Introduction to Digital Forensics:

CIS2204

Clinton Opara

U2164507

Serving as the Senior member of the digital investigation unit in west Yorkshire police, I have been tasked in formulating this technical report which portrays my findings through this digital forensic investigation. The suspect in question denies any involvement, however the evidence does relay back to the individual.

Assuming that best practices for on crime scene was taken to document and preserve data, this document has passed integrity check. Using virtualisation and Microsoft remote desktop, a virtual machine was created for the investigation and toolkit to run robustly without having to wipe my Mac's memory and storage blocks. Digital forensic readiness is advised for the bank, despite their best efforts.

Despite the bank's strong security measures in place, the attacker(s) still managed to gain, steal and exploit both staff and customers' personal details. Despite following fraud prevention protocols, this has caused financial loss, reputation, and legal challenges. This document is for non-expert readers also.

Task 1:

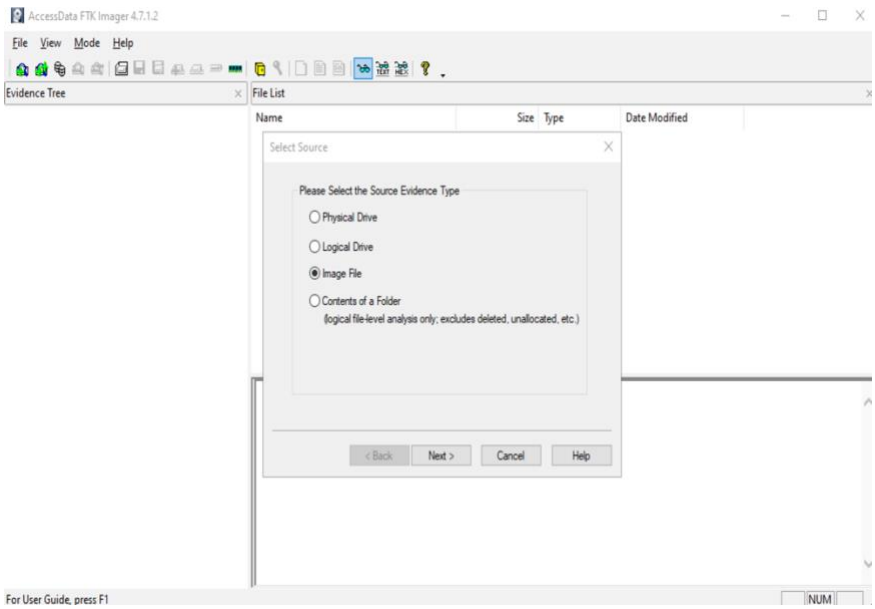
	FTK Imager	Encase	Autopsy	Paladin 4.0
Encryption	Yes	Yes	Yes	Yes
Decrypt	Yes	No	Yes	Yes
Capture Memory	Yes	Yes	Yes	Yes
Compression	Yes	Yes	Yes	No
Carving Fragmentation	Yes	Not with integrity	Yes	Yes
Hash	SHA1 MD5	SHA1 MD5	SHA1 MD5	SHA1 MD5
Write block				Yes
Built in reports	Yes	Yes	Yes	Yes

There is a very strict conduct that DF practitioners must abide by, luckily, we have guidelines constituted by global and national organisations such as the homeland security division in the US, and the closer NIST organisation here in the UK, alongside others.
These guidelines are appraised according to the region's legal stances and citing; however, there are order of operations that speak to practitioners across the globe in unity. The CFTT program act as purpose-built guidelines to efficiently convey the order of operations and cautions to take place. For the suspect's laptop, android tablet, and SSD, I used NIST DF:

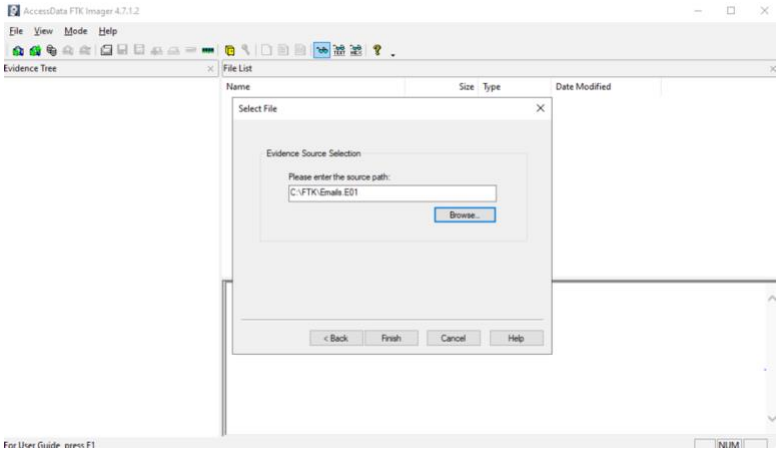
Tool Name: FTK Imager
Operating system: Windows 10
Testing Organisation: West Yorkshire Police

FTK Imager is a tool used in digital forensics and is used to conduct investigations and collecting evidence digitally. Using forensic imaging process, I will demonstrate how the FTK imager was used. I firstly started the Azure Virtual machine.

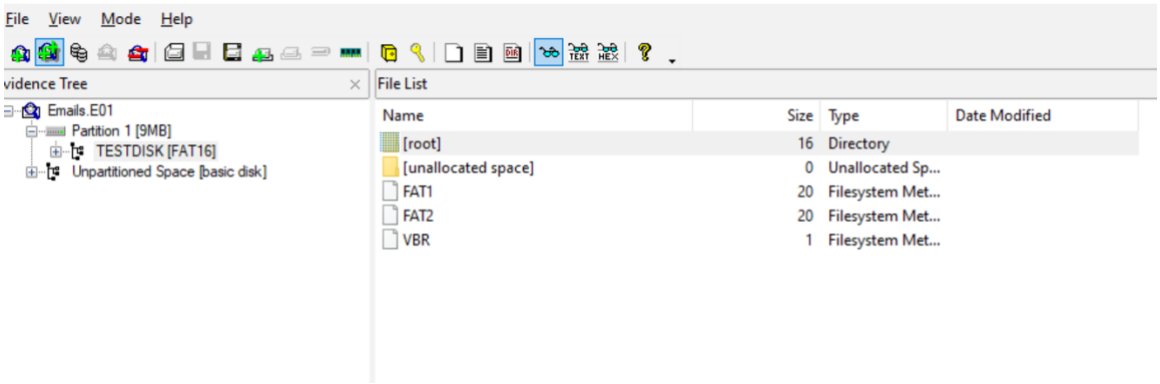
Assuming the data quality of the provided source is free from any contamination, I firstly launched the FTK Imager app, I then used data and created a digital image of the source:



I then chose my source selection which can be seen by the GUI below:

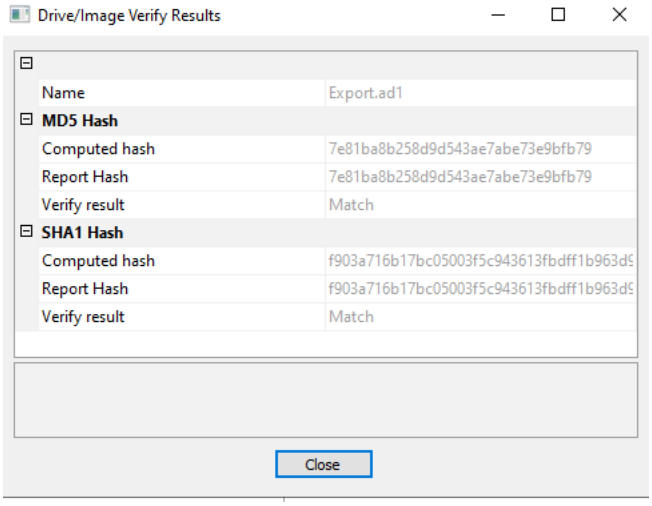


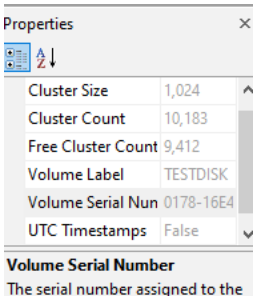
The software started successfully because the kernel, which is the core software that connects the hardware components, which in this case is the motherboard and CPU, to the software components which is the FTK Tool. Moreover, a software write blocker was used to block any interferences, and to keep the data integrity in check throughout the process.



SEDs are not too difficult to possess or even make, therefore having a tool that can decrypt the suspect's laptop is essential. SEDs are remote and the suspect could have remotely encrypted files. Therefore, FTK imagery is a good tool for the laptop, and upon testing, the tool managed to access RAM within approximately 57 seconds, so time efficiency is also involved. as this fact helps maintain authenticity of my in-depth investigation, and completeness of the provided data. I strongly believe that FTK Imager tool should be used for the data acquisition of the persistent storage on the laptop. The suspect's laptop has access to the bank's private network, personal information's and other sensitive information's stored in the network, or on the new technology file system (NTFS). Moreover, I used hash to verify the reliability of not only the software, but also if I was following guidelines.

Below, I used the hash value to determine whether the integrity was kept before advancing to the examination and report section of the NIST. The hash created for the original image, which is the evidence, should match the copied image.





As shown above, the cluster size is smaller than the cluster count, this means that 4KB, which is the default cluster size x 256 is what equals the largest volume size that can be stored.

Having said this, the imager has been used to create an image file of the evidence source, which is a laptop the suspect uses daily for work purposes without contaminating or condemning the integrity of the evidence. However, FTK has a not too difficult to comprehend user interface, which a non-expert would not find too difficult to follow. Due to the fact that FTK Imager operates well with Windows, FTK is exceptional when it comes to NTFS, this is because the metadata in the files were mirrored. This means that even the deleted files can be recovered with FTK possibly even using external software too: hexadecimal converters. The laptop is operating on a magnetic disk, data can be hidden and ASDs can be used by the suspect. FTK was used to analyse the MFT, partition 1 is good at managing metadata, and due to it's lack of limits using soft write blocker and the ftk imager .. The scientific methodology used, through NIST, is digital forensic processing model.. due to lack of standardisation, I chose to use NIST processing model. NIST is collection, examination, analysis, then reporting.

