2- Rules of Evidence

2-1 Design Systems with Forensic Needs in Mind

Tools that are designed for detecting malicious activity on computer networks are rarely قلما **designed with evidence collection in mind**. Some organizations are attempting to support their existing systems with forensics tools in order to address تبين authentication issues that arise in court. Other organizations are implementing تتبنى additional systems specifically designed to secure digital evidence, popularly called Network Forensic Analysis Tools (NFATs).

The purpose of design such system is to enable Digital detectives to monitoring, acquiring relative data that can be considered as digital evidence from suspect system الانظمة المشكوك بها.

Digital system may be Computer, Network, Mobile device etc…..,
all these equipment potentially has the ability to be used as tools to run a digital attack against victims such as denial of service or hacking other computers. On the other hand, they can be used for threating others تهديد للأخرين such as writing blackmail (**Simple Definition of blackmail: the crime of threatening to tell secret information about someone unless the person being threatened gives you money or does what you want)** and so on.

Forensics tools can help investigators to determine many facts تحدد العديد من الحقائق **that can be used legally to prosecute criminal** لمقاضاة المجرمين **when evidence collect in its real time.**

Because the digital data are volatile, it can be removed quickly in a way that make it hard to trace من الصعوبة تتبعها or to be collect while investigators collect data.

For PCs, "for instance " the data in RAM which reflect the current process can be disappear تختفي when computer powered off, in this scenario we believe that pre-installing forensics software tools on digital devises can help collect such sensitive data البيانات المهمة in critical timeوقت حرج او وقت مهم جدا. Other digital system can be monitored using suitable software برامجيات مناسبة, for example, Networks can be supplied with IDS or WIRESHARK to monitor and record مراقبة وتسجيلmost activities that can help track the suspect activity**. These tools when installed prior to the crime, it will help detectives to gain a lot of information about the crime and the attack.**

One of the main benefits of considering the design of any system to be forensically minded is to collect evidence in a way that help digital detectives to collect; identify and analyze the electronic evidence in the best way to be inadmissible in the court. But even so, the rules of electronic evidence must be implemented to persuade the judge to accept this evidence.

2-2The principles of digital evidence: مهمة جدا

According to ((ACPO), 2016), the main principles can be summarized as:

Principle 1: No action taken by law enforcement agencies staff member(s) should change data which may subsequently بعد ذلكbe relied upon يتم الاعتماد in court.

Principle 2: In circumstances where a person finds it necessary to access original data, that person must be specialist متخصص to do so and be able to give evidence explaining the relevance اهمية and the implications الاثارof their actions.

Principle 3: An audit trail التدقيق or other record of all processes applied to digital evidence should be created and preservedتحفظ . An independent third party جهة ثالثة مستقاة should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Operating systems and other programs frequently alter, add and delete the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed. **In order to comply with the principles of digital evidence, an image should be made of the device. This will ensure ستؤكدthat the original data is preserved البيانات الاصلية تبقى محفوة, enabling an independent third party to re-examine it and achieve the same result, as required by principle 3.**

The process of imagine original data عملية استنساخ او تصوير البيانات الاصليةmay be a physical / logical block image of the entire device, or a logical file image containing partial or selective data (which may be captured as a result of a triage processعملية الفرز).

In cases where dealing with data which is stored at a remote, possibly inaccessible location, it may not be possible to obtain an image. It may become necessary for the original

data to be directly accessed to recover the data. With this in mind, it is essential that a person who is competent الشخص المختص to retrieve استرجاع the data and then able to give evidence to a court of law makes any such access.

2-3 Rules of evidence

The rules of evidence were developed over several centuries and are based upon the rules from Anglo-American common law المستوطنون او المستعمرون.brought to the New World by early settler's Their purpose is to be fair to both parties, disallowing the raising of allegations without a basis in provable fact.

Rules of evidence govern when, how, and for what purpose the evidence used.

Wining the case in court ربح القضية في المحكمةrequires a good understanding of the rules of evidence in the given venue مكان الدعوى. One reason to have a lawyer among others**, is that he or she should be familiar with the rules of evidence**.

Rules that derived from the main principles mentioned earlier in this lecture can be listed as below:

Rule 1. An examination should never be performed on the original media.

Rule 2. A copy is made onto forensically sterile media وسط خالي من الشوائب. New media should always be used if available.

Rule 3. The copy of the evidence must be an exact, bit-by-bit copy. (Sometimes referred to as a bit-stream copy).

Rule 4. The computer and the data on it must be protected during

the acquisition of the media to ensure that the data is not modified. (Use a write blocking device when possible)

Rule 5. The examination must be conducted تجريin such a way as to prevent any modification of the evidence.

