Chapter 19

ASSESSING THE LEGAL RISKS IN NETWORK FORENSIC PROBING

Michael Losavio, Olfa Nasraoui, Vincent Thacker, Jeff Marean, Nick Miles, Roman Yampolskiy and Ibrahim Imam

Abstract This paper presents a framework for identifying the legal risks associated with performing network forensics on public networks. The framework is discussed in the context of the Gnutella P2P network protocol for which the legal issues related to authorized access have not yet been addressed.

Keywords: Network forensics, legal issues, authorized access, Gnutella protocol

1. Introduction

The analysis of legal issues related to investigations of network misuse can help avoid misunderstandings about the application of law to computer and network conduct. An understanding of the issues is important for researchers who wish to avoid legal entanglements in the course of conducting their research and for investigators who are working on cases without the luxury of legal counsel.

An understanding of the application of law in this domain can also influence the course of litigation. For example, Craig Neidorf was prosecuted for the interstate transportation of stolen property (18 U.S.C. §2314) for the electronic BBS transmission and posting of a BellSouth 911 manual sent to him by a friend [6]. However, the prosecution was derailed when the government could not establish that the electronic version of the publicly available document was property of any type. One commentator attributed this to the conflict between traditional property law concepts and online activity. Similarly, Robert Morris Jr., the developer of the Internet worm, argued that he did not intend to cause damage with the release of his worm and was, therefore, not guilty un-

Table 1. Digital contraband and illegal conduct.

Contraband	Illegal Conduct
Child pornography	Possession; Receipt (18 U.S.C. §2251)
Obscene materials	Possession; Distribution (18 U.S.C. §1460)
Creative content distributed in violation of copyright laws	Copying; Distribution (18 U.S.C. §2319)
Trade secret information	Distribution (18 U.S.C. §1831)
Technology for circumventing copyright protection	Distribution (Digital Millennium Copyright Act)
Access devices (including passwords)	Possession; Distribution (18 U.S.C. §1029)

der the Computer Fraud and Abuse Act. In the Morris case, the court found that malicious intent to do damage was not an element of the crime, only the intent to access without authorization [22].

The core issue is one of "authorized access," which addresses the concerns found with the application of the concepts of trespass and invasion of privacy to computers. Criminal and civil prohibitions on trespass protect against physical intrusion or interference with property. However, prosecutions for trespass via electronic interactions with a computer lack an actual physical invasion of property. The idea of access as an element was developed for computers, and authorized access delineates permitted and non-permitted access to data and system resources.

Digital forensic analysis of the distribution of contraband material occurs in a variety of environments. These range from the examination of a local machine on a network to the active harvesting of data by a system that crawls a network, which includes node-based probing and traffic monitoring [9, 13, 16]. This paper examines the legal implications of active harvesting in which a local peer machine probes or monitors a P2P network.

2. Basic Legal Framework

Contraband refers to artifacts or objects associated with illegal activity, which includes their possession, distribution or use as prohibited by law. State and private investigators and researchers are not immune from criminal or civil liability for examining contraband items, regardless of motive. The conduct that is illegal varies with the contraband items as described in Table 1.

Each offense may require a different level of criminal intent for guilt. However, the conduct described may be sufficient for arrest and issuance

of a search warrant to search/seize any machine that may have evidence of such conduct.

Because of the range of offenses, five basic types of conduct form a framework for legal analyses relating to computer misuse. The European Convention on Cybercrime describes them as offenses against the confidentiality, integrity and availability of computer data and systems [5, 15]. The five basic types of conduct are:

- Unauthorized access to a computer, including exceeding authorized access
- Unauthorized interception of data
- Unauthorized interference with data
- Unauthorized interference with a system
- Misuse of devices

Before using a network forensic tool on a network, the impact of the tool should be evaluated in terms of these five types of conduct. A checklist consisting of the conduct and the relevant offense may be made in which the offense is identified as present, not present or unknown. For each conduct and offense, the authority or claim of right must then be identified. We demonstrate the application of this checklist on P2P research in the context of United States law, specifically 18 U.S.C. §1030 and the Computer Fraud and Abuse Act (CFAA) [11, 25].

