Maria Valencia

CSC 154

Lab 11

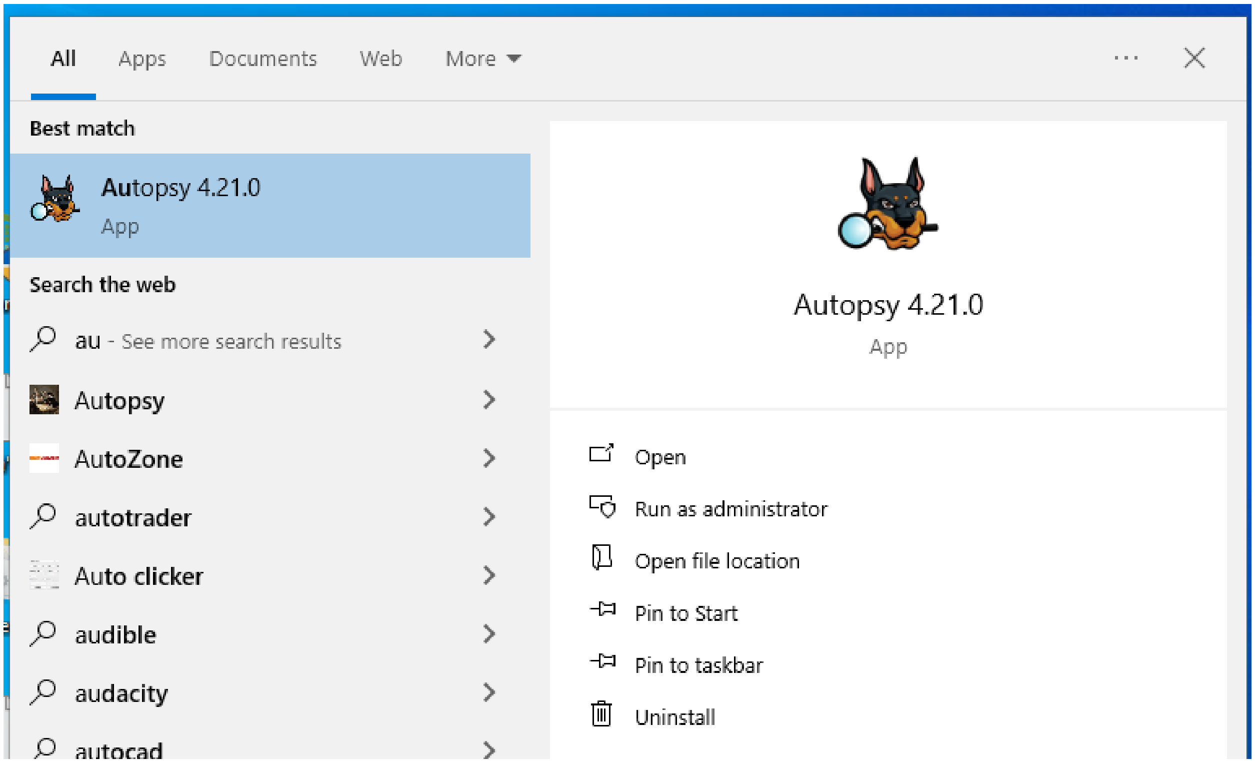
Lab 11: Forensics and Malware Analysis

Exercise 11.1 Forensic Investigation

In this task, I will complete various tasks against an acquired USB image from EnCase using Autopsy on my Windows VM in Bridge Adapter network mode.

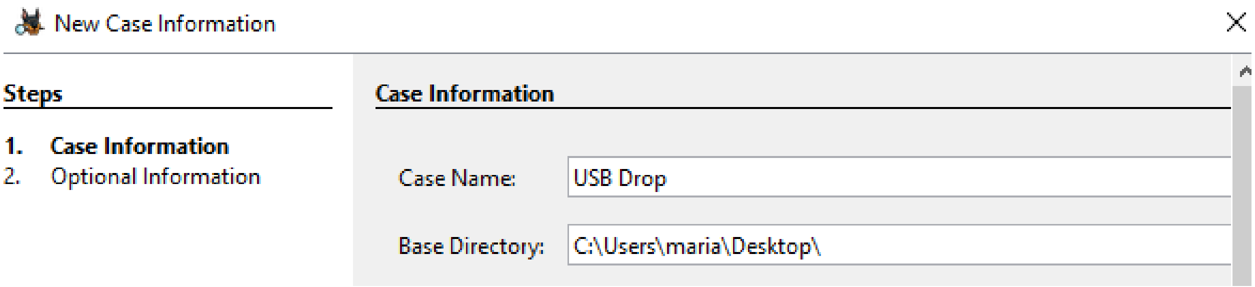
Step 1: Install Autopsy

I already have Autopsy installed.



Step 2: Case Setup

With Autopsy installed, run the application from the Desktop shortcut and Create a New Case. Name the case "USB Drop", set the Base Directory in a folder on your Desktop, and assign a case number.



New Case Information

Steps

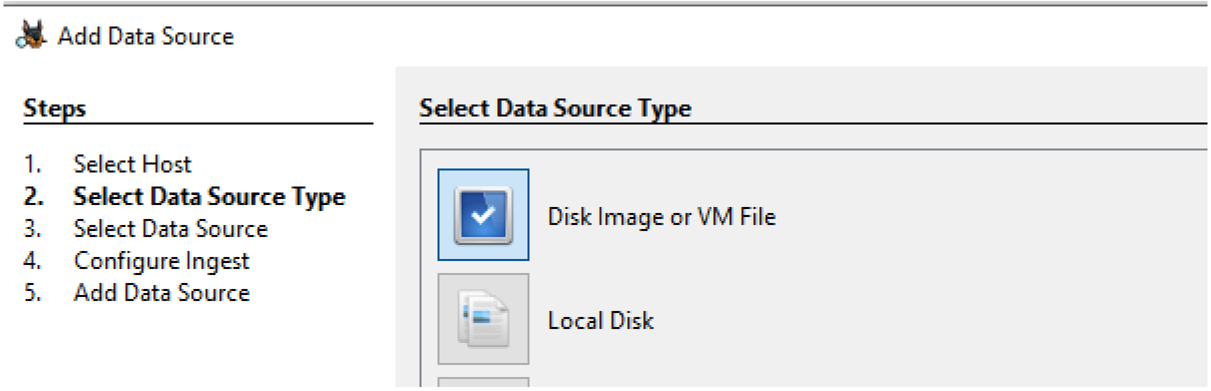
1. **Case Information**
2. Optional Information

Case Information

Case Name: USB Drop

Base Directory: C:\Users\maria\Desktop\

Save the forensics.E01 file to your Windows VM and Add Data Source as a "Disk Image or VM File". Select the forensics.E01 as the Data Source path and select all Ingest Modules. Once added wait a couple minutes for the analysis to complete by observing the status bar in the bottom right corner of Autopsy.

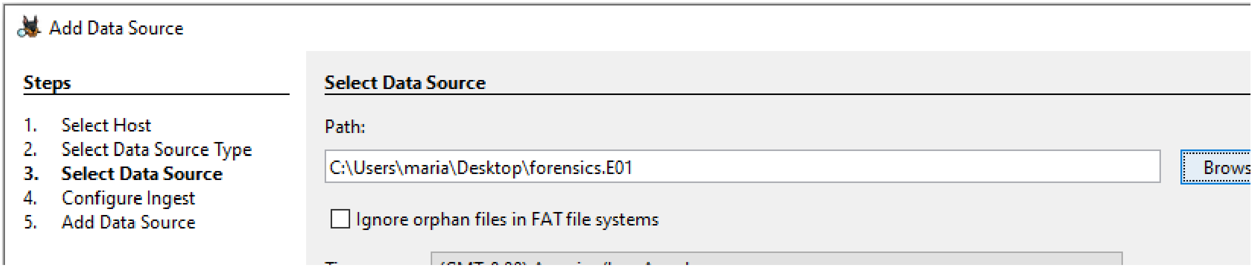


Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

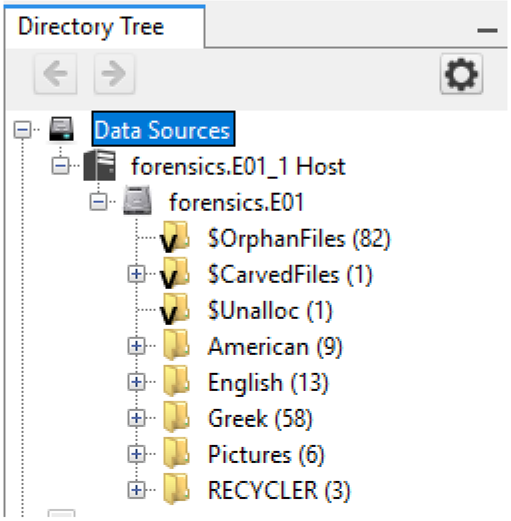
Select Data Source

Path:

C:\Users\maria\Desktop\forensics.E01

□ Ignore orphan files in FAT file systems

Once the ingest modules have been fully analyzed, expand the Directory Tree's Data Sources hierarchy and confirm the drives folders are displayed (eg "American", "Pictures", and other folders)

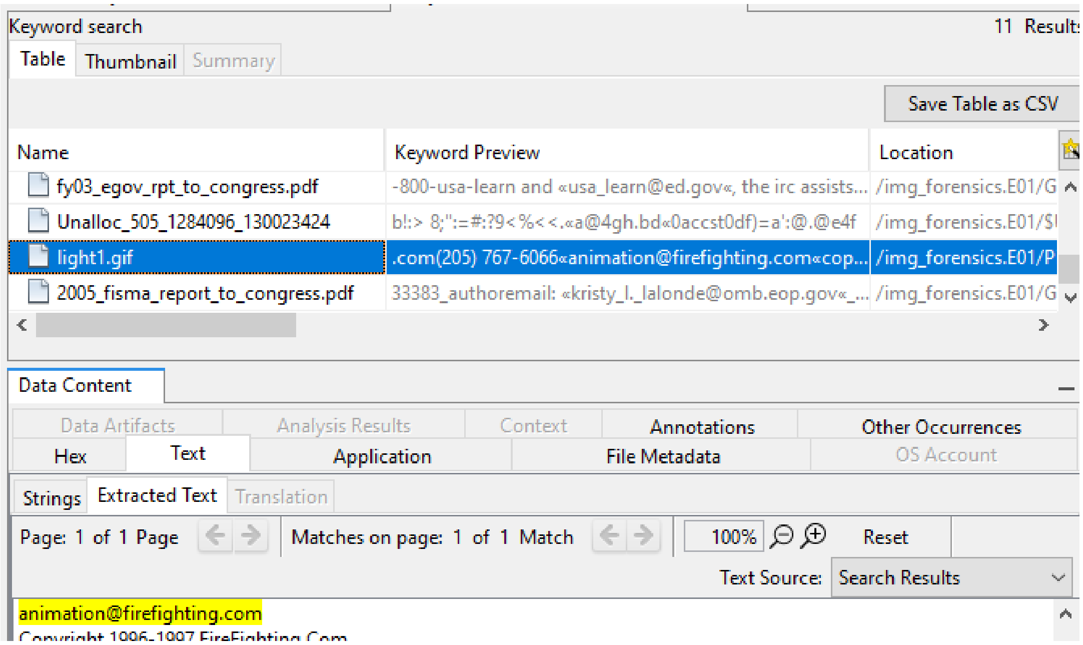


Step 3: Analyze USB

Analyze the data source by finding the following evidence using the search features (upper right corner) and the tree pane module results. Make sure to provide a screenshot and description of HOW and WHERE you found the evidence.

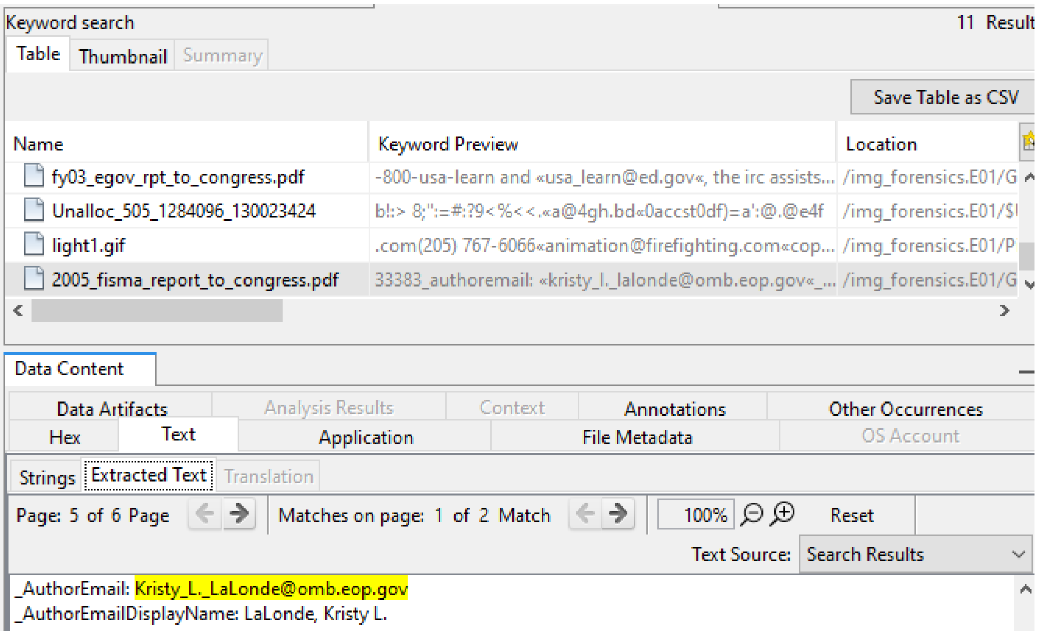
2 Email Addresses

- I found these by using the "Keyword Lists" on the top right of Autopspy and selecting Email Addresses. Then I searched through the file and looked for emails in the Text tab of each content.



Name	Keyword Preview	Location
fy03_egov_rpt_to_congress.pdf	-800-usa-learn and «usa_learn@ed.gov«, the irc assists...	/img_forensics.E01/G
Unalloc_505_1284096_130023424	b!:> 8;":=#:?9<%<<.«a@4gh.bd«0accst0df)=a':@.@e4f	/img_forensics.E01/$
light1.gif	.com(205) 767-6066«animation@firefighting.com«cop...	/img_forensics.E01/P
2005_fisma_report_to_congress.pdf	33383_authoremail: «kristy_l._lalonde@omb.eop.gov«_...	/img_forensics.E01/G

animation@firefighting.com
Copyright 1996-1997 FireFighting.Com

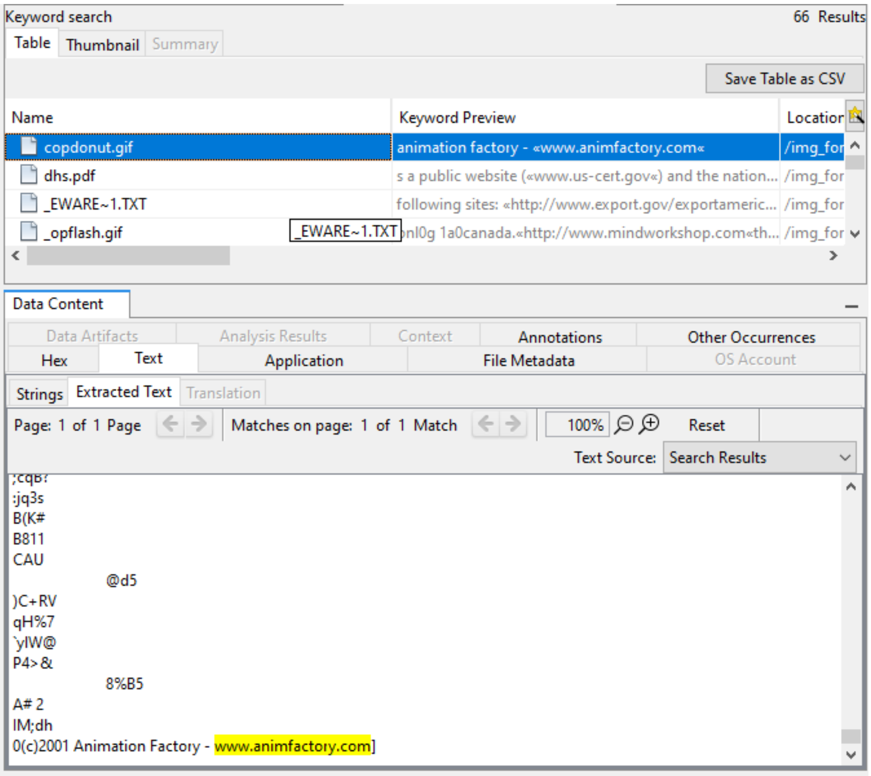


Name	Keyword Preview	Location
fy03_egov_rpt_to_congress.pdf	-800-usa-learn and «usa_learn@ed.gov«, the irc assists...	/img_forensics.E01/G
Unalloc_505_1284096_130023424	b!:> 8;":=#:?9<%<<.«a@4gh.bd«0accst0df)=a':@.@e4f	/img_forensics.E01/$U
light1.gif	.com(205) 767-6066«animation@firefighting.com«cop...	/img_forensics.E01/P
2005_fisma_report_to_congress.pdf	33383_authoremail: «kristy_l._lalonde@omb.eop.gov«_...	/img_forensics.E01/G

```
_AuthorEmail: Kristy_L._LaLonde@omb.eop.gov
_AuthorEmailDisplayName: LaLonde, Kristy L.
```

