

# CONCEPTUALIZATION PRINCIPLES OF DIGITAL FORENSICS ANALYSIS FOR CYBER WARFARE

<sup>1</sup>Waziri Onomza Victor, PhD, <sup>2</sup>Lukman Ibrahim, <sup>3</sup> Matthew O. Adigun, PROF

<sup>1,2</sup> Department of Cyber Security, Federal University of Technology Minna, Nigeria,.

<sup>3</sup>University of Zululand, Centre for Excellence, Computer Science Department, KwaDklangezwa Campus, South Africa,

## **Abstract**

*Cyber crimes activities have become a worst-important part of everyday life of both corporate world and the general public. The digital crime phenomenon has achieved what one may call the overwhelming factor. In this paper, we propose a more efficient solution to perform a safe screening of the target systems and take only the relevant data and systems to the lab. Such screenings can be performed by using soft computing heuristics and communication resources of the targets. The paper further explores the field of digital forensics as*

*applied to cyber warfare, mainly for defensive and intelligent operations especially algorithmic crimes that are data related which requires collection and collation of fact for evidences. It reviews various digital forensics investigations and uses open source tools that give justification for their applications. We present the Bluepipe concept for an on-the-sop forensic investigation in a non-invasive way that is sensitive to privacy instead of removing suspect machines from site for a Laboratory based investigation processes.*

**Keywords:** Digital Forensic, Bluepipe, cyber warfare, preservation, vulnerabilities

## **1. Introduction**

Current approach to forensics investigative evidence on impounding suspect's computer or allied media and examine them in a Forensic laboratory where all analysis are carried out on a copy of the original evidence obtained poses several problems. This practice are heavyweight and becoming more expensive by the day thereby making enterprise who are the victim of digital crimes become more worried and more defensive for not allowing forensic practice to achieve its full potentials [1].

Digital forensics investigators have access to a wide range of tools, both commercial and open source, that assist in the preservation and analysis of digital evidences. Unfortunately, most current digital forensics tools fall short in several ways such as electronic evidences to validate the issue under investigation; also most evidences lack international criminological laws to cover all countries jurisdiction boundaries. Today, computer systems are often invaluable for businesses and in most cases, personal services. Computer systems store valuable resources for corporate institutions and personal information. Besides, Computer networks provide convenient data access and processing services. These aforementioned make them to become naturally very tempting targets; as shown by statistics that track the frequency and prevalence of cybercrimes. In recent times, the Federal Bureau of Investigation (FBI) and Crime Scene Investigators (CSI) are working on various strategies and are updating them from time to time in order to be up-to-date in their technologies

innovations not to be left behind by the growing array of attackers on Cyber highways. For example, a CSI/FBI survey found that 71% of organizations had experienced at least one attack in 2004, while the remaining organizations did not know the number of attacks [ibid].

The simplicity of carrying out digital attacks is compounded by the temptation for attackers' frequent up-to-date advancement. It is a public assumption that computer systems have numerous vulnerabilities, although not every attack exploits vulnerabilities [2].

In the second half of 2004, over 54 new vulnerabilities per week were discovered on the average, and over 50% of them were so serious to the extent that it was rated as very severe, which was interpreted to mean that exploitation of the vulnerability could lead to complete compromise of a system [3]. Attackers are usually aware of new vulnerabilities because it takes time for organizations to set up adequate protection against such vulnerabilities; and in most cases, the organization is oblivious of the vulnerabilities existence. New vulnerabilities are announced along with a software patch, but organizations are sometimes slow to either download or acquire and apply those patches for their protection. In late 2009, exploit codes for new vulnerabilities appeared on the average after the announcement of the vulnerability. Organizations that are slow to download and implement patch are often vulnerable to new exploits.

Attackers are also well aware that virtually all computers are interconnected by the Internet or private networks. Moreover, the growth of mobile and handheld sophisticated

digital devices with Internet connectivity is sending serious signals to security issues in one hand and creating more potentials for the attackers thereby making more people and their electronics garget more vulnerable. The new waves of Networks of things make even make it more terrified as the attackers to carry out so many unimaginable hits on their targets remotely and are more difficult to track to their roots.

A wide variety of digital forensics tools, both commercial and open sources, are currently available to digital forensics investigators and it is a good news to state that as the awareness for needs for digital evidence is increasing more tools will become more available because open source software initiatives teams are subjecting their codes and patches to open criticism and open contributions without compromise. These tools, in various ways, provide levels of abstraction that allow investigators to safely make copies of digital evidence and perform routine investigations, without becoming overwhelmed by low-level details, such as physical disk organization or the specific structure of complicated file types, like the Windows registry. Many existing tools provide an intuitive user interface that turns an investigation into something resembling a structured process, rather than an arcane craft.

A study by the University of California, Berkeley in 2006 indicates that 93% of new information created today is in the digital format. Computers are involved in today's crimes in diverse ways, as reported by the President's Working Group on Unlawful Conduct on the Internet [4]. Computers can be targets of the crime where the damage is done to the integrity, confidentiality, and/or availability of the information stored in the computer. Unauthorized access is gained to a target system in order to acquire information stored in it or to disrupt its normal operations. In a second way, computers can be used as data storage devices to store stolen credit card numbers, social security numbers, medical records, proprietary information, and more.

