Understanding Cybersecurity Series

UCS Vol. 3 — October 2026

BCCC
Behaviour-Centric
Cybersecurity Center

Content

From the Founder's Desk	3
Executive Summary	4
Global Impact	5
UCS Analyzer & Analytics Series	6
UCS Dataset Series	22
UCS Book Series	41
UCS Blog Series	52
UCS Workshop Series	61
UCS Cartoon Contest Series	65
UCS Contributors	68

From the Founder's Desk

To address the growing challenges of cybersecurity resilience, it is essential to advance both AI use in cybersecurity and the development of Secure AI. On the one hand, AI-driven tools are needed to support daily security projects by detecting anomalies, analyzing threats, and automating responses at scale. On the other hand, AI models must be robust, private, and trustworthy to withstand adversarial attacks, poisoning, and misuse. Researchers and developers urgently require open-source tools, datasets, and analyzers that make these capabilities accessible, reproducible, and adaptable to real-world threats. With this mission, the **Understanding Cybersecurity Series (UCS)**, developed and led by the **Behaviour-Centric Cybersecurity Center (BCCC)** at York University**,** delivers inclusive, AI-powered, and secure-by-design resources that bridge research, industry, and education. Through open datasets, analyzers, training programs, and simplified outreach, UCS empowers students, academics, developers, and professionals to both apply AI effectively in cybersecurity and to safeguard AI systems themselves, fostering innovation and resilience across the ecosystem.

As a Canada Research Chair in Cybersecurity and Founder and Director of the BCCC, I recognized the need for a comprehensive knowledge mobilization program that could address the diverse needs of a broad spectrum of stakeholders, including K–12 students, postsecondary learners, educators, researchers, industry professionals, organizations, policymakers, and the general public. The UCS program was created to bridge this gap by delivering accessible, relevant, and impactful cybersecurity knowledge tailored to audiences with varying levels of technical expertise and experience, including through the **Cybersecurity Cartoon Award (CSCA)**, an international initiative promoting cybersecurity awareness through creativity. Through this initiative, we aim to advance cybersecurity education and research while equipping the community with the tools and awareness needed to navigate and secure an increasingly digital world. The UCS represents a commitment to inclusivity, accessibility, and innovation in the pursuit of a more resilient cybersecurity ecosystem.

Arash Habibi Lashkari, PhD
Canada Research Chair (CRC) in Cybersecurity
Full Professor at York University, Canada
Founder and Director, BCCC

Executive Summary

The Understanding Cybersecurity Series (UCS), an initiative of the Behaviour-Centric Cybersecurity Center (BCCC) at York University, serves as a comprehensive knowledge mobilization platform that translates cybersecurity research into accessible resources for academia, industry, government, and the broader community. Through open-source tools, educational materials, and outreach activities, UCS promotes cybersecurity awareness, supports innovation, and strengthens resilience against emerging cyber threats. Over the years, UCS resources have been adopted by thousands of researchers, educators, students, government agencies, organizations, and industry professionals across more than 120 countries. Through its open datasets, analyzers, educational resources, and cybersecurity solutions, UCS has become a trusted platform for advancing cybersecurity research, supporting innovation, enhancing education, and enabling evidence-based decision-making across diverse sectors.

As of October 2026, UCS has delivered 15 analyzers, 18 datasets, 10 books, 45 blogs, 18 workshops, and 3 cybersecurity cartoon contests. Collectively, these resources support research, education, training, and public engagement across diverse areas, including AI for cybersecurity, secure AI, network and IoT security, malware analysis, blockchain security, digital privacy, and cybersecurity governance. The growing global adoption of UCS resources reflects their value as trusted and widely used references for advancing cybersecurity knowledge and practice.

15
Analyzers

18
Datasets

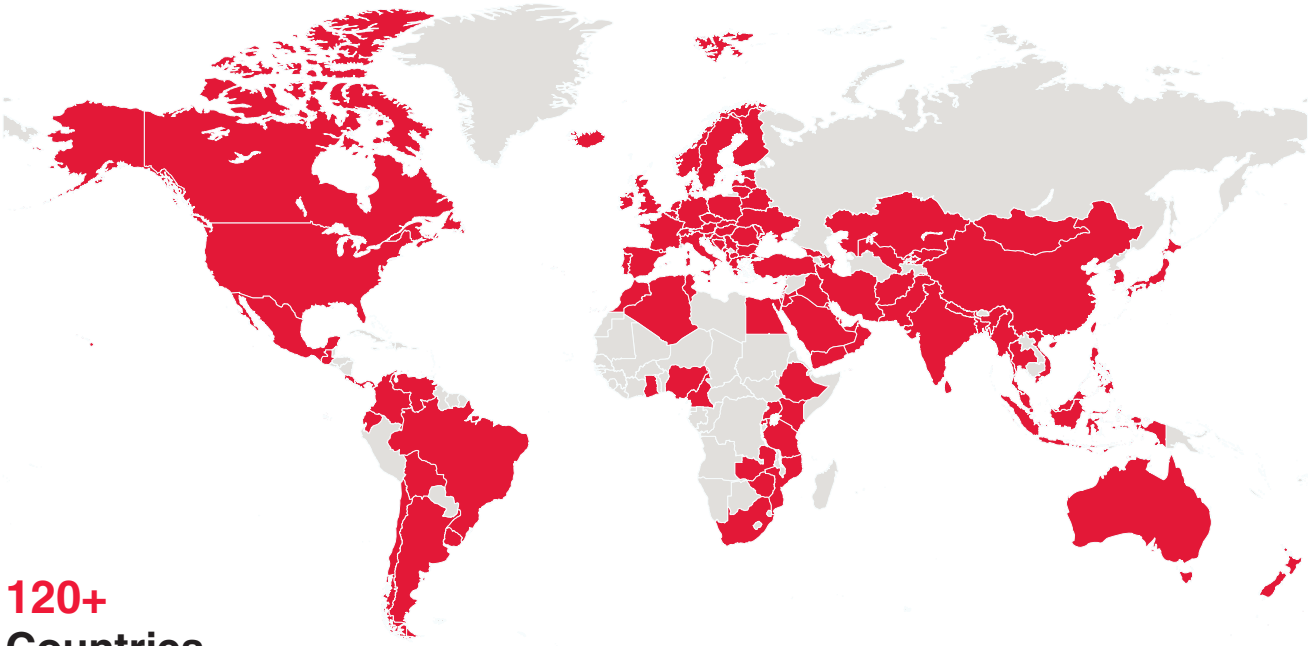
10
Books

45
Blogs

18
Workshops

3
Contests

Global Impact



120+
Countries

Thousands of researchers, universities, companies, government agencies, and organizations have used and benefited from UCS resources worldwide

220K+
Downloads

Total downloads of UCS datasets worldwide

500+
Adoptions

Community forks of UCS open-source analyzers on Github

15K+
Citations

Citations of UCS published articles and books

50+
HQPs

Highly Qualified Personnel who are contributing to UCS

5K+
Participants

Participants reached across all UCS workshops and talks

20+
Partners

Sponsors and collaborators supporting the UCS mission

Analyzers & Analytics

Powerful open-source tools for research and development

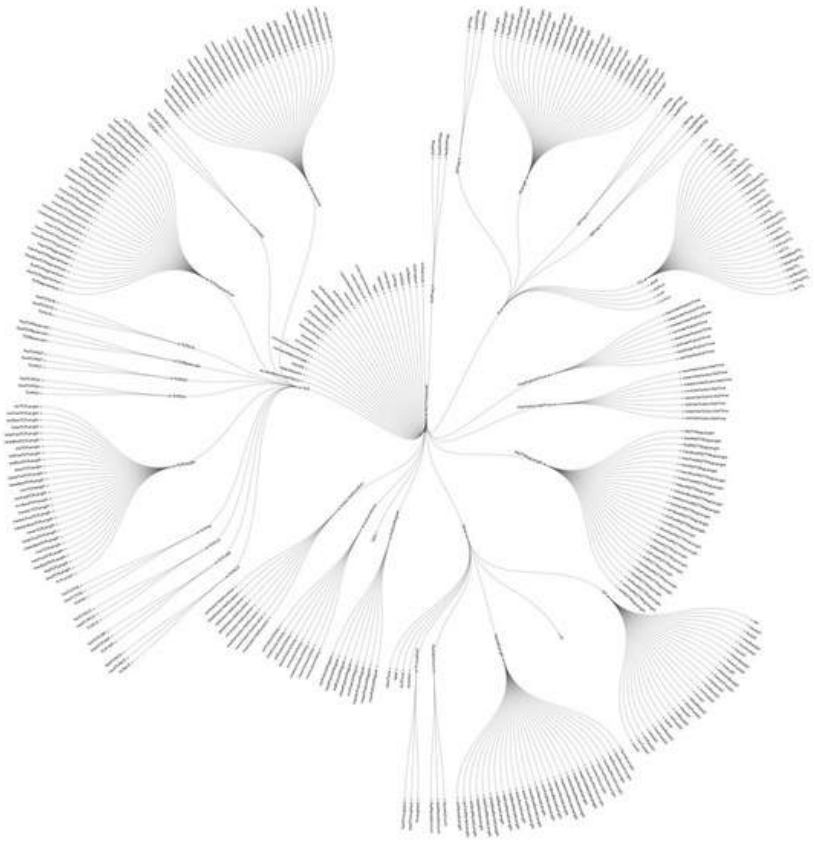
01 MQTTFlowLyzer
02 QUICFlowLyzer
03 UDPFlowLyzer
04 VehCANSigLyzer
05 IoT-ZwaveNetLyzer V1.0
06 DeFiTransLyzer V1.0
07 SCsVulLyzer V2.0, V1.0
08 NTLFlowLyzer V3.0, V2.0, V1.0
09 ALFlowLyzer V1.0
10 VolMemLyzer V2.0, V1.0
11 BUP V1.0
12 SCsVulSegLytix
13 AuthAttLyzer
14 PDFMalLyzer
15 DoHLyzer

MQTTFlowLyzer

Message Queuing Telemetry Transport (MQTT) Network Traffic Analyzer

As part of the UCS, MQTTFlowLyzer is an open-source Python library developed to extract features from MQTT-based network traffic. It analyzes all MQTT packets in a PCAP file and generates a dataset that is essential for developing an intrusion detection system (IDS). MQTTNetLyzer is a session-based analyzer; it essentially extracts packet-level features and aggregates them to generate a session. There are several criteria for the aggregation: all packets in a session must have the same source/destination IP address, source/destination port number, client ID, and pub-sub topic.

A session is initiated by a CONNECT packet and ended by either a DISCONNECT packet or by implemented constraints, such as maximum session duration and inactivity timeouts. MQTTFlowLyzer is a bidirectional session generator, with the forward direction determined by the CONNECT packet. MQTTFlowLyzer also extracts relevant features from an MQTT packet's Network and Transport layers. Additionally, MQTTFlowLyzer calculates new features beyond raw features and adds them to the session. It also calculates statistical features for some features, such as mean, median, variance, and skewness, in both directions. It can extract 321 features from a pcap file.

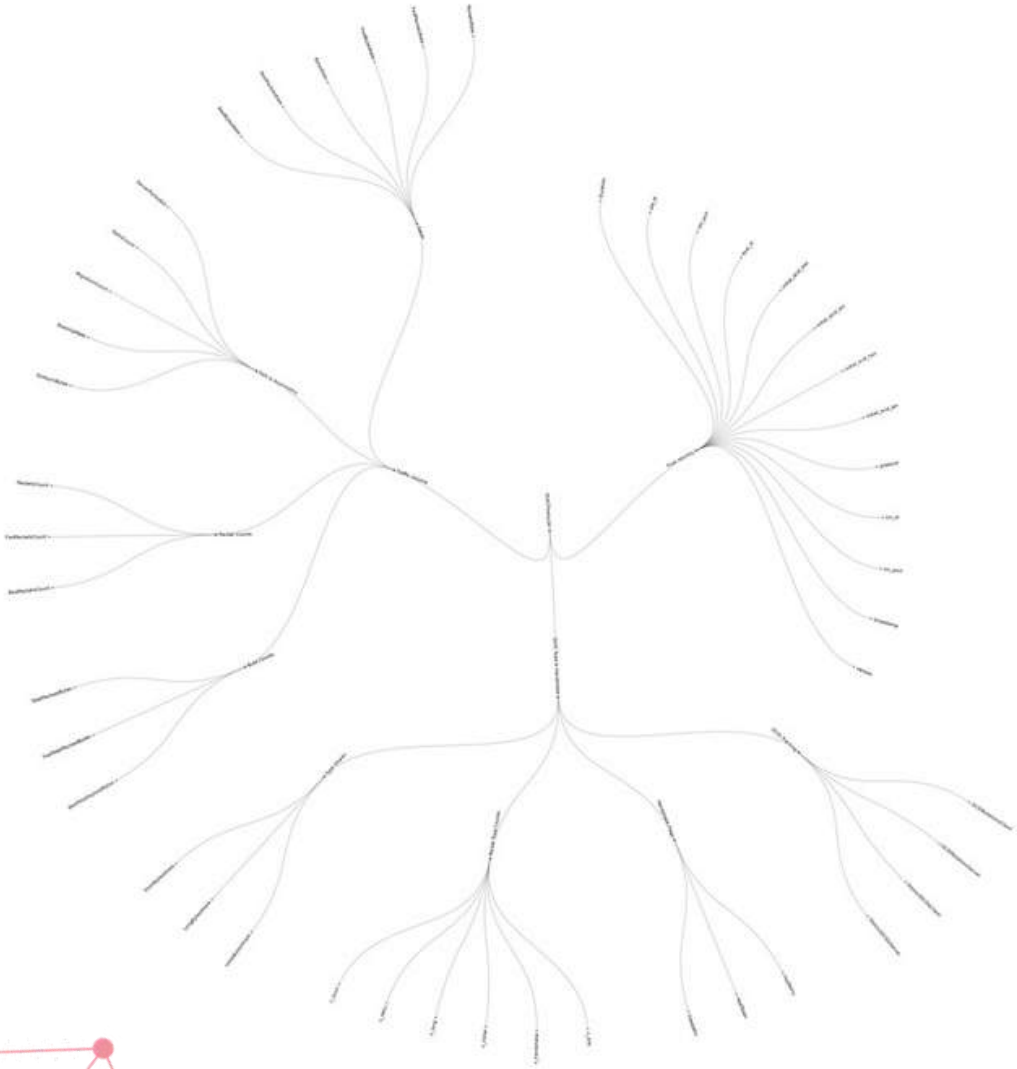


QUICFlowLyzer

QUIC Network Traffic Flow Analyzer

As part of the UCS, QUICFlowLyzer is a lightweight, header-only QUIC network traffic analyzer that extracts packet- and flow-level features from PCAP and PcapNG network captures without requiring payload decryption. The tool parses QUIC protocol header fields to generate structured flow records and feature tables suitable for network monitoring, traffic characterization, cybersecurity research, and machine learning applications.

QUICFlowLyzer supports the analysis of individual PCAP files, large collections of traffic captures through batch processing, and VXLAN-decapsulated traffic environments. Extracted QUIC-specific features are exported in CSV format, enabling efficient integration with data analytics, intrusion detection, traffic classification, and behavioral modeling workflows.

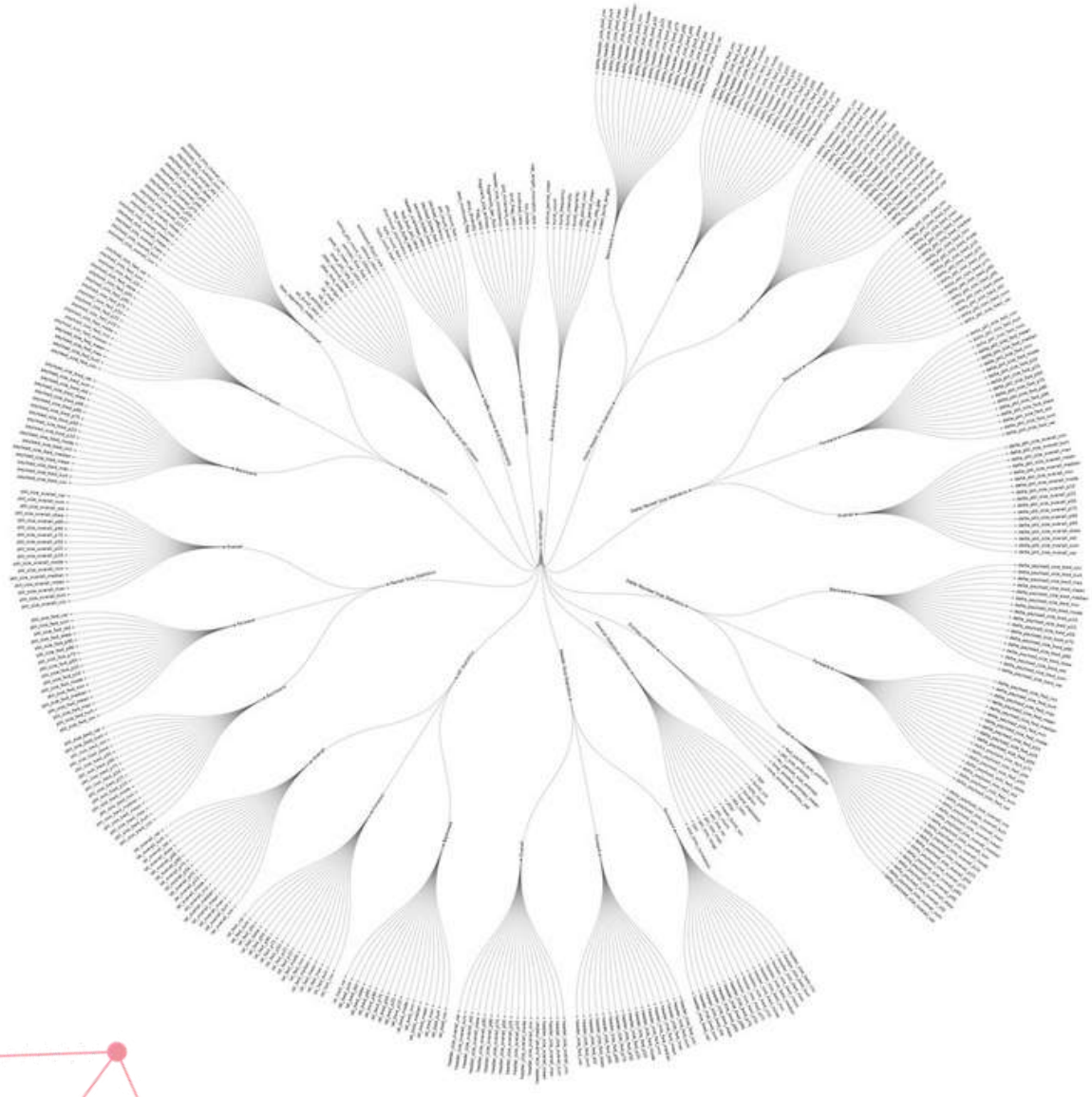


UDPFlowLyzer

UDP Network Traffic Analyzer

As part of the UCS, UDPFlowLyzer is a specialized network traffic flow analyzer designed to extract comprehensive flow-level features from UDP communications captured in PCAP and PcapNG files. The framework generates a rich set of statistical, temporal, volumetric, and behavioral features, including UDP header characteristics, packet timing statistics, traffic volume metrics, burst behavior, entropy measurements, percentile-based descriptors, and advanced flow analytics.

