Table of Content

Experiment 1

Cyber Attack Case 1: Ransomware Attack on Colonial Pipeline through exposed password ofVPN Accounts.

Aim: To perform a case study on Ransomware attack that happened on Colonial Pipeline.

Abstract:

The Colonial Pipeline is one of the largest and most vital oil pipelines in the U.S. It began in 1962 to help move oil from the Gulf of Mexico to the EastCoast states. The Colonial Pipeline comprises more than 5,500 miles of pipeline. It starts in Texas and moves all the way up through New Jersey, supplying nearly half of the fuel for the East Coast. The Colonial Pipeline delivers refined oil for gasoline, jet fuel and home heating oil.

The Colonial Pipeline hack is the largest publicly disclosed cyber-attack againstcritical infrastructure in the U.S. The attack involved multiple stages against Colonial Pipeline IT systems. The pipeline's operational technology systems that actually move oil were not directly compromised during the attack.

On May 6th 2021, the attacker group named "DarkSide" got access to the Colonial Pipeline network through exposed passwords of VPN accounts. Theystole around **100 GBs** of data within a **2-hour** window frame. Following the data-theft the attacker also infected the Colonial Pipeline IT network with a **Ransomware** that affected many systems on May 7th. The attacker demanded75 Bitcoins worth $4.4 Million at that time.

Colonial Pipeline took the proactive step of shutting down their pipeline to prevent the ransomware from spreading. They engaged security investigation firm Mandiant to conduct an inquiry into the attack. Additionally, they notifiedthe FBI, Cybersecurity and Infrastructure Security Agency, U.S. Department of Energy, and Department of Homeland Security about the incident.

To regain control of their systems, Colonial Pipeline made a payment to the Dark Side hackers in exchange for the decryption key.
Following this, they successfully restarted pipeline operations on May 12.

Timeline:

May 6, 2021: Initial Intrusion and data theft

May 7, 2021: Ransomware attack begins, Colonial Pipeline pays $4.4 Million as ransom.

May 12, 2021: Pipeline restarted as normal operation resumed.

June 7, 2021: Department of Justice recovered 63.7 Bitcoin worth $2.3 Million.

Who was responsible for this attack?

The group named **"DarkSide"** were identified as the attacker. DarkSide's first publicly reported activity was in August 2020, when it began a malicious campaign of infecting victims with ransomware. DarkSide is thought be operating out of Eastern Europe or Russia though there is no confirmed link with any nation-state sponsored activity. The Russian government has also denied involvement with DarkSide or the pipeline operator attack.

Who was affected?

The Colonial Pipeline hack had significant and immediate effects. Notably, the airline industry experienced a jet fuel shortage affecting carriers like American Airlines. Other airports, including Atlanta and Nashville, also faced limited disruptions.

The fear of a gas shortage prompted panic-buying, resulting in long lines at gas stations across several states, including Florida, Georgia, Alabama, Virginia, and the Carolinas. As a consequence, the average gas price surged, with regular gasoline exceeding $3 per gallon after the Colonial Pipeline shutdown. In some areas, panic-buying led to actual shortages as consumers purchased more fuel than usual.

Need of software bill of materials

In the aftermath of the Colonial Pipeline ransomware attack, industry and government set out to find ways to mitigate or prevent similar incidents fromhappening in the future.

In supply chain attacks such as the one that affected Colonial Pipeline, it is a vulnerable component that is in use somewhere within an organization's infrastructure that is the root attack vector. And it is often a challenge for largeorganizations to know what's inside of all the applications that are in use and ifthere are software dependencies that could include known vulnerabilities.

In May 2021, the Biden Administration issued an executive order directing U.S. government agencies to take a series of proactive steps to bolster cybersecurity. One of the steps that the order advocates is the use of a software bill of materials (SBOMs).

"An SBOM allows the builder to make sure those components are up to dateand to respond quickly to new vulnerabilities".

Conclusion / Result:

The cyber attack on Colonial Pipeline was one of the US's largest public disclosed attacks. The password of the user that got in the hands of the attackerswere also used as the measure in another data theft as the user has used the samepassword for both. Emergency was declared by President Biden. The residents of the US got affected as their was increase in the Fuel and the production got closed to stop the spread of the ransomware. The company manage to regain
$2.4 Million worth of ransom with the help of Dept. of Justice.

Experiment 2

Cyber Attack Case 2: Malware attack on SolarWinds supply Chain

Aim: To perform a case study on the Malware attack that happened onSolarWind's Supply Chain.

Abstract:

SolarWinds Corporation is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure. It is headquartered in Austin, Texas, with sales andproduct development offices in a number of locations in the United States andseveral other countries.

In **December 2020**, a sophisticated cyberattack targeted SolarWinds, a software provider by the group named **"APT29** or **Cozy Bear"** which is thehacking arm of Russia's foreign intelligence service. Hackers exploited a vulnerability in SolarWinds' Orion platform, injecting malicious code into legitimate software updates. This code allowed them access to thousands of organizations worldwide. The attack remained undetected for months, affecting U.S. government agencies including **Pentagon** and the **U.S. Departments of Homeland Security, Justice, State, Commerce and Treasury**, and private companies including **Microsoft, Deloitte, Intel, Cisco**. SolarWinds faced legal costs upto **$90 Million**, the shares of the company fell by almost **40%** by the end of the week, operational disruptions, and reputational damage. Affected organizations incurred financial losses, data exposure, and operational impact.

Timeline:

December 8, 2020: FireEye, a prominent cybersecurity firm, announced they were victims of a nation-stateattack. Their Red Teamtoolkit was stolen.

December 13, 2020:
FireEye discovers thesupply chain attack while investigating their own Red Team toolkit breach. They find evidence thatattackers entered a backdoor in SolarWinds' software, trojanizing SolarWinds Orion business software updates to distribute malware. This malware is dubbed**"SUNBURST"**.

December 13: SolarWinds starts notifying customers to upgrade immediately toaddress the security vulnerability.

December 14: SolarWinds files an SEC Form 8-K report, acknowledging the cyberattack and the vulnerability within its Orion monitoring products.

December 15, 2020: The Wall Street Journal reports that several U.S. government departments (Commerce, Treasury, Homeland Security, NIH, andState Department) were affected. The attack's initial date is attached to sometime in March 2020, indicating it had been ongoing for months before detection

Who was responsible for the attack?
APT29, also known as **Cozy Bear**, is a sophisticated Russian state-sponsored cyber espionage group. They have been active since at least 2008 and are associated with the Russian Foreign Intelligence Service (SVR). Cozy Bear is known for its stealthy and persistent attacks, often targeting government agencies, defense contractors, and critical infrastructure. Their tactics include spear-phishing, zero-day exploits, and supply chain compromises. The group gained notoriety during the SolarWinds supply chain attack in 2020, where theytrojanized software updates to infiltrate organizations worldwide.

Who was affected?

The SolarWind supply chain attack affected a lot of companies, FireEye was theone who discovered the malware in the SolarWinds Orion software. The US government, top companies (SolarWinds customers included 425 of the U.S. Fortune 500, top telecommunications firms, accounting firms, and branches of the U.S. Military). SolarWind suffered also from this as their reputation went down, the stock prices fell by 40%.

Access controls can offer a strong defence

Although it's unknown whether SolarWinds' access control protocols or password blunders contributed to the incident, IT experts attest that bolstering these cybersecurity elements can play a major role in defending against hackersand subsequent attacks. It was soon discovered that a handful of the company's employees possessed weak passwords leading up to the incident (one
employee's password was **"solarwinds123"**).

Conclusion / Result:

SolarWinds supply chain attack exposed the vulnerability of software supply chains. Russian state-sponsored hackers, known as APT29 or Cozy Bear, exploited a SolarWinds software update to infiltrate thousands of organizationsglobally. The attack remained undetected for months, impacting U.S. government agencies, major companies, and critical infrastructure providers.
SolarWinds faced legal costs and reputational damage, while affected organizations incurred financial losses and operational disruptions. This incident underscores the urgent need for robust supply chain security, continuous monitoring, and proactive defence against sophisticated threats.

Experiment 3

Cyber Attack Case 3: Zero Day Exploit on Microsoft Exchange Server

Aim: ***To perform a case study on the Zero Day exploit that happened on Microsoft Exchange Server***

Abstract:

Microsoft Exchange Server is a mail server and calendaring server developedby Microsoft. It runs exclusively on Windows Server operating systems. The first version was called Exchange Server 4.0, to position it as the successor tothe related Microsoft Mail 3.5. Exchange initially used the X.400 directory service but switched to Active Directory later. Until version 5.0, it came bundled with an email client called Microsoft Exchange Client. This was discontinued in favor of Microsoft Outlook.

On **March 2, 2021** Microsoft detected multiple **zero-day exploits** being used toattack on-premises versions of Microsoft Exchange Server. Over the next few days, over **30,000 organizations** in the US were attacked as hackers used several Exchange vulnerabilities to gain access to email accounts and install web shell malware, giving the cybercriminals ongoing administrative access to the victims' servers.

On the same day, Microsoft announced they suspected the attacks were carried out by a previously unidentified Chinese hacking group they dubbed **Hafnium** astate sponsored China operated group.

TimeLine:

January 3, 2021: Cyber espionage operations against Microsoft Exchange Server begin using the Server-Side Request Forgery (SSRF) vulnerability CVE- 2021-26855, according to cybersecurity firm Volexity.

January 5, 2021:

Researcher Cheng-da Tsai ("Orange Tsai") and security firm Devcore disclose related vulnerabilities to Microsoft.The timing results in some speculation about whether the exploit leaked from Devcore or
Microsoft, Bank Info Security later reported.

February 26-27, 2021: Earlier targeted exploits turn global as Hafnium hackers accelerate the back-dooring of vulnerable servers.

March 2, 2021: Microsoft releases an emergency security update to plug thefour flaws in Exchange Server ver. 2013-2019 to counter the Hafnium attack.

March 2, 2021: Microsoft Threat Intelligence Center (MSTIC) announces Chinese Hacker Group Hafnium was responsible for the attack targeting on- premises Exchange Software.

March 3, 2021: The Cybersecurity and Infrastructure Security Agency (CISA)issues Emergency Directive 21-02 for all federal agencies to disconnect from Microsoft Exchange on-premises servers and begin incident response procedures.

March 5, 2021: Microsoft recommends customers investigate Exchange deployments to ensure they are not compromised.

March 6, 2021: The Wall Street Journal Reports the Exchange Serverhack may have infected up to **250,000** organizations.

March 5-8, 2021: Microsoft sees increased attacks by malicious actors beyondHafnium, also targeting the vulnerabilities the Chinese group exploited.

March 8, 2021: The CISA issues an alert recommending five

steps organizations can take to address Exchange vulnerabilities immediately.The process starts with creating a forensic image of the system.

March 10, 2021: ESET Research finds 10 Advanced Persistent Threat (APT) cybercrime groups are exploiting the Exchange flaws for various purposes. Thisincludes groups known as **LuckyMouse**, **Calypso**, **TontoTeam**, and **DLTMiner**.

March 10, 2021: According to Reuters, up to **60,000** Exchange Servers inGermany are exposed to Exchange Server vulnerabilities.

March 13, 2021: CISA adds seven Malware Analyst Reports (MARs) toidentify webshells associated with Exchange vulnerabilities.

March 11-15, 2021: According to Check Point Software's observations, thenumber of attempted Exchange attacks increased **10X**, from **700** to **7,200** in these four days.

March 15, 2021: Microsoft releases a "one-click" On-Premises Mitigation Tool to assist

customers who do not have dedicated IT security to apply updatesto Exchange Server.

March 16, 2021: At least **1,200** Dutch servers reported affected by the Exchange hacks.

March 18, 2021: Microsoft announces their Defender Antivirus and System Center Endpoint Protection now automatically mitigates CVE-2021-26855 onany vulnerable server.

March 22, 2021: Researchers from F-Secure report thousands of cyberattackscontinue daily due to unpatched Exchange vulnerabilities. They state that onlyhalf of Exchange Servers visible on the internet have applied required patches.

March 31, 2021: CISA releases supplemental direction on Emergency Directive for Exchange Server Vulnerabilities.

April 13, 2021: The Department of Justice announced that the FBI was granteda search and seizure warrant by a Texas court that allows the agency to copy and remove web shells from hundreds of on-premises Microsoft Exchange servers owned by private organizations.

Who was responsible for the attack?

Hafnium a Chinese state-controlled group has engaged in a number of attacks using previously unknown exploits targeting on-premises Exchange Server software. To date, Hafnium is the primary actor we've seen use these exploits. The attacks included three steps. First, it would gain access to an Exchange Server either with stolen passwords or by using the previously undiscovered vulnerabilities to disguise itself as someone who should have access. Second, itwould create what's called a web shell to control the compromised server remotely. Third, it would use that remote access run from the US based privateservers to steal data from an organization's network.

Who was affected?

Up to 250k organization were affected by the Microsoft Exchange server exploit. Almost 60k exchange servers in Germany and 1200 Dutch Servers wereaffected as per the given reports by various reports. Microsoft also suffered financial losses as to fix the issue and release the patches and all.

The Case for Auto Update, API Security

According to Mr. Firstbook(Gartner's Distinguished VP Analyst) organizationsusing on-premises servers often neglect managing updates, even though these updates are crucial. He emphasizes that those who can't effectively patch on- premises servers should consider moving to the cloud. However, for small businesses, this transition may be costly and impractical.

Firstbrook also highlights the growing risk associated with Application Programming Interfaces (APIs). The **Exchange** and **SolarWinds** attacks both exploited API vulnerabilities. Despite this, many organizations overlook API security. As APIs become more prevalent, investing in understanding and protecting them will be essential to prevent future attacks.

Conclusion / Result:

The Microsoft Exchange Server attack exposed critical vulnerabilities in on- premises servers. While patching remains essential, some organizations strugglewith effective updates. For those unable to secure on-premises servers, transitioning to the cloud is advisable, though it may be costly for smaller businesses. Additionally, the attack highlighted the growing risk associated withAPIs. As APIs become more prevalent, investing in API security becomes crucial. Organizations must recognize APIs as a rich attack vector and allocate resources to better understand and protect these critical components of their infrastructure.

Experiment 4

Cyber Attack Case 4: SQL injection attack on Guntrader UK's website

Aim: To perform a case study on the SQL injection attack that happened on theGuntrader UK's website.

Abstract:
GunTrader is the UK's leading marketplace for guns for sale, with thousands oflisting of rifles, shotguns, pistols and air-rifles. They are the UK number 1 gun marketplace, connecting more than 2.6million people with more than 310,000 guns every year.

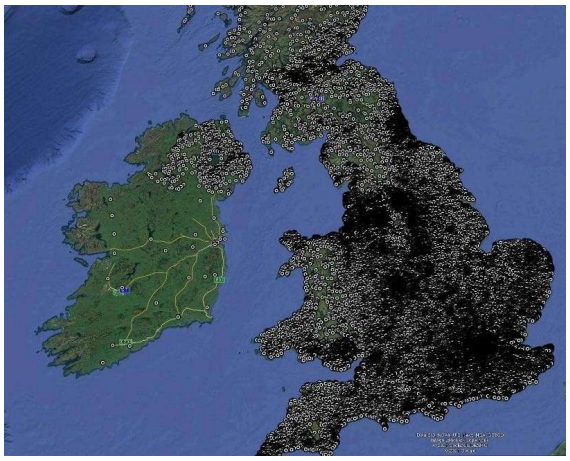
In July 2021, the UK-based firearms sales website **Guntrader** suffered a **data breach**. Approximately **100,000 customer records** were exposed due to a **SQLinjection attack**.

The names and home addresses of **111,000** British firearm owners have been dumped online as a Google Earth-compatible CSV file that pinpoints domestichomes as likely firearm storage locations – a worst-case scenario for victims ofthe breach.

Firearms are attractive to criminals. Targeted robberies and burglaries to steal them, while unusual, are certainly notunknown. Police have previously issued warnings to the licensed firearms community emphasising personal safety after a spate of robberies targeting licensed firearms owners outside their homes and at rifle ranges; the Guntrader breach could lead to a spate of such crimes.

One worried shooter who spoke to The Register said that while his details werein the stolen data, the geolocation information pointed to his parents' home and

ot his own. A registered firearms dealer who initially scoffed at being included"because I don't have signs outside" could be traced down to his warehouse's industrial estate; Googling his name revealed the precise unit number.



Timeline:

July 2021: Guntrader UK found that their database has been breached by anunknown attacker that used SQL injection on their website.

Who was responsible orthe attack?

Unknown
hacker or a group pulled this off. Andrew Barratt, UK MD of infosec biz Coalfire, analysed the database after it was dumped on the RaidForums website.He told The Register: "I suspect it was probably a drive-by style attack. So gut feeling looking at the response from the attackers that they posted on forums, it was completely un-targeted, it was kind of very much like **'lol we pulled another site'** and then it's like, **oh, wow**."

Who was affected?

More than 100k customers of Guntrader got affected due this, their names,precise co-ordinates, mobile phone numbers, email addresses, and more including bcrypt-hashed passwords.

Conclusion / Result:

The leaked data caused a panic among the hundreds of thousands of customers.The breach was done with the help of SQL injection attack. If your data has been compromised, please **DO NOT use same password** in any other website especially e-mail service, e-banking, as the attackers are testing the gained account info.

Experiment 5

Cyber Attack Case 5: Ransomware attack on Royal Mail

Aim: To perform a case study on the Ransomware Attack that happened onRoyal Mail.

Abstract:

The Royal Mail Group Limited is a British postal service and courier company.It is owned by International Distribution Services. It operates the brands Royal Mail (letters and parcels) and Parcelforce Worldwide (parcels).

In January 2023, the **Royal Mail** fell victim to a **cyber incident** composed bythe Russian ransomware gang **LockBit**. The attack forced the company to suspend international export services and caused delays in national postage services.

Although services resumed two months later, LockBit escalated the situation byreleasing data belonging to Royal Mail's staff. The gang demanded a hefty ransom, threatening to leak sensitive information if payment wasn't made. Theirultimatum was clear: "**Pay $40 million, or we release everything**".

Royal Mail chose not to pay the ransom. Instead, they invested **£10 million** in enhancing their cyber defences. Unfortunately, this breach compounded the company's woes, contributing to a half-year loss of **£319 million**.

Timeline:

November 2022: Initialprobing by threat actors.

January 2023: LockBitransomware attack paralyzes overseas mailcapacity.

Remediation: The RoyalMail spends £10 million on recovery efforts .

Who was responsible for the attack?

LockBit a Russian based group that operates a **ransomware-as-a-service (RaaS)** model targeted Royal Mail's **international shipping devices** used for parcels and letters. They encrypted these devices, disrupting overseas deliveries.

Who was affected?

Royal Mail's recovery efforts cost approximately **£10 million**. This amount

primarily went toward improving their Heathrow Worldwide Distribution Centre, the target of the attack.

The cyberattack led to a **6.5%** decline in international revenue (approximately **£22 million** or **$27 million**) due to disruptions in parcel volume.

Royal Mail's total half-year losses stood at **£319 Million**, partly attributed to the ransomware attack and other factors.

Conclusion / Result:

Critical Infrastructure Vulnerabilities, although not fully public sector, the Royal Mail is considered critical infrastructure. Unfortunately, it lacked digital maturity and robust controls, leaving it vulnerable to attacks. The November incident appeared to be an initial probing by threat actors. Subsequently, the attack disrupted overseas mail capacity. Threat actors often test boundaries gradually to assess their reach. Timely communication about incidents is crucial. Citizens and impacted parties prefer prompt information over delayed apologies. Transparency helps others learn and prepares them for similar threats. Cybercriminals conduct reconnaissance months before launching attacks. Identifying weaknesses allows them to explore deeper and compromise the organization.

