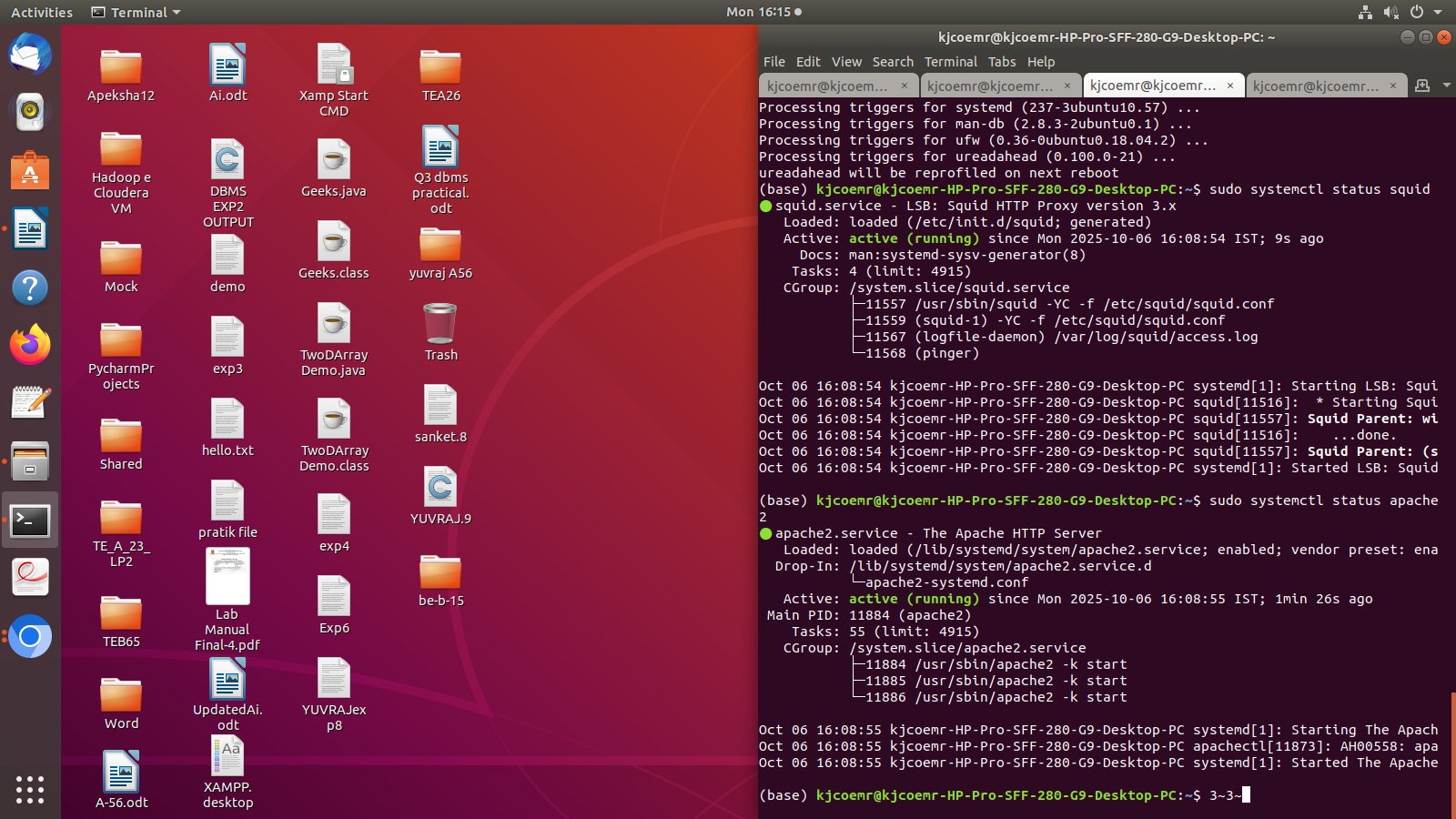
Log Capturing and Event Correlation

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ sudo apt update

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ sudo apt install squid sarg apache2 -y



(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ sudo systemctl status squid

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ export http\_proxy=http://127.0.0.1:3128

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ curl -I https://www.google.com

HTTP/1.1 200 OK

Content-Type: text/html; charset=ISO-8859-1

Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-4o5niEVgcBBMQedCtzJKpw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp

Accept-CH: Sec-CH-Prefers-Color-Scheme

P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."

