المجلة الإلكترونية الشاملة متعددة التخصصات
العدد السادس والاربعون شهر (٤) ٢٠٢٢

Experimental Evaluation of Digital Forensic Tools

By: Jasir Adel Altheyabi

Master's in Cyber Security, Cyber Security Department, College of Computer and Information Science, Majmaah University, Kingdom Of Saudi Arabia

Email: Eng.Jasir@Gmail.com

Abstract:

In this paper. We will look at criminal digital investigation and testing among a set of digital investigation tools to achieve the best results in digital investigation incidents and the .problems that are verified in criminal digital investigation

Several tests has been conducted on a set of digital investigation tools in several aspects. Such as tool validation. Interoperability of tools. Accuracy of forensics tools and Capability of tools. We have found that analyzing and discovering the strengths of the digital investigation tool can help digital investigators to form an integrated set of digital tools for .all types of cyber crime

The methodology includes an interpretation of the experiment design and the test framework. and discussion of the specifications of the tools used in this research, I used the below tests for conducting this research: Accuracy of forensics tools, capabilities of forensics tools, validation of forensics tools, comprehensive of forensic tools, and iin the end I discuss the results of list of tests on digital forensics tools.

Keywords: Digital Forensic Tools**,** Experimental Evaluation

1. introduction

With the increasing reliance on computers and therefore their use for nan-cial transactions and the maintenance of non-public records. There has been a relative increase within the incidence and value of cyber crime committed using computers or related devices. the rise within these crimes and their values highlights the importance and value of computer forensic evidence in the foreground. the method of collecting. Processing and presenting evidence to the courts. Inquiries or courts is subject to criteria that has to be adhered to so as to make sure the admissibility of evidence. Computer forensics tools will be simpler than other forensics tools. And there has been an extended debate over when to be superior. While increasing the accuracy and challenge of digital tools. Moreover. The worth of digital evidence has become more important. And its acceptability and weight are evaluated in terms of public and legal law likewise because the Telecommunications and knowledge Technology Law 7/3/1428 Hijri. This thesis discusses this discussion and therefore the capabilities of the medical toolkit Legitimate with relation to variety of common varieties of technical evidence extracted from computers. This chapter provides an summary of computer forensics. Followed by an summary of the structure of this thesis.

1.2. Objectives:

Through this research, we seek to achieve the following objectives:

- Testing of computer forensics tools.
- Explain the specifications of the computer forensics tools.
- Capabilities of forensics tools.
- Validation of forensics tools
- Analyzing and discovering the strengths of the digital investigation tool

1.3. Terminology

Legal Computer Science. Just like the case with numerous other software engineering disciplines. Used a lot of expert terms. It is in this way important to de ne. These terms and the manner by which they are used. The following is a list of definitions of terms used in this thesis.

MAC: Refers to the remaining Modified. Accessed and Created times. The final modified time refers to the ultimate time that adjustments to the le had been saved. Last accessed time is the final time that a le become accessed. Created time is the time that a le turned into created at a given location

VM: Virtual Machine is a software laptop that acts further to a physical computer (vmware. N.D.). The virtual system is in truth am operating device hooked up on a hypervisor which is software that emulates a hardware platform. Making the experience of the use of a virtual machine similar to that of a physical device

Digital Forensic Image: A bit-for-bit reproduction of goal media. The copy does now not add or pass over any facts from the authentic media and is an accurate illustration of the copied media

Static evidence: Evidence that has been acquired in the form of a forensic image of non-volatile media and then added to a case as evidence

Volatile evidence: Evidence that may be overwritten at the same time as operating a pc or this is lost whilst the pc is powered o

Write Blocker: Is a device that blocks all write commands passing through it. Thereby avoiding unintentional addition or deletion of records on the target media.

2. Literature Review

2.1. The Computer Forensic Process

This road map created via the Digital Forensic Research Workshop protected what is probable the first recognized framework for the virtual forensic method. This technique version consisted of seven phases. These phases are Identification. Preservation. Collection. Examination. Analysis. Presentation and Decision.

