FINAL PROJECT
CSCI362-662 M01- INFORMATION SYSTEM SECURITY ENGINEERING AND ADMINISTRATION

Name: Priyanshu Tomar
Semester: SPRING 2023
Telephone: +15513301531
Email: ptomar@nyit.edu

Welcome to XYZ Inc., a fictional organization that operates in the technology industry. The company specializes in providing software solutions to small and medium-sized businesses. XYZ Inc. has been in operation for the past ten years, and it has established itself as a reputable provider of quality software solutions.

Network Design: The network design of XYZ Inc. consists of the following devices:
8 Desktop computers
6 Laptops
1 Servers
5 Routers
2 Firewalls
5 Switches

1. The desktop computers are used by employees in the company's administrative and development departments, while the laptops are used by sales representatives who travel frequently. The servers are used to host the company's software applications and store data. The network design is configured in a way that ensures that all devices are connected and can communicate with each other.

2. To ensure that the network is secure, XYZ Inc. has implemented multiple layers of security. The company has installed firewalls to prevent unauthorized access to the network, and all devices are protected by antivirus software. Additionally, the company has implemented strict password policies to prevent unauthorized access to sensitive information.

3. The routers are used to manage network traffic and ensure that all devices are connected to the internet. The network design includes redundant routers to ensure that the network remains operational in the event of a failure.

4. In conclusion, XYZ Inc. is a technology company that provides software solutions to small and medium-sized businesses. The company's network design consists of 8 desktop computers, 6 laptops, 1 servers, 5 routers, 2 firewalls, and 5 switches. The network design is configured to ensure that all devices can communicate with each other, and it includes multiple layers of security to prevent unauthorized access to the network and data.

5. The 8 desktop computers and 6 laptops are connected to a local area network (LAN) switch. The LAN switch is connected to a router, which serves as the gateway to the internet and pro-

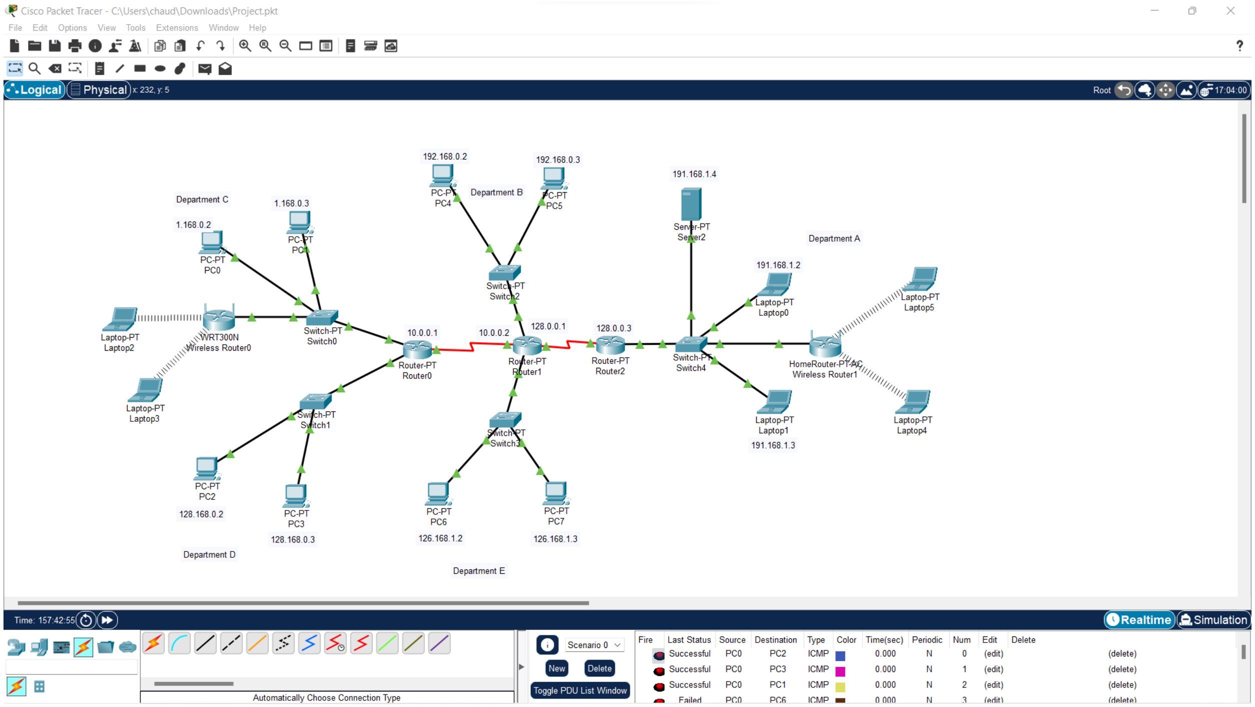
vides access to external networks.

6. Server is a web server, which host the organization's website and provide access to web applications. These servers are connected to the LAN switch.

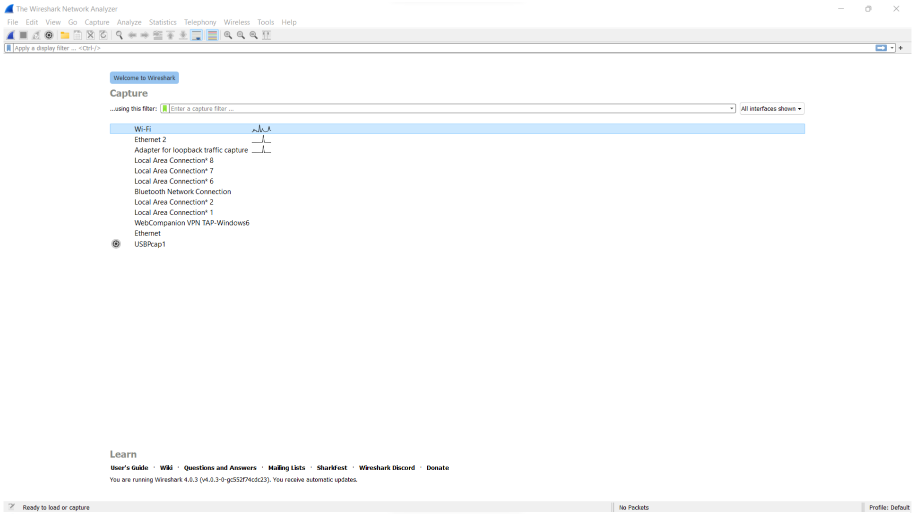
7. The two firewalls are configured in a high-availability (HA) pair to provide redundancy and load balancing. The firewalls are connected to the router and are responsible for filtering and securing traffic to and from the organization's network.

