# Project Report

## INT301: OPEN-SOURCE TECHNOLOGY

Submitted in partial fulfilment of the requirements for the award of degree of

**Batchelor of Technology**

Science and Engineering

Submitted to Prof: Rajeshwar Sharma: 29484

LOVELY PROFESSIONAL UNIVERSITY
PHAGWARA, PUNJAB

Submitted By:

*Name: Suyash Mishra*

*Registration Number: 11905209*

# 1. INTRODUCTION

- What are open-source technologies?
  Technologies referred to as "open-source" are programmes or devices whose source code is publicly accessible and available for anyone to see, use, change, and distribute. The phrase "open-source" means that the source code of the programme is available to the public and that it can be improved by the community. Increasingly more people are using open-source technology because of its adaptability, transparency, and affordability.

  Recent years have seen a major expansion of the open-source movement, leading to the availability of a large number of software programmes and tools. The fact that open-source technologies are frequently more economical than their proprietary versions is one of their key advantages. Anyone with access to the source code can alter and change the software to suit their own requirements without paying exorbitant licencing fees.

- What are hardware and software?
  Hardware and software are two essential components of a computer system. Hardware refers to the physical components that make up a computer, such as the central processing unit (CPU), memory, storage devices, input/output devices, and other peripherals. In other words, hardware encompasses all the tangible, physical parts of a computer that you can touch and see.

  Software, on the other hand, refers to the intangible components of a computer system, including programs, applications, and operating systems. Software is a set of instructions that tell the hardware what to do and how to do it. Without software, the hardware would not be able to perform any useful tasks or functions. There are two main categories of software: system software and application software. System software includes the operating system, device drivers, and other tools that enable the computer to run, manage hardware resources, and provide a platform for other software applications. Application software includes programs that perform specific tasks, such as word processing, web browsing, or gaming.

  In summary, hardware and software are the two critical components that work together to make a computer system function. Hardware provides the physical infrastructure and resources, while software provides the instructions and programs that utilize those resources to perform specific tasks and functions.

## 1.1) Objective of the project

Suppose you are a network analyst, working in the Infotech department of LPU. You have been assigned the responsibility of inspecting HTTP Traffic and retrieving usernames and passwords from the BSNL website, using an appropriate tool.

## 1.2) Description of the project

Analysing the information sent between a client and a server via the HTTP protocol is part of inspecting HTTP traffic. Network analysts can learn more about the magnitude, content, and destination of the data being transmitted through this process. Network analysts can spot potential security holes in the network, including malware infections or cyberattacks, by examining HTTP traffic. They can also assess how well web apps are doing and find any potential problems or bottlenecks that might be interfering. Overall, examining HTTP traffic is a crucial activity for network analyzers because it contributes to the efficiency and security of networks and web services.

In order to retrieve usernames and passwords from the BSNL website, one must first extract the login information that users use to access their accounts there. To check the website's security and find any potential flaws, network analysts often perform this method. A network packet analyzer or password cracking programme that can intercept and decode network traffic may be useful for recovering usernames and passwords. It is crucial to remember that it is illegal and immoral to retrieve usernames and passwords without the right authorization or approval. As a result, this procedure should only be carried out by authorised individuals who have undergone the appropriate training and have the required permission.

