Book 4 – Business Aspects of Digital Forensics and Ethics

1. Introduction to Security and Digital Forensics

Scope Template

Number 1

Title Introduction to Security and Digital Forensics

Introduction This chapter serves as a background to introduce the business aspects of digital forensics within organisations. It starts by exploring the concept of cyberspace and its related implications on business organisations. Then, it discusses the various threats and cybercrimes that have become very popular in today online business environments. Furthermore, it defines several cybersecurity concepts, principles and terminologies that the reader need to be familiar with in order to understand the topics of the following chapters.

Outcomes - Demonstrate an understanding of the wider aspects of cyberspace and its security implications on business organisations.
- Build a working knowledge of various cybersecurity principles, concepts and terminologies.

Topics 1.1.Cyberspace and business organisations.
1.2. Cybercrimes and threats.
1.3. Cybersecurity principles and terminologies.

Study Guide

Task	**Time**
Preparation (Introduction and On-line Planning):	2 hr
Textbook Content:	4 hr
Thinking (On-line discussions, Review questions)	1 hr
Tutorial Work:	2 hr
Related Course Work:	1 hr
Total	**10 hours**

• Required study time: **4 one-hour lectures, 6 hour of preparations, solving review questions and other course work.**
• Required external resources including links and books:
1. **ISO/IEC 27000:2018** Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, https://www.iso.org/standard/73906.html
2. RFC 2828 Internet Security Glossary, https://www.ietf.org/rfc/rfc2828.txt
3. UK National cybersecurity strategy 2016-2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Content Template

Section Number 1.1

Section Title Cyberspace and business organizations

Introduction In this section, we start with a brief history about the Internet and the emergence of the World Wide Web as they represent the core components in the underling infrastructure of today cyberspace.

Content The early reported efforts to create a computer network environment was the ARPANET project of US Department of Defense (DoF) back in 1960s. The project was implemented as an academic network between two universities. In 1969, the first message was sent over this academic network.

The Internet

Various other packet switching networks were also developed, however, using different communication protocols. In 1970, the Internet Protocol suite TCP/IP became the standard communication protocol for ARRANET which later declared by the DoF as a standard communication protocol for all military networks. With the development of routing protocols, it became possible to connect several networks together, hence, the term internetworking emerged and abbreviated as "internet" which mean a network of networks.

Initially, the internet use was restricted and only utilized by research centers, military and other government agencies. Early 1990s the original ARPANET project decommissioned and in 1995 internet became commercially available by several Internet Service Providers.

The World Wide Web

Based on the idea of hypertext and linked applications, the British computer scientist Berners-Lee developed World Wide Web in 1989. It allowed browsing digital documents over the internet and the sharing information in a form of web pages. Later several web browsers became available such as Netscape, Internet Explorer and Chrome.

At the early days of the public internet (1990s-2000s), the Web became very popular and people started using it for communication, accessing information and shopping. At the beginning of that period, Websites were static HTML pages with hyperlinks and no backend databases. This period is usually called Web 1.0. Later interactive Web became very popular and web-programming languages such as PHP and ASP were extensively used to develop dynamic and database-driven website. This development has encouraged companies to move from static website into interactive ones to allow commercial transactions over the Internet.

This followed by another web development stage in 2004 which is named Web 2.0 and was based on the use of Ajax technology to allow instant user-generated content, collaborative content, virtual communities and online social networks. As a result, web application such as wiki, blogs, video sharing and online social network have become very popular.

Content Template

Section Number 1.1.1

Section Title The emergence of the cyberspace

Introduction This section introduces the concept of cyberspace, its components, and characteristics and benefits.

- Definition
- Characteristics
- Benefits

Content Nowadays we hear and read the prefix "Cyber" in several terms related to the online environment. For instance, cyberspace, cybersecurity and cyberattack. According to Oxford dictionary the term is related to and characterizes computer related cultures and environments including Information Technology and virtual reality. It abbreviated from the term cybernetic which refers to how technology is used to govern systems and their communications.

When it comes to the term "*Cyberspace*", it seems there is no agreement on a single definition, however, most of definitions share several aspects related to the meaning of the aforementioned term "Cyber". Maurer & Morgus (2014) define cyberspace as "The communication space created by the worldwide interconnection of automated digital data processingequipment". Another definition is presented by Kuehl who described it as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies".

Maurer & Morgus (2014) compiled a list of definitions, which represents how different countries view cyberspace. A sample from their list is presented in the table below:

Table 1.1: How different countries view Cyberspace

Country	Definition
France	A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them (individual, organizational, state)
Russia	Cyberspace is an interactive domain made up of digital networks that is used to store, modify andcommunicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.
UK	Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.
USA	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Lebanon	The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.

It is clear from the above various definitions that the cyberspace has the following characteristics:

1- Cyberspace is interactive allowing several stakeholders (individual, organizations or states) to interact with each other and perform different transactions and activities such as backing, trading, learning, socializing and even military cyber operations.

2- It comprises computing devises, digital storages and networking technologies to facilitate processing storage and communication.

3- It depends on utilizing the Internet and its related web technologies and protocol.

4- It is global and its boundaries are hard to be defined.

5- It is subject to security threats that could lead to security beaches with various level of impact on organizations, governments and individual.

Accordingly, we could identify the benefits of the cyberspace as follow:

1- Economic growth.

2- Promoting democracy, openness and transparency.

3- Improving and streamlining services.

4- Reducing pollution and traffic.

5- Cost reduction.

6- Knowledge dissemination.

Content Template

Section Number 1.1.2

Section Title Business organizations in cyberspace

Introduction This section discusses how organizations transformed from traditional physical ones into e-Business with various degrees of digitization to benefit from the cyberspace.

Content With the emergence of the cyberspace, business organizationshave realised that without utilising the technological related capabilities of this online environment, they will not be able to compete and survive. Adopting various online business processes including internal automation, e-marketing, e-commerce and online supply chain management, can give them the chance to expand their business, speed up operations and increase customer satisfaction. Nowadays, digital enterprises are very popular and they streamline most of their business transaction using information and commutation technologies. The following table adopted from Turban et al (2017) outline the how organisations have changed by comparing between traditional retail company and a digital one.

Table 1.2: Traditional versus Digital OrganisationTurban et al (2017)

Physical traditional organizations	**Digital organizations**
Selling in physical stores	Selling online
Internal inventory/ production planning	Online collaborative inventory forecasting
Paper catalogs	Smart electronic catalogs
Physical marketplace	Electronic marketplace
Use of telephone, fax, VANs, and traditional EDI	Use of computers, smartphones, the Internet, and extranets and EDI
Physical auctions, infrequently	Online auctions, everywhere, any time
Broker-based services, transactions	Electronic infomediaries, value-added services
Paper-based billing and payments	Electronic billing and payments
Paper-based tendering	Electronic tendering (reverse auctions)
Push production, starting with demand forecasting	Pull production, starting with an order (build-to-order)
Mass production (standard products)	Mass customization, build-to-order
Physical-based commission marketing	Affiliated, virtual marketing
Word-of-mouth, slow and limited advertisement	Explosive viral marketing, in particular in social networks
Linear supply chains	Hub-based supply chains
Large amount of capital needed for mass production	Less capital needed for build-to-order; payments can be collected before production starts
Large fixed cost required for plant operation	Small fixed cost required for smaller and less complex plant operation
Customers’ value proposition is frequently a mismatch (cost > value)	Perfect match of customers’ value proposition (cost < = value)

Content Template

Section Number 1.2

Section Title Cybercrimes and threats

Introduction This section starts by defining the term cybercrime in additional to the concepts of threat and threat agent. Then it presents various forms of cybercrimes.

Content While there is no agreement on a single universal definition for cybercrimes, one can think about any illegal activity related to information and communication systems. Where these systems was the subject of the crime or a means for committing the crime. Broadhead (2018) offered three definitions for the cybercrime:
1- Any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT).
2- Cybercrime in a narrow sense ("computer crime" [a.k.a. "cyber-dependent crime"]): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
3- Cybercrime in a broader sense ("computer-related crime" [a.k.a. "cyber-enabled crime"]): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as possession, offering or distributing information by means of a computer system or network.

Cybercrimes are associated with the existence of a threat, which represents a potential for violating security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm where internationally or accidentally (RFC2828). Table 1.X is list the consequences of security threats.

Table 1.3: consequences of security threats

Consequence	**Description**
1. (Unauthorized) Disclosure	A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
a. Interception	A threat action whereby an unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations
b. Inference	A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications.
c. Intrusion	A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections
2. Deception	A circumstance or event that may result in an authorized entity receiving false data and believing it to be true
a. Masquerade	A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
b. Falsification	A threat action whereby false data deceives an authorized entity.
c. Repudiation	A threat action whereby an entity deceives another by falsely denying responsibility for an act.
3. Disruption	A circumstance or even that interrupts or prevents the correct operation of system services and functions.
a. Incapacitation	A threat action that prevents or interrupts system operation by disabling a system component.
b. Corruption	A threat action that undesirably alters system operation by adversely modifying system functions or data.

c. Obstruction	A threat action that interrupts delivery of system services by hindering system operations.
4. Usurpation	A circumstance or event that results in control of system services or functions by an unauthorized entity.
a. Misappropriation	A threat action whereby an entity assumes unauthorized logical or physical control of a system resource.
b. Misuse	A threat action that causes a system component to perform a function or service that is detrimental to system security.

Usually, threat is associated with threat agent to represents an individual or a group with the potential to commit a cybercrime.Table 1.X is adopted
from Broadhead (2018) who categorizedthreat agents based on identities, group affiliations, capabilities and motivations.

Table 1.4: threat agent classification (Broadhead,2018)

Threats Agent	**Description**
Individuals and small criminal groups	Primary motivation is profit-seeking. This group includes opportunistic offender, and habitual offenders and criminals.
Insiders	Represent those who work inside the organization. They are a source for intentional threat, negligence and error. This groupincludes employees, individuals (e.g., contractors) with access and/or credentials to Information and communicationstechnology (ICT) of organizations.
Organised criminal groups (OCGs)	defined as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences, in order to obtain, directly or indirectly, a financial or other material benefit. This group include traditional organized crime groups (ICT enhances OCGs' terrestrial criminal activities) and organizedcybercrime groups (OCG with online-exclusive operations)
State and state-affiliated agents	Those who operate for political, diplomatic, technological, commercial and strategic advantage, targeting government, defense, finance, energy and telecommunications sectors. This group includes foreign intelligence services and agencies, and State-sponsored individuals and small groups.
Hacktivists	Ideologically motivated individuals or groups who utilized cyberspace to perform cyberattacks as a form of protest. This group includes specific-issue-motivated individuals (e.g., Anonymous) and groups co-operating based on various events in an ad hoc manner.
Cyberterrorists	Cyber terror activities are mainly targeting critical infrastructure, networks an online service. Usually the goals is to cause financial loses, raise fear among the masses, and force the political leadership to implement the terrorists' demands. Additionally, they target social media accounts; however, propaganda and planning attacks (especially via encryptedcommunication applications such as Telegram) are also major activities and threats. This group include extremists or racist groups.
Script kiddies	Those who use online available hacking tools to conduct cyberattacks, such as web defacements and DOS attack. This group includes young individuals (hence 'kiddies').

Accordingly, we can identify the following forms of cybercrimes:
- **Vandalism**: the act of destroying Information system resources, which might affect availability and/or reputation. A popular form this attack is website defacement by which attacker change the content of a particular web page.
- **Espionage:** the act of spying to collect sensitive information using various electronic means to achieve political, economic or military advantages.
- **Denial of Service (DoS):** any act which renders system resource or information unavailable. A common form of such crime is to flood a system with large number of requests, thus, it cannot process any additional request.
- **Intrusion:** is the act of accessing or attempt to gain access to system resource without having authorization to do so.
- **Phishing**: is a crime by which criminal obtain sensitive information by the mean of sending fraudulent communication such as email or instance message disguising as trusted organizations such as bank or well-known company. It is a form social engineering attack, which exploits human weaknesses. Attacker tricks victim to share information or to perform act that might help the criminal to perform further authorized actions.
- **Using Malware/Ransomware**: a popular form of cybercrimes realized by malicious software to infect the victim system for the purposed of bypassing access controls, stealing information or blackmailing. Recently we have witnessed increased number of crime related to Ransomware, which is a form of malicious software to lock/encrypt victim’s personal information and them ask him/her for a ransom (usually in a form of cryptocurrency) to get it back.

Content Template

Section Number 1.3

Section Title Cybersecurity principles and terminologies

Introduction This section defines several cybersecurity concepts, principles and terminologies that the reader need to be familiar with in order to understand the topics of the following chapters. Definitions in this section adopted from the Internet Engineering Task Force’s Request For Comments 2828 (IETF RCF 2828).

Content Information security is usually defined using three concepts: Confidentiality, Integrity and Availability. A secure system is the one, which ensure these three properties by providing the required countermeasures to prevent or detect any form of crime that might affect these characteristics. They can be defines as follow:

- **Confidentiality**: It means that information is only accessible/readable by those who has the authorization to do so.
- **Integrity**: It is all about the accuracy of information and detection of authorized modification or tampering with data.
- **Availability**: It is related to the accessibility of the information and system resource whenever they are needed.

Additionally, security concepts are related to the above mentioned concepts:

- **Authentication**: is the process of verifying that the use is the one who is claiming to be. It consists identification step by presenting identification information, and verification step by presenting authentication information to proof the claimed identify.
- **Authorization**: is the process of identifying access permissions. It consists of identifying who can assess to system resources and what action he/she can perform on these resources.
- **Accountability**: the ability to trace all actions performed on the system resources. Usually, this can be done by logging all the action related details such as: what type of action, who performed the action, on which resources and when the action was performed. Thus, a user can be held responsible for his/her action.
- **Non-repudiation**: the ability to prevent the false denial of being part of action/communication. Digital signature can be used to implement Non-repudiation service.
- **Attack**: an assault on the system that can lead to violate its security policy.
- **Vulnerability:** a weakness in the system or its environment, which can lead to security attack.
- **Risk:** is the probability that a threat agent would utilize an existing vulnerability to attack system resources and cause a harm.

Activity Template

Number	1.1
Title	**Real Cybercrime cases**
Type	Reflection
Aim	ILOs: 1 and 2 The activity aims to let the student read more on recent real cybercrime cases and related them to what he/she has learnedin this chapter.
Description	Section 1.2: Cybercrimes and threats Search for three recent (in the last five years) major security incidents representing different types of cybercrimes. Discuss their nature, threat agents, motivation and impact on targeted organizations.
Timeline	Time: 1-3 hours of reading.
Assessment	Each student is required to submit a 1-2 pages report of his/her findings and then present it in the class as open discussion session.

Activity Template

Number	1.2
Title	The Insider Threat: Real Defense for Real Businesses
Type	Reflection
Aim	ILOs: 1, 2 The activity aims to allow student to explore the threat of insider and how it can affect business organisations
Description	Section 1.2: Cybercrimes and threats Visit DARK Reading archive at: https://www.darkreading.com/webinar_archives.asp Watch the one-hour webinar titled: The Insider Threat: Real Defense for Businesses. Write one page summarizing what youhave learned from this Webinar.
Timeline	Time: 1-3 hours.
Assessment	The student should submit one page summary of what he learned from the webinar.

Think Template (MCQs)

Number 1.1

Title Cyberspace and business organisations

Type Fill in the blanks

Question In 1970, the Internet Protocol suite ____________ Protocolbecame the standard communication protocol for ARRANET which later declared by the DoF as a standard communication protocol for all military networks.

Answers a) Border Gateway Protocol (BGP).

b) Global System for Mobile communications (GSM).

c) Transmission Control Protocol/Internet Protocol (TCP/IP).

d) Open Shortest Path First (OSPF).

Answer: c

Think Template (MCQs)

Number 1.2

Title Cyberspace and business organisations

Type Choose correct answer

Question Which of the following is a characteristic of Web 2.0?

Answers a) Static web

b) Allow instant user-generated content

c) Traditional server-side web application

d) Secure

Answer: b

Think Template (MCQs)

Number	1.3
Title	The emergence of the cyberspace
Type	Choose correct answer
Question	Which of the following is not a benefit of the Cyberspace
Answers	a) Economic Growth b) Promoting Democracy c) Disseminating Knowledge d) Increasing Pollution **Answer: d**

Think Template (MCQs)

Number 1.4

Title Cybercrimes and threats

Type Fill in the blanks

Question Message ________ means that the sender and the receiver expect secrecy

Answers a) Confidentiality.

b) Integrity.

c) Availability

Answer: a

Think Template (MCQs)

Number	1.5
Title	Cybercrimes and threats
Type	MCQ
Question	A customer purchases an item from an e-commerce site. The e-commerce site must maintain proof that the data exchange took place between the site and the customer. Which Security Services is achieved
Answers	a) Confidentiality. b) Integrity. c) Availability d) Non-repudiation **Answer: a**

Extra Template

Number	1.1
Title	The History of the Internet
Topic	• 1.1
Type	Byung-Keun Kim, Internationalizing the Internet: The Co-evolution of Influence and Technology, Edward Elgar Publishing, 2005

Extra Template

Number	1.2
Title	Compilation of existing cybersecurity and information security related definitions.
Topic	• 1.1.1
Type	Maurer, T., & Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. New America. https://www. newamerica. org/cyber-global/cyberdefinitions.

Extra Template

Number	1.3
Title	Electronic commerce 2018: a managerial and social networks perspective
Topic	1.1.2
Type	Book:

Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2017). Electronic commerce 2018: a managerial and social networks perspective. Springer.

Extra Template

Number	1.4
Title	The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments
Topic	1.2
Type	Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. Computer Law & Security Review.

Extra Template

Number	1.4
Title	The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments
Topic	1.2
Type	

ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, https://www.iso.org/standard/73906.html

Extra	**Template**
Number	1.5
Title	The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments
Topic	1.2
Type	

UK National cybersecurity strategy 2016-2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Extra Template
Number 1.6
Title RFC 2828–Internet security glossary
Topic - 1.2

- 1.3

Type IETF technical Document:

Shirey, R. (2003). RFC 2828–Internet security glossary, 2000. URL: http://www. faqs. org/rfcs/rfc2828. html.

2. Managing Security in Business Organisation

Scope Template

Number	2
Title	Managing Security in Business Organization
Introduction	This chapter establishes the foundation for the understanding of information security management. It explains the importance of planning and presents its components. Also, it explores a method for managing risks by identifying, analyzing and then treating them. Furthermore, it describes the need for contingency planning and summarizes its components. Finally, it introduces the steps of incident response methodology.
Outcomes	Demonstrate a solid understanding on the way to manage information security. ILO 1: Understand major concepts related to security governance ILO 2: Understand major concepts related to risk management ILO 3: Understand major concepts related to contingency planning ILO 4: Understand major concepts related to incident response methods & preparations
Topics	2.1.Security governance, planning and policies 2.1.1.Security governance 2.1.2.Security Planning 2.1.3.Security Policies 2.2.Security Risk Management 2.2.1.Risk Identification 2.2.2.Risk Analysis 2.2.3.Risk Treatment 2.3.Contingency planning 2.3.1.Business Impact Analysis 2.3.2.Disaster Recovery Plan 2.3.3.Business Continuity Plan 2.4. Incident Response 2.4.1 Planning and Preparation 2.4.2 Methodology

Study Guide

Task	**Time**
Preparation (Introduction and On-line Planning):	2 hr
Textbook Content:	4 hr
Thinking (On-line discussions, Review questions)	2 hr
Tutorial Work:	2 hr
Related Course Work:	1 hr
Total	**11 hours**

1. Required study time: **4 one-hour lectures.**

2. Required external resources including links and books:
1. Whitman, M., Mattord, H. (2018). **Management of Information Security**, 6th Ed. Cengage Learning.
2. ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management
https://www.iso.org/standard/75281.html
3. Brotby, K. (2009). **Information Security Governance: A Practical Development and Implementation Approach**, Wiley.

4. Peltier, T. (2010). **Information Security Risk Analysis**, 3rd edition, Auerbach Publications.
5. ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security
https://www.iso.org/standard/43754.html
6. ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview
and vocabularyhttps://www.iso.org/standard/73906.html
7. Luttgens, J., Pepe, M., Mandia, K. (2014), **Incident Response & Computer Forensics**, 3rd edition, McGraw

Content Template	
Chapter	2
Section Title	Managing Security in Business Organization
Introduction	This chapter establishes the foundation for the understanding of information security management. It explains the importance of planning and presents its components. Also, it explores a method for managing risks by identifying, analyzing and then treating them. Furthermore, it describes the need for contingency planning and summarizes its components. Finally, it introduces the steps of incident response methodology.
Content	Each organization collects, transmits and stores sensitive information. Such information should be kept confidential, and available whenever needed by authorized users. This information is considered as the assets of organization which requires protection. The loose of one of its security properties such as confidentiality, integrity, and availability could be catastrophic to the organization and might lead to massive financial loose. Protecting information assets is essential for the organization to achieve its goals and objectives. An information security management system (ISMS) is a systematic approach for managing information and keeping it secure. It consists of policies, procedures, guidelines, and activities defined and managed by an organization to protect information assets. It is based on identifying, analyzing risks, and then implementing appropriate controls to protect these assets from any potential risks. This chapter consists of four sections. The first one introduces security governance and policies. Then, section two focuses on risk management. Section three is about contingency planning. Finally, section four explains how an organization should respond to incidents.

Content Template	
Section Number	2.1
Section Title	Security governance, planning and policies
Introduction	This section gives an overview of the governance security of an organization. It presents the objectives of governance and the responsibilities of the roles. Also, it introduces the ISO/IEC 27014:2013 standards. Furthermore, this section introduces the elements of a security plan and the characteristics of policies.
Content	The first step of the information security management is defining the framework and plan that aims at tackling security in the organization, and states the security policies together with the guidelines.

Content Template	
Section Number	2.1.1
Section Title	Security governance
Introduction	// same as above
Content	Information Security Governance is an information security management at the organizational level. The Information Security Audit and Control Association (ISACA) states that governance is: "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly". Governance is the basis of the information security management system, as it defines the framework for handling policies in the organization. It describes security at a high level, and states the outlines that should be followed and implemented in the organization. 1. The objective of information security governance is to provide a security framework that satisfies the needs of the organization. This framework includes a comprehensive strategy for information security in line with the organization objectives. Furthermore, the framework includes the security policies and the standards for each policy. 2. 3. An effective security governance should provide the following six outcomes (Brotby, 2009): 1. Strategic alignment: The alignment of security strategy and activities with the business strategy of the organization to support its objectives. 2. Risk management: The identification and analysis of security risks to minimize their impact to an acceptable level. 3. Business process assurance/convergence: Investigating the possibility of integrating all assurance processes to maximize the effectiveness and efficiency of security activities. 4. Value delivery: The optimization of Security investments in order to support organizational objectives. Optimal investment levels are accepted when strategic goals ofsecurity are achieved. Also, an acceptable risk level is attained by the organization at the lowest possible cost of security activities that consume considerable resources. 5. Resource management: The efficient and effective use of information security knowledge infrastructure. 6. Performance measurement: The measurement of information security processes to ensure that organizational objectives are achieved. Information security governance is tackled by different roles in an organization at different levels which are required for effective information security governance. These roles and their responsibilities are:

- **Board of directors:** A board of directors is a group of people that represents the stakeholders of the organization. Usually they are elected by the stakeholders or the organization to act on their behalf. The main responsibility of the board of directors related to the information security governance is establishing policies and security strategic plans to ensure the proper management of information security.

- **Executive Management:** The executive management is responsible for daily management of the organization. It consists of individuals that represent the highest level of management in the organization, such as the president of the organization and chief executive officer (CEO) and other executives. Their main responsibility is providing support to the information security projects to succeed.

- **Steering Committee**: It includes members of executives from the organization such as chief executive officer (CEO), chief financial officer (CFO), information officer (CIO), chief information security officer (CISO), human resources, legal, risk management, audit, operations and public relations. This committee serves as a communicating channel between different departments in the organization as information security affects all aspects of the organization.

- **Chief Information Security Officer (CISO):** CISO is the highest position in the information security department. Almost all organizations have CISO responsible for establishing and implementing strategies to protect the confidentiality, integrity, and availability of information assets in the organization.

ISO/IEC 27014:2013

One of the well-known standards in information security governance is The ISO/IEC 27014:2013. It was released on the 15th of May 2013 as part of the ISO/IEC 27000 series of standards. This standard is aimed at helping organizations govern their information security arrangements. It provides guidance related to the concepts and principles of the governance of information security applicable to all types and sizes of organizations. The standard provides a framework of six principles and five processes. The principles are:

i Principle 1: Establish organization-wide information security.

i Principle 2 - Adopt a risk-based approach.

i Principle 3 - Set the direction of investment decisions.

i Principle 4 - Ensure conformance with internal and external requirements.

i Principle 5 - Foster a security-positive environment.

i Principle 6 - Review performance in relation to the business outcomes.

The five processes are: evaluate, direct, monitor, communicate, and assure. These five processes form a cycle for the governance of information security. The governing body ***givesdirection*** regarding the information security objectives, and strategy that needs to be implemented. The outputs of these processes are security strategies and policies. The performance of these strategies are ***monitored***. Based on the output of the monitor process, the governing body ***evaluates*** the current achievement of security objectives and determines if any adjustments are required to optimize the

	achievement of strategic objectives in the future. In the ***communicate***process, the governing body and stakeholders exchange information about information security appropriate to their specific needs. Finally, the ***assure*** process identify and validate the objectives and actions related to carrying out governance activities and conducting operations in order to attain the desired level of information security.

