

Geetanjali Institute of Technical Studies

(Approved by AICTE, New Delhi and Affiliated to Rajasthan Technical University Kota (Raj.))

DABOK, UDAIPUR, RAJASTHAN 313022

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

B. Tech - VII SEMESTER



ACADEMIC YEAR – 2022-23

CYBER SECURITY LAB

7CS4-22

**Submitted to:
Ms. Ayushi Ghill
Assistant Professor, CSE
GITS**

**Submitted by:

Roll Number:**

INDEX – LAB MANUAL

S. No.	CONTENT / ITEM NO.	PAGE NO.
1.	Vision and Mission of The Institute	3
2.	Vision and Mission of The Department	3
3.	Program Educational Objective of Department (PEO's)	3
4.	Program Outcomes of Department (PO's)	5
5.	Course Outcome (COs)	6
6.	COs mapping with Pos and PSOs	6
7.	Course Syllabus	7
8.	Prescribed Books	7
9.	List of Experiment	8
10.	Practical's Beyond RTU Syllabus	8
11.	Experiment No.1	9
12.	Experiment No.2	12
13.	Experiment No.3	14
14.	Experiment No.4	16
15.	Experiment No.5	26
16.	Experiment No.6	29
17.	Experiment No.7	33
18.	Experiment No.8	37
19.	Outcome of Lab	47
20.	Computer Lab's Do's and Don'ts and Safety Rules	48

VISSION & MISSION OF INSTITUTE

INSTITUTE VISION

TO ACHIEVE EXCELLENCE IN TECHNICAL AND MANAGEMENT EDUCATION THROUGH QUALITY TEACHING AND INNOVATION.

INSTITUTE MISSION

M1:To provide an excellent learning environment to produce socially responsible and productive technical professionals.

M2:To set up the state-of-the-art facilities for quality education and innovation.

M3:To impart knowledge & Skills leading to shaping a budding manager as a quality executive.

M4:To encourage for life-long learning and team-based problem solving through learning environment.

VISION & MISSION OF DEPARTMENT

VISION

To nurture the students to become employable graduates who can provide solutions to the societal issues through ICT.

MISSION

M1:To focus on practical approach towards learning and exposing the students on the latest ICT technologies.

M2:To foster logical thinking among the students to solve real-time problems using innovative approaches.

M3:To provide state-of-the-art resources that contributes to inculcate ethical and life-long learning environment.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

The Programme Educational Objectives of the programme offered by the department are listed below:

PEO1: To enable the students to think out-of-the-box solutions for addressing societal issues through ICT.

PEO2: To impart skills in students to analyze, design and implement Software/Hardware solutions to solve interdisciplinary and complex problems.

PEO3: To expose the students towards effective dissemination of research findings in order to become successful entrepreneurs or to pursue higher education.

PROGRAM SPECIFIC OUTCOMES (PSO's)

- **PSO1: Professional Skills:** The ability to understand, analyze and develop electronic systems in the areas related to hardware and software development, communication systems and networking for efficient design of electronic-based systems of varying complexity.
- **PSO2: Problem-Solving Skills:** The ability to apply standard practices and strategies in electronic system project development on both hardware and software environments to deliver a quality product for business success.
- **PSO3: Successful Career and Entrepreneurship:** The ability to employ modern electronic solutions on different platforms, in creating innovative career paths to be an entrepreneur, and a zest for higher studies.

PROGRAMME OUTCOMES (POs)

A student will develop:

1. **ENGINEERING KNOWLEDGE:** An ability to apply knowledge of Mathematics, Science and Engineering Fundamentals in Electronics and Communication Engineering.
2. **PROBLEM ANALYSIS:** An ability to analyze and interpret data by designing and conducting experiments. Develop the knowledge of developing algorithms, designing, implementation and testing applications in electronics and communication related areas.
3. **DESIGN/ DEVELOPMENT OF SOLUTION:** An ability to Design a system Component or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability.
4. **CONDUCTION OF INVESTIGATION OF COMPLEX PROBLEMS:** An ability to Identify, formulate and solve engineering problems.
5. **MODERN TOOL USAGE:** An ability to use the techniques, skills and modern engineering tools necessary for engineering practice.
6. **THE ENGINEERING AND SOCIETY:** Broad education necessary to understand the impact of engineering solutions in a global, economic, environmental and societal context.
7. **ENVIRONMENT & SUSTAINABILITY:** Understand the impact of professional engineering solution in societal and environmental contexts, and demonstrate the knowledge of, and need of sustainable development.
8. **ETHICS:** An ability to understand the professional, social and ethical responsibility.
9. **INDIVIDUAL AND TEAM WORK:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **COMMUNICATION:** An ability to Communicate effectively in order to succeed in their profession such as, being able to write effective reports and design documentation, make effective presentations.
11. **PROJECT MANAGEMENT & FINANCE:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in team, to manage projects and in multidisciplinary environment.
12. **LIFE-LONG LEARNING:** Recognize the need and an ability to engage in life-long learning.

COURSE OUTCOMES (COs)

CO1	Students will be able to solve and relate mathematic concepts behind the cryptographic algorithms.
CO2	Students will be able to explain basic operations of cryptographic algorithms.
CO3	Students will be able to describe various private and public key security algorithms used for network security along with its encryption and decryption.
CO4	Students will be able to evaluate various scenarios and apply the required type of algorithm for ensuring security.
CO5	Students will be able analyze protocols for various security objectives with cryptographic tools.

COs MAPPING WITH POs AND PSOs

Course Outcome	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	2	2	1	1	0	0	0	0	0	0	1	2	1	1
CO2	2	3	3	2	2	0	0	0	0	0	0	1	3	2	2
CO3	1	1	2	2	1	0	0	0	0	0	0	1	2	1	1
CO4	1	1	2	1	0	0	0	0	0	0	0	1	1	2	2
CO5	2	1	2	2	2	0	0	0	0	0	0	1	2	1	1

COURSE SYLLABUS



RAJASTHAN TECHNICAL UNIVERSITY, KOTA

Scheme & Syllabus

IV Year- VII Semester: B. Tech. (Computer Science & Engineering)

7CS4-22: Cyber Security Lab

Credit: 2

Max. Marks: 100(IA:60, ETE:40)

OL+OT+4P

End Term Exam: 2 Hours

SN	List of Experiments
1	Implement the following Substitution & Transposition Techniques concepts: a) Caesar Cipher b) Rail fence row & Column Transformation
2	Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).
3	Implement the following Attack: a) Dictionary Attack b) Brute Force Attack
4	Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TCP datagram.
5	Installation of rootkits and study about the variety of options.
6	Perform an Experiment to Sniff Traffic using ARP Poisoning.
7	Demonstrate intrusion detection system using any tool (snort or any other s/w).
8	Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures.
	<p>PROJECT:In a small area location such as a house, office or in a classroom, there is a small network called a Local Area Network (LAN). The project aims to transfer a file peer-to-peer from one computer to another computer in the same LAN. It provides the necessary authentication for file transferring in the network transmission. By implementing the Server-Client technology, use a File Transfer Protocol mechanism and through socket programming, the end user is able to send and receive the encrypted and decrypted file in the LAN. An additional aim of the project is to transfer a file between computers securely in LANs. Elements of security are needed in the project because securing the files is an important task, which ensures files are not captured or altered by anyone on the same network. Whenever you transmit files over a network, there is a good chance your data will be encrypted by encryption technique.</p> <p>Any algorithm like AES is used to encrypt the file that needs to transfer to another computer. The encrypted file is then sent to a receiver computer and will need to be decrypted before the user can open the file.</p>

TEXT / REFERENCE BOOKS

- The Network Security Test Lab: A Step-by-Step Guide, Wiley, Michael Gregg
- AtulKahate, Cryptography and Network Security, TMH Publication.

Scheme & Syllabus of 4th Year B. Tech. (CS) for students admitted in Session 2021-22

7CS4-22: Cyber Security Lab

Credit: 2

Max. Marks: 100 (IA: 60, ETE: 40) 0L+0T+4P

End Term Exam: 2 Hours

S.NO.	NAME OF EXPERIMENT	CO Mapped
1	Implement the following Substitution & Transposition Techniques concepts: a) Caesar Cipher b) Rail fence row & Column Transformation	CO2
2	Implement the Diffie-Hellman Key Exchange mechanism Consider the end user as one of the parties (Alice) and the other party (Bob).	CO3
3	Implement the following Attack: Brute Force Attack	CO1
4	Installation of Wire shark, tcpdump, etc and observe data transferred in client server communication using UDP/TCP and identify the UDP/TCP datagram.	CO2
5	Installation of rootkits and study about the variety of options.	CO5
6	Perform an Experiment to Sniff Traffic using ARP Poisoning.	CO4
7.	Demonstrate intrusion detection system using any tool (snort or any other s/w).	CO5
8.	Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures.	CO4

Prerequisites:

- Students are expected to have knowledge of Network and Cyber Security.
- Students are expected to have knowledge of C, Java Programming.

Software requirements:

- Turbo C/ Borland C++ 5.02 or Higher
- JDK Java

PRACTICALS BEYOND RTU SYLLABUS

Not Applicable

EXPERIMENT NO. 1

AIM: Implement the following Substitution & Transposition Techniques concepts:

- a) Caesar Cipher
- b) Rail fence row & Column Transformation

PROGRAM: (a)

```
#include<stdio.h>
int main()
{
    char msg[100], ch;
    int i,key;
    printf("Enter an Encrypted text:");
    gets(msg);
    printf("Enter key:");
    scanf("%d",&key);
    for(i=0; msg[i]!='\0'; i++)
    {
        ch=msg[i];
        if(ch>='a'&&ch<='z')
        {
            ch=ch-key;
            if(ch<'a')
            {
                ch=ch+'z'-'a'+1;
            }
            msg[i]=ch;
        }
        else if(ch>='A'&& ch<='Z')
        {
            ch=ch+key;
            if(ch>'Z')
            {
                ch=ch+'Z'-'A'+1;
            }
            msg[i]=ch;
        }
    }
    printf("Decrypted message: %s", msg);
    return 0;
}
```

CODE OUTPUT: (a)

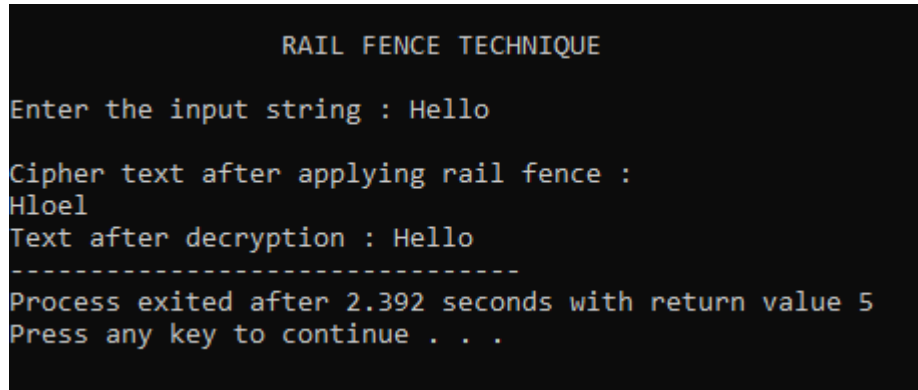
```
Enter an Encrypted text:Hello how are you
Enter key:3
Decrypted message: Kbiil elt xob vlr
-----
Process exited after 13.04 seconds with return value 0
Press any key to continue . . .
```

PROGRAM: (b)

```
#include<stdio.h>
#include<string.h>
void main()
{
    int i,j,k,l;
    char a[20],c[20],d[20];
    printf("\n\t\t RAIL FENCE TECHNIQUE");
    printf("\n\nEnter the input string : ");
    gets(a);
    l=strlen(a);
    /*CIPHERING*/
    for(i=0, j=0;i<l; i++)
    {
        if(i%2==0)
            c[j++]=a[i];
    }
    for(i=0;i<l;i++)
    {
        if(i%2==1)
            c[j++]=a[i];
    }
    c[j]='\0';
    printf("\nCIPHER text after applying rail fence :");
    printf("\n%s",c);
    /*DECIPHERING*/
    if(l%2==0)
        k=l/2;
    else
        k=(l/2)+1;
    for(i=0,j=0;i<k;i++)
    {
        d[j]=c[i];
        j=j+2;
    }
    for(i=k,j=1;i<l;i++)
    {
        d[j]=c[i];
```

```
        j=j+2;
    }
    d[l]='\0';
    printf("\nText after decryption : ");
    printf("%s",d);
}
```

CODE OUTPUT: (b)



```
RAIL FENCE TECHNIQUE

Enter the input string : Hello

Cipher text after applying rail fence :
Hloel
Text after decryption : Hello
-----
Process exited after 2.392 seconds with return value 5
Press any key to continue . . .
```

EXPERIMENT NO. 2

AIM: Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).

PROGRAM:

```
#include<stdio.h>
#include<conio.h>
long long int power(int a, int b, int mod)
{
    long long int t;
    if(b==1)
        return a;
    t=power(a,b/2,mod);
    if(b%2==0)
        return (t*t)%mod;
    else
        return (((t*t)%mod)*a)%mod;
}
long int calculateKey(int a, int x, int n)
{
    return power(a,x,n);
}
void main()
{
    int n,g,x,a,y,b;
    printf("Enter the value of n and g : ");
    scanf("%d%d",&n,&g);
    printf("Enter the value of x for the first person : ");
    scanf("%d",&x);
    a=power(g,x,n);
    printf("Enter the value of y for the second person : ");
    scanf("%d",&y);
    b=power(g,y,n);
    printf("key for the first person is :%lld\n",power(b,x,n));
    printf("key for the second person is :%lld\n",power(a,y,n));
    getch();
}
```

CODE OUTPUT:

```
Enter the value of n and g : 23
9
Enter the value of x for the first person : 4
Enter the value of y for the second person : 3
key for the first person is :9
key for the second person is :9
```

EXPERIMENT NO. 3

AIM: Implement the following Attack: Brute Force Attack

PROGRAM:

```
#include <stdio.h>
#include <string.h>
#define MAX 100

/* try to find the given pattern in the search string */
int bruteForce(char *search, char *pattern, int slen, int plen) {
    int i, j, k;

    for (i = 0; i <= slen - plen; i++) {
        for (j = 0, k = i; (search[k] == pattern[j]) && (j < plen); j++, k++);
        if (j == plen)
            return j;
    }
    return -1;
}

int main()
{
    char searchStr[MAX], pattern[MAX];
    int res;
    printf("Enter Search String:");
    fgets(searchStr, MAX, stdin);
    printf("Enter Pattern String:");
    fgets(pattern, MAX, stdin);
    searchStr[strlen(searchStr) - 1] = '\0';
    pattern[strlen(pattern) - 1] = '\0';
    res = bruteForce(searchStr, pattern, strlen(searchStr), strlen(pattern));
    if (res == -1)
    {
        printf("Search pattern is not available\n");
    }
    else
    {
        printf("Search pattern available at the location %d\n", res);
    }
    return 0;
}
```

CODE OUTPUT:

```
Enter Search String:Hello
Enter Pattern String:e
Search pattern available at the location 1

-----
Process exited after 3.245 seconds with return value 0
Press any key to continue . . .
```

EXPERIMENT NO. 4

AIM: Installation of Wire shark, tcpdump,

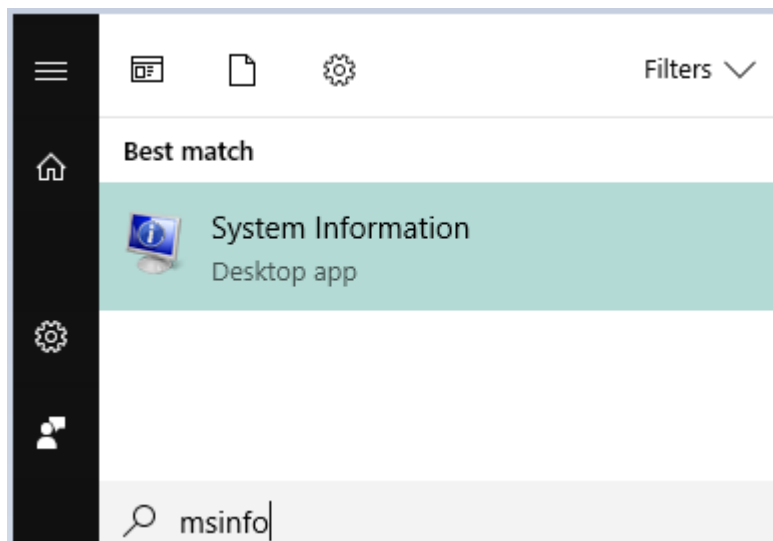
PROGRAM:

Wireshark is an invaluable packet analyzer used for network troubleshooting and analysis. This tutorial will show you how to download and install Wireshark in a Windows 10 system.

