14 JANVIER 2026

NETWORK TRAFFIC ANALYSIS TOOL - USER MANUAL

SEE SUMMARY

ABIDERRAHMANE ADAM
STUDENT - BUT NETWORKS & TELECOMMUNICATIONSIUT ROANNE

SUMMARY

I. WHAT'S THIS ABOUT? :

So basically, we had this network issue at the India site - super slow connection, packets dropping everywhere. Turned out we needed to analyze tcpdump captures to find what's causing the problem.

I built this toolkit with 2 Python scripts and an Excel macro. It's pretty straightforward once you get it, trust me.

Setup (Do This First) :

- Script 1 converts messy tcpdump files into clean CSV

- Script 2 analyzes the CSV and makes nice charts

- Excel macro does extra analysis if you need it

Let's go through it step by step.

II. SETUP (DO THIS FIRST) :

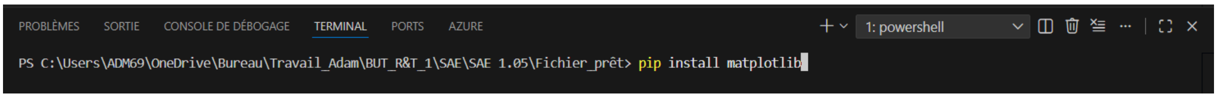
You need Python 3 installed. If you don't have it:

- Go to python.org and download it

- When installing, CHECK that box that says "Add to PATH" (important!)

Then open cmd/terminal and run:

```
pip install matplotlib
```



```
PS C:\Users\ADM69\OneDrive\Bureau\Travail_Adam\BUT_R&T_1\SAE\SAE 1.05\Fichier_prêt> pip install matplotlib
```

That's the graphing library. Takes like 30 seconds to install.

For the Excel part, you obviously need Excel (2016 or newer works fine).

III. PART 1: CONVERTING TCPDUMP TO CSV :

What You're Doing :

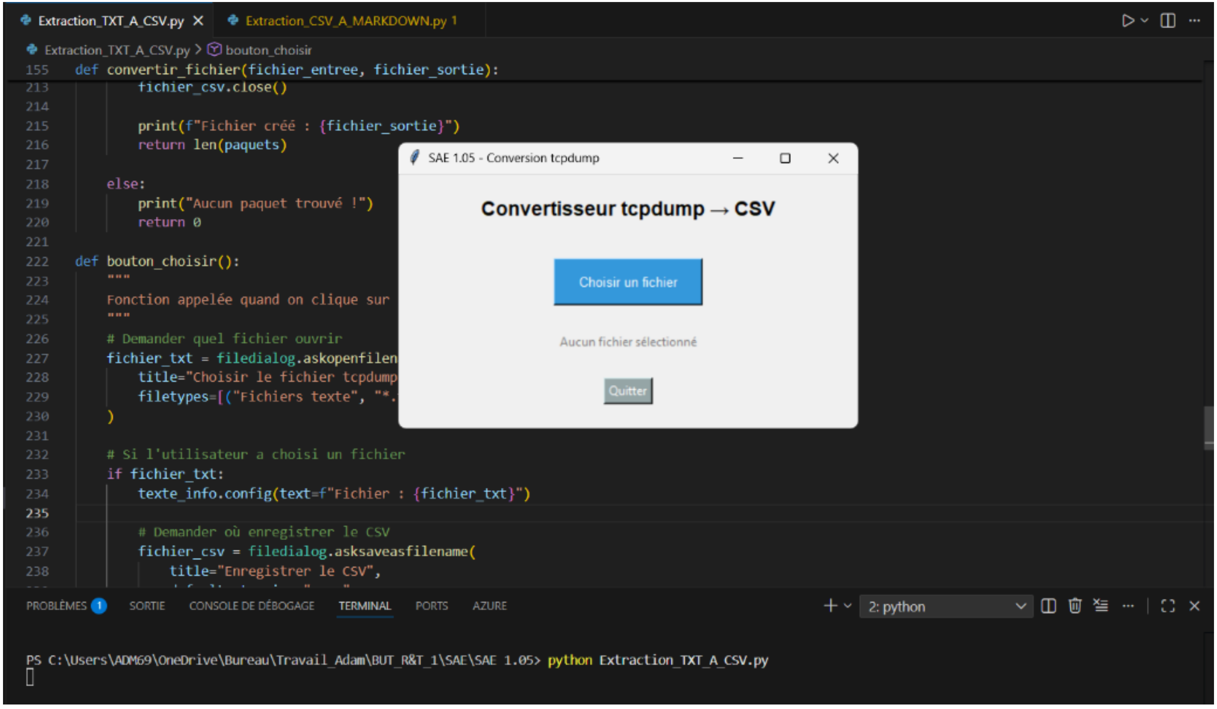
Tcpdump files are unreadable. This script parses them into a proper spreadsheet format.

Steps :