8. The three routers are configured in a redundant mesh topology to provide resilience and failover capabilities in case of a router failure.

9. Overall, this network topology is designed to provide high availability, scalability, and security for the fictional organization's IT infrastructure.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC2	ICMP	🟦	0.000	N	0	(edit)	(delete)
●	Successful	PC0	PC3	ICMP	🟪	0.000	N	1	(edit)	(delete)
●	Successful	PC0	PC1	ICMP	🟨	0.000	N	2	(edit)	(delete)
●	Failed	PC0	PC6	ICMP	🟫	0.000	N	3	(edit)	(delete)


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Capture

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

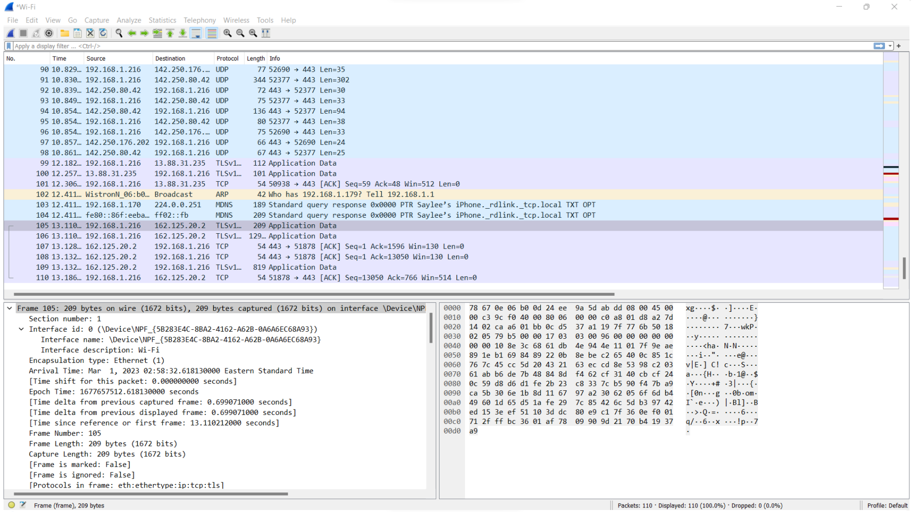
```
Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
WebCompanion VPN TAP-Windows6
Ethernet
USBPcap1
```

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

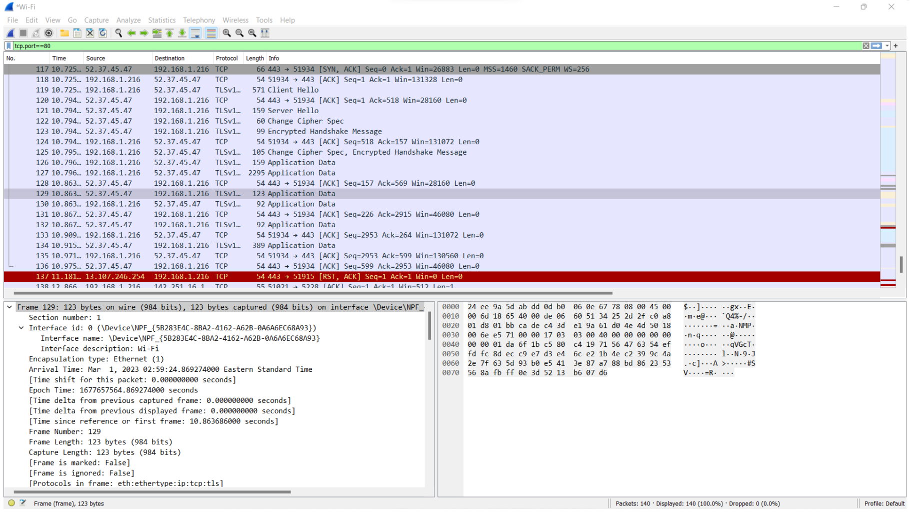

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time      Source            Destination       Protocol Length Info
     90 10.829…   192.168.1.216     142.250.176.…     UDP        77 52690 → 443 Len=35
     91 10.830…   192.168.1.216     142.250.80.42     UDP       344 52377 → 443 Len=302
     92 10.839…   142.250.80.42     192.168.1.216     UDP        72 443 → 52377 Len=30
     93 10.849…   192.168.1.216     142.250.80.42     UDP        75 52377 → 443 Len=33
     94 10.854…   142.250.80.42     192.168.1.216     UDP       136 443 → 52377 Len=94
     95 10.854…   192.168.1.216     142.250.80.42     UDP        80 52377 → 443 Len=38
     96 10.854…   192.168.1.216     142.250.176.…     UDP        75 52690 → 443 Len=33
     97 10.857…   142.250.176.202   192.168.1.216     UDP        66 443 → 52690 Len=24
     98 10.861…   142.250.80.42     192.168.1.216     UDP        67 443 → 52377 Len=25
     99 12.182…   192.168.1.216     13.88.31.235      TLSv1…    112 Application Data
    100 12.257…   13.88.31.235      192.168.1.216     TLSv1…    101 Application Data
    101 12.306…   192.168.1.216     13.88.31.235      TCP        54 50938 → 443 [ACK] Seq=59 Ack=48 Win=512 Len=0
    102 12.411…   WistronN_06:b0…   Broadcast         ARP        42 Who has 192.168.1.179? Tell 192.168.1.1
    103 12.411…   192.168.1.170     224.0.0.251       MDNS      189 Standard query response 0x0000 PTR Saylee’s iPhone._rdlink._tcp.local TXT OPT
    104 12.411…   fe80::86f:eeba…   ff02::fb          MDNS      209 Standard query response 0x0000 PTR Saylee’s iPhone._rdlink._tcp.local TXT OPT
    105 13.110…   192.168.1.216     162.125.20.2      TLSv1…    209 Application Data
    106 13.110…   192.168.1.216     162.125.20.2      TLSv1…    129… Application Data
    107 13.128…   162.125.20.2      192.168.1.216     TCP        54 443 → 51878 [ACK] Seq=1 Ack=1596 Win=130 Len=0
    108 13.132…   162.125.20.2      192.168.1.216     TCP        54 443 → 51878 [ACK] Seq=1 Ack=13050 Win=130 Len=0
    109 13.132…   162.125.20.2      192.168.1.216     TLSv1…    819 Application Data
    110 13.186…   192.168.1.216     162.125.20.2      TCP        54 51878 → 443 [ACK] Seq=13050 Ack=766 Win=514 Len=0
```

