International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 01 | Jan 2026 www.irjet.net p-ISSN: 2395-0072

A Comparative Analysis of Digital Forensics Tools Based on Performance Parameters

Aditya Choudhary[1]

Aditya Choudhary Department of Computer Applications Maharaja Surajmal Institute New Delhi, India

---

Abstract - *Digital forensics is essential for investigating cyber incidents because modern crimes leave digital traces on devices and services. A wide range of tools — both commercial and open-source — help examiners acquire, analyze, and report on evidence. This paper compares four widely used forensic tools (EnCase, FTK, Autopsy, and X-Ways) against practical performance parameters: acquisition/processing speed, accuracy/recovery, usability, platform and file-system support, resource usage, reporting, and cost. The comparison is based on vendor documentation, standards guidance, and recent comparative studies. The goal is to help students and beginner investigators choose tools appropriate to their needs and resources.*

Keywords -Digital Forensics, Cybersecurity, Digital Evidence, Forensic Tools, Performance Analysis

I. Introduction

Most people use devices and cloud services nowadays, so cybercrime is not something that hardly ever happens. It is affecting both individuals and companies all around us. When something bad happens on the internet the people who investigate need to find evidence to understand what exactly went wrong. But there is a problem: digital evidence can be easily ruined if you are not careful with it. That is where digital forensics comes into play helping with evidence and cybercrime and that is why digital forensics is so important, for solving cybercrime cases and dealing with digital evidence. The digital evidence system provides investigators with the methods and tools to collect protect study and present digital evidence in ways that courts and investigations trust.

The tools you choose are very important.

They decide how quickly you can work and how information you can find.The tools also decide whether your findings will be accepted when someone questions them. So it is not just the experts who want to know which tools are the students and people who are new, to this field want to know too.

The digital evidence system is something that students and newcomers care about because they want to use the tools to do their job. In this paper, I break down the main digital forensic tools, pulling info from public docs and fresh research, and lay out a clear, beginner-friendly comparison.

II. Background and Standards

The National Institute of Standards and Technology or NIST for short has guidance documents that tell you how to handle evidence. These documents from the National Institute of Standards and Technology along with other sources say what you need to do to keep evidence safe and make sure it can be used in court.

You must do things like display evidence protect it gather it review it examine it and then evaluate and report on it. If you follow these guidelines from the National Institute of Standards and Technology, you can be sure that the evidence you collect during an investigation will be good and legal. This is important, for an investigation.

The National Institute of Standards and Technology or NIST has a Special Publication called 800.86. This publication is like a guide for people who must figure out what happens when a crime is committed using computers. People who study this sort of thing and people who do this work are very interested in comparing the tools that are available to help with this process. They want to know which tools are easy to use and which ones work well when it comes to dealing with crimes that happen on computers and they want to do this in a way that's fair and legal.

The findings from these reviews provide a means for synthesizing previously published data about the respective strengths and weaknesses of both types of forensic software tools.

III. Digital Forensics Process

Order. Nonetheless, this is so that digital evidence is reliable and can be used in court. The main steps of forensics are described below. Identification: This step is about finding devices and data sources that have information. Nevertheless, Devices, like computers, mobile phones, storage devices or servers may have the evidence we need. Hence, we need to look at these devices and data sources to see what they can tell us about what happened. The devices we are looking for include computers, mobile phones, storage devices and servers. Consequently, Preservation: When we find evidence we have to make sure it does not get changed. We follow the steps to keep the evidence safe and make sure the information is good. Nonetheless, this way we can be sure that the evidence is real and that the information is accurate. We have to protect the evidence from people who might try to modify it. The people in charge follow these steps to keep the data good and to maintain the integrity of the evidence. Collection: At this point people get evidence of using special tools. They make copies of the storage devices, so they do not work on the original information. Moreover, this way the original data, from the evidence, remains safe. Analysis: We look at the data we have collected to find out what is useful. Moreover, this includes things, like files and logs and timestamps and what the user is doing. Hence, we want to know what the user activity is so we can understand what is going on with the user activity and the files and the logs and the timestamps. Presentation: Finally, the findings are documented in a clear and understandable format so that they can be used for legal or official purposes.

IV. Overview of Digital Forensics Tools

Digital forensics investigators use tools when they work on a case. They have to look closely at everything to figure out what happened. Digital forensics investigators need these tools to help them do their job. I am going to talk about four digital forensics tools that digital forensics investigators like to use.

A. EnCase Forensic

EnCase is a tool that many law enforcement agencies use. It has a lot of features for making copies of disks and recovering files from the disks. EnCase also helps people look closely at the data on their computers.

People like EnCase because EnCase works well and EnCase is good to use in court when people need to show evidence. The bad thing about EnCase is that EnCase costs a lot of money. People also need to learn how to use EnCase to get the most, out of En Case.

B. FTK (Forensic Toolkit)

FTK is another name in the field. This tool is also something you must pay for. It is known for being very fast at looking through data and having tools to search for things. FTK works with file systems. It is used a lot when companies are investigating something. FTK is good at what it does. The cost of using FTK is a problem. The fees for FTK are high like the fees for EnCase. This makes it hard for students who want to use FTK to get it. FTK is out of reach, for a lot of students who want to use FTK.