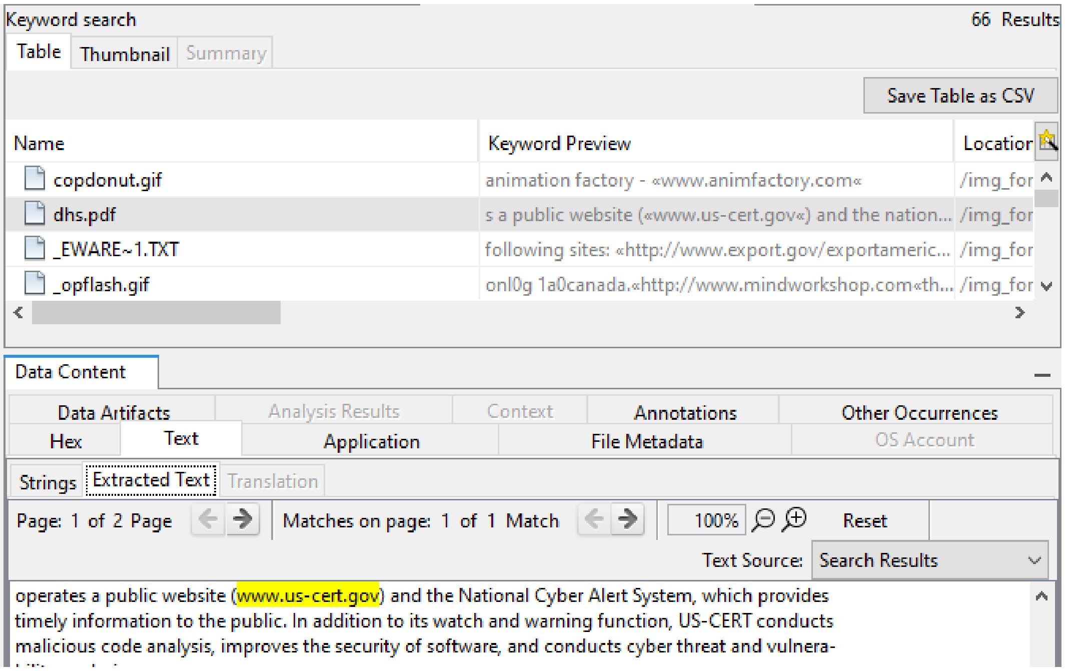
2 URLs

- I found these by using the "Keyword Lists" on the top right of Autopspy and selecting URLs. Then I searched through the file and looked for URLs in the Text tab of each content.



Name	Keyword Preview	Locatior
copdonut.gif	animation factory - «www.animfactory.com«	/img_for
dhs.pdf	s a public website («www.us-cert.gov«) and the nation...	/img_for
_EWARE~1.TXT	following sites: «http://www.export.gov/exportameric...	/img_for
_opflash.gif	nl0g 1a0canada.«http://www.mindworkshop.com«th...	/img_for

```
;cqB?
:jq3s
B(K#
B811
CAU
              @d5
)C+RV
qH%7
`yIW@
P4>&
              8%B5
A# 2
IM;dh
0(c)2001 Animation Factory - www.animfactory.com]
```

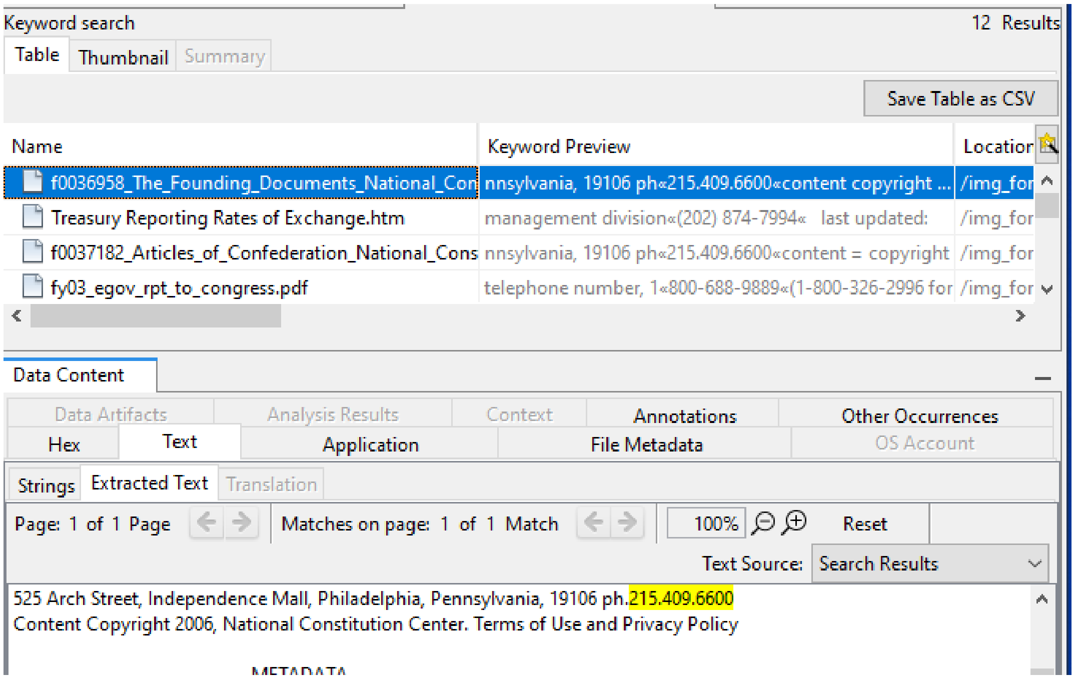


Name	Keyword Preview	Locatior
copdonut.gif	animation factory - «www.animfactory.com«	/img_for
dhs.pdf	s a public website («www.us-cert.gov«) and the nation...	/img_for
_EWARE~1.TXT	following sites: «http://www.export.gov/exportameric...	/img_for
_opflash.gif	onl0g 1a0canada.«http://www.mindworkshop.com«th...	/img_for

operates a public website (www.us-cert.gov) and the National Cyber Alert System, which provides
timely information to the public. In addition to its watch and warning function, US-CERT conducts
malicious code analysis, improves the security of software, and conducts cyber threat and vulnera-

2 Phone Numbers

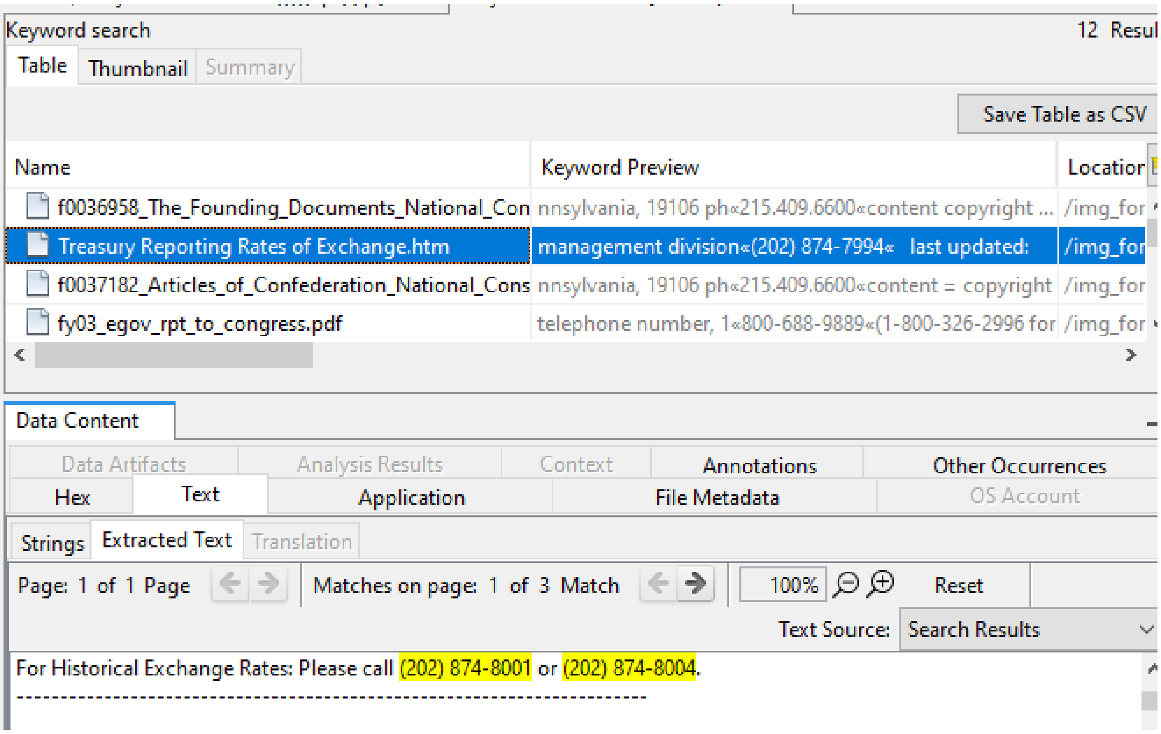
- I found these by using the “Keyword Lists” on the top right of Autopspy and selecting Phone Numbers. Then I searched through the file and looked for phone numbers in the Text tab of each content.



Name	Keyword Preview	Locatior
f0036958_The_Founding_Documents_National_Con	nnsylvania, 19106 ph«215.409.6600«content copyright ...	/img_for
Treasury Reporting Rates of Exchange.htm	management division«(202) 874-7994« last updated:	/img_for
f0037182_Articles_of_Confederation_National_Cons	nnsylvania, 19106 ph«215.409.6600«content = copyright	/img_for
fy03_egov_rpt_to_congress.pdf	telephone number, 1«800-688-9889«(1-800-326-2996 for	/img_for

525 Arch Street, Independence Mall, Philadelphia, Pennsylvania, 19106 ph.215.409.6600
Content Copyright 2006, National Constitution Center. Terms of Use and Privacy Policy

METADATA



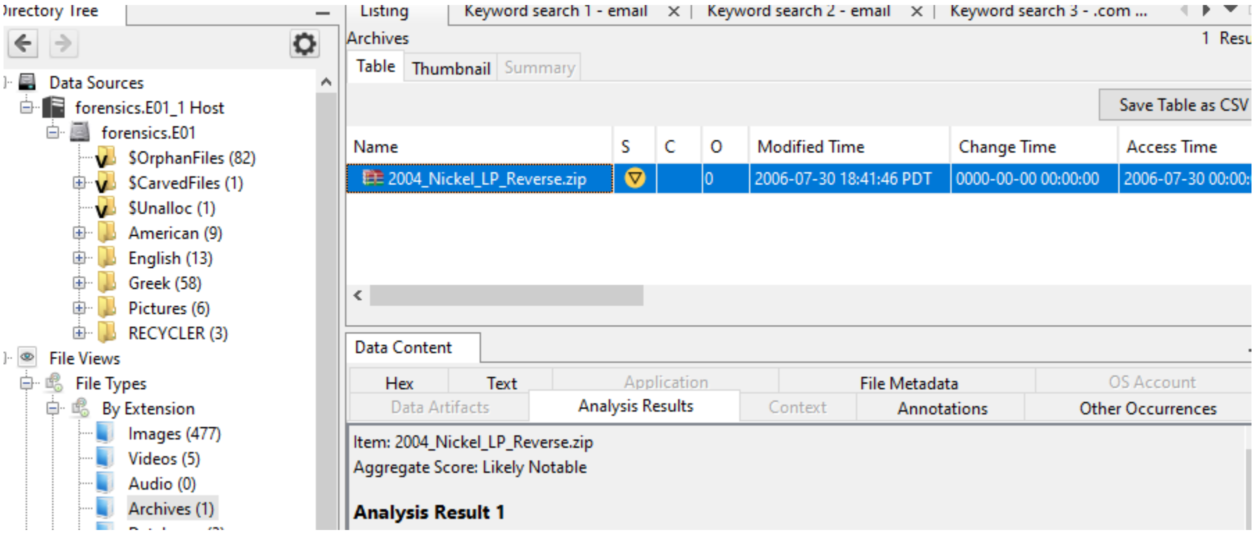
Name	Keyword Preview	Locatior
f0036958_The_Founding_Documents_National_Con	nnsylvania, 19106 ph«215.409.6600«content copyright ...	/img_for
Treasury Reporting Rates of Exchange.htm	management division«(202) 874-7994« last updated:	/img_for
f0037182_Articles_of_Confederation_National_Cons	nnsylvania, 19106 ph«215.409.6600«content = copyright	/img_for
fy03_egov_rpt_to_congress.pdf	telephone number, 1«800-688-9889«(1-800-326-2996 for	/img_for

For Historical Exchange Rates: Please call (202) 874-8001 or (202) 874-8004.

----

1 Zip File

- I clicked on File views ->File types->By Extension-> Archives in the directory tree and found a zip file.



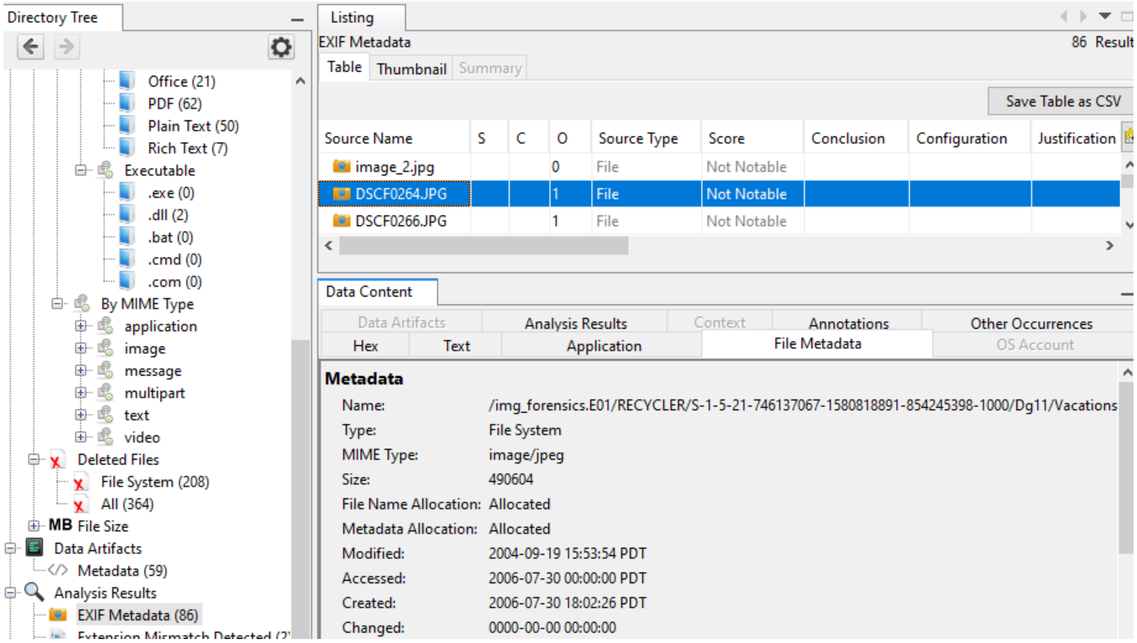
Name	S	C	O	Modified Time	Change Time	Access Time
2004_Nickel_LP_Reverse.zip	▽		0	2006-07-30 18:41:46 PDT	0000-00-00 00:00:00	2006-07-30 00:00:

Item: 2004_Nickel_LP_Reverse.zip
Aggregate Score: Likely Notable

Analysis Result 1

1 JPG Metadata

- I went to Analysis Results -> EXIF metadata -. clicked a jpg and then clicked the file metadata of the content.