Content Template	
Section Number	2.1.2
Section Title	Security Planning
Introduction	// same as above
Content	This section describes the security planning at the organizational level and the plan for information security systems. This plan is different from contingency planning, which describe plans for an abnormal event. Contingency planning is described in Section 2.3. Planning is an important step in the information security management. Good planning enables the organization to get the maximum of its resources. The primary goal of organizational planning is to meet the organization objectives. The first step for developing a plan is to define the value statements, vision, and the mission of the organization. The vision statement states what the organization wants to become, while the mission expresses what the organization is. For example, Google mission is "to organize the world's information and make it universally accessible and useful", while its vision is "to provide access to the world's information in one click". Each department in the organization should have its vision and mission in line with the mission and the vision of the organization. Once the values, mission, and vision are stated, the next step is defining the strategic plan, goals, objectives and the action plan. The strategic plan contains the approach on how to achieve the vision from the mission. The goals are the statements that the organization or department wants to achieve. Usually, the goals of information security department emphasize the confidentiality, integrity and the availability of information. In order to achieve the goals, objectives should be defined to measure the progress needed to achieve the goal. Finally, the action plan is defined to include all the detailed actions and activities needed to achieve the goals within the constraints of the objectives. Example: A company may target one of its goals to protect the confidentiality of information of their employees within the organization. In order to achieve this goal, the organization defines the following objectives: • Install an anti-virus software on all machines in the organization and update it regularly. • Install a firewall. • Implement an intruder detection system.

Content Template	
Section Number	2.1.3
Section Title	Security Policies
Introduction	// same as above
Content	The success of information security plans depends on the security policies defined in the organization. A policy is a high level statement of the organization that states the acceptable and unacceptable behavior to assure the confidentiality, integrity, and availability of information. Security policies identify their requirements without specifying any implementation. They are placed in other documents called standards, procedures, practices, and guidelines. All policies should contain the following basic components: • **Purpose:** describes the need for the policy, typically to protect the confidentiality, integrity, and availability of information. • **Scope:** describes the people, systems, and organization covered by the policy. • **Responsibilities:** describe the responsibilities of the members in the organization as well as the information security employees. • **Compliance:** describes how to measure the policy. *Standard* is a more detailed statement of what must be done to comply with the policy. *Guidelines* are more general statements designed to achieve the policy objectives by providing a framework within which to implement procedures. *Procedures*spell out the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment. A procedure is a step-by-step guide for accomplishing a task. They are low level and specific. Example: assume that there is a policy restricting access to information security. In this case, the policy could be stated as: "access to organization information systems is restricted to authorized users only." The standard can specify that each user should have a user ID and a confidential password. Guideline can specify restriction on the password such as the length of the password be at least eight characters and contains alphabet and number. Passwords should be five to eight alphanumeric characters. The procedure of getting the password can be described by the following steps: iThe user should apply for a username and password. iThe user is assigned a role based on the role assignment procedure. iThe user should agree and sign the user account security policy. iCreate a username and initial password, and force the user to change the password on the next login.

Content Template	
Section Number	2.2
Section Title	Security Risk Management
Introduction	This section introduces the method for coping with risks. It describes how to identify, analyze, and evaluate risks. Then, it presents techniques to treat risks.

Content	Security risk management is an ongoing process of identifying risks, and then implements plans to treat them using a risk treatment plans. The objective of risk management is to create a level of protection that mitigates vulnerabilities to threats and potential consequences, thereby reducing risk to an acceptable level. The process consists of two steps: risk assessment and risk treatment. Risk assessment includes identifying, analyzing, and evaluating the risk. The main goal is to make risk level acceptable.

Content Template	
Section Number	2.2.1
Section Title	Risk Identification
Introduction	// same as above
Content	Risk identification includes identifying the assets, threats, existing controls, vulnerabilities, and consequences. **Identification of Assets**: The first step in risk identification is systematically discover and identify assets. An asset is anything that has value to the organization, and therefore requires protection. An asset can be information, software, hardware, etc. The most important issue at this step is having a comprehensive list of assets, and this requires interviews with the people in the organization and the head of the departments. **Identification of Threats:** After identifying the assets that require protection, the threats to those assets must be identified as well. Threats are possible dangerous to the assets, and therefore they are a potential source that could affect the confidentiality, integrity, or availability of the system. Threats can be natural such as earthquake or human being. They may arise from inside the organization or from outside. One of the most common threats that affects the security of information system is the unauthorized access to information through bugs in the system. Another threat is the spreading of viruses in the network of the organization either through emails or via USB driver. **Identification of existing control:** The third step is determining the current existing controls. The goal of this step is determining the adequacy of these controls for avoiding the identified threats, and also to avoid duplication of controls. **Identification of vulnerabilities:** After identifying assets, threats, existing controls in the organization, the next step is identifying vulnerabilities that can be exploited by threats to cause harm to assets or to the organization. Vulnerability does not cause harm unless the existence of a threat to exploit it. As an example to distinguish between threats and vulnerabilities, is a system that allows weak passwords. The vulnerability is that a password is vulnerable for dictionary or brute force attacks, whereas the threat is an intruder that can exploit the password weakness to break into the system. Examples of vulnerabilities in a system include insufficient software testing, unchecked user input, insecure network communication. **Identification of consequences:** The last step is identifying the consequences of losing confidentiality, integrity and availability that may have on the assets.

<table>
<tr><th colspan="2">Content Template</th></tr>
<tr><td><b>Section Number</b></td><td>2.2.2</td></tr>
<tr><td><b>Section Title</b></td><td>Security Analysis</td></tr>
<tr><td><b>Introduction</b></td><td>// same as above</td></tr>
<tr><td><b>Content</b></td><td>
Risk analysis is the process of analyzing the risks and their consequences on the organization. Risk analysis could be qualitative or quantitative. Qualitative risk analysis is usually based on a scale such as low, medium, high to describe the potential affect of the consequences of a risk. Whereas, quantitative analysis uses a numerical rating between 0.1 (low) to 1.0 (high) or from 1 to 100. The analysis is based on the impact of threats on the organization. Also, it is based on the overall rating of the probability that a specific vulnerability can be exploited.
After determining the probability and the impact, the risk level is calculated based on a matrix. An example of such a matrix for qualitative risk measure is given in the following table:

Table 1: Probability Impact Matrix*
<table>
<tr><td colspan="2"></td><td colspan="3"><b>Impact</b></td></tr>
<tr><td colspan="2"></td><td><b>High</b></td><td><b>Medium</b></td><td><b>Low</b></td></tr>
<tr><td><b>Probability</b></td><td><b>High</b></td><td>High</td><td>High</td><td>Medium</td></tr>
<tr><td></td><td><b>Medium</b></td><td>High</td><td>High</td><td>Medium</td></tr>
<tr><td></td><td><b>Low</b></td><td>Medium</td><td>Medium</td><td>Low</td></tr>
</table>
<b>High - Corrective action must be implemented</b>
<b>Medium - Corrective action should be implemented</b>
<b>Low - No action required at this time</b>

*Dumbrava, V. and Iacob, V.-S. (2013) Using Probability-Impact Matrix in Analysis and Risk Assessment Projects, Journal of Knowledge Management, Economics and Information Technology, 2013

After the risk level is determined, the risk management team should identify the controls or safeguards that could possibly eliminate the risk, or at least reduce the risk to an acceptable level.

Therefore, it will be important to identify all of the controls and safeguards that the team believes could reduce the risk to an acceptable level. By doing so, the team will be able to document all of the options for consideration.

Example: The following table describes three risks in an organization. The first risk is guessing the password of users. The likelihood of such risk is medium and the effect is also medium on users. Therefore, based on the table, the risk level is high and needs actions to be implemented.

The second risk is the SQL injection attack on the user login page on the organization website. The likelihood of such attack is medium but the impact is very high and, therefore, the risk level is high and needs action. Finally, the likelihood of spreading viruses in the organization network is high and its impact is high as well. Therefore, the risk level is high, and an immediate action is required.
<table>
<tr><td>Risk</td><td>Likelihood</td><td>Impact</td><td>Risk Rating</td></tr>
<tr><td>User passwords can be guessed</td><td>M</td><td>M</td><td>H</td></tr>
</table>
</td></tr>
</table>

SQL injection attack	M	H	H
Spreading of viruses	H	H	H

Content Template	
Section Number	2.2.3
Section Title	Risk Treatment
Introduction	
Content	The next step after evaluating the risks of the threats and identifying their levels is to control the risks. There are four strategies to deal with risks. These strategies are: 1. **Avoidance:** This control strategy attempts to prevent the exploitation of vulnerability by changing policies, training employees, or implementing security controls. For example, to deal with the password guessing attacks, new security policies should be defined to make password more difficult. This can be done by enforcing users to have complex passwords by including numbers and special characters. Security awareness training for employees could help to reduce such a risk. 2. **Transference:** This control strategy attempts to shift the risk outside the entities. In this case, instead of hiring employees or buying hardware and software to deal with the risk, the company may decide to outsource this process to a specialized company to deal with the risk. For example, if the company has a Web services, then it can transfer the process of implementation and dealing with its associated risks to a third party. 3. **Mitigation:** This control strategy attempts to reduce the damage caused by the exploitation of the vulnerability. This approach includes three types of plans: incident response, disaster recovery, and business continuity. More details of these plans are given in Sections 4.1, 2.3 and 2.4. 4. **Acceptance:** This strategy decides to take no action. This is because the security risk level is low, and the cost of dealing with such a risk is usually higher than the consequences of the risk itself.

Content Template	
Section Number	2.3
Section Title	Contingency Planning
Introduction	This section presents the way to plan for unexpected events such as attacks. First, it describes the business impact analysis, and then introduces two plans: Disaster Recovery Plan and Business Continuity Plan.
Content	Section 2.1.2 introduced the topics of planning for an organization in general and for information security in particular. This section focuses on planning for unexpected events. A contingency plan states the required actions for unexpected events such as a security breach. The overall process of contingency planning is based on preparation to detect, response, and recover from the unexpected events. The main goal is to restore the normal mode of the organizational operation with a minimal cost after the occurrence of unexpected events. The plan consists of following four components: • Business Impact Analysis (BIA): to determine critical business functions and information systems. • Incident Response Plan (IR): to respond immediately to an incident • Disaster Recovery Plan (DR): to focus on restoring operations at the primary site. • Business Continuity Plan (BC): to enable business to continue at an alternate site**.** The following subsections describe BIA, DR, and BC plans. While the next section present the incident response plan.

Content Template	
Section Number	2.3.1
Section Title	Business Impact Analysis (BIA)
Introduction	
Content	The Business impact analysis is a key step in the contingency planning process. It is the process of identifying and understanding the impact of a disruption on the organization operations. The two primary impact of any business disruption are the operational impact and the financial impact. The BIA analysis is different from that of risk analysis. Risk analysis focuses on risks that organization can be exposed to and determine the measures to be taken to minimize the risk. Whereas, BIA analyzes the consequences of incidents. Business impact analysis includes the following steps: • **Threat Identification:** in this step, all potential threats are identified, similar to the risk identification step. It is used in the contingency planning to determine the extent of damage for a successful attacks. • **Business Unit Analysis**: in this step, all business functions are identified. Also, the functions are prioritized to determine the importance of the function to the organization. Furthermore, the interdependencies between the functions are identified. • **Potential Damage Assessment**: In this step, the damage that could result from an attack is identified, and the cost is estimated. This allows the organization to identify the actions to be taken in the case of attacks. • **Establishing Recovery Time Objective (RTO)** In this step, the RTO is identified to indicate the targeted duration of time a system will not be available, and must be restored before unacceptable impact occurs to the operations. • **Establishing Recovery Point Objective (RPO)** in this step, the RPO is identified to indicate the maximum targeted period in which data might be lost from an IT service due to a major incident. Assets that have a higher criticality score will obviously have smaller RTOs and RPOs and will need to be recovered as quickly as possible.

Content Template	
Section Number	2.3.2
Section Title	Disaster Recovery Plan
Introduction	
Content	Disaster recovery plan is the preparation for recovery from a disaster whether natural or from human being. A disaster occurs when the organization is unable to control the impact of an incident or the damage from the incident is very sever. Disasters are usually classified into natural disasters such as flood or fire, and human made disasters such as cyber attacks. The role of the disaster recovery plan is to define the way the organization can reestablish its operation at the same location of the organization. The main steps to establish a disaster recovery plan are: 1. Develop a disaster recovery planning policy statement. The policy presents an overview of the organization philosophy regarding the operations of disaster recovery. 2. Review BIA to identify the critical IT systems and components. 3. Identify the measures to be taken in order to reduce the effects of the system disruption. 4. Develop a strategy to ensure a quick recovery from a disruption. 5. Develop a disaster recovery plan document that contains a procedure to restore from a disaster. 6. Plan testing to identify gaps in the plan. 7. Updating the plan regularly. A number of operations are available to help an organization in protecting its information and recovering from a disaster, such as data backup into off site server regularly. Therefore, data can be restored.

Content Template	
Section Number	2.3.3
Section Title	Business Continuity Plan
Introduction	
Content	Business continuity plan is to ensure the continuation of the functionality of an organization after a disaster occurred. The business continuity (BC) plan reestablishes critical business functions at an alternate site. It is managed by the CEO of the company, unlike the disaster recovery (DR) plan which is managed by an IT team and its main goal is to reestablish the technical infrastructure and business operations at the primary site. The main steps of BC process is similar to that of RD process, which starts by defining a policy statement. Then reviewing the BIA report, and identifying the preventive control. After that, developing a relocation strategies and continuity plan. Finally, testing and upgrading the plan regularly.

Content Template	
Section Number	1.4
Section Title	Incident Response
Introduction	This section introduces how an organization should handle incidents. First, it presents the components of the incident response plan, and then it describes the procedure to be followed in case of an incident.
Content	Information security management includes the deployment of proper security controls to reduce the risk of successful attacks. However, despite all these measures, security incidents do occur. Incidents are unacceptable actions occur when an attack (natural or human being) affect the information resources and causing damage. Examples of such incidents may include denial of service attacks, unauthorized access to data, massive malware infection, etc. Therefore, a plan to handle incidents need to be prepared in advance for an efficient and effective recovery from occurred incidents. Incident response is a set of procedures that commence as soon as an incident is detected. Most organizations establish an incident response team responsible of dealing with any security incident. The team consists of members from different departments of the organization such as information security specialist, human recourse, legal, etc. Incident handling begins with planning and developing procedures to be followed when an incident occurs. The items of an incident response plan are given in Section 2.4.1. Incident handling includes other activities which are presented in Section 2.4.2.

Content Template	
Section Number	1.4.1
Section Title	Planning and preparation
Introduction	// same as above
Content	Each organization should define an incident response plan to cope with incidents. The objectives of the plan are: • Ensure that the required resources are available to deal with the incidents. • Ensure that all responsible roles have clear understanding of the tasks they should perform during an incident by following predefined procedures. • Ensure that the response is systematic and efficient to achieve prompt recovery of the compromised system. • Minimize the possible impact of the incident. • Prevent further attacks and damages. Incident response planning should contain the following items: • ***Overview***: Should present an overview of the plan and its objectives. • ***Scope***: It defines all the systems included in the plan, which the incident response team is responsible for. • ***Roles and Responsibilities***: The plan defines the roles and responsibilities of all those involved in the incident response. For example, the plan may define the role incident response coordinator who is responsible for reporting an incident status during and after the investigation. • ***Identification of incidents***: This item contains the events that have the potential to compromise the confidentiality, integrity, and the availability of information. Such events may include the unauthorized access to users account, the infections of machines with viruses, and denial of service attack, etc.

	• ***Incident reporting:*** This item contains the procedure for reporting an incident, if discovered by an employee in the organization. • ***Incident response:*** This item contains the procedure to be followed once an incident is discovered to mitigate the potential for additional damage. Usually the response is based on the classification of the incident as critical, major, or minor. • ***Incident close-up***: This item contains the type of documentation required to report. The document usually contains a complete report that describes the incident, the cause of the incident , its impact on the organization, and the action taken. Also, the document contains a remedy plan for the incident to ensure it would not be repeated. • ***Incident Response Plan Testing:*** This item includes a testing method for the plan to ensure that all processes and procedures defined in the plan are adequate.

Content Template	
Section Number	1.4.2
Section Title	Methodology
Introduction	// same as above
Content	The management of an incident is a complex task that consists of several steps. In this section, 7 steps are described to handle an incident: 1. **Pre-incident analysis:** In this step, the team analyzes the possible incidents and prepares the organization before an incident occurs. 2. **Detection of an incident:** Detection of an incident is one of the most important aspects of incident response. This is because if an organization cannot detect a response effectively, then it cannot succeed in responding to the incident. A response maybe identified by an end user, an administrator, an intruder detection system, and other means. 3. **Initial response:** Once an incident is detected. The team should, as an initial response, perform an investigation and recording the basic details surrounding the incident. In this phase, the team determines the type of the incident and its impact. 4. **Develop a response strategy:** Based on the collected facts, the team formulates a response strategy for this incident and gets the management approval. Strategies vary based on the circumstances of the incident and its impact. 5. **Investigate the incident:** After getting the approval, the team conducts a thorough analysis of the incident by collecting data. Then, the team reviews the data to get answers to questions such as what happened, who did it, and how it can be prevented in the future. 6. **Reporting:** After the investigation is finished, the team should report the incident to the upper management. 7. **Resolution:** When the incident is closed, follow up actions should be taken to evaluate the incident and to strengthen security protection to prevent recurrence of the incidents in the future.

Activity Template

Number	1.1
Title	Security Risk Management
Type	
Aim	ILOs: 3 The activity aims to investigate the possible threats in an organization and investigate the controls than be used to eliminate them.
Description	Section 2.2: Security Risk Management Identify the security risks in a university, then analyze them and suggest solutions to treat these risks.
Timeline	Time: 1-3 hours of reading.
Assessment	Each student is required to submit a no longer than a one page report about the identified assets and threats. Also, the report should contain calculation of the risks level and the suggest controls

Activity Template

Number	1.2
Title	Incident Response
Type	
Aim	ILOs: 6 The activity aims to expose the students to different plans and enables them to analyze them.
Description	Section 2.4: Incident Response Many organizations have their incident response plan available online. Compare between any three of them.
Timeline	Time: 1-3 hours.
Assessment	Each student should submit one page containing the comparison of the three plans and including the advantage and disadvantage of each plan.

Think Template (MCQs)

Number	2.1
Title	Contingency planning
Type	Choose correct answer
Question	What are the three continuity strategy plans?
Answers	a) Incident response plans (IRP), Disaster recovery plans (DRP), and business continuity plans (BCP). b) Incident detection plans, incident reaction plans, incident containment strategies plans. c) Incident detection plans, incident reaction plans, incident Recovery plans. d) Incident plans, incident recovery plans, incident response plans. **Answer: A**

Think Template (MCQs)

Number	2.2
Title	Incident Response
Type	Choose correct answer
Question	When do we classify an attack as an incident?
Answers	a. The attacks are directed against information assets b. The attacks have a realistic chance of success c. The attacks could threaten confidentiality, integrity, or availability of information resources d. All of the above.

Answer: D

Think Template (MCQs)

Number 2.3

Title Security governance, planning and policies

Type Fill in the blank

Question ______________________ is a discretionary set of directions designed to achieve objectives of an established security policy.

Answers a) guideline
b) standard
c) procedure
d) best practice

Answer:
a

Think Template (MCQs)

Number 2.4

Title Security Risk Management

Type Choose correct answer

Question How should the level of risk for an organization be determined?

Answers A) Combining consequence and likelihood of events
B) Combining importance and acceptance of events
C) Combining acceptable and tolerable events
D) Combining profitability and analysis of events
Answer: A

Think Template (MCQs)

Number 2.5

Title Business Impact Analysis

Type Choose correct answer

Question What is one of the purposes of the Business Impact Analysis (BIA)?

Answers A) to determine the business continuity strategy
B) to determine minimal acceptable outage
C) to identify risks
Answer: A

Think Template (MCQs)

Number	2.6
Title	Incident Response
Type	Choose correct answer
Question	Business impact analysis gives an idea about the timing of the recovery and the timing of the backup. How is the timing of the backup determined?
Answers	A) Via Maximum Acceptable Outage (MAO) B) Via Recovery Time Objective (RTO) C) Via Recovery Point Objective (RPO) D) Via Single Point Of Failure (SPOF) **Answer:** **C**

Think Template (MCQs)

Number 2.7

Title Risk Identification

Type Match Pairs

Question Match between terms and their definitions

Terms:
a) Attacks
b) Vulnerabilities
c) Threats

Definitions:
i) A weakness which can be exploited by an attacker
ii) A potential for violation of security
iii) An action that compromises the security on information owned by an organization

Answers **Answer:**
a, iii
b, i
c, ii

Extra Template

Number	2.1
Title	**Management of Information Security**
Topic	• 2.1 • 2.2 • 2.3
Type	Michael E. Whitman , Herbert J. Mattord , Management of Information Security, 6th Edition, Cengage Learning, 2018

Extra Template

Number	2.2
Title	**Information Security Governance: A Practical Development and Implementation Approach**
Topic	• 2.1
Type	Krag Brotby, Information Security Governance: A Practical Development and Implementation Approach, Wiley, April 2009

Extra Template

Number	2.3
Title	Governance of information security
Topic	2.1
Type	ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security URL: https://www.iso.org/standard/43754.html

Extra Template

Number	2.4
Title	**Information Security Risk Analysis**
Topic	2.2
Type	Thomas R. Peltier, Information Security Risk Analysis, 3rd Edition, Auerbach Publications, March 2010

Extra Template

Number	2.5
Title	Information security risk management
Topic	2.4
Type	ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management URL: https://www.iso.org/standard/75281.html

Extra Template

Number	1.6
Title	**Incident Response & Computer Forensics**
Topic	2.4
Type	Luttgens**,** J., Pepe, M**.**, Mandia, K. (2014), **Incident Response & Computer Forensics**, 3rd edition, McGraw

3. Handling and investigating security incidents from a business perspective

Scope Template

Number 3

Title Handling and investigating security incidents from a business perspective.

Introduction This chapter explores the concept of digital forensics from a business and a managerial perspective. It will also discuss the security related issues to any organization from a business process angle. International standards are core issues to be discussed as students should be aware of them when setting any frameworks or principles in the future. The chapter will wrap up with ethical issues related to digital forensics in business organizations.

Outcomes Demonstrate a solid understanding of the various security and ethical issues related to incident handling in business organizations.
ILO1: Understanding the major concepts related to incident response
ILO2: Understanding the details of incident handling, and how it can be applied

Topics **1.1 Introduction to Events and Incidents**
1.2 The Need for Incident Response
1.3Incident handling
Preparation
1.3.1 Preparing to Handle Incidents
1.3.2 Preventing Incidents
Detection and Analysis
1.3.3 Incident Categories
1.3.4 Signs of an Incidents
1.3.5 Sources of Precursors and Indicators
1.3.6 Incident Analysis
1.3.7 Incident Documentation
1.3.8 Incident Prioritization
1.3.9 Incident Notification
Containment, Eradicating, and Recovery
1.3.10 Choosing a Containment Strategy
1.3.11 Evidence Gathering and Handling
1.3.12 Identifying the Attacking Hosts
1.3.13 Eradication and Recovery
Post-Incident Activity
1.3.14 Lessons Learned
1.3.15 Using Collected Incident Data
1.3.16 Evidence Retention
1.4Incident Handling Checklist
1.5 Recommendations

Study Guide

Task	**Time**
Preparation (Introduction and On-line Planning):	2 hr
Textbook Content:	6 hr
Thinking (online discussion review questions)	1 hour
Tutorial Work on incident handling	3 hr
Related Course Work	1 hour
Total	**11 hours**

• Required study time: **4 one-hour lectures, and 1 three-hour tutorial lecture** on incident handling **(1.3).**

• Required external resources including links and books:
• NIST Computer Security Incident Handling Guide

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- Guide to Integrating Forensic Techniques into Incident Response
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

- Additional References:

Beebe, N.L. and J.G. Clark, 2005. A hierarchical, objectives-based framework for the digital investigations process. Digital Invest., 2: 147-167.

CSI, 2011. 15th annual computer crime and security survey. Computer Security Institute.

May, C., 2002. Computer forensic: The morse or clouseau approach. Comput. Fraud Security, 2002: 14-17.

McDowell, B., 2012. Tech companies collaborate to fight phishing. http://www.itp.net/popup/print/587806.

Morris, R., 2003. Uncovering a user's hidden tracks. Comput. Fraud Security, 2003: 11-13.

Norton Cybercrime, 2011. The shocking scale of cybercrime: Report. http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/.

Savona, E.U., 2012. Organized crime enablers, Global council on organized crime. World Economic Forum, July 2012. http://reports.weforum.org/organized-crime-enablers-2012/#chapter-enablers-of-cybercrime.

Stahl, B., Elizondo, D., Carroll-Mayer, M., Zheng, Y. and Wakunuma, K., 2010, July. Ethical and legal issues of the use of computational intelligence techniques in computer security and computer forensics. In *Neural Networks (IJCNN), The 2010 International Joint Conference on* (pp. 1-8). IEEE.

Teelink, S. and R. Erbacher, 2006. Improving the computer forensic analysis process through visualization. Communi. ACM., 49: 71-75.

Wang, Y., J. Cannady and J. Rosenbulth, 2005. Foundations of computer forensics: A technology for the fight against computer crime. Comput. Law Security Report, 21: 119-127.

IRIS (http://www.irisinvestigations.com/wordpress/digital-evidence-standards-and-best-practices/)

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, US Department of Justice, Report, 2004

Scientific Working Group on Digital Evidence (https://www.swgde.org/documents)

Content Template

Section Number 1.1

Section Title **Introduction to Events and Incidents**

Introduction This section will introduce computer security incident in relation to the responses to the events and procedures related to digital forensics. The section will give a brief understanding of the main concepts that will be discussed throughout the chapter by introducing some definitions, authority, scope, audience and the structure of the chapter.

Upon completion of this section the student will be able to:

- Have clear understanding of the concept of incident handling.
- Define the main audience that need to address to an incident with dealing with a digital forensic evidence.

Content Studying incident responses is crucial for digital forensics s that incident can promptly be reported and perceived. The importance of detecting incidence in digital forensics contributes to preserving the evidence by minimizing any losses or demolition in it. However, not all evidences and incidents are dealt with in the same means, there is a particularity for each incident. The NICT guideline provides a concrete outline for procedures on how to handle such incidents. This will be discussed in details later in this chapter.