For the purpose of this paper we shall consciousness on Preservation. Collection. Examination. Analysis and Presentation being the five stages which are involved with the real investigation of virtual media and the presentation of findings (Clinton et al., 2009).

1. **Preservation**

The protection segment is concerned with imaging of the virtual media and preserving the chain of custody (Jordaan, 2015).

2. **Collection**

Areas of focus during this segment are to ensure that necessary authority is obtained. And that regularly occurring methods. Software and hardware are used in the recovery and collection of the information.

3. **Examination**

During the examination section. Hidden records could be recovered. Data validation could be achieved and information would be extracted from the media (Digital Forensic Research Workshop, 2006) (Carrier, 2003).

4. **Analysis**

This phase involves developing timelines. Extracting value or evidence from the statistics and growing a photo of what might also have occurred (Shanmugam, 2011).

5. **Presentation**

Presentation consists of compiling a report. Explaining findings. Making hints and testifying

2.2. Computer forensics tool testing (CFTT):

The Computer Forensic Tool Testing (CFTT) venture. A collaborative effort through the National Institute of Standards (NIST) and various United States Law Enforcement Agencies has created a number of specifications for check processes and criteria for the exams of virtual forensic equipment. The goal of the CFTT challenge is to offer customers of computer forensic tools with an know-how of the abilities of the diverse tools and their abilities or shortcomings.

Furthermore the results of those assessments can be utilized by the developers of those gear to improve or debug the tools. CFTT simplest assessments equipment used for acquisition of photos. Disc instruction and write blocking. It does not test pc forensic equipment used to perform evaluation on photos or computers (National Institute of Standards. N.D.) (Lyle, 2012).

There is an essential need in the law enforcement network to ensure the reliability of computer forensic tool.

The purpose of the Computer Forensic Tool Testing (CFTT) task at the National Institute of Standards and Technology (NIST) is to set up a technique for testing laptop forensic software tools by improvement of general device specifications. Test procedures. Check criteria. Take a look at sets. And take a look at hardware. The results offer the information vital for toolmakers to enhance tools. For users to make informed picks about acquiring and using computer forensics tools. And for interested parties to understand the equipment capabilities. A functionality is required to make certain that forensic software equipment always produce accurate and objective test results. Our approach for checking out computer forensic tools is based totally on well-diagnosed worldwide methodologies for conformance testing and ne testing.

Accuracy and completeness are two critical attributes of virtual acquisition equipment identified by NIST (National Institute of Standards, 2005). In order to fulfill these

requirements. NIST identified the following obligatory attributes which computer forensic acquisition tools need to exhibit (National Institute of Standards and Technology, 2004a).

1. A digital forensic imaging tool has so that it will use all interfaces visible to it to acquire the target (National Institute of Standards and Technology, 2004).

These interfaces encompass ATA. SATA. SCSI. USB. IEEE 1394 and remote access via community or parallel cable (National Institute of Standards, 2005).

2. Users have to be able to use virtual forensics tools to create either photos or clones of digital sources. Digital sources consist of all FAT. EXT2. EXT3. FreeBSD. HPFS. Linux switch and NTFS files systems on either hard power or stable country media.

3. Digital forensic tools should be able to acquire sources in each execution environment in which they are in a position to function. Tools ought to be able to function in one or more environments. The most excellent environments are Windows. Linux. DOS and Mac OS (National Institute of Standards, 2005).

4. All data sectors of the source whether seen or hidden need to be as it should be recovered by virtual forensic tools. Accuracy of acquired pics may be verified through the usage of hashes

5. All unresolved reading errors from a digital source need to be pronounced to the user. Such reports must include the error type and location

6. Destination photos have to include benign fill in the vicinity of unread-able records that turned into inaccessible due to unresolved errors.

3. Materials and Methods

This section will show all tools and practical devices and methods used for this study and the different fashion of software in many operation system.

3.1. Forensics Tools:

1. FTK
2. Prodiscover
3. Autopsy
4. OSForensics
5. P2Commander

3.2. Operation System:

- Windows 10.
- Kali Linux.
- Virtual Machine.

3.3. Devices:

- Digital Intelligence.
- External Drives.
- Write Blockers.