Tool Name: Autopsy Imager
Operating system: Windows 10
Testing Organisation: West Yorkshire Police

Paladin lacks in integrity when it comes to encrypt and decrypt, hence why not a good option.

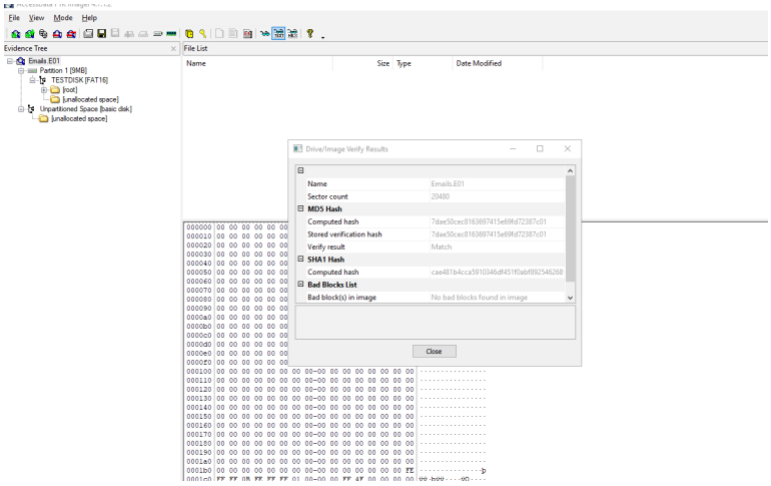
For the android tablet I chose autopsy because of how scalable the tool is. The tool can work with image file, physical and logical evidence types. The tablet is much more portable which means that the suspect could have accessed the network via spoofing his location over several geographical locations and more user friendly and works off linux kernel open source operating system. Through autopsy tool, I can see the geographical location of the device over a stretched amount of time. Moreover, deleted files on the tablet can be swiftly recovered.

Physical addresses were once hardcoded into file systems, but not anymore. It provides forensic capabilities for taking forensic snapshots of both physical and logical memory, reading forensic snapshots, decrypting data, and reporting of digital evidence.

Due to both technical and judicial reasons, I believe that the autopsy tool is again the best for the SSD drive because tool is best because of how the SSD functions. SSDs have short life spans and are commonly used to store images as secondary storage. Precisely, an Operating system can be kept on SSDs and be used for malicious intent. SSDs can typically rewrite from 3000 to 100000, but as the investigator I do not know if the SSD has already started to rewrite certain data that are needed for the investigation. Moreover, due to how vulnerable SSDs can be to data loss, autopsy tool can implement cryptographic hashing to verify the integrity of the disk and log any input and output errors. When the SSD was communicating with the work device, memory was saved into it and each cell takes one bit typically, so each cell becomes allocated. To avoid for instance, the plugged in SSD to communicate with the journal, and the journal writing, saving or feeding information back to the SSD, the autopsy tool is used.

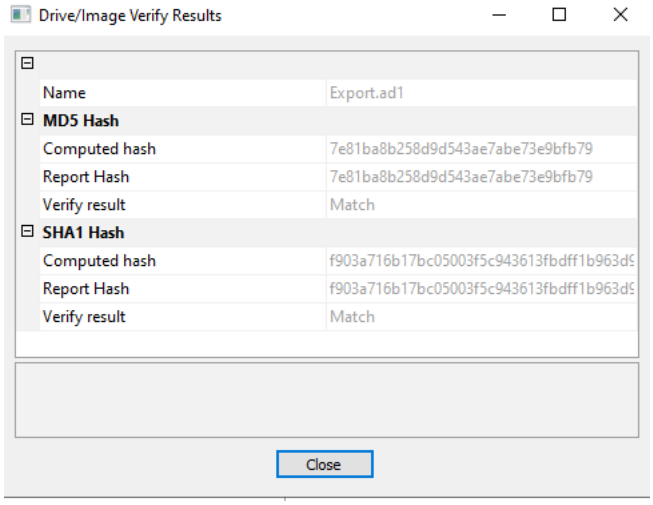
I have made sure that this takes place in a forensically sound manner by making sure that data integrity is kept, and improper methodologies are avoided as this can damage the integrity and accuracy of the court case.

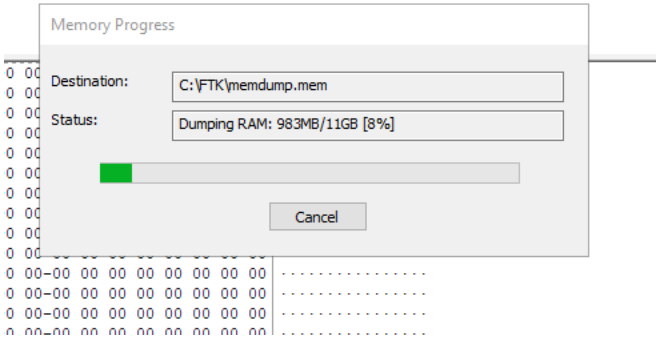
The process of importing the image to FTK took longer than autopsy, even though all of them were capable of recognising and reflecting forensically significant information. Practitioners from all around the world who were questioned claimed that the FTK graphical user interface (GUI) allowed users to work on their analyses without having to invest a lot of time in training. Encase provides extra search tools including EnScript commands and string conditions that enable quick and effective data searching. However, for practitioners to use the orders properly, they must spend a lot of time in training.



