# Chapter Nineteen

- What is **Digital Forensics**?
- History of Digital forensics
- Objectives of computer forensics
- Process of Digital forensics
- Types of Digital Forensics
- Challenges faced by Digital Forensics
- Example Uses of Digital Forensics
- Advantages of Digital forensics
- Disadvantages of Digital Forensics

343

## ماهو الطب الشرعي الرقمي؟

- **يعُرفّالطب الشرعي الرقمي بأنه عملية الحفاظ على أدلة الكمبيوتر وتحديدهاواستخراجها وتوثيقها والتي يمكن أن تستخدمها محكمة القانون**. إنه علم للعثور على أدلة من الوسائط الرقمية مثل a**حاسوب**و **تليفونمحمول**و**الخادم**، أو**شبكة**. يزود فريق الطب الشرعي بأفضل التقنياتوالأدوات لحل القضايا الرقمية المعقدة.

- **الطبالشرعي الرقمي**يساعد فريق الطب الشرعي على تحليل وفحص وتحديدهوية وحفظ الأدلة الرقمية الموجودة على أنواع مختلفة من الأجهزة الإلكترونية.

# What is Digital Forensics?

- **Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law**. It is a science of finding evidence from digital media like a **computer**, **mobile phone**, **server**, or **network**. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.
- **Digital Forensics** helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

344

## تاريخالطب الشرعي الرقمي

- **هانزجروس**(1847-1915): أول استخدام للدراسة العلمية لرئاسة التحقيقاتالجنائية
- **مكتبالتحقيقات الفدرالي**(1932): إنشاء مختبر لتقديم خدمات الطب الشرعي لجميع الوكلاء الميدانيين والسلطات القانونية الأخرى في جميعأنحاء الولايات المتحدة الأمريكية.
- فيعام 1978**أول جريمة كمبيوتر**تم الاعتراف بها في قانون فلوريدا لجرائم الكمبيوتر.
- **فرانسيسجالتون**(1911-1982): أجرى أول دراسة مسجلة ل**بصمات الأصابع**
- فيعام 1992 ، تم استخدام مصطلح الطب الشرعي الحاسوبي**الأدب الأكاديمي**.
- 1995**المنظمة الدولية للأدلة الحاسوبية (IOCE)**تم تشكيل.
- فيعام 2000 ،**أول مختبر جنائي للحاسوب الإقليمي لمكتب التحقيقات الفيدرالي**مقرر.
- في2002،**مجموعة العمل العلمية المعنية بالأدلة الرقمية (SWGDE)**نشر أول كتاب عنالطب الشرعي الرقمي بعنوان "أفضل ممارسات الطب الشرعي الحاسوبي".
- في2010،**سيمسون جارفينكل**القضايا المحددة**تواجه التحقيقات الرقمية**.

# History of Digital forensics

- **Hans Gross** (1847 -1915): First use of scientific study to head criminal investigations
- **FBI** (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the **first computer crime** was recognized in the Florida Computer Crime Act.
- **Francis Galton** (1982 - 1911): Conducted first recorded study of **fingerprints**
- In 1992, the term Computer Forensics was used in **academic literature**.
- 1995 **International Organization on Computer Evidence (IOCE)** was formed.
- In 2000, the **First FBI Regional Computer Forensic Laboratory** established.
- In 2002, **Scientific Working Group on Digital Evidence (SWGDE)** published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, **Simson Garfinkel** identified issues **facing digital investigations**.

345

345

## أهدافالطب الشرعي الحاسوبي

- يساعدعلي**استعادة**و**تحليل**، و**يحفظ**الكمبيوتر والمواد ذات الصلة بطريقة تساعد وكالةالتحقيق على تقديمها كدليل في محكمة قانونية.
- يساعدعلى افتراض**الدافع وراء الجريمة**و**هوية الجاني الرئيسي**.
- **إجراءاتالتصميم**في مسرح جريمة مشتبه به مما يساعدك على التأكد من أن**الأدلة الرقمية**تم الحصول عليها**لا تالف**.
- **الحصولعلى البيانات**و**الازدواجية**: استعادة الملفات المحذوفة والأقسام المحذوفةمن الوسائط الرقمية لاستخراج الأدلة والتحقق من صحتها.
- يساعدكعلى**التعرف على الأدلة بسرعة**، ويسمح لك أيضاً بتقدير التأثير المحتمل للنشاطالضار على الضحية
- إنتاج**أتقرير الطب الشرعي الكمبيوتر**الذي يقدم تقريراً كاملاً عن عملية التحقيق.
- **-حفظ الأدلة**باتباع سلسلة الوصاية.

