Computer Networks Assignment-1
Ramya Vellore Ramesh (219123243)

1.1

Arp: manipulates the kernel's ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting up one. Option **–v,--verbose** tells the user what is going on by being verbose.**-n,--numeric** shows numerical addresses instead of trying to determine symbolic host, port or user names. **-a [hostname], --all [hostname]** option shows the entries of the specified hosts. If the hostname parameter is not used, all entries will be displayed. **-d hostname,** --delete hostname option removes any entry for the specified host.

arping: sends ARP **(**Address Resolution Protocol**)** to a neighbor host. **–b** option sends only MAC level broadcasts. Normally arping starts from sending broadcast, and switch to unicast after reply received**. -c** count option stops after sending count ARP REQUEST packets. With deadline option, arping waits for count ARP REPLY packets, until the timeout expires. **-I** interface specifies the name of network device where to send ARP REQUEST packets. This option is required. **–U** Unsolicited ARP mode to update neighbors' ARP caches. No replies are expected.

ifconfig: used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. **interface** option specifies the name of the interface. This is usually a driver name followed by a unit number, for example eth0 for the first Ethernet interface. **up** - flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface. **down**-flag causes the driver for this interface to be shut down.**[-]arp** enables or disables the use of the ARP protocol on this interface.

tcpdump: prints out a description of the contents of packets on a network interface that match the boolean expression. **–A** option prints each packet (minus its link level header) in ASCII. Handy for capturing web pages.**-c** is used to exit after receiving count packets.**-C** is used before writing a raw packet to a save file, check whether the file is currently larger than file size and, if so,we close the current save file and open a new one.

ping: sends ICMP ECHO_REQUEST to network hosts.**-A** Adaptive ping. Interpacket interval adapts to round-trip time, so that effectively not more than one (or more, if preload is set) unanswered probes present in the network.**-b** allow pinging a broadcast address.**-B** option does not allow ping to change source address of probes. The address is bound to one selected when ping starts. **-i** interval option is used to wait interval seconds between sending each packet.

netstat: prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships**. --verbose , -v** tells the user what is going on by being verbose. Especially print some useful information about unconfigured address families.**--numeric , -n** shows numerical addresses instead of trying to determine symbolic host, port or user names.**--numeric-hosts** shows numerical host addresses but does not affect the resolution of port or user names.**--numeric-ports** shows numerical port numbers but does not affect the resolution of host or user names.

traceroute: prints the route packets trace to network host. **-4, -6** option explicitly forces IPv4 or IPv6 traceouting. By default, the program will try to resolve the name given, and choose the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, traceroute will use IPv4.**-I**: specifies ICMP ECHO to use for probes.**-T**: specifies TCP SYN to use for probes.**-d** option enables socket level debugging .**-F** option specifies not to fragment probe packets.

nslookup: queries internet name servers interactively. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.**IN**-the Internet class.**CH**-the Chaos class.**HS**-the Hesiod class. **host [server]** -look up information for host using the current default server or using server, if specified.

wireshark: androiddump - provides interfaces to capture from Android devices. **capinfos** - prints information about capture files .**captype** - prints the types of capture files.**ciscodump** - provide interfaces to capture from a remote Cisco router through SSH.**dftest** - shows display filter byte-code, for debugging dfilter routines.**dumpcap** - dump network traffic .**editcap** - edit and/or translate the format of capture files. **mergecap** - Merges two or more capture files into one

1.2

a. http.cap :

1) What is the IP address of the client?

145.254.160.237 is the IP address of the client.

2) In packet 4, explain which transport protocol is being used, which http command

is used, and what source port is used?

- TCP is being used as transport protocol in packet 4 to issue a GET command to the server.
- GET is the http command being used.
- the source port no is 3372.

3) In packet 38, what is the Last-Modified field set to?

Tue,20 Apr 2004 13:17:00 GMT\r\n

b. dns.cap :

1) In packet 1, what is the name being looked up? Is recursion desired? What is the IP address of the DNS server? Which transport protocol is being used?

