

**Ex. No:**

**Date:**

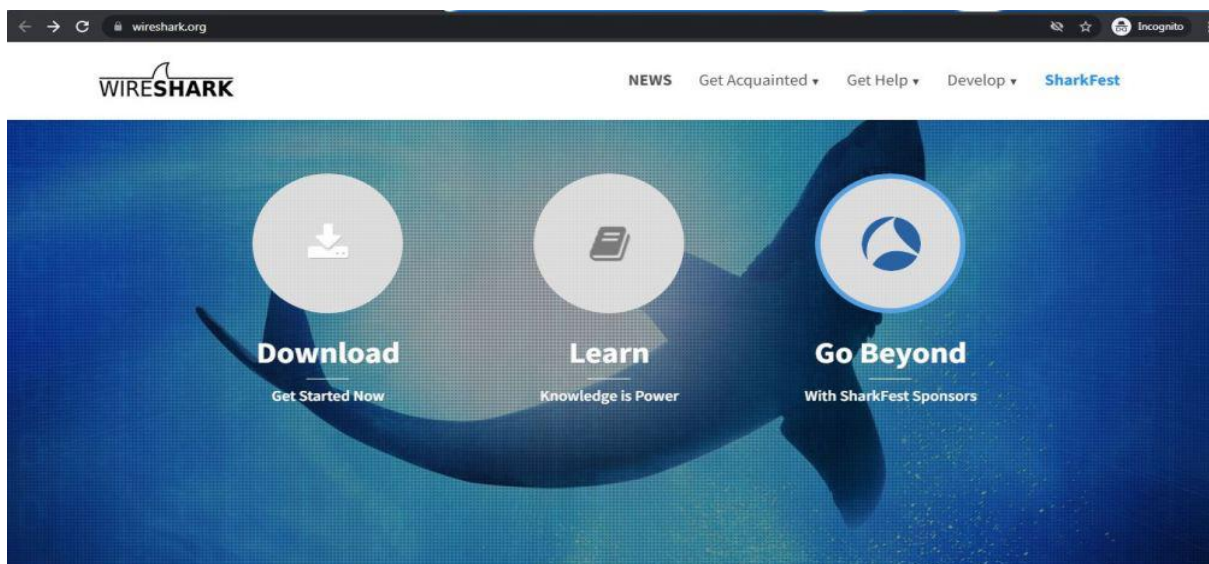
**Aim:**

To install Wireshark in windows and Ubuntu.

**Wireshark:**

Wireshark is software that is widely used in the analysis of data packets in a network. Wireshark is completely free and open source. This packet analyzer is used for a variety of purposes like troubleshooting networks, understanding communication between two systems, developing new protocols, etc. The original name of Wireshark was Ethereal which was changed in 2006 due to some company's copyright issues. This software is written in C and C++, and its initial release was in the year 1998. Its latest release is 3.6.0 which got released on 22 November 2021. Wireshark is a cross-platform software, it can be run on Linux, windows, mac, and any other operating system.

**Procedure in Windows:**



**Step 1:** Visit the official Wireshark website using any web browser.

**Step 2:** Click on Download, a new webpage will open with different installers of Wireshark.



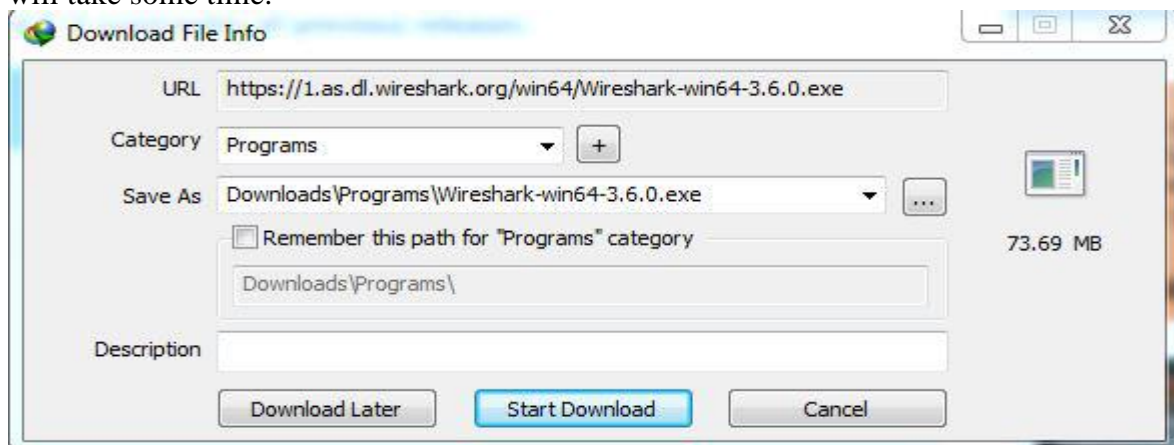
**Name:**

**Register. No.:**

**Ex. No:**

**Date:**

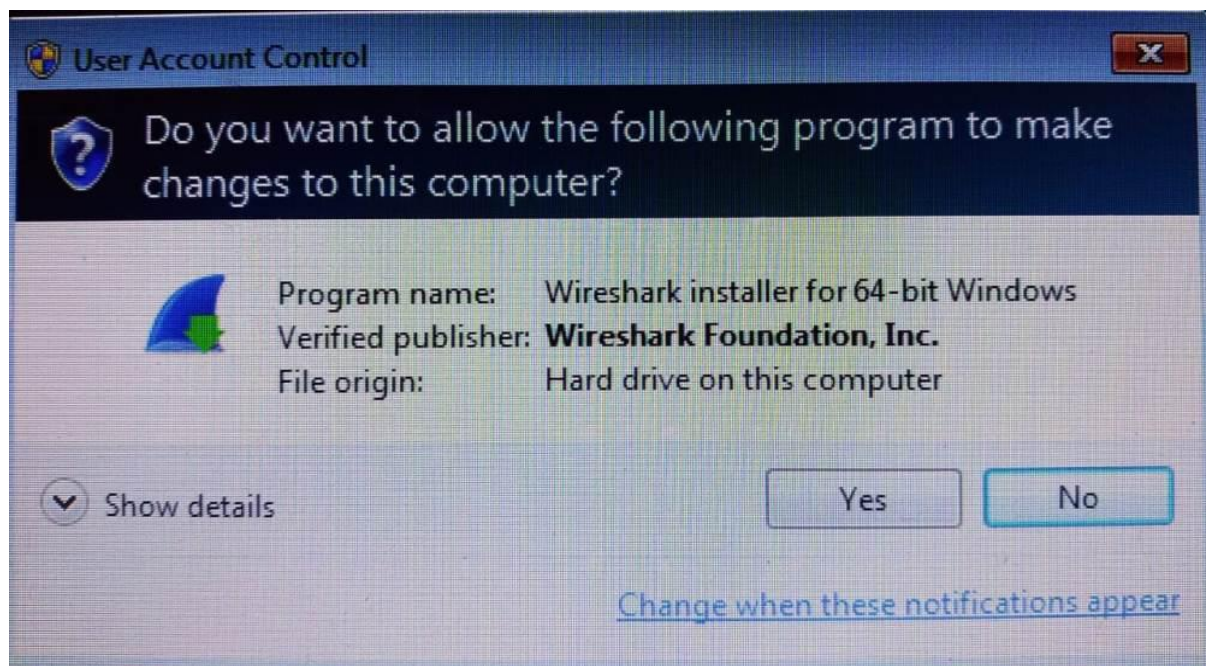
**Step 3:** Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.