Supporting configurable flow generation and scalable processing of large network traces, UDPFlowLyzer produces structured feature datasets for intrusion detection, traffic classification, anomaly detection, and cybersecurity research.

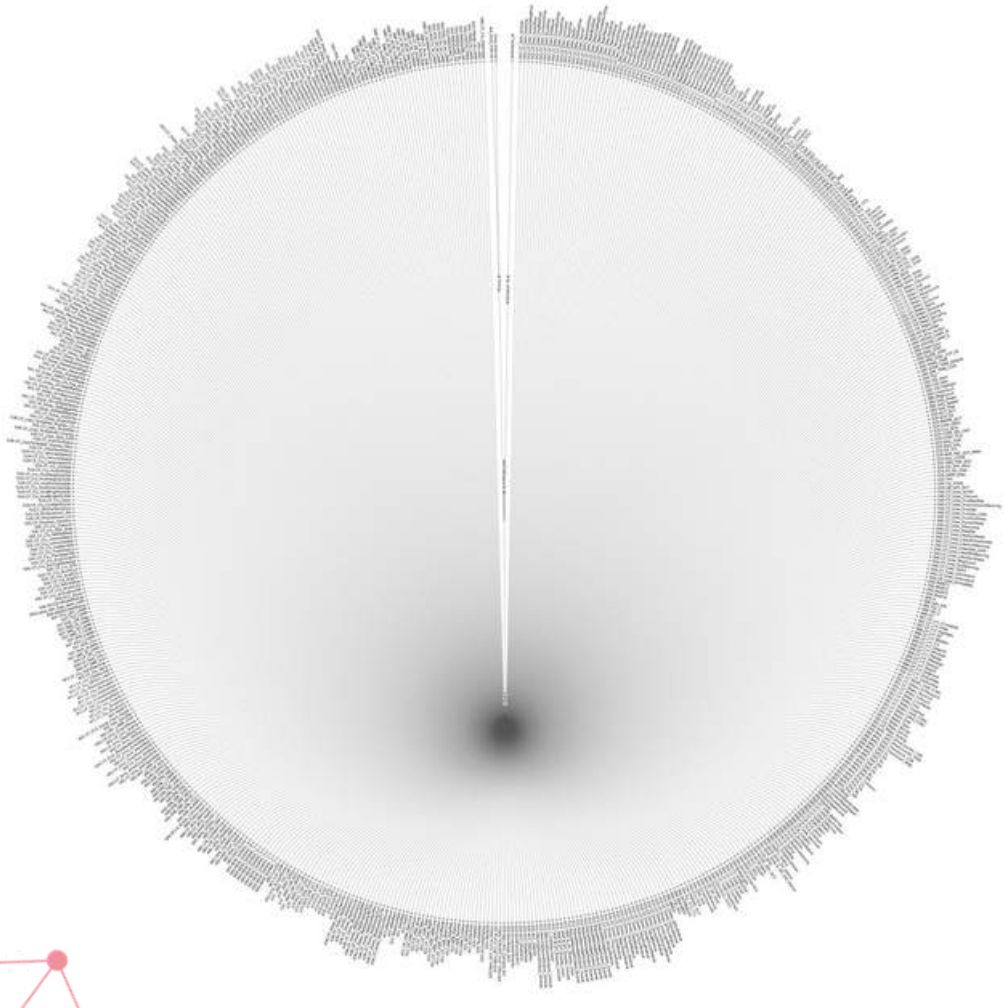


VehCANSigLyzer

Vehicular CAN Signal Analyzer

VehCANSigLyzer, a part of the UCS, is a Python-based tool for extracting timing-based and signal-level features from Controller Area Network (CAN) traffic. Applicable to CAN logs collected using the can-utils Linux utility, VehCANSigLyzer converts timestamp data to two timing-based features: time intervals between successive frames and time intervals within individual identifier streams. Additionally, it utilizes the cantools library with open-source database container (DBC) files to decode signal-level features from CAN frame payloads, resulting in over 600 signal features.

VehCANSigLyzer converts CAN logs into a final feature set that includes time intervals, signals, and arbitration identifiers. These features together capture the anomalies introduced by various CAN attacks, from fabrication attacks like denial of service, replay, and spoofing, to advanced attacks like masquerade and suspension. The analyzer provides a comprehensive representation of temporal and semantic CAN bus behaviour to support robust intrusion detection.

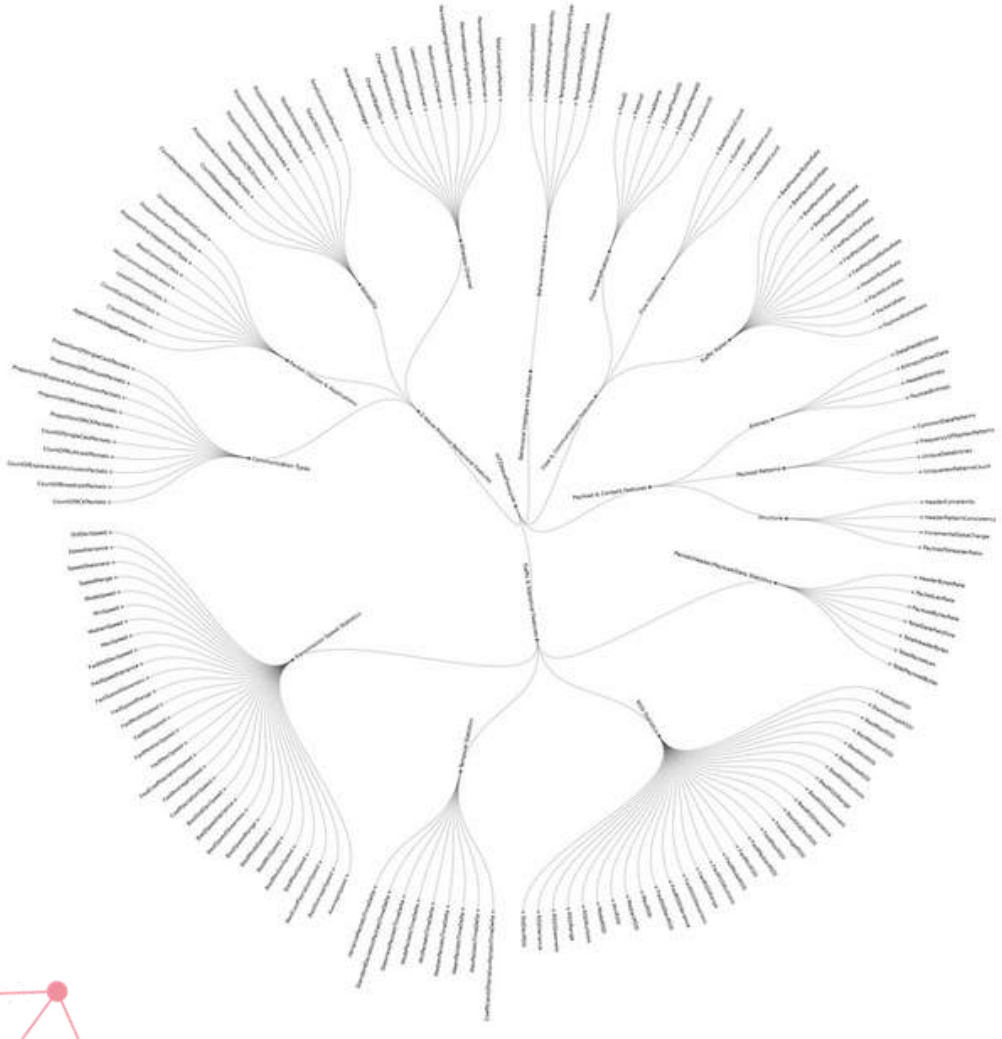


IoT-ZwaveNetLyzer V1.0

IoT Zwave Network Analyzer

As part of the UCS, IoT-ZwaveNetLyzer is an open-source Python project developed for analyzing Z-Wave network traffic in IoT environments. It generates bidirectional traffic flows and extracts over 400 statistical and protocol-level features, such as signal strength (RSSI), packet speed, acknowledgement ratios, and channel use patterns. By profiling both forward and backward communication streams, it enables a fine-grained understanding of device behaviour and communication efficiency across smart home and industrial IoT networks.

Designed for scalability and transparency, IoT-ZwaveNetLyzer supports both Linux and Windows environments and can be customized through simple configuration files, enabling flexible use in research and experimentation. The analyzer is a crucial tool for building and validating IoT intrusion detection systems, providing a structured framework to characterize device behaviour, network stability, and traffic anomalies in both real and simulated environments.

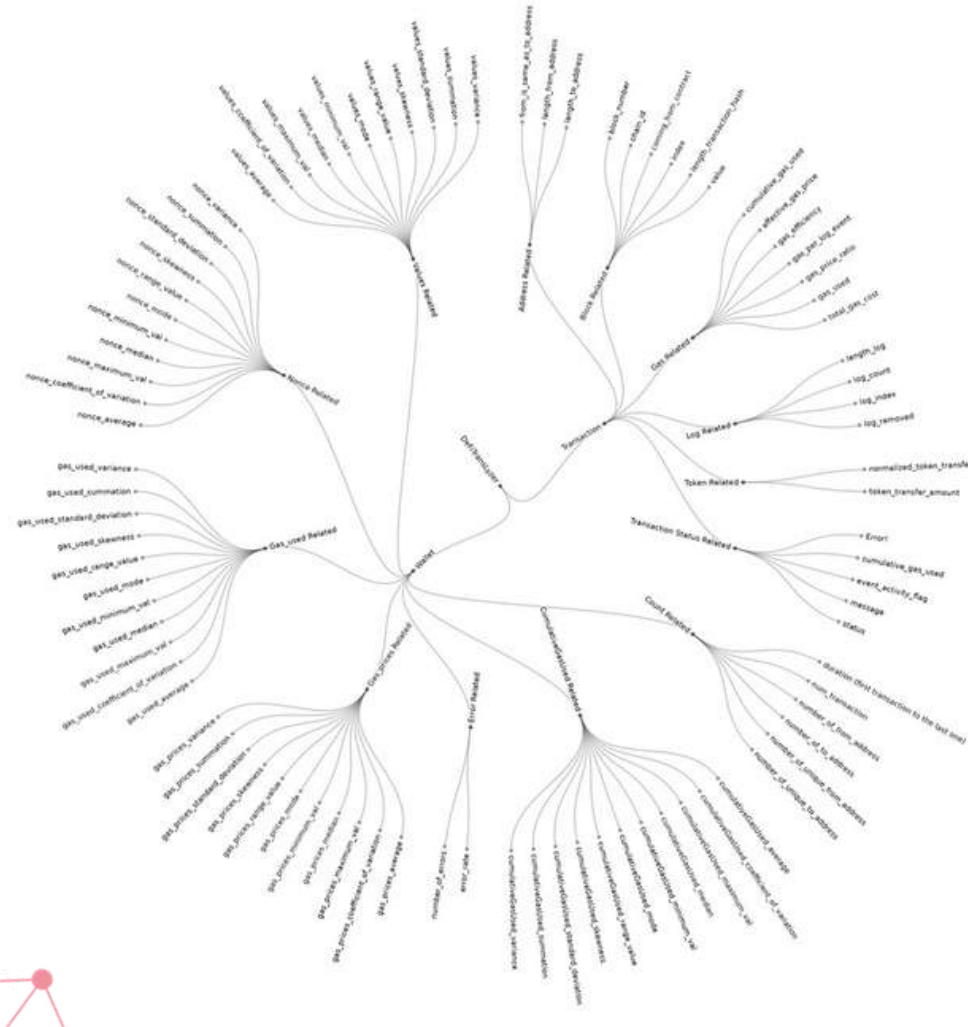


DeFiTransLyzer V1.0

Decentralized Finance Transaction Analyzer

DeFiTransLyzer, part of the UCS, is an open-source Python framework designed to extract and analyze features from Ethereum wallets and transactions. Its Wallet Analyzer processes JSON-based wallet records to compute statistical measures such as averages, variance, skewness, gas usage, and transaction values, while also capturing dynamics like durations, error rates, and interacting addresses. The results are returned as a structured feature dictionary, providing a clear view of wallet-level behaviour.

The Transaction Analyzer complements this by parsing individual transaction data. It extracts gas usage, values, and efficiency ratios, while also analyzing event logs, token transfers, contract creation, and self-interactions. By returning structured transaction-level features, it provides detailed insights into blockchain activity. Together, the two modules form a unified toolchain for profiling Ethereum behaviour, supporting vulnerability research, behavioural modelling, and broader DeFi security studies.

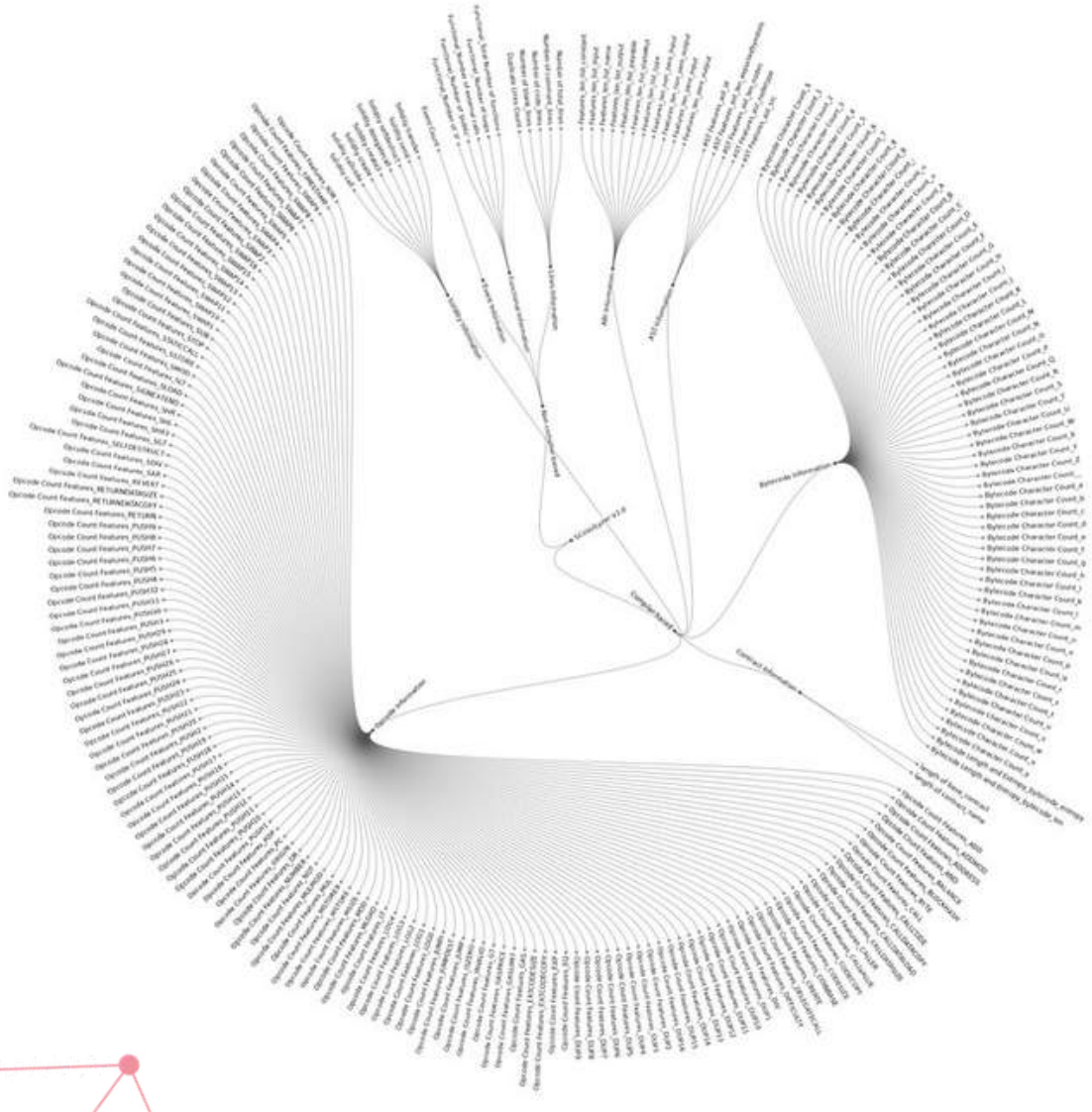


SCsVulLyzer V2.0, V1.0

Smart Contracts Vulnerability Analyzer

SCsVulLyzer V2.0, part of UCS, is an open-source Python tool that extracts over 240 features to profile Ethereum Smart Contracts for vulnerability detection. It extends V1.0 by classifying features into compiler-based (e.g., AST, ABI) and non-compiler-based categories, the latter using natural language processing (NLP) to detect critical security-related keywords.

