THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

ABOUT THE AUTHOR

Carl J. Franklin has more than twenty years experience in the criminal justice profession. He spent almost thirteen of those years in a uniform working as a Community Service Officer, Police Officer, and in various roles as investigator and supervisor. He has worked in a uniform position with the University of Oklahoma, Norman, and Oklahoma City police departments. While a police officer, Franklin returned to the University of Oklahoma to complete a Bachelor's of Arts degree in Law Enforcement Administration. He later attended the Oklahoma University College of Law where he completed the Juris Doctor degree and was honored on three occasions with national awards for his writing in the areas of computers and constitutional law. He has also recently completed the Ph.D. in Business with an emphasis in Public Administration.

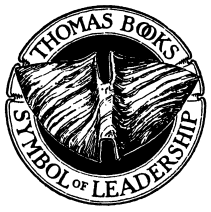
Franklin has also worked with the Oklahoma Court of Criminal Appeals, the Cleveland County District Attorney's Office, and as a private practitioner. He was appointed in three counties as the chief attorney for indigent defense, and maintained an active practice in criminal defense, police civil liability, and related areas.

He is the author of five books, including the *Police Officer's Guide to Civil Liability* (Charles Thomas) and more than forty professional and academic articles. Franklin currently works as an Assistant Professor (Tenure Track) at Southern Utah University where he teaches criminal and constitutional law, criminal procedure, ethics, and related classes.

THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

By

CARL J. FRANKLIN, J.D., PH.D.



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

ISBN 0-398-07601-4 (hard)
ISBN 0-398-07602-2 (paper)

Library of Congress Catalog Card Number: 2005050873

With THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

Printed in the United States of America
MM-R-3

Library of Congress Cataloging-in-Publication Data

Franklin, Carl J., 1958-
The investigator's guide to computer crime / by Carl J. Franklin.
p. cm.
Includes bibliographical references and index.
ISBN 0-398-07601-4 – ISBN 0-398-07602-2 (pbk.)
1. Computer crimes–Investigation–Handbooks, manuals, etc. I. Title.

HV8079.C65F73 2005
363.25'968–dc22

2005050873

To Christopher, Michael, and Stacey.
You make me very proud.

CONTENTS

Section 2: Specific Computer Crimes

Section 3: The Computer Crime Investigation

Section 4: Search, Seizure, and Digital Evidence

FIGURES

TABLES

THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

Section 1

ESTABLISHING STANDARDS FOR THE COMPUTER CRIME INVESTIGATION

Chapter 1

THE GROWING TREND OF COMPUTER CRIME

A. INTRODUCTION TO COMPUTER CRIME

In the past half-century we have gone from a world where computers were science fiction to a world where computers are everyday fact. Just thirty years ago the computer that flew with the first astronauts to the moon had less computing power than the computer on the average student's desk today. Computers have grown in popularity, acceptance, and computing power. The average Personal Computer has doubled its computing capacity every eighteen months for more than a decade. Today, we find computers common in almost all parts of our life and there is no reason to believe that usage will decrease in the near future.

Along with the acceptance of computers in our everyday life has emerged a new line of crime revolving around the computer. Just as computers make daily business transactions more efficient they have also made many crimes more efficient. Computers have given us many new advances in our lives and provided great improvement as a whole. This is also true of the criminal element; computers have created contemptible new crimes as well as modernized many of the old ones.

For the law enforcement officer the first major issue is the determination

of how much emphasis to put on the problem. Clearly, computers have become a growing part of our everyday work as criminal investigators, but does that mean they should become a specialization unto themselves? Should departments create a "computer crime" unit similar to our traditional homicide, robbery, and burglary units?

We know that computers have made a substantial impact on our society, but have computer crimes become so significant that they demand special attention? The short answer is that it has not; at least yet. While the number of computer-related crimes has increased over the last two decades the vast majority of police officers rarely are involved in a computer crime. What this means is that while we should be conscious of the increase in computer-related crime, we need not create entire new branches of investigative theory to deal with that crime. For the most part, focused education and training can prepare the majority of police investigators to handle almost any computer crime they encounter.

One should not infer from the above statement that computer crime is not a problem. The fact is that computer crime is on the increase, and there is firm evidence to believe that the growth trend will continue for some time to come. Investigators should also keep in mind the rise in computers as both a tool and potential element of crime. Just as computers have helped the police in becoming more efficient, so too, have they assisted wary criminals in perpetrating a wide variety of crimes. This trend is likely to continue, and for that reason alone police investigators should make themselves better prepared for computer-related crime investigations.

The obvious choice for most police agencies is a combination of upgrading our technology along with an increase of our knowledge so that we become more efficient in our pursuits. Of course, this will vary according to specific needs of the department or the investigative unit. It is clear that a vice unit does not need an advanced computer system when making routine prostitution arrests, but it is equally clear that an investigator will need some computer knowledge if he is to track money transactions stored by pimps on laptop computers. Simply stated, the increased use of computers by traditional criminals significantly increases the need for investigators to be computer competent.

The above example illustrates a crime which is not traditionally considered a computer crime but which does involve the use of a computer. Basic computer knowledge may be all that is needed to conduct this investigation, but what about crimes where the computer is a substantial part of the *modus operandi*? In coming chapters we will examine this issue in much more detail, but for now it is important to recognize that computer crime extends far beyond the original definitions set out by the industry.

Another, and sometimes more pressing issue, which often arises focuses

on the logistics of computer use in both crime and criminal detection. A nagging question facing the police community today is whether police agencies expend significant man-hours and resources preparing for crimes that are often difficult to detect and even more difficult to prosecute? A better way to look at this issue is to ask whether traditional investigative techniques, those that are used in less technologically advanced crimes, are enough to determine who has released the latest virus?

The potential for computer crime is almost limitless. As computers invade more of our everyday lives the need for competent investigators grows. For each of the issues set out above the answers all appear to be relatively the same. In each instance we can find a need for increased knowledge as well as better technology. In other words, to be effective, investigators in today's climate must move ahead both in understanding technology and in their preparedness to investigate computer-related crime.

To better prepare we must focus on training that will upgrade our knowledge and skills. That is the purpose of this book. To begin this task we must first establish some basic guidelines so that all readers will advance significantly in their knowledge and skills. We do this by first establishing basic principles, definitions, and techniques. The first of these is a definition of computers and computer crime.

B. DEFINING COMPUTER AND TECHNOLOGY CRIME

Defining computers and computer-related crime might seem simple on the surface, but therein lays the difficulty of the task. If we define both too broadly then we risk creating a menace that never appears. Define the terms too narrowly and we chance missing the real problem when it comes. In order to hit the proverbial nail on the head we should start with a simple definition, refine it, and then establish a usable working definition that will serve our purposes.

The simplest definition we can use is that "computer crime is any crime involving a computer." Almost immediately one can see that such a simple definition creates critical problems. In our highly mechanized and computerized world to define computer crime so broadly would be to catalog almost any crime as a computer crime. After all, consider the number of appliances in our homes that have some sort of computer system built into them. Today it is hard to buy a microwave, refrigerator, dishwasher, or any other major appliance without having it operate with a *Central Processing Unit* (CPU) of some type.

One of the problems with such a broad definition is that the investigator spends more time defining the crime than investigating it. Imagine for a