Network Traffic Analysis – Phase 2: Anomaly Detection

Phase 2 focuses on the simulation and analysis of clear-text HTTP traffic within a controlled laboratory environment. The objective of this phase is to observe and document communication patterns that, while legitimate, could appear suspicious if detected outside a lab setting.

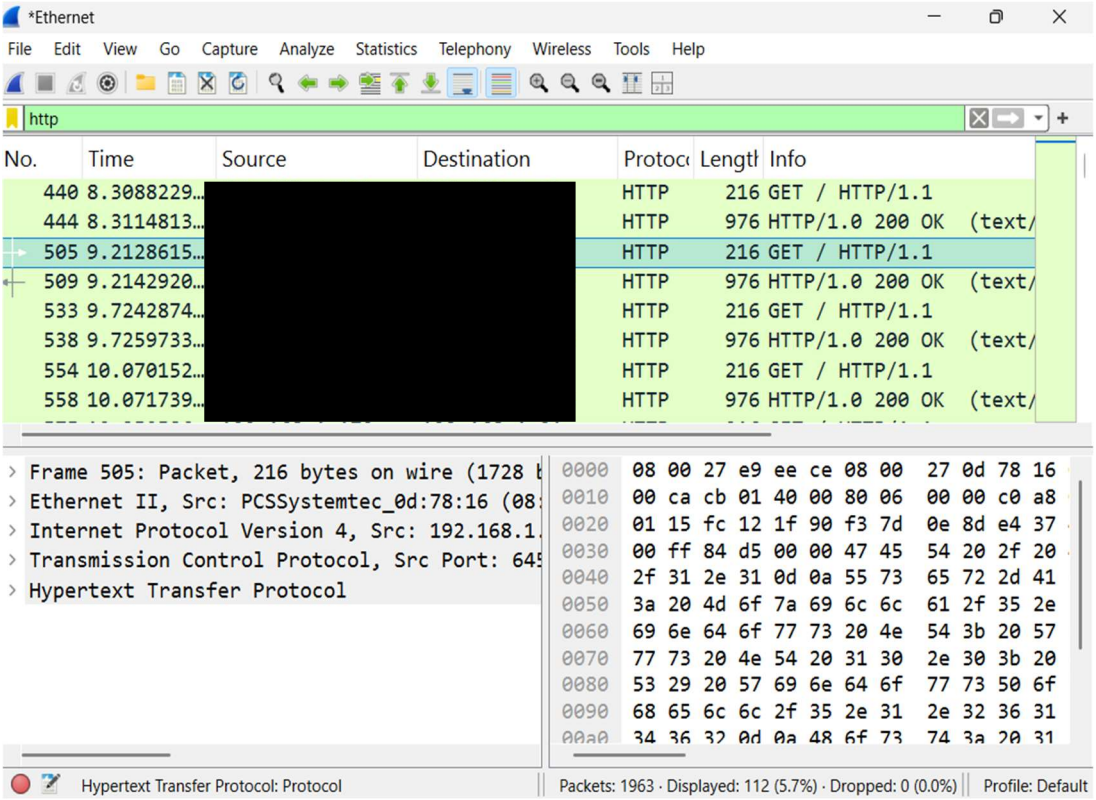
Lab Setup and Traffic Generation

The traffic was generated in an isolated lab environment composed of Windows and Linux virtual machines. The Windows host acted as the client, while the Linux host provided a simple HTTP service. Repetitive HTTP requests were generated using command-line tools and captured on the Windows host using Wireshark with protocol-based filtering applied.

Simulated HTTP Communication

The captured traffic demonstrates simulated HTTP traffic captured in a controlled lab environment using Wireshark with an HTTP display filter applied. The Windows host initiates multiple HTTP GET requests toward a Linux server, which responds consistently with HTTP 200 OK messages.

