INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2025-2026 – 1st Period

Digital Forensics Report Lab3

Group number:	51	Name	IST Number
Student 1:		Nuno Martins	107273
Student 2:		Olha Buts	116276
Student 3:		Vasco Conceição	106481

1. Acquired artifacts

Name	Type	SHA-256 Value
Cleaned_full_chat_freenode	txt	b5fb983d59d3caaa33eeba9d6b6831a92974b3989b70ab318c75310e6e331e99
t1-tcp_stream_0	txt	a449263a629e157dbbd60c753b93cb49fa543f05051c543925edb7cd9684e97c
t1-tcp_stream_129	txt	256a46def583ac7861ed46755941d1eeb91b2741a45b5cf78bd2a838b8366175
t1-tcp_stream_130	txt	82cfe3d44716c3cc4da4ac1615f26972af2789672d29e2eb9a1c4b829cf0a18b
t2-tcp_stream_1620	txt	1a784c9fe8d3749327c8e5af60c9687ab7ba0eb35dbe983d937a5fab4c9fd021
t3-tcp_stream_16	txt	15c670ed081724b8dc12e268d1c480b7d701d2d57ed30b5744b9bab0e1b35a78
t3-tcp_stream_2054	txt	fa92c463f98c14b3e49ce7f0ecbf08a6a5d18a949b5b4201af66cbf0cc29c2d6
cleaned_full_chat_chatgpt	txt	aaf1ba60b1f9db7e8740d5d83ed0ccb29b6204a6deb5f7e215ef4e3a4ebc951f
jygyt1	png	c938a05b84f2d749fc6ac65a88f57ccc0c860d4169577947425cc01aa1bbd1c3
nyinuq	png	ff56d339f5affe0279530214dec0ef01950828beb4af6bfa83fe8465a71da7d8
diff	txt	69ed8e73d0874169f52e8e69eed928e29a82a439cc3d12aa28ea9c8b3ed6a489
t2-tls_stream	txt	35ea5dd8fc92bdb00e0142c36d7ec66527e157a14bbdb270ef7ad55a8a68288
t2-tls_stream_cleaned_responses	txt	c2445b1c61063d0690a5a62779afce977a717fc85d4424348a18664d10f5a53f
t3-tls_stream	txt	6ebaea5000dbc88c417569fbcea1b0f24bc108035af5cc375ecea0531e715b1c
t3-tls_stream_cleaned_responses	txt	f36cf6711e79cecec70ef06f890f064c6caba6860bd72157c3e2c695018e2a29
adelino	eml	49b2145a07148626cfd58527947eddecd332996c7740283450d0a14f599ec90
parking	db	23108d6552bbd633ed80c3de50449e0698294c0da3a049a61bbaed41e0edcea0

smart_algorithm	eml	043dc8284a24e3cfaea036259569261079dad68c5b40a0689715cabd5d586481
t2-miguel_finds_db	txt	63946e4efc85fabf9a4f6f95e8144577667454c4df073d0be900318d613a6b78
FinancialReport_recovered	pdf	c648f998562c67ef9ae45cea8c21f2f462fe14401ffc5687fb4980240a4414b8
Invoice_recovered	pdf	6237e452e109592c5abf87b027975ff113651658c2581febf86064d43cd31779
pdf1	txt	92ab7f0ec01eba22f4dc23ad2363d56460878f873cb2f0f656aeb7f9b25ede02
pdf2	txt	a93b0984764f3837bcc71e7a1822585ef54ad04aa7b873d512ad5e782a6f3935

2. Report of all findings

Artifacts were extracted from three Wireshark capture files provided as evidence. The analysis involved searching for files, communications, correlations, and behavioral traces across multiple network sessions. By filtering and inspecting network packets, we were able to reconstruct user activity, identify potential intrusion attempts, and recover communication logs between internal MEMEL employees. The findings were correlated by timestamp and IP address, confirming the sequence of events and the relationships between the individuals involved.

