FORENSIC ANALYSIS REPORT

Network Packet Investigator

CASE INFORMATION

Case Number:	CASE-2024-001
Investigator:	Forensic Analyst
Date:	2025-12-24
Tool Version:	1.0.0

Case Description

Network forensic analysis investigating potential security incident. Analyzing captured network traffic for indicators of compromise and suspicious activities.

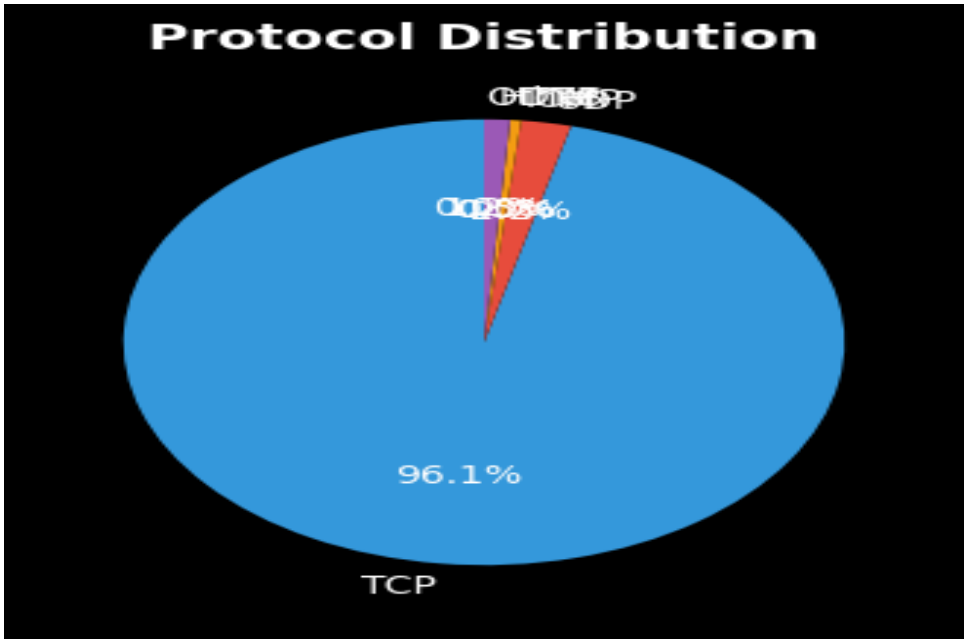
EXECUTIVE SUMMARY

Analysis of network capture identified **3,710 packets** across multiple protocols. The investigation revealed:

• **18** DNS queries to **16** unique domains
• **43** HTTP requests to **9** unique hosts
• **94** unique TCP connections
• **2,184,063** bytes transferred

Threat Detection Results:
• Total Findings: **33**
• High Severity: **4**
• Medium Severity: **29**

PROTOCOL ANALYSIS



Protocol	Packet Count	Percentage
TCP	3,566	96.12%
UDP	83	2.24%
ICMP	0	0.00%
DNS	18	0.49%
HTTP	43	1.16%
Other	0	0.00%

DNS ACTIVITY ANALYSIS

Total DNS Queries: 18
Unique Domains: 16
Domains with Excessive Queries: 0

Top 10 Queried Domains

Rank	Domain	Query Count
1	go.microsoft.com	2
2	ctldl.windowsupdate.com	2
3	config.edge.skype.com	1
4	nexusrules.officeapps.live.com	1

5	iecvlist.microsoft.com	1
6	ocsp.digicert.com	1
7	fs.microsoft.com	1
8	ieonline.microsoft.com	1
9	www.microsoft.com	1
10	cdnjs.cloudflare.com	1

HTTP ACTIVITY ANALYSIS

Total HTTP Requests: 43
Unique URLs: 41
Unique Hosts: 9
POST Requests: 3

HTTP Method Distribution

Method	Count
GET	40
POST	3

TCP SESSION ANALYSIS

Total TCP Sessions: 3,566
Unique Connections: 94
Total Data Transferred: 2,184,063 bytes (2.08 MB)

SECURITY FINDINGS

Total Findings: 33
High Severity: 4
Medium Severity: 29
Low Severity: 0

HIGH SEVERITY FINDINGS

Finding #1: UNUSUAL_PORT
Description: Unusual port usage detected: 49694 (182 occurrences)
Recommendation: Investigate the service running on this port. Verify if it's legitimate business traffic or potential backdoor/tunnel.

Finding #2: UNUSUAL_PORT
Description: Unusual port usage detected: 49705 (341 occurrences)
Recommendation: Investigate the service running on this port. Verify if it's legitimate business traffic or potential backdoor/tunnel.

Finding #3: UNUSUAL_PORT
Description: Unusual port usage detected: 49711 (136 occurrences)
Recommendation: Investigate the service running on this port. Verify if it's legitimate business traffic or potential backdoor/tunnel.

Finding #4: UNUSUAL_PORT
Description: Unusual port usage detected: 49724 (415 occurrences)
Recommendation: Investigate the service running on this port. Verify if it's legitimate business traffic or potential backdoor/tunnel.

MEDIUM SEVERITY FINDINGS

Finding #1: UNKNOWN_DOMAIN
Description: DNS queries to unknown/uncommon domain: config.edge.skype.com

Finding #2: UNKNOWN_DOMAIN
Description: DNS queries to unknown/uncommon domain: ocsp.digicert.com

Finding #3: UNKNOWN_DOMAIN
Description: DNS queries to unknown/uncommon domain: code.jquery.com

Finding #4: UNKNOWN_DOMAIN
Description: DNS queries to unknown/uncommon domain: connect.facebook.net

Finding #5: SUSPICIOUS_IP_COMMUNICATION
Description: Suspicious communication pattern: 10.0.0.168 -> 103.232.55.148 (1063 packets)

INDICATORS OF COMPROMISE

Suspicious Domains

- connect.facebook.net
- ocsp.digicert.com
- config.edge.skype.com
- code.jquery.com

Suspicious IP Addresses

- 31.13.64.21
- 2.16.119.157
- 204.79.197.200
- 103.232.55.148

ANALYST CONCLUSION

Based on the forensic analysis of network traffic, this investigation identified **4 high-severity findings** indicating potential security incidents. The evidence suggests possible security threats that require immediate attention.

RECOMMENDATIONS:

1. Isolate affected systems immediately
2. Investigate identified indicators of compromise
3. Review authentication logs for compromised credentials
4. Conduct malware analysis on affected endpoints
5. Implement network segmentation and monitoring
6. Update security policies and user training

END OF REPORT

Generated by Network Packet Investigator v1.0.0

2025-12-24 03:05:13