Experiment 6

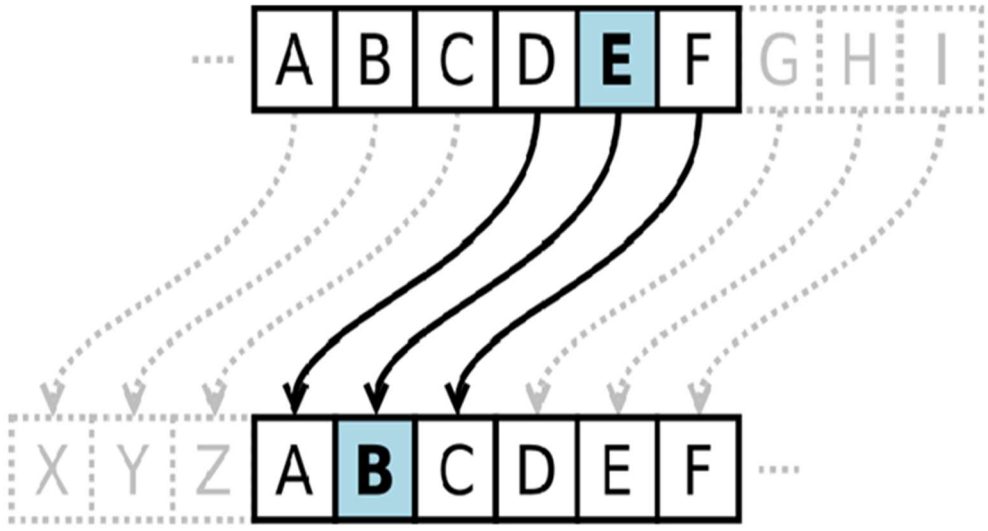
Experiment: ***Write a Program in C for simple substitution technique named Caesar cipher using C language.***

AIM: ***To implement the simple substitution technique named Caesar cipher using C language.***

DESCRIPTION:

To encrypt a message with a Caesar cipher, each letter in the message is changed using a simple rule: shift by three. Each letter is replaced by the letter three letters ahead in the alphabet. A becomes D, B becomes E, and so on. For the last letters, we can think of the alphabet as a circle and "wrap around". W becomes Z, X becomes A, Y becomes B, and Z becomes C. To change a message back, each letter is replaced by the one three before it.

EXAMPLE:



ALGORITHM:

STEP-1: Read the plain text from the user.

STEP-2: Read the key value from the user.

STEP-3: If the key is positive then encrypt the text by adding the key with eachcharacter in the plain text.

STEP-4: Else subtract the key from the plain text.

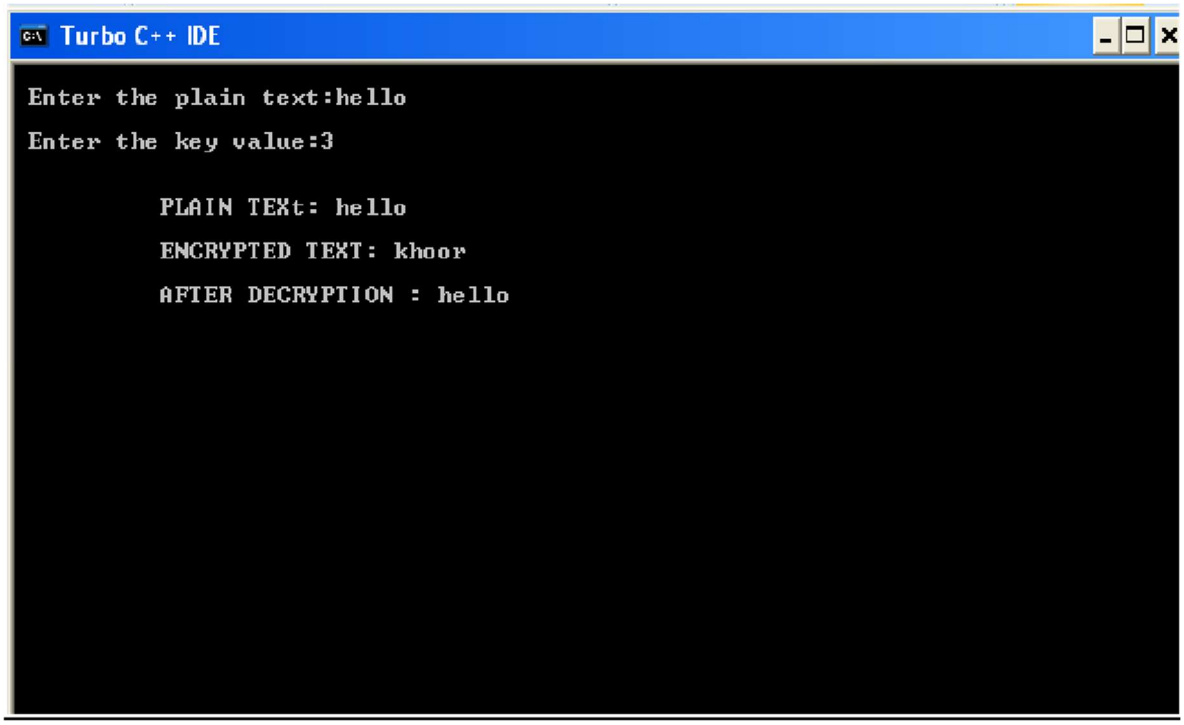
STEP-5: Display the cipher text obtained above.

PROGRAM: (Caesar Cipher)

```
#include <stdio.h>
#include <string.h>
#include<conio.h>
#include <ctype.h>
void main()
{
 char plain[10], cipher[10];
 int key,i,length;
 int result;clrscr();
 printf("\n Enter the plain text:");
 scanf("%s", plain);
 printf("\n Enter the key value:");
 scanf("%d", &key);
 printf("\n \n \t PLAIN TEXt: %s",plain);
 printf("\n \n \t ENCRYPTED TEXT: ");
 for(i = 0, length = strlen(plain); i < length; i++)
       {
       cipher[i]=plain[i] + key;
```

```
        if (isupper(plain[i]) && (cipher[i] > 'Z'))
        cipher[i] = cipher[i] - 26;
        if (islower(plain[i]) && (cipher[i] > 'z'))
        cipher[i] = cipher[i] - 26;
        printf("%c", cipher[i]);
        }
        printf("\n \n \t AFTER DECRYPTION : ");
 for(i=0;i<length;i++)
        {
                plain[i]=cipher[i]-key;
                if(isupper(cipher[i])&&(plain[i]<'A'))
                plain[i]=plain[i]+26;
                if(islower(cipher[i])&&(plain[i]<'a'))
                plain[i]=plain[i]+26;
                 printf("%c",plain[i]);
 }
getch();
}
```

OUTPUT:



Result : Text Converted Successfully

Code in Python:

```
def encrypt(text,s):
result = ""
  # transverse the plain text
  for i in range(len(text)):
    char = text[i]
    # Encrypt uppercase characters in plain text

    if (char.isupper()):
      result += chr((ord(char) + s-65) % 26 + 65)
    # Encrypt lowercase characters in plain text
    else:
```

```
    result += chr((ord(char) + s - 97) % 26 + 97)
    return result
#check the above function
text = "CEASER CIPHER DEMO"
s = 4

print "Plain Text : " + text
print "Shift pattern : " + str(s)
print "Cipher: " + encrypt(text,s)
```

Output:

```
E:\Cryptography- Python>python caeserCipher.py
Plain Text  : CEASER CIPHER DEMO
Shift pattern : 4
Cipher: GIEWIVrGMTLIVrHIQS

E:\Cryptography- Python>
```

Experiment 7

Experiment: Write the steps for TCP / UDP connectivity using Netcat

Aim:- To demomstrate TCP / UDP connectivity using Netcat.

Hardware / Software Required: NMAP Tool.

What is Netcat?

Netcat (nc) is a computer networking service for reading from and writing to network connections using TCP or UDP.
it is a feature-rich network debugging and investigation tool

- Its list of features includes
- port scanning
- port binding
- transferring files
- port listening
- it can be used as a backdoor
- Ability to use any local source port

Netcat Command Flags:-

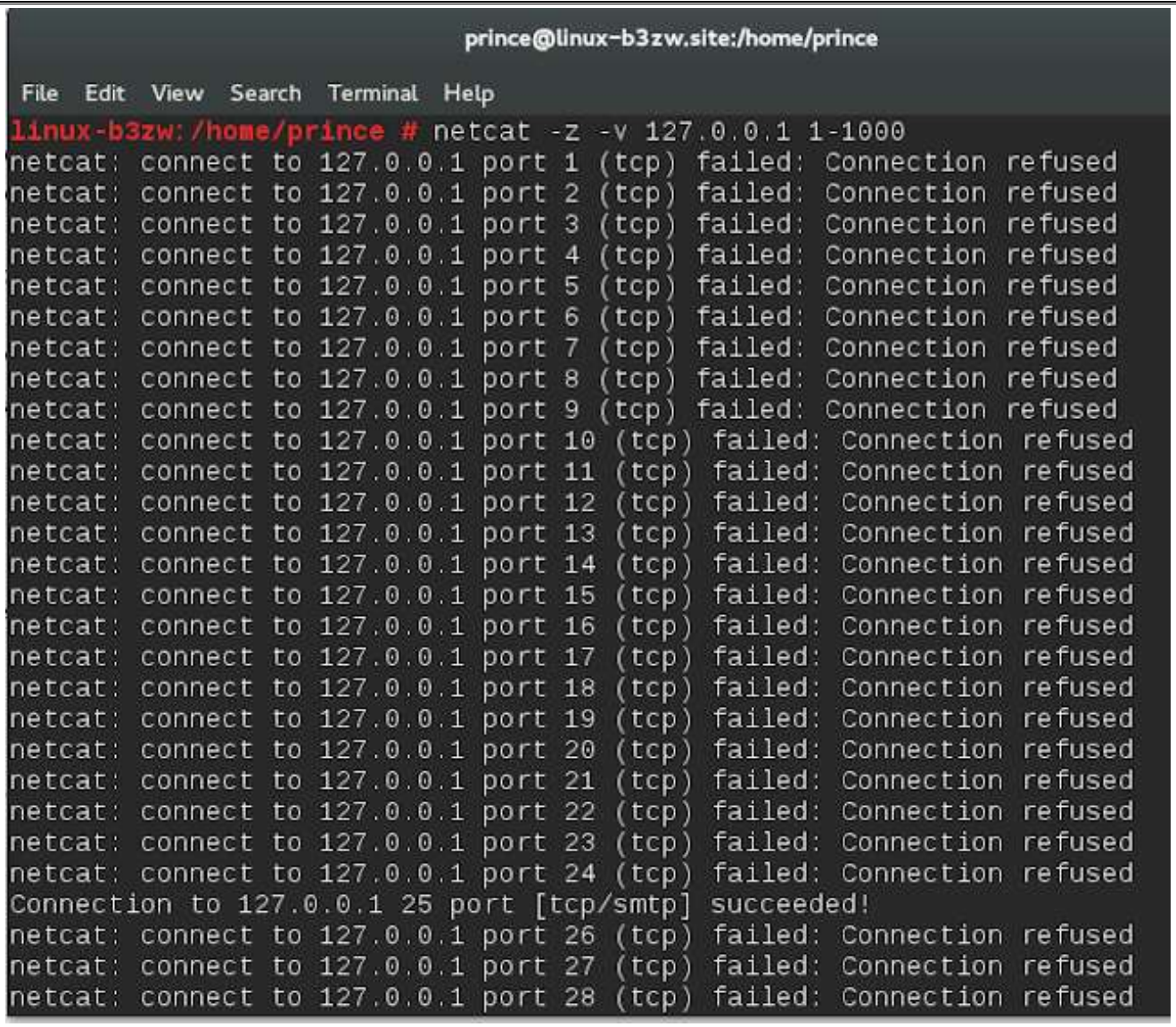
Command Flags	Description
-u	UDP (User Datagram Protocol)
-z	Don't send any Data, just emit a packet without payload(scanning)
-v	be verbose : print out messages on standard information
-n	do not perform DNS lookup on name of system on the other side
-l	Listen mode
-L	Listen harder

How to use Netcat for Port Scanning?

Here, we can scan all ports up to 1000 by issuing this command:

- Netcat -z -v targetdomain.com 1-1000

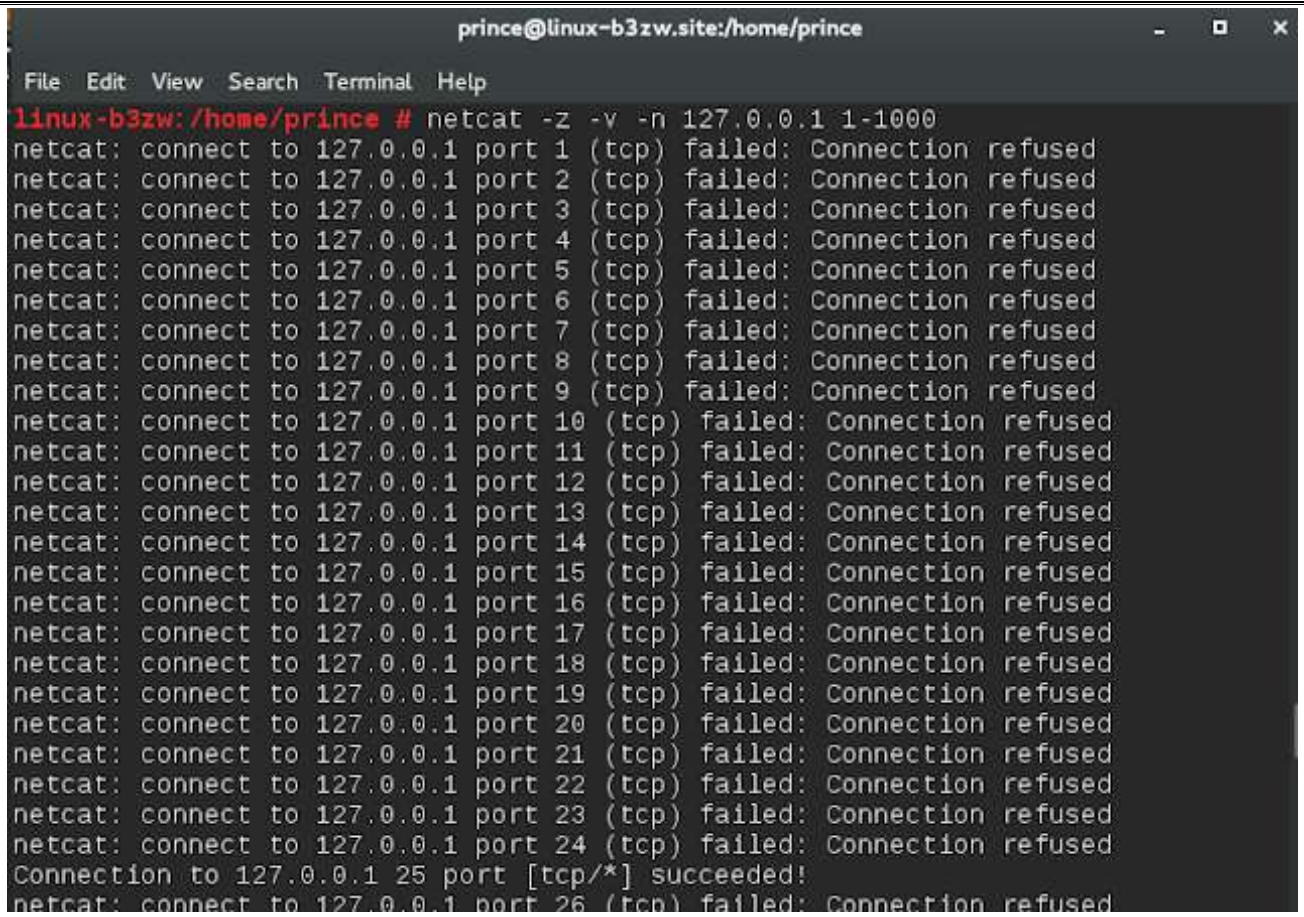
Output:-



Scan will go much faster if you know the IP address that you need.

netcat –z -n -v 127.0.0.1 1-1000

Output



How to communicate through Netcat?

Netcat is not restricted to sending TCP and UDP packets. It also can listen on a port for connections and packets. This gives us the opportunity to connect two instances of netcat in a client-server relationship.
one system, you can tell netcat to listen to a specific port for connections.

Netcat -I 1234

This will tell netcat to listen for TCP connections on port 1234 second server, we can connect to the first machine on the port number we choose

Netcat targetdomain.com 1234

Type a message and press ENTER. It will appear on both the local and remote screen. This works in the opposite direction as well. When you are finished passing messages, you can press CTRL-D to close the TCP connection

Result/ Conclusion:- TCP / UDP connectivity using Netcat is successfully demonstrated.

Experiment-8

Experiment: Perform an experiment to demonstrate sniffing of router traffic by using the tool Wireshark.

Aim:- Study of packet sniffer tools like wireshark.

Objectives:- To observe the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters.

Outcomes:- The learner will be able to:-

- Identify different packets moving in/out of network using packet sniffer for network analysis.
- Understand professional, ethical, legal, security and social issues and responsibilities. Also will be able to analyze the local and global impact of computing on individuals, organizations, and society.
- Match the industry requirements in the domains of Database management, Programming and Networking with the required management skills.

Hard ware / Software Required: Wireshark, Ethereal and tcpdump.

Theory:- Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Applications: Network administrators use it to troubleshoot network problems Network security engineers use it to examine security problems Developers use it to debug protocol implementations People use it to learn network protocol internals beside these examples can be helpful in many other situations too.

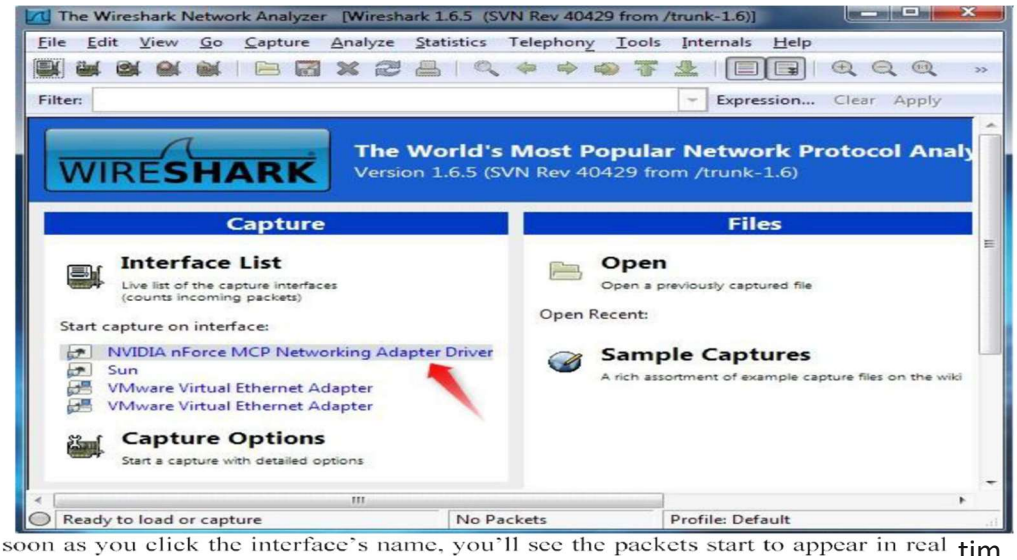
Features: The following are some of the many features wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data. Display packets with very detailed protocol information.
- Export some or all packets in a number of capture file formats. Filter packets on many criteria.
- Search for packets on many criteria. Colorize packet display based on filters. Create various statistics.

