MANIPAL INSTITUTE OF TECHNOLOGY
BENGALURU
(A constituent unit of MAHE, Manipal)

B.TECH. SIXTH SEMESTER

DEPARTMENT

OF

INFORMATION TECHNOLOGY

B. Tech CSE (CYBER SECURITY)

Cyber Security and Forensics Lab (CSF Lab) (IT_ 3262)

LABORATORY MANUAL

MANIPAL INSTITUTE OF TECHNOLOGY
BENGALURU
(A constituent unit of MAHE, Manipal)

IT 3262

Manipal Academy of Higher Education, Bengaluru

DEPARTMENT OF INFORMATION TECHNOLOGY

CERTIFICATE

This is to certify that Ms./Mr. ……………..………………………………………………………………………..

Reg. No.: ………………………………………… Section: …………………… Roll No.: …………………………

has satisfactorily completed the **LAB EXERCISES PRESCRIBED FOR Cyber Security and Forensics Lab (IT_ 3262)** of Third Year-Sixth semester, B.Tech. Degree in Computer Science and Engineering-Cyber Security at MIT, Bengaluru, in the Academic Year2024– 2025.

Date: ………………………………

Signature
Faculty In Charge

CONTENTS

Course Objectives and Outcomes

The main objective of the course are as follows:

- To enable the students to setup a virtual machine and install kali Linux.
- To enable the students to develop the skill to identify the stages of attacks and
- identify tools for each of these stages.
- To enable the students to develop the skill of packet analysis through various tools.
- To enable the students to develop skills to demonstrate different security attacks
- using the existing tools in kali Linux.
- To enable the students to develop to implement different cryptographic
- algorithms.
- To enable the students to design and develop a project related to the cyber security
- domain

Course Outcomes: At the end of the course, students will be able to

- Identify and analyse the real-world network traffic using the tools in Kali Linux
- Implement and demonstrate the working of cryptographic algorithms and also able to demonstrate web-based attack and generate self-signed certificates using the tools .
- Implement the organization rules to firewalls and intrusion detection system.
- Demonstrate security attacks and able to perform Memory capture and perform analysis on it

Evaluation plan

- Internal Assessment Marks: 60%
- Continuous evaluation component which includes as follows:
- **Regular Lab :30 Marks**
- *Total 3 rounds each of 10 marks -10*3=30*
- *Record /file :03 marks*
- *Execution: 02 marks*
- *Viva :05marks*
- **Project :30 Marks**
- Synopsis (Hard copy)-5 marks
- Synopsis presentation -5 marks
- ***End evaluation:20***
- Presntation:05 Marks
- Implementation:10 Marks
- Report :05 Marks
- **End semester assessment of 2-hour duration: 40 %**

- The Execution will carry 20 marks (15 marks- program & 5 marks -tool)

- The Viva will be for 10 marks

- The write up will be for 10 marks

INSTRUCTIONS TO THE STUDENTS

Pre-Lab Session Instructions

1. Students should carry the Lab Manual Book and the required stationery to every lab session

2. Be in time and follow the institution dress code

3. Must Sign in the log register provided

4. Make sure to occupy the allotted seat and answer the attendance

5. Adhere to the rules and maintain the decorum

In-Lab Session Instructions

- Follow the instructions on the allotted exercises
- Show the program and results to the instructors on completion of experiments
- On receiving approval from the instructor, copy the program and results in the Lab record
- Prescribed textbooks and class notes can be kept ready for reference if required

General Instructions for the exercises in Lab

- Implement the given exercise individually and not in a group.
- The programs should meet the following criteria:

o Programsshould be interactive with appropriate prompt messages, error messages if any, and descriptive messages for outputs.

o Programs should perform input validation (Data type, range error, etc.) and give appropriate error messages and suggest corrective actions.

o Comments should be used to give the statement of the problem and every member function should indicate the purpose of the member function, inputs and outputs.

o Statements within the program should be properly indented.

o Use meaningful names for variables, classes, interfaces, packages and methods.

o Make use of constant and static members wherever needed.

- Plagiarism (copying from others) isstrictly prohibited and would invite severe penalty in evaluation.
- The exercises for each week are divided under three sets:

o Solved exercise

o Lab exercises – to be completed during lab hours

o Additional Exercises – to be completed outside the lab or in the lab to enhance the skill which will be informed by instructor during the lab session.

- In case a student misses a lab class, he/she must ensure that the experiment is completed during the repetition class with the permission of the faculty concerned but credit will be given only to one day’s experiment(s).

• Questions for lab tests and examination are not necessarily limited to the questions in the manual but may involve some variations and / or combinations of the questions.

• A sample note preparation is given as a model for observation.

Mini Project

Objectives and Guidelines

Objectives:

• Select a domain and identify the possible innovative work in it.

• Formulate the synopsis for mini project by briefly describing the domain.

• List the requirements that can be implemented in the project.

• Implement the functional requirements by identifying appropriate concept.

• Front end design emphasis is very less core working is of relevance.

Guidelines: All the students are instructed to form a team of three members. The team members must be from the same lab batch. Once the synopsis is submitted, no change of team member(s) shall be entertained. A single copy of the Synopsis must be submitted by the team on or before the end of the fourth week. Title and code of the mini project should be unique among the teams.

Synopsis Format:

• Title, Team Members

• Abstract (Briefly describe the selected domain and various functionalities that can be modelled via Object Oriented Concepts)

• Flowchart to show the entire working model of the project

• Functional Requirements (List all the functions that the working project can demonstrate)

• Expected output of the project

PROJECT REPORT FORMAT

- Front Page, Title, Team Members.
- Certificate
- DECLARATION
- ABSTRACT
- Table of contents
- List of figures and tables.
- Introduction
- Requirement analysis
- Functional requirements
- Design & development
- Conclusion & future work
- References
- Appendix

General Guidelines

The students should not

- Bring mobile phones or any other electronic gadgets to the lab.
- Go out of the lab without permission

Project deadlines and other details

S.I.N.o.	Task	Date	Submission details
1	Identification of team members (max of 3 in team)	17th Jan 2025 5 PM	CR will collect and submit team details in soft copy format
2	Identification of project and submission of synopsis (please mention the time line,objective,individual contribution etc)	31st Jan 2025 5 PM	Hard copy of synopsis by the team to the instructor in person
3	Synopsis presentation	1st and 2nd week of february during Lab hours	Proper PPT with Objectives, Individual contribution etc
4	Final Presentation	2 weeks before the End semester Lab examination	Report has to be submitted 2 days before the presentation to the instructor

LAB NO: 1 **Date:**

INSTALLATION OF
VIRTUAL BOX, KALI LINUX

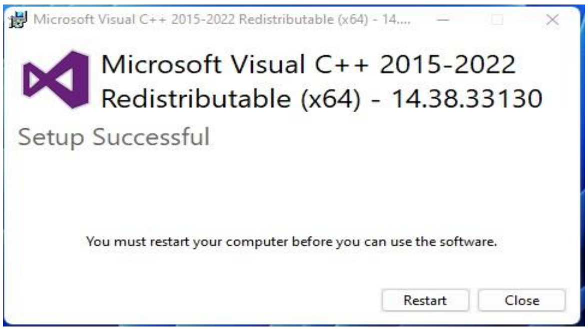
Objectives:

In this lab, student will be able to:

- Identify the prerequisite to set up Kali linux to perform experiments in further labs.
- Configure the Oracle VM Box.
- Viewing the graphical interface and dirt their hands on the kali linux.
- Identify and list out different tools available in Kali Linux platform.

Installation Steps:

1. Install VC_redist.x64.exe



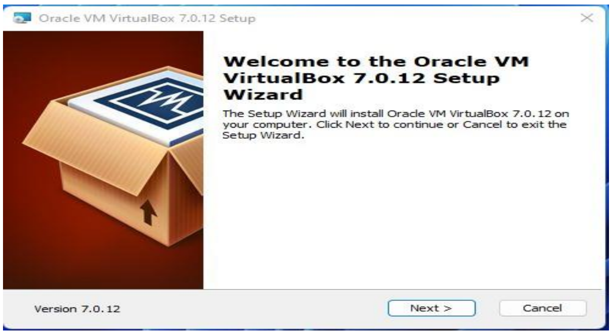
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14....

Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.38.33130

Setup Successful

You must restart your computer before you can use the software.

2. Install VirtualBox-7.0.12-159484-Win.exe



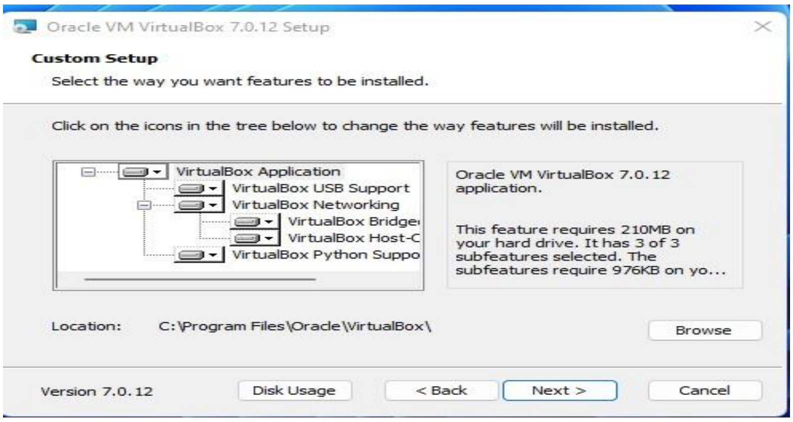
Oracle VM VirtualBox 7.0.12 Setup

Welcome to the Oracle VM VirtualBox 7.0.12 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 7.0.12 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Version 7.0.12

3. Select default settings



Oracle VM VirtualBox 7.0.12 Setup

Custom Setup

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridge
VirtualBox Host-C
VirtualBox Python Suppo

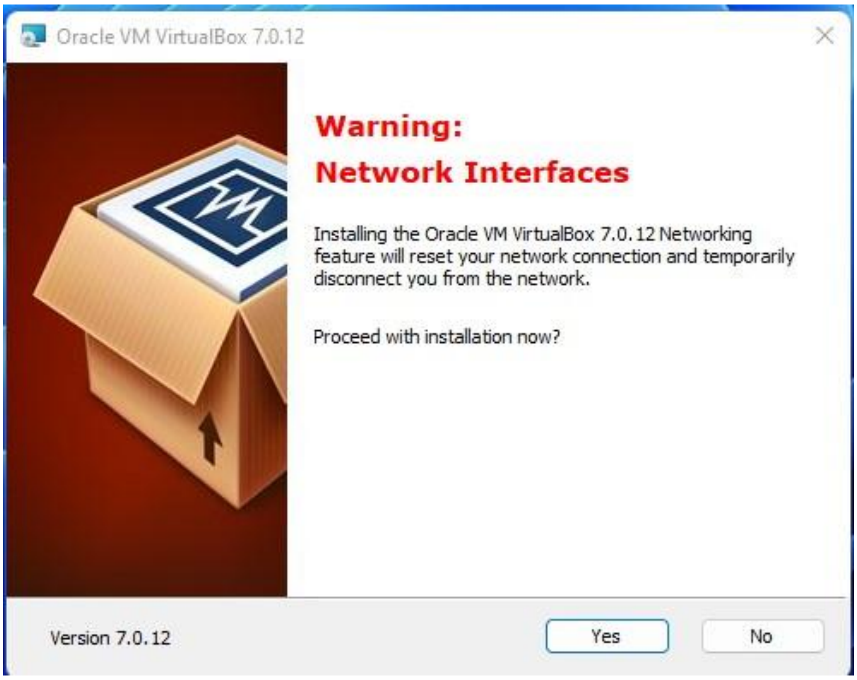
Oracle VM VirtualBox 7.0.12 application.

This feature requires 210MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 976KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

Version 7.0.12

4. Proceed installation



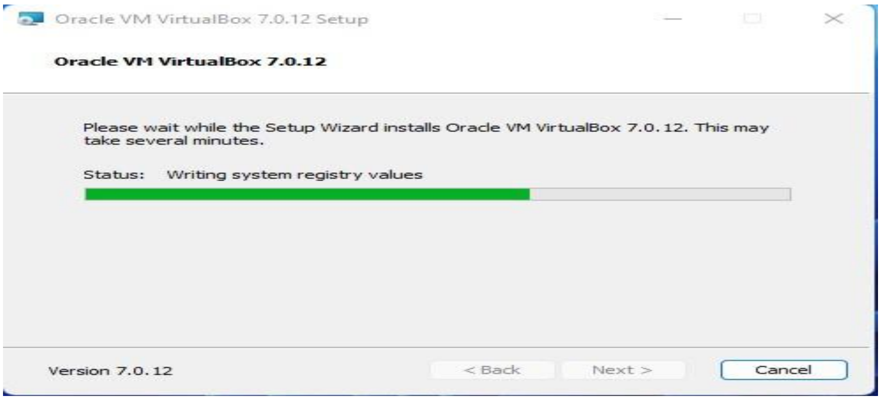
Oracle VM VirtualBox 7.0.12

Warning:
Network Interfaces

Installing the Oracle VM VirtualBox 7.0.12 Networking feature will reset your network connection and temporarily disconnect you from the network.

Proceed with installation now?

Version 7.0.12



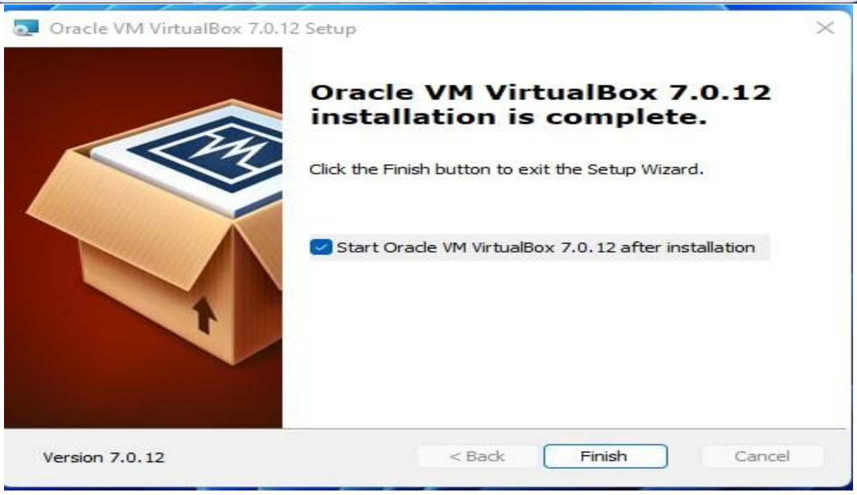
Oracle VM VirtualBox 7.0.12 Setup

Oracle VM VirtualBox 7.0.12

Please wait while the Setup Wizard installs Oracle VM VirtualBox 7.0.12. This may take several minutes.

Status: Writing system registry values

Version 7.0.12



Oracle VM VirtualBox 7.0.12 Setup

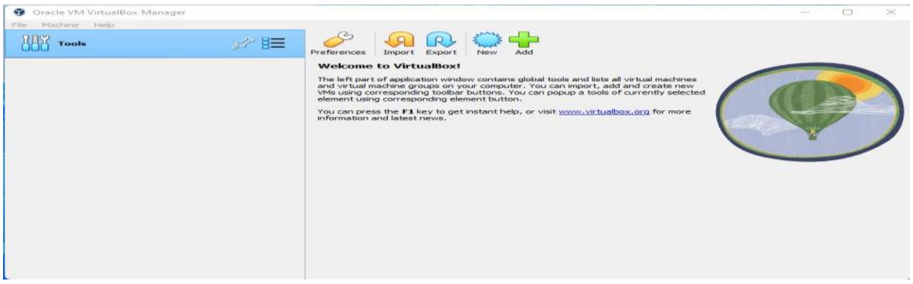
Oracle VM VirtualBox 7.0.12 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 7.0.12 after installation

Version 7.0.12

5. Select new in VB window

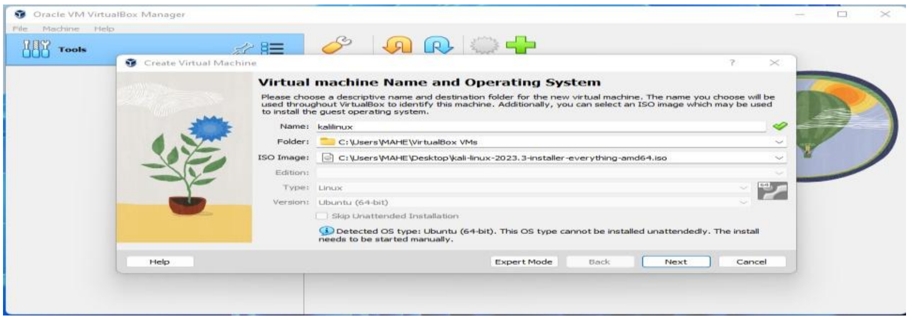


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

6. Give the Details regarding kalilinux and select ISO file from desktop



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: kalilinux

Folder: C:\Users\MAHE\VirtualBox VMs

ISO Image: C:\Users\MAHE\Desktop\kali-linux-2023.3-installer-everything-amd64.iso

Edition:

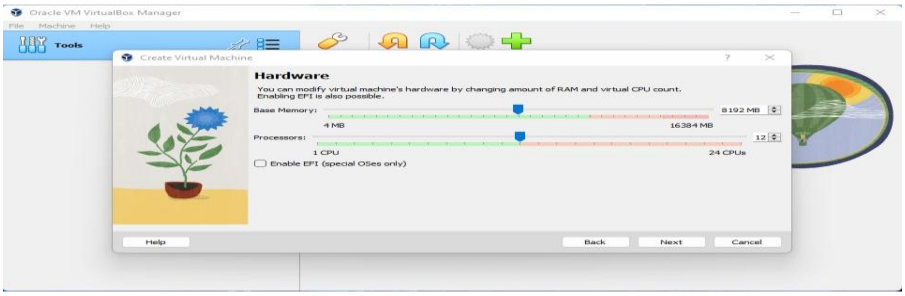
Type: Linux

Version: Ubuntu (64-bit)

☐ Skip Unattended Installation

Detected OS type: Ubuntu (64-bit). This OS type cannot be installed unattendedly. The install needs to be started manually.

