

Forum:[Hack Forums](#)

Thread: [DIGITAL FORENSICS](#)

dindarolo66 - April 18, 2017, 9:53 am

WHAT ARE THE BEST PROGRAMS FOR DIGITAL FORENSICS

Xphile - April 18, 2017, 11:24 am

Although I'm not very experienced with digital forensics, I'll link you to a few tools I have heard of:

- [GuyMager](#) - Forensic Disk Imager
- [FTK](#) - Forensic Toolkit (I have an eBook for usage of FTK in [this thread](#) if you need it.)
- [chkrootkit](#) - Rootkit diagnosis utility
- [HashDeep](#) aka. MD5Deep - Creates multiple message digests of a file (MD5, SHA1, SHA256 etc.)
- [Binwalk](#) - Firmware analysis tool, searches for embedded files and executable code.

Hope this helped, OP. ?

djsp1k3sm0k3r - April 18, 2017, 11:30 am

I'm not very experienced with digital forensics as well, but I did manage to find a link that has these free tools with url links here if you wanted to check them out.

<http://resources.infosecinstitute.com/computer-forensics-tools/#gref>

Disk and data capture tools

File viewers

File analysis tools

Registry analysis tools

Internet analysis tools

Email analysis tools

Mobile devices analysis tools

Mac OS analysis tools

Network forensics tools

Database forensics tools

novemb3r - April 27, 2017, 5:01 pm

Dumplt is probably the best tool to extract volatile memory from a Windows machine as it creates the smallest possible fingerprint on the machine

For Linux use LiME, but it becomes tricky if your target has a custom kernel so you have to create V-Types first.

FTK Imager Lite is pretty good. You can make a .ad1 file of the memory and then examine it. you can basically investigate a whole filesystem without worrying of compromising anything. And i mean anything. You can carve files and even registry keys, if you know where and who to search! ;)

Volatility is the #1 go-to tool for RAM examinations but it doesn't support latest Linux kernels.

For file carving use bulk_extractor, exiftool, scalpel, and foremost

The Beep Beep Sheep - April 28, 2017, 3:26 pm

Your answer has been given. There's some pretty good tools in here. However, don't forget people

don't really enjoy reading posts that are typed in caps. Blink twice and you'll have some angry Ubers on your ass lmao.