IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. II (May-Jun. 2016), PP 01-08
www.iosrjournals.org

Investigating DHCP and DNS Protocols Using Wireshark

Sameena Naaz, Firdoos Ahmad Badroo
Department of Computer Science and Engineering , Faculty of Engineering and Technology, Jamia Hamdard, New Delhi, INDIA

Abstract: *For different computers to communicate on the same network or on different networks they need to know one another's IP address or MAC address. Involving the IP address and MAC address has led to a challenging task for a network analyst to secure the communication. There are various ways to mitigate the attacks in application, transport and network layers of a network. Mitigating the attacks in data link layer is a challenging task for a network analyst as adequate security is not assigned to a data link layer. DHCP and DNS are the most widely used in host configuration and they work in data link layer. Mostly these protocols are vulnerable to number of attacks like in DHCP the attacks are DHCP Starvation attack and Rogue DHCP attack while in DNS the attacks are DNS Hijacking Attack and DNS Cache Poisoning Attack. These protocols have been investigated in this research where DHCP and DNS packets have been captured and analysed them with the help of Wireshark. Mainly we have analysed how IP address is assigned to a client from a DHCP Server and how packets are exchanged between the DHCP client and DHCP Server and DNS is used for resolution of URL into IP address.*

Keywords*: DNS, DNS Packets, DHCP, DHCP Packets, Rogue DHCP server*

I. Introduction

The increase and rise of network has led to the difficult task for a network administrator to analyse the network. Understanding the network protocol means solving the network problems in an efficient manner so that we can secure the path on which packets are transmitted along with the data. So network security becomes an important concern as it makes the packets less vulnerable to different types of attacks like rogue DHCP attack [1].

DHCP stands for Dynamic Host Configuration Protocol which is an internal protocol. It is a way by which networked computers get their IP addresses dynamically; and it is used both in wired and wireless LANs. One of the important features of DHCP server is that they avoid IP address conflict [2]. In the network, every website is recognized by its uniquely assigned IP address, but remembering all IP addresses is not possible therefore DNS (Domain Name Server) protocol comes to rescue in order to resolve this.

Both the protocols play a vital role and have significance therefore there security is an important task. Hence, DHCP is used to assign an IP address to hosts while the DNS is used for the resolution of URL into IP address. Both the protocols are independent services and may run on the same server or on different servers [3]. The organisation of this paper is as follows:

The organization of the paper is as follows: DHCP packets have been investigated in section II and a way for finding Rogue DHCP Server has been explained. Section III discusses the DNS Packets. Detection of DNS errors using Wireshark has been investigated in Section IV and finally Section V talks about our proposed model based on DHCP Password Authentication.

II. Dynamic Host Configuration Protocol

DHCP stands for Dynamic Host Configuration Protocol and it is an extension of BOOTP (the previous IP allocation specification) and it is an internal protocol in which computers dynamically get IP addresses from DHCP Servers [4]. The basic functionality of the DHCP Server is to automatically assign the IP address to client machines and other network information such as the subnet mask, the default gateway, and the Domain Name system (DNS) address. DHCP also eliminates the involvement of network administrator and also it prevents from IP address conflicts among client machines connected to the same network. This can help us to manage the large networks easily.

DHCP is used extensively in corporate, University and home network to assign IP address dynamically to hosts and it is used both in wired and wireless LANs. In an IP network, when we connect our machine (host or client) connecting to the Internet it needs a unique IP address. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically assign a new IP address when a computer is plugged into a network. As DHCP server automatically assigns IP address to a host from a pool of address; there is an issue of IP address conflict. As we know DHCP client may receive multiple offers from DHCP Server and what happens here, the client accepts the first offer it receives.

To keep track of how IP address is assigned, a DHCP server uses the concept of leasing; it means that IP address is assigned for a fixed duration of time, called leasing. Just before the expiry of the lease, a computer should request the DHCP server for renewal. Otherwise, that IP address cannot be used further [5].

