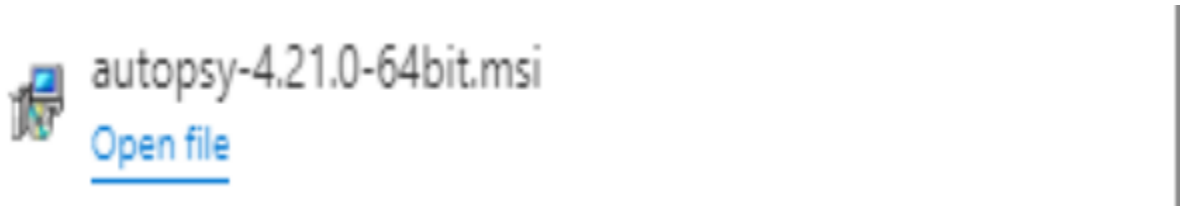
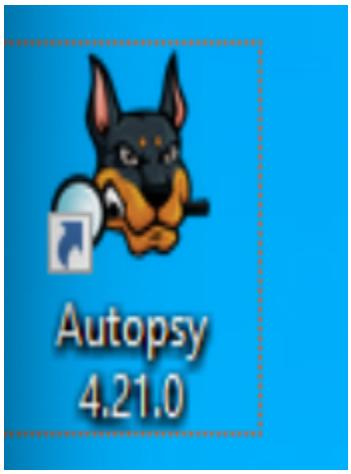
Kevin Cendana
CSC 154 - 01
Spring 2024

Lab 08-1 - Forensics and Malware Analysis

Task 1

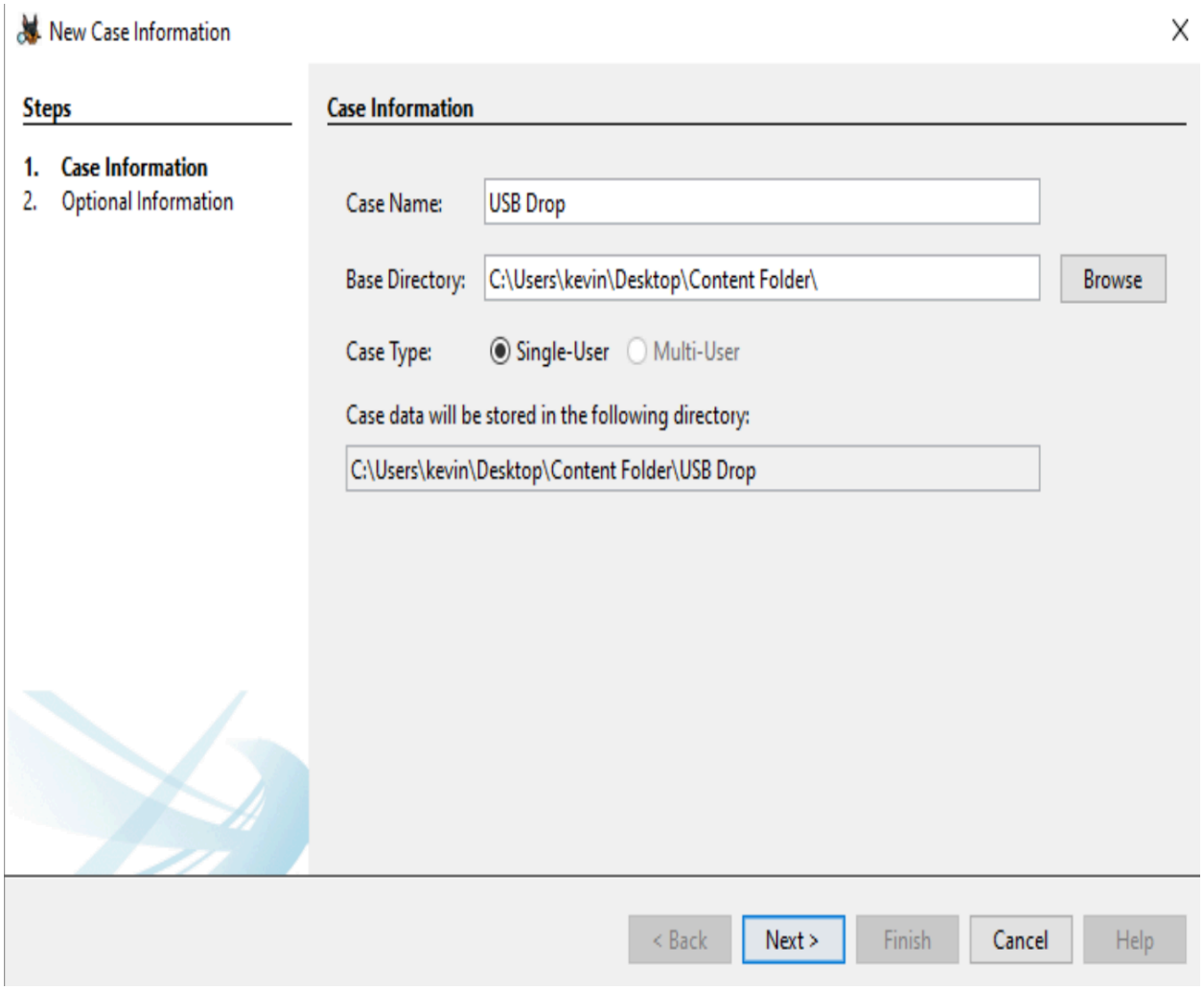
1) Installed Autopsy on my Windows VM, navigating through the usual setup steps and handling a few security blocks that tried to prevent the installation.



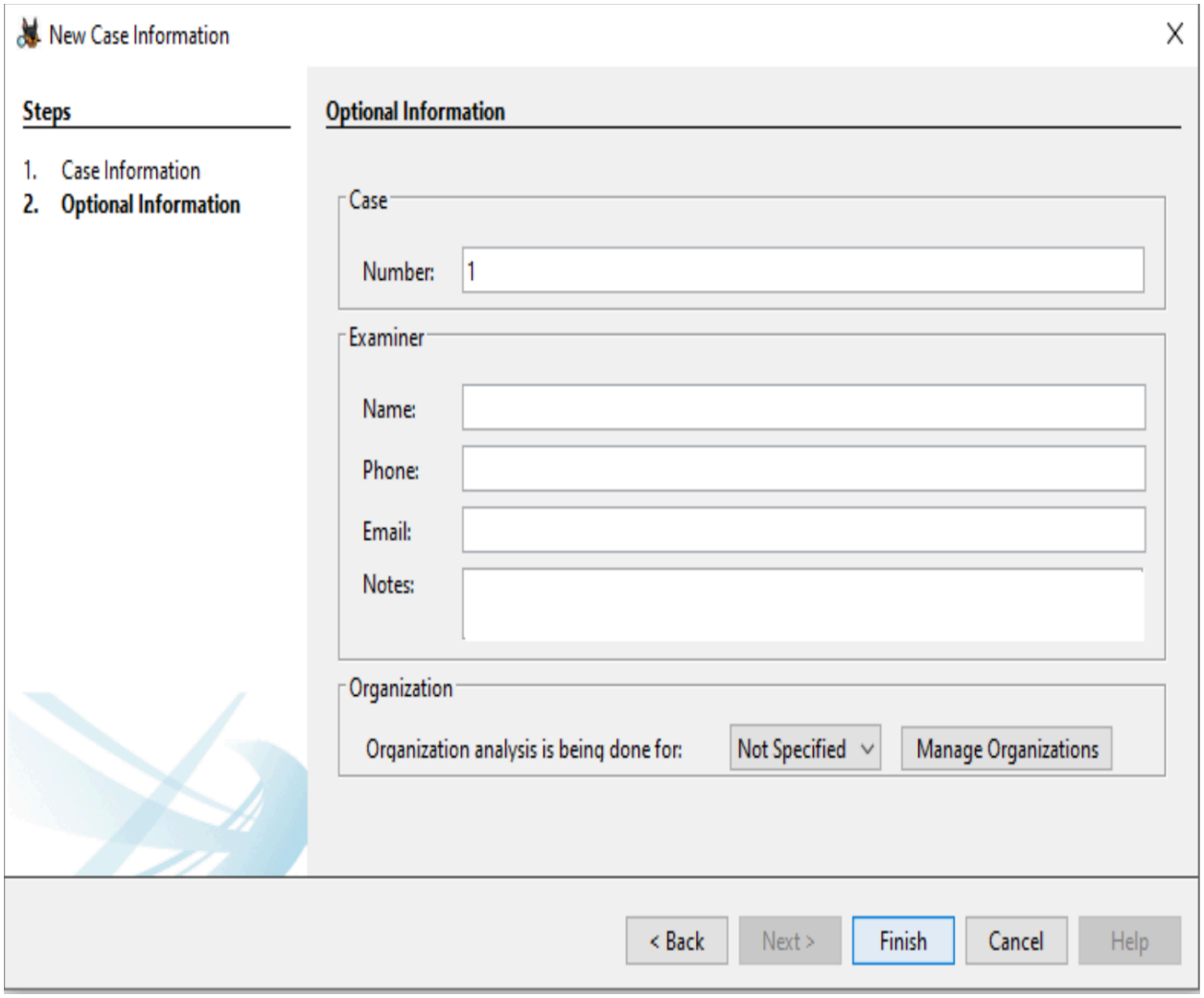


2) Created a new forensic case in Autopsy named "USB Drop," set up the base directory, and added the USB image on Canvas as a data source, selecting all ingest modules for a comprehensive analysis.