7. Define RAM as 8GB AND 12 PRCOESSORS



Hardware

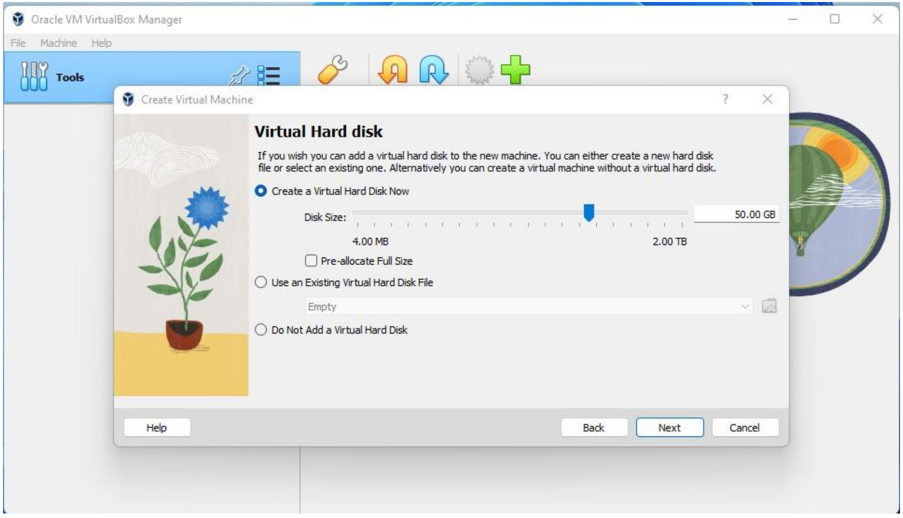
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 8192 MB

Processors: 12

☐ Enable EFI (special OSes only)

8. Provide 50GB space



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 50.00 GB

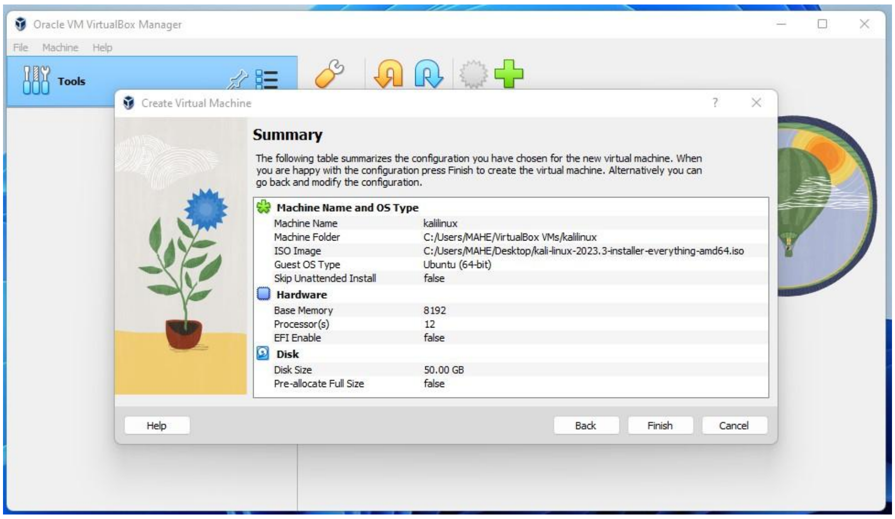
☐ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

Empty

○ Do Not Add a Virtual Hard Disk

9. Finish settings

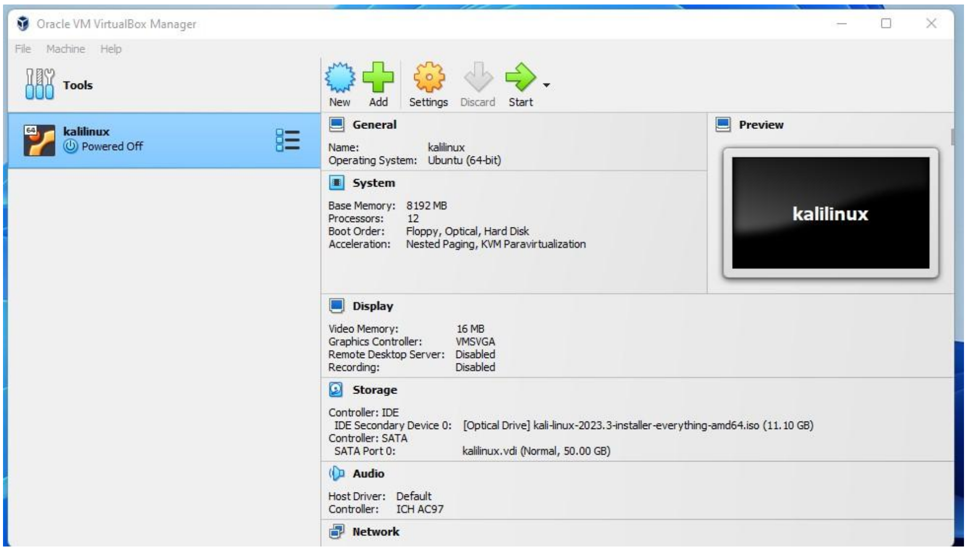


Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	kalilinux
Machine Folder	C:/Users/MAHE/VirtualBox VMs/kalilinux
ISO Image	C:/Users/MAHE/Desktop/kali-linux-2023.3-installer-everything-amd64.iso
Guest OS Type	Ubuntu (64-bit)
Skip Unattended Install	false
Hardware	
Base Memory	8192
Processor(s)	12
EFI Enable	false
Disk	
Disk Size	50.00 GB
Pre-allocate Full Size	false

10. Start Kali linux iso



General

```
Name:              kalilinux
Operating System:  Ubuntu (64-bit)
```

System

```
Base Memory:   8192 MB
Processors:    12
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, KVM Paravirtualization
```

Display

```
Video Memory:           16 MB
Graphics Controller:    VMSVGA
Remote Desktop Server:  Disabled
Recording:              Disabled
```

Storage

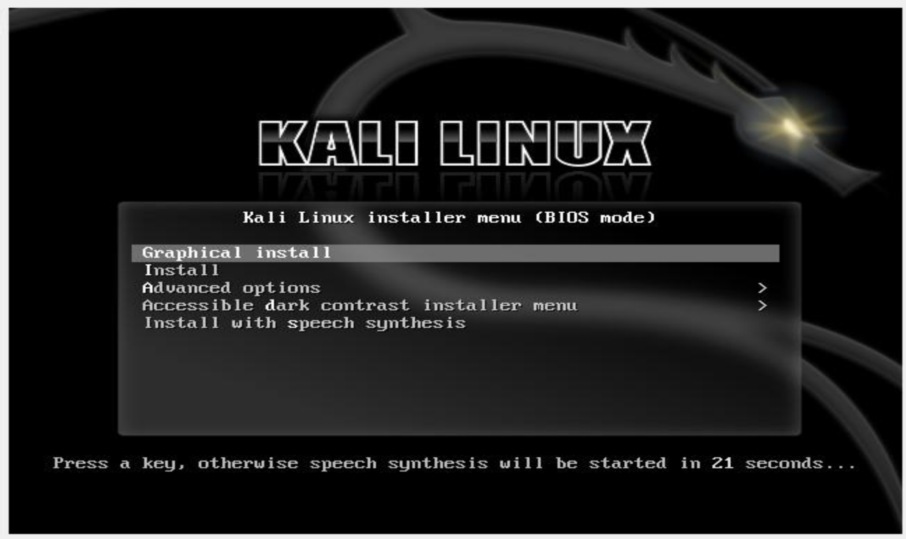
```
Controller: IDE
 IDE Secondary Device 0:  [Optical Drive] kali-linux-2023.3-installer-everything-amd64.iso (11.10 GB)
Controller: SATA
 SATA Port 0:             kalilinux.vdi (Normal, 50.00 GB)
```

Audio

```
Host Driver:  Default
Controller:   ICH AC97
```

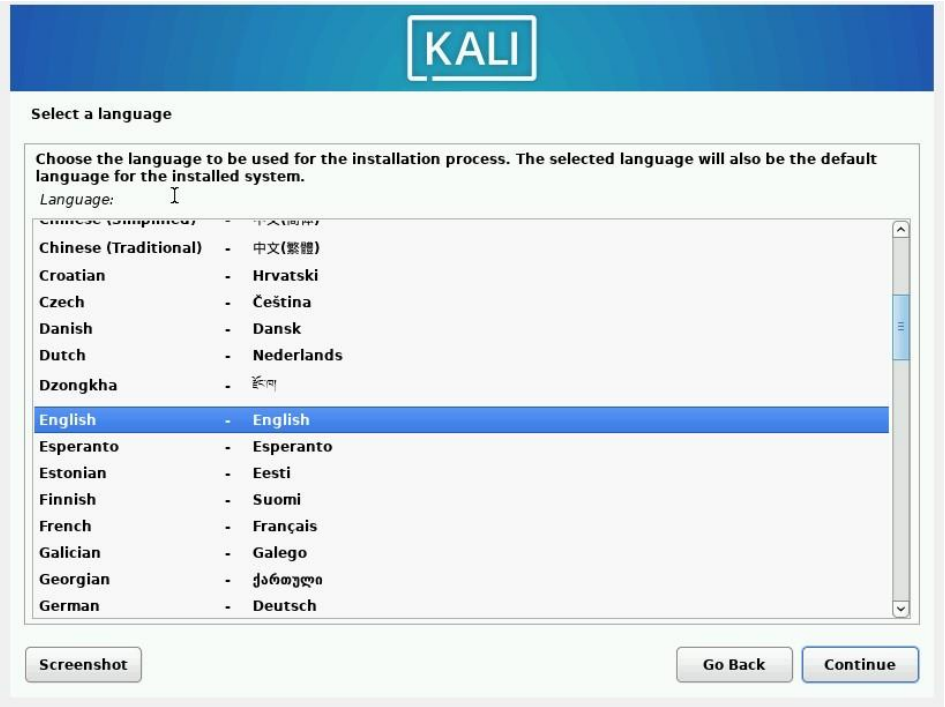
Network

11. Select graphical install



```
Kali Linux installer menu (BIOS mode)

Graphical install
Install
Advanced options                                    >
Accessible dark contrast installer menu             >
Install with speech synthesis

Press a key, otherwise speech synthesis will be started in 21 seconds...
```

12. Select language as English



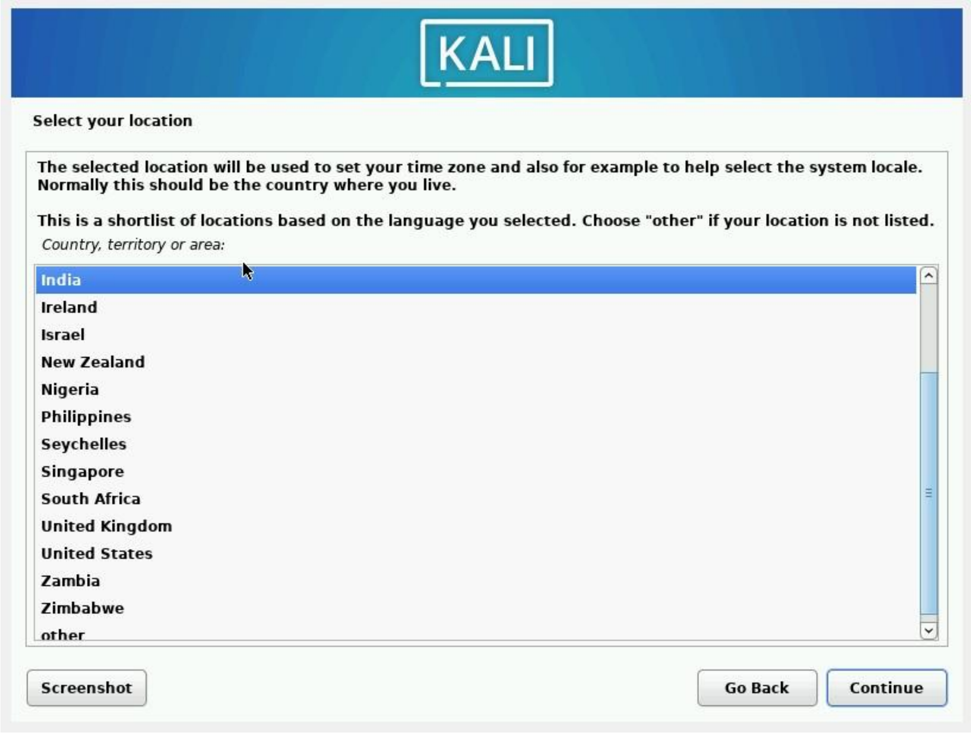
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

13. Select region



Select your location

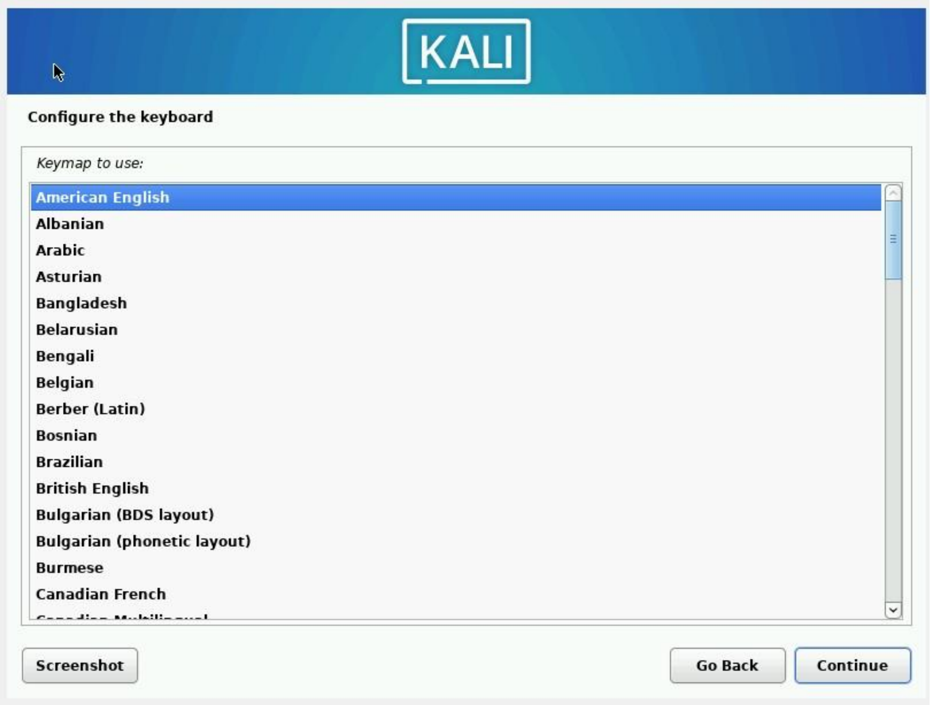
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

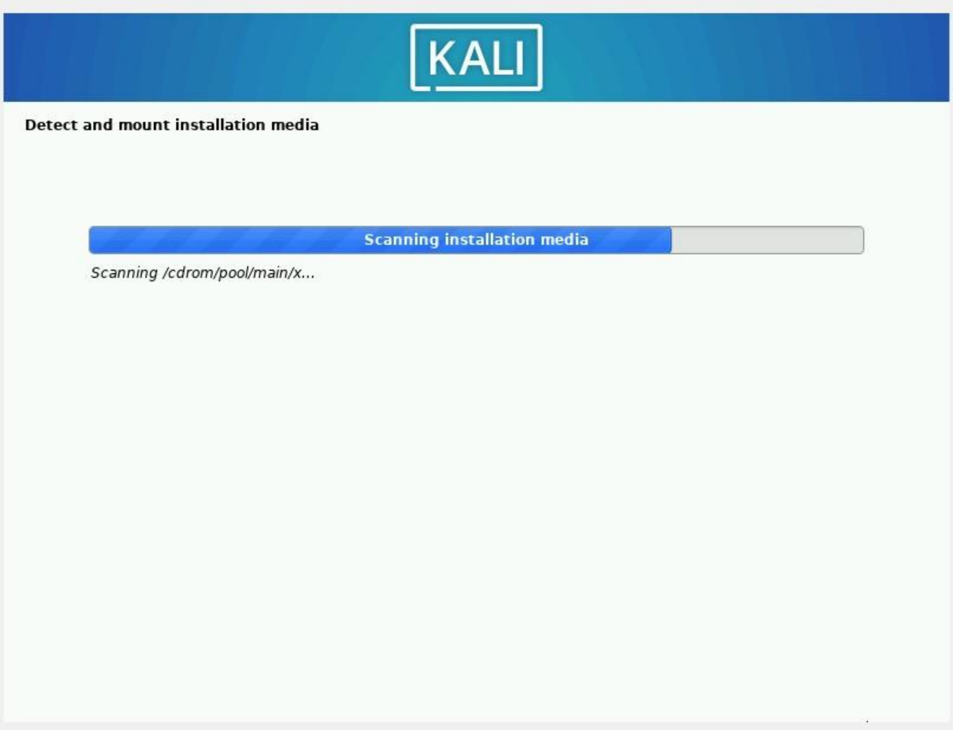
14. Select keyboard language



Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Berber (Latin)
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French

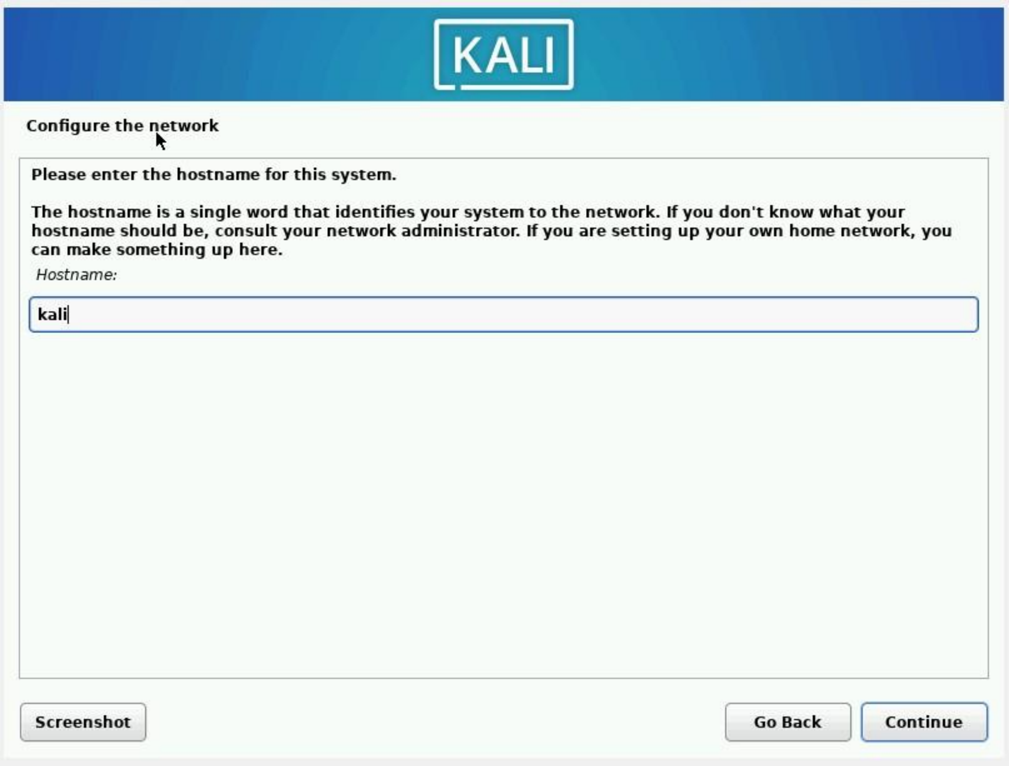


Detect and mount installation media

Scanning installation media

Scanning /cdrom/pool/main/x...

