

# Analytical Study of Domain Name System, its disputes and legal issues

**Prof. Vandana . Narvade. Kadam**

Dept. of Information technology,  
The Kelkars Education Trust's V.G. Vaze College of Commerce, Arts and Science, Mulund (E),  
Mumbai- 4000 81, India.  
v7n8s6@gmail.com.

*Abstract*— This research paper presents detail study and analysis of the domain names, domain name system, domain name disputes, and its dispute resolution procedures in brief. In this research paper, the analysis of world wide various domain name registrars, domain name root servers, domain name registries are presented by collecting data from Internet Corporation for Assigned Names and Numbers corporation's website, and continent-wise statistical report is prepared. The technical control and administration of domain name system as a whole is identified. Various disputes and legal issues related to domain names are also studied.

The preliminary results of this work is that, more than seventy five percent of domain name system is operated, administered and managed under the control of United States. And India's participation in domain name system is not even noticeable.

The DNS disputes and issues are identified. And to control the domain name disputes, its disputes resolution procedures, domain name registration procedures needs to be made more stringent with a global involvement.

By using simple probe tool method to measure the response time of the root servers from various locations around the world, results that regions in Oceania, Africa, South America and part of Asia are under-served by the current root servers. [1] In such scenario, applying First Come and First Serve policy [2] for domain name registration is unfair and not reliable for registrants from under served regions.

*Keywords*— Domain name system (DNS), Registrars, Registries, Root servers, Internet corporation for assigned names and numbers (ICANN), Internet's Assigned Number Authority(IANA), World Intellectual Property Organization (WIPO)

## I. INTRODUCTION

Domain names are names used to identify websites on the Internet. They are unique addresses of computers connected to the Internet. But the computers understands language of numbers, Technically, a typical Internet address appears as "120.11.23.55". These all-numeric form addresses are known as the IP addresses, as with IP addresses, domain names are also delimited with periods (dots), a typical domain name appears as www.google.com

The dominant purpose of the domain name is simply to provide an easy method for remembrance of another's electronic address. Domain name is a unique name used to identify, among other things, a specific web site. Domain names are nothing but proxies for the IP address, there is no logical correspondence between the IP address and the domain name

Since it is not possible to remember each and every numerical value of an IP address, the system of domain names evolved which is known as Domain name system (DNS). The DNS is used "to translate human friendly domain names in to its corresponding computer friendly IP address and vice-versa." The DNS has an involvement of central authority, registry system, registrars, root servers system; they are responsible for overall operation of DNS.

It is a perfect co-ordination system it is a distributed database of information that computers use to match domain names to IP addresses.

Any computers communicating on Internet, do not 'talk' in terms of domain names, but interpret a domain name into corresponding IP addresses. All servers on the Internet interpret the same domain names in same way. That is why when one types 'esselpropack.com', is taken to the web site hosted by Essel Propack (a company) irrespective of where the person accessing the data is located or which server he or she is connected to. It is essential for this reason that domain names are unique and therefore, similar domain names cannot be offered to two separate entities. The unique feature of domain names is that the said domain names are registered on

'first come, first serve' basis. This feature of domain names has given rise to domain name disputes like Cyber-squatting. Cyber-squatting is a form of speculation where a domain name is registered with the intention of selling off the same. It is a practice by means of which a person or legal entity books up the trade mark, business name or service mark of another as his own domain name for the purpose of holding on to it and thereafter selling the same domain name to other person for valuable premium and consideration. Usually, Cyber-squatters book up domain names of important brands in the hope of earning quick millions. For instance, the domain name 'www.microsoft.org' was available and was registered by Amit Mehrotra much before Microsoft Corporation could think of it. This led to numerous ticklish legal issues. Microsoft Corporation, despite of possessing the trademark Microsoft, could not get the domain name 'www.microsoft.org' because of the 'first come, first serve' criteria of domain name registration. The first reported Indian case is that of Yahoo! Inc. Versus Akash Arora. The plaintiff, who is the registered owner of the domain name 'yahoo.com', succeeded in obtaining an interim order restraining the defendant and his agents from dealing in service or goods on the Internet or otherwise under the domain name 'yahooindia.com' or any other trademark / domain name which is deceptively similar to the plaintiff's trademark, 'Yahoo!'.

There are conflicts between domain names and Trademark to put it simply, as the domain names are indeed different from trademarks. While it is possible that the same trademark may be registered by different persons in different categories and different lines of businesses, but in case of domain name it may be possible to register only one domain name corresponding to such trademark. This aspect of domain names has also led to legal problems.

Cyber-squatting occurs when domain names bearing a resemblance to famous trademarks are registered by persons, those hopes to sell the registration to corresponding trademark holder. Typically, in such cases, persons who have absolutely nothing to do with the name, virtually pirate the name by obtaining a second level domain name (SLD, like word 'Google' from 'google.com' ) registration with the '.com' top level domain name, TLD of a well-known company or brand. There are many other sensitive legal issues related to domain names which are concurrent claims for same domain name, passing-off of domain names, domain name verses trademark etc.

A global study of domain name disputes would show that they could be broadly classified under the following heads:

**Infringement-** This refers to a dispute where the original registrant intentionally trades off the resemblance between domain name and another famous trademark. Thereafter, the registrant tries to encash on the reputation of trademark holder by running a business similar to that of trademark holder. In such cases, the use of the mark (domain name) would be

illegal under the existing trademark law, regardless of whether the infringement occurred as an Internet domain name or in any other context.

The standard factors, which determine infringement under the traditional trademarks, law like: i. The strength of the trademark, ii. The deceptive similarity between the plaintiff's and the defendant's mark, iii. The likelihood of confusion in the minds of the public, etc., would apply in cases of infringement of domain names also.