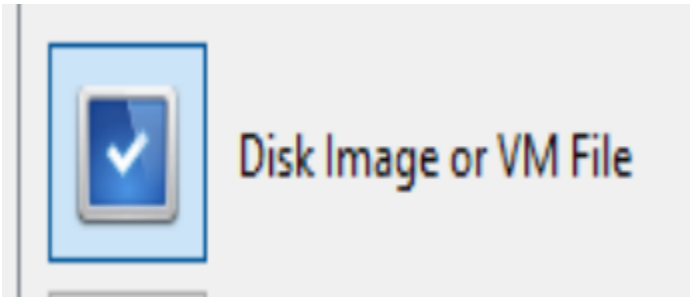
Kevin Cendana
CSC 154 - 01
Spring 2024

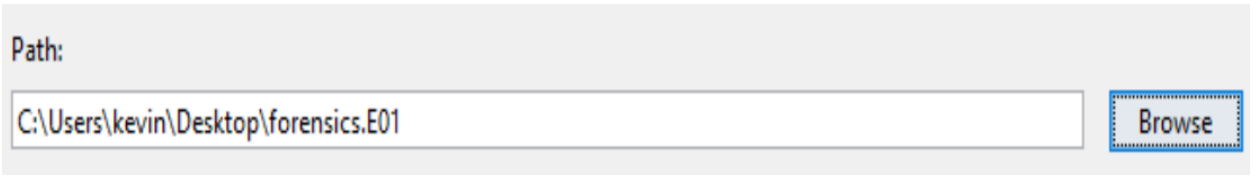


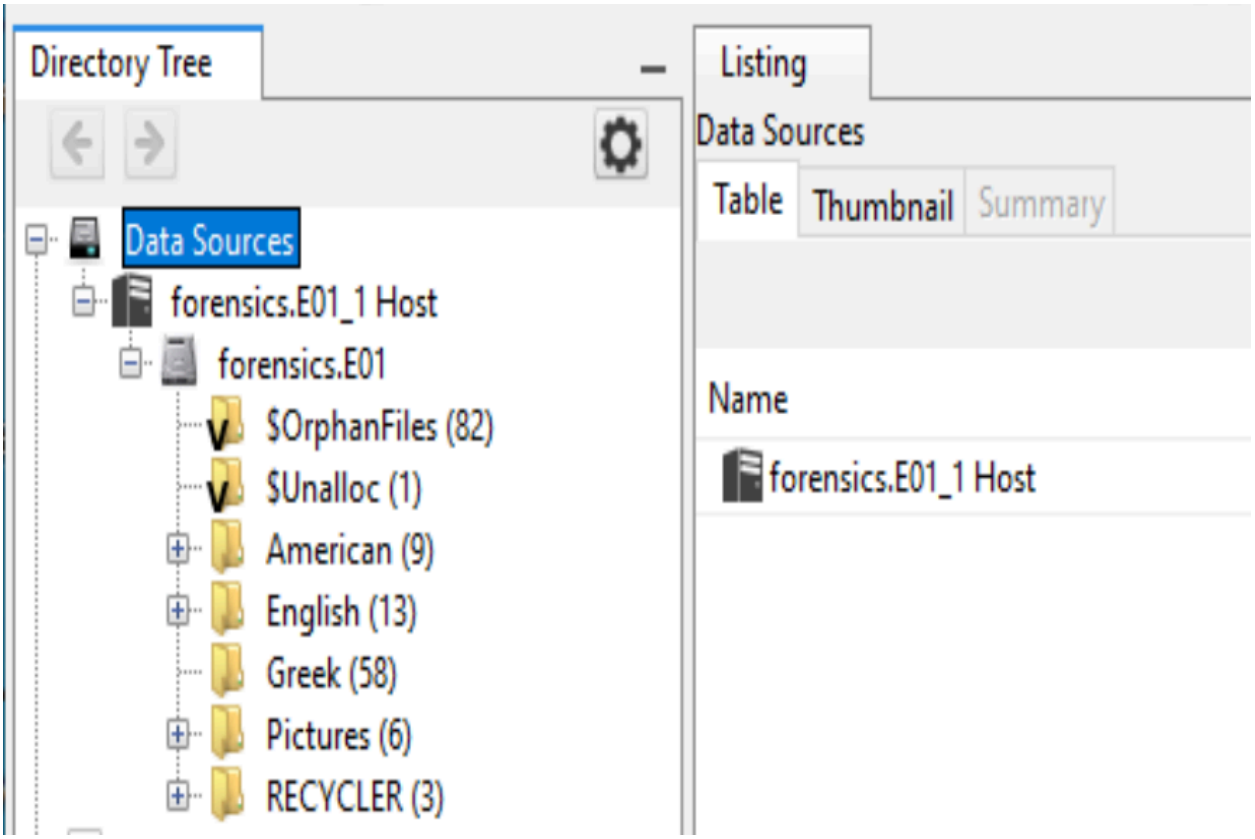
Kevin Cendana
CSC 154 - 01
Spring 2024



Kevin Cendana
CSC 154 - 01
Spring 2024



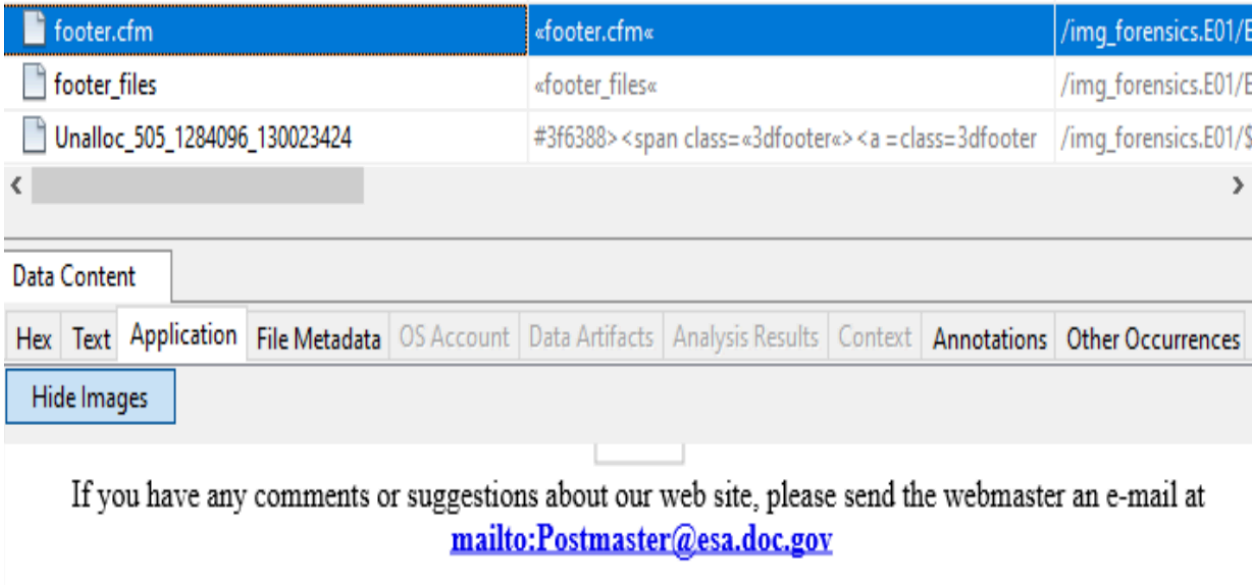




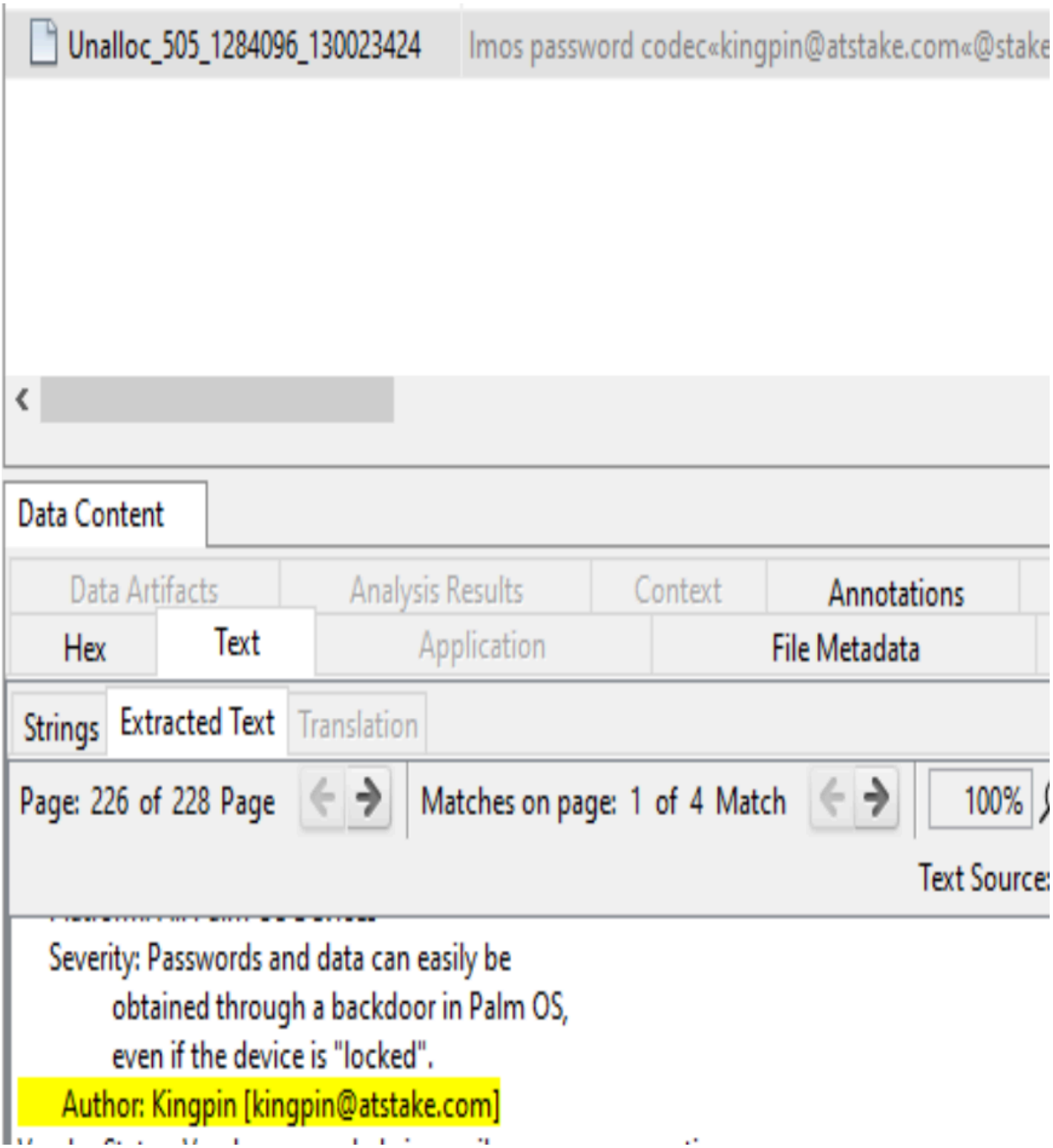
3) Used Autopsy's search tools and directory tree to find specific items like email addresses, URLs, and phone numbers, documenting each discovery with screenshots for evidence.