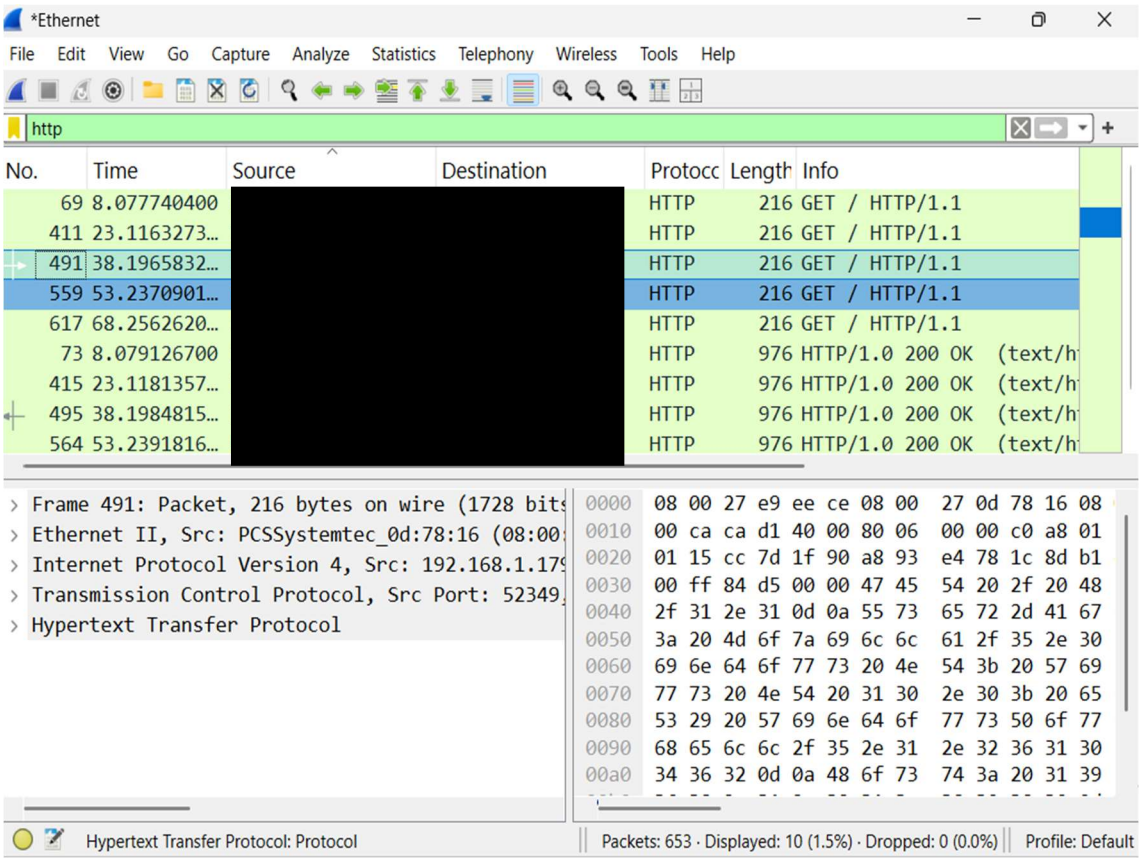
The repetitive request-and-response pattern demonstrates clear, unencrypted HTTP communication, making it suitable for observing traffic frequency, request paths, and response behavior. This type of traffic can be used as a reference when identifying anomalies such as excessive requests, unusual endpoints, or unexpected response patterns.



Repetitive HTTP Request Pattern

This screenshot shows repetitive HTTP GET requests exchanged between two hosts within a local network. The client repeatedly requests the same resource, and the server consistently responds with HTTP 200 OK messages.

This behavior represents a controlled traffic pattern commonly used to simulate beaconing-like communication patterns or automated polling. While benign in this lab scenario, similar repetitive communication patterns may warrant further investigation in real-world environments when observed at unexpected intervals or destinations



Conclusion

Phase 2 demonstrated how controlled HTTP traffic can be generated and observed within a lab environment. The captured traffic showed clear and repetitive request-and-response patterns, providing a useful example of communication behavior that may appear suspicious when compared against normal baseline traffic.

This phase highlights the importance of understanding traffic patterns before labeling activity as malicious, reinforcing a core SOC skill: distinguishing between legitimate automated behavior and potential indicators of compromise.

Skills demonstrated: Network traffic analysis, HTTP protocol analysis, Wireshark filtering, baseline comparison, SOC investigation methodology.