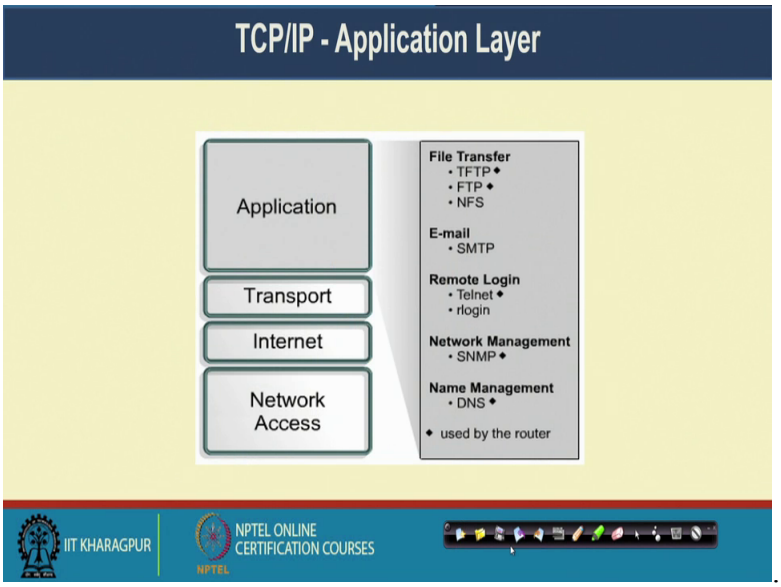
Computer Networks and Internet Protocol
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 06
Application Layer - II (DNS)

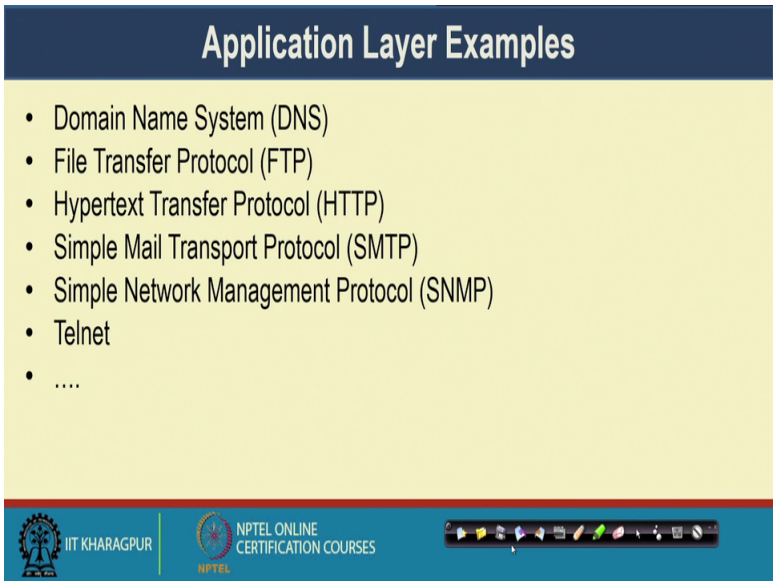
Hello. So, welcome to the next lecture on Computer Networks and Internet Protocols. Today we will be discussing one of the important application layer product all namely DNS right. So, this DNS helps us in dissolving name to IP conversant. So, we will we will go on looking at it.

(Refer Slide Time: 00:40)



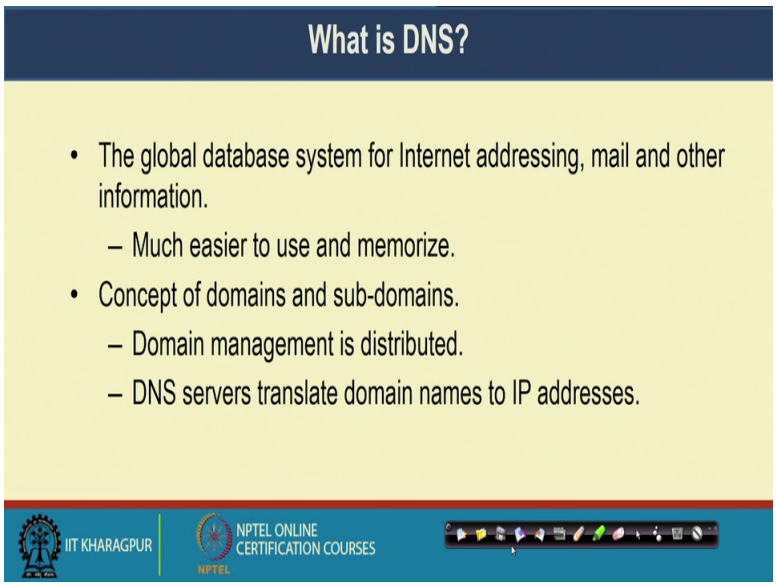
So, as if you just quick recollect, so we have seen this application layer. There are various protocols right like some related to file transfer, email, remote login network management and there is a name management or name resolution for name resolution which is DNS.

(Refer Slide Time: 00:59)



So, Domain Name Systems, FTP, Hypertext Protocol and so and so forth as some of the important protocols. Today we will discuss on domain name system or DNS.

(Refer Slide Time: 01:11).



So, what is DNS? It is a sort of a global data base for internet addressing mail and other information. So, why suddenly we require this? Now you see, whenever you want to communicate one packet or one data packet from one to another, what we require? We require primarily the IP address of the destination right. So, specially when we do internetworking IP address is the of the destination what we require.

Now, remembering IP address is the tedious job right. If you want to say if you want to open iitkgp www iitkgp ac dot in and instead of this if I say that you remember the IP address of iitkgp at 203 dot 16 dot so and so forth it is very tedious to remember. So, in other sense whether I can have some naming convention; so, that mean some names which intern can be resolved to IP right. Now on the other if you see the routers which can open up to or look up to network layer or IP, we will not understand this names right names can be only understood at the application level right.

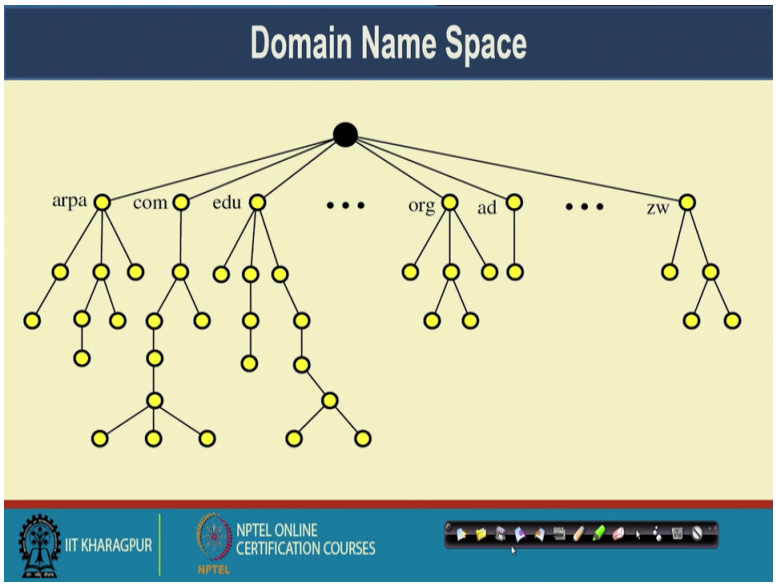
So, routers should be given data in form of IP only. So, I require somebody who can covert this name to IP that exactly the job of the primary job of DNS. DNS does some few more things that will see, but primarily it works on this resolving name to IP. So, there is a concept of domain and sub domains as a in a sense that how much I will cover my in my DNS. So, have suppose IIT Kharagpur DNS. So, what it its responsibility whether it will take care the iitkgp as its domain can have sub domain and so and so forth like we iitkgp dot ac dot in may be a domain cac dot iitkgp is ac dot in a sub domain on the things, and the type of the and there are concept of DNS servers which translate the domain name to the IP address.

So, one is that management of this distributed domain, another is that I require domain name server which we will transport which we will translate this domain name to IP address right. These two are the primarily one of the major activities of the things.

(Refer Slide Time: 03:36)

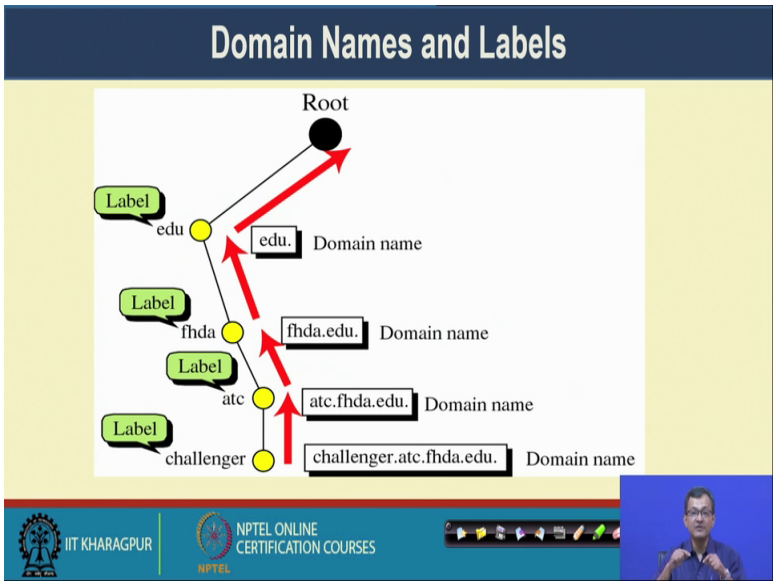
So, we have seen there are some of the Top Level Domains or what you say TLDs like com org net and so and so forth. Typically these top level domains are three character length and there are few country domains. There are rather for every country there is a country domain which are a two character length like in for India US, for US United States of America and CA for Canada and so and so forth. So, these are what we say top level domain; so or TLDs.

(Refer Slide Time: 04:16).



Now, if we like to see the domain name space right. So, the domain name space is something like that. So, we have some of the top level domains like arpa com edu org and so and so forth and then, under than I have sub domains like suppose in India. Under India there are ac under a c iitkgp under iitkgp cac. So, there is the overall domain name space right. So, that those domain name space need to be defined.