Incident handling goes through three main processes; these processes start from data collection to data analysis to data reporting. Then the process moves towards the stakeholdersor the audience including the internal or external groups that will be discussed in details later on.

The report that answers to any incident should include a number of actions as follows:

1. An incident response policy and plan.
2. The procedures for handling and reporting incidents.
3. The guidelines for communications between the outside audiences involved in the incidents.
4. Deciding on the team structure and the staffing model.
5. Teams come together to respond to the incident – internal and external groups.
6. Choosing the appropriate service, the incident response team should provide.
7. Giving the response team the needed training and provide the needed staff as appropriate.

This action plan seeks to help organizations in alleviating the risks coming from computer security incidents by providing these procedures that can help them in acting promptly and in an effective and efficient way.

These guidelines can be tailored according to the organization special nature and its mission requirements.

The audience of these guidelines includes anyone who will be dealing with digital forensics incident handling. This includes networks administrators, security staff, technical support staff, CIOs, computer security program managers and any other personal involved.

The structure of the chapter will be as follows; the following the section will be the need for incident response, followed by incident handling and all the related details, followed by recommendations and finally the check list for the audience.

Content Template

Section Number 1.2

Section Title **The Need for Incident Response**

Introduction To effectively design a computer security incident response, several major decisions and actions should be considered. At first, an organization-specific definition of the term "incident" should be clarified. In addition, the services and teams' structures and models should be identified including a plan, policy, and procedure to maintain an effective, efficient, and consistent services. The plan, policies, and procedures should also reflect the interactions with other possible incident involved teams i.e. law enforcement, media, and other incident response organizations.

Content Events and Incidents

A computer security incident can be identified as a violation of computer security/use policies. Examples of incidents are:

- A DDOS on a web server, causing it to crash.
- Email including a malware; infecting their computers and establishing several connections to an external host.
- Data theft for ransom (ransomwares).
- Peer-to-peer file sharing.

Need for Incident Response

Attacks generally aim at compromising useful data, and when security breaches occur it is critical to respond quickly and effectively. The concept of computer security incident response supports responding to incidents systematically, taking appropriate actions to minimize loss or theft of information and disruption of services caused by incidents. In addition, facilitates the reusability information gained during incident handling for better preparing for future incidents. Further, Incident response helps with dealing properly with legal issues that may arise during/after incidents.

Incident Response Policy, Plan, and Procedure Creation

Policy Elements

Taking into considerations that different organizations have various incident response requirements and policies, some key commonalities (Whitman, 2017) can be found as follows: 1) management commitment, 2) Purpose, objectives, and scope of the policy, 3) Organizational structure and definition of roles, responsibilities, and levels of authority, 4) Prioritization or severity ratings of incidents, 5) Performance measures, and 6) Reporting and contact forms.

Plan Elements

The incident response plan should include the following elements: 1) Mission, 2) Strategies and goals, 3) Senior management approval, 4) Organizational approach to incident response, 5) Internal and External communications, 6) Metrics for measuring the incident response capability and its effectiveness, 7) Roadmap for maturing the incident response capability, and 8) How the program fits into the overall organization. (NIST Computer Security Incident Handling Guide, Revision 2, 2012)

Once an organization develops an approved plan, the plan should be implemented and reviewed annually to ensure the fulfilling & capability of incident response goals.

Procedure Elements

Procedures should comply with the incident response policy and plan. Priorities of the organization in response operations are described in Standard Operating Procedures (SOPs)covering technical processes, techniques, checklists, and forms used by the incident response team.

Sharing Information with Outside Parties

Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever needed. An example is discussing incidents with Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams. All contacts and communications with outside parties must be documented for liability and evidentiary purposes.

Incident Response Team Structure

An incident response team should be available all the time. The number of team members handling an incident will vary depending on the incident severity and availability of personnel. The incident handlers analyze the incident data, and act appropriately to limit the damage and restore services. The incident response team's success depends on the participation and cooperation of individuals throughout the organization, and dependencies outside the organization (if any).

Team Models

Possible structures for an incident response team include the following:

Central Incident Response Team that handles incidents throughout the organization. This model is effective for small organizations.

Distributed Incident Response Teams each of which responsible for a particular logical or physical segment of the organization. This model is effective for large organizations.

Coordinating Team advising to other teams without having authority over those teams.

Incident response teams can use the following staffing models: 1) employees, 2) partially outsourced, or 3) fully outsourced.

Employees. incident response work is handled by the employees with limited support from contractors.

Partially Outsourced. incident response work is partially outsourced, especially the tasks that employees can not handle.

Fully Outsourced. incident response work is completely outsourced due to the lack of qualified employees.

Team Model Selection

Few factors that need to be considered when structuring and staffing an incident response team:

• The Need for 24/7 Availability. This is basically required to minimize the time and damage in case an incident happened.

• Full-Time Versus Part-Time Team Members. the trade-off between part-timers and full timers should be consideredbased on funding, staffing, or needs.

• Employee Morale Boosting. Morals can be boosted significantly through segregating roles, and minimizing administrative work responsiblitis.

• Cost. Staff costs, funding for training and maintaining skills need to be considered especially with the rapid changes in everyday technologies.

• Staff Expertise. Outsourcers may possess deeper knowledge of security aspects (e.g. intrusion detection, forensics, vulnerabilities, exploits, among others) than employees of the organization. On the other hand, technical staff members within the organization usually have much better knowledge of the organization's environment than an outsourcer would, which can be beneficial in identifying false positives associated with organization-specific behavior and the criticality of targets.

When considering outsourcing, organizations should keep these issues in mind:

Maintaining and continuously assissing the outsourcer's Quality of Work.

Division of Responsibilities. Basically, define who can make a decision on what and in which situation?

How Sensitive the Information Revealed to the Contractor can be? and when to interfere? Employees can take over an investigation as soon as a certain level of information is revealed. Non-disclosure agreements (NDAs) are one possible option for protecting the disclosure of sensitive information in case revealed.

Lack of Organization-Specific Knowledge will make it hard to prioritize incidents in case happened simultaneously.

Lack of Correlation. There is a tradeoff between granting remote administrative privileges on critical systems and security device logs to an outsourcer, compared to the administration costs and the risk of unauthorized disclosure of sensitive information.

Proximity of Handling Incidents on site, off-site, and permissions to unauthorized areas should/shouldn't be granted.

Maintaining Basic Incident Response Skills In-House.

Incident Response Personnel

Team Managers:

Team managers act as a liaison between upper management and other teams and organizations, handling crisis situations, and assure that teams have necessary personnel, resources, and skills.

Managers should possess excellent communication/technical skills. They are, also, responsible for ensuring appropriateness of incident response activities.

Technical Leads:

strong technical skills and incident response experience is a must for technical leads. They generally assume oversight and responsibility of the team's technical work quality.

Employees:

A single employee (who must have backups) should be in charge of incident response. In a fully outsourced model, this employee monitors and evaluates the outsourcers' work quality and process.

Excellent technical skills, problem solving skills, and critical thinking abilities are mandatory pillars for the incident response team members. Moreover, it is important to provideopportunities for learning and growth. Examples to do so can be by securing sufficient training fund, organizing mentoring between seniors and juniors, rotating tasks between team members for an opportunity of gaining different experiences, and holding continuous team training sessions. A major characteristic is that employees should be team players, with leading skills (for some of them).

Team members may provide additional services, such as:

Intrusion Detection. Detecting illegal penetration efforts and threats.

Advisory Distribution. Issue advisories and disseminate information on new vulnerabilities and threats within the organization.

Education and Awareness. Through workshops, websites, newsletters, posters, among others.

Information Sharing. information sharing groups are considered effective collaboration method for aggregatinginformation related to incidents.

Dependencies within Organizations

Management. Management establishes incident response policy, budget, and staffing while held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting.

Information Assurance. Information security staff members may be needed during certain stages of incident handling to, for example, alter network security controls.

IT Support. Because of the expertise they possess, and the understanding of the technology they manage, and to ensure that the appropriate actions are taken for the affected system.

Legal Department. Legal experts should review incident response plans, policies, procedures, and various types of agreements (NDA, MOU, etc) to ensure their compliance with law.

Public Affairs and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media.

Human Resources. handling suspect employees, and take drastic disciplinary actions.

Business Continuity Planning Experts. Because they should be aware of incidents and their impacts, and due to their extensive expertise in minimizing operational disruption during severe circumstances, business continuity planners are valuable in planning responses to certain situations, fine-tune business impact assessments, risk assessments, and continuity of operations plans.

Conclusions

Organizations should be prepared to respond quickly and effectively when computer security defenses are breached. Therefore, a formal incident response capability should be established. It is apparent that the incident response policy defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting

incidents, among other items. Based on the incident response policy an incident response plan should be developed providing a roadmap for implementing an incident response in harmony with the organization’s policy. Following, incident response procedures should be developed to provide detailed steps for responding to an incident.
Furthermore, policies and procedures for communicating media and law agencies regarding incident-related information sharing should be established.
Additionally, incident response team members should possess adequate skills taking into account their credibility and proficiency.

References

Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 6th Edition, Cengage Learning, 2017
NIST (800-61) Computer Security Incident Handling Guide: https://clearwatercompliance.com/wp-content/uploads/NIST-SP-800-61-Revision-2-Computer-Security-Incident-Handling-Guide.pdf

Content Template

Section Number 1.3

Section Title **Handling an Incident**

Introduction In this section and the following sections students are expected to
1. develop a clear understanding of the different processes of incident handling.
2. Understand how each process of incident handling works individually.

Content This section will introduce how to deal with incident when they occur. The section will be then followed by sub-sections explaining in details each process. The main processes are preparation, detection and analysis, containment, eradication and recovery and post incident activity.

• The life cycle of the incident response is illustrated in the figure below.

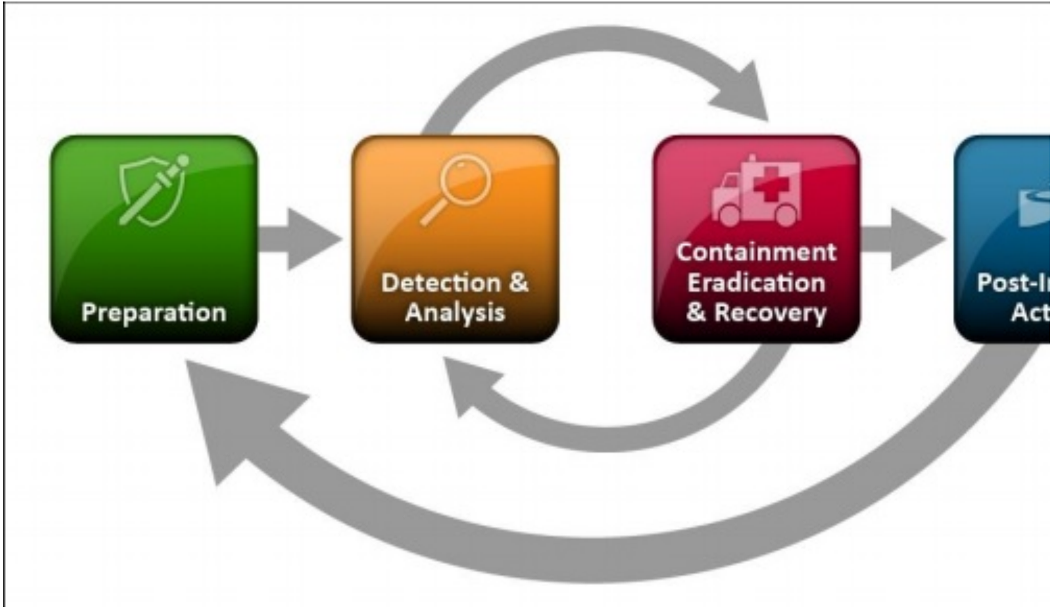


Figure 1: Incident Response Life Cycle*
Courtesy of: NIST (800-61) Computer Security Incident Handling Guide

Content Template

Section Number 1.3.1

Section Title Preparation –Preparing to handle incidents

Introduction The concept of preparation here covers two aspects; the first one is pre- incident occurring as teams should be ready for any external attacks by prevention. Adding to that the steps that happen when the incidents happen and how to deal with it when happening.

Content Incident handing is not an easy procedure, it requires a number of tools and resources summarized as follows;

Communication and Facilities tools

- Contact information: these contacts include members from inside and outside the organization; including law enforcement. The information includes phone numbers, emails and encryption keys.
- On-call information: this information is dedicated for internal dedicated teams such as the escalation information.
- Incident reporting mechanisms: people should be able to report incident anonymously so organizations should provide contacts so people can do that conveniently.
- Issue tracking systems.
- Smartphones to keep on contact with team members.
- Encryption software for communications between internal and external groups using FIPS- validated algorithm.
- War room is created when need for communication and coordination purposes.
- Secure storage facility for keeping evidences and sensitive material safe.

Incident analysis hardware and software

- Specialized digital forensic workstation with associated backup devices for the purposes of taking images, keeping log files and keeping other relevant data.
- Laptops for data analysis and writing reports.
- Networking equipment, servers' other workstations for extended work.
- Blank removable media.
- Portable printers.
- Digital forensics software
- Packet sniffers and protocol analyzers to analyze network traffic.
- Portable media.
- Evidence gathering accessories such as cameras, audio recorders.

Incident Analysis Resources

- Ports lists
- Documentation
- Network diagrams and list of databases servers and other critical assets.
- The worked on baseline for the network, system and the applications.
- Cryptographic hashes of critical files.

Incident Mitigation software

- Access to images for recovery purposes.

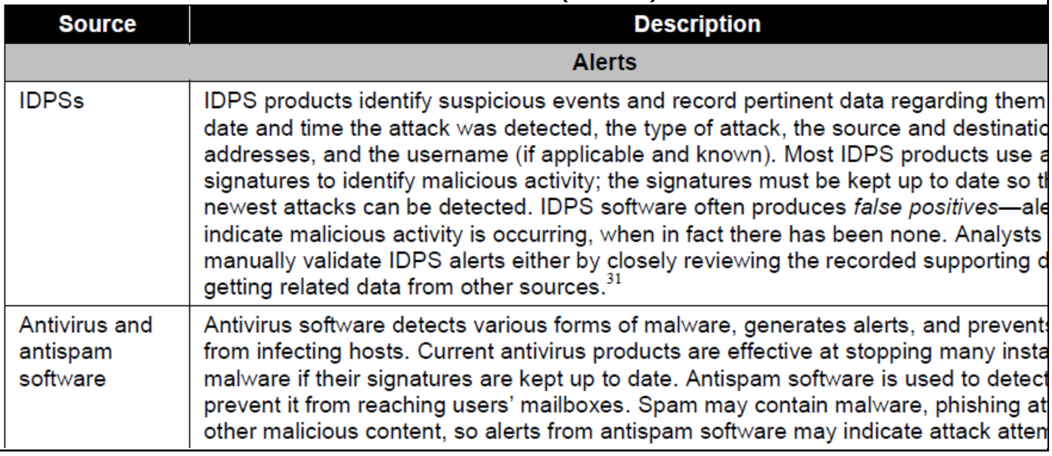
Many teams create what they call the *jump kit*. This is a very accessible kit that has the needed tools to be used throughout investigation. The tool tends to be easy to use and portable. It usually includes a laptop and software – digital forensic software with other important material such as backup devices, blank media and networking equipment.

One computer is not enough at each incident handling. Each incident handler needs two computers, one laptop and another one to deal with network issues such as packet sniffers or malware analysis.

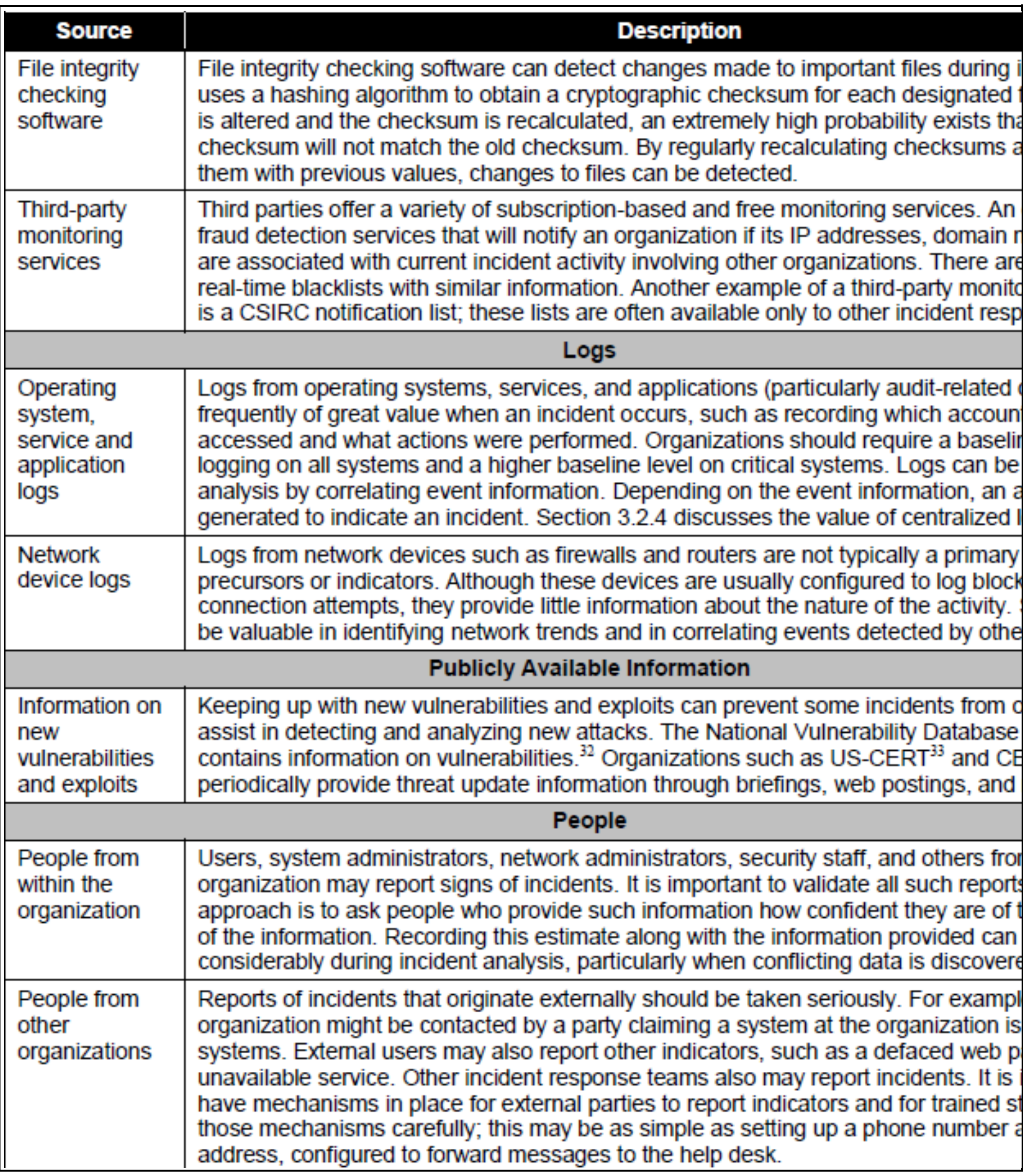
Content Template	
Section Number	1.3.2
Section Title	Preparation – Preventing Incidents
Introduction	// Same as above
Content	One of the main processes of incident handing is actually preventing it before happening. This is due to the fact that low incidents rate can safeguard business practices of the organizations. For the purpose of prevention here are a list of recommended practices for securing networks, systems and applications: • Risk assessment: conducting intervallic risk assessment can help organizations assess the threats and vulnerabilities that are posed on them. These risks, threats and vulnerabilities are then prioritized, mitigated, transferred, or accepted until the level of risk assessment is achieved and reached. Staff can also control mentoring activities on resources by having regular risk assessment. • Host security: all software, hardware. Operating systems and related applications should be well kept in terms of security. This is also should be supported by continuous security reports and security check lists. • Network security: network security is one of the crucial components over the information systems to be protected. All activities should be monitored and a network perimeter should be established to deny any service outside it. All connection points should be secured internally and externally. • Malware prevention: this should be established in both the hosting level and the application level to ensure maximum protection over the information systems. • User awareness and training: policies and procedures regarding network, applications, software, hardware and processes on the information system should be made clear for the users. Their actions and reactions on the system affect the whole organization and ensuring their awareness about different incidents and how to deal with them is crucial and reduce the frequency of any incident occurrence.

Content Template	
Section Number	1.3.3
Section Title	*Detection and Analysis* - Incident Categories
Introduction	// same as above
Content	It is quite hard to categorize incidents or put them into specific forms or types. This is due to the fact that they can occur in many different ways and there is no step-by step way to be described as pathway to handle every incident that occurs. However, there are a set of common attacks that can happen as fellow: • External/ removable media: these are one of the common attacks that can occur from removable media that can attack a whole system or network. • Attrition: • Web: an attack from a website or a web based application or malwares. • Email: attacks from emails via infected messages with attachments, links connected with infected links. • Improper usage: this occurs as a result of authorized users' improper usage of the system by mistake. • Loss or theft of equipment: equipment, devices, media can be stolen or lost. • Other: any other attacks can occur in the organizations that do not fit the above categories.

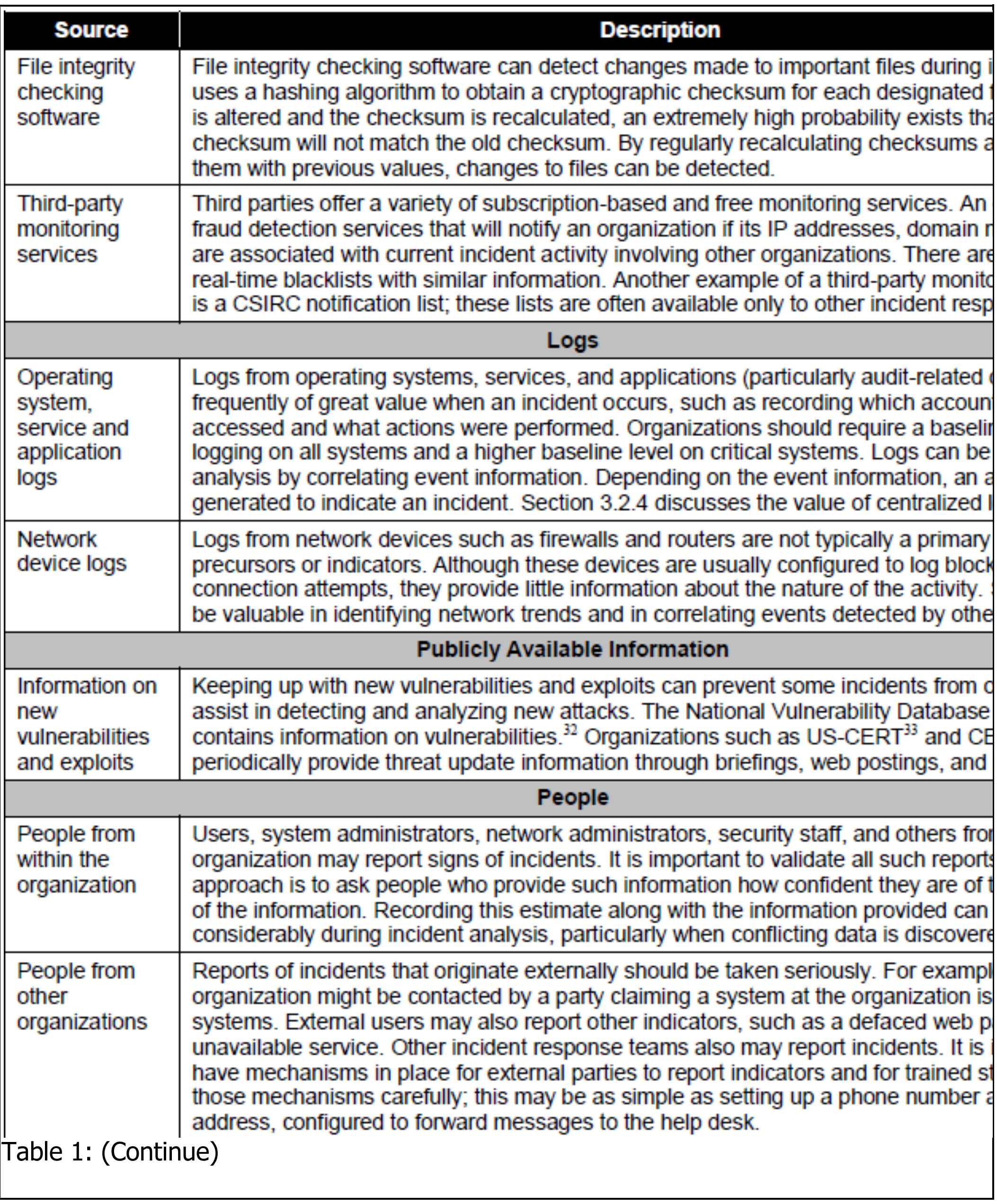
Content Template	
Section Number	1.3.4
Section Title	*Detection and Analysis* – Sign of an Incident
Introduction	// same as above
Content	Accurately detecting an incident is one of the challenging parts of incidents process response. This is due the fact, that the incident needs to be first allocated and determined if it actually has occurred, then the type of it, the size of the incident. There are some factors that affect the incident indications as follow: • The different means of incident detections. Some means may be electronic and other may be manual and some maybe impossible to detect. • The volume of alerts and signs of incidents per day is high and can get up to thousands or millions. • Technical and extensive knowledge is needed for efficient analysis for data and issues related to the incidents. The two categorizes of incidents are: • Precursors: these are signs that incidents may occur on the future. • Indicator: these are signs that incidents are occurring now or have occurred already. Here are some examples of precursors in an organization; threats of external groups on the organization, attacks on the vulnerability of the mail server and the vulnerability of the scanning the attacks as shown from the web log. Precursors' examples include; sensor alert of a network when buffer overflow occurs, anti-virus alerts of malwares and worms, the appearance of unusual characters in file namesand un unusual traffic in the network to mention some.

