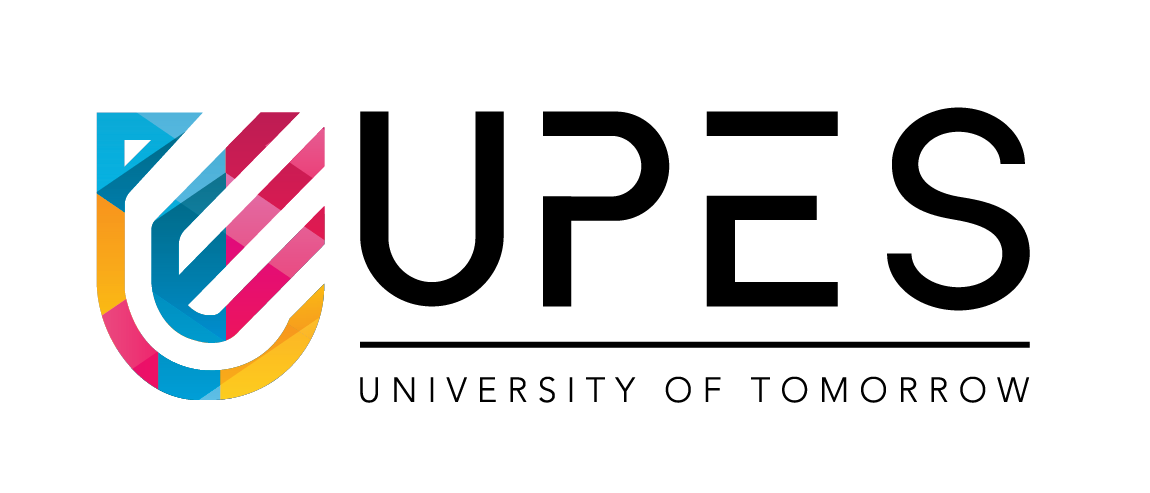
**SCHOOL OF COMPUTER SCIENCE**

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**DEHRADUN, UTTARAKHAND**



**IT DATA SECURITY LAB**

**LABORATORY FILE**

**(2024-2025)**

**For**

**Vth Semester**

**Submitted To: Submitted By:**

Dr. Narendra Kumar Dewangan Mr. Akshat Negi

Assistant Professor Cybersecurity 500106533(SAP ID)

[Vth Semester] R2142220414(Roll No.)

School of Computer Science B.Tech. CSF (Batch-1)

**LAB EXPERIMENT – 1 (a)**

**NMAP on Different Sites**

Nmap, short for "**Network Mapper**," is a powerful open-source tool used for network discovery and security auditing. It's widely used by network administrators, security professionals, and hackers alike. Nmap allows users to discover devices and services running on a network, as well as gather information about them.

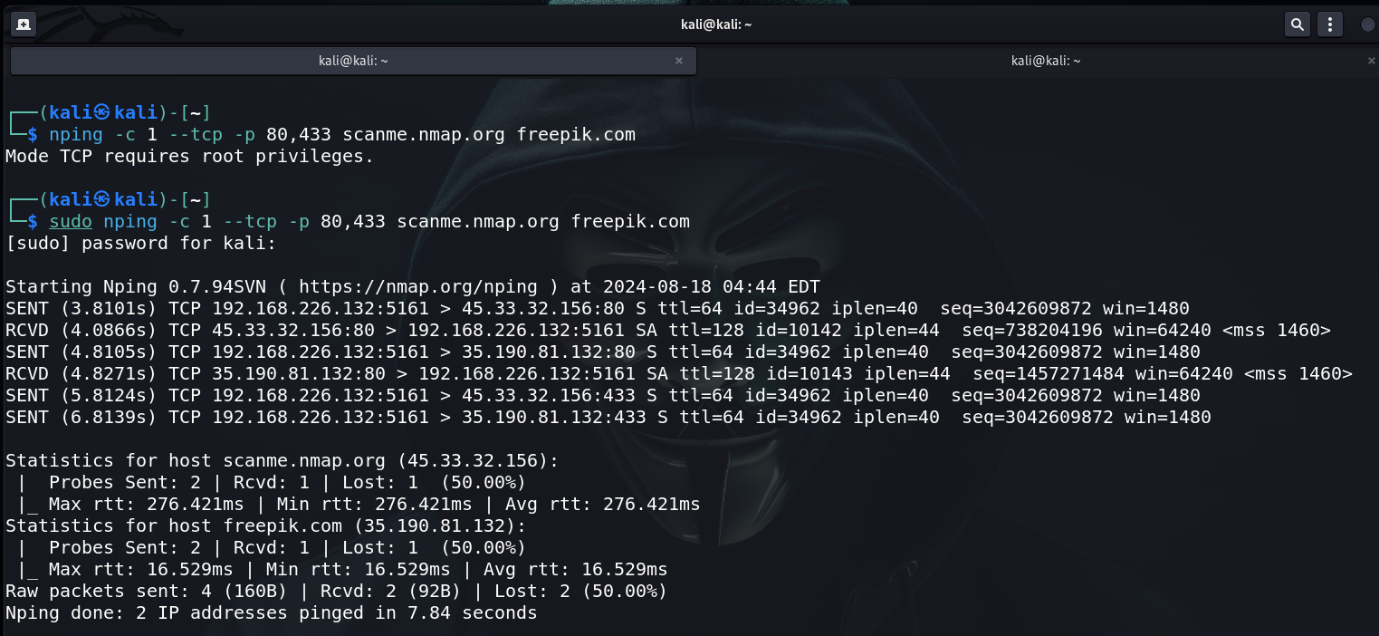
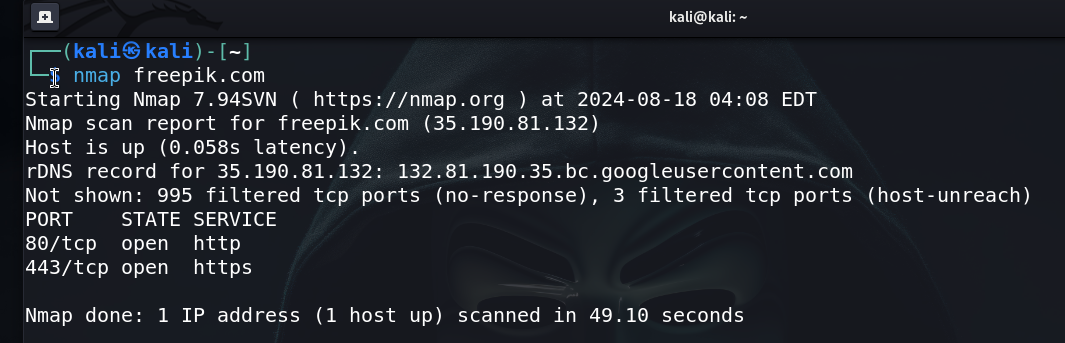
Here are some common uses of Nmap:

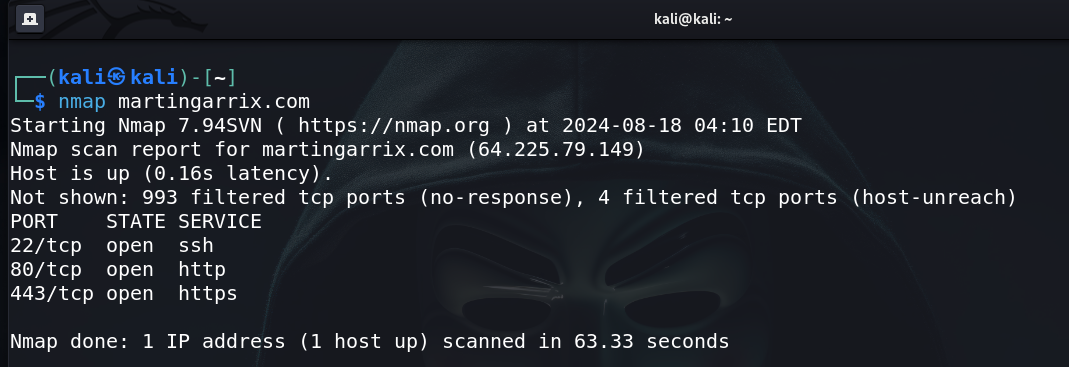
* Network Discovery: Nmap can scan networks to discover hosts, services, and open ports. This is useful for network inventory and mapping.
* Port Scanning: It can scan for open ports on a target system, helping to identify potential vulnerabilities and services running on those ports.
* Service Version Detection: Nmap can attempt to determine the version of services running on open ports, which can help in vulnerability assessment and patch management.
* OS Detection: Nmap can sometimes identify the operating system running on a target host by analyzing network responses.
* Scripting: Nmap comes with a scripting engine called Nmap Scripting Engine (NSE), which allows users to write and execute scripts to automate tasks, perform advanced network scans, and gather more information from the target systems.
* Firewall Detection: It can sometimes detect the presence of firewalls and other security devices by analyzing responses to its probes.