**Concurrent claims-** In this category of domain name dispute, there is more than one legitimate user of the domain name. Apparently, there is no intention to trade off a trademarked name and little or no potential for confusion between the products of the conflicting claimants. Both parties have a particular trademark of their own or a valid reason to use a particular domain name. For example, both Moonlight Computers and Moonlight Dry Cleaners would be interested in registering the domain name 'moonlight.com'

The organization responsible for overall coordination and management of the DNS is the 'Internet assigned number authority' [Hereinafter to be referred as IANA]. In the United States today, the major part of the assignment of Domain Name is done by registry called as 'Network Solutions Inc [Hereinafter to be referred as NSI]. The world over the assignment and registration of domain names are carried out by registries called as 'Network Information Center' [Hereinafter to be referred as NIC]. However the most significant development in the world of Internet has been the establishment of non-profit organisation called as 'Internet Corporation for Assigned Names and Numbers' [Hereinafter to be referred as ICANN]. It is a global organization created in OCTOBER 1998 by a broad coalition of Internet's business, technical, academic and user communities. ICANN is assuming responsibility for a set of technical function previously performed under the U.S Government contracted by IANA and other groups. ICANN today is responsible for managing and coordinating the DNS to ensure 'Universal Resolvability'. To categorically state, the core ambit of ICANN's function is to develop and manage Internet policy and logistics related to (i) Internet Protocol (ii) IP address and (iii) Domain Names.

The assignment of Domain Names is carried out by the administrator, of a desired Top Level Domain [Hereinafter to be referred as TLD], who is authorized by ICANN, called as registrars. Application can be made electronically by means of online forms for the registration of domain name available with the respective TLD administrators. Only domain names which had previously not been assigned are open for assignment and every applicant must ensure that the domain name he or she seeks to register does not infringe any others trademark.

There is an international treaty organisation "World Intellectual property organizations" (WIPO), with more than 185 nation states as its members, undertook a series of consultations concerning the management of domain name system. Finally, in April 1999, WIPO issued its final report including its recommendations to ICANN (Internet Corporation for assigned names and numbers). Most of the WIPO recommendations were approved by the ICANN and have been incorporated in the current Uniform Domain Name Dispute Resolution Policy (UDNDRP), which has come into effect from 1st January 2000. The Uniform Domain Name Dispute Resolution Policy is the latest breathe of fresh air in the fight against cyber-squatting. Under the said Policy, a summary procedure is adopted to adjudicate the complaint of any complainant relating to any domain name on payment of processing fees. This policy is in operation. Under the said Policy, Indian companies have won back their legitimate domain names like 'www.theeconomictimes.com' and 'www.timesofindia.com' and even 'www.tata.org' and 'www.philipsindia.com' of TATA and Philips India respectively have won back their legitimate domain names under the said policy.

Disputes can be prevented through technical innovations as per one of statement made by International bureau in seminar organized by WIPO.

## II. METHODOLOGY USED

In this research work a study of domain names, domain name system and domain name disputes in detail and the dispute resolution procedures in brief. During this study, the analysis of world wide various domain name registrars, domain name root servers are done by collecting data from Internet and continent-wise statistical report is prepared. Various disputes and legal issues on domain names are studied. Most of the data is collected from InterNIC's website. And the various case laws are reviewed and studied for analysis from WIPO's website.

## III. THEORITICAL BACKGROUND

**3.0 Domain Name-** A domain name is the Internet equivalent of a telephone number or a geographical address. The communications format used on the Internet is known as the Internet Protocol (IP). As part of the IP, Internet addressees are comprised of a string of digits delimited by periods (commonly called "dots"). The delimited field indicates the network, sub-network and the local address, read from left to right. A typical Internet address might appear as '11.23.55' where '11' denotes the network, '23' denotes the sub-network and '55' denotes the computer itself. This all-numeric form is known as the IP address. As with IP addresses, domain names are also delimited with periods (dots), which are read from right to left. Thus, the domain name 'esselpropack.com' indicates '.com' as the network and 'esselpropack' as the sub-network. The domain name at the extreme right is called the 'Top Level

Domain' (TLD) and any domain to the left of the TLD and separated by a '.' (dot) is the Second Level Domain (SLD). A domain to the left of the SLD is known as the Sub-domain (SD). The Sub-domain, Second Level Domain and the Top-Level Domain put together comprise a 'Domain Name'. Thus, in the domain name 'law.esselpropack.com', '.com' is the TLD, 'esselpropack' is the SLD and 'law' is the SD.

**3.1 Types of top level domains-** They are as follows: 1. Generic TLD 2. Geographic or country code TLD. The current generic TLD's are as follows: i) .com for Commercial organization, ii) .int for International treaty organization, iii) .mil for defense in US. iv).edu for educational, v) aero Intended for members of aviation only, vi) .org for miscellaneous and non-profit organisations, vii) .biz Intended for bonafide businesses, viii) .net For network service providers, ix) .gov For government organizations, x) .coop Sponsored gTLD for cooperatives xi) .info open gTLD without restriction, xii) .museum sponsored TLD for museums

Private parties are not permitted to register ".mil", ".int" and ".gov" TLDs. Generic domain names are issued by Network Solutions Inc., (NSI) as part of the InterNIC Generic domain names are unique to the entire world. To register a domain names with NSI, one needs to visit the InterNIC www website and fill in the forms and comply with the other stipulated formalities. Generally, NSI or ICAAN uses allocation policy of "first-come, first-served" (FCFS) for existing gTLDs. [3] And assigns domain names on a first come, first served basis. NSI will not exercise veto power over a requested name, so long as that name is not identical to one already assigned within the TLD.

Geographical TLDs (TLD) end with a two-letter code, which is assigned to each country. It is also referred as country code TLD (ccTLD) and corresponds to a country, territory, or other geographic location. These TLDs with two letters have been established for over 240 countries and external territories. They are delegated to designated managers, who operate the ccTLDs according to local policies that are adapted to best meet the economic, cultural, linguistic, and legal circumstances of the country or territory involved. Following are some examples of the same: i) .in for India, ii) .uk for United kingdom, iii) .fr for France, iv) .us for USA, etc

Each country has an agency that handles registration of geographic domain names. These agencies are also known as NICs (Network Information Centres). Each country has its own registration policy and domain names ending with a geographic TLD are issued only to persons operating within the said country.

