DR. A P J ABDUL KALAM UNIVERSITY, INDORE

SYLLABUS

of

MASTER OF TECHNOLOGY (CYBER SECURITY)

Department of Information Technology

(First Year)

(Session July- December 2016)

College of Engineering

Dr. A P J Abdul Kalam University, Indore

DR. A P J ABDUL KALAM UNIVERSITY, INDORE

Syllabus for Master of Technology (Cyber Security)

Department of Information Technology

List of Subject (First Year)

S. No.	Subject Code	Subject Name	Page No.
1	MTCYS 101	Cyber law & Intellectual Property Rights	3
2	MTCYS 102	Operating system and security	5
3	MTCYS 103	Computer Network & security	7
4	MTCYS 104	Data Base & Security	8
5	MTCYS 105	Cyber Security	10
6	MTCYS 106	Lab-I (Network Security Lab)	11
7	MTCYS 107	Lab-II (Database Security Lab)	12
8	MTCYS 201	Cryptography & Network Security	13
9	MTCYS 202	Digital forensics	15
10	MTCYS 203	Biometric Systems & Biometric Image Processing	17
11	MTCYS 204	Computer Forensic analysis & Investigation	19
12	MTCYS 205	File System Forensics	21
13	MTCYS 206	Lab-III(Ethical hacking lab)	23
14	MTCYS 207	Lab-IV(Computer forensics lab)	24

Unit 1: Cyber Space- Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction - Enforcement agencies – Need for IT act - UNCITRAL – E-Commerce basics .Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction

Unit 2: Electronic Governance – Legal Recognition of Electronic Records and Electronic Evidence -Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws .

Cyber Crimes -Meaning of Cyber Crimes –Different Kinds of Cyber crimes – Cyber crimes under IPC,

Unit 3: Cr.P.C and Indian Evidence Law - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism-Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases.

Unit 4: Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases,

Unit 5 : Patents - Understanding Patents - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases

References:

1. Justice Yatindra Singh: Cyber Laws, Universal Law Publishing Co., New Delhi

2. Farouq Ahmed, *Cyber Law in India,* New Era publications, New Delhi

3. S.R.Myneni: *Information Technology Law(Cyber Laws),* Asia Law House, Hyderabad.

4. Chris Reed, *Internet Law-Text and Materials*, Cambridge University Press.

5. Pawan Duggal: *Cyber Law- the Indian perspective* Universal Law Publishing Co., New Delhi

Sub Code : MTCYS 102 Sub Name : Operating System and Security 4 Credits

UNIT 1: Evolution of operating systems, basic operating system functions, understanding how operating systems work, the kernel, resource managers, device drivers, the role of application software, the role of BIOS, mainframe systems, desktop systems, multiprocessor systems, distributed systems, clustered systems, network operating system, handheld system, operating system services, operating system structure, system calls, system programs, operating system design & implementation, types of operating systems

UNIT 2: Process Concept, process scheduling, operations on processes, cooperating processes, inter-process communication, multithreading models, CPU scheduling algorithms, critical section problem, semaphores, classical problems of synchronization, critical regions, monitors, atomic transactions, deadlock characterization, methods for deadlock handling, Swapping, paging, segmentation, demand paging, page replacement, thrashing, file concept, access methods, directory structure, file sharing, file system implementation, disk storage basics, block allocation, partitions, formatting, Windows file system, Unix file system, disk scheduling.

UNIT 3: Introduction to security in operating system, requirements for operating system security, secure operating systems, the security problem, protection mechanisms, domain of protection, user oriented access control, data oriented access control, access matrix, implementation of access matrix, access rights, language based protection, user authentication, threat model, program threats, system threats, malicious software, intruders, security vulnerabilities, security violations, securing systems and facilities, implementing security defenses, file sharing, file system security, Trojan horse defense,

UNIT 4: Multics security, UNIX security, windows security, verifiable security goals, security kernels, secure capability systems, secure virtual machine systems

UNIT 5: Trusted operating system, trust vs. security, trust model, trusted computing base, security policy, models of security, trusted operating system design, security features of trusted operating system, assurance in trusted operating systems.

References:

[1]. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, "Operating System Concepts", Sixth Edition, John Wiley & Sons (ASIA) Pvt. Ltd, 2003.

[2]. William Stallings, "Operating System", Prentice Hall of India, 4th Edition, 2003.

