MAC Spoofing Detection Via Wireshark

Ms. Konika Abid , Mr. Ajay Kumar Singh

Abstract—**When computers are, connect on any network a network card is used, known as NIC card which is having a MAC address. This address is use to distinguish one system from another we may say that it is the physical address given by the manufacturer to provide a unique identity to equipment. We have studied that MAC address is permanent and cannot be changed but there are different ways in which MAC address of equipments could be changed whether it is a pc/laptop or mobile. We could use wire shark to know the changed MAC address of any system for which the packet is been send or received. The change in MAC is called MAC spoofing, which is having advantages as well as disadvantages.**

Index Terms— **MAC, NIC, ARP, LAN, IP, OS.**

I. Introduction

Media access control (MAC) stands for media access control. MAC addresses [1] are permanent addresses, which are assigned to every network connected devices. MAC address also is known as physical address, which is unique and cannot be changed. Computer network uses two types of addresses to deliver network data. The transmission control address or node address is use to differentiate between different nodes connected to transport medium segment. The transport protocol known as Ethernet uses a MAC 48-bit address (12- digit hexadecimal number) for this purpose. A MAC address usually encodes the manufacturer's registered identification number. It is also known as Ethernet hardware address (EHA), hardware address, adapter address, or physical address. The MAC protocol encapsulates a payload data by adding a 14- byte header protocol control information (PCI) before the data and appending a 4-byte cyclic redundancy check (CRC) after the data. The entire frame proceeds by a small idle period (the minimum inter-frame gap, 9.6 μs and an 8-byte preamble including the start of frame delimiter. The MAC address is the physical address of the machine, the physical identifier of the host on a segment. It needs to be unique only on a given segment. Theoretically two host could have same transport layer address provided they were not connected to the same network segment but both transport address and network address are two different things. In other words, we call network address as IP address, which is used as the unique identifier throughout the complete network, and it is statically defined 32-bit address. These network protocols are use to exchange data between different networks. MAC is assigned by the manufacturer and is burned into the ROM of the NIC card [2], which is a layer2 device of the OSI model [3]. This is divided into 24-bit vendor code and 24-bit serial address. These addresses are used as a network addresses for most IEEE 802 [4] network technologies, including Ethernet and Wi-Fi [5].

Konika abid , and M.Tech Student, CSE Deptt.from Meerut Institute of Engineering and Technology, Meerut, U.P, India.
Dr, Ajay Kumar,, Professor (CSE),Meerut Institute of Engineering & Technology, Meerut, U.P, India.

II. RULES FOR WRITING MAC ADDRESS

Institute of Electrical And Electronics Engineers (IEEE) manages MAC addressing rules. Three numbering spaces, managed by, are in common use for managing a MAC address: MAC-48, EUI-48, and EUI-64. Where, "EUI" stands for Extended Unique Identifier.

A. Notations for MAC Address

MAC address represented, in hexadecimal form. In these 12 hexa digits, starting 6 digits are Ethernet [6] interface given by IEEE and the last/right 6 digits which specify the interface serial number provided by the manufacturer. The Standard IEEE 802 format for printing MAC-48 addresses [7] is six groups of two hexadecimal digits separated by hyphens (-) or colon (:) in transmission order e.g. 01-12-23-34-56-AB.

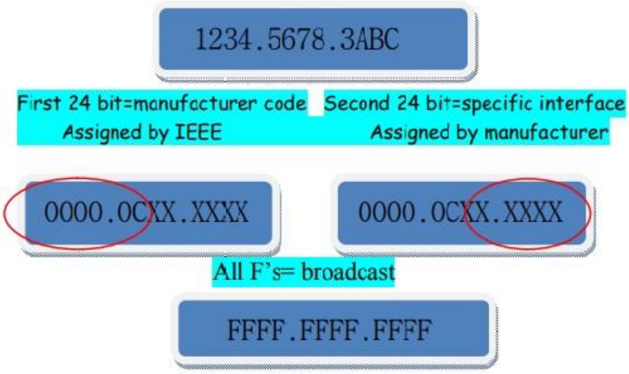


Fig. 1 Notation of MAC address.