2.1 DHCP Process

Understanding the basics of a DHCP Process will help us to understand and remember the how to configure the IP Address for a host available in DHCP Pool. The DHCP Server can also issue other configurations to the client that help to function on the network such as the addresses Domain Name System [DNS], Default Gateway Windows Internet Naming Service [WINS] servers. Wireshark[6] has been used to investigate the DHCP packets in detail. This protocol helps reduce administrative overhead on an IP-based network. The DHCP request process breaks down into four steps:

2.1.1 DHCP Discover

The investigation of DHCP Discover packet has been carried out in a home network where a single PC was connected to that network. There has been an exchange of four different packets in which the PC broadcasts a message to the DHCP Server. The function of the DHCP Server is the reply to the DHCP client and assign an IP address that is unicast. From Fig. 1 it is clear that a unique transaction ID is assigned to these packets[7].

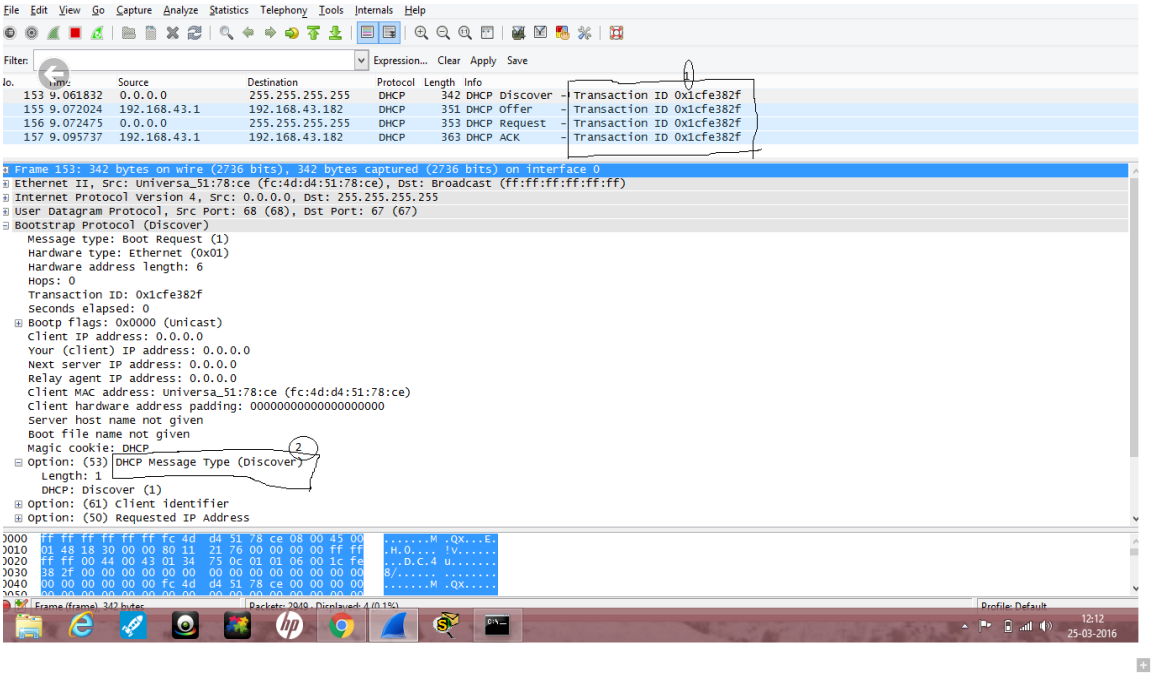

Figure 1: Analysis of DHCP Discover packets in Wireshark

2.1.2 DHCP Offer

The Server responds with a DHCP Offer (unicast), however if there are many offers from a different DHCP Servers the client accepts the first offer [7]. Additionally, the offer from the DHCP Server is not an assurance that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. From Fig. 2 it is clear that there is an offer for DHCP Server to DHCP Client.

1. The offered IP address to the DHCP Client is based on lease. Here on this home network the lease that is offered to DHCP Client is one hour. After the expiration of this lease, it will not be renewed. The default time of the lease is one hour. DHCP Server will block this IP address and it will be unavailable for other DHCP Clients.
2. The DHCP offer has also mentioned the renewal time that is 30 minutes.
3. The rebinding time value is 52 minutes 30 seconds.