[3]. Pramod Chandra P. Bhatt , "An Introduction to Operating Systems, Concepts and Practice", PHI, 2003.

[4]. Trent Jaeger, "Operating system Security", Morgan and Claypool publishers, 2008

Unit 1: Introduction to ISO's OSI Network Architecture, Internet Model, IP Design and Implementation, Internetworking and routing protocols, Transport layer services and variants, Peer to Peer Networks, Application Layer protocols,

Unit 2: Introduction to network Security and associated techniques, Firewall Design principles, VPNs, Worms, Viruses, Vaccine Programs, Security of Network Layer, Security of Application layer protocols, BSD sockets, Elementary and Advanced system calls.

Unit 3: Raw sockets: Raw Socket Creation, Raw socket output, raw socket input, packet sniffing and routing algorithms: Router IOS- Static and Default Routing-Interior Gateway Routing Protocols: RIP V1&V2, OSPF, EIGRP- Exterior Gateway Routing Protocol: BGP

Unit 4: Introduction to socket programming- Concurrent Processing in Client-Server Software-Byte ordering and address conversion functions – Socket Interface - System calls used with sockets - Iterative server and concurrent server- Multi protocol and Multi service server- TCP/UDP Client server programs – Thread Creation and Termination – TCP Echo Server using threads- Remote Procedure Call.

Unit 5: Symmetric ciphers: Classical Encryption Techniques: SubstitutionTechniques, Transposition Techniques, Steganography. Block Ciphers and the Data Encryption Standard, Block Cipher Principles, The Data Encryption Standard. Basic Concepts in Number Theory and Finite Fields: Divisibility and the Division Algorithm, The Euclidean Algorithm. Advanced Encryption Standard, Pseudorandom Number Generation and Stream Ciphers.

References:

[1]. Richards Stevens, Unix network programming, , Vol I & Vol II, 4th edition, Prentice Hall, 2007.
[2]. Stallings, Cryptography and Network Security, Pearson Education,2007

Unit 1: Overview of Relational Model, SQL, Building of database, Manipulation of data Goals of Database Security, access points of database security, database security levels, and menaces to databases. Database security methods and methodologies**.** Security controls: flow control, inference control and access control.

Unit 2: Database Application Security models – Types of users, access matrix model, access modes model, commonly used application types. Classes of access control: Discretionary access control (DAC), Mandatory access control (MAC) and Role based Access control (RBAC); Discretionary Access Control (DAC) mechanisms such as capabilities, profiles, access control lists, passwords, and permission bits.

Unit 3: RBAC based security models features like User role assignment, Support for role relationships and Constraints, Assignable privileges. MAC based security models. Information leakages through convert channels and inference channels. Security support in popular commercial database packages. Implementing Fine Grained access controls with views .

Unit 4: Virtual Private databases: need for VPDs, Implementing VPD using views, The Database Security Design includes the controls that will be implemented to restrict users from accessing information, based on how the information is classified and the security model. For Example;- Restricting the rights a user has to access information, Restricting the rights a user has to perform certain functions, e.g. only letting a system user drop tables Tracking activities in the database to provide an audit trail if needed.

Unit 5: Application Security, SQL Injection and Defensive programming (An approach to improve software and source code, in terms of: General quality - Reducing the number of software bugs and problems. Making the source code comprehensible - the source code should be readable and understandable so it is approved in a code audit.), Auditing process, auditing models, application of Auditing. Statistical database security; Database privacy – Hippocratic databases.

References:

[1]. Database Security by Silvano Castano, Fugini, Martella, Samarati – Addison Wesley

[2]. Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server,Db2 Udb, Sybase. Ben-Natan, R. B. 2005, Digital Press

Unit 1: **Systems Vulnerability Scanning :** Overview of vulnerability scanning, Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark, Ettercap, Hping Kismet.

Unit 2: Network Defense tools: Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, How a Firewall Protects a Network, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, the basic of Virtual Private Networks, Linux Firewall, Windows Firewall, Snort: Introduction Detection System.

Unit 3: Web Application Tools: Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sqlmap. DVWA, Webgoat, Password Cracking and Brute-Force Tools – John the Ripper, L0htcrack, Pwdump, HTC-Hydra.

Unit 4: Introduction to Cyber Crime and law: Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Computer Language, Network Language, Realms of the Cyber world, A Brief History of the Internet, Recognizing and Defining Computer Crime, Contemporary Crimes, Comp. as Targets, Contaminants and Destruction of Data, Indian IT ACT 2000.

