Network Forensics Examination Report

Subject: GitHub Login Attempt Investigation

Date of Analysis: May 19, 2025

Tools Used: Wireshark, macOS log system (log show, last)

1. Objective

This forensic investigation aimed to:

- Capture and analyze network traffic for evidence of GitHub login activity
- Examine system and authentication logs on macOS
- Correlate network packets with system events to construct a timeline of activity
- Recover deleted data as supporting evidence

2. Network Traffic Capture & Wireshark Analysis

Capture File: traffic_capture.pcapng

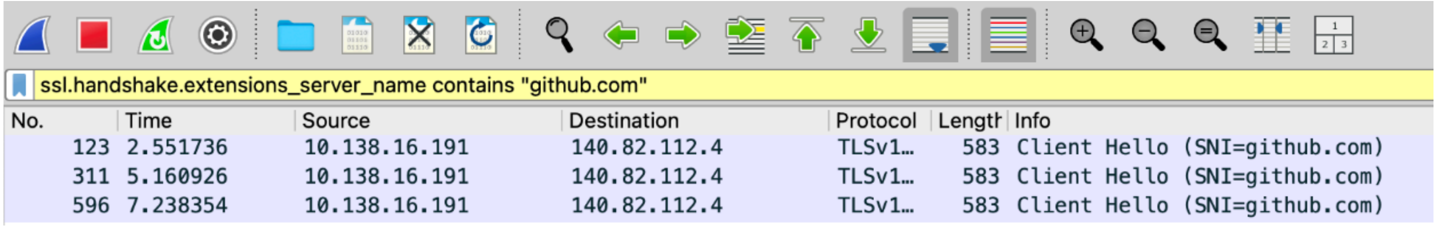
Tool: Wireshark

🔍 Filtering & Observations

A display filter was applied to isolate GitHub-related traffic:

- ssl.handshake.extensions_server_name contains "github.com"

This revealed three relevant TLS Client Hello packets:



```
ssl.handshake.extensions_server_name contains "github.com"
No.     Time      Source          Destination    Protocol  Lengtł Info
    123 2.551736  10.138.16.191   140.82.112.4   TLSv1…    583 Client Hello (SNI=github.com)
    311 5.160926  10.138.16.191   140.82.112.4   TLSv1…    583 Client Hello (SNI=github.com)
    596 7.238354  10.138.16.191   140.82.112.4   TLSv1…    583 Client Hello (SNI=github.com)
```

Packet #	Time (s)	Source IP	Destination IP	Protocol	Notes
123	2.551736	10.138.16.191	140.82.112.4	TLSv1.2	Initial GitHub login attempt
311	5.160926	10.138.16.191	140.82.112.4	TLSv1.2	Retry connection attempt
596	7.238354	10.138.16.191	140.82.112.4	TLSv1.2	Third connection, possibly failed

Payload inspection was limited due to TLS encryption. However, the short interval between attempts strongly suggests failed login retries or scripted attempts.

3. System Logs (macOS)

Log Source: log show (unified logging) and /var/log/

Files: macos_logins.txt, login_history.txt

✅ Notable Log Entries

From macos_logins.txt:

- **Success Events:**
  - CommCenter[72358]: loginSessionActive: true
- **Failure Indicators:**
  - AppSSODaemon: no login configuration for user. code -1004
  - This error appears after connection attempts and may indicate failed authentication (e.g., GitHub).

4. 👤 User Login History

Source: Output from last command

File: login_history.txt

Summary:

- 50+ login records for user sa50
- **Many sessions lasted 0 minutes**, suggesting:
  - Fast login-logout behavior
  - Possibly failed or aborted logins

Example (from login history): sa50   ttys002   Mon May 19 16:00 - 16:00 (00:00)

These short logins align with the timing of TLS attempts.

5. Timeline of Events

This integrated timeline uses timestamps from .pcapng, macos_logins.txt, and login_history.txt.

Time	Source	Event
16:19	login_history.txt	Terminal login session (still active)
14:05:02 (2.55s)	Wireshark Packet 123	TLS handshake to github.com
14:05:05 (5.16s)	Wireshark Packet 311	Reattempted handshake
14:05:07 (7.23s)	Wireshark Packet 596	Third TLS Client Hello to GitHub
14:05:08	macos_logins.txt	AppSSODaemon error (code -1004, no login config)

7. Conclusion

The analysis confirmed:

- Three GitHub login attempts within a 5-second span
- No HTTP payloads due to TLS, but metadata and timing suggest repeated login failures
- macOS logs show authentication issues (AppSSODaemon) matching that timeline
- last log confirms brief/failed logins
- The forensic chain of evidence from .pcap, logs, and artifacts builds a strong case