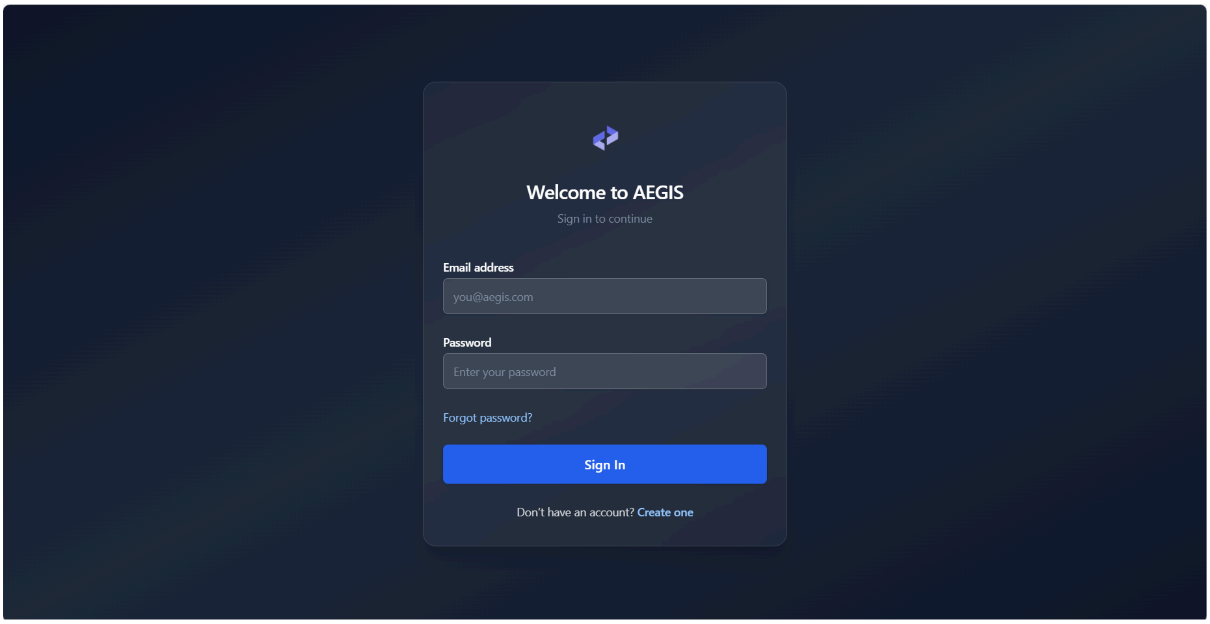
Getting Started

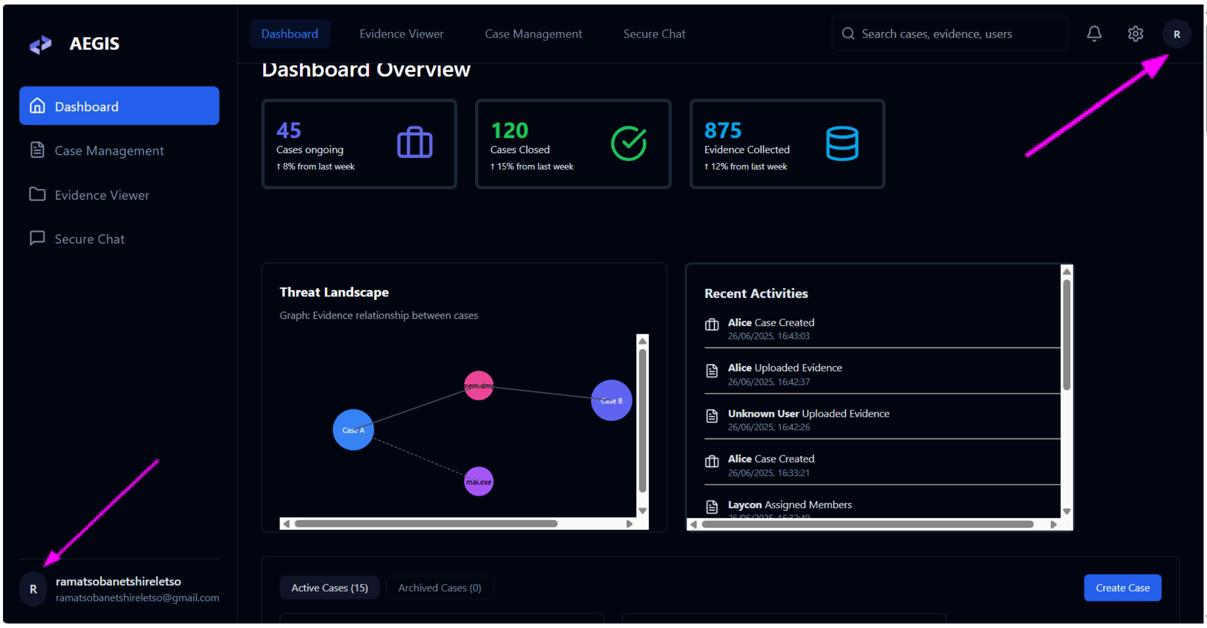
Logging In

- Step-by-step:
  1. Go to the AEGIS landing page.
  2. Click on Get Started.
  3. You will be directed to the login page.
  4. Enter your email and password.
  5. Click "Sign In".

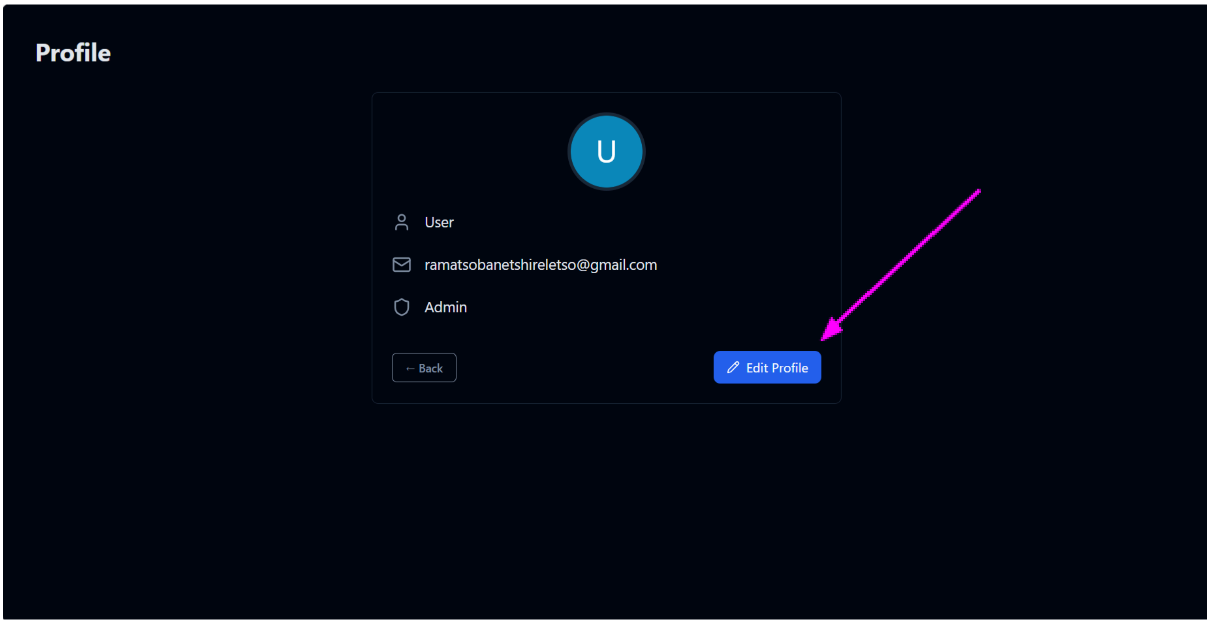


Setting Up Your Profile

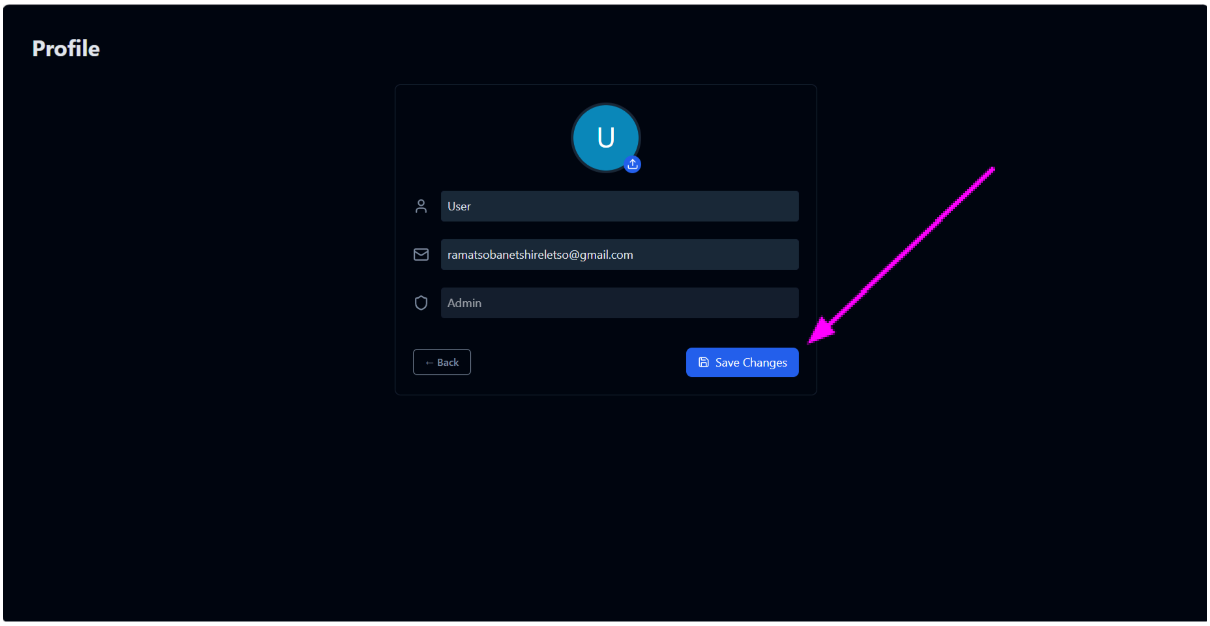
- Step-by-step:
    1. Once logged in, navigate to the bottom left corner or top right corner of the Dashboard page.
    2. Click on the icon.



