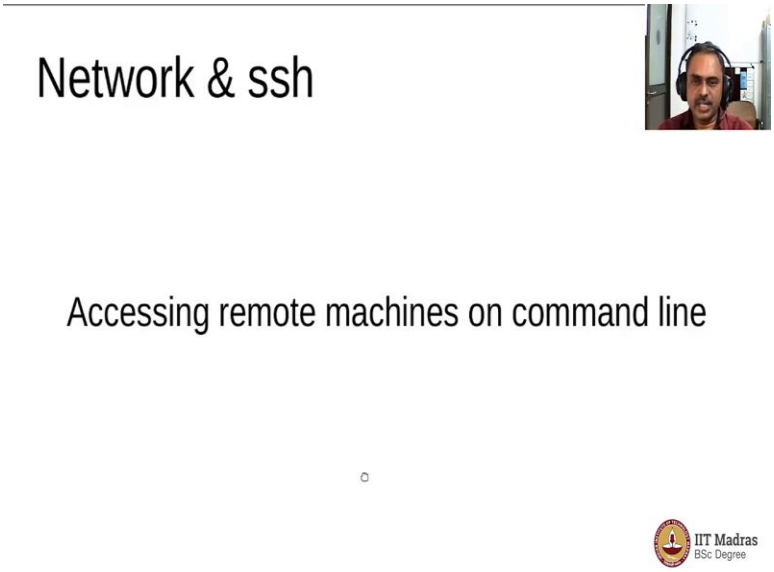
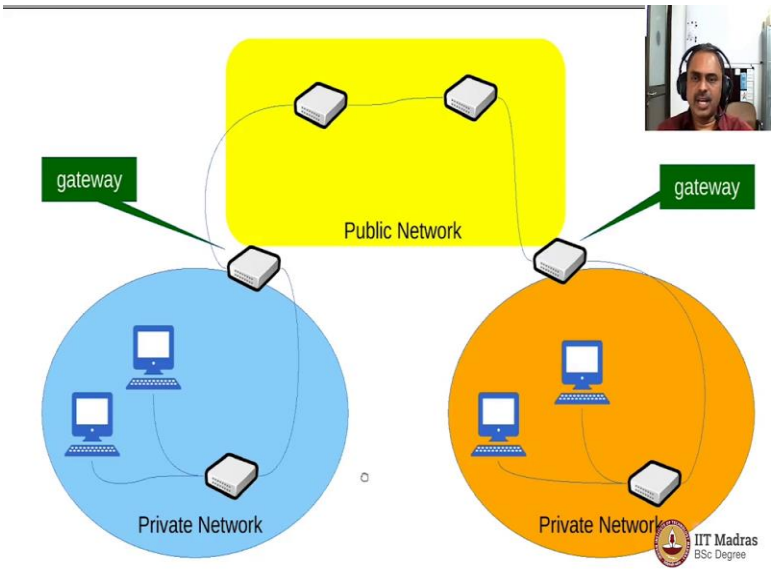
Systems Command
Professor Gandham Phanikumar
Metallurgical and Materials Engineering
Indian Institute of Technology, Madras
Networking Commands and SSH

(Refer Slide Time: 00:14)



Welcome to this session on Network and ssh. In this session we will look at how to access remote machines using a command line utility.

(Refer Slide Time: 00:25)



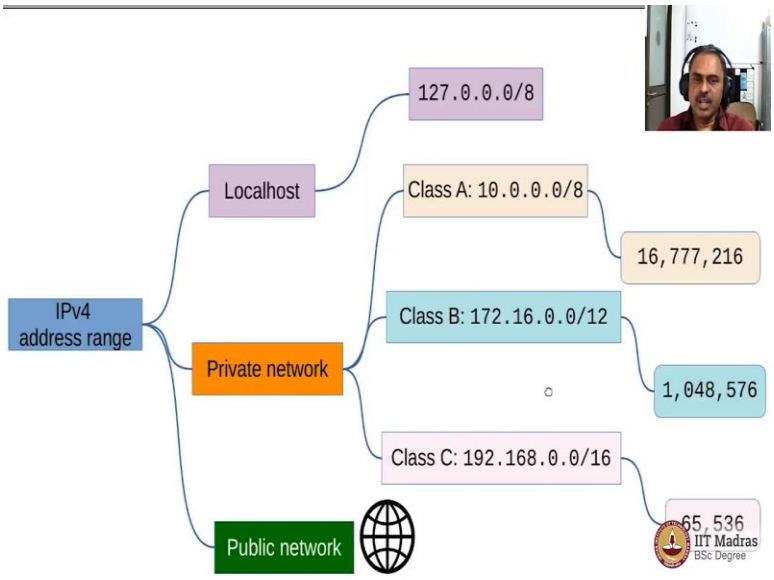
So, here is how most of our daily life would be that is, we are at home in a private network, our computer is connected to the telephone as a hotspot and then the telephone is then connected to the internet service provider, let us say Jio or Airtel or whatever, and then it is able to access the internet.

So, public network is basically the internet and a lot of routing of packets happen within the internet. And from our home, we would like to access let us say a particular website. So, that website may be sitting in another network of a different campus or organization. So, for example, sitting at home in your hometown, you want to access the website of IIT Madras.

So, the IIT Madras is this blue private network, let us say and one of those computers running the web server of IIT Madras would then be making its content available through the campus LAN followed by a network switch, which then pass on the content onto the public network, which will come through all these connections to the internet service provider for your home telephonic network, and then onto your computer device.

So, that you can look at the homepage. And all of this happens within a fraction of a millisecond. So, that you are having a very live experience of browsing. Now, what it is also important for us to realize is that we do not have a direct access to the private networks in respect to organizations.

(Refer Slide Time: 01:59)



So, we need to understand how is that made possible. So, the way it is made possible is because of the different type of IP addresses that are given. So, there are two types of IP addresses. So, the version 4 and version 6. So here I am giving the examples of the IPv4 version 4, which are still being used.

So, there are three types of addresses that you would have in a machine. One address that will be there for every machine is the so-called local host address. Whereby the system can refer to itself. So, if it wants to refer to itself through any network connection, there must be some address. So, the local host address is 127 dot 0 dot 0 dot 0 and then after the 4 digit or 4 path IP address, there is a slash and then a number is given.

It tells you how many IP addresses are possible with that particular combination. And so, you can see that most of the computers will have an IP address which is 127 dot 0 dot 0 dot 1 and some may have more of those type of series depending upon the configuration. Now, any private network IP address would be falling into one of the three categories here listed as class A, class B or class C.

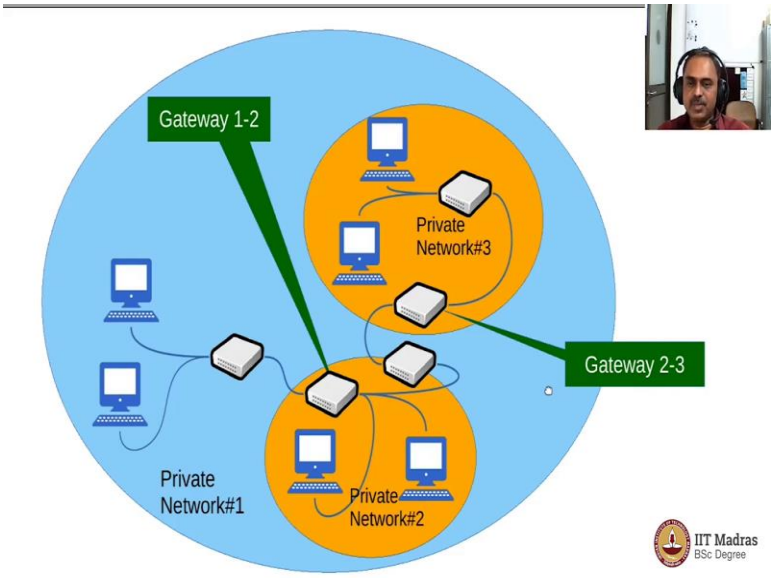
So, class A is the kind of network meant for large organizations let us say, IIT Madras campus LAN or (())(03:28) LAN or the Infosys internal LAN. So, all of these have several thousands of computers if not tens of thousands. So, the IP address range will be 10 dot and after that the three parts can be any number between 0 and 255.

And that would give you a total of 16 million IP addresses that are possible. So, a large organization can assign these IP addresses to the machines within its organization. The class B addresses are starting with 172 dot 16 and then the last two parts can be varied and you have about 1 million IP addresses that are possible.

Now, class C would actually have 65,000 IP addresses that are possible. So, now these three addresses 10 dot something 172 dot 16 dot something 192 dot 168 dot something these three addresses are called the private addresses, which means there cannot be any publicly visible website or a service provider with these addresses because they will not be honoured by the routing machines that take the packets from your machine to another machine. And every other

address would then fall into the category of a public network which I have shown you here as the globe.

(Refer Slide Time: 04:45)

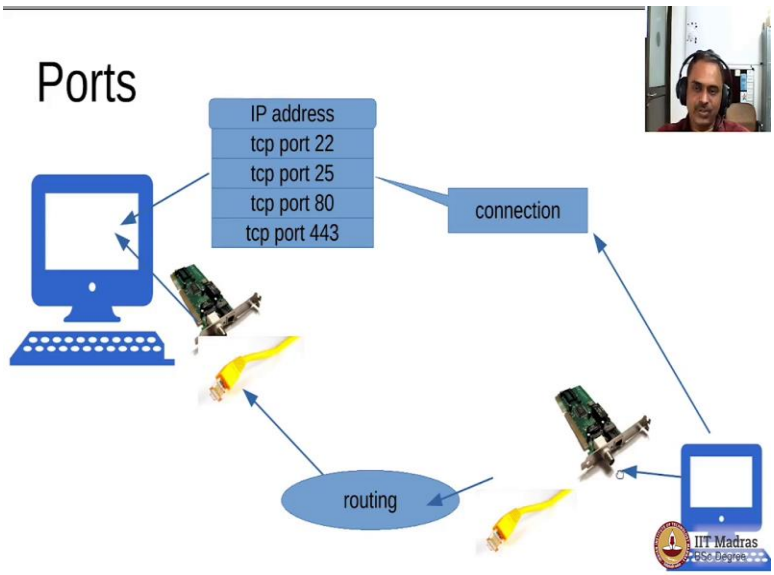


Now, when you have the 3 types of addresses, you can actually have a possibility that within a private network, you can have multiple private networks up to 3 levels of hierarchy, because you have three address range that are possible. And you can actually prevent access from anyone within the campus LAN to access your private network.

And let us say this private network 2 is the computer centre and private network 3 is for example, an internal network within the computer centre. So, you can actually protect a storage box connected to a high-performance computer from the campus user by having two layers of routing that is required to reach it.

And you can have rules for these switches in such a way that a storage box within the private network is not visible to campus user and definitely not to a user from outside is a public internet. So, this is how basically we are able to protect our machines as far as the network access is concerned. Of course, there are ways by which a person can penetrate into the network, campus network take control of one of the machines and thereby cause harm. So, those safety nets also have to be thought of.

(Refer Slide Time: 06:07)

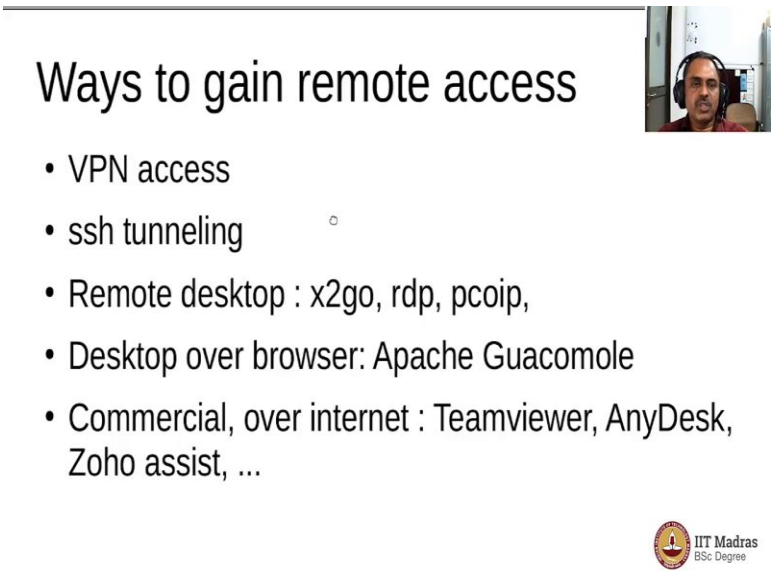


Now, the concept of port is also something that we must be familiar. So, when a computer is connecting to another computer. So, we may see that as a physical connection, where the network card is connected with a wire which goes into a network switch, and then some routing happens and then those packets are going through a wire to the network card into the other machine.

So, that is the physical network. But the connection itself needs to talk to the IP address of the server on a specific port, it is like when you go to the bank, you have various counters, one counter is to get your passbook printed, updated et cetera and let us say another counter is for your service queries.

And a third counter is to open accounts, new accounts, and a fourth counter maybe to pick up cash from your savings bank. Now, it is the same bank on the other side of the desk, but each window is meant for his particular action. Similarly, network connections are also like that each port number is meant for a particular service. So, what are those services and these port numbers are already standardized. So, what are those mappings is something that we need to look at.

(Refer Slide Time: 07:21)



So before that, I want to also tell you that if you want to get access to a remote computer. So, you can actually get it in many ways. So, virtual private network is one way. So, all IIT Madras matters, students have ability to connect from their home, as if they are coming from the campus by a VPN account, if they have a good reason to have that particular facility.

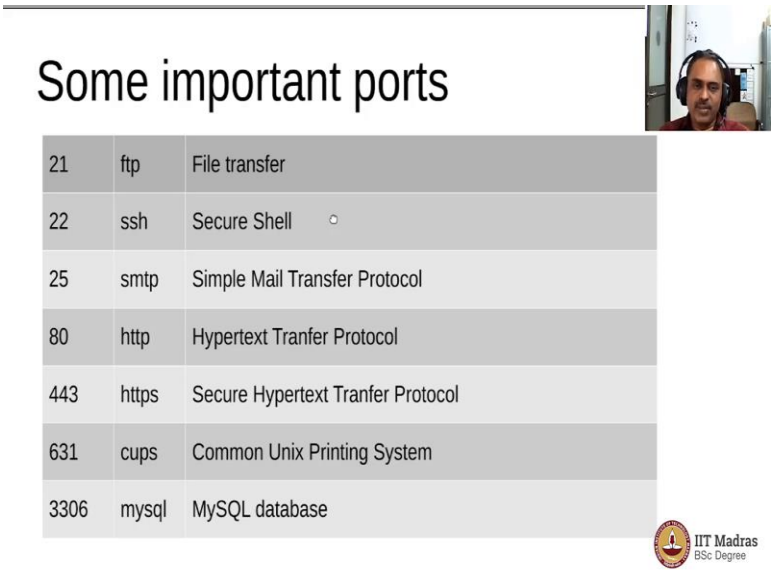
Another way of connecting to a remote computer is by using what is called ssh tunnelling that is you can open a secure shell connection by going through multiple hops, and also perhaps change in the port number along the way. So, that for security reasons, you can actually connect from your machine all the way to a machine in the campus through machines that allow for this kind of tunnelling to happen.

And you can also have a remote desktop access that is GUI access also is possible using tools like x2go to go or remote desktop protocol, which is very popular among the windows machine, or pcoip which is also possible a possible option. If you are using let us say VMware tools. And you can also have ability to access a remote desktop as a part of the browser window.

And there is a free software called Apache Guacamole which is useful for you to configure that if somebody sets it up for you. It means that life is very simple, because you just need to open the browser window and then the browser itself shows you the desktop environment that you can work with. Sometimes it is needed because you may want to plot and look at the plots on a computer which is remotely located.

And there are also commercial tools, which would help you see the remote desktop via internet, maybe not very safe, but they are available and very easy. A free versions are also available. So, like TeamViewer, AnyDesk and Zoho assist et cetera. So, these actually help you access a remote computer which is deeply located within a private network and by learning one of these techniques, you can actually start using facilities that are available in a remote location and work for a good productivity right form home.

(Refer Slide Time: 09:35)



Now, some of the ports that I mentioned earlier, and their mapping with respective services are listed here. So, these port numbers are standard port numbers. So, most of the computers will have those services on those respective ports. A exception would be like ssh, which may open not only on port 22, but maybe also on port some other number meant for a public network so that there is a security by which you slow down essentially somebody who is trying to check which port number you are listening to et cetera.

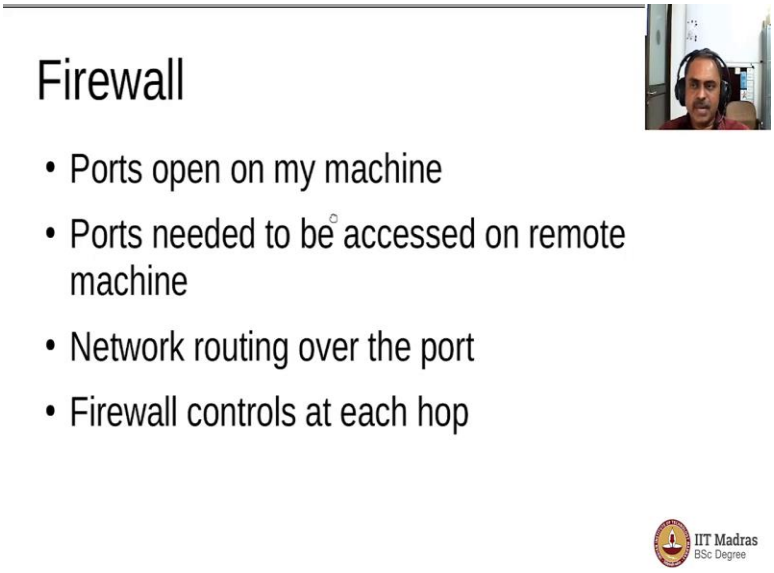
21 is the port number for ftp file transfer, 25 is a port number for unencrypted mail transfer. So when you are sending an email, so what you are doing is you are opening a network connection with the remote computer over port 25 and then sending the data. And that is how the mail is actually sent between machines.

Port 80 is the HTTP unsecured web server access basically website access without any security settings and 443 is when you have the security certificate present. So, most of the time, HTTPS

connections are what we use today. So, the port number or which this service is provided is 443. Now, every Linux machine allows for printing from any service via the network connection over the port number 631.

So, if you open localhost colon 631 in a Linux computer, you can see what are the printers that are connected, what are the jobs that are being executed right now for the printing purpose and so on. So, you can do a lot of configurations for printing by simply accessing a website, which is localhost colon 631. And if you have configured a database like MySQL for remote connectivity, the port number is typically 3306. So, like this, many software will have a standard port number over which the service is made available.

(Refer Slide Time: 11:34)



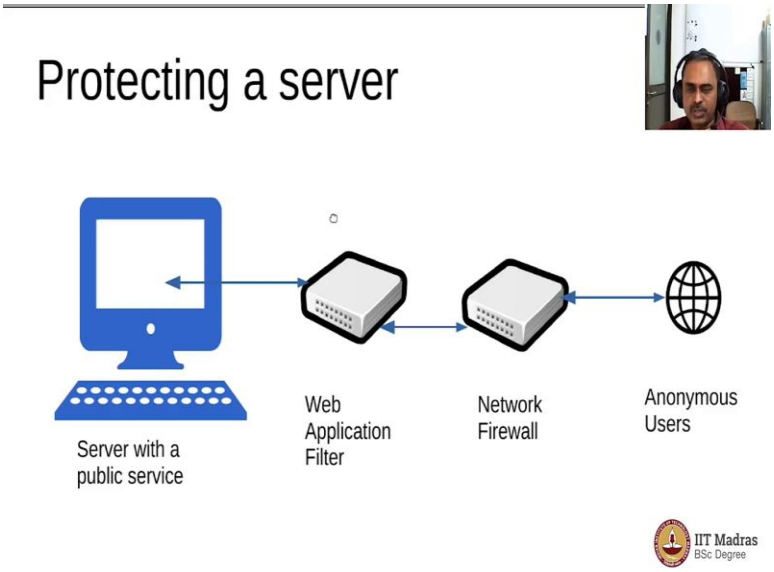
Now, there is the concept of firewall that we must be aware of, because we must know that some software is not opening up ports on my machine without my knowledge and they may actually open up security issues for me. How do I prevent such things to happen is by setting up a firewall to prevent the connections, except on those ports, on which I am actually explicitly giving permission.

So, that is something that we can configure quite easily on a Linux machine. We also need to check the firewall settings when we are trying to access a service on a remote machine because our service may not be able to go through if there is a firewall on the way, which does not allow connections over that particular port number.

And usually, the network switches can be configured to either allow or deny communications over a specific port number. So, if things do not work, we have to also know up to what point we are able to communicate over the port number and beyond what point there is a problem therefore, we can help the computer centre to debug the problem for us.

And at every hop between the computers, there is a way by which firewall controls can be set up in place. So, one has to be aware of these possibilities so that one can learn more about them to secure their own machine, as well as to maintain a server if they are responsible for a server for a service that they are providing over internet.

(Refer Slide Time: 13:13)

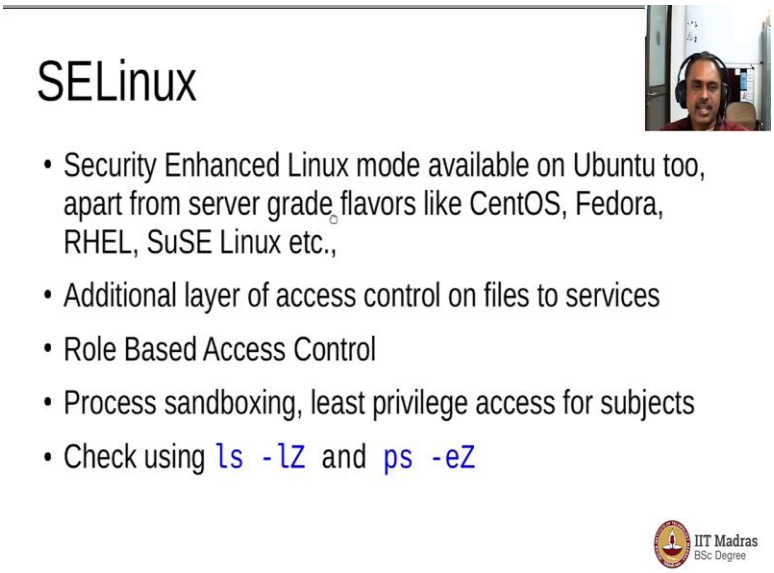


Now, how do we protect a server when we are providing a service over internet? So, there are anonymous users coming from all over the world. And if we are not careful, they may inject viruses within the service request that they are making to the web browser through their web browser to our service and thereby take control of our machine.

