Italian national
interuniversity consortium
for telecommunications

National Lab RaSS
Radar and Surveillance Systems

Network Forensics

Eng. Alessandro Cantelli-Forti, PhD

Parma, 26.11.24

PoC and Reference Materials

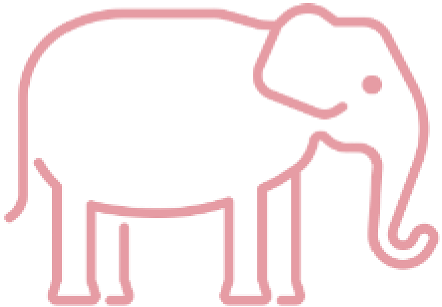
- **“Introduction to Network Forensics”**
enisa - European Agency for Cybersecurity

- **Messier Ric – “Network Forensics” – Wiley**

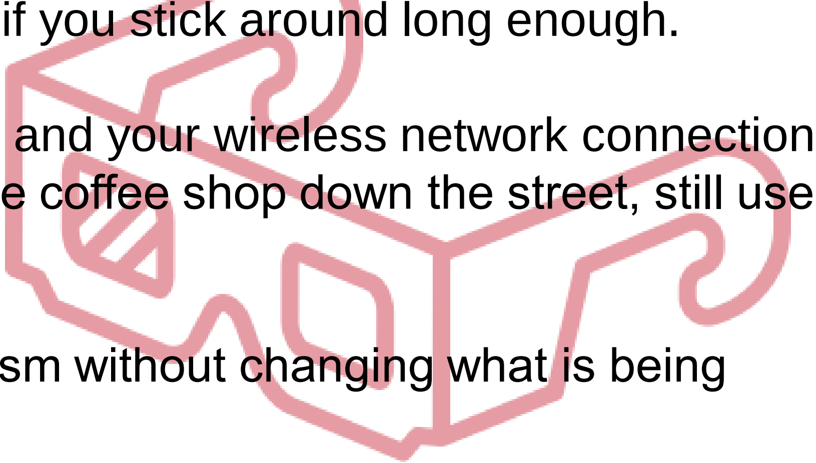
- **Nipun Jaswal – “Hands-On Network Forensics” - Pakt**

Email: alessandro.cantelli.forti@cnit.it
Mob: 3472651552

HOW AND WHY



- We need to understand the **why and how** of things
- When I understand the why and how, I don't get stuck
- Technology continues to **cycle around** a number of central ideas. This has always been true.
- When you understand what underpins the technology, you'll see it's a **variation on something you've seen before**, if you stick around long enough.



- Ethernet was developed in the 1970s and your wireless network connection, whether it's at home or at your favorite coffee shop down the street, still uses Ethernet.
- We're changing the delivery mechanism without changing what is being delivered!
- If you learned how **Ethernet** worked in the early 1980s, you could look at a frame of **wifi traffic** today and still understand exactly what is happening.

Forensic as a Science

- The word **forensics** comes from the Latin *forens*, meaning belonging to the public. It is related to the word **forum** and **scientia**, meaning “on the forum” and “knowledge”. In ancient Rome, criminal proceedings were held in public at the market place (forum).

- **Forensic science is hence referring to the process of applying scientific methods to criminal and civil proceedings.**

- Technical aspects of forensic investigations have **evolved** into **sub-fields** relating to the special conditions of the evidence involved, like toxicology, fingerprint analysis, etc. **with digital forensics being the branch of forensic science encompassing the recovery and investigation of material found**

Five Main Principles of D.F. 1/2

- *From Jones et al. (2013, see also ENISA 2013a): «There are five main principles that draw up a basis for all dealings with electronic evidence. These principles were adopted as part of* ***European Union and the Council of Europe*** *project to develop a '**seizure of e-evidence**' guide»*

1. **Data integrity:** No action taken should change electronic devices or media, which may subsequently be relied upon in court.

2. **Audit trail:** An audit trail or other record of all actions taken when handling electronic evidence should be created and preserved. An independent third party should be able to examine those actions and achieve the same result.

3. **Specialist support:** If it is assumed that electronic evidence may be found in the course of an operation, the person in charge should notify specialists, often external advisers, in a timely fashion.

Five Main Principles 2/2

4 **Appropriate training:** First responders must be appropriately trained to be able to search for and seize electronic evidence if no experts are available at the scene.

5 **Legality:** The person and agency in charge of the case are responsible for ensuring that the law, the general forensic and procedural principles, and the above listed principles are adhered to. This applies to the possession of and access to electronic evidence.

«While laws regarding admissibility of evidence differ between countries, using these principles is considered appropriate, as they are common internationally».

Introducing Network Forensics

- “**Network forensics** is one of the **sub-branches** of **digital forensics** where the data being analyzed is the network traffic going to and from the **system under observation**.

  The purposes of this type of observation are:
  - collecting information,
  - obtaining legal <u>evidence</u>,
  - establishing a root-cause analysis of an event,
  - analyzing malware behavior, and so on.

- Professionals familiar with digital forensics and incident response (DFIR) **know that even the most careful <u>suspects</u> leave traces and <u>artifacts</u> behind.**

- But forensics generally also includes imaging the systems for memory and hard drives, which can be analyzed later.

- So, how do network forensics come into the picture? Why do we need to perform network forensics at all?

Why do we need network forensics?

- *“Until recently, it was sufficient to look at individual computers as isolated objects containing digital evidence. Computing was disk-centred—collecting a computer and several disks would assure collection of all relevant digital evidence. Today, however, computing has become network-centred as more people rely on e-mail, e-commerce, and other network resources. It is no longer adequate to think about computers in isolation as many of them are connected together using various network technologies. Digital investigators/examiners must become skilled at following the cybertrail to find related digital evidence on the public Internet, private networks, and other commercial systems. An understanding of the technology involved will enable digital investigators to recognise, collect, preserve, examine, and analyse evidence related to crimes involving networks.”*
- **Casey, E. (2011), Digital evidence and computer crime: forensic science, computers and the internet, 3rd ed., Academic Press, 2011, ISBN 978-0-12-374268-1 (p. 607).**

Why do we need network forensics?

- «Let's consider a scenario where you are hunting for some unknown attackers in a **massive corporate infrastructure** containing thousands of systems. In such a case, it would be practically impossible to image and analyze every system.»

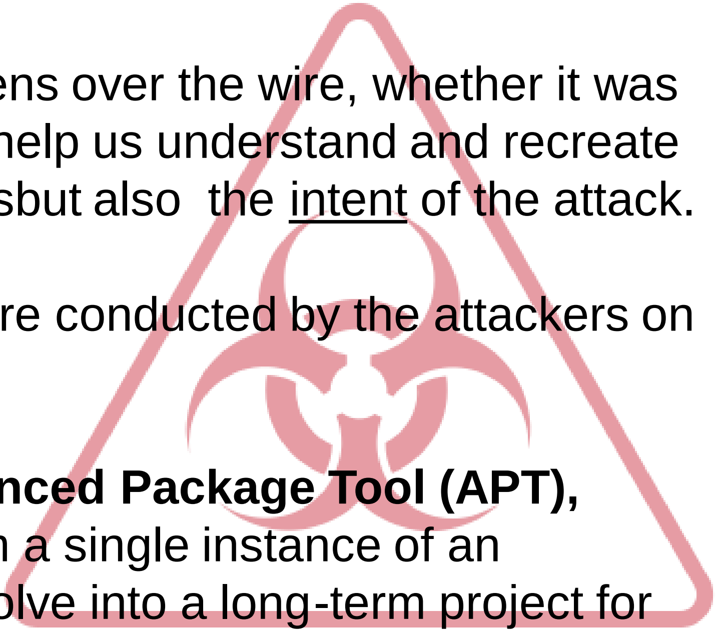
- Instances where the disk drives may not be available

- Cases where the attack **is in progress**, and you may not want to tip off the attackers

- Whenever an intrusion or a digital crime happens over the wire, whether it was successful or not, the artifacts left behind can help us understand and recreate not only the <u>actions</u> performed by the attackersbut also the <u>intent</u> of the attack.

- If the attack was successful, what activities were conducted by the attackers on the system? What happened next?

- Generally, most severe attacks, such as **Advanced Package Tool (APT),** ransomware, espionage, and others, start from a single instance of an unauthorized entry into a network and then evolve into a long-term project for the attackers until the day their goals are met; however, throughout this period the information flowing in and out of the network goes through many different

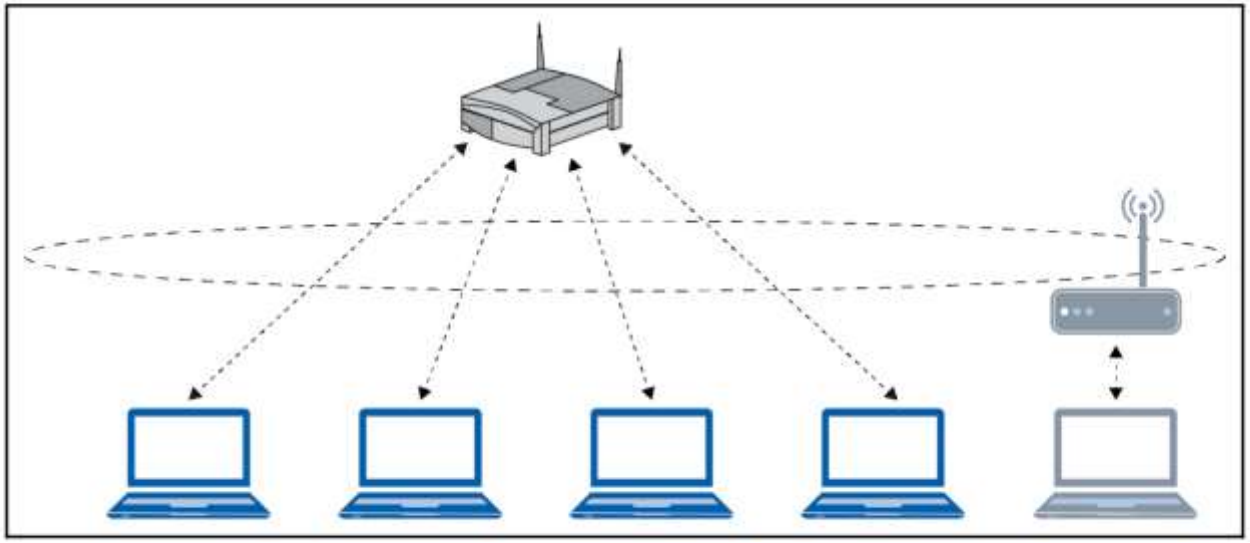


HOST SIDE ARTIFACTS

Host-side artifacts. After all, not everything happens over the bare wire.

