Journal of Applied Engineering, Technology and Management (JAETM)

Forensic analysis of Scientific Linux image using commercial and opensource forensic tools

Tashi Wangchuk[1*], Younten Tshering[2], and Ngaira Mandela[3]

[1,2]*Department of Information Technology, Jigme Namgyel Engineering College, Royal University of Bhutan*

[3] *School of Digital Forensics and Cyber Security, National Forensic Sciences University*

[*]*Corresponding author: Tashi Wangchuk, tashiwangchuk.jnec@rub.edu.bt*

Published: June 2024

DOI: https://doi.org/10.54417/jaetm.v4i1.133

Abstract

Depending on their needs and personal preferences, people choose to use different operating systems (OS) such as Windows, Linux, and Mac. The scientific Linux Operating System (SLOS) is designed to provide a stable, secure, and high-performance computing environment for scientific research and education in a steady, scalable, and extensible manner. When criminal activities are committed by suspects involving computers and the internet, it calls for digital forensics which involves the use of scientific procedures and tools to carry out the forensic investigation and analysis of digital evidence for legal and investigative purposes. Forensic investigators use commercial and opensource tools for analysis and gathering inculpatory and exculpatory pieces of evidence. This paper presents a comparative analysis of EnCase, FTK, Autopsy, bulk-extractor, and Scalpel for analyzing the Scientific Linux image. The test scenarios were designed to find out if the selected forensic tools can be appropriately used for investigating crimes committed using the SLOS. The test scenarios include extraction and analysis of operating system details, user accounts, web browsing history, and the recovery of deleted and shredded files and this paper compares and evaluates the capability of the tools in retrieving the evidence designed in the scenarios. This systematic comparison and evaluation results would assist digital forensics practitioners, researchers, and law enforcement agencies in making informed decisions regarding the selection of tools for Scientific Linux image forensics.

Keywords— Digital forensics, evidence gathering, forensic analysis, forensic tools, Scientific Linux

1 Introduction

Digital forensics entails the collection, preservation, analysis, and presentation of digital evidence from various sources, such as computers, mobile devices, networks, and cloud services, and computer forensics involves extracting information from various sources like software, databases, the internet, and emails [1]. It plays a vital role in the investigation and prosecution of cybercrimes, such as hacking, fraud, identity theft, cyberterrorism, and child pornography. In addition, digital forensics also supports other domains, such as civil litigation, corporate security, and incident response. Investigations uncovering network details are beneficial, as they facilitate communication and information sharing between computers [2].

The rise of virtualization, distributed, and cloud computing poses new challenges in forensic science [3][4]. One of the challenges of digital forensics is the diversity and complexity of operating systems (OS) that the suspects and the victims of cybercrimes use. An OS is the software that manages a computer's hardware and software resources and provides the interface for the user to interact with the computer. There are different types of operating systems which include Windows, Linux, and Mac. OS has different features, functions, architectures, file systems, and security mechanisms.

Today's technology allows for evidence gathering from diverse hardware, including memory cards, smart cards, dongles, cameras, biometric scanners, routers, pagers, printers, answering machines, and GPS systems. This analysis concentrates on key features essential for the forensic examination of evidence. Areas not covered in this study include forensic readiness planning, evidence acquisition, protocols, protecting evidence integrity, and legal considerations in forensic investigations. Various digital data formats and types have led to the development of multiple analysis types, as classified by the Digital Forensics Research Workshop (DFRWS). [5] details the procedure and progression of digital forensic investigations.

Forensic investigators' selection of digital forensic tools depends on each case's unique characteristics and requirements [6][7]. Ideal forensic tools should support multiple platforms and operating systems, analyze different file systems, incorporate scripting for function automation, feature significant automated capabilities, and offer robust product support. Tools that provide comprehensive features and multi-platform support are typically more advantageous. A thorough evaluation of each tool's features aids investigators in choosing the most suitable tool, thus optimizing investigation time and effort. This allows investigators to concentrate on other investigation facets like case preparation, evidence collection, custody chain maintenance, and report writing.

OS Forensics (tool) identifies suspect files and activities through hash matching and drives signature comparisons, focusing on emails, memory, and binary data [8]. This tool facilitates rapid forensic evidence extraction and efficient data management, supporting various Windows versions and server platforms. OS Forensics, available in both trial and paid versions, boasts features like Misnamed file searching, Drive signature comparison, and discovering hidden disk areas.

The file system's significance in computing lies in organizing files indicating data locations, beginnings, and endings. Each file system, unique in size, follows a structure recognizable by any supporting computer [9]. File systems vary in structure, speed, flexibility, security, and size, with some tailored for specific applications, like ISO 9660 for optical discs [10].

Various storage devices support different file systems, for example, SSDs [11]. Examples include RAM as a temporary file system and network-accessible systems like NFS and SMB. File system analysis involves processing data within a partition or disk, including file listing, recovery of deleted content, and viewing sector content. [12] conducted a comprehensive review of the current state of research on dark web forensics, focusing on the methods, tools, and challenges associated with this field, emphasizing the importance of continuous improvement in darknet forensics technology for combating darknet crimes.

[13] explored Linux system architecture and forensic tools in "Linux Forensic Triage." This study delved into Linux system layers (Hardware, Kernel, Shell, Application) and various tools for Linux forensics, highlighting the value of open-source tools and the role of auditing, logging, and file system journaling. [14] examined open-source and closed-source tools for forensic analysis in "A Study of Linux Forensics." The study emphasized the effectiveness of open-source tools in Linux forensics, focusing on auditing, logging, and file system journaling as primary information sources. [15] in the State-of-the-art Tools and Techniques for Remote Digital Forensic Investigations", compared

advanced software and hardware tools for remote forensic acquisition, evaluating them based on outputs from memory, timeline, and live forensic imaging to determine the most effective techniques for remote investigations under various conditions.

Scientific Linux (SL) is a Linux distribution based on Red Hat Enterprise Linux (RHEL). Fermilab, CERN, and other scientific and academic institutions developed it. It is designed to provide a stable, secure, and high-performance computing environment for scientific research and education. SL is widely used in various fields, such as physics, astronomy, biology, and engineering. SL is also a potential platform for cybercriminals who seek to exploit its features and avoid detection. For example, SL offers a high degree of customization, allowing users to modify the OS according to their needs and preferences. SL also supports encryption and anonymization tools, such as LUKS, GPG, and Tor, which can protect the user's data and identity from unauthorized access and surveillance.

Operating System Forensics involves gleaning crucial information from a computer or mobile device's operating system [16] to secure empirical evidence against suspects. An OS, the first application to run at system startup, is analyzed for configuration files and output data to deduce possible events. [17] conducted a forensic analysis of the unencrypted layer in the Tor network to investigate the potential for de-anonymizing Tor users and determining their online activities. They focused on capturing and analyzing network traffic from the Tor Browser running in the Tails operating system.

Forensic tools must be able to handle each OS's specific characteristics and requirements and extract and analyze the relevant data and artifacts. Therefore, evaluating the performance and suitability of forensic tools for investigating digital crimes committed using the Scientific Linux operating system is important. However, there is a lack of research and literature on this topic. Most existing studies focus on comparing forensic tools for Windows, Mac OS, or Android OS, which are more popular and widely used than SL. Moreover, there is a debate on the advantages and disadvantages of commercial and open-source forensic tools, which have different features, costs, and licenses.

This paper aims to fill this gap by conducting a comparative analysis of five forensic tools, namely EnCase, FTK, Autopsy, bulk-extractor, and Scalpel for investigating digital crimes committed using SL. EnCase and FTK are commercial forensic tools widely used by law enforcement and the private sector. Autopsy, bulk-extractor, and Scalpel are open-source forensic tools that are freely available and can be modified by the user. The paper presents four test scenarios that cover the extraction and analysis of operating system details, user accounts, web browsing history, and deleted files. The paper compares and evaluates the tools' capability to retrieve artifacts. The paper also discusses the advantages and disadvantages of commercial and open-source forensic tools and provides recommendations for forensic practitioners and researchers.

2 Methods and Materials

2.1 Experimental design

As a part of the scenario preparation, the following environmental scenario was arranged to simulate how the suspects would use a device for committing the crime. The Scientific Linux 7.5 release was installed on the Oracle VM VirtualBox Manager (Version 5.2.16) and allocated the hard drive size of 8GB, 2048MB of RAM, and the system's timezone was set to Asia/Kolkata. The password for the root user was set to "abcde123" and another user with the name "zala" was created and assigned the password "abcde123". The Scientific Linux 7.5 was run and accessed the websites using the default browser of the operating system, that is "Konqueror", and in addition, files were also downloaded. While browsing the IP address was noted to be 10.0.2.15 (VirtualBox NAT). The sites visited are www.gfsu.edu.in and www.kuenselonline.com, downloaded file (QuickTimeInstaller.exe) from "ftp://jnec.edu.bt". To /mnt directory "FindMyDevice.pdf", "FindMyDevice.docx", "WHOIS.pdf", and "WHOIS.docx" were copied from the USB drive. The file FindMyDevice.pdf was removed using the remove (rm) command from the directory and the file WHOIS.docx was overwritten and removed securely using the command "shred -zvu 5 WHOIS.docx" command from the terminal.

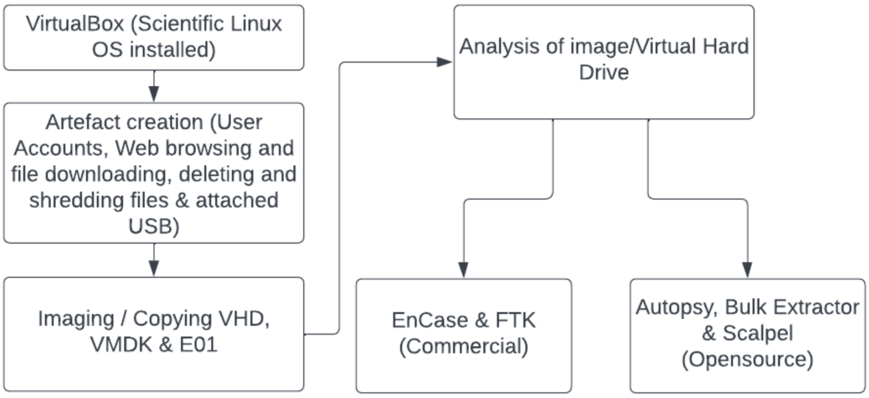

VirtualBox (Scientific Linux OS installed)
Artefact creation (User Accounts, Web browsing and file downloading, deleting and shredding files & attached USB)
Imaging / Copying VHD, VMDK & E01
Analysis of image/Virtual Hard Drive
EnCase & FTK (Commercial)
Autopsy, Bulk Extractor & Scalpel (Opensource)

Figure 1: Artefact creation and analysis process

2.2 Software used for image analysis

The forensic artifacts are subdivided into sections based on the different Forensic Tools used for analysing the evidence file and the expected type of evidence to be recovered from the evidence file after the analysis. The Forensic tools used for the analysis of the evidence file are EnCase, FTK, Autopsy, Bulk_extractor, and Scalpel.