1. Put `Extraction_TXT_A_CSV.py` and your tcpdump file in the same folder (makes life easier)

2. Open terminal/cmd in that folder and run:

```
python3 Extraction_TXT_A_CSV.py
```

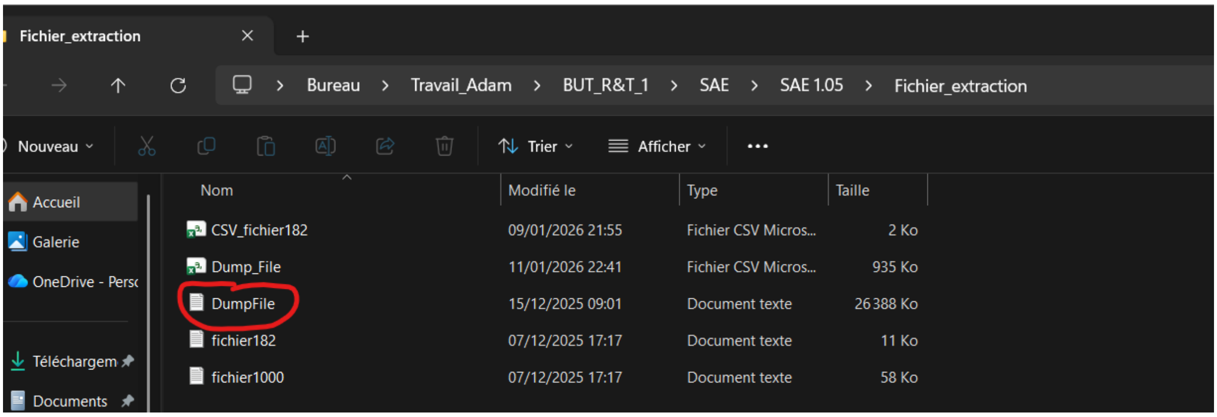

Extraction_TXT_A_CSV.py
Extraction_CSV_A_MARKDOWN.py 1
Extraction_TXT_A_CSV.py > bouton_choisir
SAE 1.05 - Conversion tcpdump
Convertisseur tcpdump → CSV
Choisir un fichier
Aucun fichier sélectionné
Quitter
PROBLÈMES 1
SORTIE
CONSOLE DE DÉBOGAGE
TERMINAL
PORTS
AZURE
2: python

```
def convertir_fichier(fichier_entree, fichier_sortie):
        fichier_csv.close()

        print(f"Fichier créé : {fichier_sortie}")
        return len(paquets)

    else:
        print("Aucun paquet trouvé !")
        return 0

def bouton_choisir():
    """
    Fonction appelée quand on clique sur
    """
    # Demander quel fichier ouvrir
    fichier_txt = filedialog.askopenfilen
        title="Choisir le fichier tcpdump
        filetypes=[("Fichiers texte", "*.
    )

    # Si l'utilisateur a choisi un fichier
    if fichier_txt:
        texte_info.config(text=f"Fichier : {fichier_txt}")

        # Demander où enregistrer le CSV
        fichier_csv = filedialog.asksaveasfilename(
            title="Enregistrer le CSV",
```

```
PS C:\Users\ADM69\OneDrive\Bureau\Travail_Adam\BUT_R&T_1\SAE\SAE 1.05> python Extraction_TXT_A_CSV.py
```

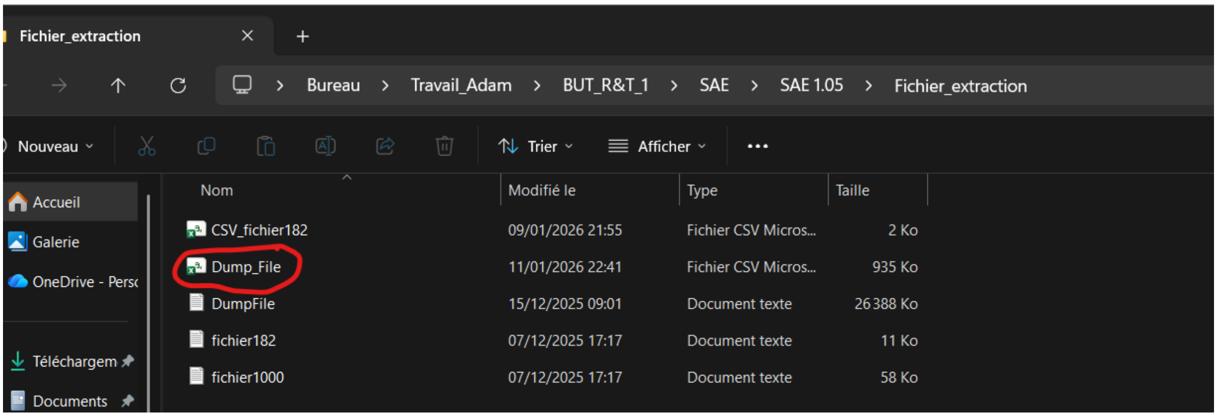
3. A window pops up. Click "Choisir un fichier" that’s choose file

4. Select your .txt tcpdump file



Nom	Modifié le	Type	Taille
CSV_fichier182	09/01/2026 21:55	Fichier CSV Micros...	2 Ko
Dump_File	11/01/2026 22:41	Fichier CSV Micros...	935 Ko
DumpFile	15/12/2025 09:01	Document texte	26 388 Ko
fichier182	07/12/2025 17:17	Document texte	11 Ko
fichier1000	07/12/2025 17:17	Document texte	58 Ko

5. Save it as DumpFile.csv



Nom	Modifié le	Type	Taille
CSV_fichier182	09/01/2026 21:55	Fichier CSV Micros...	2 Ko
Dump_File	11/01/2026 22:41	Fichier CSV Micros...	935 Ko
DumpFile	15/12/2025 09:01	Document texte	26 388 Ko
fichier182	07/12/2025 17:17	Document texte	11 Ko
fichier1000	07/12/2025 17:17	Document texte	58 Ko

6. Wait a bit. The console shows you progress:

- Lines read
- Packets extracted
- Lines ignored

7. Done! Your CSV is ready.

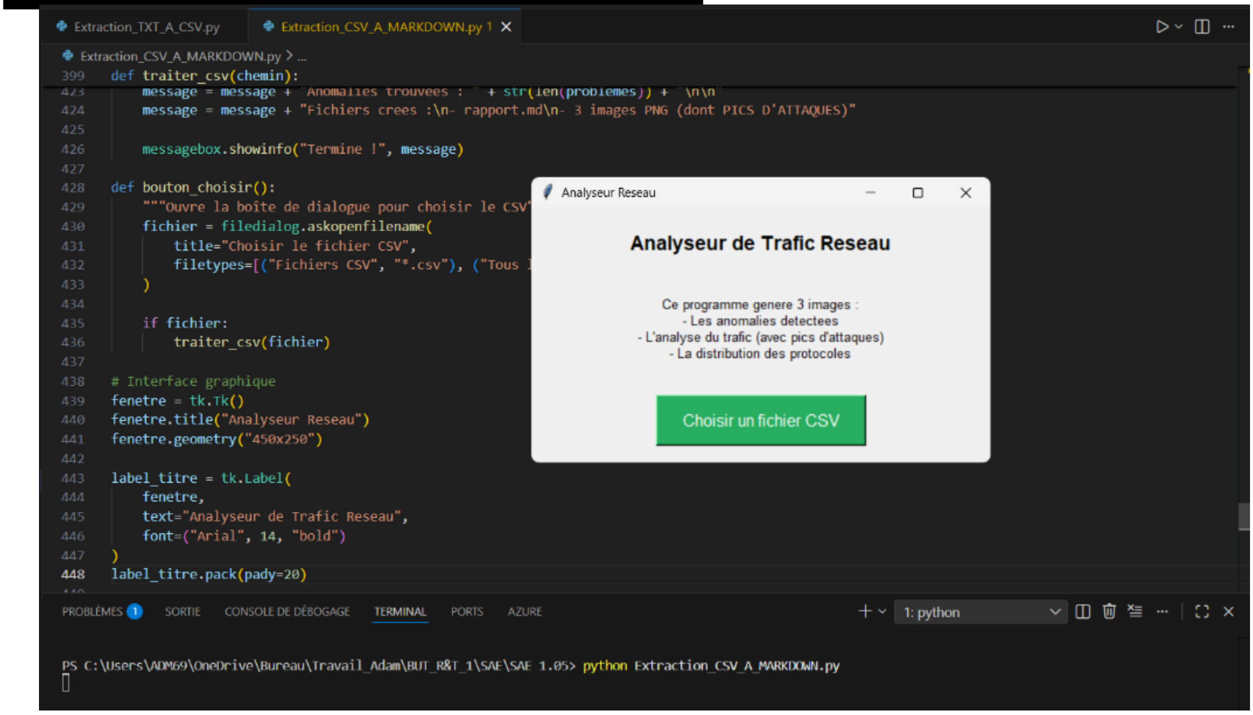
IV. PART 2: ANALYSIS & CHARTS :

This is where it gets interesting. The script analyzes everything and detects anomalies automatically.

