Usability of Digital Forensics Tools

Hanan Hibshi

Timothy Vidas

Lorrie Cranor

Carnegie Mellon

CyLab **U**sable **P**rivacy and **S**ecurity Laboratory

http://cups.cs.cmu.edu/

Agenda

- Digital Forensics Tools: (Types, Users, Challenges)
- Sample investigative Scenario
- Motivation
- Our research methodology
- Results & analysis
- Conclusion
  - Usability Problems
  - Guidelines for tools developers
  - Future Work

Digital Forensics Tool - Introducation

- Digital devices always leave breadcrumbs: evidence
- Forensic tools help analyze digital evidence.
- Used for:
  - Debugging and data recovery
  - Criminal investigation

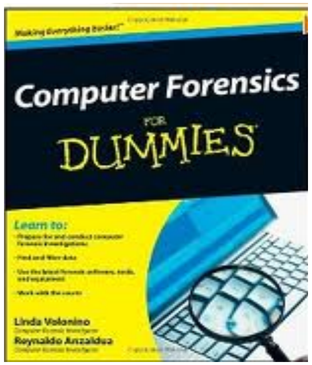
- Users:
  - Government Law enforcement personnel.
  - Private sector investigators.
  - Others: maintenance purposes, Hobbyists, Savvy criminals

Types of Tools

- Commercial vs. open source
  - http://www2.opensourceforensics.org/tools
  - http://www.forensicswiki.org/wiki/Tools
- Full-fledge platforms vs. specialized tools.
- Some examples:
  - FTK & Encase: commercial platforms, most common.
  - The Sleuth kit (TSK), Autopsy: by Brian Carrier
  - Others…

Why Usability of Forensics Tools?

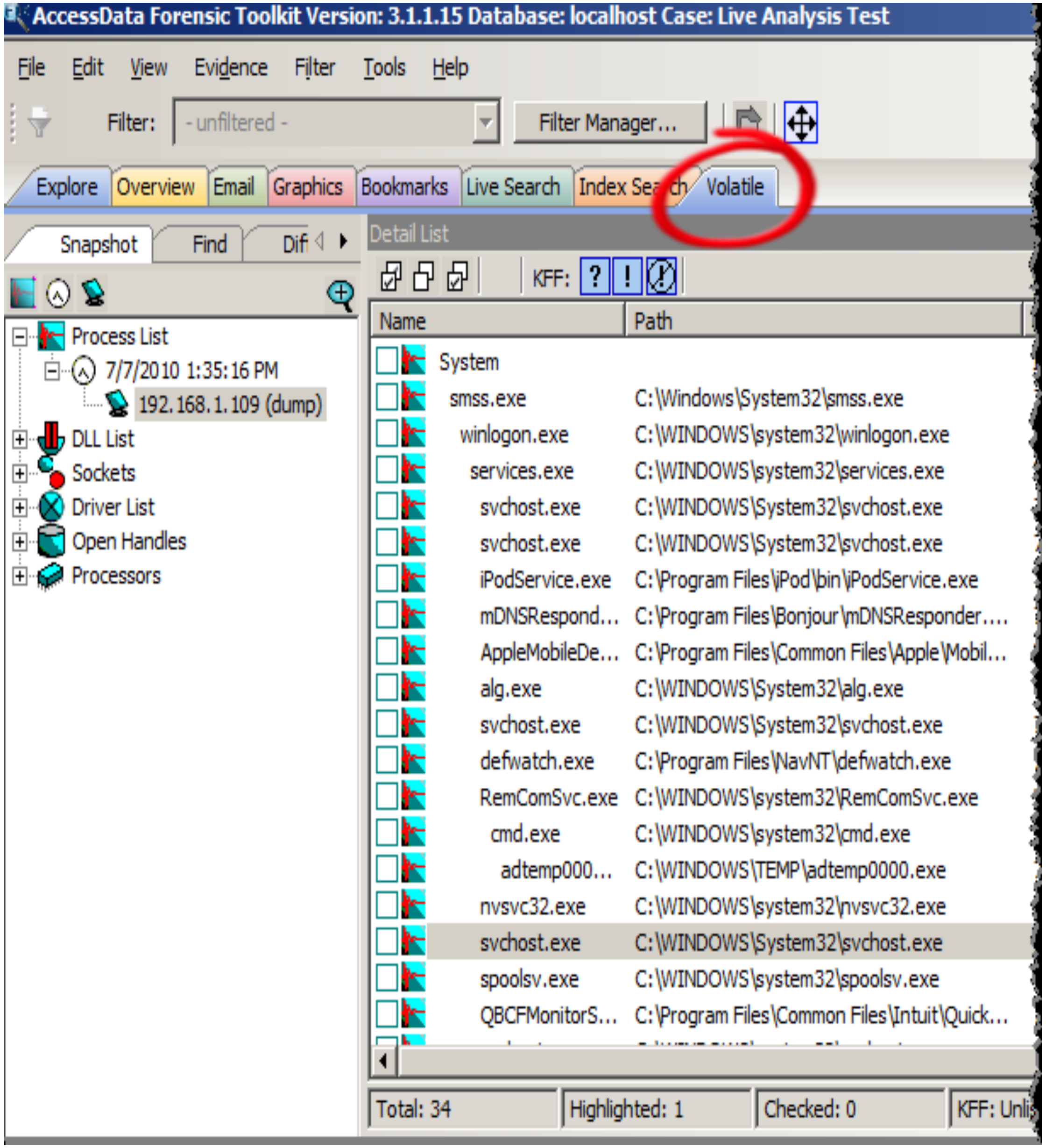
- A lot of training and education is required.
- Very low level computer systems concepts.
- Books and manuals:
  - huge in size
  - still not enough



- College level courses: in a number of universities.
- Ongoing training sessions for users.
- Users of these tools are not necessary interested in learning low-level concepts of technology.

