Cyber Law and Forensics (CS402)

Lab Assignment 6

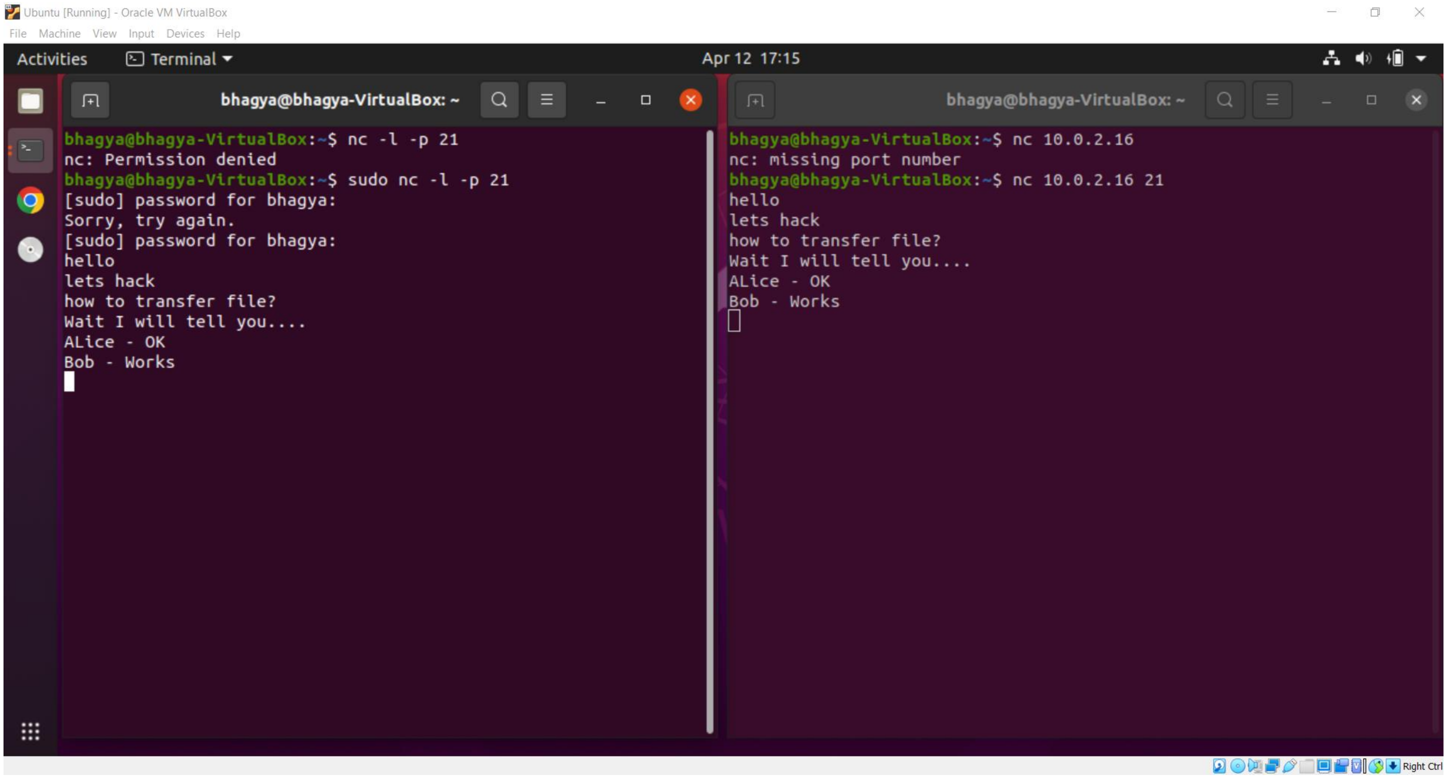
U19CS012

A.) Remote data acquisition using Netcat Command

Link 1: https://www.youtube.com/watch?v=cq9RHDL2yMM

Link 2: https://www.youtube.com/watch?v=OcSS34Lw910

Link 3: https://www.youtube.com/watch?v=HehVavsBhgI


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 12 17:15
bhagya@bhagya-VirtualBox: ~
bhagya@bhagya-VirtualBox: ~
Right Ctrl

```
bhagya@bhagya-VirtualBox:~$ nc -l -p 21
nc: Permission denied
bhagya@bhagya-VirtualBox:~$ sudo nc -l -p 21
[sudo] password for bhagya:
Sorry, try again.
[sudo] password for bhagya:
hello
lets hack
how to transfer file?
Wait I will tell you....
ALice - OK
Bob - Works
```