15. Hostname should be “kali”



Configure the network

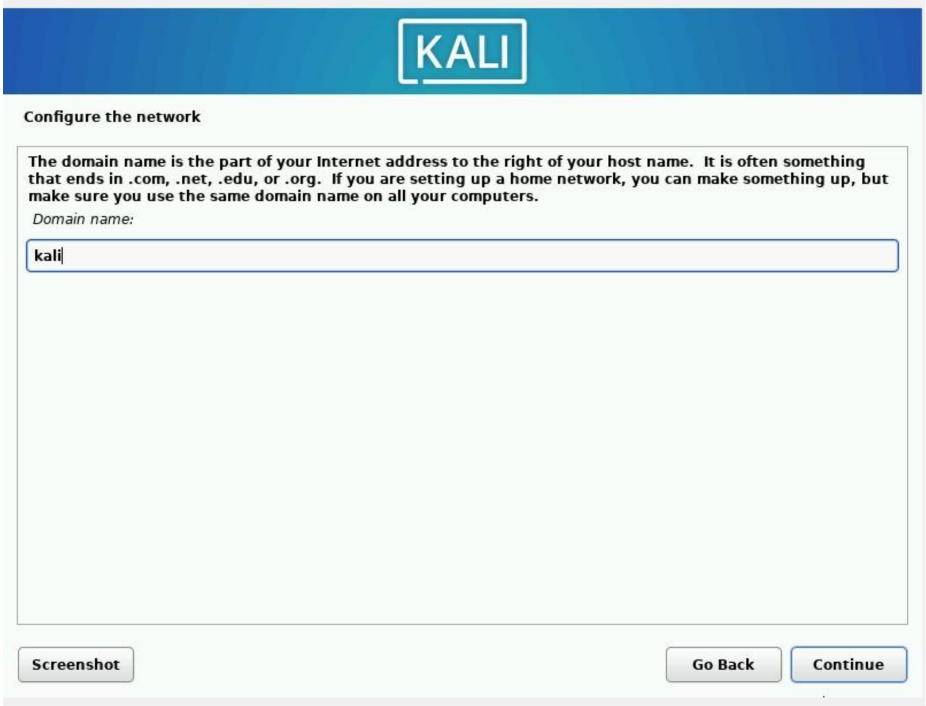
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

16. Domain name should be "kali"



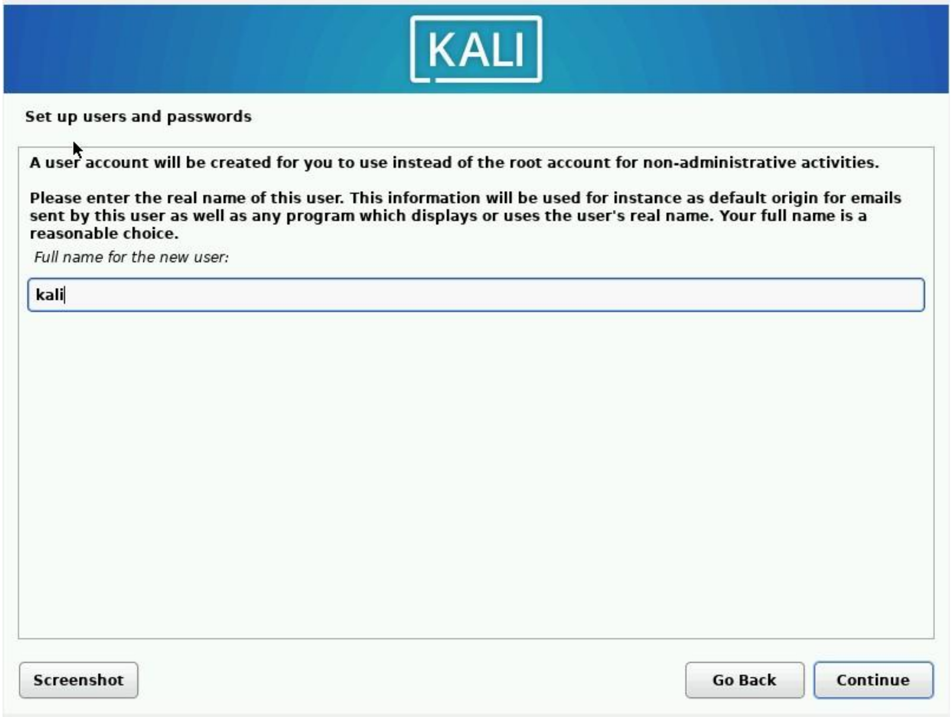
Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

kali

17. User name should be "kali"



Set up users and passwords

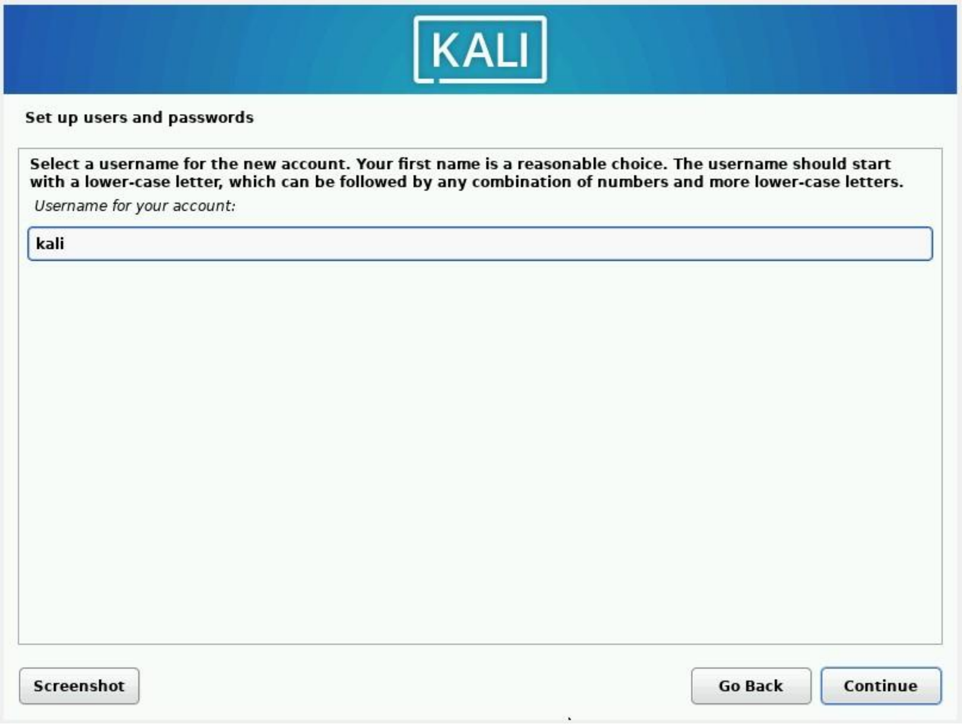
A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

kali

18. Username for account should be “kali”



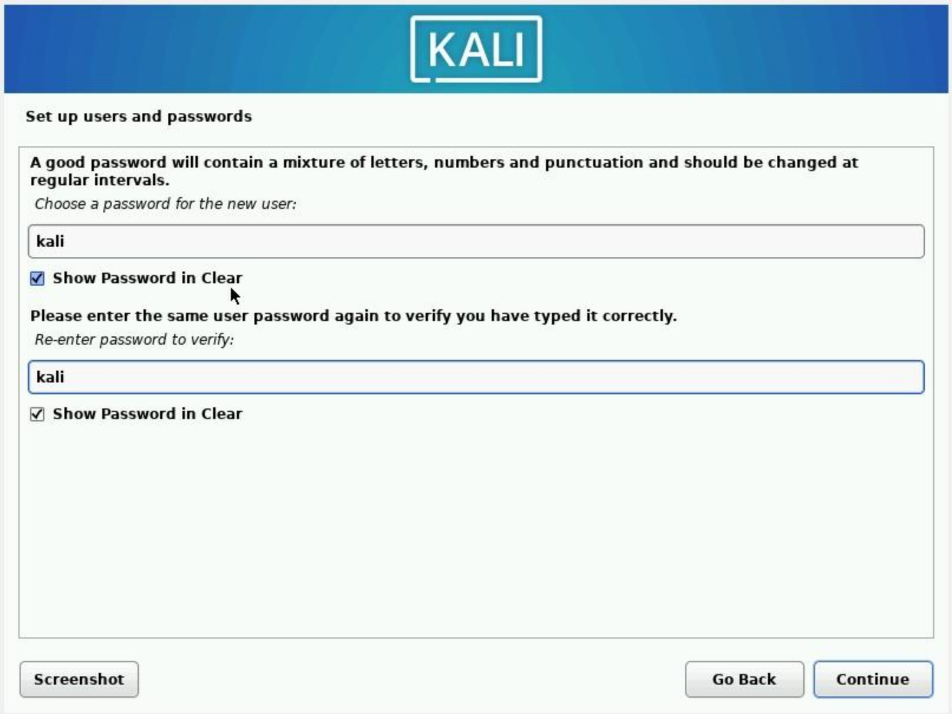
Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

kali

19. Password should be “kali”



Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

kali

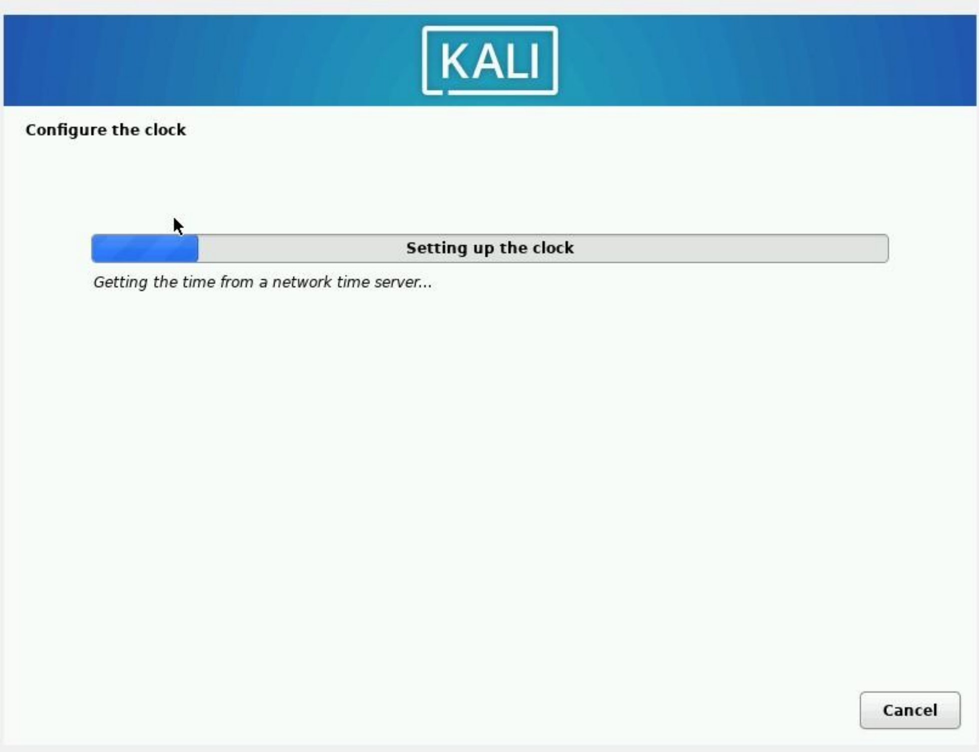
☑ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

kali

☑ Show Password in Clear

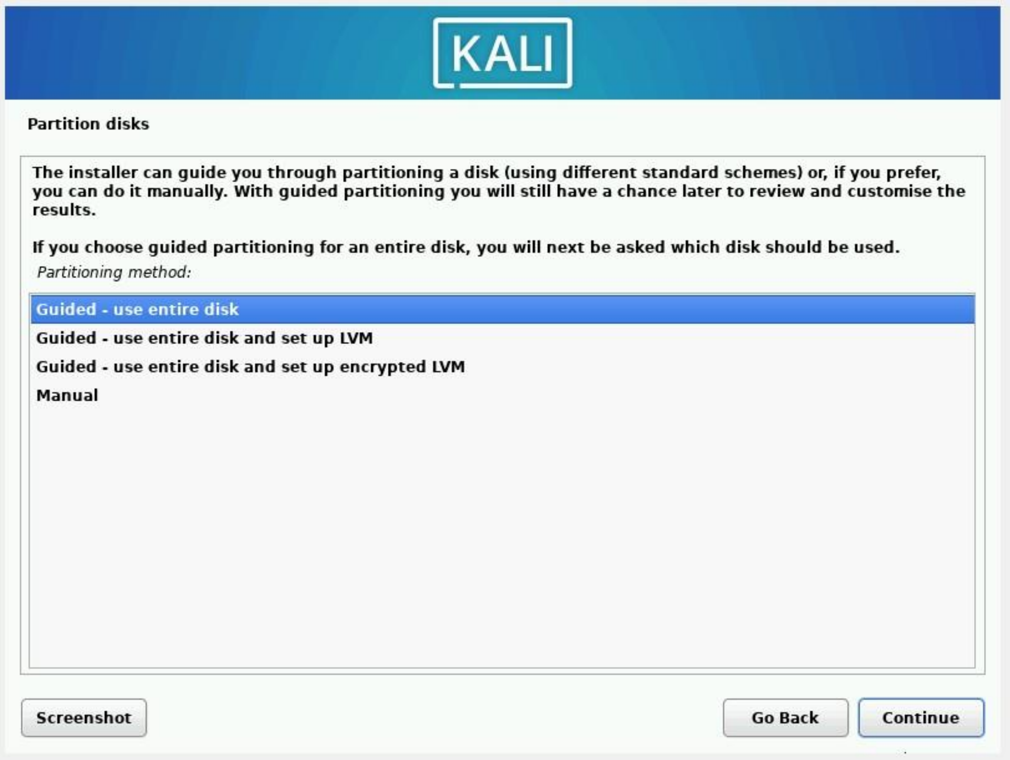


Configure the clock

Setting up the clock

Getting the time from a network time server...

20. Select entire disk



Partition disks

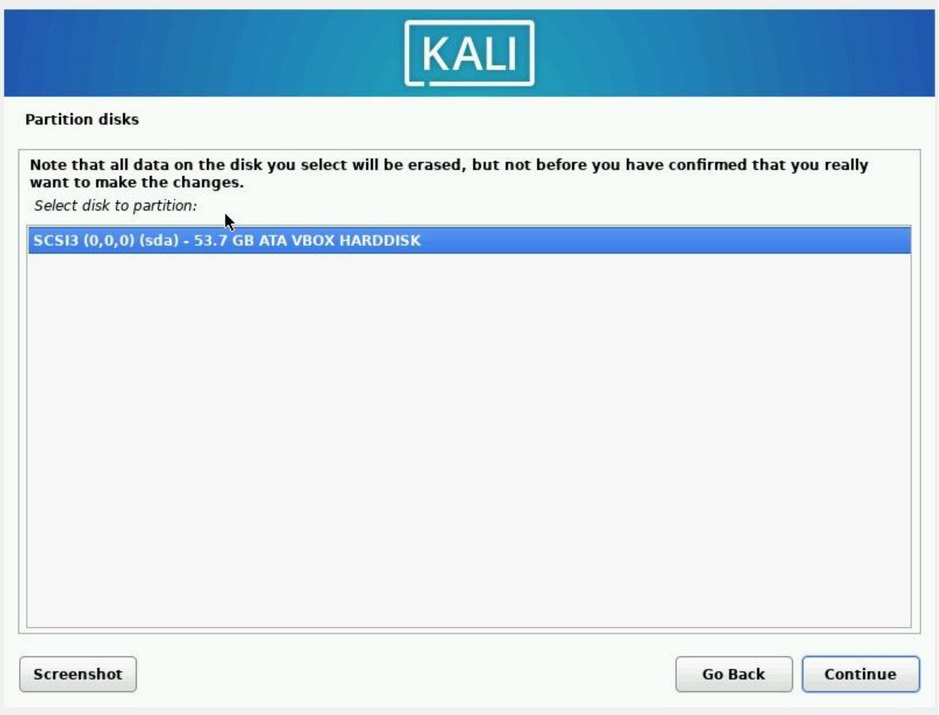
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

