

Analysis and Reporting

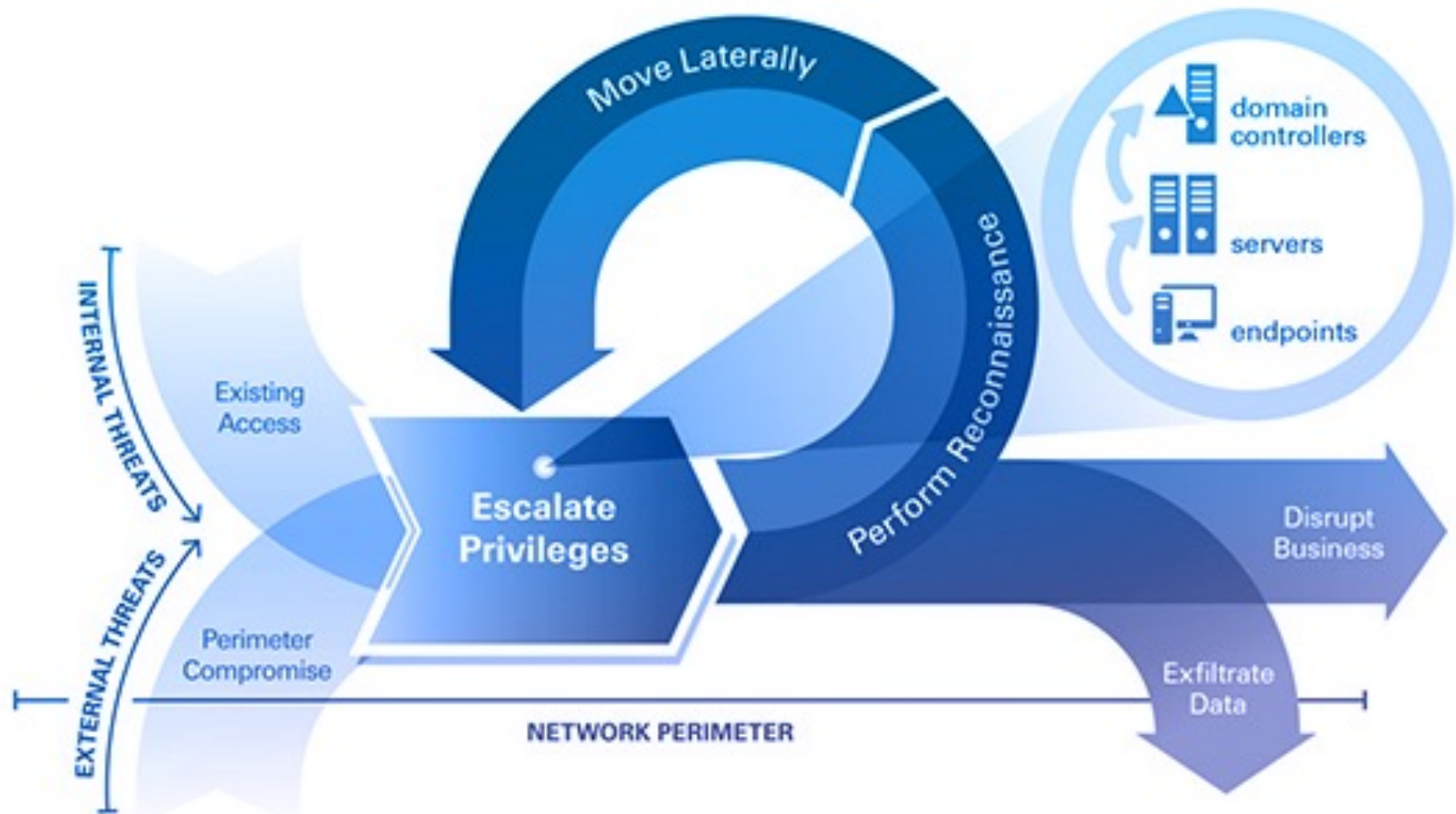
Examination and Analysis

- Searching for evidence
- Interpreting evidence
- Analysis of the evidence in the context of the incident / investigation

Analysis In-Depth

- Useful to think of graphs and timelines
- Use investigative loops to process evidence:
 - Determine hypothesis
 - Recover / extract data from available sources
 - Harvest data and metadata about all items of interest
 - Organize and search data
 - Reduce data to aid in analysis

Attack Lifecycle



Example Analysis

- Map out a theoretical attack / walk through with a phishing attack and malware installation
- Walk through attack lifecycle, sample artifacts, timeline
- Work backwards / forwards in the timeline
- Practice discovery / filtering (reduction)

Example Analysis

1

- Initial Phish
- Email message, contents, malicious link or attachment.

2

- Initial execution
- Evidence of document executing on system.
- Evidence of malware loader / execution (powershell, rundll32, etc.)

3

- Malware installation
- Evidence of malware binary execution
- Evidence of malware persistence (Autoruns, registry, etc.)

