ALAGAPPA UNIVERSITY

(A State University Accredited with A+ Grade By NAAC (CGPA:3.64) in the Third Cycle and Graded as Category-I University By MHRD-UGC)
Karaikudi – 630003.
Tamil Nadu

Directorate of Distance Education

PROGRAMME PROJECT REPORT

DIPLOMA IN CYBER SECURITY (PPR)

December 2020

Table of contents

DIRECTORATE OF DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY

Credit Based Curriculum and Evaluation System

(With effect from Calendar Year 2021 Onwards)

(a) PROGRAMME'S MISSION AND OBJECTIVES

Mission

Mission is to impart employability and creativity to the students and lives up to the standards of Government Organizations, Computer science, Computer Applications and Information Technology (IT) industry.

Programme Objectives

The Cyber Security course familiarizes students with the basic concepts of Cryptography and Network Security. This Course will help the students to Secure the computers in Banking, Insuranceand Government Organization / Business and Industry and also from Outside Hackers.

(b) PROGRAMME OUTCOME

- ✓ To widen the ability to analyze, design, implement & maintain the Computers from outside Hackers.
- ✓ After learning the course, the students should be able to understand cyber-attack, types of cybercrimes, cyber laws and also how to protect them self and ultimately society from such attacks.

(c) NATURE OF PROSPECTIVE TARGET GROUP OF LEARNERS

The nature of prospective target group of learners is students from college students from various discipline like Commerce, Mathematics, Physics, Electronics, and Engineering etc. It also includes the learners who want to become Cyber Security Specialist, Information Security Professional etc.

d) APPROPRIATENESS OF PROGRAMME TO BE CONDUCTED IN DISTANCE LEARNING MODE TO ACQUIRE SPECIFIC SKILLS AND COMPETENCE;

Diploma in Cyber Security Programme through Distance Learning mode is developed in order to give subject-specific skills including i) Cryptography ii) Knowledge about various Systems Security, Web Security etc.

(E) INSTRUCTIONAL DESIGN

e.1 Revisions of Regulation and Curriculum Design

1. The University reserves the right to amend or change the regulations, schemes of examinations and syllabi from time to time based on recent market dynamics, industrial developments, research and feedback from stakeholders and learners.
2. Each student should secure 16 credits to complete certificate programme.
3. Each theory and practical course carry2 credits with 75 marks in the University End Semester Examination (ESE) and 25 marks in the Continuous Internal Assessment (CIA).

Programme code:

Diploma in Cyber Security	XXXXX

Course of Study and Scheme of Examinations

S.No	Course Code	Name of the Course	CIA Marks Max.	ESE Marks Max.	Total Marks Max.	Credits
I SEMESTER						
1	51911	Cryptography and Network Security	25	75	100	2
2	51912	Fundamentals of Cyber Security	25	75	100	2
3	51913	Cyber Security Law & Practice	25	75	100	2
4	51914	Cryptography – LAB	25	75	100	2
II SEMESTER						
5	51921	Web Application Security	25	75	100	2
6	51922	Malware Analysis and Network Security	25	75	100	2
7	51923	Mobile Security	25	75	100	2
8	51924	Cyber Security - LAB	25	75	100	2
		TOTAL	**200**	**600**	**800**	**16**

CIA: Continuous Internal Assessment ESE: End semester Examination

Course Code Legend:

			S	C

– Programme code for Certificate Course in Office Automation
S -- Semester Number
C – Course Number in the Semester

e.2 Detailed Syllabi

The detailed Syllabi of study and shall be as shown in Appendix.

e.3 Duration of the Programme:

The certificate programme shall consist of a period ofoneyear (Two Semesters). Maximum duration to complete the course is 3 Years.

e.3.1 Medium of Instruction

The medium of instruction is only in **English**.

The course material is also in **English.**

e.4 Faculty and Support Staff Requirements:

The following faculty and support staff are required for this programme.

