker is responsible for the damage done and the only way to bring him to justice is to seek recompense and to deter further attacks is to convict them with adequate evidence to prove his actions.19

Victims also have an ethical, if not legal, responsibility to the community. Sites that have been compromised and used to launch attacks against third parties may find that theyâ€”not the attackerâ€”are sued for liability for the attack. The grounds for such a lawsuit might be that by failing to comply with the accepted minimum standards in network security they acted negligently. Public companies have a particular responsibility to their shareholders to ensure that business continuity and data confidentiality and integrity are not compromised. For ethical reasons, some victims may see merit in sharing information gathered after a compromise with others to prevent further attacks.

Methods of collection There are two basic forms of collectionâ€”â€œfreezing the sceneâ€• and â€œhoneypottingâ€•. The two a mutually exclusive, you can collect frozen information after or during any honeypotting.

Freezing the scene involves taking a snapshot of the system in its compromised state. The necessary authorities should be notified (for instance the police and our incident response and legal teams) but we should not go out and tell the world just yet. Next, one should then start to collect whatever data is important onto removable non-volatile media in a standard format and make sure that the programs and utilities used to collect the data is also collected onto the same media as the data. All data collected should have a cryptographic message digest created and those digests should be compared to the original for verification.

Honeypotting is the process of creating a replica system and luring the attacker into it for further monitoring. A related methodâ€”sandboxingâ€”involves limiting what the attacker can do while still on the compromised system so they can be

monitored without much further damage. The placement of misleading information and the attackerâ€™s response to it is a good method for determining the attackerâ€™s motives. We must make sure that any data on the system that refers to the attackerâ€™s detection and actions should be either removed or encrypted; otherwise they can cover their tracks by destroying it.

Preservation of digital evidence The success of a computer forensic investigation is determined by both the availability and preservation of digital evidence sources. Without any specific malicious intent, organisations suffering data compromise commonly tamper with evidence sources before engaging a formal forensic investigation, handing investigators an unnecessary handicap.

A constant challenge facing computer forensic investigators is the inherent fragility of digital evidence. When handled improperly, digital evidence can easily be altered or even eliminated, creating a significant investigative handicap. In the minutes and hours immediately following the discovery of a crime involving digital evidence, the actions taken by the first respondent should ensure that evidence is preserved in a secure and forensically sound manner.20

Preservation measures Most of the agencies take some measures to prevent deletion of digital evidence.

Searches, raids and inspections A number of agencies reported that when entering the premises, personal computers, data carriers and other relevant electronic equipment and network cables are unplugged. One agency reports that upon entry to the premises, establishing control is one of the first priorities. In the context of digital evidence, controlling the premises may require that computer users be moved away from keyboards of computers identified as key search priorities and that portable devices covered by the search warrant be collected and held under the control of an officer until such time as they have been examined. The search team leader will request the company official to direct company staff not to impede the inquiry by deleting, destroying or removing any records (including digital records) from the premises covered by the warrant during the course of the search. The Act requires the company official to allow the officer searching at the premises to use or â€œcause to be usedâ€• any computer system at the premises.21

Compelled discovery One agency reported that digital information must be produced in â€œread-onlyâ€• digital format so that there is no chance that it might be inadvertently changed or deleted by the agencies or investigative staff. Finally, staffs make copies of the electronic media (e.g. CD-ROMs) containing the digital evidence as soon as it has been received by the agency. The â€œoriginalâ€• copy of the media is then secured with other important documents and is not examined or reviewed for evidence; thereafter, staffs handle only the â€œworking copiesâ€• of the media (i.e. a duplicate CD-ROM).22

Authentication of digital evidence The legal rules of evidence present strong challenges to the use of digital information as legally acceptable records. A technique is needed whereby digital recordings (including images) can be offered and accepted as legal evidence. The most difficult rule of evidence for digital recording to meet is authentication.

Authentication is the means to prove, first, the conditions under which the record was made, and, second, that the recording is offered in its original unaltered form.23

The conditions under which the record was made include date, time, location, people present, and other relevant conditions. The best evidence rule requires that the original document (recording) be admitted into evidence if it is available. Digital recordings are very susceptible to alteration. When the originality of a recording is questioned, often expert witnesses provide testimony as to whether or not the recording appears altered.