So, one way by which we can protect is by setting up a network firewall, which would ensure that the connections are coming from legitimate sources and on legitimate port numbers and so on and also at a particular speed that we would like to control. And then we also have a possibility of what is called web application filter, which is a another form of a network firewall, but specifically for a particular server.

So, for example, for HTTPS, it would actually look at the HTTP request, and analyse various fields that are being sent to the web server and see if any of them contain malicious code, such as SQL injection, attack et cetera. So, by having these two layers of protection, the server is slightly better placed in offering the services without too much of a problem from anonymous users who may be attempting to take control of the server.

(Refer Slide Time: 14:38)



An extreme way of securing it is actually to enable what is called security enhanced Linux mode. Earlier it was only available for CentOS, Fedora, RedHat Linux or SUSE Linux et cetera which are the server grade and Ubuntu being a desktop operating system and user friendly et cetera. Did not have it in the past, but of let we have it as part of the Ubuntu operating system also. And what it does is just like a sentry at the entrance of a gate, it would have, it would provide an additional layer of access control on files to services.

So, if there is any web server that is supposed to access files and provide them over internet, so SELinux would provide one more layer of security by limiting what parts of the file system can be read by the web server, and what files are visible to it or not. So, this is a layer beyond the file system permissions that we are familiar already.

And SELinux offers what is called role-based access control. So, different services different users can have different levels of access to different directories. And thereby, we can actually

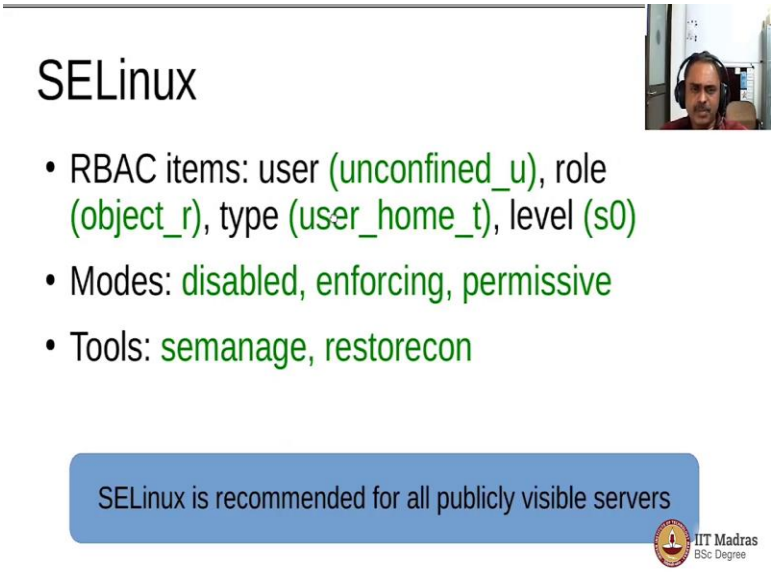
protect the operating system from being taken over by malicious intent from a remote location through the services that we are offering.

And SELinux also provides what is called sandboxing for every process that means every process will have a restriction of reading information about the processes or memory locations or files that are belonging to other processes. And by default, it will operate in the least privileged access mode for all the subjects which means that by default, the doors are closed.

So, that is a mode in which SELinux work. So, that is one of the reasons why people do not enable it because slightly painful once you enable it to do some routine work, but it is going to be a little bit more secure way of going (())(16:38). Now, how do you know whether SELinux was enabled in your machine or not?

So, instead of ls minus l, you can add one more option capital Z and see if there is something more that is actually appearing on the screen. And if it is, then that means that perhaps SELinux was enabled, same thing for the processes, if you add the capital Z option for ps command, then you can also see whether such a mod has been enabled.

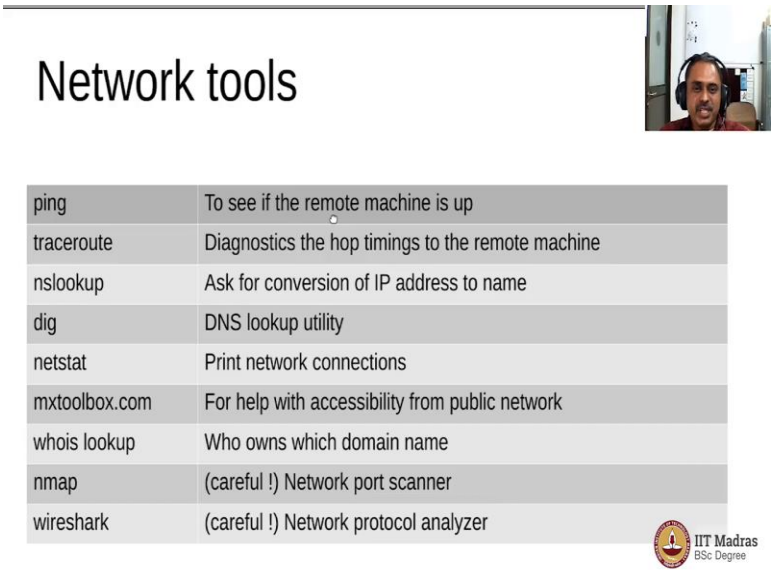
(Refer Slide Time: 17:04)



There are 4 types of items that are coming under the (())(17:08) of RBAC role based access control system. So, the users the roles, the types, and the level of security can be controlled quite elaborately. So, in the brackets, I have given some example of such types of entities. And there are many modes in which secure, Linux can be configured.

So, you can have it disabled mode by default, but you can enforce it or you can even keep it in a permissive mode, where it would actually do all the checks, but only log them, but let you actually proceed further. So, that is useful when you want to configure it before going live and there are tools like semanage and restorecon, which help you in managing the permissions of directories and services once the SELinux has been enabled. So, if you have any publicly visible server, it is a very good idea to enable SELinux.

(Refer Slide Time: 18:06)



Now, there are some tools that are useful in network to understand how the communications happen, so that you can debug any given problem situation. So, things like ping. So, if you want to know whether a machine is up, you can actually try to ping it using the IP address and if there is a response, it means the machine is up.

If there is no response, it does not mean the machine is down. The reason is that one can configure a machine to not respond to ping requests for security purposes. So, only the positive thing has to be interpreted correctly. That is if the ping is responded to, it means a machine is up. That is all.

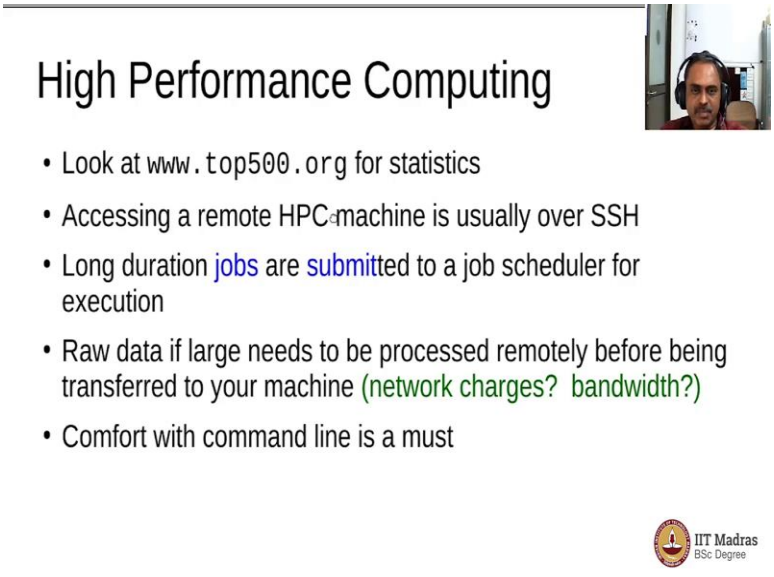
And you can also look at what is the route taken by the network packets to a remote machine by using the trace route. And you can convert the names of the machines to IP addresses by using nslookup or dig utility. And you can check what are all the network activities that are happening on your machine by using netstat.

And if you want to know if the machine that you are working on is having a public access. So, then you need actually a different machine in the internet to look at your machine. So, for that is a website called mxtoolbox dot com, it is helps you to do some debugging. And if you encounter a machine name, and you want to know whether it is a genuine machine or not, you can actually find out who registered the name for that machine.

And if the name and address of that particular person who has registered that machine appear to be reasonable, then maybe that the name of the machine is perhaps genuine. But there are a lot of fake DNS entries out there. So, one has to be careful. Now, if you are in a campus and you want to look at what are all the ports that are open around your computer in the network, you can run the to utility called nmap.

But you should not do it without permission of the network administrator because it can cause a lot of network traffic. And there is even more dangerous tool called wireshark, where you can sniff packets through the network to do some diagnostics of the network protocol. It is again meant for usage by the network administrator, a regular user is not supposed to do nmap and wireshark without permission.

(Refer Slide Time: 20:24)



Now, we will actually go and look at the website, top500 dot org to look at statistics and it will be interesting to note that every single machine in the top500 HPC facilities in the world are

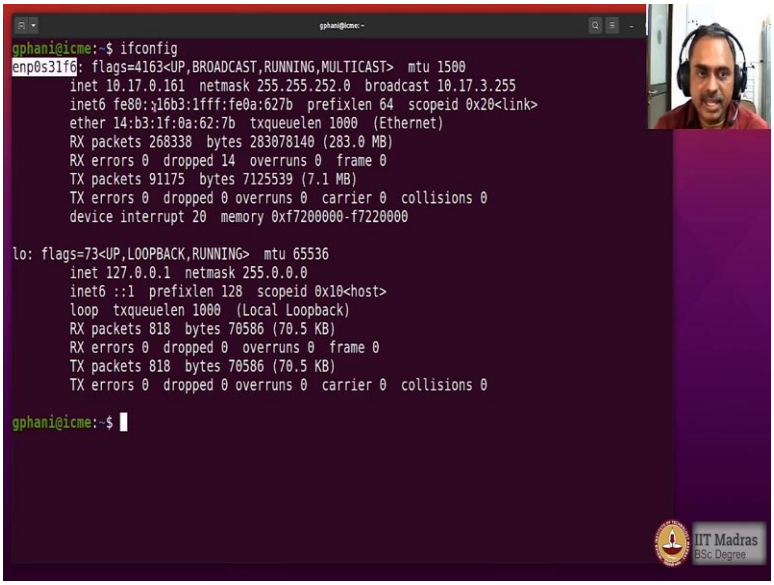
actually Linux based, which means that if you are good at Linux, then you are able to access remotely located high performance computing machines quite comfortably.

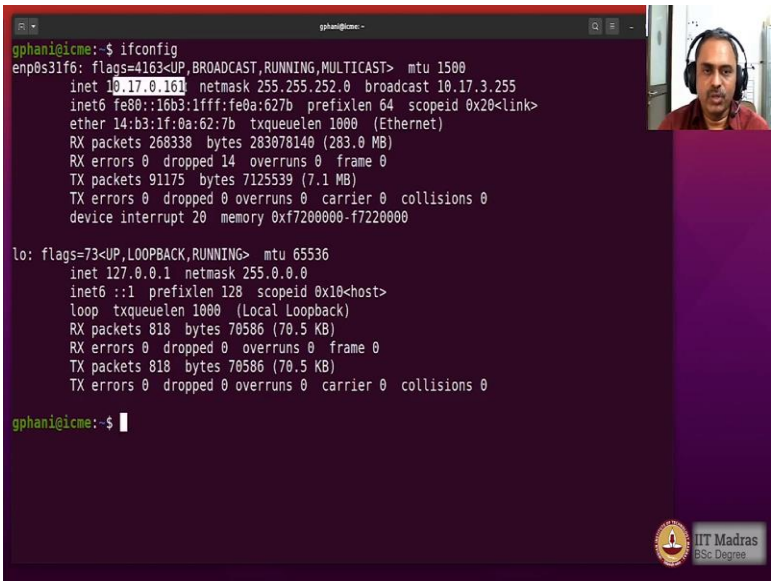
And one cannot run the tasks on a HPC machine directly, you need to submit a job which will be sent to a job scheduler and it will be executed whenever it is time comes in a sequential manner as per the policies. So, therefore one has to learn how to run heavy tasks on a remote computer. And knowing Linux very well will help a lot.

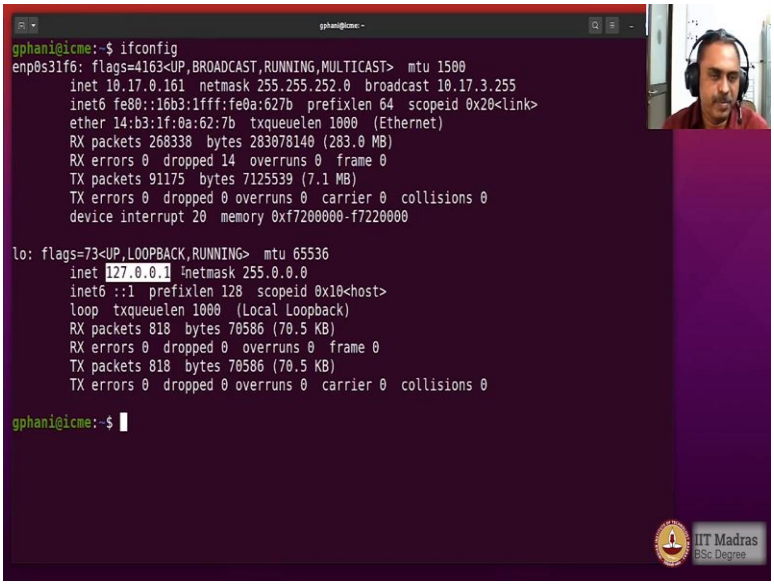
And very often you cannot bring the whole data out to your laptop because the internet costs will be there for such transfers. And also, you may have too much of data that the bandwidth may not be sufficient. So, it is very useful if you know Linux and the command line environment, then you can actually do ssh to a high-performance computer and process the data remotely and bring only the process to data out. So, that you can save both the network charges as well as bandwidth.

So, being comfortable with the command line is almost a must. If you are into high performance computing I hope that will be acting like a motivation for you that whatever you have learned till now in the course will be quite useful in case you are going to high permanence computing, which enables machine learning and things like that. So, let us go to the demo now.

(Refer Slide Time: 22:07)

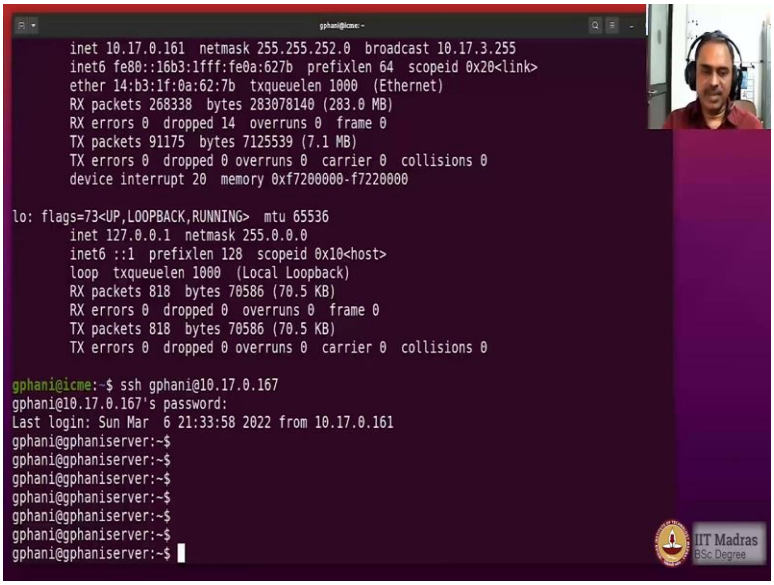






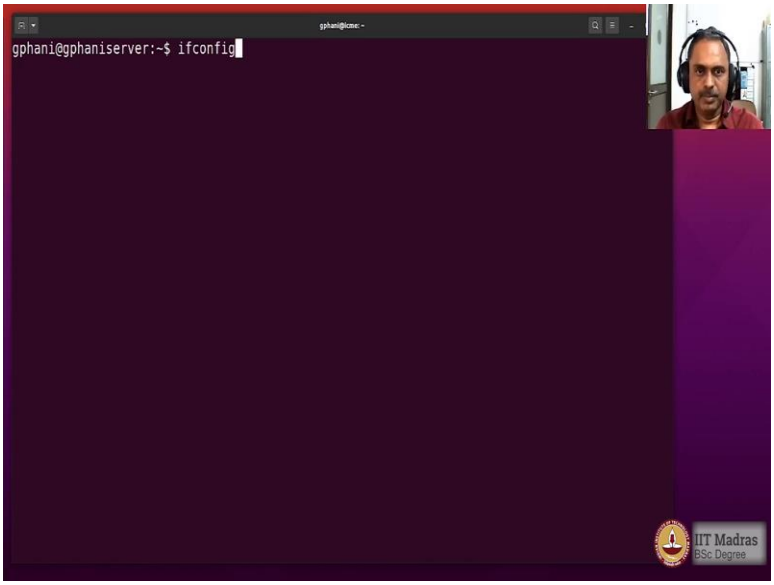
So, ifconfig is a utility that lets me know, what are the addresses that I have and here we have the LAN connection, which is giving me an IP address of 10 series which means it is a class A network which is in the campus and loopback device, local loop devices also here which is having an IP address of 127 dot 0 dot 0 dot 1 which will be there were every machine. To contrast this, I will actually log into my desktop computer and show you.

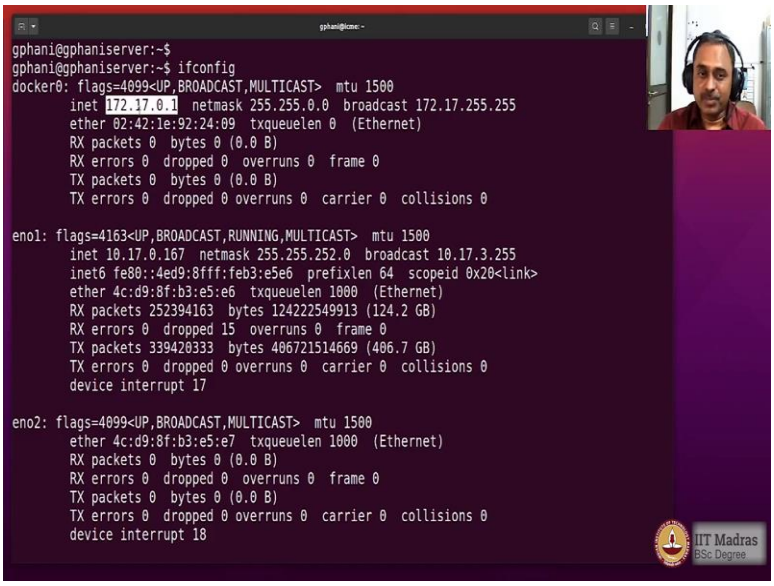
(Refer Slide Time: 22:40)

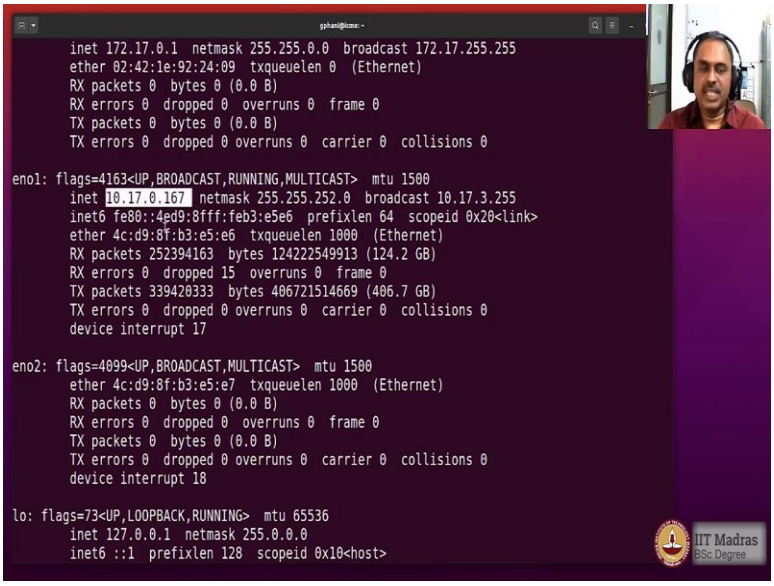


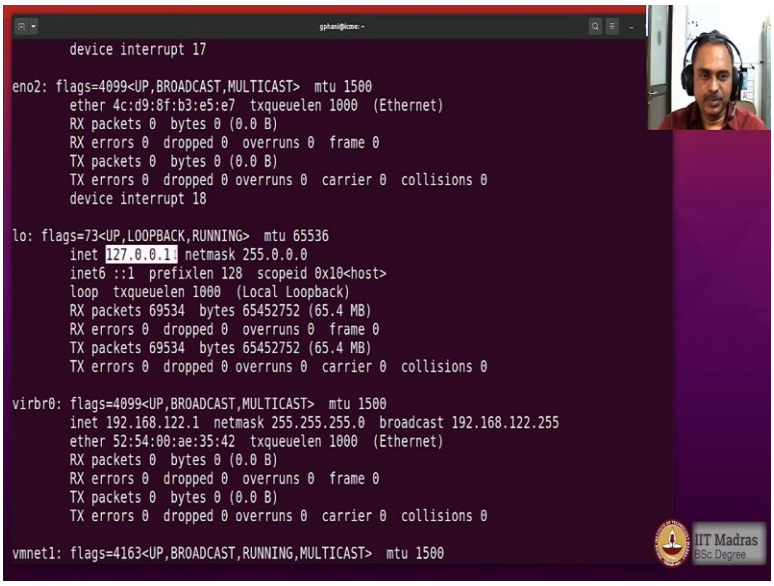
So, I am doing the remote connection through ssh. So, you can see that the hostname is now gphaniserver and the machine on which I was recording is ICME. So, you can see that from here within the terminal environment, we are able to ssh into a different machine and we are able to use that machine without shifting on the place. That is because the secure shell is allowing us to do this particular command line way of using the remote machines.

