Name: Muhammad Izham Bin Norhamadi

Matrix No: B032020039

Lab 2

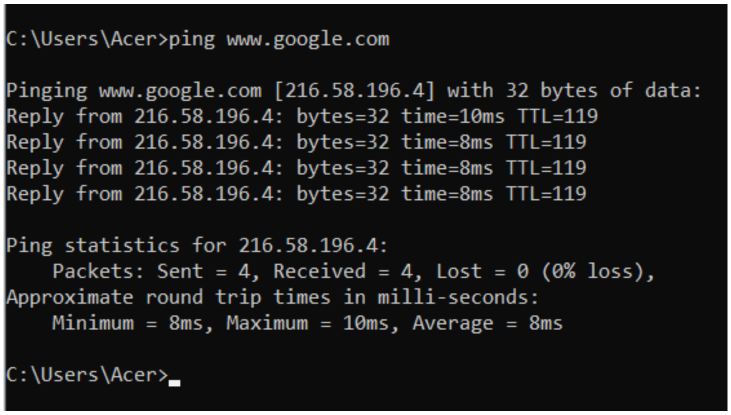
CMD Commands in security

Lab Steps

Open CMD in Administrator mode

1. **Know the IP Address of any website**
   - C:\WINDOWS\system32>ping www.google.com

   a) Show and explain the results.



```
C:\Users\Acer>ping www.google.com

Pinging www.google.com [216.58.196.4] with 32 bytes of data:
Reply from 216.58.196.4: bytes=32 time=10ms TTL=119
Reply from 216.58.196.4: bytes=32 time=8ms TTL=119
Reply from 216.58.196.4: bytes=32 time=8ms TTL=119
Reply from 216.58.196.4: bytes=32 time=8ms TTL=119

Ping statistics for 216.58.196.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 10ms, Average = 8ms

C:\Users\Acer>
```

- Information about the domain such as the ip address, packet loss rate and latency to the destination

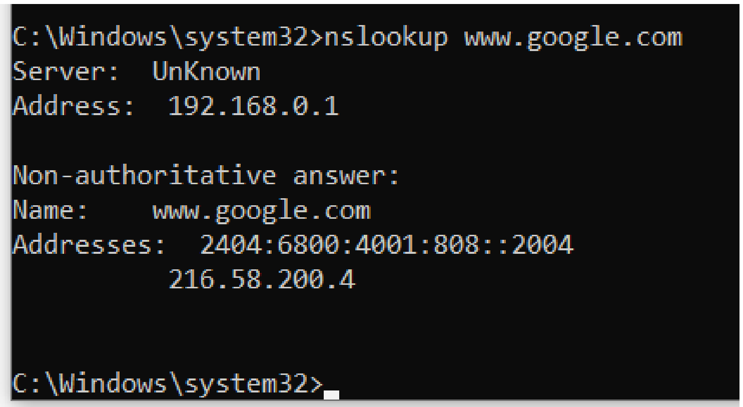
   b) What is the purposes of “ping” command?

- Ping the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution

2. Resolving DNS into IP

- C:\WINDOWS\system32>nslookup www.google.com

a) Show and explain the results.



```
C:\Windows\system32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4001:808::2004
          216.58.200.4


C:\Windows\system32>
```

- Information shown is IPv4 address of the domain and IPv6 address

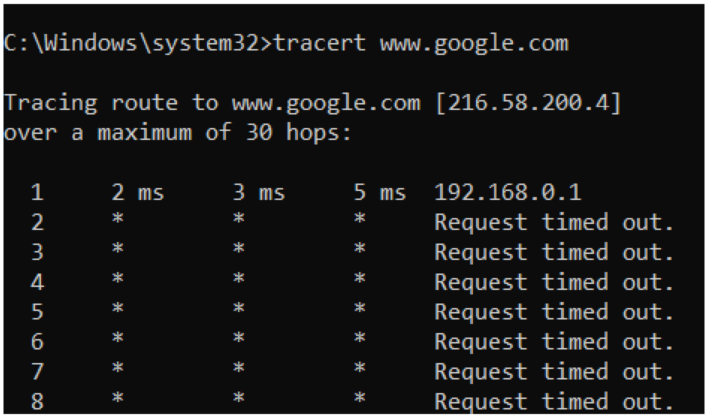
b) How the results of "nslookup" can be used by network administrator?