- google.com is the name being looked up.
- In packet 1,recursion desired bit is set to 1.If the Available bit is set in response, then recursion is available, otherwise it isn't.Here the recursion available bit is not set to 1 in the response.Hence recursion is not desired.
- 192.168.170.20
- UDP is the transport protocol.

2) In packet 3, what type of lookup is requested?

Reverse DNS lookup is requested.

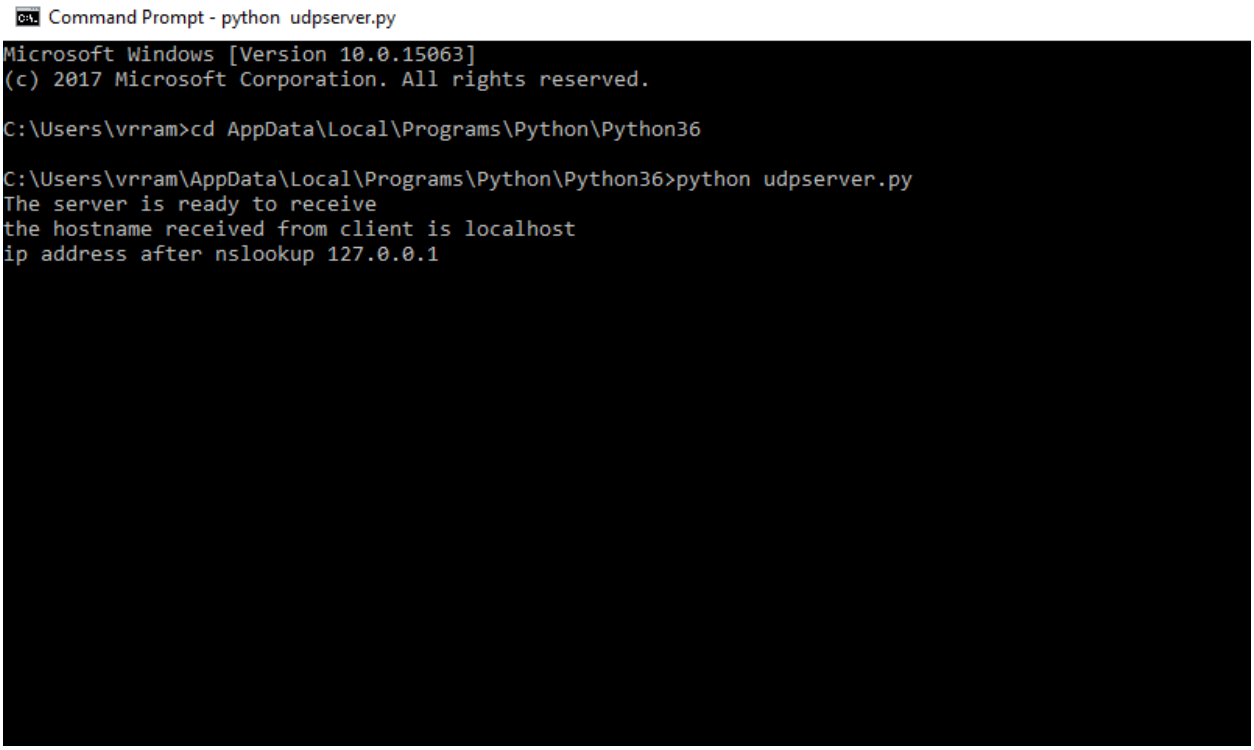
3) In packet 4, what is the host name in the first answer? What type of resource record type contains this? What is the IP address of this host name? What resource record type contains this?