3. Here you can edit your profile details.
4. Click on the Edit Profile button and change your details as you see fit.



5. After editing your profile, click the Save Changes button to finalise your changes.

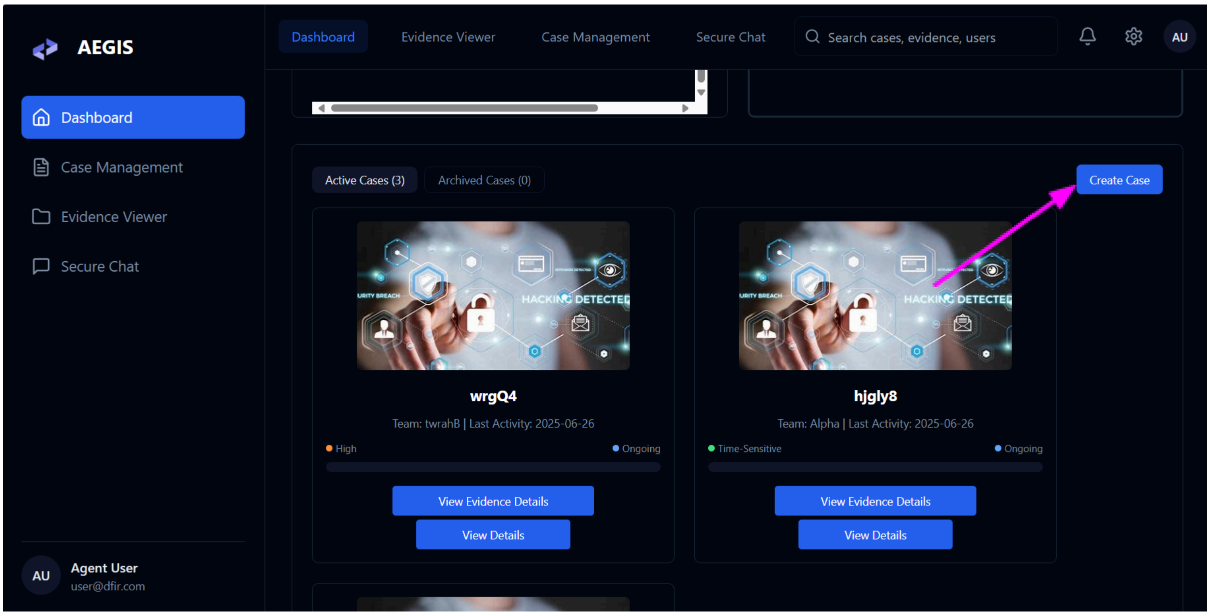


Core Features and Navigation

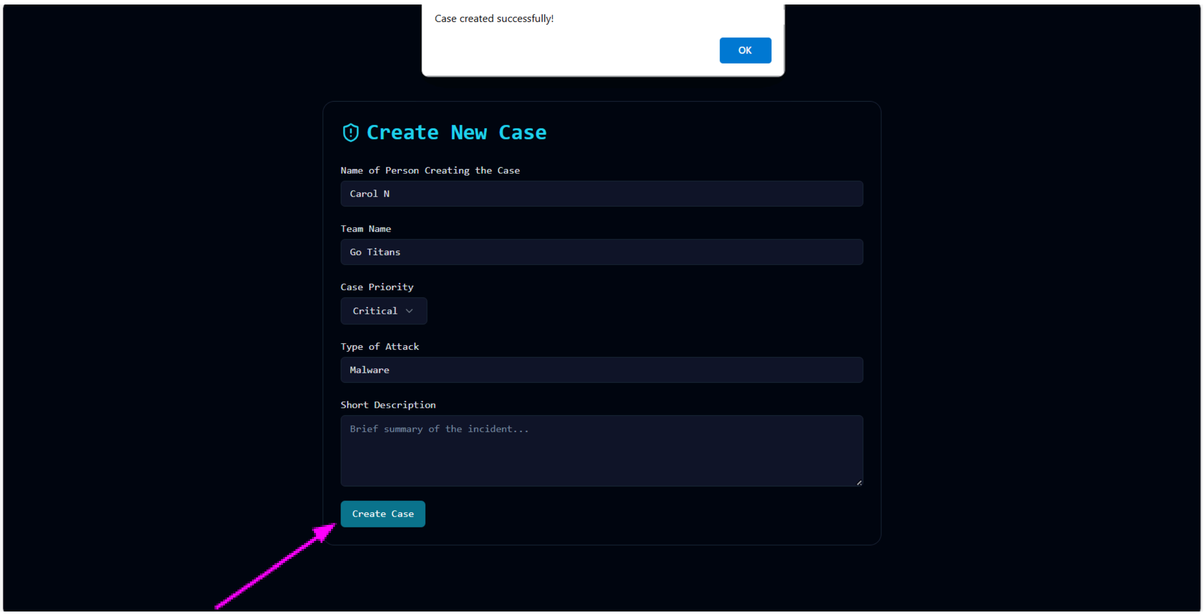
Dashboard Overview

Case Creation

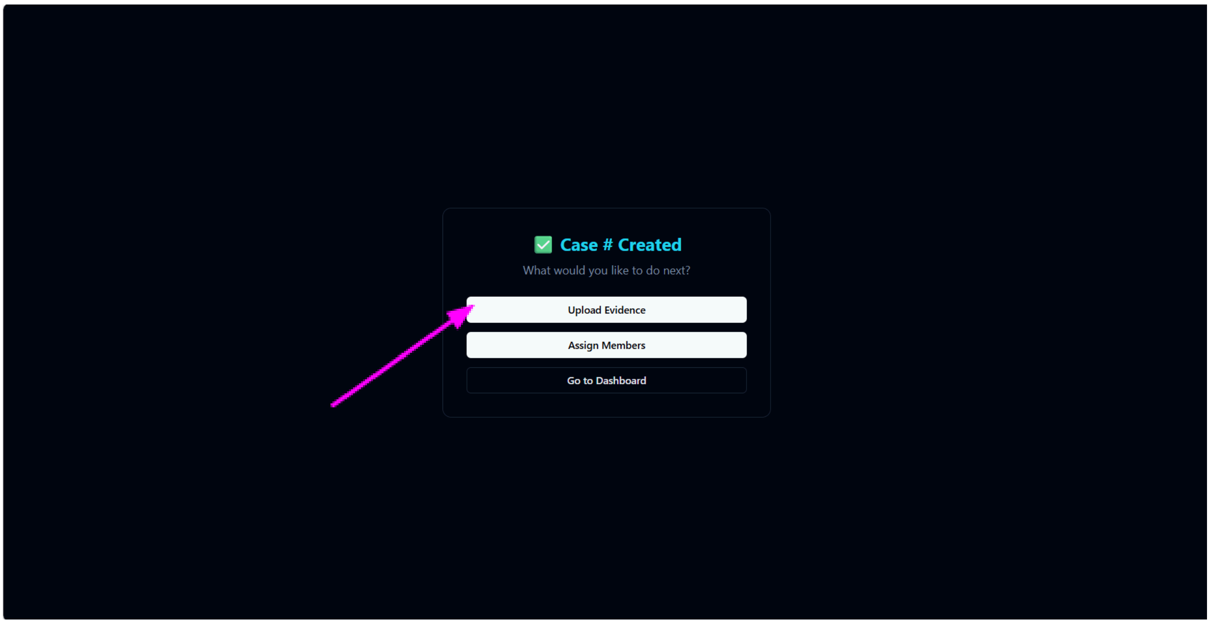
- Step-by-step:
    1. Once logged in you will be shown your dashboard page.
    2. Scroll down to view your currently active or archived cases.
    3. In order to create a case, click on the Create Case button.



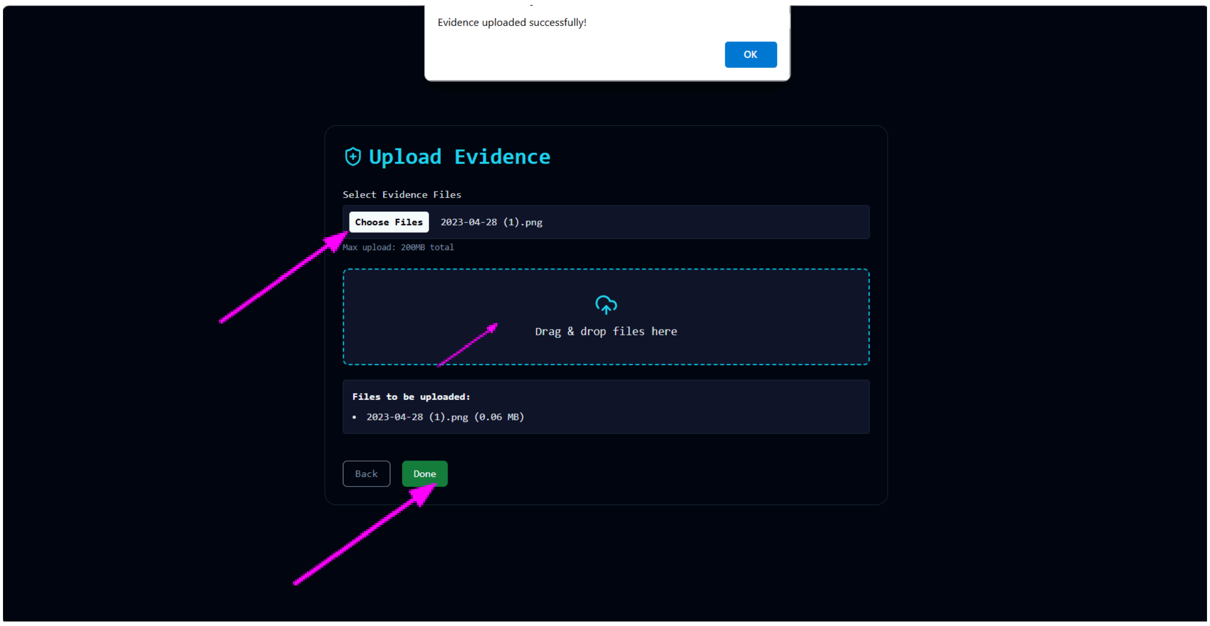
4. You will be shown a form required to create a case.
5. Fill in the form and click Create Case



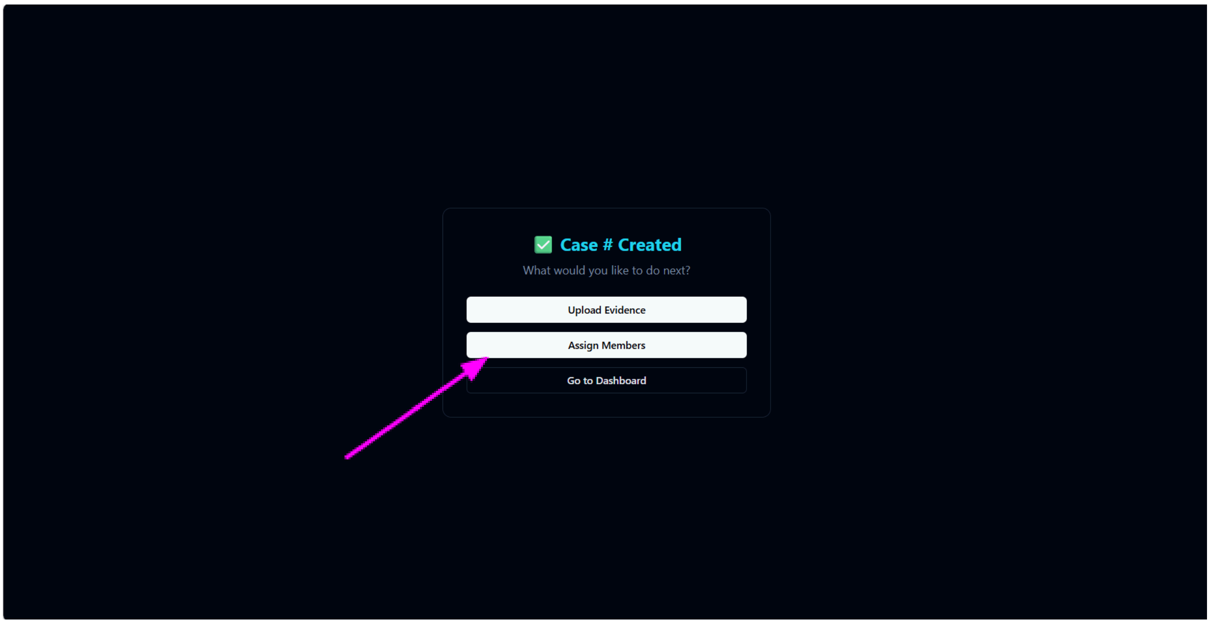
6. You will then be presented with two options, you can choose to Upload Evidence or Assign Members.