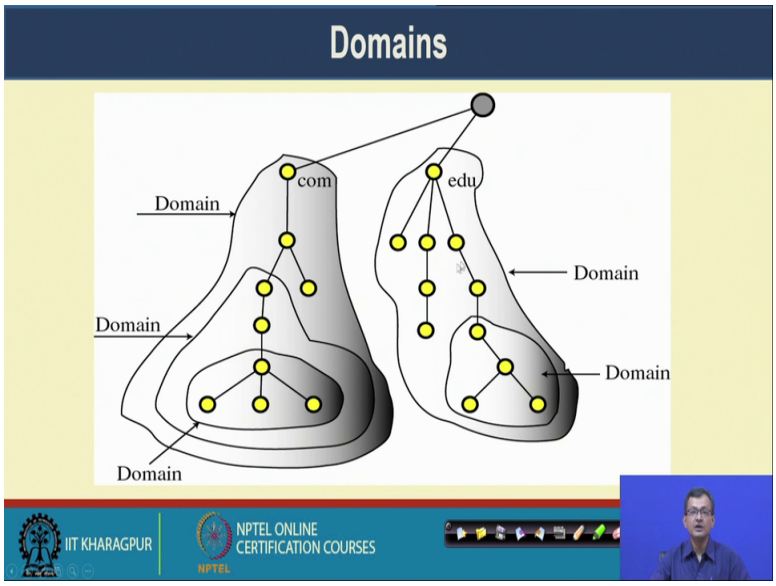
(Refer Slide Time: 04:52)



Now so, that above the TLD, we what we do or is the root domain. So, what we have say, if this is a typical example of say challenger or atc fhda dot edu. So, this is a overall domain name. So, if we go on this hierarchy. So, the next level is this one, next level is fhda dot edu and edu is the top level domain this dot indicates the root domain.

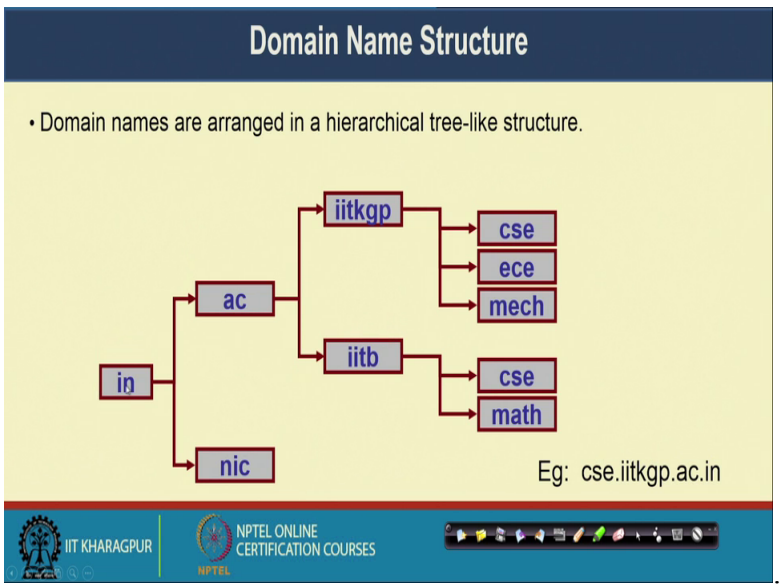
So, these are the top level domains, which are they are which is there. So, this typical example may be from (Refer Time: 05:34) books you can refer that, but nevertheless this is the hierarchy of the things. So, see the manageability of the name has been done in this way now at the level there is a IP address. So, I if I want to resolve if I want to go to this domain I need to resolve. So, there should be somebody will reserve as we know about this client server thing. So, say I give www dot iitkgp ac dot in in my browser. So, browser is a client or an http client which requires my DNS for a resolution right. So, give me the IP sort of things. So, the DNS resolve and send me back the IP address, you taking this IP address the less of the communication goes on. Intermediate routers and other devices understand the IP address right at the end it will be delivered to the destination IP address.

(Refer Slide Time: 06:31)



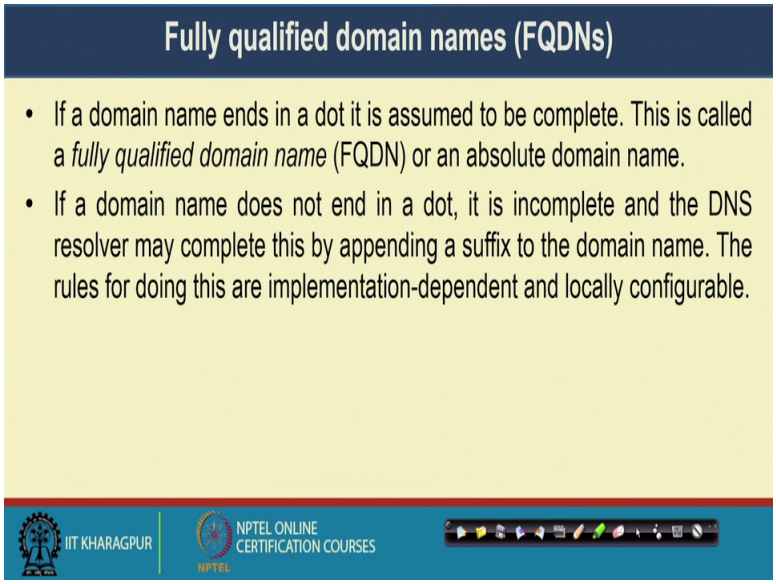
Now, if we look at these domains; so, this is a domain, this is a domain, this is a domain and there are difference. So, this dot com as the responsibility of the thing and if we are if it is having another intermediate thing, then it has to go for other domains to look at and so and so forth right. So, every domain server or the DNS server have some record of what it is under that right that we will see that we call that it has a resource record. So, what are the resources it is having right. So, it has or we it has some sort of a control authority of the domain. It can have sub domain it delicate that thing to things right and go so and so forth. Similarly, here also in the edu case we see this one.

(Refer Slide Time: 07:25)



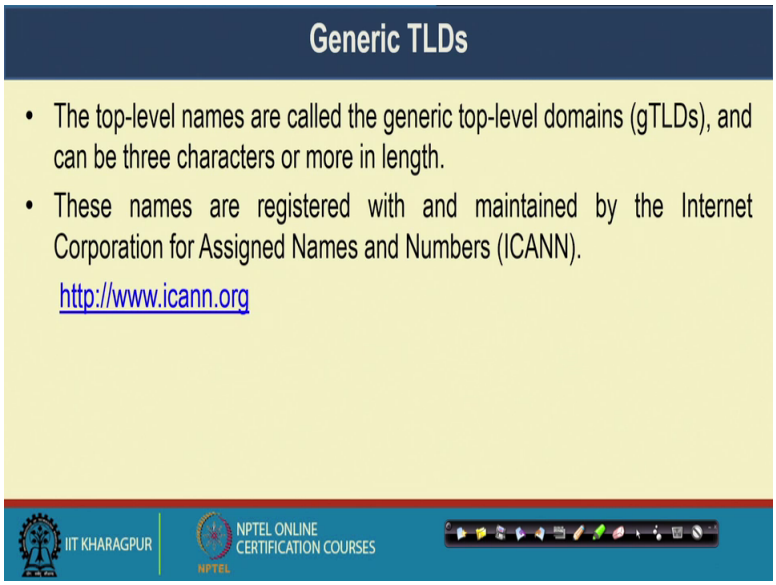
So, like if I have cse dot iitkgp ac dot in, then in ac iitkgp cse like this is a top level domain country domain and we above this is the root domain dot which is dot. So, domain names are arranged in a hierarchical tree like structure. So, see I can have multiple cse at some level, they are also cse iit b also have a cse, but the overall thing will not disturbed right. So, individually iitkgp only if you look at the cse, so that may clash right every iit or every iit has a cse department and their domain names have cse and it will clash, but that is partially qualified or partially defined. But if I have fully qualified cse dot iitkgp ac dot in this will never will be duplicated so; that means, I can uniquely define that thing and uniquely define that IP address of the things.

(Refer Slide Time: 08:25)



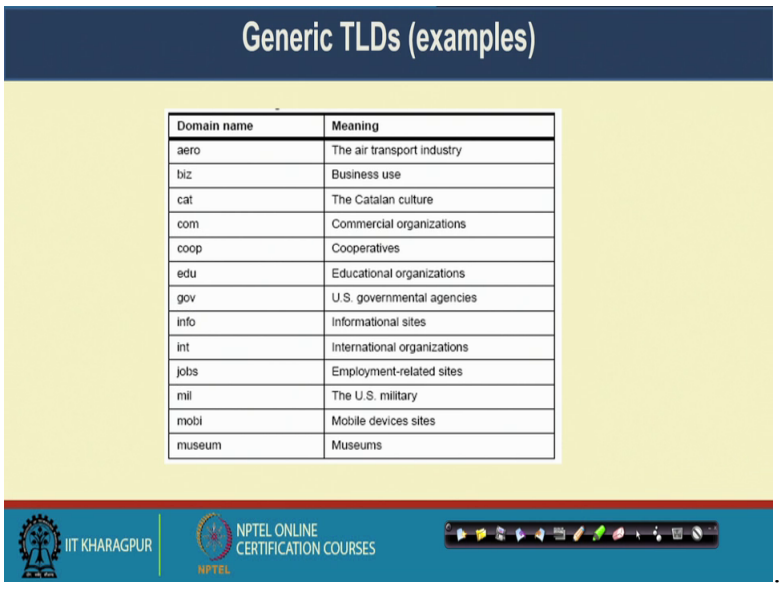
Now, that is why we have a fully qualified domain name that if a domain name ends with a dot it is assumed to be complete. This is called fully qualified domain name or FQDN or an absolute domain name right like it should be iitkgp cse dot iitkgp ac dot ac dot in dot so; that means, fully qualified. Only if I see only cse dot iitkgp, this is partially qualified; that means you require something to make it fully qualified. If a domain name does not end in a dot it is incomplete and the DNS resolver may complete these by appending a suffix to this domain. The rules for doing are implementation dependent and locally configurable. So, what how you will be there? So, DNS server can make it fully qualified before going to the other things

(Refer Slide Time: 09:16)



So, we have some generic TLDs as we are discussing that top level domains, top level domains are called generic TLDs or g TLD sometimes and can be three characters or more in length. So, there is a top level domain typically three characters or there are aero etcetera which is four characters. These names are registered with and maintained by what we say authoritative agency or vice what we can what we call and I can. So, these are top level domain, which has three plus three or more characters can be are defined by the ICANN.