Unit 5: Introduction to Cyber Crime Investigation : Firewalls and Packet Filters, password Cracking, Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless Networks.

Reference Books:

1. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley.

Network security lab

1. Learn to install wine / virtual box or any other equivalent Software on the host os.
2. Perform an experiment to grab a banner with telnet and perform The task using netcat utility
3. Perform an experiment for port scanning with nmap, superscan Or any other software
4. Using nmap

1) find open ports on a system

2) find the machines Which are active

3) find the version of remote os on other systems

4) find the version of s/w installed on other system

5. Perform an experiment on active and passive finger Printing using xprobe2 and nmap.
6. Performa an experiment to demonstrate how to sniff for router Traffic by using the tool wireshark.
7. Perform an experiment how to use dumpsec.
8. Perform an wireless audit of an access point / router and Decrypt wep and wpa.
9. Perform an experiment to sniff traffic using arp poisoning.
10. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, symmetric crypto algorithm, hash and digital/pki Signatures
11. Demonstrate intrusion detection system (ids) using any tool Eg . Snort or any other s/w
12 . Install rootkits and study variety of options
13. Generating password hashes with openssl
14. Setup a honey pot and monitor the honeypot on network

Database Security lab

1. Introduction to Database Security
2. Discretionary Access Control
3. Mandatory Access Control
4. Statistical Database Security
5. Role-based Access Control
6. SQL injection its forms, and defense.
7. No SQL injection and defense.
8. Database attack approaches.
9. Database defense approach.
10. Database encryption
11. SQLite Cipher encryption

Sub Code : MTCYS 201 Sub Name : Cryptography & Network Security 4 Credits

UNIT: 1 An overview of computer security ,Goals of information security, confidentiality, integrity, Availability, Security policies: Types of access control, Basic cryptography, OSI security architecture , Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.

UNIT: 2 Authentication: Authentication basics, Passwords, Key management , Diffie Hellman key exchange , Elliptic curve architecture and cryptography , Introduction to number theory , Confidentiality using symmetric encryption , Public key cryptography and RSA.

UNIT: 3 Security Attacks, Trojan Horses, Security Services, Security Mechanisms, and a Model for Network Security ,Non Cryptographic Protocol Vulnerabilities DoS, DDoS, Session Hijacking and Spoofing, Software Vulnerabilities, Phishing, Buffer Overflow, Format String Attacks, SQL Injection, Basics of Cryptography Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties Confusion, Diffusion, Block and Stream Ciphers.

UNIT: 4 SQL injection and cross-site scripting, symmetric encryption, SSL and TLS, PKI and Certificate Systems, Passwords and Secure Cookies, IPsec, Ingress filtering, and Firewalls, Digital signatures, Digital Signature Schemes, Authentication Protocols, Digital Signature Standards, files and devices, Program security,

UNIT: 5 Intrusion Detection ,Firewalls and proxy, Image Security-Biometrics, Web Security: Web Security Considerations, Secure Sockets Layer and Transport Layer Security, Electronic Payment Combining security Associations, Internet Key Exchange, Virus and worms.

References:

[1]. Introduction to computer security by Matt Bishap Sathyanarayana S.Venkatramanayya.

[2]. Cryptography and network security by Atul Kahate, TMH

[3]. Cryptography and network security: Principles and Practice: Fourth or Fifth Edition by William Stalling, Printice Hall.

[4]. Network security Essentials: Application and Standards by William Stallings, Prentice Hall.

[5]. Cryptography and Security: Padmanabhan, Wiley India

Unit-1 Digital forensic

Computer forensics and investigations as a profession, Understanding computer forensics, computer forensics versus other related disciplines, A brief History of computer Forensics, Understanding case laws, Developing computer forensics resources, Preparing for computer investigations, Understanding law enforcement agency investigations, Following the legal process, Understanding corporate investigations, Establishing company policies, Displaying warning Banners.

UNIT – 2 Windows Systems and artifacts

Windows Systems and Artifacts: Introduction, Windows File Systems, File Allocation Table, New Technology File System, File System Summary, Registry, Event Logs, Prefetch Files, Shortcut Files, Windows Executables.

