C-DAC
IACSD,PUNE

ENCRYPTED TRAFFIC ANALYSIS USING SSL-PROXY

PG -DITISS

Project No.25

MACHANI CHANDRA MOULI	230941223010
BACHHAV YOGESH HIRALAL	230941223053

Supervisor: Ms.Rutuja Kulkarni

Center for Development of Advanced Computing

CONTENTS

- ➢INTRODUCTION
- ➢MAIN CONCEPT
- ➢BLOCK DIAGRAM
- ➢SSL-SPLIT
- ➢APPLICATIONS OF SSL-SPLIT
- ➢IMPLEMENTATIONS
- ➢CONCLUSION
- ➢REFERENCES

INTRODUCTION

- SSL proxy is a proxy for SSL/TLS encrypted network connections.
- Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet.
- SSL, also called Transport Layer Security (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity.
- SSL relies on certificates and private-public key exchange pairs for this level of security.

INTRODUCTION

- Intercepts connections, decrypts and diverts packets to other programs (proxy specification).
- SSL proxy re-encrypts the packets and sends them to their
- original destination.
- SSL proxy supports POP3 and SMTP protocols as well.

MAIN CONCEPT

- The main concept of this project is to decrypt SSL traffic to obtain granular application information

- The scope is to control what needs to be decrypted by using Selective SSL Proxy and study encrypted traffic analysis on SSL or HTTPS.

BLOCK DIAGRAM

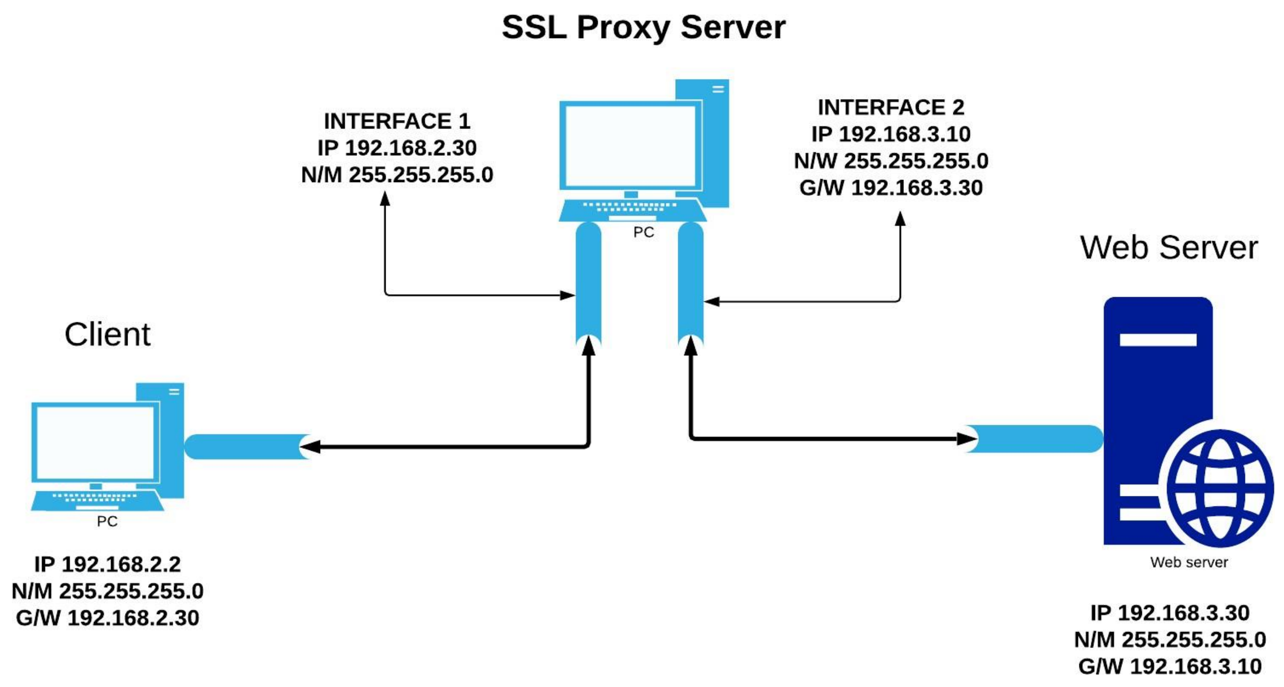
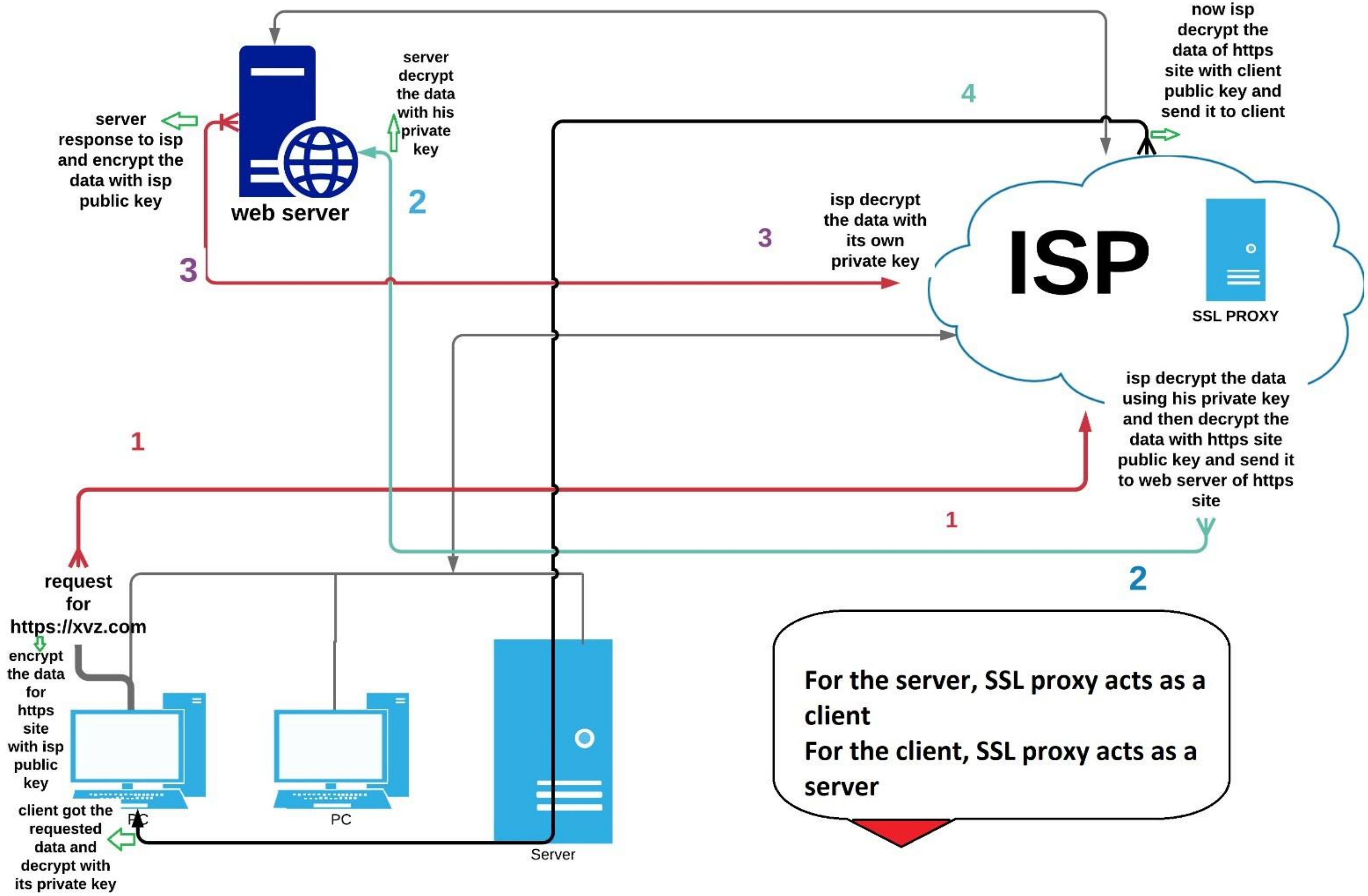