21. Select ATA VBOX HARDDISK



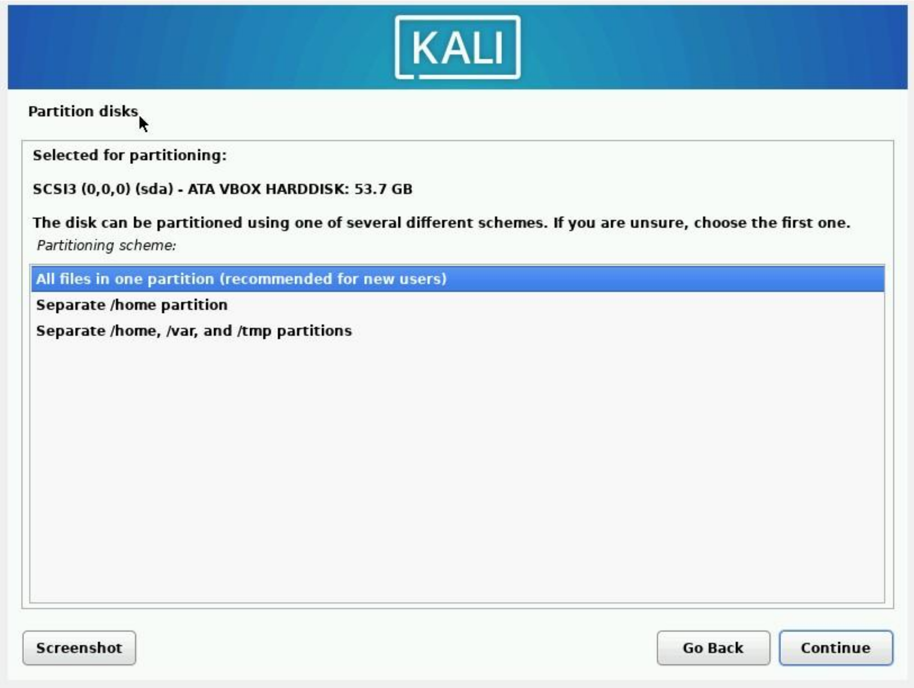
Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

- SCSI3 (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK

22. All files should be in one partition



Partition disks

Selected for partitioning:

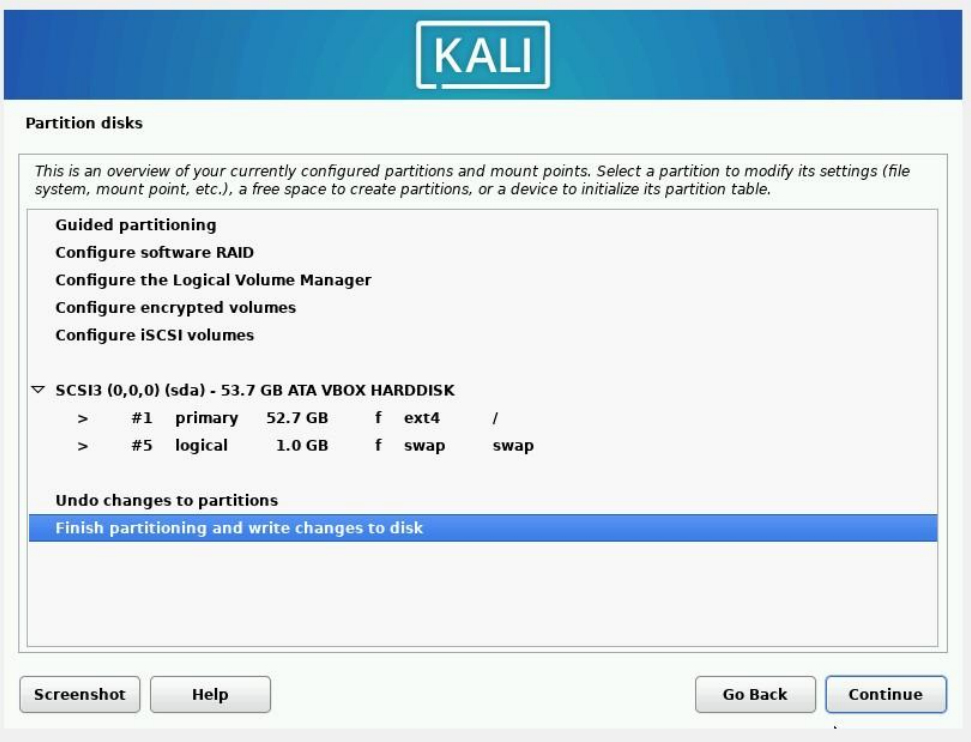
SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 53.7 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions

23. Finish partitioning

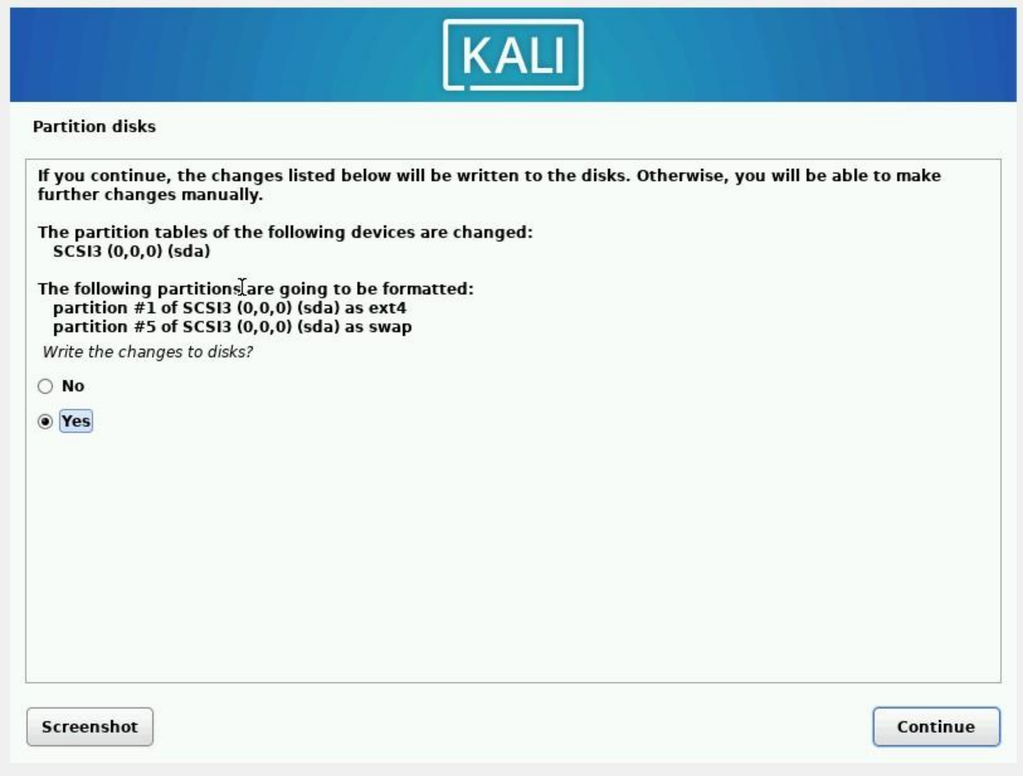


Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 53.7 GB ATA VBOX HARDDISK
     >    #1   primary   52.7 GB    f   ext4      /
     >    #5   logical    1.0 GB    f   swap      swap