Content Template	
Section Number	1.3.5
Section Title	*Detection and Analysis* – sources of Precursors and Indictors
Introduction	// same as above
Content	As there are many sources for precursors and indicators, the common sources can bethe alerts coming from computer security software, log files, publically available information, and the people. Each category can be summarized as follow: Table 1: Sources of Precourses and Indicators (Source) 

Source	Description
	Alerts
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them date and time the attack was detected, the type of attack, the source and destinatio addresses, and the username (if applicable and known). Most IDPS products use a signatures to identify malicious activity; the signatures must be kept up to date so th newest attacks can be detected. IDPS software often produces *false positives*—ale indicate malicious activity is occurring, when in fact there has been none. Analysts manually validate IDPS alerts either by closely reviewing the recorded supporting d getting related data from other sources.[31]
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents from infecting hosts. Current antivirus products are effective at stopping many insta malware if their signatures are kept up to date. Antispam software is used to detect prevent it from reaching users' mailboxes. Spam may contain malware, phishing at other malicious content, so alerts from antispam software may indicate attack attem



Source	Description
File integrity checking software	File integrity checking software can detect changes made to important files during i uses a hashing algorithm to obtain a cryptographic checksum for each designated f is altered and the checksum is recalculated, an extremely high probability exists tha checksum will not match the old checksum. By regularly recalculating checksums a them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An fraud detection services that will notify an organization if its IP addresses, domain n are associated with current incident activity involving other organizations. There are real-time blacklists with similar information. Another example of a third-party monito is a CSIRC notification list; these lists are often available only to other incident resp
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related d frequently of great value when an incident occurs, such as recording which accoun accessed and what actions were performed. Organizations should require a baselin logging on all systems and a higher baseline level on critical systems. Logs can be analysis by correlating event information. Depending on the event information, an a generated to indicate an incident. Section 3.2.4 discusses the value of centralized l
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary precursors or indicators. Although these devices are usually configured to log block connection attempts, they provide little information about the nature of the activity. S be valuable in identifying network trends and in correlating events detected by othe
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from o assist in detecting and analyzing new attacks. The National Vulnerability Database contains information on vulnerabilities.[32] Organizations such as US-CERT[33] and CE periodically provide threat update information through briefings, web postings, and
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others fro organization may report signs of incidents. It is important to validate all such reports approach is to ask people who provide such information how confident they are of t of the information. Recording this estimate along with the information provided can considerably during incident analysis, particularly when conflicting data is discovere
People from other organizations	Reports of incidents that originate externally should be taken seriously. For exampl organization might be contacted by a party claiming a system at the organization is systems. External users may also report other indicators, such as a defaced web p unavailable service. Other incident response teams also may report incidents. It is have mechanisms in place for external parties to report indicators and for trained st those mechanisms carefully; this may be as simple as setting up a phone number a address, configured to forward messages to the help desk.



Source	Description
File integrity checking software	File integrity checking software can detect changes made to important files during i uses a hashing algorithm to obtain a cryptographic checksum for each designated f is altered and the checksum is recalculated, an extremely high probability exists tha checksum will not match the old checksum. By regularly recalculating checksums a them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An fraud detection services that will notify an organization if its IP addresses, domain n are associated with current incident activity involving other organizations. There are real-time blacklists with similar information. Another example of a third-party monito is a CSIRC notification list; these lists are often available only to other incident resp
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related d frequently of great value when an incident occurs, such as recording which accoun accessed and what actions were performed. Organizations should require a baselin logging on all systems and a higher baseline level on critical systems. Logs can be analysis by correlating event information. Depending on the event information, an a generated to indicate an incident. Section 3.2.4 discusses the value of centralized l
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary precursors or indicators. Although these devices are usually configured to log block connection attempts, they provide little information about the nature of the activity. S be valuable in identifying network trends and in correlating events detected by othe
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from o assist in detecting and analyzing new attacks. The National Vulnerability Database contains information on vulnerabilities.[32] Organizations such as US-CERT[33] and CE periodically provide threat update information through briefings, web postings, and
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others fro organization may report signs of incidents. It is important to validate all such reports approach is to ask people who provide such information how confident they are of t of the information. Recording this estimate along with the information provided can considerably during incident analysis, particularly when conflicting data is discovere
People from other organizations	Reports of incidents that originate externally should be taken seriously. For exampl organization might be contacted by a party claiming a system at the organization is systems. External users may also report other indicators, such as a defaced web p unavailable service. Other incident response teams also may report incidents. It is have mechanisms in place for external parties to report indicators and for trained st those mechanisms carefully; this may be as simple as setting up a phone number a address, configured to forward messages to the help desk.

Table 1: (Continue)

Content Template

Section Number 1.3.6

Section Title *Detection and Analysis-* Incident Analysis

Introduction // same as above

Content One of the main issues regarding incident analysis is the preprocessing of it. They relay a lot on the precursors and the indictors to be correct and accurate and this is not always the case. Also, the amount of indications that may occur makes it impossible sometimes to analyze all the indicators that occur. However, some indications may be correct and accurate but may not have occurred sometimes crashes over system have happened that appeared as an incident. Here are a list of recommendations of how to make incident analysis easier and effective:

- Profiling for the network and the systems, which means measuring the expected activities that may occur over the network and the systems and put a threshold that a system can go above or below.
- Understanding the normal behavior of the networks, systems, applications and related systems. Any abnormality of the behavior over any part of the information system should be located and handled.
- Have a strong log retention policy, all log files should be easily returned, studied and retrieved in case needed for any incident that may occur. The guideline *NIST SP 800-92 Guide to Computer Security Log Management*can be read for further knowledge.
- Correlation between different events that may have caused or will cause an incident should be studied through log files, IP addresses applications log with the user name.
- Keep all host clocks synchronized, this indicates that all the protocols synchronize clocks among hosts in the same time as the NTP. Any problems with the synchronization will make the correlation between the devices more complex and reporting process harder to follow.
- Maintain and uses a baseline of information, by this it is meant that the reference to information should be well known during incident analysis. Information can be available in known forms such as text documents, spreadsheets and simple databases to share information to explain the significance and validity of precursors and indicators as an example.
- Using the internet to search for unusual or uncommon activities that may not be easy to detect or know about.
- To collect additional information about the incident the handler runs a packet sniffer over the network to understand what is going over the network.
- Data filtering, is an important technique as mentioned earlier there are huge amount of indicators, not all of them can be analyzed. As a result, data filters are used to categorize them based on significance as one example.
- The last recommendation is to seek assistance when the team cannot determine the causes and the nature of the incident.

Content Template

Section Number	1.3.7
Section Title	*Detection and Analysis-* Incident Documentation
Introduction	// same as above
Content	The documentation process starts immediately within the incident. There are many tools to do the documentation starting from log books, to laptops, to audio records to digital cameras to mention some. All the documentation should be done and timestamped. The incident handler should make sure each document is dated and signed by the incident handler. This is due to the fact that these documents can be used later in court as evidences. Tracking systems can help a lot on the process of documentation. There main jobs are to keep records of the information gathered along with any related pertinent information. The tracking system should keep information about the documents collected. This information includes; the current status of the incident, a summery, any indicators related to it, actions taken by the incident handlers, the impact assessment, the contact information for all the people involved in the incident, a list of the evidence gathered, any further comments and what is the next steps to be considered. All this information should be well kept and safeguarded because they contain very sensitive information about the incident that occurred.

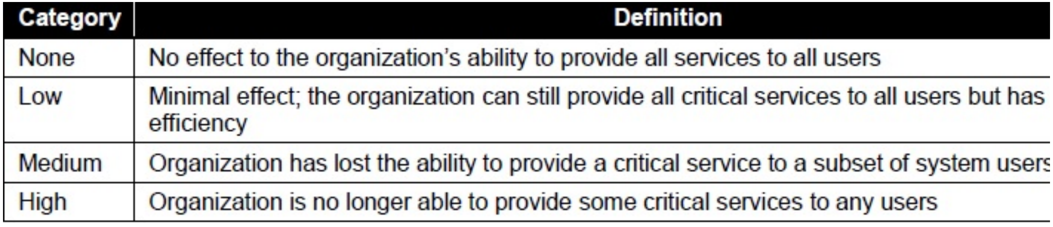
Content Template

Section Number	1.3.8
Section Title	*Detection and Analysis*- Incident Prioritization
Introduction	// same as above

Content Incident prioritization is the one of the most critical decision to be made in the whole incident handling process. It does not depend on first come first serve policy, it rather depends on n the severity of the incident and limitation of the resources. The factors that affect an incident is served as a priority are:

• **Functional impact of the incident**: the functional impact of an incident effects the business processes of an organization as a result of the IT system fault that occurred. The incident handler should consider how these incident will affect the organization as a whole not only the systems effected.

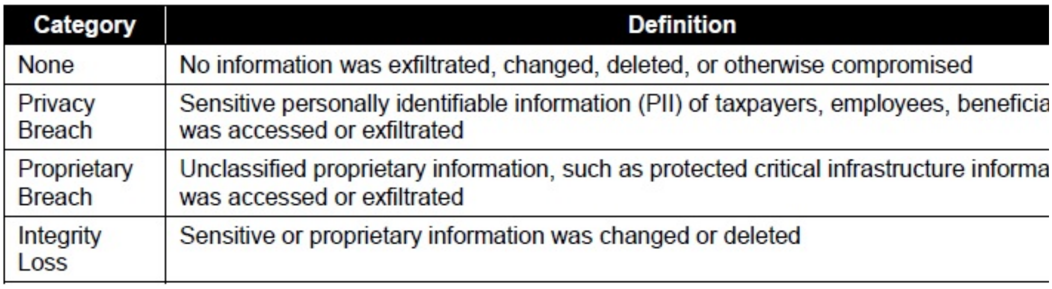
Table 2: Functional Impact Categorizes



Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

• **Information impact pf the incident**: this impact is quite a critical one. This is due to the fact that the attack on the organization may cause leak of sensitive information which can jeopardize the integrity, confidentiality and integrity of the organization.

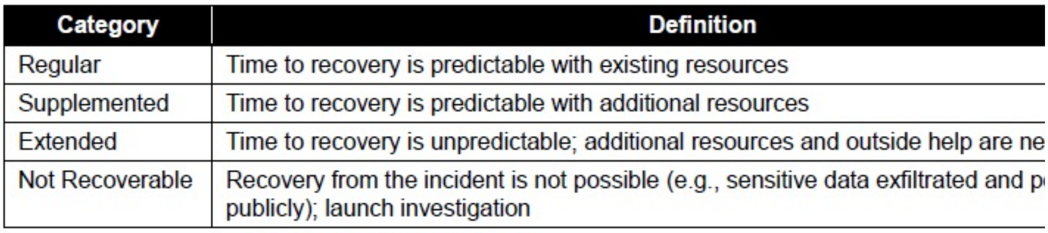
Table 3: Information Impact Categories



Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficia was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure informa was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

• **Recoverability from the incident:** the recovery of the incident depends on the size, the amount of recourses it consumed, the amount time it needed to be all over. Some incidents can never be recovered from and others and not even detected. It depends on the severity of the incident.

Table 4: Recoverability Effort categories



Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are ne
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and p publicly); launch investigation

Content Template

Section Number	1.3.9
Section Title	*Detection and Analysis*- Incident Notification
Introduction	// same as above
Content	After the incident have been analyzed and prioritized all the people involved in the incident should be notified in their roles. The reporting policies include everyone’s role, to whom they should report, the timing of the report, the content of the report. Typical people to report include; CIO, Head of information security, local information security officer, incident teams within the organization, external teams involved, system owners, HR, public affairs – if needed, legal department federal government for the US and related agencies in other countries. On the media level it should be communicated through emails, website, telephone calls, in person, paper and voice mail box of the incident.

Content Template	
Section Number	1.3.10
Section Title	*Containment, Eradicating, and Recovery -* Choosing a Containment Strategy
Introduction	// same as above
Content	Containment is the process of handling the incident before it increases or makes more damages. There are many strategies to deal with incidents such as disconnecting the machine from the network or shutting down the system. These strategies should be predefined as a part of containment process. The criteria for deciding the appropriate strategy depends on the following: • The potential damage of the resources. • Preservation of the evidence. • The availability of the service. • The implementation of the strategy needs in terms of time and resources. • The strategy effectiveness. • The solution duration. In some cases, the containment strategy is delayed so the pattern of the attacker can be studied and then can be handled and stopped.

Content Template	
Section Number	1.3.11
Section Title	*Containment, Eradicating, and Recovery –* Evidence gathering and handing
Introduction	// same as above
Content	In the process of incident handling these documents as mentioned previously may be used as evidences in legal curt. As a result, all the evidence gathering should be clearly documented how it was gathered, compromised and persevered. The way evidence was collected should meet the applicable laws and regulations from the law enforcement agencies. The detailed log should have included the following: • All the identifying information that should be labeled on the evidence such as – the location collected, the serial number, the model number, host name, media access, MAC address, IP address. • The individual full information whole collected or handled the evidence. • The evidence handling occurrence time and date. • The exact place where the evidence is stored. This is one of the challenging steps, as it is desired to collect the evidence as soon as the evidence is collected.

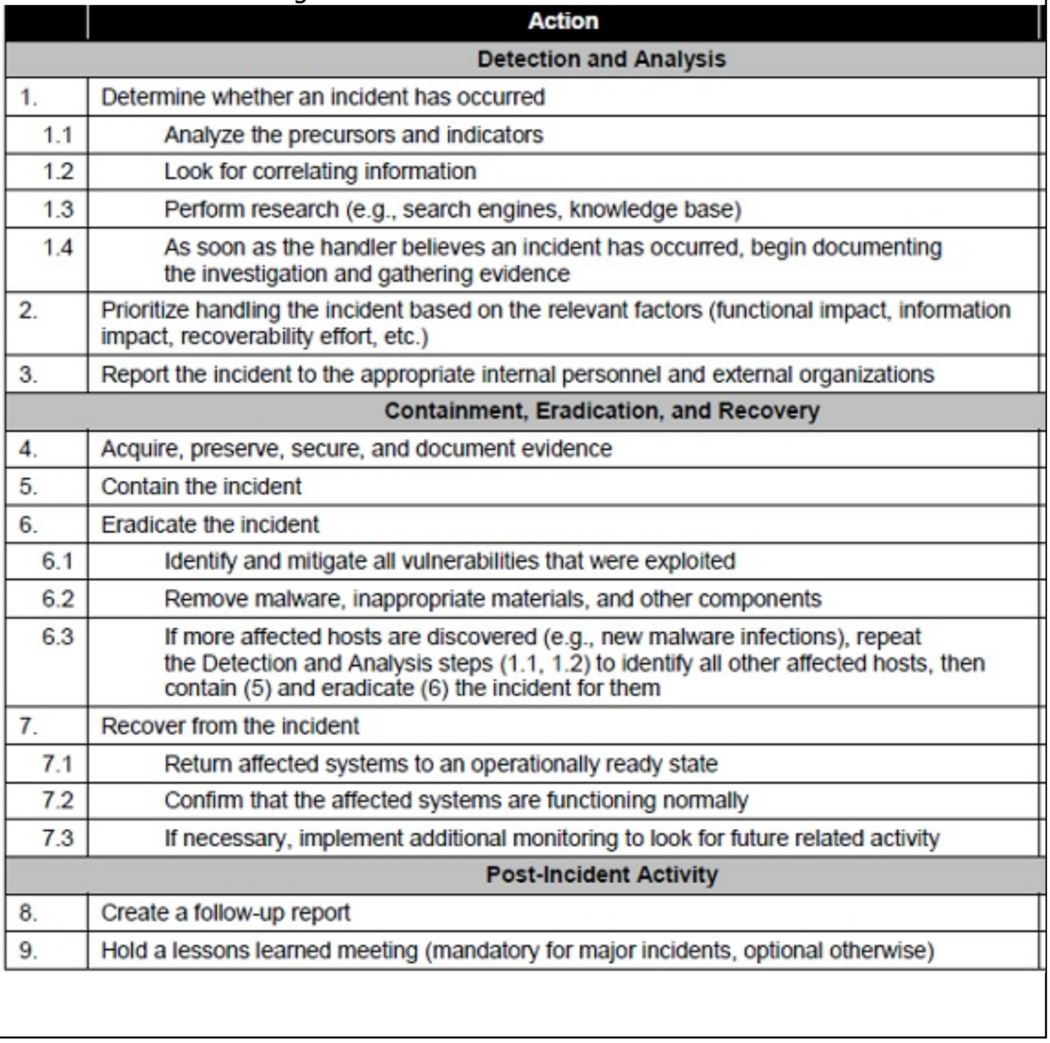
Content Template	
Section Number	1.3.12
Section Title	*Containment, Eradicating, and Recovery –* Identifying the attacking hosts
Introduction	// same as above
Content	Identifying the hosts that has been identified may be one of the most worrying issues arising when handling an incident. However; although it is a worrying issue focusing on minimizing the business impact is crucial. In order to identify the host been attacked the following activities are performed: • Validated and check the host IP address: • Search the host through the search engines. • Run an incident databases search • Monitor the communication channels to check if the attacker is using any.

Content Template	
Section Number	1.3.13
Section Title	*Containment, Eradicating, and Recovery –* Eradication and Recovery
Introduction	// same as above
Content	After the incident has been handled and all the processes around it has been done it is time for eradication and recovery. Eradication can happen by deleting malware and making sure there is no breaches on the systems. As for the recovery, system administrators start restoring the systems to the pints where they were functioning properly. They also start doing system clean backups, rebuilding the systems, installing new software, changing passwords tighten networks and other operations.

Content Template	
Section Number	1.3.14
Section Title	*Post incident activity –* lessons learned
Introduction	// same as above
Content	One of the stages that are usually overlooked after the incident is handled, is the learning and improving stage. This stage can be very informative as the threats can be studied, new technologies can be suggested and the security measures can be highly improved. Usually a meeting is conducted to answer a set of questions to address to the incident that has occurred, a sample of the questions that can be asked; • What happened? And what time? • How did the staff deal with the incident? Did the document all the procedures? How adequate were they? • What information was late? What could be provided sooner? • What should have been done to ensure a better recovery? Any steps were taken that delayed the recovery? • What are the rights and the wrongs done by the staff? • What was the information sharing strategy? Was it sufficient? Should it be done differently next time? • What tools are needed for next time that were missing this time? For small incident post incident activity can be hold right after incident handling. As for big incidents post incident activity is usually postponed until information sharing is finished. The agenda of the meeting should be clear and well written. Rules should be well established so moderators can run the meeting well. All the related documents should be reviewed and looked at in relation to its designated intervals. One final activity on the post-incident activity is the follow up report. This report provides works as a reference for future incident handling.
Content Template	
Section Number	1.3.15
Section Title	*Post incident activity –* using collected incident data
Introduction	// same as above
Content	The lessons learned should provide a set of subjective and objective data about each incident. These data accumulate over time to provide a background to study any threats or weakness in security systems and understanding the trends in systems' attacks. Also, these type of data pay a role in risk assessment and help in the development in implementation and control tools. There are a number of matrices for incident related data as follow: • Number of incidents handled The number of incident handled doesn't always need to be high. It is the quality of the incident handling and the efficiency. Usually for each incident category an incident count is done. • Time per incident The time indicator is one of the crucial elements in the process of measuring incident data, the amount of time labor spent working on the incident. The total cycle time from the time the incident was discovered till the time the incident was recovered. The time needed for the team to respond to the initial report for the incident. The needed time for the team to call for external help and external entities. • Objective assessment of each incident After each incident has occurred an objective assessment is conducted to evaluated the effectiveness of the it, these assessments can include: o Reviewing all the documentation related to the incident including log files, reports, policies and procedures.

	o The identification of indicators and precursors to define how an incident was located. o Defining the damages that was caused by the incident before it was located. o Define if the actual cause of the incident and what caused the attack, the vulnerability of the system and what are the weak points from a network and application perspective. • Subjective assessment per each incident Each team can do their own kind of assessment based on their performance. However; there are a general accepted practices to me evaluated as follow: • The policies, plans and producers. • The resources and tools. • The structure of the teams and models. • The education and training of the incident handler. • The documentation and reports. • All the measures discussed earlier.

Content Template	
Section Number	1.3.16
Section Title	*Post incident activity –* Evidence Retention
Introduction	// same as above
Content	Evidence retention should be covered by a policy by the organization, as they usually keep it for months for years based on its importance. However, it is kept based on a number of factors as following: • Prosecution: this is a very important issue, if the attacker is going to be prosecuted or not. Then the evidence should be retained for a longer time so any time it will be asked for it in the court of law it can be available. • Data retention: these are usually kept by organization policy that state for how long the data is kept. Each organization is different based on its internal policy. • Cost: keeping data is costly especially if data is stored for a long time. That cost piles up for hardware and hard disks and the space can be freed for other data to be put.

Content Template	
Section Number	1.4
Section Title	Incident handling checklist
Introduction	In this section the students should be able to • Summarize and understand the major steps for handling an incident.
Content	The actual steps for handling an incident may vary from one incident to another, however; this this a general checklist that incident handler can follow to make sure that all the general steps has been followed. Table 5: Incident handling checklist 

	Action
	Detection and Analysis
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
	Containment, Eradication, and Recovery
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
	Post-Incident Activity
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)

Content Template	
Section Number	1.5
Section Title	Recommendations
Introduction	In this section student should be able to • Give key recommendations on how to handle incidents
Content	The main recommendations any incident handler should follow are: • Acquire the tools: make sure to have the tools and recourses that have value during the incident handling process. These include all the hardware and software needed. • Incident prevention is always better than incident handling. This is done by securing the networks, systems and applications very well using antivirus, firewalls and spreading awareness through people. • Early identification of incidents is always better by identifying the precursors and indicators by understanding the different alerts that comes from the system. • Better communication with outside people and parties to report for any incidents by setting a policy or a reporting mechanism. • Leveling up the base line for logging in and auditing and especially for critical systems. • System and network profiling makes easier to measure the normal behavior of the system and network against the abnormal one. • Have a log retention policy? • Make a correlation between events to understand if there are any issues between different events. • Make all clocks synchronized. • Always have an information baseline of knowledge. • Start documenting all the information as soon as the incident starts. • All data regarding incidents should be kept safe. • Incidents should be prioritizing and dealt with based on severity not based on come first come first serve. • Incident should be reported according to its response policy. • Contain policies and strategies should be well established. • Evidences should follow clear procedures for both handling and gathering. • Any data captured from system can be used as evidence. • Digital forensics snapshots should be kept in disk images not in file systems. • Lessons learned should be documented in meetings after major and minor incidents.

Activity Template

Number 1.1

Title Identify the incident from the following scenario and apply the appropriate incident handling techniques.

Type Reflection

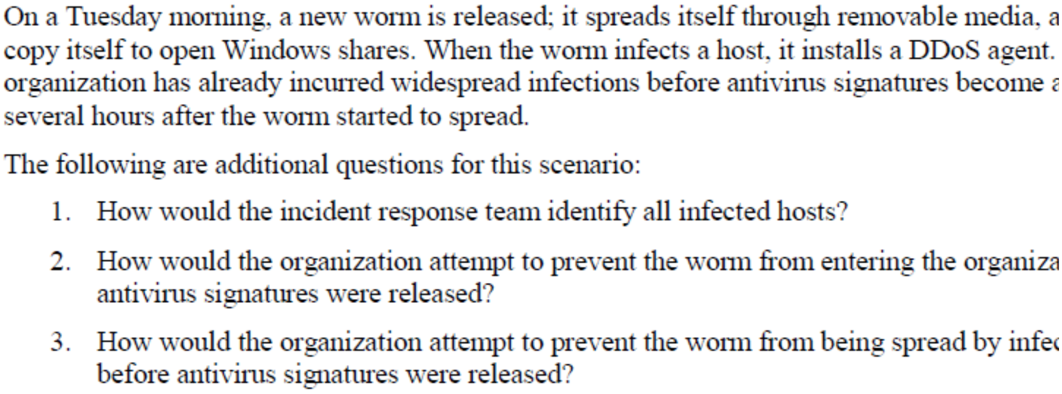
Aim ILOs: 6
Write standard policy and plan for handling and investigating security incidents.

Description Sections 1.3 and 1.4
https://csrc.nist.gov

Timeline Time: 1 hour of reading.

Assessment Each student is required to submit a one-page report of the possible implications and then present it in the class as open discussion session.

Scenario Worm and Distributed Denial f Service (DDoS) Agent Infestation



On a Tuesday morning, a new worm is released; it spreads itself through removable media, a copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. organization has already incurred widespread infections before antivirus signatures become a several hours after the worm started to spread.

The following are additional questions for this scenario:

1. How would the incident response team identify all infected hosts?
2. How would the organization attempt to prevent the worm from entering the organiza antivirus signatures were released?
3. How would the organization attempt to prevent the worm from being spread by infe before antivirus signatures were released?

Reference https://csrc.nist.gov

Think Template (MCQs)

Number	1.1
Title	**Introduction to Events and Incidents**
Type	Rank Options
Question	Incident handling goes through three main processes; these processes start from ________________ to ________________ to ________________.
Answers	a) data collection to data reporting to data analysis b) data reporting to data analysis to data collection c) data collection to data analysis to data reporting d) data reporting to data analysis to data collection **Answer: C**

Think Template (MCQs)

Number	1.2
Title	**The Need for Incident Response**
Type	Choose correct answer
Question	All of the following are incident response policy elements except:
Answers	a) Mission b) Management commitment c) Purpose, objectives, and scope d) Organizational structure and definition of roles, responsibilities, and levels of authority e) Prioritization or severity ratings of incidents f) Performance measures g) Reporting and contact forms. **Answer: A**

Think Template (MCQs)

Number 1.3

Title **Handling an Incident**

Type Choose correct answer

Question Risk Assessment can be considered as:

Answers A. Incident Prevention
B. Incident Handling
C. Incident Detection
D. Incident Indicator
E. All of the above

Answer: A

Think Template (MCQs)

Number 1.3

Title **Handling an Incident**

Type Match options

Question The factors that affect an incident is served as a priority are:

a) Functional impact of the incident.
b) Information impact of the incident.
c) Recoverability from the incident.
Match each of the factors to its sub factors.