3 Results and Discussion

The image or virtual hard drives copied from the VirtualBox were loaded into EnCase, FTK, Autopsy, Bulk Extractor, and Scalpel for analysis and retrieving the evidential artefacts. The results are presented in the following sections.

3.1 Analysis using EnCase

The EnCase after loading and analysing the image of the Scientific Linux 7.5 (Operating System), failed to show, the operating system version, operating system installation date, user accounts details, browsing and download history, file transfer history, deleted and shredded files (Recover), and the attached USB devices' details. Figure 2 shows the result of searching www.kuenselonline.com as the keyword but failed.

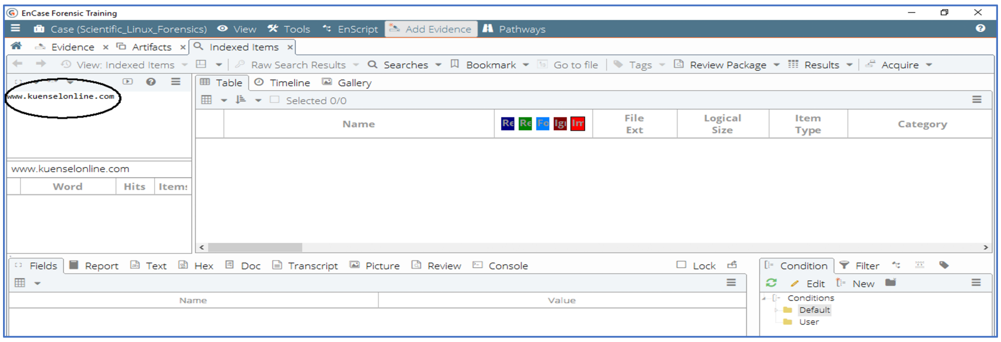


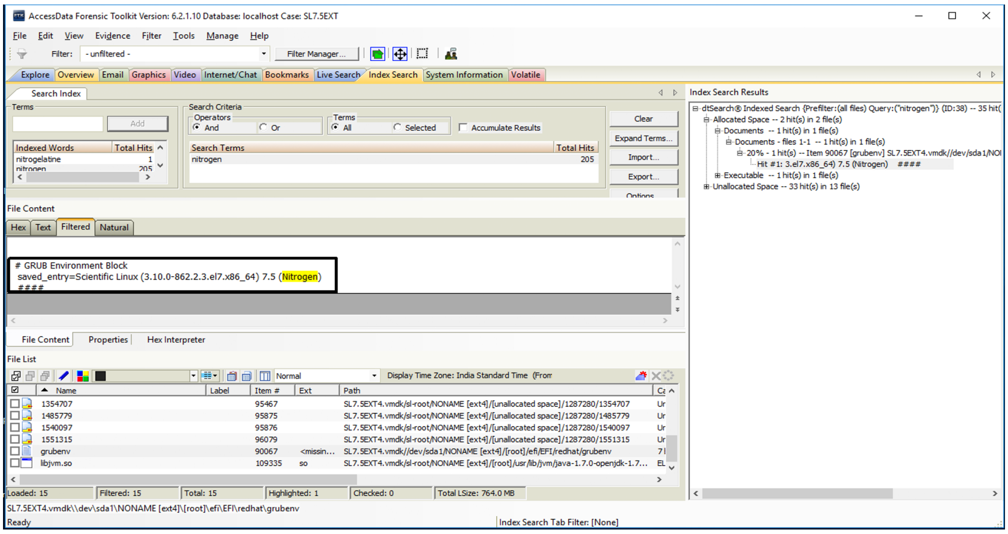
Figure 2: Searching the browsed website (www.kuenselonline.com) in the indexed items

3.2 Analysis using FTK

To recover the artifacts, FTK 6.2.1.10 was installed and the evidence file in the vmdk format was loaded. The FTK was able to analyse the evidence file but artifacts had to be manually searched using the index search feature. FTK after loading and analysing the image of the Scientific Linux 7.5 (Operating System), could not populate results and hence the index search feature was used to fetch the probable evidence. The following details were found using the keyword search as indicated by Figure 3, Figure 4Figure 5Figure 6Figure 7.

3.2.1 Operating System Version

The following figure shows the Operating System as Scientific Linux and version 7.5 (Nitrogen).



AccessData Forensic Toolkit Version: 6.2.1.10 Database: localhost Case: SL7.5EXT

File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Search Index
Terms
Add
Search Criteria
Operators
Clear
Expand Terms...
Import...
Export...
Options
File Content
Hex Text Filtered Natural
Properties
Hex Interpreter
File List

● And ○ Or | Terms: ● All ○ Selected | □ Accumulate Results

Indexed Words	Total Hits
nitrogelatine	1
nitrogen	205

Search Terms	Total Hits
nitrogen	205

```
# GRUB Environment Block
saved_entry=Scientific Linux (3.10.0-862.2.3.el7.x86_64) 7.5 (Nitrogen)
####
```

Index Search Results

```
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("nitrogen")} (ID:38) -- 35 hit(
   ⊟ Allocated Space -- 2 hit(s) in 2 file(s)
      ⊟ Documents  -- 1 hit(s) in 1 file(s)
         ⊟ Documents - files 1-1  -- 1 hit(s) in 1 file(s)
            ⊟ 20% - 1 hit(s) -- Item 90067 [grubenv] SL7.5EXT4.vmdk//dev/sda1/NOI
               Hit #1: 3.el7.x86_64) 7.5 (Nitrogen)   ####
      ⊞ Executable  -- 1 hit(s) in 1 file(s)
   ⊞ Unallocated Space -- 33 hit(s) in 13 file(s)
```

Normal | Display Time Zone: India Standard Time (From

☑	Name	Label	Item #	Ext	Path	Ca
□	1354707		95467		SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/[unallocated space]/1287280/1354707	Ur
□	1485779		95875		SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/[unallocated space]/1287280/1485779	Ur
□	1540097		95876		SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/[unallocated space]/1287280/1540097	Ur
□	1551315		96079		SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/[unallocated space]/1287280/1551315	Ur
□	grubenv		90067	<missin...	SL7.5EXT4.vmdk//dev/sda1/NONAME [ext4]/[root]/efi/EFI/redhat/grubenv	7 I
□	libjvm.so		109335	so	SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/[root]/usr/lib/jvm/java-1.7.0-openjdk-1.7...	EL

Loaded: 15 | Filtered: 15 | Total: 15 | Highlighted: 1 | Checked: 0 | Total LSize: 764.0 MB

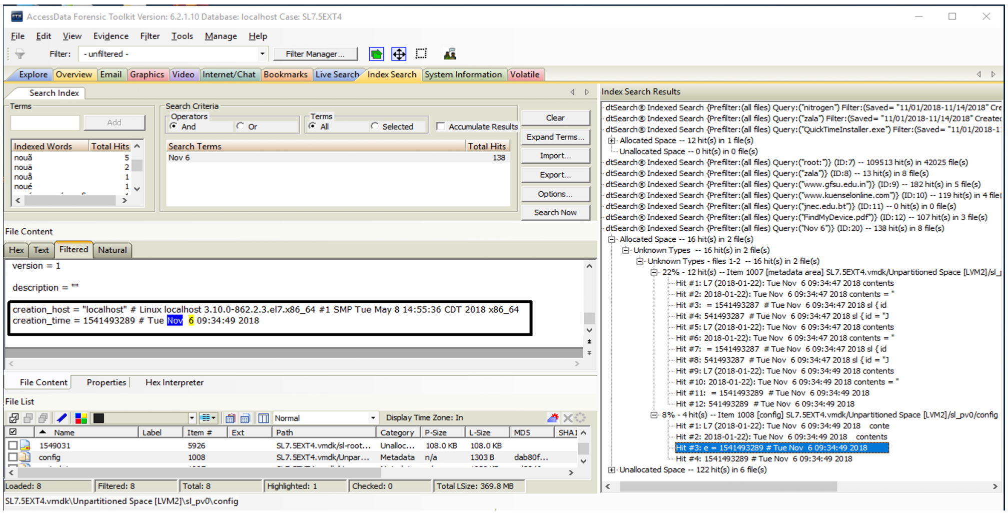
SL7.5EXT4.vmdk\\dev\sda1\NONAME [ext4]\[root]\efi\EFI\redhat\grubenv

Ready | Index Search Tab Filter: [None]

Figure 3: FTK showing OS name and version

3.2.2 Operating System Installation Date

The FTK has shown that the Operating System installation date in GMT format is Tuesday, 6th November 2018, and an approximate time also.