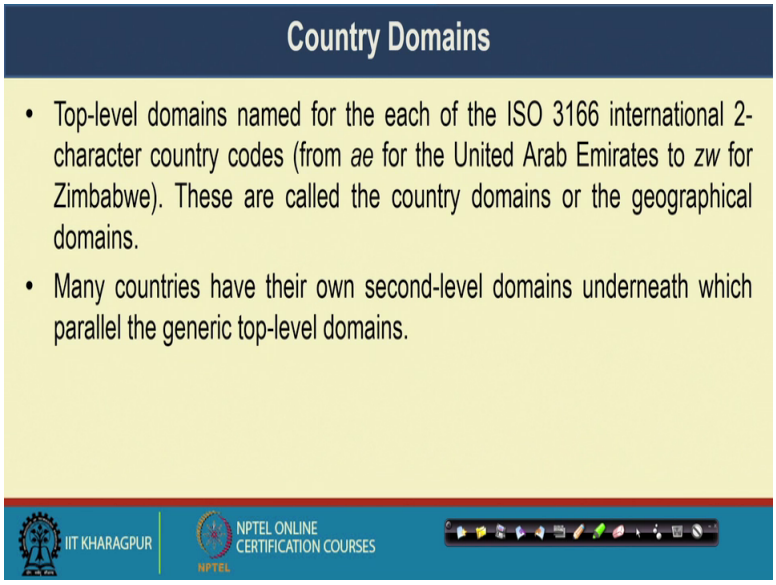
(Refer Slide Time: 09:54)



Domain name	Meaning
aero	The air transport industry
biz	Business use
cat	The Catalan culture
com	Commercial organizations
coop	Cooperatives
edu	Educational organizations
gov	U.S. governmental agencies
info	Informational sites
int	International organizations
jobs	Employment-related sites
mil	The U.S. military
mobi	Mobile devices sites
museum	Museums

Now, this are some of the examples of top level domains are aero biz etcetera that is minimum three character even there is a top level domain called museum which is much more than that.

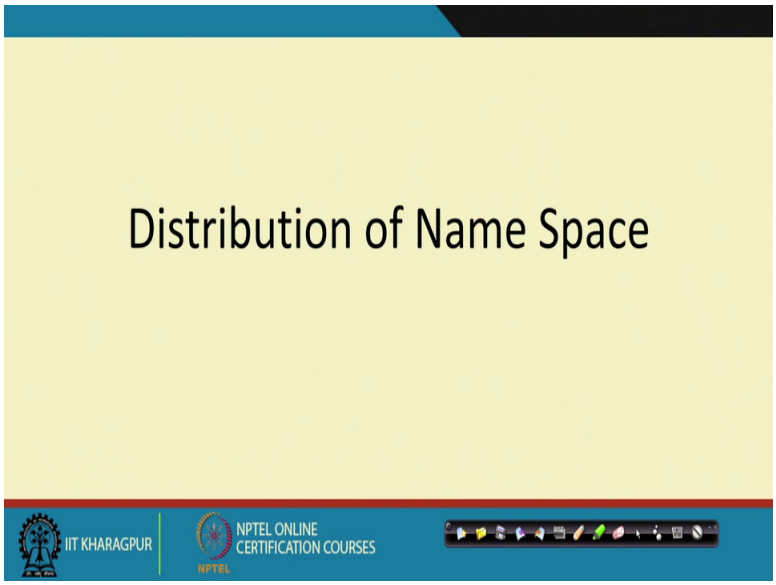
(Refer Slide Time: 10:04)



There is a concept of country domain, top level domains named for each of the ISO 3166 international two character country codes.

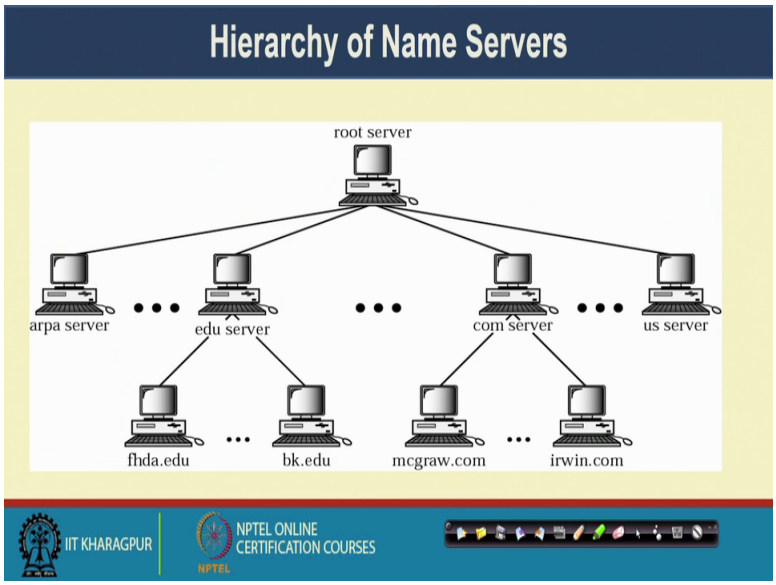
So, that everybody has a things like a e for United Arabs I n for India a u for Australia and so, these are the country domain or the geographical domain. So, it is country specific many countries have their own second level domain underneath the parallel which parallel the generic domain name this top level domain right like what we say like ac dot in right. So, there can be ac dot or what we say co dot in. So, there can be some other domain where that is co dot say something edu is could can be there right or something. So, what we have a iitlkgp dot ac dot in these are underneath that in domain.

(Refer Slide Time: 11:04)



Now, this distribution of domain space right.

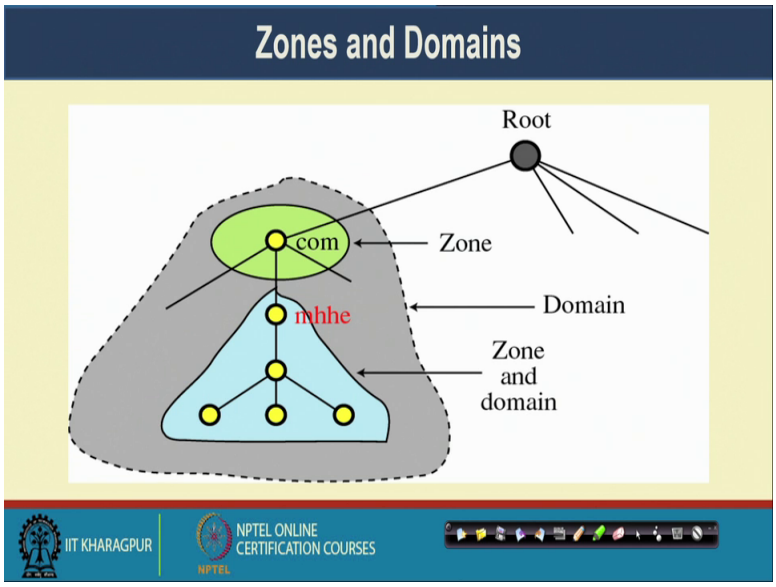
(Refer Slide Time: 11:09)



So, if I if we see. So, if the root server primarily understands the top level domains. Now t if there is any resolution, it will go to that next level domains. Say if there is a request coming from something dot com or something that edu, it will send it to the next level server which resolves the next level things. So, every domain server has their particular authoritative zone, where it keeps the information records regarding that zone right. So, while resolution it helps in doing that.

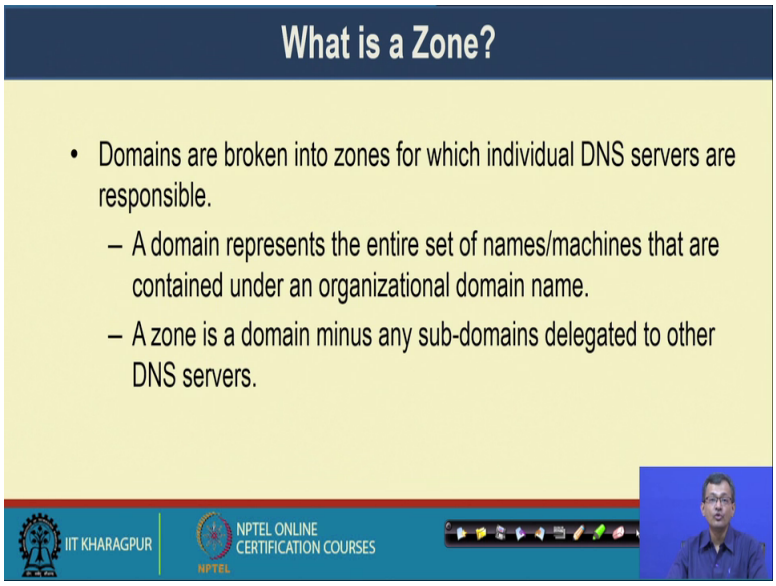
Now this hierarchical structure allows me to expand or add delete update type of things right. So, if there is a update in say somewhere bk dot edu so, that that is server or edu dot server understands. So, the root server sends it to that right. So, it depends on where like iitkgp tomorrow opens up a new domain it basically put it into its own resource record of iitkgp ac dot in domain name server, which in turn are resolved when a request for that particular sub domain comes into play.

(Refer Slide Time: 12:27).



So; that means, we have zone and domain. So, this is a domain. So, there is one zone this is zone and domain in the same so; that means, it takes care of that where the authoritative is there. So, the data for which it has the authoritative. So, it its responses with a no authoritative tensor or it responses with a non authority, it get it if it gets update from somebody other domain. So, what is a zone?

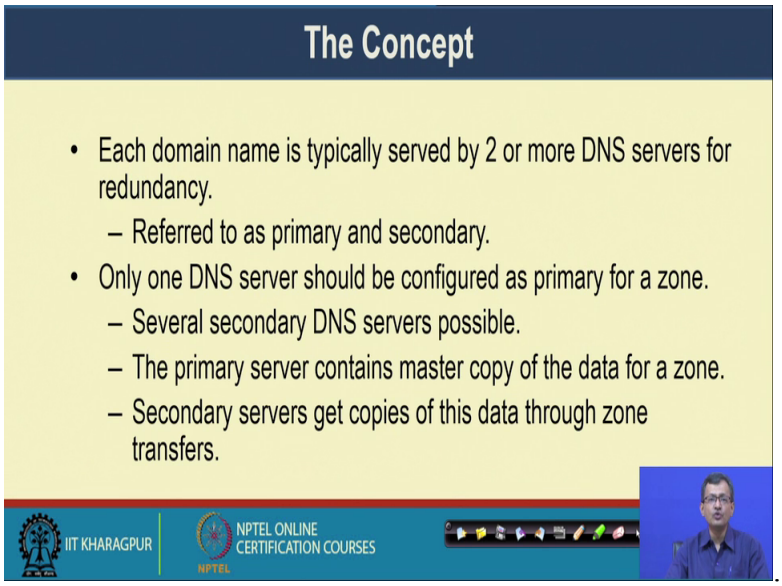
(Refer Slide Time: 12:54).



Domains are broken into zone for which individual DNS server are responsible. So, a particular domain is broken into zone for which individual DNS servers are responsible. A domain represents the interstate of names and machines that are contained under an organisational domain name

So, a domain represents the interstate of name like iitkgp ac dot in. So, it takes care of the interstate of name and machines or names versus IP address that are within that particular domain a zone is a domain minus the sub domain delicates into the other things. So, it has delegated at the server like ac dot in domain as delectated that iitkgp relate it to the iitkgp dot ac dot in. So, that domain of that particular ac dot in is restricted to the things, which excludes it is like minus those or excluding those sub domain delegated to other DNS server if at all.