EXIF Metadata 86 Result

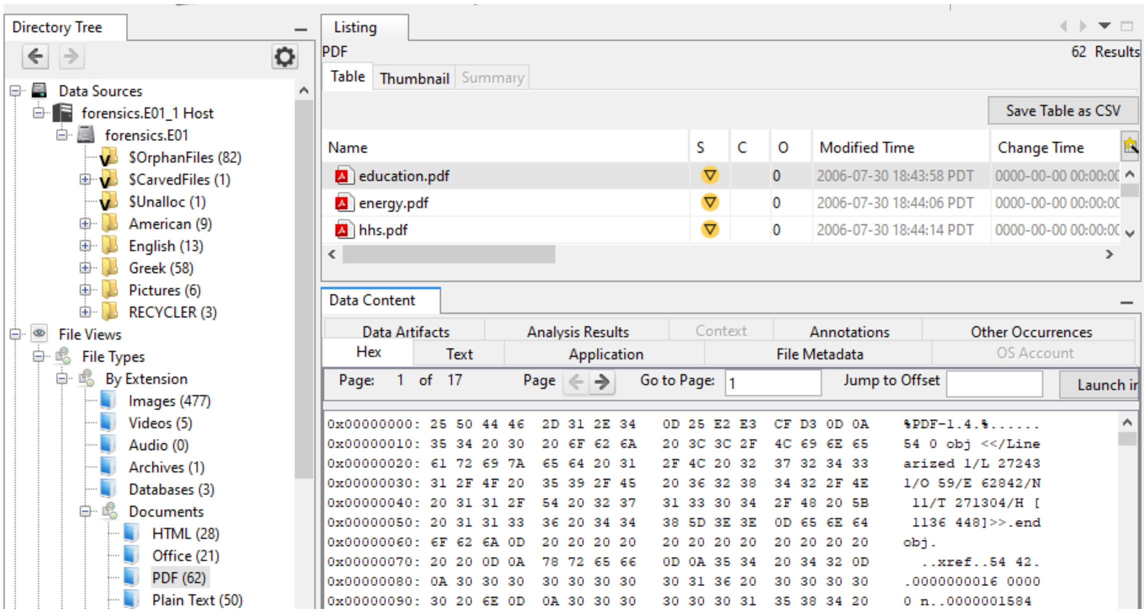
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification
image_2.jpg			0	File	Not Notable			
DSCF0264.JPG			1	File	Not Notable			
DSCF0266.JPG			1	File	Not Notable			

Metadata

Name:	/img_forensics.E01/RECYCLER/S-1-5-21-746137067-1580818891-854245398-1000/Dg11/Vacations
Type:	File System
MIME Type:	image/jpeg
Size:	490604
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2004-09-19 15:53:54 PDT
Accessed:	2006-07-30 00:00:00 PDT
Created:	2006-07-30 18:02:26 PDT
Changed:	0000-00-00 00:00:00

1 PDF Magic Byte Hex Code

- I went to file views-> file types -> Documents -> PDF in the directory pane and clicked a pdf and clicked the hex tab to see the Magic Byte Hex Code.



PDF 62 Results

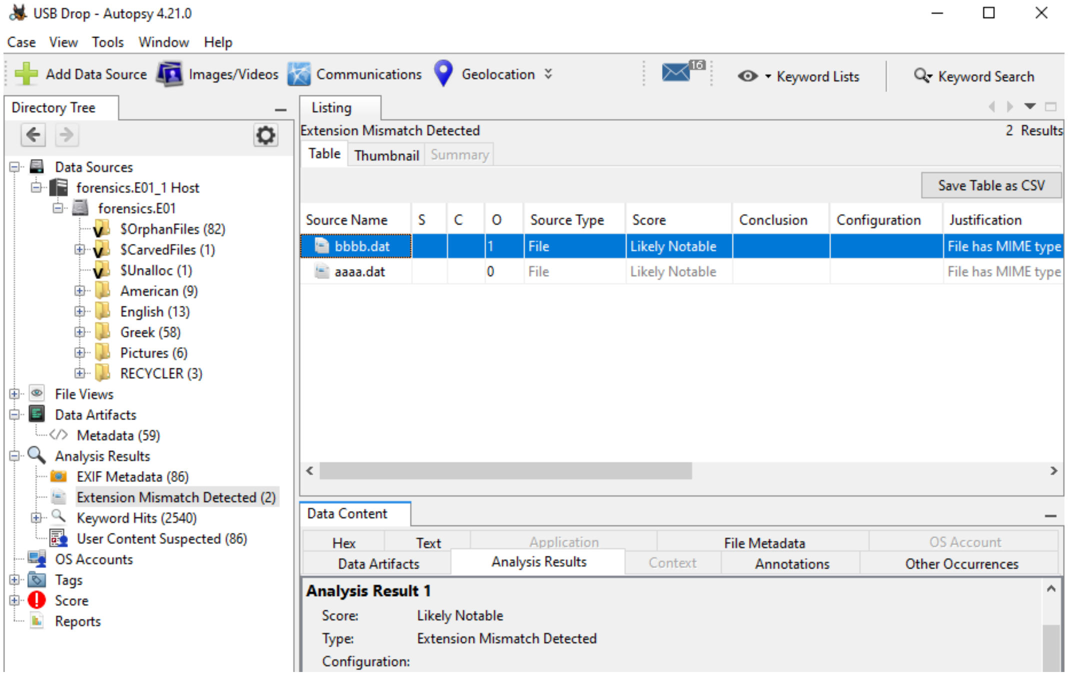
Name	S	C	O	Modified Time	Change Time
education.pdf			0	2006-07-30 18:43:58 PDT	0000-00-00 00:00:0C
energy.pdf			0	2006-07-30 18:44:06 PDT	0000-00-00 00:00:0C
hhs.pdf			0	2006-07-30 18:44:14 PDT	0000-00-00 00:00:0C

Page: 1 of 17 Go to Page: 1

```
0x00000000: 25 50 44 46  2D 31 2E 34   0D 25 E2 E3  CF D3 0D 0A    %PDF-1.4.%......
0x00000010: 35 34 20 30  20 6F 62 6A   20 3C 3C 2F  4C 69 6E 65    54 0 obj <</Line
0x00000020: 61 72 69 7A  65 64 20 31   2F 4C 20 32  37 32 34 33    arized 1/L 27243
0x00000030: 31 2F 4F 20  35 39 2F 45   20 36 32 38  34 32 2F 4E    1/O 59/E 62842/N
0x00000040: 20 31 31 2F  54 20 32 37   31 33 30 34  2F 48 20 5B     11/T 271304/H [
0x00000050: 20 31 31 33  36 20 34 34   38 5D 3E 3E  0D 65 6E 64     1136 448]>>.end
0x00000060: 6F 62 6A 0D  20 20 20 20   20 20 20 20  20 20 20 20    obj.
0x00000070: 20 20 0D 0A  78 72 65 66   0D 0A 35 34  20 34 32 0D      ..xref..54 42.
0x00000080: 0A 30 30 30  30 30 30 30   30 31 36 20  30 30 30 30    .0000000016 0000
0x00000090: 30 20 6E 0D  0A 30 30 30   30 30 30 31  35 38 34 20    0 n..0000001584
```

1 File with an Extension Mismatch

- I went to Analysis report-> Extension Mismatch Detected on the Directory plane and found a mismatch.



Extension Mismatch Detected 2 Results

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification
bbbb.dat			1	File	Likely Notable			File has MIME type
aaaa.dat			0	File	Likely Notable			File has MIME type

Analysis Result 1

Score: Likely Notable

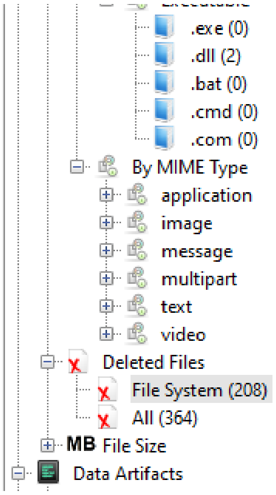
Type: Extension Mismatch Detected

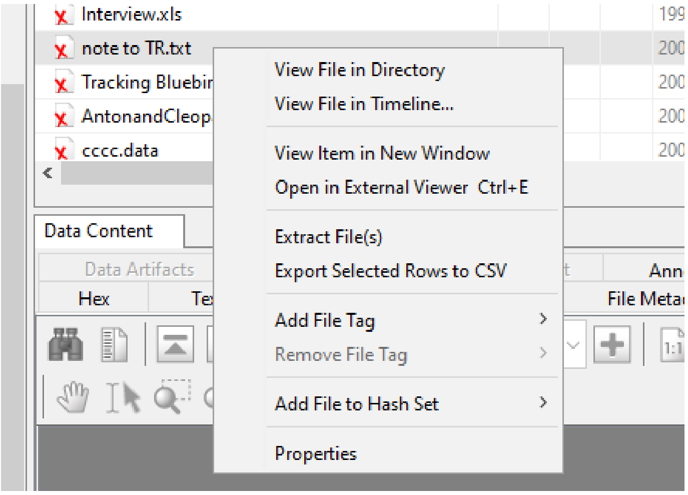
Configuration:

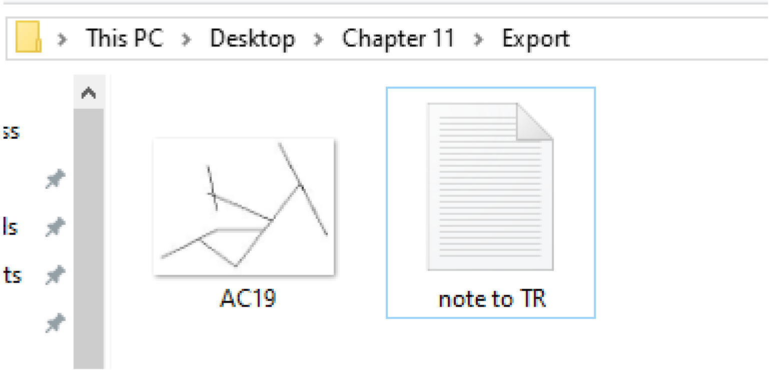
Step 4: Carve Deleted File

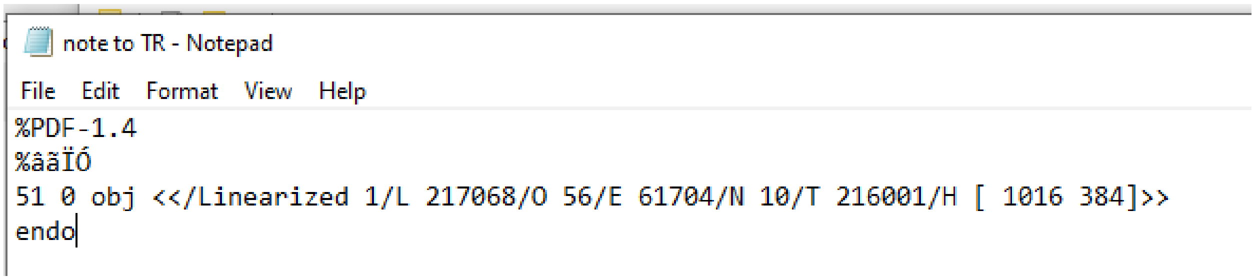
Find a deleted file (tree) and carve/export (right-click) the file locally to your forensics workstation. Identify the file type, meta data, and its contents.

- File type: text file

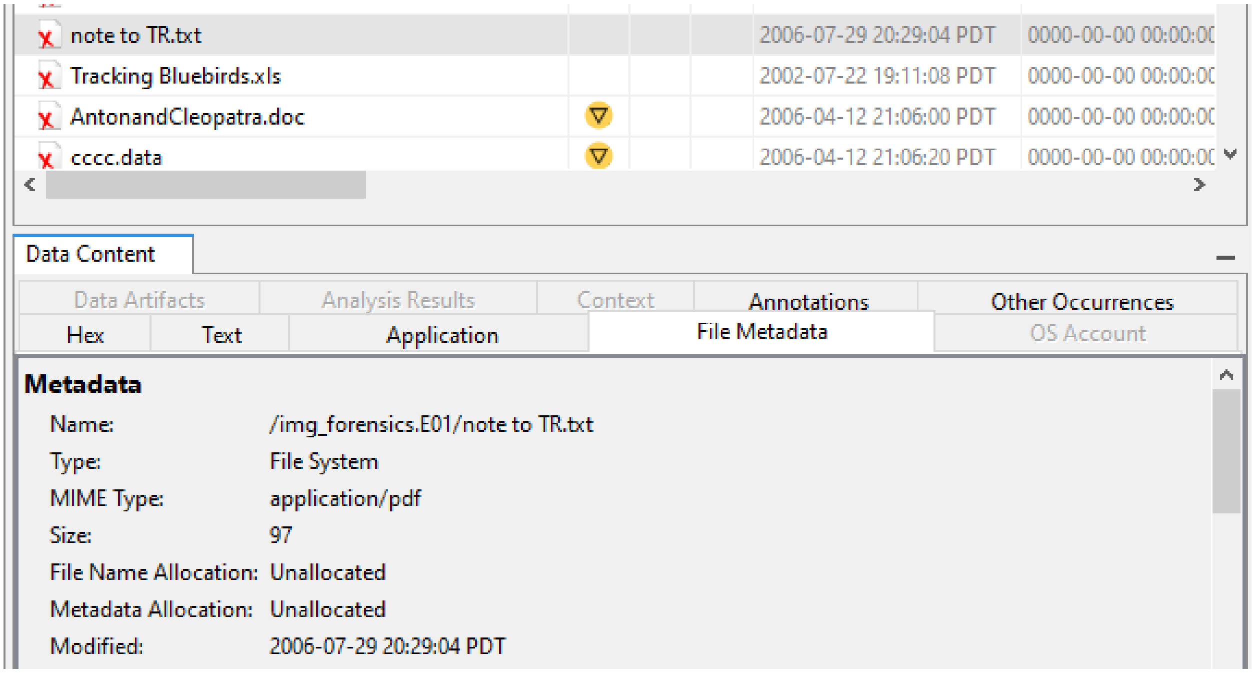








```
%PDF-1.4
%âãÏÓ
51 0 obj <</Linearized 1/L 217068/O 56/E 61704/N 10/T 216001/H [ 1016 384]>>
endo
```



Data Content
Data Artifacts Analysis Results Context Annotations Other Occurrences
Hex Text Application File Metadata OS Account

```
note to TR.txt                        2006-07-29 20:29:04 PDT   0000-00-00 00:00:00
Tracking Bluebirds.xls                2002-07-22 19:11:08 PDT   0000-00-00 00:00:00
AntonandCleopatra.doc                 2006-04-12 21:06:00 PDT   0000-00-00 00:00:00
cccc.data                             2006-04-12 21:06:20 PDT   0000-00-00 00:00:00
```