AccessData Forensic Toolkit Version: 6.2.1.10 Database: localhost Case: SL7.5EXT4

File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Search Index
Terms
Add
Search Criteria
Operators
Clear
Expand Terms...
Import...
Export...
Options...
Search Now
File Content
Hex Text Filtered Natural
Properties
Hex Interpreter
File List

● And ○ Or | Terms: ● All ○ Selected | □ Accumulate Results

Indexed Words	Total Hits
nouã	5
nouä	2
nouå	1
noué	1

Search Terms	Total Hits
Nov 6	138

```
version = 1

description = ""

creation_host = "localhost" # Linux localhost 3.10.0-862.2.3.el7.x86_64 #1 SMP Tue May 8 14:55:36 CDT 2018 x86_64
creation_time = 1541493289 # Tue Nov  6 09:34:49 2018
```

Index Search Results

```
dtSearch® Indexed Search {Prefilter:(all files) Query:("nitrogen") Filter:(Saved= "11/01/2018-11/14/2018" Cre
dtSearch® Indexed Search {Prefilter:(all files) Query:("zala") Filter:(Saved= "11/01/2018-11/14/2018" Createc
dtSearch® Indexed Search {Prefilter:(all files) Query:("QuickTimeInstaller.exe") Filter:(Saved= "11/01/2018-1
   ⊞ Allocated Space -- 12 hit(s) in 1 file(s)
     Unallocated Space -- 0 hit(s) in 0 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("root:")} (ID:7) -- 109513 hit(s) in 42025 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("zala")} (ID:8) -- 13 hit(s) in 8 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("www.gfsu.edu.in")} (ID:9) -- 182 hit(s) in 5 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("www.kuenselonline.com")} (ID:10) -- 119 hit(s) in 4 file(
dtSearch® Indexed Search {Prefilter:(all files) Query:("jnec.edu.bt")} (ID:11) -- 0 hit(s) in 0 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("FindMyDevice.pdf")} (ID:12) -- 107 hit(s) in 3 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("Nov 6")} (ID:20) -- 138 hit(s) in 8 file(s)
   ⊟ Allocated Space -- 16 hit(s) in 2 file(s)
      ⊟ Unknown Types  -- 16 hit(s) in 2 file(s)
         ⊟ Unknown Types - files 1-2  -- 16 hit(s) in 2 file(s)
            ⊟ 22% - 12 hit(s) -- Item 1007 [metadata area] SL7.5EXT4.vmdk/Unpartitioned Space [LVM2]/sl_
               Hit #1: L7 (2018-01-22): Tue Nov  6 09:34:47 2018 contents
               Hit #2: 2018-01-22): Tue Nov  6 09:34:47 2018 contents = "
               Hit #3:  = 1541493287  # Tue Nov  6 09:34:47 2018 sl { id
               Hit #4: 541493287  # Tue Nov  6 09:34:47 2018 sl { id = "J
               Hit #5: L7 (2018-01-22): Tue Nov  6 09:34:47 2018 contents
               Hit #6: 2018-01-22): Tue Nov  6 09:34:47 2018 contents = "
               Hit #7:  = 1541493287  # Tue Nov  6 09:34:47 2018 sl { id
               Hit #8: 541493287  # Tue Nov  6 09:34:47 2018 sl { id = "J
               Hit #9: L7 (2018-01-22): Tue Nov  6 09:34:49 2018 contents
               Hit #10: 2018-01-22): Tue Nov  6 09:34:49 2018 contents = "
               Hit #11:  = 1541493289  # Tue Nov  6 09:34:49 2018
               Hit #12: 541493289  # Tue Nov  6 09:34:49 2018
            ⊟ 8% - 4 hit(s) -- Item 1008 [config] SL7.5EXT4.vmdk/Unpartitioned Space [LVM2]/sl_pv0/config
               Hit #1: L7 (2018-01-22): Tue Nov  6 09:34:49 2018   conte
               Hit #2: 2018-01-22): Tue Nov  6 09:34:49 2018   contents
               Hit #3: e = 1541493289 # Tue Nov  6 09:34:49 2018
               Hit #4: 1541493289 # Tue Nov  6 09:34:49 2018
   ⊞ Unallocated Space -- 122 hit(s) in 6 file(s)
```

Normal | Display Time Zone: In

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1
□	1549031		5926		SL7.5EXT4.vmdk/sl-root...	Unalloc...	108.0 KB	108.0 KB		
□	config		1008		SL7.5EXT4.vmdk/Unpar...	Metadata	n/a	1303 B	dab80f...	

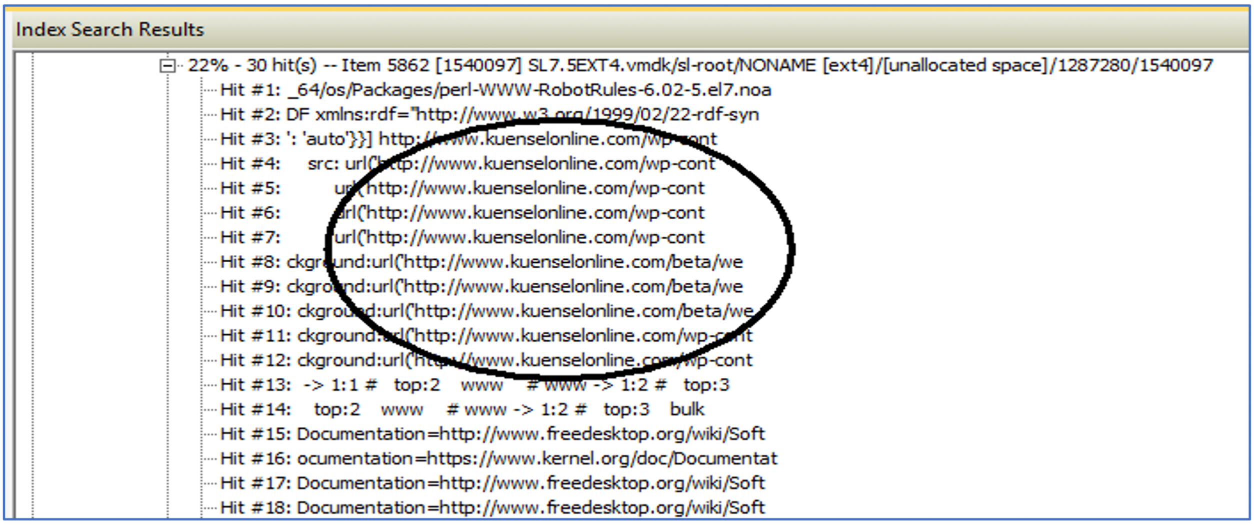
Loaded: 8 | Filtered: 8 | Total: 8 | Highlighted: 1 | Checked: 0 | Total LSize: 369.8 MB

SL7.5EXT4.vmdk\Unpartitioned Space [LVM2]\sl_pv0\config

Figure 4: FTK showing OS installation date and time in GMT

3.2.3 Browsing History

The autopsy shows the websites and the FTP sites being browsed when it is being searched using the keyword feature. The websites http://www.gfsu.edu.in and http://www.kuenselonline.com, and also the FTP site ftp://jnec.edu.bt are being fetched from the browsing history as shown in the following figures respectively.

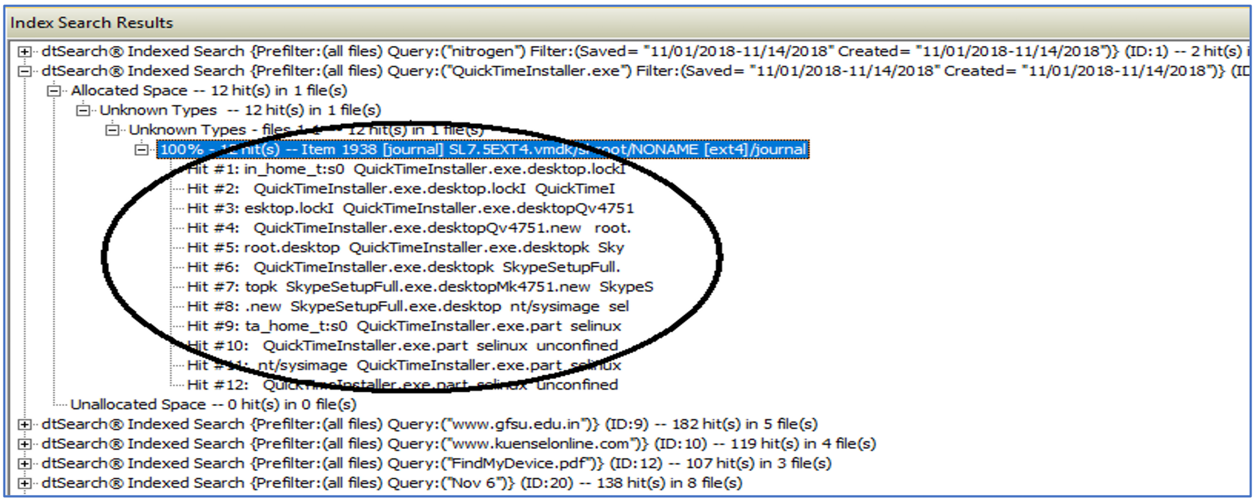


```
Index Search Results
22% - 30 hit(s) -- Item 5862 [1540097] SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/[unallocated space]/1287280/1540097
    Hit #1: _64/os/Packages/perl-WWW-RobotRules-6.02-5.el7.noa
    Hit #2: DF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syn
    Hit #3: ': 'auto'}}] http://www.kuenselonline.com/wp-cont
    Hit #4:     src: url('http://www.kuenselonline.com/wp-cont
    Hit #5:         url('http://www.kuenselonline.com/wp-cont
    Hit #6:         url('http://www.kuenselonline.com/wp-cont
    Hit #7:         url('http://www.kuenselonline.com/wp-cont
    Hit #8: ckground:url('http://www.kuenselonline.com/beta/we
    Hit #9: ckground:url('http://www.kuenselonline.com/beta/we
    Hit #10: ckground:url('http://www.kuenselonline.com/beta/we
    Hit #11: ckground:url('http://www.kuenselonline.com/wp-cont
    Hit #12: ckground:url('http://www.kuenselonline.com/wp-cont
    Hit #13:  -> 1:1 #   top:2    www     # www -> 1:2 #   top:3
    Hit #14:    top:2    www     # www -> 1:2 #   top:3    bulk
    Hit #15: Documentation=http://www.freedesktop.org/wiki/Soft
    Hit #16: ocumentation=https://www.kernel.org/doc/Documentat
    Hit #17: Documentation=http://www.freedesktop.org/wiki/Soft
    Hit #18: Documentation=http://www.freedesktop.org/wiki/Soft
```

Figure 5: FTK showing www.kuenselonline.com in the browsing history

3.2.4 Download History

The following figure shows the QuickTimeInstaller.exe being downloaded from the ftp://jnec.edu.bt FTP site.