Date: Mon, 06 Oct 2025 10:51:57 GMT

Server: gws

X-XSS-Protection: 0

X-Frame-Options: SAMEORIGIN

Transfer-Encoding: chunked

Expires: Mon, 06 Oct 2025 10:51:57 GMT

Cache-Control: private

Set-Cookie: AEC=AaJma5vtqs\_TLle5M\_-Rjm4bRghXI8Uo6bdjKTkD\_gZShAz6MMyMGLRJDtw; expires=Sat, 04-Apr-2026 10:51:57 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax

Set-Cookie: NID=525=feJxt6i-N3ML09HvtYWl4LdSWmNtMPW0tEmpYhf\_4QLJtChjFq1KmkojUt6IXjIyFps\_-ZOKDOayY3F0qTorOhSNdQNBnByFKsQ475ZuUINUNgDuhuaWMeukY29GYjeI5WBsKfJUjVYMBuZGv4zru3Zso50clQTmLdot66laZO32JkyaHFtXKXT\_6iKIapanmo9fD6eFcGyR7rg; expires=Tue, 07-Apr-2026 10:51:57 GMT; path=/; domain=.google.com; HttpOnly

Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ curl -I https://www.github.com

curl: (60) SSL certificate problem: self signed certificate

More details here: https://curl.haxx.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not

establish a secure connection to it. To learn more about this situation and

how to fix it, please visit the web page mentioned above.

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ curl -I https://www.ubuntu.com

HTTP/1.1 301

server: nginx/1.14.0 (Ubuntu)

