# WRITING REPORTS, EXPERT TESTIMONY AND ETHICS FOR THE EXPERT WITNESS
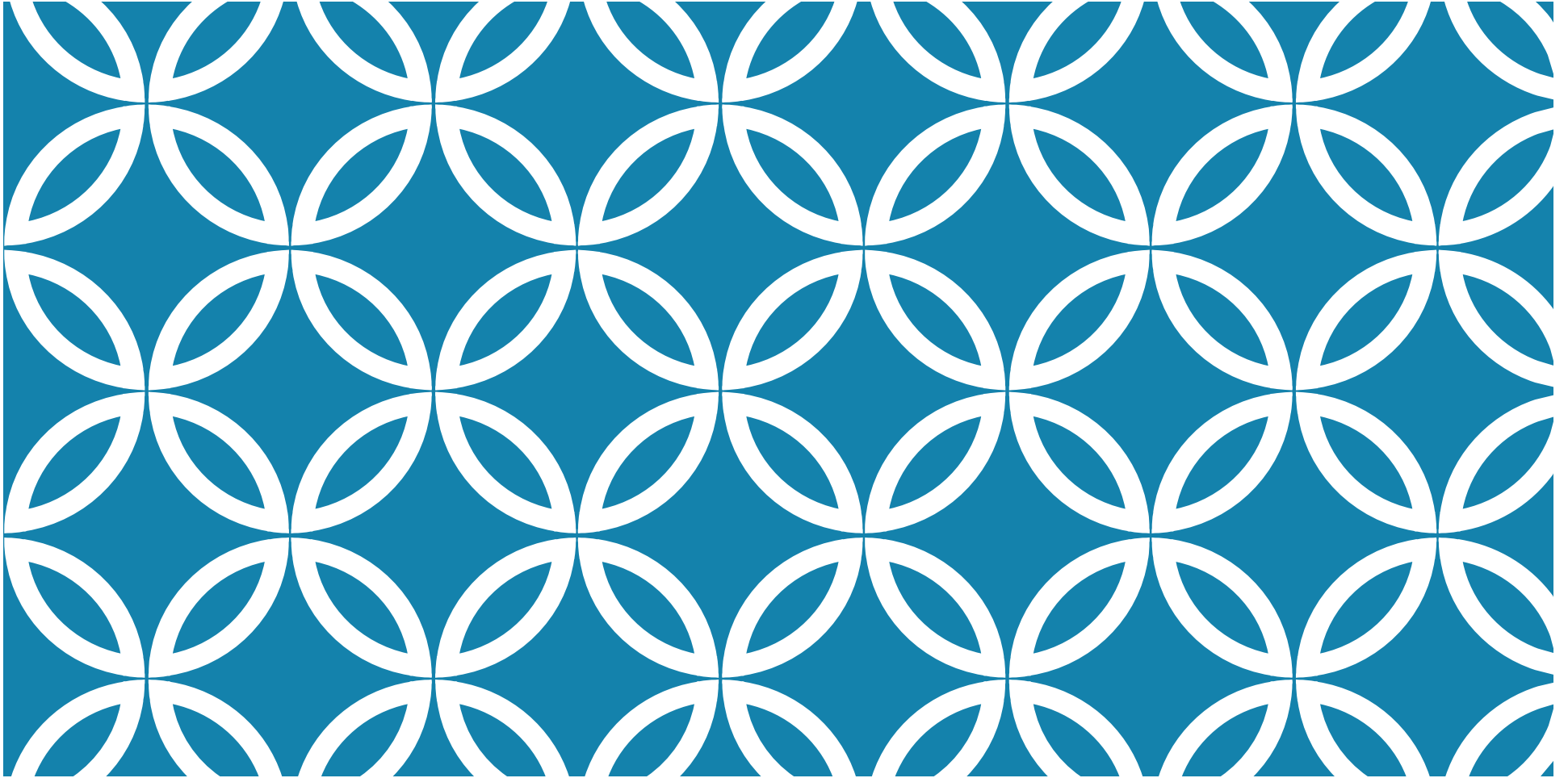
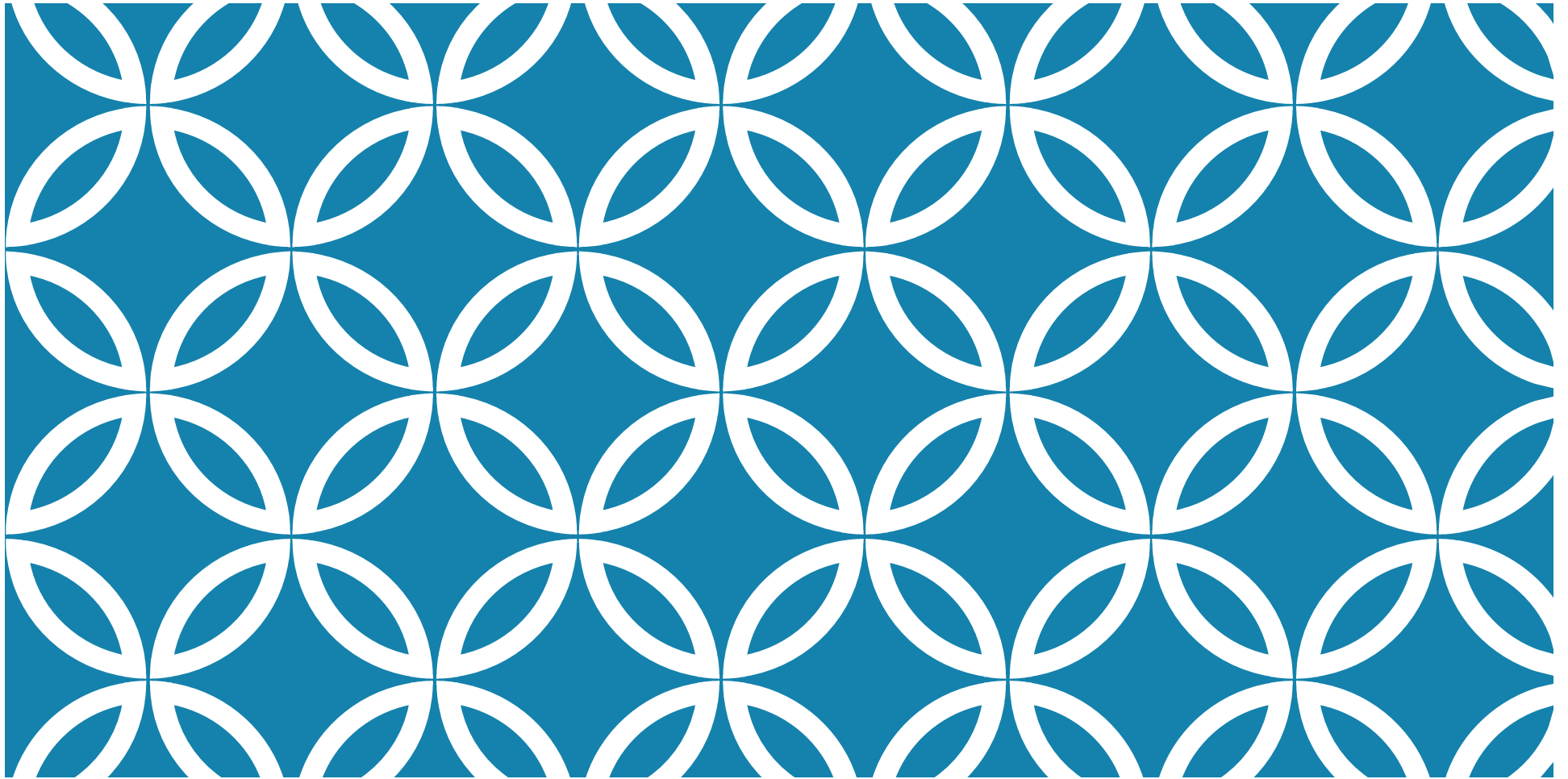*Chapter 13*