FTK Interface

- Described by most forensics community as more friendly
- This GUI is for the FTK v3 that has many improvements over previous versions.
- Previewed in 2009 during HTCIA conference, released in 2010
- License: Standalone + 1 year subscription costs $3,835.00



AccessData Forensic Toolkit Version: 3.1.1.15 Database: localhost Case: Live Analysis Test

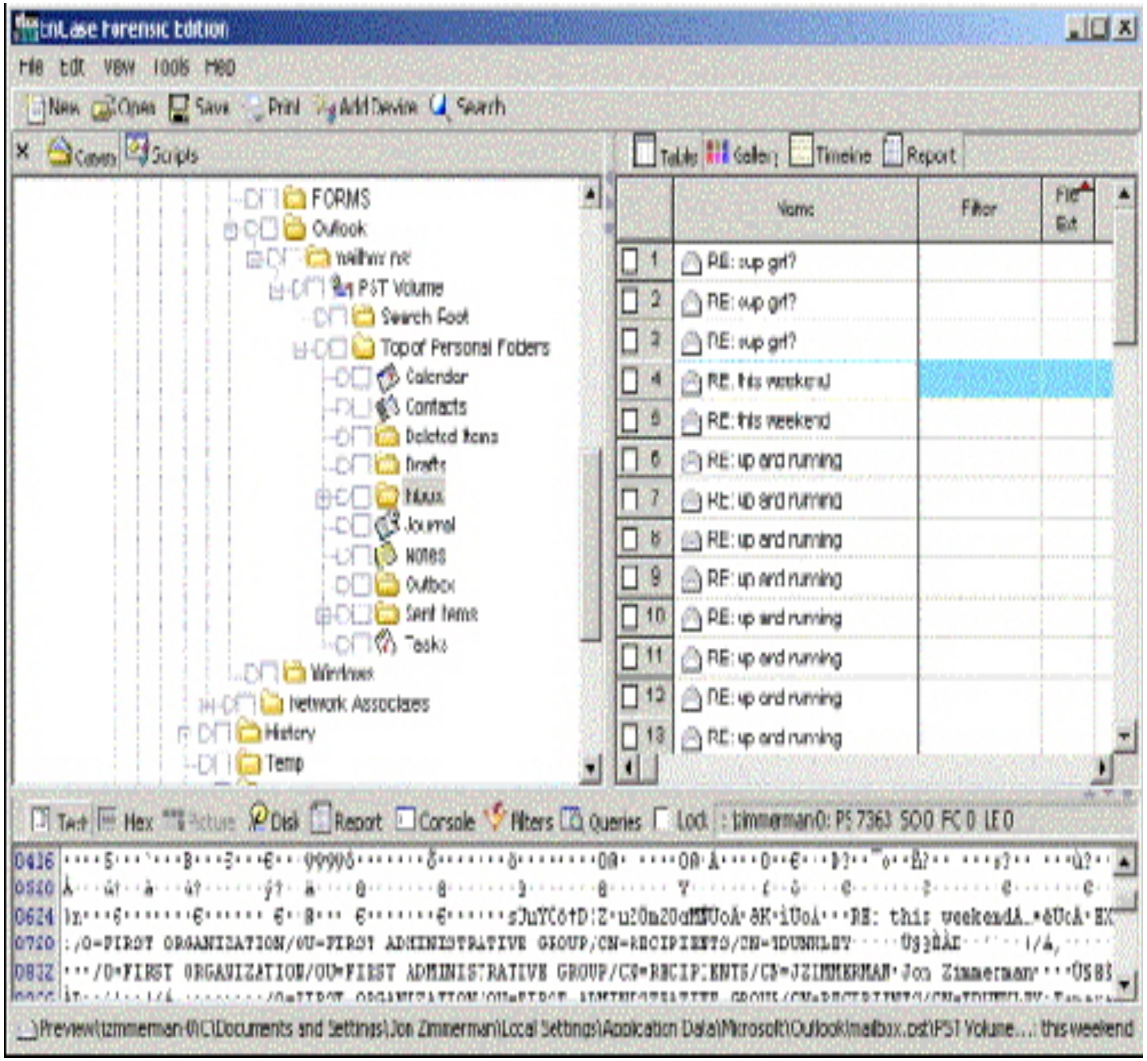
- Process List
  - 7/7/2010 1:35:16 PM
    - 192.168.1.109 (dump)
- DLL List
- Sockets
- Driver List
- Open Handles
- Processors

Name	Path
System	
smss.exe	C:\Windows\System32\smss.exe
winlogon.exe	C:\WINDOWS\system32\winlogon.exe
services.exe	C:\WINDOWS\system32\services.exe
svchost.exe	C:\WINDOWS\System32\svchost.exe
svchost.exe	C:\WINDOWS\System32\svchost.exe
iPodService.exe	C:\Program Files\iPod\bin\iPodService.exe
mDNSRespond...	C:\Program Files\Bonjour\mDNSResponder....
AppleMobileDe...	C:\Program Files\Common Files\Apple\Mobil...
alg.exe	C:\WINDOWS\System32\alg.exe
svchost.exe	C:\WINDOWS\System32\svchost.exe
defwatch.exe	C:\Program Files\NavNT\defwatch.exe
RemComSvc.exe	C:\WINDOWS\system32\RemComSvc.exe
cmd.exe	C:\WINDOWS\system32\cmd.exe
adtemp000...	C:\WINDOWS\TEMP\adtemp0000.exe
nvsvc32.exe	C:\WINDOWS\system32\nvsvc32.exe
svchost.exe	C:\WINDOWS\System32\svchost.exe
spoolsv.exe	C:\WINDOWS\system32\spoolsv.exe
QBCFMonitorS...	C:\Program Files\Common Files\Intuit\Quick...

Total: 34 | Highlighted: 1 | Checked: 0 | KFF: Unli

Encase Interface

- Less intuitive than FTK.
- Does stuff that users aren't usually familiar with.
- Very dense display of data.
- However, the program has some advanced functionality and the ability to add advanced scripts using Enscript scripting language.



