Jamhuriya University of Science and Technology (JUST)

جامعة جمهورية للعلوم والتكنولوجيا

Home of Quality Education

Information Security

Group

1. **Naqib Ali Hassan**

2. **A.aziiz Mohamed Shariif**

3. **Zakarie Ahmed Hashi**

Chapter One: Exercises

1.1 On Analyzing the number of virus outbreaks which had occurred in the past 7 days are: -

1. **Clop Ransomware**

Ransomware is malware which encrypts your files until you pay a ransom to the hackers. “Clop” is one of the latest and most dangerous ransomware threats. It’s a variant of the well-known CryptoMix ransomware, which frequently targets Windows users.

Before beginning the encryption process, the Clop ransomware blocks over 600 Windows processes and disables multiple Windows 10 applications, including Windows Defender and Microsoft Security Essentials — leaving you with zero chance of protecting your data.

The Clop ransomware has evolved since its inception, now targeting entire networks — not just individual devices. Even the Maastricht University in the Netherlands became a victim of the Clop ransomware, with almost all Windows devices on the university’s network being encrypted and forced to pay a ransom.

2. **Fake Windows Updates (Hidden Ransomware)**

Hackers have been increasingly sending emails that instruct readers to install urgent Windows OS updates. The emails trick readers into installing the “latest” Windows updates, which are actually ransomware ‘.exe’ files in disguise.

The ransomware contained in these emails is known as “Cyborg”. It encrypts all of your files and programs and demands a ransom payment to un-encrypt the files.

Unfortunately, many email service providers and basic antivirus software aren’t able to detect and block these emails. This is why you must be using an antivirus that provides proper internet security, protecting you from dangerous emails.

3. **Zeus Gameover**

Zeus Gameover is part of the “Zeus” family of malware and viruses. This piece of malware is a Trojan — malware disguised as something legitimate — that accesses your sensitive bank account details and steals all of your funds.

The worst thing about this particular variant of the Zeus malware family is that it doesn’t require a centralized “Command and Control” server to complete transactions — which is a flaw found in many cyberattacks that authorities can target. Instead, Zeus Gameover can bypass centralized servers and create independent servers to send sensitive information. In essence, you cannot trace your stolen data.

4. **RaaS**

“RaaS” — also known as “Ransomware as a Service” — is a growing industry in the underground hacker community. People without the knowledge to carry out a sophisticated ransomware attack can pay to hire a professional hacker or team of hackers to perform the attack for them.

The growth of the underground RaaS industry is worrying, as it shows how easy it is to infect people with ransomware despite the bad actors having no previous experience with designing or coding malware.

5. News Malware Attacks

Cybercriminals often use current news stories and global events to target people with malware.

One example is hackers using the wave of the COVID-19 (Coronavirus) outbreak to target individuals with malware. Hackers send out emails that are disguised as legitimate information about the outbreak. Readers are prompted to click a link to learn more about the information, but the link contains malware that copies the files on your device and steals your personal information.

Research currently focuses on the spread of this malware in Japan. Still, it will become an issue worldwide during any kind of newsworthy outbreak.

6. Fleeceware

Fleeceware continues to charge app users large amounts of money despite users deleting those apps. Recent research has found that over 600 million Android users have downloaded "Fleeceware" onto their device in the past few years.

Although Fleeceware doesn't pose a considerable security threat to a user's device and data, it's still very common, and it's a shady practice by app developers wanting to cash in on unsuspecting users.

7. IoT Device Attacks

As the popularity of IoT (Internet of Things) devices grows in 2020 — things like smart speakers and video doorbells — hackers are looking to exploit these devices for valuable information.

There are multiple reasons why hackers choose to target IoT devices. For one, most IoT devices don't have enough storage to install proper security measures. These devices often contain easy-to-access data such as passwords and usernames, which then can be used by hackers to log into user accounts and steal valuable information, such as banking details.

Hackers can also use internet-based cameras and mics to spy on and communicate with people — including young children via smart baby monitors.

These devices can also act as weak points in a corporation's network, meaning hackers can gain access to entire systems through unsecured IoT devices — spreading malware to other devices across the network.

8. Social Engineering

Humans are possibly the weakest link in any security protocol. This is why cybercriminals are now turning to human psychology and deception to try and gain access to personal information.