Metadata

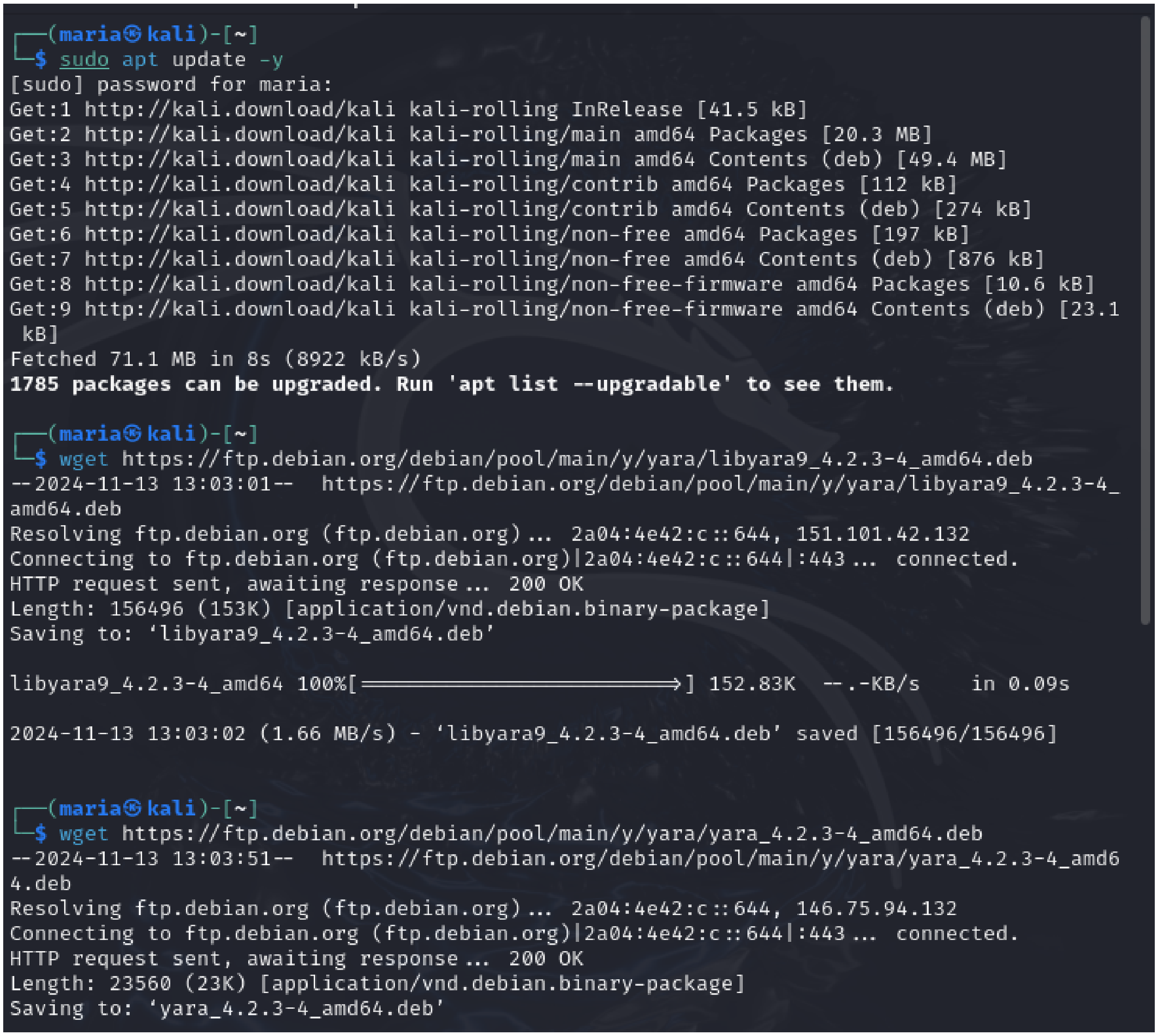
Name:	/img_forensics.E01/note to TR.txt
Type:	File System
MIME Type:	application/pdf
Size:	97
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2006-07-29 20:29:04 PDT

Exercise 11.2 Malware Detection

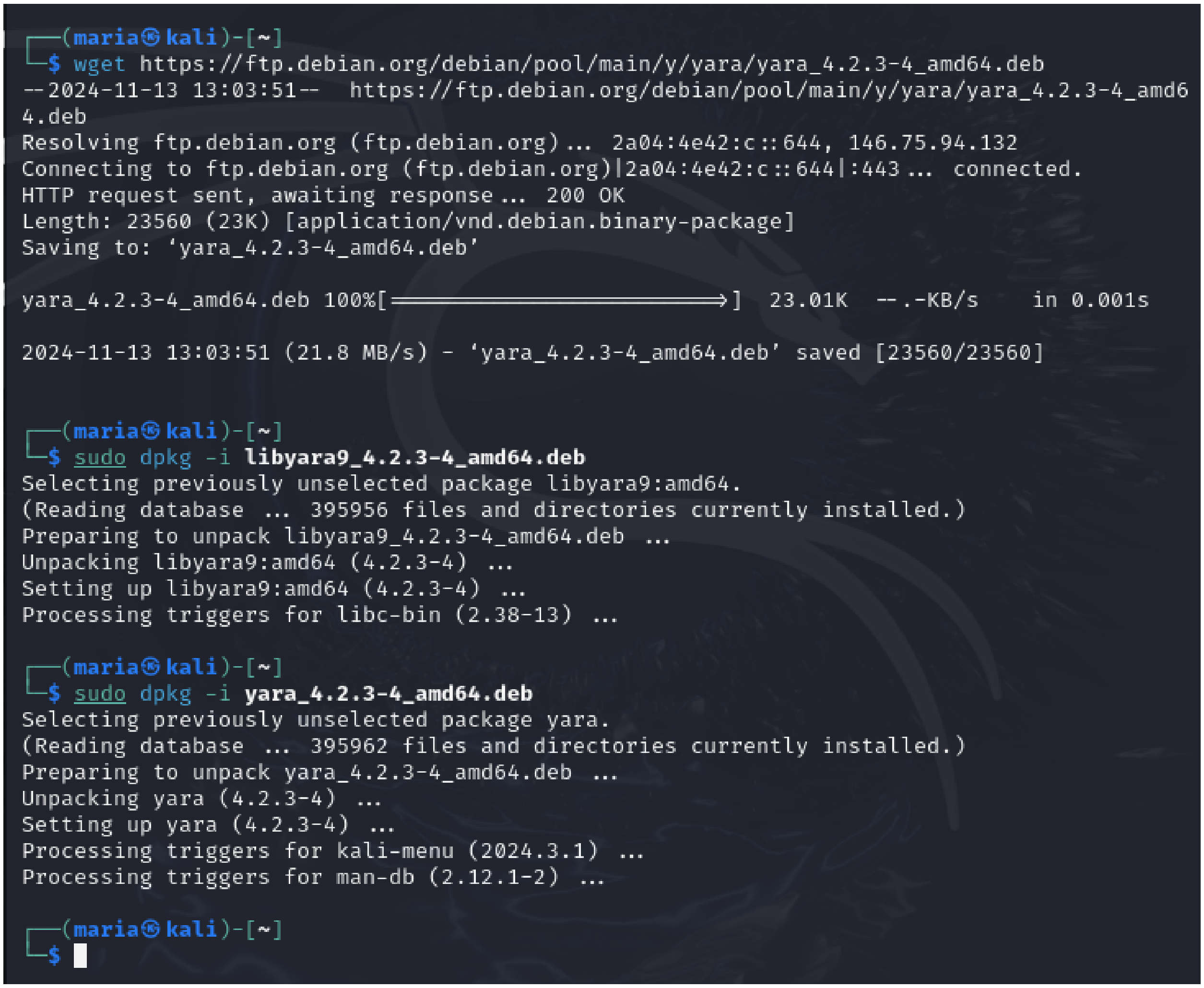
Yara is a malware detection tool supported by a large opensource and commercial community. The tool enables an analyst to quickly create a ruleset that can be used to detect malicious software. In this task you will create a custom Yara rule to identify a malicious file using your Kali VM running in Bridge Adapter network mode.

Step 1: Install Yara

In your Kali VM, launch a terminal, update your system, and install Yara using the following commands.

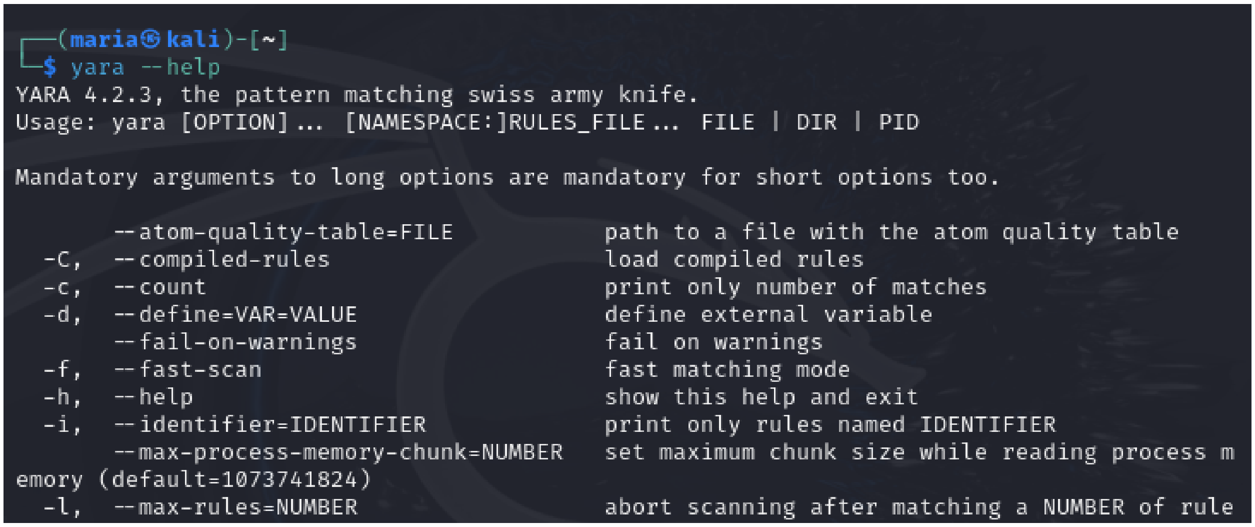


```
┌──(maria㉿kali)-[~]
└─$ sudo apt update -y
[sudo] password for maria:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [274 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [876 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.1
 kB]
Fetched 71.1 MB in 8s (8922 kB/s)
1785 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(maria㉿kali)-[~]
└─$ wget https://ftp.debian.org/debian/pool/main/y/yara/libyara9_4.2.3-4_amd64.deb
--2024-11-13 13:03:01--  https://ftp.debian.org/debian/pool/main/y/yara/libyara9_4.2.3-4_
amd64.deb
Resolving ftp.debian.org (ftp.debian.org)... 2a04:4e42:c::644, 151.101.42.132
Connecting to ftp.debian.org (ftp.debian.org)|2a04:4e42:c::644|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 156496 (153K) [application/vnd.debian.binary-package]
Saving to: ‘libyara9_4.2.3-4_amd64.deb’

libyara9_4.2.3-4_amd64 100%[=========================>] 152.83K  --.-KB/s    in 0.09s

2024-11-13 13:03:02 (1.66 MB/s) - ‘libyara9_4.2.3-4_amd64.deb’ saved [156496/156496]


┌──(maria㉿kali)-[~]
└─$ wget https://ftp.debian.org/debian/pool/main/y/yara/yara_4.2.3-4_amd64.deb
--2024-11-13 13:03:51--  https://ftp.debian.org/debian/pool/main/y/yara/yara_4.2.3-4_amd6
4.deb
Resolving ftp.debian.org (ftp.debian.org)... 2a04:4e42:c::644, 146.75.94.132
Connecting to ftp.debian.org (ftp.debian.org)|2a04:4e42:c::644|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23560 (23K) [application/vnd.debian.binary-package]
Saving to: ‘yara_4.2.3-4_amd64.deb’
```



```
┌──(maria㉿kali)-[~]
└─$ wget https://ftp.debian.org/debian/pool/main/y/yara/yara_4.2.3-4_amd64.deb
--2024-11-13 13:03:51--  https://ftp.debian.org/debian/pool/main/y/yara/yara_4.2.3-4_amd6
4.deb
Resolving ftp.debian.org (ftp.debian.org)... 2a04:4e42:c::644, 146.75.94.132
Connecting to ftp.debian.org (ftp.debian.org)|2a04:4e42:c::644|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23560 (23K) [application/vnd.debian.binary-package]
Saving to: ‘yara_4.2.3-4_amd64.deb’

yara_4.2.3-4_amd64.deb 100%[═══════════════════════════>]  23.01K  --.-KB/s    in 0.001s

2024-11-13 13:03:51 (21.8 MB/s) - ‘yara_4.2.3-4_amd64.deb’ saved [23560/23560]


┌──(maria㉿kali)-[~]
└─$ sudo dpkg -i libyara9_4.2.3-4_amd64.deb
Selecting previously unselected package libyara9:amd64.
(Reading database ... 395956 files and directories currently installed.)
Preparing to unpack libyara9_4.2.3-4_amd64.deb ...
Unpacking libyara9:amd64 (4.2.3-4) ...
Setting up libyara9:amd64 (4.2.3-4) ...
Processing triggers for libc-bin (2.38-13) ...

┌──(maria㉿kali)-[~]
└─$ sudo dpkg -i yara_4.2.3-4_amd64.deb
Selecting previously unselected package yara.
(Reading database ... 395962 files and directories currently installed.)
Preparing to unpack yara_4.2.3-4_amd64.deb ...
Unpacking yara (4.2.3-4) ...
Setting up yara (4.2.3-4) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.12.1-2) ...

┌──(maria㉿kali)-[~]
└─$ 
```

Verify Yara installed by running the help menu and reviewing its capabilities.

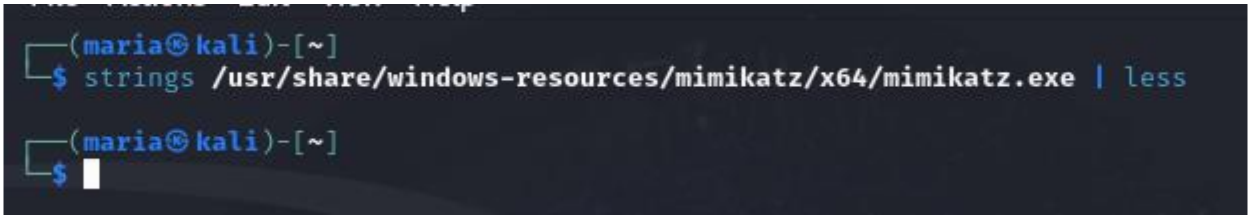


```
┌──(maria㉿kali)-[~]
└─$ yara --help
YARA 4.2.3, the pattern matching swiss army knife.
Usage: yara [OPTION]... [NAMESPACE:]RULES_FILE... FILE | DIR | PID

Mandatory arguments to long options are mandatory for short options too.

       --atom-quality-table=FILE           path to a file with the atom quality table
  -C,  --compiled-rules                    load compiled rules
  -c,  --count                             print only number of matches
  -d,  --define=VAR=VALUE                  define external variable
       --fail-on-warnings                  fail on warnings
  -f,  --fast-scan                         fast matching mode
  -h,  --help                              show this help and exit
  -i,  --identifier=IDENTIFIER             print only rules named IDENTIFIER
       --max-process-memory-chunk=NUMBER   set maximum chunk size while reading process m
emory (default=1073741824)
  -l,  --max-rules=NUMBER                  abort scanning after matching a NUMBER of rule
```

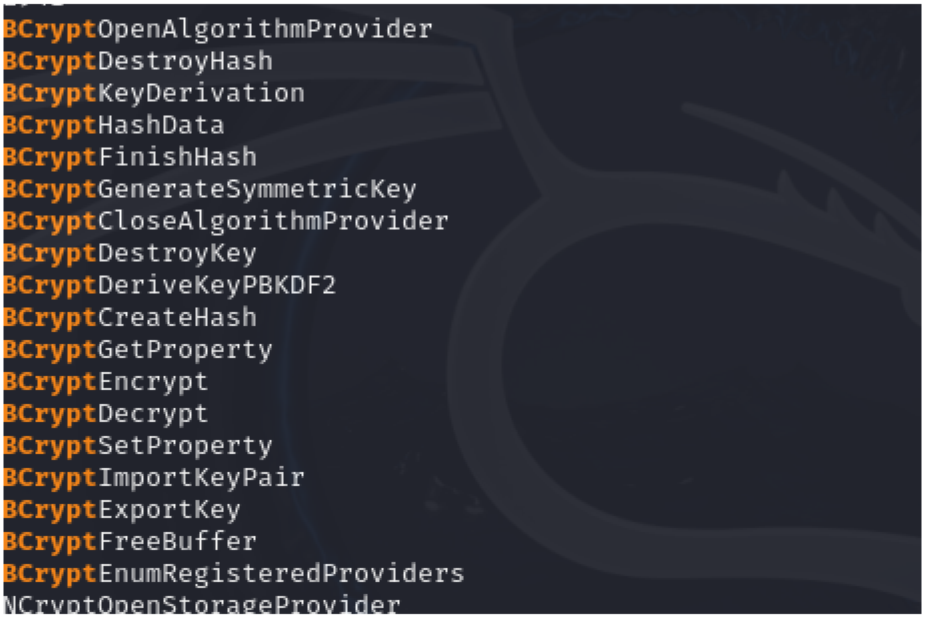
Step 2: Analyze Known Malware

We will analyze the local copy of mimikatz.exe installed on your Kali VM. Mimikatz is a Windows credential dumping utility used to extract Windows passwords and is often integrated in other malware. The 64 bit executable is located at the following path on your Kali VM " /usr/share/windows-resources/mimikatz/x64/mimikatz.exe ".