The administration of a ccTLD is left to the specific country concerned. For example, the Administration of Domain Names within the .in (Indian) ccTLD is looked after by the NCST. In addition to gTLDs and ccTLDs, there is one special TLD, and The .arpa domain name is used for technical

infrastructure purposes. ICANN (Internet Corporation for assigned names and numbers) administers the .arpa TLD in cooperation with the Internet technical community under the guidance of the Internet Architecture Board. Its name refers to the ARPAnet, the precursor of the modern Internet (in turn named for the United States Defense Advanced Research Projects Agency, ARPA). Today this domain is used for reverse name resolution.

**3.2 Central authority (ICANN)-** It is the nonprofit organisation that manages and coordinates the DNS is Internet Corporation for Assigned Names and Numbers (ICANN).

**3.3 Registries-** These are organizations that operate top-level domains (TLDs), such as .ORG, .COM and .NET. These Registries are Person(s) or entity(ies) responsible for providing registry services, via contract with ICANN. Registry services include customer database administration, zone file publication, DNS operation, marketing and policy determination in accordance with the general principles outlined in RFC 1591. The "Registry" is the authoritative, master database of all domain names registered in each Top Level Domain. The registry operator keeps the master database and also generates the "zone file" which allows computers to route Internet traffic to and from top-level domains anywhere in the world. There are currently five Regional Internet Registries (RIRs): AfriNIC (Africa), APNIC (Asia pacific NIC), ARIN (North America and sub-saharan Africa), LACNIC (Latin America and caribbean islands) and RIPE NCC. These non-profit organizations are responsible for distributing IP addresses on a regional level to Internet service providers and local registries. Internet users don't interact directly with the registry operator.

**3.4 Registrar-** Is a person or entity that, via contract with ICANN, provides front-end domain name registration services to registrants, providing a public interface to the registry services. There are total eight hundred and ninety six ICANN approved registrars with the participation of only fifteen countries world-wide.

**3.5 Root Server-** A machine that has the software and data needed to locate name servers that contain authoritative data for the TLDs (e.g., root servers know which name servers contain authoritative data for .COM, .NET, .FR, .UK, etc.). The root servers are, name servers and contain authoritative data for the very top of the DNS hierarchy. The root servers contain the IP addresses of all the TLD registries both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .fr (France), .cn (China), etc. This is critical information. If the information is not 100% correct or if it is ambiguous, it might not be possible to locate a key registry on the Internet. In DNS parlance, the information must be unique and authentic. Technical specifications currently limit the number of root servers to thirteen. These machines are located around the globe, in the United States, the United Kingdom, Sweden and Japan.

**3.6 Domain name system (DNS):** One of the conveniences of computer technology is that it often hides complex interactions behind a simple human experience. The Internet is a perfect example. Everyday, millions of users move from Web site to Web site by simply typing domain names (e.g., www.xyz.com.) into a computer's Internet browser. Yet, unseen and often unknown to the user, each entry actually triggers a critical, time-sensitive process before the Web site can be accessed. In order for Internet users to reach a Web site, their computer must find the address of the Web server that hosts the desired site. Computers locate one another across the Internet using numbers, not letters. For each web site on the Internet there is a unique domain name and numeric address, known as an Internet Protocol (IP) address (e.g., 205.139.94.60). This number, while quite convenient for the computer to use, is difficult for Internet users to remember; thus the need for domain names. Each time a user enters a domain name into a computer's browser, a process translates the user-friendly name into the computer friendly IP address needed to locate the appropriate Web server. This critical process is the primary function of the Domain Name System (DNS).

The DNS is a distributed database of information that computers use to match domain names to IP addresses. The data that makes up the Internet's DNS is propagated through a network of thousands of name servers, each responsible for pointing the users it supports in the right direction to get the information they need. It all starts with a component called a resolver that is a part of a user's browser application. Once a domain name is keyed into the browser, a request is forwarded to the local name server.

**3.7 DNS basic name resolution techniques-** The Iterative and Recursive Resolution are Conventional name resolution transforms a DNS name into an IP address. At the highest level, this process can be considered to have two phases. In the first phase, we locate a DNS name server that has the information we need: the address that goes with a particular name. In the second phase, we send that server a request containing the name we want to resolve, and it sends back the address required.

In iterative resolution, if a client sends a request to a name server that does not have the information the client needs, the server returns a pointer to a different name server and the client sends a new request to that server. In recursive resolution, if a client sends a request to a server that doesn't have the requested information, that server takes on the responsibility for sending requests to other servers to find the necessary records, then returns them to the client. A server doing this takes on the role of client for its requests to other servers.

Both methods eventually lead to the right device, but they differ in how they assign responsibility for resolution when it requires multiple steps.

