

AI and Digital Forensics

Dr Simson Garfinkel, Chief Scientist
BasisTech
simsong@basistech.com

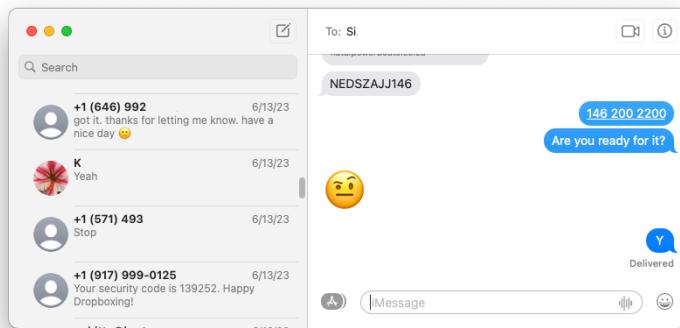
**NIST Long-Term Vision and Strategic Priorities
for Forensic Science in the United States:
Roundtable Discussion with Thought Leaders
Sept. 6-7, 2023**



AI and Digital Forensics: Two Possible Meanings

AI for Digital Forensics

Helping forensic practitioners
Interpreting evidence
Performing investigations



Digital Forensics for AI Systems

Explaining an AI decision (XAI)
Analyzing an AI system – for example, at an accident or crime scene



AI for Digital Forensics

AI for Digital Forensics

Let's consider how AI might be used in:

- Translation (human text)
- Translation (machine text)
- Tool recommendation
- Report writing

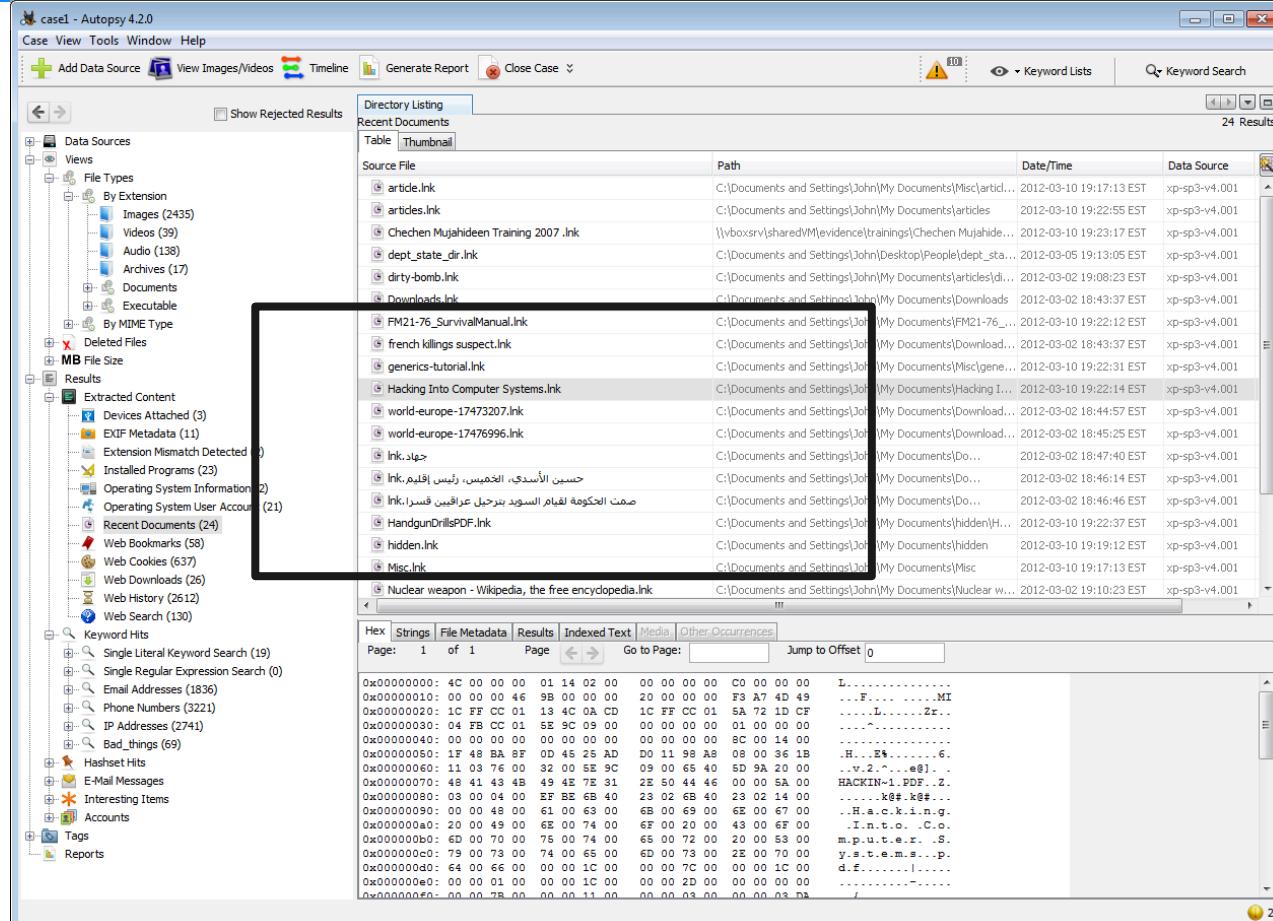
Translation (human text) is a traditional AI task...

The screenshot shows the Autopsy 4.2.0 digital forensics platform interface. The main window displays a list of found files in a table format. The table has columns for Source File, Path, Date/Time, and Data Source. The data source for most files is 'xp-sp3-v4.001'. The table includes the following entries:

Source File	Path	Date/Time	Data Source
article.lnk	C:\Documents and Settings\John\My Documents\Misc\article.lnk	2012-03-10 19:17:13 EST	xp-sp3-v4.001
articles.lnk	C:\Documents and Settings\John\My Documents\articles.lnk	2012-03-10 19:22:55 EST	xp-sp3-v4.001
Chechen Mujahideen Training 2007.lnk	\\\vboxsrv\shared\My\ evidence\trainings\Chechen Mujahideen Training 2007.lnk	2012-03-10 19:23:17 EST	xp-sp3-v4.001
dept_state_dir.lnk	C:\Documents and Settings\John\Desktop\People\dept_state_dir.lnk	2012-03-05 19:13:05 EST	xp-sp3-v4.001
dirty-bomb.lnk	C:\Documents and Settings\John\My Documents\articles\dirty-bomb.lnk	2012-03-02 19:08:23 EST	xp-sp3-v4.001
Downloads.lnk	C:\Documents and Settings\John\My Documents\Downloads.lnk	2012-03-02 18:43:37 EST	xp-sp3-v4.001
FM21-76_SurvivalManual.lnk	C:\Documents and Settings\John\My Documents\FM21-76_SurvivalManual.lnk	2012-03-10 19:22:12 EST	xp-sp3-v4.001
french killings suspect.lnk	C:\Documents and Settings\John\My Documents\Downloads\french killings suspect.lnk	2012-03-02 18:43:37 EST	xp-sp3-v4.001
generics-tutorial.lnk	C:\Documents and Settings\John\My Documents\Misc\generics-tutorial.lnk	2012-03-10 19:22:31 EST	xp-sp3-v4.001
Hacking Into Computer Systems.lnk	C:\Documents and Settings\John\My Documents\Hacking Into Computer Systems.lnk	2012-03-10 19:22:14 EST	xp-sp3-v4.001
world-europe-17473207.lnk	C:\Documents and Settings\John\My Documents\Download\world-europe-17473207.lnk	2012-03-02 18:44:57 EST	xp-sp3-v4.001
world-europe-17476996.lnk	C:\Documents and Settings\John\My Documents\Download\world-europe-17476996.lnk	2012-03-02 18:45:25 EST	xp-sp3-v4.001
Ink.جاء	C:\Documents and Settings\John\My Documents\Ink.جاء	2012-03-02 18:47:40 EST	xp-sp3-v4.001
Ink.ink	C:\Documents and Settings\John\My Documents\Ink.ink	2012-03-02 18:46:14 EST	xp-sp3-v4.001
صمت الحكومة لغمام السويس تدخل عراقيون فسرا	C:\Documents and Settings\John\My Documents\صمت الحكومة لغمام السويس تدخل عراقيون فسرا	2012-03-02 18:46:46 EST	xp-sp3-v4.001
HandgunDrillsPDF.lnk	C:\Documents and Settings\John\My Documents\hidden\HandgunDrillsPDF.lnk	2012-03-10 19:22:37 EST	xp-sp3-v4.001
hidden.lnk	C:\Documents and Settings\John\My Documents\hidden.lnk	2012-03-10 19:19:12 EST	xp-sp3-v4.001
Misc.lnk	C:\Documents and Settings\John\My Documents\Misc.lnk	2012-03-10 19:17:13 EST	xp-sp3-v4.001
Nuclear weapon - Wikipedia, the free encyclopedia.lnk	C:\Documents and Settings\John\My Documents\Nuclear weapon - Wikipedia, the free encyclopedia.lnk	2012-03-02 19:10:23 EST	xp-sp3-v4.001

