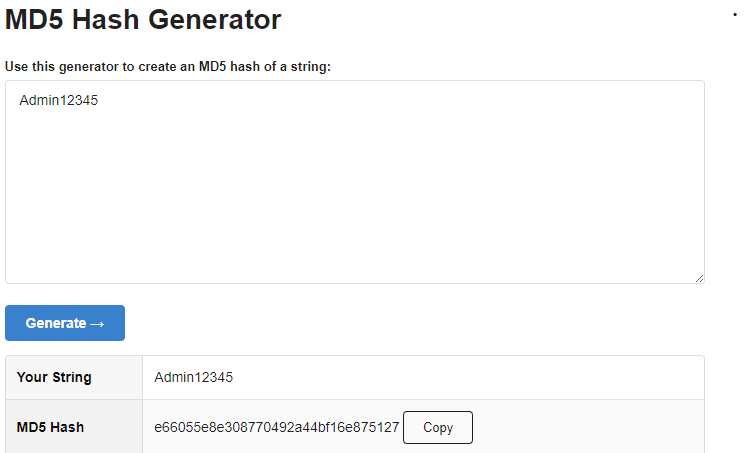
**3A. Password Cracking**

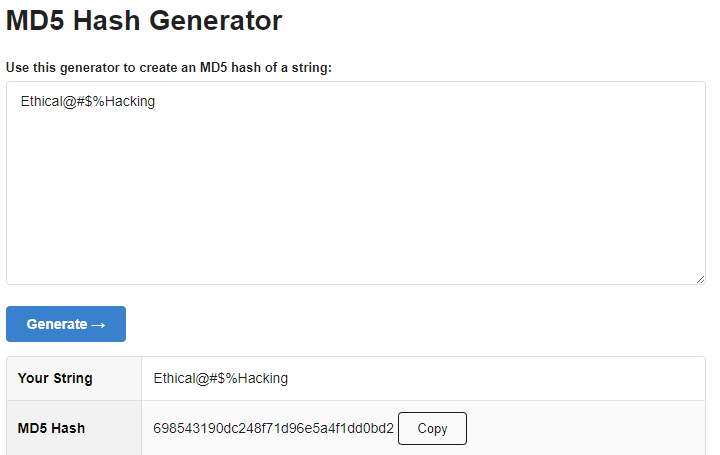
Use MD5 generator to find out the MD5 hash for the following words

1. Admin12345
2. Ethical@#$%Hacking

Output md5 hash

1. Admin12345 - e66055e8e308770492a44bf16e875127
2. Ethical@#$%Hacking - 698543190dc248f71d96e5a4f1dd0bd2





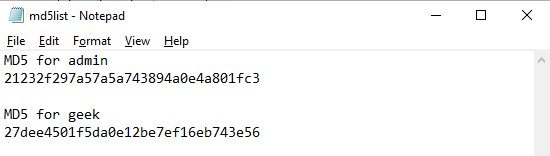
**3B Dictionary Attack**

Files:

**Passlist.txt**



**Md5list.txt**



**Code:**

**Dictattack.py**

import hashlib

flag=0

p\_hash=input("Enter MD5 hash")

dictionary=input("Enter dictionary Filename:")

try:

password\_file=open(dictionary,"r")

except:

print("No file found")

quit()

for word in password\_file:

enc\_word=word.encode('utf-8')

digest =hashlib.md5(enc\_word.strip()).hexdigest()

if(digest==p\_hash):

print("password has been found")

print("password is :" +word)

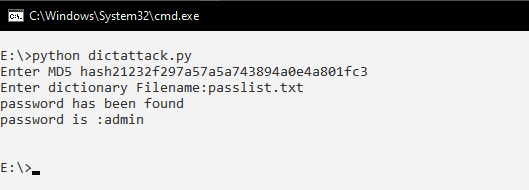
flag=1

break

if(flag==0):

