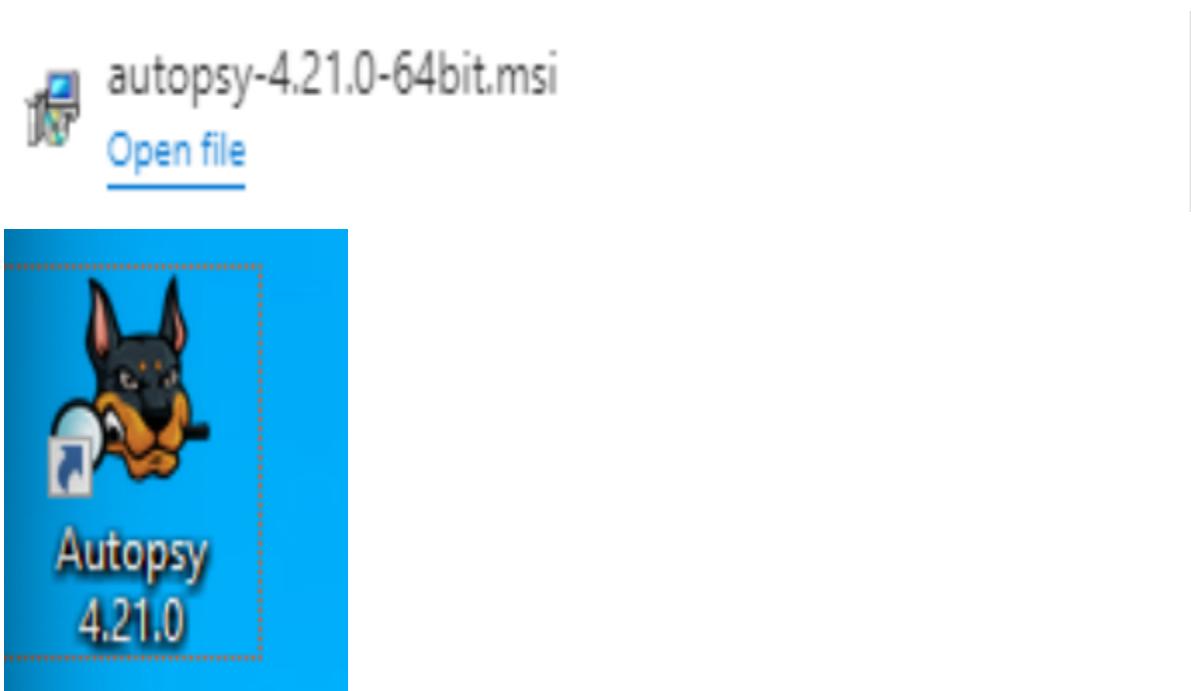


Lab 08-1 - Forensics and Malware Analysis

Task 1

- 1) Installed Autopsy on my Windows VM, navigating through the usual setup steps and handling a few security blocks that tried to prevent the installation.



- 2) Created a new forensic case in Autopsy named "USB Drop," set up the base directory, and added the USB image on Canvas as a data source, selecting all ingest modules for a comprehensive analysis.

Kevin Cendana

CSC 154 - 01

Spring 2024

 New Case Information X

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory: Browse

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

Kevin Cendana

CSC 154 - 01

Spring 2024

 New Case Information X

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number:

Examiner

Name:

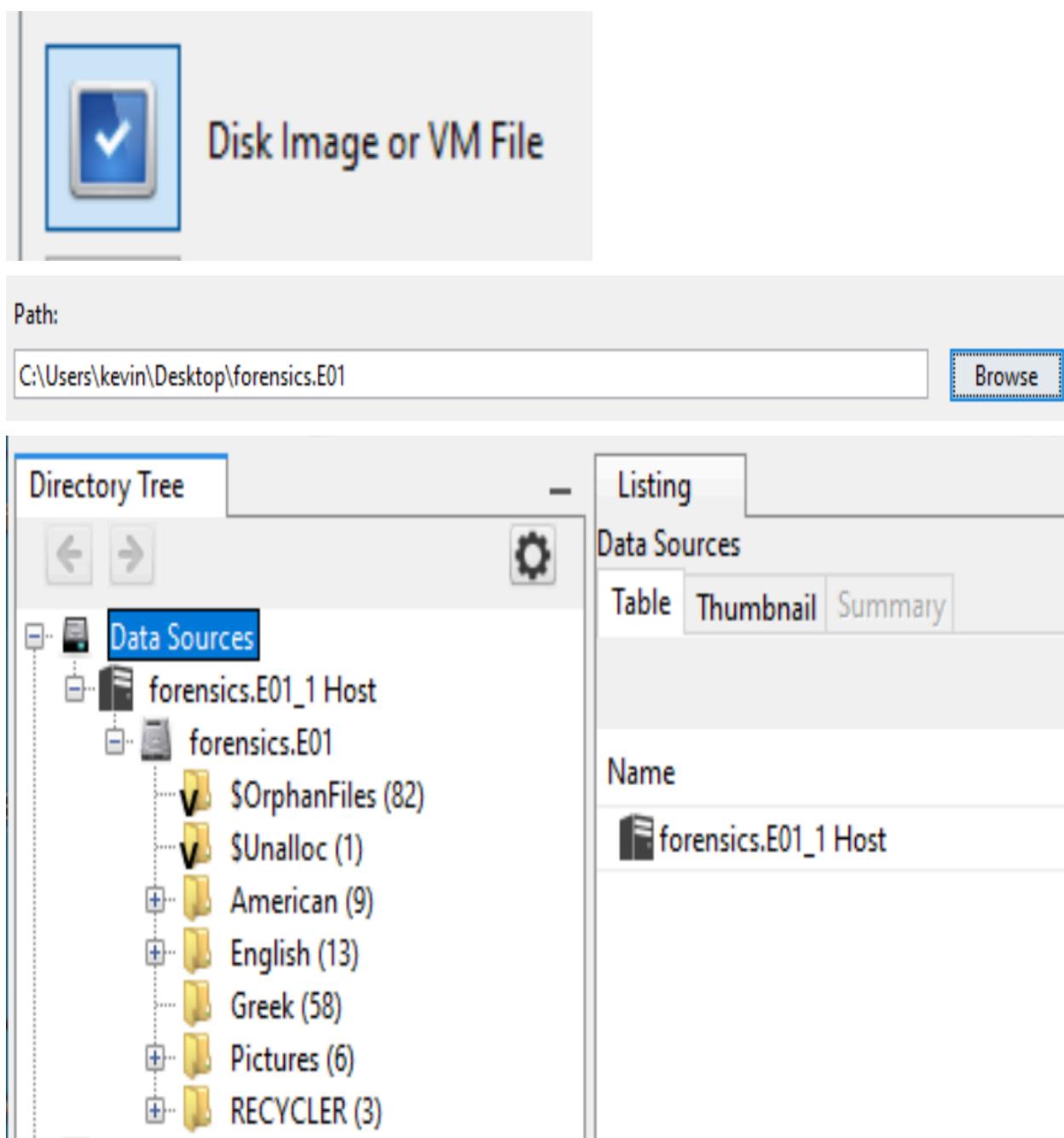
Phone:

Email:

Notes:

Organization

Organization analysis is being done for:



- 3) Used Autopsy's search tools and directory tree to find specific items like email addresses, URLs, and phone numbers, documenting each discovery with screenshots for evidence.

2 Emails: Found with keywords 'footer', '.com'

The screenshot shows a digital forensics tool interface with the following details:

- File List:** A table with three columns. The first column contains file icons and names: "footer.cfm", "footer_files", and "Unalloc_505_1284096_130023424". The second column contains file types: "«footer.cfm«", "«footer_files«", and "#3f6388><a =class=3dfooter". The third column contains URLs: "/img_forensics.E01/E", "/img_forensics.E01/E", and "/img_forensics.E01/\$".
- Navigation:** Below the file list are navigation arrows (left, right) and a "Data Content" button.
- Tab Bar:** A horizontal bar with tabs: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The "Text" tab is selected.
- Content Area:** A large text area containing the following message:

If you have any comments or suggestions about our web site, please send the webmaster an e-mail at
<mailto:Postmaster@esa.doc.gov>
- Buttons:** A "Hide Images" button is located in the bottom left of the content area.

Unalloc_505_1284096_130023424 lmos password codec«kingpin@atstake.com»@stake

Data Content

Data Artifacts Analysis Results Context Annotations

Hex Text Application File Metadata

Strings Extracted Text Translation

Page: 226 of 228 Page ← → Matches on page: 1 of 4 Match ← → 100% Text Source

Severity: Passwords and data can easily be obtained through a backdoor in Palm OS, even if the device is "locked".