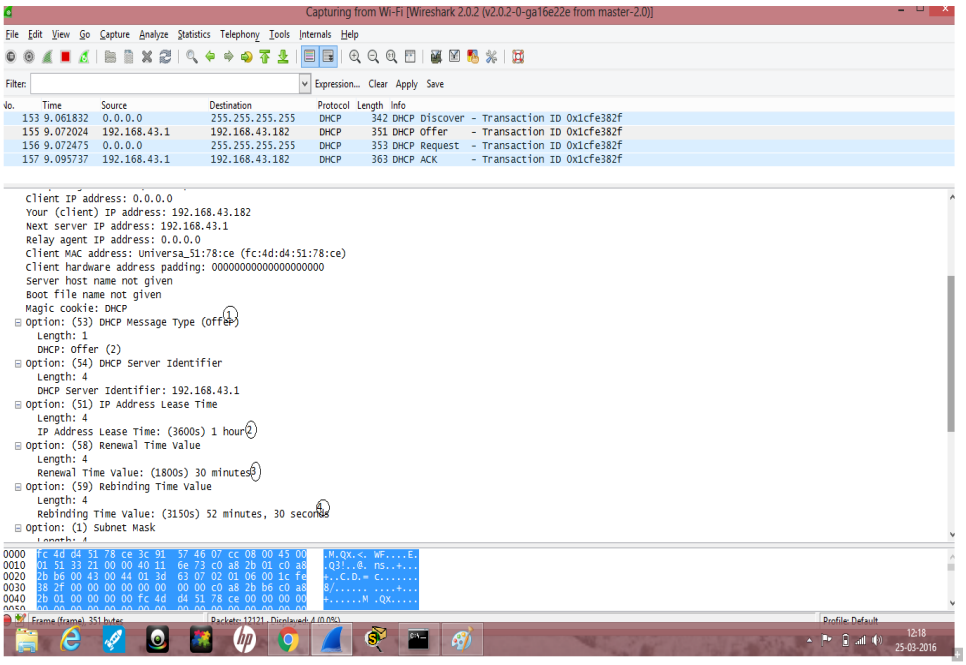

Figure 2: Analysis of DHCP Offer packets in wireshark

2.1.3 DHCP Request

The client sends DHCP Request (Broadcast) that it has accepted the offered IP and it implicitly declines other offers from other servers if any. From Fig 3 the following contents were found while analysing the DHCP Request packets:

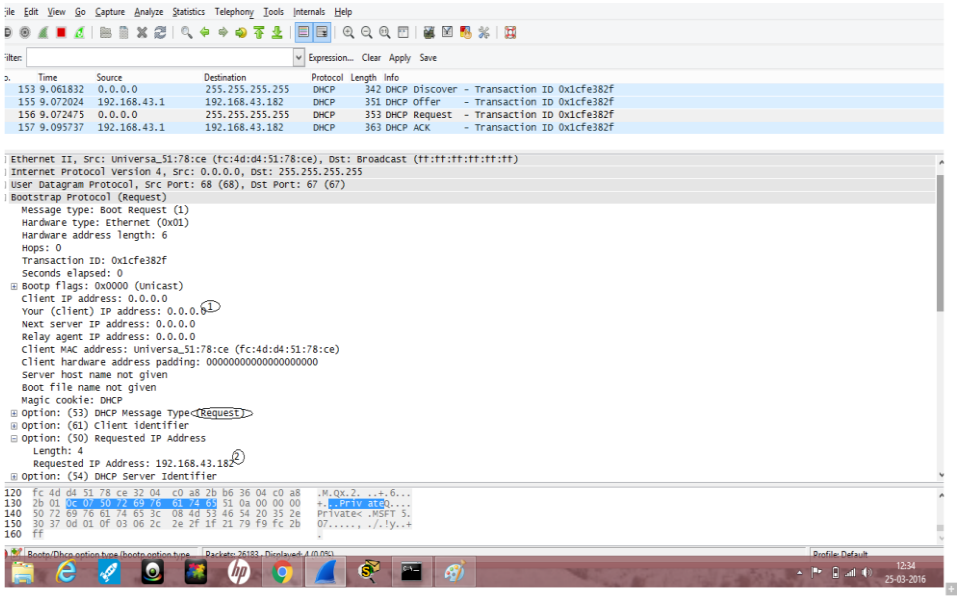

Figure 3: Analysis of DHCP Offer packets in wireshark

1. The Client IP address is still 0.0.0.0. This means that IP address has not been assigned to the DHCP Client. The destination IP address is 255.255.255.255 which means DHCP request is also broadcasted [6].
2. The IP address that is offered from DHCP Server to DHCP Client is 192.168.43.182