Undo changes to partitions
Finish partitioning and write changes to disk
```

24. Select yes to write changes to disks.



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

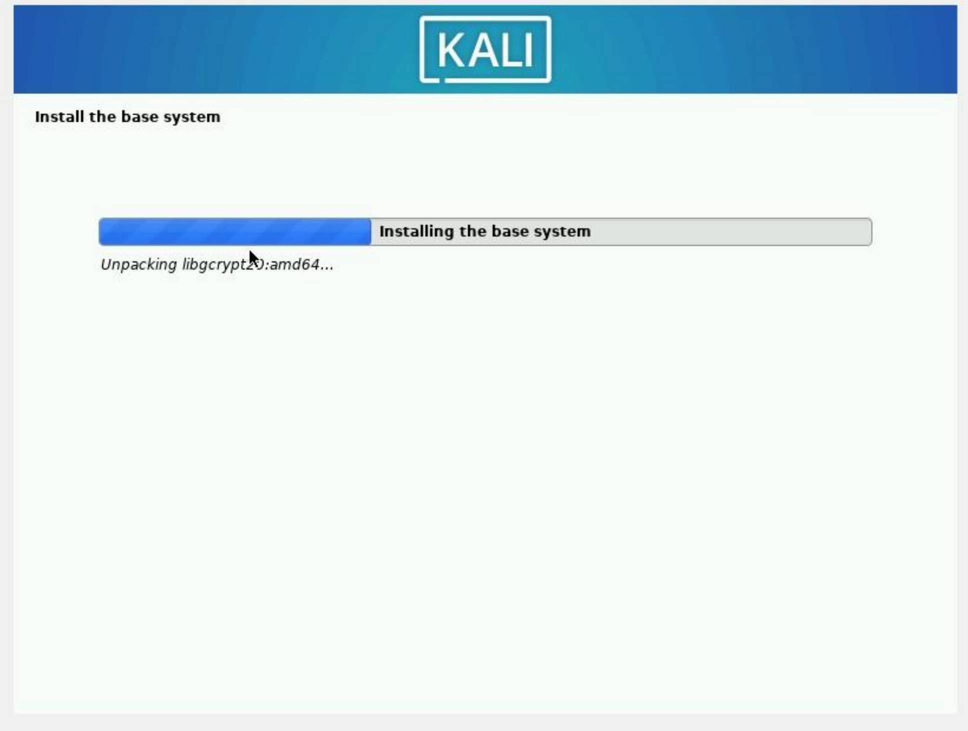
The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

○ No

● Yes

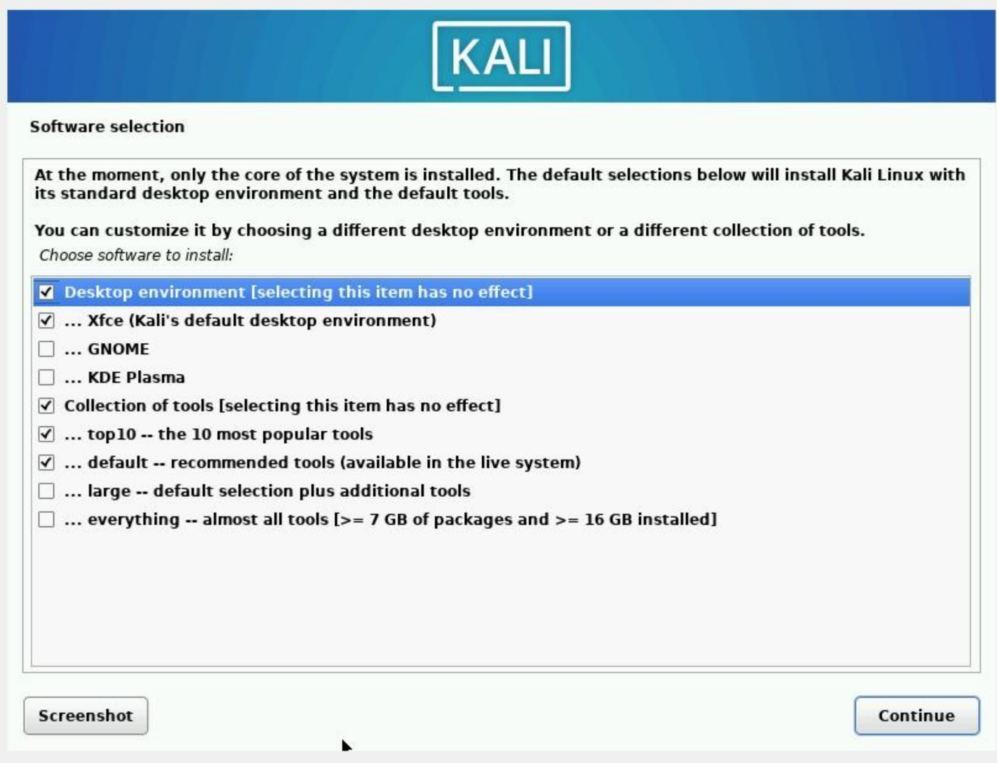


Install the base system

Installing the base system

Unpacking libgcrypt20:amd64...

25. Select continue without making changes



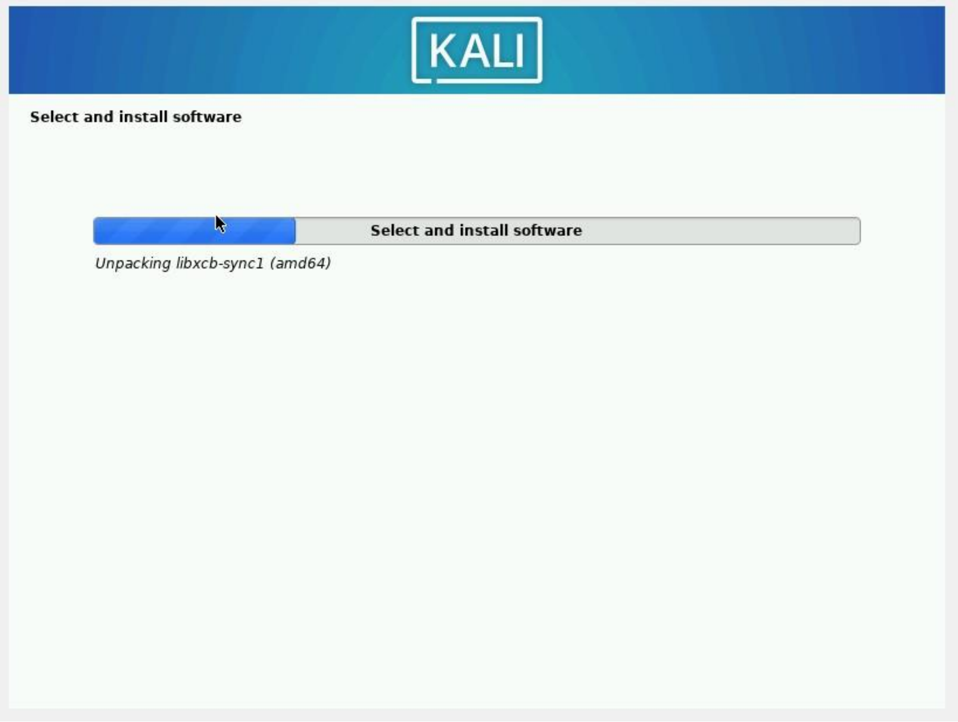
Software selection

At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of tools.

Choose software to install:

- ☑ Desktop environment [selecting this item has no effect]
- ☑ ... Xfce (Kali's default desktop environment)
- □ ... GNOME
- □ ... KDE Plasma
- ☑ Collection of tools [selecting this item has no effect]
- ☑ ... top10 -- the 10 most popular tools
- ☑ ... default -- recommended tools (available in the live system)
- □ ... large -- default selection plus additional tools
- □ ... everything -- almost all tools [>= 7 GB of packages and >= 16 GB installed]

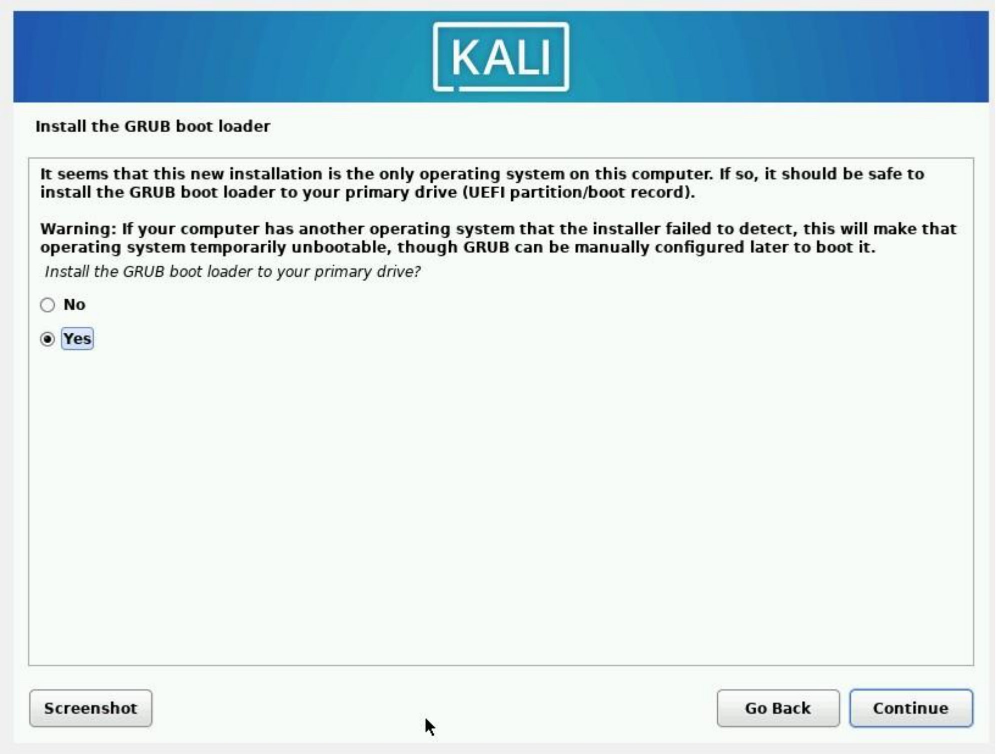


Select and install software

Select and install software

Unpacking libxcb-sync1 (amd64)

26. Select yes for GRUB loader and click on continue



Install the GRUB boot loader

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

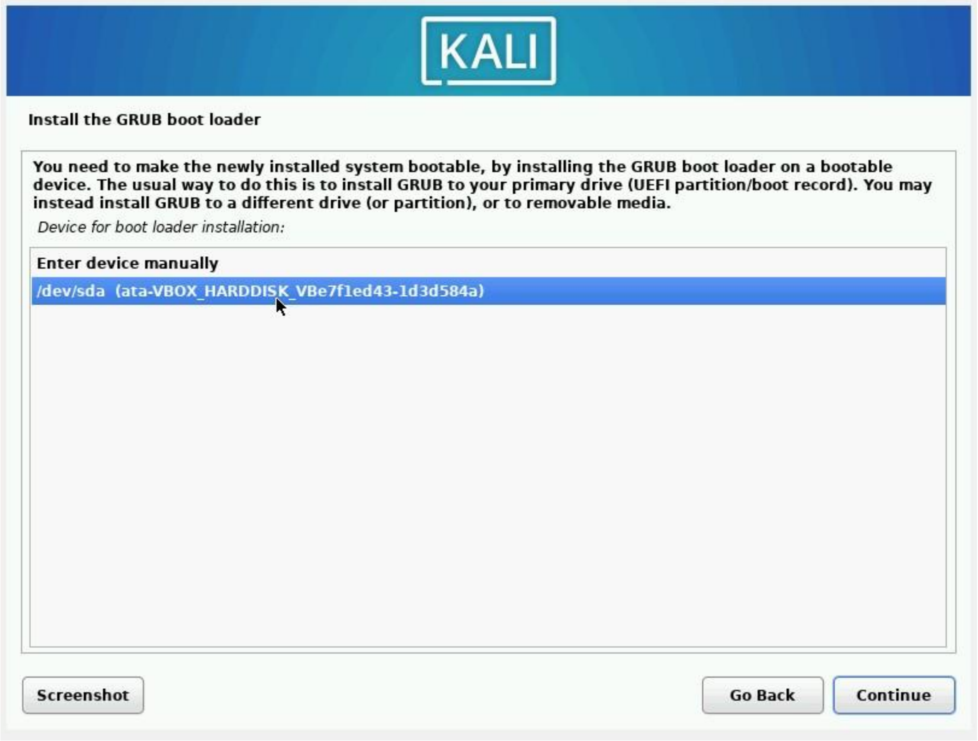
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to your primary drive?

○ No

● Yes

27. Select VBOX hard disk and click continue



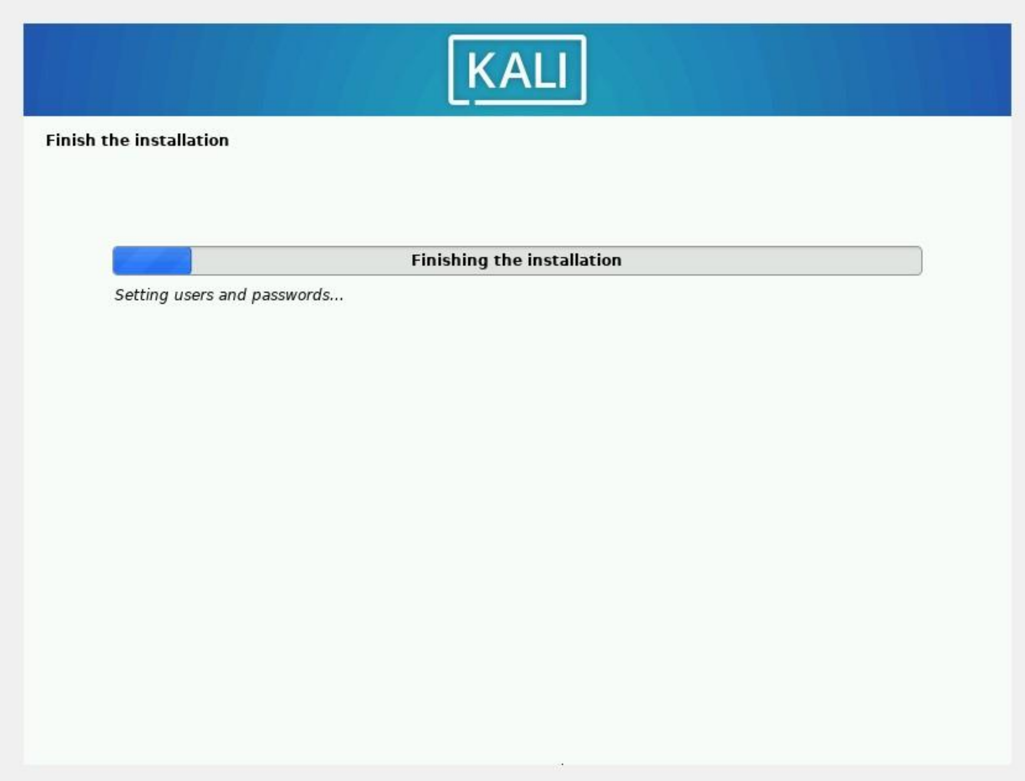
Install the GRUB boot loader

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

Device for boot loader installation:

Enter device manually

/dev/sda (ata-VBOX_HARDDISK_VBe7f1ed43-1d3d584a)

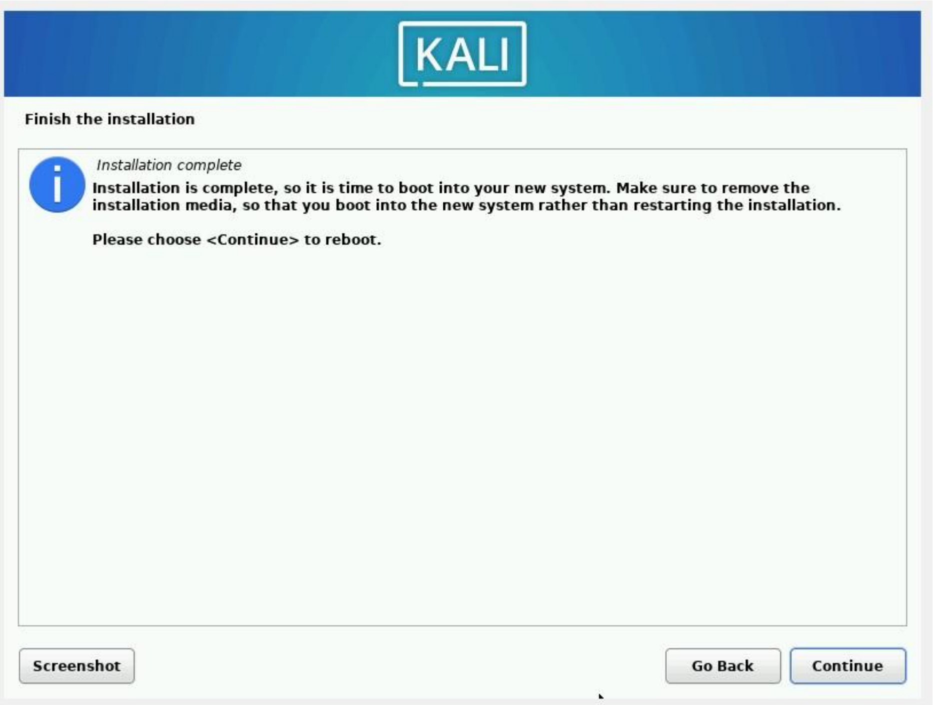


Finish the installation

Finishing the installation

Setting users and passwords...

28. Select continue and finish installation



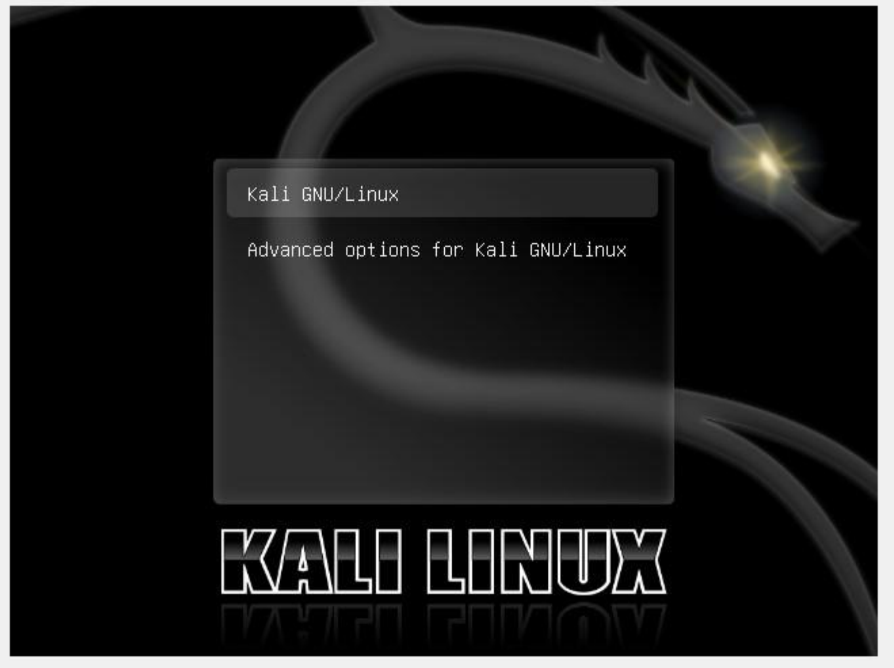
Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

Please choose <Continue> to reboot.

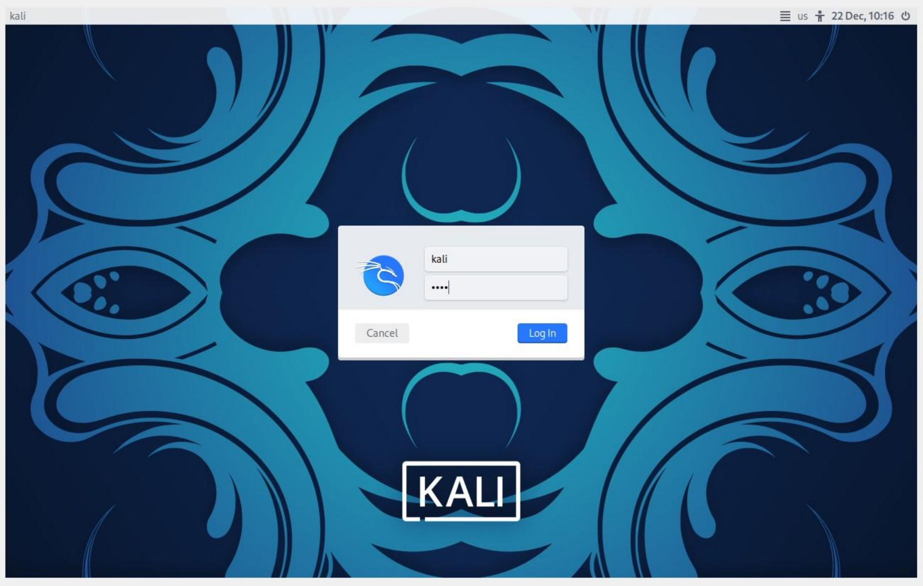
29. Restart and select Kali GNU/Linux



Kali GNU/Linux

Advanced options for Kali GNU/Linux

30. Enter user name and password



LAB NO: 2 **Date:**

WIRESHARK

Objectives:

In this lab, student will be able to:

- Identify the details about data communication, working of the protocols involved in communication using Wireshark.
- Analyze the working of network protocols and identify the vulnerabilities in the communication system related to confidentiality using Wireshark.
- Viewing the input/output traffic graph using Wireshark.
- View and Analyze Packet Contents of real network.

Description:

Wireshark is a network protocol analyser, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

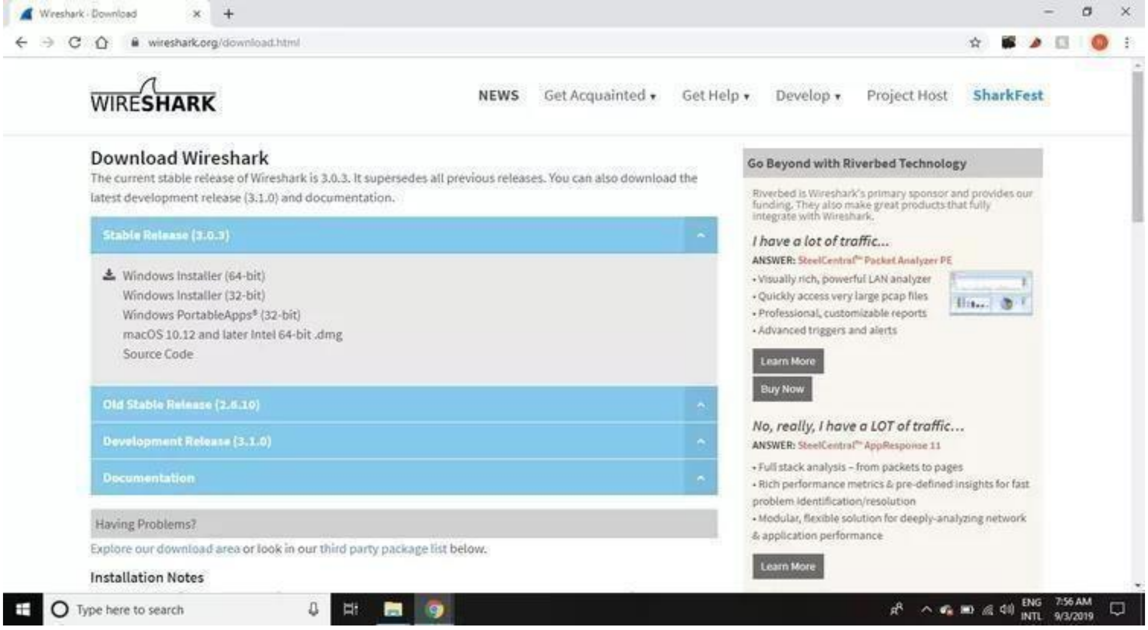
The use of Wireshark:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals.

I. SOLVED EXERCISE:

1) Install, Capture and Analyze Data Packet Contents using Wireshark

Wireshark can be downloaded at from the Wireshark Foundation website for both macOS and Windows.



Download Wireshark

The current stable release of Wireshark is 3.0.3. It supersedes all previous releases. You can also download the latest development release (3.1.0) and documentation.

Stable Release (3.0.3)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.12 and later Intel 64-bit .dmg
- Source Code

Old Stable Release (2.6.10)

Development Release (3.1.0)

Documentation

Having Problems?

Explore our download area or look in our third party package list below.

Installation Notes

Go Beyond with Riverbed Technology

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products that fully integrate with Wireshark.

I have a lot of traffic...

ANSWER: SteelCentral™ Packet Analyzer PE

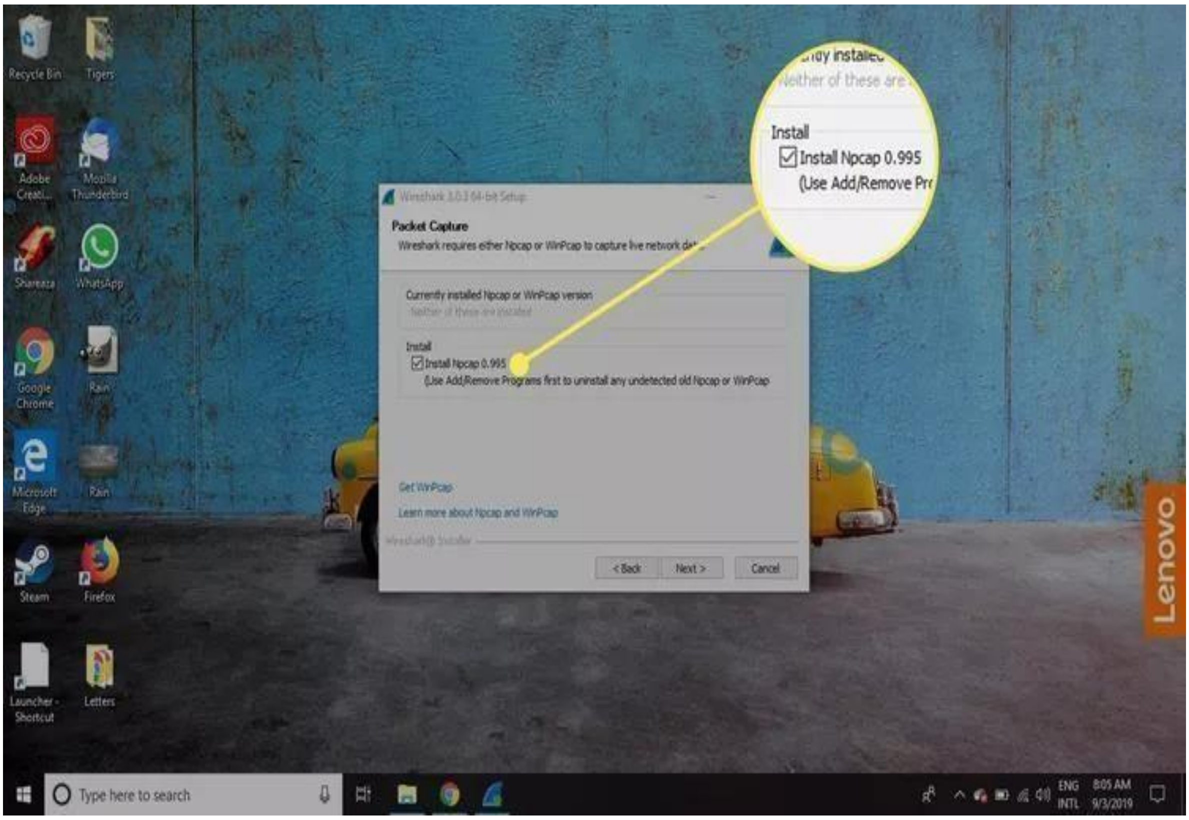
- Visually rich, powerful LAN analyzer
- Quickly access very large pcap files
- Professional, customizable reports
- Advanced triggers and alerts

No, really, I have a LOT of traffic...

ANSWER: SteelCentral™ AppResponse 11

- Full stack analysis – from packets to pages
- Rich performance metrics & pre-defined insights for fast problem identification/resolution
- Modular, flexible solution for deeply-analyzing network & application performance

During the Windows setup process, choose to
install **WinPcap** or **Npcap** if prompted as these include libraries required for live data capture**.**



Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap or WinPcap version

Neither of these are installed

Install

☑ Install Npcap 0.995

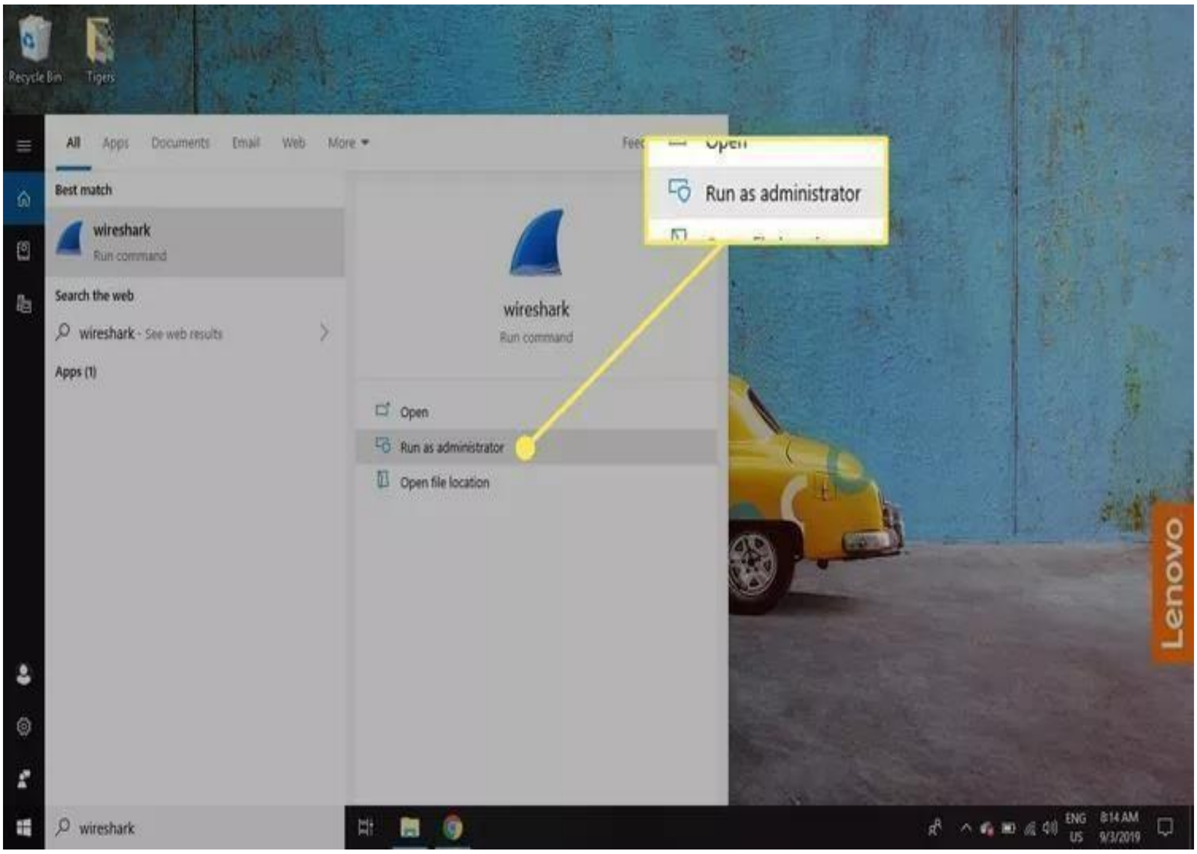
(Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap

Get WinPcap

Learn more about Npcap and WinPcap

Wireshark® Installer

You must be logged in to the device as an administrator to use Wireshark. In Windows 10, search for Wireshark and select **Run as administrator**. In macOS, right-click the app icon and
select **Get Info**. In the **Sharing & Permissions** settings, give the admin **Read & Write** privileges.



The application is also available for Linux and other UNIX-like platforms including Red Hat, Solaris, and FreeBSD. The binaries required for these operating systems can be found toward the bottom of the Wireshark download page under the **Third-Party Packages** section. You can also download Wireshark's source code from this page.

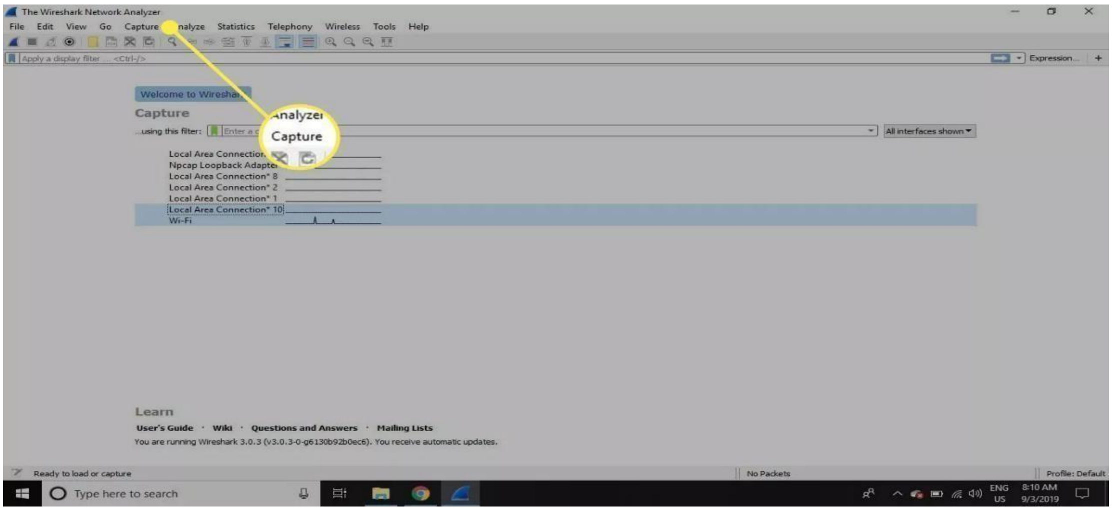
How to Capture Data Packets With Wireshark

When you launch Wireshark, a welcome screen lists the available network connections on your current device. Displayed to the right of each is an EKG-style line graph that represents live traffic on that network.

To begin capturing packets with Wireshark:

1. Select one or more of networks, go to the menu bar, then select **Capture**.

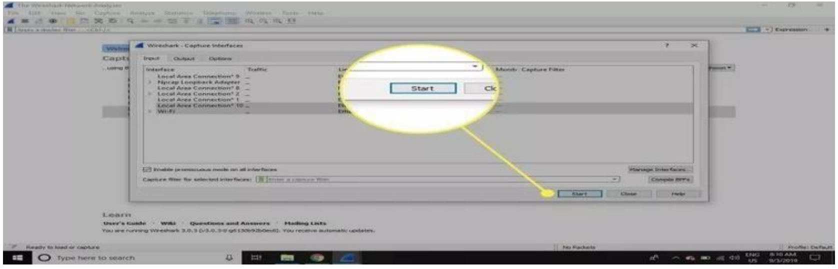
   To select multiple networks, hold the **Shift** key as you make your selection.



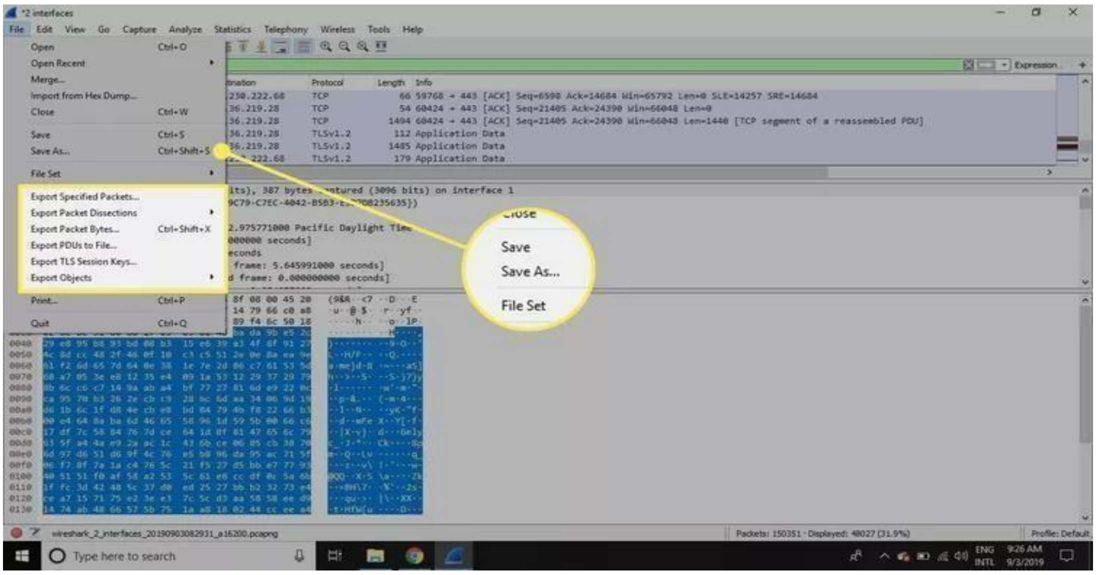
You are running Wireshark 3.0.3 (v3.0.3-0-g6130b92b0ec6). You receive automatic updates.

2. In the **Wireshark Capture Interfaces** window, select **Start**.

   There are other ways to initiate packet capturing. Select the **shark fin** on the left side of the Wireshark toolbar, press **Ctrl+E**, or double-click the network.


Wireshark · Capture Interfaces
Input Output Options
Interface Traffic
Start
Close
Help
Manage Interfaces…
Compile BPFs
Enable promiscuous mode on all interfaces
Capture filter for selected interfaces:

3. Select **File** > **Save As** or choose an **Export** option to record the capture.



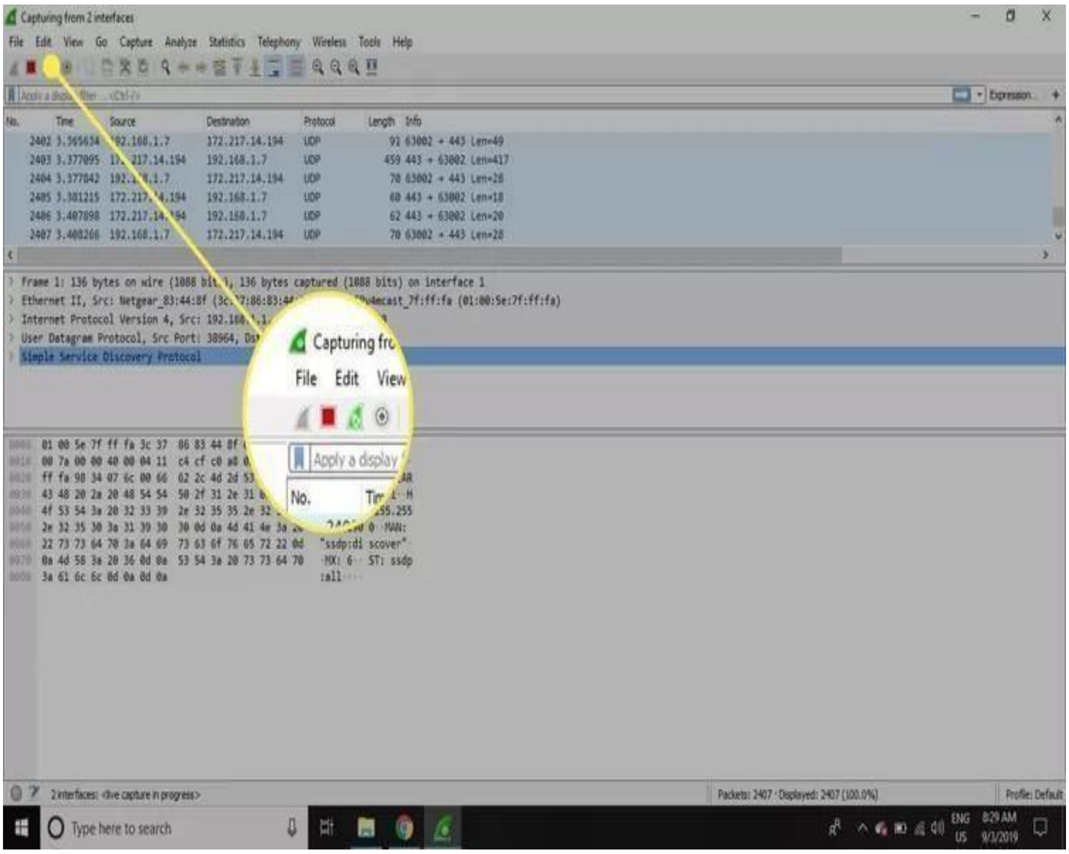
```
tination        Protocol   Length  Info
230.222.68      TCP            66  59768 → 443 [ACK] Seq=6598 Ack=14684 Win=65792 Len=0 SLE=14257 SRE=14684
36.219.28       TCP            54  60424 → 443 [ACK] Seq=21405 Ack=24390 Win=66048 Len=0
36.219.28       TCP          1494  60424 → 443 [ACK] Seq=21405 Ack=24390 Win=66048 Len=1440 [TCP segment of a reassembled PDU]
36.219.28       TLSv1.2       112  Application Data
36.219.28       TLSv1.2      1485  Application Data
  .222.68       TLSv1.2       179  Application Data
```