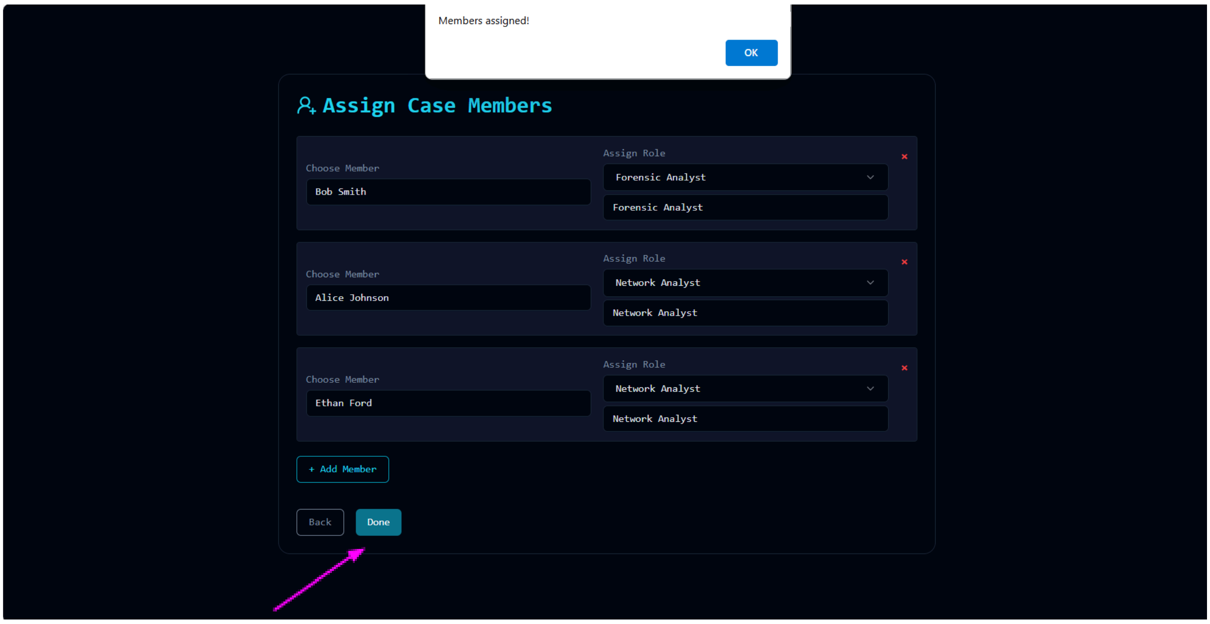
7. Click on the Upload Evidence button
8. Here you can either Choose Files or Drag & Drop as a method of upload.
9. Click on the Done button and you have successfully uploaded evidence to the case you created.
10. You will then be redirected back to the page above.



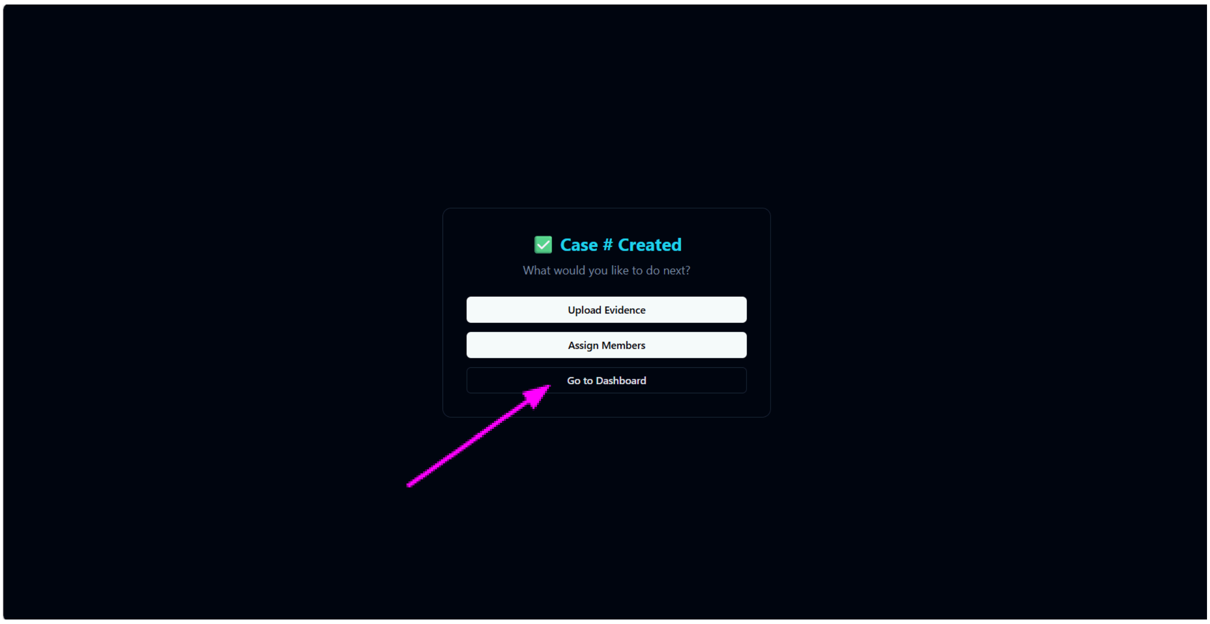
11. Next, click on the Assign Members button.



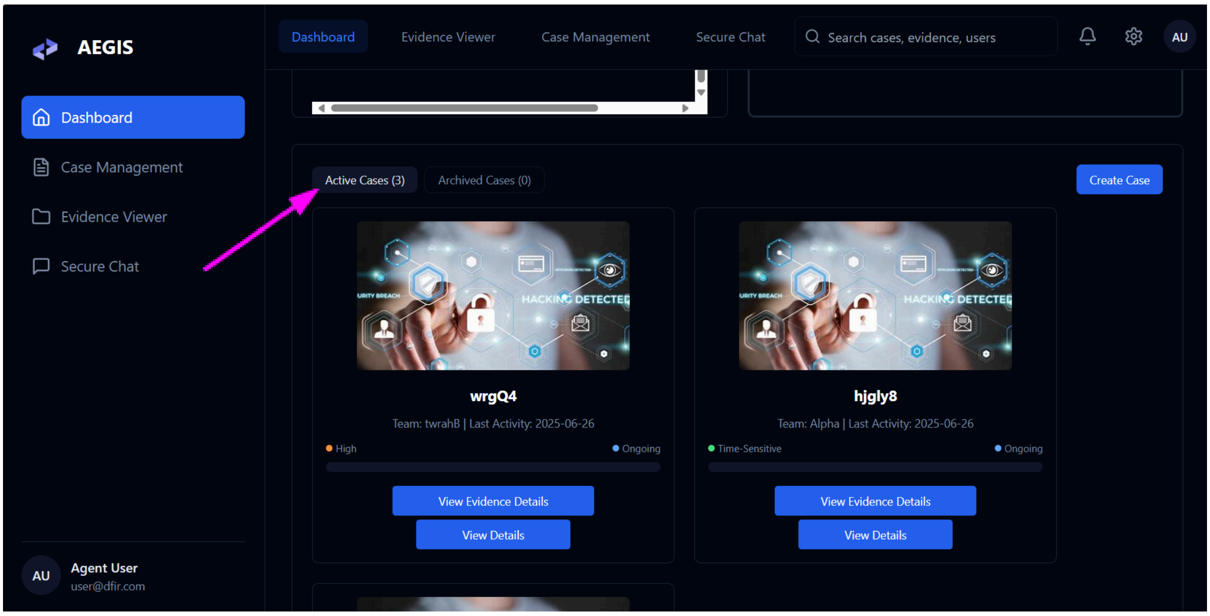
12. Here you have the option to either manually type in a user, or choose a user from the drop-down menu. Similarly, you have the option to choose that user's role from a predefined list of roles or specify a custom role.
13. You can assign up to 10 members per case.
14. Next, click the Done button.



15. You will then be navigated back to this page. Click the Go to Dashboard button.

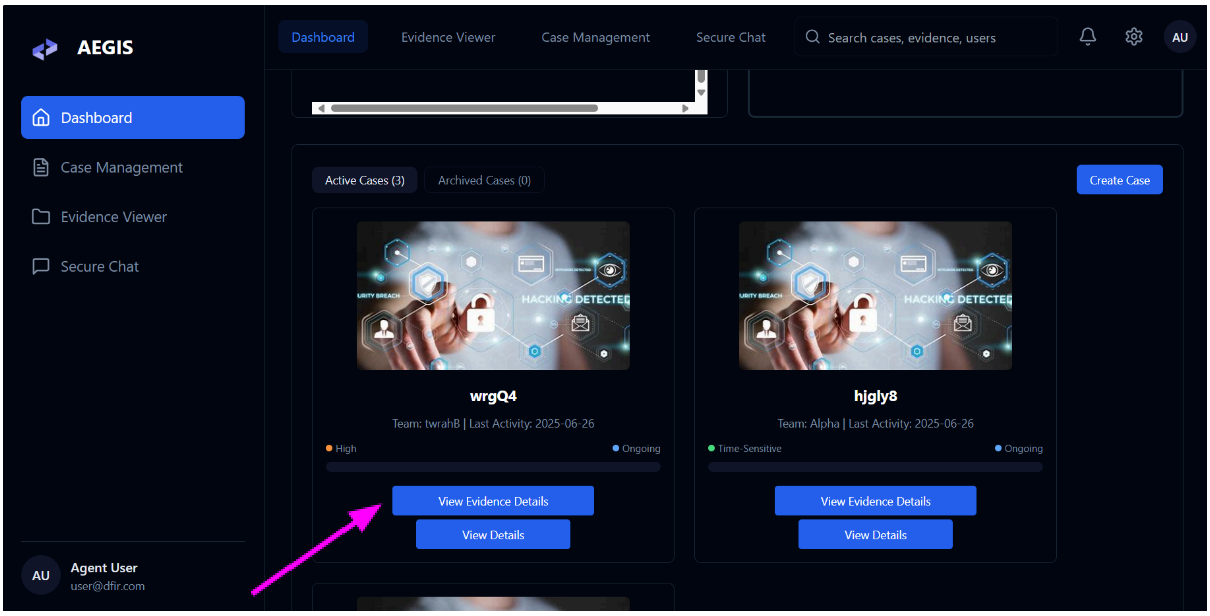


16. You will then be navigated to your dashboard page.
17. Scroll down to view your currently active or archived cases. Here, you should be able to view the case you have recently created.

