

# *Pentesting VOIP*

## *with Wireshark*

---

Presenter – Sanchay Singh  
@ THM Delhi, eSec Forte, Gurgaon  
21 July, 2024



# >\_whoami

- > **Founder of HackersVilla Community**
- > Security Consultant/Trainer at **MakeIntern**
- > Working as SME with **Upgrad**
- > Trained Employees of **KPMG, Cognizant**, etc
- > Security Mentor at **OWASP Delhi & BSides Noida**
- > Speaker at **BSides, DEF CON 9111, CRACCon** etc.
- > Active part of **NULL** and **THM** Delhi Chapter



sanchayofficial



sanchayofficial@gmail.com



**Sanchay Singh**

CYBERSECURITY EXPERT | CORPORATE  
TRAINER | PUBLIC SPEAKER



hackersvilla.xyz

# My Journey



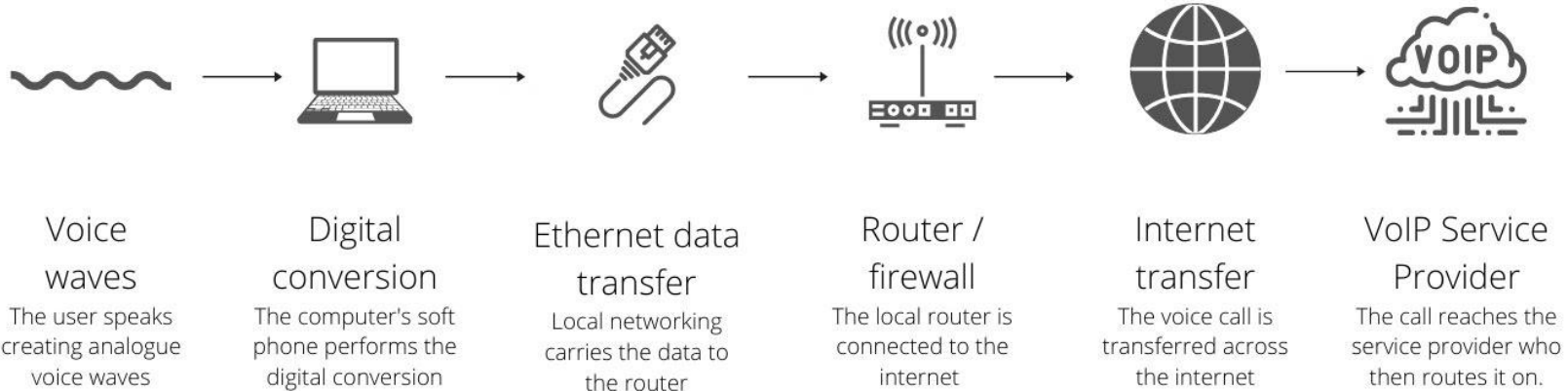
hackersvilla.xyz

# Introduction to VOIP

# What is VOIP?








# How VOIP works?



# Key Benefits of VOIP



## Benefits of VoIP

-   
Easy Install
-   
Virtual Phone Numbers
-   
Use existed Internet
-   
Link Phone Numbers
-   
Simple Integration
-   
Advance Voicemail
-   
High Audio Quality
-   
Power over Ethernet