4. Experimental Evaluation

4.1 Physical Equipment

4.2 Test Cases

4.2.1 DF-01

We will create an image by each forensics tool and compare the size of the images with original size of drive.

Test Evaluation Criteria

We create an image of local disk using Forensics Tools then compare the size of these images from both tools

Item	Identi er	Size Speci cation
Test Computer	Huawei MateBook Pro14	8GB RAM. Intel Core i5, CPU@1.60 GHz
Test Image	cfreds.Nist images	Data Leakage images: 5.3Gb Mobile Image: 14.5 Gb Drones Image: 15.5 Gb
VM Workstation	Ubunto Distribution	30GB
Accessories	SanDisk FlashMemory	32GB

Test Case Result

- Original source drive Size: is 32 GB.
  - FTK Image size: 12.520 GB.
- Prodiscover image size: 20.9 GB.
- P2Commander image size: 566.9 KB
- Autopsy image size: 723 KB
- OSForensic image size: 387 KB

Case Summary

FTK:

In FTK. We create an image for disk size 32 Gb and the elapsed time is 21 minutes and 39 seconds without display Estimated Time Left. And review the image elapsed 1 minutes and 37 seconds. The advantage of imaging in FTK tool is summary verification of image le containing:

- Name of the image
- Sector Counts
- Verification of MD5 Hash: (Computed hash. Reported hash. Verify Result)
- Verification of SHA1 Hash: (Computed hash. Reported hash. Verify Result)
- Bad Block List: check if any corrupted block during imaging

Also for large disks. FTK divide the image into files each size is 1.5 Gb to facilitate the investigation of the image and preserve the time. Based on image formats the FTK Forensic toolKit the most Compatible tool with other forensics tool

Prodiscover:

In Prodiscover. Imaging process has many options such as compression the image and image formats its dd format and Prodiscover format. dft and its display the Estimated time is 28 minutes which is identical to elapsed time is 28 minutes also display acquired number of sectors. And 10 seconds for imaging 32 Gb source drive. The most disadvantage there is no summary of image creation like hashing verification.

P2Commander:

in P2Commander. The biggest disadvantage is the time its elapsed 1 hour and 16 minutes and 44 seconds. Its not have hash verification. Its have forensic container which secure database. Data in forensic containers is encrypted and locked by password. And able to determine the contents of the image and also able to extract case history which record all investigation process, also it don't have hash verification

Autopsy:

In Autopsy. The time consumed for creating an image is 15 minutes and 44 seconds. It has many option for imaging such as Emails Parser. Virtual Machine Extractor and File Type Identification. Also support Arabic language in carving Arabic contents files.

Able to extract Emails from files to discover all parties in the crime during investigation. The most advantage is timeline of files dates and the investigator able to tag the evidence in several categories like child exploitation. Harassment. Thefts and several categories crimes. Which make autopsy the best tool in recovering user activities.

