A Progressive Approach Towards Securing Hospital Networks from Packet Sniffing Using Wireshark

Rudranil Maity and Rajdeep Chakraborty

March 13, 2022

A PROGRESSIVE APPORACH TOWARDS SECURING HOSPITAL NETWORKS FROM PACKET SNIFFING USING WIRESHARK

Rudranil Maity
Netaji Subhash Engineering College
Department of Computer Science
Kolkata-700152, India
rudranilmaity01@gmail.com

Rajdeep Chakraborty
Netaji Subhash Engineering College
Department of Computer Science
Kolkata-700152, India
rajdeep.chakraborty@nsec.ac.in

***Abstract* -** In recent times, we have been facing serious security breaches in computer-based hospital database systems, carried by the drastic growth in use of the internet and mobile devices. In this context, 'Packet Sniffing' can be mentioned as one of the most important terms. This is the technique/attack through which data, flowing as data-packets across the network can be detected and monitored. Some types of this attack; applied on a large range of data transmission are MAC (Media Access Control) Flooding, DHCP (Dynamic Host Configuration Protocol) attacks, Rogue DHCP server attack, DHCP starvation attack, ARP (Address Resolution Protocol) Spoofing, DNS (Domain Name Server) Poisoning, MAC spoofing **[1].** In this paper, a demonstration has been discussed on how packet sniffing works by using Wireshark; widely used packet sniffing tool and its effect on our healthcare systems followed by the ways to get protected from this kind of malicious attacks in the cyber world.

Keywords – Packet Sniffing, MAC, DHCP, ARP, DNS, Wireshark, hospital network security.

1. Introduction

Because of a broad area which could be attacked through web and poor security systems, the healthcare industry has seen a hike in cyber-attacks in recent times. As an example; over 70% of the hospitals in United States took this under their threat management protocols. It is clear from statistical data that hospitals that, user consents are needed and also, a pressurized situation should be created by the board of director; which will drive the hospitals to undertake substantiative cybersecurity protocols **[2]**.

Despite these, massive amount of data breaches is happening every day in the world. Most of the attacks are done through MITM attacks, like packet sniffing.

If we want to take a look into large industries, many organizations use hubs in their infrastructure to connect a chain of internal network with outer networks. These systems are quite vulnerable towards passive sniffing; which is extremely difficult to uncover. Hackers target these systems many times; to see and capture on all the traffic flowing through the system.

Table.1: Approximate losses due to web attacks up to 2020

Year	Approx. amount of losses
2018	$8 Billion
2019	$11.5 Billion
2020	$20 Billion

Table.1 shows the numerous amounts of net losses worth money due to cyber breaches and malicious attacks over years 2018 to 2020; in not only hospitality systems but also other affected fields too. From this we can understand how dangerous this issue has become and how important the study about cybersecurity is.

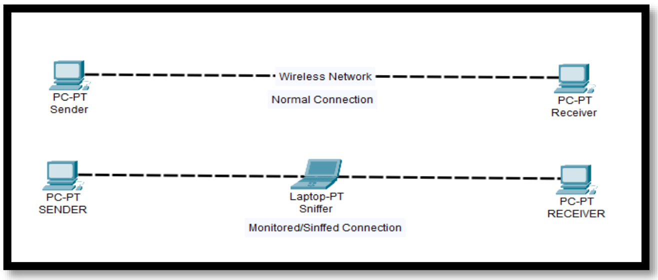


Fig.1: Displayed the structure of packet sniffing

The above shown diagram(fig.1) demonstrates the basic mechanism of packet sniffing techniques; which is the prime topic of this paper; used by network operators for managing network traffic or in malicious activities like overlooking on personal data by hackers. This overlooking, i.e., the process of packet sniffing gets chance to be done when data, which flows as data packets, are captured by the network administrators and in case of malicious activity, hackers. The process of data transferring can be demonstrated as: while being transferred to destinations, data packets break into smaller pieces and then reform at the end. This can be described more intensely with the example slow loading of images in a slow network when pixels of the images don't get emerged at once, instead of that they slowly emerge in steps; which means data is being delivered to the destination slowly.

