# Article information:

Which VM do you use for your OSINT investigations ? : OSINT
<https://www.reddit.com/r/OSINT/comments/je1fie/which_vm_do_you_use_for_your_osint_investigations/>

# Article summary:

1. Users discuss which virtual machines (VMs) they use for OSINT investigations, including Manjaro Linux, Parrot on VirtualBox, and Ubuntu 20.04.

2. Some users express concerns about privacy and resource usage when using certain VMs or operating systems for OSINT investigations.

3. The discussion also includes mentions of Kali on WSL and Tails as potential options for OSINT investigations.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article discusses the virtual machines (VMs) that users prefer for their OSINT investigations. While it provides some useful insights, there are several biases and missing points of consideration that need to be addressed.

Firstly, the article seems to focus primarily on Linux-based VMs, with only one mention of using Ubuntu on a digital ocean droplet. This bias towards Linux may not accurately represent the preferences of all OSINT investigators, as some may prefer Windows or Mac-based VMs.

Secondly, there is a lack of discussion around the potential risks and security concerns associated with using certain VMs for OSINT investigations. For example, while Kali Linux is a popular choice for many investigators due to its pre-installed tools and ease of use, it can also be a target for hackers looking to exploit vulnerabilities in the system. Similarly, using Parrot or Tails may provide greater privacy and anonymity but could also raise red flags if detected by authorities.

Thirdly, there is no mention of the legal implications of using certain VMs or tools for OSINT investigations. Investigators must be aware of any laws or regulations that may restrict their use of certain tools or techniques.

Additionally, some claims made in the article are unsupported or unexplored. For example, one user claims that Tsurugi requires too many resources and has a heavy GUI without providing any evidence to support this claim. Another user suggests that using Kali via WSL may not be secure due to mistrust in Microsoft without providing any further explanation.

Overall, while the article provides some useful insights into preferred VMs for OSINT investigations, it falls short in addressing potential biases and risks associated with these choices. It would benefit from more balanced reporting and exploration of counterarguments to provide readers with a more comprehensive understanding of the topic at hand.

# Topics for further research:

* Risks and security concerns associated with using Kali Linux for OSINT investigations
* Legal implications of using certain VMs or tools for OSINT investigations
* Windows or Mac-based VMs preferred by OSINT investigators
* Potential vulnerabilities in Parrot or Tails VMs for OSINT investigations
* Best practices for maintaining privacy and anonymity in OSINT investigations
* Trustworthiness and security of using Kali Linux via WSL

# Report location:

<https://www.fullpicture.app/item/ec2f338d1a5c0819f4d82e0e3ace7e60>