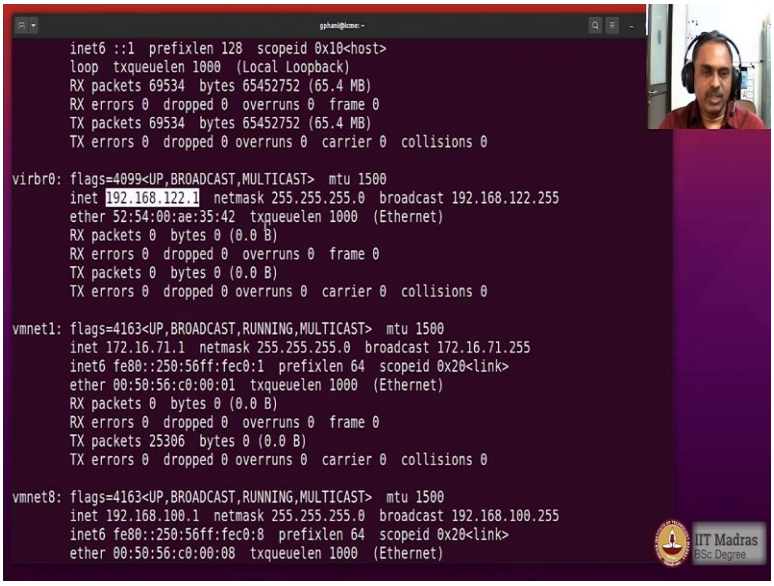
(Refer Slide Time: 23:12)

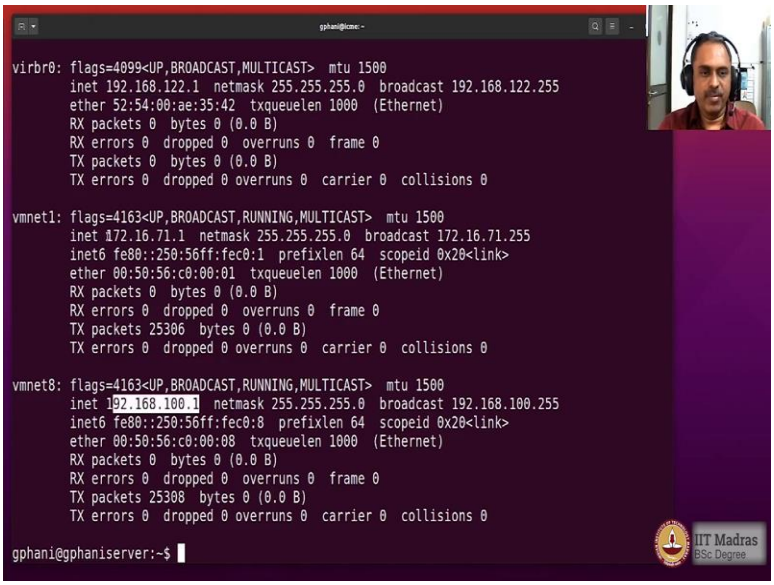


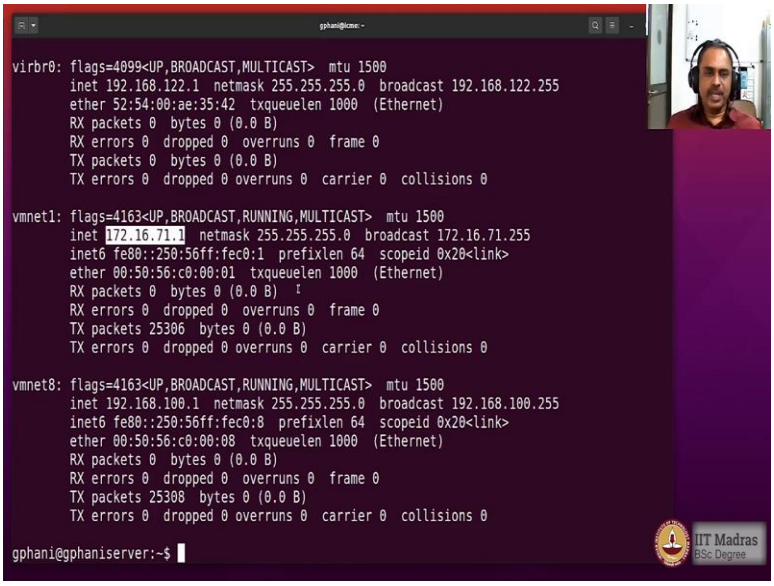

gphani@gphaniserver:~$
gphani@gphaniserver:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:1e:92:24:09 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.17.0.167 netmask 255.255.252.0 broadcast 10.17.3.255
inet6 fe80::4ed9:8fff:feb3:e5e6 prefixlen 64 scopeid 0x20<link>
ether 4c:d9:8f:b3:e5:e6 txqueuelen 1000 (Ethernet)
RX packets 252394163 bytes 124222549913 (124.2 GB)
RX errors 0 dropped 15 overruns 0 frame 0
TX packets 339420333 bytes 406721514669 (406.7 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 17
eno2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 4c:d9:8f:b3:e5:e7 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 18
IIT Madras
BSc Degree


inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:1e:92:24:09 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.17.0.167 netmask 255.255.252.0 broadcast 10.17.3.255
inet6 fe80::4ed9:8fff:feb3:e5e6 prefixlen 64 scopeid 0x20<link>
ether 4c:d9:8f:b3:e5:e6 txqueuelen 1000 (Ethernet)
RX packets 252394163 bytes 124222549913 (124.2 GB)
RX errors 0 dropped 15 overruns 0 frame 0
TX packets 339420333 bytes 406721514669 (406.7 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 17
eno2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 4c:d9:8f:b3:e5:e7 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 18
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
IIT Madras
BSc Degree


gphani@icme: ~
device interrupt 17
eno2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 4c:d9:8f:b3:e5:e7 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 18
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 69534 bytes 65452752 (65.4 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 69534 bytes 65452752 (65.4 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
ether 52:54:00:ae:35:42 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vmnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
IIT Madras
BSc Degree


gphani@icme: ~
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 69534 bytes 65452752 (65.4 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 69534 bytes 65452752 (65.4 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
ether 52:54:00:ae:35:42 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vmnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.71.1 netmask 255.255.255.0 broadcast 172.16.71.255
inet6 fe80::250:56ff:fec0:1 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:c0:00:01 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 25306 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.100.1 netmask 255.255.255.0 broadcast 192.168.100.255
inet6 fe80::250:56ff:fec0:8 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:c0:00:08 txqueuelen 1000 (Ethernet)
IIT Madras
BSc Degree

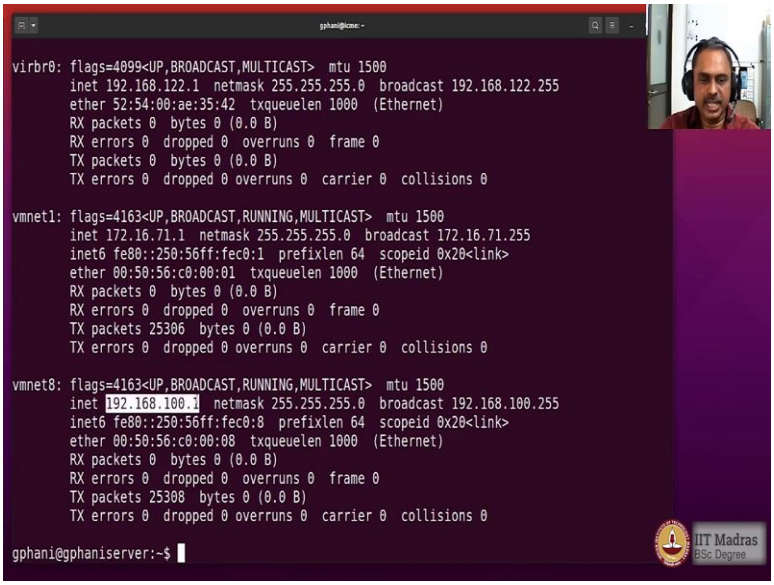


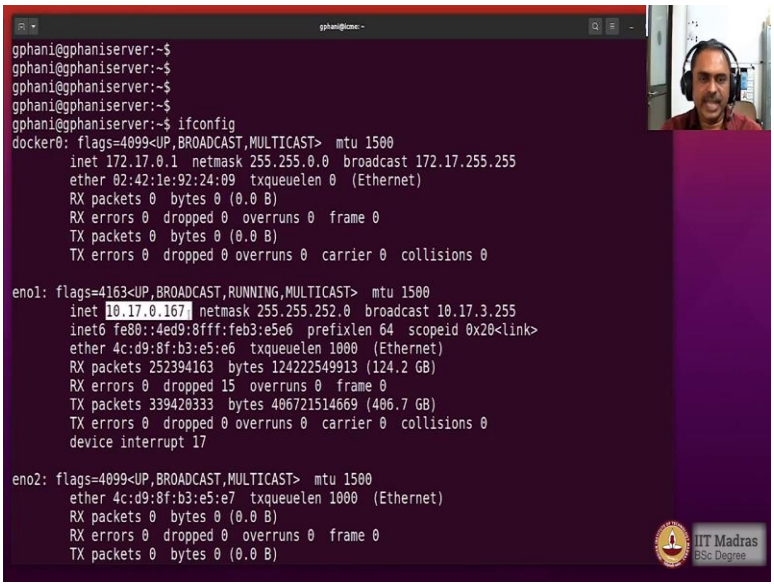


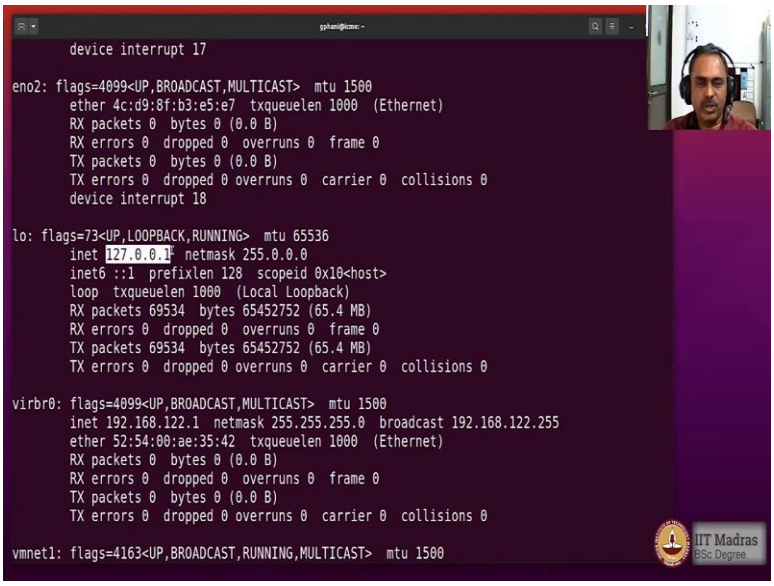
And if you look at the ifconfig for the other machine that I have logged into, you see that it has a way more number of devices. So, it has a internet IP of class B and then it has also class A address coming from the LAN and then it has a loopback address of 127 dot 0 dot 0 dot 1 and then it also has a class C type of a address also. And two of them the class B second one.

So, why does it have so many IP addresses? That is because in my server, I have got a bunch of virtual machines and containers that are running. And they will communicate with each other using a separate network. And I also have a private network set up in my own office using a small dealing adapter that I bought from Amazon.

(Refer Slide Time: 24:14)

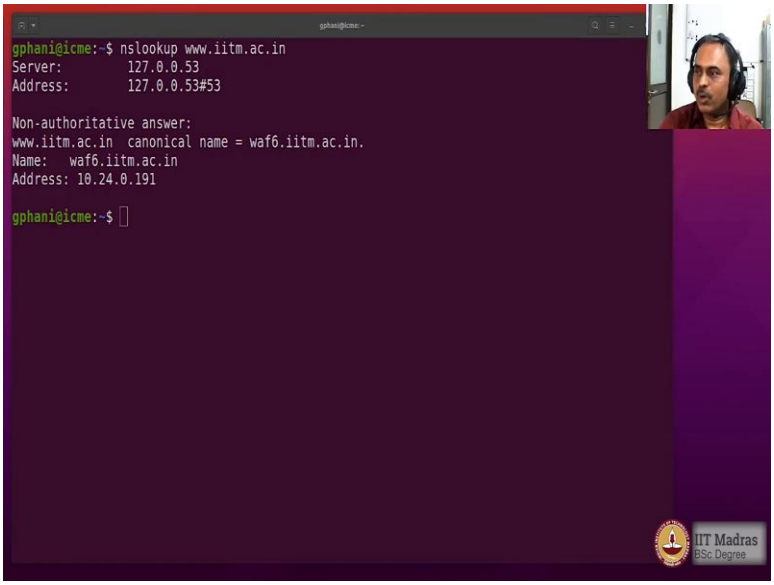






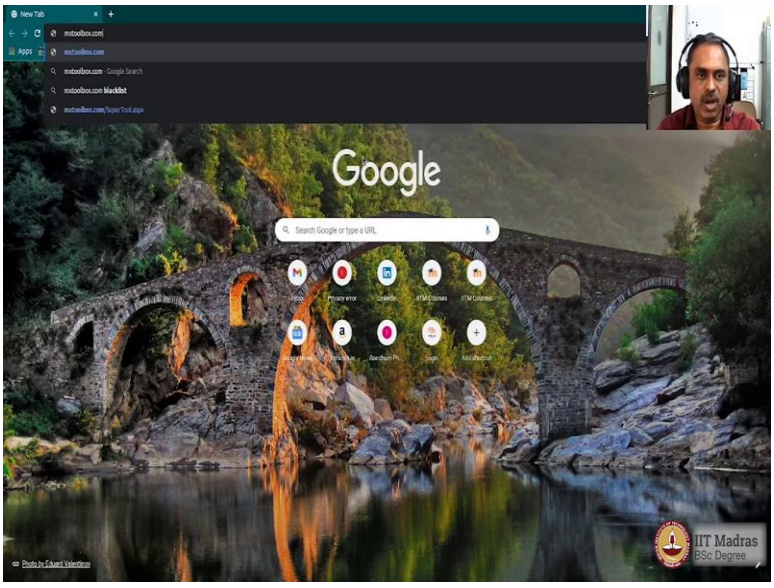
So, I have this network also configured for communication within the room which is totally cut off from the campus LAN. The campus LAN is communicating with the IP address range of 10. something. So, you can see that all these addresses will be different for different machines. So, there will be a 10 series address a 172 series address there is a 198 series address. And then there is one address which is common for every machine that is 127 dot 0 dot 0 dot 1 it is basically saying me. So, everybody knows who is me, themselves. So, that kind of address is available always.

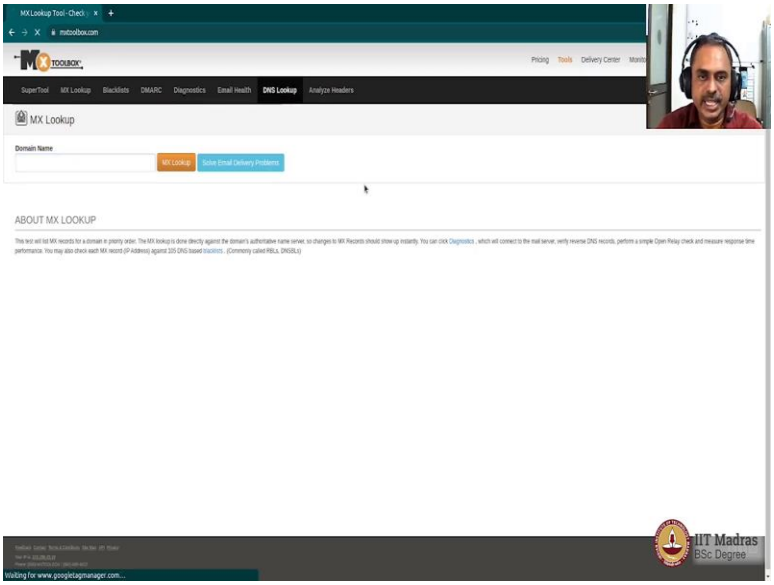
(Refer Slide Time: 24:59)

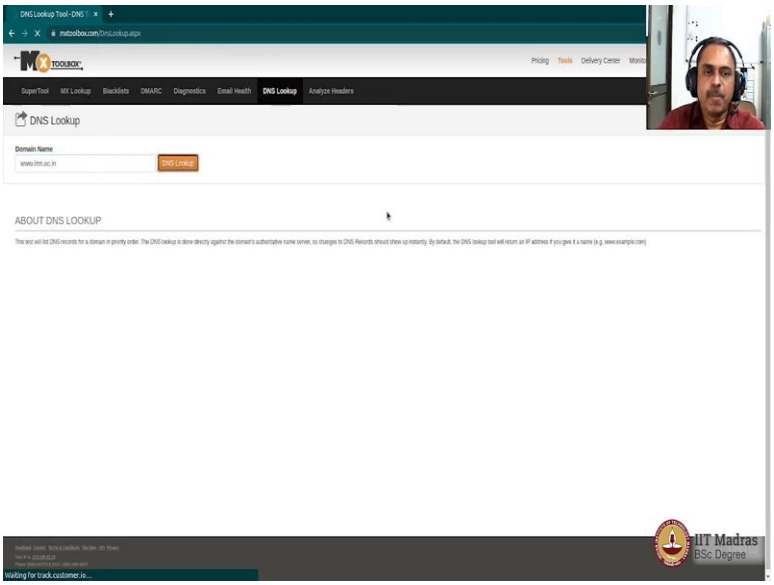


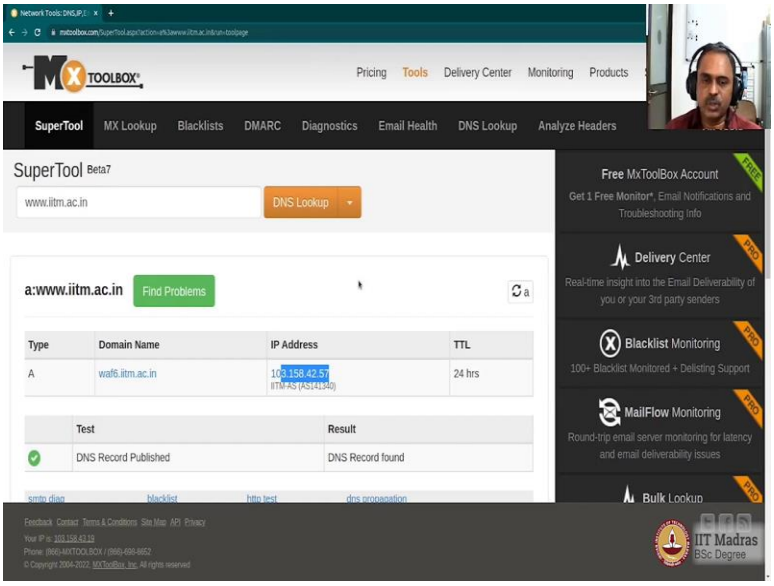
One way by which you can use network tools on the command line, or to convert names to IP addresses is to check nslookup on some machine name. So, iitm dot ac dot in is one machine name that I want to check this is a web server of our institute. So, you see that it is connected to a web application filter, and it has an IP address of 10 dot 24 dot 0 dot 191 which means that it is a internet IP. Now, because I am trying it from campus, it is an internet IP. However, if I try the same thing from the website, mxtoolbox, the IP address will be different. So, let us check that out.