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

Kevin Cendana
CSC 154 - 01
Spring 2024

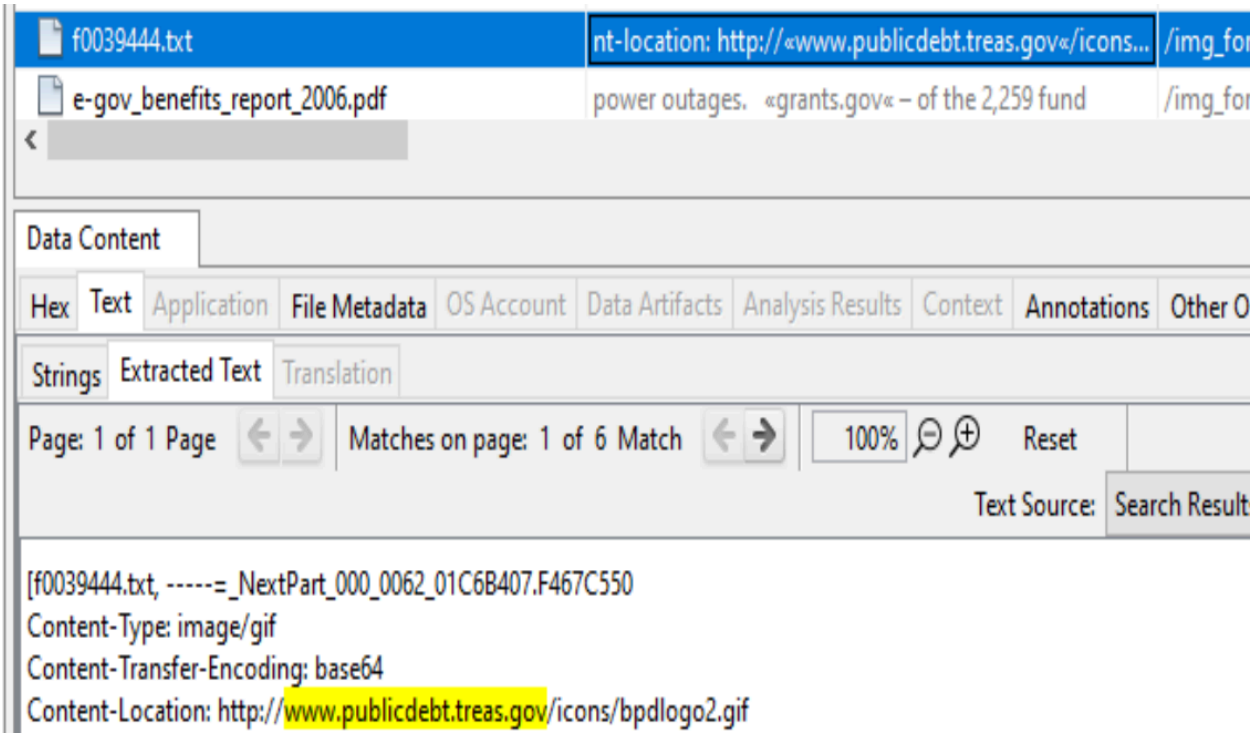


Kevin Cendana
CSC 154 - 01
Spring 2024

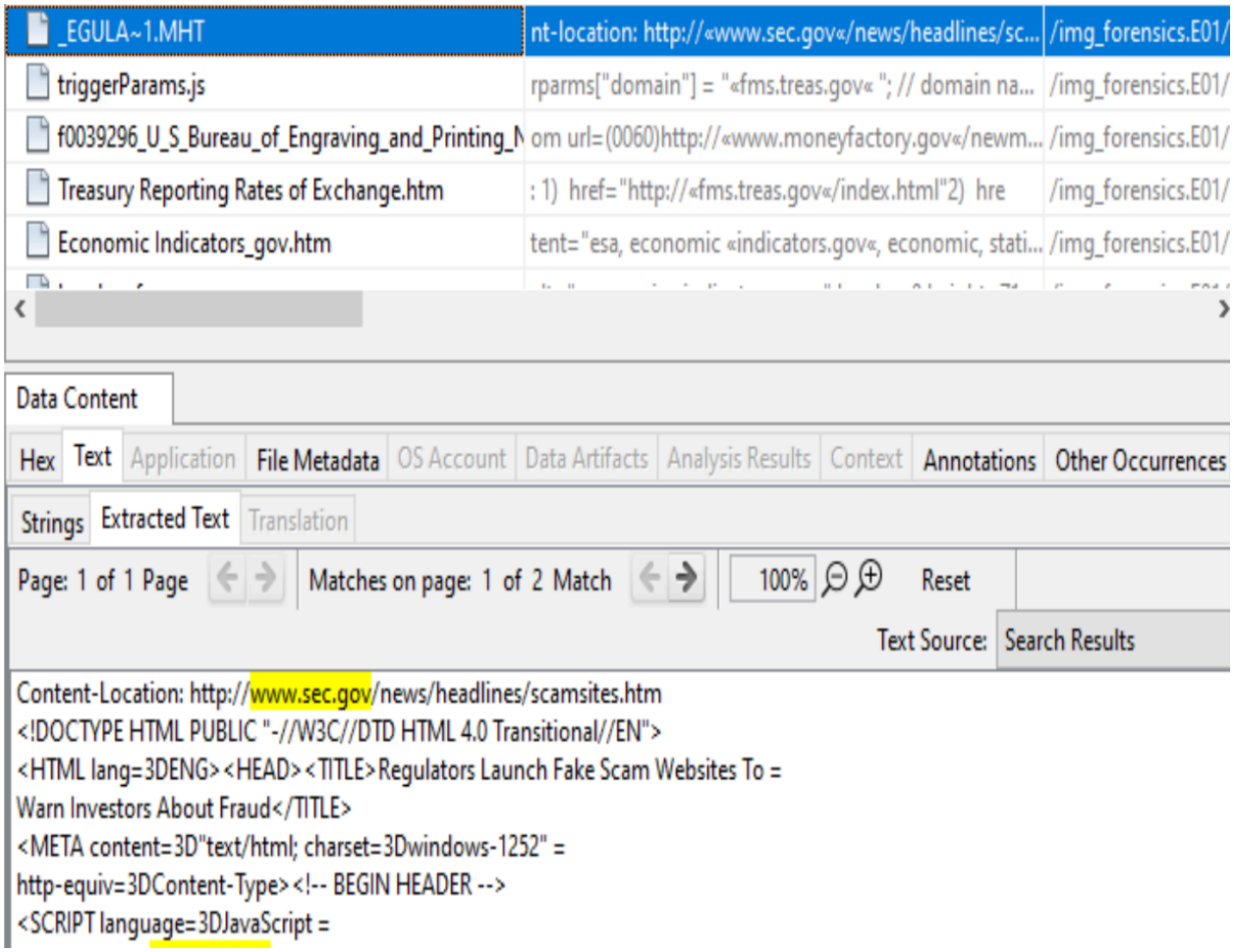


2 URLS found by searching ‘gov’:

Kevin Cendana
CSC 154 - 01
Spring 2024



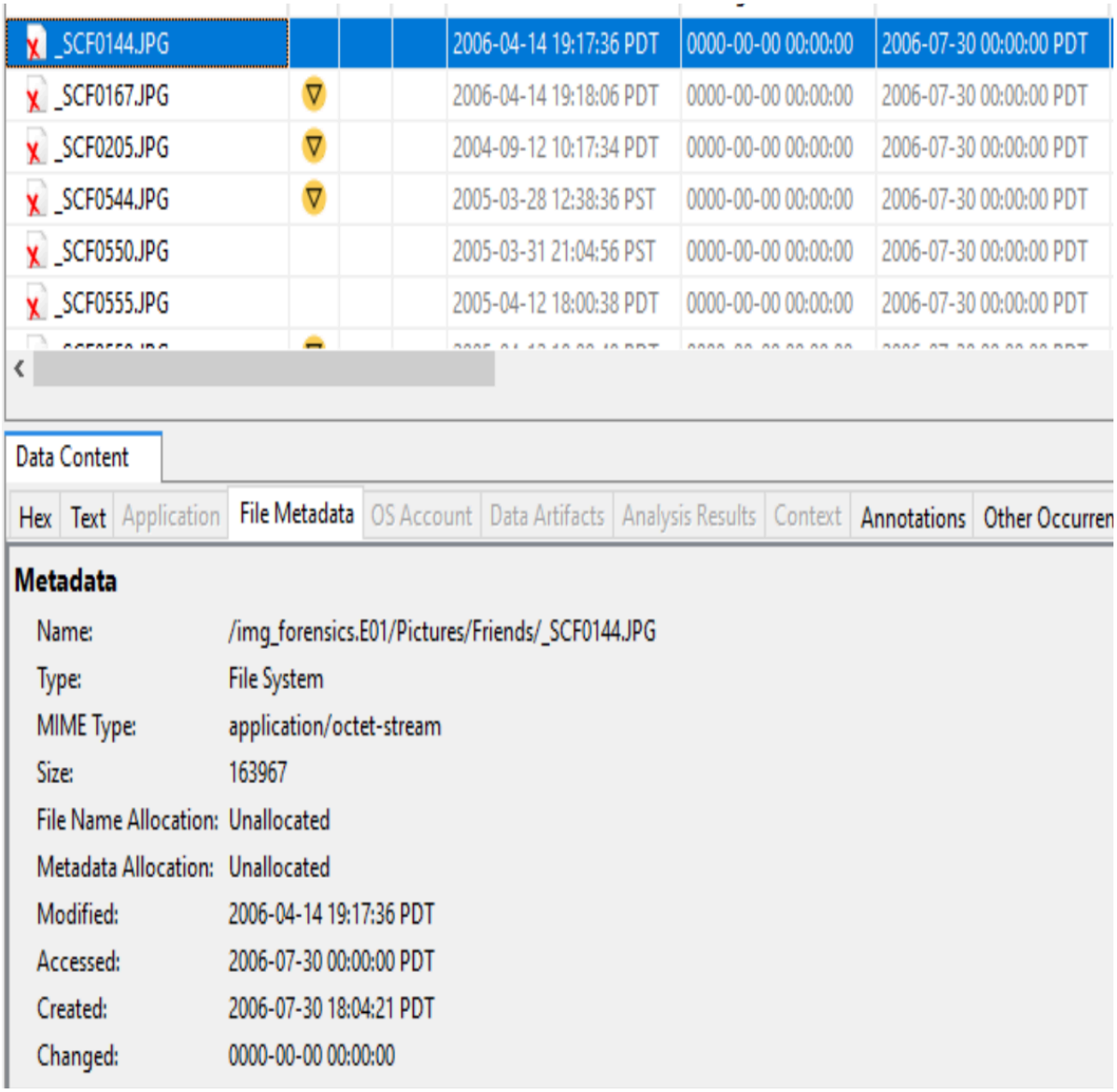