# Objectives of computer forensics

- It helps to **recover**, **analyze**, and **preserve** computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the **motive behind the crime** and **identity of the main culprit**.
- **Designing procedures** at a suspected crime scene which helps you to ensure that the **digital evidence** obtained is **not corrupted**.
- **Data acquisition** and **duplication**: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to **identify the evidence quickly**, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a **computer forensic report** which offers a complete report on the investigation process.
- **Preserving the evidence** by following the chain of custody.

346

346

## Process of Digital forensics

- **Digital forensics** entails the following steps:
  - Identification
  - Preservation
  - Analysis
  - Documentation
  - Presentation

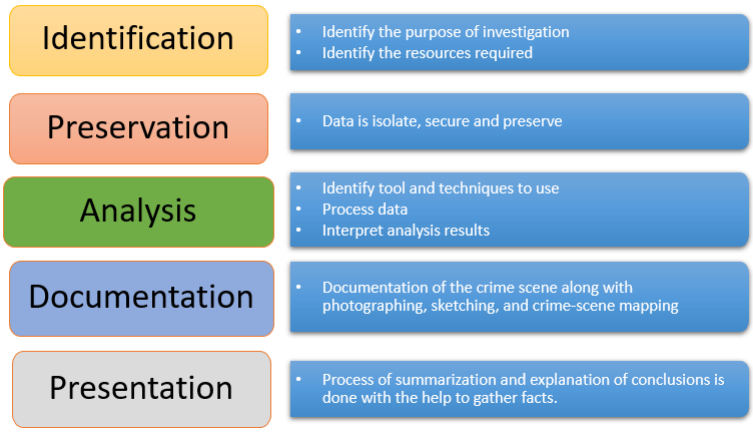
عمليةالطب الشرعي الرقمي

- **الطب الشرعي الرقمي** يستلزم الخطوات التالية:
  - تعريف
  - الحفظ
  - تحليل
  - توثيق
  - عرض تقديمي

347

347

## Process of Digital forensics-cont.




348

348

عمليةمتابعة الطب الشرعي الرقمي.

- **تعريف**
  - إنهاالخطوة الأولى في عملية الطب الشرعي. تتضمن عملية تحديد الهوية بشكل أساسيأشياء مثل ما هو الدليل الموجود ، ومكان تخزينه ، وأخيرا ، كيفية تخزينه ( باي تنسيق).
  - يمكن أن تكون وسائط التخزين الإلكترونية**حواسيب شخصية**و**الهواتف المحمولة**و **أجهزة المساعد الرقمي الشخصي**، إلخ.
- **الحفظ**
  - في هذه المرحلة ،**يتم عزل البيانات وتأمينها وحفظها**. ويشمل منع الأشخاص من استخدام الجهاز الرقمي حتى لا يتم العبث بالأدلة الرقمية.
- **تحليل**
  - في هذه الخطوة ، وكلاء التحقيق**إعادة بناء أجزاء من البيانات واستخلاص النتائج بناء على الأدلة التي تم العثور عليها**. ومع ذلك ، قد يتطلب الأمر تكرارات عديدة من الفحص لدعم نظرية جريمة معينة.

# Process of Digital forensics-cont.

- **Identification**
  - It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).
  - Electronic storage media can be **personal computers**, **Mobile phones**, **PDAs**, etc.
- **Preservation**
  - In this phase, **data is isolated, secured, and preserved**. It includes preventing people from using the digital device so that digital evidence is not tampered with.
- **Analysis**
  - In this step, investigation agents **reconstruct fragments of data and draw conclusions based on evidence found**. However, it might take numerous iterations of examination to support a specific crime theory.

personal digital assistant

349

عمليةمتابعة الطب الشرعي الرقمي.

349

- **توثيق**
  - في هذه العملية،**يجب إنشاء سجل لجميع البيانات المرئية**. يساعد في إعادة إنشاء مسرح الجريمة ومراجعته. وهي تنطوي على التوثيق الصحيح لمسرح الجريمة إلى جانب التصوير ،والرسم ، ورسم خرائط مسرح الجريمة.
- **عرض تقديمي**
  - في هذه الخطوة الأخيرة ،**عملية تلخيص وشرح الاستنتاجات**تم.
  - ومع ذلك ، يجب أن تكتب بمصطلحات شخص عادي باستخدام مصطلحات مجردة.يجب أن تشير جميع المصطلحات المستخرجة إلى التفاصيل المحددة.