(Refer Slide Time: 13:57)

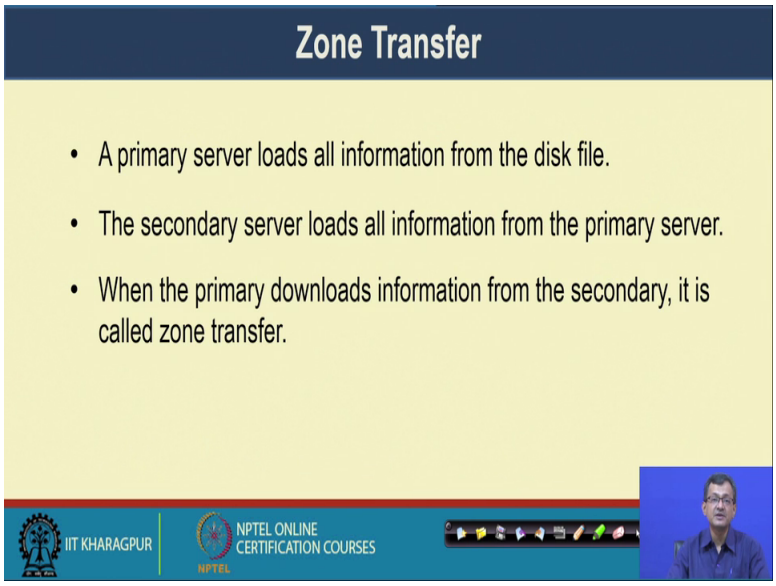


So, conceptually is domain name is typically served by two or more DNS server for redundancy.

So, if there is a failure of one DNS other should be able to resolve. So, again the resolving means primarily mapping from name to IP. So, if the one of the server face the other server takes up the responsibility. Only one DNS servers should be configured as primary of a zone. The primary server contains the master copy of the data of the zone; secondary servers can get copies of the data through a zone transfer. So, that is a intermediate things, which goes on to the zone transfer and goes on for this sort of update to the secondary servers right.

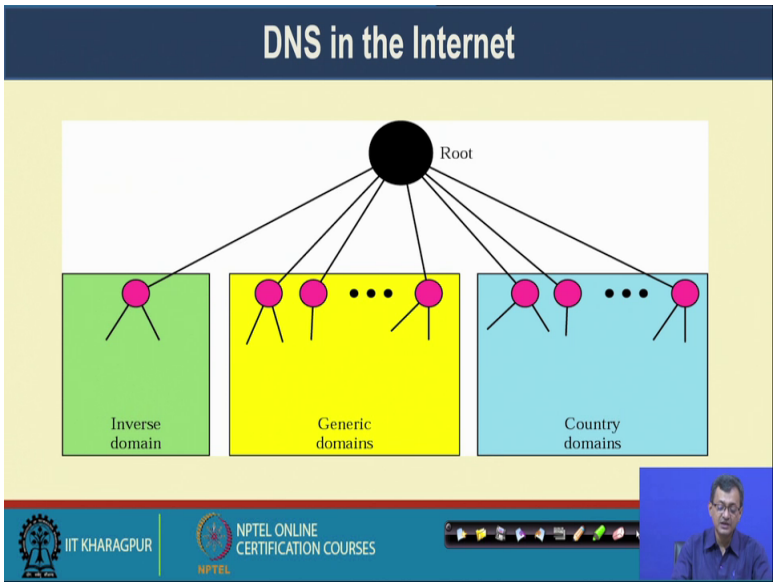
So, there can be one or more secondary server. So but nevertheless the master recorder is with the things and this secondary server get synched or transfer of zone from the primary to secondary.

(Refer Slide Time: 14:53).



Zone transfer a primary server loads all the information from the disc, the secondary server loads all information from the primary server, when the primary downloads information from the secondary it is called zone transfer. So, it is required that zone transferring there is a need like that DNS in the uf role of DNS in the internet working or DNS in the internet.

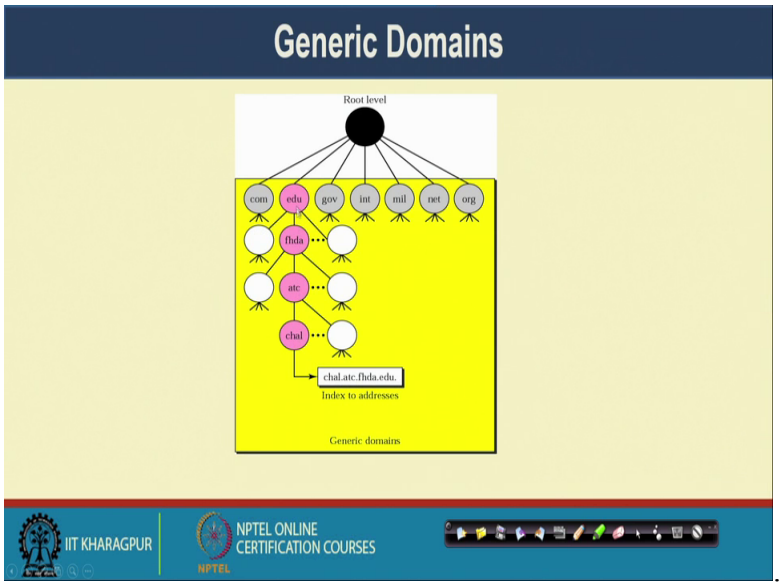
(Refer Slide Time: 15:19).



So, there are three categories as we have seen generic domain and country domain. One is three or more and one is two character, a two character length; now there is a third

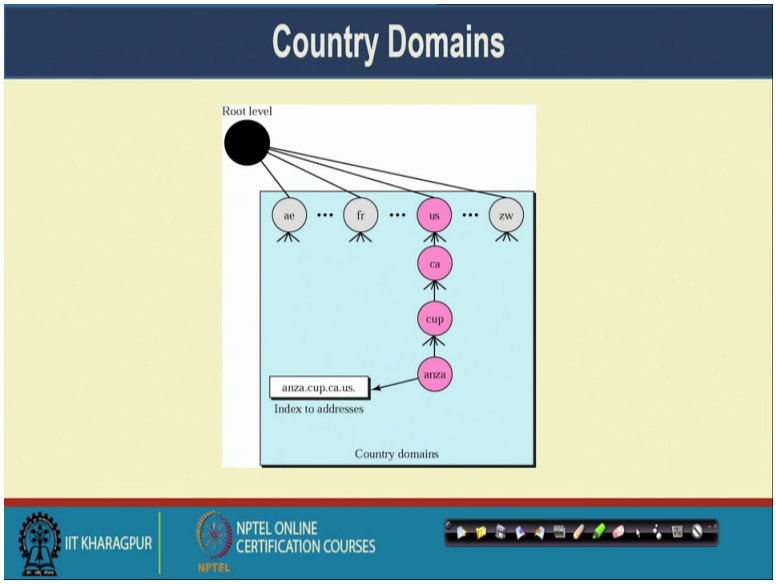
category called inverse domain or reveres domain right. So, that is these are all domain name to IP. If there is a inverse is required name to a number IP to domain, then we have a inverse domain data base right or inverse domain server which is which does a inverse domain resolution.

(Refer Slide Time: 16:00)



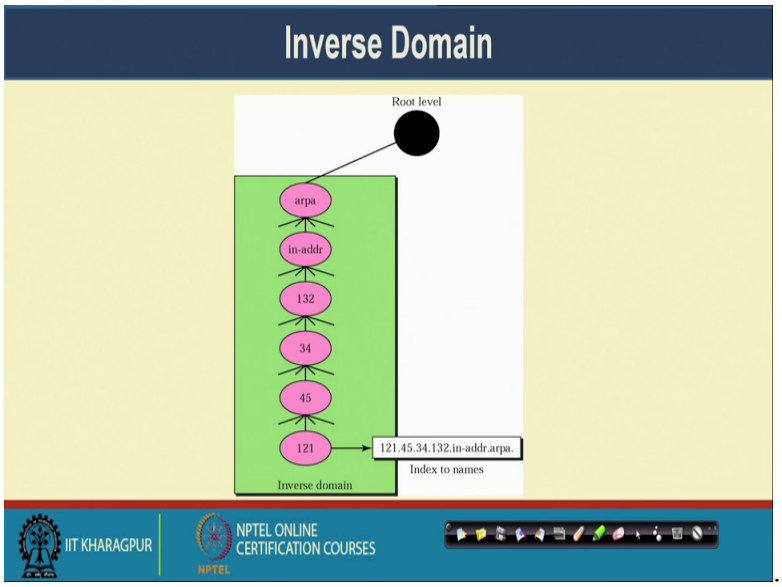
Like for generic domain like in this chal dot atc dot fhda dot edu. So, in this path it is defined. So, it is chal atc fhda dot edu dot chal atc fhda edu dot right similarly any other paths will be defined.

(Refer Slide Time: 16:22)



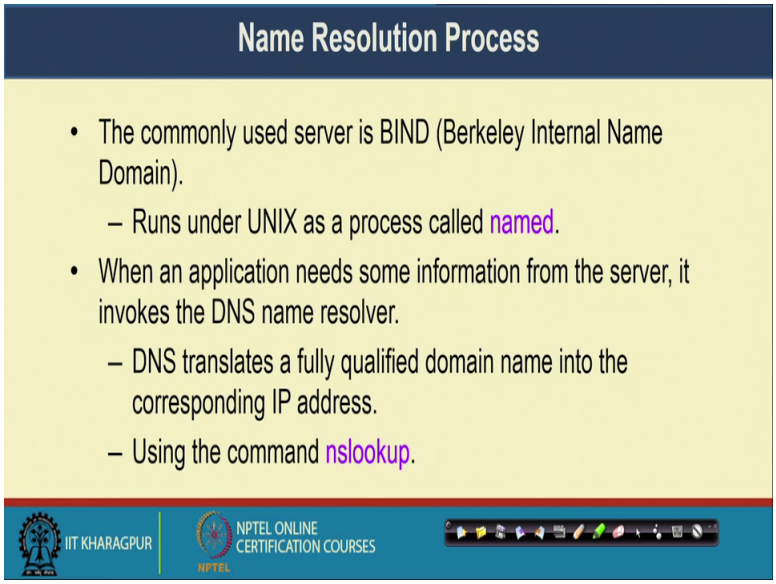
So, for country domain like here also the paths are defined like that.