The hacker will start by contacting a company or service provider and pretend to be a specific person. They'll ask questions regarding the victim's account and trick the customer support team into handing over pieces of sensitive information. Then, they'll exploit that information to gain access to a person's account and data, including payment details.

Although this isn't a type of malware perse, social engineering is an alarming trend, as it doesn't require hackers to know about coding or malware development. Instead, all the attacker needs is to be convincing and allow human error and complacency to reward them with the data they need.

9. Cryptojacking

Cryptojacking malware is designed to use a person's computing power to help "mine" cryptocurrencies, such as Bitcoin. Mining requires a huge amount of computing power to generate new crypto coins, which is why hackers are attempting to install cryptojacking malware on computers and mobile devices to help with the mining process — slowing down the user's device considerably.

Although cryptojacking attacks dropped significantly in previous years — mainly due to the sharp fall in the value of cryptocurrencies, this trend remains a threat. As cryptocurrency prices continue to rise through 2020, cryptojacking malware attacks will continue to be lucrative for cybercriminals.

10. Artificial Intelligence (AI) Attacks

As more tools become available to developers who want to program AI scripts and software, hackers will be able to use this same technology to carry out devastating cyberattacks.

Although cybersecurity companies are using artificial intelligence and machine learning algorithms to help combat malware, these technologies can also be exploited to hack devices and networks on a massive scale.

Cyberattacks can often cost cybercriminals a lot in terms of time and resources. So, with the expansion of AI and machine learning technologies, we can only expect hackers to develop highly-advanced and destructive AI-based malware in 2020 and beyond.

1.2 Cookeis invade your privacy, and they do it in a pretty big way. Cookies literally don`t ask you for the access to your private information, they just get it in a way that might seem illegal, and that probably is illegal. Cookies are pretty many digital stalkers. They find all about you, about your habits, what you love, what you like, what you dislike, where you love to go, who do you hate and etc.

Just like a real person which is a stalker would know about you when they would stalk you. But cookies can do it 24/7 without a rest. Don`t get us wrong, there is some cookie software that is even beneficial to you. But most of them are the kind that is invasive to your privacy. Because this reason you should use the software that will protect you from those cookies and never allow the website to install their cookies on your computer. That is the only way that you can protect yourself from them.

No one likes to be watched and spied on, and that is exactly what cookies do.

1.3 Hackers are the computer hobbyist. The gain unauthorized access to enter on the highly secured computer or the network.