This form is also commonly used for EUI-64. Other convention use three groups of four hexadecimal digits separated by dots (.) e.g. 0123.4567.89AB. Address either can be universally administered address or locally administered address. A universally administered address is uniquely assign to a device by its manufacturer, which is sometimes known as burned in address (BIA). The 48-bit address space contains potentially 248, 281, 474, 976, 710 or 656 possible MAC address.

III. TYPES OF MAC ADDRESSES

MAC addresses are mainly of two types:

A. Universal

B. Local

The manufacturer assigns the universally administrated address. The first three octets in transmission order identify the organization and is known as Organizationally Unique Identifier (OUI) the remaining octets are assigned by the manufacturer in any manner subject to the constraint of uniqueness. A network administrator, overriding the burned-in address, assigns a locally administered address to a device.

IV. . VULNERABILITIES WITH MAC ADDRESS

Even if the network is secure, enough then also the MAC address is send over the network regularly and some applications uses these to hack the network.

V. MAC SPOOFING

We have studied that MAC address are physical address, which cannot be change but there is a possibility to change the MAC address of almost every hardware. This process of changing the MAC address is known as MAC spoofing [8] which is different from that of IP spoofing [9] as in it the sender spoofs the receivers address as a request where as in this spoofing party gets the response

A. *Advantages of MAC Spoofing*

Some licenses are also hook up to specific MAC addresses so reverting the MAC address physical storage may help in using the software in simple words it can estimate the use of re-register the software. Perform security vulnerability testing, penetration testing on MAC address based authentication and authorization systems, i.e. wireless Access Points. It also helps in checking network management tools [10] and troubleshooting the system problems. Some Cable Modem Internet Service Provider assign IP addresses based on the device MAC addresses. For whatever reason, if you need to swap two systems regularly to connect to the cable modem, it would be a lot easier to change the MAC addresses rather than to change Network Interface Card (NIC). Test Intrusion Detection Systems (IDS) [11], whether they are Host and Network Based IDS.

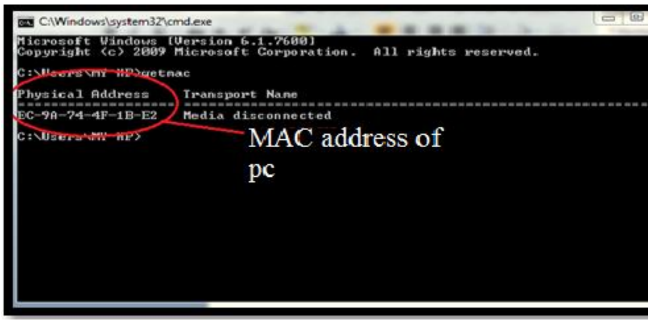
B. *Disadvantages of Spoofing MAC Address*

Now a day it is pretty simple to find the different wireless networks using our phones or laptops, so any unauthorized user could use MAC spoofing easily to get access to these networks depending on the level of security. It is possible to track illegal internet traffic to a specific IP• and to retrieve the name and address of the IP's registrant. MAC spoofing allows unauthorized access to someone else's network; therefore, responsibility for any illegal activity will fall on the authentic user. As a result, the real offender may go undetected by law enforcement.

