Digital Forensics

Federico Conti

2024/25

Contents

Network Forensics 2
Who(/Where) 3
Correlation of different sources 6
Collecting network-based evidence 7

Network Forensics

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.

- Shift to network-centric computing

  Computing has evolved from isolated computers to network-centered systems as people rely on networks for various activities

- Importance of following the cybertrail

  Digital investigators must now trace evidence across networks including the public Internet, private networks, and commercial systems to collect relevant digital evidence

Process

The investigation process identifies communicating hosts in terms of time, frequency, protocol, application, and data. It tries to answer the 5W and 1H

- **Who**: identifying the source

  determining who is behind an attack or suspicious activity by identifying originating hosts or users

- **What**: identifying the payload and activities

  identifying exactly what data or malicious payloads are being transmitted

- **Where**: determining the destination or target

  identifying which users, systems, or resources are being targeted or have been compromised

- **When**: establishing a timeline

  defining the exact timeframe of events to reconstruct incident progression

- **Why**: understanding motivation and intent

  determining the attacker's goal (gaining initial access, obtaining credentials or escalating privileges, collecting specific sensitive data, establishing persistence, lateral movement, . . .)

- **How**: techniques and methods used

  understanding the attacker's methodology, tactics, and specific exploits

he 5Ws and 1H framework is always relevant and necessary at every investigative step (or for homogeneous groups of steps)

Applying this framework systematically ensures completeness, consistency, and analytical rigor, enabling investigators to precisely reconstruct the timeline of an attack

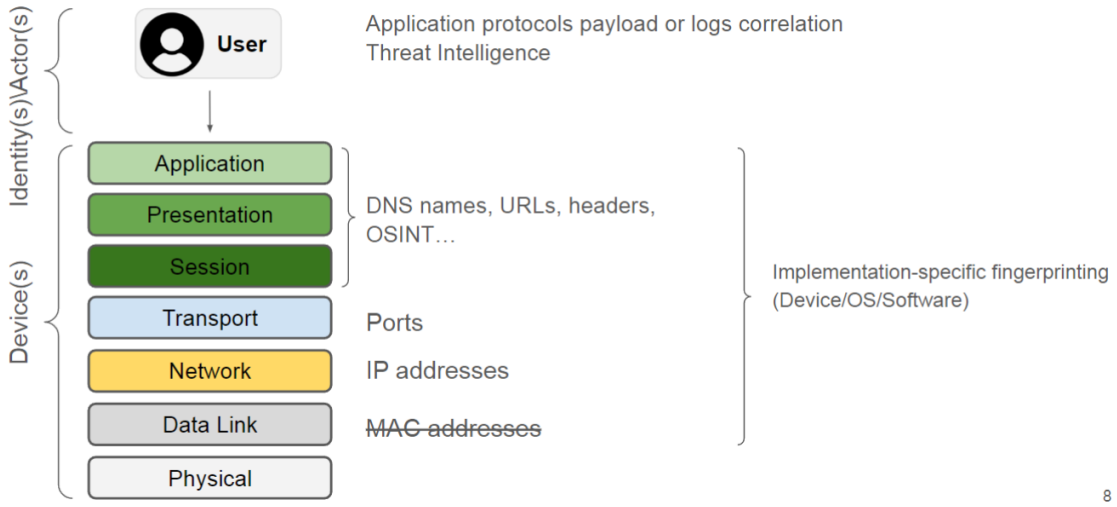
When	Who	What	Where	Why	How
2024-03-28 03:15 AM	IP: 1.2.3.4 User: Unknown	Initial unauthorized access attempt (login)	IP: 10.0.2.20 (Webserver, port 443)	Gaining initial foothold in network	Exploiting known vulnerability (RCE on web application)
2024-03-28 03:20 AM	IP: 10.0.2.20 (compromised Webserver)	Lateral movement attempt via SSH	IP: 10.0.3.15 (Internal DB Server, port 22)	Access to sensitive database data	Exploitation of SSH credentials (private key on 10.0.2.20)
...	...	...	...	...	...