(Refer Slide Time: 16:31)



For inverse domain if it is IP to this. So, the IP and IP this basically this server is in addr dot arpa dot net arpa in addr dot arpa and the IP it is written in reverse way. So, 132 34 45 121 is written here that 121 45 34th 132 in addr an arpa dot net. So, the IP representation in a inverse way this inverse resolution right. So, it is if the IP there it they it basically sends back the name of the things, usually we have we all primarily we have forward resolution this is a inverse resolution.

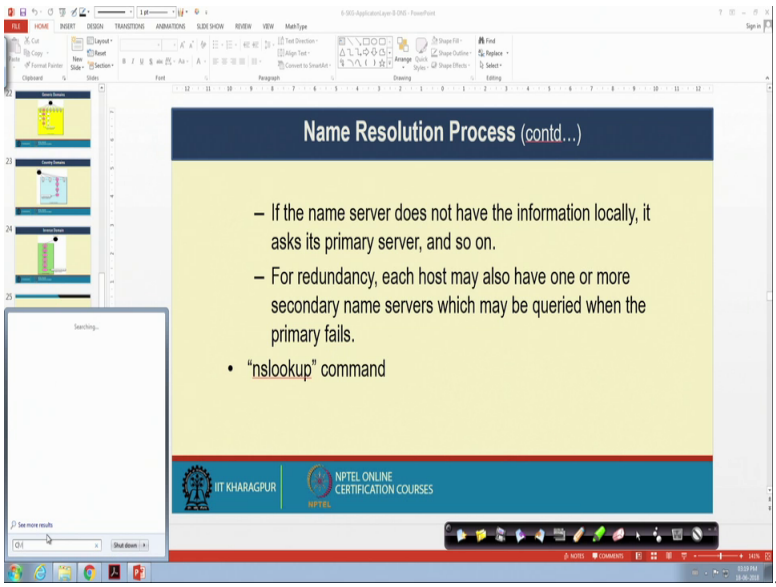
(Refer Slide Time: 17:25)



Name resolution the commonly used server is BIND that is Berkeley Internal Name Domain runs under UNIX or Linux as a process and called named so; that means, named is the demon which is the DNS demon.

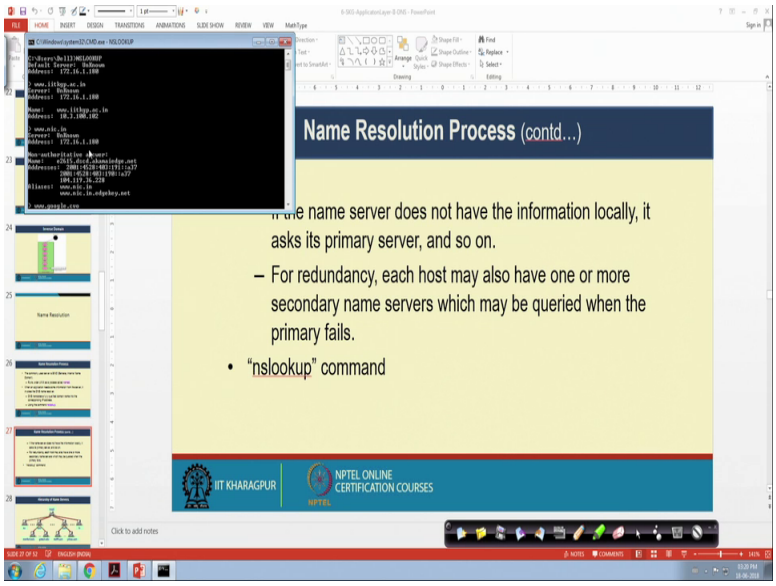
When application needs some information from the user, it invokes DNS name resolution resolver. So, it resolve the name, the DNS translate a fully qualified domain name into a corresponding IP address using the command called nslookup. So, when you give nslookup, then it is resolved into the particular com particular resolution.

(Refer Slide Time: 18:13)



You can pretty easily use any command from this one. So, if the name of the server does not have an information locally, it asks the primary server and so on for the redundancy each host may also have one or more secondary name server which may be queried when the primary fails.

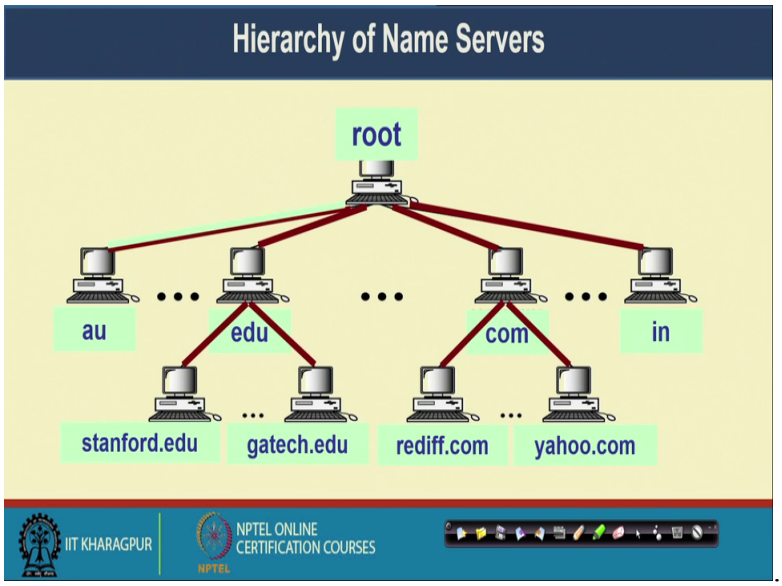
(Refer Slide Time: 18:44).



So, there is a command in nslookup. We can have a quick look into the thing so that it will be say, cmd if I give hopefully the ns sorry nslookup. Suppose I give www dot first of all a iitkgp dot ac dot in, it will resolves the returns the IP address as I am a local d accessing it. So, it gives me the local IP address. Suppose I give some other things like www dot say something like nic dot in.

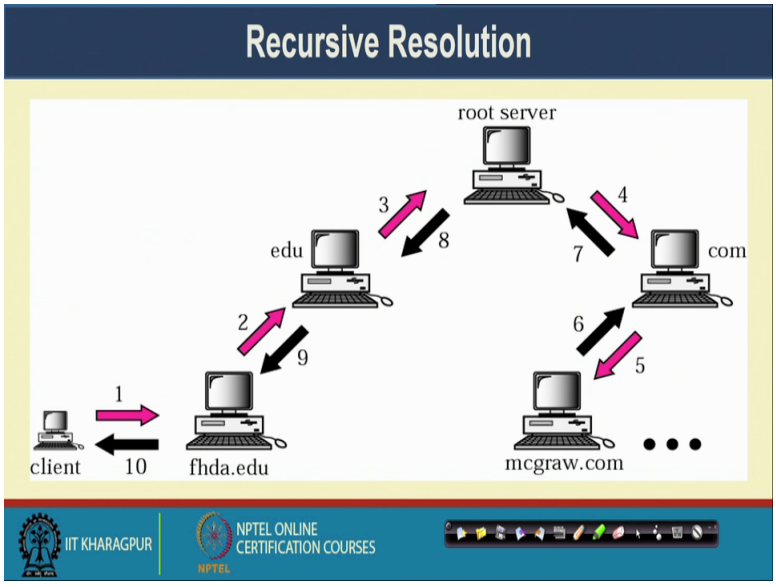
So, I get a resolution for that whatever it is showing is the IP, similarly www say Google dot com. So, it is all there Google IP as 216 dot this. So, this type of what it is doing? It is asking the DNS server give me the names. So, it is some sort of a resolution process which is going on right.

(Refer Slide Time: 19:58)



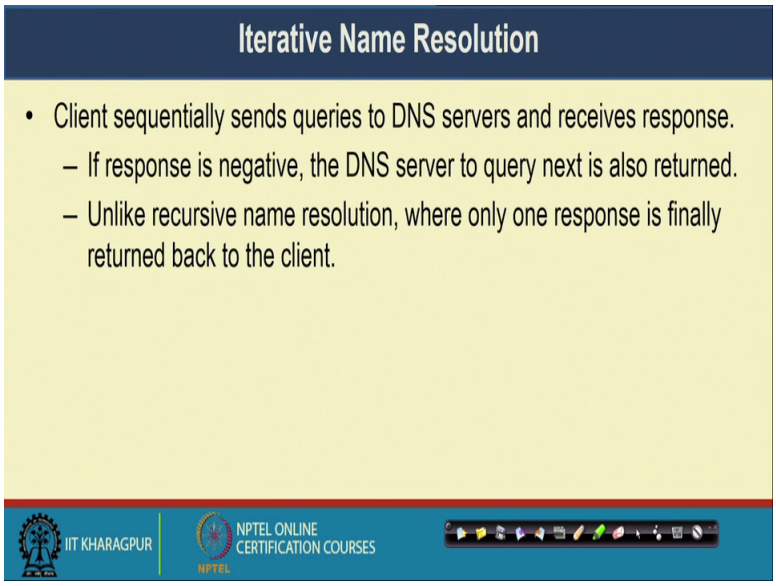
So, this is the hierarchy as we have seen of the domain names.

(Refer Slide Time: 20:04).



And if the resolution goes on so, there can be recursive resolution name servers asks to a edu that what it wants to resolve a particular client and that fhda. So, it go on resolving it request goes on the things and resolving in a recursive way. So, it go on recursing one in server asks the next and go on recursive way.

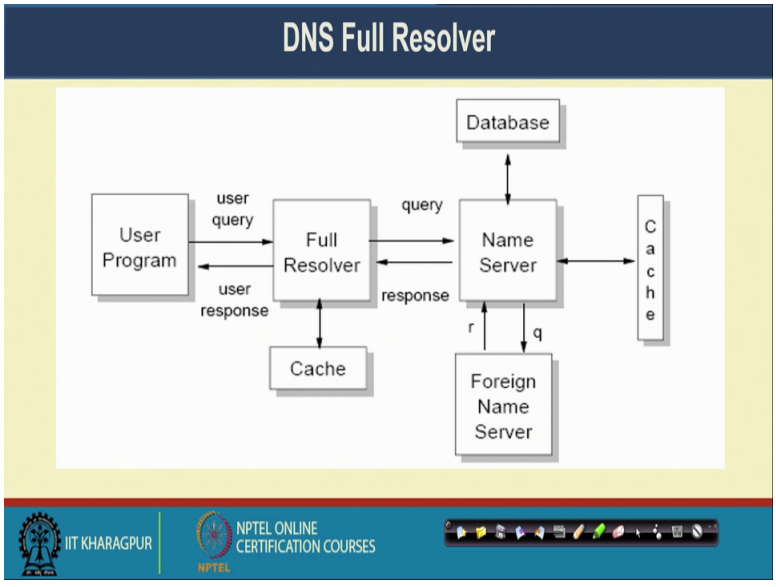
(Refer Slide Time: 20:25).