- Nslookup can be used to get information from DNS server such as IP address and DNS record. It can also be used to troubleshoot DNS related problems.

3. Displaying the route path between your computer to website

- C:\WINDOWS\system32>tracert www.google.com

a) Show and explain the results.



```
C:\Windows\system32>tracert www.google.com

Tracing route to www.google.com [216.58.200.4]
over a maximum of 30 hops:

  1     2 ms     3 ms     5 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
```

- Testing route for packets to send to google.com

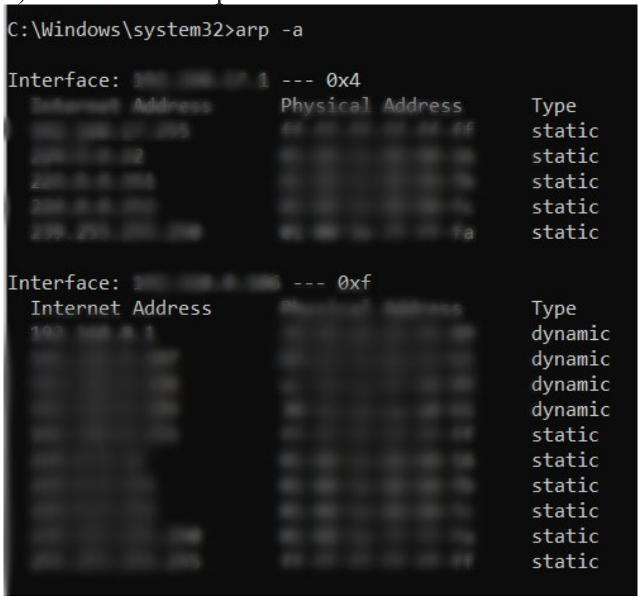
b) How can “tracert” help network administrator during network analysis?

- tracert diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. Tracert can be used to find out where a packet stopped on the network and troubleshoot from there.

4. ARP table

- C:\WINDOWS\system32>arp –a

a) Show and explain the results.



```
C:\Windows\system32>arp -a

Interface: [redacted] --- 0x4
  [redacted]          Physical Address      Type
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static

Interface: [redacted] --- 0xf
  Internet Address    [redacted]            Type
  [redacted]          [redacted]            dynamic
  [redacted]          [redacted]            dynamic
  [redacted]          [redacted]            dynamic
  [redacted]          [redacted]            dynamic
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
  [redacted]          [redacted]            static
```

- List of the network interface, target system and physical (MAC) address of each system

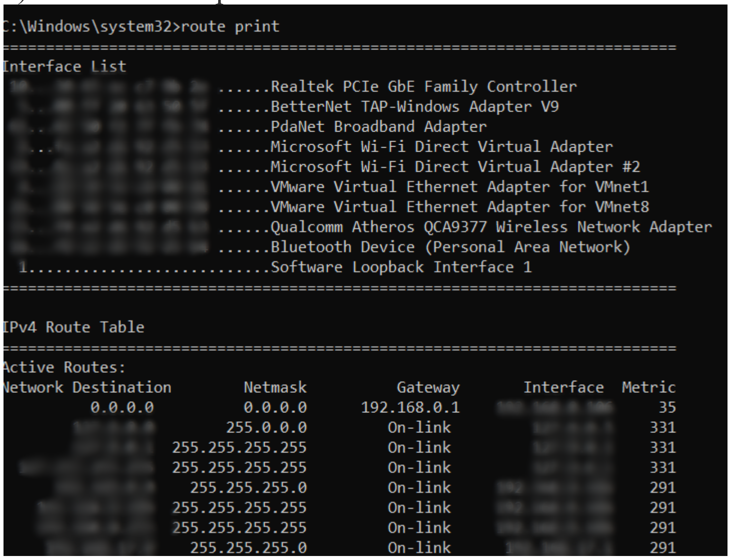
b) What is the purposes of ARP?

- Each time a computer's TCP/IP stack uses ARP to determine the Media Access Control (MAC) address for an IP address, it records the mapping in the ARP cache so that future ARP lookups go faster. ARP is useful when diagnosing duplicate IP assignment problems.

