

```
kali_linux@kali: ~/forensics_project_phase4
File Actions Edit View Help

(kali_linux@kali)-[~/forensics_project_phase4]
$ md5sum drug_trials_data.zip > cloud_file_hash.txt

(kali_linux@kali)-[~/forensics_project_phase4]
$ cat cloud_file_hash.txt
93c8d792f49b2b5690186e2c919e9db0  drug_trials_data.zip

(kali_linux@kali)-[~/forensics_project_phase4]
$
```

```
kali_linux@kali: ~/forensics_project_phase4
File Actions Edit View Help

(kali_linux@kali)-[~/forensics_project_phase4]
$ grep "drug_trials_data.zip" sharepoint_audit.log > audit_results.txt

(kali_linux@kali)-[~/forensics_project_phase4]
$ cat audit_results.txt
2025-04-05 02:20:00 - Action: Upload - File: drug_trials_data.zip - User: jsmith - IP: 198.168.64.4
2025-04-05 02:20:05 - Action: Access - File: drug_trials_data.zip - User: competitor_user - IP: 24.24.0.118

(kali_linux@kali)-[~/forensics_project_phase4]
$
```

```
kali_linux@kali: ~/forensics_project_phase4
File Actions Edit View Help

(kali_linux@kali)-[~/forensics_project_phase4]
$ grep "198.168.64.4" api_access.log > api_results.txt










(kali_linux@kali)-[~/forensics_project_phase4]
$ cat api_results.txt
2025-04-05 02:19:55 - API Call: POST /upload - Endpoint: competitor.sharepoint.com - IP: 198.168.64.4 - Script: upload.py
2025-04-05 02:20:00 - API Call: PUT /files/drg_trials_data.zip - IP: 198.168.64.4

(kali_linux@kali)-[~/forensics_project_phase4]
$
```

Geolocation data from


IPapi.co

Product: API, real-time

 IP ADDRESS: 24.24.0.118	 ISP: TWC-11351-NORTHEAST
 COUNTRY: United States 	 ORGANIZATION: TWC-11351-NORTHEAST
 REGION: New York	 LATITUDE: 42.3414
 CITY: Bath	 LONGITUDE: -77.3049

Incorrect location?

[Contact IPapi.co](#)

 [view map](#)

```
kali_linux@kali: ~/forensics_project_phase4
File Actions Edit View Help

(kali_linux@kali)-[~/forensics_project_phase4]
$ sha256sum sharepoint_audit.log > audit_hash.txt

(kali_linux@kali)-[~/forensics_project_phase4]
$ cat audit_hash.txt
fd1afdf6907660a316b24713a851823da9fb5ee0273465c0ee06835bb9aab3a5 sharepoint_audit.log

(kali_linux@kali)-[~/forensics_project_phase4]
$ sha256sum api_acces.log > api_hash.txt
sha256sum: api_acces.log: No such file or directory

(kali_linux@kali)-[~/forensics_project_phase4]
$ cat api_hash.txt

(kali_linux@kali)-[~/forensics_project_phase4]
$ sha256sum api_access.log > api_hash.txt

(kali_linux@kali)-[~/forensics_project_phase4]
$ cat api_hash.txt
40f96bfcceeb1afe0e0892105ccd3863572a51b8ddaee4046ec6e65cc2e5487 api_access.log

(kali_linux@kali)-[~/forensics_project_phase4]
$
```

```
kali_linux@kali: ~/forensics_project_phase4
File Actions Edit View Help

(kali_linux@kali)-[~/forensics_project_phase4]
$ cat chain_of_custody.txt
Date: 2025-04-06

Evidence: sharepoint_audit.log
Handler: Billy Kidd
Action: Analyzed cloud audit logs
Hash: fd1afdf6907660a316b24713a851823da9fb5ee0273465c0ee06835bb9aab3a5

Evidence: api_access.log
Handler: Billy Kidd
Action: Analyzed API access logs
Hash: 40f96bfceeeb1afe0e892105ccd3863572a51b8ddaee4046ec6e65cc2e5487

(kali_linux@kali)-[~/forensics_project_phase4]
$
```

2. Images Drive Link => [AXIOM - Apr 08 2025 140159](#)

3. Below are 25 Capture The Flag (CTF) questions based on the case story of the pharmaceutical company data breach, designed to be solved using Magnet AXIOM. Each question includes the related artifacts from the story, instructions on how to approach it in Magnet AXIOM, and the specific techniques involved. These questions span the phases of the investigation, from initial discovery to resolution, and cover a variety of forensic techniques like log analysis, file system forensics, network forensics, and cryptanalysis.

