

جامعة نايف العربية للعلوم الأمنية

كلية الدراسات العليا

قسم العلوم الشرطية



# مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت

" دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية "

بحث مقدم استكمالاً لمتطلبات الحصول على درجة الماجستير في قسم  
العلوم الشرطية - تخصص القيادة الأمنية

إعداد

محمد بن نصير محمد السرحاني

إشراف

الأستاذ الدكتور/ عبد الرحمن بن إبراهيم الشاعر

الرياض

١٤٢٥ هـ - ٢٠٠٤ م

/

-

:  
:



:

/ :

... :

:

( )  
( )  
( )

. . -  
. -  
. -

/ /

/ / :

:

:

:

:

:

:

:

( )  
( )  
( , )

:

( , )  
( , )  
( , )  
( , )  
( , )  
( , )  
( , )  
( , )  
( , )  
( , )

( , )

## College of Graduate Studies

**Division** : Police Science.

**Specialty**: Security leadership.

**Thesis Abstract**  **Master degree Msc.**  **Doctorate degree PhD.**

**Thesis title**: Skills of criminal investigation in computer and internet crimes.

**Prepared by**: Mohammad Nusair Alserhani.

**Supervised by**: Prof. Dr. Abdurrahman Ibrahim Asha'er.

**Thesis disputation committee** :

- 1-Prof. Dr. Abdurrahman Ibrahim Asha'er. (Supervisor & Reporter)
- 2-Dr. Abdullah Abdulaziz Almosa. (Member)
- 3- Dr. Salih Saad Assalih. (Member)

**Disputation date** : 28/04/1425 H Corresponding to 16/06/2004 G

### **Research Problem:**

Computer and internet crimes investigation needs skills of a special nature in the police officers to be capable of dealing with this kind of investigation, this subject lead us to the main question: what are the technical skills of criminal investigation in computer and internet crimes the eastern province police officers have?

### **Research Importance:**

It could be a pathway that lead us to the real skills available in the police officers in the field of investigation in the crimes of computer and internet, and a step for the workers in security fields to the importance of following the new in criminal fields. The results and findings could be of such importance for the strategic planners and for the training programs of the security departments and specially for the workers at the investigation field.

### **Research Objectives:**

To specify the technical skills which must be available in the police officers to be able to investigate in the crimes of computer and internet, and to measure the technical criminal skills which available in the eastern province police officers, and internet and noticing if there is any statistical differentials in technical skills of criminal investigation in computer and internet crimes according to the demographic changes.

### **Research Questions:**

What are the technical skills of criminal investigation in computer and internet crimes must be available in the police officers?

The availability of technical skills of criminal investigation in computer and internet crimes in the eastern province police officers.

Is there any statistical differentials in technical skills of criminal investigation in computer and internet crimes according to the demographic changes in the study?

### **Research methodology:**

I used the analytical descriptive method using comprehensive social scanning with the aid of questionnaire formula. I distributed 340 questionnaire to all police officers working in the Eastern province police administration. The percentage of returned formulas is 91.2%.

### **Important results:**

I found the following:

1. The technical level of knowledge of recognizing the computer hardware is moderate, statistically (2.961).
2. The technical level of knowledge of the basics of computer networking and its terms is low (2.250).
3. The technical level of knowledge of recognizing the different operating systems and dealing with it is low (2.383).
4. The technical level of knowledge of recognizing the different file extensions and its operating programs is low (2.194).
5. The skill level of capability to use internet services is moderate (2.603).
6. The skill level of knowing the tools and ways used in computer and internet crimes is low (1.831).
7. The skill level of knowing the important technical computer and internet security programs and tools is low (1.949).
8. The skill level of knowing the nature of these crimes is low (2.046).
9. The skill level of knowing the computer and internet crimes and the specificity of each crime is low (1.801).
10. The skill level of knowledge of some programs and tools used in the investigation in the crimes of computer and internet is low (1.974).

Dr. Amer Al-kobaisi

Head, Management Science Dept

Dr. Mohammad Abu Sak

Head, Criminal Justice Dept

Dr. Ahsan Taleb

Head, Social Science Dept

L. General Dr. Abbas Abu Shama

Head, Police Science Dept

Prof. Dr. Abdul-A'aty Alsayyad

Head, Colloge graduate studies

-

·

·

·

·

·

·

-

·

:

/

.

.

:

(

)

/

(

)

/

)

/

(

)

/

.(

-





	:
	:
	:( )
	:( )





		.
	LSD	.
		.
	LSD	.
		.
	LSD	.
		.
	LSD	.
		.
	LSD	.
		.
	( )	.
	( )	.

:

.

.

Cyberspace

.

:

"

( : )".

Cybercrime

(Digital Evidence)

.Cybercrime

Computer Security Institute

FBI

.(Richardson, 2003)

International Planning and

Research Corporation (IPR)

( , )

( , )

(IPR, 2002)

.

.

.

.

.

.

.

.

-

.

-

.

-

.

:

:

:

-

-

-

:

:

:Skills

-

)

.(

: -

:Computer -

"

( : )

PC

.Server

:The Internet -

The Federal Networking Council

" : (FNC)

/ IP

/ TCP/IP

.(FNC, 1995) "

:Cybercrime -

/

.

.

:

-

.



"

"

:

:

-

.

:

-

.

:

-

.

:

-

.

.( )

.

:

:

.

Joseph Jacquard

-

.(UN, 1999)

-

.( )

(Gustaluk, 2003)

.(Greek, 2000)

Computer-related

Computer Crime

Crime

.(Sieber, 1998)

.(Kovacich & Boni, 2000)

(Sieber,

– SRI

.1998)

–

GAO

( )

Gerald

Computer Crime

Crime by Computer

Computer Crime

Computer Fraud and

McKnight

Donn B. Parker

August Bequai

Leonard I. Krauss

Countermeasures

( )

.(Sieber, 1998)

Piracy

Hacking

Internet Worm

(Sieber, 1998) Worms

Viruses

.( )

( )

.(Sieber, 1998)

( )

.( )

.(NUA, 2002)

(Brenner, 2001)

Transnational Crime

.(Herrera, 2001)

( )

(Ajeeb, 2001) , ,

.(ISU, 2003) , ,

Networking

.(Kovacich & Boni, 2000)

( )

Convention

on Cybercrime

.(COE, 2001)

.(Roman, 2001)

:

:

.

.(Goodman, 2001)

Computer Abuse

.Computer Misuse

Harm

Information

Harm done *with*

done *to* information

Misuse Abuse

(Parker, 1998) information

( )

.

High Technology Crime

High-Tech Crime

E- E-crime Electronic Crime

(Haynes, E-cash E-commerce E-mail 2002)

Mobile New Zealand (New Zealand Police, 2003 ) Phone

( )

Philippe Drefus Informatique Information ( ) Automatique

"

)"

( :

( )

Informatique

Static

.Dynamic

Information Technology Crime

Information Systems Crime

IT-Crime

"

"

( : )

Computer Crime

Computer-related Crime

(Parke, 1998; Sieber, 1998 )

Computer Crime

.(UN, 1999)

.Internet Crime

.( )

Computer Crime

-  
) -  
(

.Cybercrime

William Gibson

Cyber

Cyber

Neuromancer

Cybernetics

Cyber

(Riemer, 2001)

Cyberspace

Cybercafe

Cybercop

Cyberlaw

Cybercrime

.(Pfaffenberger, 2001)

( )

Imaginable

Cyber

. Cyber

Brenner & )

.(Goodman, 2002 ; Etter, 2001

Computer Abuse

( )

.Informatique

Cyber

Cybercrime

/

:

:

.(Goodman, 2001)

(UN, 1999)

)

Convention on Cybercrime

(

)

.(COE, 2001

Resists Definition

"

( : )"

"

.( : )"

Cybercrime

OECD

(Sieber, " /

1998 :19)

(Roman,

.2001)

" Computer Crime

(Goodman, 2001 "

:11)

" Parker

) "

.(USSC, 1993 :1

Parker

)

"

(Parker, "

(

"

1998 :57-58)

)

) "

(

( :

( )

"

) "

Digital Evidence

( :

"

( : ) "

(Casey, 2000 :8)

.

OECD

"

( : )"

.( )

"

)"

( :

( )

.

( )

.

"

( : )"

"

( : )"

:

-

-

.

.

.

.

.

.

.

.

.

.

.

.

:

/

.



( ) :

(

.( ) .

.( )

( )

.( )

( )

)

.(

//

// /

( )

( )

:

:

(Kovacich &

.Boni, 2000)

:

:

-

: Malicious Code

(Grimes, 2001)

.symantec.com

:

:Virus -

"

"

(Skoudis & Zeltser, 2003)

.( )

.(Bagnall *et al.*, 2000)

.

