1.1 Introduction:

In today's interconnected world, where digital devices pervade تنتشر nearly every aspect of our personal and professional lives, the need for robust cybersecurity measures has never been more pronounced. As individuals and organizations increasingly rely on digital technologies to store, transmit, and process sensitive information, the risks associated with cybercrime, data breaches, and illicit digital activities النشاطات الرقمية الغير مشروعة have escalated exponentially ارفعت ضمنيا . In response to these evolving threats, the field of digital forensics has emerged as a critical discipline aimed at uncovering, analyzing, and mitigating cyber incidents and criminal activities perpetrated through digital means.

Digital forensics, often referred to as computer or cyber forensics, encompasses a broad range of investigative techniques and methodologies used to extract, preserve, and examine digital evidence from various electronic devices and digital media. From computers and smartphones to servers and cloud storage platforms, digital forensics practitioners employ specialized tools and methodologies to collect and analyze digital artifacts, such as files, emails, metadata, and network traffic, with the objective of reconstructing events, identifying perpetrators, and facilitating legal proceedings.

The scope of digital forensics extends beyond traditional crime investigation to encompass a myriad لا تعد ولا تحصى of applications across diverse domains, including law enforcement, corporate security, incident response, and litigation support (دعم الدعوى). In criminal investigations, digital forensics plays a pivotal role دور محوري in uncovering evidence of cybercrimes such as hacking, fraud, intellectual property theft, and online exploitation. Similarly, in the corporate sector, digital forensics assists organizations in detecting and mitigating insider threats, data breaches, and unauthorized access incidents, thereby safeguarding sensitive data and preserving the integrity of digital assets.

As technology continues to evolve at a rapid pace خطوة, digital forensics faces a myriad of challenges and complexities, including the proliferation انتشار of encrypted

communications, the advent of emerging technologies such as artificial intelligence and blockchain, and the globalization of cyber threats. Moreover, legal and ethical considerations surrounding the collection, admissibility, and preservation of digital evidence further underscore the interdisciplinary nature of digital forensics, requiring collaboration among law enforcement agencies, cybersecurity experts, legal professionals, and forensic analysts.

In light of these challenges, the importance of robust digital forensics practices and the need for continuous research, training, and collaboration within the field cannot be overstated. By leveraging cutting-edge technologies, adopting best practices, and fostering تعزيز interdisciplinary collaboration, digital forensics professionals play a vital role in enhancing cybersecurity resilience, promoting accountability, and upholding justice in the digital age.

1.2 Forensics Science

Def. Forensic science is a special branch of crime investigation that utilizes scientific principles to support or negate نفي theories surrounding the evidence discovered at the scene of a crime. مسرح الجريمة

The role of forensic scientists is analyzing evidence gathered from crime scenes in order to develop reasonable hypothesizes فرضبيات معقوله ومقبولة which led up تقودto discover the evident that prove how the crime happened. The evidences range from images of child pornography صور الاطفال ذات الطابع الجنسي الفاضح to encrypted data considered as criminal activities. Even in investigations that are not primarily electronic in nature, ليس اساسا يكون ذات طابع الكتروني at some point in the investigation computer files may be discovered and further analysis required (Give example).

1.3 Subdivisions of Forensic Science

Forensic science encompasses a broad spectrum of subdivisions تشتمل على طيف واسع من الفروعin order to provide answers to questions of interest for the legal system. Next sections will focus on some of the divisions relating to criminal justice.

1- Computational مهم

Computational forensics defines as the branch of forensics where specialists can accurately assess data بدقة البيانات اختبار using computer software through the development of algorithms to assist forensic examination.

2- Digital مهم

Digital forensics role is to provide our legal system with a way to recover data from electronic or digital devices.

Digital forensics can be seen as a matter of looking at computer systems and networks to determine who, what, when, where, how and why of things happening.

الانواع التالية للاطلاع فقط

3- Criminalistics علم الاجرام

4- DNA Analysis

5- Psychology

6- Toxicology علم السموم

Each division has a different purpose, but they all work together to analyze evidence from a crime scene.