Phase 1: Initial Discovery of the Breach

- 1. What time were the unauthorized database queries executed?**
 - **Artifact:** Database Access Logs
 - **How to Solve in Magnet AXIOM:** Load the database server log file into AXIOM. Use the “Timeline” view to filter events by timestamp, focusing on the night hours (e.g., 12:00 AM - 6:00 AM). Look for **SELECT * FROM drug_trials** queries.
 - **Answer:** 2:03 AM
- 2. Which employee account was used for the unauthorized login?**
 - **Artifact:** Authentication Logs
 - **How to Solve in Magnet AXIOM:** Load the authentication log file. In the “Evidence Sources” tab, filter for successful login events around 2:00 AM. Check the username field.
 - **Answer:** jsmith
- 3. What is the source IP address of the unauthorized login?**
 - **Artifact:** Authentication Logs
 - **How to Solve in Magnet AXIOM:** From the same authentication log in AXIOM, locate the login event for **jsmith** at 2:00 AM. Extract the source IP address from the log entry.

- **Answer:** 192.168.1.100
- 4. **Does the source IP match any known company device?**
 - **Artifact:** Authentication Logs + Company IP Whitelist (assumed)
 - **How to Solve in Magnet AXIOM:** Export the IP from the authentication log (192.168.1.100). Use AXIOM's "Search" feature to cross-reference it against a provided whitelist of company IPs. If no match is found, it's external.
 - **Answer:** No
- 5. **How many database queries were executed during the breach?**
 - **Artifact:** Database Access Logs
 - **How to Solve in Magnet AXIOM:** In the "Artifacts" tab, filter for database query events (e.g., **SELECT**) between 2:00 AM and 2:15 AM. Count the distinct query entries.
 - **Answer:** (Assume 5 for this example; adjust based on provided logs)

Phase 2: Tracing the Insider Threat

- 6. **What is the name of the phishing email attachment?**
 - **Artifact:** Email Client Data (Outlook PST)
 - **How to Solve in Magnet AXIOM:** Load the PST file into AXIOM. Navigate to the "Email" artifact category, filter for emails received before the breach date, and search for "credentials" in the subject or attachment name.
 - **Answer:** credentials_update.docx
- 7. **When was the phishing email received?**
 - **Artifact:** Email Client Data
 - **How to Solve in Magnet AXIOM:** In the "Email" view, locate the email with **credentials_update.docx**. Check the timestamp in the email metadata.
 - **Answer:** (Assume hours before 2:00 AM, e.g., 1/15/2025 10:00 PM)
- 8. **What script was executed to escalate privileges?**

- **Artifact:** Registry Artifacts
 - **How to Solve in Magnet AXIOM:** Load the workstation's forensic image. In the "Registry" artifact category, filter for **RunOnce** keys. Look for PowerShell script executions.
 - **Answer:** elevate_privileges.ps1
- 9. What is the name of the deleted file containing stolen data?**
- **Artifact:** File System Artifacts
 - **How to Solve in Magnet AXIOM:** Load the workstation image. Go to "File System" view, enable "Recover Deleted Files," and search for **.zip** files in unallocated space.
 - **Answer:** drug_trials_data.zip
- 10. What is the MD5 hash of the recovered .zip file?**
- **Artifact:** File System Artifacts
 - **How to Solve in Magnet AXIOM:** After recovering **drug_trials_data.zip**, right-click the file in AXIOM's "File System" view and select "Calculate Hash." Note the MD5 value.
 - **Answer:** (Generate a sample hash, e.g., **d41d8cd98f00b204e9800998ecf8427e**)