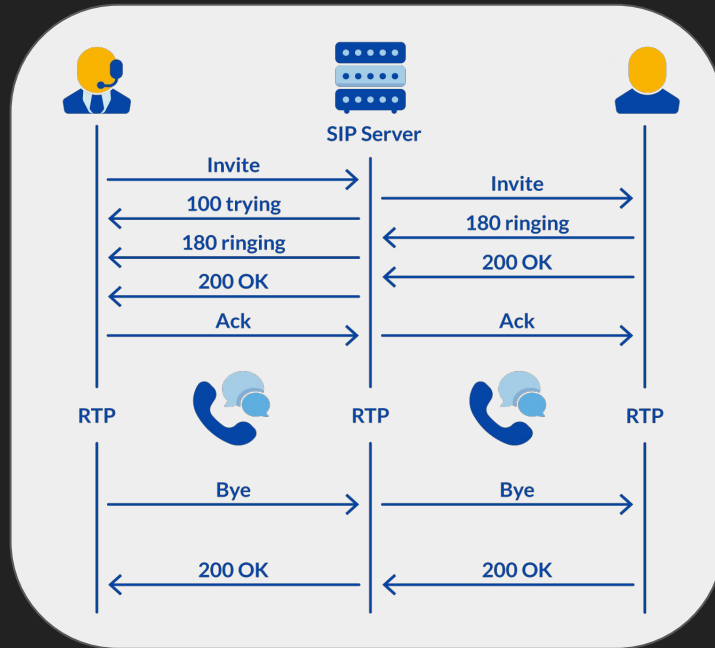


hackersville.xyz

# Common VOIP Protocols



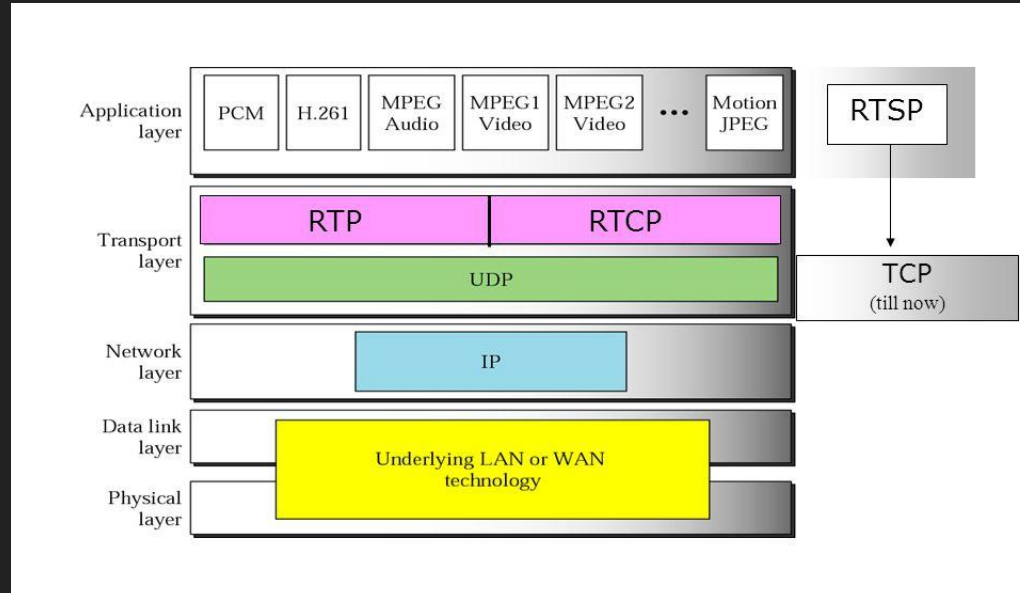
# SIP (Session Initiation Protocol)



## Response Codes

1xx	Provisional	Example	100 Trying, 180 Ringing, 183 Session Progress
2xx	Success	Example	200 OK
3xx	Redirect	Example	301 Moved Permanently, 302 Moved Temporarily
4xx	Request Failure	Example	401 Unauthorized, 403 Forbidden, 480 Temporarily Unavailable
5xx	Server Failure	Example	500 Server Internal Error, 503 Service Unavailable
6xx	Global Failure	Example	600 Busy Everywhere, 604 Does Not Exist Anywhere

# RTP (Real-Time Transport Protocol)





hackersvilla.xyz

# VOIP Security Risks

# Common Vulnerabilities

## **Vulnerabilities:**

- Eavesdropping
- Man-in-the-Middle Attacks
- Registration Hijacking
- Call Interception
- DOS Attacks

## **Mitigations:**

- Encryption
- Strong Authentication
- Regular Monitoring

# Impact on VOIP Attacks on orgs.

- **Privacy Violation**
  - Eavesdropping on personal or business calls exposes sensitive information.
- **Financial Loss**
  - Unauthorized calls can lead to increased costs and billing issues.
- **Reputation Damage**
  - Breaches can damage an organization's reputation and trustworthiness.

# Imp. of securing VOIP Systems

## **1. Preventing Data Breaches**

Ensuring the confidentiality and integrity of communications.

## **2. Maintaining Service Availability**

Protecting VOIP systems from DOS attacks to ensure continuous service.

## **3. Building Trust**

Ensuring secure communication channels to maintain user trust and business credibility.



hackersvilla.xyz

# Introduction to Wireshark

# What is Wireshark?





# Wireshark Interface Overview

**Red Box Shows Wireshark is Running**

The image shows the Wireshark 1.12.6 interface. A red box highlights the top-left corner where the application icon is located, with the text "Red Box Shows Wireshark is Running". Another red box highlights the "Filter:" and "Expression..." fields, labeled "1. Filter Toolbar". A third red box highlights the packet list table, labeled "2. Packet List Pane". A fourth red box highlights the packet details pane, labeled "3. Packet Details Pane". A fifth red box highlights the packet byte pane, labeled "4. Packet Byte Pane".