Hacker Temrinlogy: -

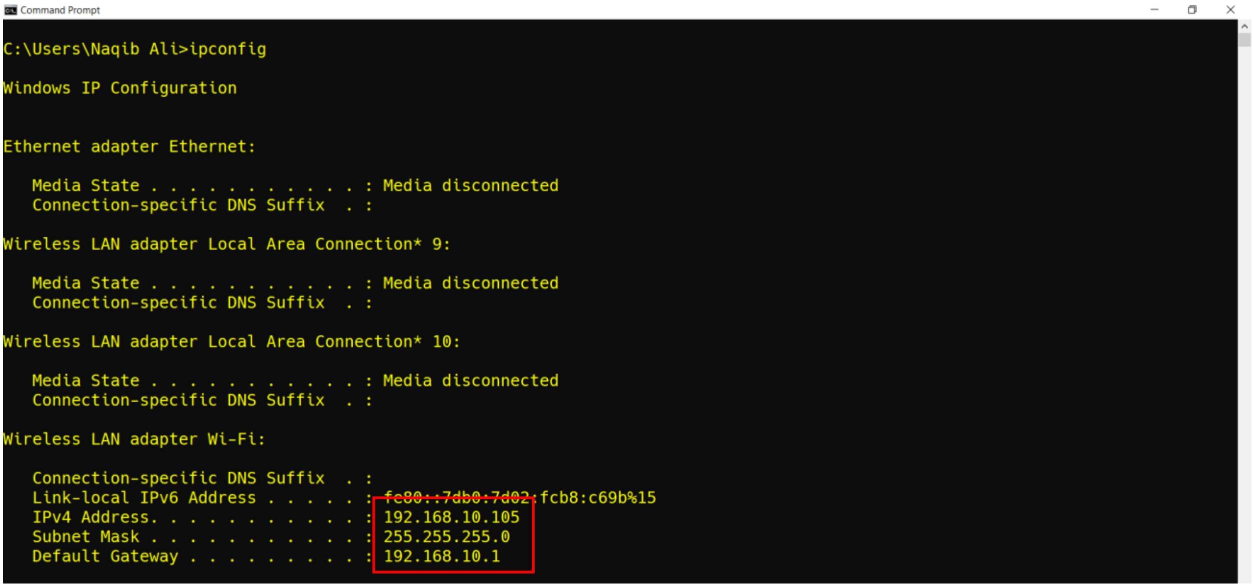
- **Alpha Geek: -** Technically skilled person in some implied perspective. That is the person is knowledgeable in some known or understanble context.
- **Grol:** - Grok means understanding in global sense. It means exhaustive and intimate knowledge. The more definite form of grok is “Grok in fullness”.
- **Red Book:** - Informal name for one of the three standard references on PostScript ("PostScript Language Reference Manual", Adobe Systems (Addison-Wesley, 1985; QA76.73. P67P67; ISBN 0-201-10174-2, or the 1990 second edition ISBN 0-201-18127-4); the others are known as the Green Book, the Blue Book, and the White Book (sense 2). 2. Informal name for one of the 3 standard references on Smalltalk ("Smalltalk-80: The Interactive Programming Environment" by Adele Goldberg (Addison-Wesley, 1984; QA76.8.S635G638; ISBN 0-201-11372-4); this too is associated with blue and green books). 3. Any of the 1984 standards issued by the CCITT eighth plenary assembly. These include, among other things, the X.400 email spec and the Group 1 through 4 fax standards. 4. The new version of the Green Book (sense 4) -- IEEE 1003.1-1990, a.k.a ISO 9945-1 -- is (because of the color and the fact that it is printed on A4 paper) known in the USA as "the Ugly Red Book That Won't Fit On The Shelf" and in Europe as "the Ugly Red Book That's A Sensible Size". 5. The NSA "Trusted Network Interpretation" companion to the Orange Book. See also book titles.
- **Wank:** - [Columbia University: prob. by mutation from Commonwealth slang /v./ `wank', to masturbate] Used much as hack is elsewhere, as a noun denoting a clever technique or person or the result of such cleverness. May describe (negatively) the act of hacking for hacking's sake ("Quit wanking, let's go get supper!") or (more positively) a wizard. Adj. `wanky' describes something particularly clever (a person, program, or algorithm). Conversations can also get wanky when there are too many wanks involved. This excess wankiness is signalled by an overload of the `wankometer' (compare bogometer). When the wankometer overloads, the conversation's subject must be changed, or all non-wanks will leave. Compare `neep-neeping' (under neep-neep). Usage: U.S. only. In Britain and the Commonwealth this word is extremely rude and is best avoided unless one intends to give offense.

1.4 Explaining the importance of the security policy documents in the organization:

- **Wireless Communication Policy:** Is important in the organization, because: -
  - To secure and to protect the data that is owned by the organization
  - The oraganization contains many resources like computers, networks, and others. Organization gives access to these resources as an honor and it must achieve them responsibly to keep the confidentiality, integrity, avialable for all the data.
- **Database credentials policy:**
  - Database credentials policy is one of the policies comes under the "Server Security of the SANS institute.
  - It is used to securely store and retrieve the data from the database in the company.
  - Everyone in the organization should adhere to the database credentials policy.
- **Web application security policy:**
  - Web application security policy comes under the "Application Security" of the SANS institute.
  - It is completed based on the rules and regulations of the company.
  - The vulnerabilities associated with the web applications are listed in this policy.