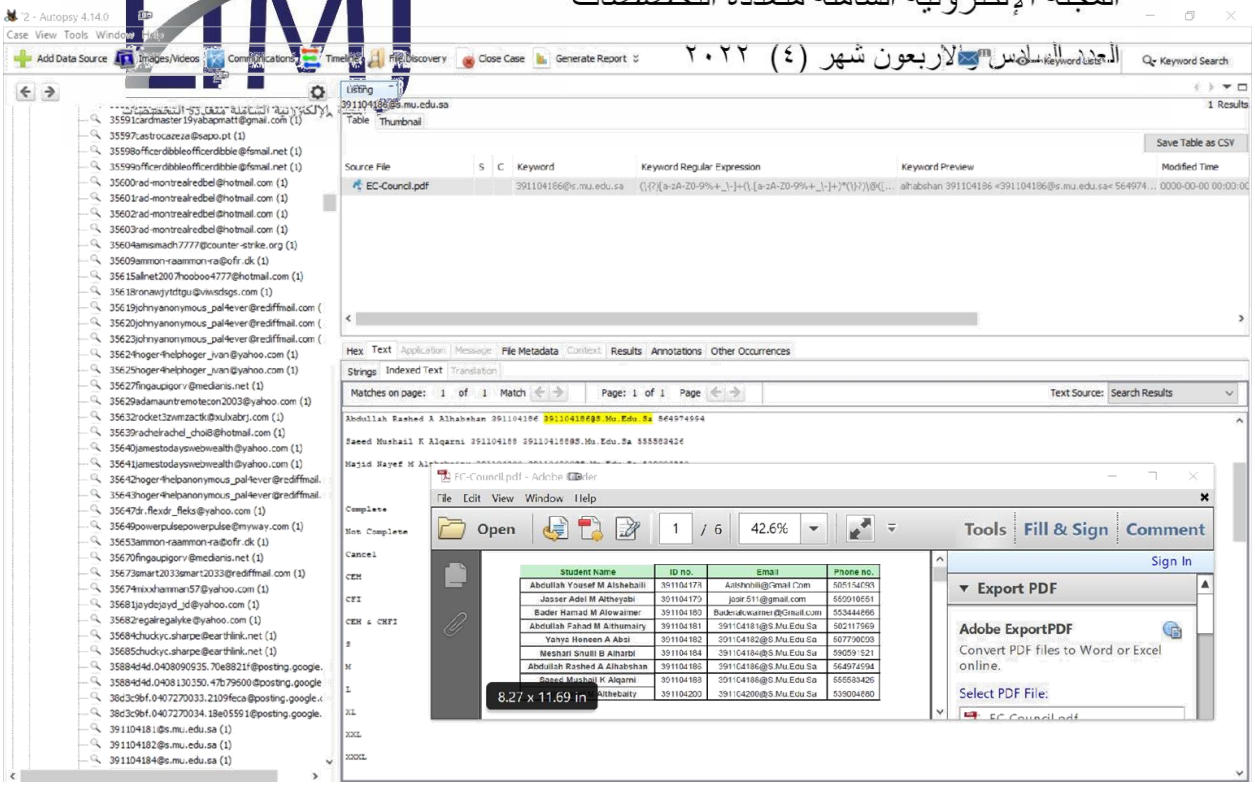

Figure 4.1: Recovering Emails of User Activities

OSForensics: the most advantage of OSForensic imaging is creating a folder containing all related contents in separated files such as Emails. Passwords and Reports. And window for monitoring the CPU during the live analysis.

The disadvantage is failure of the tool to restore the ownership and permission of the files and only create raw format image.

4.2.2. DF-02

Compare the hash value of specific image le extension (.png) in each forensic tool Before And After acquiring data.

Figure 4.2: The Monitoring CPU Interface

Test Evaluation Criteria

- Delete seven formats of pictures (Jpg. Png. Svg. Tga. Ti. Gif and EPS)
- Recover the picture formats from the image
- Calculate the hash value of the image using HashCalc
- Compare the hash value between each forensic tools using HashCalc.

Test Case Result

In FTK. Some pictures are partial corrupted and still recovered and extracted in excel sheet with calculated hash value In OSForensics.

The le recovered and the calculated hash is equal to original hash In Prodiscover. The image created by prodiscover was covered the deleted pictures format. In Autopsy and P2Commander. The deleted files has corrupted after recovering process,

4.2.3. DF-03

Create an image without enough spaces and notice the decision of each forensic tools

Test Evaluation Criteria

We will create full local disk and ask the each forensic tool To create an image to see the behavior decisions

Test Case Result

Prodiscover Decision: It's decline starting the process and alert the disk is full.

FTK Decision: Its decline the process and ask to write the remaining image segments in a new location.

OSForensics Decision: its alert not be enough space on the destination drive to create the disk image. And ask the user if continuous the image process with missing details.

Autopsy Decision: the worst action was taken by autopsy, which is starting imaging process, And when there is not enough space its stop the imaging process. P2commander Decision: same decision of OSforensics the space is not enough in destination drive

4.2.4 . DF-04

Test and verify the supported image le format from other tools

Test Evaluation Criteria

We will test the flexibility of all computer forensic tool format and check weather is supported by other tools or not. By create an image using other tools with different format and try to analysis the image with different tool.