The interface also includes a left sidebar with navigation links such as 'Data Sources', 'Views', 'File Types', 'Results', 'Extracted Content', 'Devices Attached (3)', 'EXIF Metadata (11)', 'Extension Mismatch Detected (2)', 'Installed Programs (23)', 'Operating System Information (2)', 'Operating System User Account (21)', 'Recent Documents (24)', 'Web Bookmarks (58)', 'Web Cookies (637)', 'Web Downloads (26)', 'Web History (2612)', 'Web Search (130)', 'Keyword Hits', 'Single Literal Keyword Search (19)', 'Single Regular Expression Search (0)', 'Email Addresses (1836)', 'Phone Numbers (3221)', 'IP Addresses (2741)', 'Bad_things (69)', 'Hashset Hits', 'E-Mail Messages', 'Interesting Items', 'Accounts', 'Tags', and 'Reports'. The bottom of the interface features a hex dump of the selected file content.

Translation (human text) is a traditional AI task...



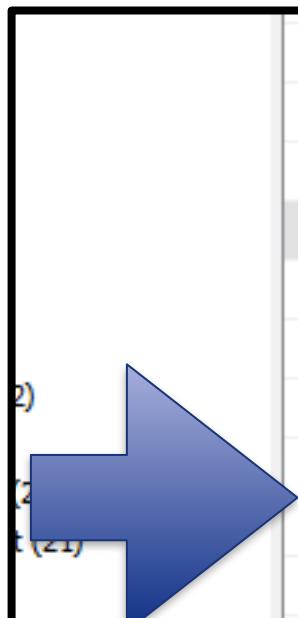
The screenshot shows the Autopsy 4.2.0 forensic analysis interface. The left sidebar contains a tree view of data sources, views, file types (including images, videos, audio, archives, documents, executable, and deleted files), MB file size, results (extracted content, devices attached, EXIF metadata, extension mismatch, installed programs, operating system information, operating system user accounts, recent documents, web bookmarks, web cookies, web downloads, web history, and web search), keyword hits (single literal keyword search, single regular expression search, email addresses, phone numbers, IP addresses, bad things, hashset hits, E-mail messages, interesting items, accounts, tags, and reports), and a timeline. The main pane displays a 'Directory Listing' of recent documents. A table lists the source file, path, date/time, and data source for each document. A black box highlights a list of Arabic file names: 'جهاز', 'حسين الأنسى, الخامس, رئيس', 'فتح', 'صمت الحكومة لفاجة السوبود بدخول عربفين قسرا', 'HandgunDrillsPDF.lnk', 'hidden.lnk', and 'Misc.lnk'. Below this, a search results pane shows the indexed text for 'Nuclear weapon - Wikipedia, the free encyclopedia.lnk', with a hex dump of the file's content.

Source File	Path	Date/Time	Data Source
article.lnk	C:\Documents and Settings\John\My Documents\Misc\article...	2012-03-10 19:17:13 EST	xp-sp3-v4.001
articles.lnk	C:\Documents and Settings\John\My Documents\articles	2012-03-10 19:22:55 EST	xp-sp3-v4.001
Chечен Mujahideen Training 2007.lnk	\\\vboxsvr\sharedM\ evidence\trainings\Chечен Mujahide...	2012-03-10 19:23:17 EST	xp-sp3-v4.001
dept_state_dir.lnk	C:\Documents and Settings\John\Desktop\People\dept_sta...	2012-03-05 19:13:05 EST	xp-sp3-v4.001
dirty-bomb.lnk	C:\Documents and Settings\John\My Documents\articles\di...	2012-03-02 19:08:23 EST	xp-sp3-v4.001
Downloads.lnk	C:\Documents and Settings\John\My Documents\Downloads	2012-03-02 18:43:37 EST	xp-sp3-v4.001
FM21-76_SurvivalManual.lnk	C:\Documents and Settings\John\My Documents\FM21-76_...	2012-03-10 19:22:12 EST	xp-sp3-v4.001
french killings suspect.lnk	C:\Documents and Settings\John\My Documents\Download...	2012-03-02 18:43:37 EST	xp-sp3-v4.001
generics-tutorial.lnk	C:\Documents and Settings\John\My Documents\Misc\gene...	2012-03-10 19:22:31 EST	xp-sp3-v4.001
Hacking Into Computer Systems.lnk	C:\Documents and Settings\John\My Documents\Hacking I...	2012-03-10 19:22:14 EST	xp-sp3-v4.001
world-europe-17473207.lnk	C:\Documents and Settings\John\My Documents\Download...	2012-03-02 18:44:57 EST	xp-sp3-v4.001
world-europe-17476996.lnk	C:\Documents and Settings\John\My Documents\Download...	2012-03-02 18:45:25 EST	xp-sp3-v4.001
جهاز	C:\Documents and Settings\John\My Documents\Do...	2012-03-02 18:47:40 EST	xp-sp3-v4.001
حسين الأنسى, الخامس, رئيس	C:\Documents and Settings\John\My Documents\Do...	2012-03-02 18:46:14 EST	xp-sp3-v4.001
فتح	C:\Documents and Settings\John\My Documents\Do...	2012-03-02 18:46:46 EST	xp-sp3-v4.001
صمت الحكومة لفاجة السوبود بدخول عربفين قسرا	C:\Documents and Settings\John\My Documents\hidden\...	2012-03-10 19:22:37 EST	xp-sp3-v4.001
HandgunDrillsPDF.lnk	C:\Documents and Settings\John\My Documents\hidden	2012-03-10 19:19:12 EST	xp-sp3-v4.001
hidden.lnk	C:\Documents and Settings\John\My Documents\Misc	2012-03-10 19:17:13 EST	xp-sp3-v4.001
Misc.lnk	C:\Documents and Settings\John\My Documents\Nuclear w...	2012-03-02 19:10:23 EST	xp-sp3-v4.001