In the section of this paper, we discuss previous works that has been carried out of digital forensics with a review on relevance of digital forensics in section two. Preservation of evidence for legal proceeding in a law court was discussed in section in the first part of section three, also in the second part of section three, we discussed various challenges of digital forensics with view to compare conventional paper evidence and digital evidence.

We also discussed various steps in digital forensic with a model to illustrate the conceptualization of digital forensics. In section four, we discussed various digital forensics tool kits and enumerate on some popular toolkits for the purpose analyzing the weakness existing digital forensics technique and potentials of Bluepipe Architecture to ameliorate the challenges of digital forensic for its development as the

technology improves and creating an emerging market for sophisticated and intelligence digital media for data manipulation and storage.

### **2.Previous works of Digital Forensics**

Digital forensics was developed during the first Digital Forensics Research Workshop (DFRWS) in 2001 and it was defined as the use of scientifically derived and proven method of preserving, collecting, identifying, validating, interpreting and analyzing documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be destructive to a planned operations [5]. This formulation stresses the scientific nature of digital forensics methods, in a point in time when it was transitioning from being a craft to an established field and rightful part of the forensic sciences.

A large number of high quality commercial version and open source software tools has long been in existence for performing digital forensics investigations. Although their data handling capacity vary since they are based on image processing paradigm, where the original of the suspected target image is first obtained including all the manipulations done on such image. Such tool was been refers to as Direct access tool because they usually provide a self-contained environment to enable investigator examine the digital evidence from the source [5].

### **3. Relevance of Digital Forensic**

Computers can otherwise be used as communication tools where e-mails and chat sessions enable planning and coordinating many crimes. Sometimes computers can be used to communicate threats or extortion demands. When a computer security incident or a computer crime is suspected, an investigator uses forensic tools to search through voluminous data for proof of guilt or innocence.

Digital forensics is a methodology to acquire and analyze evidence in the digital format. Note that the nature of digital evidence is such that special procedures for obtaining and handling this evidence are required. Electronic evidence may be easily altered unless strict procedures are followed. For example, rebooting a system may cause the loss of any information in volatile memory and destroy valuable traces.

From the general perspective, the objective of digital forensics in a warfare situation is very different from what is needed in the civilian society, a sound evidence, to be used in a court of law (civil or criminal) or at least that can be used, in principle.

### 3.1 Preservation of Evidence

As computer and computing devices or other electronic devices with computing capability such as PDA and smart mobile phones and networks becomes more widely used both in work places, social centres and other general places, the chances that crimes involving the use of digital devices and networking tools (cyber crimes) occur will surely be on the increase.

The above submission goes without saying that in order to prosecute crimes, evidence must be first of all be gathered both in adequate quantity in order to substantiate any criminal or civil charges and properly handled so that such evidence with hold in court of law but such evidences must also be captured in a manner that justify its integrity for justice. However, as long as all of these evidences will be in a digital form, the ability to extract such digital evidence in a manner that preserves their true value and their actual integrity is critical.

On this note, it is therefore very important to state in this paper categorically that the ability to retrieve and preserve data plays an essential role in the prosecution of a case and it is important that anyone gathering such data should know where to find it, gather it, how to properly preserve such evidence otherwise it will lose its original value. In order to ensure that digital evidence is admissible in a law court, it must be generally proved that the evidence is both authentic and has not been modified in any form. For example, if an investigator copies a transaction from a client for the purpose of investigation, between when the file is copied and when it gets to his/her system for further work/analysis, such data has lost its integrity ab-initio. However, in order ensure that digital evidence is admissible in a court of law, such data must be generally be proved that it is both authentic and has not been modified.

### 3.2 Challenges of Digital Evidence

Since electronic data is clearly different from the traditional paper documents, it is therefore needed to be handled accordingly.

#### 3.2.1 Paper documents and Electronic documents

Electronic documents are created at a very higher rate nowadays than the regular paper works because of the high acceptability of the digital world, we are all aware of the paperless works environment, even in the developing and underdeveloped nations across the globe. All over the world today, over 7.5 trillion of E-mails messages are generated around the United State of America alone each year in addition to all other electronic files that are generated such as Electronic Spreadsheets, database records, word processing documents, graphic files and even the voice messages file.

Almost everyone will agree that electronic documents are more easily replicated and changed than the regular paper documents. We believe that normal paper documents can be copied, however, copying physical documents results in degradation with each copy you make. In the case of electronic information, it can be subjected to rapid and large scale user-created and automated replication without degradation of the original data.

Unlike the conventional paper file discovery, electronic documents may not be easily identified for reproduction because the documents itself are usually stored randomly on a various type of storage medium on the host system. As a result of these, forensic investigators may need to thoroughly review each document indecently, not just the file.

It should also be noted that digital based information, unlike paper based information has dynamic contents that may be design to change over a period of time even without any further human intervention. For example, a web page that are constantly being updated with records of information from other online application or those intelligent e-mails that can reorganise and adjust data automatically, even with colors.