Phase 3: Reconstructing the Data Exfiltration

- 11. What protocol was used for the data exfiltration?**
- **Artifact:** Packet Captures (PCAP Files)
 - **How to Solve in Magnet AXIOM:** Load the PCAP file. In the "Network" tab, filter for outbound traffic around 2:15 AM. Check the protocol field.
 - **Answer:** HTTPS
- 12. What is the destination IP address of the exfiltration traffic?**
- **Artifact:** Packet Captures
 - **How to Solve in Magnet AXIOM:** In the "Network" view, filter for HTTPS traffic at 2:15 AM. Extract the destination IP from the packet details.
 - **Answer:** (Assume a sample IP, e.g., 104.18.40.123)
- 13. What domain was resolved during the exfiltration?**
- **Artifact:** DNS Query Logs

- **How to Solve in Magnet AXIOM:** Load the DNS logs. Filter for queries around 2:15 AM in the “Network” or “Logs” tab. Identify the resolved domain.

- **Answer:** competitorcorp.sharepoint.com

14. What was the volume of outbound traffic during the breach?

- **Artifact:** NetFlow Data
- **How to Solve in Magnet AXIOM:** Load the NetFlow data. In the “Timeline” view, filter for outbound traffic at 2:15 AM and sum the byte count.
- **Answer:** (Assume 500 MB for this example)

15. At what exact time did the exfiltration begin?

- **Artifact:** Packet Captures
- **How to Solve in Magnet AXIOM:** In the “Network” tab, sort HTTPS traffic by timestamp. Find the first packet to competitorcorp.sharepoint.com.
- **Answer:** 2:15 AM

Phase 4: Following the Data to the Cloud

16. What time was the stolen file uploaded to the cloud?

- **Artifact:** Cloud Service Audit Logs
- **How to Solve in Magnet AXIOM:** Load the SharePoint logs. In the “Logs” tab, filter for upload events and check the timestamp for drug_trials_data.zip.
- **Answer:** 2:20 AM

17. What IP address uploaded the file to SharePoint?

- **Artifact:** Cloud Service Audit Logs
- **How to Solve in Magnet AXIOM:** From the same upload event in the SharePoint logs, extract the source IP address.
- **Answer:** (Assume John’s home IP, e.g., 73.12.45.67)

18. Does the uploaded file’s hash match the recovered .zip file?

- **Artifact:** File Metadata in Cloud Storage
- **...

Here’s the continuation of the 25 CTF questions based on the pharmaceutical company data breach case story, designed for

Magnet AXIOM. I'll pick up where I left off (Question 19) and complete the list through Phases 4, 5, and 6. Each question includes the related artifacts, instructions for solving in Magnet AXIOM, and sample answers where applicable.

Phase 4: Following the Data to the Cloud (Continued)

19. What method was used to upload the file to the cloud?

- **Artifact:** API Access Logs
- **How to Solve in Magnet AXIOM:** Load the API access logs from the cloud provider into AXIOM. In the “Logs” tab, filter for events around 2:20 AM related to **drug_trials_data.zip**. Look for API call details (e.g., **POST** requests) indicating programmatic access.
- **Answer:** Scripted upload via API

20. Where does the IP address of the upload geolocate to?

- **Artifact:** Cloud Service Audit Logs
- **How to Solve in Magnet AXIOM:** Extract the source IP (e.g., 73.12.45.67) from the SharePoint upload event. Use AXIOM’s “Connections” or “Search” feature with an integrated geolocation tool (or manually check with MaxMind GeoIP) to trace the IP.
- **Answer:** John Smith’s home address (e.g., a city like “Boston, MA”)

Phase 5: Uncovering Encrypted Communications

21. What encryption algorithm was used for the suspect’s emails?

- **Artifact:** Encrypted Email Backups
- **How to Solve in Magnet AXIOM:** Load the email server backup image. In the “File System” view, recover the encrypted email file from unallocated space (e.g., using “Recover Deleted

Files”). Analyze the file header or metadata to identify the encryption type.

