**UMKC**

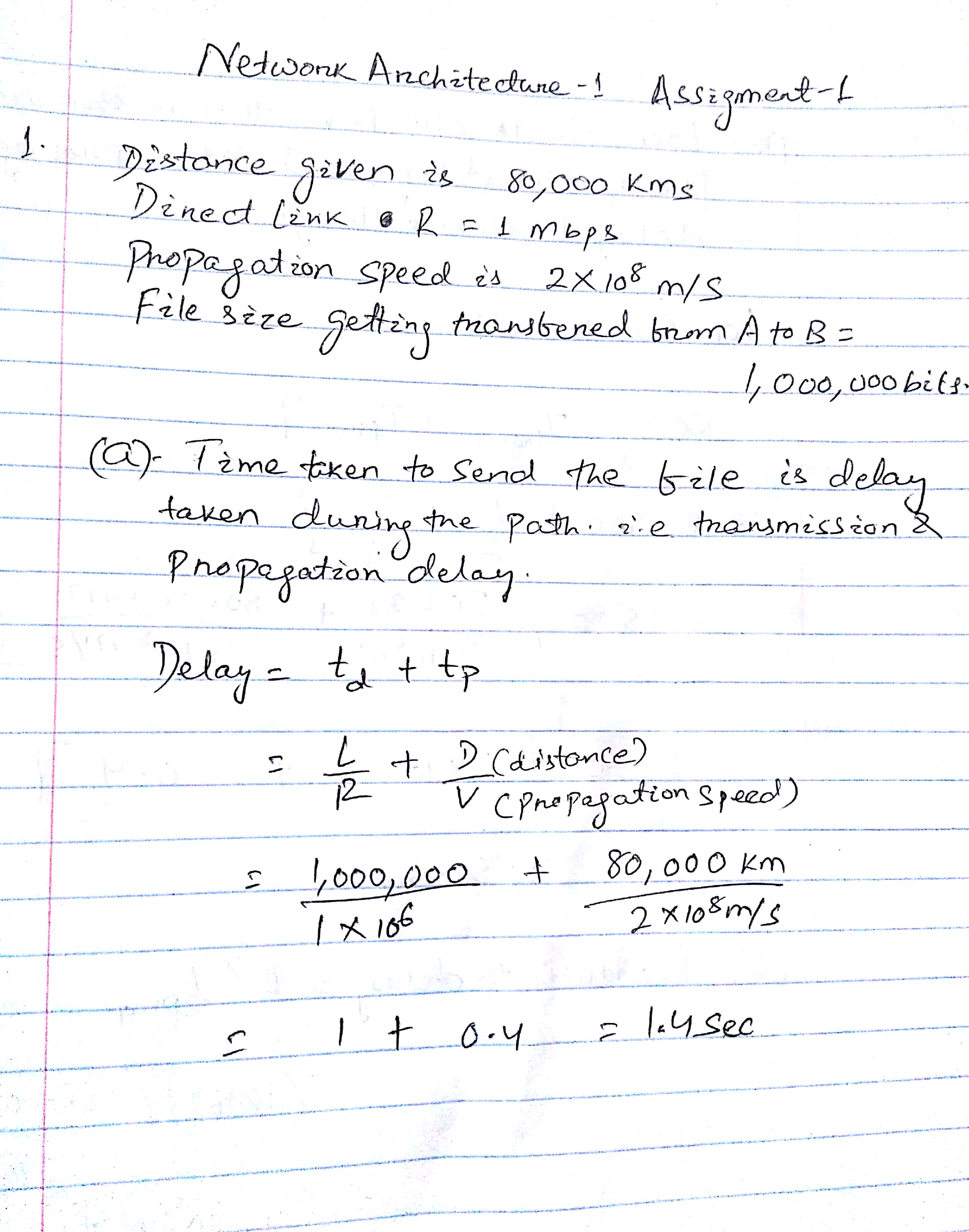
**Dwarkamoye Mohanty**

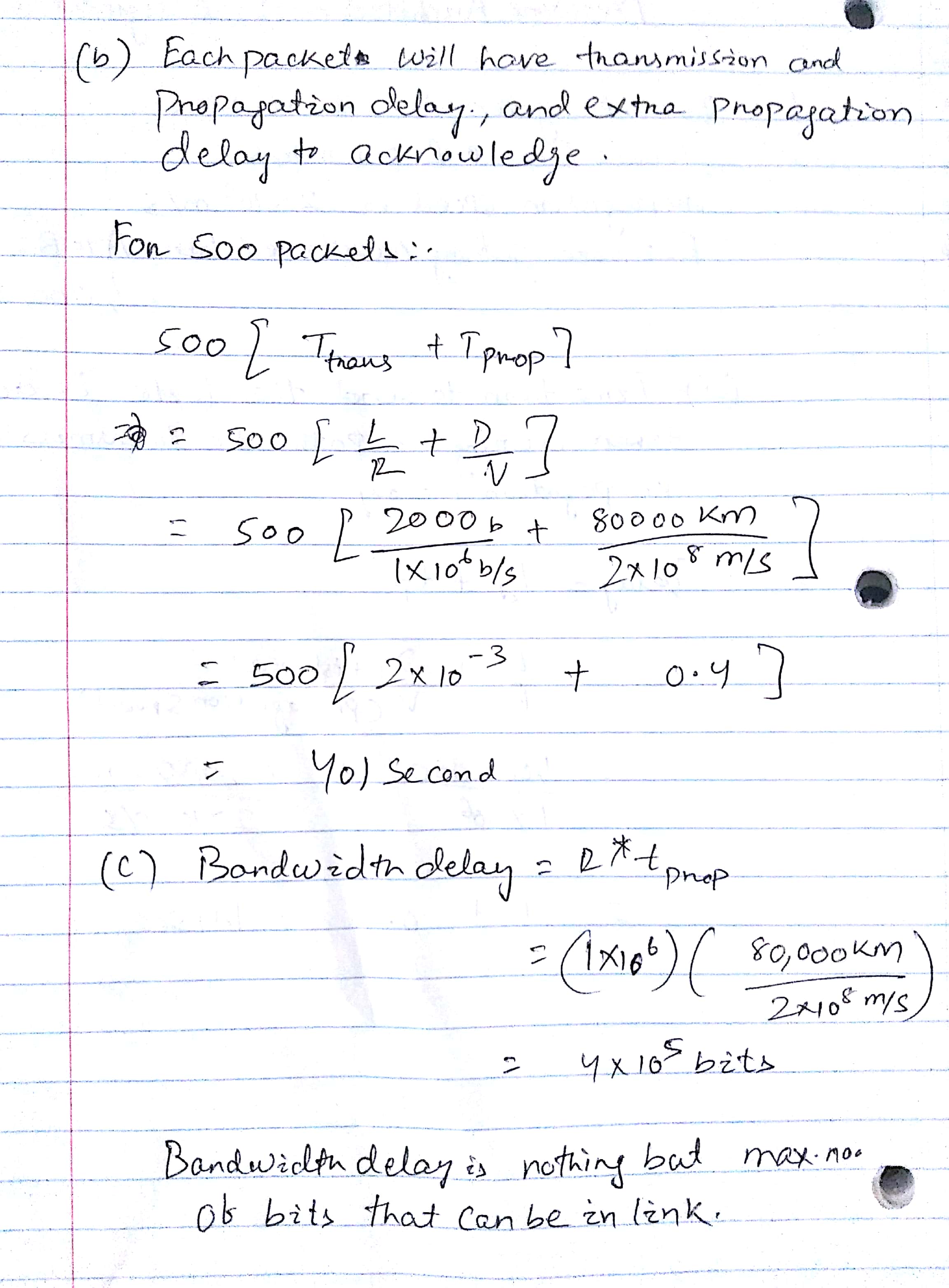
**16281824**

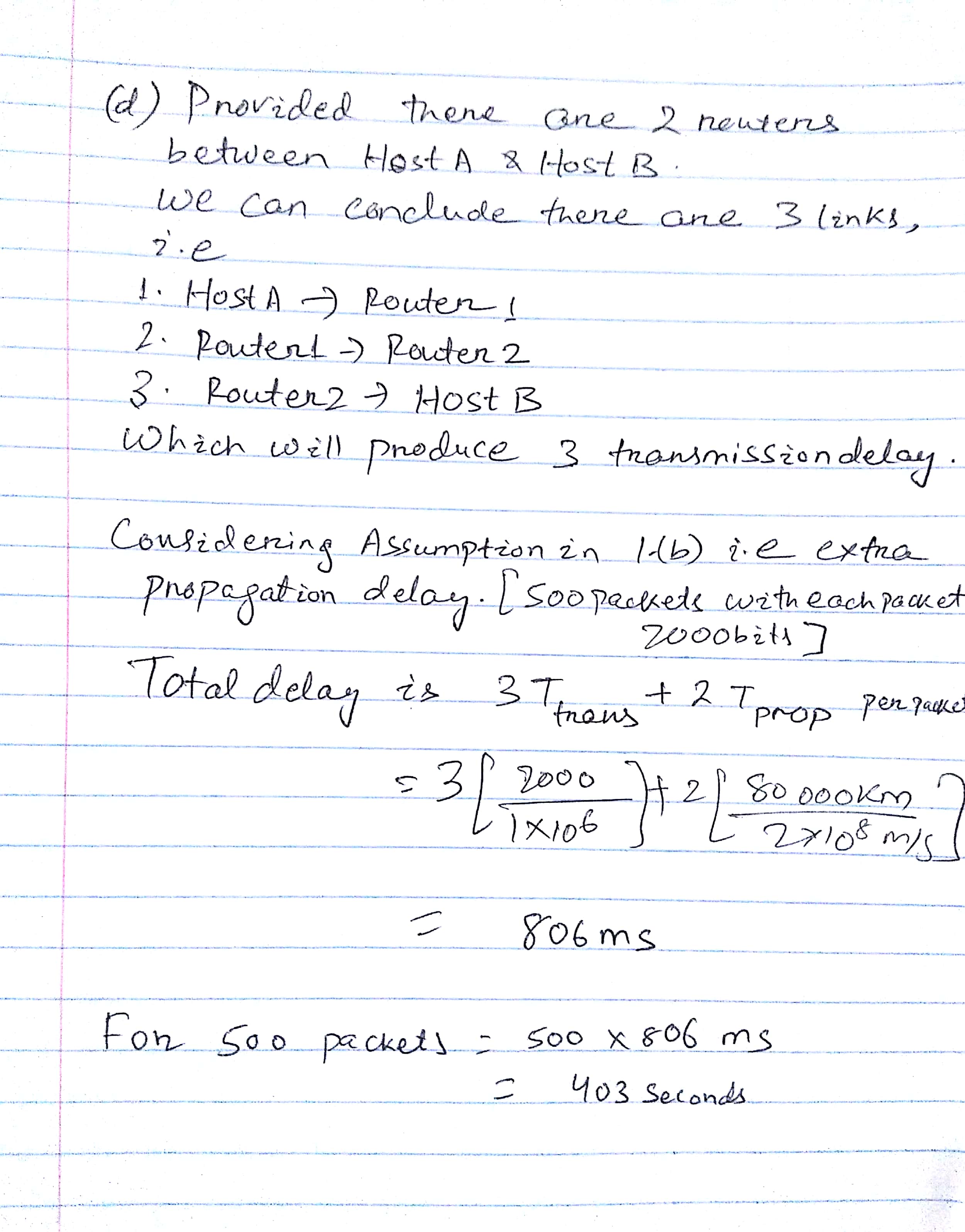
**Network Architecture- 1**

**Assignment- 1**

1.







2.

**Vint Cerf:**

Generally known as a "Father of the Internet," Cerf is the co-planner of the TCP/IP conventions and the design of the Internet. Cerf's group of draftsmen and specialist’s configuration propelled Internet structures for conveying a mix of information, data, voice and video administrations for business and buyer use. He has led the IPv6 forum and has been in the team of U.S Presidential Information Technology Advisory Committee.