This version also introduces new feature groups—Contract Information, Source Code Information, and Solidity Information—that capture metrics such as function counts, loops, and lines of code. A key addition is bytecode entropy, which measures randomness and complexity in smart contracts, enabling deeper insights for vulnerability analysis, anomaly detection, and cryptographic risk assessment.

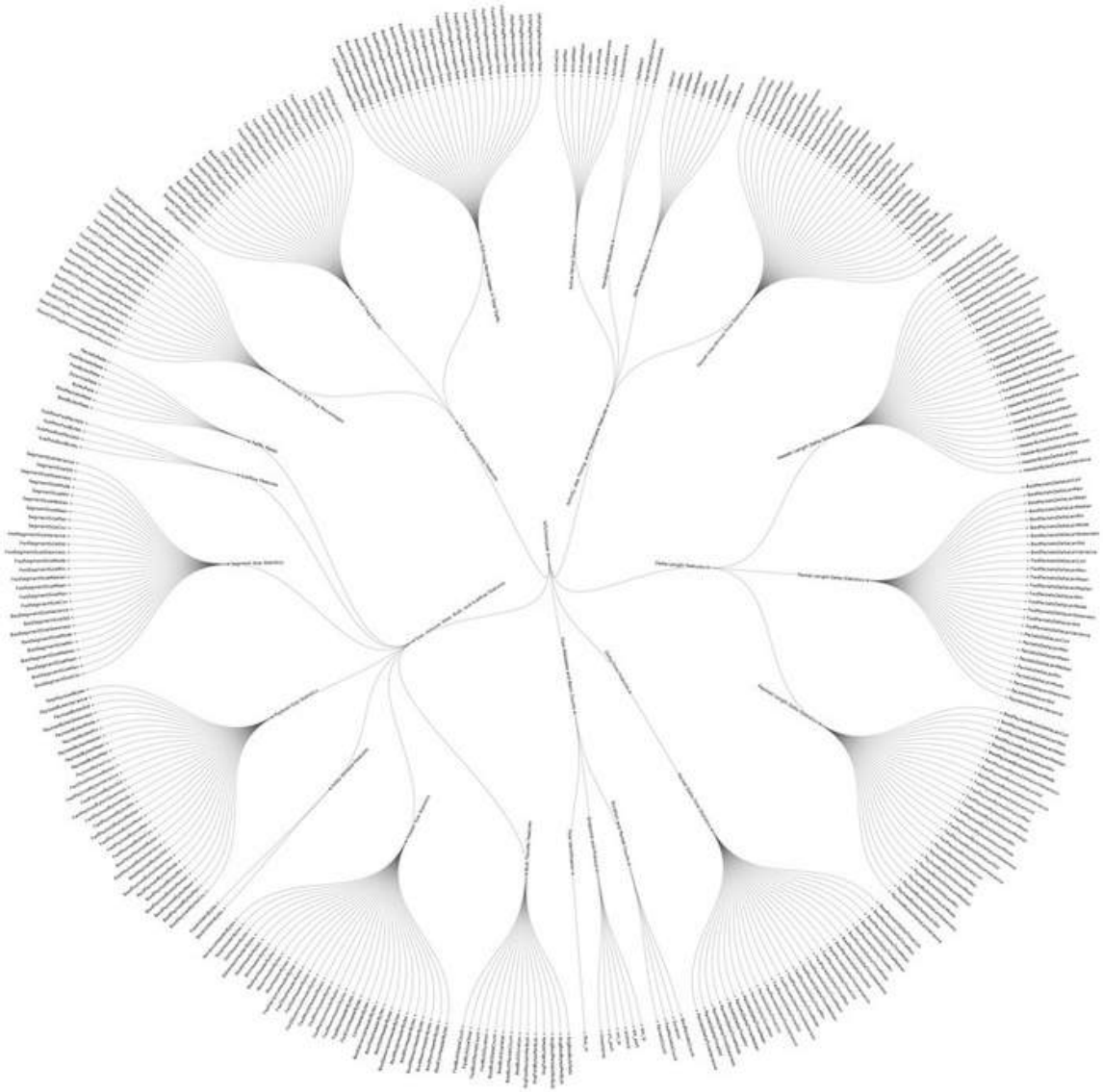


NTLFlowLyzer V3.0, V2.0, V1.0

Network and Transportation Layer Flow Analyzer

NTLFlowLyzer, part of the UCS and the second component of NetFlowLyzer, is an open-source Python tool for extracting network layer features from TCP-based traffic to support anomaly profiling. It builds bidirectional flows at the network and transport layers, with the first packet defining forward and backward directions for separate statistical and time-based analysis.

The tool allows users to select or add features and adjust flow timeout settings. TCP flows are terminated automatically when a connection ends (FIN or RST), when maximum duration is reached, or after inactivity, ensuring accurate and flexible flow profiling for security research.

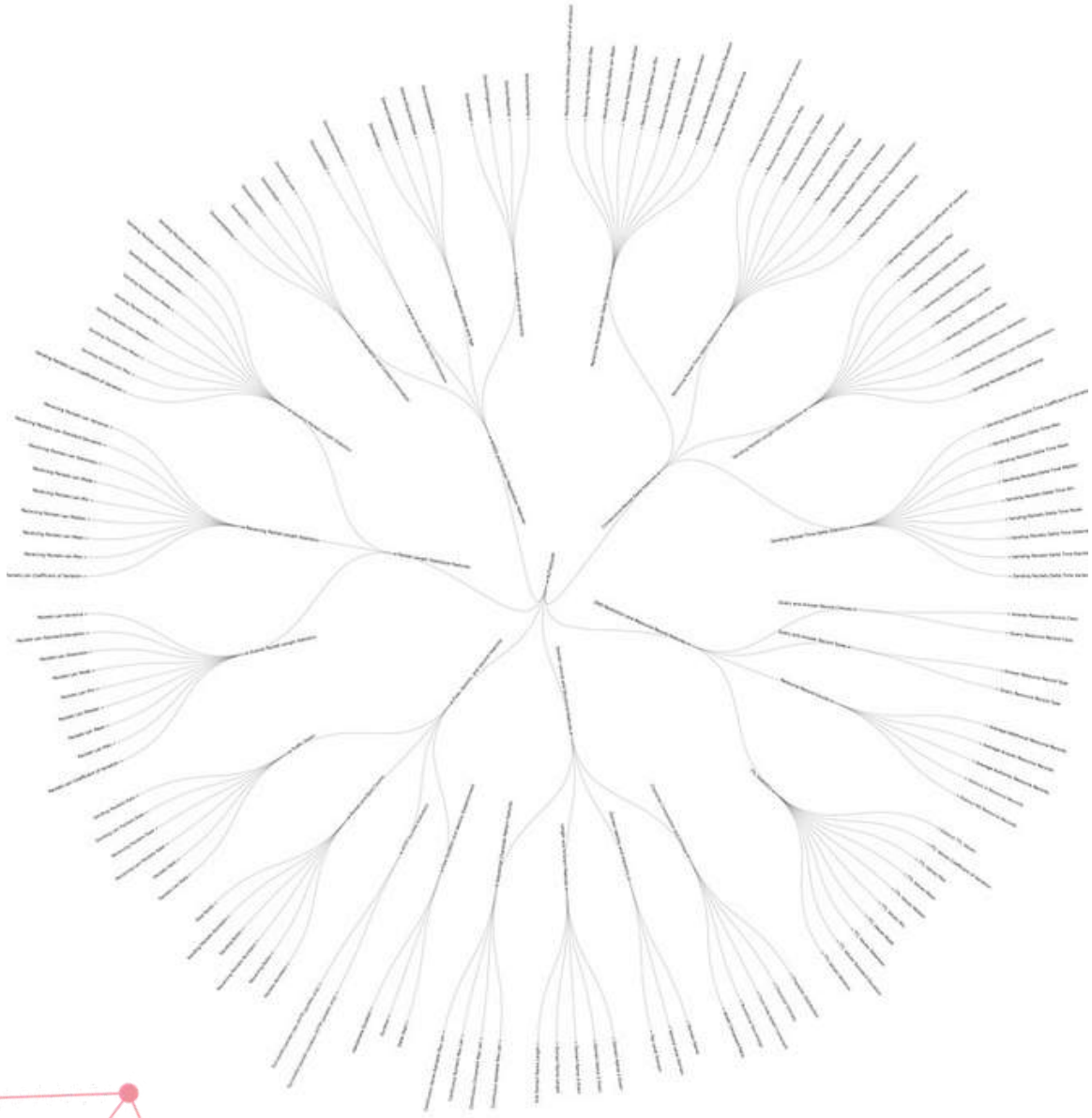


ALFlowLyzer V1.0

Application Layer Flow Analyzer

ALFlowLyzer, part of the UCS and the third component of NetFlowLyzer, is an open-source Python tool for extracting application-layer features from network traffic to support anomaly profiling. It focuses on flows where threats often emerge, extending analysis beyond transport and network layers.

The tool builds bidirectional flows with separate forward and backward statistics, allows feature selection or addition, and supports flow timeout customization. The first release targets the DNS protocol, with future versions planned to cover additional application-layer protocols.

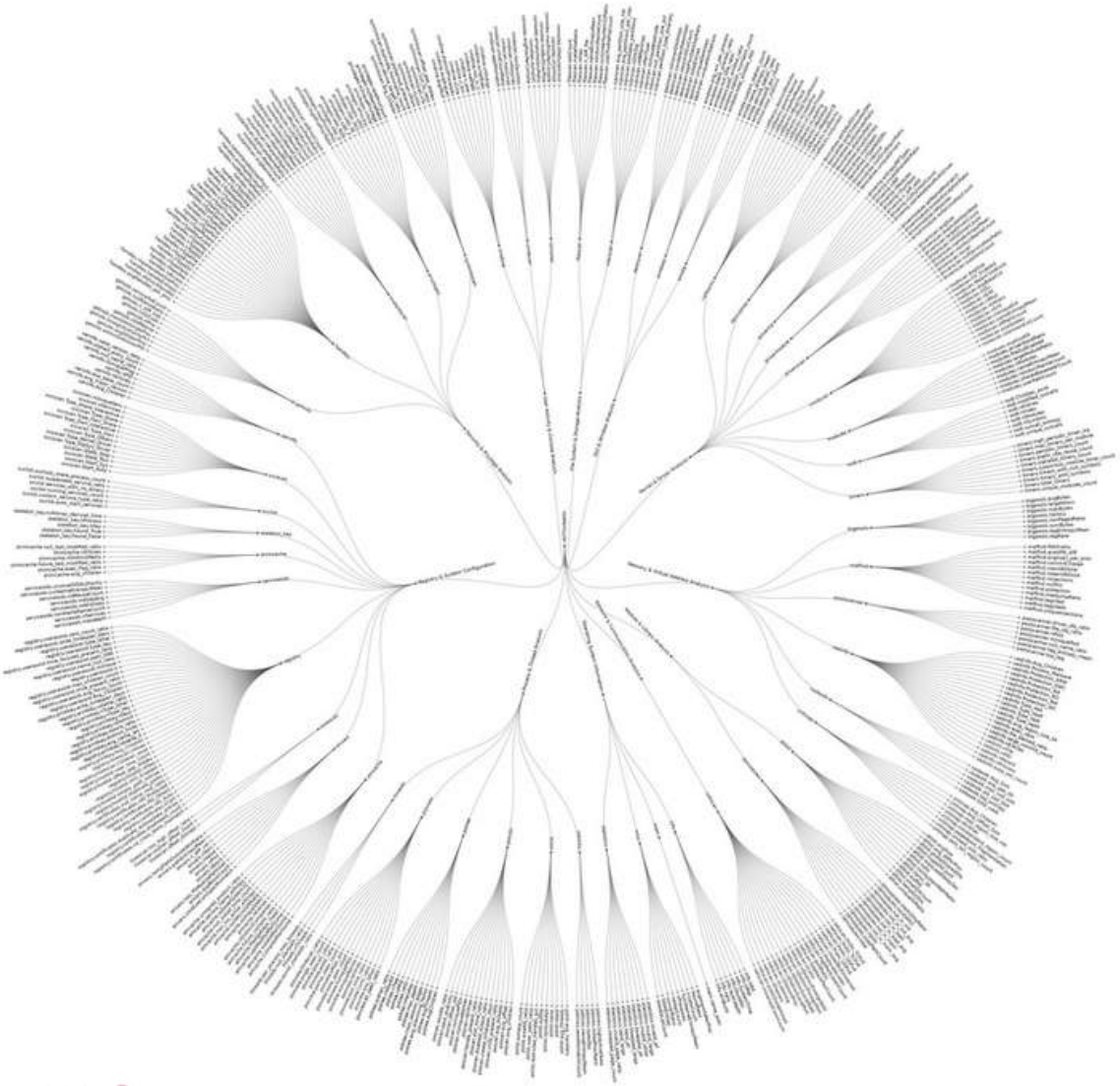


VolMemLyzer V2.0, V1.0

Volatile Memory Analyzer

Memory forensics is essential in cybersecurity and digital forensics, especially for fighting advanced threats and malware. In this dynamic environment, memory analysis tools and methods must be efficient. By prioritizing the prominent features in a memory, investigators can speed up their analysis. The VolMemLyzer (Volatile Memory Analyzer) can extract over 250 features from memory snapshots, speeding up analysis and enabling deeper explorations. It serves as a catalyst for memory forensics research and innovation.

The new VolMemLyzer V2.0 is a tool based on the functional programming paradigm with dependencies on updated Volatility3 Framework based on Python 3.

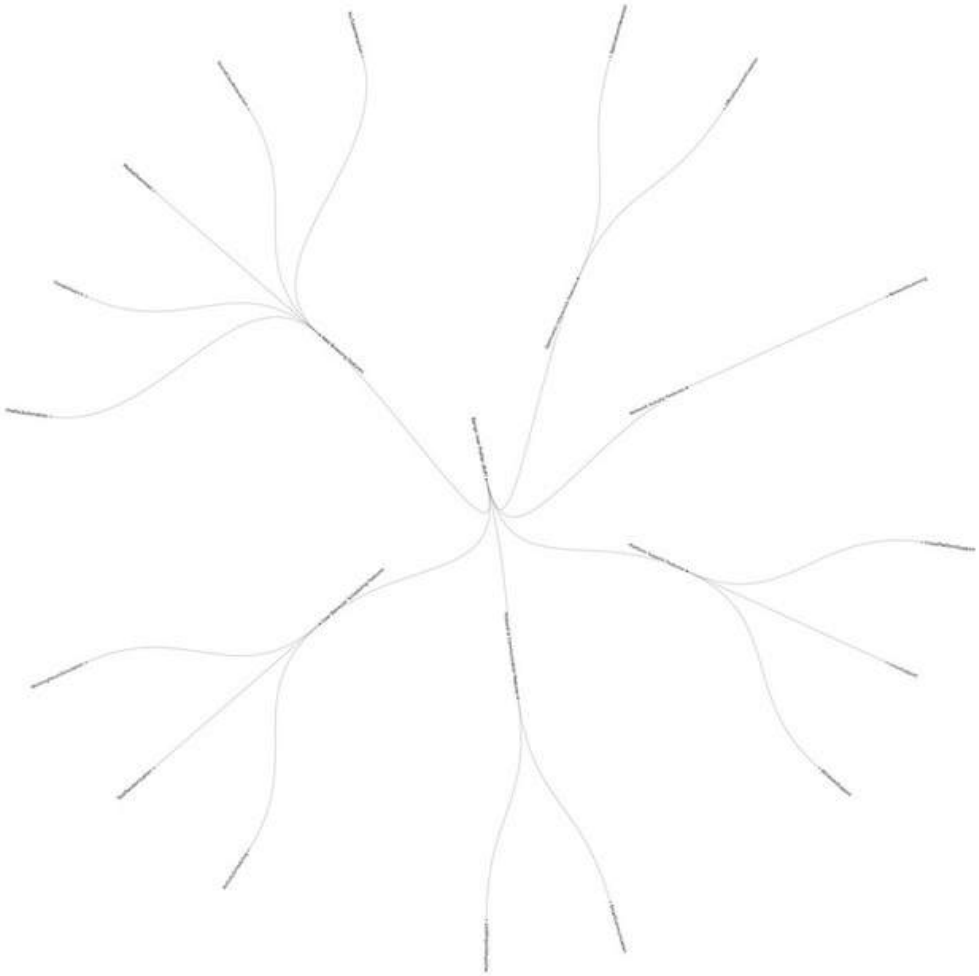


BUP V1.0

Benign User Profiler

Benign User Profiler (BUP), part of the UCS, is an open-source Python project designed to capture and model normal user behaviour across systems and networks. Instead of focusing only on malicious activity, BUP emphasizes benign actions, creating accurate baselines that improve the reliability of anomaly detection.

The framework extracts and analyzes behavioral features to build structured profiles of typical user activities. These profiles can be used to support machine learning models, enhance behavioral analytics, and reduce false positives, ultimately strengthening cybersecurity solutions with a clearer distinction between normal and abnormal behaviours.

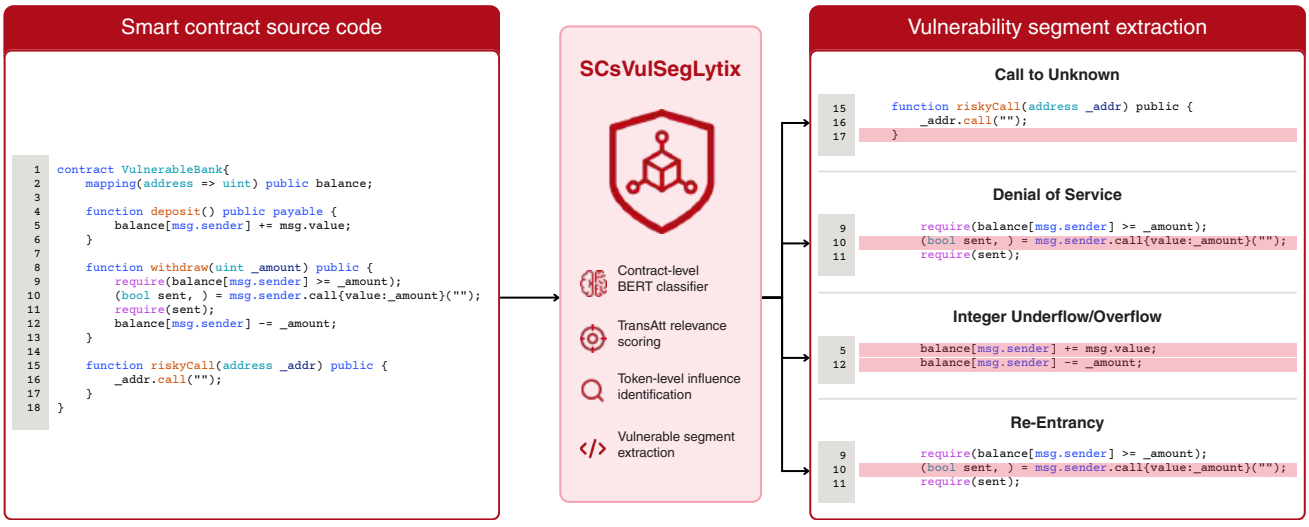


SCsVulSegLytix

Smart Contracts Vulnerable Segment Analytics

SCsVulSegLytix is an open-source smart contract vulnerability analysis framework designed to move beyond contract-level vulnerability detection to fine-grained identification of vulnerable source code segments. The framework first uses a BERT-based model to classify Solidity smart contracts and then applies TransAtt relevance scoring to identify influential tokens and statements associated with the detected vulnerability. Rather than extracting predefined statistical or source-code features, SCsVulSegLytix directly analyzes the contract source code to distinguish vulnerable segments from secure ones.

The framework currently supports four smart contract vulnerability categories: CallToUnknown, Denial of Service, Integer Under/Overflow, and Re-entrancy. By producing vulnerability-specific source code segments, SCsVulSegLytix provides researchers, developers, auditors, and security practitioners with more fine-grained information than contract-level classification alone, thereby supporting vulnerability analysis, model interpretation, and the development of more targeted smart contract security solutions.

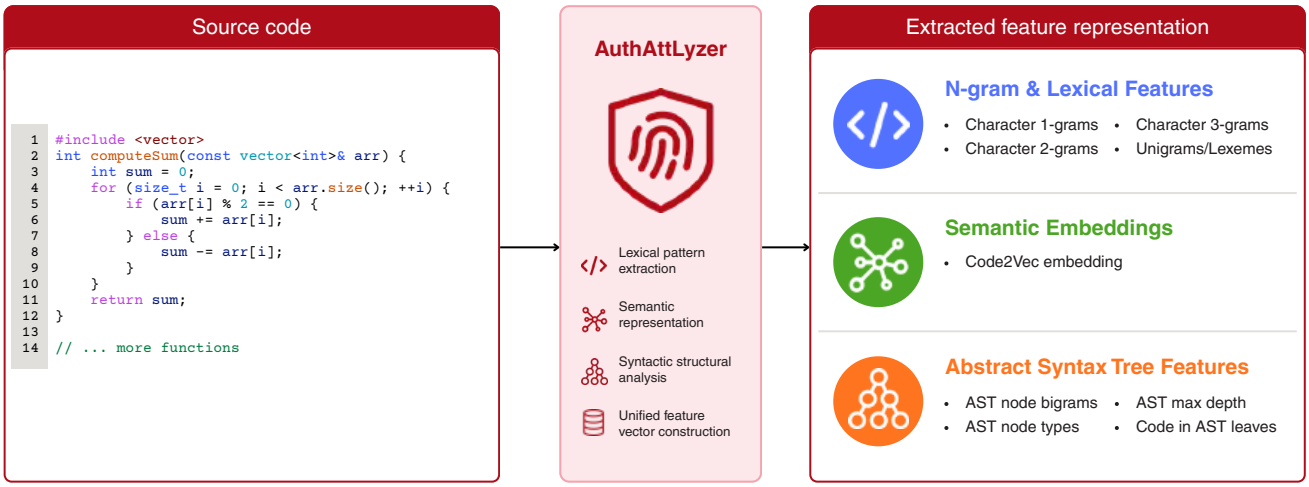


AuthAttLyzer

Authorship Attribution Analyzer

AuthAttLyzer is an open-source source-code analysis framework designed to support code authorship attribution by extracting multiple complementary representations of individual programming styles. Rather than relying on a single type of source-code characteristic, the analyzer captures lexical, semantic, and structural information through three feature categories: N-gram and lexical features, word-based embedding features, and Abstract Syntax Tree (AST)-based features. These representations capture characteristics ranging from character-level patterns and lexemes to Code2Vec embeddings and structural properties of source code.

By combining these complementary perspectives on features, AuthAttLyzer provides a rich representation of coding patterns that can support authorship attribution and related source-code analysis research. The extracted features include character N-grams, unigrams/lexemes, Code2Vec embeddings, AST node bigrams, AST node types, AST maximum depth, and code contained in AST leaves. These representations can be used by researchers and cybersecurity practitioners to investigate source-code authorship and behavioral coding patterns and to support applications in software forensics and cybersecurity research.

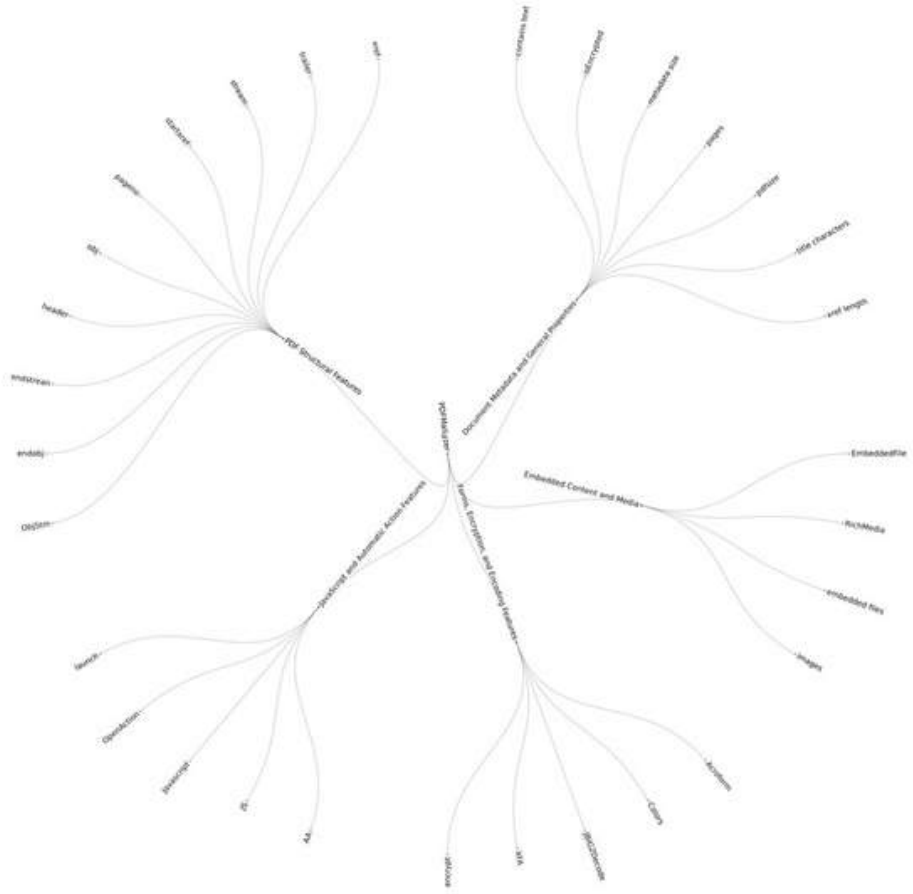


PDFMalLyzer

Malicious PDF Analyzer

PDFMalLyzer is an open-source PDF analysis tool designed to extract general and structural characteristics from PDF files for cybersecurity analysis. The tool processes collections of PDF documents and extracts 31 features, exporting the results to structured CSV files. Its feature extraction combines the PyMuPDF (fitz) library with the open-source PDFiD tool, enabling systematic characterization of PDF structure and content-related properties to distinguish normal and potentially malicious documents.

The structured feature representation generated by PDFMalLyzer supports malicious PDF detection, document profiling, malware analysis, and machine-learning-based classification. By transforming PDF files into compact tabular representations, the tool enables researchers and cybersecurity practitioners to develop and evaluate learning-based approaches to identify malicious PDF documents and investigate behavioral and structural indicators associated with PDF-based threats.

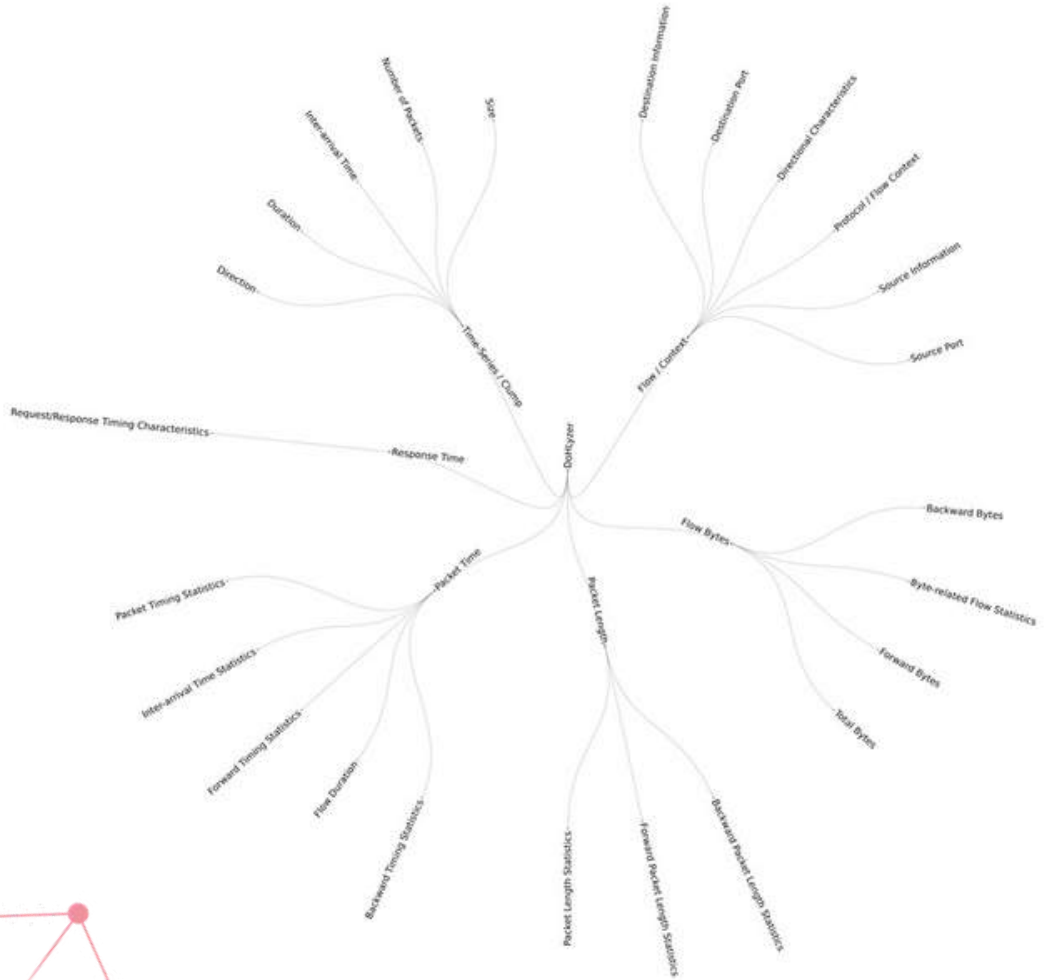


DoHLyzer

DNS over HTTPS Analyzer

DoHLyzer is an open-source traffic analysis framework designed to extract and characterize features from DNS over HTTPS (DoH) network traffic. By analyzing encrypted HTTPS flows, the analyzer generates statistical and behavioral representations across multiple feature categories, including flow bytes, packet lengths, packet timing, response timing, and flow context. These features capture both forward and backward communication characteristics, enabling detailed profiling of DoH traffic without relying on the visibility of traditional plaintext DNS communications.

In addition to statistical flow features, DoHLyzer provides a time-series representation based on traffic clumps characterized by inter-arrival time, duration, size, number of packets, and direction. Combining statistical and sequential traffic characteristics provides researchers and cybersecurity practitioners with complementary perspectives for profiling encrypted DNS behavior and developing machine-learning-based approaches to distinguish benign from malicious DoH traffic. DoHLyzer therefore supports research in encrypted traffic analysis, behavioral profiling, anomaly detection, and DoH-based threat detection.



Dataset Series

Trusted resources for research, training, evaluation, and innovation

01 BCCC-IoT-IDS-ZWave-2025
02 BCCC-UDP-QUIC-IDS-2025
03 BCCC-DeFiFraudTrans-2025
04 BCCC-IoT-MQTT-IDS-2025
05 BCCC-DarkNet-2025
06 BCCC-Mal-NetMem-2025
07 BCCC-MalMem-SnapLog-2025
08 BCCC-SCsVuls-2024
09 BCCC-Aposemat-IoT-BoT-2024
10 CIC-BCCC-NRCTabularIoTAttack-2024
11 BCCC-cPacket-Cloud-DDoS-2024
12 BCCC-CIC-Bell-DNS-2024
13 BCCC-VulSCs-2023
14 BCCC-SFU-SQLInj-2023
15 YU-SCAA-2022
16 BCCC-CIRA-CIC-DoHBrw-2020
17 BCCC-CSE-CIC-IDS2018
18 BCCC-CIC-IDS2017

BCCC-IoT-IDS-ZWave-2025

IoT ZWave Intrusion Detection Network Traffic Dataset

The BCCC-IoT-IDS-Zwave-2025 dataset is a large-scale, multi-source IoT intrusion detection dataset developed at BCCC, York University. It was created over five months using a realistic smart home testbed with more than 50 IoT devices and 88 distinct attack scenarios, capturing both IP-based and Z-Wave protocol communications, a first of its kind to integrate these layers in a unified dataset. The dataset encompasses multi-modal data sources including Z-Wave traffic, IP network traffic, MQTT logs, and device activity records, providing a comprehensive view of smart home behavior under benign and malicious conditions.

To enable deep protocol-aware analysis, the research team designed IoT-ZwaveNetLyzer, the first dedicated Z-Wave traffic analyzer capable of extracting over 400 features from network flows. The dataset is publicly available through BCCC's GitHub repository and serves as a benchmark for researchers focusing on device profiling, anomaly detection, and multi-protocol IoT threat analysis. By combining realistic smart home traffic with extensive attack scenarios and diverse communication protocols, the BCCC-IoT-IDS-Zwave-2025 dataset represents a major advancement in cybersecurity dataset creation and supports the development of next generation IoT intrusion detection systems.