Requirements:

Before installing Wireshark, Determine your system type by pressing the Windows button and typing 'msinfo'.

CODE OUTPUT:



The Windows system has two types which can be X86-based PC (32-bit system) or X64-based PC (64-bit system).

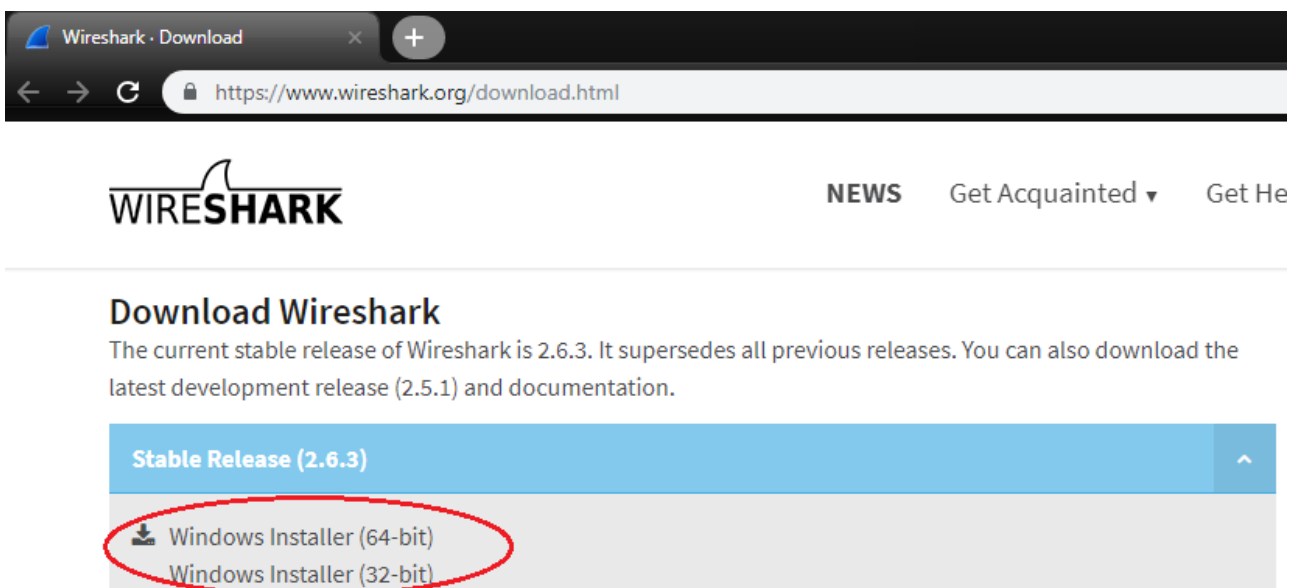
System Information	
File Edit View Help	
System Summary	
Hardware Resources	
Components	
Software Environment	
Item	Value
OS Name	Microsoft Windows 10 Home Single Language
Version	10.0.16299 Build 16299
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	
System Manufacturer	LENOVO
System Model	80Q7
System Type	x64-based PC
System SKU	
Processor	Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 2400 Mhz, 2 Core(s), 4 Logical Pr...
BIOS Version/Date	LENOVO D5CN43WW, 16/12/2015

Installing Wireshark on Windows 10

1. Select the Wireshark Windows Installer matching your system type, either 32-bit or 64-bit as determined.

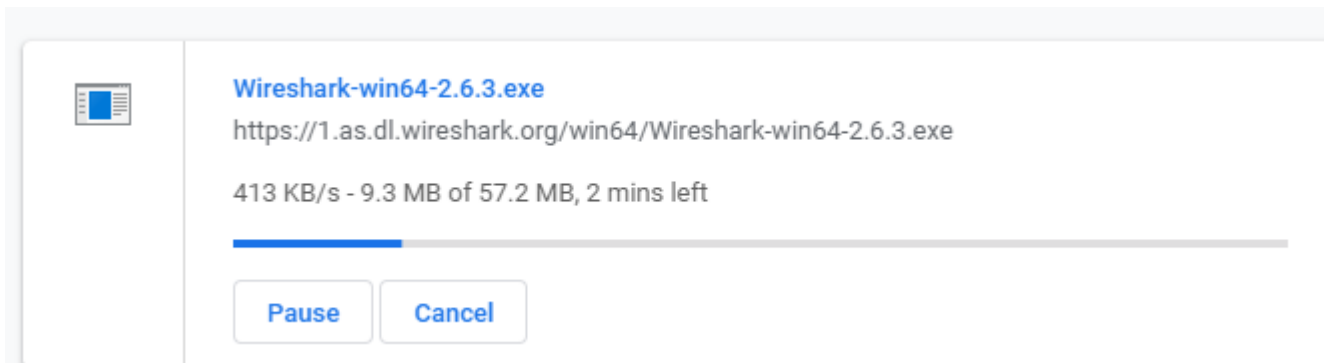
2. Download and install Wireshark

NOTE: If you are a beginner with using Wireshark, please select the stable release version.



The screenshot shows the Wireshark download page in a web browser. The URL is <https://www.wireshark.org/download.html>. The page features the Wireshark logo and navigation links like 'NEWS', 'Get Acquainted', and 'Get Help'. The main heading is 'Download Wireshark', followed by text stating the current stable release is 2.6.3. Below this, a blue bar highlights the 'Stable Release (2.6.3)' section. Underneath, two download links are listed: 'Windows Installer (64-bit)' and 'Windows Installer (32-bit)'. The '64-bit' link is circled in red, indicating it is the selected option.

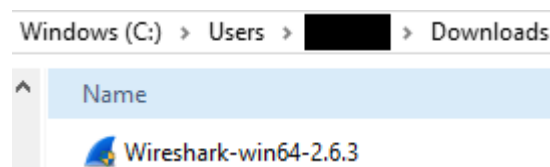
3. The download should start automatically once you selected the compatible Windows Installer for your Windows 10 platform.



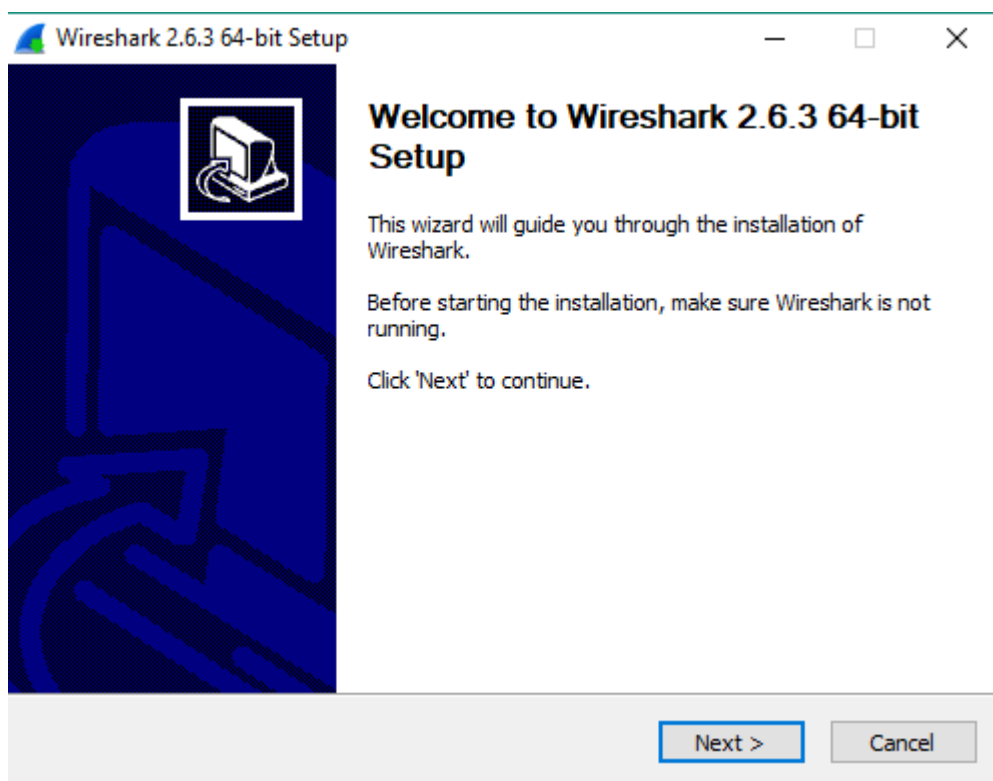
4. Save the program in the Downloads folder, then Close the web browser.

Install Wireshark

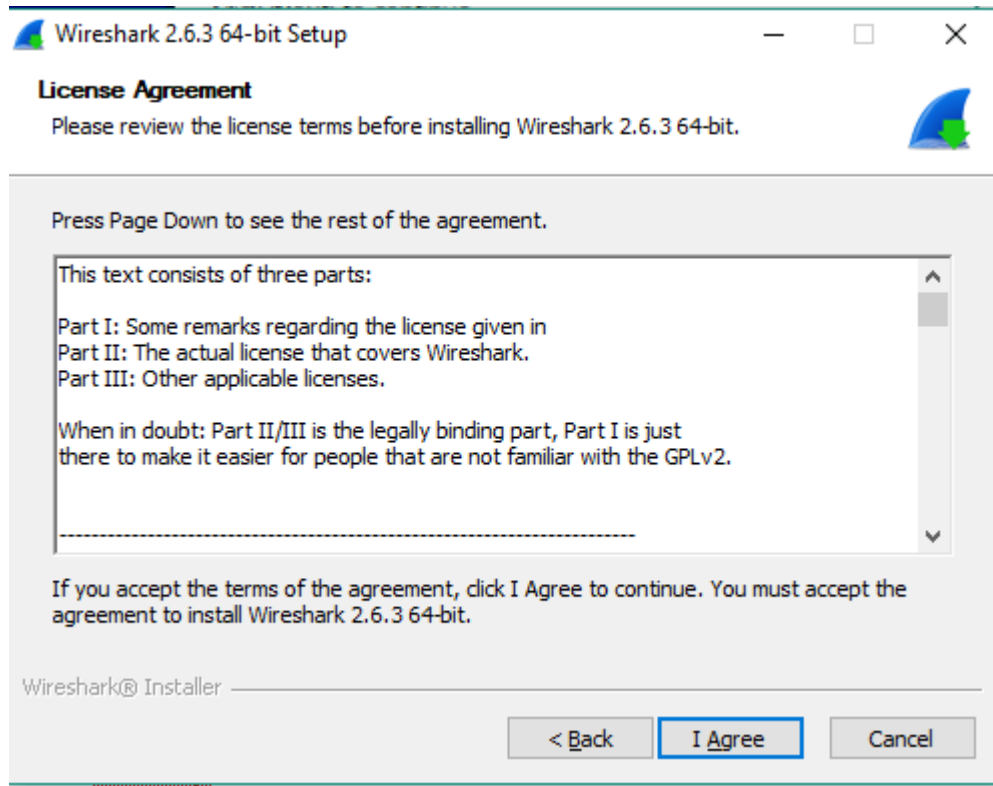
1. Open Windows Explorer.
2. Select the Downloads folder.



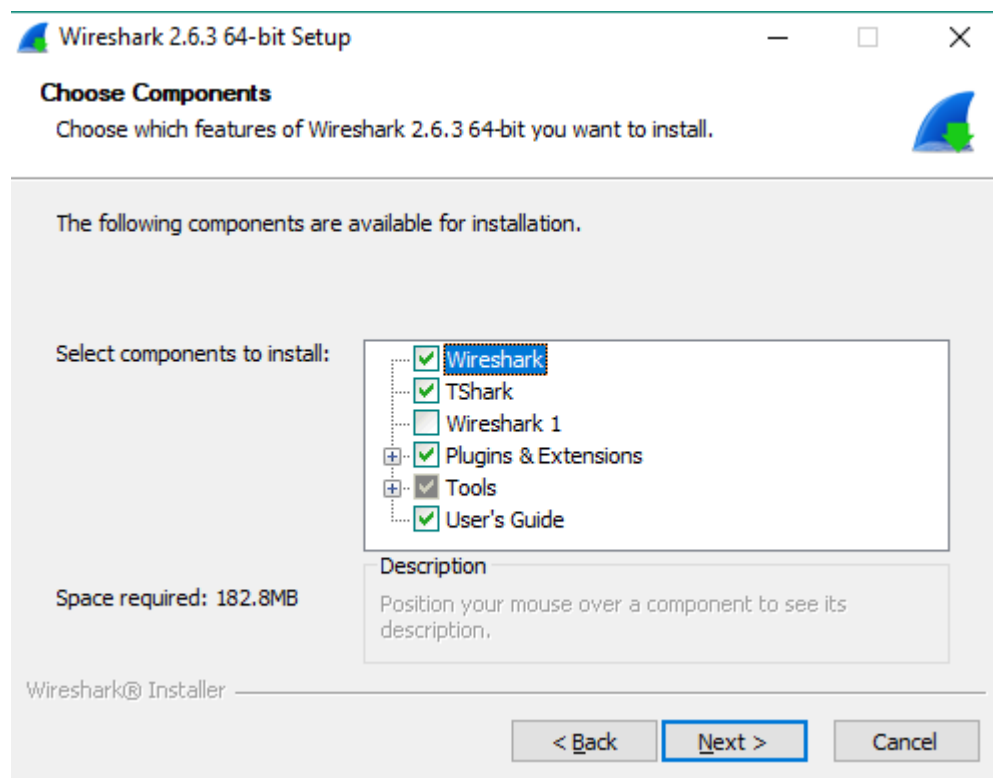
3. Locate the version of Wireshark you downloaded.
4. Double-click on the file to open it. If you see a User Account Control dialog box, select Yes to allow the program to make changes to this computer.
5. Select Next to start the Setup Wizard.



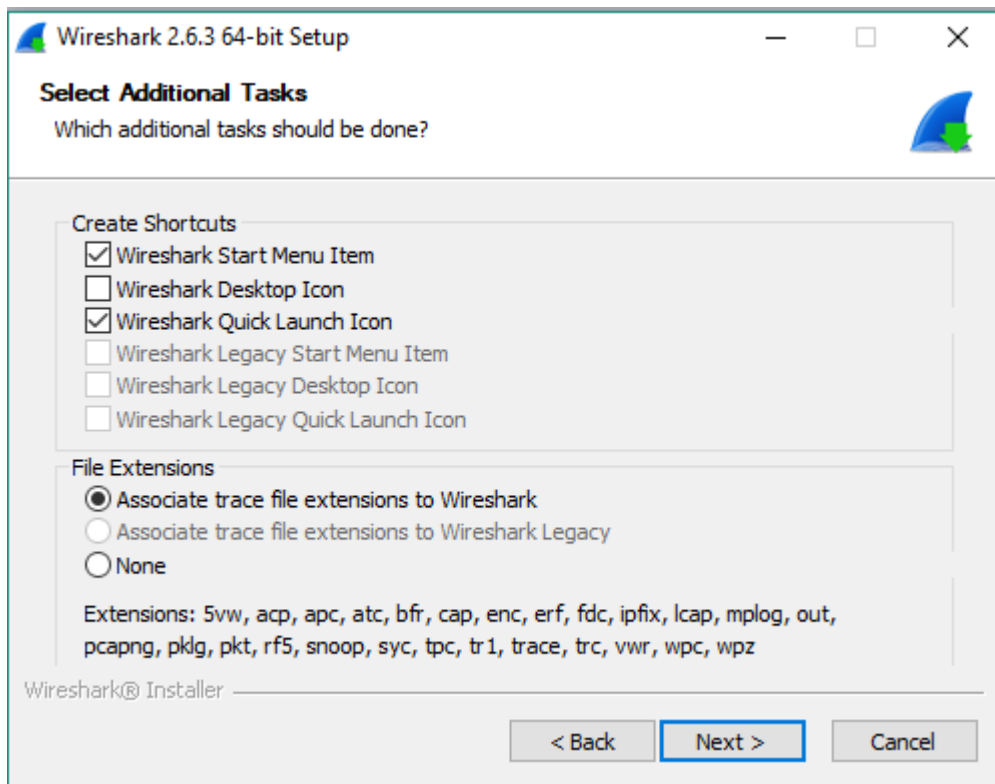
6. Review the license agreement. If you agree, select I Agree to continue.



