



[SandySekharan](#) / [CTF-tool](#)

Watch

4

Star

61

Fork

27

Code

Issues **1**

Pull requests **0**

Projects **0**

Insights

## Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

[Sign up](#)

Dismiss

A curated list of Capture The Flag (CTF) frameworks, libraries, resources and softwares.

**2** commits

**1** branch

**0** releases

**1** contributor

Branch: **master** ▾

[New pull request](#)

[Find file](#)

[Clone or download](#) ▾



**SandySekharan** Update README.md

Latest commit 9578edb on Apr 9, 2016

[README.md](#)

Update README.md

2 years ago

[README.md](#)

# CTF-tool

---

A curated list of Capture The Flag (CTF) frameworks, libraries, resources and softwares.

## Awesome CTF

---

A curated list of [Capture The Flag](#) (CTF) frameworks, libraries, resources and softwares.

### Contributing

Please take a quick look at the [contribution guidelines](#) first.

***If you know a tool that isn't present here, feel free to open a pull request.***

### Why?

It takes time to build up collection of tools used in ctf and remember them all. This repo helps to keep all these scattered tools at one place.

### Contents

- [Awesome CTF](#)
  - [Create](#)
    - [Forensics](#)
    - [Web](#)

- [Solve](#)
  - [Attacks](#)
  - [Bruteforcers](#)
  - [Cryptography](#)
  - [Exploits](#)
  - [Forensics](#)
  - [Reversing](#)
  - [Services](#)
  - [Steganography](#)
  - [Web](#)
- [Resources](#)
  - [Starter Packs](#)
  - [Tutorials](#)
  - [Wargames](#)
  - [Websites](#)
  - [Wikis](#)
  - [Writeups Collections](#)

## Create

---

*Tools used for creating CTF challenges*

## Forensics

---

*Tools used for creating Forensics challenges*

- [Registry Dumper](#) - Dump your registry

## Web

---

*Tools used for creating Web challenges*

*JavaScript Obfuscators*

- [Metasploit JavaScript Obfuscator](#)
- [Uglify](#)

## Solve

---

*Tools used for solving CTF challenges*

## Attacks

---

*Tools used for performing various kinds of attacks*

- [Bettercap](#) - Framework to perform MITM (Man in the Middle) attacks.
- [Layer 2 attacks](#) - Attack various protocols on layer 2

## Crypto

---

*Tools used for solving Crypto challenges*

- [PkCrack](#) - A tool for Breaking PkZip-encryption
- [RSATool](#) - Generate private key with knowledge of p and q
- [XORTool](#) - A tool to analyze multi-byte xor cipher

## Bruteforcers

---

*Tools used for various kind of bruteforcing (passwords etc.)*

- [John The Jumbo](#) - Community enhanced version of John the Ripper
- [John The Ripper](#) - Password Cracker
- [Ophcrack](#) - Windows password cracker based on rainbow tables.

## Exploits

---

*Tools used for solving Exploits challenges*

- [binjitsu](#) - CTF framework and exploit development library
- [Metasploit](#) - Penetration testing software
- [pwntools](#) - CTF Framework for writing exploits
- [qira](#) - QEMU Interactive Runtime Analyser
- [ROP Gadget](#) - Framework for ROP exploitation

## Forensics

---

*Tools used for solving Forensics challenges*

- [Aircrack-Ng](#) - Crack 802.11 WEP and WPA-PSK keys

- `apt-get install aircrack-ng`
- [Audacity](#) - Analyze sound files (mp3, m4a, whatever)
  - `apt-get install audacity`
- [bkhive and samdump2](#) - Dump SYSTEM and SAM files
  - `apt-get install samdump2 bkhive`
- [CFF Explorer](#) - PE Editor
- [creddump](#) - Dump windows credentials
- [DVCS Ripper](#) - Rips web accessible (distributed) version control systems
- [Exif Tool](#) - Read, write and edit file metadata
- [extundelete](#) - Used for recovering lost data from mountable images
- [Foremost](#) - Extract particular kind of files using headers
  - `apt-get install foremost`
- [fsck.ext4](#) - Used to fix corrupt filesystems
- [Malzilla](#) - Malware hunting tool
- [NetworkMiner](#) - Network Forensic Analysis Tool
- [PDF Streams Inflater](#) - Find and extract zlib files compressed in PDF files
- [ResourcesExtract](#) - Extract various filetypes from exes
- [Shellbags](#) - Investigate NT\_USER.dat files
- [UsbForensics](#) - Contains many tools for usb forensics
- [Volatility](#) - To investigate memory dumps
- [Wireshark](#) - Analyze the network dumps
  - `apt-get install wireshark`

