DIFO432180 - Digital Forensics

Week 5: Network Forensics Fundamentals

PhD. Nguyen Ngoc Tu

September 18, 2025

Motivations – Classic View (Động cơ – Góc nhìn truyền thống)

- **Cyberattacks increasingly rely on network vectors** (Tấn công mạng ngày càng tinh vi):
  - **Phishing (tấn công lừa đảo qua email/mạng xã hội)**
  - **Lateral movement (di chuyển ngang trong hệ thống)**
  - **Data exfiltration (rò rỉ/đánh cắp dữ liệu ra ngoài)**
- **Network Forensics (Điều tra số trên mạng)** cho phép:
  - **Capture (Thu thập)**: gói tin, luồng (packet, flow)
  - **Analyze (Phân tích)**: phát hiện hành vi bất thường
  - **Reconstruct (Tái dựng)**: ghép lại phiên giao dịch, sự kiện
- **Essential for (Ứng dụng thiết yếu):**
  - Intrusion detection & incident response (Phát hiện xâm nhập & ứng phó sự cố)
  - Regulatory compliance (Tuân thủ pháp lý: GDPR, Luật An ninh mạng VN)
  - Court-admissible digital evidence (Bằng chứng số có giá trị pháp lý)
- **CHFI v10 Module 08:** Network Forensics → Capture (thu thập), Reduce (lọc nhiễu), Reconstruct (tái dựng), Correlate (tương quan)

Motivations – Modern View (Động cơ – Bối cảnh hiện đại)

- **DevOps (Phát triển + Vận hành):**
  - Hệ thống CI/CD thay đổi liên tục → bề mặt tấn công động
  - Network Forensics giúp giám sát, phân tích API, container, microservices, applications
- **DevSecOps (Bảo mật tích hợp vào DevOps):**
  - Pentesting (kiểm thử thâm nhập) trong pipeline
  - Phát hiện cấu hình sai (misconfiguration) hoặc rò rỉ dữ liệu
  - Cung cấp *forensic artifacts* (bằng chứng số) khi pipeline bị khai thác
- **SecOps / SOC (Vận hành an ninh):**
  - Kết nối giám sát an ninh (security monitoring) với điều tra số
  - Điều tra cảnh báo (alert) bằng cách tái dựng traffic thật sự
  - Cung cấp bằng chứng cho quy trình Incident Response (Ứng phó sự cố)
- **Tóm lại:** Network Forensics ngày nay không chỉ phục vụ pháp lý và compliance, mà còn trở thành **năng lực cốt lõi trong DevSecOps và SecOps hiện đại**.

Warm-up Activities (Hoạt động khởi động) – Part 1

Scenario (Tình huống): Your company (doanh nghiệp) detects unusual outbound traffic (lưu lượng ra ngoài bất thường).

1. **Think-Pair-Share (Suy nghĩ – Thảo luận cặp – Chia sẻ lớp)** What logs would you check first? (Bạn sẽ kiểm tra nhật ký nào đầu tiên?)
   - Firewall logs (nhật ký tường lửa): kiểm tra địa chỉ IP/tên miền đích.
   - DNS logs (nhật ký DNS): phát hiện truy vấn tên miền lạ.
   - Proxy logs (nhật ký Proxy): xác định nội dung web bị truy cập.
2. **Quick demo** Wireshark shows a suspicious DNS query (Wireshark hiển thị một truy vấn DNS bất thường):
   - Ví dụ: `abc123.malicious-domain.xyz`
   - Dấu hiệu: DNS tunneling hoặc kết nối đến máy chủ C2.
   - Filter trong Wireshark: `dns && dns.qry.name contains "xyz"`

Warm-up Activities (Hoạt động khởi động) – Part 2

Group brainstorm (Động não nhóm) Which evidence sources (nguồn bằng chứng) exist in different environments? (Sinh viên lựa chọn loại log nào quan trọng nhất cho từng môi trường)

Environment (Môi trường)	**Possible Evidence Sources (Các nguồn có thể có)**
SMB (Doanh nghiệp nhỏ)	Firewall logs, router logs, proxy logs, endpoint antivirus, simple syslog
University (Trường đại học)	DHCP logs, VPN logs, DNS resolver logs, SIEM, IDS/IPS, web proxy
ISP (Nhà cung cấp dịch vụ Internet)	NetFlow/IPFIX, DNS resolver logs, RADIUS logs, IDS/IPS, backbone router logs

Key lesson (Bài học chính):

- Không phải tất cả log đều tồn tại trong mọi môi trường.
- Cần *chọn lọc và tranh luận* nguồn log nào là quan trọng nhất.