Digital evidence is evidence that has some kind of connection to computers and other digital devices. Digital files that show evidence of a physical crime include JPEGs showing child exploitation, Excel files tracking drug sales, Emails documenting a conspiracy among others.



Excel File



Email File



Personal Computer

Physical evidence unlike digital evidence may also include Blood and DNA, Bullets, Guns and Ballistics, Tire Tread marks, foot prints, collated photographs are all based on physical objects.

Therefore, digital forensic experts must take cursory measure to protect all digital evidence from any deliberate or inadvertent changes or modification. Otherwise, the digital evidence collected may not be considered valid as evidence for legal proceedings unless it is handle in a forensically manner.

### 3.3 Steps in Computer Forensics

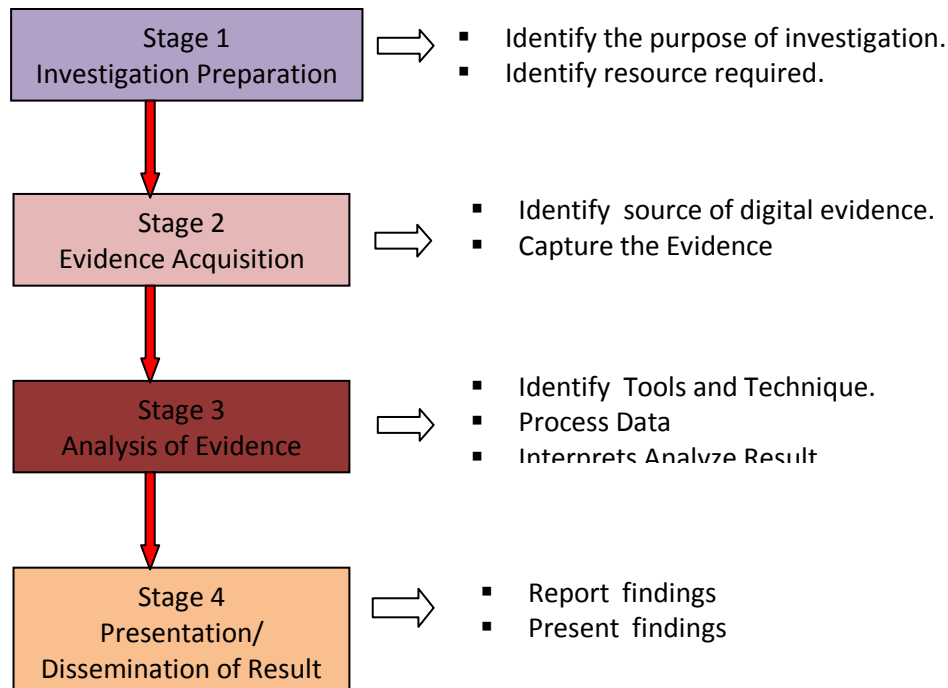
There are many steps in a computer-related investigation for the retrieval and analysis of digital evidence. In this paper, we identified, three main steps, which we called the three A's, in the investigation process:

1. Acquire

2. Authenticate
3. Analyze.

Figure 3.1. It shows a typical digital forensic investigation stages. The actual tasks that are involve in each of the stage are further illustrated in Figure 3.3.1.

The first three steps and the final step of Presentation/Dissemination are elaborated upon further in



**Figure 3.3.1: Digital Forensic Stage Model**

However, from the forensics actual real life scenario when a suspect drive is obtained from a seized computer, a copy of the drive is made.

The copy is then analyzed to identify available valuable evidence such as log files, deleted files, modified files and etc. Analysis of identified evidence yields reconstructed files or other useful information. That process is further illustrated in Figure 3.2.2 below. From Figure 3.3.2, we can see that the suspect computer system (Seized PC) and media device (Suspect Drive) can be mirrored to enable the investigator do a proper analysis of available document files, E-mail among other related cyber crime committed acts perpetrated by the suspect.

Activities in Figure 3.3.2 further gives a clearer details of events that was conceptualized in Figure 3.3.1 above.

### 3.4 Digital Forensic Tools

Computer examiners use several different types of tools to identify and attain computer evidence. Forensic tools have been developed for the various steps of forensic analysis as previously described in this paper. There are many different tools available to use for forensic analysis.

There is no single solution for all the diverse requirements of a computer forensic investigation. The tools have been developed for different operating platforms. Some tools are open source tools while others are proprietary. Different tools exist for performing evidence acquisition from live systems and analyzing the evidence. Some commonly used computer forensics tools includes the following:

#### 3.4.1 Imaging Tools

Among these are: EnCase, Safeback, Norton Ghost, iLook, Mares, SMART, ByteBack, SnapBack, Drive Image, X-Ways Forensics among others.

#### 3.4.2 Digital Forensic Analysis Tools

Forensic analysis activities differ based on the type of media being analyzed, the file system used, and so on. Some activities involved in forensic analysis were discussed in prior passages. Some of the widely-used analysis tools are further described in Forensic Toolkits below.

