AUDIT: Automated Disk Investigation Toolkit

Umit Karabiyik

Department of Computer Science
Florida State University

September 19, 2014
Outline

- Introduction & Motivation
- Related Work
- AUDIT: Automated Disk Investigation Toolkit
- Testing AUDIT
- Conclusion & Future Work

Outline

- Introduction & Motivation
- Related Work
  - AUDIT: Automated Disk Investigation Toolkit
  - Testing AUDIT
- Conclusion & Future Work
Outline

- Introduction & Motivation
- Related Work
- AUDIT: Automated Disk Investigation Toolkit
  - Testing AUDIT
  - Conclusion & Future Work
Outline

- Introduction & Motivation
- Related Work
- AUDIT: Automated Disk Investigation Toolkit
- Testing AUDIT
- Conclusion & Future Work
Outline

- Introduction & Motivation
- Related Work
- AUDIT: Automated Disk Investigation Toolkit
- Testing AUDIT
- Conclusion & Future Work
Complexity and Learning

**Complexity** arises due to wide variety and availability of forensic investigation tools.

- How do I properly use these tools?
- When/Where can I effectively use them?
- How can I configure/parameterize them for a purpose?

Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).

Today's tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Introduction & Motivation

- Complexity and Learning

- **Complexity** arises due to wide variety and availability of forensic investigation tools.
  - How do I properly use these tools?
  - When/Where can I effectively use them?
  - How can I configure/parameterize them for a purpose?

- Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).

- Today’s tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Introduction & Motivation

- Complexity and Learning

- **Complexity** arises due to wide variety and availability of forensic investigation tools.
  - How do I properly use these tools?
    - When/Where can I effectively use them?
    - How can I configure/parameterize them for a purpose?

- Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).

- Today’s tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Complexity and Learning

**Complexity** arises due to wide variety and availability of forensic investigation tools.

- How do I properly use these tools?
- When/Where can I effectively use them?
- How can I configure/parameterize them for a purpose?

Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).

Today’s tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Complexity and Learning

**Complexity** arises due to wide variety and availability of forensic investigation tools.
- How do I properly use these tools?
- When/Where can I effectively use them?
- How can I configure/parameterize them for a purpose?

Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).

Today’s tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Complexity and Learning

**Complexity** arises due to wide variety and availability of forensic investigation tools.

- How do I properly use these tools?
- When/Where can I effectively use them?
- How can I configure/parameterize them for a purpose?

Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).

Today’s tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Introduction & Motivation

