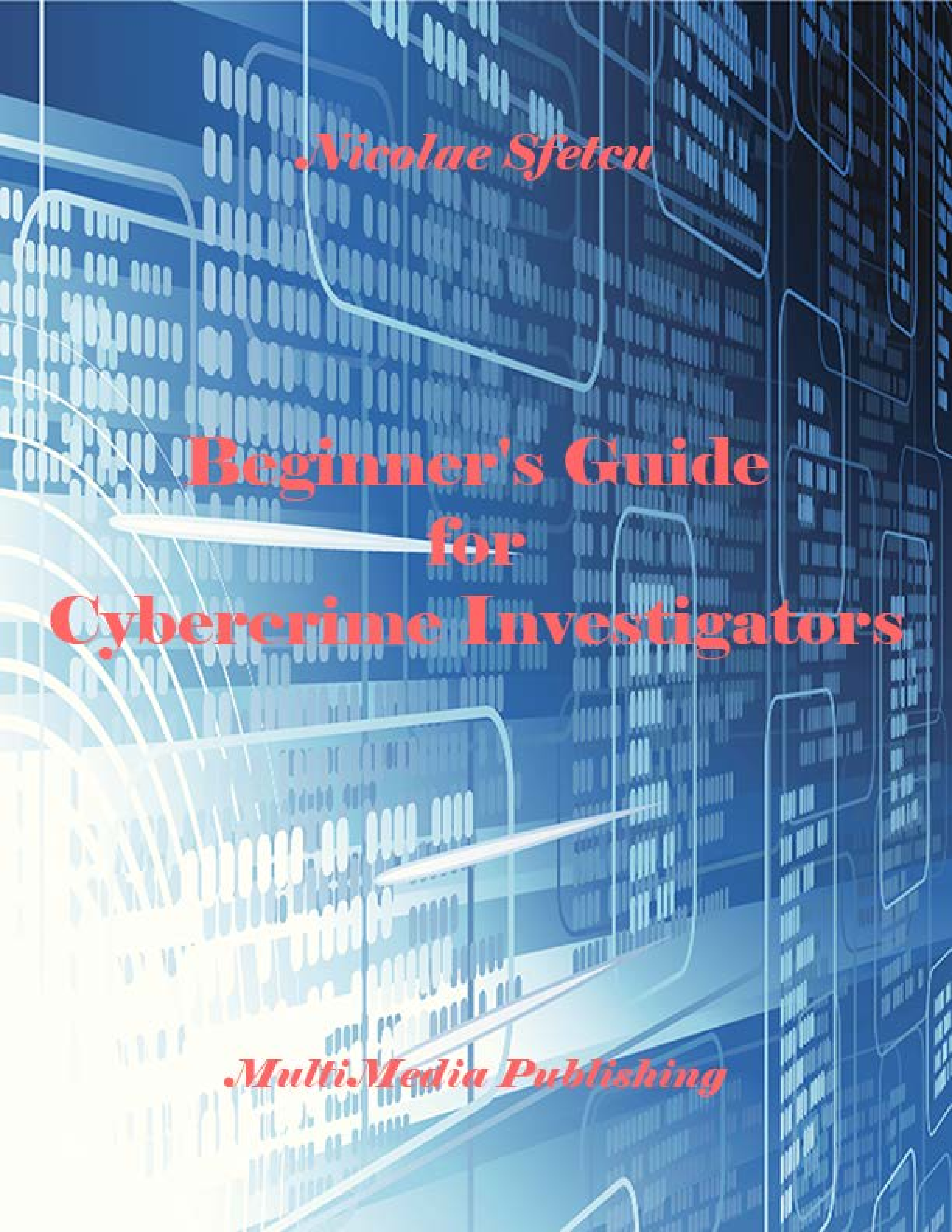


Nicolae Sfetcu

Beginner's Guide for Cybercrime Investigators

MultiMedia Publishing

Beginner's Guide for Cybercrime Investigators

Nicolae Sfetcu

Published by Nicolae Sfetcu

BOOK PREVIEW

Computing systems and storage media

Computing devices

The computer itself is the main source of information for the investigator. In the computer, information is stored on the hard disk. A hard disk drive is a device that can record magnetic data, consisting of one or more rigid discs, read / write heads and mechanical mechanisms protected by a metal casing, hermetically sealed. The storage capacity of a hard disk is normal nowadays tens or hundreds of gigabytes. A computer may have one or more hard disks of different types and capacities.

