FBI Law Enforcement Bulletin

September 1989

The Enrique Camarena Case

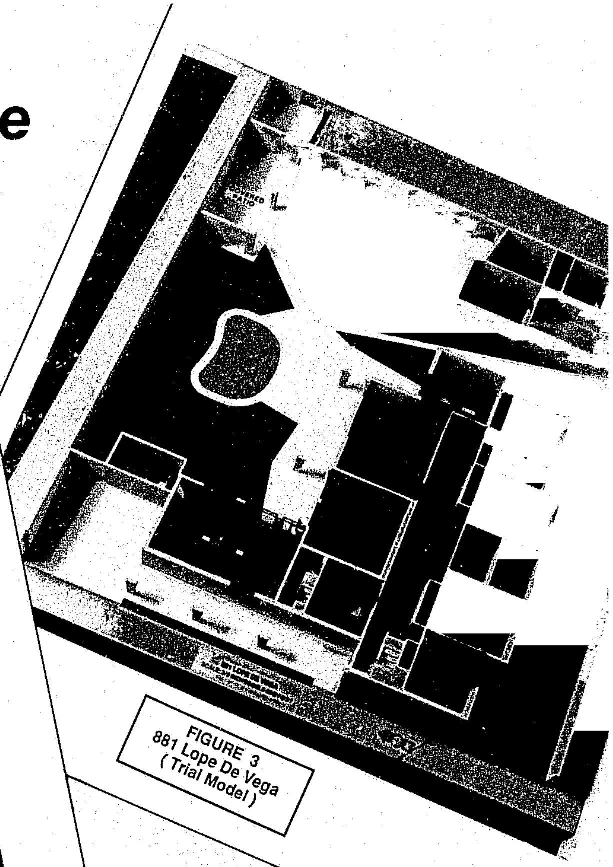


FIGURE 3
881 Lope De Vega
(Trial Model)

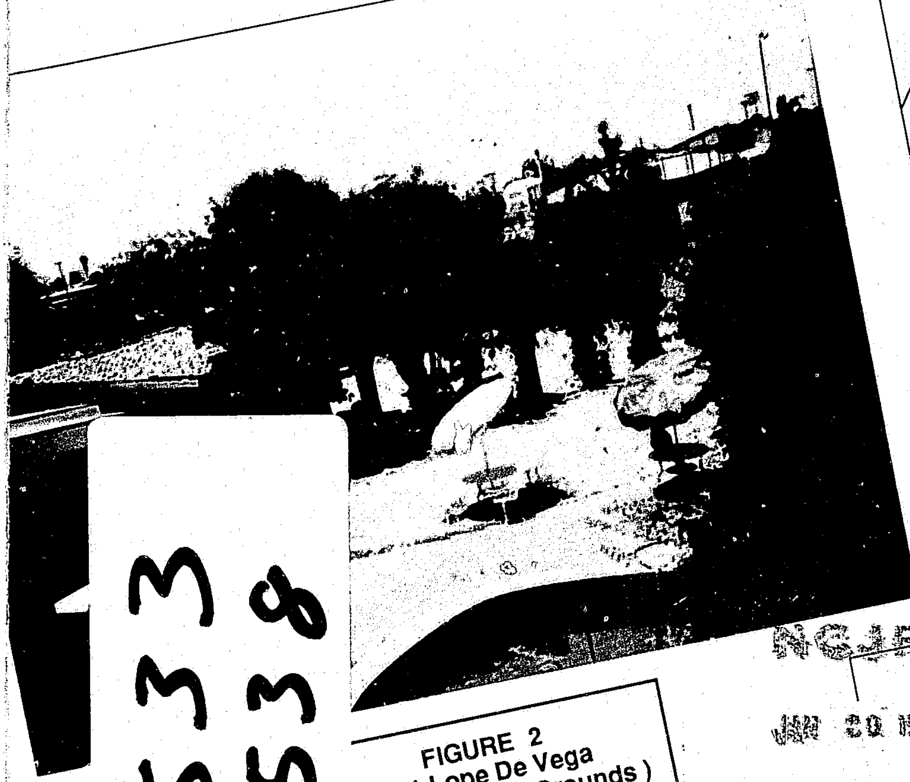


FIGURE 2
881 Lope De Vega
Interior View of Grounds)

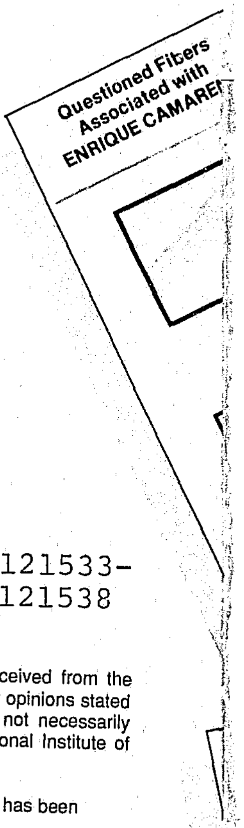
FIGURE 1
Special Agent
Enrique Camarena

Also In This Issue:

Contents

September 1989, Volume 58, Number 9

Features



Departments

FBI
Law Enforcement Bulletin

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

William S. Sessions, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget.