5. Routing table, gateway, interface and metric

- C:\WINDOWS\system32>route print

a) Show and explain the results.



```
C:\Windows\system32>route print
===========================================================================
Interface List
 [redacted] ......Realtek PCIe GbE Family Controller
 [redacted] ......BetterNet TAP-Windows Adapter V9
 [redacted] ......PdaNet Broadband Adapter
 [redacted] ......Microsoft Wi-Fi Direct Virtual Adapter
 [redacted] ......Microsoft Wi-Fi Direct Virtual Adapter #2
 [redacted] ......VMware Virtual Ethernet Adapter for VMnet1
 [redacted] ......VMware Virtual Ethernet Adapter for VMnet8
 [redacted] ......Qualcomm Atheros QCA9377 Wireless Network Adapter
 [redacted] ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1      [redacted]     35
       [redacted]        255.0.0.0         On-link       [redacted]    331
       [redacted]  255.255.255.255         On-link       [redacted]    331
       [redacted]  255.255.255.255         On-link       [redacted]    331
       [redacted]    255.255.255.0         On-link       [redacted]    291
       [redacted]  255.255.255.255         On-link       [redacted]    291
       [redacted]  255.255.255.255         On-link       [redacted]    291
       [redacted]    255.255.255.0         On-link       [redacted]    291
```

- Displaying Local Routing Table

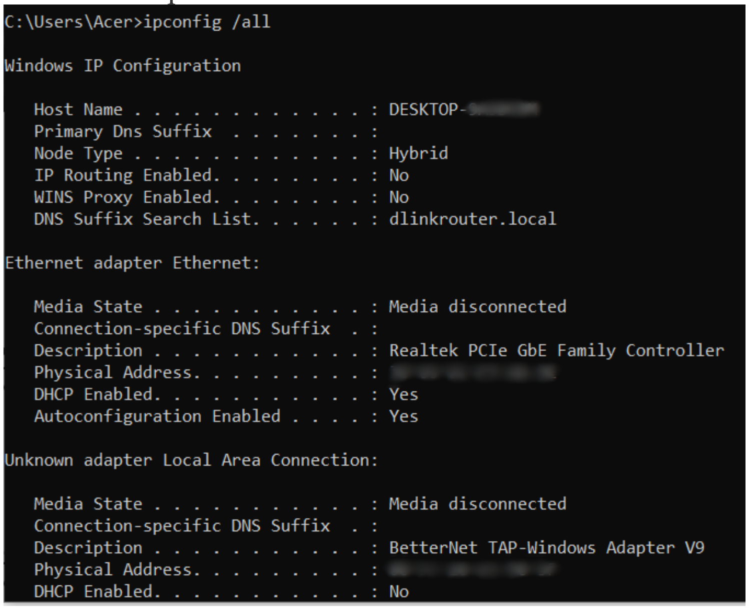
b) What is the use of "route" command?

- The local routing table allow the system to route to the appropriate interface to reach an address. The route command allows you to make manual entries into the network routing tables.

6. See IP, gateway, DNS and other info

- C:\WINDOWS\system32>ipconfig/all

a) Show and explain the results.



```
C:\Users\Acer>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-[redacted]
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : dlinkrouter.local

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : BetterNet TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : No
```

IP configuration for Windows devices and adapters

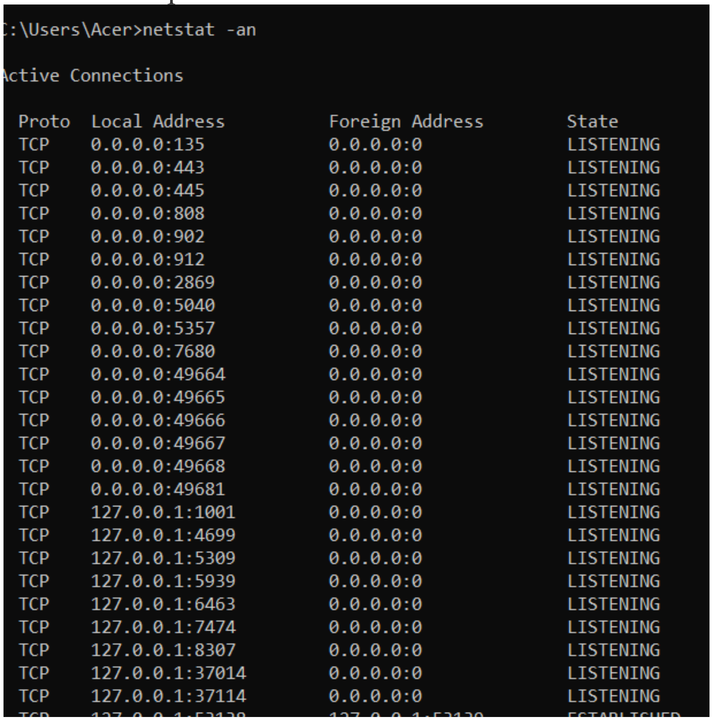
b) How can "ipconfig" used for troubleshooting network connectivity issues?