Kevin Cendana
CSC 154 - 01
Spring 2024



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

Kevin Cendana
CSC 154 - 01
Spring 2024



_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

Data Content

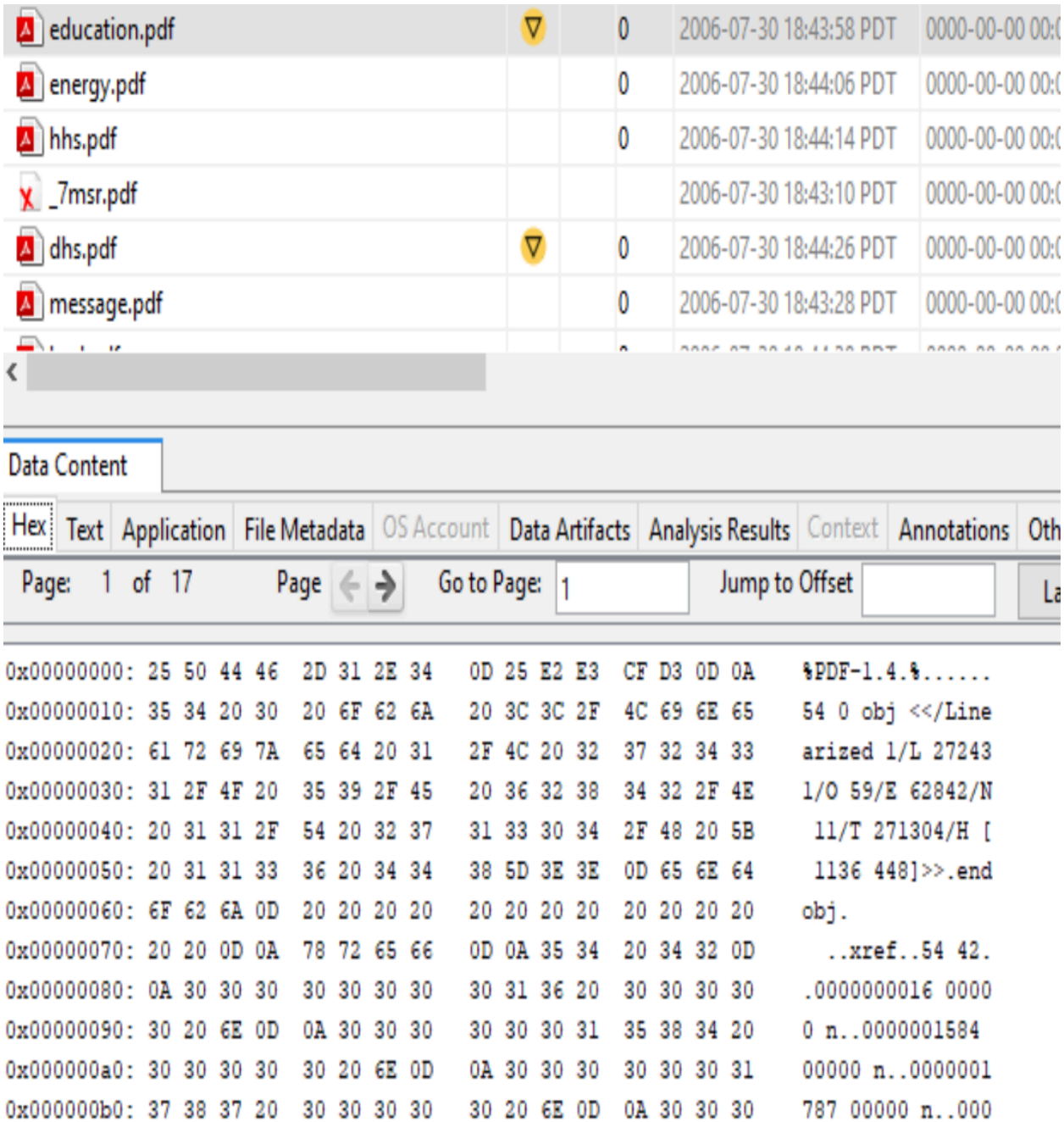
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurren

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

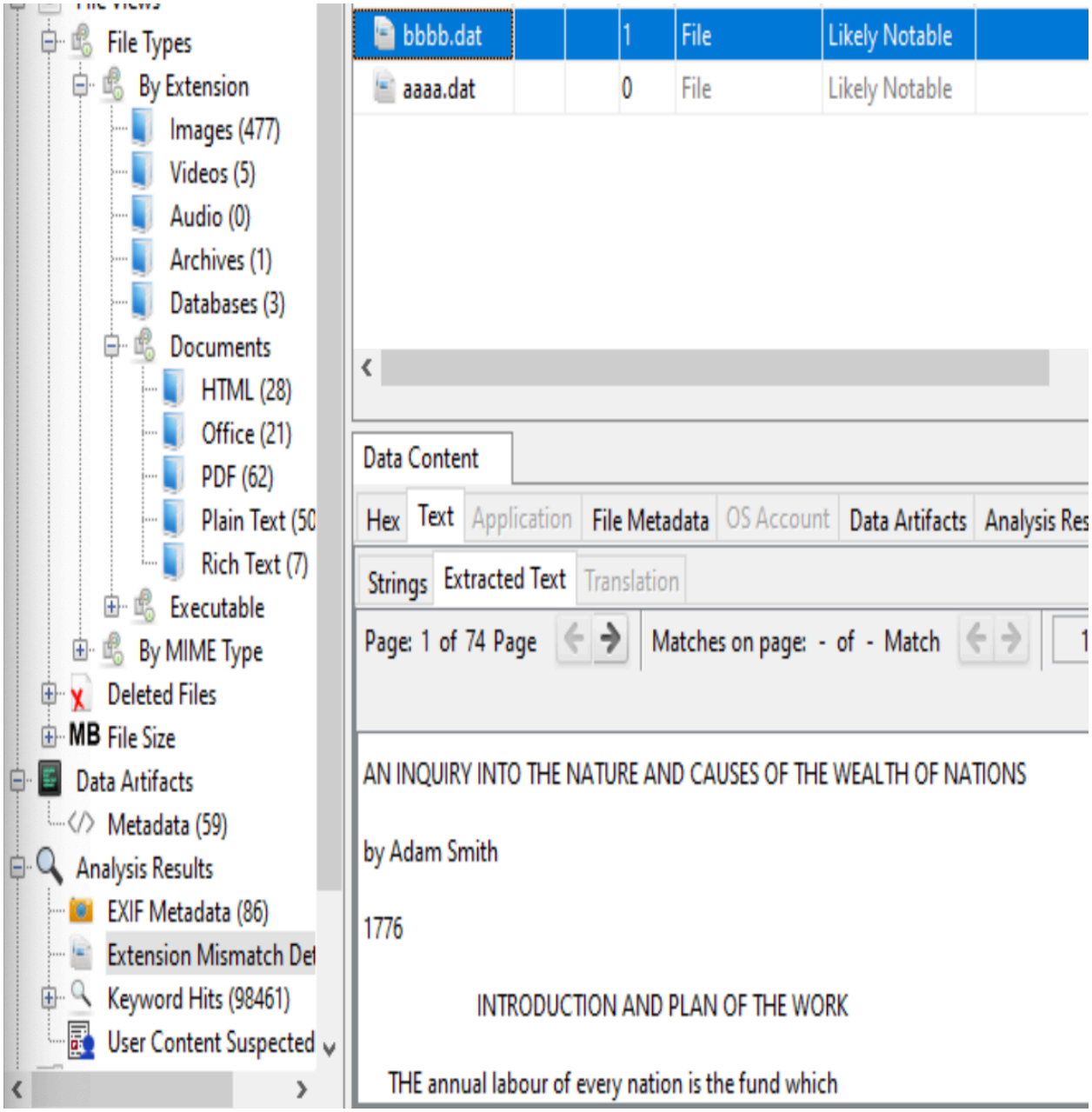
Kevin Cendana
CSC 154 - 01
Spring 2024

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



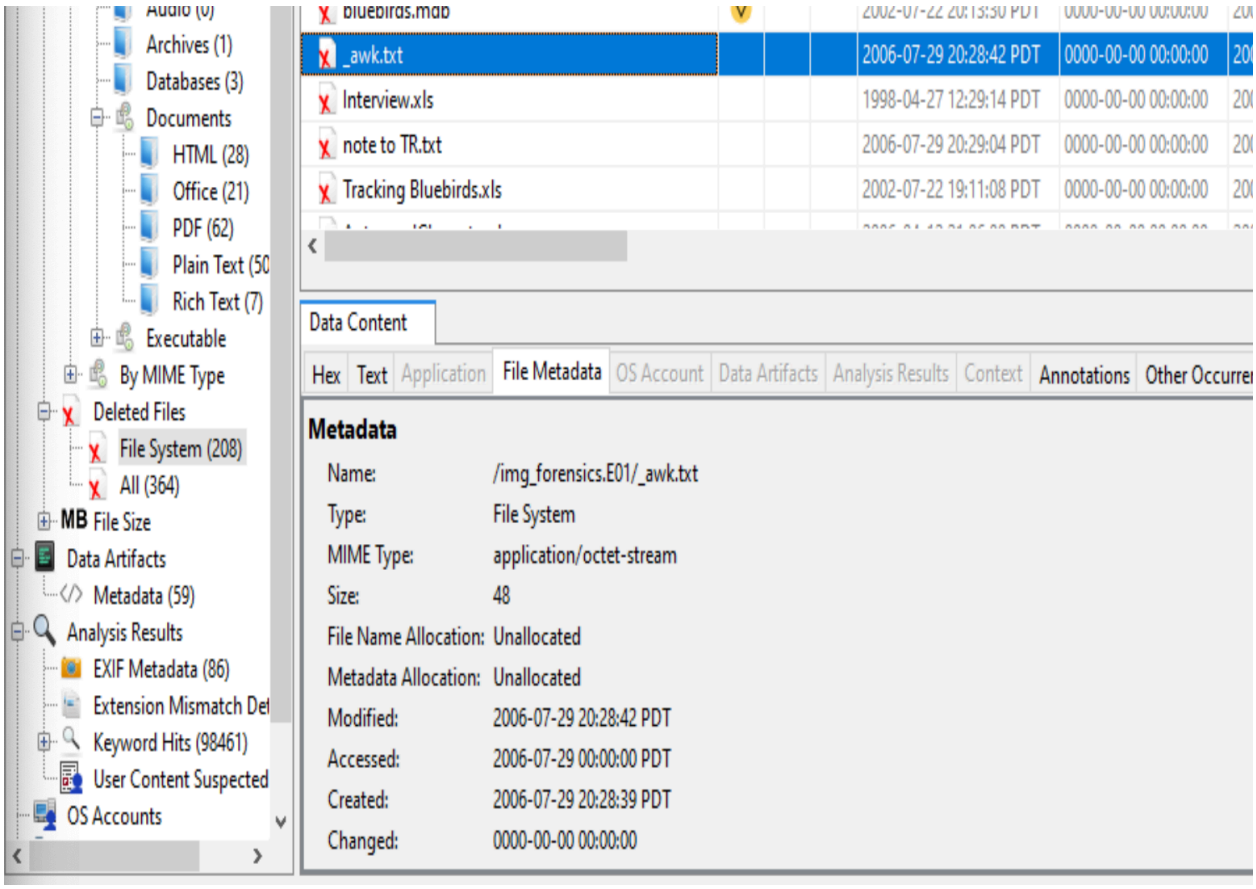
1 File with an Extension Mismatch found in Analysis Results -> Extension Mistmatch Detected

Kevin Cendana
CSC 154 - 01
Spring 2024

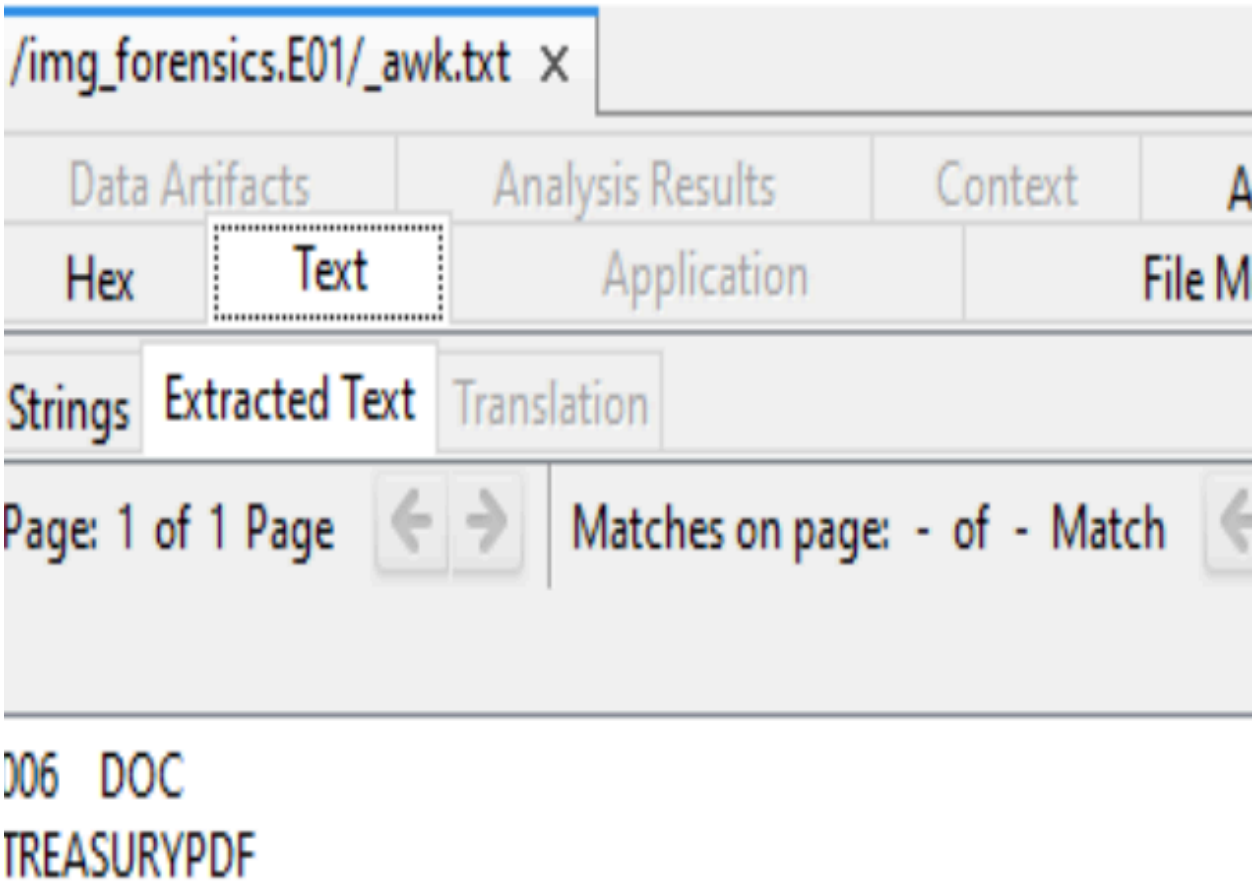


4) Found a deleted file in Deleted Files -> File System. File Type: .txt, Meta Data & Content in screenshot.

