# VULNERABILITY ASSESSMENT & PENETRATION TESTING


**Author: Sunny Thakur**

# Table of Contents

# What is VAPT?

**V-Vulnerability**

**A-Assessment**

**P-Penetration**

**T-Testing**

## Vulnerability Assessment

A process to evaluate and review key systems, networks and applications. To identify vulnerabilities and configuration issues that may put the organization at risk of being breached or exploited Effective in identifying vulnerabilities, but it cannot differentiate between exploitable vs non exploitable vulnerabilities

## Penetration Testing

Goal-driven test focused on identifying all possible routes of entry an attacker could use to gain unauthorized entry into the target. Identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. Proof of concept strategy to investigate, exploit and validate the extent of the identified vulnerability.

# What is the difference between a Pen Tester and a Hacker?

- Pen Testers have prior approval from Senior Management  Hackers have prior approval from themselves.
- Pen Tester's social engineering attacks are there to raise awareness
- Hackers social engineering attacks are there to trick the DMV into divulging sensitive information about the where abouts of their estranged ex-spouse.
- Pen Tester's war driving = geeks driving cars with really long antennas, license plate reading "r00t3d" while dying their hair green looking to discover the hidden, unapproved networks your users thought it would be OK to install for you.
- Hackers wireless war driving doesn't happen so often because 14 year olds typically don't have their license yet.

# Difference between Penetration Testing and Vulnerability Assessment?

## Vulnerability Assessment:

» Typically is general in scope and includes a large assessment.

» Predictable.

» Unreliable at times and high rate of false positives.

» Vulnerability assessment invites debate among System Admins.

» Produces a report with mitigation guidelines and action items.

## Penetration Testing:

» Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)

» Unpredictable by the recipient. (Don't know the "how?" and "when?")

» Highly accurate and reliable. (I've got root!)

» Penetration Testing = Proof of Concept against vulnerabilities.

» Produces a binary result: Either the team owned you, or they didn't.

**Scope of Penetration Testing**

*Targeted Recon.*

» Targeted exploitation of vulnerable software.

*Social Engineering*

» Hi Help Desk…I'm Mr. Jones…Can you tell me what my password is?

*Physical facilities audit*

» Hmm, I forgot my badge... but there's 200 yards of fence missing on the east side of the center

*Wireless War Driving*

» Detection of rogue or weakly encrypted AP's.

*Dumpster Diving*

» How much fun can I have in the dumpster…whoops…I've found someone's Tax forms with SSN.

# Why Bother?

Active pen-testing teaches you things that security planning will not.

» What are the vulnerability scanners missing?

» Are your users and system administrators actually following their own policies?

» host that claims one thing in security plan but it totally different in reality

» Audit Physical Security

» Just what is in that building no one ever goes in?

» The strongest network based protections are useless if there is a accessible unlocked terminal, unlocked tape vault, etc.

Raises security awareness

- I better not leave my terminal unlocked because I know that those security guys are lurking around somewhere.
- Helps identify weakness that may be leveraged by insider threat or accidental exposure.
- Provides Senior Management a realistic view of their security posture
- Great tool to advocate for more funding to mitigate flaws discovered

- If I can break into it, so could someone else!

# Types of Testing

| | Black-Box<br>*aka close box penetration testing* | Grey-Box<br>*combination of black box and white box testing* | White-Box<br>*aka open box penetration testing* |
|---|---|---|---|
| Goal | Mimic a true cyber attack | Assess an organization's vulnerability to insider threats | Simulate an attack where an attacker gains access to a privileged account |
| Access Level | Zero access or internal information | Some internal access and internal information | Complete open access to applications and systems |
| Pros | Most realistic<br>Testing is performed from point of view of attacker | More efficient than black-box andsaves on time and money<br>Testing is performed from point of view of attacker | More comprehensive, less likely to miss a vulnerability and faster<br>Testing is performed from point of view of attacker |
| Cons | Time consuming and more likely to miss a vulnerability | No real cons for this type of testing | More data (ex, source code) is required to be released to the tester and more expensive |

# Penetration Testing at Ames

- Network Vulnerability Testing
- Web Vulnerability Testing
- Wireless War Driving / Walking
- Phone Network Testing
- Social Engineering Testing
- Walk-throughs and Dumpster Diving
- Physical Security Auditing

## Network Vulnerability Testing

**ABOUT ASSUMPTIONS:**

» We don't want to impact operations, so no DOS, no offensive disabling of IDS/IPS/Firewalls/etc.

» Above assumptions impact tests, so other assumptions made. Consider though, that if you find a vuln that'd allow you to bypass IDS/IPS, that such findings cannot be used as mitigations.

**Rules of Engagement:**

» Consistent with RoE document, we don't perform tests if we think they'll damage/interrupt important work.

» Example: "Damaging" tests turned off in Nessus; SQL injection of production/mission systems; etc

» Notify sysadmins/staff for critical and mission systems of pentest window, so they can be on hand in case of crashes, etc. (Note: Decreases effectiveness but is a necessary trade-off)

# Web Vulnerability Testing

During network testing, check out some of the websites your developers have put together. If possible (in scope), get permission to test sites that contractors run on behalf of NASA.

Remember, many systems now considered 'critical' are web systems throughout. An agency can be 'owned' without touching a router or system, if you nail IFMP (for example)

Seen on one contractor system (the login page):

```
<!-- 0) SQL2K=true
CONN=Provider=SQLOLEDB;server=XXX;database=YYY;uid=ZZZ;
pwd=ZZZ;SQL=undefined  --->
```

- Fuzzers, webapp tests, OWASP. Other testing frameworks are useful here
- Consider metasploit ;)

# Wireless War Driving / Walking

- Is your campus wireless accessible from outside the campus? Have you checked? Can it be cracked?
- Drive the campus w/ Laptops equipped with 802.11, antennas if possible.
- Record any wireless network NOT authorized by the center.
- Shut down if possible!
- Bluetooth? Do the same! See what wireless shares are being broadcast (short-range) from inside locked buildings to the outsides of the building, lab, etc.
- Look for “hpsetup”, “Free Public Wifi” (a worm), “linksys” and others.
- In the future, “MiFi” mobile hotspots in employees' possession are going to become numerous accidental wifi connection points.

## Phone Network Tests

- Phones? Yep, we still use 'em.
- War-dialing: Using a modem to call every number in your block looking for modems/backdoors
  - » Best done at night, or employees may get upset
- Don't forget VOIP services, Skype IDs, etc
- Use CallerID spoofing(Check with legal office) and redirection services (google voice, etc) to try to fool helpdesk staff into revealing information/passwords/etc – or to impersonate helpdesk for others

## Social Engineering / Phishing Tests

- Your users are being socially engineered and phished every day!
- They are falling for it, pretty regularly.
- Send your users a phishing email w/ Remote IP that you monitor
- Check which users download the file
- Go further! Send them a script to run; the script pings a webserver whose logs you monitor.
- Again, see who executes the file.
- Place this file on a USB thumb drive named 'Financials', drop the drive in the cafeteria
- Start a Facebook group... find people on LinkedIn... etc.

Remedial training needed for employees who respond to phsihing!

## Walk-throughs and Dumpster Diving

**Goal: See what kind of sensitive information your employees are leaving in:**

» recycling/trash

» Printer and copy rooms

» Unlocked file cabinets

» Unattended “archival” areas

» Check for unlocked terminals. Check for unlocked but unattended offices w/ sensitive information in them

- Look for macguyvered IT setups in labs, offices, etc

- Use a cell phone w/ GPS tags in camera (iphone style), or GPS camera to take photos of findings. Will help with mapping problem areas, providing feedback to users.

## Physical security auditing

- Test the efficacy of your physical security controls. These are the controls we take for granted!

**Common things to look for:**

» Double doors unpinned (pull n' open)

» Door locks w/ no front plate

» Poorly installed door locks

» Digital door locks with default passcodes, or malfunctioning latch

» Removable floors which extend beyond gateway doors

» Ceilings which don't run "all the way"

» Are your badge reader door locks fail-safe... or fail-open?

» Circuit breakers outside sensitive areas?

## Physical Sec: Safety Considerations

- Safety precautions for pen-test team:
- Buddy system (minimum of 2 testers)
- Have a management "Bosley" for people to contact, and to run confirmation w/ police

- Have cell phone or radio contact with team members at all times

Pre-train for safety:

# High Level Outputs

## Training and awareness

» Birds of a Feather

» Division and Directorate training

» Management awareness

» Reports sent to Senior Management and anyone with a need to know.

» Security Posture reports. What is the centers risk posture?

## Trends for ARC since inception of program:

» Significant decrease in unlocked terminals

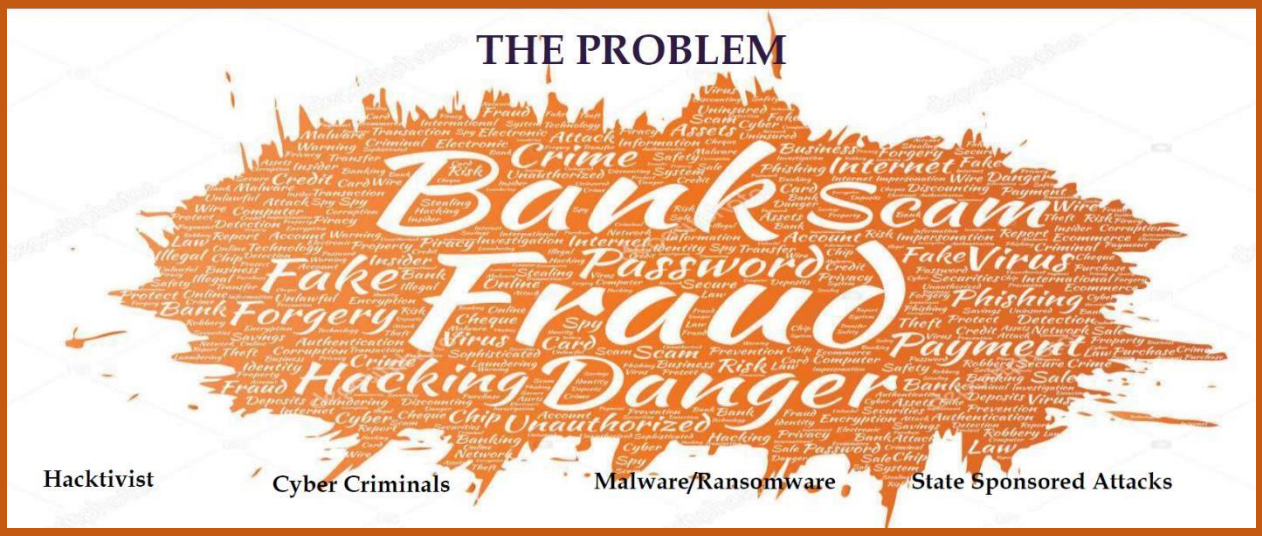
» Increase in reports of Spam & Phishing to Security Office.

» Significant decrease in the amount of Sensitive information being discovered during tests.

» More requests for All-Hands training by the Security Office. »

Significant increase in overall Security Awareness

# Why VAPT?


THE PROBLEM
Bank
Scam
Fraud
Fake
Forgery
Hacking
Danger
Password
Virus
Payment
Phishing
Crime
Internet
Unauthorized
Hacktivist
Cyber Criminals
Malware/Ransomware
State Sponsored Attacks

# Cybersecurity Myths for SMEs

**I have a firewall, so I'm safe from attacks.**

- Hackers understand strategies adopted by a firewall quite well. Disrupting codes and exploiting basic ITboversights to gain access to your system is easy.
- While most cyber security threats are avoidable, your organizations can not rely solely on firewalls for protection.