Technique for authentication of digital information24 Accurate Automation Corporation (AAC) has been developed to authenticate digital recordings by automatically including authentication information in records at the time of recording that can be used later to prove the conditions in which the recording was made and to prove the originality of the recording. This technique is based on encryption processes endorsed by national security agencies using very large keys which would require centuries to defraud on the fastest available computers. Yet, this technique does not impair the use or viewing of the recording by existing tools. In fact, this technique does not impair the alteration of the digital recording, but it provides a means to detect that an alteration has occurred. This technique is called â€œauto-notaryâ„¢â€• and is owned ar has patent pending by Accurate Automation Corporation of Chattanooga, Tamil Nadu.

Two information elements are automatically included in the digital record at the time of recording with auto-notaryâ„¢. One information element is the context in which the recording is made. The other information element is a digital signature of the combination of the original recording and the context information. Adding these two information elements at the time of recording is the auto-notaryâ„¢ encode process. If the authenticity of a recording is questioned, the recording can undergo the auto-notaryâ„¢ decode process which views the context information element and determines if the recording is unaltered. The techniques of auto-notaryâ„¢ does not impair viewing of digital recordings or even altering of digital recordings, but simply provides a means to determine the authenticity of the recording. Auto-notaryâ„¢ is applicable to any digital recording such as photographs, motion video, audio, financial data, and personnel or equipment records. In addition, auto-notaryâ„¢ can be applied to office automation such as e-mail, word processing, spreadsheets, and desktop publishing.

When a photograph is introduced as evidence, the context in which the photograph was taken and the degree to which the photograph matches the original recording are both questioned. Traditionally, the person taking the photograph offers testimony as to the date, time, location, etc. of the photograph. In addition, it may be necessary to obtain testimony of people involved with the chain of custody of the photograph. It may be necessary to offer testimony from expert witnesses to attest to the fact that the photograph is unaltered. The ease with which digital photographs can be altered has deterred the use of digital photography in situations where a photograph is likely to be used as evidence. A digital photograph that has been through the auto-notaryâ„¢ encode process can undergo the auto-notaryâ„¢ decode process in the presence of the judge to prove the context of the photograph and the unaltered condition of the photograph. In addition, it may be appropriate to offer altered photographs derived from the original that are zoomed or brightened or enhanced in some way. But these alterations can be offered side by side with the original.

Another form of authentication in use today is â€œwatermarkingâ€•. The advantages of auto-notaryâ„¢ over watermarking are: Auto-notaryâ„¢ leaves the recording completely unaltered, whereas watermarking embeds the authentication information within the recording (image) in a manner that is supposedly imperceptible to a user. Auto-notaryâ„¢ includes the context of the recording within the authentication, whereas watermarking only verifies the originality but not the context of the recording.

Some organisations attempt to shield recorded information from alteration by hiding the information within encrypted records or requiring passwords for access to records. These techniques limit the ease of use of digital records, and the security can always be questioned since alterations cannot be proven with shielded records.

Errors, uncertainty and loss in digital evidence The need for measuring error in forensic analysis of computer systems is apparent in the history of scientific evidence.25 Generally accepted guidelines for evaluating scientific evidence include quantifying the techniqueâ€™s potential rate of error.26 More rigorous requirements are being called for.

Separation: Time, space and abstraction Digital data are separated by both time and distance from the events they represent. A log file that records network activities is a historic record of events that happened at various places in the world. Even when viewing network traffic using a sniffer, there is a delay between the activity that generated the traffic and the display of the data on the monitor. Additionally, networks are comprised of layers that perform different functions from carrying electronic pulses over network cables to presenting data in a form that computer applications can interpret.27

Log tampering, corruption and loss Errors and losses can be introduced into log files at various stages:
Â· At the time of the event
Â· During observation
Â· At the time of the log creation
Â· After creation
Â· During examination
Â· During analysis

When dealing with networked systems, it is crucial to extend oneâ€™s thinking beyond the single computer and consider other connected systems. However, one should keep in mind that DNS records can be modified to make an attackerâ€™s computer appear to be a trusted computer, logging programs such as top-wrappers can be maliciously altered,28 and many other components of a network can be tampered with to create error and loss.