Indexed Text for Nuclear weapon - Wikipedia, the free encyclopedia.lnk

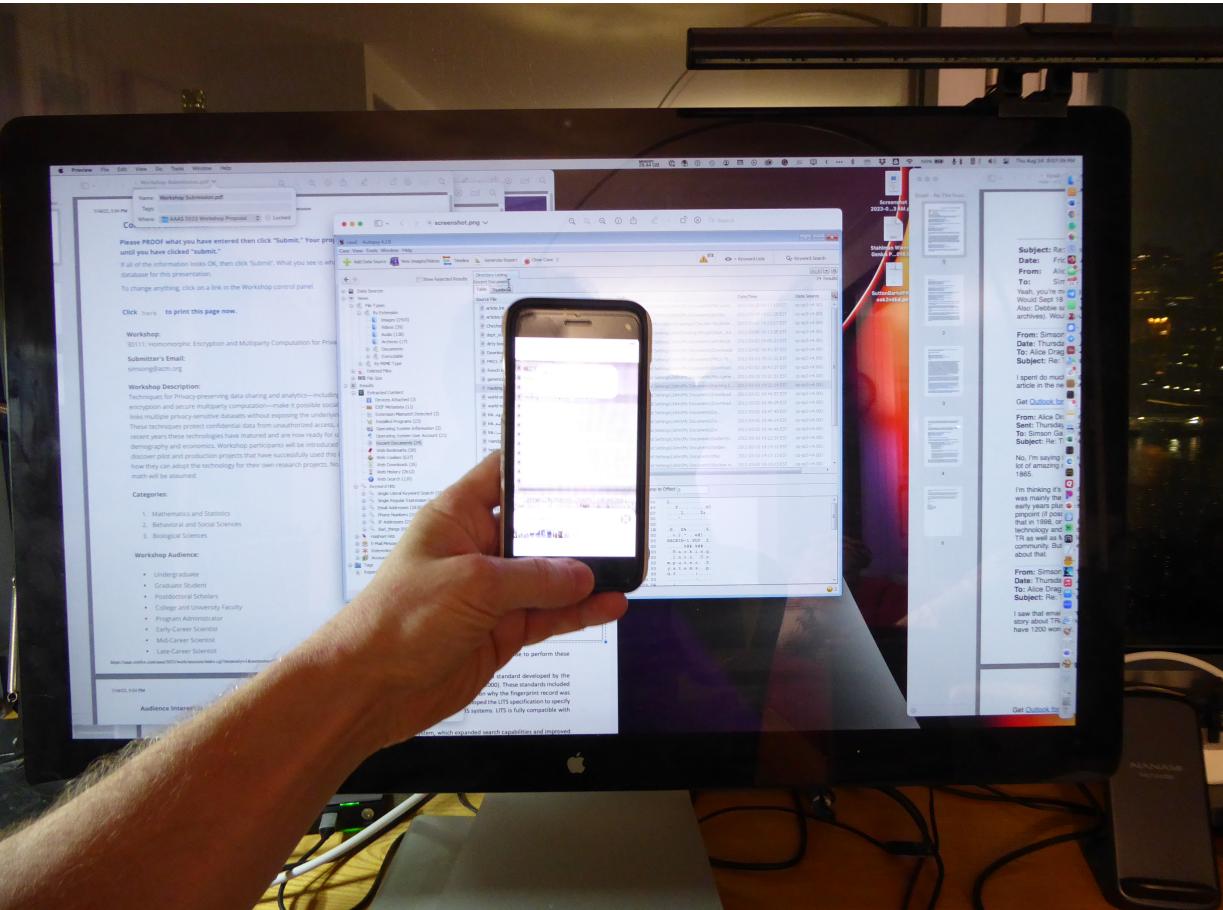
Page: 1 of 1	Page	Go to Page:	Jump to Offset:
0x00000000: 4C 00 00 00 01 14 02 00 00 00 00 00 00 00 00 00 L.....			0
0x00000010: 00 00 00 46 98 00 00 00 20 00 00 00 F3 A7 4D 49 ..F.....MI			
0x00000020: 1C FF CC 01 18 4C 0D CD 1C FF CC 01 6A 72 1D CF ..L.....Zr..			
0x00000030: 04 FB CC 01 55 9C 09 00 00 00 00 01 00 00 00 ..			
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..			
0x00000050: 1F 48 BA 87 00 45 25 AD 00 11 98 A8 08 00 36 1B ..H.....6.			
0x00000060: 11 03 76 00 32 00 5E 9C 00 00 65 40 5D 9A 20 00 ..v.2.e@! .			
0x00000070: 41 41 43 4B 49 4E 7E 31 20 54 46 00 00 5A 00 HACKIN-1.PDF.Z.			
0x00000080: 00 00 04 00 EF BE 40 23 02 60 23 02 14 00 ..k@.k@... .			
0x00000090: 00 00 48 00 61 00 63 00 6B 00 60 00 6E 00 67 00 ..H.a.c.k.i.n.g.			
0x000000A0: 20 00 49 00 6E 00 74 00 6F 00 20 00 43 00 6F 00 ..I.n.t.o. .C.o.			
0x000000B0: 60 00 70 00 75 00 74 00 65 00 72 00 20 00 53 00 m.p.u.t.e.r. .S			
0x000000C0: 79 00 73 00 74 00 65 00 6D 00 73 00 2E 00 70 00 y.s.t.e.m.s.-p.			
0x000000D0: 64 00 66 00 00 00 1C 00 00 00 7C 00 00 00 1C 00 d.f..... .			
0x000000E0: 00 00 01 00 00 00 00 00 1C 00 00 00 2D 00 00 00 00 ..			
0x000000F0: ..			

What do these filenames mean in English?



2)	FM21-76_SurvivalManual.lnk	C:\Documents and Settings\Joh
2)	french killings suspect.lnk	C:\Documents and Settings\Joh
2)	generics-tutorial.lnk	C:\Documents and Settings\Joh
2)	Hacking Into Computer Systems.lnk	C:\Documents and Settings\Joh
2)	world-europe-17473207.lnk	C:\Documents and Settings\Joh
2)	world-europe-17476996.lnk	C:\Documents and Settings\Joh
2)	Ink.جihad	C:\Documents and Settings\Joh
2)	حسين الأسدی، الخميس، رئيس إقليم.lnk	C:\Documents and Settings\Joh
2)	صمت الحكومة لقيام السويد بترحيل عراقيين قسرا.lnk	C:\Documents and Settings\Joh
2)	HandgunDrillsPDF.lnk	C:\Documents and Settings\Joh
2)	hidden.lnk	C:\Documents and Settings\Joh
2)	Misc.lnk	C:\Documents and Settings\Joh

Just hold your phone up to the computer screen and use the Google Translate app...