Test Case Result

- FTK create many image file formats like:

- E01. S01 and L01
- AFF
- AD1
- RAW/DD

And support:

- vc4. Nrg. Vmdk. Vhd

- Prodiscover create. EVE Project le and support:

- DD
- E01
- Vhd

- Autopsy supports disk images in the following formats: Raw Single (For example: *.img, *.dd, *.raw. Etc)

Raw Split (For example: *.001, *.002, *.aa, *.ab. Etc) EnCase (For example: *.e01, *e02. Etc)

- P2Commander: Raw Single (For example: *.img, *.dd, *.raw. Etc)
- OSForensics create Raw image format and support: (DD. AFF. AFM. VMDK. VHD and all EnCase Versions E01)

4.2.5 DF-05

Splitting the image using each forensic tool

Test Evaluation Criteria

We will split an image using Forensic Tool, which give investigator more space to analysis the image in different time and separate the image for many investigator.

Test Case Result

In FTK. Investigator can split the image into specific size by default 1500 Mb

In Prodiscover. Investigator cannot split the image bur has many option rather than splitting which is compression and conversion of the image

In Autopsy. Investigator cannot create image in segmented files in OSForensics. Investigator cannot split the raw image

In P2Commander. Investigator also cannot split the image

4.2.6 DF-06

Detect errors in imaging process

Test Evaluation Criteria

Create an image and check for errors in the image through imaging corrupted files

Test Case Result

FTK: the image is completed. But the files is corrupted.

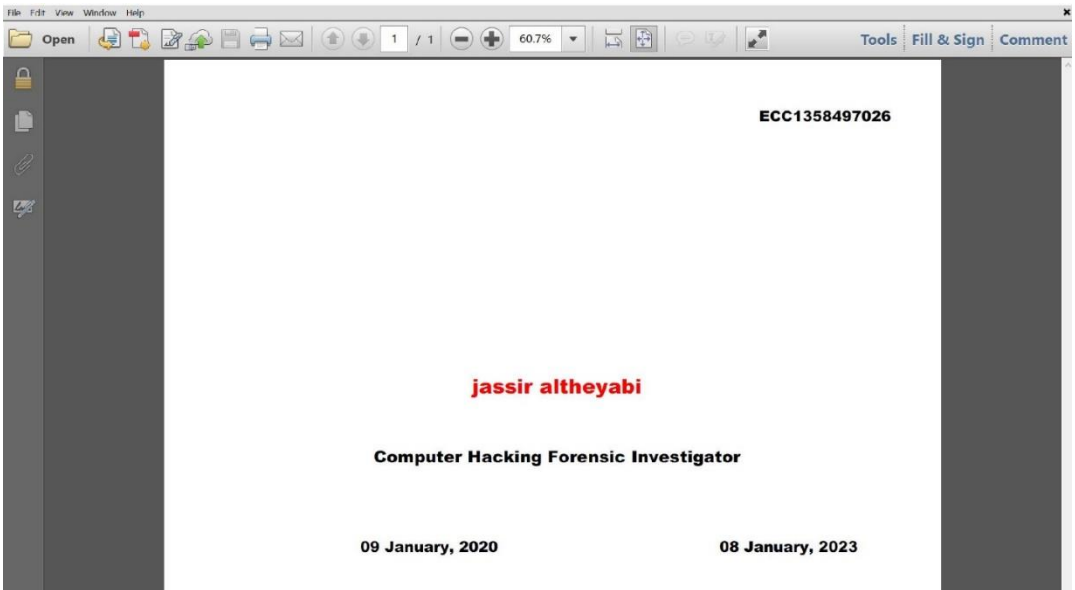

Figure 4.3: The Corrupted PDF File

Pro[illegible] imaging process is successfully completed. The "FTOI_Errors " is created to show any errors in the image.