**Step 4:** Now check for the executable file in downloads in your system and run it.



**Step 5:** It will prompt confirmation to make changes to your system. Click on Yes.



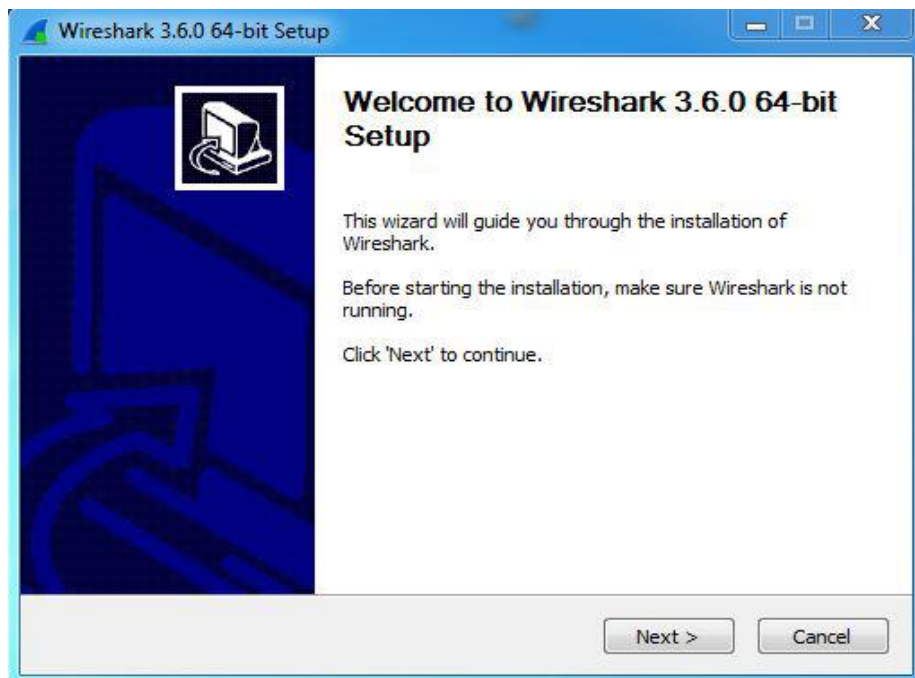
**Name:**

**Register. No.:**

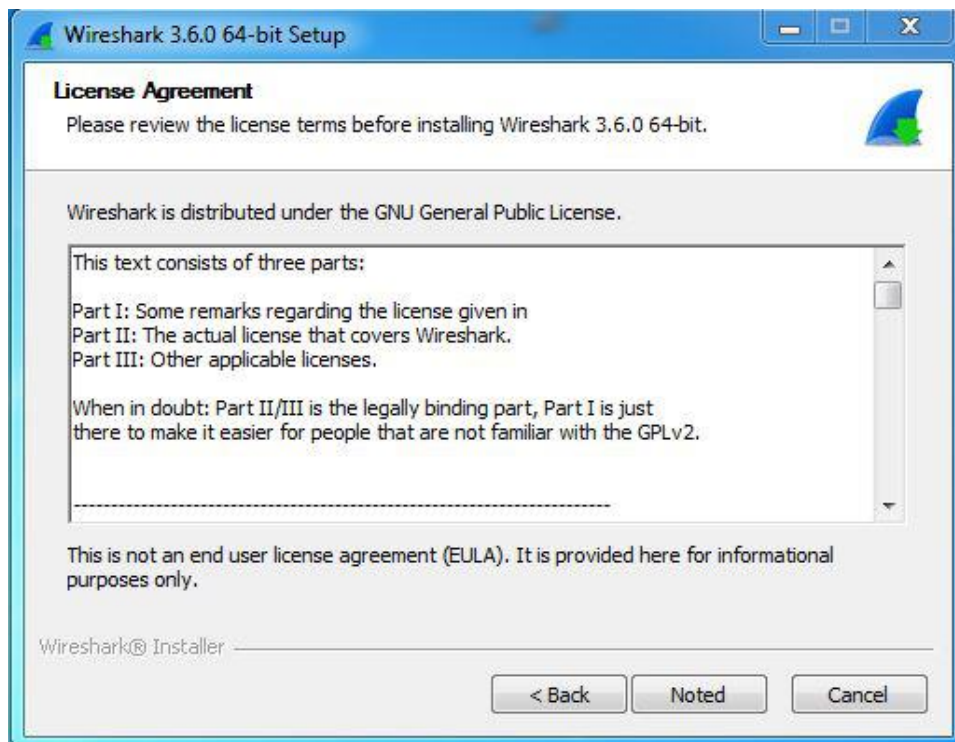
**Ex. No:**

**Date:**

**Step 6:** Setup screen will appear, click on Next.



**Step 7:** The next screen will be of License Agreement, click on Noted.



**Step 8:** This screen is for choosing components, all components are already marked so don't change anything just click on the Next button.

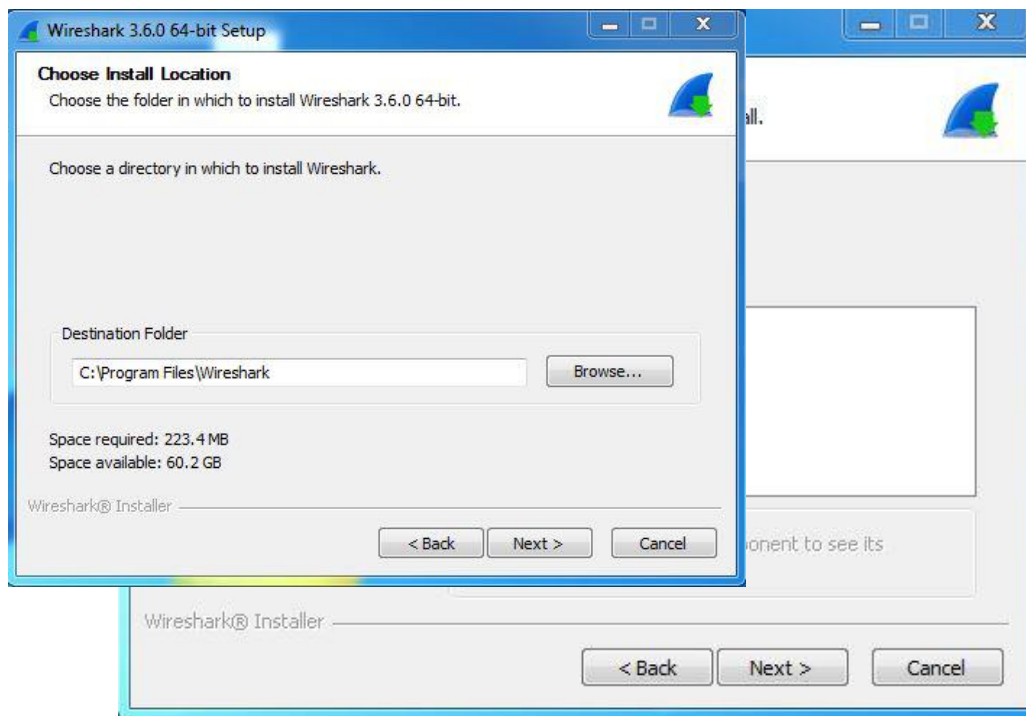
**Name:**

**Register. No.:**

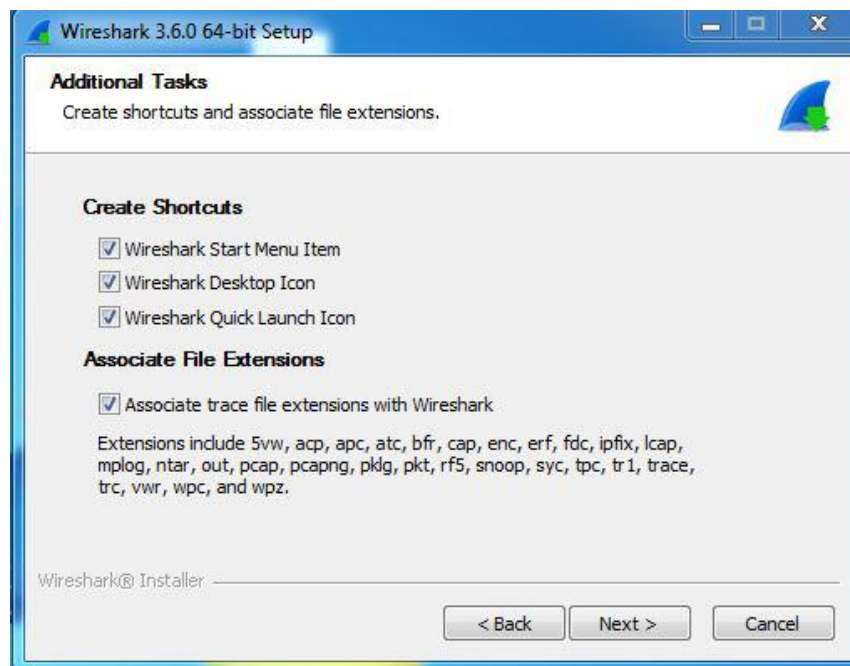


**Ex. No:**

**Date:**



**Step 9:** This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.



**Step 10:** The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed only a memory space of 223.4 MB.

**Step 11:** Next screen has an option to install Npcap which is used with Wireshark to capture packets *pcap* means packet capture so the install option is already checked don't change anything and click the next button.

**Name:**

**Register. No.:**

Ex. No:

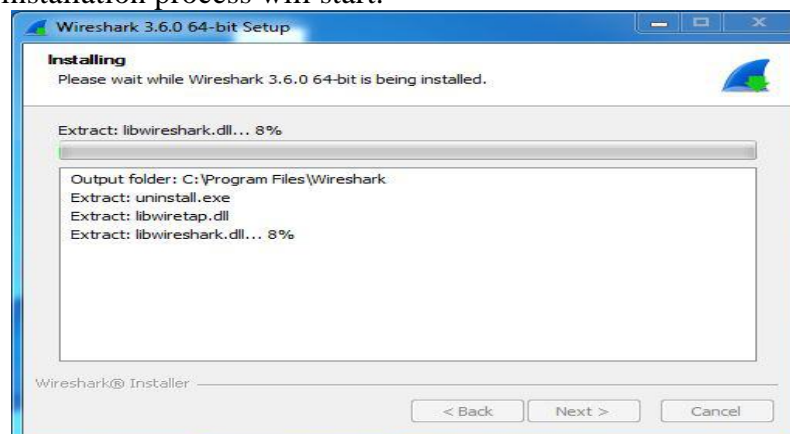
Date:



**Step 12:** Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.



**Step 13:** After this installation process will start.



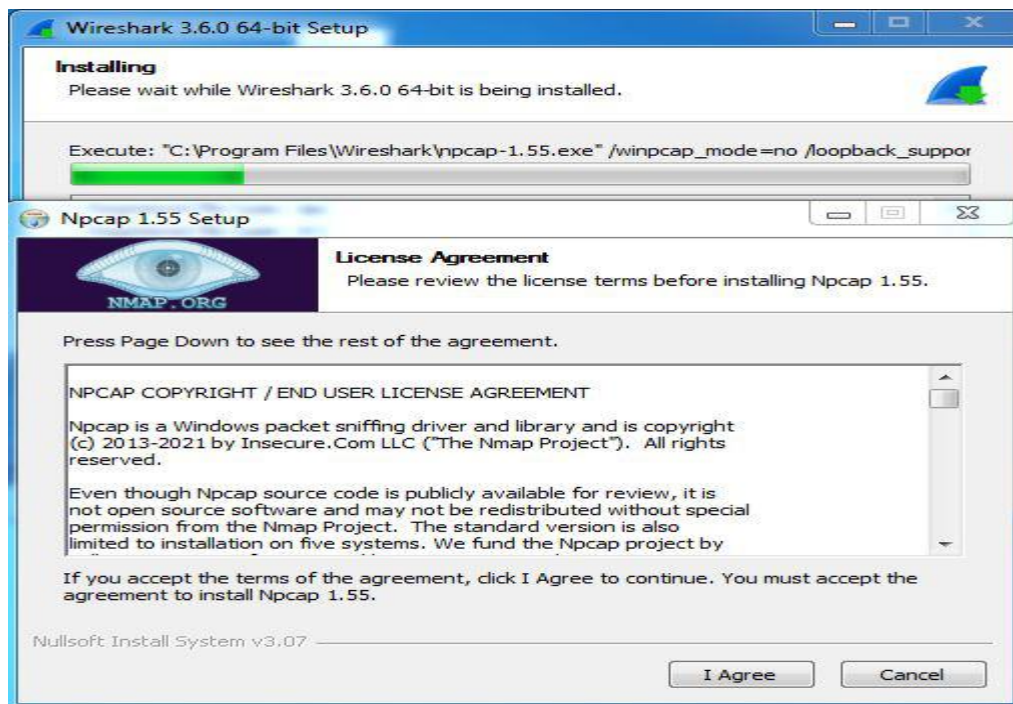
**Step 14:** This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the *I Agree* button.

Name:

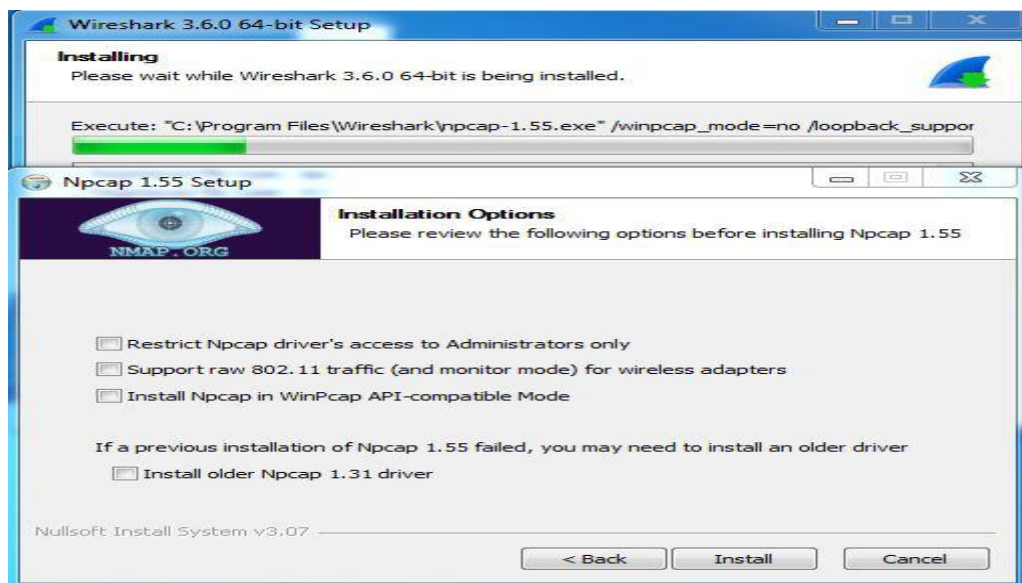
Register. No.:

Ex. No:

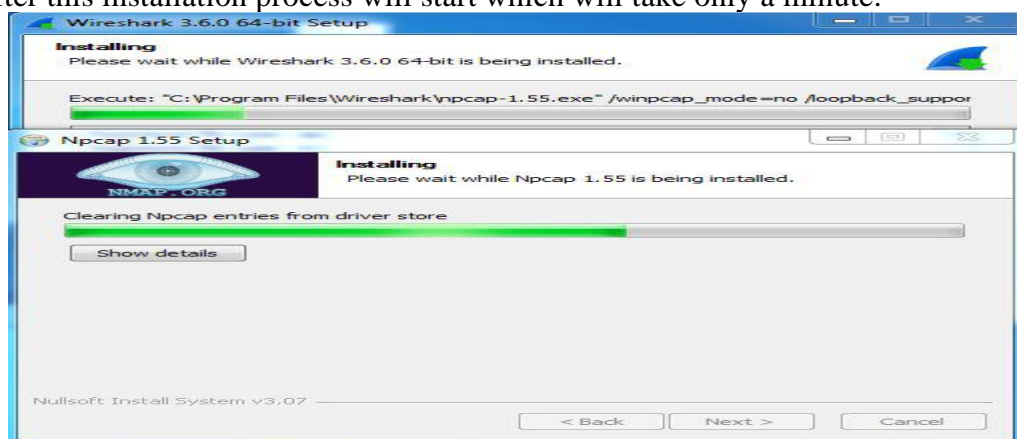
Date:



**Step 15:** Next screen is about different installing options of *npcap*, don't do anything click on Install.



**Step 16:** After this installation process will start which will take only a minute.



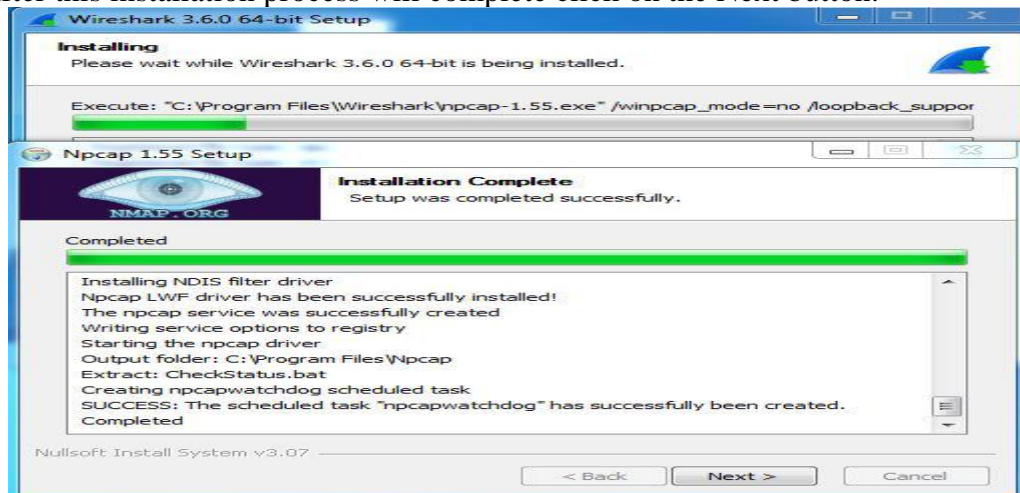
Name:

Register. No.:

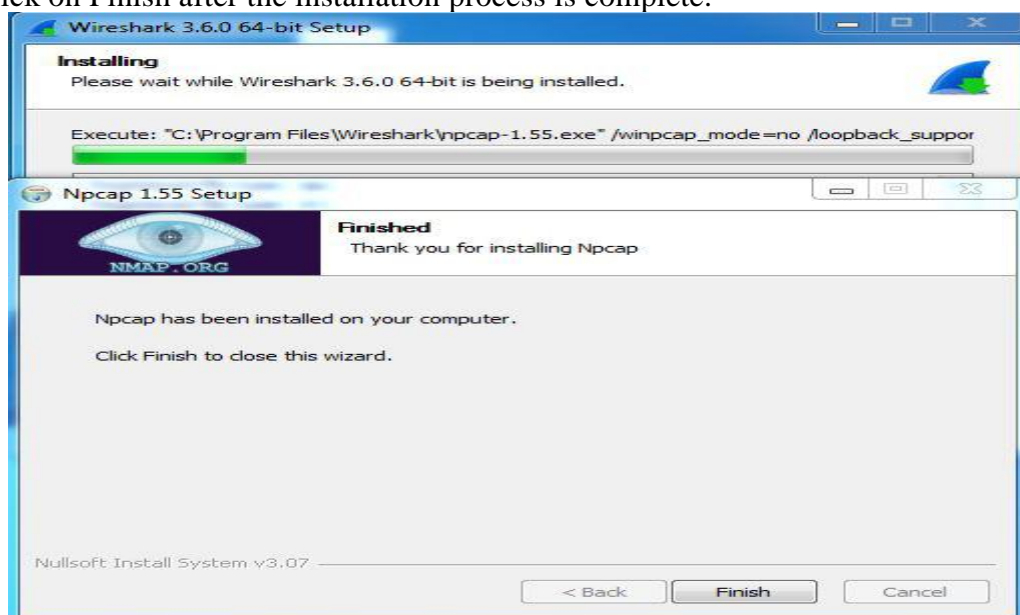
Ex. No:

Date:

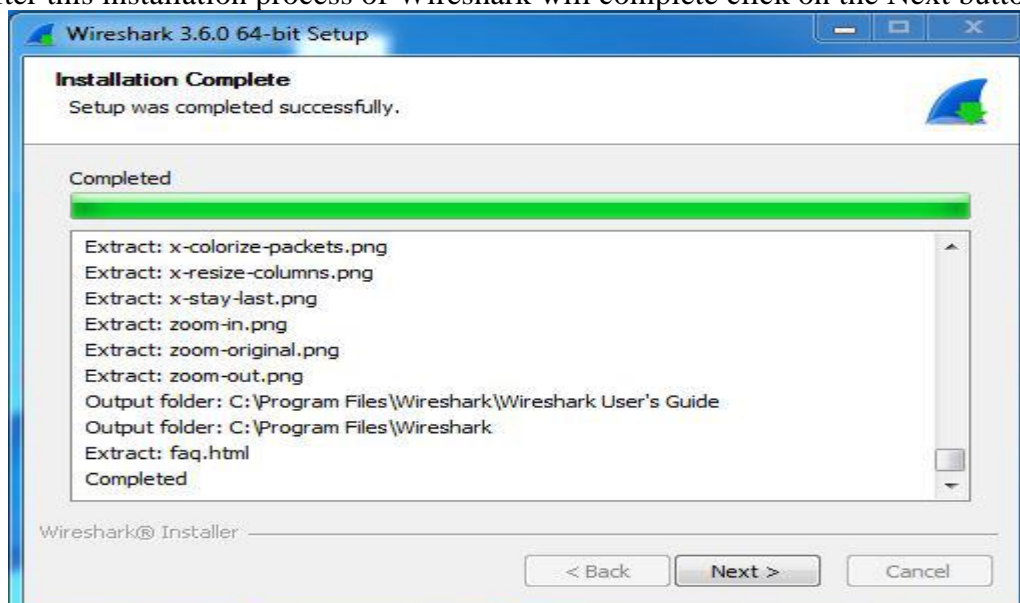
**Step 17:** After this installation process will complete click on the Next button.



**Step 18:** Click on Finish after the installation process is complete.



**Step 19:** After this installation process of Wireshark will complete click on the Next button.



**Step 20:** Click on Finish after the installation process of Wireshark is complete.

Name:

Register. No.:

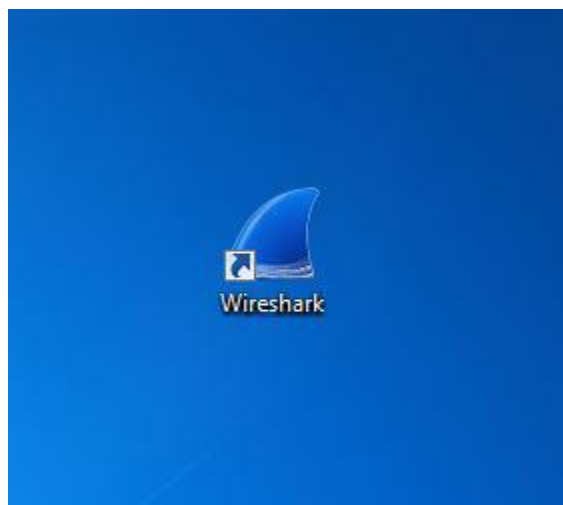


Ex. No:

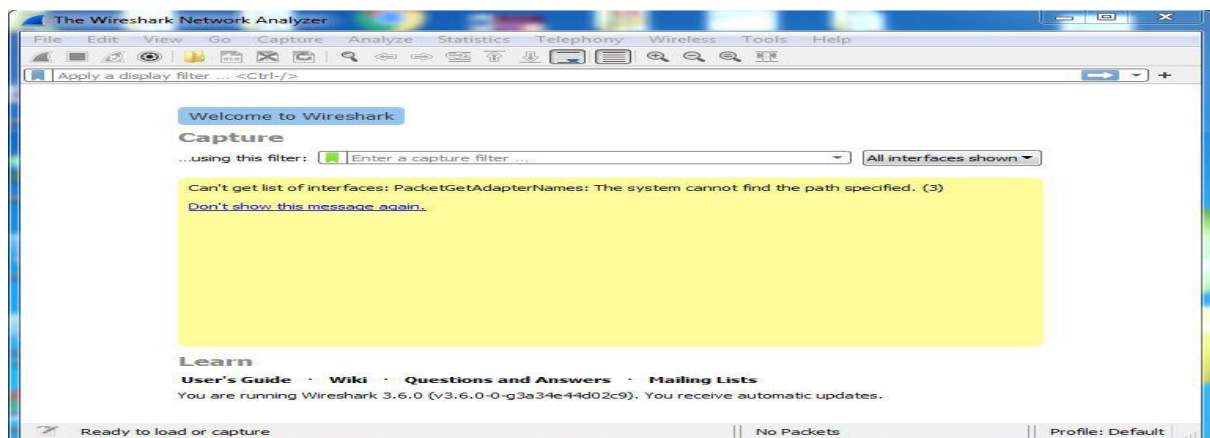
Date:



Wireshark is successfully installed on the system and an icon is created on the desktop as shown below:



Now run the software and see the interface.



Result:

Name:

Register. No.:



**Ex. No:**

**Date:**

**Aim:**

To Analyze the difference between HTTP vs HTTPS.

**Algorithm:**

Step 1: Start

Step 2: Install wireshark

Step 3: Start wireshark

Step 4: Analyze the difference between HTTP vs HTTPS

Step 5: View Server Output

Step 6: Stop

**Difference between HTTP and HTTPS:**

**HyperText Transfer Protocol (HTTP)**

- HyperText Transfer Protocol (HTTP) is a protocol using which hypertext is transferred over the Web.
- Due to its simplicity, HTTP has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using HTTP isn't as secure as we would like it to be.
- In fact, hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data.
- The acronym for Hypertext Transfer Protocol is HTTP.
- The web server delivers the desired data to the user in the form of web pages when the user initiates an HTTP request through their browser. Above the TCP layer lies an application layer protocol called HTTP. It has given web browsers and servers certain standard principles that they can use to talk to one another.
- Because each transaction on the HTTP protocol is carried out independently of the others and without reference to the history, the connection between the web browser and the server ends after the transaction is finished. This makes HTTP a stateless protocol.

**Advantages of HTTP**

- Because there are fewer connections running at once, it delivers reduced CPU and memory utilization.
- It allows requests and answers to be pipelined via HTTP.
- Because there are fewer TCP connections, it provides less network congestion.
- During the first stage of connection establishment, handshakes are exchanged. Because there is no handshaking, it provides lower latency for subsequent requests.
- Without terminating the TCP connection, it reports problems.

**Disadvantages of HTTP**

- It is applicable to point-to-point connections.
- It isn't mobile-friendly.
- It is not capable of being pushed.
- It uses far too many words.
- It doesn't provide trustworthy exchange (in the absence of retry mechanism).
- When the client receives all the data it requires, the connection is not terminated. Therefore, the server won't be accessible during this time.

**Hypertext Transfer Protocol Secure (HTTPS)**

- Hypertext Transfer Protocol Secure (HTTPS) is an extended version of the Hypertext Transfer Protocol (HTTP). It is used for secure communication.

**Name:**

**Register. No.:**

**Ex. No:**

**Date:**

- In HTTPS, the communication protocol is encrypted using Transport Layer Security.
- HTTPS stands for Hypertext Transfer Protocol Secure.
- While HTTP guarantees data security, the HTTP protocol does not provide data security.
- As a result, HTTPS can be defined as a secure variant of the HTTP protocol. Data can be transferred using this protocol in an encrypted format.
- In most cases, the HTTPS protocol must be used while entering bank account information.
- The HTTPS protocol is mostly utilised in situations when entering login credentials is necessary. Modern browsers like Chrome distinguish between the HTTP and HTTPS protocols based on distinct markings.
- HTTPS employs an encryption mechanism called Secure Sockets Layer (SSL), also known as Transport Layer Security, to enable encryption.

#### **Advantages of HTTPS**

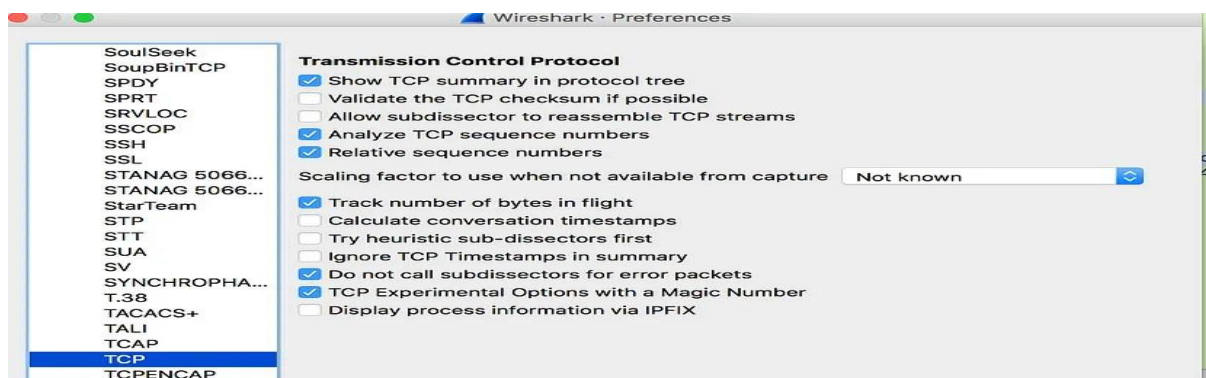
- Provides in-transit data security.
- Shields your website from data breaches, phishing, and MITM attacks.
- Increases the visitors' trust to your website.
- Eliminates the "NOT Secure" alerts.
- Assist you in raising your website's ranking.