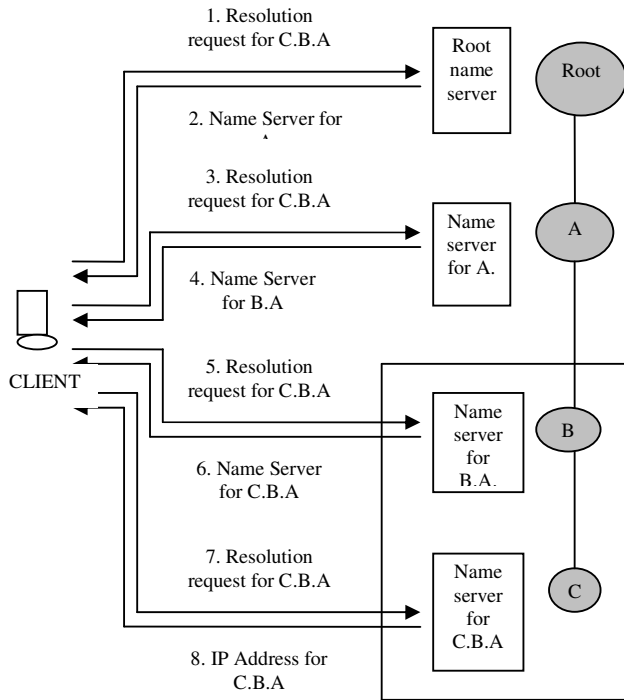


Figure 1. Iterative DNS name resolution

**Iterative resolution-** When a client sends an iterative request to a name server, the server responds back with either the answer to the request (for a regular resolution, the IP address we want) or the name of another server that has the information or is closer to it. The original client must then iterate by sending a new request to this referred server, which again may either answer it or provide another server name. The process continues until the right server is found; the method is illustrated in Figure 1 given above.

In this example, the client is performing a name resolution for “C.B.A.” using strictly iterative resolution. It is thus responsible for forming all DNS requests and processing all replies. It starts by sending a request to the root name server for this mythical hierarchy. That server doesn’t have the address of “C.B.A.”, so it instead returns the address of the name server for “A.”. The client then sends its query to that name server, which points the client to the server for “B.A.”. That name server refers the client to the name server that actually has the address for “C.B.A.”, which returns it to the client.

**Recursive resolution-** When a client sends a recursive request to a name server, the server responds back with the answer if it has the information sought. If it doesn't, the server takes responsibility for finding the answer by becoming a client on behalf of the original client and sending new requests to other servers. The original client only sends one request, and

eventually gets the information it wants (or an error message if it is not available). This technique is shown in Figure. 2

This is the same theoretical DNS resolution that as shown in previous figure, but this time, the client asks for the name servers to perform recursive resolution and they agree to do so. As in the iterative case, the client sends its initial request to the root name server. That server doesn’t have the address of “C.B.A.”, but instead of merely returning to the client the address of the name server for “A.”, it sends a request to that server itself. That name server sends a request to the server for “B.A.”, which in turn sends a request to the server for “C.B.A.”. The address of “C.B.A.” is then carried back up the chain of requests, from the server of “C.B.A.” to that of “B.A.”, then “A.”, then the root, and then finally, back to the client.

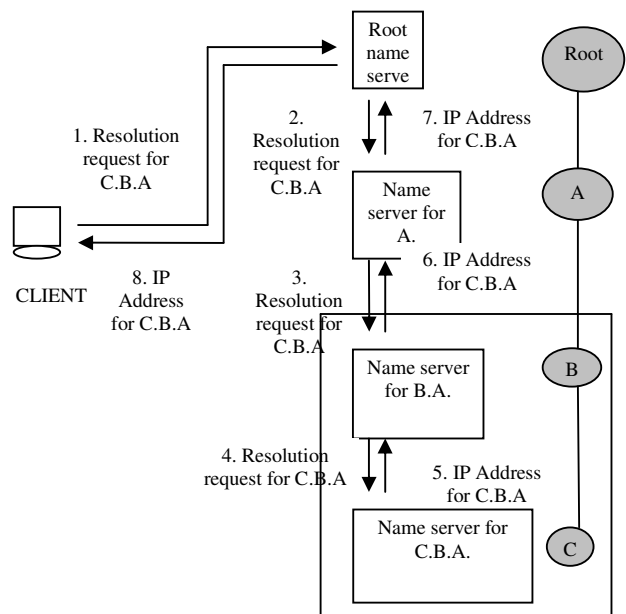


Figure 2. Recursive DNS name resolution.

Thus, The DNS has an involvement of central authority, registry system, registrars, root servers system; they are responsible for overall operation of DNS.

**3.8 Domain Name Disputes-** In today’s cyber world, where businesses are conducted on Internet media, domain names play very important role, domain names are used for promoting, advertising, conducting businesses and for many more. As the number of websites or domain names starts growing the disputes related to it also started increasing rapidly.

The domain name in the online world is just like trade name in the offline world which serves to identify the goods/services provided by the company. In domain name disputes, domain names are conflicting with trade marks and trade names this is due to fact first, global nature of domain names and country specific nature of trademark laws. Second, domain names have not yet received legal recognition as that of trademarks even though the domain names are very important element for conducting online businesses. Third, there is no connection and coordination between domain name registration and trademark registration procedure.

Any computers communicating on Internet, do not 'talk' in terms of domain names, but interpret a domain name into the corresponding IP address. All servers on the Internet interpret the same domain names the same way. That is the reason why when one types 'yahoo.com', one is taken to the web site hosted by Yahoo a company, irrespective of where the person accessing the data is located or which server he is connected to. It is essentially for this reason that domain names are unique and therefore, similar domain names cannot be offered to two separate entities. The unique feature of domain names is that the said domain names are registered on 'first come, first serve' basis. This feature of domain names given rise to domain name disputes like cyber-squatting, cyber-squatting is a form of speculation where a domain name is registered with the intention of selling off the same. Here a person or legal entity books up the trade mark, business name or service mark of another as his own domain name for the purpose of holding on to it and thereafter selling the same domain name to the other person for valuable premium and consideration. Usually, cyber-squatters book up domain names of important brands in the hope of earning quick millions. For instance, the domain name *www.microsoft.org* was available and was registered by Amit Mehrotra much before Microsoft Corporation could think of it. This led to numerous ticklish legal issues. Microsoft Corporation, despite having the trademark Microsoft, could not get the domain name 'www.microsoft.org' because of the 'first come, first serve' criteria of domain name registration. And registration of Trademarks and trade names are carried out as per respective countries jurisdictions or their own trade mark laws