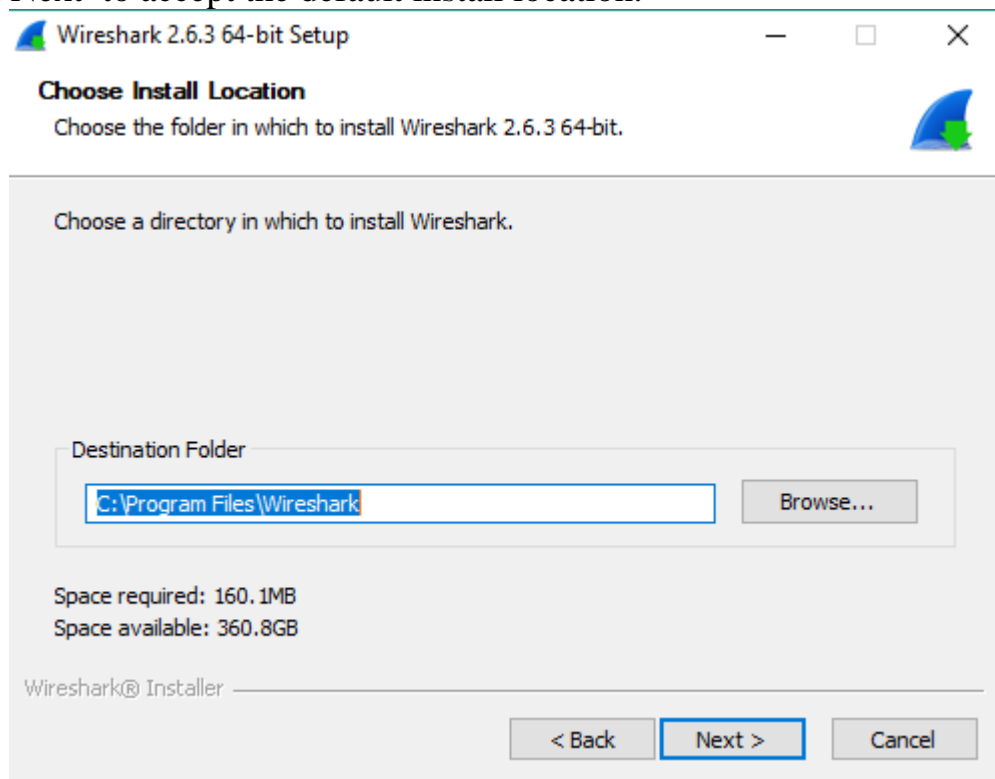
7. Select “Next” to accept the default components.



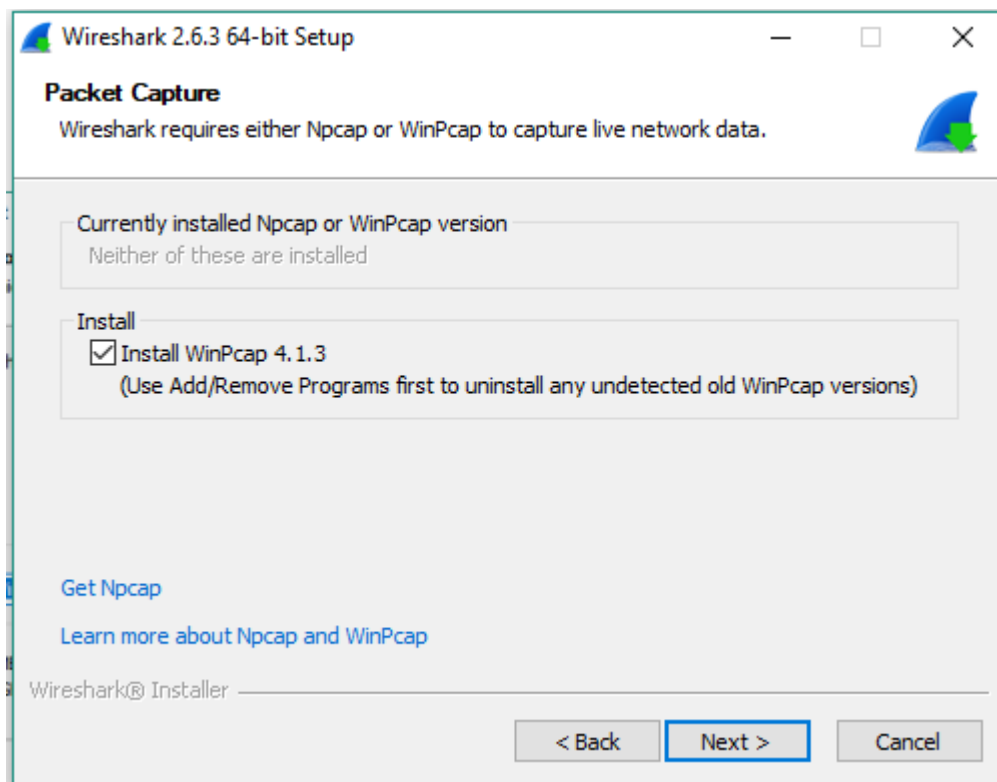
8. Select the shortcuts you would like to have created. Leave the file extensions selected. Select **Next** to continue.



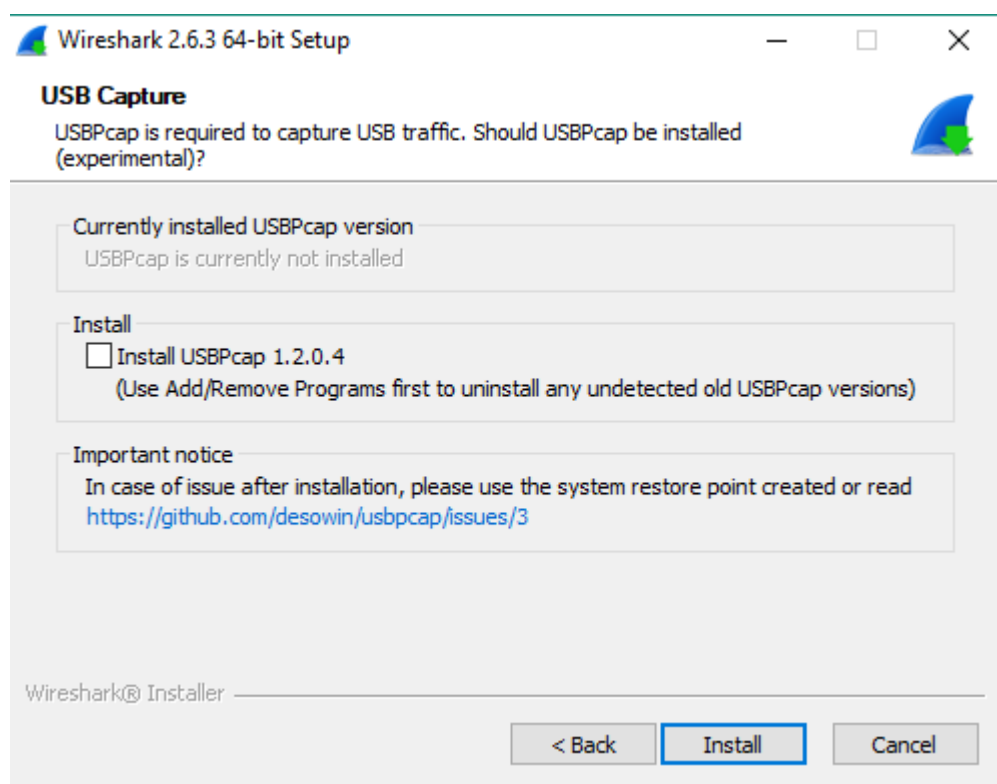
9. Select **Next** to accept the default install location.



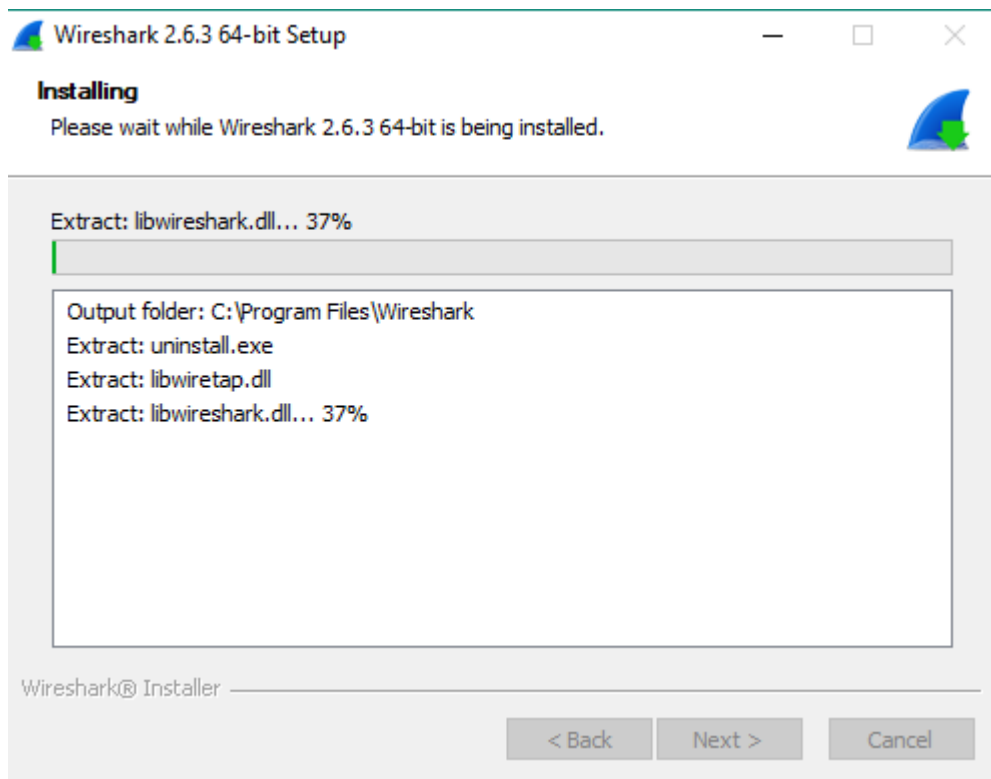
10. Select Next to install WinPcap.



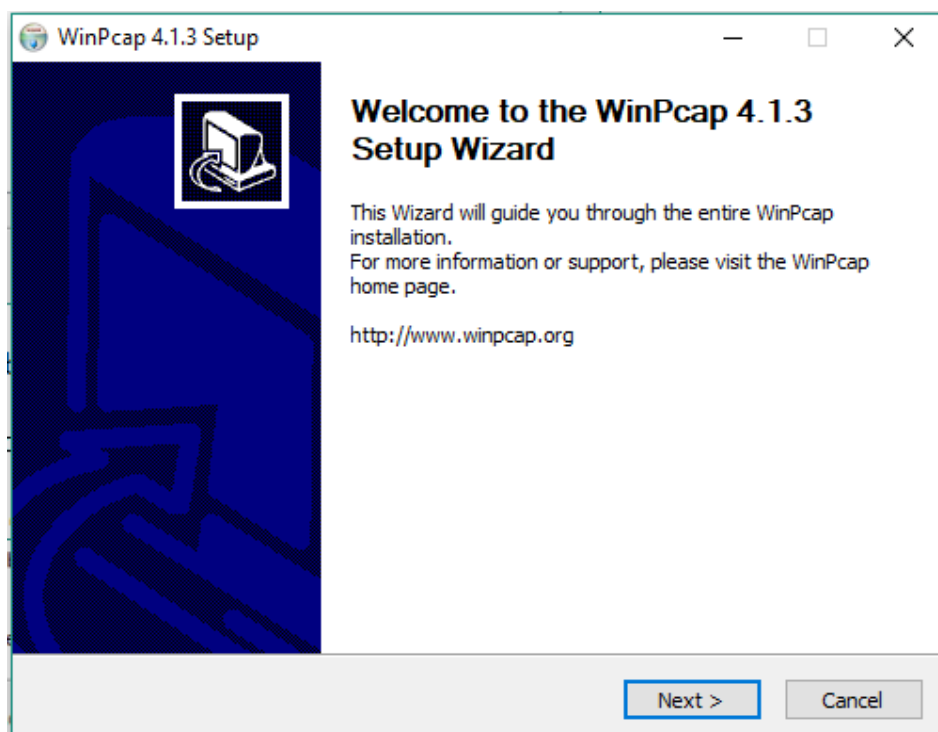
11. If you would like to capture USB traffic, install USBPcap as well.



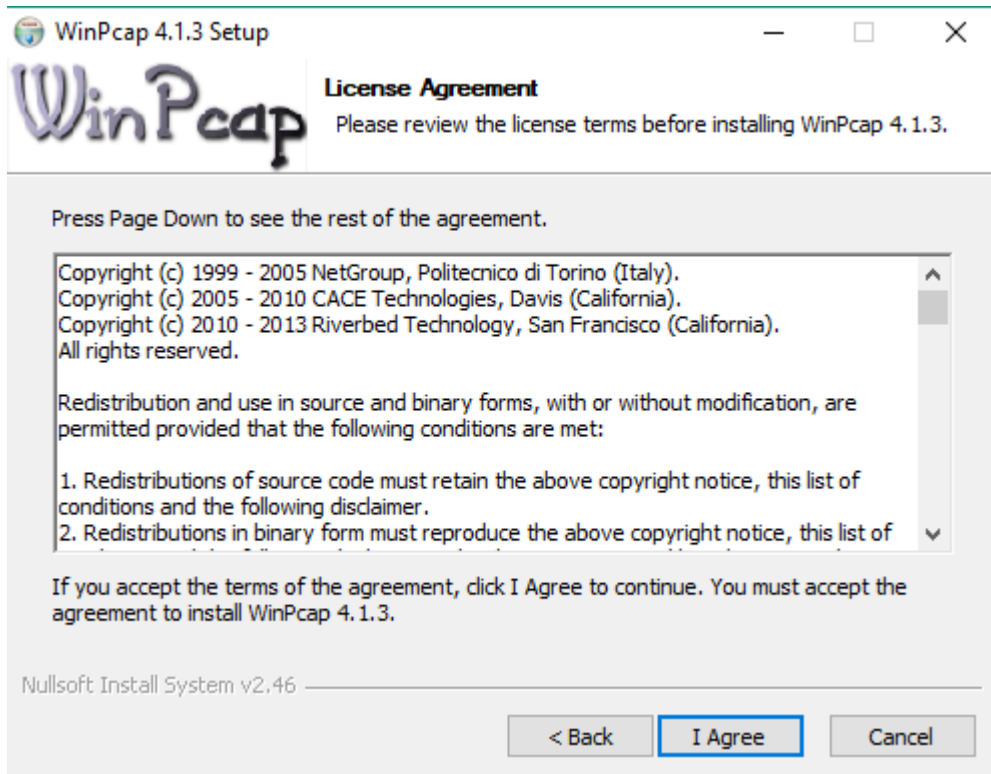
12. Select **Next** to start the Setup Wizard.



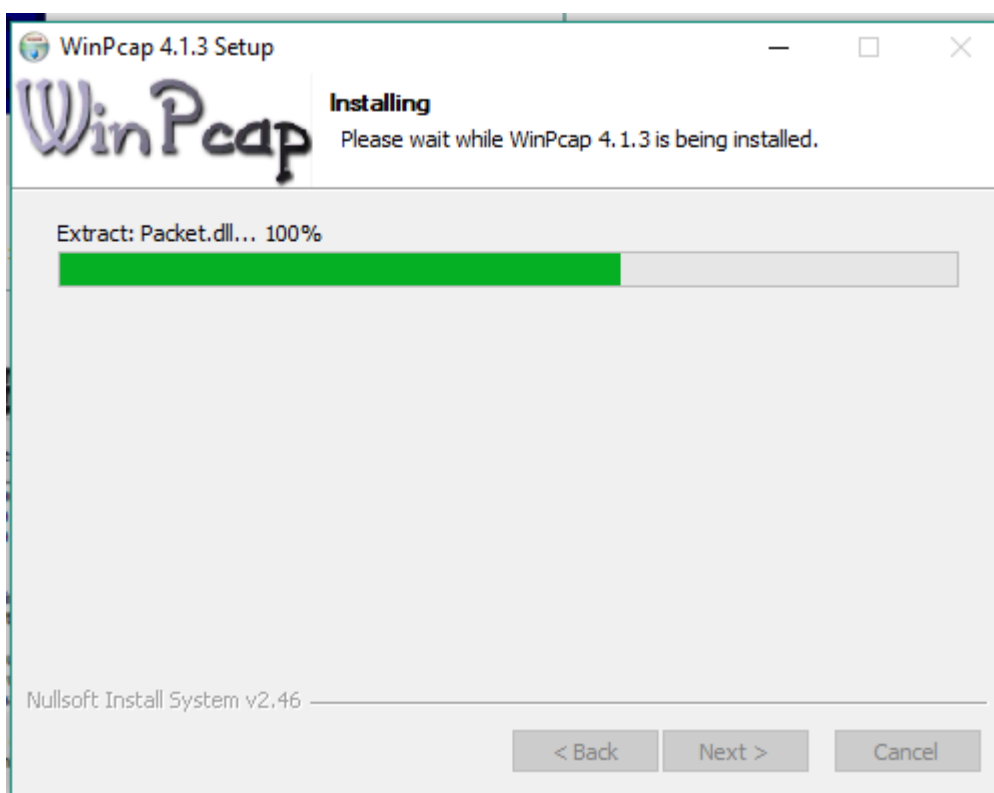
13. Select **Install** to proceed with the installation the requisite software WinPCap. Please note that WinPcap is a mandatory software to ensure Wireshark Packet Analyzer works properly.