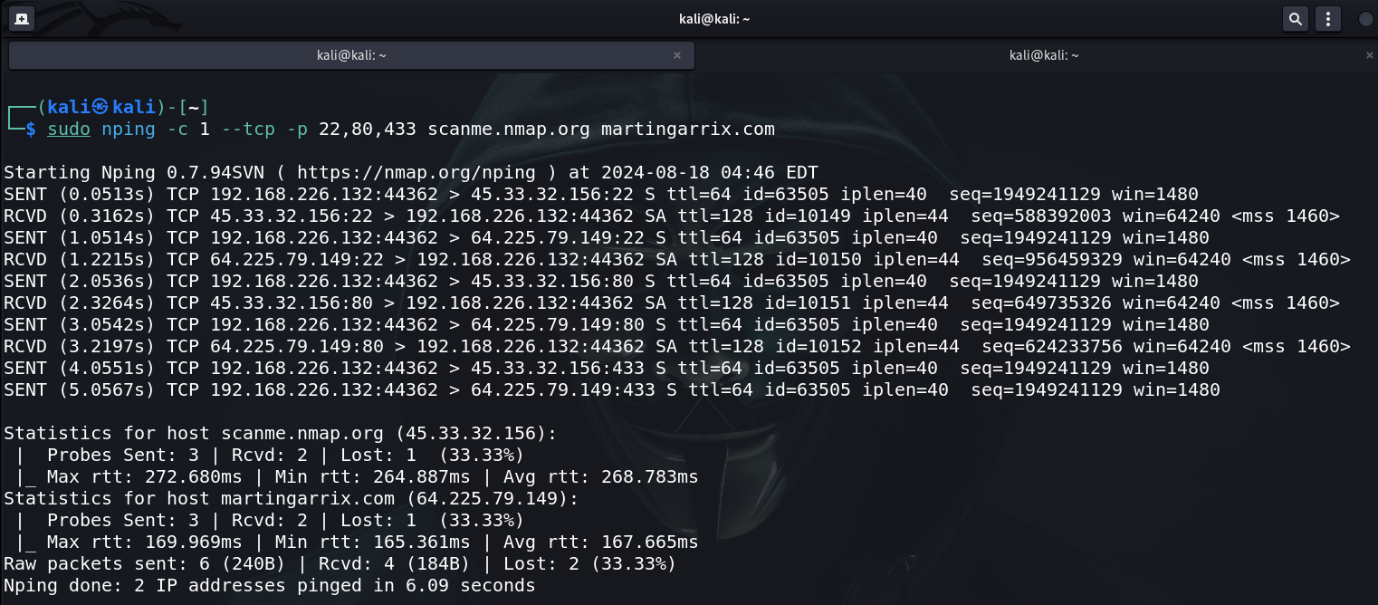
*Keep in mind that while Nmap is a valuable tool for network administrators and security professionals, its powerful capabilities can also be misused by malicious actors. Therefore, it's essential to use Nmap responsibly and ethically, respecting the laws and regulations governing network security and privacy.*

**Enhanced Scan Results:** The output of Nmap scans performed with the -sC option can include additional information gathered by the default scripts, providing users with more comprehensive scan results.

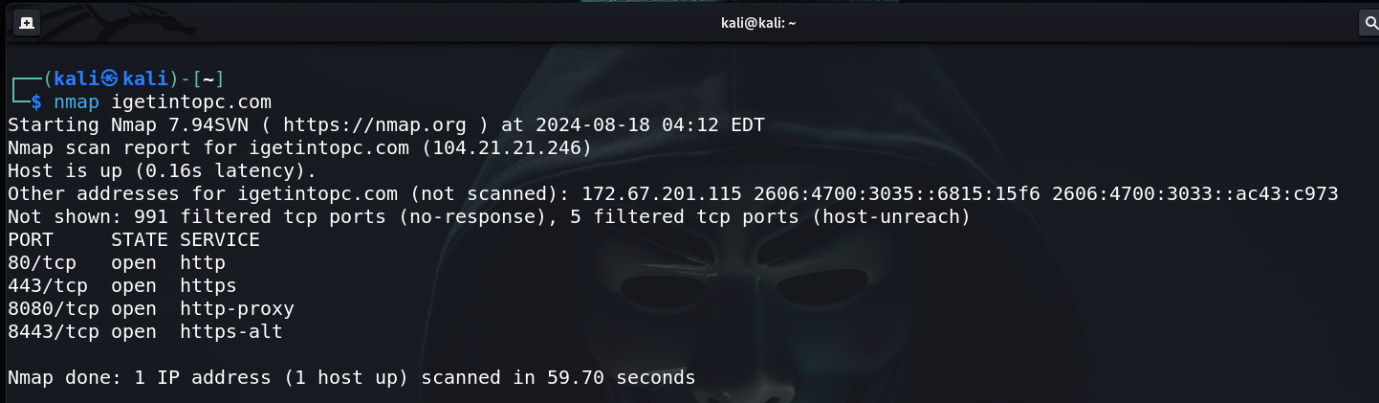
**Nmap and Nping On 4 Different Websites:**

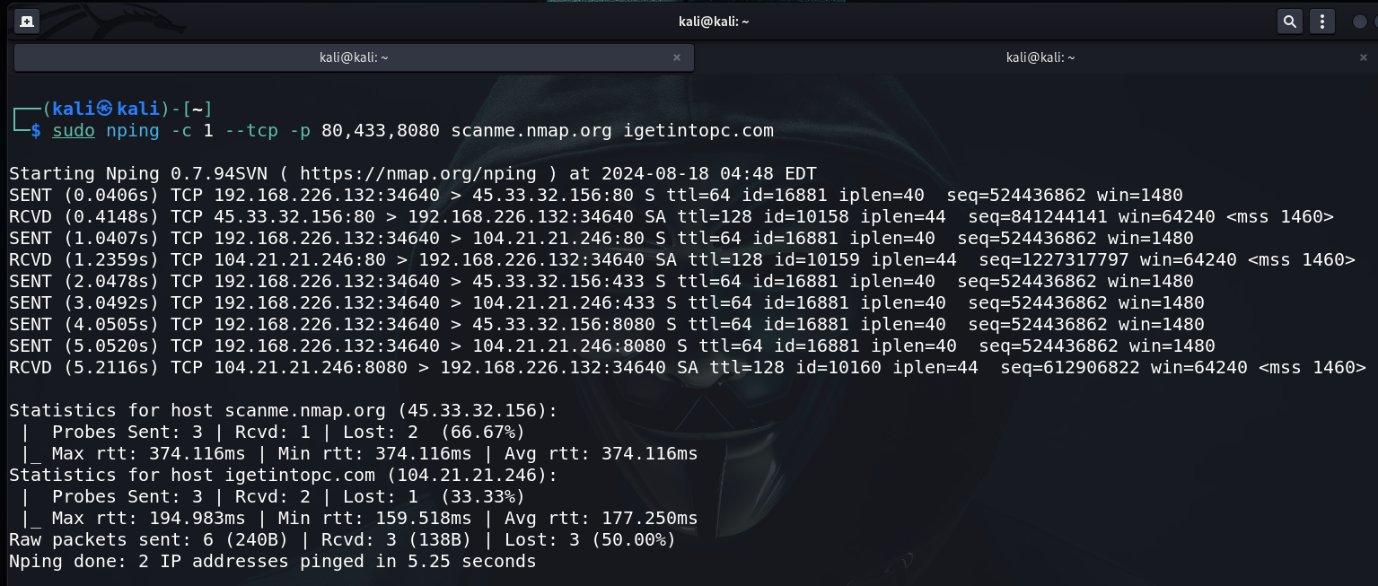
* ******freepik.com**
* **martingarrix.com**