VI. METHOD TO CHECK YOUR MAC ADDRESS

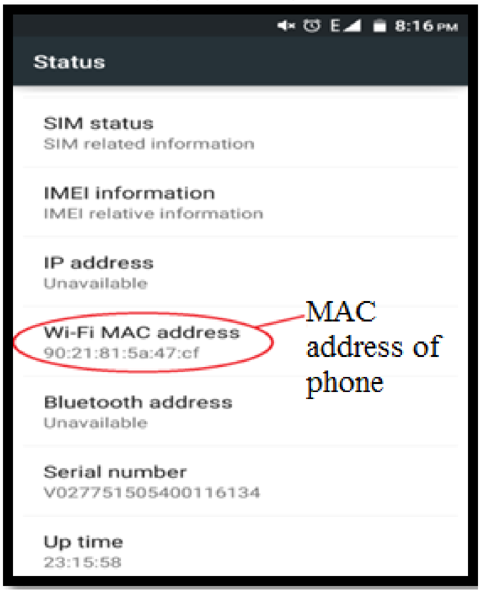
A. Checking of MAC address for the laptop or PC is shown in figure 2.

B. Checking of MAC address for the mobile is shown in figure 3.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\MY HP>getmac

Physical Address    Transport Name
=================== ==========================================
EC-9A-74-4F-1B-E2   Media disconnected

C:\Users\MY HP>
```

Fig. 2 Checking MAC address of laptop.



8:16 PM

Status

SIM status
SIM related information

IMEI information
IMEI relative information

IP address
Unavailable

Wi-Fi MAC address
90:21:81:5a:47:cf

Bluetooth address
Unavailable

Serial number
V027751505400116134

Up time
23:15:58

Fig. 3 Checking MAC address of mobile.

A. *Checking of MAC address in pc.*

Go to start and type cmd in search bar .

Write getmac and press enter. and colons.

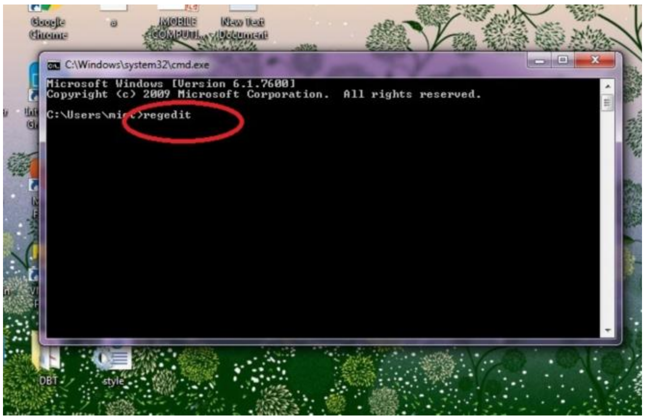
B. *Steps for checking MAC of mobile.*

Go to setting. Click about phone in system column.Now go to Status. In status, you will see Wi-Fi MAC address or the϶ MAC address of the mobile as shown in figure 3.

VII. SPOOFING/CHANGING MAC ADDRESS OF PC FOR WINDOWS

Following is the method by which MAC address of pc could be changed.

1) Open run dialog box and write REGEDIT.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\miet>regedit
```

FIG. 4 OPEN REGEDIT.

2) Open registry editor as shown in the figure 4 which allow changing the network cards settings.

3) Navigate the registry key, shown in figure 5:

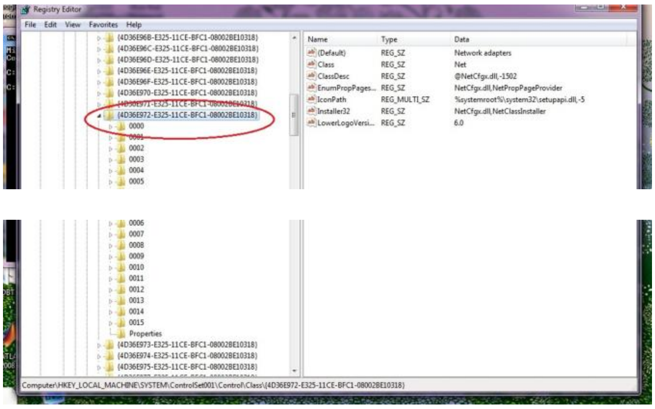
i. HKEY_LOCAL_MACHINESYSTEM
ii. CurrentControlSet
iii. Control
iv. Class
v. 4D36E972-E325-11CE-BFC1-08002BE10318

4) Open each folder one by one and check NetCfgInstanceID field and match it with the MAC address of your pc refer to figure 2 in above pages.