**3.9 Categorisation of Domain Name Disputes:** Although the nature of Domain Name Disputes varies, still they can categorically be grouped under the distinct heads:

**Cybersquatting** In the disputes relating to Cybersquatting, cases of 'Illegitimate claims to Domain Names' form a core. Cyber squatting is a form of speculation where a domain name is registered with the intention of selling the same. The hallmark of cybersquatters is that they do not use the names, i.e. domain names are not a part of a commercial product or service offering that might confuse or deceive customers or damage the distinctiveness of a mark. Therefore, the most important criteria for determining trademark infringement, likelihood of confusion, is completely absent in the case of

cyber squatting, as no one can be confused by a blank screen. Cyber squatters never make pretence of being a company whose name they control. The problem of cyber squatting is more acute than it seemingly is, because, as already mentioned, any given Internet domain name - consisting of the exact combination of numbers, letters and characters, can be registered to one entity only. If someone attempts to register a domain name previously registered to someone else, he will be prevented from doing so because of the prior registration of that domain name by the first user.

A close corollary to 'Cyber squatting' is 'Typo squatting' - herein a 'Typo squatter' registers a Domain Name which is a variant of a famous trademark with the intent of profiting out of the goodwill of the famous trademark. The Rediff case [Rediff communications limited .V. Cyberbooth.] It is one such illustration of 'Typo squatting' wherein the respondent registered a domain name which was similar to the plaintiff's domain name.

**Cases-** The leading case is Panavision .V. Toeppen; Toeppen registered the panavision.com and approached Panavision to sell it. Rather than pay, Panavision sued Toeppen and won an injunction on a trademark-dilution theory. The court found commercial use because Toeppen's business was to reserve trademarks as domain names and then sell to the trademark owners. Before this case, in Intermatic, Inc. V. Toeppen, ransom of domain name was also found to be commercial use.

In the UK One in a Million case, the cyber squatters registered a lot of domain names incorporating famous UK trademarks and trade names. They then attempted to resell them, posting details of availability on a website. Eventually, they were sued under the Trademarks Act. The court found for the plaintiffs because the cyber squatters' activity amounted to a threat of passing off because it was a deliberate practice with a clear intent to deceive people as to the origin of the domain. This activity in itself constituted appropriation of the plaintiff's goodwill. In another UK case Harrods Ltd. V. UK Network Service Ltd., the respondent registered the 'harrods.com' and attempted to secure payment from Harrods. The court ordered the respondent to give up 'harrods.com' and to refrain from infringing or passing off its service as those of Harrods.

More and more similar cases were reported. It seems clear that cybersquatting is recognized to be a kind of trademark infringement. However, it cannot be concluded from the traditional trademark theory. As the Ninth Circuit of USA in Panavision v. Toeppen found that using federal anti-dilution law to cover cyber squatting was creating a new form of dilution outside of traditional tarnishment and blurring. Then the principle is confirmed by the USA Anticybersquatting Consumer Protection Act and WIPO final report.

**Disputes based on legitimate claims** The disputes based on legitimate claims pose a great problem for the adjudicators. These kind of disputes involve parties having a legitimate claim to a Domain Name and since there can be only one registration for a particular Domain Name there lies a matter for adjudication. As the trademark laws are territorial in nature many parties use the same name as a trademark without causing infringement. But the area of Domain Names is universal in nature thus giving voice to the issue of territoriality. The possibility of such conflict arises from the lack of connection between the system for registering trademarks and the system for registering domain names. The trademarks registration system is administered by a governmental authority on a territorial basis, while the domain names registration system is usually administered by a non-governmental organization without any functional limitation. Further, trademarks generally are issued for one or only a few categories of goods or services at a time, unless the trademark is famous or well-known, while domain names are registered on a first-come, first-served basis and offer a unique, global presence on the Internet. Trademark registrations generally require use to remain effective, while domain names can be reserved for future use.

It is identified that there are two types of legitimate competing claims dispute. Both the parties have a trademark claim in the domain name, only one party have a trademark claim. While the other has only a legitimate claim to the domain name. Since the DNS is not an outcome to the trademark system it is not incumbent for a legitimate Domain Name holder to have a trademark claim.

An illustration of a legitimate claim dispute can be seen in Infospace.com. Inc .Vs. Infospace Technology Co. Ltd, wherein both the parties had asserted a legitimate claim over a domain name.

In this case, The Complainant is Infospace.com Inc., a corporation organized and existing under the laws of the State of Delaware and having its principal place of business in Redmond, Washington, USA ("the Complainant"). And the Respondent is Infospace Technology Co. Ltd., a company registered under the laws of Jiangsu Province and having its principal place of business in Nanjing, China ("the Respondent").

While the Domain Name is similar to the Complainant's trade marks, the Complainant has failed to prove that the Respondent had no right or legitimate interest in the Domain Name and has failed to prove that the Domain Name was registered and is being used in bad faith.

Accordingly the remedy requested by the Complainant is denied and the Respondent is not required to transfer the Domain Name to the Complainant. The Panel judged giving the benefit to the Respondent stated that the obligation is on

the complainant to show that the Respondent lacked a right or legitimate interest in the domain name.

As legitimate claim disputes are the most challenging types of disputes for the adjudicators and since there is lacunae in the law to decide disputes of legitimate claims the best approach to adjudicate such matters would be to base the adjudication based only purely on facts and circumstances that surround the dispute.

*Register trademarks as domain names for own use-*

Since trademarks are registered in different classes, while domain name is unique on the Earth, this issue should be discussed respectively.

Register trademarks as domain names in same class of product or service.

**Cases-** In Bell Actimedia, Inc. vs. Puzo, et al., the Canadian court issued a preliminary injunction against the defendants who had just established a website under the domain "lespagesjaunes.com" as a French language business directory. The plaintiff telephone giant has long-standing registered marks for "yellow pages" and "pagesjaunes." The injunction prohibits acts of the defendant that infringe on the plaintiff's marks, including use of the domain name.