#### **Disadvantages of HTTPS**

- When switching to HTTPS, an SSL certificate needs to be bought. Even though website hosts often give SSL certificates, these should be renewed annually by paying a charge.
- Encrypting and decrypting data across HTTPS connections requires a lot of computation.
- There will be issues with caching some information over HTTPS. Public caching of those that previously took place won't happen again.
- Certain proxy servers and firewalls prevent users from accessing HTTPS websites. Both deliberate and inadvertent actions might result from this.
- If there are configuration issues, HTTP will be used by your website to obtain files rather than HTTPS.

#### **Procedure:**

**Step 1:** Before start analyzing any packet, please turn off "Allow subdissector to reassemble TCP streams" (Preference → Protocol → TCP) (This will prevent TCP packet to split into multiple PDU unit)



**Step 2:** By opening http website, the click start analyze in wireshark tool. The corresponding http packets shown in the dialog box.

**Name:**

**Register. No.:**

Ex. No:

Date:

4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.602419	65.208.228.223	145.254.160.237	HTTP	1434	HTTP/1.1 200 OK
7	1.812606	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	1.812606	65.208.228.223	145.254.160.237	HTTP	1434	Continuation
9	2.012894	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	2.443513	65.208.228.223	145.254.160.237	HTTP	1434	Continuation

Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)

Ethernet II, Src: Superlan\_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)

Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223

Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479

Hypertext Transfer Protocol

GET /download.html HTTP/1.1\r\n

Host: www.ethereal.com\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,\*/\*;q=0.1\r\n

Accept-Language: en-us,en;q=0.5\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

Referer: http://www.ethereal.com/development.html\r\n

\r\n

[Full request URI: http://www.ethereal.com/download.html]

[HTTP request 1/1]

[Response in frame: 6]

**Step 3:** By opening https website (Ex. Gmail), then click start analyze in wireshark, it shows multiple packets coming/ out over ethernet in encrypted data. In https, all the data security protocols, algorithms and handshake mechanisms are carried out.

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ssl						
No.	Time	Source	Destination	Protocol	Length	Info
510	5.645867	149.96.89.35	10.88.33.165	TLSv1.2	620	Application Data
512	5.648038	149.96.89.35	10.88.33.165	TLSv1.2	152	Server Hello, Change Cipher Spec
515	5.717896	216.58.199.35	10.88.33.165	TLSv1.2	138	Application Data
516	5.718706	216.58.199.35	10.88.33.165	TLSv1.2	454	Application Data
518	5.727261	216.58.199.35	10.88.33.165	TLSv1.2	92	Application Data
519	5.728059	216.58.199.35	10.88.33.165	TLSv1.2	100	Application Data
522	5.740371	149.96.89.35	10.88.33.165	TLSv1.2	1342	Application Data
525	5.741258	149.96.89.35	10.88.33.165	TLSv1.2	99	Encrypted Handshake Message
531	5.810038	149.96.89.35	10.88.33.165	TLSv1.2	195	Application Data
535	5.862373	149.96.89.35	10.88.33.165	TLSv1.2	314	Application Data
561	6.648526	216.58.199.35	10.88.33.165	TLSv1.2	138	Application Data
562	6.649393	216.58.199.35	10.88.33.165	TLSv1.2	458	Application Data
564	6.651127	216.58.199.35	10.88.33.165	TLSv1.2	92	Application Data
565	6.652381	216.58.199.35	10.88.33.165	TLSv1.2	100	Application Data
603	6.968464	151.101.81.67	10.88.33.165	TLSv1.2	1466	Server Hello
607	6.972510	151.101.81.67	10.88.33.165	TLSv1.2	1466	Certificate [TCP segment of a reassembled PDU]
610	6.973838	151.101.81.67	10.88.33.165	TLSv1.2	827	Certificate Status, Server Key Exchange, Server Hell

**Step 4:** Apply filters to check the individual packets coming in and out over the internet.

**Result:**

Name:

Register. No.:

**Ex. No:**

**Date:**

**Aim:**

To Analyze the various security mechanism embedded with different protocols.

**Algorithm:**

Step 1: Start

Step 2: Start wireshark

Step 3: Analyze the various security mechanism embedded with different protocol

Step 4: View Server Output

Step 5: Stop

**Procedure:**

1. In the menu bar, Capture → Interfaces.
2. Select a particular Ethernet adapter and click start.
3. After this, browse to any web address and then return to Wireshark. Browsing would get packets captured and in Wireshark click the stop in the Capture menu to stop the capture.
4. If you haven't got the packet list by now, you can access it using Edit → Find Packets. This will give you the packet list.

Follow these steps to read SSL and TLS packets:

1. In the "Packet List" pane, focus on the "Protocol" column and look for "SSL."
2. Find the SSL or TLS packet you're interested in and open it.

Follow these steps to read IPsec traffic:

1. To just check if traffic is going through the VPN I just use the "show crypto ipsec sa". Then you will be able to see if traffic is being encrypted and decrypted.

Follow these steps to read SSH traffic:

1. To view the SSH packets, type SSH into the Wireshark filter. Many client and server packets should be displayed. Notice keys are exchanged and the packets are encrypted. This does show that SSH is a secured protocol.

Follow these steps to read WPA/WPA2 traffic:

1. Wireshark can decrypt WEP and WPA/WPA2/WPA3 in pre-shared (or personal) mode, as well as in enterprise mode. Security improvements in more recent 802.11 releases require distinct session keys, instead of being able to decipher all traffic to a given access point with a single known password and SSID.

Follow these steps to read DNSSEC traffic:

1. To analyze DNS we shall be studying only DNS packets and to get DNS packets, only you can apply DNS in the filters. You can have access to the DNS details of any packet by clicking the Domain Name System label in the frame detail section of the Wireshark window.

Follow these steps to read OAuth traffic:

**Name:**

**Register. No.:**



**Ex. No:**

**Date:**

1. To load the Authentication Traffic filter that shows packets containing Kerberos tickets as well. You can do this by clicking the Load Filter button, choose Standard Filters, and then click Authentication Traffic.
2. If there is a lot of traffic, remove the lines for NLMP to reduce some of the noise. Remember to click the Apply button again to make the changes effective.

Note: #after capturing packets , analyze them using wireshark:

```
wireshark -r <filename.pcap>
```

Replace <filename.pcap> with the name of the captured file. This open Wireshark with the specified packet capture file for detailed analysis.

**Result:**

**Name:**

**Register. No.:**

**Ex. No:**

**Date:**

**Aim:**

To Identify the Vulnerabilities Using Owasp Zap Tool.

**INSTALLATION OF OWASP ZAP:**

- ZAP (short for Zed Attack Proxy), formerly known as OWASP ZAP, is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP). ZAP is designed specifically for testing web applications and is both flexible and extensible.
  - **Penetration Testing** – The system undergoes analysis and attack from simulated malicious attackers.
  - Penetration Testing (pentesting) is carried out as if the tester was a malicious external attacker with a goal of breaking into the system and either stealing data or carrying out some sort of denial-of-service attack.
- At its core, ZAP is what is known as a “man-in-the-middle proxy.”
- It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.



If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.



**Name:**

**Register. No.:**

**Ex. No:**

**Date:**

## Install and Configure ZAP

The first thing to do is install ZAP on the system you intend to perform pentesting on. Download the appropriate installer from the Download page.

Note that ZAP requires Java 11+ in order to run. The macOS installer includes an appropriate version of Java but you must install Java 11+ separately for Windows, Linux, and Cross-Platform versions.

**Download link:** <https://www.zaproxy.org/download/>

### ZAP 2.11.1

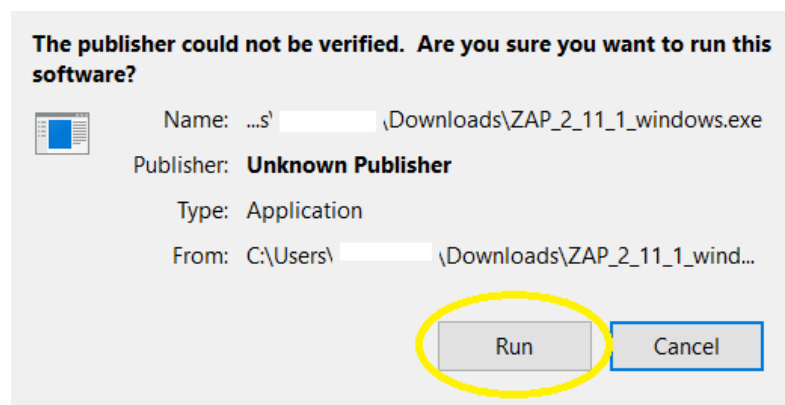
<a href="#">Windows (64) Installer</a>	183 MB	<a href="#">Download</a>
<a href="#">Windows (32) Installer</a>	183 MB	<a href="#">Download</a>
<a href="#">Linux Installer</a>	188 MB	<a href="#">Download</a>
<a href="#">Linux Package</a>	186 MB	<a href="#">Download</a>
<a href="#">MacOS Installer</a>	213 MB	<a href="#">Download</a>
<a href="#">Cross Platform Package</a>	204 MB	<a href="#">Download</a>
<a href="#">Core Cross Platform Package</a>	55 MB	<a href="#">Download</a>

Now, you can follow the steps below.