.

.

.

(Grimes, 2001)

:Trojan Horse -

(Grimes, 2001)

.

:Backdoor -

(Skoudis & Zeltser, 2003)

.(Smith & Komar, 2003)

Trapdoor

.(Smith & Komar, 2003)

.(Chirillo, 2002 b)

.(Skoudis & Zeltser, 2003)

:Worm -

(Grimes, 2001)

.(Bagnall, *et. al.* 2000)

.(Denning, 1999)

: -

.(Oppliger, 2003)

(Denning, 1999)

.

**:Hacking/Cracking** -

Hacker

Hacking

(Taylor, 2002)

MIT

.(Levy, 2001)

"

(Intranet)

(PC-Server)

"

.( : )

.(Denning, 1999)

.  
**:Unauthorized Use**

-

.(Icove *et al.*, 1995)

.( )

**:Denial of Service Attacks**

-

DoS

.(Cole, 2002)

" :

grc.com

(Gibson, "

.2002)

DoS

Distributed Denial of Service

DDos

.(Fithen, 2000)

.(Tulloch, 2003) Zombie

.(Vacca, 2002)

**:Phreaking**

-

Phreaker

(Furnell, 2002)

.(Shinder, 2002)

**:Data Sabotage**

-

"

.(Furnell, 2002) "

Crackers

.(Stephenson, 2000)

(Denning, 1999)

.

**:Data Theft/Alteration**

-

( )

.(Shinder, 2002)

**:Identity Theft**

-

"

.(Vacca, 2003 :4) "

.(Bidwell, 2002)

.(Mchlein, 2003)

.(Lane, 2002)

**:Cyberfraud**

-

.(Schneier, 2000)

Cyberfruad

eBay.com

.(Goodman & Brenner, 2002)

.(Denning, 1999)

**:Embezzlement** -

.(Shinder, 2002)

.(Denning, 1999) Salami

**:Harassment** -

.(Denning, 1999)

)

.(

Stalking

(Goodman & Brenner,

.2002)

:

-

.

.( )

( )

.

.( ) Chain Letters

.( )

.( )

.

**:Pornography**

-

.Child Pornography

.( )

.( )

Proxy

.

:

-

.( )

E-Mail Forgery

.

POP

Webmail

.(Denning, 1999)

IP Address

.(Stephenson, 2000)

Remailers

.(Shinder, 2002)

(Denning, 1999) E-Mail Flooding

.(Shinder, 2002) E-Mail Bombing

**:Software Piracy**

-

.(Shinder, 2002)

.( )

.( )

.Crack

**:Internet Gambling** -

(Shiple, 2002)

,  
.(Creer, 2003)

:

:

.(Creer, 2003)

(GAO, 2002)

**:Cyber-Terrorism**

-

.( )

(Erbschloe, 2001)

.(Denning, 2000)

:

-

"

(Stansell- "

**Gamm, 2002)**

"

Denning, ) "

.(1999

:(Furnell, 2002)

: .

: .

: .

: .

Denning, ) "

"

.(1999

Chameleon

.(Furnell, 2002)

Cyberwar

.(Denning, 2001)

**:Cyber-Laundering** -

"

.( : )"

( )

Cyberbanking

.( )

(Lilley, 2000)

,

,

,

.( : )

**:Cyber-Espionage** -

.(Icove *et al.*, 1995)

(Stephenson,

.2000)

.(Power, 2000)

:

.(The HoneyNet Project, 2002)

Tools

Methods

-:

**:Social Engineering**

-

(Cole, 2002)

.(Mitnick & Simon, 2002)

.(Chirillo, 2002 b)

**:Port Scanning -**

Listening

(McClure *et al.*, 2001)

.(Chirillo, 2002 a)

Idle Scanning

Stealth SYN Scan

Erickson, )

Spoofing Decoys

.(2003

Port Scanners

Super Scanner WinScan

.(McClure *et al.*, 2001)

netcat nmap

## **:Password Cracking**

-

.(Garfinkel *et al.*, 2003)

.(Denning, 1999)

root

.(Chirillo, 2002b)

Dictionary Attack

Brute-Force Attack

(Cole, 2002)

L0phtCrack Webcrack Unsecure

.(Chirillo, 2002 b)

## **:Packet Sniffing**

-

Sniffers

(Shema & Johnson, 2004)

.(Skoudis, 2002)

sniffit tcpdump

EtherPeek Ethereal Windump

.(Rubin, 2001)

SuperSniffer Ethereal

**:Vulnerability Scanning**

-

.(Furnell, 2002)

Bugs

.(Cronkhite & McCullough, 2001)

.... Titan SAINT SATAN

.

**:War Dialing**

-

(Schwartau, 2000)

( )

.(Furnell, 2002)

THC-Scan

Toneloc

.(Tulloch, 2003)

**:Remote Administration**

-

.(Furnell, 2002)

.

.(Tulloch, 2003) Back Orifice Net Bus Sub 7

**:Keystroke Monitoring**

-

.(Denning, 1999)

Keystroke Loggers

Hardware

Keyghost

.(Shinder, 2002) Data Interception Spector Pro

**:Buffer Overflows** -

.(Cole, 2002)

)

++ (

.(Chuvakin & Peikari, 2004)

**:Session Hijacking** -

McClure *et al.*)

.(*al.*, 2001)

.Hunt Juggernaut

(Cole, 2002)

**:IP Spoofing** -

(Shinder, 2002)

.(Stephenson, 2000)

IP Address

.(Schwartau, 2000)

**:Anonymity** -

IP Address

Remailers

(Denning, 1999)

(Jamsa, 2002) Anonymizers

**:Cryptography** -

)

(

.(Denning & Baugh, 1999)

Littman

DES

.(Littman, 1997)

.(Hollis *et al.*, 2001)

**:Steganography**

-

(Denning, 1999)

.(Shinder, 2002)

StegoDos Steganos Hide and Seek

.(Vacca, 2002) SFS

.(Denning, 1999)

.(Shinder, 2002)

:

-

.(Stephenson, 2000)

:(Icove, *et al.*, 1995)

Log Files

Computer Manuals

. . . . .

.(Kabay, 2002)

(Icove *et al.*,

1995)

Firewall Systems

Antivirus Systems

Intrusion Detection Systems

- -

.(Mandia & Prosise, 2001)

-

(Icove *et al.*, 1995)

.(Mandia & Prosise, 2001)

-

.(Icove *et al.*, 1995)

:

:

-

eUniverse

.

Maxus

,

,

,

.(ZDNet News, 2000)

-:

-

Adrian

.

Lamo

.(McCullagh, 2003)

.

:

"

.( : )"

.( )

.

:

-

:

:

-

.

.(Hollis *et al.*, 2001)

FBI

CSI

.(Richardson, 2003)

( )

.(Kabay, 2002)

-:

-

.(Goodman, 2001)

-

.( )

-

(Cowens &

Miora, 2002)

.(Stephenson, 2000)

-

.(Goodman, 2001)

-

( )

.

-

.

:

-

.(Stucki, 2002)

.

(Sterneckert,

:2004)

.

.

.

.

.

.

.

.

.

.

.....

.(Middleton, 2002)

:

-

-

-

;(Middleton, 2002)

-

-

-

: :

(Icove *et al.*,

.1995)

: -

.(Icove *et al.*, 1995)

:  
: -

(Platt, 2002)

(The White House, 2003)

)

.(

Guidelines

.

:

-

.

(Konvacich & Boni, 2000)

.

:(Schultz & Shumway, 2002)

:

-

.

:

-

.

·  
:

·  
:

·  
:

·

·

·  
:

·  
:

·

(Icove *et al.*, 1995)

)

.(

-

(Mandia

.

: & Prosis, 2001)

.

-

.

-

.

-

.

-

.

-

.

-

.

-

.

-

-

(Schultz & Shumway, 2002)

.(Wright, 2000 d)

-

.( )

:

:

.(Groover, 1996)

.

.

...

.( )

.(Erdonmez, 2002)

.( )

.

:

:

.

:

. ....

:

:

.(Icove *et al.*, 1995 ; Wright, 2000 d )

:

)

.(Icove *et al.*, 1995

:

Icove *et*

)

.(*al.*, 1995

:Financial Auditor

Icove *et al.*, 1995 ; Stephenson, )

.(2000

:

.(Wright, 2000 d )

:

)

.(

( )

:

.(Wright, 2000 d)

.

( ) :

"

.( : )"

( )

.( )

.

:( )

:

.

.

:

.

.

:(Wright, 2000 b)

.

.

.

.

.