- Complexity and Learning
- **Complexity** arises due to wide variety and availability of forensic investigation tools.
  - How do I properly use these tools?
  - When/Where can I effectively use them?
  - How can I configure/parameterize them for a purpose?
- Forensic examiners might have any level of IT background and technical expertise (Hibshi et al., 2011).
- Today’s tools are not user friendly and require domain specific knowledge (Bebee, 2009) (Hibshi et al., 2011).
Figure 1: Output of a command line tool `mmls`. 

```
utk@umit-VB:/Desktop/diskimages$ mmls ext-part-test-2.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

<table>
<thead>
<tr>
<th>Slot</th>
<th>Start</th>
<th>End</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0000000000</td>
<td>0000000000</td>
<td>0000000001</td>
<td>Primary Table (#0)</td>
</tr>
<tr>
<td>01</td>
<td>0000000000</td>
<td>0000000062</td>
<td>0000000063</td>
<td>Unallocated</td>
</tr>
<tr>
<td>02</td>
<td>00:00</td>
<td>0000000063</td>
<td>00000052415</td>
<td>DOS FAT16 (0x04)</td>
</tr>
<tr>
<td>03</td>
<td>00:01</td>
<td>0000052416</td>
<td>0000104831</td>
<td>DOS FAT16 (0x04)</td>
</tr>
<tr>
<td>04</td>
<td>00:02</td>
<td>0000104832</td>
<td>0000157247</td>
<td>DOS FAT16 (0x04)</td>
</tr>
<tr>
<td>05</td>
<td>000157248</td>
<td>0000312479</td>
<td>0000155232</td>
<td>DOS Extended (0x05)</td>
</tr>
<tr>
<td>06</td>
<td>000157248</td>
<td>0000157248</td>
<td>0000000001</td>
<td>Extended Table (#1)</td>
</tr>
<tr>
<td>07</td>
<td>000157248</td>
<td>0000157248</td>
<td>0000000063</td>
<td>Unallocated</td>
</tr>
<tr>
<td>08</td>
<td>01:00</td>
<td>0000157311</td>
<td>0000209663</td>
<td>DOS FAT16 (0x04)</td>
</tr>
<tr>
<td>09</td>
<td>01:00</td>
<td>0000209664</td>
<td>0000209726</td>
<td>Unallocated</td>
</tr>
<tr>
<td>10</td>
<td>01:01</td>
<td>0000209727</td>
<td>0000262079</td>
<td>DOS FAT16 (0x04)</td>
</tr>
<tr>
<td>11</td>
<td>000262080</td>
<td>0000312479</td>
<td>000052353</td>
<td>DOS Extended (0x05)</td>
</tr>
<tr>
<td>12</td>
<td>000262080</td>
<td>0000262080</td>
<td>0000000001</td>
<td>Extended Table (#2)</td>
</tr>
<tr>
<td>13</td>
<td>000262080</td>
<td>0000262142</td>
<td>0000000063</td>
<td>Unallocated</td>
</tr>
<tr>
<td>14</td>
<td>02:00</td>
<td>0000262143</td>
<td>0000312479</td>
<td>DOS FAT16 (0x06)</td>
</tr>
</tbody>
</table>
```
Learning arises because learning is necessary even for IT experts for target disk.

- Necessary to know details of the digital target.
- People in digital forensics area would like to work with data on target w/o having a deep and specific knowledge (Garfinkel, 2009).
Learning arises because learning is necessary even for IT experts for target disk.

- Necessary to know details of the digital target.
- People in digital forensics area would like to work with data on target w/o having a deep and specific knowledge (Garfinkel, 2009).
Learning arises because learning is necessary even for IT experts for target disk.

- Necessary to know details of the digital target.
- People in digital forensics area would like to work with data on target w/o having a deep and specific knowledge (Garfinkel, 2009).
Figure 2: Digital disk warrens (Berghel et al., 2006)
**Solution:** Taking long training sessions both on tool usage and also on digital targets (%68 + %31) (Hibshi et al., 2011).
**Proposed Solution**

- **AUDIT: Automated Disk Investigation Toolkit**
  - Designed to support configuration, parameterization and integration of open source tools
  - Embedded expert system and knowledge base
Proposed Solution

- **AUDIT**: Automated Disk Investigation Toolkit
- Designed to support configuration, parameterization and integration of open source tools
- Embedded expert system and knowledge base
**Proposed Solution**

- **AUDIT: Automated Disk Investigation Toolkit**
- Designed to support configuration, parameterization and integration of open source tools
- Embedded expert system and knowledge base
Expert System

Source of image: http://www.igcseict.info/theory/7.2/expert/
Related Work

- Expert systems with decision tree and fuzzy logic are used in order to detect network anomalies and certain attacks.
- The Open Computer Forensics Architecture (OCFA)
- The Digital Forensics Framework
- Fiwalk
- MultiAgent Digital Investigation toolKit (MADIK)
Related Work

- Expert systems with decision tree and fuzzy logic are used in order to detect network anomalies and certain attacks.

- The Open Computer Forensics Architecture (OCFA)
  - The Digital Forensics Framework
  - Fiwalk
  - MultiAgent Digital Investigation toolKit (MADIK)
Expert systems with decision tree and fuzzy logic are used in order to detect network anomalies and certain attacks.