<table>
<tr><th colspan="5">BCCC-IoT-IDS-ZWave-2025</th></tr>
<tr><td colspan="5">IP traffic (PCAP) → NTLFlowLyzer → 350 features (CSV)
Z-Wave Zniffer raw packets (CSV) → IoT-ZwaveNetLyzer → 340 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="4">IoT smart home / IP, Z-Wave, MQTT, WebSocket, HTTP/S</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Benign</td><td colspan="2">220,424</td></tr>
<tr><td colspan="2">Malicious</td><td colspan="2">16,235,416</td></tr>
<tr><td rowspan="6">Label distributions</td><td>Benign</td><td>220,424</td><td>TCP-Slowloris-hping3</td><td>1,120,514</td></tr>
<tr><td>BYPASS-MHDDoS</td><td>2,420,346</td><td>SYN-Flood-Simple</td><td>918,309</td></tr>
<tr><td>SYN-PSH-hping3</td><td>2,298,274</td><td>ACK-Flood-hping3</td><td>820,000</td></tr>
<tr><td>ACK-Flood-simple</td><td>2,044,057</td><td>SYN-PSH-URG-hping3</td><td>780,000</td></tr>
<tr><td>SYN-Flood-MHDDoS</td><td>1,842,819</td><td>+21 Attacks</td><td>4,189,897</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="4">350 IP features
340 ZWave features</td></tr>
</table>

BCCC-UDP-QUIC-IDS-2025

UDP-QUIC Network Threat Dataset

The BCCC-UDP-QUIC-IDS dataset provides a realistic cloud-based benchmark for intrusion detection research involving UDP and QUIC traffic, with particular emphasis on volumetric and application-specific UDP DDoS attacks in enterprise environments. Generated using UDPFlowLyzer and QUICFlowLyzer, it combines realistic benign organizational activities with multiple attack campaigns executed across a multi-tier cloud infrastructure. The dataset contains more than 1.29 million bidirectional flows, including 826,953 UDP and 470,926 QUIC flows, characterized by over 442 temporal, statistical, directional, and protocol-aware features.

It covers benign, suspicious, and multi-class attack traffic involving VSE, OVH, HULK, MULTI, RAW, GAME, and bypass variants. The dataset further incorporates auditable labeling, timestamp normalization, deterministic flow generation, realistic benign user profiling through BUP, and reproducible CSV generation from raw PCAP traces, supporting robust intrusion detection and low-FPR evaluation.

BCCC-UDP-QUIC-IDS-2025			
PCAP → **UDPFlowLyzer + QUICFlowLyzer** → 442+ features (CSV)			
Platform / Protocol	UDP and QUIC		
Total samples	UDP flows	826,953	
	QUIC flows	470,926	
Label distributions		UDP	QUIC
	Benign	47,060	15,131
	Attack	780,586	456,566
	UDP-RAW	776,472	453,982
	Suspicious	1,113	216
	UDP-MULTI, VSE, OVH, HULK, GAME, ByPass	1,615	826
Number of extracted features in CSVs	442+		

BCCC-DeFiFraudTrans-2025

Decentralized Finance Fraud Transactions Dataset

BCCC-DeFiFraudTrans-2025 is a large-scale, Ethereum-based benchmark designed explicitly for profiling fraudulent and legitimate DeFi transactions. It contains 1,026,867 annotated transaction samples spanning from 2017 to 2024, drawn from 9,374 unique wallet addresses. The dataset integrates both wallet-level and transaction-level attributes, with 79 features extracted via the DeFiTransLyzer-V1.0 analyzer. These features are organized into categories, including gas usage, cumulative gas consumption, token transfers, nonce behaviour, block identifiers, transaction status, and error rates, providing a fine-grained view of transaction dynamics.

Unlike many prior datasets, BCCC-FraudDefi-2025 was curated to be balanced, feature-rich, and validated: fraudulent labels were assigned based on Etherscan tags and then cross-checked with anomaly detection, consistency verification, and duplicate removal. The dataset enables evaluation of advanced fraud detection methods, including zero-day attacks, by eliminating reliance on prior wallet history and focusing purely on transaction-level behavior.

<table>
<tr><th colspan="4">BCCC-DeFiFraudTrans-2025</th></tr>
<tr><td colspan="4">Transaction / Wallets (JSON) → DeFiTransLyzer → 89 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="3">Ethereum</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Transactions</td><td>1,026,867</td></tr>
<tr><td colspan="2">Wallet addresses</td><td>9,374</td></tr>
<tr><td rowspan="3">Label distributions</td><td></td><td>Transactions</td><td>Wallet addresses</td></tr>
<tr><td>Legitimate</td><td>938,074</td><td>7,611</td></tr>
<tr><td>Fraud</td><td>88,793</td><td>1,763</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="3">89</td></tr>
</table>

BCCC-IoT-MQTT-IDS-2025

IoT Message Queuing Telemetry Transport (MQTT) Intrusion Dataset

BCCC-IoT-MQTT-IDS-2025 is an augmented IoT intrusion detection dataset designed to provide a comprehensive benchmark for analyzing MQTT-based network behavior and cyber threats. The dataset integrates three established sources, MQTTSet, DDoS-IoT-2023, and IoT-IDS-2020, bringing together diverse benign and malicious MQTT communication patterns and attack scenarios within a unified dataset. Using MQTTFlowLyzer, network traffic is transformed into bidirectional flows characterized by 404 statistical, temporal, directional, and MQTT protocol-aware features.

By combining multiple datasets and standardizing their traffic representation, BCCC-IoT-MQTT-IDS-2025 provides greater diversity than relying on a single MQTT environment or attack collection. It supports research on IoT intrusion detection, MQTT attack classification, behavioral profiling, machine-learning-based threat detection, and model generalization, providing researchers with a structured benchmark for developing and evaluating cybersecurity solutions for MQTT-enabled IoT environments.

<table>
<tr><th colspan="6">BCCC-IoT-MQTT-IDS-2025</th></tr>
<tr><td colspan="6">MQTT traffic (PCAP) → MQTTFlowLyzer → 404 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="5">Internet of Things (IoT) / MQTT</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Benign</td><td colspan="3">12,883,421</td></tr>
<tr><td colspan="2">Malicious</td><td colspan="3">36,013,669</td></tr>
<tr><td rowspan="6">Label distributions</td><td>Benign</td><td>12,883,421</td><td>Brute force</td><td>1,033,773</td></tr>
<tr><td>Invalid Subscription Flooding</td><td>17,254,716</td><td>MalariaDoS</td><td>188,957</td></tr>
<tr><td>Basic Connect Flooding</td><td>5,947,010</td><td>Sparta</td><td>71,585</td></tr>
<tr><td>Connect Flooding with WILL payload</td><td>3,189,028</td><td>Scan_A</td><td>21,258</td></tr>
<tr><td>Delayed Connect Flooding</td><td>2,444,376</td><td>Malformed</td><td>2,925</td></tr>
<tr><td>SYN TCP Flooding</td><td>1,833,565</td><td>Slowite</td><td>1,024</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="5">404</td></tr>
</table>

BCCC-DarkNet-2025

Encrypted Traffic Dataset

BCCC-DarkNet-2025 is an augmented, research-driven dataset that supports encrypted traffic analysis and threat detection across anonymized communication networks. It integrates and extends two benchmark datasets, CIC-Darknet2020 and Darknet-Dataset-2020, selected for their robust coverage of encryption protocols and darknet-specific traffic behaviors. The dataset includes diverse encrypted traffic types like VPN, Tor, I2P, Freenet, and ZeroNet, with multi-class labeling and protocol-specific annotations. These sources were chosen based on well-defined criteria, including support for time-dependent patterns, entropy measures, and behavioral features critical to identifying obfuscated malicious activities.

The dataset has been standardized to ensure consistency and scalability using NTLFlowLyzer V3.0, a custom flow-based feature extractor. This preprocessing step harmonizes temporal, statistical, and protocol-level features across both datasets, enabling seamless integration into machine learning pipelines. The result is BCCC-DarkNet-2025, a unified and enriched dataset that significantly improves classifier performance in encrypted traffic scenarios by capturing structural and behavioral anomalies. It is a valuable resource for developing AI-powered cybersecurity solutions in dynamic and evasive threat environments.

BCCC-DarkNet-2025		
Encrypted Traffic (PCAP) → **NTLFlowLyzer** → 475 features (CSV)		
Platform / Protocol	Zeronet, I2P, VPN, ToR, FREENET	
Total Samples	Non-encrypted	18,570
	Encrypted	6,968
Encrypted Samples	ZERONET	2,327
	I2P	2,099
	VPN	2,081
	TOR	1,258
	FREENET	156
Number of extracted features in CSVs	475	

BCCC-Mal-NetMem-2025

Large-Scale Multisource Malware Analysis Dataset Using Network Traffic and Memory

The BCCC-Mal-NetMem-2025 dataset is a multi-source behavioral malware analysis dataset that captures malicious activity from two complementary perspectives: volatile memory and network communication. Rather than relying on a single observation source, it provides memory-dump characteristics alongside network-flow behavior for benign executions and multiple malware families, enabling researchers to investigate how malicious activity manifests both within an infected system and through its external communications.

By preserving memory and network data as distinct yet complementary sources of behavioral evidence, the dataset enables cross-source malware analysis and supports the development and evaluation of AI-driven approaches for malware detection, family classification, behavioral profiling, and multi-source intelligence. This combination provides researchers with a richer view of malware execution and communication behavior, helping advance malware analysis beyond single-source and purely static representations.

<table>
<tr><th colspan="4">BCCC-Mal-NetMem-2025</th></tr>
<tr><td colspan="4">TCP/IP traffic (PCAP) → NTLFlowLyzer → 85 features (CSV)
Memory snapshot (VMEM) → VolMemLyzer → 252 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="3">TCP/IP and VMem</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Network Flows</td><td>2,552,621</td></tr>
<tr><td colspan="2">Memory Snapshots</td><td>2,057</td></tr>
<tr><td rowspan="3">Label distributions</td><td></td><td>Network</td><td>Memory</td></tr>
<tr><td>Benign</td><td>2,533,761</td><td>135</td></tr>
<tr><td>Malicious (8 attacks)</td><td>18,860</td><td>1,922</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="3">85 Network features
252 Memory features</td></tr>
</table>

BCCC-MalMem-SnapLog-2025

Malware Memory Snapshot and Process-Level Log Dataset

BCCC-MalMem-SnapLog-2025 is a large-scale malware analysis dataset designed to capture runtime memory behavior and process-level dynamics over time. Developed in a controlled execution environment, the dataset combines interval-based memory snapshots and process-level behavioral logs from 2,000 malware and 250 benign samples, representing eight malware categories: Backdoor, Hoax, HackTool, Trojan, Worm, Virus, Rootkit, and Exploit. With approximately 40 TB of memory snapshots and associated behavioral records, the dataset captures memory and process characteristics across multiple execution intervals, enabling observation of both transient and persistent system behaviors.

A distinguishing characteristic of the dataset is its temporal memory-based representation, which tracks process persistence and behavioral transitions across successive memory snapshots rather than analyzing individual memory dumps in isolation. Processes can therefore be characterized according to single, repeated, or timeout-based appearances across snapshots, providing a fine-grained representation of runtime evolution. By integrating memory snapshots with behavioral logs and cross-snapshot relationships, this approach supports malware profiling and detection approaches that exploit temporal evolution, contextual behavior, process persistence, and cross-snapshot correlations.

BCCC-MalMem-SnapLog-2025								
Memory snapshots (VMEM) + Windows event logs (EVTX)								
Platform / Protocol	VMem, Windows							
Total samples	Benign				1,125 VMem, 916 EVTX			
	Malicious				9,245 VMem, 7,679 EVTX			
Label distributions		VMem	1-snap	5-snap		VMem	1-snap	5-snap
	Exploit	1,250	0	250	Worm	1,186	16	234
	Backdoor	1,234	4	246	hoax	1,100	39	209
	Virus	1,210	10	240	Rootkit	1,098	38	212
	Trojan	1,198	13	237	Hacktool	969	69	180

BCCC-SCsVuls-2024

Smart Contracts Vulnerabilities Dataset

BCCC-SCsVuls-2024 is a large-scale dataset designed for analyzing and detecting vulnerabilities in Solidity-based smart contracts. It contains 111,897 labeled samples covering 11 major vulnerability types, including Re-entrancy (17,698), IntegerUO (16,740), Denial of Service (12,394), and 26,914 Secure contracts. Curated from trusted sources such as Smart Bugs, Ethereum SCs, and SmartScan-Dataset, it offers a diverse and representative collection to support blockchain security research.

BCCC-SCsVuls-2024		
Smart Contract Source code (Solidity) → **SCsVulLyzer V2.0** → 240 features (CSV)		
Platform	Ethereum	
Total samples	Solidity source code	111,897
Label distributions	Secure	26,914
	External bug	3,604
	Gas exception	6,879
	Mishandled exception	5,154
	Timestamp	2,674
	Transaction order dependence	3,562
	Unused return	3,229
	Weak access mod	1,918
	Call to unknown	11,131
	Denial of service	12,394
	Integer underflow/overflow	16,740
	Re-entrancy	17,698
Number of extracted features in CSVs	240	

BCCC-Aposemat-IoT-BoT-2024

IoT Botnet Intrusion Dataset

This dataset is a large-scale IoT botnet intrusion detection dataset developed by augmenting and refining the Aposemat-Bot-IoT-23 dataset to improve class balance, labeling consistency, and the representation of behavioral features. It contains TCP/IP network traffic reconstructed into bidirectional flows and represents multiple botnet families, including Mirai, Gagfyt, IRCBot, Kenjiro, Torii, Linux Mira, and Okiru, as well as benign traffic. The dataset includes more than 235 million malicious bot records, with 315 network- and transport-layer features extracted using NTLFlowLyzer to characterize packet-level, statistical, temporal, and bidirectional traffic behaviors.

The dataset employs a precise labeling process that aligns reconstructed flow records with Zeek-generated logs using IP-port matching, enabling reliable binary and multi-class annotations. To improve data quality and manage the substantial scale and class imbalance, ambiguous suspicious samples are removed, while cluster-based undersampling (CBUS), normalization, and proportional sampling are applied to preserve representative traffic characteristics and computational feasibility. The resulting dataset provides a scalable, behavior-centric resource for developing and evaluating AI- and LLM-based intrusion detection systems against diverse IoT botnet threats.

<table>
<tr><th colspan="5">BCCC-Aposemat-IoT-BoT-2024</th></tr>
<tr><td colspan="5">Network traffic (PCAP) → NTLFlowLyzer → 315 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="4">TCP/IP</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Benign</td><td colspan="2">24,528,833</td></tr>
<tr><td colspan="2">Malicious</td><td colspan="2">235,808,130</td></tr>
<tr><td rowspan="5">Label distributions</td><td>Benign</td><td>24,528,833</td><td>Okiro</td><td>13,634,438</td></tr>
<tr><td>Mirai</td><td>77,900,176</td><td>Linux, Mirai</td><td>11,337,694</td></tr>
<tr><td>IRCBot</td><td>73,561,853</td><td>Gagfyt</td><td>3,578,485</td></tr>
<tr><td>Kenjiro</td><td>55,795,484</td><td></td><td></td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="4">315</td></tr>
</table>

CIC-BCCC-NRC TabularIoTAttack-2024

Tabular IoT Attacks Dataset

The CIC-BCCC-NRC TabularIoTAttack-2024 dataset is a large-scale IoT cybersecurity benchmark developed to support the training and evaluation of AI-based intrusion detection and attack classification models. It provides diverse, labeled IoT network traffic representing 70 attack types across 10 major attack groups, including Flood, DDoS, DoS, Brute Force, MQTT, Reconnaissance/Scanning, Web/Injection, Malware, Man-in-the-Middle (MITM), and Mirai attacks. Network traffic is represented in tabular form using features extracted with CICFlowMeter, capturing flow-level characteristics together with information such as timestamps, source and destination addresses, and attack labels.

The dataset contains more than 20 million attack records, providing substantial diversity in both attack behavior and class prevalence. Its hierarchical organization enables cybersecurity models to be evaluated at different levels of granularity, from broader attack-group identification to more detailed attack-type classification. The combination of large-scale traffic, diverse IoT attack scenarios, and structured flow-level representations makes the dataset suitable for research on IoT intrusion detection, multi-class attack classification, behavioral profiling, model generalization, and AI-based cybersecurity analytics.

CIC-BCCC-NRC TabularIoTAttack-2024				
Network Traffic (PCAP) → **CICFlowLyzer** → 86 features (CSV)				
Platform / Protocol	TCP/IP			
Total samples	Benign		2,357,186	
	Malicious (48 attacks)		20,503,263	
Label distributions	Flood (19 types)	15,063,504	Recon / Scan (12 types)	1,252,474
	DDoS (9 types)	8,179,338	Web / injection (3 types)	726,129
	DoS (7 types)	2,568,939	Malware (2 types)	573,860
	Brute force (6 types)	2,340,415	MITM (2 types)	127,406
	MQTT (5 types)	1,671,060	Mirai (5 types)	26,691
Number of extracted features in CSVs	86			

BCCC-cPacket-Cloud-DDoS-2024

Cloud-Based Distributed Denial of Service (DDoS) Dataset

The BCCC-cPacket-Cloud-DDoS-2024 dataset is a large-scale cloud-based network security benchmark developed after analyzing 16 publicly available DDoS datasets and addressing limitations identified in existing resources. Created within a realistic cloud infrastructure, it captures more than eight benign user activities and 17 DDoS attack scenarios and is fully annotated with 26 labels. Using NTLFlowLyzer, more than 300 network- and transport-layer features are extracted from bidirectional traffic flows to characterize statistical, temporal, directional, and behavioral network patterns. The dataset supports research on benign user profiling, DDoS detection, attack classification, behavioral analysis, and learning-based cybersecurity modeling, providing a comprehensive resource for developing and evaluating robust DDoS detection and mitigation approaches in cloud environments.

