

THESIS

2
2000



3 1293 02048 6605

This is to certify that the
dissertation entitled

**THE CRIMINOLOGY OF COMPUTER HACKERS:
A QUALITATIVE AND QUANTITATIVE ANALYSIS**

presented by

D. KALL LOPER

has been accepted towards fulfillment
of the requirements for

Doctoral degree in Social Science

A handwritten signature in cursive script, reading "Judith M. Collins". The signature is written in black ink and is positioned above a horizontal line.

Major professor

Date August 16, 2000

PLACE IN RETURN BOX to remove this checkout from your record.
TO AVOID FINES return on or before date due.
MAY BE RECALLED with earlier due date if requested.

DATE DUE	DATE DUE	DATE DUE
NOV 02 2003 05 14 04		

**THE CRIMINOLOGY OF COMPUTER HACKERS: A QUALITATIVE AND
QUANTITATIVE ANALYSIS**

By

D. Kall Loper

A Dissertation

**Submitted to
Michigan State University
In partial fulfillment of the requirements
for the degree of**

DOCTOR OF PHILOSOPHY

College of Social Science

2000

ABSTRACT

THE CRIMINOLOGY OF COMPUTER HACKERS: A QUALITATIVE AND QUANTITATIVE ANALYSIS

By

D. Kall Loper

This multi-part dissertation uses qualitative and quantitative methods to examine computer hackers. The research addresses three problems. First, there is no broadly agreed upon definition of hacker. The distinction between computer criminals and hackers is the subject of conflicting literature. Second, direct observation of hacker activities is not reported in the literature. Direct observation does not rely upon the subject's interpretations of events. Third, there is no quantitative study of hackers. Previous quantitative research has used proxy populations rather than hackers. Previous quantitative research has not attempted to generate predictor models of hacker activity.

Part I develops a typology of hackers based on subculture theory. The typology is the product of a triangulation of three sources (1) media definitions from news sources; (2) the self-definitions of hackers from their Internet communications; and from (3) the foundational materials (e.g., books, movies, web sites, etc.) found in the hacker subculture. The types defined in this typology will differentiate types within the hacker subculture and explain why hackers are so difficult to describe. The typology provides empirically derived definitions of computer hacker for the present and future research.

Part II is a field study of computer hacker activities. Since the vast majority of hacker interactions occur online, the unit of analysis is the interpersonal communication of hackers: E-mail messages. Part II uses ethnographic methods to categorize hacker on-line activities. Grounded theory guides this inductive examination of hacker activities. The products of this study are activity profiles of hacker, on-line activities organized with categories suggested by the grounded theory analysis.

Part III tests hypothetical, mathematical models created from the activity profiles developed in Part II. These activity profiles (the independent variables) predict the dependent variable: hacker competency. A mathematical model based on observable activities can be used to forecast competencies of computer hackers, and provides concrete guidance in the application of the typology in Part I to computer criminals and hackers.

Copyright by Donald Kall Loper Jr.

2000

ACKNOWLEDGMENTS

I gratefully acknowledge the invaluable assistance of Dr. Judith Collins in the preparation of this dissertation. Dr. Collins first suggested a quantitative application of the data set used herein. Her technical assistance with issues of measurement, analysis, and scientific writing made this work possible.

I am also grateful to the members of the dissertation committee: Dr. David Carter, Dr. Betsy Cullum-Swan, Dr. Steven Gold, Dr. Cynthia Perez-McCluskey, and Dr. Judith Collins (Chair). Each member has gone beyond the requirements of their office to accommodate the timely completion of this dissertation. The thoughtful comments and assistance provided by the committee have improved the quality of this dissertation.

Finally, I am grateful to Paul Saxman, writer of MailParser--the program used to enter data in Part III of this dissertation. Mr. Saxman has also provided expert assistance in validating the measure of hacker competency used in Part III. Mr. Saxman has released his program to all that might benefit from its use (under the standard GNU license).

PREFACE

Conventions used in this Dissertation

Due to the frequent use of quoted materials, this dissertation uses several conventions to distinguish quotes. All long quoted material is formatted in a proportional font and off-set ½" from the left and right margins. Thus, long quotes look like this:

Hafner, who was primarily responsible for the characterization of Mitnick as a darkside hacker, admitted to Charles Platt in his review of "Takedown" that it "might have been a mistake to call him a darkside hacker." Hafner, in fact, has come to regret the characterization and its fallout. "There are malicious characters out there," she told Platt, "but Kevin is not one of them."
(Thomas, 1998a).

Ethnographic material presented in the form of long quotes is similarly formatted, but includes the ">" character on the left side. When a subject quotes another subject, an additional character is used (i.e. ">>"). Ethnographic material is not listed in the bibliography. Quotes are identified by the Date, From, and Subject lines of the message they come from. Material quoted by a subject is only attributed to a source if the subject did so. Quoted ethnographic material looks like this:

>On Tue, 10 Nov 1998, Hyprstatik wrote:
>
>> If you read cyberpunk by John Markoff remeber he is the
>>same guy that helped to write Takedown and has bad
>>mouthed hackers. Also remember that Kate ----- the
>>other author is trying to be accurate but I am not so
>>sure if she is.
>
>There are lots of issues here. Katie Hafner is Markoff's
>ex, but she was (and still is) absolutely committed to
>being fair and accurate in that book. She wrote the book
>without Kevin's input, which was Kevin's choice. The
>things that are problematic in that book (at least to me)
>are the ways in which Kevin is characterized as a
>"darkside hacker" and the things that bother Kevin are
>mostly the details that he claims are wrong, which portray

>him in a negative light (such as stealing his mom's tip
>money to rent motel rooms to hack from). Most of those
>details came from Lenny.
>
>Date: Tue, 10 Nov 1998 14:01:12 -0800 (PST)
>From: Douglas Thomas <snip!>
>Subject: Re: [mitnick] Books...

Due to the quantity of technical terms associated with the study of hackers, a glossary has been provided to define these terms and offer context for understanding their use. Terms appearing in the glossary are noted in **bold text**. In the interest of conceptual clarity, technical detail has been simplified wherever possible; however, it is often necessary to understand how the technology works to understand how hackers conceive it.

Finally, nothing in this dissertation should be read to imply that hackers are all *de facto* criminals. The use of criminological theory to describe the hacker subculture is a product of my disciplinary knowledge base, not an attempt to prove that hackers are criminals. The subtlety of the distinction drawn between hackers and computer criminals does not diminish the fact it represents: hackers have goals that differ from those of the dominant culture, but malicious destruction is not part of the hacker subculture. Like any culture, some members deviate from accepted norms, but hacker who do so act as individuals, not representatives of their subculture's ideal.

TABLE OF CONTENTS

LIST OF TABLES.....	xi
LIST OF FIGURES	xiixii
Introduction.....	1
Statement of the Problems	2
Part I: Typology of Hackers.....	2
Part II: Profile of Activities.....	2
Part III: Prediction of Hacker Competency	3
Research Rationale.....	3
Part I: Defining Computer Criminals and Hackers with a Typology	5
Literature Review.....	5
Hackers	5
Hackers versus Computer Criminals	6
Computer Criminals.....	7
Summary	8
Theory	9
Method	10
Symbolic Interactionism	11
Triangulating Sources: Media, Internet Discussions, Materials	12
Results.....	18
Computer Criminals and Hackers.....	18
Typology of Hackers.....	19
Discussion	22
Distinguishing Criminals from Hackers	22

The Hacker Subculture: The Social Context of Hacking.....	23
Prosocial Hacking	25
The Hacker Ethic	27
Context for the Hacker Typology	29
Conclusion	36
Part II: Profile of Activities.....	38
Literature Review.....	38
Theory	38
Method	39
Participants.....	40
Data Collection	41
Data Analysis	41
Procedure	41
Results.....	44
Discussion	46
Communication.....	46
Identity	55
Hacker Subculture.....	62
Hacktivism	71
Conclusion	78
Summary	80
Part III: Predicting Hacker Competency	81
Purpose.....	81
Literature Review.....	81
Theoretical Overview of the Four Constructs.....	82

Method	83
Subjects	84
Variables	85
Procedure	87
Results.....	89
Descriptive Statistics.....	89
Regression Analysis.....	90
Overall Discussion of the Triangulation: Parts I, II, and III	91
Substantive Findings.....	93
Limitations of the Study	94
Indications for Future Research	95
Policy Implications	96
Increasing Law Enforcement Computer Competency	96
Law Enforcement Lobbying for Expanded Powers	97
Conclusion	101
GLOSSARY	103
APPENDIX A.....	123
APPENDIX B	126
APPENDIX C	128
APPENDIX D.....	133
APPENDIX E	153
BIBLIOGRAPHY	156

LIST OF TABLES

Table 1: Hacker Typology Concepts

Table 2: Constructs and Components of Constructs

Table 3: E-mail Client and Level of Sophistication

Table 4: Descriptive Statistics and Correlations for Hacker Competency Prediction Model

Table 5: List of All Known E-mail Clients Used on the Mitnick List During This Research, With Coding Values

LIST OF FIGURES

Figure 1: The relationship between hacking, criminal hacking, and computer crime. The Venn diagram shows the overlap these concepts.

Figure 2. An example of ASCII art

Figure 3: The ISO seven layer reference model

Introduction

The three-fold purpose of this dissertation is to (1) create a typology of computer hackers and compare it to existing definitions of computer criminals; (2) create a profile of hacker activities; and (3) develop and statistically test a prediction model of hacker competency. The research is guided by subcultural theory, which provides descriptions of deviance from the normative culture, and the theory of intrinsic motivation (Katz, 1988). The dissertation applies these theories to the subculture of computer hackers. The overriding goal is to advance theory and future research on computer crime and to identify theoretically meaningful differences between hackers and computer criminals.

There is a popular conception that the word 'hacker' and the term 'computer criminal' are synonymous. However, "hacker" and "computer criminal" have not been formally defined in the theoretical or empirical literature so there is no scientific rationale for the current conceptions. Originally, the word "hacker" referred to an unorthodox problem solver and virtuoso programmer; in fact, hackers made the machines and the programs that are vital to modern society (Levy, 1984; Duff & Gardiner, 1996; Hafner & Lyon, 1996). Recognizing this fact, some media sources coined terms like "computer cracker" and "black hat" to describe criminal hackers. Consequently, references to hackers and computer crime are problematic because there is no *formal* consensus as to the meaning of the word "hacker" or the term "computer crime." However, there is a *vague* consensus that hackers are bad people who do bad things (Chandler, 1996). The dissertation aims to clarify the "hacker" and "computer criminal" conceptually and empirically.

Statement of the Problems

The general concepts of computer crime and hacking present great concerns for economies built on information. Parker (1999) notes that the growth of computer and Internet connection has been “explosive” since 1995. Carter and Katz (2000) indicate that superlatives are often appropriate when describing the growth of information technology. Carter and Katz also note that there is too little empirical research being applied to computer crime (2000). This dissertation cannot address the spectrum of needed research described by Carter and Katz; however, it can begin the process and present methodology and conceptual tools to facilitate such research.

Part I: Typology of Hackers

The literature reports no universally accepted definition of hacker. Part I will develop a typology of hackers using subcultural theory as the guiding framework. The typology will be developed from a systematic investigation of three sources of communication: (1) media definitions; (2) hacker self-definitions; and (3) books, movies, web sites, and other materials used by the hacker subculture. The results from Part I will reveal potentially different “types” of hackers. Part I is definitional and qualitative; therefore no formal hypotheses have been proposed.

Part II: Profile of Activities

There is currently no accepted consensus of what hackers do. Part II investigates the activities of computer hackers. Since the majority of hacker interactions occur online, the unit of analysis is the interpersonal communication of hackers. Such interactions are conducted in publicly available E-mail messages. A pilot study conducted in preparation for this dissertation (Loper, 1998) identified three overarching constructs in online messages: (1) communication (content and method); (2) self-definitions, and (3) culture.

Part II develops these constructs and seeks to identify their underlying activities. In addition, Part II seeks to identify other constructs using the E-mail data. Part II is ethnographic and posits no formal hypothesis.

Part III: Prediction of Hacker Competency

There is currently no measure of hacker skill. A prediction model of hacker skill, or competency, can be used to statistically estimate the effects of the subculture.

Therefore, Part III develops a mathematical model to predict hacker competency. Formal hypotheses are proposed in Part III.

Research Rationale

In addition to the lack of theory and empirical research on computer hacking and crimes, the research is justified by the disparities in computer competency that exist between some criminal justice experts and computer hackers. Couturie (1995) concluded that the gap in expertise between law enforcement and computer hackers would continue to widen as the complexity of computer crime increases (also see Gollman, 1999; Icove, Seger, & VonStorch, 1995; Russell & Gangemi, 1991).

In addition, computer crime has been targeted by the U. S. government as an increasing problem. Recently, the Federal Bureau of Investigation (FBI) prioritized computer crime by creating the National Infrastructure Protection Center (NIPC). The Center's inauguration address began with the following statement:

[T]he NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based (Vatis, 1998).

However, the federal government lacks the conceptual and empirical tools to predict hacker behavior (Couturie, 1995; Sterling, 1992). A prediction model of hacker competency can be useful to understand hackers including perhaps hackers who may also be criminals.

The research is further justified by the substantial interest shown by the general public in the topic of computer crime. An online literature review in preparation for this dissertation revealed over 400 news articles reported between September, 1998 and January, 2000 on computer crime, computer hacking, and court trials of hackers. These articles represent only a portion of articles on this subject, pointing to the great interest by the public in computer hacking and crimes.

To summarize, there is little or no theoretical guidance for research on computer hacking and crime. Few reported empirical studies examine these issues of National importance and public interest. Results from this dissertation may therefore be theoretically and pragmatically useful.

Paradigms of Inquiry

The dissertation integrates quantitative and qualitative research methods, an often-cited goal (e.g., Brink, 1995; Erzberger & Prein, 1997) that is often preferred over mechanical integration (e.g., using qualitative data as a surrogate for quantitative data) or incomplete integration (using qualitative and quantitative analyses to independently answer same question; King, Keohane, & Verba, 1994). The dissertation integrates qualitative and quantitative methods as follows: Part I uses qualitative methods to define hackers and computer criminals, Part II uses a field study of hacker communication to develop a profile of hacker activities, and Part III uses the information generated in Part

II to develop the hacker competency prediction model. The advancement of scientific knowledge is the rationale for uniting these qualitative and quantitative methods (King, Keohane, & Verba, 1994).

Part I: Defining Computer Criminals and Hackers with a Typology

The purpose of Part I is to address the competing definitions of hacker and computer criminal. The preferred definition of computer crime must address hacker's distinction between lawful hacking and crime. At the same time, the preferred definition hacking must acknowledge legal definitions of crime. This mission requires the reconciliation of directly opposing definitions. Simplistic definitions of computer crime and hacking cannot achieve the purpose set for Part I.

Literature Review

Hackers

Jordan and Taylor described the world of the hacker subculture using the concept of the imagined community (Anderson, 1991). Imagined communities are "dispersed networks of individuals...that combine through a collectively articulated identity"(Jordan & Taylor, 1998, p.763). The hacker subculture is "a community that offers certain forms of identity through which membership and social norms are negotiated" (Jordan & Taylor, p.763). The dissertation will be guided by the Jordan and Taylor (1998) conceptualization of subculture.

Other approaches have been used to conceptualized hackers. For example, Chandler (1996) conducted a review of news media reports on the hacker subculture to identify the metaphors applied to hackers. Popular images of hackers included 'cowboys on the electronic frontier,' 'intellectual joyriders,' 'potential murderers,' 'mad hackers,' and 'spies.' The dissertation does not use these definitions because they represent the popular

understanding and not the understanding that hackers have of themselves. Using sources described below, the typology will be generated using information gathered from and used by the hackers themselves.

Others conceptualize hackers as white-collar criminals. The popular press and some literature (e.g., Grabosky & Smith, 1998; Barrett, 1997) associate hackers, computer crime, and white-collar crime, but others distinguish hackers and white-collar criminals (Duff & Gardiner, 1996). Those authors argued that there are differences between the enterprises of hackers and white-collar criminals who are also computer criminals. The hacker offenses tended to be trivial and they were incidental to the pursuit of other goals (Duff & Gardiner, 1996). Specifically,

[U]nauthorized access to computer systems should not be a crime because there is no economic motive... the driving force is intellectual challenge.... So arguably, most forms of computer hacking cannot be seen as white-collar crime (Duff & Gardiner, 1996, p.214).

Thus, previous research theoretically supports the current trend that associates hacking with street crime (e.g. vandalism and 'robbery' of credit card information) rather than white-collar crime (Duff and Gardiner, 1996).

Hackers versus Computer Criminals

There is little scientific literature that distinguishes hackers and computer criminals (see Mann & Sutton, 1998). However, in the underground hacker media, the distinction was a subject of primary importance (Goldstein, 1999a; Goldstein, 1993). Goldstein (1996; 1999b) has addressed the distinction between hackers and computer criminals in three ways. First, he minimized the criminal damage caused by hacking, implying that very little actual harm is caused. Second, he defended the criminal actions of hackers based on their motives and adherence to hacker subcultural values, which were

not viewed as criminal by Goldstein. Third, he disavowed hackers who commit crimes that violate hacker values, such as crimes of financial gain. Thus, it appears that at least some elements of the hacker subculture do not condone computer crime.

Mann and Sutton (1998) distinguished hackers from criminals using computers to further their criminal enterprise, but those authors did not directly compare hackers and criminals. Mann and Sutton compared television satellite pirates and locksmiths who used computers to distribute methods for defeating security, and distinguished these groups from hackers. Mann & Sutton reported that the satellite pirates were more sophisticated than the group of locksmiths but that both groups communicated through Usenet **newsgroups** (public E-mail lists). The locksmiths distributed information on how to defeat locks using simple tools, but their communication was in the idiom of professionals encouraging apprentices and they maintained a hierarchy, similar to a medieval guild, to protect the highest secrets from the general public. In contrast, satellite pirates did not disguise their intent and shared information freely.

By Goldstein's definition, the locksmiths were criminals using the Internet to further crime. In contrast, the satellite pirates were explorers seeking understanding of a complex technology and libertarians defending their individual sovereignty (Goldstein, 1999c) which also characterizes the values of the hacker subculture (Goldstein, 1996; Levy, 1984).

Computer Criminals

Shelley (1998) described several types of computer crime and distinguished computer crime from other crime but this description did not refer to hackers. According to Shelley, computer crimes are those crimes committed only in the digital medium and

that can be conducted entirely on the computer, crimes like money laundering, tax evasion, and trafficking in child pornography. Shelley did not discuss crimes attributed to hackers, such as denial of service, network intrusion, or defacement of websites; thus the distinction proposed offers little guidance for the study of hackers.

Barrette distinguished computer criminals from hackers using the term "crime supported by computers" (1997, p. 66). Barrette placed the hackers, virus writers, and even thieves of computer hardware in a category termed "crime against computers" (1997, p. 31). Other literature similarly suggests that computer crime is separate from hacking in substance and in motivation (Mango & Cough, 1992).

Summary

Researchers have recently reported on hackers and criminal activities related to computers. Most of the literature investigated hackers from conceptual and qualitative perspectives, but there is little primary research on the direct activities of hackers. Some literature strongly suggests a difference between hacking and computer crime. Computer crime is a legal artifact more than it is a criminological phenomenon, made possible by a skill set and access to a computer, but computer crimes do not depart from traditional legal definitions of crime. Hacking, however, exists within a subculture that values deviant action that is not considered criminal (within that subculture). Although some of the literature draws a distinction between computer crime and hacking, there is no consensus on the definition of hacker. The literature fails to adequately address the need for an empirically based definition reconciling the differences and acknowledging the overlap of these phenomena.

Theory

Subculture theory (Beaker, 1963; Collard & Olin, 1960; Coven, 1955) and the theory of intrinsic motivation (Katz, 1988) can help to define computer criminals and hackers. Similar to other subgroups that deviate from the norms of society (Becker, 1963), hackers appear to understand that they are violating the laws of the dominant culture. However, they share a separate subcultural understanding of their actions.

According to traditional subculture theory (Collard & Ohlin, 1960; Cohen, 1955), subcultures share an identity in time and place and unity of purpose. However, Jordan and Taylor defined the geographically dispersed hacker community as a subculture based on Anderson's (1991) concept of the imagined community--a group of people with no geographic boundaries. Specifically, Anderson conceptualized imagined communities as "dispersed networks of individuals...that combine through a collectively articulated identity"(Jordan & Taylor, 1998 p.763).

Subculture theory explains enculturation into the hacker community. Since subcultural values may be formed in opposition to dominant cultural values, socialization is required to appreciate the new values offered by the subculture (Cohen, 1955). Subcultural activities are not instinctive--they often require knowledge, skill, preparation, and resources. Whether a hacking activity is a criminal violation or an elegant solution to a difficult problem, its results must be understood in terms of the subculture to be appreciated.

Hackers seem to be individually motivated to join the hacker subculture, which can be explained at least in part by the theory of intrinsic motivation (Katz, 1988).

Hacking is innately rewarding to experienced hackers who report a sense of power and

total absorption in the pursuit (Levy, 1984; Hanford & Mark, 1991; Litton, 1997). These claims recall Katz's (1988) formulation of an appeal to higher values in the justification of crime. Katz emphasized the role of individual needs in decisions regarding deviant behavior.

Based on Katz, it is possible that the personal needs of hackers can be met in a subculture in which they can express their interests and abilities, and the values of this subculture may not necessarily be congruent with the values of the dominant culture. For both Katz (1988) and Becker (1963), deviance from the norm is not the product of an economic calculation; rather, it is the result of a divergence between subcultural values and the dominant culture's legal values. Although the legalities and consequences of hacker activities are known, they are simply not considered.

Method

Triangulation of sources will be used to help define the word 'hacker' and distinguish it from 'computer criminal.' The terms of symbolic interactionism will help explain this qualitative data analysis. Methodological triangulation uses disparate methods to compensate for known weakness of each component method (Erzberger & Prein, 1997; Miller, 1983). Goddard (1997) adapted the methodological triangulation to include disparate sources, rather than methods, to provide a more comprehensive answer to the research question. The present typology of hackers will be created using three sources of information: (1) what the rest of the world knows of hackers through the media, (2) the actual self-definitions of hackers from their discussions on the Internet, and (3) the books, movies, and other materials used by the hacker subculture. Each of

these sources, which will be described further below, conveys ideas about how the word 'hacker' and the term 'computer criminal' might be defined.

Symbolic Interactionism

Symbolic interactionism is a conceptual tool that can be used to understand the observations of the social world (see Plummer, 1990) and perhaps the hacker subculture. Symbolic interactionism has been used to clarify ambiguous definitions of the self and of the social world (Becker, 1982). The typology will be developed, in part, from the ongoing Internet dialogs of hackers and their exchanges of ideas. The exchange of ideas and sharing of meanings is at the core of symbolic interaction (Blumer, 1969). The unit of analysis is an individual meaning or idea expressed through one of the three sources (media, self-definitions, and materials), therefore, the symbolic interaction refers to meanings that are shared with members of the hacker subculture through communication.

There are three basic premises of Symbolic Interactionism: 1) symbol making, 2) communication through symbols, and 3) the process of evolving meaning. One, it is human nature to make and manipulate symbols, and inherent in a symbol is the meaning attached by a social actor. All forms of communication involve symbols, however, their assigned meanings are often complex and ambiguous. Two, communication is the interactive manipulation of symbols (Goffman, 1959). Three, meaning attached to a symbol evolves as new meanings are negotiated in the process of communication (Strauss, 1978).

The present study applies these concepts to the creation of an identity as a hacker. Symbolic interactionism uses the symbol as the basis of communication. This applies in the spoken medium and in computer mediated communication. Mead's (1934) looking

glass self defines the process of creating an identity through interaction with others. In the hacker subculture, identity is the product of interaction. Identity depends upon negotiated interactions with members of the hacker subculture.

On a larger scale, the definition of the hacker subculture is also a process mediated by symbols. The earliest hackers claim an immutable definition of the word: hacker. The hacker subculture has appropriated the word and used it differently. The typology describing these groups is based on the negotiated meaning of the communication of the hacker subculture and an understanding of the ongoing process of interaction in the hacker subculture. The attachment of a name (i.e. symbol) to each type of hacker is only a descriptive label for an observable phenomenon and has no enduring meaning. In other words, there is no existential meaning to a label in this typology.

Triangulating Sources: Media, Internet Discussions, Materials

A Note about a "Mitnick List"

The Mitnick List is an E-mail discussion list maintained by supporters of convicted hacker, Kevin Mitnick (henceforth referred to as the "List" or "Mitnick List"). The List provides the most readily available collection hackers. Kevin Mitnick is known by his supporters and others to be a convicted computer intruder. Kevin Mitnick's case is unusual in that his last arrest, in 1995, was not brought to trial until the end of 1999.

During that time, Mitnick was denied fundamental rights such as a bail hearing, discovery of evidence, and a speedy trial. Popular support for Mitnick's plight grew, largely, from publicity generated by Emmanuel Goldstein, editor of *2600* magazine. Mitnick's treatment after apprehension was seen by many as defying the common sense understanding of the rights of the accused, in part due to questionable practices of the

federal prosecution team (Thomas, 1998b). To counter the perceived (and possibly real) wrongs against Mitnick, Emmanuel Goldstein established the "Mitnick List" to coordinate efforts in support of Mitnick.

Triangulating Source #1: Media Sources

The popular and underground media provide qualitative data for developing the typology. However, media sources often contain bias and error, and one major activity of the Mitnick List members was to identify factual errors in the popular media accounts of Kevin Mitnick's story (Loper, 1998). Errors can be identified in part by reviewing and comparing information from a variety of sources (Erzberger & Prein, 1997), however, many media sources simply reprint errors from previously reported articles or news services.

There is also a tendency in the media toward publishing the lurid or frightening aspects of crimes, including hacker crimes. An example is a list of credit card numbers found on Kevin Mitnick's computer when he was arrested. The press often reported that there were approximately 20,000 credit card numbers contained in the file. The press consistently failed to report that the same file was publicly available in **newsgroups**; the file was years out of date; and there was no indication that Mitnick used or tried to use any of the credit card numbers. According to Mitnick, the card numbers were a source of information for later use in guessing the system for credit card number generation (Mitnick, 2000).

In addition to errors in media reports, an inherent bias is their "legitimacy." That is, facts, issues, and events are explained to the readers in terms of the dominant culture. Even when events are depicted accurately, the conclusions reached and the apparent

conclusions often left to the readers do not reflect a hacker's understanding of an event. Alternative or underground sources are also subject to bias or error, but they often do manage to capture the essence of a hack or the meaning of an activity to hackers. Thus, there is considerable media information but those reports include error and bias. The method of triangulation attempts to overcome those deficiencies by using multiple sources.

To be included as a media source for this research, a news story must have been mentioned on the Mitnick List; a computer crime news abstract service (e.g. SANS bites, RISKS Digest, The Computer Underground Digest, or the Hacker News Network); or through links from previous stories (i.e. a snowball sample). In a snowball sample, each source is asked to refer other sources until a sufficient number of sources is achieved (Kinkade, Jenkins, & Loper, 1994).

An example of information obtained from a media source is illustrated in an article from the Hacker News Network (HNN) which reported on the socialization of "script kiddies," unenculturated hackers:

I run a hacking website that attracts exactly these types [script kiddies]. I can't count the number of times that I have received "Do you have the latest AOL scroller?" through the feedback form. My good friend and site sysadmin tells me that before we got the firewall, he had several users break in and start by trying to "dir"¹. However, I don't ignore these emails, and I don't send back nasty "Go Away" notes.
Flaming Cow (1998)

¹ MS DOS uses the command "dir" to display the contents of a directory. Unix uses the command "ls -l" to display similar information. The unspoken assumption is that DOS users are inferior to Unix users, or at least one should be able to tell the difference to be a credible hacker.

Flaming Cow identifies subcultural attitudes toward novices and toward the role of experienced hackers in socializing them into the subculture. This definition of types and roles has implications for the typology.

Ideally, the snowballing method would be used until all such media sources were retrieved, reviewed, and documented. However, pursuing this process to exhaustion is difficult, if not impossible, due to the many links in Internet sources that provide referral links to other sources, which in turn provide more links. Thus, the stopping point will be defined by saturation: when an idea is examined to the point where no further new information is introduced with new sources, the point of saturation will have been reached.

The information derived from this process should indicate the popular opinion of hackers and provide detailed and non-technical descriptions of notable hacks and their chronology. However, it is reasonable to assume that the popular media is not aware of all hacks because successful hacks may go undetected or be hidden by embarrassed companies and unsuccessful hacks may be ignored as unimportant. Thus, as a source, the dissertation considers popular accounts as informative but not definitive.