Quantifying and reducing losses Because of the transient nature of evidence on a network, there is usually only one opportunity to capture it, and it can be difficult to determine what information was not collected. Although it may not be possible to infer the content of lost datagrams, it is useful to quantify the percentage loss. Quantifying the amount of loss gives a sense of completeness of the logs and the resulting crime reconstruction. High losses during the monitoring and collection phase translate to low level of certainty in the crime reconstruction phase. Furthermore, quantification can help identify and minimise the cause of data loss.

Errors in reconstruction and interpretation Given the complexity of networked systems, large amounts of data, and occurrence of evidence dynamics there is a high potential for mistakes and misinterpretations in the analysis phase of an investigation. Tools exist to help us process and examine the vast amounts of data common in network investigations but these tools add another layer of abstraction and are useful only when sufficient data are obtained and the meaning of the data are understood. Windows Event Log analysis provides a useful example of how analysis tools can introduce errors. To facilitate analysis of Windows NT Event Logs, many examiners dump the log entries into a text file using dumpel or dempevt. Although dempevt presents more information than dumpel, it can incorrectly interpret date/time stamps after one hour is inserted for daylight savings time. The output from dempevt fails to correct for the time change and represents times prior to daylight savings one hour off.29

To reduce the incidence of incorrect conclusions based on unreliable or inaccurate data it is necessary to quantify uncertainty and effect correction whenever possible. In addition to using corroborating data from multiple, independent sources, forensic examiners should attempt to rate their level of confidence in the relevant digital evidence. Using of

systematic method like practical approach to categorising uncertainty in digital data to qualify conclusions helps decision-makers assess the reliability of the information they are being given and anticipates the challenges that will be raised in courts as attorneys become more familiar with digital evidence. Describing measures taken to document and minimise loss of data can further raise the confidence in evidence collected from a network.

Digital evidence: reliability When one examines the issue of reliability of digital evidence there arises a number of questions. Should forensic software (digital evidence) be entitled to a judicial presumption of reliability? When, if ever, should courts compel non-party forensic software vendors to reveal proprietary source code to party experts in order to assure a fairer trial? And what does reliability mean in the context of digital evidence anyway?

These questions have been raised by a recent criminal prosecution in Florida. In Florida v. Bjorkland30, the defendant was charged with driving under the influence of alcohol (DUI). In response, the defendant moved to exclude evidence of intoxication obtained from the Intoxilyzer 5000 breath-alcohol analysis computer (IT5000). Although the defendant advanced several theories in support of her motion, the broader issue presented by the case is whether experts should be entitled to audit software source code to ensure the reliability of digital evidence. The Court held that when the source code is material to the theory of defense then expert is entitled to audit software source code to ensure the reliability of digital evidence. At the same time the source code shall be disclosed and delivered only to expert and he shall not disclose to any other person and shall return the information to the State once he has completed the examination.

Courts have a seemingly unflappable faith in the ability of software to render reliable evidence. Broadly speaking, this â€œpresumption of reliabilityâ€• is well entrenched in American law. For example, in Olympic Insurance Co. v. H.D. Harrison Inc.31, the Court wrote that digital evidence had a â€œprima facie aura of reliabilityâ€•32. Likewise, in United States v. Moore33 the Court noted that â€œordinary business circumstances â€¦ suggest trustworthiness. â€¦ at least where absolutely nothing in the record in any way implies the lack thereofâ€•34. Similarly, in People v. Martinez35, the Court noted that testimony on the â€œacceptability, accuracy, maintenance, and reliabilityâ€• of computer software is not prerequisite to admission of computer records.36 And in Missouri v. Dunn37, the appellate court agreed with the trial court in â€œconcluding that such records were uniquely reliable in that they were computer generated rather than the result of human entriesâ€•.38 Although the presumption of reliability may have found roots in the context of business records, it is by now so pervasive that it should be recognised to be coextensive with the law of digital evidence itself.39

As it currently stands, the presumption of reliability has two important problems. First, it facilitates the admission of inaccurate digital evidence. When forensic software lacks independent, thorough and scientific testing, and when it may have been prematurely sold to customers in beta form so as to meet quarterly sales requirements, there is little justification for presuming either reliability or unreliability, that is, we should not presume to know one way or the other. There is a further problem with the presumption of reliability. By facilitating the admission of inaccurate results, the presumption of reliability is economically inefficient in that it fails to force developers to internalise costs.40 Instead, costs from code defects are passed on to parties in the form of faulty criminal convictions, improper civil judgments, lost opportunity, and the like. If these costs were assigned monetary values, in many cases the failure to correct various forensic software defects would impose on society a net loss.