3. Authorized Access

One may not legally access a computer or its resources without permission. This statement belies the complexity regarding what constitutes access and what constitutes authorized access. For example, an individual may have permission to access some computer resources but may not have permission to access all the resources.

It is useful to employ an analogy to physical trespass when analyzing access issues, especially when considering the need to possess certain items residing in some physical location. In an electronic environment, the possession of digital objects can take place without any physical invasion, but simply by transmitting certain commands across the network [11].

The CFAA is the primary criminal statute that addresses the unauthorized access to computers that fall under federal jurisdiction. It prohibits conduct ranging from simple (unauthorized) access to the impairment of data integrity via the transmission of hostile code.

The key elements of access and authorized access are not defined by the CFAA. Instead, they are left to jurisprudential interpretation. A U.S. federal court defined access as "to gain access to [or] to exercise the freedom or ability to make use of something" in the America Online (AOL) v. National Health Care Discount case [24]. In this case, the defendant's emailers harvested the addresses of AOL members and sent unsolicited bulk email to the members [24]. AOL's terms of service prohibited this particular conduct and, as such, it was deemed unauthorized access for which AOL was entitled to civil relief.

Another court dismissed an unauthorized access charge when the evidence only showed that the defendant dialed up a computer using a modem and viewed the login screen, but did not otherwise modify, copy or possess anything from the computer. The appellate court noted that until the defendant went beyond the initial banner and entered the appropriate password, there was no ability to use and, thus, no access as commonly understood [20].

Related to the access issue is the possession of digital objects and the use of system resources. In the case of United States v. Simpson [23], the federal court defined possession as "the holding or having something (material or immaterial) as one's own, or in one's control." In this particular case, gaining root access to a remote machine gave dominion and control and, thus, possession to all the files and resources on the machine.

Kerr [8] notes that the technical/physical perspective is present in other cases, as where evidence of repeated dialing activity coupled with an admission that the conduct sought to find long-distance access codes were found to be sufficient for access/computer trespass. Kerr also suggests that access should be defined by an analogy to physical trespass as the making of a "virtual entrance" into a computer or from the technical/physical operation of a computing machine over a network. Under this definition, a failed attempt to log into a machine would not be an access, but inputting and sending data to it would constitute access.

Similarly, Madison [12] suggests that the analysis varies between "Internet as a place" (i.e., a trespass model) and "information as a thing" (i.e., a theft model). This leaves little guidance as to what conduct constitutes access. Instead, the definition becomes subject to a requirement of authorization or right.

"Authorized (with right)" is the express granting of permission or right authorizing access. User agreements for online services may expressly grant access, although special terms of use may apply. States, by statute, may authorize certain types of access to certain groups of individuals. A court order issuing a search warrant gives the serving

officer permission to search and access a computer or system regardless of the owner's wishes. Similarly, a consent to access authorizes access just as any consent to search a physical premises obviates the need for a search warrant. The many exceptions to the requirement of a search warrant in the United States may offer other examples of *de jure* authorization (e.g., search incident to arrest), but these exceptions apply only to state law enforcement officers acting within their police powers.

The difficult issue is online activity where there is no express permission or right. There may or may not be an implicit authorization to access online systems configured for open access, which accounts for most of the content on the World Wide Web. The definition of what constitutes "implicit authorization" is a distinct issue that must be separated from conduct.

Implicit authorization is a complex issue. Hale [7] posits that the use of an open wireless local area network without express authorization is a violation of the CFAA – there is no implicit authority to use it simply due to its lack of access controls. Bierlein [2] notes that accessing an open wireless local area network is potentially a misdemeanor under the CFAA, but opines that the criminalization of such an act is unlikely. Nevertheless, such cases have been prosecuted in several jurisdictions, including the United States, Canada and Singapore [1, 10, 17].

The U.S. Court of Appeals for the First Circuit noted there could be an implicit limit on authorized access and expressly declined to adopt the view that there is a presumption of open access to Internet information [21]. The court noted that a "public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like reasonable expectations." Express "terms of service" have been used to delineate authorized access such that any violation of the terms becomes unauthorized access to the system [24]. However, Stanley [19] argues that access to a public web page without any violation of the terms of service should not be a CFAA violation in his analysis of the SCO Group's accusations against IBM employees who visited its website.