The identified participants and their corresponding IP addresses are as follows:

- Duarte Calado – IT Director – IP: 194.210.61.134
- Adelino Estoiro – Financial Director – IP: 194.210.61.135
- Miguel Pontes – Gateway Security Intern – IP: 194.210.61.136

September 5, 2025 - t1.pcapng:

Miguel Pontes, a Gateway Security Intern at MEMEL, overheard a conversation between Duarte Calado, the IT Director, and Alcibiades. Alcibiades was asking Duarte to pull some strings to avoid paying for parking. When Miguel entered the kitchen, both men noticed his presence and abruptly changed the subject, joking about mining Bitcoin to buy the new iPhone. This behavior raised Miguel's suspicions, prompting him to share the incident with his colleague Catarina Pato, an intern in the information systems team.

Following Miguel's report, Catarina investigated a database bug and discovered irregularities in the company's code repository. She found that Duarte had previously committed code directly to production, containing unusual and suspicious rules. This finding was linked to the diff file recovered during earlier investigation steps.

Miguel researched parking fee complaints in Lisbon and found Reddit posts from foreign visitors stating they were charged more than Portuguese residents at parking facilities. He shared a screenshot of these posts with Catarina, confirming that the discriminatory pricing rules in the code were actively impacting real customers.

All details above are corroborated by the recovered chat logs between Miguel and Catarina ("CatDucky"), on September 5, available in *Cleaned_full_chat_freenode.txt*.

Wireshark display filter	Starting packet	Time (from/until)	Description
tcp.stream eq 0	21	09:05:17 -- 09:07:50	Miguel was chatting with CatDucky (during this conversation Miguel was also on Spotify, probably hearing the music that CatDucky sent him).
tcp.stream eq 129	19669	11:27:32 -- 11:31:21	Miguel was chatting with CatDucky.
tcp.stream eq 130	19994	15:27:30 -- 15:37:45	Miguel was chatting with CatDucky.
(also in) tcp.stream eq 130	20201	15:29:32 -- 15:30:04	CatDucky sends Miguel the diff file from previous investigation via text.
----------	20390	15:35:34	Miguel sends Catarina a link to the reddit image from previous investigation via chat.

Morning of September 6, 2025 - t2.pcapng:

Wireshark display filter	Starting packet	Time (from/until)	Description
tcp.stream eq 59	4505	11:00:00 -- 11:03:02	Miguel was on https://www.kali.org/tools/arp-scan/.
arp	8573	11:00:52 -- 11:01:17	Miguel ran an arp scan on the sub-network.
tcp.stream eq 140	16604	11:01:05 -- 11:01:13	Miguel was on https://nmap.org/book/man-port-scanning-techniques.html.
tcp.stream eq 170	18156	11:01:33 -- 11:04:28	Miguel was on https://www.geeksforgeeks.org/ethical-hacking/port-scanning-techniques-by-using-nmap/.
(tcp.flags.syn == 1 and tcp.flags.ack == 0 and ip.dst == 194.210.61.134) or (tcp.flags.reset == 1 and ip.dst == 194.210.61.136)	30258	11:01:49 -- 11:01:49.	Miguel ran a port scan on Duarte.
tcp.stream eq 1344	34316	11:01:59 -- 11:07:51	Miguel opened ChatGPT. Conversation is in discoveries/chatgpt/t2-tls_stream.txt.
----------	61103	11:05:18	Miguel searched "how to use medusa" in google.
tcp.stream eq 1414	62951	11:05:26 -- 11:08:18	Miguel was on https://www.kali.org/tools/medusa/.
tcp.stream eq 1415	63285	11:05:51 -- 11:05:52	Duarte downloaded: http://archive.ubuntu.com/ubuntu/pool/main/p/poppler/poppler-utils_24.02.0-1ubuntu9.7_amd64.deb.