C. Autopsy

Autopsy does things in its way. The thing about Autopsy is that it is an open-source tool. Autopsy is built on The Sleuth Kit. What I like about Autopsy is that it has a graphical interface. This interface makes it easy for me to do analysis of disks and search for keywords and even work with timelines. One of the things about Autopsy is that it is free. Autopsy is also very easy to use. That is why Autopsy is so popular. I have seen Autopsy being used in universities. Autopsy is also used in training programs because Autopsy is a great tool to learn from.

D. Sleuth Kit

Sleuth Kit itself is open-source too, but it's command-line based. It's designed for deep file system analysis and supports lots of file systems. This one's best for folks who are comfortable with technical details and aren't afraid of a terminal window.

V. Performance Parameters

When we compare forensics tools, people who study this and people who actually use digital forensics tools look at a few important things to see which digital forensics tool really works. These things are not just ideas. They are used in investigations and are often talked about in research. Digital forensics tools are very important. The people who use digital forensics tools need to know which ones are the best.

Processing Speed: - Let us start with speed. The speed of a tool is important because it shows how fast the tool can look at a lot of data. This data can come from things like drives, memory dumps, phones and network logs. People who investigate usually must look at an amount of data. If the tool they use is slow then the whole investigation takes longer. When we look at studies, we see that tools that work faster are better at looking at data putting it in order and finding what is important. This means that investigators do not have to wait long and they can spend more time trying to understand the evidence, from the speed of the tool. The speed of the tool is very important. When you do not have a lot of time like when you're dealing with cybercrime cases it is important to do things quickly. Cybercrime cases are an example of this because speed really makes a difference, in cybercrime cases.

Accuracy:- Getting things right is very important. A tool must be able to find deleted files, understand the information about the files and figure out what the user was doing without making any mistakes. People who write about this stuff say it again: digital evidence must be trustworthy if it is going to be used in court. If you make one mistake or if you do not understand something correctly you might come to the wrong conclusion or the evidence might not be allowed. That is why people always want to use tools that are known for being accurate. Digital evidence and tools that recover deleted files and parse metadata. Reconstruct user activity must be right all the time.

Ease of Use: - A good tool should not make life harder. The tool should be easy to use. This means the tool should look nice and be simple to navigate. It should also have instructions that are easy to understand. We do not want the tool to be difficult to learn. Research shows that tools with simple and easy to use interfaces are better. These tools reduce the chance of people making mistakes. Clean and intuitive interfaces are easier for everyone to use, including investigators, students and law enforcement officers who are new, to forensics like digital forensics. When it comes to the tools they need to be simple for everyone to use. At the time the best tools also need to have advanced options for experts. The best tools make it easy for people to use them. They also have a lot of advanced options. This means the best tools balance being simple and being deep, so the best tools have both simplicity and depth. The best tools are good for experts because they have options and the best tools are good for everyone else because they are simple, to use.

Platform Support: - Then there is the issue of platform support. The thing is does the tool work on Windows, Linux, and macOS and can it really handle data from all kinds of devices? As people use smartphones, cloud storage and different file systems increasingly it is clear that platform support is not a good thing to have. It is essential. Tools that only work on one operating system or look at several file types are not going to be used as much as technology keeps moving forward. Platform support is very important for these tools.

Cost: - The cost is something we have to think about. It is not about how much something costs when we buy it. We also have to think about the cost of using it and taking care of it over time. For students and schools and smaller groups the cost is usually the thing they consider. Tools that we have to pay for usually have a lot of features and people to help us. Tools that are free to use are popular because they are cheap and can do a lot of things. The main thing to remember is that we should not just think about the cost. We should also think about what the tool can do, for us.

All these factors—speed, accuracy, usability, platform support, and cost—form a solid framework for comparing digital forensics tools. Focusing on these criteria helps investigators and students alike choose the right tool for the job, balancing investigation needs, technical requirements, and budget.

VI. Methodology

This research paper is about forensics tools. It looks at tools and compares them. The information for this study comes from things that're already out there like books and articles. The people who wrote this paper did not do their experiments to get the information. They just used what other people have already found out. This is a way to do research especially when you want to see how different tools and technologies work. The paper uses a research methodology to study digital forensics tools and compare digital forensics tools.

The information for this study came from places like research papers that were published official documents for digital forensics tools, articles from academic websites and resources to learn about cybersecurity. We looked at these sources carefully to see how each digital forensics tool works and what it can do. We paid attention to sources that are trustworthy and used a lot so that the digital forensics information in this paper is correct and useful. We wanted to make sure the digital forensics tools information is accurate.

The digital forensics tools that were chosen were looked at to see how well they worked. We wanted to know how fast they could process things how accurate they were, how easy they were to use, what kinds of platforms they worked on and how

much they cost. We looked at each digital forensics tool on its own to see what it was good at and what it was not so good at. Then we compared the forensics tools to each other to see what made them different from one another.