………………………..

Computer networks

There are few computer users who have never used a network. Whether to send a message or to find certain information, increasingly more people are using networks. Both for people, as well as for business, currently being connected to a network is to be able to communicate.

Computers can perform independent almost anything, but it is more effective if available resources are shared. When it is desired that all people in an office to be able to print the documents they drafted, each person can buy a printer. It is a solution, but certainly not the happiest. It’s much easier and cheaper to buy one printer that is attached to a single computer and are shared by all others as would be connected to their computer.

It can be said that the main purpose of computer networks is to share resources. These resources are very diverse, among them are modems, printers, storage space for files, and information such as that contained in the database. From this point of view, the computers on a network are divided into **servers** (that serves resources), and customers who use them.

A network is more than two computers connected. It is the equipment, software and the people who created them. Principles of networks, however, are simple enough. Networks are classified primarily by geographical area which can be from a few meters to thousands of kilometers.

…………………………………

Software and services

Client/server architecture

Internet and most networks use the principle of client/server. Servers across the globe provide certain types of services, and clients (PCs, laptops or mobile) connects them to access the information.

The main reasons for using so wide of this architecture are:

- storing information in one place, where it can be easily redistributed to customers;
- dedication of computing resources (servers) for specific tasks such as for example email - where safety is involved moving information from one point to another.

Customers (ie those who work with computers as a network client) can have a huge variety and can be off and on without affecting the proper functioning of the network.

What should be noted first of all that the vast majority of Internet services is that there are:

- a program (software) client on the one hand;
- a server program on the other side;
- connections between client and server;
- connections between multiple servers;
- direct connections between clients.

The transfer of files from the server to client is called *downloading*, and the reverse is called *uploading*.

………………………………..

Vulnerabilities

The first attacks on the Internet

November 2, 1988 is an important day for the Internet. On that day a graduate of Cornell University in the United States, Robert Morris Jr., executed a worm type program, the first program that has affected in a very serious Internet. In seconds, thousands of computers across the United States have been out of service by the unusual program. Hundreds of networks of research institutes, universities, and of the few companies that were connected to the Internet at that time were affected.

Within a few hours was formed a volunteer group to resolve this situation as quickly as possible. Members of the group called "Virus Net" communicate with their phone and the non-affected segments of the network. After a failed effort to identify cause of the problem, they isolate the virus and find a weakness in the code. This discovery made the spread of the virus to be stopped in a record time of 24 hours after onset.

The way the program called *worm* as it propagates through the network and infected so many computers, is very simple. After infecting a computer, the program create two copies of itself in memory, whose purpose was to look for other computers that may be infected. The two copies are created every turn two copies of the virus. A simple calculation shows that for the 16th "generation" of computers there were more than 65.000 copies of the program on the infected system, and other 65.000 for other computers investigated to see if they were infected.

………………………………………..

Cybercrime laws

The concept of "cybercrime"

Cybercrime is a phenomenon of our time, often reflected in the media. One study indicates that fear of attacks even exceed the intensity to ordinary theft or fraud. Criminological research on crime made by computer systems is still under exploration. Even the most accomplished to date tend to change the way are seen the offenses in current systems of criminal justice.