**I use HTTPS, so my site is secure**

- HTTPs safeguards the transmission of information from source to destination. This is web security at a minimal.
- It does not block attacks like DDoS, brute force, injections, etc.
- There is also the issue of organizations using fake SSL certificates, resulting in their organization being compromised **SMEs are safe because they are not worthwhile targets**
- SMEs are considered to be low hanging fruits for hackers because so many do not take security seriously.
- One of the most popular attacks that hackers use against SMEs is ransomware.

## Audit vs Penetration testing?

| Audit | Penetration testing |
|---|---|
| Check set of standards | Find vulnerabilities |
| - | Foot printing |
| - | Exploiting |
| Create report by standards | Generate report |

# Why do SMEs need VAPT?

## Basic security measures are not enough.

- Firewalls or anti-virus solutions are not sufficient to protect against attacks.

## Security budget

- Unlike MNCs, SMEs do not have the budget to implement everything.
- There is limited or no resource for security expertise.
- What VAPT adds value to is to streamline what is needed for the organization.

## Reputation

- Potential clients or business partners will feel insecure on collaboration.
- Contributing factors can be issues like safeguard of important data.

## SMEs also lose out on potential/existing business.

- Compared to SMEs, larger organizations have a much greater potential to survive an attack due to the help of current investors and existing large clients. (E.g. Sony (04/2011) survived through the attack.)

Phishing attempts and ransomware were the most common methods used.

*https://www.insurancebusinessmag.com/asia/news/breakingnews/smes-hit-by-40-of-cyberattacks-in-singapore-103736.aspx*

**Company: Fortnite / Online Gaming**

In January 2019, it was announced that all 200 Million user accounts on Fortnite had been

compromised through a company-wide data breach.

https://research.checkpoint.com/2019/hacking-fortnite/

**Instagram / Social Media**

On May 20th, 2019, news broke that over 49 million Instagram influencers, celebrities, and companies had large amounts of their personal data compromised.

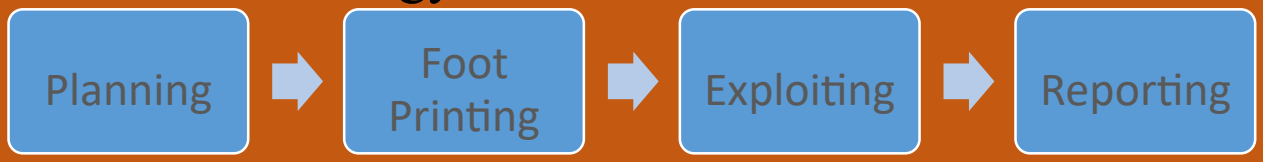
The data compromised included personal telephone numbers, emails, and location data.

https://techcrunch.com/2019/05/20/instagram-influencer-celebrityaccounts-scraped/

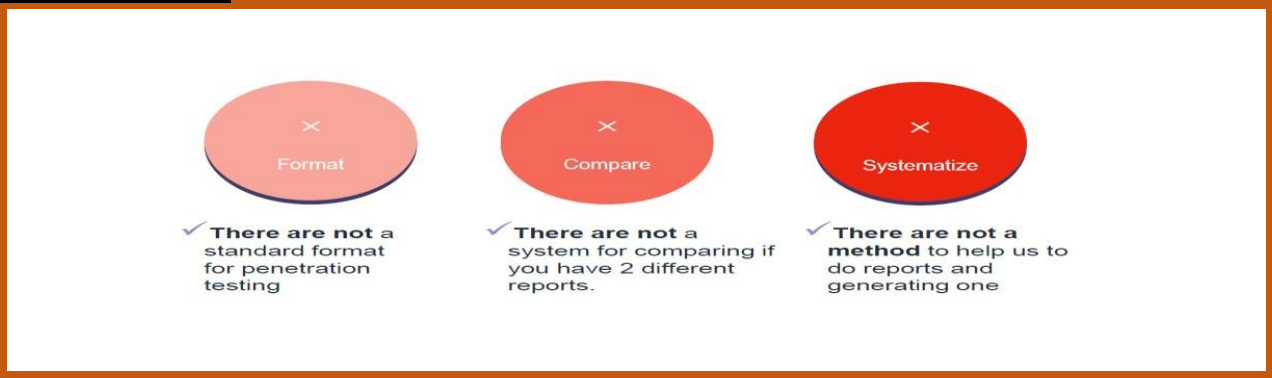
# Methodologies

1. Planning, Discovery, Exploiting, Reporting*
2. Preparation, Anonymity, Foot Printing, Analysis, Exploiting, Reporting, Advisory**
3. Preparation, Reconnaissance, Analysis of Information / Risks, Active Intrusion Attempts, Final Analysis / Clean-Up***
4. Planning, Discovery, Attack, Reporting****

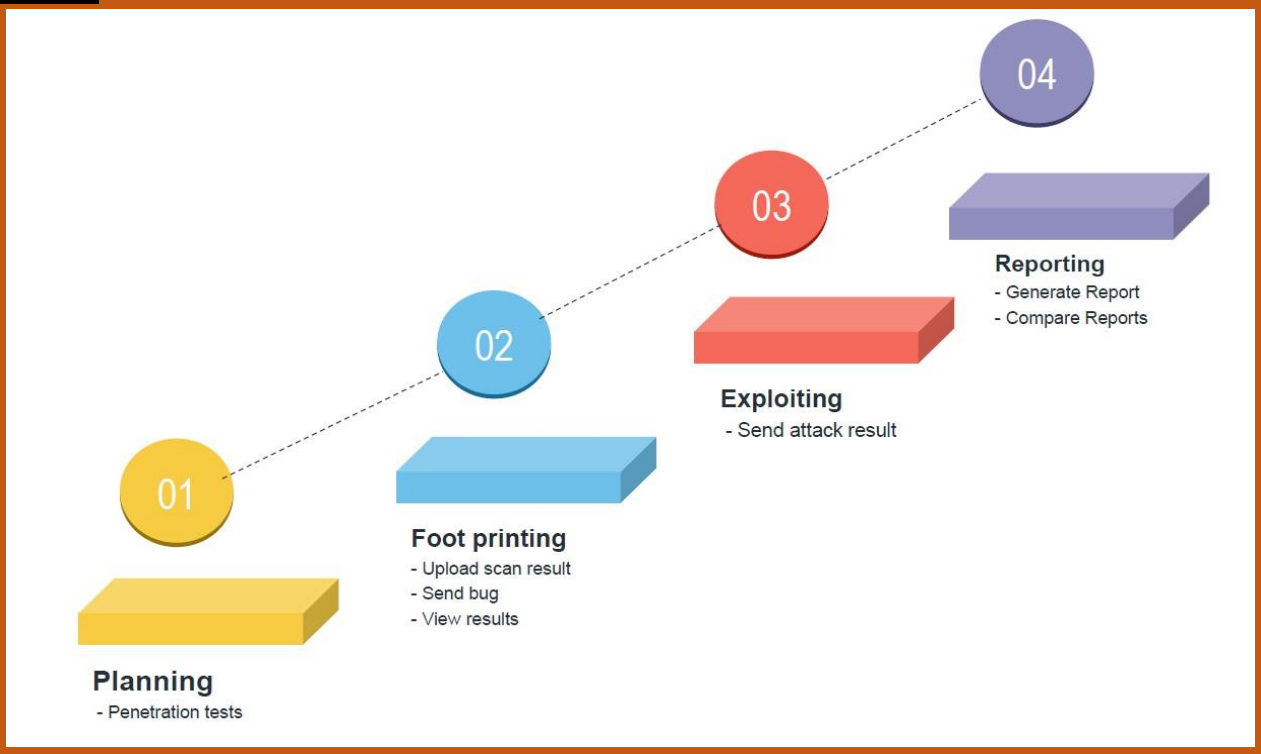
# Used Methodology




## The Problem




## IDEA

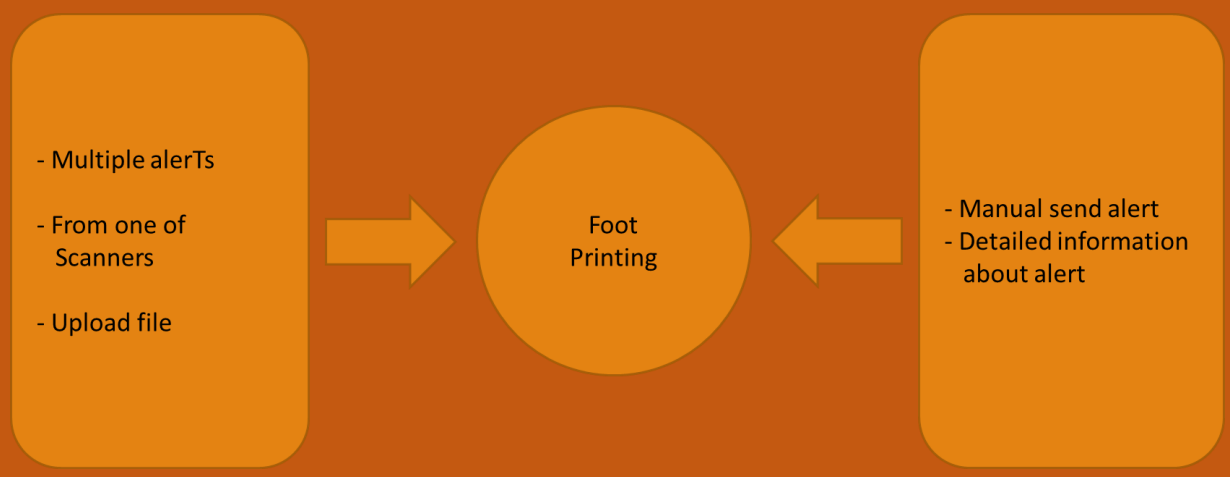


# How to Start ?

## 01. Planning

- Test name
- Scope of Work
- Contract or NDA
- Conduct (Whitebox, Greybox,Blackbox)
- Type (Internal, External, Application-layer, Network-layer) □ Team detail

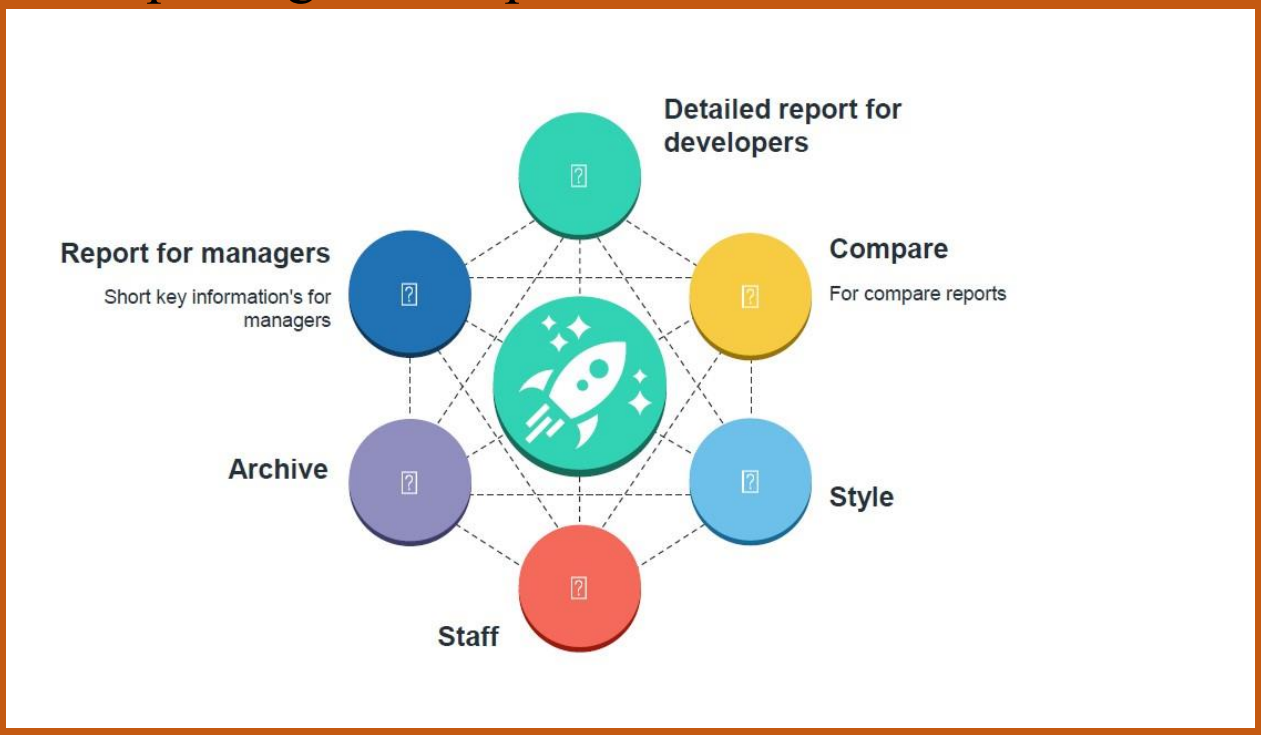
## 02. Foot Printing




## 03. Exploiting

- Alert Level - Low, Medium or High level of alert
- Detailed information about alert

## 04. Reporting & Compare




**Future Work**


# Practical Implementation

# HTTrack

HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility.