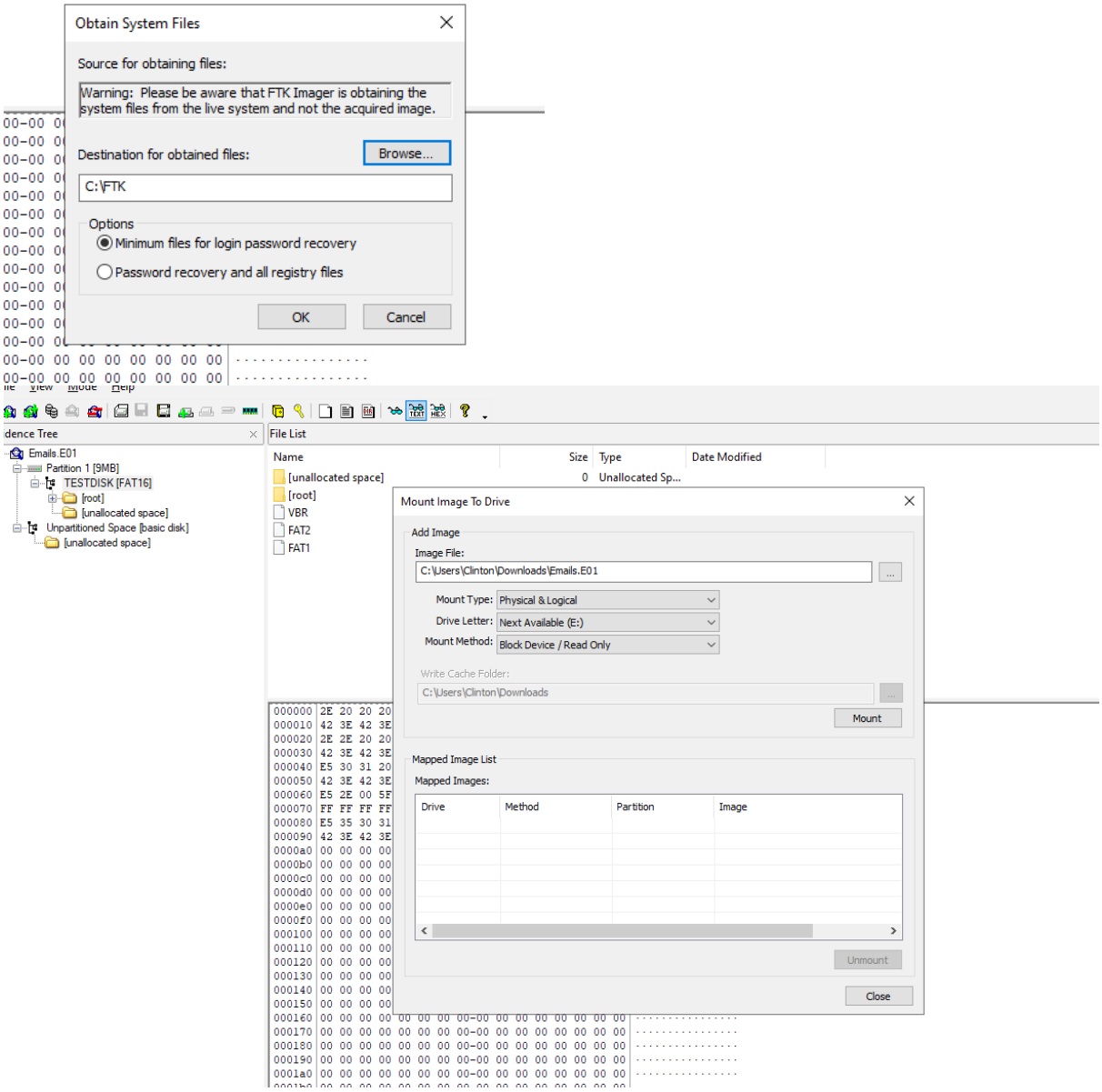
Above is the hash

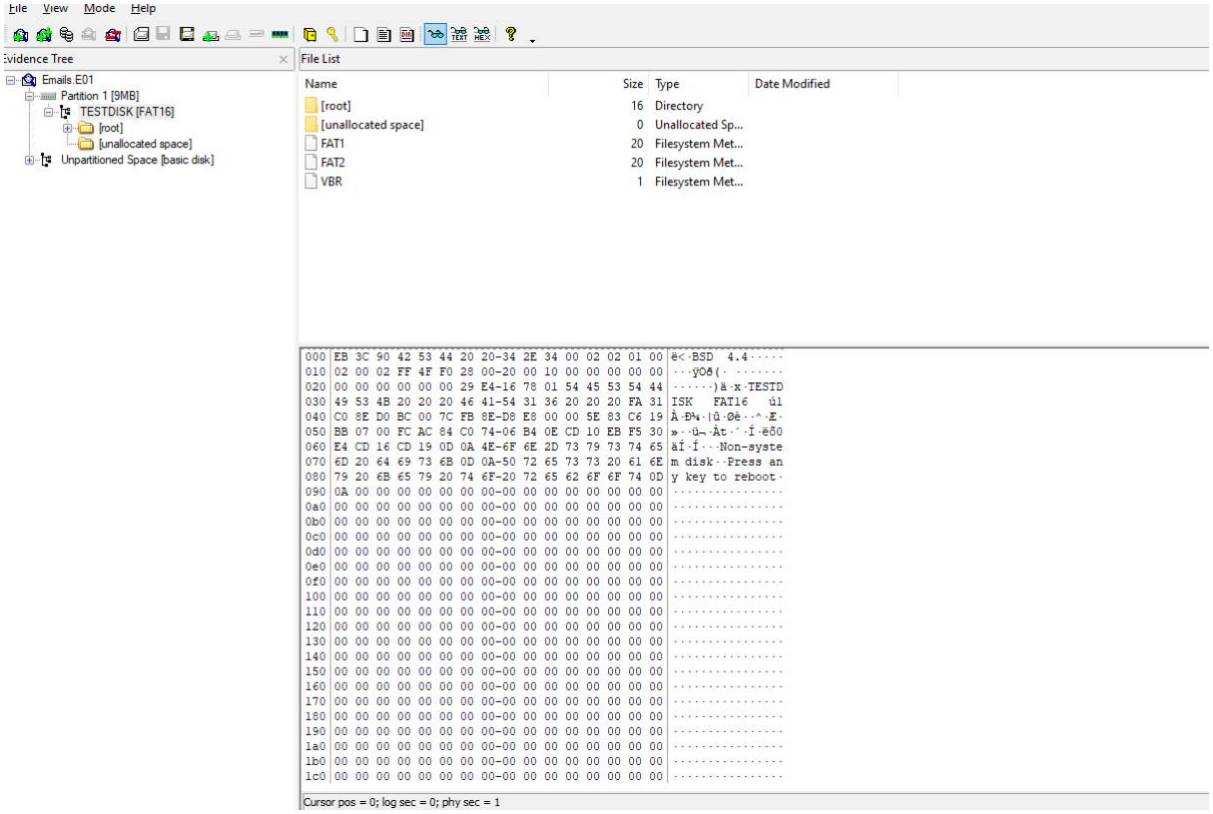
Verified the results



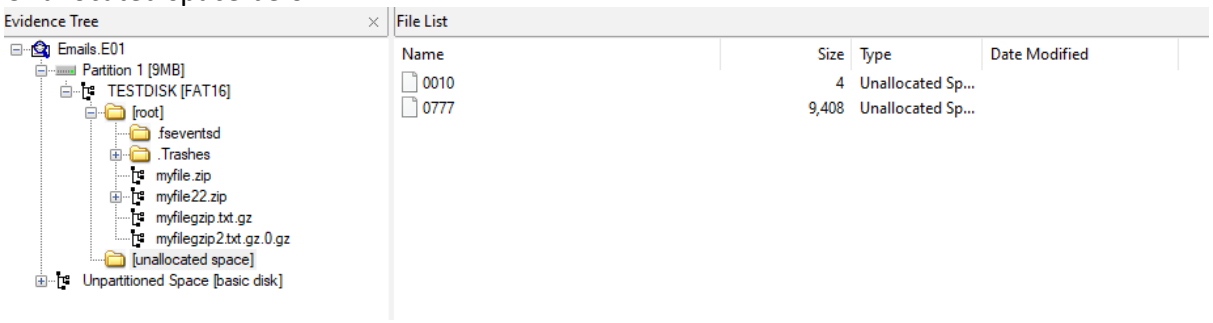


Above is the memory capture loading

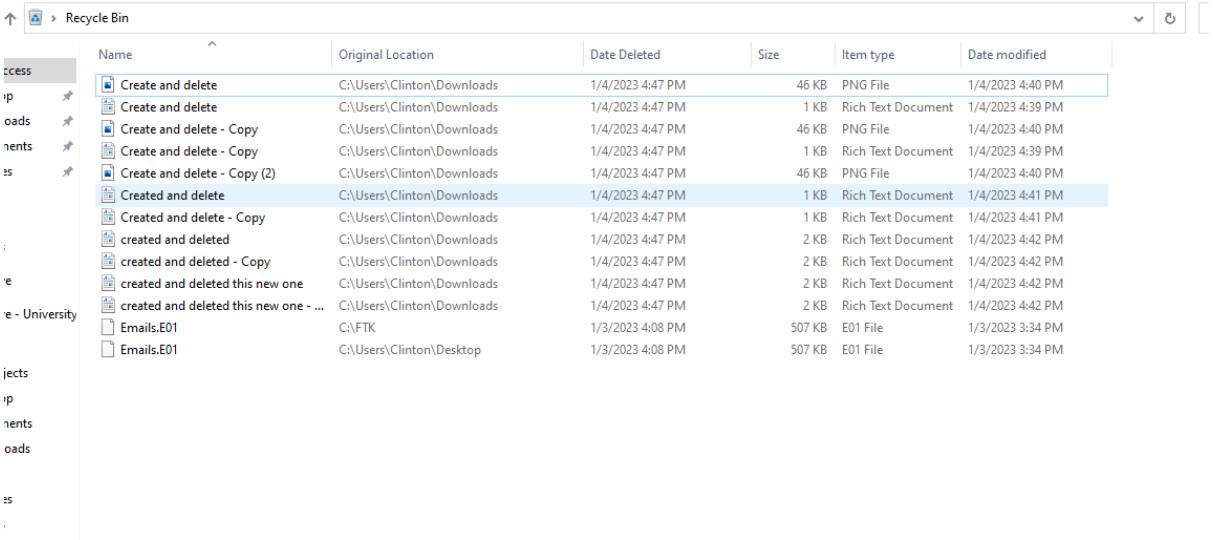

Obtain System Files
Source for obtaining files:
Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.
Destination for obtained files:
Browse...
C:\FTK
Options
Minimum files for login password recovery
Password recovery and all registry files
OK
Cancel
Mount Image To Drive
Add Image
Image File:
C:\Users\Clinton\Downloads\Emails.E01
Mount Type:
Physical & Logical
Drive Letter:
Next Available (E:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
C:\Users\Clinton\Downloads
Mount
Mapped Image List
Mapped Images:
Drive
Method
Partition
Image
Unmount
Close
Emails.E01
Partition 1 [9MB]
TESTDISK [FAT16]
[root]
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name
Size
Type
Date Modified
[unallocated space]
[root]
VBR
FAT2
FAT1

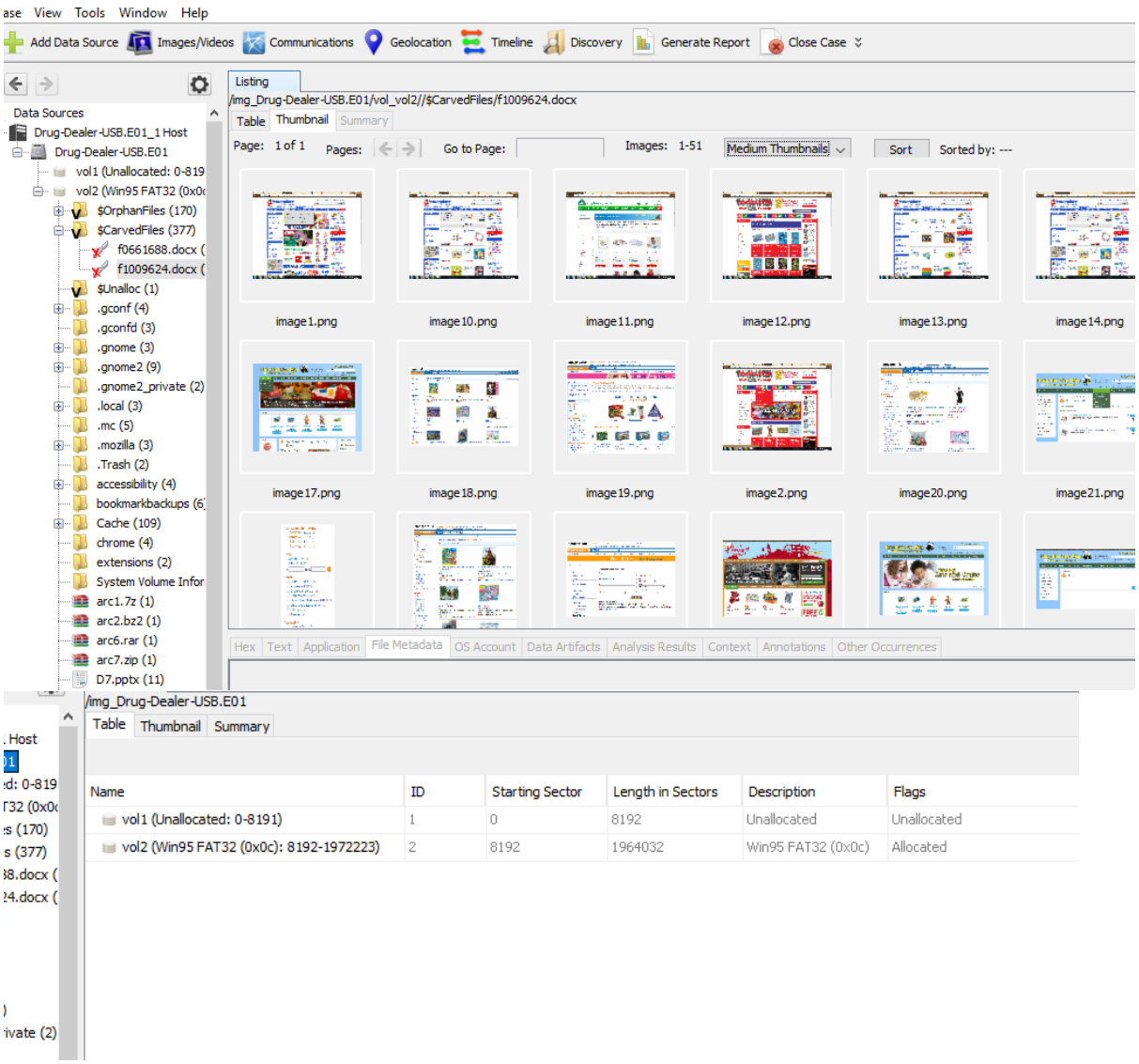


Unallocated space below:

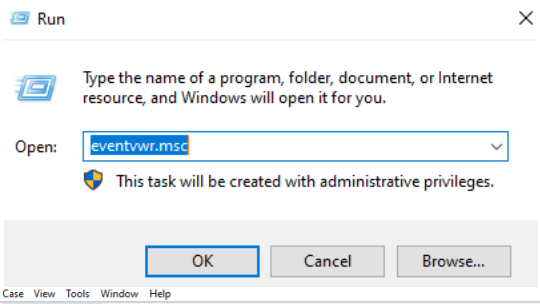


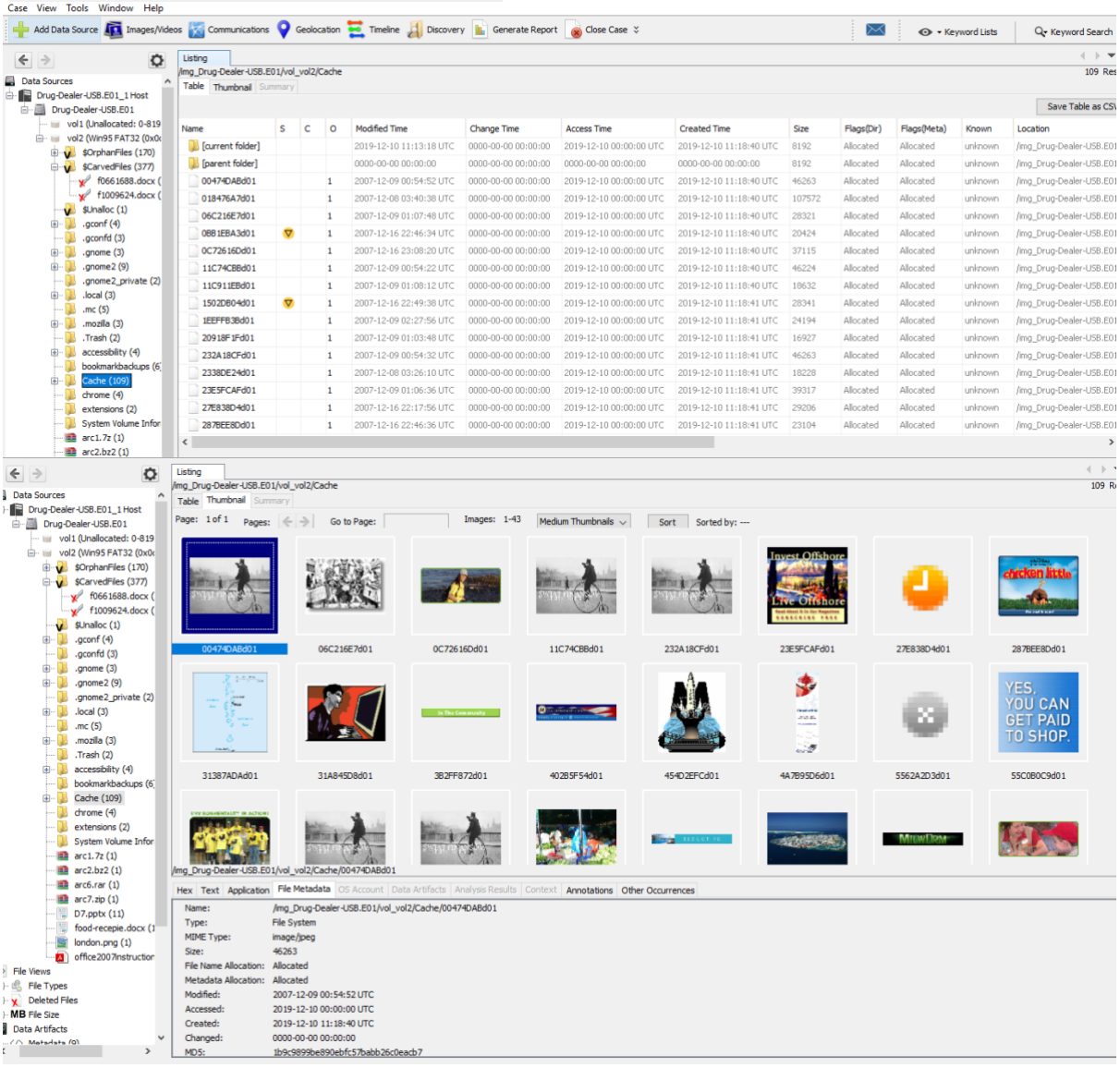
Artefact of windows: recycle bin

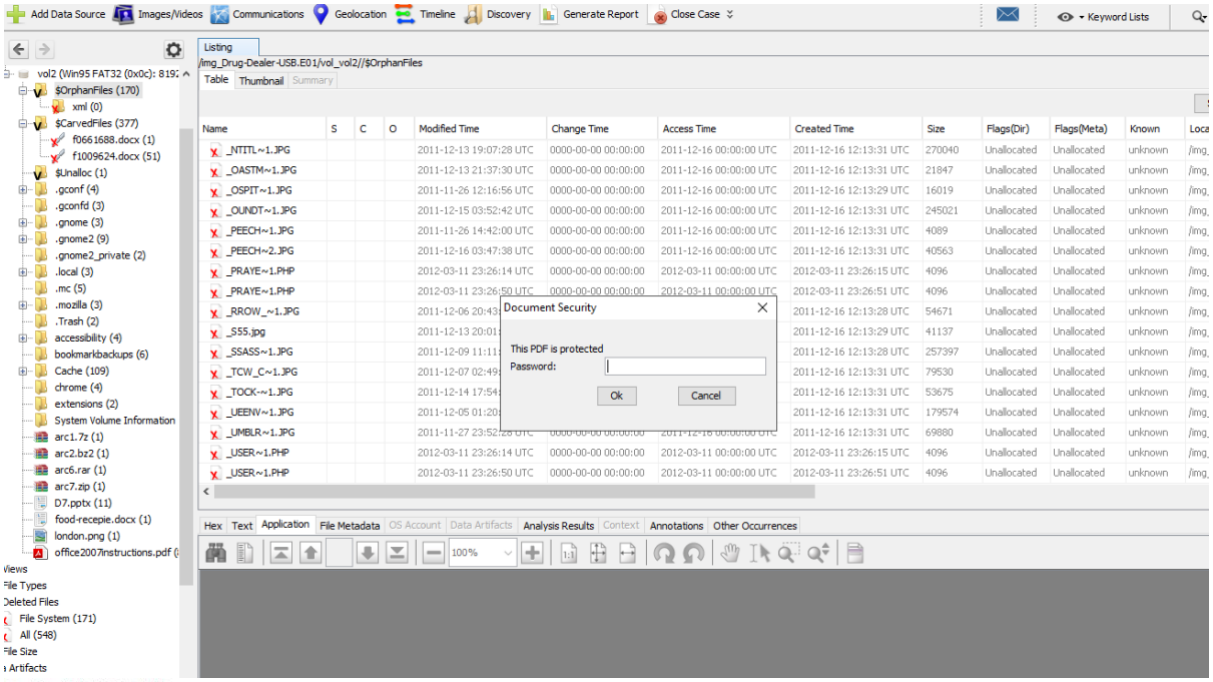


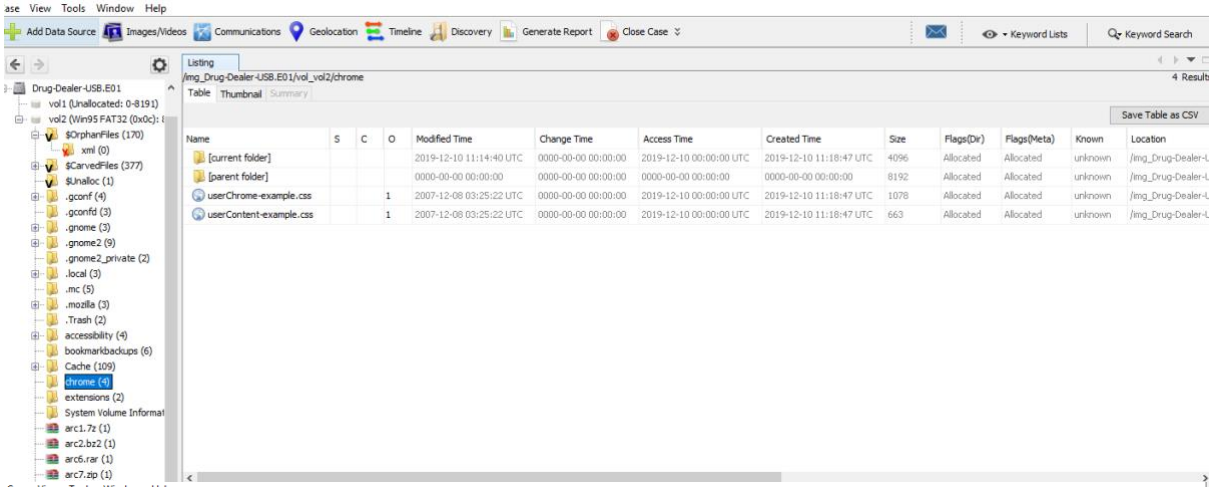


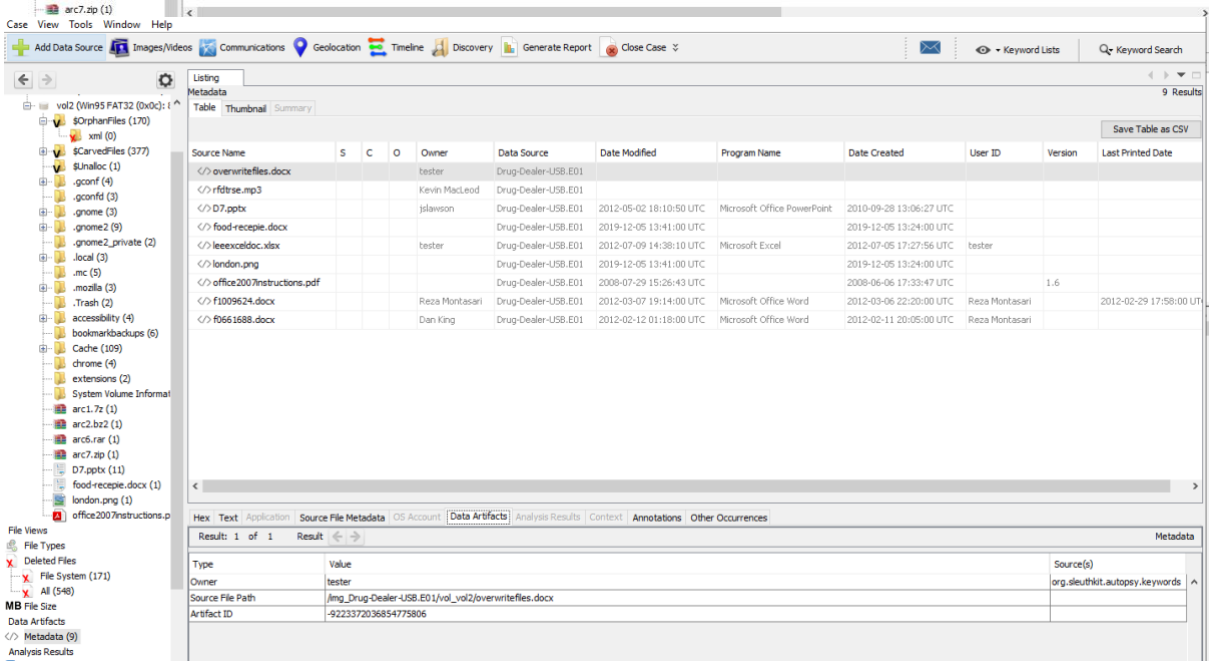
Below is used to event logs

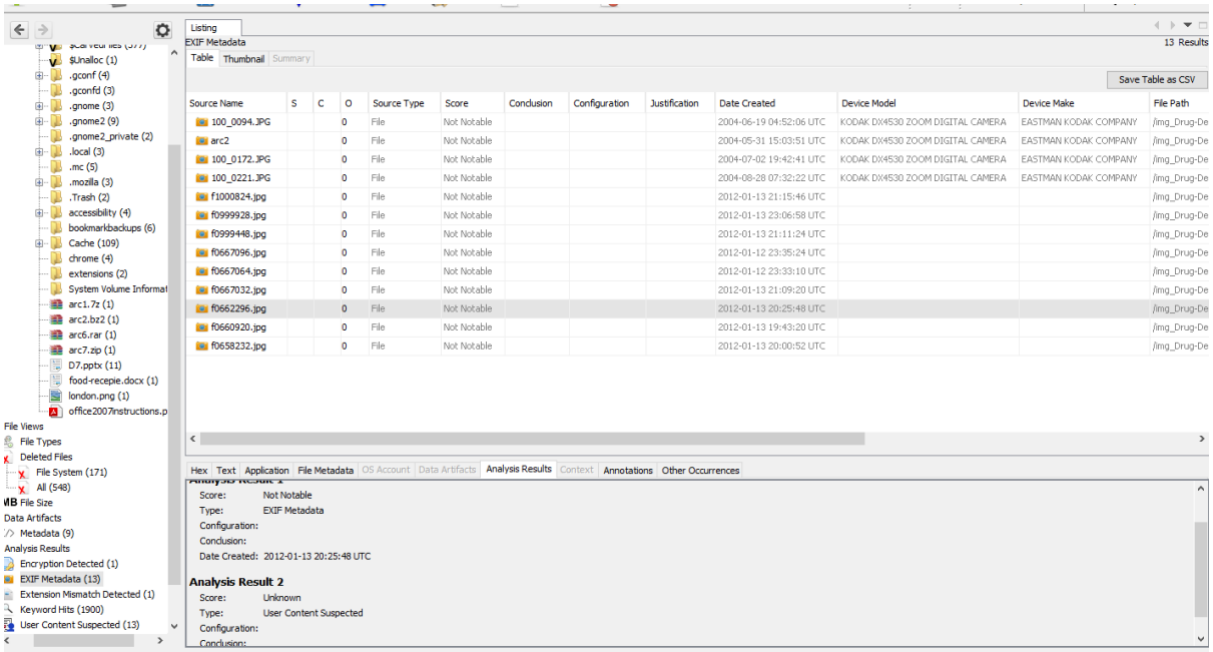

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
eventvwr.msc
This task will be created with administrative privileges.
OK
Cancel
Browse...

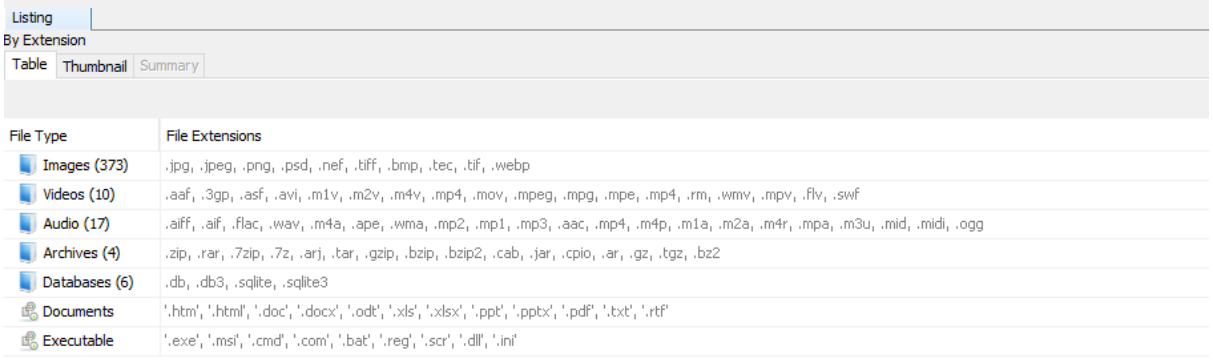

Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