### 1.3) Scope of the project

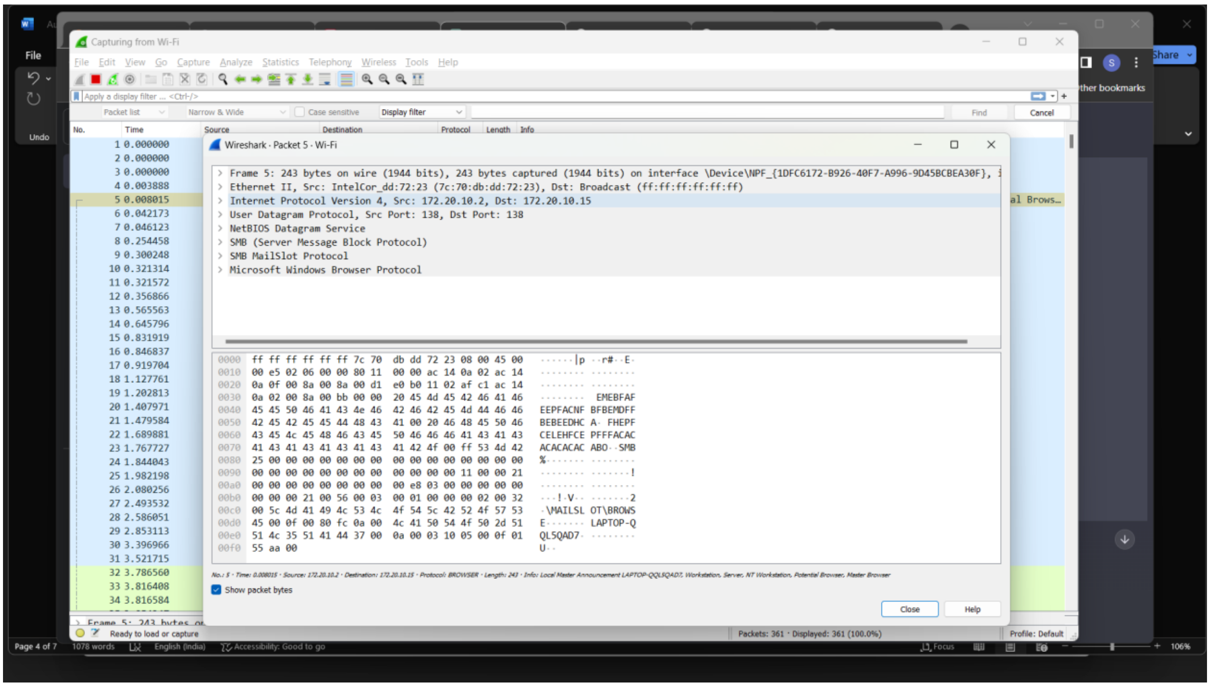
Examining HTTP traffic has a wide range of applications in network analysis and security. Using HTTP traffic inspection, network researchers can find performance hiccups, security flaws, and other network-related problems. The purpose of HTTP traffic inspection specifically is examining HTTP requests' and answers' contents to find potential security threats like malware, online attacks, or data breaches. Additionally, it can be used to assess the effectiveness of online apps and spot any potential problems. Additionally helpful for analysing network traffic patterns, spotting suspect activity, and ensuring adherence to security regulations is HTTP traffic inspection.

The scope of obtaining usernames and passwords from the BSNL website includes evaluating the site's security measures and locating any weaknesses, assuming that the retrieval is authorised. This procedure can be included in a thorough security audit that aims to determine how well the website's security features work and how well user data is safeguarded. Additionally, if a user has forgotten or lost their login information and needs assistance, recovering usernames and passwords may be helpful. Overall, only authorised staff should be able to retrieve usernames and passwords from a website, and it must adhere to all ethical and regulatory requirements.

## 2.) System Description

The system has 8 GB of RAM installed, but only 7.83 GB is available for use. The processor is an Intel Core i5-10300H CPU running at a clock speed of 2.50 GHz. The graphics processing unit (GPU) is an integrated Intel UHD Graphics, which has a total available graphics memory of 4139 MB. The dedicated video memory of the GPU is 128 MB, while the shared system memory is 4011 MB. This information provides a summary of the hardware specifications of the computer, including the RAM, CPU, and GPU details.

