

# Threat Hunting

---

HW02

---

Name: 劉定睿 ID: M11409313

Date: 2025-09-25

# 目錄

---

- Investigating the Local Computer
- Investigating the Network Environment
- Reflection

# Investigating the Local Computer

- First of all I use command: `netstat -ano` to list all of the connection

```
C:\Users\foren>netstat -ano
使用中連線

協定    本機位址          外部位址          狀態          PID
TCP     0.0.0.0:135       0.0.0.0:0         LISTENING     1468
TCP     0.0.0.0:445       0.0.0.0:0         LISTENING     4
TCP     0.0.0.0:902       0.0.0.0:0         LISTENING     5616
TCP     0.0.0.0:912       0.0.0.0:0         LISTENING     5616
TCP     0.0.0.0:2179      0.0.0.0:0         LISTENING     2752
TCP     0.0.0.0:5040      0.0.0.0:0         LISTENING     5588
TCP     0.0.0.0:7680      0.0.0.0:0         LISTENING     8704
TCP     0.0.0.0:8834      0.0.0.0:0         LISTENING     7020
TCP     0.0.0.0:49664     0.0.0.0:0         LISTENING     1204
TCP     0.0.0.0:49665     0.0.0.0:0         LISTENING     1028
TCP     0.0.0.0:49666     0.0.0.0:0         LISTENING     3108
TCP     0.0.0.0:49667     0.0.0.0:0         LISTENING     3088
TCP     0.0.0.0:49668     0.0.0.0:0         LISTENING     4928
TCP     0.0.0.0:49694     0.0.0.0:0         LISTENING     1156
TCP     127.0.0.1:8053    0.0.0.0:0         LISTENING     3864
TCP     127.0.0.1:9080    0.0.0.0:0         LISTENING     5228
TCP     127.0.0.1:22350   0.0.0.0:0         LISTENING     11232
TCP     127.0.0.1:36167   0.0.0.0:0         LISTENING     15060
TCP     127.0.0.1:49692   127.0.0.1:49693   ESTABLISHED    7020
TCP     127.0.0.1:49693   127.0.0.1:49692   ESTABLISHED    7020
TCP     127.0.0.1:49697   127.0.0.1:49698   ESTABLISHED    7020
TCP     127.0.0.1:49698   127.0.0.1:49697   ESTABLISHED    7020
TCP     127.0.0.1:49698   127.0.0.1:49697   ESTABLISHED    7020
TCP     127.0.0.1:50708   127.0.0.1:55017   ESTABLISHED    23740
TCP     127.0.0.1:55017   0.0.0.0:0         LISTENING     11612
TCP     127.0.0.1:55017   127.0.0.1:50708   ESTABLISHED    11612
```

- There's too much log so we need to filter it by `id=3`.
  - use: `netstat -ano | findstr ESTABLISHED`

```
C:\Users\foren>netstat -ano | findstr ESTABLISHED
TCP     127.0.0.1:49692    127.0.0.1:49693    ESTABLISHED    7020
TCP     127.0.0.1:49693    127.0.0.1:49692    ESTABLISHED    7020
TCP     127.0.0.1:49697    127.0.0.1:49698    ESTABLISHED    7020
TCP     127.0.0.1:49698    127.0.0.1:49697    ESTABLISHED    7020
TCP     127.0.0.1:50708    127.0.0.1:55017    ESTABLISHED    23740
TCP     127.0.0.1:55017    127.0.0.1:50708    ESTABLISHED    11612
TCP     192.168.1.143:50672 172.166.106.148:443 ESTABLISHED    6016
TCP     192.168.1.143:50678 91.108.56.122:443   ESTABLISHED    16980
TCP     192.168.1.143:50680 172.167.2.3:443     ESTABLISHED    4792
TCP     192.168.1.143:50745 31.13.87.4:443      ESTABLISHED    14908
TCP     192.168.1.143:50749 31.13.87.53:443     ESTABLISHED    14908
TCP     192.168.1.143:50750 31.13.87.1:443      ESTABLISHED    14908
TCP     192.168.1.143:50757 44.230.16.251:443   ESTABLISHED    14908
TCP     192.168.1.143:50758 175.97.131.54:443   ESTABLISHED    14908
TCP     192.168.1.143:50761 104.18.27.48:443    ESTABLISHED    14908
TCP     192.168.1.143:50763 31.13.87.1:443      ESTABLISHED    14908
TCP     192.168.1.143:50765 43.174.225.10:443   ESTABLISHED    14908
TCP     192.168.1.143:50769 31.13.87.1:443      ESTABLISHED    14908
TCP     192.168.1.143:50776 140.82.114.25:443   ESTABLISHED    14908
TCP     192.168.1.143:50807 146.75.46.137:443   ESTABLISHED    14908
TCP     192.168.1.143:50817 52.17.119.191:8282  ESTABLISHED    14908
TCP     192.168.1.143:50825 34.36.213.229:443   ESTABLISHED    14908
TCP     192.168.1.143:50827 34.36.213.229:443   ESTABLISHED    14908
TCP     192.168.1.143:50828 3.169.36.96:443     ESTABLISHED    14908
TCP     192.168.1.143:50838 146.75.93.91:443    ESTABLISHED    14908
TCP     192.168.1.143:50841 146.75.93.91:443    ESTABLISHED    14908
```