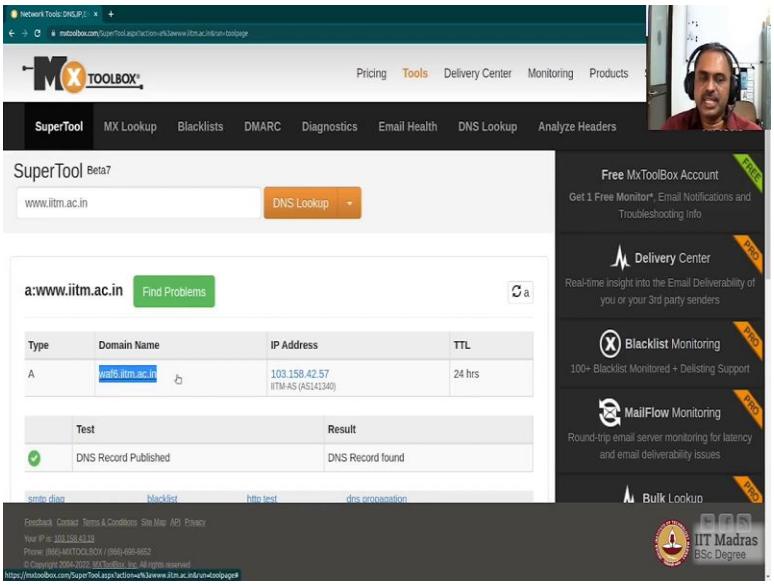
(Refer Slide Time: 25:32)

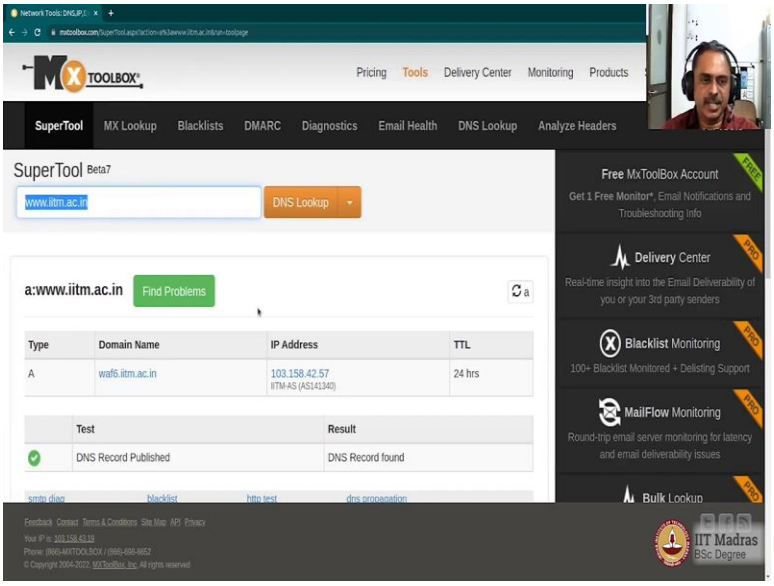





DNS Lookup Tool - DNS
mxtoolbox.com/DnsLookup.aspx
Pricing
Tools
Delivery Center
SuperTool
MX Lookup
Blacklists
DMARC
Diagnostics
Email Health
DNS Lookup
Analyze Headers
DNS Lookup
Domain Name
www.iitm.ac.in
DNS Lookup
ABOUT DNS LOOKUP
Waiting for track.customer.io...
IIT Madras
BSc Degree

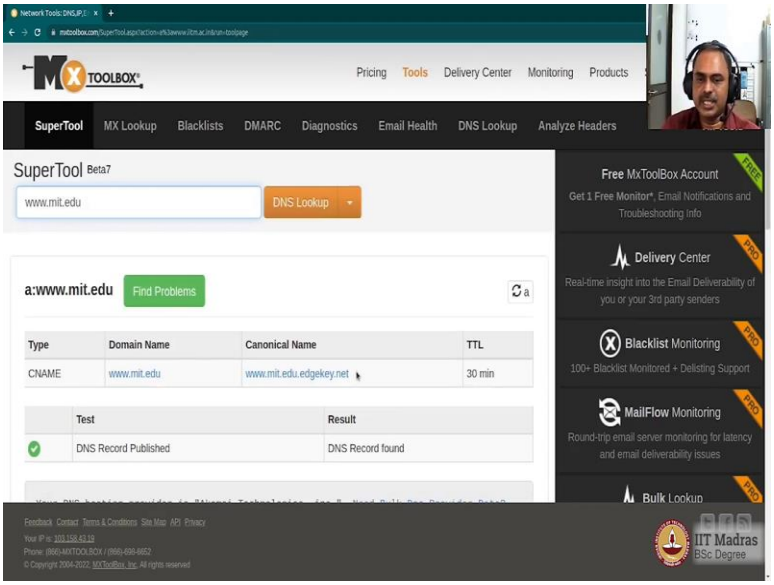

Network Tools: DNS,IP,E...
mxtoolbox.com/SuperTool.aspx?action=a%3awww.iitm.ac.in&run=toolpage
TOOLBOX
Pricing
Tools
Delivery Center
Monitoring
Products
SuperTool
MX Lookup
Blacklists
DMARC
Diagnostics
Email Health
DNS Lookup
Analyze Headers
SuperTool Beta7
www.iitm.ac.in
DNS Lookup
a:www.iitm.ac.in
Find Problems
Type
Domain Name
IP Address
TTL
A
waf6.iitm.ac.in
103.158.42.57
ITM-AS (AS41340)
24 hrs
Test
Result
DNS Record Published
DNS Record found
smtp diag
blacklist
http test
dns propagation
Free MxToolBox Account
Get 1 Free Monitor*, Email Notifications and Troubleshooting Info
Delivery Center
Real-time insight into the Email Deliverability of you or your 3rd party senders
Blacklist Monitoring
100+ Blacklist Monitored + Delisting Support
MailFlow Monitoring
Round-trip email server monitoring for latency and email deliverability issues
Bulk Lookup
Feedback Contact Terms & Conditions Site Map API Privacy
IIT Madras
BSc Degree

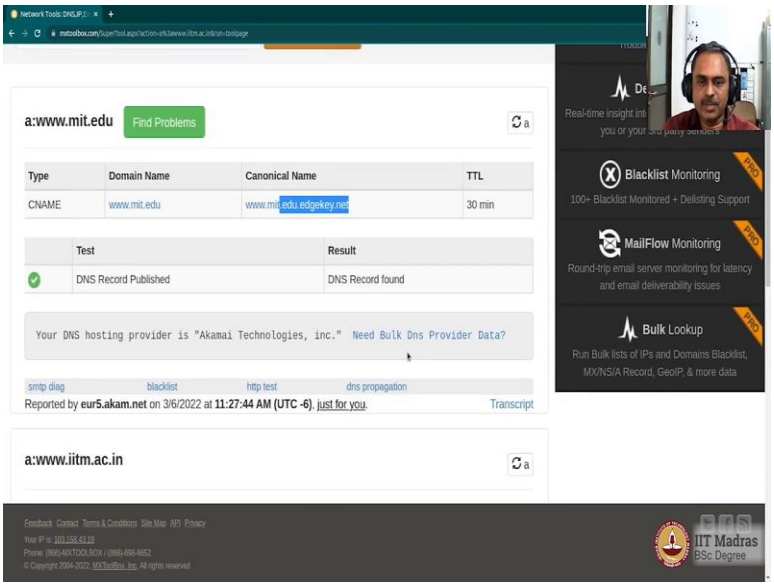


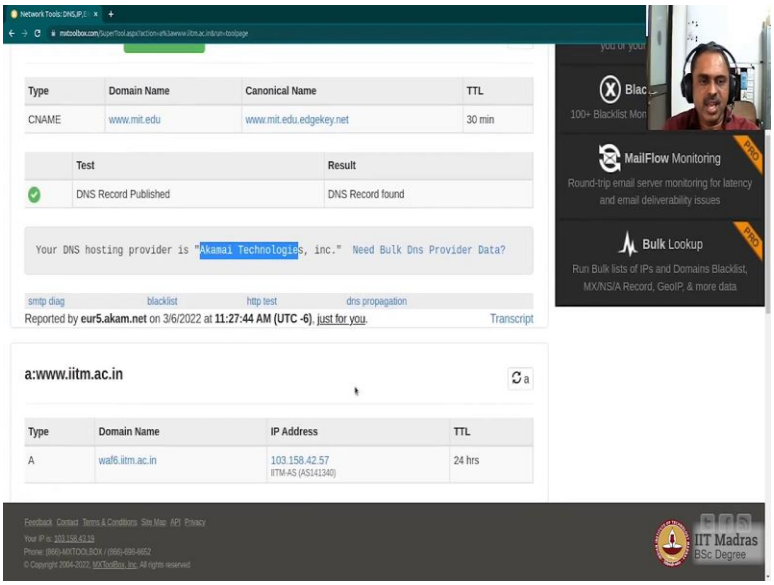


So, I am opening a browser and I go to mxtoolbox dot com. Here in this, I will go to the DNS lookup, and type www dot iitm dot ac dot in DNS lookup. So, this is coming from the public network. So, from the public network, as the rest of the world looks at our IP address happens to be 103 dot 158 dot 42 dot 57. So, that is an IP address coming from outside. So, now you see that this is a public IP address. And from the IP address, you can also see that it is also basically transparently tell him that we have a web application filter in place. And this is a name that is translating to another name, which means there are some aliases that are possible.

(Refer Slide Time: 26:31)

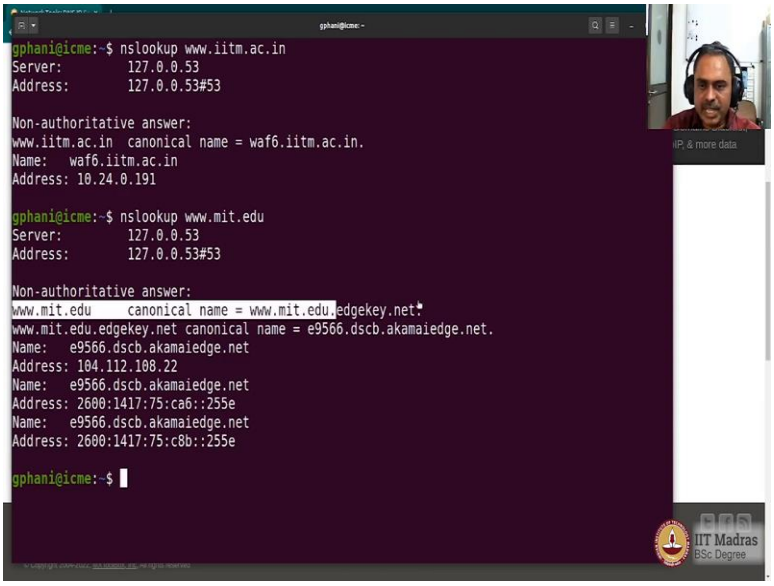






So, let us see for any other address, let us say for mit dot edu and you will see that it is having a DNS record pointing to a edgekey dot net a domain and Akamai technologies is maintaining that.

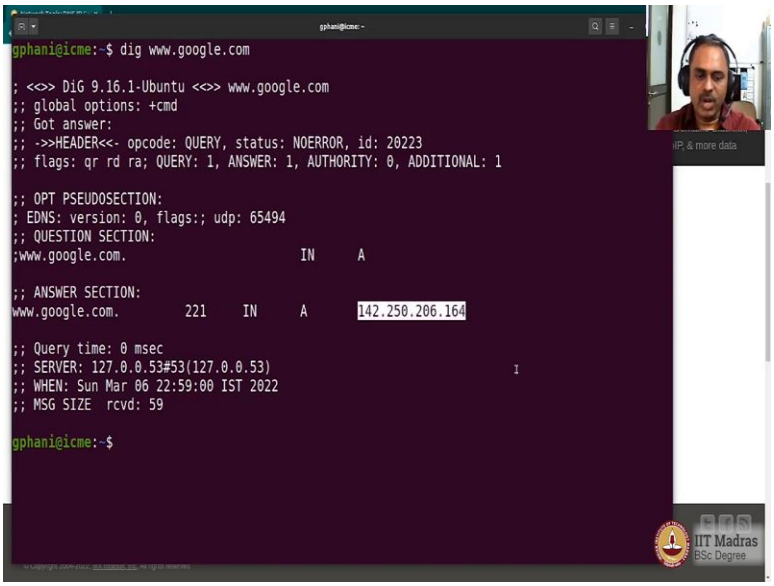
(Refer Slide Time: 26:50)



And what we can see here is the same kind of information will come out here also. And you see that edgekey dot net the domain name and Akamai is made maintaining that and of course, some addresses are also being (())(27:08). So, what this means is that mit dot edu website is actually maintained by a service provider, which is actually having multiple machines all over the globe, very fast dissemination of information across the globe.

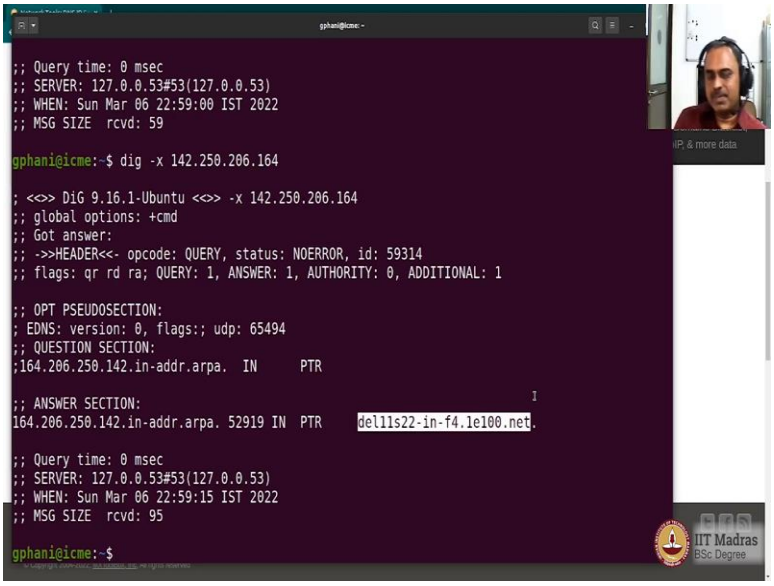
And that kind of a address is being resolved uniformly from outside the campus as well as on the inside the campus. The reason is that this is not our machine, so it is not located in our LAN. So therefore, we do not get to see what was the internet IP for that particular machine. Yes, it is a global IP that we will know.

(Refer Slide Time: 27:46)



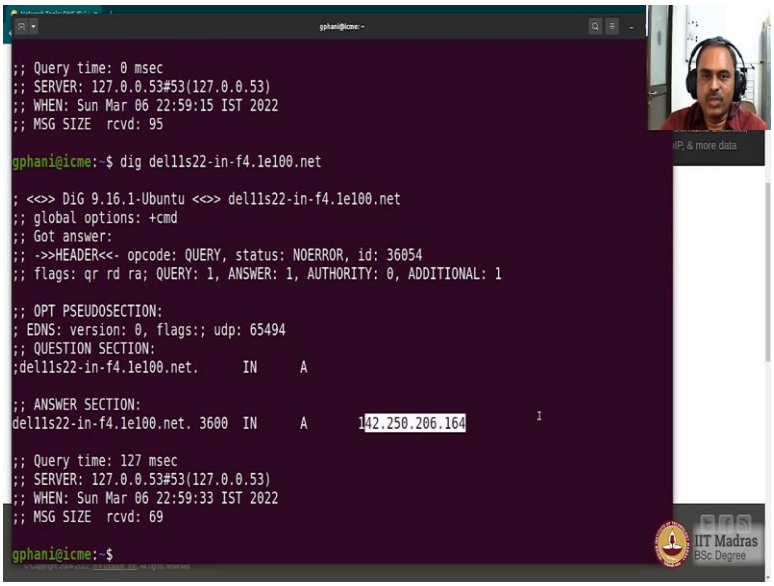
So, what we will do now is we can also look at a tool called dig, which does the same task. So, dig would actually go and get you the IP address of a particular machine and the IP address happens to be here this way.

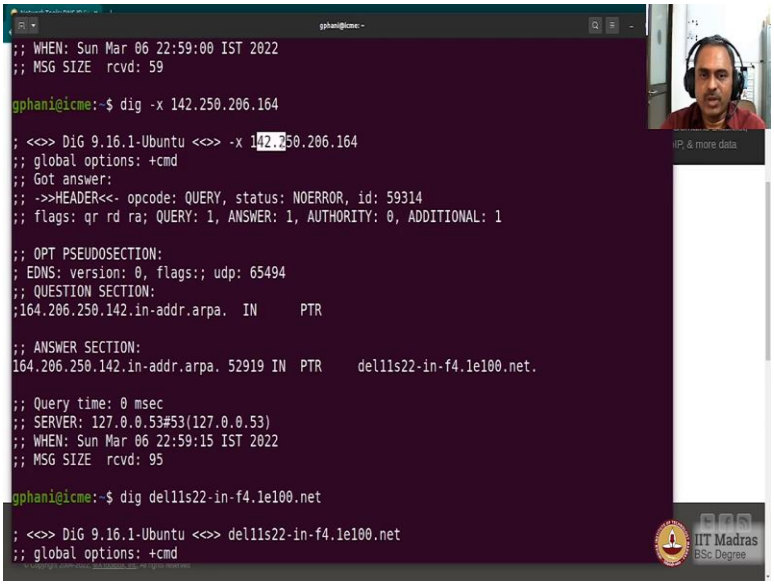
(Refer Slide Time: 28:00)

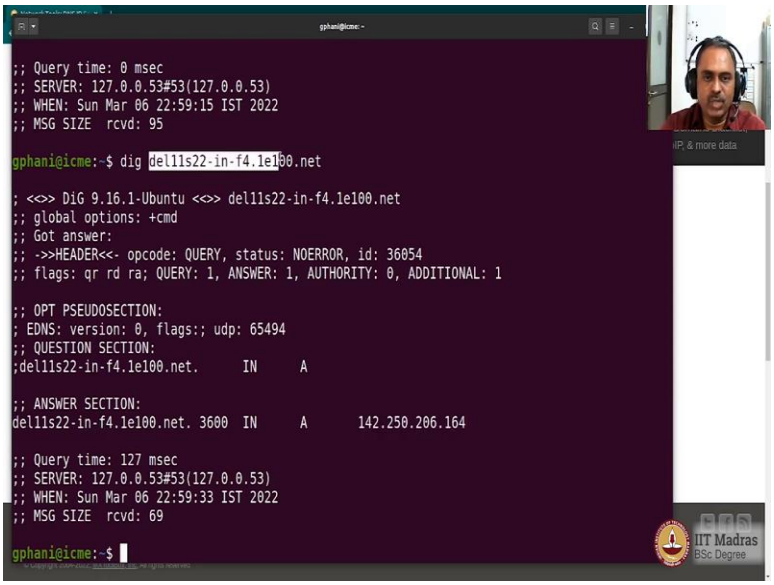


Now, what we do is that dig minus x, then it will do a reverse lookup. Now, you see that when it does a reverse lookup the name for the particular IP address is different. So, what this means is that very often the names that we are actually typing in a browser window may not be the canonical names, they could be basically aliases.

(Refer Slide Time: 28:21)

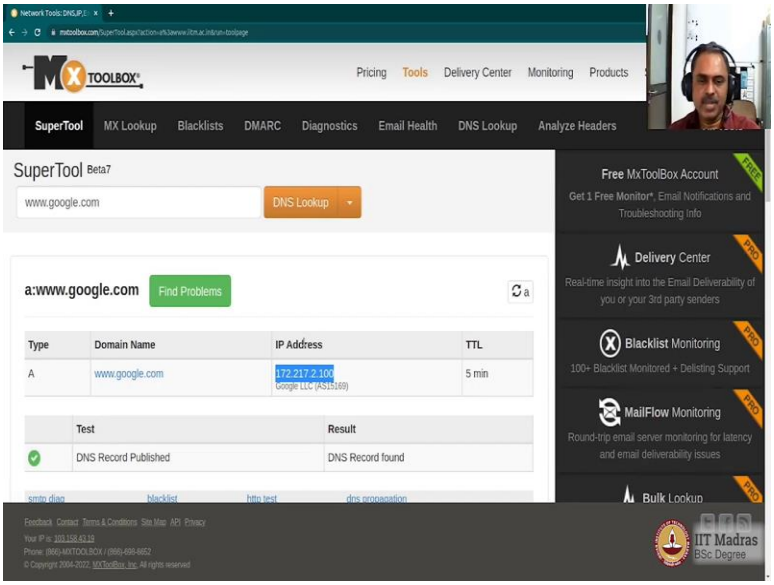


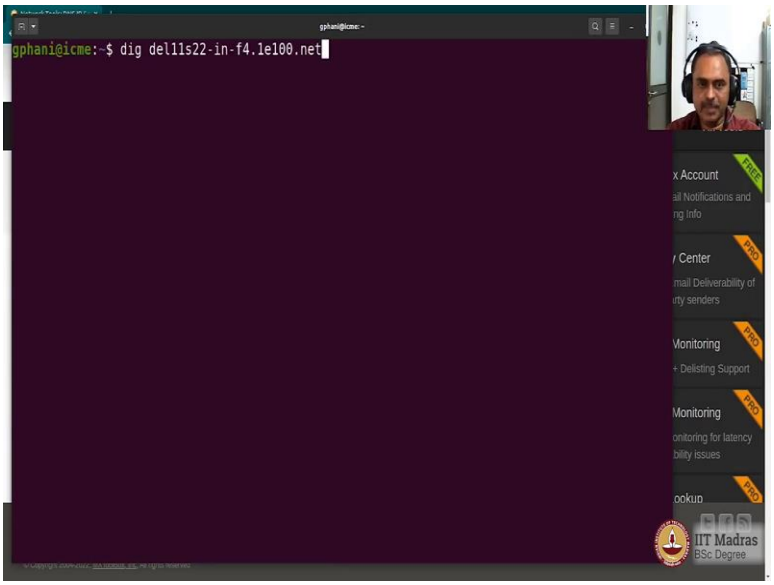




So, now let us look at the IP address of this machine. And sure enough, that will be matching with what we originally had here. Here you see 142 dot 250 dot 206 dot 164. So, it matches. So, which means that for this particular IP address, the machine name actually happens to be this one, but one of the aliases is basically google dot com. Now, this address will not be matching with what we see from browser.

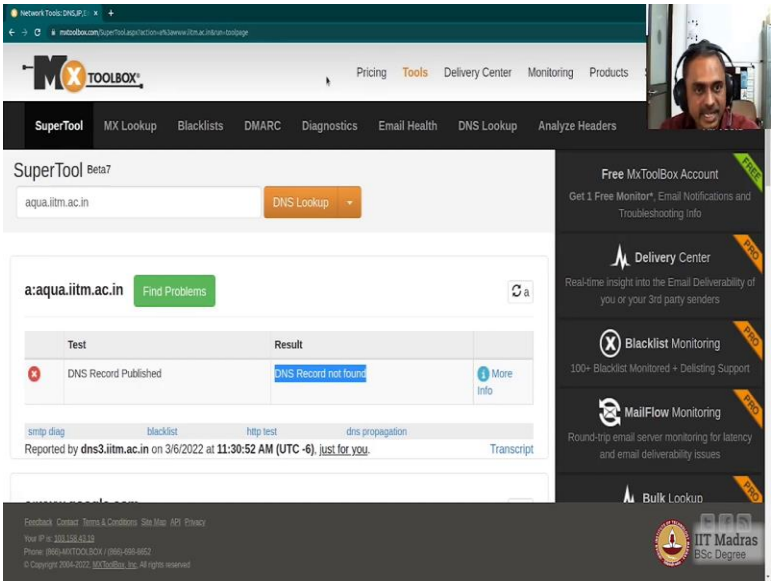
(Refer Slide Time: 28:49)





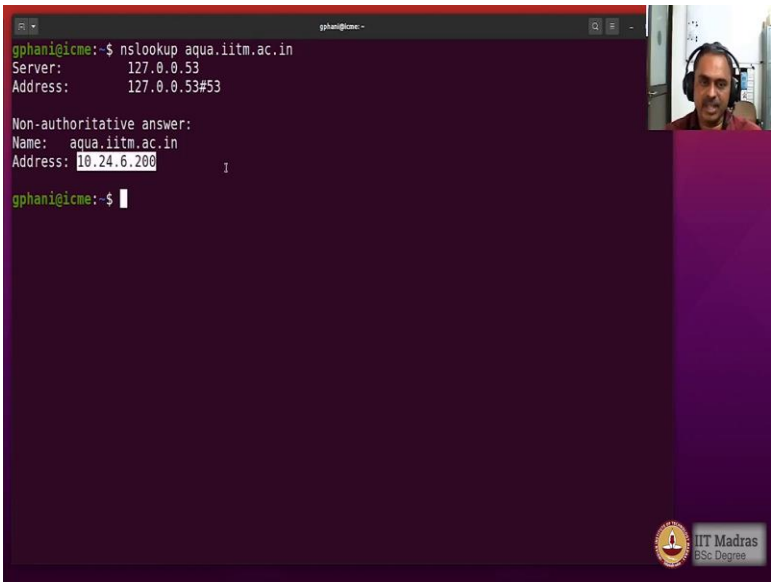
So, let us look at that. So, you see the IP address here is different. The reason is that google dot com is served by many many machine across the globe. And therefore, the mission IP that you would get when you look up is what is given by the nearest domain name server. So, my mxtoolbox is located perhaps somewhere in California and when we are running this particular command at the campus then we are looking at our campus DNS server. So, therefore, these are very different geographical locations. So, therefore, the IP addresses that we get for those hostnames will be also different.