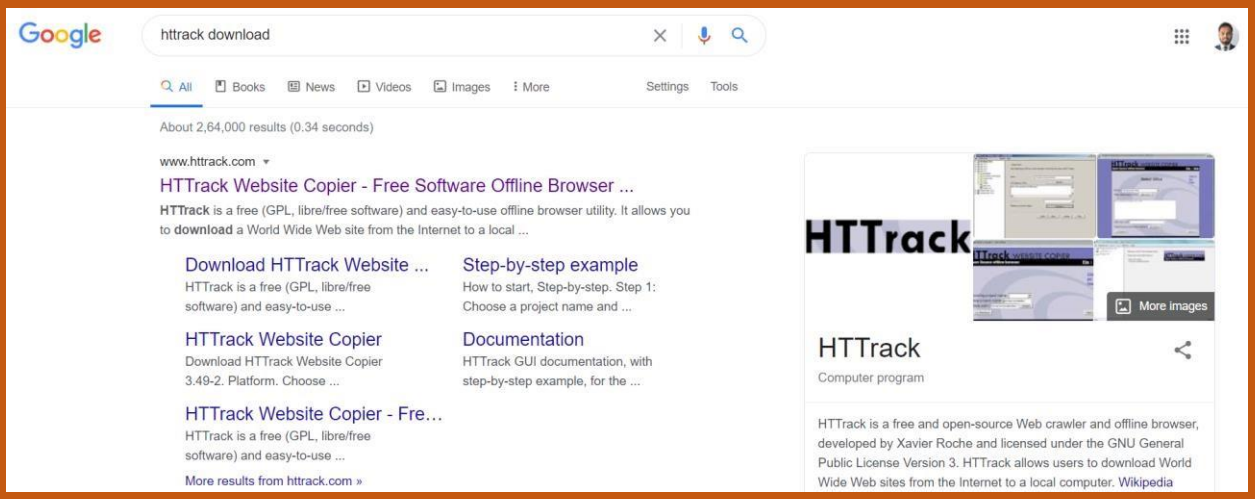
It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

Link to Download Tool for windows.

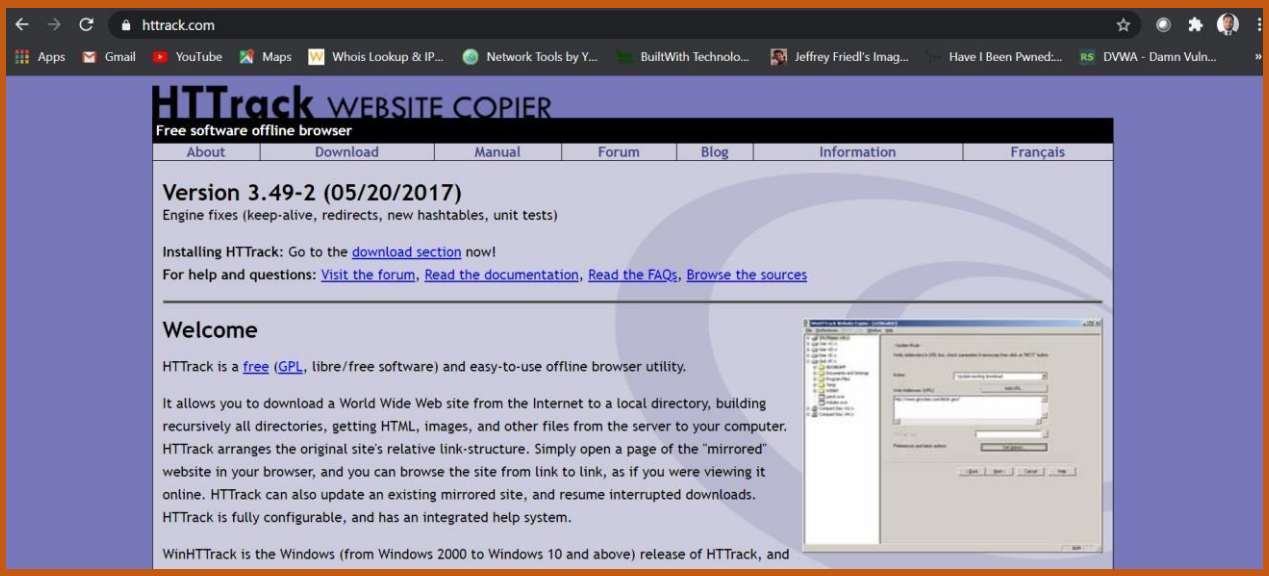
https://www.httrack.com/

# How to Download HTTrack

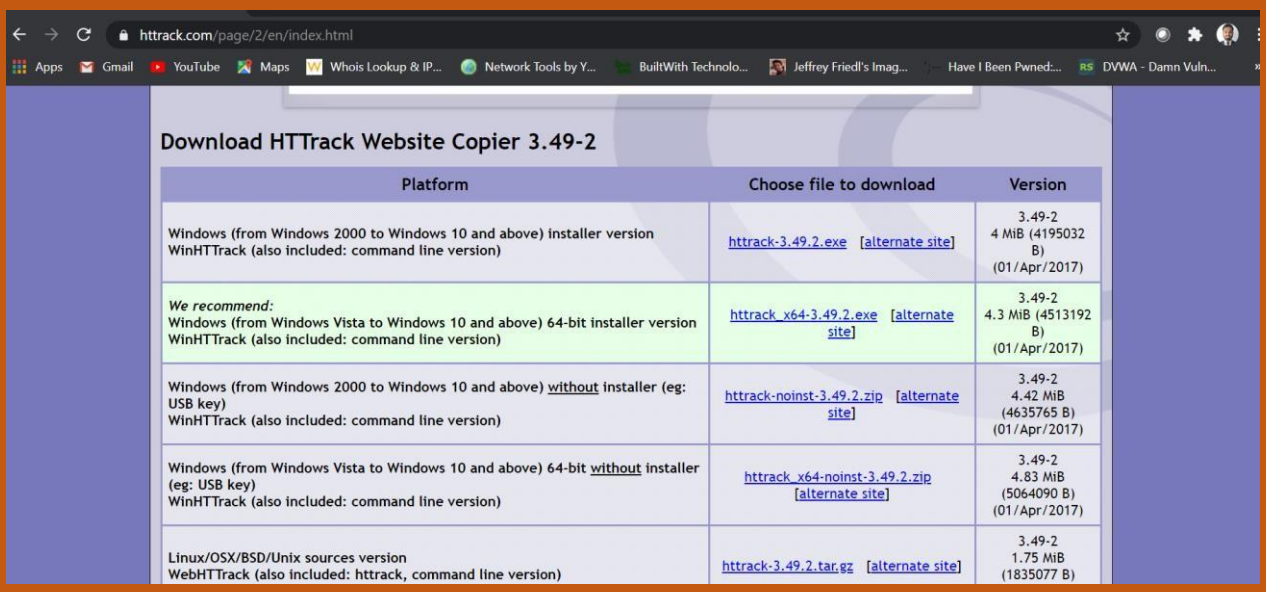
Step 1: Search for Httrack download in google.



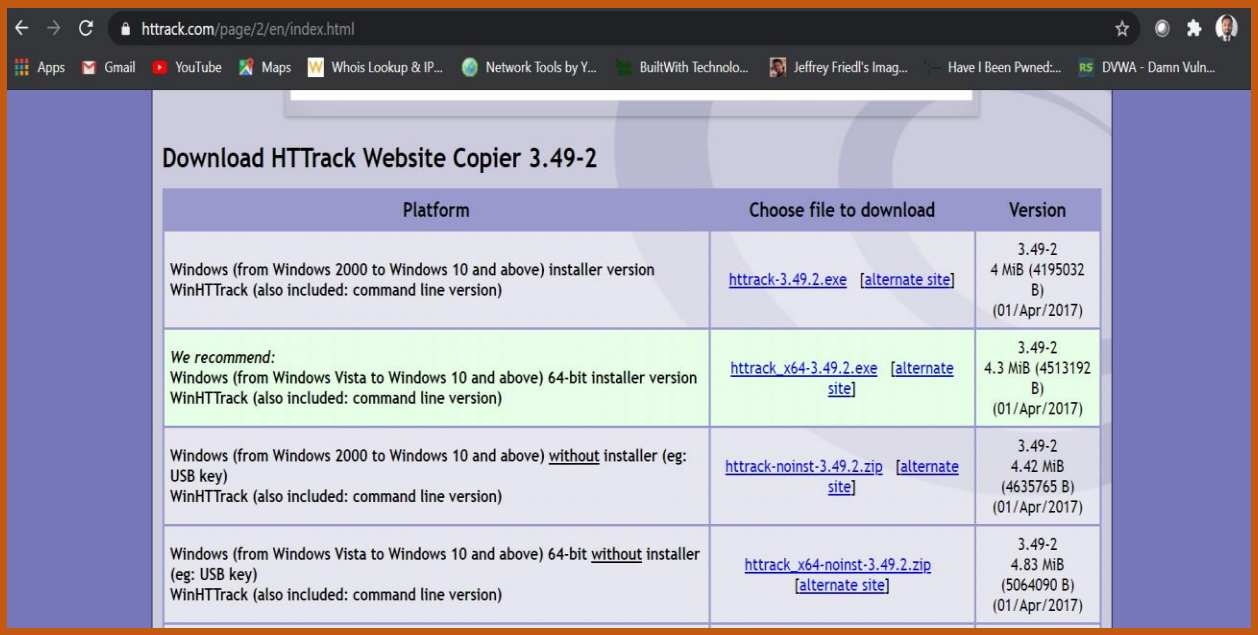

Step 2: Screendump of official website of Httrack.