Triangulation Source #2: Internet Communications

The Mitnick List provides input from individuals who define themselves as hackers. The fact that many of them lack the technical skills associated with the popular conception of hackers lends to the immediacy of the need for an empirically based definition.

The List has an open membership available to anyone who knows about it and has the interest to join. There is no supposition that all or any of the List participants are

involved in criminal activity. Further, there is no supposition that all of the members post their opinions as many may simply read from the List. Several List users show evidence of sophistication using computers and the Internet and some are well-known, skilled hackers. Given the intent of the List, freeing Mitnick, it also includes politically active hackers. These individuals are more likely to discuss the meaning of hacking and the relationship of hackers to the dominant society whereas other "elite" hackers are more often concerned with technical matters (Jordan & Taylor, 1998).

Although the List is useful as a primary source of communication between politically active individuals, it is not the definitive voice of hackers in general and it is not even a comprehensive record of the communication among hacker participants. Many List members interact through Internet Relay Chat (IRC); Internet newsgroups; 2600 meetings held across the country; through private E-mail; by telephone; or through other unknown means. Thus, the communication used to generate the typology is not taken from a comprehensive collection of sources; the List communication represents a single, but important source. Specifically, the research seeks communications that refer to self-definitions, for use in the typology.

The data analysis uses postings to the Mitnick List from September 16, 1998 to April 3, 2000. Any message deemed relevant to the definition of hacker, delineation of computer crime, or the hacker subculture is included as an ethnographic source. An example follows from a direct statement by Emmanuel Goldstein about the use of the word 'hacker':

```
>wired likes to use that word [cracker]. so does markoff,  
>coincidentally. it's mostly because of pressure from some  
>of the older west coast crowd who thinks that use of the  
>word 'hacker' has been subverted by today's young punks.  
>to them, 'cracker' means criminal hacker. the way i see
```

>it, if someone becomes a criminal, then they're a
>criminal. do we have a special word for black criminals or
>truck driving criminals? no, we just call them criminals.
>the logic of this whole 'cracker' thing has always escaped
>me.
>
>Date: Mon, 7 Dec 1998 03:41:39 -0500
>From: Emmanuel Goldstein <snip!>
>Subject: Re: [mitnick] No More a Hacker,now a cracker

According to this message and others like it observed in the preliminary review, the word 'cracker' may not be a suitable type, for the typology. The message also suggest factions within the hacker subculture which, if observed in other messages, can help to distinguish different types.

Triangulation Source #3: Subcultural Materials

To be included as a foundational source, the item--novel, comic book, movie, or other--must have been mentioned in the media, the Mitnick List, or through links on web pages suggested by either. The process of cumulating information from source material is analogous to the snowball sampling procedure. The number of sources is determined by saturation: a sufficient number of sources has been retrieved and reviewed and when additional sources provide no new information. Appendix A lists the source materials--books, movies, and others--used to generate information for the typology.

There is precedent for including subcultural sources (books and other materials) in this research (Chandler, 1996; also see Duff & Gardiner, 1996; Jordan & Taylor, 1998; Mann & Sutton, 1998). Aspiring hackers often become acquainted with these sources before they begin to interact with hackers. Subcultural sources can offer insight into the self-definitions of hackers, and, often, hackers actually draw the inspiration for their Internet aliases (i.e. handles) from subcultural sources. For example, George Orwell's

mythical revolutionary in 1984 inspired hactivist Eric Corley to adopt the name Emmanuel Goldstein as his alias.

To summarize, there is no universally accepted definition of hacker. The research will develop a typology of hackers using subcultural theory as the guiding framework, and qualitative data will be generated from three sources of communication: (1) media definitions; (2) hacker self-definitions from the Mitnick List; and (3) books, movies, web sites, and other materials used by the hacker subculture. Each of the three sources, news reports, E-mails, and subcultural materials will be identified for use in this dissertation, retrieved, and reviewed. Using the method of triangulation for aggregating common information across sources, categories of hacker types will be developed.

Results

Computer Criminals and Hackers

Computer criminals may be defined as those who engage in crimes involving computers (Barrett, 1997). This definition can include hacker activities that fall outside of the goals of the hacker subculture for which recognition and subgroup membership are valued over financial gain. Therefore, the key distinction between a computer criminal and a hacker is not whether a hacker violates the law but whether the hacker acts in a way prescribed in the hacker subculture.

For various reasons, such as the pursuit of higher goal (versus financial gain), the subculture accepts actions that violate law. These may be called "criminal *hacking*." However, some actions are not accepted by the subculture and these may be called "computer *crime*." Figure One depicts this relationship.



Figure 1. The relationship between hacking, criminal hacking, and computer crime. The Venn diagram shows the overlap these concepts.

Definitions that equate all hacking with criminal behavior are offensive to hackers and inaccurate. Similarly, definitions that deny that any meaningful criminal action is committed by hackers are also inaccurate. This Venn diagram depicts a subset of hacker behavior that is illegal, but condoned by the hacker subculture (labeled criminal hacking) and the relationship of such actions to both computer crime and hacking.

Typology of Hackers

The following categories of hackers evolved as a typology using the triangulation procedure. The names for each category are names used by the hacker community. However, no empirical descriptions were previously associated with the following hacker names.

Old School Hackers

Old school hackers are not motivated by profit. Crime is incidental and trivial to their purpose. Laws that prevent the pursuit of a goal are disregarded rather than broken.

Bedroom Hackers

Bedroom hackers often work from their homes. They are characterized by limited resources. They are willing to steal services that facilitate exploration yet tend to hold a self-conscious ethic. Some of these criminal actions are self-serving although the goals are mediated by the hacker subculture.

Larval Hackers and Newbies

Larval hackers are characterized by limited knowledge. They are unsocialized in the hacker subculture and may unknowingly violate the hacker ethic. They tend to be eager to prove their skill and acquire status.

WaRez D00dz

Warez Doodz trade pirated software. Acquisition, collection, and recognition of their activities appear to be the primary goals. Their activities are specific and conscious violations of law.

Internet Hackers

The contemporary hacker has Internet access. Through this connection they have virtually unlimited access to knowledge and virtually unlimited access to resources prized by the above bedroom hackers. Where the bedroom hackers relied on the subculture to maximize scarce resources, Internet hackers rely on the subculture for the sense of community.

Hactivists

The common characteristic of hactivists is the use of hacker skills and attitudes to convey a political message.

Script Kiddies

Like larval hackers, script kiddies are characterized by limited knowledge and lack of socialization in the hacker subculture. The chief distinction between script kiddies and larval hackers is the apparent lack of desire to learn more than the most direct route to an effect.

Although it is not possible to provide consistent scaled descriptions from the available data, it is possible to provide a conceptual map of three common defining

characteristics for the types of hackers. Placing numerical values on the relative levels of these concepts is not possible given the available data. Even ordinal measures among the types would be questionable; however, the relative presence or absence of these concepts helps define the hacker types above. Further, there are numerous other characteristics unique to each type. Some of the unique aspects of each type are presented in the discussion section.

Characteristics common to most types include 1) access to resources, 2) enculturation, and 3) skill. Access to resources is the ability of a type of hacker to access computer hardware or information. Enculturation is the degree to which a type of hacker is expected to adhere to the values of the hacker subculture. Skill is the expectation of technical sophistication for a given type. Table 1 presents qualitative descriptions of the level of each characteristic found in each type. An arrow up or down indicates relatively more or less of a concept, respectively. A dot indicates the inapplicability of a concept to a given type; each dot is explained below.

Table 1

Hacker Typology Concepts

	Resources	Enculturation	Skill
Old School	•	↑	↑
Bedroom Hacker	↓	↑	↑
Larval Hacker	↓	•	↑
Warez Doodz	↓	↓	•
Internet Hacker	↑	↑	↑

Script Kiddies	↑	↓	↓
Hacktivists	↑	•	•

Old School hackers traditionally had almost unlimited access to computer hardware, but could not readily access knowledge bases because they had not yet been constructed. Further, although access to hardware resources was unlimited, the hardware was very limited. Larval hackers are unenculturated, by definition, but actively attempt to become enculturated. Warez doods have a wide range of skill. The most skilled can dismantle sophisticated software copy protection; while, the least sophisticated can do little more than follow simple instructions to crack or distribute software. Hacktivists often subordinate the values of the hacker subculture to their political goals. For instance, the prohibition against hacking for personal gain does not prevent hacktivists from using hacking to spread their ideology. Hacktivists skill ranges from very low, to very high. At the high end, the Cult of the Dead Cow has provided technical assistance to the Hong Kong Blondes in their protests against China's human rights policies; at the low end, some hacktivists have only minimal skill (e.g. many hacktivists in this study were confused by mailing list software).

Discussion

Distinguishing Criminals from Hackers

It is clear from each of the triangulating sources that hackers distinguish themselves from computer criminals. For example, the following communication on the Mitnick List expresses indignation over the labeling of criminals as hackers and vice versa.

>An entire community of people has been calling themselves
>hackers since before there was security to break. These
>people call those who make a practice of breaking security

```
>'crackers', and tend to think of them as nuisances more
>than anything else. This isn't to say that a True Hacker
>doesn't break security; he may well do so --- it's just
>that being a peeping tom isn't his goal in life.
>
>Date: Mon, 7 Dec 1998 01:38:20 -0500 (EST)
>From: "Aaron D. Ball" <snip!>
>Subject: Re: [mitnick] No More a Hacker, [sic] now a cracker
```

In another example where the word 'cracker' is synonymous with 'criminal hacker,' a convention used by some List members, the discussion involves the death penalty imposed upon Chinese embezzlers by the People's Republic of China:

```
>They aren't even hackers. I'd call them crackers. They
>are just stealing plain and simple. If anyone could make
>the distinction I'd think Wired would and could. I guess
>not. :(
>-Iconoclast
>
>Date: Tue, 29 Dec 1998 01:57:04 -0500 (EST)
>From: Roger Harrison - ACM2 Admin <snip!>
>Subject: Re: [mitnick] CHECK THIS SHIT OUT
```

The distinction between hackers who commit crimes not sanctioned by the hacker subculture and other computer criminals rests upon the attitudes with which a hacker approaches the activity (of hacking). The distinction can be understood by considering the social context of hacking.

The Hacker Subculture: The Social Context of Hacking

The hacker subculture provides the context in which hackers situate their actions. Mill's (1990) concept of vocabularies of motive can help explain the mutual agreements and stated principles of hackers. A key concept of Mill's work is that motives are not inner needs but rather the products of ones' environment, or social context, defined through interactions. Accordingly, hacking would not be considered an instinctive activity. The act of hacking requires elaborate preparation, resources, and extensive knowledge, often obtained through socialization within the hacker subculture. The hacker subculture therefore provides the social context in which certain activities are

normative but which may be indefensible when confronted with the mores of the dominant culture. The examples below provide some insight into the hacker subculture and the social context that distinguishes "criminal hacker" and "computer criminal," beginning with the following brief background information.

Foundational sources obtained through the present triangulation procedure (Hafner & Markoff, 1991; Littman & Donald, 1997; Slatalla & Quittner, 1995) depicted hackers as markedly different after being taken into custody. Hafner and Markoff (1991) present Kevin Mitnick as cold and vindictive while hacking, but prone to weeping and nausea when captured. Captured hackers are notorious for accepting plea bargains, which include testimony against their fellows. In the following excerpt, Kenneth Sooyna begins a diatribe against Agent Steal, an informant hacker accused of trying to entrap Mitnick, with a grudging acceptance of Steal's initial plea bargain.

```
>to agent steal, justin peterson or what ever you call  
>yourself,  
>  
>i forgive you for snitching on mitnick.  
>i'm sure many of us would snitch if put under  
>extreme pressure or under other circumstances.  
>  
>Date: Sat, 21 Nov 1998 11:30:09 PST  
>From: "kenneth sooyna" <snip!>  
>Subject: [mitnick] stir up some trouble
```

In another example that was consistently observed across the triangulating sources, hackers seem to experience a feeling of power and control not found in real life. In the following excerpt, a reporter asks a hacker about website defacements:

```
"Defacing a site to me is showing the admins, government  
[and others] that go to the site that we own them," wrote  
"soupnazi," one of the founding members of the Keebler  
Elves, in a chat with ZDNN. "They wouldn't even know we  
were in [their systems], if we didn't deface [them]."  
(Lemos, 1999)  
[All brackets and quotation marks original]
```

In yet another example, "Phoenixknt" expresses the tangible benefit to self-esteem that comes from the power and control found in hacking.

```
>I agree, it's [hacking] not harmful, possibly helpful. I
>mean, confidence can be gained, and though it may not be
>well placed at times, it can be carried over into p-space
>(physical-space), and hackers who were losers (i stress
>that i don't know many, but a few) now won't give off the
>"I'm helpless come pick on me vibes" though not too many
>give off the "I'll fuck you up" vibe either...that I know
>of.
>-Absolute Matter
>
>From: Phoenixknt@<snip!>
>Date: Sun, 23 May 1999 23:23:24 EDT
>Subject: Re: [mitnick] Other case
```

The agreed upon values of the hacker community provides the social context for the hacking activities that violate the standards of the normative culture. The disjunction between the morals of the hacker subculture and the morals of normative society helps to define the activities of "criminal hackers."

Prosocial Hacking

Sometimes members of "deviant" communities define their activities as prosocial (Becker, 1963). The prosocial aspects of hacking define the subculture and differentiate it from computer crime. For example, the triangulation revealed hacker reports of learning experiences, including creative problem-solving, and educating others about security vulnerabilities. In the following example, Social Mysfyt responds to another List user's request for a shortcut to hacker prowess. In so doing, Mysfyt appeals to one of the most fundamental tenets of the hacker subculture: learning.

```
>"hacker" means many things to many people, however i
>believe that one of the only *common* threads is the DRIVE
>to learn more and do more. by asking for help in getting
>started this person already defeated themself in a *game*
>he knew nothing about. if you don't have the initiative
>and heart to push yourself to find all the answers
>possible first, you'll never amount to anything
>
```

>From: "social mysfyt" <snip!>
>Subject: Re: [mitnick] help me out! II
>Date: Thu, 2 Dec 1999 22:44:47 -0500

Another user commented on an ad by IBM depicting hackers as breaking into a company's computer system. In the ad, the security team discovered that the hackers had distributed salary information throughout the company. Ksandre sees a perverse victory for hackers in an ad that was almost universally decried on the List. To Ksandre, the ad extols the egalitarianism attributed to hacking.

>The interesting part about that ad is that they showed the
>hackers as exposing the inequities of the corporation into
>which they gained access. It seems there is a mixed
>message in it, depending from which side of the fence one
>views it. (Note especially that the hackers _only_
>emailed inside the corporate office.)...
>I thought it was a very mixed-message ad - almost kinda
>'promoting' hackers-as-wistle-blowers against the
>inequities of IBM.
>
>Date: Fri, 18 Sep 1998 04:38:32 -0400 (EDT)
>From: ksandre <snip!>
>Subject: Re: [mitnick] ibm
[ellipses original]

In both cases, user comments support an idea found in the other triangulating sources on the hacker subculture: hackers can act in ways that support a higher cause. As Katz (1988) found, the crime is often contextualized as a positive action for one that is more relevant--such as the higher goals claimed by many hackers.

Again, Mill's (1990) vocabularies of motive helps explain the relationship of the on-line interactions in reconceptualizing the meanings of hacker's actions. By defining actions as prosocial, the hacker subculture both neutralizes blame under other systems of belief (e.g. the dominant culture's legal structure) and furthers the subculture's goals (e.g. exploration). It is the vocabulary of motives found in the above messages that defines the subculture's values and the individual hacker's moral self (Perinbanayagam, 1985).

The Hacker Ethic

Insight into an hacker ethic can be derived from the triangulation. For example, one subcultural-material source revealed how "old school" hackers developed a code of conduct and ideology:

1. Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total. [p.27]
 2. All information should be free. [p.27]
 3. Mistrust authority - promote decentralization. [p.28]
 4. Hackers should be judged by their hacking, not bogus criteria such as degress, age, race, or position. [p. 30]
 5. You can create art and beauty on a computer. [p.30]
 6. Computers can change your life for the better. [p.33]
- (Levy, 1984)

These norms are the product of a particular type of hacker: the "old school" hacker.

When hackers left the university setting, they were forced to adapt aspects of their behavior to their new environments. Therefore, we see an evolution of the hacker ethic to fit the expanded domain of later hackers.

The evolution of the hacker ethic is demonstrated in an example from another subcultural-material source: "The Hacker Manifesto." The manifesto introduces a new type of hacker. It evokes the angst of young bedroom hackers and the notion of oppression by greater society. This excerpt is taken from the end of the Manifesto:

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all...
(Blankenship, 1986, webpage).

The full text of the manifesto can be found in Appendix B. The Mentor, author of the Hacker Manifesto, was a member of the Legion of Doom (LOD). LOD was the most prominent hacker group of the 1980's (Sterling, 1992), the era of the bedroom hacker.

One of the more recently published subcultural materials is a definition of hacker ethic that stressed the importance of information sharing and the requirement of no harm:

1. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source and facilitating access to information and to computing resources wherever possible.
2. The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality. (Raymond, 1996, website).

The requirement to do no harm may be an evolutionary step in hacker subculture: previously, hackers existed in the universities--the "old school"; then the crime of curiosity was described in The Hacker Manifesto; and now above, a norm of minimizing damage has been added.

The triangulation uncovered a comment by one List user describing Kevin Mitnick as a traditional hacker and affirming the above hacker ethic:

```
>The only justification I can think of for calling Kevin a
>'Cracker' has to do with skin color, not because of his
>alleged computer fraud. The fact is that Kevin is the
>textbook definition of the traditional hacker. One with a
>deep understanding and respect for the technology he uses,
>which is reflected in his ethics...

>"The Jargon File" is hardly an officiating source, it's
>just another demonstration of the failure of mainstream
>and technology publications to accurately report on the
>hacker community.
>
>Date: Mon, 7 Dec 1998 00:38:00 -0500 (EST)
>From: Macki <snip!>
>Subject: Re: [mitnick] No More a Hacker,now a cracker
```

The prohibition against damage was also discovered in subcultural material describing Phiber Optik (Slatalla & Quittner, 1995). According to the report, Phiber Optik damaged an electronic bulletin board system as part of a prank; however, the incident affected him deeply and thereafter he tried to follow the definition reported above by Raymond (1996).

However, there is considerable evidence that not all hackers adhere to the hacker ethic in all of their activities. One triangulation source (Hafner & Markoff, 1991) alleged that Kevin Mitnick attacked and damaged the computer of a shipping company that refused him access. Also, the media sources revealed numerous articles detailing the criminal actions of web vandals, thieves, and stalkers. Hackers who act outside of the hacker ethic are simply criminals.

Adherence to the hacker ethic and pursuit of subcultural goals define the difference between computer criminals and criminal hackers. The majority of hacker activities (i.e. those encouraged by the subculture) may be deviant by the standards of the dominant culture, but they are not criminal. The great difficulty in differentiating these three groups is that human behavior is dynamic and contextual. There is therefore no simple dichotomy between hackers and computer criminals. However, the process of triangulation uncovered historical backgrounds that can provide contexts for a better understanding of the different hacker "types."

Context for the Hacker Typology

Old School Hackers

The Massachusetts Institute of Technology (MIT) is famous for the birth of hacking, although U.C. Berkeley, Carnegie Melon and Stanford simultaneously spawned hackers (Levy, 1984). Hackers first developed in the earliest days of computers when

researchers had to experiment with computers to see what they could do. Invariably, this was accomplished at universities or corporate research campuses. There was no concept of home computers in those days (Hafner & Lyons, 1996).

These same researchers recognized that they had written the book on computers and were under no obligation to follow the book. They solved problems on the fly and often just 'hacked' out programs to solve a problem. Hacker ethos was different from corporate or engineering ethos. The latter required understanding and a plan before a solution. Hackers just worked with the problem and depended on their own intimate know of the machine and software to discover the most direct solution. Levy (1984) based his hacker ethic on the "old school" hackers of MIT.

Like their programming skills, the ethic evolved in the absence of another option. What began as an obvious and convenient conduct became an ideology. Most of the imperatives of the hacker ethic revolved around access to or distribution of computer knowledge. When norms blocked access to the computer, hackers determined that information must be free.

The ultimate goal of these early hackers was to reduce the number of instructions needed to solve problems or produce results, and a hacker-optimized code may have been the best way to produce a result. The quest for efficiency became so embedded in the early hacker culture that it persists even after the machines have reached the point where it is not necessary. Cleverness and concise code have taken on an aesthetic value that transcends necessity. This trait may be at the root of the hacker's legendary cleverness and tendency to brag about good hacks. Quick and clever solutions gave hackers their name.

The term hacker came about in response to the interactive programming style used by these amateurs. In the late fifties, computer processor time was at a premium. Programs were laboriously checked by hand before entering them via Hollerith Cards into batch processing machines. Errors could not be corrected once the process began; they would often remain unknown until the end of the batch process. An early error could render the whole batch unusable and unproductive. To minimize the waste of computer time and to protect the machine, technicians would not allow users to interact with the machine. They submitted cards and received output.

The MIT hackers had direct access to an old unused machine²(TX-0) and developed interactive programming. An error would present itself and the run would stop while the hacker fixed it. This style placed a greater value on clever fixes than original accuracy. It also encouraged more risk taking. Changing a command on another machine might waste the entire batch time allotment for a project for that week; thus, batch processed programs tended to be more conservatively written. The hackers had no reason not to take chances to optimize their programs to get the best result for the least input. Hackers not in the control seat of the TX-0 developed a habit of collaboratively working out the bugs in each other's programs. This collaboration remains a tenet of hacking today (Levy, 1984).

Bedroom Hackers

In the early 1980s when home computers became widely available, bedroom hackers used their new-found computer skills to gain access to other people's systems. Electronic bulletin boards flourished and disseminated techniques and passwords to allow

hackers to explore the network. Phone phreaks (see below) entered the hacking scene and spread their own techniques, revolutionary politics, and street culture to the bedroom hackers. By the mid-eighties hackers and phreaks were virtually indistinguishable. During this time, groups called the Legion of Doom and the Masters of Destruction intruded into the switching system of American Telephone and Telegraph (AT&T) itself. Thus, the hackers/phreakers could now use the computers that controlled the phone lines to mask their own intrusions into other computer systems.

Bedroom hackers created an entire social milieu separate of corporate research parks and universities. They created their own dialect. Numbers were substituted for visually similar letters. Capitol letter were freely and randomly used. For instance, 'elite hackers' became 31337 HaXorZ. Letter substitutions are common like z for s or especially k for c. Typographic symbols on the IBM terminal standard were also used, for example, H@xOr, and jargon became important to understanding the communication of these bedroom hackers. Even the strange written-phonetic-visual puns has a name: **l33t sPeaK** or elite speach or any variation thereof. An example of this communication was discovered through a news report material source, the New York Times hacked web page at <http://www.2600.com/hackedphiles/nytimes/>. The crackers who hacked this page left their mark in almost indecipherable k-rad.

Bedroom hackers reached their zenith before E-mail moved out of the universities. They communicated through text files written in ASCII (a plain text standard with no formatting so as to be compatible with the various standards of the day).

These PHilez became the standard of communication through telephone bulletin board systems (BBS). The reliance on long distance telephone lines may be the primary reason for the alliance between hackers and phone phreaks. It may also be a shared infatuation with high technology and complex systems. Before computers, the telephone system was the single most complex system in the world.

Levy describes the hacker ethic implicitly adopted by the "old school" hackers. Hackers will not harm the computers they explore nor will they destroy the data they find (1984). Some bedroom hackers, like Phiber Optik, respect this ethic. The corollary to the hacker ethic is disrespect for those who hoard knowledge or seek to unfairly restrict computer access. The Mentor (Blankenship, 1986) described this corollary in the Hacker Manifesto:

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals
[Material omitted; ellipses original]

The tone of The Hacker Manifesto predates the literary movement in science fiction known as cyberpunk. It may well be that the anti-corporate tone of that genre is the product of the Mentor. From the sources reviewed, it seems that the bedroom hacker is aware of this literary tradition and may likely also be aware of The Hacker Manifesto.

Internet Hackers

While there are remnants of the previous types of hackers, they appear to be products of their times, although the "old school" still exists in L0pht Heavy Industries, a Boston based hacker group. L0pht has devoted considerable effort to warning Microsoft and Microsoft users about potential security flaws. Microsoft replied that these problems

were only theoretical. L0pht responded by creating scripts to exploit these flaws and distributing them via the Internet. The L0pht motto is "Making the theoretical practical." The members of this group do not profit from their work; they work for the satisfaction of forcing the software industry to fix its flawed products and admit its faults. Like the hackers of old, they cannot stand intentionally imperfect systems.

Recently, there has been an increase in the political activity of self-identified hackers. Hackers have combined to challenge the treatment of their peers by the government. Early cases like those of Phiber Optik drew the attention of hactivists who also rallied around Kevin Mitnick. Examples include Kevin Poulsen, a convicted hacker, who now writes a column for the Ziff-Davis web magazine and who has spoken out about Mitnick's case in numerous columns in that magazine; Phiber Optik, also a convicted hacker, who has spoken out on a radio show he co-hosts; and Emmanuel Goldstein, editor of *2600: The Hacker Quarterly*, who started the Mitnick E-mail List for the intention of assisting Kevin Mitnick.

Recent web page hacks serve as evidence of this growing search for political notice. Many web page hacks target servers with weak security or high volume traffic. Unsecured web servers are accessible through a number of well-known exploits. High volume sites, which are usually more secure, are sought after by politically active skilled hackers to spread a message. For instance, Portuguese hackers cracked the Indonesian government's web page to protest the government's actions in East Timor. In other cases messages about Kevin Mitnick have appeared on cracked sights ranging from the New York Times to UNICEF.

The technology of choice for the contemporary hacker is the Internet. Bedroom Hackers are in their twilight, but the research revealed that files have been archived on web servers to maintain the historical connection with the hackers and phreaks of old. The relatively low costs of Internet access and the proliferation of powerful home computers may greatly impact the traditional alliance between hackers and phone phreaks. Powerful home computers means there is no longer a need to connect to a host mainframe via long distance phone lines. The Internet allows rapid communication and information archival services without toll connections to Bedroom Hackers.

Larval Hackers and Newbies

Larval hackers tend to be excited about exploration, but based on the source materials they are easily misguided or diverted to cracking, vandalism, bragging, or other vices. Larval hackers seem to not know where to start, but to want to start immediately. The term "Larval Hacker" is really an entry category. They have existed since the "Old School" days, but there they were socialized to respect the machines and the rights of others. At the zenith of the Bedroom Hacker, they had no such guidance and were often rejected until they proved the worth by finding useful information or committing a notable hack. A group called The Legion of Doom maintained a 'secret' Bedroom hack site where only elite hackers could peruse the accumulation of hacker/pheaker knowledge (as well as the usual brags and boasts) amassed by the group. Newbies had to find a way into the secret hack site to be considered adequate.

Crackers and Script Kiddies

The review indicated that "Crackers" is derogatory word for a hacker with criminal or vandalous intent. It stems from the distinction made by the Mentor in the

Hacker Manifesto (described above): "Real" hackers explore and "Crackers" harm. A variant of crackers is the "Script Kiddy." Script Kiddies download other people's programs to perform their crack. They often care little for the underlying technology or intricacies of the glitches they exploit. Script kiddies resemble Larval Hackers, but they do not share the curiosity of the latter.

Where Larval Hackers may cause harm, Script Kiddies revel in it. If Larval Hackers are incompletely socialized hackers, Script Kiddies do not desire entry into the hacker subculture. The distinction between Larval Hackers and Script Kiddies is largely a matter of definition at the initial stages.

Conclusion

The goal of Part I was to establish a working definition of the word "hacker" based on observable facts generated from sources that are relevant to hackers. That is, the aim was to define computer crime and hacking in a way that is consistent with hacker's understanding of the phenomena. From this definition, existing theories can be adapted or new theories can be developed to explain and predict the actions and responses of hackers.

The material reviewed indicates that hackers do not consider themselves criminals although they acknowledge the necessity of some criminal actions in pursuit of subcultural goals. Their activities therefore can include crimes that facilitate access to information; crimes that cause little or no damage; and crimes that repair an injustice.

The present research revealed empirical differences between computer criminals and hackers, however, the existence of a real difference between two groups committing crime does not imply that punishment must differ. Further research might investigate

legal ramifications of criminal activities that are committed for different reasons. The rationale being that some more than others may be amenable to treatment or legal punishments other than incarceration and statutory guidelines may therefore differ for different groups.