Forensic Process & CHFI / NIST Mapping (Quy trình điều tra)

- Map CHFI v10 Module 08: Capture → Reduce → Reconstruct → Correlate (CHFI).
- Map NIST SP 800-86 / Alansari: Identification, Verification, Gathering, Preservation, Examination, Analysis, Reporting.
- Practical implication: mỗi bước cần artifact cụ thể (pcap, flow, DHCP log), và checkpoint (hash, metadata).

Forensic Process Models (Mô hình điều tra số)

- **NIST SP 800-86**: tích hợp forensic vào quy trình ứng phó sự cố.
- **Alansari 6-phase model:** Identification (Nhận dạng), Verification (Xác minh), Gathering (Thu thập), Preservation (Bảo quản), Examination (Kiểm tra), Analysis (Phân tích), Reporting (Báo cáo).
- Điểm chung: nhấn mạnh **chain-of-custody (chuỗi lưu giữ)** và sử dụng NFATs.

Comparative Process Models (NIST vs Alansari vs CHFI)

NIST SP 800-86	**Alansari (2023)**	**CHFI v10 (Module 08)**
Collection	Identification & Verification	Capture
Examination	Gathering & Preservation	Reduce/Filter
Analysis	Examination & Analysis	Reconstruct sessions
Reporting	Reporting	Correlation + Report

Timekeeping & Timestamp Accuracy (Đồng bộ thời gian & Timestamp)

- Always use UTC timestamps; record timezone/NTP server used (Ghi UTC, lưu NTP).
- Common issues: clock skew giữa router, endpoints, capture boxes → ảnh hưởng timeline.
- Practical: capture with high-precision timestamps (e.g. libpcap nanoseconds), record device sysinfo and NTP offsets.
- Instructor note: show example clock skew correction when building timeline.

Timestamp Normalization (Chuẩn hoá dấu thời gian) – Windows Host

Goal (Mục tiêu): build one trustworthy timeline across devices.

1. Challenges (Thách thức)

- Devices use different timezones (múi giờ khác nhau).
- Windows Event Log uses local time (giờ địa phương), not always UTC.
- NTP misconfiguration → clock skew (đồng hồ lệch).

2. Windows Example (Ví dụ Windows)

Convert Event Logs to UTC with PowerShell:

```
Get-WinEvent -LogName Security |
  Select-Object -First 5 @{Name="UTCTime";
    Expression={$_.TimeCreated.ToUniversalTime()}}, Id, Message
```

Check NTP configuration and offsets:

```
w32tm /query /status
```

3. Integration (Tích hợp)

- Align Zeek logs (epoch → UTC) with Windows Event Logs.
- Note and annotate clock skew corrections in incident timeline.

Timestamp Normalization (Chuẩn hoá dấu thời gian) – Ubuntu/Linux Host

1. Linux Characteristics (Đặc điểm Linux)

- Syslog usually in localtime (giờ địa phương).
- Journalctl (systemd) stores monotonic + realtime timestamps.
- NTP/chrony maintain offset info.

2. Linux Example (Ví dụ Ubuntu)

Convert Syslog timestamps to UTC:

```
journalctl --utc --since "2025-09-18 09:00"
```

Check NTP offset:

```
timedatectl status
chronyc tracking
```

Parse Zeek logs into UTC:

```
cat conn.log | zeek-cut -d ts id.orig_h id.resp_h > conn_utc.tsv
```

3. Callout (Lưu ý)

- Normalize all sources (firewall, DNS, endpoint) to UTC.