His work had created the foundation of every advance discovery in today’s world be it FTP, WWW, Wi-Fi and 3G/4G.

His contributions and inventions speak to all breadth and width and the honorary degrees like Alexander Graham Bell Award, the NEC Computer and communications Prize, the Marconi Prize, the Turing Award will always be talked.

**Bob Metcalfe:**

He started spearheading the Internet in 1970 by building a fast system interface and convention programming between a bundle exchanging ARPAnet IMP and PDP-10 time-sharing minicomputer at MIT Project MAC.

In 1979, Bob established 3Com Corp, supplier of Internet equipment and programming, including the main business usage of TCP/IP and the principal Ethernet for PCs. 3Com opened up to the world in 1984, did $5.7 billion of income in 1999, and converged into Hewlett Packard in 2010.

He was excited about ARPAnet and made it as topic for doctoral dissertation, but he was rejected. During all these he came across a paper in ALOHA network which was having some issues because they were losing packets due to collision as they were using radio waves. This excited him, and he reworked, improved the design which avoided the earlier issue and he also made it as topic of his dissertation. Going ahead he removed his earlier improvements to create the brand-new Ethernet.

3.

(a) Computer Virus: A piece of malicious code or program which once executed alter the computer operation and has the ability to spread from one system to other. It holds potential to cause unexpected or damaging effects to operating system, data stored other programs running in the system. Stealing data and passwords, corrupting data files, spamming contacts and emails are some irritating things virus can do. Extra caution should be taken while surfing web, downloading files and clicking any link or attachment over email. Some computer viruses are: Resident Virus, Polymorphic virus, Boot sector virus, Web scripting virus etc.

(b) Worm : A type of malware which has the ability to get spread from one system to another creating copies of itself. It doesn’t need any human interaction neither attaching to any software program to create havoc. We can always keep an eye on hard drive space as worm creates copies it takes up memory spaces. Sometimes they hamper the speed and performance. They have the ability to modify, delete and inject any malicious software into system. First worm was detected in Iran in July 10 named as Stuxnet.

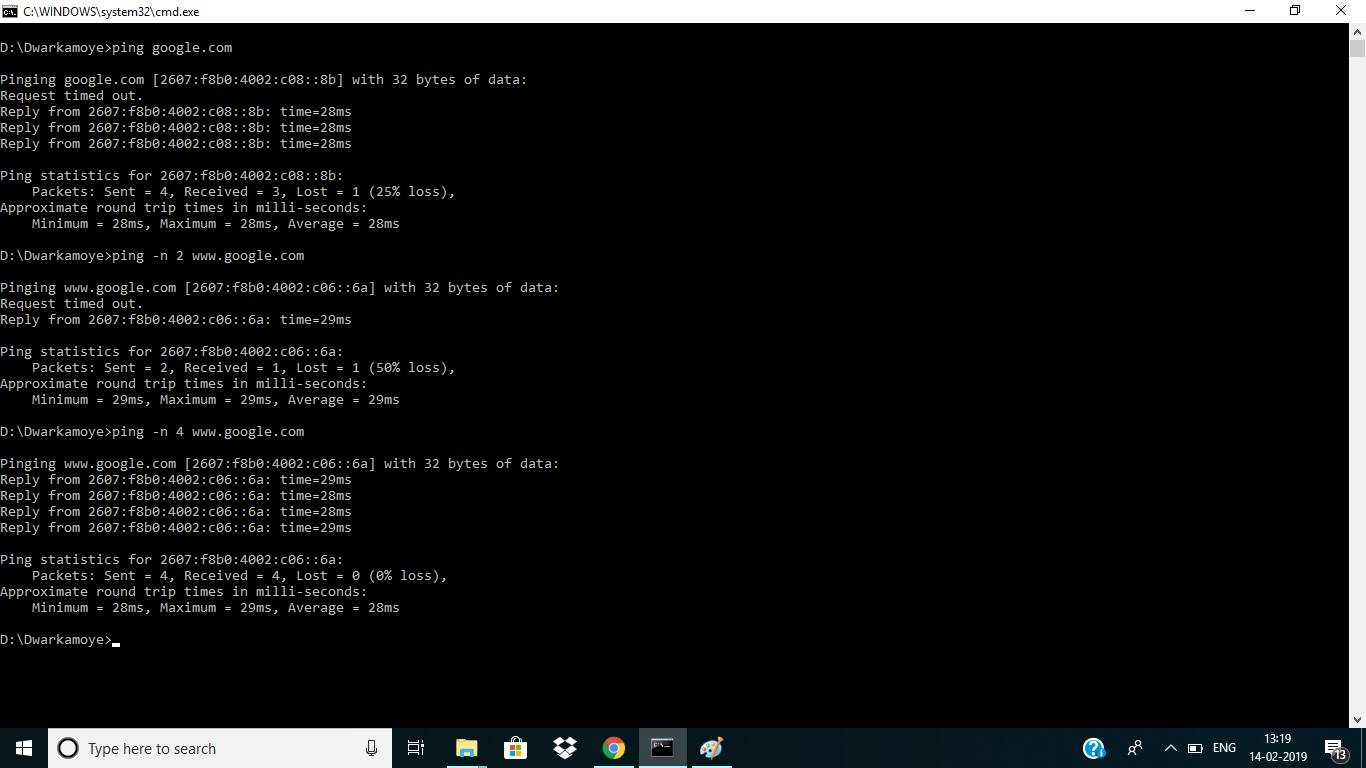
(c) Spyware: Any unwanted software which steals internet usage data and sensitive data by infiltrating in the system. Few activities such as email addresses harvesting, PINS and credit card numbers, tracking browsing habits are the actions of spyware. Sometimes it is injected in disguise, but other times it is included information as license agreement, while not mentioning it, but making user install it which then passes data from the system to third party system of all the activities in the system. It also gets included sometimes if we visit any website which is compromised.