# REPORT WRITING FOR HIGH-TECH INVESTIGATIONS

# OBJECTIVES

- ❑ Explain the importance of reports

- ❑ Describe guidelines for writing reports

- ❑ Explain how to use forensics tools to generate reports

# UNDERSTANDING THE IMPORTANCE OF REPORTS

# UNDERSTANDING THE IMPORTANCE OF REPORTS

❑ Communicate the results of your investigation
  ❑ Including expert opinion

❑ Courts require expert witness to submit written reports

❑ Written report must specify fees paid for the expert's services
  ❑ And list all other civil or criminal cases in which the expert has testified for the preceding 4 years

❑ **Deposition banks**
  ❑ Examples of expert witness' previous testimonies

# LIMITING A REPORT TO SPECIFICS

❑ All reports to clients should start with the job mission or goal

  ❑ Find information on a specific subject

  ❑ Recover certain significant documents

  ❑ Recover certain types of files

❑ Before you begin writing, identify your audience and the purpose of the report

# TYPES OF REPORTS

❑ Computer forensics examiners are required to create different types of reports

❑ **Examination plan**

   ❑ What questions to expect when testifying

   ❑ Attorney uses the examination plan to guide you in your testimony

   ❑ You can propose changes to clarify or define information

   ❑ Helps your attorney learn the terms and functions used in computer forensics

**WITNESS EXAMINATION PLAN**

WITNESS:_Karen Stolz_____/Factors:_____Expert and Treating for P.

Direct Examination - Expected Testimony                     Objection/Rule/

Testimony on CV

Identity and Address Iowa Bureau of Criminal Investigation

Position (Current) Computer Forensic Examiner

Undergraduate   Iowa State University summa cum laude 1990 BS Computer Engineering

Summer Internship 1989 Des Moines Police Department

Neurology residency, University of Massachusetts MC 86-89

Chief resident in neurology, UM MC 88-89____explain neurology

Fellowship in Electroencephalography and Clinical Neurophysiology, UWMC-Seattle 89-90

Fellowship in Sleep Disorders Medicine, Univ. Michigan MC, 90-91

Academic Appointments

Lecturer, Dept of Computer Science, University of Iowa  1998-Current

Instructor, Iowa Police Academy, 1999-Current

Professional Society Certifications

P.E.   1999

CISSP 2001

Membership

American Society for Industrial Security

Publications

    Journal of the Iowa State Bar Association, May 1999,  "Computer Forensics on Raid Servers-Testifying to a Reasonable Certainty"

How many systems have you conducted forensic examination on?

What is your relationship to the Plaintiff?   Retained by his attorney to examine the hard drive of his computer for all financial records.  I have never actually met or talked with Mr. Smith.

How long did it take you conduct this examination?

What types of files were you looking for?   Why those file types?   Where did you find those file types?

What condition were the files in?

What is your opinion as to the cause of that condition?

Can you say for a reasonable certainty that the financial data files were deleted intentionally?  Yes.

Are you able to state to a reasonable certainty who deleted the financial data files?  Yes.

What is your fee for examining the hard drive, preparing a report and testifying?

Cross Examination - Expected Testimony

How many times have you worked for Mr. Sawyer as an expert witness?  I've had 16 contracts as consulting expert or expert witness.

Have you ever previously testified that overwrite utilities are not 100% reliable?  Yes, but that was in 1994 and utilities are so far as I can tell 100% reliable today.

**Figure 14-1**   A sample examination plan

# TYPES OF REPORTS (CONTINUED)

- ❑ Verbal report
    - ❑ Less structured
    - ❑ Attorneys cannot be forced to release verbal reports
    - ❑ Preliminary report
    - ❑ Addresses areas of investigation yet to be completed
        - ❑ Tests that have not been concluded
        - ❑ Interrogatories
        - ❑ Document production
        - ❑ Depositions

# TYPES OF REPORTS (CONTINUED)

❑ Written report

    ❑ Affidavit or declaration

    ❑ Limit what you write and pay attention to details

        ❑ Include thorough documentation and support of what you write

# GUIDELINES FOR WRITING REPORTS

- ❑ Hypothetical questions based on factual evidence
  - ❑ Less favored today
  - ❑ Guide and support your opinion
  - ❑ Can be abused and overly complex

- ❑ Opinions based on knowledge and experience

- ❑ Exclude from hypothetical questions
  - ❑ Facts that can change, cannot be used, or are not relevant to your opinion

# GUIDELINES FOR WRITING REPORTS (CONTINUED)

- As an expert witness, you may testify to an opinion, or conclusion, if four basic conditions are met:
  - Opinion, inferences, or conclusions depend on special knowledge or skills
  - Expert should qualify as a true expert
  - Expert must testify to a certain degree of certainty
  - Experts must describe facts on which their opinions are based, or they must testify to a hypothetical question

# WHAT TO INCLUDE IN WRITTEN PRELIMINARY REPORTS

- ❑ Anything you write down as part of your examination for a report
    - ❑ Subject to discovery from the opposing attorney
- ❑ Considered **high-risk documents**
- ❑ **Spoliation**
    - ❑ Destroying the report could be considered destroying or concealing evidence
- ❑ Include the same information as in verbal reports

# WHAT TO INCLUDE IN WRITTEN PRELIMINARY REPORTS (CONTINUED)

❑ Additional items to include in your report:

 ❑ Summarize your billing to date and estimate costs to complete the effort

 ❑ Identify the tentative conclusion (rather than the preliminary conclusion)

 ❑ Identify areas for further investigation and obtain confirmation from the attorney on the scope of your examination

# REPORT STRUCTURE

- ❑ **Structure**
  - ❑ Abstract
  - ❑ Table of contents
  - ❑ Body of report
  - ❑ Conclusion
  - ❑ References
  - ❑ Glossary
  - ❑ Acknowledgements
  - ❑ Appendixes

# WRITING REPORTS CLEARLY

- ☐ Consider
  - ☐ Communicative quality
  - ☐ Ideas and organization
  - ☐ Grammar and vocabulary
  - ☐ Punctuation and spelling

- ☐ Lay out ideas in logical order

- ☐ Build arguments piece by piece

- ☐ Group related ideas and sentences into paragraphs
  - ☐ Group paragraphs into sections

# WRITING REPORTS CLEARLY (CONTINUED)

- ❑ Avoid jargon, slang, and colloquial terms

- ❑ Define technical terms
  - ❑ Consider your audience

- ❑ Consider writing style
  - ❑ Use a natural language style
  - ❑ Avoid repetition and vague language
  - ❑ Be precise and specific
  - ❑ Use active rather than passive voice
  - ❑ Avoid presenting too many details and personal observations

- ❑ Include signposts
  - ❑ Draw reader's attention to a point

# DESIGNING THE LAYOUT AND PRESENTATION OF REPORTS

- ❑ Decimal numbering structure
  - ❑ Divides material into sections
  - ❑ Readers can scan heading
  - ❑ Readers see how parts relate to each other

- ❑ Legal-sequential numbering
  - ❑ Used in pleadings
  - ❑ Roman numerals represent major aspects
  - ❑ Arabic numbers are supporting information

# DESIGNING THE LAYOUT AND PRESENTATION OF REPORTS (CONTINUED)

- ❑ Providing supporting material
  - ❑ Use material such as figures, tables, data, and equations to help tell the story as it unfolds

- ❑ Formatting consistently
  - ❑ How you format text is less important than being consistent in applying formatting

- ❑ Explaining examination and data collection methods
  - ❑ Explain how you studied the problem, which should follow logically from the purpose of the report

# DESIGNING THE LAYOUT AND PRESENTATION OF REPORTS (CONTINUED)

❑ Including calculations
  ❑ If you use any hashing algorithms, be sure to give the common name

❑ Providing for uncertainty and error analysis
  ❑ Protect your credibility

❑ Explaining results and conclusions
  ❑ Explain your findings, using subheadings to divide the discussion into logical parts
  ❑ Save broader generalizations and summaries for the report's conclusion

# DESIGNING THE LAYOUT AND PRESENTATION OF REPORTS (CONTINUED)

❑ Providing references
  ❑ Cite references by author's last name and year of publication
  ❑ Follow a standard format

❑ Including appendixes
  ❑ You can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits
  ❑ Arrange them in the order referred to in the report
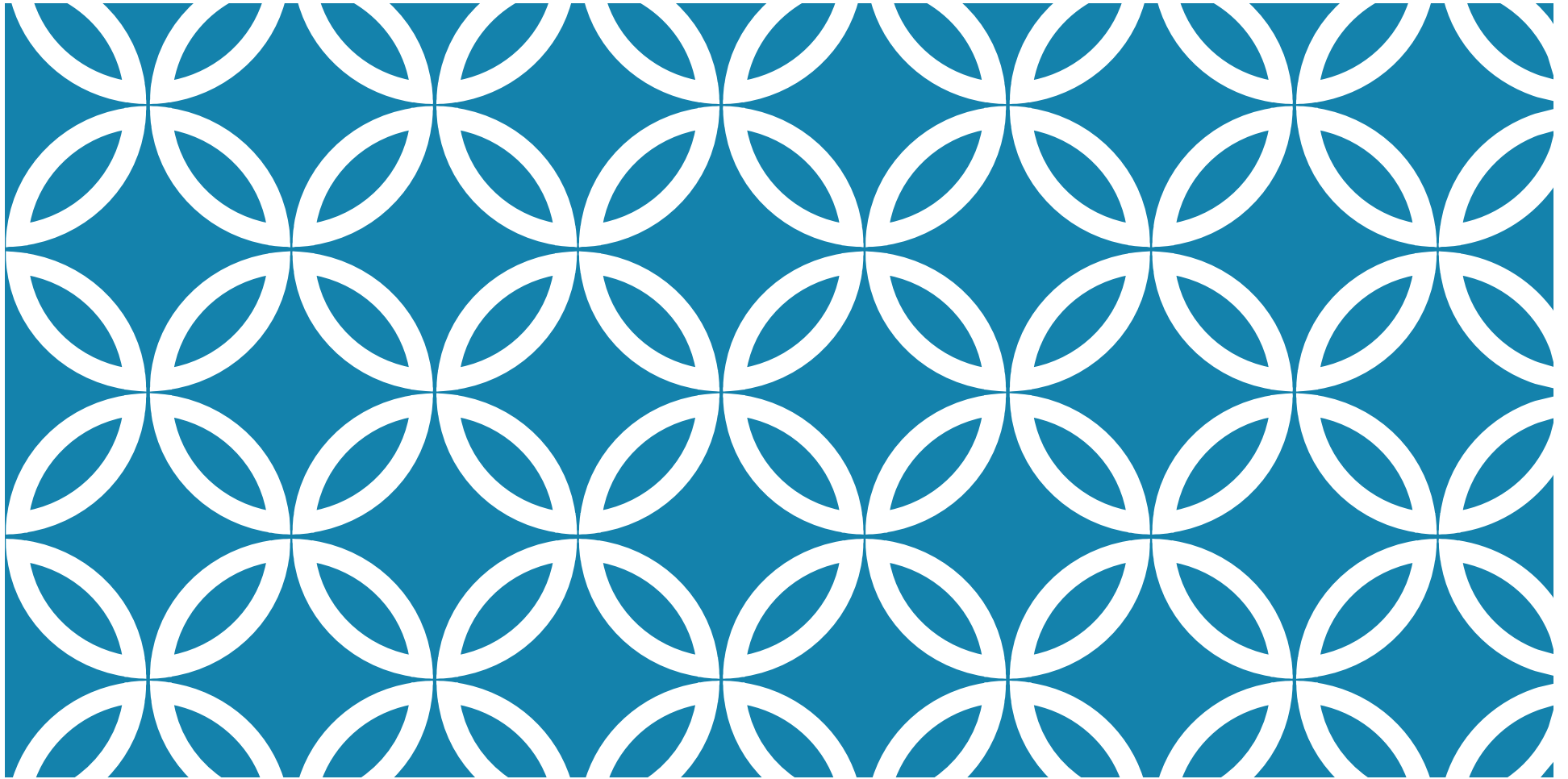
# GENERATING REPORT FINDINGS WITH FORENSICS SOFTWARE TOOLS

# GENERATING REPORT FINDINGS WITH FORENSICS SOFTWARE TOOLS
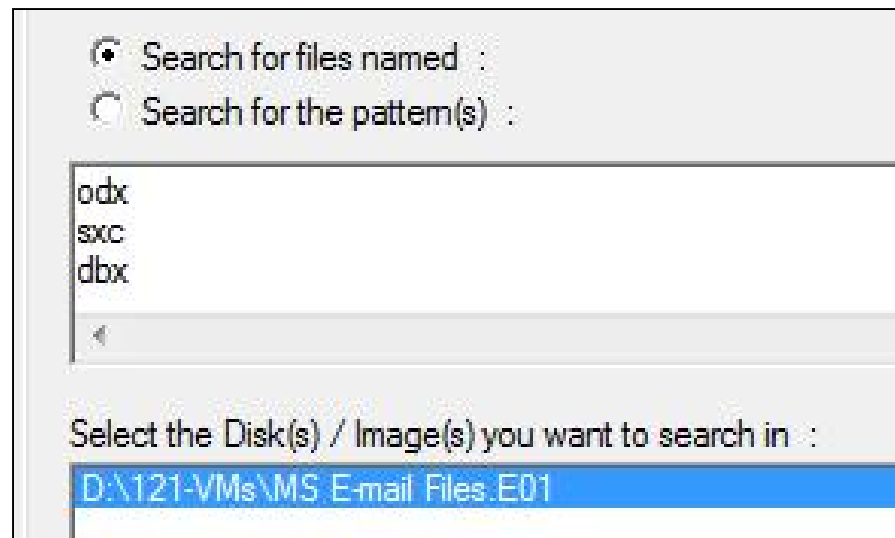
❑ Forensics tools generate reports when performing analysis

❑ Report formats
  ❑ Plaintext
  ❑ Word processor
  ❑ HTML format

# USING PRODISCOVER BASIC TO GENERATE REPORTS

❑ Create a new project

❑ Add an image file to the project

❑ Search for file extensions

# SEARCHING FOR FILE EXTENSIONS

# USING PRODISCOVER BASIC TO GENERATE REPORTS (CONTINUED)
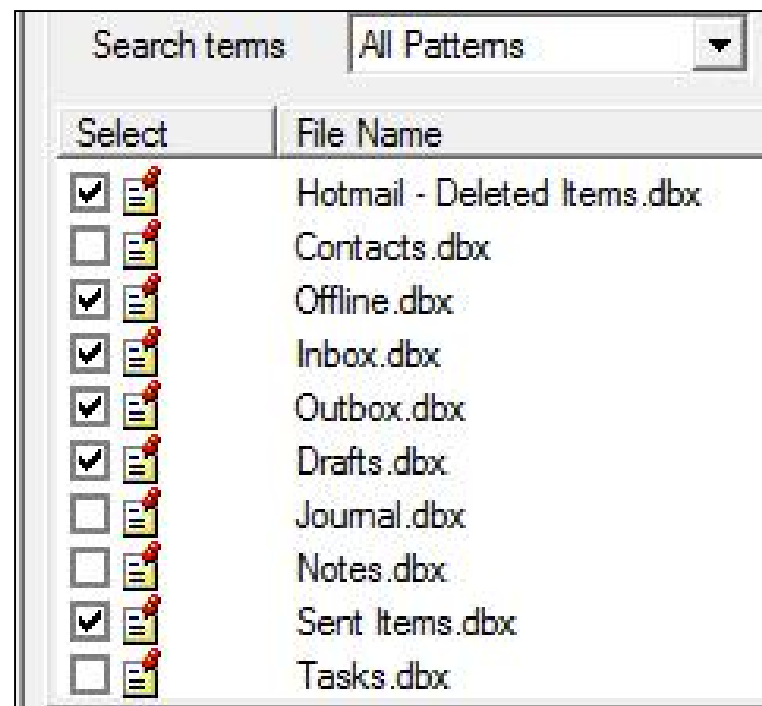
# USING FTK DEMO TO GENERATE REPORTS

❑ Create a new case

❑ Add evidence to the case

❑ Analyze evidence with FTK
   ❑ Look for image files
   ❑ Locate encrypted files
   ❑ Search for specific keywords
      ❑ Indexed search
      ❑ Live search

# USING FTK DEMO TO GENERATE REPORTS

❑ Create bookmarks

❑ Generate a report from your bookmarks