.

.

.

.

.

.

.

(Sammes & Jenkinson, 2002)

Hardware

(Casey, 2000) Software

.(Shinder, 2002)

.(Wright, 2000 a)

(Vacca, 2002)

(Shinder, 2002)

(Wright, 2000 f)

.(Wright, 2000 e)

(NIJ, 2001)

)

(

.(Champlain, 2003)

CD-Rom

.(Casey, 2000)

:(Wright, 2000 c)

Bit

(Vacca, 2002) Bit Stream Back-up

(Smith & Komar, 2003)

(Kruse & Heiser, 2002)

.(Brenner & Frederickson, 2002)

:

A4

(Sammes & Jenkinson, 2002)

.

)

.(

-

-

(AME Info, 2003)

.

-:

-: (Hardware)

.(Casey, 2000) ....

-: (Software) .

(Sammes & Jenkinson, 2002)

: .

)

.(

-:

-: .

.(Casey, 2000) Flash Memory

Manuals .

.( )

.(Casey, 2000)

(Sammes &

.Jenkinson, 2002)

:

.

-:

:

. :

: :

Logs

.

-:

**: Firewall -**

(Cheswick *et al.*, 2003)

.(Black, 2000)

Logs

.(Northcutt *et al.*, 2001)

.

**:Proxy Server -**

# Application Gateway

.(Northcutt *et al.*, 2003)

(Brenton & Hunt, 2003)

.(Shinder, 2002)

## Cache

(Hall, 2000)

(Stanger *et al.*, 2001)

.

.(Zwicky *et al.*, 2000)

Logs

**:Intrusion Detection System**

-

IDS

.(Bace, 2000)

(Signature)

Logs

(Northcutt & Novak, 2003)

**: Honeypot -**

(Spitzner, 2003)

**: Auditing Tools -**

Logs

(Champlain, 2003)

syslogd                      Event Viewer

:

:

-:

: -

BitStream Backup

.(Vacca, 2002)

ProDiscover Encase Safeback  
.(Casey, 2000) DD (Shinder, 2002)

: -

(Mandia & Prorise, 2001)

String etSearch .  
. Search

: -

.(Shinder, 2002) Format

Extractor GetFree  
.(Shinder, 2002)

**:Hexadecimal Editors** -

(Sammes & Jenkinson,

.WinHex

Gander

2002)

:

-

Office

Password Recovery Suit

Recovery Enterprise

Advanced PDF Password Recovery Pro

Advanced Archive Password Recovery

. .Ace .Rar .Zip

:

-

(Mandia & Prosis, 2001) Tracing Back

(Stephenson, 2000)

Tracert

Traceroute

NT/2000 /XP

Visualroute

Neotrace Pro

Domain Name

IP Address

.ACDSee ThumsPlus

(Sammes & Jenkinson, 2002)

Quick View Plus

.Compressing

.

Gzip

Winace Winrar Winzip

:

-

.

.(Shinder, 2002)

:

.

)

.(

.(Sterneckert, 2004)

(Mclean, 2002)

.(Shinder, 2002)

.( )

:

Cyberspace

.(Mendell, 1998)

)

:(

.  
. .  
. .  
. .  
. .  
. .  
. .  
. .

:( )

. : .  
. : .

.

(Strang,

.2002)

IP

( )

ISP

Address

.

( )

.

.(Davis, 1998)

.

)

.(

Tracing-Back

Visualroute

( )

.

.

Mandia & )

.(Prorise, 2001

.FBI

Carnivore

.(Smith *et al.* 2000)

Sniffing

(Holland, 2002)

Ahmad *et al.* )

.(2002

( )

( )

.( )

.

.

:

-

.

-

.

-

.

-

.

-

.

:

:

-

(Erbschloe, 2001)

(NIJ, 2001)

DVD

CD-Rom

.

(USSS, 2002)

( )

(Thompson, 1990)

.

(Kruse & Heiser, 2002)

.(IOCE, 2000)

:

-

.(Morrison, 1990)

DHCP

.(Shinder, 2002) Client/Server

TCP/IP

Peer-to-Peer Networks

.(Shinder, 2002)

:

-

ISTS, )

.(2002

.(Sammes & Jenkinson, 2002)

(Shinder, 2002)

/

:

-

Format

( )

(Vacca, 2002)

( )

		*.doc
		*.htm *.html
Real Player		*.rm *.ram
XingMPEG		*.mpeg *.mpg

		*.wmv
		*.gif
		*.jpg
/	Winzip	*.zip
/	Winrar	*.rar

.(Sammes & Jenkinson, 2002)

:

-

.(David, 1998)

Chatting

Furnell, )

.(2002

.(Stephenson, 2000)

.(Thompson, 1991)

:

-

.(Denning, 1999)

(Shinder, 2002)

.(Vacca, 2002)

:

-

.

.(Shinder, 2002)

IDS

Firewall

Proxy Server

Tracing

:

-

:

-

-

-

-

-

Safeback Encase (Smith & Komar, 2003)

(Chirillo, 2002 a)

DD

ACDSee ThumpsPlus

(Kruse & Heiser, 2002)

Winrar Winzip

:

( )

.

( )

Hardware

( )

( , )

( , )

( , )

( )

( )

.

( )

.

.

.

( )

.

.

(Erdoğan, 2002)

DNA

Dartmouth College

(ISTS, 2002)

Cyber-attack

IP Address

Spoofing

DDoS

Sniffing

Steganography

Signature

Root kits

( )

( )

(Furnell, 2002)

(Erbschloe, 2001)

Cyber-attackers

(Etter, 2001)

(Smith, 2001)

(Hollis *et al.*, 2001)

(Wahlert, 1998)

(Goodman, 1997)

Technophobia

(Thompson, 1991)

(Carter & Katz, 1996)

(Groover, 1996)



(Kelly, 1995)

(Thompson, 1990)







.

.

:

.( )

)

.(

:

:

:

.

:

.( -

.

:

.

:

:

. ( )

:

:

( )

.( , )

( , )

:

:

:  
:-

( ) : -  
: ( )

. ( ) : -  
. ( ) : -  
( ) : -

( ) : -

. ( ) : -  
: -

. ( ) : -  
( ) : -

( ) : -

. ( ) : -  
: -

. ( )

(Closed Questionnaire)

“Likert scale” ( )

“ ”

( )

)

(

)

)

(

.(

:

-

:( )

-

( )

:

-

(Pearson “ ”

Correlation)

.( )

( )



: -

( )

( , )

(Cronbach's Alpha)

.( )

( )

,	( )
,	( )
,	( )
,	( )
,	( )
,	( )
,	( )
,	( )
,	( )
,	( )
,	( )
,	( )

:

:

-

-

( )

-

.( , ) ( ) -

-

:

(SPSS) (Statistical Package for Social Sciences)

:

(Pearson Correlation) " "

-

-

-

( )  
( ) , ( ) ,  
( , ) , ( ) ,  
( ) ( , ) ,

-

(T-test) ( ) -

- ( )

-

(One-way ANOVA) ( ) -

( )

(Least-significant difference) LSD -

(Chi-Square) -



(SPSS) (Statistical Package for Social Sciences)

:

( )

( )

: ( )

-

( )

,		
,		

,		
,		
,		
,		
,		
,		

( , )

( )

( , )

( , )

( , )

( , )

( , )

( , )

.

( , )

.( )

( )

,		
,		
,		
,		
,		

( )

( , )

( , )

( , )

( , )

( , )

( )

,		
,		-
,		-
,		-
,		
,		

( )

( , )

( , )

( , )

( , )

( , )

( , )

( )

,		
,		-
,		-
,		



,		
,		

( )

( , )

( , )

( , )

( , )

( )

,		
,		
,		-
,		
,		

( )

( , )

( , )

( , )

( , )

( )

,		

,		
,		

( )

( , )

( , )

( , )

.

( )

,		
,		
,		

( )

( , )

( , )

( , )

.

.

( )

,		
,		
,		-
,		-
,		
,		

( )

( , )

( , )

( , )

( , )

( , )

( , )

( )

,		
,		
,		-
,		-
,		-
,		
,		

( )

( , )

( , )

( , )

( , )

( , )

( , )

( , )

( )

,		
,		
,		-
,		-
,		-
,		
,		

( )

( , )

( , )

( , )

( , )

( , )

( , )

( , )

( )

,		

,		
,		-
,		-
,		-
,		
,		

( )

( , )

( , )

( , )

( , )

( , )

( , )

.

:

.

.

