# Mastering Open Source Threat Analysis Strategies

*Strategic approaches, practical insights, and case studies for effective cyber security*

**Vishal Rai**

www.bpbonline.com

First Edition 2024



ISBN: 978-93-55516-398



## LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

## Dedicated to

*The unwavering support of my family and*
*the invaluable contributions of the publications support team*

# About the Author

**Vishal Rai** has done B.Sc. and Masters in Mathematics, A-Level, MCA, Cyber Law (Symbiosis, Pune), AWS Solutions Architect and multiple certifications related to database and networking. He has worked as a Jr. Consultant (Incident Response)/Sr. System Administrator/Project Associate/Trainer in Govt./Private organizations. He also has more than 10 years of experience in various domains like Mathematics, Database, Networking, Cyber Security and Virtualization etc. Along with this, he deployed the Lab for Cyber Security Training using Virtualization, and trained Govt. Employee of various organizations related to cyber security.

The author has experience in the area of Information Security, System administration and process advocacy, along with live experience in maintenance/implementation of various organizational level policies, and network administration of more than 600 nodes. He has worked in the field of lab designing, information security policies designing/implementation, making presentation to the big audience.

Vishal is well versed with most of the latest software productions in the field of virtualization, setting up various organization level information network setups, guides. His work expertise also includes Deployed Moodle Server (E-Learning) & Integrate with BigBlueButton with the help of programming team (Video Conferencing System). Alongwith this, he has designed, installed and configured VMware ESXi, with vSphere 5.x/6.x environments with Virtual Center management, Consolidated Backup, DRS, HA, vMotion and VMware Data. He has previously authored "Expert Linux Administrator Guide" published by BPB Publications.

# About the Reviewer

**Ayushi Shukla** is a Senior Cybersecurity professional with over seven years of experience in Threat Intelligence, OSINT Investigation, Vulnerability Assessment and Cybersecurity Product Solutioning. Ayushi started her journey with the Offensive Security domain and then navigated to the Defensive Security. Her experience includes working closely with the stakeholders, advising them on advanced threat mitigation strategies, and security best practices while conducting security assessments and investigations. Ayushi, an advisory board member for the GIAC, holds a bachelor's degree in Computer Science and Engineering and has several professional certifications to her credit like CISSP, GCTI, ISO 27001 and CEH. Ayushi is an avid reader and often engages herself in mentoring upcoming grads in the field of cybersecurity. When she is not being the guardian of the digital realm, you may find her seeking pleasure in nature and music.

# Acknowledgement

I am deeply thankful to my family for their unwavering encouragement throughout the book-writing journey. Gratitude extends to the educational course and supportive companies that facilitated my learning of web scraping tools, with a special acknowledgment for the behind-the-scenes support. Furthermore, my appreciation goes to the BPB Publications team for their steadfast support, providing both time and flexibility to complete and publish the book. This approach proved crucial in delving into the diverse problem classes within image processing without overwhelming the content with excessive volume.

Finally, I extend my thanks to my brother who has supported me to complete the research work directly or indirectly.

# Preface

There is a rising trend in cyberspace where cyber criminals are trying to contact vulnerable people, causing a sense of threat or fear. The impact of cybercrime can be as severe as physical offenses, even though the cyber criminal is not physically visible and their location may be unknown. Internet and intranet exploitations can result in extortion, lottery scams, credit card scams, etc. This is due to the lack of proper organizational structure to counter cyber threats effectively. Therefore, law enforcement agencies, citizens, and educational institutions, should keep updating themselves with new technologies. This will help them understand the possibilities that may be created by criminals and how they can be used as tools for fighting cyber crime.

To handle the increasing volume of cyber crimes and its complexity, it is necessary that corporates, police, judiciary and people be sensitized about cyber crime related problems. On the other hand, cyber forensics is also important in terms of evidence gathering, creation and presentation purposes to solve cyber crime cases. Internationally, cyber law has evolved into a distinct legal field aimed at addressing cybercrime, enhancing the capabilities of cyber experts and investigators in effectively combating cybercriminal activities.

In this book, we have discussed various cyber crimes with the help of examples, along with discussing the I.T Act. We have also explained how to setup cyber lab using open source softwares. Furthermore, this book will provide you with some critical aspects of cyber crime and investigation processes.