- **Answer:** AES-128

22. What is the weak encryption key used in the communications?

- **Artifact:** Encryption Keys (Configuration File)
- **How to Solve in Magnet AXIOM:** Load the workstation image. In the “File System” tab, search for configuration files (e.g., **.cfg** or **.ini**) containing key-like strings. Locate the file with **P@ssw0rd123**.
- **Answer:** P@ssw0rd123

23. What tool can crack the weak encryption key, and how long did it take?

- **Artifact:** Encryption Keys
- **How to Solve in Magnet AXIOM:** Export the encrypted email and key (**P@ssw0rd123**) from AXIOM. While AXIOM itself doesn’t crack keys, note that an external tool like John the Ripper was used (per the story). Simulate this by documenting the key’s weakness (e.g., common password).
- **Answer:** John the Ripper, cracked in hours (e.g., 3 hours)

24. What was the content of the decrypted email to the competitor?

- **Artifact:** Encrypted Email Backups
- **How to Solve in Magnet AXIOM:** After cracking the key externally, re-import the decrypted email into AXIOM. In the “Email” tab, view the message content.
- **Answer:** “The data is yours for \$5 million. Upload complete.”

25. Who was the recipient of the encrypted email?

- **Artifact:** Encrypted Email Backups
- **How to Solve in Magnet AXIOM:** In the decrypted email from the “Email” tab, check the “To” field or metadata for the recipient’s address or name.
- **Answer:** A competitor executive (e.g., **exec@competitorcorp.com**)

Phase 6: Resolution and Legal Action

(Note: Phase 6 focuses on reporting and chain of custody, which are less about active discovery in AXIOM but still involve evidence handling. I've adjusted the last question to fit the CTF format.)

25. Which artifact confirms the exact time the forensic image of the server logs was created?

- **Artifact:** Chain of Custody Documentation
- **How to Solve in Magnet AXIOM:** Load the chain of custody documentation (e.g., a text or PDF file) into AXIOM. In the “Documents” tab, search for the entry related to the database server log forensic image creation. Extract the timestamp.
- **Answer:** (Assume a sample time, e.g., 1/16/2025 9:00 AM)

Summary of Artifacts and Techniques in Magnet AXIOM

- **Artifacts Used:**
- **Database Access Logs, Authentication Logs, Email Client Data (PST), Registry Artifacts, File System Artifacts (deleted .zip), Packet Captures (PCAP), DNS Query Logs, NetFlow Data, Cloud Service Audit Logs, File Metadata, API Access Logs, Encrypted Email Backups, Encryption Keys, Forensic Report, Chain of Custody Documentation.**
- **Techniques Demonstrated in AXIOM:**
- **Log file analysis (filtering by timestamp/IP), file system forensics (recovering deleted files), registry parsing, network forensics (PCAP analysis, DNS lookups), hash comparison, email analysis, data carving (unallocated space), and documentation review.**

How to Set Up the CTF in Magnet AXIOM

1. Prepare Evidence Files:

- Create sample log files (e.g., database and authentication logs with timestamps/IPs), a PST file with a phishing email, a forensic image with a deleted .zip and registry keys, a PCAP file with HTTPS traffic, DNS/NetFlow logs, cloud audit logs, an encrypted email file, and chain of custody docs.
2. Load into AXIOM:
 - Use AXIOM Process to ingest all evidence files (logs, images, PCAPs, etc.) into a single case.
 3. Guide Participants:
 - Provide a brief of the case story and instructions to use AXIOM's "Timeline," "Artifacts," "File System," "Network," and "Search" features to answer each question.
 4. Validate Answers:
 - Check participant responses against the predefined answers (e.g., timestamps, IPs, file names) embedded in the evidence.

This CTF setup mimics a real-world digital forensics investigation, leveraging Magnet AXIOM's capabilities to explore logs, recover files, analyze network traffic, and more. Let me know if you'd like sample evidence files or further refinements!

4. Report Drive Link - [Export](#)