( )

:

:

( )

				( )	( )	( )	( )	( )		
	'	'	' **							(Desktop, Laptop, Notebook, Handheld, Tablet PC)
	'	'	' **							( )
	'	'	' **							CD- DVD Rom
	'	'	' **							) Flash Memory Backup Tapes
	'	'	' **							Analog Modem, ) (DSL Modem
	'	'	' **							Hub, Repeater, Router, ) (Switch
	'	'	' **							

( , ) \*\*

( )

( , )

:

: ( , - , )

:

(Desktop, Laptop, Notebook, Handheld,

-  
Tablet PC)

( , )

( , )

( , )

( , )

( , )

( , )

( )

-

( , )

( , )

( , )

( , )

( , )

( , )

DVD

CD-Rom

-

( , )

( , )

( , )

( , )

( , )

( , )

)

-

(Backup tapes

Flash Memory

( , )

( , )

( , )

( , )

( , )

( , )

(Analog Modem, DSL Modem)

-

( , ) ( , )

( , )

( , )

( , )

. ( , )

,

:

:

(Hub, Repeater, Switch)

-

( , ) ( , )

( , )

( , )

( , )

. ( , )

-

( , )

( , )

( , )

( , )

( , )

. ( , )

:

-

( )

				( )	( )	( )	( )	( )		
	'	'	**							IP Address
	'	'	**							Port
	'	'	**							Server
	'	'	**							Client
	'	'	**							Data Packet
	'	'	**							Bandwidth
	'	'	**							TCP/IP
	'	'	**							DHCP
	'	'	**							Peer-to- / Peer Networks

( , ) \*\*

( )

( , )

:

( , )

IP Address

-

( , )

( , )

( , )

( , )

( , )

( , )

.

Port -

	( , )	( , )	
	( , )	( , )	
( , )			( , )

.

Server -

	( , )	( , )	
	( , )	( , )	
( , )			( , )

.

Client -

	( , )	( , )	
	( , )	( , )	
( , )			( , )

.

Data Packet -

	( , )	( , )	
	( , )	( , )	
( , )			( , )

.

Bandwidth -

	( , )	( , )	
( , )	( , )		
			( , )
			( , )

.

TCP/IP -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

DHCP -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

Peer-to-Peer Networks -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

:

( )

				( )	( )	( )	( )	( )		
	'	'	'							XP
	'	'	'							/
	'	'	'							
	'	'	**'							

										MS Dos
			**							Macintosh (OS 8/9, OS X)
			**							Linux (any distribution)
			**							UNIX (any flavor)

( , ) \*\*

( )

( , )

:

: ( , - , )

:

XP

-

( , )

( , )

( , )

( , )

( , )

. ( , )

/

-

( , )

( , )

( , )

/

( , )

( , )

. ( , )

/

-

( , )

( , )

( , )

( , ) ( , )

. ( , )

MS Dos -

( , ) ( , )

( , ) ( , )

( , )

. ( , )

Macintosh (OS 8/9, OS X) -

( , ) ( , )

( , ) ( , )

( , )

( , )

.

Linux (any distribution) -

( , ) ( , )

( , ) ( , )

( , )

( , )

.

Unix (any flavor) -

( , ) ( , )

( , ) ( , )

( , )

. ( , )

( )

				( )	( )	( )	( )	( )	
	'	'	**						*.doc
	'	'	**						*.zip
	'	'	**						*.htm *.html
	'	'	**						*.jpg
	'	'	**						*rm *.ram
	'	'	**						*.rar
	'	'	**						*mpg *.mpeg
	'	'	**						*.pdf
	'	'	**						*.wmv

( , ) \*\*

( )

( , )

,

:

\*.doc -

( , )

( , )

( , )

( , )

\*.doc

( , )

. ( , )

\*.zip -

( , ) ( , )

( , ) ( , ) \*.zip

( , )

. ( , )

\*.htm \*.html -

( , ) ( , )

( , ) \*.html \*.htm

( , )

( , )

. ( , )

\*.jpg -

( , ) ( , )

( , ) ( , ) \*.jpg

( , )

. ( , )

\*.rm \*.ram -

( , ) ( , )

( , ) \*.ram \*.rm

( , )

( , )

. ( , )

\*.rar -

( , ) ( , ) ( , )  
( , ) ( , ) \*.rar  
( , )  
( , )  
\*.mpg \*.mpeg -  
( , ) ( , )  
( , ) \*.mpeg \*.mpg  
( , ) ( , )  
( , )  
\*.pdf -  
( , ) ( , )  
( , ) ( , ) \*.pdf  
( , )  
( , )  
\*.wmv -  
( , ) ( , )  
( , ) \*.wmv  
( , ) ( , )  
( , )

( )

-

				( )	( )	( )	( )	( )		
	'	'	**	'						Browsing
	'	'	**	'						E-Mail
	'	'	**	'						Search Engines
	'	'	**	'						( ) Instant Messaging
	'	'	**	'						IRC
	'	'	**	'						Voice Chat
	'	'	**	'						FTP
	'	'	**	'						Newsgroups
	'	'	**	'						Telnet
	'	'								

( , ) \*\*

( )

( , )

:

: ( , - , )

:

Browsing

-

( , )

( , )

( , )

( , )

( , )

( , )

.

E-mail

-

( , )

( , )

( , )

( , )

( , )

. ( , )

Search Engines

-

( , )

( , )

( , )

( , )

( , )

. ( , )

Instant Messaging ( )

-

( , )

( , )

( , )

( , )

( , )

( , )

.

IRC

-

( , )

( , )

( , )

( , )

( , )

( , )

.

Voice Chat

-

( , )

( , )

( , )

( , )

( , )

( , )

.

: ,

:

FTP

-

( , )

( , )

( , )

( , )

. ( , )

( , )

Newsgroups

-

( , )

( , )

( , )

( , )

( , )  
( , )

Telnet -

( , ) ( , )  
( , ) ( , )  
( , )

( , )

.

( )

-

									/
				( )	( )	( )	( )	( )	
	,	,	**						Computer Virus
	,	,	**						Computer Worm
	,	,	**						Trojan Horse
	,	,	**						Password Crackers
	,	,	**						Network Scanners
	,	,	**						E-Mail Flooders
	,	,	**						Key Loggers
	,	,	**						Packet Sniffers
	,	,	**						IP Spoofing
	,	,	**						Wardialers
	,	,	**						CC Numbers Generator
	,	,	**						Anonymity
	,	,	**						Social Engineering

( , ) \*\*

( )

( , )

,

:

Computer Virus

-

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

Computer Worm -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

Trojan Horse -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

Password Crackers -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

Network Scanners -

( , ) ( , ) ( , ) ( , ) ( , ) ( , )

E-Mail Flooders

-

( , ) ( , )  
 ( , ) ( , )  
 . ( , ) ( , )

Key Loggers

-

( , ) ( , )  
 ( , ) ( , ) ( , )  
 . ( , ) ( , )

Packet Sniffers

-

( , ) ( , )  
 ( , ) ( , )  
 . ( , ) ( , )

IP Spoofing

-

( , ) ( , )  
 ( , ) ( , ) ( , )  
 . ( , )

Wardialers

-

( , ) ( , )  
 ( , ) ( , )

( , )

( , )

### CC Numbers Generator

-

( , )

( , )

( , )

( , )

( , )

( , )

### Anonymity

-

( , )

( , )

( , )

( , )

( , )

( , )

.

### Social Engineering

-

( , )

( , )

( , )

( , )

( , )

( , )

( )

										/	
				( )	( )	( )	( )	( )			
	'	'	**	'							Antivirus Software
					'	'	'	'	'		
	'	'	**	'							Firewalls
					'	'	'	'	'		
	'	'	**	'							Data Backup
					'	'	'	'	'		
	'	'	**	'							Antispam Software
					'	'	'	'	'		
	'	'	**	'							Antitrojan Software
					'	'	'	'	'		
	'	'	**	'							Undelete/ Unerase Tools
					'	'	'	'	'		
	'	'	**	'							Http Proxy Server TCP
					'	'	'	'	'		
	'	'	**	'							Intrusion Detection Systems
					'	'	'	'	'		
	'	'	**	'							Computer Security Auditing
					'	'	'	'	'		
	'	'	**	'							Connection Source Tracing
					'	'	'	'	'		
	'	'	**	'							E-Mail Tracing
					'	'	'	'	'		
	'	'									

( , ) \*\*

( )

( , )

,

:

Antivirus Software

-

( , ) ( , )  
( , ) ( , )

( , )  
( , )

Firewalls

-

( , ) ( , )  
( , ) ( , )  
( , )

( , )

Data Backup

-

( , ) ( , )  
( , ) ( , )

( , )  
( , )

Antispam Software

-

( , ) ( , )  
( , ) ( , )

( , )  
( , )

Antitrojan Software

-

( , ) ( , )  
( , ) ( , )  
( , )

( , )

Undelete/ Unerase Tools

-

( , ) ( , )  
( , ) ( , )

( , )

( , )

Http Proxy Server

TCP

-

( , ) ( , )  
( , ) ( , )

( , )

( , )

Intrusion Detection Systems

-

( , ) ( , )  
( , ) ( , )

( , )

( , )

Computer Security Windows

-

( , ) ( , )  
( , ) ( , )

( , )

( , )

Connection Source Tracing

-

( , ) ( , )  
 ( , ) ( , )

( , )  
 ( , )

E-Mail Tracing

-

( , ) ( , )  
 ( , ) ( , )

( , )  
 ( , )

-

( )

				( )	( )	( )	( )	( )		
	'	'	**							
	'	'	**							
	'	'	**							
	'	'	**							
	'	'	**							
	'	'	**							
	'	'	**							
	'	'	**							
	'	'								

( , ) \*\*

( )

( , )

:

,

-

( , )

( , )

( , )

( , )

( , )

.