Author: Kingpin [kingpin@atstake.com]

2 URLs found by searching 'gov':

The screenshot shows a digital forensic analysis interface. At the top, there are two tabs: 'f0039444.txt' and 'e-gov_benefits_report_2006.pdf'. The 'f0039444.txt' tab is active, displaying file metadata. The metadata includes:

- File location: http://www.publicdebt.treas.gov/icons/bpdlogo2.gif
- File type: image/gif
- Content-Type: image/gif
- Content-Transfer-Encoding: base64
- Content-Location: http://www.publicdebt.treas.gov/icons/bpdlogo2.gif

Below the metadata, there is a 'Data Content' section with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other, and Translation. The 'Text' tab is selected. Under 'Text', there are sub-tabs for Strings, Extracted Text, and Translation. The 'Extracted Text' tab is selected. The text pane displays the following content:

```
[f0039444.txt, -----=_NextPart_000_0062_01C6B407.F467C550
Content-Type: image/gif
Content-Transfer-Encoding: base64
Content-Location: http://www.publicdebt.treas.gov/icons/bpdlogo2.gif]
```

At the bottom of the interface, there are search and navigation controls: 'Page: 1 of 1 Page', 'Matches on page: 1 of 6 Match', zoom controls ('100%', 'Reset'), and 'Text Source: Search Result' buttons.

The screenshot shows a digital forensics analysis interface. At the top, there's a file list for a file named '_EGULA~1.MHT'. Below the file list is a 'Data Content' section with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Text' tab is selected. Under 'Text', there are three tabs: Strings, Extracted Text, and Translation. The 'Extracted Text' tab is selected. It displays the following HTML code:

```
Content-Location: http://www.sec.gov/news/headlines/scamsites.htm
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML lang=3DENG><HEAD><TITLE>Regulators Launch Fake Scam Websites To =
Warn Investors About Fraud</TITLE>
<META content=3D"text/html; charset=3Dwindows-1252" =
http-equiv=3DContent-Type><!-- BEGIN HEADER -->
<SCRIPT language=3DJavaScript =
```

1 Zip File found w/ '.zip' and sort by file type, although I could've used the File Types folder:



1 JPG Metadata found by going into File Types -> Images -> File Metadata

✗ _SCF0144.JPG			2006-04-14 19:17:36 PDT	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT
✗ _SCF0167.JPG	▼		2006-04-14 19:18:06 PDT	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT
✗ _SCF0205.JPG	▼		2004-09-12 10:17:34 PDT	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT
✗ _SCF0544.JPG	▼		2005-03-28 12:38:36 PST	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT
✗ _SCF0550.JPG			2005-03-31 21:04:56 PST	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT
✗ _SCF0555.JPG			2005-04-12 18:00:38 PDT	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT
✗ _SCF0556.JPG	▼		2005-04-12 18:00:38 PDT	0000-00-00 00:00:00	2006-07-30 00:00:00 PDT

< [redacted]

Data Content

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

Metadata

Name: /img_forensics.E01/Pictures/Friends/_SCF0144.JPG
Type: File System
MIME Type: application/octet-stream
Size: 163967
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2006-04-14 19:17:36 PDT
Accessed: 2006-07-30 00:00:00 PDT
Created: 2006-07-30 18:04:21 PDT
Changed: 0000-00-00 00:00:00

1 PDF Magic Byte Hex Code found with File Types -> Documents -> PDF
-> Hex

File Name	Last Modified	File Type
education.pdf	2006-07-30 18:43:58 PDT	0000-00-00 00:00:00
energy.pdf	2006-07-30 18:44:06 PDT	0000-00-00 00:00:00
hhs.pdf	2006-07-30 18:44:14 PDT	0000-00-00 00:00:00
_7msr.pdf	2006-07-30 18:43:10 PDT	0000-00-00 00:00:00
dhs.pdf	2006-07-30 18:44:26 PDT	0000-00-00 00:00:00
message.pdf	2006-07-30 18:43:28 PDT	0000-00-00 00:00:00

Data Content

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

Page: 1 of 17 Page ← → Go to Page: 1 Jump to Offset [] La

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 1/0 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 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 30 30 30 30 30 30 30 .00000000016 0000
0x00000090: 30 20 6E 0D 0A 30 30 30 30 30 30 30 30 30 30 30 30 30 0 n..00000001584
0x000000a0: 30 30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 30 30 31 00000 n..00000001
0x000000b0: 37 38 37 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30 787 00000 n..000

1 File with an Extension Mismatch found in Analysis Results -> Extension Mismatch Detected

The screenshot shows a digital forensic analysis interface. On the left is a tree view of analysis categories:

- File Types
 - By Extension
 - Images (477)
 - Videos (5)
 - Audio (0)
 - Archives (1)
 - Databases (3)
 - Documents
 - HTML (28)
 - Office (21)
 - PDF (62)
 - Plain Text (50)
 - Rich Text (7)
 - Executable
 - By MIME Type
 - Deleted Files
 - MB File Size
 - Data Artifacts
 - Metadata (59)
 - Analysis Results
 - EXIF Metadata (86)
 - Extension Mismatch Det.
 - Keyword Hits (98461)
 - User Content Suspected

On the right, there are two main panes:

- A top pane displays a table of files:

	bbbb.dat	1	File	Likely Notable
	aaaa.dat	0	File	Likely Notable
- A bottom pane titled "Data Content" shows extracted text from a file:

AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS
by Adam Smith
1776
INTRODUCTION AND PLAN OF THE WORK
THE annual labour of every nation is the fund which

- 4) Found a deleted file in Deleted Files -> File System. File Type: .txt, Meta Data & Content in screenshot.

Kevin Cendana

CSC 154 - 01

Spring 2024

The screenshot shows a digital forensic analysis interface with a sidebar navigation menu and a main content area.

Left Sidebar:

- File Types: Audio (0), Archives (1), Databases (3), Documents (HTML (28), Office (21), PDF (62), Plain Text (50), Rich Text (7)), Executable, By MIME Type, Deleted Files, File System (208), All (364).
- MB File Size
- Data Artifacts: Metadata (59)
- Analysis Results: EXIF Metadata (86), Extension Mismatch Det., Keyword Hits (98461), User Content Suspected, OS Accounts.

Main Content Area:

File List:

File Name	Modified	Accessed	Created	Changed
bluebirds.mab	2002-07-22 20:13:30 PDT	0000-00-00 00:00:00	2002-07-22 20:13:30 PDT	0000-00-00 00:00:00
_awk.txt	2006-07-29 20:28:42 PDT	1998-04-27 12:29:14 PDT	0000-00-00 00:00:00	2006-07-29 20:28:42 PDT
Interview.xls				
note to TR.txt	2006-07-29 20:29:04 PDT	0000-00-00 00:00:00	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	2002-07-22 19:11:08 PDT	0000-00-00 00:00:00

Data Content Tab: Hex, Text, Application (selected), File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences.

Metadata Section:

Name:	/img_forensics.E01/_awk.txt
Type:	File System
MIME Type:	application/octet-stream
Size:	48
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2006-07-29 20:28:42 PDT
Accessed:	2006-07-29 00:00:00 PDT
Created:	2006-07-29 20:28:39 PDT
Changed:	0000-00-00 00:00:00

The screenshot shows a software interface for analyzing digital artifacts. The title bar at the top reads "/img_forensics.E01/_awk.txt X". Below the title bar is a navigation menu with tabs: "Data Artifacts", "Analysis Results", "Context", "A", "Hex", "Text" (which is currently selected), "Application", and "File M". Underneath this is another set of tabs: "Strings", "Extracted Text" (which is currently selected), and "Translation". At the bottom of the interface, there are buttons for navigating through pages and matches, with the text "Page: 1 of 1 Page" and "Matches on page: - of - Match".

006 DOC
TREASURYPDF

Task 2

- 1) Installed Yara on my Kali VM and ensured the tool was set up correctly by checking its commands and capabilities like we usually do.

