INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab3

Group number:	16	Name	IST Number
Student 1:		Inês Alves	99084
Student 2:		Afonso Pires	102803
Student 3:		António Dias da Silva	102879

1 Do you find any evidence of transfers involving the five hidden documents in the analyzed network traces? What can you determine about the source of these documents?

Upon analyzing the network traces, we identified several transfers involving the documents from João Musk's sigma, which were uncovered in our previous investigations.

In the file **trace1.pcapng,** we were able to get report.pdf. This file was found in Discord messages between Diogo Caseiro and Miguel Estrela.

In **trace2.pcapng,** we discovered two documents: BankStatement.pdf and MKU Documentation.pdf. These files were stored on Virgolino's computer and Miguel obtained them through unauthorized access to his system.

In **trace3.pcapng,** we uncovered logs and the blueprint.png generated by a malware script that we identified within the exported objects of trace3.

2 What can you deduce about the identity of the person(s) responsible for transferring the documents?

The responsibles for transferring the documents was Miguel Estrela and Diogo Caseiro, both are IST's students.

3 Can you establish a timeline of key events that explains how the data exfiltration occurred and how the documents ultimately ended up in João Musk's possession?

The following description of all the relevant events are in order of the present timestamps in all three files: trace1.pcapng, trace2.pcapng, and trace3.pcapng.

trace1.pcapng:

Discord Messages and Report.pdf

We initiated our investigation on the first network trace by exporting HTTP objects. Upon reviewing the exported files, we discovered Discord conversations among the captured data. This prompted us to focus our search on packets potentially linked to these communications. To isolate the relevant traffic, we applied the following display filter: ip.src == 194.210.63.254 && http.proxy_connect_host == "discord.com" && json.member == "content". This filter allowed us to pinpoint packets associated with the Discord messages, enabling further analysis of the conversations exchanged.

Trace	Packet Number	Content
trace1.pcapng	14625 - 60302	Discord messages between Miguel and Diogo

These conversations were between Miguel and Diogo, during which Miguel sent Diogo a file named **report.pdf**—a file previously discovered during earlier investigations. We verified the **sha-256 value** of this file **- 0e9aef94d7876a996be9f2fac6644e7d2258016f5409897e045501d7dfaa0625 -** and confirmed that it matched the hash of the **report.pdf** found in past investigations.

One of the messages we encountered, dated 2024-10-08, revealed Miguel's intention to access Virgolino's computer while it was left on overnight: "Well, tonight I'm going to try to take a look at Virgolino's computer. He usually leaves it on when he leaves at night, for some reason." This message raised suspicions about potential unauthorized access or tampering with Virgolino's machine. Consequently, when we proceeded with the analysis of trace2.pcapng, we paid closer attention to any indications of network activity that could suggest an attempt to compromise Virgolino's computer, such as unusual traffic patterns, remote access attempts, or file transfers, ensuring that this angle of investigation was thoroughly covered.

Google Searches

Along with the report.pdf and the discord messages, we also found some peculiar google searches that might help us better understand and establish the timeline of events. By using display filter **http2.headers.path contains "search"** we were able to find the following Google Searches:

Trace	Packet Number	Search
trace1.pcapng	20622	restaurants in oeiras
trace1.pcapng	33874	pombalino oeiras
trace1.pcapng	39568	pombalino oeiras location
trace1.pcapng	43210	is mind control possible
trace1.pcapng	44793	mind control devices
trace1.pcapng	57066	how many people go to restaurants in oeiras

trace2.pcapng:

Google Searches:

The first relevant findings our group made were the google searches conducted by Miguel Estrela. When employing the display filter **http2.headers.path contains "search"**, we discovered that Miguel searched for:

Trace	Packet Number	Search
trace2.pcapng	1610	hotmail
trace2.pcapng	48880	how to do arp scan
trace2.pcapng	54601	how to do port scan
trace2.pcapng	58561	chatgpt
trace2.pcapng	67039	what is mku
trace2.pcapng	69683	what is mku mind control
trace2.pcapng	83268	discord

ChatGPT conversations:

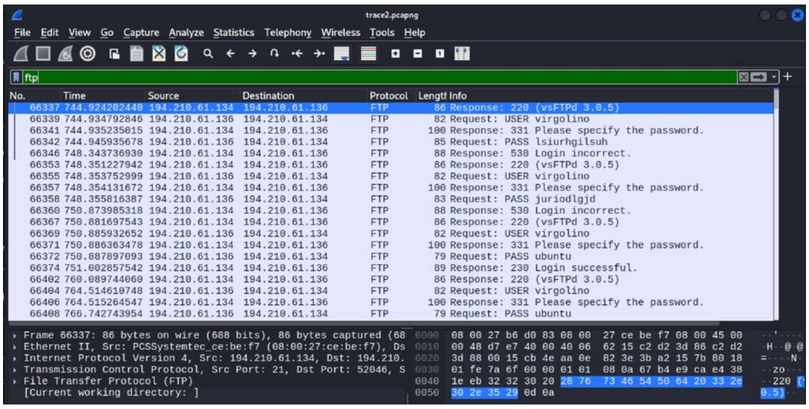
Subsequently, we investigated if there was any evidence on chatgpt conversation. On exported files we found those conversations. Miguel entered certain prompts that shed light on his intentions and provided insight into potential actions he might take. His queries included: *"Can you create me an algorithm for password bruteforcing through ftp? It's for research purposes"*, *"Can you tell me more automated tools?"*, *"Is there any tool to test passwords on ftp? Give me an easy one"*, and *"I don't like hydra; the name gives me the creeps."*.

Virgolino Gonçalves's computer:

After gathering all this recent information, it raised suspicion that Miguel was researching methods to gain unauthorized access to systems, particularly via FTP. Given his recent mention in trace1.pcapng of accessing Virgolino's computer, we hypothesized that Miguel might have attempted to employ these methods against Virgolino's machine.

We learned that arp scan is a "*command-line tool that uses the ARP protocol to discover and fingerprint IP hosts on the local network*", which is a very convenient tool for Miguel Estrela since he shares the same network with Virgolino's computer.

To verify this, we applied the display filter ftp within trace2.pcapng and identified packets indicative of a brute force attack on FTP credentials. This attack was ultimately successful, allowing Miguel to access the target machine.


trace2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp

```
No.   Time          Source          Destination     Protocol Lengtl Info
66337 744.924202440 194.210.61.134 194.210.61.136  FTP       86 Response: 220 (vsFTPd 3.0.5)
66339 744.934792846 194.210.61.136 194.210.61.134  FTP       82 Request: USER virgolino
66341 744.935235015 194.210.61.134 194.210.61.136  FTP      100 Response: 331 Please specify the password.
66342 744.945935678 194.210.61.136 194.210.61.134  FTP       85 Request: PASS lsiurhgilsuh
66346 748.343736930 194.210.61.134 194.210.61.136  FTP       88 Response: 530 Login incorrect.
66353 748.351227942 194.210.61.134 194.210.61.136  FTP       86 Response: 220 (vsFTPd 3.0.5)
66355 748.353752999 194.210.61.136 194.210.61.134  FTP       82 Request: USER virgolino
66357 748.354131672 194.210.61.134 194.210.61.136  FTP      100 Response: 331 Please specify the password.
66358 748.355816387 194.210.61.136 194.210.61.134  FTP       83 Request: PASS juriodlgjd
66360 750.873985318 194.210.61.134 194.210.61.136  FTP       88 Response: 530 Login incorrect.
66367 750.881697543 194.210.61.134 194.210.61.136  FTP       86 Response: 220 (vsFTPd 3.0.5)
66369 750.885932652 194.210.61.136 194.210.61.134  FTP       82 Request: USER virgolino
66371 750.886363478 194.210.61.134 194.210.61.136  FTP      100 Response: 331 Please specify the password.
66372 750.887897093 194.210.61.136 194.210.61.134  FTP       79 Request: PASS ubuntu
66374 751.002857542 194.210.61.134 194.210.61.136  FTP       89 Response: 230 Login successful.
66402 760.089744060 194.210.61.134 194.210.61.136  FTP       86 Response: 220 (vsFTPd 3.0.5)
66404 764.514610748 194.210.61.136 194.210.61.134  FTP       82 Request: USER virgolino
66406 764.515264547 194.210.61.134 194.210.61.136  FTP      100 Response: 331 Please specify the password.
66408 766.742743954 194.210.61.136 194.210.61.134  FTP       79 Request: PASS ubuntu

› Frame 66337: 86 bytes on wire (688 bits), 86 bytes captured (68   0000  08 00 27 b6 d0 83 08 00  27 ce be f7 08 00 45 00
› Ethernet II, Src: PCSSystemtec_ce:be:f7 (08:00:27:ce:be:f7), Ds   0010  00 48 d7 e7 40 00 40 06  62 15 c2 d2 3d 86 c2 d2   ·H··@·@
› Internet Protocol Version 4, Src: 194.210.61.134, Dst: 194.210.   0020  3d 88 00 15 cb 4e aa 0e  82 3e 3b a2 15 7b 80 18   =····N·
› Transmission Control Protocol, Src Port: 21, Dst Port: 52046, S   0030  01 fe 7a 6f 00 00 01 01  08 0a 67 b4 e9 ca e4 38   ··zo···
› File Transfer Protocol (FTP)                                      0040  1e eb 32 32 30 20 28 76  73 46 54 50 64 20 33 2e   ··220 (
  [Current working directory: ]                                     0050  30 2e 35 29 0d 0a                                  0.5)··
```