```
its), 387 bytes captured (3096 bits) on interface 1
9C79-C7EC-4042-B5B3-E  708235635})
2.975771000 Pacific Daylight Time
000000 seconds]
econds
 frame: 5.645991000 seconds]
d frame: 0.000000000 seconds]
```

wireshark_2_interfaces_20190903082931_a16200.pcapng

Packets: 150351 · Displayed: 48027 (31.9%)

4. To stop capturing, press **Ctrl+E**. Or, go to the Wireshark toolbar and select the red **Stop** button that's located next to the shark fin.


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Capturing fro
File Edit View
Apply a display
No.
Tim
2 interfaces: <live capture in progress>
Packets: 2407 · Displayed: 2407 (100.0%)
Profile: Default
Type here to search
ENG US
8:29 AM 9/3/2019

```
No.     Time      Source          Destination     Protocol  Length Info
   2402 3.365634  192.168.1.7     172.217.14.194  UDP           91 63002 → 443 Len=49
   2403 3.377095  172.217.14.194  192.168.1.7     UDP          459 443 → 63002 Len=417
   2404 3.377842  192.168.1.7     172.217.14.194  UDP           70 63002 → 443 Len=28
   2405 3.381215  172.217.14.194  192.168.1.7     UDP           60 443 → 63002 Len=18
   2406 3.407898  172.217.14.194  192.168.1.7     UDP           62 443 → 63002 Len=20
   2407 3.408266  192.168.1.7     172.217.14.194  UDP           70 63002 → 443 Len=28
```

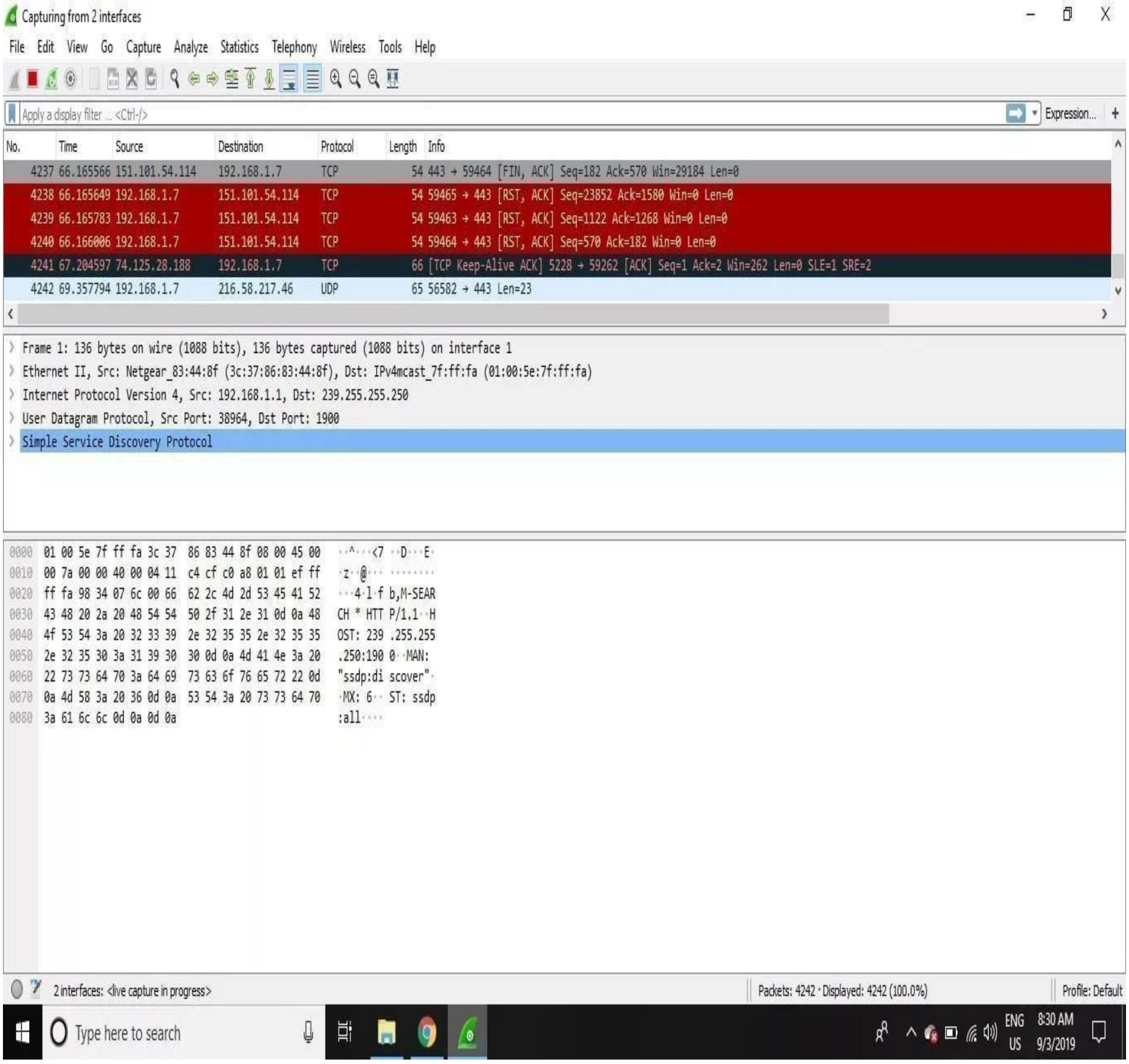
```
> Frame 1: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 1
> Ethernet II, Src: Netgear_83:44:8f (3c:37:86:83:44:    IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1
> User Datagram Protocol, Src Port: 38964, Dst
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 3c 37  86 83 44 8f
0010  00 7a 00 00 40 00 04 11  c4 cf c0 a8 0
0020  ff fa 90 34 07 6c 00 66  02 2c 4d 2d 53              AR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31              1 ·H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32           55.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20     0 ·MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 36 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 6·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 0d 0a                            :all····
```

View and Analyze Packet Contents

The captured data interface contains three main sections:

- The packet list pane (the top section)
- The packet details pane (the middle section)
- The packet bytes pane (the bottom section)


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
2 interfaces: <live capture in progress>
Packets: 4242 · Displayed: 4242 (100.0%)
Profile: Default
Type here to search
ENG US
8:30 AM 9/3/2019