- I found a connection that connect to 8282 port. It's not usual to see. So I assume it to be abnormal.

```
TCP     192.168.1.143:50807 146.75.46.137:443   ESTABLISHED    14908
TCP     192.168.1.143:50817 52.17.119.191:8282  ESTABLISHED    14908
TCP     192.168.1.143:50825 34.36.213.229:443   ESTABLISHED    14908
```

Then I try to investigate the IP address and port.

- `whois 52.17.119.191`

It shows that this IP address is host at a AWS machine. And It locate at I

```
└─$ whois 52.17.119.191
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

# start
NetRange:      52.0.0.0 - 52.79.255.255
CIDR:          52.64.0.0/12, 52.0.0.0/10
NetName:       AT-88-Z
NetHandle:     NET-52-0-0-0-1
Parent:        NET52 (NET-52-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Amazon Technologies Inc. (AT-88-Z)
RegDate:      1991-12-19
Updated:      2024-02-05
Comment:      Geofeed http://ip-ranges.amazonaws.com/geo-ip-feed.csv
Ref:          https://rdap.arin.net/registry/ip/52.0.0.0

OrgName:       Amazon Technologies Inc.
OrgId:         AT-88-Z
Address:       410 Terry Ave N.
City:          Seattle
StateProv:    WA
```

- `nslookup reverse lookup (IP to Domain name): nslookup 52.17.119.191 .`

```
└─$ nslookup 52.17.119.191
191.119.17.52.in-addr.arpa      name = ec2-52-17-119-191.eu-west-1.compute.amazonaws.com.

Authoritative answers can be found from:
```

Looks like a AWS server

- Use `nmap` to check the service name at 8282 port

```
└─$ nmap -sV -sC 52.17.119.191 -p 8282
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 09:30 CST
Nmap scan report for ec2-52-17-119-191.eu-west-1.compute.amazonaws.com (52.17.119.191)
Host is up (0.0010s latency).

PORT      STATE      SERVICE VERSION
8282/tcp  filtered  libelle

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

- Check the service name: `libelle`

8282	libelle	TCP	Libelle EnterpriseBus	Registered: 2016-02-17
8282	libelle-disc	UDP	Libelle EnterpriseBus discovery	Registered: 2016-02-17
8282		SCTP/DCCP	Reserved	

ref: <https://www.gaijin.at/en/infos/port-numbers?page=13>

(<https://www.gaijin.at/en/infos/port-numbers?page=13>).

- Gain more information in libelle

## what is Libelle EnterpriseBus in 8282 port?

Perplexity 圖像 來源 · 14 步驟

iana.org Service Name and Transport Protocol Port...

iana.org Service Name and Transport Protocol Port...

gaijin.at Port Numbers

SpeedGuide 8282/tcp

Libelle EnterpriseBus 是由德國 Libelle AG 公司開發的一種企業級中介 (middleware) 產品，其在 8282/tcp 端口上註冊了專用服務名 "libelle"。根據 IANA (國際指派數字局) 公開資料，8282/tcp (libelle) 與 8282/udp (libelle-disc) 分別對應 Libelle EnterpriseBus 以及其發現 (discovery) 功能。 [iana +3](#)

### 8282 Port 與 Libelle EnterpriseBus 的用途

- 8282/tcp 是 Libelle EnterpriseBus 的預設通訊端口，主要用於系統內部不同元件之間通訊。 [vwnet +1](#)
- 8282/udp (libelle-disc) 通常用於服務發現，即讓系統內的其他服務或節點能自動偵測 Libelle EnterpriseBus 的存在。 [gaijin +1](#)

### Libelle EnterpriseBus 簡介

- 這是一種企業服務匯流排 (Enterprise Service Bus, ESB) 產品，用於整合多個後端應用、數據庫和系統，實現資料流轉、彈性調度與系統整合。
- 主要客群為大型企業需實現系統彼此高速且可靠的資料交換。 [iana +2](#)

ref: perplexity

- Check the process: `tasklist /FI "PID eq 14908"` .

Shows that PID is from my browser executable file. So I consider that could be normal.