Report (a possible structure)

There is no single "official" format for network forensics reports

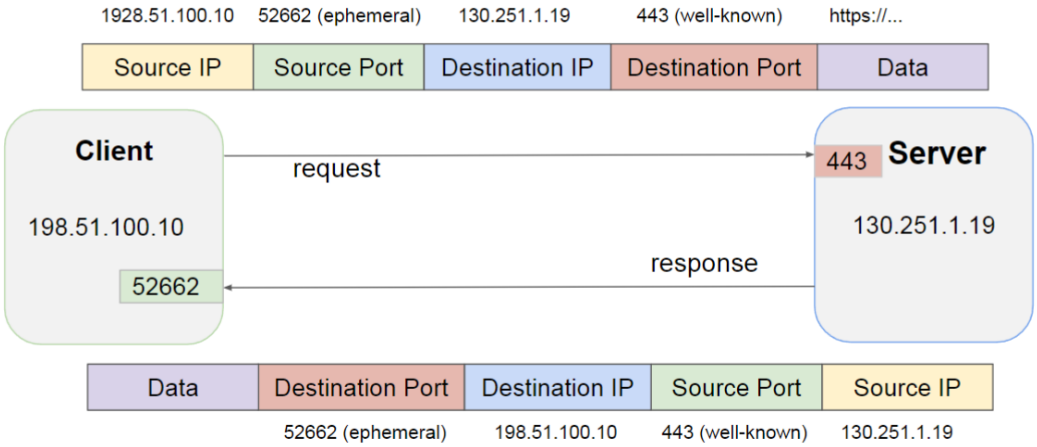
- An overview of the investigation objectives
- A recap of events
- What digital forensics tools (and methodologies) have been used
- Detailed timeline
- Clearly identify each artifact and include its cryptographic hash
- Recommendations and mitigations
- Suggest improvements to security processes based on lessons learned from the incident

Who(/Where)



MAC addresses (crossed out) – once useful for identifying local devices, but:

- They're not preserved across networks (only visible on the same LAN)
- Easily spoofed or obfuscated (e.g., by VPNs or virtual interfaces)



ayer 4 is in charge of the process-to-process communication. Transmitter and receiver are identified using ports

16-bit unsigned integer (0-65535, 0 reserved) conventionally divided into:

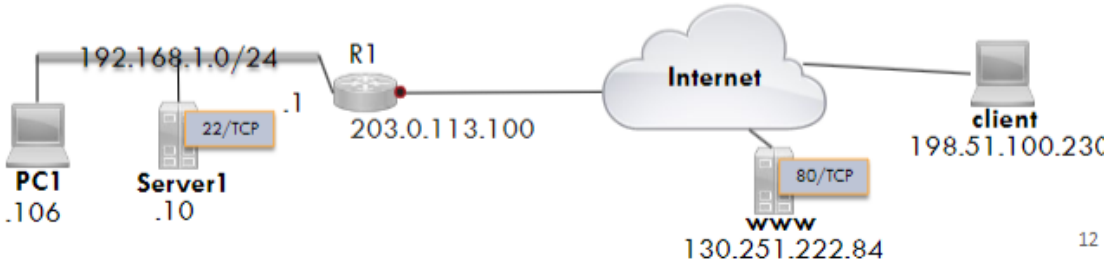
- Well-known ports (0-1023): used by system processes that provide widely used types of network services (requires superuser privileges)
- Registered ports(1024-49151): assigned by a central authority (the Internet Assigned Numbers Authority, IANA) for specific services
- Ephemeral ports(49152–65535): contains dynamic or private ports that cannot be registered with IANA

(see /etc/services)

Source NAT and Masquerade

Network Address Translation (NAT) generally involves rewriting the source and/or destination addresses of IP packets as they pass through a router or firewall

- NAT affects answering Who/Where questions
  - 192.168.1.0/24 is a private network and it is not routable on the Internet
- Masquerade is a source NAT rule, i.e., it is related to the source address of a packet
- The popular usage of NAT Masquerade is to translate a private address range to a single public IP address



Example:

NAT Table (Dynamic)