S.No	Staff Category	Numbers
1	Core Faculty	4
2	Lab Assistant	1
3	Clerical Assistant	1

e.5 Instructional Delivery mechanisms

The instructional delivery mechanisms of the programme includes SLM- Study materials, Lab instruction manual, Personal contact session for both theory and practical courses of the programme, e-version of the course materials in the form of e-book, e-tutorials, Power Point, Video Lecture Links, Video Lectures, Open Educational Resources (OER) and Virtual lab.

e.6 Identification of media

The printed version of SLM – study material shall be given to the learners in addition to MOOC, e-tutorial and virtual lab.

e.7 Student Support Services

The student support services will be facilitated by the Directorate of Distance Education, Alagappa University, Karaikudi and its approved learning centres located in various parts of Tamilnadu.

The pre-admission student support services like counseling about the programme including curriculum design, mode of delivery, fee structure and evaluation methods will be explained by the staff at Directorate of Distance Education or Learning centres.

The post-admission student support services like issuing Identity card, study materials will be provided thru Directorate or Learning centres. The face to face contact sessions of the programme for both theory and practical's will be held at the Directorate or Learning centres.

The student support regarding the conduct of examinations, evaluations, publication of results and certificates are done by Office of the Controller of Examinations, Alagappa University, Karaikudi.

F. PROCEDURE FOR ADMISSION:

f.1 Minimum qualification for admission

Candidates for admission to the Diploma programme shall be required to have passed in H.S.C of Tamilnadu State or Equivalent Examination of any Recognized institution or authority accepted by the Syndicate of the Alagappa University as equivalent thereto shall be eligible.

f.2 Curriculum transaction

- The face to face contact sessions in class room teaching with the support of SLM, Power Point Presentations, web-based tools, audio and animated videos.
- The practical classes are based on the respective subject study materials containing requirement for the laboratory experiments.
- Face to face contact sessions will be conducted for both theory and practical courses in the following manner.

Course Type	**PCP (in Hours)**
Theory courses (3 Courses with 2 credits each)	18
Practical course (1 Course with 2 credit)	60
Total	**78**

f.3 Evaluation

There shall be two types of evaluation systems; internal assessment and end semester examination will be conducted by the University according to the following scheme. The maximum marks for the internal assessment for both theory and practical's is 25 marks. The maximum marks for end semester examination is 75 marks for each course. The candidate failing in any course(s) will be permitted to appear for each failed course(s) in the subsequent examination.Candidates who have passed the examination in all prescribed courses as per the above regulations shall be eligible for the award of the programme.

Internal assessment

- Internal assessment of theory courses is through home assignment with workbook, case studies, review questions, quiz, multiple choice questions etc., for 25 marks.
- The internal assessment for the practical courses shall be through home assignment which includes TCP Scanning, Port Scanning, Web Application Testing etc., for 25 marks.
- Student should submit assignment for theory and practical courses of every course.

Division of Internal Marks (Assignment)

Theory		**Practical**	
Assignment	**Marks**	**Assignment**	**Marks**
Class test/Review questions Workbook, case studies, quiz, multiple choice questions	25	Model practical Test. Algorithm Design, Writing Source Code and final Result.	25

End Semester Examination (ESE)

The university end Semester Examinations shall be of three hours duration with maximum of 75 Marks for both theory and practical courses.

f.3.1 Minimum for a pass:

To pass in each course, a candidate is required to secure 40% marks in the End Semester Examination and 40% marks in the aggregate (marks in End Semester Examination + marks in Internal Assessment).

The student who does not secure required minimum marks for pass in a course(s) shall be required to reappear and pass the same in the subsequent examination.

f.3.2 Question Paper Pattern - Theory

The end semester examination will be conducted in the duration of 3 Hours and maximum of 75 Marks.

All the units Should be covered in each Part

Part – A (10 x 2 Marks: 20 Marks) Answer all questions

Part – B (5 x 5 Marks: 25 Marks) Answer all questions choosing either (a) or (b)

Part – C (3 x 10 Marks: 30 Marks) (Answer any 3 out of 5 questions)

End Semester Examination (ESE) - Practical

Students are required to prepare a separate lab record for each lab course. The practical counsellor should duly sign this lab record after each session.