Figure 4.4: The Original PDF File

For Autopsy. P2Commander and OSForensics create an image without demonstrating the errors

Description	Number of Documents Recovered					
	# To Recover	FTK	Prodiscover	Autopsy	P2Commander	OS Forensics
Excel	7	7	7	7	5	5
PDF	10	10	10	10	10	10
Pictures	7	7	7	7	7	7
Video	5	5	5	5	0	0
Word	8	8	8	8	6	6
Zip	5	5	5	5	5	5
All e-mails	25	25	25	25	25	25
PST	3	3	3	3	3	0
Presentations	7	7	7	7	7	7

4.2.7 DF-07

Create an image with the same previous image name

Test Evaluation Criteria:

To notice the accuracy of the tool in image modification.

Test Case Result:

FTK: able to overwritten the image after approval from the user. Autopsy: deny starting the image process. And ask the user to change the image name ProDiscover: display alert " FAT Volume may not handle " and ask the user for proceed the imaging anyway OSForensics: display alert that authenticate from the user to replace the existing image le. P2Commander: authenticate the changing of the existing image.

4.2.8 DF-08

This test builds up whether the devices can check the hash estimation of a picture. Pictures may should be hashed before preparing begins or after they have been explored to exhibit their respectability.

Findings of Hash Verification Test

Prodiscover:

At the point when a image le is opened in prodiscover that has not been verified. Prodiscover automatically verifies the image. Images can likewise be verified from inside Prodiscover at any phase by choosing Verify Evidence Files under the Tools Menu button in the Evidence tab. At the point when the Prodiscover images were made. The scientist chose just the MD5 hash choice and the coordinating securing and verification hash value. are recorded in the significant appendixes. The coordinating hashes of the pictures

FTK: FTK Images were verified in FTK by choosing the Verify Image Integrity choice for the Tools drop down menu. The verified hashes show that the digital forensics image were unaltered.

Autopsy: There was no choice to test the image hash inside Autopsy exhibit that the pictures had not been adjusted since they were made

OSForensics: Hash verification should be possible whenever by utilizing the md5sum or sha1sum group contingent upon which hash expected to be determined and contrasting them with those deter-mined after the picture was made.

P2Commander the matching acquisition and verification hashes for the images made can be viewed

Conclusion of Hash Verification Test:

Examination does not have the usefulness to check hash wholes. The various devices tried had the option to confirm the hash wholes of the pictures. Prodiscover played out this task automatically on unverified images.

Results:

FTK had the option to introduce the metadata from the E01 images opened in it and exceptionally distinguish the imaged media used to make all the images.

Prodiscover and Autopsy could not peruse this data and it must be acquired from the images logs. OSforensics had the option to set up the subtleties from E01 pictures

Prodiscover furnished the most detail as to the sequential quantities of the objective media from which the windows pictures were made.

Anyway the data gave by P2Commander in such manner was in-adequate to exceptionally identify the objective media. Measurable pictures made in Autopsy would not have contained this information as dd pictures do not contain metadata not at all like

Utilizing the Case Analyser the analyst had the option to create a Software. This Report from the Image. This report demonstrated that the Operating System was Windows 7 Home Basic and that it had been introduced on 1 May 2020 at 15:55. Remembered for this report were the Version. Item ID and establishment way

In autopsy. The tool has many advantages. Most notably that it fully supports the Arabic language and the flexibility to take a copy for certain parts of the hard disk such as extracting all emails that were contacted in any way. And a timeline for files.