CHAPTER TWO: Exercise

Exercise 2.1: Using Ipconfig



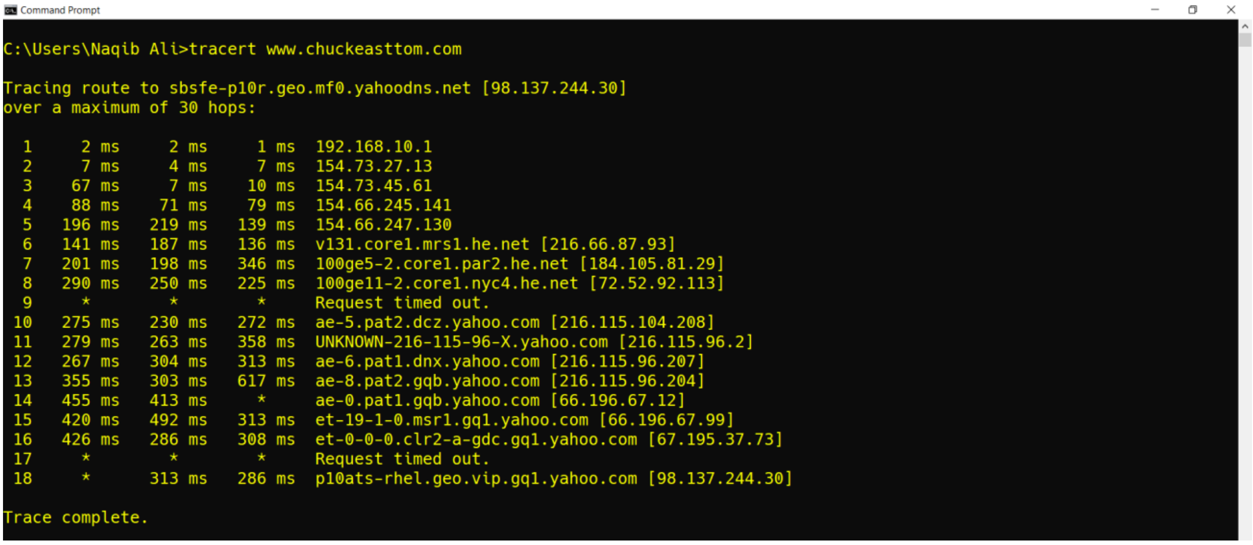
```
C:\Users\Naqib Ali>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7db0:7d02:fcb8:c69b%15
   IPv4 Address. . . . . . . . . . . : 192.168.10.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

Exercise 2.2: Using tracert

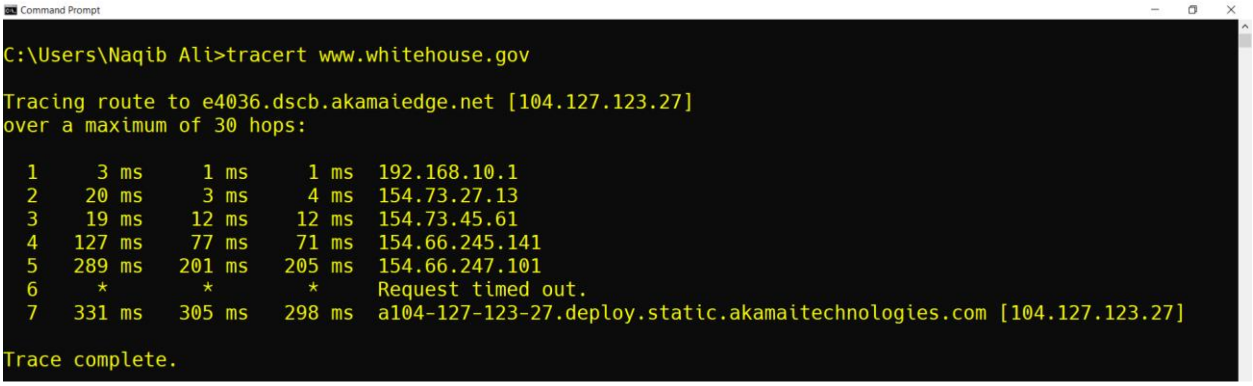
Hops for www.chuckeasttom.com = 18

Hops for www.whitehouse.gov = 7

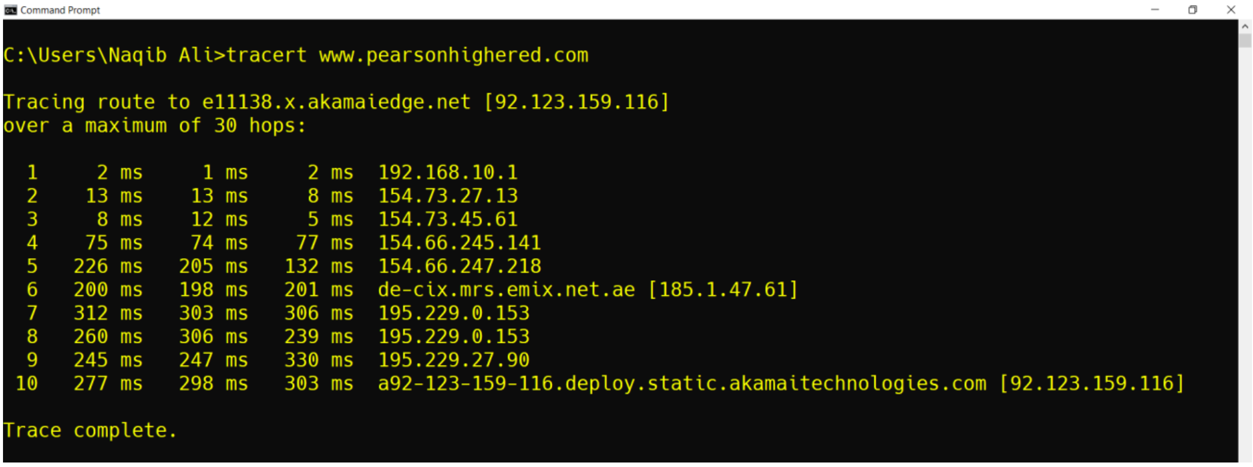
Hops for www.pearsonhighered.com = 10