These examples do not clarify the legality surrounding the authority to access a computer or network where there is not an explicit permission or right. It leaves open a risk of a charge for lack of authority to which an implicit authority claim must be made as a defense. One perspective is that the Internet is based on the open exchange of information and technologies, and this inherently provides implicit authority. Alternatively, access to open systems such as wireless networks without authority has led to criminal prosecution. Perhaps, the extent of access may work

along a sliding scale of access rights judged against the interference or loss to the accessed machine, data or subject of the data.

4. Gnutella Case Study

Nasraoui, *et al.* [13] have presented a technical approach for monitoring contraband exchanges on Gnutella P2P networks. The approach [4] involves crawling through a P2P network to collect network topology data, P2P connections between nodes that identify their accessible neighbors and actual network identifiers (e.g., IP addresses of nodes). The Gnutella protocol has five messaging descriptors:

- **Ping:** A Ping is used by a machine to find other host machines that are active in a P2P network.
- **Pong:** A Pong is a response to a Ping that notes that the node is active and returns its IP address and what data it is sharing.
- **Query:** A Query is issued by a node to find out if a particular data resource is available for sharing by an active P2P node.
- **QueryHit:** A QueryHit is the positive response by a node to a Query noting that it has the data resource available for sharing.
- **Push:** A Push permits a responding machine to share its data through a firewall.

Common usage of the Gnutella protocol is to invoke an application that pings other nodes, queries for available files, and then downloads the files using the HTTP Get command.

5. Analysis of Authorized Access

Authorized access or access with right are assumed once a machine is placed in a network and a P2P application is started without blocking the service in some way. Each Gnutella messaging descriptor makes demands on a target machine for services, responses and data. Such demands may be acceptable under an implicit authority theory for the service. Gnutella has been described as "an open, decentralized group membership and search protocol" [14], which implies permissions to participate as part of the group through open access. The Gnutella specification offers support for this feature because it describes an open exchange system that may implicitly authorize access by the very use of the protocol [4].

Table 2. Checklist for basic legal issues in network access.

Service	**Category**	**Machine Access**	**Authority or Claim of Right**
Ping	Unauthorized access to a computer	No	
Query	Unauthorized access to a computer	No (Probably)	
Get	Unauthorized access to a computer	Yes	Not clear

But this assumption may be unwarranted, as indicated in the Zefer Corp. case [21], just as leaving a door unlocked does not authorize trespass into a home. Also, in the Neidorf case [6], the defendant plead guilty to unauthorized access although the access was via an open telephone dial-up modem.

Assuming a sliding scale approach is tied to system demands, the authority/right issue may be avoided for minimal message descriptors like Ping. At the other end of the spectrum, implicit authority may be required when services and data are made available (as with Get). However, this may depend on some evidence of a knowing act by the possessor of the target machine to open its services.

Ping, Query and Get constitute the bulk of the request and response services used by Gnutella P2P applications. Table 2 presents an analysis of these message descriptors in terms of authorized access.

The Ping messaging descriptor evokes a Pong response from a participating node. A Ping does not access the pinged computer as defined by statute. Rather, it makes use of a remote machine in that it provokes a response that consumes system resources (no matter how small). Note that it does not give a machine or user control over the remote machine nor does it make any machine services available for use, which is one definition of access.

When compared with the traditional notion of trespass, Ping is equivalent to knocking on a door rather than actually entering the premises, which is not considered trespass. While such analogies in computer law and technology have occasionally led litigation astray (as in the Neidorf case [6]), they can help analyze how the issue might be resolved by the courts.

The Query messaging descriptor requests information on the resources available from a particular node. A Query requires the remote machine to examine certain resources, format a response and return the requested information. A Query uses more node resources than a Ping. But it may

not represent control sufficient to use the broader services of the remote machine. Using the trespass analogy, a Query is analogous to knocking on a door and asking who is behind the door without any physical entry. When viewed in terms of dominion and control of a remote system, a Query exercises minimal demands or control of system resources; it merely acquires data from the system.