	Name	Filter	File Ext
□ 1	RE: sup grl?		
□ 2	RE: sup grl?		
□ 3	RE: sup grl?		
□ 4	RE: this weekend		
□ 5	RE: this weekend		
□ 6	RE: up and running		
□ 7	RE: up and running		
□ 8	RE: up and running		
□ 9	RE: up and running		
□ 10	RE: up and running		
□ 11	RE: up and running		
□ 12	RE: up and running		
□ 13	RE: up and running		

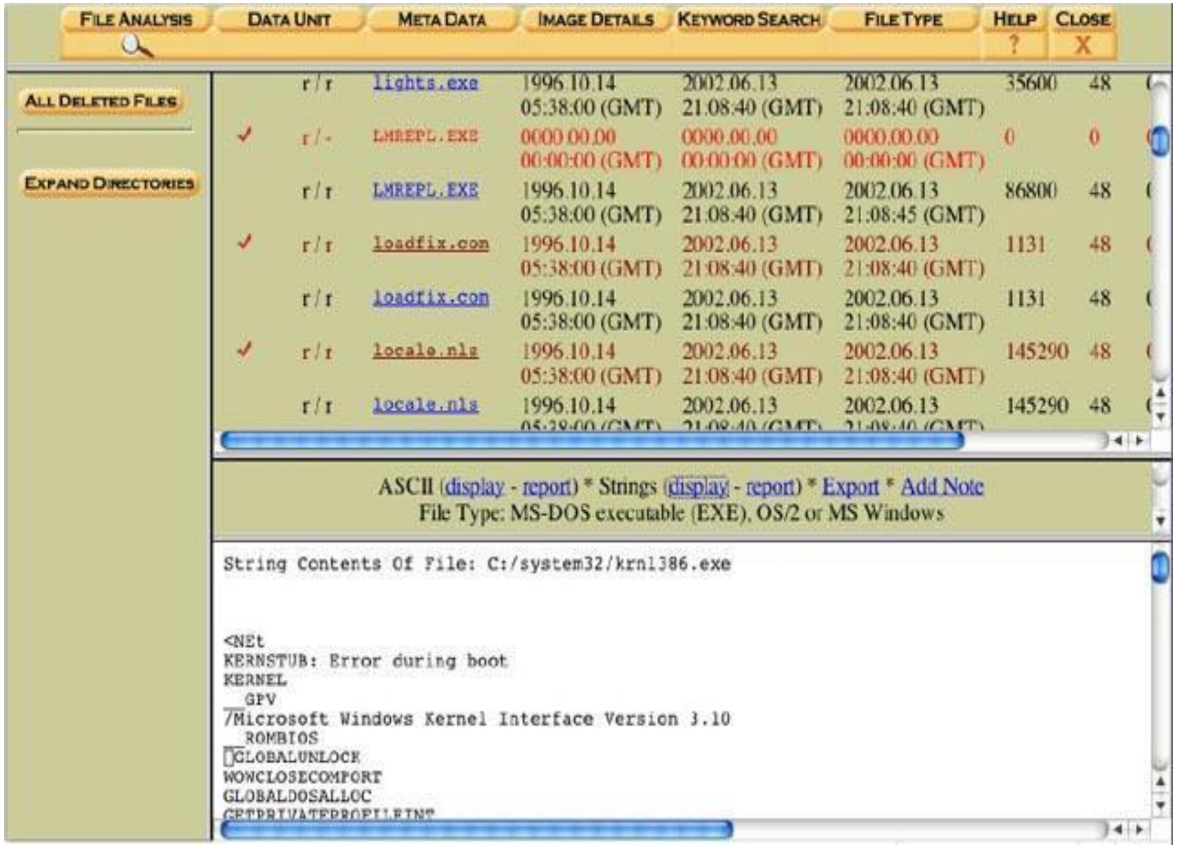
: jzimmerman0: PS 7363 SO 0 FO 0 LE 0

```
0624 ...RE: this weekend...
0720 :/O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=TDUNNLEY
0832 .../O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=JZIMMERMAN.Jon Zimmerman
```

Preview\jzimmerman-0\C\Documents and Settings\Jon Zimmerman\Local Settings\Application Data\Microsoft\Outlook\mailbox.pst\PST Volume...: this weekend

Open Source Interfaces

- Autopsy was meant to be the GUI for The Sleuth Kit, but its not helpful.
- Most open-source tools are command-line based.
- Intended to solve a problem that is hard to find with commercials frameworks.



	r / r	lights.exe	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	35600	48
✓	r / -	LMREPL.EXE	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0	0
	r / r	LMREPL.EXE	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:45 (GMT)	86800	48
✓	r / r	loadfix.com	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	1131	48
	r / r	loadfix.com	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	1131	48
✓	r / r	locale.nls	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	145290	48
	r / r	locale.nls	1996.10.14 05:38:00 (GMT)	2002.06.13 21:08:40 (GMT)	2002.06.13 21:08:40 (GMT)	145290	48

ASCII (display - report) * Strings (display - report) * Export * Add Note
File Type: MS-DOS executable (EXE), OS/2 or MS Windows

```
String Contents Of File: C:/system32/krnl386.exe



<NEt
KERNSTUB: Error during boot
KERNEL
  GPV
7Microsoft Windows Kernel Interface Version 3.10
  ROMBIOS
GLOBALUNLOCK
WONCLOSECOMPORT
GLOBALDOSALLOC
GETPRIVATEPROFILEINT
```

Sample Scenario: Picture Search

- Plug in the captured image.
- Check hashes.
  - Automatically done with Encase tools, not with others.
- Preprocessing can be done in advance in FTK case.
- Hashing every file / file signatures.
- Setting time zone.
- Time analysis.
- Check warrant limitations.
- Eliminate common system files with common hashes.
  - Again depends on platform.
- Apply filters.
- If in temporary internet files, do more investigation to prove it was downloaded.
- If no hits, check encryption/ steganography.