- google.com is the host name in the first answer
- Mail exchanger (MX) resource record type contains this
- 192.168.170.20 is the IP address of the host name
- Type A resource record type contains this

3a

udpserver.py

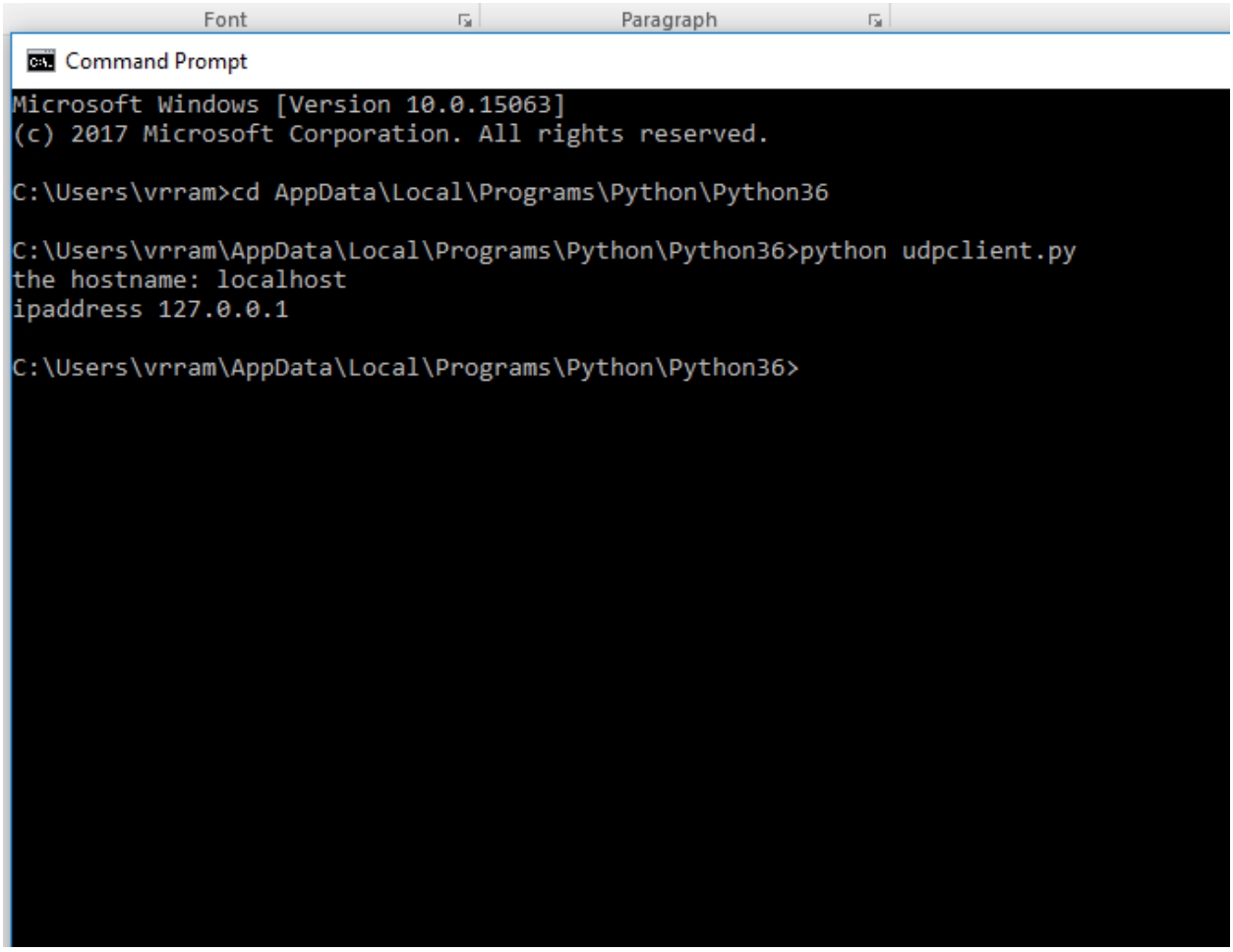
hostname: localhost



Computer Networks Assignment-1
Ramya Vellore Ramesh (219123243)