date: Mon, 06 Oct 2025 10:52:10 GMT

content-type: text/html

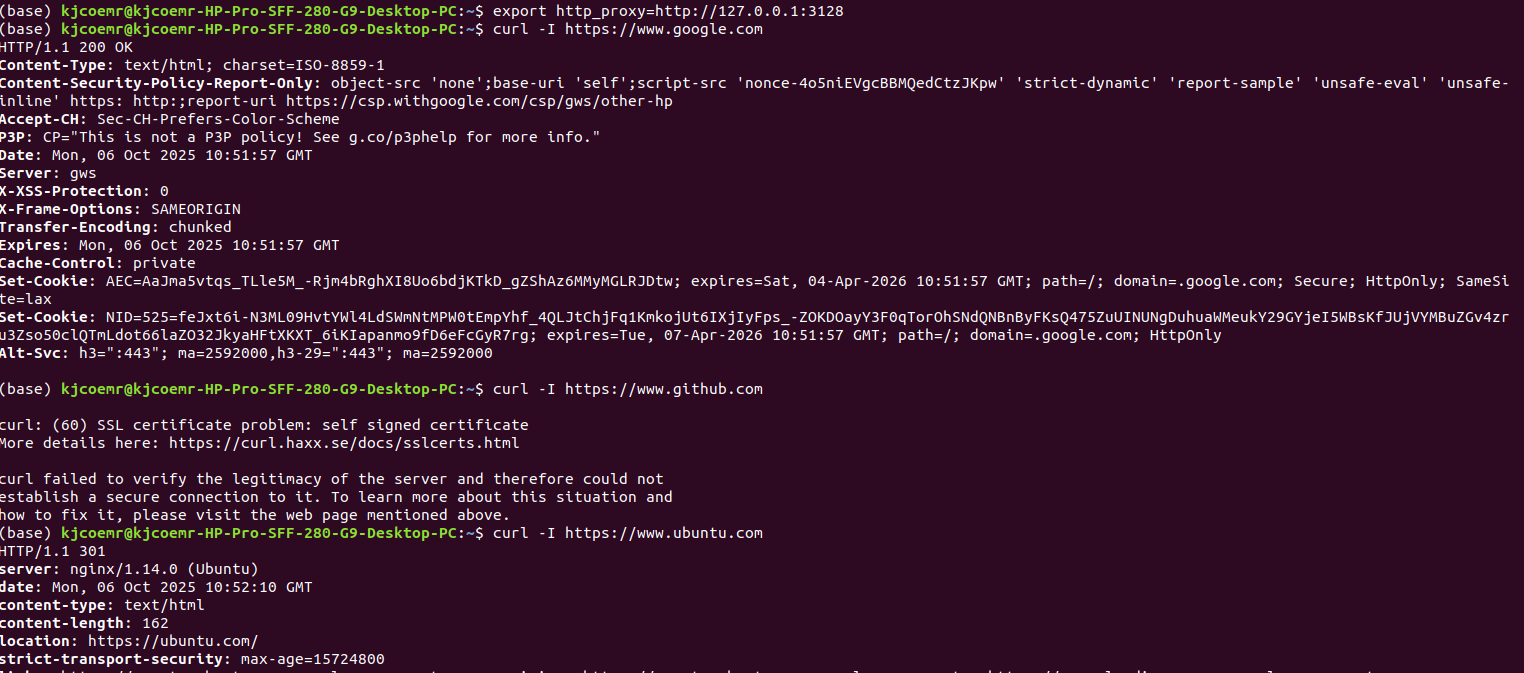
content-length: 162

location: https://ubuntu.com/

strict-transport-security: max-age=15724800