# 3.) System Snapshots and full Analysis Report



```
No.  Time
 1 0.000000
 2 0.000000
 3 0.000000
 4 0.003888
 5 0.008015
 6 0.042173
 7 0.046123
 8 0.254458
 9 0.300248
10 0.321314
11 0.321572
12 0.356866
13 0.565563
14 0.645796
15 0.831919
16 0.846837
17 0.919704
18 1.127761
19 1.202813
20 1.407971
21 1.479584
22 1.689881
23 1.767727
24 1.844043
25 1.982198
26 2.080256
27 2.493532
28 2.586051
29 2.853113
30 3.396966
31 3.521715
32 3.786560
33 3.816408
34 3.816584
```

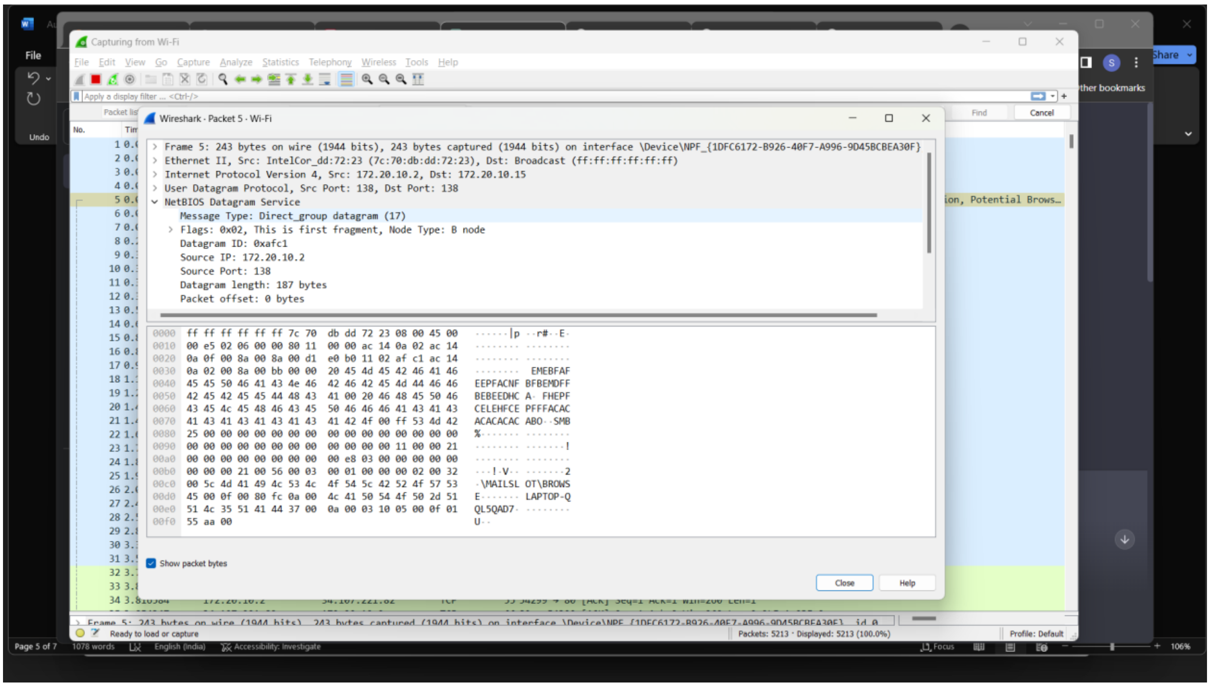
Wireshark · Packet 5 · Wi-Fi

```
> Frame 5: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{1DFC6172-B926-40F7-A996-9D45BCBEA30F}, i
> Ethernet II, Src: IntelCor_dd:72:23 (7c:70:db:dd:72:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.15
> User Datagram Protocol, Src Port: 138, Dst Port: 138
> NetBIOS Datagram Service
> SMB (Server Message Block Protocol)
> SMB MailSlot Protocol
> Microsoft Windows Browser Protocol
```

```
0000  ff ff ff ff ff ff 7c 70  db dd 72 23 08 00 45 00   ······|p ··r#··E·
0010  00 e5 02 06 00 00 80 11  00 00 ac 14 0a 02 ac 14   ········ ········
0020  0a 0f 00 8a 00 8a 00 d1  e0 b0 11 02 af c1 ac 14   ········ ········
0030  0a 02 00 8a 00 bb 00 00  20 45 4d 45 42 46 41 46   ········  EMEBFAF
0040  45 45 50 46 41 43 4e 46  42 46 42 45 4d 44 46 46   EEPFACNF BFBEMDFF
0050  42 45 42 45 45 44 48 43  41 00 20 46 48 45 50 46   BEBEEDHC A· FHEPF
0060  43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE PFFFACAC
0070  41 43 41 43 41 43 41 43  41 42 4f 00 ff 53 4d 42   ACACACAC ABO··SMB
0080  25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %······· ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 21   ········ ·······!
00a0  00 00 00 00 00 00 00 00  00 e8 03 00 00 00 00 00   ········ ········
00b0  00 00 00 21 00 56 00 03  00 01 00 00 00 02 00 32   ···!·V·· ·······2
00c0  00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   ·\MAILSL OT\BROWS
00d0  45 00 0f 00 80 fc 0a 00  4c 41 50 54 4f 50 2d 51   E······· LAPTOP-Q
00e0  51 4c 35 51 41 44 37 00  0a 00 03 10 05 00 0f 01   QL5QAD7· ········
00f0  55 aa 00                                           U··
```