Students shall prepare practical record note book which includes aim, algorithm, source code, input, expected output and result of the experiment and submit during end semester practical examination.

Division of marks in ESE – Practical (Maximum 75 marks)

The end semester practical examination will be conducted in the duration of 3 Hours and maximum of 75 Marks.

Practical details	**Max. Marks**
Algorithm / Procedure	10
Source Code	20
Debugging	10
Execution	10
Results	10
Viva-Voce	5
Record	10
Total	75

f.3.3 Procedure for Completing the Course:

The candidate will qualify for the certificate programme only if he/she passes all the (including arrears) courses with in a period of TWO years from the date of admission.

f.3.4 Results:

Results will be declared at the end of each semester of the University examination and the marks/grade obtained by the candidate will be forwarded to them by the Controller of Examinations, Alagappa University.

f.4 Fees Structure:

Fee Particulars	Rs.
Admission Processing Fees	100
Course Fees	5200
ICT fees	150
Total Fees	**5,450**

The above-mentioned fees structure is exclusive of examination fees.

G. REQUIREMENT OF THE LABORATORY SUPPORT AND LIBRARY RESOURCES

g.1 Laboratory Support

A well- equipment Computer Laboratory was established in the Alagappa University, Karaikudi with necessary software's as per the practical's syllabi for conducting face to face contact sessions for practical courses of this programme. Model Practical Questions is available to the learners in the university website.

g.2 Library Resources

The Directorate of Distance Education, Alagappa University provides library facility with number of books and Self Learning materials for Computer Science Programmes. The Central library of Alagappa University provides the collection of volumes of Self Learning Materials, Printed books, Subscriptions to printed periodicals and Non-book materials in print form for the learner's references. All these library resources are meant for learner's reference purpose only.

h)Cost estimate of the programme and the provisions:

Expense details	Amount in (Rs.) Approx.
Programme development (Single time Investment)	10,00,000/-
Programme delivery (Per Sem)	24,00,000/-
Programme maintenance (per Sem)	5,00,000/-

(i) Quality assurance mechanism and expected programme outcomes:

i.1 University's Moto:

'Excellence in Action'

i.2 University's Vision and Mission

Vision

Achieving Excellence in all spheres of Education, with particular emphasis on ' PEARL' - Pedagogy, Extension, Administration, Research and Learning.

Mission

Affording a High-Quality Higher Education to the learners so that they are transformed into intellectually competent human resources that will help in the uplift of the nation to Educational, Social, Technological, Environmental and Economic Magnificence (ESTEEM).

i.3 University Objectives

1. Providing for instructions and training in such branches of Learning at the university may determine.
2. Fostering Research for the Advancement and Dissemination of Knowledge and Application.

i.4 Quality Policy

Attaining Benchmark Quality in every domain of 'PEARL' to assure Stakeholder Delight through Professionalism exhibited in terms of strong purpose, sincere efforts, steadfast direction and skillful execution.

i.5 Quality Quote

Quality Unleashes Opportunities Towards Excellence (QUOTE).

i.6. Course benchmarks

The benchmark qualities of the programme may be reviewed based on the performance of students in their end semester examinations and number of enrolments of students. Feedback from the alumni, students, parents, stakeholders and employers will be received to analyse the benchmark qualities for the further improvement of the programme.

$$$$$

Appendix A

Detailed Syllabi

11 - CRYPTOGRAPHY AND NETWORK SECURITY

Course Objectives

- To understand the computer security concepts
- To understand the Data Encryption Standard mechanism

Course Outcome

- At the end of this course, the student will be able to;
- Able to know AES, RSA cryptography principles
- Able to know Digital Signatures, E-mail security

UNIT 1:

Introduction: The OSI security architecture, security attacks, Security Services, Security mechanism, A model for network security, classical Encryption techniques, Symmetric cipher model, Substitution techniques.