Chain of Custody & Evidence Preservation (Chuỗi lưu giữ & Bảo quản)

- For each artifact: record collector, time, tool/version, SHA256 hash, storage path, access log.
- Source preservation: store read-only copy; keep original capture and working copy; note capture filters used.
- Legal note: prepare exportable report + verified hashes for court-admissible evidence.

Evidence Integrity & Immutability

Hash Manifest Example (SHA-256), HMAC (optional):

```
file: session1.pcap
sha256: 91bd4fa8b8...c5f2
```

- Compute **before & after** every transfer or parse.
- Export logs to **WORM storage** (e.g., S3 Object Lock, immutable buckets).
- Use built-in features (e.g., CloudTrail log file validation) where available.
- Document chain-of-custody (time, handler, hash).

Packets (Gói tin) vs. Flows (Luồng) vs. Logs (Nhật ký)

- **Packets (pcap, Gói tin):** full capture, low-level headers, payloads.
  - Ví dụ: PCAP chứa toàn bộ HTTP GET request với header & payload.
- **Flows (NetFlow/IPFIX, Luồng):** summarized traffic (5-tuple: srcIP, dstIP, srcPort, dstPort, protocol).
  - Ví dụ: NetFlow record cho thấy luồng TCP từ 10.0.0.5:12345 đến 8.8.8.8:53 (DNS).
- **Logs (Nhật ký):** sự kiện được ghi lại từ hạ tầng mạng hoặc end-host.
  - *Network/Middleware logs (nhật ký hạ tầng):* Firewall, DNS, DHCP, Proxy, VPN, IDS/IPS.
  - *End-host logs (nhật ký máy trạm/mindware):* Windows Event Log, Syslog (Linux), ứng dụng bảo mật EDR.
  - Ví dụ: `Zeek` sinh `conn.log`, `http.log`, `dns.log`, `ssl.log`.

Packets (PCAP, Gói tin)

1. Definition & Characteristics (Định nghĩa & Đặc điểm)

- **Packets (Gói tin):** smallest unit of network traffic, includes *headers (tiêu đề)* + *payload (dữ liệu tải)*.
- **PCAP (Packet Capture file):** standard format to store raw packets.
- Characteristics:
  - Most detailed view (chi tiết nhất), can reconstruct full sessions.
  - Very large in size (dễ phình to), difficult to retain long-term.

2. How to Collect (Cách thu thập)

- Passive capture (nghe lén): tcpdump, Wireshark, SPAN port, network tap.
- Inline capture (chèn luồng): IDS/IPS, firewall with raw packet logging.
- Host-level capture (máy trạm): Windows `netsh trace`, Linux `tcpdump`.
- Preserve with hashes (SHA256) and store read-only (*chuỗi lưu giữ bằng chứng*).

Packets (PCAP, Gói tin)

3. Useful Information (Thông tin hữu ích)

- L2/L3: MAC, IP addresses, TTL, fragmentation.
- L4: TCP/UDP ports, flags (SYN, ACK, RST), sequence numbers.
- L7:
  - HTTP requests/responses (URI, cookies, files).
  - DNS queries/responses (tên miền, IP).
  - TLS handshakes (SNI, certificates, JA3).
- Reconstruction (Tái dựng): full sessions, extracted files, attack payloads.
- Example: CIC-IDS2017: https://www.unb.ca/cic/datasets/ids-2017.html

Flows (NetFlow/IPFIX, Luồng)

1. Definition & Characteristics (Định nghĩa & Đặc điểm)

- **Flows (Luồng):** summarized record of communication between two endpoints.
- Defined by **5-tuple (5 thành phần):** srcIP, dstIP, srcPort, dstPort, protocol.
- Standards:
  - **NetFlow** (Cisco) – widely deployed.
  - **IPFIX** (IETF standard) – flexible extensions.
- Characteristics:
  - Lightweight (gọn nhẹ) compared to PCAP.
  - Scales well for large networks (ISP, data center).
  - Cannot recover payload (không có nội dung ứng dụng).