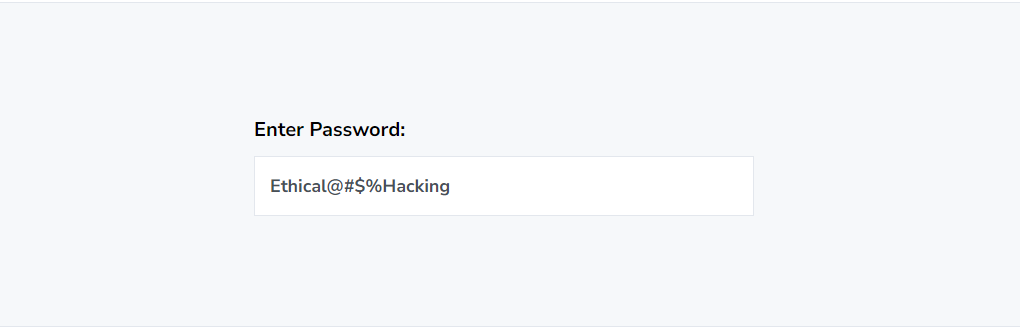
print("No password found")

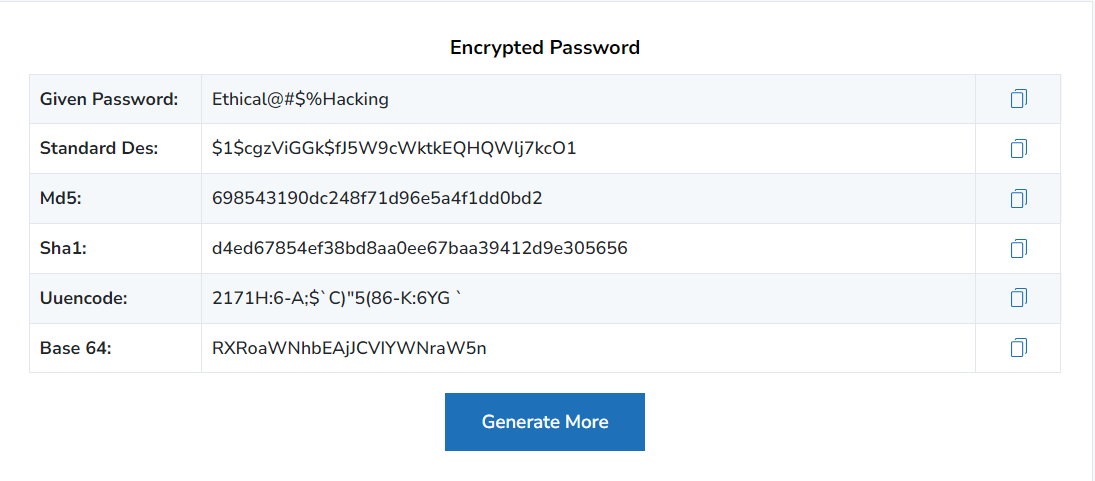
**Output:**



**3C. Encrypt and Decrypt Passwords**

Using the link <https://smallseotools.com/password-encryption-utility/> to enter password and generate encrypted data by various algorithms.





**3D. DoS Attack**

**DoS: Ping of Death Attack**

The attacker tries to crash a remote system by sending a single ICMP IP packet. They are historical. Any operating system after 1998 are patched with this attack. This attack is not actually focused on ICMP but just a general attack using a bigger packet than the permitted size.

**Working:**

1. The attacker creates an ICMP echo request (PING). Ping packets are small in size and used to get the status of the remote system. Most system accepts and responds to ping requests. Ping packets can be 65,536 bytes in length and it contains IP Header, IP Options and the Data.
2. The attacker will create an IP packet that is bigger than 65,536 in length by using the technique called as fragmentation. The packet is fragmented into multiple pieces which contains the offset (Fragment ID) and the data.
3. The receiving system reconstructs the pieces by joining them using the offset. As the packet is bigger than 65,536 bytes the memory buffer of the receiving system will overflow and this causes the system to crash or reboot or freeze.

**Solution:**

This attack can be prevented by just adding more checks when reconstructing the fragmented pieces. Just by checking the offset and the length of the packet before reconstruction can help prevent the attack.

**ICMP Echo Request Ping**

**Target System**

**Header**

**Data**

**Options**

**Data**

**Packet Reassembly**

**Data Fragmentation**

**Dos: TCP SYN Flooding**

TCP/IP is the protocol used for communication between two systems. The communication takes place by a 3-way handshake. The 3-way handshake takes place in the following way. Consider a client and server wants to communicate.

