



Network Telescope at Merit Network: Advancing Cybersecurity Research and Internet Measurement

Dr. Shereen Ismail, Research Scientist: Networking and Cybersecurity
Merit Network Inc., University of Michigan, MI 48108, USA



Outline



Merit Network

Introduction

Academic & Research Benefits

Major Active and Long-running Network Telescopes

ORION Pipeline

SCOPE-X Project

ORION Intelligence Archive

20+ Years of Darknet Intelligence

Data Sharing

Current Research

Future Research

Recent Publications

Dynamic Network Telescope Project

International Distributed Network Telescope Project

Researchers and Student Collaborators

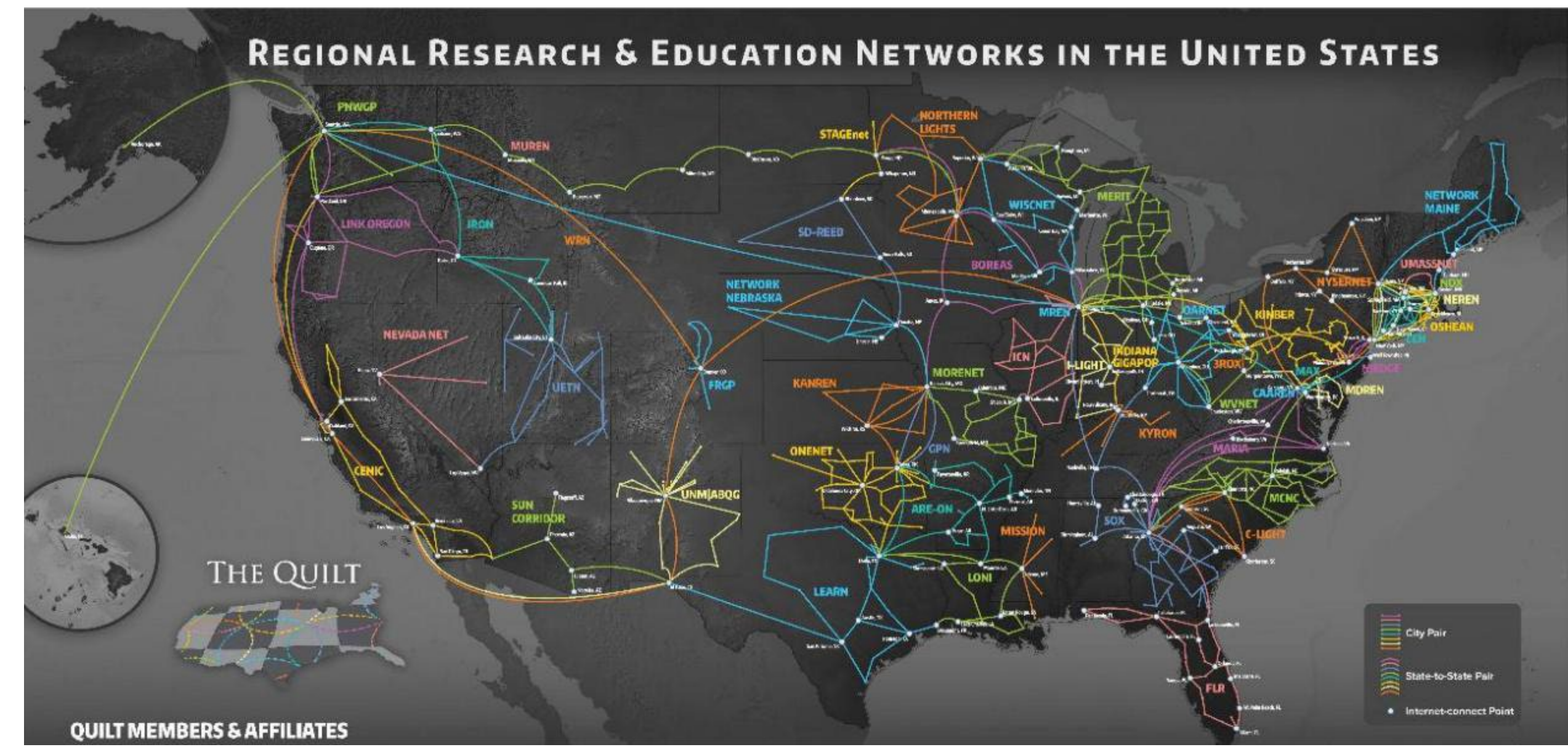
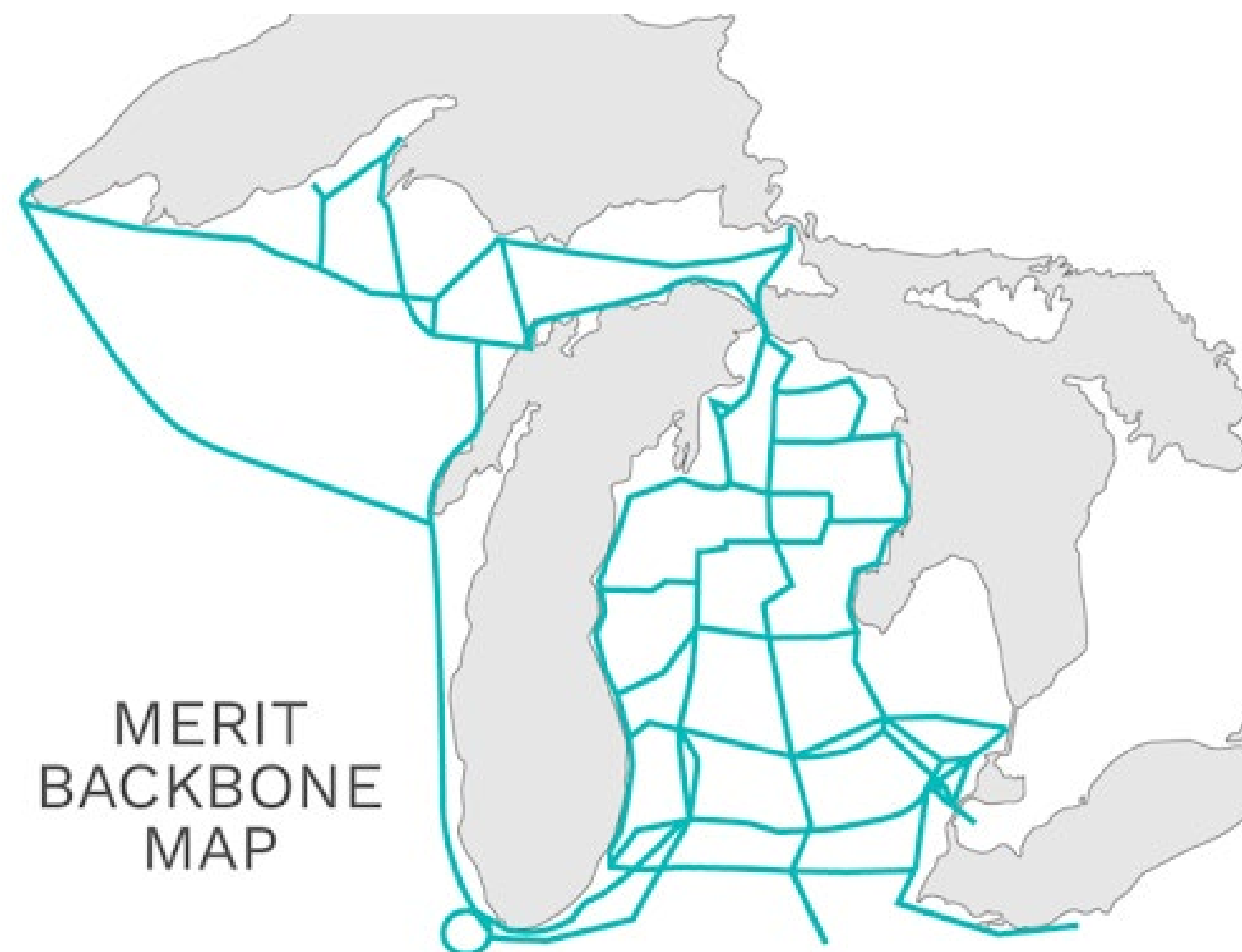
Merit Network



Merit Network, Inc. is an independent nonprofit corporation governed by Michigan's public universities.

Founded in 1966, Merit owns and operates America's longest-running regional Research and Education (**R&E**) network.

After almost 60 years of innovation, Merit continues to provide high-performance services to the educational communities in Michigan and beyond.





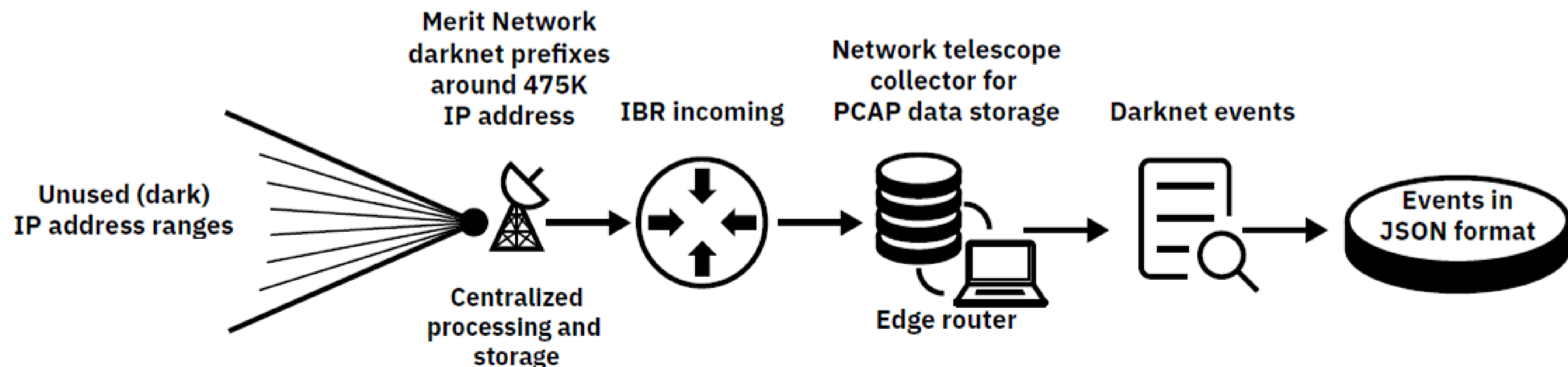
Introduction

- **Network telescopes** monitor large blocks of unallocated IPv4/IPv6 address space (darknets).
- Any traffic arriving at these unused addresses is inherently suspicious - no legitimate services exist there.
- Passive monitoring captures all incoming packets without responding (one-way traffic collection).
- Traffic is routed to collection infrastructure via BGP announcements of monitored prefixes.
- What Gets Captured:
 - Backscatter from DDoS attacks - Response traffic generated when attackers use spoofed source IP addresses.
 - Scanning activity – automated scanners and bots probing for vulnerable systems.
 - Worm propagation attempts - Self-replicating malware scans for new vulnerable hosts.
 - Misconfigured systems - legitimate traffic sent to wrong IP addresses.
- Internet Background Radiation (IBR) - continuous, unsolicited traffic observed across unused address space, including scanning, malware activity, backscatter, and other Internet noise.



Introduction (cont.)