Our Study

- Examine these tools for usability problems by:
  - Interviews: 8 tools experts (done).
  - Surveys: 115 responses (done).
  - Heuristic evaluation: (in future publication)
  - User lab study: (in future publication)
- Results: guidelines to design these tools.

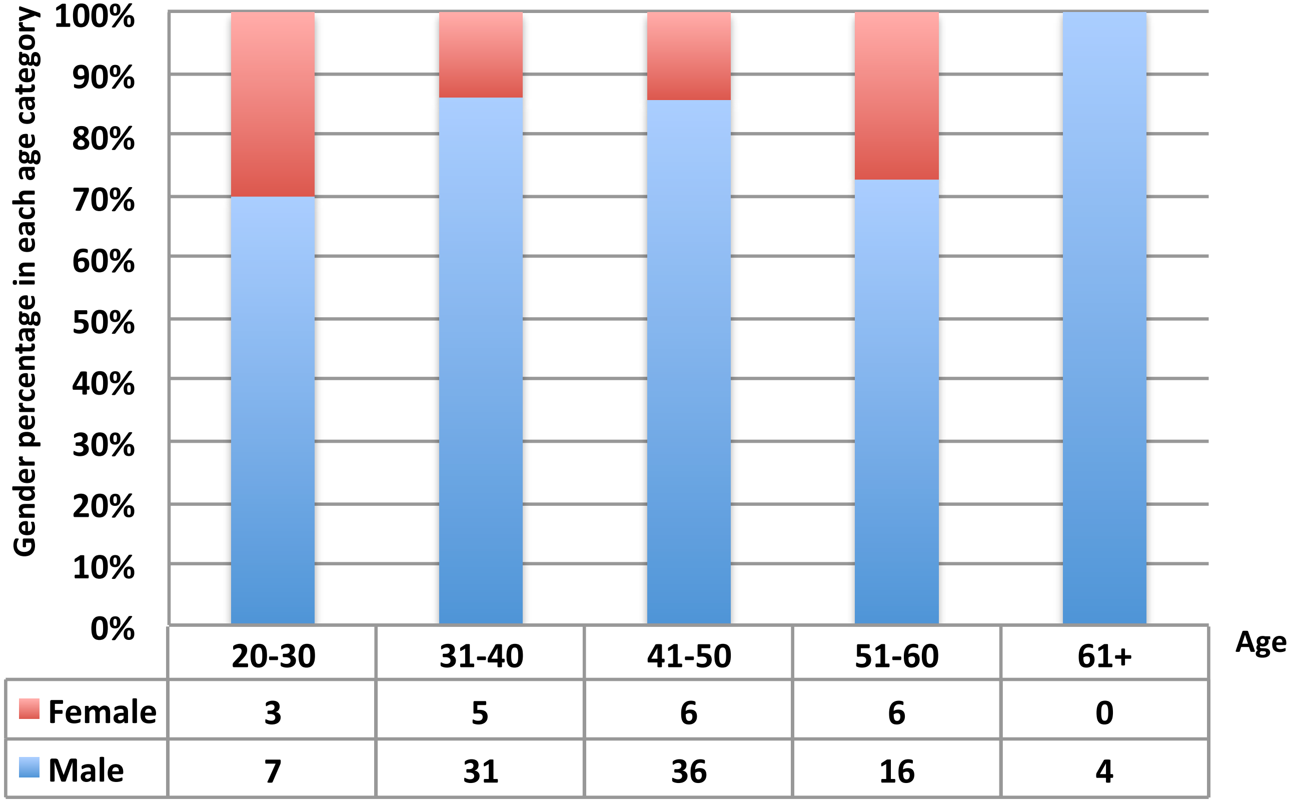
Interviews

- 2 preliminary interviews
  - Get an idea of available tools
  - Get details about the experts we will be interviewing
  - Helped us draft our interview questions
- Followed by 8 interviews
  - Between 60-90 min
  - Extra information that gave us better insight.
  - Stories and anecdotes.

Survey Population

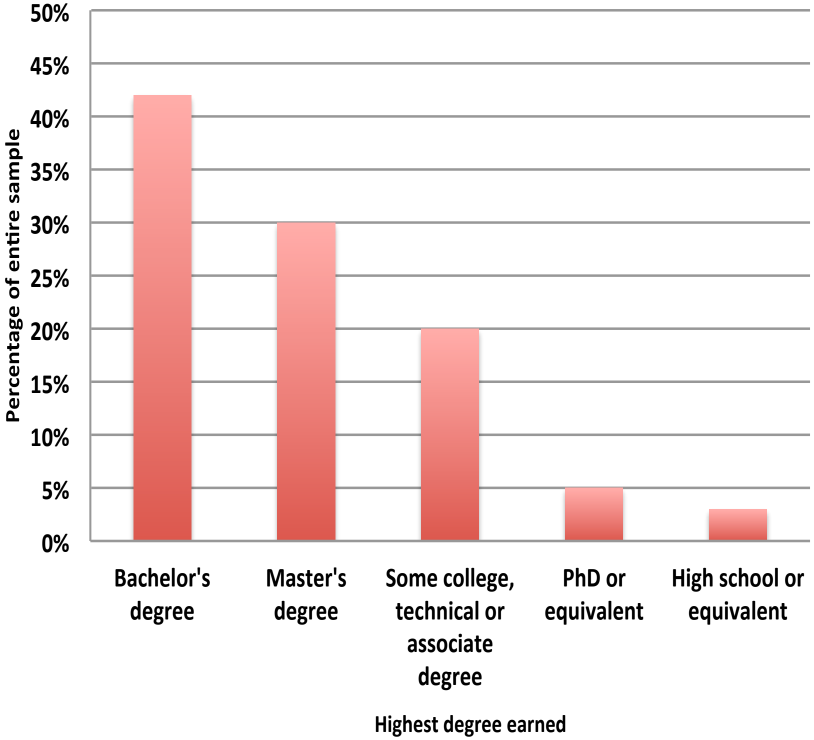
- 5 students of INI program- Forensics Track.
- 110 forensics professionals who attended the High Technology Crime Investigation Association (HTCIA) conference.
- Each participant was rewarded a $10 gift card.
- Total survey participants: 115.
- Online survey launched: 15 participant till now.

