# Digital Forensics CTFs with FTK Imager

## Complete Beginner to Advanced Guide (A to Z)

### Introduction

This guide explains how to use FTK Imager for Digital Forensics Capture The Flag (CTF) challenges. It is written in simple English and starts from zero knowledge.

The main goal in CTF forensics is to find a hidden flag inside digital evidence.

### Main Objective in Forensics CTFs

In CTF challenges, your goal is to find hidden flags inside:

- Files

- Deleted data

- Images

- Browser history

- RAM memory dumps

- Metadata

- Slack and unallocated space

### Chapter 1: What is Digital Forensics?

Digital Forensics is the science of collecting, preserving, and analyzing digital evidence. It is used in investigations and cybersecurity competitions.

### Chapter 2: What is FTK Imager?

FTK Imager is a free forensic tool used to view, analyze, and create forensic images without changing original data.

### Chapter 3: Installation

Download FTK Imager from the official Exterro website and install it with default settings.

### Chapter 4: Interface Overview

FTK Imager has three main panels: Evidence Tree, File List, and Preview Pane.

### Chapter 5: Loading Evidence

CTF challenges usually provide files such as:

disk.img, memory.mem, challenge.E01, usb.dd

To load them: File > Add Evidence Item > Image File > Select File.

### Chapter 6: Finding Deleted Files

Many CTF flags are hidden in deleted files.

Navigate to the partition and look for red-colored files marked as deleted.

Check orphan files and lost files.

## Chapter 7: Keyword Searching

Use Find > Find to search for important words.

Common keywords: flag, FLAG, ctf{, CTF{, password, secret, key, admin.

Enable ASCII and Unicode search.

## Chapter 8: File Signature Analysis

Sometimes files have fake extensions.

Open Hex View and check magic numbers.

JPG: FF D8 FF | PNG: 89 50 4E | PDF: 25 50 44

If mismatch is found, export and rename the file.

## Chapter 9: Slack Space and Unallocated Space

Deleted data may remain in free space.

Navigate to Root > Unallocated Space > Free Space.

Search for readable strings.

## Chapter 10: Metadata Analysis

Check metadata inside images, documents, and PDFs.

Look for author names, comments, and software fields.

Example: Author: flag{example}

## Chapter 11: Browser Artifacts

Browser data often contains important evidence.

Common locations:

Users\Username\AppData\Local\Chrome\User Data\

History, Cookies, Login Data

Look for suspicious searches and websites.

## Chapter 12: Recycle Bin Analysis

Check the $Recycle.Bin folder.

Analyze $I and $R files to find original file names and paths.

## Chapter 13: Password and Log Files

Search for text and log files:

.txt, .log, .bak, .old, .save

Search for: password=, admin:, login:

## Chapter 14: Memory Forensics

Analyze .mem files to find passwords, processes, and commands.

Combine FTK Imager with Volatility for advanced analysis.

**Chapter 15: Exporting Evidence**

Right-click suspicious files and choose Export.

Analyze exported files with external tools.

**Chapter 16: External Analysis Tools**

Useful tools: ExifTool, Binwalk, Steghide, Strings, Volatility.

**Chapter 17: Timeline Analysis**

Check file creation, modification, and access times.

Reconstruct user activity.

**Chapter 18: Where Flags Are Usually Hidden**

In most CTF challenges, flags are commonly found in:

- Deleted text files
- Hidden folders
- Image metadata
- Steganography inside images
- Browser history searches
- Password files
- Memory dumps
- Unallocated space
- Backup and temporary files

**Chapter 19: Common CTF Workflow**

1. Load the image.
2. Check deleted files.
3. Search for keywords.
4. Analyze unallocated space.
5. Check metadata.
6. Inspect browser artifacts.
7. Export suspicious files.
8. Use external tools.

**Chapter 20: Reporting**

Document your findings: tools used, hashes, evidence, and flags.

**Chapter 21: Best Practices**

Always work on copies, verify hashes, and take notes.

Never modify original evidence.

### Chapter 22: Troubleshooting

If files cannot be opened, export them.

Check file signatures and permissions.

### Chapter 23: Practice Platforms

TryHackMe, Hack The Box, CTFtime, PicoCTF, CyberDefenders.

### Conclusion

FTK Imager is a powerful tool for solving forensic CTF challenges. With practice and structured analysis, you can find flags efficiently.