Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

DIGITAL FORENSICS

Training Course on Forensic Challenges of Encrypted Traffic Analysis

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
10 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Training Course on Forensic Challenges of Encrypted Traffic Analysis

Digital Forensics • 10 Days Intensive • Accredited Certification

Course Overview

Training Course on Forensic Challenges of Encrypted Traffic Analysis (Post-Quantum Crypto) addresses the urgent need for quantum-resilient cybersecurity strategies. We will explore the fundamental principles of post-quantum cryptography, including lattice-based, hash-based, and code-based algorithms, and their implications for forensic investigations.

Key Skills & Software Tools Covered

TLS/SSL analysis • packet inspection tools • traffic decryption

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
5 Jan 2026 – 16 Jan 2026	Nairobi	Classroom / 10d	**$3,000 USD / KES 220,000**
5 Jan 2026 – 16 Jan 2026	Kigali	Classroom / 10d	**$6,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Dubai	Classroom / 10d	**$10,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Cape Town	Classroom / 10d	**$9,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Addis Ababa	Classroom / 10d	**$6,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Singapore	Classroom / 10d	**$10,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Istanbul	Classroom / 10d	**$10,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Bangkok	Classroom / 10d	**$10,000 USD / KES 110,000**
5 Jan 2026 – 16 Jan 2026	Accra	Classroom / 10d	**$8,000 USD / KES 110,000**
19 Jan 2026 – 30 Jan 2026	Nairobi	Classroom / 10d	**$3,000 USD / KES 220,000**
19 Jan 2026 – 30 Jan 2026	Kigali	Classroom / 10d	**$6,000 USD / KES 110,000**
19 Jan 2026 – 30 Jan 2026	Dubai	Classroom / 10d	**$10,000 USD / KES 110,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Training Course on Forensic Challenges of Encrypted Traffic Analysis (Post-Quantum Crypto)

Introduction

The proliferation of encrypted network traffic, driven by heightened privacy concerns and pervasive digital communication, presents a formidable challenge to cybersecurity professionals and digital forensics investigators. Traditional traffic analysis techniques are rendered ineffective as the content of communications remains opaque. This course delves into the intricate world of encrypted traffic analysis (ETA), equipping participants with cutting-edge methodologies and tools to glean actionable intelligence from seemingly inscrutable data. As the threat of quantum computing looms, capable of breaking conventional cryptographic algorithms, understanding and implementing Post-Quantum Cryptography (PQC) becomes paramount. This training is crucial for organizations to maintain data confidentiality, integrity, and availability in the evolving threat landscape.

Training Course on Forensic Challenges of Encrypted Traffic Analysis (Post-Quantum Crypto) addresses the urgent need for quantum-resilient cybersecurity strategies. We will explore the fundamental principles of post-quantum cryptography, including lattice-based, hash-based, and code-based algorithms, and their implications for forensic investigations. Participants will gain practical skills in identifying encrypted anomalies, metadata analysis, and threat detection within encrypted streams, preparing them for the inevitable transition to a quantum-safe future. The course emphasizes real-world case studies and hands-on labs to ensure participants are proficient in applying advanced forensic techniques to post-quantum encrypted traffic, safeguarding critical data against harvest now, decrypt later attacks.

Course Duration

10 days

Course Objectives

- Develop expertise in techniques to analyze and interpret encrypted network traffic without decryption.
- Comprehend the underlying mathematical problems and cryptographic primitives of quantum-resistant algorithms
- : Recognize the vulnerabilities of present-day RSA, ECC, and TLS/SSL to Shor's algorithm and Grover's algorithm.
- Learn strategies and tools for lawfully intercepting and storing quantum-resistant encrypted communications for future analysis.
- Utilize NetFlow, IPFIX, and packet telemetry for anomaly detection and threat intelligence.
- Gain proficiency in using SSL/TLS fingerprinting to identify malware and suspicious applications within encrypted sessions.
- Discover techniques for uncovering hidden communications and steganography within seemingly innocuous encrypted traffic.
- Evaluate various PQC transition frameworks and best practices for securing digital infrastructure.
- Become adept at using specialized digital forensics tools and open-source intelligence (OSINT) for encrypted data.
- Navigate the complex legal landscape surrounding data privacy, warrant requirements, and chain of custody in encrypted investigations.
- Formulate robust incident response strategies to address security breaches involving post-quantum encrypted data.
- Understand the integration of classical and post-quantum algorithms for backward compatibility and future-proofing.
- Analyze practical scenarios of encrypted malware, ransomware, and advanced persistent threats (APTs) in a post-quantum context.

Organizational Benefits

- Proactively defend against evolving quantum threats and zero-day exploits concealed in encrypted traffic.
- Mitigate the impact of "harvest now, decrypt later" attacks by transitioning to quantum-safe encryption.
- Accelerate threat detection and forensic analysis of encrypted communications, minimizing breach containment time.
- Prepare for upcoming post-quantum cryptography standards and data privacy laws.
- Safeguard critical business data and proprietary information from advanced adversaries.
- Gain deeper insights into network activities, even with pervasive encryption, leading to more effective network security monitoring.
- Position the organization as a leader in cybersecurity innovation and quantum readiness.
- Prevent disruptions caused by encrypted malware and denial-of-service (DoS) attacks.
- Ensure that third-party communications and data exchanges are quantum-resistant.

Target Audience

- Digital Forensics Investigators
- Cybersecurity Analysts
- Incident Response Teams
- Network Security Engineers.
- Security Operations Center (SOC) Analysts
- Law Enforcement and Government Agencies.
- IT Security Managers
- Cryptographers and Security Researchers.

Course Outline

Module 1: Introduction to Encrypted Traffic Analysis & Quantum Computing

- Overview of the current encrypted traffic landscape and its challenges for forensics.
- Traditional network forensics vs. encrypted traffic analysis (ETA).
- Introduction to quantum computing principles and their cryptographic implications.
- Shor's Algorithm and Grover's Algorithm: How they break current cryptography.
- Case Study: The impact of pervasive TLS 1.3 adoption on enterprise security monitoring.

Module 2: Fundamentals of Post-Quantum Cryptography (PQC)

- The NIST PQC Standardization Process and selected algorithms
- Overview of lattice-based cryptography
- Introduction to hash-based cryptography and its applications.
- Understanding code-based cryptography .
- Case Study: Analyzing the security claims and practical performance of the NIST PQC finalists.

Module 3: Encrypted Traffic Visibility and Monitoring

- Techniques for gaining visibility into encrypted traffic without decryption
- NetFlow, IPFIX, and packet telemetry for anomaly detection.
- Leveraging DNS traffic and SSL/TLS handshake metadata for insights.
- Deep Packet Inspection (DPI) limitations and alternatives for encrypted data.
- Case Study: Detecting C2 communication obscured by legitimate encrypted traffic using flow analysis.

Module 4: TLS/SSL Forensics in a PQC Context

- In-depth analysis of TLS 1.3 and its cryptographic components.
- SSL/TLS fingerprinting using JA3 and JA3S hashes for malware identification.
- Analyzing certificate chains, certificate transparency logs, and revocation mechanisms.
- Impact of hybrid key exchange on TLS session analysis.
- Case Study: Tracing a ransomware attack hidden within a seemingly legitimate HTTPS connection, focusing on anomalous certificate usage.

Module 5: Metadata Analysis for Threat Detection

- Extracting and analyzing network metadata
- Using machine learning and AI for anomaly detection in encrypted traffic patterns.
- Identifying suspicious communication patterns
- Geolocation and time-based analysis of encrypted connections.
- Case Study: Pinpointing insider threat activity by analyzing unusual communication patterns to encrypted cloud storage.

Module 6: Advanced Packet Analysis Techniques

- Utilizing Wireshark and other packet analysis tools for encrypted traffic.
- Identifying and reconstructing encrypted sessions.
- Techniques for analyzing encrypted payload size and timing variations.
- Practical application of Bypassing SSL/TLS encryption for authorized forensics
- Case Study: Reconstructing a data exfiltration incident by analyzing encrypted tunnel traffic characteristics.

Module 7: Forensic Challenges of Hybrid Cryptography

- Understanding hybrid cryptographic constructions
- Challenges of analyzing traffic secured by quantum-resistant key exchange and digital signatures.
- Interoperability issues and fallback mechanisms in hybrid deployments.
- Forensic implications of quantum-safe VPNs and secure protocols.
- Case Study: Investigating a communication channel protected by a new hybrid PQC algorithm, focusing on identifying the PQC components.