2. How to Collect (Cách thu thập)

- Routers/switches export NetFlow/IPFIX records.
- Flow collectors (ví dụ: nfdump, SiLK, ELK integration).
- Cloud providers: VPC Flow Logs (AWS, Azure, GCP).

Flows (NetFlow/IPFIX, Luồng) – Analysis

3. Useful Information (Thông tin hữu ích)

- Communication patterns (mô hình giao tiếp):
  - Who talks to whom? (IP nguồn IP đích).
  - Frequency, duration, volume (số byte, số gói).
- Detect anomalies:
  - Port scans (quét cổng), DoS/DDoS (khối lượng bất thường).
  - Data exfiltration (rò rỉ dữ liệu) – long duration, large bytes.
  - Botnet C2 (điều khiển từ xa) – beaconing with fixed interval.
- Correlation (Tương quan):
  - Combine with DHCP logs → identify host.
  - Feed into SIEM → timeline of incidents.

Example (Ví dụ): `10.0.0.5:12345 → 8.8.8.8:53 (UDP, 45 packets, 2 KB, duration 5s)` → repeated every 30s → possible DNS tunneling.

Flow Fidelity: Timeouts & Sampling

- **Active timeout**: exporter emits long-lived flows every N seconds.
- **Inactive timeout**: flow exported after silence (e.g., 15s).
- **Sampling**: 1/100 or hardware sampling can undercount bytes.
- **Forensics tip**: When quantifying exfil, state sampling/timeout settings to avoid misestimation.

Encrypted Traffic Challenges (Thách thức phân tích lưu lượng mã hoá)

1. **Why it is difficult (Tại sao khó)**
   - **Payload hidden (ẩn nội dung):** TLS/SSL, QUIC encrypt application data → cannot see commands or files.
   - **Protocol evolution:** new versions (TLS 1.3, QUIC) encrypt even handshake fields.
   - **Pervasive encryption (mã hoá toàn diện):** >80% web traffic today is HTTPS.
   - **False negatives:** malicious traffic (C2, exfiltration) looks "normal" when encrypted.
   - **False positives:** without payload, anomaly detection may trigger too many alerts.
2. **Typical forensic impact (Ảnh hưởng đến điều tra)**
   - Harder to reconstruct full sessions or extract malware.
   - Attribution challenge: cannot directly see commands or data exfiltrated.

Encrypted Traffic Solutions (Giải pháp phân tích lưu lượng mã hoá)

1. **Metadata analysis (Phân tích siêu dữ liệu)**
   - TLS handshake fields: **SNI (Server Name Indication)**, **ALPN**, **TLS version**, certificate CN/issuer.
   - Flow features: packet sizes, burst patterns, inter-arrival timing (IAT).
   - QUIC metadata: connection IDs, version, packet length.
2. **Fingerprints & heuristics (Dấu vết và kinh nghiệm)**
   - **JA3/JA3S fingerprints:** hash of TLS ClientHello / ServerHello for identifying malware families.
   - Detect beaconing (traffic at fixed intervals) $\rightarrow$ often C2 channels.
   - DNS tunneling detection: many small queries, high-entropy domains.
3. **Practical tools (Công cụ thực hành)**
   - **Wireshark filters:** `tls.handshake.type == 1` (Client Hello), `quic`.
   - Zeek scripts: extract SSL certificate logs, JA3 fingerprints.
   - SIEM rules: correlate unusual SNI with threat intel.

Scaling & Flow Strategies (Quy mô & Chiến lược luồng mạng)

1. Why we need scaling (Tại sao cần quy mô hoá)

- Network traffic volume grows rapidly (khối lượng lưu lượng tăng nhanh).
- Storing all packets (pcap) is impractical for weeks/months → storage & performance issues.
- Investigators need both *breadth* (xu hướng toàn mạng) and *depth* (chi tiết gói tin).

2. Strategies (Chiến lược)

- Use **flows (luồng)** for long-term monitoring, trend analysis, IDS triage.
- Keep **sampled/aggregated pcaps** only for deep-dive investigations.

