NETWORK SECURITY AND TRAFFIC ANALYSIS

Network sniffing : Network sniffing is a process that involves capturing, examining, and observing data packets as they travel through a network.

Network sniffing tools are:

1.Wireshark

2.Auvik

Wireshark: Open source software tool designed to track network packets.

* Used to analyses network packets.
* Troubleshooting problems
* Check the malicious and hacking possibilities

A screenshot of a computer

Description automatically generated

The graph beside the network represents the amount of traffic passing over them.

A screenshot of a computer

Description automatically generated

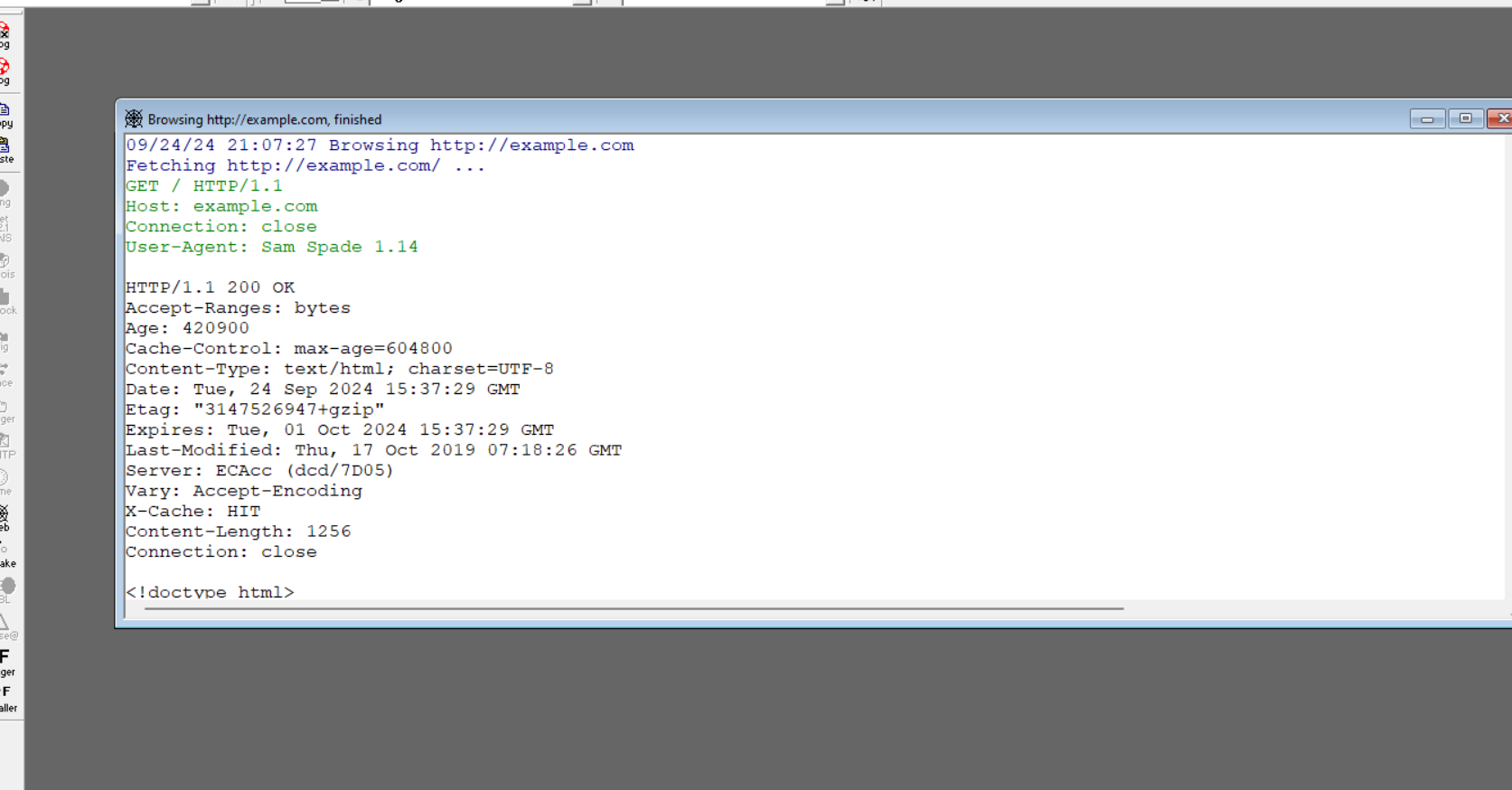
We can even the particular website address which is using by us

* Command for it is

•tcp contains "simplilearn"

* We can see like this many protocol.

SAM SPADE:



Network Sniffing: SpamSpade captures network traffic, allowing users to monitor packets and analyze data moving through the network.

Spam Detection: The tool is particularly focused on identifying spam emails and suspicious traffic patterns. It can be used to detect email-related traffic, which can help in understanding how spam is sent and received.

Protocol Analysis: SpamSpade helps in analyzing the details of specific protocols (like SMTP, POP3) involved in email communications. This is useful for identifying unwanted or harmful communications.

Security Testing: It is often used in security environments for testing how a network handles spam emails, as well as detecting potential vulnerabilities that spammers might exploit.