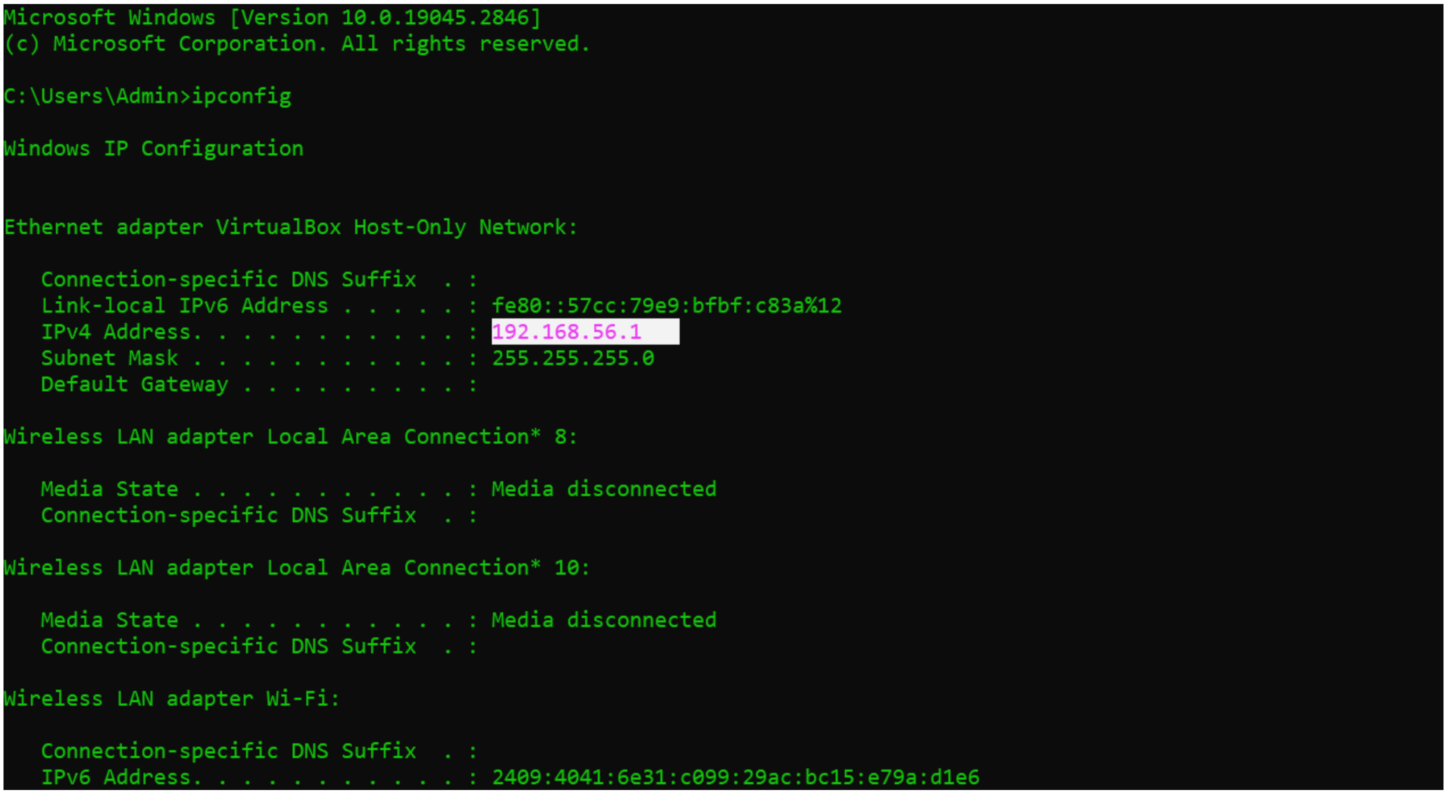
```
bhagya@bhagya-VirtualBox:~$ nc 10.0.2.16
nc: missing port number
bhagya@bhagya-VirtualBox:~$ nc 10.0.2.16 21
hello
lets hack
how to transfer file?
Wait I will tell you....
ALice - OK
Bob - Works
```