5) Right click on the folder that matches your device and then Select New → String Value. Name the new value "Network Address" as shown in figure 6.

6) Double-click the new Network Address entry. In the "Value data" field, enter your new MAC address. Note: MAC addresses should be of 12-digit and should be entered without any dashes or colons. For example, you would enter "2A1B4C3D6E5F" as given in figure 7.

7) Ensure that MAC should be formatted properly otherwise it is not accepted. DEXXXXXXXXXX



Registry Editor
File Edit View Favorites Help
{4D36E96B-E325-11CE-BFC1-08002BE10318}
{4D36E96C-E325-11CE-BFC1-08002BE10318}
{4D36E96D-E325-11CE-BFC1-08002BE10318}
{4D36E96E-E325-11CE-BFC1-08002BE10318}
{4D36E96F-E325-11CE-BFC1-08002BE10318}
{4D36E970-E325-11CE-BFC1-08002BE10318}
{4D36E971-E325-11CE-BFC1-08002BE10318}
{4D36E972-E325-11CE-BFC1-08002BE10318}
0000
0001
0002
0003
0004
0005
0006
0007
0008
0009
0010
0011
0012
0013
0014
0015
Properties
{4D36E973-E325-11CE-BFC1-08002BE10318}
{4D36E974-E325-11CE-BFC1-08002BE10318}
{4D36E975-E325-11CE-BFC1-08002BE10318}

Name	Type	Data
(Default)	REG_SZ	Network adapters
Class	REG_SZ	Net
ClassDesc	REG_SZ	@NetCfgx.dll,-1502
EnumPropPages...	REG_SZ	NetCfgx.dll,NetPropPageProvider
IconPath	REG_MULTI_SZ	%systemroot%\system32\setupapi.dll,-5
Installer32	REG_SZ	NetCfgx.dll,NetClassInstaller
LowerLogoVersi...	REG_SZ	6.0

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}

Fig. 5 Navigating registry key.

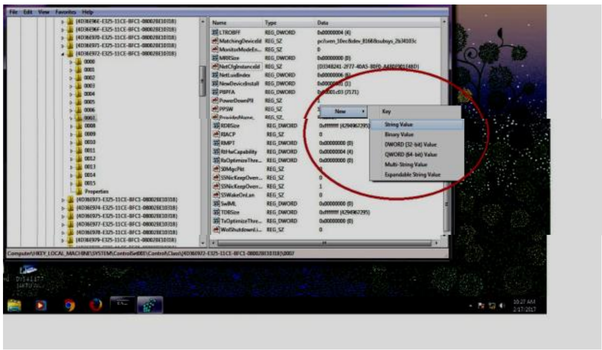
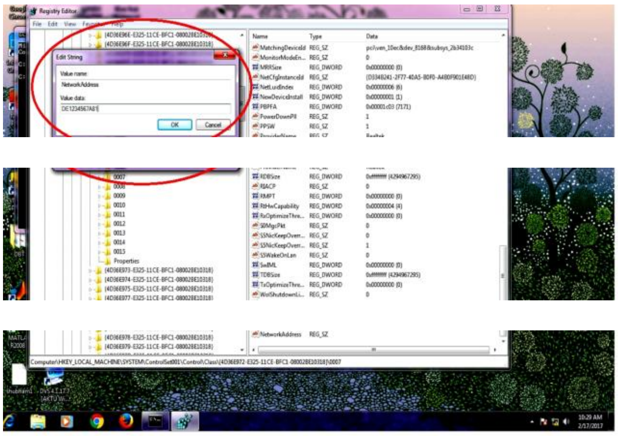