link: <https://assets.ubuntu.com>; rel=preconnect; crossorigin, <https://assets.ubuntu.com>; rel=preconnect, <https://res.cloudinary.com>; rel=preconnect

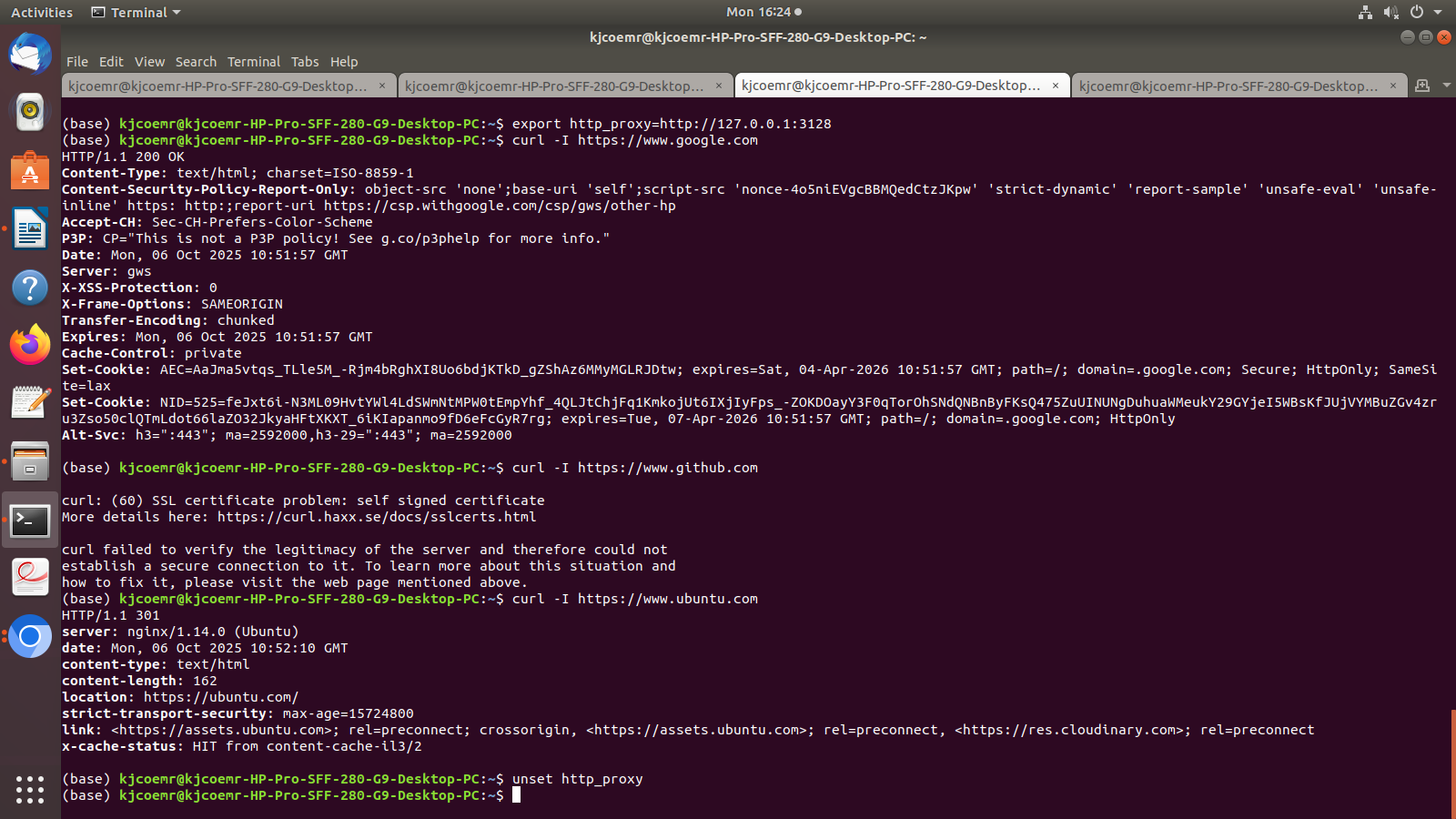
x-cache-status: HIT from content-cache-il3/2