(Refer Slide Time: 29:37)



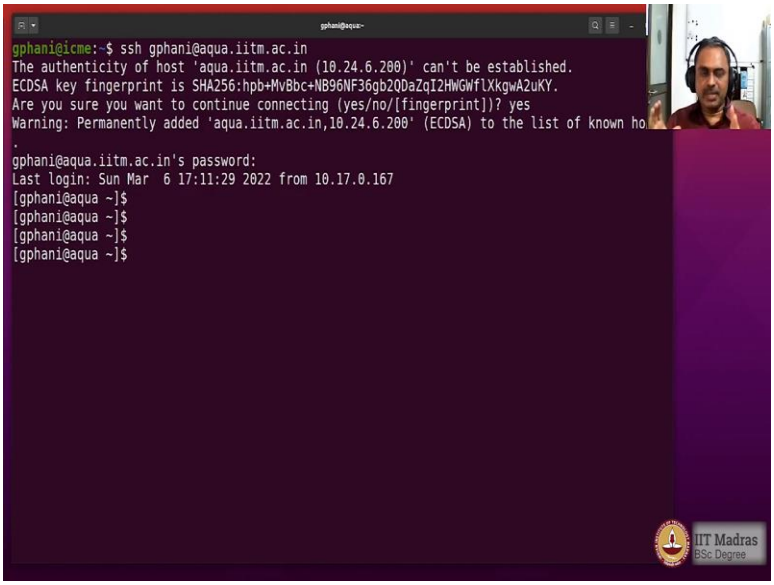
Now, let us see if there is a particular machine called aqua, I know is a machine from IIT Madras, does it have a IP address visible from the internet? So, you see that it is not found so which means that our HPC cluster called aqua is not visible from the globe. But it will have an IP address visible from the campus.

(Refer Slide Time: 29:56)



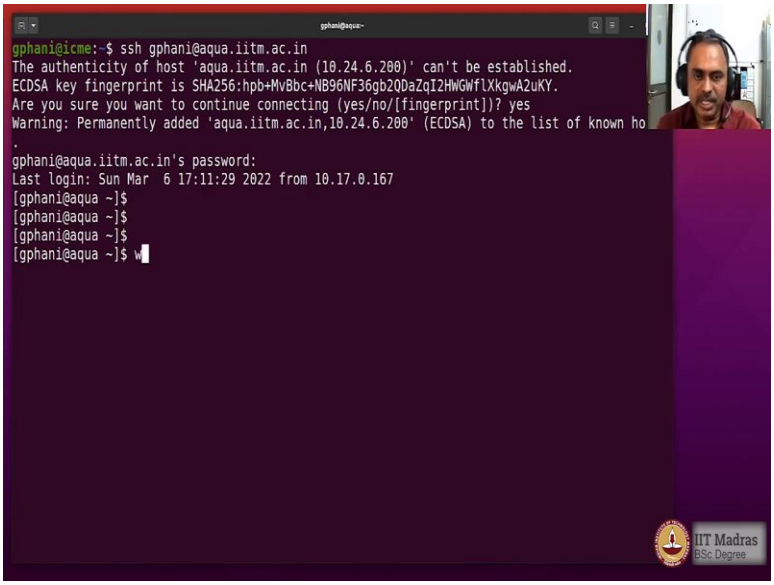
So, you can look at it now. So, it would have a local IP address, so you can see that it is a internet IP address, it will not have a global IP. So, it is only available from within the campus which means that if you need to have access to our petaflop supercomputer on campus, then you need to find ways of entering the campus because the machine is not available as a visible to outside the campus. So, which means that you must have a VPN access or you must use some other remote desktop options to come into the campus and then you can access the high-performance computer.

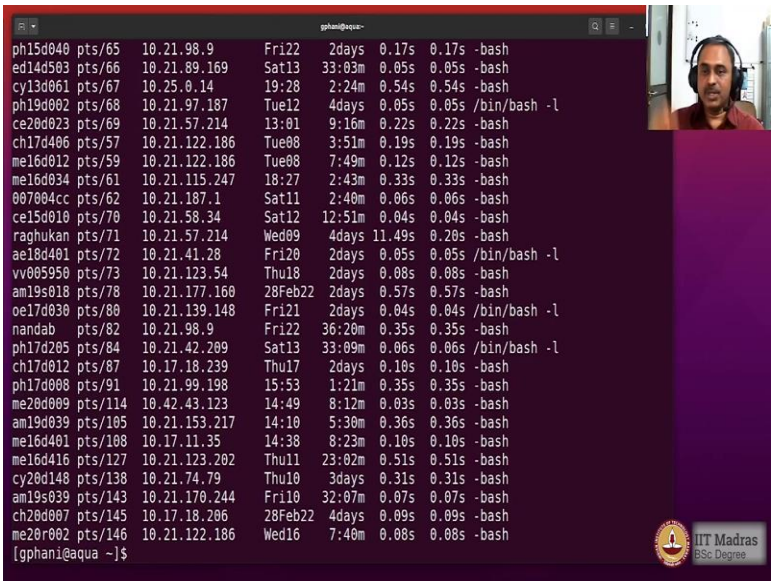
(Refer Slide Time: 30:41)

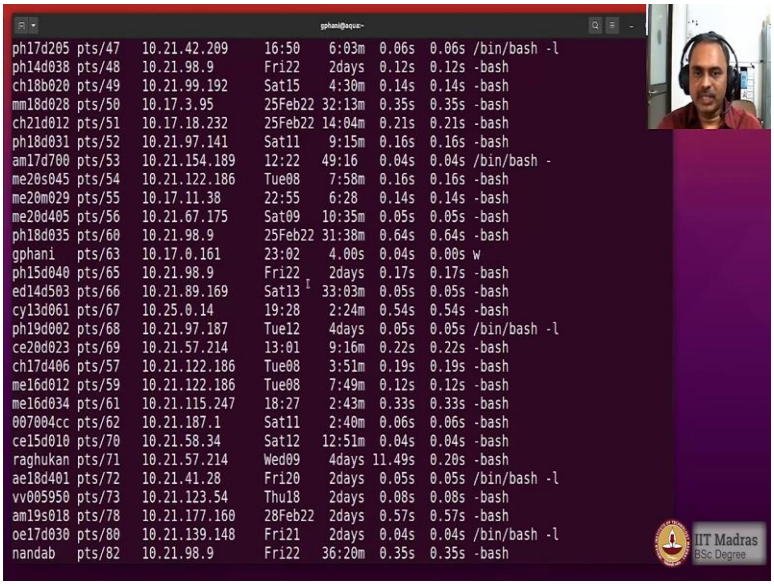


Now, let us look at how we can connect with a remote machine like this. So, we have got this machine so I can ssh into that machine and then I need to give a password. So, once I give me a password, then I am entering the now machine. So, you can see that within the terminal, we are able to log into a remote machine. So, in our case, we are logging into the supercomputer of our campus.

(Refer Slide Time: 31:08)

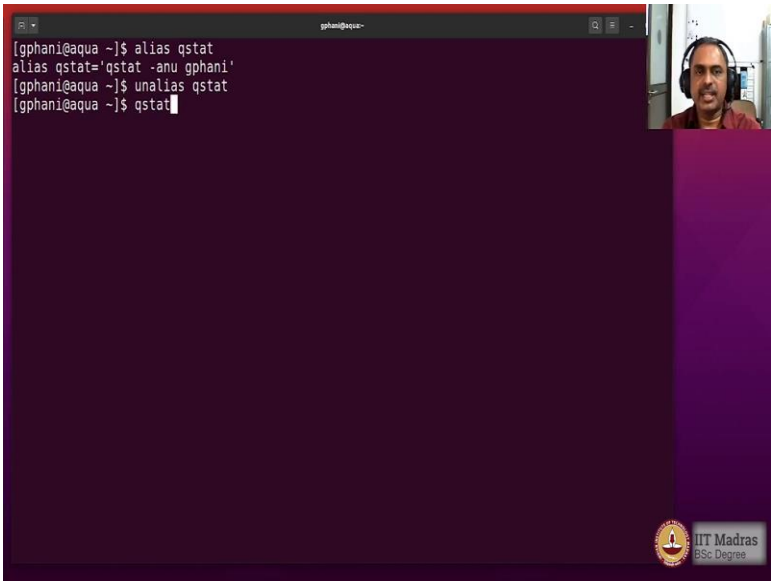


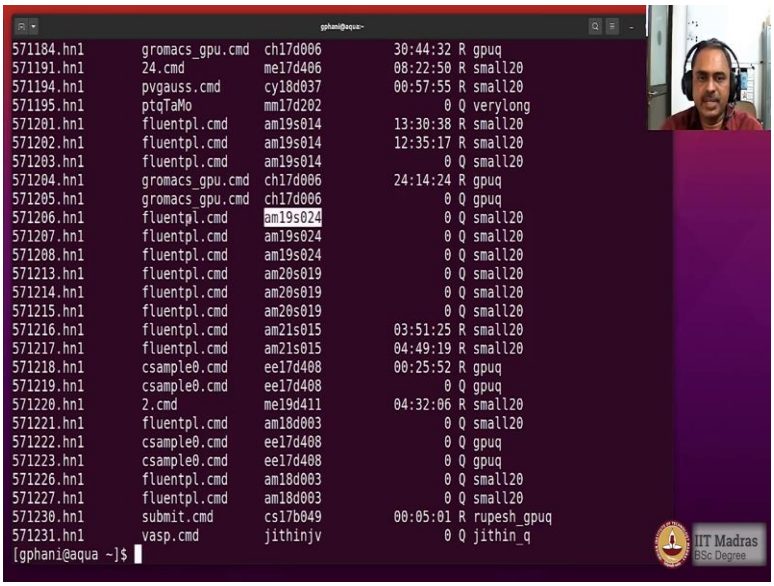


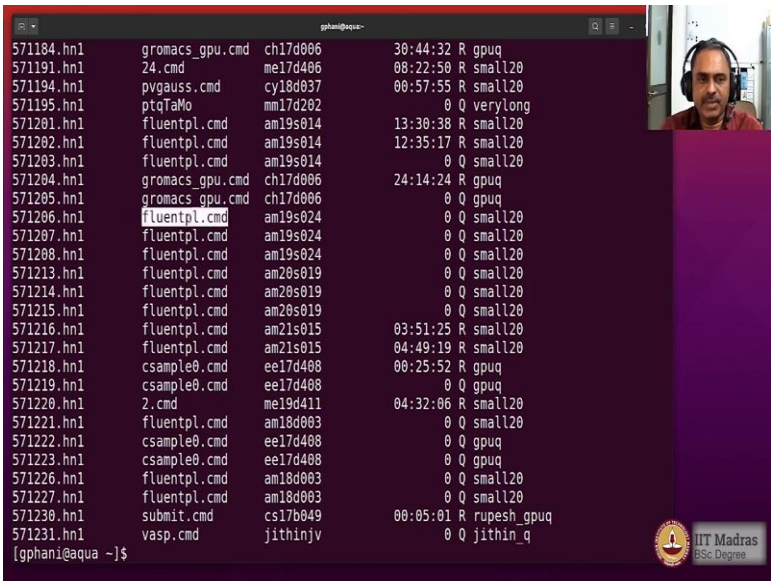


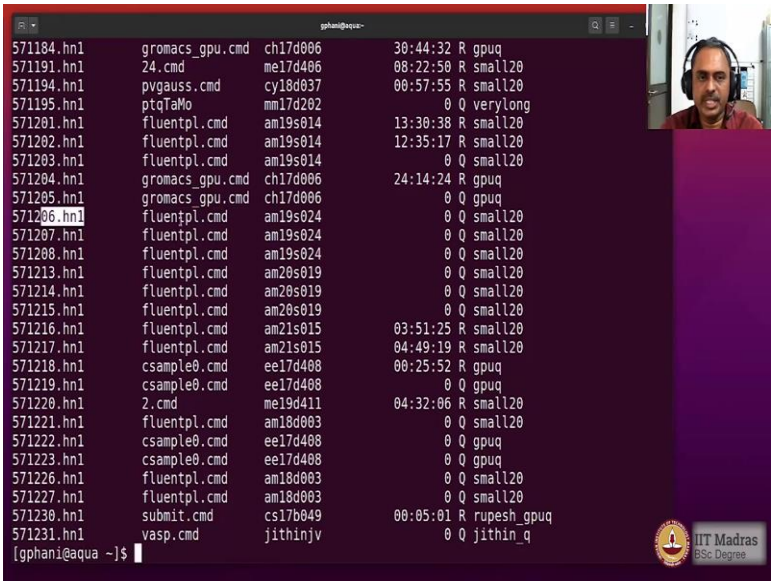
Now, if I put w it tells me who are all the people who are logged on. So, you can see how many students are logged on and from various machine on the campus at what time they are logged on, what are they doing and all that. So, this is a super cluster, 100 of people can log in and submit jobs and get them executed because we have got more than 200 nodes of computer 200 computers connected in a big network and jobs will be executing on those nodes as we submit to a job scheduler.

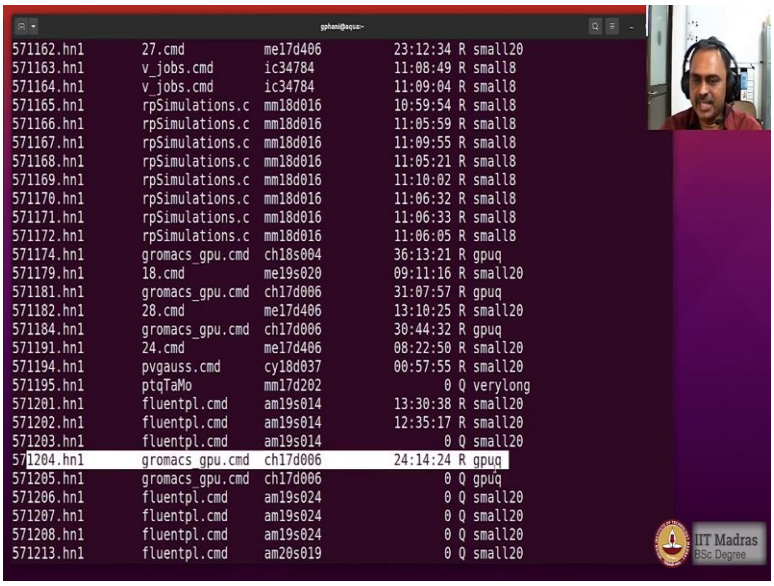
(Refer Slide Time: 31:40)

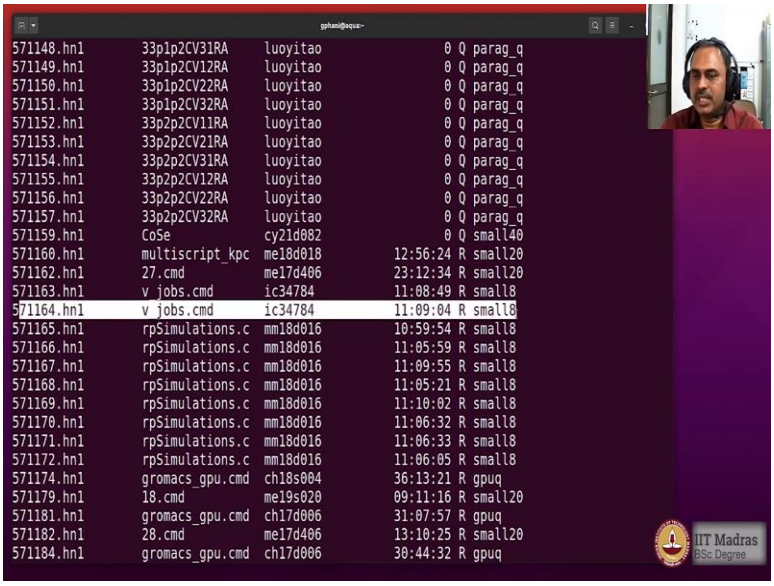


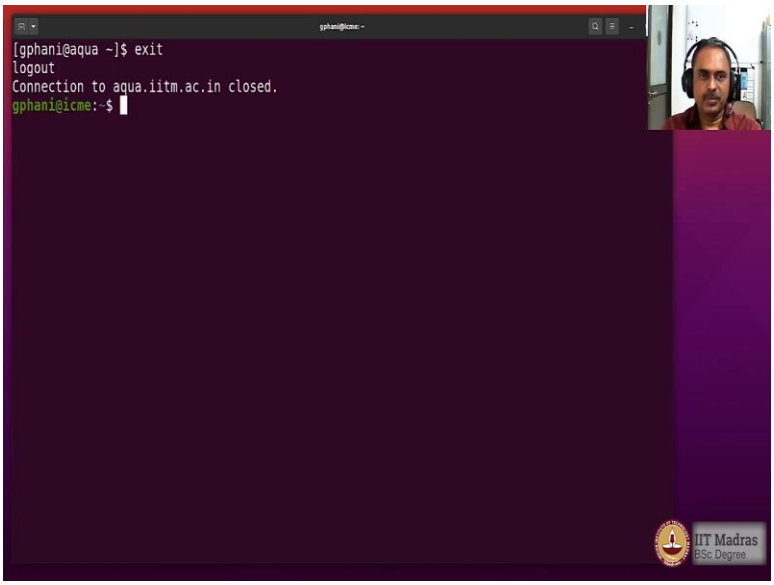



gphani@aqua:~
571184.hn1 gromacs_gpu.cmd ch17d006 30:44:32 R gpuq
571191.hn1 24.cmd me17d406 08:22:50 R small20
571194.hn1 pvgauss.cmd cy18d037 00:57:55 R small20
571195.hn1 ptqTaMo mm17d202 0 Q verylong
571201.hn1 fluentpl.cmd am19s014 13:30:38 R small20
571202.hn1 fluentpl.cmd am19s014 12:35:17 R small20
571203.hn1 fluentpl.cmd am19s014 0 Q small20
571204.hn1 gromacs_gpu.cmd ch17d006 24:14:24 R gpuq
571205.hn1 gromacs_gpu.cmd ch17d006 0 Q gpuq
571206.hn1 fluentpl.cmd am19s024 0 Q small20
571207.hn1 fluentpl.cmd am19s024 0 Q small20
571208.hn1 fluentpl.cmd am19s024 0 Q small20
571213.hn1 fluentpl.cmd am20s019 0 Q small20
571214.hn1 fluentpl.cmd am20s019 0 Q small20
571215.hn1 fluentpl.cmd am20s019 0 Q small20
571216.hn1 fluentpl.cmd am21s015 03:51:25 R small20
571217.hn1 fluentpl.cmd am21s015 04:49:19 R small20
571218.hn1 csample0.cmd ee17d408 00:25:52 R gpuq
571219.hn1 csample0.cmd ee17d408 0 Q gpuq
571220.hn1 2.cmd me19d411 04:32:06 R small20
571221.hn1 fluentpl.cmd am18d003 0 Q small20
571222.hn1 csample0.cmd ee17d408 0 Q gpuq
571223.hn1 csample0.cmd ee17d408 0 Q gpuq
571226.hn1 fluentpl.cmd am18d003 0 Q small20
571227.hn1 fluentpl.cmd am18d003 0 Q small20
571230.hn1 submit.cmd cs17b049 00:05:01 R rupesh_gpuq
571231.hn1 vasp.cmd jithinjv 0 Q jithin_q
[gphani@aqua ~]$
IIT Madras
BSc Degree


gphani@aqua:~
571184.hn1 gromacs_gpu.cmd ch17d006 30:44:32 R gpuq
571191.hn1 24.cmd me17d406 08:22:50 R small20
571194.hn1 pvgauss.cmd cy18d037 00:57:55 R small20
571195.hn1 ptqTaMo mm17d202 0 Q verylong
571201.hn1 fluentpl.cmd am19s014 13:30:38 R small20
571202.hn1 fluentpl.cmd am19s014 12:35:17 R small20
571203.hn1 fluentpl.cmd am19s014 0 Q small20
571204.hn1 gromacs_gpu.cmd ch17d006 24:14:24 R gpuq
571205.hn1 gromacs_gpu.cmd ch17d006 0 Q gpuq
571206.hn1 fluentpl.cmd am19s024 0 Q small20
571207.hn1 fluentpl.cmd am19s024 0 Q small20
571208.hn1 fluentpl.cmd am19s024 0 Q small20
571213.hn1 fluentpl.cmd am20s019 0 Q small20
571214.hn1 fluentpl.cmd am20s019 0 Q small20
571215.hn1 fluentpl.cmd am20s019 0 Q small20
571216.hn1 fluentpl.cmd am21s015 03:51:25 R small20
571217.hn1 fluentpl.cmd am21s015 04:49:19 R small20
571218.hn1 csample0.cmd ee17d408 00:25:52 R gpuq
571219.hn1 csample0.cmd ee17d408 0 Q gpuq
571220.hn1 2.cmd me19d411 04:32:06 R small20
571221.hn1 fluentpl.cmd am18d003 0 Q small20
571222.hn1 csample0.cmd ee17d408 0 Q gpuq
571223.hn1 csample0.cmd ee17d408 0 Q gpuq
571226.hn1 fluentpl.cmd am18d003 0 Q small20
571227.hn1 fluentpl.cmd am18d003 0 Q small20
571230.hn1 submit.cmd cs17b049 00:05:01 R rupesh_gpuq
571231.hn1 vasp.cmd jithinjv 0 Q jithin_q
[gphani@aqua ~]$
IIT Madras
BSc Degree


gphani@aqua:~
571162.hn1 27.cmd me17d406 23:12:34 R small20
571163.hn1 v_jobs.cmd ic34784 11:08:49 R small8
571164.hn1 v_jobs.cmd ic34784 11:09:04 R small8
571165.hn1 rpSimulations.c mm18d016 10:59:54 R small8
571166.hn1 rpSimulations.c mm18d016 11:05:59 R small8
571167.hn1 rpSimulations.c mm18d016 11:09:55 R small8
571168.hn1 rpSimulations.c mm18d016 11:05:21 R small8
571169.hn1 rpSimulations.c mm18d016 11:10:02 R small8
571170.hn1 rpSimulations.c mm18d016 11:06:32 R small8
571171.hn1 rpSimulations.c mm18d016 11:06:33 R small8
571172.hn1 rpSimulations.c mm18d016 11:06:05 R small8
571174.hn1 gromacs_gpu.cmd ch18s004 36:13:21 R gpuq
571179.hn1 18.cmd me19s020 09:11:16 R small20
571181.hn1 gromacs_gpu.cmd ch17d006 31:07:57 R gpuq
571182.hn1 28.cmd me17d406 13:10:25 R small20
571184.hn1 gromacs_gpu.cmd ch17d006 30:44:32 R gpuq
571191.hn1 24.cmd me17d406 08:22:50 R small20
571194.hn1 pvgauss.cmd cy18d037 00:57:55 R small20
571195.hn1 ptqTaMo mm17d202 0 Q verylong
571201.hn1 fluentpl.cmd am19s014 13:30:38 R small20
571202.hn1 fluentpl.cmd am19s014 12:35:17 R small20
571203.hn1 fluentpl.cmd am19s014 0 Q small20
571204.hn1 gromacs_gpu.cmd ch17d006 24:14:24 R gpuq
571205.hn1 gromacs_gpu.cmd ch17d006 0 Q gpuq
571206.hn1 fluentpl.cmd am19s024 0 Q small20
571207.hn1 fluentpl.cmd am19s024 0 Q small20
571208.hn1 fluentpl.cmd am19s024 0 Q small20
571213.hn1 fluentpl.cmd am20s019 0 Q small20
IIT Madras
BSc Degree

