

ASSIGNMENT COVER LETTER

For use with online submission of assignments

Unit Name: ADVANCED CYBERSECURITY

Unit Code: ISYS6002

Tutor’s Name: RAHUL RAGHAVAN

Assignment No: 2

Assignment Tittle: CASE STUDY

Student name: Kashaboina Tharun Kumar

Student ID: 24137157

ISYS6002: Assessment 2

Name: Kashaboina Tharun Kumar

University: SOUTHERN CROSS UNIVERSITY

**Table of Contents**

[Task 1: 3](#_Toc136625098)

[Summary: 3](#_Toc136625099)

[Cybersecurity Strategy and Objectives: 3](#_Toc136625100)

[Mitigation methods: 3](#_Toc136625101)

[Questions: 4](#_Toc136625102)

[Task 2: 6](#_Toc136625103)

[Task 3: 9](#_Toc136625104)

[References: 15](#_Toc136625105)

# Task 1:

## Summary:

The main purpose of this task is to perform cyber audit conducted for QBE Insurance Group Ltd. The aim of the audit is helping the company’s present cyber security posture and identification of areas those need attention.

## Cybersecurity Strategy and Objectives:

Client Response: "We believe that reducing cyber risk should be the main deliverable of the company's cybersecurity strategy and outcome of the risk assessment decided by senior management."

## Mitigation methods:

The strategies are given as follows:

1. Implementing robust access controls and authentication mechanisms to prevent unauthorized access.
2. Regularly updating and patching software and systems to address known vulnerabilities.
3. Conducting regular security awareness training for employees to educate them about potential risks and best practices.
4. Deploying firewalls and intrusion detection/prevention systems to monitor and protect the network from malicious activities.
5. Encrypting sensitive data both in transit and at rest to protect against unauthorized access.
6. Establishing incident response plans and conducting regular drills to ensure a swift and effective response to security incidents.
7. Performing regular vulnerability assessments and penetration testing to identify and remediate vulnerabilities proactively.
8. Implementing a strong backup and recovery strategy to ensure business continuity in the event of data loss or system failure.
9. Conducting due diligence on third-party vendors and contractors to ensure they meet cybersecurity standards.
10. Establishing a comprehensive risk management framework to identify, assess, and mitigate risks across the organization.

## Questions:

Questions are:

1. How does your company handle user access management and authentication controls to ensure secure access to systems and data?
2. What measures are in place to protect sensitive customer and employee data, such as personally identifiable information (PII) and financial information?
3. Does your company conduct regular security awareness training for employees to educate them about common cyber threats and best practices?
4. How are third-party vendors and contractors vetted and managed to ensure they meet cybersecurity standards and do not pose a risk to the organization?
5. Are there documented incident response plans and procedures in place to effectively respond to and recover from cybersecurity incidents?
6. Does your company have a business continuity and disaster recovery plan that addresses cybersecurity incidents and ensures minimal disruption to operations?
7. How is physical access to critical IT infrastructure, such as data centers and server rooms, controlled and monitored?
8. Are there regular vulnerability assessments and penetration tests conducted to identify and address potential weaknesses in the company's IT systems and applications?
9. Does your company have a process for monitoring and detecting security incidents and intrusions, such as the use of intrusion detection systems (IDS) or security information and event management (SIEM) solutions?
10. How are software and hardware assets managed to ensure timely patching and updates to address known vulnerabilities?
11. Is data encryption used to protect sensitive information in transit and at rest, such as customer data and intellectual property?
12. What measures are in place to prevent and detect unauthorized access or use of privileged accounts, such as system administrator or root accounts?
13. Are there controls in place to monitor and audit user activities and detect any suspicious or anomalous behaviour?
14. Does your company have a process for regular data backup, and are backups tested to ensure the recoverability of critical data in case of a data loss event?
15. How is the security of mobile devices, such as smartphones and tablets, managed for employees who access company systems and data remotely?

# Task 2:

Basically, the GoldRekt is a nation-state threat group which has been active since so many years ago. It is believed to conduct cybercrime for the financial advantage of the country. Also, there are some indicators of the association with other notorious threat groups like ATP28, Sandworm Team, FIN4 and ATP29. With the monetization of the compromised targets and a focus on the cyber espionage, the GoldRekt has developed its strategic objectives over the time.

The primary object of the GoldRekt is the cyber espionage that involves the interception of the details for strategic decision-making purchase. Thus, the group employs multiple techniques and tactics which are outlined in the MITRE ATT&CK framework to achieve this objective. Also, an initial access is one of the relevant tactic that employed by the GoldRekt. It includes multiple methods like links to compromise the system of the target or spear phishing emails with malicious attachments. Also, the users may utilize crafted emails which is aiming individuals within the financial organizations or institutions that associated with the financial sector.