Control information and user data stored in data packets help them to reach the desired destination. The data packets with no intended destinations, mainly broadcasted data packets, bring the best help to the administrators to monitor the network because the data packets with certain information only get delivered to their selected destination, making them less important in case of studying and network monitoring **[3].**

Section 2 discusses about the history of security breaches. Then section 3 describes the prerequisites of packet sniffing. After that, section 4 discusses the working mechanism of Wireshark. Following that, section 5 demonstrates the process through which data is being leaked. Then section 6 discusses the ways to get secured from packet sniffing and section 7 gives us the conclusion of the paper. References are listed in the last.

2. History of Security Breaches in Hospitals

Containing a sheer difference to real world wars; in cyber-attacks; hackers have no such scruples about their targets. According to John Halamka, CIO of the Boston hospital Beth Israel Deaconess; we're being attacked digitally on almost every moment and the attackers are organized criminals, cyberterrorists and even MIT students.

Some of the major and most horrifying hospital hacks from recent times were discussed by Kevin Fu, a professor at University of Michigan, who studies medical device security: at a conference about hacking incidents in medical industry.

1. Once a system in China was so contaminated with malware that, x-ray data of over 2000 patients were stolen within moments.
2. In 2014, Boston Children Hospital faced a DDoS attack which was used to steal data of a controversial and important patient.
3. Various cases of fake websites are being deployed daily, which lures doctors and patients in buying gift card etc. and then stealing their personal data.
4. **The lure of angry birds:** This intrusion took place when a nurse at Beth Israel Deaconess downloaded the 'angry bird' game, but from a Bulgarian website which came with a malware which stole her email credentials when she logged in into that game.
5. **Pay up or else**: This is basically cyber-blackmailing, which is a seriously growing threat and applies to not only hospital industries but also other fields too. In this case, hackers breach into a computer network and block access or encrypt the personal data of individuals linked to that network. Then they blackmail people and demand ransoms in exchange to not release the data **[4]**.

All these histories point us at some seriously growing issues of web attacks and our topic of discussion: Packet Sniffing; is one of the very dangerous kind of threats.

The first network monitors and packet sniffer devices were LANalyser and Microsoft Network Monitor. These devices could capture data packets and once that is done; the population in the network segments could be seen and also, analyzing in details to examine the network problems was possible. Over time, new programs, with more functions and updated settings, with the capability to sniff over networks and decipher communication exchanges, were developed. But, with developing technologies and increasing ease of access; some network monitors and packet sniffers started using their skills in a wrong way; by attacking network and deploying schemes to steal information which were meant to be secured. Although some precautions like, using multiple switches within network, rather than hubs. As this technique limits data packets from travelling across multiple interfaces; it has been proved as a reducer to the threat of successful web-attacks. **[5].**

This section gives us a list of the most used network protocol analyzers: 1. Wireshark, 2. SolarWinds Network Performance Monitor, 3. Paessler PRTG Network Monitor, 4. ManageEngine NetFlow Analyzer, 5. Savvius Omnipeek, 6. tcpdump, 7. WinDump, 8. Telerik Fiddler, 9. NETRESEC Network Miner, 10. Colasoft Capsa **[6].**

In this paper, mainly the functionalities and working mechanisms of Wireshark will be discussed.

In this section we will see the progressive history of Wireshark. It runs on almost every computing platform including Windows, OS X, Linux, and UNIX and it is used globally by Network professionals, security experts, developers, and educators in a regular manner. It is an open-source software, and is released under the "GNU General Public License version 2". It has been developed and maintained by a global team of protocol experts, and it is an example of a disruptive technology. Wireshark formerly used to be known as Ethereal which was released in 1998 by a Gerald Combs, computer science graduate from University of Missouri-Kansas City who was working on an internet service provider system. was working on a small ISP. But from June 2006 it was renamed because of trademark issues. The use of Wireshark can be divided into two categories: firstly; it is used for troubleshooting by network engineers and secondly; it is used widely for studying and analysing the characteristics and behaviours of networks and data packets. It is also used for developing new protocols which help in improving quality of networks. With reference to Banerjee, Ashutosh and Saxena **[7]**; with the appropriate driver support, Wireshark can capture traffic "from the air" and decode it into a format that helps administrators track down issues that are causing poor performance, intermittent connectivity, and other common problems.

3. Packet Sniffing Prerequisites

Some common rules which can be stated as the prerequisites of packet sniffing. As we're using Wireshark to demonstrate the procedures, prerequisites of using Wireshark are as follows;

We have to be ensured that, we are permitted to capture data packets from the specific network. As an example, corporate policies or applicable laws might prevent capturing if the site is not permitted to be sniffed.

