Digital Forensics Fundamentals
# Table of Contents

1. Overview of Digital Forensics .................................................................................. 3

2. Evaluation of Digital forensic tools ......................................................................... 5
   2.1 Encase Digital forensic tool .................................................................................. 5
      2.1.1 Benefits with Encase Digital forensic tool ...................................................... 6
      2.1.2 Limitations with Encase Digital forensics tool ................................................ 9
   2.2 FTK (Forensics Tool Kit) ..................................................................................... 10
      2.2.1 Advantages of FTK ....................................................................................... 10
      2.2.2 Limitations with FTK ................................................................................... 13
   2.3 Helix Digital forensics tool ................................................................................... 13
      2.3.1 Benefits with Helix digital forensics tool ....................................................... 13
      2.3.2 Limitations with Helix digital forensics tool ................................................... 16

3. Comparison of Digital Forensics tools FTK, Encase and Helix ................................... 17

4. Digital forensics tools and techniques examination ................................................... 19
   4.1 Digital examination techniques ............................................................................ 19
      4.1.1 Live forensics analysis .................................................................................. 20
      4.1.2 Recovery of windows registry ....................................................................... 20

5. ACPO guidelines for Digital forensics analysis ......................................................... 22

6. Conclusion ................................................................................................................. 23

References ..................................................................................................................... 24
1. Overview of Digital Forensics

Traditional computer forensics tools and techniques are being replaced with the latest and sophisticated Digital forensics and being applied over many forensics cases as well. There are many features and advantages with digital forensics when compared to traditional computer forensics in terms of acquiring, analyzing and reporting the respective forensics evidence. Evidence gathering is the primary step with any forensics analysis and digital forensic tools have unique methodology in this context. The main difference of digital forensics and computer forensics will be at the source of evidence, where digital sources are analyzed with the case of digital forensics (Fowler, 2011).

Digital sources are investigated across the digital forensics analysis and these sources can be either a simple mobile device, operating system, PDA devices, smartphones and tablets or mobile memory devices. Digital forensics tools and techniques are applied against the digital sources gathered and further data acquisition, investigation and analysis will be done. Most of the cyber crimes involve or use the digital forensic techniques and the level of crime over the investigation process can be analyzed using the high end forensic techniques (Bennett, 2012). Basic steps involved across the digital forensic analysis and investigation are presented in the below image.
There are many applications with the digital forensic techniques and the actual implementation of the respective forensic tool depends on the nature of the crime and investigation respectively. Main goal of the current report is to evaluate and compare various digital forensic tools across various cases and scenarios with respective to ACPO guidelines and given as below.
2. Evaluation of Digital forensic tools

A brief overview of digital forensic tools is given in the previous section and the review it is clear that, there are many steps and techniques involved across digital forensic analysis and investigation as given in the previous image. There are many digital forensic techniques and the corresponding tools against digital forensic investigation and it can be noted that, only few of them are successful and popular in gathering the accurate digital evidence acquisition, investigation and analysis.

Efficiency of any digital forensic tool depends on the level of contribution towards each and every step involved across the digital forensic investigation and analysis. As the current objective is to evaluate and compare various digital forensic tools, the popular tools like Encase, FTK (Forensics Tool Kit) and Helix are considered for the evaluation and comparison. Two to three forensic analysis scenarios or steps are considered and the required comparison is made (Beebe, 2009). Both the advantages and limitations of each tool are discussed and as provided below.

2.1 Encase Digital forensic tool

As mentioned there are ample digital forensic tools and techniques and only few of them are popular, where Encase is one among them. Encase is one of the widely used network and digital forensic tools and can be applied across each and every step of digital forensic evidence acquisition, investigation and analysis process. Encase has many features and inbuilt sub tools those can be used over digital data acquisition. Advanced search option with the recent relies of Encase V7 can be used to investigate and analyze both the traditional computer and digital sources and produce the respective reports (Rocha, 2011). Encase has many benefits and few limitations as well and few of them are as provided below.
2.1.1 Benefits with Encase Digital forensic tool

As discussed there are many advanced features, advantages and benefits with the latest releases of Encase digital forensic tools and few of them are as provided below