Fig: Implementation diagram for SSL proxy


now isp decrypt the data of https site with client public key and send it to client
4
server decrypt the data with his private key
server response to isp and encrypt the data with isp public key
web server
2
3
isp decrypt the data with its own private key
3
ISP
SSL PROXY
isp decrypt the data using his private key and then decrypt the data with https site public key and send it to web server of https site
1
1
2
request for https://xvz.com
encrypt the data for https site with isp public key
client got the requested data and decrypt with its private key
PC
PC
Server

For the server, SSL proxy acts as a client

For the client, SSL proxy acts as a server

SSL SPLIT

- SSL-split is a generic transparent TLS/SSL proxy for intercepting and save SSL-based traffic and thereby listen in on any secure connection.
- Works quite similar to other transparent SSL proxy tools: It acts as a middle man between the client and the actual server.
- SSL-split picks up SSL connections and pretends to be the server the client is connecting to.
- Dynamically generates a certificate and signs it with a the private key of a CA certificate that the client must trust.

Applications of SSL-SPLIT

- Network forensics
- Application security analysis
- Penetration testing

IMPLEMENTATIONS

SERVER SIDE

- Establishing APACHE web server
- Installing self-signed certificate to Apache using Open-SSL

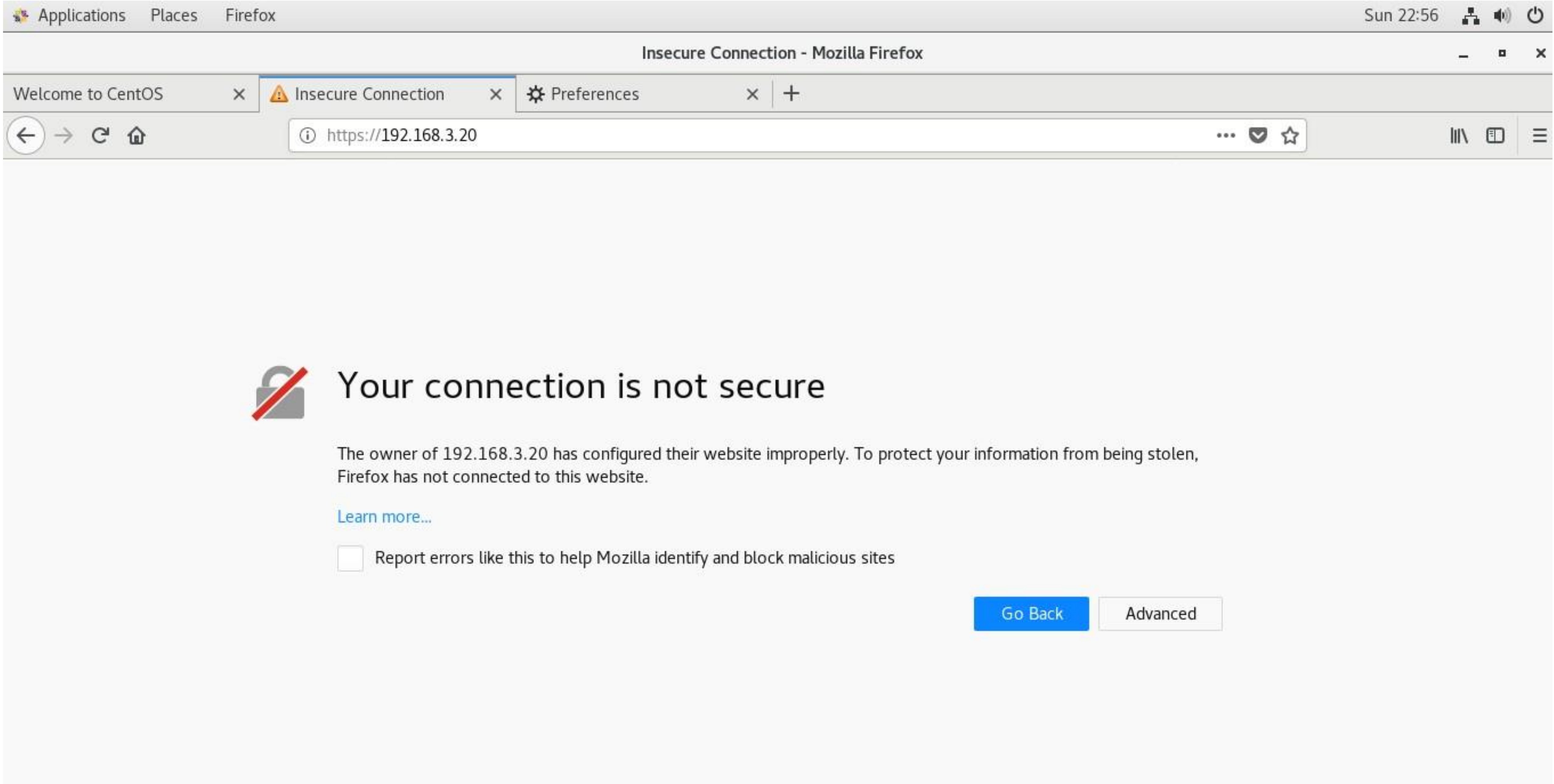
PROXY SIDE

- Installing and deploying SSL-split
- IP-Forwarding and applying IP-tables rules

CLIENT SIDE

- Setting the Gateway IP as that of SSL-PROXY’s IP
- Installing the CA certificate of SSL-PROXY

We are using a self signed certificate,so it is showing as “connection is not secure”