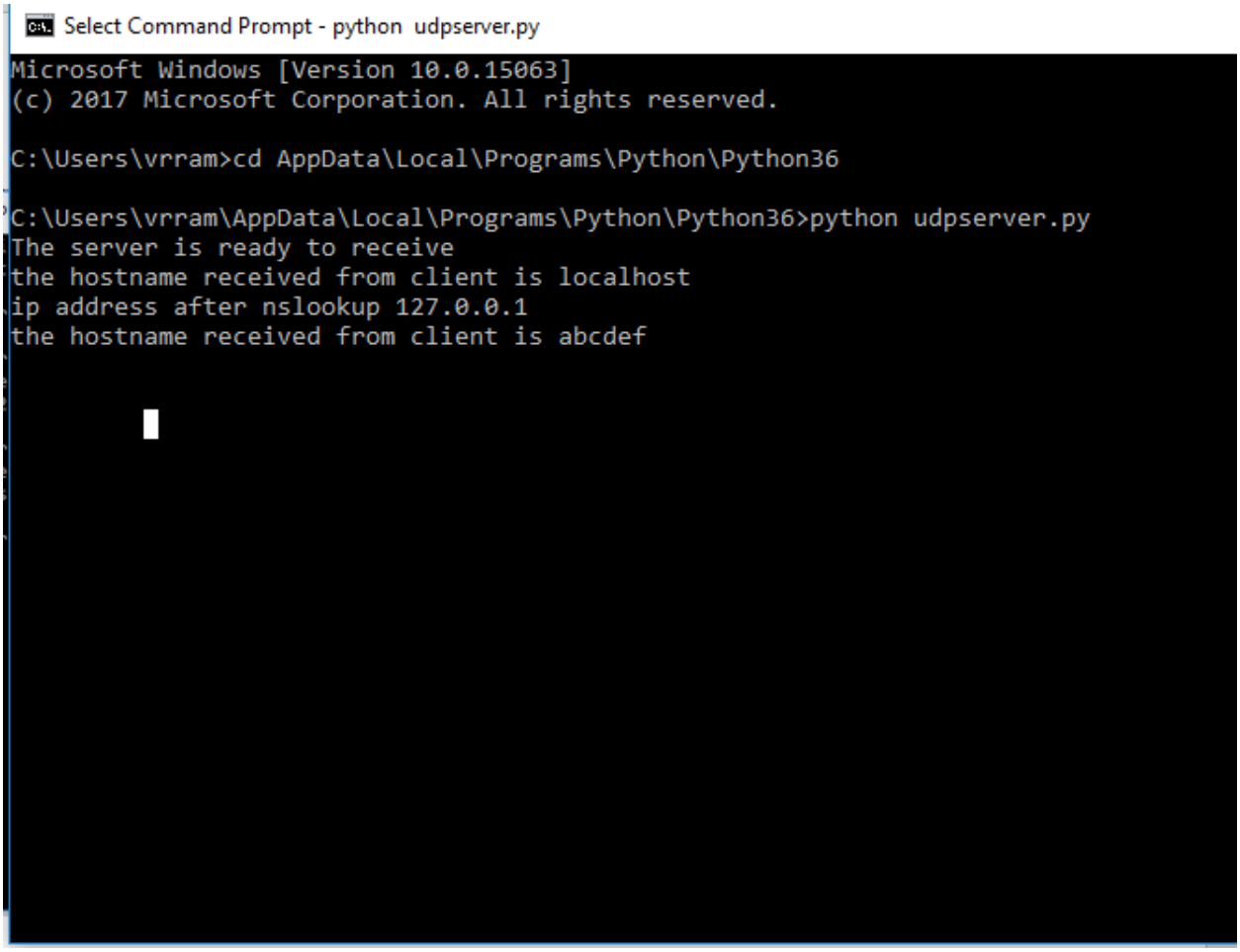
udpclient.py

ipaddress:127.0.0.1



udpserver.py