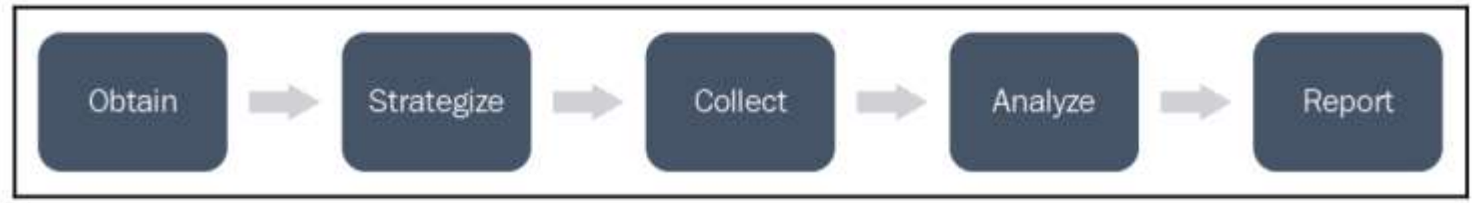
- Communication originates and terminates from end devices like computers, tablets, phones, and a variety of other devices. **When communication happens between two devices, there are traces on those devices**. What those artifacts might be and how you might recover them

- The word **forensics** also describes the process of **identifying** digital artifacts within a large collection of data, where law enforcement isn't involved.



OSCAR

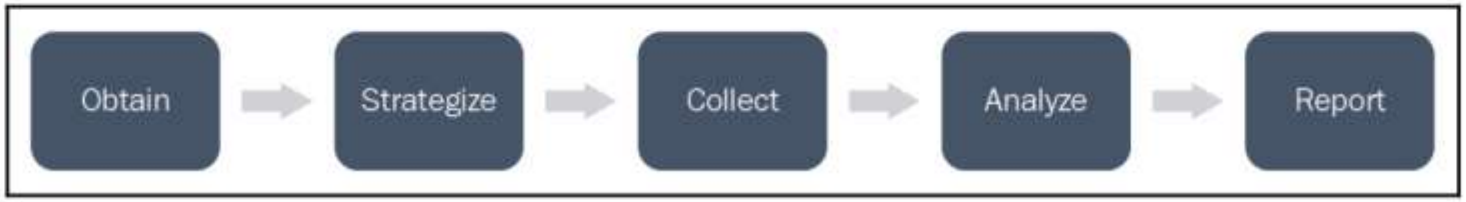
- Network forensics follow the same basic principles of digital forensics: the **OSCAR methodology.**
- One such framework that ensures appropriate and **constant** results


Obtain → Strategize → Collect → Analyze → Report

Obtain information about the incident and the environment is one of the first things to do to familiarize a forensic investigator with the type of incident. The timestamps and timeline of the event, the people, systems, and endpoints involved in the incident are crucial in building up a detailed picture of the event.

- Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior DOI: 10.6633/IJNS.201809

OSCAR



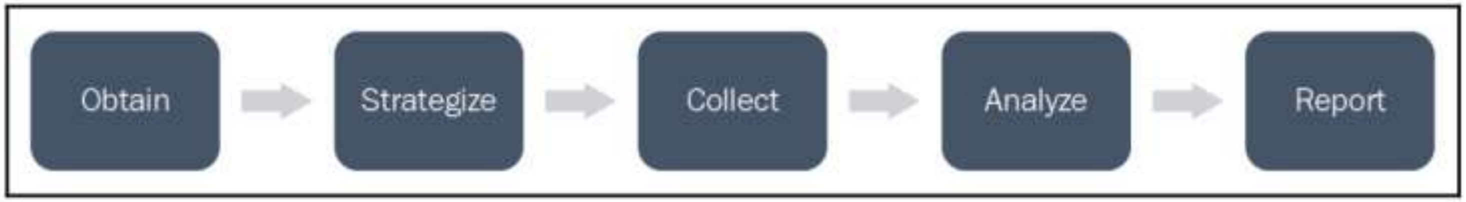
Obtain → Strategize → Collect → Analyze → Report

Strategize ie. planning the investigation is critical, since logs from various devices can differ in their nature; for example, **the volatility of log entries from a firewall** compared with that of details such as the **ARP of a system would be very different**.

- Define clear goals and timelines
- Find the sources of evidence
- Analyze the cost and value of the sources
- Prioritize acquisition
- Plan timely updates for «the client»

- This priority list should be starting point for allocating resources and personnel to conduct the present tasks such as acquiring information and evidence.

OSCAR



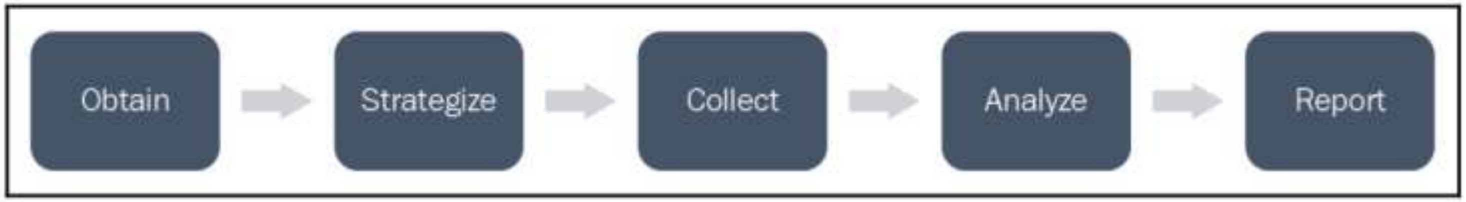
Obtain → Strategize → Collect → Analyze → Report

Collect: In the collect phase, we acquire the evidence as per the plan. collecting the evidence itself requires you to document all the systems that are accessed and used, capturing and saving the data streams to the hard drive and collecting logs from servers and firewalls.

Best practices for evidence collection include the following (1/2):

- Make **copies** of the evidence and generate **cryptographic hashes** for verifiability: packets are captured, copying logs, imaging hard drives of systems(*), etc
- Never work on the **original** evidence; use copies of the data instead
- Use industry-standard **tools**

OSCAR

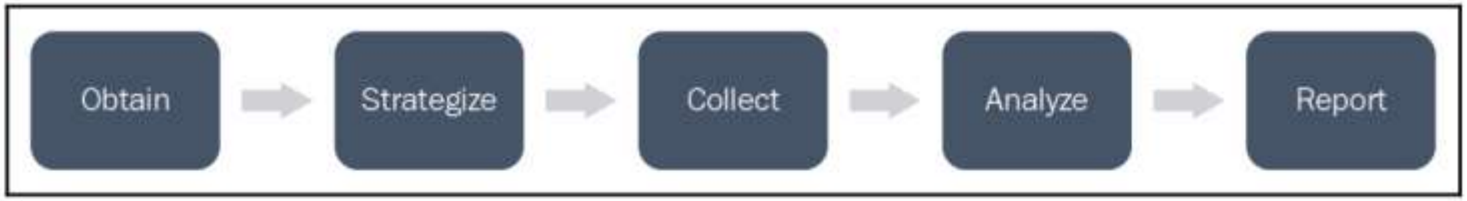


Best practices for evidence collection include the following (2/2):

- Document all your actions (**documentation**): All actions taken, and all systems accessed should be logged and the log safely stored following the same guidelines as the evidence itself. The log should include time, source of the evidence, acquisition method and the involved investigator(s).

- **Store/Transport:** This is about maintaining the Chain of Custody, i.e. "showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic." (EDRM Glossary)

OSCAR


Obtain → Strategize → Collect → Analyze → Report

Analyze: The analysis phase is the core phase (?) where you start working on the data and try your hands at the riddle. You will make use of multiple automated and manual techniques using a variety of tools to correlate data from various sources, establishing a timeline of events, eliminating false positives, and creating working theories to support evidence. You will spend most of the time in this course discussing the analysis of data.

CORRELATION OR CAUSATION?