"nc" - netcat

-v = verbose output

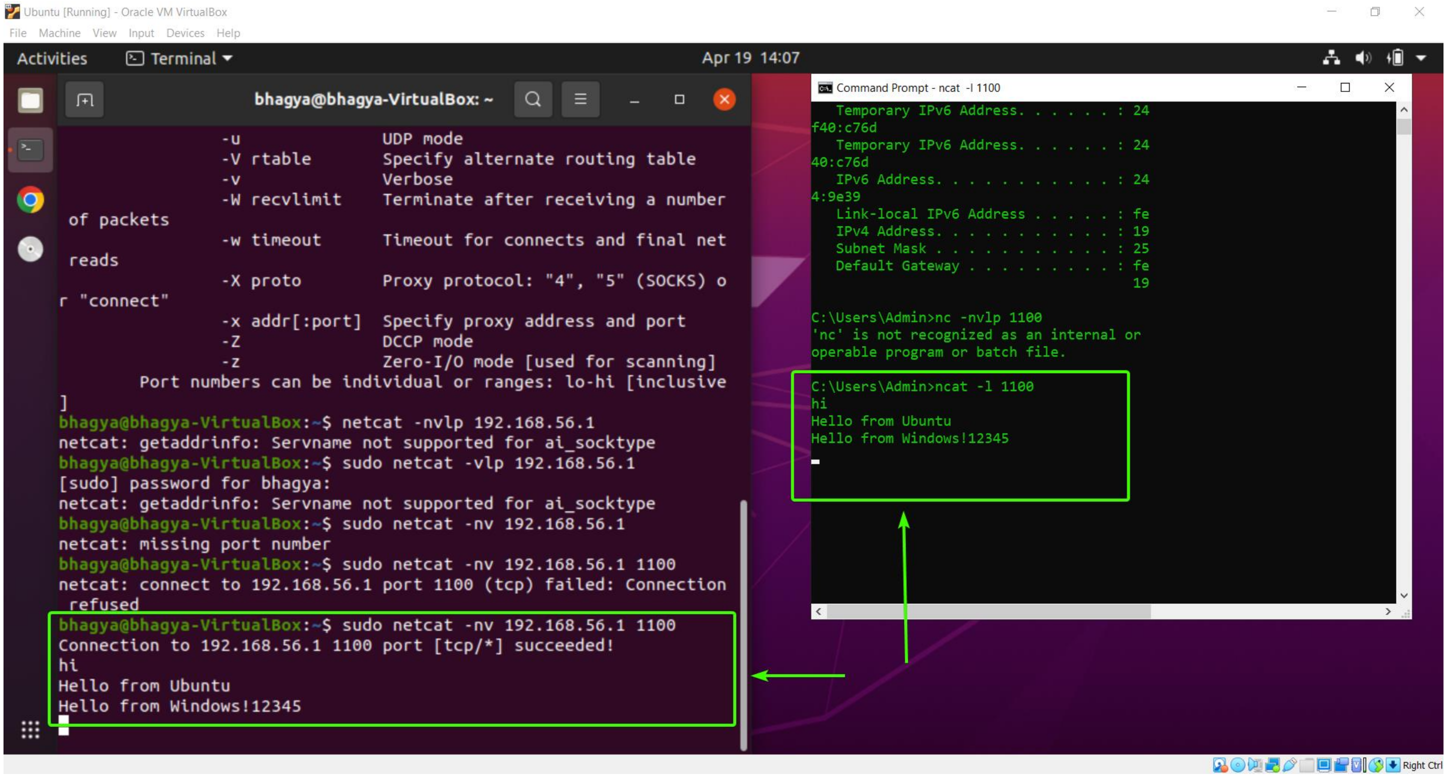
-l = listening

-p = port number



```
Microsoft Windows [Version 10.0.19045.2846]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::57cc:79e9:bfbf:c83a%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4041:6e31:c099:29ac:bc15:e79a:d1e6
```

Get the IP Address of Windows Machine using "ipconfig".