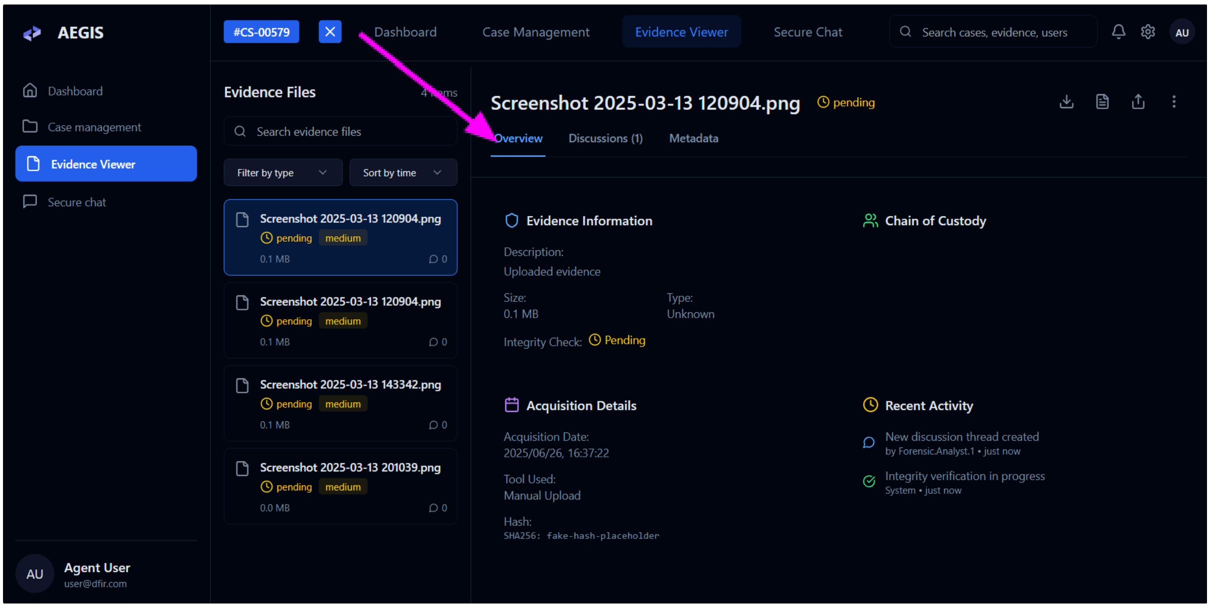


Case Overview

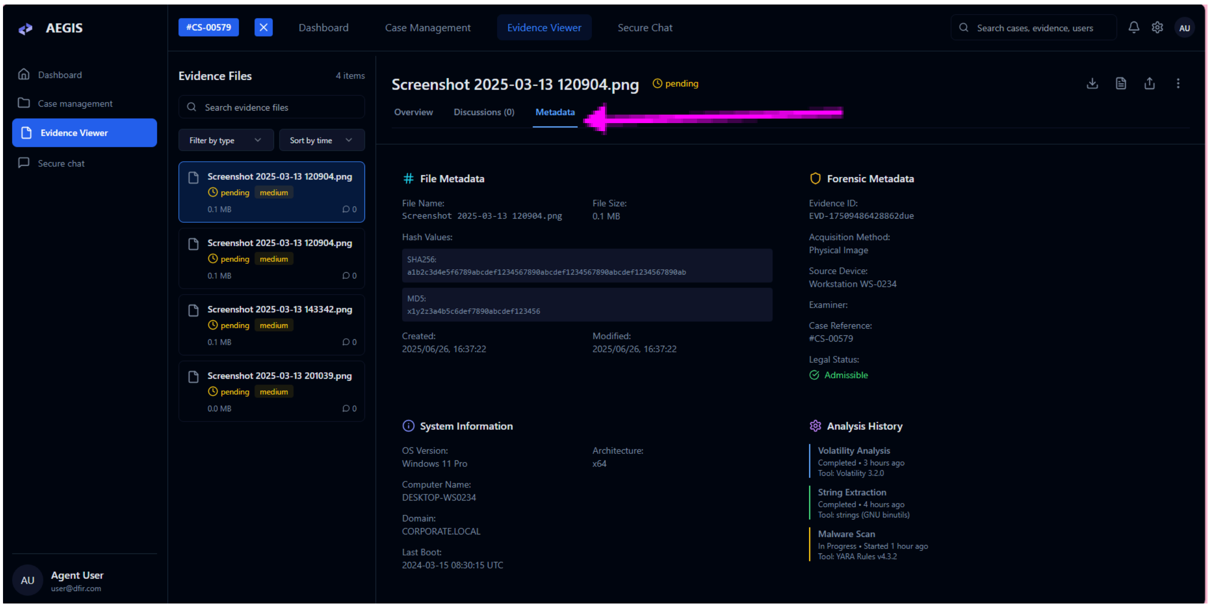
- Step-by-step:
  1. Click on the View Evidence button of any Case Card.



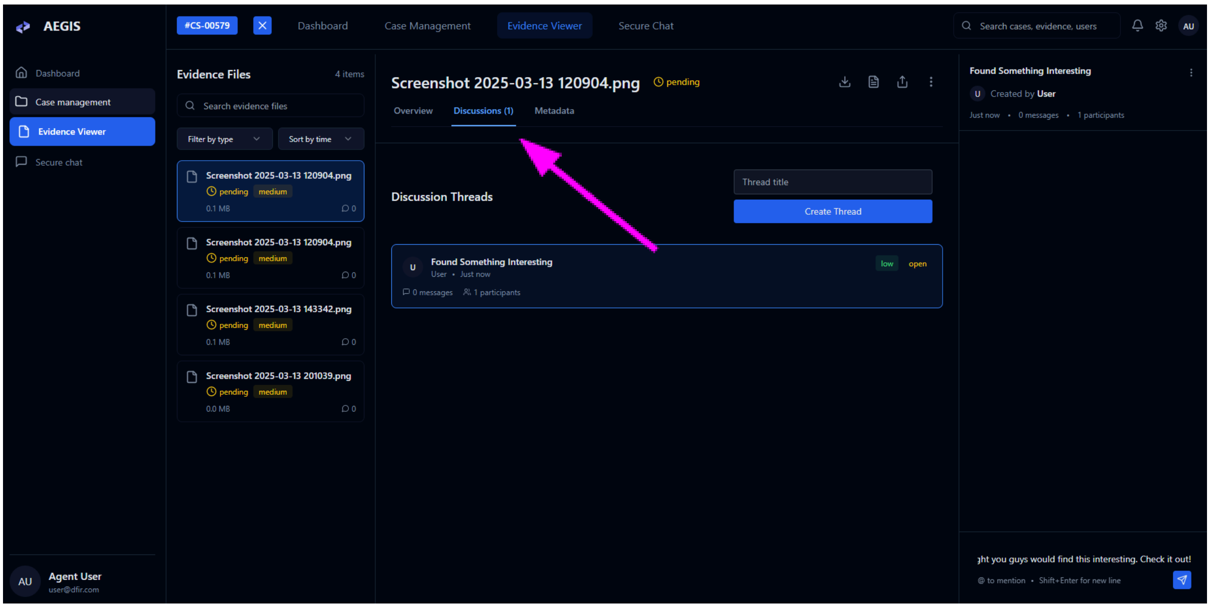
2. You will then be navigated to the Evidence Viewer Page, where you can view the evidence related to the case you have selected above.
3. Here you can click on Overview to view the Acquisition Details of the selected evidence file.



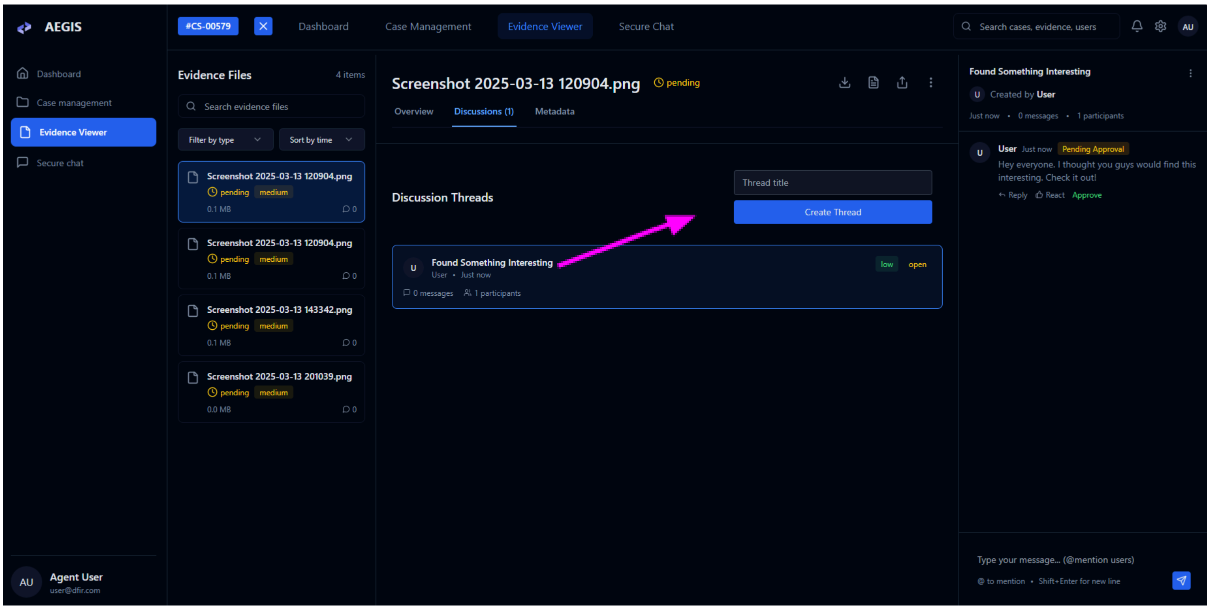
6. You can also click on Metadata to view details about the creation and modification dates and times of the selected evidence file.



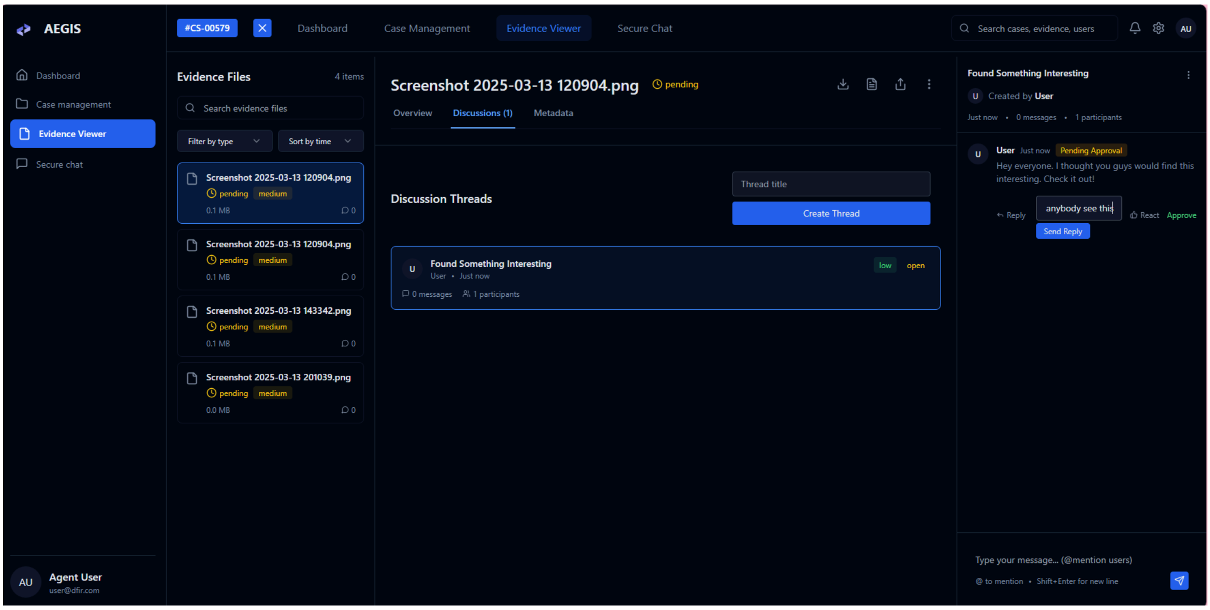
7. You can click on Discussions which also shows the current number of threads associated with the selected evidence file.