Steps :

1. Run the second script:

```
python3 Extraction_CSV_A_MARKDOWN.py
```



```python
def traiter_csv(chemin):
    message = message + "Anomalies trouvees : " + str(len(problemes)) + "\n\n"
    message = message + "Fichiers crees :\n- rapport.md\n- 3 images PNG (dont PICS D'ATTAQUES)"

    messagebox.showinfo("Termine !", message)

def bouton_choisir():
    """Ouvre la boîte de dialogue pour choisir le CSV
    fichier = filedialog.askopenfilename(
        title="Choisir le fichier CSV",
        filetypes=[("Fichiers CSV", "*.csv"), ("Tous 
    )

    if fichier:
        traiter_csv(fichier)

# Interface graphique
fenetre = tk.Tk()
fenetre.title("Analyseur Reseau")
fenetre.geometry("450x250")

label_titre = tk.Label(
    fenetre,
    text="Analyseur de Trafic Reseau",
    font=("Arial", 14, "bold")
)
label_titre.pack(pady=20)
```

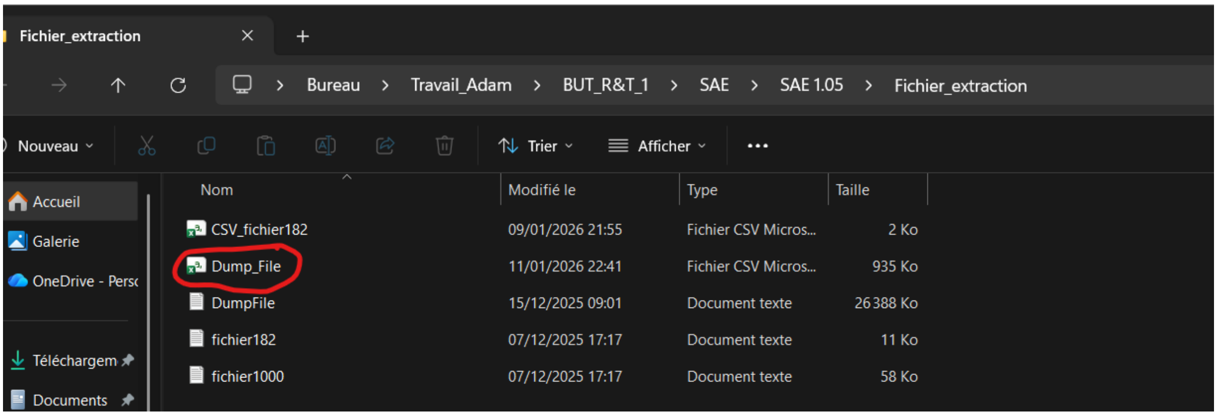
Analyseur Reseau

Analyseur de Trafic Reseau

Ce programme genere 3 images :
- Les anomalies detectees
- L'analyse du trafic (avec pics d'attaques)
- La distribution des protocoles

```
PS C:\Users\ADM69\OneDrive\Bureau\Travail_Adam\BUT_R&T_1\SAE\SAE 1.05> python Extraction_CSV_A_MARKDOWN.py
```

2. Window opens, choose your CSV file from Part 1

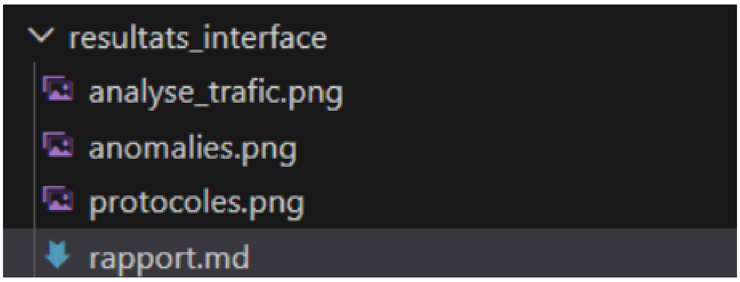


Nom	Modifié le	Type	Taille
CSV_fichier182	09/01/2026 21:55	Fichier CSV Micros...	2 Ko
Dump_File	11/01/2026 22:41	Fichier CSV Micros...	935 Ko
DumpFile	15/12/2025 09:01	Document texte	26388 Ko
fichier182	07/12/2025 17:17	Document texte	11 Ko
fichier1000	07/12/2025 17:17	Document texte	58 Ko

3. It crunches the numbers (takes 1-2 mins for big files)

4. Check the ` resultats_interface/` folder that gets created:

- **anomalies.png** - Shows if something's wrong (red = bad, green = all good)
- **analyse_trafic.png** - 3 graphs showing traffic patterns and top IPs
- **protocoles.png** - Pie chart of protocols (TCP, UDP, ICMP, etc.)
- **rapport.md** - Full text report with all the stats



```
resultats_interface
    analyse_trafic.png
    anomalies.png
    protocoles.png
    rapport.md
```

What to Look For :

If anomalies.png shows red text, you've got issues:

1. **SYN FLOOD** (serious)

   - One IP sending 100+ SYN packets
   - Usually means DDoS attack or infected machine
   - Action: Block that IP asap

2. **PORT SCAN** (medium)

   - One IP trying 50+ different ports
   - Someone's looking for open services
   - Action: Investigate, might be recon

3. **TRAFFIC FLOOD** (serious)

   - One IP = 40%+ of all traffic
   - Could be legit (backup server) or problem (compromised host)
   - Action: Check what that IP is doing

