Lab10: TeamSpy Endpoint Forensics Challenge

Grade Weight: 6%

Background:

Lecture notes + resources provided.

Scenario Overview:

An employee reported that his machine started to act strangely after receiving a suspicious email with a document file. The incident response team captured a couple of memory dumps from the suspected machines for further inspection. As a soc analyst, analyze the dumps and help the IR team figure out what happened.

Objectives:

- Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/93#nav-overview
- Create an account and Login.
- Download the Challenge. Uncompress the challenge (pass: cyberdefenders.org).
- Answer the 16 challenge questions.
- The file is also attached to the ZIP on Blackboard under Lab 10.zip
- Tool Used:
    - Volatilty 2.6
        - https://www.volatilityfoundation.org/26
        - https://github.com/volatilityfoundation/volatility/wiki/Command%20Reference
    - OSTviewer https://www.sysinfotools.com/recovery/ost-file-viewer.php
    - OfficeMalScanner https://www.aldeid.com/wiki/OfficeMalScanner
    - VirusTotal
    - Dotnetfiddle https://dotnetfiddle.net/

Show complete screenshots of all your work.

Challenge Questions

1. File->ecorpoffice: What is the PID the malicious file is running under?
2. File->ecorpoffice: What is the C2 server IP address?
3. File->ecorpoffice: What is the Teamviewer version abused by the malicious file?
4. File->ecorpoffice: What password did the malicious file use to enable remote access to the system?

5. File->ecorpoffice: What was the sender's email address that delivered the phishing email?
6. File->ecorpoffice: What is the MD5 hash of the malicious document?
7. File->ecorpoffice: What is the bitcoin wallet address that ransomware was demanded?
8. File->ecorpoffice: What is the ID given to the system by the malicious file for remote access?
9. File->ecorpoffice: What is the IPv4 address the actor last connected to the system with the remote access tool?
10. File->ecorpoffice: What Public Function in the word document returns the full command string that is eventually run on the system?
11. File->ecorpwin7: What is the MD5 hash of the malicious document?
12. File->ecorpwin7: What is the common name of the malicious file that gets loaded?"
13. File->ecorpwin7: What password does the attacker use to stage the compressed file for exfil?
14. File->ecorpwin7: What is the IP address of the c2 server for the malicious file?
15. File->ecorpwin7: What is the email address that sent the phishing email?

Use the following as a guide –

https://medium.com/@JakubLakomy/teamspy-blue-team-challenge-cyberdefenders-org-6711d1641a59

https://www.youtube.com/watch?v=rAbckmM12QQ – Part 1

https://www.youtube.com/watch?v=tfJKZ2Q3J6A – Part 2

https://www.youtube.com/watch?v=IUh7S428Ys0 – Part 3

https://0x3ifa.notion.site/TeamSpy-Write-up-0033436402304336b80c4fa2b4469abe

Reminders

- Submit your report name: CYT215-Lab10-Student Name & ID
- Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
- NOTE – THIS IS AN INDVIDUAL REPORT AND MUST BE IN YOUR OWN WORDS. ALL THOUGH COLLABORATION IS ENCOURAGED, YOUR REPORT SHOULD BE YOUR OWN. Feel free to reference google when answering the above questions.
- Show your genuine signs of your work is done on your machine. This includes:
- Screenshots that show your desktop background with Date/Time.

- Show a pop-up bx that shows “your name + IP”.
- Show your logged account when applicable. Optional: Your photo.

Please follow and abide by the Seneca Academic Integrity policy –

Academic Integrity at Seneca

What is Academic Integrity?

The International Center for Academic Integrity defines academic integrity as a commitment, even in the face of adversity, to six Fundamental Values of Academic Integrity: honesty, trust, fairness, respect, responsibility, and courage. From these values flow principles of behavior that enable academic communities to translate ideals into action.

Why does Academic Integrity Matter?

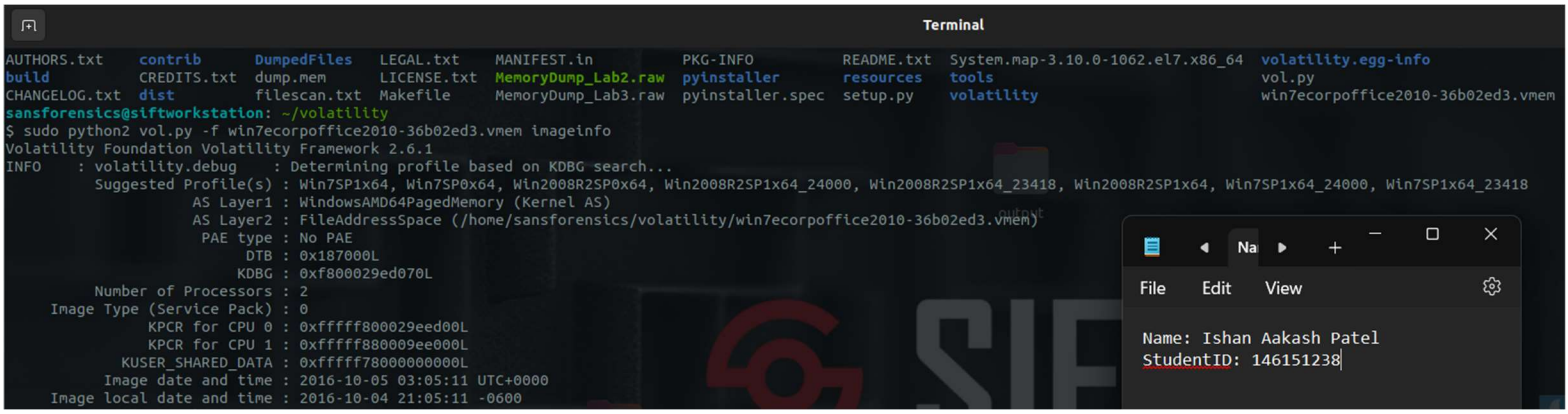
When each member of the Seneca Community embraces and incorporates these values into our teaching, learning and working environments, then we are able to maintain the college’s reputation as a leading educational institution and to graduate high quality students who are poised to succeed in their careers and contribute meaningfully to society.

Academic Integrity - Student Resources

----------**Report goes Below** ----------

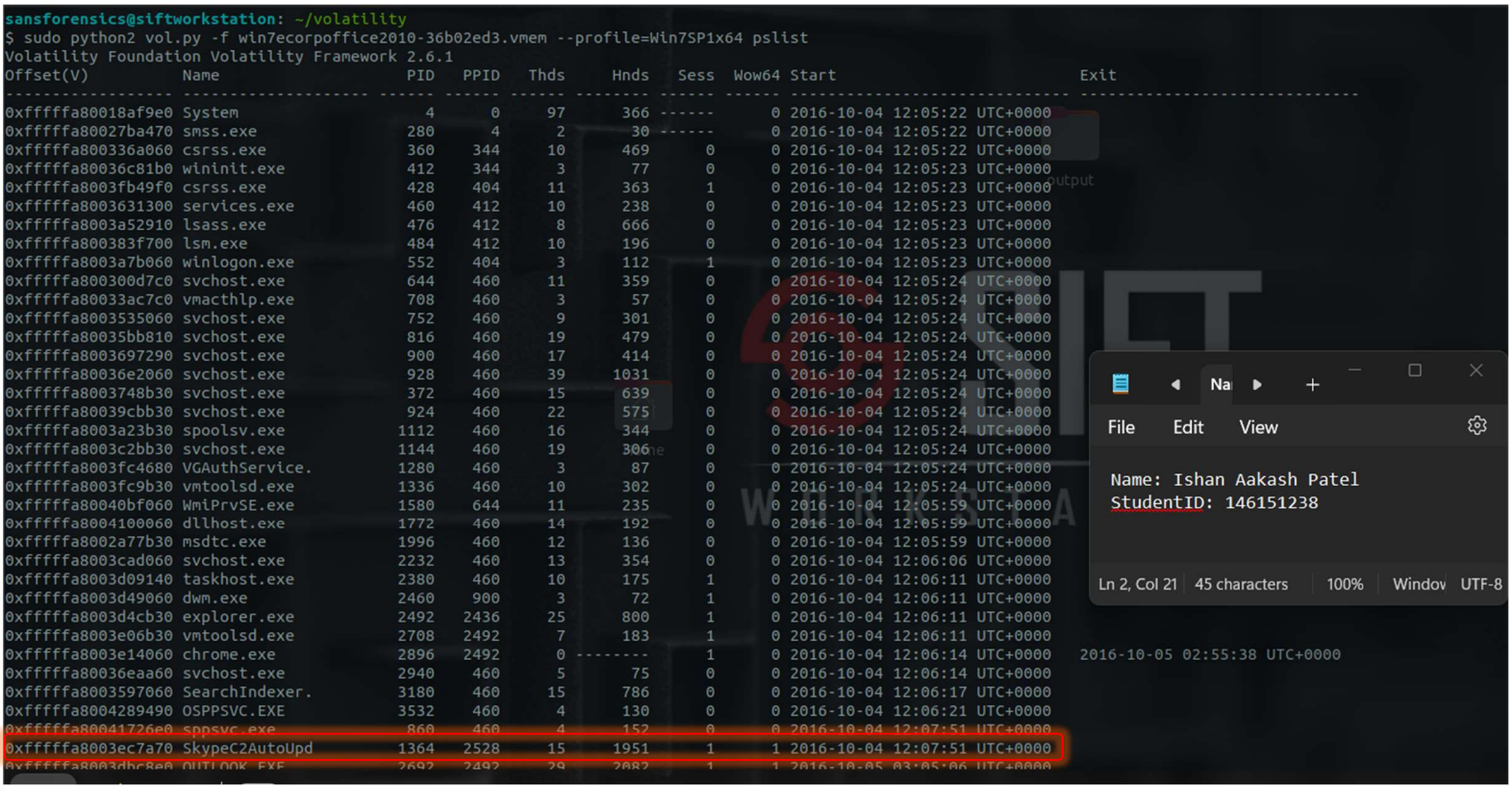
Challenge Questions

1) File->ecorpoffice: What is the PID the malicious file is running under?



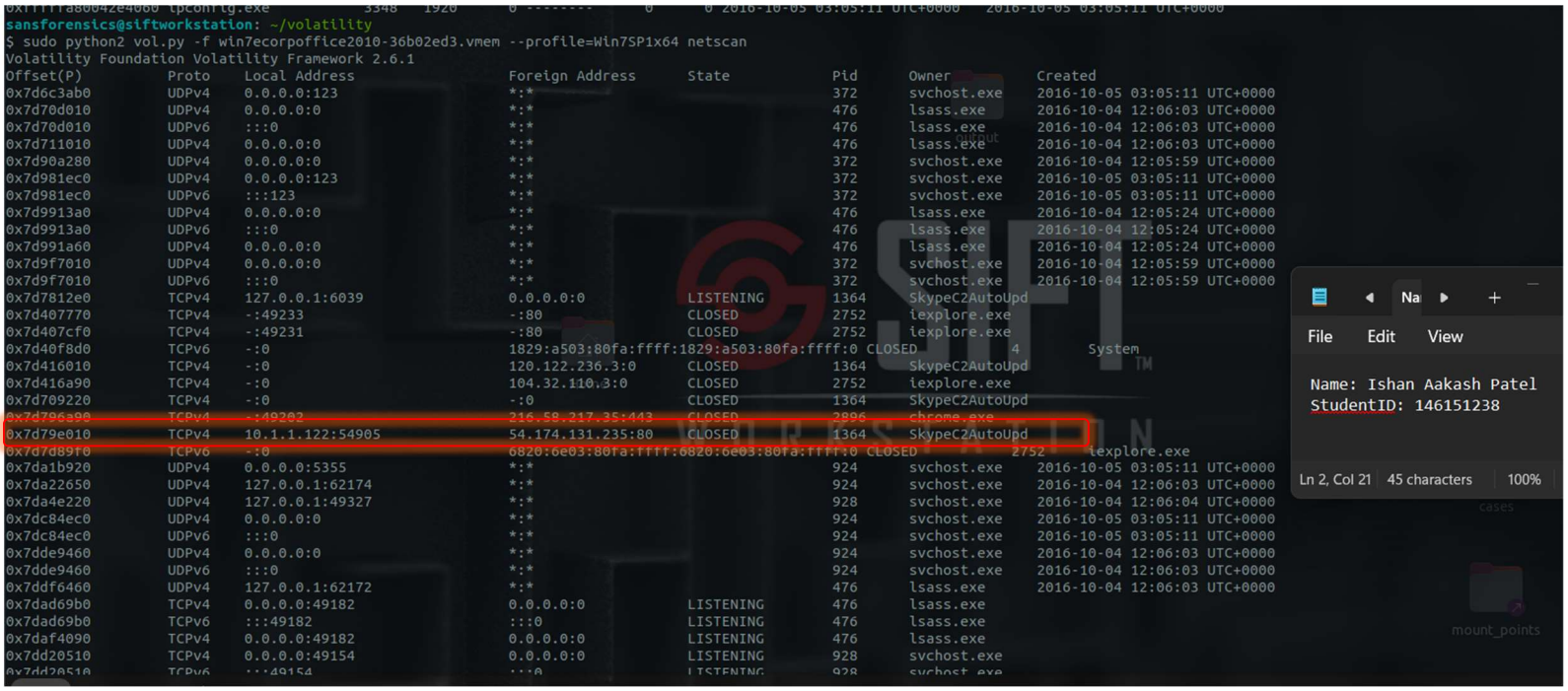
Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem image info

sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 pslist



Answer : 1364

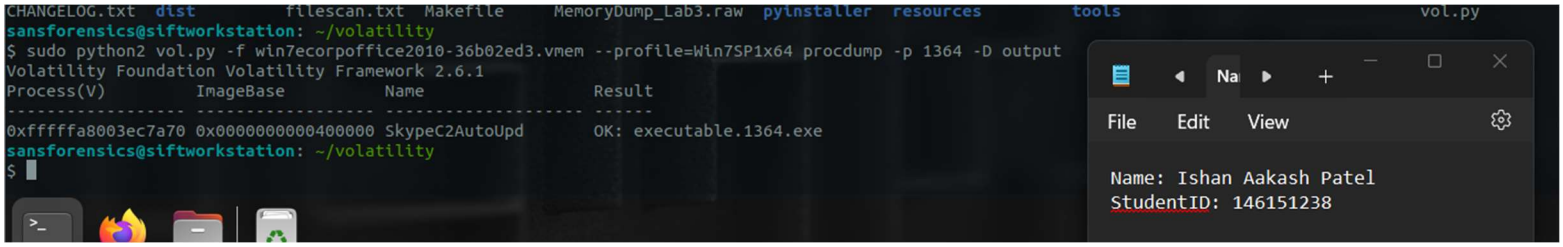
2) File->ecorpoffice: What is the C2 server IP address?



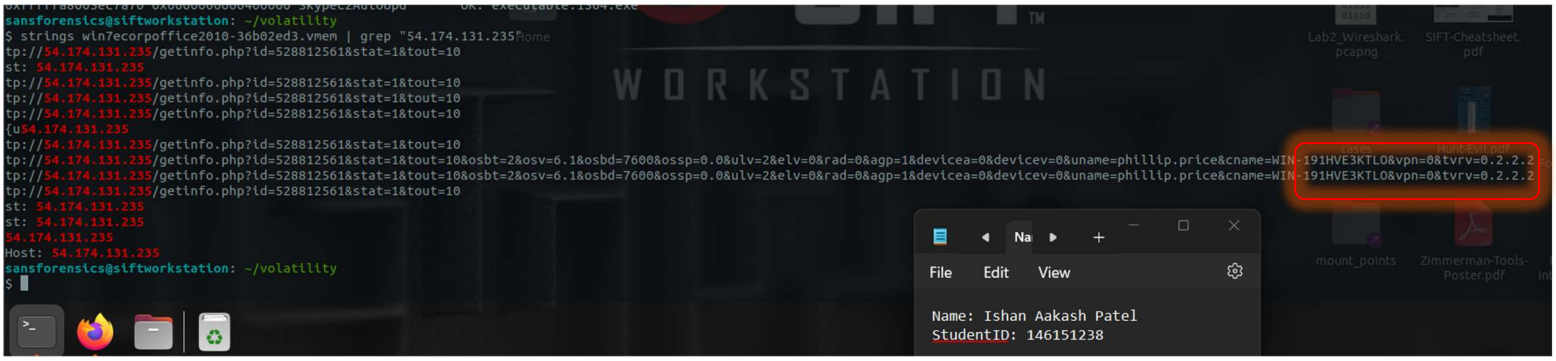
Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 netscan

Answer : 54.174.131.235

3) File->ecorpoffice: What is the Teamviewer version abused by the malicious file?



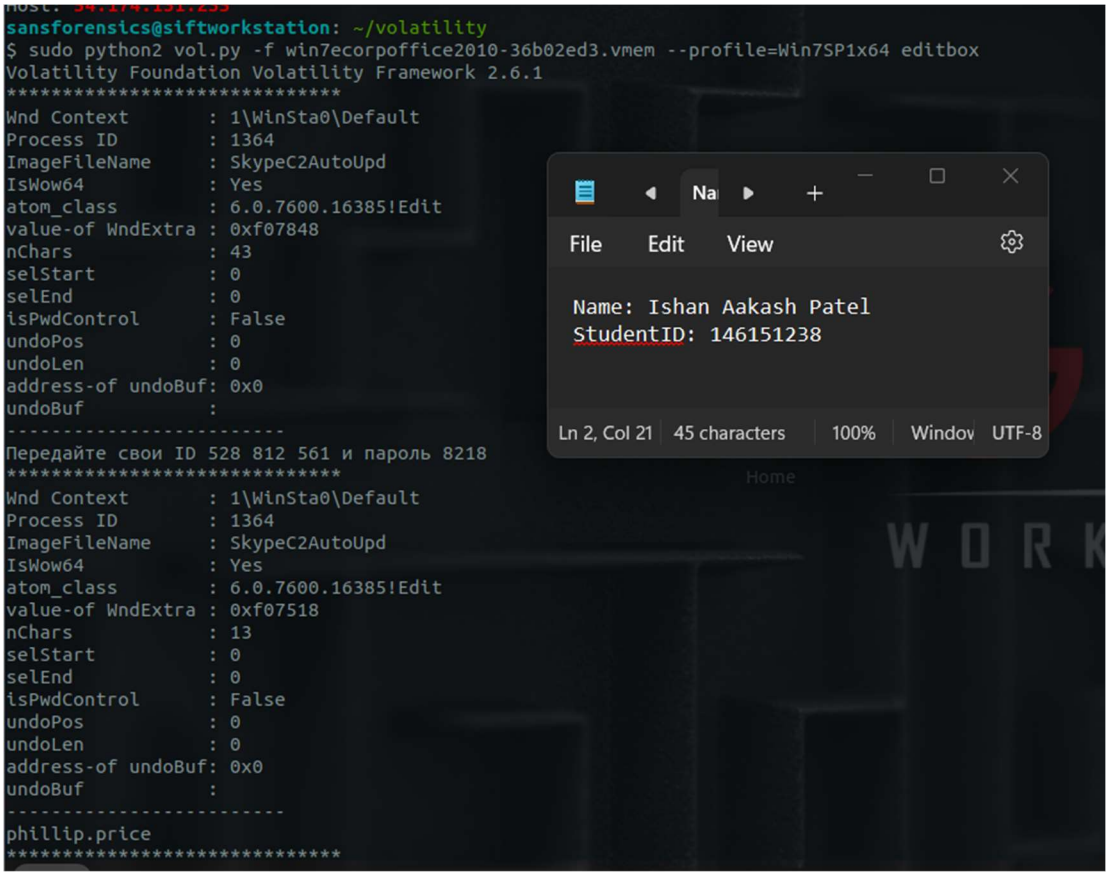
Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 prodump -p 1364 -D output

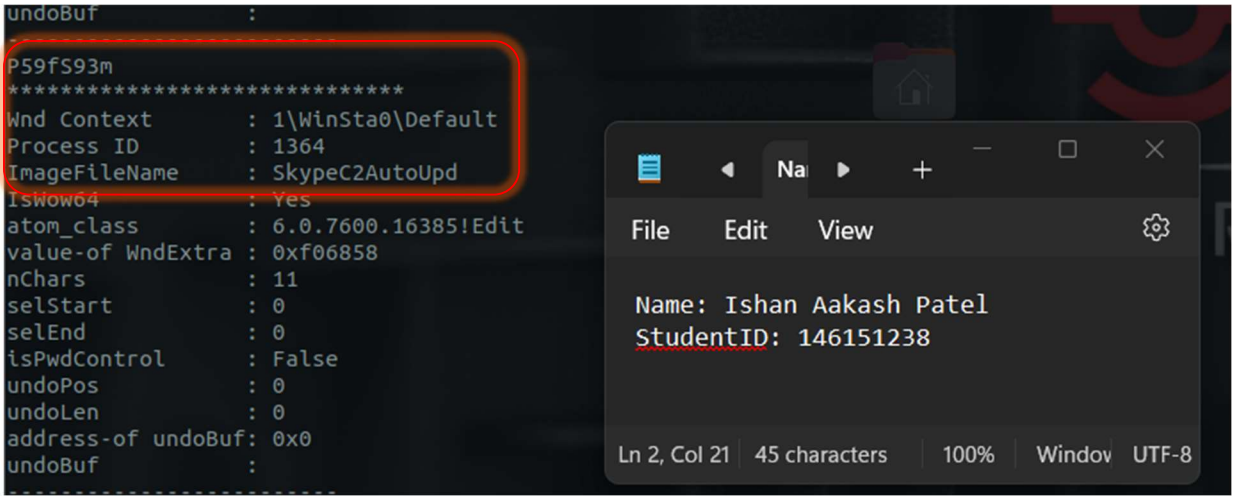


Command : strings win7ecorpoffice2010-36b02ed3.vmem | grep "54.174.131.235"

Answer : 0.2.2.2

4) File->ecorpoffice: What password did the malicious file use to enable remote access to the system?

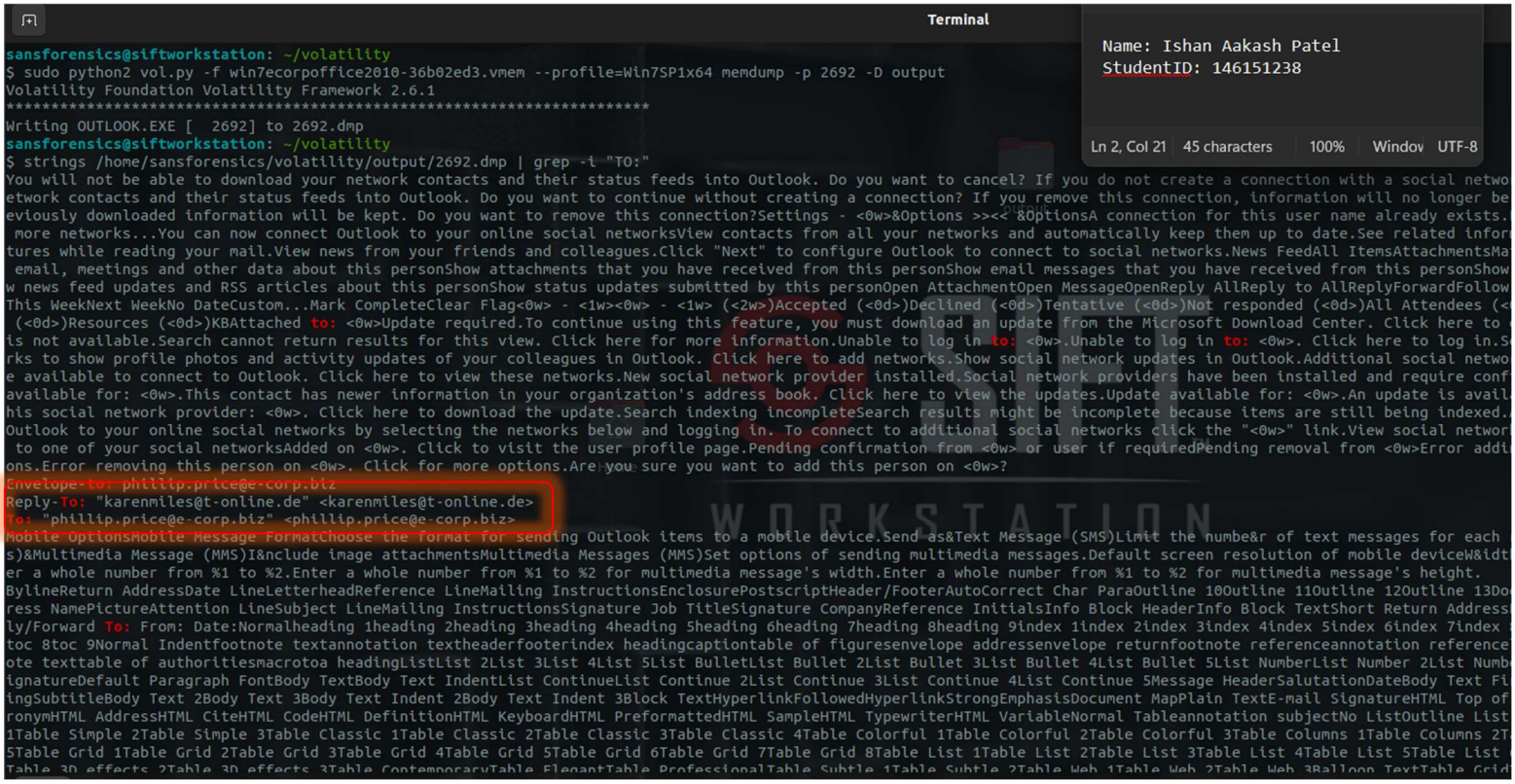




Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 editbox

Answer : P59fS93m

5) File->ecorpoffice: What was the sender's email address that delivered the phishing email?

