

WIRESHARK NETWORK ANALYSIS REPORT

Student Name: Grace Daka
Course Code: ICT414
Course Title: Information Security
Practical: Wireshark Network Analysis
Institution: Rockview University
Student number: 202201084

Introduction

This report presents a simple analysis of an HTTP request captured using Wireshark. The task involved visiting the website www.rocktv.app and capturing one HTTP GET request and its corresponding server response.

Client and Server Information

Client (Source) IP: 192.168.1.218
Server (Destination) IP: 18.171.137.67 (AWS-hosted server for rocktv.app)
Protocol Used: HTTP

HTTP Request Details

HTTP Method: GET
URL Requested: `^` (root page of www.rocktv.app)
Packet Size: 42 bytes on wire (336 bits)

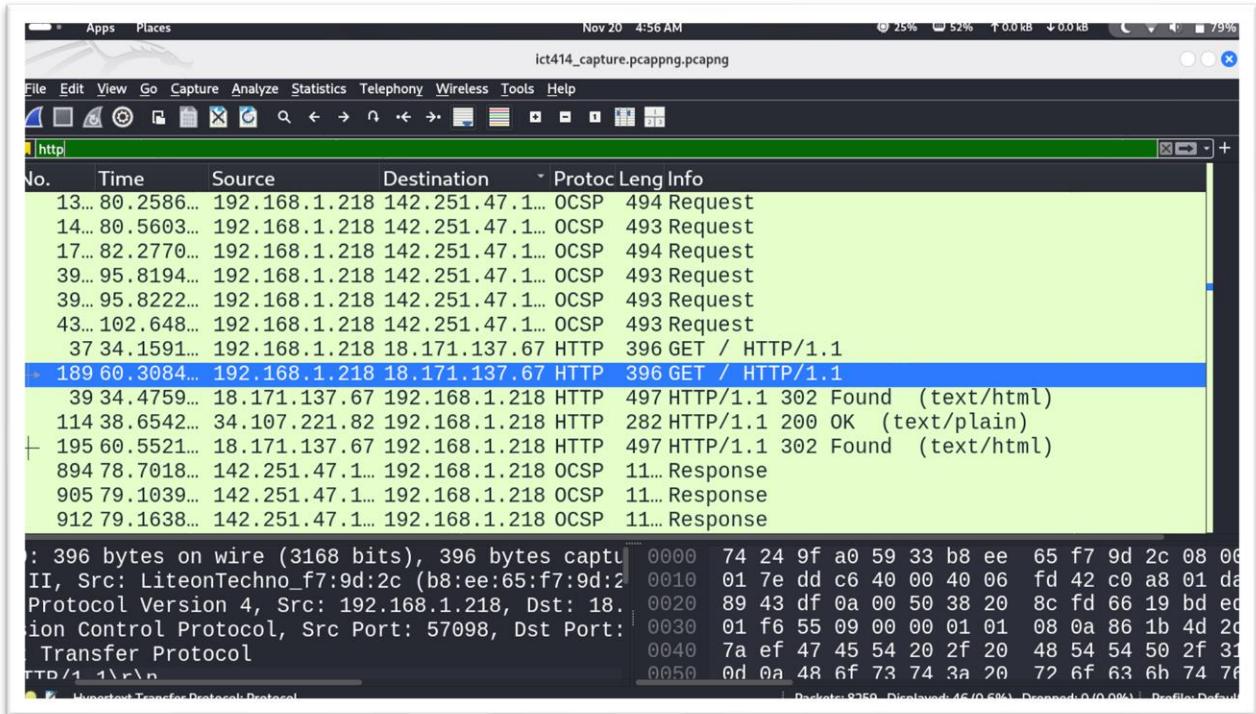
HTTP Response Details

Response Code: 302 Found
Meaning: The server redirected the request to another page (common for login or HTTPS redirection).
Follow-up Response: 200 OK (after the redirect, the page loaded successfully).

Interpretation

The communication was successful.
The server responded correctly with a redirect (302) followed by a successful 200 OK message.
The server is hosted on Amazon Web Services (18.171.137.67 IP range).
OCSP certificate validation traffic was also present (normal browser behavior).
Response packets were larger than the request, indicating more metadata being returned.

Screenshot



Files Included in Submission

ict414_capture.pcapng
report_wireshark_capure.pdf
README.md describing steps

Conclusion

This practical demonstrates basic Wireshark skills including capturing, filtering, and analyzing simple HTTP communication.