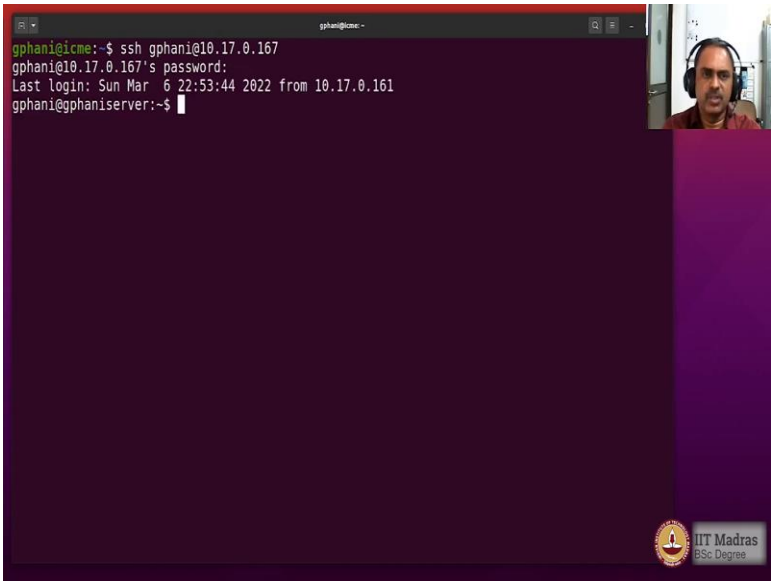

gphani@aqua:~
571148.hn1 33p1p2CV31RA luoyitao 0 Q parag_q
571149.hn1 33p1p2CV12RA luoyitao 0 Q parag_q
571150.hn1 33p1p2CV22RA luoyitao 0 Q parag_q
571151.hn1 33p1p2CV32RA luoyitao 0 Q parag_q
571152.hn1 33p2p2CV11RA luoyitao 0 Q parag_q
571153.hn1 33p2p2CV21RA luoyitao 0 Q parag_q
571154.hn1 33p2p2CV31RA luoyitao 0 Q parag_q
571155.hn1 33p2p2CV12RA luoyitao 0 Q parag_q
571156.hn1 33p2p2CV22RA luoyitao 0 Q parag_q
571157.hn1 33p2p2CV32RA luoyitao 0 Q parag_q
571159.hn1 CoSe cy21d082 0 Q small40
571160.hn1 multiscript_kpc me18d018 12:56:24 R small20
571162.hn1 27.cmd me17d406 23:12:34 R small20
571163.hn1 v_jobs.cmd ic34784 11:08:49 R small8
571164.hn1 v_jobs.cmd ic34784 11:09:04 R small8
571165.hn1 rpSimulations.c mm18d016 10:59:54 R small8
571166.hn1 rpSimulations.c mm18d016 11:05:59 R small8
571167.hn1 rpSimulations.c mm18d016 11:09:55 R small8
571168.hn1 rpSimulations.c mm18d016 11:05:21 R small8
571169.hn1 rpSimulations.c mm18d016 11:10:02 R small8
571170.hn1 rpSimulations.c mm18d016 11:06:32 R small8
571171.hn1 rpSimulations.c mm18d016 11:06:33 R small8
571172.hn1 rpSimulations.c mm18d016 11:06:05 R small8
571174.hn1 gromacs_gpu.cmd ch18s004 36:13:21 R gpuq
571179.hn1 18.cmd me19s020 09:11:16 R small20
571181.hn1 gromacs_gpu.cmd ch17d006 31:07:57 R gpuq
571182.hn1 28.cmd me17d406 13:10:25 R small20
571184.hn1 gromacs_gpu.cmd ch17d006 30:44:32 R gpuq
IIT Madras
BSc Degree

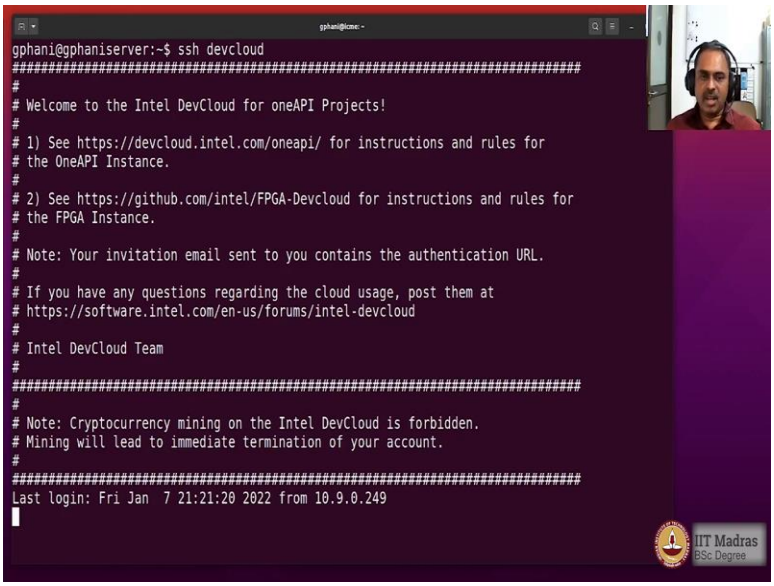


So, the job scheduler is called queue stat to just tell the statistics of the queues that are available. And it has alias so I do not want that alias. So, I will remove that alias and I run the command without the alias. So, that it is meant for jobs of everybody. And now you can see that which student has submitted which kind of a job and on which node it is running, what job ID it is running and what is the status. For example, this is in queue, but this job is actually running and it is a GPU queue. And this job is running and it is occupying all these 8 cores.

So, like this, you can actually see that a super computer is available to you within the secure shell by just a command line environment, you can look at the jobs you can submit jobs and you can actually make use of the supercomputer facilities quite nicely. If you know the ssh very well. So, from this desktop, which is ICME where we are doing the recording of the videos, we have connected to till now, three different machines we have connected to my desktop, the a qua supercluster and we have connected also to my laptop and you see that I have not moved from here. So, from the terminal, we are able to connect to multiple machines.

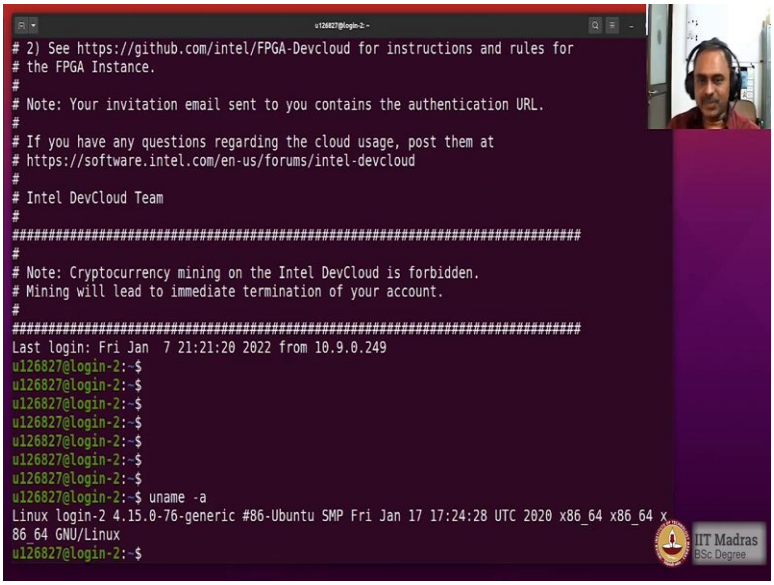
(Refer Slide Time: 33:08)

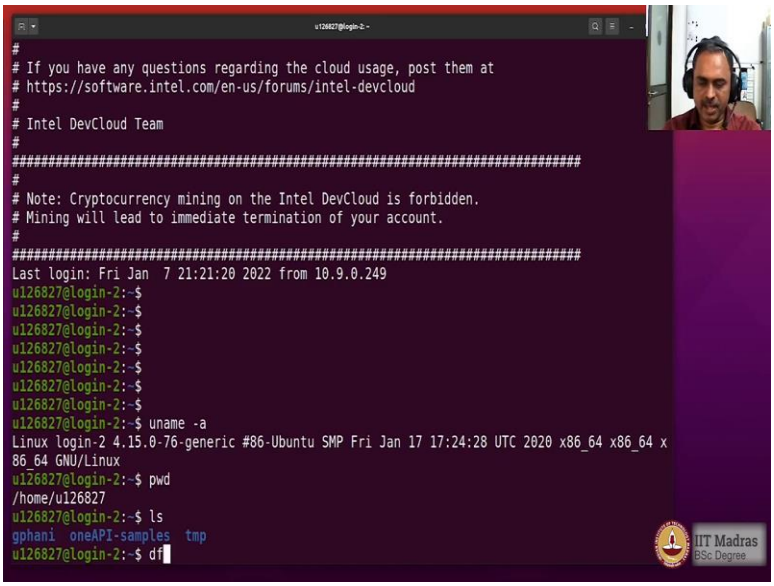


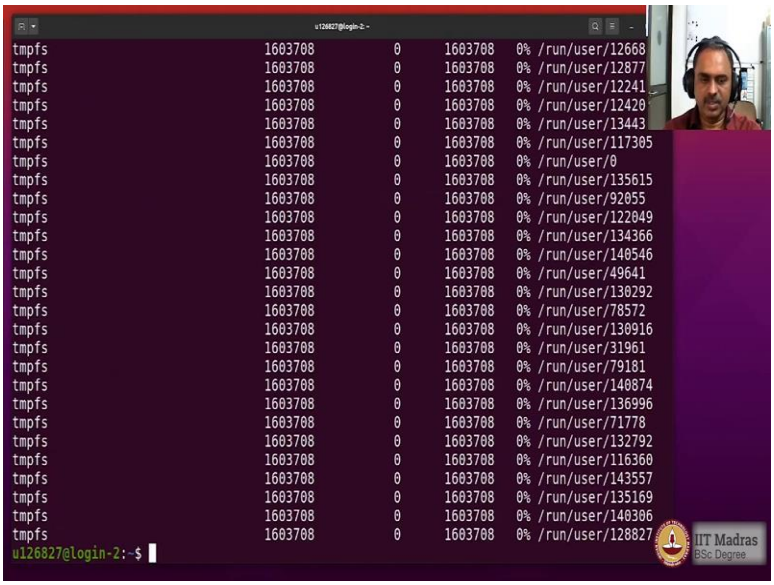


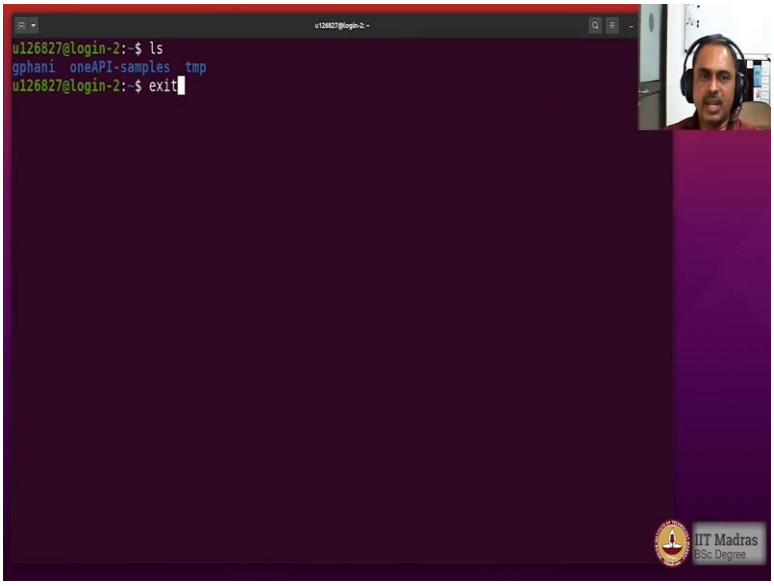
Now, I will also connect with the Intel developer cloud via my desktop through ssh. I have configured it already. So, it actually already has the ssh keys shared, so it does not ask me for a password. So, you can also have an account on Intel developer cloud by registering on their website. So here is a opportunity for you to see that sitting in IIT Madras by just using ssh I am now logging on to a machine that is actually located in the Intel high performance facility that they have made available for education sector for free.

(Refer Slide Time: 33:51)







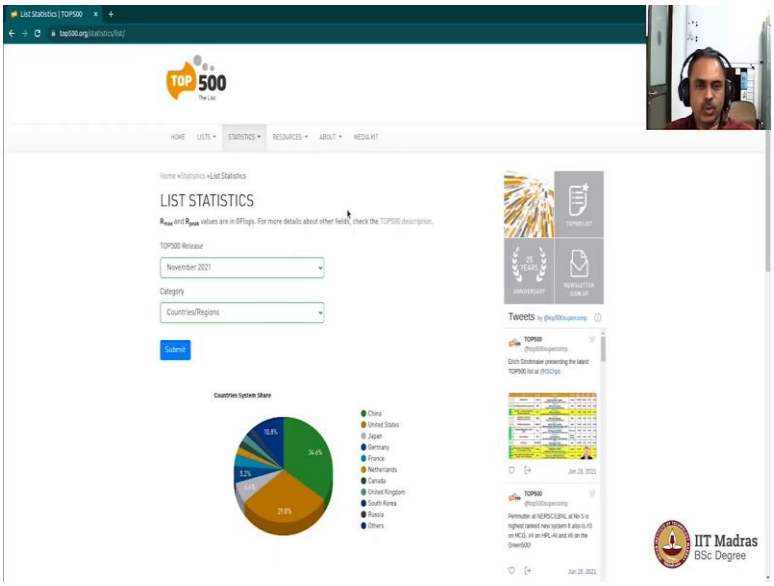


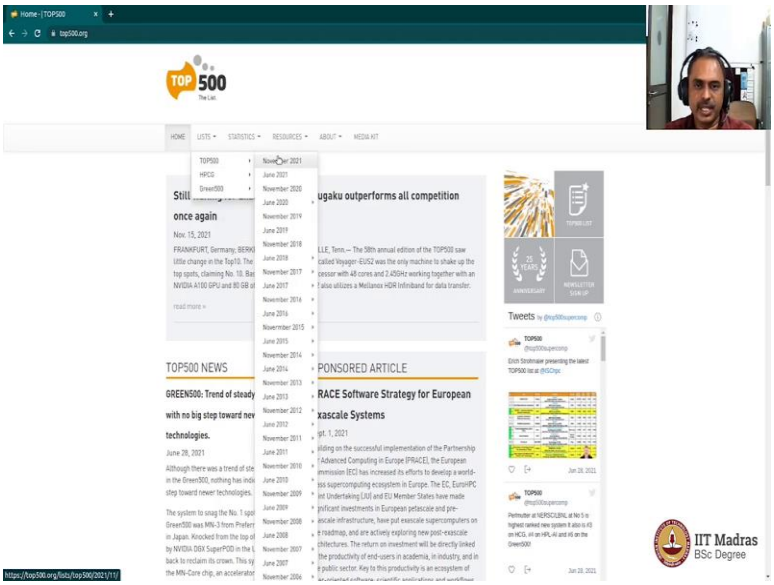
And what kind of machines it is it is a Ubuntu Linux machine, thank God because it means that we are in a familiar territory and therefore we can go on to use this particular machine as if it is our own Linux laptop. So, most of the commands that we know will work there. So, you have got all kinds of stuff out there that you can work with.

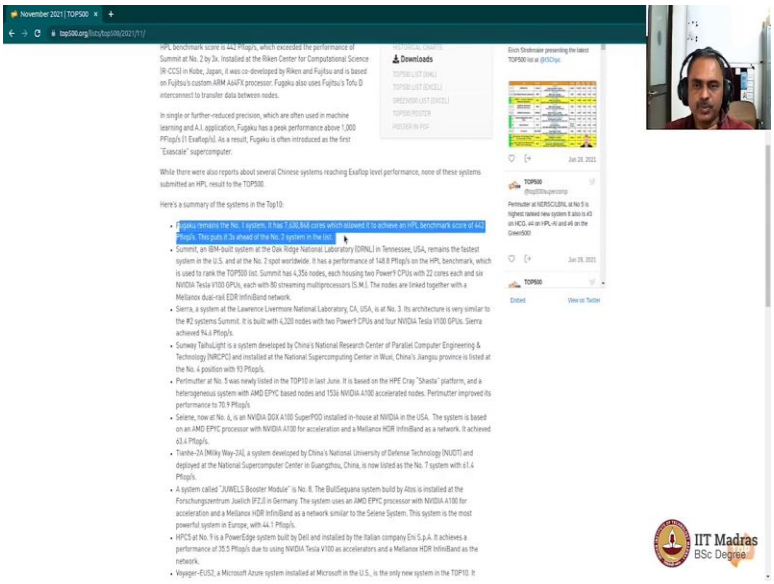
So, as you can see, we have connected using the ssh from the terminal and environment from this machine to a desktop machine in the room, a laptop in the room, a supercomputer within the campus and Intel developer cloud which is actually sitting somewhere in California perhaps. So, this is possible because the routing et cetera are taken care of and secure shell is providing us a way by which we can connect over a terminal.

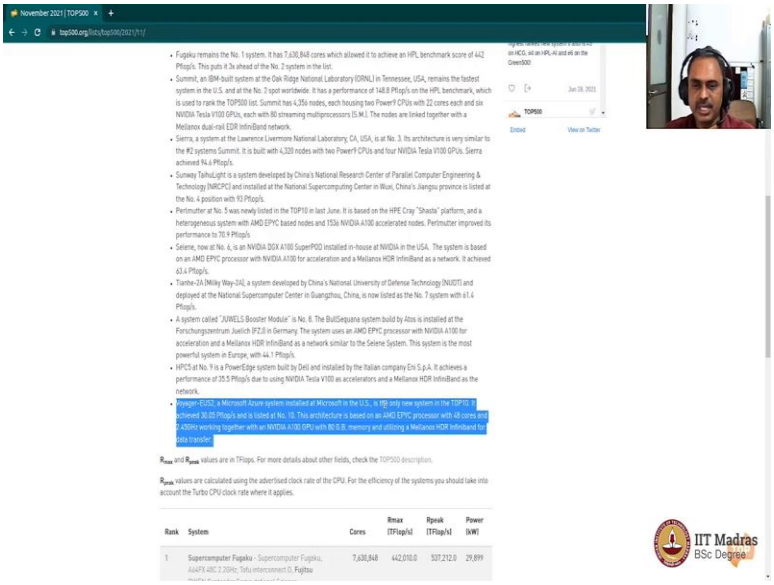
And just because a terminal is a very limited amount of communication needed for us to view what is there on the screen, it tends to be quite fast in terms of response and therefore, learning the bash shell over ssh connection would be very useful because we will then be able to work on remote computers quite effectively and your knowledge of Ubuntu will come after us in almost every such machine. Let us, look at the top 500 dot org to look at what are those supercomputers the world and how fast are they.