# Process of Digital forensics-cont.

- **Documentation**
  - In this process, **a record of all the visible data must be created**. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.
- **Presentation**
  - In this last step, **the process of summarization and explanation of conclusions** is done.
  - However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

350

350

- **الطب الشرعي للقرص:**
  - يتعاملمع استخراج البيانات من وسائط التخزين عن طريق البحث **نشيط** و**معدل**، أو **الملفات المحذوفة**.
- **الطب الشرعي للشبكة:**
  - إنهفرع فرعي للطب الشرعي الرقمي. إنها تتعلق بالرصد و**تحليل حركة مرور شبكة الكمبيوتر** لجمع المعلومات الهامة والأدلة القانونية.
- **الطب الشرعي اللاسلكي:**
  - إنهقسم من الطب الشرعي الشبكي. الهدف الرئيسي للطب الشرعي اللاسلكي هو تقديم الأدوات اللازمة لجمع وتحليل البيانات من **حركة مرور الشبكة اللاسلكية**.
- **الطب الشرعي لقاعدة البيانات:**
  - إنهفرع من فروع الطب الشرعي الرقمي يتعلق بالدراسة و**فحص قواعد البيانات** والبيانات الوصفية ذات الصلة.

# Types of Digital Forensics.

- **Disk Forensics:**
  - It deals with extracting data from storage media by searching **active**, **modified**, or **deleted files**.
- **Network Forensics:**
  - It is a sub-branch of digital forensics. It is related to monitoring and **analysis of computer network traffic** to collect important information and legal evidence.
- **Wireless Forensics:**
  - It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from **wireless network traffic**.
- **Database Forensics:**
  - It is a branch of digital forensics relating to the study and **examination of databases** and their related metadata.

351

- **التحاليل الجنائية للبرامج الضارة:**
  - هذاالفرع يتعامل مع **تحديد الشفرة الخبيثة**، لدراسة **الحمولة** و**الفيروسات** و**الديدان**، إلخ.
- **البريدالإلكتروني الطب الشرعي**
  - يتعاملمع **استعادة وتحليل رسائل البريد الإلكتروني**، مشتمل **رسائل البريد الإلكتروني المحذوفة** و**التقويمات**، و**جهات الاتصال**.
- **الطب الشرعي للذاكرة:**
  - يتعاملمع جمع البيانات من ذاكرة النظام (**سجلات النظام** و**مخبأ** و **كبش**) في شكل خام ثم نحت البيانات من مكب الخام.
- **التحاليل الجنائية للهواتف المحمولة:**
  - إنهيتعامل بشكل أساسي مع فحص وتحليل **أجهزة محمولة**. يساعد على استرداد الهاتف و**جهات اتصال** SIM و**سجلات المكالمات** و**واردة**، و**الرسائل القصيرة** / **رسائل الوسائط المتعددة الصادرة** و**صوتي** و**أشرطة فيديو**، الخ.

351

# Types of Digital Forensics-cont.

- **Malware Forensics:**
  - This branch deals with the **identification of malicious code**, to study their **payload**, **viruses**, **worms**, etc.
- **Email Forensics**
  - Deals with **recovery and analysis of emails**, including **deleted emails**, **calendars**, and **contacts**.
- **Memory Forensics:**
  - It deals with collecting data from system memory (**system registers**, **cache**, **RAM**) in raw form and then carving the data from Raw dump.
- **Mobile Phone Forensics:**
  - It mainly deals with the examination and analysis of **mobile devices**. It helps to retrieve phone and **SIM contacts**, **call logs**, **incoming**, and **outgoing SMS/MMS**, **Audio**, **videos**, etc.

352

352

## التحدياتالتي يواجهها الطب الشرعي الرقمي

- زيادةأجهزة الكمبيوتر والاستخدام المكثف لـ**خدمة الإنترنت**
- سهولةتوافر**أدوات القرصنة**
- **عدموجود أدلة مادية**يجعل المحاكمة صعبة.
- كميةكبيرة من مساحة التخزين في**تيرابايت**مما يجعل مهمة التحقيق صعبة.
- تتطلبأي تغييرات تكنولوجية وجود**يرقي**أو**التغييرات**إلى الحلول.