Only a small proportion of criminal offenses related to the use of computer systems come to the attention of the criminal investigation bodies, so it is very difficult to achieve an overview of the extent and evolution of the phenomenon. If it is possible to achieve an adequate description of the types of offenses encountered, it is very difficult to present a synthesis based on the extent of losses caused by them, and the actual number of crimes committed. The number of cases of computer crime is growing. Thus, in Germany was evidentiated in 1996 32.128 recorded in such cases, in the Netherlands in the period 1981-1992 was found 1400 cases, and in Japan between 1971 and 1995, 6671 cases. It is estimated that only 5% of their deeds come to the knowledge of the prosecution. To counter this lack of information, was used the process of surveys. The survey conducted by the Computer Crime Institute and Federal Bureau of Investigation (FBI) in 2003 indicated losses of 201,797,340 dollars for the 538 surveyed U.S. businesses and institutions.

……………………………………

Investigations

Computer forensic investigations

Forensic investigation of computer systems has a number of features that differentiate it fundamentally from other types of investigations.

Forensic investigation of computer systems can be defined as:

> *Using scientific and safe of insurance tightening, validation, identification, analysis, interpretation, documentation and presentation of digital evidence obtained from such sources such as computer science to facilitate the discovery of truth in criminal trials.*

……………………………

Convention on Cybercrime

Council of Europe: Convention on Cybercrime - CETS No.: 185

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

……………………….

Recommendation No. R (95) 13

COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (95) 13

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURAL LAW CONNECTED WITH INFORMATION TECHNOLOGY

*(Adopted by the Committee of Ministers on 11 September 1995,
at the 543rd meeting of the Ministers' Deputies)*

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Having regard to the unprecedented development of information technology and its application in all sectors of modern society;

Realising that the development of electronic information systems will speed up the transformation of traditional society into an information society by creating a new space for all types of communications and relations;

Aware of the impact of information technology on the manner in which society is organised and on how individuals communicate and interrelate;

……………………………

Rules for obtaining digital evidence by police officers

(Source: Australasian Centre for Policing Research)

- OFFICER SAFETY COMES FIRST!
- Search any visible or broken cable. If you have doubts about the safety of handling, ask an expert.
- Make sure you have the right to frisk and lift the evidence.
- DO NOT use the keyboard or mouse.
- DO NOT attempt to examine the contents of the computer, you could alter evidence.
- Record all actions for lifting samples.
- If the computer system is closed, DO NOT open.
- If the computer system is open, shoot the screen before going further.
- DO NOT close the computer system in the normal manner. Remove the power cord from the computer directly, not from the socket. Make sure you do this safely.
- Do not ignore other types of evidence such as fingerprints on the equipment.

Standards in the field of digital forensics

(Source: Scientific Working Group on Digital Evidence)

Principle 1

In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.

Standards and Criteria 1.1
All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

....

Principles in digital evidence

(Source: International Organization on Computer Evidence)

1. In the process of obtaining digital evidence, actions taken should not alter the evidence.

2. Where it is necessary for a person to access original digital evidence, that person must be competent in terms of crime.

3. All activities related to the investigation, storage, examination or transfer of digital evidence must be fully recorded in writing, kept and available for evaluation.

4. A person is responsible for all activities related to digital evidence as long as they are in his possession.

5. Any organization responsible for investigating, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Procedures model for the forensic examination

(Source: International Association of Computer Investigation Specialists)

Hard disk examination

- Sterile conditions are established in terms of crime. All storage media used during the examination are prepared recently, cleaned of extraneous data, anti-virus checked and tested before use;

- All used software licensed and can be used by the institution;

- The original computer is physically examined. It is provided a description of the hardware that is registered. Comment any unusual item encountered during the physical examination of the computer system.