At the level of cases and controversies, judges should more closely scrutinise digital evidence emerging from cyber investigations. One way of elevating the foundational requirements for such evidence is to consider whether the software yielding it has been validated in accordance with the procedures set forth in Daubert v. Merrell Dow Pharmaceuticals Inc.41. The Court in this case provided a four-part test to assist in the determination of reliability of scientific evidence. In assessing reliability, trial courts applying federal law should consider:

(1) whether the theory or technique has been reliably tested;
(2) whether it has been subjected to peer review;
(3) the known or potential rate of error of the theory or technique has been done;
(4) whether the technique is generally accepted.

The holding of Daubert42 was subsequently extended to technical evidence in Kumho Tire Co. v. Carmichael.43

What should proper Daubert testing mean in the context of forensic software? The independent source code review of all software is perhaps the singlemost revealing method to uncover defects. In many cases, however, the proprietary nature of source code means that it is unavailable for such review. In such cases, unless a court compels source code disclosure, black box testingâ€”also referred to as zero-knowledge application reviewâ€”becomes an indispensable way to validate particular software scientifically.

Inadequacy of existing law The criminal procedure changes considerably when we switch from traditional investigations, involving eyewitness testimony and physical evidence, to investigations requiring the collection of digital evidence.44

There are three basic mechanisms of digital evidence collectionâ€”the collection of stored evidence from third parties, the collection of stored evidence from the target, and the collection of evidence in transit. Applying existing doctrines to these three mechanisms one finds several difficulties. The traditional rules tend not to translate well to the new facts. Caution is

warranted. Surprisingly few cases exist that apply traditional doctrine to the collection of digital evidence. Mapping the old rules on to the new facts requires some speculation. At the same time, a comparison of the basic contours of existing law and the dynamics common to digital evidence cases demonstrates the poor fit between them. In many circumstances, the traditional rules fail to provide any real limit on law enforcement practices. In other circumstances, they allow phantom privacy threats to block necessary investigative steps.

I. Evidence from third parties and the subpoena process Consider the first stage of most electronic crime investigations, in which investigators contact system administrators and obtain stored evidence relating to the crime from servers used in the course of the crime.45 This process raises important privacy concerns suggesting the need for careful legal regulation.46 Internet users routinely store most if not all of their private information on remote servers, and all of that information is available to system administrators.47 System administrators can read private e-mail, look through stored files, and access account logs that record how individual subscribers used the network. As a result, the power to compel evidence from ISPs can be the power to compel the disclosure of a userâ€™s entire online world. Plus, disclosure can occur without notice to the user, and it can involve multiple accounts. The power to compel evidence from ISPs can be the power to disclose the online profile of hundreds or even thousands of users at once, all in total secrecy.

Currently, the criminal procedure provides virtually no privacy protection to regulate this process. Investigators can compel system administrators to disclose information stored on their servers using subpoenas. The limits of burdensomeness are similarly toothless in the context of electronic evidence. It is generally simple for an ISP to copy voluminous files and give the copy to investigators.48 ISPs find it easier to hand over information en masse rather than filter painstakingly through files to identify the precise file sought. The person under investigation need not be informed of the subpoenaâ€™s existence.49

In the early case of Boyd v. United States50, the Supreme Court of US took the view that an order to compel the disclosure of evidence should be regulated just as carefully as a direct search involving the police knocking down your door.51 The Court backed off that standard twenty years later in Hale v. Henkel52, however, when it replaced Boyd with the low threshold that a subpoena satisfied the â€œright to privacyâ€• so long as it was not â€œsweepingâ€•.53

Officers can simply fax a copy of the subpoena to the ISPâ€™s headquarters and await a package or return fax with the relevant documents.54 No technical expertise or travel to the ISP is required. A reasonable rule developed in response to the realities of physical world investigations turns into an unreasonable and unbalanced rule when applied to the new facts of digital crime investigations.