## Challenges faced by Digital Forensics

- The increase of PC's and extensive use of **internet access**
- Easy availability of **hacking tools**
- **Lack of physical evidence** makes prosecution difficult.
- The large amount of storage space into **Terabytes** that makes this investigation job difficult.
- Any technological changes require an **upgrade** or **changes** to solutions.

353

## استخداماتالمثال للطب الشرعي الرقمي

353

- سرقةالملكية الفكرية
- التجسسالصناعي
- منازعاتالعمل
- تحقيقاتالاحتيال
- الاستخدامغير الملائم للإنترنت والبريد الإلكتروني في مكان العمل
- المسائلالمتعلقة بالتزوير
- تحقيقاتالإفلاس
- قضاياالقلق مع الامتثال التنظيمي

## Example Uses of Digital Forensics

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

354

354

## مزاياالطب الشرعي الرقمي

- لضمان**نزاهة**من نظام الكمبيوتر.
- لانتاج**دليل في المحكمة**مما قد يؤدي إلى معاقبة الجاني.
- يساعدالشركات في الحصول على معلومات مهمة إذا كانت أنظمة أو شبكاتالكمبيوتر الخاصة بهم**مساومة**.
- يتتبعبكفاءة**مجرمو الإنترنت**من أي مكان في العالم.
- يساعدعلى حماية**أموال المنظمة**ووقت ثمين.
- يسمحل**يستخرج**و**عملية**، و**يفسر**الأدلة الواقعية ، لذلك فهي تثبت عمل المجرمينالإلكترونيين في المحكمة.

# Advantages of Digital forensics

- To ensure the **integrity** of the computer system.
- To produce **evidence in the court**, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are **compromised**.
- Efficiently tracks down **cybercriminals** from anywhere in the world.
- Helps to protect the **organization's money** and valuable time.
- Allows to **extract**, **process**, and **interpret** the factual evidence, so it proves the cybercriminal action's in the court.

355

## عيوبالطب الشرعي الرقمي

- قبولالأدلة الرقمية في المحكمة. ومع ذلك ، يجب إثبات عدم وجود تلاعب

355

- يعدإنتاج السجلات الإلكترونية وتخزينها أمراً مكلفاً للغاية
- يجبأن يكون لدى الممارسين القانونيين معرفة واسعة بالكمبيوتر
- الحاجةإلى إنتاج أدلة حقيقية ومقنعة
- إذاكانت الأداة المستخدمة في الطب الشرعي الرقمي لا تتوافق مع معايير محددة ،فعندئذٍفي محكمة القانون ، يمكن رفض الأدلة من قبل العدالة.
- قدلا يؤدي نقص المعرفة الفنية من قبل ضابط التحقيق إلى النتيجة المرجوة

# Disadvantages of Digital Forensics

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

356

356

## Summary

- **Digital Forensics** is the **preservation**, **identification**, **extraction**, and **documentation** of computer evidence which can be used in the court of law
- **Process of Digital forensics** includes 1) Identification, 2) Preservation, 3) Analysis, 4) Documentation and, 5) Presentation
- **Different types of Digital Forensics** are Disk Forensics, Network Forensics, Wireless Forensics, Database Forensics, Malware Forensics, Email Forensics, Memory Forensics, etc.
- **Digital forensic Science** can be used for cases like 1) Intellectual Property theft, 2) Industrial espionage 3) Employment disputes, 4) Fraud investigations.

## ملخص

357

- **الطبالشرعي الرقمي**هل**الحفظ**و**تعريف**و**استِخلاص**، و **توثيق**من أدلة الكمبيوترالتي يمكن استخدامها في المحاكم
- **عمليةالطب الشرعي الرقمي**يتضمن 1) تحديد الهوية ، 2) الحفظ ، 3) التحليل ، 4) التوثيق ، 5) العرض التقديمي
- **أنواعمختلفة من الأدلة الجنائية الرقمية**هي الطب الشرعي للقرص ، والطب الشرعي للشبكة ، والطب الشرعي اللاسلكي ،والطب الشرعي لقاعدة البيانات ، والطب الشرعي للبرامج الضارة ، والطب الشرعي للبريد الإلكتروني ، والطبالشرعي للذاكرة ، وما إلى ذلك.
- **علومالطب الشرعي الرقمي**يمكن استخدامها في قضايا مثل 1) سرقة الملكيةالفكرية ، 2) التجسس الصناعي 3) نزاعات التوظيف ، 4) التحقيقات فيالاحتيال.