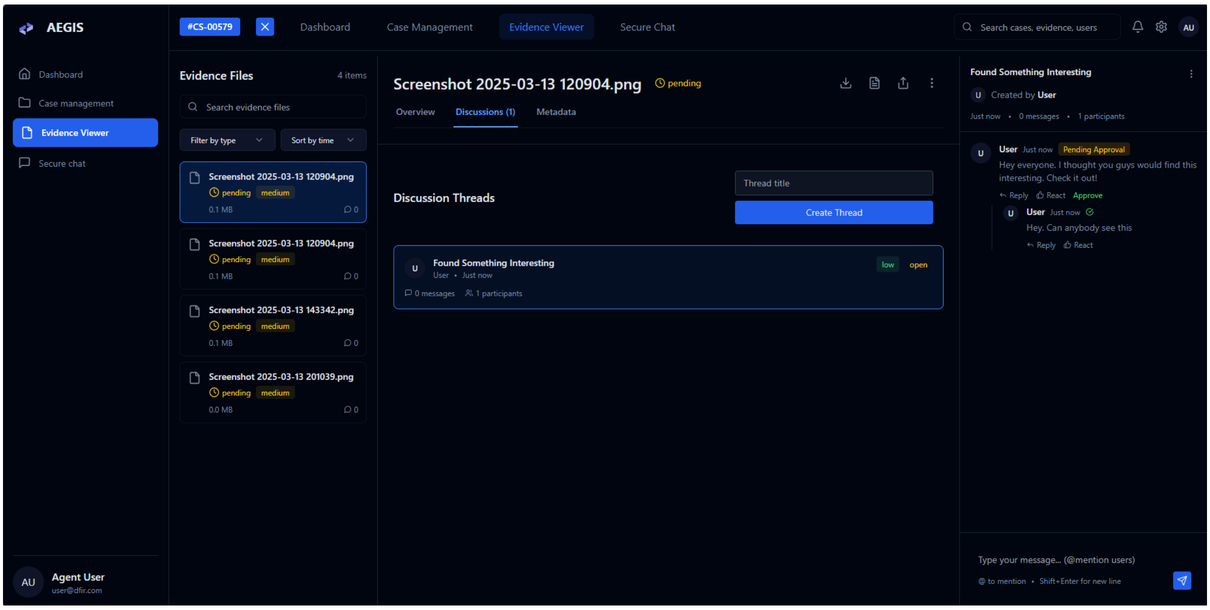


8. You can then click on the Create Thread button to create a case.
9. Utilise the text box above to enter the thread title.
10. On the farther right hand side, the selected thread displays the messages.

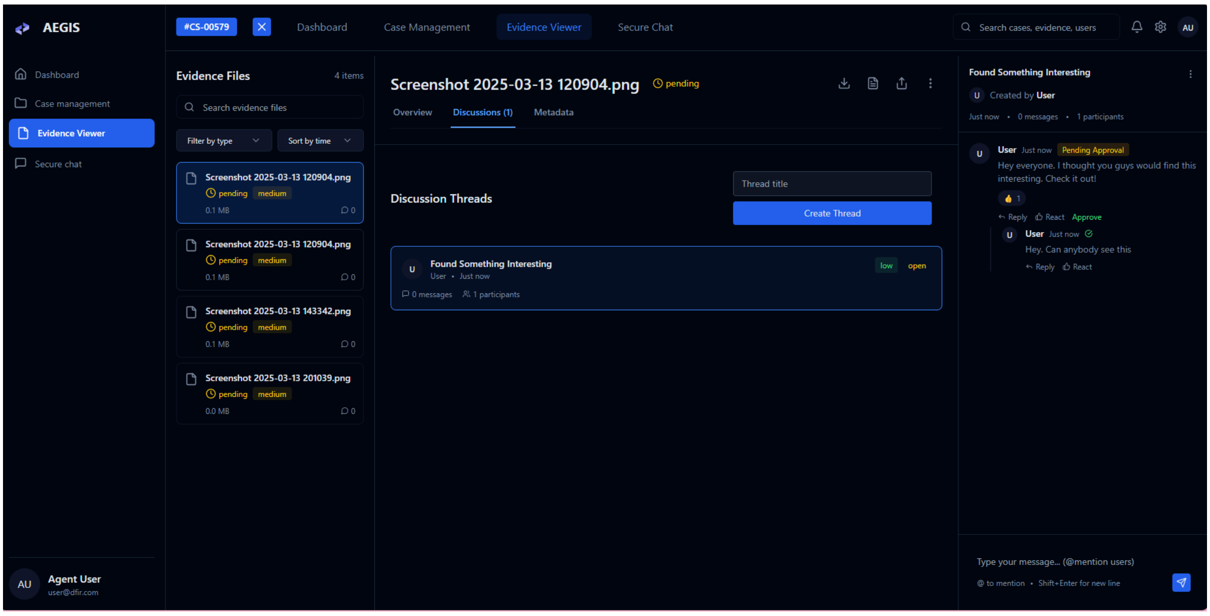


11. On the bottom right corner, you can type in your comment, and click the send icon, your message will appear in the above space.
12. You can then click reply, to reply to the message. Enter the message in the text box that appears.



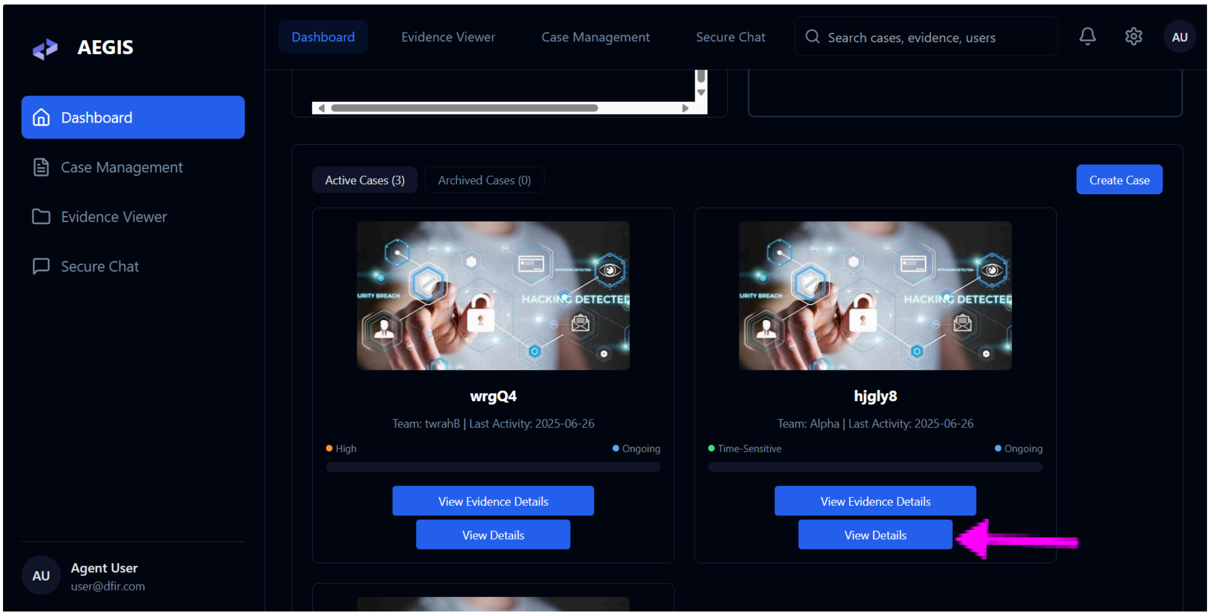


13. You can also react to the message or the reply.

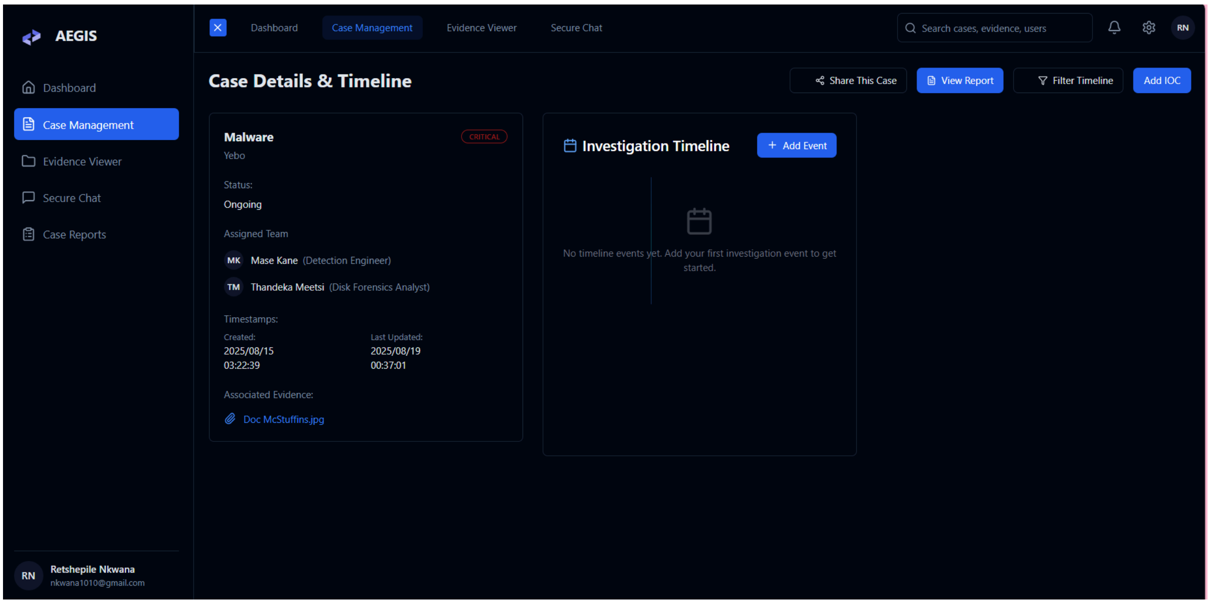


Case management:

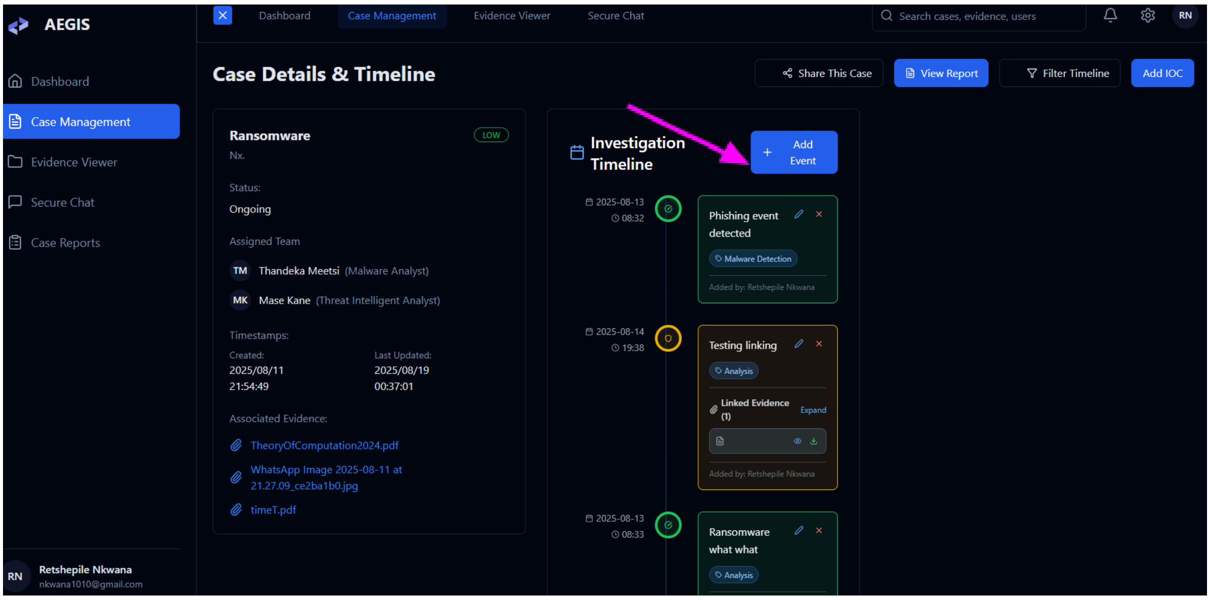
- Step-by-step:
    1. Scroll down to active cases.
    2. Click on “view details”.



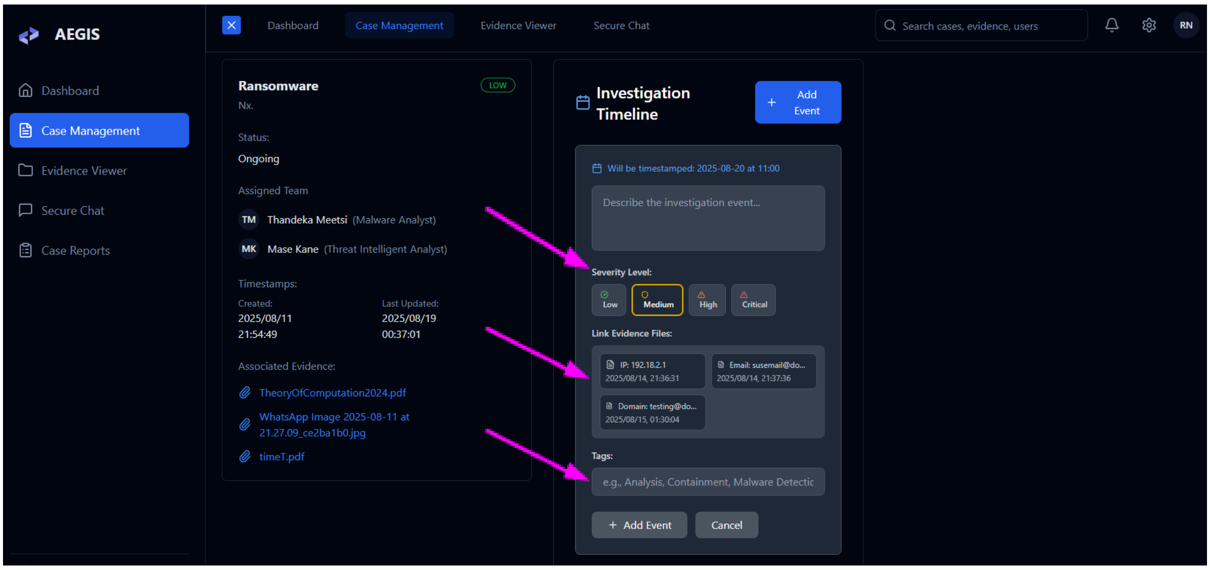
3. In the top left corner you can add events to your timeline by clicking “Add event” and entering the associated information.
4. You can also filter your timeline by date and keyword.
5. Here you can also view the time at which the case was created, and when the last modifications occurred.



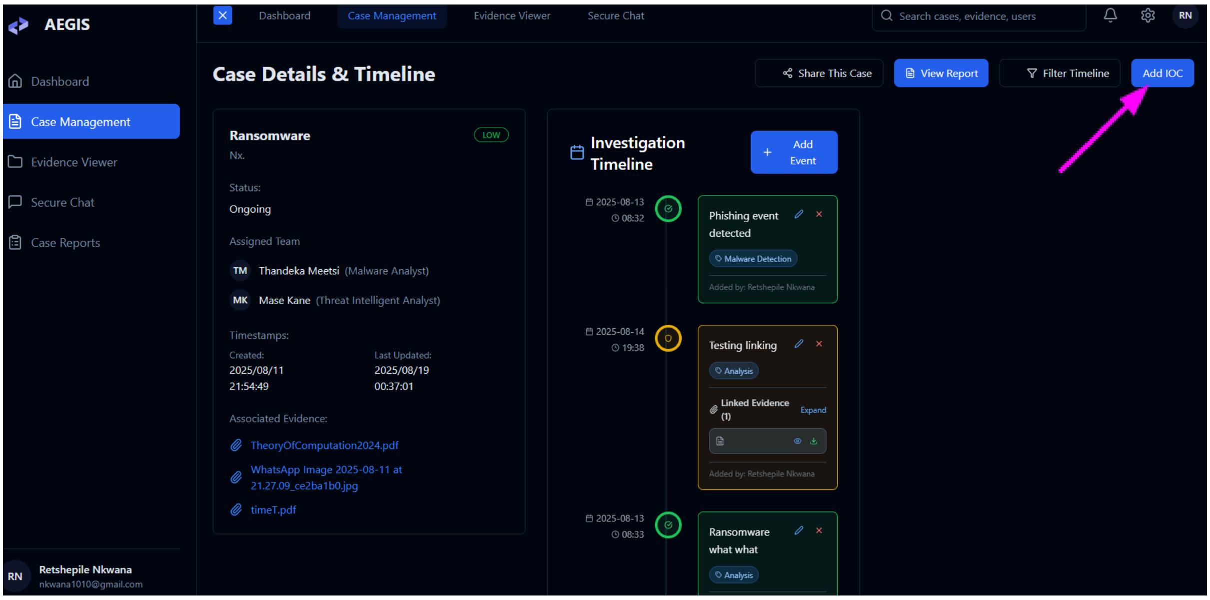
6. On the top right of the investigation Timeline card, is an Add Event button.



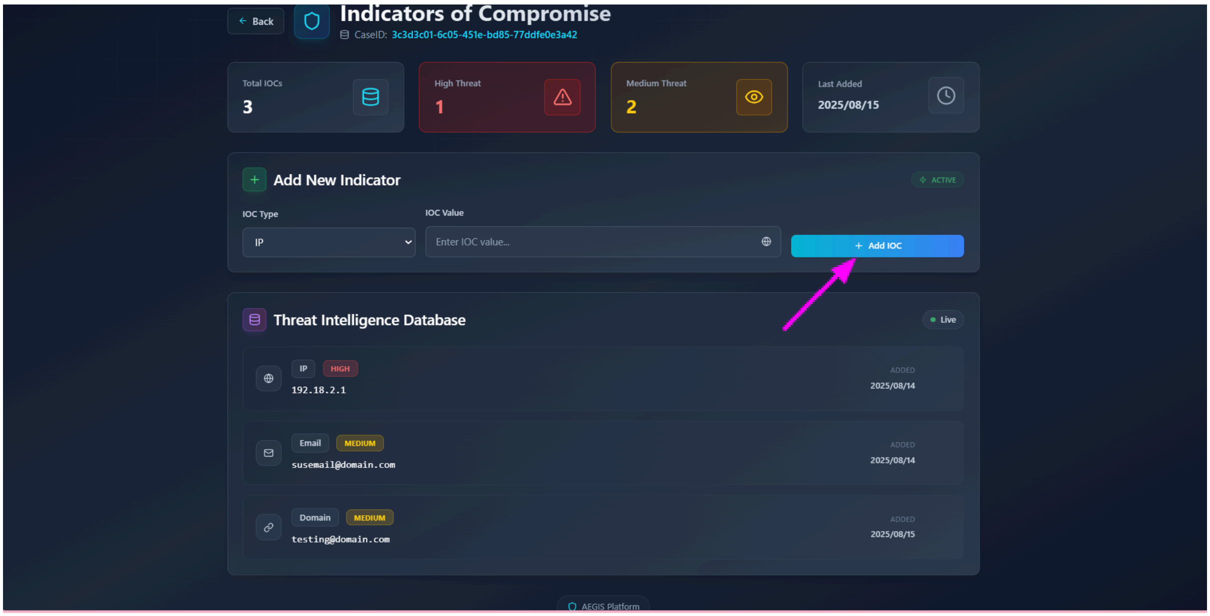
7. When you click the Add Event, you will be shown a form provided for you to enter an event that occurred during the investigation.



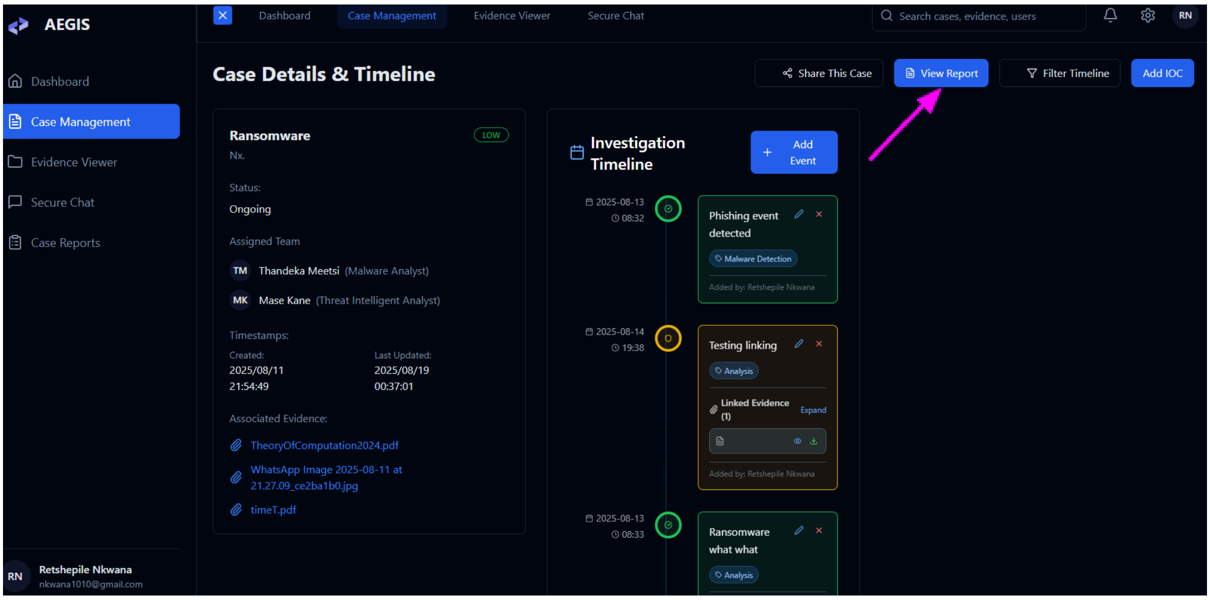
8. On this form you can select the security level of each event (how detrimental it could be to the system being attacked), attach an evidence file around which the event is centred.
9. You can also tag the event, describing what it would be investigated for (analysis etc). You can proceed to adding an event.
10. The timeline will appear with the added event, colour coded with the security level.