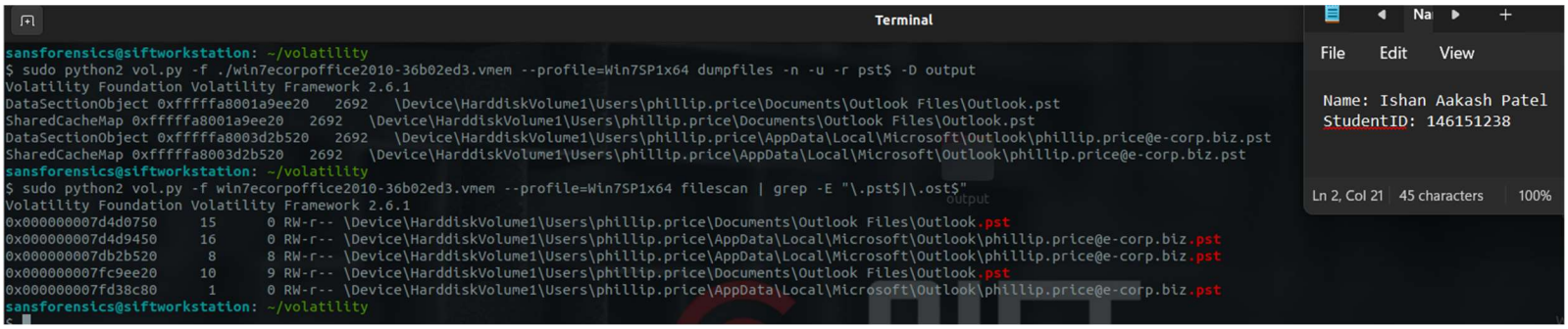


Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 memdump -p 2692 -D output

Command : strings /home/sansforensics/volatility/output/2692.dmp | grep -I “TO:”

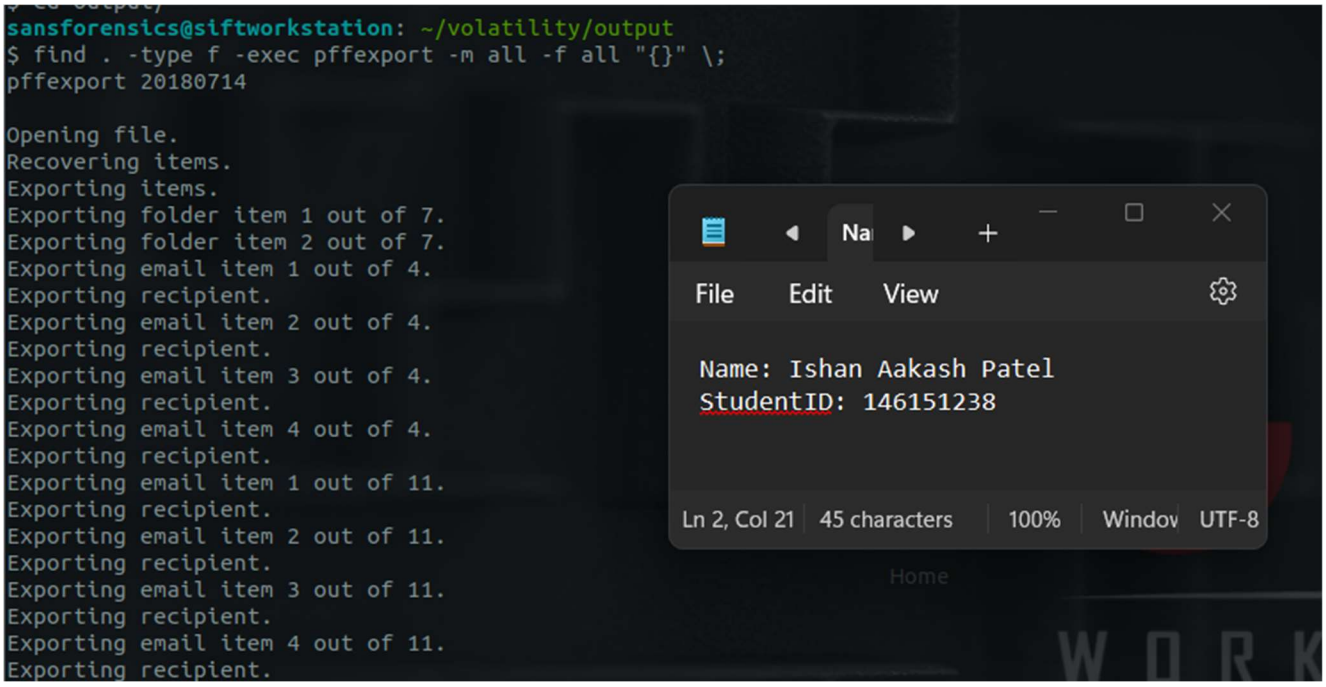
Answer : karenmiles@t-online.de

6) File->ecorpoffice: What is the MD5 hash of the malicious document?



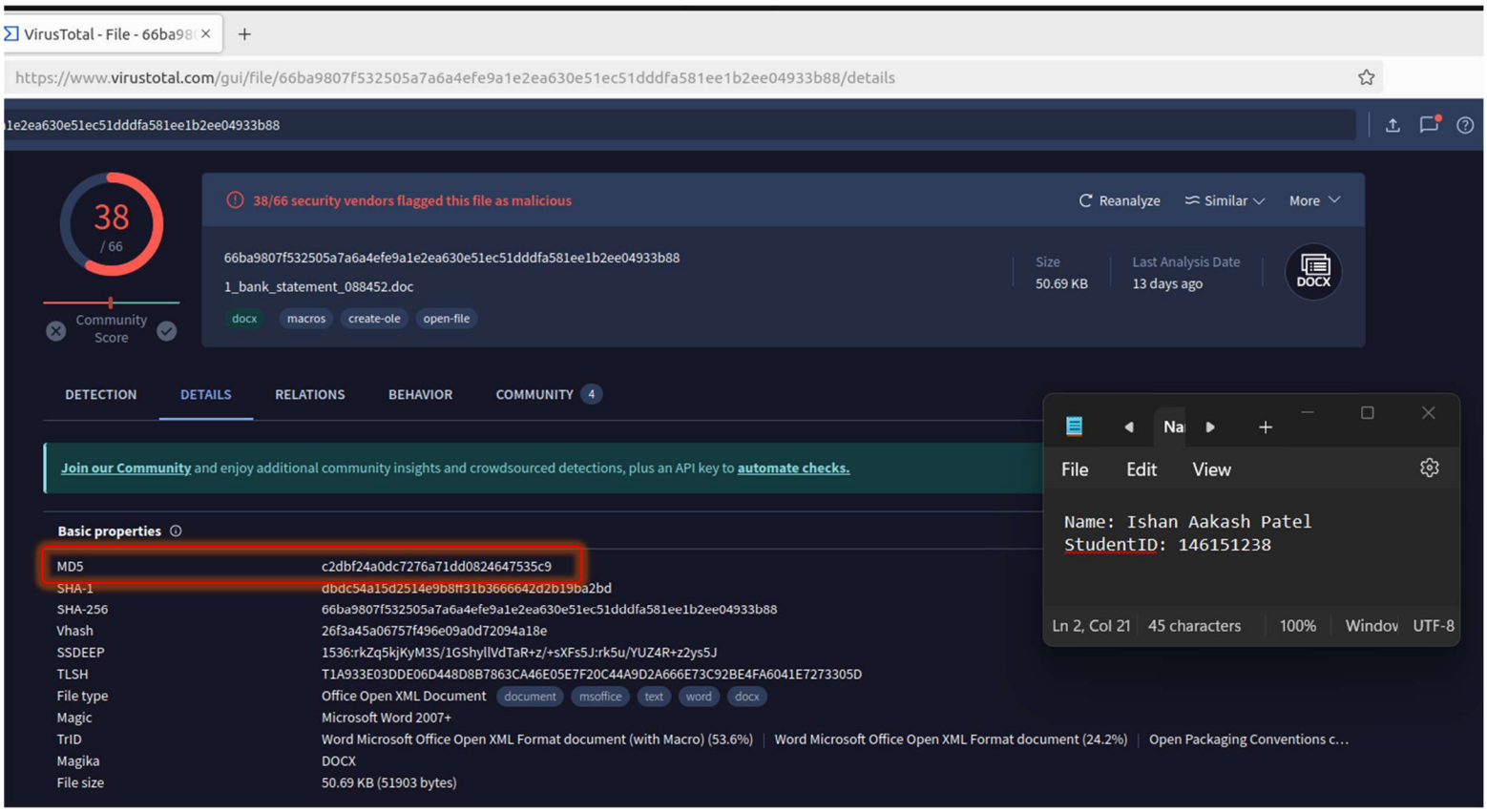
Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 filescan | grep -E "\.pst$|\.ost$"

sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 dumpfiles -n -u -r pst$ -D output



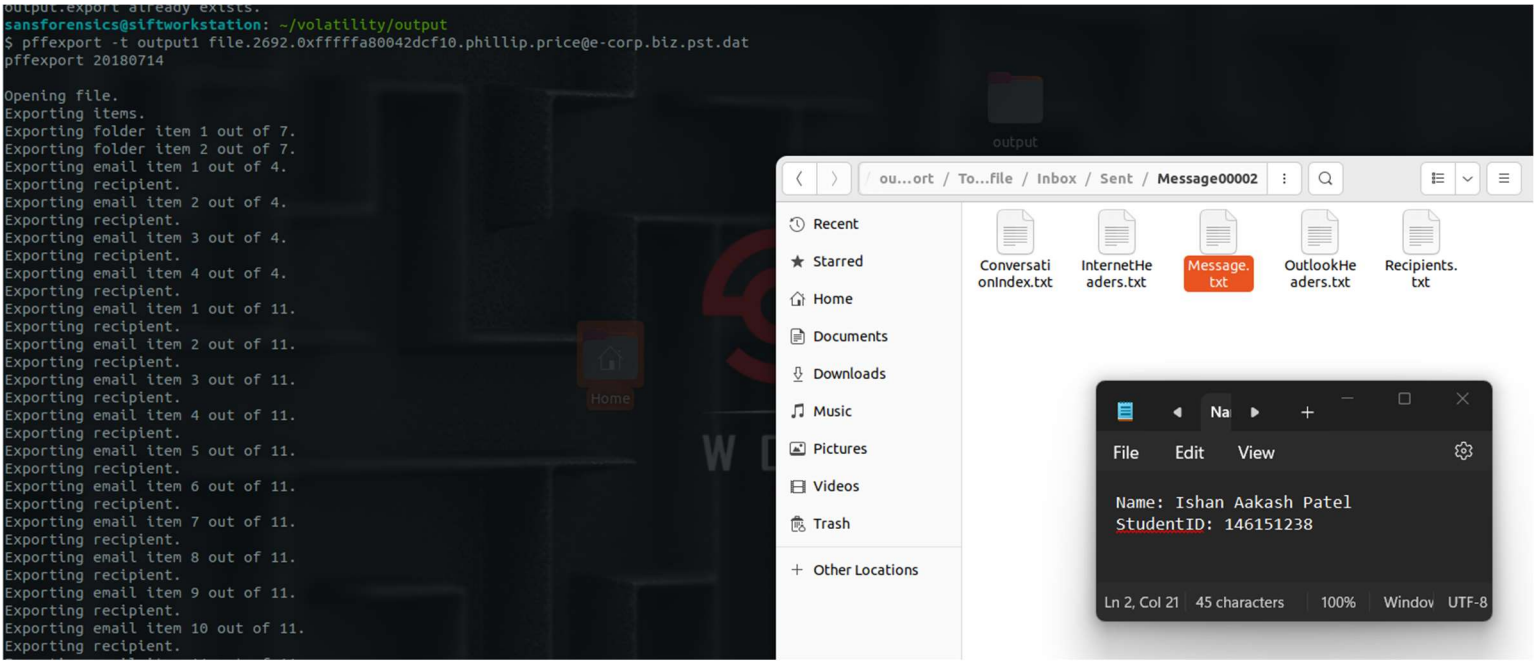
Command : find . -type f -exec pffexport -m all -f all "{}" \;