- Traditional computer and advanced digital forensic evidence acquisition, investigation and analysis can be accomplished with Encase digital forensics tool.
- Query processing and MLI (Multiple Language Indexing) can be accomplished easily against the process of digital source of evidence extraction and further investigation process with the Encase digital forensics tool.
- Production of binary duplicates is the key benefit with Encase digital forensic tool, where the examiners are provided with the option to preview the evidence data in parallel to actual digital evidence source acquisition process.
- Programming language customizations can be done with Encase digital forensic tools, where the object oriented programming languages like Java and C++ can be used in this context.
- Encase has simple reporting architecture when compared to most of the digital forensic tools like Helix and FTK. (Simon, 2012)

Below are some of the Encase Snapshots against digital evidence source acquisition, investigation and analysis process
Fig 2.1.1.1: Digital evidence data acquisition process with Encase (Simon, 2012)
Fig 2.1.1.2: Digital evidence investigation process with Encase (Simon, 2012)
2.1.2 Limitations with Encase Digital forensics tool

There are few identifiable disadvantages or limitations with Encase digital forensic tools and are as provided below.

- Encase tools suffers with complex features in terms of user interface and design patterns.
- Encase also have time constraint limitations in terms of end user training and live search features when compared to other digital forensic tools like Helix and FTK (Simon, 2012).
2.2 FTK (Forensics Tool Kit)

Many advanced techniques, characteristics and features are available with FTK (Forensics Tool Kit) when compared with Encase and AccessData provides the basic techniques of FTK. Simplest way of scanning the digital evidence sources like hard disks and memory card is possible with FTK and has the capability to retrieve the information related to remove data like emails, passwords and other relevant text strings as well. FTK Image is one of the tools with FTK digital forensics tool, where it can scan and retrieve the hard disk images in the form of either single or multiple disk images. Calculation of complex MD5 has values can be accomplished with FTK in a simpler manner when compared to other popular digital forensic tools (Chan, 2011). FTK is the most popular digital forensic tool used over many investigations and cyber crimes and the key benefits with FTK are as provided below.

2.2.1 Advantages of FTK

Below are some of the benefits with FTK (Forensics Tool Kit)

- Reading of multiple digital evidence sources and the related files which includes mobiles, smartphones, tablets, PDA’s, laptops and computers is simple with FTK when compared with other popular digital forensics tools.
- Data packets of both the protocol like IPV4 and IPV6 can be processed, searched and recovered easily with FTK.
- Different file formats can be read with FTK unlike other popular digital forensic tools which include FAT and NFTS.
- Efficient network, memory and file management can be achieved with FTK with the level of customization and user interface simplicity when compared with Encase.
- Digital source evidence data integrity can be achieved against the complex encryption and hash value calculations using the FTK digital forensics tool. (Chan, 2011)
- Easy and fast recovery of ARP Ethernet frames is another important advantage with FTK when compared to other network and digital forensic tools like Helix and Encase.

Below are some of the FTK digital forensic analysis snapshots

*Fig 2.2.1.1: Digital evidence acquisition with FTK (Chan, 2011)*
Fig 2.2.1.2: Digital forensics evidence investigation process with FTK (Chan, 2011)
2.2.2 Limitations with FTK

Below are some of the key limitations with FTK digital forensics tool:

- FTK digital forensics tool suffers with the response time against incidence analysis across the network forensics investigation process.
- Integrating FTK with third party forensics tools is a tedious and complex process, where the configuration complexity limits the scope of tool level integration techniques. (Chan, 2011)

2.3 Helix Digital forensics tool

Helix is a pure UNIX operating system oriented digital forensics tool and builds over the Ubuntu OS architecture. Main goal of the Helix digital forensics tool is to digitally acquire, investigate, analyze and generate the respective incident reports for both the traditional computer and digital forensics requirements. Helix runs over portable memory devices like live CD and has the capability to operate across multiple operating system environments which include Windows, Linux and Solaris respectively. Helix is a forensically sound tool and never considered the host computer across the digital forensics analysis process. Below are some of the noted benefits with Helix digital forensics tool (Cheong, 2008).

2.3.1 Benefits with Helix digital forensics tool

- The main benefit with Helix when compared with Encase and FTK is that, the ability to run over a As Helix is a live CD makes Helix to acquire, investigate and analyze the source device and make the existing OS inactive during the digital forensics analysis process.
• Entire picture of the required network can be gathered with Helix and it has the capability to run over the complex suspected network and all the devices connected to the network as well.

