FUNDACIÓN RAMÓN ARECES

Digital Evidence
Emerging Challenges

Peter Sommer

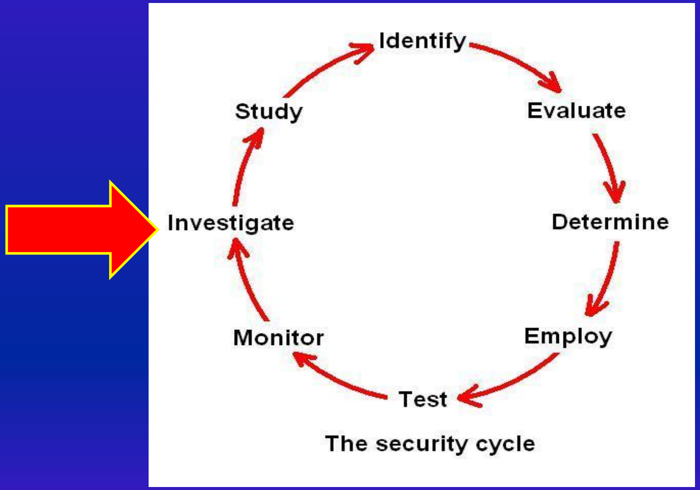
peter@pmsommer.com

Why Digital Evidence?

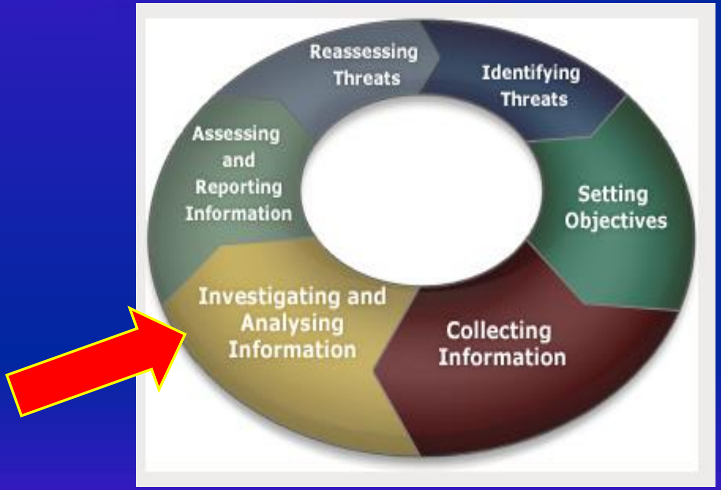
- Within “Cyber Security”: it’s about recovery, loss mitigation, remediation; *not* prevention and detection
- Main needs are:
  - ➔ to be able to prove what events have occurred
  - ➔ to withstand potential litigation
  - ➔ to demonstrate compliance with a regulatory regime
  - ➔ to make successful insurance claims
  - ➔ to assist law enforcement / respond to their requests / respond to court order