Capturing Packets

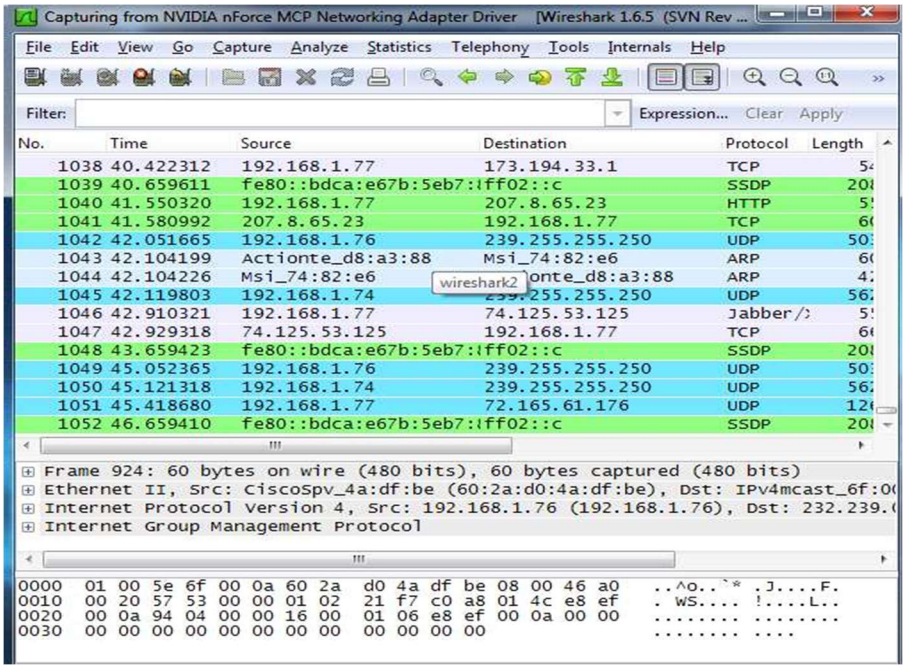
After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic

on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

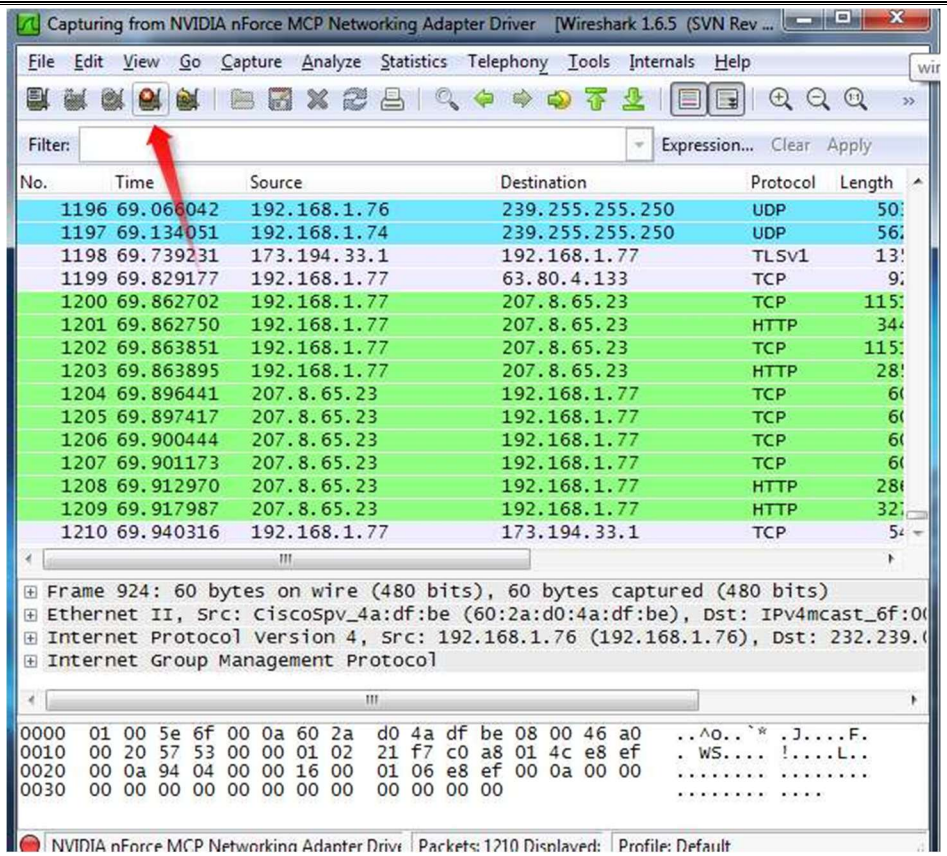


As soon as you click the interface's name, you'll see the packets start to appear in real tim

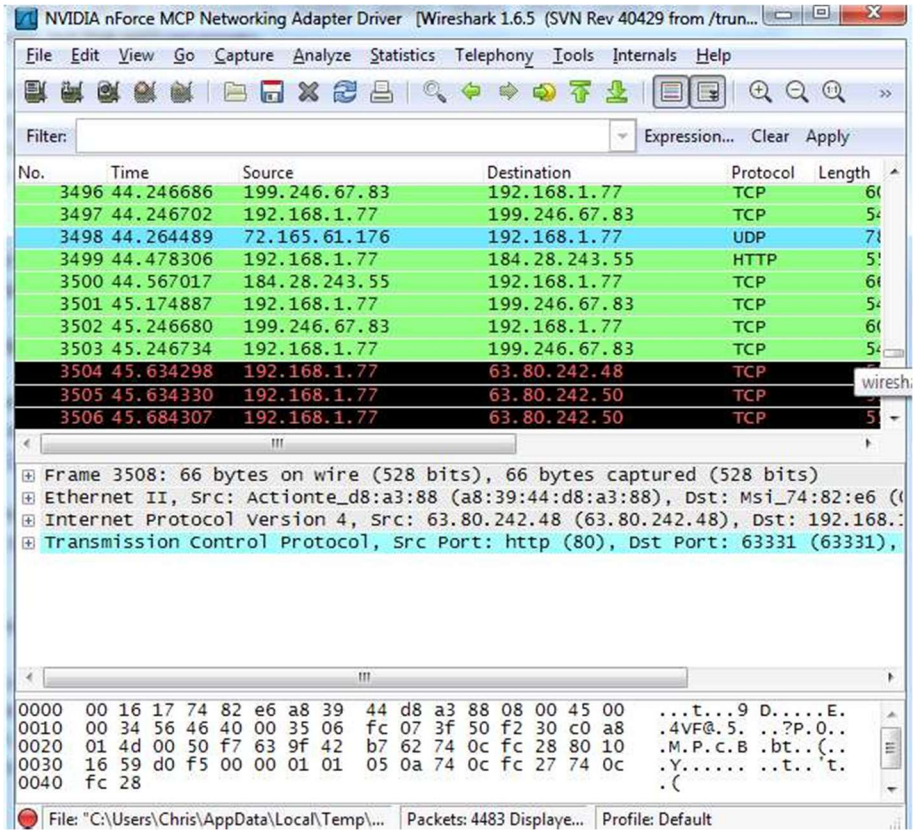
Wireshark captures each packet sent to or from your system. If capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network.



Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.



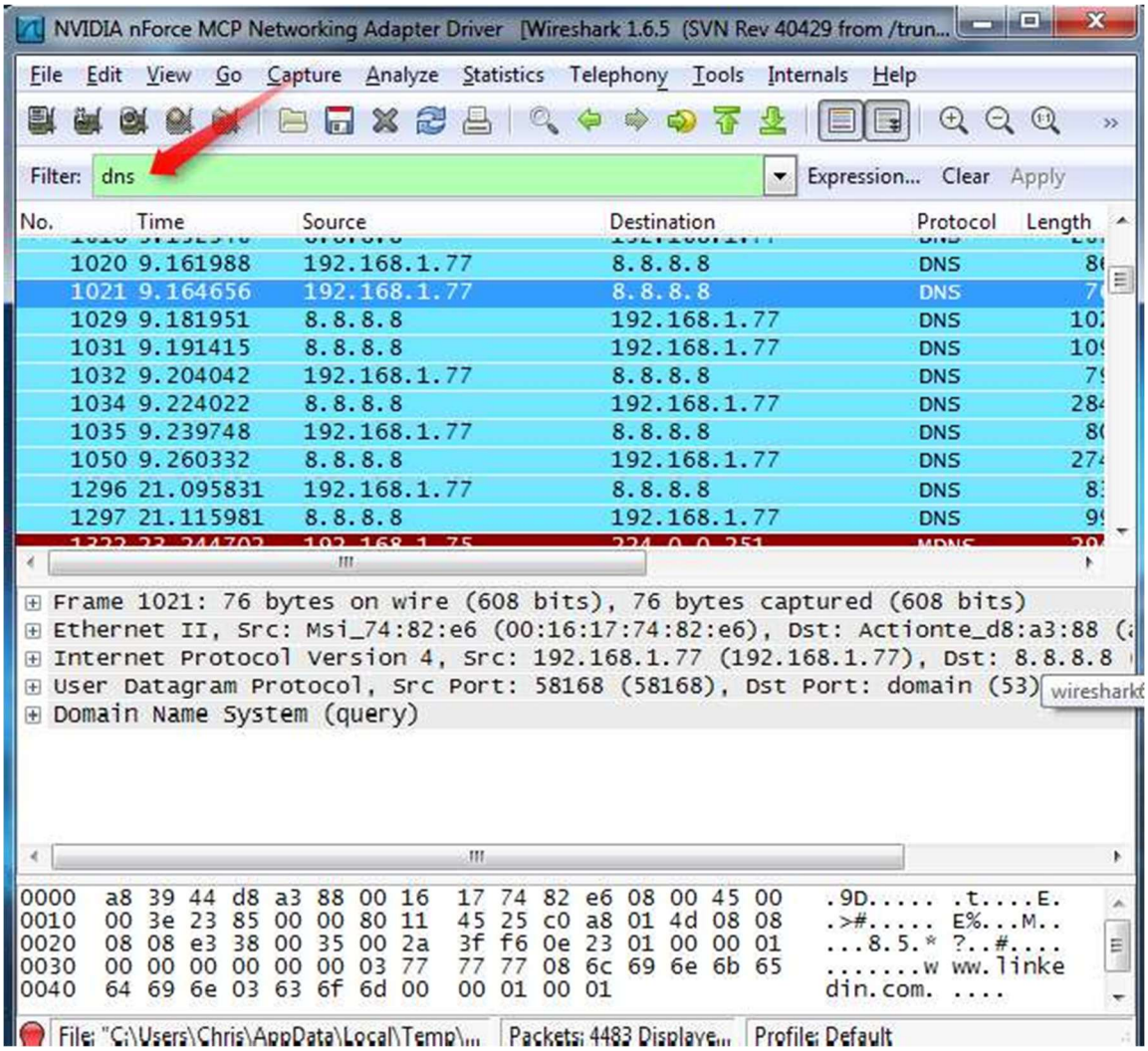
Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems for example, they could have been delivered out-of-order.



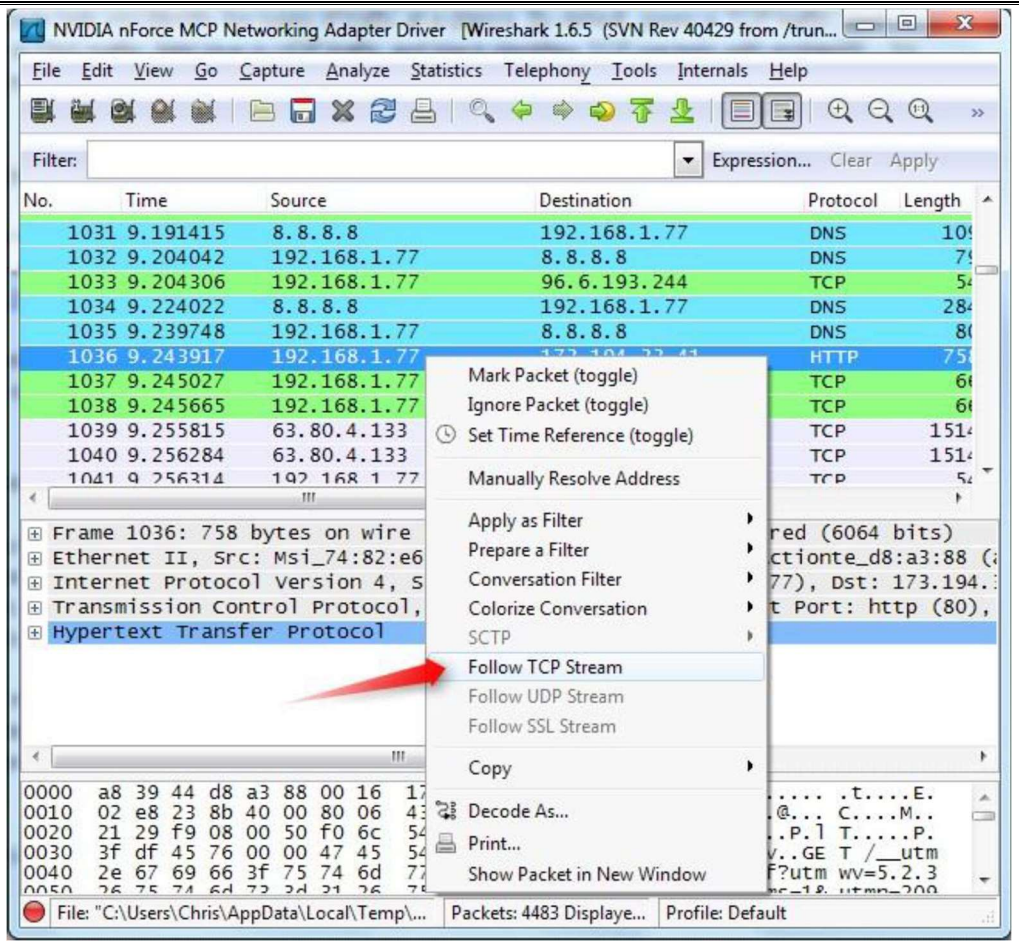
Filtering Packets

If you're trying to inspect something specific, such as traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

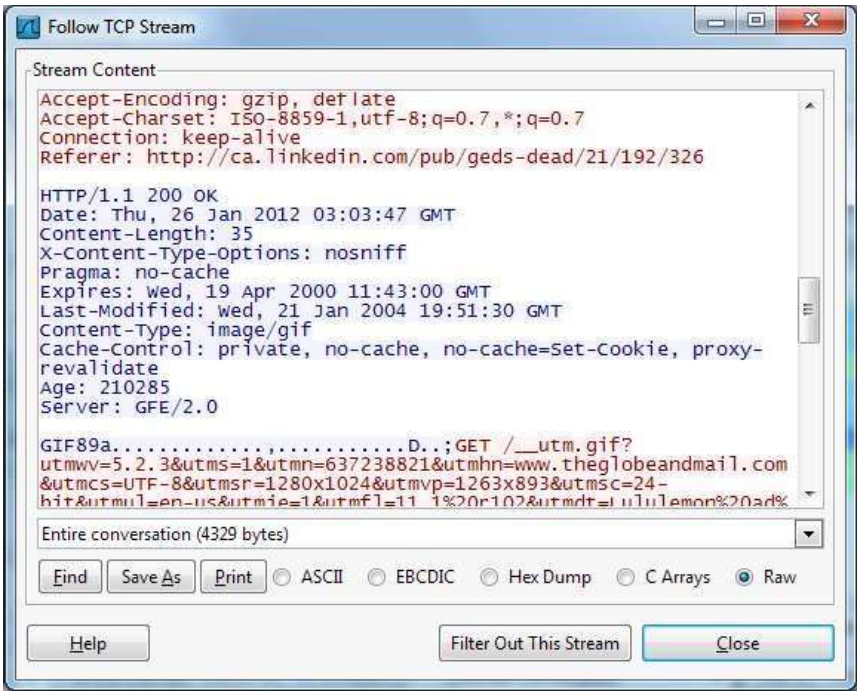
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



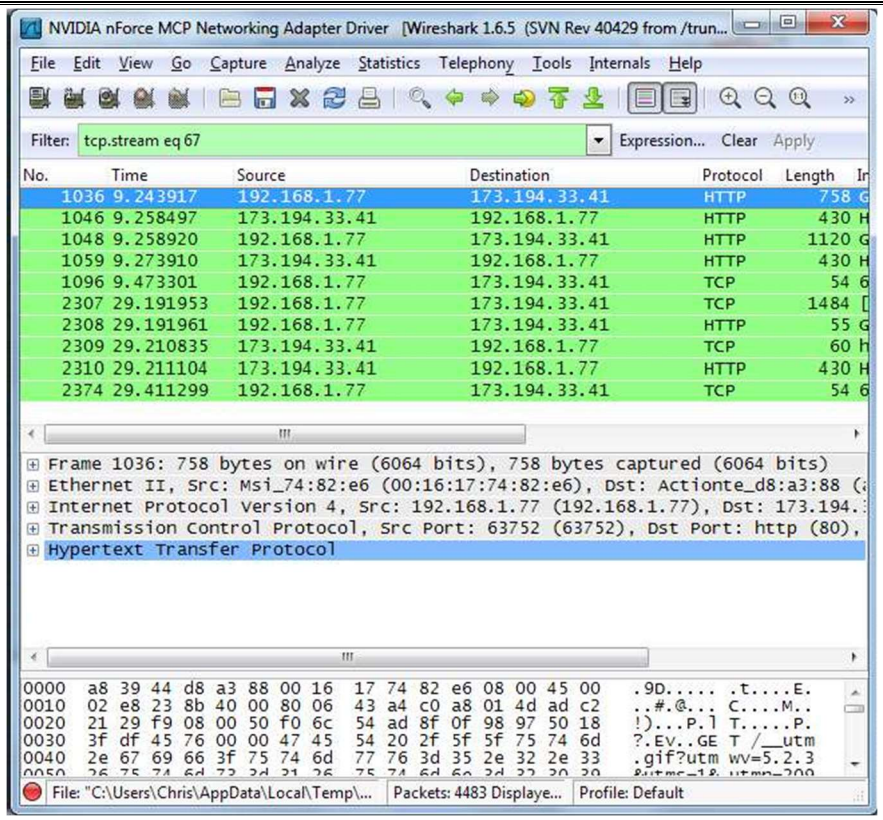
Another interesting thing you can do is right-click a packet and select Follow TCPStream.