```
Frame 105: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NP
    Section number: 1
  Interface id: 0 (\Device\NPF_{5B283E4C-8BA2-4162-A62B-0A6A6EC68A93})
      Interface name: \Device\NPF_{5B283E4C-8BA2-4162-A62B-0A6A6EC68A93}
      Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  1, 2023 02:58:32.618130000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677657512.618130000 seconds
    [Time delta from previous captured frame: 0.699071000 seconds]
    [Time delta from previous displayed frame: 0.699071000 seconds]
    [Time since reference or first frame: 13.110212000 seconds]
    Frame Number: 105
    Frame Length: 209 bytes (1672 bits)
    Capture Length: 209 bytes (1672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
```

```
0000  78 67 0e 06 b0 0d 24 ee  9a 5d ab dd 08 00 45 00   xg····$· ·]····E·
0010  00 c3 9c f0 40 00 80 06  00 00 c0 a8 01 d8 a2 7d   ····@··· ·······}
0020  14 02 ca a6 01 bb 0c d5  37 a1 19 7f 77 6b 50 18   ········ 7···wkP·
0030  02 05 79 b5 00 00 17 03  03 00 96 00 00 00 00 00   ··y····· ········
0040  00 00 10 8e 3c 68 61 db  4e 94 4e 11 01 7f 9e ae   ····<ha· N·N·····
0050  89 1e b1 69 84 89 22 0b  8e be c2 65 40 0c 85 1c   ···i··"· ···e@···
0060  76 7c 45 cc 5d 20 43 21  63 ec cd 8e 53 98 c2 03   v|E·] C! c···S···
0070  61 ab b6 de 7b 48 84 8d  f4 62 cf 31 40 cb cf 24   a···{H·· ·b·1@··$
0080  0c 59 d8 d6 d1 fe 2b 23  c8 33 7c b5 90 f4 7b a9   ·Y····+# ·3|···{·
0090  ca 5b 30 6e 1b 8d 11 67  97 a2 30 62 05 6f 6d b4   ·[0n···g ··0b·om·
00a0  49 60 1d 65 d5 1a fe 29  7c 85 42 6c 5d b3 97 42   I`·e···) |·Bl]··B
00b0  ed 15 3e ef 51 10 3d dc  80 e9 c1 7f 36 0e f0 01   ··>·Q·=· ····6···
00c0  71 2f ff bc 36 01 af 78  09 90 9d 21 70 b4 19 37   q/··6··x ···!p··7
00d0  a9                                                ·
```

Frame (frame), 209 bytes | Packets: 110 · Displayed: 110 (100.0%) · Dropped: 0 (0.0%) | Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

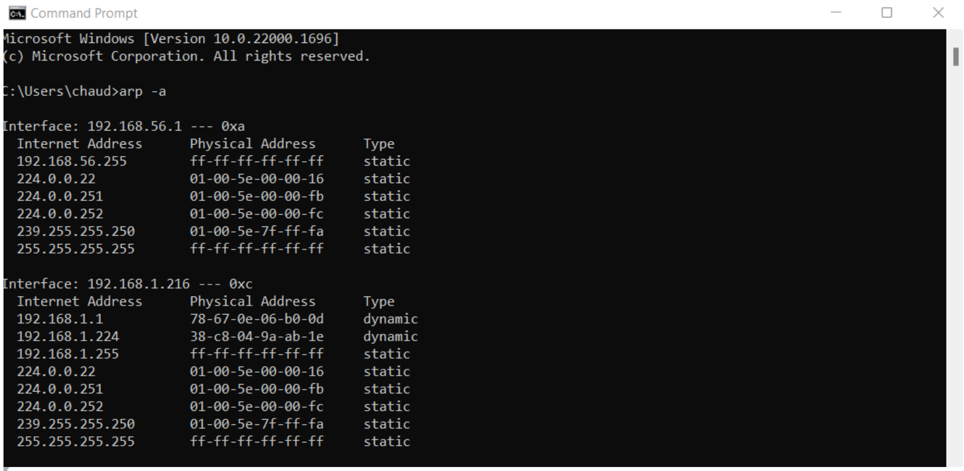
tcp.port==80

```
No.     Time      Source            Destination       Protocol Length Info
    117 10.725…   52.37.45.47       192.168.1.216     TCP        66 443 → 51934 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM WS=256
    118 10.725…   192.168.1.216     52.37.45.47       TCP        54 51934 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    119 10.725…   192.168.1.216     52.37.45.47       TLSv1…    571 Client Hello
    120 10.794…   52.37.45.47       192.168.1.216     TCP        54 443 → 51934 [ACK] Seq=1 Ack=518 Win=28160 Len=0
    121 10.794…   52.37.45.47       192.168.1.216     TLSv1…    159 Server Hello
    122 10.794…   52.37.45.47       192.168.1.216     TLSv1…     60 Change Cipher Spec
    123 10.794…   52.37.45.47       192.168.1.216     TLSv1…     99 Encrypted Handshake Message
    124 10.794…   192.168.1.216     52.37.45.47       TCP        54 51934 → 443 [ACK] Seq=518 Ack=157 Win=131072 Len=0
    125 10.795…   192.168.1.216     52.37.45.47       TLSv1…    105 Change Cipher Spec, Encrypted Handshake Message
    126 10.796…   192.168.1.216     52.37.45.47       TLSv1…    159 Application Data
    127 10.796…   192.168.1.216     52.37.45.47       TLSv1…   2295 Application Data
    128 10.863…   52.37.45.47       192.168.1.216     TCP        54 443 → 51934 [ACK] Seq=157 Ack=569 Win=28160 Len=0
    129 10.863…   52.37.45.47       192.168.1.216     TLSv1…    123 Application Data
    130 10.863…   192.168.1.216     52.37.45.47       TLSv1…     92 Application Data
    131 10.867…   52.37.45.47       192.168.1.216     TCP        54 443 → 51934 [ACK] Seq=226 Ack=2915 Win=46080 Len=0
    132 10.867…   52.37.45.47       192.168.1.216     TLSv1…     92 Application Data
    133 10.909…   192.168.1.216     52.37.45.47       TCP        54 51934 → 443 [ACK] Seq=2953 Ack=264 Win=131072 Len=0
    134 10.915…   52.37.45.47       192.168.1.216     TLSv1…    389 Application Data
    135 10.971…   192.168.1.216     52.37.45.47       TCP        54 51934 → 443 [ACK] Seq=2953 Ack=599 Win=130560 Len=0
    136 10.975…   52.37.45.47       192.168.1.216     TCP        54 443 → 51934 [ACK] Seq=599 Ack=2953 Win=46080 Len=0
    137 11.181…   13.107.246.254    192.168.1.216     TCP        54 443 → 51915 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    138 12.866    192.168.1.216     142.251.16.1      TCP        55 51021 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
```

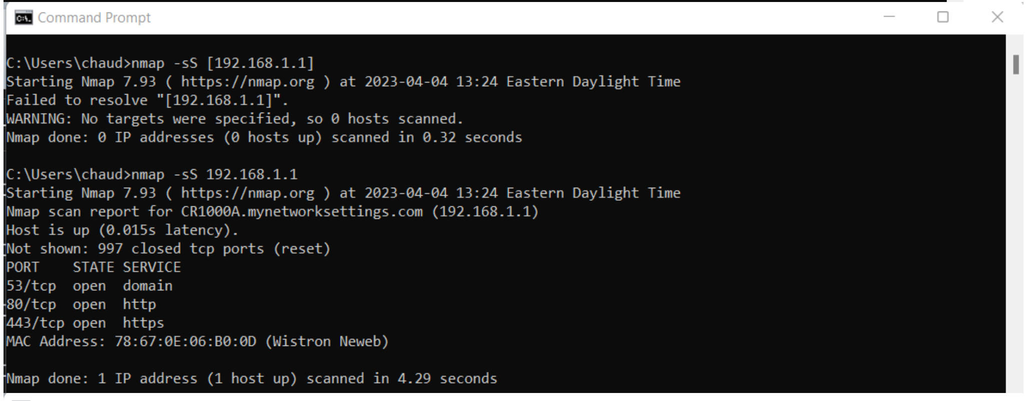
```
Frame 129: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF_
    Section number: 1
  Interface id: 0 (\Device\NPF_{5B283E4C-8BA2-4162-A62B-0A6A6EC68A93})
      Interface name: \Device\NPF_{5B283E4C-8BA2-4162-A62B-0A6A6EC68A93}
      Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  1, 2023 02:59:24.869274000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677657564.869274000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 10.863686000 seconds]
    Frame Number: 129
    Frame Length: 123 bytes (984 bits)
    Capture Length: 123 bytes (984 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
```