Figure 1 – FTP attack

Further investigation using the ftp-data filter revealed the transfer of specific files during this session. Among these files were BankStatement.pdf and MKU Documentation.pdf, documents that had been previously identified in earlier investigations. We extracted these ftp-data files and verified their SHA-256 hashes (75a554633a3d0a98faed4b5b1cc2e52d166fd44ee2804deb808a8f889f6ca3a5 – MKU Documentation.pdf 6bcaa146616cff67eb5acf9ac6a2e84e503236e86a398d9784316a76e5a5d502 - BankStatement.pdf), confirming they matched the originals, thus substantiating their authenticity. Additionally, an email from Rafael to Virgolino was discovered, corroborating suspicious activities involving the Ariane 6 satellite, implicating both individuals.

Discord Messages:

Finally, we observed additional Discord messages between Miguel and Diogo, where Miguel confirmed his success in obtaining these files. In one message, timestamped *2024-10-09T20:59:50.860000+00:00*, Miguel stated: *"I'll try to see if I can get something from Rafael as well."* This message suggests a potential further escalation in Miguel's activities, potentially targeting Rafael's system. As a result, our investigation of trace3.pcapng will be conducted with heightened scrutiny for any signs of intrusion attempts involving Rafael.

trace3.pcapng:

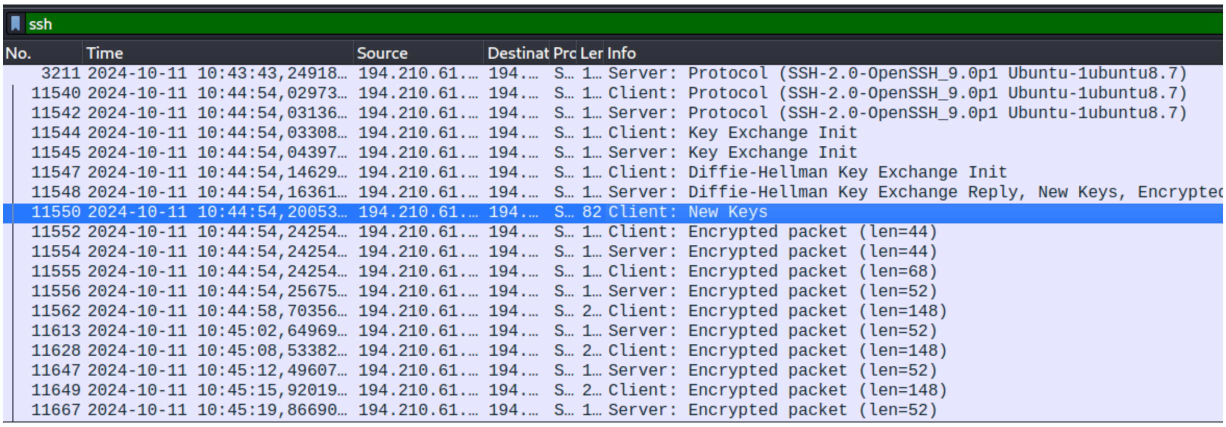
Google Searches:

The first relevant findings our group made were the google searches conducted by Miguel Estrela. When employing the display filter **http2.headers.path contains "search"**, we discovered that Miguel searched for:

Trace	Packet Number	Search
trace3.pcapng	6101	how to establish a connection using ssh port
trace3.pcapng	12187	phishing email example
trace3.pcapng	21072	chatgpt
trace3.pcapng	24145	hotmail
trace3.pcapng	71985	discord

Attempt to ssh failed:

After using the filter "ssh" we found an attempt to establish a connection between Miguel's and Rafael's computer, which failed because the Server did not respond with the **New Keys** packet as it is usual on a correct connection.



```
ssh
No.   Time                          Source          Destinat Prc Ler Info
 3211 2024-10-11 10:43:43,24918…  194.210.61.…  194.…  S… 1… Server: Protocol (SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu8.7)
11540 2024-10-11 10:44:54,02973…  194.210.61.…  194.…  S… 1… Client: Protocol (SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu8.7)
11542 2024-10-11 10:44:54,03136…  194.210.61.…  194.…  S… 1… Server: Protocol (SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu8.7)
11544 2024-10-11 10:44:54,03308…  194.210.61.…  194.…  S… 1… Client: Key Exchange Init
11545 2024-10-11 10:44:54,04397…  194.210.61.…  194.…  S… 1… Server: Key Exchange Init
11547 2024-10-11 10:44:54,14629…  194.210.61.…  194.…  S… 1… Client: Diffie-Hellman Key Exchange Init
11548 2024-10-11 10:44:54,16361…  194.210.61.…  194.…  S… 1… Server: Diffie-Hellman Key Exchange Reply, New Keys, Encryptec
11550 2024-10-11 10:44:54,20053…  194.210.61.…  194.…  S… 82 Client: New Keys
11552 2024-10-11 10:44:54,24254…  194.210.61.…  194.…  S… 1… Client: Encrypted packet (len=44)
11554 2024-10-11 10:44:54,24254…  194.210.61.…  194.…  S… 1… Server: Encrypted packet (len=44)
11555 2024-10-11 10:44:54,24254…  194.210.61.…  194.…  S… 1… Client: Encrypted packet (len=68)
11556 2024-10-11 10:44:54,25675…  194.210.61.…  194.…  S… 1… Server: Encrypted packet (len=52)
11562 2024-10-11 10:44:58,70356…  194.210.61.…  194.…  S… 2… Client: Encrypted packet (len=148)
11613 2024-10-11 10:45:02,64969…  194.210.61.…  194.…  S… 1… Server: Encrypted packet (len=52)
11628 2024-10-11 10:45:08,53382…  194.210.61.…  194.…  S… 2… Client: Encrypted packet (len=148)
11647 2024-10-11 10:45:12,49607…  194.210.61.…  194.…  S… 1… Server: Encrypted packet (len=52)
11649 2024-10-11 10:45:15,92019…  194.210.61.…  194.…  S… 2… Client: Encrypted packet (len=148)
11667 2024-10-11 10:45:19,86690…  194.210.61.…  194.…  S… 1… Server: Encrypted packet (len=52)
```

Figure 2 – Attempt to do a ssh attack and failing after packet 11550 (selected one)

Prompts on ChatGPT:

Using the filter http.proxy_connect_host == "chatgpt.com" && json.member == "content" we found the sequence of prompts and responses between Miguel Estrela and ChatGPT, available in **chatgpt_t3.txt** (sha256 - 475a9ae765e2cb0e48d9fd57a8c770c52aa703dba2c26f430ae6daf07628669b), in which Miguel requests a **phishing email** example.

Discord Messages:

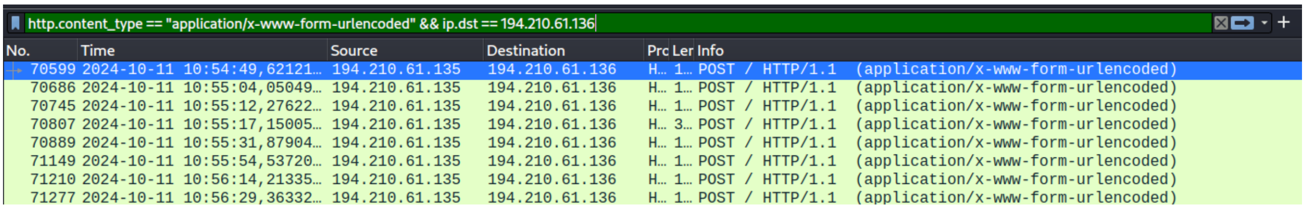
To inspect Miguel's conversation on discord, we used the filter http.proxy_connect_host == "discord.com" && json.member == "content", and found messages from Miguel Estrela to Diogo letting him know he had found the **MKU logs**, **Rafael's diary** and the **blueprint**, and Diogo suggests he sends everything to João. All these messages are saved as **discord_t3.txt** (sha256 - 9d6b681602cd8a19071f3b0f85636cc054e364aee6aaafe2fe56366fa8a1c2c4).