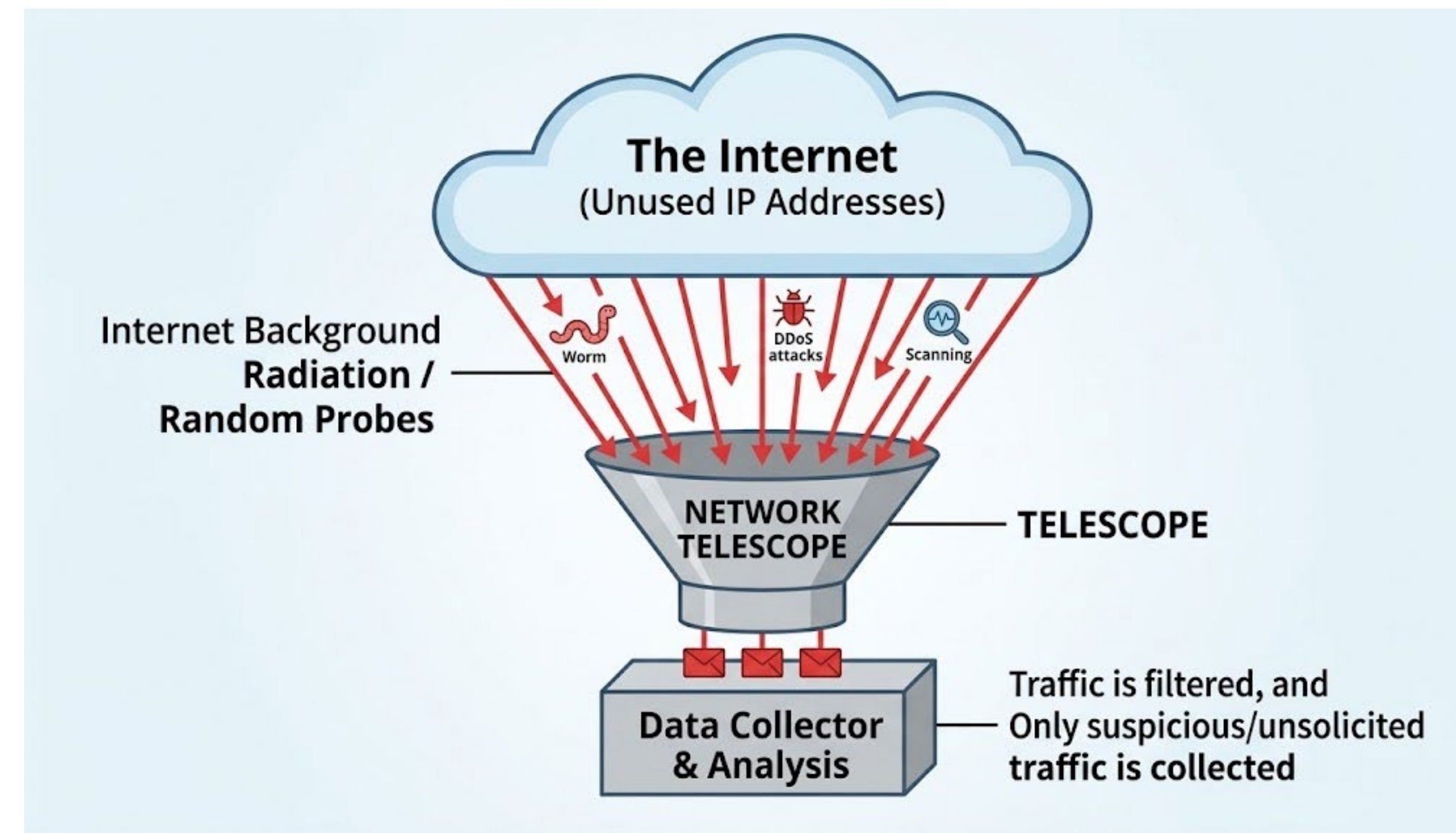
- **ORION**, Merit's Network Telescope, is one of the largest network telescopes in the US operated by Merit Network which enables large-scale security monitoring and research into emerging cyber threats.
- Network telescopes collect around 150 GB daily. The captured unsolicited Internet traffic provides visibility into global threat activities: scanning, botnets, malware propagation, and DDoS.
- ORION spans 20+ years of continuous darknet packet captures between 2005 and 2026. Datasets collected from ORION offer a rare longitudinal view of Internet threats.





Academic & Research Benefits

- **Strengthening Cybersecurity Curriculum:** Supports courses and labs in network forensics, threat intelligence, internet measurement, and anomaly detection using real-world data
- **Hands-On Student Learning:** Provides undergraduate and graduate students with Internet-scale datasets for capstone projects, labs, and research
- **Faculty Research Opportunities:** Enables cross-institutional collaboration, new grant proposals, and scholarly publications in cybersecurity, networking, and internet measurement science.
- **Democratizing Access to Research Data:** Expands access to darknet datasets beyond R1 institutions to regional universities and community colleges.
- **Supporting Program Development:** Helps institutions strengthen cybersecurity programs by providing access to modern real-time datasets and research infrastructure.

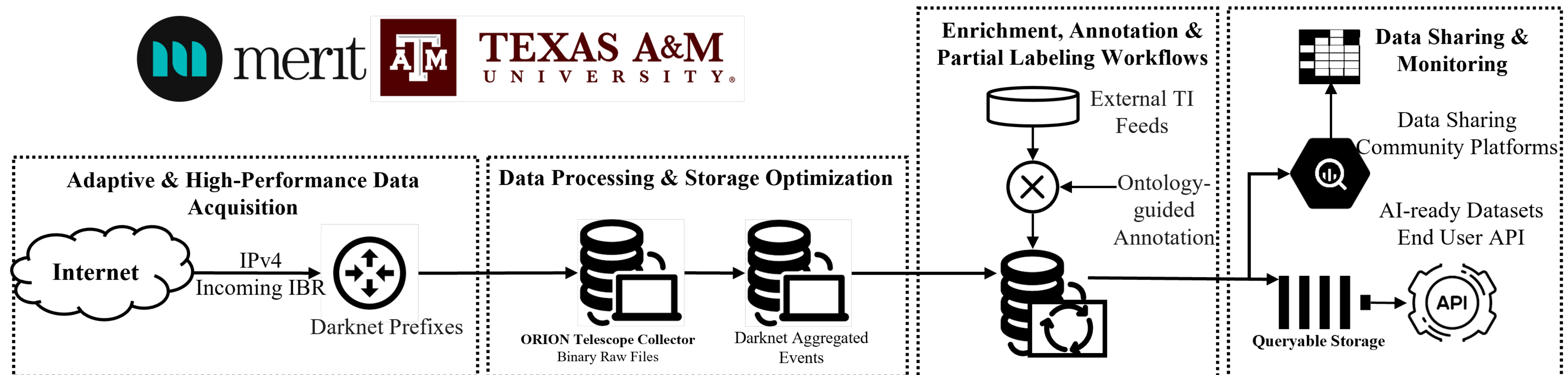


Major Active and Long-running Network Telescopes

PROJECT	LARGEST SIZE	CURRENT SIZE	GEOGRAPHY	SCOPE
CAIDA/UCSD	/8 (~16.7M IPs)	/9 & /10 (~12.6M IPs)	USA	Academic (Long-term
Merit Network (ORION)	/8 (~16.7M IPs)	/13 (~524k IPs)	USA	Academic (NSF Funded)
MICTER (Japan)	~300k IPs	~300k IPs	Japan/Asia	National CERT/Research
Team Cymru	Undisclosed	Distributed	Global	Commercial Intelligence
DarknetBR (Brazil)	/19 (~8k IPs)	/19 (~8k IPs)	Brazil	Academic/Regional
SURFnet (NL-Darknet)	/15 (~131k IPs)	Variable	Netherlands	National R&E Network
MAWI Working Group	/16 (~65k IPs)	/16 (~65k IPs)	Japan	Academic (WIDE Project)
SWITCH (Switzerland)	~2M IPs	~2M IPs	Switzerland	National R&E Network
Farsight/DomainTools	~524k IPs	~524k IPs	Global	Commercial (Subscription)

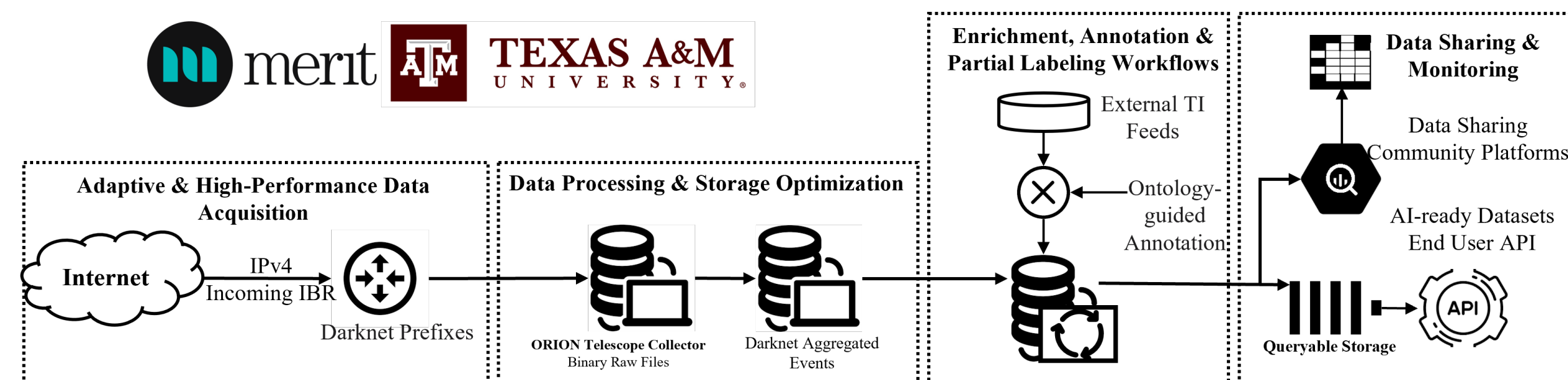
ORION Pipeline

IPv4 Traffic Acquisition and Data Processing



SCOPE-X Project

Optimizing Merit's Network Telescope for High-Quality Large-Scale Datasets



- Led by Merit Network in collaboration with Texas A&M University
- Supported by: Cybersecurity Innovation for CyberInfrastructure-Reference Scientific Security Datasets (CICI-RSSD), Office of Advanced Cyberinfrastructure, National Science Foundation
- 3-year project. Started on September 2026.
- SCOPE-X (Scalable Cyberinfrastructure for Observatory Pipeline Enhancement) three key contributions:
 - (1) Resilient Capture: Developing adaptive, multi-threaded methods for raw packet processing to ensure high-fidelity capture during extreme traffic bursts, evolving attack behaviors, and dynamic traffic patterns
 - (2) AI-Ready Curation: Designing a reproducible, research-grade dataset generation framework that enhances dataset fidelity via improved cleaning, feature engineering, partial labeling, and enrichment with contextual metadata, including integration with external threat-intelligence feeds
 - (3) FAIR-Aligned Access: Modernizing dataset delivery via APIs and code-to-data environments to ensure long-term sustainability, reproducibility, and broad usability.