II. Prospective surveillance and the problem of wiretapping We encounter similar problems when investigators conduct prospective surveillance by monitoring a stream of internet traffic. Prospective surveillance can be broad or narrow, depending on what information the investigators seek. The basic investigative step is the same in every case, however, the only difference between broad and narrow surveillance lies in how the filter is configured. This is true because the internet works by jumbling information together during transmission, and tasking computers that receive the information to reassemble it.55

The zeros and ones passing through a particular cable at a particular time could be anythingâ€”part of a very private message, the front page of NYTimes.com, an image of pornography, a hackerâ€™s command to a remote server, or generally meaningless computer-to-computer network traffic. The filter setting determines the information collected, with an open setting resulting in total surveillance and an advanced setting tightly regulating the type and amount of information collected.

The problem that arises is very complex. The police need a warrant to enter oneâ€™s home regardless of the purpose.56 Similarly, the police do not need a warrant to collect and analyse oneâ€™s private documents left out in a public park.57 The traditional focus on the entry into the space makes sense for physical investigations. In the physical world, regulation of where an officer goes determines what the officer will see, smell, hear and feel. The officerâ€™s human senses will record observations that the officer can later recall and testify about in court. Regulating entry therefore serves as a functional way of regulating evidence collection. This focus makes little sense when applied to prospective surveillance. The entry to the tapped line of internet traffic occurs regardless of whether the monitoring is extremely narrow or breathtakingly broad. Instead of representing a crossing of the line between public and private, entry is now merely a prerequisite for any evidence collection.58

III. Searching the targetâ€™s computer and the warrant rules The final stage of computer crime investigations exposes particularly deep problems of fit between traditional rules and the new facts. At this stage, the police seize and then analyse the suspectâ€™s personal computer. A warrant is plainly required, both to enter the home and to seize the suspectâ€™ property.59 But how much does the warrant actually limit what the police can do? In traditional cases, the rules governing the warrant process ensure that the search and seizure remain relatively narrow. The warrant must name both the specific place to be searched and the specific evidence to be seized.60 The seizure must be limited to the evidence described in the warrant, if any, which itself is limited by the scope of probable cause to believe that the evidence is on the premises, as well as other evidence discovered in plain view during the course of the search. These rules help ensure that warrant searches do not devolve into general warrants that authorise general rummaging through a suspectâ€™s

property.

Applying these rules to digital evidence, however, sets up a series of puzzles. For example, the first step of the seizure process, in which investigators take the defendantâ€™s computer off-site for forensic testing is necessary for practical reasons. But it cannot be justified under the traditional rules. In many cases, computer hardware is merely a storage device for evidence rather than evidence itself. The evidence is the electronic file that the police are looking for and that just happens to be stored along with many innocuous files inside the container of the computer hardware.61 Under traditional rules, then, seizing computer hardware to get a handful of files would appear to be overbroad.62 It is roughly analogous to seizing an entire house and carting off its contents to mine them for evidence of crime.63

New criminal procedure Digital evidence exposes the contingency of the existing rules. It changes the basic assumptions of the physical world that led to the prior rules of investigation.64 It is interesting and fruitful to jump-start thinking about new solutions, rather than lay out detailed proposals. Such changes may have begun to occur already. A new set of rules applicable in computer crime investigations has begun to emerge.

I. Collection of stored evidence from third parties The increase in the amount and importance of information stored with third parties in a network environment creates the need for new limits on the subpoena power. The most obvious limit would come in the form of a higher legal threshold to compel disclosure; the law should require a more burdensome factual showing to obtain private information about suspects, such as their personal e-mail. Other limits may be considered as well.65 Perhaps the law should limit the number of target accounts that can be compelled at any one time, at least absent special justification. Perhaps prior notice should be required in some cases, or targets of investigations should be informed within a period of time after the disclosure occurs. Use of restrictions might be a good way to limit the dangers arising from otherwise broad disclosures.66

II. Prospective surveillance The mechanisms of prospective surveillance also require a new legal regime. The most basic need is for the relevant legal thresholds to focus, to the extent possible based on existing technology, on the type of information to be collected rather than on whether the space to be entered is public or private. The rules should attempt to correlate the showing required to conduct surveillance with the degree of the privacy threat raised by that type of surveillance. When a filter is configured to collect information of a type that tends to be private, a high threshold should be required. In contrast, prospective surveillance should be allowed under a lower threshold when less private information is collected. This approach would require the law to classify internet communications based on the degree of the privacy interests at stake.67