- The Open Computer Forensics Architecture (OCFA)
- The Digital Forensics Framework
- Fiwalk
- MultiAgent Digital Investigation toolKit (MADIK)
Related Work

- Expert systems with decision tree and fuzzy logic are used in order to detect network anomalies and certain attacks.
- The Open Computer Forensics Architecture (OCFA)
- The Digital Forensics Framework
- Fiwalk
- MultiAgent Digital Investigation toolKit (MADIK)
Related Work

- Expert systems with decision tree and fuzzy logic are used in order to detect network anomalies and certain attacks.
- The Open Computer Forensics Architecture (OCFA)
- The Digital Forensics Framework
- Fiwalk
- MultiAgent Digital Investigation toolKit (MADIK)
None of this work is focused on assisting examiners during the examination and analysis phases of the investigation by providing an automated and reasonably expert system.

These systems do not support general open source tool integration but rather integrate some task specific modules.
Related Work

- None of this work is focused on assisting examiners during the examination and analysis phases of the investigation by providing an automated and reasonably expert system.
- These systems do not support general open source tool integration but rather integrate some task specific modules.
AUDIT: Automated Disk Investigation Toolkit

- Designed with the goal that very little technical knowledge would be required of the users.
- AUDIT is able to integrate and configure the tools automatically for the purpose of both general and specific investigations.
- Searching the disk for evidence in graphic files, emails, documents in “hidden” locations.
- Detailed search for items such as credit card and social security numbers is also done.
AUDIT: Automated Disk Investigation Toolkit

- Designed with the goal that very little technical knowledge would be required of the users.
- AUDIT is able to integrate and configure the tools automatically for the purpose of both general and specific investigations.
- Searching the disk for evidence in graphic files, emails, documents in “hidden” locations.
- Detailed search for items such as credit card and social security numbers is also done.
AUDIT: Automated Disk Investigation Toolkit

- Designed with the goal that very little technical knowledge would be required of the users.
- AUDIT is able to integrate and configure the tools automatically for the purpose of both general and specific investigations.
- Searching the disk for evidence in graphic files, emails, documents in “hidden” locations.
- Detailed search for items such as credit card and social security numbers is also done.
AUDIT: Automated Disk Investigation Toolkit

- Designed with the goal that very little technical knowledge would be required of the users.
- AUDIT is able to integrate and configure the tools automatically for the purpose of both general and specific investigations.
- Searching the disk for evidence in graphic files, emails, documents in “hidden” locations.
- Detailed search for items such as credit card and social security numbers is also done.
High-level design

- **AUDIT consists of three components:**
  - a database of investigative tasks and tools,
  - a knowledge base with constructs defining rules and facts,
  - a core engine (expert system).

- **Domain specific knowledge is designed and implemented:**
  - when configuration and/or parameterization of the tools is needed
  - when tools integration is needed
High-level design

- **AUDIT consists of three components:**
  - a database of investigative tasks and tools,
  - a knowledge base with constructs defining rules and facts,
  - a core engine (expert system).

- **Domain specific knowledge is designed and implemented:**
  - when configuration and/or parameterization of the tools is needed
  - when tools integration is needed
High-level design

• **AUDIT** consists of three components:
  - a database of investigative tasks and tools,
  - a knowledge base with constructs defining rules and facts,
  - a core engine (expert system).

• Domain specific knowledge is designed and implemented:
  - when configuration and/or parameterization of the tools is needed
  - when tools integration is needed
High-level design

- **AUDIT** consists of three components:
  - a database of investigative tasks and tools,
  - a knowledge base with constructs defining rules and facts,
  - a core engine (expert system).

- Domain specific knowledge is designed and implemented:
  - when configuration and/or parameterization of the tools is needed
  - when tools integration is needed
High-level design

• AUDIT consists of three components:
  • a database of investigative tasks and tools,
  • a knowledge base with constructs defining rules and facts,
  • a core engine (expert system).

• Domain specific knowledge is designed and implemented:
  1. when configuration and/or parameterization of the tools is needed
  2. when tools integration is needed
High-level design

- **AUDIT** consists of three components:
  - a database of investigative tasks and tools,
  - a knowledge base with constructs defining rules and facts,
  - a core engine (expert system).