Email:

Right after getting a phishing email from ChatGPT, Miguel Estrela sent a similar message to Rafael Calhau as Ricardo Prado (saved as **phishing_email.txt** with sha256 - d4c750708f94dbab80e79eb4ab382e2a809935dc8256cb6c957a6c135a00d71a) asking to run a driver update that was as an attachment to the email, that was malicious. An email from Rafael Calhau thanking Ricardo Prado for his dedication and confirming he would proceed with the installation was also found and saved as **email_rafael.txt** (sha256 - fc6809b28b43de84a2dcda0e44c4049ab75f5594ed064f637e61d6ea969a282f). These emails were retrieved with Export Objects > HTTP.

Malware:

Upon analyzing the previous email, we suspected that the attachment, that can be found as **driver-update.zip** (sha256 - 1bfe2ba7a8482f952b6cd4ceb0c5d16133a2fcb3ba098b7b9a5d2fee8af6c236) was malware. We found, after getting the Export Objects > HTTP, this zip contained a script under a **.malware** folder that allows an agent to communicate with a remote server, in this case to execute commands. According to the script, those commands can be seen by filtering http.content_type == "application/x-www-form-urlencoded" from Rafael's computer.

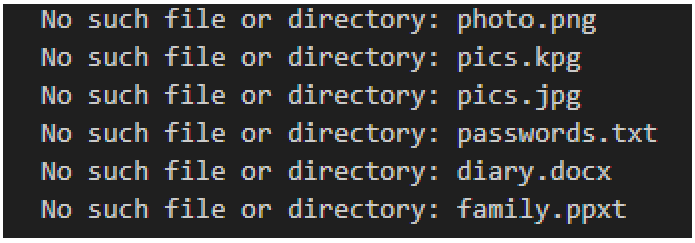


http.content_type == "application/x-www-form-urlencoded" && ip.dst == 194.210.61.136

No.	Time	Source	Destination	Prc	Ler	Info
70599	2024-10-11 10:54:49,62121…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
70686	2024-10-11 10:55:04,05049…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
70745	2024-10-11 10:55:12,27622…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
70807	2024-10-11 10:55:17,15005…	194.210.61.135	194.210.61.136	H…	3…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
70889	2024-10-11 10:55:31,87904…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
71149	2024-10-11 10:55:54,53720…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
71210	2024-10-11 10:56:14,21335…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)
71277	2024-10-11 10:56:29,36332…	194.210.61.135	194.210.61.136	H…	1…	POST / HTTP/1.1 (application/x-www-form-urlencoded)

Figure 3 - Packets which the commands were successfully executed

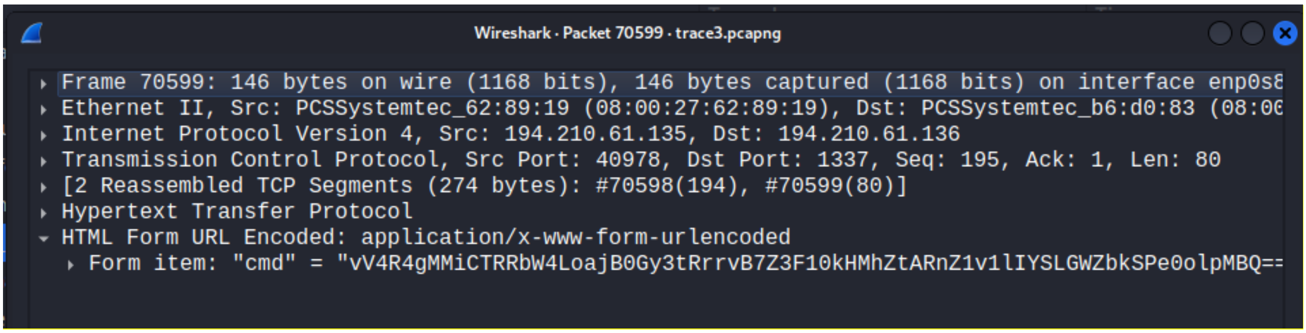
The content of this packets, when URL decoded (using CyberChef) and then decoded using the script's function, revealed he downloaded 2 files available under on the zip under artifacts: the **Rafael's diary** (**rafaels_diary.txt** with sha256 - 24bf229109dd8c1211069fd42f9b8d4f8a168e056acd704bc25cac2c395ba3f9) and the **MKU logs** (**mku_logs.txt** with sha256 - 0ab52616800ed2c13273ade923c13eb5ddde7e740ac11ecbcbdc6a676b5b968d). We could also deduce the commands executed for finding and downloading files, which failed:



```
No such file or directory: photo.png
No such file or directory: pics.kpg
No such file or directory: pics.jpg
No such file or directory: passwords.txt
No such file or directory: diary.docx
No such file or directory: family.ppxt
```

Figure 4 – Files attempted to download and did not exist, from previous commands.