<table>
<tr><th colspan="5">BCCC-cPacket-Cloud-DDoS-2024</th></tr>
<tr><td colspan="5">Network Traffic (PCAP) → NTLFlowLyzer → 324 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="4">TCP/IP</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Benign (8 types across 6 families)</td><td colspan="2">413,199</td></tr>
<tr><td colspan="2">Attacks (17 types across 6 families)</td><td colspan="2">228,469</td></tr>
<tr><td rowspan="7">Label distributions</td><td colspan="2">Benign</td><td colspan="2">Malicious</td></tr>
<tr><td>Generic</td><td>302,284</td><td>TCP Bypass
(TCP-BYPass-V1)</td><td>138,368</td></tr>
<tr><td>Web browsing</td><td>51,272</td><td>TCP Flag
(10 TCP-Flag-* types)</td><td>49,823</td></tr>
<tr><td>Systemic</td><td>48,074</td><td>TCP SYN
(TCP-Valid-SYN, TCP-SYN)</td><td>14,996</td></tr>
<tr><td>Remote access
(Telnet, SSH)</td><td>7,753</td><td>Killer
(Killer-TCP, Killall-v2)</td><td>12,287</td></tr>
<tr><td>Email
(Send, Receive)</td><td>3,333</td><td>TCP IGMP</td><td>7,251</td></tr>
<tr><td>FTP</td><td>483</td><td>TCP Control</td><td>5,744</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="4">324</td></tr>
</table>

BCCC-CIC-Bell-DNS-2024

Malicious DNS and Attacks Dataset

The BCCC-CIC-Bell-DNS-2024 dataset is an augmented DNS security dataset developed from two existing datasets, CIC-Bell-DNS-2021 and CIC-Bell-DNS-EXF-2021, to provide a richer benchmark for analyzing DNS-based data exfiltration. Using ALFlowLyzer, raw network traffic is reconstructed into flows and transformed into structured CSV files containing DNS metadata and application-layer features, enabling detailed characterization of DNS communication behaviors under benign and malicious conditions.

The dataset integrates both light and heavy data exfiltration traffic and organizes the resulting traffic into six distinct subcategories, providing greater diversity for studying different patterns of DNS-based information leakage. Its application-layer representation supports research on DNS traffic profiling, data exfiltration detection, attack classification, anomaly detection, and AI-based cybersecurity modeling, providing a structured resource for developing and evaluating behavioral approaches to identifying malicious DNS activities.

BCCC-CIC-Bell-DNS-2024		
Application Layer Traffic (PCAP) → **ALFlowLyzer** → 113 features (CSV)		
Platform / Protocol	DNS	
Total samples	Benign	102,720
	Malicious	3,595,920
Label distributions	Benign	102,720
	Spam	3,470,874
	Malware	81,698
	Phishing	43,348
Number of extracted features in CSVs	113	

BCCC-VulSCs-2023

Vulnerable Smart Contracts - 2023

The BCCC-VulSCs-2023 dataset is a benchmark developed to support the analysis and detection of vulnerabilities in Solidity-based smart contracts. It contains 36,670 smart contract samples, each represented through 70 feature columns, including the raw smart contract source code, a hashed representation of the source code for secure referencing, and a binary label identifying each contract as secure (0) or vulnerable (1). This structured representation provides a substantial resource for examining the behavioral and structural characteristics of vulnerable smart contracts.

The dataset was developed in conjunction with research on profiling vulnerable smart contracts using a genetic-algorithm-based approach, providing data suitable for learning-based smart contract security analysis. Its combination of source-code information, derived attributes, and vulnerability labels supports research on vulnerability detection, smart contract profiling, security classification, pattern identification, and machine-learning-based blockchain security, thereby enabling the development and evaluation of models to distinguish secure from vulnerable smart contracts.

BCCC-VulSCs-2023		
Smart contract source code (Solidity) → **SCsVulLyzer V1.0** → 70 features (CSV)		
Platform / Protocol	Ethereum	
Total samples	Secure	26,914
	Vulnerable	9,756
Number of extracted features in CSVs	70	

BCCC-SFU-SQLInj-2023

Malicious SQL Dataset

The BCCC-SFU-SQLInj-2023 dataset is a specialized cybersecurity dataset developed to support the analysis and detection of SQL injection attacks. It contains 11,011 malicious SQL query records, providing a focused collection of attack-oriented queries for examining the patterns and structures used to manipulate database operations and exploit vulnerable applications. The dataset offers a structured resource for investigating SQL injection behavior at the query level.

By concentrating specifically on malicious SQL queries, the dataset supports research on SQL injection detection, malicious query analysis, application security, and AI-based attack detection. It can be used to develop and evaluate learning-based approaches for recognizing malicious query patterns and strengthening the protection of database-driven applications against SQL injection attacks.

BCCC-SFU-SQLInj-2023		
Malicious SQL Queries (CSV) → **Genetic Algorithm** → 2 (CSV)		
Platform / Protocol	Database Query	
Total samples	Attacks	11,000
Number of extracted features in CSVs	2 (Index and Payload)	

YU-SCAA-2022

Source Code Authorship Attribution Dataset

The YU-SCAA-2022 dataset was developed to support research on identifying source code authors based on individual programming characteristics. Source Code Authorship Attribution (SCAA) has applications in software forensics, including identifying the authors of malicious applications, detecting ghostwriting, resolving copyright disputes, and other source-code analysis tasks. The dataset was constructed by extracting source-code samples from the Google Code Jam (GCJ) and GitHub datasets and contains 1,632 code files from 204 authors.

The dataset also includes attack samples and adversarial examples generated with the Source Code Imitator, enabling researchers to investigate the robustness of authorship attribution approaches to adversarial manipulation. It was developed in association with the AuthAttLyzer research framework and provides a benchmark for evaluating source-code authorship attribution, adversarial robustness, software forensics, and learning-based source-code analysis.

YU-SCAA-2022		
GCJ & GitHub Source Code (Code Files) → **Source Code Imitator** → 23 features (CSV)		
Platform / Protocol	Source Code	
Total samples	Source files	1632
Number of extracted features in CSVs	23	

BCCC-CIRA-CIC-DoHBrw-2020

Balanced DNS-over-HTTPS (DoH) Dataset

The BCCC-CIRA-CIC-DoHBrw-2020 dataset was created to address the imbalance in the CIRA-CIC-DoHBrw-2020 dataset. Unlike the CIRA-CIC-DoHBrw-2020 dataset, which is skewed with about 90% malicious and only 10% benign Domain over HTTPS (DoH) network traffic, the BCCC-CIRA-CIC-DoHBrw-2020 dataset offers a more balanced composition. It includes equal numbers of malicious and benign DoH network traffic instances, with 249,836 instances in each category. This balance was achieved using the Synthetic Minority Over-sampling Technique (SMOTE). The BCCC-CIRA-CIC-DoHBrw-2020 dataset comprises three CSV files: one for malicious DoH traffic, one for benign DoH traffic, and a third that combines both types.

BCCC-CIRA-CIC-DoHBrw-2020		
Network traffic (PCAP) → **DoHLyzer + SMOTE** → 28 features (CSV)		
Platform / Protocol	DNS-over-HTTP (DoH)	
Total samples	Benign	249,836
	Malicious	249,836
Number of extracted features in CSVs	28	

BCCC-CSE-CIC-IDS2018

Large-Scale Intrusion Detection Dataset

The BCCC-CSE-CIC-IDS2018 dataset is an enhanced version of CSE-CIC-IDS2018 with 46 million labelled records and 300 features, addressing key issues to improve data quality and reliability for behavioural profiling in IDS research. Labeling inconsistencies, particularly for DoS attacks, were corrected by aligning attack labels with attacker IPs instead of timestamps. NTLFlowLyzer, a new network traffic analyzer, was developed to resolve anomalies in extracted features and refine feature implementation.

Additionally, protocol issues were fixed by removing UDP-based attacks previously misclassified due to TCP-specific analysis. Attacks with insufficient flow counts were retained but excluded from analysis and profiling. The dataset now includes an expanded feature set to detect evolving cyber threats better, making it a robust benchmark for AI-driven IDS/IPS research.

<table>
<tr><th colspan="5">BCCC-CSE-CIC-IDS2018</th></tr>
<tr><td colspan="5">Network traffic (PCAP) → NTLFlowLyzer → 300 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="4">TCP/IP</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Benign</td><td colspan="2">40,000,000+</td></tr>
<tr><td colspan="2">Malicious</td><td colspan="2">5,089,770</td></tr>
<tr><td rowspan="5">Label distributions</td><td>Benign</td><td>40,000,000+</td><td>GoldenEye</td><td>29,485</td></tr>
<tr><td>Bot</td><td>286,099</td><td>SlowHTTP</td><td>289,527</td></tr>
<tr><td>DoS HULK</td><td>1,824,450</td><td>Slowloris</td><td>8,269</td></tr>
<tr><td>DDoS HOIC</td><td>2,164,586</td><td>Brute FTP</td><td>193,360</td></tr>
<tr><td>DDoS LOIC</td><td>105,550</td><td>Brute SSH</td><td>188,444</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="4">300</td></tr>
</table>

BCCC-CIC-IDS2017

Intrusion Detection Dataset

Using NLFlowLyzer, we successfully generated the BCCC-CIC-IDS2017 dataset by extracting key flows from raw network traffic data of CIC-IDS2017, resulting in CSV files integrating essential network and transport layer features. This new dataset offers a structured approach for analyzing intrusion detection, combining diverse traffic types into multiple sub-categories. The BCCC-CIC-IDS2017 dataset enriches the depth and variety needed to rigorously evaluate our proposed profiling model, advancing research in network security and enhancing the development of intrusion detection systems.

<table>
<tr><th colspan="5">BCCC-CIC-IDS2017</th></tr>
<tr><td colspan="5">Network traffic (PCAP) → NTLFlowLyzer → 114 features (CSV)</td></tr>
<tr><td>Platform / Protocol</td><td colspan="4">TCP/IP</td></tr>
<tr><td rowspan="2">Total samples</td><td colspan="2">Benign</td><td colspan="2">1,786,239</td></tr>
<tr><td colspan="2">Malicious</td><td colspan="2">651,813</td></tr>
<tr><td rowspan="3">Label distributions</td><td>Benign</td><td>1,786,239</td><td>Botnet
(ARES)</td><td>5,508</td></tr>
<tr><td>DoS
(GoldenEye, Hulk, LOIT, SlowHTTP, Slowloris)</td><td>465,374</td><td>Port scan</td><td>161,323</td></tr>
<tr><td>Brute force
(FTP Patator, SSH Patator, Web)</td><td>18,214</td><td>Vulnerability exploit
(SQL injection, Web XSS, Heartbleed)</td><td>1,394</td></tr>
<tr><td>Number of extracted features in CSVs</td><td colspan="4">114</td></tr>
</table>

Book Series

Essential reads for every cybersecurity enthusiast

01 Understanding Cybersecurity for Smart Contracts
02 Understanding Cybercrime Victim Services
03 Understanding Cybersecurity Management in the Construction Industry
04 Understanding AI in Cybersecurity and Secure AI
05 Understanding Cybersecurity Management in Healthcare
06 Understanding Cybersecurity on Smartphones
07 Understanding Cybersecurity Management in FinTech
08 Understanding Cybersecurity Law and Digital Privacy
09 Understanding Cybersecurity Management in Decentralized Finance
10 Understanding Cybersecurity Law in Data Sovereignty and Digital Governance

Understanding Cybersecurity for Smart Contracts

Challenges, Strategies, and Trends

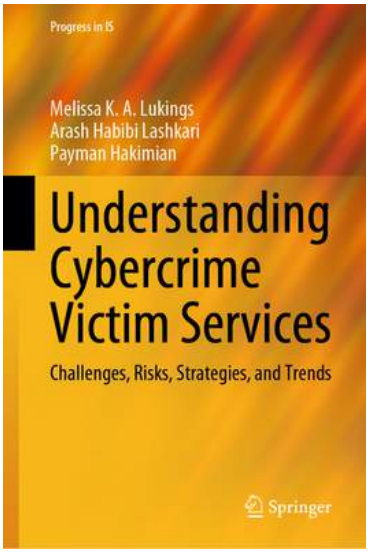
This book provides a comprehensive introduction to the cybersecurity of smart contracts, covering blockchain fundamentals, smart contract design, programming languages, vulnerabilities, threats, attacks, analysis tools, countermeasures, and future research directions. It adopts a cybersecurity-centered perspective by systematically connecting vulnerabilities to real-world threats, attacks, detection techniques, and defensive strategies while combining theoretical concepts with practical Solidity examples, case studies, and comparative analyses.

A major strength of the book is its structured progression from foundational concepts to advanced security topics. It introduces blockchain architectures, smart contract platforms, secure development practices, vulnerability taxonomies, attack analyses, auditing tools, and mitigation techniques in a coherent manner, supported by code examples, real-world incidents, and visual illustrations that enhance both learning and practical application.

Overall, the book serves as a valuable resource for students, researchers, developers, auditors, and cybersecurity professionals by integrating current research, industry practices, and educational content into a single reference. Its broad coverage of smart contract security, together with practical guidance and emerging research directions, makes it a strong contribution to cybersecurity education and professional practice.

Understanding Cybercrime Victim Services

Challenges, Risks, Strategies, and Trends



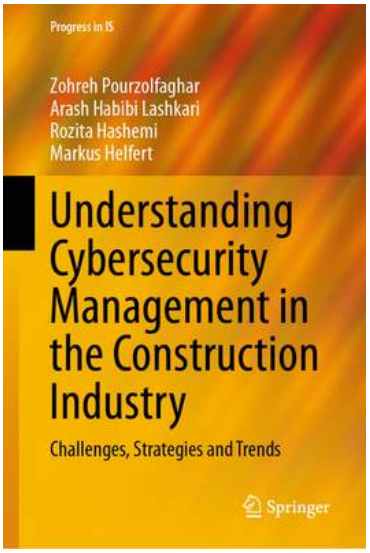
Cybercrime has become one of the fastest-growing threats in the digital age, affecting individuals, organizations, and communities worldwide. Beyond financial losses, cybercrime can have significant psychological, emotional, social, and legal consequences for victims. As cyber threats continue to evolve, understanding victims' needs and providing effective support services have become essential components of a comprehensive cybersecurity strategy.

This book provides a comprehensive understanding of cybersecurity victim services by introducing readers to the fundamentals of cybercrime, victimology, and the legal landscape surrounding cyber incidents. It examines the types of cybercrime victims, the impacts of victimization, reporting and response mechanisms, legal rights, victim support frameworks, and recovery strategies. The book also discusses national and international victim service models, public awareness, prevention initiatives, and the roles of governments, law enforcement agencies, and community organizations in supporting cybercrime victims.

By understanding the challenges faced by cybercrime victims and the services available to assist them, readers can better appreciate the human dimension of cybersecurity and contribute to more effective prevention, response, and recovery efforts. This book equips researchers, policymakers, victim service providers, law enforcement personnel, and cybersecurity professionals with the knowledge needed to strengthen victim support systems and foster a safer and more resilient digital society.

Understanding Cybersecurity Management in the Construction Industry

Challenges, Strategies, and Trends



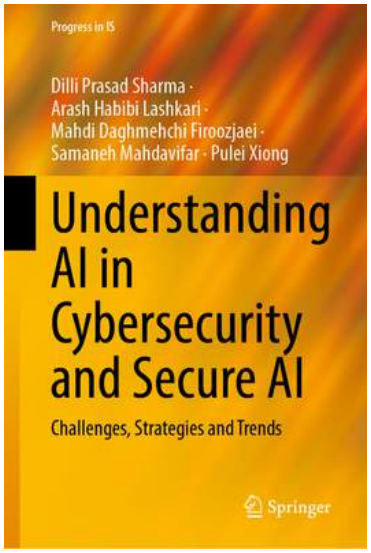
Digital transformation is rapidly reshaping the construction industry through the adoption of technologies such as Building Information Modeling (BIM), Internet of Things (IoT), cloud computing, digital twins, and smart construction systems. While these technologies improve productivity, collaboration, and project efficiency, they also introduce new cybersecurity risks that threaten sensitive project data, connected infrastructure, and critical construction operations. Understanding these evolving threats is essential for protecting digital construction ecosystems and ensuring resilient project delivery.

This book provides a comprehensive introduction to cybersecurity management in the construction sector, beginning with the fundamentals of construction technologies, cybersecurity principles, and the evolving cyber threat landscape. It explores cybersecurity governance, risk assessment, vulnerability management, data protection, software and infrastructure security, supply chain security, cloud-based collaboration, and the security challenges associated with connected construction environments. The book also discusses cybersecurity policies, standards, and best practices that enable organizations to effectively manage cyber risks throughout the construction project lifecycle.

By combining technical foundations with practical management strategies, this book equips engineers, project managers, researchers, students, and industry professionals with the knowledge needed to design, operate, and manage secure digital construction environments. It promotes cybersecurity awareness, strengthens organizational resilience, and supports the safe adoption of emerging digital technologies across the construction industry.