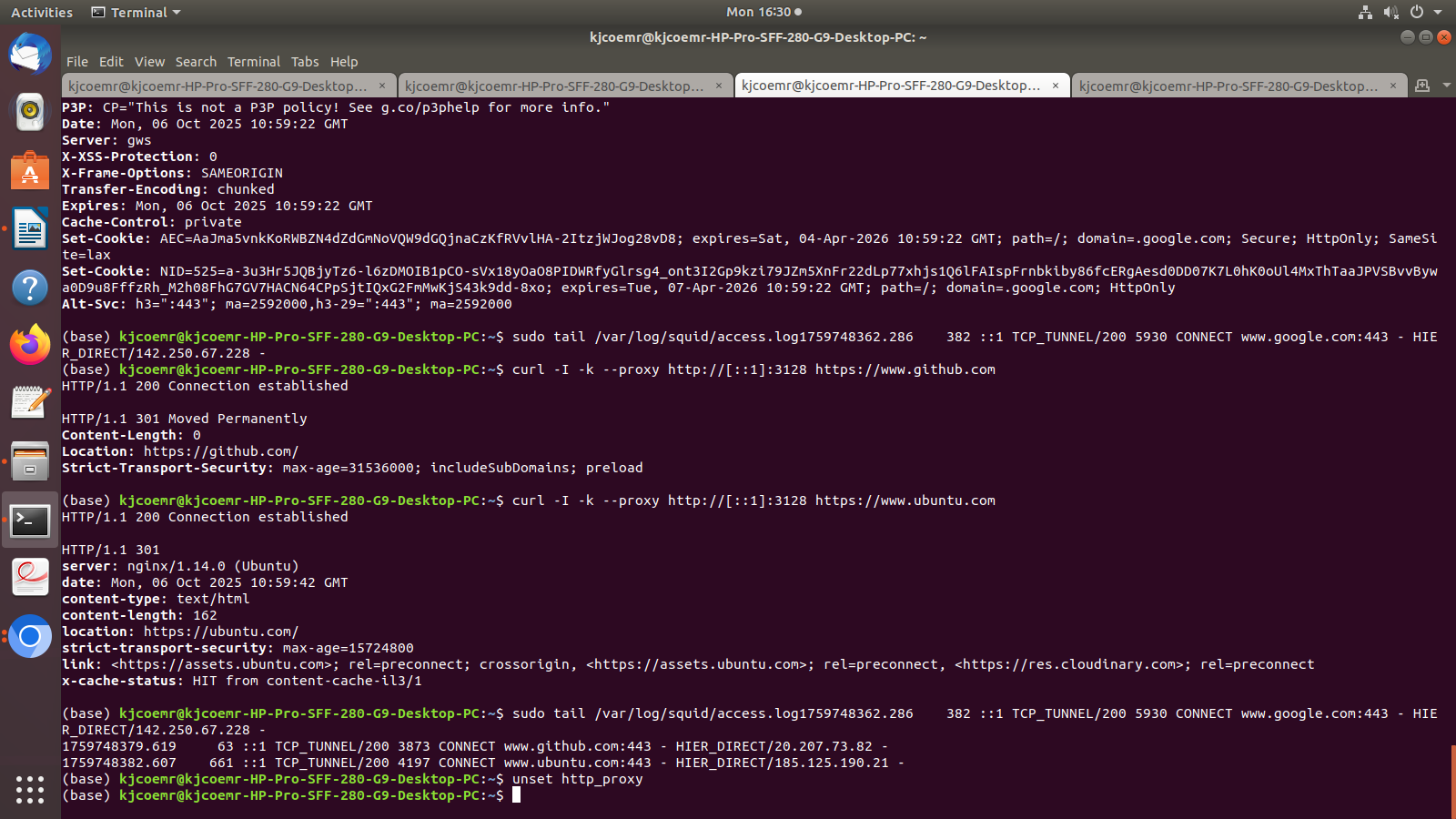


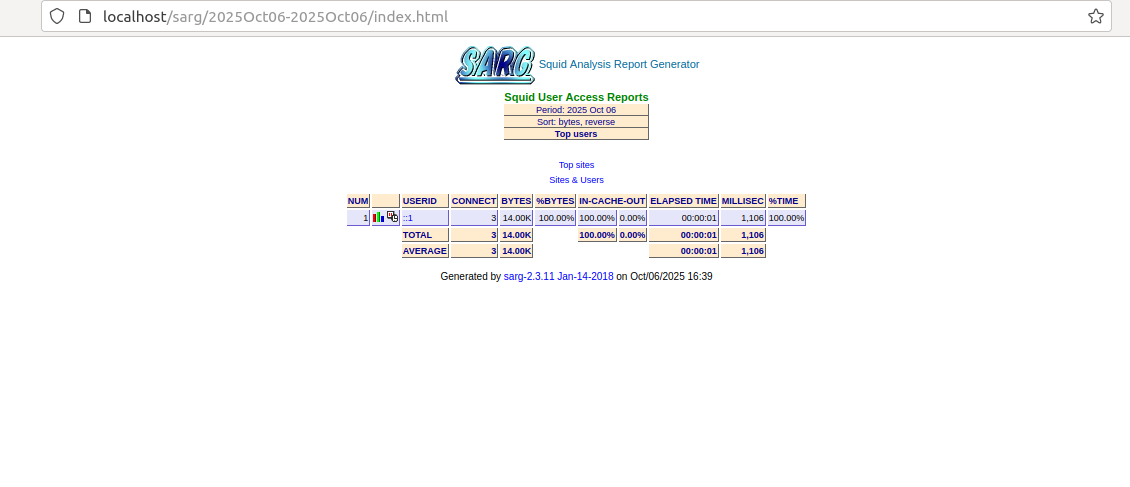
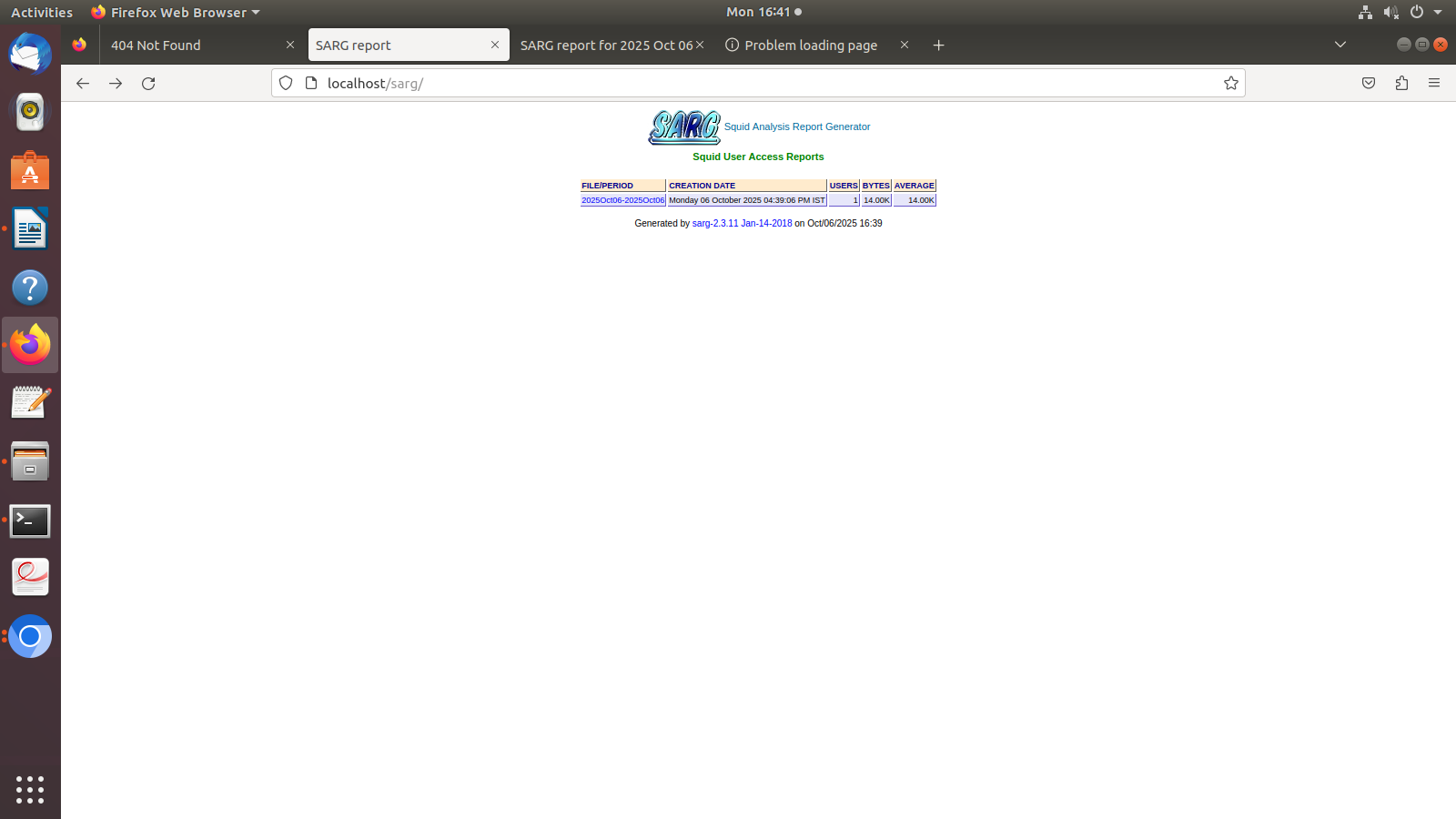
(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~$ sudo tail /var/log/squid/access.log1759748362.286 382 ::1 TCP\_TUNNEL/200 5930 CONNECT www.google.com:443 - HIER\_DIRECT/142.250.67.228 -