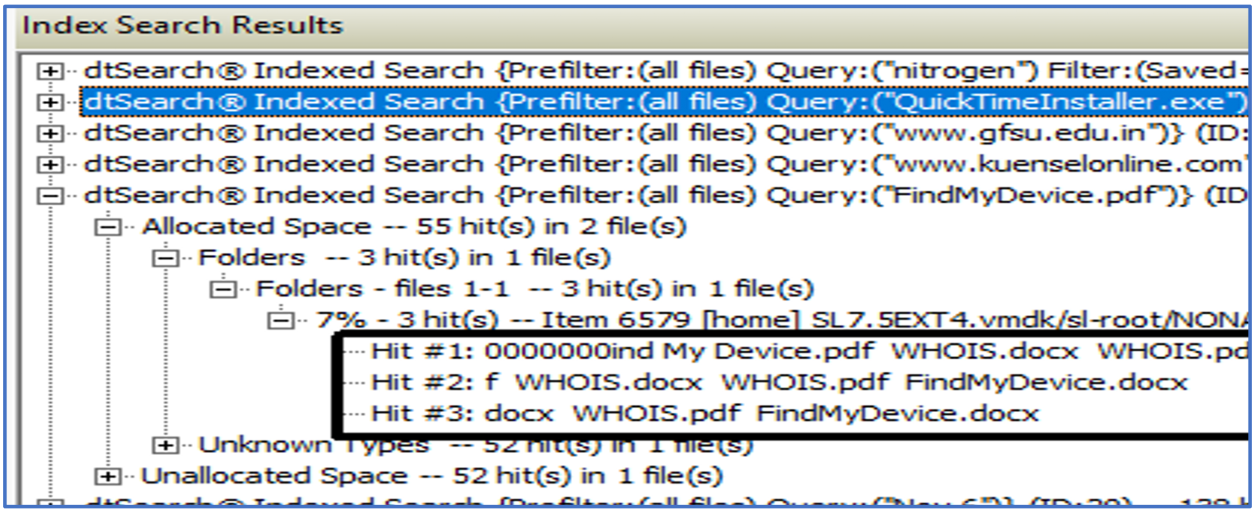


```
Index Search Results
+ dtSearch® Indexed Search {Prefilter:(all files) Query:("nitrogen") Filter:(Saved= "11/01/2018-11/14/2018" Created= "11/01/2018-11/14/2018")} (ID:1) -- 2 hit(s) i
- dtSearch® Indexed Search {Prefilter:(all files) Query:("QuickTimeInstaller.exe") Filter:(Saved= "11/01/2018-11/14/2018" Created= "11/01/2018-11/14/2018")} (ID
   - Allocated Space -- 12 hit(s) in 1 file(s)
      - Unknown Types  -- 12 hit(s) in 1 file(s)
         - Unknown Types - files 1-1 -- 12 hit(s) in 1 file(s)
            - 100% - 12 hit(s) -- Item 1938 [journal] SL7.5EXT4.vmdk/sl-root/NONAME [ext4]/journal
                Hit #1: in_home_t:s0  QuickTimeInstaller.exe.desktop.lockI
                Hit #2:   QuickTimeInstaller.exe.desktop.lockI  QuickTimeI
                Hit #3: esktop.lockI  QuickTimeInstaller.exe.desktopQv4751
                Hit #4:   QuickTimeInstaller.exe.desktopQv4751.new   root.
                Hit #5: root.desktop  QuickTimeInstaller.exe.desktopk  Sky
                Hit #6:   QuickTimeInstaller.exe.desktopk  SkypeSetupFull.
                Hit #7: topk  SkypeSetupFull.exe.desktopMk4751.new  SkypeS
                Hit #8: .new  SkypeSetupFull.exe.desktop  nt/sysimage  sel
                Hit #9: ta_home_t:s0  QuickTimeInstaller.exe.part  selinux
                Hit #10:   QuickTimeInstaller.exe.part  selinux  unconfined
                Hit #11:  nt/sysimage  QuickTimeInstaller.exe.part  selinux
                Hit #12:   QuickTimeInstaller.exe.part  selinux  unconfined
   Unallocated Space -- 0 hit(s) in 0 file(s)
+ dtSearch® Indexed Search {Prefilter:(all files) Query:("www.gfsu.edu.in")} (ID:9) -- 182 hit(s) in 5 file(s)
+ dtSearch® Indexed Search {Prefilter:(all files) Query:("www.kuenselonline.com")} (ID:10) -- 119 hit(s) in 4 file(s)
+ dtSearch® Indexed Search {Prefilter:(all files) Query:("FindMyDevice.pdf")} (ID:12) -- 107 hit(s) in 3 file(s)
+ dtSearch® Indexed Search {Prefilter:(all files) Query:("Nov 6")} (ID:20) -- 138 hit(s) in 8 file(s)
```

Figure 6: FTK showing QuickTimeInstaller.exe being downloaded from ftp://jnec.edu.bt

3.2.5 File Transfer History

The following figure shows four files Find My Device.pdf, WHOIS.pdf, WHOIS.docx, and FindMyDevice.docx being transferred.

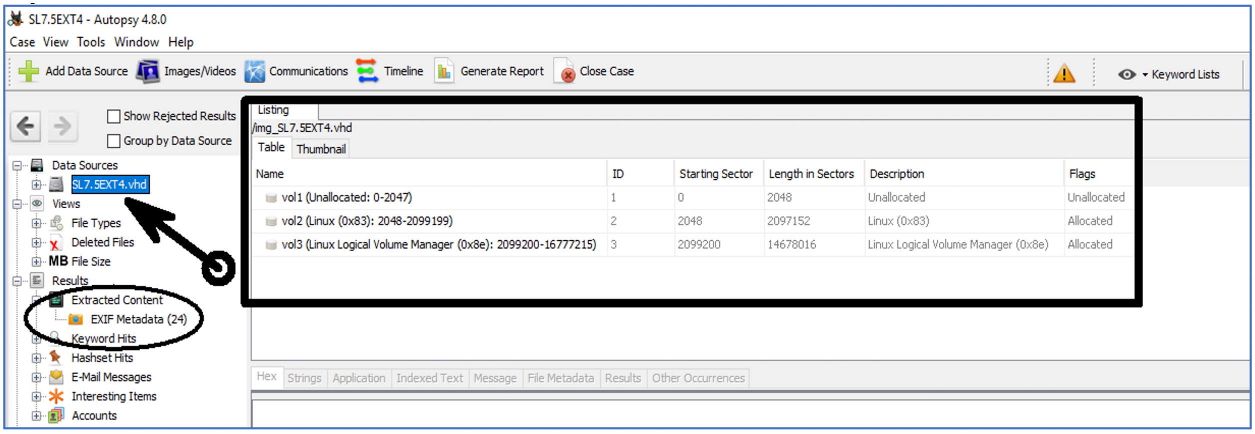


```
Index Search Results
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("nitrogen") Filter:(Saved=
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("QuickTimeInstaller.exe")
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("www.gfsu.edu.in")} (ID:
⊞ dtSearch® Indexed Search {Prefilter:(all files) Query:("www.kuenselonline.com"
⊟ dtSearch® Indexed Search {Prefilter:(all files) Query:("FindMyDevice.pdf")} (ID
    ⊟ Allocated Space -- 55 hit(s) in 2 file(s)
        ⊟ Folders -- 3 hit(s) in 1 file(s)
            ⊟ Folders - files 1-1 -- 3 hit(s) in 1 file(s)
                ⊟ 7% - 3 hit(s) -- Item 6579 [home] SL7.5EXT4.vmdk/sl-root/NON
                    Hit #1: 0000000ind My Device.pdf WHOIS.docx WHOIS.pd
                    Hit #2: f WHOIS.docx WHOIS.pdf FindMyDevice.docx
                    Hit #3: docx WHOIS.pdf FindMyDevice.docx
        ⊞ Unknown Types -- 52 hit(s) in 1 file(s)
    ⊞ Unallocated Space -- 52 hit(s) in 1 file(s)
```

Figure 7: FTK shows four files being transferred

3.3 Analysis using Autopsy

To recover the artifacts, Autopsy 4.8.0 was installed and the evidence file in the vhd format was loaded. The Autopsy was able to analyse the evidence file but did not populate any pieces of evidence in the Extracted Contents category under the Results section. The artifacts had to be manually searched using the keyword search feature.



/img_SL7.5EXT4.vhd

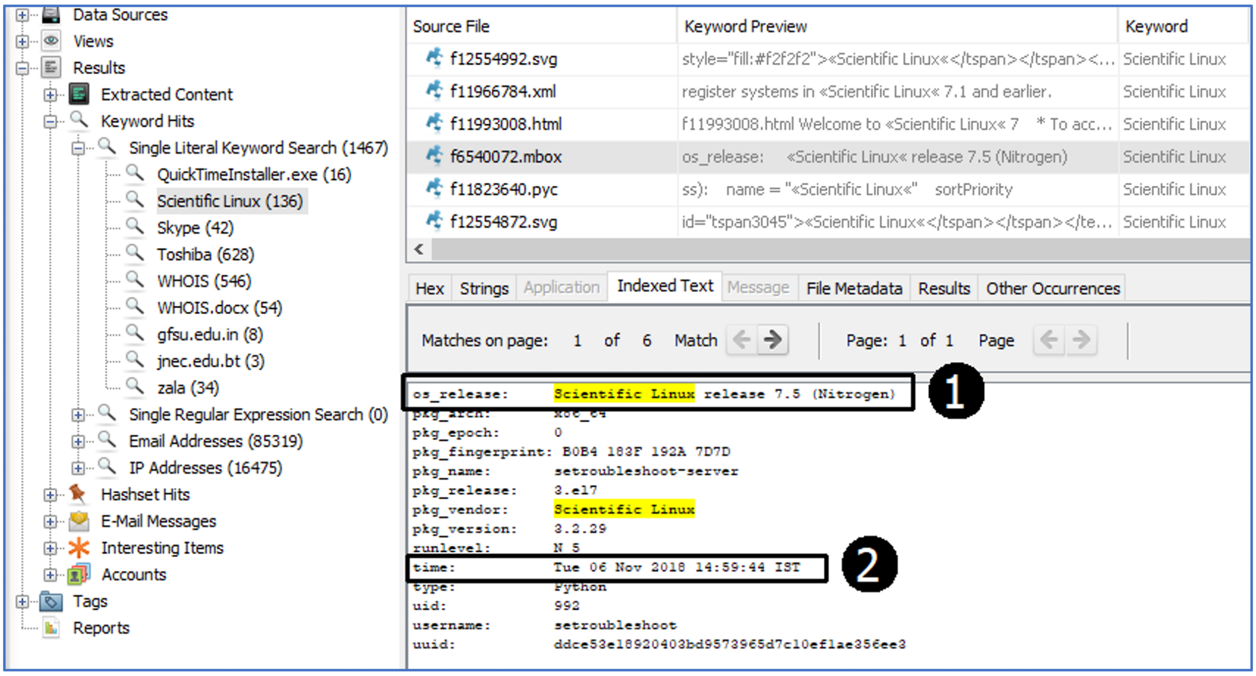
Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (Linux (0x83): 2048-2099199)	2	2048	2097152	Linux (0x83)	Allocated
vol3 (Linux Logical Volume Manager (0x8e): 2099200-16777215)	3	2099200	14678016	Linux Logical Volume Manager (0x8e)	Allocated

Figure 8: Image loaded in the vhd format in Autopsy

The Autopsy after loading and analysing the image of the Scientific Linux 7.5 (Operating System), could not populate results and hence the keyword search feature was used to fetch the probable evidence. The following details were found using the keyword search as indicated by Figure 9, Figure 10, Figure 11, Figure 12, Figure 13, Figure 14, and Figure 15.