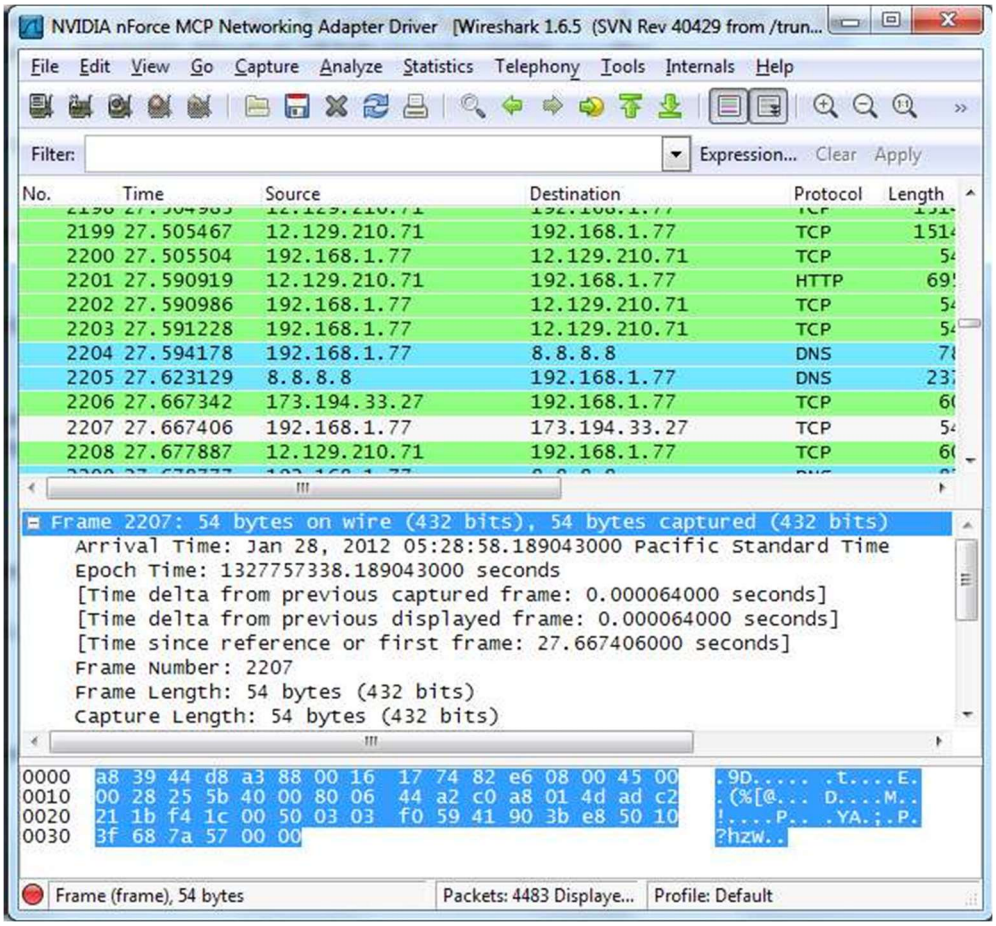
You'll see the full conversation between the client and the server.



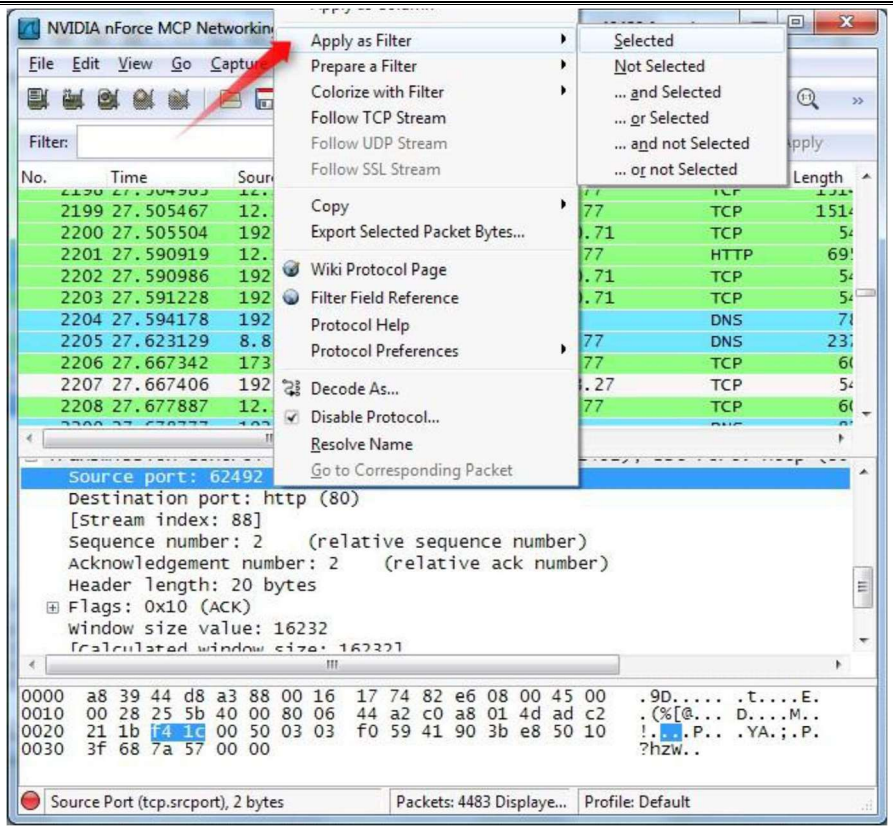
Close the window and you'll find a filter has been applied automatically – Wireshark is showing you the packets that make up the conversation.



Inspecting Packets:- Click a packet to select it and you can dig down to view its details.



You can also create filters from here --- just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

Result / Conclusion:-

In this experiment we analyze various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is network monitoring tool. It is opted for network monitoring, traffic analysis, troubleshooting, Packet grapping, message, protocol analysis, penetration testing and many other purposes.

Experiment-9

Experiment:- Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures.

AIM: Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG).

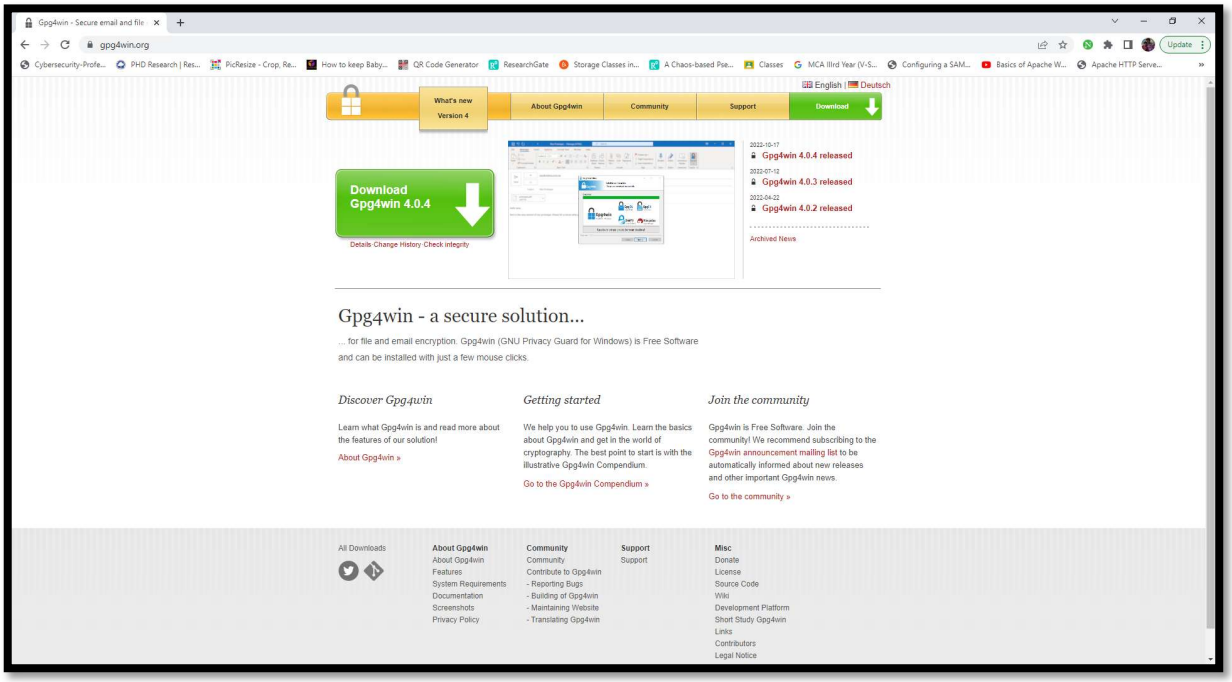
INTRODUCTION:

Here's the final guide in my PGP basics series, this time focusing on Windows the OS in question will be Windows 7, but it should work for Win8 and Win8.1 as well Obviously it's not recommended to be using Windows to access the DNM, but I won't go into the reasons here. The tool will be using is GPG4Win

INSTALLING THE SOFTWARE:

Visit www.gpg4win.org. Click on the "Gpg4win 2.3.0" button

On the following screen, click the "Download Gpg4win" button.

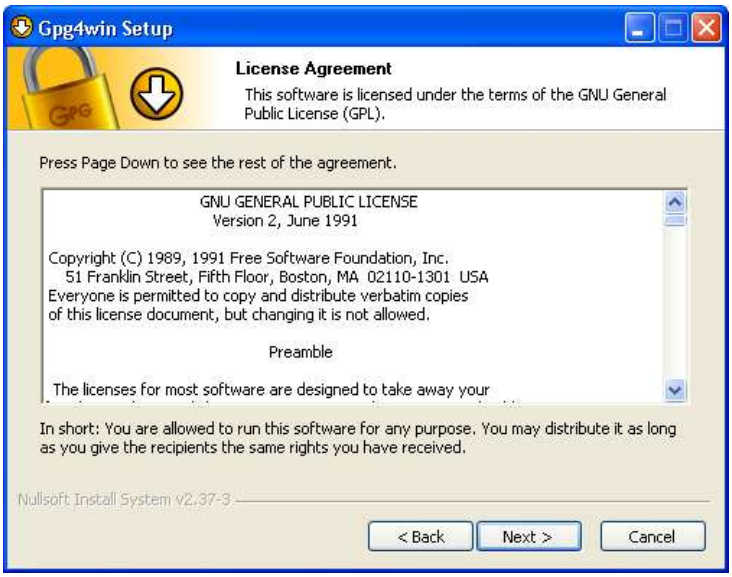


You can load and install Gpg4win from the Internet or a CD. To do this, you will need administrator rights to your Windows operating system. If you are downloading Gpg4win from the Internet, please ensure that you obtain the file from a trustworthy site, e.g.: www.gpg4win.org. To start the installation, click on the following file after the download:

gpg4win-2.0.0.exe (or higher version number). If you received Gpg4win on a CD ROM, please open it and click on the "Gpg4win" installation icon. All other installation steps are the same. The response to the question of whether you want to install the program is [*Yes*]. The installation assistant will start and ask you for the language to be used with the installation process:

Confirm your language selection with [*OK*]. Afterwards you will see this welcome dialog:

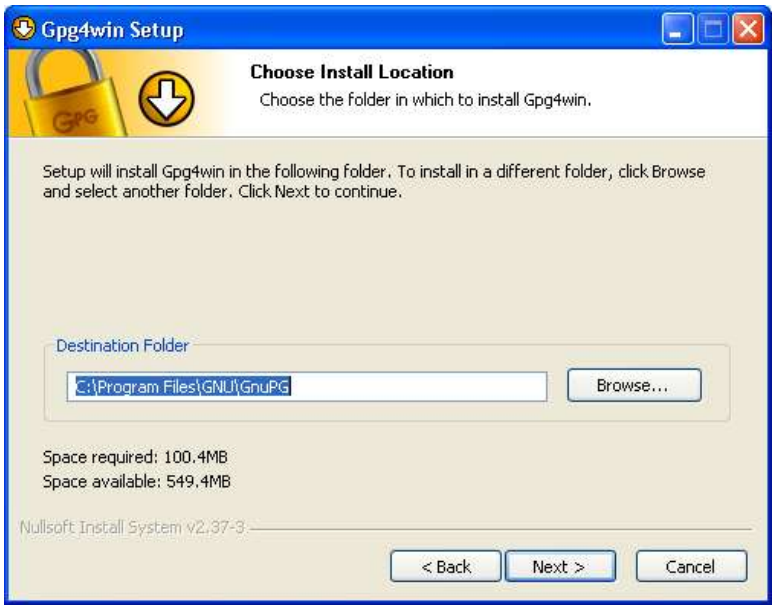
Close all programs that are running on your computer and click on [Next]. The next page displays the licensing agreement - it is only important if you wish to modify or forward Gpg4win. If you only want to use the software, you can do this right away - without reading the license.



Click on [Next].

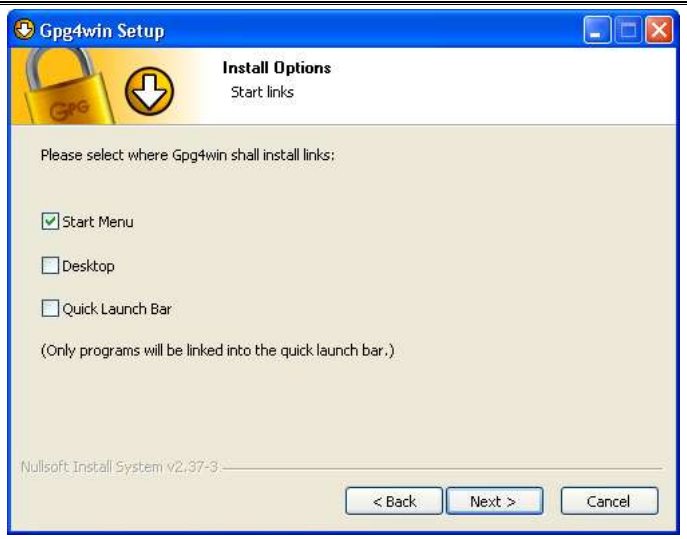
On the page that contains the selection of components you can decide which programs you want to install. A default selection has already been made for you. You can also install individual components at a later time. Moving your mouse cursor over a component will display a brief description. Another useful feature is the display of required hard drive space for all selected components.

Click on [*Next*]. The system will suggest a folder for the installation, e.g.: C:\Programme\GNU\GnuPG. You can accept the suggestion or select a different folder for installing Gpg4win.



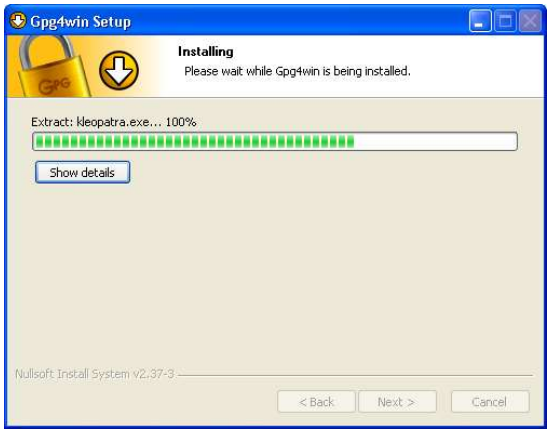
Then click on [*Next*].

Now you can decide which **links** should be insalled - the system will automatically create a link with the start menu. You can change this link later on using the Windows dashboard settings.



Then click on [*Next*]. If you have selected the default setting - **link with start menu** - you can define the name of this start menu on the next page or simply accept the name.

Then click on [*Install*]. During the **installation** process that follows, you will see a progress bar and information on which file is currently being installed. You can press [*Show details*] at any time to show the installation log.



Once you have completed the installation, please click on [*Next*]. The last page of the installation process is shown once the installation has been successfully completed:

You have the option of displaying the README file, which contains important information on the Gpg4win version you have just installed. If you do not wish to view this file, deactivate this option.

Then click on [*Finish*]. In some cases you may have to restart Windows. In this case, you will see the following page:

Now you can decide whether Windows should be restarted immediately or manually at a later time.

Click on [*Finish*]. Please read the README file which contains up-to-date information on the Gpg4win version that has just been installed. You can find this file e.g. via the start menu: *Start -> Programs -> Gpg4win -> Documentation -> Gpg4win README*

And that's it! You have successfully installed Gpg4win and are ready to work with the program.

CREATING YOUR PUBLIC AND PRIVATE KEYS

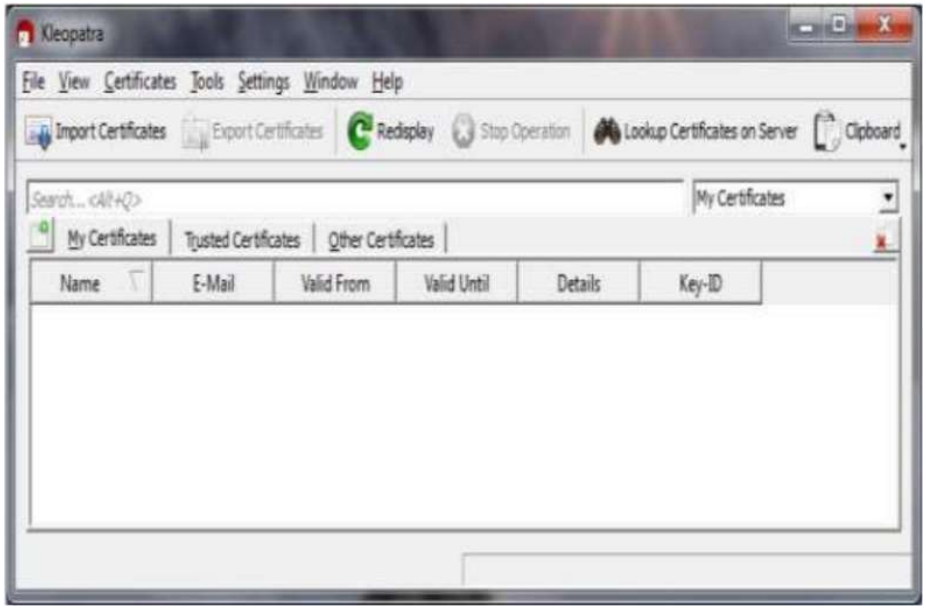
GPG encryption and decryption is based upon the keys of the person who will be receiving the encrypted file or message. Any individual who wants to send the person an encrypted file or message must possess the recipient's public key certificate to encrypt the message. The recipient must have the associated private key,

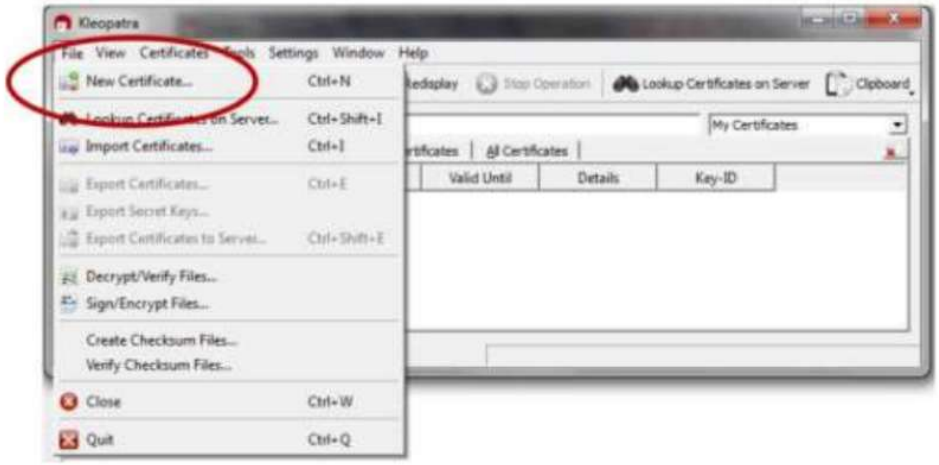
which is different than the public key, to be able to decrypt the file. The public and private key pair for an individual is usually generated by the individual on his or her computer using the installed GPG program, called “Kleopatra” and the following procedure:

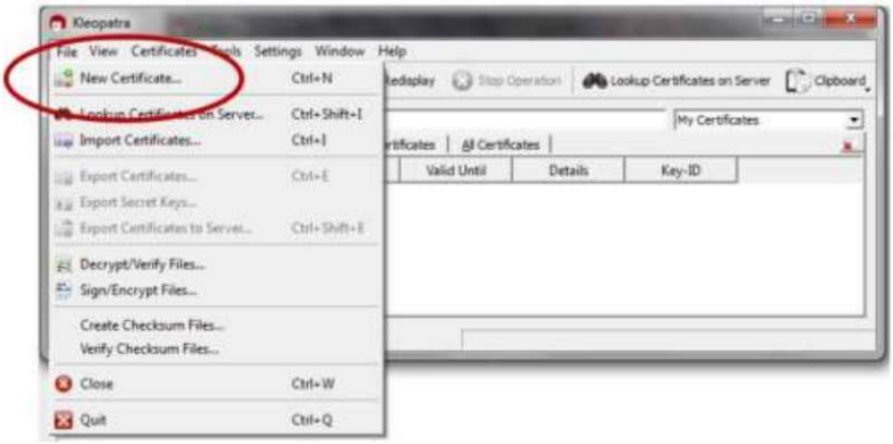
From your start bar, select the “Kleopatra” icon to start the Kleopatra certificate management software