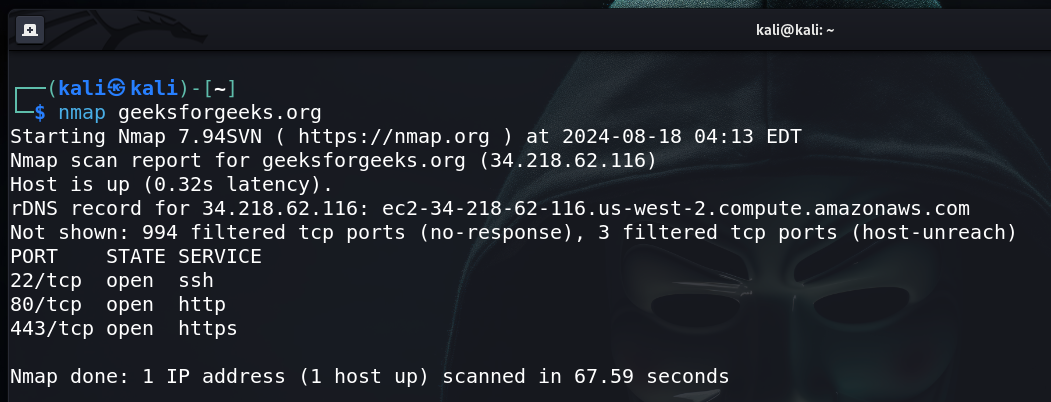


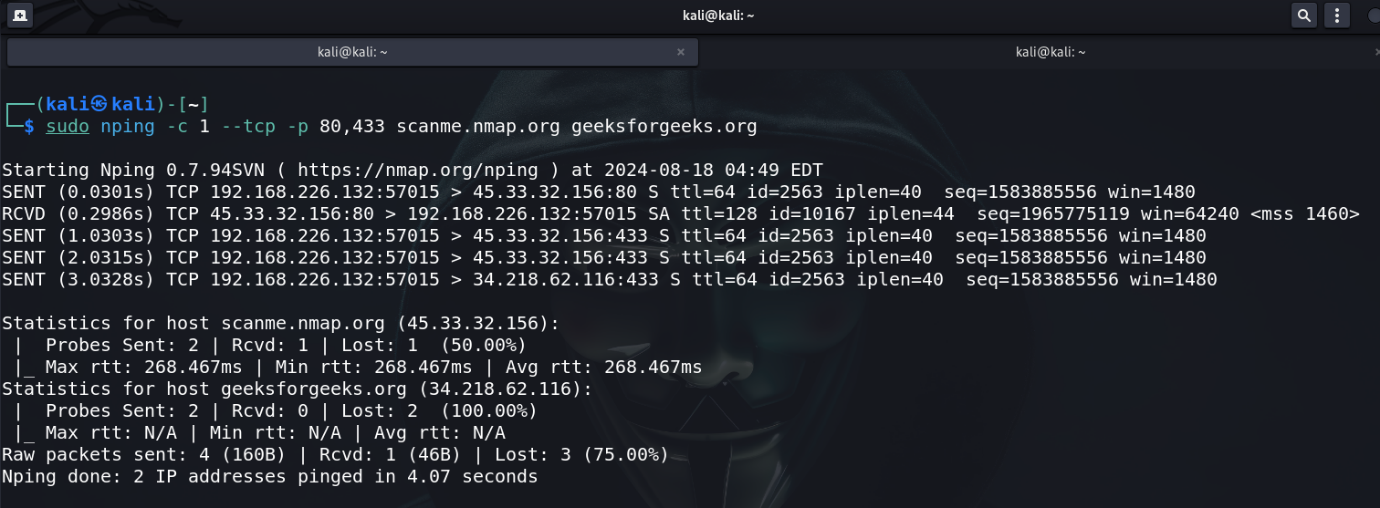


* **igetintopc.com**

****

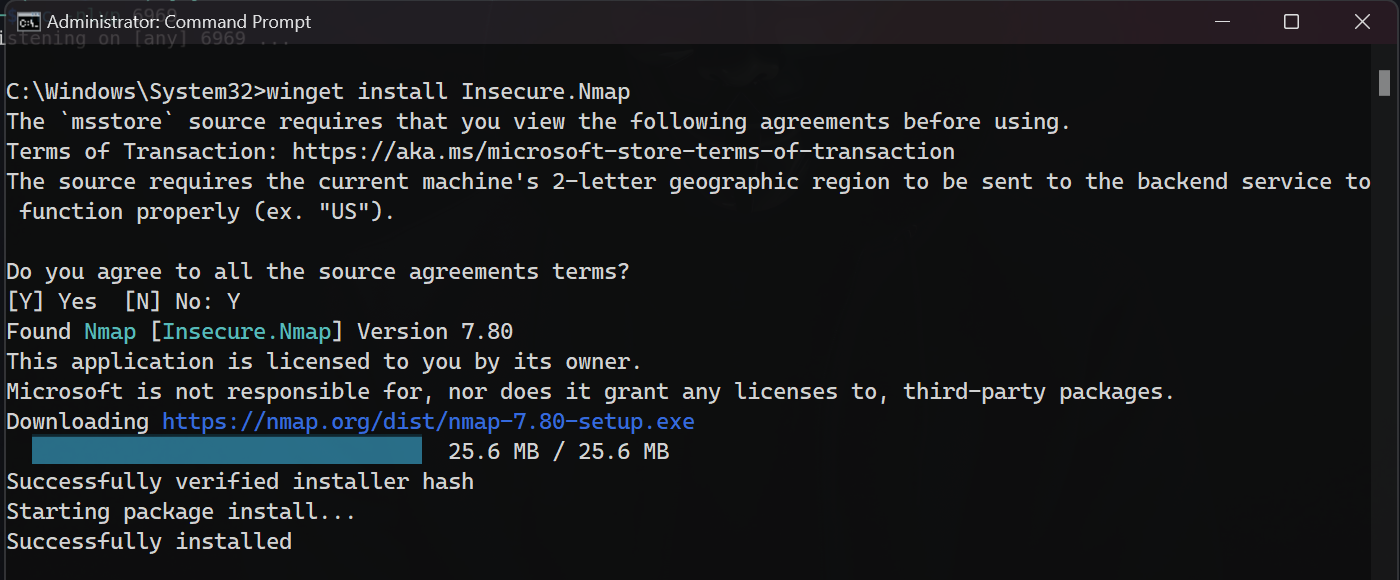
****

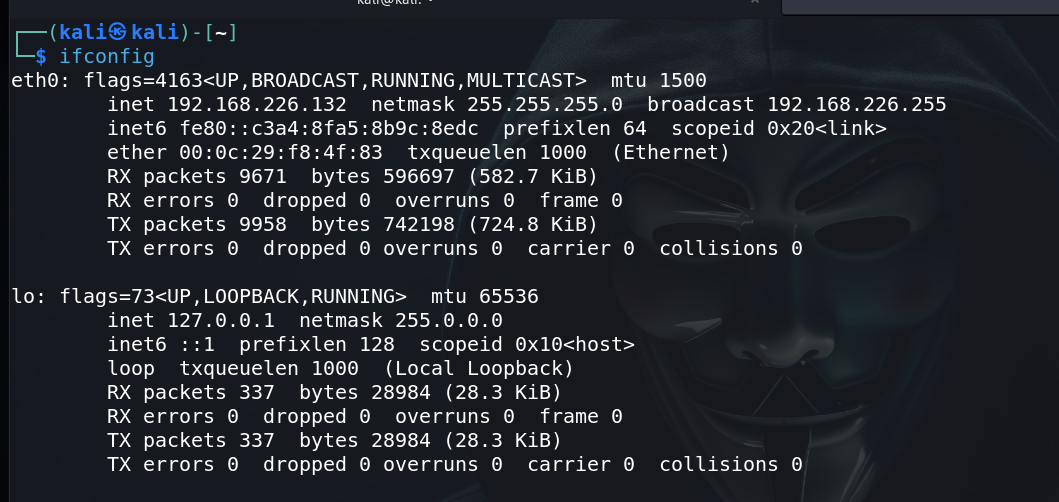
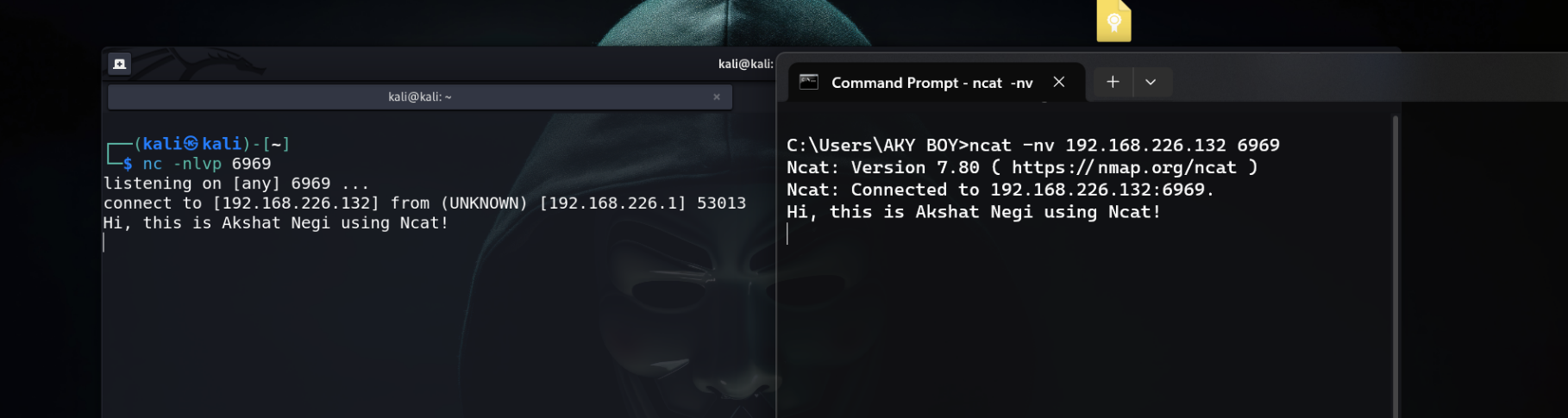
* **geeksforgeeks.org**

****

**Ncat Usage between Windows and VM Kali Linux.**

* **Installation of Ncat on Windows.**

****

* **Check the IP on Kali Linux. i.e., 192.168.226.132**
* **Connected and Interaction between two machines on a Network using Ncat.**