- Ipconfig displays all current TCP/IP network configuration values. This can be used to find network addresses from the system such as IPv4 address and IPv6

7. See connection status

- C:\WINDOWS\system32>netstat –an

a) Show and explain the results.



```
:\Users\Acer>netstat -an

ctive Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:808            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49681          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4699         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5309         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7474         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:37014        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:37114        0.0.0.0:0              LISTENING
```

- Shows incoming and outgoing connections, as well as listening ports

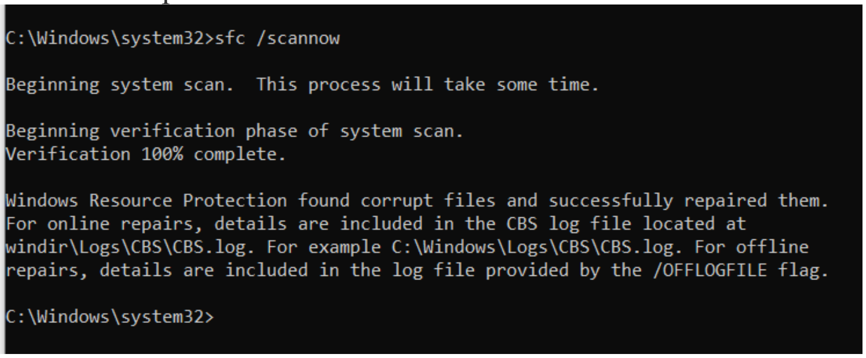
b) How can "netstart" help network administrator during network analysis?

- Network statistics (netstat) is a networking tool used for troubleshooting and configuration as well as monitoring tool for connections over the network

8. System File Checker

- C:\WINDOWS\system32>sfc /scannow

a) Show and explain the results.



```
C:\Windows\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them.
For online repairs, details are included in the CBS log file located at
windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline
repairs, details are included in the log file provided by the /OFFLOGFILE flag.

C:\Windows\system32>
```

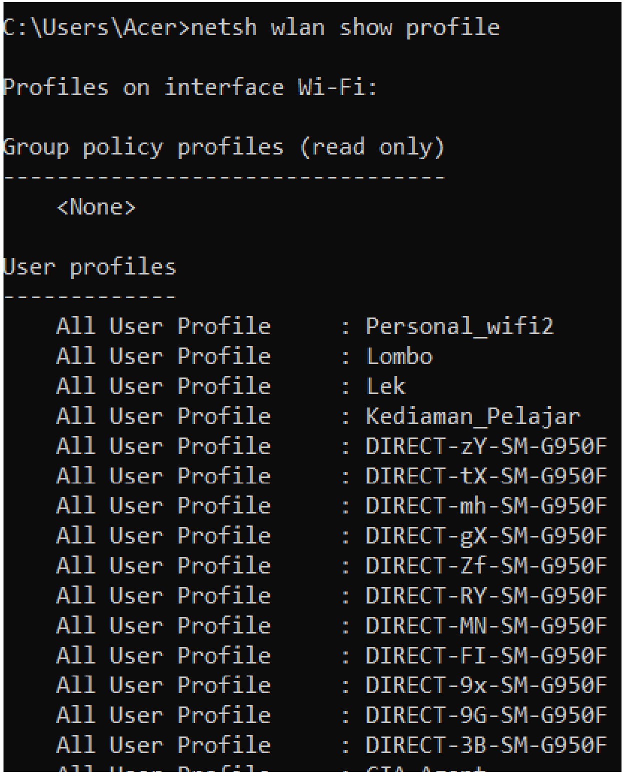
Result of scanning system files

b) How can “sfc /scannow” help network administrator during network analysis?