- Domain specific knowledge is designed and implemented:
  1. when configuration and/or parameterization of the tools is needed
  2. when tools integration is needed
AUDIT consists of three components:
- a database of investigative tasks and tools,
- a knowledge base with constructs defining rules and facts,
- a core engine (expert system).

Domain specific knowledge is designed and implemented:
1. when configuration and/or parameterization of the tools is needed
2. when tools integration is needed
AUDIT Database

- **Tools and Knowledge Tables**
  - **Tools Table** maintains information regarding:
    - Specifications of tools
    - Configuration and parameterization of tools
  - **Knowledge Table** maintains information regarding:
    - Investigative tasks
AUDIT Database

- Tools and Knowledge Tables
  - **Tools Table** maintains information regarding:
    - Specifications of tools
    - Configuration and parameterization of tools
  - **Knowledge Table** maintains information regarding:
    - Investigative tasks
AUDIT Database

- **Tools and Knowledge Tables**
  - **Tools Table** maintains information regarding:
    - Specifications of tools
    - Configuration and parameterization of tools
  - **Knowledge Table** maintains information regarding:
    - Investigative tasks
AUDIT Database

- Tools and Knowledge Tables
  - **Tools Table** maintains information regarding:
    - Specifications of tools
    - Configuration and parameterization of tools
  - **Knowledge Table** maintains information regarding:
    - Investigative tasks
AUDIT Database

- Tools and Knowledge Tables
  - **Tools Table** maintains information regarding:
    - Specifications of tools
    - Configuration and parameterization of tools
  - **Knowledge Table** maintains information regarding:
    - Investigative tasks
AUDIT Database

- **Tools and Knowledge Tables**
  - **Tools Table** maintains information regarding:
    - Specifications of tools
    - Configuration and parameterization of tools
  - **Knowledge Table** maintains information regarding:
    - Investigative tasks
Figure 3: The tools table in the AUDIT database
AUDIT Core Engine

- Creates new rules and facts as needed
- Links investigative tasks and tools
- Configuration / Parameterization of tools
- Integration of tools
AUDIT Core Engine

- Creates new rules and facts as needed
- Links investigative tasks and and tools
  - Configuration / Parameterization of tools
  - Integration of tools
AUDIT Core Engine

- Creates new rules and facts as needed
- Links investigative tasks and tools
- Configuration / Parameterization of tools
- Integration of tools
AUDIT Core Engine

- Creates new rules and facts as needed
- Links investigative tasks and tools
- Configuration / Parameterization of tools
- Integration of tools
AUDIT Knowledge Base

- Contains pre-defined rules and facts
- Open source expert system tool CLIPS is used.
- Create rule and object based expert system and represent expert’s technical knowledge
- Rule-based programming is used
AUDIT Knowledge Base

- Contains pre-defined rules and facts
- Open source expert system tool CLIPS is used.
- Create rule and object based expert system and represent expert’s technical knowledge
- Rule-based programming is used
AUDIT Knowledge Base

- Contains pre-defined rules and facts
- Open source expert system tool CLIPS is used.
- Create rule and object based expert system and represent expert’s technical knowledge
- Rule-based programming is used
AUDIT Knowledge Base

- Contains pre-defined rules and facts
- Open source expert system tool CLIPS is used.
- Create rule and object based expert system and represent expert’s technical knowledge
- Rule-based programming is used
Building the knowledge base

- Updated with new rules and facts during the investigation

- Input from User

- Running tools to collect data

- Data converted to facts
  - New rules created

- Knowledge base updated
Building the knowledge base for AUDIT

(defrule determine-investigator-level ""
    (declare (salience 10))
    (not (investigator is ?))