Kevin Cendana
CSC 154 - 01
Spring 2024



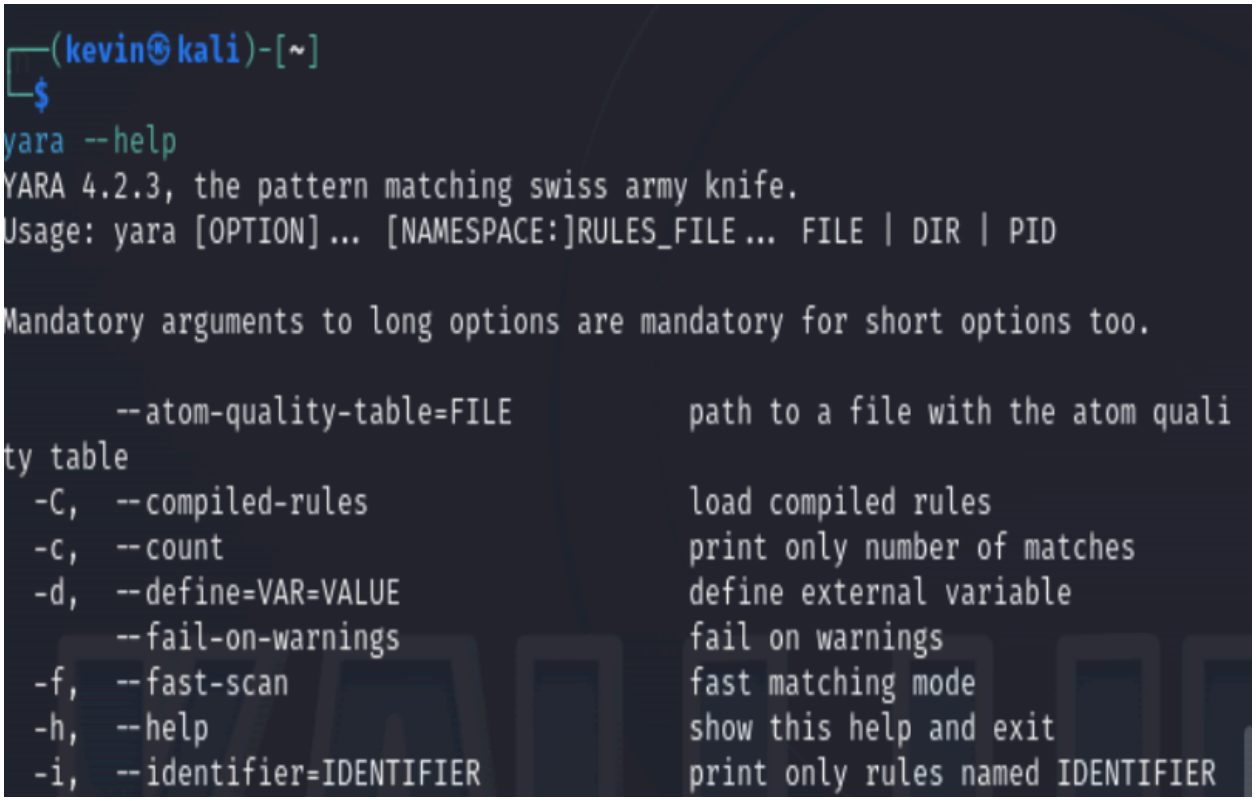
Kevin Cendana
CSC 154 - 01
Spring 2024



Task 2

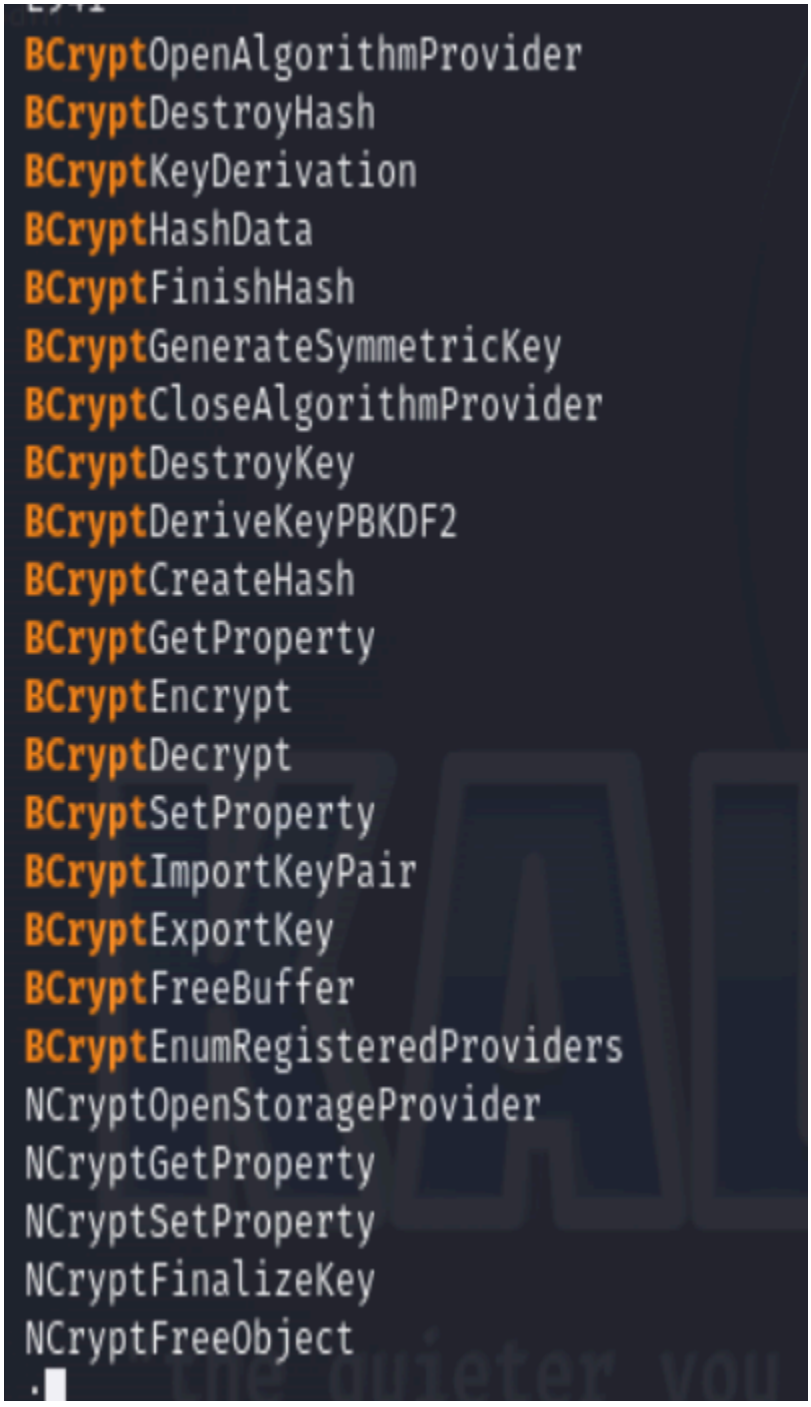
1) Installed Yara on my Kali VM and ensured the tool was set up correctly by checking its commands and capabilities like we usually do.