#### 3.5 Forensic Toolkits

Current tools, such as the Forensics Toolkit (FTK) from AccessData Corp., attempt to reduce the need to read an

entire forensics image repeatedly (e.g. for each search operation) by performing an initial preprocessing step that builds index structures to speed up keyword searches, disk carving, and to provide file categorization [11]. While this technique is effective in many scenarios, it is limited by the computational resources available on a single workstation. First, it may take several days just to perform the preprocessing step. Second, the system indexes only strings that it judges to be of use in the investigation: for example, character sequences that appear to be similar to English words and those that are useful for file carving. Regular expression searches, as well as simple searches for character sequences that are not in the index, such as words in foreign languages with different encoding, still require an exhaustive examination of the entire target image.

On targets of hundreds of gigabytes or terabytes, investigators may (necessarily) be disinclined to perform searches that may take days of execution time, particularly as caseloads grow. Finally, the index structure of a large target will also become large, which will prevent it from being kept in main memory.

Generally, there are two possible approaches to improve machine scalability, improve the efficiency of the algorithms and their implementations to get more from the current hardware platforms or enable the use of more machine resources in a distributed fashion. These two approaches are to a great extent complementary, however, the former is likely to yield only incremental improvements in performance, whereas the latter has the potential to bridge the hardware performance gaps discussed earlier.

As already discussed above, any kind of digital forensics analysis is inherently I/O-constrained because of the need to process vast amounts of data, however, it can also become CPU constrained if more sophisticated analytical techniques, such as automatic image classification, are used. A distributed solution can address both the I/O and the CPU constraints. For example, a 64-node Beowulf cluster with 2GB of RAM per node can comfortably cache over 100GB of data in main memory. Using such a system, the cost of the I/O transfer of a large forensic image can be paid once and any subsequent I/O can be performed at a fraction of the cost. Taking the idea a step further, the data cached by each node can be made persistent so that if the system needs to shutdown and restart, each node need only autonomously read in its part of the data from a local disk. At the same time, having multiple CPUs performing the CPU-intensive operations obviously has the potential to dramatically improve execution time [6]. Reviews on some major digital forensics tools includes the following:

#### **SafeBack**

SafeBack is an industry standard self-authenticating computer forensics tool commonly used by law enforcement agencies throughout the world. It is a DOS-based utility used to create evidence grade backups of hard drives on Intel-based computer systems.[6] SafeBack copies all areas of the hard disk accurately. Remote operation via parallel port connection allows the hard disk on a remote PC to be read or written by the master system.[9]

#### **DriveSpy**

DriveSpy is a forensic DOS shell. It is designed to emulate and extend the capabilities of DOS to meet forensic needs. It can examine DOS and non-DOS partitions using a built-in sector (and cluster) hex viewer. Configurable documentation capabilities are included in DriveSpy to record all the activities of an investigation. DriveSpy can save and restore compressed forensic images of a hard drive. MD5 hash of an entire drive, a partition or selected files can also be obtained. Using DriveSpy, extensive architectural information for entire hard drives and individual partitions can be obtained [12].

#### **4. The Bluepipe Architecture for On-the-Spot Live Digital Forensics**

The Bluepipe Architecture concepts identified numbers of challenges on the existing approaches to digital forensics such as physical movement of computer and allied equipment from client site to a forensics lab. It is often noted that the safety of such computer can not be guaranty in actual sense, such computer can be easily damaged, not all data are relevant to the proposed investigation. From economic perspective, most of the enterprise today are highly dependent on their IT infrastructure for their daily operations, imagine retrieving a data server from a major commercial bank for the purpose of forensic investigation, there would be natural reluctance by the users to shut down operations for forensics investigation purposes, among others [1] [7]. The application of Bluepipe Architecture provide opportunities for various on-the-spot assessment to cyber related crimes. This scenarios though is similar to the previous one but it provide a better and meaningful usage both on the part of ICT infrastructure since they are advancing almost everyday, therefore potentially more valuable inquiry can be effectively carried out forensically.

Bluepipe architecture provides for Portability and Scalability of investigation. Scalability in the sense, the challenges of scale in digital forensics activities can be perceived from two major points.[9] First, an increased scale of investigative target and an increased number of independent investigation. Secondly, scalability problems usually call for different approaches to ascertain a presentable evidence before the law court.[18]

The first scenario look more like a classical problem of scale of distributed application where the concurrent activities of large number of computer equipment are effectively and efficiently coordinated [1]. The second one represents what look like human related problem of scale in which there is an increase in the number of potential investigative suspected device that outpaces the increase in the number of people dealing with them[1,6]. This means that even in the developing nations, it is obviously important that technological Enterprise Resource Program (ERP) solutions for digital forensics work become available to a large numbers of law enforcement officers. This will enable forensically trained security agents conduct preliminary inquiries in a smaller community even from remote locations.

In other cases, the forensic target might be a huge fileserver, whose operation is critical for the well-being of a business enterprise. Performing an imaging operation on every machine in a large laboratory setting will be a very daunting task, as will be imaging a multi-terabyte fileserver [10] [7]. Even if logistical problems with the imaging process are overcome, a huge interruption of service is obvious during a traditional imaging operation, during which normal operation of the computer systems is impossible. Finally, analyzing the drives of a large group of machines (or of a terabyte fileserver) will consume considerable resources.