Answers 1. Regular, Supplemented, Extended, Not-Recoverable
2. Minimal Effect, Losing Critical Services, Losing all Services
3. Privacy Breach, Proprietary Breach, Integrity Loss

Answer:
1 >>>> C
2 >>>> A
3 >>>> B

Think Template (MCQs)

Number	1.3
Title	**Handling an Incident**
Type	Choose correct answer
Question	In order to identify the host been attacked the following activities are performed:
Answers	a) Validated and check the host IP address: b) Search the host through the search engines. c) Run an incident databases search d) Monitor the communication channels to check if the attacker is using any. e) All of the above f) A + C + D only **Answer: E**

Think Template (MCQs)

Number	1.4
Title	**Incident handling checklist**
Type	Fill in the blank
Question	Determining whether ______________________ is the first check on the list.
Answers	a) an incident has actually occurred b) priorities has been considered c) incident was contained d) the organization has recovered from the incident e) a report has been drafted **Answer: A**

Extra Template

Number	1.1
Title	**Introduction to Events and Incidents**
Topic	**1.3**
Type	NIST Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Extra Template

Number	1.2
Title	**The Need for Incident Response**
Topic	**1.2**
Type	Guide to Integrating Forensic Techniques into Incident Response
	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Extra Template

Number	1.3
Title	**1.3 Incident handling**
Topic	1.1.1-1.1.16
Type	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

4. NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response ; by Prof. Rizik Alsayyed

Scope Template

Number 4

Title **NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response ; by Prof. Rizik Alsayyed**

Introduction This part presents "NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response". Advanced Forensics is a blend of customary criminal science, software engineering, and systems to extricate computerized proof from PCs, organize gadgets, gadgets, and computerized media. Computerized proof (information) put away in PCs or advanced frameworks or transmitted by them can be utilized in demonstrating or denying a wrongdoing that might be advanced or non-computerized. The primary point of advanced criminology is to address computerized violations, which are submitted utilizing PC equipment or those situated on computerized frameworks or systems. Computerized Forensics is the utilization of innovation methods in the criminal examination of illicit cases, including the examination of the gadget or framework target, investigation of activities and recovery of information and records so as to get an advanced proof utilized in legitimate examinations.

Outcomes Use innovation procedures in the criminal examination of illicit cases so as to acquire a computerized proof utilized in lawful examinations.
ILO1: Understand the major concepts related to forensics capability building
ILO2: Understand the details of the forensic process
ILO3: Understand the concepts of file, OS, and network forensics

Topics
4.1 Introduction
4.1.1 Publication Structure
4.2 Building up a Forensics Capability
4.2.1 Why Forensics? Which Staffing and What Other Teams?
4.2.2 Applied Policies
4.2.3Governed Procedures and Guidelines
4.2.4 Reached Recommendations
4.3 Phases of Forensic Process
4.3.1 Phase 1: Data Collection
4.3.2 Phase 2: Examination
4.3.3 Phase 3: Analysis
4.3.4 Phase 4: Reporting
4.3.5 Reached Recommendations
4.4 How to excerpt data from a given data
4.4.1 File Basics
4.4.2 Gathering Files
4.4.3 Examining Data Files
4.4.4 Extracted Data Analysis
4.4.5 Reached Recommendations
4.5 Using data from Operation Systems
4.5.1 OS Basics
4.5.2 Collecting OS Data
4.5.3 Examining and Analyzing OS Data
4.5.4 Reached Recommendations
4.6 Using Data From Network Traffic
4.6.1 TCP/IP Basics
4.6.2 Network Traffic Data Sources
4.6.3 Collecting Network Traffic Data
4.6.4Examining and Analyzing Network Traffic Data

4.6.5 Reached Recommendations
4.7 Using Data from Applications
4.8 Using Data from Multiple Sources

Study Guide

Task	**Time**
Preparation (Introduction and On-line Planning):	2 hr
Textbook Content:	6 hr
Thinking (On-line discussions, Review questions):	2 hr
Tutorial Work:	2 hr
Related Course Work:	2 hr
Total	**14 hours**

- Required external resources including links and books:

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. NIST Special Publication, 10(14), 800-86.

Content Template	
Chapter	4
Section Title	NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response
Introduction	This section abridges and displays an essential archive (NIST 800-86) and goes for helping associations to manage PC security occurrences. It likewise gives some reasonable direction on the legal execution of PCs and systems. SP 800-86 portrays the execution of viable legal exercises to help episode reaction and gives counsel on different information sources, including records, working frameworks, organize traffic and applications.
Content	Computer criminology or forensics is the way toward utilizing the most recent science and innovation information with software engineering to gather proof and submit it to criminal or common courts. The system director and security faculty who oversee and deal with the systems and data frameworks must have full information of computer crime scene investigation. The importance of the word scientific is to convey it to court. Measurable is a procedure that bargains in discovering proof and recuperating information. The manual incorporates numerous models, for example, fingerprints, DNA testing, total records on computer hard drives, etc. The unification of computer crime scene investigation has not been unequivocally perceived and united through the courts since it is another framework. It is basic that the system administrator and security work force in system related foundations practice computer legal sciences and must be comfortable with the laws on the grounds that the rate of cybercrime increments drastically. It is extremely intriguing for chiefs and representatives who need to know how computer crime scene investigation can turn into a key component in the security of their association. Workers, security staff and the system overseer should realize all issues identified with scientific prescription. Computer specialists utilize propelled devices and systems to recuperate erased, harmed, or harmed information and proof against assaults and interruptions. This proof is gathered to seek after cases in criminal and common courts against those wrongdoers who have carried out computer crimes. There are numerous dangers in the event that you practice criminology for your PC severely. On the off chance that you don't consider, indispensable proof might be obliterated. New laws are being created to secure customer information; yet on the off chance that a specific kind of information isn't appropriately ensured, numerous duties can be allocated to the association. New guidelines can convey associations to criminal or common courts if associations neglect to ensure customer information. Endeavor assets can likewise be spared by applying scientific proof to the computer.

Content Template	
Section Number	4.1
Section Title	Introduction
Introduction	This is a prologue to give the peruser an introduction about the topic; for the most part: the expert, the reason and extension, the audience, and the structure of publication.
Content	This chapter introduces "NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response". Digital Forensics is a combination of traditional criminal science, computer science, and networks to extract digital evidence from computers, network devices, devices, and digital media. Digital evidence (data) stored in computers or digital systems or transmitted by them can be used in proving or denying a crime that may be digital or non-digital. The main aim of digital forensics is to address digital crimes, which are committed using computer hardware or those located on digital systems or networks. Digital Forensics is the use of technology techniques in the criminal investigation of illegal cases, including the examination of the device or system target, analysis of operations and retrieval of data and files in order to obtain digital evidence used in legal investigations. The body that built up this document (distribution) on upgrading the lawful obligation regarding data security the executives for 2002 is the National Institute of Standards and Technology (NIST) and has turned into the open law 107-347. This rule is set up for use by government offices. Non-administrative associations may utilize them on an intentional premise and are not expose to copyright, despite the fact that attribution is required. Nothing in this record will be translated as conflicting with the norms and rules made by the Minister of Commerce compulsory and official on government organizations under the legitimate specialist. These Guidelines will not be understood as modifying or supplanting the present forces of the Minister of Commerce, the Director of OMB or some other government official. This rule ought not be viewed as authoritative on law authorization authorities for the examination of crime. The reason for this distribution is to help associations in checking PC wellbeing episodes and to investigate and investigate some operational IT issues by giving down to earth direction on the execution of PC and system crime scene investigation. Gives legal proof from an IT point of view, not from a law authorization viewpoint; explicitly, the distribution depicts the working of successful legal exercises and gives exhortation on different information sources, including documents, working frameworks (OS), organize traffic and applications. The distribution ought not be utilized as a well ordered manual for the usage of computerized measurable examination or its translation as legitimate counsel. Its motivation is to illuminate perusers of the different advancements and conceivable approaches to utilize them in the execution of occurrence reaction or investigating exercises. Perusers are encouraged to apply suggested rehearses simply after interview with the administration and lawful insight to consent to laws and guidelines (ie neighborhood, state, government, and global) identifying with their status. This distribution was mainly made for teams of incident response, measurable experts, framework executives, system and security; computer security program administrators and scientific proof supervisors for examination, occurrence reaction or investigating purposes. Suggested rehearses.

Content Template	
Section Number	4.1.1
Section Title	Publication Structure
Introduction	This is a prologue to give the peruser an introduction about the topic; for the most part: the expert, the reason and extension, the audience, and the structure of publication.
Content	The rest of this publication is organized as follows: Section 4.2 provides information about to build up a forensics capability. Section 4.3 discusses the phases of forensic process. Section 4.4 presents how to excerpt data from a given data. Section 4.5 shows how to use data from operation systems, section 4.6 shows how to use data from network traffic, and section 4.7 is concerned with using data from applications, while using data from multiple sources is covered in section 4.8.

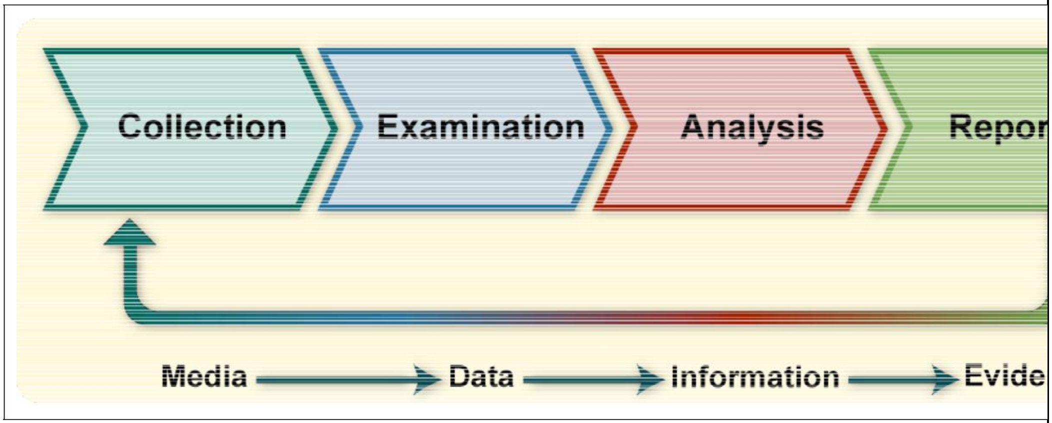
Content Template	
Section Number	4.2
Section Title	Building up a Forensics Capability
Introduction	This section discusses many aspects of the institution's forensic capacity management.
Content	This part talks about numerous parts of the establishment's measurable limit the board. It starts by appearing wide scope of potential employments of crime scene investigation, and afterward gives an abnormal state outline of the criminological procedure. The following sub-area of the subsection talks about how to give commonplace scientific administrations and gives direction on structure and keeping up the abilities expected to perform measurable errands. The Section likewise discloses the need to incorporate different groups from everywhere throughout the association, for example, legitimate consultants and physical security work force, in some criminological exercises. The area finishes up with a discourse of how to deal with scientific arrangements, rules and strategies, (for example, characterizing jobs and obligations, giving direction on the right utilization of apparatuses and methods, and coordinating legal sciences into the existence cycle of the data framework). The methods and procedures in this manual depend on the standards of advanced crime scene investigation. Legal science is commonly characterized as the utilization of science to law. Advanced legal sciences, otherwise called PC crime scene investigation and the system, has numerous definitions. All in all, the use of science is to distinguish, gather, look at and dissect information while keeping up data honesty and keeping up an exacting chain of information preservation. Since various associations are liable to various laws and guidelines, this distribution ought not to be utilized as a manual for the usage of computerized criminological examination or its elucidation as legitimate counsel or as a reason for exploring crime. Rather, associations should utilize this guide as a beginning stage for the improvement of measurable limit related to extensive direction given by legitimate consultants, law requirement officers and the board.

Content Template	
Section Number	4.2.1
Section Title	Why Forensics? Which Staffing and What Other Teams?
Introduction	This section discusses many aspects of the institution's forensic capacity management
Content	Over the previous decade, the quantity of computer related violations has expanded, impelling an expansion in organizations and items that mean to help law implementation use computer based proof to figure out who, where, when, and how, for wrongdoings. Thus, computer and system criminology have developed to guarantee that proof of computerwrongdoings is legitimately submitted to the court. Scientific instruments and strategies are regularly considered with regards to criminal examinations and computer security occurrences - used to react to an occasion by researching suspected frameworks, gathering and looking after proof, recreating occasions, and evaluating the ebb and flow condition of an occasion. Nevertheless, scientific instruments and systems are additionally valuable for some different sorts of undertakings, for example, • Operational Troubleshooting, such as detecting incorrect network configuration • Log Monitoring, such as analyzing log entries over multiple systems • Data Recovery, such as restoring deleted entries/data • Data Acquisition, such as collecting data from hosts being redeployed or retired • Due Diligence/Regulatory Compliance, such as protecting data by following the organization’s information protection policy Notwithstanding the circumstance, the legal procedure incorporates the accompanying fundamental stages: • Collection, by identifying and acquiring data from all possible sources • Examination, by forensically processing acquired data • Analysis, using legally justifiable methods to derive useful information from the examined data • Reporting the results of the analysis The **essential clients** of criminological instruments and strategies inside the association can be categorized as: • Investigators responsible of investigating allegations of misconduct. • IT Professionals responsible of performing simple forensic tasks related to their fields of expertise • Incident Handlers responding to variety of computer security incidents using wide variety of tools and techniques during investigations. While recognizing interior or outside gatherings that must arrangement with each part of measurable science, associations ought to think about the accompanying elements: • Cost. • Response Time. • Data Sensitivity. To **encourage correspondence between groups**, each group must relegate at least one contact focuses. These people are in charge of knowing the experience of every individual from the group and guiding request for help to the ideal individual. Associations ought to keep up a rundown of contacts that suitable groups can allude to when required. The rundown ought to incorporate both standard specialized techniques, (for example, office telephone) and crisis, (for example, PDA).

Content Template	
Section Number	4.2.2
Section Title	Applied Policies
Introduction	This section discusses many aspects of the institution's forensic capacity management
Content	Organizations ought to guarantee that their arrangements contain clear proclamations that address all major legal contemplations, for example, reaching law authorization, performing checking, and leading customary surveys of criminological approaches, rules, and methodology. At an abnormal state, arrangements ought to enable approved work force to screen frameworks and organizes and perform examinations for real reasons under suitable conditions. Associations may likewise have a different approach for episode handlers and others with criminological jobs; this arrangement would give increasingly point by point principles to fitting conduct. Such work force ought to be acquainted with and comprehend the arrangement. Approaches may should be refreshed much of the time, especially for associations that length numerous wards, due to changes to laws and guidelines, just as new court decisions. Furthermore, the association's measurable strategy ought to be predictable with the association's different strategies, including arrangements identified with sensible desires for security.

Content Template	
Section Number	4.2.3
Section Title	Governed Procedures and Guidelines
Introduction	This section discusses many aspects of the institution's forensic capacity management
Content	Each organization ought to make and keep up rules and techniques for performing legal assignments, in light of the organization's arrangements, occurrence reaction staffing models, and different groups recognized as members in legal exercises. An organization's legal rules ought to incorporate general strategies for examining an occurrence utilizing measurable methods, since it isn't attainable to create thorough techniques custom fitted to each conceivable circumstance. Data is quickly moving to a structure in which all the data resources exist in electronic structure. In both general society and private divisions, it is progressively vital to exhibit decisively the validness, believability, and unwavering quality of electronic records, for example, the execution of a particular activity or choice, or the presence of a specific thing of data. Measurable rules and methodology ought to be predictable with the organization's approaches and every single pertinent law. The rules and systems should bolster the acceptability of proof into lawful procedures, including data on social affair and taking care of proof legitimately, protecting the trustworthiness of instruments and gear, keeping up the chain of care, and putting away proof safely. It is additionally imperative to keep up the rules and systems once they are made with the goal that they stay exact.

Content Template	
Section Number	4.2.4
Section Title	Reached Recommendations
Introduction	This section discusses many aspects of the institution's forensic capacity management
Content	The key proposals on setting up and sorting out a measurable ability are as per the following: • Organizations ought to have a capacity to perform computer and network legal sciences. • Organizations ought to figure out which gatherings should deal with every part of crime scene investigation. • Incident taking care of groups ought to have powerful criminological capacities. • Many groups inside an association ought to partake in crime scene investigation. • Forensic contemplations ought to be unmistakably tended to in strategies. • Organizations ought to make and keep up rules and systems for performing measurable undertakings.

Content Template	
Section Number	4.3
Section Title	Phases of Forensic Process
Introduction	In this section, the phases of the forensics will be described.
Content	This part depicts the fundamental phases of the criminological procedure: collection, examination, investigation and revealing. Amid gathering, information identifying with a specific occasion is resolved, ordered, recorded, gathered, and kept up. In the second stage, the examination and the fitting scientific devices and instruments are performed for the information types gathered to distinguish and remove the important data from the information gathered with its security insurance. The output may utilize a scope of robotized devices and manual procedures. The following stage; investigation, dissects the aftereffects of the test to infer valuable data tending to the inquiries that spurred the gathering and examination. The last stage incorporates writing about the aftereffects of the investigation, which may incorporate portraying finished methods, recognizing different activities to be embraced, and prescribing upgrades in strategies, rules, techniques, apparatuses and different parts of the criminological procedure.  Collection Examination Analysis Repor Media Data Information Evide **Figure 4.3-1. Forensic Process** As can be seen at the base of figure 4.3-1, the legal procedure transforms the media into a proof (evidence), regardless of whether proof is essential for law implementation or for the inner utilization of the organization. In particular, the primary move happens while looking at information gathered, which separates information from the media and changes over it into an arrangement that can be prepared by legal apparatuses. Second, information is changed over into data through examination. At last, the change of data into learning to-business exchange guides is undifferentiated from utilizing the data that the examination delivers in at least one different ways amid the detailing stage. For instance, it tends to be utilized as a manual for help sue a specific individual or implementable data to help stop or moderate some movement or information in making new prospects for a circumstance.

Content Template	
Section Number	4.3.1
Section Title	Phase 1: Data Collection
Introduction	In this section, the phases of the forensics will be described.
Content	The initial phase in the criminological procedure is to distinguish potential wellsprings of information and acquire information from them. First part portrays an assortment of accessible information sources and talks about moves that foundations can make to help the nonstop gathering of information for measurable purposes. Second part portrays suggested ventures for information gathering, including extra activities to help lawful or inward disciplinary activities. Third part talks about occurrence reaction contemplations, underscoring the need to survey the estimation of information gathered versus the expenses and effect of the association of the accumulation procedure. • Possible Sources of Data Identification: Wellsprings of personal computers, servers, arrange capacity gadgets, and workstations are the most obvious and normal wellsprings of information. These frameworks regularly contain inward media-satisfactory drives, for example, CDs and DVDs, and contain a few sorts of ports (for instance, Universal Serial Bus [USB], Firewire, and the International Personal Computer Memory Association (PCMCIA) External information on which media and gadgets can be appended. Notwithstanding PC related gadgets, numerous sorts of versatile computerized gadgets, (for example, PDAs, cell phones, advanced cameras, computerized recorders, and sound players) may likewise contain information. Investigators ought to have the capacity to check a physical zone, for example, an office, and distinguish potential wellsprings of information. Investigators ought to likewise consider potential information sources somewhere else. Gaining or Acquiring the Data: In the wake of distinguishing conceivable information sources, the investigator needs to get information from the sources. Information gathering ought to be finished utilizing a three-advance procedure: build up an arrangement to acquire information, get information, and check the honesty of the information got. In spite of the fact that the accompanying things give a review of these three stages, the particular subtleties behind stages 2 and 3 vary contingent upon the kind of information that is gotten. Subsections 4.4.2, 4.5.2, 4.6.3, and 4.7.3 give increasingly itemized clarifications to the uprightness and veracity of information documents, working framework information, organize traffic information, and application information, individually. 1. Develop an active plan to gain the data; keep in mind: • Possible Value. • Volatility. • Required Efforts Amount. 2. Di gain/collect the data. 3. Verify data integrity. • Before the analyst starts gathering data, a choice ought to be made by the investigator or the executives (as per the organization's arrangements and lawful counsels) on the need to gather and protect proof such that underpins its utilization in future legitimate or inner disciplinary procedures. In such circumstances, an obviously characterized chain of guardianship ought to be pursued to stay away from claims of misusing or altering of proof. This includes keeping a log of each individual who had physical authority of the proof, archiving the activities that they performed on the proof and at what time, putting away the proof in a protected area when it isn't being utilized, making a duplicate of the proof and performing examination and investigation utilizing just the replicated proof, and checking the uprightness of the

	first and replicated proof. On the off chance that it is hazy whether proof should be protected, as a matter of course it by and large ought to be safeguarded. • Considerations to Incident Response: During the response to an incident and when performing forensics, a critical inquiry that ought to be considered is: how and when the occurrence ought to be contained?

Content Template	
Section Number	4.3.2
Section Title	Phase 2: Examination
Introduction	In this section, the phases of the forensics will be described.
Content	After information has been gathered, the following stage is to look at the information, which includes evaluating and extricating the applicable snippets of data from the gathered information. This stage may likewise include bypassing or relieving OS or application includes that dark information and code, for example, information pressure, encryption, and access control components. A gained hard drive may contain a huge number of information documents; recognizing the information records that contain data of enthusiasm, including data covered through document pressure and access control, can be an overwhelming assignment. Also, information documents of intrigue may contain unessential data that ought to be sifted. For instance, yesterday's firewall log may hold a huge number of records; however, just five of the records may be identified with the occasion of intrigue.

Content Template	
Section Number	4.3.3
Section Title	Phase 3: Analysis
Introduction	In this section, the phases of the forensics will be described.
Content	When the pertinent data has been removed, the expert should examine and break down the information to make determinations from it. The establishment of criminology is utilizing a systematic way to deal with achieve suitable ends dependent on the accessible information or confirm that no end can yet be drawn. The examination ought to incorporate recognizing individuals, spots, things, and occasions, and deciding how these components are connected with the goal that an end can be come to. Frequently, this exertion will incorporate corresponding information among various sources. For example, a system interruption location framework (IDS) log may connect an occasion to a host, the host review logs may interface the occasion to a particular client account, and the host IDS log may demonstrate what activities that client performed. Devices, for example, incorporated logging and security occasion the board programming can encourage this procedure via naturally assembling and relating the information. Contrasting framework qualities with realized baselines can recognize different kinds of changes made to the framework. We portray this examination procedure in more detail in the last section.

Content Template	
Section Number	4.3.4
Section Title	Phase 4: Reporting
Introduction	In this section, the phases of the forensics will be described.
Content	Lastly we do the reporting stage, which is the way toward getting ready and exhibiting the data coming about because of the examination stage. Numerous elements influence revealing, including the accompanying: • Alternative Explanations. At the point when the data in regards to an occasion is deficient, it may not be conceivable to touch base at a complete clarification of what occurred. At the point when an occasion has at least two conceivable clarifications, each ought to be given due thought in the announcing procedure. Investigators should utilize an efficient way to deal with endeavor to demonstrate or refute every conceivable clarification that is proposed. • Audience Consideration. Knowing the group of onlookers to which the information or data will be appeared vital. An episode requiring law implementation inclusion requires exceptionally nitty gritty reports of all data accumulated, and may likewise require duplicates of every single evidentiary datum got. A framework overseer should need to see arrange traffic and related insights in extraordinary detail. Senior administration may basically need an abnormal state review of what occurred, for example, an improved visual portrayal of how the assault happened, and what ought to be done to counteract comparative episodes. • Actionable Information. Detailing additionally incorporates distinguishing significant data picked up from information that may enable an expert to gather new wellsprings of data. For instance, a rundown of contacts might be created from the information that may prompt extra data around an episode or wrongdoing. Likewise, data may be gotten that could anticipate future occasions, for example, a secondary passage on a framework that could be utilized for future assaults, a wrongdoing that is being arranged, a worm booked to begin spreading at a specific time, or a weakness that could be abused.

Content Template	
Section Number	4.3.5
Section Title	Reached Recommendations
Introduction	In this section, the phases of the forensics will be described.
Content	The key suggestions presented in this subsection for the criminological procedure are as per the following: • Organizations ought to perform crime scene investigation utilizing a predictable procedure. • Analysts ought to know about the scope of conceivable information sources. • Organizations should be proactive in gathering helpful information. • Analysts ought to perform information accumulation utilizing a standard procedure. • Analysts should utilize a systematic way to deal with contemplating the information. • Analysts should survey their procedures and practices.

Content Template	
Section Number	4.4
Section Title	How to excerpt data from a given data
Introduction	This part exhibits the normal media types and filesystems
Content	This part gives an outline of the most widely recognized media types and filesystems—strategies for naming, putting away, sorting out, and getting to documents. It at that point talks about how records ought to be gathered and how the honesty of the documents ought to be safeguarded. The subsection likewise talks about different specialized issues identified with record recuperation, for example, recouping information from erased documents. The last bit of the area depicts the examination and investigation of documents, giving direction on devices and strategies that can help investigators. A file (or data file) is a gathering of data consistently assembled into a solitary element and referenced by a one of a kind name, for example, a filename. A record can be of numerous information types, including an archive, a picture, a video, or an application. Fruitful legal handling of PC media relies upon the capacity to gather, look at, and investigate the documents that live on the media.