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

Collecting network-based evidence

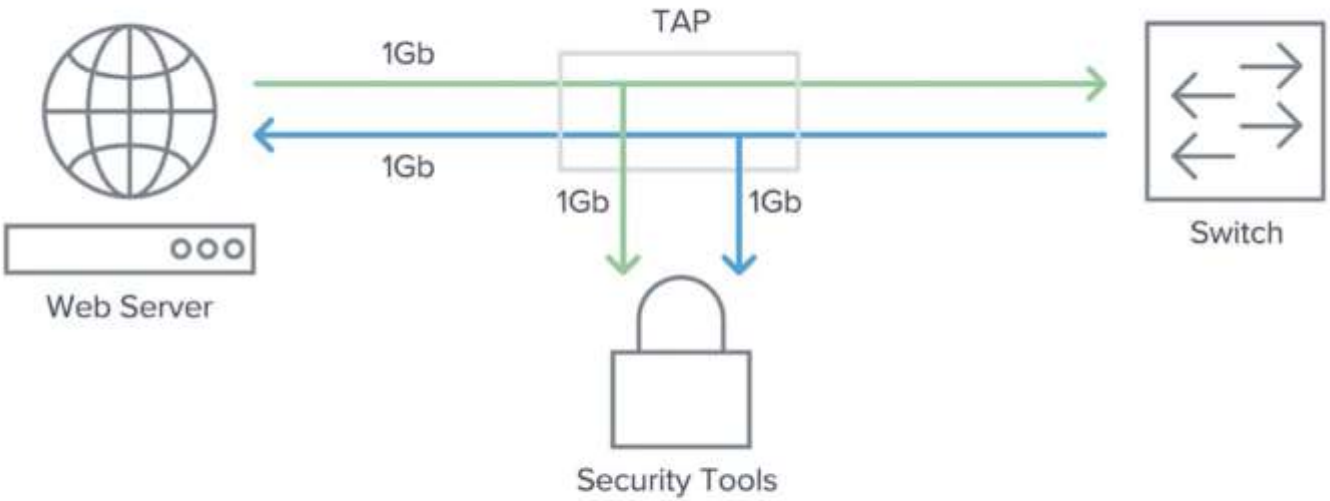
- Passive acquisition happens when data is gathered without emitting data at link layer or above.
- Traffic acquisition, or capturing, or sniffing is passive acquisition.
- Active acquisition happens when evidence is gathered by interacting with systems on the network, i.e. by sending queries to them, or systems logging to a log host, SIEM or management station.
- This may even include scanning the network ports of systems to determine their current state.
- To preserve as much of the evidence as possible, acquisition should not change the packets, send out additional packets or alter the network configuration.

"Ideally, we would like to obtain perfect-fidelity evidence, with zero impact on the environment. For copper wires, this would mean only observing changes in voltages without ever modifying them. For fibre cables, this would mean observing the quanta *without ever injecting any. For radio frequency, this would mean observing RF waves without ever emitting any. In the real world, this would be equivalent to a murder investigator collecting evidence from a crime scene without leaving any new footprints."* (Davidoff and Ham, 2012, p. 45).

Snoop the traffic: network TAP

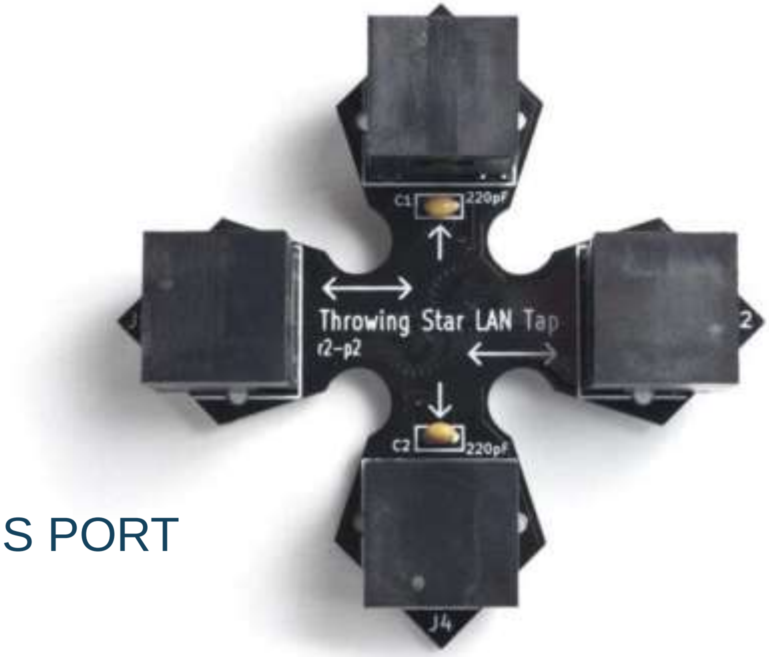
- One of the most raw forms of information capture is to put taps on network and optical fiber cables to snoop on traffic

- Most vendors provide network taps and SPAN ports on their devices for snooping where they will forward all traffic seen on the particular port to the analyzer system.



Snoop the traffic: network TAP

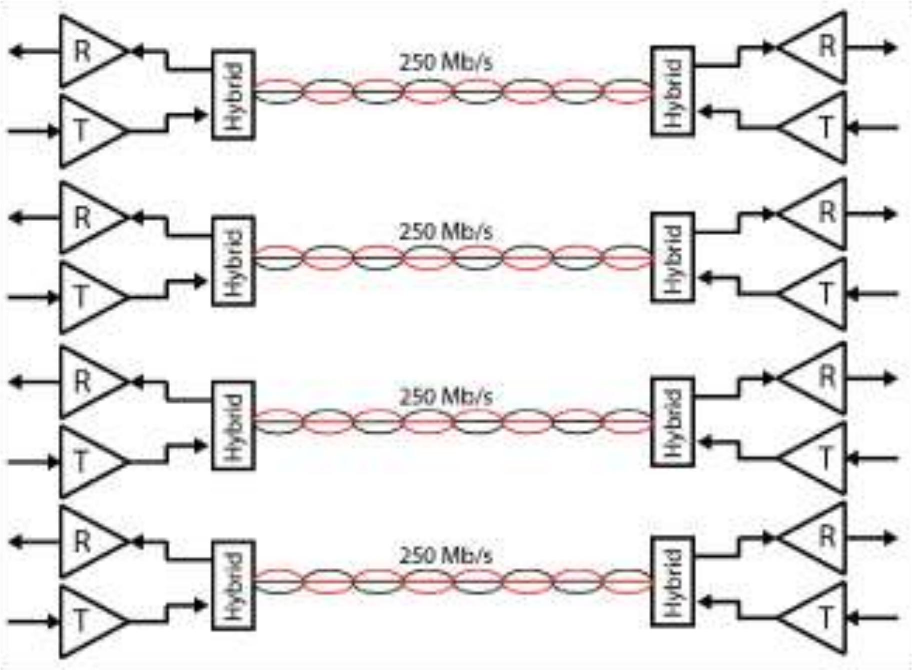
- Inline network taps are physical devices which can be inserted inline between two physically connected network devices.
- It physically replicate copies to one or more monitoring ports.
- Network taps commonly have four ports: two connected inline to facilitate normal traffic, and two sniffing ports, which mirror that traffic (one for each direction).
- Insertion of an inline network tap typically causes a brief disruption, since the cable must be separated to connect the network tap inline. (mmmmm…)
- They are commonly designed to require no power for passively passing packets (why?). F bit Ethernet



TEST ACCESS PORT

Gigabit Base-T TAP issues

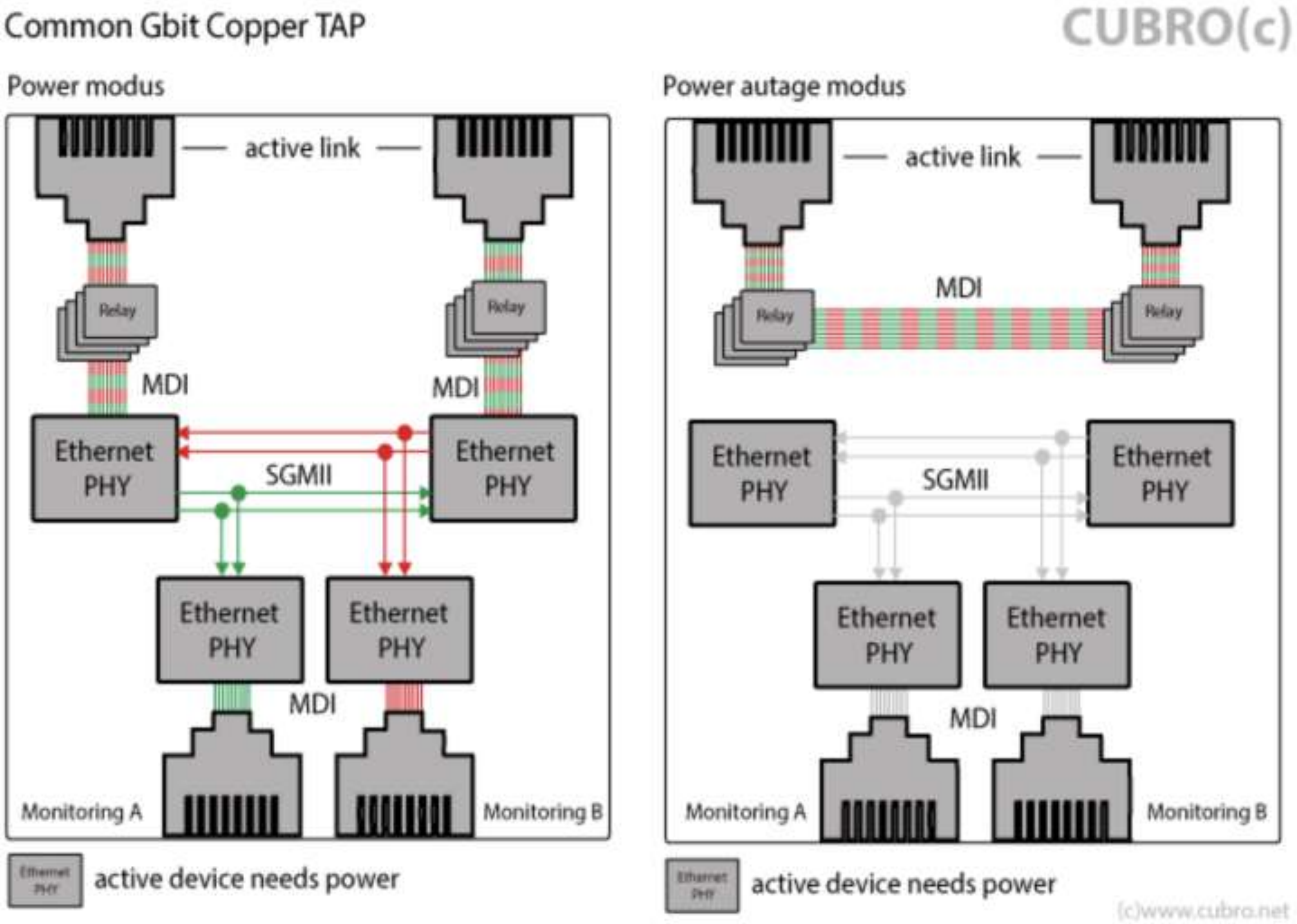
- To transport 1 Gbit of traffic full duplex a very complex signal is used to reach the desired performance and quality. T
- The signal is called PAM 5 modulation, meaning that each cable pair transports 5 bits simultaneously in both directions.
- The PHY chips at each end of must separate the two signals from each other. This is only possible because they know their own signal