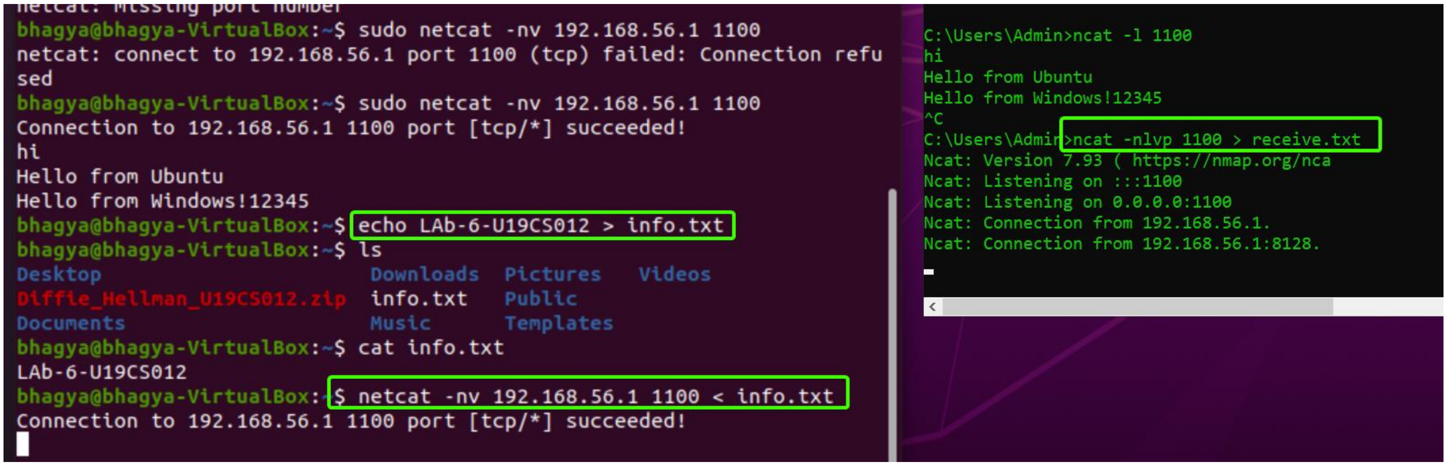


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Apr 19 14:07
bhagya@bhagya-VirtualBox: ~
Command Prompt - ncat -l 1100
Right Ctrl

```
                -u              UDP mode
                -V rtable       Specify alternate routing table
                -v              Verbose
                -W recvlimit    Terminate after receiving a number
 of packets
                -w timeout      Timeout for connects and final net
 reads
                -X proto        Proxy protocol: "4", "5" (SOCKS) o
r "connect"
                -x addr[:port]  Specify proxy address and port
                -Z              DCCP mode
                -z              Zero-I/O mode [used for scanning]
        Port numbers can be individual or ranges: lo-hi [inclusive
]
bhagya@bhagya-VirtualBox:~$ netcat -nvlp 192.168.56.1
netcat: getaddrinfo: Servname not supported for ai_socktype
bhagya@bhagya-VirtualBox:~$ sudo netcat -vlp 192.168.56.1
[sudo] password for bhagya:
netcat: getaddrinfo: Servname not supported for ai_socktype
bhagya@bhagya-VirtualBox:~$ sudo netcat -nv 192.168.56.1
netcat: missing port number
bhagya@bhagya-VirtualBox:~$ sudo netcat -nv 192.168.56.1 1100
netcat: connect to 192.168.56.1 port 1100 (tcp) failed: Connection
 refused
bhagya@bhagya-VirtualBox:~$ sudo netcat -nv 192.168.56.1 1100
Connection to 192.168.56.1 1100 port [tcp/*] succeeded!
hi
Hello from Ubuntu
Hello from Windows!12345
```

```
   Temporary IPv6 Address. . . . . . : 24
f40:c76d
   Temporary IPv6 Address. . . . . . : 24
40:c76d
   IPv6 Address. . . . . . . . . . . : 24
4:9e39
   Link-local IPv6 Address . . . . . : fe
   IPv4 Address. . . . . . . . . . . : 19
   Subnet Mask . . . . . . . . . . . : 25
   Default Gateway . . . . . . . . . : fe
                                       19

C:\Users\Admin>nc -nvlp 1100
'nc' is not recognized as an internal or
operable program or batch file.

C:\Users\Admin>ncat -l 1100
hi
Hello from Ubuntu
Hello from Windows!12345
```

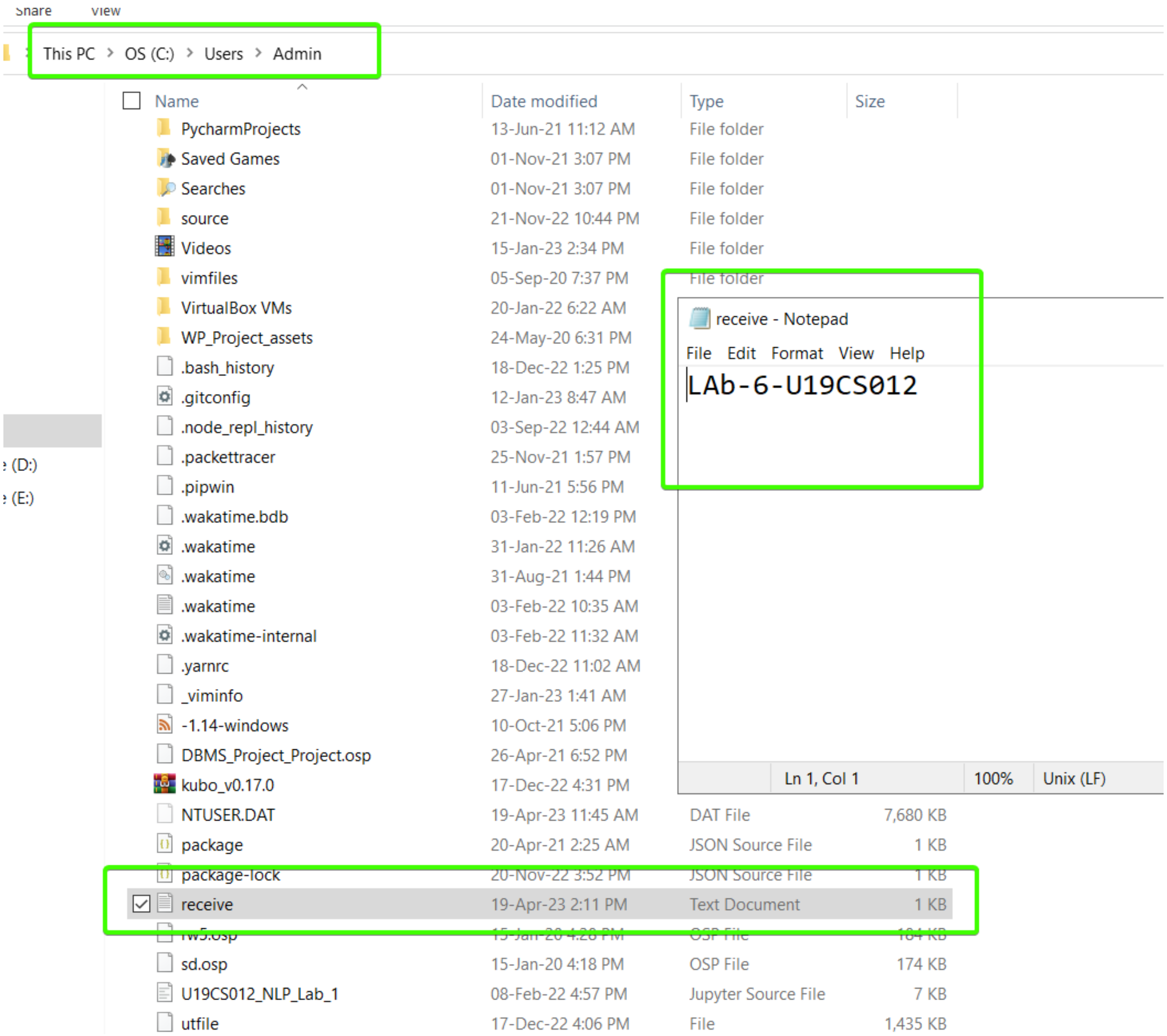
Once we have checked that message Transfer is Possible and Correct, Lets do the same for File Transfer.



```
netcat: missing port number
bhagya@bhagya-VirtualBox:~$ sudo netcat -nv 192.168.56.1 1100
netcat: connect to 192.168.56.1 port 1100 (tcp) failed: Connection refu
sed
bhagya@bhagya-VirtualBox:~$ sudo netcat -nv 192.168.56.1 1100
Connection to 192.168.56.1 1100 port [tcp/*] succeeded!
hi
Hello from Ubuntu
Hello from Windows!12345
bhagya@bhagya-VirtualBox:~$ echo LAb-6-U19CS012 > info.txt
bhagya@bhagya-VirtualBox:~$ ls
Desktop                        Downloads  Pictures   Videos
Diffie_Hellman_U19CS012.zip    info.txt   Public
Documents                      Music      Templates
bhagya@bhagya-VirtualBox:~$ cat info.txt
LAb-6-U19CS012
bhagya@bhagya-VirtualBox:~$ netcat -nv 192.168.56.1 1100 < info.txt
Connection to 192.168.56.1 1100 port [tcp/*] succeeded!
```

```
C:\Users\Admin>ncat -l 1100
hi
Hello from Ubuntu
Hello from Windows!12345
^C
C:\Users\Admin>ncat -nlvp 1100 > receive.txt
Ncat: Version 7.93 ( https://nmap.org/nca
Ncat: Listening on :::1100
Ncat: Listening on 0.0.0.0:1100
Ncat: Connection from 192.168.56.1.
Ncat: Connection from 192.168.56.1:8128.
```