Understanding AI in Cybersecurity and Secure AI

Challenges, Strategies, and Trends



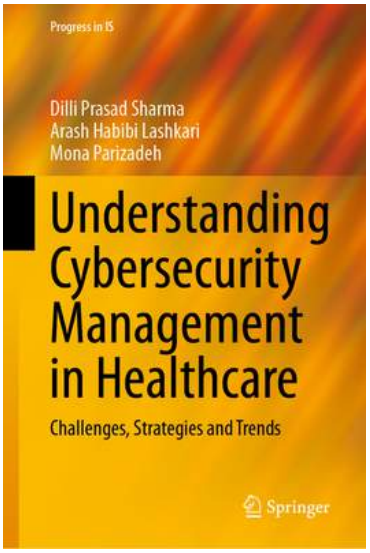
This book presents an overview of the emerging topics in Artificial Intelligence (AI) and cybersecurity and addresses the latest AI models that could be potentially applied to a range of cybersecurity areas. Furthermore, it provides different techniques of how to make the AI algorithms secure from adversarial attacks. The book presents the cyber threat landscape and explains the various spectrums of AI and the applications and limitations of AI in cybersecurity. Moreover, it explores the applications and limitations of secure AI.

The authors discuss the three categories of machine learning (ML) models and reviews cutting-edge recent Deep Learning (DL) models. Furthermore, the book provides a general AI framework in security as well as different modules of the framework; similarly, chapter four proposes a general framework for secure AI. It explains different aspects of network including malware and attacks.

The book also includes a comprehensive study of various scopes of application security; categorized into three groups of smartphone, web application, and desktop application and delves into the concepts of cloud security. The authors discuss state-of-the-art Internet of Things (IoT) security and describe various challenges of AI for cybersecurity, such as data diversity, model customizing, explainability, and time complexity and includes some future work. They provide a comprehensive understanding of adversarial machine learning including the up-to-date adversarial attacks and defenses. The book finishes off with a discussion of the challenges and future work in secure AI.

Understanding Cybersecurity Management in Healthcare

Challenges, Strategies, and Trends



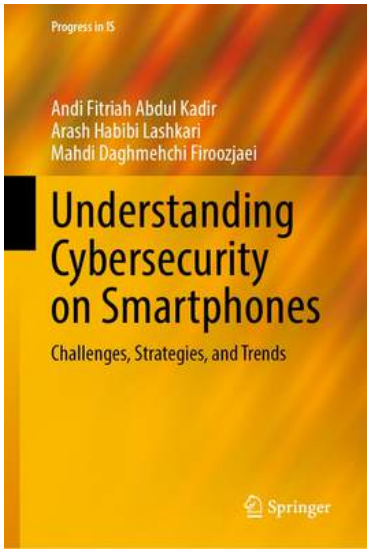
Digital technology is increasingly used in the healthcare sector, and healthcare organizations handle sensitive and confidential information that needs to be kept secure and protected. Therefore, the importance of cybersecurity in healthcare cannot be overstated. Cyber threats can compromise patient data, disrupt healthcare services, and put personal safety at risk.

This book provides an understanding of cybersecurity in healthcare, which is crucial for protecting personal information, ensuring compliance with regulations, maintaining patient trust, and preventing cyber-attacks. Before defining cybersecurity in healthcare, the authors introduce the healthcare environment and cybersecurity basics to readers. They then emphasize the importance of data protection and privacy, software, and personal cybersecurity. Also, they highlight the importance of educating staff about cybersecurity. The discussion continues with data and information security in healthcare, including data threats and vulnerabilities, the difference between data protection and privacy, and how to protect data. Afterward, they focus on the software system frameworks and types of infra-security and app security in healthcare.

By understanding the risks and challenges of cybersecurity in healthcare, healthcare providers and organizations can better protect sensitive and confidential data and ensure the safety and privacy of those they serve.

Understanding Cybersecurity on Smartphones

Challenges, Strategies, and Trends



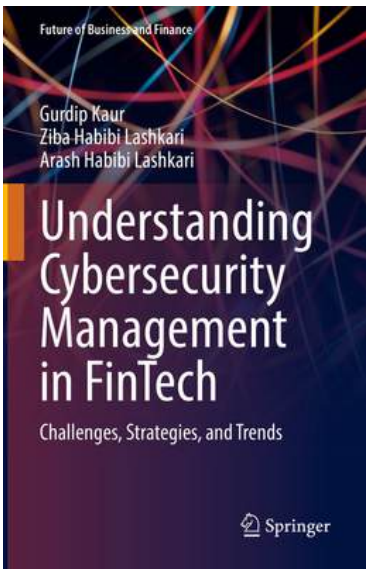
Smartphones have become indispensable tools for communication, banking, healthcare, education, and everyday life, making them attractive targets for cybercriminals. As mobile technologies continue to evolve, users face increasing risks from malware, phishing attacks, insecure applications, network threats, and privacy violations. Understanding smartphone cybersecurity is therefore essential for protecting personal information, digital identities, and sensitive data in an increasingly connected world.

This book provides a comprehensive understanding of smartphone cybersecurity by introducing readers to the architecture and security features of major mobile operating systems, including Android, iOS, Windows, and emerging platforms. It explores mobile application security, device and network protection, Mobile Device Management (MDM), cloud-based mobile services, and cybersecurity best practices for both users and developers. The book also examines the security implications of emerging technologies, including IoT, artificial intelligence, machine learning, and blockchain, within the mobile ecosystem.

By understanding the evolving mobile threat landscape and effective security strategies, readers will be better equipped to safeguard smartphones, applications, and digital communications against modern cyber threats. This book provides researchers, students, cybersecurity professionals, developers, and mobile users with the knowledge required to enhance mobile security, protect digital privacy, and promote the secure adoption of smartphone technologies.

Understanding Cybersecurity Management in FinTech

Challenges, Strategies, and Trends



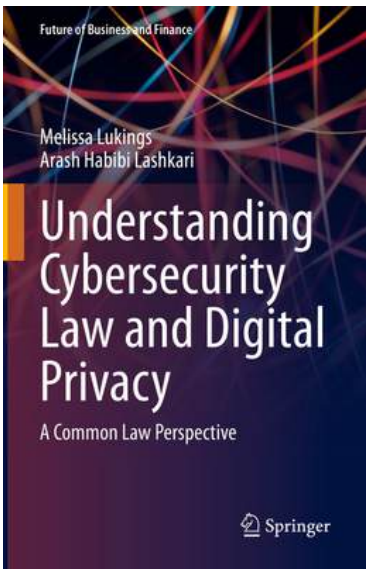
Financial technology (FinTech) has transformed the delivery of financial services by enabling faster, more accessible, and innovative digital banking, payment, investment, and financial management solutions. However, the rapid adoption of digital financial technologies has also increased the exposure of financial institutions and consumers to sophisticated cyber threats, data breaches, fraud, and financial crimes. Understanding cybersecurity in the FinTech ecosystem is therefore essential to ensuring the security, privacy, and resilience of modern financial services.

This book provides a comprehensive understanding of cybersecurity management in FinTech by introducing readers to the fundamentals of financial technology, cybersecurity principles, and information security governance. It examines cybersecurity threats and vulnerabilities, risk management, secure financial market infrastructures, and threat modeling strategies, and presents practical cybersecurity policies, frameworks, and best practices for protecting digital financial systems. The book also discusses emerging challenges and provides recommendations for strengthening cyber resilience across the FinTech ecosystem.

By understanding the cybersecurity challenges facing financial technologies and the strategies available to mitigate cyber risks, readers will be better equipped to protect digital financial assets, customer data, and critical financial infrastructures. This book provides researchers, students, cybersecurity professionals, financial institutions, and policymakers with the knowledge needed to design, manage, and secure next-generation FinTech systems while fostering trust and resilience in the evolving digital economy.

Understanding Cybersecurity Law and Digital Privacy

A Common Law Perspective



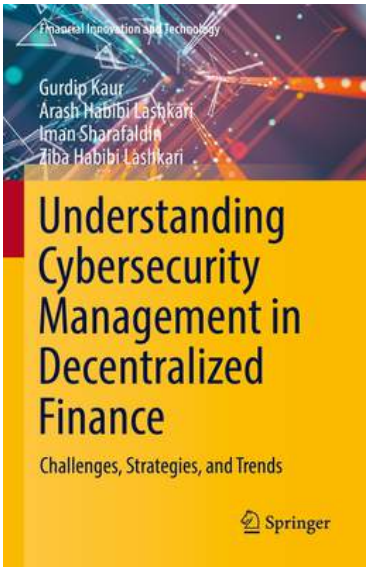
As digital technologies continue to transform how individuals, businesses, and governments collect, process, and share information, concerns about cybersecurity and digital privacy have become increasingly important. The growing volume of personal and organizational data, together with evolving cyber threats and expanding legal obligations, requires a clear understanding of both the technical and legal dimensions of protecting information in the digital age.

This book provides a comprehensive introduction to cybersecurity law and digital privacy by examining the legal principles, regulatory frameworks, and technological concepts that govern the protection of digital information. It explores topics such as privacy rights, data protection legislation, cybersecurity governance, cybercrime, digital evidence, regulatory compliance, and the legal responsibilities of individuals and organizations. The book also discusses emerging legal challenges posed by evolving technologies and offers practical insights into managing cybersecurity and privacy risks.

By integrating legal perspectives with cybersecurity fundamentals, this book equips students, researchers, legal practitioners, policymakers, cybersecurity professionals, and business leaders with the knowledge needed to navigate today's complex digital landscape. It promotes a deeper understanding of the relationship between law, technology, and cybersecurity, supporting informed decision-making and the development of secure, privacy-preserving digital environments.

Understanding Cybersecurity Management in Decentralized Finance

Challenges, Strategies, and Trends



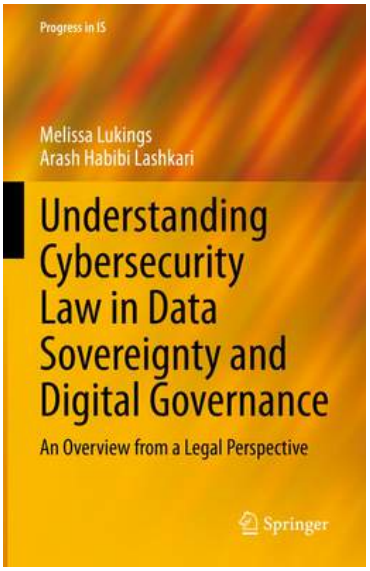
This book discusses understand cybersecurity management in decentralized finance (DeFi). It commences with introducing fundamentals of DeFi and cybersecurity to readers. It emphasizes on the importance of cybersecurity for decentralized finance by illustrating recent cyber breaches, attacks, and financial losses. The book delves into understanding cyber threats and adversaries who can exploit those threats. It advances with cybersecurity threat, vulnerability, and risk management in DeFi. The book helps readers understand cyber threat landscape comprising different threat categories for that can exploit different types of vulnerabilities identified in DeFi. It puts forward prominent threat modelling strategies by focusing on attackers, assets, and software.

The book includes the popular blockchains that support DeFi include Ethereum, Binance Smart Chain, Solana, Cardano, Avalanche, Polygon, among others. With so much monetary value associated with all these technologies, the perpetrators are always lured to breach security by exploiting the vulnerabilities that exist in these technologies. For simplicity and clarity, all vulnerabilities are classified into different categories: arithmetic bugs, re-Entrancy attack, race conditions, exception handling, using a weak random generator, timestamp dependency, transaction-ordering dependence and front running, vulnerable libraries, wrong initial assumptions, denial of service, flash loan attacks, and vampire.

Since decentralized finance infrastructures are the worst affected by cyber-attacks, it is imperative to understand various security issues in different components of DeFi infrastructures and proposes measures to secure all components of DeFi infrastructures. It brings the detailed cybersecurity policies and strategies that can be used to secure financial institutions. Finally, the book provides recommendations to secure DeFi infrastructures from cyber-attacks.

Understanding Cybersecurity Law in Data Sovereignty & Digital Governance

An Overview from a Legal Perspective



This book provides an overview of the topics of data, sovereignty, and governance with respect to data and online activities through a legal lens and from a cybersecurity perspective. This first chapter explores the concepts of data, ownerships, and privacy with respect to digital media and content, before defining the intersection of sovereignty in law with application to data and digital media content. The authors delve into the issue of digital governance, as well as theories and systems of governance on a state level, national level, and corporate/organizational level. Chapter three jumps into the complex area of jurisdictional conflict of laws and the related issues regarding digital activities in international law, both public and private.

Additionally, the book discusses the many technical complexities which underlay the evolution and creation of new law and governance strategies and structures. This includes socio-political, legal, and industrial technical complexities which can apply in these areas. The fifth chapter is a comparative examination of the legal strategies currently being explored by a variety of nations. The book concludes with a discussion about emerging topics which either influence, or are influenced by, data sovereignty and digital governance, such as indigenous data sovereignty, digital human rights and self-determination, artificial intelligence, and global digital social responsibility.

Cumulatively, this book provides the full spectrum of information, from foundational principles underlining the described topics, through to the larger, more complex, evolving issues which we can foresee ahead of us.

Blog Series

Insights, Trends, and Expert Perspectives

01 Understanding AI in Cybersecurity and AI Security
02 Understanding Cybersecurity Management in Healthcare
03 Understanding Cybersecurity on Smartphones
04 Understanding Cybersecurity Management in DeFi
05 Understanding Current Cybersecurity Challenges in Law
06 Understanding Cybersecurity Management for FinTech
07 Understanding Android Malware Families
08 Understanding Canadian Cybersecurity Laws

Understanding AI in Cybersecurity and AI Security

UCSAISec (2025)

The Understanding AI in Cybersecurity and AI Security (UCSAISec) blog series provides a comprehensive and accessible introduction to the rapidly evolving intersection of artificial intelligence, cybersecurity, and AI security. Across five articles, the series systematically explores the application of AI in cybersecurity, AI-driven protection for IoT and OT environments, security and privacy threats targeting AI systems, defense mechanisms against adversarial attacks and privacy leakage, and the broader challenges of AI safety, alignment, transparency, bias, and fairness. By combining foundational concepts, practical examples, structured taxonomies, security frameworks, and emerging research directions, the series bridges the gap between technical depth and educational accessibility, offering readers a unified perspective on both using AI to strengthen cybersecurity and securing AI systems themselves in increasingly intelligent and interconnected environments.

01 AI in Cybersecurity

02 AI in IoT and OT Security

03 AI Security and Privacy

04 Defence Methods for Adversarial Attacks and Privacy Issues in Secure AI

05 AI Safety and Fairness Nowadays Explained

Understanding Cybersecurity Management in Healthcare

UCSMH (2024)

The Understanding Cybersecurity Management in Healthcare (UCSMH) series provides a comprehensive introduction to cybersecurity management across modern digital healthcare ecosystems. Through four interconnected articles, the series systematically examines the foundations of healthcare cybersecurity, common vulnerabilities, threats, and cyberattacks, detection and prevention strategies, governance and ethical principles, data governance, privacy protection, regulatory compliance, and emerging cybersecurity challenges and future research directions. By integrating healthcare-specific security concepts, governance frameworks, real-world cyber threats, industry standards such as HIPAA, GDPR, ISO/IEC 27001, COBIT, and NIST, together with practical best practices for healthcare professionals and IT administrators, the series offers a structured educational resource that bridges cybersecurity, healthcare management, data governance, patient privacy, and operational resilience, making it valuable for healthcare practitioners, researchers, students, and decision-makers seeking to strengthen cybersecurity across the healthcare sector.

01 Defining Cybersecurity in Healthcare

02 Detection and Prevention of Cyber-Attacks in Healthcare

03 Cybersecurity Governance and Ethics in Healthcare

04 Cybersecurity Challenges, Best Practices, and Future Work in Healthcare

Understanding Cybersecurity on Smartphones

UCSph (2024)

The Understanding Cybersecurity on Smartphones (UCSph) series provides a comprehensive introduction to smartphone cybersecurity by examining the architecture, security mechanisms, vulnerabilities, malware, adversarial techniques, and current security trends across multiple mobile operating systems. Through four interconnected articles, the series explores the security foundations of Apple's iOS, Microsoft's Windows Phone, and several alternative smartphone operating systems, including Symbian, Tizen, Sailfish, Ubuntu Touch, KaiOS, Sirin OS, and HarmonyOS, before concluding with a practical discussion of modern mobile application security challenges for both users and developers. By integrating operating system architectures, vulnerability analysis, malware taxonomies, attack techniques, mitigation strategies, secure application development practices, and emerging mobile security trends, the series offers a structured educational resource that bridges smartphone operating system security, mobile malware analysis, secure software development, and practical cybersecurity best practices for researchers, developers, students, and mobile users.

01 iOS Operating System

02 Windows Phone Operating System

03 Exploring Alternative Smartphone OSs: Beyond Android and iOS for Security

04 The Challenges in Mobile Application Security 2024

Understanding Cybersecurity Management in DeFi

UCM-DeFi (2023)

The Understanding Cybersecurity Management in Decentralized Finance (UCM-DeFi) series provides a comprehensive introduction to the rapidly evolving ecosystem of decentralized finance by systematically examining its foundations, enabling technologies, security challenges, and emerging cyber threats. Across five interconnected articles, the series explores the evolution of modern finance from centralized to decentralized systems, the fundamentals and operational processes of smart contracts, major DeFi platforms and blockchain ecosystems, blockchain attacks and corresponding countermeasures, and the security vulnerabilities and threats affecting smart contracts and decentralized applications. By integrating blockchain architectures, cryptocurrencies, consensus mechanisms, smart contract programming, DeFi applications, platform security, attack taxonomies, and practical mitigation strategies, the series offers a structured educational resource that bridges financial technologies, blockchain security, and cybersecurity management, providing valuable guidance for students, researchers, developers, investors, and cybersecurity professionals seeking to understand and secure decentralized financial ecosystems.