Content Template	
Section Number	4.4.1
Section Title	File Basics
Introduction	This part exhibits the normal media types and filesystems
Content	Before endeavoring to gather or look at documents, experts ought to have a sensibly exhaustive comprehension of records and filesystems. To start with, investigators ought to know about the assortment of media that may contain records; first media type (File Storage Media) gives a few instances of the media utilized in PCs and different kinds of advanced gadgets.Second media type clarifies how filesystems are utilized to arrange records and gives an outline of a few normal filesystems. Third media type talks about how information from erased documents can even now exist inside filesystems. **File Storage Media** The across the board utilization of PCs and other computerized gadgets has brought about a noteworthy increment in the quantity of various media types that are utilized to store documents. Notwithstanding conventional media types, for example, hard drives and floppy circles, records are frequently put away on customer gadgets, for example, PDAs and phones, just as on more up to date media types, for example, streak memory cards, which were made prominent by computerized cameras. Table 4 - 1 records media types that are generally utilized on PCs and computerized gadgets. This rundown does exclude each medium sort accessible; rather, it is expected to demonstrate the assortment of media types that an expert may go over. **Filesystems** Before media can be utilized to store records, the media should for the most part be apportioned and designed into intelligent volumes. Apportioning is the demonstration of legitimately partitioning a media into segments that work as physically separate units. A sensible volume is a segment or a gathering of parcels going about as a solitary element that has been organized with a filesystem. A few media types, for example, floppy circles, can contain at most one segment (and thus, one sensible volume). The organization of the coherent volumes is dictated by the chose filesystem A filesystem characterizes how documents are named; put away, sorted out, and got to on intelligent volumes. Various filesystems exist, each giving one of a kind highlights and information structures. Be that as it may, all filesystems share some normal attributes. To start with, they utilize the ideas of catalogs and documents to sort out and store information. Registries are hierarchical structures that are utilized to bunch records. Notwithstanding documents, indexes may contain different registries called subdirectories. Second, filesystems utilize a few information structures to point to the area of records on media. Furthermore, they store every datum document kept in touch with media in at least one record assignment units. These are alluded to as bunches by some filesystems (e.g., File Allocation Table [FAT], NT File System [NTFS]) and as squares by different filesystems (e.g., UNIX and Linux). A document allotment unit is basically a gathering of parts, which are the littlest units that can be gotten to on media. **Other Data on Media** As depicted in the second media type, filesystems are intended to store documents on media. Notwithstanding, filesystems may likewise hold information from erased records or before variants of existing documents. This information can give imperative data. (Subsection 4.4.2 examines systems for gathering this kind of information.) The data includes:

	•Deleted Files. •Slack Space. •Free Space.

Content Template	
Section Number	4.4.2
Section Title	Gathering Files
Introduction	This part exhibits the normal media types and filesystems
Content	While gathering data, the investigator should make various duplicates of the significant documents or filesystems—commonly an ace duplicate and a working copy. The examiner would then be able to utilize the working duplicate without influencing the first records or the ace duplicate. First subsection depicts the essential strategies and devices for duplicating documents and leftover record information from media. Second subsection talks about the significance of keeping up the respectability of the records and gives direction on equipment and programming that can help with safeguarding and confirming document honesty. Usually critical to gather the documents, yet additionally noteworthy timestamps for the records, for example, when the documents were last adjusted or gotten to. Third subsection portrays the timestamps and clarifies how they can be saved. Other specialized issues identified with document accumulation, for example, finding concealed records and duplicating documents from excess cluster of economical plates (RAID) executions, are tended to in the last subsection. **First subsection : Copying Files from Media** Documents can be duplicated from media utilizing two distinct strategies: •Logical Backup. •Bit Stream Imaging. **Second subsection : Data File Integrity** To guarantee that the reinforcement or imaging process does not adjust information on the original media, examiners can utilize a review blocker while doing backing up or imaging the media. **Third subsection : File Modification, Access, and Creation Times** Some data are imperative to be think about documents and should be recorded: •Modification Time. •Access Time. •Creation Time. **Fourth subsection : Technical Issues** A few specialized issues may emerge in gathering information records. As noted in the first subsection, the essential issue is the gathering of erased records and leftovers of documents existing in free and slack space on media. People can utilize an assortment of strategies to impede the gathering of such information.

Content Template	
Section Number	4.4.3
Section Title	Examining Data Files
Introduction	This part exhibits the normal media types and filesystems
Content	This subsection describes the procedures associated with looking at records and information, just as strategies that can speed up examination. **First subsection : Locating the Files** The plate picture can catch numerous gigabytes of free space and free space, which may contain a large number of documents and record parts. Physically extricating information from unused space can be a tedious and troublesome procedure, since it requires learning of the essential record framework position. Luckily, there are numerous instruments that can computerize the way toward extricating information from unused space and sparing it in information records, just as reestablishing erased documents and records inside the reusing holder. **Second subsection : Extracting the Data** Investigators can all the more precisely recognize the kind of information put away in numerous documents by taking a gander at their record headers. **Third subsection : Using a Forensic Toolkit** Investigators ought to approach different apparatuses that empower them to perform examinations and examination of information, just as some accumulation exercises. Numerous scientific items enable the investigator to play out a wide scope of procedures to examine documents and applications, just as gathering records, perusing plate pictures, and extricating information from documents. Most investigation items additionally offer the capacity to create reports and to log all mistakes that happened amid the examination. In spite of the fact that these items are important in performing investigation, it is basic to comprehend which procedures ought to be raced to respond to specific inquiries concerning the information. An investigator may need to give a speedy reaction or simply answer a basic inquiry regarding the gathered information. In these cases, a total criminological assessment may not be important or even possible. The scientific toolbox ought to contain applications that can achieve information examination and investigation from multiple points of view and can be run rapidly and productively from floppy plates, CDs, or a measurable workstation. The accompanying procedures are among those that an investigator ought to have the capacity to perform with an assortment of apparatuses: •Using File Viewers. •Uncompressing Files. •Graphically Displaying Directory Structures. •Identifying Known Files. •Performing String Searches and Pattern Matches. •Accessing File Metadata.

Content Template	
Section Number	4.4.4
Section Title	Extracted Data Analysis
Introduction	This part exhibits the normal media types and filesystems
Content	After finishing the examination, analysis to the extracted data has to be performed. As pointed out in subsection 4.4.3, there are numerous apparatuses accessible that can be useful in examination of various sorts of information. When utilizing these apparatuses or performing manual surveys of information, experts ought to know about the benefit of utilizing framework times and document times.

	Knowing when an episode happened, a record was made or altered, or an email was sent can be basic to measurable examination. For instance, such data can be utilized to recreate a course of events of exercises. In spite of the fact that this may appear to be a straightforward errand, usually convoluted by inadvertent or deliberate errors in time settings among frameworks. Knowing the time, date, and time zone settings for a PC whose information will be broke down can extraordinarily help an expert; Section 4.5 portrays this in more detail.

Content Template	
Section Number	4.4.5
Section Title	Reached Recommendations
Introduction	This part exhibits the normal media types and filesystems
Content	The key suggestions exhibited in this subsection for utilizing information from information documents are as per the following. • Analysts ought to look at duplicates of records, not the first documents. • Analysts should protect and confirm record honesty. • Analysts ought to depend on record headers, not document expansions, to recognize record content sorts. • Analysts ought to have a measurable toolbox for information examination and investigation.

Content Template	
Section Number	4.5
Section Title	Using data from Operation Systems
Introduction	Data collected from operating systems will be helpful to provide guidance for analysis.
Content	This section talks about the parts of an OS that may be significant to crime scene investigation and gives direction on gathering, looking at, and dissecting information from regular workstation and server OSs.

Content Template	
Section Number	4.5.1
Section Title	OS Basics
Introduction	Data collected from operating systems will be helpful to provide guidance for analysis.
Content	The OS data exists in two states: volatile and non-volatile.Non-volatile data alludes to data that perseveres even after a PC is shut down, for example, a filesystem put away on a hard drive. Volatile data alludes to data on a live framework that is lost after a PC is shut down, for example, the present system associations with and from the framework. Numerous kinds of non-volatile and volatile data might be of enthusiasm from a legal sciences point of view. This subsectiontalks about both of these kinds of OS data. **First subsection : Non-Volatile Data** The essential wellspring of non-unpredictable information inside an OS is the filesystem. The filesystem is likewise as a rule the biggest and most extravagant wellspring of information inside the OS, containing the vast majority of the data recouped amid a common legal occasion. The filesystem gives stockpiling to the OS on at least one media. A filesystem regularly contains numerous kinds of records, every one of which might be of an incentive to experts in various circumstances. What's more, as noted in the second subsection, essential remaining information can be recouped from unused filesystem space. A few kinds of information that are ordinarily found inside OS filesystems are as per the following: • **Configuration Files**. The OS may utilize design documents to store OS and application settings. For instance, setup documents could list the administrations to be begun consequently after framework boot, and determine the area of log records and impermanent records. Clients may likewise have singular OS and application design records that contain client explicit data and inclinations, for example, equipment related settings (e.g., screen goals, printer settings) and document affiliations. Design documents quite compelling are as per the following: – Users and Groups – Password Files. – Scheduled Jobs. • **Logs**. OS log records contain data about different OS occasions, and may likewise hold application-explicit occasion data. Contingent upon the OS, logs might be put away in content documents, exclusive arrangement paired records, or databases. Some OSs composes log sections to at least two separate documents. The sorts of data normally found in OS logs are as per the following: – System Events. – Audit Records. – Application Events – Command History. – Recently Accessed Files. • **Application Files**. Applications can be made out of numerous sorts of records, including executable, contents, documentation, design records, log records, history records, illustrations, sounds, and symbols. Section 4.7 gives a top to bottom exchange of utilization records. • **Data Files**. Information documents store data for applications. Instances of normal information records are content records, word preparing reports, spreadsheets, databases, sound documents, and illustrations documents. Furthermore, when information is printed, most OSs makesat least one brief print document that contains the print-prepared rendition of the

information. Sections 4.4 and 4.7 talk about application information records in more profundity.

• **Swap Files**. Most OSs use swap documents related to RAM to give impermanent capacity to information regularly utilized by applications. Swap documents basically broaden the measure of memory accessible to

• **Dump Files**. Some OSs can store the substance of memory naturally amid a mistake condition to aid resulting investigating. The document that holds the put away memory substance is known as a dump record.

• **Hibernation Files**. A hibernation document is made to protect the present condition of a framework (ordinarily a workstation) by account memory and open records before stopping the framework. At the point when the framework is next turned on, the condition of the framework is reestablished.

• **Temporary Files**. Amid the establishment of an OS, application, or OS or application updates and redesigns, brief documents are regularly made. Albeit such documents are normally erased toward the finish of the establishment procedure, this does not generally happen. Moreover, transitory records are made when numerous applications are run; once more, such documents are generally erased when the application is ended, however this does not generally occur. Impermanent documents could contain duplicates of different records on the framework, application information, or other data.

Second subsection : Volatile Data

OSs execute inside the RAM of a framework. While the OS is working, the substances of RAM are always showing signs of change. At some random time, RAM may contain numerous sorts of information and data that could be of intrigue. For instance, RAM regularly contains much of the time and as of late gotten to information, for example, information documents, secret key hashes, and late directions. What's more, as filesystems, RAM can contain remaining information in slack and free space, as pursues:

• **Slack Space**. Memory slack space is substantially less deterministic than document slack space. For instance, an OS by and large oversees memory in units known as pages or squares, and apportions them to mentioning applications. In some cases, in spite of the fact that an application probably won't demand a whole unit, it is given one at any rate. Leftover information could in this way live in the unit of memory allotted to an application, in spite of the fact that it probably won't be addressable by the application. For execution and effectiveness, some OSs differ the extent of the units they allot, which will in general outcome in littler memory slack spaces.

• **Free Space**. Memory pages are designated and deallocated much like record bunches. When they are not allotted, memory pages are regularly gathered into a typical pool of accessible pages—a procedure frequently alluded to as refuse accumulation. It isn't phenomenal for leftover information to live in these reusable memory pages, which are closely resembling unallocated document bunches.

• Some other noteworthy kinds of unstable information that may exist inside an OS are as per the following:

• **Network Configuration**. Albeit numerous components of systems administration, for example, arrange interface card (NIC) drivers and setup settings, are normally put away in the filesystem, organizing is dynamic in nature. For instance, numerous hosts are allocated Internet Protocol (IP) addresses progressively by another host, implying that their IP addresses are not part of the put away arrangement. Numerous hosts additionally have different system interfaces characterized, for example, wired, remote, virtual private system (VPN), and modem; the present system arrangement shows which interfaces are as of now being used. Clients additionally might probably adjust arrange interface setups from the defaults, for example, physically changing IP addresses. In like manner, investigators should utilize the present system design, not the put away arrangement, at whatever point conceivable.

• **Network Connections**. The OS encourages associations between the framework and different frameworks. Most OSs can give a rundown of current approaching and active system associations, and some OSs can list ongoing associations also. For approaching associations, the OS normally shows which assets are being utilized, for example, document offers and printers. Most OSs can likewise give a rundown of the ports and IP addresses at which the framework is tuning in for associations. Section4.6 gives a top to bottom examination of the importance of system associations.

• **Running Processes**. Procedures are the projects that are at present executing on a PC. Procedures incorporate administrations offered by the OS and applications kept running by directors and clients. Most OSs offer approaches to see a rundown of the as of now running procedures. This rundown can be concentrated to decide the administrations that are dynamic on the framework, for example, a Web server, and the projects that singular clients are running (e.g., encryption utility, word processor, email customer). Procedure records may likewise show which direction choices were utilized, as depicted in Section 4.7. Recognizing the running procedures is likewise useful for distinguishing programs that ought to run yet have been incapacitated or evacuated, for example, antivirus programming and firewalls.

• **Open Files**. OSs may keep up a rundown of open records, which normally incorporates the client or procedure that opened each document.

• **Login Sessions**. OSs normally keep up data about presently signed in clients (and the begin time and span of every session), past fruitful and fizzled logons, special use, and impersonation.65 However, login session data may be accessible just if the PC has been designed to review logon endeavors. Logon records can decide a client's PC use propensities and affirm whether a client account was dynamic when a given occasion happened.

• **Operating System Time**. The OS keeps up the present time and stores light reserve funds time and time zone data. This data can be valuable when assembling a course of events of occasions or corresponding occasions among various frameworks. Experts ought to know that the time introduced by the OS may contrast from that displayed by the BIOS due to OS-explicit settings, for example, time zone.

Content Template	
Section Number	4.5.2
Section Title	Collecting OS Data
Introduction	Data collected from operating systems will be helpful to provide guidance for analysis.
Content	As mentioned in subsection 4.5.1, OS data exists in two states: non-volatile and volatile. Non-volatile OS data, for example, filesystem data can be gathered utilizing the methodologies talked about in Section 4 for performing legitimate reinforcements and bit stream imaging. Volatile OS data ought to be gathered before the PC is shut down. The first and the second subsections give proposals to gathering non-volatile and volatile OS data, separately. Third subsection talks about specialized issues that can block the accumulation of information. **First subsection : Collecting OS Data** Unstable OS information including an occasion can be gathered just from a live framework that has not been rebooted or closed down since the occasion happened. Each activity performed on the framework, regardless of whether started by an individual or by the OS itself, will more likely than not change the unstable OS information somehow or another. Along these lines, experts ought to choose as fast as conceivable whether the unpredictable OS information ought to be safeguarded. Preferably, the criteria for settling on this choice ought to have been recorded ahead of time with the goal that the examiner can settle on the best choice right away. The significance of this choice can't be focused on enough, on the grounds that driving off the framework or notwithstanding disengaging it from a system can wipe out the chance to gather conceivably imperative data. For instance, if a client as of late ran encryption instruments to verify information, the PC's RAM may contain secret word hashes, which could be utilized to decide the passwords. Then again, gathering unstable OS information from a running PC has characteristic dangers. For example, the likelihood dependably exists that records on the PC may change and other unpredictable OS information may be modified. What's more, a malevolent gathering may have introduced rootkits intended to return false data, erase records, or perform different malignant acts. In choosing whether to gather unstable information, the dangers related with such accumulation ought to be weighed against the potential for recouping essential data. As noted in subsection 4.3.2, if proof might be required, the examiner ought to completely record what is seen on the screen before contacting the framework. On the off chance that a live framework is in rest mode or has unmistakable secret phrase assurance, examiners ought to likewise choose whether to change the condition of the framework by waking it from rest mode or endeavoring to split or sidestep the secret key security with the goal that investigators can endeavor to gather unpredictable information. On the off chance that the exertion expected to gather the unpredictable information isn't justified, examiners may rather choose to play out a shutdown, as depicted in subsection 4.5.2. Forensic Tool Preparation part depicts how measurable devices ought to be accumulated in anticipation of gathering unpredictable OS information. Next, subsection 4.5.2 examines a few sorts of information and notices classifications of apparatuses or explicit OS devices that are viable in gathering each kind of information. At last, subsection 4.5.2 discloses the need to distinguish the sorts of unstable OS information that are well on the way to be significant in a specific circumstance and after that to organize the accumulation of information dependent on significance and relative unpredictability. **Types of Volatile OS Data.**

The accompanying rundown demonstrates a few kinds of unstable OS information and clarifies how measurable instruments can be utilized in gathering each sort of information:

• **Contents of Memory**. There are a few utilities that can duplicate the substance of RAM to an information record and aid ensuing examination of the information. On most frameworks, it is beyond the realm of imagination to expect to maintain a strategic distance from modification of RAM when running a utility that endeavors to make a duplicate of RAM. Rather, the objective is to play out the replicating with as little an impression as conceivable to limit the interruption of RAM.

• **Network Configuration**. Most OSs incorporates an utility that shows the present system setup, for example, **ifconfig**on UNIX frameworks and **ipconfig** on Windows frameworks. Data that can be given through system arrangement utilities incorporates the hostname, the physical and legitimate system interfaces, and design data for every interface (e.g., IP address, Media Access Control [MAC] address, current status).

• **Network Connections**. OSs regularly gives a strategy to showing a rundown of the present system associations. The two Windows and UNIX-based frameworks as a rule incorporate the **netstat** program, which records arrange associations by source and goal IP locations and ports, and furthermore records which ports are open on each interface.68 Third-party utilities are accessible that can show port assignments for each program. Most OSs likewise can show a rundown of remotely mounted filesystems, which gives more point by point data than a system association list. Subsection 4.6.2 gives extra data about social affair arrange association data.

• **Running Processes**. All UNIX-based frameworks offer the **ps** direction for showing at present running procedures. In spite of the fact that Windows offers a graphical UI (GUI) – based procedure list utility, the Task Manager, it is generally desirable over have a content based posting. Outsider utilities can be utilized to produce a content rundown of running procedures for Windows frameworks.

• **Open Files**. All UNIX-based frameworks offer the **lsof**direction for showing a rundown of open documents. Outsider utilities can be utilized to create content arrangements of open documents for Windows frameworks.

• **Login Sessions**. Some OSs have worked in directions for posting the presently signed on clients, for example, the w order for UNIX frameworks, which likewise records the source address of every client and when the client signed onto the framework. Outsider utilities are accessible that can list at present associated clients on Windows frameworks.

• **Operating System Time**. There are a few utilities accessible for recovering the present framework time, time zone data, and sunlight reserve funds time settings. On UNIX frameworks, **the date order** can be utilized to recover this data. On Windows frameworks, **the date**, **time**, and **nlsinfo** directions can be utilized altogether to recover this data.

Notwithstanding the instruments in the first show, usually helpful to incorporate some broadly useful apparatuses in the criminological toolbox, for example, the accompanying:
• **OS Command Prompt**. This utility gives an OS direction brief through which different instruments in the toolbox can be executed, for example, **cmd** on Windows frameworks.

• **SHA-1 Checksum**. A utility that can process the SHA-1 message overview of information records is useful in document confirmation. It might likewise be valuable to incorporate into the toolbox a rundown of SHA-1 message summaries for framework information documents related with the objective OS to aid record check. Utilities are accessible for different OSs for this purpose.

• **Directory List**. A utility for posting the substance of catalogs ought to be incorporated for exploring a filesystem and seeing its substance. For all intents and purposes all OSs incorporate such a utility; for instance, the ls order is utilized on UNIX frameworks, though on Windows frameworks, the **dir** direction is utilized.

• **String Search**. A utility for playing out a content string hunt can be helpful in recognizing information documents of intrigue. UNIX frameworks offer the grep order for performing content string looks, and an outsider grep utility is additionally accessible on Windows systems.

• **Text Editor**. A basic content tool can be valuable for review content documents or making notes. Various word processors are accessible, for example, Notepad on Windows frameworks and **vi** on UNIX frameworks.

Prioritizing Data Collection.

The kinds of unstable information that ought to be gathered with the toolbox rely upon the particular need. For example, if a system interruption is suspected, it may be helpful to gather arrange setup data, organize associations, login sessions, and running procedures to decide how somebody accessed a framework. In the event that an examination concerns wholesale fraud, at that point the substance of RAM, the rundown of running procedures, the rundown of open documents, arrange setup data, and system associations may uncover government managed savings and Visa numbers, programs used to get or scramble information, secret key hashes, and strategies that may have been utilized to get the data over a system. If all else fails, it is typically a smart thought to gather however much unpredictable information as could be expected in light of the fact that all chances to gather

Such information will be lost once the PC is shut down. Afterward, an assurance can be made with respect to which gathered unpredictable information ought to be inspected. A computerized content on a toolbox CD can be utilized for consistency in gathering unpredictable information. The content can incorporate approaches to exchange the gathered data to neighborhood stockpiling media, for example, a thumb drive, and to arrange drive areas.

Since unstable information has a penchant to change after some time, the request and practicality with which unpredictable information is gathered is imperative. By and large, experts should initially gather data on system associations and login sessions, since system associations may break or be separated and the rundown of clients associated with a framework at any single time may change. Unpredictable information that is more averse to change, for example, organize arrangement data, ought to be gathered later.

The suggested request in which unstable information for the most part ought to be gathered, from first to last, is as per the following:

1. Network associations
2. Login sessions
3. Contents of memory
4. Running procedures
5. Open documents
6. Network design
7. Operating framework time.

Second subsection : Collecting Non-Volatile OS Data

Subsequent to getting unpredictable OS information, examiners frequently should gather non-unstable OS information. To do as such, the examiner initially ought to choose whether the framework ought to be closed down. Closing down the framework not just influences the capacity to perform bit stream imaging and numerous consistent reinforcements, yet can likewise change which OS information is safeguarded. Most frameworks can be closed down through two strategies:

• **Perform a Graceful OS Shutdown**. Almost every OS offers a shutdown alternative. This makes the OS perform cleanup exercises, for example, shutting open records, erasing transitory documents, and potentially clearing the swap record, before closing down the framework. A smooth shutdown can likewise trigger evacuation of noxious material; for instance, memory-occupant rootkits may vanish, and Trojan steeds may expel proof of their malevolent movement. The OS is commonly closed down from the record of the head or the present client of the framework (if the present client has adequate benefits).

• **Remove Power from the System**. Disengaging the power string from the back of the PC (and evacuating the batteries on a PC or other versatile gadget) can safeguard swap records, transitory information documents, and other data that may be modified or erased amid a smooth shutdown.73 Unfortunately, an abrupt loss of intensity can make some OSs degenerate information, for example, open records. Also, for some buyer gadgets, for example, PDAs and PDAs, evacuating battery power can cause lost information.

• **Users and Groups**. Working frameworks keep up a rundown of clients and gatherings that approach the framework. On UNIX frameworks, clients and gatherings are recorded in/and so forth/passwd and/and so on/gatherings, individually. Also, the gatherings and clients directions can be utilized to recognize clients who have signed onto the framework and the gatherings to which they have a place. On Windows frameworks, the net client and net gathering directions can be utilized to specify the clients and gatherings on a framework.

• **Passwords**. Most OSs keep up secret word hashes for clients' passwords on circle. On Windows frameworks, outsider utilities can be utilized to dump secret word hashes from the Security Account Manager (SAM) database. On UNIX frameworks, secret key hashes are generally in the/and so forth/passwd or/and so forth/shadow document. As portrayed in subsection 4.4.3, secret word breaking projects can be utilized to remove passwords from their hashes.

• **Network Shares**. A framework may empower nearby assets to be shared over a system. On Windows frameworks, the SrvCheck utility can be utilized to list arrange shares. Third-party utilities can give comparative data to different OSs.

• **Logs**. Logs that are not put away in content records may require utilization of log extraction utilities. For instance, specific utilities can recover data about later effective and fizzled logon endeavors on Windows frameworks, which are put away in twofold arrangement logs. Most log sections on Unix frameworks are put away in content documents by syslog or in the/var/log registry, so exceptional utilities are not expected to procure data from the logs. Hunting down filenames finishing off with .log ought to recognize most log documents.

Third subsection : Technical Issues with Collecting Data

Specialized issues may likewise obstruct gathering of OS information. Section 4.4 depicts a few filesystem-related issues; this subsection centers around extra gathering issues and gives direction on what, in the event that anything, should be possible to moderate them. The expectation of this subsection isn't to give a thorough

	dialog of every single imaginable issue, however to give some fundamental data on basic ones. •OS Access. •Log Modification. •Hard Drives with Flash Memory. •Key Remapping.

Content Template	
Section Number	4.5.3
Section Title	Examining and Analyzing OS Data
Introduction	Data collected from operating systems will be helpful to provide guidance for analysis.
Content	Different apparatuses and strategies can be utilized to help the examination procedure. A significant number of the apparatuses and procedures are presented in subsection 4.4.3 for looking at gathered information documents can likewise be utilized with gathered OS information. Likewise, as mentioned in Section 4.7, security applications, for example, record honesty checkers and host IDSs, can be useful in distinguishing vindictive movement against OSs. For example, record honesty checkers can be utilized to process the message condensations of OS documents and analyze them against databases of realized message reviews to decide if any documents have been undermined. In the event that interruption location programming is introduced on the PC, it may contain logs that demonstrate the activities performed against the OS.

Content Template	
Section Number	4.5.4
Section Title	Reached Recommendations
Introduction	Data collected from operating systems will be helpful to provide guidance for analysis.
Content	The key recommendations exhibited in this subsection for utilizing information from OSs are as per the following. • **Analysts should act fittingly to save unpredictable OS information**. The criteria for deciding if unpredictable OS information must be protected ought to be recorded ahead of time with the goal that investigators can settle on educated choices as fast as would be prudent. To decide if the exertion required to gather unpredictable OS information is justified, the dangers related with such accumulation ought to be weighed against the potential for recouping essential data. • **Analysts should utilize a legal toolbox for gathering unpredictable OS information**. Utilization of a measurable toolbox empowers exact OS information to be gathered while limiting the unsettling influence to the framework and shielding the apparatuses from changes. The examiner should realize how each instrument is probably going to influence or change the framework amid gathering of information. • **Analysts ought to pick the suitable shutdown strategy for every framework**. Every technique for closing down a specific OS can make distinctive kinds of information be protected or defiled; experts ought to know about the ordinary shutdown conduct of every OS.