1. The client sends a message to the server requesting for service and this message is called the SYN request. SYN stands for Synchronized.
2. The server responds back with a message called the SYN ACK where ACK stands for acknowledgement. This means the server received the request and is providing an opportunity for the client to connect with the server.
3. The client confirms the connection by sending an ACK back to the server and this establishes the connection between the client and the server.

This process is subject to an attack called as DoS: TCP SYN Flooding attack.

**Working:**

1. Whenever the server receives an SYN request from the client it has to allocate some space in the state-table for the request because the server has to provide resources to the client.
2. At this point we have a connection that is called a half open connection between the client and the server until the final ACK message is sent.
3. When the server receives multiple SYN request it will allocate multiple space in the state-table for the requests. But when the server does not receive the final ACK message from the client then that space allotted remains open for some period of time.
4. Usually, the SYN request contains the users IP address. But in case of an attacker, he will send a spoof IP address. There is no way for the server to know whether the client is legitimate.
5. So now when the state-table is filled up completely and the server receives a SYN request the server has no space to allocate so it does not send a SYN ACK back. In some cases, this may lead to crashing of the server. This leads to a legitimate user not being able to get the service.

**Server**

Half Open Connection

**Internet**

**Spoof IP**

**SYN (Synchronize)**

**Client**

**SYN-ACK (Acknowledgement)**

**ACK (Acknowledgement)**

**Dos: Smurf Attack**

It was created in the year 1998 and was designed to perform a Denial-of-Service attack on a targeted system. It takes advantage of the ICMP protocol. ICMP is used to get the status of the targeted system by pinging the system called the echo request. The targeted system will send a response known as the ICMP echo response.

**Working:**

It takes advantage of the ICMP (Internet Control Messaging Protocol) protocol. The protocol is used to get the status of a given machine with the help of the ping command. In older times, whenever an IP address received a ping request it broadcasts it to multiple systems. The Smurf attack takes advantage of this broadcasting process in order to attack a target system.

1. The attacker sends an Echo Ping Request to the broadcasting system by passing the targeted systems IP address.
2. The ICMP protocol generally doesn’t check for authenticity of the IP address sent in the request.
3. Once the broadcasting system receives the ping request it send the same request to multiple systems by passing the targeted systems IP address.
4. Now all the systems send the Echo Response to the targeted system all at once.
5. This overloads the targeted systems resources and completely block the system from responding to a legitimate user’s request.

**Target System**

**Ping Response**

**IP – 2.4.6.8**

**IP – 2.4.6.8**

**IP – 2.4.6.8**

**Broadcasting System**

**IP – 2.4.6.8**

**IP – 1.3.5.7**

**Attacker**

**3E. ARP Poisoning in Windows**

**What is ARP Poisoning:**

ARP Poisoning consists of abusing the weaknesses in ARP to corrupt the MAC-to-IP mappings of other devices on the network. Security was not a paramount concern when ARP was introduced in 1982, so the designers of the protocol never included authentication mechanisms to validate ARP messages. Any device on the network can answer an ARP request, whether the original message was intended for it or not. For example, if Computer A “asks” for the MAC address of Computer B, an attacker at Computer C can respond and Computer A would accept this response as authentic. This oversight has made a variety of attacks possible. By leveraging easily available tools, a threat actor can “poison” the ARP cache of other hosts on a local network, filling the ARP cache with inaccurate entries.

**Steps in ARP Poisoning:**

1. The first step in planning and conducting an ARP Poisoning attack is selecting a Target. This can be a specific endpoint on the network, a group of endpoints, or a network device like a router. Routers are attractive targets because a successful ARP Poisoning Attack against a router can disrupt traffic for an entire subnet.
2. A wide variety of tools are easily available to anyone looking to carry out an ARP Poisoning attack. After launching the tool of his or her choice and configuring applicable settings, the attacker will begin the attack. They may immediately begin broadcasting ARP messages, or wait until a request is received.
3. Once the ARP cache on a victim machine or machines has been corrupted, the attacker will typically perform some type of action with the incorrectly steered traffic. They may inspect it, alter it, or cause it to be “blackholed” and never reach its intended destination. The exact action depends on the attacker’s motives.