3. Retention (Lưu trữ)

- Hot storage (7–30 days): full fidelity for fast query.
- Warm storage (3–12 months): aggregated/flow-level only.
- Cold archival (nhiều năm): compressed logs for compliance.

4. SIEM indexing (Chỉ mục trong SIEM)

- Index logs with good field mappings (IP, port, user, timestamp).
- Enables quick correlation (tương quan nhanh) across firewall, DNS, DHCP, proxy.

Logs (Nhật ký mạng / middleware)

1. Definition & Characteristics (Định nghĩa & Đặc điểm)

- **Logs (Nhật ký):** structured records of events (các sự kiện) created by systems or applications.
- **Network / middleware logs (nhật ký hạ tầng mạng):**
  - Firewall logs (tường lửa) – allow/deny traffic, NAT mappings.
  - Gateway / Proxy logs – HTTP requests, URLs, users.
  - IDS/IPS alerts – signatures, anomaly detection.
  - VPN logs – authentication, session duration, source IP.
- Characteristics:
  - Higher-level view than packets (ít chi tiết hơn gói tin).
  - Usually pre-parsed, structured (JSON, CSV, syslog).
  - Persistent and easier to store long-term.

Logs (Nhật ký mạng / middleware) – Collection

2. How to Collect (Cách thu thập)

- Export to SIEM (Splunk, ELK, Graylog) via syslog or API.
- Configure firewalls, proxies, IDS/IPS to forward logs centrally.
- Cloud equivalents: AWS CloudTrail, Azure NSG Flow Logs.
- Preserve integrity with hashing or write-once storage (WORM).

3. Useful Information (Thông tin hữu ích)

- Firewall: source/destination IP, port, action (allow/deny).
- Proxy: full URL, user identity, timestamps.
- IDS/IPS: attack signatures, severity, payload snippet.
- VPN: user login, session start/stop, device info.

Example (Ví dụ): `2025-09-18 10:15:23 Firewall DENY 192.168.1.10` → `203.0.113.50:22 (SSH)` → suspicious outbound SSH attempt.

Logs (Nhật ký máy trạm / ứng dụng)

1. **Definition & Characteristics (Định nghĩa & Đặc điểm)**
   - **Host logs (nhật ký máy trạm):**
     - Windows Event Log: Security, System, Application.
     - Syslog (Linux/Unix): authentication, kernel, services.
     - Endpoint Detection & Response (EDR): process creation, network activity.
   - **Application logs (nhật ký ứng dụng):**
     - Web server (Apache/Nginx) – access, error.
     - Database logs – queries, authentication failures.
     - Email server – send/receive metadata.
   - Characteristics:
     - Provide context of user activity (hành vi người dùng).
     - Rich semantic information, but often fragmented across systems.

Logs (Nhật ký máy trạm / ứng dụng) – Analysis

2. How to Collect (Cách thu thập)

- Use agents (Sysmon, osquery, Wazuh) to collect host logs.
- Centralize via SIEM or log collectors.
- Cloud services: Azure Sentinel, Google Chronicle.

3. Useful Information (Thông tin hữu ích)

- Windows Event ID 4624 – successful logon, ID 4625 – failed logon.
- Syslog: SSH login attempts, sudo usage.
- EDR: process hashes, parent-child relationships.
- Application logs: unusual queries, large file transfers, mail relays.

Example (Ví dụ): `Sep 18 11:02:15 server sshd[1032]: Failed password for user admin from 203.0.113.20 port 44512` → brute-force attack attempt detected.

Threat-Hunting Playbooks & Example Queries (Playbook săn mối đe dọa)

1. Why Playbooks? (Tại sao cần playbook)

- Provide repeatable steps (các bước lặp lại được) for analysts.
- Reduce time-to-detect (giảm thời gian phát hiện).
- Ensure consistent quality across SOC/IR teams.