**Chapter 1: Setting up OSINT Environment –** Open Source Intelligence (OSINT) is a technique used to describe the search, collection, analysis, and use of information from open sources, about a particular target. The target may be cyber criminal/cyber terrorist/public enemy. In other words, OSINT refers to all the information that is available to the general public. The investigation through OSINT requires proxy identity, hence, in this chapter, we have given an introduction and showed how to setup OSINT lab for investigation.

**Chapter 2: Secure Browsers –** Concealing digital identity is essential for investigations using OSINT. There are multiple techniques available in OSINT to hide a person's digital identity. Keeping this in view, Chapter 2 explains how to secure the web browser using ad-ons and in-built feature of web browser. It will also equip you with hiding digital identity, such IP address, geo-location etc.

**Chapter 3: Exploring OS Security –** Operating system is the core part for communication devices. Without it, you cannot share data globally or locally. OS security means protecting the OS from threats, viruses, worms, malware or remote hacker intrusions. This chapter discusses OS security, encompassing all preventive-control techniques which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

**Chapter 4: Online Privacy and Security –** Privacy is very important when you are working as an OSINT investigator. Most companies are selling user data to advertisers, making it very likely that your data will fall into the wrong hands at some point. However, there is no one best tool for privacy. This chapter will cover the best way to boost your online privacy, i.e., using a combination of tools.

**Chapter 5: Tail OS in Use –** According to Tail OS community, Tails is a portable operating system that protects against surveillance and censorship. In other words, Tail OS can be used to access the internet while keeping your identity anonymous. In this chapter, we have explained how to use Tail OS for tracing cyber criminal footprint.

**Chapter 6: Using Tor Browser –** Torbrowser is used to hide the user's IP address. It is a useful tool for a cyber investigator to track the presence of a cyber criminal on various social media platforms. This is also used by hackers and cyber criminal to access the dark web. In this chapter, we have explained how to use Torbrowser and its features.

**Chapter 7: Advanced Search Tools –** The pages that belong to the dark web cannot be discovered by a simple search. The number of pages on these websites continually changes according to many factors, hence, Google and other search engines cannot index the entire web. Therefore, the user must know how to use advanced searching technique by using OSINT which is discussed in this chapter.

**Chapter 8: Sock Puppet Accounts –** Sock puppets are fake social media accounts used for OSINT investigation. This account can be used by law enforcement agencies, police, and even hackers. The objective of creating sock puppets account is to hide the digital identity of users such as real name and geo-location. In this chapter, we have explained how to create sock puppets accounts for OSINT investigation.

**Chapter 9: Exploring Footprinting –** Digital footprints include user logins identity such as IP address, geolocation, and visited website. An example of a digital footprint may be browsing history, likes, text messages, search history, tagged photos, and videos, basically anything that leaves a digital trace that may be linked back to users. You can review digital footprint by using privacy setting of the web browser. The digital foot print is also known as digital shadow and is unique. In this chapter, we have explained footprinting based on scenarios such as private networks and public networks to clear the fundamentals. We have also described how to use OSINT tools to gather information about the remote target.

**Chapter 10: Investigating E-mails –** In this chapter, we have explained how to analyze e-mail headers in technical and non-technical ways. We have described phishing e-mail on the basis of OSINT tools. We have also explained how the law enforcement agency gathers the information from ISPs as well as the role of CERT-IN which is the apex agency of Govt. of India, working in the field of cyber security.

**Chapter 11: Utilizing Social Media –** In this chapter, we have explained how to create an anonymous social media account and then use the same to locate a target on available social media platforms using OSINT tools. We have also explained how to fetch the social media ID along with its date of creation.

**Chapter 12: Tracking Family and Friends –** In this chapter, we have explained how to search a person using OSINT tools. Some search engines explained in this chapter work better in some countries like the USA, UK, and more. Do check if your country supports the tool, before buying a paid subscription.

**Chapter 13: Mobile Identity Search –** Mobile identity is related to data from mobile network operators, such as a subscriber's mobile phone number, name and addresses. When you forensically examine the suspicious digital device, such as mobile phone, it will provide a lot of information related to suspect such as the geo-location of suspect at the time of crime etc. We can say that mobile identity is a digital identity. In this chapter, we have explained how to search for a person using OSINT tools.