2.1.4 DHCP ACK

The DHCP server sends back DHCP ACK (unicast) which includes additional network parameters (gateway and DNS server addresses). Fig. 4 gives the contents found while analysing the DHCP ACK packets:

1. The DHCP Server will now assign the IP address to the Client i.e.; 192.168.43.182 and blocks this IP address for further use till lease time expires.
2. The IP address that is assigned to DHCP Client has a lease time. After the expiration of the lease it will be taken away from the DHCP Client and will become available in the DHCP Pool.
3. The renewal time value of an IP address is 30 minutes. This means the end of the renewal time the IP address of the DHCP Client is changed.
4. The rebinding time value is 52 minutes and 30 seconds.
5. The subnet mask of the IP address is 255.255.255.0.This means there can be 254 available IP address in the DHCP Pool.

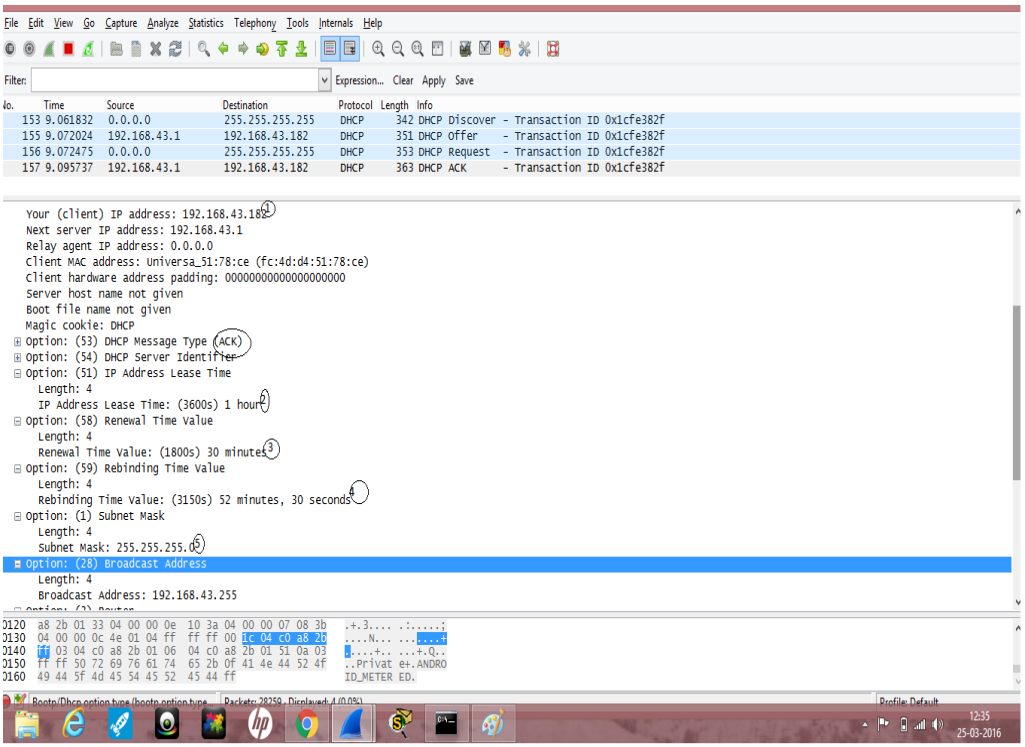

Figure 4: Analysis of DHCP ACK packets in wireshark

2.2 Rogue DHCP Server

After analyzing these packets in detail, our approach was to find the possible attacks on DHCP in which one of the attacks we have analyzed in wireshark is DHCP Rogue Server. As we know DHCP Client receives multiple offers from DHCP servers and can accept one of these offers [8]. However there are some unauthorized Servers (called as Rogue DHCP) that invites intruders and attackers to intercept the network traffic and exploit the vulnerabilities of DHCP Client. The purpose of this attack is to provide an illegal IP address to the DHCP Client so that they can block and access the legitimate traffic and alter the communication according to their requirement.