Further development of theory and practice rely on the recognition of computer crime as a complex phenomenon. To accurately explain or predict such phenomena cannot be defined simplistically. The typology presented here can be useful for describing hackers who conform to the hacker subculture (versus a criminal subculture) and for explaining and understanding differences in the activities of hackers. The typology explains why 1) some hackers commit crimes but do not consider themselves criminals, and 2) other hackers do not commit those crimes and do not consider those who do to be criminals either.

Part II: Profile of Activities

Literature Review

Jordan & Taylor (1998) offer the only direct survey of hackers found in the literature; they interviewed hackers to obtain material for a grounded theory analysis of the hacker subculture which identified several themes, including "technology, secrecy, anonymity, membership fluidity, male dominance, and motivations" (p.757). The term membership fluidity refers to hackers entering and leaving the hacker community. Secrecy and anonymity are related concepts, but distinguished from each other; anonymity refers to the hacker's identity, while secrecy refers to the hacker's activity.

Jordan and Taylor's profile of the hacker subculture provides methodological guidance to this dissertation and offers the chance for confirmation or disconfirmation of equivalent findings. Their study also defined basic concepts of the hacker subculture (e.g. anonymity and identity) that provide guidance for categorizations of hacker activity. However, Jordan & Taylor (1998) neither quantified nor theoretically developed the themes involved in computer activities.

Theory

The goal of this study is to identify meaningful themes in the on-line activities of hackers. The themes will be organized into relevant categories. Grounded theory (see Strauss & Corbin, 1998) will be used to guide an unbiased and systematic data collection.

In a grounded approach, research question development and revision are guided by the emergent quality of the information and the continuous feedback of the information into the analytical process...it reduces the likelihood that the researchers will impose irrelevant, preexisting theoretical categories on the data and instead allows the data to speak for itself. (Kinkade & Jenkins, 1994 p. 39 internal quotation marks omitted)

Using this approach, consistent categories are noted in the data. These categories are explained and reported in the context of their source (Jordan and Taylor, 1998). Whyte (1983) recommends that field data be organized by grounded theory based. Using preconceived data indexing can influence data collection. Actors and events provide an unbiased system to organize notes. Thus, initial categories should be purely descriptive because inductively derived categories are appropriate to the data (Whyte, 1983).

Method

This study conducts an ethnographic, extended-case study of a hacker mailing list using the complete-observer method (Gold, 1969). In the complete observer method, the researcher announces neither the intentions of the research, nor the fact that it is being conducted. In essence, the researcher does not interact with the research population. This observational strategy is unusual in ethnography because the researcher must often interact with subjects to be included in the subjects' culture. The unique nature of hacker interaction allows the complete-observer method to be used without sacrificing opportunities to observe. In addition, this method was chosen because the entire content of the mailing list is taken from an archive; thus, there is no opportunity for direct interaction.

In the interests of disclosure, I will briefly note my previous participation in the list. In a pilot study for this dissertation, I acted as a participant observer on the Mitnick list. In this capacity, I posted messages to the list and actively engaged in the activities of the list. My role as participant observer ended after I completed the pilot study (Loper, 1998). The data subsequently collected and used in this dissertation does not contain my posts.

This research uses ethnographic techniques to discover consistent categories that can then be analyzed with quantitative methods. Ethnography is a complete method by itself, but for my purposes, it is subordinated to the quantitative process. Cromwell (1996) described the elements of ethnography used in this study:

Field research, also called ethnography, provides a way of looking at the complex contexts in which any research problem exists. Good field research results in... thick description--access to often conflicting and detailed views of the social world held by the subjects being studied. (p. x)

This research seeks to categorize common activities in the hacker culture rather than present the detailed understanding of hackers used to create the categories.

The 'activities' data for this research will be drawn from the Mitnick list, which was also used in Part I to define hackers. The results of this analysis using grounded theory will be a collection of meaningful categories of hacker activity from which a profile of hacker on-line activities will be generated.

Participants

Selection

The E-mail list was chosen as a source of observation because of the self-conscious discussions involving the (a) legal status of Kevin Mitnick, (b) ethics of hacking, and (c) activity of hackers. These topics are expected to produce a more explicit discussion of the hacker subculture.

Demographics

The unavailability of demographics for the E-mail list users is not unique to this research. Jordan and Taylor (1998) described the problems with acquiring accurate demographic information on hackers:

The global and anonymous nature of computer mediated communication exacerbates [the basic problem of studying an illicit community]... because generating a research population from the computer underground necessitates self-selection by subjects and it will be difficult to check the credentials of each subject (p.760).

Data Collection

All data obtained for this study are taken from an archive of E-mail to the Mitnick list. The list was sponsored by *2600*, a magazine devoted to the hacker community. The list was not moderated. All messages sent by users were distributed to all list members. The archive represents the entirety of list interaction.

Data Analysis

Grounded theory suggests that emergent qualities of the data are best suited to organizing the content of the data (Kinkade & Jenkins, 1994). Thus, there are no categories a priori imposed, nor are there specific, a priori research hypotheses associated with an inquiry (Glaser, 1992). A criticism of grounded theory is that it is an idiosyncratic method that cannot generalize (Strauss & Corbin, 1998). However, the purpose of the present study is not to predict or generalize. This study will provide categories for the activities of hackers. The categories present a quantifiable description of interactions among the list members not biased by the imposition of theory. Whyte (1983) recommends grounded theory for these purposes.

Procedure

As themes emerge from the data they define initial categories. Each communication is then sorted into an initial category. Initial categories are simply descriptive; they do not rely on assessments of list user's motives (even when apparently stated). Some categories are removed or merged into others. This process represents the natural growth of ideas and expansions of understanding. In some cases, a

communication contains more than one theme; these messages are noted and will be used in all relevant categories. The initial categorization of messages does not change their content.

Components are created from the initial categories. Components indicate a consistent quality across the topic of messages. Like the initial categories, components are removed or merged with others depending on the natural growth of ideas and expansion of understanding. The components are arranged into constructs. Each construct is represented by a computer directory that contains a file named for its component. The file contains individual E-mail messages. Arrangement into components and constructs does not alter to content of the message; if necessary, the original unsorted database could be reconstructed by moving all messages to a single computer file.

The categorization process is a search for ideas, not words. Therefore, it is important to maintain the context of the messages during each subsequent recategorization. To aid this goal, I use a duplicate database of the messages sorted by date rather than topic. With this, I can locate a particular message from a category being resorted and read the previous messages in the **thread**.

As an example of the categorization procedure, one list user: Colt started an intense **flame war** by stating his belief that China would invade the United States in 2024. The majority of the posts over then next several days dealt with refutations of the statement and the conjecture offered to support it. Many of the posts relied upon ad hominem attacks on Colt. This behavior is a classic flame war. Even these apparently gratuitous personal attacks become relevant activities. The first category for this group of

postings was called **"trolls and replies."** Upon reflection, I decided that this category called for an assessment of the list users' motives. I revised it to a more descriptive **"china invades."** In the final sort, it was merged with **"flames"** within the category **"Internet Conventions."** Because "flames" indicated behavior beyond the idiosyncratic exchange on China's pending invasion, it is a component.

Reporting Format

Exemplary quotes from messages will be used to explain each component. Transcribed messages can be uniquely identified without identifying the sender. The computer program used for collection of data was designed to delete the domain name from the sender's E-mail address. For example, the E-mail address: JohnDoe@foo.com would be reported as JohnDoe@<snip!>. Thus, the reader can associate the sender of the message with other quotes, but there will not be enough information to allow contact with the sender.

Apparatus

The E-mail messages were collected using an Eudora™: an E-mail software client that is widely available. Eudora™ was chosen for compatibility with existing archival data and because Eudora allows quick searches for words in text and the sorting of messages by sender, date, or subject. The various sorts are accomplished by arranging directories and sub-directories in the hierarchy of Eudora's mailboxes.

Human Subjects

The research design of this dissertation received approval from the University Committee on Research Involving Human Subjects at Michigan State University. The list users are aware that the list is open to the public and that their communications have no expectation of privacy. The communications are public behaviors. To minimize the

effects of attention drawn to particular users, the analysis will delete the user's E-mail domain rendering the remaining alias useless for purposes of identification. Since the data come from an archive, rather than direct interaction with list members, no verifiable informed consent was possible. Further, the contents of the list are public information.

Results

Several categories of response were identified on the list. Components present meaningful and consistent themes found on the list. Components address the basic research question: what are hacker activities? Table 2 provides a summary of the four constructs and the components within each.

Table 2

Constructs and Components of Constructs

Construct	Components with an example
Communication	• Medium of the List, A List user explained the procedure for leaving the list. • Execution of Communication, A List user corrected other user's grammar. • Internet Conventions, A List user objected to posts not related to Mitnick's case.
Identity	• Spoofing, A List user explained how a spoofer impersonated a list user. • Change of Address or Alias, A List user created a new identity by changing his or her E-mail address.

- **Multiple Identities**, A List user frequently changed his or her apparent identity on the List.
- **Limited Purpose Identity**, One List user apparently created a new identity to attack another from a position of anonymity.

Subcultural Activities

- **Definition of Hacker**, A List user defined hackers by their actions.
- **Ethics of Hacking**, A List user suggested acceptable reasons for hacking.
- **Scene**, A List user demonstrated knowledge of hacker history.
- **Corporate and Government Distrust**, A List user responded to a corporation's legal claim on his web address.
- **Fiction and Literature**, A List User noted the technical flaws of a movie about hackers.
- **Enculturation**, A List user encouraged inexperienced members to find their own answers.

Hackivism

- **Media Coverage**, A list user expresses frustration about inaccurate and sensationalistic coverage of Mitnick's case.
- **Grassroots Publicity**, A list user helps plan a protest with local knowledge.
- **Support for Mitnick**, A list user asks for help in sending a package to Mitnick in prison.

Each component is a general summary of ideas that apply to several initial categories.

Examples are representative of the component, not exhaustive.

Discussion

As noted in Part I, there are many types of hackers. The users of the Mitnick list may fit into several types, but most are hacktivists. Thus, components may include discussion of subjects not directly related to hacking, but closely associated with hacktivist activity in addition to strictly hacking related subjects. Each section below indicates a construct with appropriate subtopics. All subtopic examples are also representative of their category. If possible, the most explicit statement of a category is used.

Communication

Three components of communication are present on the list. The first: medium of the list, deals with the nature of communication on the mailing list. Hackers seek to understand the way computers work (Levy, 1984). List users support Levy's assertion by exploring and manipulating concepts related to the technology behind list communication. The second: execution of communication deals with the conduct of text-based communication. Topics in this component range from grammar and rhetorical skills to the use of **ASCII art** and **emoticons** like this ":-)". The importance of computer-mediated communication in maintaining the hacker subculture makes it reasonable to expect emphasis on effective execution of that communication. Finally, the third subcategory found in communication is that of Internet conventions. Certain styles of activity are commonly found on the Internet (Blanco, 1999; Christensen, 1996; Kendall, 1996). These conventions are also found on the list. The presence of Internet

conventions, supports the placement of hackers in the Internet hacker type. Each of these components relates to the construct of communication.

Medium of the List

A consistent example of the list user's awareness of the medium of their communication came when an unskilled user tried to leave the list. The Majordomo™ software used to conduct the list has two channels of communication. By sending messages to the broadcast channel, a user can post to the list. Each discussion list has its own broadcast channel. For instance, 2600 provided the Mitnick list and the H2K list. A user would have to subscribe to both to receive both because they are broadcast through separate channels. All messages in the present study come from the Mitnick broadcast channel. To send a message to the broadcast channel, a user would send E-mail to Mitnick@2600.com. The second channel is the command channel. It is **out of band** with the broadcast channel so users do not have to see administrative messages. To send a message to the command channel, a user would send E-mail to Majordomo@2600.com.

To subscribe to the list every user was required to send a message on the command channel. With Majordomo, a typical message would be to Majordomo@2600.com with the words "subscribe Mitnick" in the body of the message. When users leave the list (i.e. unsubscribe), they are also required to use the command channel. If a user mistakenly sends the unsubscribe message to the broadcast channel, all of the list users receive the message "unsubscribe Mitnick." To prevent such mistakes, a message is included in the header of every E-mail sent on the broadcast channel:

```
>Reply-To: mitnick@2600.com
>X-Comment: To unsubscribe, send mail to majordomo@2600.com
>from the address you're subscribed from, with the body
>"unsubscribe mitnick".
```

Unskilled users often ignore the headers or use software that conceals the headers from them. Responses to unsubscribe messages ranged from helpful to belligerent.

```
>On Thu, 29 Apr 1999 atomix@<snip!> wrote:
>>unsubscribe mitnick
>>
>ok, I'll explain this only once, so you'd better pay
>attention,
>write to majordomo@2600.com
>subject: (blank)
>body: unsubscribe Mitnick
>if you have a signature, either erase it or write end
>after the unsubscribe
>
>Date: Thu, 29 Apr 1999 16:17:57 -0500 (CDT)
>From: Rodrigo Saldaña Zárata <snip!>
>Subject: Re: [mitnick] De Payne pleads
```

Below, Colt sends a more harshly worded reply to a list user who made an unsuccessful attempt to leave the list by sending the message to the list rather than the Majordomo™ control channel. This occurred shortly after several others attempted to leave and received assistance from list users.

```
>At 12:19 AM 6/28/99 EDT, you wrote:
>>unsubscribe mitnick
>>
>I swear I'm gunna kill the next jack ass that does this. I
>have had enough danm it! Read the fucking directions in
>the reply mail when you subscribe! If you refuse to read
>the mailing list instructions, then stay the hell off
>mailing lists!!!
>
>Date: Mon, 28 Jun 1999 00:16:33 -0500
>From: "Colt" <snip!>
>Subject: Re: [mitnick] (no subject)
[sic]
```

It would seem that those improperly unsubscribing draw list user's ire by both abandoning the group and showing a lack of technical competency; however, it is also possible that list users are simply annoyed by the frequency of the irrelevant messages.

Other references to the mechanics of the list indicate that hackers are aware of the fact that their communication is computer-mediated. In this case, a list user questions and tests the reason for apparent inactivity on the list:

```
>i was wondering if anyone else has been without mail
>lately???? just wanted to see if i got this one, then
>i'll know the server is up.
>
>Date: Fri, 6 Aug 1999 17:34:50 -0400
>From: "mysfyt" <snip!>
>Subject: [mitnick] anyone else not getting anything???
```

In the following case, a user ponders a missing post. It was later determined that the original post was made to look like a reply (a petty example of spoofing).

```
>uh, i never got the original "[mitnick] OT: New Hotmail
>Hole Discovered I can't believe somuch fun!".. when did
>this start?
>
>Date: Sat, 11 Dec 1999 01:45:50 -0500
>From: "dangerz" <snip!>
>Subject: RE: [mitnick] OT: New Hotmail Hole Discovered I
>can't believe somuch fun!
[brackets surrounding "Mitnick" are original]
```

When users looked for a previous post for the original, there was none. This indicates that at least some users maintain personal archives for their own curiosity or research. This also indicates a form of communication that is more intentional than simply making immediate replies; however, there is also ample evidence on the list of hasty replies.

Execution of Communication

The prominence of computer mediated communication among hackers is reflected in the abundance of posts dealing specifically with the 1) language, 2) grammar, and 3) rhetorical effectiveness of messages. This finding comes with a warning; there are indications that some attacks on a user's grammar, command of the English language, or rhetorical skills are **trolls**. However, corrections were frequently made on the list.

Some list users contributed to the list from countries where English is not the native language. Although many such users were skilled writers of English, some failed to make themselves clear.

```
>This world is fucking!
>Why , I want to die?
>
>Date: Sun, 25 Apr 1999 20:46:03 +0600
>From: Fedor Ignatov <snip!>
>Subject: [mitnick] It's fucking world
```

This user from Russia, made no further posts to the list after considerable discussion and ridicule of his language skills. It should be noted that Kevin Mitnick has a following in Russia, Belarus, and Ukraine. One of Mitnick's former associates rebuked the list members who ridiculed Fedor.

```
>As soon as I saw this message, the first thing I did was
>examine the message headers. Guess what?! The originator
>is RUSSIAN. Perhaps that explains his less-than-ideal
>grip of the English language's complex syntax!
>
>Before any more of you go making fun of his syntax, I'd
>like to know: How many of YOU speak any Russian?
>
>Date: Sun, 25 Apr 1999 12:56:20 -0700
>From: "Susan Thunder" <snip!>
>Subject: Re: [mitnick] It's fucking world
```

Another user who attempted to defend a non-English speaker introduces the topic of rhetorical skills. rOTTEN was particular about clear expression of ideas and proper word choice.

```
On Tue, 20 Oct 1998, terje wrote:
>>no offense but you know what this was an offer of someone
>>who wants to help let them....why criticize their
>>language...i mean hell the english language
>>is one of the more obscure languages to learn.
>
>The English language is by no means "obscure".
>
>Date: Mon, 19 Oct 1998 23:37:10 -0700 (PDT)
>From: rOTTEN <snip!>
>Subject: Re: [mitnick] OT: Language and the Internet
```

In the following post, Colt makes a statement that is hard, if not impossible, to verify.

```

>On Thu, 17 Feb 2000, Colt wrote:
>>Pedophilia was at about the same rates as now I
>>believe.. may be wrong..
>
>I'm interested to know where you derive your conclusion.
>For I know as FACT that there is nary one Masters &
>Johnson pedophilia poll which was conducted in ancient
>Greece.
>
>Date: Thu, 17 Feb 2000 03:27:18 -0800 (PST)
>From: rOTTEN <snip!>
>Subject: Re: [mitnick] How about a new topic?
[ellipses original]

```

In many such cases rOTTEN debunked statements by list users. In an early post made by rOTTEN, he unilaterally claimed his role as "list cop." He took it upon himself to correct or ridicule spelling, grammar, and rhetorical error. rOTTEN explicitly took the role often assumed by prominent list members. Friends and former associates of Kevin Mitnick were extended this privilege on the Mitnick list. Mitnick's co-defendant, Lewis DePayne, also ridiculed users for their errors in grammar and rhetoric.

Unlike rOTTEN and DePayne, some experienced hackers tended to be gentler in their corrections. Elder or noteworthy hackers on the list often tried to correct younger hackers in matters of doctrine or expression.

```

>>And to give you an example of what "brain cells" are, my
>>IQ is higher than yours, I have tons of common sense, I
>>think logically, I have a lightning wit, I am street
>>smart, possess a keen library of general knowledge, I
>>type faster than you and I know how to spell.
>
>Naturally, this kind of criticism of others invites
>scrutiny of your e-mail.
>
>>IQ in and of itself doesn't tell much. If you have
>>aspirations of applying for membership in Mensa, they'll
>>soon be impressed by your knack for abject stupidity. IQ
>>score, like a college degree, doesn't tell much
>>about a person's intelligence anymore...I doubt it ever
>>did. I've known too many hi-scoring college educated
>>jackoffs to believe otherwise.
>
>That would be "high-scoring". :)
>
>Date: Fri, 30 Jul 1999 08:43:18 -0700

```

>From: "Ryan Russell" <snip!>
>Subject: Re: [mitnick] Why do we need to free Kevin again?

This comment is softened with both the prefacing statement "Naturally, this kind of criticism of others invites scrutiny of your e-mail" and the use of an **emoticon**. The element of enculturation found in corrections of communication helps distinguish them from pure flaming. Flaming and other standard practices of Internet communication found on the Mitnick list are described in more detail in the next section.

Internet Conventions

E-mail lists and **newsgroups** are similar technologies. Each acts as a conduit for communication among users (see Mann and Sutton, 1998). Newsgroups are older than the Internet, and have developed a unique culture with jargon and practices differing from other media. Much of the Internet culture is actually derived from newsgroup culture (Hafner & Lyon, 1996). This section presents the artifacts of the newsgroup culture, and E-mail artifacts found in the Mitnick list. To a lesser extent, other Internet devices played a roll in the Mitnick list. For instance Links to the World Wide Web are ubiquitous. The general term "Internet conventions" is used to acknowledge the general convergence of the hacker and Internet cultures in Internet hackers.

The most common expression of Internet culture on the Mitnick list is the **flame**. Flames encompass many subtle varieties of insult and verbal jab. Some users seek flame wars (protracted flaming) by using **trolls**. An obvious troll by rOTTEN caused extended debate on the list.

>Because it's physically impossible to get a toothbrush in
>your rectum. If it were possible, you could brush your
>teeth from the inside.
>
>Date: Thu, 7 Oct 1999 00:10:43 -0700 (PDT)
>From: rOTTEN <snip!>
>Subject: Re: [mitnick] more antihacker rhetoric

The following definition from the *New Hacker Dictionary* was posted without further comment.

troll /v.,n./

[From the Usenet group alt.folklore.urban] To utter a posting on Usenet designed to attract predictable responses or flames. Derives from the phrase "trolling for newbies" which in turn comes from mainstream "trolling", a style of fishing in which one trails bait through a likely spot hoping for a bite. The well-constructed troll is a post that induces lots of newbies and flammers to make themselves look even more clueless than they already do, while subtly conveying to the more savvy and experienced that it is in fact a deliberate troll. If you don't fall for the joke, you get to be in on it.
(Raymond, 1996, website) [note: Usenet maintains newsgroups]

This direct introduction of the newsgroup terms explicitly includes the Internet conventions in hacker activity. There are usually detached and a humorous qualities to flames. Although there is no way to tell exactly what a list user felt when he or she wrote a given message, flames on the list often have a humorous component of one-upmanship.

During protracted flame wars, flames can lose all pretense of humor and rely on gratuitous insults, sophomoric puns, and apparently pointless acts of defiance.

```
>also..i dont even know where this punctuation thing came
>from. are you saying all that b/c i use "b/c"? is it b/c
>i use ".."? wait..sorry.."..?". there..thats better.
>maybe i should consult you b4 writing a sentence. wait,
>am i allowed to use b4? get back to me on that one. now,
>as i said b4..shut the fuck up. we dont need ppl
>critisizing other ppl on this list. it isnt about you
>trying to insult me. as you said..you are making fun of
>my silly ass comment. GET THE HELL OFF THE LIST
>
>Date: Sun, 27 Sep 1998 14:35:47 EDT
>From: WyRmXx@<snip!>
>Subject: [mitnick] that fight with that guy..
```

In another flame war, a user continuously used the word "misteak" in place of mistake. It appeared to be a gratuitous act directed at the user's opponent. The user extended the

correction over several posts by explaining his or her need to get the authoritative spelling from a dictionary being used to hold up the broken leg of a bookcase.

As noted in the previous quote, flammers are often directed to continue their fight "off-list." In newsgroup culture, this is conducted through private E-mail. On the Mitnick list, there is evidence that fights are also continued through private E-mail (i.e. messages directed to the offending user rather than the list. This behavior recognizes the medium of the list and its appropriate use.

```
[quoting WyRmXx]
>>GET THE HELL OFF THE LIST
>
>The only connection between my being on this list and my
>sending you insulting email is the fact that I did the
>latter in response to your behavior on the list. You're
>into that disconnected rambling thing again.
>
>"Please don't shout, you're hurting my ears."
>
>Date: Sun, 27 Sep 1998 15:21:20 -0400 (EDT)
>From: Aaron Ball <snip!>
>Subject: NOT-[mitnick] Re: that fight with that guy..
[Original style of quotation changed for consistency;
quotation marks original]
```

By directing the fight off the list, the user acknowledges another Internet convention.

Aaron's message also reflects a second convention borrowed from IRC and newsgroups: the use of all capital letters for "shouting." Directing a user to stop shouting indicates irritation with their visually distracting use of capital letters or, perhaps, just their tone.

Newsgroups are defined by their purpose; for instance, a Mitnick newsgroup would deal primarily with Mitnick. When users violate the intention of the list, the user becomes subject to sanctions from the list. In some cases, sanctions can be avoided by posting with "off-topic" prominently in the subject line. This allows other users to determine if they want to read an off-topic post.

```
>Those of us who write off-topic posts to the mitnick list
```

```
>should at least keep the subject line up-to-date; better  
>yet, let's just let this die. This isn't even topic drift  
>-- the original post was completely irrelevant.  
>  
>Date: Wed, 25 Nov 1998 17:02:09 -0500 (EST)  
>From: "Aaron D. Ball" <snip!>  
>Subject: Re: non-[mitnick] what am i gonna do now?
```

It is clear from the common use of Internet conventions that the hackers on the Mitnick list are familiar with the Internet culture. Hacktivists, as a subcategory of Internet hackers are expected to act (i.e. communicate) in the idiom of the Internet. They are unlike old school hackers, who might be expected to communicate the idiom of programming (i.e. using programming syntax to express an idea to other people (Levy, 1984). They are also unlike the bedroom hackers, who might be expected to communicate in telephone company jargon and the **l33t sPeaK** of electronic bulletin board systems (BBS's). The communication activities of hackers both demonstrate activities of their subculture and help define the type of hacker.

Identity

It is relatively well known that things are not always as they appear on the Internet. The question of identity is fundamental to this dissertation. Shared identity as hackers, individual identity through the use of one or more aliases, and obfuscation of true identity are regularly addressed on the list. Further, the conceptualization of identity is a valid methodological question that should be posed in any research relying on Internet communications. List members participate in and discuss various methods of manipulating their identities. Methods include 1) stealing another's identity through spoofing, 2) a change of address or handle, 3) the use of multiple simultaneous identities 4) the use limited purpose identities.

Manipulation of identity is assisted by relatively anonymous free E-mail service. A variety of free service accounts are available to anyone with web access. The essential element of all of these services is free and unverified service. To obtain an account, the user need only submit possibly spurious personal information along with a username and password. This section examines applications of these technologies and techniques from the list.

Spoofing

A forged message was sent under the name of a list regular named koolwip. It is a simple matter to use someone else's name, but the impersonator also forged koolwip's return address. The content of the message was offensive and degraded koolwip. It was obvious that the spoofer wanted recognition. The list responded in several ways.

Some of the experienced computer users and administrators responded with bored disapproval.

```
>Maybe it's just my paranoid nature, but I suspect that
>koolwip didn't send that. It looks like the sort of
>juvenile thing my friends and I would have done (and in
>fact often did) to each other when I was about twelve.
>Giggle, delete, and move on is how I tend to respond to
>such things...
>
>Date: Mon, 21 Sep 1998 21:14:56 -0700
>From: Caliban Tiresias Darklock <snip!>
>Subject: Re: [mitnick] I AM A LAMER
```

Other list users stated that only a "**lamer**" would create such an obvious ploy for attention. Some explained the stunt.

```
>It is fairly obvious that Koolwip did not write this
>letter. Even if I weren't as knowledgeable about
>computers as I am, I think that I would pick up the fact
>that no one would insult themselves [sic] like that.
>Alright, so you want proof that no one cracked
>Koolwip's account? Fine. In comparing one of Koolwip's
>actual letters to the spoofed one, you will find that the
>mail servers are totally different. Also, the ESMTP id's
>are different...
```

>
>From: JediHamstr<snip!>
>Date: Tue, 22 Sep 1998 19:36:29 EDT
>Subject: [mitnick] E-mail Spoofing.....

Others examined the transmission information of the spoofed posts and traced the spoofer back to his original account.

>The mail is being spoofed from a interland.net domain.
>With more research we discover that interland.net is a
>web hosting and web site design firm based in Atlanta,
>Georgia. Now we also have the ip [sic] address for the
>spoofer, it is <snip!> [IP deleted for privacy].
>So this is most likely a private user, although it is
>almost certainly someone who maintains a page through
>[I]nterland. I highly doubt that anyone imature [sic]
>enough to spoof E-mail in this manner is also
>sophisticated enough to break into a web hosting company.
>So what we have here is a wannabe hacker who doesn't
>quite realize that changing the "from" address in his
>copy of Netscape is not an effective way to spoof E-mail.

>Date: Tue, 22 Sep 1998 22:12:10 -0700
>From: hugh field <snip!>
>Subject: [mitnick] Koolwhip's E-mail junk

Some users of the list railed against the statement first and then the spoofer. VlaD80's reaction is typical of the general list users. In this case, the spoofer used koolwip's name to make a racist and apparently self-depreciatory statement. The list turned on what was obviously a spoof with anger. Comments were clearly directed at the writer (spoofer) rather than the intended victim (i.e. koolwip).

>what kind of idiot says something like that... that
>offends me.
>
>Date: Mon, 21 Sep 1998 23:44:38 EDT
>From: VlaD80<snip!>
>Subject: Re: [mitnick] I AM A LAMER

Regardless of the orientation of writer, the spoofing was universally regarded as a negative act. It was an unskillful manipulation of the medium and it was pointless. Spoofing disrupts identity on the list because there is no convenient way to be sure that any given message is legitimate. Even the users who found koolwip's spoofer would

probably not recognize a spoofed message in the first place without some indication in the content.