No hands-on experiments or live testing were done in this study. The people in charge made this decision so that the research would be good for a student-level paper that compares things. They did not want to buy software or set up a fancy laboratory. So, the focus of this research is on comparing things by looking at what other people have found out. The research is about making conclusions from the information that is already available which is what this study is really, about this research.

This methodology helps in providing a clear and simple comparison of digital forensics tools. It is especially useful for students and beginners who want to understand the basic work and performance of different tools without going into complex technical testing.

VII. Comparative analysis

In this section, a comparison of selected digital forensics tools has been carried out. The tools are compared based on important performance parameters, and the results of this comparison are shown in the table below.

Parameter	EnCase	FTK	Autopsy	Sleuth Kit
Tool Type	Commercial	Commercial	Open source	Open source
Speed	High	High	Medium	Medium
Accuracy	Very High	High	Good	Good
Interface	GUI	GUI	GUI	CLI
Platform Support	Windows	Windows	Multi-OS	Linux/macOS
Cost	Very High	High	Free	Free

The comparison shows that commercial tools such as EnCase and FTK provide strong performance and advanced features, making them suitable for professional investigations. However, their high cost and system requirements limit their accessibility for students and small organizations. Open-source tools such as Autopsy and Sleuth Kit offer cost-effective alternatives with reasonable performance. Autopsy is particularly suitable for beginners due to its graphical interface, while Sleuth Kit is more suitable for advanced analysis

VIII. Conclusion

I am writing this paper to look at forensics' tools. Therefore, I want to find out what makes each digital forensics tool unique. To do this I am reading information that people have already written about forensics tools. Additionally, I do not need to run my tests because I can use the information that other people have already found about digital forensics tools. This way of doing research is good for my work, on forensics tools. It helps me understand the digital forensics tools that are already out there and how they work. Therefore, I can get an understanding of digital forensics tools and the technology that digital forensics tools use. I found information from places like research papers and official documentation for tools. I also read articles on the internet. Moreover, used things I learned about cybersecurity. I made sure to use sources that people trust and that have been around for a while. Additionally, this way I can be certain that the information about cybersecurity is correct and makes sense. The more I looked at each source the more I understood the tools and what they can do for me. Consequently, I started to see how the tools work and what the tools can do. Furthermore, the tools became clearer as I learned more about the tools and cybersecurity. Therefore, I understood how the tools work and what the tools can do for me as I kept learning about cybersecurity. I wanted to do things the way, so I looked at the tools. Saw how well they worked in different areas. They had to

be fast at processing things. The tools also had to be accurate and easy to use. I checked which platforms the tools worked on and how much they cost. Furthermore, I made a list of what each tool was good at and what each tool was not good at. Additionally, Then I compared the tools to each other to see the differences between the tools. I compared the tools to see what made each tool different, from the tools. I did this by looking at the processing speed of the tools. The accuracy of the tools was also important to me. I considered how easy the tools are to use. Nevertheless, the tools must work on platforms. Therefore, I thought about the cost of the tools. I thought about all these things when I looked at the tools. Moreover, the cost of the tools and the processing speed of the tools were factors, for me. I did not do any hands-on testing or live experiments for this study. Additionally, this is because I wanted to make research into something that is easy to do for a student level paper. It means I do not need to buy software or have a big laboratory with a lot of equipment. I can just focus on the study itself. That is what makes it practical for me. The study of this research is what is important to me. That is what I want to learn more about the research itself. I do not look at things. Additionally, Instead I look at what we know about the study. Additionally, I think about what this means and draw conclusions from what we know about the study. This helps me understand the study. Additionally, this approach makes for a straightforward, accessible comparison of digital forensics tools. Moreover, it's especially helpful for students and beginners who want to understand how these tools stack up—without wading into complicated technical testing.

IX. Future Scope

Future research in digital forensics may focus on the use of artificial intelligence for automated analysis, cloud and IoT forensics, and advanced techniques for handling encrypted data. Improvements in automation and efficiency will further enhance digital forensic investigations.

References

[1] E. Casey, *Digital Evidence and Computer Crime*, 3rd ed., Academic Press, 2011.

[2] J. T. Luttgens, M. A. Pepe, and K. Mandia, *Incident Response & Computer Forensics*, 3rd ed., McGraw Hill, 2014.

[3] B. Carrier, *File System Forensic Analysis*, Addison-Wesley, 2005.

[4] M. T. Britz, *Computer Forensics and Cyber Crime*, Pearson, 2013.

[5] G. Gogolin, *Digital Forensics Explained*, Routledge, 2024.

[6] J. Kävrestad, *Fundamentals of Digital Forensics*, Springer, 2023.

[7] H. Diwaker, "A Review on Comparative Analysis of Commercial and Open-Source Digital Forensic Tools," *Innovation and Integrative Research Center Journal*, Apr. 2025.

[8] "Comparative Study of Digital Forensic Tools," ResearchGate, 2019.

[9] "Comparative Analysis of Digital Forensic Extraction Tools," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, 2024.

[10] "Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools," Infonomics Society, 2024.

[11] C. Cruz, "Innovative Learning in a Digital Forensics Laboratory," *Applied Sciences*, 2024.