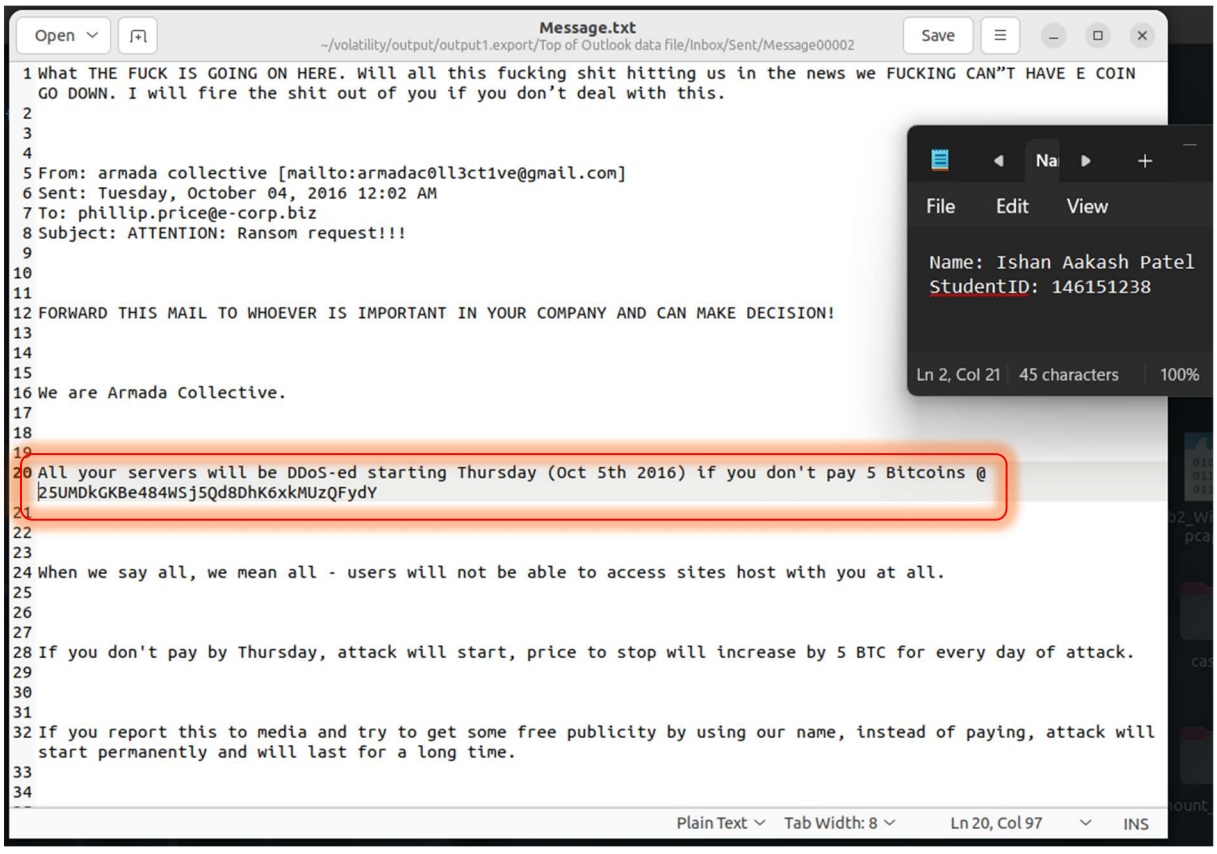
Got the file now check this into virustotal website



Answer : c2dbf24a0dc7276a71dd0824647535c9

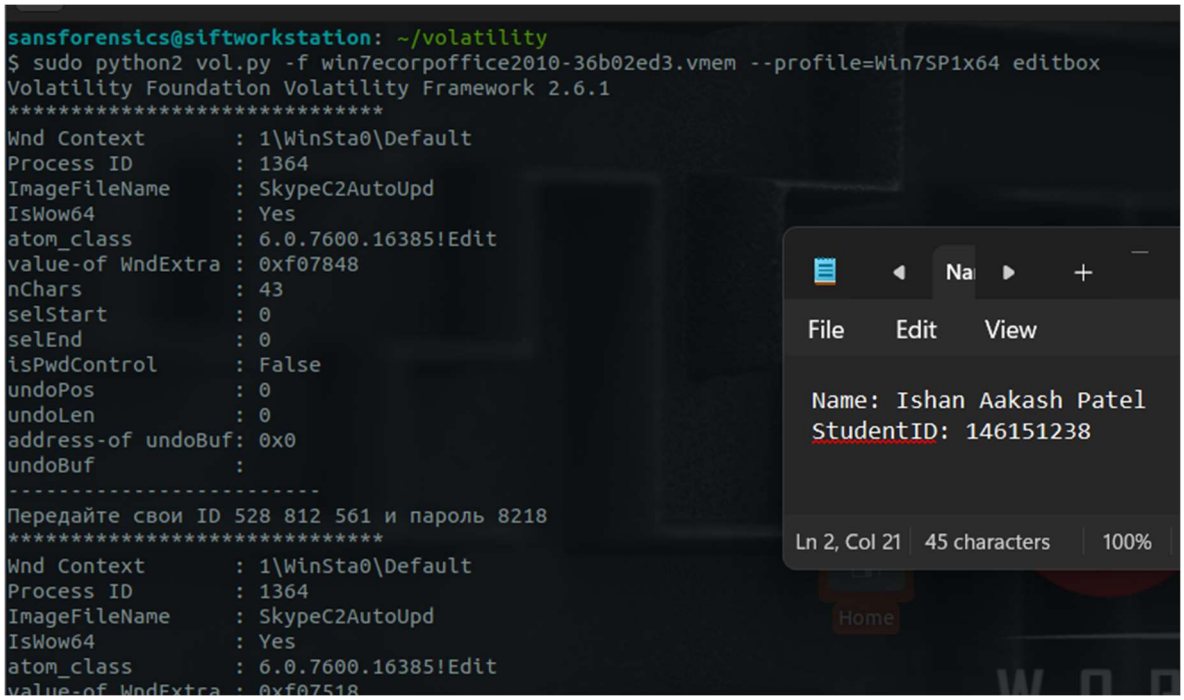
7) File->ecorpoffice: What is the bitcoin wallet address that ransomware was demanded?

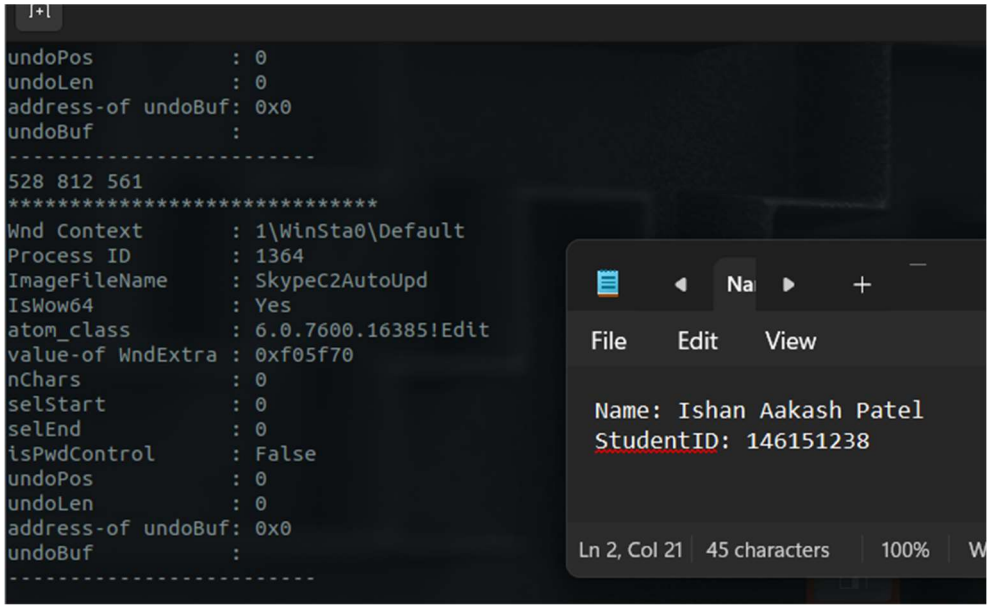




Answer : 25UMDkGKBe484WSj5Qd8DhK6xkMUzQFydY

8) File->ecorpoffice: What is the ID given to the system by the malicious file for remote access?

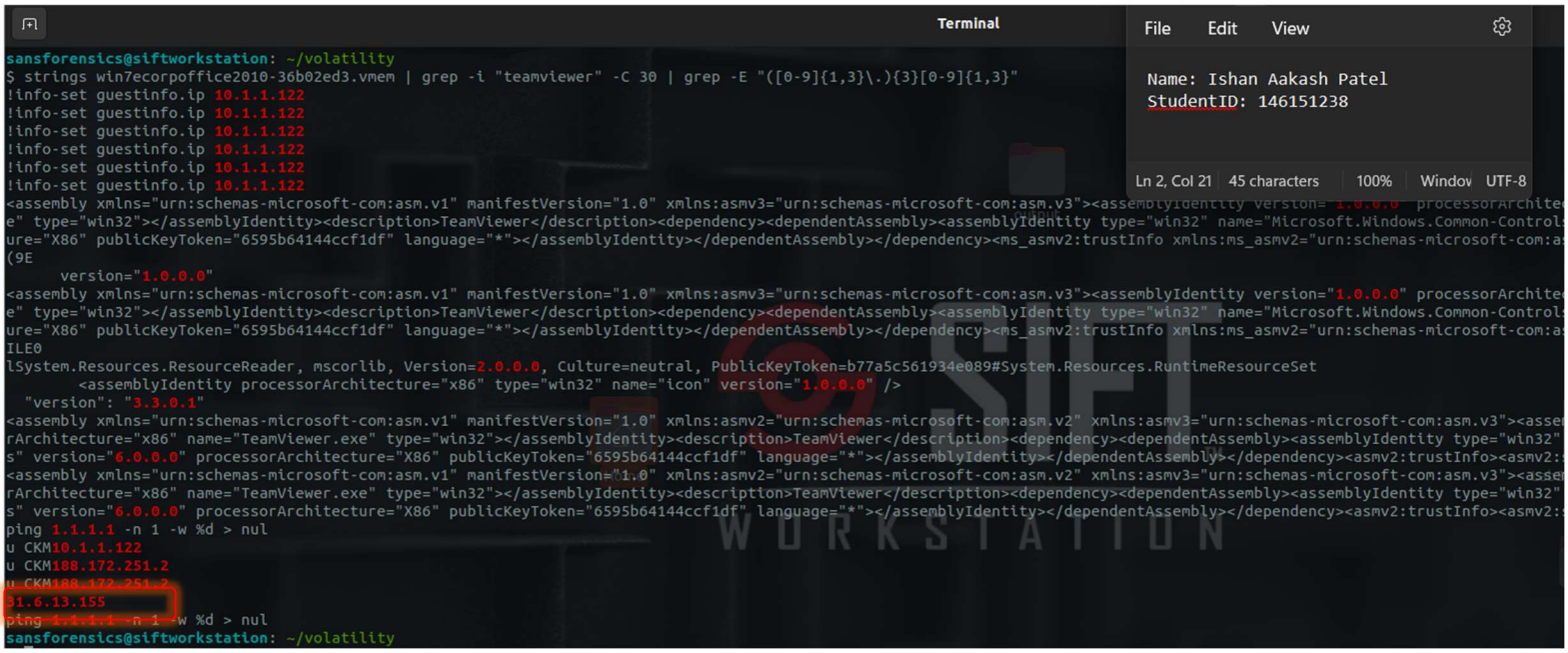




Command : sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem –profile=Win7SP1x64 editbox

Answer : 528 812 561.