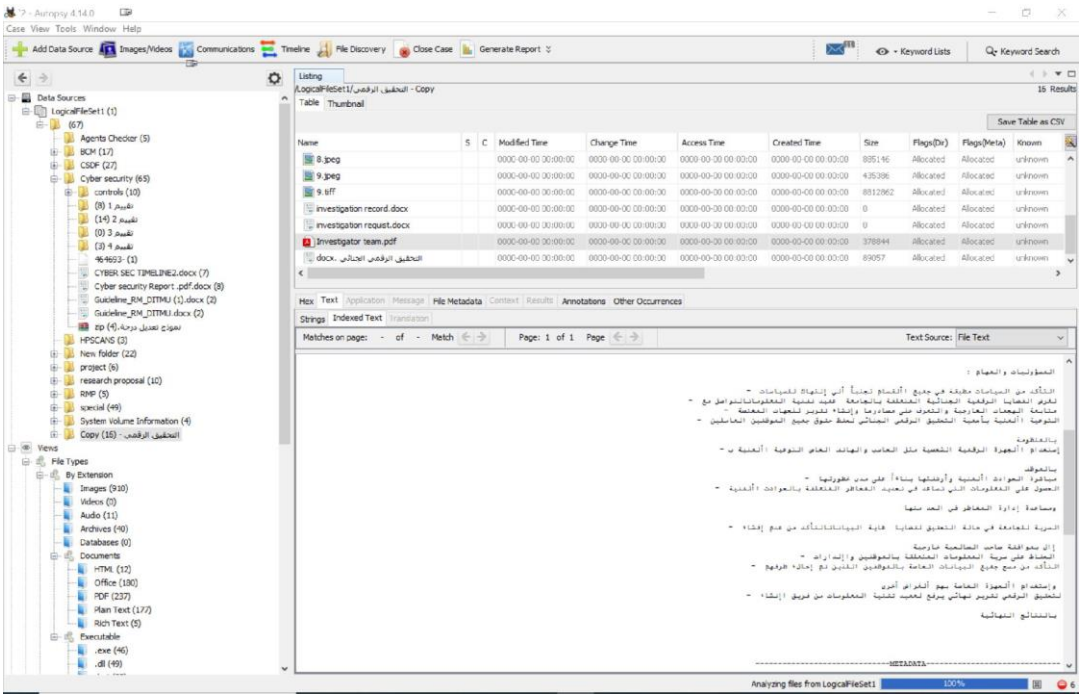

Figure 4.5: Supported Arabic Evidence

All instruments utilized had the option to accurately build up the subtleties of the working framework. The analyst couldn't build up the working framework date from any of the organized media.

Building up a software inventory was a simple matter of knowing to where to search. On condition of Windows PCs. The Software Key of the Windows Vault. And on condition of Linux. Programming inventories were found in the Debian Package Manger log (dpkg.log) situated in the/var/log catalog. In cases where these files were not automatically recuperated. Finding them was an issue of realizing what to look for. On account of Autopsy. A scan for a solitary expression brought about the whole well-suited reserve being recouped.

All instruments tried had the option to introduce total programming inventories for the Windows and Linux erased test images. Proof of introduced programming on the Windows and Linux organized test images could be discovered utilizing search capacities.