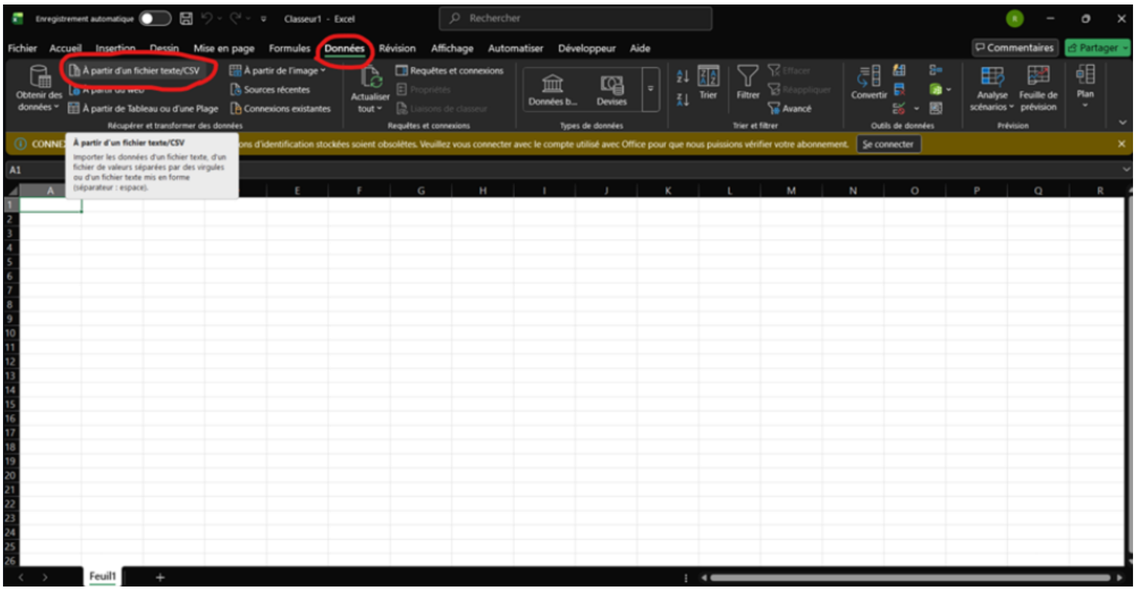
The thresholds (100, 50, 40%) are in the code if you want to adjust them.

This tool was specifically designed to identify the two suspicious activities reported on the India production site: SYN Flood and Port Scan

V. PART 3: EXCEL ANALYSIS (OPTIONAL) :

If you want more details or prefer working in Excel:

1. Open Excel



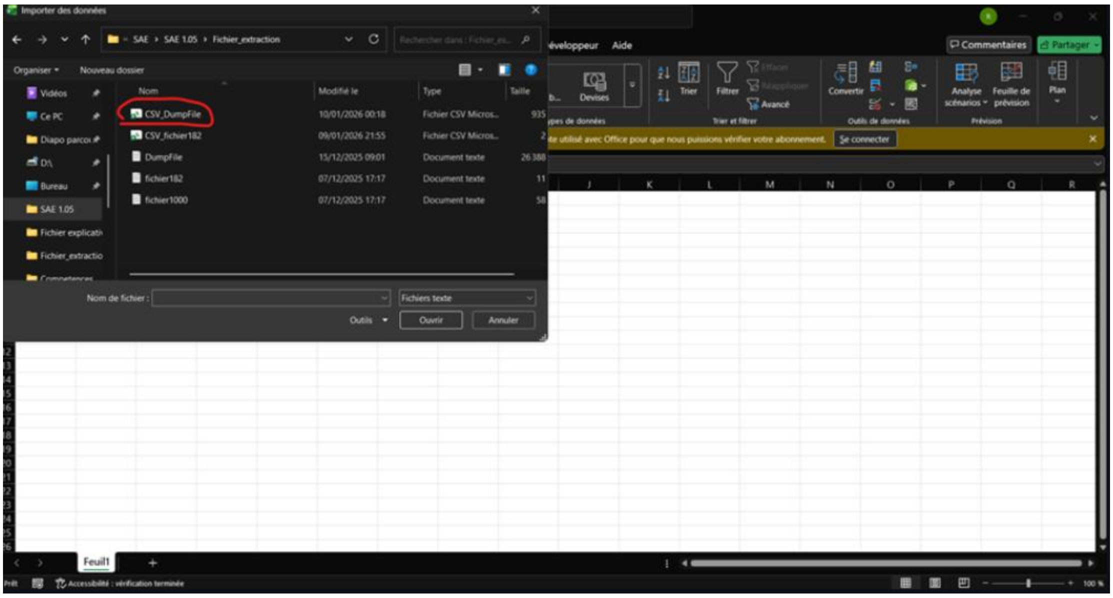
2. Import your CSV:

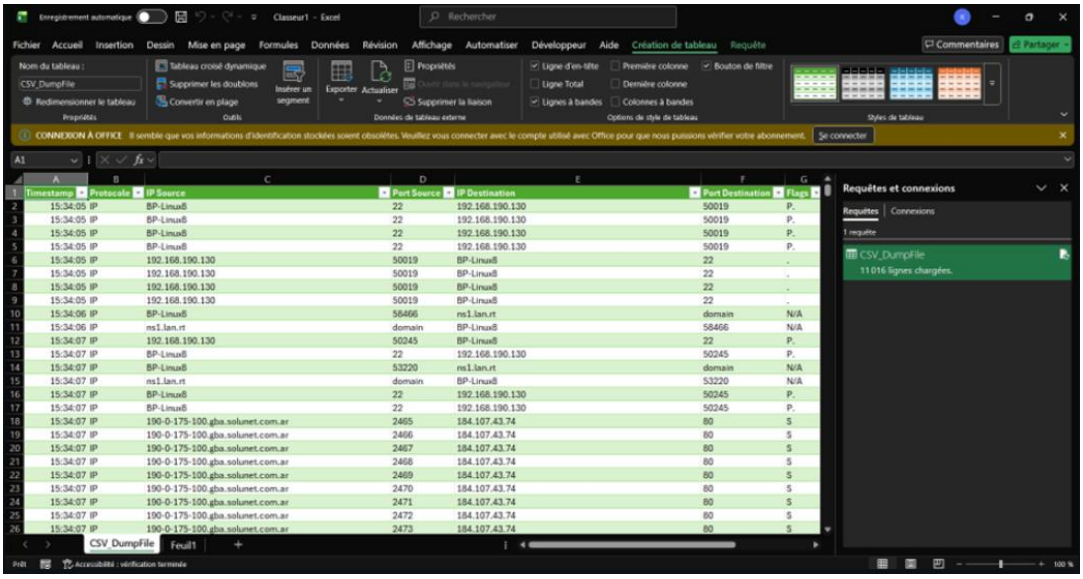
- Data tab → From Text/CSV

- Pick your file

- Make sure delimiter is set to **semicolon** (not comma!)