```
C:\Users\Naqib Ali>tracert www.chuckeasttom.com

Tracing route to sbsfe-p10r.geo.mf0.yahoodns.net [98.137.244.30]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.10.1
  2     7 ms     4 ms     7 ms  154.73.27.13
  3    67 ms     7 ms    10 ms  154.73.45.61
  4    88 ms    71 ms    79 ms  154.66.245.141
  5   196 ms   219 ms   139 ms  154.66.247.130
  6   141 ms   187 ms   136 ms  v131.core1.mrs1.he.net [216.66.87.93]
  7   201 ms   198 ms   346 ms  100ge5-2.core1.par2.he.net [184.105.81.29]
  8   290 ms   250 ms   225 ms  100ge11-2.core1.nyc4.he.net [72.52.92.113]
  9     *        *        *     Request timed out.
 10   275 ms   230 ms   272 ms  ae-5.pat2.dcz.yahoo.com [216.115.104.208]
 11   279 ms   263 ms   358 ms  UNKNOWN-216-115-96-X.yahoo.com [216.115.96.2]
 12   267 ms   304 ms   313 ms  ae-6.pat1.dnx.yahoo.com [216.115.96.207]
 13   355 ms   303 ms   617 ms  ae-8.pat2.gqb.yahoo.com [216.115.96.204]
 14   455 ms   413 ms     *     ae-0.pat1.gqb.yahoo.com [66.196.67.12]
 15   420 ms   492 ms   313 ms  et-19-1-0.msr1.gq1.yahoo.com [66.196.67.99]
 16   426 ms   286 ms   308 ms  et-0-0-0.clr2-a-gdc.gq1.yahoo.com [67.195.37.73]
 17     *        *        *     Request timed out.
 18     *      313 ms   286 ms  p10ats-rhel.geo.vip.gq1.yahoo.com [98.137.244.30]

Trace complete.
```



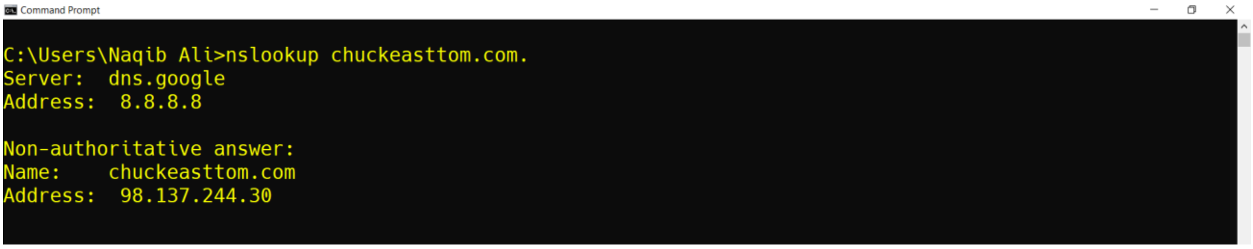
```
C:\Users\Naqib Ali>tracert www.whitehouse.gov

Tracing route to e4036.dscb.akamaiedge.net [104.127.123.27]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  192.168.10.1
  2    20 ms     3 ms     4 ms  154.73.27.13
  3    19 ms    12 ms    12 ms  154.73.45.61
  4   127 ms    77 ms    71 ms  154.66.245.141
  5   289 ms   201 ms   205 ms  154.66.247.101
  6     *        *        *     Request timed out.
  7   331 ms   305 ms   298 ms  a104-127-123-27.deploy.static.akamaitechnologies.com [104.127.123.27]