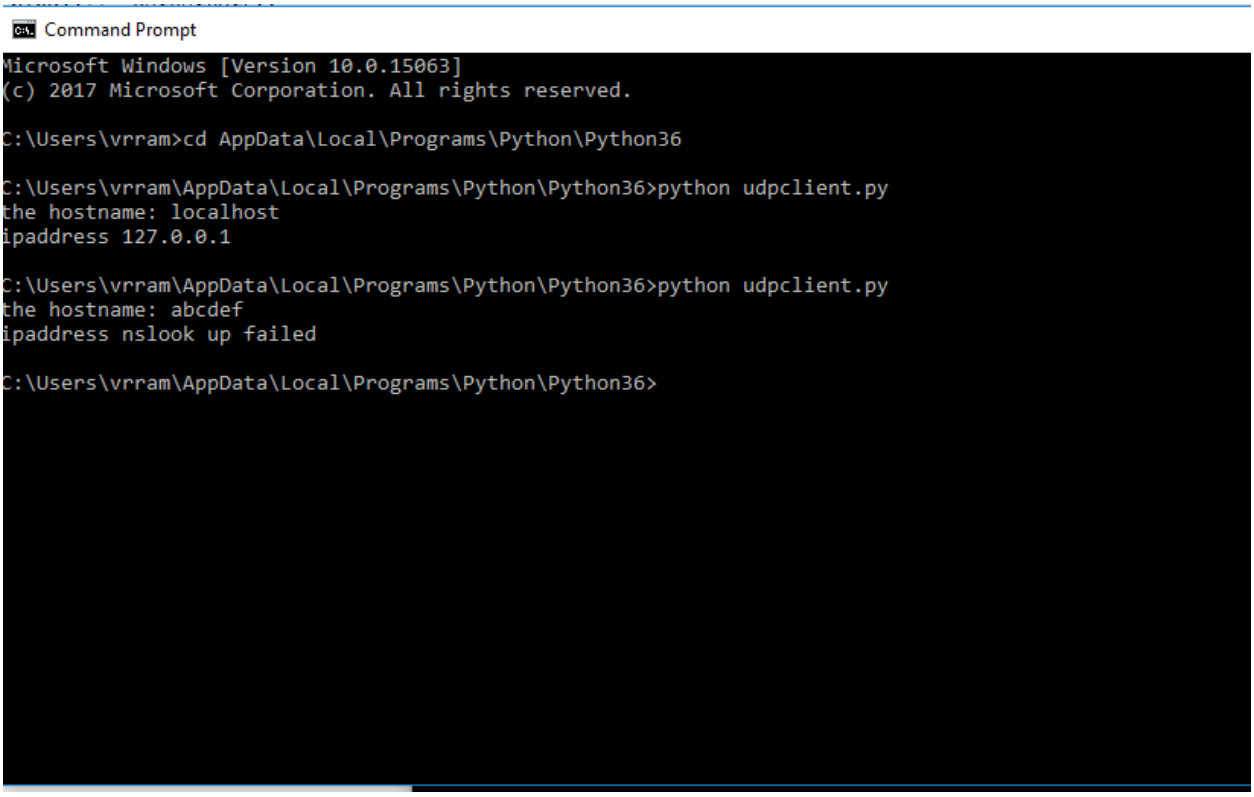
hostname: abcdef



Computer Networks Assignment-1
Ramya Vellore Ramesh (219123243)