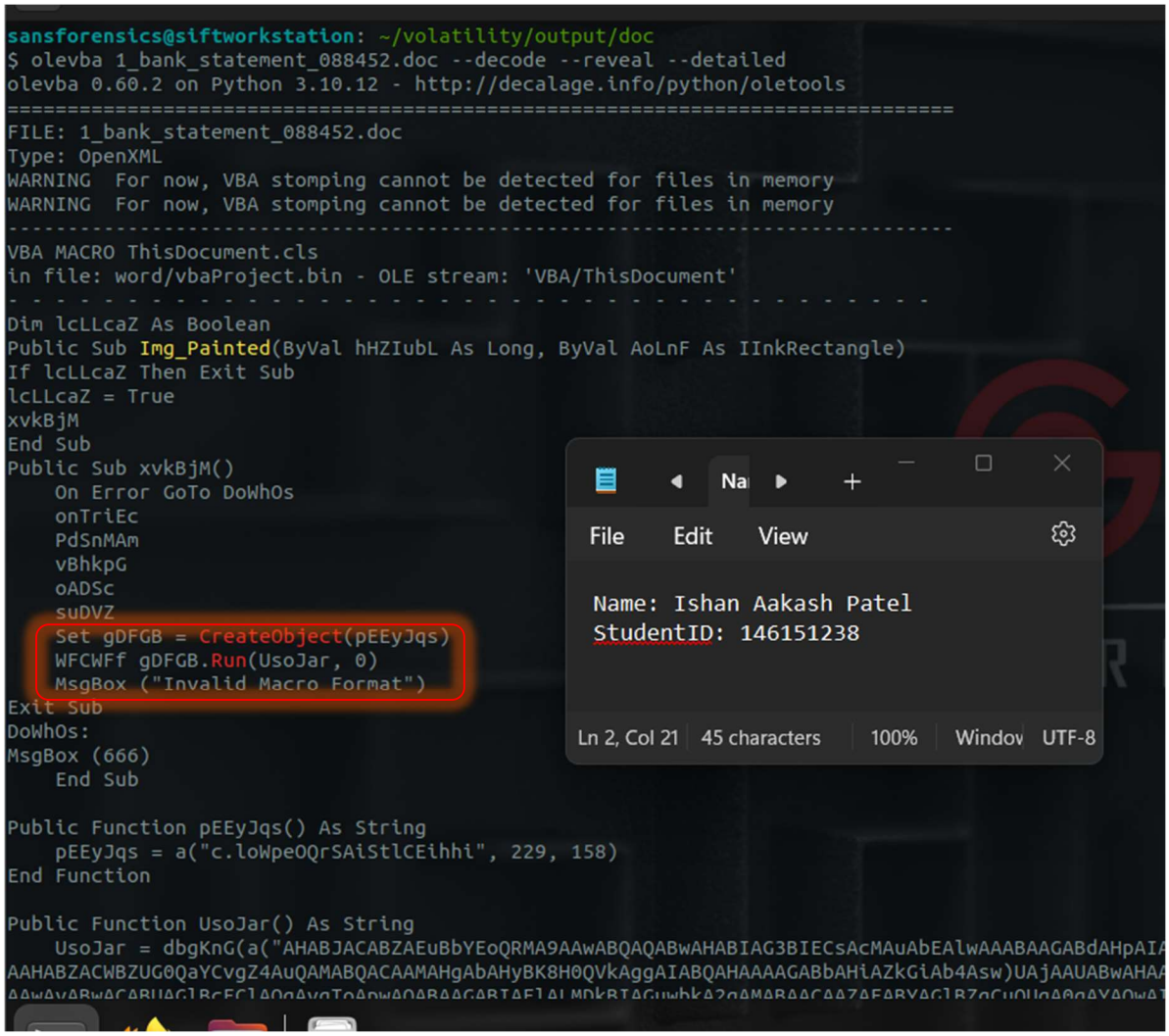
9) File->ecorpoffice: What is the IPv4 address the actor last connected to the system with the remote access tool?



Command : strings win7ecorpoffice2010-36b02ed3.vmem | grep -i “teamviewer” -C 30 | grep -E “([0–9]{1,3}[\.]){3}[0–9]{1,3}”

Answer : 31.6.13.155

10) File->ecorpoffice: What Public Function in the word document returns the full command string that is eventually run on the system?

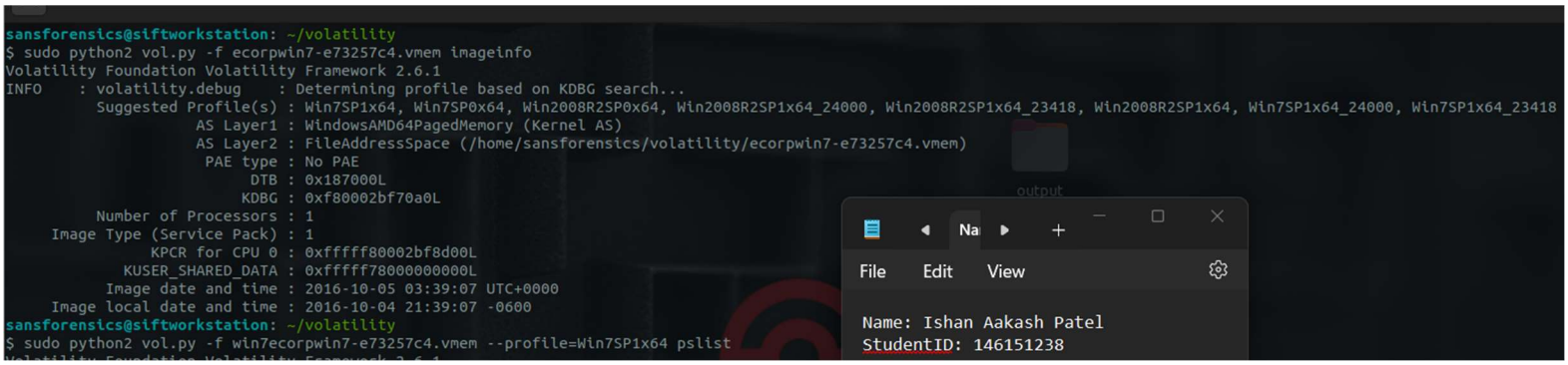


Command : olevba 1_bank_statement_088452.doc –decode –reveal –detailed

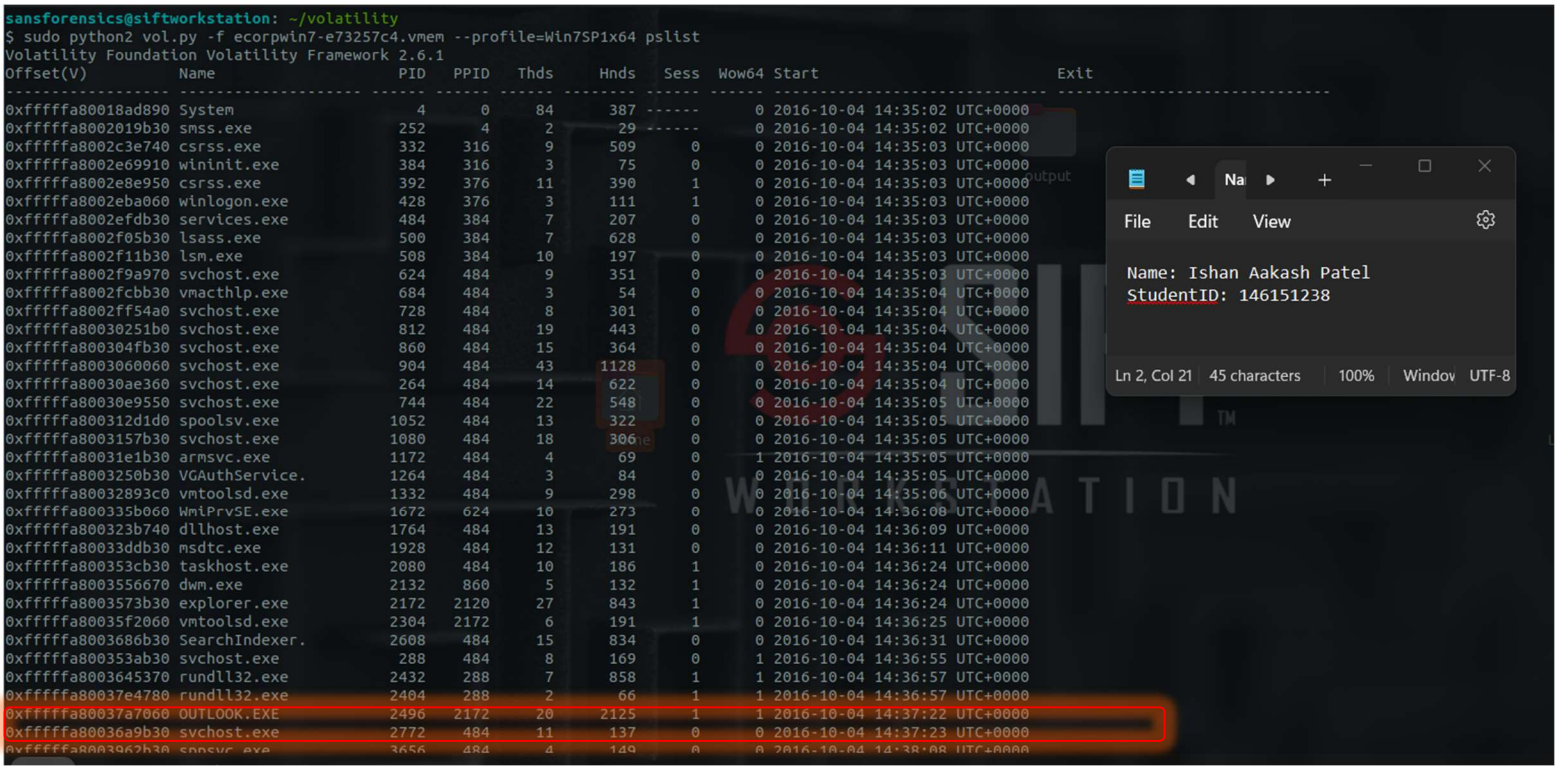
Opening the malware without actually opening it…

Answer : UsoJar

11) File->ecorpwin7: What is the MD5 hash of the malicious document?