### *Registry Viewers*

- [RegistryViewer](#) - Used to view windows registries

- [Windows Registry Viewers](#) - More registry viewers

## Reversing

---

### *Tools used for solving Reversing challenges*

- [Androguard](#) - Reverse engineer Android applications
- [Apk2Gold](#) - Yet another Android decompiler
- [ApkTool](#) - Android Decompiler
- [BinUtils](#) - Collection of binary tools
- [BinWalk](#) - Analyze, reverse engineer, and extract firmware images.
- [Boomerang](#) - Decompile x86 binaries to C
- [GDB](#) - The GNU project debugger
- [IDA Pro](#) - Most used Reversing software
- [Jadx](#) - Decompile Android files
- [Krakatau](#) - Java decompiler and disassembler
- [radare2](#) - A portable reversing framework
- [Uncompyle](#) - Decompile Python 2.7 binaries (.pyc)
- [WinDbg](#) - Windows debugger distributed by Microsoft
- [z3](#) - a theorem prover from Microsoft Research

### *JavaScript Deobfuscators*

- [Detox](#) - A Javascript malware analysis tool
- [Revelo](#) - Analyze obfuscated Javascript code

### *SWF Analyzers*

- [RABCDAsm](#) - Collection of utilities including an ActionScript 3 assembler/disassembler.
- [swftools](#) - Collection of utilities to work with SWF files
- [xxxswf](#) - A Python script for analyzing Flash files.

## Services

---

*Various kind of useful services available around the internet*

- [CSWSH](#) - Cross-Site WebSocket Hijacking Tester
- [Request Bin](#) - Lets you inspect http requests to a particular url

## Stegano

---

*Tools used for solving Steganography challenges*

- [pngtools](#) - For various analysis related to PNGs
  - `apt-get install pngtools`
- [SmartDeblur](#) - Used to deblur and fix defocused images
- [Steganabara](#) - Tool for stegano analysis written in Java
- [Steghide](#) - Hide data in various kind of images
- [Stegsolve](#) - Apply various steganography techniques to images

## Web

---

*Tools used for solving Web challenges*

- [SQLMap](#) - Automatic SQL injection and database takeover tool



- [w3af](#) - Web Application Attack and Audit Framework.
- [XSSer](#) - Automated XSS testor

## Resources

---

*Where to discover about CTF*

## Starter Packs

---

*Collections of installer scripts, useful tools*

- [CTF Tools](#) - Collection of setup scripts to install various security research tools.

## Tutorials

---

*Tutorials to learn how to play CTFs*

- [CTF Field Guide](#) - Field Guide by Trails of Bits
- [CTF Resources](#) - Start Guide maintained by community
- [How to Get Started in CTF](#) - Short guideline for CTF beginners by Endgame
- [MIPT CTF](#) - A small course for beginners in CTFs (in Russian)

## Wargames

---

*Always online CTFs*

- [Backdoor](#) - Security Platform by SDS Labs.

- [Ctfs.me](#) - CTF All the time
- [Exploit Exercises](#) - Variety of VMs to learn variety of computer security issues.
- [Hack This Site](#) - Training ground for hackers.
- [Over The Wire](#) - Wargame maintained by OvertheWire Community
- [Ringzer0Team](#) - Ringzer0 Team Online CTF
- [SmashTheStack](#) - A variety of wargames maintained by the SmashTheStack Community.
- [VulnHub](#) - VM-based for practical in digital security, computer application & network administration.
- [WeChall](#) - Always online challenge site.

## Websites

---

*Various general websites about and on ctf*

- [CTF Time](#) - General information on CTF occurring around the worlds
- [Reddit Security CTF](#) - Reddit CTF category

## Wikis

---

*Various Wikis available for learning about CTFs*

- [Bamboofox](#) - Chinese resources to learn CTF
- [ISIS Lab](#) - CTF Wiki by Isis lab

## Writeups Collections

---

*Collections of CTF write-ups*

- [Captf](#) - Dumped CTF challenges and materials by psifertex
- [CTF write-ups \(community\)](#) - CTF challenges + write-ups archive maintained by the community
- [pwntools writeups](#) - A collection of CTF write-ups all using pwntools
- [Shell Storm](#) - CTF challenge archive maintained by Jonathan Salwan
- [Smoke Leet Everyday](#) - CTF write-ups repo maintained by SmokeLeetEveryday team.