Content Template	
Section Number	4.6
Section Title	Using Data From Network Traffic
Introduction	This sections discusses the processing of wired and wireless networks traffic
Content	In this sub section we talk about the attacks of wired and wireless networks and how to resolve them. Email messages or sound could help specialist once gathered. Also, the sectiontalks about procedures for gathering information from these sources and brings up the potential legitimate and specialized issues in such information accumulation. The consequent sub section center around the strategies and apparatuses for inspecting and breaking down information from system traffic.

Content Template	
Section Number	4.6.1
Section Title	TCP/IP Basics
Introduction	This sections discusses the processing of wired and wireless networks traffic
Content	The TCP/IP convention is an alternate way to the Transmission Control Protocol/Internet Protocol. The Internet Protocol (IP) is the Internet convention that gives every gadget (device) a location to associate with the system and every gadget takes an alternate location from the remainder of the gadgets. IPV4 is a 32-bit segment, 4octets, and every octet is made out of 8 bits. The TCP (Transmission Communication Protocol): A correspondence convention that transmits information over a network. This TCP/IP convention is like the English language. It is the fundamental language for human correspondence on the planet. This convention is the principle convention for correspondence between various working frameworks. The TCP/IP convention gets its significance from having the capacity to associate a wide range of gadgets, organizes and working frameworks, The Internet was initially planned explicitly for the US Department of Defense (DOD) and afterward turned into the principle Internet convention. You ought to likewise realize that this convention comprises of numerous conventions.

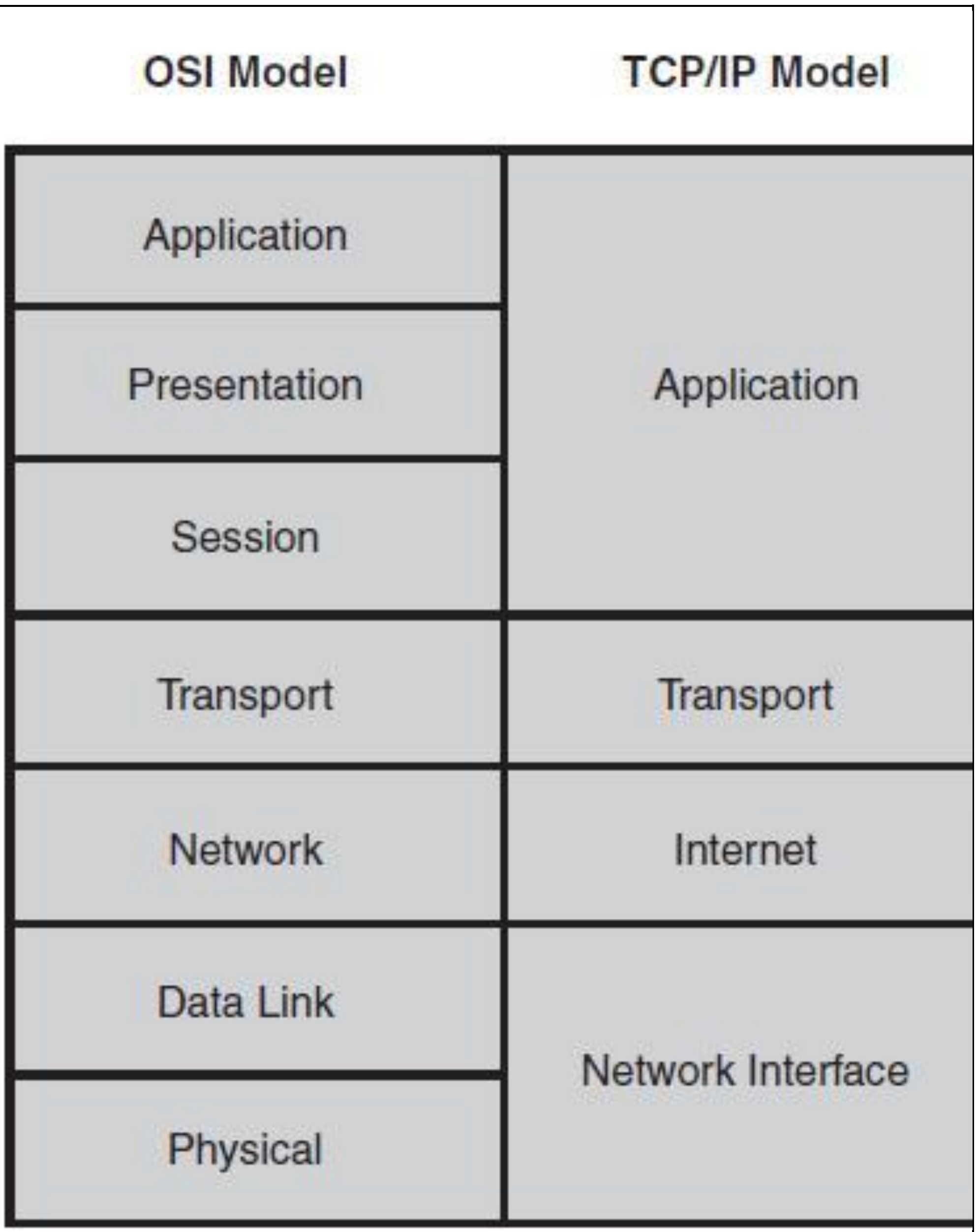


Figure 1: OSI vs TCP/IP layers (Source)

TCP/IP Layer comprises of four layers through which information passes; as shown in the figure above. In each layer a lot of conventions serve the capacity of this layer. For instance, in the application layer, a lot of administration conventions that assistance me to utilize certain projects, for example, **ftpm, smtp, rdp, pop3, http, dns.**

In the vehicle layer there are information exchange conventions **tcp, udp**.

In the Internet layer (or the supposed system layer in OSI), two IP conventions are utilized, which are utilized by numerous conventions (**icmp, igmp, arp, rarp**) and Nat convention, and their motivation is to build up correspondence with gadgets and systems.

At long last, the system interface layer works with a convention, for example, **mac, arp, IPSec**, the principal layer that manages the information sent to it by the other party and in this way the numbering began from it.

Content Template	
Section Number	4.6.2
Section Title	Network Traffic Data Sources
Introduction	This sections discusses the processing of wired and wireless networks traffic
Content	Numerous associations have information sources on the network that may contain valuable criminal proof. These sources gather critical information from the four TCP/IP layers. **First subsection : Firewall and Routers** A firewall is a gadget that organizations or associations spot to guarantee that their projects and records are shielded from interruption and robbery from outside gatherings. This gadget is explicitly situated between the interior system of the association and the Internet, with the goal that the unfortunate gatherings are distinguished and penetrated into the association's inner PC system and afterward educated by the chairman of the framework. The firewall isn't just used to give security against outside assaults, yet can be utilized to distinguish destinations that are not permitted to enter, including It merits referencing that there are numerous organizations that still don't utilize the firewall for staggering expense, or for their need specialists or authorities to manage them. A firewall can be a product or gadget that recognizes any hacking endeavors. It likewise demonstrates the nearness of infections that upset the task of the PC, which is a need that must be utilized to secure the PC system of the client, so as to avoid the spread of infections The switch sends and guides bundle parcels to collectors. Its principle task is to decide the best possible manner by which these bundles will be transmitted to the collector. Notwithstanding the points of interest and administrations we will gain from a couple of the significant organizations in the assembling of switches are Cisco and Juniper organizations and to contemplate the testaments of these organizations This product has names, for example, IOS and JUNOS. Numerous clients have a great deal of telecasters that call the ADSL modems they lease from or purchase from Internet specialist co-ops - they consider it a switch and this is totally off-base. These gadgets are just modem that changes over the information from advanced to simple computerized to simple however these gadgets don't The essential capacity of the switch is to manage parcels to the right ways. **Second subsection: Packet Sniffers and Protocol Analyzers.** System Sniffer is a product apparatus, considered the Network Sniffer that screens or tracks information streaming over constant system associations. This product instrument is either an independent program or a gadget that contains the fitting programming or firmware. System clients take fast duplicates of information that streams over the system without being diverted or changed. A few gadgets just work with TCP/IP bundles, yet the more complex devices work with numerous other system conventions and lower levels, including Ethernet outlines. **Third subsection: Intrusion Detection Systems.** Interruption Detection System is a mix of equipment and programming that screens property and offices for any pernicious exercises, unlawful or constrained passage or strategy infringement and after that sends reports to the administration focus.

Interruption Detection System arrives in an assortment of setups and methodologies, and its objective is to identify any suspicious development. There is a system based interruption discovery framework and host-based interruption identification frameworks. A few frameworks may endeavor to stop the interruption endeavor however this isn't required and isn't normal from the checking framework. Interruption location frameworks typically record data about critical occasions, advise security and detailing authorities.

Fourth subsection: Remote Access

Remote access is valuable if:

1. The need to enter the system and get a few information while voyaging or being far from the system.
2. Temporary or discontinuous utilization of system assets.

All in all, remote access frameworks utilize one of the accompanying conventions to accomplish network:

1. Serial Line Internet Protocol (SLIP).
2. Point-to-Point Protocol (PPP).

The SLIP convention is a standard used to address interchanges utilizing TCP/IP over sequential lines (for more data, if you don't mind sit tight for a convention exercise). It enables the client to remotely get to the Internet through his neighborhood organize.

The PPP convention is intended to be an advancement of the past SLIP convention. Since the SLIP convention is just utilized in TCP/IP bolster interchanges, the PPP convention can deal with multi-convention systems.

PPP is currently the favored decision for remote access as a result of its speed and unwavering quality.

Fifth subsection: Security Event Management (SEM) Software.

Security Information System and Event Management SIEM consolidates two frameworks, the first SIM framework data security the board framework, the second SEM framework security occasion the executives framework.

SIEM is a strategy and instruments for the administration of data security in the association, which looks to give a thorough perspective on all occasions in the composed system. The essential rule of the SEM framework is to gather the association's security information in a solitary framework that makes it simple for the director to screen security occasions and to distinguish irregular examples and occasions.

The SEM framework breaks down the data in record time and advises the individual in charge of checking the security occasions to make cautious move rapidly. The SIM framework gathers information in a bound together information room, recovers and examines long haul information, for instance, gathering information inside a year or a half year and giving reports - naturally - to help the association in consistence. In these frameworks, the SIEM framework was made to give examination and recovery of security occasions. The framework enables consistence supervisors to guarantee that the association meets the lawful consistence prerequisites of the association or a consistence endorsement.

Sixth subsection: Network Forensic Analysis Tools.

Legal Network Analysis Tools (NFAT) regularly gives a similar usefulness as parcel sniffer, convention analyzers, and SEM programs in a solitary item. While the SEM program centers around connecting occasions between current information sources (normally including a few system traffic sources), NFAT centers fundamentally around gathering, testing and dissecting system traffic. NFAT likewise gives extra highlights that encourage further system legal sciences, for example, revamping occasions by restarting system traffic inside the apparatus and picturing traffic streams and host connections.

Seventh subsection: Other Sources.

Most of associations have different wellsprings of system traffic data, for example,

- Dynamic Host Configuration Protocol Servers.
- Network Monitoring Software.
- Internet Service Provider Records.
- Client/Server Applications.
- Hosts' Network Configurations and Connections.

Content Template	
Section Number	4.6.3
Section Title	Collecting Network Traffic Data
Introduction	This sections discusses the processing of wired and wireless networks traffic
Content	Many specialized and legitimate issues that may confuse information accumulation: • Legal Considerations: Collecting system traffic can present legitimate issues. • Technical Issues: Many issues, for example, – Data Storage. – Encrypted Traffic. – Services Running on Unexpected Ports. – Alternate Access Points. That could cause Monitoring Failures.

Content Template	
Section Number	4.6.4
Section Title	Examining and Analyzing Network Traffic Data
Introduction	This sections discusses the processing of wired and wireless networks traffic
Content	This subsection concentrates on the fundamental strides of the examination and investigation procedures and features some noteworthy specialized issues that experts ought to consider. **First subsection: Identify an Event of Interest.** Distinguishing even of enthusiasm through one of two techniques: Someone inside the association or amid an audit of security occasion information. **Second subsection: Examine Data Sources.** Experts may likewise need to look at auxiliary system traffic information sources, for example, have based firewall logs and parcel catches, and non-organize traffic information sources, for example, have OS review logs and antivirus programming logs. The most widely recognized explanations behind doing this are as per the following: •No Data on Primary Sources. •Insufficient or Invalidated Data on Primary Sources. •Best Source of Data Elsewhere. **Data Source Value.** Associations regularly have a wide range of wellsprings of system traffic information. Since the data gathered by these sources shifts, the sources may have distinctive incentive to the expert, both all in all and for explicit cases. The accompanying things depict the average estimation of the most widely recognized information sources in system crime scene investigation: •IDS Software. •NFAT Software. •Firewalls, Routers, Proxy Servers, and Remote Access Servers. •DHCP Servers. •Packet Sniffers. •Network Monitoring. •ISP Records. **Examination and Analysis Tools.** Since system crime scene investigation can be performed for some reasons with many information source types, examiners may utilize a few distinct apparatuses all the time, each appropriate to specific circumstance. Investigators ought to know about the conceivable ways to deal with looking at and breaking down system traffic information and should choose the best apparatuses for each case, as opposed to applying a similar instrument to each circumstance. Examiners ought to likewise be aware of the inadequacies of apparatuses; for instance, a specific convention analyzer probably won't most likely decipher a specific convention or handle unforeseen convention information (e.g., unlawful information field esteem). It very well may be useful to have a substitute instrument accessible that probably won't have a similar insufficiency. **Third subsection: Draw Conclusions.**

A standout amongst the most testing parts of system legal sciences is that the accessible information is regularly not complete. As a rule, if not most, some system traffic information has not been recorded and thus has been lost. By and large, investigators should think about the examination procedure as a deliberate methodology that creates ends dependent on the information that is accessible and suppositions in regards to the missing information (which ought to be founded on specialized learning and ability). In spite of the fact that experts ought to endeavor to find and inspect every accessible datum with respect to an occasion, this isn't commonsense at times, especially when there are numerous repetitive information sources. The expert ought to inevitably find, approve, and dissect enough information to have the capacity to reproduce the occasion, comprehend its noteworthiness, and decide its effect. As a rule, extra information is accessible from sources other than system traffic– related sources (e.g., information documents or host OSs). Section 4.8 gives instances of how investigation can connect this other information with information from system traffic to get a progressively precise and exhaustive perspective on what happened.

Fourth subsection: Attacker Identification.

While examining most assaults, distinguishing the aggressor isn't a quick, essential concern: guaranteeing that the assault is ceased and recuperating frameworks and information are the principle interests. On the off chance that an assault is progressing, for example, an all-inclusive forswearing of administration assault, associations should need to distinguish the IP address utilized by the assailant with the goal that the assault can be ceased. Sadly, this is regularly not as basic as it sounds. The accompanying things clarify potential issues including the IP delivers obviously used to direct an assault:

Mock IP Addresses. Numerous assaults use parodied IP addresses. Mocking is unquestionably progressively hard to perform effectively for assaults that expect associations with be set up, so it is most generally utilized in situations where associations are not needed.111 When parcels are parodied, as a rule the aggressor has no enthusiasm for seeing the reaction. This isn't in every case genuine—aggressors could parody a location from a subnet that they screen, with the goal that when the reaction goes to that framework, they can sniff it from the system. Now and again caricaturing happens unintentionally, for example, an assailant misconfiguring an apparatus and inadvertently utilizing inner NAT addresses. Here and there an aggressor parodies a specific location deliberately—for instance, the satirize address may be the genuine expected focus of the assault, and the association seeing the action may just be a mediator.

- Many Source IP Addresses.
- Validity of the IP Address.
- Contact the IP Address Owner
- Send Network Traffic to the IP Address.
- Seek ISP Assistance.
- Research the History of the IP Address.
- Look for Clues in Application Content.

Content Template	
Section Number	4.6.5
Section Title	Reached Recommendations
Introduction	This sections discusses the processing of wired and wireless networks traffic
Content	Key suggestions exhibited in this subsection for utilizing information from system traffic are as per the following: • Organizations ought to have approaches with respect to protection and delicate data • Organizations ought to give satisfactory capacity to arrange activity– related logs. • Organizations ought to design information sources to improve the accumulation of data. • Analysts should have sensibly far reaching specialized learning. • Analysts ought to consider the devotion and estimation of every datum source. • Analysts ought to for the most part center around the qualities and effect of the occasion.

Content Template	
Section Number	4.7
Section Title	Using Data from Applications
Introduction	The application covers two aspects: applications design and collecting, examining, and analyzing application data.
Content	This section portrays application designs notwithstanding gathering, looking at, and examining application information. **Application Components** All applications contain code notwithstanding the accompanying segments: arrangement settings, confirmation, logs, information, and supporting documents: • **Configuration Settings**: Most applications enable clients or executives to redo certain parts of the application's conduct by modifying design settings. Setup settings might be put away in a few different ways, including the accompanying: – Configuration File. – Runtime Options. – Added to Source Code. • **Authentication**: Common validation strategies incorporate the accompanying: – External Authentication. – Proprietary Authentication. – Pass-Through Authentication. – Host/User Environment. • **Logs**: Although a few applications (essentially exceptionally basic ones) don't record any data to logs, most applications compose log sections to working frameworks explicit documents. Regular sorts of log sections are as per the following: – Event. – Audit. – Error. – Installation. – Debugging. • **Data**: Nearly every application is explicitly intended to deal with information in at least one different ways; application information regularly dwells briefly in memory, and incidentally or forever in documents. The configuration of a record containing application information might be nonexclusive (e.g., content documents, bitmap illustrations) or exclusive. Information may likewise be put away in databases, which are exceedingly organized accumulations of records and information determinations. A few applications make brief records amid a session, which may contain application information. In the event that an application neglects to close down effortlessly, it might leave brief records on media. Applications may likewise contain information record layouts and test information records (e.g., databases, reports). • **Supporting Files**: Types of supporting records incorporate the accompanying: – Documentation. – Links. – Graphics.

	• **Application Architecture**: Most applications are intended to tail one of three noteworthy application engineering classes, as pursues: – Local. – Client/Server. – Peer-to-Peer. **Types of Applications** The application covers two aspects: applications design and collecting, examining, and analyzing application data. Applications can usage of document, file sharing, web usage, e-mail, data concealment tools, or interactive communications. **Collecting Application Data** This class of application incorporates volatile OS, network traffic, and filesystems. **Examining and Analyzing Application Data** Examining and analyzing application data to a great extent comprises of seeing explicit segments of use data (filesystems, data of volatile OS, and traffic of network) utilizing the apparatuses and methods as already mentioned. Another conceivable issue in examination includes utilization of use - based security controls, such as data/information encryption and passwords. Numerous applications utilize such security controls. **Reached Recommendations** We mention here the key suggestions for utilizing information from applications are as per the following: • Analysts should consider all conceivable application information sources. Analysts ought to unite application information from different sources.

Content Template	
Section Number	4.8
Section Title	Using Data from Multiple Sources
Introduction	Other sources that could be considered are presented in this section.
Content	Two instances are presented here of the utilization of different information sources amid computerized crime scene investigation: • Determining which worm has contaminated a framework and recognizing the worm's attributes • Reconstructing the arrangement of digital occasions including an undermining email. **Suspected Network Service Worm Infection** The interruption identification investigator's underlying theory is that a worm may have assaulted a powerless system administration and contaminated the server, which is presently endeavoring to taint different frameworks. On the off chance that a brought together wellspring of information isn't accessible, the handler should check singular potential wellsprings of assault attributes, for example, the accompanying: •Network IDS. •Network-Based Firewall. •Host IDS and Firewall. •Antivirus Software. •Application Logs. To accumulate more data, the investigator can look at the contamination through the accompanying techniques: •Current State of the Host. •Host's Network Activity. **Threatening E-mail** The email ought to be examined and checked on; subsequent to inspecting the header, the episode handler ought to next assemble more data about the sending of the email. The header should list the IP address and the email customer utilized by the sender; the episode handler ought to figure out which have was utilizing that IP address at the time the email was sent. There are three conceivable outcomes for the IP address: •Local E-mail Client. •Server-Based E-mail Client. •Spoofed. **Reached Recommendations** The key suggestions in this subsection for utilizing data from different sources are as per the following: • Analysts can deal with numerous circumstances most viably by examining a few individual information sources and afterward corresponding occasions among them. Organizations ought to know about the specialized and strategic unpredictability of investigation.

Activity Template

Number 4.1

Title Applied Policies

Type

Aim ILOs: 3
The activity aims to expose the students to policies.

Description **Section 4.2:**
It is important for companies to formally establish and publish their policies regarding forensic investigations:
(a) Give 4 aspects or areas where these polices should addressed; (b) Give 4 benefits that the company can get establishing these.

Timeline Time: 1-3 hours.

Assessment Each student should submit one page containing his/her findings.

Answer A. Four aspects or areas where these polices should addressed:
1. Record Management Policy
2. Security Guidance
3. Digital Preservation Policy
4. ICT Acceptable Use Policy
B. Four benefits that the company can get establishing these:
1. Maintenance and monitoring of the log files
2. Authorization to provide forensic evidence
3. Digital evidence must be stored and handled securely.
4. Disciplinary issues: negligence, malpractice, abuse of acceptable use policy, grievance procedures.

Activity Template

Number 4.2

Title Using data from Operation Systems

Type

Aim ILOs: 2
The activity aims to digital forensics when mobile and digital devices are used.

Description **Section 4.3:**
Cell phones and mobile devices have often been used in committing crimes. Find the main concerns in the search and seizure procedures for cell phones and mobile devices? Give reasons for these concerns. Define any term you use as well.

Timeline Time: 1-2 hours of reading.

Assessment Each student is required to submit a one page report abouthis/her findings.

Answer What are the main concerns in the search and seizure procedures for cell phones and mobile devices? Give reasons for these concerns.

The main concerns with mobile devices are loss of power, synchronization with cloud services, and remote wiping.

Volatility refers to the memory or storage content loss when the power is switched off; this forms a big issue from a criminological perspective.
Reason: All mobile devices have volatile memory- Making sure they don't lose power before you can retrieve RAM data is critical.

Mobile device attached to a PC via a USB cable should be disconnected from the PC Immediately.
Reason: Helps prevent synchronization that might occur automatically and overwrite data

Activity Template

Number 4.3

Title Network Traffic Data Sources

Type

Aim ILOs: 5
The activity aims to investigate when Internet is used.

Description **Sections 4.4, 4.5, 4.6, 4.7, and 4.8:**
If you are going to investigate a case of an Internet abuse in an organization, what fundamental items do you require for conducting this investigation?

Timeline Time: 1-2 hours of reading.

Assessment Each student is required to submit a one page report about the fundamental items.

Answer To conduct an investigation involving Internet abuse, you need the following:

1. The organization’s Internet proxy server logs
2. Suspect computer’s IP address obtained from your organization’s network
3. Administrator
4. Suspect computer’s disk drive.
5. Your preferred digital forensics analysis tool (ProDiscover, Forensic Toolkit, EnCase,X-Ways Forensics, and so forth)

Think Template (MCQs)

Number	4.1
Title	Why Forensics? Which Staffing and What Other Teams?
Type	“Choose correct answer”
Question	“Which of the following is NOT an essential client category of criminological instruments and strategies inside the association?”
Answers	a) Investigators. b) Organization visitors. c) IT Professionals. d) Incident Handlers. **Answer: b**

Think Template (MCQs)

Number 4.2

Title Reached Recommendations

Type “Choose correct answer”

Question “Which of the following statements is WRONG?”

Answers a) Organizations ought to have a capacity to perform computer and network legal sciences.

b) Organizations ought to figure out which gatherings should deal with every part of crime scene investigation.

c) Few teams within an organization should participate in forensics.

d) Forensic contemplations ought to be unmistakably tended to in strategies.

Answer: c

Think Template (MCQs)

Number	4.3
Title	Data Collection
Type	“Choose correct answer”
Question	“What is the initial phase in the criminological procedure?”
Answers	a) Distinguish potential wellsprings of information and acquire information from them b) Hide the data securely in case you have to view it. c) Inform the press. d) Wait and control the processes.

Answer: a

Think Template (MCQs)

Number 4.4

Title OS Basics

Type “Choose correct answer”

Question “OS data exists in ….. .”

Answers a) Volatile state.
b) Non-volatile state.
c) Both volatile and non-volatile states.
d) Cannot be found.

Answer: c

Think Template (MCQs)

Number	4.5
Title	Network Traffic Data Sources
Type	“Choose correct answer”
Question	“The letter S in SLIP stands for ….. .”
Answers	a) Segmented.
	b) Straight.
	c) Super.
	d) Serial.

Answer: d

Extra Template

Number	From 4.1 to 4.8
Title	**Integrating techniques of forensic into response of incident; a guide**
Topic	• “4.1” • “4.2” • “4.3” • “4.4” • “4.5” • “4.6” • “4.7” • “4.8”
Type	“Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, *10*(14), 800-86.”