Command : sudo python2 vol.py –f ecorpwin7-e73257c4.vmem imageinfo

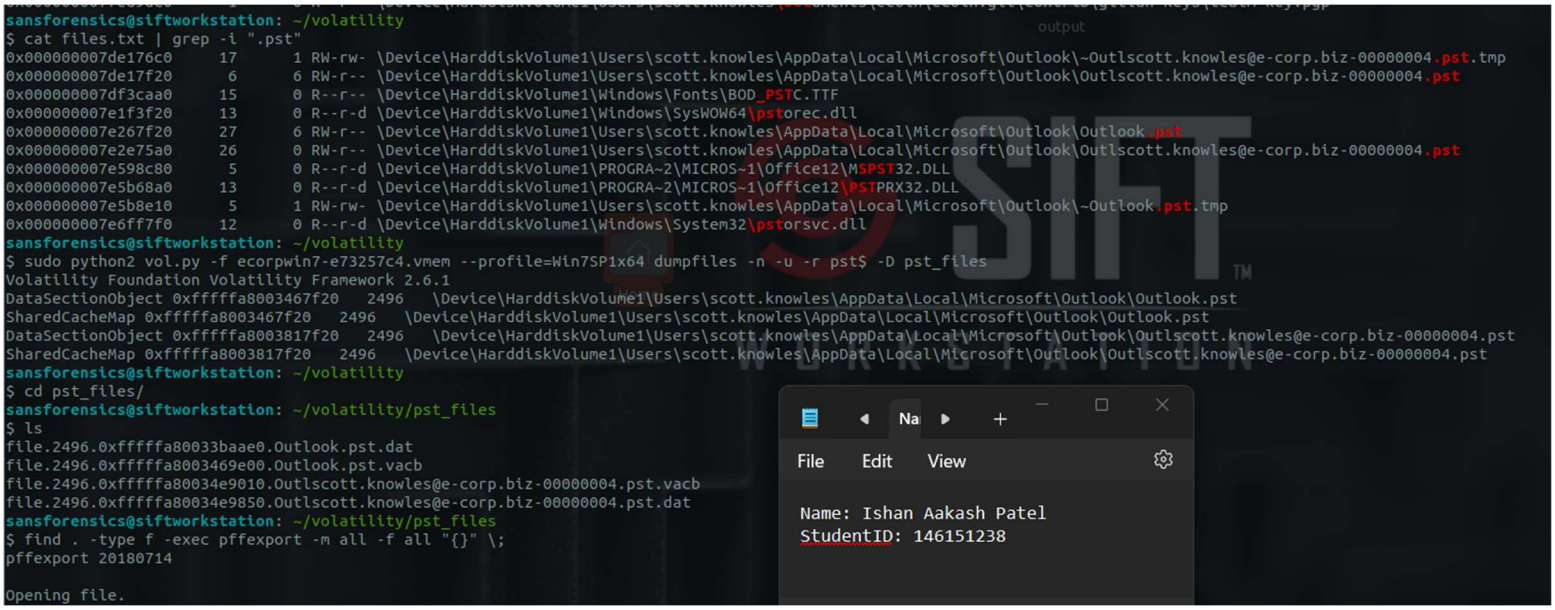


Command : sudo python2 vol.py –f ecorpwin7-e73257c4.vmem –profile=Win7SP1x64 pslist

Command : sudo python2 vol.py –f ecorpwin7-e73257c4.vmem –profile=Win7SP1x64 filescan > files.txt

Cat files.txt | grep -i “.doc”

This is to find any documents with .doc extension and .pst extension

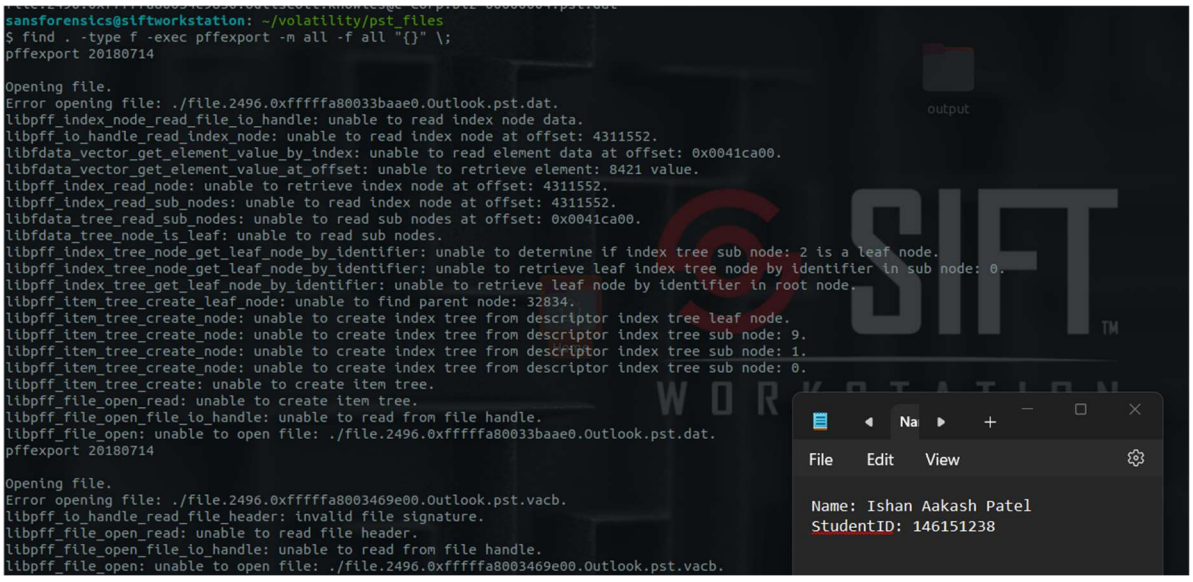


Dumping the .pst files and then exporting them using pffexport tool…

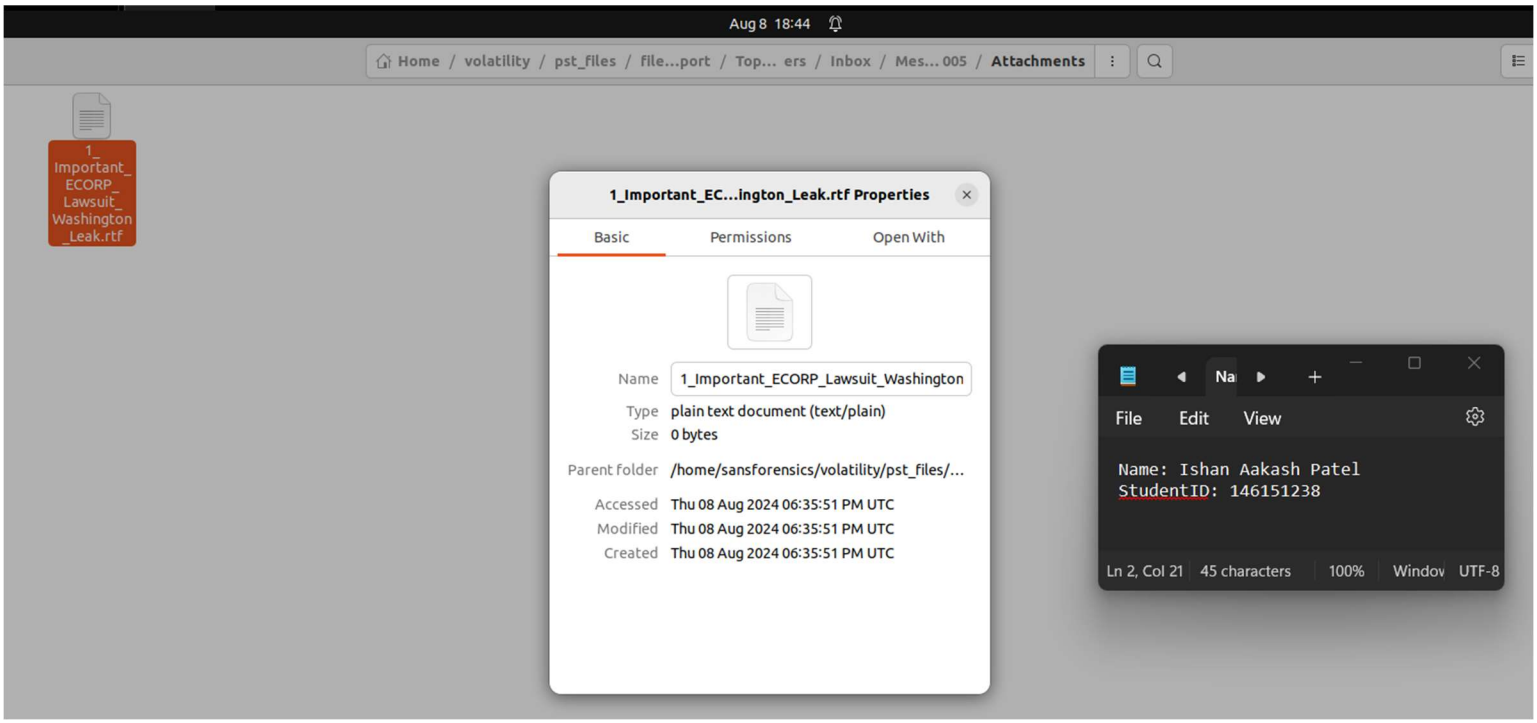
Command : cat files.txt | grep -I “.pst”

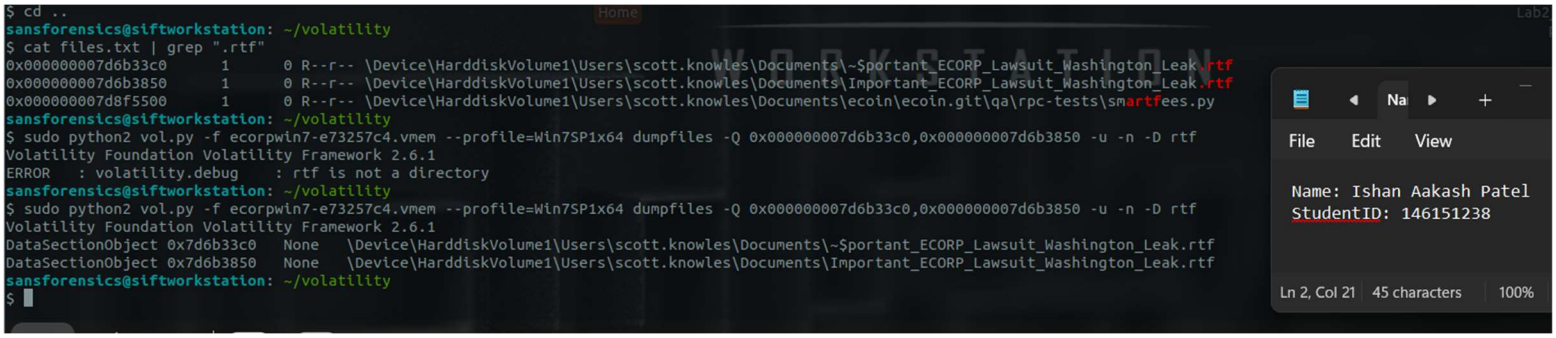
sudo python2 vol.py –f ecorpwin7-e73257c4.vmem –profile=Win7SP1x64 dumpfiles -n -u -r pst$ -D pst_files

find . -type f -exec pffexport -m all -f all “{}” \;

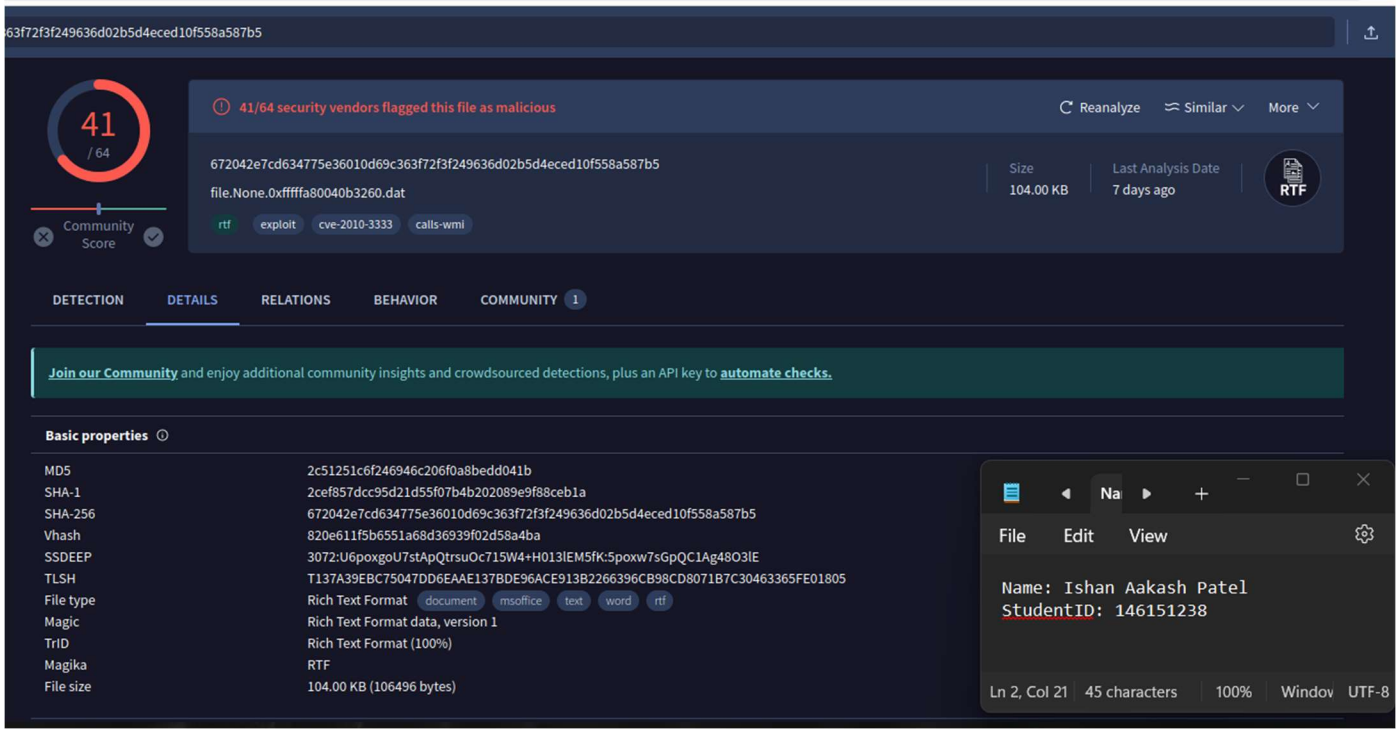


Searching through .pst files in one of the email, I found a attachment of .rst extension.