ip.dst == 194.210.61.134 and ip.src == 194.210.61.136 and ftp	64468	11:06:20 -- 11:08:48	1. Miguel connects to FTP service (port 21) on Duarte's machine. 2. Logs in as duarte, after 13 failed attempts, he uses the correct the password: "duartinhothebest". 3. Browses directories. 4. Downloads files (files recovered by pressing File -> Export Objects -> FTP-DATA).
----------	65042	11:08:01	Miguel downloads parking.db from Duarte's computer.
----------	65339	11:08:32	Miguel downloads adelino.eml from Duarte's computer.
----------	65359	11:08:37	Miguel downloads smart_algorithm.eml from Duarte's computer.
tcp.stream eq 1468	67741	11:10:40 -- 11:10:46	Miguel was on https://belocal.pt/en/parking-in-lisbon/.
tcp.stream eq 1530	80005	11:11:09 -- 11:14:10	Miguel was on https://en.wikipedia.org/wiki/Smart_city.
tcp.stream eq 1555	81404	11:11:25 -- 11:12:01	Miguel was on https://lisboaaberta.cm-lisboa.pt/index.php/pt/lisboa-inteligente.
tcp.stream eq 1576	85873	11:12:01 -- 11:12:08	Miguel was on https://futurointeligente.pt.
tcp.stream eq 1620	91054	11:14:57	Miguel was chatting with CatDucky.

Afternoon of September 6, 2025 - t3.pcapng:

Wireshark display filter	Starting packet	Time (from/until)	Description
tcp.stream eq 16	178	15:12:20 -- 15:17:12	Miguel was chatting with CatDucky.
----------	491	15:14:15	Miguel sends Catarina a link to the WhatsApp image from previous investigation via chat.
arp	679	15:17:30 -- 15:17:43	Miguel Ran an arp scan on the sub-network.
(tcp.flags.syn == 1 and tcp.flags.ack == 0 and ip.dst == 194.210.61.135) or (tcp.flags.reset == 1 and ip.dst == 194.210.61.136)	2812	15:17:44 -- 15:17:44	Miguel ran a port scan on Adelino.
----------	5025	15:17:49	Miguel searched "How to establish a connection using ssh port" in google.
tcp.stream eq 1058	7018	15:17:54 -- 15:20:46	Miguel was on https://askubuntu.com/questions/264046/how-to-run-the-ssh-server-on-a-port-other-than-22.
tcp.stream eq 1160	12523	15:18:09 -- 15:21:19	Miguel was on https://www.digitalocean.com/community/tutorials/how-to-use-ssh-to-connect-to-a-remote-server.
tcp.stream eq 1268	20241	15:18:32 -- 15:20:34	Miguel was on https://opensource.com/article/20/9/ssh.

ssh	23560	15:18:56 -- 15:18:56	Miguel tested a ssh connection to Adelino's computer on port 22.
----------	23666	15:19:02	Miguel searched for "phishing" in google.
tcp.stream eq 1348	27160	15:19:13 -- 15:20:26	Miguel was on https://www.malwarebytes.com/pt/phishing.
tcp.stream eq 1447	32848	15:19:37 -- 15:23:53	Miguel opened ChatGPT. Conversation is in discoveries/chatgpt/t3-tls_stream.txt.
----------	47541	15:22:02	Adelino searched for "what to do with excess money" in google.
tcp.stream eq 1555	52748	15:22:06 -- 15:26:18	Adelino was on https://www.reddit.com/r/FinancialPlanning/comments/umjp5b/what_to_do_with_extra_money/.
----------	60407	15:22:41	Adelino searched for "gambling" in google.
tcp.port = 1337	95057	15:31:57 -- 15:35:16	Adelino's computer connects multiple times to Duarte's computer via port 1337, to a Python-based HTTP server, probably backdoor.
----------	95556	15:33:19	Adelino's computer sends 1 encrypted file to Miguel's computer.
----------	95913	15:34:50	Adelino's computer sends 1 encrypted file to Miguel's computer (later we found that these 2 files were the pdfs from previous investigations, Memel's financial report and Invoice tied to Futuro Inteligente).
tcp.stream eq 2054	96095	15:35:55 -- 15:44:54	Miguel was chatting with CatDucky.

All findings that required additional analysis or code execution were saved in the *discoveries* directory:

Name	Discovery Method and Context	Evidentiary Value
Cleaned_full_chat_freenode.txt	Cleaned full chat from chat.freenode.com streams	Reveals all the story from Miguel's perspective in a chat with CatDucky.
t1-tcp_stream_0.txt	In file t1.pcapng, apply display filter in Wireshark: tcp.stream eq 0 Right click packet -> Follow -> TCP Stream -> Save as -> t1-tcp_stream_0.txt	Part of Miguel's chat with CatDucky.
t1-tcp_stream_129.txt	t1: tcp.stream eq 129	Part of Miguel's chat with CatDucky.
t1-tcp_stream_130.txt	t1: tcp.stream eq 130	Part of Miguel's chat with CatDucky.
t2-tcp_stream_1620.txt	t2: tcp.stream eq 1620	Part of Miguel's chat with CatDucky.
t3-tcp_stream_16.txt	t2: tcp.stream eq 16	Part of Miguel's chat with CatDucky.
t3-tcp_stream_2054.txt	t3: tcp.stream eq 2054	Part of Miguel's chat with CatDucky.