- Load it





	Timestamp	Protocole	IP Source	Port Source	IP Destination	Port Destination	Flags
2	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
3	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
4	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
5	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
6	15:34:05	IP	192.168.190.130	50019	BP-Linux8	22	.
7	15:34:05	IP	192.168.190.130	50019	BP-Linux8	22	.
8	15:34:05	IP	192.168.190.130	50019	BP-Linux8	22	.
9	15:34:05	IP	192.168.190.130	50019	BP-Linux8	22	.
10	15:34:06	IP	BP-Linux8	58466	ns1.lan.rt	domain	N/A
11	15:34:06	IP	ns1.lan.rt	domain	BP-Linux8	58466	N/A
12	15:34:07	IP	192.168.190.130	50245	BP-Linux8	22	P.
13	15:34:07	IP	BP-Linux8	22	192.168.190.130	50245	P.
14	15:34:07	IP	BP-Linux8	53220	ns1.lan.rt	domain	N/A
15	15:34:07	IP	ns1.lan.rt	domain	BP-Linux8	53220	N/A
16	15:34:07	IP	BP-Linux8	22	192.168.190.130	50245	P.
17	15:34:07	IP	BP-Linux8	22	192.168.190.130	50245	P.
18	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2465	184.107.43.74	80	S
19	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2466	184.107.43.74	80	S
20	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2467	184.107.43.74	80	S
21	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2468	184.107.43.74	80	S
22	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2469	184.107.43.74	80	S
23	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2470	184.107.43.74	80	S
24	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2471	184.107.43.74	80	S
25	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2472	184.107.43.74	80	S
26	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2473	184.107.43.74	80	S

CONNEXION À OFFICE Il semble que vos informations d'identification stockées soient obsolètes. Veuillez vous connecter avec le compte utilisé avec Office pour que nous puissions vérifier votre abonnement.

Requêtes et connexions

CSV_DumpFile
11 016 lignes chargées.

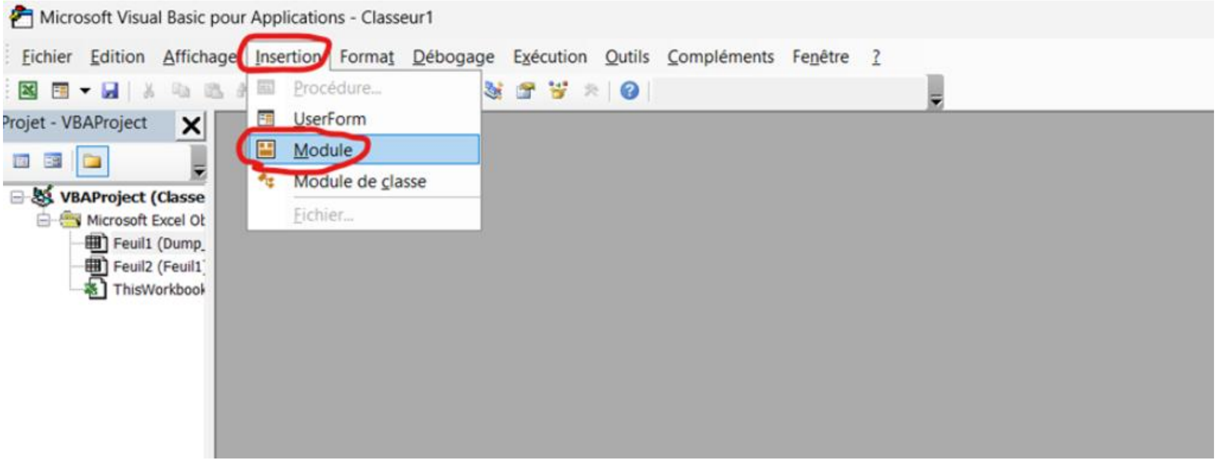
3. Install the macro:

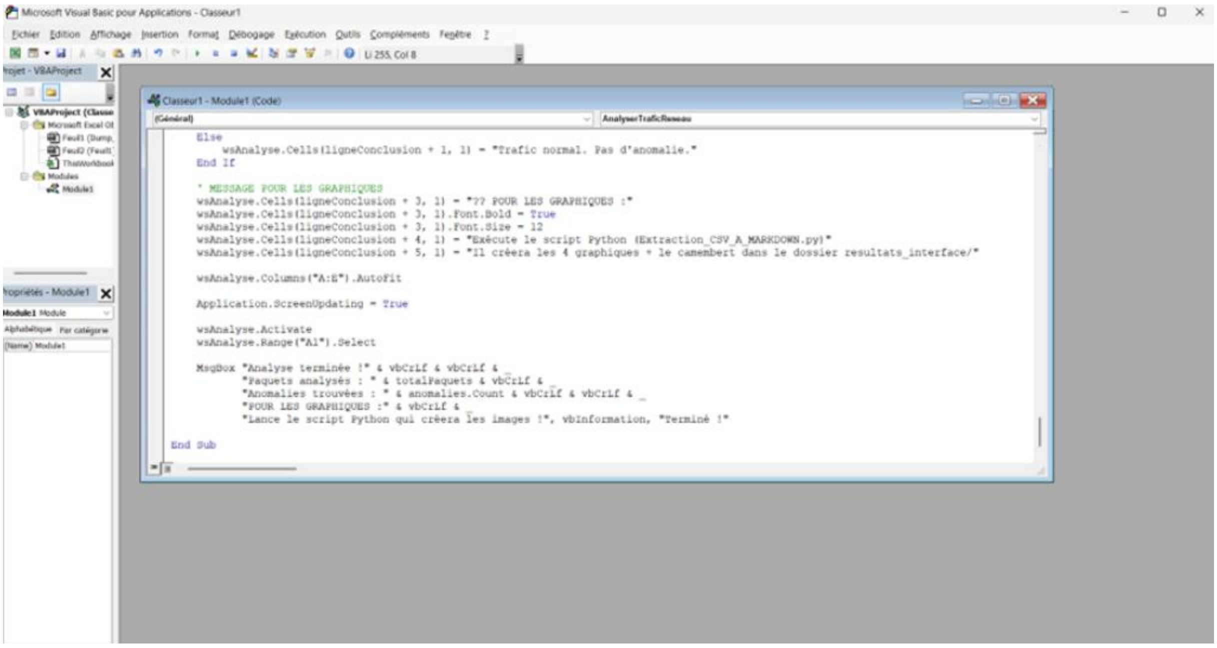
- Alt+F11 to open VBA editor

- Right click → Insert Module

- Copy everything from my github ` vba.txt` and paste it

- Alt+F11 to close

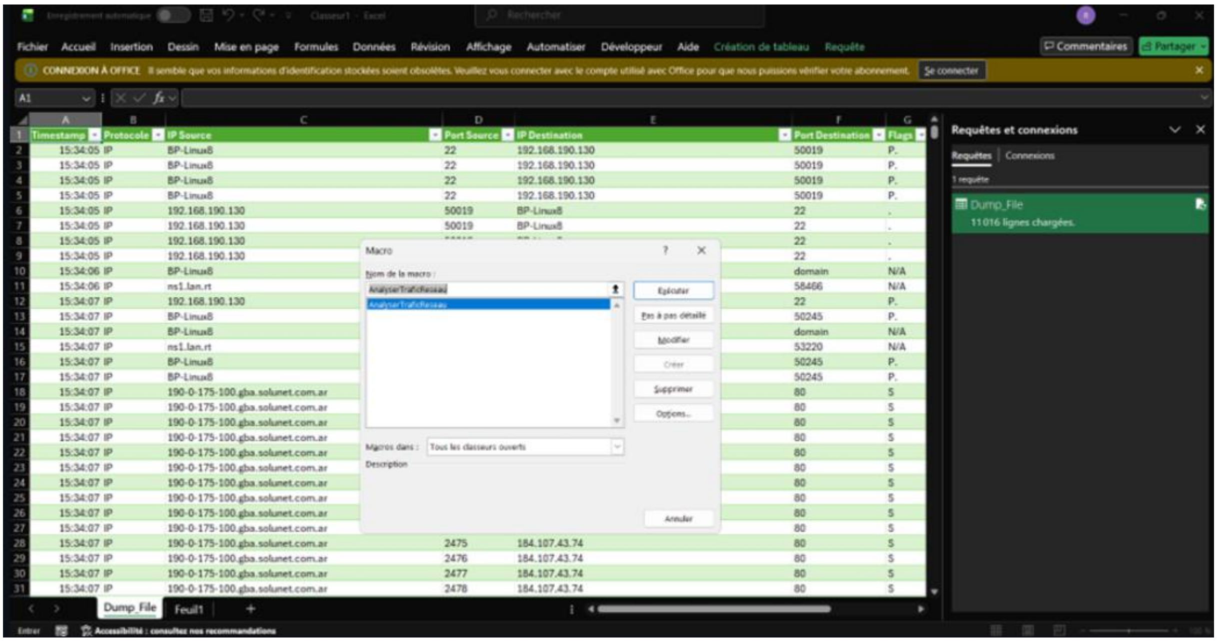




```
    Else
        wsAnalyse.Cells(ligneConclusion + 1, 1) = "Trafic normal. Pas d'anomalie."
    End If

    ' MESSAGE POUR LES GRAPHIQUES
    wsAnalyse.Cells(ligneConclusion + 3, 1) = "?? POUR LES GRAPHIQUES :"
    wsAnalyse.Cells(ligneConclusion + 3, 1).Font.Bold = True
    wsAnalyse.Cells(ligneConclusion + 3, 1).Font.Size = 12
    wsAnalyse.Cells(ligneConclusion + 4, 1) = "Exécute le script Python (Extraction_CSV_A_MARKDOWN.py)"
    wsAnalyse.Cells(ligneConclusion + 5, 1) = "Il créera les 4 graphiques + le camembert dans le dossier resultats_interface/"

    wsAnalyse.Columns("A:E").AutoFit

    Application.ScreenUpdating = True

    wsAnalyse.Activate
    wsAnalyse.Range("A1").Select

    MsgBox "Analyse terminée !" & vbCrLf & vbCrLf & _
           "Paquets analysés : " & totalPaquets & vbCrLf & _
           "Anomalies trouvées : " & anomalies.Count & vbCrLf & vbCrLf & _
           "POUR LES GRAPHIQUES :" & vbCrLf & _
           "Lance le script Python qui créera les images !", vbInformation, "Terminé !"

End Sub
```

4. Run it with the macro:

- Alt+F8



Enregistrement automatique
Classeur1 - Excel
Rechercher
Fichier Accueil Insertion Dessin Mise en page Formules Données Révision Affichage Automatiser Développeur Aide Création de tableau Requête
Commentaires
Partager
A1
Macro
Exécuter
Pas à pas détaillé
Modifier
Créer
Supprimer
Options...
Annuler
Dump_File
Feuil1
Entrer
Accessibilité : consultez nos recommandations

CONNEXION À OFFICE Il semble que vos informations d'identification stockées soient obsolètes. Veuillez vous connecter avec le compte utilisé avec Office pour que nous puissions vérifier votre abonnement. Se connecter

	Timestamp	Protocole	IP Source	Port Source	IP Destination	Port Destination	Flags
2	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
3	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
4	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
5	15:34:05	IP	BP-Linux8	22	192.168.190.130	50019	P.
6	15:34:05	IP	192.168.190.130	50019	BP-Linux8	22	.
7	15:34:05	IP	192.168.190.130	50019	BP-Linux8	22	.
8	15:34:05	IP	192.168.190.130			22	.
9	15:34:05	IP	192.168.190.130			22	.
10	15:34:06	IP	BP-Linux8			domain	N/A
11	15:34:06	IP	ns1.lan.rt			58466	N/A
12	15:34:07	IP	192.168.190.130			22	P.
13	15:34:07	IP	BP-Linux8			50245	P.
14	15:34:07	IP	BP-Linux8			domain	N/A
15	15:34:07	IP	ns1.lan.rt			53220	N/A
16	15:34:07	IP	BP-Linux8			50245	P.
17	15:34:07	IP	BP-Linux8			50245	P.
18	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
19	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
20	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
21	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
22	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
23	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
24	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
25	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
26	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
27	15:34:07	IP	190-0-175-100.gba.solunet.com.ar			80	S
28	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2475	184.107.43.74	80	S
29	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2476	184.107.43.74	80	S
30	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2477	184.107.43.74	80	S
31	15:34:07	IP	190-0-175-100.gba.solunet.com.ar	2478	184.107.43.74	80	S