Module 8: Identifying Encrypted Malware and APTs

- Indicators of Compromise (IoCs) in encrypted traffic for malware detection.
- Analyzing Command and Control (C2) communication over encrypted channels.
- Techniques for detecting encrypted tunneling and covert channels.
- Threat hunting for Advanced Persistent Threats (APTs) using encrypted traffic analysis.
- Case Study: Dissecting an APT campaign that uses custom encrypted protocols to evade traditional security tools.

Module 9: Quantum-Resilient Digital Signatures & Authentication

- Introduction to post-quantum digital signature schemes
- Forensic analysis of PQC-signed documents and software updates.
- Implications for digital certificates and Public Key Infrastructure (PKI) in a quantum era.
- Challenges in verifying authenticity and non-repudiation with PQC signatures.
- Case Study: Validating the authenticity of a PQC-signed firmware update after a potential supply chain attack.

Module 10: Legal, Ethical, and Privacy Considerations

- Legal frameworks and regulations governing encrypted traffic interception and analysis.
- Balancing national security and individual privacy in forensic investigations.
- Ethical dilemmas in decrypting and analyzing sensitive encrypted communications.
- Chain of Custody for encrypted digital evidence.

- Case Study: Navigating a complex legal request to analyze encrypted communications while adhering to privacy regulations.

Module 11: Tooling and Technologies for PQC Forensics

- Overview of commercial and open-source tools for ETA and PQC analysis.
- Utilizing forensic workstations and specialized hardware for large-scale data processing.
- Scripting and automation for encrypted traffic analysis workflows.
- Integrating threat intelligence feeds with PQC forensic tools.
- Case Study: Setting up a PQC forensic lab environment and demonstrating the use of a new quantum-safe analysis tool.

Module 12: Preparing for the Post-Quantum Transition

- Developing an organizational PQC migration roadmap.
- Cryptography inventory and risk assessment for quantum vulnerabilities.
- Strategies for crypto-agility and quick adaptation to new cryptographic standards.
- Best practices for securing long-term data storage against "harvest now, decrypt later" attacks.
- Case Study: A company's journey in auditing their current cryptographic footprint and planning their PQC transition.

Module 13: Future Trends in Quantum Computing and Cryptography

- Emerging quantum computing technologies and their impact on cybersecurity.
- Advancements in quantum key distribution (QKD) and its role in secure communications.
- The role of AI and machine learning in both attacking and defending cryptographic systems.
- Potential for new post-quantum attack vectors and countermeasures.
- Case Study: A forward-looking discussion on hypothetical quantum-enabled attacks and proactive defensive measures.

Module 14: Practical Labs & Simulations (Hands-on)

- Lab: Identifying anomalous patterns in encrypted network flows using ELK Stack
- Lab: Performing JA3/JA3S fingerprinting to identify specific applications and malware.
- Lab: Analyzing a captured PQC-encrypted session for metadata and protocol anomalies.
- Lab: Simulating a "harvest now, decrypt later" scenario and demonstrating PQC resilience.
- Lab: Using a forensic tool to extract and analyze metadata from a quantum-resistant encrypted file.

Module 15: Capstone Project & Advanced Topics

- Individual or group forensic investigation simulation involving complex encrypted traffic scenarios.
- Deep dive into selected advanced topics in post-quantum cryptanalysis or quantum-safe network architecture.
- Presentation of findings and defense of investigative methodologies.
- Q&A with industry experts and discussions on emerging challenges.
- Case Study: A full-scale simulated cyberattack scenario requiring comprehensive encrypted traffic analysis and PQC vulnerability assessment.

Training Methodology

- Instructor-Led Sessions: Engaging lectures, interactive discussions, and Q&A sessions with industry experts.
- Hands-on Labs: Practical exercises and simulations using industry-standard and specialized forensic tools to reinforce theoretical concepts.
- Real-World Case Studies: In-depth analysis of actual cyber incidents involving encrypted traffic and quantum-related challenges.
- Group Activities & Discussions: Collaborative problem-solving and knowledge sharing among participants.
- Demonstrations: Live demonstrations of tools, techniques, and PQC algorithm implementations.
- Capstone Project: A comprehensive, simulated forensic investigation to apply learned skills in a realistic scenario.
- Resource Materials: Access to course slides, whitepapers, research articles, and a curated list of tools and references.
- Continuous Assessment: Quizzes, lab exercises, and project evaluations to gauge understanding and progress.

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

<p class="MsoNormal" s

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/training-course-on-forensic-challenges-of-encrypted-traffic-analysis to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.