diff.txt	t1 : tcp.stream eq 131	Diff file from previous investigation retrieved from Miguel and CatDucky chats.
nyinuq.png	t1: packet 20390	Reddit image from previous investigation retrieved from Miguel and CatDucky chats.
jygyt1.png	t3: packet 49	WhatsApp image from previous investigations retrieved from Miguel and CatDucky chats.
cleaned_full_chat_chatgpt.txt	Cleaned full chat from chatgpt streams	Part of Miguel's chat with ChatGPT.
t2-tls_stream.txt	t2: tcp.stream eq 1447 (extracted by following TLS stream)	Part of Miguel's chat with ChatGPT.
t2-tls_stream_cleaned_responses.txt	t2: Cleaned ChatGPT responses from chatgpt_responses.py script (password brute force)	Part of Miguel's chat with ChatGPT.
t3-tls_stream.txt	t3: tcp.stream eq 1344 (extracted by following TLS stream)	Part of Miguel's chat with ChatGPT.
t3-tls_stream_cleaned_responses.txt	t3: Cleaned ChatGPT responses from chatgpt_responses.py (email)	Part of Miguel's chat with ChatGPT.
t2-miguel_finds_db.txt	t2: packet 65042	Shows FTP access to Duarte Calado's account and retrieval of files, including emails.
adelino.eml	t2: packet 65339	E-mail from Adelino Estoiro to Duarte Calado confirming the payment to Futuro Inteligente, for AI services.
parking.db	t2: packet 65042	Database extract showing license plates flagged as testers, matching those listed for preferential treatment.
smart_algorithm	t2: packet 65359	Shows directive from the mayor to alter a system for preferential treatment of specific license plates.
pdf1.txt	t3: packet 95556	Encrypted PDF.
pdf2.txt	t3: packet 95913	Encrypted PDF.
FinancialReport_recovered.pdf	Decrypted from pdf1.txt using decrypt_pdfs.py	One of the PDFs from previous investigation.
Invoice_recovered.pdf	Decrypted from pdf2.txt using decrypt_pdfs.py	The other PDF from previous investigation.

We can deduce that Catarina is CatDucky, found in previous investigations and this chat retrieved from their chats helps with that:

PRIVMSG: Hey Ducky!!!

CatDucky: Oh god... don't call me like that you know that I don't like my surname..

(Pato is Catarina's surname, which translates to ducky from Portuguese to English)

3. Analysis of relevant findings

3.1 Do the analyzed network traces contain evidence of transfers involving any of the six hidden documents identified in previous assignments? What can you infer about the source and origin of these documents within MEMEL's network?

The analyzed network traces contain clear evidence of transfers involving the six hidden documents of the previous assignments.

- The diff file was sent from CatDucky to Miguel.
- Miguel received 2 files from Adelino's backdoor.
- Miguel got the Database file from Duarte's PC (FTP).
- Miguel sent CatDucky 2 pictures (WhatsApp and reddit).

In total, 6/6 documents were present in the analysis of the network traces.

Network trace evidence clarifies the origin of the documents obtained from MEMEL's network. Duarte Calado's workstation acted as a local repository for operational data, including parking.db and personal email exchanges with Mayor Eurico Trocos. The presence of production database copies and private correspondence indicates that Duarte kept sensitive data locally and used personal accounts for communications related to the fraudulent scheme.

Adelino Estoiro's machine stored key financial records such as the annual report and vendor invoices. Their retrieval through a backdoor connection, shows that the Financial Director maintained local copies of crucial documents evidencing payments to Futuro Inteligente and revenue diversion. These files were in directories accessible to the malware Miguel installed via phishing.