( , )

-

( , )

( , )

( , )

( , )

( , )

.

( , )

-

( , )

( , )

( , )

( , )

( , )

.

( , )

-

( , )

( , )

( , )

( , )

( , )

.

( , )

-

( , )

( , )

( , )

( , )

( , )

( , )

-

( , )

( , )

( , )

( , )

( , )

( , )

.

-

( , )

( , )

( , )

( , )

( , )

( , )

.

( )

				( )	( )	( )	( )	( )		
	'	'	**							
	'	'	**							
	'	'	**							Hacking
	'	'	**							Denial of Service
	'	'	**							E-Mail Hacking
	'	'	**							E-Mail Flooding
	'	'	**							
	'	'	**							Data Sabotage
	'	'	**							
	'	'	**							Data Theft
	'	'	**							
	'	'	**							E-Mail Forgery
	'	'	**							Software Piracy
	'	'	**							Sniffing
	'	'	**							Fraud and Embezzlement
	'	'	**							Phreaking
	'	'	**							
	'	'	**							Identity Theft
	'	'	**							Cyber-Terrorism

( , ) \*\*

( )

( , )

,

:

-

( , )

( , )

( , )

( , )

( , )

. ( , )

**Hacking/Cracking**

-

( , )

( , )

( , )

( , )

( , )

. ( , )

**Denial of Service (DoS)**

-

( , )

( , )

( , )

( , )

( , )

. ( , )

**E-Mail Hacking**

-

( , )

( , )

( , )

( , )

( , )

. ( , )

E-Mail Flooding

-

( , )

( , )

( , )

( , )

( , )

. ( , )

-

( , )

( , )

( , )

( , )

( , )

. ( , )

Data Sabotage

-

( , )

( , )

( , )

( , )

( , )

. ( , )

-

( , )

( , )

( , )

( , )

( , )

. ( , )

Data Theft/Alteration

-

( , ) ( , )  
( , )

( , ) ( , )  
( , )

Pornography

-

( , ) ( , )  
( , )

( , ) ( , )  
( , )

E-Mail Forgery

-

( , ) ( , )  
( , ) ( , )

( , )  
( , )

Software Piracy

-

( , ) ( , )  
( , ) ( , )

( , ) ( , )  
.

Sniffing

-

( , ) ( , )  
( , )

( , ) ( , )  
( , )

Fraud and Embezzlement

-

( , )  
( , )

( , )  
( , )

( , )  
( , )

Phreaking

-

( , )  
( , )

( , )

( , )

( , )

( , )

-

( , )  
( , )

( , )

( , )

( , )

( , )

Identity Theft

-

( , )  
( , )

( , )

( , )

( , )

( , )

Cyber-Terrorism

-

( , )      ( , )      ( , )  
( , )      ( , )

( , )  
.      ( , )

( )

				( )	( )	( )	( )	( )		/
	'	'	**							/
				'	'	'	'	'		Gzip ) (Winzip Winrar
	'	'	**							(Thumps Plus)
				'	'	'	'	'		(Quick View Plus)
	'	'	**							(dtSearch)
				'	'	'	'	'		Archive ) MS PDF Files ( Office Files
	'	'	**							SafeBack DD ) (Ghost
				'	'	'	'	'		VisualRoute ) (Traceroute
	'	'								

( , ) \*\*

( )

( , )

,

:

Winar Gzip Winzip

/

-

( , )

( , )

( , )

/

( , )

( , )

( , )

/

(Thumps Plus)

-

( , )

( , )

( , )

( , )

( , )

( , )

(Quick View Plus)

-

( , )

( , )

( , )

( , )

( , )

( , )

(dtSearch)

-

( , )

( , )

( , )

( , )

( , )

( , )

.

MS Office PDF Archieve Files

-

Files

( , )

( , )

( , )

( , )

( , )

( , )

Ghost Safeback DD

-

( , ) ( , )

( , )

( , )

( , )

( , )

Traceroute VisualRoute

-

( , )

( , )

( , )

( , )

( , )

( , )

.

:

.

( )

	( )				
**	'	'	'	'	
		'		'	
				'	

( , ) \*\*

( )

.

( )

LSD

							'		
							'		
	*						'		
							'		
							'		
							'		
							'		

\*

( )

.

.

( )

	( )				
**	'	'		'	
		'		'	
				'	

( , ) \*\*

( )

.

( )

LSD

				'		
				'		
*				'		
				'		

\*

( )

.

.

( )

	( )				
'	'	'		'	
		'		'	

				,	
--	--	--	--	---	--

( )

( , )

( )

	( )				
,	,	,		,	
		,		,	
				,	

( )

( , )

( )

	( )				
* ,	,	,		,	
		,		,	
				,	

( , ) \*

( )

( )

LSD

			/		
*			/		
			/		

\*

( )

( )

	( )				
**	/	/		/	
	/	/		/	
				/	

( , )

\*\*

( )

( )

LSD

			/		
			/	-	
		*	/		

\*

( )

.

( )

.

	( )				
**	/	/	/	/	
	/	/	/	/	
	/	/	/	/	

( , )

\*\*

( )

.

( )

LSD

				/		
				/		
				/	-	

			*	,		
--	--	--	---	---	--	--

\*

( )

( )

	( )				
**	,	,		,	
		,		,	
				,	

( , )

\*\*

( )

( )

LSD

					,		
					,		
					,		-
					,		-
				*	,		

\*

( )

. -

( )

	( )				
**	'	'		'	
		'		'	
				'	

( , ) \*\*

( )

.

( )

LSD

						'		
						'		
						'	-	
						'	-	
						'	-	
					*	'		

\*

( )

.

. -

( )

	( )				
**	'	'		'	
		'		'	

					,	
--	--	--	--	--	---	--

( , ) \*\*

( )

.

( )

LSD

						,		
						,		
						,	-	
						,	-	
						,	-	
					*	,		

\*

( )

.

. -

( )

	( )				
**	,	,	,	,	
		,		,	
				,	

( , ) \*\*

( )

( )

LSD

						,		
						,		
						,	-	
						,	-	
						,	-	
					*	,		

\*

( )

( )

( )

	( )				
**	,	,	,	,	
		,	,		

( , ) \*\*

( )

-

( )

( )

	( )				
** ,	,	,	,		
		,	,		

( , )

\*\*

( )

.

.

:

(Desktop, Laptop, Notebook, Handheld, Tablet PC)

CD-Rom ( )

DVD

Flash Memory )

(Analog Modem, DSL

(Backup tapes

.Modem)

(Hub, Repeater, Switch)

(Erbschle,

2001)

Data

Server

Port

IP Address

TCP/IP

Bandwidth

Packet

Peer-to-Peer

Networks

DHCP

(Erdonmez, 2002)

( )

/ XP

.

Linux (any (Macintosh (OS 8/9, OS X MS Dos  
Unix (any flavor) distribution)

(ISTS, 2002)

.

\*.ram \*.jpg \*.htm \*.html \*.zip \*.doc  
\*.wmv \*.pdf \*.mpg \*.mpeg \*.rar \*.rm

(Smith, 2001)

.

Search E-mail Browsing  
.IRC Instant Messaging ( ) Engines

Newsgroups FTP Voice Chat  
Telnet

(Erdonmez, 2002)

( )

.

Computer Virus

Password

Trojan Horse

Computer Worm

E-Mail

Network Scanners

Crackers

Packet

Key Loggers

Flooders

Wardialers

IP Spoofing

Sniffers

Anonymity

CC Numbers Generator

Social Engineering

( )

.