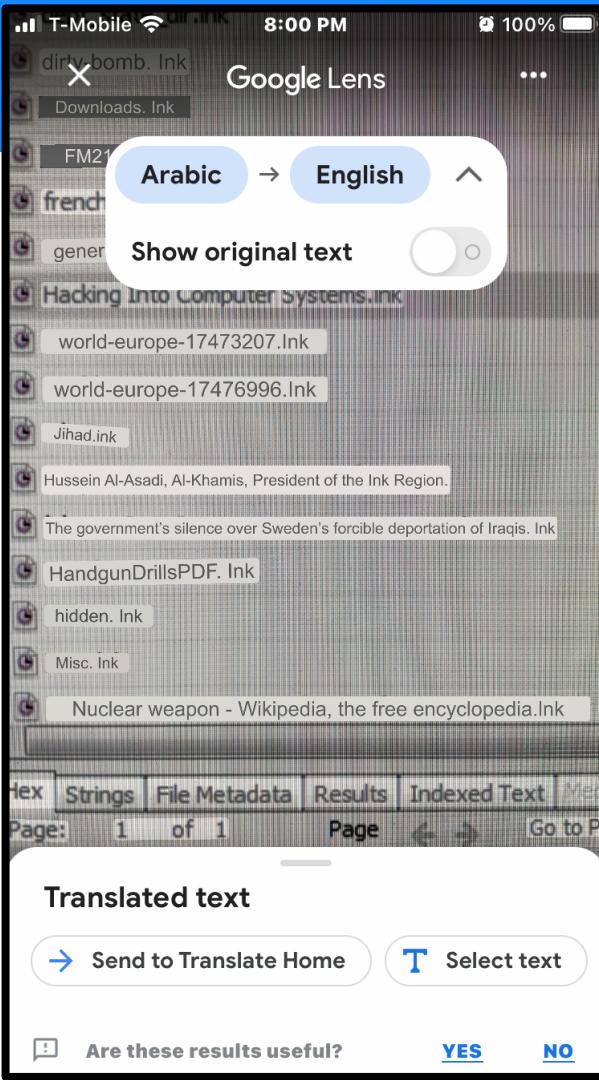


This works surprisingly well...
but it's awkward! (and hard to take into court)

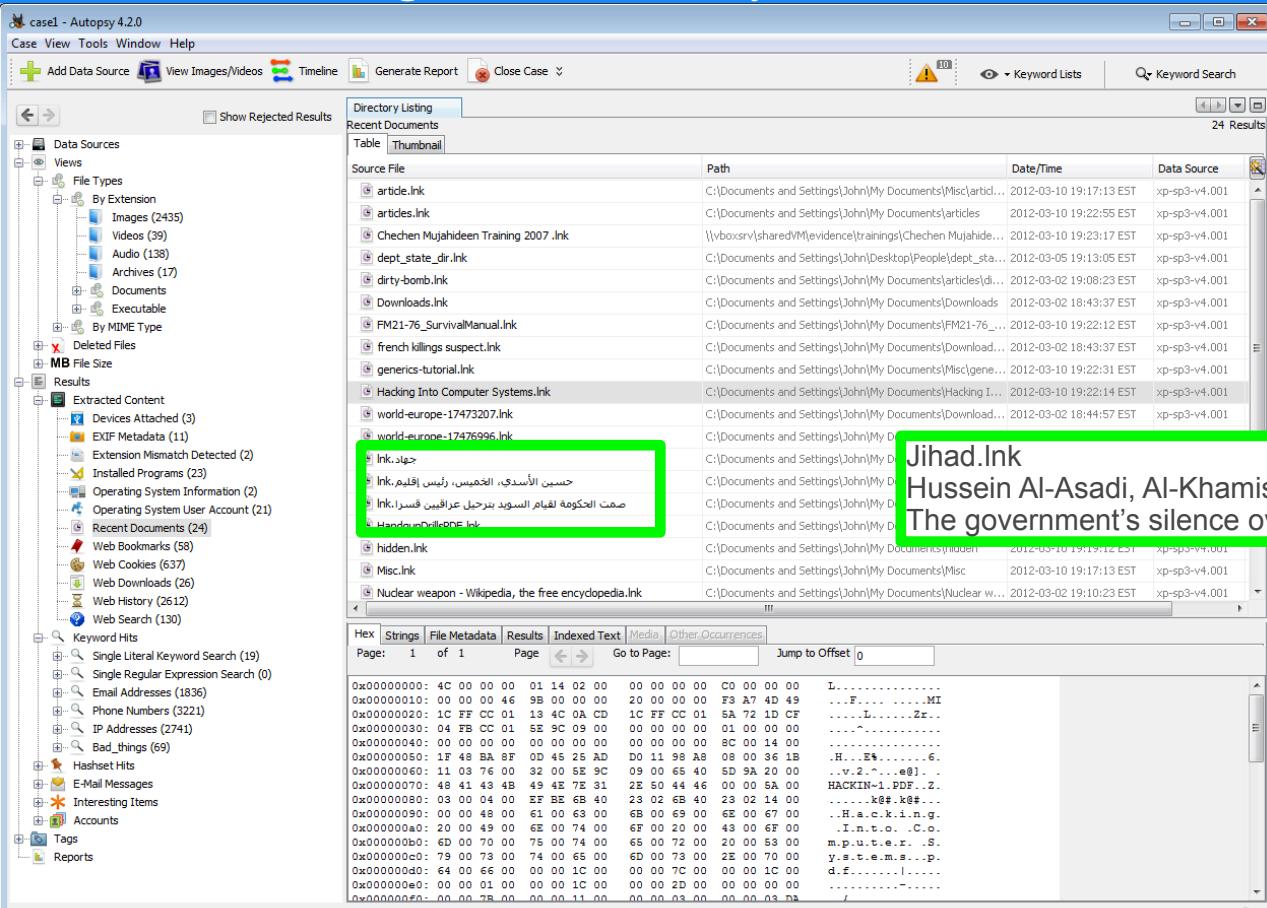
french killings suspect.lnk	C:\Documents and Settings\John\
generics-tutorial.lnk	C:\Documents and Settings\John\
Hacking Into Computer Systems.lnk	C:\Documents and Settings\John\
world-europe-17473207.lnk	C:\Documents and Settings\John\
world-europe-17476996.lnk	C:\Documents and Settings\John\
Ink.جهاز	C:\Documents and Settings\John\
حسين الأسد، الخميس، رئيس إقليم.	C:\Documents and Settings\John\
صمت الحكومة لقيام السويد بترحيل عراقيين قسرا.	C:\Documents and Settings\John\
HandgunDrillsPDF.lnk	C:\Documents and Settings\John\
hidden.lnk	C:\Documents and Settings\John\

Options:

- Build translation into every forensic tool
- Build translation into the OS
 - Web browsers do this already!
 - Do we need “validated translation” for forensics?



We can't update every tool – but a “forensic CoPilot” could watch the screen, look for non-English text, and provide translation in overlays...