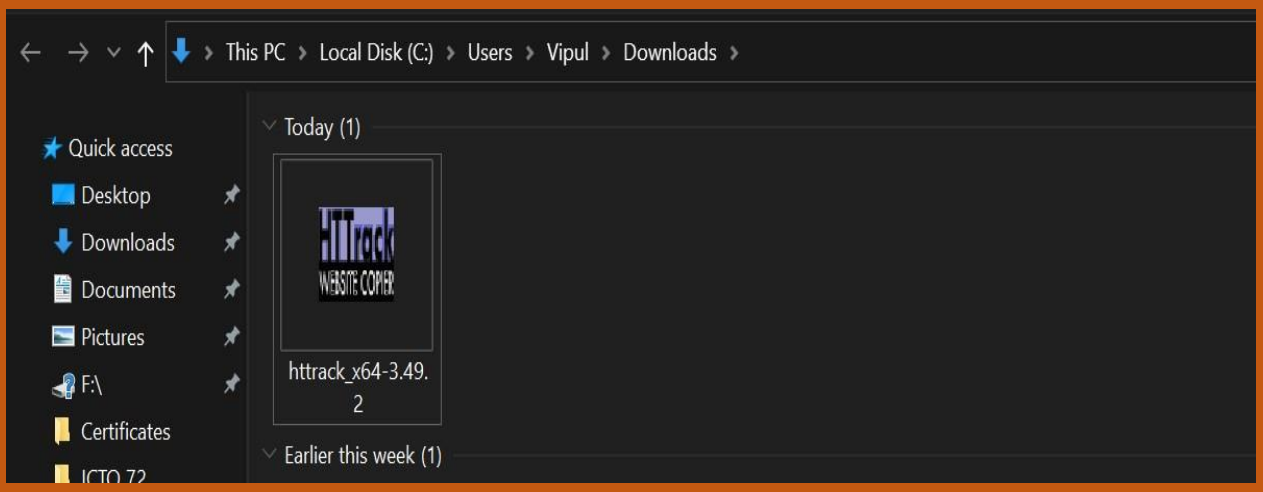

Step 3: Platform and Versions details of HTtracks.




Step 4: Choose the file to download according to system configurations.

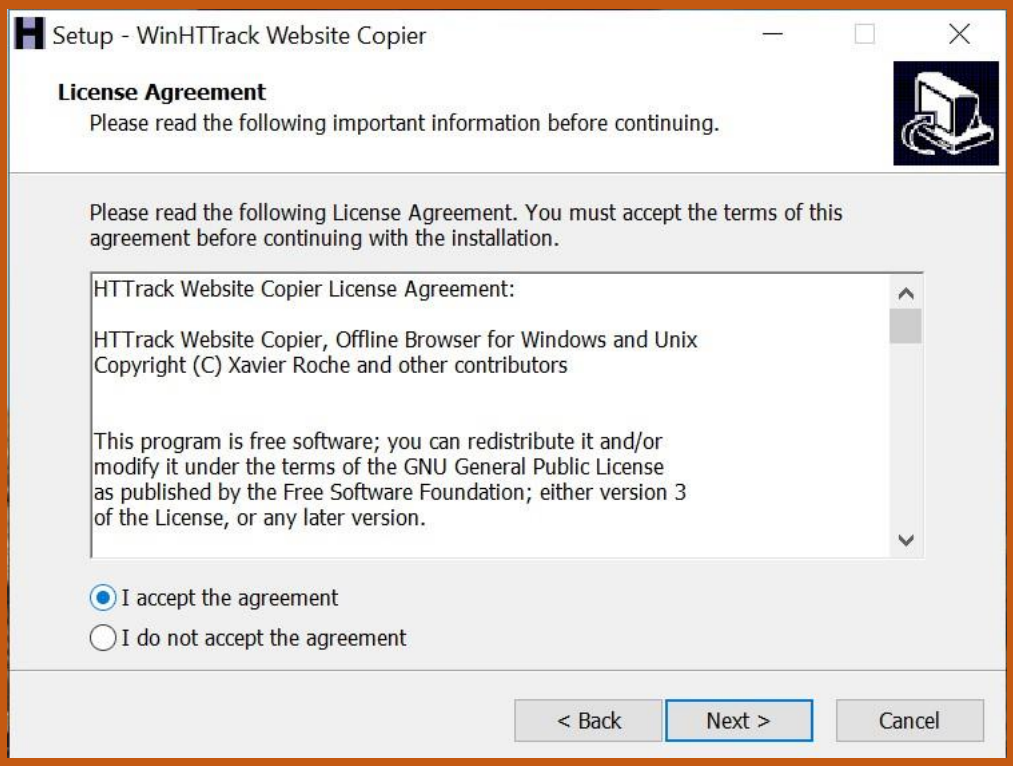



Step 5: After download file with name Httrack appears on download folder of the system.

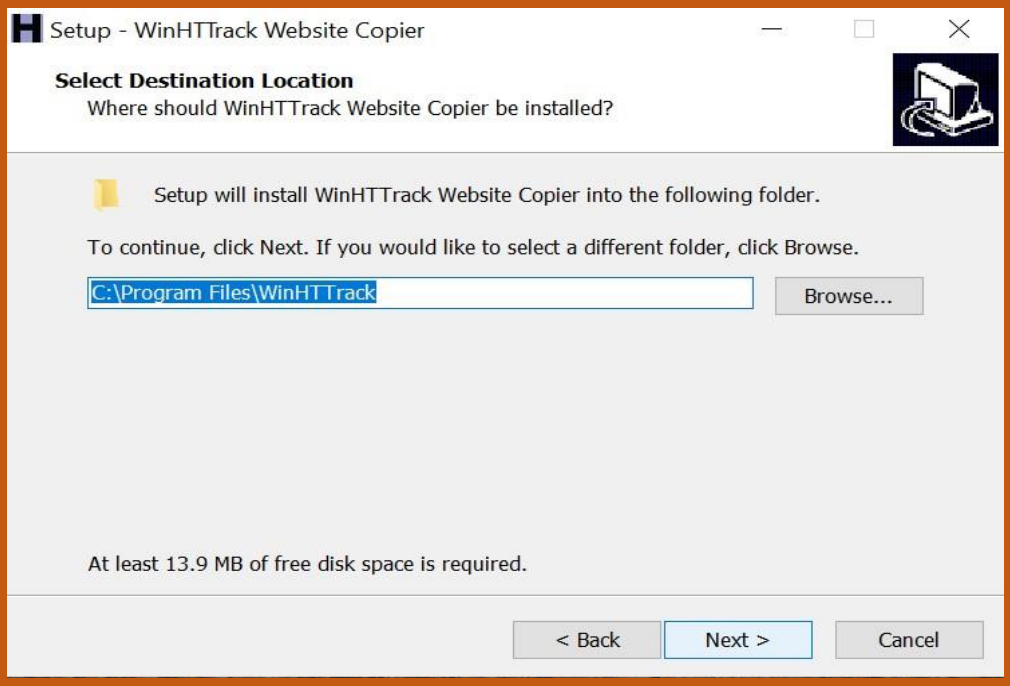



Step 6: Click on NEXT to Install the software.

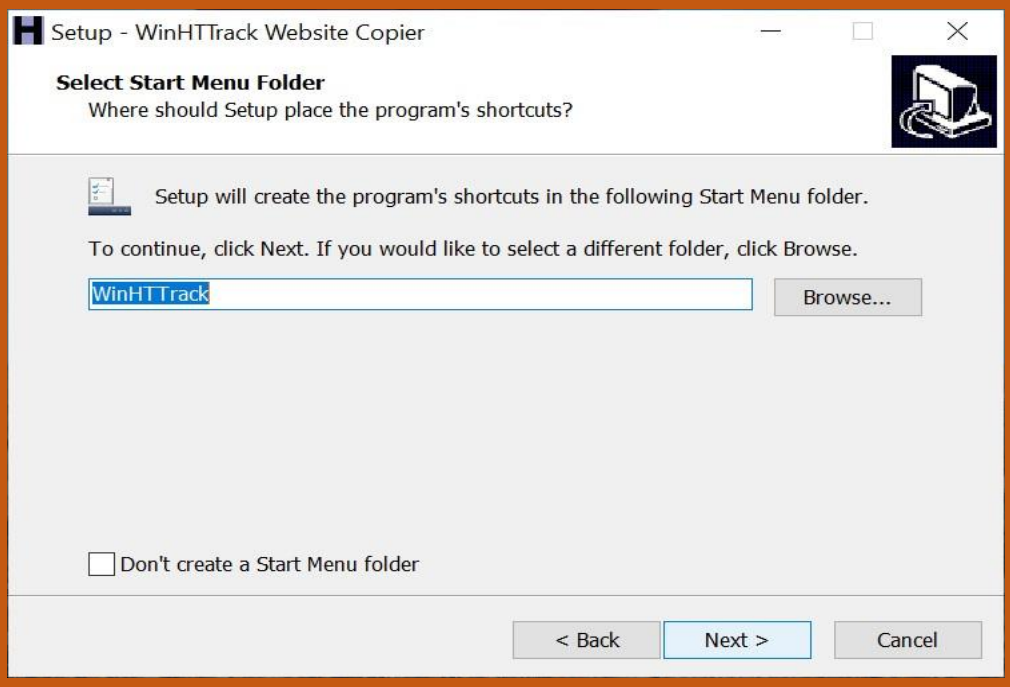

Step 7: Accept the agreement and click on NEXT.



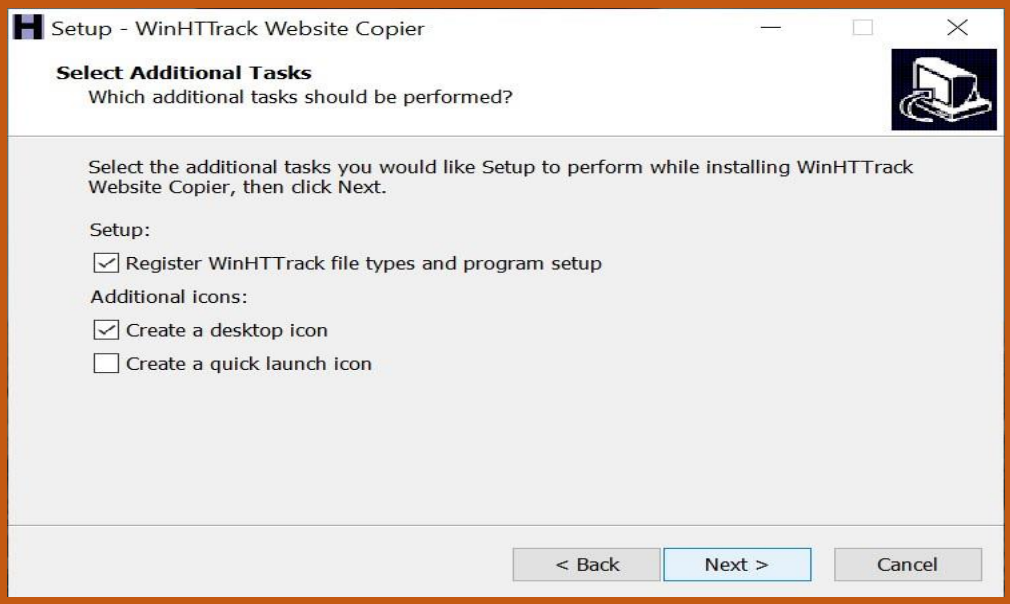

Step 8: Choose the path to INSTALL the file.



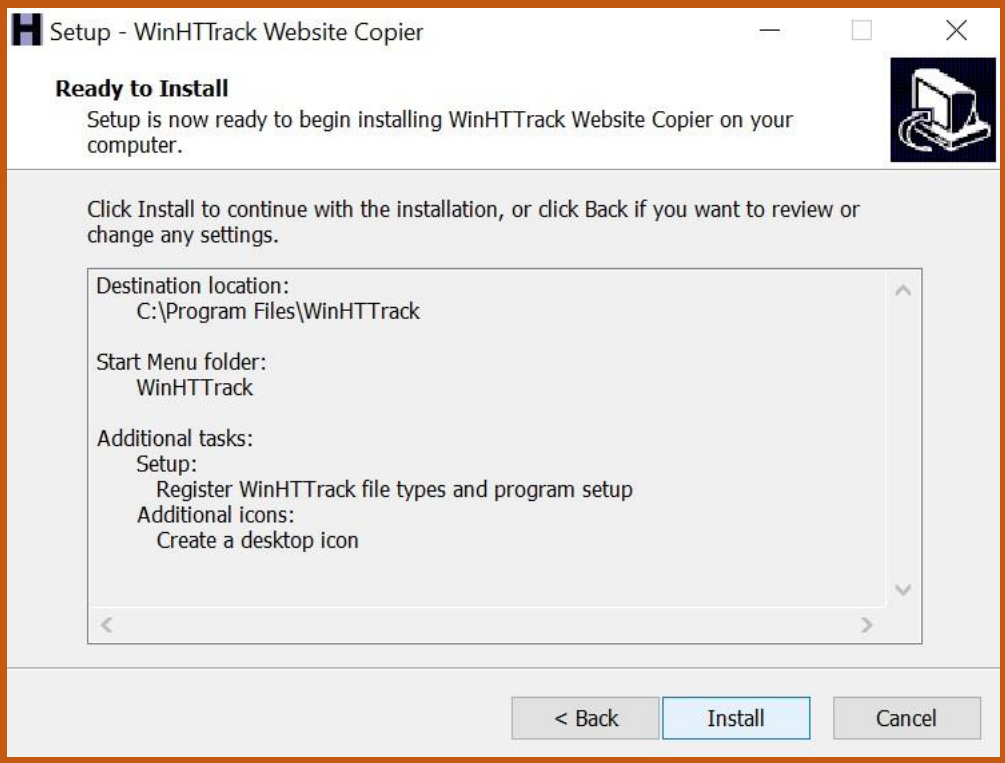

Step 9: Click on NEXT to continue.