**Chapter 14: Mining Online Communities –** The online or internet community is a group of people with a shared interest or purpose who communicate with each other digitally. Online communities have their own set of guidelines. The primary difference between an online community and social media is that the online community caters to an audience with a specific objective and social media is related to broad audiences. Some online communities are not indexed by search engines. Hence, it may be used by cyber criminals to pass the information. In this chapter, we have explained all these things using OSINT.

**Chapter 15: Investigating Domain and IP –** In layman's language, the website is also known as a domain name. DNS and IP Address collectively can tell us about subscriber's information such as IP address, geo-location and payment details. In case of threatening e-mails, we have to investigate DNS and IP addresses to determine who is behind the illegal act. In order to retrieve an IP address from some Internet Service Providers (ISP) it will require warrant, or court order of the company for information. In this chapter, we have explained from scratch to the advanced level, how the domain name works and what IP address works behind a specific domain name, registrar, registrant, and IP Address providers.

**Chapter 16: Detection of Data Leaks –** Data leaks can cause companies to lose millions of dollars and their reputation. In this chapter, we have explained various OSINT tools to detect the data leaks. We have also discussed how to find data breaches using social medial platforms.

**Chapter 17: Understanding Encryption and Digital Certificates –** The learning objective for this chapter is to understand the fundamentals of encryption, symmetric, asymmetric, hashers, SSL, TLS, certificates, SSL stripping, and the weaknesses inherent in encryption. The objective of this chapter is to explain digital certificates along with its security risk and how to mitigate it.

**Chapter 18: Access Fake News –** In this chapter, we have discussed how to detect fake news. We have also explained topics like, what is fake news, how to identify it, why detect fake news and the efforts of various organisations towards tackling the issues of fake news.

**Chapter 19: Reverse Image Search –** Reverse image search is a technology that takes an image file as input and returns an output related to the image. Search engines that offer reverse image capability include Google, TinEye, Bing, Yandex, Baidu etc. In this chapter, we have explained cropped reverse image searching. After reading this chapter, you will be able to detect the differences between morphed and real images.

**Chapter 20: Geo-location –** In this chapter, we have explained how to use online maps such as google, yandex, bing , mapillary and many more. The aerial maps are helpful when you are trying to know about the street or other location. This is useful when law enforcement agencies want to move in a particular street/location for investigation purposes.

**Chapter 21: Identify Real Images –** In this chapter, we have explained how to detect websites for sharing photo and reveal the meta data of the photo such as longitude, latitude etc. We have also explained the default extension used by cameras when you capture the objects.

**Chapter 22: Use of Aadhaar and Social Security Number –** With the crime rates increasing day-by-day, governments have assigned a unique identification to each citizen that can help law enforcement agency track criminals. and cyber criminals. In this chapter, we have discussed the use of Aadhar, and Social Security Number.

**Chapter 23: Tracking Fraud SMS –** SMS services are used by various organizations to promote their product. Schools/colleges are also using SMS to provide information related to students' enrolment/examinations. This is the positive use of SMS services. In this chapter, we will understand how law enforcement agencies find who is behind a cyber crime by tracking a fraudster/malicious user's SMS sent to victims.

# Coloured Images

Please follow the link to download the
***Coloured Images*** of the book:

## https://rebrand.ly/fcw7v2n

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

# Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

**errata@bpbonline.com**

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

## Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

## If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

## Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

# Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

**https://discord.bpbonline.com**

# Table of Contents

# Chapter 1
# Setting up OSINT Environment

## Introduction

**Open-source Intelligence** (**OSINT**) is a technique to describe the search, collection, analysis, and use of information from open sources about a particular target. The target may be a cyber-criminal, a cyber-terrorist, or a public enemy. In other words, OSINT refers to all the information that is available to the general public. This information can be used for intelligence gathering. The investigation through OSINT requires an anonymous identity. Hence, in this chapter, we have explained the introduction as well as how to set up an OSINT lab for investigation.

## Structure

In this chapter, we will cover the following topics:

- Introduction to OSINT
- Setting up a virtual lab for OSINT
- Creating snapshots for VMs
- Introduction to Linux command line
- Antivirus
- VPN and its uses
- Lab using proton VPN

## Objectives

After reading this chapter, the reader will be able to understand the open-source intelligence tools and techniques and learn about setting up a lab using an open-source operating system, basic operating system commands, and its file system, along with the lab using a virtualization platform (virtual box).