Jihad.Ink

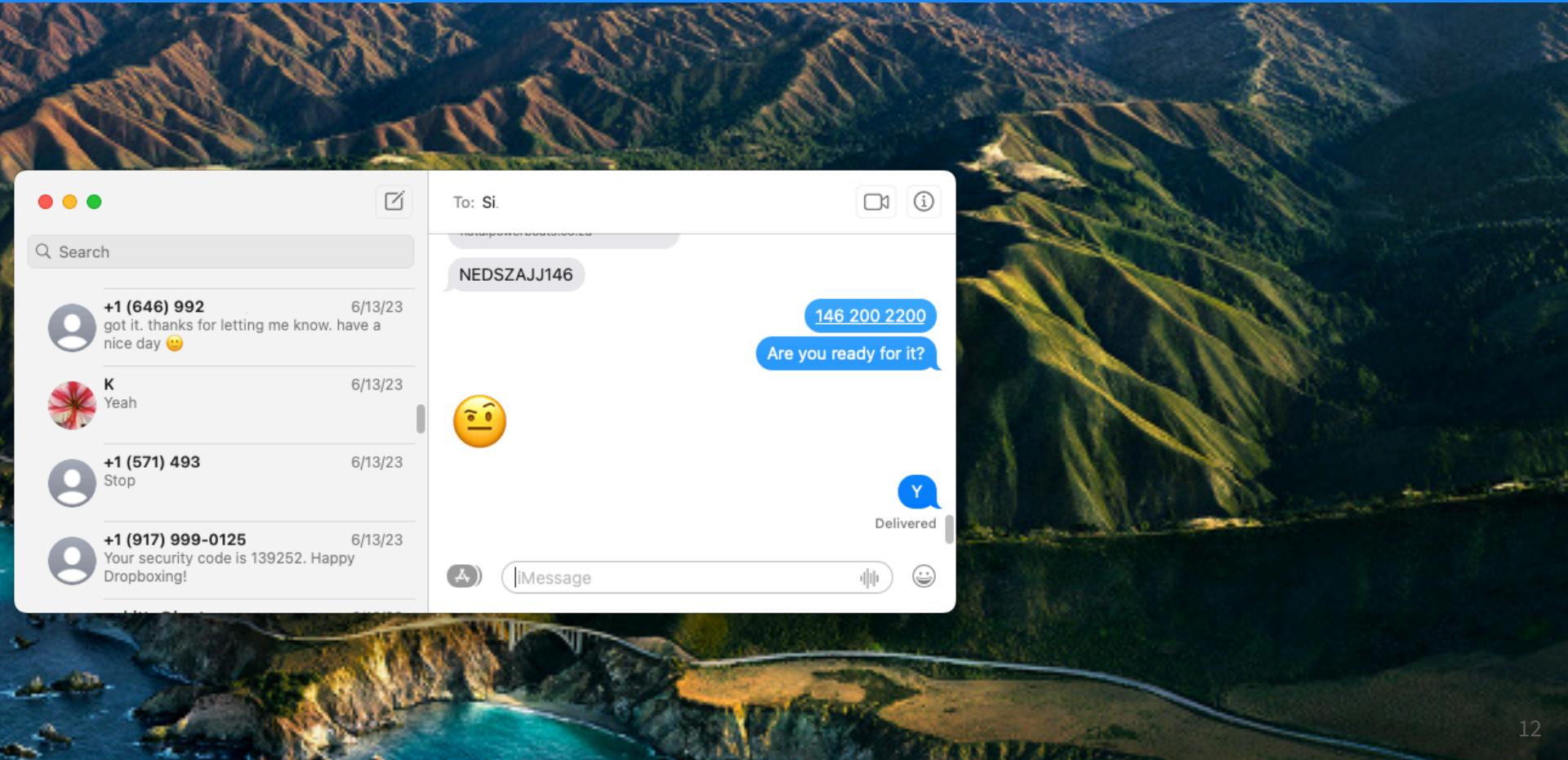
Hussein Al-Asadi, Al-Khamis, President of the Region.lnk

The government's silence over Sweden's forcible deportation of Iraqis. In

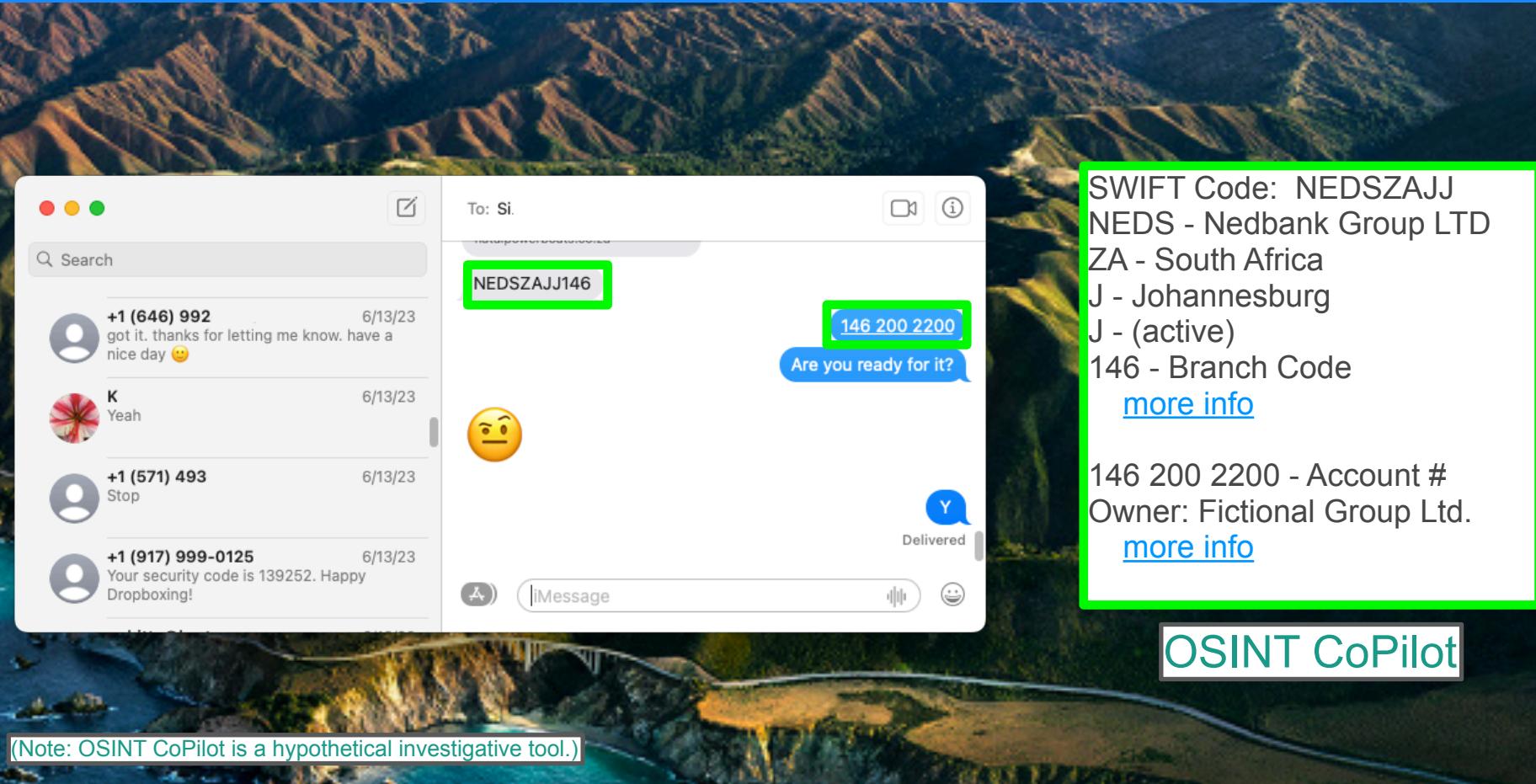
The Forensic CoPilot could provide additional context.
Consider a hypothetical case involving Apple Messenger...



The examiner encounters information that is unfamiliar...



AI can watch the investigator's screen and provide context.