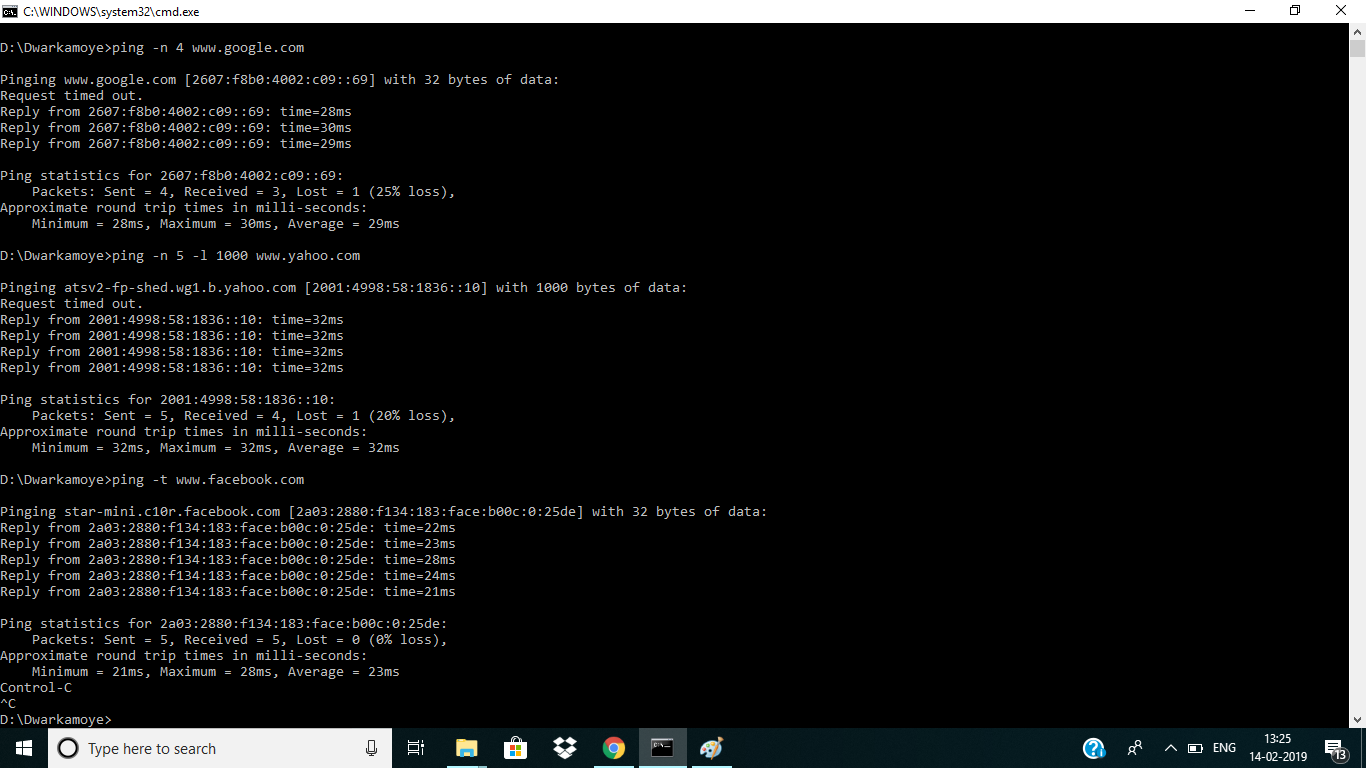
(d) Malware: Malware is a term for malicious software. The software which is written to harm other system, to steal data, to get access to sensitive data. This has grown recent times due to money-making reasons using other’s data. Spyware, ransomware, virus, worm are the malware types. The security of the system is more important to avoid malware like defects in OS design, giving user too many permissions or installing abrupt applications, surfing suspicious website not updating antivirus program regularly.

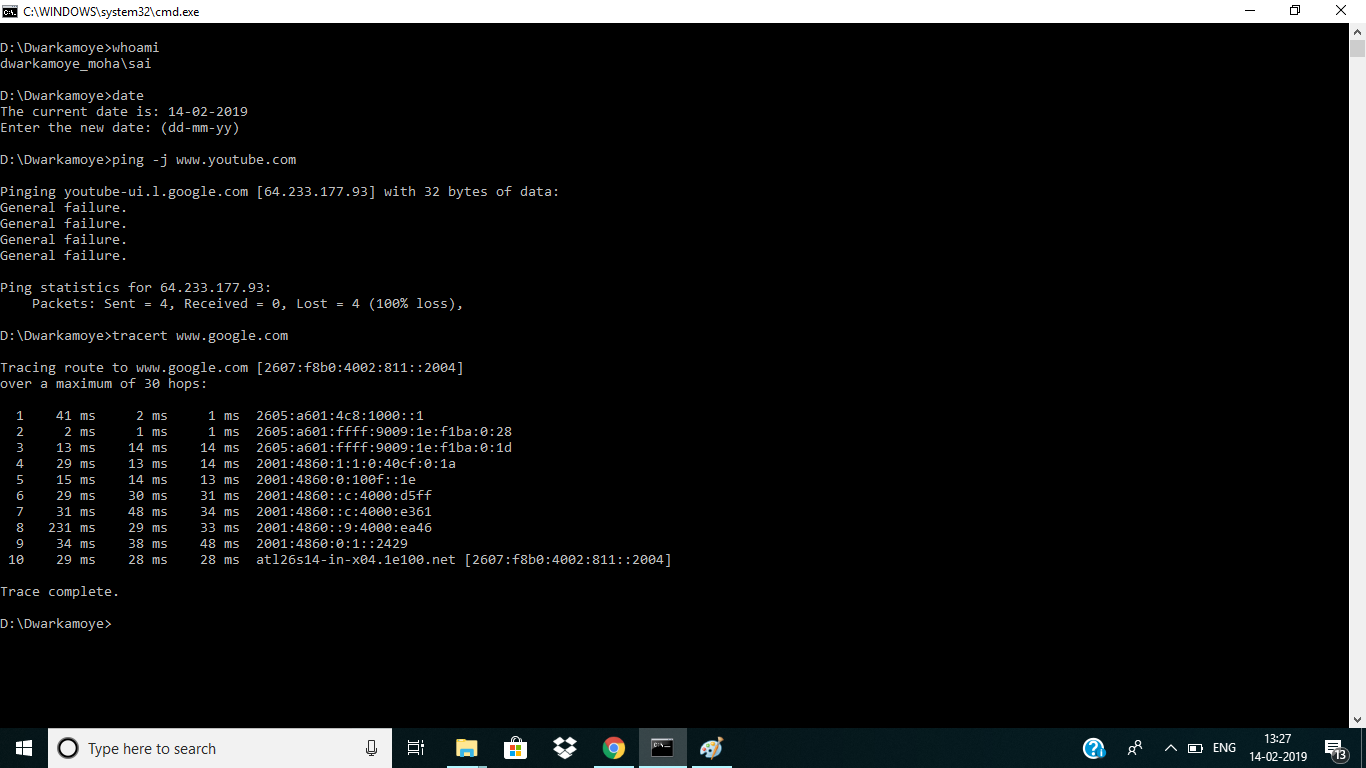
(e) Trojan Horse: A Trojan horse is not a virus technically. Unlike a computer virus, a Trojan horse is not able to replicate itself, nor can it propagate without an end user's assistance. Attackers use social engineering tactics to trick the end user into executing the Trojan without there knowledge. Typically, the malware programming is hidden in an email attachment or free download. When the user clicks on the email attachment or downloads the free program, the malware that is hidden inside is transferred to the system.

