Course Name : Introduction to Digital Forensics	**Course Code** : ITSY 402
Pre Requisite : Network Security Assessment (ITSY302)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2

Goal: The course aims to provide the students with the foundational knowledge and skills necessary to conduct basic network forensics investigation using special forensics techniques and tools.

Objectives:
Upon completion of this course, the students should be able to:

1. Discuss the fundamental concepts pertaining to digital forensics.
2. Demonstrate the usage of the required skills, tools and techniques used in digital forensics.
3. Adopt an organized approach to ensure a successful investigation.

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Discuss the technical overview of networking and its various elements and their importance to forensics investigation.	Theory
2.Discuss important digital evidence concepts and methodologies in approaching network-based investigations, evidence acquisition and handling.	Theory
3.Demonstrate basic usage of common proprietary and open source tools for digital forensics.	Theory
4.Formulate a plan to perform a forensic investigation in a controlled environment.	Theory
5.Collect digital evidences in various forms such as packets and statistical flows.	Practical
6.Analyze evidences that were gathered from sources such as wired and wireless networks, intrusion detection systems, networking devices, end-user devices, web proxies, etc.	Practical
7.Submit the evidences and the results of the investigation in an organized and comprehensive form.	Practical

Software & Hardware Tools: Any tool

PHIL 3200	التخاطب باللغة العربية	ثلاث ساعات معتمدة
المتطلبات السابقة	لا يوجد	
الهدف العام	تقوية صلة الطالب بلغته العربية والأعتزاز بها وتأكيد دورها في حياته العلمية والعملية لاستيعاب ما يتلقاه من معارف وعلوم.	

النتائج	الأهداف الخاصة
١. قدرة الطالب على الكتابة والحديث بأسلوب علمي تقل فيه الأخطاء الاملائية والاسلوبية.	١. أن يمتلك الطالب المهارات الاساسية للتخاطب باللغة العربية حديثا وكتابة.
٢. الملم الطالب بمهارات الاختصار والايجاز في رسائل المخاطبات.	٢. أن يكتسب الطالب وسائل الاقناع لعرض ما يريد من أفكار واراء بأسلوب واضح ومعاني دقيقة.
٣. احتفاظ الطالب بالكثير من المعلومات التي اكتسبها في ثقافته الادبية واللغوية خلال تعليمه وتثقيفه الذاتي.	٣. أن يعمل الطالب على زيادة معرفته واهتمامه بلغته العربية لتنمية ذوقه الجمالي وزيادة مهاراته فيها.
٤. زيادة مهارات الطالب في لغته العربية حديثا وكتابة.	٤. أن يتمكن الطالب من توظيف معلوماته اللغوية لصالح ما اكتسبه من علوم وخبرات.

Course Name: Connecting Networks (Network-IV)	Course Code: ITNT401
Pre-Requisite: ITNT 301	Credit Hours: 3
Passing Grade: C	Level: B-tech – Year 4
No. Of Theory & Practical Hours : 1-4	

Goal: This course describes the architectures and considerations related to designing, securing, operating, and troubleshooting enterprise networks. This course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access. Also introduces software-defined networking, virtualization, and automation concepts that support the digitalization of networks

Objectives: The course should enable the student to learn the following areas

1. OSPF Concepts and Configuration
2. Network Security
3. WAN Concepts
4. Optimize, Monitor, and Troubleshoot Networks
5. Emerging Network Technologies

Outcomes At the end of this course, students should be able to:	Method
1. Explain how single-area OSPF operates in both point-to-point and broadcast multi-access networks.	Theory
2. Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.	Practical/ Theory
3. Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.	Practical/ Theory
4. Explain how ACLs are used as part of a network security policy.	Practical/ Theory
5. Implement IPv4 ACLs to filter traffic and secure administrative access.	Practical/ Theory
6. Configure NAT services on the edge router to provide IPv4 address scalability.	Practical/ Theory
7. Explain how WAN access technologies can be used to satisfy business requirements.	Practical/ Theory
8. Explain how VPNs and IPsec secure site-to-site and remote access connectivity.	Practical/ Theory
9. Explain how networking devices implement QoS	Practical/ Theory
10. Implement protocols to manage the network.	Practical/ Theory
11. Explain the characteristics of scalable network architectures.	Practical/ Theory
12. Troubleshoot enterprise networks.	Practical/ Theory
13. Explain the purpose and characteristics of network virtualization.	Practical/ Theory
14. Explain how network automation is enabled through RESTful APIs and configuration management tools.	Practical/ Theory