Firewalls

Antivirus Software

Antispam Software

Data Backup

Undelete/Unerase Tools

Antitrojan Software

Intrusion

Http Proxy Server TCP

Event

Computer Security Windows

Detection Systems

Connection Source Tracing

Viewer

E-Mail Tracing

(Furnell, 2002)

.

( )

(Erdonmez, 2002)

Denial of Service (DoS)

Hacking/Cracking

E-Mail Flooding

E-Mail Hacking

Data Sabotage

Data Theft/Alteration

Software

E-Mail Forgery

Pornography

Fraud and

Sniffing

Piracy

Phreaking

Embezzlement

Cyber-Terrorism

Identity Theft

(Wahlert, 1998)

/

(Thumps

Winar Gzip Winzip

(Quick View Plus)

Plus)

Archive

(dtSearch)

Ghost Safeback DD

MS Office Files PDF Files

Traceroute VisualRoute

(Etter, 2001)

(Goodman, 1997)

( , )

(Thompson, 1990)

(Hollis *et al.*, 2001)

( )

( )

.

.

.

.



•

•

-

•

-

•

-

•

-

•

-

•

-

•

-

.

-

.

-

.

-

.

.



⋮

.( )

.

⋮

.( )

.

.

⋮

.

.( )

.

.( )

.

-

( )

.

.( )

.

-

( )

.

⋮

.

-

⋮

.( )

.

.( )

.

⋮

.( )

.

.

⋮

.( )

.

⋮

.( )

.

.

⋮

.( )

⋮

.

⋮

.( )

.

⋮

.( )

.

⋮

.





.( )  
.  
.( )  
.  
.( )  
.  
.( )  
.  
.( )  
.  
.( - )  
.  
.( )  
.  
.( )  
.  
.  
.( )  
.  
/  
.( )  
.  
.( )  
.  
- )  
.  
.( )  
.  
.  
.( )  
.  
.  
.( )  
.

. ( )  
 / -  
 . ( )  
 -  
 . ( - )  
 ). ( )  
 . ( )  
 : . ( )  
 . ( )  
 -  
 . ( - )  
 : . ( )  
 : ( )  
 - ( )  
 : . ( )

:

1. Ahmad, D., Dubrawsky, I., Flynn, H., Grand, J., Graham, R., Johnson, N., Kaminsky, D., Lynch, F., Manzuik, S., Permeh, R., Pfeil, K., Puppy, R., Russell, R. & K2 (2002) **Hack Proofing Your Network**. Rockland, MA: Syngress Publishing.
2. Ajeeb, website (2001). **Number of Internet subscribers and users in the region**. [Online]. available: [http://eit.ajeeb.com/ViewArticle.asp?Article\\_ID=28132](http://eit.ajeeb.com/ViewArticle.asp?Article_ID=28132) [09-04-2003]
3. AME Info, website (2003). **Western Digital continues to thrive in the Saudi market**. [Online]. Available: <http://www.ameinfo.com/news/Detailed/20452.html> [06-07-2003]
4. Bace, Rebecca (2000). **Intrusion Detection**. Indianapolis, Indiana: Macmillan Technical Publishing.
5. Bagnall, B., Broomes, C. & Russell, R. (2000). **E-Mail Virus: Protection Handbook**. Rockland, MA: Syngress Publishing.
6. Bidwell, Teri (2002). **Hack Proofing Your Identity in The Information Age**. Rockland, MA: Syngress Publishing.
7. Black, Uyles (2000). **Internet Security Protocols: Protecting IP Traffic**. Upper Saddle River, New Jersey: Prentice Hall.
8. Brenner, S. & Frederickson, B. (2002). **Computer Searches and seizures: Some Unresolved Issues**. [Online]. Available: <http://www.mttl.org/voleight/Brenner.pdf> [22-05-2002]
9. Brenner, S. & Goodman, M. (2002). **Cybercrime as an Emerging Type of Transnational Organized Crime**. [Online]. Available: [http://essex.ac.uk/ecpr/standinggroups/crime/noticeboard\\_files/IPSA/brenner-goodman.pdf](http://essex.ac.uk/ecpr/standinggroups/crime/noticeboard_files/IPSA/brenner-goodman.pdf) [14-06-2003]
10. Brenner, Susan (2001). **Model Code of Cybercrimes Investigative Procedure**. [Online]. Available: <http://cybercrime.net/MCCIP/MCCIP.doc> [05-04-2003]
11. Brenton, C. & Hunt, C. (2003). **Mastering Network Security**. Alameda, California: Sybex.
12. Carter, D. & Katz, A. (1996). **Computer Crime: An Emerging Challenge for Law Enforcement**. [Online]. Available: <http://www.fbi.gov/publications/leb/1996/dec961.txt> [06-06-2003]
13. Casey, Eoghan (2001). **Digital Evidence and Computer Crime**. London: Academic Press.
14. Champlain, Jack (2003). **Auditing Information Systems**. Hoboken, New Jersey: John Wiley & Sons.
15. Cheswick, W., Bellovin, S. & Rubin, A. (2003). **Firewalls and Internet Security: Repelling the Wily Hacker**. Boston: Addison-Wesley.
16. Chirillo, John (2002) a. **Hack Attacks Denied**. Indianapolis, Indiana: Wiley Publishing.
17. Chirillo, John (2002) b. **Hack Attacks Revealed**. Indianapolis, Indiana: Wiley Publishing.
18. Chuvakin, A. & Peikari, C. (2004). **Security Warrior**. Sebastopol, California: O'Reilly & Associates.
19. COE, Council Of Europe (2001). **Convention on Cybercrime**. [Online]. Available: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [25-07-2003]

20. Cole, Eric (2002). **Hackers Beware: Defending Your Network From The Willy Hacker**. Indianapolis, Indiana: New Riders Publishing.
21. Cowens, B. & Miora, M. (2002). Computer Emergency Quick-response Team. In Bosworth S. & Kabay M. (Ed.), **Computer Security Handbook**. (pp 40.1-40.15). Hoboken, New Jersey: John Wiley & Sons.
22. Creer, Mark (2003). **Internet Gambling: Problems and Options**. [Online]. Available: <http://www.math.byu.edu/~jarvis/gambling/Student-papers/Mark-Creer.pdf> [26-06-2003]
23. Cronkhite, C., & McCullough, J. (2001). **Access Denied: The Complete Guide to Protecting Your Business Online**. Berkeley, California: Osborne/McGraw-Hill.
24. Davis, David (1998). **Internet Detective: An Investigator's Guide**. West Midland, UK: Police Research Group.
25. Denning, D. & Baugh, E. (1999). **Hiding Crimes in Cyberspace**. [Online]. Available: <http://www.cs.georgetown.edu/~denning/crypto/hiding1.doc> [13-06-2003]
26. Denning, Dorothy (1999). **Information Warfare and Security**. Boston: Addison-Wesley.
27. Denning, Dorothy (2000). **Cyberterrorism**. [Online]. Available: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc> [13-06-2003]
28. Denning, Dorothy (2001). **Cyberwarriors**. [Online]. Available: <http://www.cs.georgetown.edu/~denning/infosec/harvard.final.rtf> [13-06-2003]
29. Erbschloe, Mechail (2001). **Information Warfare: How to Survive Cyber Attacks**. Berkeley, California: Osborne/McGraw-Hill.
30. Erdonmez, E. (2002). **Investigation of Computer Crime**. Unpublished master's thesis, University of North Texas, Denton. Texas.
31. Erickson, Jon (2003). **Hacking: The Art of Exploitation**. San Francisco: No Starch Press.
32. Etter, Barbara (2001). **Computer Crime**. Paper presented at the 4<sup>th</sup> National Outlook Symposium on Crime in Australia, New Crimes or New Response. [Online]. available: <http://www.aic.gov.au/conferences/outlook4/Etter.pdf> [19-04-2003]
33. Fithen, Katherine (2000) **Internet Denial of Service Attacks and the Federal Response**. [Online]. Available: [http://www.cert.org/congressional\\_testimony/Fithen\\_testimony\\_Feb29.html](http://www.cert.org/congressional_testimony/Fithen_testimony_Feb29.html) [14-11-2003]
34. FNC, The Federal Networking Council (1995). **Definition of Internet**. [Online]. available: [http://www.itrd.gov/fnc/Internet\\_res.html](http://www.itrd.gov/fnc/Internet_res.html) [19-04-2003]
35. Furnell, Steven (2002). **Cybercrime: Vandalizing the Information Society**. Boston: Addison-Wesley.
36. GAO, Government Accounting Office (2002). **Internet Gambling: an overview of the issues**. [Online]. Available: <http://www.gao.gov/new.items/d0389.pdf> [26-06-2003]
37. Garfinkel, S., Spafford, G., & Schwartz, A. (2003). **Practical Unix & Internet Security**. Sebastopol, California: O'Reilly & Associates.
38. Gibson, Steve (2002) **The Strange Tale of the Denial of Service**. [Online]. Available: <http://grc.com/dos/grcdos.htm> [02-11-2003]
39. Goodman, M. & Brenner, S. (2002). **The Emerging Consensus on Criminal Conduct in Cyberspace**. [Online]. Available: [http://www.lawtechjournal.com/articles/2002/03\\_020625\\_goodmanbrenner.pdf](http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf) [14-06-2003]