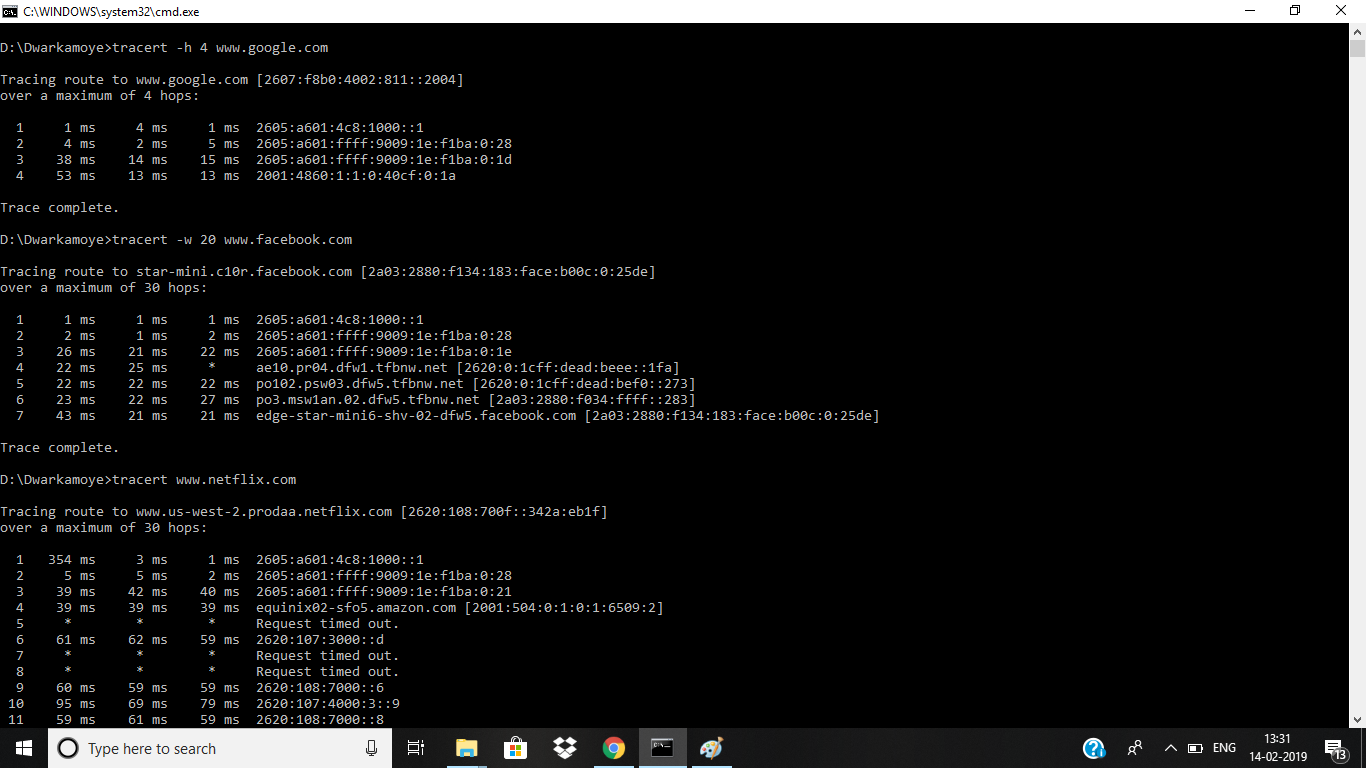
(f) Botnet: A botnet is a group of computers connected in a coordinated fashion intended to serve malware activities. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam. This is like an ecosystem which survives when malware is spread making the system compromised and serving as an extra bot. Attackers attack system without firewalls and antivirus software. This is gaining more attention as planned crime and illegal activities can be conducted using these.

