Information Technology Systems Architecture

Chimene Tchokoko Diboma

School or Institution Name (University at Place or Town, State)

**Information Technology Systems Architecture**

**Introduction:**

Information technology plays the role of utility in modern life. Businesses rely on information technology systems for their operations. With exponential penetration of information technology into businesses and everyday processes, attacks on such systems have also increased tremendously. Most of the organizations collect and process personally identifiable information of customers for service delivery. Headlines are filled with news of successful targeted attacks on organizations and individuals as well (Martini & Choo, 2012). To investigate such attacks and criminal activities involving information technology systems digital forensic investigation methods are utilized. The paper describes the methods involved in digital forensic investigations, tools and technologies, and issues involved in such investigations.

**Digital Forensics Methodology:**

Steps involved in the investigations of digital crime may be similar to those of ordinary investigations, but the methods are totally different. There are various tools that need to be utilized effectively in order to collect digital evidence. The first step in digital forensic investigations involves preparation of the investigation. Preparations for each investigation event may be different based on the nature of the digital crime being investigated. There may be no physical footsteps in digital forensics to be investigated. Therefore, there must be an appropriate plan of investigation before initiating the actual investigation process. In digital crimes, computer systems can be used as an object of crime or as a tool to commit the crime. Computer systems have central importance in any digital investigation.

Digital forensics is the process of collecting information while maintaining the integrity of the information. It is crucial in such investigations to maintain the integrity of evidence being collected because criminals can further obfuscate the available details or digital fingerprints on machines. During the preparation phase of digital forensic, the investigators have to decide about the point of initiation (Ab Rahman, Glisson, Yang, & Choo, 2016). That requires identification that what should be analyzed to find evidence. In case of a vast computer network, it is highly possible that the whole network was compromised or involved in an attack or just a part of the network. Once, the physical point of the investigation is determined then various data analysis tools are used to extract information from the systems. It involves the collection of metadata along with the actual data that can help in identification of the criminals. Evidence collected in this phase is then analyzed using sophisticated file analysis tools. Findings are then reported using standardized formats because most of the time digital forensics data may be used in a court case later in time.

Collection of equipment or evidence in a particular investigation is crucial. The identified place of crime may have a different type of hardware connected to a network. For example, if storage disks are configured or connected to a computer system using RAID technologies, then appropriate RAID levels must be preserved to extract the data from the disks (Mitchell, Anandaraja, Hara, Hadzhinenov, & Neilson, 2017). Otherwise, careless handling of digital evidence will result in the loss of information that could be crucial in moving forward. Physical samples collected must be preserved against tampering so, that actual information can be retrieved from the source.

**Digital Forensic Tools:**

There are many tools and utilities that can be used in digital forensic analysis. One such tool is known as EXIF tool. The tool is used to reveal metadata of any particular file. Metadata is known as the data about the data. Such as the metadata of an image may reveal about the geolocation where the image was captured, exact date and time, time of last modification of the image file. All of these information bits help in the investigation of digital crime. Computers preserve last accessed timestamp of all the files stored in them in the metadata of the file. Therefore, extracting metadata of files in crucial in digital forensic investigations. Many other forensic investigation tools are to be used at this step such as forensic toolkit software that allows the researchers to scan complete data storage drives for evidence.

A significant hurdle in the collection of the evidence is that a criminal may have deleted the files and crime tools from the storage. In such cases the use of forensic tools is inevitable. FTK software scans full hard drive storage to locate the data and provide granular visibility into related metadata of discovered files. It uses sophisticated algorithms to retrieve pieces of data that were previously deleted by the criminal. Even if the complete file is not retrieved, the tool will be able to reveal necessary pieces of metadata of the file. It is especially helpful in the retrieval of deleted emails from a computer system. Emails can reveal many relevant data points helpful in such investigations (Tassone, Martini, & Choo, 2017). An email can be tracked down to the original destination or vice versa. Internet protocol addresses involved in network communication helps in the discovery of the geographical location of the criminals. As there are plenty of devices connected to a particular network, specialized tools such as FTK are used in the extraction of metadata from the devices. Data storage devices containing valuable information may be encrypted by the criminals. It will be hard for investigators to crack the encryption of any storage device based on the algorithms of encryption used by the criminals. Tools for extraction of metadata of files help investigators to build a dictionary of collected data that can in turn help in breaking the encryption of device.