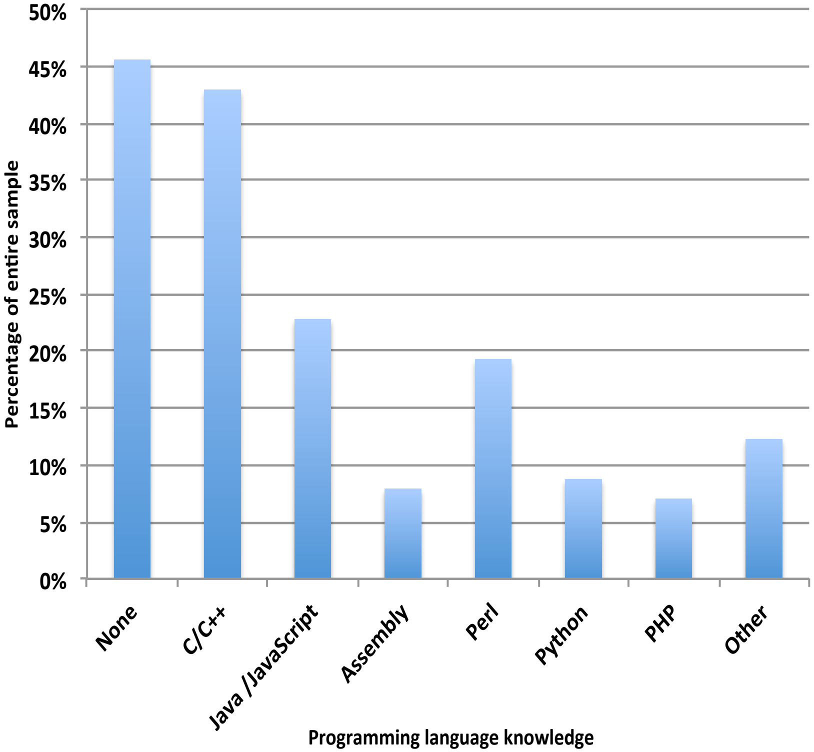
Results:
Demographics – Age & Gender



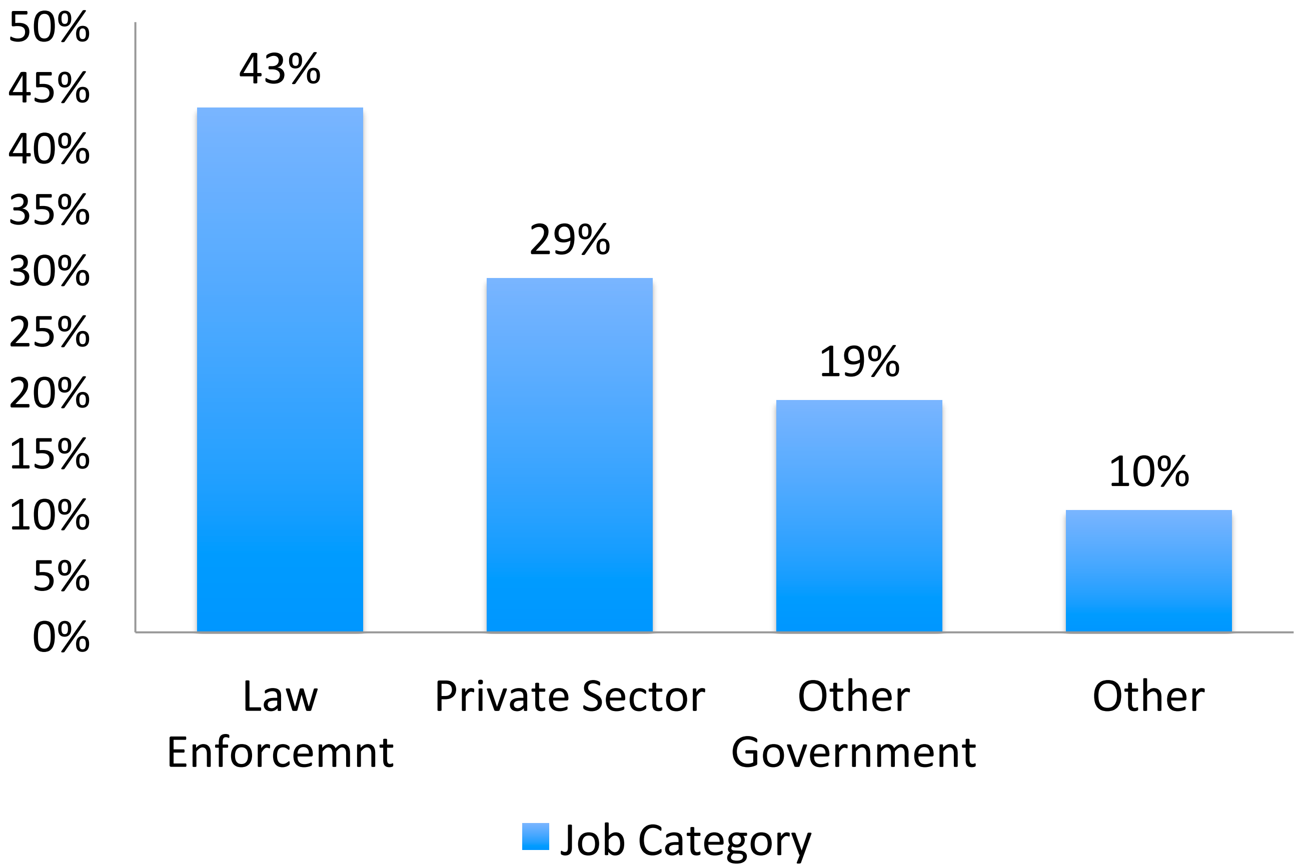
	20-30	31-40	41-50	51-60	61+
🟥 Female	3	5	6	6	0
🟦 Male	7	31	36	16	4