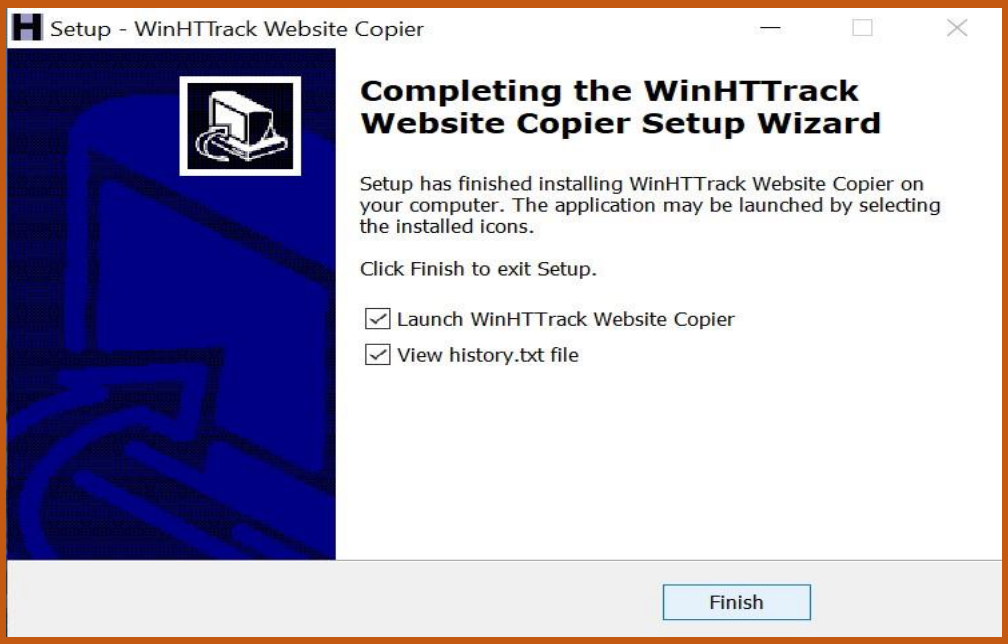

Step 10: Select additional Task and click on NEXT.



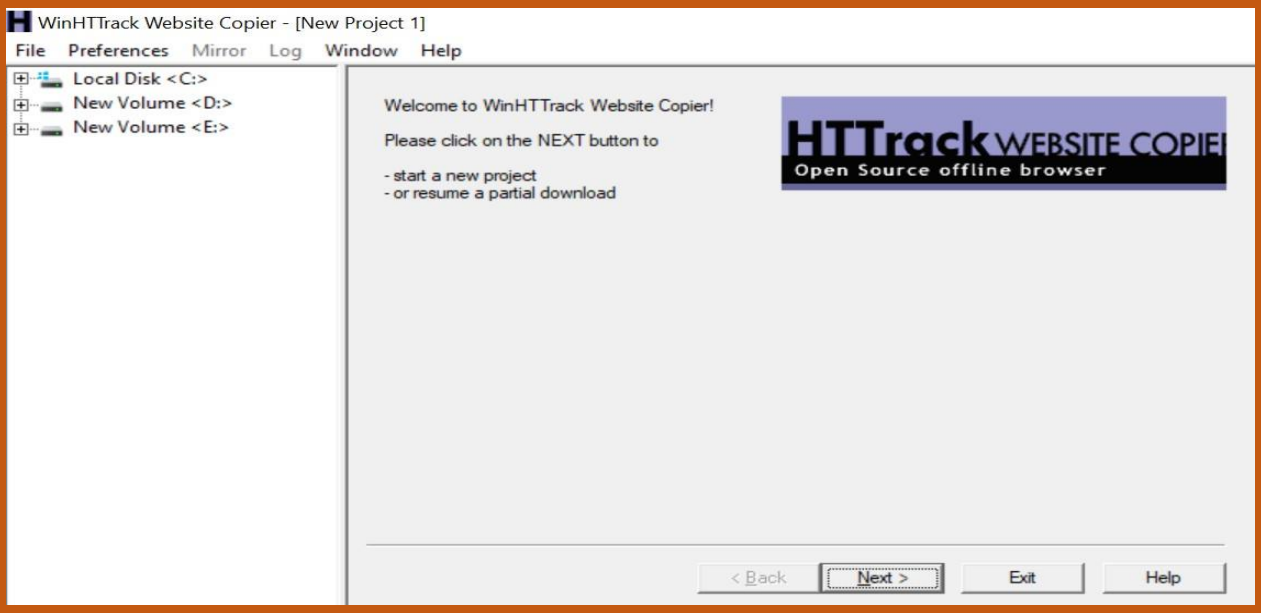

Step 11: Click on INSTALL.



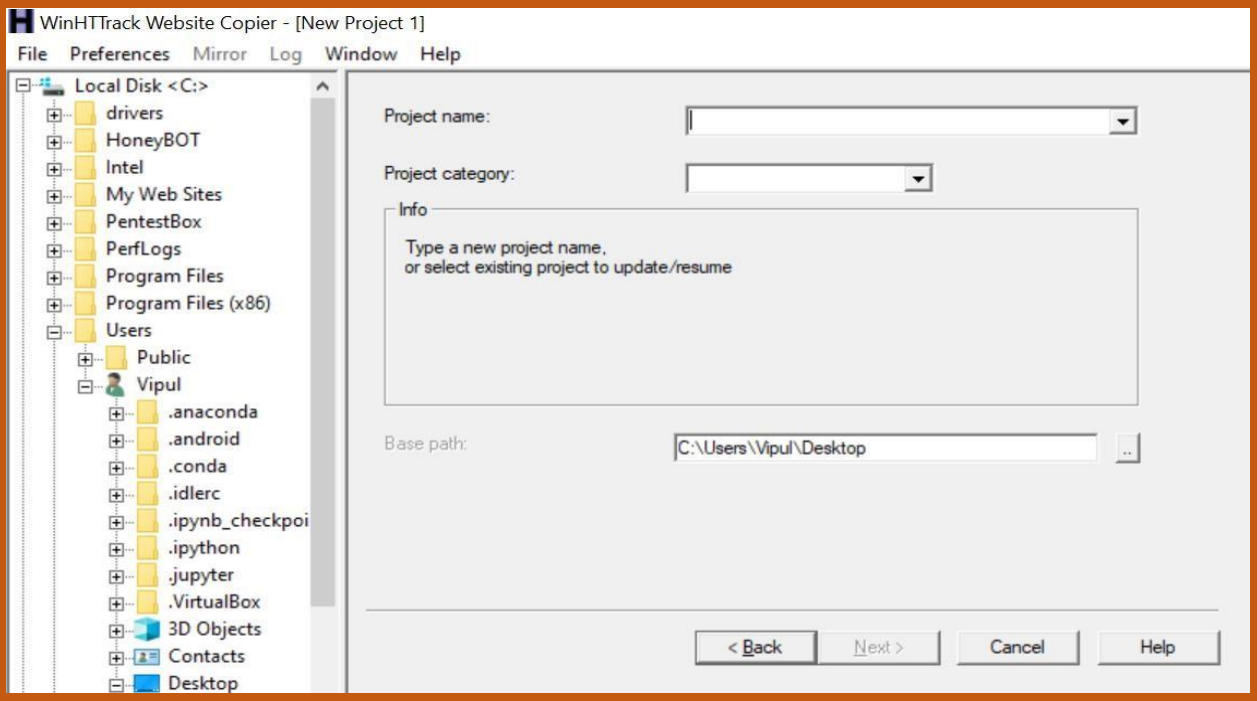

Step 12:Click on FINISH to complete the Setup.



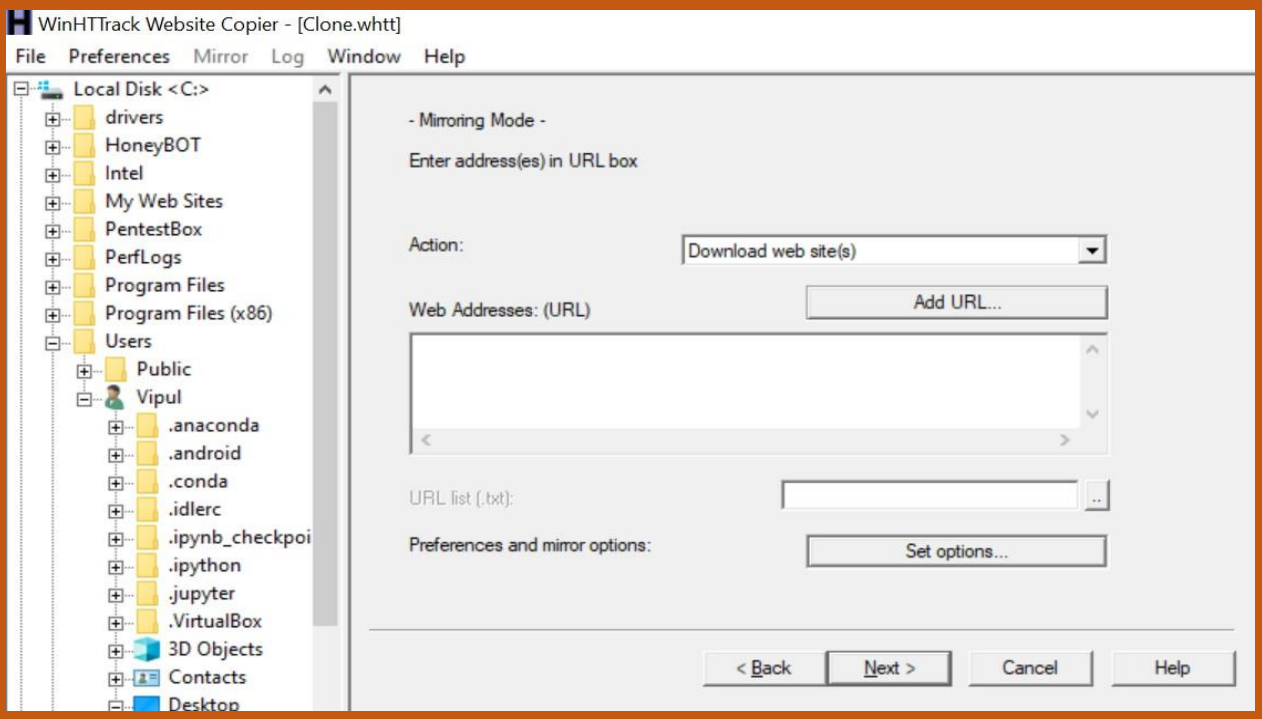

Step 13: Run the file and click on Next.