As clients connect to the network, both the rogue and legal DHCP server will offer them IP addresses as well as default gateway, DNS servers, among others. If the information provided by the rogue DHCP differs from the real one, clients accepting IP addresses from it may experience network access problems, including speed issues as well as inability to reach other hosts because of incorrect IP network or gateway. In addition, if a rogue DHCP is set to provide as default gateway an IP address of a machine controlled by a misbehaving user, he can sniff all the traffic sent by the clients to other networks, violating network security policies as well as user privacy (see man in the middle). VMware or virtual machine software can also act as a rogue DHCP server inadvertently when being run on a client machine joined to a network [9].The VMware will act as a rogue DHCP server handing out random IP addresses to the clients around it on the network. The end result can be that large portions of the network are then cut off from both the Internet and the rest of the domain without any access at all [10].

2.2.1 Investigation Of Rogue DHCP Server

The purpose of this investigation is to find a rogue DHCP server using wireshark[10]. While doing the investigation the following steps were followed:

1. Start the Wireshark with no capture filter.
2. At the same time go to command prompt and release the IP address immediately "IPconfig/release".
3. Then renew the IP address with the command "IPconfig/renew".
4. Save the trace file that is to be investigated.
5. Using the filter of the wireshark type "bootp"there may be a multiple offers or a single offer depending upon the network.
6. Select the offer packet and go to the top and use their command menus and mark the packet details.
7. As it can be seen from Fig. 5, the wireshark automatically uses the syntax "bootp.option.dhcp==2" or we can write it in the display filter specification.
8. Using the bootstrap protocol in the packet header we click on "DHCP Message type (offer) and right click on that and apply as filter and select it.
9. While using the statistics from the command menus and select the end points there we find a report. Then click on the limit to display filters.
10. From Fig. 6 it is clear now that the IP address that is assigned to the PC is from the legitimate DHCP Server.

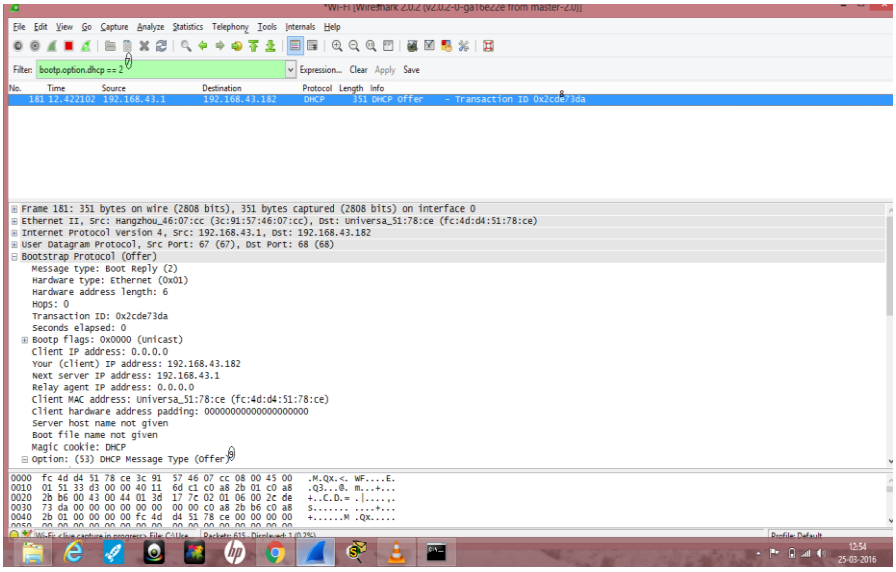

Figure 5: Analysis of Rogue DHCP Server.