(Refer Slide Time: 35:31)



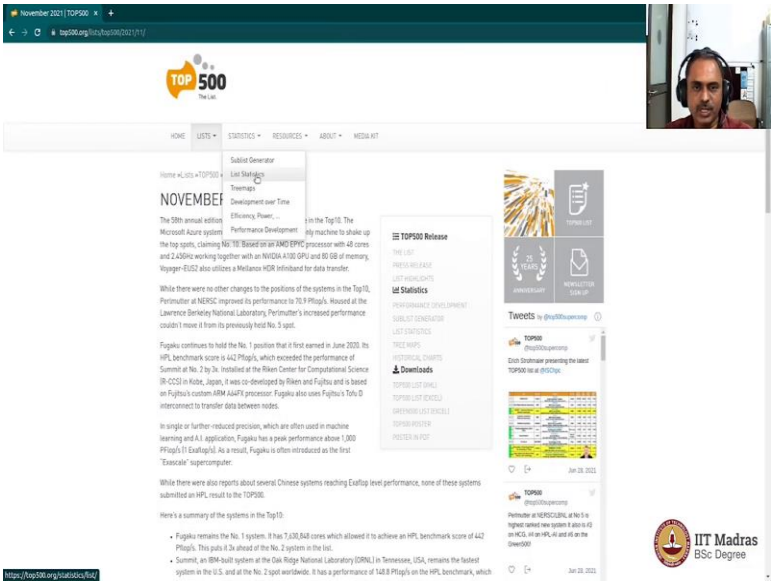


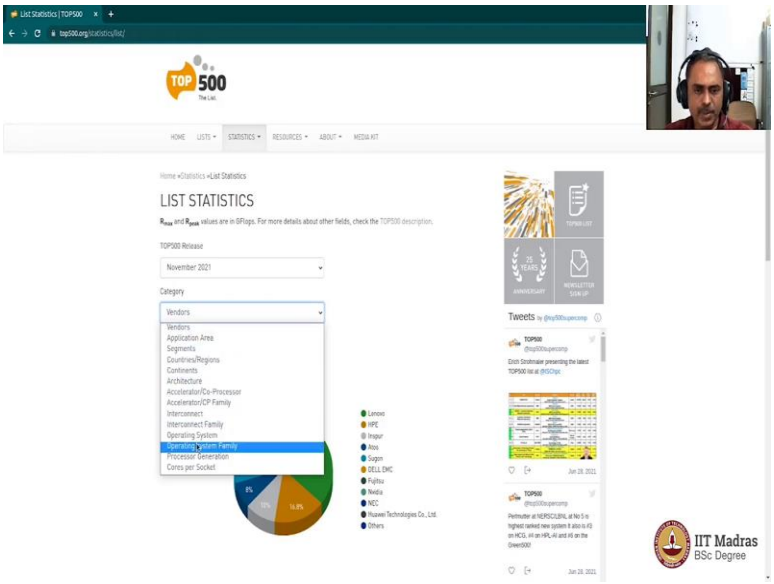


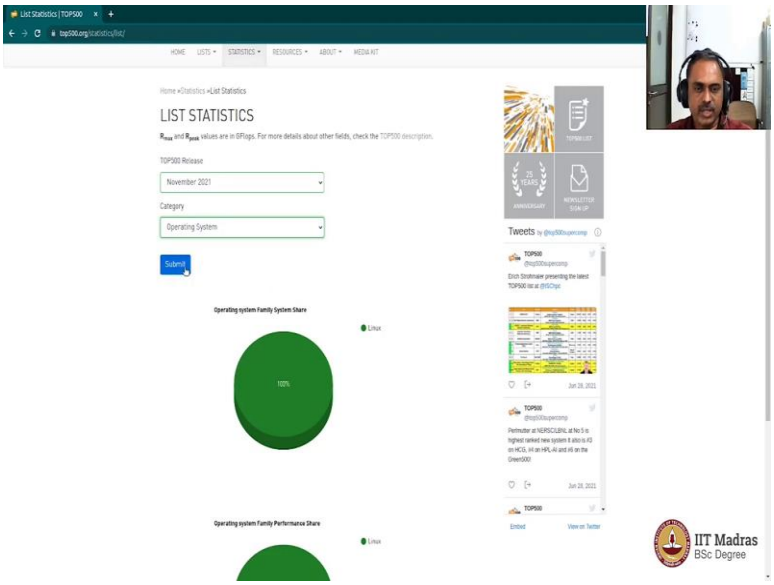


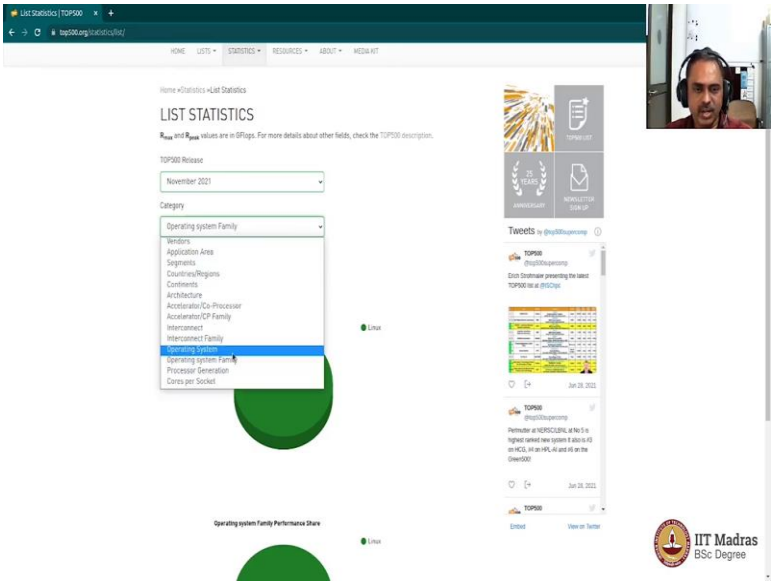
So, let us look at the top 500 dot org website, you have the top computers in the world are being listed every 6 months. So, you could look at the November 2021 listing which is the latest as of now, it shows that Fugaku is at half an hexa flop capacity at the number one in the world, which means that we are in the hexa flop regime already. And Microsoft Azure system is at the number 10 position which means the public cloud which you can access by paying for it is already available at number 10 in the world.

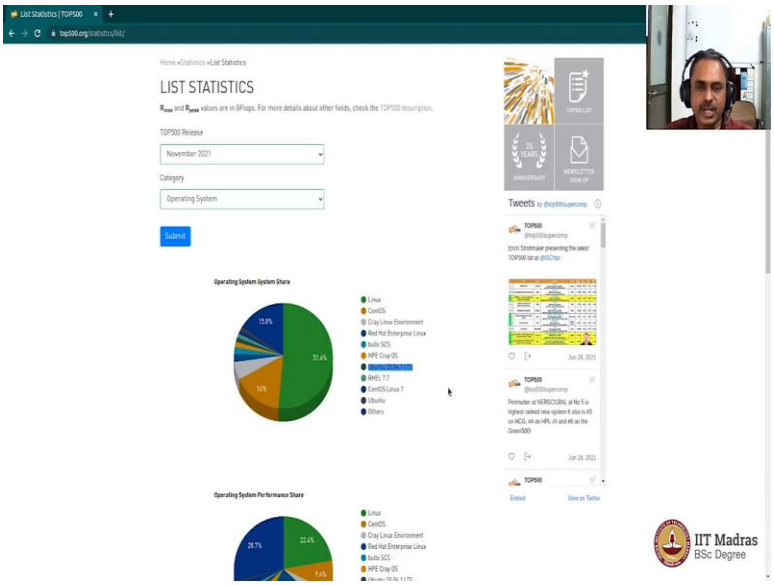
(Refer Slide Time: 36:10)






List Statistics | TOP500
top500.org/statistics/list/
HOME
LISTS
STATISTICS
RESOURCES
ABOUT
MEDIA KIT
Home » Statistics » List Statistics
LIST STATISTICS
Rmax and Rpeak values are in GFlops. For more details about other fields, check the TOP500 description.
TOP500 Release
November 2021
Category
Operating System
Submit
Operating system Family System Share
Linux
100%
Operating system Family Performance Share
Linux
Tweets
IIT Madras
BSc Degree

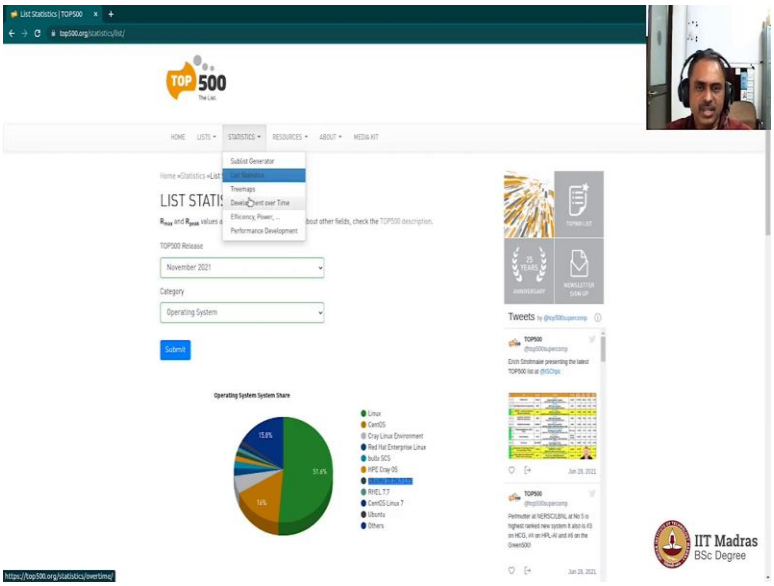

List Statistics | TOP500
top500.org/statistics/list/
HOME
LISTS
STATISTICS
RESOURCES
ABOUT
MEDIA KIT
Home » Statistics » List Statistics
LIST STATISTICS
Rmax and Rpeak values are in GFlops. For more details about other fields, check the TOP500 description.
TOP500 Release
November 2021
Category
Operating system Family
Vendors
Application Area
Segments
Countries/Regions
Continents
Architecture
Accelerator/Co-Processor
Accelerator/CP Family
Interconnect
Interconnect Family
Operating System
Operating system Family
Processor Generation
Cores per Socket
Linux
Operating system Family Performance Share
Linux
Tweets
IIT Madras
BSc Degree

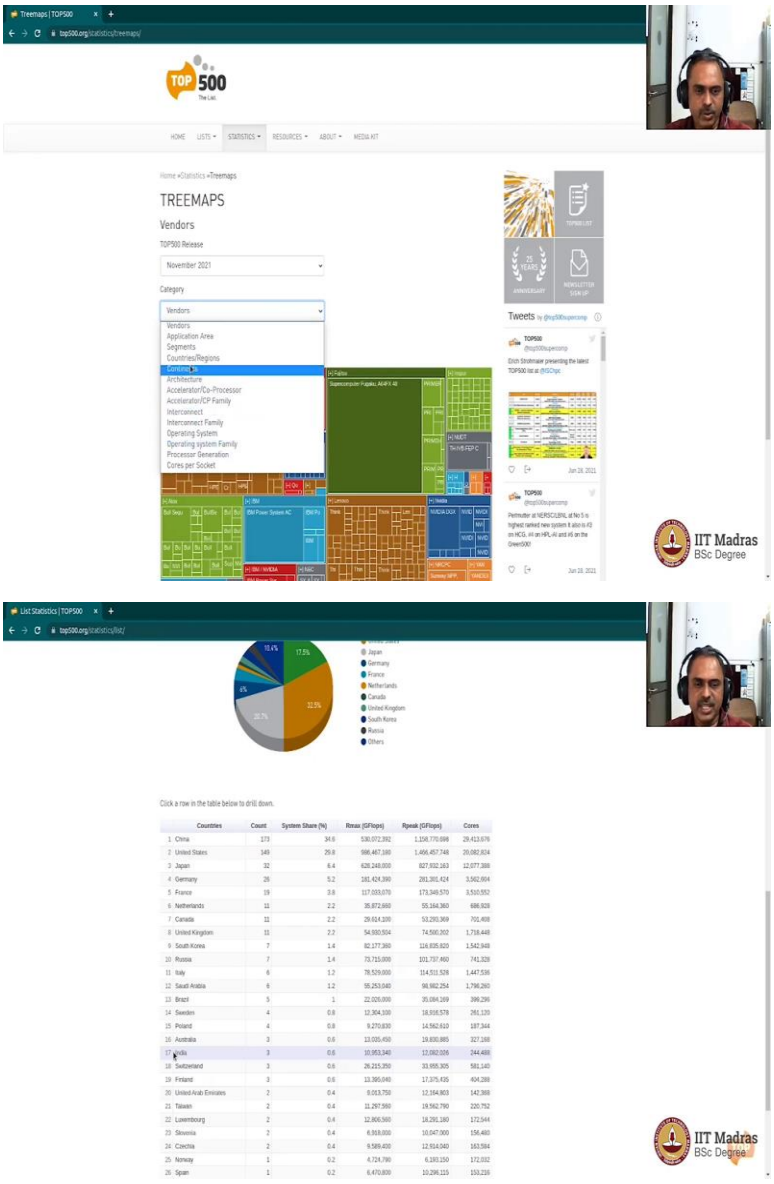


And let us see what are the kind of statistics with respect to the operating system. So, in terms of operating system fam ily, you can see that 100 percent of these supercomputers are Linux family. That is exciting for us because we are now familiar with the Linux operating system and which flavour of open system is also listed here.

Ubuntu 20.04 is also listed here, along with RedHat enterprise, Linux and CentOS, HPE Cray OS and all that. So, all these are basically Linux. So, they will have the same file system with the same structure, and also the bash shell. So, therefore we are at home in any of these top 500 supercomputers in the world.

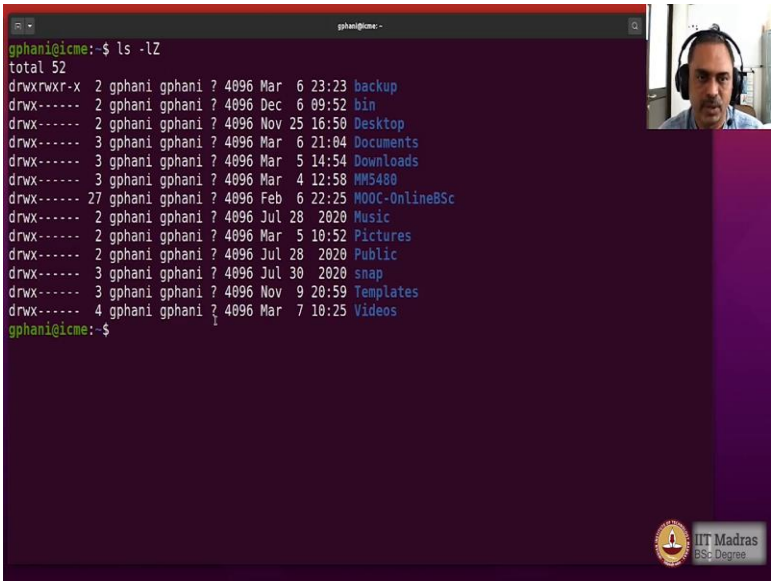
(Refer Slide Time: 36:55)





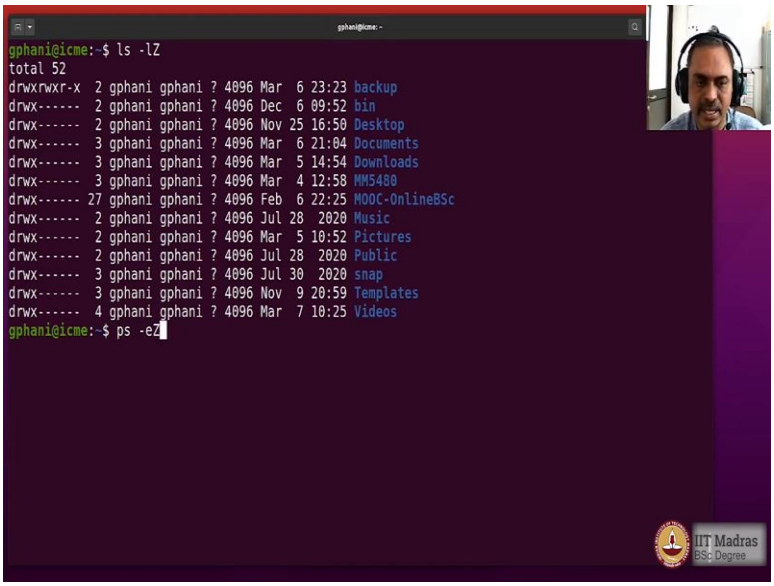
And where are we with the countries. When it comes to India, we could look at that. So, here we see that India is at position 17, which is not bad. But I am sure that it will climb up in the next couple of years because several national supercomputing machine facilities are being set up in the country. And we are at home in any of this mission, because they are all going to use Linux. So, I hope it was useful for you to find the application of learning supercomputer, learning the operating system that powers the supercomputers in the world.

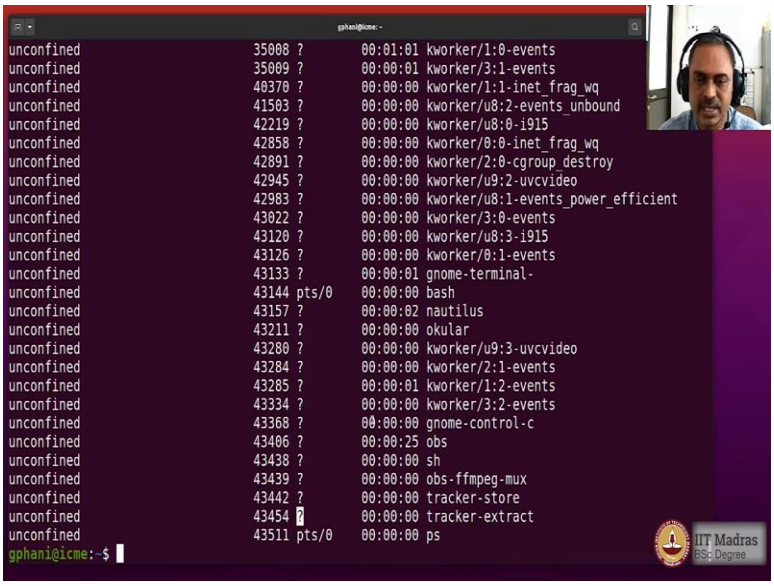
(Refer Slide Time: 37:31)



So, here is a brief demo on checking the SELinux, whether it was enabled or not. So, on the machine where I am recording, so I will just put ls minus lz and you would see that there is a question mark, which means that perhaps SELinux was not enabled on this machine.

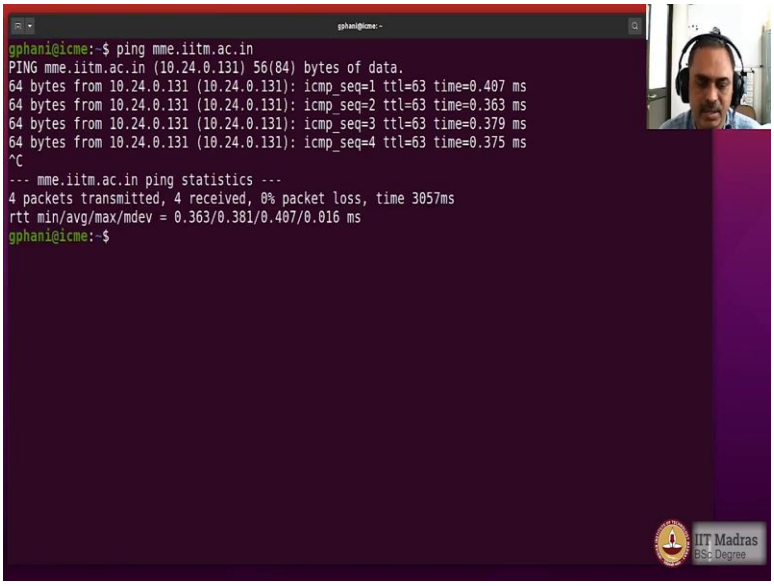
(Refer Slide Time: 37:51)





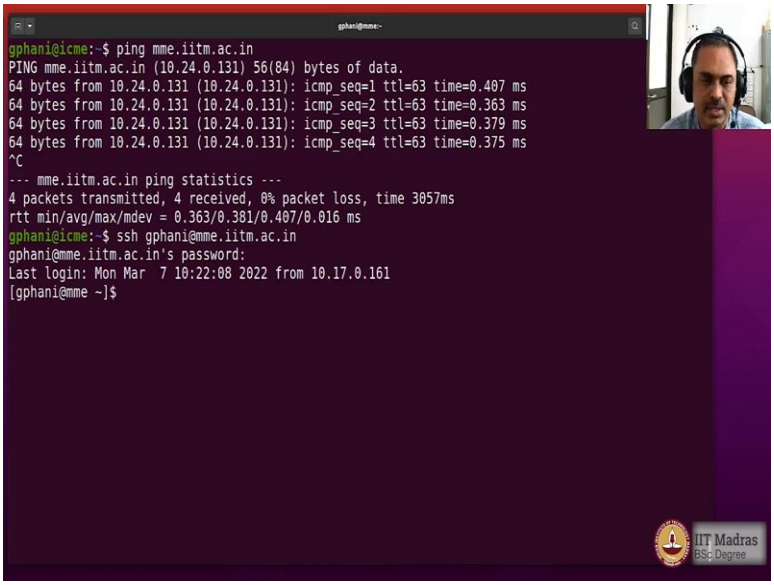
And also, I would use the ps minus ez option. And again, there is a question mark here, which means that the processes also do not have the SELinux security pitch is enable.

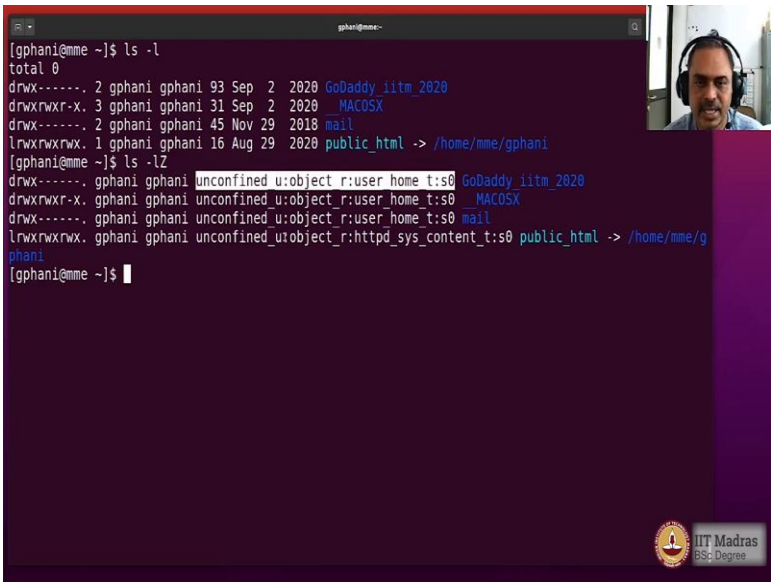
(Refer Slide Time: 38:08)



So, I would see for the web server, or our department is up using the ping and it appears to be available.