- System File Checker tool (sfc) can scan and repair missing or corrupted system files that may cause network problems

9. Wi-Fi password

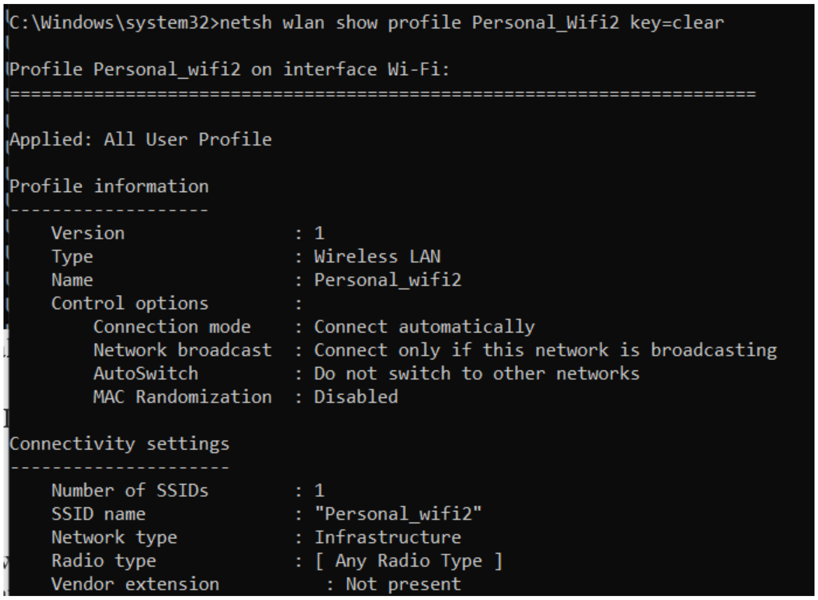
- C:\WINDOWS\system32> netsh wlan show profile



```
C:\Users\Acer>netsh wlan show profile

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : Personal_wifi2
    All User Profile     : Lombo
    All User Profile     : Lek
    All User Profile     : Kediaman_Pelajar
    All User Profile     : DIRECT-zY-SM-G950F
    All User Profile     : DIRECT-tX-SM-G950F
    All User Profile     : DIRECT-mh-SM-G950F
    All User Profile     : DIRECT-gX-SM-G950F
    All User Profile     : DIRECT-Zf-SM-G950F
    All User Profile     : DIRECT-RY-SM-G950F
    All User Profile     : DIRECT-MN-SM-G950F
    All User Profile     : DIRECT-FI-SM-G950F
    All User Profile     : DIRECT-9x-SM-G950F
    All User Profile     : DIRECT-9G-SM-G950F
    All User Profile     : DIRECT-3B-SM-G950F
    All User Profile     : CIA Agent
```

List of all wireless network profiles

- C:\WINDOWS\system32> netsh wlan show profile SSID key=clear (replace SSID with the name of the network)



```
C:\Windows\system32>netsh wlan show profile Personal_Wifi2 key=clear

Profile Personal_wifi2 on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : Personal_wifi2
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "Personal_wifi2"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present
```

Detailed information on the specified wireless profile as well as clear password

a) Show and explain the results.
b) What is the purposes of "netsh wlan show profile SSID key=clear" command?

- To retrieve password for the specified wifi

Analysis Questions

1. You have been called in to troubleshoot client's computer, which is unable to connect to the local area network. What command would you use to check the configuration? What information would you look for?
    - Use ipconfig to check IPv4 address of the client's computer to check if it's properly assigned to the computer and unique to other IP address in the LAN

2. You have been called in to troubleshoot a client's computer, which is able to connect to local area network but unable to connect to any other network. What command would you use to check the configuration? What information would you look for?
    - Use ping command and check the connection with a common domain such as Google.com. If it was unable to connect then the internet provider is not properly configured to connect to the internet.

3. If you needed to obtain a user's MAC address as well as the user's network configuration information, what command and switch would you enter?
    - Use 'arp -a' command to display list of network interface, ip address, and physical address of each system.

4. You have just pinged a remote computer. You would now like to retrieve the MAC address of the remote computer locally. How would you obtain the remote computer's MAC address?
    - Use 'arp -a' command

5. What information does ping return to the user?
    - Information about the domain such as the ip address, packet loss rate and latency to the destination