For example, the classification on the basis of the following categories: The first category would be the prospective surveillance of â€œcontentsâ€• of communications,68 and the second, prospective surveillance of â€œdialing, routing, addressi signalling informationâ€• (DRAS).69 The former is the more private category of communication. Although its scope is not entirely clear, it includes the contents of e-mails and probably the text of internet commands70 and search terms.71 The latter is the less private category of communications, including internet packet headers, e-mail addresses, and other data used for routing internet communications (and, presumably, anything else that is not contents).72

III. The computer forensics process The computer forensics process also needs a regime of rules tailored to the privacy threats and needs raised by modern uses of computers. On the one hand, the law should respect technological limitations of existing search methods and techniques. On the other hand, the rules should look beyond the traditional dynamic of regulating searches and seizure to counterbalance the burden that such technical limitations may impose. For example, if technical needs require off-site searches of seized computers, then off-site searches should be allowed. But the law need not stop there.

The rules might provide an explicit mechanism allowing suspects to stipulate that a mirror image of their computers is accurate and then enjoy a right to have their computer returned within a specific period of time.73 The rules might also require that investigators erase any copies of seized files when a criminal case has been closed, or at the very least bar investigators from opening or reviewing seized computer files after that point absent special court authorisation.

A number of judges have concluded that computer searches are â€œspecialâ€•74, â€œuniqueâ€•75, and â€œdifferentâ€•76, for new rules of criminal procedure that restore the function of the old rules given the new facts. Taken as a whole, such changes would attempt to balance law enforcement needs and individual rights in property and privacy in light of existing technological realities.77

Conclusion Whereas computer forensics is defined as â€œthe collection of techniques and tools used to find evidence in a computerâ€•, digital forensics has been defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations.

Maintaining the integrity of digital evidence throughout the process of examination presents different problems from those encountered when handling traditional physical or documentary evidence. Mistakes in interpretation and analysis

can be reduced by rigorous application of the scientific methodâ€"performing exhaustive investigation and research, questioning all assumptions, and developing a theory that explains the facts. Ultimately, abiding by the scientific method will help forensic examiners to avoid egregious errors. Carefully exploring potential sources of error, hypothesis testing and qualifying conclusions with appropriate uncertainty will protect forensic examiners from overstating or misinterpreting the facts.

Digital evidence should trigger new rules of criminal procedure because computer-related crimes feature new facts that will demand new law. The law of criminal procedure has evolved to regulate the mechanisms common to the investigation of physical crimes, namely, the collection of physical evidence and eyewitness testimony. Existing law is naturally tailored to law enforcement needs and privacy threats they raise. Digital evidence is collected in different ways than eyewitness testimony or physical evidence. The new ways of collecting evidence are so different that the rules developed for the old investigations often no longer make sense for the new.

* . Gold Medalist, Assistant Professor, Faculty of Law, National Law University, Jodhpur.

â€ . Simultaneously published in the SCC Journal Section at (2011) 5 SCC J-54.