01 The Origin of Modern Decentralized Finance
02 Introduction to Smart Contracts and DeFi
03 DeFi Platforms
04 Blockchain Security
05 Smart Contracts and DeFi Security and Threats

Understanding Current Cybersecurity Challenges in Law

UCCCL (2022)

The Understanding Current Cybersecurity Challenges in Law (UCCCL) series provides a comprehensive exploration of the legal, regulatory, and governance challenges emerging from the rapid evolution of cyberspace, digital technologies, and artificial intelligence. Across six interconnected articles, the series examines data sovereignty and cross-border data transfers, digital governance and social responsibility, online jurisdictional authority, digital content censorship, data breaches and privacy protection, and the legal implications of artificial intelligence and technological innovation. By integrating principles of cybersecurity, privacy law, international law, digital governance, human rights, regulatory policy, and emerging technologies, the series offers a balanced interdisciplinary perspective on how legal frameworks must evolve to address modern cybersecurity challenges while protecting innovation, privacy, freedom of expression, and public trust. This makes the series a valuable educational resource for students, researchers, legal professionals, policymakers, and cybersecurity practitioners seeking to understand the intersection of law, technology, and digital governance.

01 Data Sovereignty & Cross-Border Data Transfers

02 Digital Governance and Social Responsibility Meet User-Generated Content

03 Determining Online Jurisdictional Authority

04 Balancing Responsibilities in Digital Content Censorship

05 Data Breaches and Increased Data Awareness

06 Legal Considerations for Artificial Intelligence and Technological Development

Understanding Cybersecurity Management for FinTech

UCMF (2021–2022)

The Understanding Cybersecurity Management for FinTech (UCMF) series provides a comprehensive introduction to cybersecurity management across the modern financial technology ecosystem by systematically examining its technological foundations, governance frameworks, cyber threats, vulnerabilities, operational risks, financial market infrastructures, and organizational security strategies. Across six interconnected articles, the series explores the evolution of FinTech and its ecosystem, information security governance, cybersecurity threats and threat actors, common vulnerabilities and cyber risks, security challenges affecting financial market infrastructures, and cybersecurity policies, resilience, and strategic defense mechanisms for financial institutions. By integrating principles of cybersecurity governance, risk management, financial technologies, information security, cyber resilience, and organizational policy with practical mitigation strategies and industry best practices, the series offers a structured educational resource that bridges financial services, cybersecurity management, and regulatory governance. The series serves as a valuable reference for students, researchers, cybersecurity professionals, financial institutions, policymakers, and FinTech practitioners seeking to understand and strengthen cybersecurity across the rapidly evolving digital financial ecosystem.

01 Understanding FinTech and the Importance of Security Objects
02 Information Security Governance in FinTech
03 Cybersecurity Threats in FinTech
04 Cybersecurity Vulnerabilities and Risk in FinTech
05 Security Issues on Financial Market Infrastructures
06 Cybersecurity Policy and Strategy Management

Understanding Android Malware Families

UAMF (2021)

The Understanding Android Malware Families (UAMF) series provides a comprehensive introduction to the Android malware ecosystem by systematically examining the foundations, behavior, evolution, detection, and mitigation of the most prevalent Android malware families. Across six interconnected articles, the series explores Android malware fundamentals, Trojan families, ransomware and scareware, riskware, adware and backdoors, and file infectors together with potentially unwanted applications (PUAs). Leveraging the publicly released CCCS-CIC-AndMal-2020 dataset and related Android malware research, the series analyzes malware behaviors, indicators of compromise, technical detection features, including memory, API, network, log, and permission-based characteristics, and practical prevention strategies for mobile devices. By integrating malware taxonomy, behavioral analysis, cybersecurity analytics, and real-world datasets into an accessible educational framework, the series serves as a valuable resource for students, researchers, cybersecurity professionals, malware analysts, and Android users seeking to better understand, detect, and defend against modern Android malware threats.

01 The Foundations
02 The Trojan – an Impersonator in the Background
03 Ransomware and Scareware
04 Riskware – Is It Worth It?
05 Adware and Backdoor
06 File Infector and Potentially Unwanted Applications

Understanding Canadian Cybersecurity Laws

UCCL (2020–2021)

The Understanding Canadian Cybersecurity Laws series provides a structured introduction to the legal foundations of cybersecurity, privacy, cybercrime, and data protection in Canada. Across ten interconnected articles, it explores Canadian privacy legislation, the Criminal Code, anti-spam regulations, cybercrime, digital privacy rights, Dark Web legal challenges, comparative international legislation, and emerging legal reforms. By combining legal principles, case studies, and practical guidance, the series serves as an accessible resource for students, cybersecurity professionals, policymakers, and organizations seeking to understand Canada's evolving cybersecurity legal landscape.

01 The Foundation

02 Privacy and Access to Information, the Acts

03 Privacy Protection in the Modern Marketplace – PIPEDA

04 Interpersonal Privacy and Cybercrime – Criminal Code of Canada

05 'Insert Something Clever Here' – Canada's Anti-Spam Legislation

06 Peer-to-Peer Privacy Protection – "Intrusion Upon Seclusion" and the Protection of Intimate Images

07 Deep, Dark, and Undetectable – Canadian Jurisdictional Considerations in Global Encrypted Networks

08 Measuring Up – Outlining Existing National Cybersecurity Legislation in Canada, the UK, Australia, and the US

09 Legislative Modernization – Responding and Adapting to Technological Change in a Global Domain

Workshop Series

Empowering cybersecurity education through global workshops

01 Shaping Young Minds: Cybersecurity Career Exploration in Schools
02 Elevating Cybersecurity Vigilance: Fusing Knowledge Dissemination via the Understanding Cybersecurity Series (UCS) Knowledge Mobilization Program
03 Securing the Digital Future: AI, Cyber Threats, and Sustainable Innovation (DIGI+ MSCA Cofund)
04 Enhancing Cybersecurity Resilience: Advancing AI-Powered Security and Security of AI Through the UCS Knowledge Mobilization Program
05 Elevating Cybersecurity Vigilance: Cybersecurity, Social Engineering, and AI Threats in K-12 Education
06 The Future of Cybersecurity: Leveraging Cybersecurity Open-Source Tools and Datasets for Enhanced AI-Driven Solutions
07 AI's Impact on Cyber Security: What You Need To Know
08 Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS) for Fintech and Digital Finance
09 Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS) – Insurance Cyber Attacks
10 Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS)
11 Navigating Cybersecurity: Empowering Public Safety and Awareness Through UCS
12 Understanding Cybersecurity Series (UCS)
13 Data Security and Governance

Workshop Series

Empowering cybersecurity education through global workshops

Western University, Canada (Apr 10, 2026)

Shaping Young Minds: Cybersecurity Career Exploration in Schools
St John Paul II Catholic High School, Canada • May 7, 2026
James Cardinal McGuigan Catholic High School, Canada • Apr 22, 2026

Elevating Cybersecurity Vigilance: Fusing Knowledge Dissemination via the Understanding Cybersecurity Series (UCS) Knowledge Mobilization Program
UWORCS 2026, Western University, Canada • Apr 10, 2026
European Institute of Innovation & Technology (EIT), Europe • Jul 18, 2025

Securing the Digital Future: AI, Cyber Threats, and Sustainable Innovation (DIGI+ MSCA Cofund)
Maynooth University, Ireland • Dec 2, 2025

Enhancing Cybersecurity Resilience: Advancing AI-Powered Security and Security of AI Through the UCS Knowledge Mobilization Program
Université du Québec en Outaouais (UQO), Canada • May 28, 2025
Dalhousie University, Canada • Mar 7, 2025

European Institute of Innovation & Technology (EIT), Europe (Jul 18, 2025)

Elevating Cybersecurity Vigilance: Cybersecurity, Social Engineering, and AI Threats in K-12 Education
Ontario School Boards' Insurance Exchange (OSBIE), Canada • Nov 21, 2024

The Future of Cybersecurity: Leveraging Cybersecurity Open-Source Tools and Datasets for Enhanced AI-Driven Solutions
McMaster University, Canada • Oct 31, 2024
University of Windsor, Canada • Sep 27, 2024

AI's Impact on Cyber Security: What You Need To Know
Markham Board of Trade, Canada • Sep 26, 2024

Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS) for Fintech and Digital Finance
European Institute of Innovation & Technology (EIT), Europe • Jul 5, 2024

Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS) – Insurance Cyber Attacks
3rd Annual GCS Client Event, Aviva, Canada • May 14, 2024

Markham Board of Trade, Canada (Sep 26, 2024)

Elevating Cybersecurity Vigilance: Understanding Cybersecurity Series (UCS)
MacEwan University, Canada • Feb 9, 2024
National Institute of Information and Communications (NICT), Japan • Dec 1, 2023

Navigating Cybersecurity: Empowering Public Safety and Awareness Through UCS
York Circle, York University, Canada • Oct 14, 2023

Understanding Cybersecurity Series (UCS)
North Carolina A&T University, USA • Apr 20, 2023

Data Security and Governance
University of Toronto, Canada • Jan 17, 2023

Cartoon Contest Series

Celebrating creativity in cybersecurity

01 CSCA 2026: 3rd Cybersecurity Cartoon Award (Norway)

02 CSCA 2025: 2nd Cybersecurity Cartoon Award (Spain)

03 CSCA 2024: 1st Cybersecurity Cartoon Award (Canada)

Cyber Security Cartoon Award (CSCA)

Celebrating creativity in cybersecurity

The UCS Cybersecurity Cartoon Award (CSCA) is an international competition that promotes cybersecurity awareness through creativity, visual storytelling, and public engagement. By encouraging participants to communicate complex cybersecurity concepts in simple and engaging ways, the competition bridges the gap between technical knowledge and public understanding. Open to students, professionals, artists, and cybersecurity enthusiasts worldwide, CSCA celebrates innovative ideas that inspire safer digital practices across diverse communities.

Beyond recognizing artistic excellence, the Cybersecurity Cartoon Award is a unique knowledge mobilization initiative that fosters cybersecurity education and outreach globally. Winning entries are showcased on the UCS platform and through international outreach activities, helping to raise awareness of emerging cyber threats, digital safety, privacy, and responsible technology use. By combining creativity with cybersecurity education, CSCA strengthens public engagement and encourages a culture of cyber awareness that extends beyond traditional technical audiences.

CSCA 2026

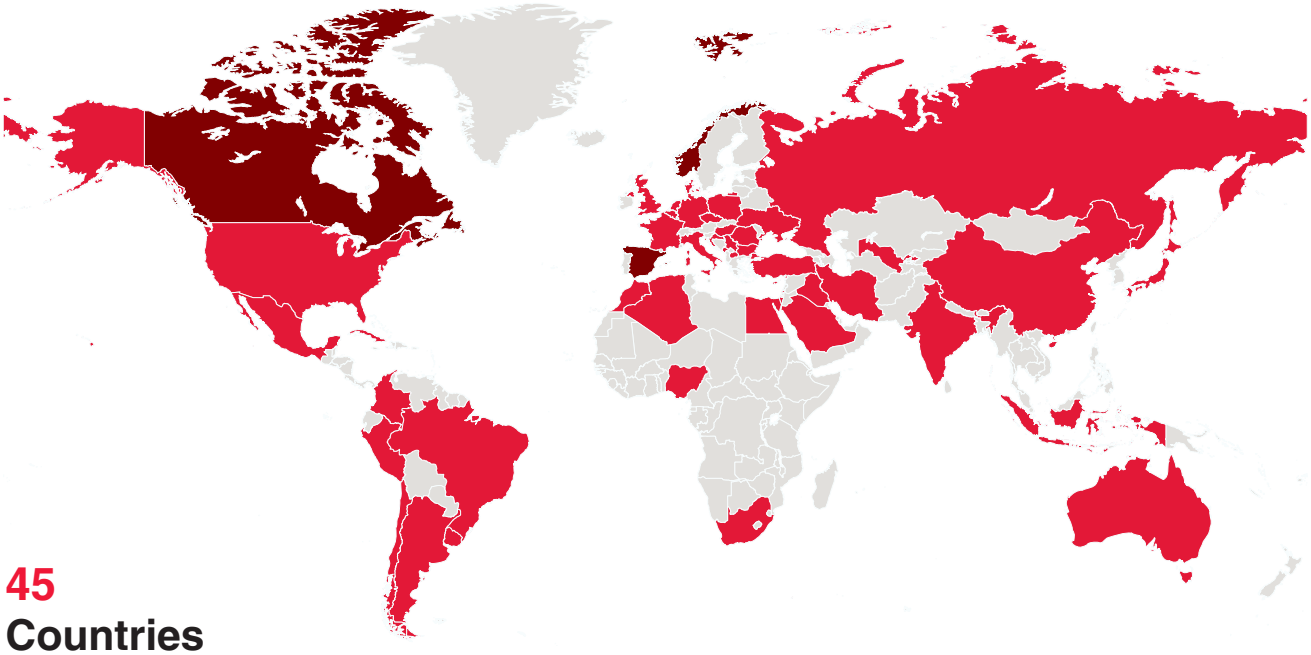
Held at the **Norwegian University of Science and Technology (NTNU)**, CSCA 2026 is the largest edition yet with 337 cartoon entries from 166 cartoonists across 38 countries.

CSCA 2025

CSCA 2025 was hosted at the **Polytechnic University of Madrid (UPM)** and welcomed 263 cartoon entries from 128 participating artists in 25 countries

CSCA 2024

The inaugural edition of CSCA was held at **York University**, seeing 114 cartoon entries submitted by 65 participating artists from 18 countries.



45
Countries

CSCA has brought together artists from more than 45 countries across five continents, with three editions hosted in Canada, Spain, and Norway.

700+
Cartoons

Original cartoon entries across three contest editions

300+
Artists

Participating cartoonists of all ages and levels of experience

24
Winners

Creative and impactful winning cartoons

60+
Finalists

Cartoons shortlisted by the jury panel

10
Judges

Cartoonists and cybersecurity experts serving as jury

$10K+
Awarded

Prize pool awarded to winning artists across all contests

Contributors

Building impact through a shared commitment to cybersecurity

01 Contributors

Contributors

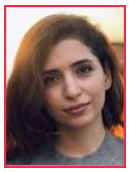
The talented team driving UCS forward together

Arash Habibi Lashkari
Canada Research Chair
Founder and Director, BCCC
York University, Canada

Shaila Sharmin
Postdoctoral Fellow

Arousha Haghighian Roudsari
Postdoctoral Fellow

Sepideh Hajihosseinkhani
PhD Candidate



Mahsa Karami
MAIST Student

Ava Ameri
MAIST (Graduated)

Mahdiye Khalaji
MASc (Graduated)

Amirhossein Ahmadnejad Roudsari
MCS (Graduated)

Reza Abbaszadeh
MCS (Graduated)

Niosha Hejazi
Master of IT (Graduated)

Arefeh Kouhi
Master of IT (Graduated)

Aditi Sharma
Master of IT (Graduated)

Moein Shafi
Master of CS (Graduated)

Yasin Dehfouli
Master of CS (Graduated)

Sepideh Niktabe
Master of CS (Graduated)

Ilkay Kaya
Master of ScMP (Graduated)

Pedram Sharifani
Graduate RA

Borna Ahmadzadeh
Undergraduate RA

Hadis Farrokhi
Undergraduate RA

Sepehr Jafari
Undergraduate RA

Maryam Issakhani
Graduate RA

Joshua Duarte
Undergraduate RA

Contributors

Mona Parizadeh
RA

Dilli Sharma
RA

Barjinder Kaur
RA

Melissa Lukings
RA

Samaneh Mahdavifar
RA

Hilda Karimpour
Undergraduate RA

Kimia Molazem
Undergraduate RA

Hirad Shirian
Undergraduate RA

Marella Bolton
Graduate RA

Isabella Lopez
Undergraduate RA

Osman Berk Er
Undergraduate RA

Xie He
Undergraduate RA

Maelle Gautrin
International Visiting Researcher

Mehrsa Khoshpasand
Undergraduate RA

Elsie Benko
Undergraduate RA

Bhaskar Joshi
Globalink Research Intern

Alaa Souabni
Globalink Research Intern

Mateus Herbele
Globalink Research Intern

Abhay Pratap Singh
Globalink Research Intern

Aditya Raj
Globalink Research Intern

Mohamed Aziz El Fadhel
Globalink Research Intern

Hardhik Mohanty
Globalink Research Intern

Nikhill Vombatkere
Globalink Research Intern

Nathan Chow
IT Team

Oksana Mizgier
IT Team

Ammar Homidan
IT Team

Rosananthi Selvarajah
IT Team

BCCC
Behaviour-Centric
Cybersecurity Center

DB 2004, Victor Phillip Dahdaleh Building
4700 Keele Street
Toronto, ON M3J 1P3

+1 (416) 736 2100 ext. 66624
yorku.ca/research/bccc
ahabibil@yorku.ca