Al Musanna College of Technology

Department of Information Technology

Course Description Details

Bachelor (Software Engineering)		
Sl.No	**Course Code/Name**	**Course Description**
	PHIL4101 - Oman Civilization	Explain theeffects of geography on Omani civilization - Investigateand describe the significance of Omani civilization during the pre-Islam era - investigateand describe Oman's embracing of Islam - Investigateand describe the significance of Omani civilization during the caliphates ,ummait, and abbasi eras - Describe thecharacteristics of Islamic civilization - Describe thedevelopment, and external and internal supporting factors for Islamiccivilization - Describe theIslamic judicial system during the post-Islam eras

Course Name : Database Security	**Course Code** : ITSY 403
Pre Requisite : Structured Query Language (ITDB202)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2

Goal: This course aims to acquaint students with fundamental security concepts in a multiuser database environment. The course aims to enable the students to identify security threats, develop and apply appropriate security policy on a real time database system to protect sensitive information.

Objectives:
Upon completion of this course, the students should be able to:

1. Understand fundamental concepts related to database security.
2. Discuss common threats, vulnerabilities and various types of attacks against database security, along with appropriate countermeasures.
3. Apply their knowledge and skills to secure DBMS.

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Describe the terminology and concepts pertaining to various aspects of database security, and the requirements that motivate the field of database security.	Theory
2.Explain various attacks against the security of Databases, along with appropriate countermeasures.	Theory
3.Develop appropriate security policies and enforce them using suitable access controls, such Discretionary, Mandatory or Role-based access controls.	Theory
4.Implement Encryption and User Management in databases (including roles, privileges and profiling) to protect sensitive information contained in a database.	Practical
5.Audit an enterprise DBMS and develop an audit checklist.	Practical
6.Create virtual databases to enhance the security of databases.	Practical
7.Recognize the importance of database backup and recovery procedures.	Practical
8.Discuss various standards for database security, as well as database design.	Theory

Software & Hardware Tools: Any tool

Course Name : B-Tech Project - II	**Course Code** : ITSY 404
Pre Requisite : ITSY424	**Credit Hours** : 3
Passing Grade : C	**Level**: Year 4
No. of Practical Hrs : 2	

Goal: This course enables a student to develop a comprehensive solution for a secure application / penetration testing project using the skills and knowledge acquired up to the Bachelor Level

Objectives:
Upon completion of this course, the students should be able to:

1. Apply the Implementation and Testing Phases of System Development Life Cycle on the project.
2. Apply the technical and soft skills to provide the implementation & testing of the project.

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1. Perform implementation and testing of the course project based on the detailed design.	Practical
2. Apply the Implementation and Testing Phases of System Development Life Cycle on the project.	Practical
3. Practice work ethics and communication skills.	Practical
4. Prepare well-formatted standard documents.	Practical
5. Prepare a well formed design for the Project.	Practical
6. Demonstrate the course project in front of audience.	Practical

Software & Hardware Tools: Any tool

Course Name: Wireless Communication	Course Code: ITNT306
Pre-Requisite: ITNT103 Network Fundamental II	Credit Hours: 3
Passing Grade: C	Level: Advanced Diploma – Year3
No. Of Theory & Practical Hours : 2-2	

Goal: Wireless and mobility technologies are essential skills for a networking career in today's Digital Transformation. Mobility Fundamentals builds upon skills taught routing and switching concpets, providing learners foundational wireless knowledge and skills.

Objectives: The course should enable the student to:

1. Understand wireless networking technology basics (1,2)
2. Configure wireless LAN components (3)
3. Understand wireless LAN security
4. Design mobile networks and set up a home Internet access
5. Understand mobile networking applications, like BOYD

Outcomes At the end of this course, students should be able to:	Method
1. Understand Wireless Technologies and Understand Wireless LAN Standards	Practical/ Theory
2. Understand Wireless LAN components, Understand how Wireless LAN works and Understand how to plan a Wireless LAN deployment	Practical/ Theory
3. configure a wireless AP and Router, configure wireless Clients, and set up a home network	Practical/ Theory
4. Understand Wireless Threats and Vulnerabilities, Wireless Security Protocols for Authentication and Encryption, Mitigation Technologies, and Understand how to secure Enterprise Wireless LANs	Practical/ Theory
5. Comprehend what BYOD is, its benefits and challenges, BYOD adoption considerations, and BYOD design and solutions	Practical/ Theory
6. Recognize types of wireless interference , how to use tools to detect and manage interference, and troubleshooting wireless LAN connectivity	Practical/ Theory