Macro

Nom de la macro : AnalyserTraficReseau

AnalyserTraficReseau

Macros dans : Tous les classeurs ouverts

Description

Requêtes et connexions

Requêtes | Connexions

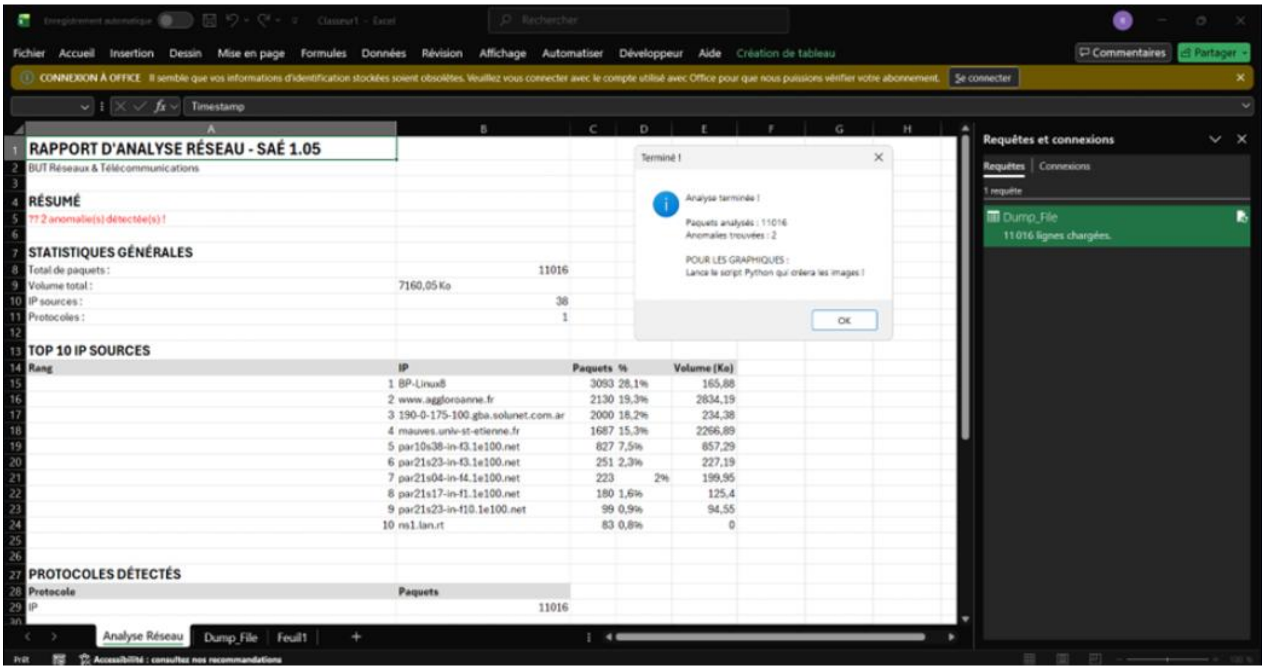
1 requête

Dump_File

11016 lignes chargées.

- Select ` AnalyserTraficReseau`

- Click Run



CONNEXION À OFFICE Il semble que vos informations d'identification stockées soient obsolètes. Veuillez vous connecter avec le compte utilisé avec Office pour que nous puissions vérifier votre abonnement.

RAPPORT D'ANALYSE RÉSEAU - SAÉ 1.05

BUT Réseaux & Télécommunications

RÉSUMÉ

?? 2 anomalie(s) détectée(s) !

STATISTIQUES GÉNÉRALES

Total de paquets :	11016
Volume total :	7160,05 Ko
IP sources :	38
Protocoles :	1

TOP 10 IP SOURCES

Rang	IP	Paquets	%	Volume (Ko)
1	BP-Linux8	3093	28,1%	165,88
2	www.agglioroanne.fr	2130	19,3%	2834,19
3	190-0-175-100.gba.solunet.com.ar	2000	18,2%	234,38
4	mauves.univ-st-etienne.fr	1687	15,3%	2266,89
5	par10s38-in-f3.1e100.net	827	7,5%	857,29
6	par21s23-in-f3.1e100.net	251	2,3%	227,19
7	par21s04-in-f4.1e100.net	223	2%	199,95
8	par21s17-in-f1.1e100.net	180	1,6%	125,4
9	par21s23-in-f10.1e100.net	99	0,9%	94,55
10	ns1.lan.rt	83	0,8%	0

PROTOCOLES DÉTECTÉS

Protocole	Paquets
IP	11016

Terminé !

Analyse terminée !

Paquets analysés : 11016
Anomalies trouvées : 2

POUR LES GRAPHIQUES :
Lance le script Python qui créera les images !

1 requête

Dump_File
11 016 lignes chargées.

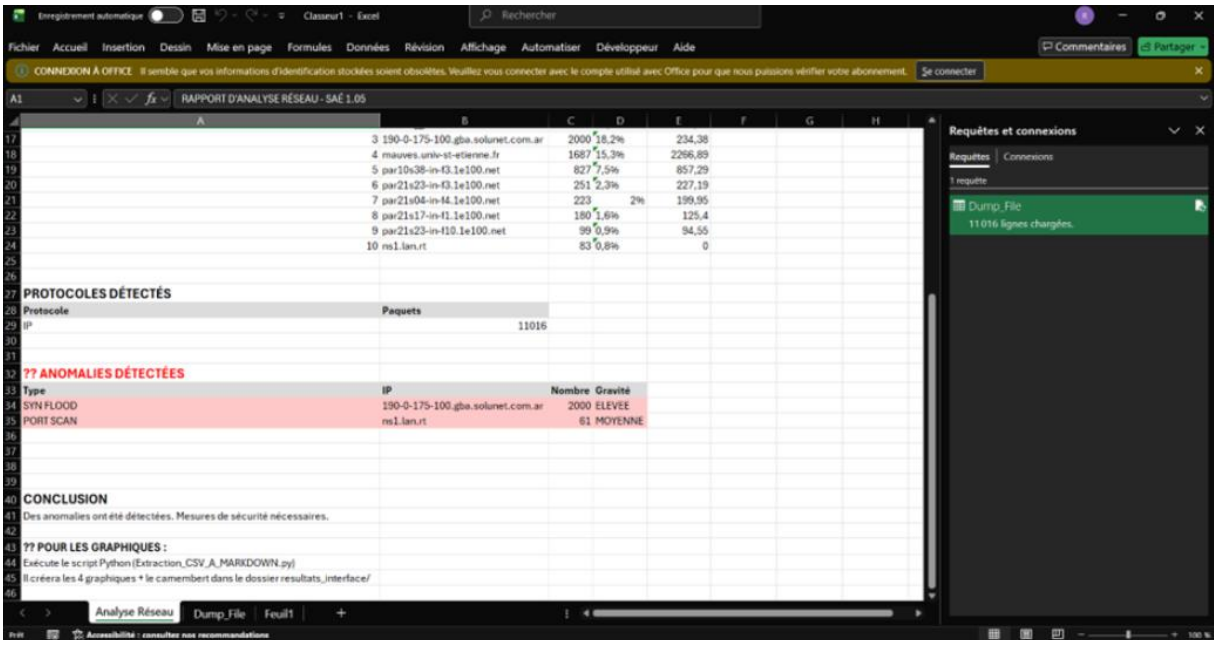
5. New sheet appears: "Analyse Réseau"

   - Top 10 IPs with stats

   - Protocol breakdown

   - Anomalies table (if any)

   - Colored cells for problems (red = issue)



CONNEXION À OFFICE Il semble que vos informations d'identification stockées soient obsolètes. Veuillez vous connecter avec le compte utilisé avec Office pour que nous puissions vérifier votre abonnement.