Tactics and Techniques Identified:

1. Initial Access:
   * Phishing (T1566.001)
   * Remote Access (T1133)
   * Public-Facing Applications (T1190)
2. Execution:
   * Malicious Point of Sale (POS) Malware (e.g., BlackPOS) (T1101.002)
3. Collection:
   * Traffic Analysis, Decryption, and Forensics (T1410)

Additional Tactics and Techniques Proposed:

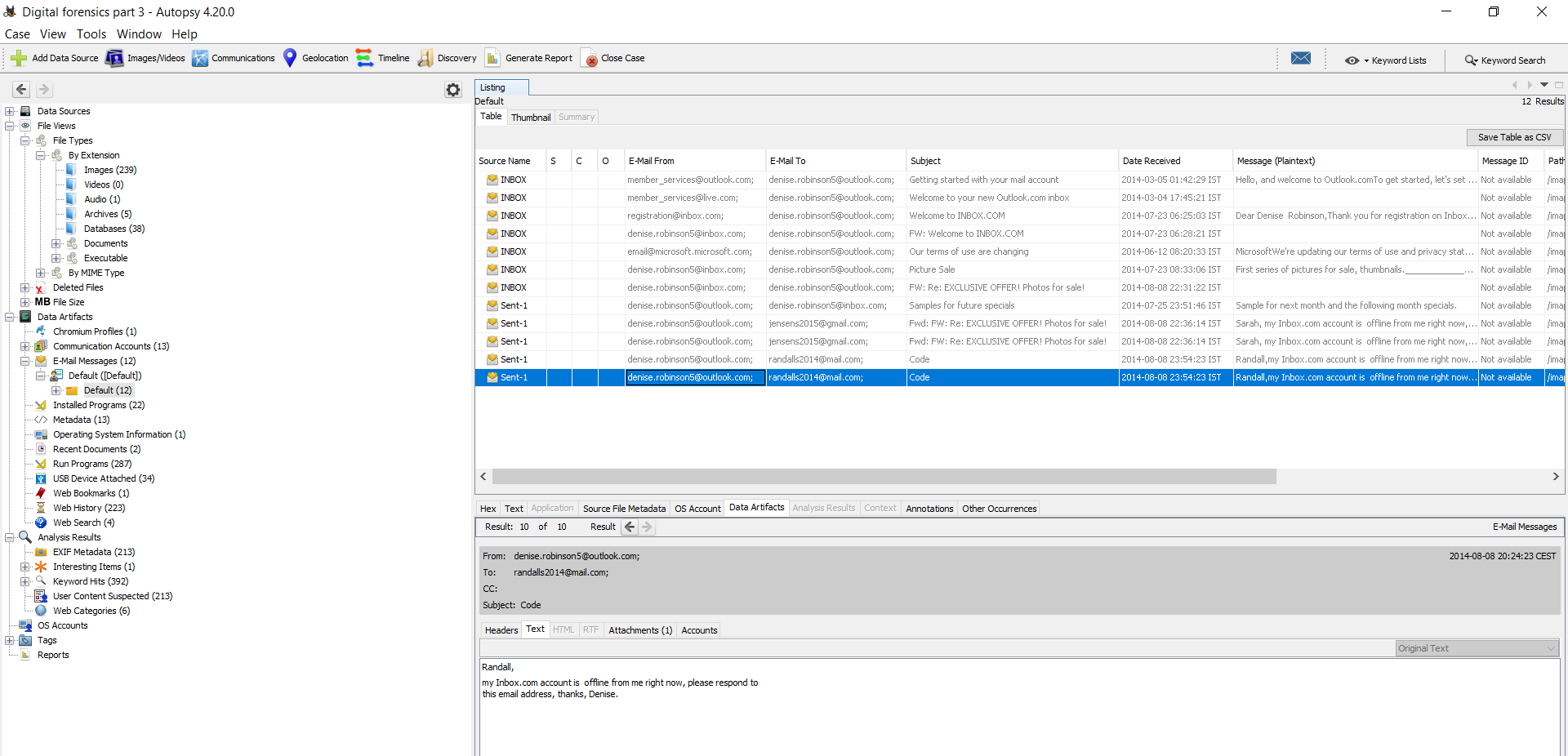
1. Defense Evasion:
   * File Deletion (T1107)
   * Virtualization/Sandbox Evasion (T1497)
2. Persistence:
   * Scheduled Task (T1053)
   * Rootkit (T1014)
3. Command and Control:
   * Domain Generation Algorithms (T1568.002)
   * Remote File Copy (T1105)
4. Discovery:
   * System Information Discovery (T1082)
   * Network Share Discovery (T1135)
5. Lateral Movement:
   * Remote Desktop Protocol (RDP) Hijacking (T1076)
   * Pass the Ticket (T1097)
6. Impact:
   * Data Encrypted for Impact (T1486)
   * Account Manipulation (T1098)