3.3.1 Operating System Version and Installation Date

The following figure shows the Operating System as Scientific Linux 7.5 and the date of installation is indicated as Tuesday, 6th of November 2018 respectively.



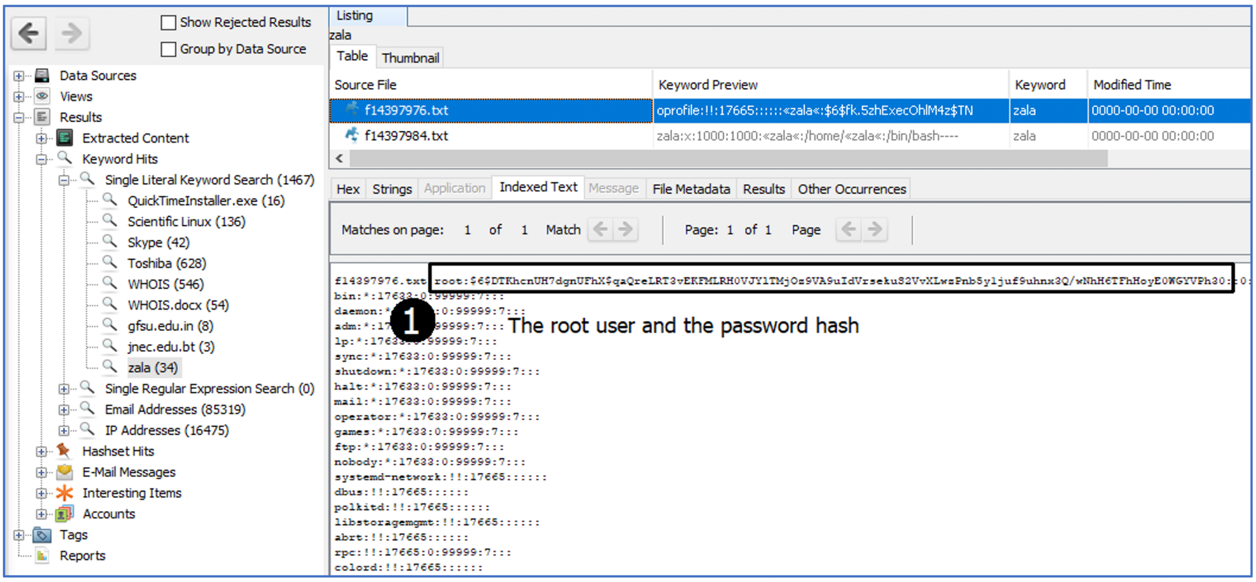
Source File	Keyword Preview	Keyword
f12554992.svg	style="fill:#f2f2f2">«Scientific Linux«</tspan></tspan><...	Scientific Linux
f11966784.xml	register systems in «Scientific Linux« 7.1 and earlier.	Scientific Linux
f11993008.html	f11993008.html Welcome to «Scientific Linux« 7 * To acc...	Scientific Linux
f6540072.mbox	os_release: «Scientific Linux« release 7.5 (Nitrogen)	Scientific Linux
f11823640.pyc	ss): name = "«Scientific Linux«" sortPriority	Scientific Linux
f12554872.svg	id="tspan3045">«Scientific Linux«</tspan></tspan></te...	Scientific Linux

```
os_release:      Scientific Linux release 7.5 (Nitrogen)
pkg_arch:        x86_64
pkg_epoch:       0
pkg_fingerprint: B0B4 183F 192A 7D7D
pkg_name:        setroubleshoot-server
pkg_release:     3.el7
pkg_vendor:      Scientific Linux
pkg_version:     3.2.29
runlevel:        N 5
time:            Tue 06 Nov 2018 14:59:44 IST
type:            Python
uid:             992
username:        setroubleshoot
uuid:            ddce53e18920403bd9573965d7c10ef1ae356ee3
```

Figure 9: Autopsy showing OS name, version, and installation date

3.3.2 User Accounts Details

The details of the user account such as the root user and the normal user account which was present in the evidence file are being fetched as indicated in the following Figure 10.



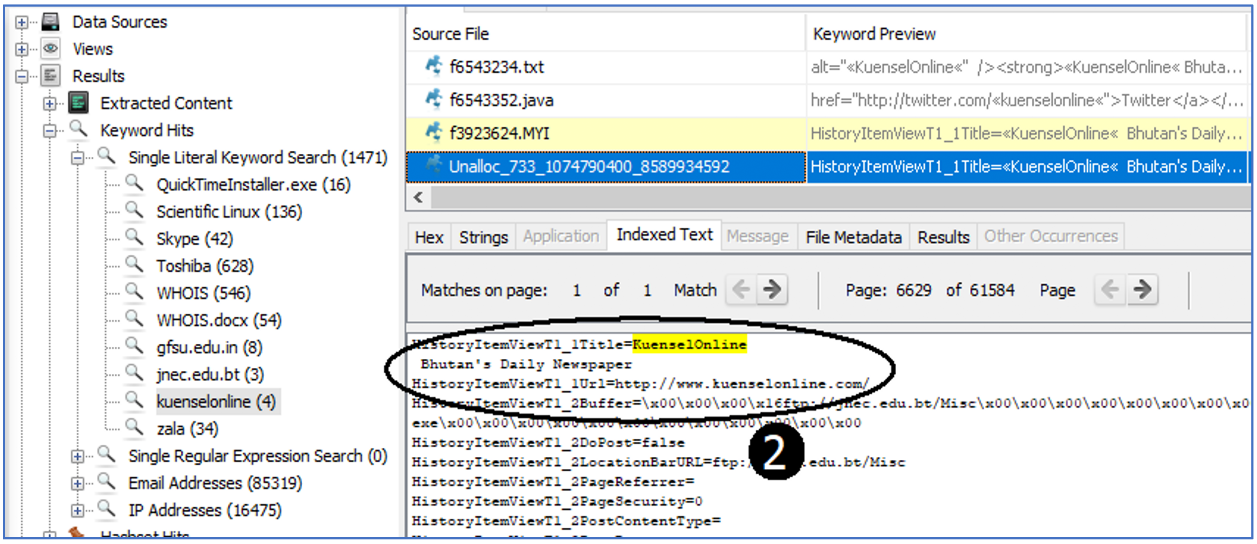
Source File	Keyword Preview	Keyword	Modified Time
f14397976.txt	oprofile:!!:17665::::::«zala«:$6$fk.5zhExecOhlM4z$TN	zala	0000-00-00 00:00:00
f14397984.txt	zala:x:1000:1000:«zala«:/home/«zala«:/bin/bash----	zala	0000-00-00 00:00:00

```
f14397976.txt root:$6$DTKhcnUH7dgnUFhX$qaQreLRT3vEKFMLRH0VJY1TMjOs9VA9uIdVrseku82VvXLwsPnb5y1juf9uhnx3Q/wNhH6TFhHoyE0WGYVPh30::0:
bin:*:17633:0:99999:7:::
daemon:*    :0:99999:7:::
adm:*:17    99999:7:::
lp:*:1763   :99999:7:::
sync:*:17633:0:99999:7:::
shutdown:*:17633:0:99999:7:::
halt:*:17633:0:99999:7:::
mail:*:17633:0:99999:7:::
operator:*:17633:0:99999:7:::
games:*:17633:0:99999:7:::
ftp:*:17633:0:99999:7:::
nobody:*:17633:0:99999:7:::
systemd-network:!!:17665::::::
dbus:!!:17665::::::
polkitd:!!:17665::::::
libstoragemgmt:!!:17665::::::
abrt:!!:17665::::::
rpc:!!:17665:0:99999:7:::
colord:!!:17665::::::
```

Figure 10: Autopsy showing root user and its password hash

3.3.3 Browsing History

The autopsy shows the websites and the FTP sites being browsed when it is being searched using the keyword feature. The websites http://www.gfsu.edu.in and http://www.kuenselonline.com, and also the FTP site ftp://jnec.edu.bt are being fetched from the browsing history as shown in the following figures respectively.



