

Digital Forensics Report Format



Prepared By: Ms.Memoona Sadaf

Instructor: Ms.Memoona Sadaf

Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi

Air University Islamabad

Digital Forensics Report Template:

Digital Forensics Report

Case Number:001

Date of Investigation: 27/02/25

Investigation Team: Rootxran

Lead Investigator: Rao Ali Nawaz

Forensic Analyst:Rao Ali Nawaz

Supporting Analyst: Analyst's Name (if any)

1. Executive Summary

Attacker is suspected to send encrypted zip containing the patent data related to research on epithelial cells of prostate in context of cancer

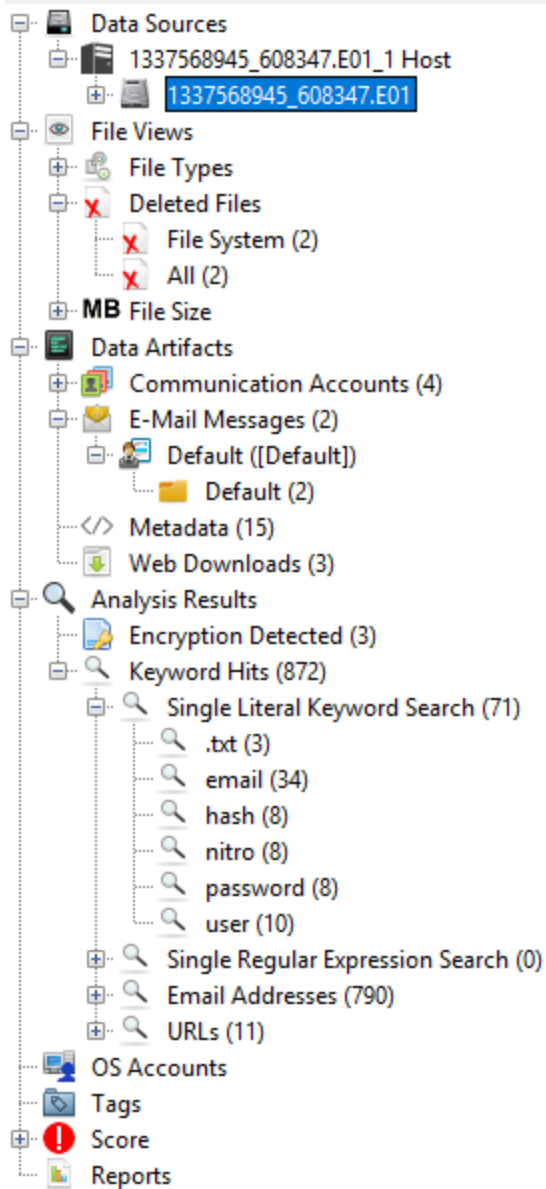
2. Case Overview

This case is related to the organization where the attacker has accessed the private patent research data