Checking the files in virustotal

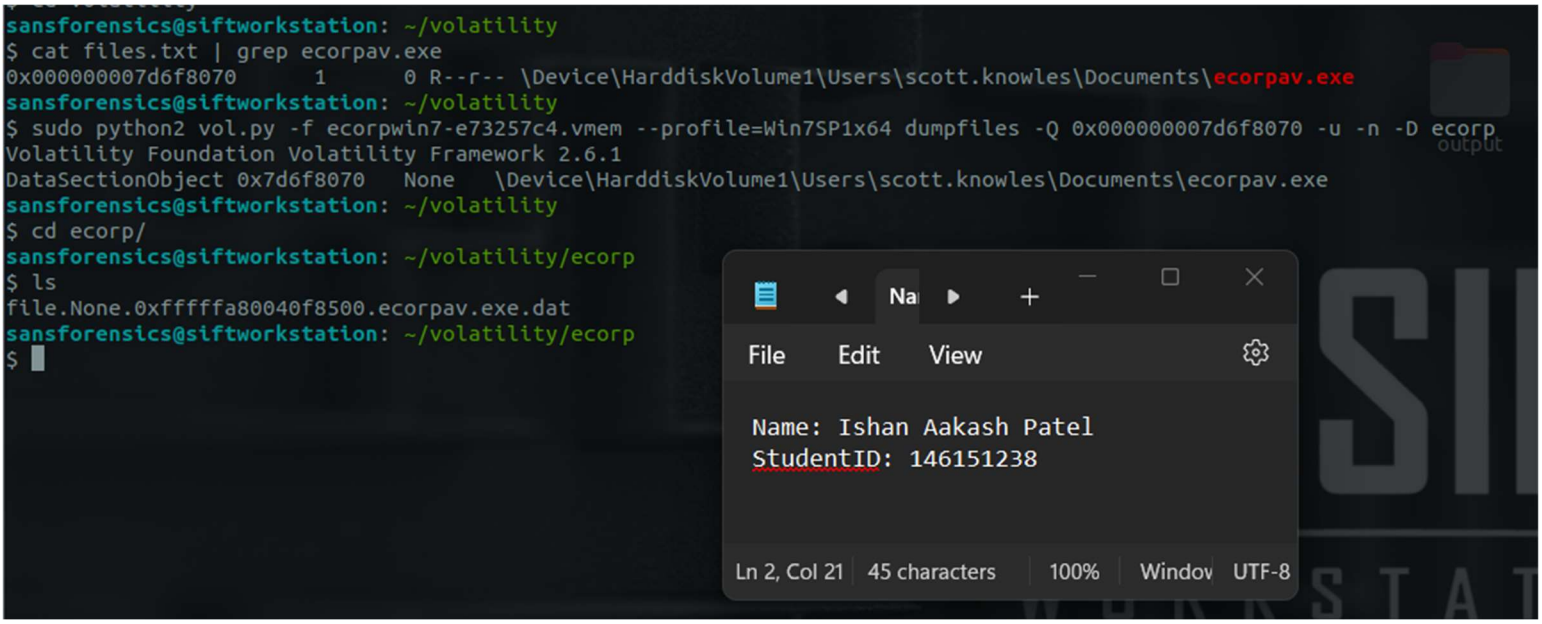


Still this hash wasn't correct (this was the correct file though), removed few bits from the file then got the hash…

Answer : 00e4136876bf4c1069ab9c4fe40ed56f

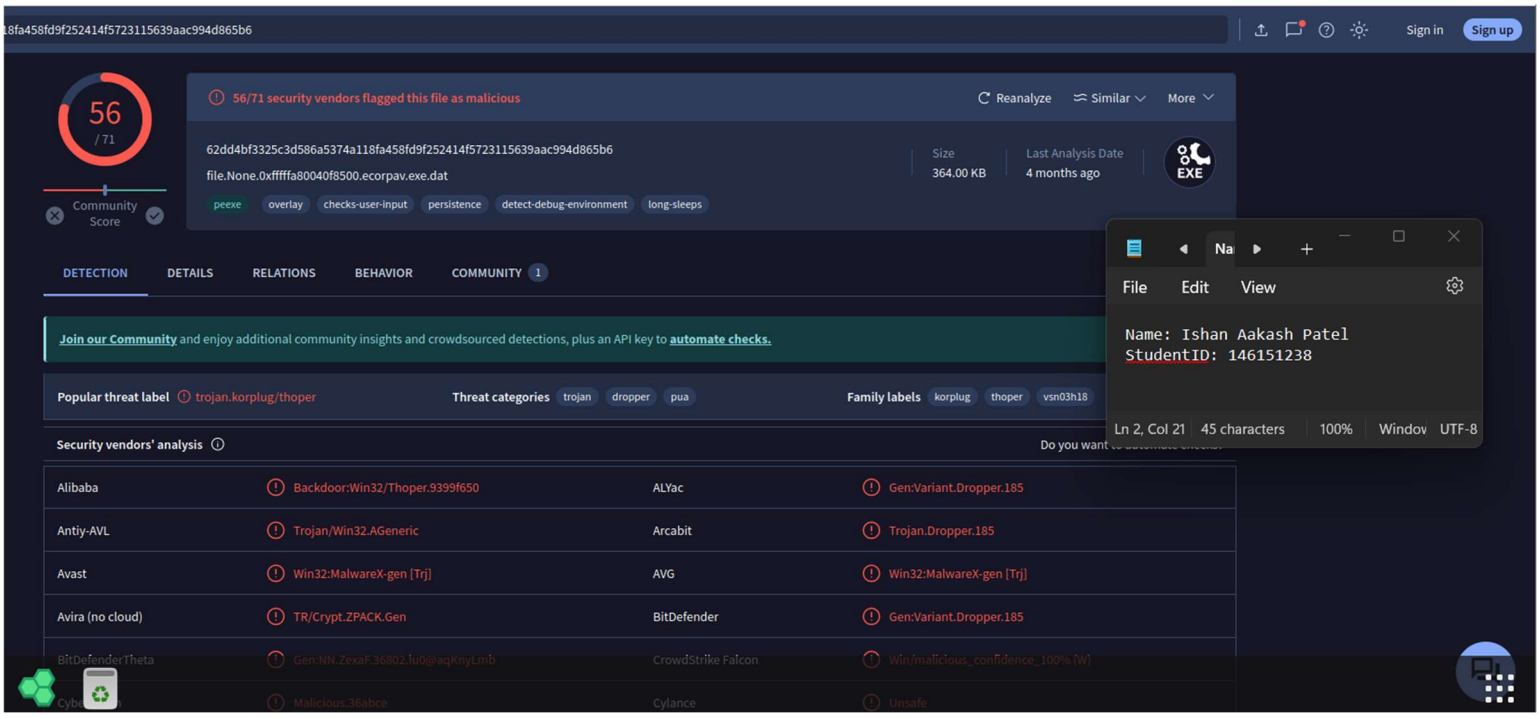
12) File->ecorpwin7: What is the common name of the malicious file that gets loaded?"

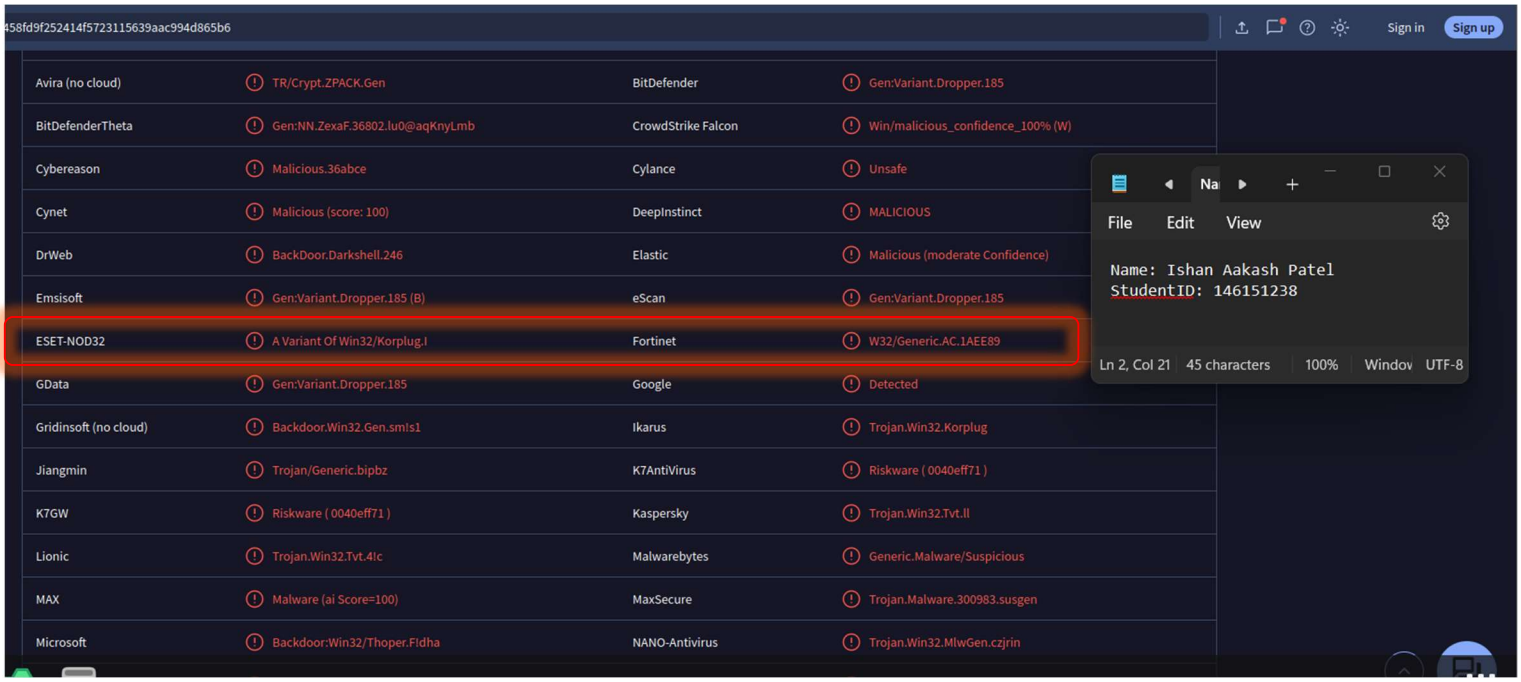
This was very difficult question for me and I could do only half…



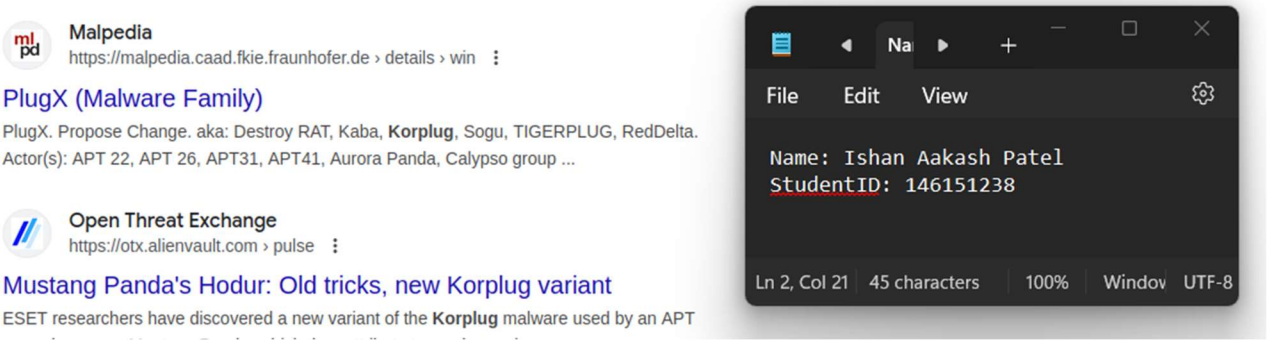
Command : sudo python2 vol.py –f ecorpwin7-e73257c4.vmem –profile=Win7SP1x64 dumpfiles -Q 0x000000007df8070 -u -n -D ecorp