We make a File "info.txt" with Text "Lab-6-U19CS012" and save it. Afterwards, We listen to Port 1100 and send the output to "receive.txt" File. Using netcat command we Successfully Transfer the File.



Name	Date modified	Type	Size
PycharmProjects	13-Jun-21 11:12 AM	File folder	
Saved Games	01-Nov-21 3:07 PM	File folder	
Searches	01-Nov-21 3:07 PM	File folder	
source	21-Nov-22 10:44 PM	File folder	
Videos	15-Jan-23 2:34 PM	File folder	
vimfiles	05-Sep-20 7:37 PM	File folder	
VirtualBox VMs	20-Jan-22 6:22 AM		
WP_Project_assets	24-May-20 6:31 PM		
.bash_history	18-Dec-22 1:25 PM		
.gitconfig	12-Jan-23 8:47 AM		
.node_repl_history	03-Sep-22 12:44 AM		
.packettracer	25-Nov-21 1:57 PM		
.pipwin	11-Jun-21 5:56 PM		
.wakatime.bdb	03-Feb-22 12:19 PM		
.wakatime	31-Jan-22 11:26 AM		
.wakatime	31-Aug-21 1:44 PM		
.wakatime	03-Feb-22 10:35 AM		
.wakatime-internal	03-Feb-22 11:32 AM		
.yarnrc	18-Dec-22 11:02 AM		
_viminfo	27-Jan-23 1:41 AM		
-1.14-windows	10-Oct-21 5:06 PM		
DBMS_Project_Project.osp	26-Apr-21 6:52 PM		
kubo_v0.17.0	17-Dec-22 4:31 PM		
NTUSER.DAT	19-Apr-23 11:45 AM	DAT File	7,680 KB
package	20-Apr-21 2:25 AM	JSON Source File	1 KB
package-lock	20-Nov-22 3:52 PM	JSON Source File	1 KB
☑ receive	19-Apr-23 2:11 PM	Text Document	1 KB
rw5.osp	15-Jan-20 4:28 PM	OSP File	184 KB
sd.osp	15-Jan-20 4:18 PM	OSP File	174 KB
U19CS012_NLP_Lab_1	08-Feb-22 4:57 PM	Jupyter Source File	7 KB
utfile	17-Dec-22 4:06 PM	File	1,435 KB

receive - Notepad

File Edit Format View Help

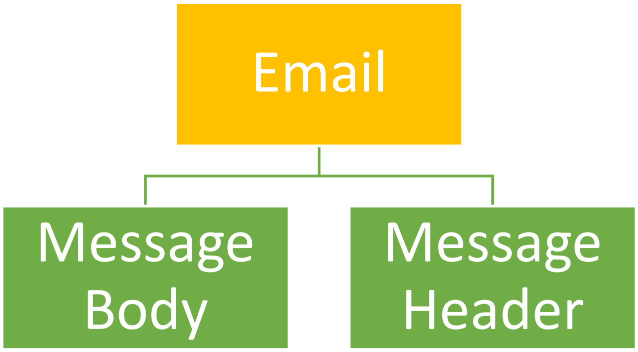
```
LAb-6-U19CS012
```

Ln 1, Col 1 | 100% | Unix (LF)

As you can see in above image, that the File is received!

B.) Identify whether the email is a **fake mail** or **legitimate email**?