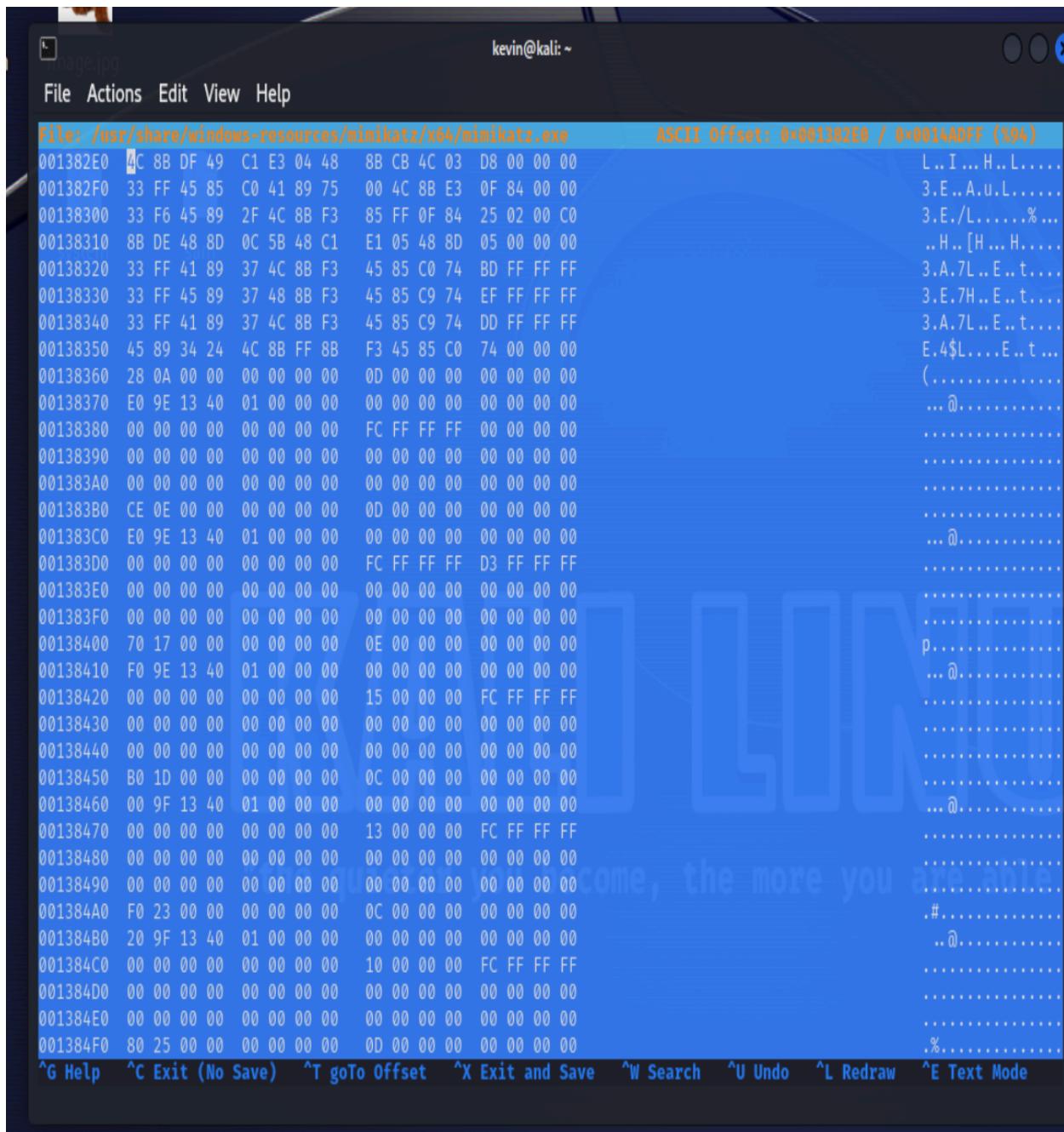
```
(kevin㉿kali)-[~]
$ yara --help
YARA 4.2.3, the pattern matching swiss army knife.
Usage: yara [OPTION] ... [NAMESPACE:]RULES_FILE ... FILE | DIR | PID

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
```

- 2) Ran tools to extract strings and hex codes from Mimikatz, focusing on identifying unique patterns that could be used in a Yara rule to detect this malware on the system.

```
BCryptOpenAlgorithmProvider  
BCryptDestroyHash  
BCryptKeyDerivation  
BCryptHashData  
BCryptFinishHash  
BCryptGenerateSymmetricKey  
BCryptCloseAlgorithmProvider  
BCryptDestroyKey  
BCryptDeriveKeyPBKDF2  
BCryptCreateHash  
BCryptGetProperty  
BCryptEncrypt  
BCryptDecrypt  
BCrypt SetProperty  
BCryptImportKeyPair  
BCryptExportKey  
BCryptFreeBuffer  
BCryptEnumRegisteredProviders  
NCryptOpenStorageProvider  
NCryptGetProperty  
NCrypt SetProperty  
NCryptFinalizeKey  
NCryptFreeObject  
■ The quieter you
```



A screenshot of a terminal window titled "image.jpg" on a Kali Linux desktop. The terminal shows the content of the file "/usr/share/windows-resources/mimikatz/x64/mimikatz.exe". The output is a hex dump with ASCII characters on the right. The terminal prompt is "kevin@kali:~". The bottom of the terminal shows various keyboard shortcuts.

