Digital forensic

Business

Discussion Topic 1: What do you See as the Two Most Significant Challenges of Cloud Computing Facing Digital Forensics? The first challenge is insufficient and insecure storage space for the data collected. In conventional investigations, the availability of sufficient storage space is a compulsory prerequisite (Biggs & Vidalis, 2010). Various authors have noticed that the ever-growing volumes of data gathered during forensic investigations, which is driven by reduced costs and increased device capacity, are even more challenging for forensic investigators.

The increase in amounts of data imposes additional costs on investigators with the responsibility to curate and store data. The deployment of cloud computing intensifies the problem of data storage. A good aspect of cloud computing for users is the resilient capability to dynamically scale the storage abilities of services based on on-going prerequisites (Garfinkel, 2009). Another challenge facing digital forensic is the problem of deleted data. According to Householder, Houle, & Dougherty (2002), cloud computing can help or interfere with the attempts of forensic investigators to recover deleted information.

For instance, in conventional forensic investigations, information which a user tried to delete, though it still exists in a storage device, is frequently a rich source of evidence. However, the elasticity and volatility of cloud environments pose significant problems to the recovery of deleted information. What are Potential Ways to Handle these Challenges? The first problem can be solved through the deloyment of triaging techniques. These techniques reduce the volumes of data that need to be analyzed by a forensic investigator. According to Jankun-Kelly, Stamps, Wilson, Franck,

Carver, & Swan II (2009), the techniques are already being implemented to decrease backlogs in conventional investigations. Triaging techniques allow forensic investigators to perform analysis of the storage device within a short duration in order to recognize the most valuable evidence without conducting full investigation.

An example of a triaging technique is the Computer Forensic Field Triage Process Model (CFFTPM). This technique works by accessing the data stored in the home directory of a user of the file system. The home directory usually contains application centric information (Kessler & Schirling, 2002). The second challenge can be solved via the adoption of a directive. For instance, the European Union is encouraging its member countries to adopt one such directive, which is called the Data Retention Directive (Marziale, 2009). Such directives should ensure that communication providers retain data concerning the user's ID, IP address at the time of communication, and the date and time of both log-in and log-off.

Such information might facilitate the real suspects who deleted evidence. Discussion Topic 2: How might Link and Visual Analysis Tools be Incorporated into a Digital Forensics Environment to Make Investigations More Effective? Link and visual analysis tools are very important for forensic investigators to filter through information in order to find evidence (Jankun-Kelly, Stamps, Wilson, Franck, Carver, & Swan II, 2009). According to Householder, Houle, && Dougherty (2002), link analysis tools survey and visualize the key structures and nodes within a network, which, according to Jankun-Kelly, Stamps, Wilson, Franck, Carver, & Swan II, (2009), are a collection of related information. They are essential tools used in forensics for examining the

relationships in information when investigating very complex cases, for instance, fraud, which involve huge volumes of information. According to Marziale (2009), link and visual analysis tools explore huge amounts of data of potentially different records and create a relationship between these records based on data fields with related or similar values. These tools use artificial intelligence to establish the relationship between data records (Jankun-Kelly, Stamps, Wilson, Franck, Carver, & Swan II, 2009).

This reduces the volume of data that forensic investigators analyze. What other Non-DF Tools may also Improve the Effectiveness of a Digital Forensics Investigation? Creating and maintaining guidelines and procedures for conducting forensic tasks according to the policies of an organization can significantly improve the efficiency of digital forensic. The guidelines and procedures need to clarify on the circumstances under which forensic should or should not be performed. According to Jankun-Kelly, Stamps, Wilson, Franck, Carver, & Swan II (2009), the guidelines need to describe the required protections for sensitive data, which might be recorded by forensic tools, like personal data, passwords, and social security number. The policies and procedures of an organization on the deployment of forensic tools should address the use of anti-forensic techniques and tools (Biggs & Vidalis, 2010).