Course Name : Research Methodology	Course Code : ITIS304
Pre Requisite : MATH311 - Probability and Statistics for Information Technology	**Credit Hours** : 3
Passing Grade : Depending on the Type of the course belongs to the Audit Degree	**Level**: Year III (Advanced Diploma)
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2
Goal: To enable students to use key concepts, terminologies, methods, techniques, and tools in writing a research relevant to Information Technology or Information System.	
Objectives: Upon completion of this course, the students should be able to: 1. Acquire knowledge on the key concepts, terminologies, methods, techniques, and tools in writing a research relevant to Information Technology or Information System. 2. Demonstrate knowledge and skills in writing a research paper. 3. Recognize the importance of research in the field of Information System.	
Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1. Discuss the key concepts and terminologies used in information technology research.	Theory
2. Discuss the methods and techniques relevant to IT research and the key issues in IT research.	Theory
3. Present the design for a particular research method in a simulated study in the information technology area	Theory
4. Use standardized software (like PSPP, SPSS, Excel, etc.) to analyze research data.	Practical
5.Interpret data emerged from the analysis and compare it with similar research areas	Practical
6. Synthesize research and technical reports to identify the decision points, to develop plans and to create action agendas.	Practical
7. Apply research findings to real world problems.	Practical

Course Name : Human-Computer Interaction	**Course Code :** ITIS401
Pre Requisite : None	**Credit Hours** : 3
Passing Grade : Depending on the Type of the course belongs to the Audit Degree	**Level**: Year IV (Bachelor)
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2

Goal: To introduce to students the principles, issues, tools and techniques of Human Computer Interaction which enable them to design, implement and evaluate interactive systems.

Objectives:

Upon completion of this course, the students should be able to:

1. Understand Human Computer Interaction and its importance in the design of interactive systems.
2. Produce prototypes of interactive systems using appropriate tools and technologies with the focus on HCI principles, methods, interaction styles, and techniques.
3. Recognize HCI issues such as Universal Design, Accessibility, Cultural Marker, and Usability.
4. Appreciate the importance of HCI in everyday lives.

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1. Discuss the basics of Human Computer Interaction and its related fields.	Theory
2. Discuss the concepts of user differences, user experiences and collaboration as well as how to design contextually.	Theory/Practical
3. Apply the concepts and principles of Human-Computer interaction.	Theory/Practical
4.Evaluate the different devices used for input and output and the issues/ opportunity associated with these devices.	Practical
5. Apply user modeling techniques and user interface principles and guidelines in the design of interactive systems to effectively meet users' needs.	Theory/Practical
6. Use different methods and techniques in HCI to carry out a complete user-centered design process.	Practical
7. Design prototypes of interactive systems using the latest tools and technologies.	Practical
8. Evaluate interactive systems using the latest techniques.	Practical
9. Discuss the new HCI innovations and emerging technologies.	Theory/Practical

Course Name : Network Security Management	**Course Code** : ITSY 405
Pre Requisite : Network Perimeter Security(ITSY304)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2

Goal: This course aims to introduce students the essential concepts and skills involved in network and security management, with particular emphasis on organization's critical functions

Objectives:
Upon completion of this course, the students should be able to:

1. Understand the network management functions, along with the tools and technologies currently available to support these functions.
2. Managing TCP/IP based networks by integrating appropriate security mechanisms into the existing network systems.
3. Use technology-based practices and a systematic approach to perform network troubleshooting.
4. Apply appropriate risk management strategy and mitigating the risks to critical data, systems, and applications.