File: /usr/share/windows-resources/mimikatz/x64/mimikatz.exe	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 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 00 FC FF FF FF 00 00 00 00
00138390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001383A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001383B0 CE 0E 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001383C0 E0 9E 13 40 01 00 00 00 00 00 00 00 00 00 00 00	...@.....
001383D0 00 00 00 00 00 00 00 00 FC FF FF FF D3 FF FF FF
001383E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001383F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00138400 70 17 00 00 00 00 00 00 00 0E 00 00 00 00 00 00	p.....
00138410 F0 9E 13 40 01 00 00 00 00 00 00 00 00 00 00 00	...@.....
00138420 00 00 00 00 00 00 00 00 15 00 00 00 FC FF FF FF
00138430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00138440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00138450 B0 1D 00 00 00 00 00 00 0C 00 00 00 00 00 00 00
00138460 00 9F 13 40 01 00 00 00 00 00 00 00 00 00 00 00	...@.....
00138470 00 00 00 00 00 00 00 00 13 00 00 00 FC FF FF FF
00138480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00138490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001384A0 F0 23 00 00 00 00 00 00 0C 00 00 00 00 00 00 00	.#.....
001384B0 20 9F 13 40 01 00 00 00 00 00 00 00 00 00 00 00	...@.....
001384C0 00 00 00 00 00 00 00 00 10 00 00 00 FC FF FF FF
001384D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001384E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
001384F0 80 25 00 00 00 00 00 00 0D 00 00 00 00 00 00 00	%......

kevin@kali:~

File Actions Edit View Help

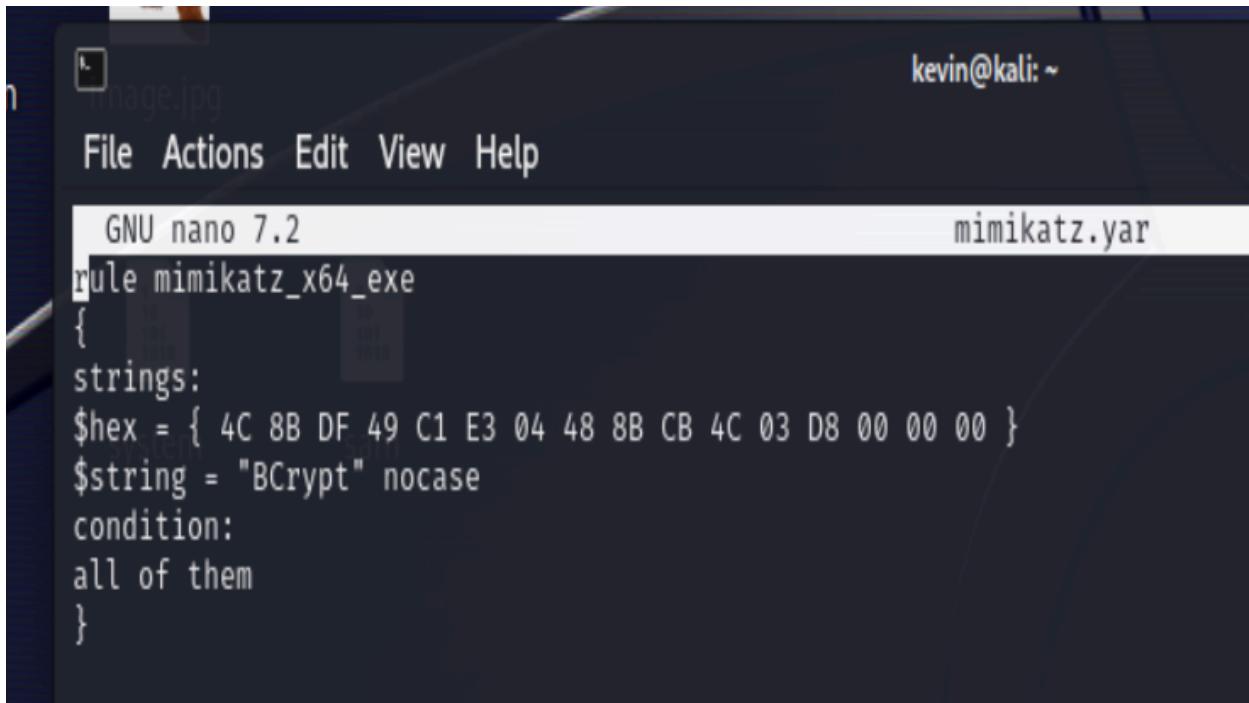
^G Help ^C Exit (No Save) ^T goTo Offset ^X Exit and Save ^W Search ^U Undo ^L Redraw ^E Text Mode

001382E0 4C 8B DF 49 C1 E3 04 48 8B CB 4C 03 D8 00 00 00

L..I...H..L.....