```
0000  24 ee 9a 5d ab dd 0d b0  06 0e 67 78 08 00 45 00   $··]···· ··gx··E·
0010  00 6d 18 65 40 00 de 06  60 51 34 25 2d 2f c0 a8   ·m·e@··· `Q4%-/··
0020  01 d8 01 bb ca de c4 3d  e1 9a 61 d0 4e 4d 50 18   ·······= ··a·NMP·
0030  00 6e e5 71 00 00 17 03  03 00 40 00 00 00 00 00   ·n·q···· ··@·····
0040  00 00 01 da 6f 1b c5 80  c4 19 71 56 47 63 54 ef   ····o··· ··qVGcT·
0050  fd fc 8d ec c9 e7 d3 e4  6c e2 1b 4e c2 39 9c 4a   ········ l··N·9·J
0060  2e 7f 63 5d 93 b0 e5 41  3e 87 a7 88 bd 86 23 53   .·c]···A >·····#S
0070  56 8a fb ff 0e 3d 52 13  b6 07 d6                  V····=R· ···
```

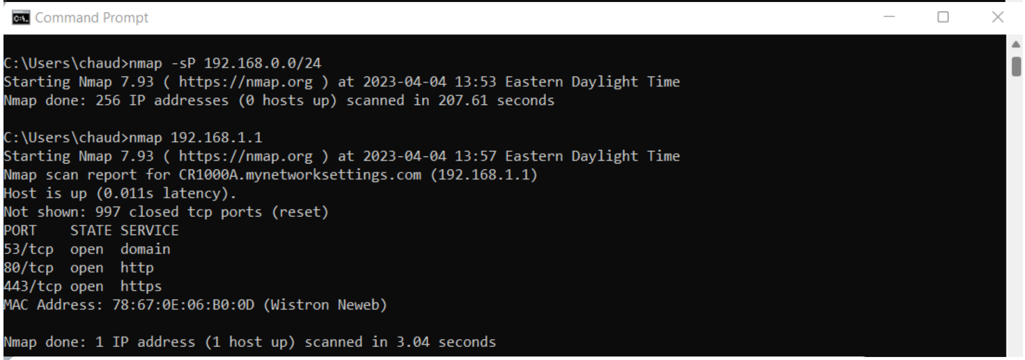
Frame (frame), 123 bytes | Packets: 140 · Displayed: 140 (100.0%) · Dropped: 0 (0.0%) | Profile: Default



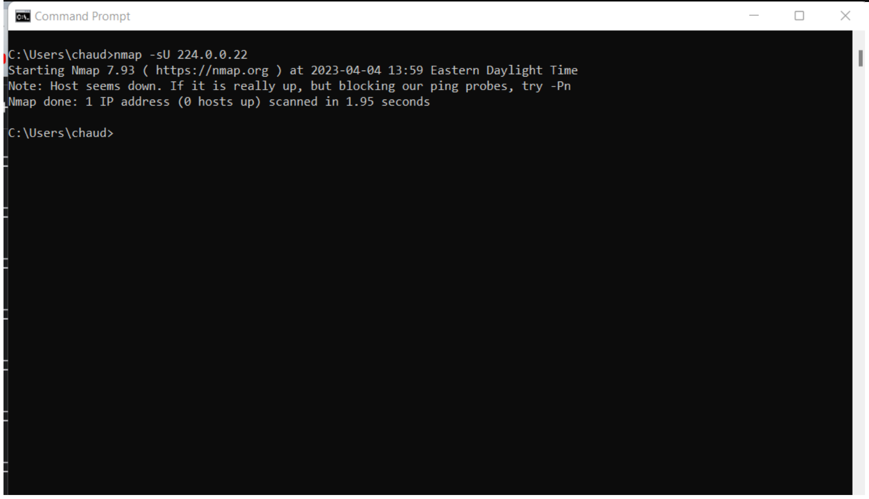
```
icrosoft Windows [Version 10.0.22000.1696]
(c) Microsoft Corporation. All rights reserved.