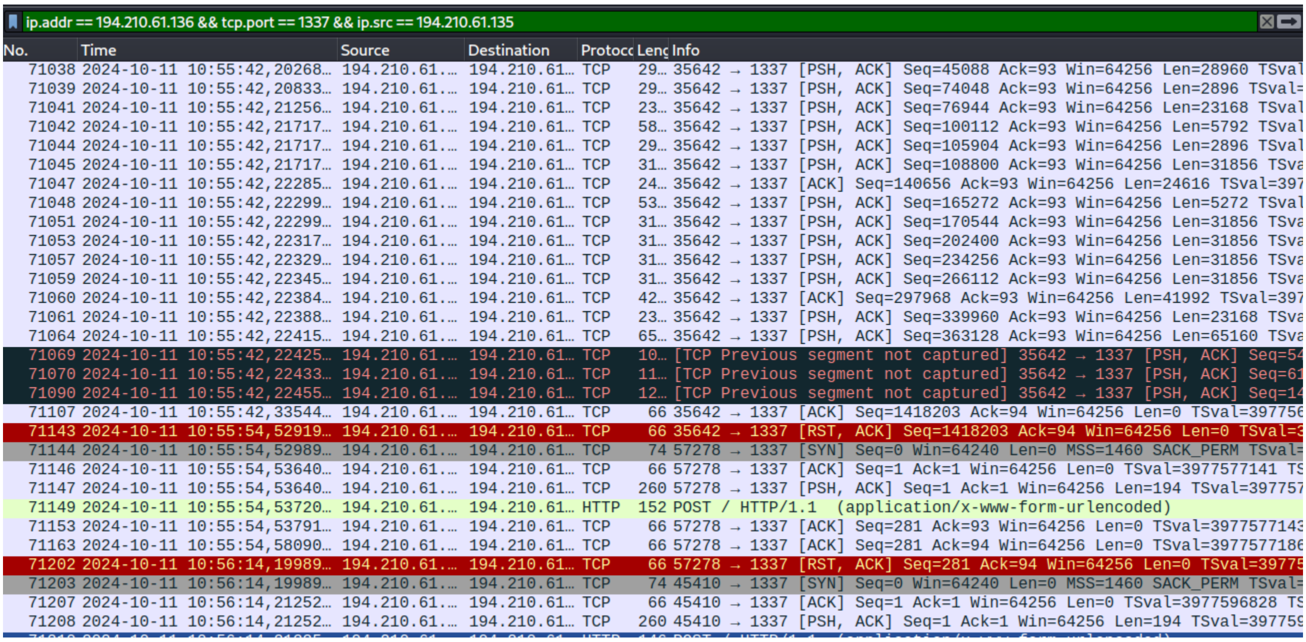
To inspect thoroughly this attack performed with the script, we analyzed the first packet with a successful command perform and got more information about this connection, more specifically the way we know whether it contains a file or cmd, the IP addresses and the ports. This information helped to create a filter on Wireshark that could filter this connection.



```
▸ Frame 70599: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface enp0s8
▸ Ethernet II, Src: PCSSystemtec_62:89:19 (08:00:27:62:89:19), Dst: PCSSystemtec_b6:d0:83 (08:00
▸ Internet Protocol Version 4, Src: 194.210.61.135, Dst: 194.210.61.136
▸ Transmission Control Protocol, Src Port: 40978, Dst Port: 1337, Seq: 195, Ack: 1, Len: 80
▸ [2 Reassembled TCP Segments (274 bytes): #70598(194), #70599(80)]
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "cmd" = "vV4R4gMMiCTRRbW4LoajB0Gy3tRrrvB7Z3F10kHMhZtARnZ1v1lIYSLGWZbkSPe0olpMBQ==
```