- Rohas Nagpal, Cyber Crime & Digital Evidence-Indian Perspective (Asian School of Cyber Laws, 2008).
- H.C. Catherine, Organizing for Computer Crime Investigation and Prosecution (National Institute of Justice, Washington DC 1989).
- George Garner, â€œForensic Acquisition Utilitiesâ€• http://users.erols.com/ gmgarner/forensics.
- Basic Considerations in Investigating and Proving Computer-Related Federal Crimes (United States Deptt. of Justice, U.S. Govt. Printing Office, Washington DC 1988).
- Donn B. Parker, Computer Crime: Criminal Justice Resource Manual (National Institute of Justice, Washington DC 1989).
- Guidelines for Searching and Seizing Computers (United States Deptt. of Justice, U.S. Govt. Printing Office, Washington DC 1994).
- â€œComputer Forensic Tool Testing (CFTT) Groupâ€• National Institute of Standards and Technology http://www.cftt.nist.gov..
- Fred Smith and Rebecca Bace, A Guide to Forensic Testimony (Addison Wesley, 2003).
- Brian D. Carrier, Basic Digital Forensic Investigation Concepts (7-6-2006).
- â€œDisk Imaging Tool Specificationâ€• National Institute of Standards and Technology, October 2001 http://www.cftt.nist.gov/DI-spec-3-1-6.doc..
- Ibid.
- Supra, n. 1.
- Ibid, 107.
- Ibid, 108.
- Steve Romig, â€œForensic Computer Investigationsâ€• 2000 http://www.net.ohio-state.edu/ security/talks/2001-10_forensic-computerinvestigations/.
- Bryon S. Collie, â€œIntrusion Investigation and Post-Intrusion Computer Forensic Analysisâ€• 2000 http://www.usyd.edu.au/su/is/comms/security/intrusion_investigation.html.
- Bryon S. Collie, â€œCollecting and Preserving Evidence after a System Compromiseâ€• 2000 http://mangrove.nswrno.net.au/dist/public/auugsec2000/Collecting%20and%20Preserving%20Evidence%20after%20a%20System%20Compromise.ppt.
- R. McKemmish, â€œWhat is Forensic Computing?â€• Australian Institute of Criminology, June 1999 http://www.aic.gov.au/publications/tandi/ti118.pdf.
- Dominique Brezenski and Tom Killalea, â€œGuidelines for Evidence Collection and Archivingâ€• Internet Engg. Task Force, July 2000 http://www.globecom.net/ietf///draft/draft-ietf-grip-prot-evidence-01.html.
- Christopher L.T. Brown, â€œComputer Evidence, Collection & Preservationâ€• Charles River Media, Hingham MA, 2006 http://www.delmarlearning.com/ charlesriver/.
- â€œGathering of Digital Evidenceâ€•, Ch. 3, Anti-cartel Enforcement Manual, Cartel Working Group, Enforcement Techniques : Sub-group 2, April 2006 http://www.international competitionnetwork.org/media/library/conference_4th_bonn_2005/Anti-Cartel_Enforcement_ Manual.pdf.
- Ibid.
- From the discussion paper on â€œauto-notaryâ„¢ Accurate Automation Corpn.: A Technique for Authentication of Digital Informationâ€• http://www.accurate-automation.com/Technology/Cvr/Auth/ authentication_description.pdf.
- T. Wright, â€œThe Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics (Part 2)â€• (26-5-2000) http://www.securityfocus. com/infocus/1245.
- G. Palmer, â€œForensic Analysis in the Digital Worldâ€• (2002) 1 IJDE Issue 1. http://www.ijde.org/gary_article.html last accessed 31-5-2002.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 125 L Ed 2d 493 : 509 US 579 : 113 S Ct 2786 (1993).
- E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (Academic Press, London, 2000).
- Cert, â€œTrojan horse version of TCP Wrappersâ€• (1999) CERT Advisory CA-1999-01 http://www.cert.org/advisories/CA-1999-01.html.
- E. Casey, Handbook of Computer Crime Investigation: Forensic Tools and Technology (Academic Press, London, 2001).