Data Sources
Hex
Text
Application
File Metadata
Annotations
Other Occurrences
Name:
Type:
MIME Type:
Size:
File Name Allocation:
Metadata Allocation:
Modified:
Accessed:
Created:
Changed:
MD5:

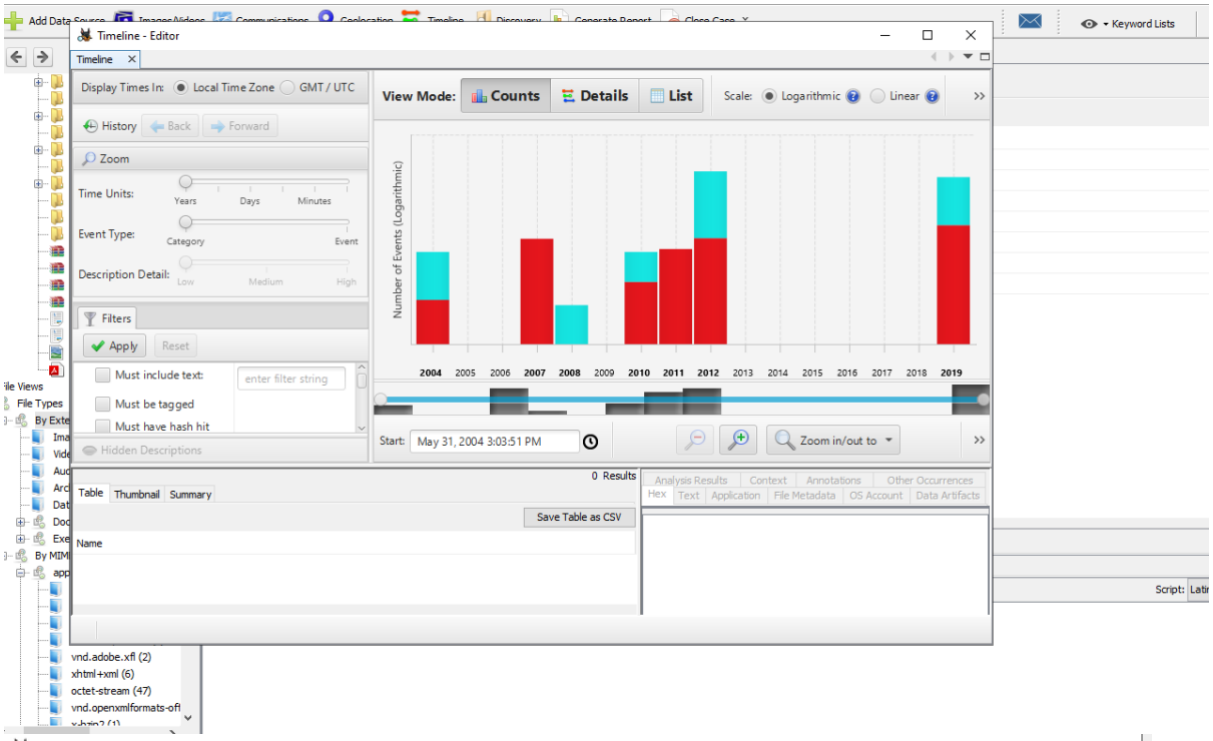

Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
/img_Drug-Dealer-USB.E01/vol_vol2//$OrphanFiles
Table
Thumbnail
Summary
Name
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Document Security
This PDF is protected
Password:
Ok
Cancel
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