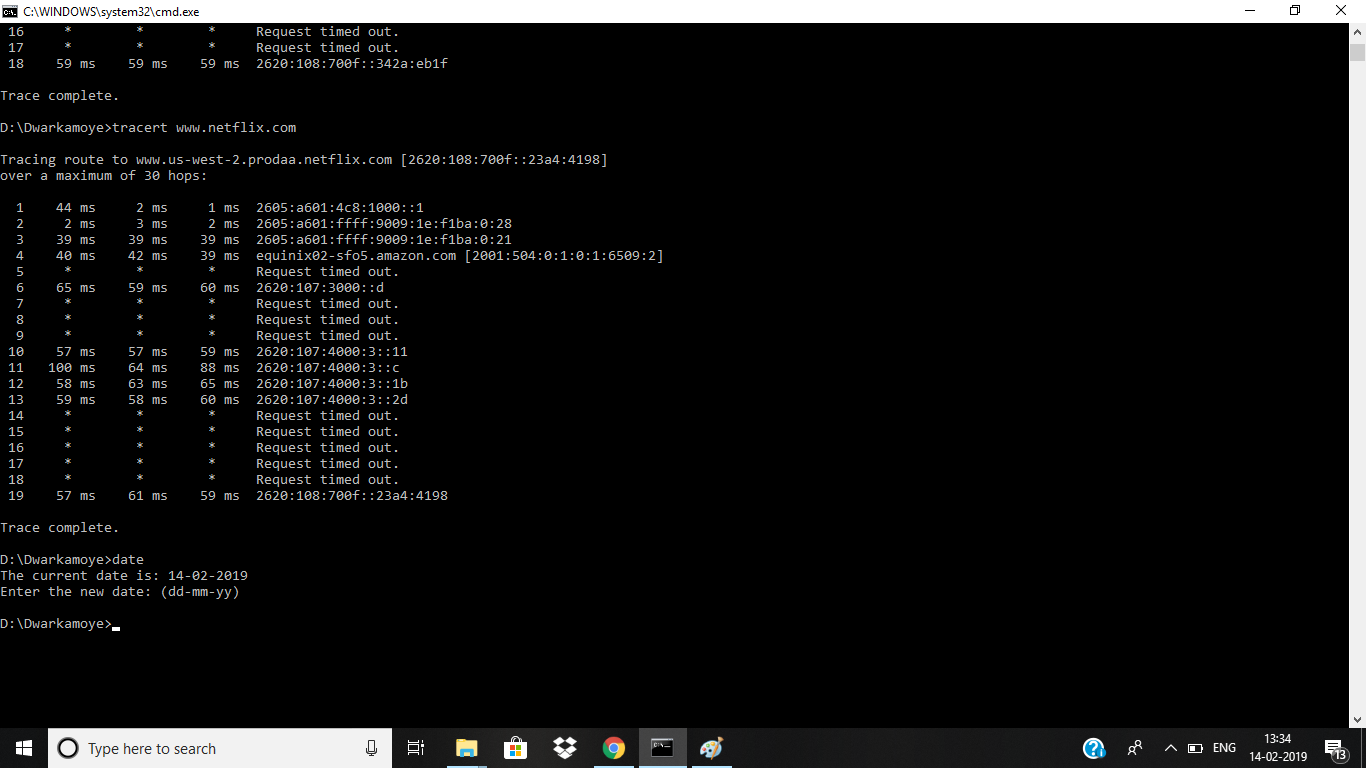
4.Ping and traceroute





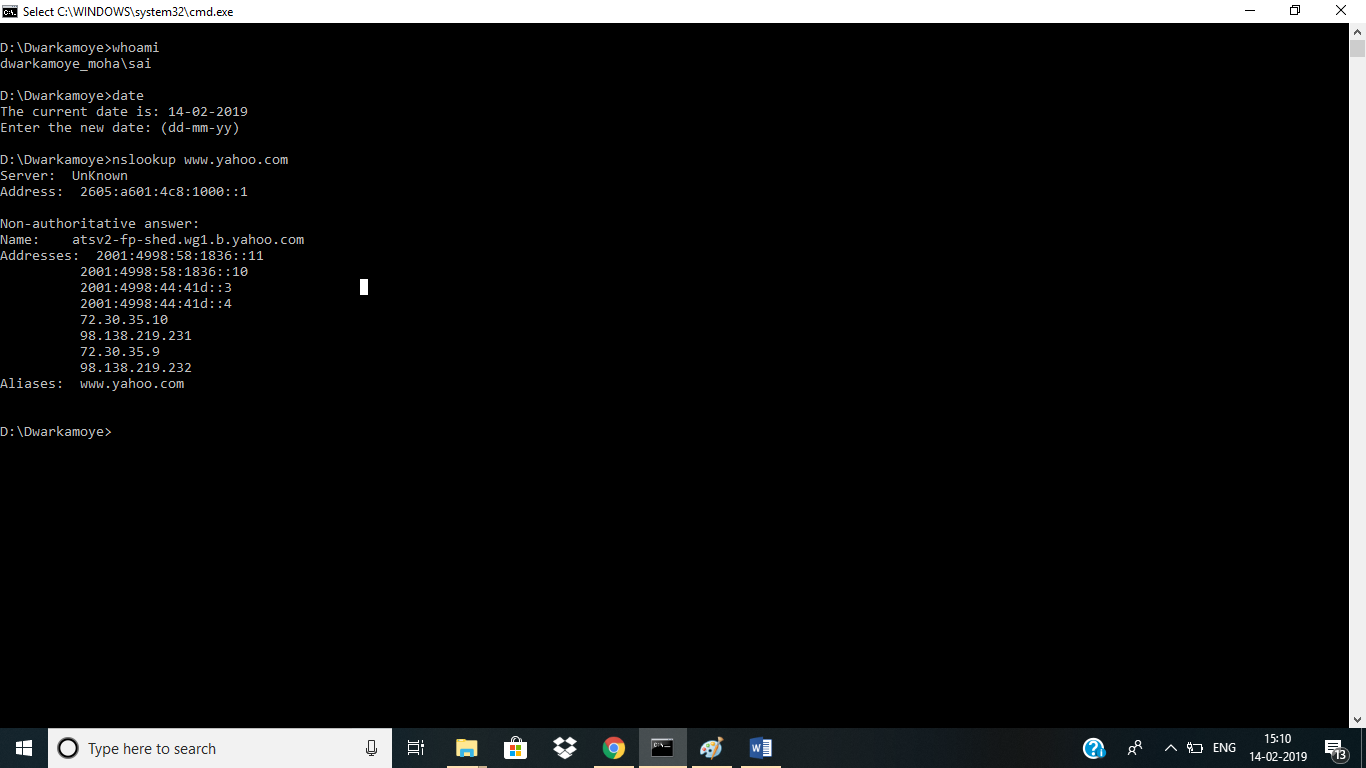