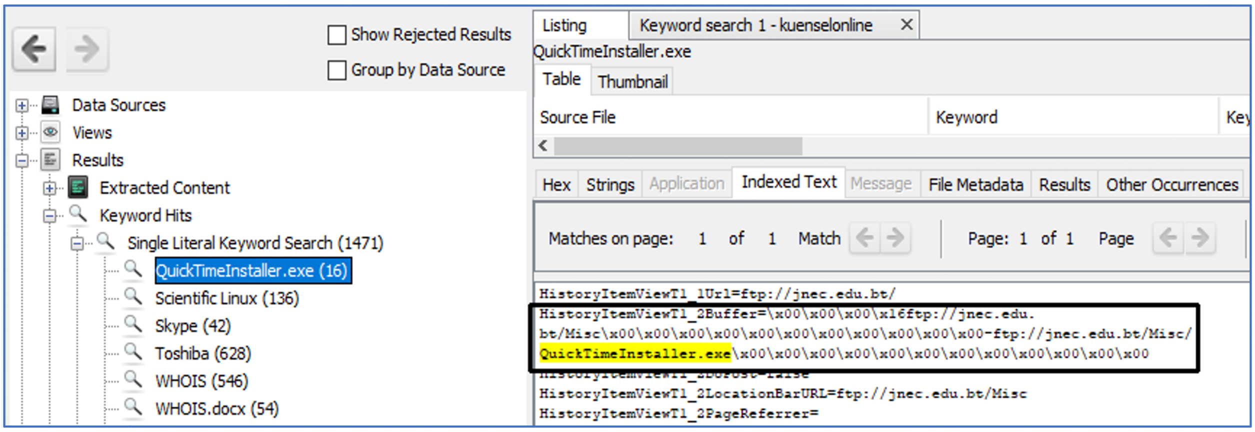
Source File	Keyword Preview
f6543234.txt	alt="«KuenselOnline«" /><strong>«KuenselOnline« Bhuta…
f6543352.java	href="http://twitter.com/«kuenselonline«">Twitter</a></…
f3923624.MYI	HistoryItemViewT1_1Title=«KuenselOnline« Bhutan's Daily…
Unalloc_733_1074790400_8589934592	HistoryItemViewT1_1Title=«KuenselOnline« Bhutan's Daily…

```
HistoryItemViewT1_1Title=KuenselOnline
 Bhutan's Daily Newspaper
HistoryItemViewT1_1Url=http://www.kuenselonline.com/
HistoryItemViewT1_2Buffer=\x00\x00\x00\x16ftp://jnec.edu.bt/Misc\x00\x00\x00\x00\x00\x00\x00\x0
exe\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
HistoryItemViewT1_2DoPost=false
HistoryItemViewT1_2LocationBarURL=ftp://jnec.edu.bt/Misc
HistoryItemViewT1_2PageReferrer=
HistoryItemViewT1_2PageSecurity=0
HistoryItemViewT1_2PostContentType=
```

Figure 11: Autopsy showing www.kuenselonline.com in the browsing history

3.3.4 Download History

The following figure shows the QuickTimeInstaller.exe being downloaded from the ftp://jnec.edu.bt FTP site.



```
HistoryItemViewT1_1Url=ftp://jnec.edu.bt/
HistoryItemViewT1_2Buffer=\x00\x00\x00\x16ftp://jnec.edu.
bt/Misc\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00-ftp://jnec.edu.bt/Misc/
QuickTimeInstaller.exe\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
HistoryItemViewT1_2DoPost=false
HistoryItemViewT1_2LocationBarURL=ftp://jnec.edu.bt/Misc
HistoryItemViewT1_2PageReferrer=
```

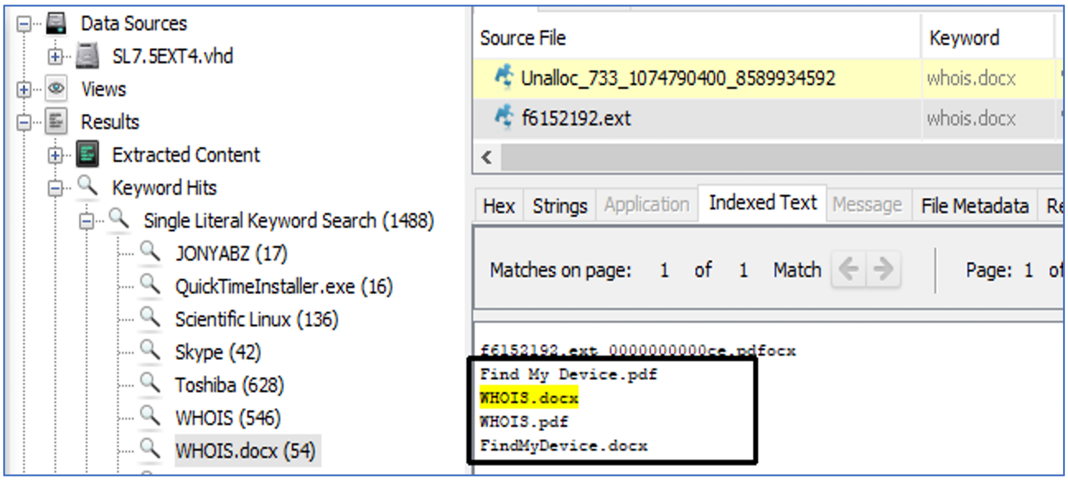
Figure 12: Autopsy showing QuickTimeInstaller.exe being downloaded from ftp://jnec.edu.bt

3.3.5 File Transfer History

The following figure shows four files "Find My Device.pdf", "WHOIS.pdf", "WHOIS.docx" and "FindMyDevice.docx" being transferred.

3.3.6 Deleted and Shredded Files (Recovery)

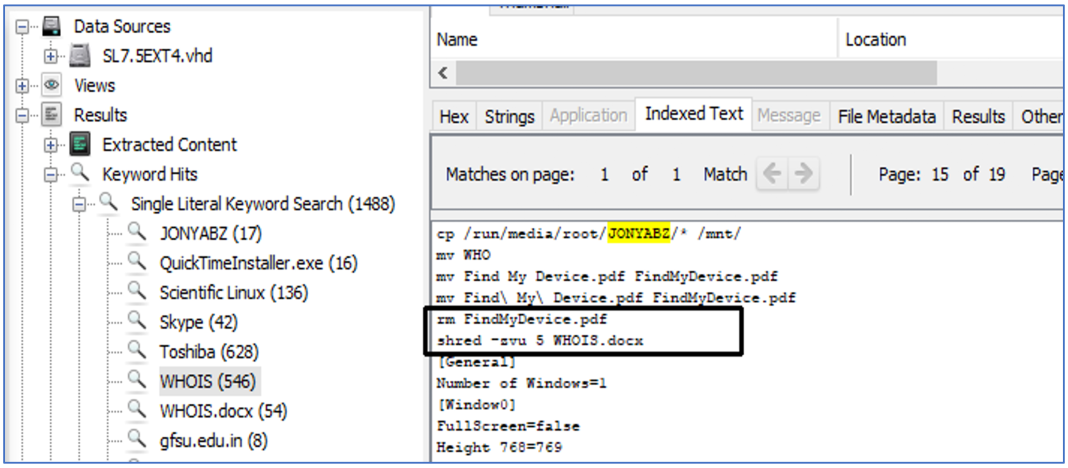
Although the files that are being removed using the rm command, overwritten and removed using the shred command are not being recovered, the command history indicates that the file "FindMyDevice.pdf" was removed and the file "WHOIS.docx" was overwritten five times and removed.



Source File	Keyword
Unalloc_733_1074790400_8589934592	whois.docx
f6152192.ext	whois.docx

```
f6152192.ext 0000000000ce.pdfocx
Find My Device.pdf
WHOIS.docx
WHOIS.pdf
FindMyDevice.docx
```

Figure 13: Autopsy showing four files being transferred

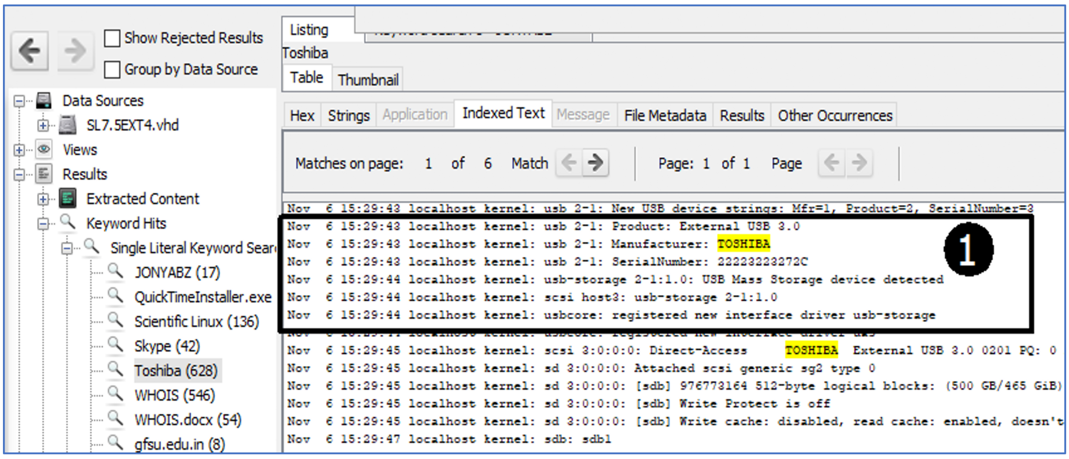


```
cp /run/media/root/JONYABZ/* /mnt/
mv WHO
mv Find My Device.pdf FindMyDevice.pdf
mv Find\ My\ Device.pdf FindMyDevice.pdf
rm FindMyDevice.pdf
shred -zvu 5 WHOIS.docx
[General]
Number of Windows=1
[Window0]
FullScreen=false
Height 768=769
```

Figure 14: Autopsy showing files being removed and shredded

3.3.7 Attached USB Devices' Details

The Autopsy has shown that two storage devices have been connected to the system (1) External USB 3.0 with serial number 22223223272C manufactured by Toshiba company.