Kevin Cendana
CSC 154 - 01
Spring 2024

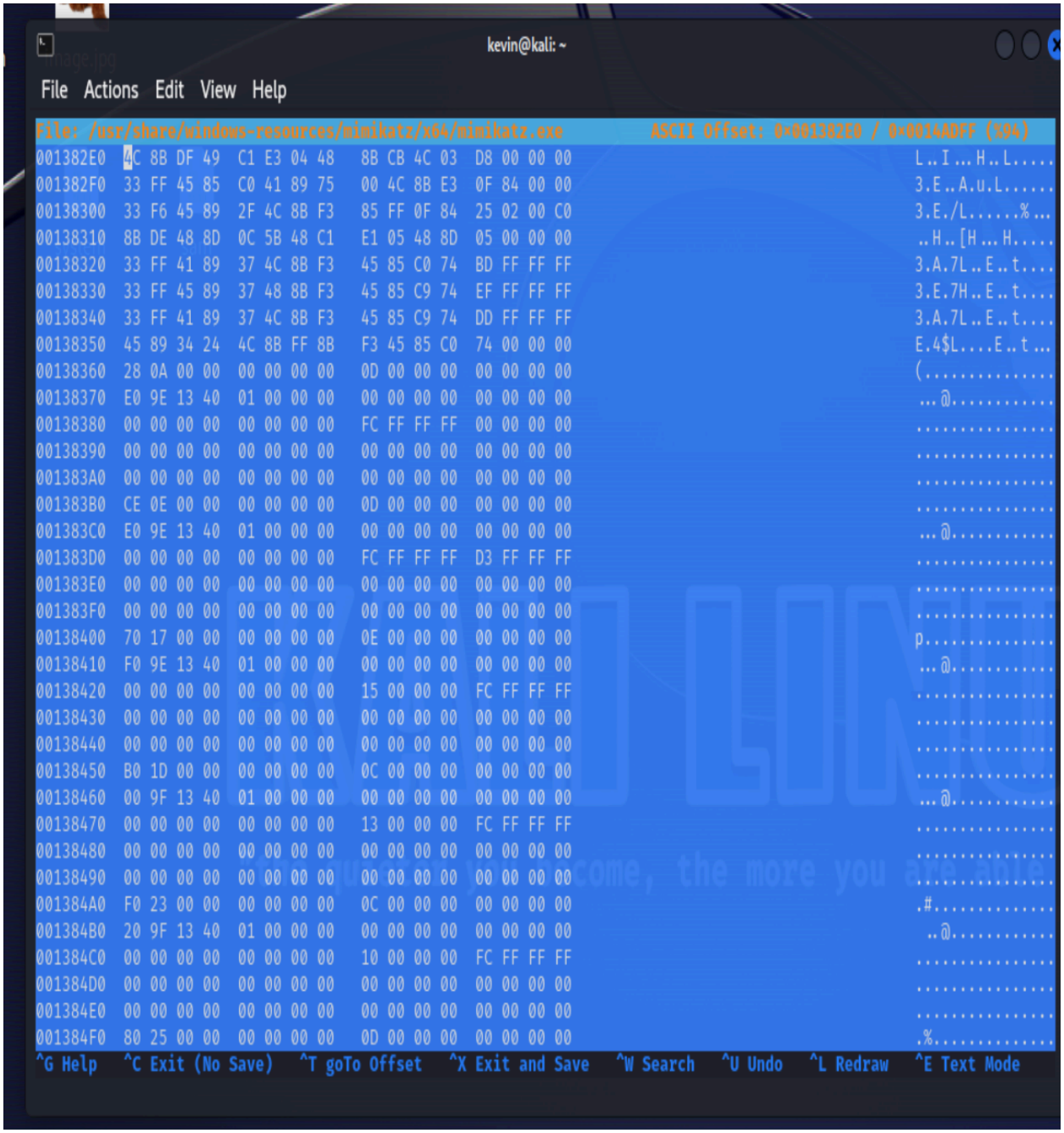


2) Ran tools to extract strings and hex codes from Mimikatz, focusing on identifying unique patterns that could be used in a Yara rule to detect this malware on the system.

Kevin Cendana
CSC 154 - 01
Spring 2024



Kevin Cendana
CSC 154 - 01
Spring 2024

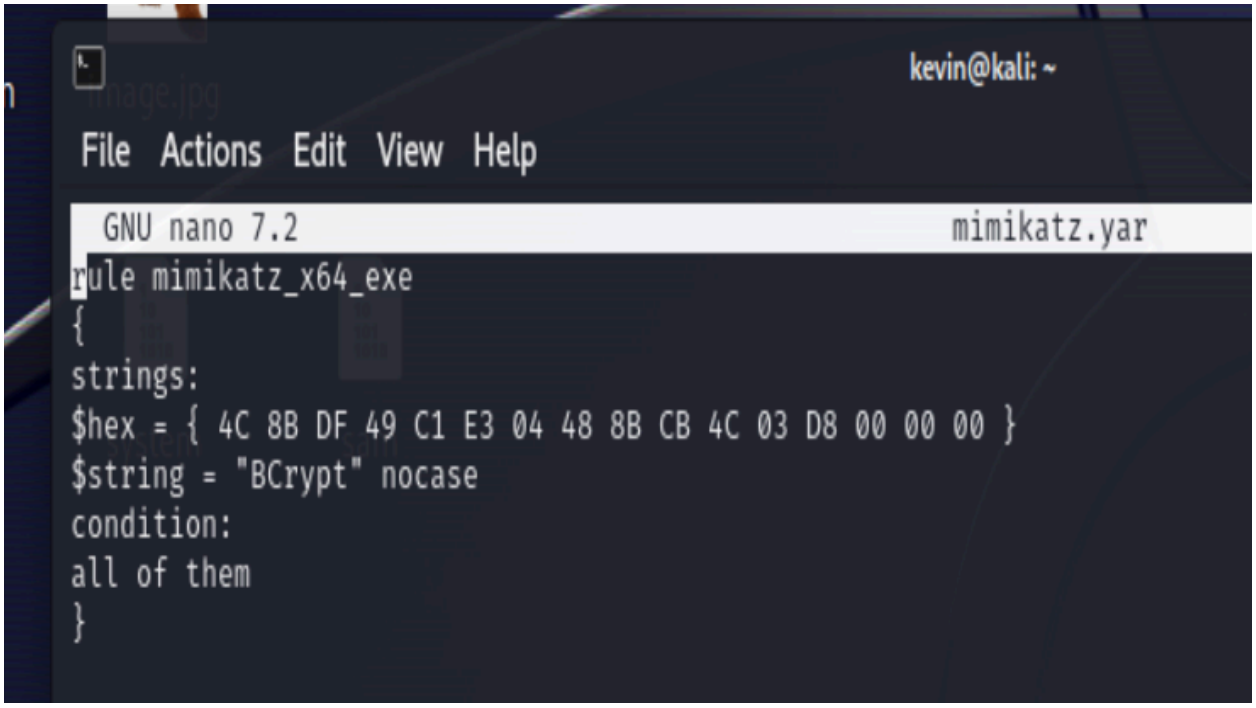


001382E0 4C 8B DF 49 C1 E3 04 48 8B CB 4C 03 D8 00 00 00
L..I...H..L.....

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

Kevin Cendana
CSC 154 - 01
Spring 2024

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



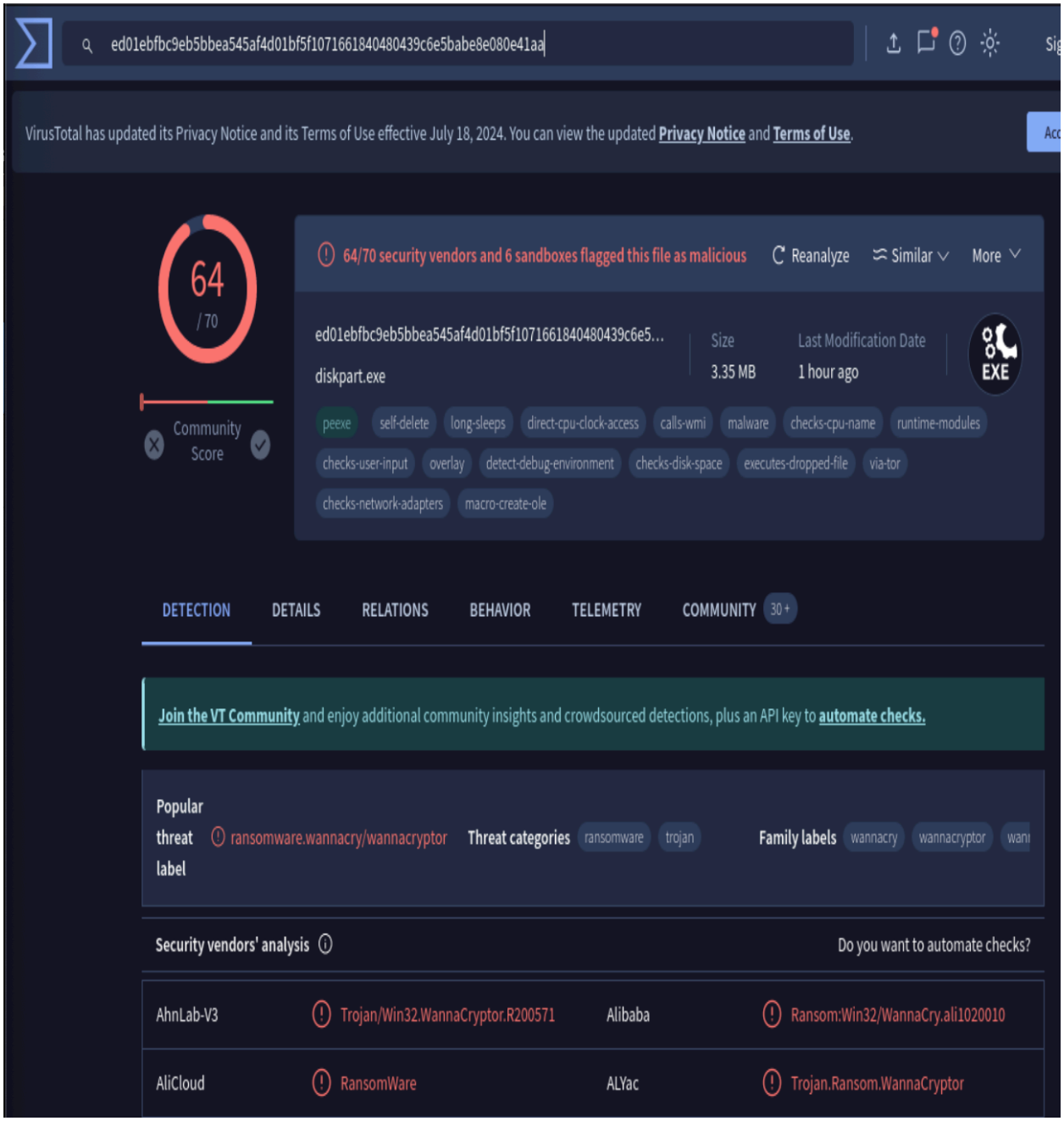
4) Executed the custom Yara rule across my Kali VM directories, successfully identifying files that matched the Mimikatz signatures.