Putting the file in virustotal



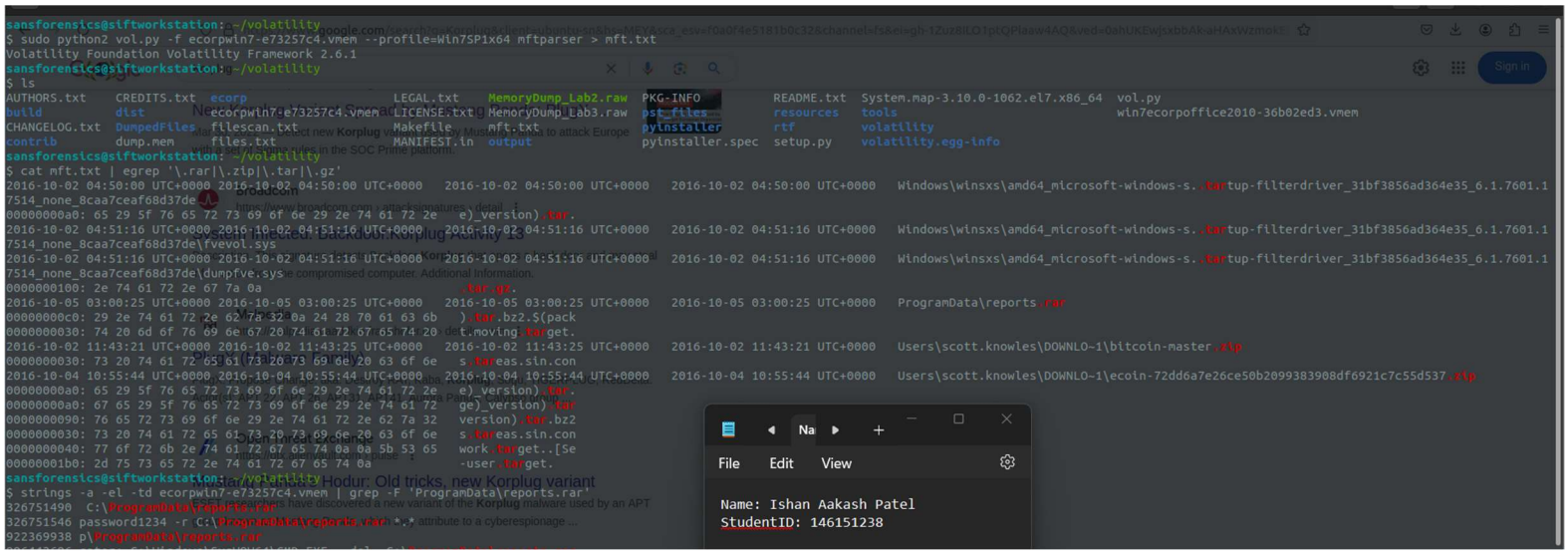


Still this was not the answer, so searched for its alternative on google and found it..



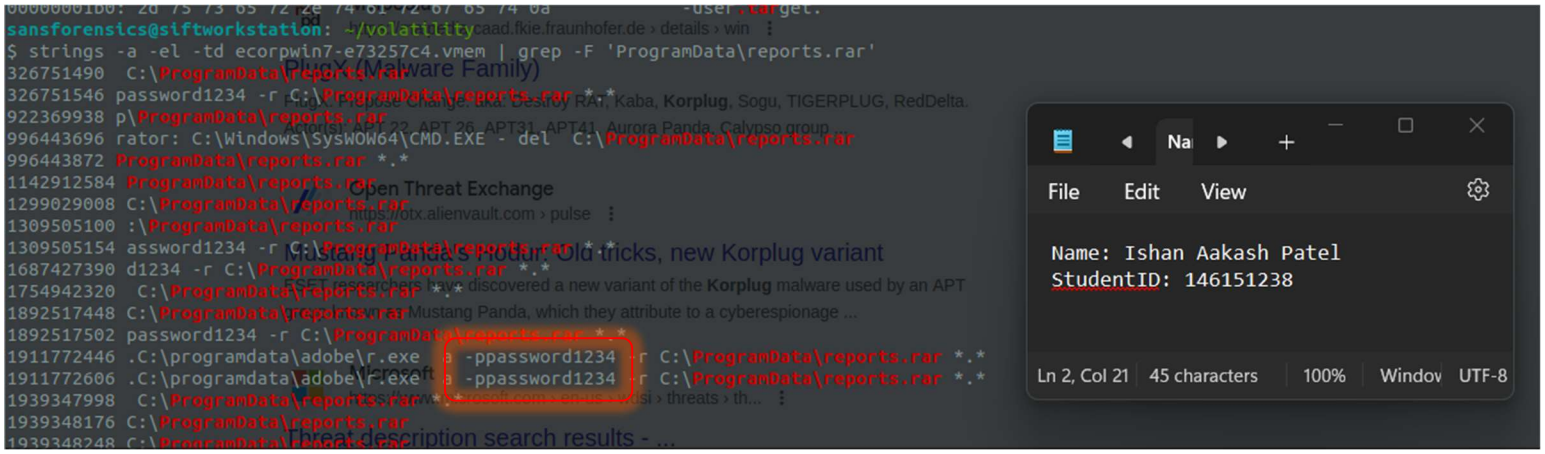
Answer : PlugX

13) File->ecorpwin7: What password does the attacker use to stage the compressed file for exfil?



Command : sudo python2 vol.py –f ecorpwin7-e73257c4.vmem –profile=Win7SP1x64 mftparser > mft.txt

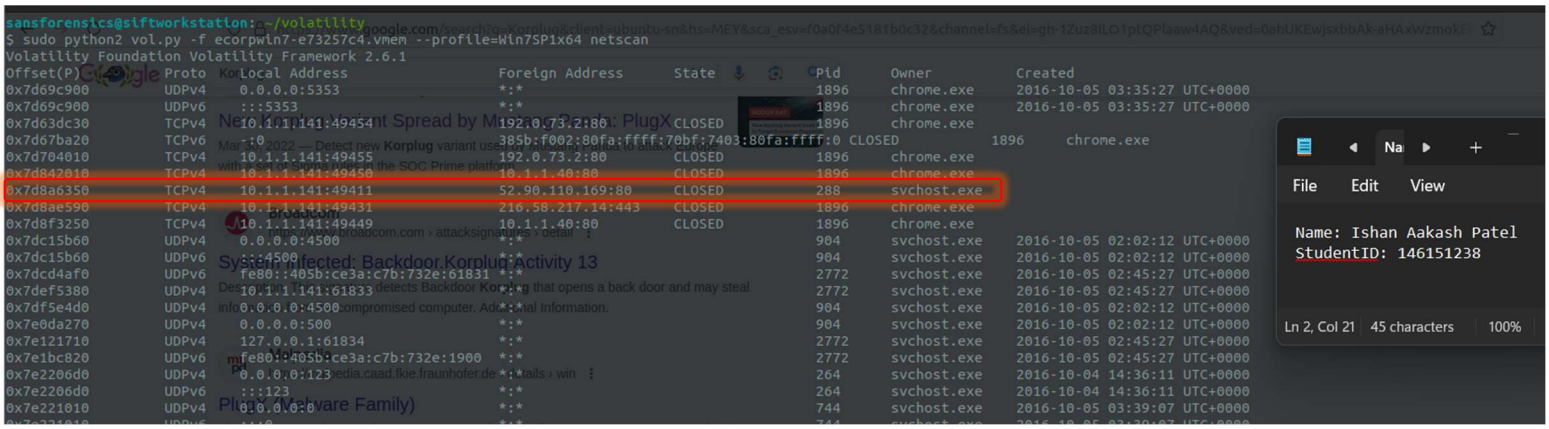
Cat mft.txt | grep '\.rar|\.zlp|\.tar|\.gz'



Command : strings -a -el -td ecorpwin7- e73257c4.vmem | grep -F 'ProgramData\reports.rar'

Answer : password1234

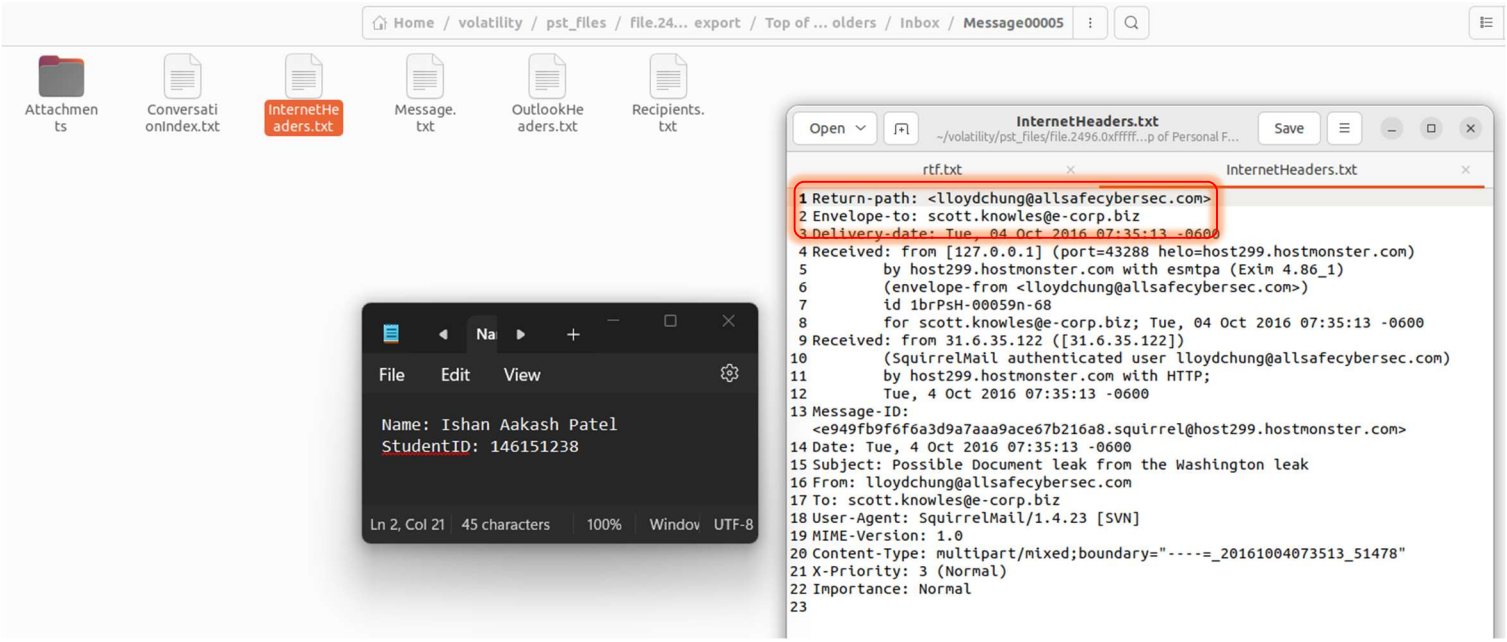
14) File->ecorpwin7: What is the IP address of the c2 server for the malicious file?



Command : sudo python2 vol.py –f ecorpwin7-e73257c4.vmem –profile=Win7SP1x64 netscan

Answer : 52.90.110.169

15) File->ecorpwin7: What is the email address that sent the phishing email?



Just was looking through exported files and found this…

Answer : lloydchung@allsafecybersec.com

Learning Experience

This challenge on TeamSpy endpoint forensics was indeed an extremely demanding and complex task. It pushed me to apply a wide range of digital forensics tools and techniques, from memory dump analysis with Volatility to examining suspicious documents and network traffic. The multi-faceted nature of the investigation, involving malware analysis, email forensics, and piecing together the attacker's actions across different systems, made it particularly challenging. While difficult, this lab provided invaluable hands-on experience in real-world incident response scenarios and significantly enhanced my skills in digital forensics and malware analysis. The complexity of the challenge underscored the importance of persistence, attention to detail, and a methodical approach when conducting cybersecurity investigations.