No.: 5 · Time: 0.008015 · Source: 172.20.10.2 · Destination: 172.20.10.15 · Protocol: BROWSER · Length: 243 · Info: Local Master Announcement LAPTOP-QQL5QAD7, Workstation, Server, NT Workstation, Potential Browser, Master Browser

☑ Show packet bytes



Wireshark · Packet 5 · Wi-Fi

```
> Frame 5: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{1DFC6172-B926-40F7-A996-9D45BCBEA30F}
> Ethernet II, Src: IntelCor_dd:72:23 (7c:70:db:dd:72:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.15
> User Datagram Protocol, Src Port: 138, Dst Port: 138
v NetBIOS Datagram Service
    Message Type: Direct_group datagram (17)
  > Flags: 0x02, This is first fragment, Node Type: B node
    Datagram ID: 0xafc1
    Source IP: 172.20.10.2
    Source Port: 138
    Datagram length: 187 bytes
    Packet offset: 0 bytes
```

```
0000  ff ff ff ff ff ff 7c 70  db dd 72 23 08 00 45 00   ······|p ··r#··E·
0010  00 e5 02 06 00 00 80 11  00 00 ac 14 0a 02 ac 14   ········ ········
0020  0a 0f 00 8a 00 8a 00 d1  e0 b0 11 02 af c1 ac 14   ········ ········
0030  0a 02 00 8a 00 bb 00 00  20 45 4d 45 42 46 41 46   ········  EMEBFAF
0040  45 45 50 46 41 43 4e 46  42 46 42 45 4d 44 46 46   EEPFACNF BFBEMDFF
0050  42 45 42 45 45 44 48 43  41 00 20 46 48 45 50 46   BEBEEDHC A· FHEPF
0060  43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE PFFFACAC
0070  41 43 41 43 41 43 41 43  41 42 4f 00 ff 53 4d 42   ACACACAC ABO··SMB
0080  25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %······· ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 21   ········ ·······!
00a0  00 00 00 00 00 00 00 00  00 e8 03 00 00 00 00 00   ········ ········
00b0  00 00 00 21 00 56 00 03  00 01 00 00 00 02 00 32   ···!·V·· ·······2
00c0  00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   ·\MAILSL OT\BROWS
00d0  45 00 0f 00 80 fc 0a 00  4c 41 50 54 4f 50 2d 51   E······· LAPTOP-Q
00e0  51 4c 35 51 41 44 37 00  0a 00 03 10 05 00 0f 01   QL5QAD7· ········
00f0  55 aa 00                                           U··
```

☑ Show packet bytes

This packet is likely part of a NetBIOS name resolution process, commonly used in Windows networking.

The packet is being sent from the IP address 172.20.10.2 to the broadcast address 172.20.10.15. The source MAC address belongs to an Intel Corporation device and the destination MAC address is the broadcast address. This indicates that the packet is being sent to all devices on the local network.