UNIT 2:

Block cipher principle, the data encryption standard, The strength of DES, Differential and Linear cryptanalysis, Block cipher design principles,Advanced Encryption Standard: Finite Field arithmetic, AES structure, AEStransformation function, Implementation

UNIT 3:

Principles of public-key cryptosystems, The RSA algorithms, Other public key cryptosystems: Diffie-Helman key Exchange, Elgamelcryptographic system, Elliptic curve cryptography, pseudorandom number generation based onasymmetric cipher

UNIT 4:

Message authentication requirements, functions, message authenticationCodes, Security of MACs, MAC based Hash functions, MAC based ciphers

UNIT 5:

Digital Signatures: ElGamal Digital Signature scheme, schnorr digital signature schemes, digital signature standard

UNIT 6:

Web security considerations, Socket layer and transport layer and transport layer security
Electronic mail security: pretty good privacy, IP security overview, IP security policy, encapsulating security payload

Text Book:

1. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson, 5th Edition.

Book for Reference:

1. A Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone,CRC Press Series on Discrete Mathematics and Its Applications

****

12- FUNDAMENTALS OF CYBER SECURITY

Course Objectives

- To understand the Basic Concepts in Cyber Security
- To know about Classification of Cyber Security
- To understand the Present and Future Cyber Security

Course Outcome

At the end of the course, students will be able to;

- To know the latest trends in Ethical Hacking
- To understand the fundamentals of computer forensics, Evidence Collection Etc.

UNIT-1:

Introduction to Cyber Crime – Types of Cyber Crime – Classification of Cyber Criminals – Tools used in Cyber Crime – Challenges – Strategies – Cryptocurrency – Bitcoin – Blockchain - Ransomware.

UNIT-2:

Cyber Forensics Definition – Disk Forensics – Network Forensics – Wireless Forensics – Database Forensics – Malware Forensics – Mobile Forensics – Email Forensics

UNIT-3:

Ethical Hacking: Essential Terminology, Hacking windows – Network hacking – Web hacking – Password hacking, Malware, Scanning, Cracking.

UNIT-4:

Digital Evidence in Criminal Investigations: The Analog and Digital World, Training and Education in digital evidence, Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence,

UNIT-5:

Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection, Intrusion detection and Prevention Techniques, Anti-Malware software, Network based Intrusion detection Systems, Network based Intrusion Prevention Systems, Host based Intrusion prevention Systems,Security Information Management, Network Session Analysis, System Integrity Validation.

UNIT-6:

Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics.

Reference Books:

1. Dejey, Dr.Murugan, "Cyber Forensics", Oxford University Press, India, 2018.

2. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall.

3. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press.

4. John W. Rittinghouse, William M. Hancock, "Cyber Security Operations Handbook", ElsevierPub.

5. Deborah G Johnson, "Computer Ethics", 4th Edition, Pearson Education Publication.

6. Earnest A. Kallman, J.P Grillo, "Ethical Decision making and IT: An Introduction with Cases", McGraw
Hill Publication.

*****

13 - CYBER SECURITY LAW & PRACTICE

Objective of the Course:

- To help the students to understand Cyber Law and its need.
- Students will be able to know Information Technology Act 2000 and its benefits.
- To know about IPR, Patent etc.

Learning Outcomes:

After completion of the course, students would be able to;

- Know the basics of Cyber Security Law and Practices.
- Attain the knowledge about Intellectual Property Rights, Patent, Copy right, Trade Mark Law.

UNIT-1:

Introduction – Need for Cyber Law - Evolution of the IT Act, Genesis and Necessity - Salient features of the IT Act, 2000, various authorities under IT Act and their powers, Penalties & Offences, amendments.

UNIT-2:

Impact on other related Acts (Amendments) - Amendments to Indian Penal Code, Indian Evidence Act, Bankers Book Evidence Act, Reserve Bank of India Act - Cyber Space Jurisdiction.

UNIT-3:

E – commerce and Laws in India - Digital / Electronic Signature in Indian Laws - E – Commerce Issues and provisions in Indian Law - E – Governance concept and practicality in India - E – Taxation issues in Cyberspace - E – Contracts and its validity in India (f) Cyber Tribunal & Appellate Tribunal.