=>
    (if (yes-or-no-p "Are you an expert (yes/no)? ")
then (assert (investigator is expert))
    (if (yes-or-no-p "Do you need help (yes/no)? ")
then
        (assert (expert needs help))
        (assert (determine disk-layout needed))
        (assert (extracting partitions from disk needed))
else
    (assert (expert needs no-help))
    (assert (self usage mode on))
    (assert (provide available tool list to user)))
else (assert (investigator is non-expert))
    (assert (non-expert needs help))
    (assert (determine disk-layout needed))
    (assert (extracting partitions from disk needed)))

Figure 4: Simple example of a CLIPS rule in AUDIT
Building the knowledge base for AUDIT

(defrule determine-investigator-level ""
  (declare (salience 10))
  (not (investigator is ?))
  =>
  (if (yes-or-no-p "Are you an expert (yes/no)? ")
    then (assert (investigator is expert))
    (if (yes-or-no-p "Do you need help (yes/no)? ")
      then
      (assert (expert needs help))
      (assert (determine disk-layout needed))
      (assert (extracting partitions from disk needed))
    else
    (assert (expert needs no-help))
    (assert (self usage mode on))
    (assert (provide available tool list to user)))
  else (assert (investigator is non-expert))
  (assert (non_expert needs help))
  (assert (determine disk-layout needed))
  (assert (extracting partitions from disk needed)))

Figure 5: Simple example of a CLIPS rule in AUDIT
Building the knowledge base for AUDIT

In AUDIT we define two different levels of knowledge:

1. Investigator Level Knowledge Base
2. Tools Level Knowledge Base
In AUDIT we define two different levels of knowledge:

1. Investigator Level Knowledge Base
2. Tools Level Knowledge Base
In AUDIT we define two different levels of knowledge:

1. Investigator Level Knowledge Base
2. Tools Level Knowledge Base
Investigator Level Knowledge Base: Relates to the technical skill level of the user.

(investigator is non-expert)  (run tsk_recover for allocated-space)
(non_expert needs help)  (run tsk_recover for unallocated-space)
(configuration needed)  (run blkls for slack-space)

==>
(runs scalp for data-carving)
(configures scalp for graphic-files)
(configures scalp for document-files)
(configures mmc for smart-carving)
Tools Level Knowledge Base

**Tools Level Knowledge Base**: Relates to usage and integration of the tools.

```lisp
(defrule credit-card-search 
  (image-file-path is ?imagePath) 
  (output-path is ?outputPath) 
  (investigative-task is ?task) 
  (investigation-type is ccsearch) 
  =>
  (printout t "Find_SSNs is running on the disk!" crlf) 
  (mount-disk-image ?imagePath ?outputPath ?task) 
  (run-blkls ?imagePath ?outputPath ?task) 
  (run-strings ?imagePath ?outputPath ?task) 
  (run-tsk_recover ?imagePath ?outputPath ?task) 
  (run-Find_SSNs ?imagePath ?outputPath ?task) 
  (assert (ccsearch performed)))
```
Open source tools used in AUDIT:

- tsk_recover is used for allocated and unallocated space analysis.
- blkls is used to extract data from slack space.
- mmls is used to analyze the input disk structure and layout.
- scalpel is used to carve out files from the input disk.
- dd is used to divide input disk into partitions.
- strings is used to filter data in the slack space.
- Find_SSNs is used to find SSN and credit card numbers.
Open source tools used in AUDIT:
- **tsk_recover** is used for allocated and unallocated space analysis.
- **blkls** is used to extract data from slack space.
- **mmls** is used to analyze the input disk structure and layout.
- **scalpel** is used to carve out files from the input disk.
- **dd** is used to divide input disk into partitions.
- **strings** is used to filter data in the slack space.
- **Find_SSNs** is used to find SSN and credit card numbers.
Open source tools used in AUDIT:

- **tsk_recover** is used for allocated and unallocated space analysis.
- **blkls** is used to extract data from slack space.
- **mmls** is used to analyze the input disk structure and layout.
- **scalpel** is used to carve out files from the input disk.
- **dd** is used to divide input disk into partitions.
- **strings** is used to filter data in the slack space.
- **Find_SSNS** is used to find SSN and credit card numbers.
Open source tools used in AUDIT:

- **tsk_recover** is used for allocated and unallocated space analysis.
- **blkls** is used to extract data from slack space.
- **mmls** is used to analyzed the input disk structure and layout.
- **scalpel** is used to carve out files from the input disk.
- **dd** is used to divide input disk into partitions.
- **strings** is used to filter data in the slack space.
- **Find_SSNs** is used to find SSN and credit card numbers.
Open source tools used in AUDIT:

- **tsk_recover** is used for allocated and unallocated space analysis.
- **blkls** is used to extract data from slack space.
- **mmls** is used to analyzed the input disk structure and layout.
- **scalpel** is used to carve out files from the input disk.
- **dd** is used to divide input disk into partitions.
- **strings** is used to filter data in the slack space.
- **Find_SSNs** is used to find SSN and credit card numbers.
Open source tools used in AUDIT:

- **tsk_recover** is used for allocated and unallocated space analysis.
- **blkls** is used to extract data from slack space.
- **mmls** is used to analyze the input disk structure and layout.
- **scalpel** is used to carve out files from the input disk.
- **dd** is used to divide input disk into partitions.
- **strings** is used to filter data in the slack space.
- **Find/ssns** is used to find SSN and credit card numbers.
Configuration, Parameterization and Integration

- Open source tools used in AUDIT:
  - **tsk_recover** is used for allocated and unallocated space analysis.
  - **blkls** is used to extract data from slack space.
  - **mmls** is used to analyzed the input disk structure and layout.
  - **scalpel** is used to carve out files from the input disk.
  - **dd** is used to divide input disk into partitions.
  - **strings** is used to filter data in the slack space.
  - **Find_SSNs** is used to find SSN and credit card numbers.
Configuration, Parameterization and Integration

- Open source tools used in AUDIT:
  - tsk_recover is used for allocated and unallocated space analysis.
  - blkls is used to extract data from slack space.
  - mmls is used to analyze the input disk structure and layout.
  - scalpel is used to carve out files from the input disk.
  - dd is used to divide input disk into partitions.
  - strings is used to filter data in the slack space.
  - Find_SSNs is used to find SSN and credit card numbers.
### The tools table in database

![The tools table in the AUDIT database](image)

**Figure 6:** The tools table in the AUDIT database
(evidence found no)
(run scalpel for data-carving)
(tsk_recover is unsuccessful)
(image-file-path is ?imagePath)
(output-path is ?outputPath)
(investigation-type is psearch)
(evidence found no)
(run scalpel for data-carving)
(tsk_recover is unsuccessful)
(image-file-path is ?imagePath)
(output-path is ?outputPath)
(investigation-type is psearch)

Feedback from user interaction
(evidence found no)
(run scalpel for data-carving)
(tsk_recover is unsuccessful)
(image-file-path is ?imagePath)
(output-path is ?outputPath)
(investigation-type is psearch)
Configuration, Parameterization and Integration

(evidence found no)
(run scalp for data-carving)
(tsk_recover is unsuccessful)
(image-file-path is ?imagePath)
(output-path is ?outputPath)
(investigation-type is psearch)

tool runs both on allocated and unallocated spaces
(evidence found no)
(run scalpel for data-carving)
(tsk_recover is unsuccessful)
(image-file-path is ?imagePath)
(output-path is ?outputPath)
(investigation-type is psearch)
(evidence found no)
(run scalpel for data-carving)
(tsk_recover is unsuccessful)
(image-file-path is ?imagePath)
(output-path is ?outputPath)
(investigation-type is psearch)

= TRUE

Scalpel run for data carving if all the above facts are in the knowledge base.
Working with AUDIT

AUDIT: Automated Disk Investigation Toolkit

What would you like to perform?
- Graphic Search
- Document Search
- Credit Card and SSN Search
- Email Search

Expertise Level
- Expert
- Non-Expert

Input Disk Image File
/home/utk/nps-2009-canon2-gen6.raw

Output Directory
/home/utk/case1

START
(defrule graphic-file-search "Graphic file search"
  (image-file-path is ?imagePath)
  (output-path is ?outputPath)
  ?falloc<- (investigation-type is graphSearch)
  =>
  (assert (search type is ?*searchType*))