Results: Demographics - Backgrounds





Results: Demographics – Job

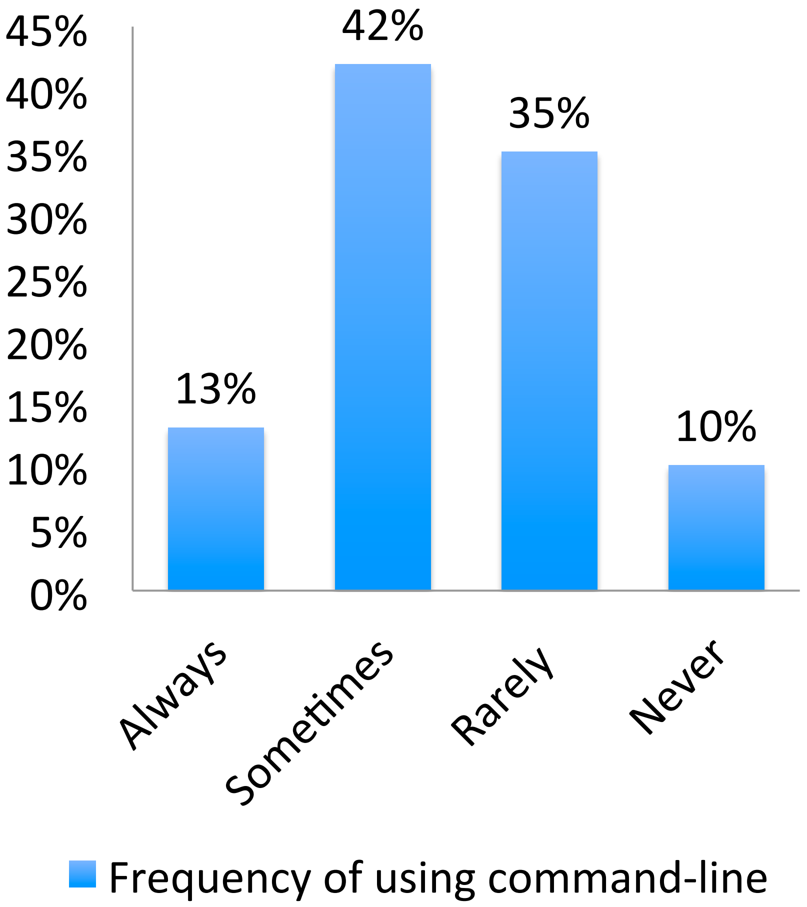


Results: Level of Expertise & Tools

- 43% Experts, 39% intermediate, and 18% beginners.
- By application:
  - FTK and Encase dominate the field around 7 out of 115 only never used each.
  - The Sleuth Kit and Autopsy were the most common open source.
- Open Source:
  - not preferred..
  - only used when needed.
  - court admissibility issue.

Results: GUI vs. Command-line

- Users try to avoid command-line.
- 45% do not know any programming language.
- Enscript Language issues:
  - Not preferred
  - Learning curve
  - Other scripting languages instead.

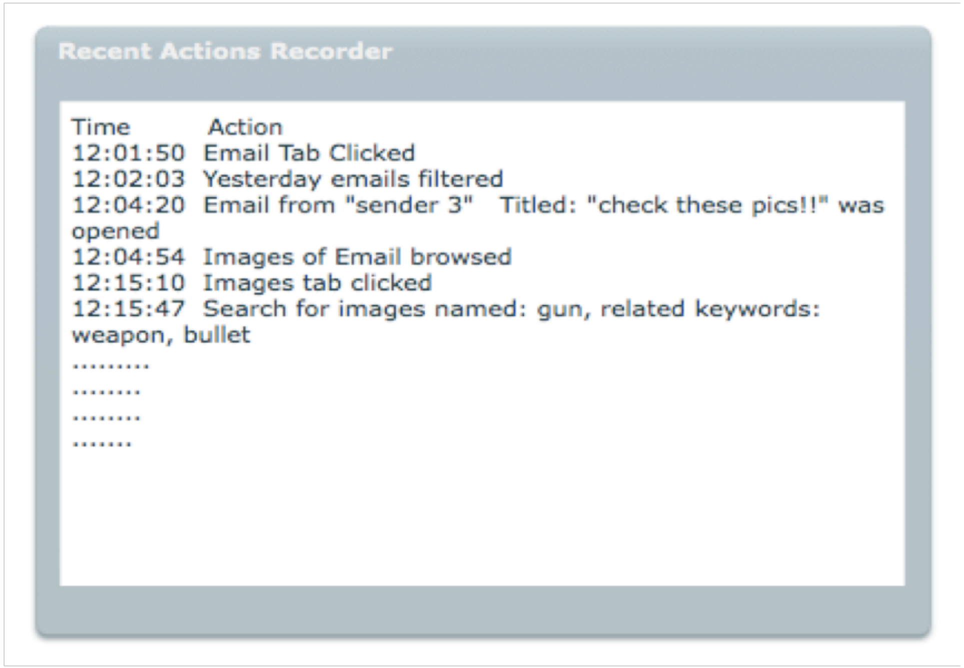


Results: Reporting - 1

- Current programs bookmarking feature: 75% of users votes.
- Pen and paper: 52%
- MS Word: 48%
- 12 users wrote in their comments that they need better reporting tools with more automated features.