In Affair Sapeso, the defendant registered its competitor's trademark as a .com domain. The French court ordered the defendant to withdraw its domain name from the Internet and enjoined the company from any further use of the trademark. The court held that the offending activity (domain registration) took place outside of France and that trademark rights are defined by territory was no bar to the court's authority since doing otherwise would allow trademark infringers to escape liability by simply registering in a foreign jurisdiction.

In the "Ozu" case, "ozu.es" is Spain's first search engine created at Advernet. Advernet received a trademark registration for "ozu" in Spain. Some of Advernet's partners broke away and started a competing company and registered the domain "ozu.com" in the USA. The Spanish court held that the trademark owner had exclusive use of the "ozu" and that all of the defendant's use was infringing.

It seems that the courts in different jurisdictions all agree to prohibit registering a domain name that is identical or similar to its competitor's trademark. However, they based on different legal reasons. The enforcement of an order that applies to an extra-territorial domain name registration is still a problem.

*Register trademarks as domain names in different classes of products or services-*

**Cases-** In China, a plaintiff registered the trademark "PDA" for the manufacture of electronic goods in 1997. When the

company planned to register the domain name 'pda.com.cn' in late 1998, it found the defendant has registered the domain name and used it to sell other's products. An action was brought under China's Trademark Law and Law against Unfair Competition. Because the plaintiff failed to provide any evidence that defendant's products were the same or similar, the court was unable to find actual infringement.

In *Avery Dennison Corp. v. Sumpton*, the plaintiff had acquired distinctiveness in the 'Avery' and 'Dennison' trademarks, the defendant registered 'avery.net' and 'dennison.net' for sale vanity e-mail address. The court held that the defendant's customer base is Internet users who desire vanity e-mail address, while the plaintiff's customer base includes purchasers of office products. There was no evidence demonstrated that the plaintiff possessed any degree of recognition among Internet users or the defendant directed e-mail service at the plaintiff's customer base.

While in France, a court refused to apply the trademark concept of specialty (classification by type of good or service) to domains and specifically prohibited a computer services company from using "alice.fr" against a trademark owner in a totally non-competing class of products in *Affair Alice*. However, this decision was reversed by the Court of appeal which applied the speciality test to conclude that two trademarks could coexist as far as there is no confusion between the services or the products. Traditional confusion analysis was therefore applied in most subsequent cases.

In the above cases, all the final decisions are based on traditional confusion analysis. However, as discussed below, both the French courts and the USA courts ruled that mere registration trademarks as domain names is trademark infringement because it block the trademark owner's ability to use the trademark online. The conflict is obvious.

*Register well-known or famous trademarks as domain names-*

**Cases-** In USA, trademark owners have successfully used the Lanham Act to protect their famous trademarks. For example, in *Hasbro, Inc. v. Internet Entertainment Group*, Hasbro brought the action after discovering that its trademark 'candyland', which is the name of one of its most popular children's games, was registered as 'candyland.com' for a pornographic website. The court held that such use of the mark as a domain name for pornography could in fact result in consumer confusion and thereby dilute the mark.

In *Planned Parenthood Federation of America, Inc. v. Bucci*, the defendant registered the plaintiff's trademark as a domain name for the purpose of bringing target audiences to the content to his non-commercial site. However, the court held that the use of the trademark had the potential to prevent some Internet users from reaching plaintiff's own website, and the use resulted in unfair competition and dilution under the Lanham Act.

Brazil enforced a new regulation in 1998 attempted to clarify some domain name conflicts. The regulation forbids third-party registration of domain names that conflict with well-known trademarks and reputed trademarks. No other trademarks are given specific protection against conflicting domain name registrations. Well-known trademarks are protected in Brazil only to the extent that the trademark is used on identical or similar goods. Reputed trademarks are those registered in Brazil but declared by the Patent & Trademark Office as being well-known within Brazil and therefore entitled to protection across all classes of goods and services.

It is no doubt that well-known trademarks should be protected specifically. WIPO suggests in its Final Report that the registration of a domain name identical to well-known trademark in any new gTLDs should be automatically blocked. It is an active suggestion. However, what is well-known trademark? So far there is no world widely confirmed list or criteria. Further, how to reach the balance between well-known trademark protection and free speech is a big problem. Should the domain names for non-commercial use also be prevented from registering?

*Register trademarks as domain names for non-commercial use-*

In USA, there are conflicting decisions. In *Jews for Jesus v. Brodsky*, the plaintiff registered the 'Jews for Jesus' trademark and the domain 'Jews-for-Jesus.org'. The defendant set up sites with the domain names 'Jews for Jesus.org' and 'Jews-for-Jesus.com' that ridiculed, maligned and parodied plaintiff's website. The court found that defendant's use of his domain name created a likelihood of confusion and blurred and tarnished the value of the 'Jews for Jesus' trademark. However, in *Bally Total Fitness Holding Corp. v. Faber*, the plaintiff brought an action against a website which domain name included the words 'bally sucks'. The site was dedicated to complaints about the plaintiff's health club business. The court held that confusion as unlikely because the defendant's site had a fundamentally different purpose from the plaintiff's site. The former was a consumer commentary while the latter was a commercial advertisement; therefore there was no trademark infringement.

What can constitute a commercial use? In Germany, a website is commercial, if there are goods or services offered on the site, if there is advertisement, or if there is a link to some commercial site. Use may also be commercial if the domain name itself shall be auctioned off. It is obvious that these interpretations are too broad. Many individuals register free domain names to establish their non-commercial site, but the free site providers always insert advertisements automatically into their non-commercial sites. Does it turn the sites into commercial? Further, many commercial sites have some useful information that is worthy linking for non-commercial



use. We cannot conclude that the sites with such links are commercial.