40. Goodman, Mark (1997). Why The Police Don't Care About Computer Crime. **Harvard Journal of Law & Technology** 10 (3), 465-494. [Online]. available: <http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf> [06-06-2003]
41. Goodman, Mark (2001). Making Computer Crime Count. **FBI Law Enforcement Bulletin** 70 (8), 10-17. [Online]. available: <http://www.fbi.gov/publications/leb/2001/aug011eb.pdf> [02-04-2003]
42. Greek, Cecel (2000). **An Outline of Computer Crime**. [Online]. Available: [http://mailer.fsu.edu/~crimdo/TA/hao/computer\\_crime2.htm](http://mailer.fsu.edu/~crimdo/TA/hao/computer_crime2.htm) [19-04-2003]
43. Grimes, Roger (2001). **Malicious Mobile Code**. Sebastopol, California: O'Reilly & Associates.
44. Groover, Richard (1996). **Overcoming Obstacles: Preparing for Computer-related Crime**. [Online]. Available: <http://www.fbi.gov/publications/leb/1996/aug962.txt> [06-06-2003]
45. Gustaluk, Mikhael (2003). **Fighting Cybercrimes**. [Online]. Available: <http://www.crime-research.org/eng/library/Gutsaluk.html> [15-10-2003]
46. Hall, Eric(2000). **Internet Core Protocols: The Definitive Guide**. Sebastopol, California: O'Reilly & Associates.
47. Haynes, S. (ED.). (2002). **Computer Dictionary**. (5<sup>th</sup> ed.). Redmond, Washington: Microsoft Press.
48. Holland, Casey (2002). **The Carnivore Internet Monitoring Device: Capabilities, Statutory Framework, and Constitutional Considerations**. [Online]. Available: <http://www.uky.edu/Kaleidoscope/fall2003/oswald/holland-article.pdf> [15-02-2004]
49. Hollis, S., David, S. B., David, J. I., Richard B., Wayne, C., & Wayne, P. W. (2001). **Electronic Crime Needs Assessment for state and Local Law Enforcement**. [Online]. Available: <http://www.ncjrs.org/pdffiles1/nij/186276.pdf> [19-10-2003]
50. Icove, D., Segar, K. & Vonstorch, W. (1995). **Computer Crime: A Crimefighter's Handbook**. Sebastopol, California: O'Reilly & Associates.
51. IOCE, International Organization on Computer Evidence (2000). **Good Practices for Seizing Electronic Devices**. [Online]. Available: <http://www.ioce.org/2000/ioce%202000%20electronic%20devices%20good%20practices.doc> [18-09-2003]
52. IPR, International Planning and Research Corporation (2002). 2002 Global-Software Piracy Study. [Online]. available: <http://www.bsa.org/middleeast/events/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=9032> [19-04-2003]
53. ISTS, Institute for Security Technology Studies (2002). **Law Enforcement Tools And Technologies for Investigating Cyber Attacks: A National Needs Assessment**. [Online]. Available: [http://www.ists.dartmouth.edu/TAG/needs/ISTS\\_NA.pdf](http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf) [04-06-2003]
54. ISU, Internet Service Unit (2003). **Estimating the number of Internet users in KSA**. [Online]. available: <http://www.isu.net.sa/surveys-&-statistics/num-users.htm> [19-04-2003]
55. Jamsa, Kris (2002). **Hacker Proof: The Ultimate Guide to Network Security**. Albany, New York: Delmar Learning.
56. Kabay, M. E. (2002). Studies and Surveys of Computer Crime. In Bosworth S. & Kabay M. (Ed.), **Computer Security Handbook**. (pp 4.1-4.26). Hoboken, New Jersey: John Wiley & Sons.

57. Kelly, Harris (1995). **Computer Crime: An Overview**. [Online]. available: <http://www.search.org/publications/pdffiles/tbcomcri.pdf> [05-06-2003]
58. Kovacich, G. L. & Boni, W.C. (2000). **High-Technology Crime Investigator's Handbook**. Woburn, MA: Butterworth-Heinemann.
59. Kruse, W. & Heiser, J. (2002). **Computer Forensics: Incident Response Essentials**. Boston: Addison-Wesley.
60. Lane, Carole (2002). **Naked in Cyberspace: How to Find Personal Information Online**. Medford, New Jersey: CyberAge Books.
61. Levy, Steven (2001). **Hackers: Heroes of the Computer Revolution**. New York: Penguin Books.
62. Lilley, Peter (2000). **Dirty Dealing: The Untold Truth About Global Money Laundering**. London: Kogan Page.
63. Littman, Jonathan (1997). **The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen**. Boston: Little, Brown and Company.
64. Mandia, K. & Prorise, C. (2001). **Incident Response: Investigating Computer Crime**. Berkeley, California: McGraw-Hill.
65. McClure, S., Scambray, J. & Kurtz, G. (2001). **Hacking Exposed: Network Security Secrets & Solutions**. Berkeley, California: McGraw-Hill.
66. McCullagh, Declan (2003). **The 'homeless hacker' talks**. [Online]. Available: <http://news.com.com/2008-1014-5076942.html> [15-10-2003]
67. Mchlein, Alan (2003). **Find it Online: The Complete Guide to Online Research**. Tempe, MA: Facts on Demand Press.
68. Mclean, J.J. (2002). Homicide and Child Pornography. In Casey, Eoghan (Ed.), **Handbook of Computer Crime Investigation: Forensic Tools and Technology**. (pp 361-373). London: Academic Press.
69. Mendell, Ronald (1998). **Investigating Computer Crime: A Primer for Security Managers**. Springfield, Illinois: Charles Thomas.
70. Middleton, Bruce (2002). **Cyber Crime Investigator's Field Guide**. Boca Raton, Florida: Auerbach Publications.
71. Mitnick, K. & Simon, W (2002). **The Art of Deception: Controlling the Human Element of Security**. Indianapolis, Indiana: Wiley Publishing.
72. Morrison, P. (1990). **Computer Crime The Improvement of Investigative Skills: Final Report: Part One**. [Online]. Available: <http://www.acpr.gov.au/pdf/ACPR96.pdf> [21-10-2003]
73. New Zealand Police (2003). **Information for New Zealanders about E-Crime**. [Online]. Available: <http://www.police.govt.nz/service/ecrime/brochure.php> [01-10-2003]
74. NIJ, National Institute of Justice (2001). **Electronic Crime Scene Investigation: A Guide for First Responders**. [Online]. Available: <http://www.ncjrs.org/pdffiles1/nij/187736.pdf> [27-08-2003]
75. Northcutt, S. & Novak, J. (2003). **Network Intrusion Detection**. Indianapolis, Indiana: New Riders Publishing.
76. Northcutt, S., Cooper, M., Fearnow, M, & Frederick, K. (2001). **Intrusion Signatures and Analysis**. Indianapolis, Indiana: New Riders Publishing.
77. Northcutt, S., Zeltser, L., Winters, S, Frederick, K, & Ritchey, R. (2003). **Inside Network Perimeter Security**. Indianapolis, Indiana: New Riders Publishing.
78. NUA, website (2002). **How Many Online**. [Online]. available: [http://www.nua.ie/surveys/how\\_many\\_online/world.html](http://www.nua.ie/surveys/how_many_online/world.html) [19-04-2003]