ORION Intelligence Archive

Two Decades of Attack Forensics & Exponential Growth



ORION DARKNET SCALE

474 Terabytes of Real Attack Intelligence Over 20 Years



474 TB
TOTAL ARCHIVE SIZE

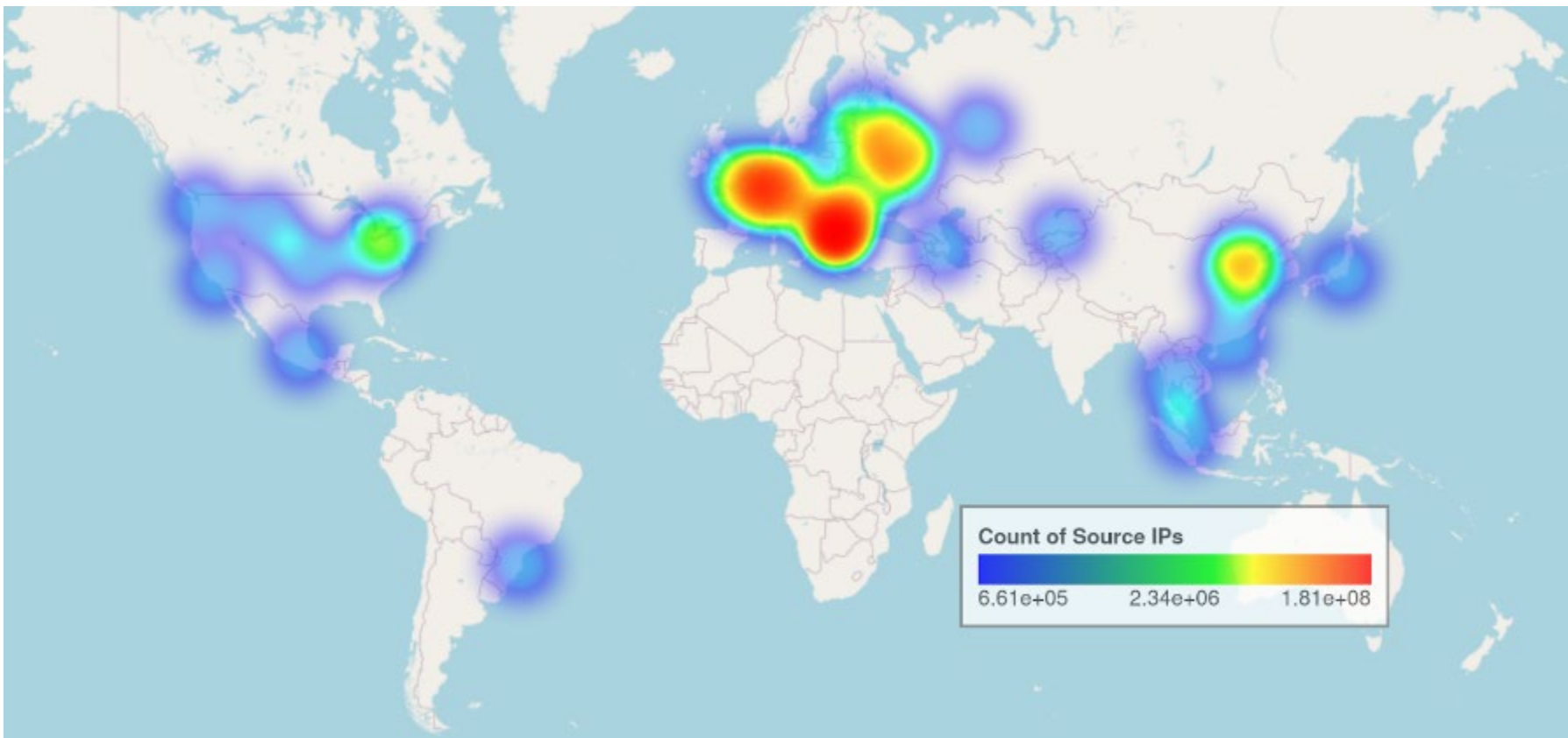
6.3 GB/hr
CURRENT CAPTURE RATE

~150 GB/day
DAILY VOLUME (2026)

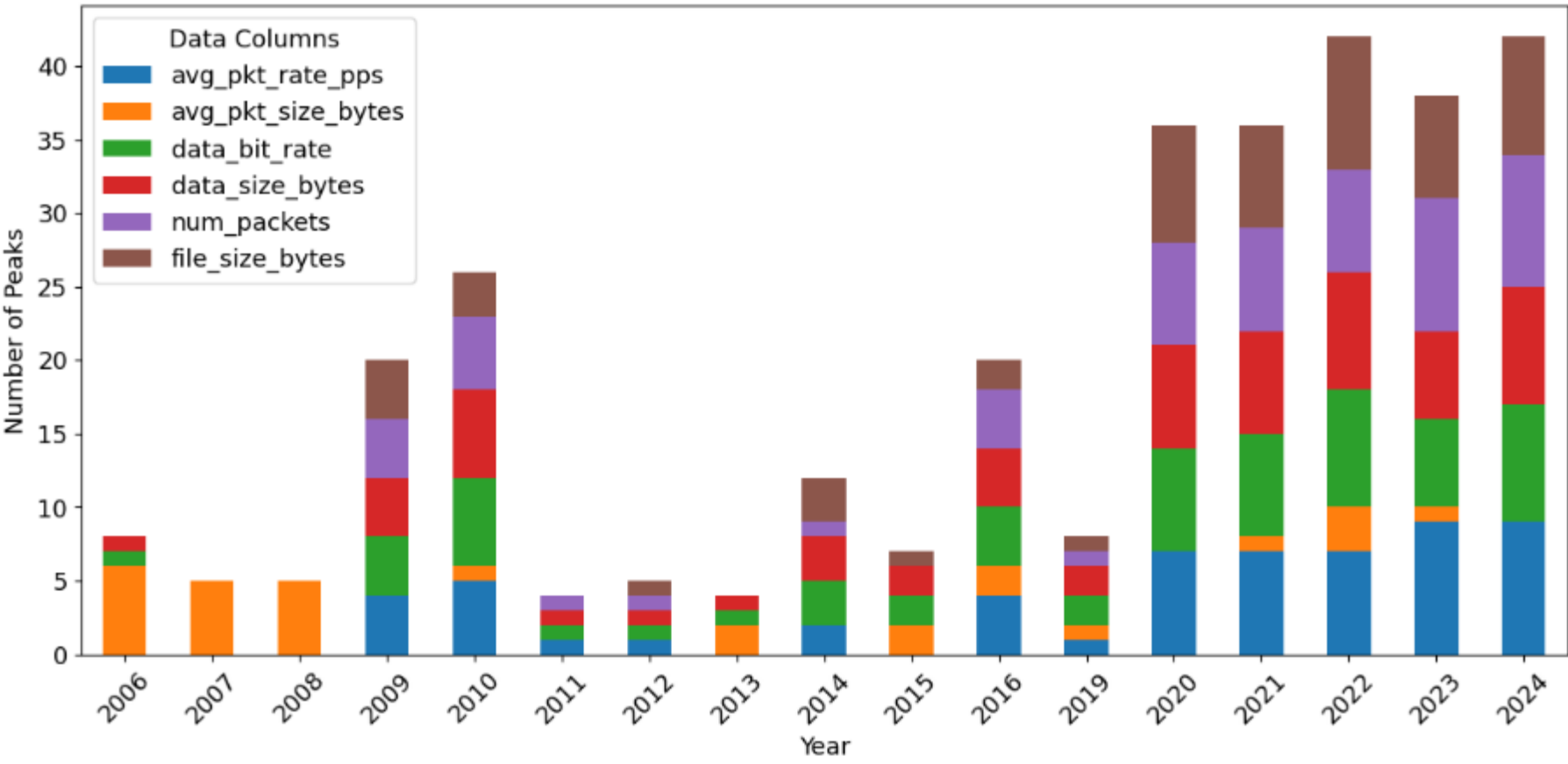
70x
GROWTH SINCE 2005

▲ LIVE DATA: Every hour, 6.3GB of new attacks are captured and analyzed in real-time

20+ Years of Darknet Intelligence



Top 10 Source IPs of the year 2024



Number of peaks per year from 2006 to 2024

✓ ~500TB of captured attack data (2005-2026)

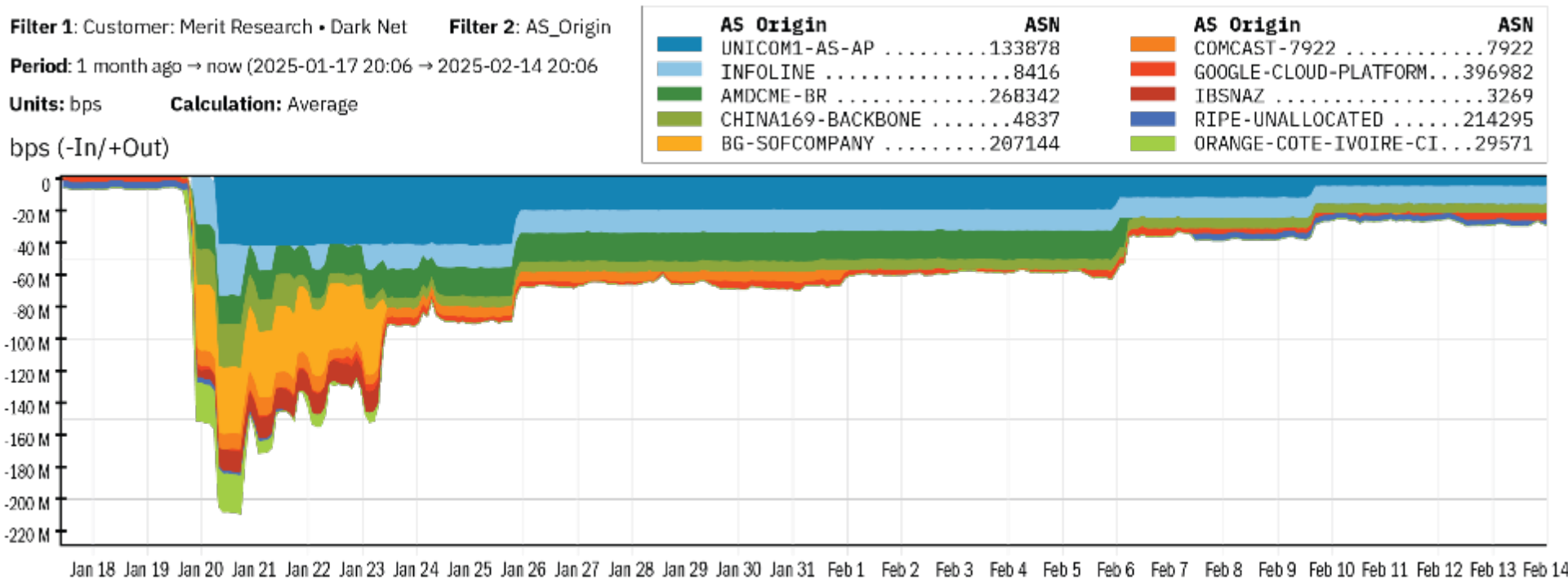
✓ 70x growth from 2005 baseline

✓ Currently capturing 6.3GB/hour (compressed)

✓ Data provided to researchers worldwide

✓ 150GB daily volume in 2025

✓ Enables threat intelligence and pattern analysis



Significant Spike in Traffic Volume at ORION (January 2025)

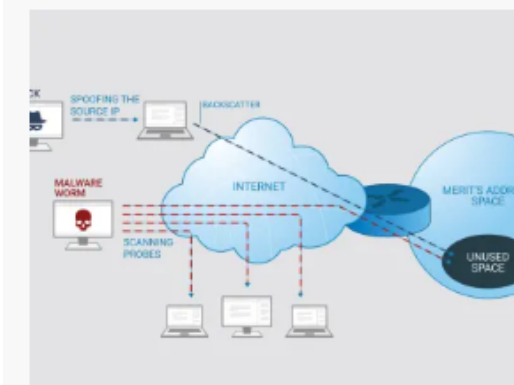


Data Sharing

- VM access (Public IP, SSH key)