Identify a string that can be used in our Yara rule. Run the strings tool on the file and pipe to the less utility to identify Windows API crypto functions. BCrypt API functions are used by Windows to perform cryptographic operations which are also used by Mimikatz to extract passwords/hashes. Type " /BCrypt " while in the less editor and press enter. Press " q " to exit less when satisfied.

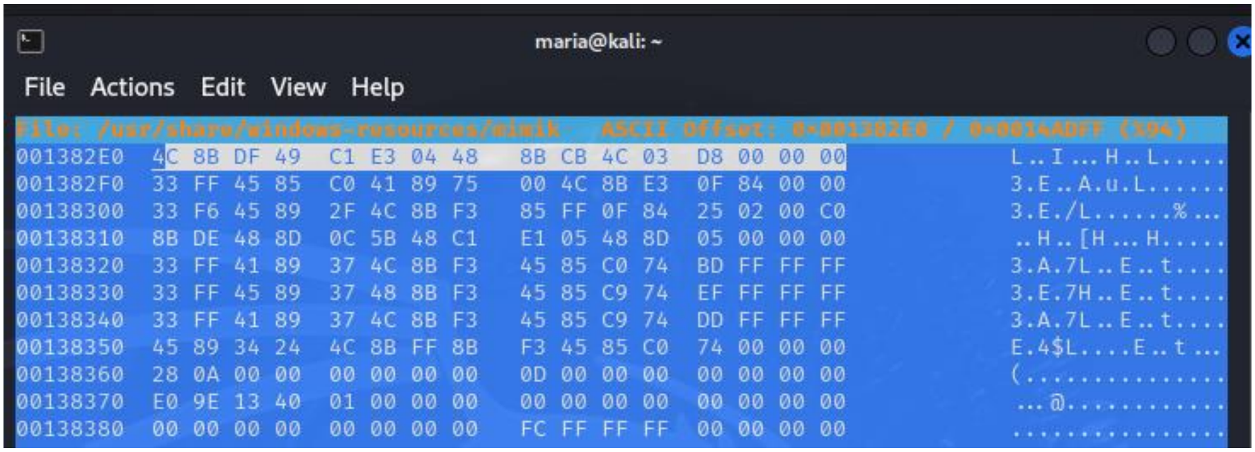


```
┌──(maria㉿kali)-[~]
└─$ strings /usr/share/windows-resources/mimikatz/x64/mimikatz.exe | less

┌──(maria㉿kali)-[~]
└─$ 
```



```
BCryptOpenAlgorithmProvider
BCryptDestroyHash
BCryptKeyDerivation
BCryptHashData
BCryptFinishHash
BCryptGenerateSymmetricKey
BCryptCloseAlgorithmProvider
BCryptDestroyKey
BCryptDeriveKeyPBKDF2
BCryptCreateHash
BCryptGetProperty
BCryptEncrypt
BCryptDecrypt
BCryptSetProperty
BCryptImportKeyPair
BCryptExportKey
BCryptFreeBuffer
BCryptEnumRegisteredProviders
NCryptOpenStorageProvider
```

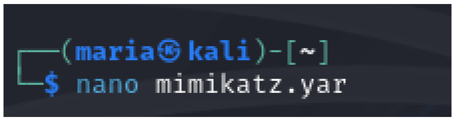
Next, identify some hexcode in the mimikatz.exe . Using hexeditor , identify a unique section of shellcode. While in the editor, go to offset 1382E0 by pressing " CTRL+T " and enter the offset value. This snippet of hexcode may be a good candidate to fingerprint Mimikatz. Copy this hex line to use in our Yara. Press " CTRL+C " to exit the editor once finished.



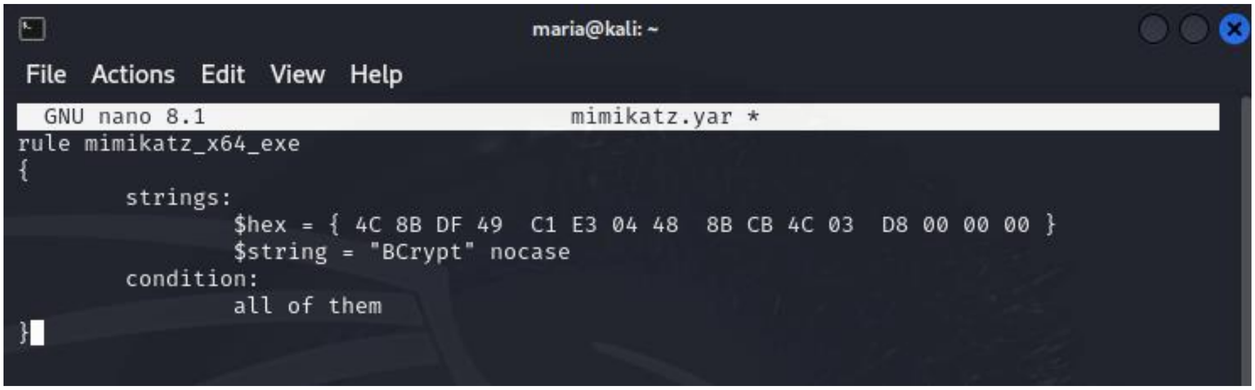
```
File: /usr/share/windows-resources/mimik   ASCII Offset: 0x001382E0 / 0x0014ADFF (%94)
001382E0  4C 8B DF 49  C1 E3 04 48   8B CB 4C 03  D8 00 00 00          L..I...H..L.....
001382F0  33 FF 45 85  C0 41 89 75   00 4C 8B E3  0F 84 00 00          3.E..A.u.L......
00138300  33 F6 45 89  2F 4C 8B F3   85 FF 0F 84  25 02 00 C0          3.E./L......%...
00138310  8B DE 48 8D  0C 5B 48 C1   E1 05 48 8D  05 00 00 00          ..H..[H...H.....
00138320  33 FF 41 89  37 4C 8B F3   45 85 C0 74  BD FF FF FF          3.A.7L..E..t....
00138330  33 FF 45 89  37 48 8B F3   45 85 C9 74  EF FF FF FF          3.E.7H..E..t....
00138340  33 FF 41 89  37 4C 8B F3   45 85 C9 74  DD FF FF FF          3.A.7L..E..t....
00138350  45 89 34 24  4C 8B FF 8B   F3 45 85 C0  74 00 00 00          E.4$L....E..t...
00138360  28 0A 00 00  00 00 00 00   0D 00 00 00  00 00 00 00          (...............
00138370  E0 9E 13 40  01 00 00 00   00 00 00 00  00 00 00 00          ...@............
00138380  00 00 00 00  00 00 00 00   FC FF FF FF  00 00 00 00          ................
```

Step 3: Create Custom Yara Rule

Create a yara ruleset in a file called mimikatz.yar that uses the string and hex code identified in the previous step. Use the following template and your favorite text editor. The strings section informs the yara tool which strings and hexcode to find in a given file. The condition section qualifies which strings need to be present for the rule to trigger. Make sure to replace HEX_CODE_HERE with the hexcode you found in hexeditor from the previous step.



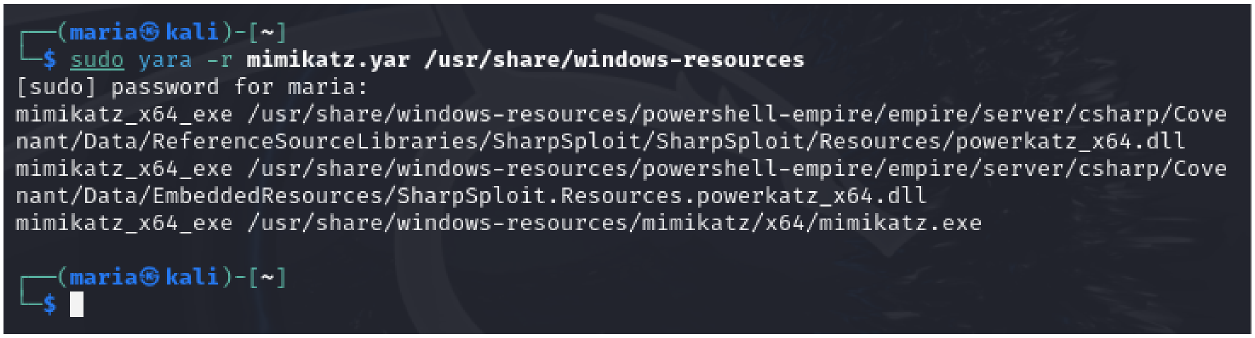
```
┌──(maria㉿kali)-[~]
└─$ nano mimikatz.yar
```



```
  GNU nano 8.1                          mimikatz.yar *
rule mimikatz_x64_exe
{
        strings:
                $hex = { 4C 8B DF 49  C1 E3 04 48  8B CB 4C 03  D8 00 00 00 }
                $string = "BCrypt" nocase
        condition:
                all of them
}
```

Step 4: Find Malware Using Yara

With the rule created, run yara on the " /usr/share/windows-resources " directory recursively to identify all files that contain the subject string and hexcode. Files listed indicate a match



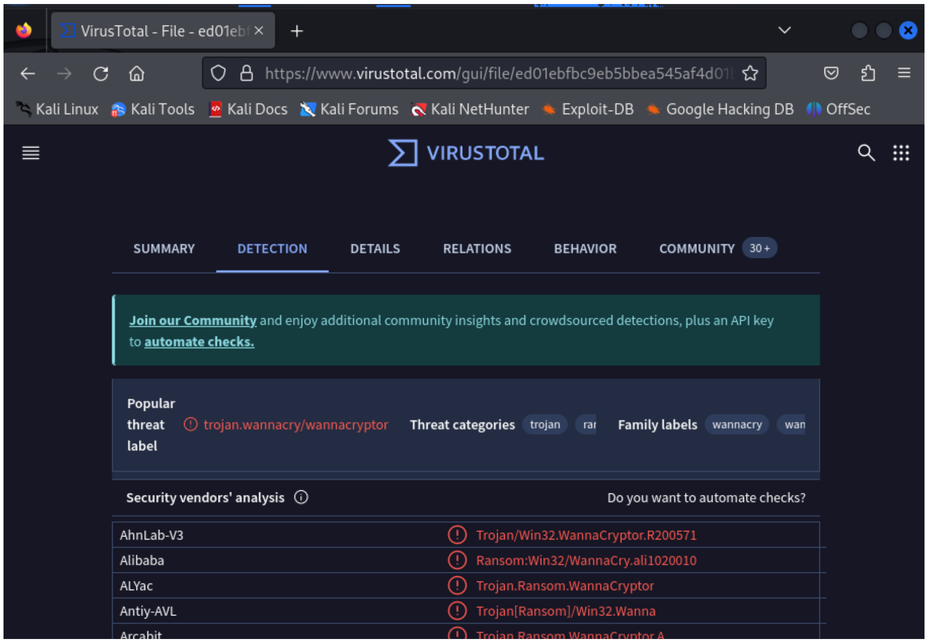
```
┌──(maria㉿kali)-[~]
└─$ sudo yara -r mimikatz.yar /usr/share/windows-resources
[sudo] password for maria:
mimikatz_x64_exe /usr/share/windows-resources/powershell-empire/empire/server/csharp/Cove
nant/Data/ReferenceSourceLibraries/SharpSploit/SharpSploit/Resources/powerkatz_x64.dll
mimikatz_x64_exe /usr/share/windows-resources/powershell-empire/empire/server/csharp/Cove
nant/Data/EmbeddedResources/SharpSploit.Resources.powerkatz_x64.dll
mimikatz_x64_exe /usr/share/windows-resources/mimikatz/x64/mimikatz.exe

┌──(maria㉿kali)-[~]
└─$ 
```

Exercise 11.3 Malware Analysis

The WannaCry ransomware leveraged wormable SMB vulnerabilities to rapidly spread across the globe in 2016. In this lab you will use online resources to statically and dynamically analyze WannaCry. You will be in close proximity to this malware so it is best to use one of your VMs with the NAT network mode. Take caution if you decide to download a sample as mishandling it may result in a ransomware infection.

Step 1: Static Analysis

Navigate to https://www.virustotal.com/gui/home/search , enter the MD5 hash " 84c82835a5d21bbcf75a61706d8ab549 ", and observe most AV vendors identify the hash as WannaCry.



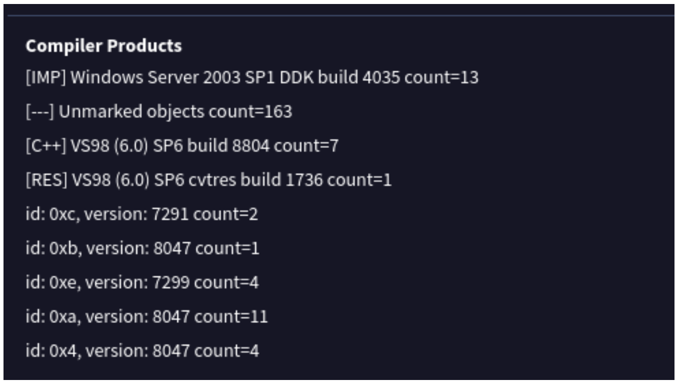
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.wannacry/wannacryptor Threat categories trojan ra Family labels wannacry wan

Security vendors' analysis Do you want to automate checks?

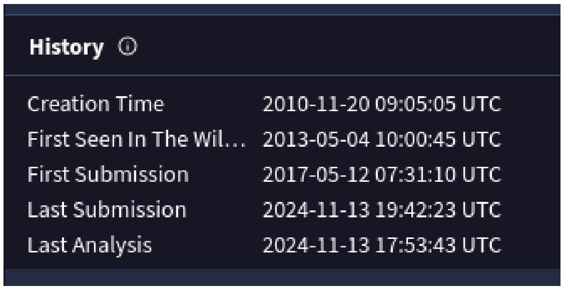
AhnLab-V3	Trojan/Win32.WannaCryptor.R200571
Alibaba	Ransom:Win32/WannaCry.ali1020010
ALYac	Trojan.Ransom.WannaCryptor
Antiy-AVL	Trojan[Ransom]/Win32.Wanna
Arcabit	Trojan.Ransom.WannaCryptor.A

Select the Details tab and review the properties. Observe what tools compiled the program and when it was created.