(c) Cubro

Gigabit Active TAP (w/ fallback)

- The Layer 1 (PHY) chips at each end of the cable must separate the two signals from each other. This is only possible because they know their own sig



Gigabit Base-T TAP w/fallback issues

- Also this solution will not detect that the link is down for a minimum of three seconds. These three seconds are a result of the autonegotiation behavior. This can not be changed because it is a vital function of the IEEE 802.3 standard.
- Even this short interruption time could cause big problems in a network.
- In some cases these links cannot be re-established without shutting down the services.
- Rerouting functions in the network may take place
- Streaming applications can collapse and cause more issues.
- The clock synchronization is affected. Sync-E over a standard Gbit copper tap is impossible and IEEE 1588 is affected, because of the additional delay a copper tap produces.

Vampire Tabs (Industrial systems)

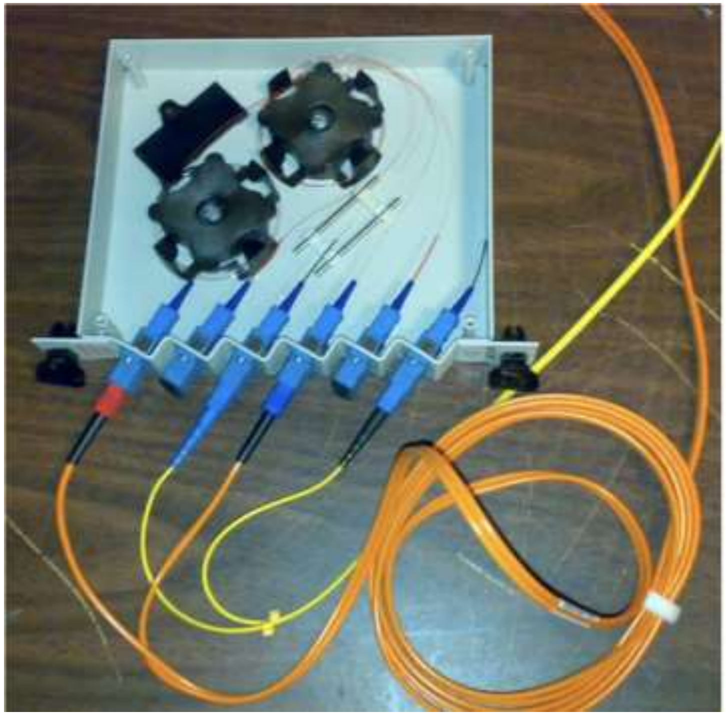
- Unlike inline network taps, the cable does not need to be severed (or disconnected) for a vampire tap to be installed.

- *Esample of: 10Base5 cabling (very very legacy, just for reference!)*

Fibre Optic network taps

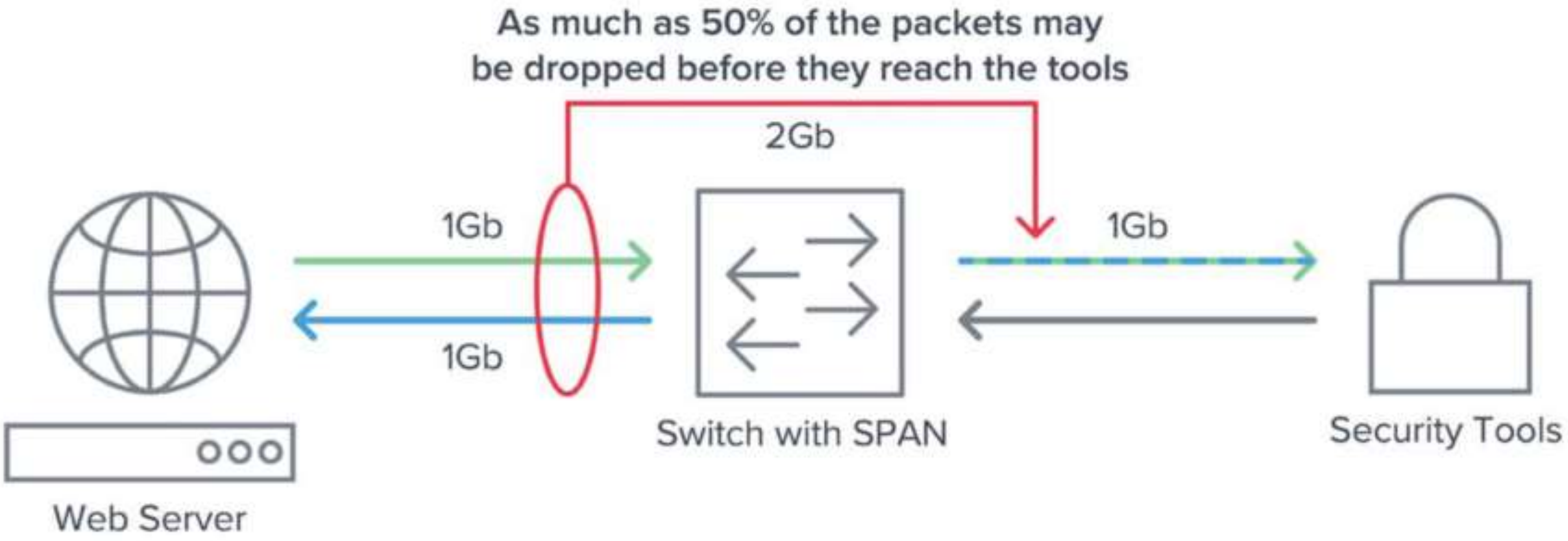
- Work similarly to inline taps for copper cables. The investigators will splice the optic cable and connect it to each port of a tap or insert a pre-fabricated tap before a switch or patch panel.
- Will disrupt the and cause some signal attenuation, although taps may amplify the signal back to its original level, but this will require some kind of power supply (active taps).

Example of Passive fibre optic tap (PON):



Snoop the traffic: SPAN port

- A SPAN port (or mirror port) is implemented in software and built into a switch or router ➛ SPAN ➛ Switch Port Analyzer
- It creates a copy of <u>selected</u> packets passing through the device and sends them to a designated SPAN port.
- Can be easily configured on what data is to be monitored.
- SPAN data is given a lower priority on the device.
- The SPAN also uses a single egress port to aggregate multiple links, so it is easily oversubscribed.


As much as 50% of the packets may be dropped before they reach the tools
2Gb
1Gb
1Gb
1Gb
Web Server
Switch with SPAN
Security Tools

SPAN port

- There are situations where a TAP is not practical ➛ Consider using SPAN:
- Limited ad hoc monitoring where a network TAP does not currently exist (but..)
- Locations with limited light budgets where the split ratio of a TAP may consume too much light. (Another possibility ? Or two?)
- Production emergencies where there is no maintenance window in which to install a TAP.
- Remote locations with modest traffic that cannot justify a full-time TAP on the link.
- Access to traffic that either stays within a switch or never reaches a <u>physical link</u> where the traffic can be tapped.
- As a low-cost troubleshooting alternative where links have low utilization.

Both network TAPs and SPAN ports can provide valid access to data if properly positioned. So TAP where you <u>can</u>, and SPAN where you <u>must</u>.