The image shows a Mac desktop with an iMessage window open. The window has a green box around the recipient field 'To: Si.' and the message 'NEDSZAJJ146'. A blue box highlights the response '146 200 2200' and the message 'Are you ready for it?'. Below the message is a yellow emoji of a face with a neutral expression. The iMessage interface includes a search bar, a list of recent messages, and a toolbar with a microphone, a camera icon, and a smiley face icon. The status bar at the bottom shows 'iMessage' and a sound icon. The background of the desktop is a scenic view of mountains and a bridge.

SWIFT Code: NEDSZAJJ
NEDS - Nedbank Group LTD
ZA - South Africa
J - Johannesburg
J - (active)
146 - Branch Code
[more info](#)

146 200 2200 - Account #
Owner: Fictional Group Ltd.
[more info](#)

OSINT CoPilot

(Note: OSINT CoPilot is a hypothetical investigative tool.)

AI can recommend tools for cyber investigations.

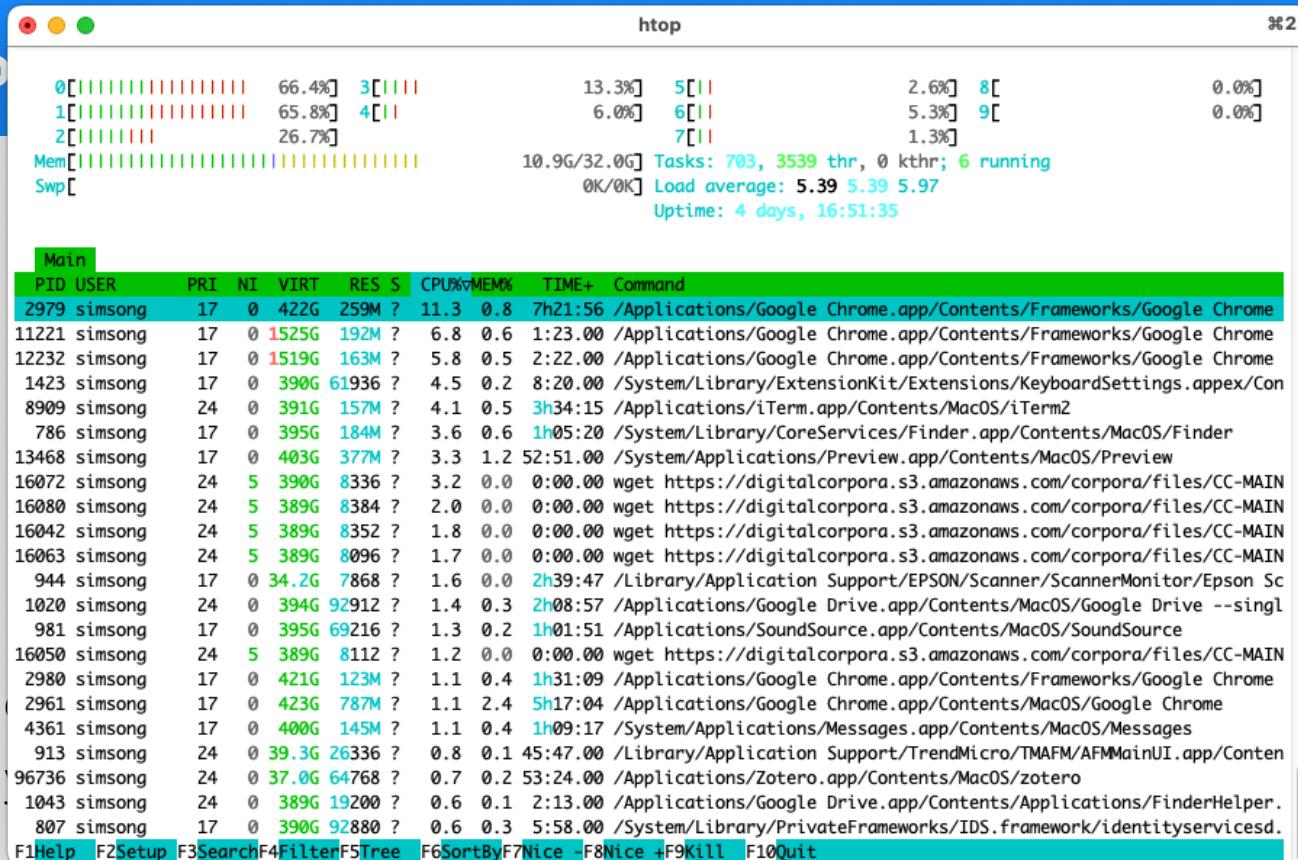
me: system sluggish.

AI: Are you on the (C) Console or accessing via (S) SSH?

me: S

AI: try: **htop**

AI can recom



me: syst

AI: Are

me: S

AI: try: htop

AI: Sluggishness may be Chrome or wget; try: iftop

AI can recover

me: system

AI: Are you using a proxy or a VPN?

me: S

AI: try: www.whatismyip.com

AI: Sluggishness may be Chrome or wget; try: **iftop**

AI: ... Checking IP addresses ...

		246Mb	491Mb	737Mb	982Mb	1.20Gb	%2
seasons			=> 52.92.161.57		31.4Kb	32.2Kb	30.7Kb
			<=		59.5Mb	64.0Mb	60.0Mb
seasons			=> s3-us-west-2-w.amazonaws.com		35.3Kb	31.7Kb	30.8Kb
			<=		42.8Mb	41.9Mb	39.5Mb
seasons			=> s3-us-west-2-w.amazonaws.com		31.1Kb	29.5Kb	28.7Kb
			<=		32.0Mb	31.0Mb	29.1Mb
seasons			=> 52.92.154.249		27.2Kb	27.9Kb	27.8Kb
			<=		24.2Mb	21.9Mb	21.3Mb
2600:4040:98b9:6800::1			=> 2620:149:a41:280::2:3		13.1Kb	2.63Kb	2.19Kb
			<=		33.9Kb	6.79Kb	5.65Kb
2600:4040:98b9:6800::1			=> 2620:1ec:21::14		0b	5.39Kb	4.49Kb
			<=		0b	3.63Kb	3.03Kb
seasons			=> ec2-3-232-15-196.compute-1.amazonaws.com		0b	5.79Kb	4.83Kb
			<=		0b	258b	215b
seasons			=> 168.142.204.15		208b	2.99Kb	2.49Kb
			<=		4.94Kb	1.47Kb	1.23Kb
seasons			=> 187.121.232.35.bc.googleusercontent.com		0b	942b	785b
			<=		0b	775b	646b
2600:4040:98b9:6800::1			=> 2600:4040:98b9:6800::1		1.24Kb	604b	657b
			<=		1.72Kb	832b	915b
seasons			=> 17.188.169.196		816b	492b	631b
			<=		816b	492b	622b
seasons			=> 192.168.1.154		208b	336b	280b
			<=		160b	394b	329b
2600:4040:98b9:6800::1			=> bi-in-f188.1e100.net		1.33Kb	320b	267b
			<=		1.31Kb	326b	272b
TX:		cum:	212KB	peak:	171Kb	rates:	
RX:			225MB		169Mb	143Kb 142Kb 141Kb	
TOTAL:			225MB		169Mb	159Mb 159Mb 150Mb	
						159Mb 159Mb 150Mb	

Download



WHOIS Details

WHOIS Lookup (52.92.161.57)

```
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/  
#  
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.  
#
```

NetRange: 52.84.0.0 – 52.95.255.255
CIDR: 52.88.0.0/13, 52.84.0.0/14
NetName: AT-88-Z
NetHandle: NET-52-84-0-0-1
Parent: NET52 (NET-52-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS16509, AS14618
Organization: Amazon Technologies Inc. (AT-88-Z)
RegDate: 1991-12-19
Updated: 2022-03-21
Ref: https://rdap.arin.net/registry/ip/52.84.0.0

OrgName: Amazon Technologies Inc.
OrgId: AT-88-Z
Address: 410 Terry Ave N.
City: Seattle
StateProv: WA
PostalCode: 98109
Country: US
RegDate: 2011-12-08
Updated: 2022-09-30

AI can recommend tools for cyber investigations

me: system sluggish.