Results: Reporting - 2

- This feature would be very useful to me: 55.3%
- This feature would be useful for someone but not for me: 20 %

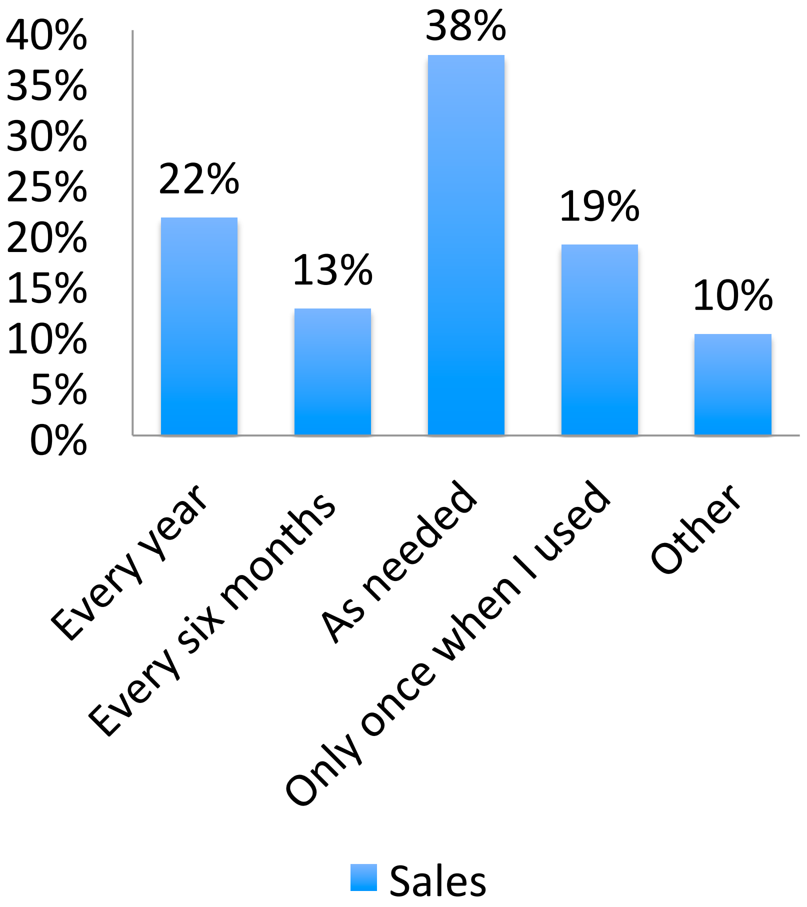


Recent Actions Recorder

```
Time        Action
12:01:50  Email Tab Clicked
12:02:03  Yesterday emails filtered
12:04:20  Email from "sender 3"   Titled: "check these pics!!" was
opened
12:04:54  Images of Email browsed
12:15:10  Images tab clicked
12:15:47  Search for images named: gun, related keywords:
weapon, bullet
..........
.........
.........
........
```

Results: Training Need

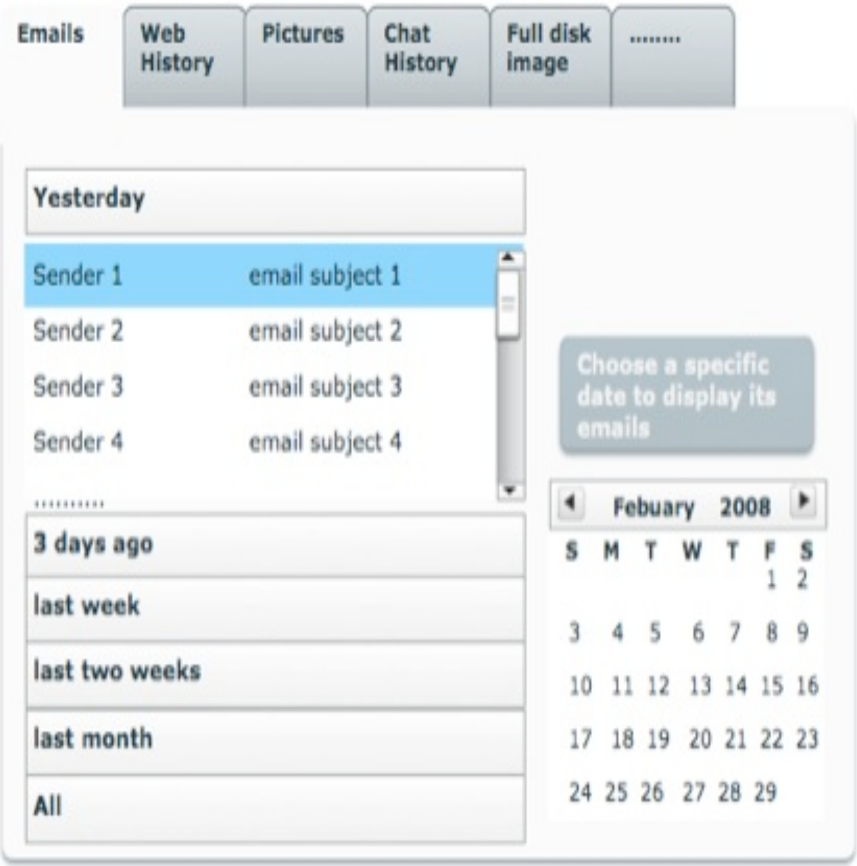
- What is the best approach to make the best use of forensics tools?
  - 68% chose more training
- "Please don't give us more command-line tools, we had enough"