Public IP	Public Port, Destination Port	Private IP
203.0.113.100	52000, 80	192.168.1.106
203.0.113.100	53000, 80	192.168.1.10

1. PC1 and Server1 accessing www (request)

SRCIP	SRCPORT	DSTIP	DSTPORT		SRCIP	SRCPORT	DSTIP	DSTPORT
192.168.1.106	52000	130.251.222.84	80	R1 →	203.0.113.100	52000	130.251.222.84	80
192.168.1.10	53000	130.251.222.84	80	R1 →	203.0.113.100	53000	130.251.222.84	80

2. PC1 and Server1 accessing www (response)

SRCIP	SRCPORT	DSTIP	DSTPORT		SRCIP	SRCPORT	DSTIP	DSTPORT
130.251.222.84	80	192.168.1.106	52000	R1 ←	130.251.222.84	80	203.0.113.100	52000
130.251.222.84	80	192.168.1.10	53000	R1 ←	130.251.222.84	80	203.0.113.100	53000

Port forwarding

Port forwarding is a destination NAT rule, i.e., it is related to the destination address of a packet

Maps external IP addresses and ports to Internal IP addresses and ports allowing access to internal services from the Internet

DNAT table (static)

Public IP Address	Ext. Port	Private IP Address	Int. Port
203.0.113.100	2222	192.168.1.10	22

Example:

1. Client connecting to Server1 (request)

SRCIP	SRCPORT	DSTIP	DSTPORT		SRCIP	SRCPORT	DSTIP	DSTPORT
192.168.1.10	22	198.51.100.230	54000	R1 →	203.0.113.100	2222	198.51.100.230	54000

2. lient connecting to Server1 (response)

SRCIP	SRCPORT	DSTIP	DSTPORT		SRCIP	SRCPORT	DSTIP	DSTPORT
198.51.100.230	54000	192.168.1.10	22	R1 ←	198.51.100.230	54000	203.0.113.100	2222

To identify internal hosts behind NAT.

1. at device translation logs (NAT table)
2. correlate ephemeral ports between pre-NAT and post-NAT sessions to identify the original internal host
3. Some protocols include internal IP information in their payloads or headers, which can help identify the internal host:
    - FTP (File Transfer Protocol) → PORT command includes the client's IP and port for data connection
    - SIP (Session Initiation Protocol) → Via: and Contact: headers may contain the internal IP address of the user agent
    - ICMP (Error messages) → Error payload includes the original IP header
    - HTTP / Custom APIs → Sometimes apps send their local IP in headers or structured payloads (e.g., JSON payload "client_ip": "192.168.1.10")

Full content data refers to every single piece of information that is transmitted over a network or networks, without any filtering or modification.

- is captured and stored in its entirety, including all the traffic that passes through the network, often referred to as packet captures or PCAP

- includes not only the payload or data portion of the network packets, but also the header information, metadata, timestamps, and any other data associated with the network communication

Session data onsists of aggregated traffic metadata and usually refers to the conversation between two network entities

- grouped together into flows and/or groups of network packets related to one another
- are able to inform the investigator about questions such as who talked to whom (who/where), when, for how long, etc. without looking at any contents of the conversation(s) at all.

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2020-04-22 12:19:58.824	0.004	TCP	44.30.248.239:443	->	44.244.6.114:54044	...AP...	16	141	204984	35250	410.0 M	1453	1
2020-04-22 12:22:37.845	0.004	TCP	175.68.86.47:80	->	44.244.6.114:53717	...AP...	128	133	184649	33250	369.3 M	1388	1
2020-04-22 12:20:37.844	0.004	TCP	175.68.86.47:80	->	44.244.6.114:53717	...AP...	128	133	184649	33250	369.3 M	1388	1
2020-04-22 12:24:37.845	0.004	TCP	175.68.86.47:80	->	44.244.6.114:53717	...AP...	128	132	184609	33000	369.2 M	1398	1

(see https://en.wikipedia.org/wiki/NetFlow)

Specific systems, typically Network Intrusion Detections System (NIDS), trigger alerts based on

- signature-based detection: looking for specific patterns, such as byte sequences
- anomaly-based detection: studies the normal behaviour of the monitored system and then looks out for any difference in it

Mainstream open source solutions are

- SNORT https://www.snort.org/
- Suricata https://suricata.io/

Statistical data provide the analyst with network-related aspects such as

- the number of bytes contained in a packet trace
- start and end times of network conversations
- number of services and protocols being used
- most active network nodes
- least active network nodes
- outliers in network usage
- average packet size, average packet rate
- ... It can therefore also act as a useful source for anomaly detection.