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Explain the layers of network management, functions of network management components/tasks and the challenges & critical factors relating to the management of computer networks.	Theory
2.Compare and contrast significant network management standards such as SNMP V1, V2, V3, RMON, CMIS/CMIP, TMN, WBEM etc	Theory
3.Differentiate between Service Level Agreement (SLA), Operational level Agreement (OLS) and Underpinning Contract (UC).	Theory
4.Use effective network management and monitoring tools.	Practical
5.Evaluate performance of computer network and systems.	Practical
6.Formulate baselines for IT infrastructure performance and security.	Practical
7.Discuss the physical security measures to be considered to protect networking and communication facilities from security threats and environmental hazards.	Theory
8.Describe respective contingency planning approaches (such as IRP, DRP, BCP) for various security incidents and disasters.	Theory
9.Formulate network security policy in accordance with the security requirements of an organization	Theory

Software & Hardware Tools: Any tool

Course Name : Python for Penetration Testing	**Course Code** : ITSY 408
Pre Requisite : Ethical Hacking (ITSY305)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2
Goal: This course aims to prepare students to use Python scripting language for conducting penetration testing	

Objectives:
Upon completion of this course, the students should be able to:

1. Become familiar with Python programming language.
2. Develop custom scripts and tools for performing penetration testing.
3. Understand how Python could be used at each layer of TCP/IP protocol suite from security perspective.
4. Write scripts to demonstrate Python efficiency in accomplishing offensive/defense tasks involved in a Pen Test.

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Demonstrate how Python can be used to create tools and solve problems.	Theory
2.Use Python scripting to maximize the effectiveness of pen tests.	Theory
3. Build network applications using TCP Sockets.	Theory
4.Describe how to parse TCP Packets and PCAP data to extract valuable information.	Theory
5.Develop web application attack tools and deal with HTTP protocol vulnerabilities.	Practical
6.Use Python for basic forensic investigations.	Practical
7.Demonstrate python usage for attacks against wireless networks.	Practical
8.Design malware capable of evading modern antivirus systems.	Practical
Software & Hardware Tools: Any tool	

Course Name : Incident Response & Disaster Recovery	**Course Code** : ITSY 409
Pre Requisite : Introduction to Digital Forensics (ITSY402)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2
Goal: This course alms to impart concepts of incident response, business continuity and disaster recovery planning. along with necessary tools and techniques.	
Objectives: Upon completion of this course, the students should be able to: 1. Understand the concepts of effective incident response planning and implementation. 2. Apply their knowledge and skills to perform incident detection and reaction. 3. Obtain adequate knowledge and skills of disaster recovery 4. Gain basic knowledge and skills of business continuity	

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Describe concepts of effective incident response planning and implementation	Theory
2.Explain the concept of Incident Forensics.	Theory
3.Apply their knowledge and skills to perform incident detection and reaction.	Theory
4.Explain concepts of disaster recovery, business continuity and risk management.	Theory
5.Recommend contingency strategies including data backup, recovery and alternate site selection for business resumption planning.	Practical
6.Develop a contingency plan for a given emergency situation.	Practical
7.Develop a disaster recovery plan for a given emergency situation.	Practical
Software & Hardware Tools: Any tool	

Course Name : Biometric Systems	**Course Code** : ITSY 410
Pre Requisite : NIL	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2
Goal: The course aims to improve students' awareness on the state-of-the art biometric technologies and related security issues.	
Objectives: Upon completion of this course, the students should be able to: 1. Understand fundamental concepts, principles, components and practices pertaining to modern biometric systems. 2. Develop ability to build biometric systems that conform to international standards,	

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Describe various biometric technologies and the generic components of biometric systems.	Theory
2.Explain pattern recognition and feature extraction in biometrics.	Theory
3.Design and implement biometric authentication systems by selecting the most appropriate biometric for a given application.	Practical
4.Explain commonly used statistical measures to evaluate biometric systems.	Theory
5.Write and interpret biometric testing reports.	Practical
6.Discuss security, ethical and legal issues associated with biometrics.	Theory
Software & Hardware Tools: Any tool	

Course Name: Wireless Communication	Course Code: ITNT306
Pre-Requisite: ITNT103 Network Fundamental II	Credit Hours: 3
Passing Grade: C	Level: Advanced Diploma – Year3
No. Of Theory & Practical Hours : 2-2	

Goal: Wireless and mobility technologies are essential skills for a networking career in today's Digital Transformation. Mobility Fundamentals builds upon skills taught routing and switching concpets, providing learners foundational wireless knowledge and skills.