udpclient.py

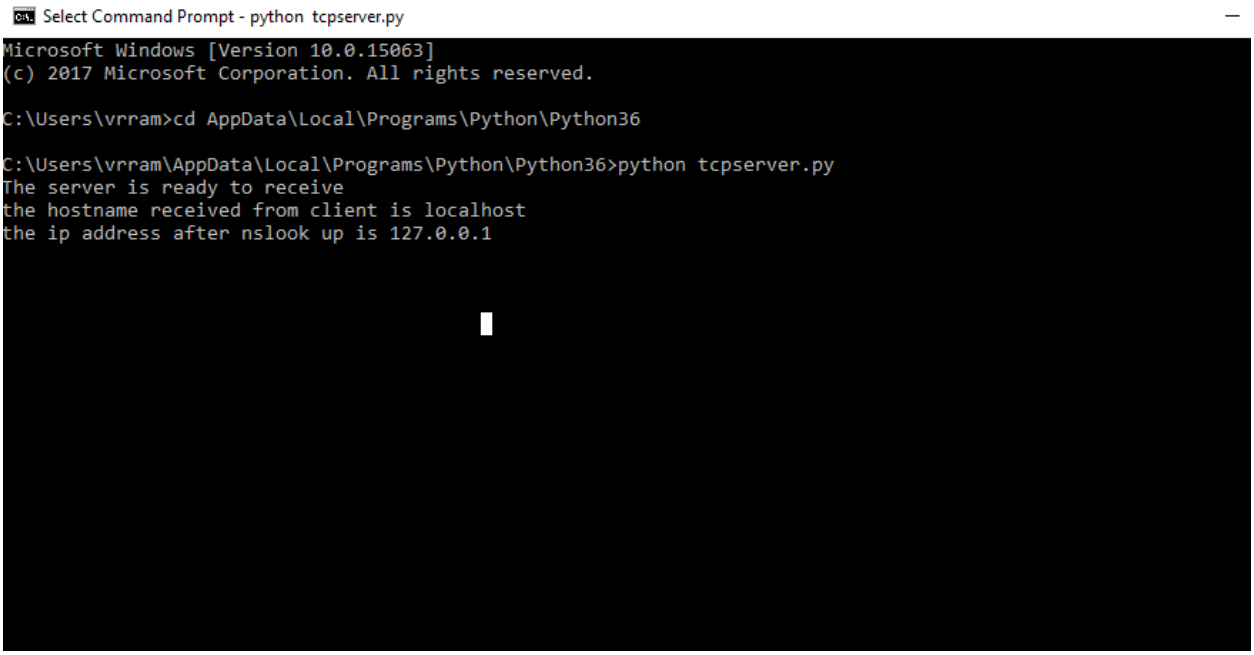
nslook up failed



3b.