Change of Address or Alias

In electronic communication, the difference of a single character can make an entirely new identity. With a large volume of communications traffic, many users rely on filters to selectively delete unwanted E-mail before the user sees it. Changing a single letter can invalidate a filter criterion and allow messages to pass. Single letters can also effect sort features used to examine archived messages. The addition of a typographic character like the tilda "~" at the beginning of a name can cause that name to appear before the letter "a" or the number "0" in a sort of messages by name while remaining perfectly intelligible to a human reader. This effect has been achieved on the list, but the intention was neither obvious nor explicitly stated.

Changing addresses and handles may be an unintentional side effect of changing the mechanics of communication. In this case, "Telephreak-a.k.a.-acidhak" shortens his handle by changing his account from acidhak@<snip!> to telephrk@<snip!>. This change allowed him to drop the cumbersome "-a.k.a.-acidhak." By making this change, he shortened his handle, but retained his identity. He also acted to preserve his identity by announcing the change to the list.

```
>this is my new email address (telephrk@<snip!>) i had
>to many problems with acidhak@<snip!>, just so no one
>thinks someone is imatating me.
>
>Date: Sat, 05 Dec 1998 15:31:46 PST
>From: "TelePhreak -" <snip!>
>Subject: [mitnick] New Email Address
[sic]
```

In other cases, the list user makes a change in service providers. In these such cases, the user usually retains significantly similar names. Here, Telephreak notifies the list of his change in service providers.

```
>just so everyone knows my new email address is
>telephrk<snip!> [New Service]
>telephrk<snip!> [Old Service] will still be alive,
>but i will be using this one more.
>
>Date: Wed, 20 Jan 1999 19:39:43 -0500
>From: "TelePhreak" telephrk<snip!> [Non-Hotmail Address]
>Subject: [mitnick] New Email Addy
```

Sorting the list by name reveals another effect that may obscure identity. When users change E-mail software, they usually re-enter their personal information. In some cases, users change small details in their data such as the capitalization of their name or handle. This, in effect, produces a minor change in identity. When intentionally different information is used, the user applies a basic form of multiple identities.

Multiple Identities

For a short time, a list user varied his or her handle with every post and thus, varied his or her apparent identity, but kept the same E-mail account. An examination of the archived contents of the list revealed that one account was associated with twenty four names. This fact was partially observed by another list member.

```
>Nice try, sport. Cruising my Trash Bin, I found these.
>
>From: electroMagnet <snip!>
>From: Stork <snip!>
>From: rice patty <snip!>
>From: Chef Botulism <snip!>
>From: "Mr. MoJo Risen" <snip!>
>From: schooner <snip!>
>From: TrailWays <snip!>
>From: skyking <snip!>
>From: Joshua <snip!>
>From: aGranRitmo <snip!>
>From: WhoreToCulture <snip!>
>
[note: all addresses are identical]
>Just offhand, I'd say you have an identity crisis.
```

```
>  
>Date: Sun, 29 Nov 1998 14:23:41 +1000  
>From: Reeza! <snip!>  
>Subject: Re: [mitnick] Wanna take a trip
```

Unlike spoofers, a user with multiple identities does not try to assume another person's identity. The user simply obscures his or her identity. In the case identified above, the user had maintained a stable name, but began to switch rapidly after insulting the list owner.

```
>What kind of Communist propaganda (bullshit) is this?  
>'Sorry to post something seemingly off-topic ', is an  
>understatement Emmanuel. Go home, manipulate yourself,  
>and play headgames on your dog.  
>  
>Date: Mon, 2 Nov 1998 19:20:44 -0800 (PST)  
>From: Rasta <snip!>  
>Subject: Re: [mitnick] election suggestion  
[The name Rasta does not appear in the list above, but  
belonged to the same user]
```

This message came as a reply to Emmanuel Goldstein's self described off-topic post about the general elections being held at that time.

Limited Purpose Identities

The fourth method to obscure identity is the use of a name for limited purposes. The list user maintains two subscriptions to the list with sufficient difference in the details such as service provider, name, handle, etc. that other list users will not connect the two. The existence of such devices is hard to determine from the list. However, one must question any list member who seems one dimension in his or her posts. If a user only seems to engage in flame wars, but never contribute to serious issues, it may be an indication of this device.

One of the most vicious flame wars on the list was conducted through a Yahoo™ account. The account may have been used by a list user holding a long-standing account under another name.

[quoting Support Services]
 >>So, this effectively serves to demonstrate to our
 >>audience at home that you really
 are full of shit, and
 >>ignorant as hell. That's why you do it under the cloak of
 >>anonymity... because you already realize you can't
 >>survive the cross-examination.
 >
 >I do it under the cloak of anonymity because you have
 >already been charged with various crimes of harassment. I
 >do not want to get involved in testifying in a State or
 >Federal court case if you choose to commit more crimes
 >against people you disagree with. Even John Littman
 >mentioned that you get a perverse (there's that word
 >again) "thrill" out of harassing people. Including
 >government agents. Especially when you are harassing them
 >while pretending to be Kevin Mitnick. OOPS! I forgot. You
 >don't want people to know that. Sorry.
 >
 >Date: Sat, 11 Sep 1999 18:03:13 -0700 (PDT)
 >From: thatsnone ofyourbusiness <beddiehaskell<snip!>>
 >Subject: [mitnick] Re: beddie hasskell ahead 2 rounds to
 >none
 [ellipses original]

I could not establish whether the beddiehaskell account had been active for a long period or if it had been created recently, but the user behind beddiehaskell had knowledge of the list content from far prior to the point he or she began posting.

>Louie's emails to this list have tried to ridicule people
 >for writing letters, and for holding national
 >demonstrations and demonstrations in other countries, and
 >for discussing the case with people who do not know much
 >about it. Usually he then writes something silly like the
 >list awaits your response as if he knows anything about
 >what the list wants.
 >
 >Date: Sun, 12 Sep 1999 09:09:15 -0700 (PDT)
 >From: thatsnone ofyourbusiness <beddiehaskell<snip!>>
 >Subject: Re: [mitnick] beddie hasskell ahead 3 rounds to
 >none

The periodic attacks on Support Services did not end until an identity was suggested for beddiehaskell. It was suggested that an insider to the case with a grievance over expert witness fees was attacking Support Services (a.k.a. Lewis Depayne--Mitnick's co-defendant).

The use of a limited purpose identity simply for the list is a similar manipulation of identity. Like previous limited purpose identities, this device is used to protect a user. There is no proof of this device on the list, but it is reasonable to assume that some aliases are not found in other E-mail lists or in other uses. This device would allow users to post to the list, squabble, and receive replies under a fabricated identity and maintain a relatively trouble-free and empty mailbox under their preferred identities.

Hacker Subculture

The hacker subculture is a complex mixture of elements. Several subcategories have emerged from the data. 1) The definition of hacker is debated. 2) There is also a debate about where ethical hacking ends and criminal hacking begins. 3) The word "scene" describes references to knowledge of prominent hackers, details of hacker history, or jargon of the hacker subculture. 4) The subculture also includes a distrust for large corporations and the government. 5) There is a body of fiction and literature common to the hacker subculture. 6) Finally, there is a style of interaction apparently designed to socialize young hackers. List user's participation in actions related to these concepts indicates their level of commitment to the hacker subculture.

Definition of Hacker

The Mitnick list continues the ongoing debate about the definition of hacker noted in Part I. An acceptable definition defies the simple statements that frequently frame the debate. In the following post, ACE responds to the improper use of the word "hacker" in a news story about the theft of an orbiting satellite.

```
>The truth is, there are people out there who would take
>control of satellites and such for their own malicious
>reasons, but they are in the minority. The term "hacker"
>used in popular form by the media is all enveloping,
>encasing actual hackers, crackers, crypto phreaks,
>phreakers, criminals, and extortionists of all kinds. This
```

>is wrong. Some of us commit crimes, yes, but thats not
>hacking. Or is it? What does MIT, the beginning of
>Hacking, defeine the word as? I know that yes, it may have
>come from the image of a writer "hacking" away at a
>typewriter creating a manuscript, but what does everyone
>else think? Will someone please help me out here? Or is it
>that this is just a pointless rant? We all use the word
>diffferently, but underneath, in my opinion we all have
>the same goal: knowledge.Newbie and elite alike, we all
>desire knowledge. Its been called, to quote someone (maybe
>E.G.) or other "The thirst for knowlege". This can be hard
>to explain to the media for obvious reasons. The media is
>afraid of us
>
>Date: Wed, 02 Jun 1999 02:25:02 -0400
>From: n/a <snip!>
>Subject: Re: [mitnick] An annoying quote
[*sic*, note: E.G. may refer to Emmanuel Goldstein]

ACE (n/a) uses the debated term as a rallying point for various members of the hacking subculture. However, in most cases the debate focused on the actions of a supposed hacker rather than an abstract debate of the word. In the following, Caliban responded to a post about a television commercial by IBM.

>[The hacker] was portrayed as being SURPRISED by his
>ability to get into the system -- as if he was just sort
>of bored and goofing off and thought he should go do
>something futile. The implication is apparently that
>hackers don't actually know what they're doing, just sort
>of mucking around to see what happens.he accessed data
>which -- while theoretically confidential -- he didn't
>actually do anything to, just distributed it. (This is
>actually, when viewed properly, somewhat positive. He
>COULD have been shown modifying or erasing important data,
>if they wanted to be really frightening.)
>
>Date: Thu, 31 Dec 1998 11:13:05 -0800
>From: "Caliban Tiresias Darklock" <snip!>
>Subject: [mitnick] IBM hacker ad

Caliban's closing statement indicates the hacker ethic and introduces the notion of hacker ethics--as presented in the list.

Ethics of Hacking

Like the debated definition of "hacker," participation in the debate of hacking ethics establishes connection to the hacker subculture while helping to define it. Posts

regarding the ethics of hacking found on the list include both actual events and hypothetical scenarios. In the following post, Emmanuel Goldstein answers Hardrock's distinction between criminal hacking and non-criminal hacking.

```
>On Wed, Dec 23, 1998 at 02:38:43PM -0800, Hardrock
>Llewynyth wrote:
>>it isn't "rude" it is theft.  even if you leave the
>>door wide open it is still theft.  saying that i
>>shouldn't have left the door open doesn't absolve the
>>thief from the crime.  it is merely the old "blame the
>>victim" game.
>
>in the real world, if you leave the door open to an office
>or a business and unauthorized people walk in, odds are
>you'll get yelled at or even fired for leaving the door
>open.  that doesn't happen when computers are involved -
>intruders are treated as if they had walked in, stolen
>everything, read everything, and burned everything.

[material omitted]

>i've wandered through everything from corporate offices to
>mental hospitals to government agencies in real life and
>the most that ever happened to me was that i got my name
>taken and got kicked out.  trespassing is a very very
>common occurrence so if we're going to make the analogy
>with computers, the penalties should also bear some
>resemblance.  right now they don't.  computer trespass is
>treated as if it were real life sabotage.  yet we continue
>to call it trespassing.  either we refer to every hacker as
>a saboteur or we start treating them as trespassers.  you
>just can't have it both ways.
>
>Date: Thu, 24 Dec 1998 15:21:57 -0500
>From: Emmanuel Goldstein <snip!>
>Subject: Re: [mitnick] on another note ..
[ellipses original]
```

Analogies play a prominent role in debates of the ethics of hacking. The following post deals with the aftermath of the defacement of the New York Times' website by Hackers For Girlies (HFG). Both list users in the exchange use analogies to explain their positions.

```
>On Thu, 24 Sep 1998, Caliban Tiresias Darklock wrote:
[material omitted]
>>But he has a valid point. Stealing people's resources
>>and web space *is* a violation of their rights and
>>freedoms, and if those people want to help Kevin Mitnick
```

>>they *should* be doing so through appropriate and *legal*
>>channels. Several of us on the list said effectively the
>>same thing.

[Original style of quotation changed for consistency]

>Err... no. What these attacks do, strictly, is add data
>to someone else's machine and move some files around --
>e.g., replacing your index.html with my index.html. So
>what they're doing is "causing unwanted operation" --
>which I'm pretty sure is illegal -- or at least some sort
>of metaphorical trespassing, but is in different ethical
>territory than stealing or destroying.

>

>It's perhaps similar to standing in front of a Nike
>billboard or storefront with signs protesting their
>policies.

[material omitted]

>It's ethically dubious to state that the NYT's "right" to
>have a web page up with stuff it wants all the time
>outweighs HFG's "right" to speak out about the NYT's (and
>the (media in general)'s) abuse of Kevin and hackers
>in general some of the time. I, for one, cheer on general
>principle when the little guy coopts the big guy's name
>recognition and pokes a hole in the uniformity of the
>media.

>

>Keep in mind that I said "ethically", not "legally",
>dubious. The two are not the same, and in the eyes of the
>law HFG is unambiguously a den of Bad Guys. The law,
>unfortunately, does not always coincide with moral truth.

>

>Date: Thu, 24 Sep 1998 17:33:40 -0400 (EDT)

>From: "Aaron D. Ball" <snip!>

>Subject: Re: [mitnick] The result from the HFG web page
>hack

Aaron's closing statement distinguishes the ethics of hacking from law. This is representative of a trend in list discussion marking hackers as moral actors rather than legal actors (Becker, 1963). Few hackers on the list express an unthinking adherence to the law except as a disclaimer after a statement appearing to condone an illegal activity. This conception of law and morally supports the distinction between criminal hacking and computer crime made in Part I. Moral actions (i.e. acceptable to the subculture) are condoned while immoral actions are simply criminal (Becker, 1963).

Scene

The scene is a miscellaneous category for references to inside information that establishes a connection with the hacker subculture. This may include bits of history, jargon, inside jokes, real world meetings (Cons) and hacker magazines ('zines). Before the Internet became part of the popular lexicon, the hacker subculture often used the word "underground" to describe these things. They were often referenced to exclude the uninitiated (Slatalla & Quittner, 1995). Today, the hacker scene is no longer underground; instead, it is readily available through websites and archives. The Cult of the Dead Cow maintains an archive of files that recall the days when the scene was underground (Psychotic Opposition, 1987).

```
>I got that from Cult of the Dead Cow:
>http://www.cultdeadcow.com/cDc_files/cDc-0021.txt
>
>Date: Thu, 31 Dec 1998 20:24:46 EST
>From: NegativZr0@<snip!>
>Subject: [mitnick] "the cold truth"
```

The archive itself has become part of the cannon of hacker reading and therefore, part of the scene. NegativZr0 acknowledges this fact by citing the source of a piece of hacker prose submitted to the list.

Other elements of the hacker scene include the monthly meetings organized by 2600 Magazine. They occur across the country at locations specified in 2600 magazine (usually mall food courts).

```
>In a message dated 12/3/98 1:59:32 PM Pacific Standard
>Time, FallOut4E@aol.com writes:
>>I agree with your suggestion, but I don't think the "MTV
>>crowd" are the ones we want to appeal to. They are the
>>same sort of crowd that goes to the mall every day to
>>hang out.
>
>Hey, wait..... i believe it was The Mentor (dare i drop
>the name?) who first stated that descrimination and bias
>(and the lack thereof) is what made hackers unique.... I
>am the "Mtv crowd". I dont watch Mtv, but I'm sure Im
```

```
>easily labeled an "Mtv watcher" or "Mallrat" (lets not
>forget that a lot of 2600 meetings are held in malls)
>I go to the mall, and I gurantee you, that you can walk
>into the arcade of your local mall, and meet people with
>interests in hacking...
>
>Date: Thu, 3 Dec 1998 18:57:01 EST
>From: SkyFireZ@<snip!> aka AcidRayne
>Subject: Re: [mitnick] bail
[sic, ellipses original]
```

AcidRayne also mentions the Mentor and The Hacker Manifesto (see Appendix B). The Mentor was a member of the premiere bedroom hacker group of the 1980's: the Legion of Doom (Sterling, 1992). Both references imply knowledge of the hacker scene.

Corporate and Government Distrust

Levy reports a distrust for government and administration among old school hackers (Levy, 1984). Bedroom hackers expressed various definitions of anarchy, but favored it in their writings and music (Psychotic Opposition, 1987). Distrust of the government is not a unique trait of hacktivists; it appears to be a consistent theme throughout the hacker subculture.

```
>Aaron D. Ball wrote:
>>It is our duty to do whatever we can within the legal
>>system, and to enlist the aid of our fellow citizens
>>through lawful action
>
>The "Legal system" is created only to further distance the
>rich from the poor. Equil representation, my ass. Just ask
>OJ if the rich and poor have equal rights under the United
>States System of Law. They do not. the rich do whatever
>they please. the HAVE the power, the money, and this
>government only applies to them.
>
>Date: Wed, 7 Oct 1998 21:02:23 EDT
>From: Antboy23<snip!>
>Subject: [mitnick] unalienable rights 2
```

Both Aaron and Antboy23 express dissatisfaction with government, but advocate different approaches to achieving change. Other list users express simple disillusion with

the system. Ironically, Che Guevara ends a post with a resigned assessment of domestic politics:

```
>looks like (sadly) that we've got ourselves an orwellian
>government, and theres nothing we can do about it
>
>Date: Thu, 08 Oct 1998 06:53:33 -0400
>From: che guevara <snip!>
>Subject: Re: [mitnick] unalienable rights
```

Feelings of distrust for the government often coincide with similar statements about large corporations.

In 1999, e-toys.com, a well-funded e-commerce company, sued a group of artists and hackers for maintaining a website at www.etoys.com. The artists had been using the site for two years before the etoys.com was incorporated. This was discussed in terms of a trend of large companies attempting to appropriate identity on the web (Goldstein & Skaletsky, 2000). Given the emphasis on identity in hacker interactions, it is not surprising that the general feelings of distrust for corporations became acute in the hacker community.

A list user was directly affected by a similar action. Shr0ud belonged to the "brotherhood of warez" who used velkro.net as their domain. Velkro is an obvious homophone of the trademark Velcro. Shr0ud posted the response of the brotherhood to a cease and desist letter from the makers of Velcro™.

```
>The Brotherhood of Warez vs. The Velcro Group

[material omitted]

>Well [attorney's name], I'm afraid we're not going to just
>give in that easily. Yes, we know you represent a large
>corporation. And of course, the big corporations always
>win. Even if it is the Velcro corporation. But that's
>certainly not going to stop us from trying.
>
>LET LOOSE THE DOGS OF WAR! BOO!
>
>Date: Thu, 9 Mar 2000 12:23:10 -0500 (EST)
```

```
>From: shr0ud <snip!>  
>Subject: [mitnick] FIGHT THE MAN!  
[original brackets omitted]
```

List members supported Shr0ud's fight by decrying the arrogance of large corporations.

Fiction and Literature

The fiction and literature consumed by hackers is often discussed on the list. It includes the movies hackers watch and the books they read. Similar to the scene, familiarity with certain works of fiction, particularly the Cyberpunk genre, demonstrates participation in the subculture. Both literature and fiction serve as the initial attraction for some hackers.

```
>Just another point about the "Takedown" movie.. Does  
>anyone think it will bring a new wave of wannabe hackers  
>onto the internet? If anyone remembers the movie  
>"Hackers", it brought in an enormous amount of zero cools  
>and acid burns.. or variations at least.. lol Does anyone  
>believe the "Takedown" movie will influence future Kevin  
>Mitnicks?  
>  
>Date: Thu, 17 Dec 1998 16:29:16 EST  
>From: Bob L Fraple <snip!>  
>Subject: [mitnick] misc..  
[Note: lol is an abbreviation of laughing out loud]
```

Another comment from a list user indicated that WarGames started his interested in hacking and phone phreaking. This indicates continuity in the role of fiction in the hacker subculture.

The act of hacking requires context to understand and appreciate. Beginning hackers may not be intuitively drawn to the puzzle of hacking the way old school hackers were. In part, the need for immediate gratification explains the disruptive and rude actions of script kiddies. The glamorization of hacking in fiction was noted on the list.

```
>no one has mentioned that the actualy act of hacking  
>looked more like a flight simulator, and the gibbon looked  
>more like a flashy light show.  
>  
>Date: Wed, 1 Sep 1999 23:07:22 +1000
```

>From: "Carlo" <snip!>
>Subject: Re: [mitnick] hackers (the actual hacking)

Carlo describes the movie Hackers, but WarGames and Sneakers also received criticism for inaccuracies. Other comments dealt with the apparent ease of hacking. In movies, everything is accomplished quickly.

>Don't get me wrong, I thoroughly enjoyed hackers... In
>fact, it fueled my interest in hacking more than anything
>else ever had. I was sure of the fact (from the beginning)
>however, that hacking wasn't how they portrayed it in the
>movie.
>
>Date: Thu, 17 Dec 1998 19:49:09 EST
>From: SkyFireZ@<snip!> aka AcidRayne
>Subject: Re: [mitnick] misc..

The combination of visual stimulation and apparent ease could serve to stimulate interest in hacking. Based on the comments of the list, media portrayals of hacking may be contributing to the masses of script kiddies being blamed for mayhem on the Internet (Lemos, 2000). Indication of a mechanism to socialize these youngsters was also found on the list.

Enculturation

Although there are notable cases of mentoring in the hacker subculture (Slatalla & Quittner, 1995; Sterling, 1992; Levy, 1984), the list does not provide any evidence of such close relationships. However, the list does provide evidence of a form of enculturation. Hacking is about exploration and discovery (Levy, 1984); experienced hackers on the list show little desire to deprive larval hackers of the opportunity to discover for themselves.

On Tue, 27 Oct 1998 RichardB3<snip!> wrote:
>>HI....it is on udp when i do a port scan i have run
>>in to port 23 with udp and i cant log in to it with my
>>telnet program can you tell me how i can log in to a udp
>>telnet?????????
>>thanx and im sorry to ask here but know one elss would
>>know.....

```
>
>No. This is not the place to ask.
>alt.2600 is significantly closer to the place to ask, but
>*please* just RTFRFC instead.
>Or search the web.
>Or learn Perl.
>
>Date: Tue, 27 Oct 1998 21:44:40 -0500 (EST)
>From: "Aaron D. Ball" <snip!>
>Subject: Re: [mitnick] a quick ? (off-subject)
[ellipses original]
```

RTFRFC is an adaptation of RTFM referring to a document called a Request For Comment (RFC). RTFM is a standard response to questions that could be answered by reading the manual. Aaron's response is typical of experienced list users. The Internet presents numerous opportunities to find information. Posting questions without attempting to find the information is disparaged on the list.

```
>TelePhreak . wrote:
>>i know this probably has been posted many times before
>>but can you please post the lists of actors.
>>(e.g: Actor - Person in real life)
>
>Lazy asshole. Open up your web browser and cruise the
>iMDB database. Then post the results to this list
>yourself.
>
>Date: Mon, 5 Oct 1998 17:41:23 -0700 (PDT)
>From: Support Services <snip!>
>Subject: Re: [mitnick] TakeDown Actors
```

The Internet Movie Database, is a relatively well-known resource. Even without specific knowledge of IMDB, a search for "cast" and "Takedown" on any major search engine would have answered his question.

Hacktivism

The final and most prominent category of posts to the Mitnick list is hacktivism. The frequency of hacktivist activity is expected on a mailing list devoted to freeing a prisoner. Ironically, the list predates the word hacktivism; Kevin Poulsen coined the word in 1998 to describe the actions of the Mitnick list.

>Post scriptum: FYI - Kevin Poulsen, a reformed computer
>hacker who now writes for ZDTV, Wired, etc. coined the
>phrase "Hacktivism".
>
>Date: Fri, 5 Feb 1999 11:30:34 -0800 (PST)
>From: rOTTEN <snip!>
>Subject: [mitnick] RE: Kevin Mitnick (fwd)

rOTTEN worked with Poulsen while the latter was restricted from using computers as a condition of supervised release related to a hacking conviction. Four hacktivist goals are the frequently addressed on the list: 1) to allow Mitnick supporters to exchange information, 2) to call attention to Mitnick's case, 3) to facilitate support for Mitnick, and 4) to correct misinformation about Mitnick.

Media Coverage

>I was just wondering. But has Kevin received any good
>media coverage at all?
>
>Date: Thu, 12 Nov 1998 13:46:18 -0700
>From: "Speckz.com's Abuse" <snip!>
>Subject: [mitnick] Media coverage
[note: abuse@... if often an open account for administrators
to receive complaints.]

List users often referred the list to popular media coverage of Mitnick's case. These posts typically gave a URL (web address) and sometimes included the text of the story. With a few exceptions, the reaction to the story was negative. Factual errors or a sensationalistic tone usually caused this reaction. In the following post, Emmanuel comments on the source of one of the most sensationalized errors printed about Mitnick.

>On Thu, Oct 01, 1998 at 10:59:52PM -0400, kerry wrote:
>>He isn't being charged with this. The media locks on to
>>it and can't seem to let it go though, because mentioning
>>stolen credit card numbers strikes fear in their readers
>>and makes em buy more newspapers. Saying Kevin was
>>"accused of possessing stolen credit card numbers" sounds
>>better to them than following that up with "1. Kevin
>>never used them, 2. a lot of other people had them too
>>and 3. they were old and had been around on the net for a
>>long time..."
>
>this mention of credit card numbers goes directly to the
>2/16/95 front page article by markoff where this was

>stated in the first paragraph. even i began to think kevin
>was up to something bad when i read that. however, if you
>read much further into the article, you would see that
>there was no indication or accusation that he had used any
>of them. putting that misleading item on the front page of
>the new york times is the biggest reason why that
>misperception has refused to die - hundreds of papers
>around the world just repeated what they saw in the times.
>most of them never bothered to mention the real truth.
>this is one element of the saga i don't think is very hard
>to blame squarely on markoff. by putting that in the first
>paragraph, he clearly was altering people's opinions
>without giving them the facts.
>
>Date: Fri, 2 Oct 1998 02:03:32 -0400
>From: Emmanuel Goldstein <snip!>
>Subject: Re: [mitnick] Mitnick Questions

His response illuminated a comment by Kerry, webmistress of the official Kevin Mitnick web page. She obtained and posted court documents and produced authoritative rebuttal of misinformation found in the press. The page, FreeKevin.com, became the primary source used by Mitnick's supporters to support their claims of injustice.

List users often reported writing to the author and/or editor of incorrect news stories that misrepresented Mitnick's record. Macki confronted a reporter from the Washington Post who wrote a story mentioning that Mitnick "will face trial here on charges that include stealing thousands of credit card numbers." (Emmanuel Goldstein quoting Rene Sanchez on 12/11/98) [an error of text duplication was deleted]."

>I just got off the phone with Rene Sanchez (the offending
>reporter at the Washington Post). It was a very
>insightfull half an hour, to say the least.
>
>Last things first, he admitted that the statment about
>Kevin (as printed) was false. He pledged to discuss making
>a correction in monday's paper with his editor.
>
>Basically, he said that since Kevin wasn't the focus of
>the article, he didn't feel the need to do any research
>beyond what the Federal Prosecutor's office said. He said
>"The clear sense that the Federal Prosecutor was giving
>me, was that the Credit Card numbers were part of it [the
>netcom part of the indictment]." But he wouldn't/couldn't
>quote exactly what Painter's office said.
>

>Date: Fri, 11 Dec 1998 20:46:18 -0500 (EST)
>From: Macki <snip!>
>Subject: [mitnick] Rene Sanchez.. Washington Post

It seemed that the error would be fixed, but the list was later informed that the editorial error was too minor to correct. Shortly thereafter, the story was republished in Macki's hometown newspaper.

>On Mon, Dec 14, 1998 at 05:53:29PM -0500, Macki wrote:
>
>>12-13-98: The San Jose Mercury News picks up the
>>Washington Post article and prints it complete with
>>inaccurate comments about Mitnick, much less
>>the fact that Peterson has already been caught.
>
>we can assume that this scenario has been repeated dozens,
>perhaps hundreds, of times as the washington post is often
>reprinted in papers all over the world. this may have even
>gone international through the herald tribune, which they
>co-publish. the post had an opportunity to make the
>correction. they chose not to and instead are allowing the
>original mistruths to propagate throughout the world.
>
>Date: Mon, 14 Dec 1998 18:54:15 -0500
>From: Emmanuel Goldstein <snip!>
>Subject: Re: [mitnick] news update

The propagation of error through failure of basic fact checking often drew list attention.

The list reacted most harshly to preventable errors like the Washington Post's error above.

Other examples of factual error confronted by the list include the charge that Mitnick was one of the FBI's ten most wanted. In fact, he was featured on a U.S. Marshall's wanted poster for leaving the area of his supervised release. It was later determined that he had not violated the terms of his supervised release and had not legally been a fugitive. The active role of the list in pursuing these errors marks the activity of hacktivists.