UNIT – 3 Linux Systems and artifacts

Linux Systems and Artifacts: Introduction, Linux File Systems, File System Layer, File Name Layer , Metadata Layer, Data Unit Layer, Journal Tools, Deleted Data, Linux Logical Volume Manager, Linux Boot Process and Services, System V , BSD, Linux System Organization and Artifacts, Partitioning, File system Hierarchy, Ownership and Permissions, File Attributes, Hidden Files, User Accounts , Home Directories, Shell History GNOME Windows Manager Artifacts, Logs, User Activity Logs, Syslog, Command Line Log Processing, Scheduling Tasks.

UNIT – 4 Current Computer Forensics Tools

Evaluating Computer Forensics Tool Needs, Types of Computer Forensics Tools, Tasks Performed by Computer Forensics Tools, Tool Comparisons, Other Considerations for Tools, Computer Forensics Software Tools, Command-Line Forensics Tools, UNIX/Linux Forensics Tools, Other GUI Forensics Tools, Computer Forensics Hardware Tools, Forensic Workstations, Using a Write-Blocker.

Unit-5 Identification of data

Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks ,Router Forensics. Cyber forensics tools and case studies.

References:

1. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress imprint of Elsevier.

2. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", Fourth Edition, Course Technology.

3. Angus M.Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.

.

Unit -1: Introduction : Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques –Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems, FAR,FRR, FTE rate, EER and ATV rate, Applications of Biometric Systems, Security and Privacy Issues. Physiological Biometrics : Leading technologies : Finger-scan – Facial-scan – Iris-scan – Voice-scan–components, working principles, competing technologies, strengths and weaknesses – Other physiological biometrics : Hand-scan, Retina-scan – components, working principles, competing technologies, strengths and weaknesses – Automated fingerprint identification systems.

Unit- 2: Behavioral Biometrics: Leading technologies: Signature-scan – Keystroke scan – components, working principles, strengths and weaknesses. **Privacy and Standards in Biometrics**: Assessing the Privacy Risks of Biometrics – Designing Privacy- Sympathetic Biometric Systems – Need for standards – different biometric standards.

Unit- 3: Fundamentals of Image Processing: Digital Image representation - Fundamental steps in Image Processing Image Enhancement: The Spatial Domain Methods, The Frequency Domain Methods – Image Segmentation: Pixel Classification by Thresholding, Histogram Techniques, Smoothing and Thresholding- Gradient Based Segmentation: Gradient Image, Boundary Tracking, Laplacian Edge Detection.

Unit -4: Fingerprint Biometrics: Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing - Minutiae Determination - Fingerprint Matching: Fingerprint
Classification, Matching policies.

Unit- 5: Iris Biometrics: Iris System Architecture, Definitions and Notations - Iris Recognition: Iris location, Doubly Dimensionless Projection, Iris code, Comparison - Coordinate System: Head Tilting Problem, Basic Eye Model, Searching Algorithm, Texture Energy Feature

References for Biometric systems:

1. Anil K Jain, Patrick Flynn, Arun A Ross, "Handbook of Biometrics", Springer, 2008

2. Anil K Jain, Arun A Ross, Karthik Nandakumar, "Introduction to Biometrics", Springer, 2011

3. Samir Nanavati, Michael Thieme, Raj Nanavati, "Biometrics – Identity Verification in a Networked World", Wiley-dreamtech India Pvt Ltd, New Delhi, 2003

4. Paul Reid, "Biometrics for Network Security", Pearson Education, New Delhi, 2004

5. John R Vacca, "Biometric Technologies and Verification Systems", Elsevier Inc, 2007

References for Biometric Image processing:

1. David D. Zhang, "Automated Biometrics: Technologies and Systems", Kluwer Academic Publishers, New Delhi, 2000.

2. Rafael C.Gonzalez, Richard E.Woods, Steven L.Eddins, "Digital Image Processing", Pearson Education, New Delhi, 2009

3. Arun A. Ross , Karthik Nandakumar, A.K.Jain, "Handbook of Multibiometrics", Springer, New Delhi, 2006

Unit-1 Computer forensics analysis

Determining what data to collect and analyze. Addressing data hiding techniques, Hiding partitions, Marking bad cluster, Bit –shifting, using steganography to hide data, Examining encrypted files, Recovering Passwords, Performing Remote Acquisitions, Remote Acquisitions with Runtime Software.