```
No.   Time      Source          Destination     Protocol  Length Info
4237 66.165566 151.101.54.114  192.168.1.7     TCP       54 443 → 59464 [FIN, ACK] Seq=182 Ack=570 Win=29184 Len=0
4238 66.165649 192.168.1.7     151.101.54.114  TCP       54 59465 → 443 [RST, ACK] Seq=23852 Ack=1580 Win=0 Len=0
4239 66.165783 192.168.1.7     151.101.54.114  TCP       54 59463 → 443 [RST, ACK] Seq=1122 Ack=1268 Win=0 Len=0
4240 66.166006 192.168.1.7     151.101.54.114  TCP       54 59464 → 443 [RST, ACK] Seq=570 Ack=182 Win=0 Len=0
4241 67.204597 74.125.28.188   192.168.1.7     TCP       66 [TCP Keep-Alive ACK] 5228 → 59262 [ACK] Seq=1 Ack=2 Win=262 Len=0 SLE=1 SRE=2
4242 69.357794 192.168.1.7     216.58.217.46   UDP       65 56582 → 443 Len=23
```

```
> Frame 1: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 1
> Ethernet II, Src: Netgear_83:44:8f (3c:37:86:83:44:8f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 38964, Dst Port: 1900
> Simple Service Discovery Protocol
```

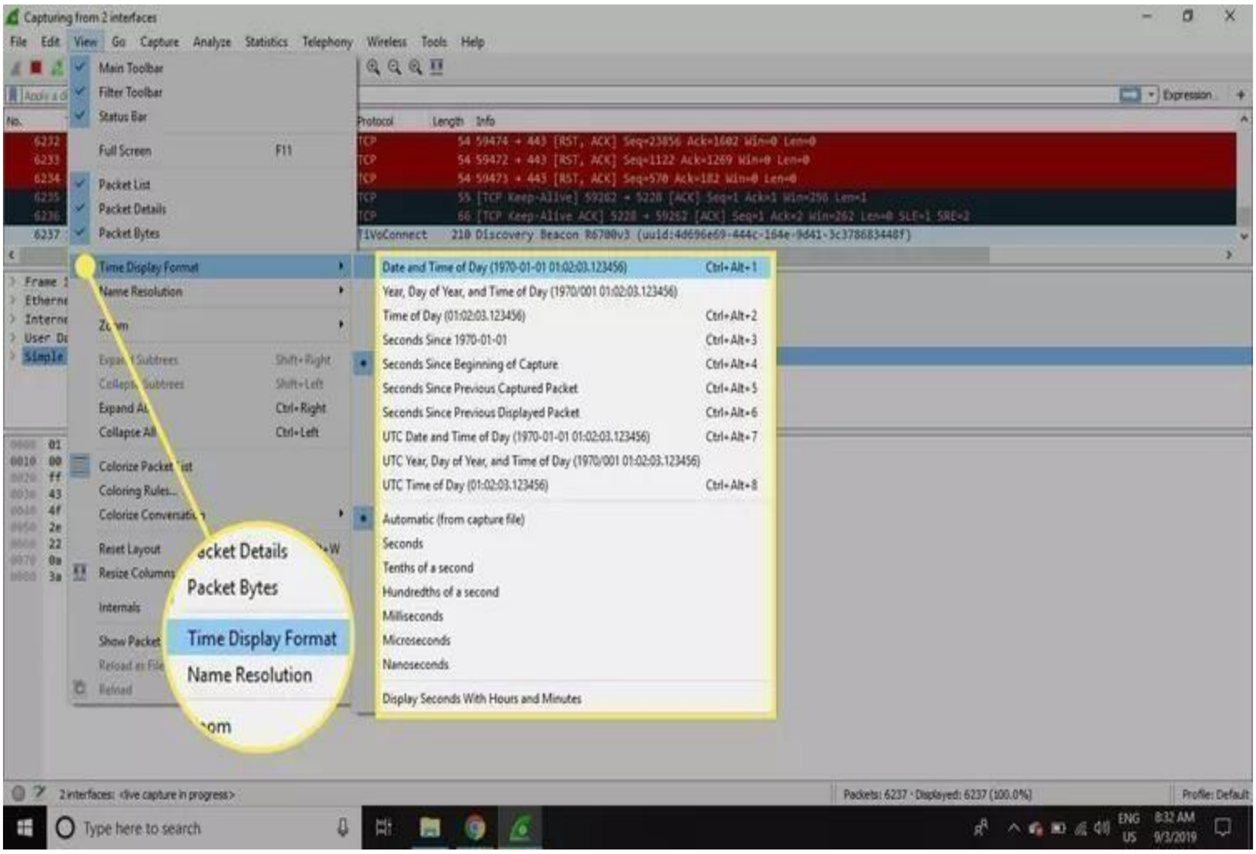
```
0000  01 00 5e 7f ff fa 3c 37  86 83 44 8f 08 00 45 00   ··^···<7 ··D···E·
0010  00 7a 00 00 40 00 04 11  c4 cf c0 a8 01 01 ef ff   ·z··@··· ········
0020  ff fa 98 34 07 6c 00 66  62 2c 4d 2d 53 45 41 52   ···4·l·f b,M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 36 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 6·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 0d 0a                           :all····
```

Packet List

The packet list pane, located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points:

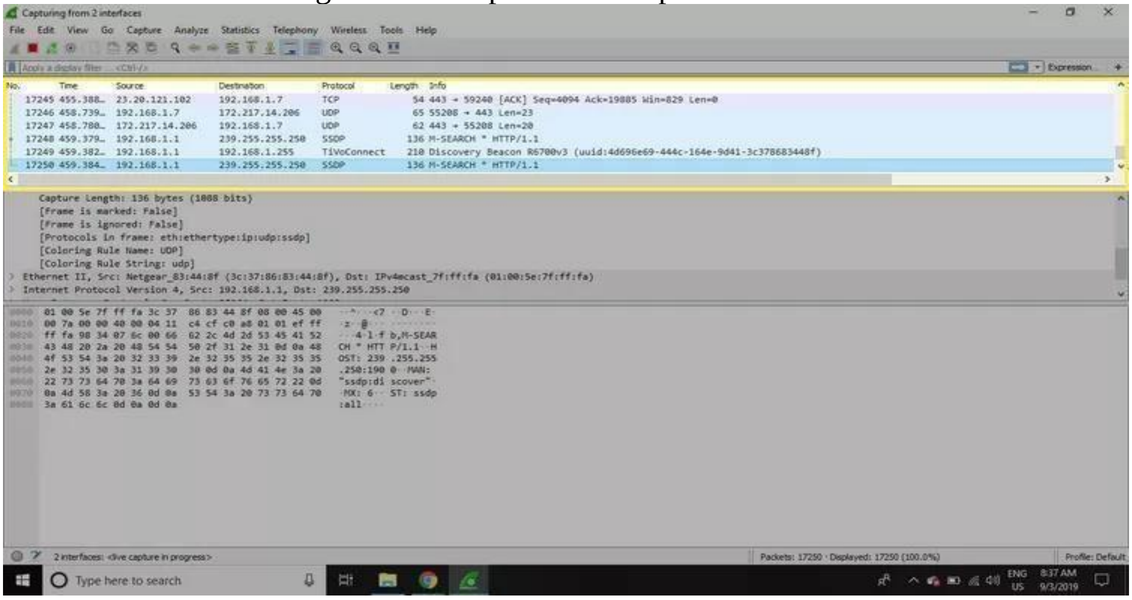
- **No**: This field indicates which packets are part of the same conversation. It remains blank until you select a packet.
- **Time:** The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture file was first created.
- **Source:** This column contains the address (IP or other) where the packet originated.
- **Destination:** This column contains the address that the packet is being sent to.
- **Protocol:** The packet's protocol name, such as TCP, can be found in this column.
- **Length:** The packet length, in bytes, is displayed in this column.
- **Info:** Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.

To change the time format to something more useful (such as the actual time of day), select **View** > **Time Display Format**.


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout
Resize Columns
Internals
Show Packet
Reload as File
Reload
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Expression...
2 interfaces: <live capture in progress>
Packets: 6237 · Displayed: 6237 (100.0%)
Profile: Default
Type here to search
8:32 AM
9/3/2019

```
No.   Protocol     Length  Info
6232  TCP              54 59474 → 443 [RST, ACK] Seq=23856 Ack=1602 Win=0 Len=0
6233  TCP              54 59472 → 443 [RST, ACK] Seq=1122 Ack=1269 Win=0 Len=0
6234  TCP              54 59473 → 443 [RST, ACK] Seq=570 Ack=182 Win=0 Len=0
6235  TCP              55 [TCP Keep-Alive] 59262 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
6236  TCP              66 [TCP Keep-Alive ACK] 5228 → 59262 [ACK] Seq=1 Ack=2 Win=262 Len=0 SLE=1 SRE=2
6237  TiVoConnect     210 Discovery Beacon R6700v3 (uuid:4d696e69-444c-164e-9d41-3c378683448f)
```

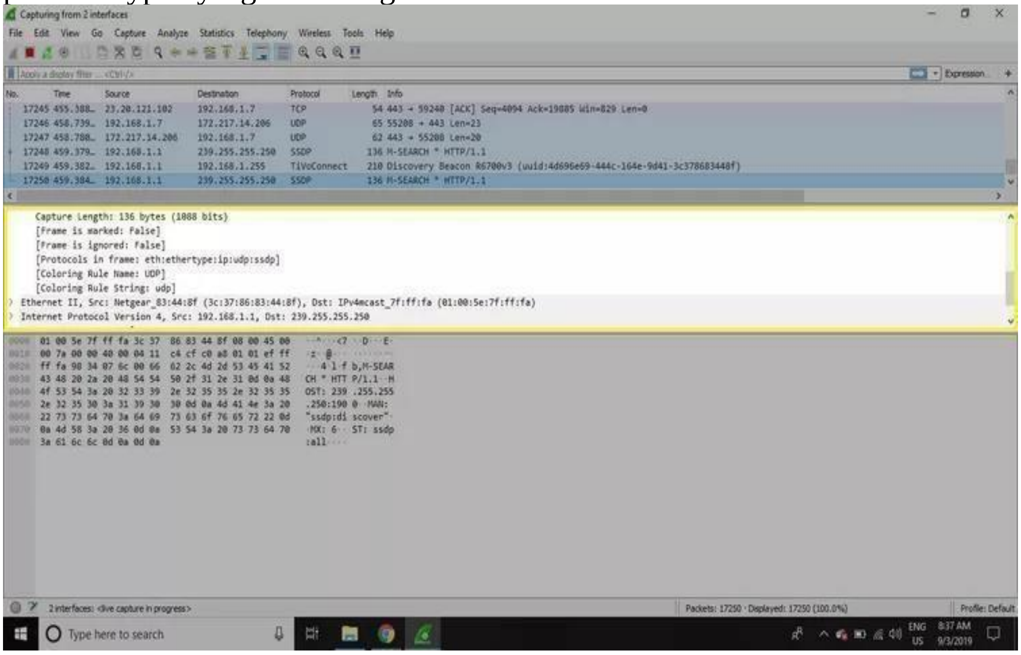
When a packet is selected in the top pane, you may notice one or more symbols appear in the **No.** column. Open or closed brackets and a straight horizontal line indicate whether a packet or group of packets are part of the same back-and-forth conversation on the network. A broken horizontal line signifies that a packet is not part of the conversation.


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
2 interfaces: <live capture in progress>
Packets: 17250 · Displayed: 17250 (100.0%)
Profile: Default
Type here to search
8:37 AM
9/3/2019

```
No.    Time      Source           Destination       Protocol     Length  Info
17245 455.388…  23.20.121.102    192.168.1.7       TCP              54 443 → 59240 [ACK] Seq=4094 Ack=19885 Win=829 Len=0
17246 458.739…  192.168.1.7      172.217.14.206    UDP              65 55208 → 443 Len=23
17247 458.780…  172.217.14.206   192.168.1.7       UDP              62 443 → 55208 Len=20
17248 459.379…  192.168.1.1      239.255.255.250   SSDP            136 M-SEARCH * HTTP/1.1
17249 459.382…  192.168.1.1      192.168.1.255     TiVoConnect     210 Discovery Beacon R6700v3 (uuid:4d696e69-444c-164e-9d41-3c378683448f)
17250 459.384…  192.168.1.1      239.255.255.250   SSDP            136 M-SEARCH * HTTP/1.1

    Capture Length: 136 bytes (1088 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:ssdp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> Ethernet II, Src: Netgear_83:44:8f (3c:37:86:83:44:8f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250

0000  01 00 5e 7f ff fa 3c 37  86 83 44 8f 08 00 45 00   ··^···<7 ··D···E·
0010  00 7a 00 00 40 00 04 11  c4 cf c0 a8 01 01 ef ff   ·z··@··· ········
0020  ff fa 98 34 07 6c 00 66  62 2c 4d 2d 53 45 41 52   ···4·l·f b,M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 36 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 6·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 0d 0a                            :all····
```

Packet Details

The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.

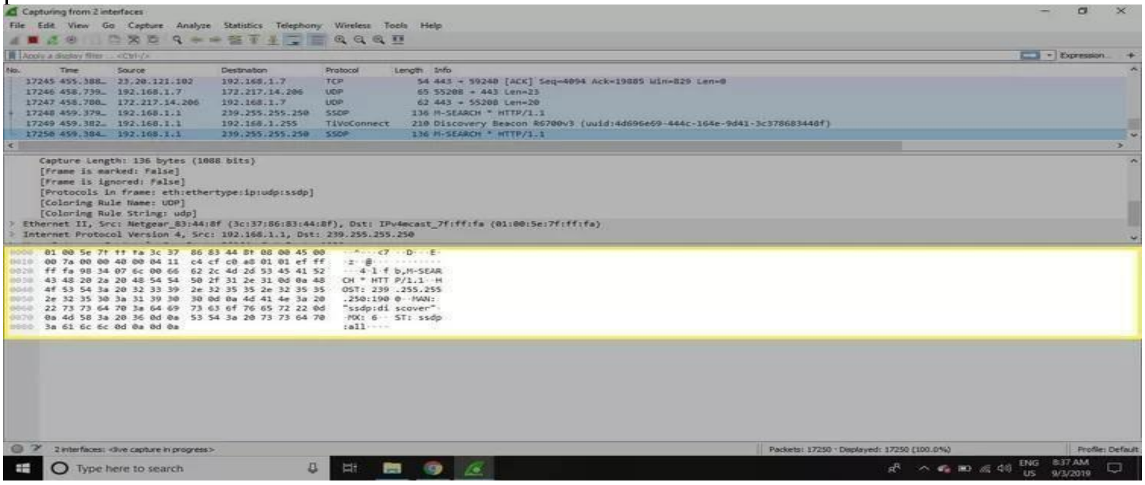

Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
2 interfaces: <live capture in progress>
Packets: 17250 · Displayed: 17250 (100.0%)
Profile: Default
Type here to search
ENG US 8:37 AM 9/3/2019

```
No.    Time      Source          Destination      Protocol     Length Info
 17245 455.388…  23.20.121.102   192.168.1.7      TCP              54 443 → 59240 [ACK] Seq=4094 Ack=19885 Win=829 Len=0
 17246 458.739…  192.168.1.7     172.217.14.206   UDP              65 55208 → 443 Len=23
 17247 458.788…  172.217.14.206  192.168.1.7      UDP              62 443 → 55208 Len=20
 17248 459.379…  192.168.1.1     239.255.255.250  SSDP            136 M-SEARCH * HTTP/1.1
 17249 459.382…  192.168.1.1     192.168.1.255    TiVoConnect     210 Discovery Beacon R6700v3 (uuid:4d696e69-444c-164e-9d41-3c378683448f)
 17250 459.384…  192.168.1.1     239.255.255.250  SSDP            136 M-SEARCH * HTTP/1.1

    Capture Length: 136 bytes (1088 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:ssdp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> Ethernet II, Src: Netgear_83:44:8f (3c:37:86:83:44:8f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250

0000  01 00 5e 7f ff fa 3c 37  86 83 44 8f 08 00 45 00   ··^···<7 ··D···E·
0010  00 7a 00 00 40 00 04 11  c4 cf c0 a8 01 01 ef ff   ·z··@··· ········
0020  ff fa 98 34 07 6c 00 66  62 2c 4d 2d 53 45 41 52   ···4·l·f b,M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 36 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 6·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 0d 0a                            :all····
```

Packet Bytes

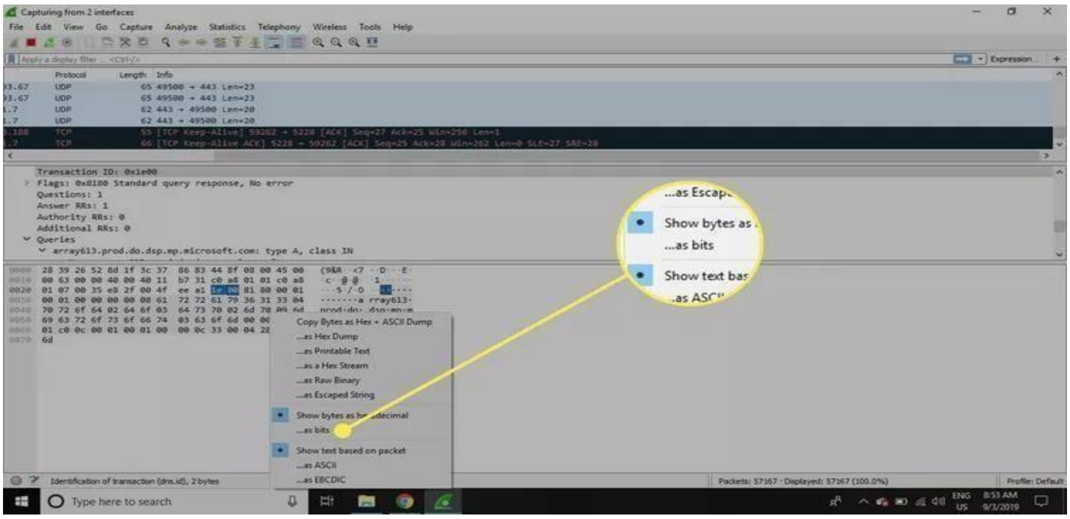
At the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.

Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that cannot be printed are represented by a period.


Capturing from 2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
2 interfaces: <live capture in progress>
Packets: 17250 · Displayed: 17250 (100.0%)
Profile: Default
Type here to search
ENG US 8:37 AM 9/3/2019

```
No.    Time      Source          Destination      Protocol     Length Info
 17245 455.388…  23.20.121.102   192.168.1.7      TCP              54 443 → 59240 [ACK] Seq=4094 Ack=19885 Win=829 Len=0
 17246 458.739…  192.168.1.7     172.217.14.206   UDP              65 55208 → 443 Len=23
 17247 458.788…  172.217.14.206  192.168.1.7      UDP              62 443 → 55208 Len=20
 17248 459.379…  192.168.1.1     239.255.255.250  SSDP            136 M-SEARCH * HTTP/1.1
 17249 459.382…  192.168.1.1     192.168.1.255    TiVoConnect     210 Discovery Beacon R6700v3 (uuid:4d696e69-444c-164e-9d41-3c378683448f)
 17250 459.384…  192.168.1.1     239.255.255.250  SSDP            136 M-SEARCH * HTTP/1.1

    Capture Length: 136 bytes (1088 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:ssdp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> Ethernet II, Src: Netgear_83:44:8f (3c:37:86:83:44:8f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250

0000  01 00 5e 7f ff fa 3c 37  86 83 44 8f 08 00 45 00   ··^···<7 ··D···E·
0010  00 7a 00 00 40 00 04 11  c4 cf c0 a8 01 01 ef ff   ·z··@··· ········
0020  ff fa 98 34 07 6c 00 66  62 2c 4d 2d 53 45 41 52   ···4·l·f b,M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 36 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 6·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 0d 0a                            :all····
```

To display this data in bit format as opposed to hexadecimal, right- click anywhere within the pane and select **as bits**.