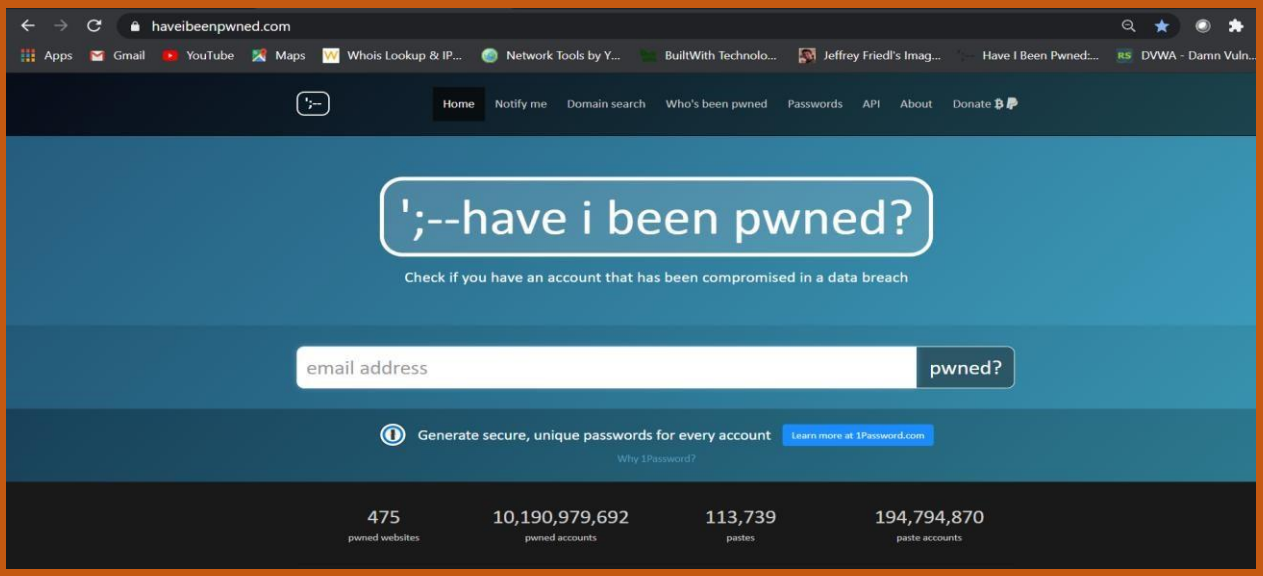

Step 14: Write the Project name and category.



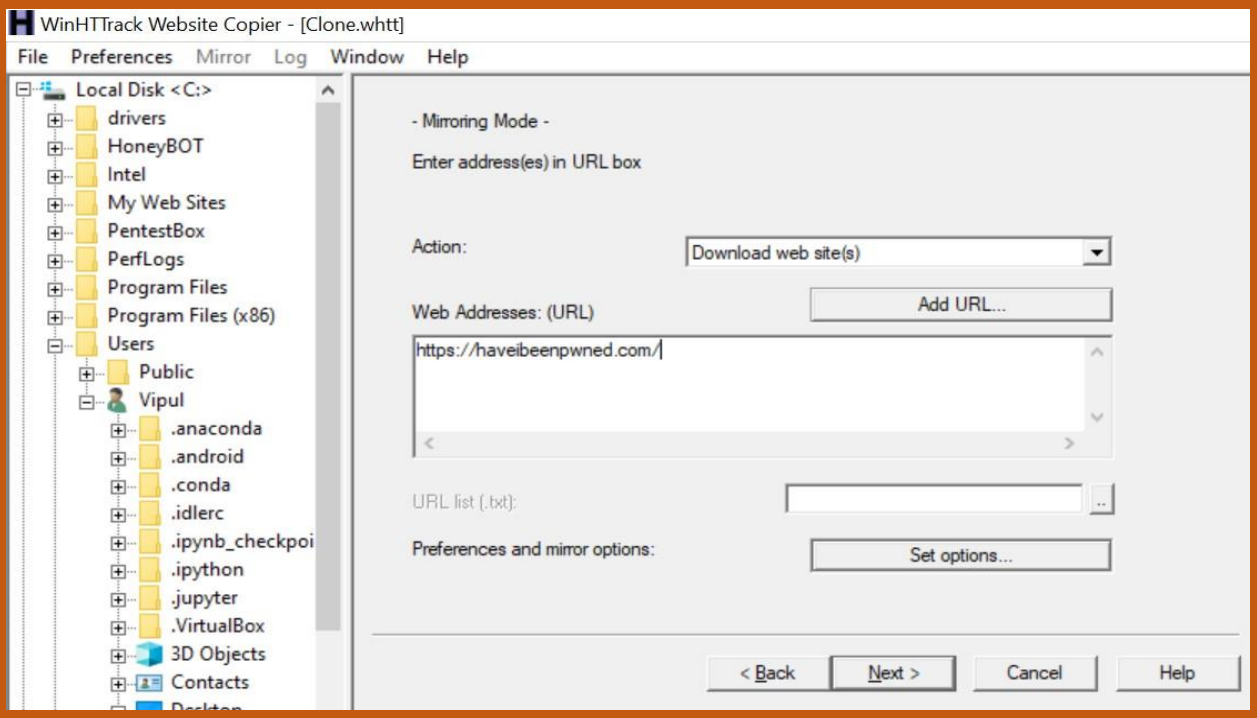

Step 15: Select the Action “Download web site” and click on NEXT.



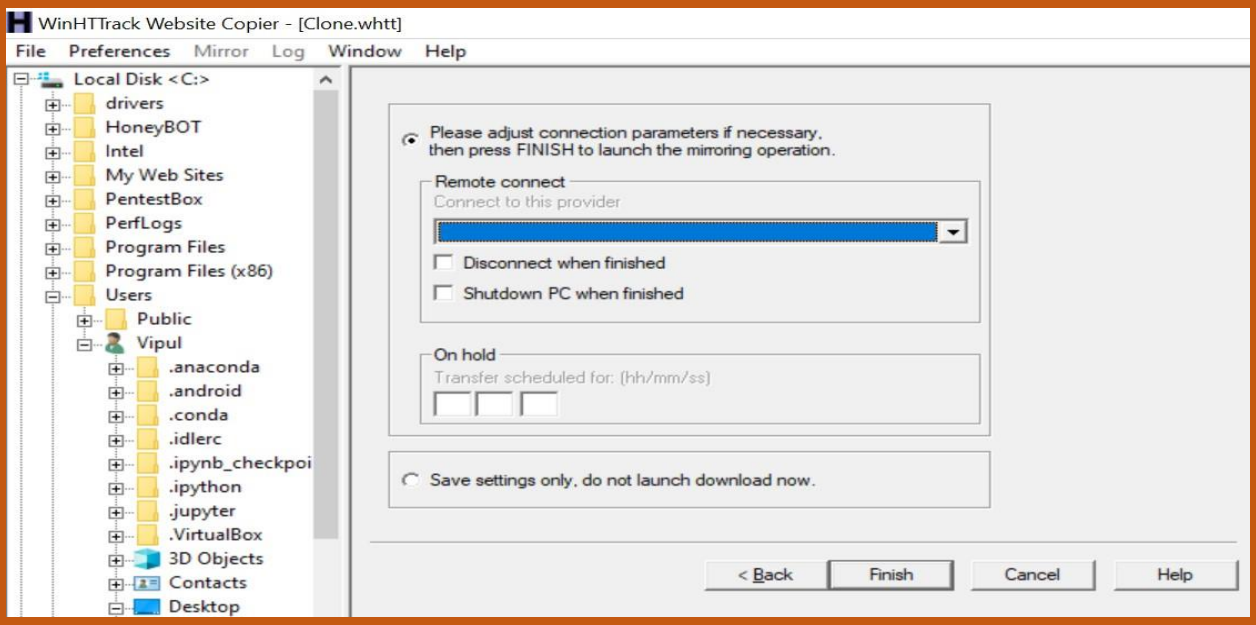

Step 16:Open the website whose clone we want to create.



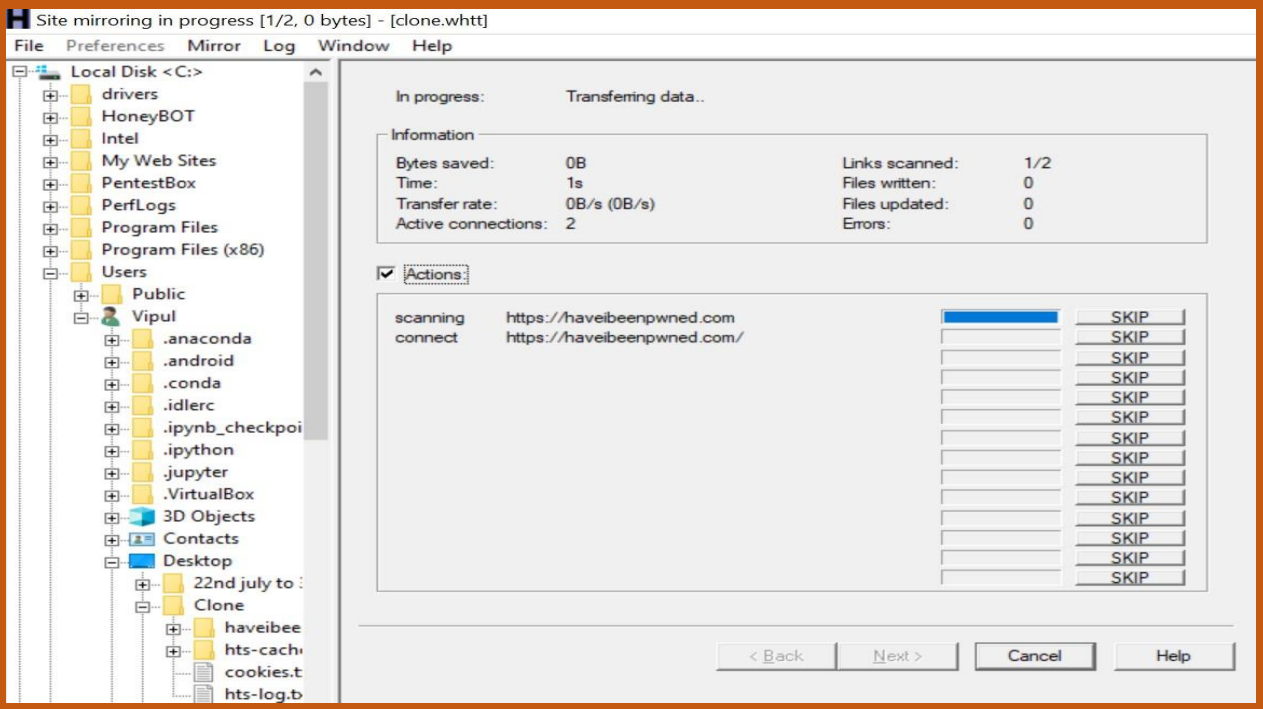

Step 17: Paste the URL of the website to clone and click on NEXT.