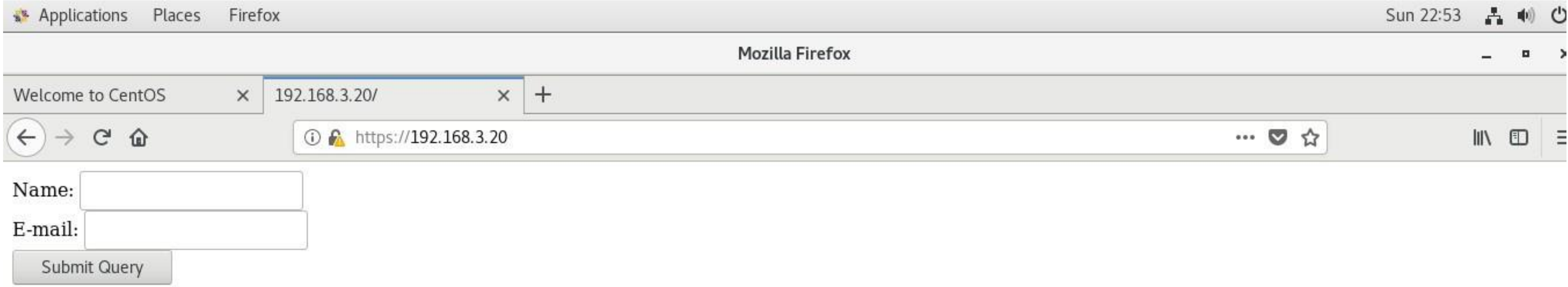
Your connection is not secure

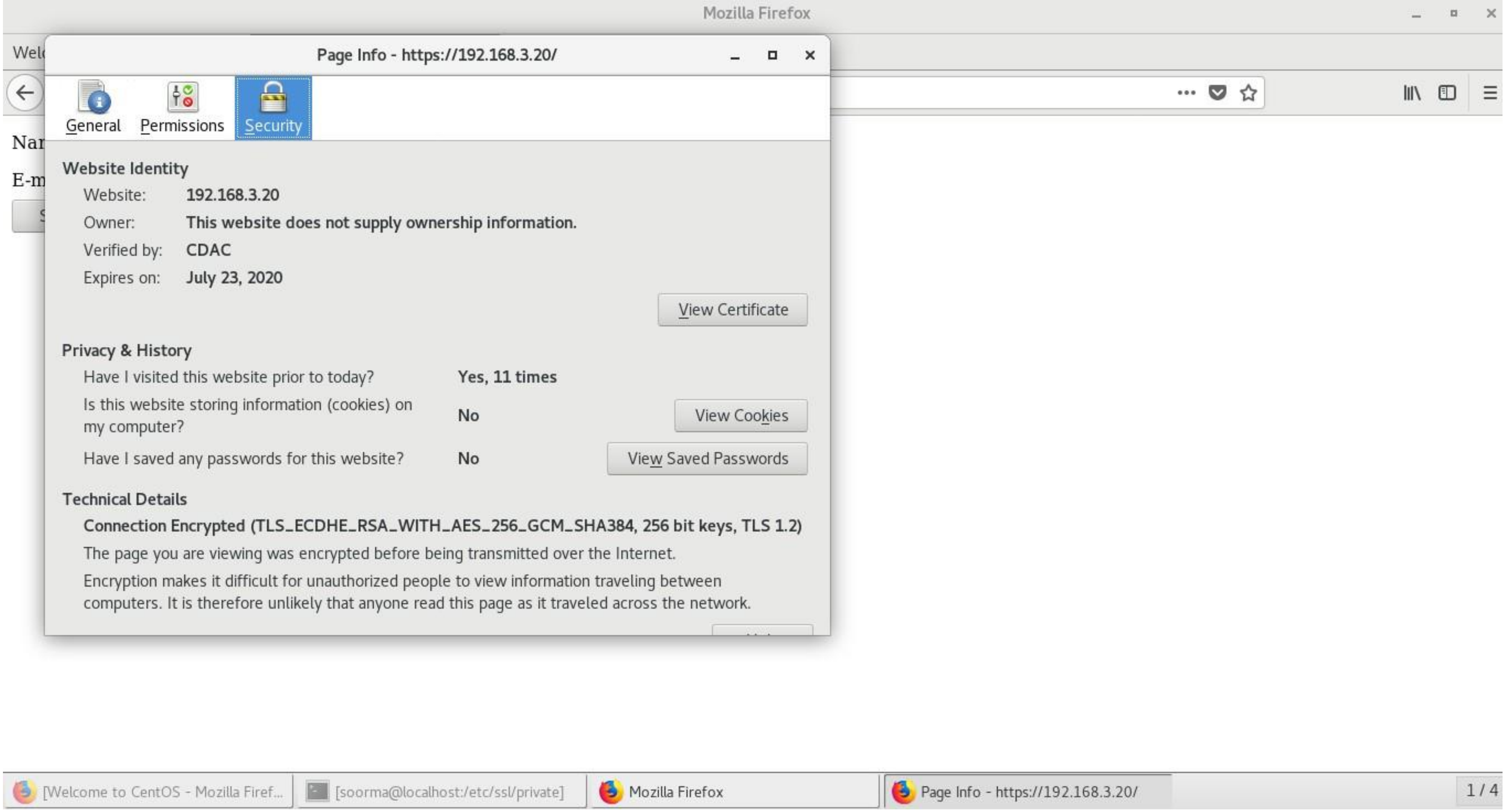
The owner of 192.168.3.20 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

After adding the exceptions that the site is showing ,we will get the site as shown:





Mozilla Firefox
Page Info - https://192.168.3.20/
General
Permissions
Security
View Certificate
View Cookies
View Saved Passwords
[Welcome to CentOS - Mozilla Firef...
[soorma@localhost:/etc/ssl/private]
Mozilla Firefox
Page Info - https://192.168.3.20/
1 / 4

Website Identity

Website: 192.168.3.20

Owner: This website does not supply ownership information.