- IEEE DataPort

Network Telescope "Darknet" Collected Dataset for Machine Learning-Based Cyber Threat Detection



Citation Author(s): Shereen Ismail (Merit Network, Inc.)
Submitted by: shereen ismail
Last updated: Wed, 03/11/2026 - 16:12
DOI: 10.21227/4hgj-et28
Data Format: *.csv (zip)

Research Article Link: A Lightweight Machine Learning Approach for Anomalous Unsolicited Network Traff...
Links: Merit's Orion Network Telescope

637 views

20245 downloads

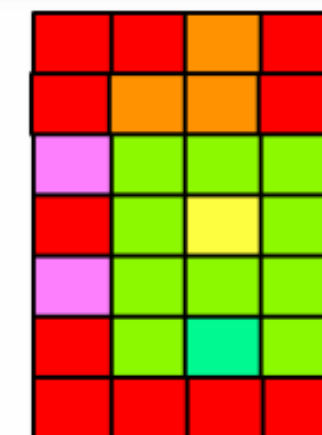
Categories: Wireless Networking

Keywords: Network Telescopes, Darknets, Unsolicited Traffic, Machine Learning, Internet Scanning, Backscatter, Internet Security, internet background radiation

CITE

SHARE/EMBED

- COMUNDA <https://comunda.isi.edu/>



COMUNDA

Community Understanding of Network Datasets

Current Research



- **Machine Learning for Cyber Threat Detection**
 - Apply supervised/semi-supervised/unsupervised ML models
 - Detect scanners, botnets, and malware patterns as well as emerging “never-seen before” threats
- **Large-Scale Data Analysis**
 - Analyze high-volumes of unsolicited traffic across multiple darknet blocks
 - Build scalable pipelines for flow-level, packet-level, and metadata extraction
- **Longitudinal Studies of Threat Evolution**
 - Perform multi-year analysis of scanning campaigns, malware families, and actor infrastructure, internet-scale threats change over time
 - Modeling the evolution of IoT malware, CVE exploitation trends, and C2 behavior
- **Dynamic Network Telescope**
 - Rotate prefixes automatically to avoid blacklisting and increase measurement diversity
 - Sustain meaningful monitoring even with IPv4 space becomes increasingly limited.

Future Research



- **Global Routing and Stability Insights**
 - Better understand BGP instability, misrouting, and prefix hijacks, misconfigurations, and global propagation irregularities
 - Assess the stability and trustworthiness of global routing paths
 - Contribute to global Internet health and routing hygiene assessments
- **Advanced AI for Threat Intelligence**
 - Enrich observations with global threat intelligence feeds
 - Automate threat classification and allow early warning of zero-day attacks.
 - Use LLM-assisted triage integrating logs, NT flows, and malware signatures
 - AI-driven correlation across honeypots, firewall logs, and NT observations
- **IPv6 Traffic Analysis**
 - Characterize unsolicited IPv6 traffic, scanning strategies, and botnet presence
 - Identifying differences between IPv4 vs. IPv6 attacker tactics
 - Prepare NT infrastructure for high-volume IPv6 darknet monitoring at scale
- **Active–Passive Hybrid Threat Sensing**
 - Transition from static → adaptive, AI-driven dynamic telescope
 - Integrate active honeypots with NT passive data for enhanced analytics

Recent Publications



WORLD AI IOT CONGRESS



7th Annual WORLD AIoT CONGRESS
Seattle Convention Center, USA (Physical Conference)
20TH - 22ND MAY, 2026

Analyzing Unsolicited Internet Traffic: Measuring IoT Security Threats via Network Telescopes

Bridging High-Level Intent and Network Execution: Detecting Violations and Intent Drift Through Low-Level Traffic Analysis

Characterizing AI-Assisted Bot Traffic in Darknet Data: Implications for ICS and IIoT Security



CERTIFICATE OF BEST PAPER
THIS IS HEREBY PRESENTED TO
SHARON SEMAIL
(University of Michigan, USA & Merit Network, Inc., USA)
FOR THE PAPER TITLED
Merit Network Telescope: Processing and Initial Insights from Nearly 20 Years of Darknet Traffic for Cybersecurity Research
IN THE CATEGORY OF
UBIQUITOUS AND PERSASIVE COMPUTING SYSTEMS
IEEE UEMCON 2025
22nd - 24th OCTOBER 2025
IBM Louis V. Gerstner, Jr. Center for Learning, NEW YORK, USA



CERTIFICATE OF BEST PRESENTER
THIS IS HEREBY PRESENTED TO
Sharon Semail
(University of Michigan, USA & Merit Network, Inc., USA)
FOR THE PAPER TITLED
Merit Network Telescope: Processing and Initial Insights from Nearly 20 Years of Darknet Traffic for Cybersecurity Research
IN THE CATEGORY OF
UBIQUITOUS AND PERSASIVE COMPUTING SYSTEMS
IEEE UEMCON 2025
22nd - 24th OCTOBER 2025
IBM Louis V. Gerstner, Jr. Center for Learning, NEW YORK, USA



CERTIFICATE OF BEST PRESENTER
THIS IS HEREBY PRESENTED TO
Sharon Semail
(University of Michigan, USA & Merit Network, Inc., USA)
FOR THE PAPER TITLED
Merit Network Telescope: Processing and Initial Insights from Nearly 20 Years of Darknet Traffic for Cybersecurity Research
IN THE CATEGORY OF
UBIQUITOUS AND PERSASIVE COMPUTING SYSTEMS
IEEE UEMCON 2025
22nd - 24th OCTOBER 2025
IBM Louis V. Gerstner, Jr. Center for Learning, NEW YORK, USA



IEEE CCWC 2025

2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)
6 -8 January 2025
University of Nevada, Las Vegas, USA



A Lightweight Machine Learning Approach for Anomalous Unsolicited Network Traffic Detection by Observing Network Telescopes



IEEE UEMCON 2025

2025 IEEE 16th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)
22 - 24 October 2025
IBM Louis V. Gerstner, Jr. Center for Learning, New York, USA



Merit Network Telescope: Processing and Initial Insights from Nearly 20 Years of Darknet Traffic for Cybersecurity Research

A Comparative Study of Packet Capture Tools for Reliable Network Telescope Traffic Collection

Characterizing Large-Scale Adversarial Activities Through Large-Scale Honey-Nets



**IEEE
cit 2025**



VALPARAISO UNIVERSITY



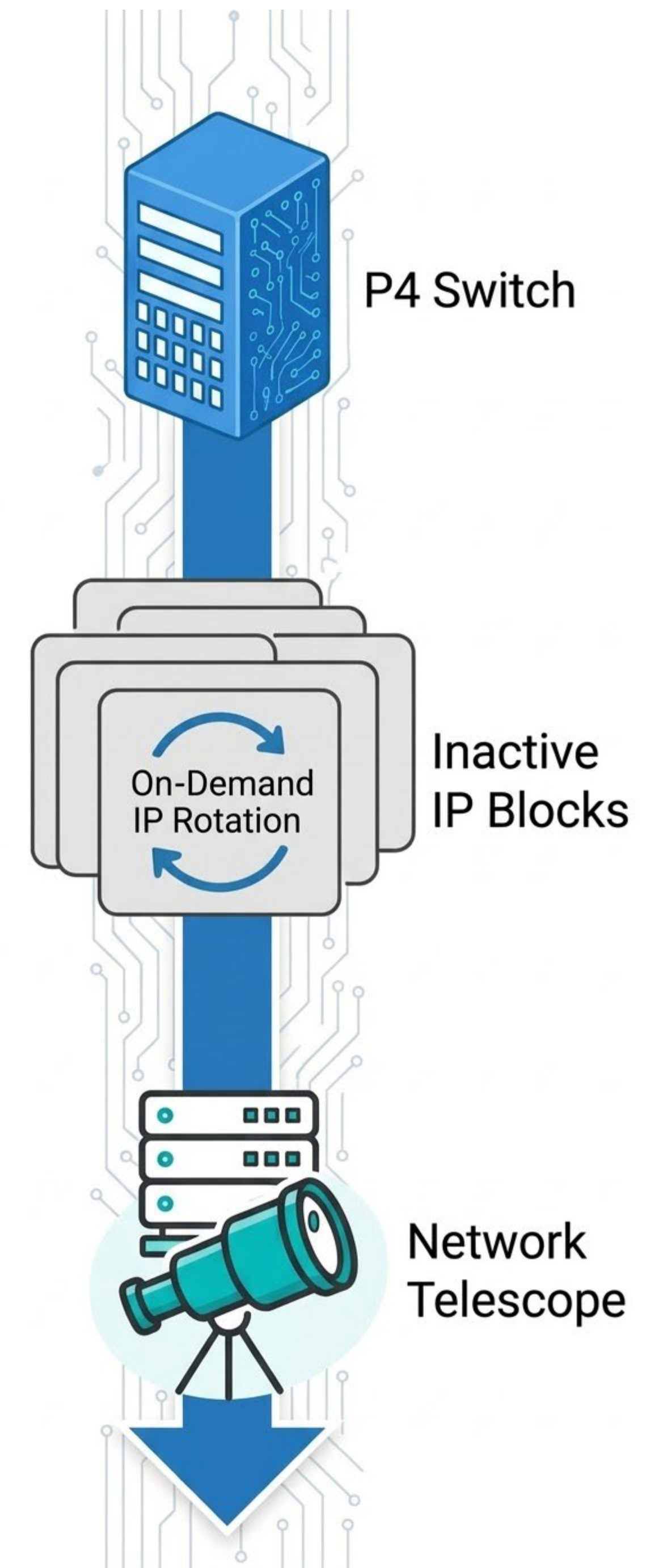
IEEE Region 4

2025 IEEE INTERNATIONAL CONFERENCE ON ELECTRO/INFORMATION TECHNOLOGY
May 29-31, 2025

Understanding Honeypots: Observing Malicious Activities Over Telnet

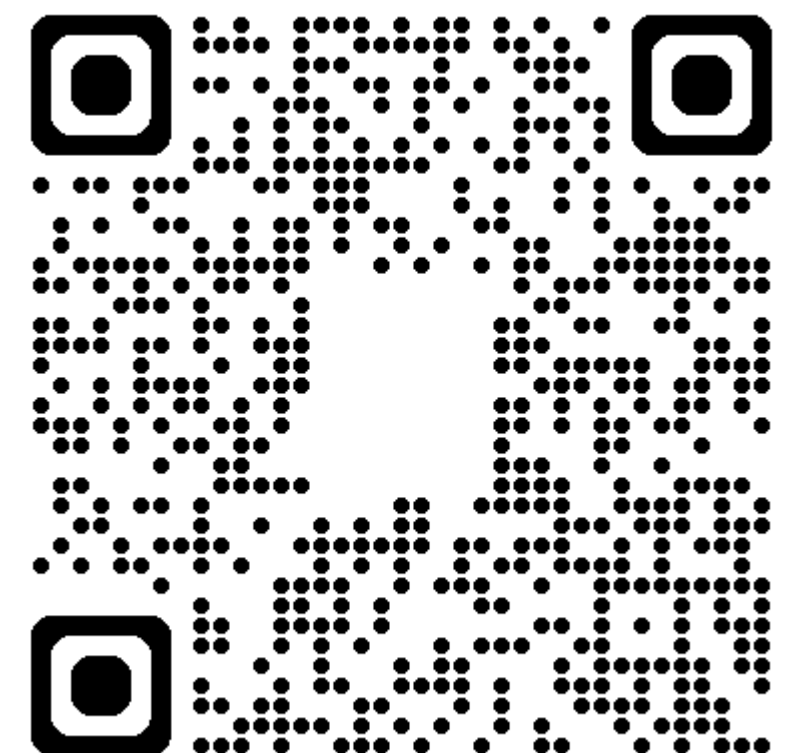
Dynamic Network Telescope Project

- Led by Georgia Tech University in collaboration with Merit Network
- Traditional static telescopes monitor fixed blocks of unused IP space
- Major telescopes have significantly scaled down:
 - CAIDA: /8 → /9 + /10 (~25% reduction)
 - Merit: /8 → /13-based (~60% reduction)
- IPv4 scarcity and rising costs force organizations to release or monetize IP space
- Smaller telescope IP ranges = less traffic visibility, greater risk of blacklisting
- Dynamic telescope enables virtual expansion of monitored space over time
- Dynamic approach uses programmable switches to watch for address blocks not being used for a set time (inactive)
- Supports on-demand IP rotation, cost control, and blacklist evasion
- Gives richer, higher-quality data