Rule 6. The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

https://www.helpnetsecurity.com/2007/07/20/the-rules-for-/computer-forensics

2-4 Search and Seizure

Def. Search and seizure are the legal term used to describe a law enforcement agent's examination of a person's home, vehicle, business; etc…. to find evidence that a crime has been committed تم ارتكابها . If evidence is found, the agent will "seize" it.

http://www.searchandseizure.org/

In Digital World, when computer crimes are committed ترتكب, law officials مسؤولي القانون work hard to obtain rights that will allow them to search and seize digital evidence necessary for the prosecution of cybercrime. They look for evidence that will allow computer forensic experts to collect the information needed in order to execute a proper arrest الاعتقالagainst the perpetrators of the computer crimes مرتكبي جرائم الكومبيوتر. **There are two basic methods for a search and seizure of digital evidence in order to prove a case in a cybercrime: one with a warrant تفويض, and one without a warrant.**

Depending on the types of computer crimes, a warrant can sometimes be obtained rather easily. For example, **if there is strong evidence supporting that the computer crimes were committed and the suspect's computer contains harmful content (i.e. child pornography or threating other's life) that might endanger someone's life, then this would be a considerable reason for a warrant to be issued. If there is strong evidence of computer crimes committed that were committed utilizing a computer that may contain evidence supporting drug deals or the production of illegal materials (i.e. unauthorized duplications of copyrighted materials), this may be another reason for a warrant to be issued.**

Q When warrant can be easy issues?

http://criminal.laws.com/computer-crime/doj-computer-crime-and-intellectual-property-section/search-and-seizure-of-digital-evidence

2-5 Requirement for Legally Seizing Computer Evidence

Legal seizing الاستحواذ القانوني على الاداة لكونها دليل must satisfy some requirement such as:

1. **Legally obtained:**

For evidence to be admissibleمقبول in a court of law it must be legally obtained. The organization's policies and procedures must be carefully followed. Corporations often have incident response plans that you should follow. The case may become a legal matter, especially if it's related to fraud, security breaches, or privacy infringements.

2. **Complete.**

Don't leave behind computer evidence just because you think it might exonerate the suspect يبرئ الشخص المتهم even if you think the suspect is an awful person. شخص سيئ

3. **Reliable**. The evidence must be untainted غير مشوب او غير ملوث

It should remain unchanged from its original. Following careful procedures will help you ensure that fragile computer evidence الدليل الرقمي القابل للتلف doesn't get altered, deleted, or changed in any way. Maintaining the chain of custody will also ensure that evidence remains reliable.

4. **Authentic**. It has to be the real thing, not a fake.
5. **Believable**. A jury and a judge (or corporate managers and auditors) need to understand and accept the evidence.

When seizing hardware, you will

1-tag it with an evidence tag وضع علامة that documents the date and time

2-your name

3-the case number

4-where you found the item

5-other facts relevant متعلقة to the case, and other information depending on the policies and procedures of your investigation team.

6-bagترزم the evidence and give it to an evidence custodian الوصي او المسؤول. Some experts call this process "bagging and tagging."

Q: what is the proper process to seize hardware?

2-6 Chain of Custody عهدة

Def. Chain of Custody (CoC), in legal contexts, refers to the chronological documentation توثيق مرتب زمنيا, showing the seizureالاستيلاء او المصادر, custody,الحجز القضائي control, transfer, analysis, and disposition تغيير او التصرف of physical or electronic evidence. You need to be able to trace the route that evidence takes from the moment you collect it until the time it is presented in court or at a corporate briefing .

2.7 WHAT IS EXPERT TESTIMONY?

The expert witness plays an essential role under the US system of jurisprudence نظام التشريع and most other systems. Courts rely on expert witness testimony البرهان او الدليل in most civil and criminal cases to explain scientific matters that may or may not be understood by jurors and judges.

Testimony of an expert witness شهادة الخبيرdiffers from that of other witnesses. "Witnesses of fact" (those testifying يشهدونbecause they have personal knowledge of the incident or are persons involved in the lawsuit(القضية , typically restrict their testimony to the facts of the case at issue. The expert witness is given more latitude مجالات اوسع للشرح. The expert witness is allowed to compare the applicable standards related to the case with the facts of the case and interpret يفسر

whether the evidence indicates a deviation from the standards or not.

An expert must be qualified. Although the rules vary among jurisdictions about whether the expert must be of the same specialty as the defendant. The expert, must demonstrate to the judge sufficient knowledge and expertise about the issue

http://pediatrics.aappublications.org/content/124/1/428

The testimony of witness f expert is useful because: مهمة

(a) The expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue.

(b) The testimony is based on sufficient facts or data.

(c) The testimony is the product of reliable principles and methods.

(d) The expert has reliably applied the principles and methods to the facts of the case.

https://www.law.cornell.edu/rules/fre/rule_702

Works Cited

(ACPO), T. A. (2016). *The Priciples of Digital Forensics.* London : Forensic Resources ltd. http://www.computerforensicsspecialists.co.uk/blog/the-principles-of-digital-evidence.