✓ https://www.gigamon.com/resources/resource-library/white-paper/to-tap-or-to-span.html

Source of network evidence

- **Tapping the wire and the air**
- **CAM table on a network switch**
- **Routing tables on routers**
- **Dynamic Host Configuration Protocol logs**
- **DNS server logs**
- **Domain controller/ authentication servers/ system logs**
- **IDS/IPS logs**
- **Firewall logs**
- **Proxy Server logs**

CAM table on a network switch

- **Network switches contain <u>content-addressable</u> memory tables that store the mapping between a system's MAC address and the physical ports.**

- **In a large setup, this table becomes extremely handy, as <u>it can pinpoint a MAC address on the network to a wall-jacked system</u>, since mappings are available to the physical ports.**

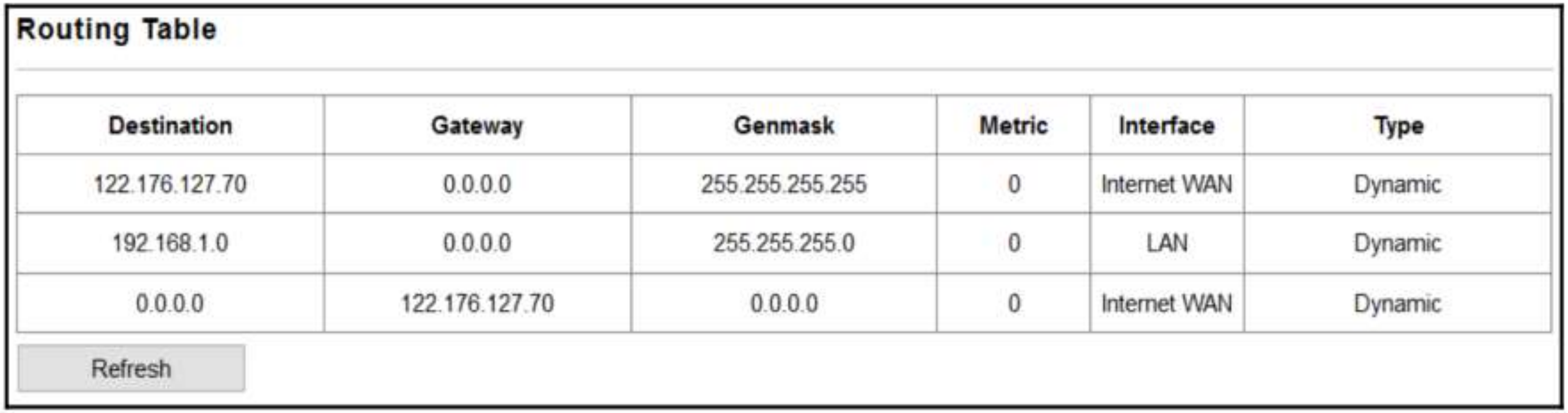
- **As we know, switches also provide <u>network-mirroring capabilities</u>, which will allow the investigators also to see all the data from other VLANs and systems.**

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

Routing tables

- Routing tables in a router maps ports on the router to the networks that they connect. These tables allow us to investigate the path that the network traffic takes while traveling through various devices:



Routing Table

Destination	Gateway	Genmask	Metric	Interface	Type
122.176.127.70	0.0.0.0	255.255.255.255	0	Internet WAN	Dynamic
192.168.1.0	0.0.0.0	255.255.255.0	0	LAN	Dynamic
0.0.0.0	122.176.127.70	0.0.0.0	0	Internet WAN	Dynamic

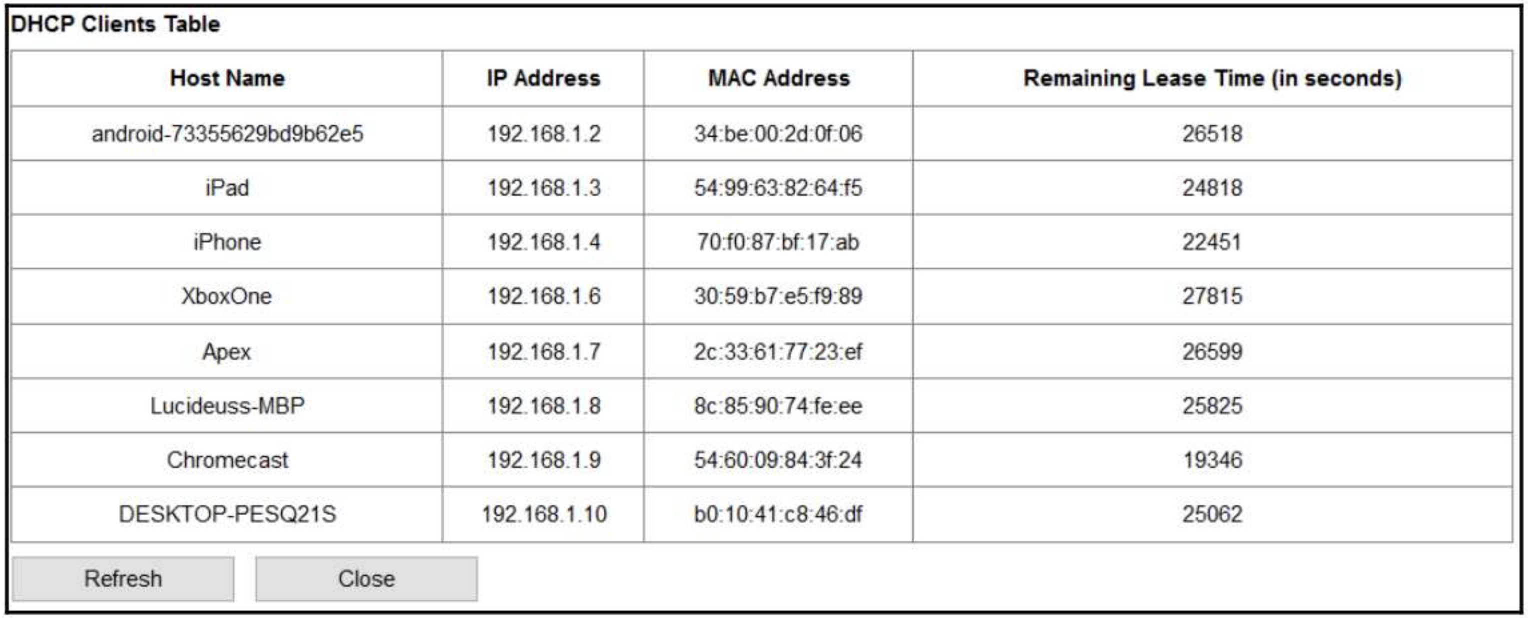
- Most of the routers have inbuilt packet filters and firewall capabilities as well. This means that they can be configured to log denied or certain types of traffic traveling to and from the network.

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

DHCP logs

- Dynamic Host Configuration Protocol (DHCP) servers generally log entries when a specific IP address is assigned to a particular MAC address, when a lease was renewed on the network, the timestamp it renewed, etc..
- It has significant value in network forensics.
- Arpwatch is a tool to perform L2 monitor in real time

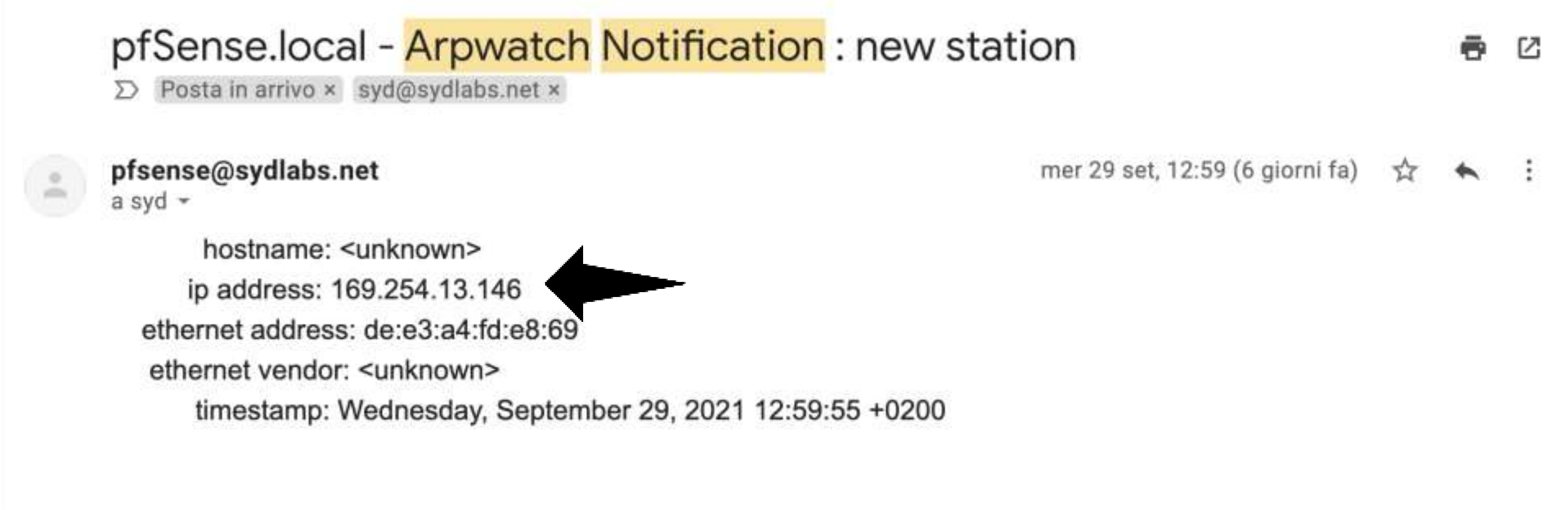


DHCP Clients Table

Host Name	IP Address	MAC Address	Remaining Lease Time (in seconds)
android-73355629bd9b62e5	192.168.1.2	34:be:00:2d:0f:06	26518
iPad	192.168.1.3	54:99:63:82:64:f5	24818
iPhone	192.168.1.4	70:f0:87:bf:17:ab	22451
XboxOne	192.168.1.6	30:59:b7:e5:f9:89	27815
Apex	192.168.1.7	2c:33:61:77:23:ef	26599
Lucideuss-MBP	192.168.1.8	8c:85:90:74:fe:ee	25825
Chromecast	192.168.1.9	54:60:09:84:3f:24	19346
DESKTOP-PESQ21S	192.168.1.10	b0:10:41:c8:46:df	25062