3.2 Based on the observed network activity, what can you deduce about the identity of the person or persons responsible for transferring the documents?,

Network evidence clearly identifies **Miguel Pontes**, the Gateway Security Intern, as the main actor responsible for the unauthorized document transfers. His workstation is directly linked to nearly all intrusion and exfiltration activity. Multiple attack vectors originated from his IP address, including ARP scans mapping the internal network and port scans against Duarte Calado's and Adelino Estoiro's machines. These reconnaissance actions preceded the unauthorized access to sensitive files.

The FTP session to Duarte's workstation came from Miguel's IP, showing thirteen failed logins before success, followed by directory browsing and retrieval of *parking.db* and email files. The backdoor on port 1337 further demonstrates his role — Miguel's system acted as the receiving server for encrypted uploads from Adelino's compromised machine. This backdoor, installed after a phishing attack crafted by Miguel, disguised file transfers as normal web traffic using HTTP POST requests and encryption, revealing both intent and technical proficiency.

Network logs also show Miguel accessing ChatGPT to research FTP brute-forcing and to draft a phishing email posing as the company's CISO. These consultations directly preceded the related attacks, evidencing planning and awareness. His browsing history included searches on hacking tools (arp-scan, nmap, Medusa), phishing methods, and research on Lisbon parking and Futuro Inteligente, indicating simultaneous technical preparation and contextual investigation. Uploads to external hosting sites such as catbox.moe confirm his role in distributing the stolen materials.

Catarina Pato, the Information Systems Intern, also participated but in a more limited, analytical capacity. Network traces show her accessing the company's code repository legitimately to retrieve the diff file exposing Duarte's discriminatory algorithms. Chat logs between the two, demonstrate collaboration: Catarina analyzed code anomalies, suggested investigative targets, and advised Miguel to explore Adelino's files for links to Futuro Inteligente. However, Miguel executed all intrusive operations while Catarina focused on interpretation and external coordination.

Catarina was also the planned recipient of the exfiltrated data. Chats show that Miguel intended to email her the files from a burner account via public Wi-Fi, enabling her to claim she had received them anonymously before passing them to her friend João, connected to the mayor's political rival. This arrangement indicates conscious coordination and an attempt to obscure their involvement.

The traces further confirm that Duarte and Adelino did not transfer the documents themselves; their workstations merely stored the incriminating data that Miguel accessed without authorization. Similarly, the WhatsApp screenshot originated from an unidentified colleague's unattended phone, which Miguel photographed and later uploaded online.

In summary, the network analysis conclusively attributes the unauthorized data exfiltration to **Miguel Pontes**, supported by clear links between his IP, timestamps, and command sequences. **Catarina Pato** acted as a collaborator, providing analytical guidance and serving as the conduit for disseminating the materials. Duarte Calado, Adelino Estoiro, and the colleague with the phone were data sources or unwitting participants rather than active accomplices.

3.3 Can you reconstruct a timeline of key events that explains how the data exfiltration took place and how the documents ultimately reached João Musk's possession? Present your reasoning clearly and reference all timestamps used to establish the chronology.

On the morning of September 5, 2025, Miguel Pontes overheard Duarte Calado and Alcibiades in the office kitchen discussing something suspicious; when Miguel arrived they abruptly switched to talking about Bitcoin and iPhones. He immediately messaged Catarina Pato, starting a joint inquiry. That day Catarina, while debugging a database issue, found the diff file. Catarina shared this with Miguel, who then found the reddit post.

On September 6, Miguel escalated to active reconnaissance. He searche for ARP scanning techniques and then he ARP-scanned the subnet. He then searched for Port Scanning techniques and performed a Port Scan on Duarte's PC. After, he searched for FTP techniques and password brute-forcing with ChatGPT. Miguel searched on how to use "medusa" and performed a password-guessing attack: after thirteen failed attempts he logged in with username "duarte" and password "duartinhothebest." He browsed Desktop, Documents, Downloads and Pictures and downloaded three key files: parking.db (showing discriminatory pricing), adelino.eml (an email from the Financial Director confirming payment to Futuro Inteligente for AI services), and email correspondence between Duarte and Mayor Eurico Trocos about special treatment for specific plates. Miguel also checked company records via a cousin at Loja do Cidadão and learned Futuro Inteligente was owned by Cremilde Trocos, the mayor's wife, linking the scheme to the mayor's family.