The following screen will be displayed From the “File” dropdown, click on the “New Certificate”

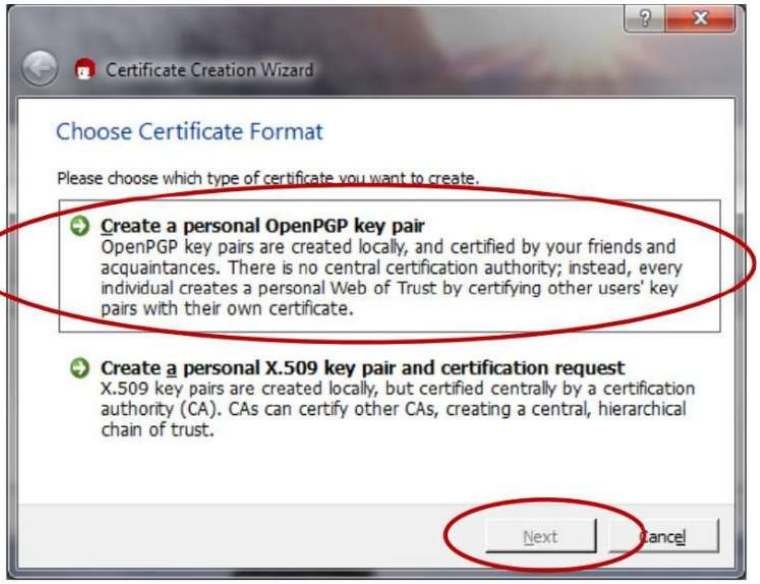
Option



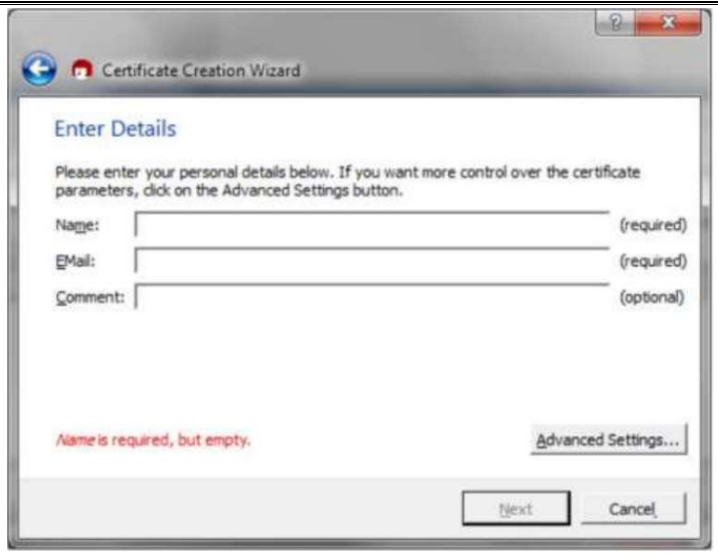




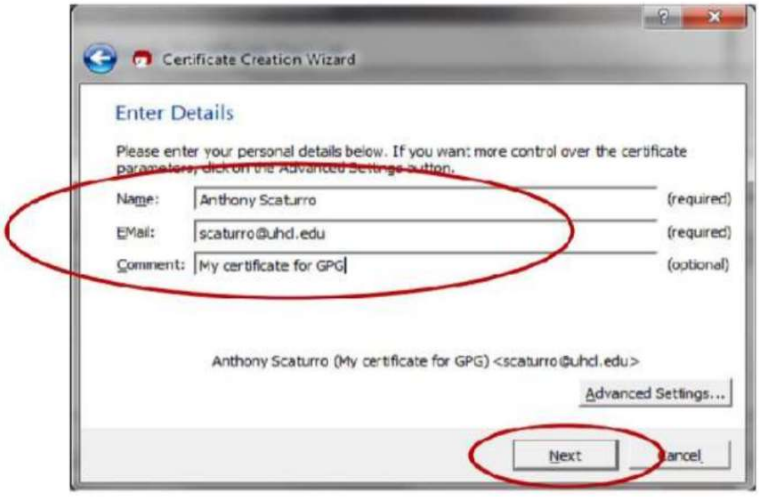
The following screen will be displayed. Click on "Create a personal OpenGPG key pair" and the "Next" button



The Certificate Creation Wizard will start and display the following:



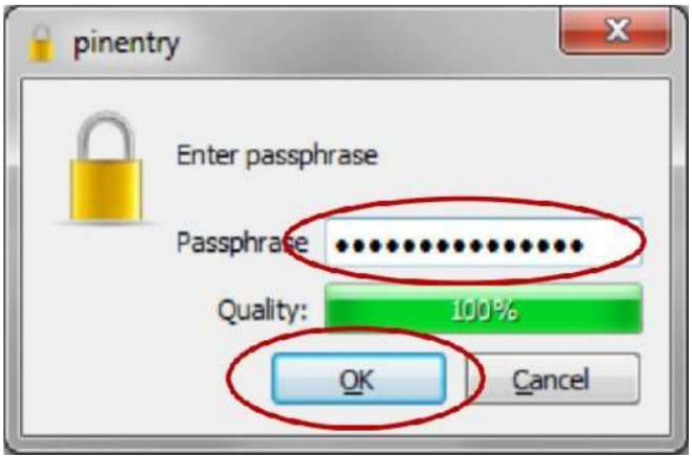
Enter your name and e-mail address. You may also enter an optional comment. Then, click the "Next" button



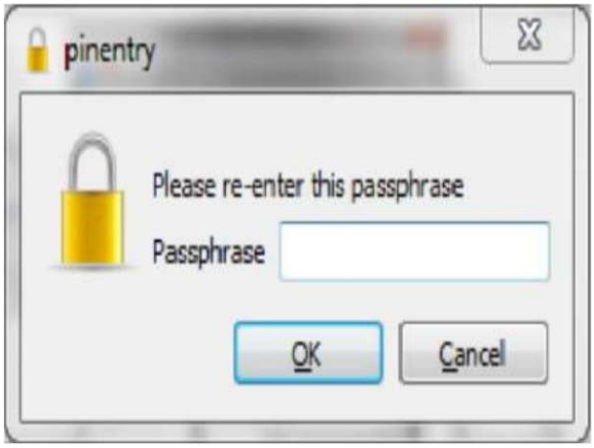
Review your entered values. If OK, click the "Create Key" button

You will be asked to enter a passphrase

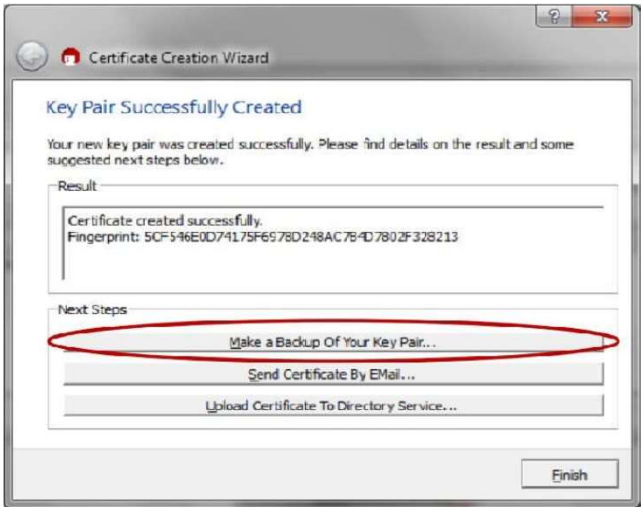
The passphrase should follow strong password standards. After you've entered your passphrase, click the "OK" button.



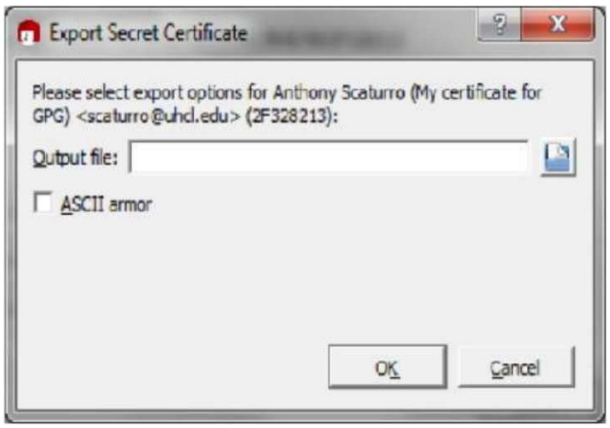
You will be asked to re-enter the passphrase Re-enter the passphrase value. Then click the "OK" button. If the passphrases match, the certificate will be created.



Once the certificate is created, the following screen will be displayed. You can save a backup of your public and private keys by clicking the "Make a backup Of Your Key Pair" button. This backup can be used to copy certificates onto other authorized computers.

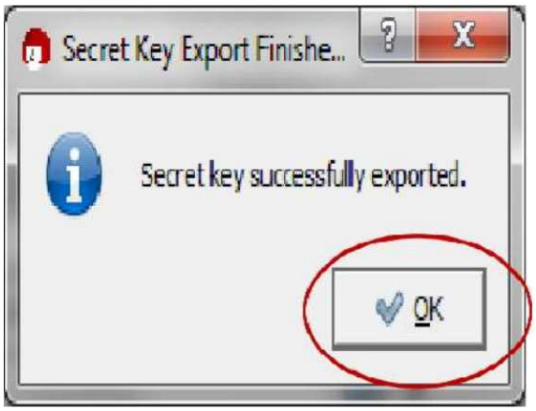


If you choose to back up your key pair, you will be presented with the following screen:



Specify the folder and name the file. Then click the “OK” button.

After the key is exported, the following will be displayed. Click the "OK" button.

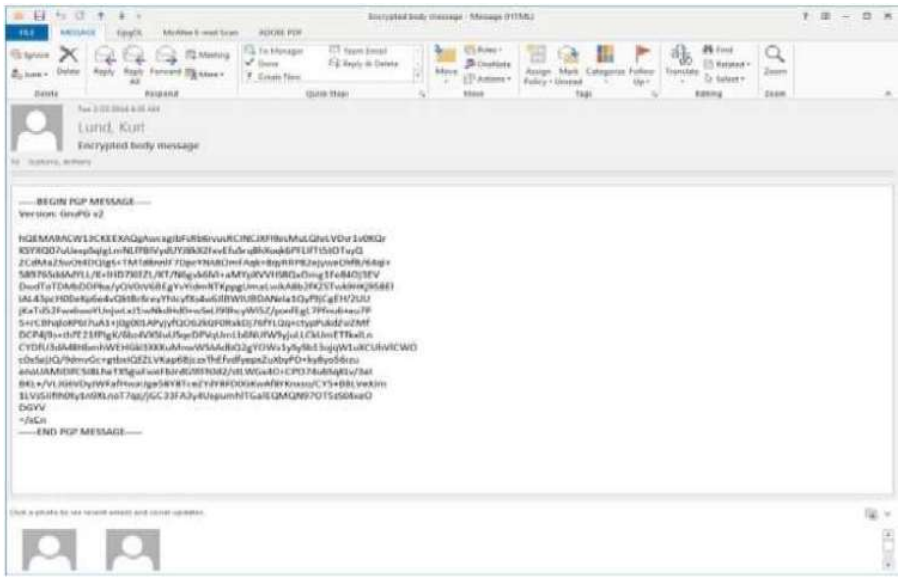


You will be returned to the "Key Pair Successfully Created" screen. Click the "Finish" button.

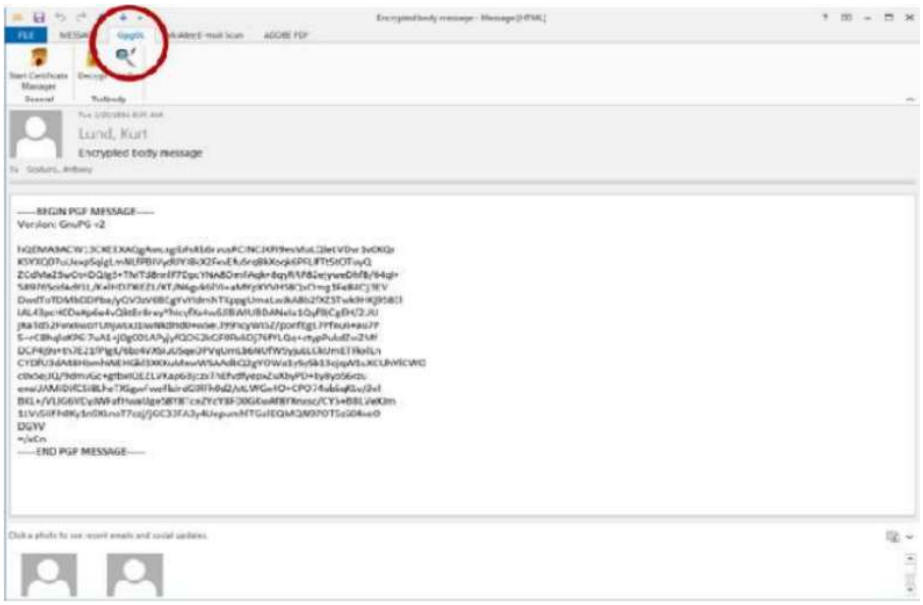
Before the program closes, you will need to confirm that you want to close the program by clicking on the "Quit Kleopatra" button

DECRYPTING AN ENCRYPTED E-MAIL THAT HAS BEEN SENT TO YOU:

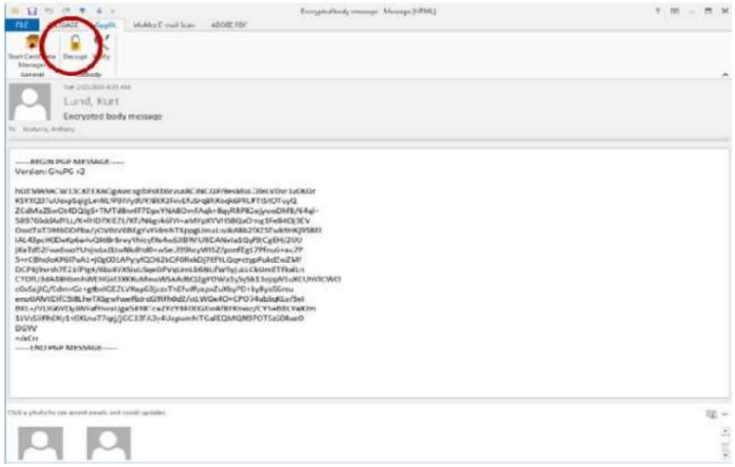
Open the e-mail message



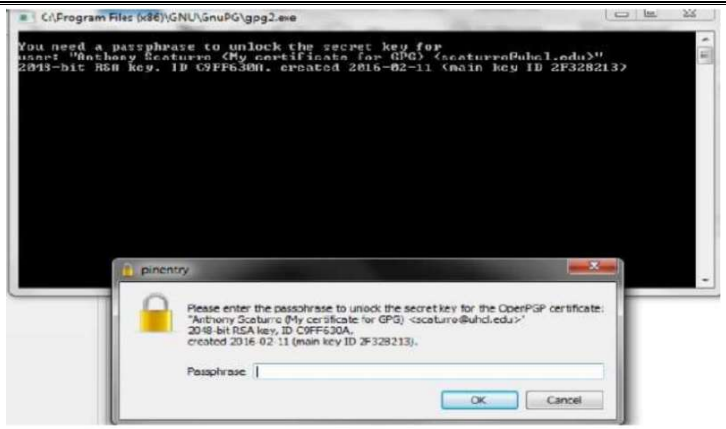
Select the GpgOL tab



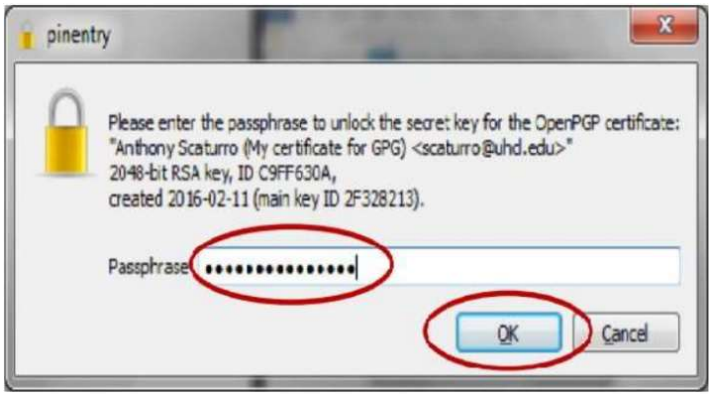
Click the “Decrypt” button



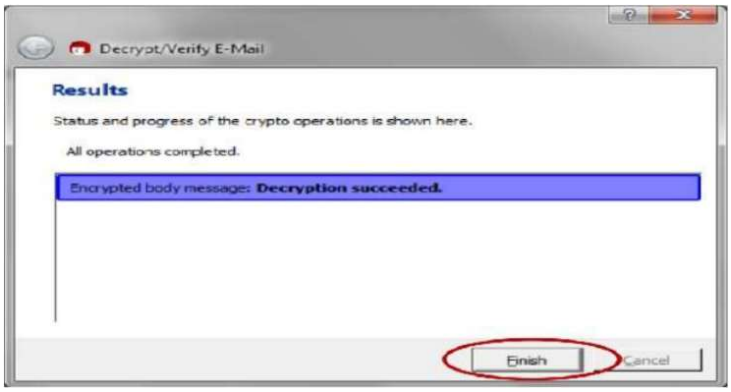
A command window will open along with a window that asks for the Passphrase to your private key that will be used to decrypt the incoming message.



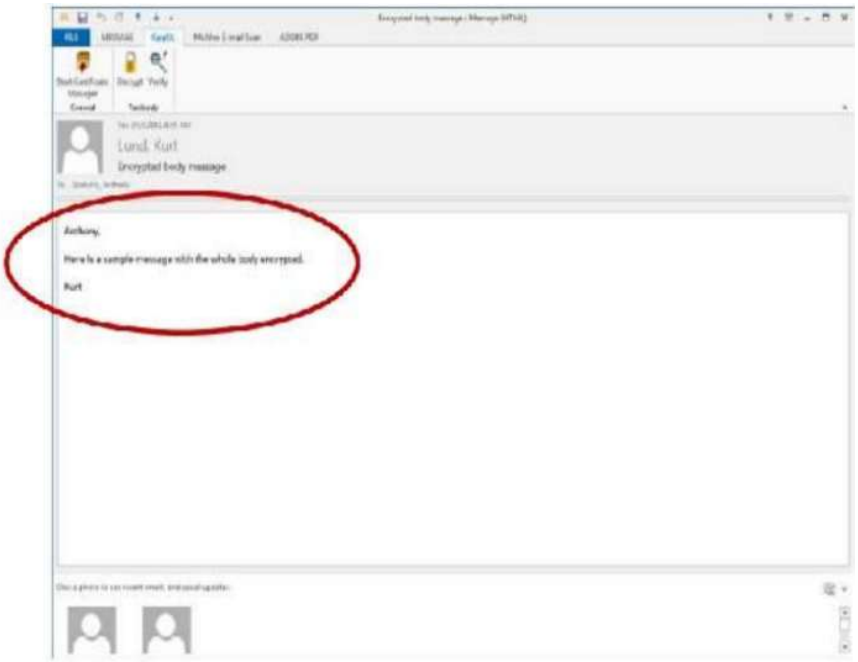
Enter your passphrase and click the “OK” button



The results window will tell you if the decryption succeeded. Click the “Finish” button top close the window



Your unencrypted e-mail message body will be displayed.