- ✓ Email Evidence is in Email itself (Header)!
- ✓ Tracing -> Examination of an Email Header to determine its **point of origin**



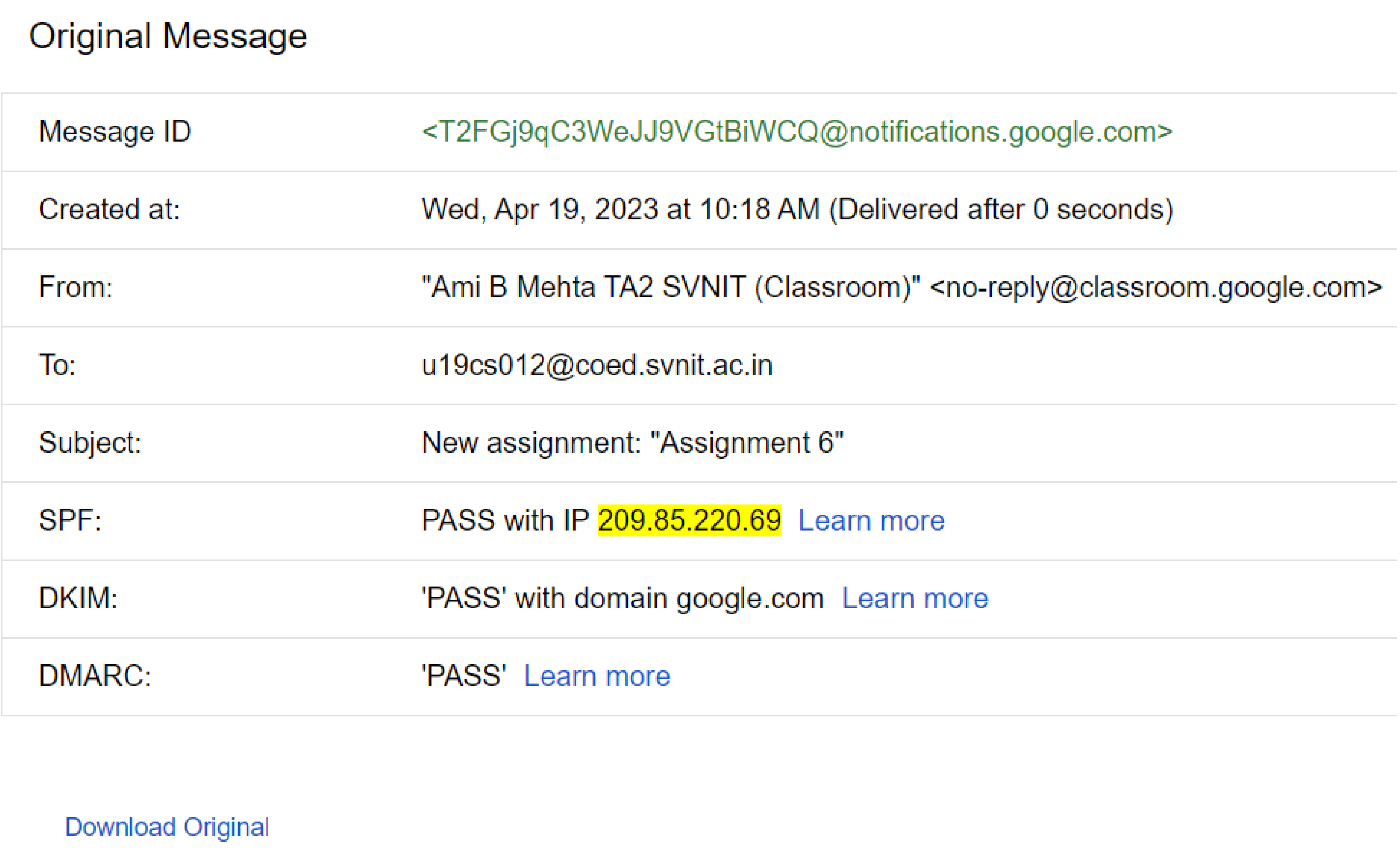
- ✓ Header – Info regarding the Sender, Receiver and the Route the Email took to the Destination

Retrieving email headers

- Office 365: Open email, click on the three dots at the top right, select 'View message details.
- Gmail: Open email, click on the three dots at the top right, select 'Show original'. The header will appear on the bottom part of the screen
- Yahoo: Open email, click on the three dots at the bottom, select 'View raw message.
- Outlook: Open email, navigate to the horizontal menu at the top and click on 'File', click on 'Properties' in the 'Info' section, the header is in the 'Internet headers' box

Select all and copy/paste into a text editor like Notepad (may need to enter line breaks)

Why? When you Forward the Phishing Email, It moves the Header Information.