Verified by: CDAC

Expires on: July 23, 2020

Privacy & History

Have I visited this website prior to today? Yes, 11 times

Is this website storing information (cookies) on my computer? No

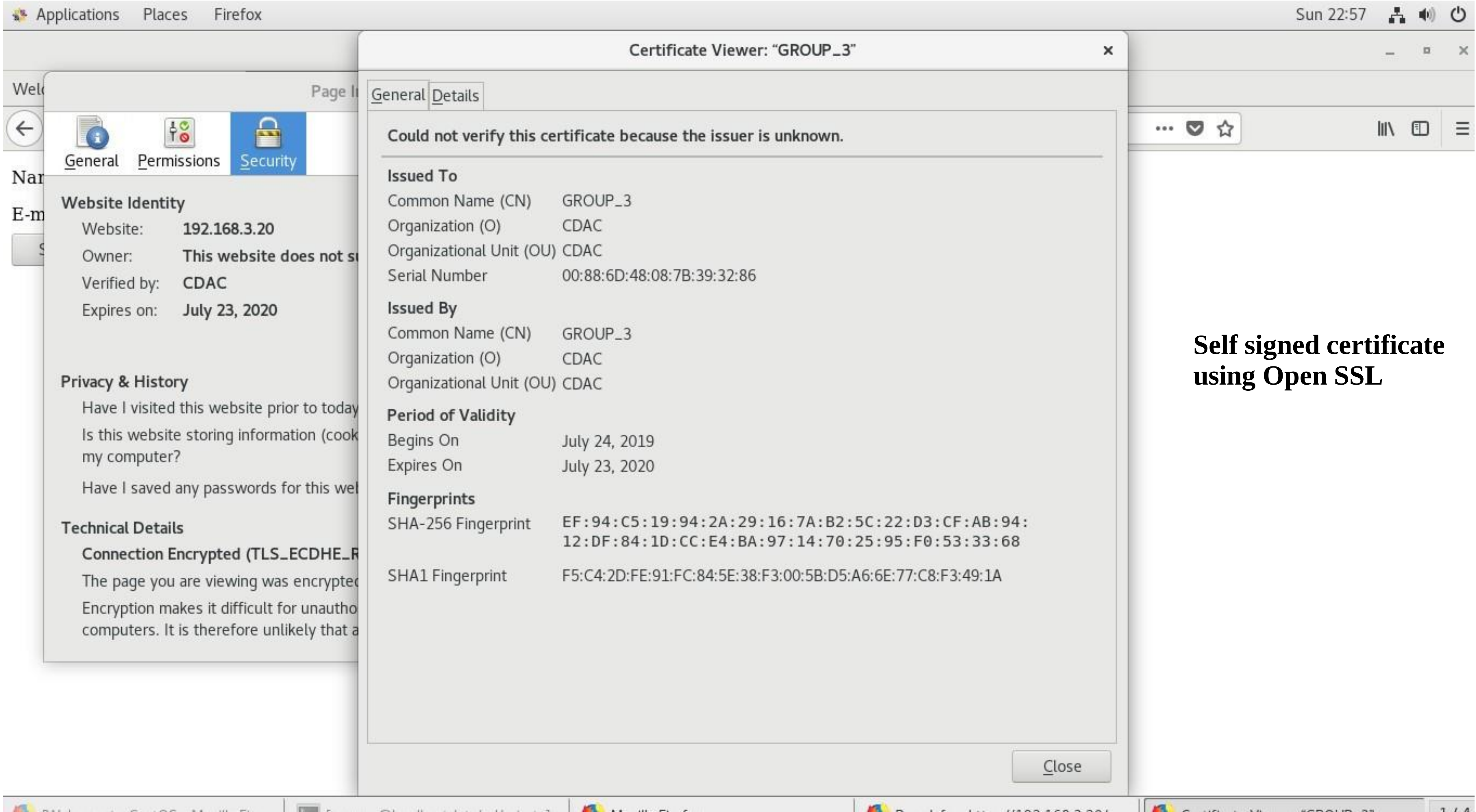
Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.



Website Identity

Website: 192.168.3.20

Owner: This website does not s

Verified by: CDAC

Expires on: July 23, 2020

Privacy & History

Have I visited this website prior to today

Is this website storing information (cook my computer?

Have I saved any passwords for this wel

Technical Details

Connection Encrypted (TLS_ECDHE_R

The page you are viewing was encrypted

Encryption makes it difficult for unautho computers. It is therefore unlikely that a

Certificate Viewer: "GROUP_3"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN) GROUP_3

Organization (O) CDAC

Organizational Unit (OU) CDAC

Serial Number 00:88:6D:48:08:7B:39:32:86

Issued By

Common Name (CN) GROUP_3

Organization (O) CDAC

Organizational Unit (OU) CDAC

Period of Validity

Begins On July 24, 2019

Expires On July 23, 2020

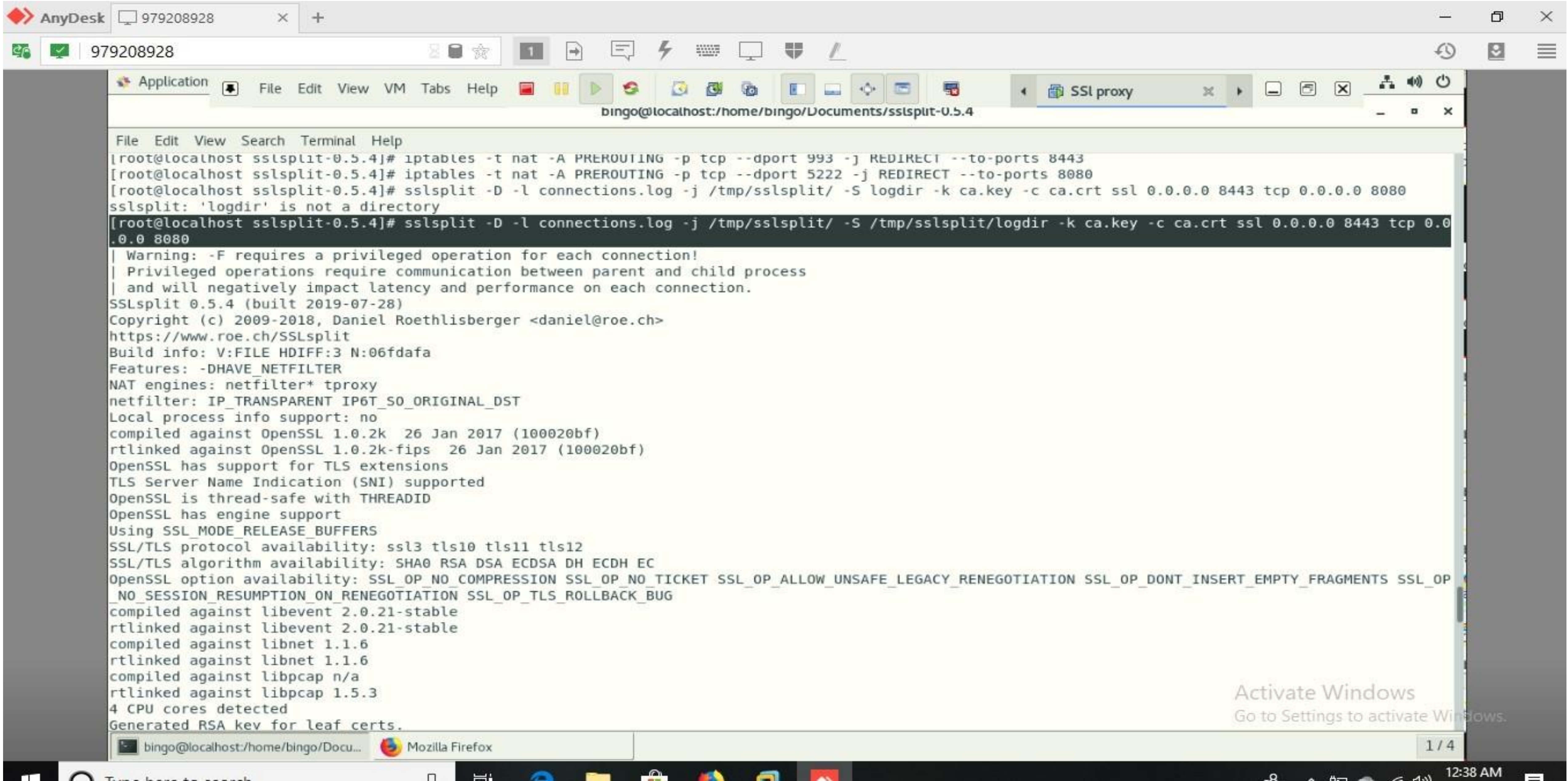
Fingerprints

SHA-256 Fingerprint EF:94:C5:19:94:2A:29:16:7A:B2:5C:22:D3:CF:AB:94:12:DF:84:1D:CC:E4:BA:97:14:70:25:95:F0:53:33:68