Compiler Products

```
[IMP] Windows Server 2003 SP1 DDK build 4035 count=13
[---] Unmarked objects count=163
[C++] VS98 (6.0) SP6 build 8804 count=7
[RES] VS98 (6.0) SP6 cvtres build 1736 count=1
id: 0xc, version: 7291 count=2
id: 0xb, version: 8047 count=1
id: 0xe, version: 7299 count=4
id: 0xa, version: 8047 count=11
id: 0x4, version: 8047 count=4
```

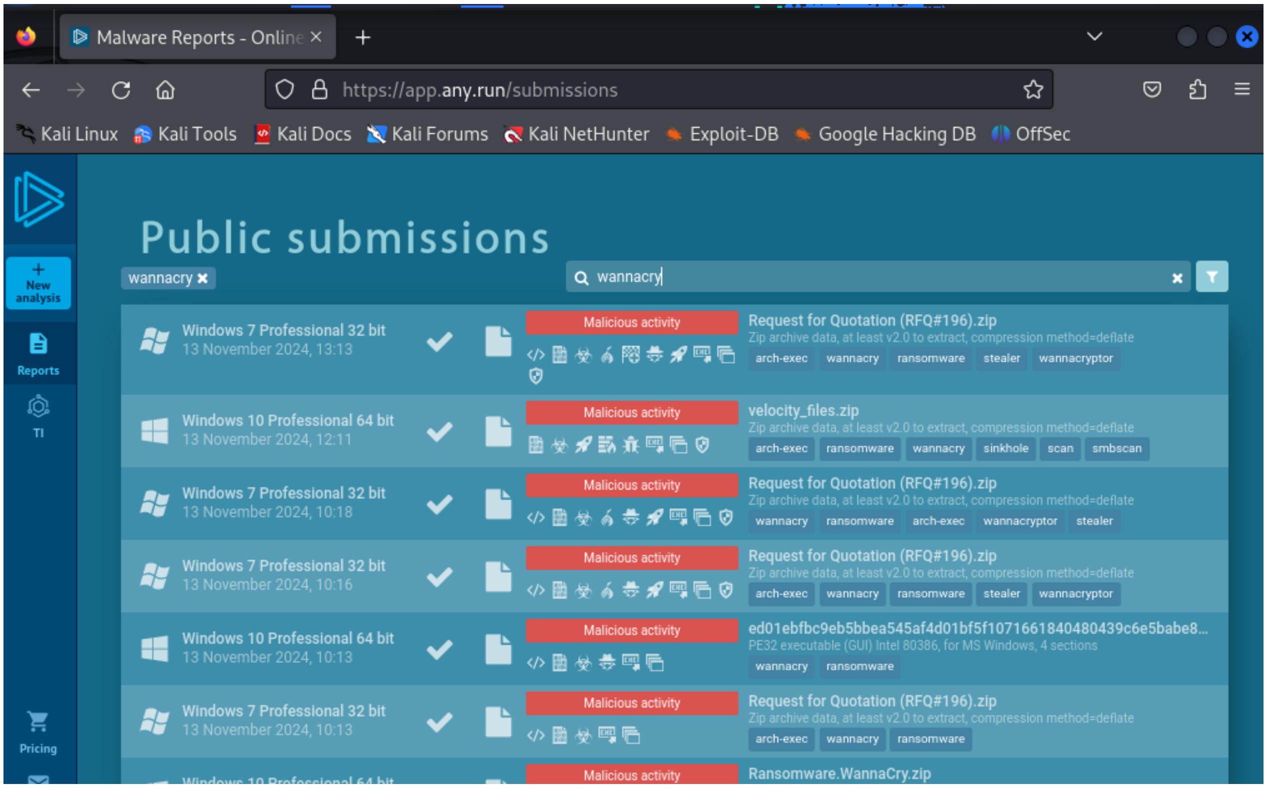


History

Creation Time	2010-11-20 09:05:05 UTC
First Seen In The Wil…	2013-05-04 10:00:45 UTC
First Submission	2017-05-12 07:31:10 UTC
Last Submission	2024-11-13 19:42:23 UTC
Last Analysis	2024-11-13 17:53:43 UTC

Step 2: Dynamic Analysis

Navigate to https://app.any.run/submissions and type " wannacry " in the search bar. Observe several submissions populate with the MD5 hash " 84c82835a5d21bbcf75a61706d8ab549 ".

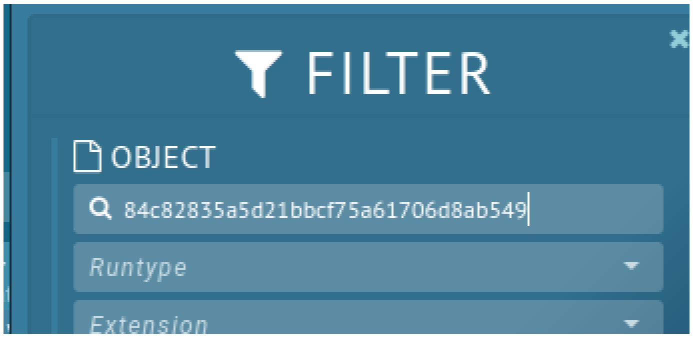


Public submissions

wannacry ✖

wannacry

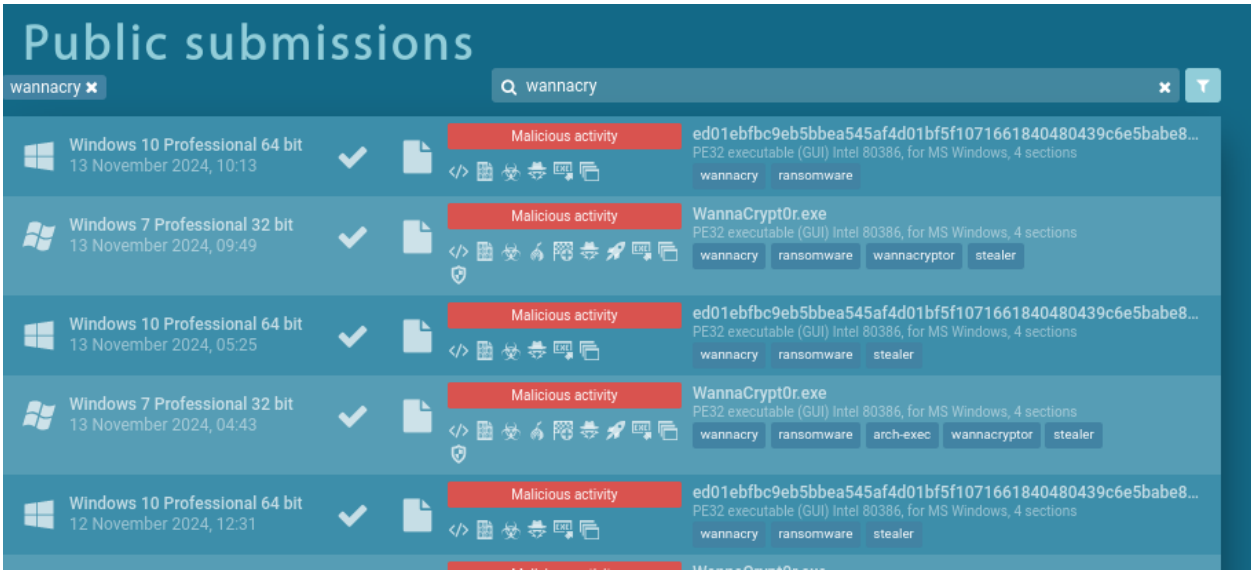
Windows 7 Professional 32 bit 13 November 2024, 13:13	✓	Malicious activity	Request for Quotation (RFQ#196).zip Zip archive data, at least v2.0 to extract, compression method=deflate arch-exec wannacry ransomware stealer wannacryptor
Windows 10 Professional 64 bit 13 November 2024, 12:11	✓	Malicious activity	velocity_files.zip Zip archive data, at least v2.0 to extract, compression method=deflate arch-exec ransomware wannacry sinkhole scan smbscan
Windows 7 Professional 32 bit 13 November 2024, 10:18	✓	Malicious activity	Request for Quotation (RFQ#196).zip Zip archive data, at least v2.0 to extract, compression method=deflate wannacry ransomware arch-exec wannacryptor stealer
Windows 7 Professional 32 bit 13 November 2024, 10:16	✓	Malicious activity	Request for Quotation (RFQ#196).zip Zip archive data, at least v2.0 to extract, compression method=deflate arch-exec wannacry ransomware stealer wannacryptor
Windows 10 Professional 64 bit 13 November 2024, 10:13	✓	Malicious activity	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8… PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections wannacry ransomware
Windows 7 Professional 32 bit 13 November 2024, 10:13	✓	Malicious activity	Request for Quotation (RFQ#196).zip Zip archive data, at least v2.0 to extract, compression method=deflate arch-exec wannacry ransomware
Windows 10 Professional 64 bit		Malicious activity	Ransomware.WannaCry.zip



FILTER

OBJECT

84c82835a5d21bbcf75a61706d8ab549



Public submissions

Windows 10 Professional 64 bit
13 November 2024, 10:13
Malicious activity
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8...
PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
wannacry ransomware

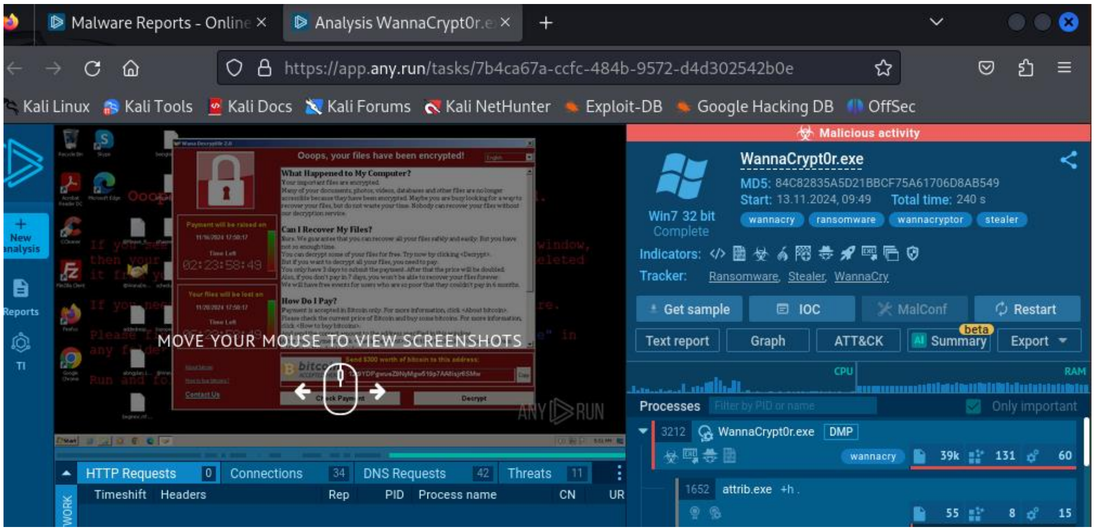
Windows 7 Professional 32 bit
13 November 2024, 09:49
Malicious activity
WannaCrypt0r.exe
PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
wannacry ransomware wannacryptor stealer

Windows 10 Professional 64 bit
13 November 2024, 05:25
Malicious activity
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8...
PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
wannacry ransomware stealer

Windows 7 Professional 32 bit
13 November 2024, 04:43
Malicious activity
WannaCrypt0r.exe
PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
wannacry ransomware arch-exec wannacryptor stealer

Windows 10 Professional 64 bit
12 November 2024, 12:31
Malicious activity
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8...
PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
wannacry ransomware stealer

Select one of the submissions to review the already ran dynamic analysis results. Cycle through the screenshots to visually see how the malware behaved. Note, some submissions may only contain one; cycle through submissions until you find one that looks the most interesting.



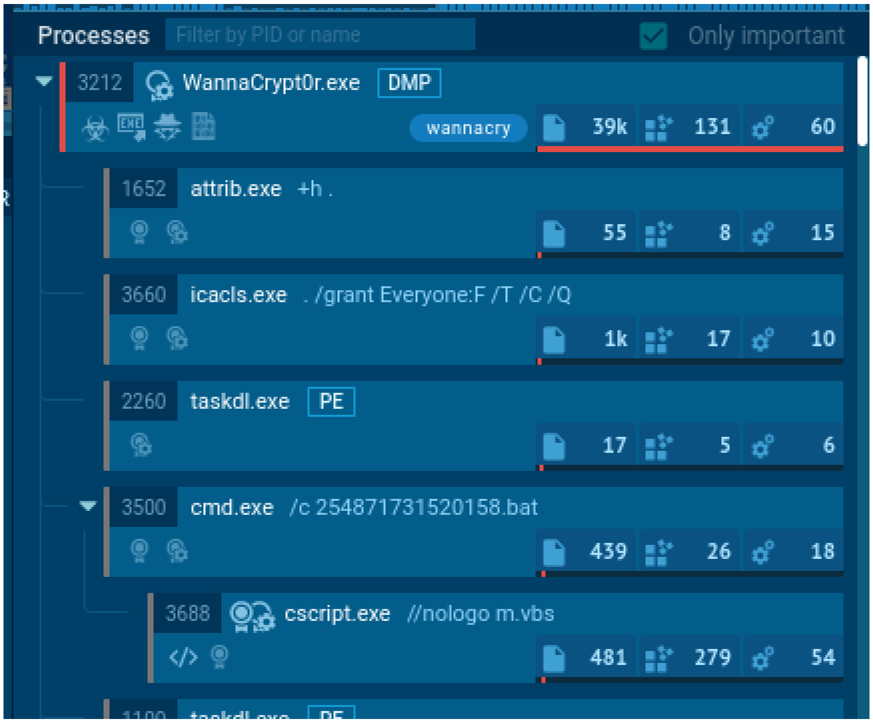
https://app.any.run/tasks/7b4ca67a-ccfc-484b-9572-d4d302542b0e

Malicious activity

WannaCrypt0r.exe
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 13.11.2024, 09:49 Total time: 240 s
wannacry ransomware wannacryptor stealer
Win7 32 bit
Complete
Indicators:
Tracker: Ransomware, Stealer, WannaCry

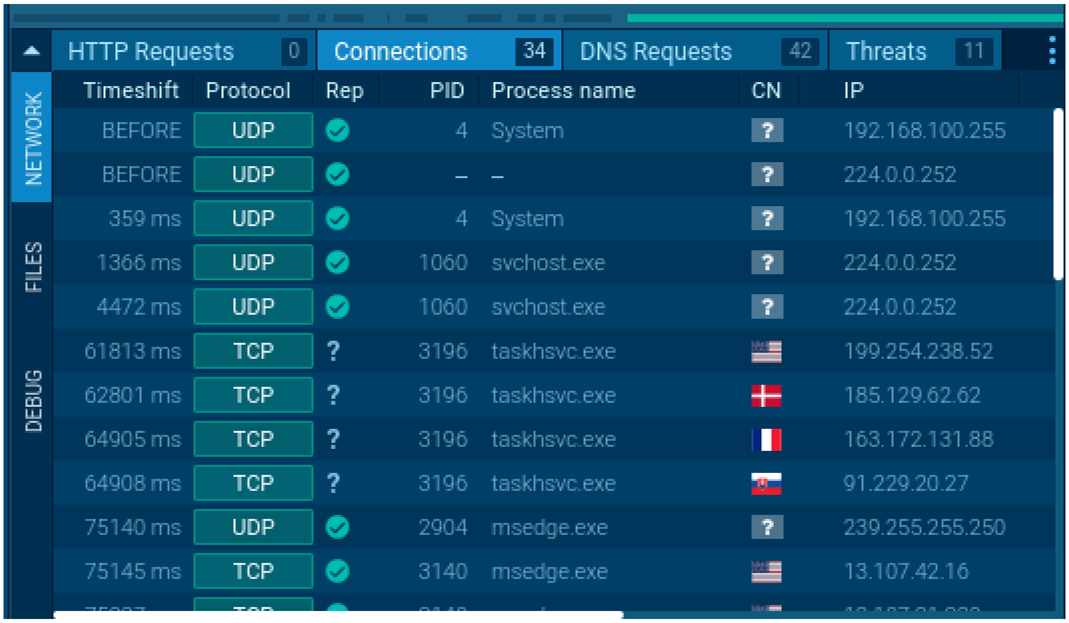
Processes
3212 WannaCrypt0r.exe DMP
wannacry 39k 131 60
1652 attrib.exe +h .
55 8 15

Observe the malware's behavior on the right pane. You should be able to see the process trees created and the commands ran in the background



```
3212  WannaCrypt0r.exe  DMP
      wannacry   39k   131   60
  1652  attrib.exe  +h .
        55   8   15
  3660  icacls.exe  . /grant Everyone:F /T /C /Q
        1k   17   10
  2260  taskdl.exe  PE
        17   5   6
  3500  cmd.exe  /c 254871731520158.bat
        439   26   18
    3688  cscript.exe  //nologo m.vbs
          481   279   54
  1100  taskdl.exe  PE
```

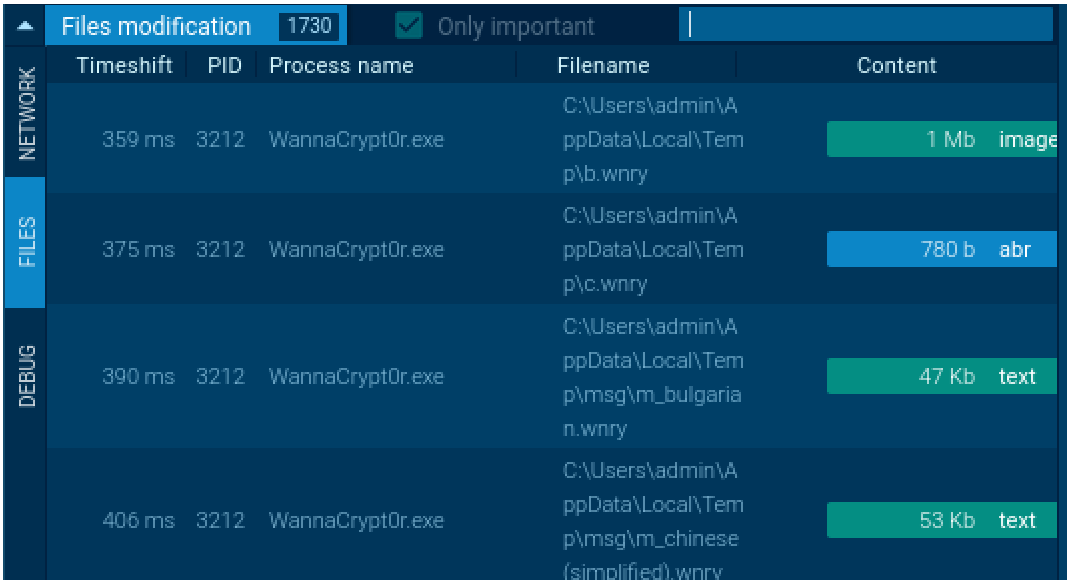
Investigate the Network activities in the bottom pane. Discover what connections were made while the malware ran.