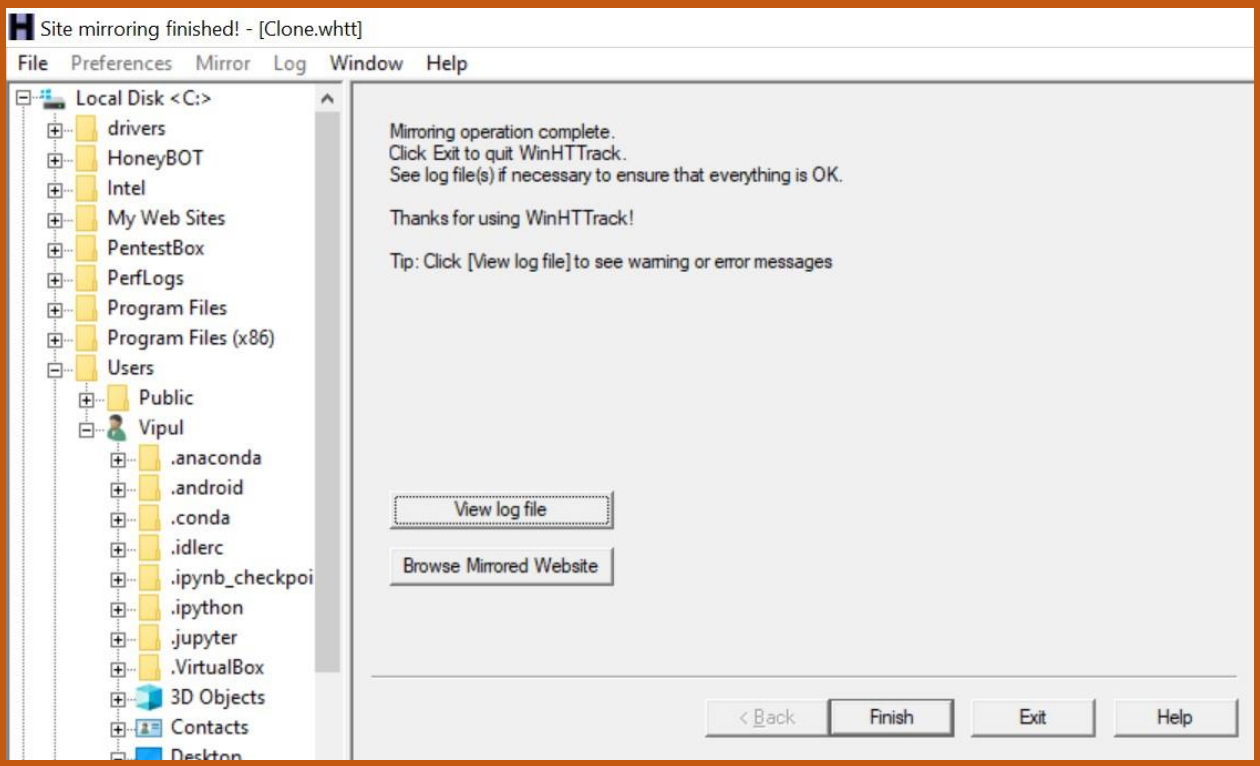

Step 18:Click on FINISH.



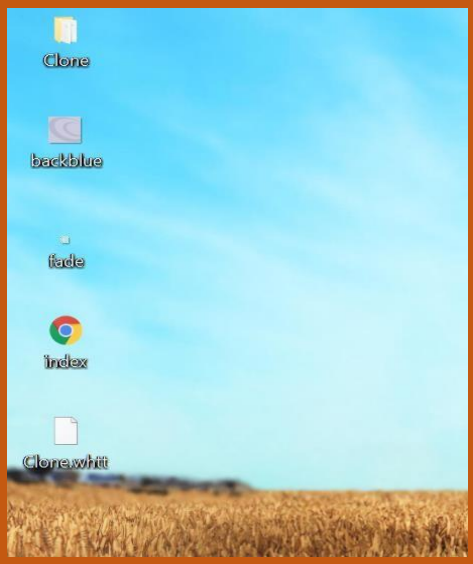

Step 19: Cloning and transferring data will take some time after that click on NEXT.




Step 20:Finally click on Finish to complete the Task.




Step 21: Following folders will be created by HTtrack in the end.




# Introduction to CURL

Curl is small computer utility which is used for transferringdata from various protocols.

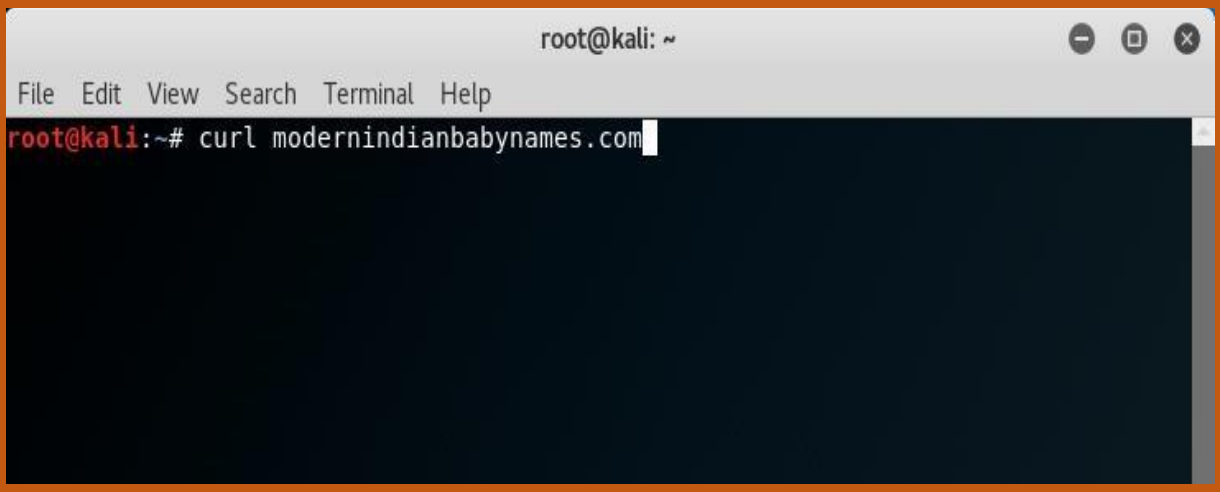
Libs curl is a free client-side URL transfer library.

It support cookies, HTTP, HTTP/2, FTP and Gopher etc.

It also performs SSL certificate verification.

## Steps to Run Curl

Step 1 To connect and fetch the data just write this command in terminal of kali.



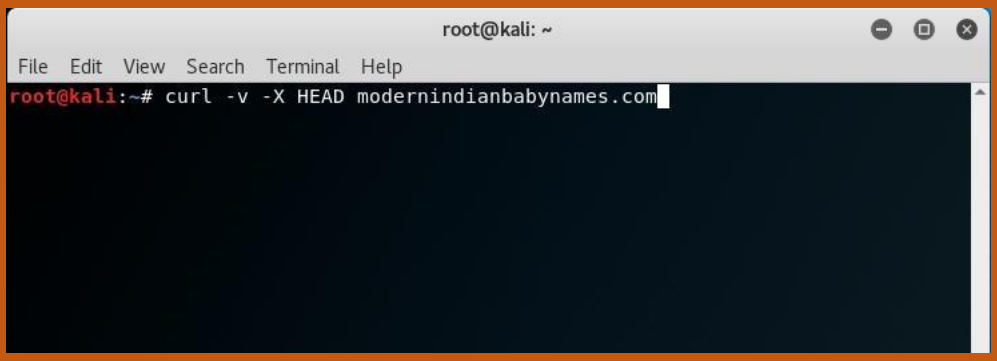

Step 2 Here it is showing the result of the command i.e. curlmodernindianbabynames.com

```
Applications  Places  Terminal                    Fri 00:50
                                  root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# curl modernindianbabynames.com
<!DOCTYPE html>
<!--[if IE 8]><html class="ie ie8"> <![endif]-->
<!--[if IE 9]><html class="ie ie9"> <![endif]-->
<!--[if gt IE 9]><!-->   <html lang="en"> <!--<![endif]-->
<head>
<!-- Basic -->
<meta charset="utf-8">
<title>Modern Indian Baby Names</title>
<meta name="Description" content="Modern Indian Baby Names - The largest Database of most beautiful and modern Hindu, Muslim, Arabic, Sikh, Bengali, English, American, Baby Boy and Gir
l Names along with meanings and search options."/>
<meta name="Keywords" content="Modern, Most, Modren, Beautiful, Meaningful, Meaning, Hindi, Hindu, Indian, Muslim, Arabic, English, American, Unique, Unecxceptional, Unusual, Topmost,
Frequently Used, Sikh, Bengali, Telugu, Sindhi, Punjabi, Kudi, Girl, Boy, Beta Beti, UnCommon, Baby, Names, Babyname, Babynames, Namkaran, Namimg, A, Baby,in, India"/>
<link rel="shortcut icon" href="/images/favicon.ico" type="image/x-icon"/>
<base href="https://www.modernindianbabynames.com/"/>
<meta name="viewport" content="width=device-width,initial-scale=1.0,user-scalable=yes">
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700,800|Shadows+Into+Light" rel="stylesheet" type="text/css">
<link href="https://fonts.googleapis.com/css?family=Concert+One" rel="stylesheet">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link rel="stylesheet" href="https://www.modernindianbabynames.com/css/custom.css"/>
<!-- Head Libs -->
<script src="/js/modernizr.js"></script>
<!--[if IE]>
<link rel="stylesheet" href="/theme/css/ie.css">
<![endif]-->
<!--[if lte IE 8]>
<script src="/theme/vendor/respond.js"></script>
<![endif]-->

<script async src="https://securepubads.g.doubleclick.net/tag/js/gpt.js"></script>
<script>
  window.googletag = window.googletag || {cmd: []};
  googletag.cmd.push(function() {
    googletag.defineSlot('/60931893/tutorial_right_bottom', [300, 250], 'div-gpt-ad-1586272311671-0').addService(googletag.pubads());
    googletag.defineSlot('/60931893/tutorial_right_top', [300, 250], 'div-gpt-ad-1586272393274-0').addService(googletag.pubads());
    googletag.defineSlot('/60931893/home_page_bottom_board', [[1024, 250], [970, 90]], 'div-gpt-ad-1586272111743-0').addService(googletag.pubads());
    googletag.pubads().enableSingleRequest();
    googletag.enableServices();
  });
</script>

<script data-cfasync="false" type="text/javascript">(function(w, d) { var s = d.createElement('script'); s.src = '//delivery.adrecover.com/18107/adRecover.js'; s.type = 'text/javascrip
t'; s.async = true; (d.getElementsByTagName('head')[0] || d.getElementsByTagName('body')[0]).appendChild(s); })(window, document);</script>

<script src="https://www.google-analytics.com/urchin.js" type="text/javascript">
</script>
<script type="text/javascript">
 uacct = "UA-232293-9";
urchinTracker();
</script>
</head>
<body>
<div class="body">
<header>
```