ARP Watch example 1

- Arpwatch is a tool to perform L2 monitor in real time



pfSense.local - Arpwatch Notification : new station

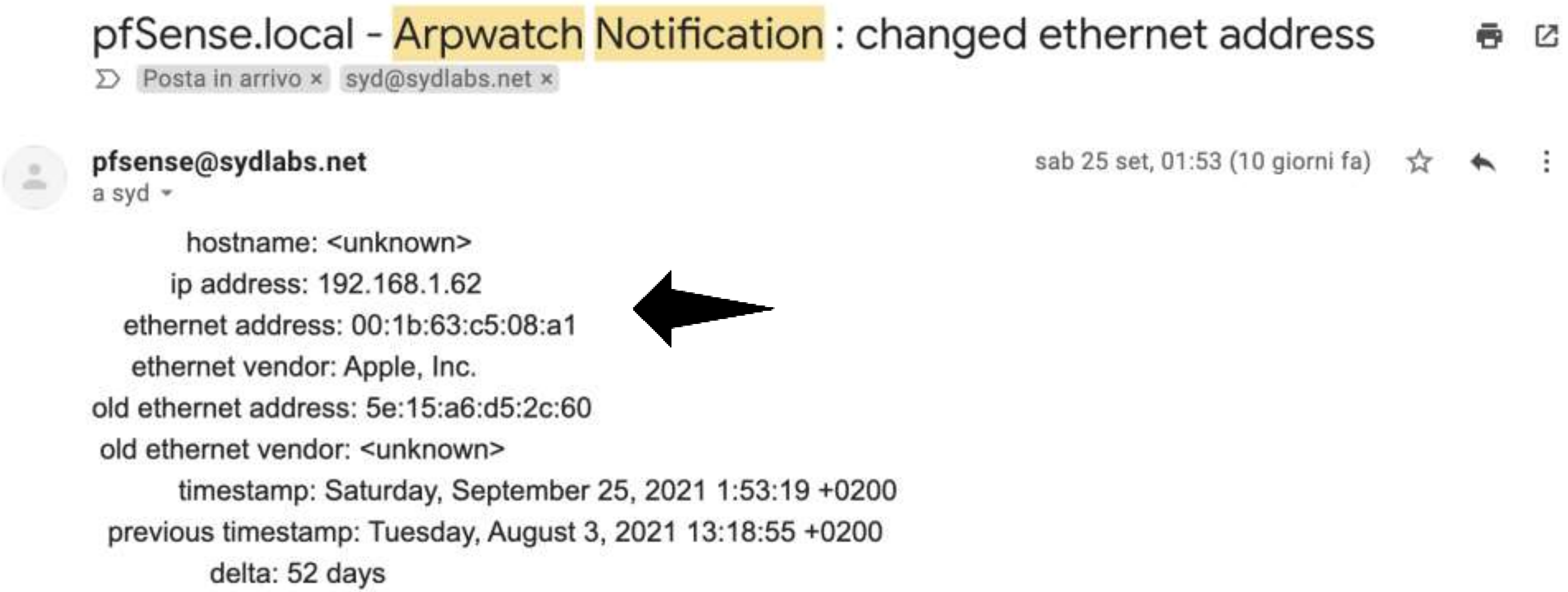
pfsense@sydlabs.net

mer 29 set, 12:59 (6 giorni fa)

```
      hostname: <unknown>
    ip address: 169.254.13.146
ethernet address: de:e3:a4:fd:e8:69
 ethernet vendor: <unknown>
     timestamp: Wednesday, September 29, 2021 12:59:55 +0200
```

ARP Watch example 2

- Arpwatch is a tool to perform L2 monitor in real time



pfSense.local - Arpwatch Notification : changed ethernet address

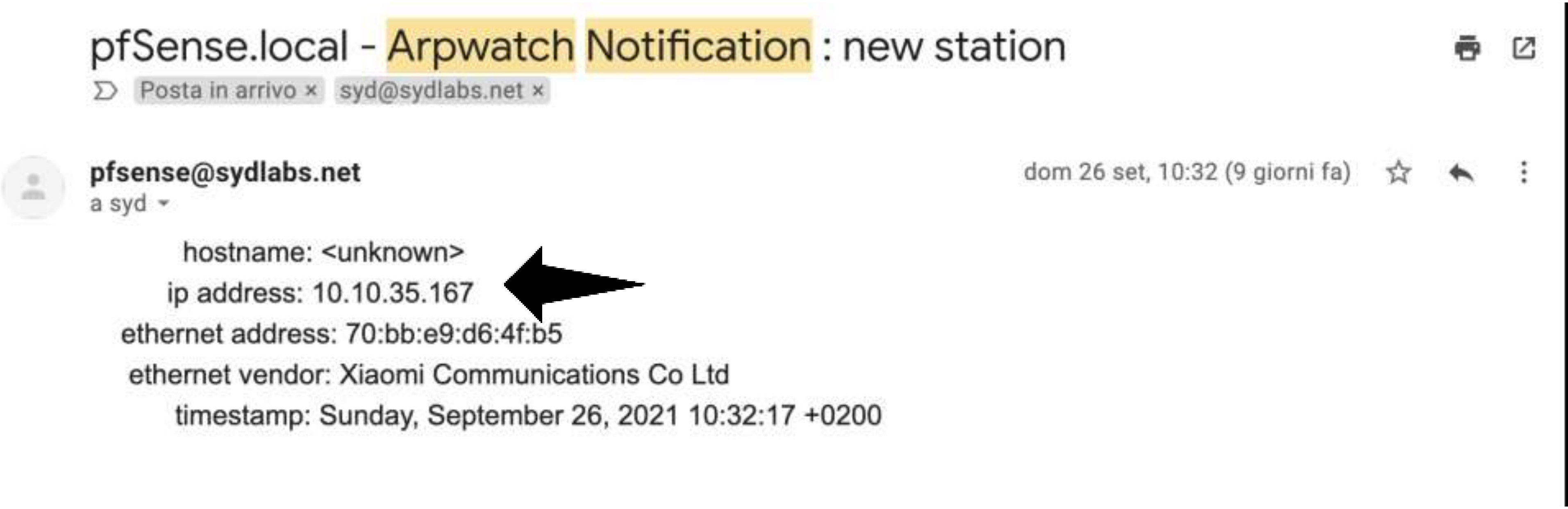
pfsense@sydlabs.net
a syd

sab 25 set, 01:53 (10 giorni fa)

```
         hostname: <unknown>
       ip address: 192.168.1.62
 ethernet address: 00:1b:63:c5:08:a1
  ethernet vendor: Apple, Inc.
old ethernet address: 5e:15:a6:d5:2c:60
 old ethernet vendor: <unknown>
        timestamp: Saturday, September 25, 2021 1:53:19 +0200
previous timestamp: Tuesday, August 3, 2021 13:18:55 +0200
            delta: 52 days
```

ARP Watch example 3

- Arpwatch is a tool to perform L2 monitor in real time



pfSense.local - Arpwatch Notification : new station

pfsense@sydlabs.net
a syd

dom 26 set, 10:32 (9 giorni fa)

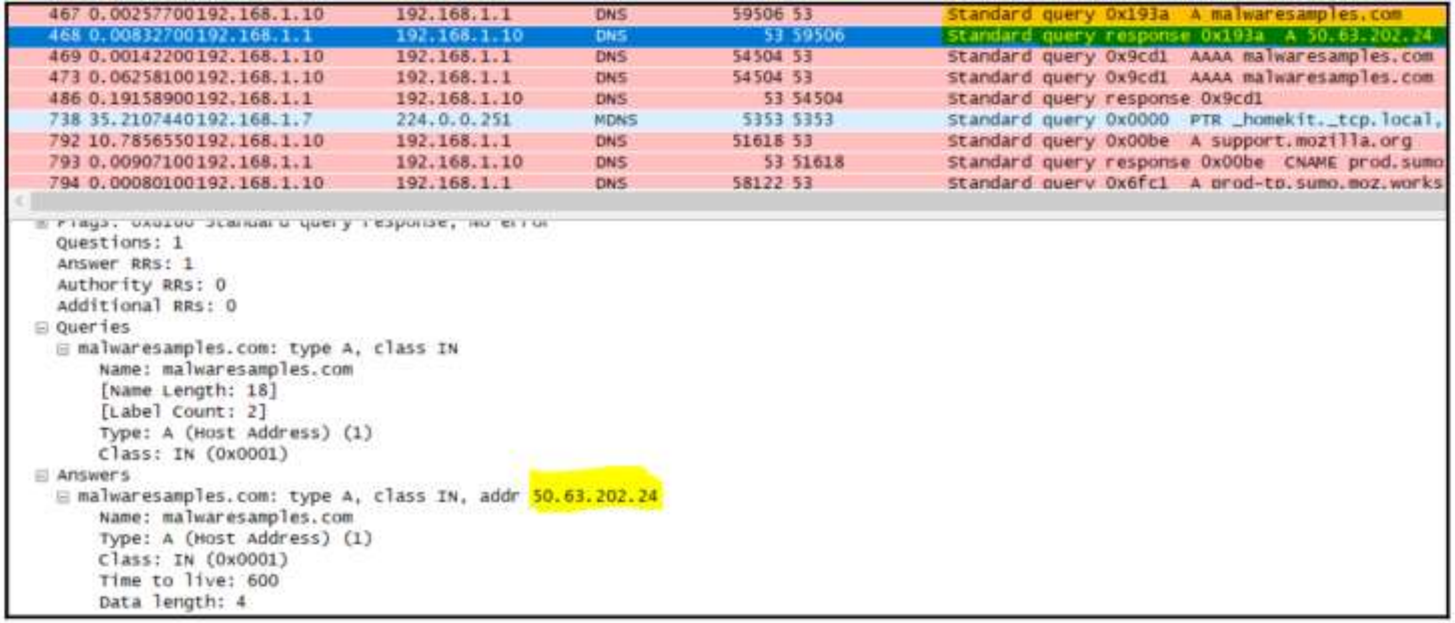
```
       hostname: <unknown>
     ip address: 10.10.35.167
ethernet address: 70:bb:e9:d6:4f:b5
 ethernet vendor: Xiaomi Communications Co Ltd
      timestamp: Sunday, September 26, 2021 10:32:17 +0200
```