(assert (start allocated space analysis))
(assert (start unallocated space analysis))
(assert (start slack space carver))
(assert (start data carver))
(assert (start mmc smart carver))
)

**Figure 7:** Initialization rule for graphic search.
Graphic Search

(defrule allocated-space-analysis-rule "Allocated space analysis is performed"
  ?faloc<- (start allocated space analysis)
  (image-file-path is ?imagePath)
  (output-path is ?outputPath)
  (search type is ?searchType*); this will be used for database connection
  (parameter for allocated space is ?parameter); gathered from the database
  =>

  ;; call function for allocated space analysis by tsk_recover
  (run_tsk_recover ?parameter ?imagePath ?outputPath)
  (retract ?faloc); remove the analysis fact
  (run_gui "Is there any interesting file for your investigation (yes/no)?")
  (while (= ?yesORno* 0)
    (bind ?dummy 0)
  ) ; infinite loop until we get response from user
)

Figure 8: Allocated space analysis for graphic search.
Figure 9: Popup showing files recovered from unallocated space
We developed AUDIT, an “intelligent assistant” to help expert and non-IT-expert investigators.

AUDIT contains an expert system and domain specific knowledge base.

AUDIT automatically configures, parameterizes and integrates some of the commonly used open source command line digital forensics tools.

AUDIT supports the investigator in conducting both general and specific investigative tasks.
We developed AUDIT, an “intelligent assistant” to help expert and non-IT-expert investigators.

AUDIT contains an expert system and domain specific knowledge base.

AUDIT automatically configures, parameterizes and integrates some of the commonly used open source command line digital forensics tools.

AUDIT supports the investigator in conducting both general and specific investigative tasks.
Conclusion

- We developed AUDIT, an “intelligent assistant” to help expert and non-IT-expert investigators.
- AUDIT contains an expert system and domain specific knowledge base.
- AUDIT automatically configures, parameterizes and integrates some of the commonly used open source command line digital forensics tools.
- AUDIT supports the investigator in conducting both general and specific investigative tasks.
We developed AUDIT, an “intelligent assistant” to help expert and non-IT-expert investigators.

AUDIT contains an expert system and domain specific knowledge base.

AUDIT automatically configures, parameterizes and integrates some of the commonly used open source command line digital forensics tools.

AUDIT supports the investigator in conducting both general and specific investigative tasks.
Future Work

- Augmenting the toolkit to collect knowledge about techniques and procedures used in an investigation.
- Incorporating the ability to rank the success of each tool
- Designing a model of learning tool specifications
- Adapting this tool to different environments (Mobile and Network)
- Being able to cover everything and possibly all places on target disk
Future Work

- Augmenting the toolkit to collect knowledge about techniques and procedures used in an investigation.
- Incorporating the ability to rank the success of each tool
  - Designing a model of learning tool specifications
  - Adapting this tool to different environments (Mobile and Network)
  - Being able to cover everything and possibly all places on target disk
Future Work

- Augmenting the toolkit to collect knowledge about techniques and procedures used in an investigation.
- Incorporating the ability to rank the success of each tool.
- Designing a model of learning tool specifications.
  - Adapting this tool to different environments (Mobile and Network).
  - Being able to cover everything and possibly all places on target disk.
Future Work

- Augmenting the toolkit to collect knowledge about techniques and procedures used in an investigation.
- Incorporating the ability to rank the success of each tool
- Designing a model of learning tool specifications
- Adapting this tool to different environments (Mobile and Network)
- Being able to cover everything and possibly all places on target disk
Future Work

- Augmenting the toolkit to collect knowledge about techniques and procedures used in an investigation.
- Incorporating the ability to rank the success of each tool
- Designing a model of learning tool specifications
- Adapting this tool to different environments (Mobile and Network)
- Being able to cover everything and possibly all places on target disk
Contact

Umit Karabiyik
Florida State University
karabiyi@cs.fsu.edu
850-212-4855