- All precautions are taken during copying or access to the original storage media in order to prevent the transfer of viruses, destructive or other inaccuracies in the content / the original storage media. It is recognized that due to hardware limitations and operating systems this is not always possible;

………………………………

Code of Ethics

(Source: International Association of Computer Investigation Specialists)

1. Maintain the highest level of objectivity in all forensic investigations and present the facts correctly;

2. Examine and analyze in detail the evidence;

3. Examine in compliance with established principles and validated by practice;

4. Issue opinions based on facts that can be reasonably demonstrated;

5. Do not hide any fact likely to remove offending or criminal liability, that might distort the elements of an investigation;

6. Do not misrepresent your education, experience and membership in professional organizations;

Contents

- Protocols and Standards
- Internet Services
- - e-Mail
- - - Spam
- - HTTP
- - Web address - URL
- - Web browsers
- - - Browser cookies
- - Working with web pages
- - - Choosing your favorite web pages
- - - Keeping track of visited web pages
- - - Saving web pages
- - Proxy servers
- - Privacy on the Internet
- FTP
- Instant Messaging
- Peer-to-peer networks

Vulnerabilities

- The first attacks on the Internet
- Cybercrime
- - Typologies of cyber attackers
- - - Classification of cyber attackers according to their skills and objectives
- Classification of risks and incidents in cyberworld
- - Classification as a list of terms
- - List of categories
- - Categories of results
- - Empirical lists
- Events, attacks and incidents
- Online security events, actions, and targets
- - Actions
- - Targets
- Attacks
- - Tools
- - Vulnerabilities
- - Unauthorized results