The Bluepipe Architecture avails a more efficient solution is to perform a safe screening of the target systems and take only the relevant data and systems to the lab. Such screening can be performed by using the local computational and communication resources of the targets. A straightforward solution that overcomes some (but not all) of the logistical problems described above is the creation of a better imaging tools, where files that are not interesting (e.g., operating systems files or file types irrelevant to an investigation) are not included in the captured image. In many cases, however, the number of files that might be excluded may be rather small, in comparison to the size of the entire target. Thus, other approaches should be explored, in addition to creating better drive imaging tools. The Bluepipe architecture [11] permits an on-the-spot investigator to perform simple queries and to capture and preserve digital evidence, using only a small amount of hardware (e.g., a PDA or laptop).

Bluepipe make use of client/server architecture, with a server running on the target machine and one or more Bluepipe clients controlling the investigation process. Client and server communicated via a SOAP-based protocol. Bluepipe clients may also serve as a proxy, which allows remote investigators to gain remote access to the target over a trusted connection, as well as collaborate with investigators right on the spot.

To begin an inquiry using the Bluepipe architecture, an investigator performs several steps: she plugs in USB dongles to enable wireless communication with the target computers, boots the target computers using Bluepipe boot CDs, and launches the Bluepipe client application on her PDA or laptop [1]. The Bluepipe boot CD invokes the server-side Bluepipe application, initializes the connection between client and server, and exposes the secondary storage devices of the target to the Bluepipe server application.

The investigator then uses the thin client Graphical User Interface (GUI on the Laptop, iPhone or PDA to issue queries and receive results [14]. All processing on the target side consists of collections of read-only operations which we refers to in this paper as Bluepipe patterns against the secondary storage on the target machine. An audit log tracks all operations performed on the target, this log is transmitted to the client at the end of the inquiry.

Because some investigatory operations are expected to complete quickly and some require substantial processing time, Bluepipe supports both synchronous and asynchronous communication.

All Bluepipe patterns preserve the state of secondary storage on the target machine. Supported pattern operations include checking for existence of files with specific names or hash values, searching files for keywords, retrieving files, and generating directory and partition table listings. Bluepipe patterns are stored on the client and transmitted to the Bluepipe server for execution as they are selected by the investigator. Results of the pattern execution are then transmitted back to the client [12].

The following pattern was used to obtain a partition table listing of a target with a single IDE hard drive to demonstrate the Bluepipe pattern:

```
<BLUEPIPE NAME="partitions">  
<!-- get a lot of drive/partition info-->  
<LISTPARTITIONS LOCAL="drives.txt"  
GENHASHES=TRUE/>  
</BLUEPIPE>
```

The result of executing this pattern, a text file named "drives.txt", illustrates that the target machine's single hard drive contains five partitions with at least two operating systems installed:

```
hda  
Model No: IC25T060ATCS05-0.  
Serial No: CSL800D8G3GNSA  
device size with M = 1024*1024: 57231 Mbytes  
Partition table:  
Disk /dev/hda: 240 heads, 63 sectors, 7752 cylinders
```



```
Units = cylinders of 15120 * 512 bytes
Device Boot Start End Blocks Id System
/dev/hda1 1 6173 46667848+ 7 HPFS/NTFS
/dev/hda2 7573 7752 1360800 1c Hidden Win95 FAT32
(LBA)
/dev/hda3 * 6174 7364 9003960 83 Linux
/dev/hda4 7365 7572 1572480 f Win95 Ext'd (LBA)
/dev/hda5 7365 7572 1572448+ 82 Linux swap
MD5 hash for drive: 463e65ec8d9f51bdd17c0347243f467b
```

The next pattern, named “findcacti”, searches for pictures of cacti using a hash dictionary[12]. A single target directory is specified, “/pics”, which is searched recursively [12]. Files that match are retrieved and stored on the client in a directory named “cactus”. No file size restrictions are imposed [11]. The %s and %h placeholders in the message will be replaced by the filename and hash value of each matching file:

```
<BLUEPIPE NAME="findcacti">
<!-- find illegal cacti pics using MD5 hash dictionary -->
<DIR TARGET="/pics/" />
<FINDFILE
USEHASHES=TRUE
LOCALDIR="cactus"
RECURSIVE=TRUE
RETRIEVE=TRUE
MSG="Found cactus %s with hash %h ">
<FILE ID=3d1e79d11443498df78a1981652be454/>
<FILE ID=ab348734f7347a8a054aa2c774f7aae6/>
<FILE ID=b57af575deef030baa709f5bf32ac1ed/>
<FILE ID=7074c76fada0b4b419287ee28d705787/>
<FILE ID=808bac4a404911bf2faca911651e051/>
<FILE ID=fffbf594bbae2b3dd6af84e1af4be79c/>
<FILE ID=b9776d04e384a10aef6d1c8258fd054/>
</FINDFILE>
</BLUEPIPE>
```