If the network cabling needs to be changed to start a capture, we need to be authorized for that too because a network operator would not want the network configurations to be changed for obvious reasons

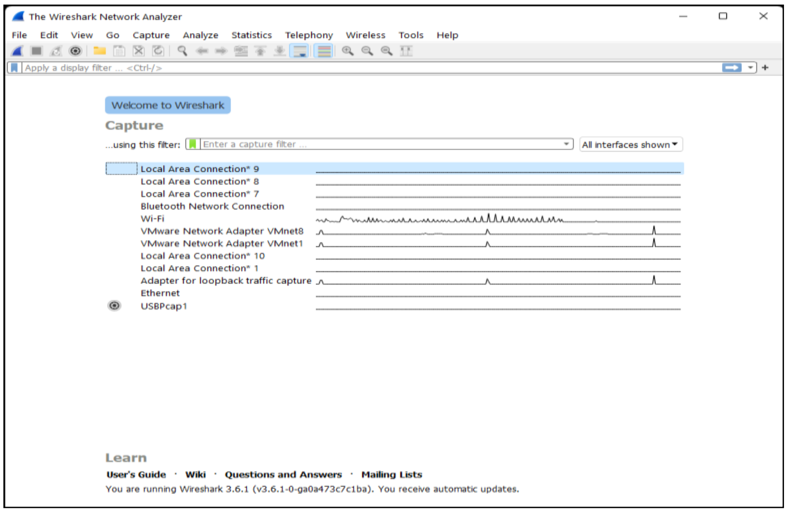
Some common pitfalls during the process of packet sniffing are:

1. Some networks or tools might require special privileges to monitor on data packets.
2. We have to choose the right network to sniff on data or the process can get failed or might led to get distorted results. **[8]**.

4. Working Mechanism of Wireshark

Wireshark is one of the most popular network protocol analyzers being used in recent times. It works similarly to TcpDump, which is a common packet analyzer. Various network taps or port monitoring can be also used by Wireshark.

In this paper, the working mechanism of Wireshark is being shown step-by-step.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

...using this filter: Enter a capture filter ... All interfaces shown

Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Bluetooth Network Connection
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 10
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
USBPcap1

You are running Wireshark 3.6.1 (v3.6.1-0-ga0a473c7c1ba). You receive automatic updates.

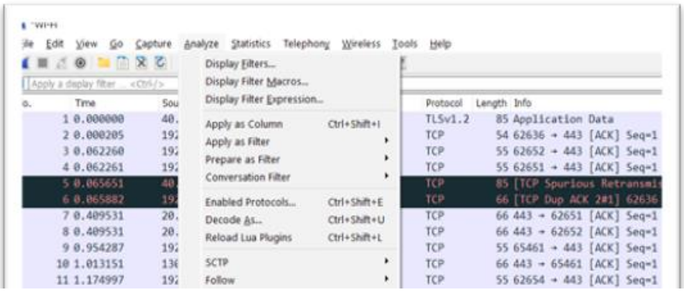
Fig.2: Displayed the Wireshark welcome window

Keeping an eye on Fig.2; it can be demonstrated as: all the network interfaces, as well as usb-connected devices are being shown through the linear graphs which also shows packet losses. Packet loss is an incident when data packets get failed to reach their destination.

Packet loss generally doesn't happen to cabled networks. Its main reasons are slow wi-fi connections, traffic in network, sudden changes in power input, non-functioning routers etc.

By using the 'capture' option in the menu, we can start capturing the data packets flowing through the selected network. Data packets, which are basically smaller pieces of data which are being sent from the sender to the receiver, can be captured mid-way by this tool. By packet capturing, network administrators monitor the data flow across the network when some problem occurs in the connection.

Data packets can be prefiltered if needed to be captured by using the "apply this filter" option. In this context, the name of "Display Filter Macros" can be mentioned, which is a mechanism to create shortcuts for complex filters. As an example, when we're trying to define a specific data packet, we can just use this function instead of writing down the whole protocol. Thus, ease of access increases for defining specific data packets and in the other hand the complexity is decreased and time is saved.