**LAB EXPERIMENT – 1 (b)**

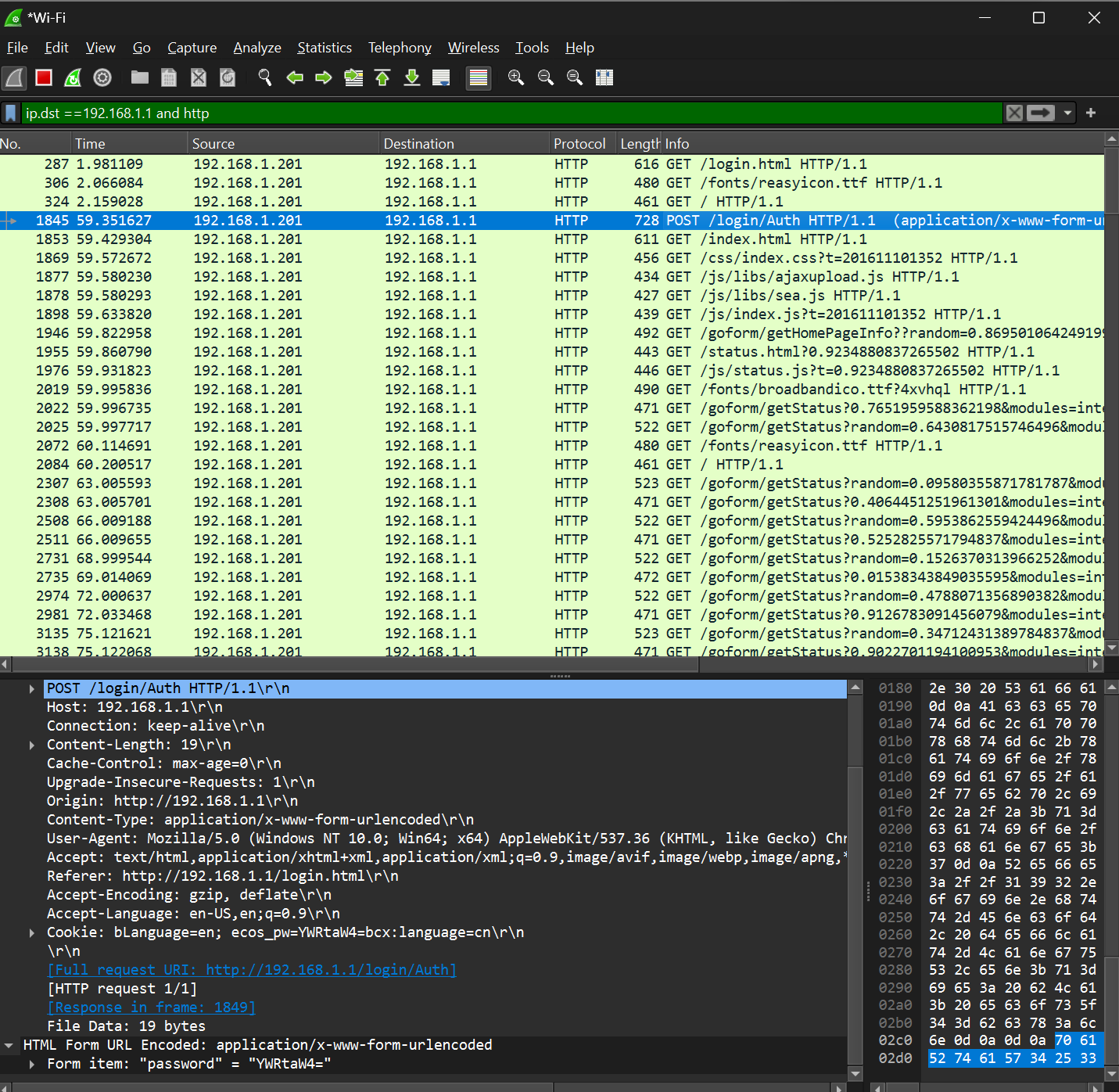
**Wireshark and**

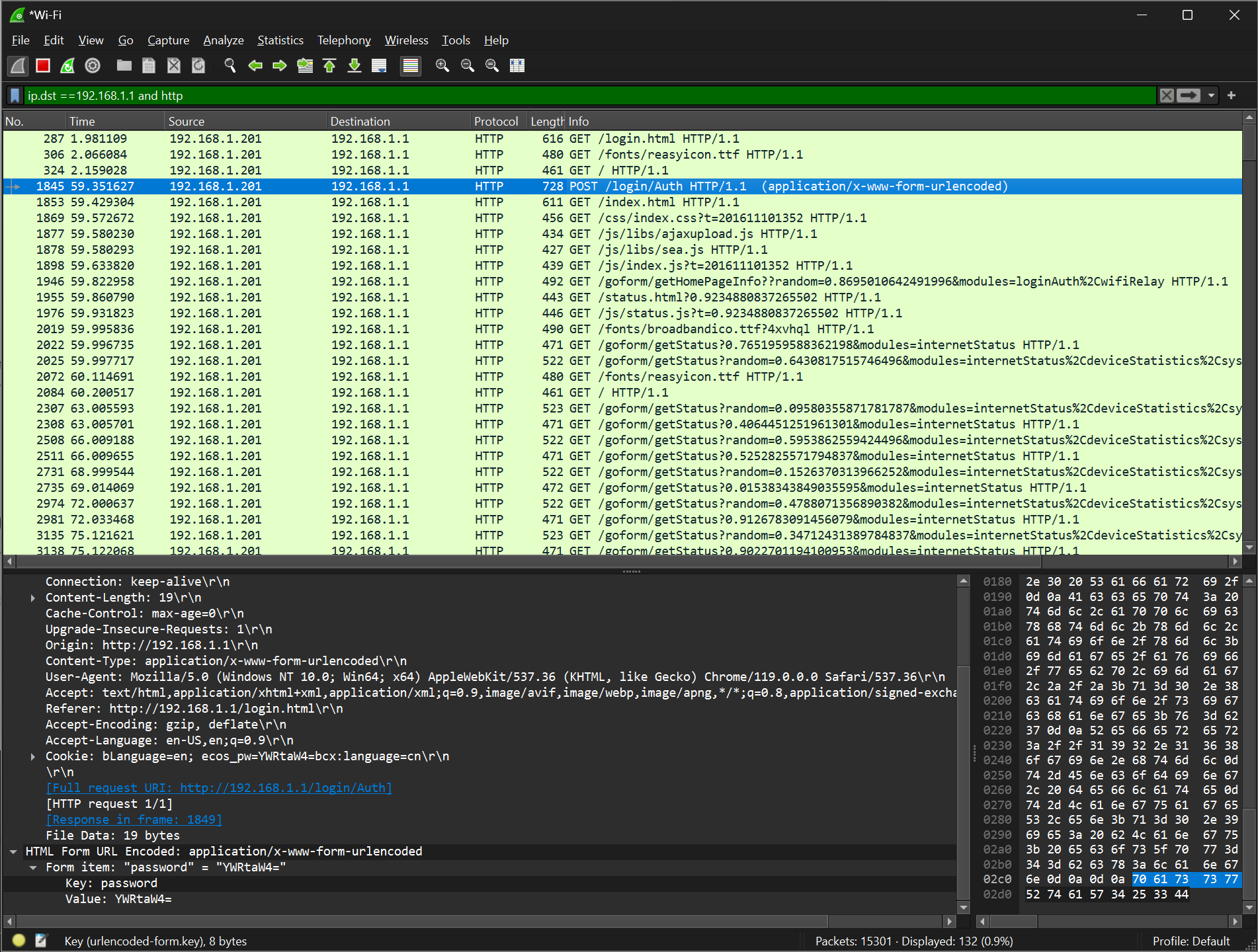
**Nagios Network Analyzer**

**Wireshark** is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

**Nagios Network Analyzer** is a cloud-based bandwidth monitoring and utilization solution that provides details on network traffic sources, potential security threats and bandwidth consumption data. It is suitable for businesses of all sizes and in various industries.