**Step 1: Click on the executable file.**



**Step 2: Click on run**



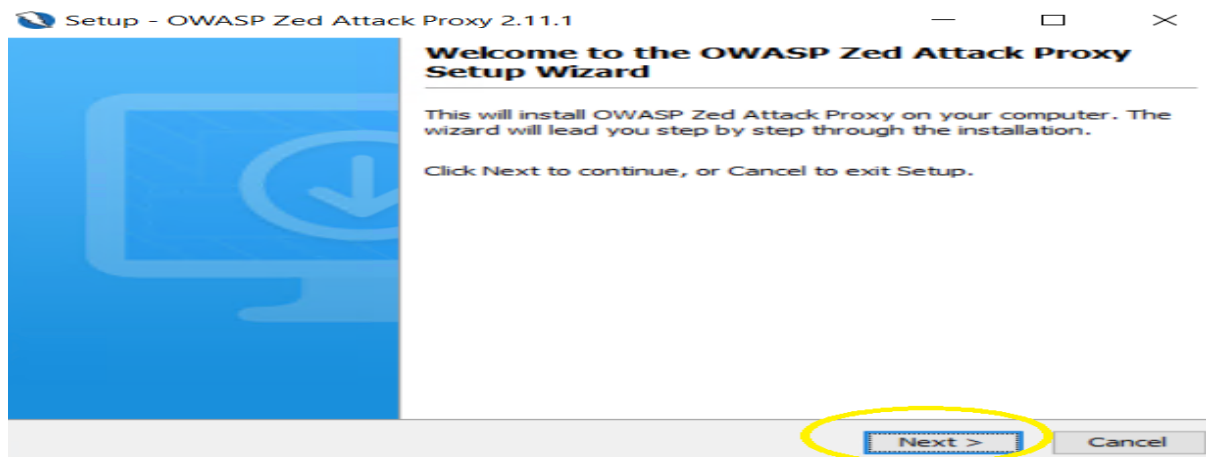
**Name:**

**Register. No.:**

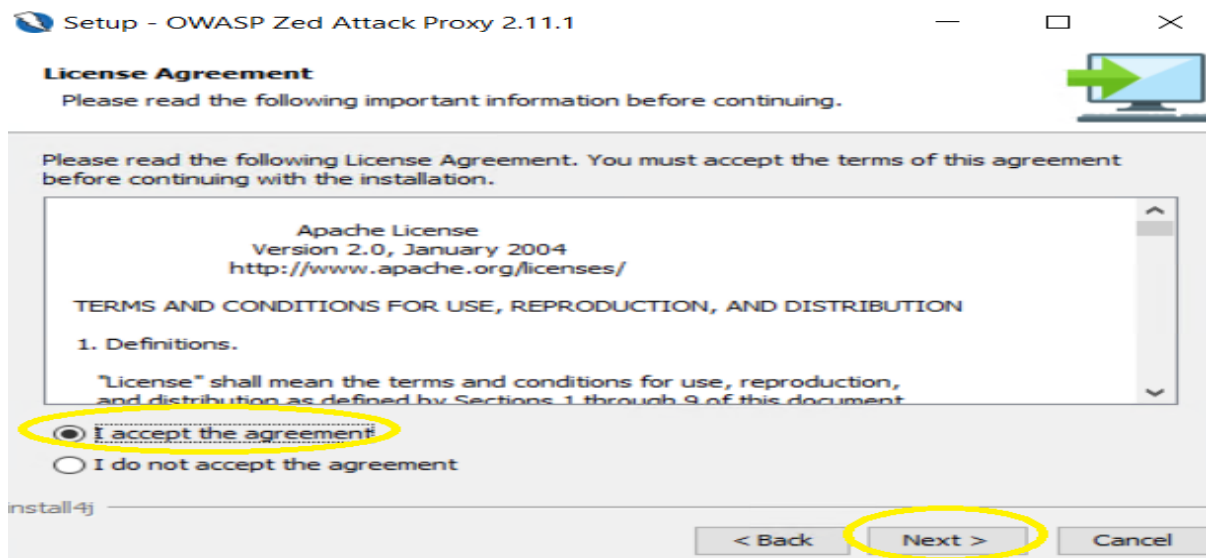
Ex. No:

Date:

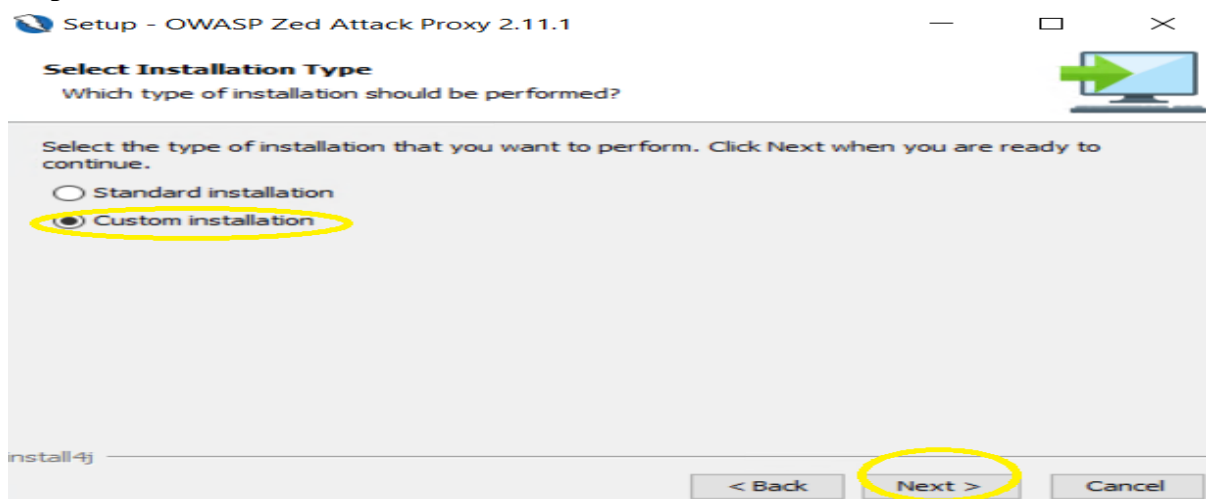
### Step 3: Click on next to continue



### Step 4: Read and accept the agreement



### Step 5: Choose standard or Customization installation



Name:

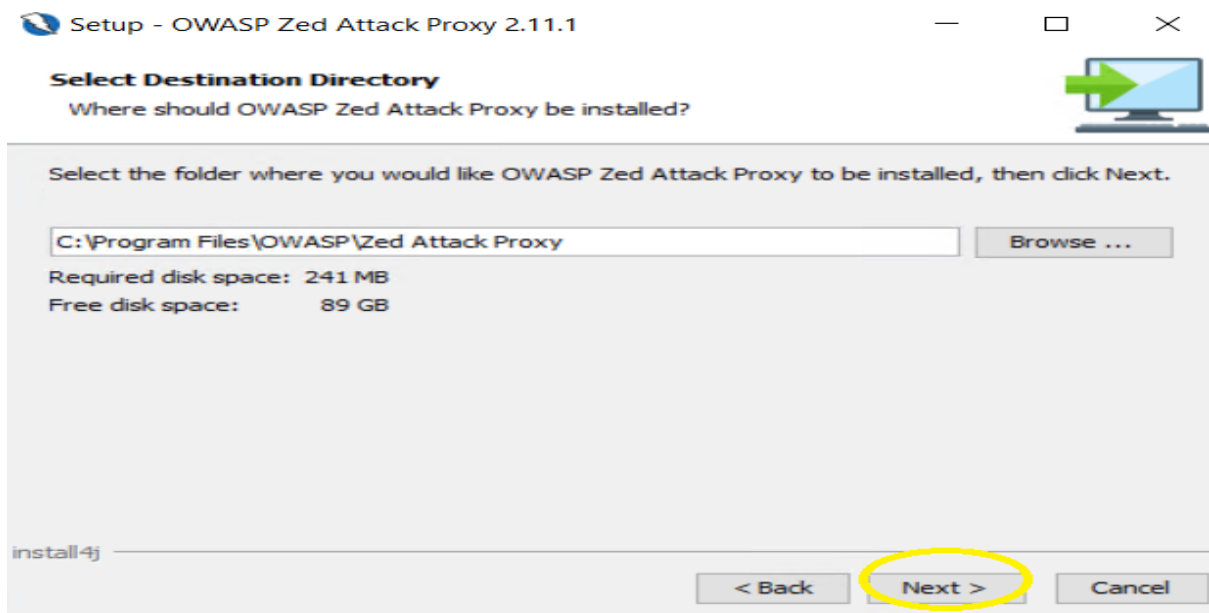
Register. No.:



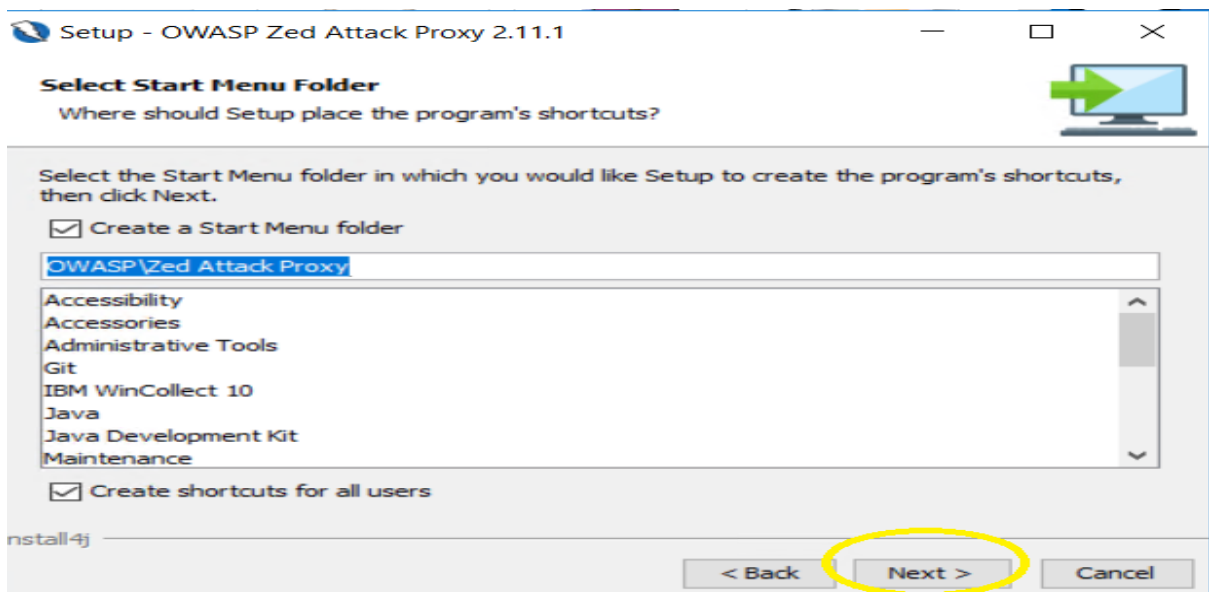
Ex. No:

Date:

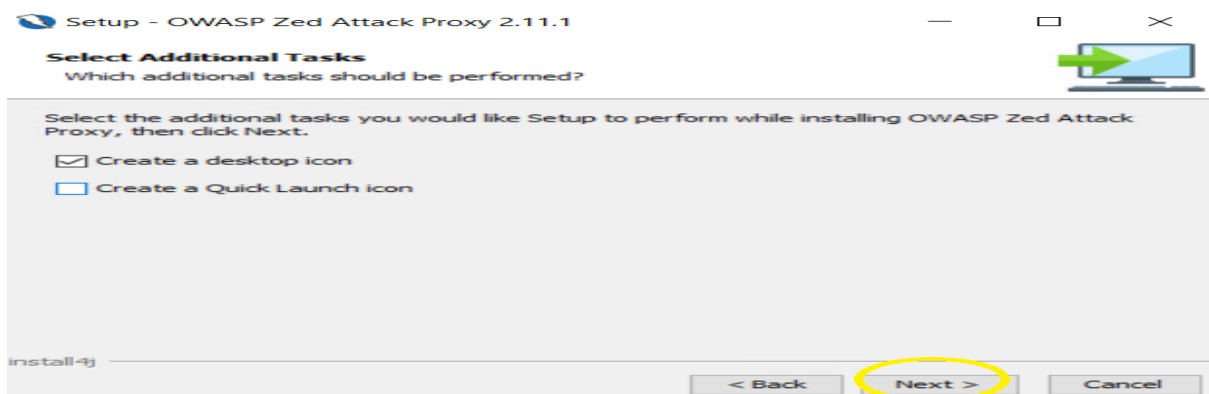
**Step 6: Select the destination where you want to save.**



**Step 7: Select start menu folder**



**Step 8: Create a desktop icon**



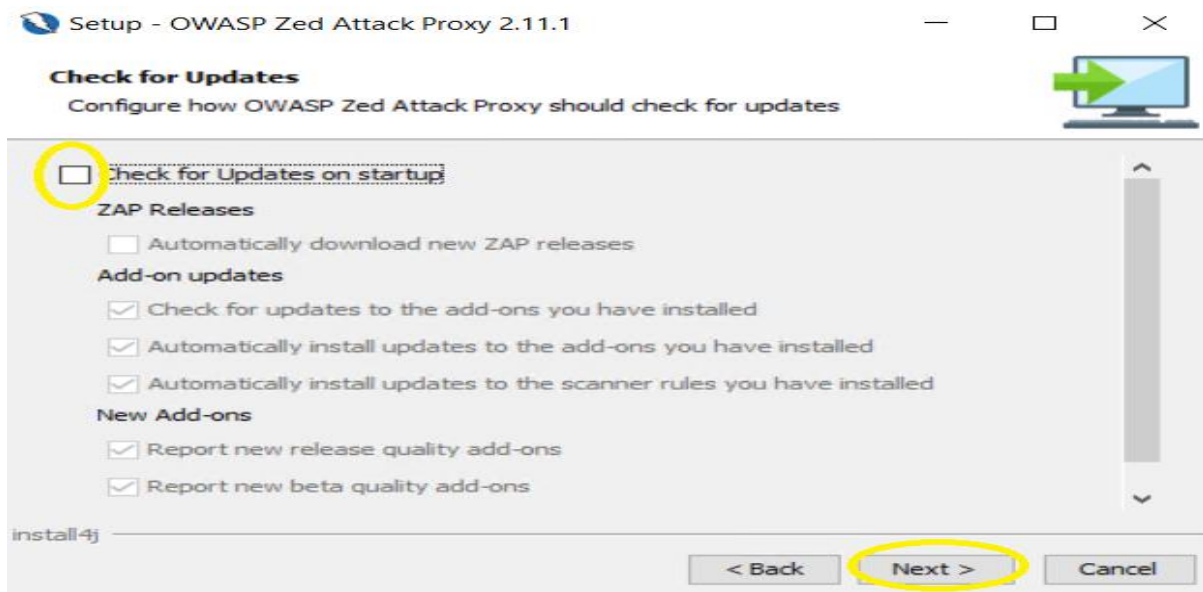
Name:

Register. No.:

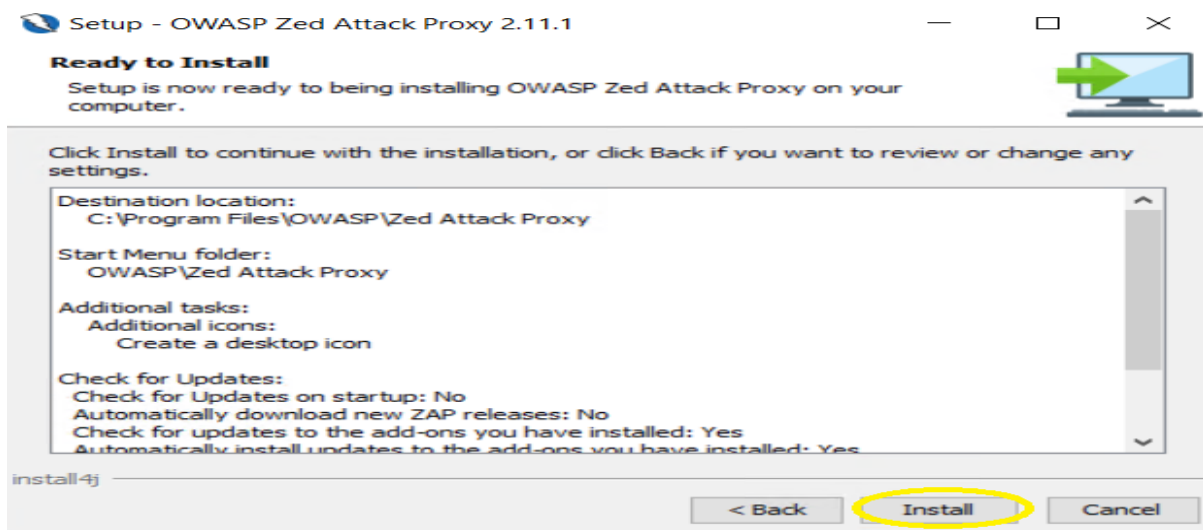
Ex. No:

Date:

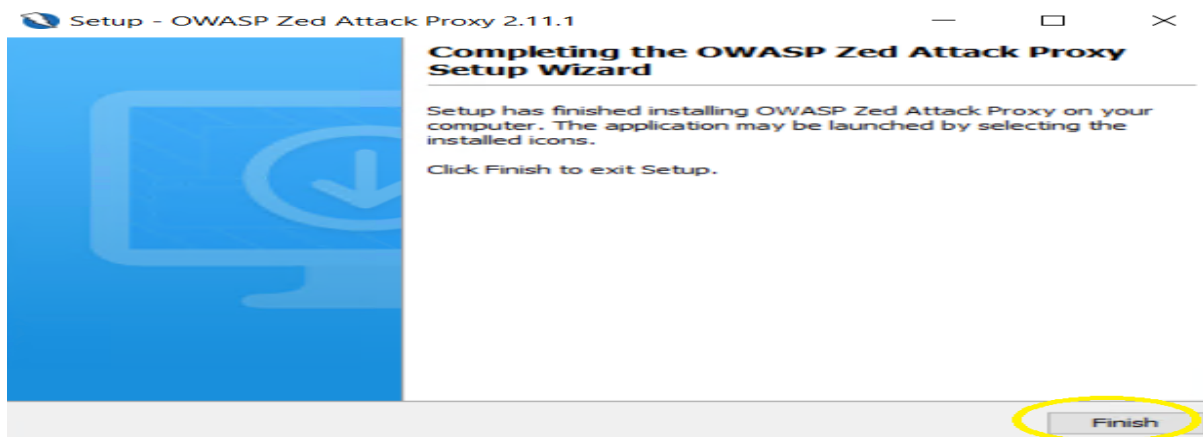
### Step 9: Select updates option



### Step 10: Click on install



### Step 11: Click on finish



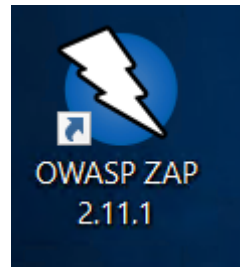
Name:

Register. No.:

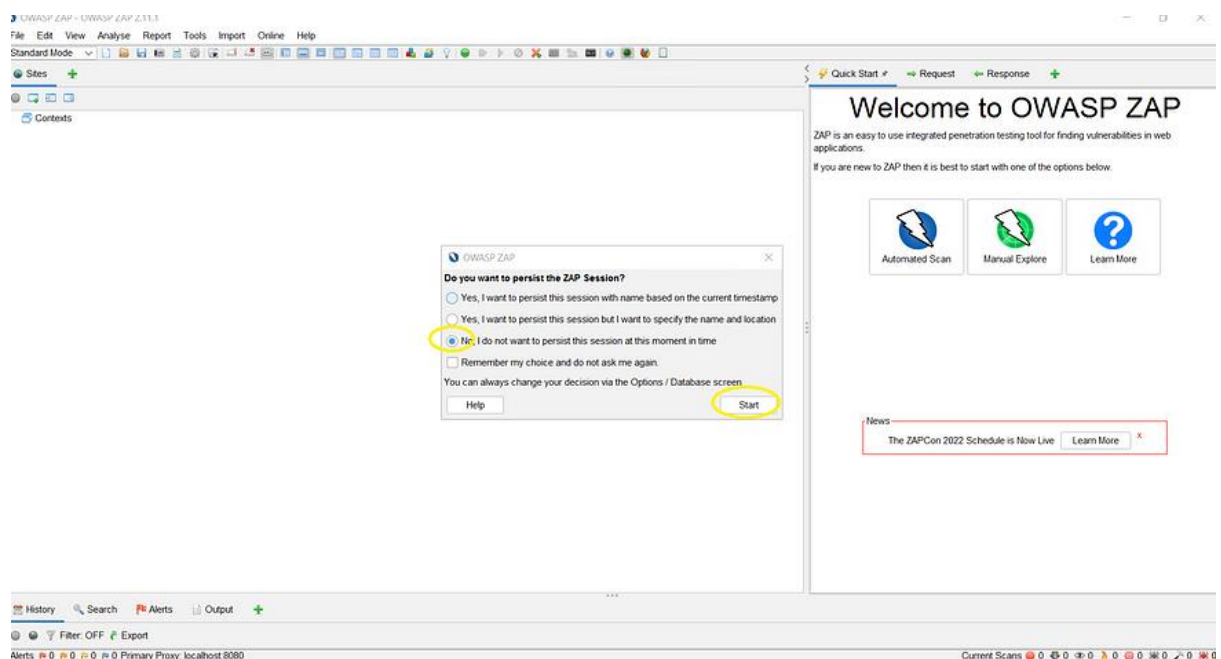
**Ex. No:**

**Date:**

- The installation has completed. Once you click the OWASP/ZAP icon on Windows desktop, OWASP/ZAP UI will be launched.



- Press the No and the Start button.



Note that ZAP requires Java 11+ in order to run. The macOS installer includes an appropriate version of Java but you must install Java 11+ separately for Windows, Linux, and Cross-Platform versions.

**Name:**

**Register. No.:**

Ex. No:

Date:

## Search for Java SE runtime environment 8 downloads

https://www.oracle.com › java › technologies › javase-j... ▼

### Java SE Runtime Environment 8 - Downloads | Oracle United ...

If you want to run Java programs, but not develop them, **download** the **Java Runtime Environment**, or **JRE™**. Important Oracle JDK License Update. The Oracle JDK ...

You've visited this page 4 times. Last visit: 24/07/21

https://www.oracle.com › java › technologies › javase-s... ▼

### Server JRE (Java SE Runtime Environment) 8 Downloads ...

Server **JRE (Java SE Runtime Environment) 8 Downloads**. Thank you for **downloading** this package of the Java™ Platform, Standard Edition **Runtime Environment** ...

https://www.java.com › download › manual ▼

### Java Downloads for All Operating Systems

... **download** page. Get the latest version of the **Java Runtime Environment (JRE)** for Windows, Mac, Solaris, and Linux. ... Recommended Version **8** Update 301.

[Download Java for Windows](#) · [Java Development Kit \(JDK\)](#) · [Windows Offline](#)

» Where can I get Java 7?

JDK

» Looking for the JDK?

**Important Oracle Java License Update**

**The Oracle Java License has changed for releases starting April 16, 2019.**

The new [Oracle Technology Network License Agreement for Oracle Java SE](#) is substantially different from prior Oracle Java licenses. The new license permits certain uses, such as personal use and development use, at no cost -- but other uses authorized under prior Oracle Java licenses may no longer be available. Please review the terms carefully before downloading and using this product. An FAQ is available [here](#).

License and support is available with a low cost [Java SE Subscription](#).




vides the latest OpenJDK release under the open source [GPL License](#) at

g to your operating system from the list below to get the latest Java for your

> [Remove Older Versions](#) > [What is Java?](#)

you acknowledge that you have read and accepted the terms of the [Oracle License Agreement for Oracle Java SE](#)

**Which should I choose?**


 <b>Windows Online</b> filesize: 2 MB	<a href="#">Instructions</a>	After installing Java, you may need to restart your browser in order to enable Java in your browser.
 <b>Windows Offline</b> filesize: 70.72 MB	<a href="#">Instructions</a>	
 <b>Windows Offline (64-bit)</b> filesize: 81.08 MB	<a href="#">Instructions</a>	

[Download Java software for Windows \(64-bit\)](#)

If you use 32-bit and 64-bit browsers interchangeably, you will need to install both 32-bit and 64-bit Java in order to have the Java plug-in for both browsers. » [FAQ about 64-bit Java for Windows](#)

Opening jre-8u301-windows-x64.exe

You have chosen to open:

 **jre-8u301-windows-x64.exe**  
which is: application/x-sdjc (81.1 MB)  
from: <https://sdjc-esd.oracle.com>

**What should Firefox do with this file?**

☐ Open with [Browse...](#)

☒ **Save File**

☐ Do this automatically for files like this from now on.

OK Cancel

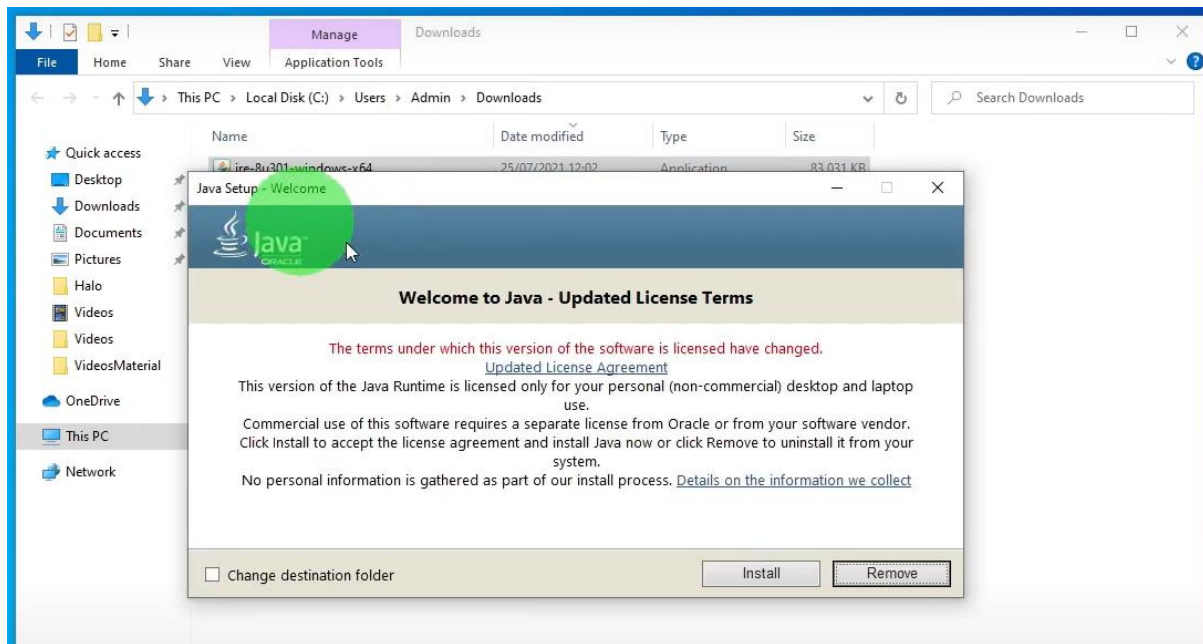
Name:

Register. No.:



**Ex. No:**

**Date:**



<https://www.youtube.com/watch?v=UXS6Bka5fY8>

**Result:**

**Name:**

**Register. No.:**