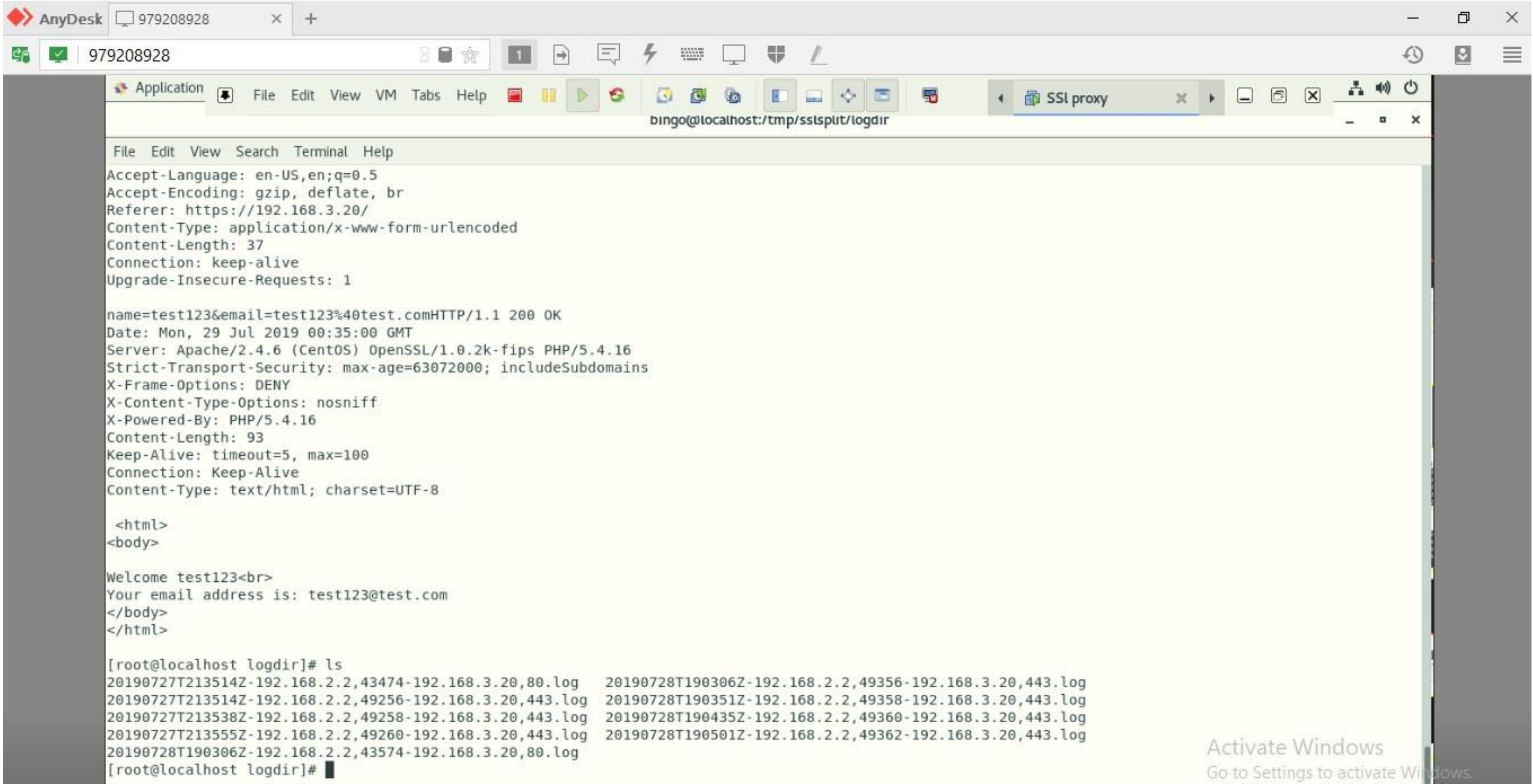
SHA1 Fingerprint F5:C4:2D:FE:91:FC:84:5E:38:F3:00:5B:D5:A6:6E:77:C8:F3:49:1A

Self signed certificate using Open SSL

Starting SSL-SPLIT

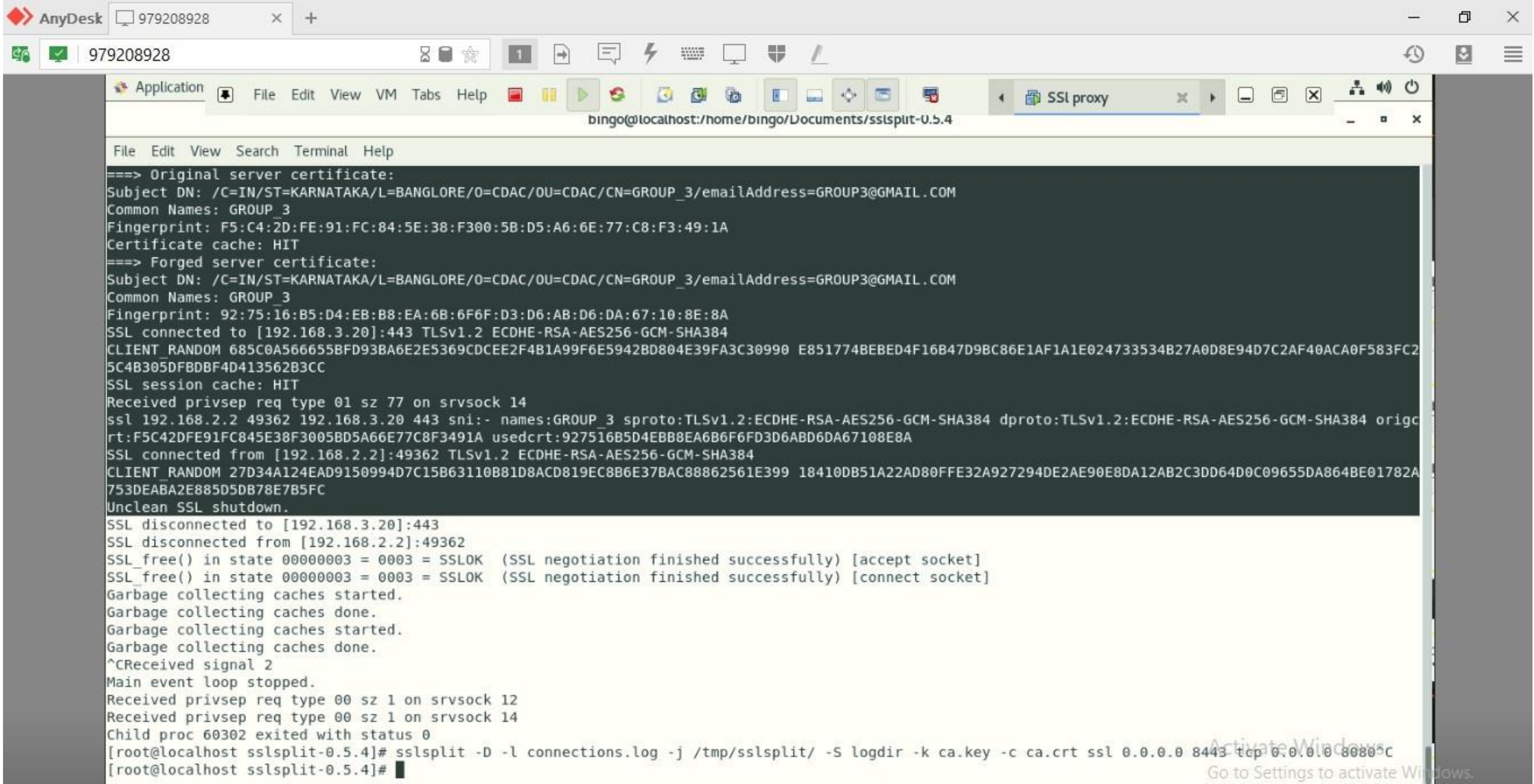


```
[root@localhost sslsplit-0.5.4]# iptables -t nat -A PREROUTING -p tcp --dport 993 -j REDIRECT --to-ports 8443
[root@localhost sslsplit-0.5.4]# iptables -t nat -A PREROUTING -p tcp --dport 5222 -j REDIRECT --to-ports 8080
[root@localhost sslsplit-0.5.4]# sslsplit -D -l connections.log -j /tmp/sslsplit/ -S logdir -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080
sslsplit: 'logdir' is not a directory
[root@localhost sslsplit-0.5.4]# sslsplit -D -l connections.log -j /tmp/sslsplit/ -S /tmp/sslsplit/logdir -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0
.0.0 8080
| Warning: -F requires a privileged operation for each connection!
| Privileged operations require communication between parent and child process
| and will negatively impact latency and performance on each connection.
SSLsplit 0.5.4 (built 2019-07-28)
Copyright (c) 2009-2018, Daniel Roethlisberger <daniel@roe.ch>
https://www.roe.ch/SSLsplit
Build info: V:FILE HDIFF:3 N:06fdafa
Features: -DHAVE_NETFILTER
NAT engines: netfilter* tproxy
netfilter: IP_TRANSPARENT IP6T_SO_ORIGINAL_DST
Local process info support: no
compiled against OpenSSL 1.0.2k  26 Jan 2017 (100020bf)
rtlinked against OpenSSL 1.0.2k-fips  26 Jan 2017 (100020bf)
OpenSSL has support for TLS extensions
TLS Server Name Indication (SNI) supported
OpenSSL is thread-safe with THREADID
OpenSSL has engine support
Using SSL_MODE_RELEASE_BUFFERS
SSL/TLS protocol availability: ssl3 tls10 tls11 tls12
SSL/TLS algorithm availability: SHA0 RSA DSA ECDSA DH ECDH EC
OpenSSL option availability: SSL_OP_NO_COMPRESSION SSL_OP_NO_TICKET SSL_OP_ALLOW_UNSAFE_LEGACY_RENEGOTIATION SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS SSL_OP
_NO_SESSION_RESUMPTION_ON_RENEGOTIATION SSL_OP_TLS_ROLLBACK_BUG
compiled against libevent 2.0.21-stable
rtlinked against libevent 2.0.21-stable
compiled against libnet 1.1.6
rtlinked against libnet 1.1.6
compiled against libpcap n/a
rtlinked against libpcap 1.5.3
4 CPU cores detected
Generated RSA key for leaf certs.
```