When you close the e-mail, you will be asked if you want to save the e-mail message in its unencrypted form.

For maximum security, click the "No" button. This will keep the message encrypted within the e-mail system and will require you to enter your passphrase each time you reopen the e-mail message

RESULT:

Thus the secure data storage, secure data transmission and for creating digital signatures (GnuPG) was developed successfully.

Experiment-10

Experiment: Write steps to install rootkit malicious software in system

AIM:

Rootkit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued privileged access toa computer.

INTRODUCTION:

Breaking the term rootkit into the two component words, root and kit, is a useful wayto define it. Root is a UNIX/Linux term that's the equivalent ofAdministrator in Windows. The word kit denotes programs that allow someone to obtain root/admin-level access to the computer by executing the programs in the kit — all of which is done without end-user consent or knowledge.

A rootkit is a type of malicious software that is activated each time your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals,network connections, and the keyboard.

Rootkits have two primary functions: remote command/control (back door) and software eavesdropping. Rootkits allow someone, legitimate or otherwise, to administratively control a computer. This means executing files, accessing logs, monitoring user activity, and even changing the computer's configuration. Therefore, in the strictest sense, even versions of VNC are rootkits. This surprises most people, as they consider rootkits to be solely malware, but in of themselves they aren't malicious at all.

The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

PROCEDURE:

STEP-1: Download Rootkit Tool from GMER website www.gmer.net.

STEP-2: This displays the Processes, Modules, Services, Files, Registry, RootKit / Malwares, Autostart, CMD of local host.

STEP-3: Select Processes menu and kill any unwanted process if any.

STEP-4: Modules menu displays the various system files like .sys, .dll

STEP-5: Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.

STEP-6: Files menu displays full files on Hard-Disk volumes.

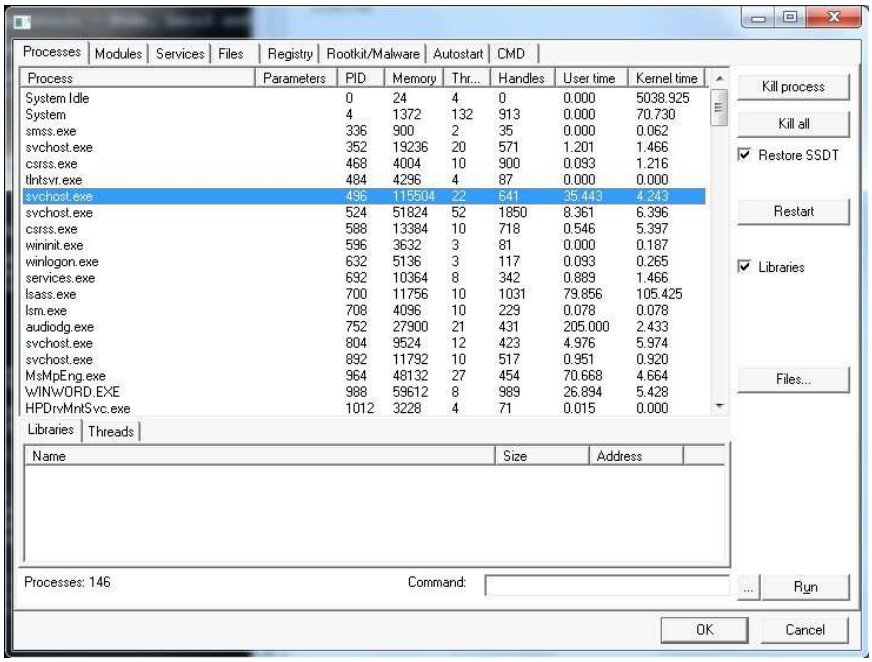
STEP-7: Registry displays Hkey_Current_user and Hkey_Local_Machine.

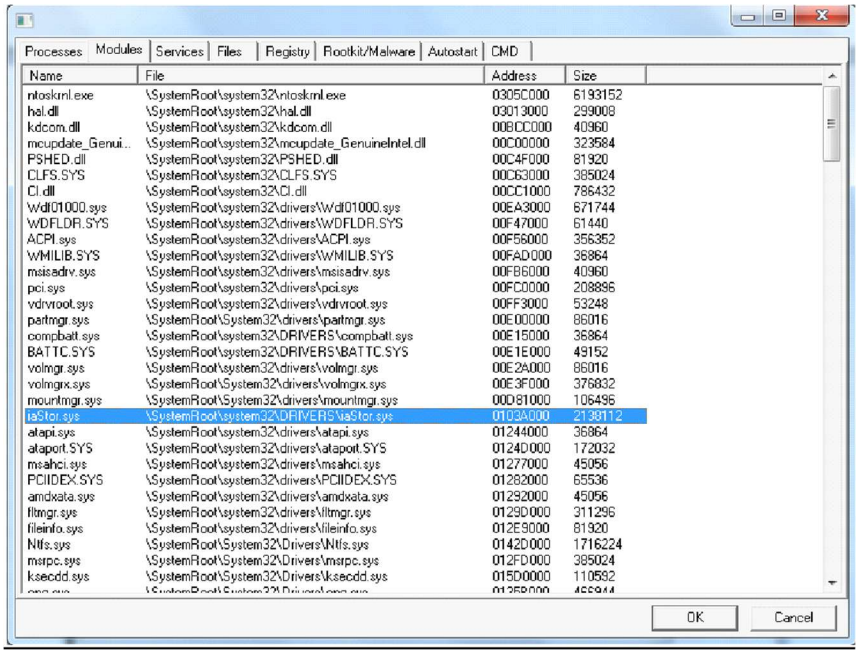
STEP-8: Rootkits / Malwares scans the local drives selected.

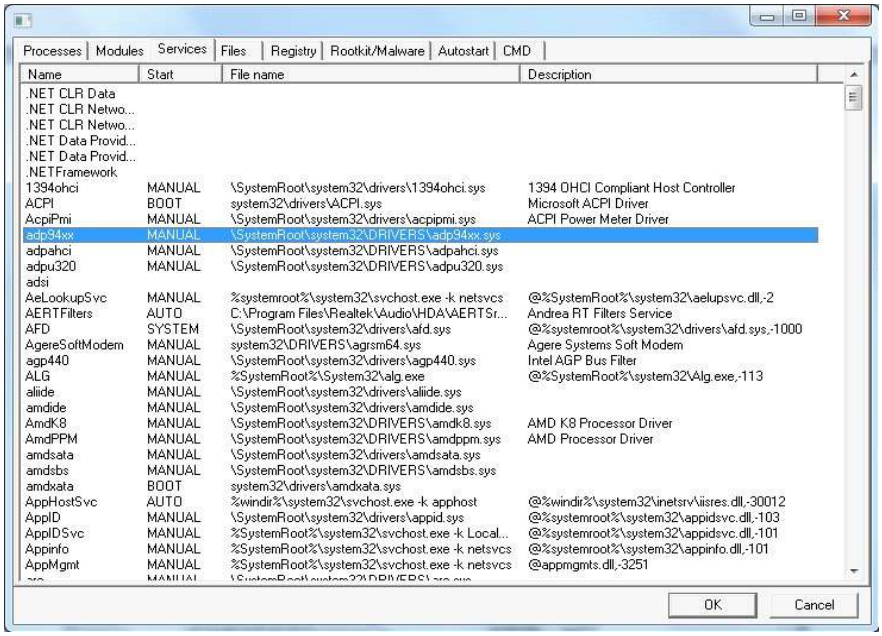
STEP-9: Autostart displays the registry base Autostart applications.

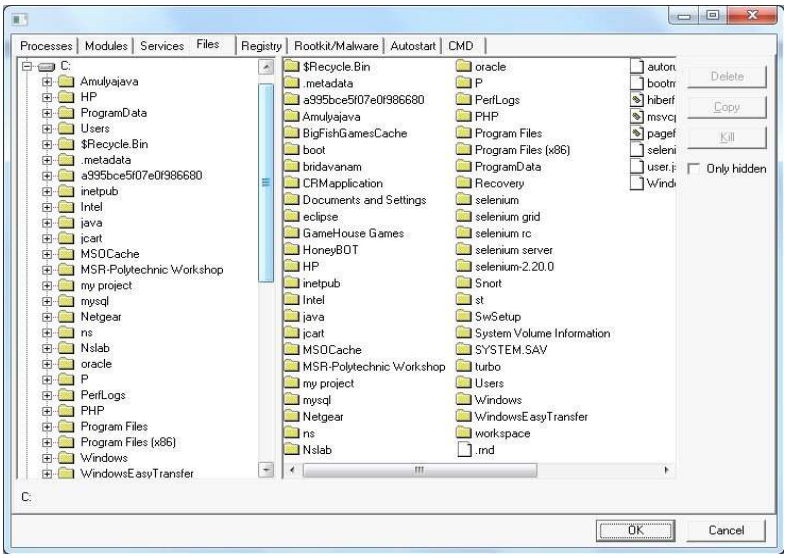
STEP-10:CMD allows the user to interact with command line utilities or Registry

SCREENSHOTS:









Result:

Thus the study of installation of Rootkit software and its variety of options weredeveloped successfully.

Experiment-11

Experiment: Perform an Experiment to Sniff Traffic using ARP Poisoning.

AIM:- *To perform sniff traffic using ARP poisoning.*

Description:

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physical addresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic.

ARP Poisoning Countermeasures

Static ARP entries: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

ARP poisoning detection software: these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC address resolutions can then be blocked.

Operating System Security: this measure is dependent on the operating system been used. The following are the basic techniques used by various operating systems.

- Linux based: these work by ignoring unsolicited ARP reply packets.
- Microsoft Windows: the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;
- AntiARP– provides protection against both passive and active sniffing
- Agnitum Outpost Firewall–provides protection against passive sniffing
- XArp– provides protection against both passive and active sniffing
- Mac OS: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.
- Computers communicate using networks. These networks could be on a local area network

LAN or exposed to the internet. Network Sniffers are programs that capture low-level package data that is transmitted over a network. An attacker can analyze this information to discover valuable information such as user ids and passwords.

- In this article, we will introduce you to common network sniffing techniques and tools used to sniff networks.

What is network sniffing?

Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address.

Network sniffing is the process of intercepting data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to;

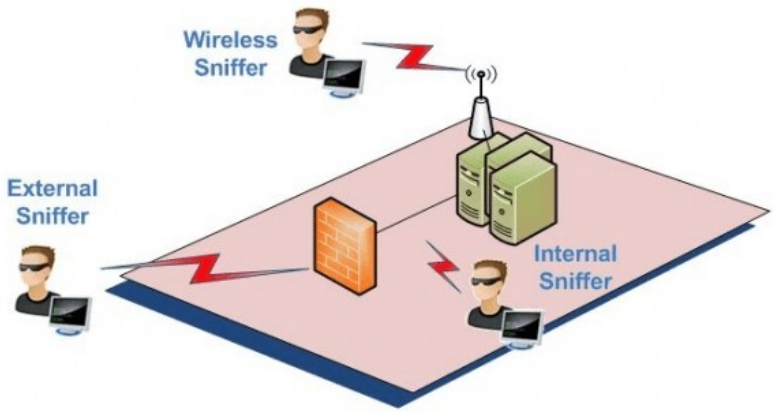
- Capture sensitive data such as login credentials

- Eavesdrop on chat messages
- Capture files have been transmitted over a network

The following are protocols that are vulnerable to sniffing

- Telnet
- Rlogin
- HTTP
- SMTP
- NNTP
- POP
- FTP
- IMAP

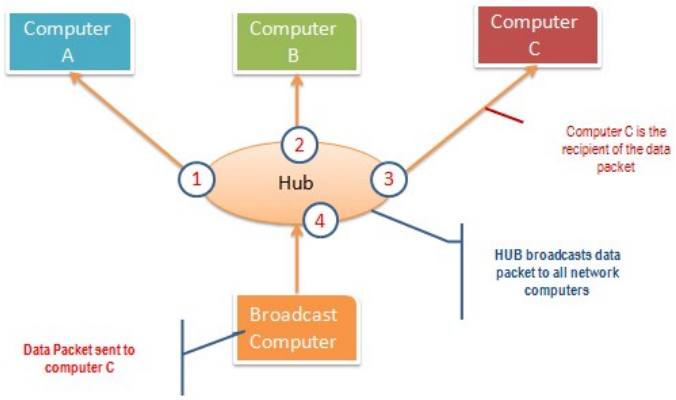
The above protocols are vulnerable if login details are sent in plain text



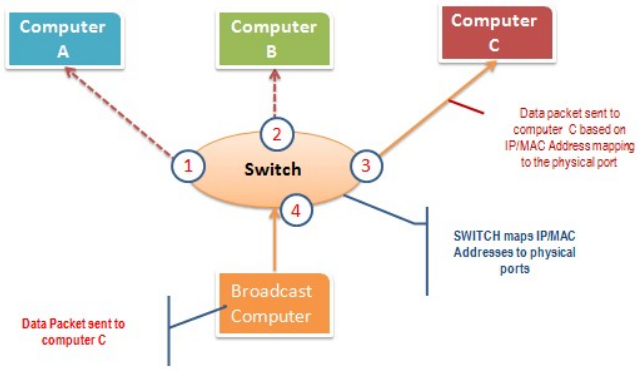
Passive and Active Sniffing

Before we look at passive and active sniffing, let's look at two major devices used to network computers; hubs and switches. A hub works by sending broadcast messages to all output ports on it except the one that has sent the broadcast. The recipient computer responds to the broadcast message if the IP address matches. This means when using a hub, all the computers on a network can see the broadcast message. It operates at the physical layer (layer 1) of the OSI Model.

The diagram below illustrates how the hub works.



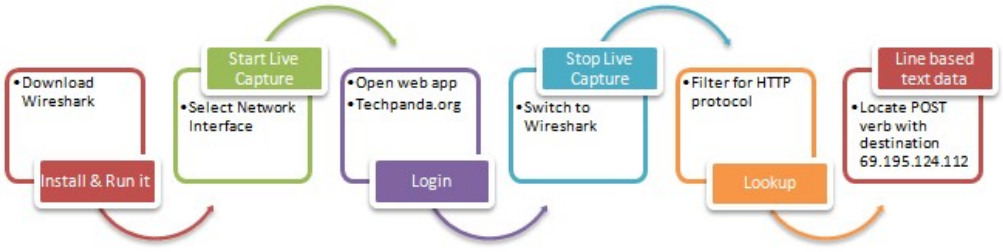
A switch works differently; it maps IP/MAC addresses to physical ports on it. Broadcast messages are sent to the physical ports that match the IP/MAC address configurations for the recipient computer. This means broadcast messages are only seen by the recipient computer. Switches operate at the data link layer (layer 2) and network layer (layer 3). The diagram below illustrates how the switch works.



Passive sniffing is intercepting packages transmitted over a network that uses a hub. It is called passive sniffing because it is difficult to detect. It is also easy to perform as the hub sends broadcast messages to all the computers on the network.

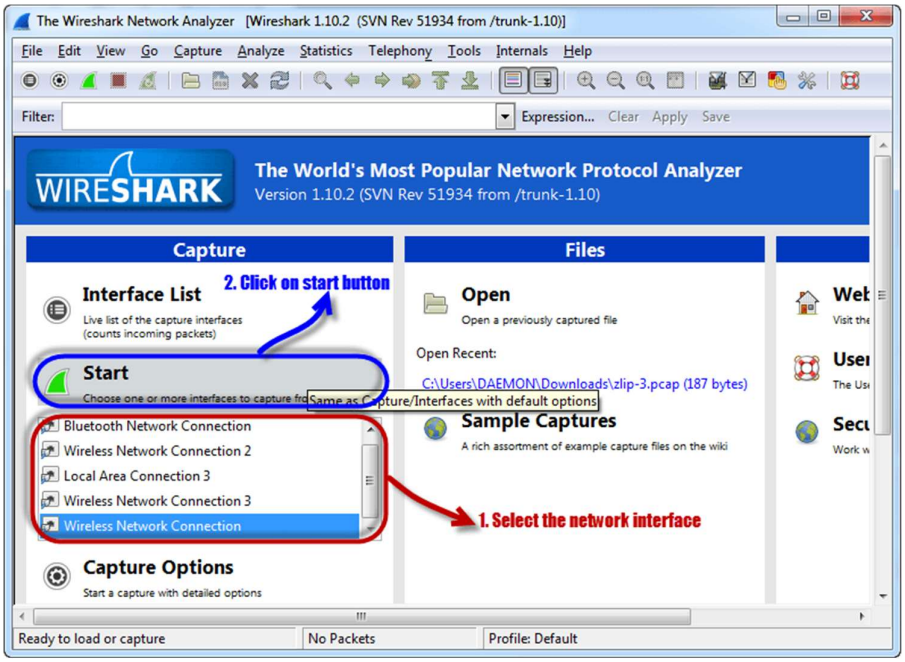
Active sniffing is intercepting packages transmitted over a network that uses a switch. There are two main methods used to sniff switch linked networks, ARP Poisoning, and MAC flooding.