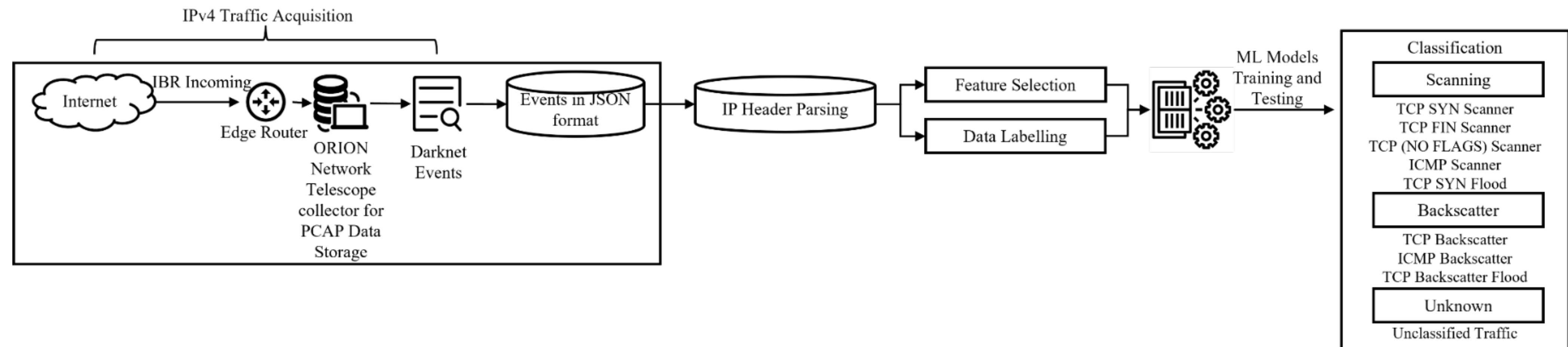
International Distributed Network Telescope (INDNT) Project

- National distributed network telescope initiative designed to provide a shared data source for researchers studying unsolicited Internet traffic.
- Distributed across multiple institutions in the U.S. that can contribute **unused IP address space**.
- Integrates participating institutions into Merit's Network Telescope, including **loaned IP prefixes** contributed by partners.

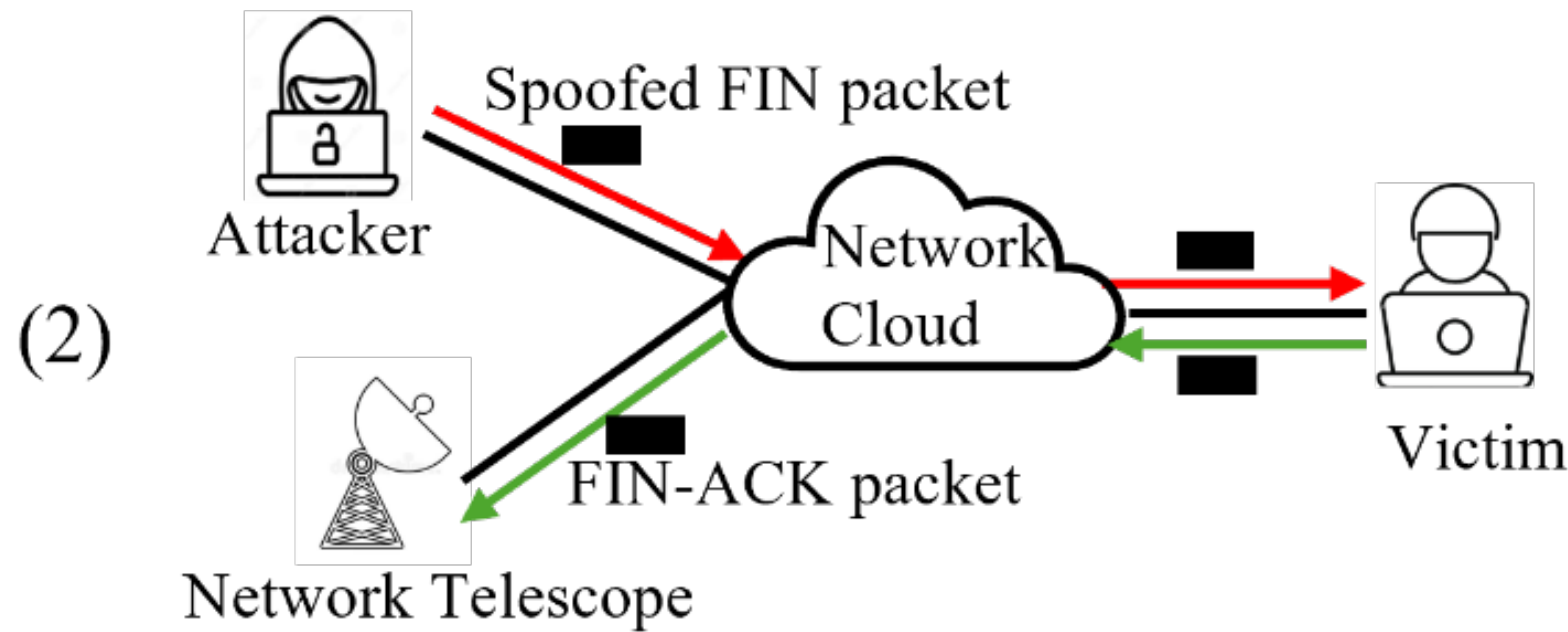
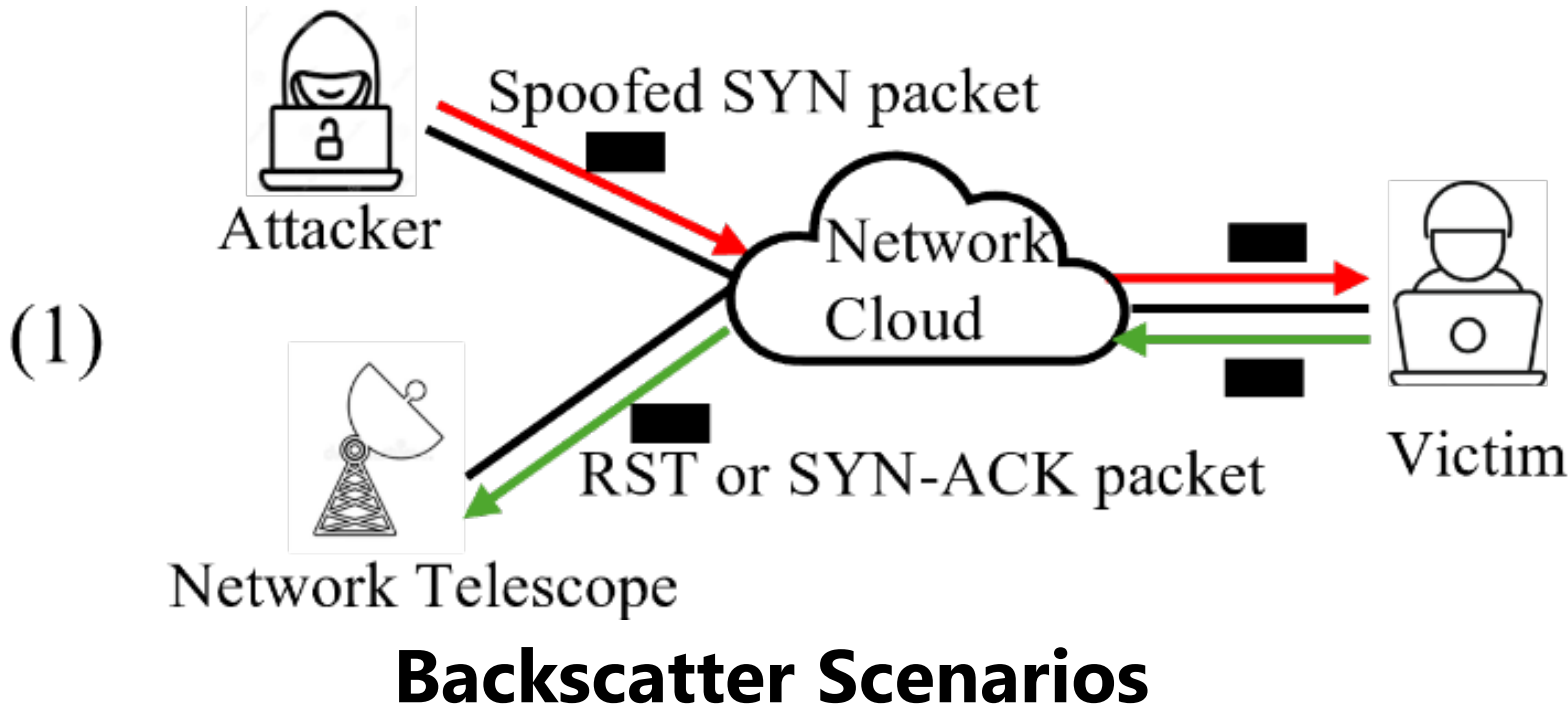


Machine Learning for Anomalous Unsolicited Network Traffic Detection by Observing Network Telescopes

- **Packet Header Analysis**
 - Utilize TCP/IPv4/ICMP header information collected from ORION to detect and classify anomalous activities.
- **Characterization and Labeling**
 - Identify and label anomalous activities, specifically scanning and backscatters, based on network characteristics observed through network telescopes.
- **Supervised Machine Learning-Based Classification**
 - Train and test multiple ML models based on extracted network traffic features, designed for near real-time deployment to identify and classify unsolicited network traffic