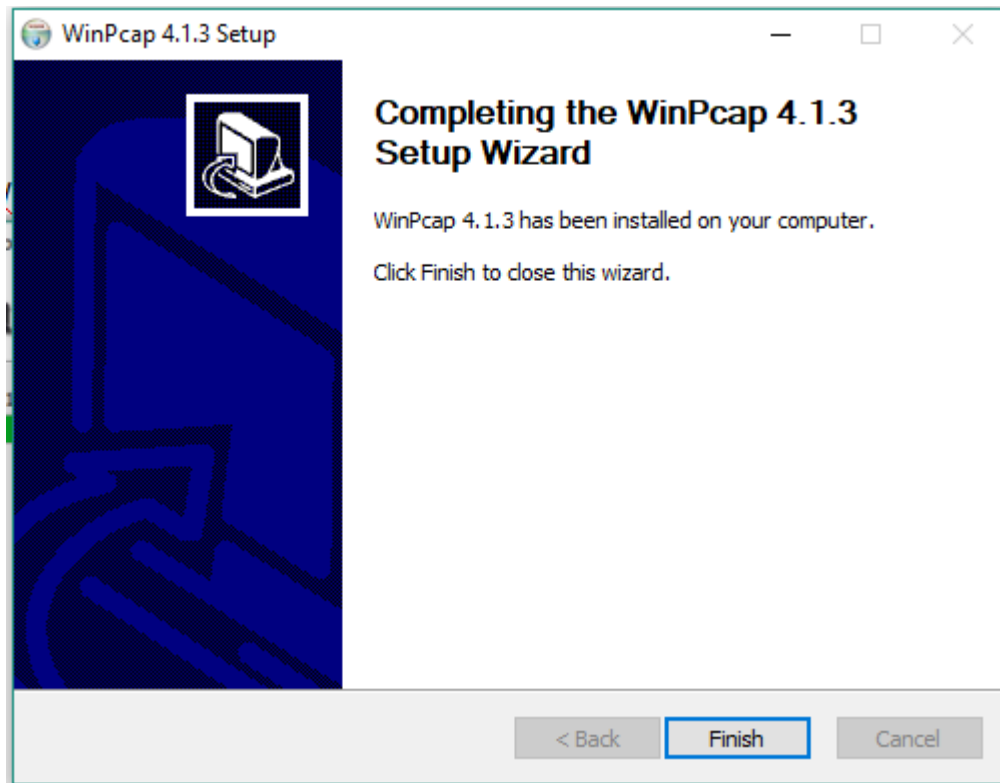
14. Review the license agreement. If you agree, select I Agree to continue.



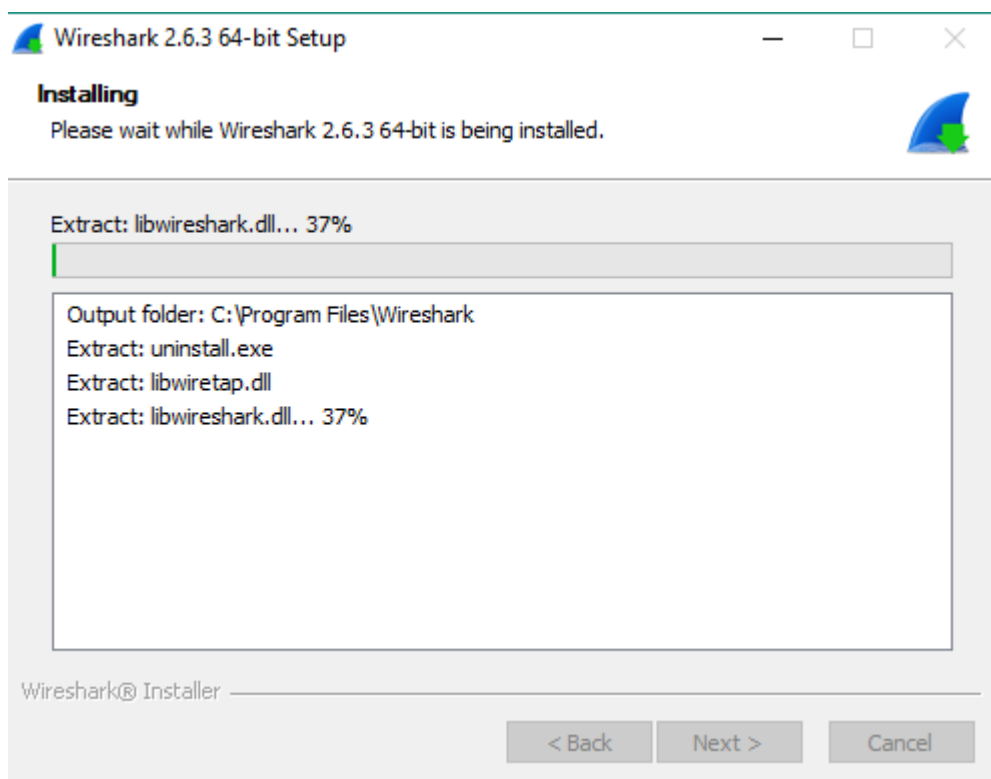
15. Installation of WinPcap should start automatically one you agreed and selected next.



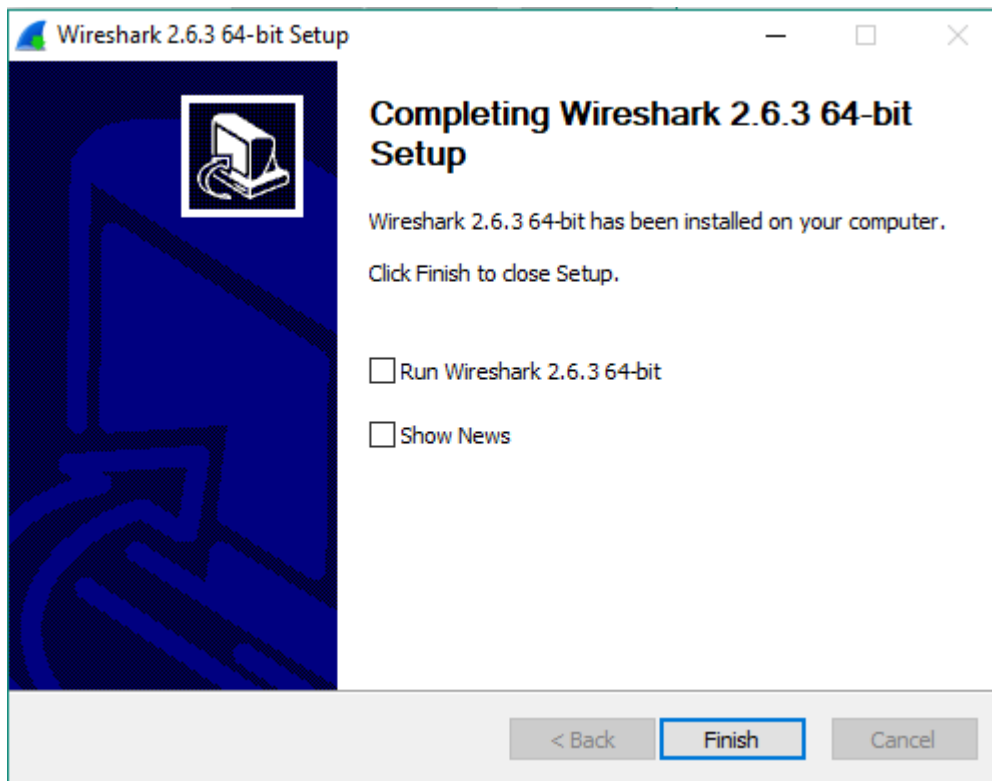
16. Select Finish to complete the installation of WinPcap.



17. Select Next to continue with the installation of Wireshark.



18. Select Finish to complete the installation of Wireshark. Once installed, you can open the Wireshark and start monitoring network traffic.



EXPERIMENT NO. 5

AIM: Installation of rootkits and study about the variety of options.

PROGRAM:

Breaking the term rootkit into the two component words, root and kit, is a useful way to define it. Root is a UNIX/Linux term that's the equivalent of Administrator 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, Auto start, 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.

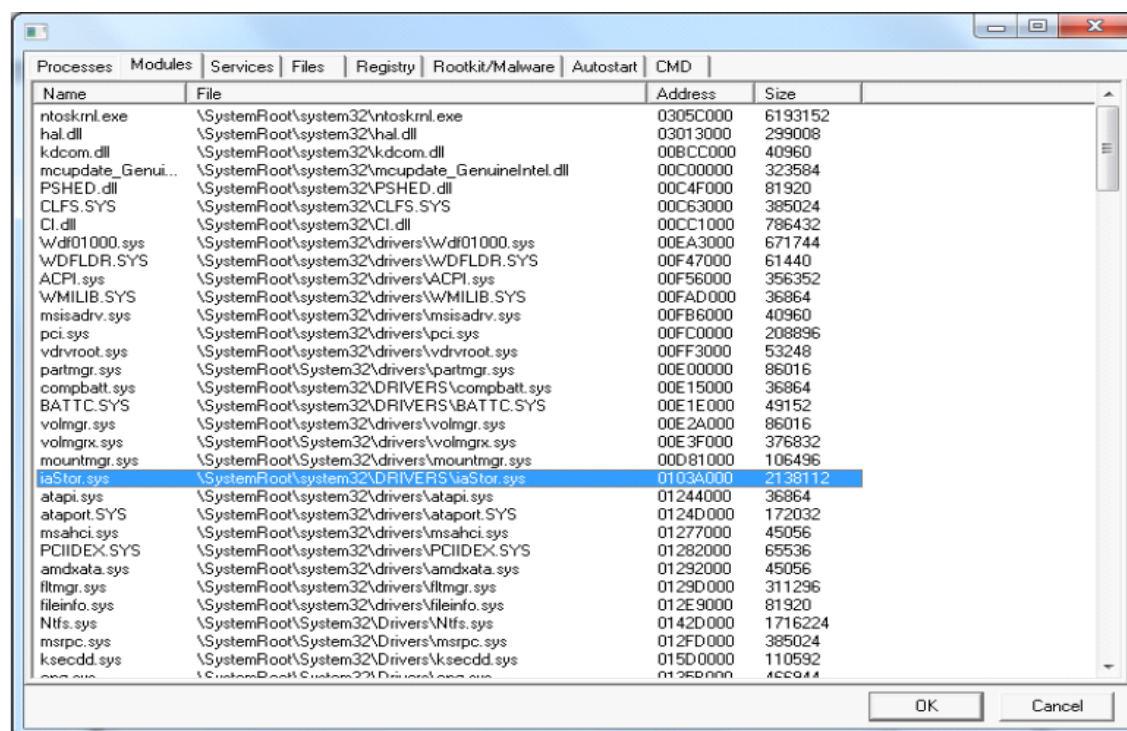
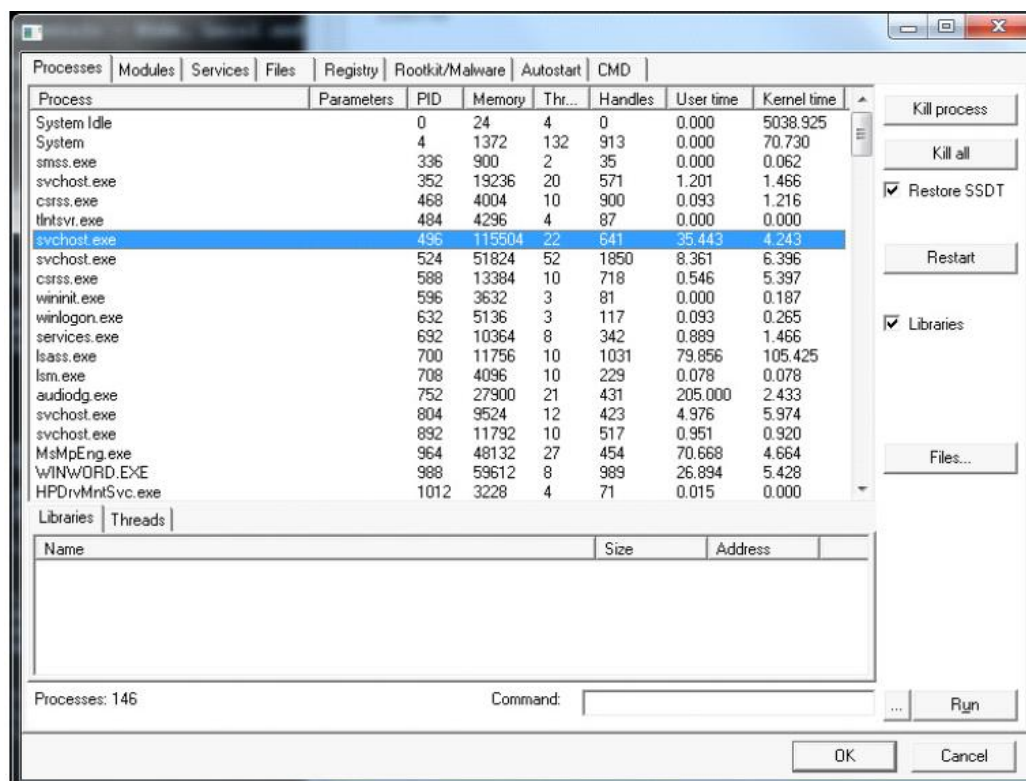
STEP-7: Registry displays Hkey_Current_user and Hkey_Local_Machine.