The Get messaging descriptor requests a particular resource from a node and initiates an action by the remote system to return the requested resource to the originating system. Get gives the requesting machine greater control over the remote machine, permitting it to have dominion and possession of digital objects on the remote machine and (based on the configuration) to direct their copying and distribution back to the requesting machine. Thus, is the use of Get an authorized access? Probably, but a clear answer may not be possible under current jurisprudence. One possible defense is mistake of fact (e.g., I didn't know), but it would depend on the wording of the particular criminal statute (e.g., as in the Morris Internet worm prosecution [22]). In effect, this leaves the authorization for P2P crawling – and a wide array of online activities – open to interpretation.

6. Authorized Access for P2P Research Tools

A P2P research tool can be used to harvest data about query traffic on a network [16]. The data is harvested by placing a machine/node on the network that sends a file (bit vector) to an ultrapeer. This file serves as a routing table with data asserting that the node can respond to all queries sent to the ultrapeer. The bits in the routing table are set to claim that all query keywords match files available at the node. When the ultrapeer passes queries to the node, the node stores the query data but does not respond to them.

The use of such a research tool may fall outside the expected use of and interaction with a node on a P2P network. Further, the routing table file is deceptive because it cannot respond to all queries as asserted. The tool makes a representation for the purposes of data collection, but does no file sharing.

With regard to the authorization for the tool, the context of implicit authorization would involve transactions across the network designed to facilitate its use for file and resource transfer. Because the tool acts only to consume alternative resources for purposes unrelated to the actual use of the network, it raises a question as to whether there is implicit authorization for its operation.

Note that federal statutes limit jurisdiction to situations as set out in 18 U.S.C. §1030(a)(5)(A)(B)(i) [25] causing "loss to one or more persons during any one year period ... aggregating at least $5,000 in value." Because it may be difficult or impossible to establish that this conduct constitutes a loss in the jurisdictional amount, there would seem to be no federal liability for this kind of research effort. However, for jurisdictions that do not have a financial limitation amount, there may be exposure to liability for the application of similar statutes.

7. Future Trends

The evolution of jurisprudence in this area is of importance to researchers and investigators, who should continuously monitor new statues and case decisions. Kerr [8] suggests developing new statutes related to authorized access that specifically address each type of computer misuse. A clear definition of access is required when a user sends a command to a machine that, in turn, executes the command. This rejects the virtual space/trespass analogy of a virtual entry into a machine. However, Kerr proposes that this broad meaning of access would change the definition of access without authorization to access that circumvents restrictions by code. This negates contract law, keeps out analogs and, as with the Digital Millennium Copyright Act, offers regulation to control access and ensure security.

The evolution of jurisprudence will also be affected as more case law develops regarding other types of contraband (i.e., not restricted to child pornography). The jurisprudence related to copyright prosecutions of operators of P2P nodes may come to treat such activity differently. Similarly, laws governing privacy rights may impact this analysis by focusing further on an invasion of rights rather than a physical machine. Simon [18], who describes a possible continuum of online privacy expectations, posits that gaining evidence from a public chat room would not violate the Fourth Amendment, but the use of services that increasingly protect privacy and control may render an online search in violation of the Fourth Amendment or the Electronic Communications Privacy Act.

It may also be necessary to consider whether legislative changes are needed to provide opportunities for open research. There is a legislative "safe harbor" for lawfully-authorized investigative activity by a law enforcement agency under the U.S. computer access statute, but this does not apply to private investigators and researchers. Indeed, closing off open research and limiting research to law enforcement entities may be handing an advantage to those using P2P networks for illegal purposes,

just as earlier federal limitations on encryption research damaged such efforts within the United States.

8. Conclusions

Several pitfalls exist concerning the analysis of system use in networks, both for investigators and researchers. Continued analysis of the legal and ethical implications of the techniques is important to performing investigations as well as developing and testing forensic tools.

Caloyannides [3] observes that, where digital evidence is concerned, "the potential for a miscarriage of justice is vast." It is essential that any network research that seeks to address misconduct in the use of networks – whether of contraband transactions or other illegal activity – take into account possible legal restrictions. Good intentions are not enough. Failure to satisfy the legal constraints can compromise the evidentiary value of investigations as well as expose investigators and researchers to legal liability and damage to reputation.

References

[1] Associated Press, Singapore teen faces 3 years' jail for tapping into another's wireless Internet, *International Herald Tribune*, November 10, 2006.