*Wi-Fi
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As... Ctrl+Shift+U
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow

o.	Time	Sou	Protocol	Length	Info
1	0.000000	40.	TLSv1.2	85	Application Data
2	0.000205	19:	TCP	54	62636 → 443 [ACK] Seq=1
3	0.062260	19:	TCP	55	62652 → 443 [ACK] Seq=1
4	0.062261	19:	TCP	55	62651 → 443 [ACK] Seq=1
5	0.065651	40	TCP	85	[TCP Spurious Retransmi
6	0.065882	19:	TCP	66	[TCP Dup ACK 2#1] 62636
7	0.409531	20.	TCP	66	443 → 62651 [ACK] Seq=1
8	0.409531	20.	TCP	66	443 → 62652 [ACK] Seq=1
9	0.954287	19:	TCP	55	65461 → 443 [ACK] Seq=1
10	1.013151	13(	TCP	66	443 → 65461 [ACK] Seq=1
11	1.174997	19:	TCP	55	62654 → 443 [ACK] Seq=1

Fig.3: Displayed the selection of Display Filter Marcos

As displayed in Fig.3; Display Filter Macros can be managed and organized in various ways from the dropdown menu of Wireshark **[9].** This feature can be used as a customized marker for patient data, i.e., can be used with certain colors for certain data columns.

Wireshark can also be launched from the command line interface of the specific device. By using the command: wireshark -h; we can view the various kinds of parameters supported by Wireshark. To start capturing the data packets flowing through the network, we have to select the preferred network and click "capture". In the image shown below, the captured data are being show

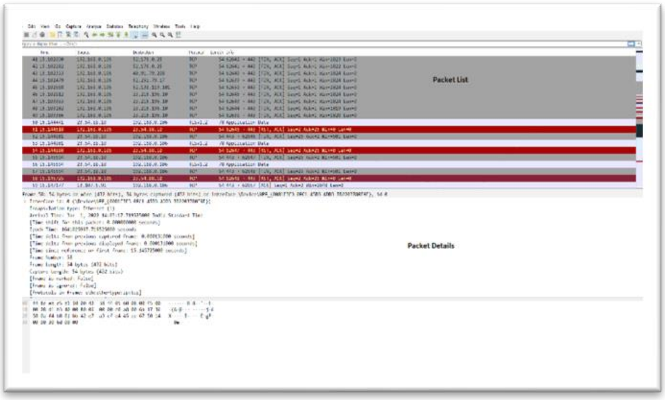


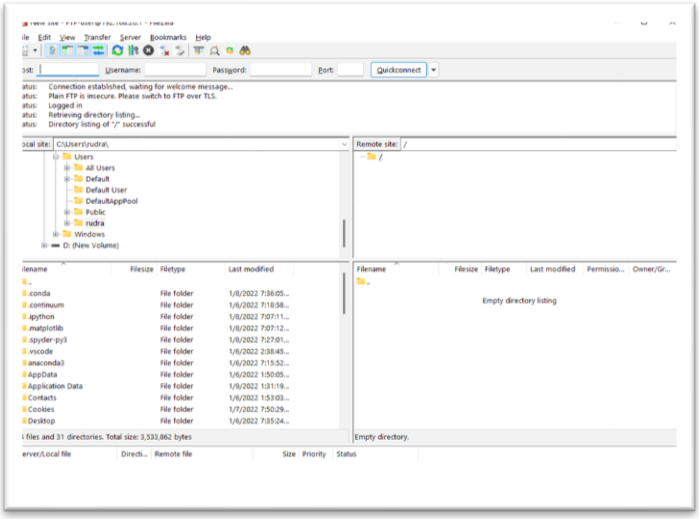
Fig.4: Displayed various kind of data packets

In the tables shown in Fig.4, we can see the captured data packets and their desired destinations. In the protocol column, we can see the various types of network protocols. As an example: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), TLSv1.2(Transport Layer Security), mDNS (Multicast Data Network Service), ARP (Address Resolution Protocol) etc.

The ‘information’ column contains the detailed description of each data packets. We can also select one data packet and see the more detailed description of that specific one by double clicking on it or one minimized view is shown just below the data packets list.