:\Users\chaud>arp -a

nterface: 192.168.56.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

nterface: 192.168.1.216 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           78-67-0e-06-b0-0d     dynamic
  192.168.1.224         38-c8-04-9a-ab-1e     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```



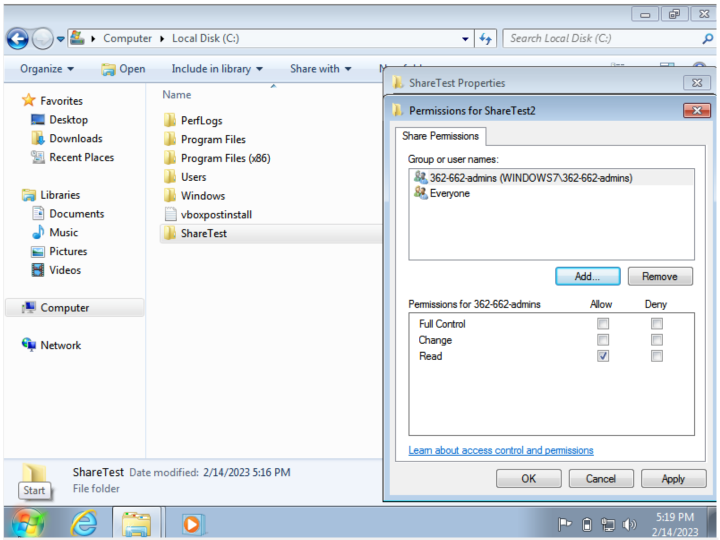
```
C:\Users\chaud>nmap -sS [192.168.1.1]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 13:24 Eastern Daylight Time
Failed to resolve "[192.168.1.1]".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.32 seconds

C:\Users\chaud>nmap -sS 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 13:24 Eastern Daylight Time
Nmap scan report for CR1000A.mynetworksettings.com (192.168.1.1)
Host is up (0.015s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 78:67:0E:06:B0:0D (Wistron Neweb)

Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds
```



```
C:\Users\chaud>nmap -sP 192.168.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 13:53 Eastern Daylight Time
Nmap done: 256 IP addresses (0 hosts up) scanned in 207.61 seconds

C:\Users\chaud>nmap 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 13:57 Eastern Daylight Time
Nmap scan report for CR1000A.mynetworksettings.com (192.168.1.1)
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 78:67:0E:06:B0:0D (Wistron Neweb)

Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds
```



```
C:\Users\chaud>nmap -sU 224.0.0.22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 13:59 Eastern Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.95 seconds

C:\Users\chaud>
```



ShareTest Date modified: 2/14/2023 5:16 PM
File folder

ShareTest Properties

Permissions for ShareTest2

Share Permissions

Group or user names:

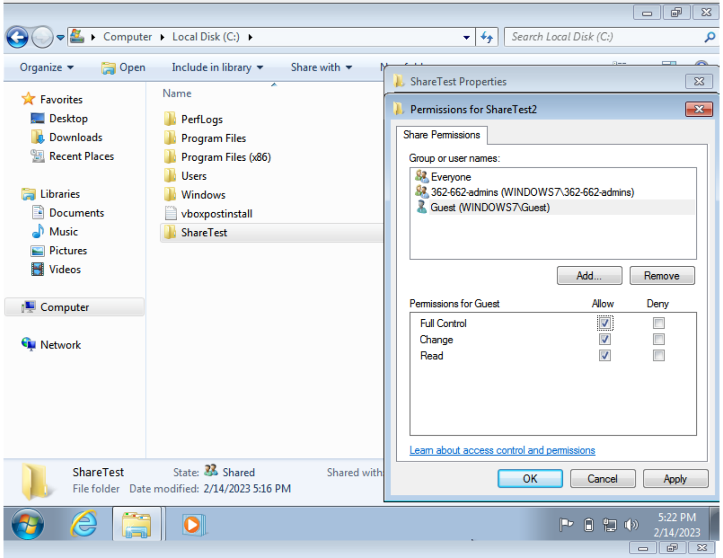
- 362-662-admins (WINDOWS7\362-662-admins)
- Everyone

Add... Remove

Permissions for 362-662-admins	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Learn about access control and permissions

OK Cancel Apply



ShareTest State: Shared Shared with:
File folder Date modified: 2/14/2023 5:16 PM

ShareTest Properties

Permissions for ShareTest2

Share Permissions

Group or user names:

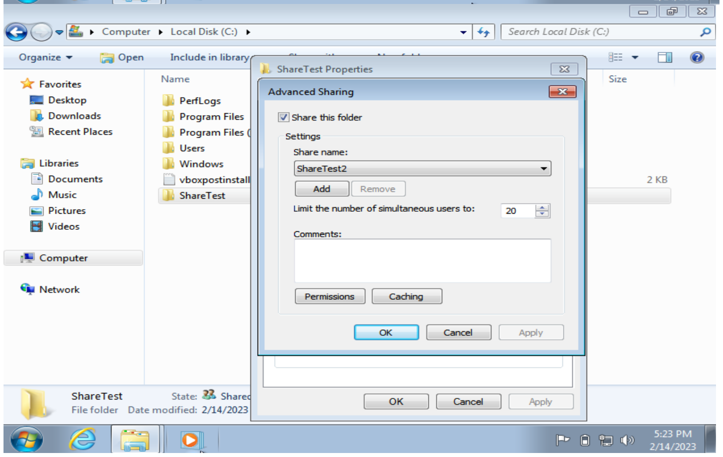
- Everyone
- 362-662-admins (WINDOWS7\362-662-admins)
- Guest (WINDOWS7\Guest)

Add... Remove

Permissions for Guest	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Learn about access control and permissions

OK Cancel Apply



ShareTest State: Shared
File folder Date modified: 2/14/2023

ShareTest Properties

Advanced Sharing

☑ Share this folder

Settings

Share name:

ShareTest2

Add Remove

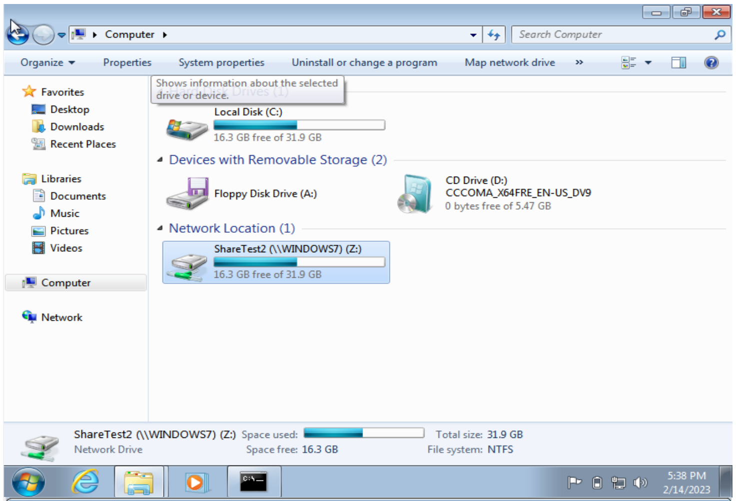
Limit the number of simultaneous users to: 20

Comments:

Permissions Caching

OK Cancel Apply

OK Cancel Apply



Shows information about the selected drive or device.