Grassroots Publicity

Geographic dispersion of the list members often worked against hacktivist goals. In several instances, members traveled hundreds of miles to gather a handful of protestors. Protests centered on major population centers. Los Angeles, where Mitnick was imprisoned, gathered protestors from as far as San Diego to support Mitnick at trial. Similarly, the New York Metropolitan area, home of 2600, gathered several protests.

```
>So what are the results of all the protests? Post some
>feedback here. The NY one went pretty well. We had
>probably more than 20 people. We handed out about 3000
>fliers to my estimates. A reporter from radio station WBAI
>was there. also a reporter from Forbes digital was there
>also. Many people were surprised to hear of this injustice
>in America, and others knew all too well about his plight.
>
>Date: Sat, 6 Jun 1998 02:14:26 -0500 (EST)
>From: icon <snip!>
>Subject: [mitnick] protest results
```

The protest of Miramax, distributor of the movie Takedown, is considered one of the most successful protests of the Free Kevin movement. The movie originally portrayed Mitnick as a violent sociopath; the script was rewritten with fewer liberties taken with Mitnick's character.

List members were not always able to attend protests. Many were underage or lacked the resources to travel to one of the protest sites. These list members reported other grassroots activities to the list. Some simply kept a tally of flier distributed.

```
>Well i'm now up to 7000 flyers, that i have handed out
>about KEVIN.
>
>Date: Mon, 16 Nov 1998 21:59:28 -0500
>From: "Scott" <snip!>
>Subject: Re: [mitnick]
```

Other reports involved convincing their high school teachers to learn more about Mitnick or overcoming a local mall's policy about distributing literature. After being ejected from the local mall, the Joplin Kansas 2600 meeting found a basis for their eventual return.

```
>Oh, and I forgot to mention while waiting for our ride we
>read the posted code of conduct. The only thing they can
>stop us for in the way of handing out flyers is if we're
>asking for money. It says something in the order of, 'No
>soliciting in the way of donations or purchase will be
>allowed' We weren't asking for donations. We were handing
>out the main, 2600 written flyer. other
>
>Date: Sun, 06 Jun 1999 03:07:24 -0500
>From: "Colt" <snip!>
>Subject: Re: [mitnick] Report: Joplin Meeting
[sic]
```

Interest in grassroots publicity did not end at the traditional methods of protests and distributing fliers.

List users invoked many untraditional methods to draw attention to Mitnick's case. The hallmark of hacktivism is use of the Internet to facilitate political protest. Most of the various attempts to gain publicity included URLs for the website. Unusual vehicles were found for the web site's message.

```
>it's official - we will have a skywriter at the nyc demo
>on 6/4. all of the new york metro area will be able to see
>the words 'free kevin' in the sky. assuming the weather
>holds up.
>
>Date: Tue, 25 May 1999 17:16:21 -0400
>From: Emmanuel Goldstein <snip!>
>Subject: [mitnick] exciting news for nyc
```

Stunts are not new to protest, but the availability of the Internet has changed the scale allowing grand gestures to carry more information (with a URL) and allowing minor gestures to be noticed by more people. Protestors have place stickers in unique places only visible to someone nearby. Images were then posted to the web site to draw interest. Russian hackers sent pictures of Soviet monuments enlisted to support Mitnick's cause. In one, a large scale Lenin in relief holds his hand up to Russians and displays a Free Kevin bumper sticker. In New York, the sticker campaign achieved sufficient notoriety

to appear in a nighttime drama. Hackers sent pictures of stickers on local landmarks and institutions.

```
>At 1:17 PM -0400 6/9/99, BadGirlnLA@aol.com wrote:
>>The NY hot dog vender picture with the guy under the
>>umbrella with the Free Kevin bumper sticker is an
>>outstanding picture.
>
>For refrence, that's actually a protester, not a vendor.
>The real vendor went out to pray, and left a protester in
>charge of his hot dog cart for "a few minutes" (turned out
>to be 20 minutes). No, we didn't take anything from the
>cart. Though three cokes were sold. See? One can trust a
>KM protester.
>
>Date: Wed, 9 Jun 1999 16:56:28 -0400
>From: Porkchop <snip!>
>Subject: Re: [mitnick] Mitnick Demo Pics
```

Traditional protest tactics mixed with the capacity for information delivery available on the Internet make hacktivists less dependent on mainstream media.

Support for Mitnick

The final topic in the hacktivism category pertains to efforts to assist Mitnick directly. His extended stay in pretrial detention left him with no income and fewer opportunities for institutional work than would normally be found in prison. Direct assistance for Mitnick was solicited by list members in regular contact with Mitnick.

```
>Kevin would greatly appreciate it if someone could send
>him any of the following soft cover books. These are all
>from O'Reilly and Associates:
>
>1) Java Script: The Definitive Guide, 3rd edition by David
>Flanagan
>2) HTML: The Definitive Guide, 3rd edition by Chuck
>Musciano and Bill Kennedy
>3) Practical C++ Programming by Steve Oualline
>
>There's a lot of material he's missed out on over the past
>four and a half years and he wants to learn as much as he
>can between now and the official date of his release:
>January 21, 2000. If you can send a copy of any of these
>books, please let the list know so that there aren't any
>duplicates. The address to mail the books is:
>
>Date: Wed, 22 Sep 1999 18:03:30 -0400
>From: Emmanuel Goldstein <snip!>
```

>Subject: [mitnick] kevin's request for books

List users could also donate money directly to Mitnick's prisoner account. A defense fund was established to help pay for Mitnick's representation. Proceeds from the sale of Free Kevin stickers went into this fund. A list user began to sell Free Kevin T-shirts and minor merchandise. The proceeds were promised to the defense fund. Another user established accounts with Internet advertisers. Each click of a banner ad on a web page maintained by the user would contribute five cents to the defense fund. In the following post, "press" refers to creating an impression count (i.e. clicking an ad).

```
>We can support kevin financially if you press some
>banners. He will get paided for that and the money orders
>will be send to his grandmother. When I know the url's you
>will get them from me.
>
>Date: Tue, 29 Sep 1998 08:33:26 +0200
>From: Hamburg Robbert <snip!>
Subject: [mitnick] Finacial support Kevin
```

Robert became a frequent poster as he alternately reminded people to go to the page or to only click once (multiple impressions by the same person would invalidate the earnings).

Conclusion

The primary conclusion of Part II is that consistent themes may be found in hacker communication. These themes can be quantified. From this basis, the analysis in Part III can proceed. The substantive findings of Part II offer insight into both the research of hackers and their specific activities.

Internet hackers tend to use on-line communication extensively. They are familiar with their chosen medium. More importantly, they are aware of the potential for manipulation of impressions on that medium. List users self-consciously manipulate the medium of the list (through its command structure). They conduct impression management (Goffman, 1959) by developing their communication skills. They also

recognize the intended function of various communication media available on the Internet. This fact presents a problem to researchers. Comprehending the intentional use of a medium also allows for the intentional misuse of it.

When assessing the motive of hackers, the capacity for gratuitous conflict should not be underestimated. The conduct of flame wars and trolling serve to indicate that the hacker subculture condones, but does not necessarily endorse attacks. Hackers tend to develop resistance to on-line attacks and may expect it of others. While there is evidence in the hacker ethic to refute the connection between hackers and web page defacements, there is also evidence that list users do not recognize on-line actions as being as serious as actions in real life (IRL). Actions like web page defacement are contextualized as simply changing the name of a file. Hackers, familiar with the vagaries of on-line identity, simply do not view attacks as seriously as businesses.

As demonstrated with the spoofing incident, it is possible to assume the identity of another list member, with varying degrees of success. It is a virtual certainty that someone will accept it, even if only temporarily. Any hacker communication should be considered questionable. Any research design requiring external verification of hacker's identity would also be questionable. Fortunately, the real life identities of list users are irrelevant to this dissertation.

The prominence of messages with a subcultural theme serve to strengthen the use of subculture in the definition of hacker derived in Part I. The findings of Part II show that subcultural elements are important to hacker on-line activities. the subculture also reveals that without a clear picture of moral rights to information and access to computer networks, we will continue to be forced to make ethical arguments based on imperfect

analogies. Among both security experts and hackers this debate has proven fruitless because it often devolves into a debate of the appropriateness of the analogy rather than the ethical or legal status of the action. By using subcultural values to define acceptable crime and unacceptable crime, the fruitless debate of what constitutes hacking may be discarded.

The prominence of hacktivism related messages further affirm the definition of the list users as hacktivists. The presence of various age groups on the list both indicates the broad appeal of hacktivism and helps define it as separate from other hacker types. Unrestrained youthful enthusiasm leads to a free-for-all atmosphere of petty rivalries and one-upmanship. Moderating list influences help restrain the bickering and maintain focus on Mitnick's case. Simultaneously, the younger list members keep the discussion lively and provide energy and enthusiasm.

Summary

To sum thus far, in Part I, the word 'hacker' and the term 'computer criminal' are defined through a typology. Based on that typology, it is clear that the users of the Mitnick list are predominantly Hacktivists, a sub-division of Internet Hackers. In Part II, I derive a list of the categories relevant to the interactions of this group of hackers. As mentioned in the conclusion, this list of categories comes with the important caveat that it applies to hacktivists, not necessarily hackers in general. In Part III, these categories will be quantified as constructs. A mathematical model will be developed to predict hacker competency, using these constructs as the independent, or predictor, variables.

Part III: Predicting Hacker Competency

Purpose

The third purpose of the dissertation is to develop and test a model that predicts "hacker competency" from the four constructs generated in Part II: communication, identity, subculture activities, and hactivism. The study tests the hypothesis that hacker competency can be predicted by the extent to which a hacker is involved in discussions with other hackers in each of these four areas. The theoretical rationale is that relatively greater membership involvement in a hacker subculture should be related to greater levels of hacking prowess.

Literature Review

Hollinger (1993) conducted a survey of undergraduates and their self-reported activities involving two kinds of computer crime: copyright infringement and unauthorized access. Hollinger's was the first reported study that applied quantitative methods to the problems of computer crime.

In a follow up study, Skinner and Fream (1997) expanded Hollinger's (1993) list of self-reported computer offenses. The results revealed correlations between social learning variables and computer crimes, indicating that certain social learning variables may predict hacker-like activities. Some of those variables may also be indicators of the effects of subculture. The present Part III elaborates upon that previous research and also extends Part II of this dissertation by using the constructs developed in Part II as indicators of a hacker subculture. In addition to Hollinger (1993) and Skinner and Fream (1997), the theories of subcultures (Becker, 1963; Cohen, 1955; Cloward & Ohlin, 1960) provide the theoretical rationale for the empirical analysis.

Theoretical Overview of the Four Constructs

Subcultural groups are known to define alternative goals that become equally or more rewarding to the membership than mainstream goals (Cohen, 1955; also, Merton, 1938). Furthermore, it is not necessary to be blocked from a dominant culture's prescribed goal, such as material success, to seek alternative status in a subculture (Agnew, 1991).

Communication and Identity

The *identity* and *communication* constructs both indicate participation in the hacker subculture. The medium of hacker interaction is electronic communication, and establishing identity establishes a hacker's membership and status within the subculture. Proficient communication is necessary to participate in the subculture, and, as reported in Part II, communication and identity are actively discussed and manipulated by hackers. Hackers' awareness of both identity and communication makes these variables mechanisms for establishing subculture.

Based on all of the above, subculture theory provides a theoretical foundation for the present model hypothesized to predict hacker competency from hactivist activities, subcultural elements such as attitudes and values, communication and identity. Subcultural theory can provide a meaningful context for interpreting the effects of these four variables on hacker competency.

Hactivist Activity

Becker (1963) suggested that an acceptable goal of the subculture may be questionable when viewed from the normative culture. For example, Hacktivists value political expression, a goal that is not overtly deviant but that displaces energy from the pursuit of goals in the normative culture (Ewald & Jiobu, 1985). The presence of the

Hactivist intent can be observed in the frequency of Hactivist activity on the Mitnick List, and the presence of such activity indicates investment in the hacker subculture.

Subcultural Activities

Cohen (1955) defined culture as commonly shared *beliefs, attitudes*, and knowledge perpetuated over time. These cultural characteristics are typically transmitted through interaction with other members of the culture--a process of enculturation that is important to existing members of the culture as well as to new members.

In deviant subcultures, neutralizing attitudes may be conveyed during enculturation. If the subculture exists in regular contact with a dominant culture, members may have difficulty operating in the dominant culture while also holding the *values* of the subculture. In the context of criminology, neutralizing attitudes (Sykes & Matza, 1957) allow the criminal to deny harm to the victim or to otherwise justify the criminal action. In the context of the hacker subculture, the denial of harm and appeal to higher motives, which are both neutralizing behaviors, are abundant in debates of the ethics of hacking. As reported in Part II, this was found to be evidence of subcultural effects. The attitudes and arguments necessary to operate with subcultural values within the dominant culture are part of the beliefs, knowledge, and attitudes communicated during enculturation.

Method

Four constructs were developed in Part II: communication, identity, hactivism and subculture activities. In Part III, these four constructs are operationalized as independent variables, or predictors, of "hacker competency."

Subjects

Selection of Subjects

The entire population of Mitnick List hackers who communicated between the dates of September 8, 1998 and January 8, 1999 were selected for this study. In all, the population was comprised of $N = 272$ subjects.

Demographics of Subjects

It is difficult or impossible to obtain reliable demographic information on hackers (Jordan and Taylor, 1998). First, many hackers are reluctant to grant face-to-face interviews with researchers or others, preferring to communicate electronically. Second, the development of the present prediction model relies on objective and direct observation of hacker activities, and those observations exist solely within computer networks where it is most difficult to obtain reliable demographics (Kendall, 1996). However, there is some available demographic information. Part II discovered that many Mitnick List users are high school students while other List users are well-know hackers, actively hacking since the early 1980's. Also, photographs made available through websites maintained by list users indicate several female List users.

Data Collection

Data were collected from the subjects' public domain accessible E-mail messages (Table 3). The conduct of this study using public domain data was approved by the human subjects Committee on Research and Integrity, Michigan State University, East Lansing, Michigan.

Variables

Dependent Variable

The dependent, or criterion, variable is "hacker competency," defined as the extent to which a hacker is technically skilled. The extent of hacker competency of each of the $N = 272$ hackers will be measured by the type of software program, also called "E-mail client" or simply "client," used by that hacker to send E-mail messages. Clients, such as Emacs, Microsoft Outlook and others, vary in the level of technical sophistication required for their configuration and use; greater numbers of options, configurations, and features require greater computer competencies.

For example, the America On-Line (AOL) TM provides little configuration flexibility because that software was designed for a general public not assumed to have extensive computer skills. At the other extreme, Unix clients have many features that offer great technical flexibility not provided by other clients; with more options, the user can manipulate the E-mail message in many ways, such as hiding one's identity from others; blocking unwanted E-mails, also called filtering; creating customized headers, and many others. There are over 200 types of clients used by List members, including each of their many updated versions (Appendix C).

Across the population of $N = 272$ hackers, 208 clients were used, each requiring greater or lesser levels of technical prowess. Standards of comparisons of technical sophistication of these clients was determined by two subject matter experts who independently evaluated the numbers and types of features, options, and configurations for each client. Cases of inconsistency were discussed and consensus was reached by the

two subject matter experts. There were only few inconsistent cases and consensus was reached for all of them.

Table 3 provides a list of the most commonly used clients across the subject population and the relative level of expertise required by each. Client sophistication was ordered on a Likert scale from one (less sophisticated)-to-five (most sophisticated; Table 3).

Table 3

E-mail Client and Level of Sophistication

Client	Sophistication
America-On-Line (AOL)	1
CompuServe	1
Microsoft Outlook	2
MS Exchange	2
Yahoo	3
Hotmail	3
Mozilla clients (except UNIX)	3
Eudora	4
Claris	4
Pine	5
Mozilla clients (X11, UNIX, Linux)	5

The dependent variable was measured as the value assigned to a hacker, based on the client used by that hacker. In cases where a hacker used more than one client, the value for the more sophisticated client was used. Thus, each of N = 272 hackers was assigned a

Likert scale value that measured the level of hacker competency, defined as the level of sophistication of client used by that hacker.

Independent Variables

Four constructs were developed in Part II. The first is *communication*: any E-mail message that referred to the style and method of communication among hackers. The second is *identity*: any message that referenced hacker's identity, such as attempting to conceal an identity. The third is *subcultural activities*: messages that referred to the subculture itself, such as discussion of ethics or the definition of a hacker. The fourth and final construct is *hactivism*: any discussions related to the purpose of the Mitnick List, such as discussion of Mitnick's court case or demonstrations to protest Mitnick's treatment.

In Part III, these four constructs were operationalized as independent variables. For each subject (i.e. hacker), the measure of each independent variable is the frequency posts in that topic. For example, if a hacker posted 15 references to communication (as described above), the total score for communication for that hacker would be 15. The other three constructs are operationalized the same way.

Procedure

The messages, sorted by construct in Part II, are associated with one or more of the four construct categories: communication, identity, hactivism, and subculture activity. For use in Part III, a database was created for each of these four categories; the database contained all messages that pertained to each category.

Using a customized program (Saxman, 2000) I converted each database from the Eudora file format to a text file usable in a spreadsheet program (See Appendix D). Next,

I wrote and implemented a procedure for Excel (Microsoft, 1997) that eliminated all fields in each of the four databases except for the user's name. The procedure also counted the number of times the user's name appeared in each category, that is, the number of times the user posted a message about that construct. The final database contained the following information: name of construct (communication, identity, hactivism, and subculture activity)³; names of users who posted messages pertaining to each constructs; and frequencies of posted messages by each user, for each construct (See Appendix E). The independent variable was operationalized as the sum total of the frequencies for each category, for each user.

Data Cleaning

The pilot study (Loper, 1998) revealed that it is possible for some users of the Mitnick E-mail list to hide their true transmittal information. To help ensure the integrity of the "hard data," the following analysis was performed on the entire database. The analysis matched the sender Internet Protocol (IP) address (when available), a unique identifier assigned to each computer on the Internet, with the sender name. Users posting under several names, but maintaining a single IP address were identified with this technique. Further analysis linked user names with multiple originating IP's. This allowed the matching of mobile users--people who use different computers in different locations--and permit cross-matching of IP addresses and sender names. Finally, entries for users with multiple names, but a single E-mail address were combined into a single entry. The final procedure was only necessary for users without an available IP address.

³ Although the database did not contain a field for this information, all entries in each of the four databases were associated with the corresponding construct.

Statistical Analysis

The analysis was performed using the Statistical Package for the Social Sciences (SPSS, 1996). Means, standard deviations, correlations and coefficient estimates of reliability were computed for all of the study variables and a mathematical model was developed by regressing measures of the dependent variable, hacker competency, on measures of the four independent variables. In a prediction model, the correlation coefficient is called a "validity" coefficient, and its' magnitude is an estimate of the extent to which the independent variables predict the dependent, criterion variable. Validity coefficients that range from .20-to-.30 provide evidence for the predictive validity of the model (Muchinsky, 1990). Thus, in this dissertation, a value approximating .20 or greater will provide evidence for the usefulness of a prediction model.

Results

Descriptive Statistics

Reliability estimates were not computed because there is no way to statistically compute reliability coefficients for the frequency data. However, the data were consistently generated across all four independent variables using the above described procedure and software that systematically generated and then summed the frequencies for each variable, i.e., category.

Table 4 presents the means, standard deviations, and correlations for the study variables. In Table 4, the means range from a low of 4.42, SD = 6.28 (identity) to a high of 13.08, SD = 15.56 (hactivism). The correlations between the dependent variable, hacker competency, and each of the independent variables were as follows: .24 (communication); .30 (identity); .32 (hactivism), and .35 (subculture activity).

Intercorrelations among the independent variables range from .42 (communication and

hactivism) to .8 (identity and communication). A high correlation was also observed for subculture activity and identity ($r = .74$).

Table 4

Descriptive Statistics and Correlations for Hacker Competency Prediction Model

	Mean	SD	1	2	3	4
1 Communication	13.00	22.50	1.00			
2 Identity	4.4	6.28	0.80	1.00		
3 Subculture	12.06	15.43	0.69	0.74	1.00	
4 Hactivism	13.08	15.56	0.42	0.47	0.67	1.00

Regression Analysis

The results of the *multiple regression* analysis for the model revealed an $R = .38$, however, the model was not statistically significant nor were any of four standardized beta weights for the four predictors: -.09 (communication), .15 (identity), .14 (hactivism), .21 (subculture activity). The results of *simple regressions* of hacker competency on each of the predictors was as follows: $r = .15$, $p < .05$ (communication); $r = .21$, $p < .05$ (identity); $r = .20$, $p < .01$ (hactivism); and $r = .21$, $p < .01$ (subculture). Thus, three of the simple regressions met the .20 criterion for predictive validity.

The above models were estimated using only cases for which there were no missing data: subjects were included only if data were included in each cell, i.e., for each of the four predictors. However, using these criteria considerably reduced the population to statistical samples. For the overall model there were only $n = 48$ List users; however, for the simple regressions, the sample sizes were larger ($n = 166$, communication; $n = 81$

identity; $n = 187$, hactivism; and $n = 159$, subculture), which explains the significant probability values for the simple regressions.

The lower sample size for the overall model also therefore explains the lack of statistical significance for this model ($r = .38$). However, a rule of thumb for sample sizes for prediction models is 10 subjects for every predictor in the model (Nunnally, 1978), a criterion that was met for the present regression model. This research was also designed with restrictive protocols for analysis. Future research with this data set will address the problems caused by excluding so many cases.

Clearly, this study did not result in a statistically significant result. However, when taken together, the overall results for the multiple regression model and the simple regressions, offer support for the hypothesis that the constructs developed in Part II and operationalized and tested in Part III predict "hacking competency."

Overall Discussion of the Triangulation: Parts I, II, and III

The hypothesized model and the simple regressions showed evidence for the prediction of "hacker competency" from four variables: communication, identity, hactivism, and subculture. The strongest predictors overall were subculture activity and hactivism. There was no contribution to the model(s) from communication and identity.

The above results suggest several points. First, the communication and identity variables are conceptually broader than both hactivism and subculture activities. It is therefore possible that a wider sampling of indicators of communication and identity would have provided incremental validity for those variables and thus for the model.

Another explanation for the study results is the relatively high correlations among some of the predictor variables and their relatively lower correlations with the dependent

variable. For example, the correlation between communication and identity was .80; the correlation between communication and subculture was .70; and the correlation between communication and the dependent variable was .23. When a variable correlates high with other variables in a model and relatively low with the dependent variable, as in this example, suppressor effects are suspect (Collins & Schmidt, 1997)--the result is an attenuated prediction model. The suppressor anomaly also explains why the validity coefficients for the simple regressions for hactivism and subculture met the .20 criterion for useful prediction.

A further contribution made by the research is the application of qualitative knowledge of hackers, acquired through immersion in the hacker subculture, from objective data provided by the hackers themselves. This qualitative information was represented in the four variables used in the prediction model.

This point is particularly relevant because hackers are notoriously resistant to attempts at research (Meeks, 2000; Jordan & Taylor, 1998). Some of the few successful studies of hackers used proxy hackers (i.e. students, see Skinner & Fream, 1998 or Hollinger, 1993) to achieve the type of data necessary to quantitatively study hacker-like activity. Most other successful studies of hackers relied solely on qualitative methods, particularly ethnography (see Sterling, 1992; Taylor, 1999, or Jordan & Taylor, 1998). The contribution this dissertation makes to the existing literature is the methods and procedures in objectifying real world data (versus surrogate student responses to questionnaires) and the integration through triangulation of qualitative and quantitative methods.

The model described in Part III applies specifically to the hacktivist subtype of Internet hacker. There is reason in Part II to believe that the all of the constructs except hacktivism may exist in similar or greater strength among other hacker types.

Substantive Findings

The foregoing analyses in Parts I, II, and III showed that the Mitnick List includes several components of subculture. First, the List users shared a sense of identity as hackers and this shared identity outside the presence of a dominant culture is what defines the hacker subculture.

Second, the List users had an articulated goal: assisting Kevin Mitnick. List users maintained order on the list--kept topics to the Mitnick subject, no infighting, etc.-- by appealing to the collective goal. Participation in the List's collective goal represents personal investments in the hacker subculture.

Third, the existence of the List in the first place was predicated on collective activities. Unlike off-line interactions, the hacker subculture cannot be sustained through a central location of the List members. The theme of communication is another mechanism of the hacker subculture.

Fifth, participation in the activities of the subculture identified members invested in the hacker subculture. Sykes and Matza (1957) conceptualize this kind of involvement as predictive of forming the neutralizing attitudes necessary to commit crime. In the hacker subculture, almost the opposite is true. Script kiddies, unsocialized as hackers, cannot seem to make the distinction between gratuitous damage and disruption (defined as computer crime in Part I) and the illegal acts condoned by the hacker subculture. Subcultural artifacts like the hacker ethic and the sense of exploration (rather than

destruction) for hackers are analogous to the neutralizing attitudes of delinquents. The enterprise of hacking is not per se criminal, but its conduct is predicated on having the proper understanding of its actions.

Limitations of the Study

That being said, there are limitations to using available data. There was no opportunity to query the Mitnick list users about particular topics; however, the pilot study revealed considerable reluctance to depart from their normal activities to address such questions. Further, the tendency of hackers to manipulate identity and message content, discovered in Part II, may render such E-mail interviews questionable at best. Further, there is reason to believe that such questions would violate a deeply held Internet convention against unsolicited commercial E-mail (i.e. **Spam**).

Another limitation of this method is that the researcher must rely on proxy measures. Using a hacker's choice of E-mail client as a measure of competency and therefore immersion in the subculture is not the optimal solution for construct validity. Other measures, discarded for problems with same source variance, included the overall frequency of posting. Frequency and Duration of posting indicates a level of interest, which corresponds to interest in hacking. Bloombecker states that many hackers achieve success by simply devoting exceptional amounts of time to their activities (1990). By operationalizing the independent variables as frequency of activities related to the constructs, issues of multicollinearity forced the removal of these variables from the model.

A further limitation of this design is that it requires considerable understanding of the hacker subculture. The detection of themes in conversation requires considerable

contextualization. The research design in this dissertation originally called for rating each message in terms of the category to which it belonged. It became apparent that there was no meaningful way to order such a scale for each subcategory.

Indications for Future Research

As noted above, Part III is limited by the lack of a valid instrument for the classification of hacker activities. Future research would profit from the creation of such a tool. If known hackers would consent to ordering the subtopics found in each of the four constructs used in Part III, a tool with known sample validity could be used to further distinguish predictive components of the model. Such a tool would have been invaluable to this study. Two measures of hacker competency were discarded because there were problem at the chosen unit of analysis (i.e. list user). If the unit of analysis could have been lowered to the individual message, the two measures could have been retained.

Validity studies of the constructs presented here present an opportunity to further develop this prediction model. Factor analysis would be able to discriminate between existing subcategories based on their predictive value to the model.

A useful continuation of this research would expand the analysis to include other types of hackers. At present, there is only speculation that the constructs predictive of hacker competence apply to other types. The aforementioned H2K list presents a group of Internet hackers. Internet Relay Chat (IRC) presents a good probability of finding script kiddies. The latter would also require establishing a measure of competence beyond the mail client. Duration and frequency may be the preferred measures; other measures might be more profitable. Part I presents that greatest immediate application of

this research to law enforcement and researchers interested in hackers, but only one of the types has been explored. A replication of these results in another type would greatly expand the external validity of this study.

Finally, almost all hacker subcultural activities are on-line. This dissertation showed one way those data can be tapped to provide useful information to further research and advance science in the area of computer technology, hackers, and computer crimes.

Policy Implications

Coutorie (1995) discovered a growing disparity between the knowledge of law enforcement and hackers. Since Coutorie's study, the Justice Department has initiated the two following attempts to address this growing gap in technical expertise. The first strategy involves attempts to increase the technical competence of its agents. The second strategy is a sustained lobbying effort with the intent to broaden existing powers and create new powers to address computer crime. This research has implications for both of these strategies.

Increasing Law Enforcement Computer Competency

While Coutorie's experts predicted an insurmountable gap between law enforcement knowledge and that of hackers, the findings of this dissertation indicate that the most common cause of damage by hackers are the least proficient members of the subculture (i.e. script kiddies and larval hackers). Thus, comparisons between the knowledge of elite hackers (old school, bedroom, or Internet) are inappropriate for the vast majority of law enforcement interaction with hackers.

A recent survey of federal computer assets by the General Account Office concluded that training for all federal information workers was the best defense against intrusion. The most notable vulnerability found in the GAO survey was the willingness of federal employees to share their passwords with convincing strangers on the telephone. The lack of technical sophistication associated with such **social engineering** attacks (Frank, 2000), does not support the conclusion the growing technical gap is insurmountable in the most common vulnerabilities found. However, this fact is lost if hackers are assumed to be a single group represented by their most elite members.