5. Sniffing on The User Credentials

Wireshark can be used to capture usernames and passwords sent through an FTP server by a user. As we all know, nowadays in the databases of the hospitals, everyone’s data gets stored through credentials like username/email id and password. A hacker can sniff on these databases and might cause a breach and leak user data, which can be very vulnerable to the management system. That’s why it’s important to know about these in case of gaining knowledge on network security.



```
atus:    Connection established, waiting for welcome message...
atus:    Plain FTP is insecure. Please switch to FTP over TLS.
atus:    Logged in
atus:    Retrieving directory listing...
atus:    Directory listing of "/" successful
```

ocal site: C:\Users\rudra\

- Users
  - All Users
  - Default
  - Default User
  - DefaultAppPool
  - Public
  - rudra
- Windows
- D: (New Volume)

Remote site: /

- /

ilename	Filesize	Filetype	Last modified
..			
.conda		File folder	1/8/2022 7:36:05...
.continuum		File folder	1/6/2022 7:18:58...
.ipython		File folder	1/8/2022 7:07:11...
.matplotlib		File folder	1/8/2022 7:07:12...
.spyder-py3		File folder	1/8/2022 7:27:01...
.vscode		File folder	1/6/2022 2:38:45...
anaconda3		File folder	1/6/2022 7:15:52...
AppData		File folder	1/6/2022 1:50:05...
Application Data		File folder	1/9/2022 1:31:19...
Contacts		File folder	1/6/2022 1:53:03...
Cookies		File folder	1/7/2022 7:50:29...
Desktop		File folder	1/6/2022 7:35:24...

files and 31 directories. Total size: 3,533,862 bytes

Filename	Filesize	Filetype	Last modified	Permissio...	Owner/Gr...
..					

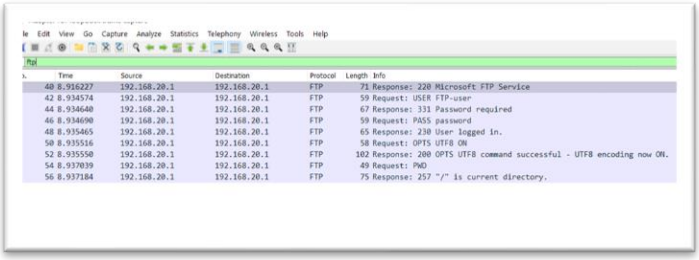
Empty directory listing

Empty directory.

erver/Local file	Directi...	Remote file	Size	Priority	Status

Fig.5: Displayed the connection with the FTP server

In the above shown diagram (Fig.5), an FTP server connection has been established and the user has been connected with username and password. Now it can be shown that, passwords, usernames or similar important information can be captured through packet sniffing if passed through this kind of networks.



ftp

.	Time	Source	Destination	Protocol	Length	Info
40	8.916227	192.168.20.1	192.168.20.1	FTP	71	Response: 220 Microsoft FTP Service
42	8.934574	192.168.20.1	192.168.20.1	FTP	59	Request: USER FTP-user
44	8.934640	192.168.20.1	192.168.20.1	FTP	67	Response: 331 Password required
46	8.934690	192.168.20.1	192.168.20.1	FTP	59	Request: PASS password
48	8.935465	192.168.20.1	192.168.20.1	FTP	65	Response: 230 User logged in.
50	8.935516	192.168.20.1	192.168.20.1	FTP	58	Request: OPTS UTF8 ON
52	8.935550	192.168.20.1	192.168.20.1	FTP	102	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
54	8.937039	192.168.20.1	192.168.20.1	FTP	49	Request: PWD
56	8.937184	192.168.20.1	192.168.20.1	FTP	75	Response: 257 "/" is current directory.

Fig.6: Displayed the captured credentials

As it can be seen on Fig.6, the steps of the connection, i.e., the outputs which the user has seen is captured as data packets. The username and password, given as input, can be seen through packet capturing. In the fourth row, the password: “password” is displayed while being sent to the source to the destination IPv4. Similarly in the second column the username: “FTP-user” can be seen being sent through the network. All these packets captured, comes under FTP connections. The above discussed scenario can be said as a classic example of data breach. And surprisingly, this is the scenario which mostly happens in the healthcare system breaches due to lack of security and as a result of using backdated hardware and software.

According to the Protenus Breach Barometer, 503 security breaches happened and the data of over 15 million people was compromised, singly in 2018, three times the amount seen in 2017. But just after passing the half of 2019, the numbers increased dramatically over 25 million. Our modern healthcare system has faced massive data breaches. From each of the 10 largest recorded, over 200,000 records breached for each. The worst part is that, some of the victim healthcare systems failed to report within the HIPAA (Health Insurance Portability and Accountability Act) within mandated time period of 60 days; and in case of the others, it went on for a long time. MITM (Man In The Middle) attacks like packet sniffing and phishing were behind these breaches. In context to this; the investigations into the largest vendor breach is still ongoing. The scary truth is that, the number of data breaches and third-party attacks through packet sniffing are increasing day by day **[10]**.