11. On the Top right corner, there is an Add IOC button.
12. On this page, you should be able to add the Indicators of Compromise(IOCs) of the case you are currently investigating.
13. After this addition, the number of indicators for the case should increase to reflect that this has been recorded.

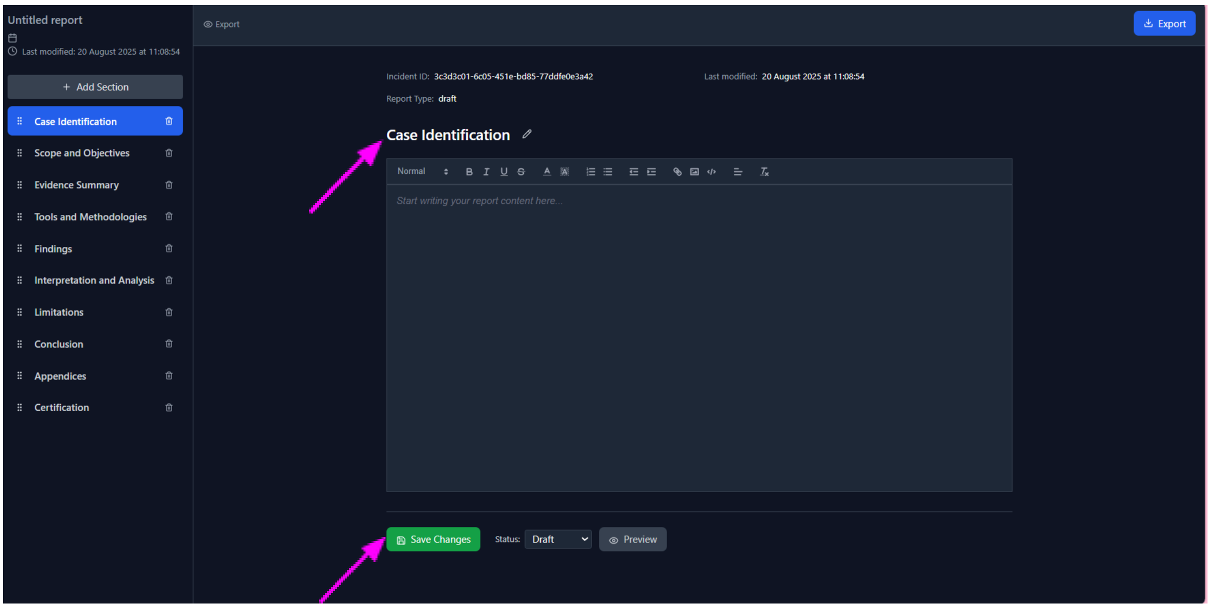


14. Still on the same page. On the top right corner, there is a “View Report” button.
15. When you click on this button, you should be redirected to the Reporting page.

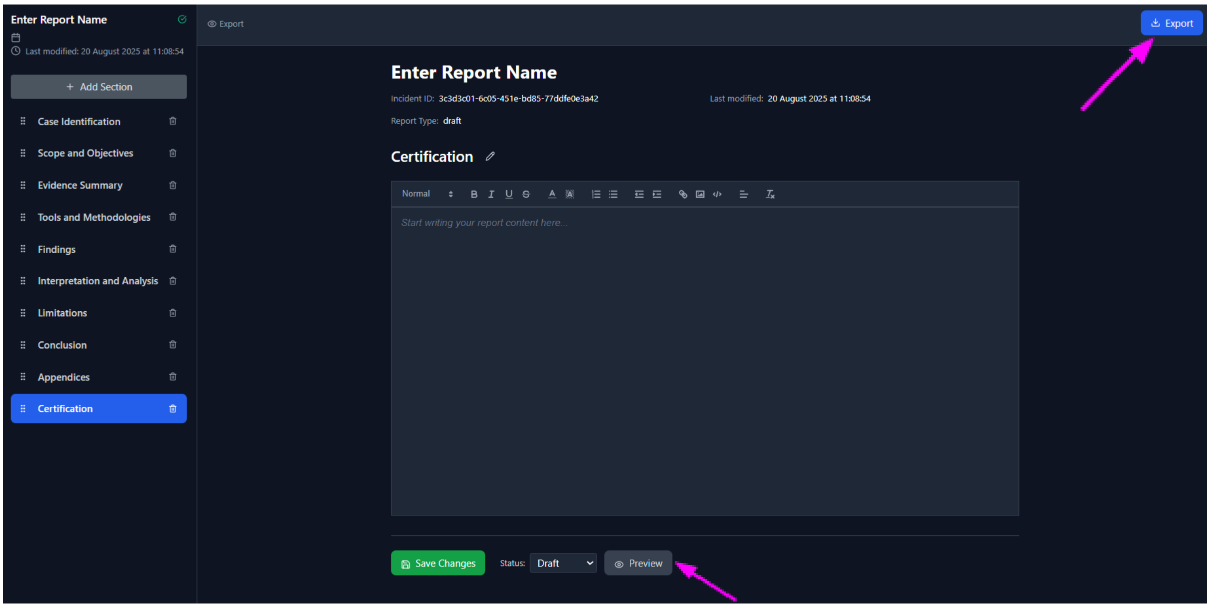


16. On this page, you should be able to create, edit, modify, and restructure your report.
17. After you have finished editing your report, you can preview the report.
18. After which, you should be able to Export the report.

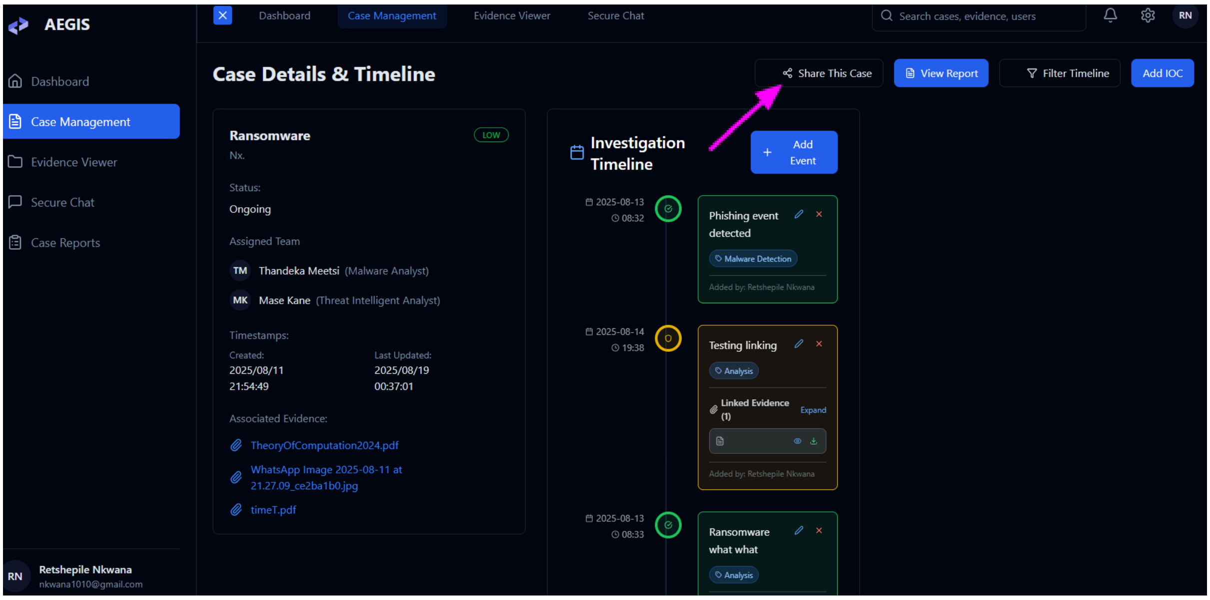
Reporting Page:



19. On the top left corner, you should be able to edit the report name which will reflect just on top of the editing area.



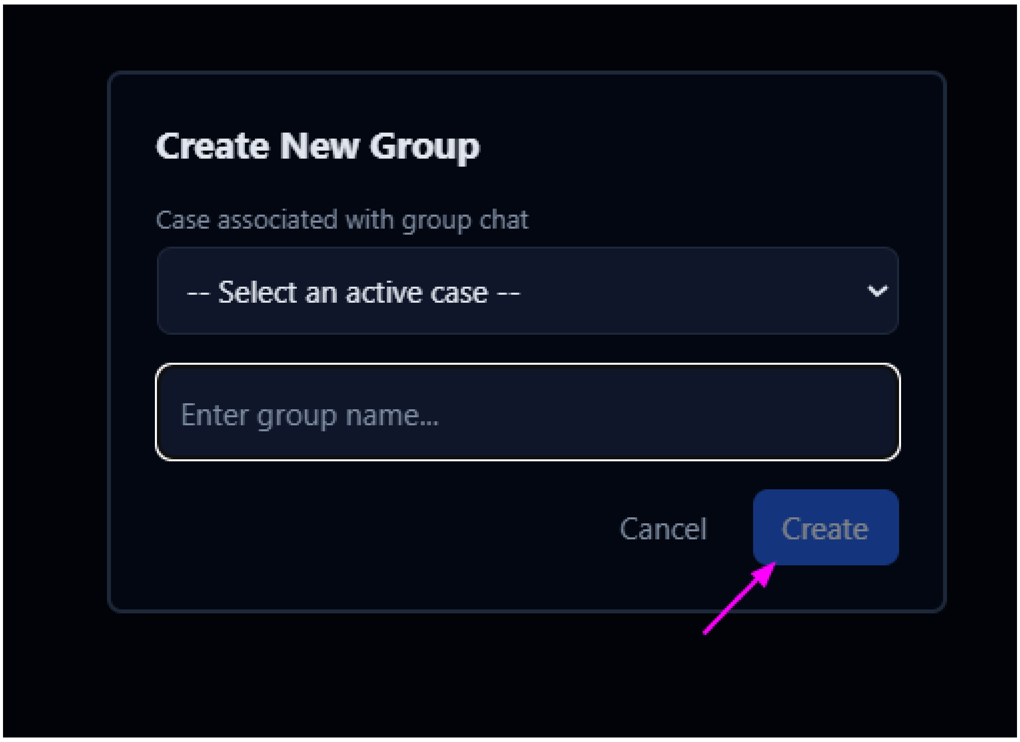
20. Still on the same page, you should be able to use a “Share Case” button. When you click on this button, you will be shown a form.