Published by the Office of Public Affairs,
Milt Ahlerich, *Assistant Director*

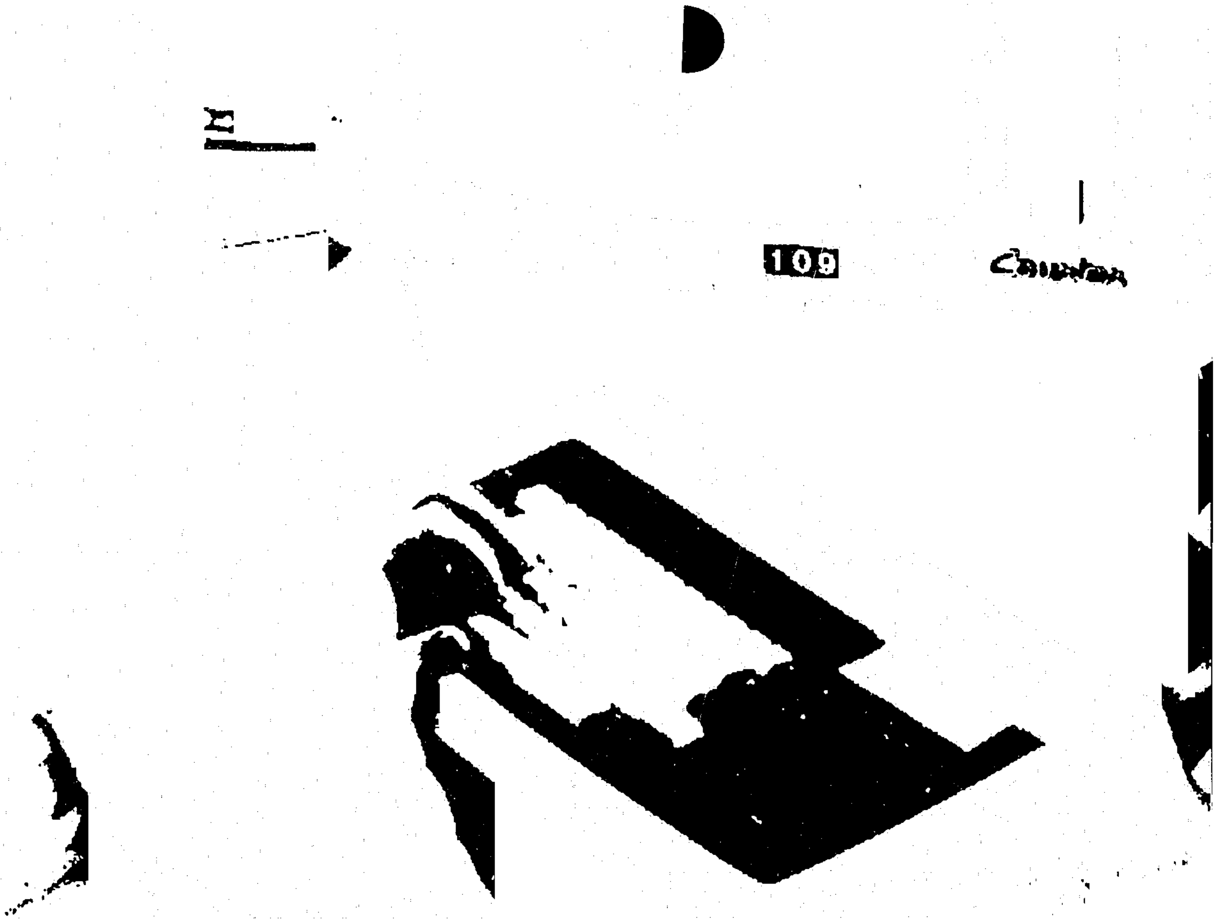
Editor—Stephen D. Gladis
Managing Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Assistant Editor—Alice S. Cole
Production Manager—Joseph Andrew DiRosa

***The Cover:** The abduction and subsequent murder of DEA Special Agent Enrique Camarena initiated one of the most extensive forensic investigations ever conducted by the FBI Laboratory. See article p. 1.*

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-Class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688

USPS 383-310


109

Lieutenant Coutourie

"... law enforcement agencies need to explore new approaches to investigating computer criminals."