## Introduction to OSINT

OSINT is the collection and analysis of data gathered from open sources, that is, publicly available sources (the sources may be websites/newspapers/others) to produce meaningful/actionable intelligence. The intelligence agencies use OSINT to track events, for example, weapons systems, public enemies, terrorists, cybercriminals, war-like situations, and so on. These are the targets of interest. Hence, OSINT is low-risk, cheap, and often highly effective. OSINT is completely legal because it only uses publicly available information through open sources. In

other words, it does not include information that is stored within an organization's database. A hacker uses OSINT to gather information before launching an attack on the target. Some of the OSINT sources are as follows:

- News and media
- Literature
- Social media
- Court filings
- Arrest records
- Public surveys
- Telephone directories
- Census data
- System vulnerability data
- Dark web
- Deep web

Online media and search engines make OSINT faster and easier, and social media is the most effective medium for gathering information about individuals/organizations. The OSINT investigator must have strong searching skills. Today, you can find most of the data on social media platforms using advanced searching techniques. The hackers and intelligence agencies view social media profiles on sites such as LinkedIn, Facebook, and Instagram and then take decisions accordingly based on the intelligence they have collected.

# Setting up the virtual lab for OSINT

In the following section, the documentation part is taken from the open-source virtual box website **https://www.virtualbox.org**. The *VirtualBox* provides the virtualization environment to set up the lab. The step-by-step process is given as follows:

The hardware/software requirements to set up the OSINT lab process are as follows:

- **Recommended hardware for Oracle VirtualBox**
  - **Memory**: 1.5 GB or 4 GB with Oracle XE
  - **Processor Type**: 32bit or 64-bit
  - **Processor speed**: 1.83 GHz
  - **Hard disk**: 5 GB
- **Recommended hardware for Linux-based operating system**
  - If hardware is running a 64-bit processor with virtualization capability (Intel VT-x or AMD-V*) and at least 3 GB of memory and 50 GB of disk space, then we can run two virtual machines, each with one GB RAM and one GB for the host machine.

  The user can perform the lab by using open-source software "VirtualBox" for Windows/Linux. You can download the 64-bit or 32-bit VBox, depending on the processor architecture. The virtual box is a virtualization platform where users can install multiple operating systems on a single host. It is also known as hosted virtualization. The step-by-step process is as follows:

1. Open the web browser and access **https://www.virtualbox.org/wiki/Downloads.** Then, select **Windows hosts** if you want to install it on the Windows operating system.
2. Double-click on **downloaded exe**. This would display *Figure 1.1*. Click on the **Next** button:


***Figure 1.1**: Welcome wizard*

3. This would display the location where your VBox file would be installed. You can change the file location by using the **Browse** button. Then, click on the **Next** button, as shown in *Figure 1.2:*