79. Oppliger, Rolf (2003). **Security Technologies for the World Wide Web**. Norwood, MA: Artech House.
80. Parker, Donn (1998). **Fighting Computer Crime: A New Framework for Protecting Information**. Hoboken, New Jersey: John Wiley & Sons.
81. Pfaffenberger, Bryan. (ED.). (2001). **Webster's Newworld: Computer Dictionary**. (9<sup>th</sup> ed.). New York: Hungry Minds.
82. Platt, Franklin (2002). Protecting the Information Infrastructure. In Bosworth S. & Kabay M. (Ed.), **Computer Security Handbook**. (pp 15.1-15.46). Hoboken, New Jersey: John Wiley & Sons.
83. Power, Richard (2000). **Tangled Web: Tales of Digital Crime From the Shadows of Cyberspace**. Indianapolis, Indiana: QUE.
84. Riemer, Andrea K. (2001). **An inventory of Preventive Multilateral Activities in the Fields of Computer-related crime and Cyberthreats in Europe**. [Online]. Available: <http://www.isn.ethz.ch/crm/intorg/cyberthreads.pdf> [06-04-2003]
85. Roman, Jari (2001). **Computer Crime**. [Online]. Available: [http://www.urova.fi/home/oiffi/enlist/commentary/computer\\_crime.html](http://www.urova.fi/home/oiffi/enlist/commentary/computer_crime.html) [06-07-2002]
86. Rubin, Aviel (2001). **White-Hat Security Arsenal: Tackling the Threat**. Boston: Addison-Wesley.
87. Sammes, T. & Jenkinson, B (2002). **Forensic Computing: A practitioner's Guide**. London: Springer.
88. Schneier, Bruce (2000). **Secrets & Lies: Digital Security in a Networked World**. Hoboken, New Jersey: John Wiley & Sons.
89. Schultz, E., & Shumway, R. (2002). **Incident Response: A Strategic Guide to Handling System and Network Security Breaches**. Indianapolis, Indiana: New Riders Publishing.
90. Schwartau, Winn (2000). **Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption**. Broadway, New York: Thunders Mouth Press.
91. Shema, M. & Johnson, B. (2004). **Anti-Hacker Tool Kit**. Berkeley, California: Osborne/McGraw-Hill.
92. Shinder, Debra (2002). **Scene Of The Cybercrime: Computer Forensics Handbook**. Rockland, MA: Syngress Publishing.
93. Shipley, Todd (2002). Internet Gambling Investigations. In Casey, Eoghan (Ed.), **Handbook of Computer Crime Investigation: Forensic Tools and Technology**. (pp 375-394). London: Academic Press.
94. Sieber, Ulrich (1998). **Legal Aspects Of Computer-related Crime in the Information Society**. [Online]. Available: <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc> [04-11-2002]
95. Skoudis, E. & Zeltser, L. (2003). **Malware: Fighting Malicious Code**. New Jersey, Upper Saddle River: Prentice Hall.
96. Skoudis, Ed (2002). **Counter Hack: a Step-by-Step Guide to Computer Attacks and Effective Defenses**. New Jersey, Upper Saddle River: Prentice Hall.
97. Smith, B. & Komar, B. (2003). **Microsoft Windows Security Resource Kit**. Redmond, Washington: Microsoft Press.
98. Smith, Russell (2001). **Computer Crime: Crisis or Beat-Up?**. Paper presented at the Australian and New Zealand Society of Criminology conference: Criminology in The 21<sup>st</sup> Century: Public Good or Private Interest?, convened by University of Melbourne,

- Melbourne, 21 February 2001. [Online]. available:  
[http://www.aic.gov.au/conferences/other/smith\\_russell/2001-02-anzsoc.pdf](http://www.aic.gov.au/conferences/other/smith_russell/2001-02-anzsoc.pdf) [11-07-2003]
99. Smith, S. P., Perrit, H., Krent, H., Mencik, S., Crider, J. A., Shyong, M. & Reynolds, L. (2000) **Independent Review of the Carnivore System**. [Online]. Available: [http://www.usdoj.gov/jmd/publications/carnivore\\_draft\\_1.pdf](http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf) [15-02-2004]
  100. Spitzner, Lance (2003). **Honeypots: Tracking Hackers**. Boston: Addison-Wesley.
  101. Stanger, J., Lane, P. & Danielyan, E. (2001). **Hack Proofing Linux**. Rockland, MA: Syngress Publishing.
  102. Stansell-Gamm, Martha (2002) **Computer Crime: How Big is it and What Can You Do?**. [Online]. Available: [http://www.jrsa.org/pubs/forum/forum\\_issues/for20\\_4.pdf](http://www.jrsa.org/pubs/forum/forum_issues/for20_4.pdf) [21-10-2003]
  103. Stephenson, Peter (2000). **Investigating Computer-Related Crime**. Boca Raton, Florida: CRC Press.
  104. Sternecker, Alan (2004). **Critical Incident Management**. Boca Raton, Florida: Auerbach Publications.
  105. Strang, Robert (2002). Searching and Seizing Computers and Obtaining Electronic Evidence. In Marcella, A. J. & Greenfield, R. S. (Ed.), **Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime**. (pp 3-17). Boca Raton, Florida: Auerbach Publications.
  106. Stucki, Carol (2002). The Goal of the Forensic Investigation. In Marcella, A. J. & Greenfield, R. S. (Ed.), **Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime**. (pp 3-17). Boca Raton, Florida: Auerbach Publications.
  107. Taylor, Paul (2002). Hackers – cyberpunks or microserfs?. In Thomas D. & Loader B. (Ed.), **Cybercrime: Law Enforcement, Security and Surveillance in The Information Age**. (pp 36-55). London: Routledge.
  108. The Honeynet Project (2002). **Know Your Enemy: Revealing The Security Tools, Tactics, and Motives of The Blackhat Community**. Boston: Addison-Wesley.
  109. The White House (2003). **The National Strategy to Secure Cyberspace**. [Online]. Available: [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf) [07-06-2003]
  110. Thompson, David (1991). **Investigative Skills for the 1990s and Beyond**. Paper presented at the Conference: Asia Pacific Police Technology, convened by the Australian Institute of Criminology, Canberra, 12-14 November 1991. [Online]. available: <http://www.aic.gov.au/publications/proceedings/18/thompspon.html> [02-07-2003]
  111. Thompson, David. (1990). **Computer Crime The Improvement of Investigative Skills: Final Report: Part Two**. [Online]. Available: <http://www.acpr.gov.au/pdf/ACPR101.pdf> [21-10-2003]
  112. Tulloch, Mitch (2003). **Microsoft Encyclopedia of Security**. Redmond, Washington: Microsoft Press.
  113. UN, United Nations (1999). **International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime**. [Online]. Available: <http://www.uncjin.org/Documents/EighthCongress.html> [04-11-2002]
  114. USSC, United States Sentencing Commission (1993). **Computer Fraud Working Group: Report Summary**. [Online]. Available: <http://www.ussc.gov/publicat/cmptfrd.pdf> [06-04-2003]

115. USSS, United States Secret Service (2002). **Best Practices for Seizing Electronic Evidence**. [Online]. available: [http://www.secretservice.gov/electronic\\_evidence.shtml](http://www.secretservice.gov/electronic_evidence.shtml) [18-09-2003]
116. Vacca, John (2002). **Computer Forensics: Computer Crime Scene Investigation**. Hingham, Massachusetts: Charles River Media.
117. Vacca, John (2003). **Identity Theft**. New Jersey, Upper Saddle River: Prentice Hall.
118. Wahlert, Glenn (1998). **Computer Crime in the Australian Financial Sector**. Paper presented at the conference: Crime Against Business, convened by the Australian Institute of Criminology, Melbourne, 18-19 June 1998. [Online]. available: <http://www.aic.gov.au/conferences/cab/wahlert.pdf> [11-07-2003]
119. Wright, Timothy (2000) (a). **An Introduction to the Field Guide for Investigating Computer Crime**. [Online]. Available: <http://www.securityfocus.com/infocus/1244> [05-09-2003]
120. Wright, Timothy (2000) (b). **The Field Guide For Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics**. [Online]. Available: <http://www.securityfocus.com/infocus/1245> [05-09-2003]
121. Wright, Timothy (2000) (c). **The Field Guide for Investigating Computer Crime: Search and Seizure Basics**. [Online]. Available: <http://www.securityfocus.com/infocus/1246> [05-09-2003]
122. Wright, Timothy (2000) (d). **The Field Guide for Investigating Computer Crime: Search and Seizure Planning**. [Online]. Available: <http://www.securityfocus.com/infocus/1247> [05-09-2003]
123. Wright, Timothy (2000) (e). **The Field Guide for Investigating Computer Crime: Search and Seizure Approach, Documentation, and Location**. [Online]. Available: <http://www.securityfocus.com/infocus/1248> [05-09-2003]
124. Wright, Timothy (2000) (f). **The Field Guide for Investigating Computer Crime, Part Six: Search and Seizure - Evidence Retrieval and Processing**. [Online]. Available: <http://www.securityfocus.com/infocus/1249> [05-09-2003]
125. ZDNet News (2000). **Data thief blackmails e-tailer**. [Online]. Available: <http://zdnet.com.com/2100-11-517749.html> [19-10-2003]
126. Zwicky, E., Cooper, S. & Chapman, D. (2000). **Building Internet Firewalls**. Sebastopol, California: O'Reilly & Associates.