**Personal Router Traffic Analysis**

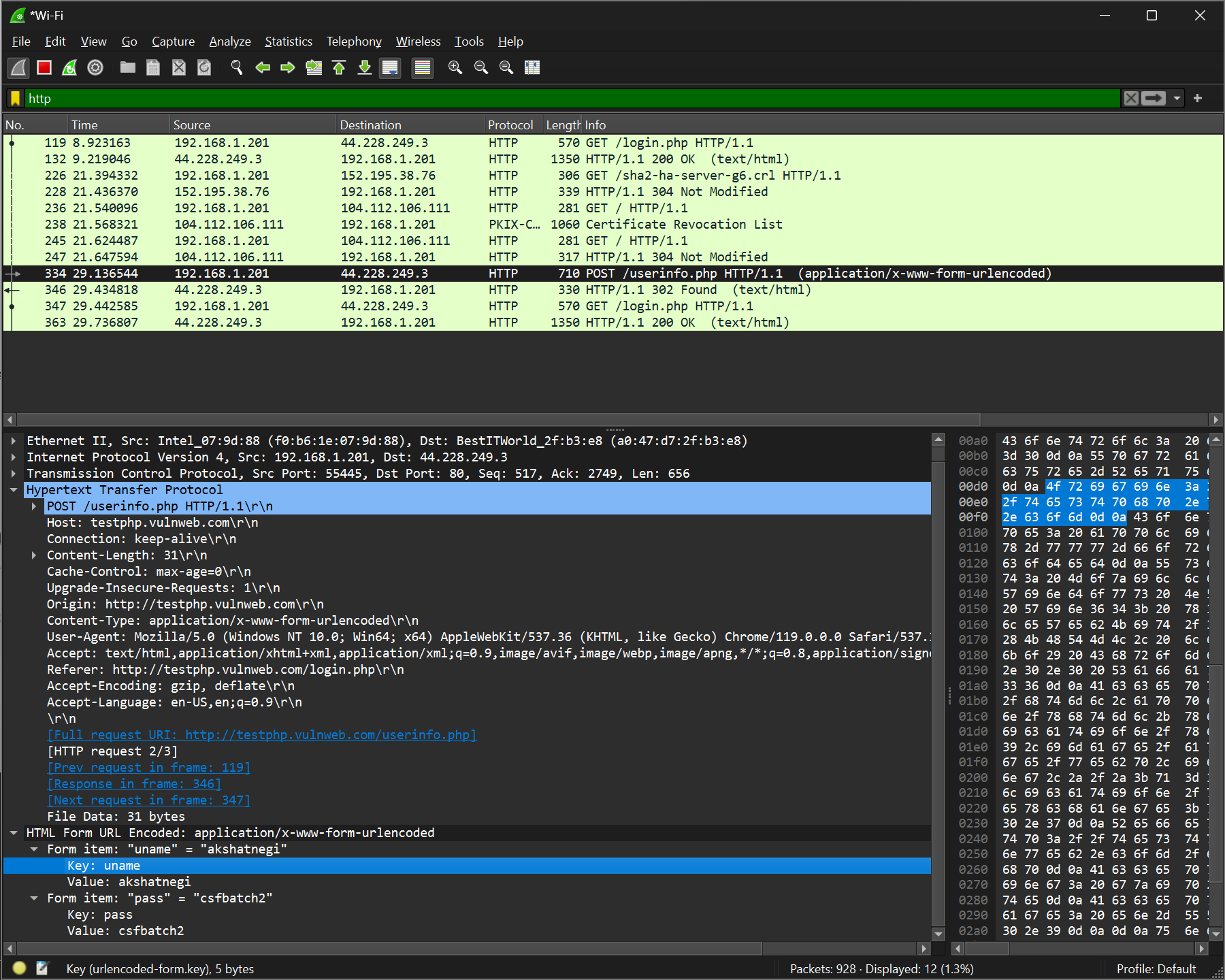




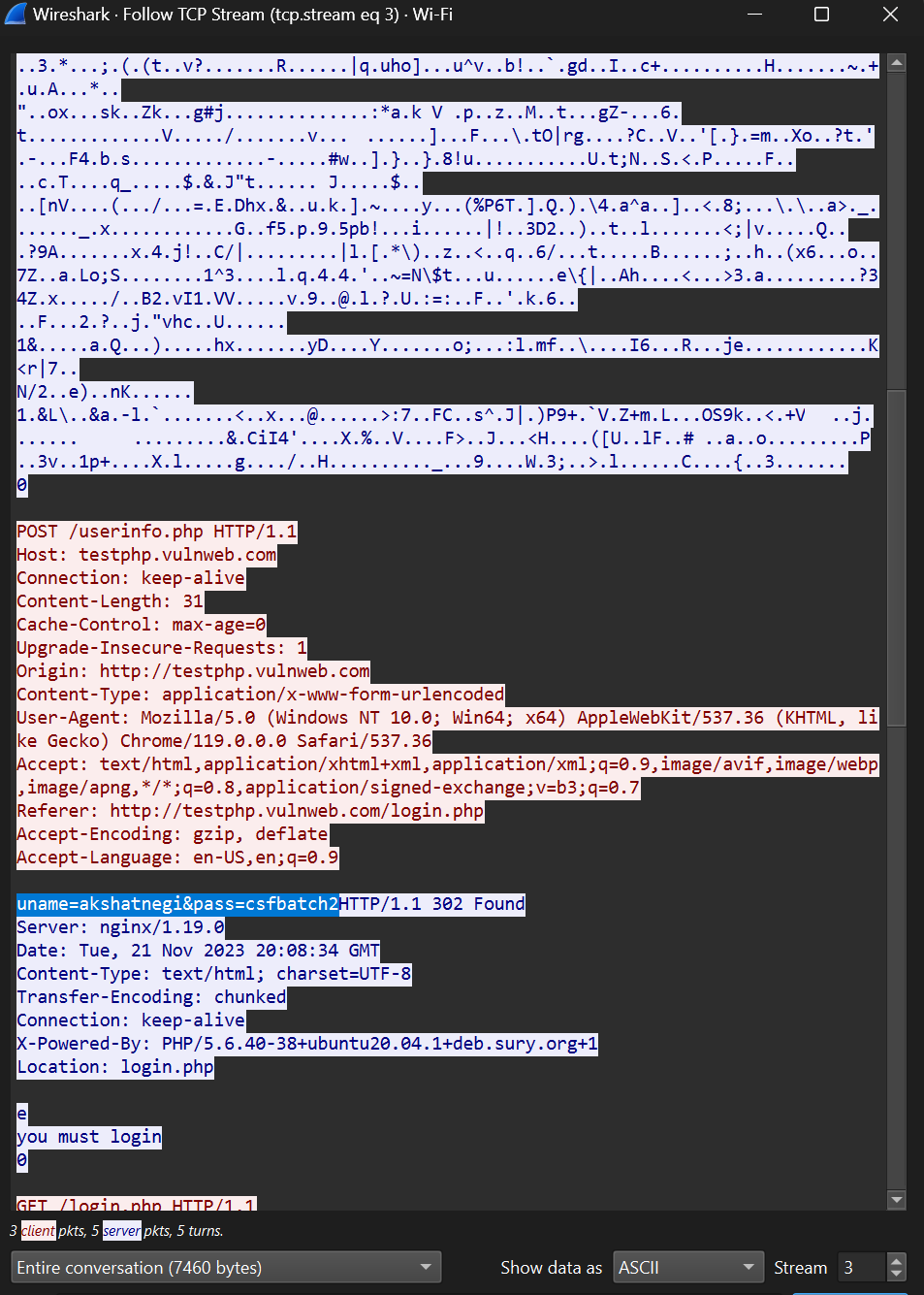
**Information Gathering from the following website:**

[**http://testphp.vulnweb.com/login.php**](http://testphp.vulnweb.com/login.php)

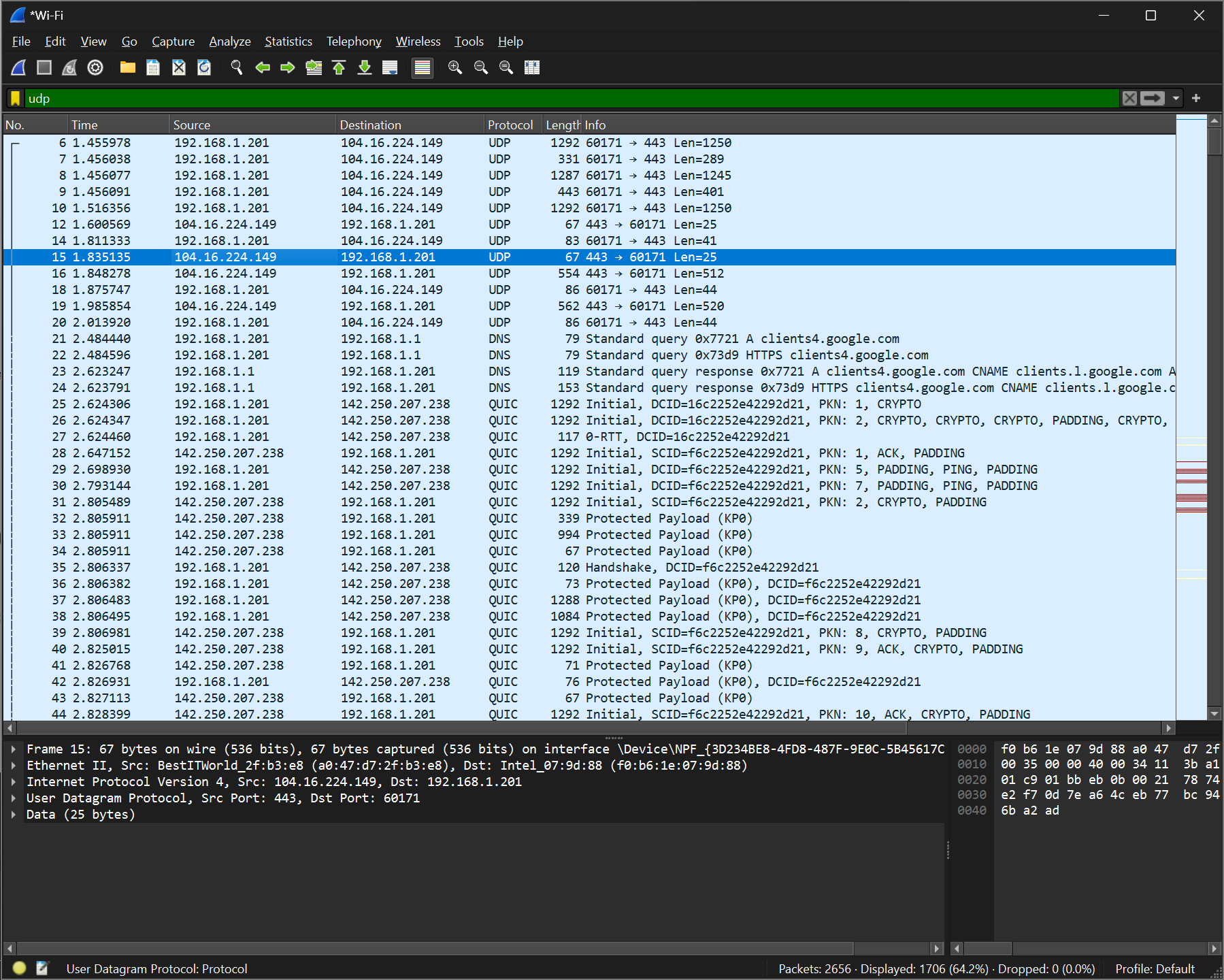
**Gathered the username and password using the Hyper-Text Transfer Protocol**