[2] M. Bierlein, Policing the wireless world: Access liability in the open Wi-Fi era, *Ohio State Law Journal*, vol. 67(5), pp. 1123–1186, 2006.

[3] M. Caloyannides, *Privacy Protection and Computer Forensics*, Artech House, Norwood, Massachusetts, 2004.

[4] Clip2 Distributed Search Services, The Gnutella Protocol Specification v0.4 (Document Revision 1.2) (www9.limewire.com/developer/gnutella_protocol_0.4.pdf), 2001.

[5] Council of Europe, Convention on Cybercrime, Strasbourg, France (conventions.coe.int/Treaty/en/Treaties/Html/185.htm), 2001.

[6] M. Godwin, Some "property" problems in a computer crime prosecution, Electronic Frontier Foundation, San Francisco, California (www.textfiles.com/law/cardozo.txt), 1992.

[7] R. Hale, Wi-Fi liability: Potential legal risks in accessing and operating wireless Internet, *Santa Clara Computer and High Technology Law Journal*, vol. 21, pp. 543–559, 2005.

[8] O. Kerr, Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes, *NYU Law Review*, vol. 78(5), pp. 1596–1668, 2003.

[9] S. Kwok, P2P searching trends: 2002-2004, *Information Processing and Management*, vol. 42(1), pp. 237–247, 2006.

[10] A. Leary, Wi-Fi cloaks a new breed of intruder, *St. Petersburg Times*, July 4, 2005.

[11] M. Losavio, The law of possession of digital objects: Dominion and control issues for digital forensic investigations and prosecutions, *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 177–183, 2005.

[12] M. Madison, Rights of access and the shape of the Internet, *Boston College Law Review*, pp. 433–507, 2003.

[13] O. Nasraoui, D. Keeling, A. Elmaghraby, G. Higgins and M. Losavio, Node-based probing and monitoring to investigate the use of peer-to-peer technologies for the distribution of contraband material, *Proceedings of the Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 135–140, 2008.

[14] M. Ripeanu, A. Iamnitchi and I. Foster, Mapping the Gnutella network, *IEEE Internet Computing*, vol. 6(1), pp. 50–57, 2002.

[15] S. Schjolberg, The legal framework – Unauthorized access to computer systems, Penal legislation in 44 countries, Moss District Court, Moss, Norway (www.mosstingrett.no/info/legal.html), 2003.

[16] S. Sharma, L. Nguyen and D. Jia, IR-Wire: A research tool for P2P information retrieval, *Proceedings of the Second Workshop on Open Source Information Retrieval*, pp. 33–38, 2006.

[17] R. Shim, Wi-Fi arrest highlights security dangers, *ZDNet News*, November 28, 2003.

[18] B. Simon, Note: The tangled web we weave – The Internet and standing under the Fourth Amendment, *Nova Law Review*, vol. 21, pp. 941–959, 1997.

[19] J. Stanley, Whose hands are "unclean?" – SCO, IBM's "agents" and the CFAA, *Groklaw* (www.groklaw.net/articlebasic.php?story=20041217091956894), December 17, 2004.

[20] Supreme Court of Kansas, State of Kansas v. Allen, *Pacific Reporter (Second Series)*, vol. 917, pp. 848–854, 1996.

[21] U.S. Court of Appeals (First Circuit), EF Cultural Travel BV v. Zefer Corp., *Federal Reporter (Third Series)*, vol. 318, pp. 58–64, 2003.

[22] U.S. Court of Appeals (Second Circuit), United States v. Morris, *Federal Reporter (Second Series)*, vol. 928, pp. 504–512, 1991.

[23] U.S. Court of Appeals (Tenth Circuit), United States v. Simpson, *Federal Reporter (Third Series)*, vol. 94, pp. 1373–1382, 1996.

[24] U.S. District Court (Northern District of Iowa, Western Division), America Online, Inc. v. National Health Care Discount, Inc., *Federal Supplementer (Second Series)*, vol. 121, pp. 1255–1280, 2001.

[25] U.S. Government, Title 18, Crimes and Criminal Procedure, *United States Code Annotated*, Washington, DC, pp. 445–453, 2000.