1.4 Why Computer Forensics is Important?

If you work as an information system and network administrator, you should understand computer forensics. Why??

Computer forensics will help you ensure:

1. The overall integrity
2. Survivability of your network infrastructure.
3. Capture vital information if your network is compromised

4. Prosecute مقاضاة the intruder (if he/she caughtبهم اذا تم الامسك).

You can help your organization if you consider computer forensics as a new basic element in what is known as a "defense-in-depth" approach to network and computer security

What happens if you ignore computer forensics or practice it badly?

1- You risk destroying اتلاف vital evidence (ذات تأثير كبير) أدلة مهمة or having forensic evidence considered inadmissible غير مقبول in a court of law.
2- You or your organization may run afoul متعارضة with new laws that mandate (تفوض او تأمر) regulatory complianceالتزامات تنظيمية and assign liability تنسب المسؤولية if certain types of data are not adequately protected. يتم حمايتها بصورة ملائمة

Recent legislation in some countries makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data.

ما هي عقوبة الافصاح عن معلومات الاخرين بدون مواقتهم حسب القانون العراقي

Digital Forensics can save organization money where managers usually allocating a greater portion of their information technology budgets for computer and network security.

Two basic types of data are collected in computer forensics.

A- Persistent data: It is the data that is stored on a local hard drive (or another medium) and preserved when the computer is turned off.

B- Volatile data: It is any data that is stored in memory, or exists in transit, but got lost when the computer loses power or turned off. Volatile متطايرة data resides تقع in registries, cache, and random access memory (RAM). Since volatile data is ephemeral,سريعة الزوال it is essential مبدأ اساسي an investigator knows reliable ways to capture it.

System administrators and security personnel موظفي شؤون امن الملومات must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential

admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

Q what is Defense in depth principle?

Q why System administrator and security personnel should have basic knowledge of Digital Forensics?

1.5 Legal Aspects of Computer Forensics

Anyone overseeing يشرف على network security must be aware of the legal implications تداعيات of forensic activity (Why?). Security professionals need to consider their policy decisions and technical actions in the context of existing laws. For instance, you must have authorization before you monitor and collect information related to a computer intrusion.

The important point for forensics investigators is that evidence must be collected in a way (why?) in order to be legally admissible in a court case.

It is becoming necessary to prove that your organization is complying with computer security best practices. **Organization that has added a computer forensics capability to its resources will be able to show that it followed security policy and potentially ضمنيا avoid lawsuits تتجنب الدعاوي القضائيor regulatory audits**

1.6 Digital Evidence الفقرة بالكامل مهمة

Def. Digital evidence is defined as "any data stored or transmitted using a computer that support or refute تدحض a theory of how an offense الجريمة occurred or that address تحدد critical elements of the offense such as intent نية مسبقة or alibi _ عذر للبراءة_ **او_حجة_الغياب**

Digital evidence can reveal communications between suspects and the victim such as online activities at key times, and other information that provides a digital dimension to the investigation.

In computer intrusions في حالة اختراق اجهزة الكومبيوتر, the attackers will leave multiple traces of their presence throughout the environment, including in the file systems, registry, system logs, and network-level logs. Such evidence can be used to link an individual to an intrusion.

In an e-mail harassment caseقضايا الازعاج عن طريق الايميل , the act of sending threatening messages via a Web-based e-mail service such as Hotmail can leave a number of traces. The Web browser used to send messages will store files, links, and other information on the sender's hard drive along with date-time–related information. Therefore, forensic analysts may find information relating to the sent message on the offender's hard drive القرص الصلب للمجرم, including the original message contents. Additionally, investigators may be able to obtain related information from Hotmail, including Web server access logs, IP addresses, and possibly the entire message in the sent mail folder of the offender's e-mail account.