Correlation of different sources

Network-based evidence can be correlated with other sources to enhance forensic investigations and root cause analysis. Examples include:

1. Network Nodes:
   - Logs and files from network nodes such as attack computers, intermediate systems, or victim computers can provide critical evidence.
2. Examples of Logs:
   - *SSH Server Logs*:
     ```
     journalctl -u sshd
     Apr 15 13:45:29 server1 sshd[3859975]: Accepted publickey for user from 10.187.10.221 port 601
     ```
   - *Proxy Server Logs*:
     ```
     tail -f /var/log/squid.log
     1681571063.731 171297 93.51.10.270 TCP_TUNNEL/200 6889 CONNECT www.google.com:443 enricorusso
     ```
   - *Mail Server Logs*:
     ```
     tail -f /var/log/mail.log
     Jul 4 19:47:58 mammon postfix/smtpd[4936]: 07A1753F: client=c-69-181-123-456.hsd1.ca.comcast.n
     ```
3. Internetworking devices (e.g., router, access point, or VPN concentrators): logs and buffers

Who: IP and Domain OSINT

Investigate suspicious IP addresses and domains using publicly available sources.

- Check if an IP or domain has been reported for malicious activity
- Identify infrastructure related to known threat actors
- Gather context (geolocation, ISP, reverse DNS, historical records)

Tools:

- *VirusTotal*
  - Multi-engine scanner for IPs, domains, files
  - Shows passive DNS, related indicators, threat labels
- *AbuseIPDB*
  - Community-powered IP reputation
  - View abuse reports, threat categories, and risk scores
- *Shodan*
  - Search engine for internet-exposed devices
  - Discover open ports, banners, services running on an IP

What/How: TTPs

Tactics, Techniques, and Procedures (TTPs) describe the behavioral patterns of threat actors.

The MITRE ATT&CK framework provides a structured knowledge base of real-world.

TTPs observed across threat campaigns.

- Tactic (What): the attacker's goal or objective at a certain stage (e.g., Credential Access, Lateral Movement)
- Technique/Procedure (How): the method or implementation used to achieve that goal (e.g., Brute Force - T1110, Exploitation of Remote Services - T1210)

How: CWE and CVE

- *Common Weakness Enumeration (CWE)*:
  - Represents a general weakness (e.g., improper input validation).
  - A community-developed knowledge base of common software and hardware weaknesses, maintained by MITRE.
  - If you only identify a CWE, you still understand what kind of mistake allowed the attack.
- *Common Vulnerabilities and Exposures (CVE)*:
  - Identifies a specific vulnerability in a real product (e.g., a buffer overflow in OpenSSL version X.Y).
  - If you know the CVE, you know exactly which hole the attacker used.
  - Searching for CVEs
    - NVD (National Vulnerability Database)
    - MITRE CVE site
    - Exploit DB
    - [Google/GitHub search + product/version or artifacts]

Collecting network-based evidence

The task of acquiring network evidence can be divided into active and passive acquisition.

- passive acquisition: refers to gathering data without emitting data at OSI Layer 2 or above, such as capturing or sniffing network traffic.
- active acquisition: involves interacting with systems on the network, such as sending queries or logging to a central host, SIEM, or management station, and may also include scanning network ports to determine system status

To preserve as much of the evidence as possible, acquisition should not change the packets, send out additional packets or alter the network configuration.

Passive acquisition

Network forensic investigators can passively acquire network traffic by

- intercepting it as it is sent across cables
- through network equipment such as (hubs) and switches
- through the air