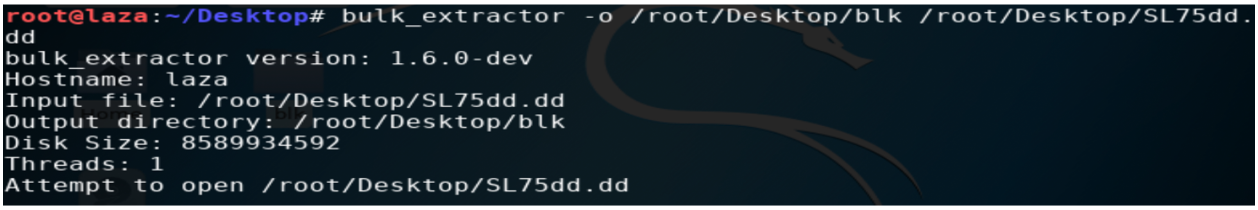


```
Nov  6 15:29:43 localhost kernel: usb 2-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
Nov  6 15:29:43 localhost kernel: usb 2-1: Product: External USB 3.0
Nov  6 15:29:43 localhost kernel: usb 2-1: Manufacturer: TOSHIBA
Nov  6 15:29:43 localhost kernel: usb 2-1: SerialNumber: 22223223272C
Nov  6 15:29:44 localhost kernel: usb-storage 2-1:1.0: USB Mass Storage device detected
Nov  6 15:29:44 localhost kernel: scsi host3: usb-storage 2-1:1.0
Nov  6 15:29:44 localhost kernel: usbcore: registered new interface driver usb-storage
Nov  6 15:29:45 localhost kernel: scsi 3:0:0:0: Direct-Access     TOSHIBA  External USB 3.0 0201 PQ: 0
Nov  6 15:29:45 localhost kernel: sd 3:0:0:0: Attached scsi generic sg2 type 0
Nov  6 15:29:45 localhost kernel: sd 3:0:0:0: [sdb] 976773164 512-byte logical blocks: (500 GB/465 GiB)
Nov  6 15:29:45 localhost kernel: sd 3:0:0:0: [sdb] Write Protect is off
Nov  6 15:29:45 localhost kernel: sd 3:0:0:0: [sdb] Write cache: disabled, read cache: enabled, doesn't
Nov  6 15:29:47 localhost kernel: sdb: sdb1
```

Figure 15: Autopsy showing External USB 3.0 attached

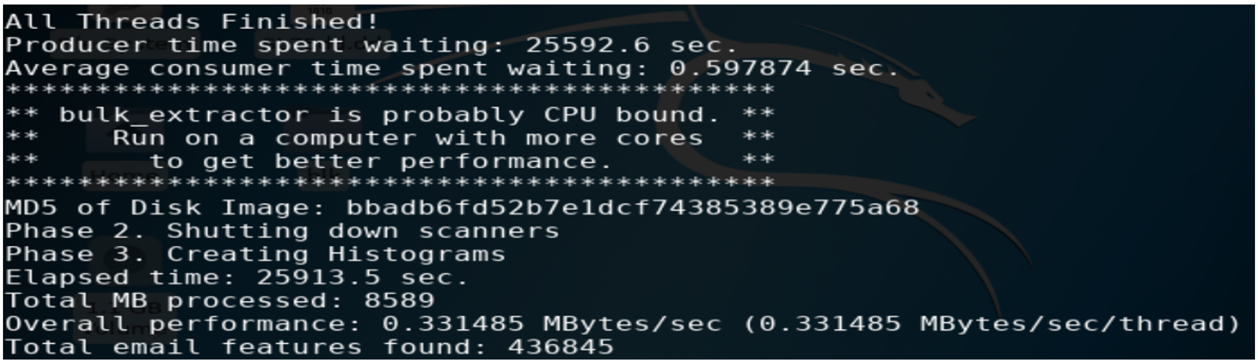
3.4 Analysis using Bulk Extractor

To extract the URL features from the evidence image file, bulk_extrcator version 6.2.1.10 was used from the Kali Linux. The image file in the raw format (dd) was fed into the bulk_extractor and was analyzed.



```
root@laza:~/Desktop# bulk_extractor -o /root/Desktop/blk /root/Desktop/SL75dd.
dd
bulk_extractor version: 1.6.0-dev
Hostname: laza
Input file: /root/Desktop/SL75dd.dd
Output directory: /root/Desktop/blk
Disk Size: 8589934592
Threads: 1
Attempt to open /root/Desktop/SL75dd.dd
```

Figure 16: Image loaded in the dd format to bulk_extractor

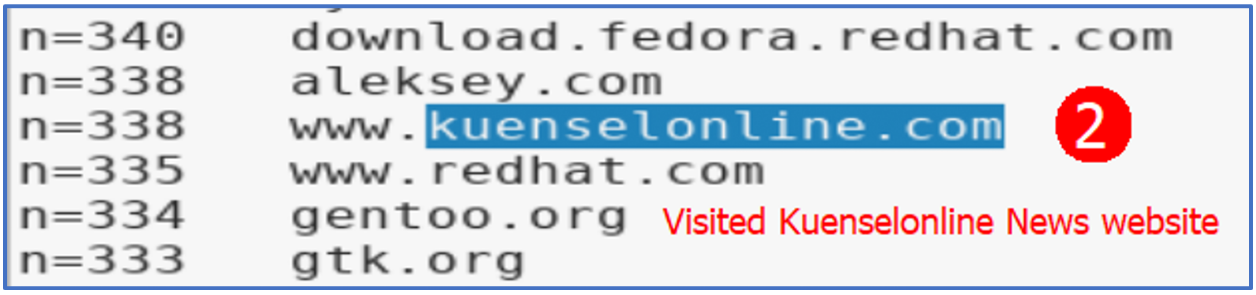


```
All Threads Finished!
Producer time spent waiting: 25592.6 sec.
Average consumer time spent waiting: 0.597874 sec.
*******************************************
** bulk_extractor is probably CPU bound.  **
**    Run on a computer with more cores   **
**      to get better performance.        **
*******************************************
MD5 of Disk Image: bbadb6fd52b7e1dcf74385389e775a68
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 25913.5 sec.
Total MB processed: 8589
Overall performance: 0.331485 MBytes/sec (0.331485 MBytes/sec/thread)
Total email features found: 436845
```

Figure 17: The image is scanned and the featured extracted

3.4.1 Browsing History Fetched using bulk_extractor

After scanning for the regular expressions, the bulk_extractor fetched the URLs which were browsed on the Scientific Linux 7.5 system.

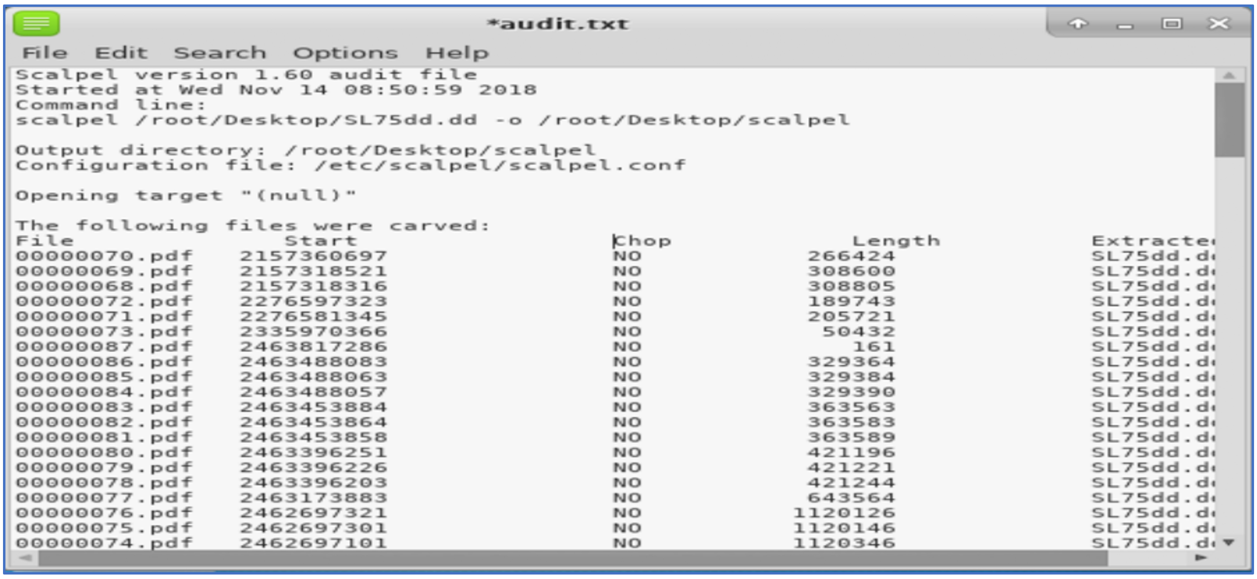


```
n=340    download.fedora.redhat.com
n=338    aleksey.com
n=338    www.kuenselonline.com
n=335    www.redhat.com
n=334    gentoo.org
n=333    gtk.org
```

Figure 18: Browsed URL www.kuenselonline.com being listed by bulk_extractor

3.5 Analysis using Scalpel

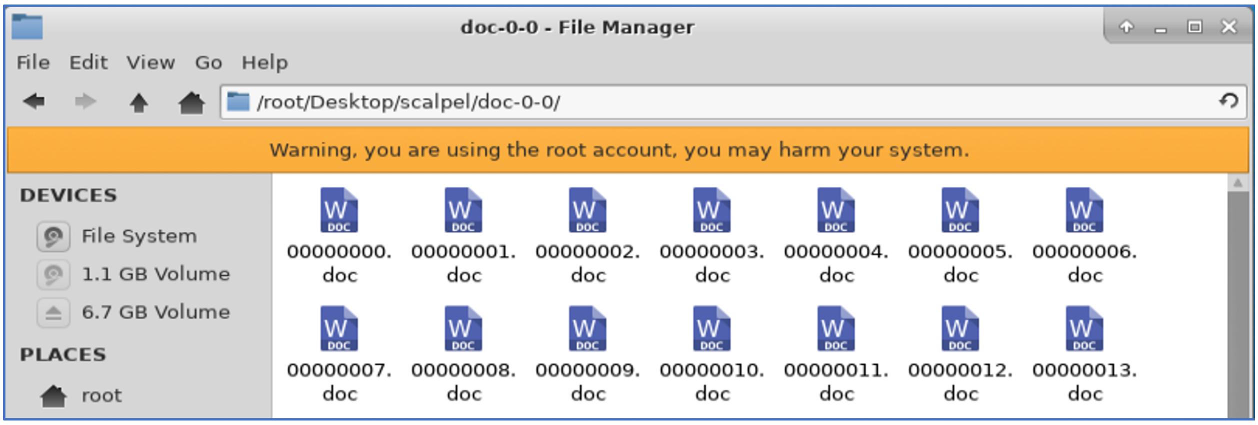
To recover the files from the evidence image, Scalpel from the Kali Linux was used and the image in dd format was fed to the Scalpel for recovery by using the command "scalpel /root/Desktop/SL75dd.dd -o /root/Desktop/scalpel" by being in the /etc/scalpel directory.



```
Scalpel version 1.60 audit file
Started at Wed Nov 14 08:50:59 2018
Command line:
scalpel /root/Desktop/SL75dd.dd -o /root/Desktop/scalpel

Output directory: /root/Desktop/scalpel
Configuration file: /etc/scalpel/scalpel.conf

Opening target "(null)"

The following files were carved:
File              Start                     Chop           Length         Extracte
00000070.pdf    2157360697                  NO             266424         SL75dd.d
00000069.pdf    2157318521                  NO             308600         SL75dd.d
00000068.pdf    2157318316                  NO             308805         SL75dd.d
00000072.pdf    2276597323                  NO             189743         SL75dd.d
00000071.pdf    2276581345                  NO             205721         SL75dd.d
00000073.pdf    2335970366                  NO              50432         SL75dd.d
00000087.pdf    2463817286                  NO                161         SL75dd.d
00000086.pdf    2463488083                  NO             329364         SL75dd.d
00000085.pdf    2463488063                  NO             329384         SL75dd.d
00000084.pdf    2463488057                  NO             329390         SL75dd.d
00000083.pdf    2463453884                  NO             363563         SL75dd.d
00000082.pdf    2463453864                  NO             363583         SL75dd.d
00000081.pdf    2463453858                  NO             363589         SL75dd.d
00000080.pdf    2463396251                  NO             421196         SL75dd.d
00000079.pdf    2463396226                  NO             421221         SL75dd.d
00000078.pdf    2463396203                  NO             421244         SL75dd.d
00000077.pdf    2463173883                  NO             643564         SL75dd.d
00000076.pdf    2462697321                  NO            1120126         SL75dd.d
00000075.pdf    2462697301                  NO            1120146         SL75dd.d
00000074.pdf    2462697101                  NO            1120346         SL75dd.d
```