Local Disk (C:)
16.3 GB free of 31.9 GB

Devices with Removable Storage (2)

Floppy Disk Drive (A:)

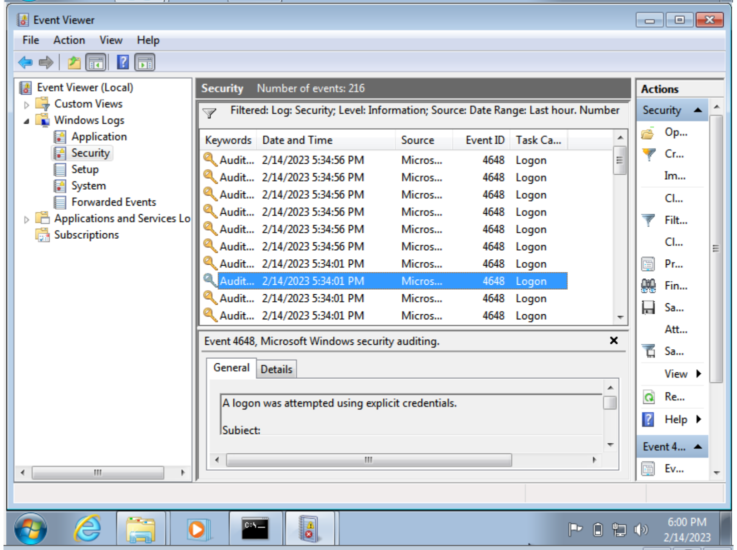
CD Drive (D:)
CCCOMA_X64FRE_EN-US_DV9
0 bytes free of 5.47 GB

Network Location (1)

ShareTest2 (\\WINDOWS7) (Z:)
16.3 GB free of 31.9 GB

ShareTest2 (\\WINDOWS7) (Z:) Space used: Total size: 31.9 GB
Network Drive Space free: 16.3 GB File system: NTFS

5:38 PM
2/14/2023



Security Number of events: 216

Filtered: Log: Security; Level: Information; Source: Date Range: Last hour. Number

Keywords	Date and Time	Source	Event ID	Task Ca...
Audit...	2/14/2023 5:34:56 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:56 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:56 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:56 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:56 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:56 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:01 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:01 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:01 PM	Micros...	4648	Logon
Audit...	2/14/2023 5:34:01 PM	Micros...	4648	Logon

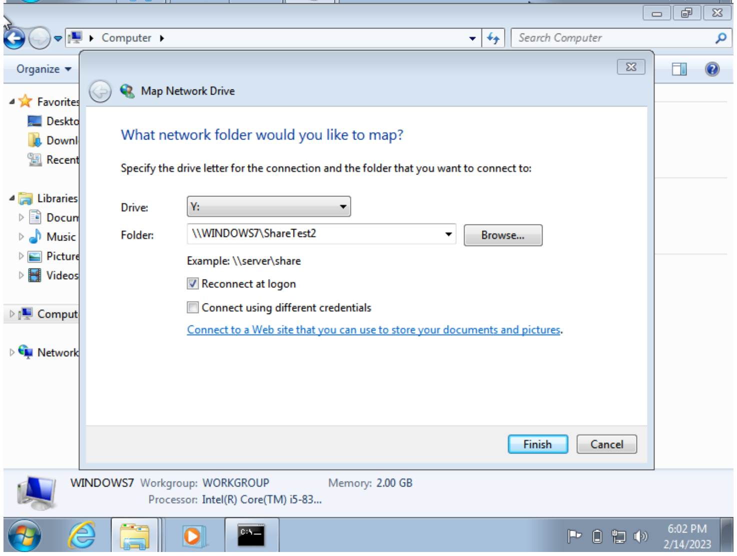
Event 4648, Microsoft Windows security auditing.

General Details

A logon was attempted using explicit credentials.

Subject:

6:00 PM
2/14/2023



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: \\WINDOWS7\ShareTest2

Example: \\server\share

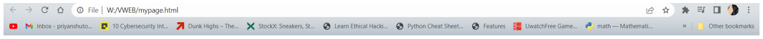
☑ Reconnect at logon

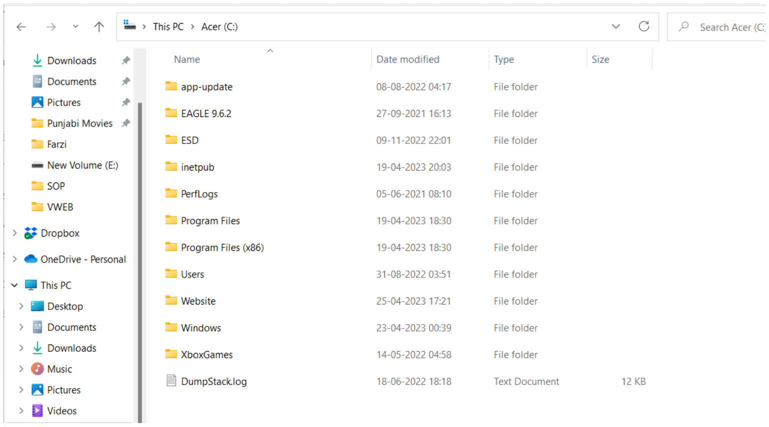
□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

WINDOWS7 Workgroup: WORKGROUP Memory: 2.00 GB
Processor: Intel(R) Core(TM) i5-83...