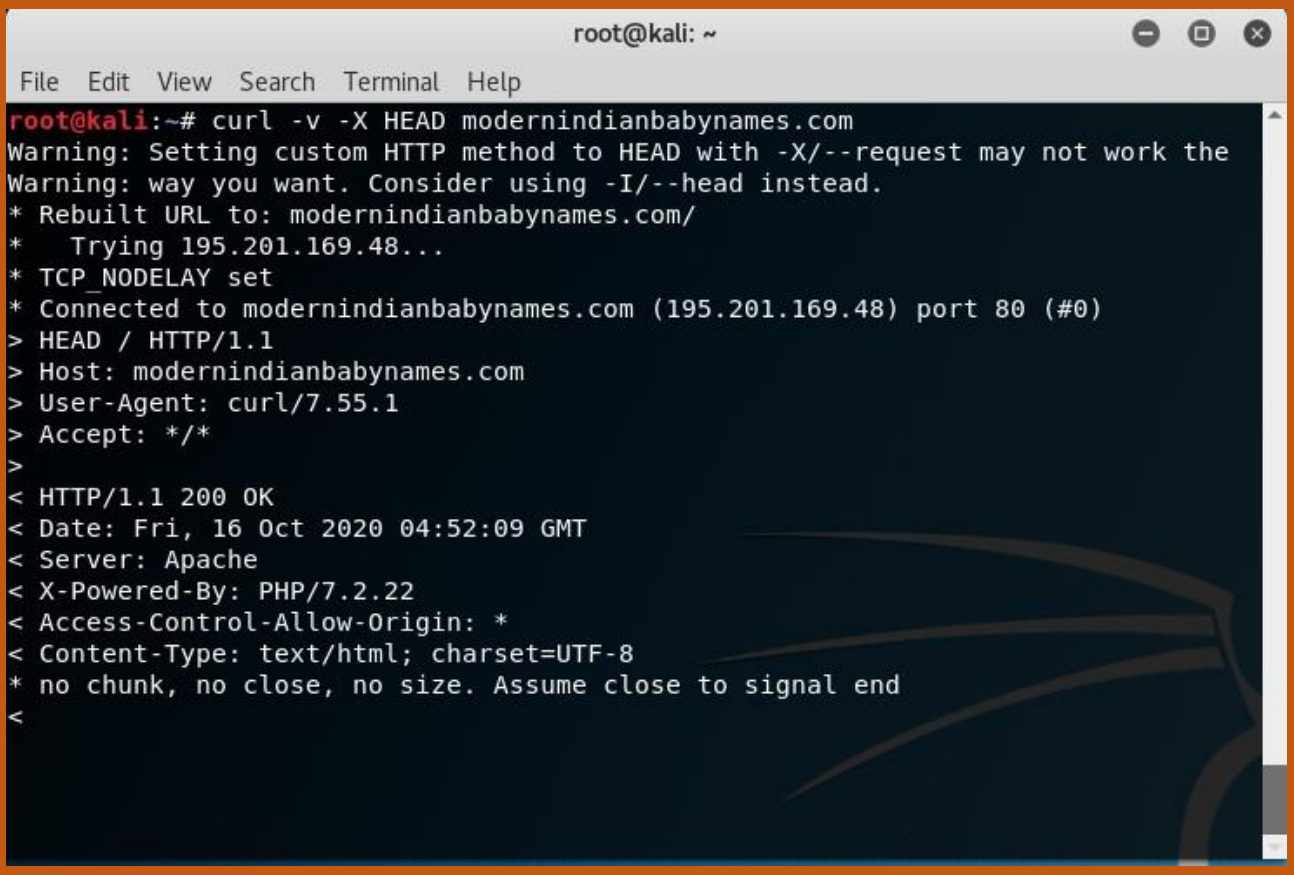
Step 3 Result continue..

```
Applications  Places  Terminal                    Fri 00:50
                                  root@kali: ~
File  Edit  View  Search  Terminal  Help
</form>
</div>
<button class="btn btn-responsive-nav btn-inverse" data-toggle="collapse" data-target=".nav-main-collapse" id="pull">
<i class="fa fa-bars"></i>
</button>
</div>
<div class="navbar-collapse nav-main-collapse collapse">
<div class="container">
<nav class="nav-main mega-menu">
<ul class="nav nav-pills nav-main" id="mainMenu">
   <li class="dropdown">
   <a class="dropdown" href="index.php">
   Home
   <i class="fa fa-home"></i>
   </a>
   </li>
   <li class="dropdown">
   <a class="dropdown" href="hindi_baby_names.php" title="Hindi Baby Names">
   Hindu
   </a>
   </li>
   <li class="dropdown">
   <a class="dropdown" href="arabic_baby_names.php" title="Arabic Baby Names">
   Arabic
   </a>
   </li>
   <li class="dropdown">
   <a class="dropdown" href="sikh_baby_names.php" title="Sikh Baby Names">
   Sikh
   </a>
   </li>
   <li class="dropdown">
   <a class="dropdown" href="biblical_baby_names.php" title="Biblical Baby Names">
   Biblical
   </a>
   </li>
   <li class="dropdown">
```

Step 4 Command if user want to send particular request by using different http method.




Step 5 Here it is showing the result of the command i.e. curl –v –X HEAD modernindianbabynames.com




Step 6 To check the redirection we use the command i.e. curl google.com

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# curl google.com
```

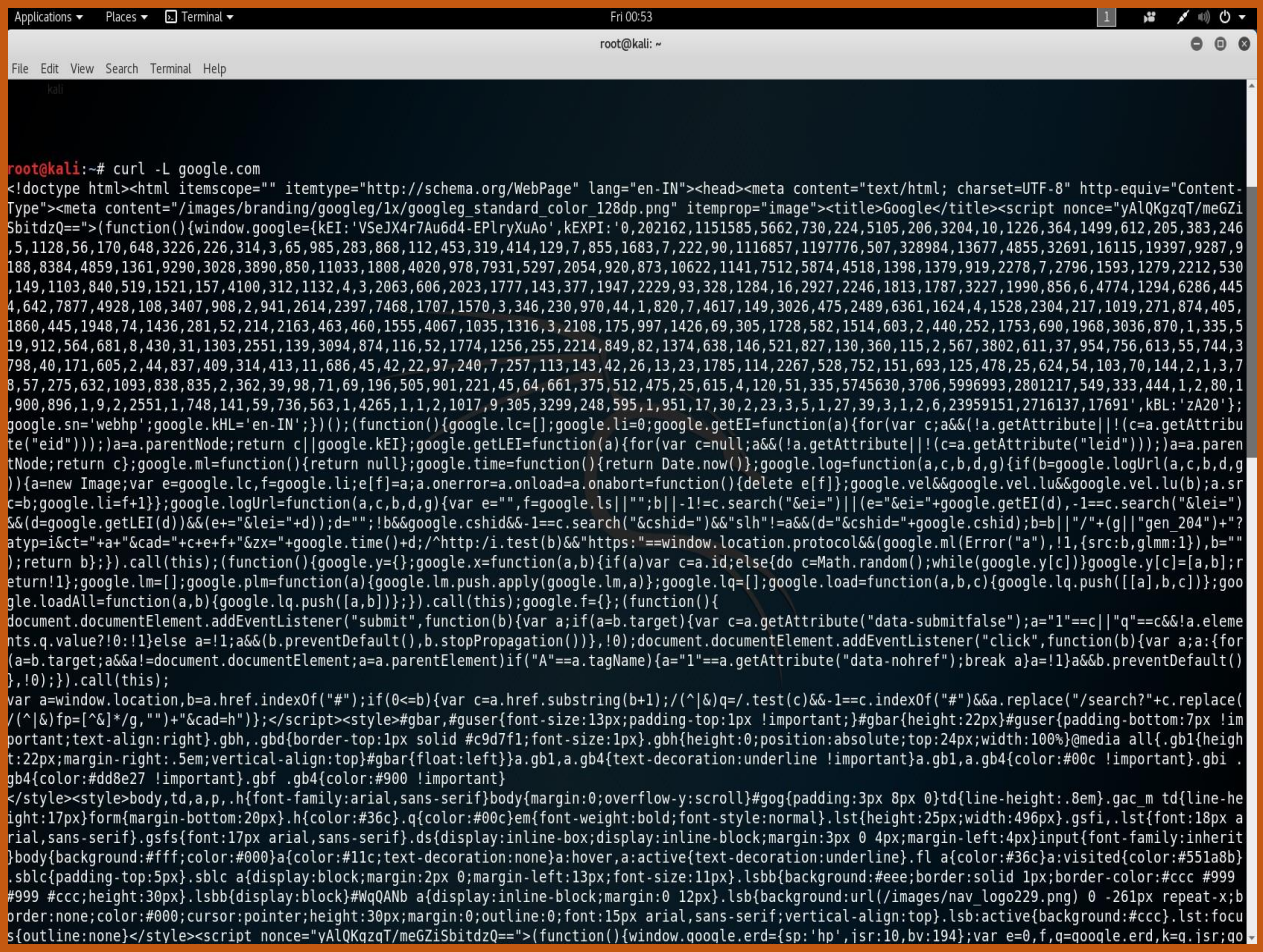
Step 7 Here the result of the command 301 and 301 Moved means it is redirected.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
root@kali:~#
```

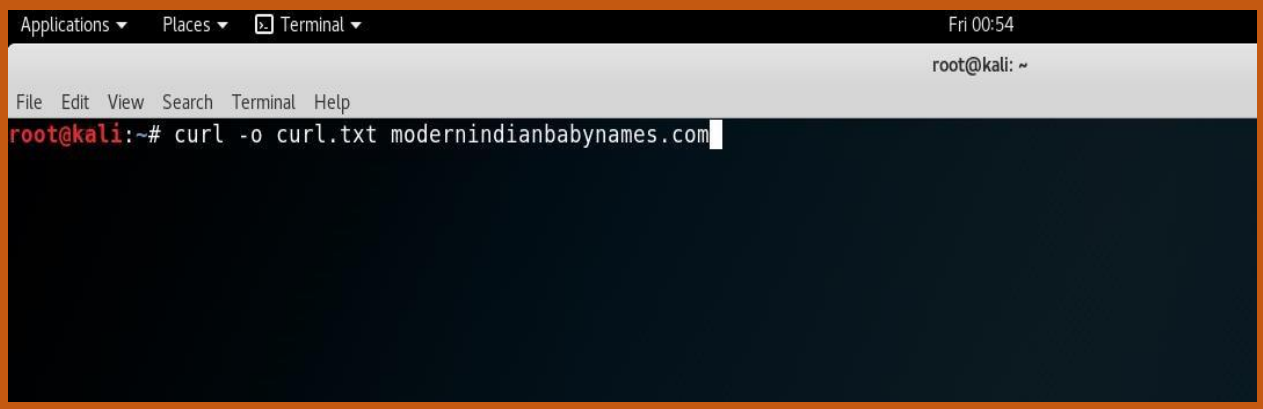
Step 8 To get the details of redirected website we use the command i.e. curl –L google.com

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# curl -L google.com
```

Step 9 Here it is showing the result of the command




Step 10 We use this command to save the websites HTML Content.




Step 11 Result of the command showing total 29859 files saved.

```
Applications ▾   Places ▾   Terminal ▾                                   Fri 00:54
                                                                        root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# curl -o curl.txt modernindianbabynames.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 29859    0 29859    0     0  29859      0 --:--:-- --:--:-- --:--:-- 35004
root@kali:~#
```

Step 12 To view the details of downloaded files use the command vim curl.txt

```
Applications ▾   Places ▾   Terminal ▾                                   Fri 00:55
                                                                        curl.txt (~) - VIM
File  Edit  View  Search  Terminal  Help
<!DOCTYPE html>
<!--[if IE 8]><html class="ie ie8"> <![endif]-->
<!--[if IE 9]><html class="ie ie9"> <![endif]-->
<!--[if gt IE 9]><!-->   <html lang="en"> <!--<![endif]-->
<head>
<!-- Basic -->
<meta charset="utf-8">
<title>Modern Indian Baby Names</title>
<meta name="Description" content="Modern Indian Baby Names - The largest Database of most beautiful and modern Hindu, Muslim, Arabic, Sikh, Bengali, En
glish, American, Baby Boy and Girl Names along with meanings and search options."/>
<meta name="Keywords" content="Modern, Most, Modren, Beautiful, Meaningful, Meaning, Hindi, Hindu, Indian, Muslim, Arabic, English, American, Unique, U
necxceptional, Unusual, Topmost, Frequently Used, Sikh, Bengali, Telugu, Sindhi, Punjabi, Kudi, Girl, Boy, Beta Beti, UnCommon, Baby, Names, Babyname,
Babynames, Namkaran, Namimg, A, Baby,in, India"/>
<link rel="shortcut icon" href="/images/favicon.ico" type="image/x-icon"/>
<base href="https://www.modernindianbabynames.com/"/>
<meta name="viewport" content="width=device-width,initial-scale=1.0,user-scalable=yes">
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700,800|Shadows+Into+Light" rel="stylesheet" type="text/css">
<link href="https://fonts.googleapis.com/css?family=Concert+One" rel="stylesheet">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link rel="stylesheet" href="https://www.modernindianbabynames.com/css/custom.css"/>
<!-- Head Libs -->
<script src="/js/modernizr.js"></script>
<!--[if IE]>
<link rel="stylesheet" href="/theme/css/ie.css">
<![endif]-->
<!--[if lte IE 8]>
<script src="/theme/vendor/respond.js"></script>
<![endif]-->

<script async src="https://securepubads.g.doubleclick.net/tag/js/gpt.js"></script>
<script>
  window.googletag = window.googletag || {cmd: []};
```