tcpserver.py

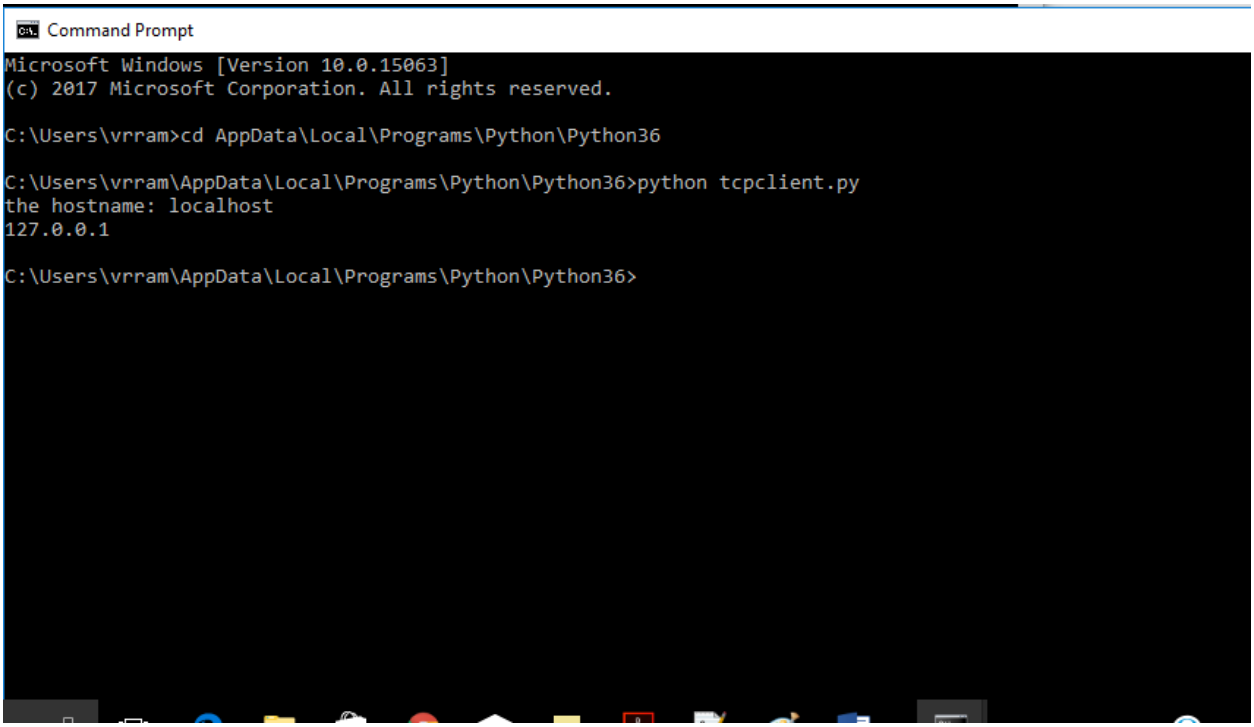
hostname: localhost



Computer Networks Assignment-1
Ramya Vellore Ramesh (219123243)

tcpclient.py

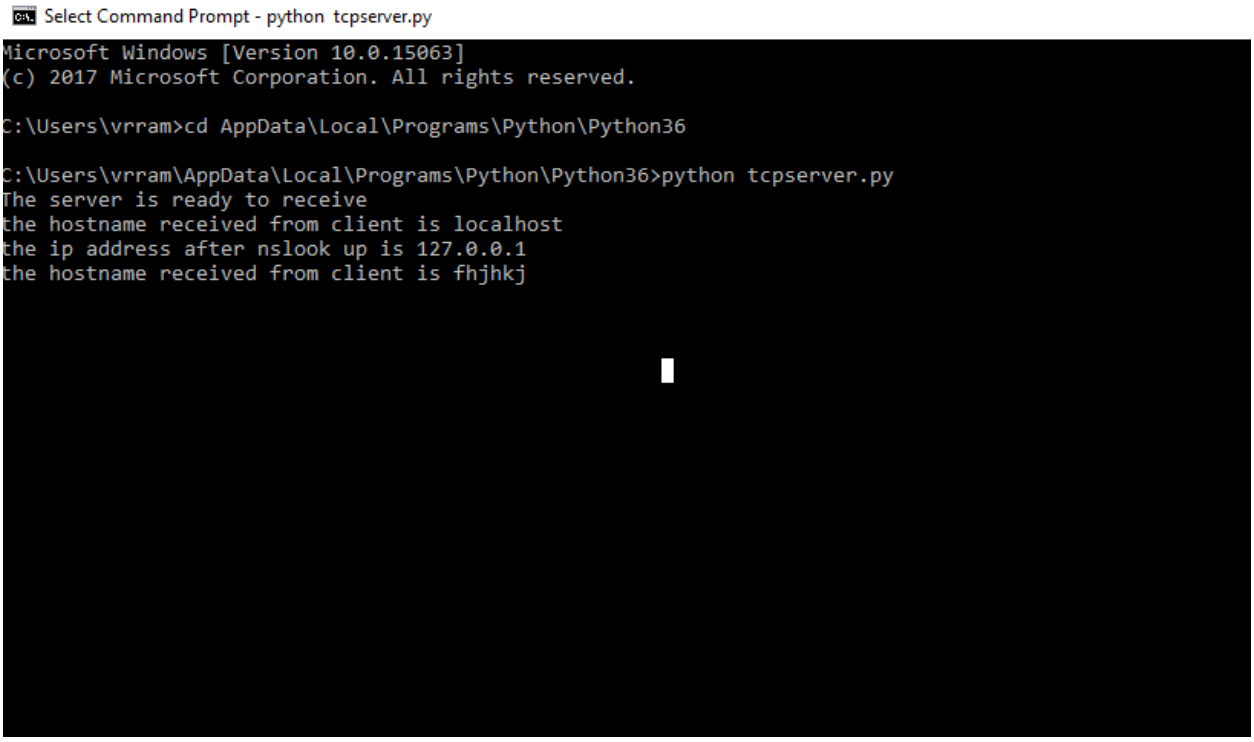
ipaddress 127.0.0.1



Computer Networks Assignment-1
Ramya Vellore Ramesh (219123243)

tcpserver.py

hostname: fhjhkj



tcpclient.py

nslook up failed