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

DNS servers logs

- Name server query logs (if exists!) can help understand IP-to-hostname resolution at specific times.
- Consider a scenario where, as soon as a system got infected with malware on the network, it tried to connect back to a certain domain for command and control



```
467 0.00257700192.168.1.10    192.168.1.1    DNS    59506 53     Standard query 0x193a  A malwaresamples.com
468 0.00832700192.168.1.1     192.168.1.10   DNS       53 59506  Standard query response 0x193a  A 50.63.202.24
469 0.00142200192.168.1.10    192.168.1.1    DNS    54504 53     Standard query 0x9cd1  AAAA malwaresamples.com
473 0.06258100192.168.1.10    192.168.1.1    DNS    54504 53     Standard query 0x9cd1  AAAA malwaresamples.com
486 0.19158900192.168.1.1     192.168.1.10   DNS       53 54504  Standard query response 0x9cd1
738 35.2107440192.168.1.7     224.0.0.251    MDNS    5353 5353   Standard query 0x0000  PTR _homekit._tcp.local,
792 10.7856550192.168.1.10    192.168.1.1    DNS    51618 53     Standard query 0x00be  A support.mozilla.org
793 0.00907100192.168.1.1     192.168.1.10   DNS       53 51618  Standard query response 0x00be  CNAME prod.sumo
794 0.00080100192.168.1.10    192.168.1.1    DNS    58122 53     Standard query 0x6fc1  A prod-tp.sumo.moz.works
```

```
⊞ Flags: 0x8100 Standard query response, No error
   Questions: 1
   Answer RRs: 1
   Authority RRs: 0
   Additional RRs: 0
⊟ Queries
  ⊟ malwaresamples.com: type A, class IN
       Name: malwaresamples.com
       [Name Length: 18]
       [Label Count: 2]
       Type: A (Host Address) (1)
       Class: IN (0x0001)
⊟ Answers
  ⊟ malwaresamples.com: type A, class IN, addr 50.63.202.24
       Name: malwaresamples.com
       Type: A (Host Address) (1)
       Class: IN (0x0001)
       Time to live: 600
       Data length: 4
```

- We can see in the preceding screenshot that a DNS request was resolved for malwaresamples.com website and the resolved IP address was returned.

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

Domain controller/authentication servers/syslogs

- Authentication servers can allow an investigator to view login attempts, the time of the login, and various other login-related activities throughout the network.

- ..or /var/log/auth.log.* (…)

- Consider a scenario where a group of attackers tries to use a compromised host to log into the database server by using the compromised machine as a launchpad (pivoting).

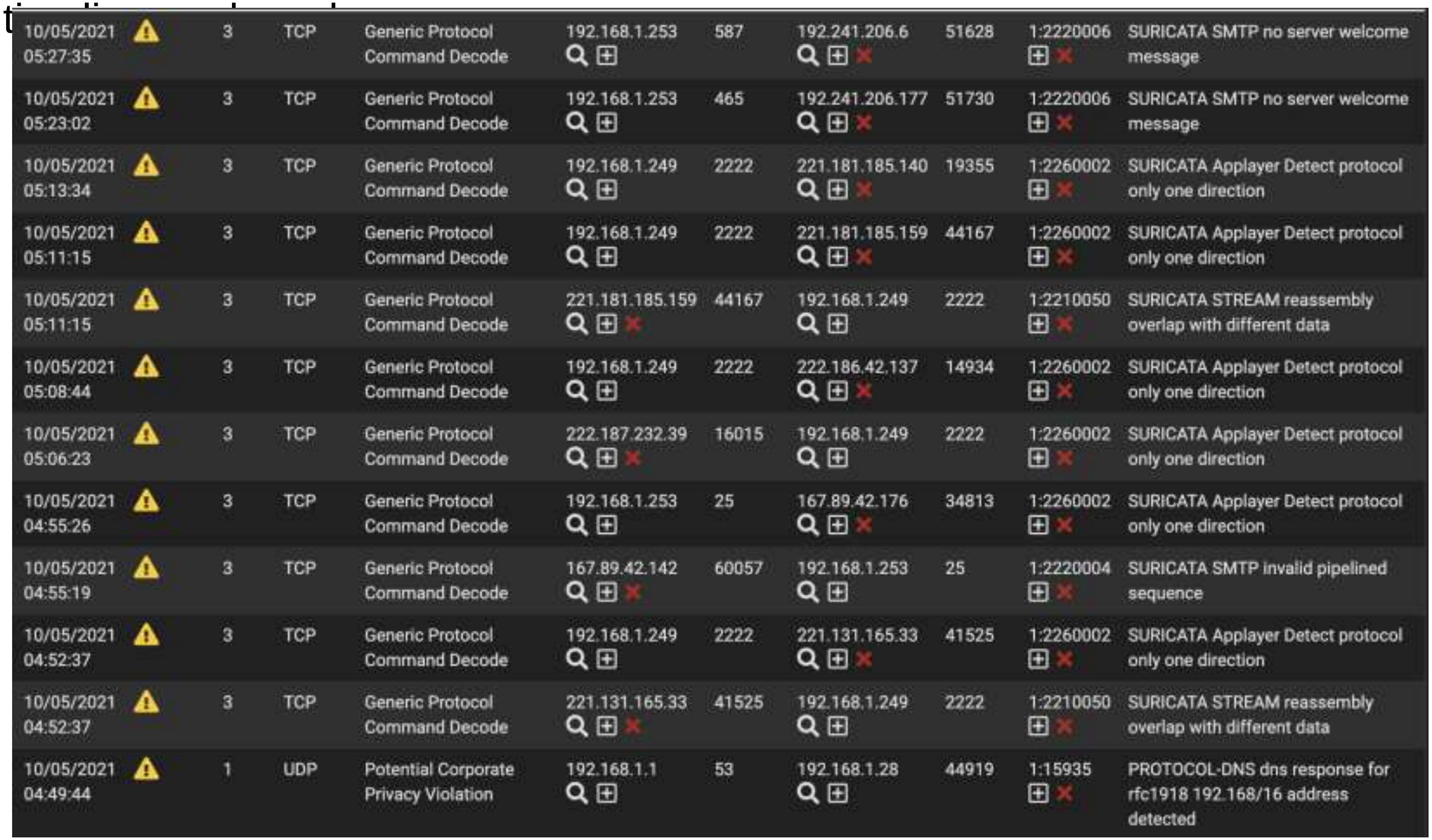
- In such cases, authentication logs will quickly reveal not only the infected system, but also the number of failed/passed attempts from the system to the database server.

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

IDS/IPS Logs

○ From a forensic standpoint, intrusion detection/prevention system logs are the most helpful. IDS/IPS logs provide not only the IP address, but also the matched signatures, on-going attacks, malware presence, command-and-control servers, the IP and port for the source and destination systems, a t