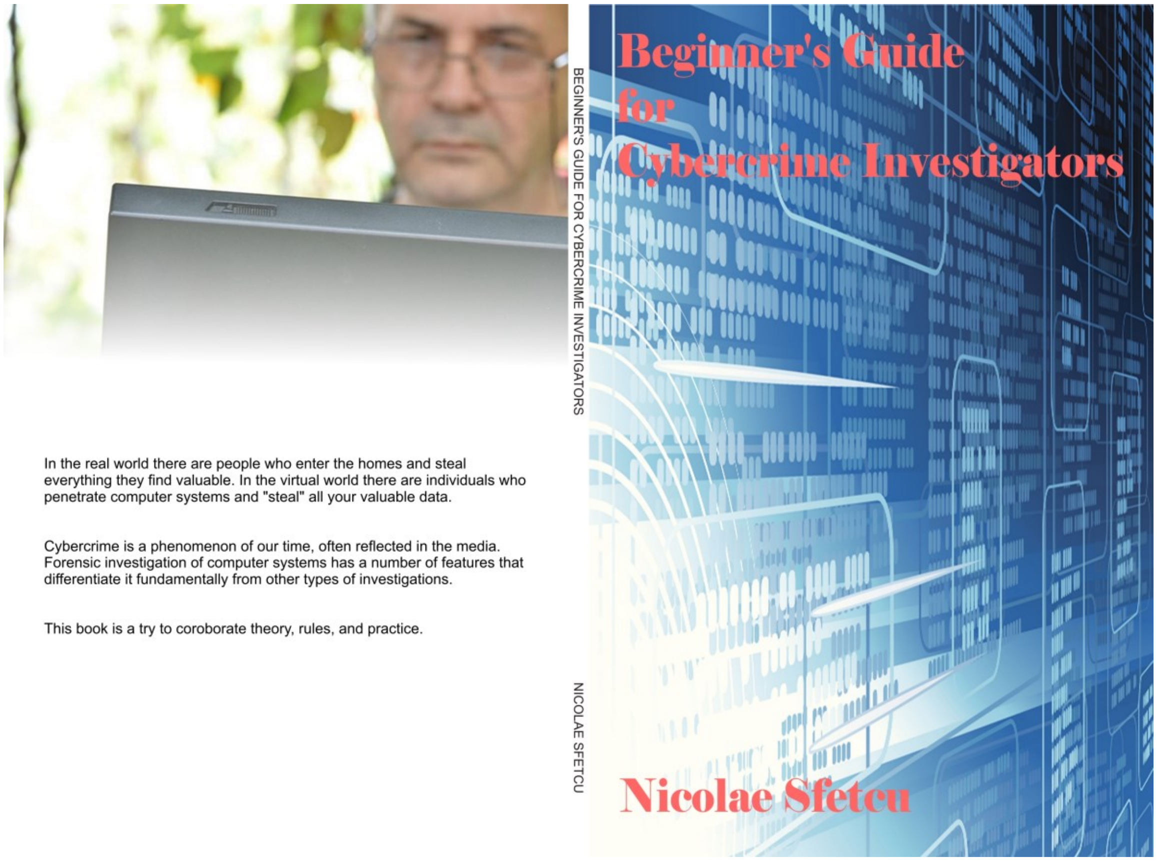
Cybercrime laws

- The concept of "cybercrime"

Investigations

- Computer forensic investigations
- Digital evidence
- Digital sampling during investigations
- The suspect
- Witnesses in cybercrime
- Transporting of samples in laboratory
- Analysis of samples
- Preparing team members

Book



In the real world there are people who enter the homes and steal everything they find valuable. In the virtual world there are individuals who penetrate computer systems and "steal" all your valuable data.

Cybercrime is a phenomenon of our time, often reflected in the media. Forensic investigation of computer systems has a number of features that differentiate it fundamentally from other types of investigations.

This book is a try to coroborate theory, rules, and practice.

BEGINNER'S GUIDE FOR CYBERCRIME INVESTIGATORS

NICOLAE SFETCU

Beginner's Guide for Cybercrime Investigators

Nicolae Sfetcu

In the real world there are people who enter the homes and steal everything they find valuable. In the virtual world there are individuals who penetrate computer systems and "steal" all your valuable data. Just as in the real world, there are uninvited guests and people feel happy when they steal or destroy someone else's property, the computer world could not be deprived of this unfortunate phenomenon. It is truly detestable the perfidy of these attacks. For if it can be observed immediately the apparent lack of box jewelry, penetration of an accounting server can be detected after a few months when all clients have given up the company services because of the stolen data came to competition and have helped it to make best deals.
Cybercrime is a phenomenon of our time, often reflected in the media. Forensic investigation of computer systems has a number of features that differentiate it

fundamentally from other types of investigations. The computer itself is the main source of information for the investigator.

MultiMedia Publishing House: https://www.telework.ro/en/e-books/beginners-guide-cybercrime-investigators/

About the author

Nicolae Sfetcu

Owner and manager with MultiMedia SRL and MultiMedia Publishing House.

Project Coordinator for European Teleworking Development Romania (ETD)

Member of Rotary Club Bucuresti Atheneum

Cofounder and ex-president of the Mehedinti Branch of Romanian Association for Electronic Industry and Software

Initiator, cofounder and president of Romanian Association for Telework and Teleactivities

Member of Internet Society

Initiator, cofounder and ex-president of Romanian Teleworking Society

Cofounder and ex-president of the Mehedinti Branch of the General Association of Engineers in Romania

Physicist engineer - Bachelor of Physics, Major Nuclear Physics. Master of Philosophy.

Contact

Email: nicolae@sfetcu.com

Facebook/Messenger: https://www.facebook.com/nicolae.sfetcu
Twitter: http://twitter.com/nicolae
LinkedIn: http://www.linkedin.com/in/nicolaesfetcu
YouTube: https://www.youtube.com/c/NicolaeSfetcu

Publishing House

MultiMedia Publishing

*web design, e-commerce and other web applications * internet marketing, SEO, online advertising, branding * software localization, English - Romanian - French translation * articles, desktop publishing, secretarial services * powerpoint, word and pdf presentation, image, audio and video editing * book and e-book conversion, editing and publishing , isbn*

Email: office@multimedia.com.ro

MultiMedia: http://www.multimedia.com.ro/
Online Media: https://www.telework.ro/

Facebook: https://www.facebook.com/multimedia.srl/
Twitter: http://twitter.com/multimedia
LinkedIn: https://www.linkedin.com/company/multimedia-srl/