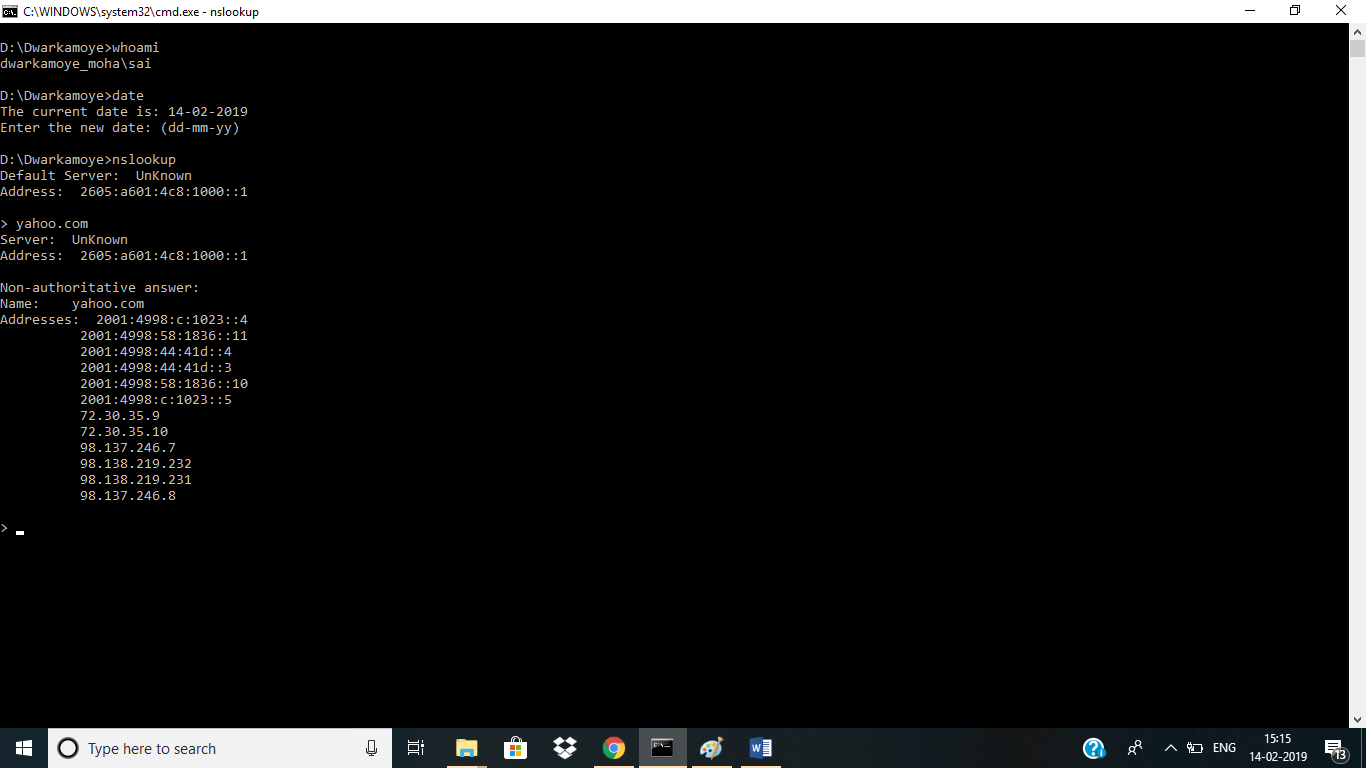


5.

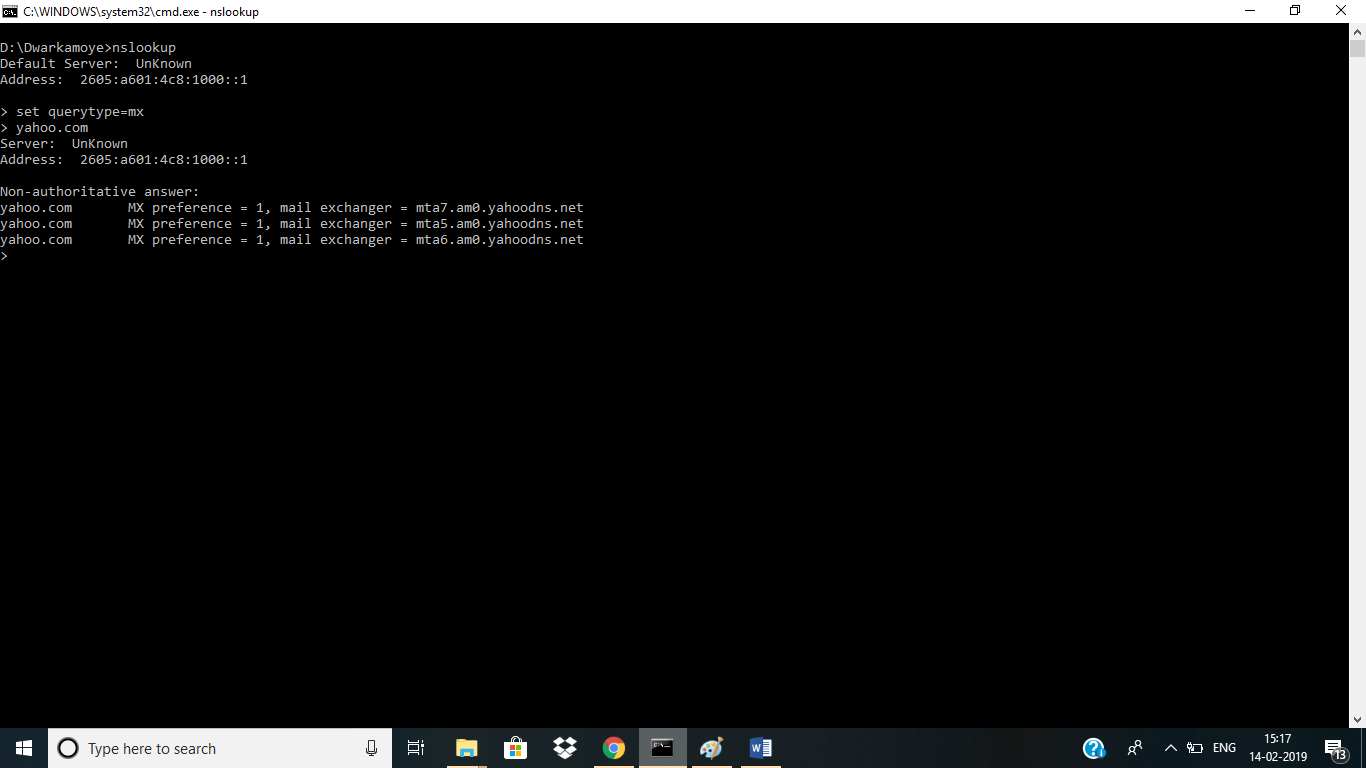
(a)