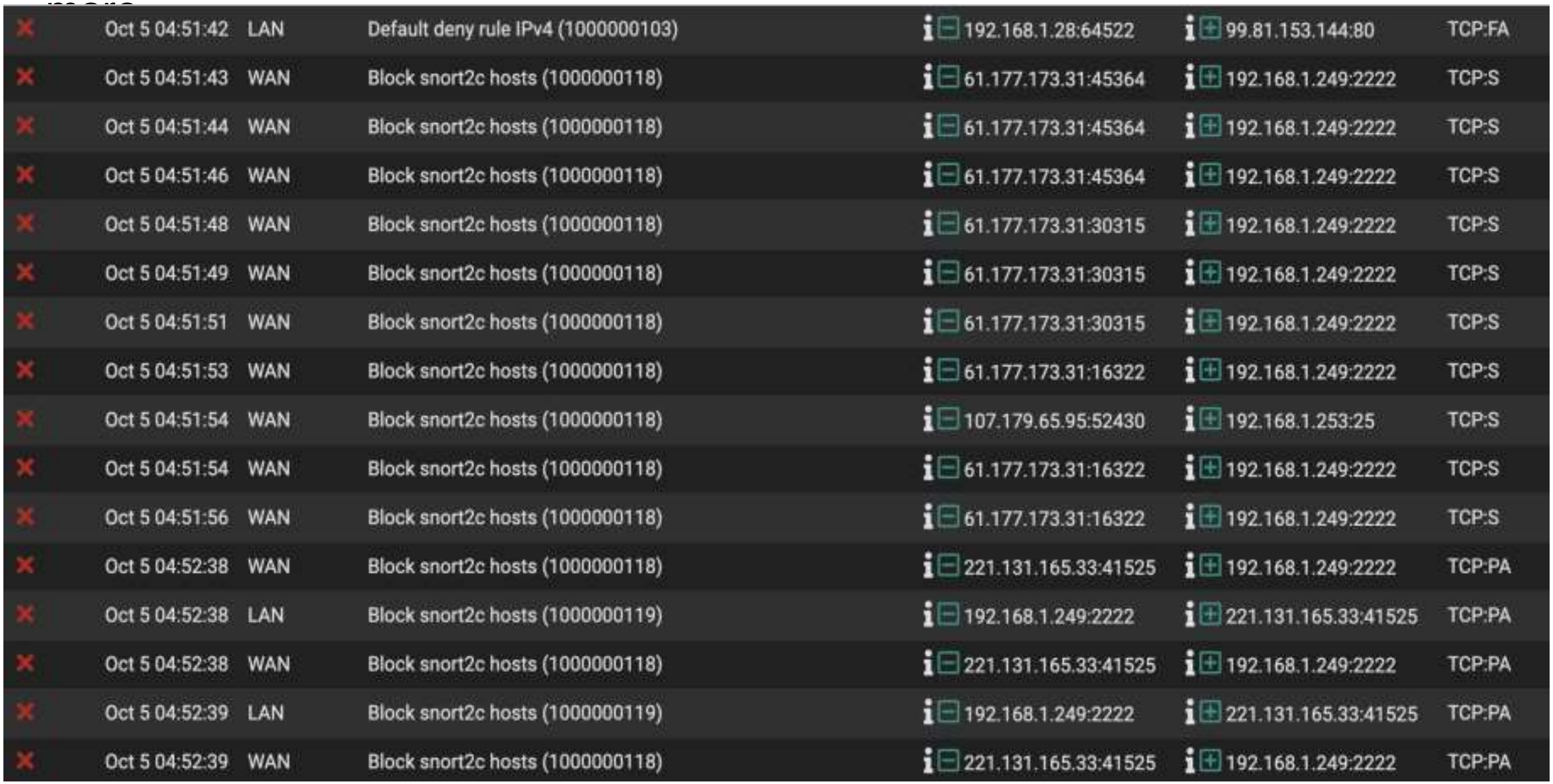
10/05/2021 05:27:35	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.253 🔍 ⊞	587	192.241.206.6 🔍 ⊞ ✕	51628	1:2220006 ⊞ ✕	SURICATA SMTP no server welcome message
10/05/2021 05:23:02	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.253 🔍 ⊞	465	192.241.206.177 🔍 ⊞ ✕	51730	1:2220006 ⊞ ✕	SURICATA SMTP no server welcome message
10/05/2021 05:13:34	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.249 🔍 ⊞	2222	221.181.185.140 🔍 ⊞ ✕	19355	1:2260002 ⊞ ✕	SURICATA Applayer Detect protocol only one direction
10/05/2021 05:11:15	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.249 🔍 ⊞	2222	221.181.185.159 🔍 ⊞ ✕	44167	1:2260002 ⊞ ✕	SURICATA Applayer Detect protocol only one direction
10/05/2021 05:11:15	⚠	3	TCP	Generic Protocol Command Decode	221.181.185.159 🔍 ⊞ ✕	44167	192.168.1.249 🔍 ⊞	2222	1:2210050 ⊞ ✕	SURICATA STREAM reassembly overlap with different data
10/05/2021 05:08:44	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.249 🔍 ⊞	2222	222.186.42.137 🔍 ⊞ ✕	14934	1:2260002 ⊞ ✕	SURICATA Applayer Detect protocol only one direction
10/05/2021 05:06:23	⚠	3	TCP	Generic Protocol Command Decode	222.187.232.39 🔍 ⊞ ✕	16015	192.168.1.249 🔍 ⊞	2222	1:2260002 ⊞ ✕	SURICATA Applayer Detect protocol only one direction
10/05/2021 04:55:26	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.253 🔍 ⊞	25	167.89.42.176 🔍 ⊞ ✕	34813	1:2260002 ⊞ ✕	SURICATA Applayer Detect protocol only one direction
10/05/2021 04:55:19	⚠	3	TCP	Generic Protocol Command Decode	167.89.42.142 🔍 ⊞ ✕	60057	192.168.1.253 🔍 ⊞	25	1:2220004 ⊞ ✕	SURICATA SMTP invalid pipelined sequence
10/05/2021 04:52:37	⚠	3	TCP	Generic Protocol Command Decode	192.168.1.249 🔍 ⊞	2222	221.131.165.33 🔍 ⊞ ✕	41525	1:2260002 ⊞ ✕	SURICATA Applayer Detect protocol only one direction
10/05/2021 04:52:37	⚠	3	TCP	Generic Protocol Command Decode	221.131.165.33 🔍 ⊞ ✕	41525	192.168.1.249 🔍 ⊞	2222	1:2210050 ⊞ ✕	SURICATA STREAM reassembly overlap with different data
10/05/2021 04:49:44	⚠	1	UDP	Potential Corporate Privacy Violation	192.168.1.1 🔍 ⊞	53	192.168.1.28 🔍 ⊞	44919	1:15935 ⊞ ✕	PROTOCOL-DNS dns response for rfc1918 192.168/16 address detected

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

Firewall Logs

- Firewall logs provide a detailed view of activities on the network. Not only do firewall solutions protect a server or a network from unwanted connections, they also help to identify the type of traffic, provide a trust score to the outbound endpoint, block unwanted ports and connection attempts, and much more



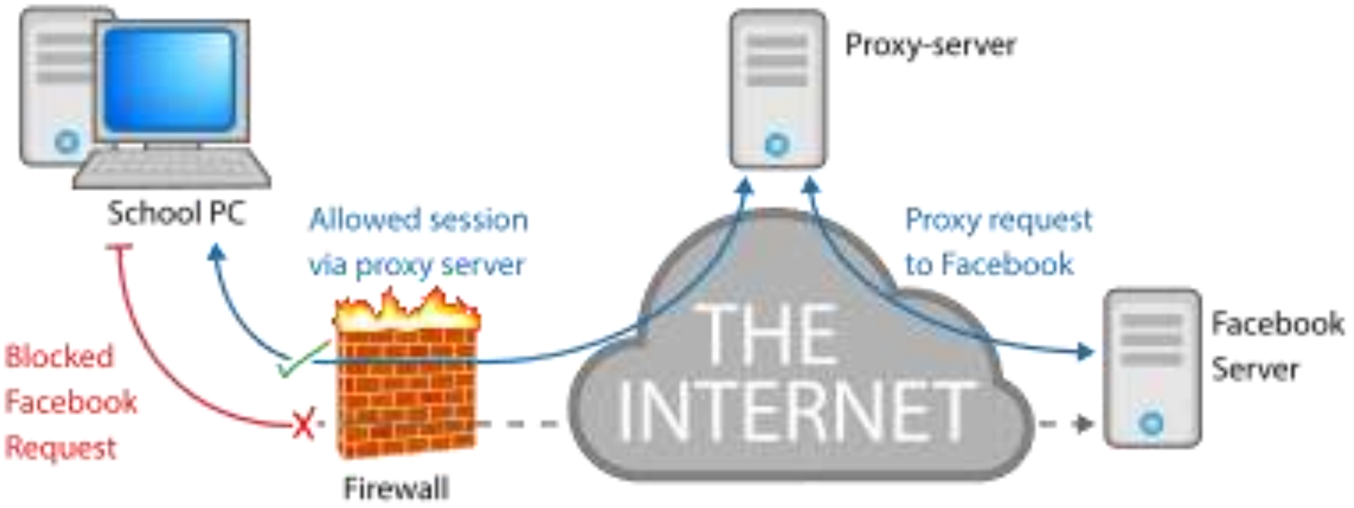
```
✕  Oct 5 04:51:42  LAN  Default deny rule IPv4 (1000000103)  192.168.1.28:64522     99.81.153.144:80        TCP:FA
✕  Oct 5 04:51:43  WAN  Block snort2c hosts (1000000118)     61.177.173.31:45364     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:44  WAN  Block snort2c hosts (1000000118)     61.177.173.31:45364     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:46  WAN  Block snort2c hosts (1000000118)     61.177.173.31:45364     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:48  WAN  Block snort2c hosts (1000000118)     61.177.173.31:30315     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:49  WAN  Block snort2c hosts (1000000118)     61.177.173.31:30315     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:51  WAN  Block snort2c hosts (1000000118)     61.177.173.31:30315     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:53  WAN  Block snort2c hosts (1000000118)     61.177.173.31:16322     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:54  WAN  Block snort2c hosts (1000000118)     107.179.65.95:52430     192.168.1.253:25        TCP:S
✕  Oct 5 04:51:54  WAN  Block snort2c hosts (1000000118)     61.177.173.31:16322     192.168.1.249:2222      TCP:S
✕  Oct 5 04:51:56  WAN  Block snort2c hosts (1000000118)     61.177.173.31:16322     192.168.1.249:2222      TCP:S
✕  Oct 5 04:52:38  WAN  Block snort2c hosts (1000000118)     221.131.165.33:41525    192.168.1.249:2222      TCP:PA
✕  Oct 5 04:52:38  LAN  Block snort2c hosts (1000000119)     192.168.1.249:2222      221.131.165.33:41525    TCP:PA
✕  Oct 5 04:52:38  WAN  Block snort2c hosts (1000000118)     221.131.165.33:41525    192.168.1.249:2222      TCP:PA
✕  Oct 5 04:52:39  LAN  Block snort2c hosts (1000000119)     192.168.1.249:2222      221.131.165.33:41525    TCP:PA
✕  Oct 5 04:52:39  WAN  Block snort2c hosts (1000000118)     221.131.165.33:41525    192.168.1.249:2222      TCP:PA
```

Source of network evidence

- Tapping the wire and the air
- CAM table on a network switch
- Routing tables on routers
- Dynamic Host Configuration Protocol logs
- DNS server logs
- Domain controller/ authentication servers/ system logs
- IDS/IPS logs
- Firewall logs
- Proxy Server logs

Web Proxy Logs

- Web proxies are also one of the most useful features for a forensic investigator.
- Web proxy logs help uncover internal threats while providing explicit detail on events such as surfing habits, the source of web-based malware, the user's behavior on the network, and so on.



Phone Number
+39 050 3820810

Info
rass@cnit.it

Website
http://labrass.cnit.it/

Where We are
Galleria Gerace 18
56124 Pisa, Italy

Director
Prof. Marco Martorella
marco.martorella@cnit.it
Ph. Office +39 3820818
Mobile: +39 3475848897
Fax: +39 0503820571

QUALITY SYSTEM CERTIFICATION
DNV·GL
ISO 9001:2015

Leading the present, enhancing the future.