2. Example Queries / Commands (Ví dụ lệnh truy vấn)

- **Zeek:** detect abnormal DNS activity
  - Many short queries from one host.
  - High-entropy domains (tên miền ngẫu nhiên).
- **Wireshark/tcpdump:**
  - Capture traffic: `tcpdump -i eth0 -w capture.pcap`
  - Filter DNS: `dns && dns.qry.name contains "xyz"`
- **SIEM (Splunk/ELK):** `index=dns sourcetype=zeek_dns qtype=A | stats count by src_ip, query`

Threat-Hunting Playbooks & Example Queries (Playbook săn mối đe dọa)

3. 3-Step Playbook (Quy trình 3 bước)

1. **Triage (Sơ loại):** summarize flows (ai nói chuyện với ai, tần suất).
2. **Enrich (Bổ sung thông tin):** resolve domains, WHOIS, threat intel feeds.
3. **Deep-dive (Phân tích sâu):** inspect PCAP, host logs, reconstruct session.

4. Example (Ví dụ minh hoạ) `Host 10.0.5.23 sends 500 DNS queries/hour to random domains → WHOIS shows no registration → PCAP reveals DNS tunneling C2 channel.`

Log Sources and Correlation (Nguồn nhật ký và Tương quan)

- Key evidence sources (Nguồn bằng chứng chính):
  - Firewall logs (Nhật ký tường lửa)
  - DNS logs (Nhật ký DNS)
  - DHCP logs (Nhật ký cấp phát IP)
  - Proxy logs (Nhật ký Proxy)
  - VPN logs (Nhật ký VPN)
  - IDS/IPS (Snort, Suricata)
  - SIEM correlation (Splunk, ELK)
  - End-host logs (Windows Event, Syslog, EDR)
- Example correlation (Ví dụ tương quan):
  1. Suspicious DNS query detected (phát hiện truy vấn DNS bất thường).
  2. Correlated with DHCP log to find user (kết hợp với nhật ký DHCP để tìm người dùng).
  3. Proxy log confirms outbound traffic (Proxy log xác nhận có lưu lượng đi ra).

Attribution Challenges (NAT / Proxy / CDN - Vấn đề phân định nguồn)

- NAT/CGNAT: public IP nhiều khách hàng → cần DHCP/NAT table/RADIUS logs to disambiguate.
- Proxy/CDN hides origin: correlate Proxy logs, HTTP headers (X-Forwarded-For), CDN logs.
- Instructor tip: case example - use DHCP lease + firewall session table to identify host behind NAT.

AI/ML in Network Forensics (AI/ML trong điều tra mạng)

- **Thách thức:** dữ liệu khổng lồ, cảnh báo giả, hành vi thay đổi (concept drift).
- **Ứng dụng:** anomaly detection, clustering, phát hiện C2 qua pattern bất thường.
- **Ý nghĩa:** hỗ trợ tự động hoá, tăng tốc độ phân tích trong môi trường IoT/Cloud.

Survey Insights: AI/ML in Network Forensics

- **AI/ML methods** increasingly used to cope with big data in traffic captures.
- Challenges: **false positives**, **concept drift**, encrypted traffic.
- Applications: anomaly detection, traffic classification, malicious flow clustering.
- Example datasets: CICIDS, UNSW-NB15, custom IoT traces.
- **Rizvi et al. (2022)**: comprehensive survey highlighting scalability issues in network forensic investigations.

Datasets & Resources (Bộ dữ liệu và tài nguyên)

- **Datasets:** CICIDS, CTU botnet, MAWI.
- **Tài liệu:** NIST SP 800-86, Zeek documentation.
- **Ứng dụng:** sử dụng để luyện tập lab, nghiên cứu học thuật.

Emerging Challenges in Network Forensics

- **QUIC / HTTP3**: encrypted-by-default, resists deep packet inspection.
- **Encrypted DNS (DoH/DoT)**: limits visibility of queries.
- **VPN & Proxy obfuscation**: attribution issues.
- **Cloud-native logs**: CloudTrail, VPC Flow, Entra Sign-ins must complement packet captures.
- **Clock skew** across multi-cloud & on-prem logs complicates timeline building.

Case Study – Global and Vietnam

Global:

- 2013 Target Breach – attackers exfiltrated data via HVAC vendor's VPN, detected through NetFlow anomalies.
- Lessons: importance of **flow logs + SIEM correlation**.