• Helix has the key feature of live network forensics acquisition, examination, investigation and analysis and thus accurate digital forensics investigation reports can be generated with this tool is possible with the Helix tool (Cheong, 2008).

Below are some of the snapshots of Helix digital forensics analysis process

![Digital forensics data acquisition process with Helix (Cheong, 2008)](image)

*Fig 2.3.1.1: Digital forensics data acquisition process with Helix (Cheong, 2008)*
Fig 2.3.1.2: Digital forensics examination process with Helix (Cheong, 2008)
2.3.2 Limitations with Helix digital forensics tool

Below are some of the key identified limitations with Helix digital forensics tool:

- User interface and complex command knowledge requirements is the main limitation with Helix digital forensics tool when compared to Encase and FTK.
- Live imaging and backup processes is complex in nature against Helix digital forensics tool implementation. (Cheong, 2008)
3. Comparison of Digital Forensics tools FTK, Encase and Helix

A brief overview and analysis of the popular digital forensics tools Encase, FTK and Helix is given in the previous sections and they are compared against various features in this section and given in the below table (Huebner, 2009)

<table>
<thead>
<tr>
<th>FTK Tool</th>
<th>Helix Tool</th>
<th>Encase Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital forensics evidence source acquisition is complex in nature with FTK when compared with Encase and Helix.</td>
<td>Live forensics acquisition, examination and analysis are possible with Helix digital forensics tool.</td>
<td>Easy and less configurable digital forensics evidence acquisition, investigation and analysis are possible with Encase when compared to FTK and Helix.</td>
</tr>
<tr>
<td>Source media acquisition is complex with FTK, where the respective data preview is simple when compared to rest of the digital forensics tools.</td>
<td>Both the digital media source acquisition and data preview are more complex with Helix when compared with FTK and Encase.</td>
<td>Encase has the advantage of parallel processing with respective to both data preview and required digital source media acquisition.</td>
</tr>
<tr>
<td>Digital forensics analysis and respective reporting structure is simple and easily configurable with FTK when compared with Encase and Helix.</td>
<td>Helix digital forensics tool suffers with the level of complexity involved over live reporting of the respective digital forensics analysis process.</td>
<td>Encase has the benefit of simple digital forensics analysis and respective reporting structure when compared with FTK and Helix.</td>
</tr>
<tr>
<td>Simple live and offline search options are available with FTK.</td>
<td>Helix digital forensics live search is complex in nature, but the search time is very less when compared with Encase and FTK.</td>
<td>Encase digital forensics tool suffers with complex and time consuming live search.</td>
</tr>
</tbody>
</table>
The main benefit with FTK digital forensics tool is that can read multiple file formats like NFTS and FTK.

<table>
<thead>
<tr>
<th>The main benefit with FTK digital forensics tool is that can read multiple file formats like NFTS and FTK.</th>
<th>Multiple file formats can’t be read with Helix digital forensics tools.</th>
<th>Encase suffers with limitations of reading various file formats.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password recovery ad registry recovery is simple with FTK digital forensics tool.</td>
<td>Helix lack proper password and registry recovery techniques.</td>
<td>Password and registry recovery process is complex and slow with Encase when compared with FTK tool.</td>
</tr>
<tr>
<td>Complex functions and data integrity are one of the key benefits with FTK.</td>
<td>Data integrity process is complex and sophisticated with Helix and level of required functionality support is low with the current digital forensics tool.</td>
<td>Encase suffers support of hash functions and thus data integrity process is not properly accomplished with Encase.</td>
</tr>
<tr>
<td>FTK offers quite simple query retrieval and processing functions when compared with Encase and Helix.</td>
<td>Helix has the benefit of better query processing on live.</td>
<td>Encase has the main benefit of query processing and supports the MLI (Multiple Language Indexing)</td>
</tr>
<tr>
<td>Object oriented and structured programming languages can be used and supported with FTK digital forensics tool.</td>
<td>Helix support the Unix based programming and shell scripting.</td>
<td>Encase purely supports Object oriented languages like C++ and Java.</td>
</tr>
</tbody>
</table>

**Table 3.1: Comparison of Encase, FTK and Helix digital forensics tools**
4. Digital forensics tools and techniques examination

Brief discussion on various digital forensics tools and techniques like Encase, FTK and Helix is provided in the previous sections. From the comparison of the respective tools it is clear that, there are both benefits and limitations with each of the tools and can be applied over various techniques. Digital evidence source plays the key role across digital forensics data acquisition, examination, and investigation and analysis process and in general the respective source can be a simple computer, memory, laptop, Smartphone and tablets.