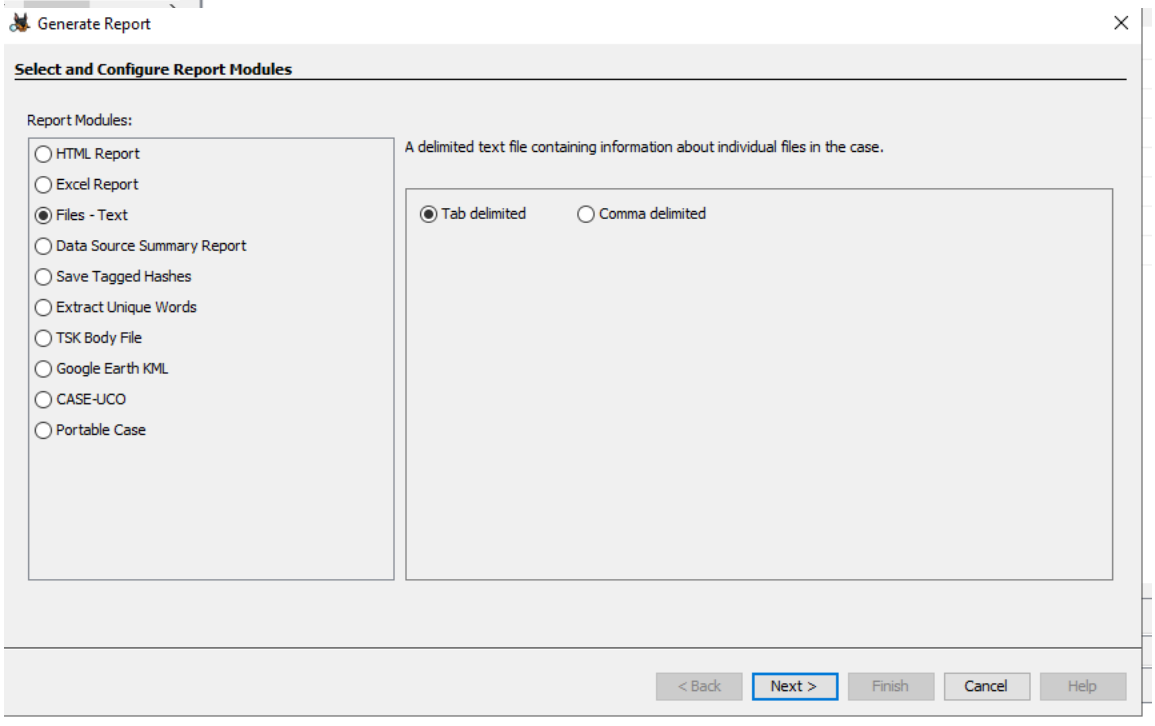

Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_Drug-Dealer-USB.E01/vol_vol2/chrome
4 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
Location
[current folder]
[parent folder]
userChrome-example.css
userContent-example.css

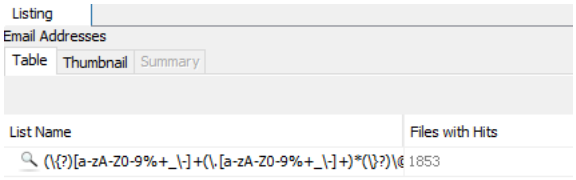

Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Metadata
9 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
Owner
Data Source
Date Modified
Program Name
Date Created
User ID
Version
Last Printed Date
overwritefiles.docx
rfdtrse.mp3
D7.pptx
food-recepie.docx
leeexceldoc.xlsx
london.png
office2007instructions.pdf
f1009624.docx
f0661688.docx
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 1 of 1
Result
Metadata
Type
Value
Source(s)
Owner
tester
org.sleuthkit.autopsy.keywords
Source File Path
/img_Drug-Dealer-USB.E01/vol_vol2/overwritefiles.docx
Artifact ID
-9223372036854775806

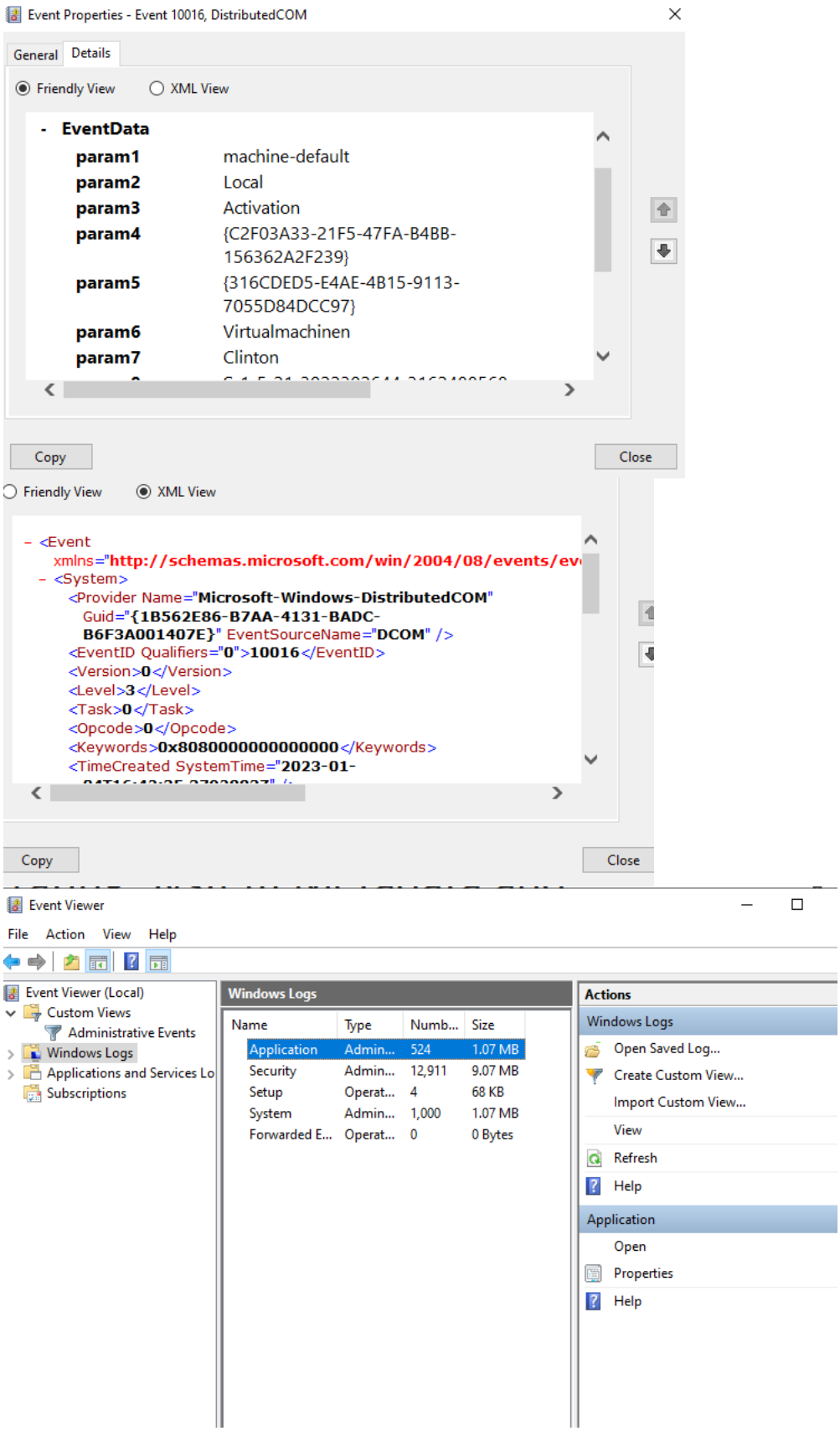

Listing
EXIF Metadata
13 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Source Type
Score
Conclusion
Configuration
Justification
Date Created
Device Model
Device Make
File Path
100_0094.JPG
arc2
100_0172.JPG
100_0221.JPG
f1000824.jpg
f0999928.jpg
f0999448.jpg
f0667096.jpg
f0667064.jpg
f0667032.jpg
f0662296.jpg
f0660920.jpg
f0658232.jpg
KODAK DX4530 ZOOM DIGITAL CAMERA
EASTMAN KODAK COMPANY
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Score: Not Notable
Type: EXIF Metadata
Configuration:
Conclusion:
Date Created: 2012-01-13 20:25:48 UTC
Analysis Result 2
Score: Unknown
Type: User Content Suspected
Configuration:
Conclusion:
File Views
File Types
Deleted Files
File System (171)
All (548)
File Size
Data Artifacts
Metadata (9)
Analysis Results
Encryption Detected (1)
EXIF Metadata (13)
Extension Mismatch Detected (1)
Keyword Hits (1900)
User Content Suspected (13)


Listing
By Extension
Table
Thumbnail
Summary
File Type
File Extensions
Images (373)
.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
Videos (10)
.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
Audio (17)
.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg
Archives (4)
.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
Databases (6)
.db, .db3, .sqlite, .sqlite3
Documents
'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx', '.pdf', '.txt', '.rtf'
Executable
'.exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'


Timeline - Editor
Timeline
Display Times In: Local Time Zone GMT / UTC
View Mode: Counts Details List
Scale: Logarithmic Linear
History Back Forward
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
Filters
Apply Reset
Must include text: enter filter string
Must be tagged
Must have hash hit
Hidden Descriptions
Number of Events (Logarithmic)
2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019
Start: May 31, 2004 3:03:51 PM
Zoom in/out to
0 Results
Table Thumbnail Summary
Save Table as CSV
Name
Analysis Results Context Annotations Other Occurrences
Hex Text Application File Metadata OS Account Data Artifacts
Keyword Lists
vnd.adobe.xfl (2)
xhtml+xml (6)
octet-stream (47)
vnd.openxmlformats-offi


Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Data Source Summary Report
Save Tagged Hashes
Extract Unique Words
TSK Body File
Google Earth KML
CASE-UCO
Portable Case
A delimited text file containing information about individual files in the case.
Tab delimited
Comma delimited
< Back
Next >
Finish
Cancel
Help


Listing
Email Addresses
Table Thumbnail Summary
List Name
Files with Hits
(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\(
1853