AnyDesk
979208928
979208928
Application
File Edit View VM Tabs Help
SSl proxy
bingo@localhost:/tmp/sslsplit/logdir
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.

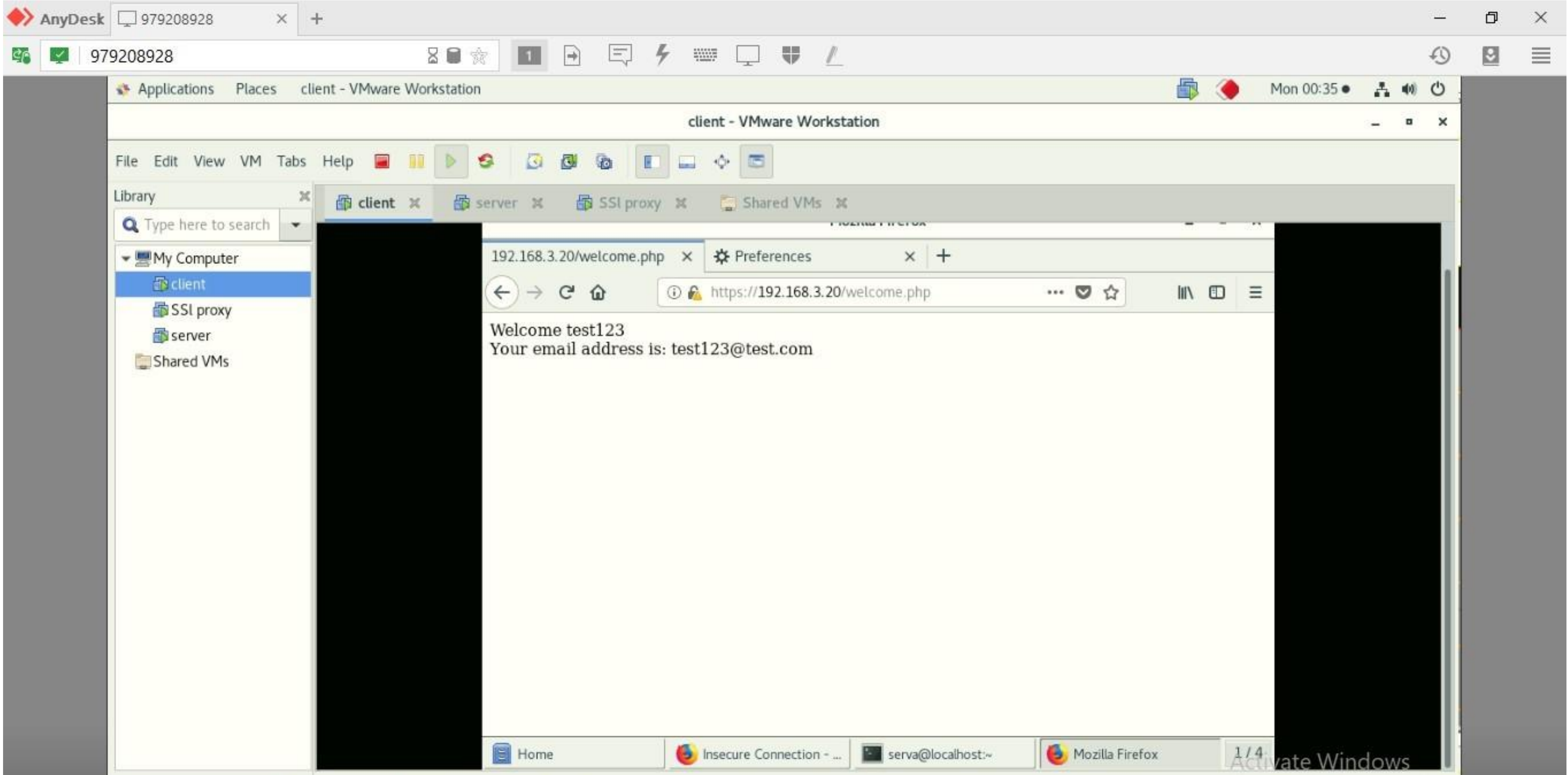
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.3.20/
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Connection: keep-alive
Upgrade-Insecure-Requests: 1

name=test123&email=test123%40test.comHTTP/1.1 200 OK
Date: Mon, 29 Jul 2019 00:35:00 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.4.16
Content-Length: 93
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

