Image tools

https://fotoforensics.com/

https://aperisolve.com/

Cryptography

Tools :- CyberChef, FeatherDuster, Hash Extender, padding-oracle-attacker, PkCrack, RSACTFTool, RSATool, XORTool, Cryptii, Keyboard Shift, and many more.

Steganography(Stego)

Steganography is tasked with finding information hidden in files or images.

Tools :- StegCracker, Steghide, Openstego, Stegsolve, Online stego tool, and many more.

Binay Exploitation/ pwn

exploiting a binary file and exploiting a server to find the flag.

Tools- readelf, formatStringExploiter, DLLInjector, libformatstr, and many more.

Reverse engineering

Reverse Engineering in a CTF is typically the process of taking a compiled (machine code, bytecode) program and converting it back into a more human readable format.

Tools :- ltrace, Hopper, Binary Ninja, gdb, IDA, radare2, Ghidra, apktool, Androguard, and many more.

Web

Tools :- BurpSuite, Commix, Hackbar, Raccoon, SQLMap, DirBuster, gobuster, nikto, wpscan, CloudFlare Bypass, Edit This Cookie, File or Directory(robots.txt, /.git/, /admin/), and many more.

Forensics

File format analysis, steganography, memory dump analysis, or network packet capture analysis. Examine and process a hidden piece of information out of static data files, instead of executable programs or remote servers.

Tools :- split, pdfinfo, pdfimages, pdfcrack, pdfdetach, Keepass, Magic Numbers, hexed.it, foremost, binwalk, Repair image online tool, photorec, TestDisk, pngcheck, pngcsum, Registry Dumper, Dnscat2, pefile, Wireshark, Network Miner, PCAPNG, tcpflow, PcapXray, qpdf, Audacity, sonic visualiser, ffmpeg strings, file, grep, scalpel, bgrep, hexdump, xxd, base64, xplico framework, zsteg, gimp, Memory dump - volatility, ethscan, and many more.