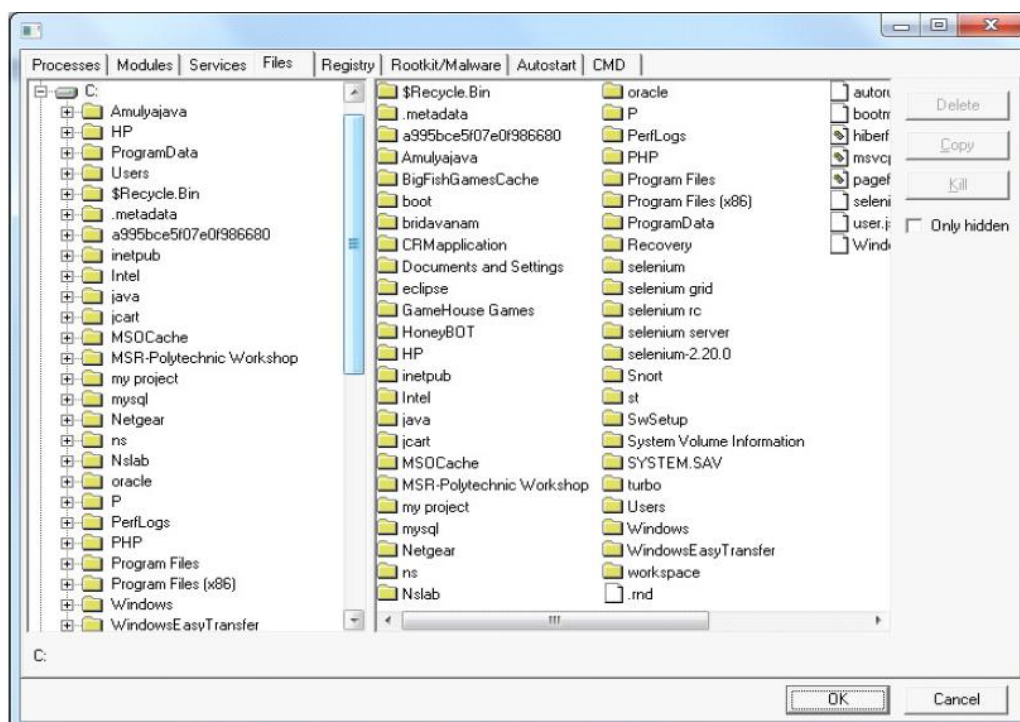
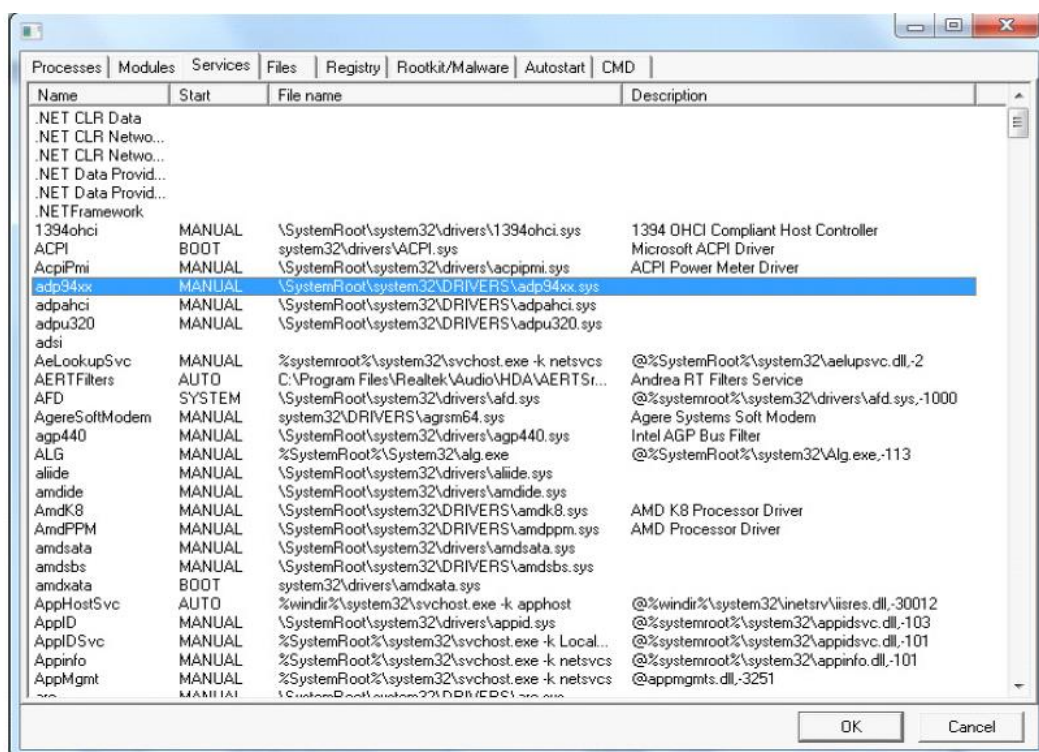
STEP-8: Rootkits / Malwares scans the local drives selected.

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

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

CODE OUTPUT:





EXPERIMENT NO. 6

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

PROGRAM:

We have used **Better CAP** to perform ARP poisoning in LAN environment using VMware workstation in which we have installed **Kali Linux** and **Ettercap** tool to sniff the local traffic in LAN.

For this exercise, you would need the following tools –

- VMware workstation
- Kali Linux or Linux Operating system
- Ettercap Tool
- LAN connection

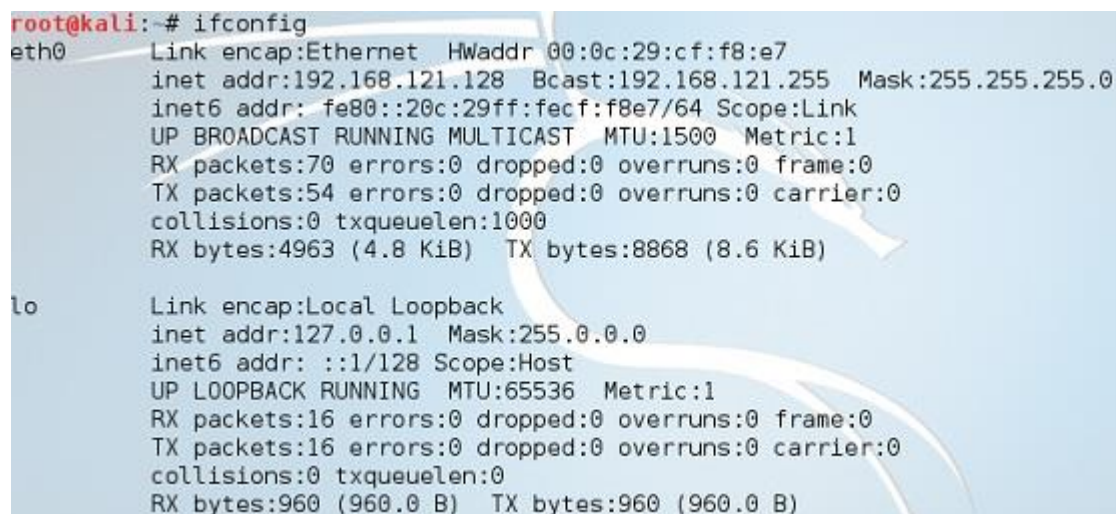
Note – This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

CODE OUTPUT:

Step 1 – Install the VMware workstation and install the Kali Linux operating system.

Step 2 – Login into the Kali Linux using username pass “root, toor”.

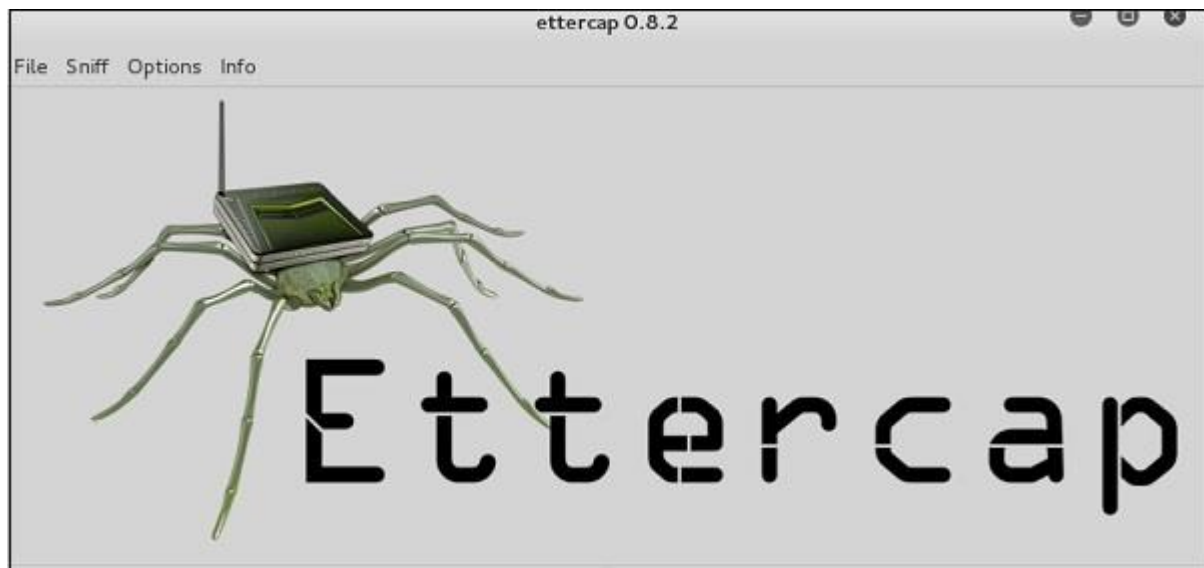
Step 3 – Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.



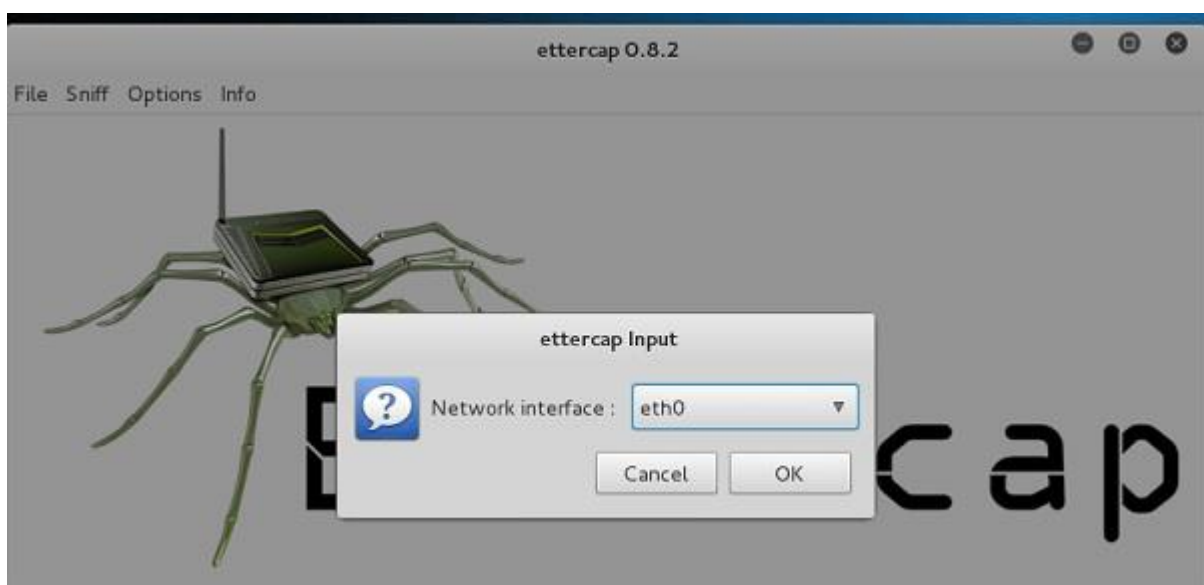
```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cf:f8:e7
          inet addr:192.168.121.128  Bcast:192.168.121.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecf:f8e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4963 (4.8 KiB)  TX bytes:8868 (8.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)
```

Step 4 – Open up the terminal and type “Ettercap –G” to start the graphical version of Ettercap.

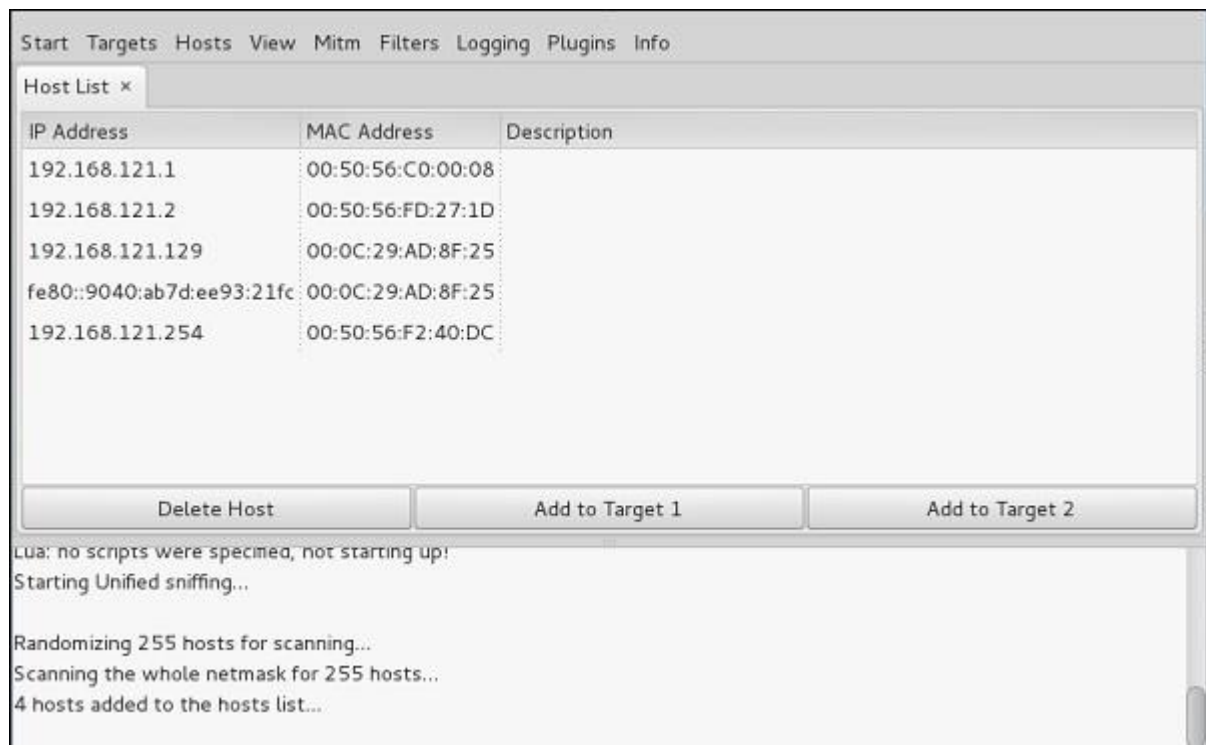


Step 5 – Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.



Step 6 – Now click the “hosts” tab in the menu bar and click “scan for hosts”. It will start scanning the whole network for the alive hosts.

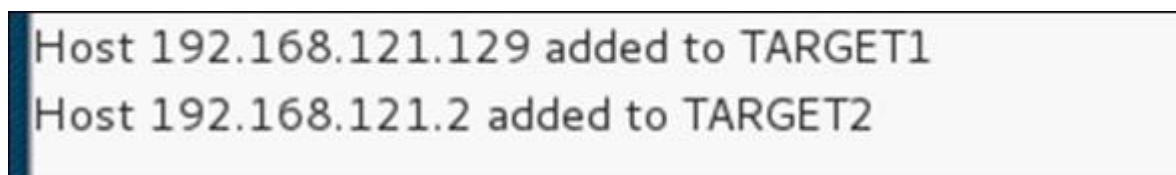
Step 7 – Next, click the “hosts” tab and select “hosts list” to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.



Step 8 – Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as “target 1” and the router address as “target 2.”

In VMware environment, the default gateway will always end with “2” because “1” is assigned to the physical machine.

Step 9 – In this scenario, our target is “192.168.121.129” and the router is “192.168.121.2”. So we will add target 1 as **victim IP** and target 2 as **router IP**.



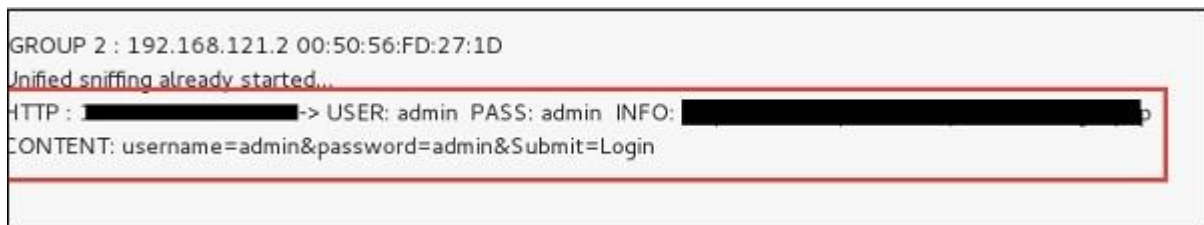
Step 10 – Now click on “MITM” and click “ARP poisoning”. Thereafter, check the option “Sniff remote connections” and click OK.



Step 11 – Click “start” and select “start sniffing”. This will start ARP poisoning in the network which means we have enabled our network card in “promiscuous mode” and now the local traffic can be sniffed.

Note – We have allowed only HTTP sniffing with Ettercap, so don’t expect HTTPS packets to be sniffed with this process.

Step 12 – Now it’s time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.



This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks.

Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

EXPERIMENT NO. 7

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

PROGRAM:

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:

- Signature-based intrusion detection systems
- 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 a pop-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.

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 -csnort.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.