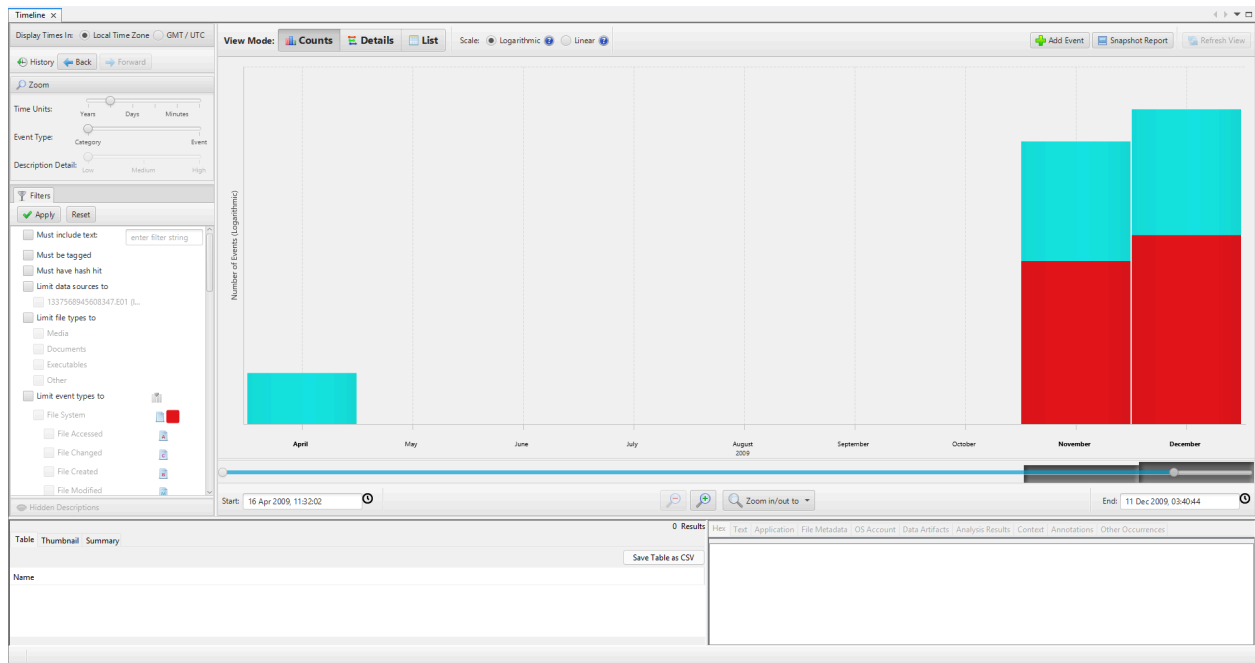
3. Findings

3.2 Relevant Files and Artifacts

Artifact Name: 1337568945_608347.E01



3.2 Timeline Analysis



3.3 Suspicious Activities




Name	Keyword Preview	Location
Charlie_2009-12-04_1306_Sent.txt	And don't forget to «delete» these emails.C	/img_1337568945_608347.E01/vol_vol2/Em
Charlie_2009-12-02_1304_Sent.txt	account. Make sure you «delete» this email.C	/img_1337568945_608347.E01/vol_vol2/Em
Charlie_2009-12-02_1305_Received.txt	account. Make sure you «delete» this email.C	/img_1337568945_608347.E01/vol_vol2/Em
\$LogFile	account. Make sure you «delete» this email.@h@{8'8p	/img_1337568945_608347.E01/vol_vol2/\$Lc
Charlie_2009-12-02_1305_Received_Interested-.eml	account. Make sure you «delete» this email.C</div>	/img_1337568945_608347.E01/vol_vol2/Em
SMFT	account. Make sure you «delete» this email.FILE0CHB...	/img_1337568945_608347.E01/vol_vol2/\$M

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings Extracted Text Translation									
Page: 1 of 1 Page Matches on page: 1 of 1 Match 100% Reset									
charlie_2009-12-04_1306_sent.txt J,									
Got the deposit. The password to get the info is nitro. Use the steg program we talked about. And don't forget to delete these emails.									
C									
-----METADATA-----									
Content-Type: message/rfc822									
X-Parsed-By: org.apache.tika.parser.DefaultParser									
dc:title:									
subject:									







4. Data Analysis

4.1 Data Recovery and Examination

We have extracted files from that case and following are the files


Table	Thumbnail	Summary		
Source Name	S	C	O	Source Ty
 01.zip			1	File
 Charlie_2009-12-04_0941_Sent_01.zip			1	File
 Charlie_2009-12-04_0941_Sent_01.zip			1	File