Sniffing the network using Wireshark :- The illustration below shows you the steps that you will carry out to complete this exercise without confusion

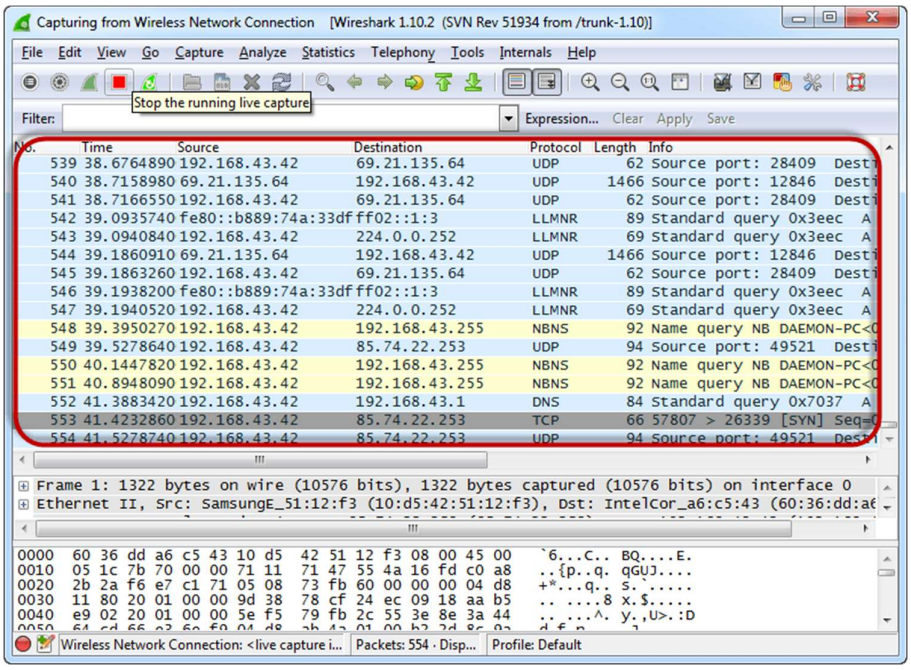


Download Wireshark from this link http://www.wireshark.org/download.html

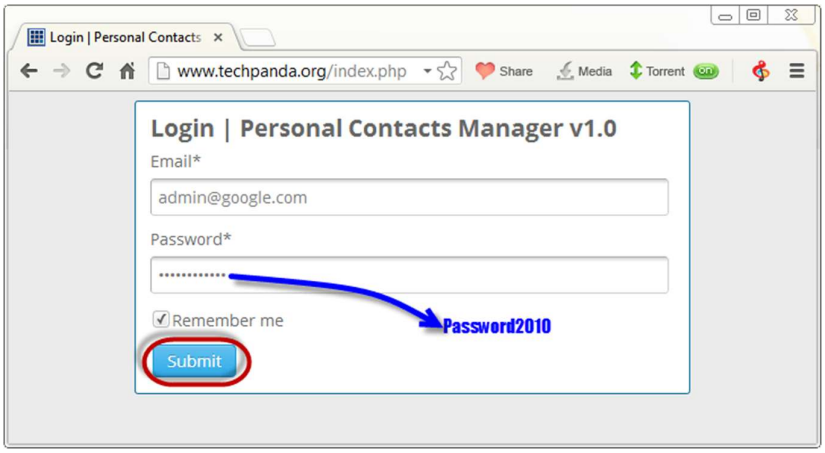
- Open Wireshark
- You will get the following screen



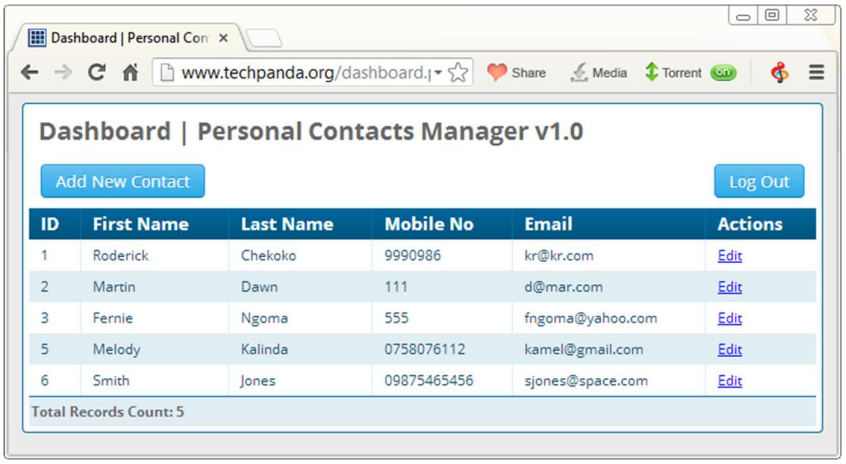
- Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.
- Click on start button as shown above



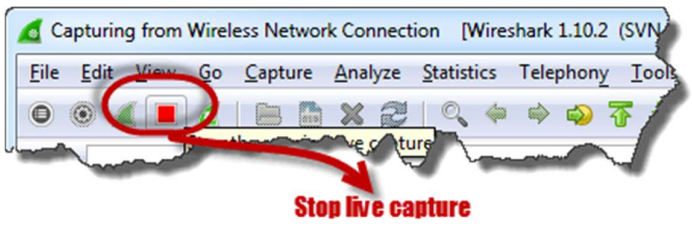
- Open your web browser and type in http://www.techpanda.org/



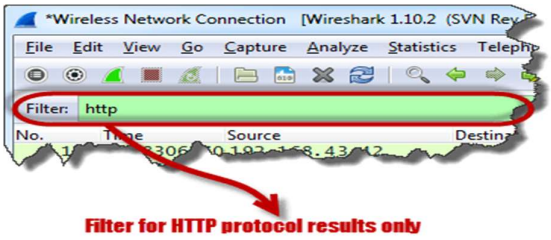
- The login email is **admin@google.com** and the password is **Password2010**
- Click on submit button
- A successful logon should give you the following dashboard



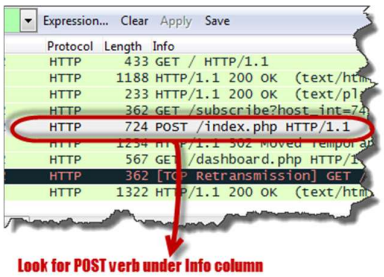
- Go back to Wireshark and stop the live capture



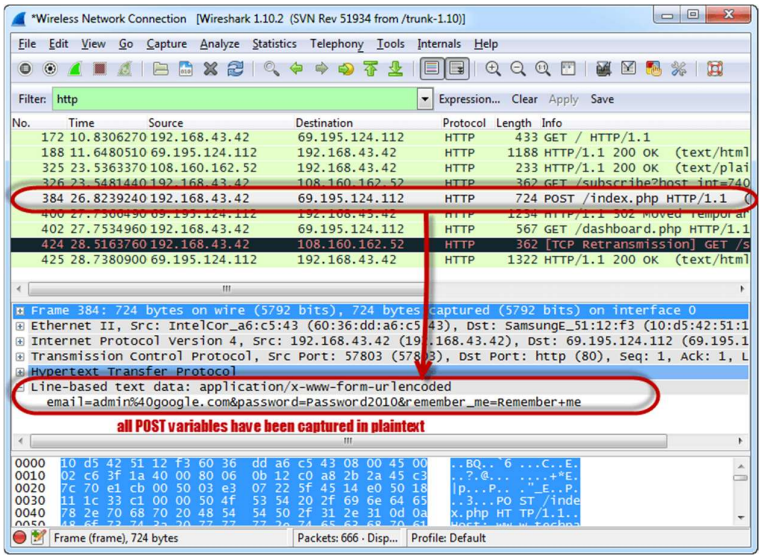
- Filter for HTTP protocol results only using the filter textbox



- Locate the Info column and look for entries with the HTTP verb POST and click on it



- Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded



- You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

RESULT:- Sniff traffic using ARP poisoning is performed successfully.

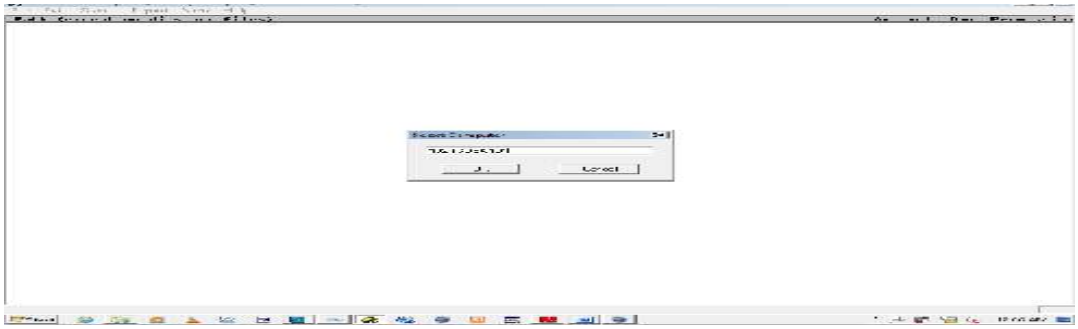
Experiment-12

Experiment: Perform an experiment on how to use Dumpsec.

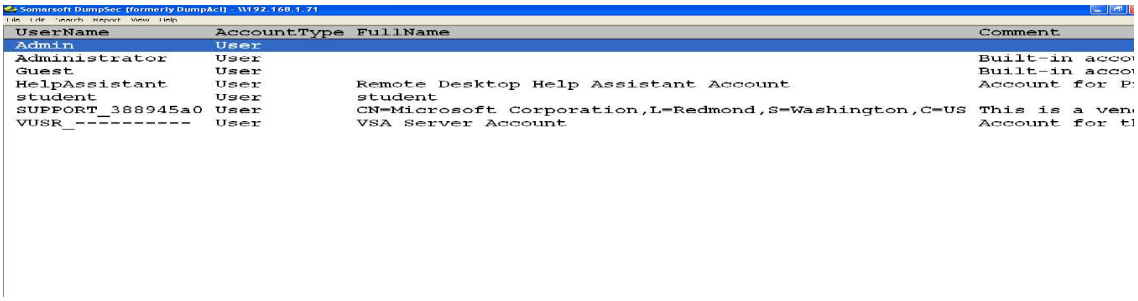
Aim: To operate Dumpsec tool for Security.

Procedure: SomarSoft's Dumper is a (free) security auditing program for Microsoft Windows NT/2000. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information. DumpSec is a must have product for Windows NT systems administrators and computer security auditors.

1. Download & install dumpsec.
2. Open dumpsec and select computer

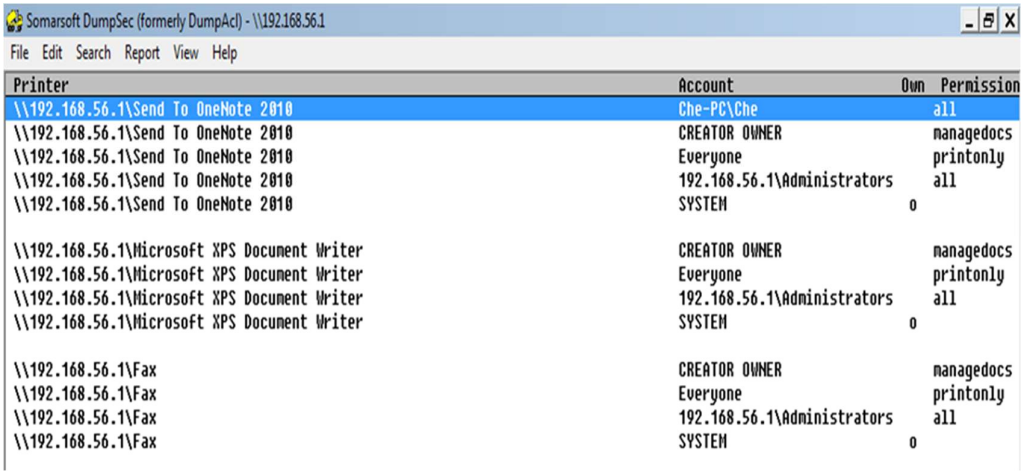


2. Now select report=> dump users as table and click ok.

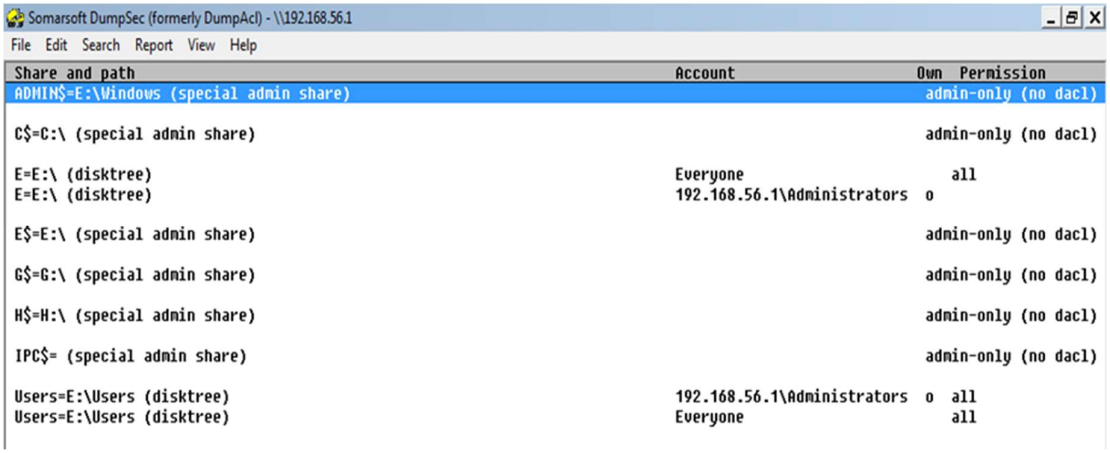


UserName	AccountType	FullName	Comment
Admin	User		
Administrator	User		Built-in acco
Guest	User		Built-in acco
HelpAssistant	User	Remote Desktop Help Assistant Account	Account for P
student	User	student	
SUPPORT_388945a0	User	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	This is a ven
VUSR_----------	User	VSA Server Account	Account for t

Printer Sharing Report



Permission on Shares:



Result:

Thus the experiment was executed successfully.

Experiment 13

Experiment :- Perform an experiment for working with kf sensor tool for creating and monitoring honeypot

AIM: To create honeypot on network

Theory:-

Honey Pot is a device placed on Computer Network specifically designed to capture malicious network traffic. KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen. If there are no alerts then green icon is displayed.

INTRODUCTION:

HONEY POT:

A honeypot is a computer system that is set up to act as a decoy to lure cyber attackers, and to detect, deflect or study attempts to gain unauthorized access to information systems. Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value. Honeypots can be classified based on their deployment (use/action) and based on their level of involvement.

Based on deployment, honeypots may be classified as:

1. Production honeypots
2. Research honeypots

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots.

Research honeypots are run to gather information about the motives and tactics of the Black hat community targeting different networks. These honeypots do not add direct value to a specific

organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats.

KF SENSOR:

KFSensor is a Windows based honeypot Intrusion Detection System (IDS). It acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and trojans. By acting as a decoy server it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. KFSensor is a system installed in a network in order to divert and study an attacker's behavior. This is a new technique that is very effective in detecting attacks.

The main feature of KFSensor is that every connection it receives is a suspect hence it results in very few false alerts. At the heart of KFSensor sits a powerful internet daemon service that is built to handle multiple ports and IP addresses. It is written to resist denial of service and buffer overflow attacks. Building on this flexibility KFSensor can respond to connections in a variety of ways, from simple port listening and basic services (such as echo), to complex simulations of standard system services. For the HTTP protocol KFSensor accurately simulates the way Microsoft's web server (IIS) responds to both valid and invalid requests. As well as being able to host a website it also handles complexities such as range requests and client side cache negotiations. This makes it extremely difficult for an attacker to fingerprint, or identify KFSensor as a honeypot.

PROCEDURE:

STEP-1: Download KF Sensor Evaluation Setup File from KF Sensor Website.

STEP-2: Install with License Agreement and appropriate directory path.

STEP-3: Reboot the Computer now. The KF Sensor automatically starts during windows boot.

STEP-4: Click Next to setup wizard.

STEP-5: Select all port classes to include and Click Next.

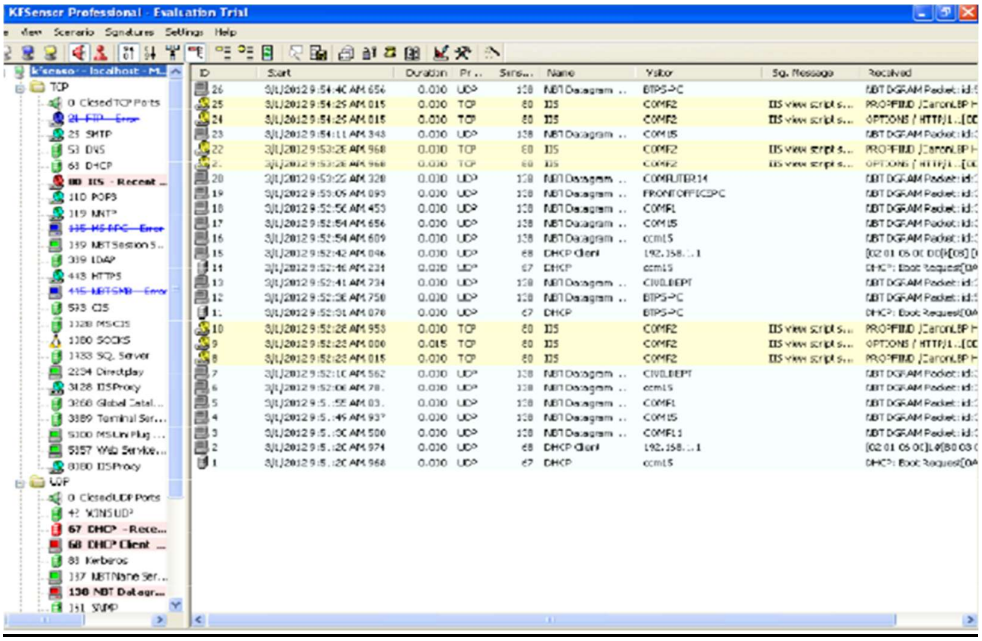
STEP-6: "Send the email and Send from email", enter the ID and Click Next.

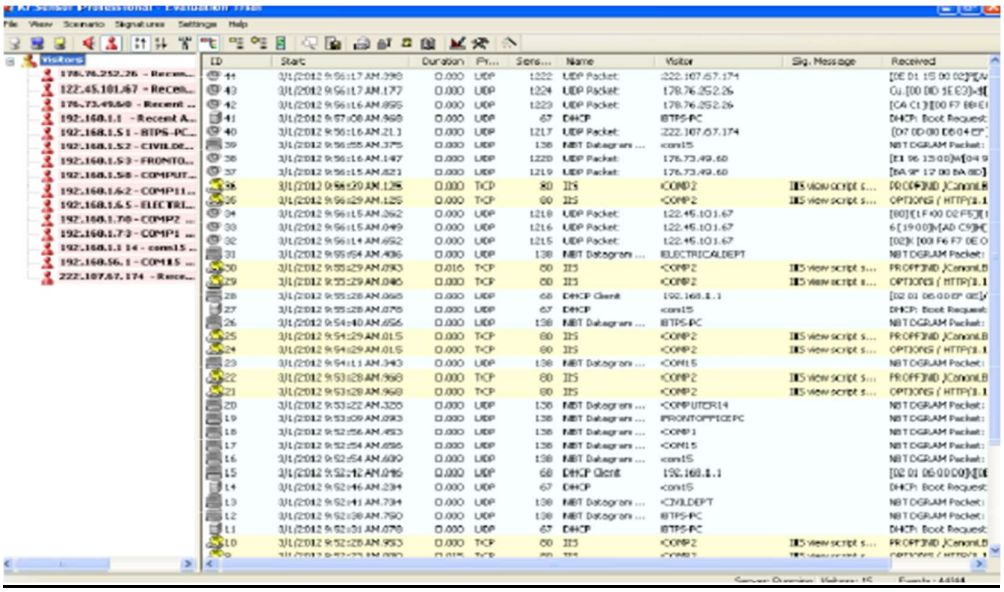
STEP-7: Select the options such as Denial of Service[DOS], Port Activity, Proxy Emulsion Network Port Analyzer, Click Next.

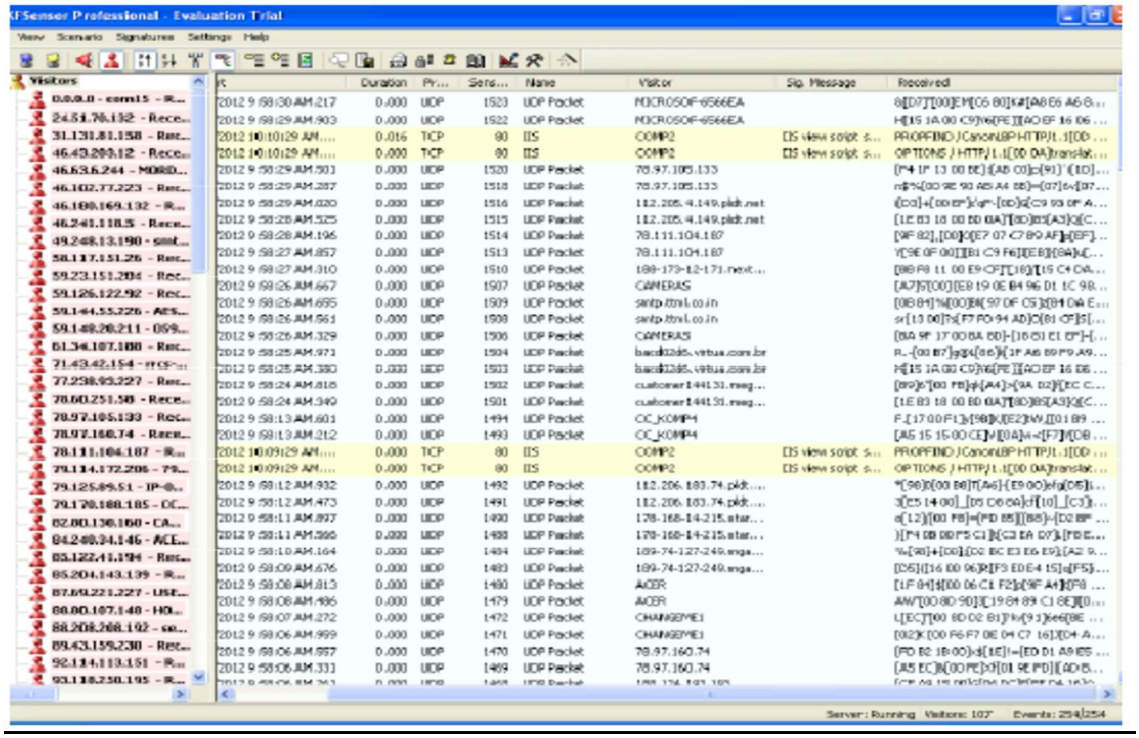
STEP-8: Select Install as System service and Click Next.