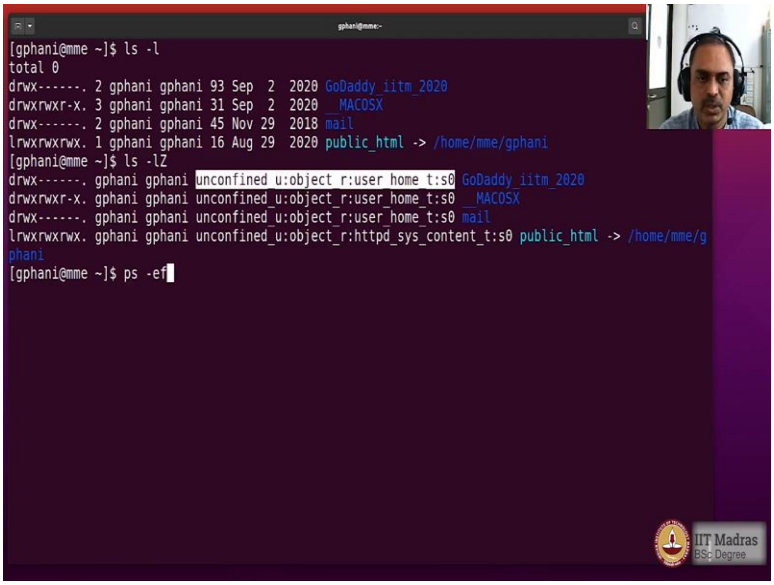
(Refer Slide Time: 38:18)

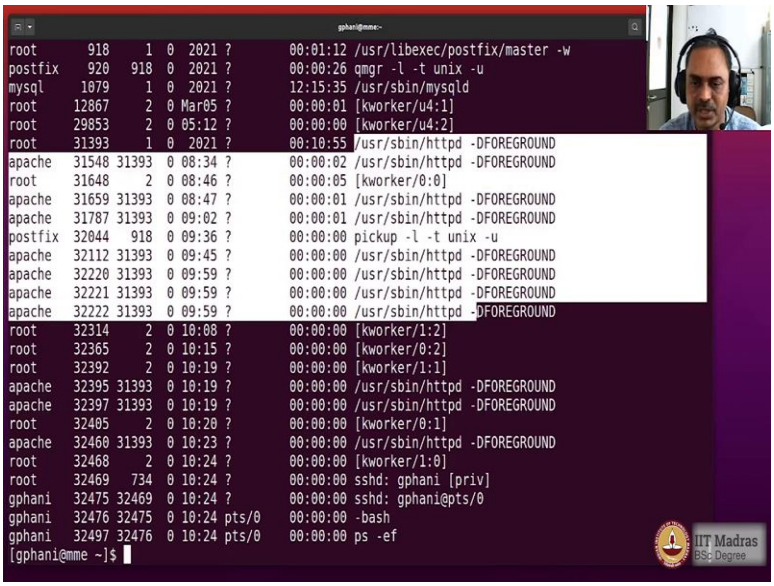




So, I happen to have an account on that. So, I will log in there. And in this web server, what I would do is look at the files and with the capital Z option, you see that there is a lot of information that is coming here. So, you see that all these options show that the filesystem has had a layer on top of it from the SELinux, which is a protection mechanism. So, on the web server our department the SELinux has been enabled.

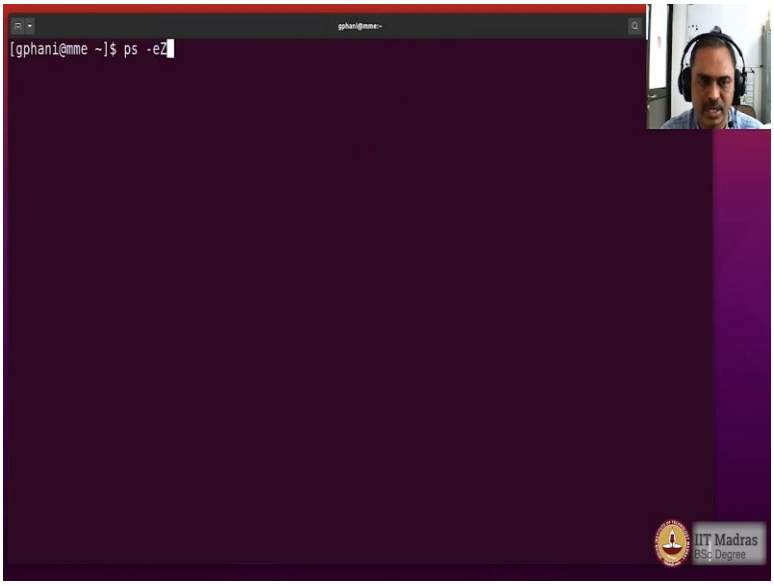
(Refer Slide Time: 38:50)

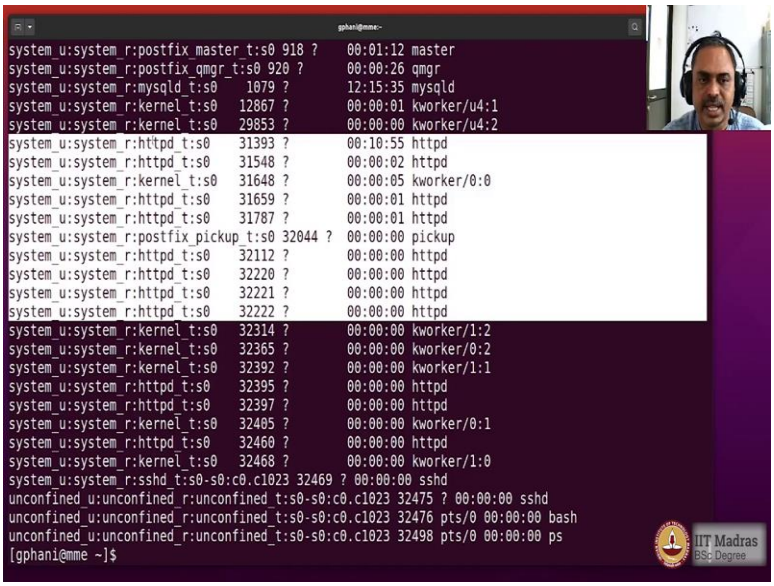


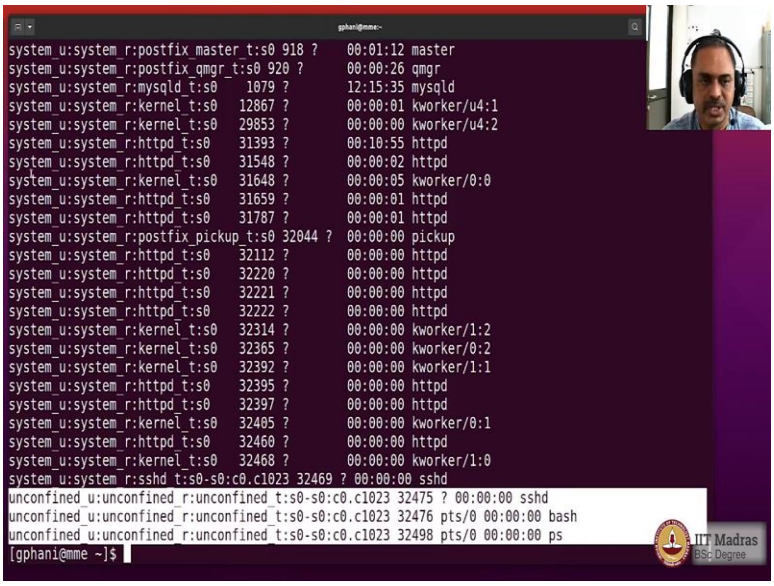


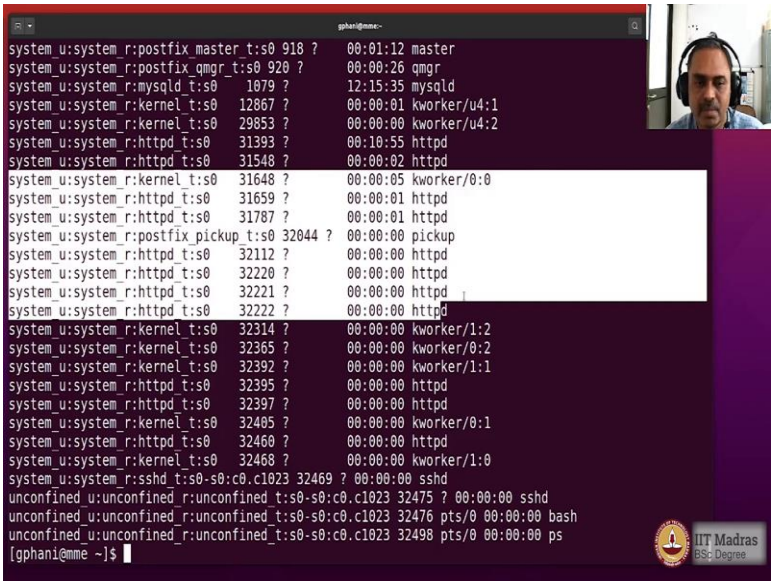
And also, the process listing, normal listing would actually show that there is a web service that is running httpd.

(Refer Slide Time: 39:00)





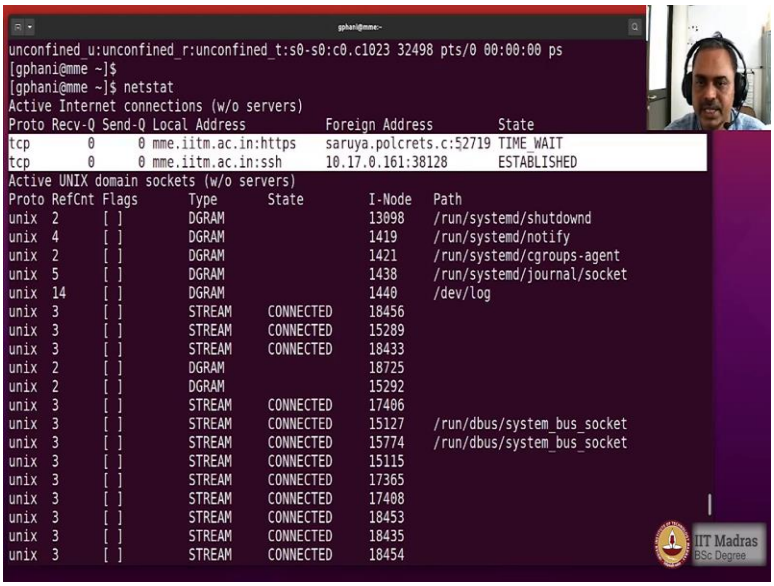


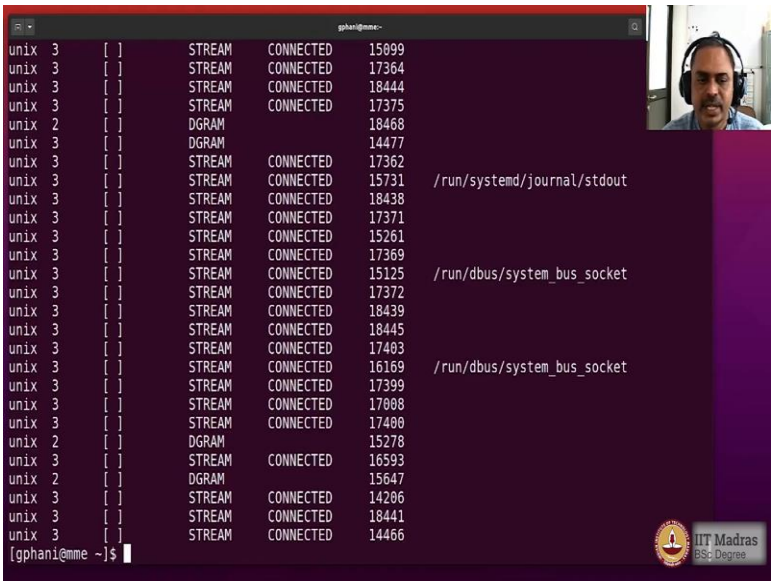


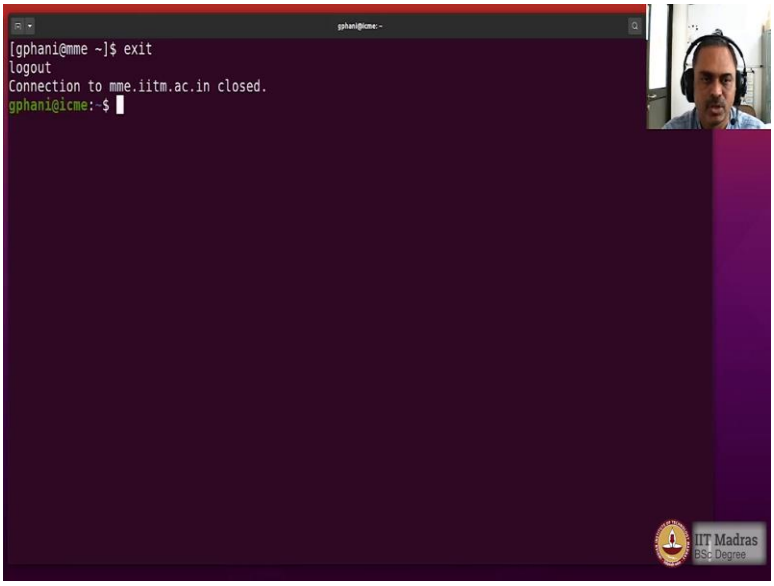
But if I use the same listing with capital Z, you will see that the web servers are running with the additional conditions where it has the fields that are available here in front of it, where the role namely the httpd underscore t is listed. So, that whatever the restrictions meant for a particular service will then be put in place.

So, you can see that there are certain other services which have different roles compared to httpd. And that is exactly what I was talking about, where the role-based access can be given to specific services keeping in mind, what kind of users that expected to connect with the machine through those services.

(Refer Slide Time: 39:48)

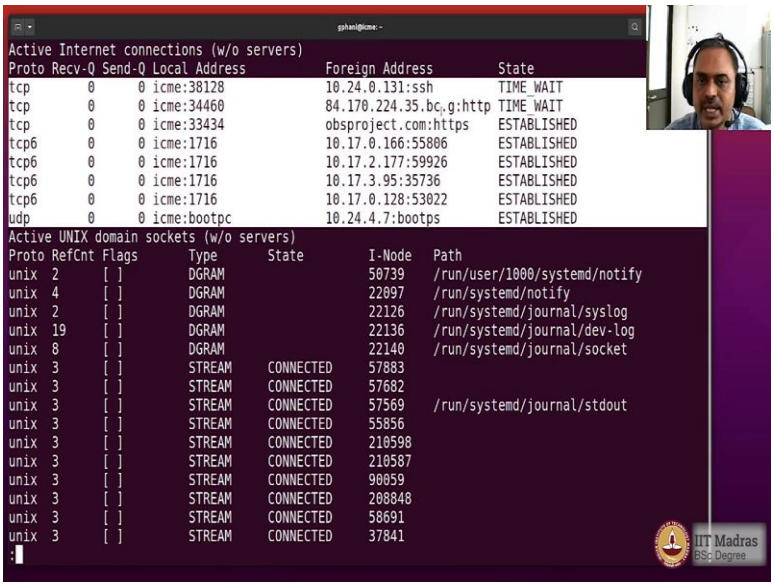


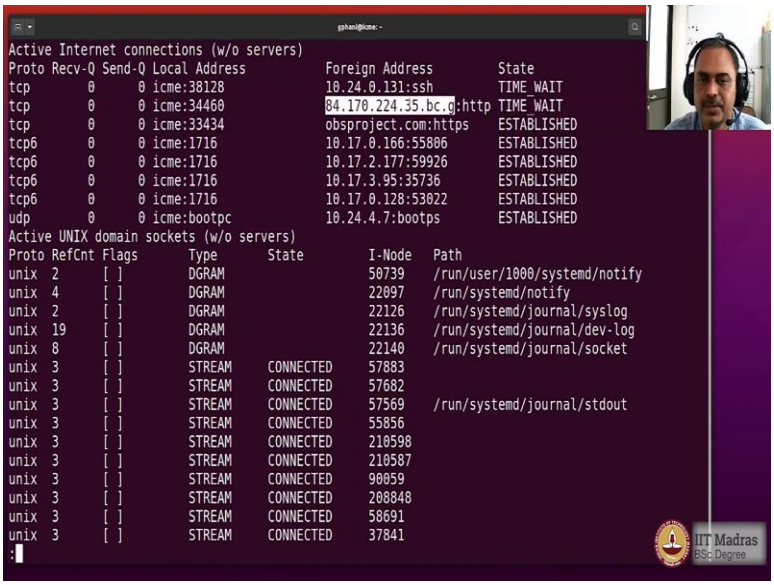


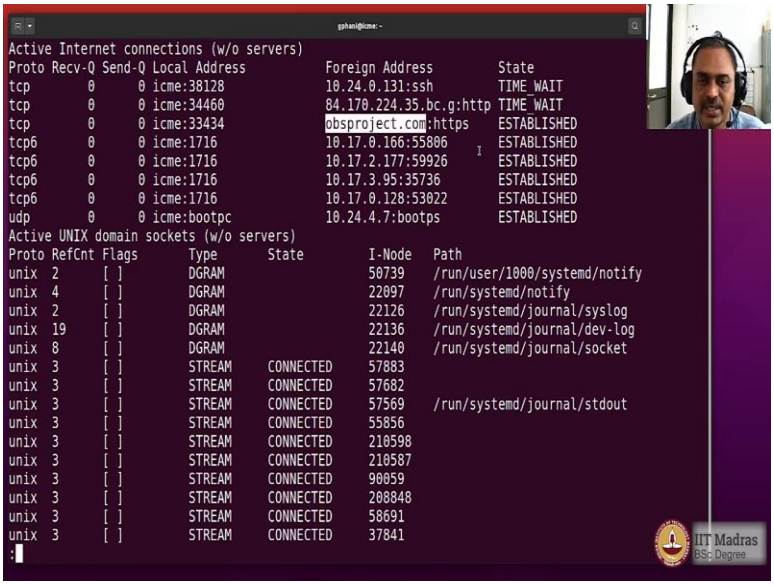


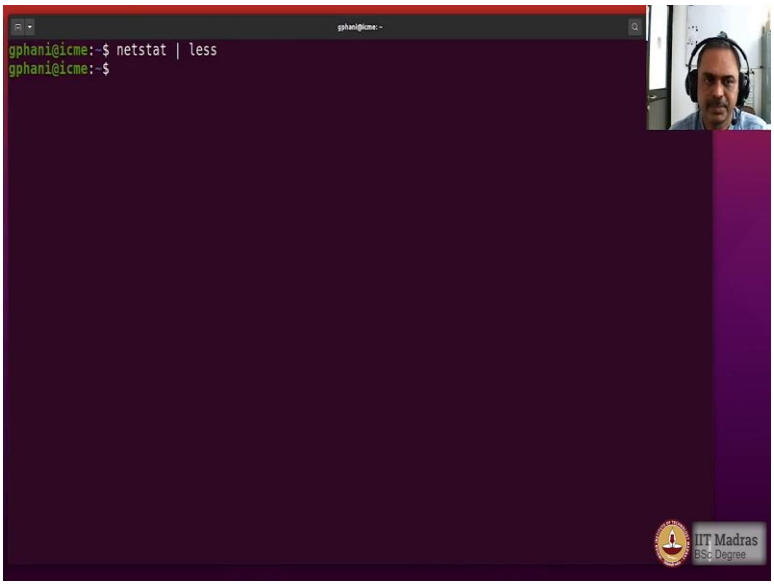
And netstat is a command to show you the network statistics and here you can look at what all the various programs that are running. And you can see that the TCP connection right now to the web server is open from a particular foreign address and the port number from the client side is also listed. And there is also an ssh connection coming from the IP address of the machine where we are recording. So, you can actually see what are the active network connections that are actually taking place in the computer using netstat.

(Refer Slide Time: 40:33)




gphani@icme: ~
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 icme:38128 10.24.0.131:ssh TIME_WAIT
tcp 0 0 icme:34460 84.170.224.35.bc.g:http TIME_WAIT
tcp 0 0 icme:33434 obsproject.com:https ESTABLISHED
tcp6 0 0 icme:1716 10.17.0.166:55806 ESTABLISHED
tcp6 0 0 icme:1716 10.17.2.177:59926 ESTABLISHED
tcp6 0 0 icme:1716 10.17.3.95:35736 ESTABLISHED
tcp6 0 0 icme:1716 10.17.0.128:53022 ESTABLISHED
udp 0 0 icme:bootpc 10.24.4.7:bootps ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ] DGRAM 50739 /run/user/1000/systemd/notify
unix 4 [ ] DGRAM 22097 /run/systemd/notify
unix 2 [ ] DGRAM 22126 /run/systemd/journal/syslog
unix 19 [ ] DGRAM 22136 /run/systemd/journal/dev-log
unix 8 [ ] DGRAM 22140 /run/systemd/journal/socket
unix 3 [ ] STREAM CONNECTED 57883
unix 3 [ ] STREAM CONNECTED 57682
unix 3 [ ] STREAM CONNECTED 57569 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 55856
unix 3 [ ] STREAM CONNECTED 210598
unix 3 [ ] STREAM CONNECTED 210587
unix 3 [ ] STREAM CONNECTED 90059
unix 3 [ ] STREAM CONNECTED 208848
unix 3 [ ] STREAM CONNECTED 58691
unix 3 [ ] STREAM CONNECTED 37841
:
IIT Madras
BSc Degree


gphani@icme: ~
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 icme:38128 10.24.0.131:ssh TIME_WAIT
tcp 0 0 icme:34460 84.170.224.35.bc.g:http TIME_WAIT
tcp 0 0 icme:33434 obsproject.com:https ESTABLISHED
tcp6 0 0 icme:1716 10.17.0.166:55806 ESTABLISHED
tcp6 0 0 icme:1716 10.17.2.177:59926 ESTABLISHED
tcp6 0 0 icme:1716 10.17.3.95:35736 ESTABLISHED
tcp6 0 0 icme:1716 10.17.0.128:53022 ESTABLISHED
udp 0 0 icme:bootpc 10.24.4.7:bootps ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ] DGRAM 50739 /run/user/1000/systemd/notify
unix 4 [ ] DGRAM 22097 /run/systemd/notify
unix 2 [ ] DGRAM 22126 /run/systemd/journal/syslog
unix 19 [ ] DGRAM 22136 /run/systemd/journal/dev-log
unix 8 [ ] DGRAM 22140 /run/systemd/journal/socket
unix 3 [ ] STREAM CONNECTED 57883
unix 3 [ ] STREAM CONNECTED 57682
unix 3 [ ] STREAM CONNECTED 57569 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 55856
unix 3 [ ] STREAM CONNECTED 210598
unix 3 [ ] STREAM CONNECTED 210587
unix 3 [ ] STREAM CONNECTED 90059
unix 3 [ ] STREAM CONNECTED 208848
unix 3 [ ] STREAM CONNECTED 58691
unix 3 [ ] STREAM CONNECTED 37841
:
IIT Madras
BSc Degree



So, we will do the same netstat on the computer where we are recording. So, you will see that you have got a bunch of ports that are open for various purposes. And there is no service which is basically per HTTP. So, I am not running any web server on this machine. But I am opening a connection outward, which basically is to connect with the Google account, as well as the OBS recording system that is running is also actually having an internet connectivity for the service. So, you can see that though I have not explicitly opened that particular site, it has been opened by the OBS software that is running in the background, perhaps to check for any update or whatever. So, this is some brief demo on SELinux and netstat.