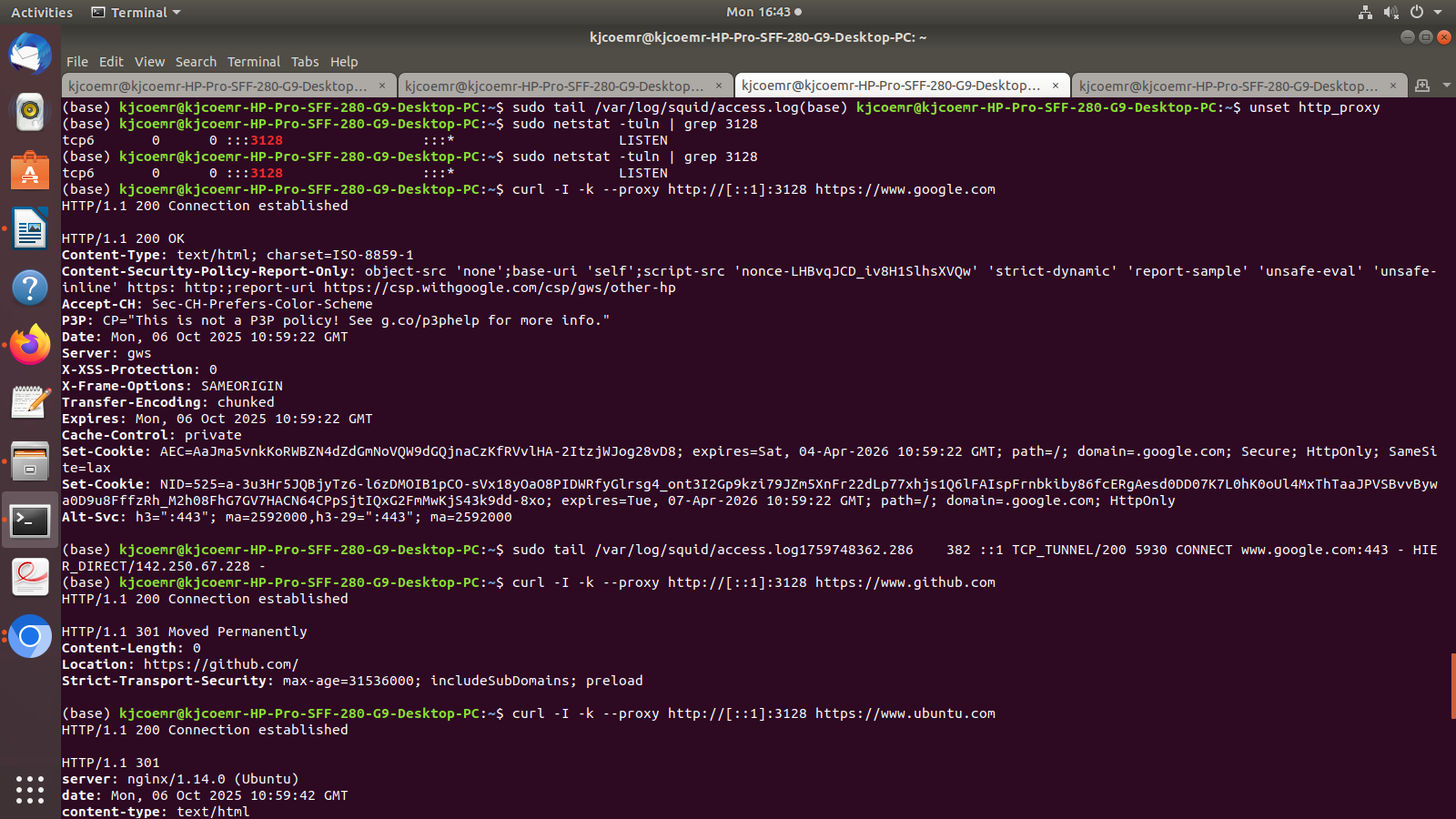
1759748379.619 63 ::1 TCP\_TUNNEL/200 3873 CONNECT www.github.com:443 - HIER\_DIRECT/20.207.73.82 -

1759748382.607 661 ::1 TCP\_TUNNEL/200 4197 CONNECT www.ubuntu.com:443 - HIER\_DIRECT/185.125.190.21 -









Python Code :

OUTPUT :

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~/Desktop/be-b-15$ nano log\_analyzer.py

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~/Desktop/be-b-15$ sudo python3 log\_analyzer.py

[sudo] password for kjcoemr:

--- Starting Analysis of /var/log/squid/access.log ---

--- Squid Log Analysis Report ---

Total Requests Logged: 3

[+] Top 5 Client IP Addresses:

- ::1: 3 requests

[+] Top 5 Accessed Websites:

- www.google.com:443: 1 requests

- www.github.com:443: 1 requests

- www.ubuntu.com:443: 1 requests

[+] Request Status Codes Summary:

- Status TCP\_TUNNEL: 3 times

--- End of Report ---

(base) kjcoemr@kjcoemr-HP-Pro-SFF-280-G9-Desktop-PC:~/Desktop/be-b-15$