The result of executing this pattern on a target appears below. Notice that the DSC00051 and bcactus5 image files have identical content:

```
Beginning execution for pattern "findcacti".
DIR cmd, added "/pics".
FINDFILE cmd.
Found cactus /pics/BBQ-5-27-2001/DSC00008A.JPG with
hash
6f5cd6182125fc4b9445aad18f412128
Found cactus /pics/BBQ-5-27-2001/DSC00009A.JPG with
hash
7de79a1ed753ac2980ee2f8e7afa5005.
Found cactus /pics/CACTUS_ANNA/DSC00051.JPG with
hash
3d1e79d11443498df78a1981652be454.
```

```
Found cactus /pics/GARDEN2002/bcactus5.JPG with hash
3d1e79d11443498df78a1981652be454.
Pattern processing completed.
Sending pattern log. Remote filename is
"findcacti.LOG".[12]
```

Ultimately, tools like Bluepipe do not attempt to replace traditional methods in digital forensics, instead, they improve the triage process and also improve the efficiency of digital forensics investigators. Another type of tool, which also improves triage but operates on live machines, is described below.

An interesting trend in next-generation of digital forensics is “live” forensics investigation, we realized that analysis of machines that are allowed to remain in operation as they are examined[21].

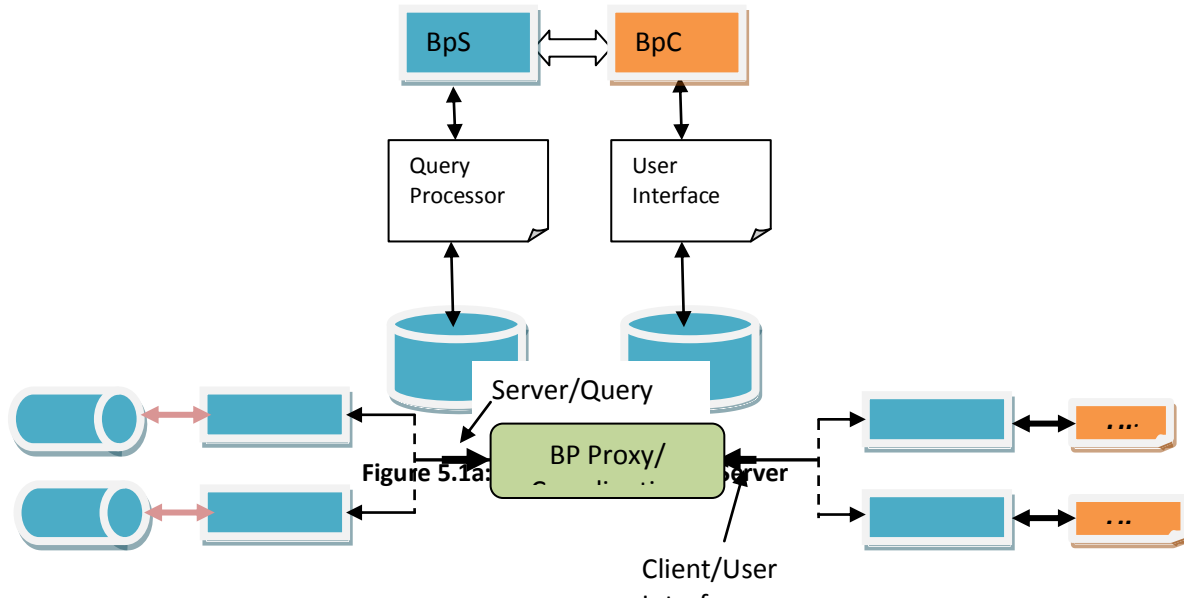
The idea is appealing, particularly for investigation of mission-critical machines, which would suffer substantial downtime during a typical “dead” analysis. The mobile forensic platform [21], now called the OnLine Digital Forensic Suite in its commercial incarnation, allows live investigation of computer systems, permitting an investigator to obtain evidence to perform a thorough examination remotely. The researchers observe, quite correctly, that in large computer networks, unauthorized activity can have devastating consequences and must be dealt with very quickly. Unfortunately, most organizations simply do not have the staff to examine each local network potentially involved in an attack[21]. In addition, in any geographically dispersed organization, the less time the investigators spend traveling, the more time they have to investigate the incident. The MFP is a network appliance, deployed on an organization’s local network, which exposes a secure, Web-based investigative interface to an organization’s computers [16]. The machines may be investigated while they perform their usual functions, without raising the suspicion that they are under investigation.

#### 4.1 The Basic Bluepipe Architecture

The basic architectural approach in this paper is based on the client/server paradigm and is described in Figure 5.1 The Bluepipe server (BpS) runs on the target machine while a Bluepipe client executes on the investigator’s machine, establishes a connection to the server, and issues queries to access the investigating machine. The communication between the two parties is managed by a SOAP-based communication protocol. The overall implementation of the current prototype is outlined below. At this point it is noted that the server software boots from a write-disabled version of Linux on a memory or a partition, mounts the hard disk of the target machine, and per-forms the requested queries.

