Network Packet Investigator

Digital Forensics Tool

Technical Report & Documentation

Students:

Kerolos Kamal Kamel 320210293

Haidy Hesham Mohamed 320210263

CNC414 - Digital Forensics Project

Table of Contents

Executive Summary

The Network Packet Investigator is a sophisticated, cross-platform digital forensics tool developed to assist security analysts and forensic investigators in analyzing network traffic captured in PCAP format. This tool addresses the critical need for accessible, efficient network forensics capabilities in modern cybersecurity operations.

Developed using Python and leveraging industry-standard libraries, the tool provides comprehensive analysis capabilities including DNS query inspection, HTTP traffic examination, TCP session analysis, and automated threat detection. The intuitive graphical user interface ensures that both novice and experienced investigators can efficiently analyze network traffic and identify potential security incidents.

This report provides complete documentation of the tool's architecture, features, capabilities, and operational procedures. It serves as both a technical reference for developers and a user guide for forensic analysts.

1. Introduction

1.1 Purpose and Scope

Network traffic analysis is fundamental to modern cybersecurity investigations. When security incidents occur, network packet captures often contain crucial evidence of attacker activities, data exfiltration attempts, and lateral movement within networks. The Network Packet Investigator was designed to streamline this analysis process by providing automated detection capabilities combined with detailed forensic reporting.

The tool specifically targets common threat scenarios including phishing attacks, data exfiltration, DNS tunneling, and suspicious network communications. By automating the identification of indicators of compromise and anomalous patterns, investigators can rapidly assess threats and take appropriate action.

1.2 Target Audience

This tool is designed for:

- Digital forensics investigators analyzing network evidence
- Security researchers studying threat patterns and attack techniques
- Educational institutions teach network security and forensics
- Penetration testers analyzing network traffic during security assessments

1.3 Document Structure

This report is organized into comprehensive sections covering tool capabilities, system architecture, operational workflows, and technical implementation details. Each section provides both high-level overviews and detailed technical specifications to serve readers with varying levels of expertise.

2. System Overview

2.1 Core Capabilities

The Network Packet Investigator provides five major areas:

2.1.1 PCAP File Analysis

- Load and parse PCAP file formats
- Support for large files with efficient memory management
- Extraction of packet metadata and payload information
- Protocol identification and classification

2.1.2 Network Traffic Analysis

- DNS query analysis with domain reputation assessment
- HTTP request inspection including methods, URLs, and headers
- TCP session tracking and data volume calculation
- Protocol distribution statistics
- IP communication pattern analysis

2.1.3 Threat Detection

The tool implements seven sophisticated threat detection algorithms:

- Unknown domain detection using whitelist comparison
- Excessive DNS query detection for DNS tunneling identification
- Large data transfer detection for exfiltration attempts
- Suspicious IP pattern recognition
- Unusual port usage identification
- HTTP POST anomaly detection
- Phishing indicator detection including suspicious TLDs

2.1.4 User Interface

- Cross-platform GUI using Tkinter
- Multi-tab interface for organized data presentation
- Interactive charts and graphs using Matplotlib
- Real-time progress indicators
- Detailed finding inspection with double-click functionality

2.1.5 Forensic Reporting

- Professional PDF reports with comprehensive analysis
- Detailed text-based reports for documentation
- CSV exports for further analysis in spreadsheet tools
- Indicators of Compromise extraction
- Chain of custody documentation support

3. Architecture and Design

3.1 Architectural Overview

The Network Packet Investigator follows a modular architecture with clear separation of concerns. The system is organized into five core modules, each responsible for a distinct aspect of functionality. This design promotes maintainability, extensibility, and testability.

3.2 Core Modules

3.2.1 PCAP Parser Module (pcap_parser.py)

Responsibility: Raw packet extraction and initial parsing

The parser module utilizes the Scapy library to load PCAP files and extract relevant packet information. It handles various packet types including DNS, HTTP, TCP, UDP, and ICMP, converting raw packet data into structured Python dictionaries for downstream processing.

Key Operations:

- Load PCAP files using Scapy's rdpcap function
- Extract packet headers and metadata
- Parse protocol-specific information (DNS queries, HTTP requests, TCP flags)
- Handle fragmented packets and reassembly when possible
- Generate structured data collections for analysis

3.2.2 Analyzer Module (analyzer.py)

Responsibility: Statistical analysis and pattern identification

The analyzer aggregates parsed packet data to identify patterns, compute statistics, and generate insights about network behavior. It processes data from the parser to create meaningful representations of traffic patterns.

Analysis Functions:

- DNS activity analysis including query frequency and domain distribution
- HTTP traffic analysis examining methods, URLs, and response codes
- TCP session tracking with connection state and data volume calculations
- Protocol distribution statistics
- IP communication pattern analysis identifying top talkers

3.2.3 Detector Module (detector.py)

Responsibility: Threat detection and anomaly identification

The detector implements seven specialized algorithms to identify potential security threats. Each algorithm examines specific aspects of network traffic and generates findings with severity classifications.

Detection Algorithms:

- Unknown Domain Detection: Identifies domains not in the safe domains whitelist
- Excessive DNS Queries: Detects potential DNS tunneling through query volume analysis
- Large Data Transfers: Identifies potential data exfiltration through volume thresholds
- Suspicious IP Patterns: Analyzes communication between private and public IPs
- Unusual Port Detection: Flags non-standard port usage
- HTTP POST Anomalies: Detects suspicious POST requests to unknown hosts
- Phishing Indicators: Identifies suspicious TLDs and domain patterns

3.2.4 Reporter Module (reporter.py)

Responsibility: Forensic report generation and data export

The reporter creates professional forensic documentation in multiple formats. Reports follow industry standards and include all necessary information for incident response and legal proceedings.

Report Formats:

- PDF Reports: Professional reports with charts, case information, and detailed analysis
- TXT Reports: Comprehensive text-based documentation
- CSV Exports: Data exports for further analysis in spreadsheet tools

3.2.5 GUI Module (gui.py)

Responsibility: User interface and interaction management

The GUI provides an intuitive interface built with Tkinter. It organizes analysis results across multiple tabs and uses threading to prevent UI freezing during intensive analysis operations.

Interface Components:

- File selection controls with browse functionality
- Progress indicators showing analysis status
- Six analysis tabs: Overview, DNS, HTTP, TCP, Security Findings, and Charts
- Interactive visualizations using Matplotlib
- Menu system for export reports and help documentation

4. Operational Workflow

4.1 Standard Investigation Process

The tool follows a structured forensic investigation workflow:

Phase 1: Evidence Collection

Obtain PCAP files from network taps, IDS systems, firewalls, or endpoints. Document chain of custody includes file hash, timestamp, and source. Verify file integrity before analysis.

Phase 2: Initial Analysis

Launch the application and load the PCAP file. Monitor the progress bar as the tool processes packets through five stages: loading, extraction, analysis, threat detection, and display update.

Phase 3: Overview Review

Examine the Overview tab for executive summary including total packets, DNS queries, HTTP requests, TCP sessions, and high-level findings. This provides context for deeper investigation.

Phase 4: Deep Dive Investigation

Navigate through specialized tabs examining DNS queries for unknown domains, HTTP traffic for suspicious URLs, and TCP sessions for large transfers. Review the Security Findings tab for detailed threat information with severity classifications.

Phase 5: Threat Correlation

Cross-reference detected indicators of compromise with threat intelligence. Identify patterns matching known attack techniques. Document findings according to frameworks like MITRE ATT&CK where applicable.

Phase 6: Report Generation

Export comprehensive reports in PDF, TXT, or CSV format. Reports include case information, detailed analysis results, security findings, and actionable recommendations.

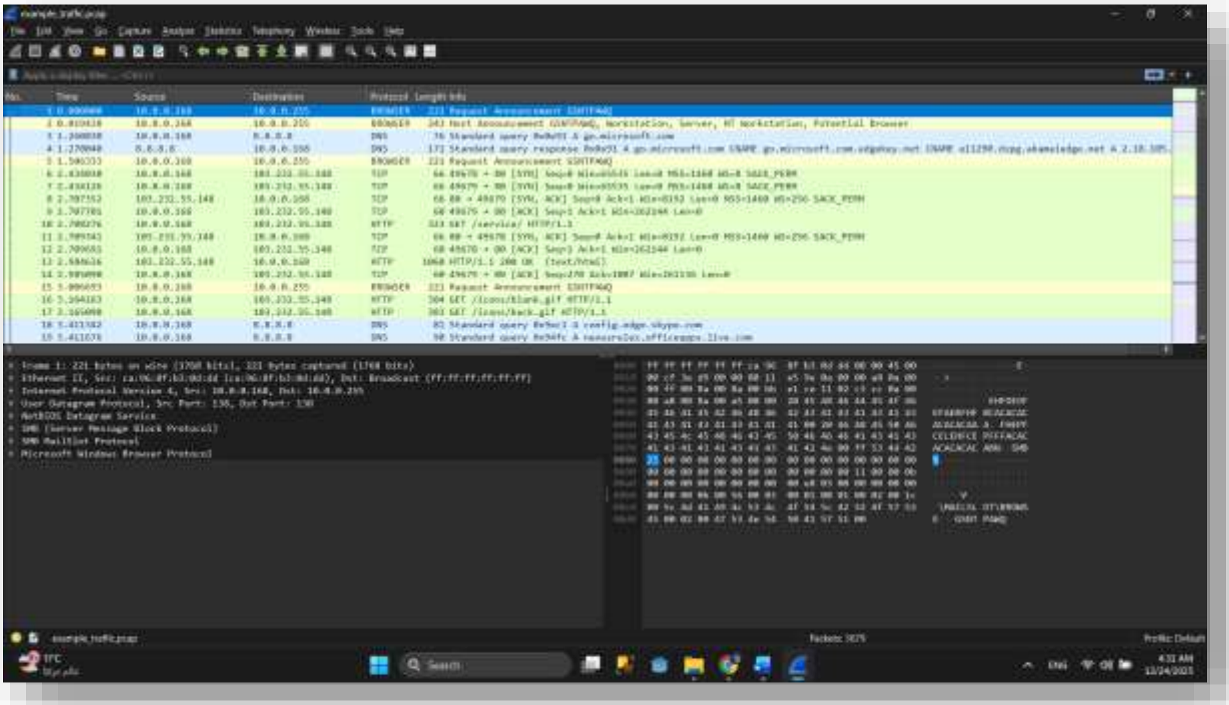
5. Technical Implementation

5.1 Technology Stack

Component	Technology / Purpose
Language	Python 3.8+ for cross-platform compatibility
Packet Processing	Scapy for PCAP parsing and packet manipulation
User Interface	Tkinter for cross-platform GUI (including with Python)
Visualization	Matplotlib for charts and graphs
Data Structures	Collections module (Counter, defaultdict) for efficient aggregation
Concurrency	Threading for non-blocking analysis
Logging	Standard logging library for application logs and audit trail

6. Test Case

Part 1: Evidence (pcap file)

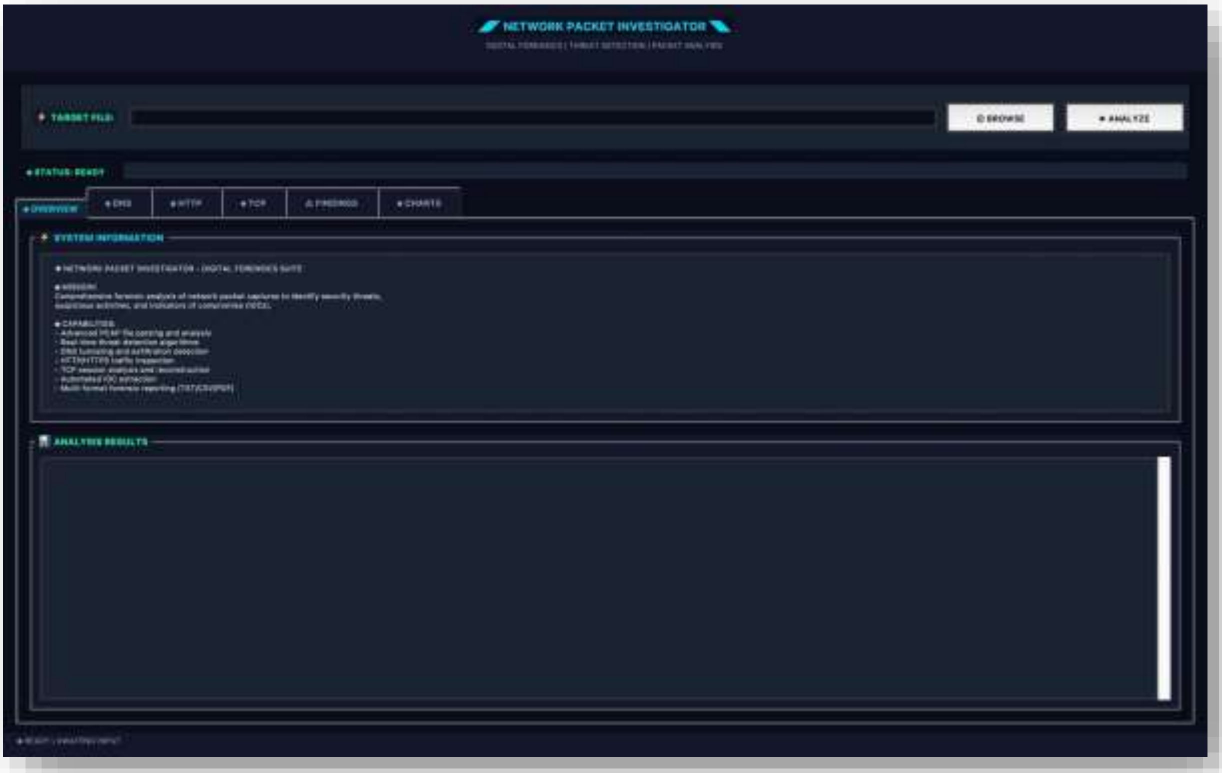


```
No.  Time      Source          Destination     Protocol Length Info
 1 0.000000   10.0.0.168      10.0.0.255      BROWSER  221 Request Announcement SIRTFAHQ
 2 0.019410   10.0.0.168      10.0.0.255      BROWSER  243 Host Announcement SIRTFAHQ, Workstation, Server, NT Workstation, Potential Browser
 3 1.260030   10.0.0.168      8.8.8.8         DNS       76 Standard query 0x0e51 A go.microsoft.com
 4 1.270040   8.8.8.8         10.0.0.168      DNS      172 Standard query response 0x0e51 A go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e11290.dspg.akamaiedge.net A 2.18.105.
 5 1.500333   10.0.0.168      10.0.0.255      BROWSER  221 Request Announcement SIRTFAHQ
 6 2.430010   10.0.0.168      103.232.55.148  TCP       66 49678 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
 7 2.430120   10.0.0.168      103.232.55.148  TCP       66 49679 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
 8 2.707352   103.232.55.148  10.0.0.168      TCP       66 80 → 49679 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
 9 2.707701   10.0.0.168      103.232.55.148  TCP       60 49679 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
10 2.708276   10.0.0.168      103.232.55.148  HTTP     323 GET /service/ HTTP/1.1
11 2.709341   103.232.55.148  10.0.0.168      TCP       66 80 → 49678 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
12 2.709551   10.0.0.168      103.232.55.148  TCP       60 49678 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
13 2.980636   103.232.55.148  10.0.0.168      HTTP    1068 HTTP/1.1 200 OK  (text/html)
14 2.995090   10.0.0.168      103.232.55.148  TCP       60 49679 → 80 [ACK] Seq=270 Ack=1007 Win=261136 Len=0
15 3.000693   10.0.0.168      10.0.0.255      BROWSER  221 Request Announcement SIRTFAHQ
16 3.164163   10.0.0.168      103.232.55.148  HTTP     304 GET /icons/blank.gif HTTP/1.1
17 3.165090   10.0.0.168      103.232.55.148  HTTP     303 GET /icons/back.gif HTTP/1.1
18 5.411362   10.0.0.168      8.8.8.8         DNS       83 Standard query 0x9e1 A config.edge.skype.com
19 5.411676   10.0.0.168      8.8.8.8         DNS       90 Standard query 0x94fc A resources.officeapps.live.com
```

```
Frame 1: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits)
Ethernet II, Src: ca:06:8f:b3:0d:dd (ca:06:8f:b3:0d:dd), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.0.0.168, Dst: 10.0.0.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
```

Packets: 3875

Part 2: Overview Review After Analysis

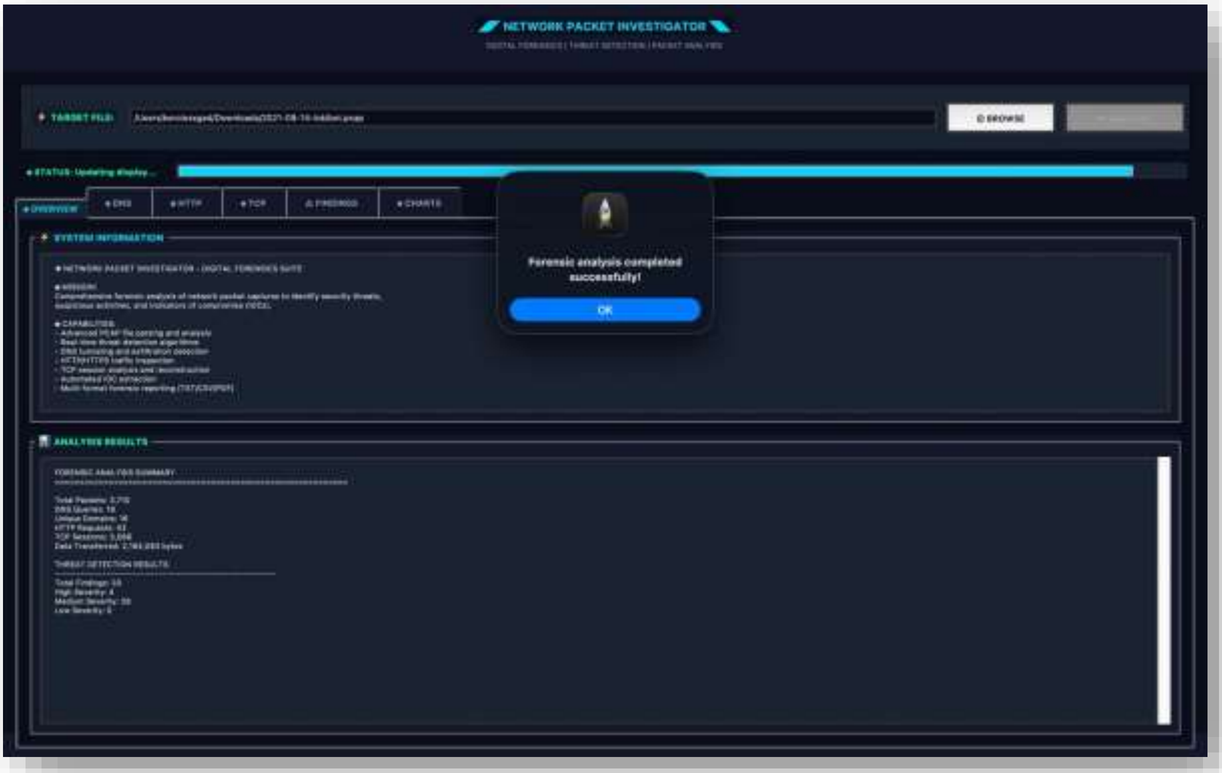


◆ NETWORK PACKET INVESTIGATOR - DIGITAL FORENSICS SUITE

◆ MISSION:
Comprehensive forensic analysis of network packet captures to identify security threats, suspicious activities, and indicators of compromise (IOCs).

◆ CAPABILITIES:
- Advanced PCAP file parsing and analysis
- Real-time threat detection algorithms
- DNS tunneling and exfiltration detection
- HTTP/HTTPS traffic inspection
- TCP session analysis and reconstruction
- Automated IOC extraction
- Multi-format forensic reporting (TXT/CSV/PDF)

◆ READY | AWAITING INPUT


NETWORK PACKET INVESTIGATOR
DIGITAL FORENSICS | THREAT DETECTION | PACKET ANALYSIS
⊙ BROWSE
◆ OVERVIEW
◆ DNS
◆ HTTP
◆ TCP
⚠ FINDINGS
◆ CHARTS
OK

TARGET FILE: /Users/[illegible]/Downloads/2021-08-16-[illegible].pcap

STATUS: Updating display...

Forensic analysis completed successfully!

SYSTEM INFORMATION

◆ NETWORK PACKET INVESTIGATOR - DIGITAL FORENSICS SUITE

◆ MISSION:
Comprehensive forensic analysis of network packet captures to identify security threats, suspicious activities, and indicators of compromise (IOCs).

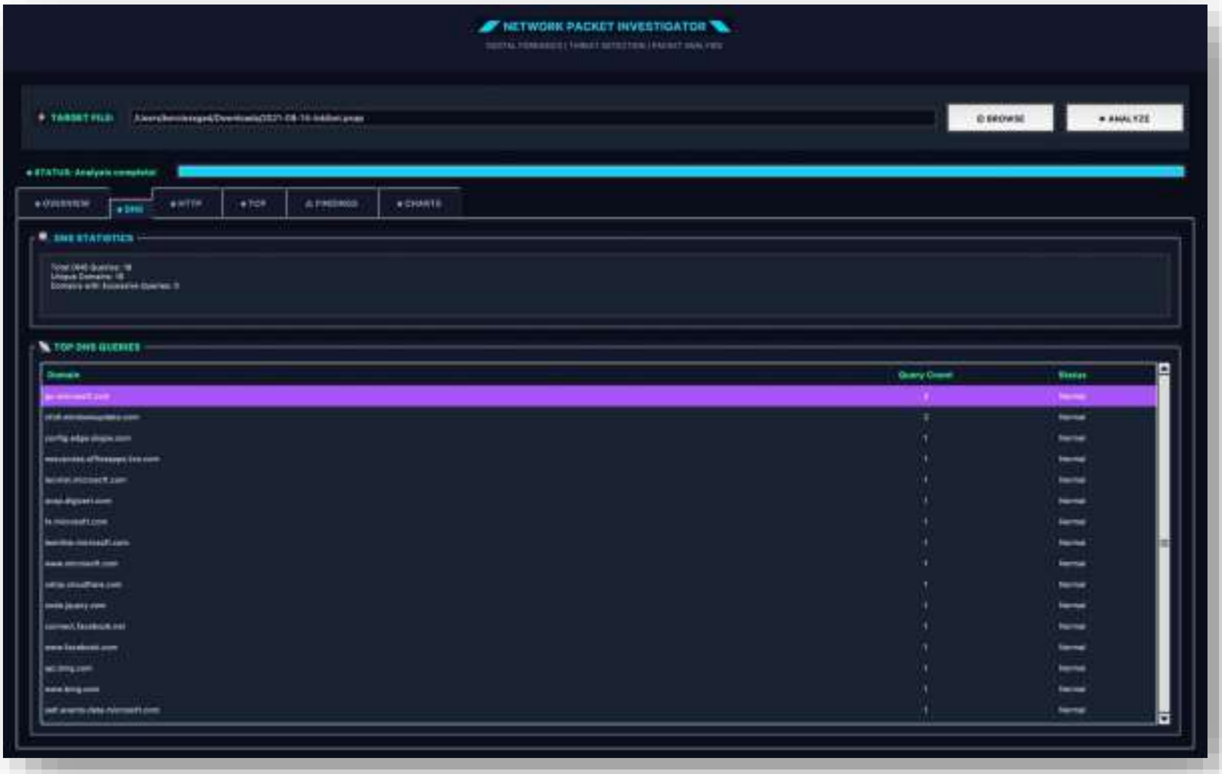
◆ CAPABILITIES:
- Advanced PCAP file parsing and analysis
- Real-time threat detection algorithms
- DNS tunneling and exfiltration detection
- HTTP/HTTPS traffic inspection
- TCP session analysis and reconstruction
- Automated IOC extraction
- Multi-format forensic reporting (TXT/CSV/PDF)

ANALYSIS RESULTS

```
FORENSIC ANALYSIS SUMMARY
==================================================
Total Packets: 3,710
DNS Queries: 18
Unique Domains: 16
HTTP Requests: 43
TCP Sessions: 5,066
Data Transferred: 2,783,293 bytes

THREAT DETECTION RESULTS
--------------------------------------------------
Total Findings: 33
High Severity: 4
Medium Severity: 29
Low Severity: 0
```

Part 3: Show DNS Analysis, HTTP Analysis, TCP Sessions


NETWORK PACKET INVESTIGATOR
DIGITAL FORENSICS | THREAT DETECTION | PACKET ANALYSIS
⊙ BROWSE
◆ ANALYZE
◆ OVERVIEW
◆ DNS
◆ HTTP
◆ TCP
⚠ FINDINGS
◆ CHARTS

TARGET FILE: /Users/[illegible]/Downloads/2021-08-16-[illegible].pcap

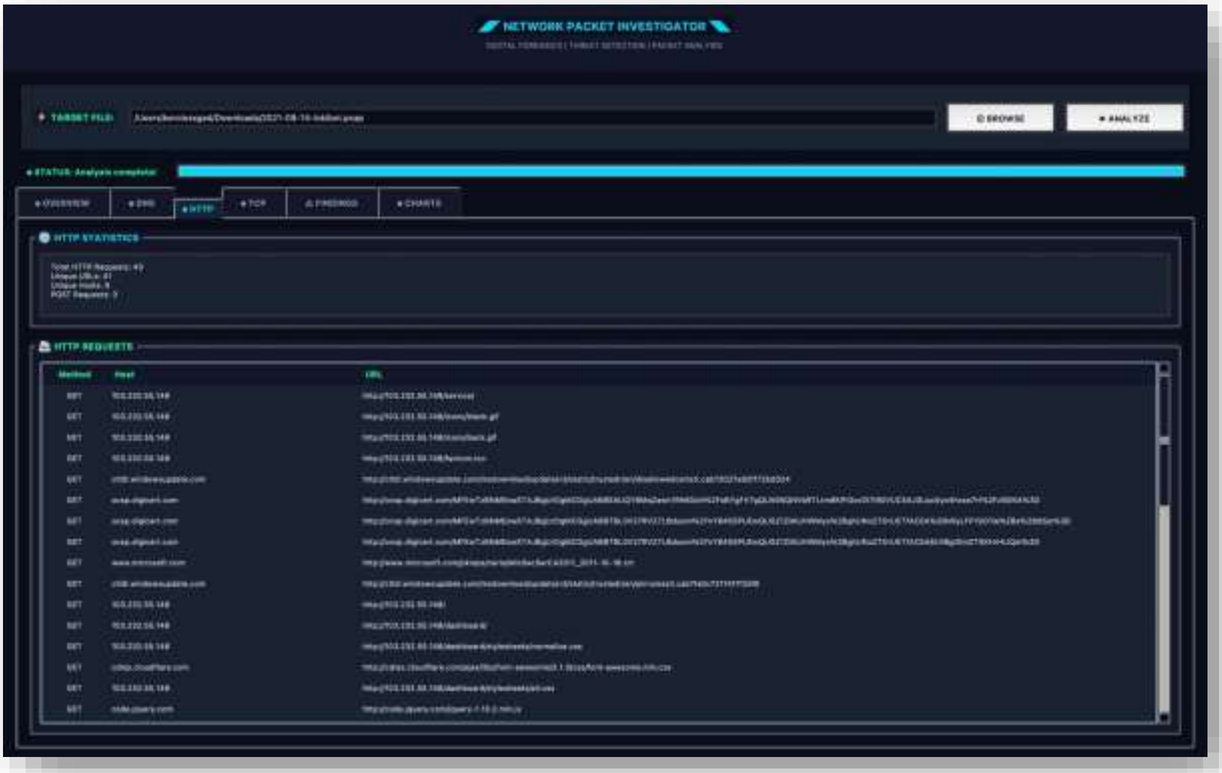
STATUS: Analysis complete!

DNS STATISTICS

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

TOP DNS QUERIES

Domain	Query Count	Status
go.microsoft.com	2	Normal
ctldl.windowsupdate.com	2	Normal
config.edge.skype.com	1	Normal
resources.officeapps.live.com	1	Normal
login.microsoft.com	1	Normal
ocsp.digicert.com	1	Normal
fe.microsoft.com	1	Normal
[illegible].microsoft.com	1	Normal
www.microsoft.com	1	Normal
cdnjs.cloudflare.com	1	Normal
code.jquery.com	1	Normal
connect.facebook.net	1	Normal
www.facebook.com	1	Normal
api.bing.com	1	Normal
www.bing.com	1	Normal
self.events.data.microsoft.com	1	Normal



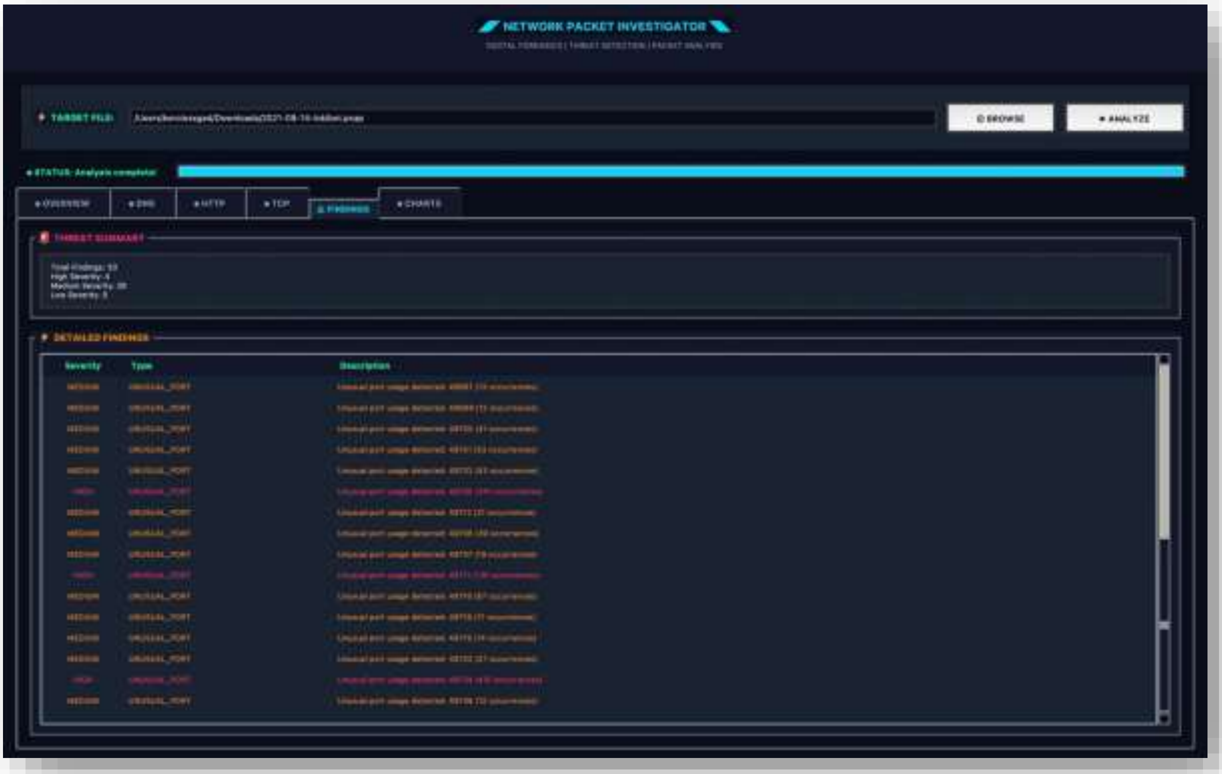
TARGET FILE: [illegible]

● STATUS: Analysis complete!

Total HTTP Requests: 49
Unique URLs: 41
Unique Hosts: 8
POST Requests: 3

Method	Host	URL
GET	103.232.55.148	http://103.232.55.148/service/
GET	103.232.55.148	http://103.232.55.148/icons/blank.gif
GET	103.232.55.148	http://103.232.55.148/icons/back.gif
GET	103.232.55.148	http://103.232.55.148/favicon.ico
GET	ctldl.windowsupdate.com	[illegible]
GET	ocsp.digicert.com	[illegible]
GET	ocsp.digicert.com	[illegible]
GET	ocsp.digicert.com	[illegible]
GET	www.microsoft.com	[illegible]
GET	ctldl.windowsupdate.com	[illegible]
GET	103.232.55.148	http://103.232.55.148/
GET	103.232.55.148	http://103.232.55.148/dashboard/
GET	103.232.55.148	http://103.232.55.148/dashboard/stylesheets/normalize.css
GET	cdnjs.cloudflare.com	[illegible]
GET	103.232.55.148	http://103.232.55.148/dashboard/stylesheets/all.css
GET	code.jquery.com	[illegible]

Part 4: Show Security Findings



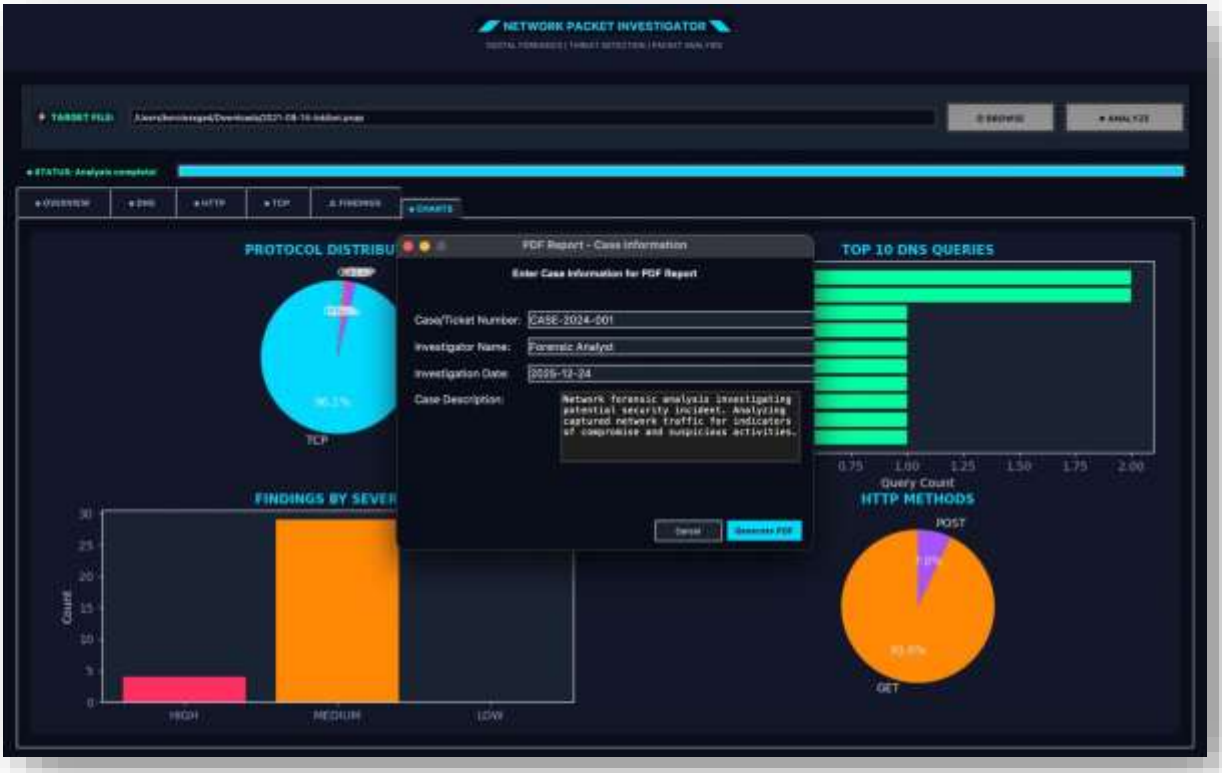
TARGET FILE: [illegible]

● STATUS: Analysis complete!

Total Findings: 53
High Severity: 4
Medium Severity: 38
Low Severity: 8

Severity	Type	Description
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
HIGH	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
HIGH	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]
HIGH	UNUSUAL_PORT	Unusual port usage detected: [illegible]
MEDIUM	UNUSUAL_PORT	Unusual port usage detected: [illegible]

Part 5: Generated report (CSV,TXT, PDF)



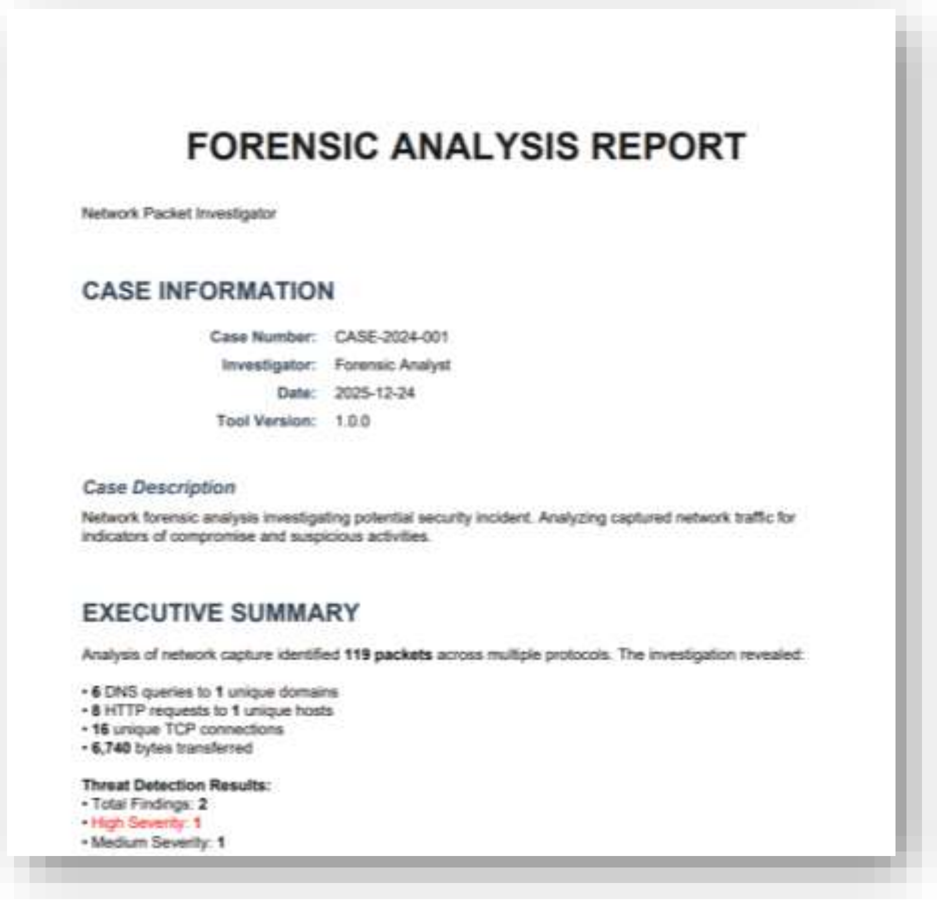
Enter Case Information for PDF Report

Case/Ticket Number: CASE-2024-001

Investigator Name: Forensic Analyst

Investigation Date: 2025-12-24

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



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.