The main sources for digital evidence are:

- Servers
- Network Computers
- Personal home computers
- Cloud storage
- Cloud application
- CD-ROMs & DVDs
- Floppy disks (rarely available nowadays)
- Tape archives (rarely available nowadays)
- Removable hard drives and flash memories

1.7 Increasing Awareness of Digital Evidence

By now it is well known that police are encountering progressively تدريجيا more digital evidence in their work. **Computer security professionals and military decision makers are concerned with digital evidence.** An increasing number of organizations are faced with the necessity of collecting evidence on their networks in response to incidents such as computer intrusions, fraud الاحتيال, intellectual property theft, sexual harassment التحرش الجنسي , and even violent crimes.جرائم العنف

More organizations are considering legal and technical processes when criminals target them, these organizations pay more attention to handling digital evidence التعامل مع الادلة الرقمية in a way that will hold up in court. **Also, by processing digital evidence properly, employees are protecting themselves against liabilities such as invasion غزو of privacy** and may be fired يطرد from their job**.** As a result, there are rising expectations that computer security professionals will have training and knowledge related to digital evidence handling.

In addition to handling evidence properly, corporations and military operations need to respond to and recover from incidents rapidly (why?) to minimize the losses caused by an incident. This task can be done properly by adopting Incident Response Plan.

Many computer security professionals deal with hundreds of simple crimes each month and there is not enough time, resources, or desire to open a full investigation for each incident. Therefore, many computer security professionals attempt to limit the damage and close each investigation as quickly as possible.

Q Why Computer securities professionals attempt to close investigation quickly after imitate the damage?

1.8 Who need for Computer Forensics?

1- **National Security**

Electronic information systems are vital for maintaining المحافضة على a national security of any state. Possible unauthorized access مخول الغير الوصول احتماليةto the critical governmental infrastructures by state and non-state entities الكيانات الحكومية والير حكومية can create a serious threat and have a negative impact on political, economic and military security of a given nation.

2- **Information Security**

3- **Corporate Espionage.**

Corporate espionage, industrial espionage, and cyber espionage all generally mean the same thing: (1) intentionally targeting or acquiring trade secrets of companies to benefit any foreign government or foreign agent.

What is Cyber Espionage?

4- **Child Pornography للاطلاع**

The war on cyber child pornography began in the mid-1990s when two FBI agents noticed that pedophilesجنسيا الشاذين we're using the internet to send and receive images of minors قاصرين. Further investigating showed that internet bulletin that lured استدراج children into the hands of pedophiles. These discoveries resulted in the creation of the "Innocent Images National Initiative", an operation who used undercover agents عملاء سريين to catch child pornographers and pedophiles who preyed مفترسين on the world's most vulnerable and innocent victims.

Since then, the program has charged nearly 5,000 criminals and opened nearly 16,000 investigations. The original handful of agents is now in the hundreds, trained specialists delving into the dark underbelly of the internet to catch and convict the lowest of predators. In 2004 the operation went international, working with agents in other countries to protect children and sharing information and resources to help insure convictions.

http://cybercrimestatistics.com/online-child-pornography/

5- Incident Response مهمة

Def. Incident response is a term used to describe the process by which an organization handles تتعامل معa data breach or cyber-attack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and recovery time and costs, as well as collateral damage الاعراض الجانبية such as brand reputation, are kept at a minimum.

Typically, incident response is conducted by an organization's Computer Incident Response Team (CIRT), also known as a cyber-incident response team. CIRTs usually are comprised من تتالف of security and general IT staff, along with members of the legal, human resources, and public relations departments. **CIRT is a group that "is responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks.** In addition to technical specialists capable of dealing with specific threats, **it should include experts who can guide enterprise executives on appropriate communication in such incidents".**

https://digitalguardian.com/blog/what-incident-response

Q: who handles incident responses?

Q: What Incident Response Team should include?

Employee Monitoring

It is everything your team does on company time and on company resources matters. Time spent on frivolous تافه او غير ذي فائدة websites can seriously reduce productivity and visiting objectionable sites on company PCs can subject your business to serious legal risks.

Why managers should Monitor their employees?

6- Privacy Issues