RAPPORT D'ANALYSE RÉSEAU - SAÉ 1.05

11 016 lignes chargées.

3	190-0-175-100.gba.solunet.com.ar	2000	18,2%	234,38
4	mauves.univ-st-etienne.fr	1687	15,3%	2266,89
5	par10s38-in-f3.1e100.net	827	7,5%	857,29
6	par21s23-in-f3.1e100.net	251	2,3%	227,19
7	par21s04-in-f4.1e100.net	223	2%	199,95
8	par21s17-in-f1.1e100.net	180	1,6%	125,4
9	par21s23-in-f10.1e100.net	99	0,9%	94,55
10	ns1.lan.rt	83	0,8%	0

PROTOCOLES DÉTECTÉS

Protocole	Paquets
IP	11016

?? ANOMALIES DÉTECTÉES

Type	IP	Nombre	Gravité
SYN FLOOD	190-0-175-100.gba.solunet.com.ar	2000	ELEVEE
PORT SCAN	ns1.lan.rt	61	MOYENNE

CONCLUSION

Des anomalies ont été détectées. Mesures de sécurité nécessaires.

?? POUR LES GRAPHIQUES :

Exécute le script Python (Extraction_CSV_A_MARKDOWN.py)

Il créera les 4 graphiques + le camembert dans le dossier resultats_interface/

Pretty useful if your boss wants an Excel report.

VI. UNDERSTANDING THE CSV :

The CSV has 11 columns. Here's what matters:

TIMESTAMP	**WHEN THE PACKET WAS SENT (HH:MM:SS)**
PROTOCOL	**TCP, UDP, ICMP,**
IP SOURCE	**Who sent it**
PORT SOURCE	**From which port**
IP DESTINATION	**Where it's going**
PORT DESTINATION	**To which port (80=web, 22=ssh, 443=https)**
FLAGS	**S=new connection, .=data, F=closing**
LENGTH	**Packet size in bytes**
SEQ	TCP sequence number
ACK	TCP acknowledgment number
WINDOWS	TCP flow control value

These three columns (Seq, Ack, Window) are used for advanced TCP debugging and connection troubleshooting. They are not needed for basic anomaly detection (SYN floods, port scans, traffic floods), which only require IP addresses, ports, flags, and packet length.

VII. COMMON PORTS (QUICK REFERENCE) :

When you see these ports in the CSV :

22	SSH	
80	HTTP	
443	HTTPS	

VIII. TROUBLESHOOTING :

- **Problem: "ModuleNotFoundError: matplotlib"**

Fix: ` pip install matplotlib ` (you probably forgot this)

- **Problem: CSV shows everything in column A**

Fix: In Excel, select column A → Data → Text to Columns → Delimited → Check "Semicolon"

- **Problem: Python script won't open**

Fix: Make sure Python is in your PATH. Reinstall Python and CHECK that box during setup.

- **Problem: Takes forever to run**

Fix: Your file is probably huge. Try analyzing just 1 hour of traffic first to test.

- **Problem: VBA macro gives error**

Fix: Make sure the CSV is actually imported (should have 11 columns). If it's all in one column, see solution above.

IX. BEST PRACTICES AND RECOMMENDATIONS :

Good practices :

- Capture traffic during normal hours (get baseline)

- Always keep the original .txt file (in case you need to reprocess)

Things to avoid :

- Don't capture passwords/sensitive data (use filters)

- Don't panic if you see unknown IPs (check first)

- Don't edit the CSV manually (breaks the analysis)

For deployment :

- Test on small capture first

- Adjust thresholds if you get too many false positives

- Document any modifications you make

X. WHAT TO DO IF YOU FIND ISSUES :

Serious (red) anomalies :

1. Note the IP address

2. Check what that IP is (user PC, server, external?)

3. Email IT/security team immediately with:

   - The IP address

   - Type of anomaly (SYN flood, port scan, etc.)

   - The charts (attach anomalies.png)

   - The timestamp range

Medium (orange) anomalies :

1. Note the IP

2. Check if it's a known scanner (security team doing their job?)

3. Monitor it for 24h

4. If it continues, escalate

No anomalies (green) :

- Great ! But still review the traffic patterns

- Sometimes issues are subtle (not caught by thresholds)

- Check the Top 10 IPs manually

XI. FILE STRUCTURE :

```
project_folder/
 ├── Extraction_TXT_A_CSV.py
 ├── Extraction_CSV_A_MARKDOWN.py
 ├── vba.txt
 ├── DumpFile.txt (your input)
 ├── DumpFile.csv (converted)
 └── resultats_interface/
     ├── anomalies.png
     ├── analyse_trafic.png
     ├── protocoles.png
     └── rapport.md
```

Keep this organized. You might need to go back to old captures later.

XII. MODIFYING DETECTION THRESHOLDS :

If you want to adjust when anomalies trigger (too sensitive/not sensitive enough):

1. Open `Extraction_CSV_A_MARKDOWN.py` in any text editor

2. Find the function `detecter_problemes()` (around line 115)

3. Change these values:

```
if nb_syn > 100:      # SYN flood threshold (default: 100)
if nb_ports > 50:      # Port scan threshold (default: 50)
if pourcentage > 40:   # Traffic flood threshold (default: 40%)
```

Lower values = more sensitive (catches more but more false positives)

Higher values = less sensitive (only catches serious issues)

XIII. DEPLOYMENT NOTES (FOR INDIA TEAM) :

When you deploy this in India:

1. Install Python 3 + matplotlib on the analysis machine

2. Test with a small capture first

3. The tool expects tcpdump format .txt

4. Results go to `resultats_interface/` folder (created automatically)

5. If you get false positives, adjust thresholds (see above)

Contact :

For technical support : adam.abiderrahmane@etu.univ-st-etienne.fr

My github : https://github.com/AdamAbiderrahmane/SAE1.05

I'll help you get it working.

XIV. FINAL NOTES :

This tool isn't perfect. It's meant to give you a starting point for investigating network issues. Always:

- Cross-reference with your IDS/firewall logs

- Verify suspicious IPs before blocking

- Document what you find

- Keep captures if needed

The thresholds work for our setup but might need adjustment for yours. Network profiles differ.

Good luck! Hope this helps solve the saturation issue.

v1.0 - Jan 2026

Created for SAE 1.05 project - BUT R&T

**Feel free to modify/improve this.*