Execution, is another tactic that employed by the GoldRekt that involves the methods that utilized to run malicious code on the target’s system. Usually, the group may exploit the vulnerabilities in the software applications and utilize several techniques like PowerShell-based attacks to enhance the execution privileges on the compromised systems. Whatever, the GoldRekt aims on the Lateral Movement within the target network to achieve the objectives. It employs the methods like exploitation of the trust relationships, credential theft and the use of the legitimate remote administration tools improve the access to important information. The aforementioned additions to the ATT&CK Navigator exercise give a more thorough picture of the probable approaches utilised by the threat group by taking into account the tactics and techniques used by GoldRekt based on the information supplied and utilising the MITRE ATT&CK framework.

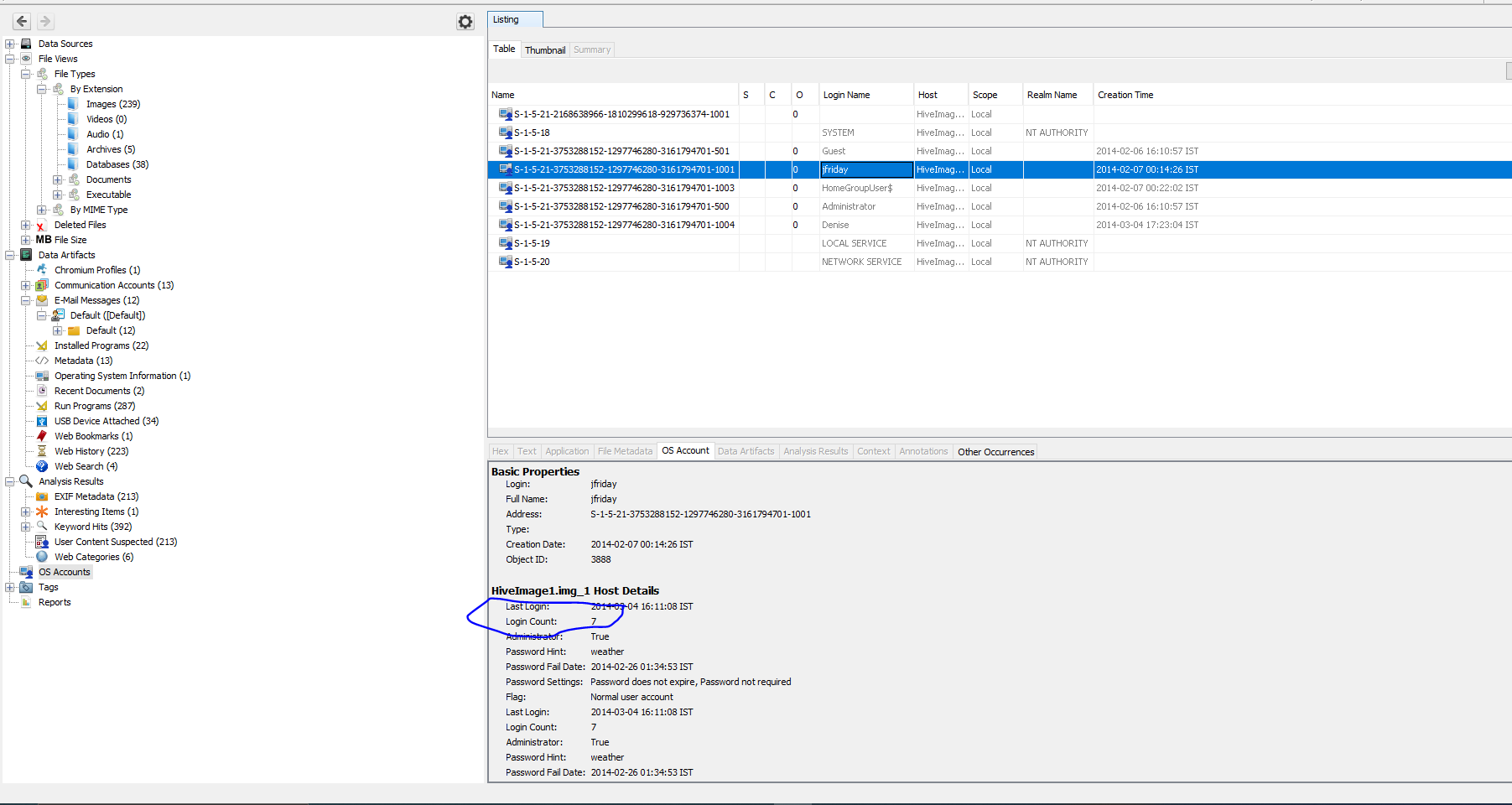
However, the activities of the GoldRekt may involve the impact to the target organization. Thus, it may engage in the destructive actions like data manipulation or storage to disrupt the operations, cover the tasks after the compromising a target and make chaos. The security professionals can also analyze and map the GoldRekt’s techniques and tactics in the systematic manner by leveraging the MITRE ATT&CK navigator.