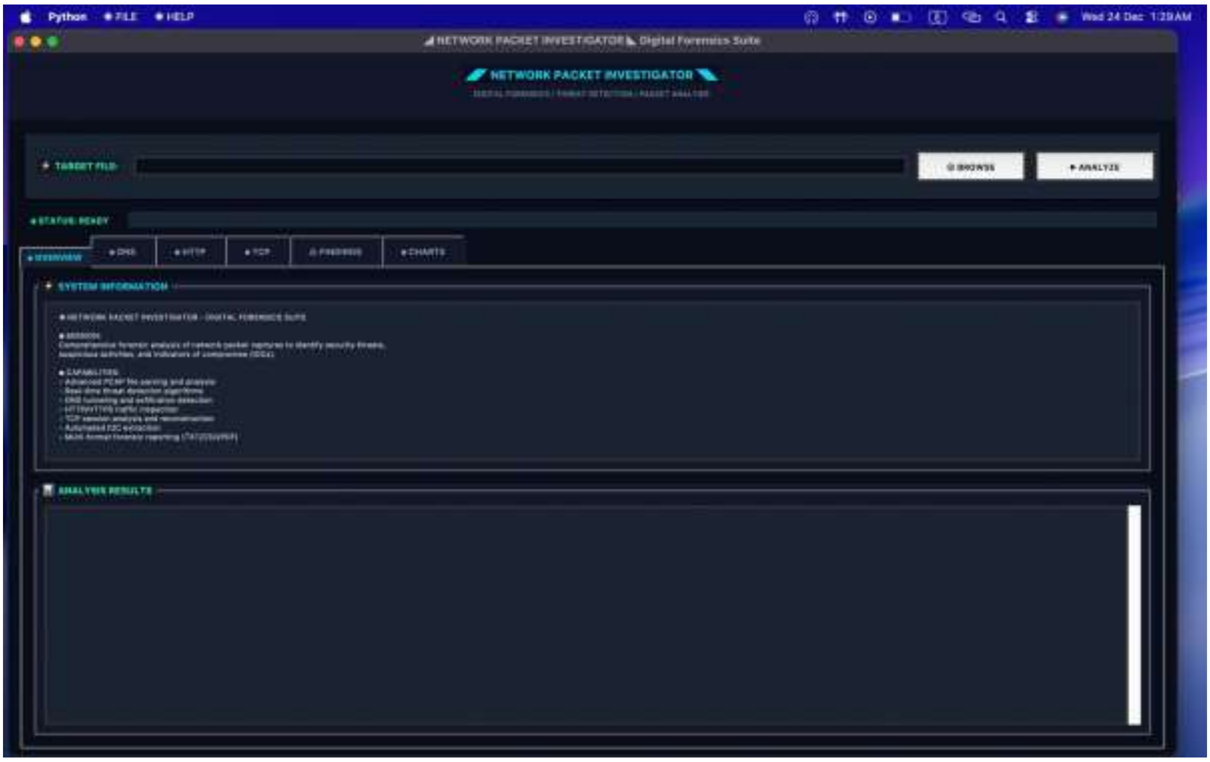
EXECUTIVE SUMMARY

Analysis of network capture identified **119 packets** across multiple protocols. The investigation revealed:

- **6** DNS queries to **1** unique domains
- **8** HTTP requests to **1** unique hosts
- **16** unique TCP connections
- **6,740** bytes transferred

Threat Detection Results:
- Total Findings: **2**
- High Severity: **1**
- Medium Severity: **1**

Part 6: Comfortable GUI



NETWORK PACKET INVESTIGATOR - DIGITAL FORENSICS SUITE

MISSION:
Comprehensive forensic analysis of network packet captures to identify security threats, suspicious activities, and indicators of compromise (IOCs).

CAPABILITIES:
- Advanced PCAP file parsing and analysis
- Real-time threat detection algorithms
- DNS tunneling and exfiltration detection
- HTTP/HTTPS traffic inspection
- TCP session analysis and reconstruction
- Automated IOC extraction
- Multi-format forensic reporting (TXT/JSON/PDF)

7. Limitations and Considerations

7.1 Current Limitations

Users should be aware of the following limitations:

- **No Packet Reassembly:** Fragmented packets are analyzed individually rather than reassembled
- **Limited Protocol Support:** Focus on DNS, HTTP, TCP, UDP, and ICMP; other protocols receive basic analysis
- **Memory Intensive:** Large PCAP files require significant RAM for processing
- **Offline Analysis Only:** No real-time capture capability; analyzes pre-captured files
- **Basic HTTPS Analysis:** Cannot inspect encrypted payload content

8. Future Enhancements

8.1 Planned Features

The following enhancements are under consideration for future releases:

- Real-time packet capture capabilities
- Additional protocol support (FTP, SMTP, IMAP, etc.)
- Machine learning-based anomaly detection
- Packet reassembly for fragmented traffic
- Timeline visualization of network events
- Integration with threat intelligence feeds
- Automated remediation suggestions
- Multi-file analysis for temporal correlation
- Baseline comparison mode
- Custom rule engine for organization-specific detection.