5. Ethical and Social issues in digital forensics

Scope Template

Number	5
Title	Ethical and Social issues in digital forensics
Introduction	This chapter explains the core concepts related to the role of ethics in digital forensics (DF). It starts by defining ethics andexploring some organizations provides legal and ethical principles for DF. Then, it highlights the ethical concerns related to computer information systems. Finally, it describes in details the most widely ethics and legal issues when performing DF.
Outcomes	Demonstrate high ethics in performing digital forensics. ILO1: Understand the ethical aspects related to information systems ILO2: Understand the ethical aspects related to digital forensics
Topics	7.1.The role of Ethics in Digital Forensics (DF) 7.2.The ethical concerns related to computer information systems 7.3.Ethics in performing digital forensics 7.3.1.Professional Ethics in Digital Forensics 7.3.2.Ethical Decision Making 7.3.3.Training for the Profession 7.3.4. Regulation of the Profession 7.3.5. Privacy and Confidentiality Issues 7.3.6. Legality of Digital Forensics Investigation Techniques

Study Guide

Task	**Time**
Preparation (Introduction and On-line Planning):	2 hrs
Textbook Content:	3 hrs
Thinking (On-line discussions, Review questions)	1 hr
Tutorial Work:	2 hrs
Related Course Work:	2 hrs
Total	**10 hours**

• Required study time: **4 one hour lectures.**
• Required external resources including links and books:
1. Guide to the CISSP CBK: 3rd Ed. Steven Hernandez (Ed.). New York: Auerbach Publications, 2012.
2. A chapter contributed by Rebecca Herold, setting forth the history of "computer ethics" http://www.infosectoday.com/Articles/Intro_Computer_Ethics.htm)

Additional References:

• Kubitschke, L., Gareis, K., Lull, F. & Müller, S. (2009). ICT & Ageing: Users, markets and technologies: compilation report on ethical issues, unpublished report.

• Nelson, Phillips, & Steuart (2010). Guide to computer forensics and investigations. (p. 508). Course Technology Ptr.

• Guide to the CISSP CBK: 3rd Ed. Steven Hernandez (Ed.). New York: Auerbach Publications, 2012.

• Garrigou-Lagrange, R. (1991). The three ages of the interior life: Prelude of eternal life. (Vol. 2). Charlotte, NC: Tan Books Publishers Inc.

• Cf. Harvard College v. Armory, 9 Pick. (26 Mass.) 446 (Mass. 1830).

- Gilbert Whittemore, Report to the House of Delegates, 2008 A.B.A. Sec. Sci. & Tech. L. 2.

- The Volgenau School of Information Technology and Engineering of the George Mason University Department of Electrical and Computer Engineering offers a class entitled, "Legal and Ethical Issues in Computer Forensics."

- Jerry Wegman, Computer Forensics: Admissibility of Evidence in Criminal Cases, 8 J. Legal Ethical & Reg. Issues 1, 2 (2005) (explaining the evolution of digital forensic experts and the legal challenges they face).

- Code of Ethics and Professional Responsibility, Int'l Soc'y of Forensic Computer Examiners, http://www.isfce.com/ethics2.htm.

- Hickman v. Taylor, 329 U.S. 495 (1947).

- Fed. R. Civ. P. 26 (b)(3)(B); see also In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1014 (1st Cir. 1988).

- Fed. R. Civ. P. 26(b)(4)(C).

- Fisher v. United States, 425 U.S. 391, 403 (1976).

- United States v. El Paso Co., 682 F.2d 530, 538 n.9 (5th Cir. 1982) (quoting 8 J. Wigmore, Evidence § 2292 (McNaughton rev. 1961)); Restatement (Third) of the Law Governing Lawyers § 68 (2000).

- Hutchinson v. People, 742 P.2d 875, 881 (Colo. 1987).

- Model Rules of Prof'l Conduct R. 1.6 (1983). Other professionals, such as accountants, are governed by similar rules. See Minn. Stat. §§ 326A.12–A.13 (2010) (discussing confidential communications, working papers, and clients' records).

- Model Rules of Prof'l Conduct R. 1.18 (1983).

- Model Rules of Prof'l Conduct R. 1.9 (1983).

- Nelson, et al., supra Note 10, at 523 ("Your only agenda should be finding the truth, so don't think in terms of catching somebody or proving something. It's not your job to win the case. Don't become an advocate.")

- Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009 2 (2009), http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf (last retrieved March 17, 2019).

- Mack Sperling, North Carolina May Require Licensing for Computer Forensic Consultants, but Do We Need It?, N.C. Bus. Litig. Rep. (Sept. 24, 2008), http://www.ncbusinesslitigationreport.com/2008/09/articles/discovery-1/north-carolina-may-require-licensing-for-computer-forensic-consultants-but-do-we-need-it/ (last retrieved March 19, 2019).

- S. 584, 2009 Gen. Assemb., Reg. Sess. (N.C. 2009), available athttp://ncleg.net/Sessions/2009/FiscalNotes/Senate/PDF/SFN0584v3.pdf (last retrieved Feb 3, 2019).

- Whittemore, supra note 29, at 14.

- See, e.g.,Marshall Tanick, The Privacy Paradox, 65 Bench & Bar Minn. 8 (Sept., 2008) (discussing privacy and investigative issues, and collecting cases).

- See, e.g., U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 500 (1994) ("An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."); United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

- 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'").
-

Content Template

Section Number 7.1

Section Title The role of Ethics in Digital Forensics (DF)

Introduction This section introduce some concepts related to the role of ethics in digital forensics (DF). It starts by defining ethics, and then it explores some organizations provides legal and ethical principles for DF.

Upon completion of this section the student will be able to:

- Have clear understanding of the role of ethics in digital forensics.

Content Ethics are sets of rules used to measure and test the performance of digital forensics (DF) examiners. The standard name for the term ethics in DF is "codes of conduct or responsibility." The field of Digital Forensics requires a well-balanced combination of technical skills, legal aspects, and ethical conduct.

When the investigation case starts at the court, the forensics analyst can have two roles to give testimony, the first role is expert witness who share his/her opinion with regards of what he/she observe, collect or found. The second role is technical witness who provide facts that he/she found during the investigation.

There is currently no universal standard used by computer digital forensics analyst to follow, but efforts have already been made to provide legal and ethical principles to help DF analyst during their investigation.

The following organizations provides the most widely used legal and ethical principles for DF.

- U.S. Department of Defense
- The Computer Fraud and Abuse Act (CFAA)
- Federal Rules of Evidence
- FBI Computer Analysis and Response Team (CART)
- The International Organization for Standardization (ISO)

Moreover, different organizations start providing certifications on various aspects of DF. These organizations designed and developed their own code of ethics, since there is no universal standard to follow as we have already mentioned.

- International Association of Computer Investigative Specialists (IACIS)
- International Society of Forensics Computer Examiner (ISFCE)
- Global Information Assurance Certification (GIAC)
- (ISC) 2 Code of Ethics
- International High Technology Crime Investigation Association (HTCIA)

Content Template	
Section Number	7.2
Section Title	The ethical concerns related to Computer Information Systems
Introduction	This section presents issues raised from the development and implementation of computer information systems. Upon completion of this section the student will be able to: • Have a clear understanding of technical, social, and legalissues related to computer information systems
Content	There are many issues raised from the development and implementation of computer information systems, these issues can be filtered under three main categories: Technical, social, and legal. Below are the main concerns. 1. **Privacy and Confidentiality** The terms privacy and confidentiality are commonly used interchangeability. These terms are related together but they are not identical. Privacy refers to the ability of individual or groups to seclude themselves or the information about themselves. This can be achieved by having the right to control access and ensuring all doors are closed during physical examination. Confidentiality is not like privacy that applies to individual (person) or group; it applies and relates to the information itself. Participants privacy is an important aspect for deploying any information system, so when procedures and policies that insures confidentiality of sensitive and non-sensitive data are not put into place, such data became available for unauthorized access by third party, where the data are flow through the information system which helps in the process of decision making for individual and organizations. Therefore, breaking these data and gaining access to it will lead to computer incidents including data breaches, identity crimes, and infringing intellectual property. 2. **Repudiation and Obfuscation** Obfuscation is the practice of making things difficult to understand. Programmers encrypt some or all the code by renaming useful class names and variables to meaningless labels, on the other hand, they add sometimes also meaningless code. Making the code Obfuscate will prevent attackers from reverse engineering the application or program. Repudiation refers to the ability of an individual or a group of people to deny that they performed a specific action or transaction. While assuring that the anonymity for individuals and employees working in organizations is an important issue, it is unknown how organizations will prevent damages and attacks resulting from anonymous user's inputs and actions. As a result, it is recommended that organizations must edit their information systems to breach the anonymity of their employees to certain aspects that allow them to identify or detect individuals to which certain inputs are attributed. 3. **Accuracy and Efficiency** Information systems store huge amount of data related to its staff and customers including work activities and processes. This data is used to identify and predict future behaviors that helps in extracting useful information. However, the accuracy of information systems can open a technical issue, whichindicates that an information system is only accurate, if the data stored and fed on it in correct and the intelligence

of its developer in designing and implementing a bug free system, where development and runtimes bugs are identified as a result of several trails before deployment.

To conclude, organizations must fix error and bugs on their information system as soon as they detect them. As a result, it is important that the information system itself must not deployed until several exhausted tests and bug free scan gone through, in order to only provide accurate results and information to support organization decision-making process.

4. **Replacement and Reduction**

Replacing traditional manual work procedures with a computerize information system is a high demand, since all Information systems have large processing capabilities that can perform fast decision making processes and produce more accurate results than manual mechanisms. On the other hand, obsoleting the manual mechanisms will render human employees surplus to such organizations requirements [1]. As a result, organizations must not directly shift their jobs to an automated computerize information system, they should try to automate jobs with the need of human involvement, due to the fact that countries around the word have an issue with regards of high unemployment rate. Thus, it is difficult to decide what to follow; automate the whole process by an information system that will maximum the organization turnover and make it more cost efficient for long-term success or on the other hand, keeping workface engagement.

5. **Manipulation and Falsification**

Unlike traditional manual mechanisms, the use of Information system allows us to have access to various types of data and documents created by a variety of users. The easy use of data manipulation techniques using information system will reproduce data to fit everyone’s need. Illegal use of data manipulation techniques by unauthorized parties or users need to be detected, where this action is identified as criminal falsifications. Detecting criminal and immoral manipulation(falsification) is a challenging task since perpetrators always find new ways to process unethical falsification on data and documents.

Therefore, the issue is to decide whether to make the manipulations techniques provided by the information systems to only specific selected users or to allow the use of manipulations techniques while trying to find ways that help in detecting criminal falsification.

To conclude, computer information systems and digital Forensics systems are classified quite similar to each other’s, but there are still some features, which extend digital forensic from the standard information systems. In the next section, we will highlight the current issues and challenges arising when performing digital forensics.

Content Template

Section Number	7.3
Section Title	Ethics in performing digital forensics
Introduction	This section describes in details the most widely ethical and legal issues when performing DF Upon completion of this section the student will be able to: • Have a clear understanding of technical, social, and legalissues when performing DF.
Content	Digital forensics examiners are facing ethical issues, becausethey have full privilege and access to computer information systems and data, while their services are always engaged incidents to controversies. In fact, examiners are not well prepared to solve these ethical dilemmas. This is due to several reasons including lack of industrial standards and regulations, a few coverage of ethics in training materials and curriculum, and the law applied to control DF is not well settled. As a result, what is needed is a combination of a well understanding evolved DF law, draft engagement contract, and a continuous ethical training.

Content Template

Section Number 7.3.1

Section Title Professional Ethics in Digital Forensics

Introduction // same as above

Content Due to the rapid development and evolution of computer information systems and the novel capabilities to store and save data. A new field of expertise has arisen like "Ethical Hacking" and "Cloud Forensics", which all added to the huge demand of specialized and well-trained DF examiners. The rapid development of computer information systems has given rise to controversies regarding intellectual property rights, privacy and confidentiality rights, and the public welfare. Although some of these controversies should somehow addressed by the contract, others are novel and need to be addressed and solved by courts of law. Furthermore, civil and criminal laws have failed to be up-to-date with technological trends, so several organizations adopted certified programs for code of professional in ethics to provide examiners and trainers with the necessary skills to avoid and decrease liabilities. As a result, the code of professional ethics will provide a foundation, a base, and clear principles that can be objectively measured during decision marking. The code can help and serve other important interests like the image and credibility of the organization including its profession, eliminating unfair competition, and fostering cooperation among professionals [2].

The code of ethics is designed to create a standard of acceptable conduct of all activities done by examiners within the profession. Some of these activities are: interactions with customers, government authorities, research and data collection, analysis of evidences, testing using hardware and software tools, consultation and advising, report writing, and continuous education [3].

Although the code of professionalism is not a law, conducting violations will harm others and may expose examiners to criminal liabilities or other consequences. Moreover, conduct in violation or ethical decision making that does not follow the code of ethics may end of distrusts of the examiner, where reputation is the examiner most important asset.

Content Template

Section Number 7.3.2

Section Title Ethical Decision Making

Introduction // same as above

Content Ethical decision marking is performed by a combination of law and ethics, where the management of ethical issues is the behavior component about what legal and ethical obligations are mainly concerned. Moreover, an issue cannot be management without classifying or categorizing it. For that reason, efficient and effective training for examiners about professional ethics will allow them to spot, classify and solve ethical issues.

An effective code of ethics consists not only on theoretical and static core principles, but it should also contains components that can be adapted by examiners over time to keep them within the law and professional ethics.

In order for the examiner to efficiently and effectively spot ethical issues, he/she must be familiar with the law and professional ethics that governs the digital and cyber forensic.

As a result, ethical decision marking in digital forensics work contains of honesty, prudence, and compliance with the law and professional ethics [3].

The first principle is honesty, which require a good moral character of the examiner, where ethical decisions cannot reliably and consistently be made without good moral. Moreover, it is widely believed that when the reward is high, it is more likely that the examiner will do the suitable thing. The honesty principle is a prerequisite for every participant or entrant in the profession.

The other two principles mentioned above prudence, and the compliance with the law and professional ethics are both equal and important as of the of honesty principle, where prudence means the ability to control and govern oneself by the use of reason and mind. Moreover, prudence is characterized as "right reason which . . . directs the acts of justice, fortitude, temperance, and the annexed virtues"[3]. As a result, prudence is usually coming with training and experience, where it is also a presumption incorporated into the code of ethics according to the law and professional ethics.

Content Template

Section Number 7.3.3

Section Title Ethics Training for the Profession

Introduction // same as above

Content Nowadays, most training and education in the field on digital forensics are mainly focused on technical aspects with less concentration on the significant legal and ethical challenges facing examiners. Therefore, it is important that most of digital forensics programs uniformly develop and implement ethics training on par with technical training. Moreover, new participants to the profession are required to help in demonstrating competencies with regards of digital forensics ethics (such as by written examination), otherwise digital forensics examiners will remain not well prepared to meet these legal and ethical issues [4]. Moreover, this issue has not gone without any notice by the courts:

"One survey of civil trials estimated that experts appear in 86% of the cases with an average of 3.8 experts per trial. While expert witnesses are appearing in civil cases in increasing numbers, the topic of expert witness ethics and professionalism is largely undeveloped and there are few definitive statements about what exactly the expert witness's ethical obligations are and how they are to handle the subtle as well as the more blatant attempts to influence them .... Even where professional associations have established ethical guidelines for conducting investigations, forming opinions, and writing reports, very few explain how the ethical boundaries imposed on judges and lawyers may bear on the performance of their role in the legal system regardless of whether they are employed as a retained forensic expert for one of the parties or as a court-appointed expert" [5].

Content Template	
Section Number	7.3.4
Section Title	Regulation of the Profession
Introduction	// same as above
Content	Several experts and researchers in the field of digital forensics who considered the codes of ethics suggests that they are insufficient at protecting the integrity of the profession. *"The problem with a field like computer forensics is the lack of universally accepted standards that anyone can view and at least have an idea of the level of competency of the expert. Other experts require some sort of professional licensing specific to their field: Certified public accountants, doctors, professional engineers, lawyers[,] etc.[,] where they have had to pass some sort of board certification prior to being allowed to practice. Of course it was not always that way for those professions in the early days, before such boards and licensing bodies were formed. And that is the state of computer forensics today" [6].* The American Bar Association (ABA) assumes that "investigation and expert testimony in computer forensics and network testing should be based upon the current state of science and technology, best practices in the industry, and knowledge, skills, and education of the expert" [7]. Moreover, since there are no standard licensing body in the United States for digital forces, all qualifications are determined by reputation standards, competency exams, and membership by certifying organizations. The membership requirement is designed in a way that it will reject unqualified applicant who did not meet the requirements for the codes of ethics. For example, the International Society of Forensic Computer Examiners (ISFCE) rejects all applications for applicants whom have criminal records as specified by the ISFCE for the reason that "An examiner with a criminal record may result in credibility issues in professional settings" [8], and therefore requires all applicants to submit a criminal background record for check. Some other entities as Texas Private Security Bureau requires applicants to pay an annual feesubject to criminal record check results, and evidences of training and work experience. As a results most of the courts in globally are adapted the ABA model rules, where lawyers are required to take ethical education annually includes passing a university course with regards of professional responsibilities in law schools [9].

Content Template	
Section Number	7.3.5
Section Title	Privacy and Confidentiality Issues
Introduction	// same as above
Content	Most digital forensics examiners work under the control of an attorney, where the attorney is responsible for finding a suitable examiner (investigator) for a specific case, and indirectly responsible for the examiner's code of conduct. The oft-overlooked inverse of that rule is that the all the ethical standards with regards of privacy and confidentiality that applies to the attorney who is responsible for hiring an examiner also applies to the examiner. These rulesgenerally fall under two categories: the work product doctrine, and the attorney-client privilege includingconfidentiality. 1. **Work Product Doctrine** Work product doctrine protects all related materialsfor a specific investigation case including written reports prepared in anticipation of litigation from discovery by opposing counsel. The doctrine enhances a lawyer's ability to render competent counsel, as the United States Supreme Court observed in *Hickman v. Taylor*: *"It is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories, and plan his strategy without undue and needless interference"* [10]. As a result, it is important for both the attorney and the examiner to understand all the requirements of the doctrine, and how it can be applied in digital forensics investigations. The doctrine can be applied in both civil and criminal cases, and protects not only documents and tangible evidences prepared by attorneys, but also those prepared by an attorney's "consultant or agent" [11]. In the context of such investigations, the work product doctrine also covers the "mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation" [11]. An intelligent expert should therefore, take positive rules to keep the confidentiality of the data including the software and hardware used during examination and investigation, as well as his or her processes, notes, tools, methods, and search queries. In 2010, Fed. R. Civ. P. Rule 26 was amended to give experts' draft reports the protection of the work product doctrine, exempting them from mandatory disclosure. The rule expressly provides that the doctrine apply to "protect drafts of any report or disclosure required under Rule 26(a) [(2)], regardless of the form in which the draft is recorded [11]. The amended rule also applies work product protection to any communications between experts and the counsel who retain them [11], with three exceptions [12]: 1) Communications pertaining to the expert's compensation; 2) Facts or data that the attorney provided and the expert considered in forming opinions; and 3) Assumptions that the attorney provided and that the expert relied on.

2. **Attorney-Client Privilege and Confidentiality**

The main function of this privilege is to:
"encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice" [3,13].

In general, communications and interaction are protected under the attorney-client privilege [14]:
1) a person is seeking legal advice from a lawyer acting in his legal capacity,
2) the communication is made for the purpose of obtaining legal advice,
3) the communication is made in confidence, and
4) the communication is made by the client.

And this can be applied to digital forensics examiners as follows:
"As both a legal and practical matter, the defense expert's relationship with the defendant and counsel has been protected from intrusions by the state. The law has recognized several doctrines that afford a degree of confidentiality to the expert-defense relationship. Thus, statements made to the expert by the defendant and counsel may be protected by the attorney-client privilege" [15].
Moreover, both the expert and the attorney would owe a duty to the client—the holder of the privilege—to maintain confidentiality. The attorney's obligation is detailed in the Model Rules of Professional Conduct in Rules 1.6 (governing disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client) [16], 1.18 (the lawyer's duties regarding information provided to the lawyer by a prospective client) [17], and 1.9 (the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client) [18]. However, the expert, who usually is not present at the time of the communication, is also responsible for protecting any information the expert discovers that implicates communications made by the client to his or her attorney. Furthermore, a competent digital forensics expert should also have good background and training with regards of information security procedures and protocols and be able to observe strict confidentiality of all data all types of data:

"Not all cases are shrouded in secrecy, but a fair proportion of them are. There are well known figures getting divorced, major companies with proprietary information at issue, public figures in the headlines, and people charged with felonies. . .. During the course of a major case where the expert has been identified, the press will undoubtedly come sniffing around the expert probing for information. A good expert knows the standard answer, "I'm sorry, I have no comment" and is as immoveable as the Great Wall of China" [19].

As a result, to protect confidentiality, the engagement contractbetween all parties should include a confidentiality clause, where any break of the contract rules will terminate it and the expert will be subject to the court's including sanctions.

Content Template	
Section Number	7.3.6
Section Title	Legality of Digital Forensics Investigation Techniques
Introduction	// same as above
Content	Another important factor for consideration by both attorneys and examiners in digital forensics examinations and investigations is the legality of investigation techniques. Consider, for example, whether an attorney or the examiner may take possession of a computer belonging to a husband, but seized by a wife in preparation for marital dissolution proceedings. If a court finds that the wife did not have equal dominion over the computer (i.e., if the computer, or some portion thereof, was password-protected by the husband, or belonged to the husband's employer), the taking of the computer for analysis might constitute a crime [20]. Likewise, evidence obtained from a key logger, spyware, or persistent cookies may violate state or federal law (e.g., the Electronic Communications Privacy Act). Moreover, certain types of "cyber sleuthing" or penetration testing may be unlawful under various countries statutes. For example, the Computer Fraud and Abuse Act, last amended in 2008, criminalizes anyone who commits, attempts to commit, or conspires to commit an offense under the Act.55 Offenses include knowingly accessing without authorization a protected computer (for delineated purposes) or intentionally accessing a computer without authorization (for separately delineated purposes). Even if prosecution seems unlikely, any evidence obtained by unlawful means is inadmissible under the exclusionary rule. Another area of legal concern "Big Data", and whether lawful datamining techniques done by investigators outside of the formal discovery procedures could lead to privacyviolation [21], where individuals must maintain privacy rights in data including reconstructed it through aggregation and inference [22]. As an example of that, technological applications and tools not available to the public are used to reveal the physical location of an internet user through IP address routing. Moreover, in some cases,the use of cookies (user browsing history profile) is a violation of the Electronic Communications Privacy Act [3, 23]. Lastly, another important consideration is the tricky issue of the cyber forensics examiner's interactions with prosecutors. One is the understanding and claim of a prosecutor "shopping" for an expert, or use of unqualified expert, which may constitute a violation of defendant's due process rights [3, 24] and may also be a violation of Rule 3.8 (Special Responsibilities of a Prosecutor) [3, 24]. The following interview selected from The Right to Expert Assistance in a Post-Daubert, Post-DNA World [25], illustrates this problem: *"Because two police crime laboratories would not declare a positive bootprint match in the infamous Rolando Cruz prosecution, prosecutors sought out a third expert, Dr. Louise Robbins, who declared a match. A detective, who resigned because he believed the wrong people had been charged, later observed: "The first lab guy says it's not the boot. . . We don't like that answer, so there's no paper [report]. We go to a second guy who used to do our lab. He says yes. So we write a report on Mr. Yes. Then Louise Robbins arrives. This is the boot, she says. That will be $10,000. So now we have evidence"* [26].

Activity Template

Number 7.1

Title Identify the role of ethics in digital forensics (DF).

Type Reflection

Aim The activity aims to let the student read more on the role of ethics in digital forensics (DF).

Description 7.1

Timeline Time: 1 hour of reading.

Assessment Each student is required to submit a one-page report of the role of ethics in digital forensics (DF), and then present it in the class as open discussion session.

Activity Template

Number 7.2

Title Describe in details the main concerns and issues raised from the development and implementation of computer information systems.

Type Reflection

Aim The activity aims to allow the student to have a hands-on experience on one of the main cellular network enabling technologies.

Description 7.2

Timeline Time: 1-2 hours of reading.

Assessment Each student is required to submit a one-page report of thesemain concerns and issues, and then present it in the class as open discussion session.

Activity Template

Number	7.3
Title	Explain the privacy and confidentiality issues related to digital forensic examination.
Type	Review
Aim	This activity aims to help developing the student skills in communicating technical forensic terms in non-technical manner.
Description	7.3.5
Timeline	Time: 1 hour
Assessment	The student will be assessed by their ability to explain the concept in non-technical terms.

Think Template (MCQs)

Number	7.1
Title	The role of Ethics in Digital Forensics (DF)
Type	Fill in the blanks
Question	____________ are sets of rules used to measure and test the performance of digital forensics (DF) examiners
Answers	a) Ethics b) privacy c) Issues. d) Confidentiality**.** **Answer: A**

Think Template (MCQs)

Number 7.2

Title The ethical concerns related to Computer Information Systems

Type Fill in the blanks

Question _________ is the practice of making things difficult to understand

Answers a) Obfuscation
b) Repudiation
c) Reduction
d) Replacement
Answer: A

Think Template (MCQs)

Number	7.3
Title	The ethical concerns related to Computer Information Systems
Type	Choose correct answer
Question	What is the type of action that illegal use data manipulation techniques by unauthorized parties.
Answers	a) Falsifications. b) Obfuscation. c) Manipulation. d) Reduction. **Answer: A**

Think Template (MCQs)

Number 7.4

Title Ethical Decision Making

Type Fill in the blanks

Question Ethical decision marking is performed by a combination of ___________ and ____________.

Answers a) Law, procedures.
b) Ethics, procedures
c) Law, Ethics.
Answer: C

Think Template (MCQs)

Number	7.5
Title	Ethics Training for the Profession
Type	Fill in the blanks
Question	Nowadays, most training and education in the field on digital forensics are mainly focused on_______
Answers	a) Technical aspects b) Theoretical aspects **Answer:** **A**

Extra Template
Number 1.1
Title Ethical aspects related to digital forensics
Topic 7.1 to 7.3.6
Type Guide to the CISSP CBK: 3rd Ed. Steven Hernandez (Ed.). New York: Auerbach Publications, 2012.
A chapter contributed by Rebecca Herold, setting forth the history of "computer ethics": http://www.infosectoday.com/Articles/Intro_Computer_Ethics.htm)