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Info
1827	8.598721	192.168.1.101	74.125.200.94	TCP	49246.443 [ACK] Seq=3161453776 Ack=3708602291 Win=4150 Len=0 TSval=595569656 TSecr=3513932058
1828	8.599091	192.168.1.101	74.125.200.94	TLSv1.2	Application Data
1829	8.631177	216.58.220.46	192.168.1.101	TCP	443.49251 [ACK] Seq=1298278402 Ack=1710850208 Win=371 Len=0 TSval=1704563776 TSecr=595569582
1830	8.644211	74.125.200.94	192.168.1.101	TCP	443.49246 [ACK] Seq=3708602291 Ack=3161453776 Win=547 Len=0 TSval=3513932109 TSecr=595569629
1831	8.658656	216.58.196.132	192.168.1.101	TCP	443.49249 [ACK] Seq=2905517011 Ack=521756204 Win=366 Len=0 TSval=1415568817 TSecr=595569630
1832	8.696484	74.125.200.94	192.168.1.101	TCP	443.49246 [ACK] Seq=3708602291 Ack=3161453845 Win=547 Len=0 TSval=3513932161 TSecr=595569656
1833	8.697547	216.58.220.46	192.168.1.101	TCP	443.49251 [ACK] Seq=1298278402 Ack=1710850277 Win=371 Len=0 TSval=1704563842 TSecr=595569642
1834	9.846595	192.168.1.101	216.239.98.121	TCP	443.49246 [ACK] Seq=1030802300 Ack=360272818 Win=4096 Len=0 TSval=595570899 TSecr=3031662643
1835	10.201531	216.239.98.121	192.168.1.101	TCP	443.49246 [ACK] Seq=360272818 Ack=1030802301 Win=173 Len=0 TSval=3031667578 TSecr=595570899
1836	11.798841	192.168.1.101	111.221.29.129	SSL	
1837	12.045607	111.221.29.129	192.168.1.101	TCP	443.65343 [ACK] Seq=41277483 Ack=1149722157 Win=7875 Len=0 TSval=212941084 TSecr=595572845
1838	12.045684	192.168.1.101	111.221.29.129	SSL	Continuation Data
1839	12.125740	111.221.29.129	192.168.1.101	TLSv1.2	Application Data
1840	12.125803	192.168.1.101	111.221.29.129	TCP	65343.443 [ACK] Seq=1149722228 Ack=41277616 Win=4091 Len=0 TSval=595573171 TSecr=212941102
1841	13.933007	192.168.1.101	17.253.26.253	NTP	NTP Version 4, client
1842	14.297892	17.253.26.253	192.168.1.101	NTP	NTP Version 4, server
1843	16.342582	fe80::1	ff02::1	ICMPv6	Router Advertisement from 94:fb:b2:b8:df:d8

Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)

Ethernet II, Src: 28:cf:e9:1e:df:a9 (28:cf:e9:1e:df:a9), Dst: 94:fb:b2:b8:df:d8 (94:fb:b2:b8:df:d8)

Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 192.168.1.1 (192.168.1.1)

User Datagram Protocol, Src Port: 49940 (49940), Dst Port: 53 (53)

Domain Name System (query)

0000 94 fb b2 b8 df d8 28 cf e9 1e df a9 08 00 45 00 .....E.....  
0010 00 4b db ee 00 00 ff 11 5b fc c0 a8 01 65 c0 a8 .....K.....  
0020 01 01 c3 14 00 35 00 37 95 bc 07 bf 01 00 00 01 .....5.7.....  
0030 00 00 00 00 00 00 07 70 61 67 65 61 64 32 11 67 .....p aead2.g  
0040 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e .....ooglesyn dication  
0050 03 63 6f 6d 00 00 01 00 01 .....com.....