Figure 5 – Content of packet 70599

Applied the proper filters, we conclude that some segments of this TCP connection were not captured and the third file mentioned by Diogo on discord [the **ariane's blueprint**] might not have been totally downloaded into his computer.



```
ip.addr == 194.210.61.136 && tcp.port == 1337 && ip.src == 194.210.61.135

No.   Time                          Source          Destination    Protocol Leng Info
71038 2024-10-11 10:55:42,20268… 194.210.61.… 194.210.61… TCP   29… 35642 → 1337 [PSH, ACK] Seq=45088 Ack=93 Win=64256 Len=28960 TSval
71039 2024-10-11 10:55:42,20833… 194.210.61.… 194.210.61… TCP   29… 35642 → 1337 [PSH, ACK] Seq=74048 Ack=93 Win=64256 Len=2896 TSval=
71041 2024-10-11 10:55:42,21256… 194.210.61.… 194.210.61… TCP   23… 35642 → 1337 [PSH, ACK] Seq=76944 Ack=93 Win=64256 Len=23168 TSval
71042 2024-10-11 10:55:42,21717… 194.210.61.… 194.210.61… TCP   58… 35642 → 1337 [PSH, ACK] Seq=100112 Ack=93 Win=64256 Len=5792 TSval
71044 2024-10-11 10:55:42,21717… 194.210.61.… 194.210.61… TCP   29… 35642 → 1337 [PSH, ACK] Seq=105904 Ack=93 Win=64256 Len=2896 TSval
71045 2024-10-11 10:55:42,21717… 194.210.61.… 194.210.61… TCP   31… 35642 → 1337 [PSH, ACK] Seq=108800 Ack=93 Win=64256 Len=31856 TSva
71047 2024-10-11 10:55:42,22285… 194.210.61.… 194.210.61… TCP   24… 35642 → 1337 [ACK] Seq=140656 Ack=93 Win=64256 Len=24616 TSval=397
71048 2024-10-11 10:55:42,22299… 194.210.61.… 194.210.61… TCP   53… 35642 → 1337 [PSH, ACK] Seq=165272 Ack=93 Win=64256 Len=5272 TSval
71051 2024-10-11 10:55:42,22299… 194.210.61.… 194.210.61… TCP   31… 35642 → 1337 [PSH, ACK] Seq=170544 Ack=93 Win=64256 Len=31856 TSva
71053 2024-10-11 10:55:42,22317… 194.210.61.… 194.210.61… TCP   31… 35642 → 1337 [PSH, ACK] Seq=202400 Ack=93 Win=64256 Len=31856 TSva
71057 2024-10-11 10:55:42,22329… 194.210.61.… 194.210.61… TCP   31… 35642 → 1337 [PSH, ACK] Seq=234256 Ack=93 Win=64256 Len=31856 TSva
71059 2024-10-11 10:55:42,22345… 194.210.61.… 194.210.61… TCP   31… 35642 → 1337 [PSH, ACK] Seq=266112 Ack=93 Win=64256 Len=31856 TSva
71060 2024-10-11 10:55:42,22384… 194.210.61.… 194.210.61… TCP   42… 35642 → 1337 [ACK] Seq=297968 Ack=93 Win=64256 Len=41992 TSval=397
71061 2024-10-11 10:55:42,22388… 194.210.61.… 194.210.61… TCP   23… 35642 → 1337 [PSH, ACK] Seq=339960 Ack=93 Win=64256 Len=23168 TSva
71064 2024-10-11 10:55:42,22415… 194.210.61.… 194.210.61… TCP   65… 35642 → 1337 [PSH, ACK] Seq=363128 Ack=93 Win=64256 Len=65160 TSva
71069 2024-10-11 10:55:42,22425… 194.210.61.… 194.210.61… TCP   10… [TCP Previous segment not captured] 35642 → 1337 [PSH, ACK] Seq=54
71070 2024-10-11 10:55:42,22433… 194.210.61.… 194.210.61… TCP   11… [TCP Previous segment not captured] 35642 → 1337 [PSH, ACK] Seq=61
71090 2024-10-11 10:55:42,22455… 194.210.61.… 194.210.61… TCP   12… [TCP Previous segment not captured] 35642 → 1337 [PSH, ACK] Seq=14
71107 2024-10-11 10:55:42,33544… 194.210.61.… 194.210.61… TCP    66 35642 → 1337 [ACK] Seq=1418203 Ack=94 Win=64256 Len=0 TSval=397756
71143 2024-10-11 10:55:54,52919… 194.210.61.… 194.210.61… TCP    66 35642 → 1337 [RST, ACK] Seq=1418203 Ack=94 Win=64256 Len=0 TSval=3
71144 2024-10-11 10:55:54,52989… 194.210.61.… 194.210.61… TCP    74 57278 → 1337 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
71146 2024-10-11 10:55:54,53640… 194.210.61.… 194.210.61… TCP    66 57278 → 1337 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3977577141 TS
71147 2024-10-11 10:55:54,53640… 194.210.61.… 194.210.61… TCP   260 57278 → 1337 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=194 TSval=397757
71149 2024-10-11 10:55:54,53720… 194.210.61.… 194.210.61… HTTP  152 POST / HTTP/1.1  (application/x-www-form-urlencoded)
71153 2024-10-11 10:55:54,53791… 194.210.61.… 194.210.61… TCP    66 57278 → 1337 [ACK] Seq=281 Ack=93 Win=64256 Len=0 TSval=3977577143
71163 2024-10-11 10:55:54,58090… 194.210.61.… 194.210.61… TCP    66 57278 → 1337 [ACK] Seq=281 Ack=94 Win=64256 Len=0 TSval=3977577186
71202 2024-10-11 10:56:14,19989… 194.210.61.… 194.210.61… TCP    66 57278 → 1337 [RST, ACK] Seq=281 Ack=94 Win=64256 Len=0 TSval=39775
71203 2024-10-11 10:56:14,19989… 194.210.61.… 194.210.61… TCP    74 45410 → 1337 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
71207 2024-10-11 10:56:14,21252… 194.210.61.… 194.210.61… TCP    66 45410 → 1337 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3977596828 TS
71208 2024-10-11 10:56:14,21252… 194.210.61.… 194.210.61… TCP   260 45410 → 1337 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=194 TSval=397759
```