Hex Code: 4C 8B DF 49 C1 E3 04 48 8B CB 4C 03 D8 00 00 00

- 3) Crafted a Yara rule using the Hex code identified in the previous step, ensuring it accurately targeted the specific characteristics of Mimikatz.



The screenshot shows a terminal window with a dark background. At the top, there's a file browser interface with a thumbnail of a file named "image.jpg". To the right of the browser, the text "kevin@kali: ~" is displayed. Below the browser is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal is a text editor titled "GNU nano 7.2". The file being edited is named "mimikatz.yar". The content of the file is a Yara rule:

```
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
}
```

- 4) Executed the custom Yara rule across my Kali VM directories, successfully identifying files that matched the Mimikatz signatures.

The screenshot shows a terminal window titled "kevin@kali: ~". The user has run several commands to generate a YARA rule for the Mimikatz payload:

```
hexeditor /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
hexeditor /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
nano mimikatz.yar
hexeditor /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
nano mimikatz.yar
nano mimikatz.yar
sudo yara -r mimikatz.yar /usr/share/windows-resources
[sudo] password for kevin:
mimikatz_x64_exe /usr/share/windows-resources/powershell-empire/empire/server/csharp/Covenant/Data/ReferenceSourceLibraries/SharpSploit/SharpSploit/Resources/powerkatz_x64.dll
mimikatz_x64_exe /usr/share/windows-resources/powershell-empire/empire/server/csharp/Covenant/Data/EmbeddedResources/SharpSploit.Resources.powerkatz_x64.dll
mimikatz_x64_exe /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
```

Task 3

- 1) Used VirusTotal for static analysis of WannaCry, entering its MD5 hash and reviewing its compilation details and origin.

The screenshot shows the VirusTotal analysis page for the file `ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa`. The main summary indicates a **Community Score** of **64 / 70**, with **64/70 security vendors** and **6 sandboxes** flagged as malicious. The file is identified as `diskpart.exe` and is categorized as an **EXE** file. It was last modified **1 hour ago** and has a size of **3.35 MB**. The threat categories listed include `peexe`, `self-delete`, `long-sleeps`, `direct-cpu-clock-access`, `calls-wmi`, `malware`, `checks-cpu-name`, `runtime-modules`, `checks-user-input`, `overlay`, `detect-debug-environment`, `checks-disk-space`, `executes-dropped-file`, `via-tor`, `checks-network-adapters`, and `macro-create-ole`.

Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, TELEMETRY, and COMMUNITY (30+). A call-to-action box encourages joining the VT Community for additional insights and automation.