**Types of ARP Poisoning Attacks:**

1. Man-in-the-Middle (MiTM) Attack.
2. Denial of Service (DoS) Attack.
3. Session Hijacking.

**Aim of ARP Poisoning:**

Hackers have a wide [variety of motives](https://www.varonis.com/blog/hacker-motives/?hsLang=en), and ARP Poisoning is no exception. An attacker might carry out an ARP poisoning attack for any number of reasons, ranging from high-level espionage to the thrill of creating chaos on the network. In one potential scenario, an attacker will use falsified ARP messages to assume the role of the default gateway for a given subnet, effectively steering all traffic to the attacker’s machine instead of the local router. They may then spy on, modify, or drop the traffic. These attacks are “noisy” in the sense that they leave evidence behind, but they need not interfere with the actual operation of the network. If espionage is the goal, the attacking machine will simply forward the traffic to its original destination, giving the end-user no indication that anything has changed.

On the other hand, the point of a DoS attack might be to create a highly noticeable disruption in network operation. While this could be targeted at depriving a business of its ability to operate, DoS attacks are often carried out by less skilled attackers for the sheer enjoyment of creating problems.

**How to Prevent ARP Poisoning Attacks**

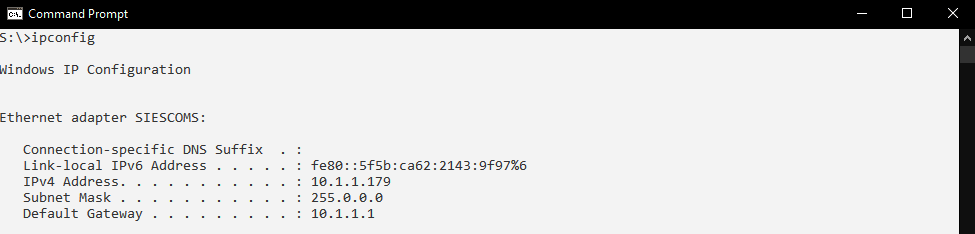
1. **Static ARP Tables**: It’s possible to statically map all the MAC addresses in a network to their rightful IP addresses. This is highly effective in preventing ARP Poisoning attacks but adds a tremendous administrative burden. Any change to the network will require manual updates of the ARP tables across all hosts, making static ARP tables unfeasible for most larger organizations. Still, in situations where security is crucial, carving out a separate network segment where static ARP tables are used can help to protect critical information.
2. **Switch Security**: Most managed Ethernet switches sport features designed to mitigate ARP Poisoning attacks. Typically known as Dynamic ARP Inspection (DAI), these features evaluate the validity of each ARP message and drop packets that appear suspicious or malicious. DAI can also typically be configured to limit the rate at which ARP messages can pass through the switch, effectively preventing DoS attacks.
3. **Physical Security**: Properly controlling physical access to your place of business can help mitigate ARP Poisoning attacks. ARP messages are not routed beyond the boundaries of the local network, so would-be attackers must be in physical proximity to the victim network or already have control of a machine on the network. Note that in the case of wireless networks, proximity doesn’t necessarily mean the attacker needs direct physical access; a signal extends to a street or parking lot may be sufficient. Whether wired or wireless, the use of technology like 802.1x can ensure that only trusted and/or managed devices can connect to the network.
4. **Network Isolation**: As stated previously, ARP messages don’t travel beyond the local subnet. This means that a well-segmented network may be less susceptible to ARP cache poisoning overall, as an attack in one subnet cannot impact devices in another. Concentrating important resources in a dedicated network segment where enhanced security is present can greatly diminish the potential impact of an ARP Poisoning attack.
5. **Encryption**: While encryption won’t actually prevent an ARP attack from occurring, it can mitigate the potential damage. A popular use of MiTM attacks was to capture login credentials that were once commonly transmitted in plain text. With the widespread use of SSL/TLS encryption on the web, this type of attack has become more difficult. The threat actor can still intercept the traffic, but can’t do anything with it in its encrypted form.