That afternoon Miguel targeted Adelino Estoiro. After ARP and port scans revealed SSH on port 22, he researched SSH and made a test connection. He searched about phishing, again consulted ChatGPT for about four minutes to draft a phishing email posing as the CISO about credential revocation; the assistant provided a formal template. Miguel sent the phishing message; Adelino complied, revoking credentials and updating tokens, which let Miguel install a backdoor. The compromised machine then connected outbound to Miguel's workstation on port 1337, where he ran a Python HTTP server; two encrypted files were transferred and, after decryption, revealed MEMEL's 2024 financial report and a Futuro Inteligente invoice.

Miguel also photographed a colleague's unattended phone showing the WhatsApp image. He AirDropped the image, deleted it from the colleague's phone, uploaded it to external hosting, and shared it with Catarina. With six documents now exfiltrated—the database, two emails, two decrypted files, and the WhatsApp screenshot—Miguel and Catarina agreed the evidence showed systematic price discrimination and revenue diversion to Futuro Inteligente.

Catarina then proposed passing the materials to João, whose father was running against Mayor Eurico Trocos in the October mayoral election. To avoid attribution, they planned a transfer

protocol: Miguel would create a burner email, send all files from a public Wi-Fi using a clean virtual machine with a vague subject like "You need to know," and Catarina would present the materials to João as anonymously received. João would then give the evidence to his father's campaign.

3.4 Considering all the evidence collected throughout the MEMELgate investigation, what can you now conclude about the hypothesis of fraudulent activity within MEMEL that initiated this inquiry? Did you uncover additional evidence supporting the existence of fraud? Identify the actors who may be involved and outline your recommendations for the next phase of the investigation.

The evidence conclusively confirms that large-scale fraudulent activity occurred within MEMEL, involving deliberate price discrimination, revenue diversion, and abuse of public office for personal gain. Code and database analyses revealed algorithms that overcharged foreign and rental vehicles while exempting privileged plates from payment. Financial records reveal that revenues were redirected to Futuro Inteligente Lda—owned by Mayor Eurico Trocos's wife, Cremilde Trocos — creating a direct link between municipal funds and the mayor's household.

Email and WhatsApp communications confirm coordination among key actors. Mayor Trocos personally instructed Duarte to favor certain vehicles, while Financial Director Adelino Estoiro approved irregular payments to Futuro Inteligente. Conversations in the "Parkinator" group show both officials actively managing the preferential treatment scheme. Alcibiades and an unidentified colleague appear to have benefited or assisted.

This evidence expands the original hypothesis, revealing a structured and concealed fraud network combining algorithmic manipulation, financial corruption, and political collusion.

Involved actors:

- Eurico Trocos (Mayor): Directed and benefited from the scheme.
- Cremilde Trocos: Owner of the beneficiary company, Futuro Inteligente.
- Duarte Calado (IT Director): Designed and implemented the fraudulent system.
- Adelino Estoiro (Financial Director): Authorized and processed illicit payments.
- Alcibiades and others in the WhatsApp group: Possible secondary participants.
- Miguel Pontes and Catarina Pato: Exposed the scheme through unauthorized digital intrusions.

Recommendations:

- Conduct immediate forensic imaging of Duarte's, Adelino's and Miguel's systems and preserve all digital evidence.
- Analyze Duarte's activity in the MEMEL parking repository.
- Retrieve and analyze the full WhatsApp "Parkinator" history.
- Subpoena Futuro Inteligente's financial records to trace funds and verify beneficiaries.
- Interview all suspects and perform a comprehensive audit of MEMEL's pricing and vendor payments to quantify damages.
- Review the mayor's and his wife's financial disclosures for undeclared income.
- Assess the legality of how the evidence was obtained to safeguard prosecutions.
- Strengthen MEMEL's internal controls, transparency mechanisms, and whistleblower protections.

Conclusion:

The investigation confirms a coordinated corruption scheme within MEMEL, combining discriminatory pricing and revenue diversion to enrich the mayor's family. The findings warrant immediate criminal prosecution, financial recovery actions, and systemic reforms to prevent future abuses.

4. Appendices

None.