Further research is needed to establish the activities of types of hackers other than hacktivists, but Part I notes that the hacker ethic is a component of the hacker subculture that is common to all hackers. The findings of Part III indicate that technical competence (i.e. the potential to cause damage) is associated with immersion in the hacker subculture and its values. Therefore, the best conclusion available from this dissertation is that the most highly skilled hackers are not generally the concern of law enforcement. Even if law enforcement training does not meet the standard of the most skilled hackers, it can be sufficient.

Law Enforcement Lobbying for Expanded Powers

Based on the limited information available on hackers, many "worst case scenarios" and hyperbole have been allowed to guide policy. Laws have become draconian and subject to gross misinterpretation in an effort to eliminate illegal hacking and protect vital data structures. In Congressional hearing held during the final days of this dissertation, the American Civil Liberties Union issued another challenge to the latest attempt by law enforcement to come to grips with the computer crime problem.

computer running specialized software -- is attached to an Internet Service Provider's network and searches through all of its customers' electronic messages (including email, web addresses and instant messages) looking for the messages of a person suspected of a crime.

The new system comes at a time of record wiretapping by federal law enforcement. In the last reporting period, Steinhardt said, the Clinton Administration conducted more wiretaps in one year than had ever been conducted before. [ACLU, 2000c]

The Carnivore debate follows a similar debate on the Electronic Communications Privacy Act of 2000 (ECPA); in turn, this follows the Child On-line Protection Act (COPA). The list is extensive (see ACLU, 2000b). In asking Congress for the powers contained in this legislation, the Department of Justice (DOJ) has been unable to provide a clear definition of the problem to be addressed.

The position put forward by the DOJ relies on progressively intrusive methods to combat computer crime. The ACLU indicates that these uncoordinated imperatives erode personal protections with no clearly articulated purpose or support. The most troubling aspect of this legislation is that there is no clear understanding of how it will help combat computer crime. In response to recommendations found in the DOJ's Report by the President's Working Group on Unlawful Conduct on the Internet:

The report contains virtually no statistics on the extent of computer-related crime, or whether such activity poses a truly significant threat to our nation. Instead, the report merely mentions several anecdotes on how a few individuals have used the computers to commit crimes. Such statistics should be disclosed before any statutory changes are even considered. [ACLU, 2000a]

This passage recalls the research problem of Part I. The lack of statistics is due to the lack of a definition of computer crime. The DOJ relies on the threat of hackers to propel legislation, but cannot discern a hacker from any other Internet user. The results of Part I present a theoretically consistent definition of hacker. This definition can serve as the

basis for meaningful and generalizable study of hackers. Such study would address the short comings indicated by the ACLU.

Clearly, there is evidence of computer crime (Barrett, 1997; Icove, Seger, & VonStorch, 1995). One problem in addressing such crime under existing law is that it can be exceedingly hard to prove financial gain (the basis of sentencing laws) when hackers seek esoteric rewards associated with their subculture rather than convention society's goals. Without clear attempts at financial gain, sentencing guidelines offer little punishment for hacker actions that are perceived as very threatening (e.g. the worst case scenario of hacking military control systems). The Computer Fraud and Abuse Act of 1986 addressed this perceived threat by assessing additional punishment for intrusions on federal interest computers.

In cases like that of Kevin Mitnick, involving no federal interest computers, the prosecution has been forced to rely of excessive estimates of damage to achieve what they consider appropriate levels of sanction (Browne, 1999). David Banisar (1999) of the Electronic Privacy Information Center (EPIC) criticized the general willingness of federal prosecutors to depart from the proportionality of punishment to actual damage in computer related cases. "Like many other crimes, there are a lot of technical violations of the law that should be stopped by other means," Banisar says. "If everyone was stopped for driving one mile an hour over the speed limit, we'd have a police state." Crimes defined by federal statute have corresponding sentencing guidelines. Both depict the intent of the creators of that statute.

The combination of expansion of powers and obvious manipulation of the intent of law presents critics of the Justice Department with opportunities for attack.

The Justice Department, the FBI, the Department of Defense and the National Security Agency are asking for increased budgets to fight cyber crime and defend against "infowar" despite the fact that fewer than one-fourth of such cases brought to federal authorities are eventually prosecuted. Critics say the feds are engaged in empire building, using a perceived threat to build new programs and extend the reach of their agencies. Critics cite February 1998, when the Pentagon suffered what Deputy Defense Secretary John Hamre called the most intense cyberattack the Pentagon had seen to date. Even after it was shown that the attacks were pulled off by an Israeli 18-year-old and two California teenagers using a widely known flaw in a computer operating system, Hamre managed to convince Congress to appropriate more funds to fight cyberterrorism. [Martinez, 1999]

Both EPIC and the ACLU have also expressed deep reservations about the DOJ's legislative agenda. The DOJ's claims that new powers requested will be exercised in good faith without external oversight or statutory controls. EPIC and the ACLU have implied that their members doubt these claims. The hyperbole and worst case scenarios that form the impetus for this legislative action have discredited the DOJ. Technology and civil rights groups have found common cause in opposing numerous ill-conceived efforts to address hackers and computer crime.

Any action resulting from the DOJ lobbying will address the myth, not the fact, of the hacker subculture. This research replaces the hacker myth with substance and verifiable measures of hacker activities. Further, this research shows a predictive relationship between these activities and the competency of hackers. Thus, it could act as the foundation of more specifically tailored lobbying efforts by the DOJ. In spite of Martinez's claim of empire building, it seems more likely that the DOJ has simply lacked theoretical tools of sufficient precision to combat computer crime and malicious hacking while safeguarding the rights of other computer users. By adapting a strategy more closely designed to combat a verifiable foe in the DOJ lobbying strategy, the courts

would also be able to uphold more tightly construed laws in the face of challenges by civil liberties groups.

An example of a strategy derived from the findings of this dissertation allows for punishment based on the actual harm done and a realistic estimate of potential harm. The current DOJ strategy is to vigorously pursue all noteworthy hacking cases regardless of actual damages. The first proposed strategy would include lobbying for flexible statutory punishments tailored to the actual harm caused. Thus, if a computer intruder achieved access to a system, but caused only inconvenience (e.g. defacing a web page) the punishment would be proportionate. When defacing a web page, the intruder has the option of saving the original and making it available through a link or deleting it entirely. Without backup copies of the page, deletion could be much more costly. The lack of harm caused by a hacker can help establish the hacker's adherence to subcultural values. Deletion of the page would indicate a malicious computer criminal. While both are crimes, these actions are different in both intent and consequences for the target company. A malicious intruder with access could cause greater harm. A hacker with evidence of subcultural values is less likely to cause significant harm. The punishment could be designed to fit the crime.

Conclusion

The dissertation provides a needed addition to the substantive literature on hackers by formally defining the word and distinguishing the concept from computer crime in general. The development of activity profiles from direct field observation complements the existing literature derived from interviews. The demonstrated predictive

power of a model based on these activity profiles provides a sound empirical basis from which to pursue further research on hackers.

GLOSSARY

Addy: A colloquialism for "address." This is often used in reference to an E-mail address, but can be used with hardware addresses.

ADSL (Asymmetric Digital Subscriber Line): Digital service over twisted **copper wire pair** (common telephone wire). Asymmetric data flow rates are determined by the line service provider. The downstream (from Internet service provider to customer) data rates can be as high as allowed by the technology which depends on the distance from the telephone company's central office. The upstream data transfer rates are determined by the line service provider. A variant called **DSL** has matched up stream and down stream data flow rates. The slow upstream speed makes ADSL less desirable for web serves with frequent hits. ADSL/DSL service is not available to customers more than 23,000 "copper feet" from the central office (see **switching office**). At 23,000 feet of wire, a repeater is inserted in the phone cable to boost signal strength. This disrupts ADSL/DSL service.

ANA (Automatic Number Announcement): A service provided for phone repair technicians. Telephone wire pairs (see **copper wire pair**) are not usually clearly marked. If a field technician is not sure which line he or she has isolated, the technician can call an ANA number at the local exchange and it will announce the number of the line. This service replaces a previous procedure that required the technician to ring an operator and ask which line pair he or she was using. See also **ANAC**.

ANAC (Automated Number Announcement Circuit): ANAC is used to implement **ANA**. It can be used to identify a **copper wire pair** by a technician. When called, an automatic

voice will read back the calling number. The ANAC number is typically 970, 114, 211, 958, 511, or 9580. Note 9581 will disconnect service for several minutes.

ANI (Automatic Number Identification): Passes information about the caller to the switch to allow for easier billing and value added services like caller ID.

ASCII Art: text characters used to draw a picture in a text-based environment like E-mail. ASCII art is related to **emoticons**. An example of ASCII art is this arrow: ==>.

The name "ASCII art" refers to the American Standard Code for Information Interchange defined characters. ASCII art can also be extensive.

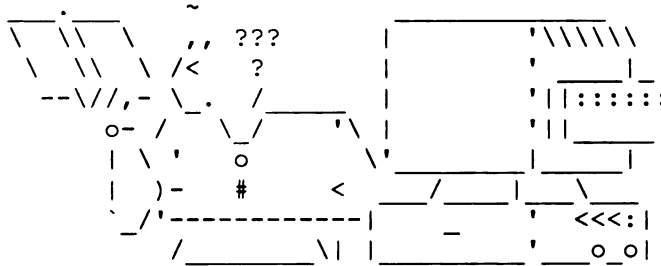


Figure 2. An example of ASCII art

Bandwidth: describes the capacity of a medium to convey data. High-bandwidth connections can carry a large amount of data. Because data travels in **packets**, the ability to carry many packets increases the apparent "speed" of a transfer; however all packets travel at the same speed (nearly the speed of light). Fewer packets moving at the same speed decreased the apparent speed of the transfer. For more see **Fiber Optic, T-1, DSL, ADSL, Modem**.

BBS (Bulletin Board System): A system of files available for transfer via telephone.

BBS's were the primary conduit for hacker communication in the 1980s. Messages for other BBS users could be left in their accounts as text files.

Bit: a single datum. It is either on or off. Bits are usually represented as 0 or 1, but this notation is arbitrary. Bits may be expressed in any medium capable of conveying binary data, but are most closely associated with electrical states.

Blue Box: A device used to produce a 2600hz tone (see **DTMF**). This tone was the default tone carried on long distance trunks. The presence of this tone tells alerts switching equipment that the line may be reassigned to another call. It also terminated the call at the distant switch. However, the local switch has not registered a user hanging up (which normally causes the 2600hz tone). With access at the local switch charged to an 800 number, the phone phreak can use **DTMF** commands to route long distance calls. The blue box works by erroneously telling a distant exchange that one party has hung up. Since this is not the case, the user of the blue box is left with an open line for about ten seconds. During this time a control sequence and new number can be dialed and still billed as if it were the original call. The original call is obviously made to a toll free number or intra-LATA. The only requisite is that the line be via a trunk connecting the central offices to a class 3 office or another central office.

Bridge: A bridge joins two **local area networks** (LANs). A bridge is a physical device that works at the data link layer of the **OSI 7-Layer Model**. Since a bridge works at the data link layer, the two networks joined must use the same protocol (e.g. **Ethernet**, **Token-Ring**). Bridges pass **frames** in a single path; thus, it does not need to be configured with tables as with routers. A similar device functions as both a router and a bridge thus, connecting two or more LANs with an extranet or the Internet. This device, a **brouter**, uses configuration tables.

Byte: An archaic term for a grouping of eight bits. This grouping is no longer universally significant as a grouping of bits. A significant grouping of bits is generically referred to as a word or an X-bit word. The term **octet** is now more common than byte. A byte is also accurately described as an 8-bit word.

Client: A client is either software or a computer that receives services from a **server**.

The status of client or server is not necessarily predetermined. For instance, a **web server** can act as a client for a database server. That web server may simultaneously provide service for client systems using web **browsers**. Desktop PCs will usually act as clients, but are capable of providing services. Personal web servers, remote access utilities like **BO2K** or PC Anywhere can allow desktop PCs act as servers. See also **server**.

Daemon: In UNIX, daemons are independent processes that service user requests.

Daemons are named after the service they provide. For instance, **File Transfer Protocol (FTP)** is serviced by **ftpd**. The "d" is added to denote the process is a daemon, not the service. When the file transfer protocol is needed, the **ftpd** starts a new process.

Decimal Dot Notation: Internet addresses are composed of 32-bit words. These words are often translated into four 8-bit segments to make human interpretation easier. The 8-bit segments are separated by "dots." The 8-bit segment is also converted from binary to decimal notation. The product is a four-segment, human-readable, Internet Address (i.e. **XXX.XXX.XXX.XXX**). Since each segment has eight bits, the maximum value of any segment is 256 unique combinations. However, counting in computer science usually starts with zero; thus, the range of values is 0-255.

DeCSS (Decode Content Scrambling System): DVD uses a security method called the Content Scrambling System (CSS). CSS is a form of data encryption used to discourage reading media files directly from the disc without a decryption key. The DeCSS utility emulates a software DVD player but instead of displaying the video and audio to screen, it simply saves it back to the disk without encryption, since there is no encryption in playback. A Norwegian group: Masters of Reverse Engineering (MoRE) discovered that one of the decryption software's licensees that makes a DVD player known as Xing DVD did not encrypt its key for decrypting DVDs. Because of this mistake these Norwegian programmers were able to create the DeCSS utility. DeCSS is a tiny program (60 KB). Reports that DeCSS facilitates copying of DVD are erroneous. DVDs can be conveniently copied without decrypting them. Adapted from

<http://www.pzcommunications.com/decss/what.htm>

DNR (Dial Number Recorder): see **pen register**

DSL (Digital Subscriber Line): Digital service over twisted copper wire pair (common telephone wire). Unlike **ADSL**, DSL has matched up stream and down stream data flow rates. The symmetric data flow makes DSL more appropriate for moderately busy web servers than ISDN or ADSL. Given full access to **bandwidth**, DSL lines are comparable to **T-1** lines. ADSL/DSL service is not available to customers more than 23,000 "copper feet" from the central office (see **switching office**). At 23,000 feet of wire, a repeater is inserted in the phone cable to boost signal strength. This disrupts ADSL/DSL service.

E-mail Client: Software that allows a computer to send and receive E-mail with a **server**. Examples include Microsoft Outlook™, Eudora™, and Pine.

Emoticons: characters used to express emotion in text-based communication. Perhaps the most familiar emoticon is the ":-)" happy face on its side. This is often used to denote a joking tone in preceding text. Although not technically emoticons, the practice of denoting actions with a pair of asterisks is also common. For examples *smiles* may be also be used to denote a joking tone.

Firewall: a hardware or software device designed to filter potentially dangerous packets on a network. Filtering criteria may be specified in the firewall's configuration.

Firewalls are often used to exclude packets directed to uncommon **ports** or from specified addresses. Firewalls can also validate the proper length or format of a packet to prevent attacks such as the "ping of death."

Frame Relay: A **bandwidth** division technique that allows users to borrow unused bandwidth from other users. Most pricing schemes include a guaranteed minimum bandwidth with the ability to share an equal portion of other's unused bandwidth. This excess bandwidth can be reclaimed by the original allocated user if needed, but otherwise is assigned to a pool for all other users to share.

Frameset or Frame: Each telephone is connected to a **copper wire pair**. This wire pair completes a circuit at the central office (see **switching office**) or **PBX** when the receiver is lifted. Wire pairs are grouped into cables that lead to the central office. At the central office the cable is broken back into its wire pairs for switching. The frame allows each wire pair to be clearly identified and switched to connect to others. Diagnostics can be performed on individual wire pairs through the frame. Wiretaps can also be attached to wire pairs at the frame. Distinguish from **Frame Relay**.

Host: A host is a named computer on a **TCP/IP** network. All current hosts (as of 2000) are uniquely named using **IPv4**. Private networks use unique internal IPv4 names described in **RFC 1918**; otherwise, each legal host has an IP address not shared by any other computer with direct access to the Internet. If a computer uses **PPP** to connect to the Internet via telephone, it becomes a host with a unique **IP** for the duration of its connection. All hosts are **nodes**, but not all nodes are hosts. Since all hosts are nodes, they can, by definition, connect to other nodes. Thus the computer serving the PPP connection is a host and the client connecting through the PPP server is also a host.

IP (Internet Address): The generic term "IP" refers to a unique identifying "**decimal dot name**" for any **node** on the Internet. Under **IPv4**, Internet addresses are expressed as a 32-bit number. These are often translated to the decimal dot notation to make them more readable by humans. Thus, IP's are often seen as XXX.XXX.XXX.XXX, where XXX is a decimal value between 0 and 255, inclusively (e.g. 35.2.3.190). Internet addresses are not reserved for **hosts** only. Routing equipment and communications infrastructure can be assigned IP's (see **router**).

IPv4 (Internet Protocol version 4): IPv4 is the most common version of Internet Protocol in use as of the year 2000. IPv4 uses a 32-bit network address, which can only support 4.3 billion unique addresses. Although this appears to be enough for years to come, the allocation of those addresses is not efficient. Large blocks are assigned to companies but not used in anticipation of later expansion. The practice of **sub-netting** makes this form of allocation more desirable than efficient allocation. For contrast, a new standard (IPv6) uses a 128-bit network address to maintain efficient routing through sub-netting and continue to current allocation schemes. (see also **decimal dot notation**)

IRC (Internet Relay Chat): A real-time, text-based message system divided into channels. Each channel is usually associated with a topic. Users can post new messages or reply to threads (i.e. strings of related messages). IRC is commonly presented on the well-known **port 194 TCP / 194 UDP**.

ISP (Internet Service Provider): ISPs range from the owners of the Internet **backbones** to small resellers of Internet service. The backbone owners are: ANS, ATMnet, BBNplanet, Compuserve, CRL, CWIX, DataXchange, DIGEX, Epoch, GetNet, GlobalCenter, GoodNet, GridNet, IBM, Interconnect, InternetMCI, iSTAR, NapNet, Netrail, NFS, PsiNet, Savvis, Sprint, and UUNET (Source, Boardwatch special Internet directory edition). ISPs buy bandwidth from these companies and sell connectivity to consumer or other ISPs. Most ISPs provide dial-up access for consumers and businesses. Internet services typically includes **E-mail**, Web space, **FTP** (File Transfer Protocol), **IRC** (Internet Relay Chat), and others as determined by the company. Value added ISP's like America On-line also provide content in the form of special news or chat services for members only.

l33t sPeaK: the dialect of hackers and phone phreaks. Numbers are substituted for visually similar letters. Capitol letters are freely and randomly used. For instance, 'elite hackers' became 31337 HaXorZ. Letter substitutions are common like z for s or especially k for c. **ASCII** characters and typographic symbols are also used, for example, H@xOr. Even the name of this dialect is a visual pun; the lowercase "l" in l33t sPeaK is the visually indistinguishable number 1.

Lamer: a derogatory term for an unskilled hacker. Lamer is often associated with script kiddies and larval hackers.

LATA (Local Access Transport Area): Local, toll, calling area. This extends beyond the United State's standard toll free calling (local) area, but is not considered long distance. **The Modified Final Judgement of 1984** divided the country into 184 LATAs. LATAs are roughly equated with area codes. Growth in metropolitan areas has caused some LATAs to serve multiple area codes. In 1984, long distance companies were only allowed to service interLATA calls. IntraLATA calls were handled by RBOCs. **The Telecommunications Reform Act of 1996** allows long distance carriers to enter the IntraLATA service market.

Man-in-the-middle Attack: The man in the middle attack relies on the interception of an encryption key during initial exchanges between users of a secure communication mechanism.

Media Access Control (MAC) address: The MAC address is a hardware identifier built into a **network interface card (NIC)**. MAC addresses are unique. A portion of each MAC identifies the manufacturer. In many cases, the MAC address is the most reliable identification of a networked computer. I have heard of NICs that allow configuration with DIP switches on the card, but I have never seen one.

Modified Final Judgement of 1984: The settlement of an anti-trust suit brought against AT&T. The 1984 MFJ was entered August 24, 1984. It modified the Final Judgement of 1954. The MFJ detailed the divestiture of the RBOC's by AT&T. The MFJ also produced deregulation of long distance rates.

Network Interface Card (NIC): A NIC is a hardware device that allows a computer to connect to a local area network or to another computer. NICs can utilize many different

physical media (e.g. twisted pair, coaxial cable, fiber optic, radio, etc.). NICs are often used to maintain persistent connections unlike **PPP** connections.

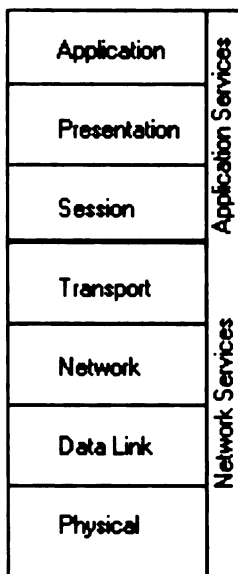
Newsgroups: an Internet service that arranges messages from users within topics. Each topic defines a group. Usenet is the most popular collection of newsgroups. Newsgroups are similar to E-mail lists but maintain an archive of messages rather than immediately disseminating them to users. News clients are used to view newsgroups, but this function is often included in **E-mail clients**. Newsgroups with a word repeated three times are jokes. For example, information from a group called hack.hack.hack would most likely contain messages designed to provoke the reader.

Node: An Internet node is any connected routing point or end-point for the network. Any **host** is a node. Non-host nodes can be routers, bridges, gateway servers, switches, and others.

Octet: An 8-bit word or segment of eight bits. (see also **byte**.)

OSI 7 Layer Model: The International Standards Organization (ISO) oversees the Open Systems Interconnection (OSI) reference model. For this reason, the OSI model can accurately also be called the ISO model. The term: eighth layer, is sometimes used to describe the human user. Ninth layer, is also used to describe business bureaucracy (the most abstract level). The official levels of the OSI model are:

- 1) The physical layer provides the medium over which data travels (e.g. wire, fiber optic cable, etc.).
- 2) The data link layer assembles **bits** into frames, provides error correction, and provided flow control (e.g. **Ethernet**).
- 3) The network layer provides connection between points.



OSI 7 Layer Reference Model

The network layer makes the interconnection of incompatible data link networks possible (e.g. IP)

4) The transport layer allows multiple simultaneous connections over the same network (e.g. TCP).

5) The session layer provides check-point services to resume partially complete transfers after interruptions and encryption.

6) The presentation layer standardizes data formats (e.g. HTML and GIF).

7) The application layer provides interaction with the user (e.g. Web browser).

Figure 3. The ISO seven layer reference model.

Out of Band: Communication between users of a given medium (e.g. E-mail) that is conducted through another medium for privacy. For instance, in-band control technology used by AT&T allows phone phreaks to access phone control systems via the **blue box**. To eliminate this form of toll fraud, AT&T implemented out of band control. Each long-distance connection uses a lower capacity channel to route and terminate the call. This channel is inaccessible to the user.

Packet Sniffer: A packet sniffer is a program designed to utilize the **promiscuous mode** of a **network interface card** to read all packets passed on an Ethernet. Packet sniffers are often used to detect passwords and logons made "in-the-clear" (unencrypted). A computer with a packet sniffer can operate anywhere on a **local area network** or can be attached to an unused **Ethernet** jack.

PBX (Private Branch Exchange): A privately owned phone switching system. PBXs typically assign extensions to individual phones rather than assigning a separate seven digit phone number to each. The extensions share a pool of seven digit phone numbers and the associated lines to reduce cost when each station is not in regular use.

Pen Register: A basic wiretap device used by the telephone companies to trap a number passed along the voice circuit in which the device is installed. Pen registers produce a list of numbers dialed. Investigators can then determine a call was made at a given time to a given number. Physical pen registers are no longer in wide use. Software that records ANI information and thus performs the function of pen register hardware is often referred to as a pen register.

Port: logical connection specified in TCP/IP. Well-known port numbers range from 0 to 1024. Well-known ports are reserved for connections with privileged services. The remaining ports (1025-65536) are usually associated with services, but can also be assigned dynamically. A connection with a server is achieved by "binding" a port to the service provided by that server.

POTS (Plain Old Telephone Service): A colloquialism for basic telephone service carried on **copper wire pairs**. Most often used to distinguish from dedicated data analog lines or digital services.

PPP (Point-to-Point Protocol): A protocol that allows communication through a serial connection. PPP is typically used to provide access to a host through phone lines. PPP replaced the previous standard, SLIP (Serial Line Interface Protocol) because it adds the capacity for **full-duplex**, connections for packet transmission over various physical layer

(see **OSI 7 layer model**) media. PPP connections can be **synchronous** or **asynchronous**.

Promiscuous mode: When set to promiscuous mode, a **network interface card (NIC)** will relay all frames received from the data link layer up through the **OSI 7 layers** to the application layer. This mode is necessary for several network diagnostic services and is the fundamental to a **packet sniffer**. The normal mode of a NIC is called discriminant mode. However, even in discriminant mode, the NIC still receives and reads all packets. In normal mode, the NIC only relays packets that are marked for its unique **MAC address** (hardware address manufactured into the NIC). When in promiscuous mode, all packets are available to an application, even those not intended for the promiscuous machine.

PSTN (Public Switched Telecommunications Network): Most commonly accessed through analog twisted **copper wire pair**. Also includes **ISDN** and **ADSL** to bring the access points up to speed with digital network infrastructure. The term 'public switched' differentiates the service from leased lines that may be constantly dedicated to a connection such as a corporate private phone network leased from the telephone company.

RBOC (Regional Bell Operating Company): Regional and local telephone service providers originally associated with AT&T. There were originally 21 Baby Bells produced by divestiture in 1984. The Baby Bells merged to form 7 RBOCs. These were: 1) Bell Atlantic 2) Ameritech 3) Bell South 4) Nynex 5) Pacific Telesis 6) Southwestern Bell 7) US West.

RFC (Request for Comment): the traditional method used to establish an Internet standard for interoperability. RFC's maintain the collegial tradition of the Internet by proposing standards rather than implementing them. They also provide the opportunity for researchers to discuss the flaws and merits of a proposed standard before adopting it. All of the RFC's are archived at <http://www.cis.ohio-state.edu/hypertext/information/rfc.html>

Router: Routers can be physical or software devices that receive, direct, and transmit packets. Some routers can be configured to filter packets based on administrator defined rules. Simple versions simply reject packets with protocol errors (like internal addresses packets coming from outside the network). More complex routers can implement rules to eliminate known attack profiles or block packets from a list or a range of addresses. Distinct functions are often combined; routing function can be included in **switches** or in dedicated **firewall** devices.

Server: A server is either software or a computer that provides services to a client. Typical services include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and many others. Servers and clients are, by definition networked computers (contrast: **stand-alone workstations**).

Spoofing: Spoofing is impersonation of another person or machine by forging address information. It is relatively simple to spoof e-mail. By stripping the first address (the real return address) from the message and making false addresses part of the message thus sent a spoofer can appear to impersonate someone else via e-mail. A **lamer** version of this technique simply has the spoofer change the registered name and return address to impersonate another sender.

Stand-alone Workstations: In the past, the distinction between workstation and personal computers was more relevant. Previously, workstations ran **UNIX** and were based on the Alpha Processor Architecture as opposed to the Intel x86 Architecture. Currently, x86 Architecture has substantially achieved the performance necessary to enter the workstation class. In broader terms, a workstation is a single-user computer. The designation: stand-alone, refers to a workstation that is not dependent upon a server.

Station Equipment: Any of a class of telecommunications equipment owned by the end user. Examples include the telephone receiver, fax machines, modems, and other devices that utilize phone lines.

Sub-net: Sub-netting trades unique host addresses for routing speed and versatility (see **router**). Although considerable attention has been given to **IPv4**'s limitation of 4.3 billion potential addresses, the most demanding limitation on Internet growth is routing speed. Sub-netting allows a reduction in the size of routing tables which produces faster routing. The operating principle is that all hosts within network x may be found through gateway x. Thus, Internet routers see all addresses within an organization as a single point. Internal routers sort out the sub-netting. Internal networks can be completely reconfigured without advertising global routing changes (see **advertising routes**). Further benefits include efficient internal allocation of IP's assigned to an organization. Sub-nets can be defined for planned growth within the organization. If the organization only needs three sub-nets (i.e. research, accounting, general), only two bits ($2^2 = 4$ and $4 > 3$) of the 32-bit IP need to be devoted to the sub-net. Further sub-netting may occur within each sub-net as needed. However, most organizations purchase routing power sufficient for

the entire sub-net, thus eliminating the need for further sub-netting. Sub-netting is formally defined in **RFC 950**.

Switch (networking): A switch determines paths for **frames** of data. A switch may duplicate the functions of a **router**. In general, switches are faster than routers but less versatile.

Switch (telephone): Switch is often used to refer to a central office or the switching equipment used in the central office.