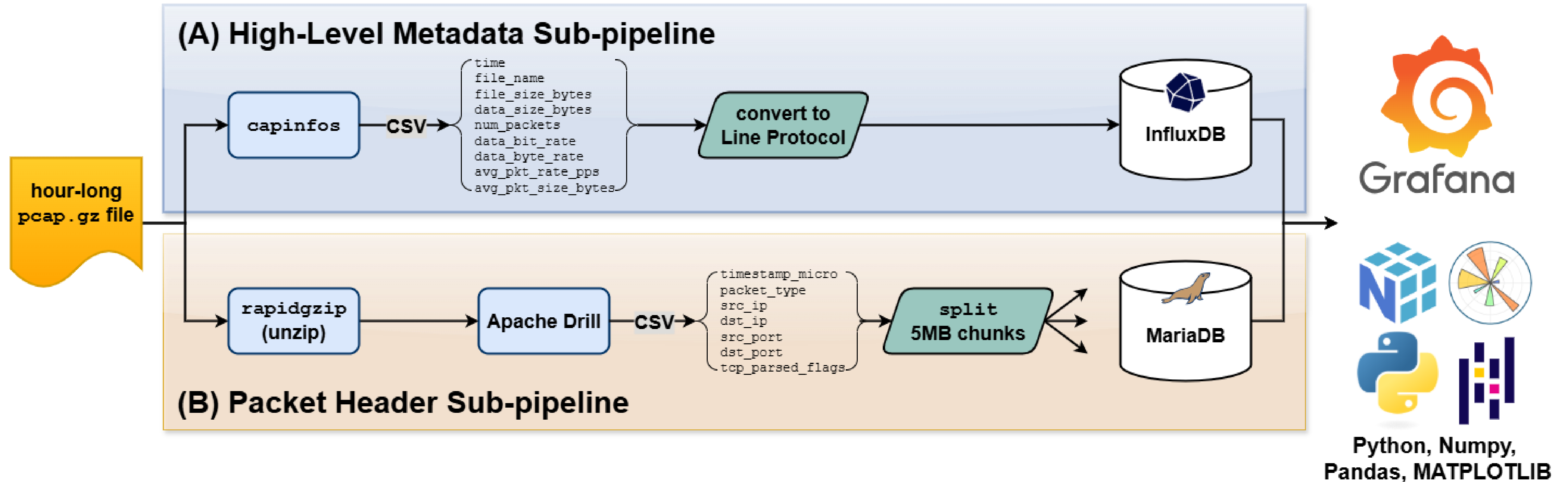


Features



Feature	Definition
SourceIP	The IP address that sent the packet(s) to the telescope.
Port	The destination TCP/UDP port that the packet(s) in this event were sent to.
Traffic	The "traffic code" that describes what kind of packet(s) were in this event.
First	The timestamp of the first packet in this event.
Last	The timestamp of the last packet in this event.
Packets	The number of packets received in this event.
Bytes	The number of bytes received in this event.
UniqueDests	The number of unique destination IP addresses in the telescope that packets were sent to.
UniqueDest24s	The number of /24s in the telescope that packets were sent to.
Lat	The SourceIP's Latitude (GeoIP).
Long	The SourceIP's Longitude (GeoIP).
Country	The SourceIP's Country (GeoIP).
City	The SourceIP's City (GeoIP).
ASN	The SourceIP's Autonomous System Number (GeoIP).
Org	The SourceIP's Autonomous System Organization Name (GeoIP).
Prefix	The SourceIP's subnet that's announced (pfx2as).
RDNS	The SourceIP's Reverse Pointer (PFX record in DNS).
Zmap	Whether all packets in the event have the IPv4 Header's Identification field set to 54321, which suggests that zmap was used.
Masscan	Whether all packets in the event have the IPv4 Header's Identification field set to the packet's Destination IP XOR Destination Port XOR TCP Sequence Number, which suggests that masscan was used.
Mirai	Whether all packets in the event have the TCP Sequence number set to the same unsigned integer value as the Destination IP.
Samples_X	Base64 encoded sample of a packet received in the event.
TCP	Text version of Traffic field for TCP events.
ICMP	Text version of Traffic field for ICMP events.
SYN	Whether the SYN flag is set in the TCP header.
ACK	Whether the ACK flag is set in the TCP header.
FIN	Whether the FIN flag is set in the TCP header.
PSH	Whether the PSH flag is set in the TCP header.
URG	Whether the URG flag is set in the TCP header.
EventType	Has six possible values. Whether the event can be confidently identified as a Scanning event, a Backscatter event, or an Unknown event.

Visualization and Dashboarding



Observations and Trends

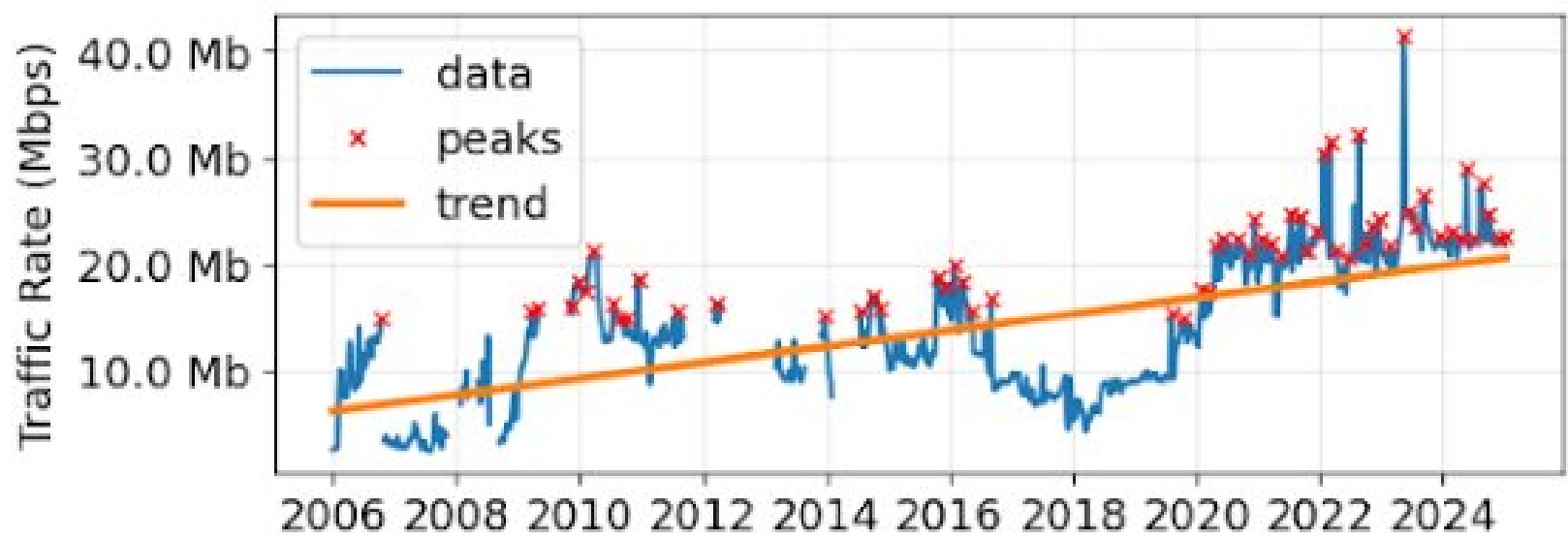
Long-term trends and traffic spikes in darknet data over the years 2006 to 2024.



(A)



(B)



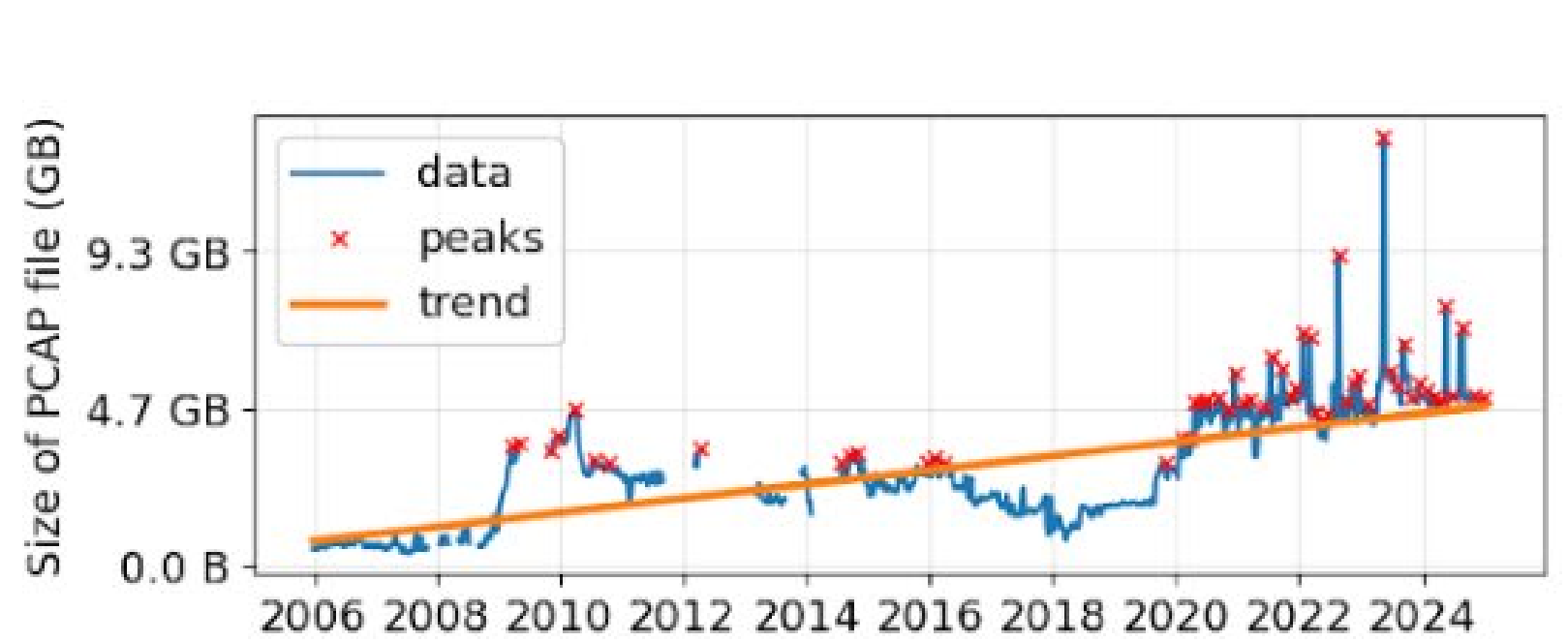
(C)



(D)