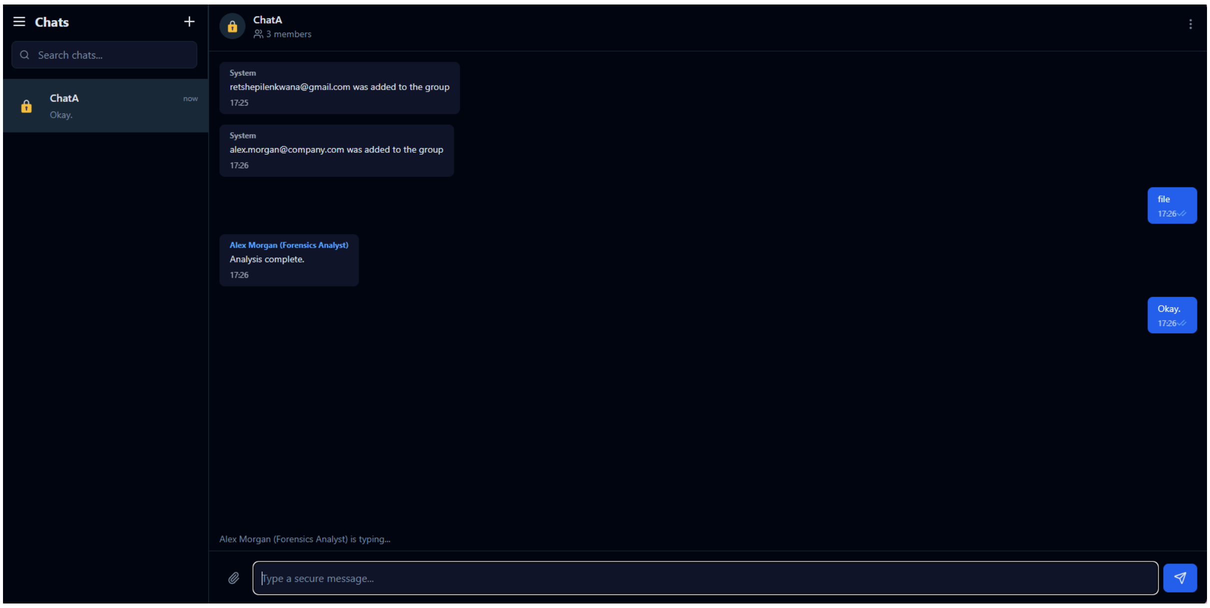
21. On this page, you will be able to enter the details of the person with whom you would like to share a case.
22. After you click the “Send Invite” button, you will be redirected back to the Case Management page.

<u>Secure chat:</u>

- Step-by-step:
    1. Once logged in, navigate to the Secure Chat page.
    2. You can create a new chat by entering the name of the chat in the text box.



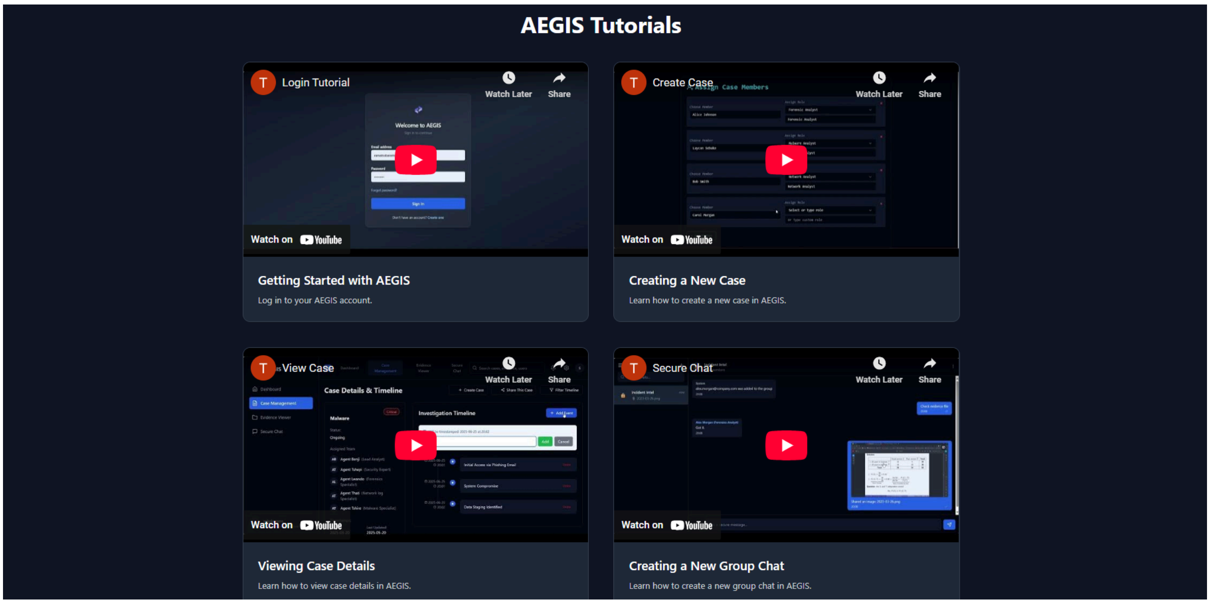
3. You can then add members to the chat.
4. Using the chat box at the bottom, you can enter a message and click the send icon to send the message to the chat.

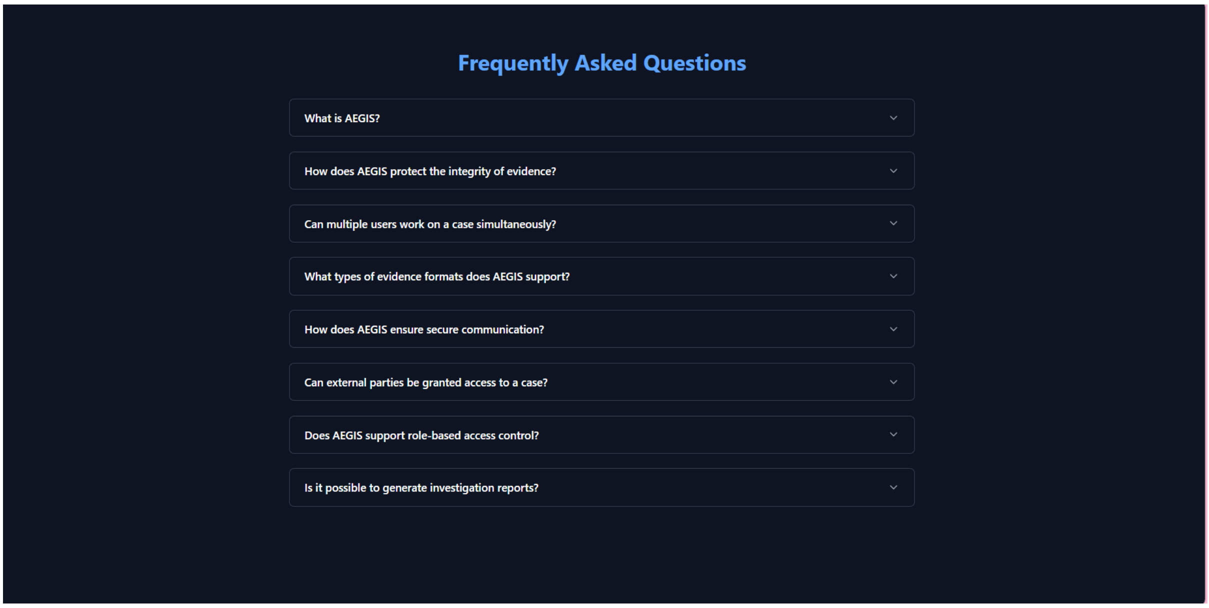


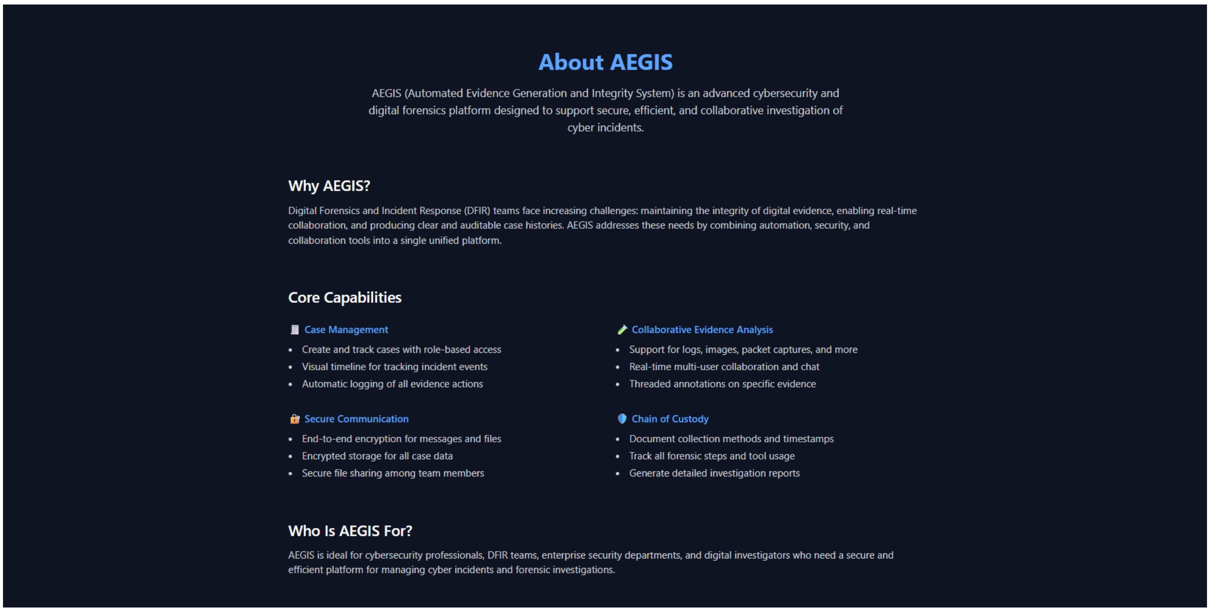
If you need tutorials, live demos or FAQS, you can navigate to the Help & Support tab on the landing page.

Tutorials & Help

1. On the bottom right corner, you can click the “?” icon, which would allow you to access the Help & Support documentation.




Frequently Asked Questions
What is AEGIS?
How does AEGIS protect the integrity of evidence?
Can multiple users work on a case simultaneously?
What types of evidence formats does AEGIS support?
How does AEGIS ensure secure communication?
Can external parties be granted access to a case?
Does AEGIS support role-based access control?
Is it possible to generate investigation reports?


About AEGIS
AEGIS (Automated Evidence Generation and Integrity System) is an advanced cybersecurity and digital forensics platform designed to support secure, efficient, and collaborative investigation of cyber incidents.
Why AEGIS?
Digital Forensics and Incident Response (DFIR) teams face increasing challenges: maintaining the integrity of digital evidence, enabling real-time collaboration, and producing clear and auditable case histories. AEGIS addresses these needs by combining automation, security, and collaboration tools into a single unified platform.
Core Capabilities
Case Management
Create and track cases with role-based access
Visual timeline for tracking incident events
Automatic logging of all evidence actions
Collaborative Evidence Analysis
Support for logs, images, packet captures, and more
Real-time multi-user collaboration and chat
Threaded annotations on specific evidence
Secure Communication
End-to-end encryption for messages and files
Encrypted storage for all case data
Secure file sharing among team members
Chain of Custody
Document collection methods and timestamps
Track all forensic steps and tool usage
Generate detailed investigation reports
Who Is AEGIS For?
AEGIS is ideal for cybersecurity professionals, DFIR teams, enterprise security departments, and digital investigators who need a secure and efficient platform for managing cyber incidents and forensic investigations.