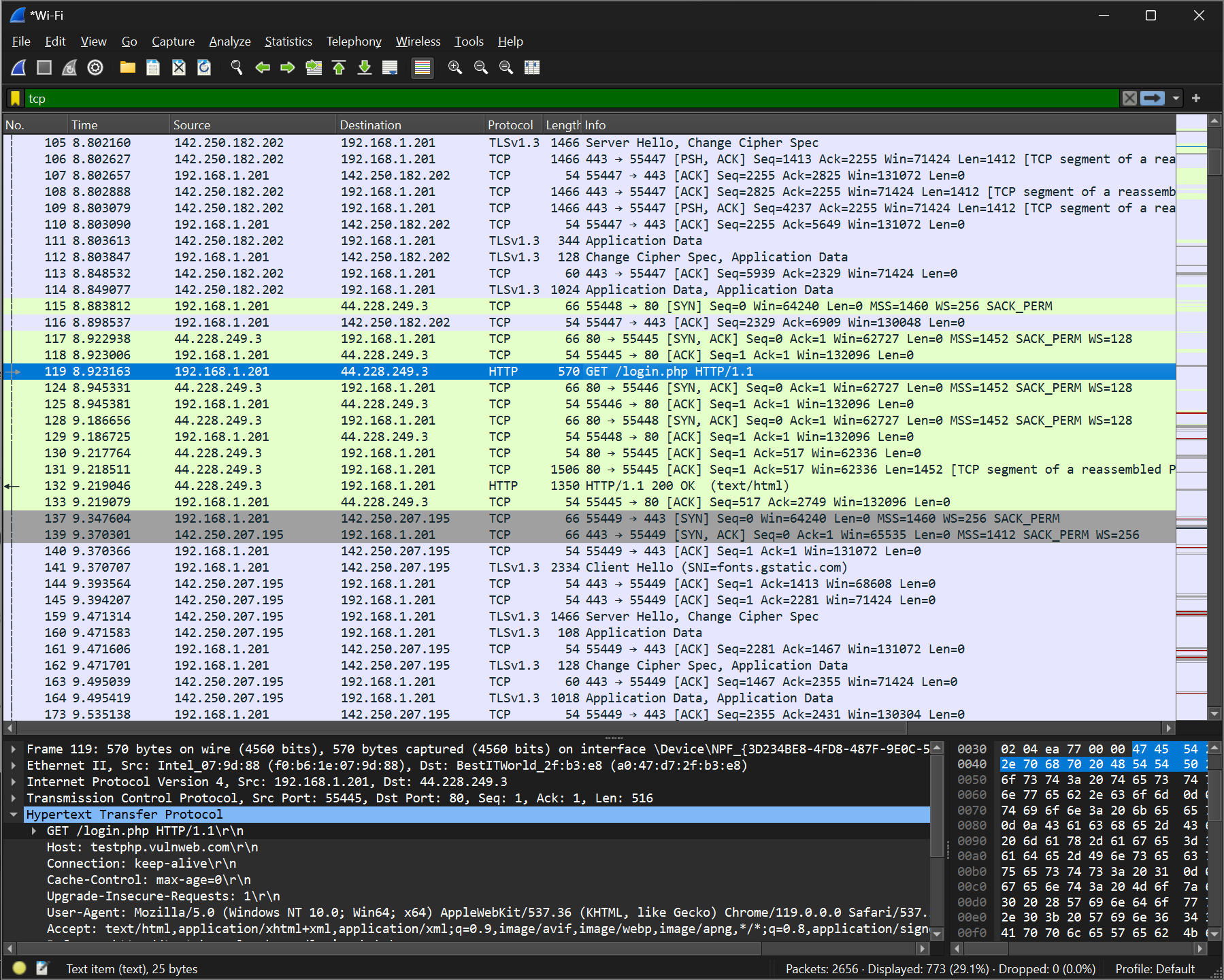




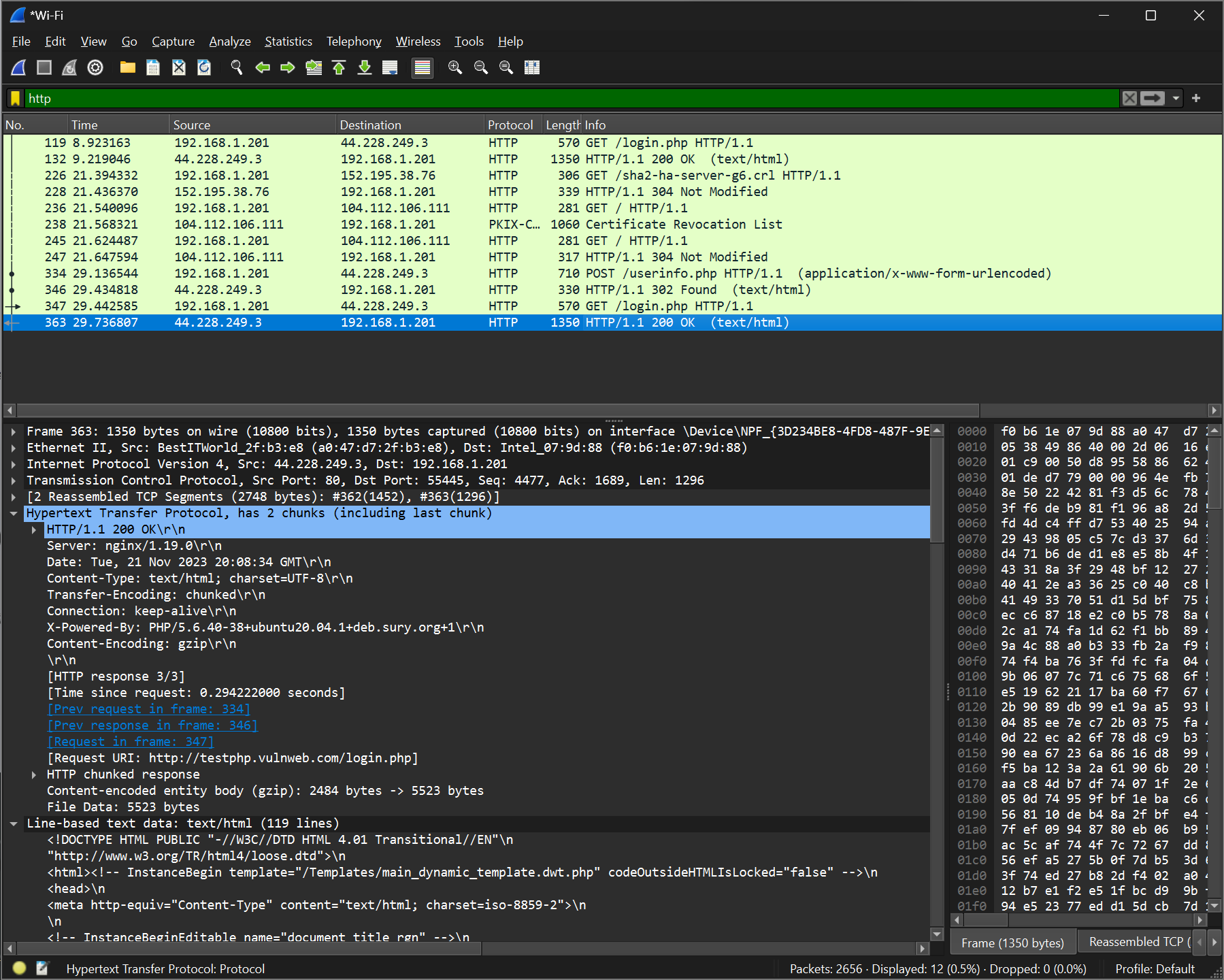
**UDP Filter**

****

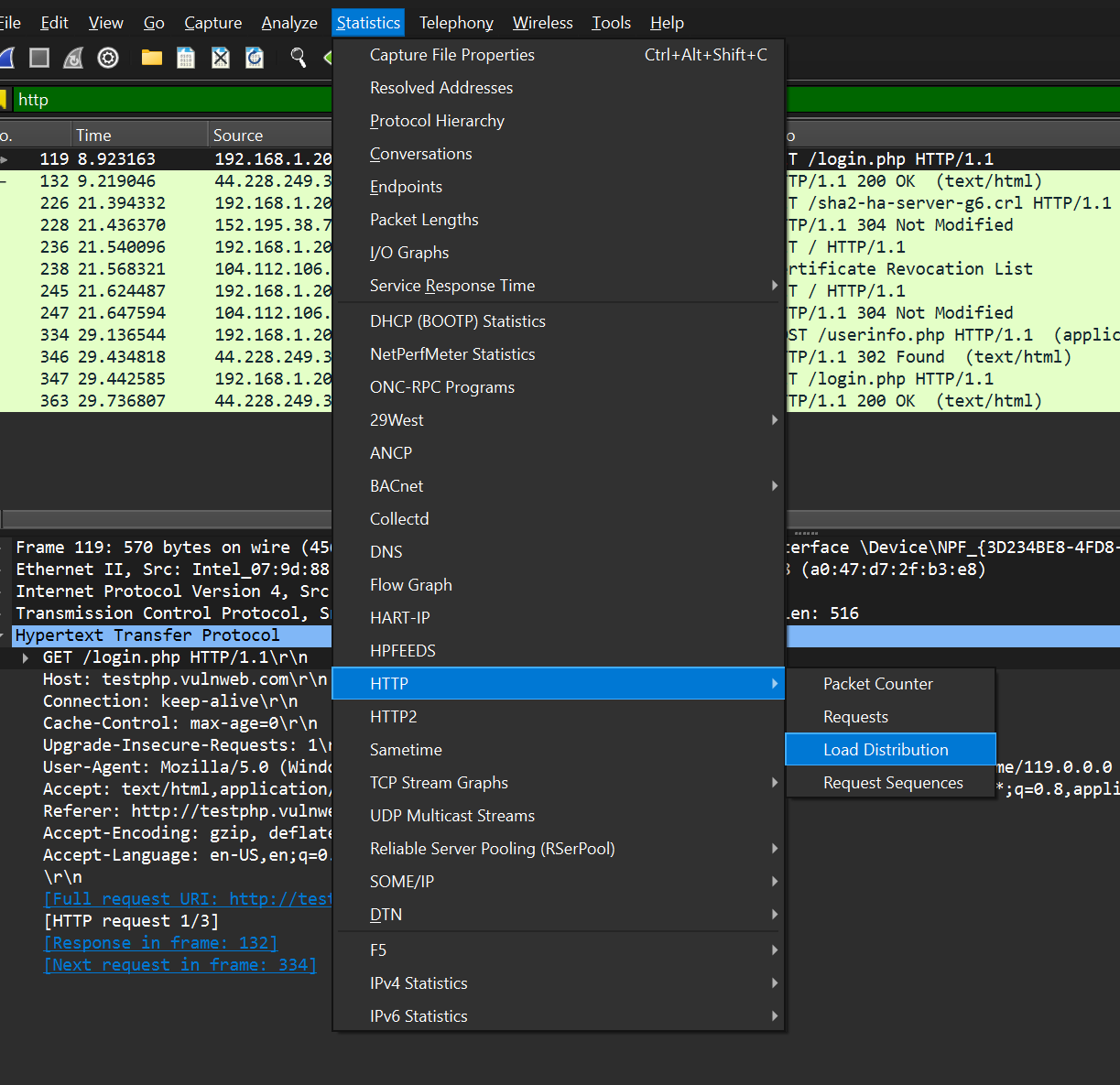
**TCP Filter**

****

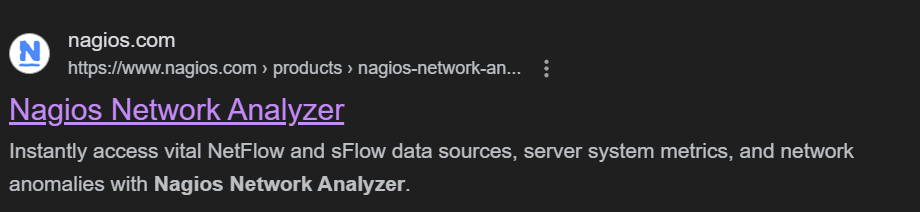