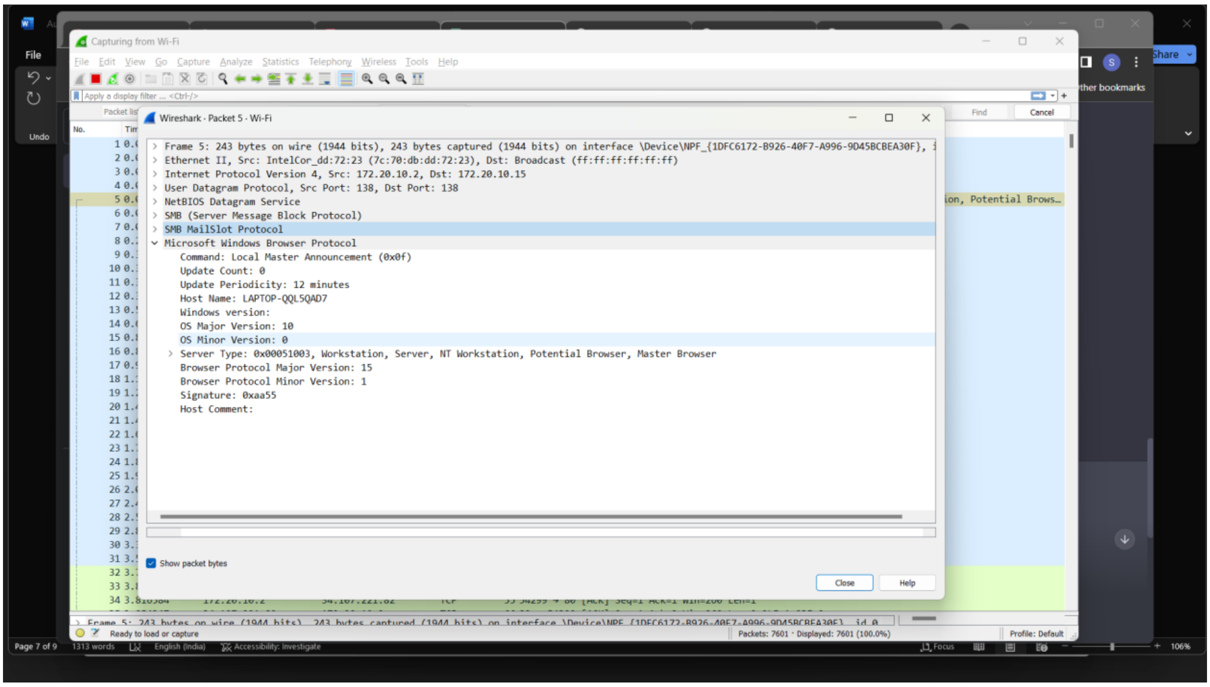
The UDP source and destination port numbers are both 138, which is the NetBIOS datagram service port number.

The NetBIOS datagram packet contains a message type of Direct group datagram (17), which indicates that the packet is being sent to a group of nodes on the network. The flags field has a value of 0x02, indicating that this is the first fragment of a larger message, and the node type is B node.

The Source name field contains the name of the sending device, which is LAPTOP-QQL5QAD7<20> (Server service), and the Destination name field contains the name of the destination, which is WORKGROUP<1e> (Browser Election Service).

The SMB protocol is also present in the packet, which is used for file and printer sharing in Windows networks. The SMB Mail Slot Protocol and Microsoft Windows Browser Protocol are also included in the packet, which are used for browser elections and browsing the network respectively.

Overall, this packet is part of a process used to discover and communicate with devices on a Windows network.