Kevin Cendana
CSC 154 - 01
Spring 2024

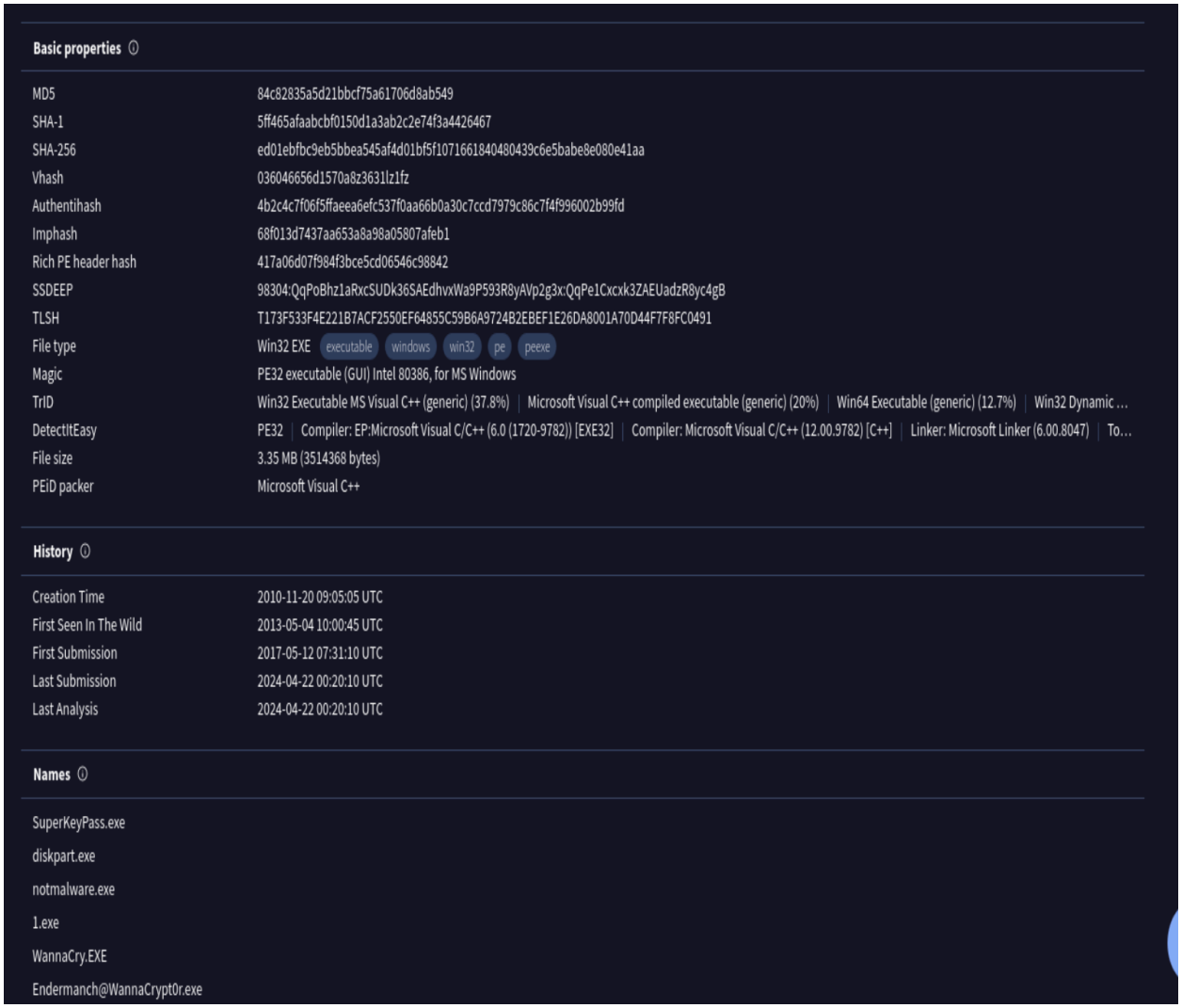
Task 3

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

Kevin Cendana
CSC 154 - 01
Spring 2024



Kevin Cendana
CSC 154 - 01
Spring 2024



Basic properties

MD5	84c82835a5d21bbcf75a61706d8ab549
SHA-1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA-256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Vhash	036046656d1570a8z3631lz1fz
Authentihash	4b2c4c7f06f5ffaeea6efc537f0aa66b0a30c7ccd7979c86c7f4f996002b99fd
Imphash	68f013d7437aa653a8a98a05807afeb1
Rich PE header hash	417a06d07f984f3bce5cd06546c98842
SSDEEP	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x: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

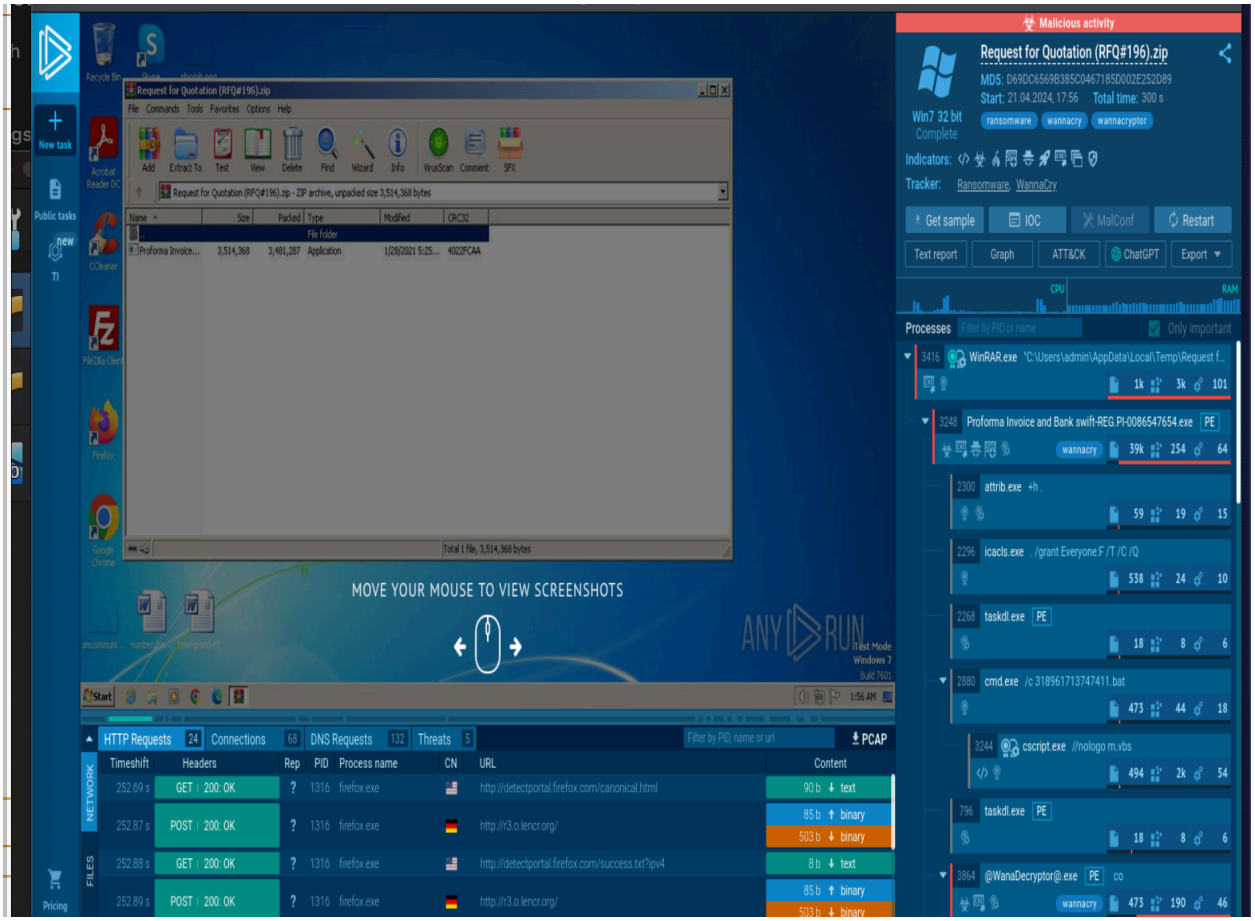
Creation Time	2010-11-20 09:05:05 UTC
First Seen In The Wild	2013-05-04 10:00:45 UTC
First Submission	2017-05-12 07:31:10 UTC
Last Submission	2024-04-22 00:20:10 UTC
Last Analysis	2024-04-22 00:20:10 UTC

Names

SuperKeyPass.exe
diskpart.exe
notmalware.exe
1.exe
WannaCry.EXE
Endermanch@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)