**HTTP Filtered**

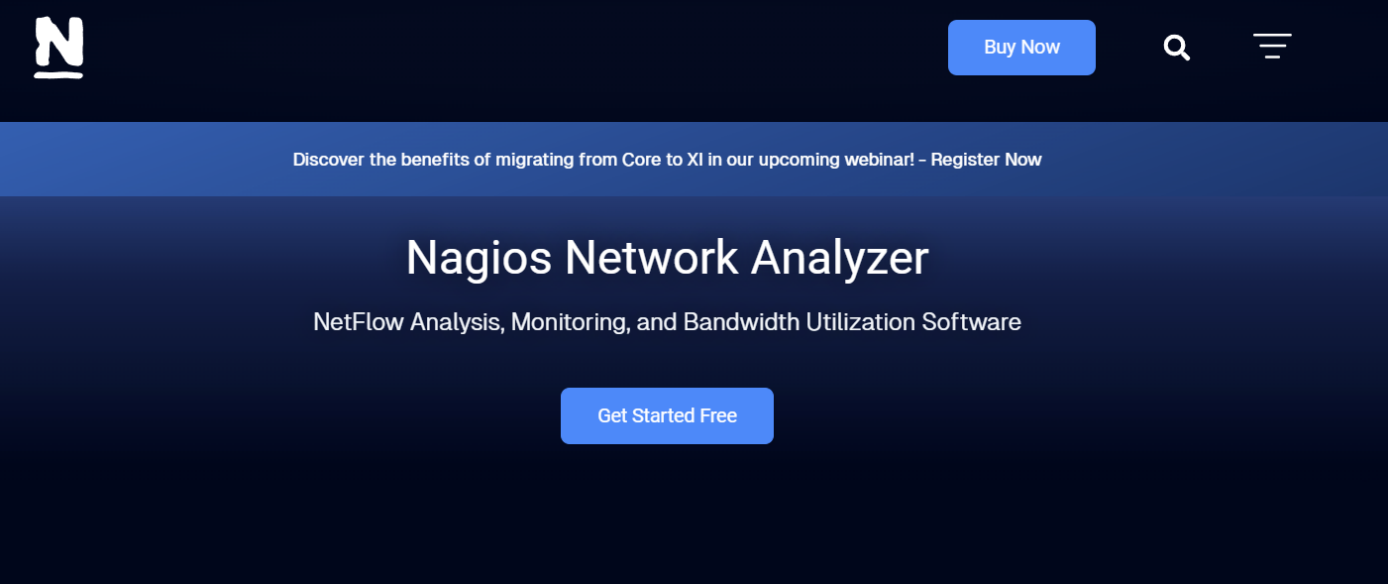
****

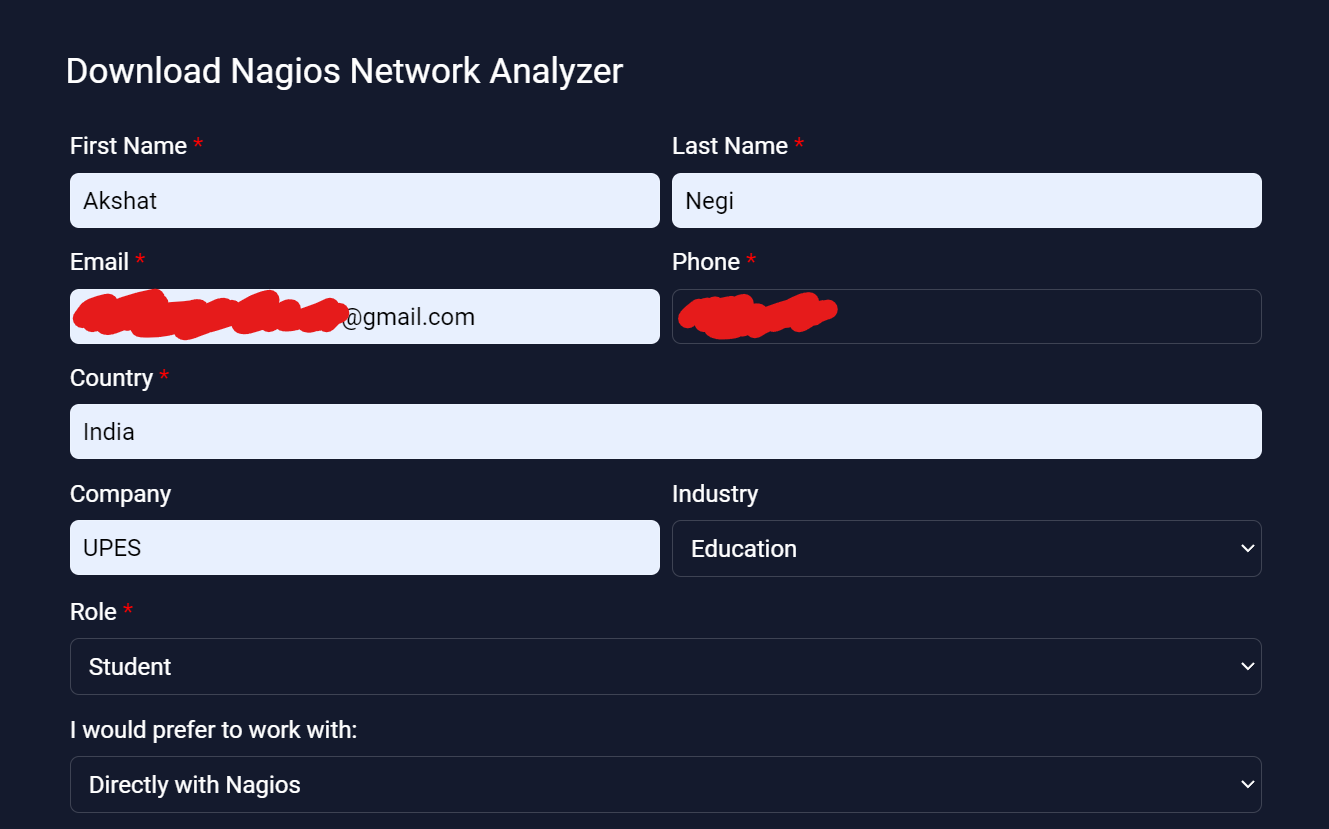
**To check which websites are surfed on a network (only http websites)**