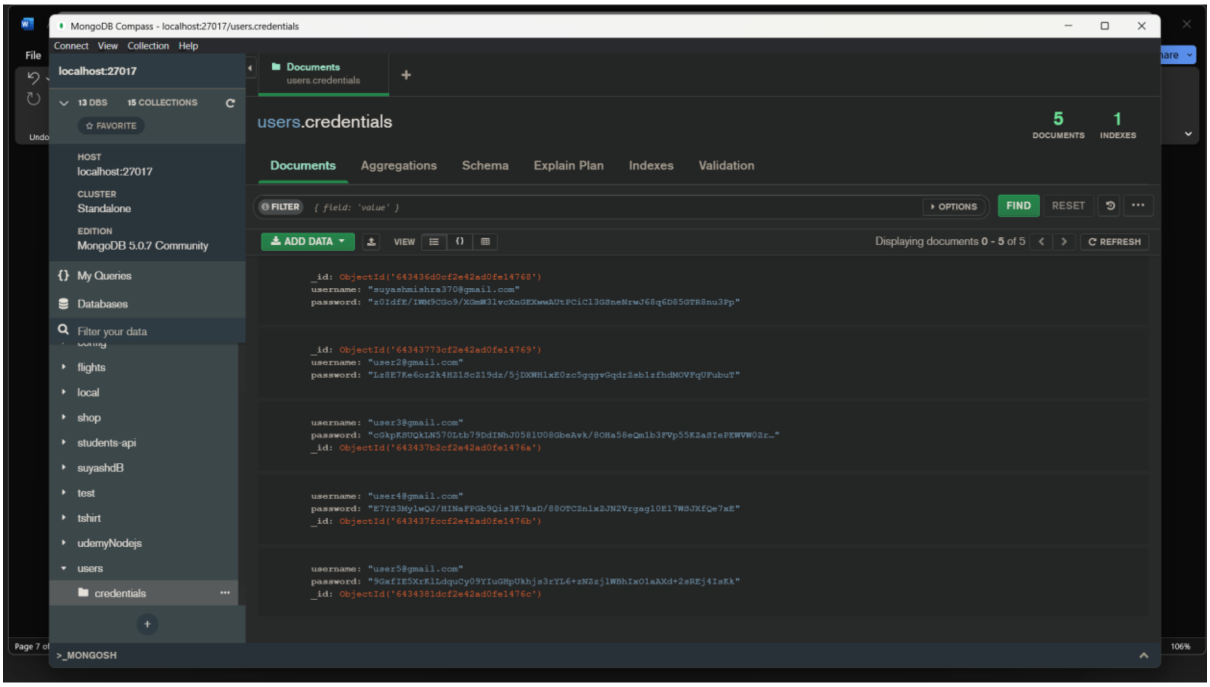
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 5 · Wi-Fi
Show packet bytes
Close
Help

```
> Frame 5: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{1DFC6172-B926-40F7-A996-9D45BCBEA30F}, i
> Ethernet II, Src: IntelCor_dd:72:23 (7c:70:db:dd:72:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.15
> User Datagram Protocol, Src Port: 138, Dst Port: 138
> NetBIOS Datagram Service
> SMB (Server Message Block Protocol)
> SMB MailSlot Protocol
v Microsoft Windows Browser Protocol
    Command: Local Master Announcement (0x0f)
    Update Count: 0
    Update Periodicity: 12 minutes
    Host Name: LAPTOP-QQL5QAD7
    Windows version:
    OS Major Version: 10
    OS Minor Version: 0
  > Server Type: 0x00051003, Workstation, Server, NT Workstation, Potential Browser, Master Browser
    Browser Protocol Major Version: 15
    Browser Protocol Minor Version: 1
    Signature: 0xaa55
    Host Comment:
```

This network capture appears to be a broadcast message from a device with source IP address 172.20.10.2 and MAC address 7c:70:db:dd:72:23, using the User Datagram Protocol (UDP) on port 138 to communicate with destination IP address 172.20.10.15.

The message is using the NetBIOS Datagram Service and the SMB (Server Message Block Protocol) to communicate with the Microsoft Windows Browser Protocol. Specifically, it is a Local Master Announcement (command 0x0f) message, which is used by devices running the Browser service in Windows networking to advertise their role and availability to other devices on the network.