UNIT-4:

Intellectual Property Rights - Domain Names and Trademark Disputes - Concept of Trademarks / in Internet Era - Cyber Squatting - Reverse Hijacking - Jurisdiction in Trademark Disputes - Copyright in the Digital Medium - Copyright in Computer Programmes.

UNIT-5:

Cyber Laws in India – Crime against Individual – Crime against Property – Crime against Nation – Indian Case Laws.

UNIT-6:

International Cyber Laws Introduction – Cybercrime Legislation in the Netherlands – Cyber Laws in Malaysia – Cyber Laws in UK – Cyber Laws in United States – Australian Law related to Privacy.

TEXT BOOK:

1. Dejey, Dr.Murugan, Cyber Forensics, 2018, Oxford University Press.

REFERENCE BOOKS:

1. Harish Chander, Cyber Law and IT Protection, PHI Publication, 2012.
2. Philips, Computer Forensics and Investigations, Cengage Learning India Edition.

****

14 -CRYPTOGRAPHY - LAB

Objective of the Course:

- To implement the cryptographic algorithms.
- To implement the security algorithms.
- To implement cryptographic, digital signatures algorithms.

Learning Outcomes:

Upon successful completion of this assignment, students will be able to:

List of Experiments:

1. Write a C program that contains a string (char pointer) with a value \Hello World'. The program should XOR each character in this string with 0 and displays the result.
2. Implementation of Diffie-Hellman algorithm
3. Write a C program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result.
4. Write a Java program to perform encryption and decryption using the following algorithms: a) Ceaser Cipher b) Substitution Cipher c) Hill Cipher
5. Write a Java program to implement the DES algorithm logic.
6. Write a C/JAVA program to implement the BlowFish algorithm logic.
7. Write a C/JAVA program to implement the Rijndael algorithm logic.

8. Implementation of RSA based signature system
9. Write a Java program to implement RSA Algorithm
10. Calculate the message digest of a text using the SHA-1 algorithm in JAVA.

****

II SEMESTER

21- WEB APPLICATION SECURITY

Course Objectives

- To understand the web basics, HTML commands
- To know about various Web Penetration Testing methods
- To understand the Web Application Technologies and Attacks

Course Outcome

At the end of the course, students will be able to;

- To know the latest trends in Web Application Security Methods
- To understand the various Web Attacks and other techniques.

UNIT-1:

Web Fundamentals – HTML, HTTP 1.0 and 1.1- Client-side scripting, Server-side scripting- Web server architecture - Windows & Linux, IIS and LAMP servers- Network topologies and DMZ

UNIT-2:

Web Penetration Testing Methodology - Types of Web Penetration Testing - Web Pen Testing Approach – Core Defense Mechanisms

UNIT-3:

Web Application Technologies – Mapping the Application – Bypassing the Client-side Controls

UNIT-4:

Attacking the Authentication – Attacking the Session Management – Attacking access Controls

UNIT-5:

Attacking Back-End Components – Attacking Users: Cross-Site Scripting – Attacking Users: Other Techniques.

UNIT-6:

Automating Customized Attacks – Attacking Application Architecture – Attacking the Application Server

Text Books:

1. Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.
2. DafyddStuttard, and Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition, John Wiley & Sons, 2011.

References:

1. Wenliang Du, Computer Security – A hands-on Approach, First Edition, Createspace Independent Pub, 2017 4. https://www.owasp.org

*****

22- MALWARE ANALYSIS AND NETWORK SECURITY

Course Objectives

- To protect the network itself;
- To reduce the susceptibility of computer systems and applications to threats originating from the network; and,
- To protect data during transmission across the network.

Course Outcome

At the end of the course, students will be able to;

- To know the latest trends in malware attacks, monitoring and execution methods
- To understand the fundamentals of firewall, LAN attacks and Network Sniffing.