Source of digital investigation also plays a key role in estimating the optimized conditions of the respective tools and techniques and the corresponding tools can be either mobile, or memory or laptop. Gathering the digital evidence is the main step across the digital forensics analysis process, where the role of each of the tools mentioned in this report is important in this context to evaluate the overall performance of the digital forensics tools. Digital examination techniques of the respective tools like Encase, FTK and Helix are discussed in this section and provided as below.

4.1 Digital examination techniques

There are many techniques involved over the digital examination process and the key among them include Window registry recovery or reconstruction and Live forensics. Performance of the respective digital forensics tools mainly depends on the source being investigated over the analysis and examination process. Two techniques are considered for the evaluation process and provided as below.
4.1.1 Live forensics analysis

Live forensics analysis is the key process across the digital forensics examination process and includes the steps of gathering the image of memory devices like hard disk over the live or offline environment. A minimum of 10 TB data is required for the corresponding live forensics analysis of a hard disk and the respective process can be in both online, live or offline.

In general a typical live forensics analysis process includes making the image of hard disk or other memory sources at both the online and offline scenarios. There are few negative impacts with the live forensics analysis process which include hash checks, timestamps, acquiring the required swap keys, gathering the registry entries and frequent memory checks.

Live forensics analysis is possible with Encase and there are limitations with evidence gathering and the required hash checks. Encase lacks the required level of support of SH1 and respective encryption techniques.

Limited live search and forensics analysis options are supported with FTK and suffer with the timestamp issues and failures and thus configuration is complex in nature.

Live forensics analysis support is provided across Helix as it runs over Live CD or USB, where little offline content is accessed against forensics analysis as well (Giustini, 2009).

4.1.2 Recovery of windows registry

In general windows registry recovery or reconstruction includes the IIS and FTP event logs and the level of system security requirements are covered over the recovery process. Windows registry holds the key information related to all the installed programs, websites visited, recent documents processed. Digital forensics analysis and investigation process can recover the required windows registry and the required windows directory reconstruction is also possible.
Windows registry reconstruction and recovery can be accomplished with Encase and the limitation in this context is that, required log files of the corresponding directory can’t be maintained with this tool.

Windows registry can be reconstructed and recovered in the best possible way with FTK digital forensics tool. Complex artifacts of windows registry like URL retrievals, log files and various documents can be searched in a simpler manner with FTK tool.

The main limitation with Helix is that, it can’t reconstruct and recover the windows registry as it purely runs over the UNIX operating system environment (Olga, 2012).
5. ACPO guidelines for Digital forensics analysis

Following are the ACPO guidelines followed across the digital forensics analysis process

- **ACPO Guideline1**: Forensics investigation is the main source of the current ACPO guideline. Required responsibilities, authorities and the respective actions implemented over the cyber crime investigation are purely with law and police and the forensic investigator has no significant role in this context.

- **ACPO Guideline2**: All the activities with respective to forensics activities over the labs are covered under the current ACPO guideline. Capabilities and ability of the forensics investigator or examiner should be considered over the digital forensics analysis. It is assumed that, all the digital forensics techniques should be considered or not task is left in middle of the process.

- **ACPO Guideline3**: ACPO Guideline 3 mainly deals with the actual data records of source of digital evidence. Required audit roles and management is given top priority in this context.

- **ACPO Guideline4**: Forensics investigation and the respective information is the main source of the current ACPO guideline. It is always the responsibility of the forensics investigator to maintain the required integrity and reliability over the digital forensics analysis process. (ACPO, 2008)
6. Conclusion

Main goal of the current research is to analyze and evaluate various digital forensics tools and techniques. Encase, FTK and Helix are considered over the current analysis process, where the respective tools are compared and evaluated at various level of digital forensics acquisition, examination and analysis process. Advantages and limitations of each and every level are discussed over the current report and the required ACPO guidelines are discussed and explained. From the entire analysis it is clear that FTK, Encase and Helix digital forensics tools have their own limitations and features and can be applied with most of the critical network and digital forensics analysis.
References