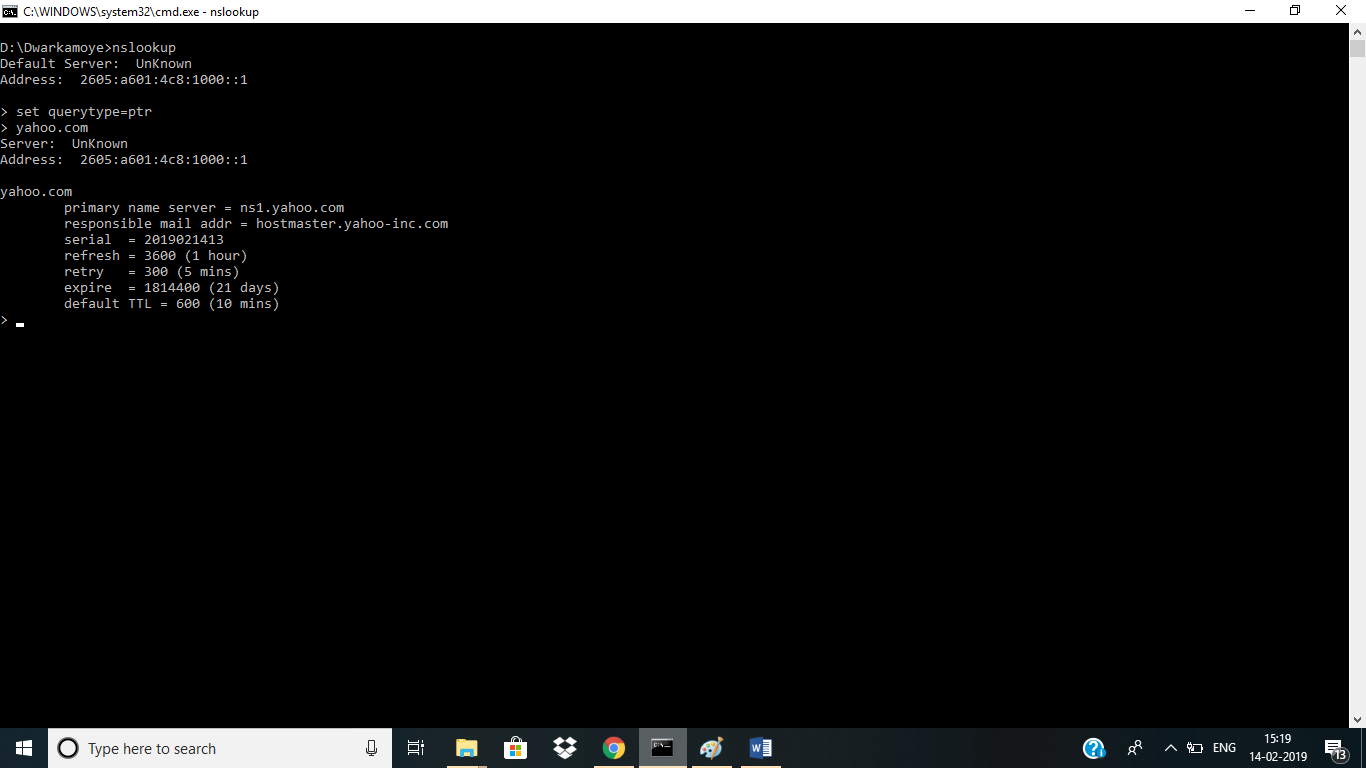
(b)



(c)



(d)



6.

There are numerous RFCs at present and we can discover them dependent on their status. The status may be web standard, draft standard, proposed standard, uncategorized (Early RFCs), official web convention principles. Ongoing RFCs incorporate RFC 8428, RFC 8443, RFC 8433, RFC 8409, RFC 8434, RFC 8435, RFC 8437, RFC 8438, RFC 8453, RFC 8436 and so on. The above recorded RFCs have their possessed application.

The five active working groups in different areas include:

* avtcore
* taps
* git
* dhc
* netconf

Among these gatherings, I need to examine about taps (transport administrations) amass from transport zone. The principle points of TAPS (transport administrations) assemble is to control system and application software engineers by giving a theoretical path for applications to make utilization of the administrations of transport layer. The taps characterize the significance of transport administrations given by transport layer and recognizes the administrations given by dynamic IETF conventions and clog control instruments. In the underlying stage, they will consider administrations gave between two end focuses. Now and again application software engineers face trouble on the off chance that they use conventions other than UDP and TCP. In greatest cases organize stacks run with just TCP and UDP as their transport conventions. Greatest firewalls just permit TCP and UDP and just some permit TCP as it conveys HTTP as its payload. So, utilizing different conventions or building another vehicle convention result in application get to disappointment. Such a large number of utilizations by and large use TCP and UDP as their transport conventions.

There are some predefined records which are distributed just as talked about in this gathering which incorporates:

* A Survey of Transport Security Protocols
* An Architecture for Transport Services
* An Abstract Application layer Interface to Transport Services