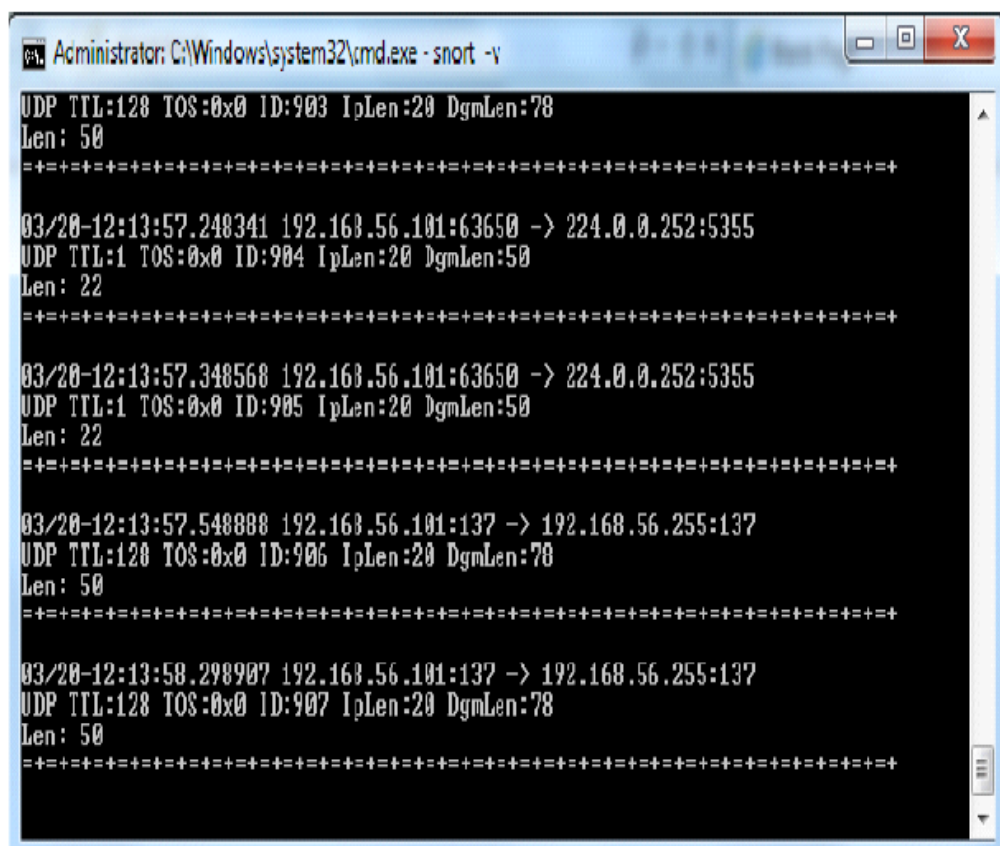
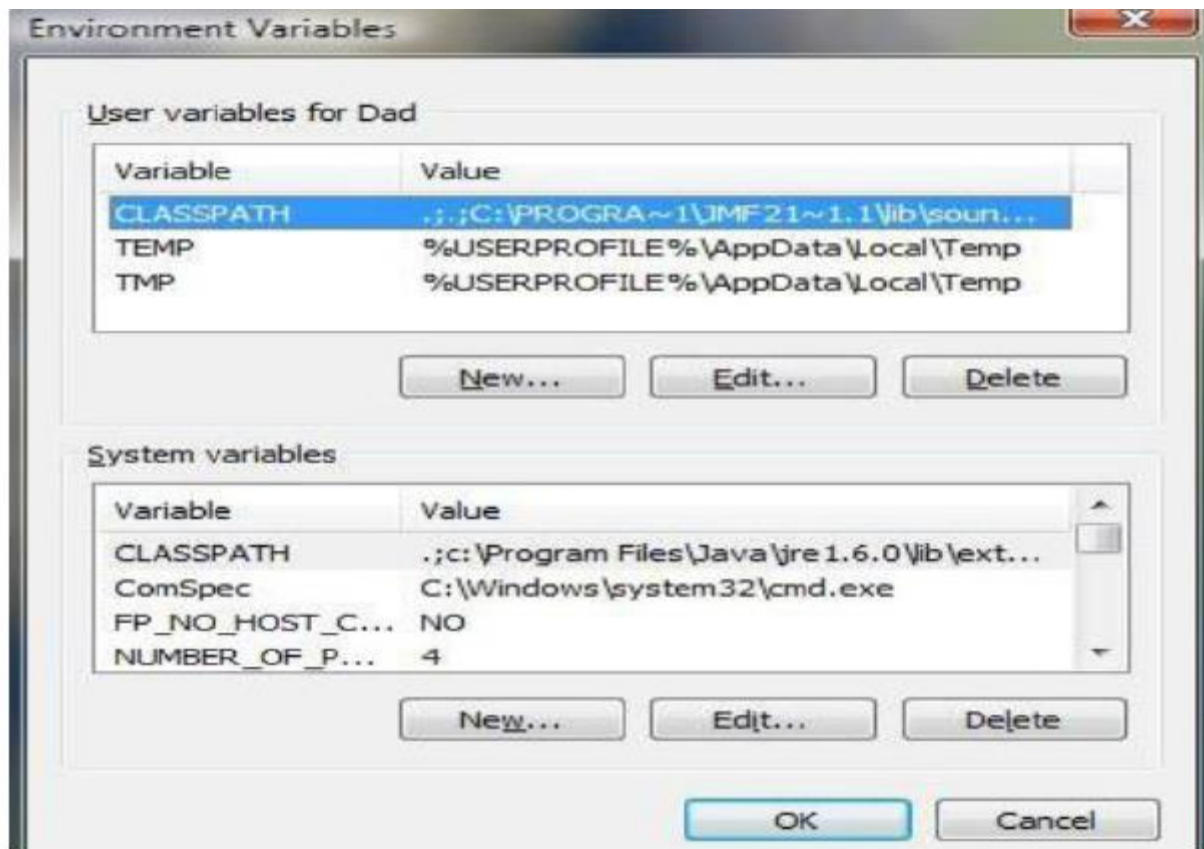
STEP-11: Add the path variable in windows environment variable by selecting new classpath.

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:

CODE OUTPUT:





```

Administrator: C:\Windows\system32\cmd.exe
-----
Run time for packet processing was 703.909000 seconds
Snort processed 1409 packets.
Snort ran for 0 days 0 hours 11 minutes 43 seconds
Pkts/min:      128
Pkts/sec:       2
-----
Packet I/O Totals:
Received:      1411
Analyzed:      1409 ( 99.858%)
Dropped:       0 ( 0.000%)
Filtered:      0 ( 0.000%)
Outstanding:   2 ( 0.142%)
Injected:      0
-----
Breakdown by protocol (includes rebuilt packets):
Eth:           1409 (100.000%)
  VLAN:        0 ( 0.000%)
  IP4:         927 ( 65.791%)
  Frag:        0 ( 0.000%)
  ICMP:        0 ( 0.000%)
  UDP:         892 ( 63.387%)
  TCP:         0 ( 0.000%)
  IP6:         473 ( 33.570%)
  IP6 Ext:     0 ( 0.000%)
  IP6 Opt:     0 ( 0.000%)
  Frag6:       0 ( 0.000%)
  ICMP6:       0 ( 0.000%)
  UDP6:        0 ( 0.000%)
  TCP6:        0 ( 0.000%)
  Teredo:      0 ( 0.000%)
  ICMP-IP:     0 ( 0.000%)
  FAPOL:       0 ( 0.000%)
  IP4/IP4:     0 ( 0.000%)
  IP4/IP6:     0 ( 0.000%)
  IP6/IP4:     0 ( 0.000%)
  IP6/IP6:     0 ( 0.000%)
  GRE:         0 ( 0.000%)
  GRE Eth:     0 ( 0.000%)
  GRE VLAN:    0 ( 0.000%)
  GRE IP4:     0 ( 0.000%)
  GRE IP6:     0 ( 0.000%)
  GRE IP6 Ext: 0 ( 0.000%)
  GRE PPIP:    0 ( 0.000%)
  GRE ARP:     0 ( 0.000%)
  GRE IPX:     0 ( 0.000%)
  GRE Loop:    0 ( 0.000%)
  MPLS:        0 ( 0.000%)
  ARP:         9 ( 0.639%)
  IPX:         0 ( 0.000%)
  Eth Loop:    0 ( 0.000%)
  Eth Disc:    0 ( 0.000%)
  IP4 Disc:    0 ( 0.000%)
  IP6 Disc:    0 ( 0.000%)
  IGP Disc:    0 ( 0.000%)
  UDP Disc:    0 ( 0.000%)
  ICMP Disc:   0 ( 0.000%)
  All Discard: 0 ( 0.000%)
  Other:       35 ( 2.484%)
Bad Chk Sum:   0 ( 0.000%)
Bad TTL:       0 ( 0.000%)
  S1 G 1:      0 ( 0.000%)
  S5 G 2:      0 ( 0.000%)
  Total:      1409
-----
Snort exiting
C:\Snort\bin>

```

EXPERIMENT NO. 8

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

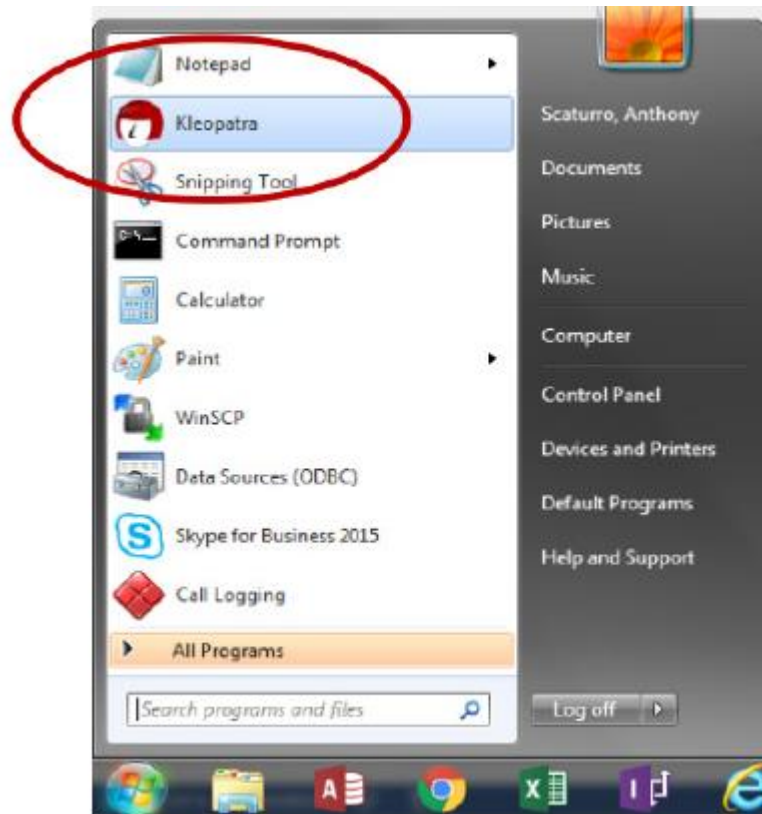
PROGRAM:

CREATING YOUR PUBLIC AND PRIVATE KEYS

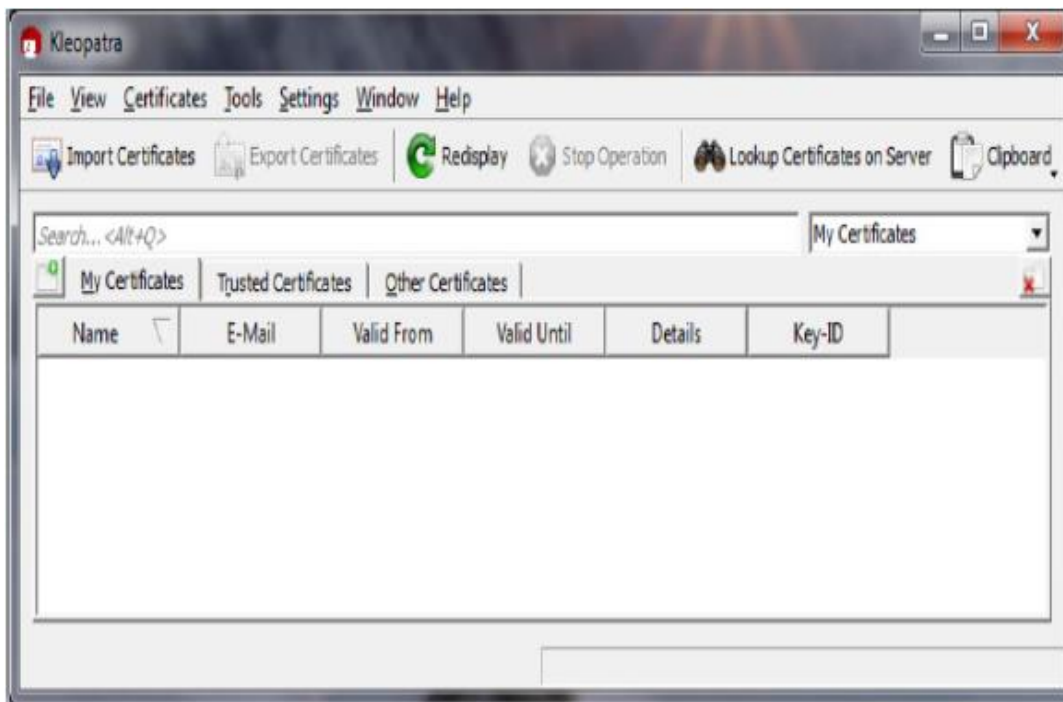
GPG encryption and decryption is based upon the keys of the person who will be receiving the encrypted file or message. Any individual who wants to send the person an encrypted file or message must possess the recipient's public key certificate to encrypt the message. The recipient must have the associated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

CODE OUTPUT:

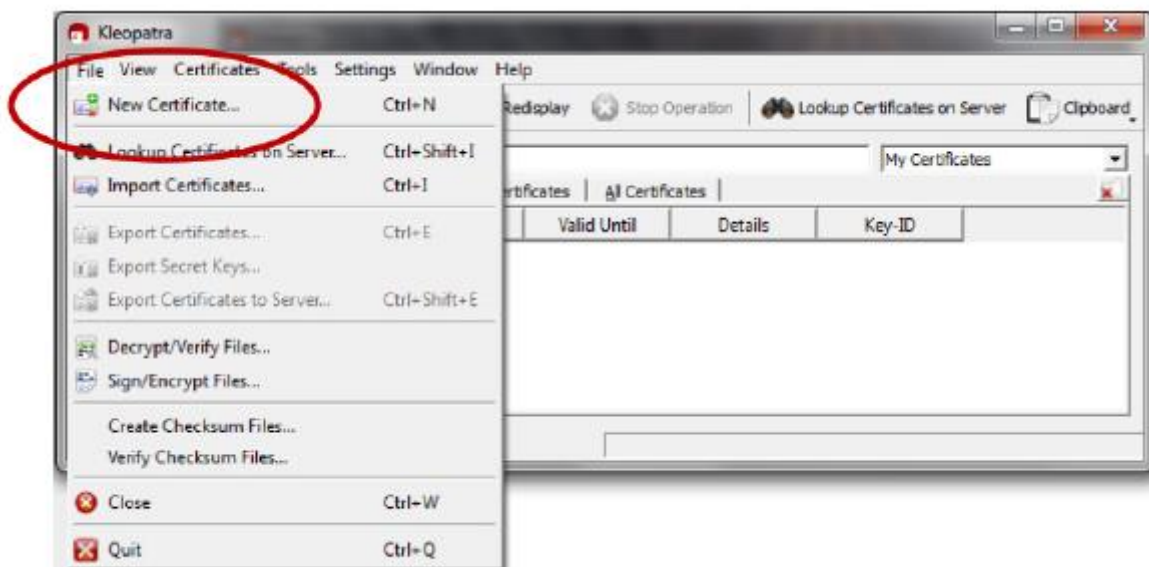
1. From your start bar, select the "Kleopatra" icon to start the Kleopatra certificate management software