Or it can be iterative client subsequently send queries to the DNS server and receive the resolution; if responses is negative DNS server to query the next is also returned.

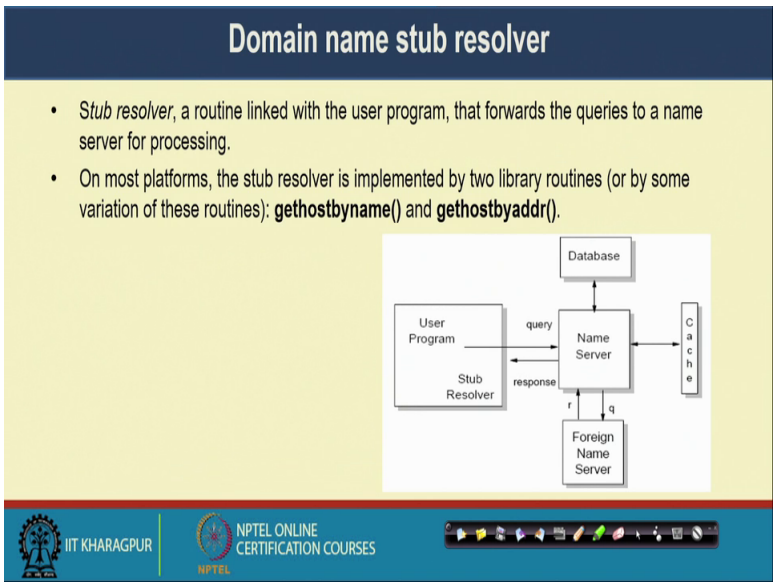
So, if it is not having, it returns that where DNS to be queried unlike recursive solution here where only one response is the final written by the things. So, in the recursive that itself recurs to the other, in case of iterative it sends that if it is not having sends the next I that address of the next DNS server. So, it is some sort of what we are discussing as the recursive resolution.

(Refer Slide Time: 21:04)



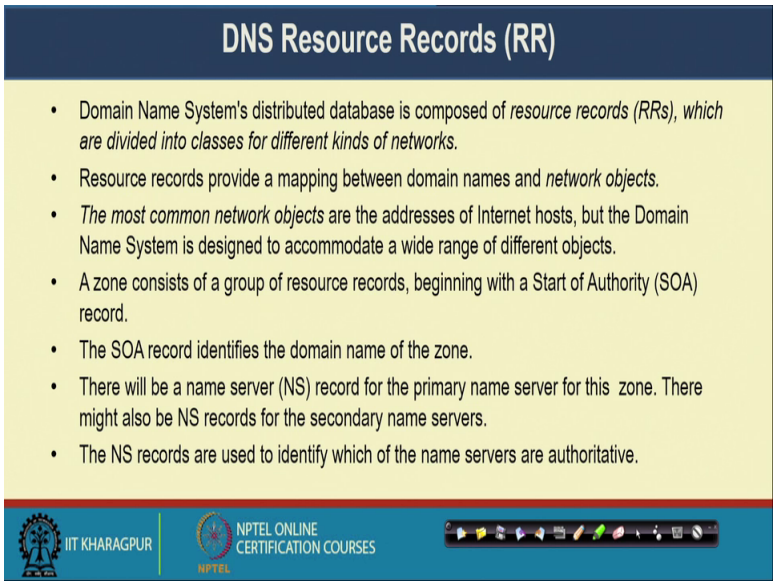
Now, they are if there are if I want to resolve a particular DNS, if you look at the DNS resolution or resolver point of I use a programs send a query user query to the full resolver. It interns send to the name server, it get resolved response and internet give the user response right. The DNS the full resolver maintenance a cache by which it remembers that what is the mapping. So, that it does it next time much faster where as the name server has a if it is has a own database and cache and if it is not having it goes to it send it to the other name server foreign name server right. This is a full resolution so, the user program in turn send to the full resolution and get it done.

(Refer Slide Time: 21:57)



There is another resolver, which is pretty popular that is a called another way of resolver that is a stub resolver. The stub resolver as a routine linked the user program that forwards queries to a name server for processing. So, it is a routine attached with that process itself. So, on most platform the stub resolver is implemented by two library routines or some variation of this like gethost by name is the routine, most of the Linux is tends supports it and gethost by address is another routine. So, in this case the resolver is embedded in the user programmed unlike that full resolver and then it goes on directly hitting to the name server. So, it is much faster and popular and mostly used DNS.

(Refer Slide Time: 22:50).



Now, let us come to the DNS messages right or also we called the DNS there is a concept of DNS resource records before going to that messages types. So, domain name systems distributed data base is composed of resource record RRs which are divided into classes for different kind of networks right.

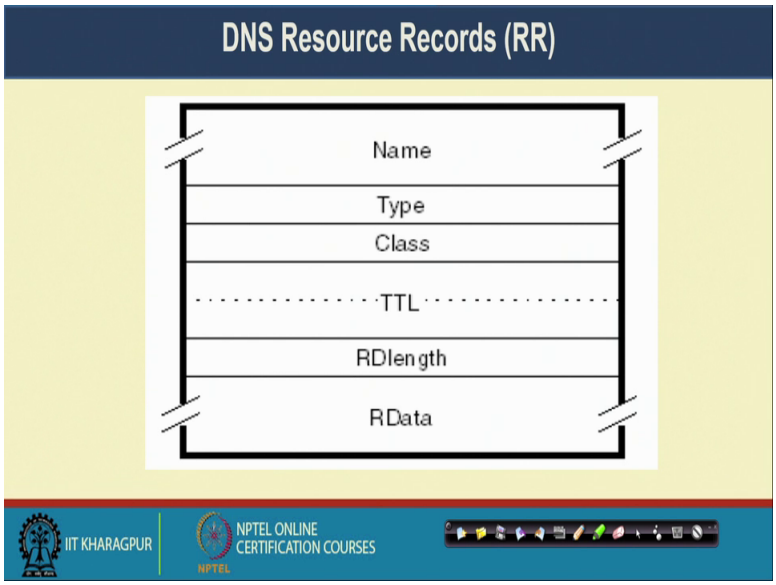
So, this is the thing resource record provide a mapping between the domain name and the network objects right. So, the domain name and the network objects are given in mapping; that is interestingly if you see say iitkgp ac dot. It can be a domain it can be a domain server it also can be a http server or I can have a FTP server over there. So, that that is a record we says based on that mapping that what sort of request I can map to that particular network object.

The most common network objects are the address is of the internet host, but the domain name is designed to accommodate a wide range of different object so; that means, it is not only the host IPs, but is something much more than that. So, it is a onset of resource records right.

So, a zone consists of a group of resource record beginning with a start of authority SOA of the record. So, it is a particular zone as a a group resource record, but it starts with the start of authoritative right. There will be a name server NS record ns record for the primary name server for this zone there may be also NS record for the secondary name servers right. So, there is a there can be ns record for the primary and secondary. The NS

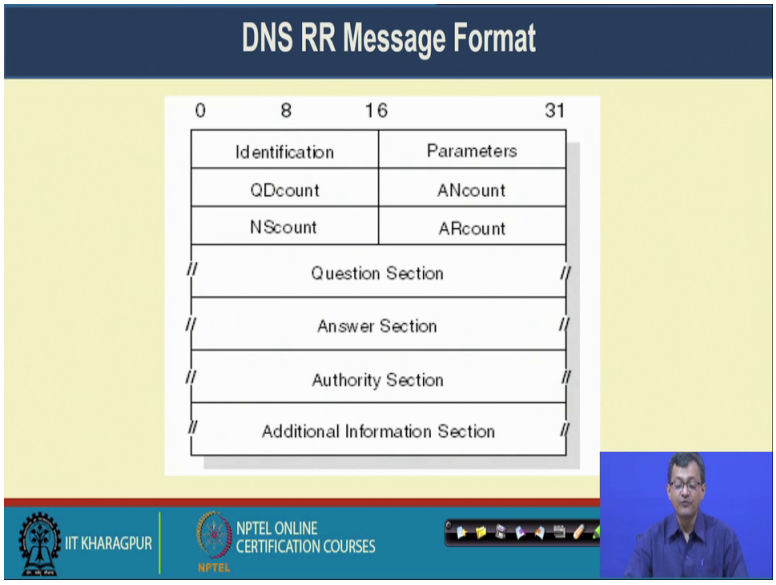
records are used to identify which of the name server are authoritative. It is whether it is authoritative or non authoritative determine by this in its record. So, that whether it is itself maintaining it ha s a authoritative of thing or it is basically updated from somebody some other name server.

(Refer Slide Time: 24:57).



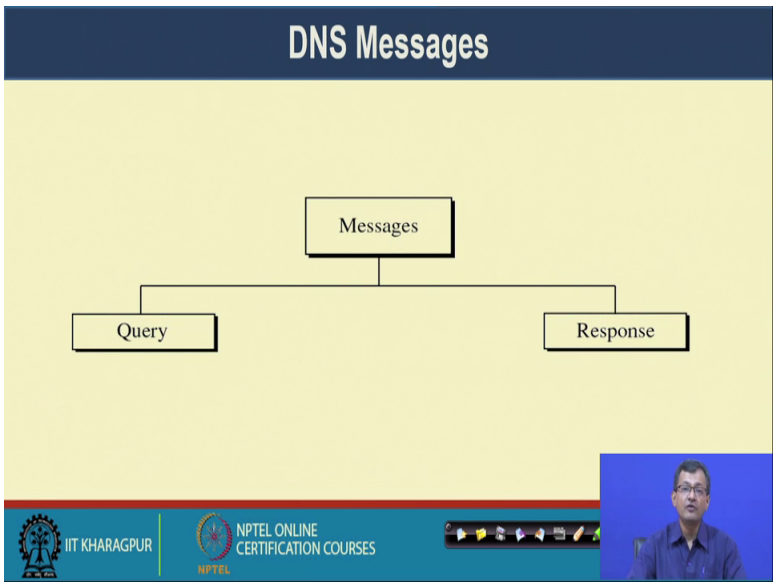
So, typical structure of this resource record we will see some example name type class TTL time to leave and rd record RDlength R data. So, these are the typical structure of the resource record.