Scientific Method

- When in doubt, use the scientific method:
 - Observation
 - Hypothesis
 - Prediction
 - Experimentation / testing
 - Conclusions

Temporal Analysis

- Using a chronological list of events, focus on people and events (when)
- Look for patterns, gaps, and anomalies

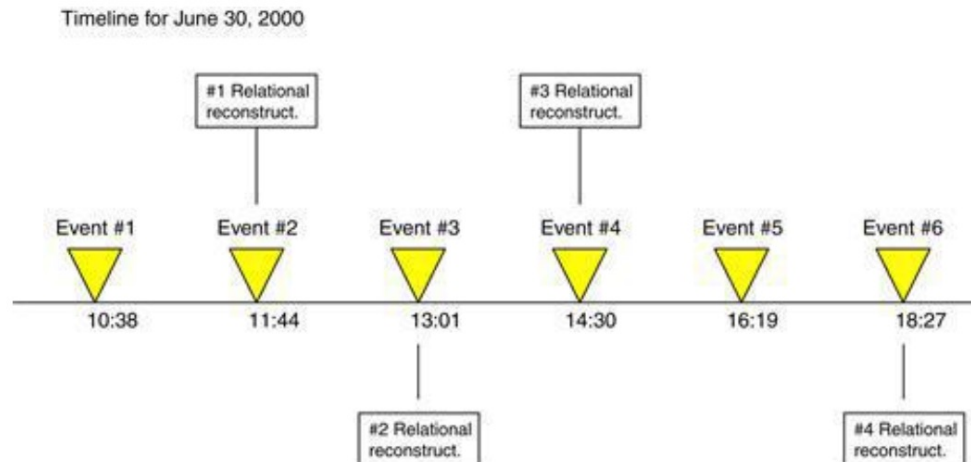


Figure 8.1 Conceptual view of timeline and relational reconstructions.

Relational Analysis

- Track objects, people and relationships (who, what, where)

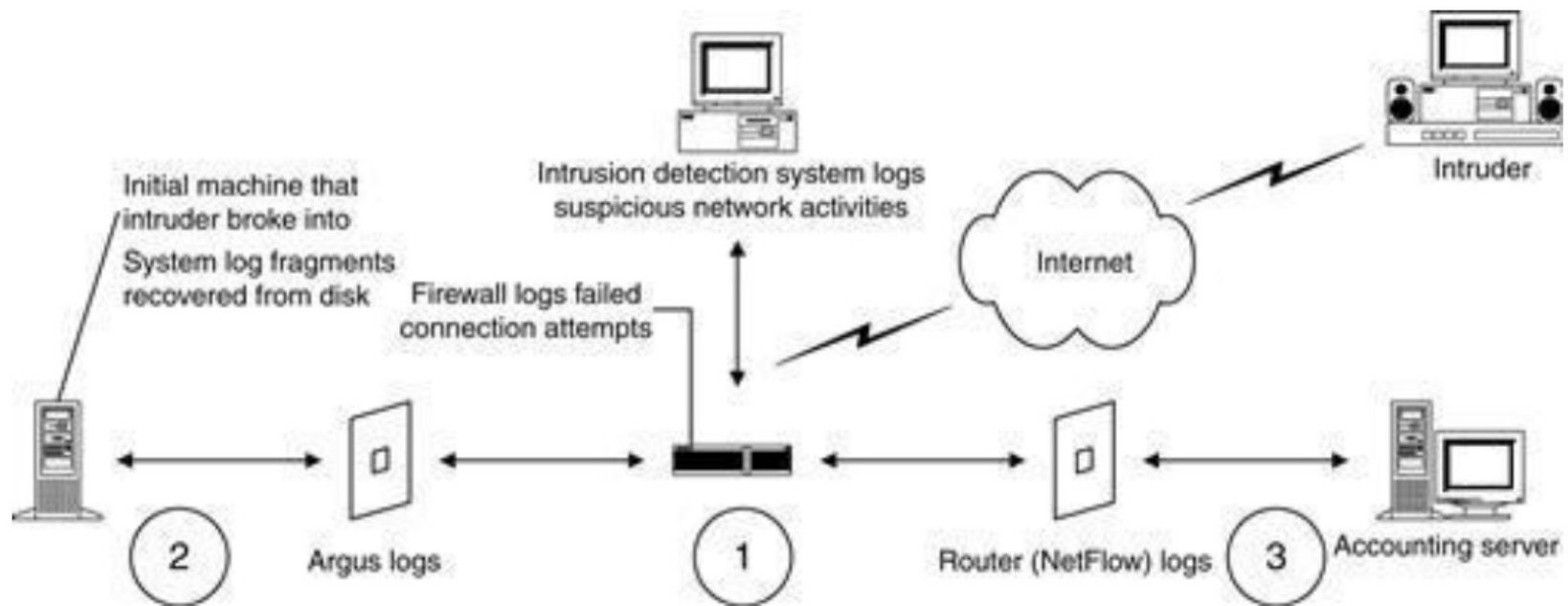
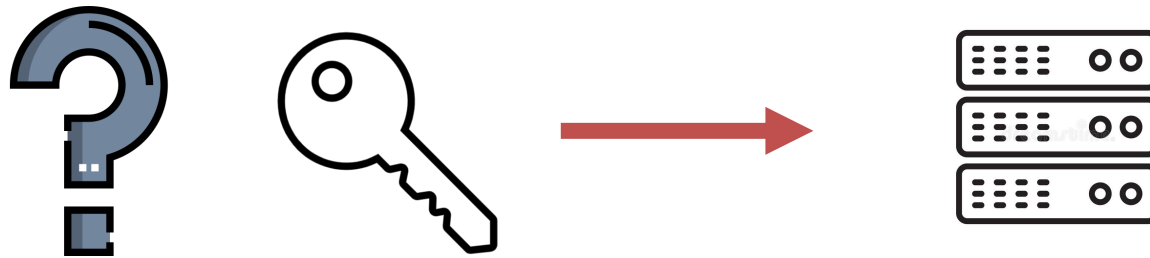