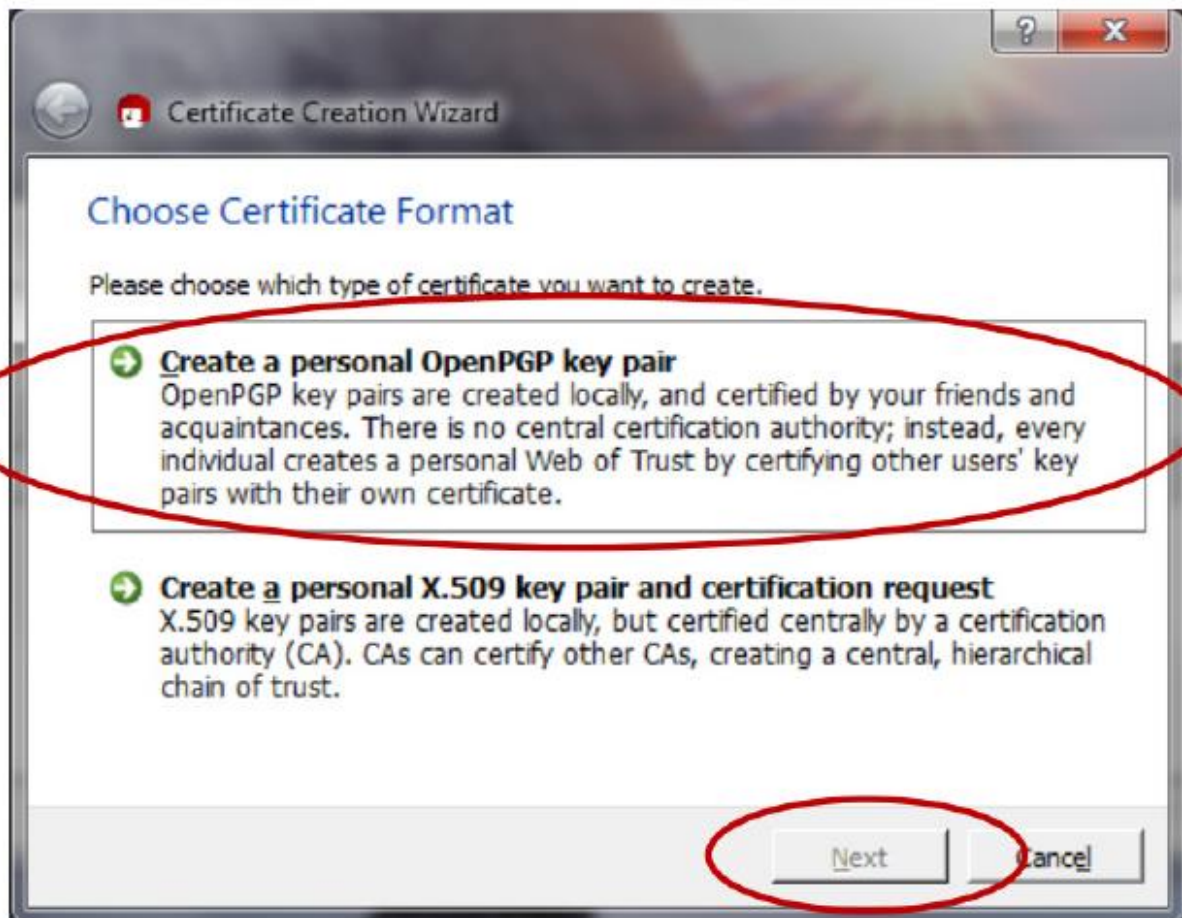
2. The following screen will be displayed



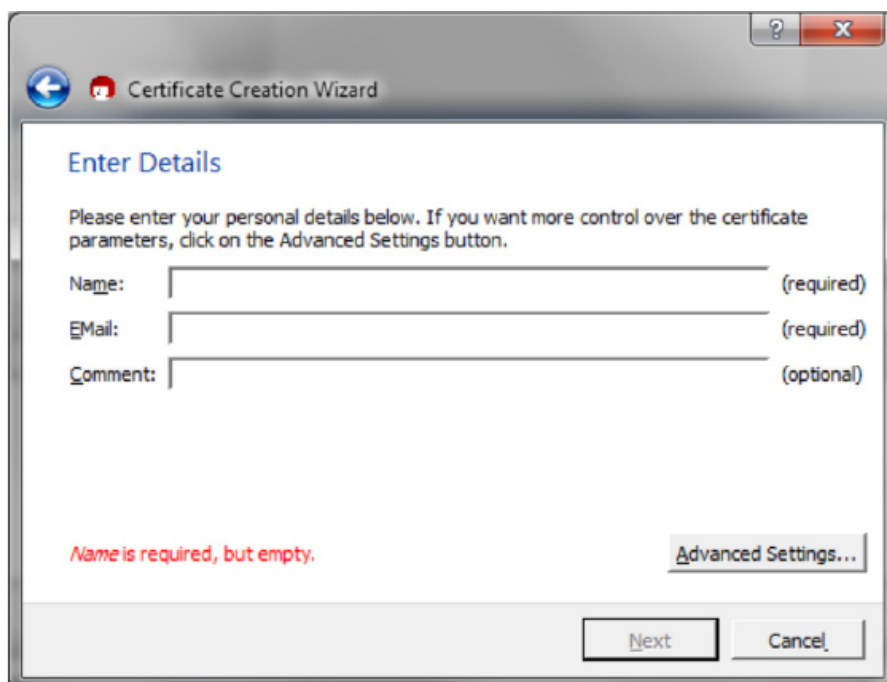
3. From the “File” dropdown, click on the “New Certificate” option



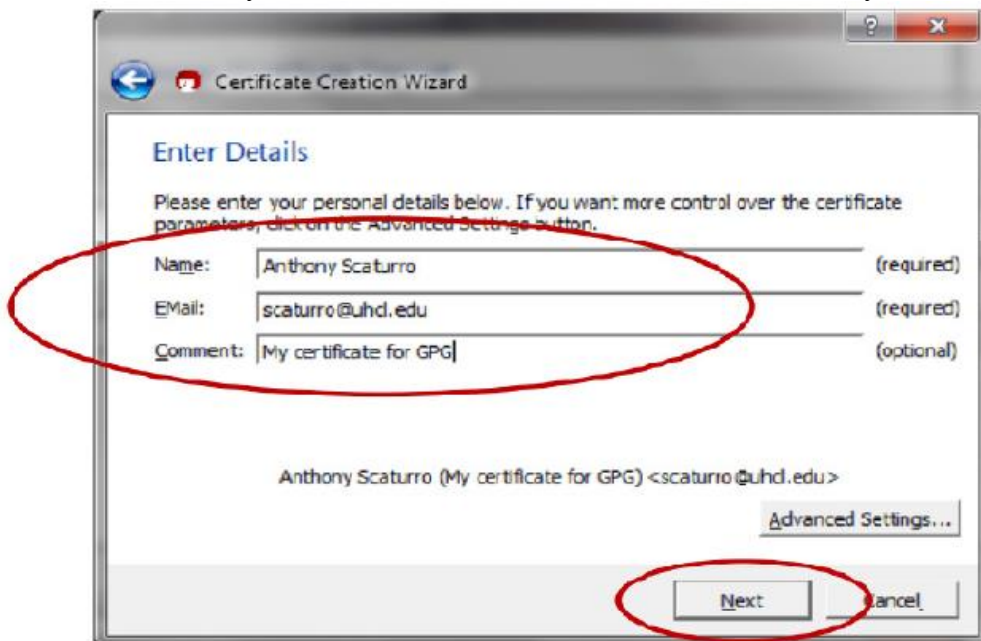
4. The following screen will be displayed. Click on “Create a personal OpenPGP key pair” and the “Next” button



5. The Certificate Creation Wizard will start and display the following:

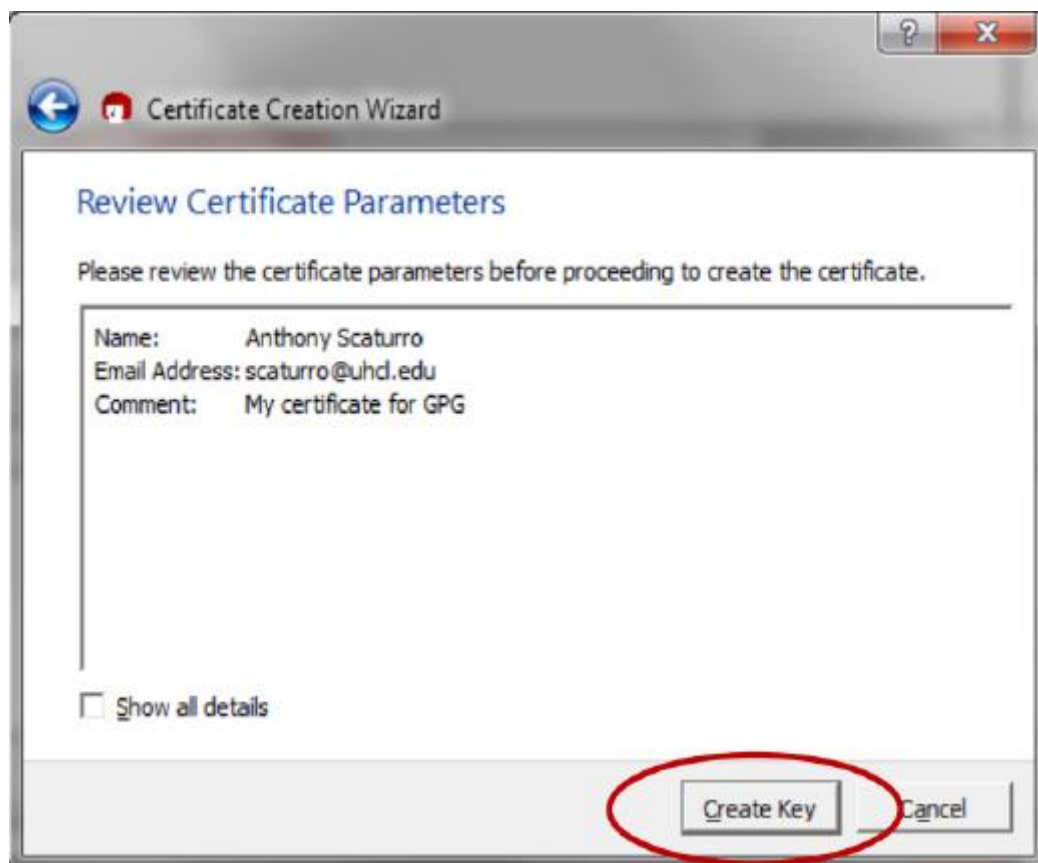


6. Enter your name and e-mail address. You may also enter an optional comment. Then, click the “Next” button. Review your entered values. If OK, click the “Create Key” button



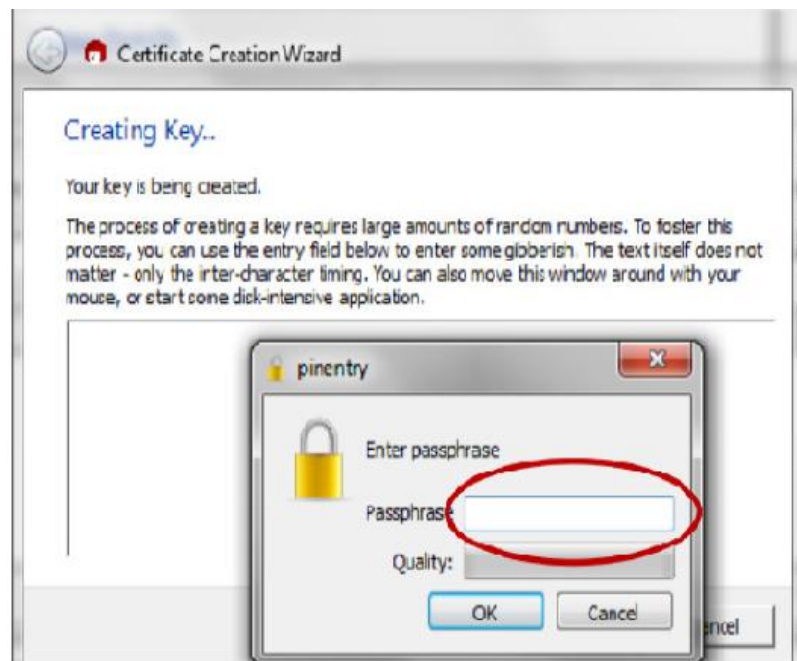
The screenshot shows the 'Enter Details' step of the Certificate Creation Wizard. The window title is 'Certificate Creation Wizard'. The instructions say: 'Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.' There are three input fields: 'Name' with the value 'Anthony Scaturro' (required), 'Email' with the value 'scaturro@uhd.edu' (required), and 'Comment' with the value 'My certificate for GPG' (optional). Below the fields, a summary line reads 'Anthony Scaturro (My certificate for GPG) <scaturro@uhd.edu>'. There is an 'Advanced Settings...' button. At the bottom right, the 'Next' button is circled in red, along with the 'Cancel' button.

7. Review your entered values. If OK, click the “Create Key” button

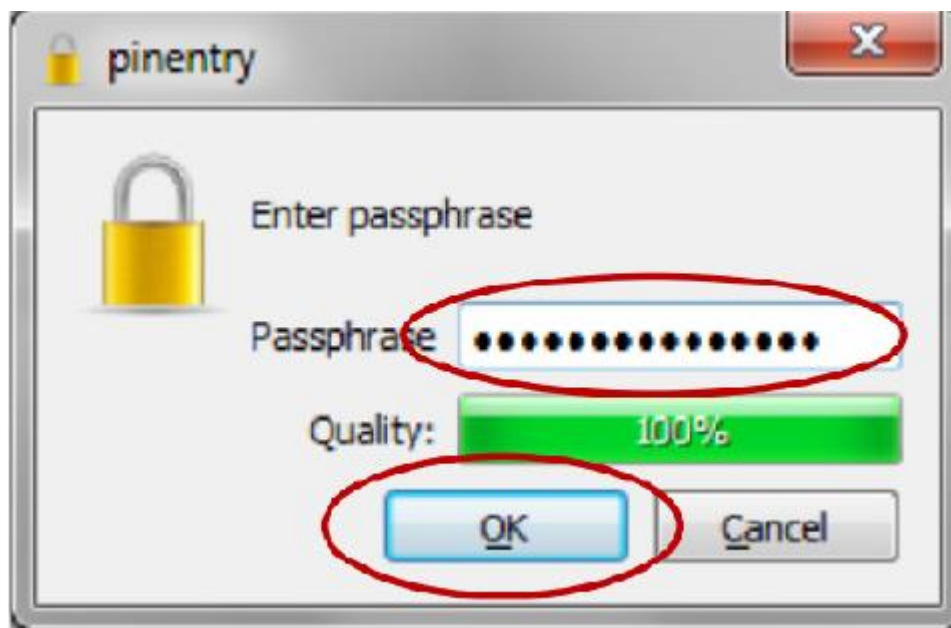


The screenshot shows the 'Review Certificate Parameters' step of the Certificate Creation Wizard. The window title is 'Certificate Creation Wizard'. The instructions say: 'Please review the certificate parameters before proceeding to create the certificate.' The parameters are listed: 'Name: Anthony Scaturro', 'Email Address: scaturro@uhd.edu', and 'Comment: My certificate for GPG'. There is a checkbox labeled 'Show all details' which is currently unchecked. At the bottom right, the 'Create Key' button is circled in red, along with the 'Cancel' button.

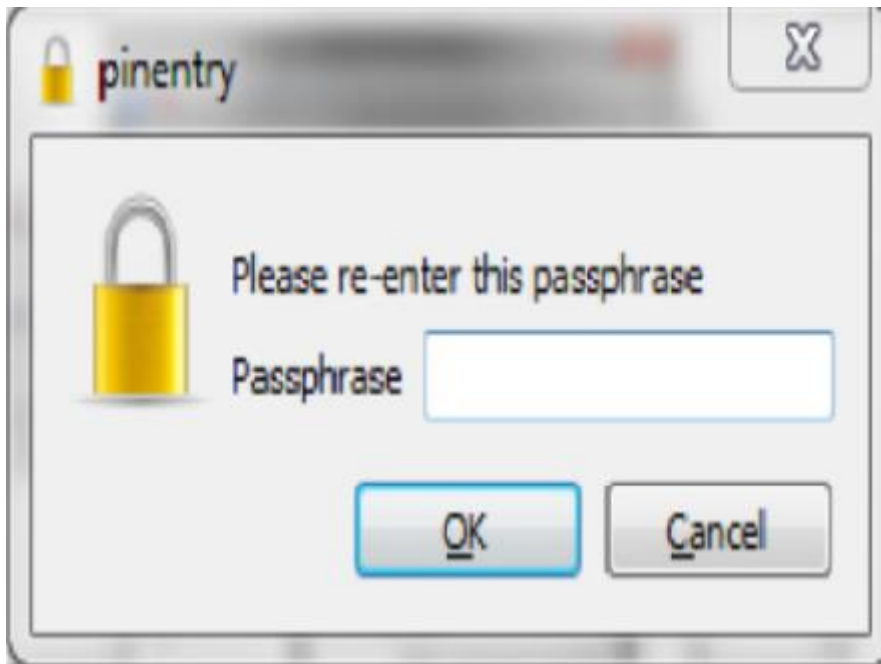
8. You will be asked to enter a passphrase



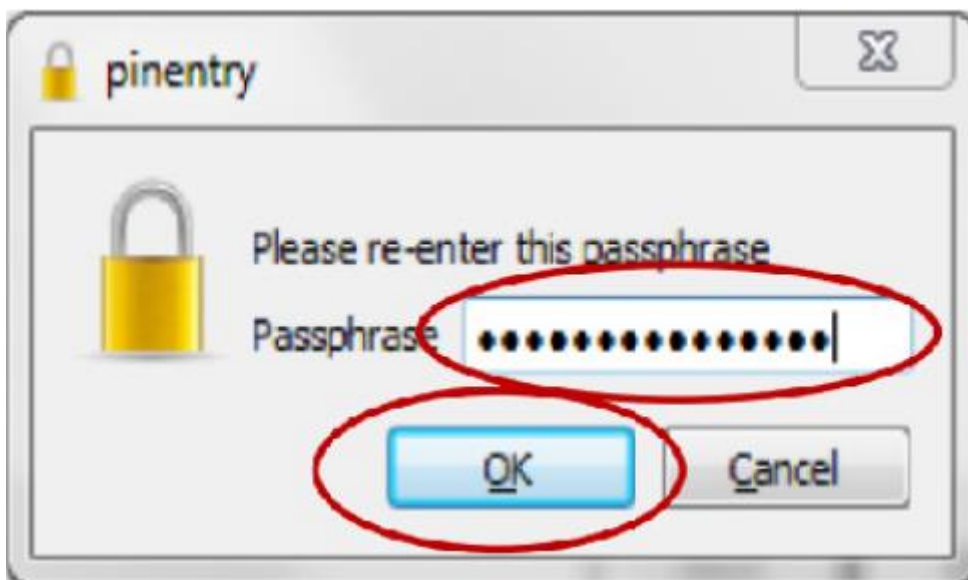
9. The passphrase should follow strong password standards. After you've entered your passphrase, click the "OK" button.