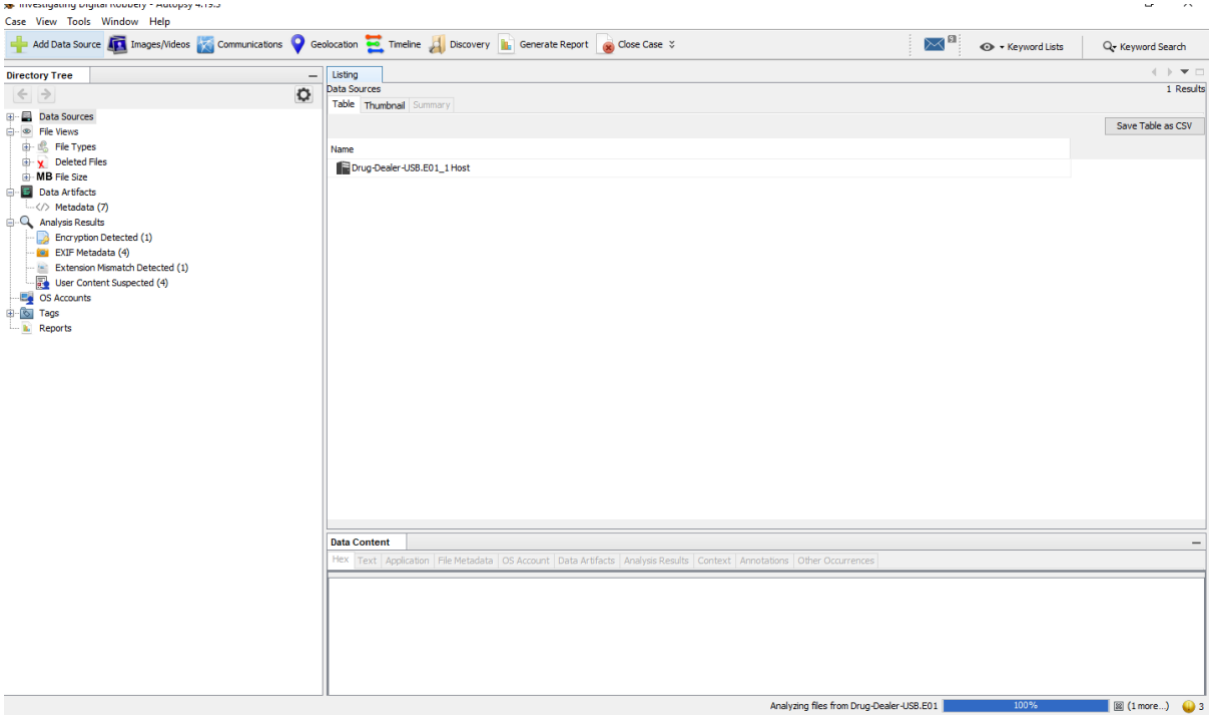


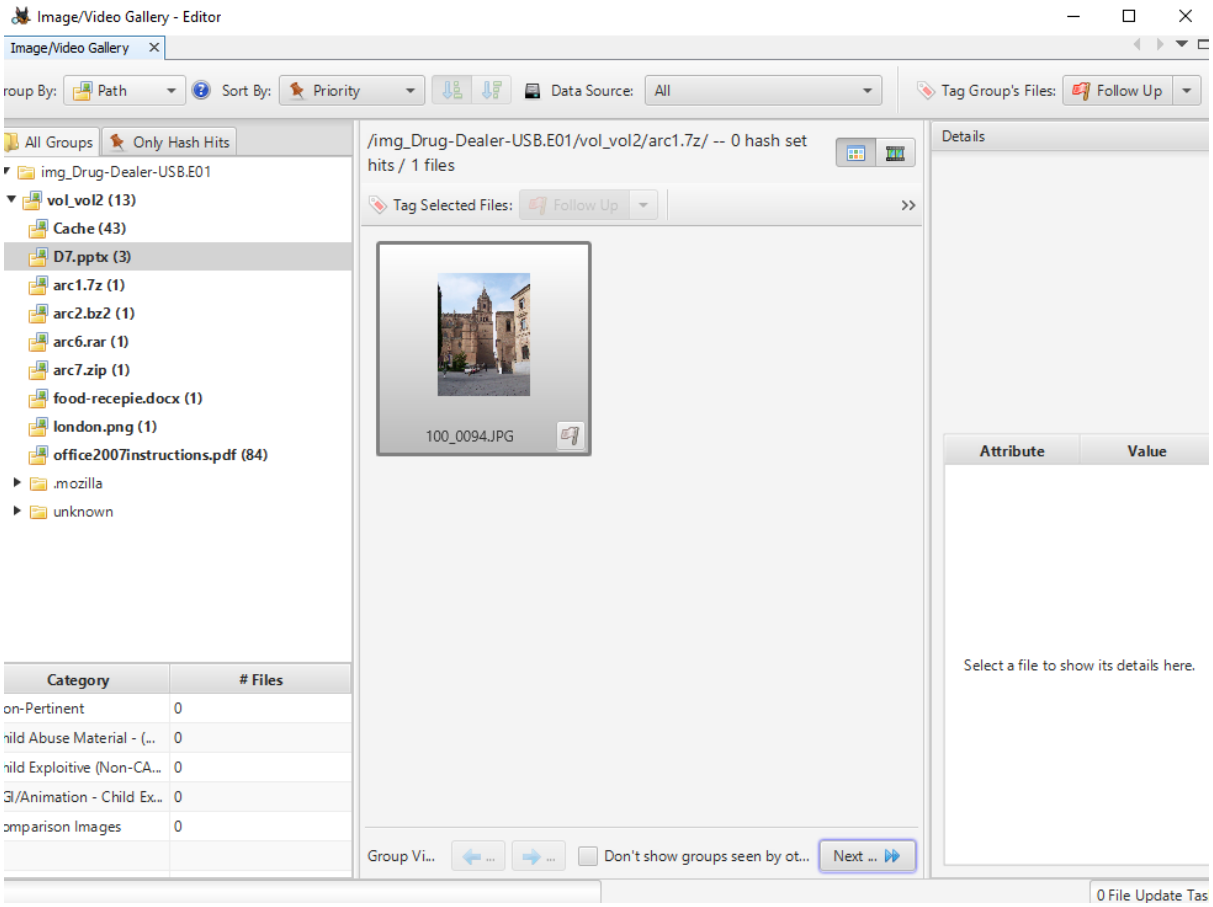
Event logs

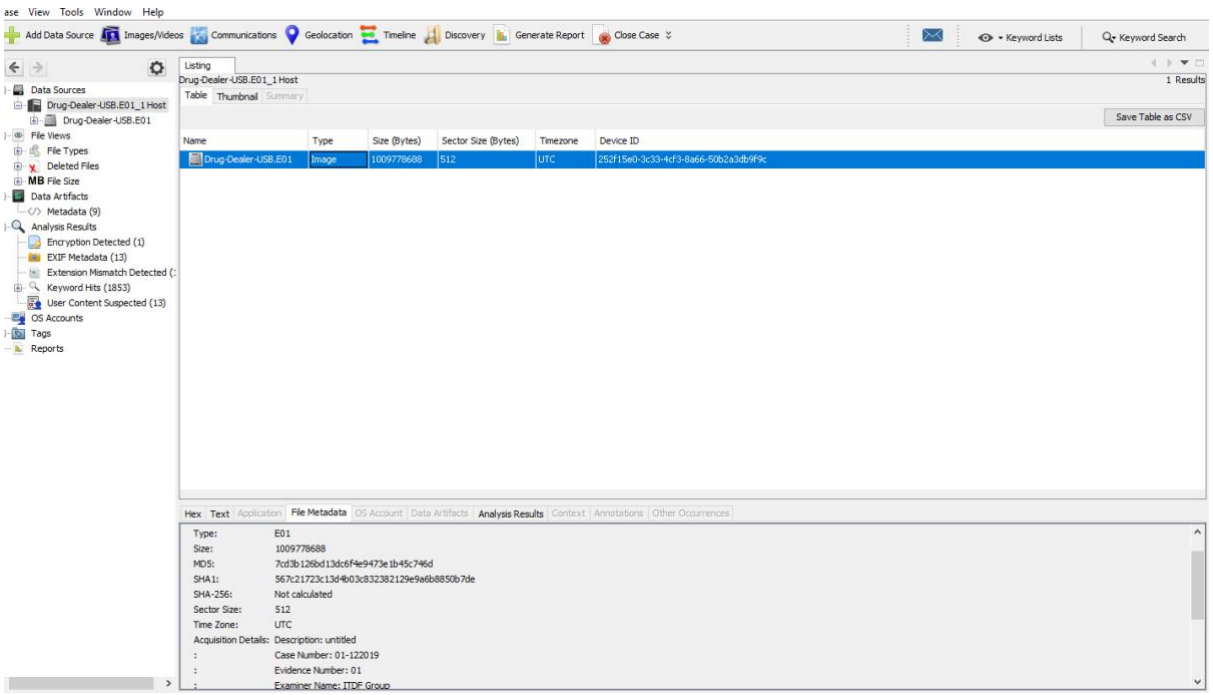
helps reconstruct malicious attacks, identifies relationships between events, detects anomalous user system activity, and identifies and predicts root causes of system failures.

File carving refers to the reconstruction of computer files without useful metadata indicators.

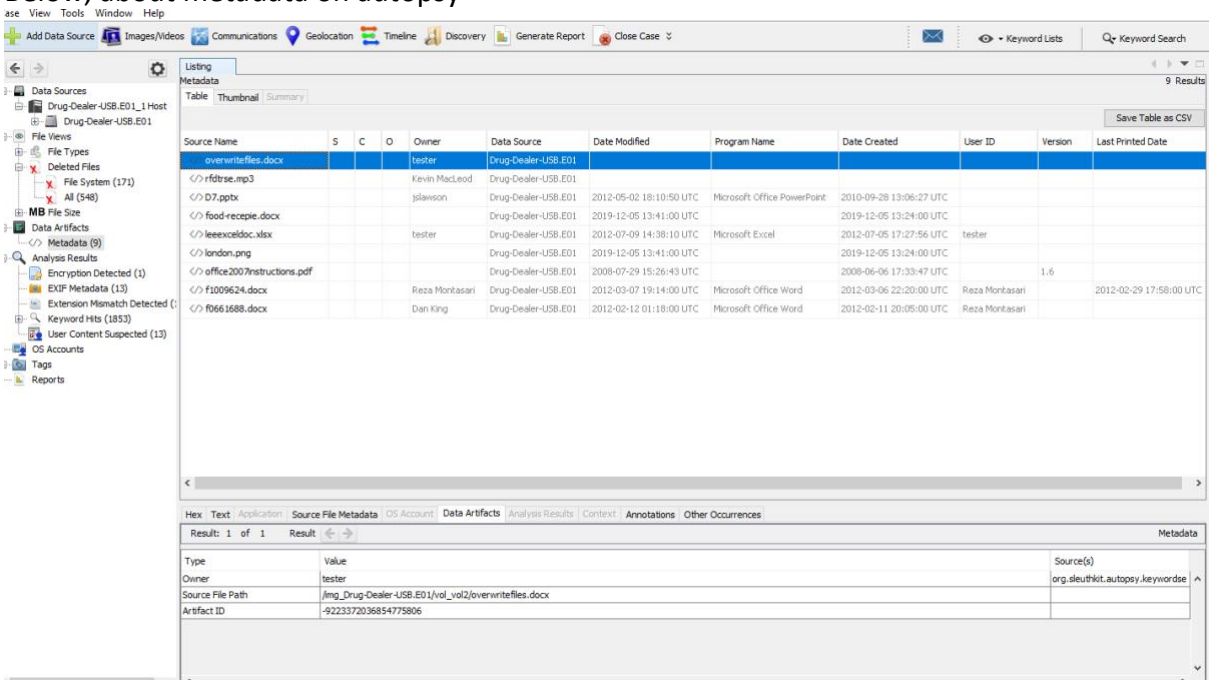
Autopsy:



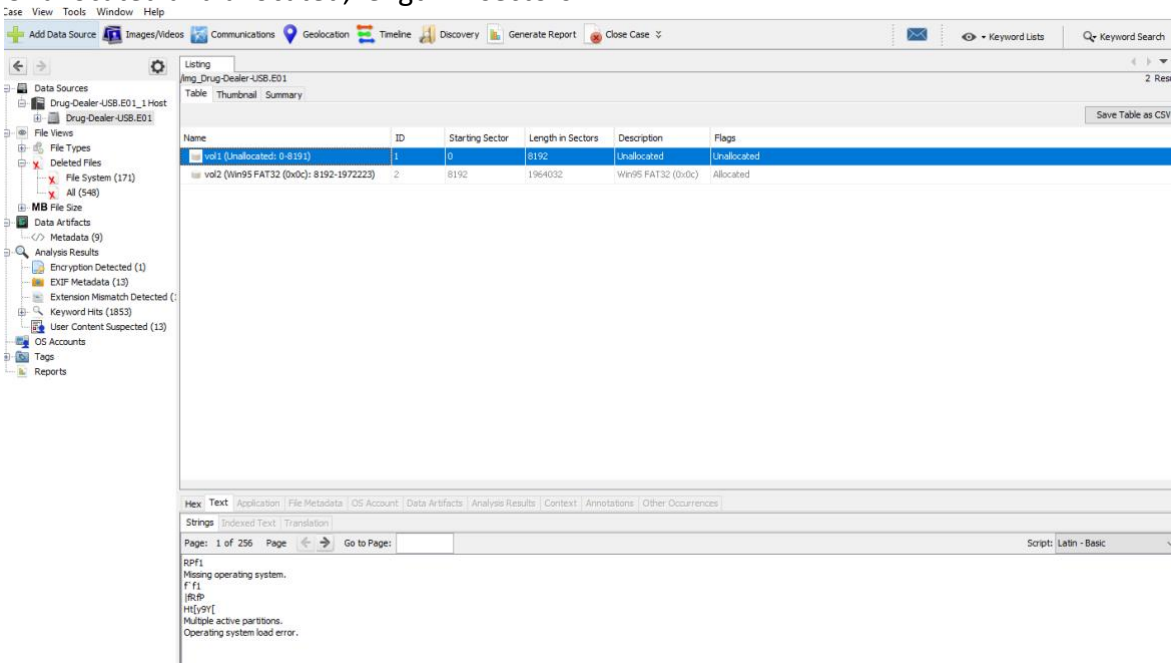

Image/Video Gallery - Editor
Image/Video Gallery
Group By: Path
Sort By: Priority
Data Source: All
Tag Group's Files: Follow Up
All Groups
Only Hash Hits
img_Drug-Dealer-USB.E01
vol_vol2 (13)
Cache (43)
D7.pptx (3)
arc1.7z (1)
arc2.bz2 (1)
arc6.rar (1)
arc7.zip (1)
food-recepie.docx (1)
london.png (1)
office2007instructions.pdf (84)
.mozilla
unknown
/img_Drug-Dealer-USB.E01/vol_vol2/arc1.7z/ -- 0 hash set hits / 1 files
Tag Selected Files:
Follow Up
100_0094.JPG
Details
Attribute
Value
Select a file to show its details here.
Category
Files
on-Pertinent 0
ild Abuse Material - (... 0
ild Exploitive (Non-CA... 0
GI/Animation - Child Ex.. 0
omparison Images 0
Group Vi...
Don't show groups seen by ot...
Next ...
0 File Update Tas


ase View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Drug-Dealer-USB.E01_1 Host
Drug-Dealer-USB.E01
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Metadata (9)
Analysis Results
Encryption Detected (1)
EXIF Metadata (13)
Extension Mismatch Detected (
Keyword Hits (1853)
User Content Suspected (13)
OS Accounts
Tags
Reports
Listing
Drug-Dealer-USB.E01_1 Host
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
Type
Size (Bytes)
Sector Size (Bytes)
Timezone
Device ID
Drug-Dealer-USB.E01
Image
1009778688
512
UTC
252f15e0-3c33-4cf3-8a66-50b2a3db9f9c
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Type: E01
Size: 1009778688
MD5: 7cd3b126bd13dc6f4e9473e1b45c746d
SHA1: 567c21723c13d4b03c83238212 9e9a6b8850b7de
SHA-256: Not calculated
Sector Size: 512
Time Zone: UTC
Acquisition Details: Description: untitled
Case Number: 01-122019
Evidence Number: 01
Examiner Name: ITDF Group

Below, about metadata on autopsy

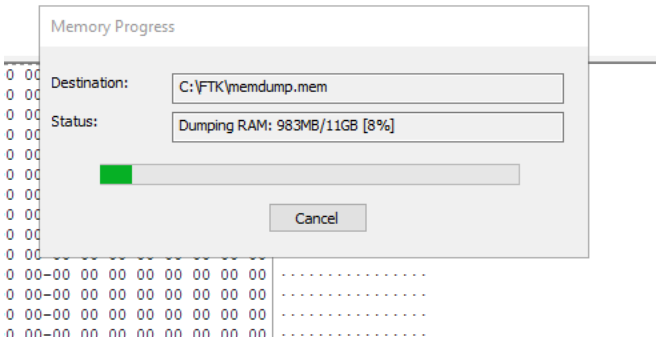


Unallocated and allocated, length in sectors.



Task 3:

Data in RAM is non-volatile, but can work in accordance with cache, which is volatile memory. Thankfully, the type of evidence that can be retrieved from a laptop's RAM using vitality framework is network information, which can be part of the registry.



Task 4:

In order to explain how both network and malware forensics can separately or in accordance work together to aid this investigation, I believe that key definitions should firstly be portrayed. Network forensics is the analysis of data trafficking on a network. However, malware forensics is the act of investigating malicious activity in order to find those or the software responsible. Firstly, network forensics is performed primarily by disconnecting the network from its power source. This is done so any valuable information does not get corrupted or deleted permanently. There is an exception of this if one is tracking and working on an active network, dependant on the practitioner. Secondly, the volatile memory is then acquired, and goes through documenting of the memory acquisition. This is vital because during network forensics, the details that were extracted by the suspect and kept in such a way that breached the code of conduct can be examined. All can help examiners reconstruct the activity prior to the attacks. SRUM extensions are used to help.

Task 5:

In the examination phase, I believe conveying the images when put through tests such as steganography, to detect illegal uses or portraying's of malicious and suspicious images.

Task 6:

Throughout this investigation, one (the designated practioneer) may encounter a challenge such as SEDs being implemented unknowingly or before the forensics team at the crime scene intercepted and collected the digital evidences. This means that a suspect could have intentionally locked the file systems, even the BOOT manager and cause a crippling effect in which the investigator may have to find the algorithm, and implement attacks in order to discover vulnerabilities in the encryption used, and in the encrypted data: cryptanalysis. This means that more time may be spent using computing resources that do not aid the main purpose of the investigation; the thorough ghosting, or cloning of the device. Due to technology and legislations around these machineries, computers are changing everyday, so legislations and laws change with them at given intervals from ordained bodies; for instance homeland security US. This can be a detriment to the investigation as the given parameters to discover any suspicious traits in the suspect's system, or suspect's geographically scattered/ partitioned files may come to an end. Furthermore, as the suspect has a android tablet, which is rather portable and can have no

administrative overhead to some degree, can also cause partitions over several geographical locations whether that be in a LAN or WAN. Gathering evidence that is hardcore is quite difficult, due to the ambiguity of certain files or network traffic that could exist. Data can hide in plain sight, through the use of ADS in file systems and this poses a quite dangerous risk to the integrity of the investigation due to the fact that in digital imaging, every bit is mirrored, meaning that the alternative data stream, which could hide within metadata, start a malware on the lab PC when triggered. This can cause a court to drop the whole case as the investigation cannot be trusted due to the breach of confidentiality, and integrity. In addition, there are digital forensic practitioners who may know of routes to uncover vulnerabilities in a suspect's device, however it may not be ethical or lawful in the operating region and may not follow any DFP.

The coming of age for social media is a peculiar topic due to the fact that media is always at it's pinacol which is great for keeping in touch, and even businesses operating online. In light of this, criminals exploit this opportunity, which has led to an increase in demand for cyber security in all aspects of the technological world, even for the criminals such as drug dealers who operate on encrypted devices such as PGP and encrochat.

Additionally, making a documentation alongside the findings can lead to inconsistencies and inaccuracies due to live acquisition imagery. This means that data entered into document at one given point in time, may no longer be liable, relevant or correct when next checked; this mainly happens with volatile memory, cloud storage/system and other. With dead acquisition imaging, the running memory cannot be tracked, one must use a live tool as the memory is also live in order to track activity in real time. Considering this, a solution for this would be live acquisition imaging. Using memory, extracting processes that had already ran either over the last nth days can help the investigation, and via memory one could check the login details and the data coming in and out. The suspect is very technical in this field, and has quite a lot of access to sensitive data so it can be difficult to narrate and convey if any data were entered with malicious intent. Live volatile data can be lost, if power was to be taken away from the power source. For windows, Sdelete can cause complete loss of data, possibly without recovery in some cases.