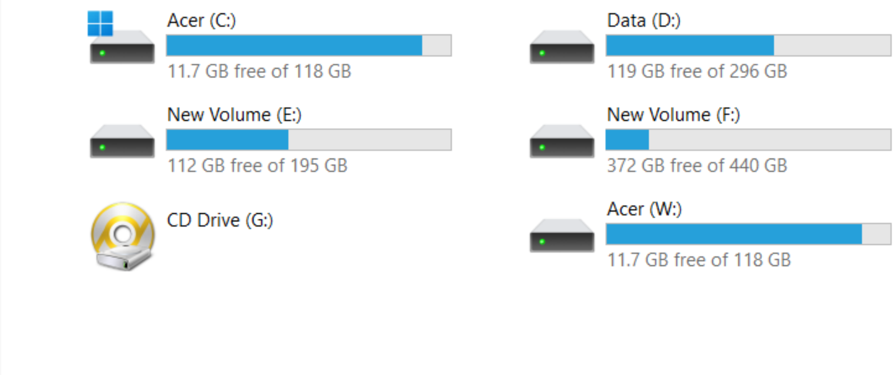
6:02 PM
2/14/2023


File | W:/VWEB/mypage.html


This PC › Acer (C:)

Search Acer (C:

Name	Date modified	Type	Size
app-update	08-08-2022 04:17	File folder	
EAGLE 9.6.2	27-09-2021 16:13	File folder	
ESD	09-11-2022 22:01	File folder	
inetpub	19-04-2023 20:03	File folder	
PerfLogs	05-06-2021 08:10	File folder	
Program Files	19-04-2023 18:30	File folder	
Program Files (x86)	19-04-2023 18:30	File folder	
Users	31-08-2022 03:51	File folder	
Website	25-04-2023 17:21	File folder	
Windows	23-04-2023 00:39	File folder	
XboxGames	14-05-2022 04:58	File folder	
DumpStack.log	18-06-2022 18:18	Text Document	12 KB


Acer (C:)
11.7 GB free of 118 GB

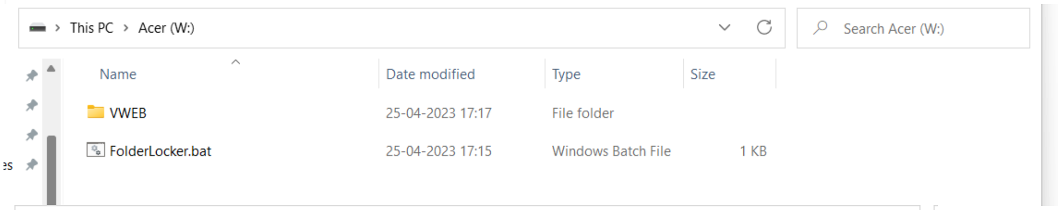
Data (D:)
119 GB free of 296 GB

New Volume (E:)
112 GB free of 195 GB

New Volume (F:)
372 GB free of 440 GB

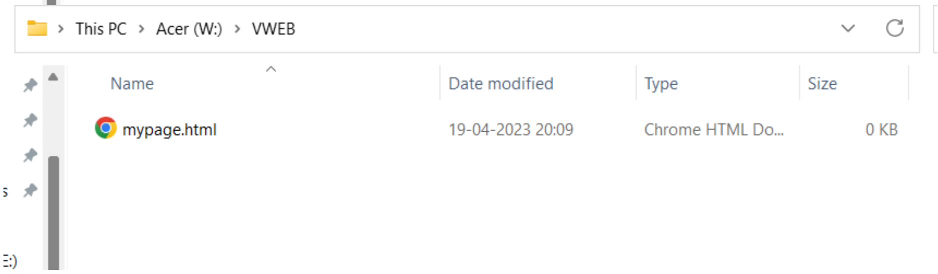
CD Drive (G:)

Acer (W:)
11.7 GB free of 118 GB

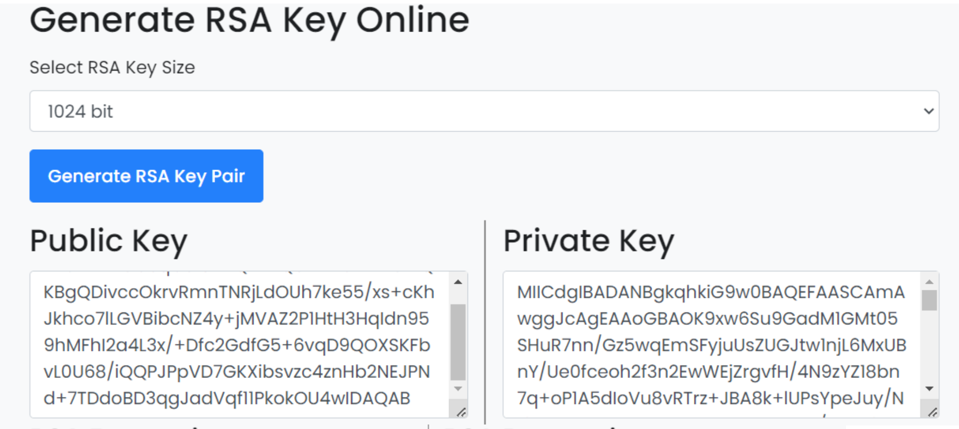

This PC › Acer (W:)

Search Acer (W:)

Name	Date modified	Type	Size
VWEB	25-04-2023 17:17	File folder	
FolderLocker.bat	25-04-2023 17:15	Windows Batch File	1 KB


This PC › Acer (W:) › VWEB

Name	Date modified	Type	Size
mypage.html	19-04-2023 20:09	Chrome HTML Do...	0 KB



Generate RSA Key Online

Select RSA Key Size

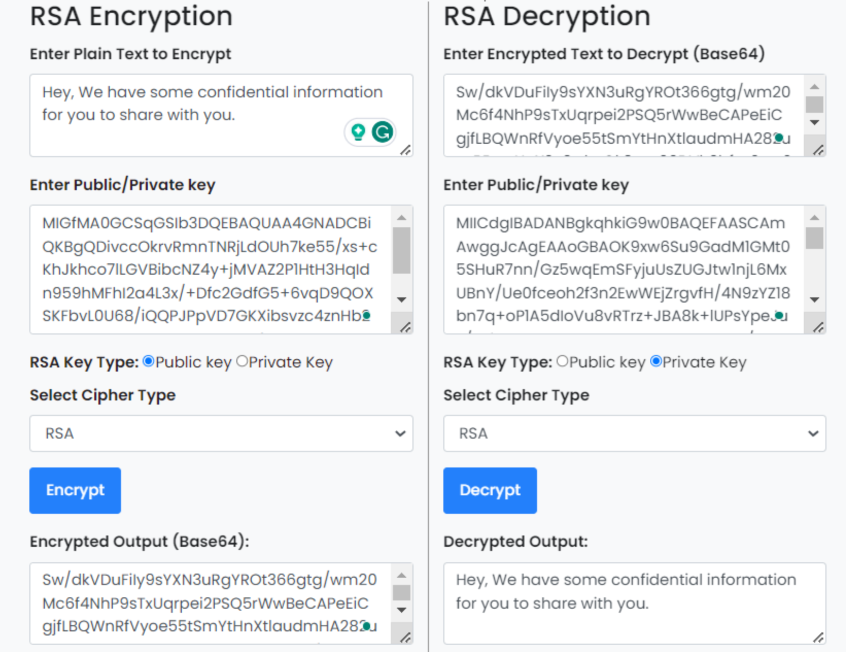
1024 bit

Public Key

KBgQDivccOkrvRmnTNRjLdOUh7ke55/xs+cKh
Jkhco7lLGVBibcNZ4y+jMVAZ2P1HtH3Hqldn95
9hMFhI2a4L3x/+Dfc2GdfG5+6vqD9QOXSKFb
vL0U68/iQQPJPpVD7GKXibsvzc4znHb2NEJPN
d+7TDdoBD3qgJadVqfl1PkokOU4wIDAQAB