**3F. Ipconfig, ping, traceroute and netstat**

1. **Ipconfig:**

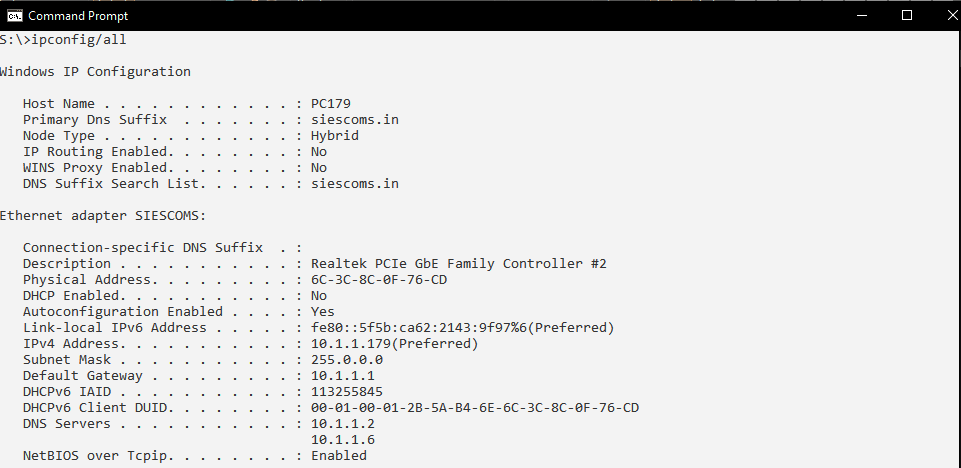
* Displays the current information about the network connected. Such as IP and MAC address of the router along with the DHCP and DNS servers.
* IP address of a device mainly helps in identifying the connection of a network
* The MAC Address, on the other hand, ensures the computer device's physical location.
* Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
* A Domain Name System (DNS) turns domain names into IP addresses, which allow browsers to get to websites and other internet resources.

**Output:**



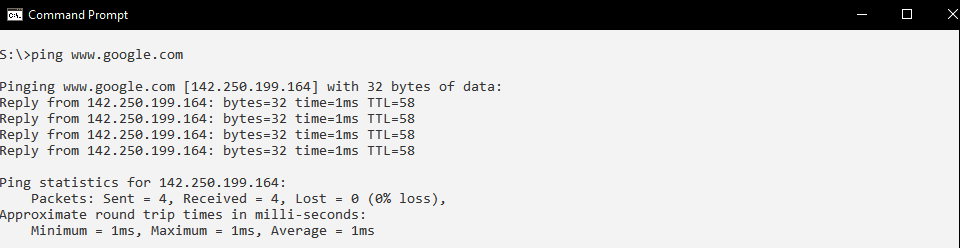
1. **Ipconfig/all**

**Output:**

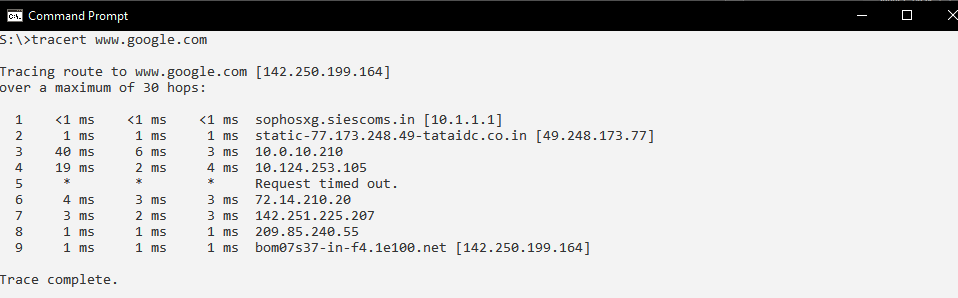


1. **Ping** www.goog`1sle.com

**Output:**

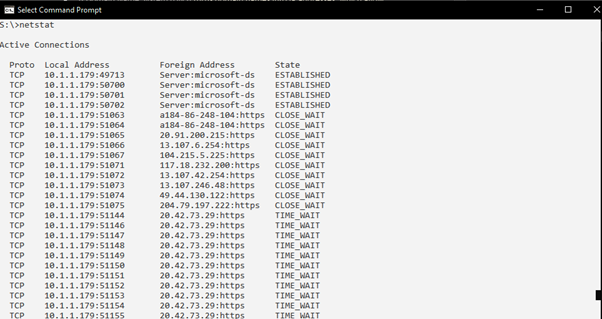


1. **tracert** [www.google.com](http://www.google.com)