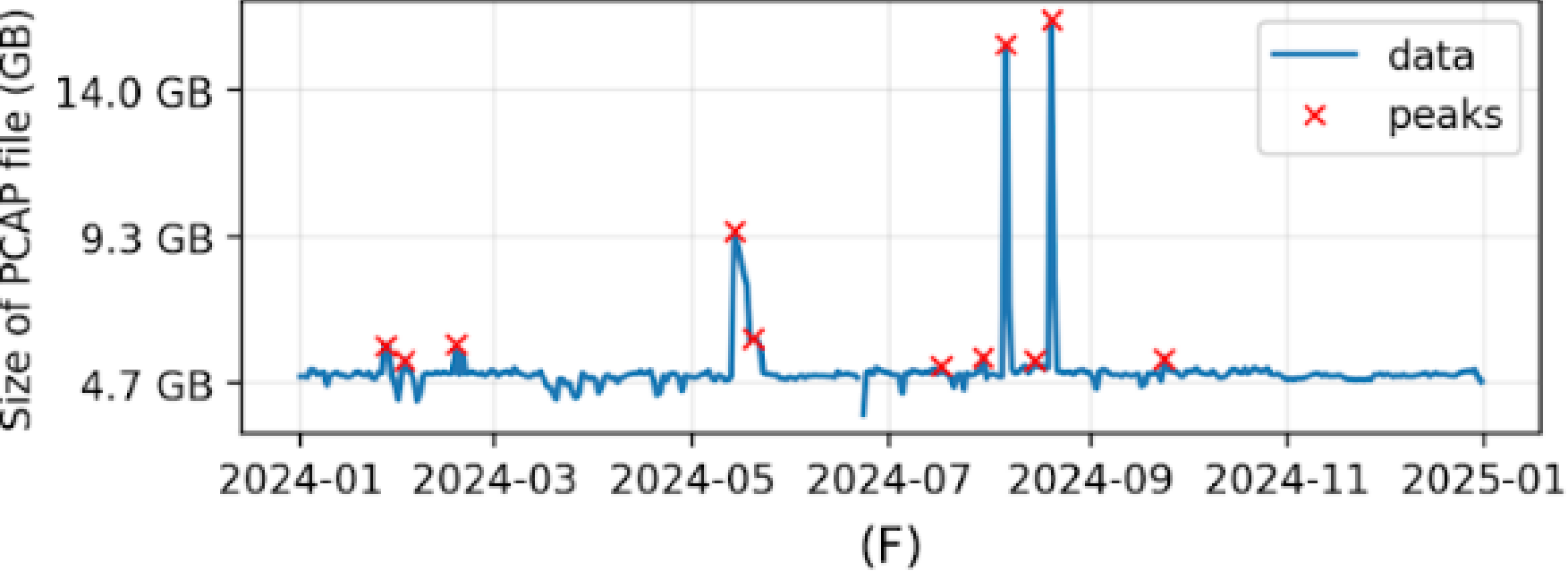
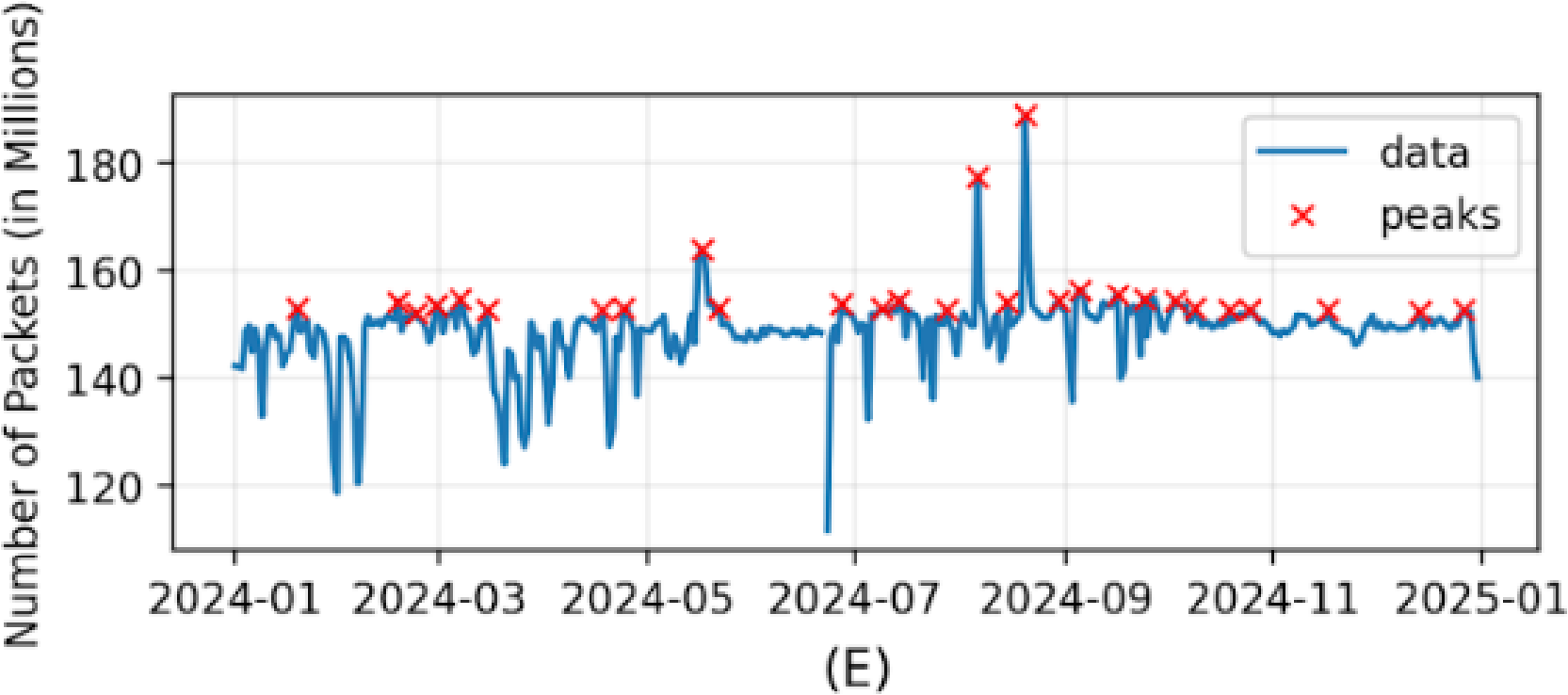
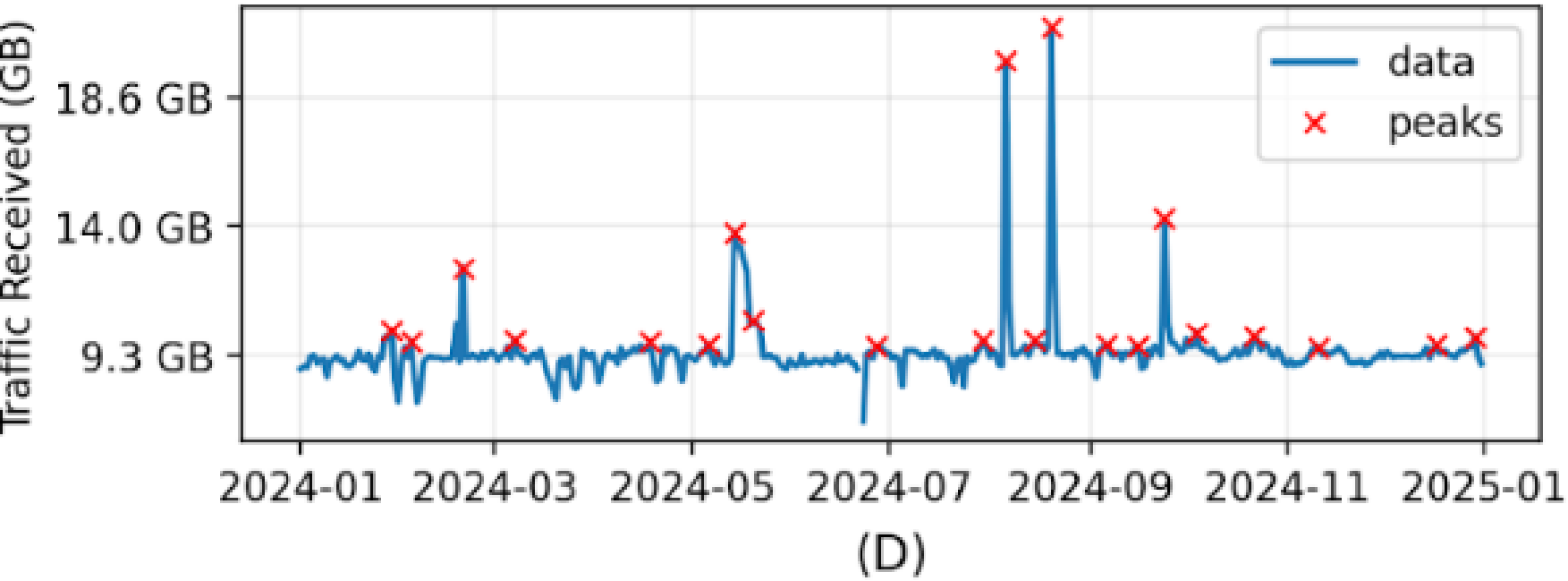
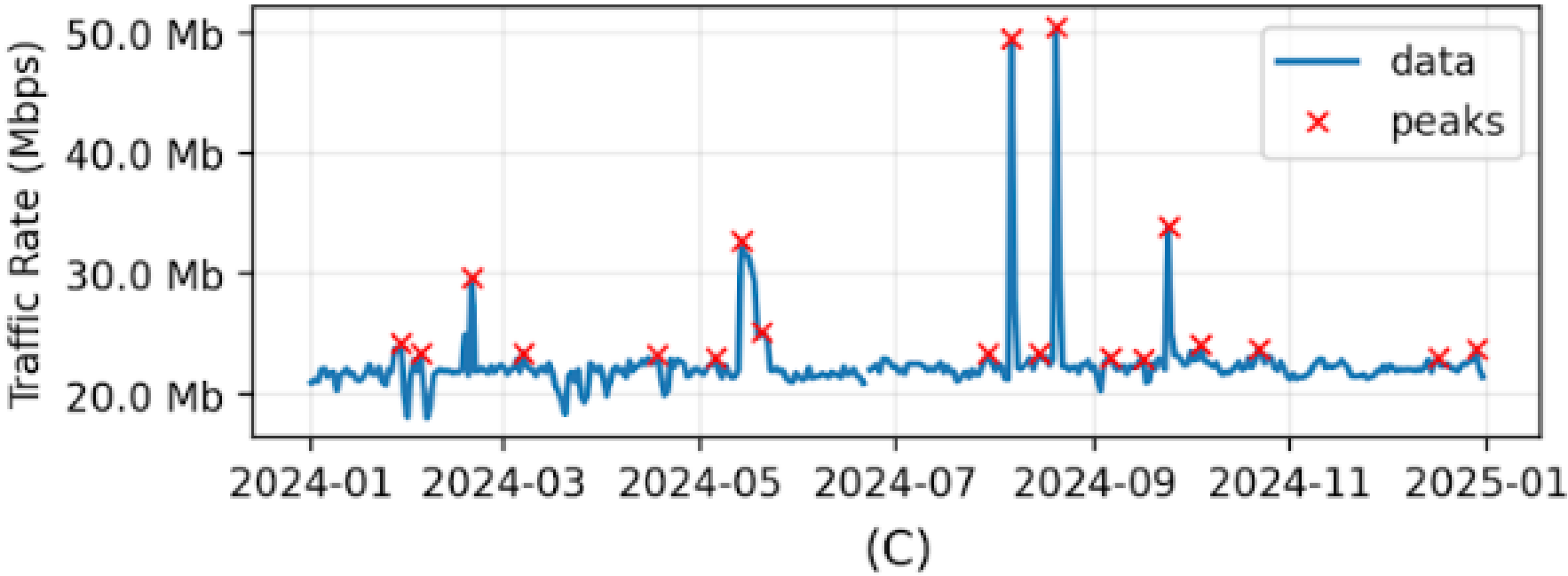
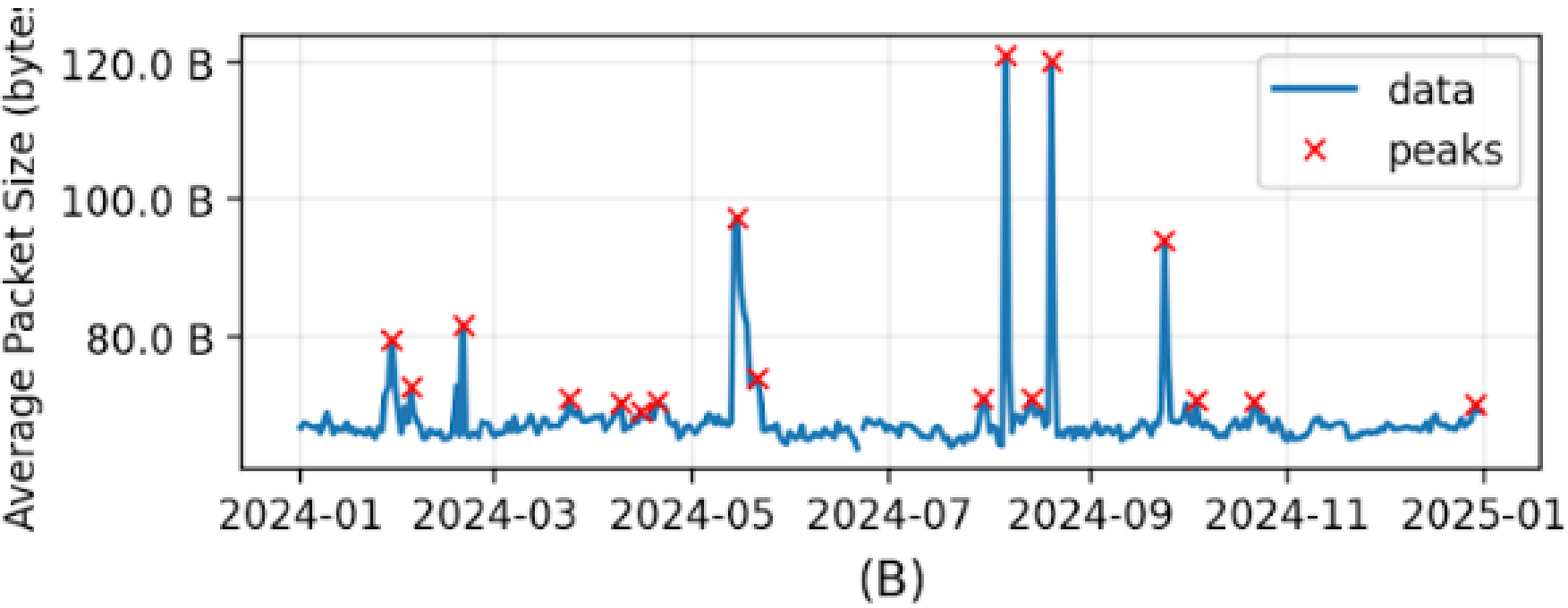
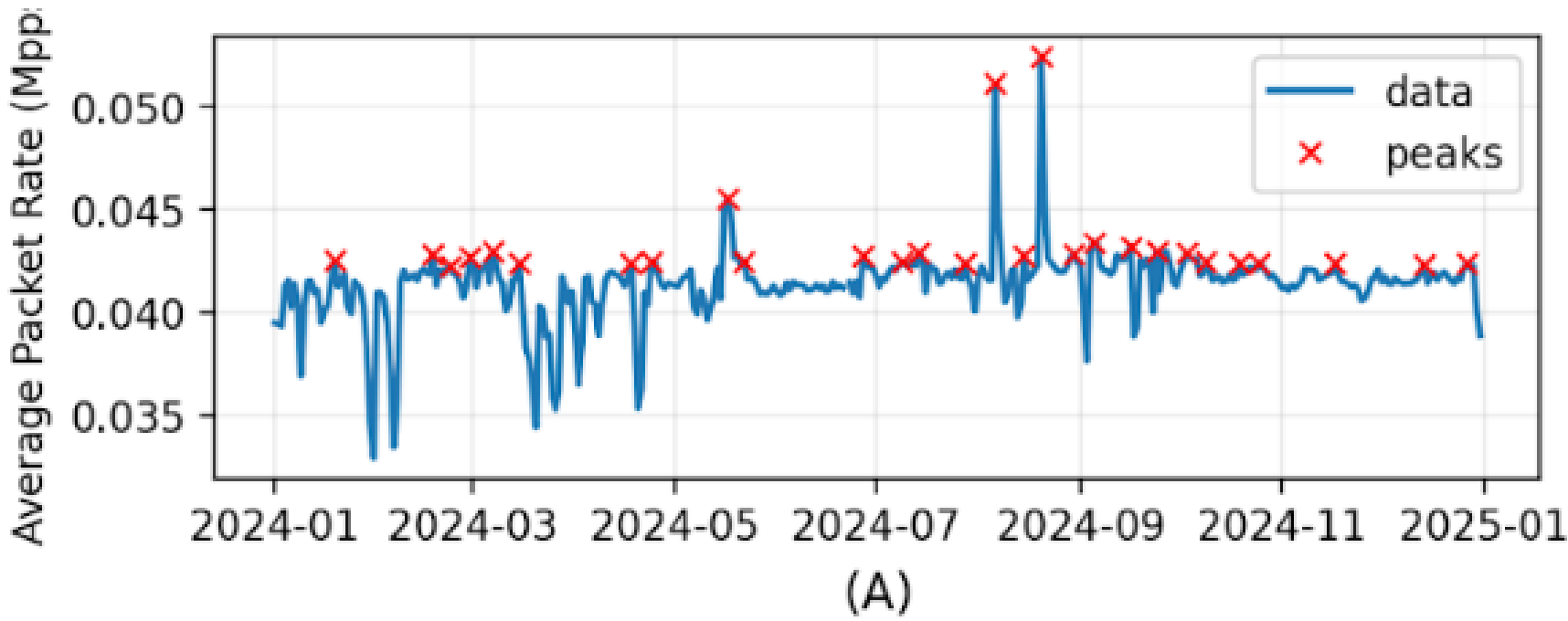
(E)