(Refer Slide Time: 25:13)



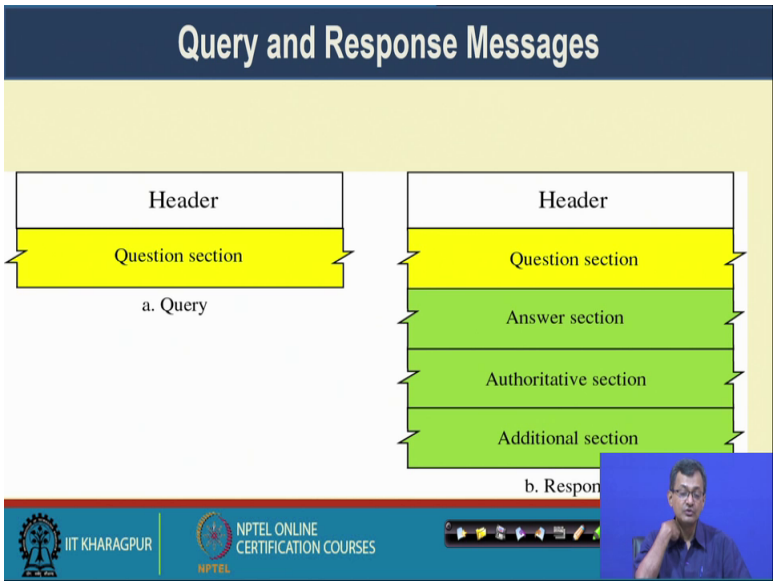
This is a typical format of a RR message format where some identification is required parameter query count answer count a total number of NScount and ARcount right. So, these are record count. So, that we have the questions section and answers section authority section and additional information. So, this compromise is a RR message format. So, whenever this RR message is being exchanged. So, these are the things which are which are used for when we do. So, this this format goes on; that means, the DNS clients are severs or DNS zone transfers the this is a standard which is follows to the everybody understands the other message.

(Refer Slide Time: 26:06).



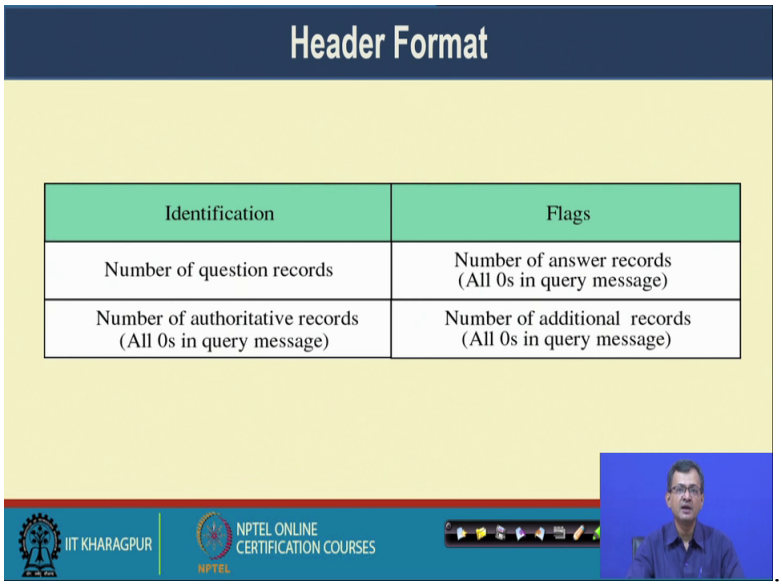
DNS message is typically of two things one is query another is response right. So, query response type of thing.

(Refer Slide Time: 26:13).



So, the query as a header and question section where as the response is having a header question section answer section or reduce section and additional section. So, this is the response is goes on the thing.

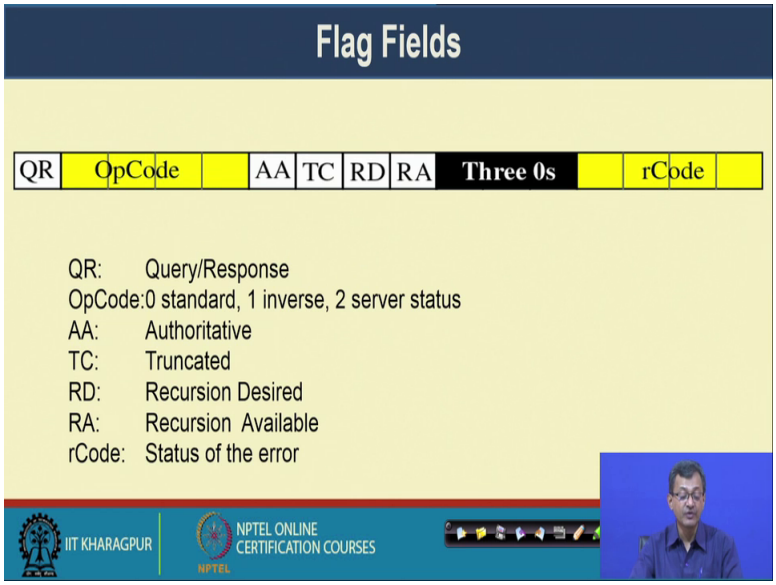
(Refer Slide Time: 26:31)



So, there is in the header format there is a two thing is identification and flags, along with the number of question records it is send number of answer records all 0s because there is no answer recording the query. So, it is all 0s in the query message number authoritative records, again all 0s in the query message number of additional records all

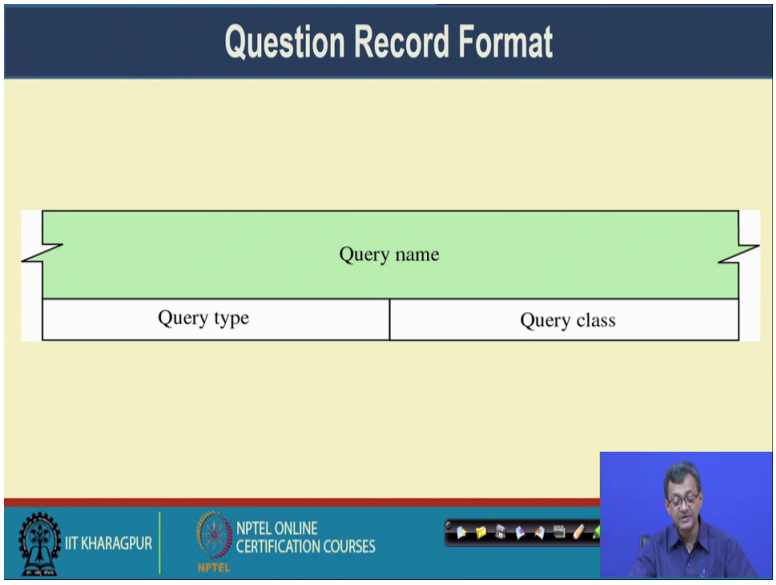
0s in the query message. And there is a flag field if you just recollect. So, there is a flag fields we just see that one.

(Refer Slide Time: 27:04).



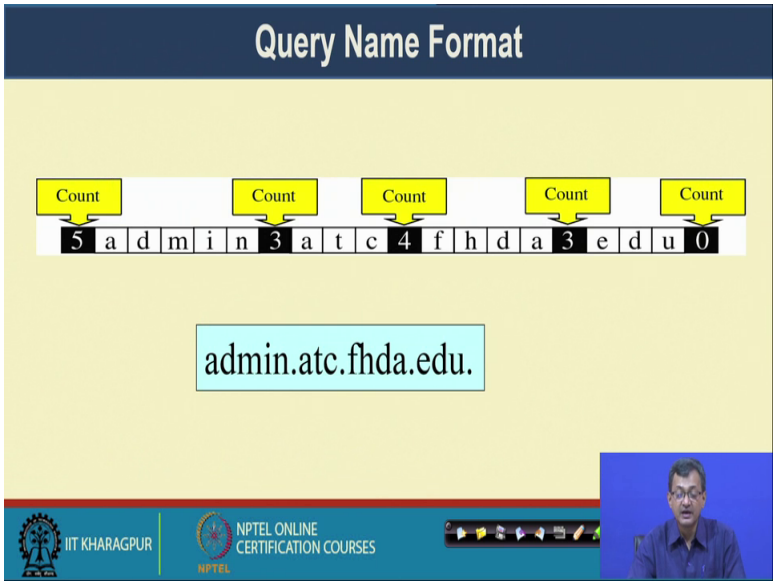
That is QR there is whether is a it indicates whether is a query or response OpCode 0 for standard inverse or server status. So, that is the operational code it is a standard manager is name to IP, IP to name is inverse and then service status. If it is authority then this AA flag is on TC is whether it is truncated of the full recordation RD is the recursive recursion desired RA is the recursion available and R code is the status of the error.

(Refer Slide Time: 27:47)



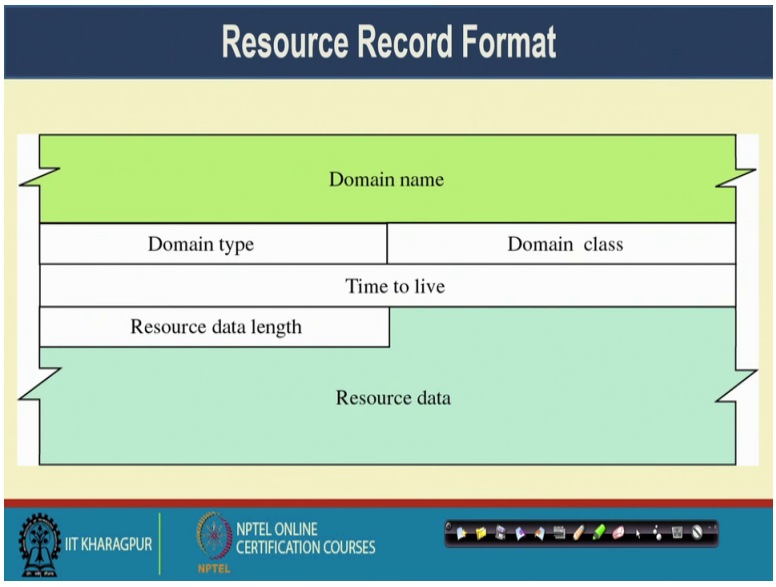
So, these are the different formats of this flag fields and the type of records as we mentioned there is a record, one is the query name, query type and query class like here.

(Refer Slide Time: 27:54).



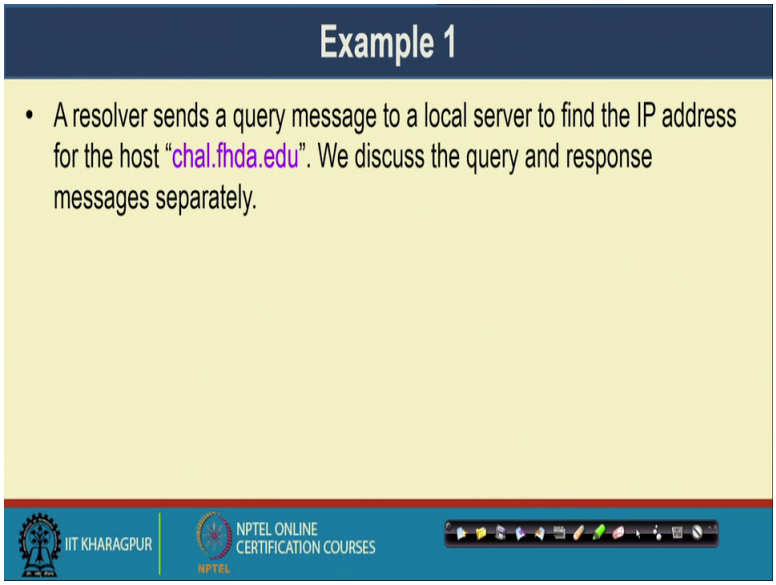
Ah Query name format suppose we want to have that admin dot atc dot fhda dot edu. So, it says that number of count 5; so, that admin 3 and so, and so forth. So, it says that these are the different names which are separated by dot by doing that; so, this is the query name format.