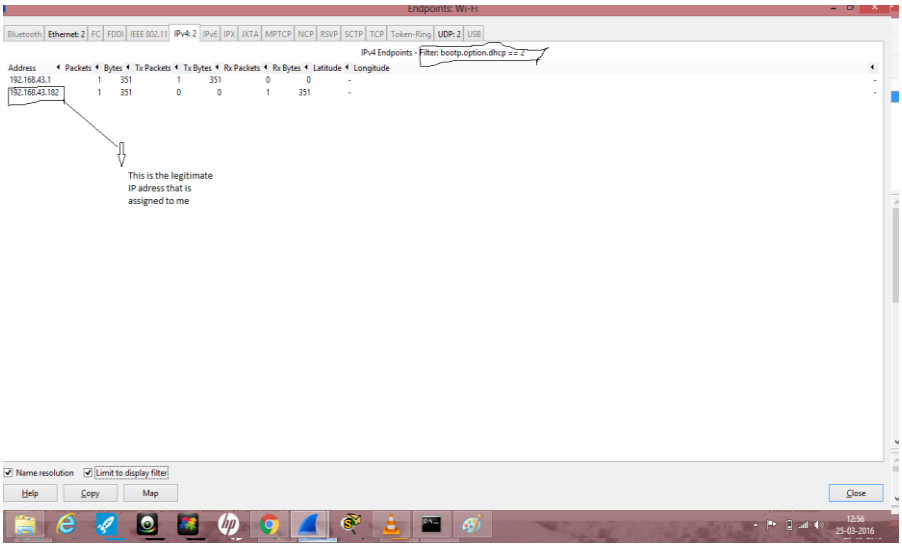

Figure 6: Analysis of assigned IP address

III. Domain Name Server

Domain Name Server is a protocol that is designed to work across different platforms over internet. In practice DNS is defined as a Client Server Application. A host that needs to map an address to a name or name to an address calls a DNS client called as resolver. The resolver then tries to access the closet DNS Server with a mapping request .If the Server has the solution it satisfies the resolver, otherwise it tries to communicate with resolvers of other servers or asks other DNS Servers to provide the information. After the resolver receives the mapping, it interrupts the response to see if it is a real resolution or an error, and accordingly results are delivered to a process that requested it. In general the, DNS protocol provides resolution in two ways either the recursive resolution or the iterative resolution. While explaining these resolutions the DNS Servers must support Iterative (non-recursive) query. The Client's role in the DNS is relatively simple it sends a query to its local DNS server and receives a response back to the Client. Moreover, there is also a concept of caching in the DNS Server where every time a Server receives a query that it is not in its domain, then it has to search its database for a Server IP address. Reduction of this search time would increase efficiency and DNS handles this mechanism with Caching [2].

DNS PACKETS

The process of analyzing the DNS in wireshark means that we have to look for DNS errors and DNS delays. Mainly we have to look for DNS responses. While detecting DNS delays in wireshark, we have to validate the IPv4 checksum and it will prevent us from false positives. Also DNS traffic doesn't have any colouring rule in wireshark but it uses the UDP Colouring rule that is setting on the top of the UDP header [11].

In this work, we have investigated DNS both in LAN and in our home network. In the LAN Network we simply start our wireshark and simply make two queries at the same time with the help of browser. We simply use the display filter specification and write the DNS there and apply it as a filter. From Fig.7 it is clear that queries receive two responses with the same transaction Id respectively. Another way is check the DNS errors in the packet header where we have to click on the domain system and from there we have to check the reply code and if 0000=reply code that mean we have no errors that is everything is fine or if there is anything other than zero that is a problem.