Computer criminals perpetrate a new type of crime that is rapidly emerging and promising to have a dramatic impact on society. However, computer criminals do not employ the same methods or have the same characteristics as "traditional" criminals. Therefore, examination and evaluation of their personalities are required.

One extremely valuable investigative technique that has produced significant results is criminal investigative analysis (formerly referred to as profiling)[1]—a technique that could also be applied to computer criminals who threaten the financial sector of our society. However, two major considerations limit the scope of effective research on the assessment of the computer criminal. First, criminal investigative analyses are traditionally done on persons involved in violent, aberrant crimes (which computer crime is not); second, studies indicate that computer criminals are emerging as such an eclectic group that it may be impossible to categorize them clearly.

Effects of Computer Criminals on Society

Although marked differences exist between the type of criminals who commit murders and those who commit computer crimes, their impact on society is great. A survey of 1,000 organizations revealed that the verifiable losses attributed to computer crime in 1985 were estimated between $145 million to $750 million.[2] Estimates show that computer criminals in the workplace alone may be costing businesses up to $3 billion a year.[3] In fact, the possibility of "corporate murder" is even more likely. Computer criminals can bring financial disaster to small businesses, as well as individuals, and can drastically affect many lives.

The Corporate Victim

As with traditional criminal investigative analysis, victim information can lead to many relevant conclusions. Corporations, the most likely victims, have a number of characteristics in common with humans, e.g., corporate occupation, residence, financial status, fiscal fitness, reputation, and background. In some cases, corporate fears and habits, corporate friends and enemies, and recent changes in corporate structure may all be relevant.

New Investigative Approaches

For the purposes of criminal investigative analysis, the differences between violent offenders and computer criminals present some very new and unique forensic problems to investigators. In order to determine personality characteristics, such as race, sex, age, marital status, employment, sexual maturity, and criminal history,[4] analysts require as much information as possible about the crime scene and the victim. However, computer criminals leave no traditional crime scene for investigators to photograph and examine. The victim is very likely to be a corporation, and the perpetrators may never be physically at the "scene of the crime," making it difficult to establish the relationship between the attacker and the victim.

Therefore, law enforcement agencies need to explore new approaches to investigate computer criminals. Investigators should be able to gather "electronic trace evidence" to determine the type of equipment used to attack the "corporate victim." With an "electronic autopsy," recovery of magnetic impulses from a disk storage unit is possible. These impulses might provide some clues about the computer criminal. And, an "electronic forensic pathologist," in the form of a highly skilled and specially trained computer scientist familiar with the victim equipment, may greatly assist investigators.

For example, it is a common occurrence for "hackers" to post on electronic bulletin boards stolen telephone credit card numbers that they claim to have ''hacked'' from a long distance carrier's computer. Investigators must locate and examine ''day files'' of logs of computer usage that indicate the type of computer used to illegally post the numbers. This information is considered essential circumstantial evidence, particularly if a criminal is found to possess or use the same type of equipment. A variety of utility programs recover data files from disks that may contain these credit card numbers or other information, possibly intentionally damaged, secured, or encrypted by those using computers to aid them in committing the crime.

''Hacking'' programs recovered from suspects (designed to obtain telephone credit card numbers from another computer) are routinely disassembled, listed, and examined for instructions that caused them to perform as indicated, thus providing additional valuable evidence. Obviously, there is a need for greater professionalism in dealing with computer criminals, who already possess the expert knowledge necessary to use computers as tools of crime. By studying and understanding the type of person likely to become involved in computer crimes, this need can be met.

> ❝ *... computer criminals present unique problems and challenges to investigators....* ❞

Assessing Computer Criminals

A proficient investigator needs to determine the motive and compile the tangible and intangible evidence that will identify the attacker. A review of past offenders can provide a base of information from which to assess computer criminals and to draw conclusions.

Examining individuals known to have been involved with computer crime aids in understanding others who use computers to commit crimes. Researchers have interviewed many known offenders and have drawn informative conclusions.

Modern hackers seem to have that driving need to dissect, examine, understand, and modify whatever captures their attention (to include what they perceive as improvements). For instance, the ''original'' hackers were college students who participated in constructing and modifying a model railroad system. Members of the group felt free to make whatever changes they believed appropriate to improve the system.