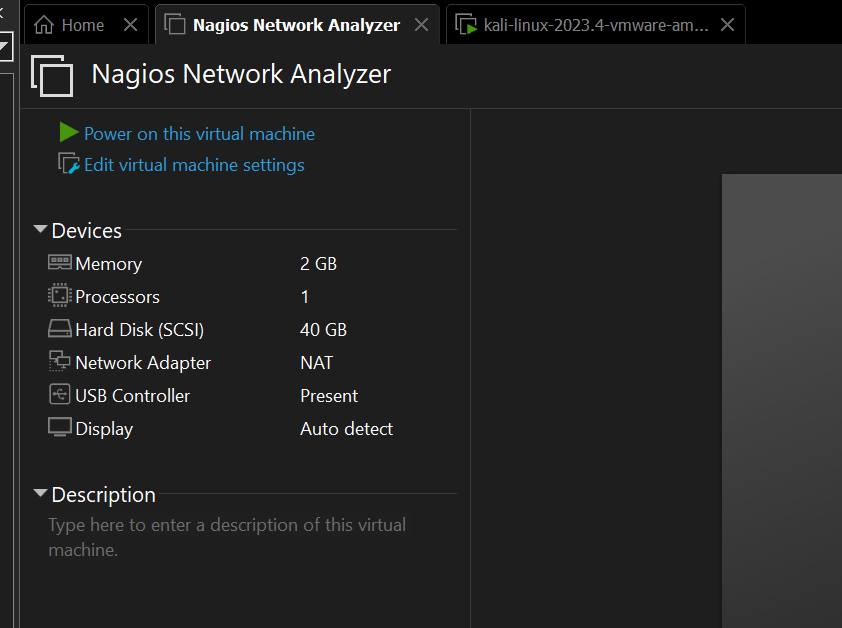
****

**Nagios Network Analyzer Installation and Analysis on VM**

****

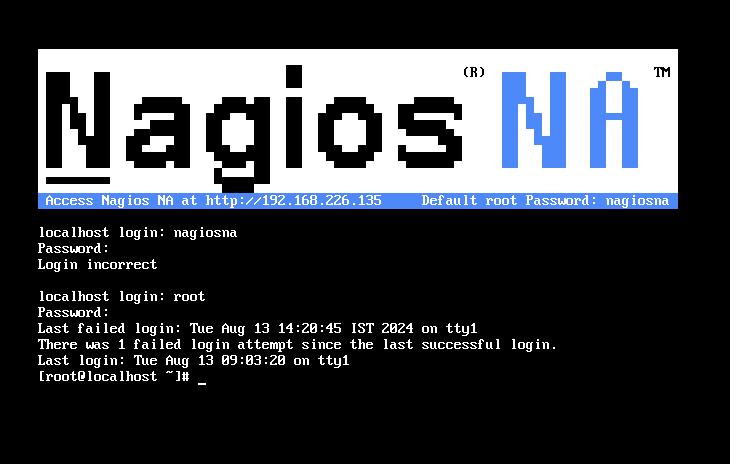
****

****

****

**Nagios Network Analyzer Interface VM**

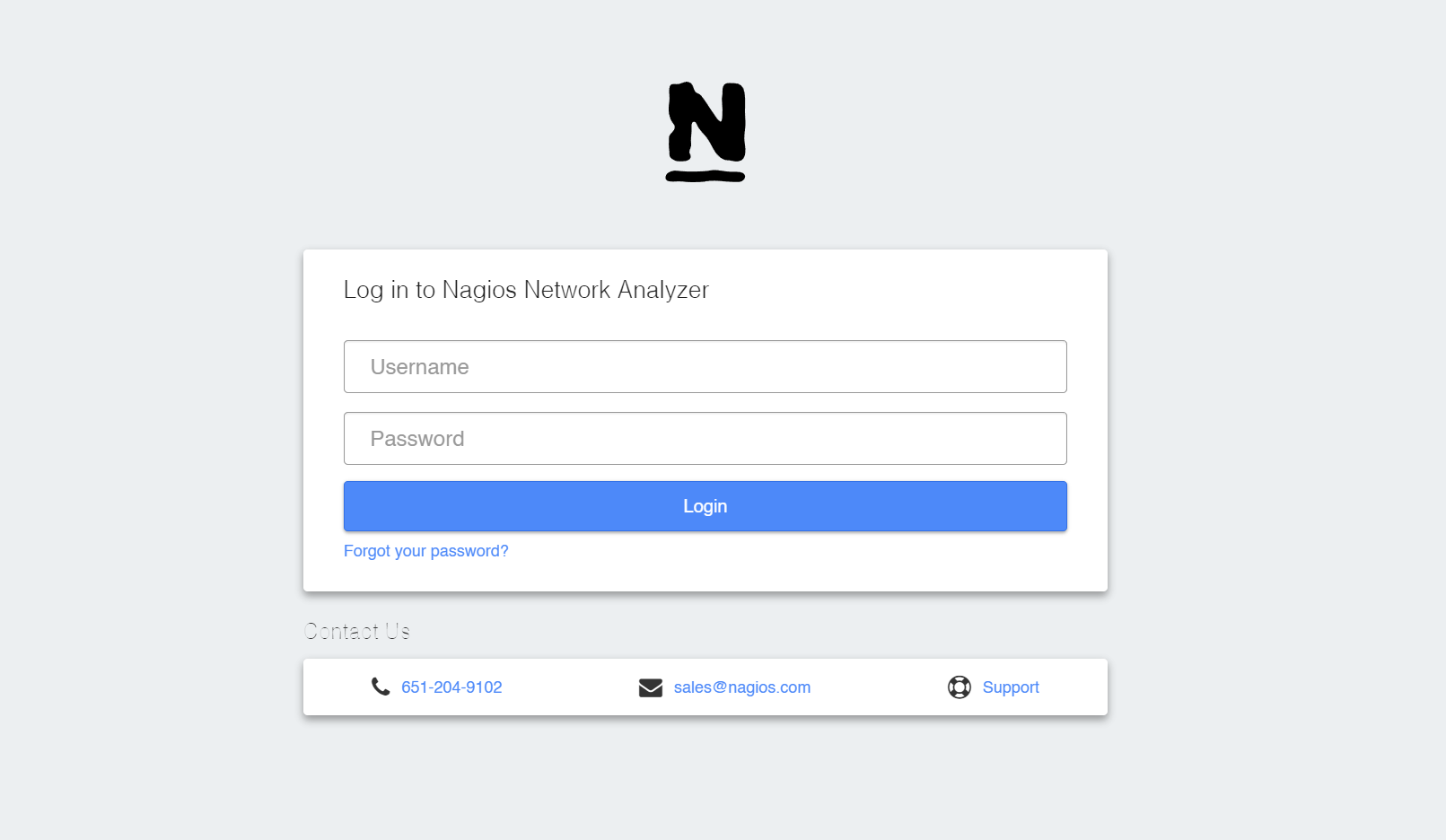
****

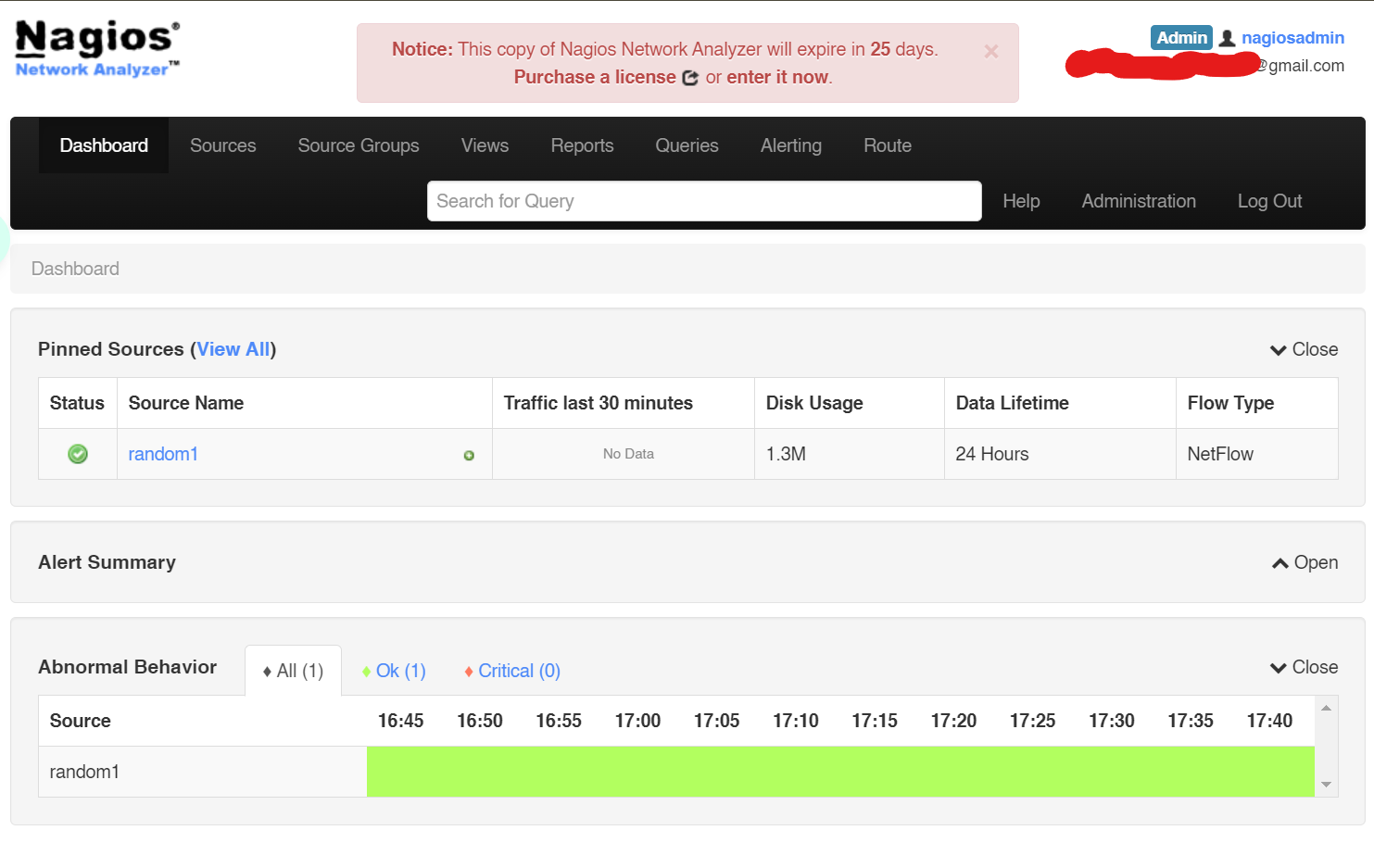
****

**LOGIN CREDENTIALS**

**ID - nagiosadmin**

**Password - kali**

****

****