The major responsibility of the Bluepipe server is to implement the server side of the Bluepipe protocol and to translate the received queries into invocations of smaller module as shown in the script below. The primary responsibility of the Bluepipe client (BpC) is to translate into the Bluepipe protocol that can queries the submitted by the investigator. Typically, these will come from the inter-face of the user's module running on the client machine as demonstrated in Figure 5.1a. Similarly, a Bluepipe

implementation may also become a proxy server by implementing the Bluepipe server (BpS) interface part as shown in Figure 5.1b below. This allows a remote client that does not have a direct connection to the target machine to gain indirect access. By allowing multiple clients to connect to it, a proxy server can also serve as a coordination server among a group of clients by dispatching the submitted queries to different investigating or target machines (Figure 1b).



**Figure 5.1: Bluepipe Architecture [Figure 5.1a and Figure 5.1b]  
Figure 5.1b: Multiple Client/Multiple Server**

Another function of the coordination server as indicated above in Figure 5.1b is to provide generic collaborative features that facilitate teamwork, such as:

- i. Selectable degrees of coupling among the displays of client machine; that is, controlling the degree to which view of different users are allowed to diverge.
- ii. Enforcement of specific concurrency and access control policies, such as ensuring that no conflicting operations are submitted in parallel and that certain actions are only executed by privileged users.

**5 Future Trends and Next Generation**

The field of computer forensics is still nascent. Tools are continually being developed to handle electronic content and the diverse operating environments. The US Department of Justice in a recent report identified finding information in the information ocean, anonymity, traceability, and encryption as the four major challenges in relation to forensic evidence collection and analysis[20]. Finding valuable evidence from the massive amount of information is nearly impossible. Digital evidence may be found in

monolithic computers, or in a distributed form in multiple computers.[24] Computer networks allow people to have a false identity thereby maintaining anonymity. This anonymity is misused by some sophisticated users who commit unlawful acts. With the computers connected to the Internet, evidence may be spread across several jurisdictions and vast geographical distances. Law enforcement agencies in different jurisdictions will have to cooperate and coordinate in the evidence collection process. Computers are increasingly embedded in larger systems with more sophisticated methods of storing and processing data[23]. Evidence collection from such systems is complicated and presentation of the collected evidence in court is a daunting task. Traceability, which deals with establishing the source and destination of computer-based communications, is very difficult to achieve because of the diversity of the Internet. Cryptography presents an additional threat to forensic analysis. Robust encryption tools can be installed easily and allow the criminals to communicate and store information in a form that is not easily accessible to law enforcement[22].



For subsequent forensic analysis, the detection of steganography software on a suspect computer is important. Many steganography detection programs work best when there are clues as to the type of steganography that was employed in the first place [24]. The next generation of digital forensics tools will employ high performance computing, more sophisticated data analysis techniques, and better collaborative functions to allow digital forensics investigators to perform examinations much more efficiently and to meet the challenges of massive data sets. In this chapter, we examine some of the technical issues in next-generation tools and discuss ongoing research that seeks to address them.

Integrated evidence gathering and analysis tools are being developed. Note that there is no complete solution for all forensic needs. Very few tools are validated and approved for use in legal proceedings. Currently there are no standardized procedures for conducting computing investigations.[23] Also, there is a shortage of skilled forensic examiners and a lack of standard certification processes. An effective forensic investigator must be familiar with systems administration practices and have a fundamental understanding of computers, operating systems, databases, and computer networks. An increased awareness of the legal issues involved in a computer forensic investigation is also essential.

A variety of portable devices such as cell phones, PDAs, among others, is used today for data communications, and can have valuable digital evidence. Development of new forensic tools for analyzing the storage media of such portable devices is gaining impetus. Computer forensic techniques and tools should adapt well to new technology products and innovations [5]. Automated techniques for detection and prevention of malware such as viruses and worms are being developed.

## **6. Conclusions**

The Computer forensics is an increasingly important field that requires one to possess an intricate mix of technical skills, legal knowledge, and ethical behavior patterns. Specialists in this field have very powerful software tools at their disposal which will uncover a myriad of data to be sorted through, and it is up to the specialist to figure out what the important facts are and how to present them appropriately in a court of law.[15] Even though the software tools are generally praised for their effectiveness, the statistics show that an improvement in the overall methodologies used in computer forensics is required. The FBI has made it known that in the year 2010 there were 6,032 cases opened in various law courts involving various cyber crime. Of those cases, only 971 were closed, the rest are still under litigations. Of those closed cases only 94

convictions were handed down in court. This is an alarming statistic, but it should not be surprising considering that the field is still in its infancy[17]. As technologies expand, more powerful and versatile software tools will be required, and more well-trained Computer Forensic Specialists will be needed because cyber crime is exploding and computer forensics is the vital discipline that has the power to control this outburst.

This paper reviewed and identified digital forensic and various tools to be used for forensics investigation as application for Cyber Warfare context. The various steps involved in a forensic investigation have been outlined. Some popular computer forensic tools and network forensic toolkits have been described in detail[24]. Although a number of tools are available today, few tools have been validated for providing evidence that can be used in a law court. In addition to developing more sophisticated forensic analysis tools, the focus of future research will be the integration of digital forensic techniques with mainstream computer and network security techniques by using open source based applications.

Security operatives and agencies around the world should intensify efforts in ensuring that more security officers are equipped with up-to date digital garget to access suspected electronic communication devices used for perpetuating cyber related crimes from remote location.