Switching Offices: AT&T originally used a hierarchy of 5 levels to switch a phone call. The unofficial sixth level is the station equipment (telephone receiver handset). The wires running from individual houses and buildings were gathered at the Local Exchange (class 5). The first three numbers of the standard seven-digit phone number refer to the Local Exchange. This implies approximately 1000 possible numbers per Local Exchange. However, the phone company reserves some of these numbers for internal use. Local Exchanges are connected to the toll office or Central Office (class 4). Central Offices receive all calls beginning with the digit one. If the call's destination is within the same Central Office, the call is switched back to a Local Exchange. If the destination is beyond the Central Office, the call is passed to a Primary Center (class 3). When they were first conceived, Primary Centers roughly equated to an area code. However, growth in major metropolitan areas and a general flattening of the telco physical connections has disturbed this relationship. If the call's destination exceeded the area code, it would be routed through a Sectional Center (class 2). Finally, if the call's destination lay in another geographical region, it would be directed to one of twelve Regional Centers. Because of uneven population distribution, there is no direct relationship between population and

telco service beyond the Local Exchange. This entire model is somewhat archaic.

Technological and legal developments in the last twenty years have flattened this hierarchy quite a bit. However, legacy terminology and technologies may still refer to class X offices (where X is an integer from 1 to 5).

Telecommunications Reform Act of 1996: This act removes the RBOC's monopoly of local service. This act makes it possible for Incumbent Local Exchange Carriers (RBOCs) to offer long distance service upon proof that they have not discouraged local competition. This act replaces the **Modified Final Judgement of 1984**.

Terminal or Dumb Terminal: A terminal is a hardware component used to access a computer system remotely. Unlike personal computers, terminals have no internal computational power. Internal storage is limited to the trivial amount needed to buffer on screen actions. All computational processes are conducted on a host system with which the terminal is coupled. Terminals may exist on-site with a time-shared computer or may be equipped with a modem to dial the remote host. Personal computers are able to execute terminal emulation software which allows communication with a remote host.

VT 100 is one of several common standards used for terminal emulation. VT 100 is simply a communications protocol that allows the host system to communicate with the terminal. Terminals that do not support a standard with the host cannot be used on the host.

Thread: A group of related messages. It is generally identified by a common subject line, but users may use the 'reply' feature of their **E-mail client** and inadvertently reuse a subject line for a new topic. Threads and thread maintenance (i.e. keeping a subject line related to content) are especially important to **newsgroup** users. News clients (see

newsgroup) allow a user to selectively download messages. **E-mail clients** retrieve all messages sent to the user. By using the wrong subject for a message, a newsgroup user creates an unexpected intrusion on other users.

Trophy: Proof of a hack. Bedroom hackers are known for their tendency to collecting trophies as proof of bragging rights. The preferred way to prove that an intrusion has been successful is to bring back a copy of some interesting document or software. The Neidorf case is based on such a trophy. The 911 document taken from AT&T computers ended as the smoking gun in the culmination of the Secret Service's Operation Sun Devil. Other variants of hackers also use trophies. Old School hackers use especially clever pieces of program code to prove their status as a master. Some Old School hackers use code techniques to "sign" their work. Others produce highly optimized program code that demonstrates their mastery. This trophy was published to the Internet. This code allows encryption of text with "strong" encryption which is illegal to export as a war munition. A hacker implemented the RC4 standard (just another encryption standard) in 3 lines. `#!/usr/local/bin/perl -0777-- -export-a-crypto-system-sig -RC4-3-lines-PERL @k=unpack('C*',pack('H*',shift));`

```
for(@t=@s=0..255){$y=($k[$_%@k]+$s[$x=$_]+$y)%256;&S}$x=$y=0;
for(unpack('C*',<>)){ $x++;$y=($s[$x%=256]+$y)%256;&S;print
pack(C,$_^=$s[(($s[$x]+$s[$y])%256))}sub S{@s[$x,$y]=@s[$y,$x]}
```

UNIX: Unix is a broad class of operating systems based on AT&T (System V) Unix, Berkeley Free Unix (BSD), or Linux. Collectively these operating systems are properly referred to as *NIX. "UNIX" is a registered trademark, but is often used as a generic name.

War Dialer: A device or program used to sequentially dial phone numbers in search of a computer tone. Named after the device used by Mathew Broderick's character in the 1983 movie *War Games*. War dialers predate the movie, but since 1983, War Dialer is the name of choice among phone phreaks for this generic function. War dialers reached their peak with ToneLoc, a program written by Chris Lamprecht a.k.a. Minor Threat. War Dialers still exist, but have generally been replaced by port scanners.

Web Server: provides hypertext transfer protocol service on **port 80**. Related services are also often provided through a web server. Database services may be built into a web server's function to provide dynamic web content.

APPENDICES

APPENDIX A

Subcultural Sources

Fiction

Gibson, W. Neuromancer

Gibson, W. Count Zero

Gibson, W. Mona Lisa Overdrive

Gibson, W. Virtual Light

Sterling, B. Global Head

Sterling, B. The Difference Engine

Sterling, B. Holy Fire

Sterling, B. Heavy Weather

Sterling, B. Schizmatrix

Sterling, B. Islands in the Net

Sterling, B. Burning Chrome

Sterling, B. Mirror Shades

The Illuminatus Trilogy.

Orwell, G. (1949). 1984. New York, NY: Penguin.

Brunner, J. (1975). The shockwave rider. Toronto: Random House of Canada

Stephenson, N. (1992). Snow crash. New York, NY: Bantam.

Periodicals

2600: The Hacker Quarterly, volumes 4, 5, 6, 7, 8, 9, 10, 11, 12, 13(#4 only), 14, 15, 16, 17 (#1 & #2 only).

Popular Press

Freedman, D. H. & Mann, C. (1997). At large: The strange case of the world's biggest Internet invasion. New York, NY: Touchstone.

Hafner, K. & Lyon, M. (1996). Where wizards stay up late: The origins of the Internet. New York: Touchstone.

Levy, S. (1984). Hackers: Heroes of the computer revolution. New York, NY: Delta.

Goodell, J. (1996). The cyberthief and the samurai. New York: Dell Publishing.

Hafner, K. & Markoff, J. (1991). Cyberpunk: Outlaws and hackers on the computer frontier. New York: Touchstone.

Littman, J. (1996). The fugitive game: Online with Kevin Mitnick. New York: Little, Brown and Company.

Littman, J. & Donald, R. (1997). The watchman : The twisted life and crimes of serial hacker Kevin Poulsen. Boston, MA: Little, Brown and Company.

Slatalla, M. & Quittner, J. (1995). Masters of deception: The gang that ruled cyberspace. New York: Harper Collins Publishers.

Stoll, C. (1989). The cuckoo's egg: Tracking a spy through the maze of computer espionage. New York: Doubleday.

Sterling, B. (1992). The hacker crack-down: Law and disorder on the electronic frontier. New York, NY: Bantam Books.

Shimomura, T. & Markoff, J. (1996). Takedown: The pursuit and capture of Kevin Mitnick, America's most wanted computer outlaw- by the man who did it.

New York, NY: Warner Books.

Movies

Hackers

The Net

Wargames

Sneakers

Colossus

APPENDIX B

The Conscience of a Hacker [The Hacker Manifesto]
<http://www.kadets.d20.co.edu/~hlewis/hacker.html>
by Mentor [Lloyd Blankenship]
Written on January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school. I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened. A door opened to a world rushing through my phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all.

Damn kid. Tying up the phone line again. They're all alike.

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals.

We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all...

After all, we're all alike.

Copyright 1986 by Loyd Blankenship (mentor@blankenship.com). All rights reserved.

APPENDIX C

Table 5

List of All Known E-mail Clients Used on the Mitnick List During This Research, With

Coding Values

E-mail Client	Code
AOL 2.5 for Windows	1
AOL 3.0 16-bit for Windows sub 38	1
AOL 3.0 16-bit for Windows sub 40	1
AOL 3.0 16-bit for Windows sub 58	1
AOL 3.0 16-bit for Windows sub 60	1
AOL 3.0 16-bit for Windows sub 61	1
AOL 3.0 16-bit for Windows sub 86	1
AOL 3.0 for Mac sub 78	1
AOL 3.0 for Mac sub 82	1
AOL 3.0 for Windows 95 sub 18	1
AOL 3.0 for Windows 95 sub 49	1
AOL 3.0 for Windows 95 sub 51	1
AOL 3.0 for Windows 95 sub 52	1
AOL 3.0 for Windows 95 sub 52	1
AOL 3.0 for Windows 95 sub 57	1
AOL 3.0 for Windows 95 sub 64	1
AOL 3.0 for Windows 95 sub 76	1
AOL 3.0.1 for Mac sub 84	1
AOL 4.0 for Mac - Post-GM sub 54	1
AOL 4.0 for Windows 95 sub 10	1
AOL 4.0 for Windows 95 sub 13	1
AOL 4.0 for Windows 95 sub 14	1
AOL 4.0 for Windows 95 sub 15	1
AOL 4.0 for Windows 95 sub 167	1
AOL 4.0 for Windows 95 sub 170	1
AOL 4.0 for Windows 95 sub 189	1
AOL 4.0 for Windows 95 sub 190	1
AOL 4.0 for Windows 95 sub 205	1
AOL 4.0 for Windows 95 sub 206	1
AOL 4.0 for Windows 95 sub 21	1
AOL 4.0 for Windows 95 sub 212	1
AOL 4.0 for Windows 95 sub 214	1
AOL 4.0 for Windows 95 sub 219	1
AOL 4.0 for Windows 95 sub 22	1

AOL 4.0 for Windows 95 sub 224	1
AOL 4.0 for Windows 95 sub 226	1
AOL 4.0 for Windows 95 sub 230	1
AOL 4.0 for Windows 95 sub 234	1
AOL 4.0 for Windows 95 sub 236	1
AOL 4.0 for Windows 95 sub 238	1
AOL 4.0 for Windows 95 sub 246	1
AOL 4.0 for Windows 95 sub 26	1
AOL 4.0 for Windows 95 sub 27	1
AOL 4.0 for Windows 95 sub 38	1
AOL 4.0 for Windows 95 sub 39	1
AOL 4.0 for Windows 95 sub 4	1
AOL 4.0 for Windows sub 11	1
AOL 4.0 for Windows sub 230	1
AOL 4.0 for Windows sub 30	1
AOL 4.0.i for Mac sub 189	1
AOL 5.0 for Windows sub 45	1
AOL 5.0 for Windows sub 47	1
AOL for Macintosh sub 189	1
AOL for Macintosh sub 201	1
AOL for Macintosh sub 201	1
AOL for Macintosh sub 24	1
AOL for Macintosh sub 249	1
AOL for Macintosh sub 56	1
AOL NetMail version 2.0	1
Windows AOL sub 24	1
Windows AOL sub 25	1
Windows AOL sub 28	1
Windows AOL sub 41	1
Windows AOL sub 45	1
Windows AOL sub 47	1
Windows AOL sub 54	1
Internet Mail Service (5.5.2448.0)	2
Microsoft Internet E-mail/MAPI - 8.0.0.4211	2
Microsoft Internet Mail & News for Macintosh - 3.0a (366)	2
Microsoft Internet Mail 4.70.1155	2
Microsoft Internet Mail 4.70.1161	2
Microsoft Outlook 8.5, Build 4.71.2173.0	2
Microsoft Outlook 8.5, Build 4.71.2232.26	2
Microsoft Outlook 8.5, Build 4.71.2377.0	2
Microsoft Outlook CWS, Build 9.0.2416 (9.0.2910.0)	2
Microsoft Outlook Express 4.71.1712.3	2
Microsoft Outlook Express 4.72.2106.4	2
Microsoft Outlook Express 4.72.3110.1	2
Microsoft Outlook Express 4.72.3110.5	2
Microsoft Outlook Express 4.72.3155.0	2

Microsoft Outlook Express 5.00.0518.4	2
Microsoft Outlook Express 5.00.0810.800	2
Microsoft Outlook Express 5.00.1012.300	2
Microsoft Outlook Express 5.00.2014.211	2
Microsoft Outlook Express 5.00.2314.1300	2
Microsoft Outlook Express 5.00.2615.200	2
Microsoft Outlook Express 5.00.2918.2701	2
Microsoft Outlook Express 5.00.2919.6600	2
Microsoft Outlook Express for Macintosh - 4.01 (295)	2
Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)	2
Netcomplete v4.0, from NETCOM On-Line Communications, Inc.	2
Novell GroupWise 5.2	2
Web Based Pronto	2
BigMailBox.com @ http://www.bigmailbox.com	3
Excite Mail	3
GNNmessenger 1.3	3
Juno 1.49	3
Juno 2.0.11	3
Juno 3.0.11	3
Juno 3.0.13	3
mail.com	3
MailCity Service	3
Mozilla 3.0 (Win95; I; 16bit)	3
Mozilla 3.01 (Win95; I)	3
Mozilla 3.01C-IDT-v5 (Win95; U)	3
Mozilla 3.01C-Voyager (Win95; U)	3
Mozilla 3.01Gold (Win95; I)	3
Mozilla 3.04 (Win95; I)	3
Mozilla 4.01 [en] (Win95; I)	3
Mozilla 4.03 [da] (Win95; I)	3
Mozilla 4.03 [en] (Win95; I)	3
Mozilla 4.03C-AtHome0402 (Macintosh; U; PPC)	3
Mozilla 4.04 (Macintosh; I; PPC)	3
Mozilla 4.04 [en] (Win95; I)	3
Mozilla 4.04 [en] (Win95; U)	3
Mozilla 4.04 [en] (WinNT; I)	3
Mozilla 4.05 [en] (Win95; I)	3
Mozilla 4.05 [en] (Win95; U)	3
Mozilla 4.05 [en] (X11; I; Linux 2.0.32 i686)	3
Mozilla 4.05 [en]C-AtHome0404 (Win95; U)	3
Mozilla 4.06 (Macintosh; I; PPC)	3
Mozilla 4.06 [en] (Win95; I)	3
Mozilla 4.06 [en] (Win95; U)	3
Mozilla 4.06 [en] (Win98; I)	3
Mozilla 4.06 [en] (Win98; U)	3
Mozilla 4.06 [en] (WinNT; I)	3

Mozilla 4.07 (Macintosh; I; PPC)	3
Mozilla 4.07 [en] (Win95; I)	3
Mozilla 4.07 [en] (Win95; U)	3
Mozilla 4.07 [en] (X11; I; Linux 2.0.34 i586)	3
Mozilla 4.07 [en] (X11; I; Linux 2.0.36 i686)	3
Mozilla 4.08 (Macintosh; I; PPC)	3
Mozilla 4.5 (Macintosh; I; PPC)	3
Mozilla 4.5 [en] (Win95; I)	3
Mozilla 4.5 [en] (Win95; U)	3
Mozilla 4.5 [en] (Win98; I)	3
Mozilla 4.5 [en] (Win98; U)	3
Mozilla 4.5 [en] (WinNT; I)	3
Mozilla 4.5 [en] (WinNT; U)	3
Mozilla 4.5 [en] (X11; I; Linux 2.0.34 i586)	3
Mozilla 4.5 [en]C-CCK-MCD {U S WEST.net} (Win98; U)	3
Mozilla 4.5 [en]C-DIAL (Win98; U)	3
Mozilla 4.51 (Macintosh; I; PPC)	3
Mozilla 4.51 (Macintosh; U; PPC)	3
Mozilla 4.51 [en] (Win95; I)	3
Mozilla 4.51 [en] (Win95; U)	3
Mozilla 4.51 [en] (Win98; I)	3
Mozilla 4.51 [en] (Win98; U)	3
Mozilla 4.51 [en] (WinNT; I)	3
Mozilla 4.5b2 [en] (Win95; I)	3
Mozilla 4.5b2 [en] (Win95; U)	3
Mozilla 4.5b2 [en] (Win98; I)	3
Mozilla 4.6 (Macintosh; I; PPC)	3
Mozilla 4.6 [en] (Win98; I)	3
Mozilla 4.6 [en] (Win98; U)	3
Mozilla 4.6 [en] (WinNT; I)	3
Mozilla 4.6 [fr] (Win98; I)	3
Mozilla 4.61 [en] (Win95; I)	3
Mozilla 4.61 [en] (Win98; U)	3
Mozilla 4.61 [en]C-gatewaynet (Win98; U)	3
Mozilla 4.7 [de] (Win98; I)	3
Mozilla 4.7 [en] (WinNT; U)	3
My Own Email v3.0	3
Netmail	3
Netmail sub 2	3
Pegasus Mail for Win32 (v3.01b)	3
Pegasus Mail for Win32 (v3.01d)	3
USANET web-mailer (M3.0.0.20)	3
USANET web-mailer (M3.0.0.30)	3
USANET web-mailer (M3.0.0.45)	3
USANET web-mailer (M3.2.0.17)	3
USANET web-mailer (M3.2.0.53)	3

USANET web-mailer (M3.3.0.24)	3
USANET web-mailer (MaintM3.3.0.77)	3
Bluto	4
Claris EMailer v2.0	4
Claris EMailer v2.0.a sub 2	4
Crackhead R US Productions Version 3.0.6 (32)	4
Mailsmith (Bluto)	4
QUALCOMM Windows Eudora Light Version 3.0.5 (32)	4
QUALCOMM Windows Eudora Pro Version 3.0.5 (32)	4
QUALCOMM Windows Eudora Pro Version 4.0	4
QUALCOMM Windows Eudora Pro Version 4.0 Demo	4
QUALCOMM Windows Eudora Pro Version 4.0.1	4
QUALCOMM Windows Eudora Pro Version 4.1	4
QUALCOMM Windows Eudora Pro Version 4.1 (Demo)	4
QUALCOMM Windows Eudora Pro Version 4.2.0.25 (Beta)	4
QUALCOMM Windows Eudora Pro Version 4.2.0.58	4
Windows Eudora Light Version 3.0.1 (32)	4
Windows Eudora Pro Version 3.0 (32)	4
Windows Eudora Version 1.4.4	4
Allaire ColdFusion Application Server	5
Becky! ver 1.23	5
ELM [version 2.4ME+ PL31H (25)]	5
Forte Agent 1.5/32.452	5
Gnus v5.7/Emacs 20.4	5
IMP/PHP3 Imap webMail Program 2.0.3	5
MUSASHI 2.2	5
Mutt 0.66e	5
Mutt 0.91.1I	5
Mutt 0.91.2	5
Mutt 0.95.1I	5
Mutt 0.95.4I	5
PCAO 1.6	5
Poco, v1.2 - Registered Version	5
XFMail 1.3 [p0] on Linux	5
YAM 1.3.5 - Amiga Mailer by Marcel Beck	5
All instances of "Pine" in Message ID	5

APPENDIX D

MailParser Source Code

```
import java.io.BufferedWriter;
import java.io.FileWriter;
import java.io.PrintWriter;
import java.io.LineNumberReader;
import java.io.FileReader;
import java.io.FileNotFoundException;
import java.io.IOException;

import java.util.Date;
import java.util.Collection;
import java.util.Map;
import java.util.Iterator;
import java.util.StringTokenizer;
import java.util.HashMap;
import java.util.TreeMap;
import java.util.LinkedList;
import java.util.NoSuchElementException;

import java.awt.FlowLayout;
import java.awt.BorderLayout;
//import java.awt.Container;

import java.awt.event.WindowListener;
import java.awt.event.WindowEvent;

import javax.swing.JFrame;
import javax.swing.JPanel;
import javax.swing.JLabel;
import javax.swing.JButton;
import javax.swing.JList;
import javax.swing.JTextArea;
import javax.swing.JScrollPane;
import javax.swing.JCheckBox;
import javax.swing.JRadioButton;
import javax.swing.JTextField;
import javax.swing.JSeparator;
import javax.swing.ButtonGroup;
import javax.swing.BoxLayout;
```

```

import javax.swing.border.EmptyBorder;

public class MailParser
{
    public static void main( String[] argv )
    {
        if ( argv.length < 2 )
        {
            System.err.println( "*** ERROR: Usage: MailParser
mailbox_file out_file" );
            System.exit( 1 );
        }

        new MailParser().read( argv[ 0 ], argv[ 1 ] );
    }

    boolean showConsole = true;
    boolean showWarnings = true;

    MPConsole console;

    EMail email = null;
    Receipt receipt = null;

    int totalRecs = 0;
    int recs = 0;

    Collection emails = new LinkedList();
    Map attributes = new TreeMap();

    PrintWriter writer = null;

    protected void read( String inFile, String outFile )
    {
        console = new MPConsole( "MP: Mail Parser v0.1.0 -
Console" );

        if ( showConsole )
            console.show();

        console.write( "MP: Mail Parser v0.1.0\n" +
                        "Paul R. Saxman
(saxmanpa@msu.edu)\n\n" );

        console.write( "- Opening input file.\n" );

        LineNumberReader reader = null;

```

```

        try
        {
            reader = new LineNumberReader( new FileReader(
inFile ), 256 );
        }
        catch ( FileNotFoundException e )
        {
            console.write( "*** ERROR: File " + inFile + " not
found.\n" );
            System.err.println( "*** ERROR: File " + inFile + "
not found." );
            return;
        }

        console.write( "- Opening ouput file.\n" );

        try
        {
            writer = new PrintWriter( new BufferedWriter( new
FileWriter( outFile, false ) ) );
        }
        catch ( IOException e )
        {
            console.write( "*** ERROR: Cannot open file " +
outFile + " for output.\n" );
            System.err.println( "*** ERROR: Cannot open file "
+ outFile + " for output." );
            return;
        }

        console.write( "- Parsing input mail file.\n" );

        String line = null;

        try
        {
            line = reader.readLine();
        }
        catch ( IOException e )
        {
            console.write( "*** ERROR: Cannot read from
file.\n" );
            System.err.println( "*** ERROR: Cannot read from
file." );
            return;
        }
    }

```

```

StringTokenizer tokenizer;
String token;
String string;

long time = new Date().getTime();

while ( line != null )
{
    if ( line.indexOf( "From ???@???" ) > -1 )
    {
        if ( recs > totalRecs )
            totalRecs = recs;

        email = new EMail();
        emails.add( email );

        recs = 0;
    }
    else if ( email.getMessage() != null )
    {
        email.append( line + "\n" );
    }
    else
    {
        tokenizer = new StringTokenizer( line );

        if ( tokenizer.hasMoreTokens() )
        {
            token = tokenizer.nextToken();

            if ( token.equals( "Received:" ) )
            {
                recs++;

                receipt = new Receipt();
                email.addReceipt( receipt );

                if ( tokenizer.hasMoreTokens() )
                    string = tokenizer.nextToken( ""
).trim();

                else
                    string = new String( "" );

                try
                {
                    reader.mark( 1024 );

```

```

    }
    catch ( IOException e )
    {
        console.write( "*** ERROR: Line " +
reader.getLineNumber() + ": Mark error.\n" );
        System.err.println( "*** ERROR: Line "
+ reader.getLineNumber() + ": Mark error." );
        return;
    }

    try
    {
        line = reader.readLine();
    }
    catch ( IOException e )
    {
        console.write( "*** ERROR: Cannot read
from file.\n" );
        System.err.println( "*** ERROR: Cannot
read from file." );
        return;
    }

    while ( line != null )
    {
        tokenizer = new StringTokenizer( line
);

        if ( tokenizer.hasMoreTokens() )
        {
            token = tokenizer.nextToken();

            if ( token.charAt( token.length() -
1 ) == ':' &&
                Character.isUpperCase(
token.charAt( 0 ) ) )
            {
                try
                {
                    reader.reset();
                }
                catch ( IOException e )
                {
                    console.write( "*** ERROR:
Line " + reader.getLineNumber() + ": Reset error.\n" );

```

```

        System.err.println( "***
ERROR: Line " + reader.getLineNumber() + ": Reset error."
);

        return;
    }

    break;
}

    string += " " + line.trim();
}

try
{
    reader.mark( 1024 );
}
catch ( IOException e )
{
    console.write( "*** ERROR: Line " +
reader.getLineNumber() + ": Mark error.\n" );
    System.err.println( "*** ERROR: Line
" + reader.getLineNumber() + ": Mark error." );
    return;
}

try
{
    line = reader.readLine();
}
catch ( IOException e )
{
    console.write( "*** ERROR: Cannot
read from file.\n" );
    System.err.println( "*** ERROR:
Cannot read from file." );
    return;
}

try
{
    receipt.parseString( string );
}
catch ( Exception e )
{
    if ( showWarnings )
    {

```

```

        console.write( "*** WARNING: Line "
+ reader.getLineNumber() + ": Cannot parse receipt
string.\n" );

        System.out.println( "*** WARNING:
Line " + reader.getLineNumber() + ": Cannot parse receipt
string." );
    }
}
}
else if ( token.charAt( token.length() - 1 )
== ':' &&
        Character.isUpperCase(
token.charAt( 0 ) ) )
{
    token = token.substring( 0,
token.length() - 1 );

    if ( email.hasAttribute( token ) )
    {
        if ( showWarnings )
        {
            console.write( "*** WARNING: Line "
+ reader.getLineNumber() +
                        ": Attribute \"" +
token + "\" repeated in e-mail #" + emails.size() + ".\n"
);
            System.out.println( "*** WARNING:
Line " + reader.getLineNumber() +
                        ": Attribute \"" +
token + "\" repeated in e-mail #" + emails.size() + "." );
        }
    }
    else
    {
        if ( attributes.containsKey( token ) )
            attributes.put( token, new Integer(
( (Integer)attributes.get( token ) ).intValue() + 1 ) );
        else
            attributes.put( token, new Integer(
1 ) );

        if ( tokenizer.hasMoreTokens() )
        {
            string = tokenizer.nextToken( ""
).trim();

            try

```

```

        {
            if ( string.charAt(
string.length() - 1 ) == ';' )
                string +=
reader.readLine().trim();
        }
        catch ( IOException e )
        {
            console.write( "*** ERROR: Line "
+ reader.getLineNumber() + ": Line wrap read error.\n" );
            System.err.println( "*** ERROR:
Line " + reader.getLineNumber() + ": Line wrap read error."
);
            return;
        }

        email.addAttribute( token, string
);
    }
    else
        email.addAttribute( token, "NULL"
);
}

    }
    else
    {
        email.append( line + "\n" );
    }
}

try
{
    line = reader.readLine();
}
catch ( IOException e )
{
    console.write( "*** ERROR: Cannot read from file
" + inFile + ".\n" );
    System.err.println( "*** ERROR: Cannot read from
file " + inFile + "." );
}
}

    console.write( "- Parsing complete.\n" +
"    time: " + ( ( new Date().getTime()
- time ) / 1000 ) + " seconds.\n" +

```

```

        "    mails: " + emails.size() + "\n" +
        "    receipts: " + totalRecs + "\n" +
        "    attributes: " + attributes.size()
+ "\n" );

    console.write( "- Closing input mail file.\n" );

    try
    {
        reader.close();
    }
    catch ( IOException e )
    {
        console.write( "*** ERROR: Cannot close input file
reader.\n" );
        System.err.println( "*** ERROR: Cannot close input
file reader." );
    }

    //console.write( "- Opening input window.\n" );

    //new MPWindow( "MP: Mail Parser v0.1.0 - Input
Window", attributes, totalRecs );

    write();
}

protected void write()
{
    console.write( "- Writing output file.\n" );

    for ( int i = totalRecs; i > 0; i-- )
        writer.print( "Receipt " + i + "\t\t\t\t\t\t\t\t\t\t"
);

    writer.print( "Attributes" );
    writer.println();

    for ( int i = 0; i < totalRecs; i++ )
        writer.print( "From\tFrom Domain Name\tFrom IP
Address\tBy\tWith\tId\tFor\tTime\t" );

    Iterator keyIterator =
attributes.keySet().iterator();
    Iterator valIterator =
attributes.values().iterator();

```

```

        while ( keyIterator.hasNext() )
            writer.print( keyIterator.next() + " (" +
valIterator.next() + ")\t" );

        writer.println();

        Iterator iterator = emails.iterator();
        String string;

        while ( iterator.hasNext() )
        {
            email = (EMail)iterator.next();
            receipt = email.nextReceipt();

            for ( int i = 0; i < totalRecs; i++ )
            {
                if ( receipt != null )
                {
                    if ( !email.hasNextReceipt() )
                    {
                        for ( ; i < totalRecs - 1; i++ )
                            writer.print( "\t\t\t\t\t\t\t\t\t\t" );
                    }

                    writer.print( receipt.getFrom() + "\t" +
+                               receipt.getFromSubnet() + "\t"
+                               receipt.getFromIP() + "\t" +
+                               receipt.getBy() + "\t" +
+                               receipt.getWith() + "\t" +
+                               receipt.getId() + "\t" +
+                               receipt.getFor() + "\t" +
+                               receipt.getTime() + "\t" );

                    receipt = email.nextReceipt();
                }
            }

            keyIterator = attributes.keySet().iterator();

            while ( keyIterator.hasNext() )
            {
                string = email.getAttribute( keyIterator.next()
);

                if ( string != null )