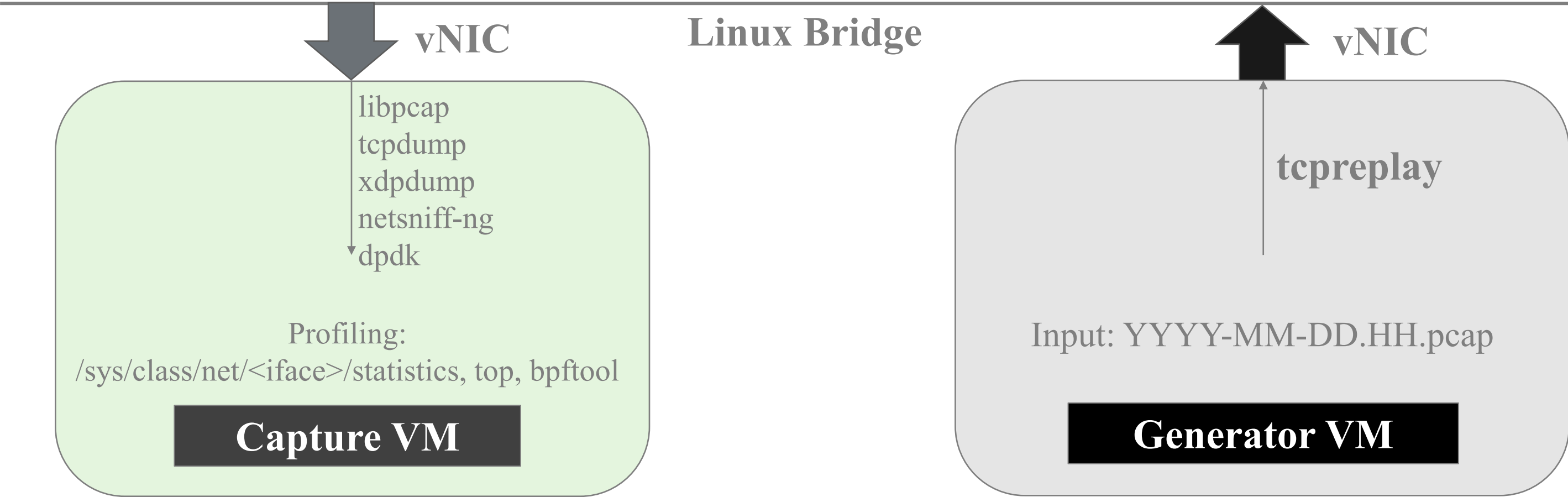
(F)

Observations and Trends (cont.)

Traffic trends and spikes in darknet data in the year 2024.

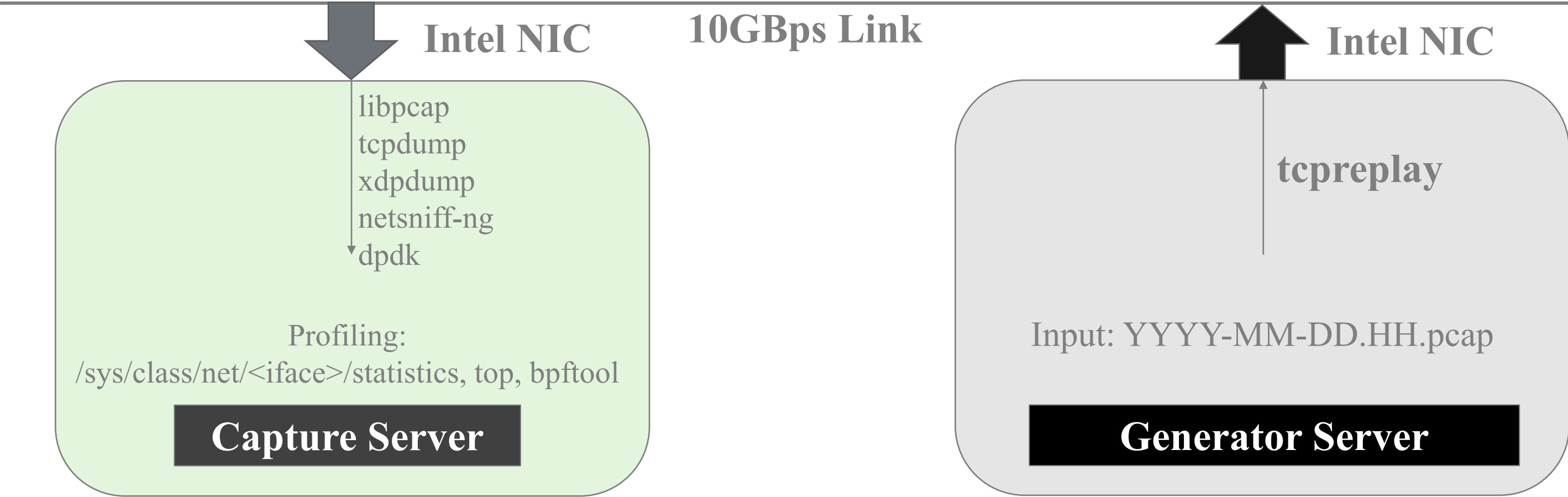


A Comparative Study of Packet Capture Tools for Reliable Network Telescope Traffic Collection



(a) Virtual Machines Setup

Tool	Virtualized Environment				Physical Environment			
	Memory Usage	CPU Usage	Drop Rate	Disk Throughput	Memory Usage	CPU Usage	Drop Rate	Disk Throughput
libpcap	5.3 KB	26.7% ❌	0%	2.03 MB/s ❌	5.2 MB	45%	0%	28.06 MB/s ❌
tcpdump	3.9 KB ✅	13%	0%	2.86 MB/s	3.1 KB ✅	81.1% ❌	0%	86.76 MB/s
netsniff-ng	150 MB ❌	1.7% ✅	0%	2.93 MB/s	2.4 GB ❌	15.7% ✅	0%	86.43 MB/s
xdpdump	4.5 KB	8.7%	0%	3.75 MB/s ✅	10 MB	20%	0%	4.67 MB/s
dpdk DUMPCAP	-	-	-	-	36 MB	85%	0%	211.07 MB/s ✅



(b) Physical Hardware Servers Setup

Researchers and Student Collaborators





Thank you!
Email: research@merit.edu