Fig. 6 Opening string value

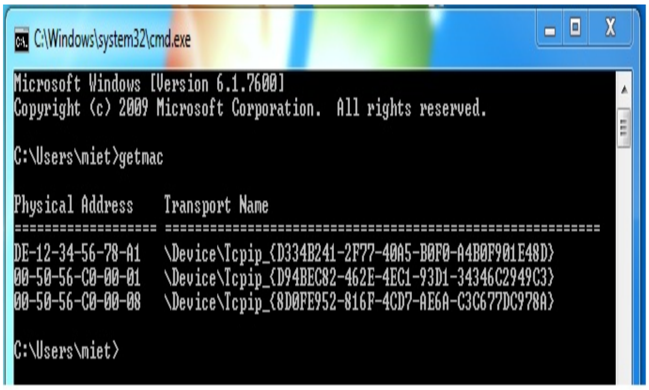


Edit String
Value name:
NetworkAddress
Value data:
DE1234567A81

Name	Type	Data
MatchingDeviceId	REG_SZ	pci\ven_10ec&dev_8168&subsys_2b34103c
MonitorModeEn...	REG_SZ	0
MRRSize	REG_DWORD	0x00000000 (0)
NetCfgInstanceId	REG_SZ	{D334B241-2F77-40A5-B0F0-A4B0F901E48D}
NetLuidIndex	REG_DWORD	0x00000006 (6)
NewDeviceInstall	REG_DWORD	0x00000001 (1)
PBPFA	REG_DWORD	0x00001c03 (7171)
PowerDownPll	REG_SZ	1
PPSW	REG_SZ	1
ProviderName	REG_SZ	Realtek
RDBSize	REG_DWORD	0xffffffff (4294967295)
RIACP	REG_SZ	0
RMPT	REG_DWORD	0x00000000 (0)
RtHwCapability	REG_DWORD	0x00000004 (4)
RxOptimizeThre...	REG_DWORD	0x00000000 (0)
S0MgcPkt	REG_SZ	0
S5NicKeepOverr...	REG_SZ	0
S5NicKeepOverr...	REG_SZ	1
S5WakeOnLan	REG_SZ	0
SwIML	REG_DWORD	0x00000000 (0)
TDBSize	REG_DWORD	0xffffffff (4294967295)
TxOptimizeThre...	REG_DWORD	0x00000000 (0)
WolShutdownLi...	REG_SZ	0
NetworkAddress	REG_SZ	

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0007

Fig. 7 Assigning MAC value

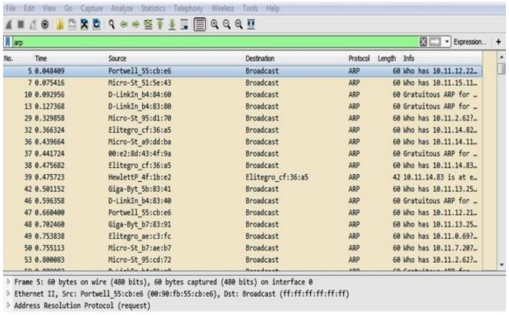


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\miet>getmac

Physical Address    Transport Name
=================== ==========================================================
DE-12-34-56-78-A1   \Device\Tcpip_{D334B241-2F77-40A5-B0F0-A4B0F901E48D}
00-50-56-C0-00-01   \Device\Tcpip_{D94BEC82-462E-4EC1-93D1-34346C2949C3}
00-50-56-C0-00-08   \Device\Tcpip_{8D0FE952-816F-4CD7-AE6A-C3C677DC978A}