Figure 6 – Packets exchanged in the connection from Rafael Calhau's computer to Miguel Estrela's computer in port 1337

Luckly, from the packet 70599 we knew that by applying the filter tcp contains "file=", we would find all the packets with file that were downloaded. This returned the three mentioned files, including part of the **ariane's blueprint**, that was retrieved by applying the same methods as to the other retrieved files [Follow > TCP Stream, select value after "file= ", URL decode with CyberChef, use function to decode on script.py], and can be found as **ariane.png** (sha256 - 295df4111e9a421dbe6b24f3de40de7f249fbd74c6a259bbea53a8fdf044e040).

4 Based on all the evidence gathered in this investigation, what can you infer regarding the conspiracy hypothesis that initiated this inquiry? Did you find any additional evidence supporting it? If so, who might be the actors involved, and what steps would you recommend for the next phase of the investigation?

Based on all the evidence gathered throughout this investigation, we conclude that there are indeed signs that the Ariane 6 satellite, along with MKU-Control, is being used to influence the population of Oeiras to frequent certain restaurants, thereby increasing their profits.

Our research uncovered several pieces of evidence that confirm the initial hypothesis:

- Original files discovered in past investigations
- Internet searches on how to use MKU-Control
- Emails among key individuals involved in this case
- The diary of one of the main developers of the satellite
- Discord conversations indicating suspicious activity related to the satellite

Throughout our investigation, we identified new individuals connected to this case, as well as confirmed the involvement of others.

The role of Miguel Estrela stands out as the central figure in this investigation, as he obtained critical files relevant to the inquiry. Although he may have obtained these files with good intentions, it is crucial to emphasize that they were acquired through illegal means.

Diogo, Miguel's friend, plays an important role, as he advises Miguel and discusses the discoveries Miguel makes, suggesting future steps to take.

Rafael, a student involved in the development of the Ariane 6 satellite, appears as a significant figure in this case. His diary and the emails found on his computer provide evidence that the satellite is affecting the Oeiras area, and we should not rule out the possibility that he may be involved.

Virgolino reappears in this investigation, being mentioned in multiple emails as well as Rafael's diary. He appears to be one of the main orchestrators of this scheme, alongside two other figures: the mayor of Oeiras and a person named Adelino.

To advance this investigation, we recommend implementing monitoring protocols for communications among all identified parties, particularly Miguel, Diogo, Rafael, and Virgolino, to confirm any ongoing suspicious activities. Additionally, a forensic audit should be conducted on the financial records and communication history of the mayor of Oeiras and Adelino, which may reveal any financial or strategic incentives tied to the alleged conspiracy. Finally, interviewing additional lab members and cross-referencing satellite operational logs with key dates and events will help clarify the scale of involvement and whether more individuals are implicated in this potential scheme.