**Hashing in Digital Forensics:**

There are many ethical issues in the collection and processing of digital evidence in investigations such as personal files may also be recovered as part of the data retrieval efforts. Hashing is helpful in limited cases of digital forensics. In one way hashing can be used to preserve the privacy of parties involved. Hash functions are algorithms that generate standardized output for any random stream of data. Such as a fixed length digital output is generated for any given file input in most of the hashing functions. An essential aspect of the hashing functions is that any hash of a file cannot be reverse engineered to the original file (S. Khan, 2017). However, metadata and necessary information about the file required for digital forensic can be obtained by analysis of the hash output. Another important characteristic of hashing is that for unique inputs unique hash values are generated, and for the same input, the same hash output will be generated by the function. This property of hashing discards the possibility of collisions in hash values. Meaning that no two different input values can have the same output hash values. This property is helpful in the identification of unique files.

On the other hand, besides protecting privacy, hashing utilities play a limited role in forensic investigations. Hash values cannot be reverse engineered back to the original file contents. This property makes hashing a limited resource in investigations. Exact file contents may be required for investigators to identify the criminal and hash values cannot help in this regard (Singh, Gaud, & Joshi, 2016). If any storage device contains the exact image of the criminal and only a hash value of the image file is retrieved by using file analysis tools such as FTK, then that hash value may not be of any use in investigation process due to the inability of reverse operation on the hash value.

**Protecting Integrity of Digital Evidence:**

Evidence collected during an investigation plays a central role in solving the case. As most of the cases are presented in a court of law, the integrity of evidence must be ensured to make it admissible in the court. Digital evidence is fragile as compared to other types of physical evidence. In digital forensic investigations, automated tools are utilized for evidence collection. These tools offer some functionalities to protect the integrity of the evidence. Chain of custody must also be preserved for a piece of evidence to be acceptable by the court of law. It must be appropriately documented that who owns the evidence from the point of collection to the presentation in the court of law (M. N. A. Khan, Ullah, Khan, & Khan, 2018). A single discrepancy or vague detail will make it difficult for investigators to prove that it was not tempered by unauthorized personnel. In a popular case, an engineer was sentenced by the court of law for four years in prison based on digital evidence against him pointing to the trafficking of child pornography. The victim then hired a computer expert who proved that the evidence was forged and tempered by unauthorized parties to prove the accused person as a criminal. Therefore, it is crucial to maintaining the integrity of the evidence after collection.

FTK is one of the popular tools that is used in digital evidence collection. The software is capable of creating disk images and storing critical metadata information about that. It provides some hashing functionality and cryptography algorithms to protect the integrity of digital evidence against tampering. However, there is a problem with the tool that it requires manual entry of the name of the investigator. Any person can enter the name of a fake person that will make the integrity of evidence questionable because it will not be possible to identify who actually generated the evidence using the tool. There are various other tools that are being used by experts to ensure the integrity of the evidence.

**References**

Ab Rahman, N. H., Glisson, W. B., Yang, Y., & Choo, K.-K. R. (2016). Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, *3*(1), 50–59.

Khan, M. N. A., Ullah, S. W., Khan, A. R., & Khan, K. (2018). Analysis of Digital Investigation Techniques in Cloud Computing Paradigm. *INTERNATIONAL JOURNAL OF NEXT-GENERATION COMPUTING*, *9*(3).

Khan, S. (2017). The Role of Forensics in the Internet of Things: Motivations and Requirements. *IEEE Internet Initiative ENewsletter*.

Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 71–80.

Mitchell, I., Anandaraja, T., Hara, S., Hadzhinenov, G., & Neilson, D. (2017). Deconstruct and preserve (DaP): A method for the preservation of digital evidence on solid state drives (SSD). In *International Conference on Global Security, Safety, and Sustainability* (pp. 3–11). Springer.

Singh, U. K., Gaud, N., & Joshi, C. (2016). A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity. *International Journal of Computer Applications*, *975*, 8887.

Tassone, C. F., Martini, B., & Choo, K.-K. R. (2017). Visualizing digital forensic datasets: a proof of concept. *Journal of Forensic Sciences*, *62*(5), 1197–1204.