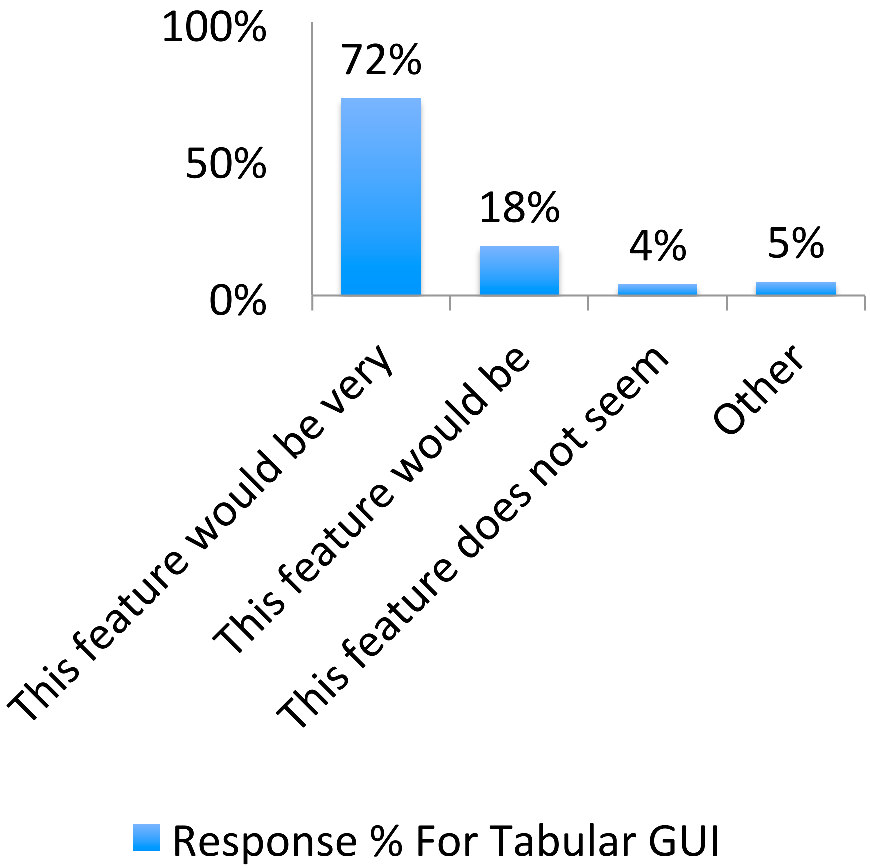
User-Interface Issues - 1

- Users comments:
  - Consistency.
  - More intuitive.
  - More familiar with what we know.
- Information overload: Screen space needed is large.
- Icons: "*how would make an icon describe: extracting a string from a Hard-Drive*"
- Graphics: satisfied but more improvements will be good.

User-Interface Issues -2



Sender 1	email subject 1
Sender 2	email subject 2
Sender 3	email subject 3
Sender 4	email subject 4



Results: Other Issues & Comments

- Users want a magic button w/o much brain power.
- Lack of a collaborative environment: can’t work simultaneously.
- Interoperability between different tools.
- Backward compatibility (e.g. FTK).
- Better help tools.
- Better error messages.
- Faster processing.
- Quick preview of the machine.

Further Work:

- Distribute the online version of the survey to a larger sample to collect more feedback (15 so far).
- Heuristic evaluation
  - 3 tools: FTK Demo, TSK, Autopsy
  - Nielsen guidelines with a little tweak
- User testing
  - 15 INI students – INI program
  - FTK and Autopsy
  - Fill survey before and after
- Define Guidelines (*Hanan Hibshi Master's thesis 2011*)

User Testing Results - 1

- 12 out of 15 users preferred Windows over other operating systems
- Level of expertise with forensics tools:
  - 10 novice, 5 intermediate
  - 10 had used Autopsy before, 5 used FTK
- Use of command line tools
  - Always: 4, Sometimes: 9, Rarely: 2
- Forensics courses taken: (None: 9, 1: 4, 2-4: 2)
- When asked about vocabulary, a significant number of users couldn't define many terms.

User Testing Results - 2

- Users opinions after performing tasks:
  - Moderate: 10, Hard: 3, easy: 2
  - Preferred tool? FTK: 7, Autopsy: 8
- Majority of users think an intermediate to expert level of technical and forensics expertise is needed to be able to use the tools.

Conclusion

- Digital Forensics tools have a number of usability issues that require more attention, research, and improvement. Current tools suffer from:
  - Non-intuitive interfaces
  - Complicated technical terms, jargon, confusing words….
  - Un-reliable help and guidance documentation.
  - High level of complexity.
  - Reliance on advanced technical skills of examiner.
  - Dense display of information.
  - Other..
- Usability problems of these tools need to be addressed for better productivity and accuracy.

Conclusion – Guidelines 1

- Have a platform independent software.
- Combine design simplicity with smart functionality.
- Examine software against known usability standards.
- Accommodate all level of users
  - Assume naïve user as the default.
  - Include functionality that assist expert users needs (example allow for advanced scripting)
- Have a smarter functionality in the program
  - Report generation and assistance
  - Log and tracking so user can track his own actions
  - Include “ready made” advanced search algorithms

Conclusion – Guidelines 2

- Avoid adding incomplete or insufficient features that lead to inaccurate results.
- Apply some technologies already available in the market:
  - Image clustering
  - Multi-threading and multi-core support
  - Interoperability and backward compatibility support
  - Collaborative environment support
- Have better help documentation and resources
  - Include hints, descriptive tool-tip text
  - Smarter help mechanisms
  - Include some general laws and procedures information

Conclusion – Guidelines 3

- Design more intuitive interfaces. Examples of improving this aspect include:
  - Improving the vocabulary used (less jargon, less technical terms)
  - Apply minimal text to menus and choose more self-explanatory keywords.
  - Anticipate users needs (this can be done in many ways)
  - Ensure consistency (platform and in-house)
- Eliminate the need for constant and heavy training by:
  - Designing intuitive interfaces
  - Improving help documentation
  - Automating some processes in a way that is transparent to the user.
  - Apply simple "click and go" mechanisms for simple routine tasks (e,g. email, pictures, documents, web history, chat sessions, etc)

Conclusion – Guidelines 4

- Automate some essential processes to reduce user frustration.
  - Installation process
  - Checking image integrity (hash values)
- Provide some status message to inform user that a task is completed
  - Example: FTK preprocessing
- Improve error messaging functionality and language
  - Think about "KFF library"

Future Work

- Examine our guidelines
  - Conduct thorough user testing on each guideline and measure importance.
- More specific suggestions on applying those guidelines
  - Have a deeper look into the technical and forensics aspects
- Conduct surveys on a larger sample
- User testing:
  - Apply user testing on actual tools
  - Include lengthy more realistic cases in user testing
  - Test some SW design methods on user and measure effectiveness.

Thank you

Q&A