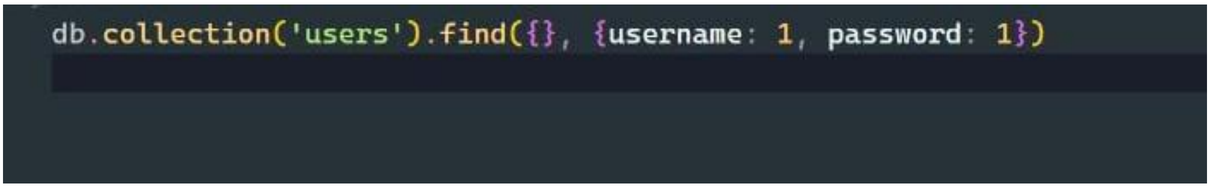
The message contains information about the device sending the message, including its hostname (LAPTOP-QQL5QAD7), operating system version (Windows 10), and the fact that it is a potential browser, master browser, and workstation/server. It also includes a host comment field, which appears to be empty in this case.



```
_id: ObjectId('643436d0cf2e42ad0fe14768')
username: "suyashmishra370@gmail.com"
password: "z0IdfE/IWM9CGo9/XGmW3lvcXnGEXwwAUtPCiCl3GSneNrwJ68q6D85GTR8nu3Pp"

_id: ObjectId('64343773cf2e42ad0fe14769')
username: "user2@gmail.com"
password: "Lz8E7Ke6oz2k4HZ18cZ19dz/5jDXWHlxE0zc5gqgvGqdrZsblzfhdMOVFqUFubuT"

username: "user3@gmail.com"
password: "cGkpKSUQkLN570Ltb79DdINhJ0581U08GbeAvk/8OHa58eQm1b3FVp55KZaSIePEWVW0Zr…"
_id: ObjectId('643437b2cf2e42ad0fe1476a')

username: "user4@gmail.com"
password: "E7YS3MylwQJ/HINaFPGb9Qis3K7kxD/88OTCZnlxZJN2Vrgagl0El7WSJXfQe7xE"
_id: ObjectId('643437fccf2e42ad0fe1476b')

username: "user5@gmail.com"
password: "9GxfIE5XrKlLdquCy09YIuGHpUkhjs3rYL6+zNZzjlWBhIxO1aAXd+2sREj4IsKk"
_id: ObjectId('6434381dcf2e42ad0fe1476c')
```

MongoDB schema with 2 fields "username" and "password" defines a user's login credentials.

MongoDB query to retrieve the "username" and "password" fields in Node.js:



```
db.collection('users').find({}, {username: 1, password: 1})
```

This query will retrieve all documents from the "users" collection and return only the "username" and "password" fields. You can then handle the query result in your Node.js code as needed.

# 4.) References

- "Inspect network activity" from the Google Chrome Developer Tools documentation - https://developer.chrome.com/docs/devtools/network/
- "How to intercept HTTP traffic using Fiddler" from the Telerik documentation - https://docs.telerik.com/fiddler/Configure-Fiddler/Tasks/InterceptHTTPS
- "Inspecting network activity" from the Mozilla Developer Network documentation - https://developer.mozilla.org/en-US/docs/Tools/Network_Monitor
- "Using Wireshark to inspect HTTP traffic" from the Wireshark documentation - https://www.wireshark.org/docs/wsug_html_chunked/ChAdvHTTPCapture.html
- MySQL - A popular open-source relational database management system (RDBMS) that is widely used for web applications. Website: https://www.mysql.com/
- PostgreSQL - Another popular open-source RDBMS known for its stability, scalability, and support for advanced SQL features. Website: https://www.postgresql.org/
- MongoDB - An open-source NoSQL document-oriented database that is designed for scalability, flexibility, and performance. Website: https://www.mongodb.com/
- Apache Cassandra - An open-source NoSQL distributed database that is designed for high availability, scalability, and fault tolerance. Website: https://cassandra.apache.org/
- Redis - An open-source in-memory data structure store that is used as a database, cache, and message broker. Website: https://redis.io/
- Apache HBase - An open-source NoSQL distributed database that is built on top of Apache Hadoop and is designed for big data applications. Website: https://hbase.apache.org/