4.2 Data Preservation

Name	Keyword Preview	Location	Modified Time
 microscope1.jpg	microscope1.jpg JFIF«password»=immortal\$3br%&()*	/img_1337568945_608347.E01/vol_vol2/microscope1.jpg	2009-11-25 03:19:21 PKT
 Charlie_2009-12-07_1144_Sent_microscope1.jpg	microscope1.jpg JFIF«password»=immortal\$3br%&()*	/img_1337568945_608347.E01/vol_vol2/Email/other/C...	2009-12-11 03:29:38 PKT
 Charlie_2009-12-04_0941_Sent.txt	bank acct number. The «password» for the zip file will	/img_1337568945_608347.E01/vol_vol2/Email/Charlie_...	2009-12-04 13:51:26 PKT
 Charlie_2009-12-04_1306_Sent.txt	Got the deposit. The «password» to get the info is nitro	/img_1337568945_608347.E01/vol_vol2/Email/Charlie_...	2009-12-04 13:51:46 PKT
 Charlie_2009-12-04_0941_Sent.txt	bank acct number. The «password» for the zip file will	/img_1337568945_608347.E01/vol_vol2/Email/Charlie_...	2009-12-05 02:51:24 PKT
 \$LogFile	Got the deposit. The «password» to get the info is nitro	/img_1337568945_608347.E01/vol_vol2/\$LogFile	2009-11-20 22:38:09 PKT

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

0°96%Reset



4.3 Data Analysis Techniques

- Finding the metadata
- Steganography

Password is in the metadata

Name	Keyw
microscope1.jpg	micro
Charlie_2009-12-07_1144_Sent_microscope1.jpg	micro
Charlie_2009-12-04_0941_Sent.txt	bank i
Charlie_2009-12-04_1306_Sent.txt	Got th
Charlie_2009-12-04_0941_Sent.txt	bank i
\$LogFile	Got th

Hex

Text

Application

File Metadata

OS Account

Data A

Strings

Extracted Text

Translation

Page: 1 of 1 Page

← →

Matches on page: 1 of 1 Mat

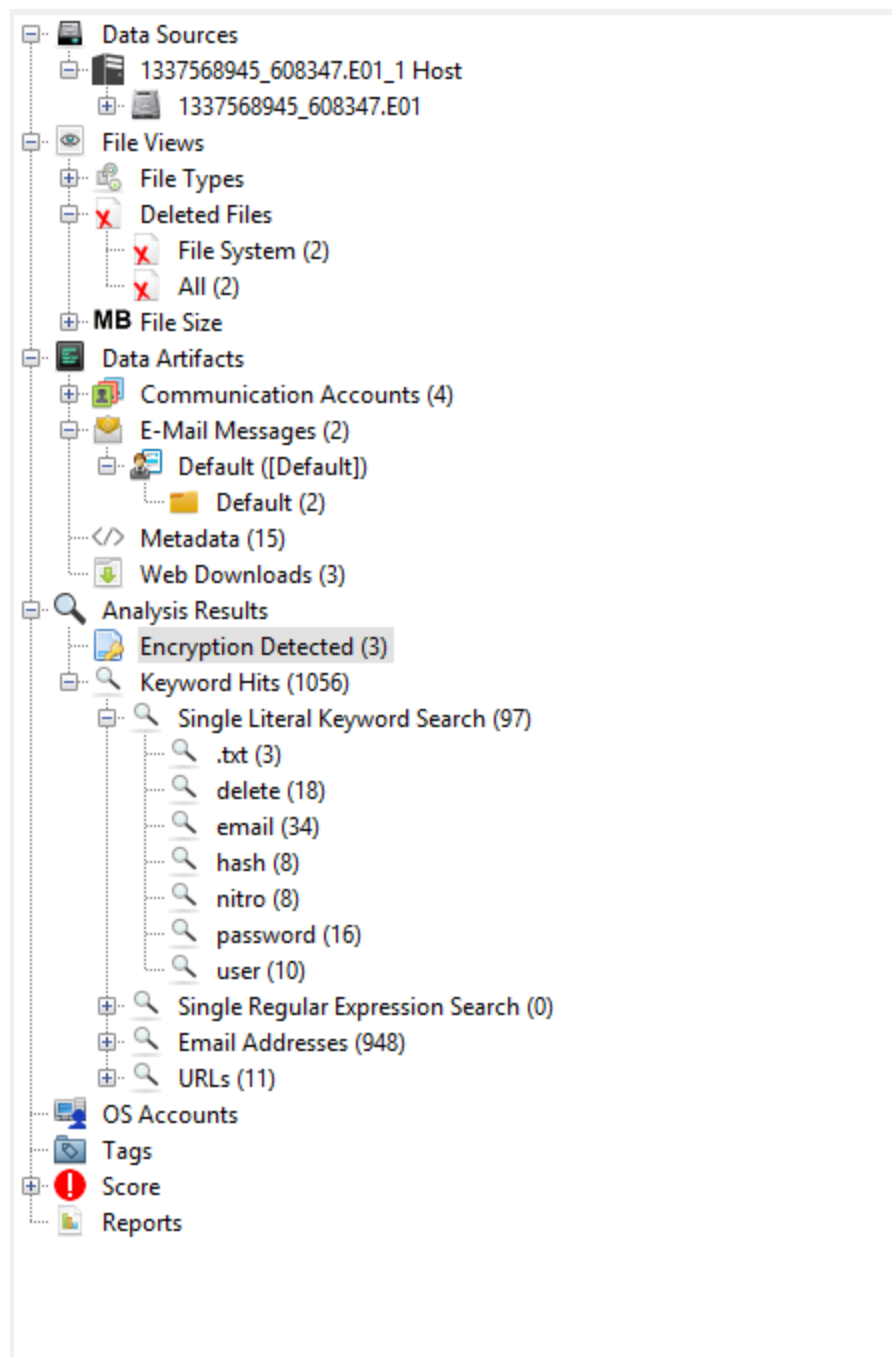
```

password=immortal
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxz
#3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxz
uKo#r
v~LF
2u'BR
sV!]
A#<`
QWZ+
nWw,0