Timeshift	Protocol	Rep	PID	Process name	CN	IP
BEFORE	UDP	✓	4	System	?	192.168.100.255
BEFORE	UDP	✓	–	–	?	224.0.0.252
359 ms	UDP	✓	4	System	?	192.168.100.255
1366 ms	UDP	✓	1060	svchost.exe	?	224.0.0.252
4472 ms	UDP	✓	1060	svchost.exe	?	224.0.0.252
61813 ms	TCP	?	3196	taskhsvc.exe	🇺🇸	199.254.238.52
62801 ms	TCP	?	3196	taskhsvc.exe	🇩🇰	185.129.62.62
64905 ms	TCP	?	3196	taskhsvc.exe	🇫🇷	163.172.131.88
64908 ms	TCP	?	3196	taskhsvc.exe	🇸🇰	91.229.20.27
75140 ms	UDP	✓	2904	msedge.exe	?	239.255.255.250
75145 ms	TCP	✓	3140	msedge.exe	🇺🇸	13.107.42.16

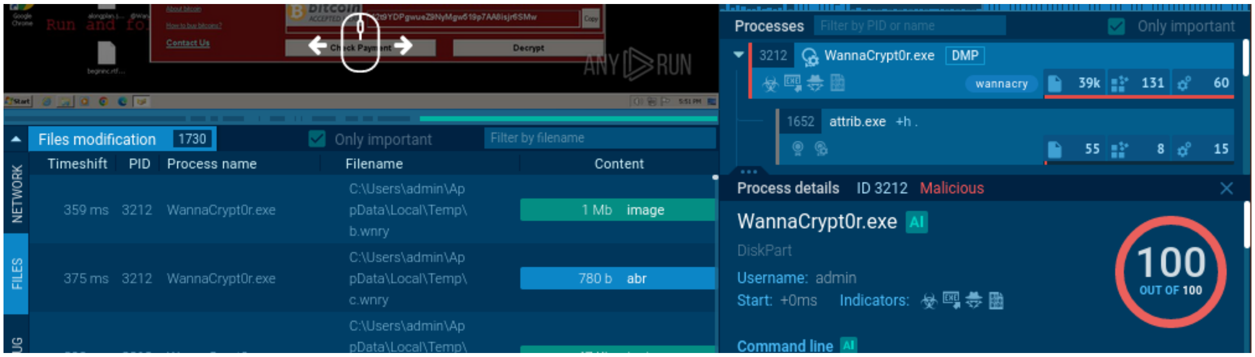
Review the Files activity in the bottom pane and determine what files were read and written to. Any file that ends in " .mnry " extension has been encrypted by the malware.

- I took a look into the first file modification shown. Overall this attack was meant to scare the owner into handing over bitcoin. The owner's files were encrypted and their wallpaper told them to click on the virus file.



Files modification 1730 ☑ Only important

Timeshift	PID	Process name	Filename	Content
359 ms	3212	WannaCrypt0r.exe	C:\Users\admin\AppData\Local\Temp\b.wnry	1 Mb image
375 ms	3212	WannaCrypt0r.exe	C:\Users\admin\AppData\Local\Temp\c.wnry	780 b abr
390 ms	3212	WannaCrypt0r.exe	C:\Users\admin\AppData\Local\Temp\msg\m_bulgarian.wnry	47 Kb text
406 ms	3212	WannaCrypt0r.exe	C:\Users\admin\AppData\Local\Temp\msg\m_chinese (simplified).wnry	53 Kb text



Files modification 1730 ☑ Only important Filter by filename

Timeshift	PID	Process name	Filename	Content
359 ms	3212	WannaCrypt0r.exe	C:\Users\admin\AppData\Local\Temp\b.wnry	1 Mb image
375 ms	3212	WannaCrypt0r.exe	C:\Users\admin\AppData\Local\Temp\c.wnry	780 b abr

Processes Filter by PID or name ☑ Only important

3212 WannaCrypt0r.exe DMP wannacry 39k 131 60

1652 attrib.exe +h . 55 8 15

Process details ID 3212 Malicious

WannaCrypt0r.exe AI

DiskPart

Username: admin

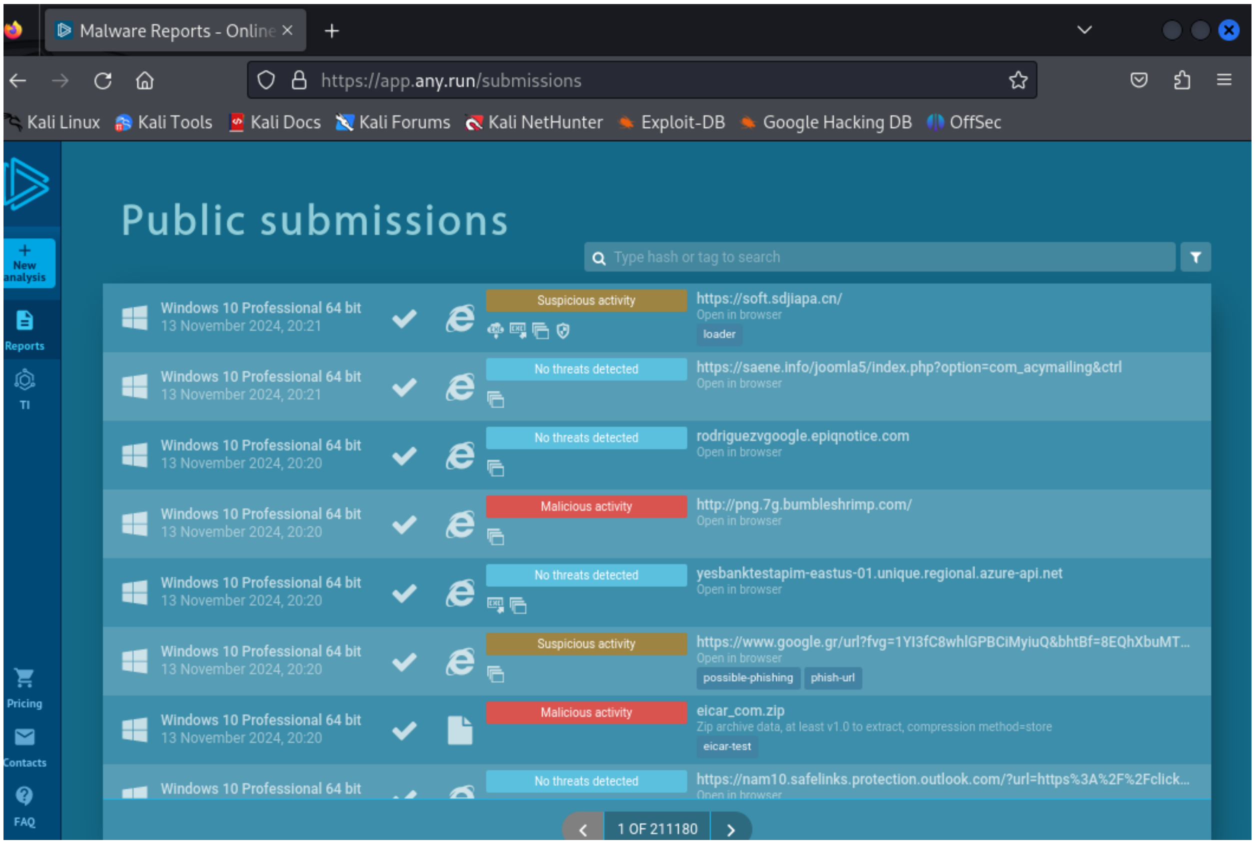
Start: +0ms Indicators:

100 OUT OF 100

Command line AI

Step 3: Explore Any Run

Navigate to https://app.any.run public submissions section and find a user submission that identifies malware. Perform your own Static and Dynamic analysis using VirusTotal and the already submitted sample in Any.Run. Describe the malware's properties and behavior in a short report.



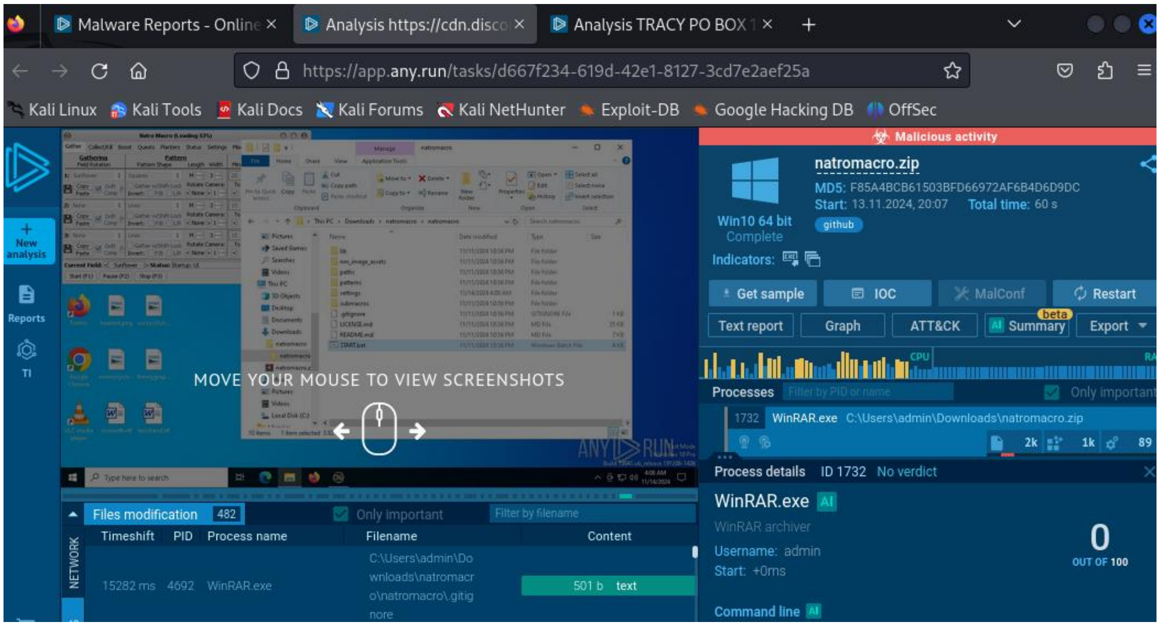
Public submissions

Type hash or tag to search

Windows 10 Professional 64 bit 13 November 2024, 20:21	Suspicious activity	https://soft.sdjiapa.cn/ Open in browser loader
Windows 10 Professional 64 bit 13 November 2024, 20:21	No threats detected	https://saene.info/joomla5/index.php?option=com_acymailing&ctrl Open in browser
Windows 10 Professional 64 bit 13 November 2024, 20:20	No threats detected	rodriguezvgoogle.epiqnotice.com Open in browser
Windows 10 Professional 64 bit 13 November 2024, 20:20	Malicious activity	http://png.7g.bumbleshrimp.com/ Open in browser
Windows 10 Professional 64 bit 13 November 2024, 20:20	No threats detected	yesbanktestapim-eastus-01.unique.regional.azure-api.net Open in browser
Windows 10 Professional 64 bit 13 November 2024, 20:20	Suspicious activity	https://www.google.gr/url?fvg=1YI3fC8whlGPBCiMyiuQ&bhtBf=8EQhXbuMT... Open in browser possible-phishing phish-url
Windows 10 Professional 64 bit 13 November 2024, 20:20	Malicious activity	eicar_com.zip Zip archive data, at least v1.0 to extract, compression method=store eicar-test
Windows 10 Professional 64 bit	No threats detected	https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Fclick... Open in browser

1 OF 211180

Although there are no malicious indicators, there is a lot of suspicious activity. This is from github using the WinRAR.exe (which was used in a previous lab). It happened by extracting the natromacro.zip file.



Malicious activity

natromacro.zip
MD5: F85A4BCB61503BFD66972AF6B4D6D9DC
Start: 13.11.2024, 20:07 Total time: 60 s
github
Win10 64 bit
Complete
Indicators:

Processes Filter by PID or name ☑ Only important

1732 WinRAR.exe C:\Users\admin\Downloads\natromacro.zip
2k 1k 89

Process details ID 1732 No verdict

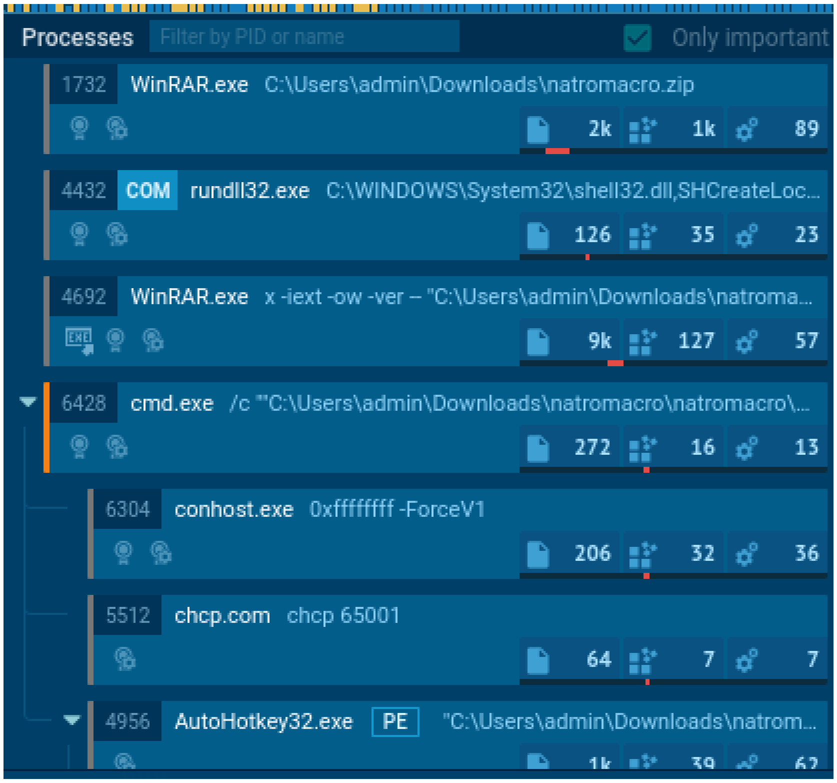
WinRAR.exe
WinRAR archiver
Username: admin
Start: +0ms
0 OUT OF 100
Command line

Files modification 482 ☑ Only important Filter by filename

Timeshift	PID	Process name	Filename	Content
15282 ms	4692	WinRAR.exe	C:\Users\admin\Downloads\natromacro\natromacro\.gitignore	501 b text

Dynamic Analysis:

Observe the malware's behavior on the right pane. You should be able to see the process trees created and the commands ran in the background