1. **netstat**

**Output:**



**3G Steganography tools. (S-Tools):**

1. Prepare the secret file that you want to hide(eg ME.txt)

A close-up of a college

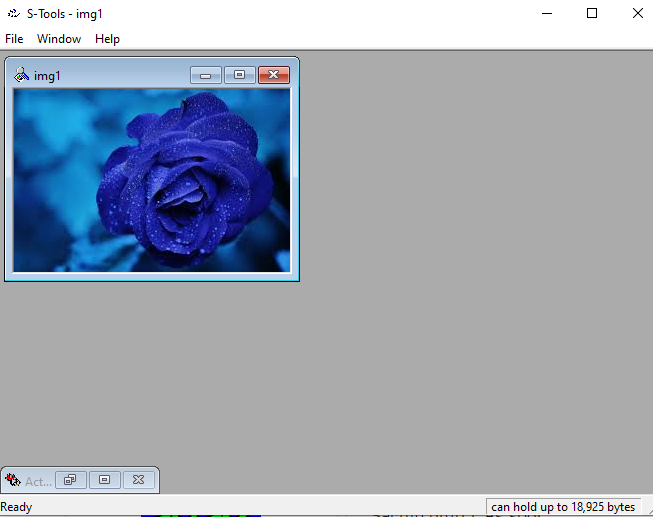
Description automatically generated

1. Launch the **S-Tools**

A screenshot of a computer program

Description automatically generated

1. Drag and drop the host file inside which you wants to hide secret file(img1.bmp)



1. Now drag and drop the secret file on image file and alert by stool to enter password and choose encryption algorithm will come.

A computer screen shot of a blue rose

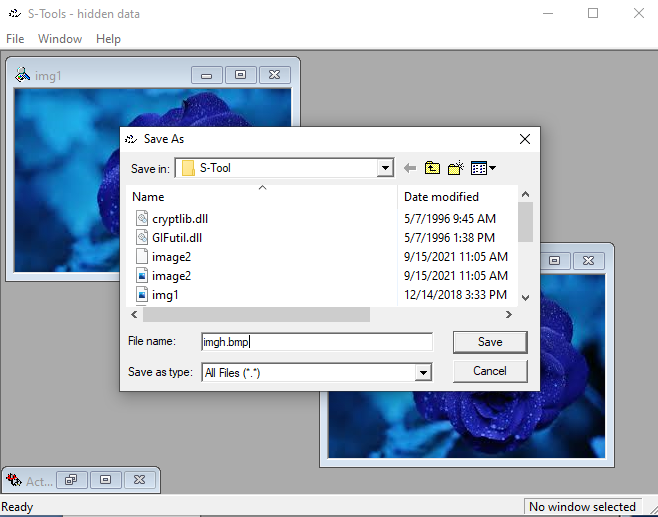
Description automatically generated

1. After entering password and algo, click ok. Tool will create identical copy hidden data.bmp

A screenshot of a computer

Description automatically generated

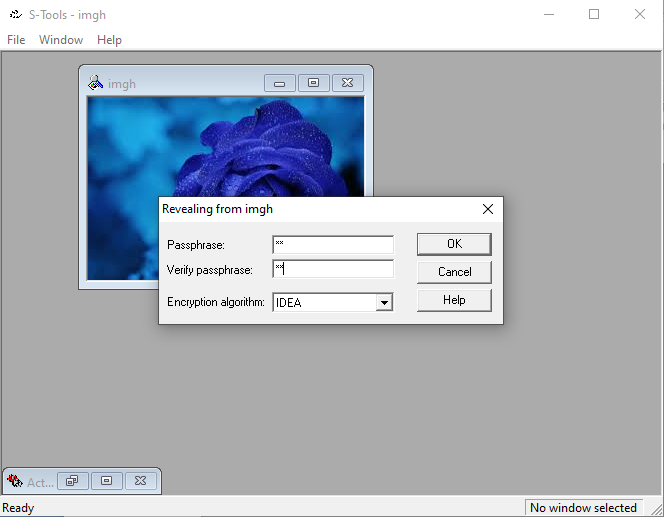
1. Right click and save it.



1. To reveal the hidden data open the file in S-Tool. Right click select reveal and put password and select algorithm.

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated