SWINBURNE UNIVERSITY OF TECHNOLOGY

ICT30010 eForensic Fundamentals

Lecture 11
Capstone Assignment

Troy Pretty

Digital Forensic Analyst

Assignment Outline

- Page 2 – Background
  - Outlines what you are investigating
    - Important information dates/times/names etc
- Page 3 – Exhibits
  - Provided by the police
    - What you are looking for
- Page 4 – Advice
  - Small prompts on what may assist
  - Not to be followed step-by-step, this is not a lab

Assignment Outline

- Page 6 – Forensic Report
  - What you are being assessed on (criteria)
    - Read and understand the criteria
    - Read the criteria again and refer to this throughout
  - Criteria 4 to 7 map to the 4 scenarios on page 2
    - Allocated marks are an indication of the amount of evidence

Chain of Custody/Continuity

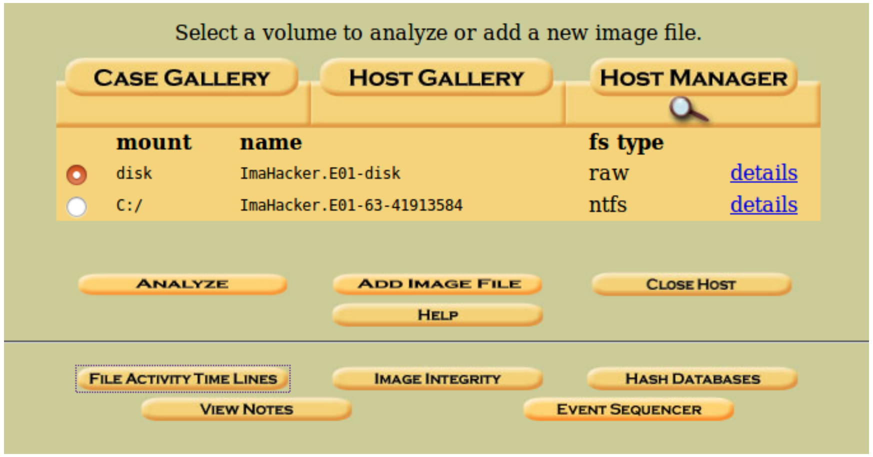
- What, when, how
  - What did you receive?
    - Forensic image, log file, compressed archive (extracted and then contained a forensic image and hash), exhibits (images/emails),
  - When did you receive it?
    - Date and time
  - How did you receive it?
    - In person, on a usb, via email, downloaded (url/link)

Chain of Custody/Continuity

- Process
  - What did you do with the item?
    - Extracted, copied to forensic workstation
  - Verification
    - What did you verify and was it a match?

Timeline Tools

- Filesystem Activity
  - Files only
    - Modify, Access, Created
  - Ran via Autopsy browser



Select a volume to analyze or add a new image file.

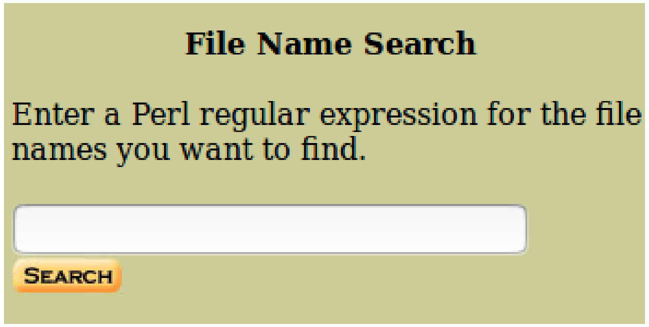
	mount	name	fs type	
●	disk	ImaHacker.E01-disk	raw	details
○	C:/	ImaHacker.E01-63-41913584	ntfs	details

Timeline Tools

- Super Timeline
  - Larger scope events
    - Configurable
    - Operating system artifacts such as internet history
    - Super Timeline provided as a part of the assessment

Searching

- Keyword Searches
  - Valuable tool to assist finding items of interest
  - Filename Searches



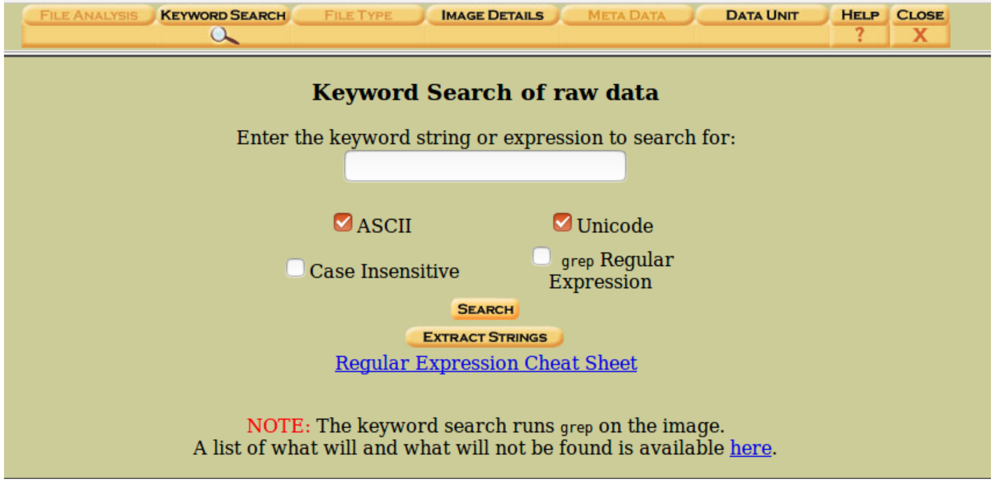
File Name Search

Enter a Perl regular expression for the file names you want to find.