Private Key

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmA
wggJcAgEAAoGBAOK9xw6Su9GadMlGMt05
SHuR7nn/Gz5wqEmSFyjuUsZUGJtw1njL6MxUB
nY/Ue0fceoh2f3n2EwWEjZrgvfH/4N9zYZ18bn
7q+oP1A5dIoVu8vRTrz+JBA8k+lUPsYpeJuy/N



RSA Encryption

Enter Plain Text to Encrypt

Hey, We have some confidential information for you to share with you.

Enter Public/Private key

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBi
QKBgQDivccOkrvRmnTNRjLdOUh7ke55/xs+c
KhJkhco7lLGVBibcNZ4y+jMVAZ2P1HtH3Hqld
n959hMFhI2a4L3x/+Dfc2GdfG5+6vqD9QOX
SKFbvL0U68/iQQPJPpVD7GKXibsvzc4znHb

RSA Key Type: ● Public key ○ Private Key

Select Cipher Type

RSA

Encrypted Output (Base64):

Sw/dkVDuFily9sYXN3uRgYROt366gtg/wm20
Mc6f4NhP9sTxUqrpei2PSQ5rWwBeCAPeEiC
gjfLBQWnRfVyoe55tSmYtHnXtlaudmHA28

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

Sw/dkVDuFily9sYXN3uRgYROt366gtg/wm20
Mc6f4NhP9sTxUqrpei2PSQ5rWwBeCAPeEiC
gjfLBQWnRfVyoe55tSmYtHnXtlaudmHA28

Enter Public/Private key

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAm
AwggJcAgEAAoGBAOK9xw6Su9GadMlGMt0
5SHuR7nn/Gz5wqEmSFyjuUsZUGJtw1njL6Mx
UBnY/Ue0fceoh2f3n2EwWEjZrgvfH/4N9zYZ18
bn7q+oP1A5dIoVu8vRTrz+JBA8k+lUPsYpe

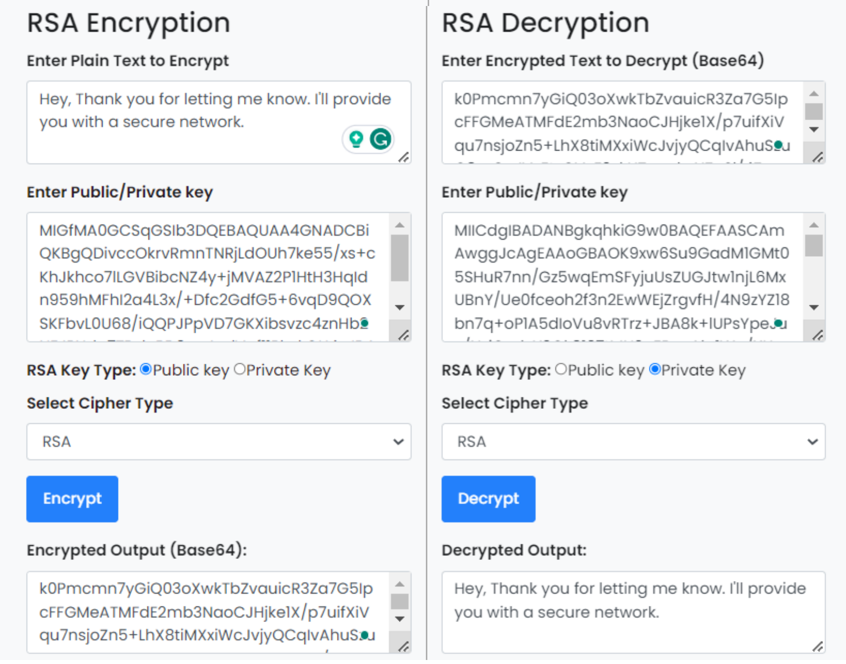
RSA Key Type: ○ Public key ● Private Key

Select Cipher Type

RSA

Decrypted Output:

Hey, We have some confidential information for you to share with you.



RSA Encryption

Enter Plain Text to Encrypt

Hey, Thank you for letting me know. I'll provide you with a secure network.

Enter Public/Private key

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBi
QKBgQDivccOkrvRmnTNRjLdOUh7ke55/xs+c
KhJkhco7lLGVBibcNZ4y+jMVAZ2P1HtH3Hqld
n959hMFhI2a4L3x/+Dfc2GdfG5+6vqD9QOX
SKFbvL0U68/iQQPJPpVD7GKXibsvzc4znHb

RSA Key Type: ● Public key ○ Private Key

Select Cipher Type

RSA

Encrypted Output (Base64):

k0Pmcmn7yGiQ03oXwkTbZvauicR3Za7G5Ip
cFFGMeATMFdE2mb3NaoCJHjke1X/p7uifXiV
qu7nsjoZn5+LhX8tiMXxiWcJvjyQCqlvAhuS

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

k0Pmcmn7yGiQ03oXwkTbZvauicR3Za7G5Ip
cFFGMeATMFdE2mb3NaoCJHjke1X/p7uifXiV
qu7nsjoZn5+LhX8tiMXxiWcJvjyQCqlvAhuS

Enter Public/Private key

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAm
AwggJcAgEAAoGBAOK9xw6Su9GadMlGMt0
5SHuR7nn/Gz5wqEmSFyjuUsZUGJtw1njL6Mx
UBnY/Ue0fceoh2f3n2EwWEjZrgvfH/4N9zYZ18
bn7q+oP1A5dIoVu8vRTrz+JBA8k+lUPsYpe

RSA Key Type: ○ Public key ● Private Key

Select Cipher Type

RSA

Decrypted Output:

Hey, Thank you for letting me know. I'll provide you with a secure network.