C:\Users\miet>
```

Fig. 8

VIII. MAPPING MAC ADDRESS WITH THE HELP OF WIRESHARK

To check our MAC address using WIRESHARK, we follow the following steps: Firstly Start capturing the packets. Then Stop capturing the packets. Apply ARP filter shown in figure 9.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Expression...
+

No.	Time	Source	Destination	Protocol	Length	Info
5	0.048409	Portwell_55:cb:e6	Broadcast	ARP	60	Who has 10.11.12.22…
7	0.075416	Micro-St_51:5e:43	Broadcast	ARP	60	Who has 10.11.15.11…
10	0.092956	D-LinkIn_b4:84:60	Broadcast	ARP	60	Gratuitous ARP for …
13	0.127368	D-LinkIn_b4:83:80	Broadcast	ARP	60	Gratuitous ARP for …
29	0.329858	Micro-St_95:d1:70	Broadcast	ARP	60	Who has 10.11.2.62?…
32	0.366324	Elitegro_cf:36:a5	Broadcast	ARP	60	Who has 10.11.14.82…
36	0.439664	Micro-St_a9:dd:ba	Broadcast	ARP	60	Who has 10.11.14.11…
37	0.441724	00:e2:8d:43:4f:9a	Broadcast	ARP	60	Gratuitous ARP for …
38	0.475682	Elitegro_cf:36:a5	Broadcast	ARP	60	Who has 10.11.14.83…
39	0.475723	HewlettP_4f:1b:e2	Elitegro_cf:36:a5	ARP	42	10.11.14.83 is at e…
42	0.501152	Giga-Byt_5b:83:41	Broadcast	ARP	60	Who has 10.11.13.25…
46	0.596358	D-LinkIn_b4:83:40	Broadcast	ARP	60	Gratuitous ARP for …
47	0.660400	Portwell_55:cb:e6	Broadcast	ARP	60	Who has 10.11.12.21…
48	0.702460	Giga-Byt_b7:83:91	Broadcast	ARP	60	Who has 10.11.13.25…
49	0.753838	Elitegro_ae:c3:fc	Broadcast	ARP	60	Who has 10.11.0.69?…
50	0.755113	Micro-St_b7:ae:b7	Broadcast	ARP	60	Who has 10.11.7.207…
53	0.800083	Micro-St_95:cd:72	Broadcast	ARP	60	Who has 10.11.2.62?…

```
> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Portwell_55:cb:e6 (00:90:fb:55:cb:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

Fig. 9 ARP filters applied on packets.

You will receive all the ARP packets as the output. Now select any of the packets.

You will see its destination and source details in the address resolution column.

There you will see the MAC address of the source as well as of the target. For example, see figure 10 for understanding this concept.

A. *Before Spoofing*

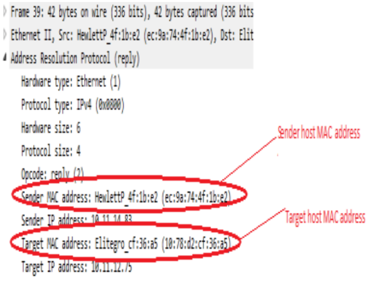
1) We have already checked our MAC address and have changed it .We can analyse our MAC as well as the IP address with the help of wireshark. To perform this we ping our system from example, you would enter "2A1B4C3D6E5F" as given in figure 7.
2) Ensure that MAC should be formatted properly otherwise it is not accepted.

DEXXXXXXXXXX

another system and analyse these packets in wireshark.We simplified our work by applying filter ICMP as shown in figure 11. Once we apply this filter we find all the ICMP packets at once and can easily search our ping request packet.

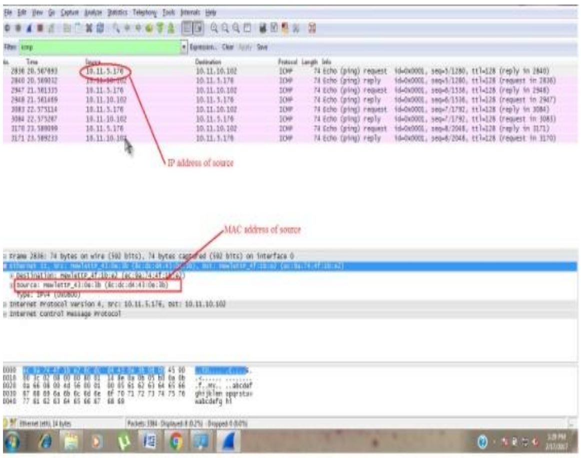
B. *After spoofing*

We see that when we again ping our system from another system and repeats the same process. Our IP address remains the same where as the MAC changes as shown in figure 12.