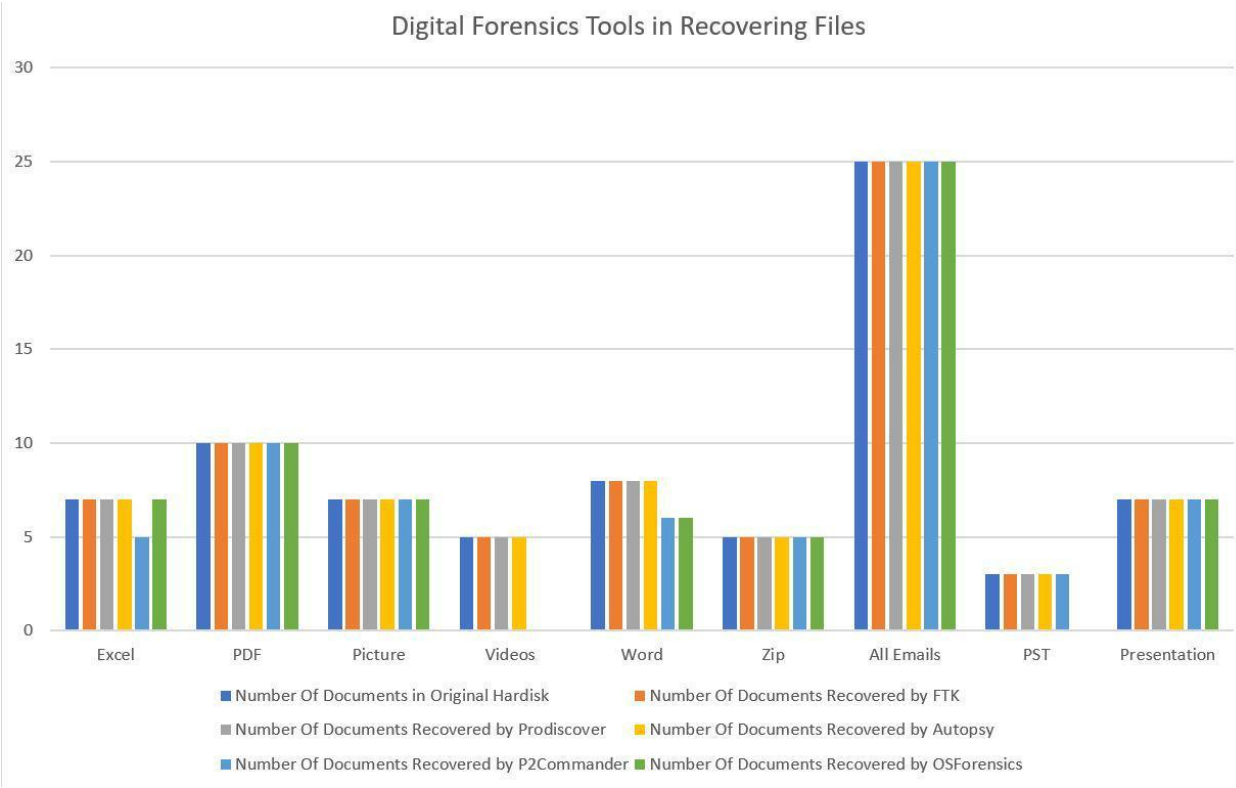

Figure 4.6: Digital Forensics Tools Comparison

Client details and log in activity could be removed from all deleted images tests utilizing all the tools tried. The specialist had the option to remove client details what's more. Activities from Windows images utilizing Prodiscover. FTK. OSForensics and P2Commander. Utilizing Autopsy the analyst had the option to build up client de-tails on the Windows images. No client activities on the organized images could be built up by the specialist utilizing Autoposy.

The relevant Registry entries and syslogs were recovered and presented from the Windows images respectively by all the tools tested.

All tools were successfully used to search for evidence of attached USB devices in unallocated space of the Windows images.

All tools were able to identify internet URLs on all images tested. FTK. Autopsy. Prodiscover. OSForensics and P2commander pre-sented internet browsing history and cookies for the deleted images and also provided last accessed dates. Only FTK was able to retrieve the browser details from the Windows Formatted Image.

5. Conclusion

The tools tried performed distinctively on the various media. No single tool set outperformed some other over all media. With all tried device sets exhibiting qualities more than each other on various media. These results exhibited that utilizing a blend of apparatuses may improve the investigative and testify capabilities of examiners. During the exploration it got obvious to the specialist that realizing where to look plays a more significant job than the apparatus in effectively recouping antiquities.

No doubt since the individual instruments sets didn't generally give similar outcomes it is judicious to have an advanced legal toolbox that comprises of various devices. It might be astute to incorporate open source instruments in such a toolbox since the cost associated with including an open source apparatus is

negligible. What is more? The potential benefit of having an extra competent tool set might be high.

6. Acknowledgements

To Doctor Talal Alharbi. My supervisor who was always available to guide and encourage me. First Majmaah University support. Resources and time o to complete my studies. Appreciation is also expressed to my colleagues for their encouragement and support.

7. References:

OShea K Clinton, T Reis, K Cohen, T Reyes, A Collins, E Schneider, S Cornell, J Schroader, A Cross, M Schuler, K Depew, L Varsalone, J Ehuan, A Wiles, J Gregg, M Wright, C Jean ,B R. Cardwell K. (2009). The Best Damn Cybercrime and Digital. Forensics Book Period. Syngress Publishing, Inc. You're Guide To Digital Information Seizure Incident Response and Computer Forensics.

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence.

Jordaan, J. (2015). Digital Forensic Examination Adavit. University of Cape Town.

Lyle, j. (2012). Computer Forensic Tool Testing Handbook. National Institute of Standards and Technology (NIST).

Shanmugam, K. (2011). Validating Digital Forensic Evidence. Ph.D. thesis, Brunel University School of Engineering and Design PhD Thesis, London.