#### **legal Issues related to domain names:**

The few of legal issues on domain names are discussed below,

##### *Protecting trade names from being registered as domain names-*

Some courts in different jurisdictions protected trade names from being registered as domain names by others, although different laws were applied. In France, bulk registration of well-known French corporation names has been condemned as cyber squatting. The defendant's plea that it was "safeguarding prestigious marks" was summarily rejected. In *Affair Champagne Céréales*, protection from competing web sites was extended to company trade names without formal mark registration.

In Germany, the Trademark law protects registered marks as well as non-registered names used in business relationships, such as trade names. The Civil Code also protects the names of corporations, partnerships, associations, trade unions, etc. Neither the commercial use nor the names be identical is required. Similarity leading to confusion can be infringement. In "epson.de" case, the court also asserted that the registration of another's name for no purpose other than to hinder the true owner from using it is an "unfair operational disturbance" under the Against Unfair Competition Law.

In *Labouchere v. IMG Holland*, a group of banks and insurance companies sued IMG for registering the names of each of the banks and insurance companies as domain names. The Holland court held that such use by IMG prevented plaintiffs from registering the names as domain names.

While some other courts were not so strict on this issue. In *Peinet Inc. V. O'Brien*, a Canadian court considered the potential for confusion between *pei.net* and the plaintiff's corporate name *Peinet* and held that the use of lower case letters and a period to separate the domain name into two parts was sufficient to avoid confusion.

In the *Capricom* case, the Belgian court held that the Belgian Company Act is inapplicable because it only restricts use of words as trade names and does not restrict or otherwise applies to words used as domain names.

##### *Protecting Geographical from being registered as Domain names-*

Geographical names are protected under the Paris Convention and in some jurisdictions, especially when they are related to the sources of some particular goods. They should also be protected from being registered as domain names by unrelated parties. A French commune of *Saint Tropez* had registered in

the name in France, the defendant registered "*saint-tropez.com*" in USA for itself. The court held that trademark rights were enforceable against domain names. A different conclusion was reached where the name only appeared as a file path. In *Affair Elancourt*, the court held that name rights could not be used to prohibit non-commercial speech about the subject matter of the name. While bulk registration of the names of cities, monuments has been condemned as cyber squatting in France.

In Germany, decisions under the Civil Code allowed *Heidelberg* and *Braunschweig* to enforce their *Namensrecht* against domain holders. However, the court of *Koln* ruled that consumers do not necessarily expect domains using geographical names to be exclusively associated with the corresponding municipality, particularly when the municipality was not well known, therefore confusion was unlikely.

The UK is just beginning to deal with this issue. A company paid 5 pounds each to register about 1500 village names and plans on reselling them for 500 pounds each.

##### *Protecting Names of celebrities from registering as domain names-*

Shortly after every Chinese athlete won an Olympic gold medal, his or her name was registered as domain name by someone else. The names of celebrities were registered as domain names all over the world. Should they be protected? As we know, *Julia Roberts* and *Madonna* have been successful in getting back the domain names which are identical to their names, while *Sting* lost his case because the panel held that "there was evidence that the Respondent had made bona fide use of the name *Sting* prior to obtaining the domain name registration and there was no indication that he was seeking to trade on the good will of the well-known singer."

In Germany, the Civil Code seeks to protect one's personality by enabling everybody to be recognized by his or her own name. If someone claims protection based on the Civil Code, the use of the domain name by the Cybersquatter does not necessarily have to be a commercial one.

#### **3.10 Domain name dispute resolution methods:**

Since Lawsuits are expensive and time consuming hence well recognized ICANN approved dispute-resolution service providers must be approached. There are a number of administrative forums or dispute resolution service providers where arbitration may be filed under ICAAN (Internet Corporation for Assigned Names and Numbers) UDRP (Uniform Domain-Name Dispute Resolution Policy). Administrative forums are: i) WIPO (World Intellectual Property Organization - Geneva), ii) NAF (The National Arbitration Forum - Minneapolis, USA), iii) ADNDRC (Asian Domain Name Dispute Resolution Centre -

Beijing and Hong Kong, China), iv) CPR (CPR Institute for Dispute Resolution - Asia). Disputes under these policies may be filed with one of the approved dispute-resolution service providers for the given policy.

**IV. DATA COLLECTION AND ANALYSIS**

**4.1 Continent-wise analysis of DNS registrars, root servers, registries:**

In this data analysis the data about, world wide ICANN accredited domain name registrars, location of root name servers and location of gTLD registries is collected from Internet source and tabulated. Then this data collected is scrutinized and arranged in country-wise then continent-wise fashion, and again tabulated. Based on which graphical report is generated about global distribution of domain name registrars, root name servers, registries using MS-Excel.

**Registrars**-The number of registrars world wide are shown below:

Table 1. Number of registrar’s continent wise (Source: compiled from <http://www.internic.net/origin.html> )

Continents	Number of registrars
Asia	60
Africa	2
America	731
Oceanic	13
Europe	84