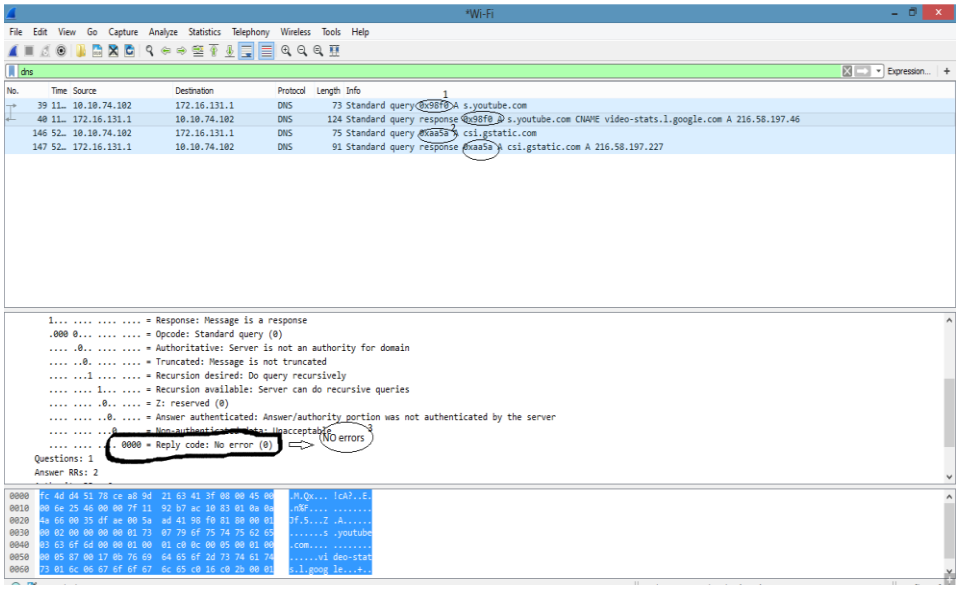

Figure 7: Analysis of DNS packets in wireshark

While investigating the DNS packets in the home network and following the same procedure as above, the DNS response that we receive is from the same query with the same transaction ID. Also reply code=0000 that means we have no errors.

Moreover in the home network we have used another method namely Right Mask Click Method [12] in wireshark. This method is used for further investigation of DNS Packets. In this method we right click on reply code and prepare a filter not selected. This will automatically use a syntax in filter specification which begins with (dns.flags.rcode!=0) and we apply this filter we will observe more DNS errors packets in detail. The above syntax is one way that looks for DNS errors.

From Fig. 8 it is clear that reply code is something other than 0000.that means there is a delay in responses from the DNS Server.

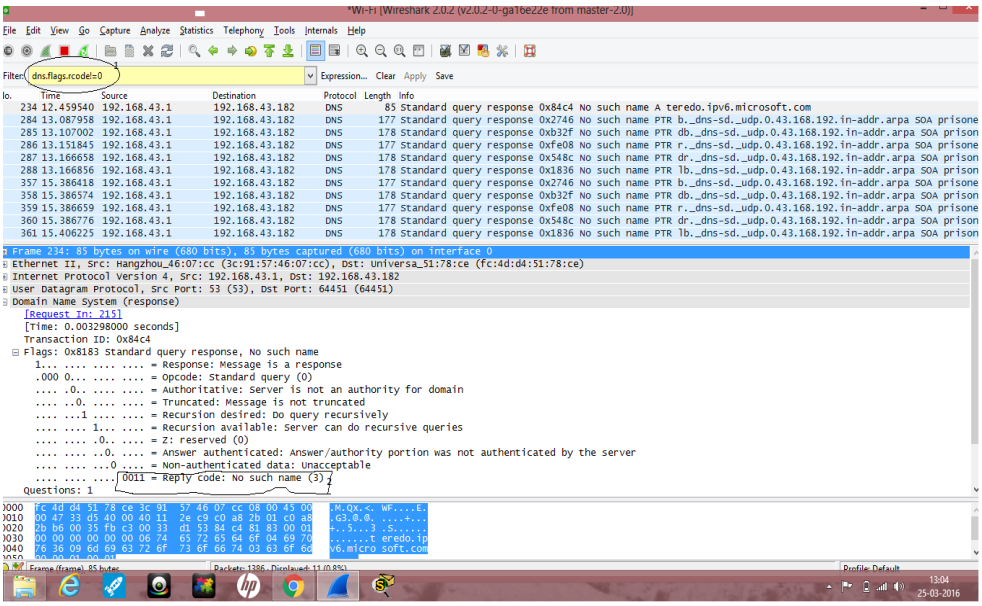

Figure 8: Analysis of DNS Packets in wireshark

IV. Proposed Solution

In this proposed scheme, we assume DHCP Server maintains a hashed password file. The passwords are maintained and assigned by network administrator. In this scheme; the DHCP clients calculate the hash of the unique identifier (password) and pass it with the MAC address i.e. the DHCP Discover. The DHCP Server has maintained a corresponding hashed file and when it receives the Discover and request process it always checks the validity of password and also assignment of IP address and if the DHCP client request process passes the both tests then an IP address is assigned to DHCP Client otherwise the request will be blocked. Also the DHCP Server stores the password in a stored file making it a triplet (MAC|Password|IP).