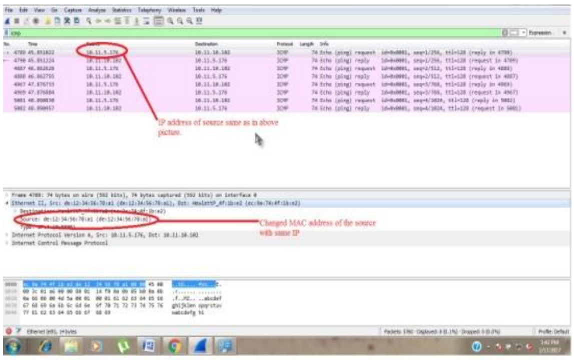
```
Frame 39: 42 bytes on wire (336 bits), 42 bytes captured (336 bits
Ethernet II, Src: HewlettP_4f:1b:e2 (ec:9a:74:4f:1b:e2), Dst: Elit
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HewlettP_4f:1b:e2 (ec:9a:74:4f:1b:e2)
    Sender IP address: 10.11.14.83
    Target MAC address: Elitegro_cf:36:a5 (10:78:d2:cf:36:a5)
    Target IP address: 10.11.12.75
```

Fig. 10 Address resolution column with MAC address.



```
Filter: icmp
No.  Time       Source        Destination   Protocol Length Info
2836 20.507893  10.11.5.176   10.11.10.102  ICMP     74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 2840)
2840 20.509032  10.11.10.102  10.11.5.176   ICMP     74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=128 (request in 2836)
2947 21.501335  10.11.5.176   10.11.10.102  ICMP     74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 2948)
2948 21.501469  10.11.10.102  10.11.5.176   ICMP     74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=128 (request in 2947)
3083 22.575114  10.11.5.176   10.11.10.102  ICMP     74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 3084)
3084 22.575267  10.11.10.102  10.11.5.176   ICMP     74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=128 (request in 3083)
3170 23.589099  10.11.5.176   10.11.10.102  ICMP     74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 3171)
3171 23.589233  10.11.10.102  10.11.5.176   ICMP     74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=128 (request in 3170)

Frame 2836: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HewlettP_43:0e:3b (8c:dc:d4:43:0e:3b), Dst: HewlettP_4f:1b:e2 (ec:9a:74:4f:1b:e2)
    Destination: HewlettP_4f:1b:e2 (ec:9a:74:4f:1b:e2)
    Source: HewlettP_43:0e:3b (8c:dc:d4:43:0e:3b)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.11.5.176, Dst: 10.11.10.102
Internet Control Message Protocol
```

Fig. 11 ICMP packets with both IP and MAC addresses.



```
Frame 4789: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: de:12:34:56:78:a1 (de:12:34:56:78:a1), Dst: HewlettP_4f:1b:e2 (ec:9a:74:4f:1b:e2)
    Source: de:12:34:56:78:a1 (de:12:34:56:78:a1)
Internet Protocol Version 4, Src: 10.11.5.176, Dst: 10.11.10.102
Internet Control Message Protocol
```

IP address of source same as in above picture.
Changed MAC address of the source with same IP

Fig. 12 Same IP addresses with change MAC address.

IX. Conclusion

In this paper, we have discussed about the MAC address also known as physical address, which is permanent, but it can be altered virtually. By following the methods discussed above we can we can compare both the MAC and could generate the beep or alert message.

This spoofed address could be detected by the WIRESHARK easily. We can detect the changes done in MAC address and accordingly we can take preventive steps.

X. Acknowledgment

We are thankful to our management and Chairman for his kind support and motivation.

References

[1]. Deepak gupta, Gaurav tiwari, Yachin kapoor and Praveen kumar, "media access control (mac) mac spoofing and is countermeasure", International Journal of Recent Trends in Engineering, Vol. 2, No. 4, pp.17-21, November 2009.