AI: Are you on the (C) Console

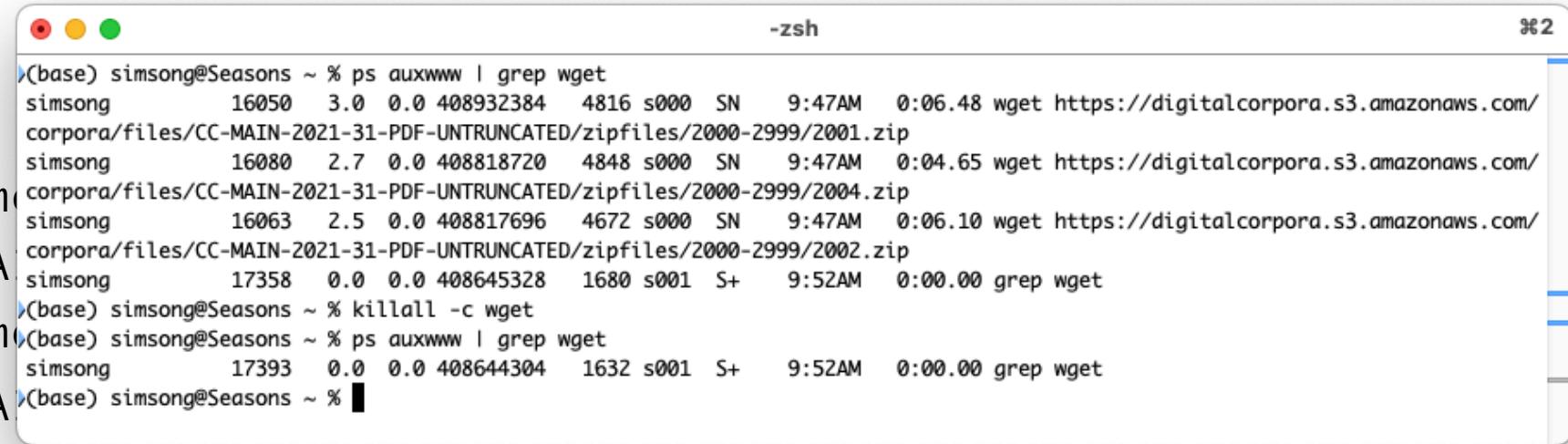
me: S

AI: try: **htop**

AI: ... Checking IP addresses ...

AI: Major data flows are from Amazon Web Services via wget

AI can recommend tools for cyber investigations.



```
(base) simsong@Seasons ~ % ps auxwww | grep wget
simsong      16050  3.0  0.0 408932384  4816 s000  SN    9:47AM  0:06.48 wget https://digitalcorpora.s3.amazonaws.com/
corpora/files/CC-MAIN-2021-31-PDF-UNTRUNCATED/zipfiles/2000-2999/2001.zip
simsong      16080  2.7  0.0 408818720  4848 s000  SN    9:47AM  0:04.65 wget https://digitalcorpora.s3.amazonaws.com/
corpora/files/CC-MAIN-2021-31-PDF-UNTRUNCATED/zipfiles/2000-2999/2004.zip
simsong      16063  2.5  0.0 408817696  4672 s000  SN    9:47AM  0:06.10 wget https://digitalcorpora.s3.amazonaws.com/
corpora/files/CC-MAIN-2021-31-PDF-UNTRUNCATED/zipfiles/2000-2999/2002.zip
simsong      17358  0.0  0.0 408645328  1680 s001  S+   9:52AM  0:00.00 grep wget
(base) simsong@Seasons ~ % killall -c wget
(base) simsong@Seasons ~ % ps auxwww | grep wget
simsong      17393  0.0  0.0 408644304  1632 s001  S+   9:52AM  0:00.00 grep wget
(base) simsong@Seasons ~ %
```

AI: ... Checking IP addresses ...

AI: Major data flows are from Amazon Web Services via wget

AI: Recommended action: document and terminate wget processes.

AI for Digital Forensics

What I promised:

- Translation (human text) ✓
- Translation (machine text) ✓
- Tool recommendation ✓

I didn't get to this:

- Report writing ✗
 - Didn't get to this!

Sorry!

Please ask ChatGPT for ideas!!!

Digital Forensics for AI

Forensics will be used to bring data from AI failures into court.

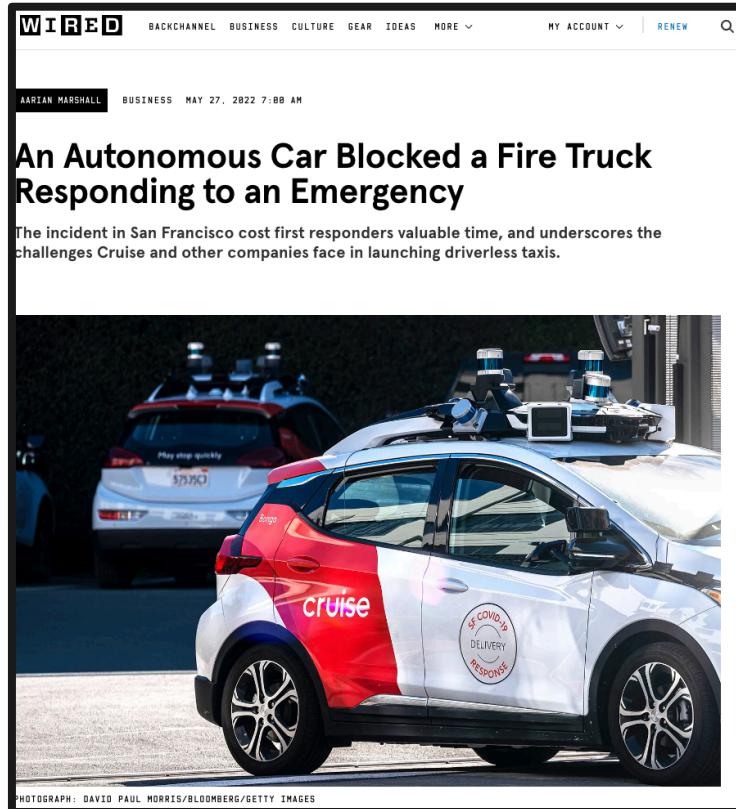
Why did the AI fail?

- Was the failure in *this particular system*?
- Was the failure in *the system's design*?

What was the source of this particular incident?

- Hardware design
- Hardware failure (sensor; computer; network)
- Software design
- Software error
- Training data coverage or bias
- A specific piece of training data
- Over-the-air update to software or model?

What kind of forensic investigation protocol would reliably answer these questions?



WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE MY ACCOUNT RENEW

AARZAN MARSHALL BUSINESS MAY 27, 2022 7:08 AM

An Autonomous Car Blocked a Fire Truck Responding to an Emergency

The incident in San Francisco cost first responders valuable time, and underscores the challenges Cruise and other companies face in launching driverless taxis.

PHOTOGRAPH: DAVID PAUL MORRIS/BLOOMBERG/GETTY IMAGES

If attacks on driverless cars become more aggressive, forensics will be used for assessing fault

npr **wnyc** NEWS CULTURE MUSIC PODCASTS & SHOWS SEARCH

NEWSLETTERS SIGN IN NPR SHOP

BUSINESS

Armed with traffic cones, protesters are immobilizing driverless cars

August 26, 2023 · 7:01 AM ET

 Dara Kerr



Members of Safe Street Rebel place a cone on a self-driving Cruise car in San Francisco. Josh Edelson/AFP via Getty Images

<https://www.npr.org/2023/08/26/1195695051/driverless-cars-san-francisco-waymo-cruise>

Researchers and practitioners need to develop new techniques for AI forensics.

Develop and validate approaches to acquire and stabilize forensic evidence from AI-enabled cyber-physical systems.

Develop the equivalent of “file hashing” for AI models:

- Detect identical or equivalent models
- Quantify model divergence and impact of model changes

Distinguish model changes and behaviors that are:

- benign vs. malicious
- emergent vs. directed

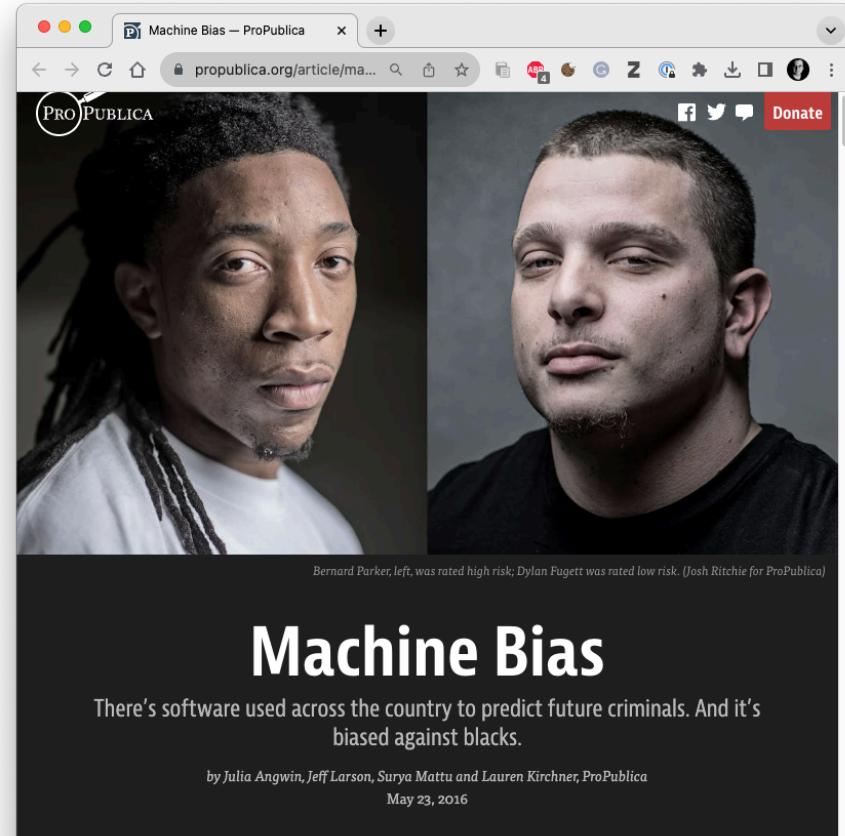
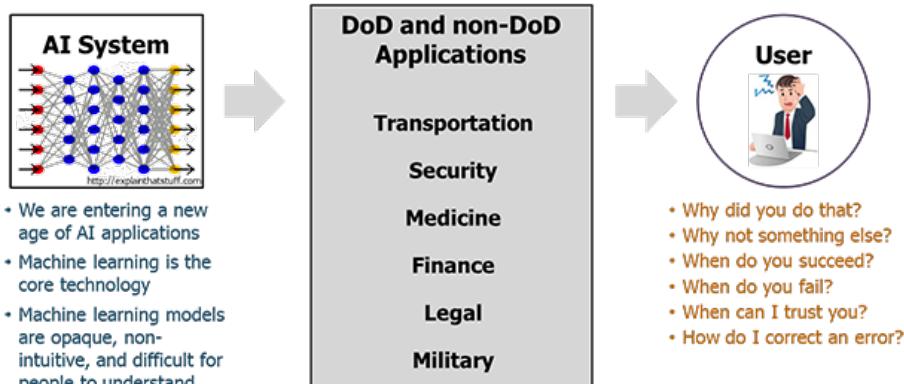


<https://en.wikipedia.org/wiki/Slaughterbots>

AI forensics is not limited to cyber-physical systems – and it's about more than simply auditing algorithms for fairness or explanation.

There is growing interest in auditing AI systems for “fairness.”

Overlaps with Explainable AI (XAI)



IBM includes AI detection in AI forensics

IBM Research Focus areas Publications Collaborate Careers Events ▶ 🔍 ⚙

📅 24 Jul 2023 📄 Explainer ⏳ 5 minute read

Did an AI write that? If so, which one? Introducing the new field of AI forensics

IBM researchers are developing AI-text detection and attribution tools to make generative AI more transparent and trustworthy.



24 July 2023
<https://research.ibm.com/blog/AI-forensics-attribution>

The first targets for “forensics of AI systems” might be AI systems that are used for conventional forensics.

NIST Study Shows Face Recognition Experts Perform Better With AI as Partner

Multidisciplinary study provides scientific underpinnings for accuracy of forensic facial identification.

May 29, 2018



<https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner>

www.nature.com/scientificreports/

scientific reports

OPEN

A comparative analysis of human and AI performance in forensic estimation of physical attributes

Sarah Barrington^{1,3} & Hany Farid^{1,2,✉}

Human errors in criminal investigations have previously led to devastating miscarriages of justice. For example, flaws in forensic identification based on physical or photographic evidence are notoriously unreliable. The criminal justice system has, therefore, started to turn to artificial intelligence (AI) to improve the reliability and fairness of forensic identification. So as not to repeat history, it is critical to evaluate the appropriateness of deploying these new AI forensic tools. We assess the feasibility of measuring basic physical attributes in a photo using a state-of-the-art AI system, and compare performance with human experts and non-experts. Our results raise concerns as to the use of current

“Our results raise concerns as to the use of current AI-based forensic identification.”

Barrington, S., Farid, H. A comparative analysis of human and AI performance in forensic estimation of physical attributes. *Sci Rep* 13, 4784 (2023). <https://doi.org/10.1038/s41598-023-31821-3>

AI and Digital Forensics: An agenda

AI for Digital Forensics

Opportunities:

Make investigators more productive.

- Tool recommendations
- Identify important artifacts
- Correlate information
- Write reports

Needed:

Policies for AI usage and scope.

Validation for bias & error

Digital Forensics for AI

Opportunities:

Understand how AI works and fails

- Pre-deployment certification
- Accountability

Needed:

Improved understanding of:

- How & why deep learning systems work
- How hardware & software interact