```

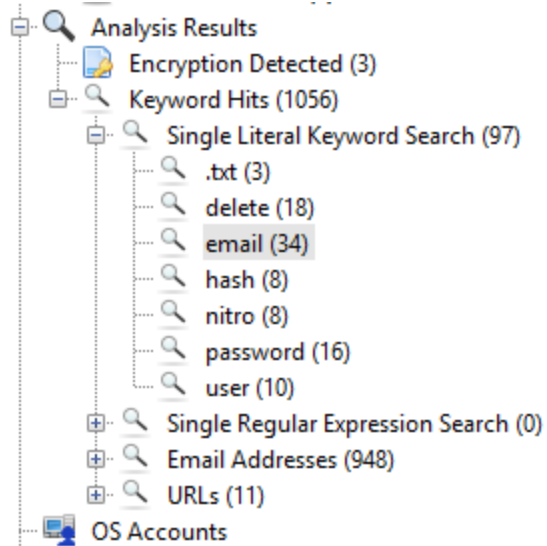
5. Evidence Acquisition

5.1 Devices Examined



5.2 Evidence Collection Methods

- Keyword searching
- Email Searching



5.3 Chain of Custody

- Patent Data
- Encrypted zip files
- Email Deletion

6. Conclusion

6.1 Summary of Findings

Using the passwords from email and picture metadata we have accessed the zip files and the zip file contains patent data pdf

6.2 Assessment of Admissibility

The person who is admissible for all the stuff is Charlie

7. Appendices

7.1 Evidence Inventory



7.2 Forensic Tools Used

- Autopsy

7.3 Detailed Analysis Results

The case contains the email and files transferred to other users

Attacker is suspected to send encrypted zip containing the patent data related to research on epithelial cells of prostate in context of cancer

8. Recommendations

8.1 Legal and Investigative Action

Attacker has accessed the private property of organization so there should be the legal action on him

8.2 Data Security Improvements

There should be secure communication between users in email and try to smtps

Organization should not sent private stuff on those mails

This digital forensics report is confidential and intended solely for the use of the authorized recipient(s). Any unauthorized use, disclosure, or distribution is prohibited.