Vietnam:

- 2020 VN-CERT reported large-scale phishing campaigns using compromised mail servers.
- Forensics: correlation of **DNS logs, proxy traffic, and user DHCP mappings** led to attacker infrastructure takedown.

Case Study: Snowflake 2024 Credential Abuse

- Attackers abused stolen credentials to access multiple customer environments.
- Indicators: suspicious **sign-ins**, anomalous **egress flows**.
- Forensic approach:
  - Review tenant sign-in logs (control-plane).
  - Correlate with VPC Flow Logs (data-plane).
  - Check for large-scale exfiltration events.
- Takeaway: cloud & network forensics are increasingly intertwined.

Vietnam Research Spotlight: SDNLog-Foren

- **Do et al. (2019)**: proposed SDNLog-Foren, a blockchain-secured system for SDN controller logs.
- Problem: attackers may erase/modify controller logs, hiding traces.
- Solution: append-only blockchain storage ensures **log integrity**.
- Relevance: ties to network forensic reliability and tamper-proofing evidence.
- Demonstrates Vietnam's contribution to global forensic research.

Workflows and Common Traps

Forensic Workflow:

1. Capture traffic (pcap/flows)
2. Reduce noise (filters, signatures)
3. Reconstruct sessions/objects
4. Correlate logs & build timeline
5. Document chain of custody

Common Pitfalls:

- NAT obscures attribution
- TLS/QUIC hides payload
- Clock skew between devices
- Over-reliance on a single log source

Key Tools (Công cụ chính trong Network Forensics)

- **Wireshark, tcpdump** – bắt gói tin (packet capture).
- **Zeek (Bro)** – sinh log dạng sự kiện (event logs).
- **Snort, Suricata** – IDS/IPS phát hiện tấn công.
- **NFATs** – hỗ trợ replay, visualization, geoIP, tích hợp SIEM.

Tool Comparison: Snort vs Suricata vs Zeek

- **Snort**: Signature-based IDS, strong rule set, limited forensic logs.
- **Suricata**: Multi-threaded IDS/IPS, EVE JSON output, strong for forensic pipelines.
- **Zeek (Bro)**: Event-driven logs (HTTP, DNS, SSL), excellent for **session reconstruction**.
- SANS whitepaper (2024): advocates combined use — Snort/Suricata for alerts, Zeek for deep evidence.

Why Combine Tools? Roles & Blind Spots

- **Snort/Suricata**: Alerts fast; limited session detail.
- **Zeek**: Rich events; no verdicts; great for correlation/timelines.
- **Wireshark**: Deep object carving; doesn't scale to days/weeks.
- **Playbook**: Alert (IDS) $\rightarrow$ Pivot (Zeek) $\rightarrow$ Prove (PCAP).

Preparation for Lab (2h)

Lab Goals:

- Gain experience using Wireshark & Zeek to:
  - Filter traffic (HTTP, DNS, SSL/TLS)
  - Extract objects from packets
  - Generate Zeek logs and analyze suspicious events
- Define workflow: capture $\rightarrow$ reduce $\rightarrow$ reconstruct $\rightarrow$ correlate
- Outcome: a short incident timeline with evidence screenshots

Summary

- Network Forensics is a core skill in Digital Forensics.
- Evidence exists in packets, flows, and logs $\rightarrow$ each has strengths.
- Investigators must apply structured workflows and avoid pitfalls.
- Case studies (Target, VN-CERT) highlight importance of correlation.
- Next: Lab session to apply Wireshark & Zeek on real-world traffic.

Lab Tasks & Assessment Rubrics (Bài lab & Tiêu chí chấm)

- Lab deliverable: incident timeline (PDF), evidence screenshots, recovered artifact hashes (SHA256), brief methods section.
- Rubric (sample): Timeline completeness (30%), Evidence integrity (20%), Analysis justification (30%), Presentation (20%).
- Suggested tasks: DNS-tunneling detection, Zeek pipeline conn/http analysis, NetFlow exfiltration detection.