[2]. W. Feng., "Network interface cards as first-class citizens", Invited Talk, The Ohio State University, 1999.

[3]. Sumit Kumar, Sumit Dalal and Vivek Dixit, "The OSI Model: Overview On The Seven Layers Of Computer Networks", International Journal of Computer Science and Information Technology Research Vol. 2, Issue 3, pp. 461-466, July -September 2014.

[4]. Jasleen Kaur and Shakti Nagpal, "Review Paper on Comparative Study of IEEE Protocols Suite", International Journal of Advanced Research in Computer Science and Software Engineering, 2014, Vol. 4, pp. 1490-1500, 5 May 2014.

[5]. Mathieu Cunche, "I know your MAC Address:Targeted tracking of individual using Wi-Fi", HAL Id: hal-00858324 https://hal.inria.fr/hal-00858324, 3 October 2013.

[6]. Bruce Lowekamp, David R. O'Hallaron and Thomas R. Gross. "Topology Discovery for Large Ethernet Networks", In Proceedings of ACM SIGCOMM, August 2001.

[7]. Umang Garg, Pushpneel Verma ,Yudhveer Singh Moudgil and Sanjeev Sharma, "MAC and Logical addressing (A Review Study)", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp. 474-480.

[8]. Mrs. Hatkar Archana A., Ms. Varade Gauri A. and Mr. Hatkar Arvind P, "Media Access Control Spoofing Techniques and its Counter Measures", International Journal of Scientific & Engineering Research, Vol. 2, pp.1-5, 6 June 2012.

[9]. Sharmin Rashid and Subhra Prosun Paul, "Proposed Methods of IP Spoofing Detection & Prevention" , International Journal of Science and Research (IJSR), Vol. 2, Issue 8, pp. 438-443, August 2013.

[10]. G.S. Nagaraja, Ranjana R.Chittal, Kamod Kumar, "Study of Network Performance Monitoring Tools-SNMP", IJCSNS International Journal of Computer Science and Network Security, Vol.7, No.7, pp. 1-5, July 2007.

[11]. Nicholas, J.Puketza, Kui Zhang,Mandy Chung, Biswanath Mukherjee and Ronald A.Olsson, "A Methodology for Testing Intrusion Detection System", National Security Agency INFOSEC University Research Program,17th National Computer Security Conference in Baltimore, MD, pp. 1-25 ,October 1994.

[12]. http://www.wikihow.com/Change-a-Computer's-Mac-Address-in-Windows

KONIKA ABID: She have done b.tech from Subharti University and M.Tech Student, CSE Deptt.from Meerut Institute of Engineering and Technology,Meerut, U.P, India.

Dr. Ajay Kumar Singh: Born in 1974 at Dhanbad (Jharkhand), India. He had done B.E (Computer Science & Engg.) from Kumaon Engineering College, M. Tech (I.T) Allahabad, Ph. D (Computer Science & Engg.) Jaypee University of Information Technology. **Work Experience:** He had been in different institution / university like Radha Govind Engineering College, Meerut, (U.P) here he worked as HoD, Sir Padampat Singhania University, Bhatewar, Udaipur, Rajasthan, Jaypee University of Information Technology, Waknaghat, Solan (H.P), Mody College of Engineering and Technology, Lakshmangarh, Sikar, Rajasthan, Regional Engineering College (Now N.I.T.) Kurukshetra (Haryana), Software Solution Integrated Ltd. (Delhi). Now he is working with MIET, Meerut, U. P. He has published many papers in international Journals like PIER, Asia Magazine EFY Elsevier, many papers in international Conference out of which 4 of them in IEEE, He has chaired two IEEE conference at ABES Engg. College and Galghotia University. Published paper in Electronic For You, Springer LNCS and presented his papers at several places like Bangalore, Pune, IT B.H.U, USA (Washington DC).

.