More modern-day hackers have the same attitude of free access to other people's computer systems. Computer information, such as long distance telephone access codes, will allow them to gain even further access to other computers. In his book, *Fighting Computer Crime*, Donn Parker characterized hackers as often being addicted to their computer capers, willing to give up food, sleep, and other bodily functions in order to sit at their computers for hours at a stretch.[5] In essence, they gave up the real world for an electronic one. They replace concepts of right and wrong with what is binary 0 or 1. Although Parker refers to high school-aged hackers,[6] age is not a real factor, because many adult hackers also have essentially the same characteristics.

Steven Levy's description includes the ''hands on imperative,'' the driving need to manipulate the computer hardware personally.[7] Early hackers would do anything to get to the computer itself, because by working the hardware, they achieved gratification.

In a study of 375 computer abuse cases, Parker reports several characteristics of individuals in a sample of 17 criminals.[8] Their average age was 29 years, they had predominantly professional/managerial skills, and in all but one case, they committed crimes in conjunction with their occupations. About 76 percent demonstrated differential association syndrome, that is, their criminal acts differentiated from accepted business practices only in small ways. For example, hackers maintain contact through electronic bulletin boards where they frequently learn hacking methods (deviant influences) from each other. However, they seem to resist behavior considered ''harmful'' to others, thus showing the normative influences in their lives.

Over 88 percent of Parker's subjects viewed their actions as a game pitting their skills against the computers or organization. These games represented challenges that made their lives exciting and filled with danger. Seventy-one percent of these subjects also demonstrated the Robin Hood syndrome, i.e., they differentiated strongly between harming people, which they considered immoral, and harming organizations, which they could rationalize.[9]

In describing private industry's problem, Jay Bloombecker, a former director of the National Center for Computer Crime Data, believes that computer criminals are not necessarily geniuses.[10] He delineates several "criminogenic" environments he believes were present in the computer crimes he surveyed, although he admits that these categories are not mutually exclusive or rigid:

The Playpen and The Fairyland—In the playpen, abusers find simply using a computer to be intrinsically satisfying; in the fairyland, the abuser sees the computer as an unreal world and thus he is doing no wrong.

The Land of Opportunity or The Toolbox—An abuser in the land of opportunity takes an attitude of nothing being wrong with the exploitation of an obvious vulnerability in a computer system; in the toolbox, the abuser views the computer as merely a tool to accomplish an end.

The Cookie Jar—This is a fund from which an abuser may "borrow" because his need is greater that the company's. This computer environment provides the opportunity for personal gain.

> **"Computer criminals ... can drastically affect many lives."**

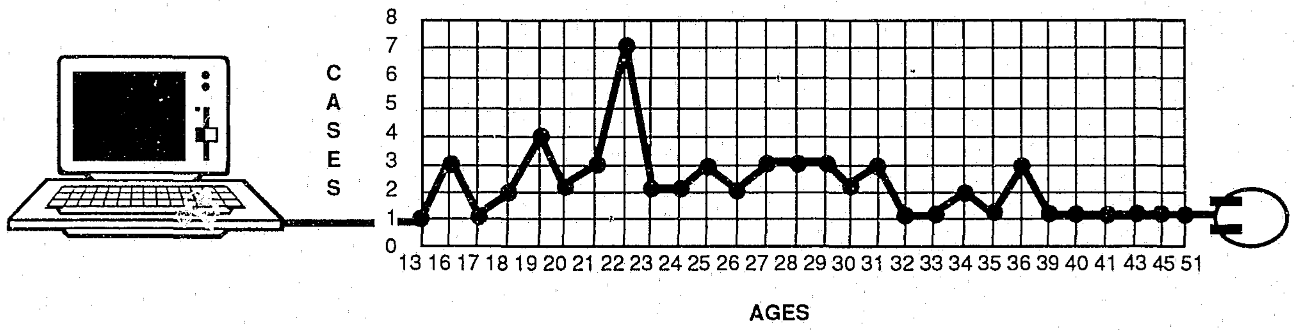
The War Zone—The war zone is a place where the abuser vents his feelings against the company while not apparently harming any individuals, thus meeting the criteria set out in the Robin Hood Syndrome which he could rationalize.

The Soapbox—The type of activity found here is frequently not harmful in the usual criminal sense and may not frequently appear as motivation for a computer crime. It may be a result of a transference defense mechanism.