Trace complete.
```



```
C:\Users\Naqib Ali>tracert www.pearsonhighered.com

Tracing route to e11138.x.akamaiedge.net [92.123.159.116]
over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  192.168.10.1
  2    13 ms    13 ms     8 ms  154.73.27.13
  3     8 ms    12 ms     5 ms  154.73.45.61
  4    75 ms    74 ms    77 ms  154.66.245.141
  5   226 ms   205 ms   132 ms  154.66.247.218
  6   200 ms   198 ms   201 ms  de-cix.mrs.emix.net.ae [185.1.47.61]
  7   312 ms   303 ms   306 ms  195.229.0.153
  8   260 ms   306 ms   239 ms  195.229.0.153
  9   245 ms   247 ms   330 ms  195.229.27.90
 10   277 ms   298 ms   303 ms  a92-123-159-116.deploy.static.akamaitechnologies.com [92.123.159.116]

Trace complete.
```

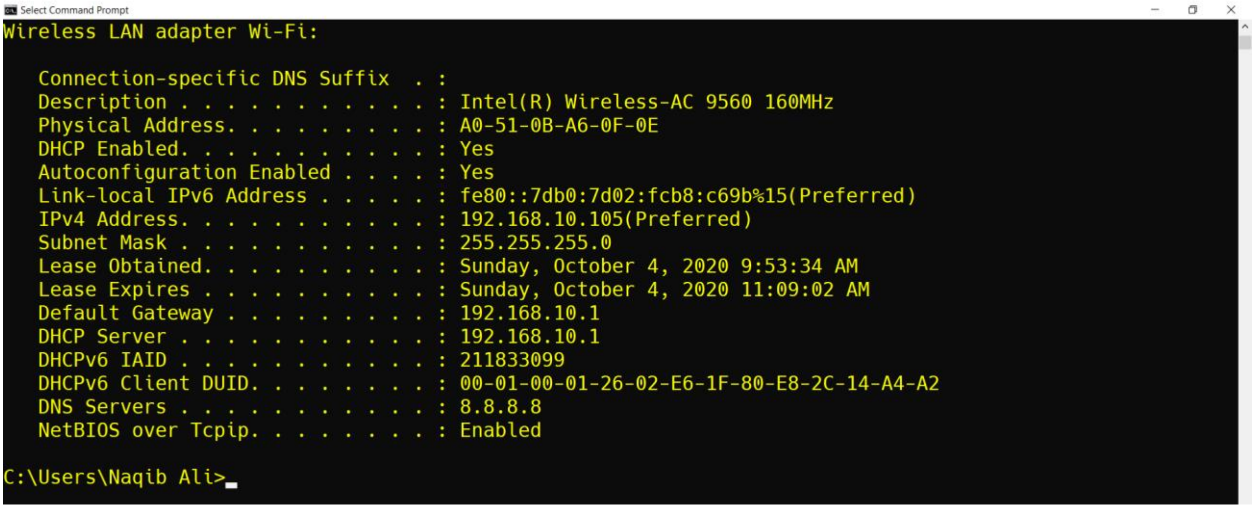
First four hops are almost same for all websites

Exercise 2.3: Using NSLookup



```
C:\Users\Naqib Ali>nslookup chuckeasttom.com.
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    chuckeasttom.com
Address:  98.137.244.30
```

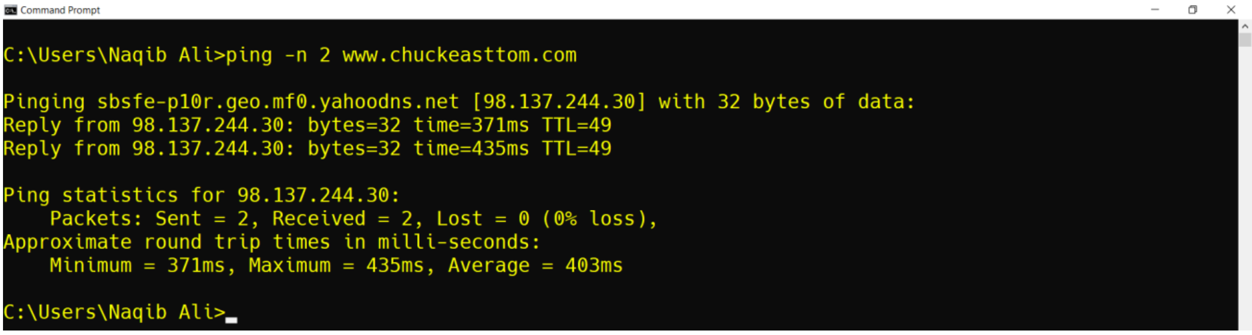
Exercise 2.4: More About Ipconfig



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Physical Address. . . . . . . . . : A0-51-0B-A6-0F-0E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7db0:7d02:fcb8:c69b%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.105(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, October 4, 2020 9:53:34 AM
   Lease Expires . . . . . . . . . . : Sunday, October 4, 2020 11:09:02 AM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 211833099
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-02-E6-1F-80-E8-2C-14-A4-A2
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Naqib Ali>_
```