 <html>
<body>

Welcome test123<br>
Your email address is: test123@test.com
</body>
</html>

[root@localhost logdir]# ls
20190727T213514Z-192.168.2.2,43474-192.168.3.20,80.log   20190728T190306Z-192.168.2.2,49356-192.168.3.20,443.log
20190727T213514Z-192.168.2.2,49256-192.168.3.20,443.log  20190728T190351Z-192.168.2.2,49358-192.168.3.20,443.log
20190727T213538Z-192.168.2.2,49258-192.168.3.20,443.log  20190728T190435Z-192.168.2.2,49360-192.168.3.20,443.log
20190727T213555Z-192.168.2.2,49260-192.168.3.20,443.log  20190728T190501Z-192.168.2.2,49362-192.168.3.20,443.log
20190728T190306Z-192.168.2.2,43574-192.168.3.20,80.log
[root@localhost logdir]# 
```

FORGING CERTIFICATE WITH SSL-SPLIT



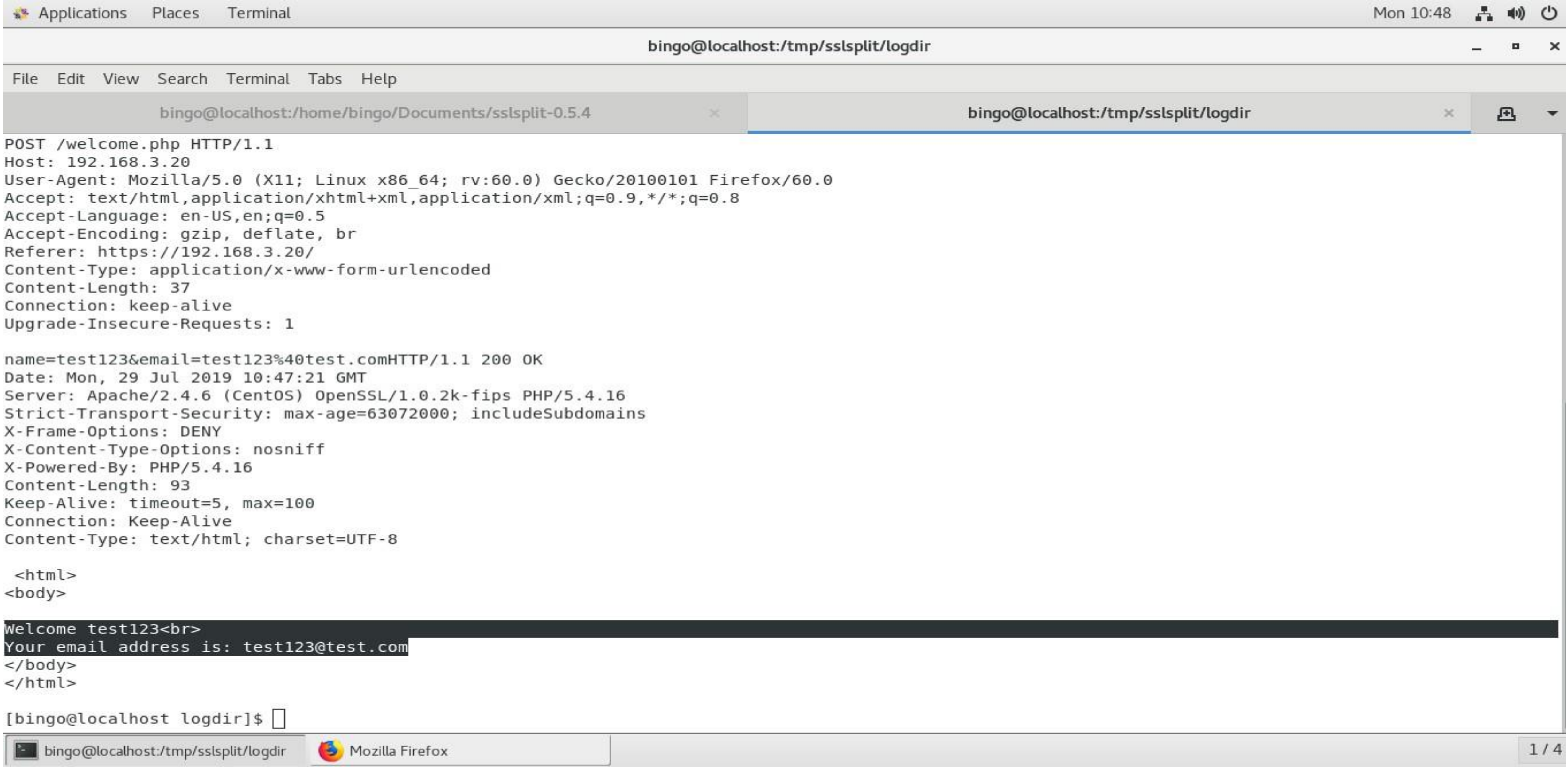
```
===> Original server certificate:
Subject DN: /C=IN/ST=KARNATAKA/L=BANGLORE/O=CDAC/OU=CDAC/CN=GROUP_3/emailAddress=GROUP3@GMAIL.COM
Common Names: GROUP_3
Fingerprint: F5:C4:2D:FE:91:FC:84:5E:38:F300:5B:D5:A6:6E:77:C8:F3:49:1A
Certificate cache: HIT
===> Forged server certificate:
Subject DN: /C=IN/ST=KARNATAKA/L=BANGLORE/O=CDAC/OU=CDAC/CN=GROUP_3/emailAddress=GROUP3@GMAIL.COM
Common Names: GROUP_3
Fingerprint: 92:75:16:B5:D4:EB:B8:EA:6B:6F6F:D3:D6:AB:D6:DA:67:10:8E:8A
SSL connected to [192.168.3.20]:443 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
CLIENT_RANDOM 685C0A566655BFD93BA6E2E5369CDCEE2F4B1A99F6E5942BD804E39FA3C30990 E851774BEBED4F16B47D9BC86E1AF1A1E024733534B27A0D8E94D7C2AF40ACA0F583FC2
5C4B305DFBDBF4D413562B3CC
SSL session cache: HIT
Received privsep req type 01 sz 77 on srvsock 14
ssl 192.168.2.2 49362 192.168.3.20 443 sni:- names:GROUP_3 sproto:TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384 dproto:TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384 origc
rt:F5C42DFE91FC845E38F3005BD5A66E77C8F3491A usedcrt:927516B5D4EBB8EA6B6F6FD3D6ABD6DA67108E8A
SSL connected from [192.168.2.2]:49362 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
CLIENT_RANDOM 27D34A124EAD9150994D7C15B63110B81D8ACD819EC8B6E37BAC88862561E399 18410DB51A22AD80FFE32A927294DE2AE90E8DA12AB2C3DD64D0C09655DA864BE01782A
753DEABA2E885D5DB78E7B5FC
Unclean SSL shutdown.
SSL disconnected to [192.168.3.20]:443
SSL disconnected from [192.168.2.2]:49362
SSL_free() in state 00000003 = 0003 = SSLOK  (SSL negotiation finished successfully) [accept socket]
SSL_free() in state 00000003 = 0003 = SSLOK  (SSL negotiation finished successfully) [connect socket]
Garbage collecting caches started.
Garbage collecting caches done.
Garbage collecting caches started.
Garbage collecting caches done.
^CReceived signal 2
Main event loop stopped.
Received privsep req type 00 sz 1 on srvsock 12
Received privsep req type 00 sz 1 on srvsock 14
Child proc 60302 exited with status 0
[root@localhost sslsplit-0.5.4]# sslsplit -D -l connections.log -j /tmp/sslsplit/ -S logdir -k ca.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080^C
[root@localhost sslsplit-0.5.4]# █
```

ON CLIENT'S BROWSER



Welcome test123
Your email address is: test123@test.com

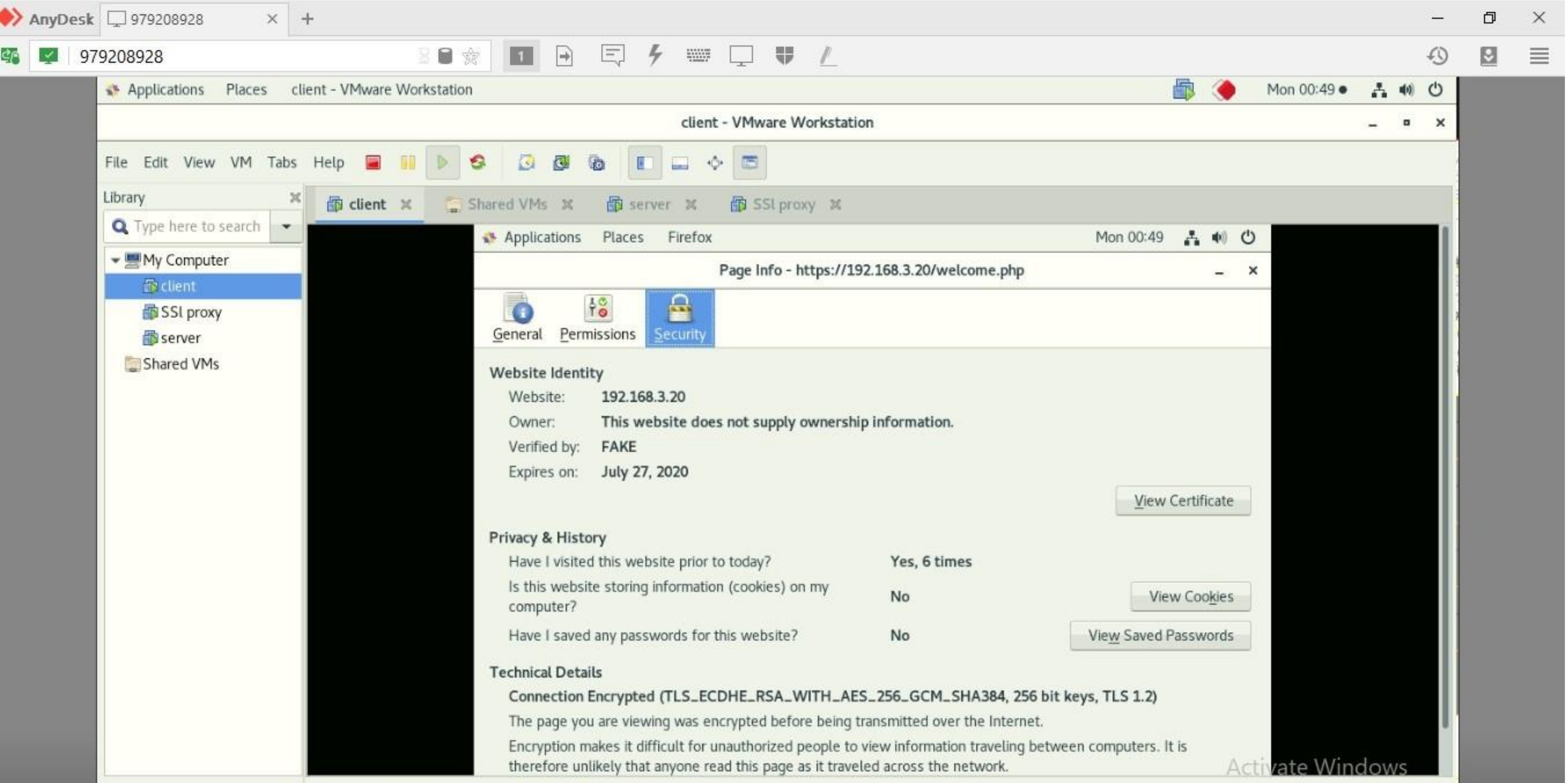
Decrypted traffic in plain text



Applications
Places
Terminal
Mon 10:48
bingo@localhost:/tmp/sslsplit/logdir
File
Edit
View
Search
Terminal
Tabs
Help
bingo@localhost:/home/bingo/Documents/sslsplit-0.5.4
bingo@localhost:/tmp/sslsplit/logdir
bingo@localhost:/tmp/sslsplit/logdir
Mozilla Firefox
1 / 4