(Refer Slide Time: 28:19).



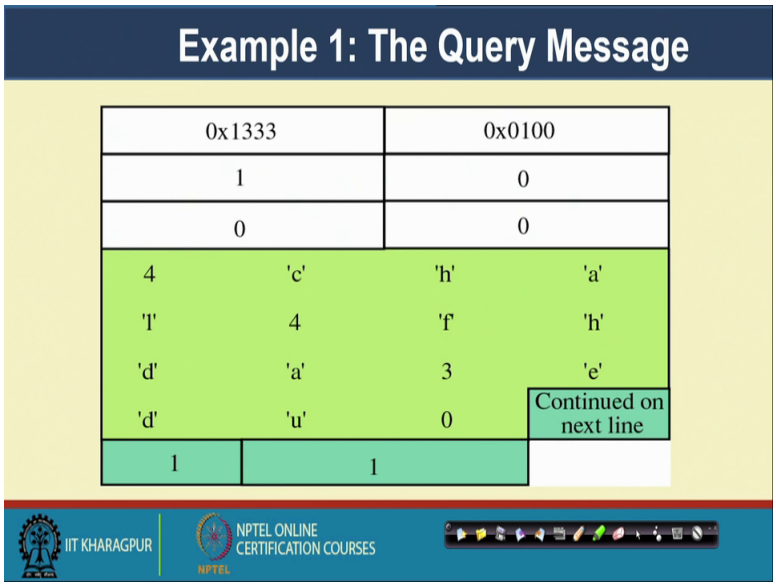
And resource record format we have seen already that domain name, domain type, domain class, time to leave, resource record, data length and the whole resource record.

(Refer Slide Time: 28:32).



So, we let us see one or two examples, a resolver wants to wants a query message to a local server to find the IP address of the chal dot fhda dot edu. We discuss the query and response separately. Let us discuss.

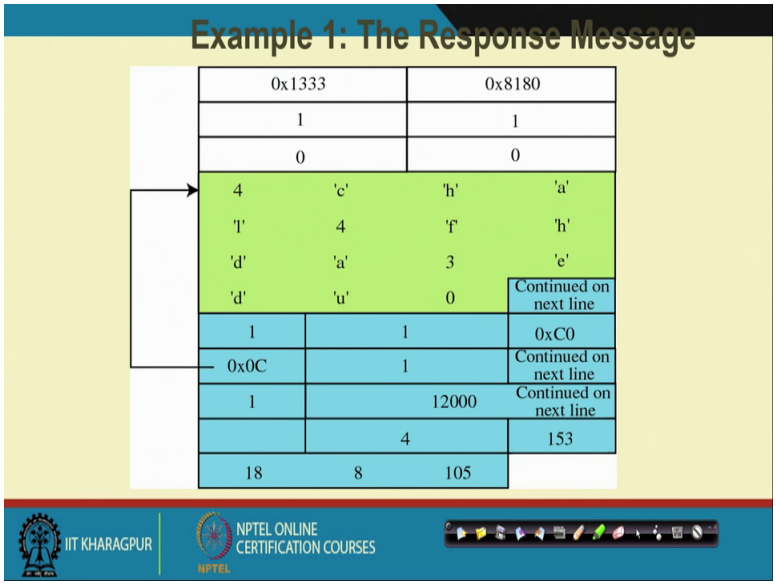
(Refer Slide Time: 28:52).



So, this is the typical format where you see that is encoded these are the different fields. So, you say query message and other things as 0 and this is c 4 c h d a c h a l, then again

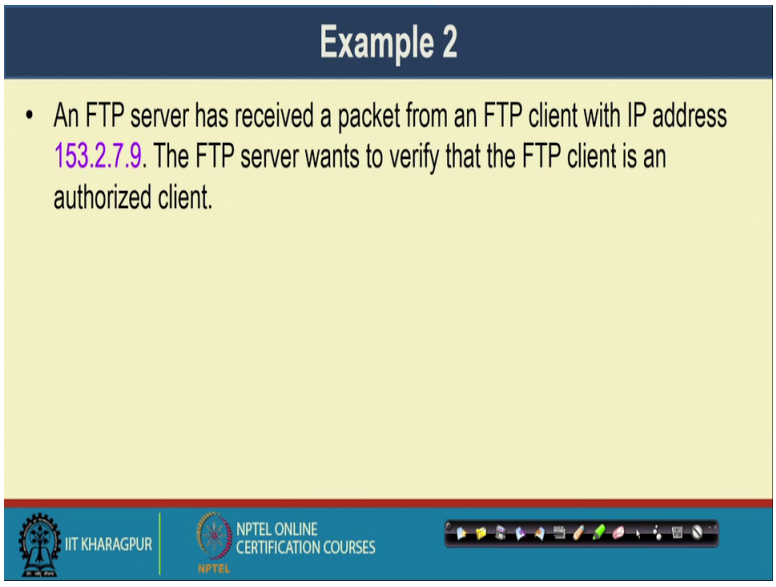
4 f h d a 3 e d u and 0; that means, that is the end of the things right. So, it has if it is a large record that continuing on the next line on node and so and so forth.

(Refer Slide Time: 29:25)



Similarly, example of a response is it query message is there and along with the response message is also there right. If you can check that particular IP is. So, it is 153 dot 18 dot 8 dot 105. So, it if the response message which is read by the system and it is the DNS is resolved.

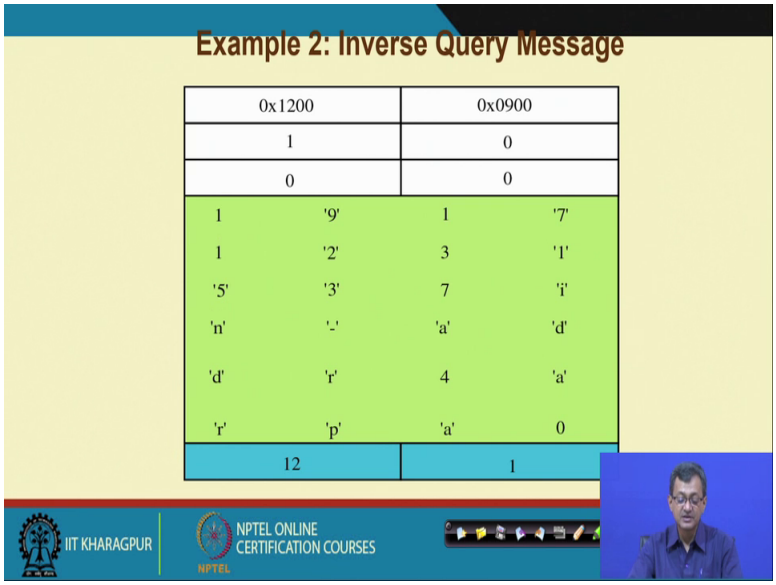
(Refer Slide Time: 29:53).



Similarly, example two an ftp server has received a packet from a ftp client, with IP address 153 dot 2 dot seventy nine dot nine 9. The ftp server wants to verify the ftp client is an authorised or not right.

So, it is getting a IP and now it wants to verify whether is authorised or not right. In other sense that it wants to know that particular which domain he has this particular IP right. So, this is the ftp server wants to the ftp client has requested and ftp server wants to do that.

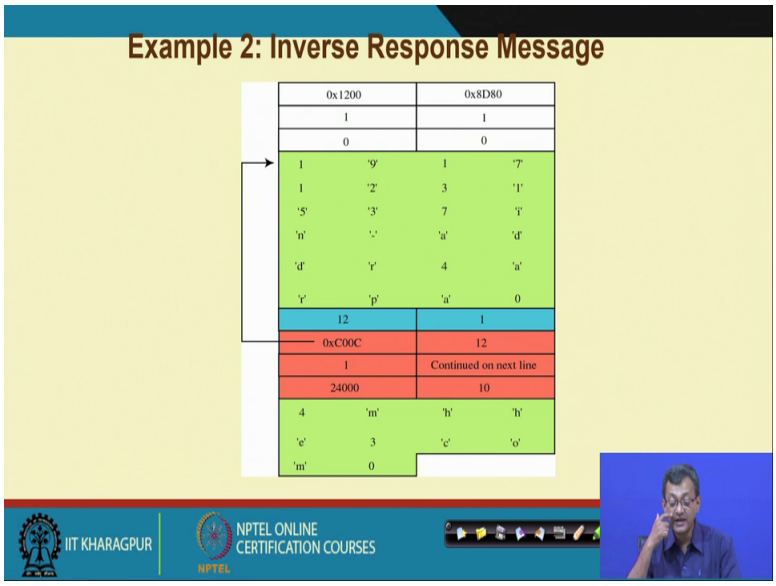
(Refer Slide Time: 30:35).



So, it is a reverse query message. So, it goes on if you if you look at there is arpa dot this is r d d a arpa dot addr slash dash in dot the IP in a other way around right.

So, if I have 9 dot s7 dot 2 dot 153. So, here 9 dot 7 dot 2 dot 153 dot I in minus addr dot arpa right. So, this is the way it resolve and inverse response file is return the particular name of the thing which is return it is m h h e dot com is the name of the particular domain.

(Refer Slide Time: 31:28).



So, why we required this? The ftp site server wants to authenticate or wants to know that whether the IP where from it is getting a request for a file transfer request or ftp request, then whether that is an authorised or not and it does as a reverse domain resolution ok.

So, what we see over all? That domain resolution is primarily for IP to a sorry domain name a name to IP and it is easier to remember name then IP. So, that any anywhere we use the name if it is if the request is going across the internet it has need to be resolved.

So, the domain resolver that every particular domain sub domain can have will have a DNS server, which basically resolve this when the request go to the DNS query it resolve it right and it goes it sends back the resulting. There is a concept of reinverse DNS where if you give the IP it returns that domain of the things, it may be required for authenticate or see the authority of a particular domain. So, with this, let us conclude our discussion today we will continue on this particular topic or basically on application layer for one or two more lectures.

Thank you.