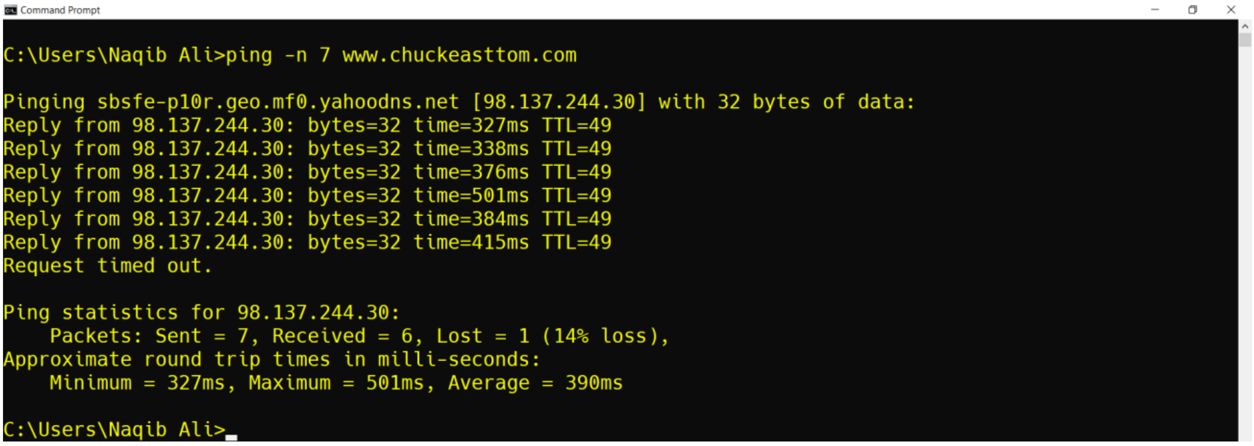
Exercise 2.5: More About Ping

→ `ping -n 2 www.chuckeasttom.com`



```
C:\Users\Naqib Ali>ping -n 2 www.chuckeasttom.com

Pinging sbsfe-p10r.geo.mf0.yahoodns.net [98.137.244.30] with 32 bytes of data:
Reply from 98.137.244.30: bytes=32 time=371ms TTL=49
Reply from 98.137.244.30: bytes=32 time=435ms TTL=49

Ping statistics for 98.137.244.30:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 371ms, Maximum = 435ms, Average = 403ms

C:\Users\Naqib Ali>_
```

→ ping -n 7 www.chuckeasttom.com



```
C:\Users\Naqib Ali>ping -n 7 www.chuckeasttom.com

Pinging sbsfe-p10r.geo.mf0.yahoodns.net [98.137.244.30] with 32 bytes of data:
Reply from 98.137.244.30: bytes=32 time=327ms TTL=49
Reply from 98.137.244.30: bytes=32 time=338ms TTL=49
Reply from 98.137.244.30: bytes=32 time=376ms TTL=49
Reply from 98.137.244.30: bytes=32 time=501ms TTL=49
Reply from 98.137.244.30: bytes=32 time=384ms TTL=49
Reply from 98.137.244.30: bytes=32 time=415ms TTL=49
Request timed out.

Ping statistics for 98.137.244.30:
    Packets: Sent = 7, Received = 6, Lost = 1 (14% loss),
Approximate round trip times in milli-seconds:
    Minimum = 327ms, Maximum = 501ms, Average = 390ms

C:\Users\Naqib Ali>_
```