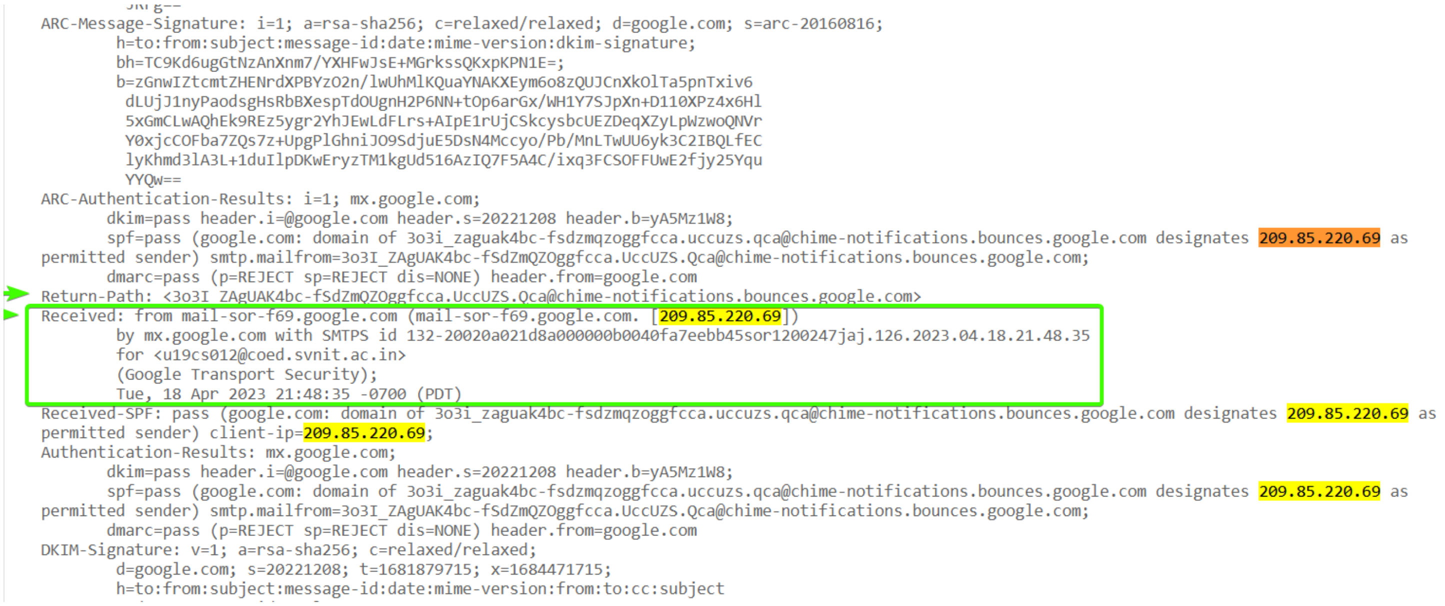


Original Message

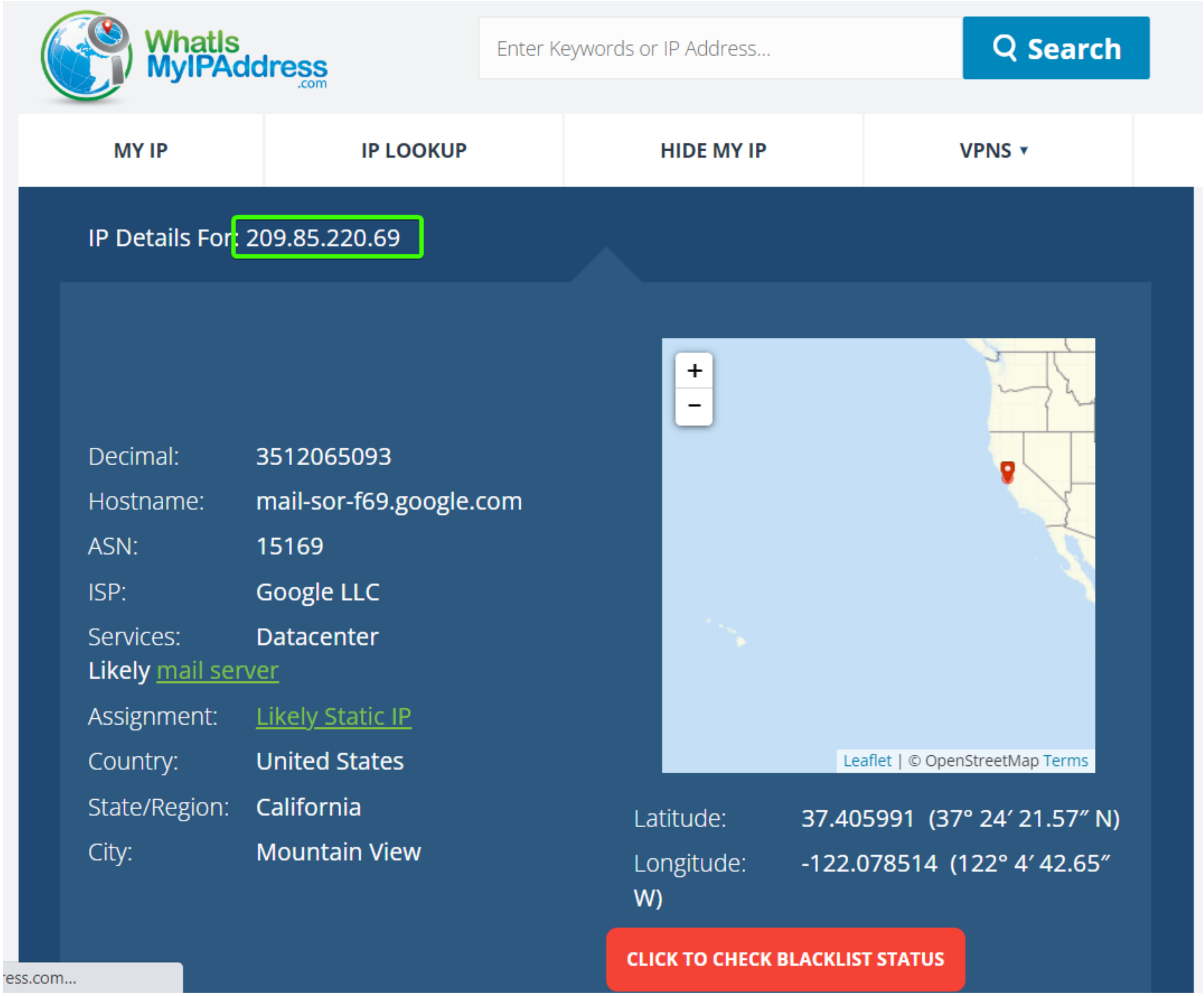
Message ID	<T2FGj9qC3WeJJ9VGtBiWCQ@notifications.google.com>
Created at:	Wed, Apr 19, 2023 at 10:18 AM (Delivered after 0 seconds)
From:	"Ami B Mehta TA2 SVNIT (Classroom)" <no-reply@classroom.google.com>
To:	u19cs012@coed.svnit.ac.in
Subject:	New assignment: "Assignment 6"
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain google.com Learn more
DMARC:	'PASS' Learn more