Unit I

Goals of Malware Analysis, AV Scanning, Hashing, Finding Strings, Packing and Obfuscation, PE file format, Static, Linked Libraries and Functions, Static Analysis tools, Virtual Machines and their usage in malware analysis, Sandboxing, Basic dynamic analysis, Malware execution, Process Monitoring, viewing processes, Registry snapshots, Creating fake networks,

Unit II

X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, Disassembly, Global and local variables, Arithmetic operations, Loops, Function Call Conventions, C Main Method and Offsets. Portable Executable File Format, The PE File Headers and Sections, IDA Pro, Function analysis, Graphing,

Unit III

Live malware analysis, dead malware analysis, analyzing traces of malware, system calls, api calls, registries, network activities. Anti-dynamic analysis techniques, VM detection techniques, Evasion techniques, Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching

Unit IV

Techniques for Network Protection: Firewalls, packet filter and stateful firewalls, application aware firewalls, personal firewalls-iptables, Proxies, NAT, Intrusion Detection System-Snort, Signature and Anomaly based detection, Honeypots and Honeynets, Network Log management-syslog or SPLUNK

Unit V

LAN attacks: ARP Cache poisoning, MAC flooding, Man in the middle attacks, Port Stealing, DHCP attacks, 10 VLAN hopping; Network Sniffing-wireshark and Password Cracking-John the Ripper;

Unit VI

Secure Network Communication: SCP, SSH, SSL3.0, TLS 1.2, STARTTLS, IPSec, VPN and Secure HTTP; Understanding the dark web, TOR traffic, Attacks on SSL/TLS: SSL stripping, Drown and Poodle attack; Encrypting and Signing Emails: PGP- GPG/openPGP,DKIM and SPF; Single Sign On (SSO)-OAUTH and OPENID; Network packet creation and Manipulation using scapy and dpkt libraries.

Text Books:

1. Michael Sikorski, Andrew Honig, Practical Malware Analysis: TheHands-On Guide to DissectingMalicious Software.

References:

1. Mike Shema, Anti-hacker toolkit, Tata McGraw Hill Publications, 2014.

*****

23- MOBILE SECURITY

Course Objectives

- To understand the Android Architecture and Framework
- To know about various Android Permission management
- To understand the information systems and software development

Course Outcome

At the end of the course, students will be able to;

- To know the latest trends in Android Application Package, Installation Process
- To understand the Android Device Security

UNIT-1:

Introduction - Android Versions – Android Architecture – Android Security Model – Android Framework

UNIT-2:

The Nature of Permissions – Permission Enforcement – System Permission – Custom Permission – Content Provider Permission

UNIT-3:

Android Application Package Format – Code Signing – APK Install Process – Package Verification

UNIT-4:

Android User Management – Types of Users – User Management – User Metadata – Per user Application Management – External Storage

UNIT-5:

Cryptographic Service Providers – JCA Engine Classes – Android JCA Providers

UNIT-6:

Network Security and PKI – Credential Storage – Device Security – Enterprise Security

Text Book:

1. Nikolay Elenkov, Android Security Internals, No Starch Press, 2015.

References:

1. Karim Yaghmour, Embedded Android, O'Reilly Publications, 2013.

*****

24 - CYBER SECURITY - LAB

Course Objectives

- To understand the TCP, Port Scanning using NMAP Tool
- To know about various SQL Injection methods
- To understand the information about Sniffing and E-mail Security
-

Course Outcome

At the end of the course, students will be able to;

- To know the latest trends in Cyber Security Tools.
- To understand the fundamentals of configuring your E-mail account against threats.

List of Experiments:

1. TCP Scanning using NMAP.
2. Port Scanning using NMAP
3. TCP/UDP Connectivity using Netcat
4. Network Vulnerability using OpenVAS
5. Web Application Testing using DVWA
6. Manual SQL Injection using DVWA
7. XSS using DVWA
8. Automated SQL Injection with SQLMAP
9. Demonstrate Sniffing using packet tool i.e. snort.
10. Configure your e-mail account against various threats. i.e. spam attack, phishing, spoofing etc.

References:

1. http://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/samplechapter/013 1407333.pdf
2. http://www.cs.nyu.edu/courses/fall04/G22.2262-01/assignments/assignment4_files/Ethereal_TCP.pdf
3. http://www.snort.org/docs
4. http://manual.snort.org/node27.html

*****