## **References**

1. Yun Gao and Golden G Richard, 2010, Scalable Architecture for On-the-Spot Digital Forensics, Department of Computer Science, University of New Orleans.
2. (Gordon, 2008). "Cyberwar- Probleme für die internationale Politik ", Universität Osnabrück. ISO/IEC (2012), "
3. Pearson, G. (2006), A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, NY.
4. Introduction to Computer Forensics, 2005, Information Security and Forensics Society (ISFS).
5. Jenkinson, B. L. (2005) The structure and operation of the master file table within a Windows 2000 NTFS environment, MSc Thesis, Cranfield University.
6. 2007, Digital Crime and Forensic Computing, Panagiotis Kanellis and Evangelos Kiountouzis, Athens University of Economics & Business, Greece.
7. International Journal of Digital Evidence (2007)
8. Arbitration. (2004). The use of computer forensics in arbitration. Online Security.



9. Pearson 2007 Operational Information Security. Information Networks Division. Defense Science and Technology Division. CFIT User Manual.
10. Farmer, D., & Venema, W. (2005) The coroner's toolkit (TCT). Retrieved April 2005.
11. Goel, A., et al. (2003). Forensix: A robust, high-performance reconstruction system. The 19th ACM Symposium on Operating Systems Principles (SOSP). New York: ACM Press.
12. Gomez, R., Adly, A., Mayergoyz, I., and Burke E. (2007) Magnetic force scanning tunneling microscope imaging of overwritten data. Magnetics, IEEE Transactions on, 28(5),3141-3143.
13. Mandelecha, S. (2005). A prototype digital forensics repository. M.S. thesis, Department of Computer Science, University of New Orleans.
14. Roussev, V., & Richard, G. G. III (2007). Breaking the performance wall: The case for distributed digital forensics. In Proceedings of the 2007 Digital Forensics Research Workshop (DFRWS 2009).
15. Information Security Governance: A Call to Action, National Cyber Security Summit Task Force. (2007).
16. Carrier, B. (n.d.). Open Source Digital Forensics Tools. Retrieved February 7, 2005.
17. CyberSecurity Institute. (2004). Code of Ethics and Conduct. Retrieved February 14, 2005.
18. `EnCase Enterprise Edition. Retrieved February 4, 2005.
19. Isner, J. D. (2003) Computer Forensics: An Emerging Practice in the Battle Against Cyber Crime. Retrieved February 8, 2005.
20. Paraben Forensic Tools. Retrieved February 4, 2005, from <http://www.paraben-forensics.com/catalog/>
- Radcliff, D. (2002). Cybersleuthing Solves the Case. Retrieved February 9, 2005
21. An Explanation of Computer Forensics. Available at <http://www.computerforensics.net/forensics.htm> SearchSecurity.com Definitions. (Jan.14, 2005).
22. Solomon, Michael G., Barrett, Diane and Broom, Neil. (2005). Computer Forensics Jump Start. San Francisco: Sybex. The DIBS Group. (2004). The DIBS Methodology. Retrieved February 5, 2005

**Bibliography of Authors**

	<p>Victor Onomza Waziri obtained his BSc/Ed (Maths) from Usmanu Danfodiyo University Sokoto (1990), M. Tech (Applied Mathematics) and PhD (Applied Mathematics) based-on Computational Optimization in 1998 and 2004 respectively From the Federal University of Technology, Minna-Nigeria. He did his PostDoctoral Fellowship in Computer Science at the University of Zululand, South Africa in 2007. He is the Current Head of Cyber Security Science, Federal University of Technology, Minna-Nigeria. His research works are in the fields of Computational Optimization, Modern Cryptography, CyberSecurity/ Malware Detection, Mobile Cloud Computing Security, Programming and Network Security. He has published many academic papers at both local and International Scene</p>
	<p>Ibrahim Lukman hold a Bachelor of Technology in Mathematics/Computer Science from Federal University of Technology, Minna in 2006. He is an Oracle Certified Administrator. He started his career with NEXIM Bank Headquarters Abuja. He has worked as Head of ICT and later became Consultant Assistant with DACA Consults and moved to Springsoft Solutions Nigeria to head the Sage Accounting software products Implementation and Training where he was actively involved in ICT process Audit and implementation of Sage Accounting software to meet the needs of various business sectors. In 2011, he joined the services of the Federal University of Technology, Minna as a Senior Web Specialist in the Centre for Open Distance and E-Learning. He is presently undergoing his Master Degree in Cyber Security Science in Federal University of Technology, Minna. Lukman has special interest in E-Learning Management, E-Commerce Security, Forensics Investigation and Systems Auditing.</p>



Prof. Matthew O. Adigun is an outstanding and accomplished Professor of Software Engineering. He obtained his BSC, MSC and PhD at the renowned University of Ile IFE; now Obafemi Owolowo ILE IFE, Nigeria He the current Head of Computer Science at the University of Zululand, Republic of Soth Africa. Has published over one hundred academic papers at both local and at International Scene. He has attended many International Conferences and has made tremendous researches the Republic of South Africa.