# Task 3:

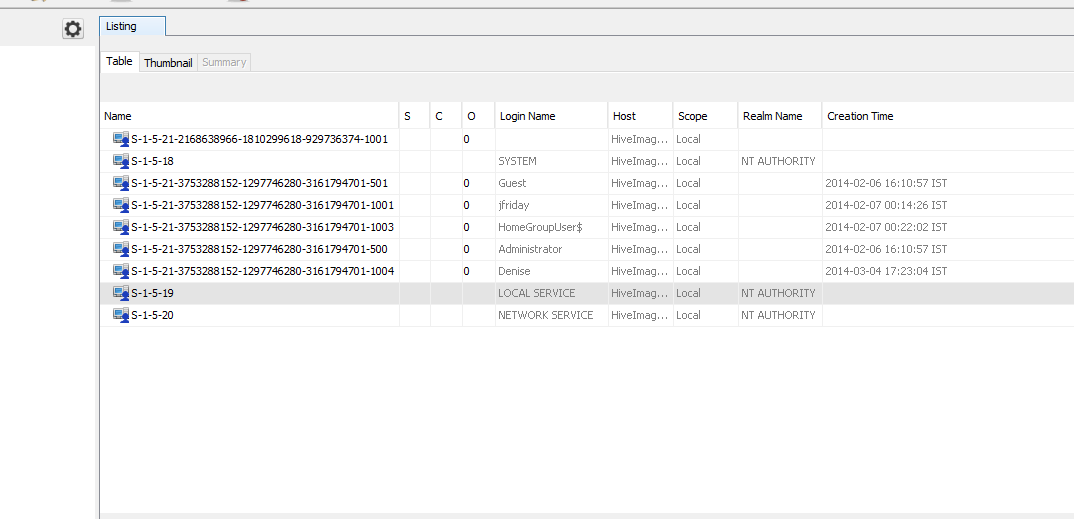
Yes Denise Robinson logged in to the computer. The email address is – denise.robinson5@outlook.com



Jfriday Account has been used 7 times:



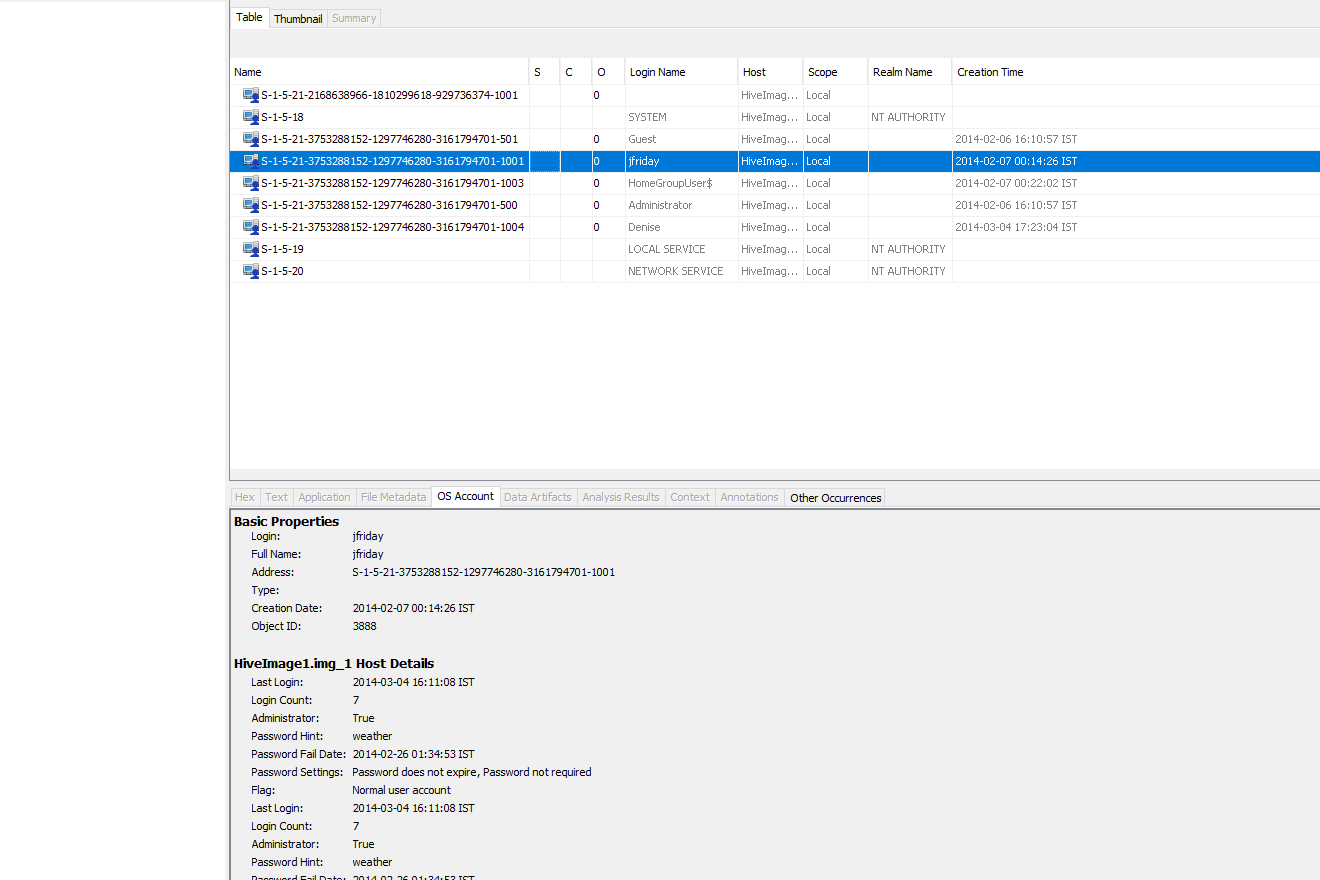
4 user accounts has been disabled:



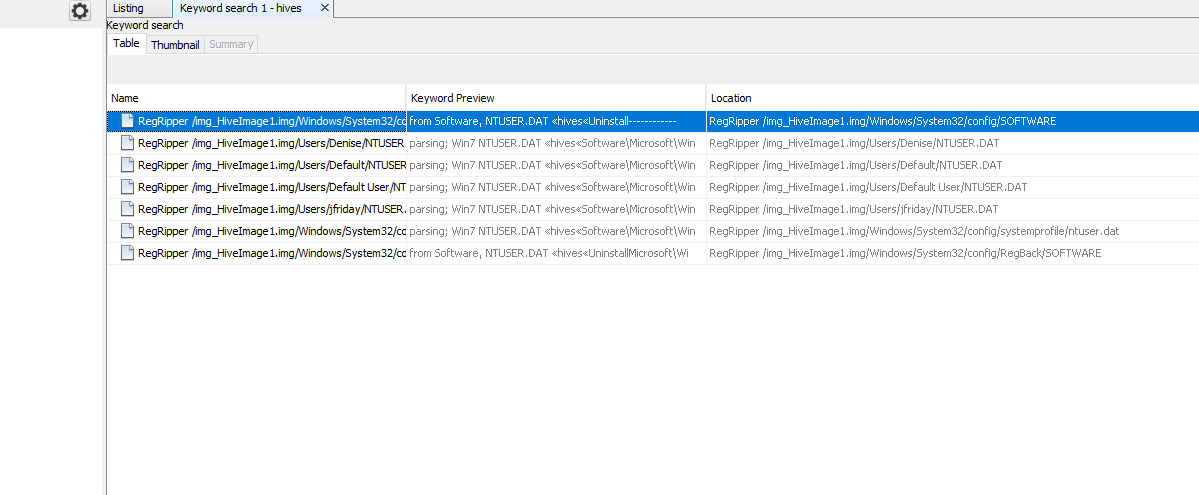
User accounts created automatically are:

|  |
| --- |
| S-1-5-21-3753288152-1297746280-3161794701-1003 |
| S-1-5-21-3753288152-1297746280-3161794701-500 |

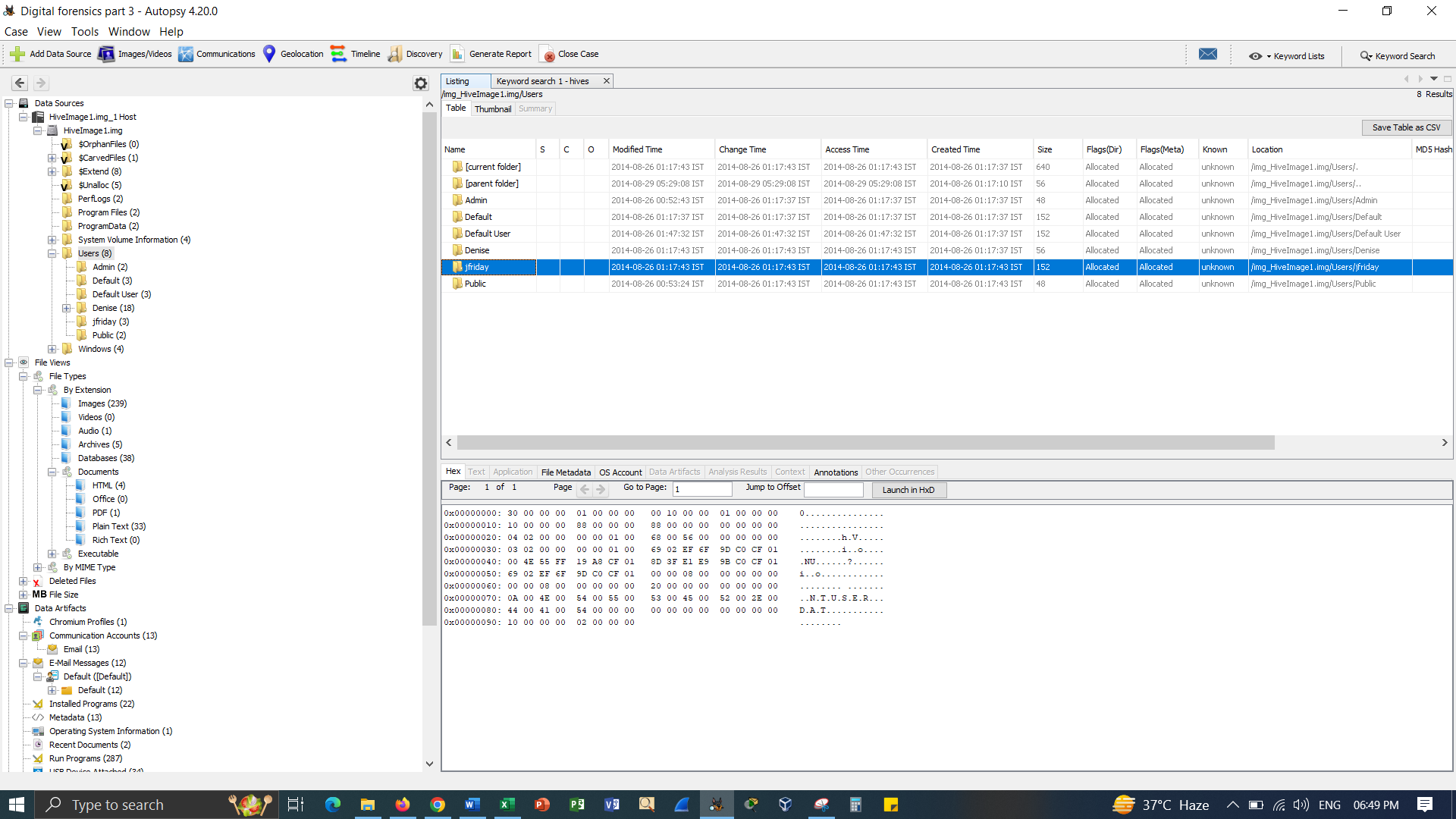
Yes its true.



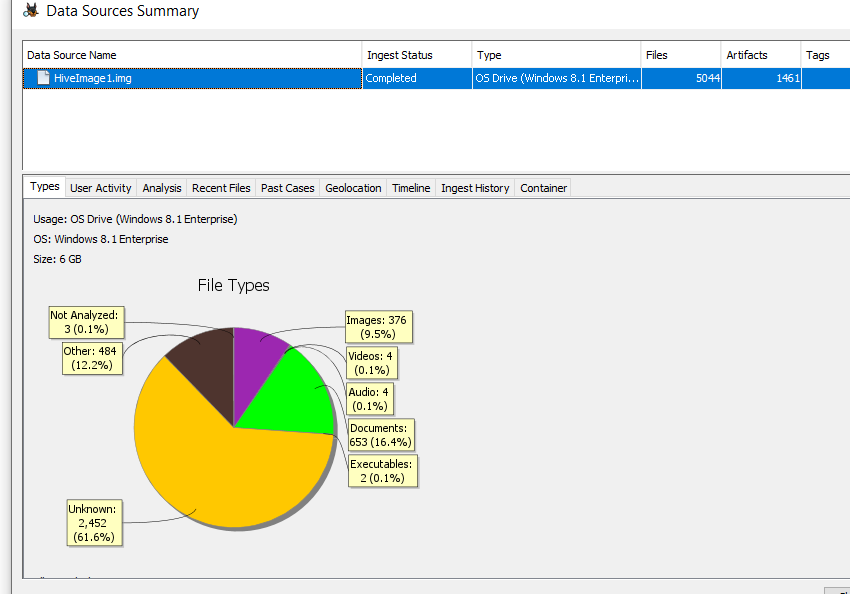
The registry contains 7 hives:



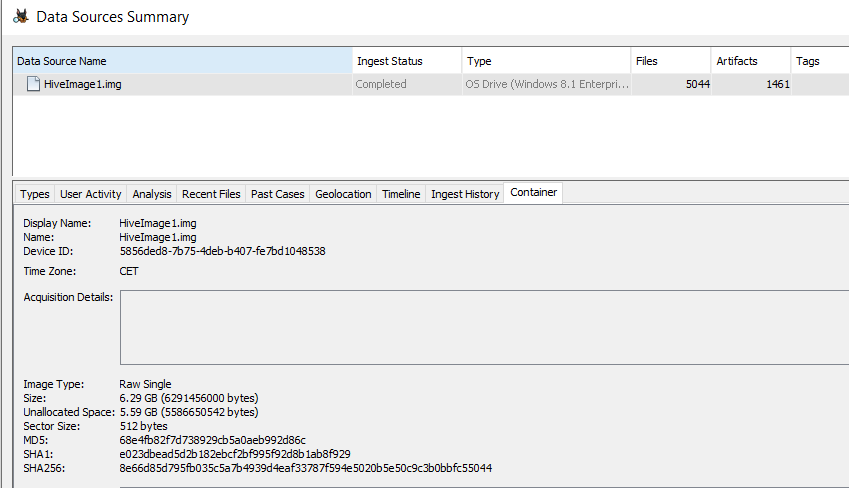
The name of the computer is Denise:



OS is windows 8.1:

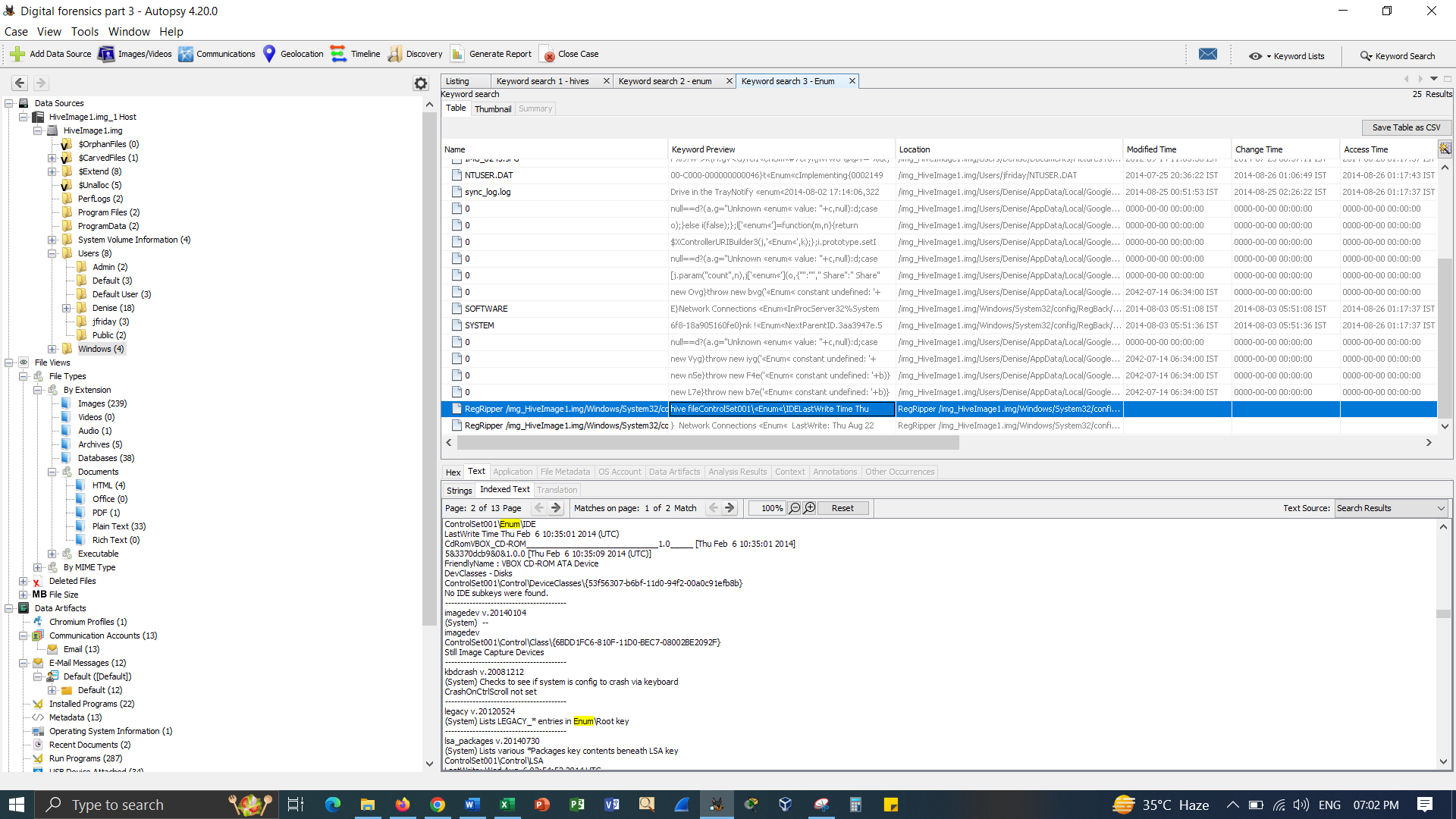


MD5 value:

  
The timezone is CET.

Uninitiated people find it amazing that we can identify which USB devices have ever been connected to a system even when those devices are no longer there. Unfortunately, this proof frequently only holds up to inspection when the alleged USB devices are not present. That is a strange statement. The problem is brought about by erroneous, inconsistent, and inadequately supported nomenclature.

The Enum folder specifies enumerated constants used to retrieve directory paths to system special folders.



Basically, the data theft incidents can have significant consequences for the organizations such as reputational damage, financial losses and regulatory penalties. Having a well-defined DFIRP is vital to effectively answer to the data theft incidents, preserve evidence for future investigation and minimize the impact. Thus, this plan outlines the key considerations and steps for controlling the data theft incidents –

* Develop incident response procedures and politics – make comprehensive and clear guidelines for responding to the data theft incidents such as communication protocols, roles and responsibilities and escalation procedures.
* Establish an incident response team – train and identify a team of the individuals with the expertise in the digital forensics, communication and incident response.
* Establish relationships with external partners – situate contracts with the legal counsel, law enforcement agencies and forensic experts who can help in the event of the data theft incident.
* Implement proactive security measures – implement powerful access controls, intrusion detection systems and monitoring tools to prevent and detect the data theft incident.

**Detection and initial response for the case**

* Activate the incident response team – the incident response team should be quickly activated and notified to start the investigation, once the incident is detected.
* Identify the indicators of a data theft incident – situate mechanisms to look for suspicious and malicious activities like unusual traffic patterns, unauthorized access or abnormal system behaviors.
* Secure the affected systems – isolate the compromised systems from the network to mitigate the future data damage or exfiltration.

**Investigation and evidence collection:**

* Collect and preserve evidence – basically, employ proper forensic procedures to preserve and store the evidence and making sure its admissibility and integrity in the potential legal procedures.
* Conduct a forensic analysis – use digital forensic methods to find the nature and the scope of the data theft incident, such as data accessed or stolen, the affected systems and the attack vectors used.
* Maintain chain of custody – document every action that taken during the investigation and make sure the integrity of the evidence by managing an informational chain of custody log.

# References:

Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Academic Press.

Karie, N.M., Kebande, V.R., Venter, H.S. and Choo, K.K.R., 2019. On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, *1*, p.100008.

Marcella, A. J., & Greenfield, D. (Eds.). (2017). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes (3rd ed.). Auerbach Publications.

Nance, K., Haynes, J. E., & Ortiz, S. (2016). Guide to Cyber Forensics: From Data to Digital Evidence. Springer.

Pollitt, M. (2017). Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace (2nd ed.). Elsevier.

Quick, D., Choo, K.-K. R., & Martini, B. (Eds.). (2016). Handbook of Digital Forensics of Multimedia Data and Devices. Wiley.

Sammons, J. (2016). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

Xiao, J., Li, S. and Xu, Q., 2019. Video-based evidence analysis and extraction in digital forensic investigation. *IEEE Access*, *7*, pp.55432-55442.