Download Original

- SPF, DKIM and DMARC authentication



```
         JKrg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:from:subject:message-id:date:mime-version:dkim-signature;
        bh=TC9Kd6ugGtNzAnXnm7/YXHFwJsE+MGrkssQKxpKPN1E=;
        b=zGnwIZtcmtZHENrdXPBYzO2n/lwUhMlKQuaYNAKXEym6o8zQUJCnXkOlTa5pnTxiv6
         dLUjJ1nyPaodsgHsRbBXespTdOUgnH2P6NN+tOp6arGx/WH1Y7SJpXn+D110XPz4x6Hl
         5xGmCLwAQhEk9REz5ygr2YhJEwLdFLrs+AIpE1rUjCSkcysbcUEZDeqXZyLpWzwoQNVr
         Y0xjcCOFba7ZQs7z+UpgPlGhniJO9SdjuE5DsN4Mccyo/Pb/MnLTwUU6yk3C2IBQLfEC
         lyKhmd3lA3L+1duIlpDKwEryzTM1kgUd516AzIQ7F5A4C/ixq3FCSOFFUwE2fjy25Yqu
         YYQw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@google.com header.s=20221208 header.b=yA5Mz1W8;
       spf=pass (google.com: domain of 3o3i_zaguak4bc-fsdzmqzoggfcca.uccuzs.qca@chime-notifications.bounces.google.com designates 209.85.220.69 as
permitted sender) smtp.mailfrom=3o3I_ZAgUAK4bc-fSdZmQZOggfcca.UccUZS.Qca@chime-notifications.bounces.google.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=google.com
Return-Path: <3o3I_ZAgUAK4bc-fSdZmQZOggfcca.UccUZS.Qca@chime-notifications.bounces.google.com>
Received: from mail-sor-f69.google.com (mail-sor-f69.google.com. [209.85.220.69])
        by mx.google.com with SMTPS id 132-20020a021d8a000000b0040fa7eebb45sor1200247jaj.126.2023.04.18.21.48.35
        for <u19cs012@coed.svnit.ac.in>
        (Google Transport Security);
        Tue, 18 Apr 2023 21:48:35 -0700 (PDT)
Received-SPF: pass (google.com: domain of 3o3i_zaguak4bc-fsdzmqzoggfcca.uccuzs.qca@chime-notifications.bounces.google.com designates 209.85.220.69 as
permitted sender) client-ip=209.85.220.69;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@google.com header.s=20221208 header.b=yA5Mz1W8;
       spf=pass (google.com: domain of 3o3i_zaguak4bc-fsdzmqzoggfcca.uccuzs.qca@chime-notifications.bounces.google.com designates 209.85.220.69 as
permitted sender) smtp.mailfrom=3o3I_ZAgUAK4bc-fSdZmQZOggfcca.UccUZS.Qca@chime-notifications.bounces.google.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=google.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=google.com; s=20221208; t=1681879715; x=1684471715;
        h=to:from:subject:message-id:date:mime-version:from:to:cc:subject
```


WhatIs MyIPAddress .com
Enter Keywords or IP Address...
Search
MY IP
IP LOOKUP
HIDE MY IP
VPNS ▾
+
−
Leaflet | © OpenStreetMap Terms
CLICK TO CHECK BLACKLIST STATUS
ess.com...

IP Details For: 209.85.220.69

Decimal:	3512065093
Hostname:	mail-sor-f69.google.com
ASN:	15169
ISP:	Google LLC
Services:	Datacenter Likely mail server
Assignment:	Likely Static IP
Country:	United States
State/Region:	California
City:	Mountain View
Latitude:	37.405991 (37° 24′ 21.57″ N)
Longitude:	-122.078514 (122° 4′ 42.65″ W)

Overall, Just check the **Received from** in Email Header and Cross Verify the IP Address, to check whether the Email is Legitimate or Not.

SUBMITTED BY:

U19CS012

BHAGYA VINOD RANA