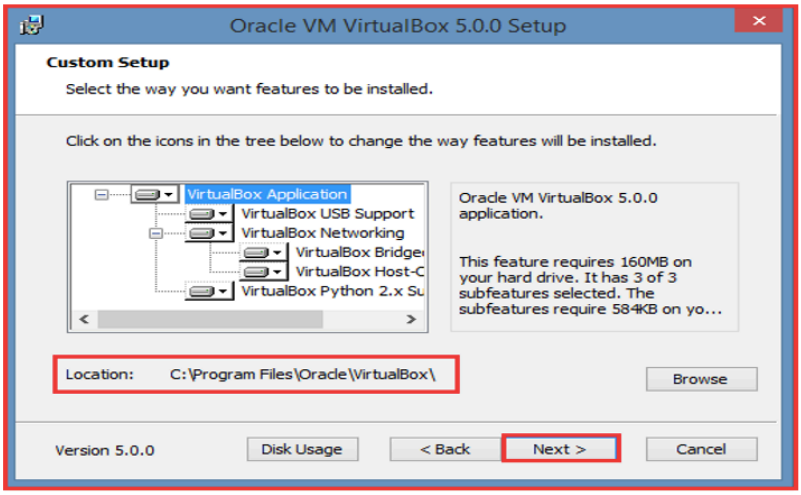


***Figure 1.2**: Location selection for installation*

4. Now, click on the **Next** button, as shown in *Figure 1.3:*

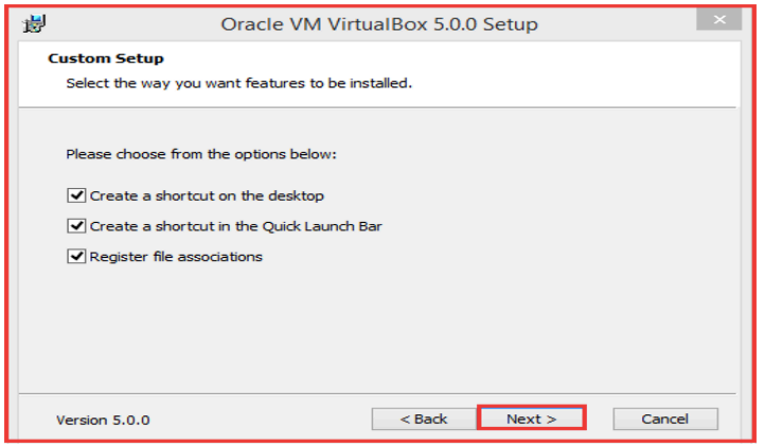


***Figure 1.3**: Selecting options*

5. This will reset the network connection temporarily and will install the **Network interface card** for VBox. Click on the **Yes** button, as shown in *Figure 1.4*:

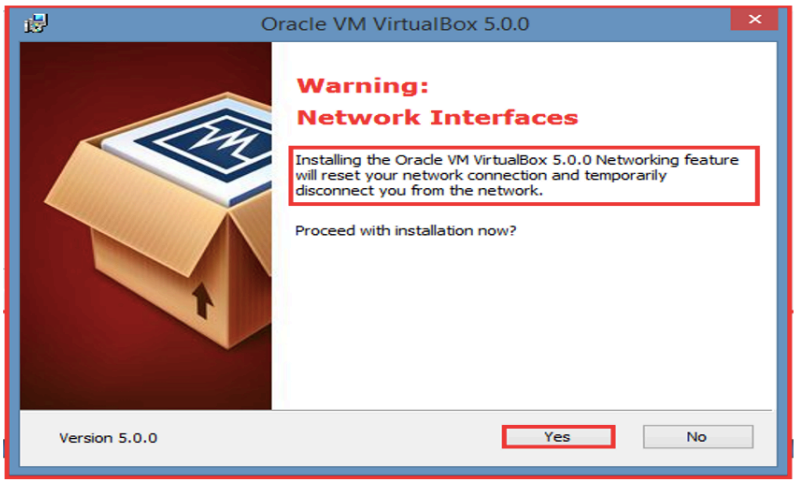


***Figure 1.4**: Network connection resetting wizard*

6. Click on the **Install** button, as shown in *Figure 1.5*:

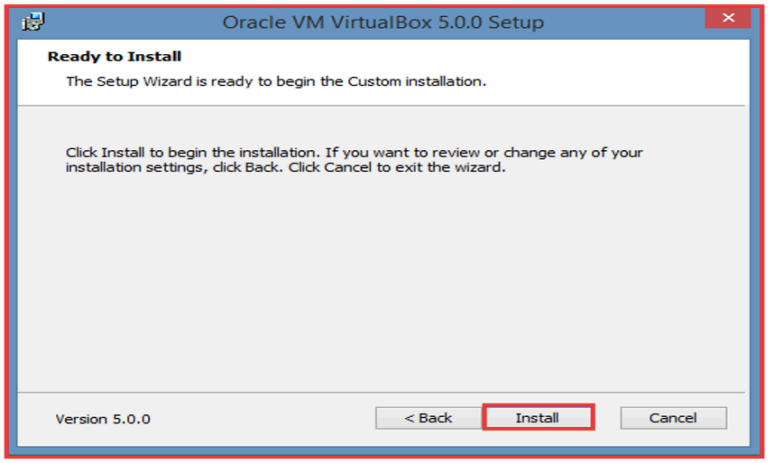


***Figure 1.5**: Installation wizard*

7. Now, the installation process will start. Refer to *Figure 1.6:*

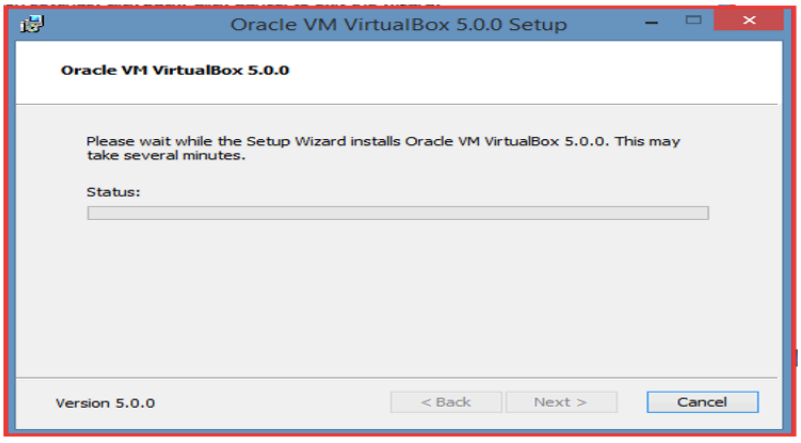


***Figure 1.6**: Installing software*

8. A user access control window would be displayed. Click on the **Yes** button to allow the VBox. Then click on the **Install** button, as shown in *Figure 1.7:*

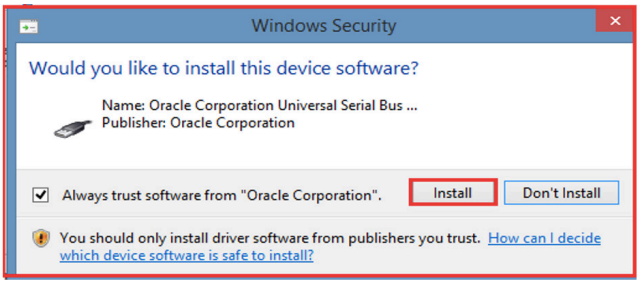


***Figure 1.7**: Installing device*

9. Click on the **Finish** button, as shown in *Figure 1.8:*


***Figure 1.8**: Installation complete wizard*

10. In *Figure 1.9,* we can see that VBox is installed:

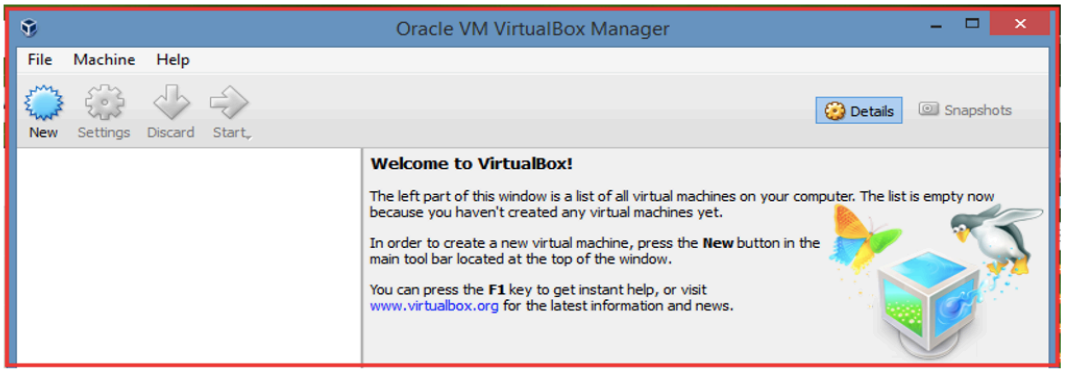


***Figure 1.9**: Displaying virtual box in default mode*

11. Now download the virtual machine for OSINT using the website **https://www.tracelabs.org/initiatives/osint-vm** and then import the OVA file on the virtual box, as shown in *Figure 1.10:*

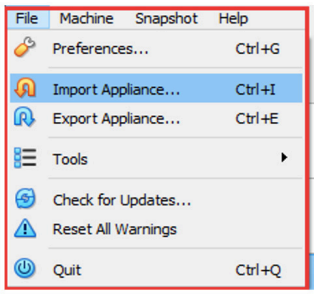


***Figure 1.10**: Importing appliances*