Unit-2 Recovering graphics files

Understanding vector Graphics, Understanding graphics file formats .Lossless and lossy compression. Identifying graphics file fragments, Repairing Damaged Headers, Searching for and carving data from unallocated space. Understanding steganography in graphics files. Using steganalusis tools. Understanding copyright issues with graphics.

Unit-3 Virtual Machines, Network forensics, and Live Acquit ions

Performing live acquit ions, Performing a live acquit ion in windows, Developing standard procedures for network forensics, Reviewing network logs. Using network tools, using Unix/Linux tools. Using packet sniffers, examining the honey net projects.

Unit-4 E-Mail Investigation

Exploring the role of email investigation, Exploring the role of client and server in email, Investigating E-mail crimes and violations, Examining E-mail Messages, Viewing E-mail headers, Examing E-mail headers, Examining additional E-mail files. Tracing an e-mail message, Using network E-mail logs, Understanding E-mail servers, Examining Unix e-mail server logs, Examining Microsoft email server logs.

Unit-5 Cell phone and mobile device forensics

Understanding mobile device forensics, Mobile phone basics, inside mobile devices, inside PDAs, Understanding acquisition procedures for cell phones and mobile devices, Mobile forensics equipment.

References:

1. Bill Nelson,Amelia Phillips,Christopher Steuart,"Guide to Computer Forensics and Investigations", Fourth Edition,Course Technology.
2. Angus M.Marshall, "Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.

Unit 1: Digital investigation foundation - Digital investigations and evidence, Digital crime scene investigation process, Data analysis, overview of toolkits, Computer foundations – Data organizations, booting process, Hard disk technology, Hard disk data acquisition.

Unit 2: Volume Analysis - introduction, background, analysis basics, PC based partitions- DOS partitions, Analysis considerations, Apple partitions, removable media, Server based partitions- BSD partitions, Sun Solaris slices, GPT partitions, Multiple disk volumes- RAID, Disk Spanning.

Unit 3: File system analysis- What is a file system, File system category, Content category, Metadata category, File name category, Application category, Application-level search techniques, Specific file systems, FAT concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. FAT data structure- Boot sector, FAT 32 FS info, FAT, Directory entries, Long file name directory entries.

Unit 4: NTFS concepts- Introduction, Everything is a file, MFT concepts, MFT entry attribute concepts, Other attribute concepts, Indexes, Analysis tools, NTFS Analysis- File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures, File system metadata files.

Unit 5: Ext2 and Ext3 concepts- File system category, Content category, Metadata category, File name category, Application Category. Ext2 and Ext3 data structures-Super block, group descriptor tables, Block bitmap, Inodes, Extended attributes, Directory Entry, Symbolic Link, Hash trees, Journal data structures, UFS1 and UFS2 concepts and analysis - Introduction, File system category, Content category, Metadata category, File name category, UFS1 and UFS2 data structures- UFS1 superblock, UFS2 superblock.

References:

1. File System Forensic Analysis – Brian Carrier, Addison Wesley, 2005
2. Digital Evidence and Computer Crime- Casey, Eoghan , edition 2, Academic Press, 2004.
3. Computer Forensics- Kruse, Warren and Jay Heiser, Addison Wesley, 2002.

Ethical hacking Lab

1. Introduction to ethical hacking.
2. Phases of Ethical hacking.
3. Networking concept.
4. Foot Printing
5. Windows linux system security.
6. Proxy server
7. Hacking Lab setup.
8. System hacking and security.
9. Windows Linux scripting.
10. Network hacking and security.
11. Foot Printing and Information gathering.
12. Google hacking.
13. Hacking attacks.
14. Web application hacking.
15. Cryptography
16. Honeypots.
17. Wireless and mobile hacking and security
18. Cyber Forensic Investigations and Cyber laws

CF can conduct the following types of computer forensic investigation:

1. Use of E-Mail, Instant Messaging, & Chat
2. Computer Hacking & Network Intrusion
3. Copyright Infringement
4. Software Piracy
5. Intellectual Property Theft
6. Identity Theft
7. Online Auction Fraud
8. Credit Card Fraud
9. Other Financial Frauds & Schemes
10. Telecommunications Fraud
11. Threats, Harassment
12. Extortion and/or Black Mail
13. Gambling
14. Drug Abuse and/or Distribution
15. Divorce
16. Adult Sexual Assault
17. Assault & Battery
18. Domestic Violence
19. Death Investigation
20. Employee or Employer Misconduct
21. Theft, Robbery and/or Burglar