```

```

        writer.write( string );

        writer.write( "\t" );
    }

    writer.println();
}

console.write( "- Closing output file.\n" );

writer.close();

console.write( "**** Program Complete ****" );

if ( !showConsole )
    System.exit( 0 );
}
}

class Receipt
{
    private String from = new String( "" );
    private String fromSubnet = new String( "" );
    private String fromIP = new String( "" );
    private String by = new String( "" );
    private String with = new String( "" );
    private String id = new String( "" );
    private String to = new String( "" );
    private String time = new String( "" );

    public void parseString( String string )
    throws Exception
    {
        String token;
        String tempString;
        StringTokenizer tokenizer = new StringTokenizer(
string );
        StringTokenizer tempTokenizer;

        while ( tokenizer.hasMoreTokens() )
        {
            token = tokenizer.nextToken();

            if ( token.equals( "from" ) )
            {
                tempString = tokenizer.nextToken();
                setFrom( tempString );

```

```

        tempTokenizer = new StringTokenizer(
string.substring( string.indexOf( tempString ) +
tempString.length() + 1 ) );
        tempString = tempTokenizer.nextToken();

        if ( tempString.charAt( 0 ) == '(' &&
            tempString.length() > 1 && // XXX Avoid
warning at 320480.
            tempString.indexOf( "HELO" ) == -1 ) //
XXX Avoid warning when "(HELO us)" encountered.
        {
            if ( tempString.charAt( 1 ) == '[' )
                this.setFromIP( tempString.substring( 2,
tempString.length() - 2 ) );
            else if ( tempString.charAt(
tempString.length() - 1 ) == ')' )
                this.setFromSubnet( tempString.substring(
1, tempString.length() - 1 ) );
            else
            {
                this.setFromSubnet( tempString.substring(
1 ) );

                tempString = tempTokenizer.nextToken();

                if ( tempString.indexOf( "UNIX" ) != -1 )
// XXX Avoid output of "[UNIX: localhost]" IPs.
                    this.setFromIP( tempString.substring(
1, tempString.length() - 2 ) );
            }
        }
    }
    else if ( token.equals( "by" ) )
    {
        setBy( tokenizer.nextToken() );
    }
    else if ( token.equals( "with" ) )
    {
        token = tokenizer.nextToken();

        if ( token.charAt( token.length() - 1 ) == ';' )
        {
            setTime( tokenizer.nextToken( "" ).trim() );
            setWith( token.substring( 0, token.length()
- 1 ) );

```

```

        }
        else
            setWith( token );
    }
    else if ( token.equals( "id" ) )
    {
        token = tokenizer.nextToken();

        if ( token.charAt( token.length() - 1 ) == ';' )
        {
            setTime( tokenizer.nextToken( "" ).trim() );
            setId( token.substring( 0, token.length() -
1 ) );
        }
        else
            setId( token );
    }
    else if ( token.equals( "for" ) )
    {
        token = tokenizer.nextToken();

        if ( token.charAt( token.length() - 1 ) == ';' )
        {
            setTime( tokenizer.nextToken( "" ).trim() );
            setFor( token.substring( 0, token.length() -
1 ) );
        }
        else
            setFor( token );
    }
    else if ( token.indexOf( "from" ) == 1 )
    {
        token = tokenizer.nextToken();
        setFrom( token.substring( 0, token.length() - 1
) );
    }
    else if ( token.charAt( 0 ) == '(' )
    {
        while ( token.indexOf( ')' ) == -1 )
        {
            token = tokenizer.nextToken();
        }

        if ( token.charAt( token.length() - 1 ) == ';' )
    }

```

```

        setTime( tokenizer.nextToken( "" ).trim() );
    }
}

public void setFrom( String from )
{
    this.from = from;
}

public void setFromSubnet( String subnet )
{
    this.fromSubnet = subnet;
}

public void setFromIP( String ip )
{
    this.fromIP = ip;
}

public void setBy( String by )
{
    this.by = by;
}

public void setWith( String with )
{
    this.with = with;
}

public void setId( String id )
{
    this.id = id;
}

public void setFor( String to )
{
    this.to = to;
}

public void setTime( String time )
{
    this.time = time;
}

public String getFrom()
{

```

```

        return from;
    }

    public String getFromSubnet()
    {
        return fromSubnet;
    }

    public String getFromIP()
    {
        return fromIP;
    }

    public String getBy()
    {
        return by;
    }

    public String getWith()
    {
        return with;
    }

    public String getId()
    {
        return id;
    }

    public String getFor()
    {
        return to;
    }

    public String getTime()
    {
        return time;
    }
}

class EMail
{
    private String message = null;
    private HashMap attributes = new HashMap();

    private LinkedList receipts = new LinkedList();
    public int listIndex = -1;

```

```

public void addAttribute( Object key, String value )
{
    attributes.put( key, value );
}

public String getAttribute( Object key )
{
    return (String)attributes.get( key );
}

public boolean hasAttribute( Object key )
{
    return attributes.containsKey( key );
}

public String getMessage()
{
    return message;
}

public void setMessage( String message )
{
    this.message = message;
}

public void addReceipt( Receipt receipt )
{
    receipts.add( receipt );
}

public void append( String message )
{
    if ( this.message == null )
        this.message = message;
    else
        this.message += message;
}

public boolean hasNextReceipt()
{
    if ( receipts.size() > 0 )
        return true;

    return false;
}

public Receipt nextReceipt()

```

```

    {
        if ( receipts.size() != 0 )
            return (Receipt)receipts.removeLast();

        return null;
    }
}

class MPConsole
extends JFrame
implements WindowListener
{
    protected JTextArea textArea = new JTextArea( 10, 25 );

    public MPConsole( String title )
    {
        super( title );

        this.addWindowListener( this );

        textArea.setBorder( new EmptyBorder( 5, 5, 5, 5 ) );
        textArea.setEditable( false );

        this.getContentPane().add( new JScrollPane( textArea
) );

        this.pack();
    }

    public void write( String string )
    {
        textArea.append( string );
    }

    public void windowActivated( WindowEvent e )
    {}

    public void windowClosed( WindowEvent e )
    {}

    public void windowClosing( WindowEvent e )
    {
        this.setVisible( false );
        this.dispose();

        System.exit( 0 );
    }
}

```

```

    public void windowDeactivated( WindowEvent e )
    {}

    public void windowDeiconified( WindowEvent e )
    {}

    public void windowIconified( WindowEvent e )
    {}

    public void windowOpened( WindowEvent e )
    {}
}

class MPWindow extends JFrame
{
    public MPWindow( String title, Map attributes, int
receipts )
    {
        super( title );

        JPanel pane = new JPanel();
        pane.setLayout( new FlowLayout( FlowLayout.CENTER, 0,
0 ) );
        this.setContentPane( pane );

        JPanel majorPanel = new JPanel();
        majorPanel.setLayout( new BoxLayout( majorPanel,
BoxLayout.Y_AXIS ) );
        majorPanel.setBorder( new EmptyBorder( 5, 5, 5, 5 )
);
        pane.add( majorPanel );

        JPanel panel = new JPanel();
        panel.setLayout( new FlowLayout( FlowLayout.LEFT, 0,
0 ) );
        panel.setBorder( new EmptyBorder( 0, 7, 0, 7 ) );
        majorPanel.add( panel );

        ButtonGroup buttonGroup = new ButtonGroup();

        JRadioButton radioButton = new JRadioButton(
"Horizontal" );
        radioButton.setSelected( true );
        buttonGroup.add( radioButton );
        panel.add( radioButton );
    }
}

```

```

        panel = new JPanel();
        panel.setLayout( new FlowLayout( FlowLayout.LEFT, 0,
0 ) );
        panel.setBorder( new EmptyBorder( 0, 7, 0, 7 ) );
        majorPanel.add( panel );

        radioButton = new JRadioButton( "Vertical" );
        buttonGroup.add( radioButton );
        panel.add( radioButton );

        panel = new JPanel();
        panel.setLayout( new FlowLayout( FlowLayout.CENTER,
0, 0 ) );
        panel.setBorder( new EmptyBorder( 5, 5, 5, 5 ) );
        majorPanel.add( panel );

        JSeparator separator = new JSeparator();
        panel.add( separator );

        panel = new JPanel();
        panel.setLayout( new FlowLayout( FlowLayout.LEFT, 0,
0 ) );
        panel.setBorder( new EmptyBorder( 0, 7, 0, 7 ) );
        panel.add( new JLabel( "Receipts " ) );
        panel.add( new JTextField( String.valueOf( receipts
), 2 ) );
        majorPanel.add( panel );

        panel = new JPanel();
        panel.setLayout( new FlowLayout( FlowLayout.CENTER,
0, 0 ) );
        panel.setBorder( new EmptyBorder( 5, 5, 5, 5 ) );
        majorPanel.add( panel );

        separator = new JSeparator();
        panel.add( separator );

        panel = new JPanel();
        panel.setLayout( new FlowLayout( FlowLayout.CENTER,
0, 0 ) );
        panel.add( new JButton( "Okay" ) );
        majorPanel.add( panel );

        majorPanel = new JPanel();
        majorPanel.setLayout( new FlowLayout(
FlowLayout.CENTER, 0, 0 ) );
        pane.add( majorPanel );

```

```

        panel = new JPanel();
        panel.setLayout( new BoxLayout( panel,
BoxLayout.Y_AXIS ) );
        panel.setBorder( new EmptyBorder( 2, 5, 2, 5 ) );
        majorPanel.add( new JScrollPane( panel ) );

        Iterator iterator = attributes.keySet().iterator();
        String string;

        while ( iterator.hasNext() )
        {
            string = (String)iterator.next();

            panel.add( new JCheckBox( string + " (" +
attributes.get( string ) + ")" ) );
        }

        this.pack();
        this.show();
    }
}

```

APPENDIX E

Data Cleaning Procedure and Commands

Delete all fields except "FROM"

NOTE: the top row is reserved for headings needed under SPSS; the formulas depend on a blank top row.

In a new worksheet named XXX-exp,

Paste all fields from edited worksheet.

To clean address:

In column B:

=IF(RIGHT(a2,1)=">",REPLACE(a2,1,SEARCH("<",a2,1),""),a2)

In column C:

=LEFT(b2,LEN(b2)-1)

Copy column C, Paste as Values, Delete columns A & B

To count each incidence of an address:

Sort (the whole set) on Column A

In column B:

=IF(EXACT(a2,a1),0,1)

In column C:

=IF(EXACT(A2,A1),C1+1,1)

In column D:

=IF(C2>=C3,C2,"")

Copy column D, Paste as Values, Delete columns B & C

To produce frequencies:

Sort (the whole set) on column B in ascending order.

Delete all rows below that last value of column B.

To prepare for export to SPSS:

Sort (the whole set) on column A in ascending order.

Name the range SPSSXXX

Name Column A "Address"

Name Column B XXX_freq

Save.

BIBLIOGRAPHY

BIBLIOGRAPHY

- Agnew, R. (1991). Strain and subcultural crime theories. In J.F. Sheley (Ed.) Criminology: A Contemporary Handbook (pp.273-294). Belmont, CA: Wadsworth.
- Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. Criminology, 30, 47-87.
- Agresti, A. & Finlay, B. (1997). Statistical methods for the social sciences (3rd ed.). Upper Saddle River, NJ: Prentice-Hall.
- Akers, R.L. (1985). Deviant behavior: A social learning approach (3rd ed.). Belmont CA: Wadsworth.
- Akers, R.L. (1997). Criminological theories: Introduction and evaluation (2nd ed.). Los Angeles, CA: Roxbury Publishing Company.
- Alford, R.R. (1995). [Review of the book *Designing social inquiry: Scientific inference in qualitative research*]. Contemporary Sociology, 24(3), 424-426.
- Anderson, B. (1991). *Imagined communities* (2nd ed.). London: Verso.
- Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: Prentice Hall.
- Banisar, D. (1999). Hacker's case raises computer crime issues. Criminal Justice Weekly, 1(9), 207, 225-227.
- Barrett, N. (1997). Digital crime: Policing the cybernation. London: Kogan Page.
- Beccaria, C. (1986). On crimes and punishments (D. Yound, Trans.). Indianapolis, IN: Hackett.
- Becker, H.S. (1963). Outsiders: Studies in the sociology of deviance. New York, NY: Free Press.
- Becker, H.S. (1982). Art worlds. Berkeley, CA: University of California Press.
- Bentham, J. (1789). An introduction to the principles of morals and legislation. New York, NY: Hafner Publishing Company.
- Blanco, R.J. (1999). Sobre sujetos virtuales y mundos digitales: El caso de las comunidades virtuales [About virtual subjects and digital worlds: The case of virtual communities]. Política y Sociedad, 30, 193-211. (From Sociological Abstracts, 2000/3).
- Blankenship, L. (1986). The hacker manifesto. Retrieved March 21, 2000 from the World Wide Web: <http://viaduct.custom.net/glitch/manif.htm>
- Blumer, H. (1969). Symbolic interactionism : Perspective and method. Englewood Cliffs, NJ: Prentice-Hall

Brink, T.L. (1995). Quantitative and/or qualitative methods in the scientific study of religion. Zygon, 30(3), 461-475.

Browne, P.W. (1999) Prosecutors seek \$1.5 million from computer hacker. Retrieved July 13, 1999 from the World Wide Web:
<http://home.digitalcity.com/losangeles/laailynews/main.dci?page=article&dciid=263542>

Burgess, R.L. & Akers, R.L. (1966). A differential association-reinforcement theory of criminal behavior. Social Problems, 14, 128-147.

Campbell, D.T. (1990). Methodology and epistemology: A dialogue. Harvard Educational Review, 60(4), 497-504.

Campbell, R. (1995). The role of work experience and individual beliefs in police officers' perceptions of date rape: An integration of quantitative and qualitative methods. American Journal of Community Psychology, 23(2), 249-277.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. International Journal of the Sociology of Law, 24(2), 229-251.

Chen, K. & Kung, S.H. (1984). Synthesis of qualitative and quantitative approaches to long-range forecasting. Technological Forecasting and Social Change, 26(3), 255-266.

Christensen, S.L. (1996). Virtuality, conversation, and morality. Technology Studies, 3(2), 199-214. (From Sociological Abstracts, 2000/3).

Cloward, R. A. & Ohlin, L.E. (1960). Delinquency and opportunity: A theory of delinquent gangs. New York, NY: Free Press.

Cohen, A.K. (1955). Delinquent boys: The culture of the gang. Glencoe, IL: Free Press.

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

Cole, M. (1999). Telecommunications. Upper Saddle River, NJ: Prentice-Hall.

Collins, J.M. & Schimdt, F.L. (1997). Can suppressor variables enhance criterion-related validity in the personality domain. Educational and Psychological Measurement, 92(4), 924-936.

Couturie, L.E. (1995). The future of high-technology crime: A parallel Delphi study. Journal of Criminal Justice, 23(1), 13-27.

Cressey, D.R. (1960). The theory of differential association: An introduction. Social Problems, 8, 2-6.

Cromwell, P. (1996). Preface. In P. Cromwell (Ed.), In their own words: Criminals on crime (pp. x-xii). Los Angeles, CA: Roxbury.

Curry, D.A. (1992). UNIX system security: A guide for users and system administrators. Menlo Park, CA: Addison-Wesley Publishing Company.

Dennis, M.L., Fetterman, D.M., & Sechrest, L. (1994). Integrating qualitative and quantitative evaluation methods in substance abuse research. Evaluation and Program Planning, 17(4), 419-427.

Duff, L. & Gardiner, S. (1996). Computer crime in the global village: Strategies for control and regulation-in defence[sic] of the hacker. International Journal of the Sociology of Law, 24(2), 211-228.

Erzberger, C. & Prein, G. (1997). Triangulation: Validity and empirically-based hypothesis construction. Quality and Quantity, 31(2), 141-154.

Ewald, K. & Jiobu, R.M. (1985). Explaining positive deviance: Becker's model and the case of runners and bodybuilders. Sociology of Sport Journal, 2(2), 144-156.

Flaming Cow (1998, December). How about those l33t d00dz? Retrieved March 21, 2000 from the World Wide Web: <http://www.hackernews.com/bufferoverflow/98/leet.html>

Flaming Cow (1998). How About Those l33t d00dz? Boston, MA: Hacker News Network. Retrieved December 21, 1998 from the World Wide Web: <http://www.hackernews.com/bufferoverflow/98/leet.html>

Frank, D. (2000). Training the security troops. Retrieved April 10, 2000 from the World Wide Web: <http://www.fcw.com/fcw/articles/2000/0410/sec-train-04-10-00.asp>

Genocide (1997, April). The Genocide2600 group history. Retrieved March 21, 2000 from the World Wide Web: <http://www.genocide2600.com/history.html>

Glaser, B.G. (1992). Basics of grounded theory analysis : Emergence vs. forcing. Mill Valley, CA: Sociology Press.

Goddard, J. (1997). Methodological issues in researching criminal justice policy: Belief systems and the 'causes of crime.' International Journal of the Sociology of Law, 25, 411-430.

Gold, R. (1969). Roles in sociological field observation. In G.J. McCall & J.L. Simmons (Eds.). Issues in participant observation. Reading, MA: Addison-Wesley.

Goldstein, E. (1993, June 13). Hacker testimony to House subcommittee largely unheard. In Thomas, J. & Meyer, G. (Eds.) Computer Underground Digest, 5.43. DeKalb, IL: Editor. Retrieved February 26, 2000 from the World Wide Web: <http://venus.soci.niu.edu/~cudigest/CUDS5/cud543.txt>

Goldstein, E. (1996). Knowledge is strength. 2600: The hacker quarterly, 13(4), 4-5.

- Goldstein, E. (1999a). Big time. 2600: The hacker quarterly, 16(1), 4-5.
- Goldstein, E. (1999b). Violence, vandals, and victims. 2600: The hacker quarterly, 16(4), pp. 5, 55.
- Goldstein, E. (1999c). Off the Hook for May 18, 1999 (Author). New York, NY: WBAI Radio. [Radio / Web simulcast]. Retrieved March 7, 2000 from the World Wide Web: <http://www.2600.com/offthehook/rafiles99/051899c.ram>
- Gollman, D. (1999). Computer security. New York, NY: John Wiley & Sons.
- Goodell, J. (1996). The cyberthief and the samurai. New York: Dell Publishing.
- Gottfredson, M.F. & Hirshci, T. (1990). A general theory of crime. Stanford, CA: Stanford University Press.
- Grabosky, P.N. & Smith, R.G. (1998). Crime in the digital age: Controlling telecommunications and cyberspace illegalities. New Brunswick, NJ: Transaction Publishers.
- Groves, W.B. & Lynch, M.J. (1990). Reconciling structural and subjective approaches to the study of crime. Journal of Research in Crime and Delinquency, 27(4), 348-375.
- Hafner, K. & Lyon, M. (1996). Where wizards stay up late: The origins of the Internet. New York: Touchstone.
- Hafner, K. & Markoff, J. (1991). Cyberpunk: Outlaws and hackers on the computer frontier. New York: Touchstone.
- Hauhart, R.C. (1991). Contemporary crime studies: Three disparate views. Sociological Forum, 6(1), 187-194.
- Hollinger, R.C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. Security Journal, 4(1), 2-12.
- Hughes, L.J. (1995). Actually useful Internet security techniques. Indianapolis, IN: New Riders Publishing.
- Icove, D. Seger, K., & VonStorch, W. (1995). Computer crime: A crimefighter's handbook. Sebastopol, CA: O'Reilly & Associates.
- Jasanoff, S. (1993). Bridging the two cultures of risk analysis. Risk Analysis, 13(2), 123-129.
- Jordan, T. & Taylor, P. (1998). A sociology of hackers. The Sociological Review, 46(4), 757-780.

Katz, J. (1988). Seductions of crime: Moral and sensual attractions in doing evil. New York, NY: Basic Books.

Kendall, L. (1996). MUDder? I hardly know 'er! Adventures of a feminist MUDder. In L. Cherny & E.R. Weise (Eds.), Wired women (pp. 242-264). Seattle, WA: Seal Press.

King, G., Keohane, R.O., & Verba, S. (1994). Designing social inquiry: Scientific inquiry in qualitative research. Princeton, NJ: Princeton University Press.

Kinkade, P.T. & Jenkins, D. (1994). Problems in establishing alternative programs in existing correctional networks. Federal-Probation, 58 37-44.

Kinkade, P.T., Jenkins, D.K., & Loper, D.K. (1994). Momentum, mix-ups, and mismatched motives: The problems involved in establishing alternative programs in existing correctional programs. Presented at the Western Society of Criminal Justice Annual Meeting in Berkeley, CA.

Lemos, R. (1999). Does the media provoke hacking? Retrieved from the World Wide Web: <http://www.zdnet.com/zdnn/stories/news/0,4586,2288043,00.html>

Lemos, R. (2000a). Author of Web attack tool speaks. Retrieved February 10, 2000 from the World Wide Web: <http://www.zdnet.com/zdnn/stories/news/0,4586,2436358,00.html>

Lemos, R. (2000b). Script kiddies: The Net's cybergangs. Retrieved July 12, 2000 from the World Wide Web: <http://www.zdnet.com/zdnn/stories/news/0,4586,2602573,00.html>

Levy, R. (1993). Believability and doubtfulness: A paradigmatic view of qualitative methods. Canadian Journal on Aging, 12(2), 233-243.

Levy, S. (1984). Hackers: Heroes of the computer revolution. New York: Dell Publishing.

Littman, J. & Donald, R. (1997). The watchman : The twisted life and crimes of serial hacker Kevin Poulsen. Boston, MA: Little, Brown and Company.

Littman, J. (1996). The fugitive game: Online with Kevin Mitnick. New York: Little, Brown and Company.

Loper, D.K. (1998). A field study of hackers. Unpublished manuscript, Michigan State University. East Lansing.

Mann, D. & Sutton, M. (1998). Netcrime: More change in the organization of thieving. British Journal of Criminology, 38(2), 201-229.

Martin, B. (1999, August). The newbie's guide to fear, uncertainty, and doubt. Hacker News Network. Retrieved August 1999 from World Wide Web: <http://www.hackernews.com/orig/fud.html>

Martinez, M.J. (1999) A Non-Prosecution Complex: Law Enforcement Struggles With Computer Crime. Retrieved August 13, 1999 from the World wide Web: <http://abcnews.go.com/sections/tech/DailyNews/cybercrime990813.html>

McCarthy, L. (1998). Intranet security: Stories from the trenches. Mountain View, CA: Sun Microsystems Press.

McClendon, M.J. (1994). Multiple regression and causal analysis. Itasca, Il: F.E. Peacock Publishers.

Meeks, B.N. (2000). Hackers stumble toward legitimacy. Retrieved July 19, 2000 from the World Wide Web: <http://www.msnbc.com/news/435153.asp>

Merton, R.K. (1938). Social structure and anomie. American Sociological Review, 3, 672-682.

Microsoft Corporation. (1997). Microsoft Excel (SR-2). [computer software]. Redmond, WA: Author.

Miller, M. (1994). The evolution of telco fraud articles in Phrack. Retrieved December 6, 1994 from the World Wide Web: <http://swissnet.ai.mit.edu/6095/student-papers/fall94-papers/miller-phrack/miller-phrack.html>

Miller, S.I. (1983). Mapping, metaphors and meaning: A note on the case of triangulation in research. Sociologia Internationalis, 21, 69-79.

Mills, C.W. (1990). Situated actions and vocabularies of motive. In D. Brissett & C. Edgly (Eds.) Life as Theater: A dramaturgical sourcebook (207-218). New York, NY: Aldine de Gruyter.

Mitnick, K.D. (2000). Off the Hook for February 8, 2000 (Emmanuel Goldstein, Producer). New York, NY: WBAI Radio. [Radio / Web simulcast]. Retrieved March 9, 2000 from the World Wide Web: <http://www.2600.com/offthehook/rafiles00/020800.ram>

Muchinsky, P.M. (1990). Psychology applied to work (3rd ed.). Pacific Grove, CA: Brooks/Cole.

Mungo & Clough (1992). Approaching zero: The extraordinary underworld of hackers, phreakers, virus writers, and keyboard criminals. New York, NY: Random House.

Nunnally, J.C. (1978). Psychometric Theory (2nd ed.). New York, NY: McGraw-Hill.

Palme, J. (1997, February). Common Internet Message Headers [RFC 2074]. Stockholm, Sweeden: Network Working Group. Retrieved March 6, 2000 from the World Wide Web: <http://www.cis.ohio-state.edu/htbin/rfc/rfc2076.html>

- Perinbanayagam, R. (1985). Identity, social acts and motives. In Author & H.A. Farberman (Eds.), *Studies in Symbolic Interaction* (pp. 193-216, Suppl. 1). Greenwich, CT: JAI Press.
- Plummer, K. (Ed.). (1991). Symbolic interactionism. Brookfield, VT: Elgar.
- Poulsen, K. (1998). Grassroots Hacktivism. Retrieved September 16, 1998 from the World Wide Web: <http://www.zdnet.com/zdtv/cda/index/0,2073,2137656-2103615,00.html>
- Poulsen, K. (September, 1998). Meet Mitnick's prosecutor. San Francisco, CA: CNet. Retrieved from the World Wide Web: <http://www.zdnet.com/zdtv/cda/index/0,2073,2000163-2103615.00.html>
- Psychotic Opposition (1987). Society sucks: And what to do about it. Retrieved July 17, 2000 from the World Wide Web: http://www.cultdeadcow.com/cDc_files/cDc-0009.txt
- Raymond, E.S. (1996). The New Hacker's Dictionary. Cambridge, MA: MIT Press.
- Rosenbaum, R. (1971, October). The secrets of the blue box. Esquire. 116-128.
- Russell, D. & Gangemi, G.T. (1991). Computer security basics. Sebastopol, CA: O'Reilly & Associates.
- Saxman, P. (2000). MailParser: Eudora to tab-delimited text. [computer programming language]. East Lansing, MI: Author.
- Schneier, B. (1995). Applied cryptography: Protocols, algorithms, and source code in C. New York, NY: John Wiley & Sons.
- Shelley, L.I. (1998). Crime and corruption in the digital age. Journal of International Affairs, 51, 605-620.
- Skaletsky, S. & Goldstein, E. (2000). Off the Hook for June 6, 2000 (Emmanuel Goldstein). New York, NY: WBAI Radio. [Radio / Web simulcast]. Retrieved June 25, 2000 from the World Wide Web: <ftp://ftp.2600.com/pub/oth/2000/060600.rm>
- Skinner, W.F. & Fream, A.M. (1997). A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 34(4), 495-518.
- Slatalla, M. & Quittner, J. (1995). Masters of deception: The gang that ruled cyberspace. New York: Harper Collins Publishers.
- Space Rouge (1999). The difficulties of reporting the underground. Boston, MA: Hacker News Network. Retrieved August 11, 1999 from the World Wide Web: <http://www.hackernews.com/orig/underreport.html>

Statistical Package for the Social Sciences 7.5.1 [Computer software] (1996). Chicago, IL: SPSS Inc..

Sterling, B. (1992). The hacker crack-down: Law and disorder on the electronic frontier. New York: Bantam Books.

Stoll, C. (1989). The cuckoo's egg: Tracking a spy through the maze of computer espionage. New York: Doubleday.

Strauss, A.L. & Corbin, J.M. (1998). Basics of qualitative research : Techniques and procedures for developing grounded theory (2nd ed.). Newbury Park, CA: Sage Publications.

Swanborn, P.G. (1996). A common base for quality control criteria in quantitative and qualitative research. Quality and Quantity, 30(1), 19-35.

Sykes, G.M. & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review, 22, 664-670.

Thomas, D. (1998a). The Making of a 'Darkside Hacker.' Retrieved July 3, 1998 from the World Wide Web: http://olj.usc.edu/sections/departments/98_stories/hacker_070398.htm

Thomas, D. (1998b). Mitnick's Trial Delayed. Retrieved December 4, 1998 from the World Wide Web: <http://www.wired.com/news/politics/0,1283,16627,00.html>

Vatis, M. (1998, February). A message from Michael Vatis, Chief of the National Infrastructure Protection Center. Washington, DC: National Infrastructure Protection Center. Retrieved February 1998 from World Wide Web: <http://www.fbi.gov/nipc/nipc.htm>

Whyte, W.F. (1983). Learning from the field: A guide from experience. Newbury Park: CA, Sage Publications.

Ziff-Davis Publications (1999). Hacker vs. Cracker [on-line poll]. Retrieved March 30, 1999 from the World Wide Web: <http://cgi.zdnet.com/zdpoll/question.html?pollid=2408>

MICHIGAN STATE UNIV. LIBRARIES



31293020486605