Figure 19: Summary of the carved file by Scalpel

After the scanning and carving, the carved files are categorized into .doc and .pdf and would be stored in the specified directory. However, the file names are not the actual file names; Scalpel is naming them with numeric values with either .doc or .pdf extensions.

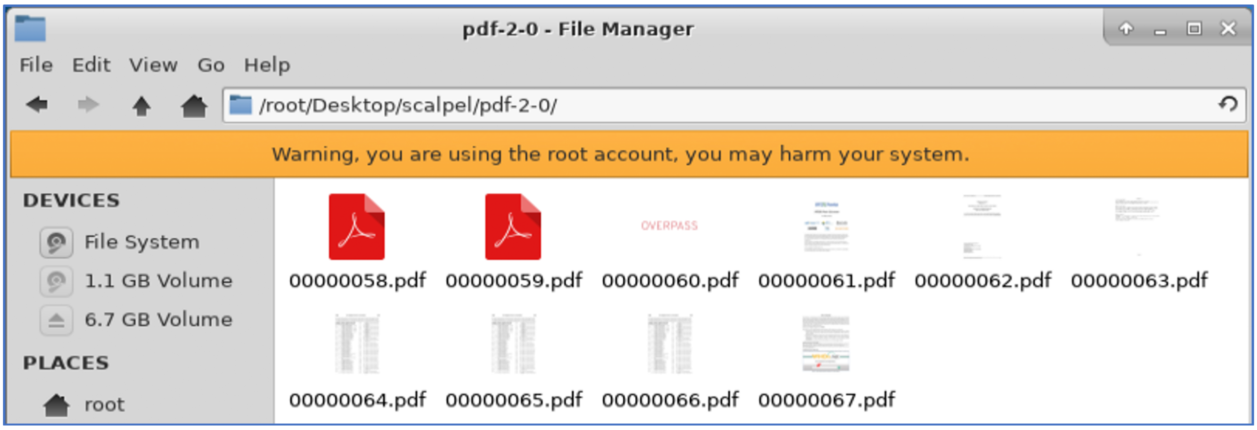


/root/Desktop/scalpel/doc-0-0/

Warning, you are using the root account, you may harm your system.

00000000.doc 00000001.doc 00000002.doc 00000003.doc 00000004.doc 00000005.doc 00000006.doc
00000007.doc 00000008.doc 00000009.doc 00000010.doc 00000011.doc 00000012.doc 00000013.doc

Figure 20: Carved doc files using the Scalpel



/root/Desktop/scalpel/pdf-2-0/

Warning, you are using the root account, you may harm your system.

00000058.pdf 00000059.pdf 00000060.pdf 00000061.pdf 00000062.pdf 00000063.pdf
00000064.pdf 00000065.pdf 00000066.pdf 00000067.pdf

Figure 21: Carved PDF files using the Scalpel

3.6 Comparison Chart

The following comparison chart was derived after the attempt to examine the Scientific Linux 7.5 image file was made using the EnCase, FTK, Autopsy, Bulk_extractor, and the Scalpel forensic tools. Table 1. Comparison Chart of forensic tools' capability

Table 1: Comparison of Forensic Tools

Forensic Evidence	**EnCase**	**FTK**	**Autopsy**	**Bulk Extractor**	**Scalpel**
OS name and version	No	Yes	Yes	No	No
OS installation date	No	Yes	Yes	No	No
User account list	No	No	Yes	No	No
Browsing history	No	Yes	Yes	Yes	No
Download history	No	Yes	Yes	No	No
File transfer history	No	Yes	Yes	No	No
Recovery of resident files	No	Yes	Yes	Yes	Yes
Deleted and shredded files recovery	No	No	No	Yes	Yes
USB attached history	No	No	Yes	No	No

4 Conclusion

The findings suggest that commercial tools excel in user-friendliness, comprehensive support, and integration of advanced features. On the other hand, open-source tools have demonstrated commendable versatility, transparency, and adaptability, enabling forensic practitioners to tailor their approaches based on specific requirements. It is evident from the comparison chart that Autopsy and FTK are the two forensic tools that can be used to investigate crime involving the use of Scientific Linux. Commercial forensic tools such as EnCase and FTK are more inclined towards the use of investigating crimes involving Windows-based devices and prove less compatible with the Linux Operating System variant such as Scientific Linux. Therefore, with restraint, it is also concluded that the investigations involving the use of Linux-based operating systems can rely more on open-source tools such as Autopsy and the like. However, modular tools such as bulk_extractor and Scalpel can be involved in carrying out specific functionality such as recovering the deleted files.

This comparative analysis of Scientific Linux image forensics using both commercial and open-source tools has provided valuable insights into the strengths, weaknesses, and practical applications of these tools in the context of digital investigations. Importantly, this study has highlighted the need for a nuanced and context-specific selection of tools based on the nature of the investigation, available resources, and the specific requirements of operating system environments. The ideal approach may involve a judicious combination of commercial and opensource tools, capitalizing on their respective strengths to overcome the limitations of each. The insights gleaned from this study findings contribute to the broader discourse on optimizing digital forensic practices, emphasizing the importance of adaptability, collaboration, and a well-informed tool selection process for effective investigations.

References

[1] M. Hina, M. Ali, A. R. Javed, F. Ghabban, L. A. Khan, and Z. Jalil, "Sefaced: Semantic-based forensic analysis and classification of e-mail data using deep learning," *IEEE Access*, vol. 9, pp. 98398–98411, 2021.

[2] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, “Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291–4300, Jul. 2021, doi: 10.1109/TITS.2020.3025875.

[3] R. Kumar and R. Goyal, “On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,” *Comput Sci Rev*, vol. 33, pp. 1–48, Aug. 2019, doi: 10.1016/j.cosrev.2019.05.002.

[4] T. Wang, Q. Yang, X. Shen, T. R. Gadekallu, W. Wang, and K. Dev, “A Privacy-Enhanced Retrieval Technology for the Cloud-Assisted Internet of Things,” *IEEE Trans Industr Inform*, vol. 18, no. 7, pp. 4981–4989, Jul. 2022, doi: 10.1109/TII.2021.3103547.

[5] R. Montasari, *The Comprehensive Digital Forensic Investigation Process Model (CD-FIPM) for Digital Forensic Practice*. University of Derby, 2016. [Online]. Available: https://books.google.bt/books?id=CAQAvwEACAAJ

[6] W. A. Bhat, A. AlZahrani, and M. A. Wani, “Can computer forensic tools be trusted in digital investigations?,” *Science & Justice*, vol. 61, no. 2, pp. 198–203, 2021.

[7] S. Grigaliunas, J. Toldinas, A. Venckauskas, N. Morkevicius, and R. Damaševičius, “Digital evidence object model for situation awareness and decision making in digital forensics investigation,” *IEEE Intell Syst*, vol. 36, no. 5, pp. 39–48, 2020.

[8] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, “Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations,” arXiv preprint arXiv:2103.17028, 2021.

[9] I. Savić and X. Lin, “The analysis and implication of data deduplication in digital forensics,” in *Cyberspace Safety and Security: 13th International Symposium, CSS 2021, Virtual Event, November 9–11, 2021, Proceedings 13*, 2022, pp. 198–215.

[10] P. M. Wanigasinghe, “Extending File Permission Granularity for Linux,” 2021.

[11] S. Maneas, K. Mahdaviani, T. Emami, and B. Schroeder, “Operational Characteristics of SSDs in Enterprise Storage Systems: A {Large-Scale} Field Study,” in *20th USENIX Conference on File and Storage Technologies (FAST 22)*, 2022, pp. 165–180.

[12] N. Mandela, A. A. S. Mahmoud, and A. Agrawal, “Implications of Forensic Investigation in Dark Web,” in *International Conference on Communication, Networks and Computing*, 2022, pp. 103–115.

[13] A. Andjelković, K. Hausknecht, and G. Sirovatka, “Linux Forensic Triage: Overview of Process and Tools,” in *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, 2020, pp. 1230–1235.

[14] G. Amarchand, Keanu, Munn, and S. Renicker, “A Study on Linux Forensics,” 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:201647446

[15] G. Shobana and others, “The State of the art tools and techniques for remote digital forensic investigations,” in *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, 2021, pp. 464–468.

[16] S. Krishnan and N. Shashidhar, “Interplay of digital forensics in ediscovery,” *International Journal of Computer Science and Security (IJCSS)*, vol. 15, no. 2, p. 19, 2021.

[17] N. Mandela, A. A. S. Mahmoud, and A. K. Agrawal, “A Forensic Analysis of the Tor Network in Tails Operating system,” in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 546–551.