- No. 2004 CT 014406 SC (Sarasota County, 2005).
- 418 F 2d 669 (5th Cir 1969).
- Ibid, 670.
- 923 F 2d 910 (1st Cir 1991).
- Ibid, 915.
- 990 P 2d 563 (2000).
- Ibid, 581.
- 7 SW 3d 427 (1999).
- Ibid, 432.
- Williford v. State, 127 SW 3d 309 (Tex Ct App 2004); State v. Scurti, 153 Ohio App 3d 183 (7th Dist 2003); State v. Yerkes, 458 A 2d 1345, 1347 (NJ Law Div 1983); People v. Lugashi, 205 Cal App 3d 632 (1988); Lattarulo v. State, 401 SE 2d 516, 519 (Ga 1991); State v. Busch, 576 NW 2d 904 (Wis 1998).
- Daubert v. Merrell Dow Pharmaceuticals Inc., 43 F 3d 1311 (9th Cir 1995).
- Ibid.
- Ibid.
- 143 L Ed 2d 238 : 526 US 137 (1999).
- United States v. Kennedy, 81 F Supp 2d 1103 (D Kan 2000).
- Register.com Inc. v. Verio Inc., 356 F 3d 393, 407 n. 4 (2d Cir 2004).
Per Parker, C.J., defining an internet protocol address as â€œthe unique identification of the location of an end-userâ€™s computer which serves as a routing address for e-mail and other data sent to that computer over the internet from other end-usersâ€•.
- Michael L. Rustad, â€œPrivate Enforcement of Cybercrime on the Electronic Frontierâ€• (2001) 11 S Cal Interdisciplinary LJ 63, 98.
- For investigators of internet crimes there are no geographical borders and thus there is no â€œtraditional crime sceneâ€•.
- Daniel J. Solove, â€œDigital Dossiers and the Dissipation of Fourth Amendment Privacyâ€• (2002) 75 S Cal L Rev 1083, 1092-94.
- William J. Stuntz, â€œCommentary, O.J. Simpson, Bill Clinton, and the Trans-substantive Fourth Amendmentâ€• (2001) 114 Harv L Rev 842, 857-58.
- While searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.
- Securities and Exchange Commission v. Jerry T. Oâ€™Brien Inc., 81 L Ed 2d 615 : 467 US 735, 743 (1984).
- 29 L Ed 746 : 116 US 616 (1886).
- Ibid, US at 630.
- 50 L Ed 652 : 201 US 43 (1906).
- Ibid, US at 76.
- United States v. Bach, 310 F 3d 1063, 1067-68 (8th Cir 2002).
- Vincenzo Medillo, â€œA Guide to TCP/IP Internetworkingâ€• 1996 http:// www.ictp.trieste.it/~radionet/nuc1996/ref/tcpip/part1.htm.
- Soldal v. Cook County, 121 L Ed 2d 450 : 506 US 56, 69 (1992); Arizona v. Hicks, 94 L Ed 2d 347 : 480 US 321, 325 (1987).
- United States v. Procopio, 88 F 3d 21, 26-27 (1st Cir 1996).
- Orin S. Kerr, â€œInternet Surveillance Law after the USA Patriot Act: The Big Brother That Isnâ€™tâ€• (2003) 97 NW U L Rev 663.
- Kyllo v. United States, 150 L Ed 2d 94 : 533 US 27, 31 (2001).
- Maryland v. Garrison, 94 L Ed 2d 72 : 480 US 79, 84 (1987).
- Davis v. Gracey, 111 F 3d 1472, 1478-80 (10th Cir 1997).
- Challenging search warrant for computer as overbroad and seizure of computer as illegal, on grounds that real evidence was merely a file contained on that computer.
- United States v. Tamura, 694 F 2d 591 (9th Cir 1982).
- Kremen v. United States, 1 L Ed 2d 876 : 353 US 346 (1957).
- Carroll v. United States, 69 L Ed 543 : 267 US 132, 149 (1925); Katz v. United States, 19 L Ed 2d 576 : 389 US 347, 353 (1967).
- See, Electronic Communication Privacy Act, Pub L No. 99-508, 100 Stat 1848 (1986); 18 U.S.C. Â§ 2703(a) (2000).
- United States v. Scott, 504 F 2d 194, 198-99 (1974).
- See, IIT Research Institute, â€œIndependent Technical Review of the Carnivore System Draft Reportâ€• 2000 http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (on file with the Columbia Law Review); IIT Research Institute (emphasising need for post-collection auditing of uses of Carnivore).
- See, 18 U.S.C. Â§ 2510(8) (defining â€œcontentsâ€• for wire or electronic communication as that which â€œincludes any information concerning the substance, purport, or meaning of that communicationâ€•). This provision was enacted in 1968 and amended in 1986.
- See, 18 U.S.C. Â§Â§ 3127(3)-3127(4) (Supp 2002) (defining pen registers and trap and trace devices as devices that record, decode, or capture â€œdialing, routing, addressing and signalling informationâ€•).
- United States Telecom Assn. v. Federal Communications Commission, 227 F 3d 450, 462 (DC Cir 2000).
- Pharmatrak Inc., In re, 329 F 3d 9, 18-19 (1st Cir 2003).

- â€œSearching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigationsâ€• (2002) Computer Crime and Intellectual Property Section, U.S. Deptt. of Justice, 104-07 http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (on file with the Columbia Law Review).
- United States v. Hill, 322 F Supp 2d 1081, 1091-92 (CD Cal 2004).
- United States v. Carey, 172 F 3d 1268, 1275 n. 7 (10th Cir 1999).
- United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930 (Dutah 2001).
- People v. Gall, 30 P 3d 145, 156 (Colo 2001) (Martinez, J., dissenting).
- James M. Rosenbaum, â€œIn Defense of the Hard Driveâ€• (2001) 4 Green Bag 2d 169, 171.