```
TCP 192.168.1.143:50807 146.75.46.137:443 ESTABLISHED 14908
TCP 192.168.1.143:50817 52.17.119.191:8282 ESTABLISHED 14908
TCP 192.168.1.143:50825 34.36.213.229:443 ESTABLISHED 14908
```

```
C:\Users\foren>tasklist /FI "PID eq 14908"
```

映像名稱	PID	工作階段名稱	工作階段 #	RAM使用量
brave.exe	14908	Console	7	72,068 K

- Use AbuseIPDB check it seems no abnormal.

Check an IP Address, Domain Name, or Subnet  
e.g. 111.251.74.246, microsoft.com, or 5.188.10.0/24

52.17.119.191 CHECK

**52.17.119.191** was not found in our database

ISP	Amazon Data Services Ireland Limited
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	ec2-52-17-119-191.eu-west-1.compute.amazonaws.com
Domain Name	amazon.com
Country	Ireland
City	Dublin, Leinster

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

REPORT 52.17.119.191 WHOIS 52.17.119.191

- Using virustotal check it seems to be safe.

52.17.119.191

Did you intend to search across the file corpus instead? [Click here](#)

**0** / 95  
Community Score

No security vendor flagged this IP address as malicious Reanalyze Similar More

52.17.119.191 (52.16.0.0/14)  
AS 16509 (AMAZON-02) IE Last Analysis Date 3 months ago

DETECTION DETAILS **RELATIONS** COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (41)

Date resolved	Detections	Resolver	Domain
2024-09-23	0 / 95	VirusTotal	ws.mailtrack.io
2024-02-26	0 / 95	VirusTotal	fd.digitaltrust.feedzai.cloud
2023-11-29	0 / 95	VirusTotal	portal.miningcadastre.go.ke
2023-11-29	0 / 95	VirusTotal	tenement.miningcadastre.go.ke
2023-11-29	0 / 95	VirusTotal	licensing.miningcadastre.go.ke
2023-11-29	0 / 95	VirusTotal	dashboard.miningcadastre.go.ke
2023-11-29	0 / 95	VirusTotal	map.miningcadastre.go.ke
2023-07-12	0 / 95	VirusTotal	collector.secretescapes.com
2023-03-15	0 / 95	VirusTotal	shs.eu.qlikcloud.com
2023-03-01	0 / 95	VirusTotal	7w4unjw4qy6ovh2.eu.qlikcloud.com

- Check which extension use it.  
I search the IP address 52.17.119.191 in google. And finally know that this IP is come from "Mailsuite" extension.

- 54.194.36.47
- 34.246.13.131
- 54.171.22.33
- 54.77.56.1
- 52.17.119.191
- 52.18.207.76
- 52.209.92.165
- 54.170.30.185
- 52.17.119.201
- 52.48.72.84

ref: <https://mailsuite.com/hc/en-us/articles/17628486344477-Whitelist-Mailsuite-IPs> (<https://mailsuite.com/hc/en-us/articles/17628486344477-Whitelist-Mailsuite-IPs>).

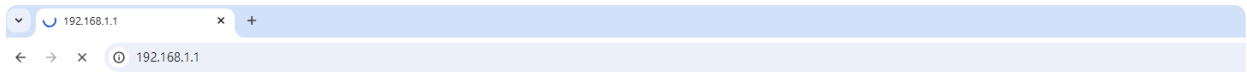
## Investigating the Network Environment

- `ipconfig` to check my gateway.

無線區域網路介面卡 Wi-Fi:

```
連線特定 DNS 尾碼 . . . . . : ██████████
IPv4 位址 . . . . . : 192.168.1.143
子網路遮罩 . . . . . : 255.255.255.0
預設閘道 . . . . . : 192.168.1.1
```

- Access to gateway. And shows that I can't connect to it.



## 無法連上這個網站

192.168.1.1 的回應時間過長。

建議做法：

- 檢查連線狀態
- 檢查 Proxy 和防火牆
- 執行 Windows 網路診斷

ERR\_CONNECTION\_TIMED\_OUT

- `nmap -F 192.168.1.1` found that I need to use 443 port to access

```
└─$ nmap -F 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-16 20:11 CST
Nmap scan report for home (192.168.1.1)
Host is up (0.011s latency).
Not shown: 94 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open      domain
80/tcp    filtered  http
443/tcp   open      https
```

← → ↻ × 不安全 https://192.168.1.1/login

**ZYXEL** | PMG4506-T20B

- But the management dashboard has not Log file. So I'm not going to deep dive into it.

## Reflection

---

In this report, I try to use the command line interface to check different network information to find the abnormal process and flow. When I see some connectio or information are different with each others. I will assume it could be malicious or abnormal. Then try to investigate the information and deep dive into it. Later, I can get the whole picture by the incident. And distinguish perhaps it is malicious or not.