Popular Threat Labels: ransomware.wannacry/wannacryptor, trojan, label

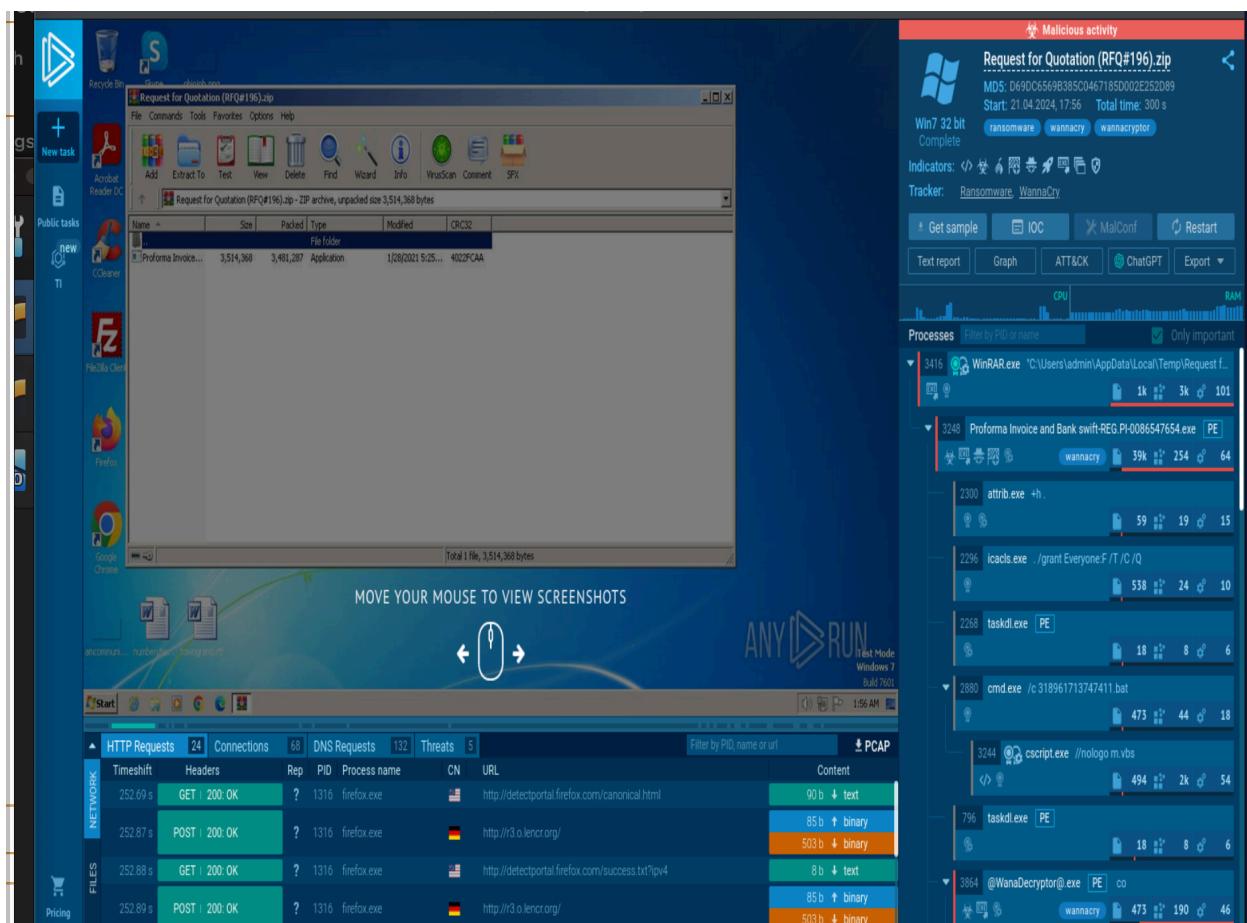
Security vendors' analysis:

Vendor	Analysis	Family labels
AhnLab-V3	Trojan/Win32.WannaCryptor.R200571	Ransom:Win32/WannaCry.ali1020010
AliCloud	RansomWare	Trojan.Ransom.WannaCryptor

Basic properties ⓘ	
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA-1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA-256	ed01ebfbcc9eb5bbea545af4d01bf5f1071661840480439c6e5bab8e080e41aa
Vhash	036046656d1570a8z3631lz1fz
Authentihash	4b2c4c7f06f5ffaaea6efc537f0aa66b0a30c7ccd7979c86c7f4f996002b99fd
Imphash	68f013d7437aa653a8a98a05807afeb1
Rich PE header hash	417a06d07f984f3bce5cd06546c98842
SSDeep	98304:QqPoBhr1aRxsSUDk36SAEdhvxWa9P593R8yAV/p2g3x:QqPe1Cxcxk3ZAEUadzR8yc4gB
TLSH	T173F533F4E221B7ACF2550EF64855C59B6A9724B2EBEF1E26DA8001A70D44F7F8FC0491
File type	Win32 EXE (executable) (windows) (win32) (pe) (peexe)
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) Microsoft Visual C++ compiled executable (generic) (20%) Win64 Executable (generic) (12.7%) Win32 Dynamic ...
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] Compiler: Microsoft Visual C/C++ (12.00.9782) [C++] Linker: Microsoft Linker (6.00.8047) To...
File size	3.35 MB (3514368 bytes)
PEID packer	Microsoft Visual C++
History ⓘ	
Creation Time	2010-11-20 09:05:05 UTC
First Seen In The Wild	2013-05-04 10:00:45 UTC
First Submission	2017-05-12 07:31:10 UTC
Last Submission	2024-04-22 00:20:10 UTC
Last Analysis	2024-04-22 00:20:10 UTC
Names ⓘ	
SuperKeyPass.exe	
diskpart.exe	
notmalware.exe	
1.exe	
WannaCry.EXE	
Endermarch@WannaCrypt0r.exe	

- 2) Explored dynamic analysis submissions on Any.Run for WannaCry, cycling through to observe the malware's behavior through process trees and network activities.

Kevin Cendana
CSC 154 - 01
Spring 2024



3)