1732 WinRAR.exe C:\Users\admin\Downloads\natromacro.zip
2k 1k 89

4432 COM rundll32.exe C:\WINDOWS\System32\shell32.dll,SHCreateLoc...
126 35 23

4692 WinRAR.exe x -iext -ow -ver -- "C:\Users\admin\Downloads\natroma...
9k 127 57

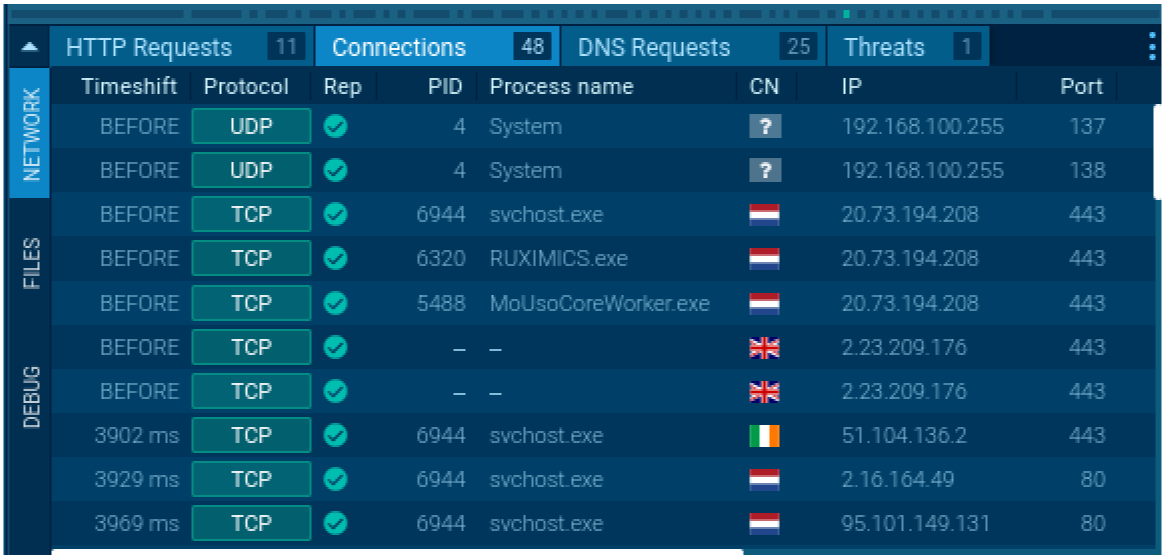
6428 cmd.exe /c ""C:\Users\admin\Downloads\natromacro\natromacro\...
272 16 13

6304 conhost.exe 0xffffffff -ForceV1
206 32 36

5512 chcp.com chcp 65001
64 7 7

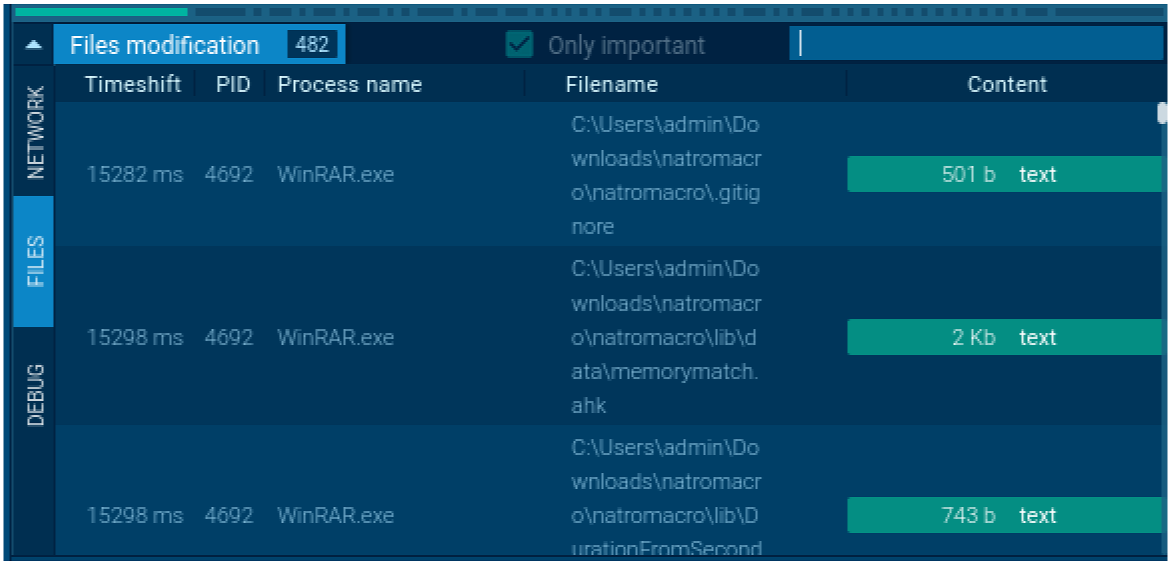
4956 AutoHotkey32.exe PE "C:\Users\admin\Downloads\natrom...
1k 39 62

Investigate the Network activities in the bottom pane. Discover what connections were made while the malware ran.

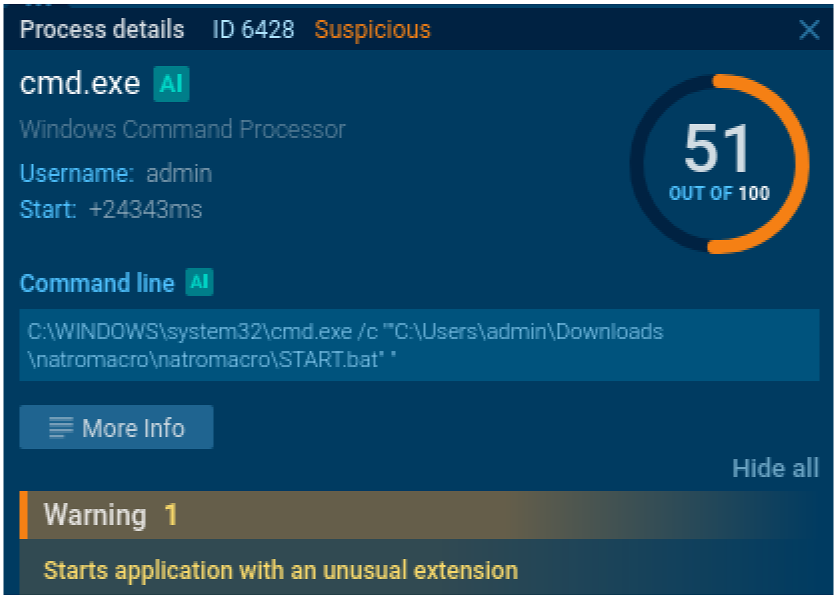


Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port
BEFORE	UDP	✓	4	System	?	192.168.100.255	137
BEFORE	UDP	✓	4	System	?	192.168.100.255	138
BEFORE	TCP	✓	6944	svchost.exe	🇳🇱	20.73.194.208	443
BEFORE	TCP	✓	6320	RUXIMICS.exe	🇳🇱	20.73.194.208	443
BEFORE	TCP	✓	5488	MoUsoCoreWorker.exe	🇳🇱	20.73.194.208	443
BEFORE	TCP	✓	–	–	🇬🇧	2.23.209.176	443
BEFORE	TCP	✓	–	–	🇬🇧	2.23.209.176	443
3902 ms	TCP	✓	6944	svchost.exe	🇮🇪	51.104.136.2	443
3929 ms	TCP	✓	6944	svchost.exe	🇳🇱	2.16.164.49	80
3969 ms	TCP	✓	6944	svchost.exe	🇳🇱	95.101.149.131	80

Review the Files activity in the bottom pane and determine what files were read and written to.



Timeshift	PID	Process name	Filename	Content
15282 ms	4692	WinRAR.exe	C:\Users\admin\Downloads\natromacro\natromacro\.gitignore	501 b text
15298 ms	4692	WinRAR.exe	C:\Users\admin\Downloads\natromacro\natromacro\lib\data\memorymatch.ahk	2 Kb text
15298 ms	4692	WinRAR.exe	C:\Users\admin\Downloads\natromacro\natromacro\lib\DurationFromSecond	743 b text


Process details ID 6428 Suspicious

cmd.exe AI

Windows Command Processor

Username: admin

Start: +24343ms

51 OUT OF 100

Command line AI

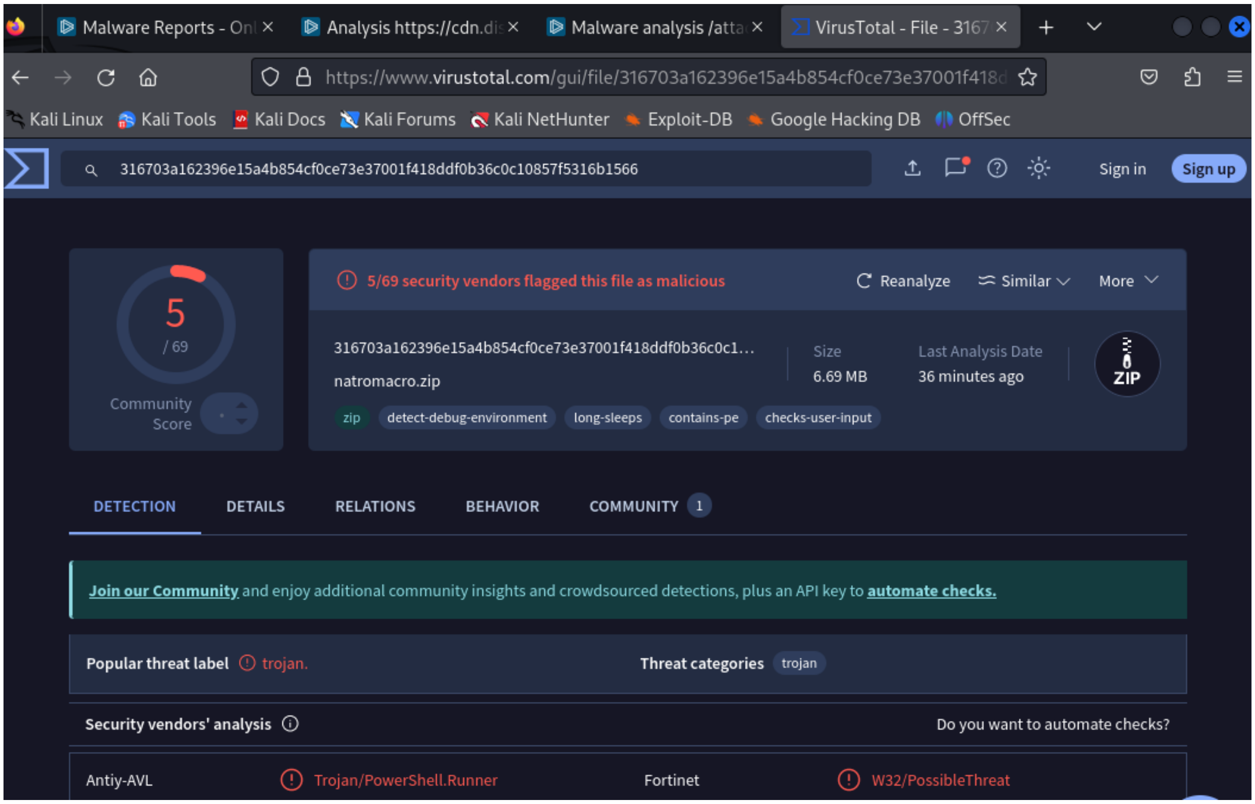
```
C:\WINDOWS\system32\cmd.exe /c ""C:\Users\admin\Downloads
\natromacro\natromacro\START.bat" "
```

Warning 1

Starts application with an unusual extension

Static Analysis;

Navigate to https://www.virustotal.com/gui/home/search and use the MD5 hash value f85a4bcb61503bfd66972af6b4d6d9dc to search.



316703a162396e15a4b854cf0ce73e37001f418ddf0b36c0c10857f5316b1566

5 / 69

Community Score

5/69 security vendors flagged this file as malicious

316703a162396e15a4b854cf0ce73e37001f418ddf0b36c0c1...

natromacro.zip

zip detect-debug-environment long-sleeps contains-pe checks-user-input

Size 6.69 MB

Last Analysis Date 36 minutes ago

ZIP

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

Popular threat label trojan.

Threat categories trojan

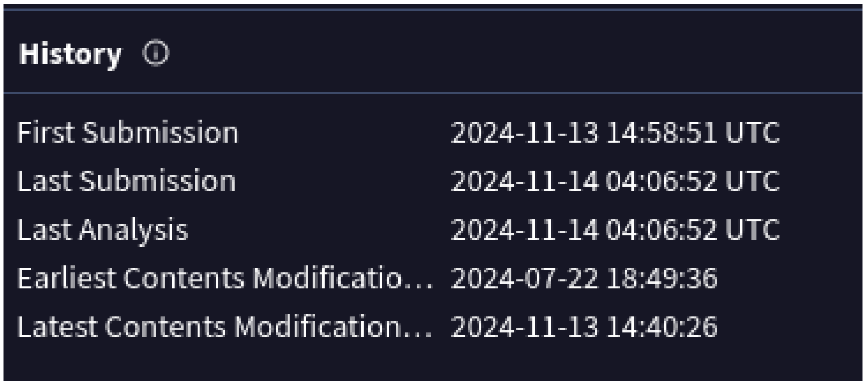
Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Trojan/PowerShell.Runner	Fortinet	W32/PossibleThreat

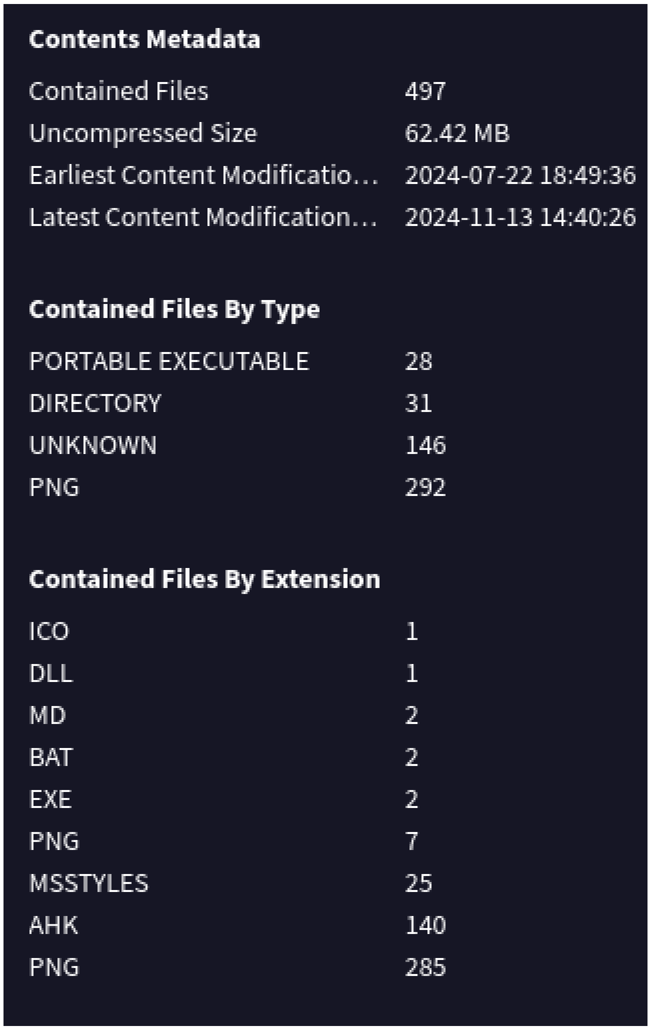
It is just labeled as a possible threat.

Select the Details tab and review the properties. Observe what tools compiled the program and when it was created. (It has no compiling history but has contained files by type).



History

First Submission	2024-11-13 14:58:51 UTC
Last Submission	2024-11-14 04:06:52 UTC
Last Analysis	2024-11-14 04:06:52 UTC
Earliest Contents Modificatio…	2024-07-22 18:49:36
Latest Contents Modification…	2024-11-13 14:40:26



Contents Metadata

Contained Files	497
Uncompressed Size	62.42 MB
Earliest Content Modificatio…	2024-07-22 18:49:36
Latest Content Modification…	2024-11-13 14:40:26

Contained Files By Type

PORTABLE EXECUTABLE	28
DIRECTORY	31
UNKNOWN	146
PNG	292

Contained Files By Extension

ICO	1
DLL	1
MD	2
BAT	2
EXE	2
PNG	7
MSSTYLES	25
AHK	140
PNG	285

Short Report

Analysis made on 11/13/2024

OS: WIndows 10

File properties:

- File Type: ZIP archive data
- Compression Method: Store
- Tags: GitHub

Hash:

- MD5: f85a4bcb61503bfd66972af6b4d6d9dc

The sample that was analyzed is a ZIP file, that is spread through GitHub. The store compression method could potentially indicate its a small or fully unpacked payload prepared for easy access and loading on the target system. Given the GitHub tag, the malware could exploit code repositories.

This malware could exploit code-sharing platforms (e.g., GitHub) to distribute its payload, targetting users that frequently download from repositories. This is scary as I am currently working on my senior project (a website) and my team, and I have had to download repositories without much investigation. Some immediate recommendations to prevent this is to include hash blocking and to monitor network activity to detect unusual repository access or unrecognized WinRAR processes.