Objectives: The course should enable the student to:

1. Understand wireless networking technology basics (1,2)
2. Configure wireless LAN components (3)
3. Understand wireless LAN security
4. Design mobile networks and set up a home Internet access
5. Understand mobile networking applications, like BOYD

Outcomes At the end of this course, students should be able to:	Method
1. Understand Wireless Technologies and Understand Wireless LAN Standards	Practical/ Theory
2. Understand Wireless LAN components, Understand how Wireless LAN works and Understand how to plan a Wireless LAN deployment	Practical/ Theory
3. configure a wireless AP and Router, configure wireless Clients, and set up a home network	Practical/ Theory
4. Understand Wireless Threats and Vulnerabilities, Wireless Security Protocols for Authentication and Encryption, Mitigation Technologies, and Understand how to secure Enterprise Wireless LANs	Practical/ Theory
5. Comprehend what BYOD is, its benefits and challenges, BYOD adoption considerations, and BYOD design and solutions	Practical/ Theory
6. Recognize types of wireless interference , how to use tools to detect and manage interference, and troubleshooting wireless LAN connectivity	Practical/ Theory

Course Name : Malware Analysis	**Course Code** : ITSY 412
Pre Requisite : Ethical Hacking (ITSY305)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2
Goal: This course aims to introduce students with malware analysis (reverse engineering) techniques.	
Objectives: Upon completion of this course, the students should be able to: 1. Identify modern malware types 2. Understand malware analysis techniques 3. Perform malware analysis using appropriate tools and techniques	
Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Identify different types of malware and their characteristics	Theory
2.Explain various malware analysis methods	Theory
3.Analyze malware through reverse engineering and behavioral analysis	Practical
4.Analyze an Operating System as a target platform for malicious code	Practical
5.Evaluate defenses against malware attacks	Practical
Software & Hardware Tools: Any tool	

Course Name: Connecting Networks (Network-IV)	Course Code: ITNT401
Pre-Requisite: ITNT 301	Credit Hours: 3
Passing Grade: C	Level: B-tech – Year 4
No. Of Theory & Practical Hours : 1-4	

Goal: This course describes the architectures and considerations related to designing, securing, operating, and troubleshooting enterprise networks. This course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access. Also introduces software-defined networking, virtualization, and automation concepts that support the digitalization of networks

Objectives: The course should enable the student to learn the following areas

1. OSPF Concepts and Configuration
2. Network Security
3. WAN Concepts
4. Optimize, Monitor, and Troubleshoot Networks
5. Emerging Network Technologies

Outcomes At the end of this course, students should be able to:	Method
1. Explain how single-area OSPF operates in both point-to-point and broadcast multi-access networks.	Theory
2. Implement single-area OSPFv2 in both point-to-point and broadcast multiaccess networks.	Practical/ Theory
3. Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.	Practical/ Theory
4. Explain how ACLs are used as part of a network security policy.	Practical/ Theory
5. Implement IPv4 ACLs to filter traffic and secure administrative access.	Practical/ Theory
6. Configure NAT services on the edge router to provide IPv4 address scalability.	Practical/ Theory
7. Explain how WAN access technologies can be used to satisfy business requirements.	Practical/ Theory
8. Explain how VPNs and IPsec secure site-to-site and remote access connectivity.	Practical/ Theory
9. Explain how networking devices implement QoS	Practical/ Theory
10. Implement protocols to manage the network.	Practical/ Theory
11. Explain the characteristics of scalable network architectures.	Practical/ Theory
12. Troubleshoot enterprise networks.	Practical/ Theory
13. Explain the purpose and characteristics of network virtualization.	Practical/ Theory
14. Explain how network automation is enabled through RESTful APIs and configuration management tools.	Practical/ Theory

Course Name : Mobile Application Security	**Course Code** : ITSY 407
Pre Requisite : Mobile Computing (ITSE403)	**Credit Hours** : 3
Passing Grade : C	**Level**: B.Tech
No. of Theory Hrs: 2	**No. of Practical Hrs :** 2
Goal: This course aims to train students to create secure applications over Google Android or Apple iOS platforms.	
Objectives: Upon completion of this course, the students should be able to: 1. Understand the theoretical concepts behind secure application development in Android or iOS. 2. Apply their knowledge and skills to develop secure applications over Android or iOS SDK platforms.	

Outcomes Upon completion of this course, the students should be able to:	**Methodologies**
1.Explain the basic rules and principles of application security	Theory
2.Describe common mobile application security threats and vulnerabilities	Theory
3.Explain the security model of Android or iOS devices	Theory
4.Develop moderately complex apps using the Android or iOS SDK	Practical
5.Use security features of Android or iOS platforms and APIs	Practical
6.Leverage encryption for storage and communications	Practical
7.Harden mobile apps against attacks	Practical
Software & Hardware Tools: Any tool	