```
POST /welcome.php HTTP/1.1
Host: 192.168.3.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.3.20/
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Connection: keep-alive
Upgrade-Insecure-Requests: 1

name=test123&email=test123%40test.comHTTP/1.1 200 OK
Date: Mon, 29 Jul 2019 10:47:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.4.16
Content-Length: 93
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

 <html>
<body>

Welcome test123<br>
Your email address is: test123@test.com
</body>
</html>

[bingo@localhost logdir]$ 
```

SSL certifcate by SSL-SPLIT (On Client’s Browser)



Page Info - https://192.168.3.20/welcome.php

Website Identity

Website: 192.168.3.20

Owner: This website does not supply ownership information.

Verified by: FAKE

Expires on: July 27, 2020

Privacy & History

Have I visited this website prior to today? Yes, 6 times

Is this website storing information (cookies) on my computer? No

Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

CONCLUSION

- Hence we are able to decrypted the non-HTTPS and HTTPS traffic into plain text through SSL-split.
- The use of this proxy will also be useful to the industries who is seeking to monitor the encrypted traffic.
- Network administrators, researchers and security experts may find this useful to detect future vulnerabilities in the implementation SSL/TLS in their organizations.

REFERENCES

- https://link.springer.com/article/10.1186/s13635-016-0030-7
- https://www.juniper.net/documentation/en_US/cso3.3/topics/concept/cp-ssl-proxy-overview.html
- https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ssl-proxy.html
- https://github.com/sonertari/SSLproxy
- https://origin-symwisedownload.symantec.com/library/SYMWISE/ENTERPRISE/sgos_ssl_proxy_deployment_guide_6_5x.pdf
- https://www.tecmint.com/install-apache-on-centos-7/
- https://www.digitalocean.com/community/tutorials/how-to-create-an-ssl-certificate-on-apache-for-centos-7
- https://blog.heckel.io/2013/08/04/use-sslsplit-to-transparently-sniff-tls-ssl-connections/

Thank you!!