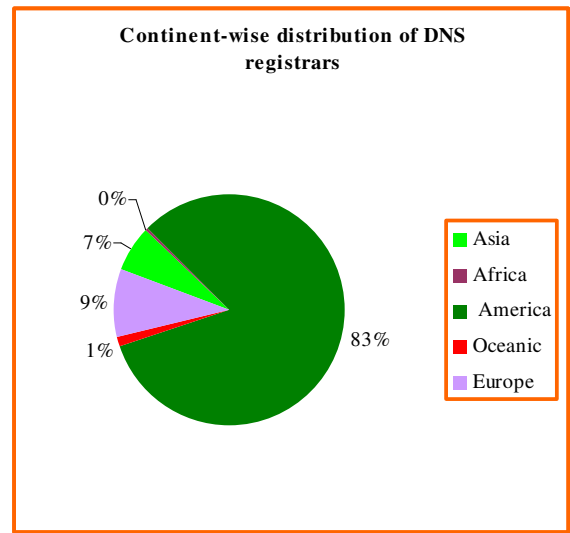


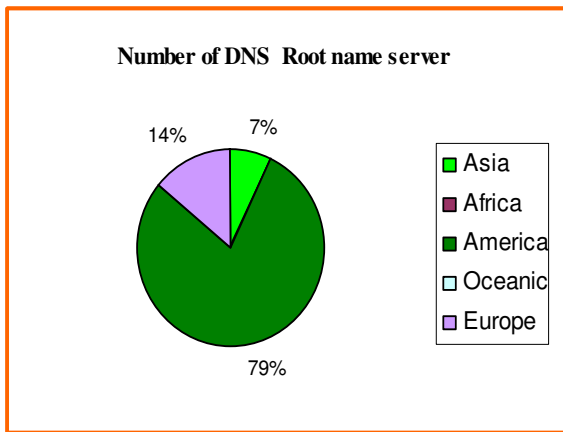
Figure 3 Graphical representations of world wide domain name registrars

**Root name servers**-The technical locations of all thirteen root name servers continent wise are shown below:

Table 2. World wide domain name root server continent wise. (Source: compiled from <http://www.icann.org> )

Continents	Number of DNS Root name server
Asia	1
Africa	0
America	11
Oceanic	0
Europe	2

Figure 4 Graphical representations of world wide domain name root servers

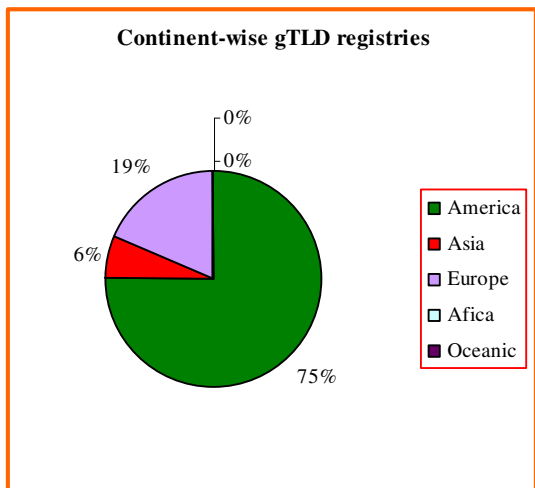


**Registry operators-** The continent-wise distribution of gTLD registry operators are shown below:

Table 3. World wide domain name registry operators continent wise (Source: compiled from <http://www.icann.org>)

Continent	Number of gTLD Registry operator
America	12
Asia	1
Europe	3
Africa	0
Oceanic	0
Total	16

Figure 5. Graphical representations of world wide domain name registry operators



## V. CONCLUSION AND FUTURE WORK

It is found that, there are total eight hundred and ninety six ICANN accredited registrars and out of which five hundred and eighty three are in US itself. So maximum revenue (eighty three percent of total) out of domain name registration goes to US.

There are sixteen gTLD registry operator, new as well old including sponsored and unsponsored, out of which twelve (seventy five percent) are based in U.S. So maximum of domain name registry service providers belongs to U.S. Hence, maximum of earning is obtained by US again. There is zero percent contribution by Africa, Oceanic continental countries

There are thirteen root name server out which of eleven are located in United states itself. Even if Internet is not owned by anybody, but seventy nine percent of distributed root name server operation is managed by U.S again.

Even though it is known, Internet is not owned by anybody, but indirectly it is administered, managed and controlled by United States of America.

The response time of the root servers from various locations around the world is not same, which results that regions in Oceania, Africa, South America and part of Asia are under-served by the current root servers. In such scenario, applying First Come and First Serve policy for domain name registration is unfair and not reliable for registrants from under served regions. There is a need to find out better domain name registration policy based on efficiency and effectiveness of domain name system's technical infrastructure.

## V. ACKNOWLEDGMENT

The author wishes to special thanks for her M.Phil research Guide, Prof. Dr. Sunita Mahajan, Principal, MET College, Banda.. teachers, for their constant support and valuable ideas during the work. And whole-hearted thanks to all teachers and Guides for their encouragement.

## REFERENCES

- [1] Yuji Sekiya, Kenjiro Choy, Akira Katoz, Ryuji Somegawa, Tatsuya Jinmei and Jun Muraik, "On Root and ccTLD DNS server observation from worldwide locations, Information Technology Center, The University of Tokyo, Tokyo, Japan
- [2]. Summit Strategies International, Evaluation of the New gTLDs: Policy and Legal Issues Prepared for the Internet Corporation for Assigned Names and Numbers(ICANN), July 10, 2004
- [3] [AL98] P. Albitz and C. Liu. *DNS and BIND (3rd ed)*. O'Reilly and Associates, 1998.
- [4] [BkcN01] N. Brownlee, k. claffy, and E. Nemeth. DNS damage. *NANOG23*,

October 2001.

[5] [DOK92] Peter B. Danzig, Katia Obraczka, and Anant Kumar. An analysis of wide-area name server traffic: A study of the domain name system. In *SIGCOMM '92*, pages 281–292, 1992.

[6] [KM01] Akira Kato and Jun Murai. Operation of a root DNS server. *IEICE transactions on communications*, E84-B(8):2033–2038, August 2001.

[7] [MD88] Paul V. Mockapetris and Kevin J. Dunlap. Development of the domain name system. In *SIGCOMM88*, pages 123–133, 1988.

[8] [SCSY03] Ryuji Somegawa, Kenjiro Cho, Yuji Sekiya, and Suguru Yamaguchi., The effects of server placement and

[9]<http://www.icann.org>

[10]<http://www.iana.org>

[11] <http://www.internic.net>

[12] <http://www.wipo.net>

[13] <http://www.nic.net>

[14] <http://www.dnjournal.com>

[15]<http://www.tcpipguide.com>

[16] <http://www.asianlaws.org>

server selection for internet services. *IEICE transactions on communications*, 2003.