6. Getting Secured

As this is considered as a major and growing threat, we must know the basic ways to get secured from these attacks. Being able to be used by both as ethically and unethically working individuals, hackers might cause a threat to our healthcare systems by using the process of MITM attacks, like packet sniffing, which is described previously. That’s why we need to get some concepts about getting protected as precautions; keeping in the prime fact that the hospitals should upgrade their computer hardware and software as backdated PCs are more vulnerable. Some of the other important steps that can be taken are as listed **[11]**:

A. Using of end-to-end encryption and ‘Secure File Transfer Protocol’ will decrease number of breaches in transfer of files and personal data.

B. WPA and WPA2 are strong encryption protocols. And SSH and SCP can be listed as encrypted sessions. If they are used in networks the data will get more secured in traffic.

C. Avoiding broadcast of SSID (Session Set Identifier).

D. Access Control List can be used in specific networks. This will allow only selected IP addresses to get passed through it, which will increase security.

E. As mentioned earlier, large organizations use hubs to make a interconnected network which creates the possibility of passive sniffing. Instead of hubs, if the companies use switch, then the system will be more secured as only specified IP addresses will get access to the data.

F. ARP tables and static IP addresses can be used to prevent ARP spoofing into networks.

G. Using PGP and S/MIME, VPN, IPSec, SSL/TLS, and one-time passwords (OTP).

7. Conclusion:

Using Wireshark, we can monitor data packets through a network by packet sniffing and on the other hand, web attacks can also be generated. In this paper, a detailed introduction and history of security breaches in hospital management systems and a brief description about Wireshark has been given based on packet sniffing. Then we have discussed the functionalities and working mechanism and prerequisites of using this this tool in details. We have also given a detailed result through diagrams on detecting and capturing data packets using Wireshark, of various protocols like, FTP, TCP, UDP, TLSv1.2, MDNS and ARP. Thus, our paper has given a comprehensive approach to protect hospital networks from web attacks like packet sniffing through the Wireshark tool.

In future, we would like to develop a new model dedicated towards secured communication line of communication ports against sniffing, phishing and Trojan attacks; which will be beneficial for the hospitals, using vulnerable systems.

References

1. Anu, P. & Vimala, S. (2017): “A survey on sniffing attacks on computer networks”; 2017 International Conference on Intelligent Computing and Control (I2C2) 1-5. 10.1109/I2C2.2017.8321914.
2. Jalali, Mohammad S, and Jessica P Kaiser. “Cybersecurity in Hospitals: A Systematic, Organizational Perspective.” *Journal of medical Internet research* vol. 20,5 e10059. 28 May. 2018, doi:10.2196/10059
3. Liveaction.com: Information about Packet Capturing: https://www.liveaction.com/resources/blog/what-is-packet-capture/
4. Eliza Strickland: “5 Major Hospital Hacks: Horror Stories from the Cybersecurity Frontlines” - https://spectrum.ieee.org/5-major-hospital-hacks-horror-stories-from-the-cyber-security-frontlines
5. UKEssays. November 2018. The History of Packet Sniffing Information Technology Essay. [online]. Available from: https://www.ukessays.com/essays/information-technology/the-history-of-packet-sniffing-information-technology-essay.php?vref=1 [Accessed 11 January 2022].
6. Dnsstuff.com: Best 10 packet sniffer and capture tools: https://www.dnsstuff.com/packet-sniffers
7. Banerjee, Usha & Ashutosh, Vashishtha & Mukul, Saxena. (2010): “Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection”. International Journal of Computer Applications. 6. 10.5120/1092-1427. Wireshark Foundation: “How to set up a capture”. https://gitlab.com/wireshark/wireshark/-/wikis/CaptureSetup
8. Wireshark Documentation: Chapter 4.2: https://www.wireshark.org/docs/wsug_html_chunked/ChCapPrerequisitesSection.html
9. Wireshark Documentation: Chapter11.8: Display Filter Marcos.https://www.wireshark.org/docs/wsug_html_chunked/ChDisplayFilterMacrosSection.html
10. Jessica Davis: The 10 biggest healthcare data breaches of 2019: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far
11. Ruchi Tuli: “Packet Sniffing and Sniffing Detection”: International Journal of Innovations in Engineering and Technology (IJIET) http://dx.doi.org/10.21172/ijiet.161.04