  - Keyword Lists
    - Start with known - Email addresses, user ids, websites
    - Adjust as the investigation progresses

Searching

- Default search is time consuming
  - Search is run each time against the evidence
- Index the item (extract the strings)
  - Slow to process initially
  - All searches are real-time against index



Keyword Search of raw data

Enter the keyword string or expression to search for:

☑ ASCII ☑ Unicode

□ Case Insensitive □ grep Regular Expression

Regular Expression Cheat Sheet

NOTE: The keyword search runs grep on the image.
A list of what will and what will not be found is available here.

Pivoting

- Critical to the success of the investigation
- The existence of an item is not sufficient
  - Keep asking your self how?
- Start with the known event
  - Locate the event in the evidence
  - Look each side of the event
  - Understand/interpret the findings
  - Construct the timeline

Pivoting Example

- x-5 – Windows start-up
- x-4 – User logon
- x-3 – Google search “How to pirate movies”
- x-2 – Website accessed
- x-1 – Search for movie title
- x – Pirated movie downloaded
- x+1 – Google search “Media Player”
- x+2 – Media player downloaded
- x+3 – Media player installed
- x+4 – Media player opened
- x+5 – Movie played

Breakdown Evidence Elements

- Not just an item of interest
- For example an email
  1. Filesystem details – Name, location, dates/times
  2. Email contents – To/from, date/time, content
  3. Attachments – Name, content, metadata
- Keep breaking down, keep explaining

How Much Evidence?

- Have you answered how?
  - Tool may be downloaded but not used/or doesn’t work
- Does your evidence tell the story?
- Unbiased
  - The lack of evidence may be evidence

Likely Evidence Sources

- Filesystem
- Internet History
- .lnk files
- Prefetch
- Application Data

Suggested Approach

- Introduction
- Chain of Custody
  - Detailed Dates and Times
- Treat each scenario as a separate investigation
  - Background
  - Process/Findings/Relevance
  - Results/Summary
  - Difficult to log detailed times for investigation (between dates)
- Conclusion

Report Content

- Process
- Present the evidence
  - Location
  - Dates/Times
  - Metadata
- Relevance
- Explanation of how the hack did/didn’t occur

Report Content

- Minimal Screenshots
  - Only where necessary to present evidence
    - E.g. Emails, websites, images
  - Don’t expect to see command windows, hex, etc.
- Tables with column headings
- Short brief sentences, avoid a wall of text
- Consider producing simple timelines
- Factual

Report Content

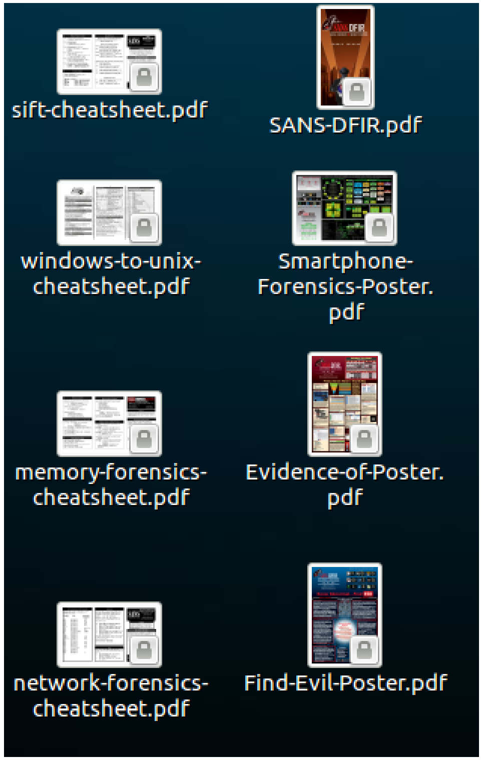
- Logical layout and easy to follow
- Language appropriate for the audience
- Glossary/Footnote to explain terms
- No assumptions or expected knowledge
  - Treat me like I don’t know
  - I wont fill in gaps when marking
- Give it to a non technical person to review

Reading Material

- All lectures and labs will assist
  - Lectures
    - Lecture 04 - Forensic Report Writing
    - Lecture 09 - Time Zones and Timelines
  - Labs
    - Lab 04 - Windows Forensics
    - Lab 05 - Introduction to Networks

Reading Material

- Desktop on the SANS SIFT Virtual Machine


sift-cheatsheet.pdf
SANS-DFIR.pdf
windows-to-unix-cheatsheet.pdf
Smartphone-Forensics-Poster.pdf
memory-forensics-cheatsheet.pdf
Evidence-of-Poster.pdf
network-forensics-cheatsheet.pdf
Find-Evil-Poster.pdf

Questions?

- Please use the Canvas discussion topics
  - Allows Aldin, Andrew or I to respond
  - Ensures all students receive the same consistent response