A study by Kusserow, in which 29 computer criminals were interviewed, produced potentially valuable data.[11] Their ages ranged from 20 to 50 with a median age of 30, and a majority (75 percent) had some college education. All had been employed for an average of 5 years before committing their crimes. During their employment, nearly three-fourths had been promoted, and 25 percent said that they had received performance awards. Further, about 20 percent had criminal records at the time they were hired; in most cases, this was known to the employer. The nature of the previous crimes committed by those with criminal records was not discussed. Most of the criminals reported that they stole due to situational factors that fell into two categories—financial problems (60 percent) and job discontentment (10 percent). Still others stole because they discovered a vulnerability in the system and could not resist the temptation. In other cases, a spe-

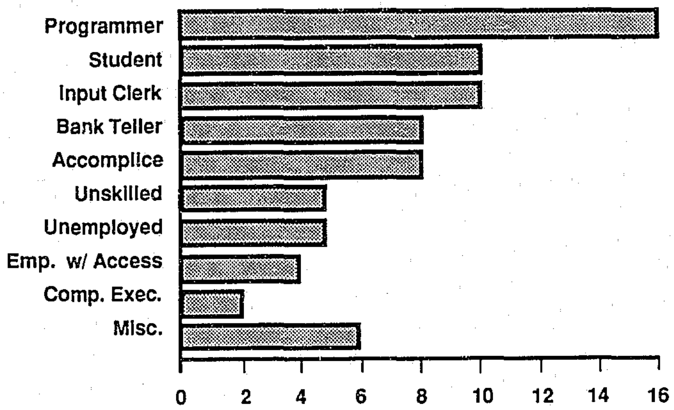
Table 1

Ages of Computer Crime Defendants



Ages of computer crime defendants as reported in a census conducted by the NCCCD over a two year period, ending in 1986.

Table 2
Computer Crime Defendants



Computer crime defendants as reported to the NCCCD in a census taken over a two year period, ending in 1986.

cific event or accidental situation. presented an opportunity. Some were bored and decided to "beat the system." One significant finding is that about one-half said that they did not consider the consequences of their crime at the time, while others assessed the risks of being caught as minimal.

A good measure of the ages of computer crime perpetrators can be found in a survey performed by the National Center for Computer Crime Data that reported the ages of defendants in computer crime cases.[12] (See table 1.) This may represent "tip of the iceberg" information because of the number of computer crimes that go undetected or unreported, but may also be a reliable index due to the origin of the data.

Table 2 shows that the occupation most often involved in computer crimes are those with computer access. The person involved in this activity represents a relatively wide cross-section of computer-related occupations. Programmers, as might be expected, show a greater frequency of committing a computer crime because of their expertise in the working of computers and the unlimited access normally granted to them. The nature of their job also requires they maintain a computer operating system.

Conclusion

Since computer criminals present unique problems and challenges to investigators, and with the meteoric rise of computer crime in the country, police departments must become more proficient in investigating and dealing with this type of criminal. The common characteristics of computer criminals and the type of environments in which they work, as detailed in this article, may provide an information base for criminal investigative analysis, which can be used as a means to apprehend the computer criminal.

Footnotes

[1] John E. Douglas and Alan E. Burgess, "Criminal Profiling: A Viable Investigative Tool Against Violent Crime," *FBI Law Enforcement Bulletin*, vol. 55, No. 12, December 1986, pp. 9–13.

[2] William J. Hughes, "Computer Crimes Isn't a Game," *The Washington Post*, July 15, 1986.

[3] Theo Stames, "A Costly Wave of Computer Crime," *Insight*, March 17, 1986.

[4] Richard Ault and James T. Reese, "A Psychological Assessment of Crime Profiling," *FBI Law Enforcement Bulletin*, vol. 49, March 1980, p. 3.

[5] Donn B. Parker, *Fighting Computer Crime* (New York: Charles Scribner's Sons, 1983).

[6] Ibid., p. 131.

[7] Steven Levy, *Hackers: Heroes of the Computer Revolution* (New York: Doubleday and Company, Inc., 1984), p. 40.

[8] Donn B. Parker, *Computer Abuse Perpetrators and Vulnerabilities of Computer Systems*, (California: Stanford Research Institute, December 1975).

[9] Ibid.

[10] Jay Bloombecker, "Who are the Computer Criminals?" *Security Management*, January 1981.

[11] Richard P. Kusserow, "An Inside Look at Federal Computer Crime," *Security Management*, May 1986.

[12] Jay Bloombecker, *Computer Crime, Computer Security, Computer Ethics*, First Annual Statistical Report, National Center for Computer Crime Data, 1986.