STEP-9: Click finish.

SCREENSHOTS:







RESULT:

Thus the study of setup a hotspot and monitor the hotspot on network has been developed successfully.

Experiment 14

Experiment: Perform an experiment for demonstrate intrusion detection system (ids) using any tool (snort or any other s/w).

AIM: To Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w).

Theory:-

Snort is an open source network intrusion detection system (NIDS) and it is a packet sniffer that monitors network traffic in real time.

INTRODUCTION:

INTRUSION DETECTION SYSTEM:

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories:

1. Signature-based intrusion detection systems
2. Anomaly detection systems.

Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts.

Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers.

SNORT TOOL:

Snort is based on libpcap (for library packet capture), a tool that is widely used in TCP/IP traffic sniffers and analyzers. Through protocol analysis and content searching and matching, Snort detects attack methods, including denial of service, buffer overflow, CGI attacks, stealth port scans, and SMB probes. When suspicious behavior is detected, Snort sends a real-time alert to syslog, a separate 'alerts' file, or to apop-up window.

Snort is currently the most popular free network intrusion detection software. The advantages of Snort are numerous. According to the snort web site, “It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflow, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more” (Caswell).

One of the advantages of Snort is its ease of configuration. Rules are very flexible, easily written, and easily inserted into the rule base. If a new exploit or attack is found a rule for the attack can be added to the rule base in a matter of seconds. Another advantage of snort is that it allows for raw packet data analysis.

SNORT can be configured to run in three modes:

1. Sniffer mode
2. Packet Logger mode
3. Network Intrusion Detection System mode

1. Sniffer mode
   - → Snort –v Print out the TCP/IP packets header on the screen.
   - → Snort –vd show the TCP/IP ICMP header with application data in transmit

2. Packet Logger mode
   - → snort –dev –l c:\log [create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.
   - → snort –dev –l c:\log –h ipaddress/24:This rule tells snort that you want to print out the data link and TCP/IP headers as well as application data into the log directory. snort –l c:\log –b This is binary mode logs everything into a single file.

3. Network Intrusion Detection System mode
   - → snort –d c:\log –h ipaddress/24 –c snort.conf This is a configuration file applies rule to each packet to decide it an action based upon the rule type in the file.
   - → Snort –d –h ipaddress/24 –l c:\log –c snort.conf This will cnfigure snort to run in its most basic NIDS form, logging packets that trigger rules specifies in the snort.conf.

PROCEDURE:

STEP-1: Sniffer mode snort –v Print out the TCP/IP packets header on the screen.

STEP-2: Snort –vd Show the TCP/IP ICMP header with application data in transit.

STEP-3: Packet Logger mode snort –dev –l c:\log [create this directory in the C drive] and snort will automatically know to go into packet logger mode, it collects every packet it sees and places it in log directory.

STEP-4: snort –dev –l c:\log –h ipaddress/24 This rule tells snort that you want to print out the data link and TCP/IP headers as well as application data into the log directory.

STEP-5: snort –l c:\log –b this binary mode logs everything into a single file.

STEP-6: Network Intrusion Detection System mode snort –d c:\log –h ipaddress/24 –c snort.conf This is a configuration file that applies rule to each packet to decide it an action based upon the rule type in the file.

STEP-7: snort –d –h ip address/24 –l c:\log –c snort.conf This will configure snort to run in its most basic NIDS form, logging packets that trigger rules specifies in the snort.conf.

STEP-8: Download SNORT from snort.org. Install snort with or without database support.

STEP-9: Select all the components and Click Next. Install and Close.

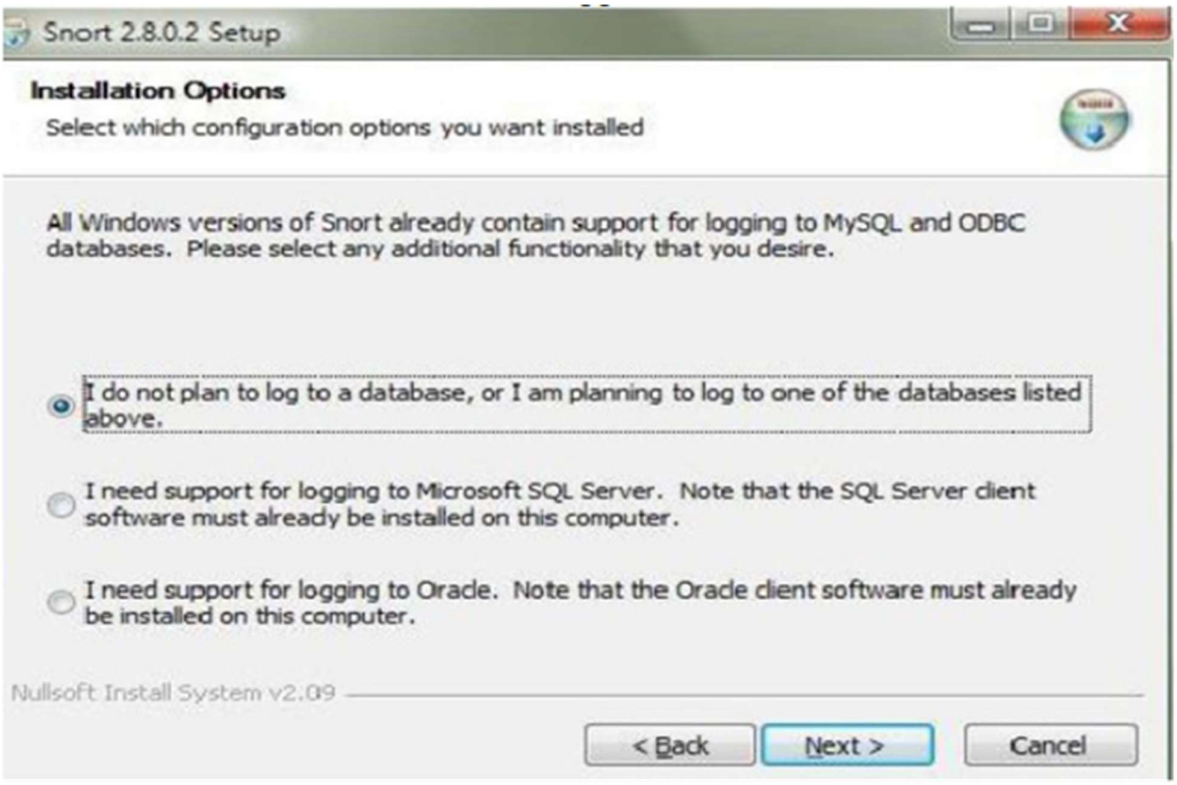
STEP-10: Skip the WinPcap driver installation.

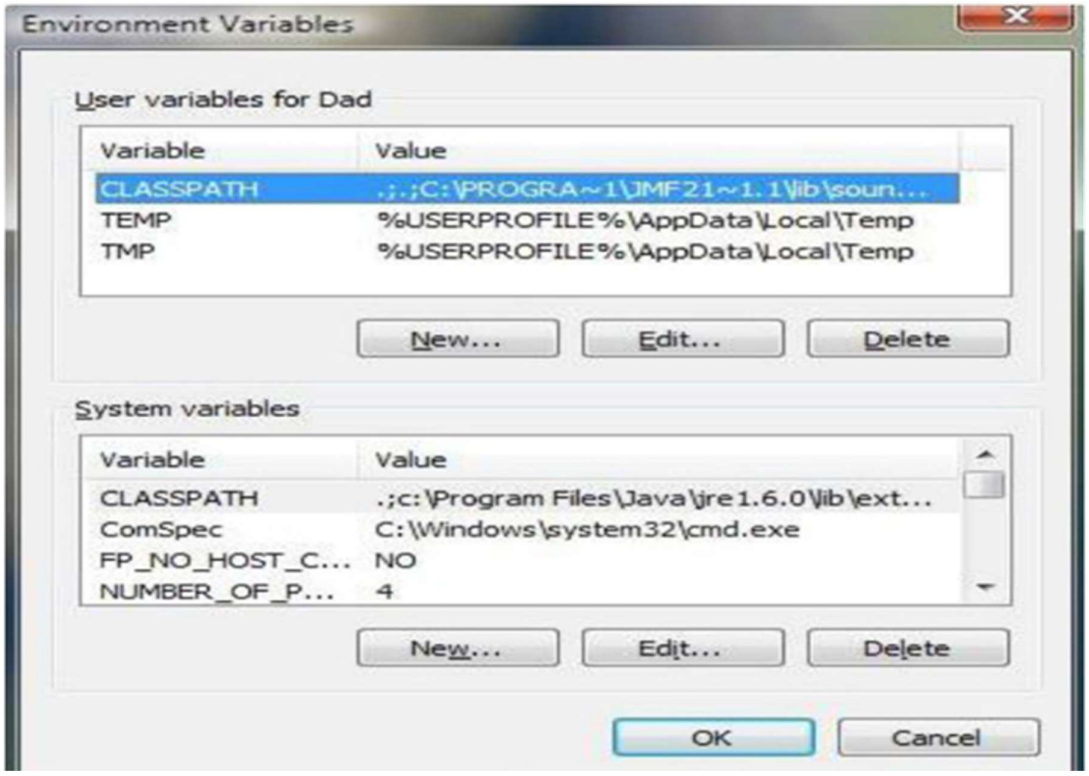
STEP-11: Add the path variable in windows environment variable by selecting new classpath.

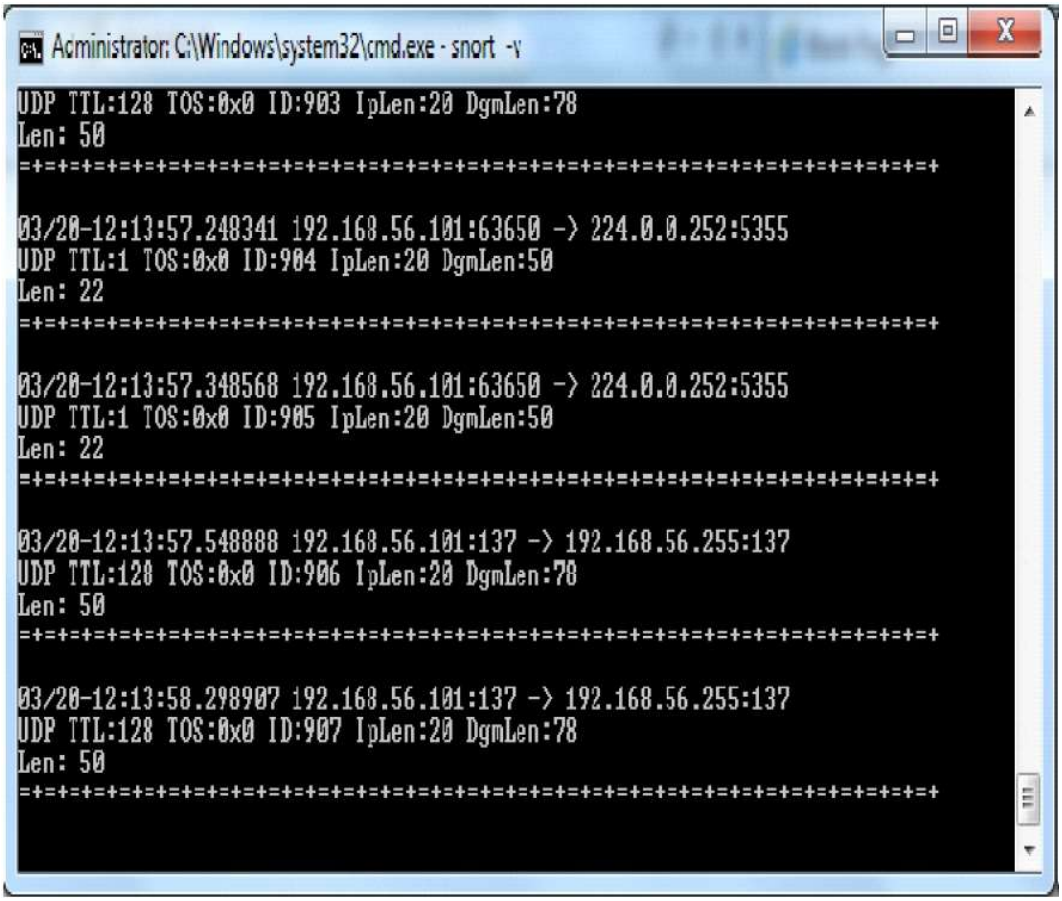
STEP-12: Create a path variable and point it at snort.exe variable name path and variable value c:\snort\bin.

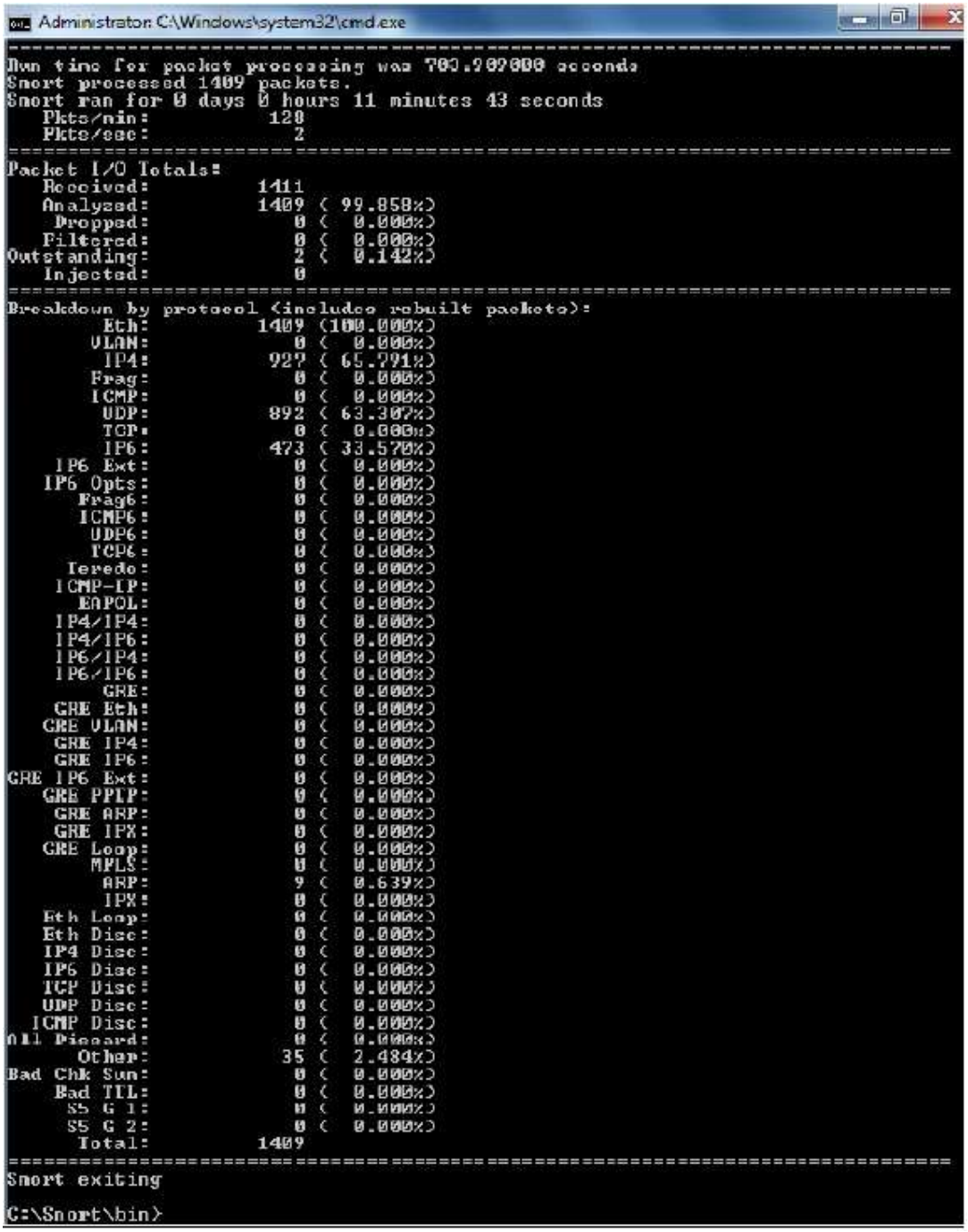
STEP-13: Click OK button and then close all dialog boxes. Open command prompt and type the following commands:

INSTALLATION PROCESS:




Environment Variables
User variables for Dad
Variable
Value
CLASSPATH
.;.;C:\PROGRA~1\JMF21~1.1\lib\soun...
TEMP
%USERPROFILE%\AppData\Local\Temp
TMP
%USERPROFILE%\AppData\Local\Temp
New...
Edit...
Delete
System variables
Variable
Value
CLASSPATH
.;c:\Program Files\Java\jre1.6.0\lib\ext...
ComSpec
C:\Windows\system32\cmd.exe
FP_NO_HOST_C...
NO
NUMBER_OF_P...
4
New...
Edit...
Delete
OK
Cancel


Administrator: C:\Windows\system32\cmd.exe - snort -v
UDP TTL:128 TOS:0x0 ID:903 IpLen:20 DgmLen:78
Len: 50
03/20-12:13:57.248341 192.168.56.101:63650 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:904 IpLen:20 DgmLen:50
Len: 22
03/20-12:13:57.348568 192.168.56.101:63650 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:905 IpLen:20 DgmLen:50
Len: 22
03/20-12:13:57.548888 192.168.56.101:137 -> 192.168.56.255:137
UDP TTL:128 TOS:0x0 ID:906 IpLen:20 DgmLen:78
Len: 50
03/20-12:13:58.298907 192.168.56.101:137 -> 192.168.56.255:137
UDP TTL:128 TOS:0x0 ID:907 IpLen:20 DgmLen:78
Len: 50



RESULT:

Thus the demonstration of the instruction detection using Snort tool was done successfully.

Experiment 15

Experiment: Perform an experiment with implementation of defeating Malware - building Tojans.

Aim: To build a Trojan and know the harmness of the Trojan malwares in a computer System.

PROCEDURE:

1. Create a simple Trojan by using Windows Batch File (***.bat***)
2. Type these below code in notepad and save it as **Trojan.bat**
3. Double click on ***Trojan.bat*** file.
4. When the Trojan code executes, it will open MS-Paint, Notepad, Command Prompt,Explorer, etc., infinitely.
5. Restart the computer to stop the execution of this Trojan.

Trojan

- In computing, a Trojan horse,or Trojan, is any malware which misleads users of itstrue intent.
- Trojans are generally spread by some form of social engineering, for example where auser is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.
- Although their payload can be anything, many modern forms act as a backdoor,contacting a controller which can then have unauthorized access to the affected computer.
- Trojans may allow an attacker to access users' personal information such as bankinginformation, passwords, or personal identity.
- ***Example:*** *Ransomware* attacks are often carried out using a *trojan*

CODE:

Trojan.bat

```
@echo off
:x
start mspaint
start notepad
start cmd
start explorer
start control
start calc
goto x
```

OUTPUT:

(MS-Paint, Notepad, Command Prompt, Explorer will open infinitely)