```
     Protocol   Length  Info
3.67  UDP         65 49500 → 443 Len=23
3.67  UDP         65 49500 → 443 Len=23
.7    UDP         62 443 → 49500 Len=20
.7    UDP         62 443 → 49500 Len=20
.188  TCP         55 [TCP Keep-Alive] 59262 → 5228 [ACK] Seq=27 Ack=25 Win=256 Len=1
.7    TCP         66 [TCP Keep-Alive ACK] 5228 → 59262 [ACK] Seq=25 Ack=28 Win=262 Len=0 SLE=27 SRE=28
```

```
  Transaction ID: 0x1e00
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
v Queries
  v array613.prod.do.dsp.mp.microsoft.com: type A, class IN
```

```
0000  28 39 26 52 8d 1f 3c 37  86 83 44 8f 08 00 45 00   (9&R··<7 ··D···E·
0010  00 63 00 00 40 00 40 11  b7 31 c0 a8 01 01 c0 a8   ·c··@·@·  ·1······
0020  01 07 00 35 e8 2f 00 4f  ee a1 1e 00 81 80 00 01   ···5·/·O  ········
0030  00 01 00 00 00 00 08 61  72 72 61 79 36 31 33 04   ·······a rray613·
0040  70 72 6f 64 02 64 6f 03  64 73 70 02 6d 70 09 6d   prod·do· dsp·mp·m
0050  69 63 72 6f 73 6f 66 74  03 63 6f 6d 00 00
0060  01 c0 0c 00 01 00 01 00  00 0c 33 00 04 28
0070  6d
```

```
Identification of transaction (dns.id), 2 bytes
Packets: 57167 · Displayed: 57167 (100.0%)
Profile: Default
```

LAB EXERCISES

1. Identify specific type of packets as mentioned by the instructor using the Wireshark Filters further use the options under statistics tab (Use all possible interface with promiscuous mode)

2. Identify and obtain the input/output traffic graph using Wireshark.

3. Identify any website and demonstrate how confidential data is compromised (example: password or any other data).

4. Demonstrate major functionalities of the Wireshark tool.

LAB NO: 3 **Date:**

HPING TOOL

Objectives:

In this lab, student will be able to:

- Identify to analyze the TCP/IPprotocol.
- Generate packets for auditing and testing of firewalls and networks.
- Exploit the Idle Scan scanning techniques.
- Identify the commands to find and fix problems in their networks

Description:
It is a packet generator and analyzer for the TCP/IP protocol. Hping is one of the de-facto tools for security auditing and testing of firewalls and networks, and was used to exploit the Idle Scan scanning technique now implemented in the Nmap port scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in a very short time.

Hping works a bit like a standard ping command. Use that command, and you will:

- Transmit. You will send an Internet Control Message Protocol (ICMP) echo request.
- Wait. The target for your ping should return your message.
- Analyze. You'll get a great deal of data, including information about how many bytes were sent, how many arrived, and how long the trip took.
- Repeat. You'll go through this process a few times, just to ensure the connection remains consistent.

Hping3 becomes even more powerful when you start exploring its advanced options. You can use it for tasks like:

- Firewall Testing: hping3 can be used to test the resilience of your firewall rules by sending packets with various TCP flags and options.
- Tracerouting: You can use hping3 to trace the path taken by packets to reach their destination.
- Traffic Generation: It can generate network traffic patterns to simulate different types of attacks or load on a network.
- Packet Crafting: Craft custom packets to test how your network devices and applications handle them.
- Fingerprinting: Identify the operating system or device type of a remote host by analyzing its response to crafted packets.

I. SOLVED EXERCISE:

1) Install Hping tool

Instructions to download hping.
Version 2: go to http://www.hping.org/download.html and download the tar.gz
Version 3 tar.gz: http://www.hping.org/hping3-20051105.tar.gz
Version 3: is inside the CVS repository. Use the following commands:

```
$ cvs -d :pserver:anonymous@cvs.sourceforge.net:/cvsroot/hping2 login
```

cvs will ask for the password, just press enter, no password is required. Then type this to download the full source code:

```
$ cvs -z8 -d :pserver:anonymous@cvs.sourceforge.net:/cvsroot/hping2 checkout hping3s

$ cvs update
```

2) The identify the IPv4 address using the DNS system using the hostname
hping resolve hostname
The resolve subcommand translate an host name in its IPv4 address using the DNS system. It is basically a gethostname() wrapper, that just returns its input if <hostname> is already an IP address.
Example:

```
hping3.0.0-alpha> hping resolve www.hping.org
192.70.106.166
```

LAB EXERCISES

1. Identify the command to send an ICMP echo request packet to particular IP address.
2. Execute the command to capture packets from the specified interface
3. Do a port scanner: By specifying the TCP flags and port numbers
4. Perform the following attacks using Hping tool
   a. A spoofed scan of the server by the attacker
   b. UDP flood attack
   c. ICMP flood attack
   d. Random Source Attack
   e. SYN flood attack (DDOS attack) on a specified IP address.
5. Identify the command to do the following task
   a. Change TTL of packet
   b. Limit Packet count
   c. Set Packet Flag (SIN,FIN,PUSH,RESET,ACKNOWLEDGE,URG)

LAB NO: 4 **Date:**

CRYPTOGRAPHIC ALGORITHMS

Objectives:

In this lab, student will be able to:

- Identify the working of cryptographic algorithms
- Identify the need for the same.
- Identify the different types of cryptosystem
- Implement the algorithms

Description:

Cryptography is the study of encrypting and decrypting data to prevent unauthorized access. The ciphertext should be known by both the sender and the recipient. With the advancement of modern data security, we can now change our data such that only the intended recipient can understand it. Cryptography allows for the **secure transmission** of digital data between willing parties. It is used to safeguard company secrets, secure classified information, and sensitive information from fraudulent activity, among other things. Crypto means hidden and graph means writing.

Note:

1. **The language of implementation is up to the student (C,Java,Python)**
2. **The students should not use the built in functions or libraries or API for the encryption/decryption steps**

LAB EXERCISES

1. Implement the following algorithms and identify the time taken for encryption and decryption using different size of plain text (plain text should be in a file) and plot a graph for each of the algorithm given (Time Vs File size,Time VS key length)

    a) S-DES Algorithm
    b) DES Algorithm
    c) AES Algorithm
    d) Diffie hellman Algorithm
    e) RSA
    f) ECC

LAB NO: 5 **Date:**

PASSWORD CRACKING TOOLS

HASHCAT/JOHN THE RIPPER /HYDRA

Objectives:

In this lab, student will be able to:

- Use the tool named Hashcat
- Identify the working of the tool
- Perform penetration testing
- Identify the strength of the password

Description:

Hashcat is a popular and effective password cracker widely used by both penetration testers and sysadmins as well as criminals and spies.Cracking passwords is different from guessing a web login password, which typically only allows a small number of guesses before locking your account. Instead, someone who has gained access to a system with encrypted passwords ("hashes") will often try to crack those hashes to recover those passwords.Passwords are no longer stored in plaintext (or shouldn't be, anyway). Instead, passwords are encrypted using a one-way function called a hash. Calculating a password like "Password1" into a hash is lightning quick. What if all you've got is the hash? A brute-force attack to reverse the hash function and recover the password could be computationally infeasible.

Hashcat's help menu using this command:

```
hashcat -h
```

John the Ripper password cracker

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types, including for: user passwords of Unix flavors (Linux, *BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "web apps" (e.g., WordPress), groupware (e.g., Notes/Domino), and database servers (SQL, LDAP, etc.); network traffic captures (Windows network authentication, WiFi WPA-PSK, etc.); encrypted private keys (SSH, GnuPG, cryptocurrency wallets, etc.), filesystems and disks (macOS .dmg files and "sparse bundles", Windows BitLocker, etc.), archives (ZIP, RAR, 7z), and document files (PDF, Microsoft Office's, etc.).

LAB EXERCISES

1. Demonstrate the working of **Hashcat tool.**
2. Demonstrate the following attacks using the Hashcat tool
   Brute-Force attack Combinator attack Dictionary attack Fingerprint attack Hybrid attack Mask attack Permutation attack Rule-based attack Table-Lookup attack Toggle-Case attack PRINCE attack**.**
3. Demonstrate the working of John the ripper tool.
4. Demonstrate the working of Hydra tool.

LAB NO: 6,7,8 **Date:**

PENTRATION TESTING

Objectives:

In this lab, students will be able to:

- Perform Penetration testing
- Identify different stages and perform the different stages of penetration testing
- Attempt to exploit the known or suspected vulnerabilities to prove thier existance.
- Report the results of their testing, including the vulnerabilities,they exploited and the severity of the exploitation.

Tools:OSWAP ZAP ,Web Application Attack and Audit Framework (W3AF),Burp Suite,Metasploit

LAB EXERCISES

1.Install the tool in your system
 a.OSWAP ZAP b.W3AF c.Burp Suite d.metasploit
2.Demonstrate the working of the above-mentioned tools
3.Demonstarte and perform the scanning of different websites using the tools.

LAB NO: 9 **Date:**

NMAP & OPENSSL

Objectives:

In this lab, students will be able to:

- scan networks and discover devices and hosts on a network, allowing network admin to understand the network more efficiently.
- Port Scanning: Determine which ports are open and which services are running on those ports, which is critical for security assessments and vulnerability scanning.
- OS Fingerprinting: Identify the operating system running on a target host by analyzing various characteristics of network packets.
- Vulnerability Assessment: It's a valuable tool for identifying potential vulnerabilities in systems and services, aiding in proactive security measures.
- Network Monitoring: Nmap can be used for continuous monitoring to detect changes in the network environment.

Description:

Nmap is an open-source network scanning and host discovery tool, which was created by Gordon Lyon and has been actively developed and maintained over two decades. Nmap was first released in 1997 by Fyodor Vaskevitch. Since then, it has grown into one of the most widely used network scanning tools in the world. it has a rich history of development and community contributions, which are constantly expanding its capabilities and ensuring to change according to the ever-changing network security. Nmap allows users to do a bunch of things that are related to a wide range of network-related tasks. Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection. A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides.

Features of Nmap

Nmap offers a wide range of features to its users, including:

1. **Comprehensive Scanning:** Nmap can scan a variety of protocols and perform different types of scans.
2. **Scripting Engine:** Nmap Scripting Engine(NSE) allows users to write and run their custom scripts to automate various tasks of Nmap such as Network auditing and vulnerability scanning.
3. **OS Detection:** Nmap can used to identify the operating system of the target hosts based on their responses to the network probes.
4. **Service and Version Detection:** Nmap can accurately identify the services and versions that are running on the open ports of the target hosts.
5. **Output Formats:** Nmap supports multiple output formats for the scan results like plain text, XML, and greppable output.

LAB EXERCISES

1. Write down the command to do Host Discovery using Nmap tool: To discover hosts on the network, use the following command:
   sudo nmap -sn www.manipal.edu
2. Write down the command to do Port Scanning: To perform a port scan on a specific host, use the following command:
   sudo nmap -p 1-65535 192.168.1.100

3. Write down the command to do a Ping Scan using Nmap
4. Write down the command to do A Host Scan
5. Write down the command to do port scanning using Nmap ie
   a.SYN scan b.TCP connect scan c.UDP scans d.TP INIT scan e.TCP NULL
6. Write down the command to do OS Scanning
7. Install Zenmap and perform all the operation as mention for Nmap tool.
8. Generate Self-Signed SSL Certificate with OPENSSL in Kali Linux

LAB NO: 10 &11 **Date:**

CYBER FORENSICS TOOL

(Autopsy/the Sleuth Kit, FTK Imager, Volatility)

Objectives:

In this lab, students will be able to:

- Identify the potential sources of digital evidence
- Preserve the evidence by storing it securely and protecting it from alteration.
- Analyze the collected data to extract relevant information.
- Document the findings of the data.
- Present the findings in a legally acceptable manner.

Description:

Computer forensics deals with the collection of evidence from digital media, such as desktops, mobile devices, cloud computing and IoT devices. This evidence can be used as part of incident remediation activities or to support law enforcement activities.

Autopsy and the Sleuth Kit are likely the most well-known forensics toolkits in existence. The Sleuth Kit is a command-line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI-based system that uses The Sleuth Kit behind the scenes.The tools are designed with a modular and plug-in architecture that makes it possible for users to easily incorporate additional functionality. Both tools are free and open-source

Autopsy/the Sleuth Kit: Used for disk analysis.

FTK Imager: For image creation.

Volatility:Memory forensics

LAB EXERCISES

1.Install the tool in your system

a.Autopsy b.Sleuth Kit c.FTK Imager d.Volatility

2.Demonstrate the working of the tools mentioned above

LAB NO: 12 & 13 **Date:**

IPTABLES & SNORT

Objectives:

In this lab, student will be able to:

- Identify the role & working of iptables.
- install iptables, configure, and use iptables in Linux
- defining a set of rules by which we can monitor, allow or block incoming or outgoing network packets.

Description:

In linux operating system, the firewalling is taken care of using netfilter. Which is a kernel module that decides what packets are allowed to come in or to go outside.iptables are just the interface to netfilter. The two might often be thought of as the same thing. A better perspective would be to think of it as a back end and a front end.The fundamentals, firewalling is the idea of deciding which packets are allowed to go in/out of the system.The packets in the internet (or any other network for that matter) are transferred using ports.We also have ports that are used by the user itself. For example when you have written a web application that runs on port 8000.To decide which port is allowed to communicate to the outside world (or even on the localhost) is the firewall's responsibility. You would command it to either accept, reject or drop a packet. Other things can also happen to a packet but let's keep it simple

LAB EXERCISES

1. Identify the current iptables ruleset Ans: iptables -S and sudo iptables -L.

2. Allowing Loopback Connections
3. (The loopback interface, also referred to as lo, is what a computer uses to forward network
4. connections to itself. For example, if you run ping localhost or ping 127.0.0.1) sudo iptables -A INPUT -i lo -j ACCEPT
5. sudo iptables -A OUTPUT -o lo -j ACCEPT

6. block network connections that originate from a specific IP address, 203.0.113.51 for example, run this command:
7. sudo iptables -A INPUT -s 203.0.113.51 -j DROP

8. To block connections from a specific IP address, e.g. 203.0.113.51, to a specific network interface, e.g. eth0, use this command:
9. iptables -A INPUT -i eth0 -s 203.0.113.51 -j DROP

10. Deleting Rules by Chain and Number
11. The other way to delete iptables rules is by its chain and line number. To determine a rule's line number, list the rules in the table format and add the --line-numbers option:
12. sudo iptables -L --line-numbers

13. delete all of the rules in the INPUT chain, run this command: sudo iptables -F INPUT

14. Flushing All Chains
15. To flush all chains, which will delete all of the firewall rules, you may use the -F, or the equivalent --flush, option by itself:
16. sudo iptables -F

17. Reject all tcp packets with (specific ip,port numbers,mac address,destination port etc)

18. Filtering Packets Based on Source

19. Dropping all Other Traffic

20. Allow Traffic on Specific Ports

21. Dropping Unwanted Traffic

SNORT Tool:

1.Install the snort tool and configure it.
2.Demonstarte the working of the snort tool by showing the setting the rules

References:

1. https://www.kali.org/docs/virtualization/install-vmware-guest-vm/
2. https://www.wireshark.org/download.html
3. https://www.wireshark.org/
4. https://www.kali.org/tools/hping3/
5. https://www.geeksforgeeks.org/java-program-to-implement-the-rsa-algorithm/
6. https://www.baeldung.com/java-aes-encryption-decryption
7. https://dev.java/learn/security/intro/
8. https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/
9. https://www.kali.org/tools/hashcat/
10. https://www.csoonline.com/article/569355/hashcat-explained-why-you-might-need-this-password-cracker.html
11. https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/
12. https://youtu.be/ThpVa7Qsnoo
13. https://youtu.be/rioBjLN4FyY
14. https://youtu.be/MZtPXZihpwc
15. https://youtu.be/kadJLB2rYWo
16. https://www.zaproxy.org/getting-started/
17. https://www.softwaretestinghelp.com/owasp-zap-tutorial/
18. https://docs.w3af.org/en/latest/
19. https://www.youtube.com/watch?v=ouDe5sJ_uC8&list=PLoX0sUafNGbH9bmbIANk3D50FNUmuJIF3
20. https://www.metasploit.com/
21. https://youtu.be/Keld6Wi8aZ4
22. https://youtu.be/8lR27r8Y_ik
23. https://nmap.org/book/intro.html
24. https://linuxconfig.org/how-to-generate-a-self-signed-ssl-certificate-on-linux
25. https://sleuthkit.org/autopsy/docs/user-docs/4.21.0//
26. https://sleuthkit.org/sleuthkit/docs.php
27. https://www.forensicfocus.com/stable/wp-content/uploads/2017/10/ftkimager_ug.pdf
28. https://volatility3.readthedocs.io/en/latest/
29. https://linux.die.net/man/8/iptables
30. https://docs.snort.org/start/help
31. https://youtu.be/8lOTUqfkAhQ