4. Packet Byte Pane



hackersville.xyz

# Setting up Lab for Pentesting VOIP

# List of Tools needed

1. **Softphone Software:** Zoiper / Linphone
2. **VOIP Server:** Trixbox
3. **Virtual Machine Software:** VMWare / Hyper-V / Qemu / VirtualBox
4. **Traffic Capture Tool:** Wireshark

# A **Great** Resource



hackersvilla.xyz



Link to Lab Setup Apps



Link to Pentesting  
Articles

# The WorkFlow

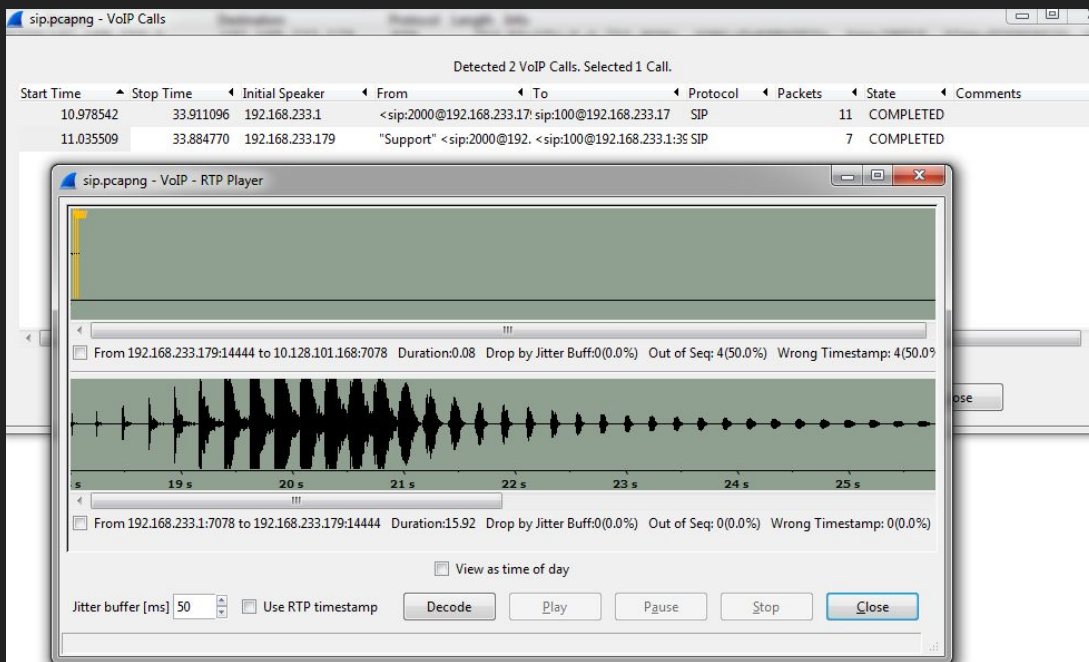
# Capturing VOIP Traffic

The screenshot displays the Wireshark network traffic analysis tool. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Filter:** The filter bar contains the text "itp" and is highlighted with a red box.
- Packet List:** A table showing a list of captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The packets are numbered 653 to 689. The Destination column for all packets is 172.16.0.145. The Protocol column shows a mix of RTP, ICMP, and UDP. The Info column provides details about each packet, such as "214 PT=ITU-T G.711 PCMU, SSRC=0x4808A888, Seq=2, Time=5" for RTP packets and "126 Destination unreachable (Port unreachable)" for ICMP packets. The entire packet list area is highlighted with a red box.
- Packet Details:** The bottom pane shows the details of the selected packet (No. 649). It includes the following sections:
  - Ethernet II:** Src: NecInfra\_de:db:d3 (00:60:b9:de:db:d3), Dst: NecInfra\_83:01:40 (00:60:b9:83:01:40)
  - Internet Protocol Version 4:** Src: 172.16.0.20 (172.16.0.20), Dst: 172.16.0.145 (172.16.0.145)
  - User Datagram Protocol:** Src Port: 10020 (10020), Dst Port: edm-std-notify (3462)
  - Real-time Transport Protocol:** This section is expanded, showing a hex dump of the packet data. The hex dump is as follows:

```
0000 00 60 b9 83 01 40 00 60 b9 de db d3 08 00 45 00  ....@.....E.
0010 00 c8 00 00 00 00 80 11 e1 5f ac 10 00 14 ac 10  ....A
0020 00 91 27 24 0d 80 00 b9 e6 d8 00 00 00 41  ....A
0030 f5 9e 4b d8 a8 88 ff ff ff ff ff ff ff ff ff ff  ....K.....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ....
```

# Analyzing RTP Streams





hackersville.xyz

# Time for the Demonstration



# Thank You

**PPT Available on**

<https://github.com/sanchayofficial/meetups-ppt>