The advantage of this scheme is that even attacker spoofing the MAC address of any DHCP Client in the LAN can't get IP address from the DHCP Server because the attacker doesn't have the legitimate password that is assigned by network administrator. The attacker can't get the IP address from the DHCP Server and thus provides the solution for both the DHCP rogue and the DHCP starvation attack where attacker was sending the requests from the spoofed MAC address.

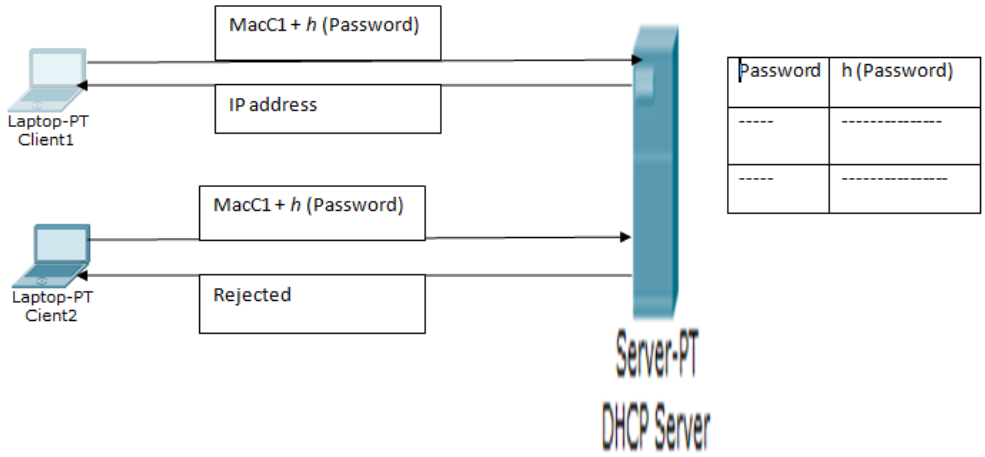

Figure 9: DHCP Password Authentication.

V. Conclusion

In this research work, we have deeply studied and investigated the DHCP and DNS protocols using wireshark. As we know there is a relation between these two protocols as the DHCP is one of the most used network protocol used for network configurations and DNS is used to resolution of URL into IP address. In this work we have configured two PCs with the DHCP and DNS Servers with the help of tool namely as Cisco Packet Tracer Student and then dynamically assigned them network parameters with these Servers. Furthermore we have investigated DHCP Packets more deeply and studied how one can detect if there are more than one offers to a DHCP Client i.e.; how can we detect Rogue DHCP Server. Also we have analysed DNS packets both in LAN and home network and found DNS errors and DNS delays.

Reference

[1] A. Razaque and K. Elleithy, "Controlling Attacks of Rogue Dynamic Host Configuration Protocol (DHCP) to improve Pedagogical Activities in Mobile Collaborative learning (MCL)", Journal of Communication. & Computer Engineering, Volume 3, Issue 1, 2013, Pages 15-29, ISSN 2090-6234.
[2] B.A Forouzan, Network Models, in Data Communication and Networking (New Delhi, Tata McGraw Hill, 2006)27-60.
[3] [online]:Available:https://technet.microsoft.com/en-us/library/cc958921.aspx
[4] [online]:Available:https://achiveswyxforum.com/community/default.aspx?tabid=138.
[5] Biju Issac, "Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks", International Journal of Network Security, Volume 8,No. 2, Page 107-118,March 2009.
[6] [Online]: Available: www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets.
[7] M. Khan, S. Alshomrani and S. Qamar, Investigation of DHCP Packets using Wireshark, International Journal of Computer Applications, Volume 63 No. 4 , February 2013, ISSN 0975 8887.
[8] Ulf Lamping, Richard Sharpe, Ed. Warnicke, Wireshark User's Guide for Wireshark 1.7 Copyright 2004-2011.
[9] [online]: Available:https://en.wikipedia.org/wiki/Rogue_DHCP
[10] Osama and S.Younes, "A secure DHCP Protocol to mitigate LAN Attacks", Journal of computer and communications, Volume 4, Page 39-50, 2016.
[11] [Online]: Available: www.wiresharktraining.com
[12] [Online]: Available :https://www.wiresharktraining.com/training.html