Figure 8.2 Diagram depicting intruder gaining access to accounting server.

Functional Analysis

- Use an understanding of the outcomes and impacts to build an understanding of what conditions are necessary (how)
- Ex: If a server was accessed from the workstation – how did that happen – need credentials for the server – how were they obtained?



Reporting

Presentation

- Without good reporting, great forensic work will go un-noticed
- Findings from the investigation must be reported in a manner which satisfies the context of the investigation

Understand Objectives

- The first step to good reporting is understanding the report format and objectives
- This should be done during investigation planning and must be done before analysis starts

Take Good Technical Notes

- The second step to good reporting is good notes
- Good technical notes are absolutely critical to good reporting
- Track every action and the outcome
- Use a scratch sheet to track key outputs and characteristics:
 - Key filenames, IP addresses, Hash values, File paths, tool outputs
- At any point you should be able to describe what your output is and how you got there

Reporting

- All good forensic reports include:
 - Affected assets (computers, identities, etc.)
 - Description of how the activity started
 - Sequential timeline of relevant events
 - Statements related how evidence supports / doesn't support hypotheses related to the goals of the investigation

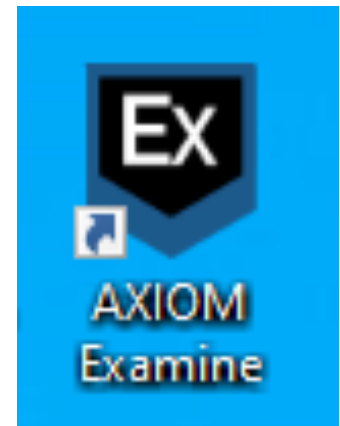
Introduction to Magnet

What is Magnet Axiom

- Axiom is the primary tool that we're going to use for forensic analysis
- Capabilities for a lot of automated analysis, however, we're going to focus on leveraging the core forensic capabilities:
 - Disk / file indexing and analysis
 - File carving
 - Memory analysis


Axiom Primary Components

- Axiom Process
 - Loads evidence and creates case files
- Axiom Examine
 - Where we actually get to look at evidence



Creating a New Case

- Axiom organizes evidence into “cases”
- To load new evidence – go to “CREATE NEW CASE”

 Magnet AXIOM Process 5.8.0.27495

File Tools Help

CREATE NEW CASE

CREATE NEW CASE

Case Preparation

LOCATION FOR CASE FILES

Folder name AXIOM - SUPERIMPORTANTCASE

File path C:\Users\wep\Downloads\AxiomT001

BROWSE

Available space: 6.82 GB

- The case defaults are fine for our purposes so we're not going to change these for now other than to make sure that our Case File folder name is unique to the lab / case that we're working

Initial Evidence Processing

- Click “Go to evidence sources” in the lower right corner

GO TO EVIDENCE SOURCES

- Select “COMPUTER”
- Select “WINDOWS”
- Select “LOAD EVIDENCE”

Initial Evidence Processing (Cont'd)

- We're primarily going to work with disk images and memory so remember these two icons:

EVIDENCE SOURCES

WINDOWS

SELECT EVIDENCE SOURCE



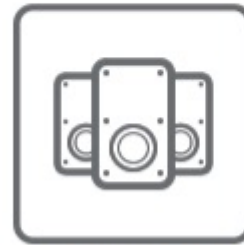
DRIVE



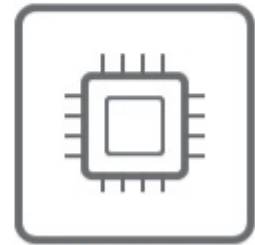
IMAGE



FILES & FOLDERS



VOLUME SHADOW COPY



MEMORY

Getting into Axiom Examine

- Start by opening the case we created – navigate to the folder and open the case
- The first time you open the case, it will be processing evidence as seen in the lower-left corner



Processing evidence...

[LOAD NEW RESULTS](#)

- It's going to take a while for evidence to index and load.
- Once processing is complete – click “LOAD NEW RESULTS”

Axiom Examine Basics

- Let's start with the aptly named “places to start”
- Click on “VIEW ALL ARTIFACT CATEGORIES”

PLACES TO START

ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source **All**

Number of artifacts **60,181**