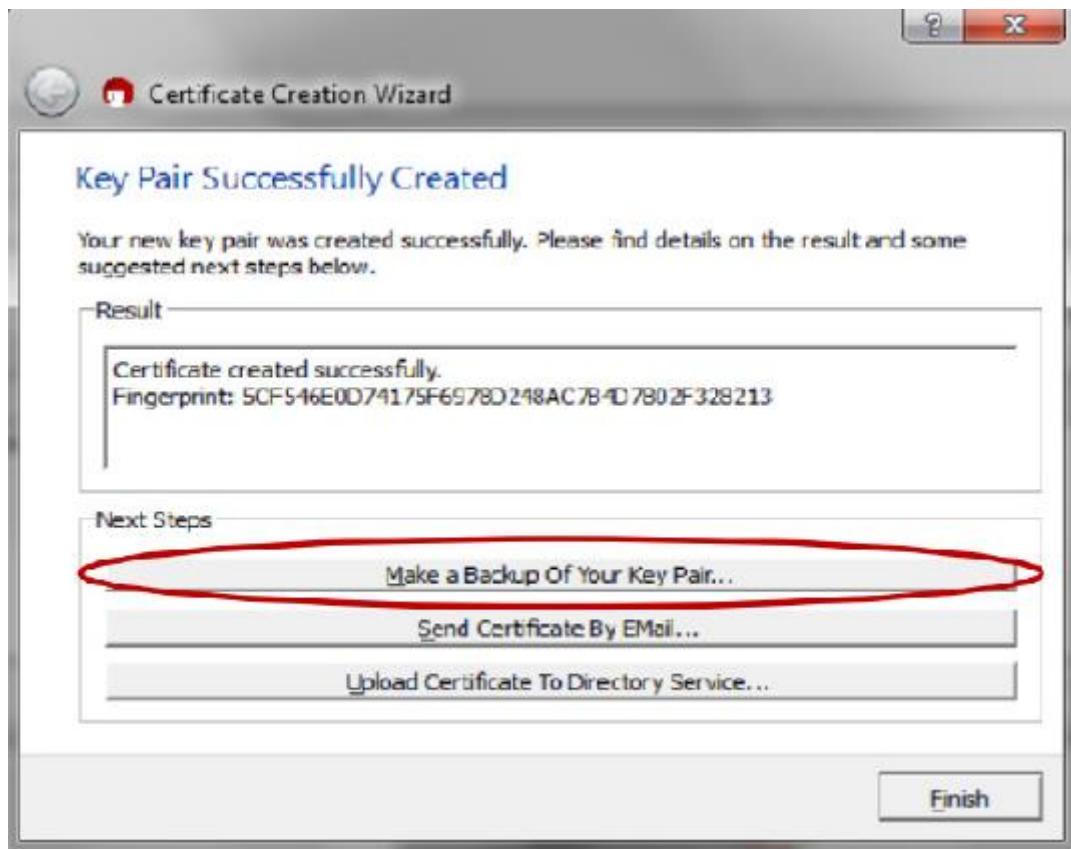
10. You will be asked to re-enter the passphrase



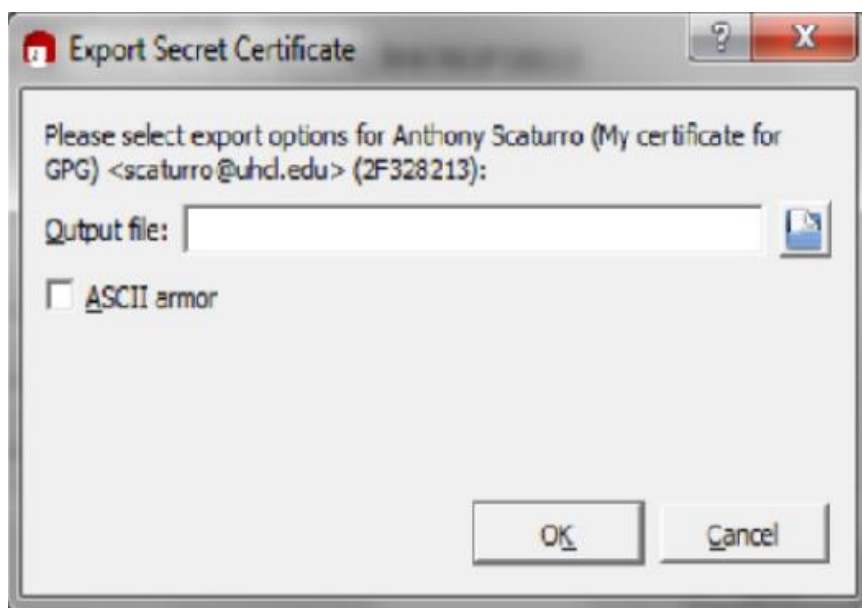
11. Re-enter the passphrase value. Then click the “OK” button. If the passphrases match, the certificate will be created.



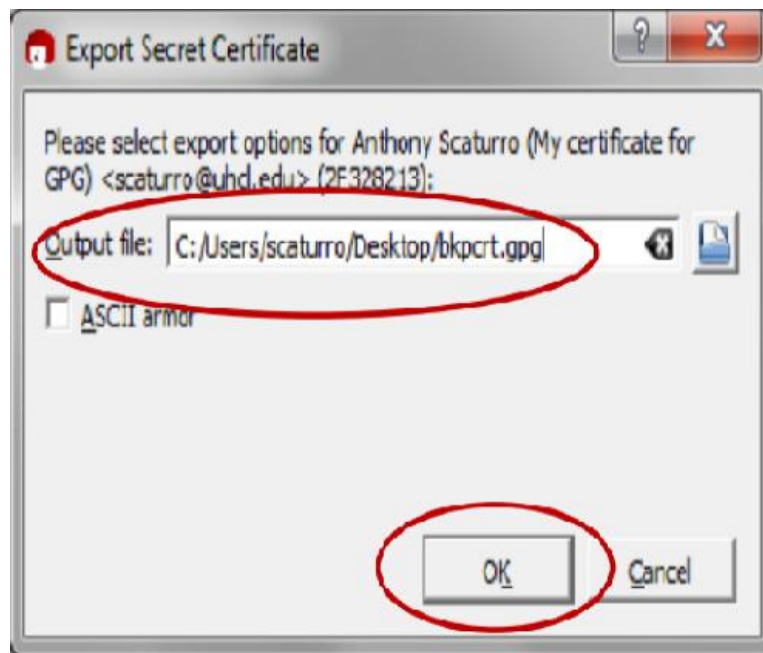
12. Once the certificate is created, the following screen will be displayed. You can save a backup of your public and private keys by clicking the “Make a backup Of Your Key Pair” button. This backup can be used to copy certificates onto other authorized computers.



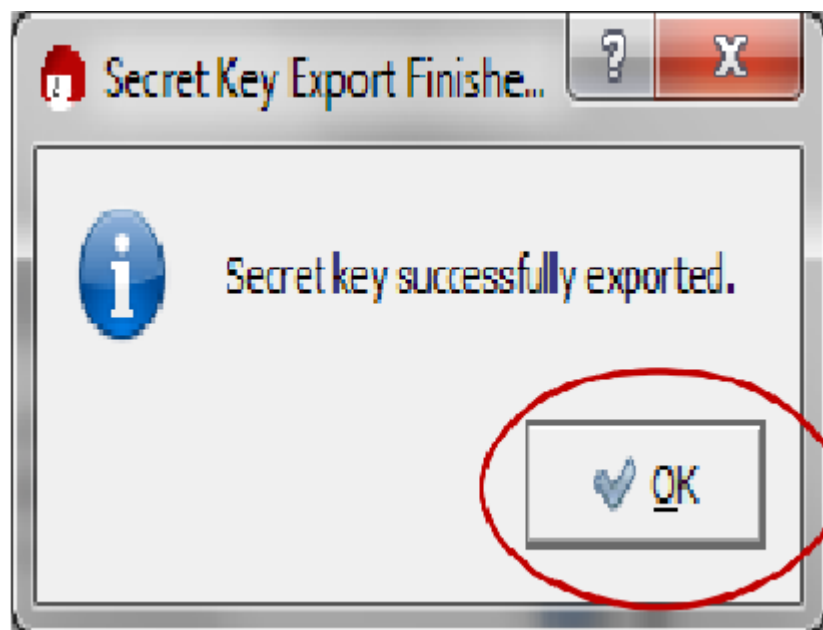
13. If you choose to backup your key pair, you will be presented with the following screen:



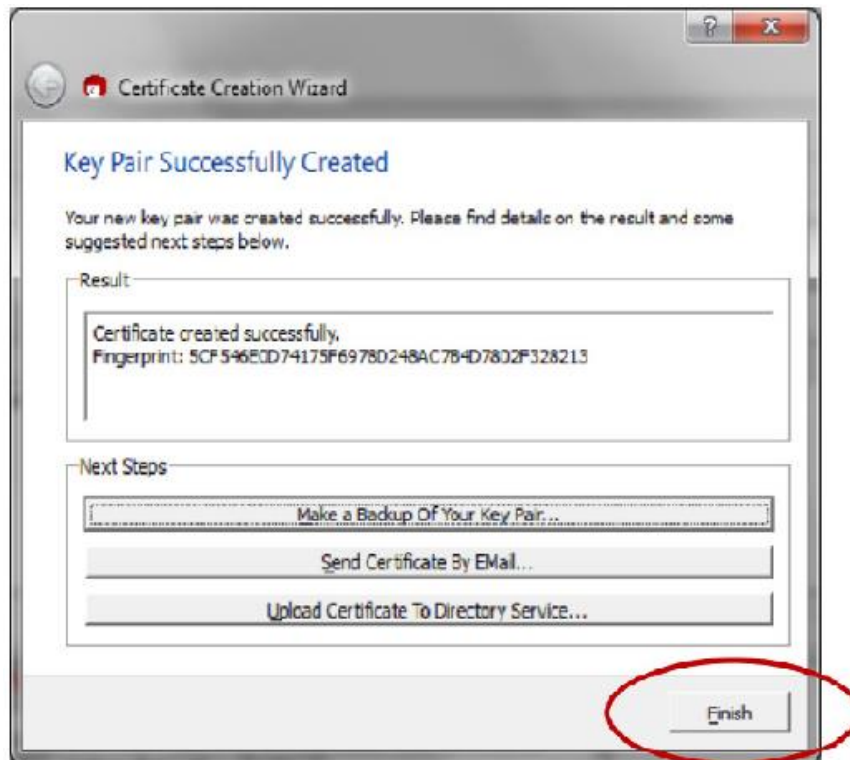
14. Specify the folder and name the file. Then click the “OK” button.



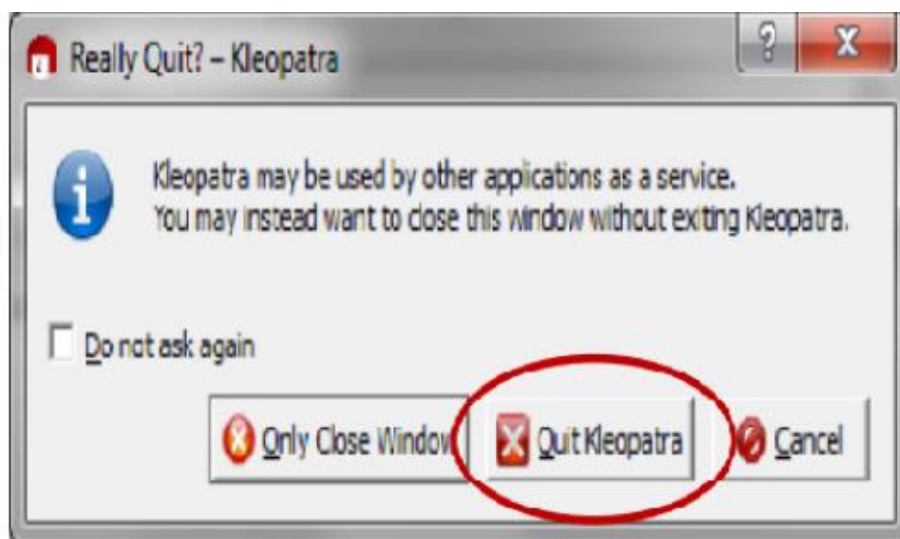
15. After the key is exported, the following will be displayed. Click the “OK” button.



16. You will be returned to the “Key Pair Successfully Created” screen. Click the “Finish” button.



17. Before the program closes, you will need to confirm that you want to close the program by clicking on the “Quit Kleopatra” button



RUBRICS EVALUATION

Performance Criteria	Scale 1 (0-25%)	Scale 2 (26-50%)	Scale 3 (51-75%)	Scale 4 (76-100%)	Score (Numerical)
Understandability Ability to analyse Problem and Identify solution	Unable to understand the problem.	Able to understand the problem partially and unable to identify the solution	Able to understand the problem completely but unable to identify the solution	Able to understand the problem completely and able to provide alternative solution too.	
Logic Ability to specify Conditions & control flow that are appropriate for the problem domain.	Program logic is incorrect	Program logic is on the right track but has several errors	Program logic is mostly correct, but may contain an occasional boundary error or redundant or contradictory condition.	Program logic is correct, with no known boundary errors, and no redundant or contradictory conditions.	
Debugging Ability to execute /debug	Unable to execute program	Unable to debug several errors.	Able to execute program with several warnings.	Able to execute program completely	
Correctness Ability to code formulae and algorithms that reliably produce correct answers or appropriate results.	Program does not produce correct answers or appropriate results for most inputs.	Program approaches correct answers or appropriate results for most inputs, but can contain miscalculations in some cases.	Program produces correct answers or appropriate results for most inputs.	Program produces correct answers or appropriate results for all inputs tested.	
Completeness Ability to demonstrate and deliver on time.	Unable to explain the code and the code was overdue.	Unable to explain the code and the code submission was late.	Able to explain code and the program was delivered within the due date.	Able to explain code and the program was delivered on time.	
TOTAL					

OUTCOMES OF LAB

After Completion of all the practical experiment students have achieved:

- The student should be able to implement the cipher techniques.
- Develop the various security algorithms.
- Use different open source tools for network security and analysis
- To learn & use the new tools and technologies used for designing some security principles.
- Analyse and resolve security issues in networks and computer systems to secure an IT infrastructure.

Computer Lab's Do's and Don'ts and Safety Rules

DO's

- Please switch off the Mobile/Cell phone before entering Lab.
- Check whether all peripheral are available at your desktop before proceeding for the session
- Arrange all the peripheral and seats before leaving the lab.
- Properly shutdown the system before leaving the lab.
- Keep the bag outside in the racks.
- Enter the lab on time and leave at proper time.
- Maintain the decorum of the lab.

DON'TS

- Don't mishandle the system.
- Don't leave the system on standing for long
- Don't bring any external material in the lab.
- Don't make noise in the lab.
- Don't bring the mobile in the lab.
- Don't enter in the lab without permission of lecturer/laboratory technician immediately
- Don't delete or make any modification in system files.
- Don't bring storage devices like pen drive without permission of lecturer/laboratory technician.

Computer Lab Safety Rules

- Know the location of the fire extinguisher and how to use them in case of an emergency.
- Report fires or accidents to your lecturer/laboratory technician immediately
- Report any broken plugs or exposed electrical wires to your lecturer/laboratory technician immediately.
- Avoid stepping on electrical wires or any other computer cables.
- Do not open the system unit casing or monitor casing particularly when the power is turned on.
- Do not touch, connect or disconnect any plug or cable without your lecturer/laboratory technician's permission.
- Do not bring any food or drinks near the machine.