Digital Forensics Strategy

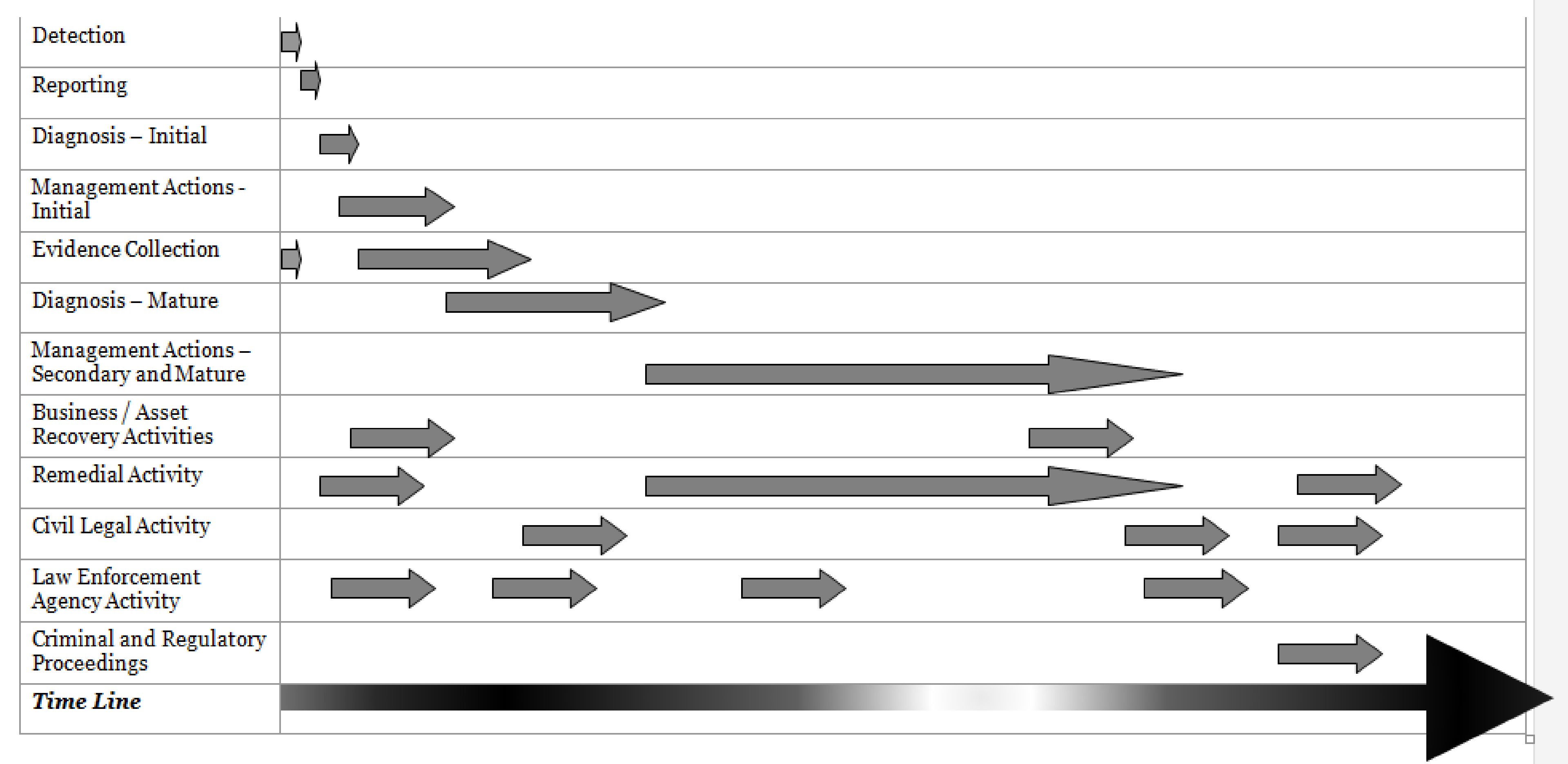
- **Subsidiary aim is:**
  - ➔ After an incident to gather reliable information so that lessons can be learnt - the security cycle



The security cycle



What happens in an “incident”



Detection

Reporting

Diagnosis – Initial

Management Actions - Initial

Evidence Collection

Diagnosis – Mature

Management Actions – Secondary and Mature

Business / Asset Recovery Activities

Remedial Activity

Civil Legal Activity

Law Enforcement Agency Activity

Criminal and Regulatory Proceedings

Time Line

What sorts of incident?

- computer outage
- network failure
- fire
- flood
- terrorism
- employee frauds
- third-party frauds
- blackmail attempts
- data breach
- regulatory breach / accusations of compliance failure
- theft of data and code – industrial espionage / trade secrets

What sorts of incident?

- unauthorised access by employees
- unauthorised access by outsiders
- unauthorised data modification
- denial of service attacks - DDoS
- e-mail and Internet abuse
- online defamation
- employee disputes
- sexual harassment
- acquisition and storage of porn / paedophilia
- use of computer resources as one stage in a complex crime, incl crypto mining
- copyright abuse, piracy

What is evidence?

- Anything which tends to persuade
  - ➔ On the balance of probabilities
  - ➔ Beyond a reasonable doubt
  - ➔ (In practice several different strands of evidence are often brought together)
- Admissibility
  - ➔ Are there laws/rules preventing consideration?
    - Hearsay, illegal acquisition, data protection etc
- Weight
  - ➔ How persuasive?

Corporate Plan

How to plan for evidence collection

- Identification of risk / threat scenarios
- Analysis and identification of likely evidence requirements
- Procedures and resources for sourcing, acquiring and preserving evidence
- Identification of need for additional logging/audit facilities
- Integration with existing BCP, HR, regulatory compliance and legal management structures

Digital Forensic Process

- ***Problem Report,*** ***then dealing with potential evidence:***
- **Identification**
- **Acquisition**
- **Preservation**
- **Analysis**
- **Presentation**

Digital Forensic Process

Identification

Material within your control

- Substantive documents and records
- Deliberately created log and audit files
- Informal records, eg emails
- Unintended but never-the-less reliable artefacts
- Deleted but recoverable instances of any of the above
- Phone / PBX records
- Physical access records (to various buildings, rooms etc)

Material required from others

- Private mobile phones
- Private mobile phone records (of calls, location etc)
- Privately held laptops etc (BYOD)
- Social media and messaging services
- Data held by third parties

Digital Forensic Process

Acquisition

- How to reliably capture the state of a device at a particular time
  - ➔ Freedom from contamination
  - ➔ "Complete"
    - Including the ability to recover deleted and hidden files
  - ➔ Audit trail of activity
- How to reliably capture data in transit at a particular location and time

Digital Forensic Process

Preservation

- Having captured your evidence, how to persuade that it remains unaltered for your examination and for others to examine
  - ➔ Write-once media
  - ➔ Hashing / digital signing
- Audit trail

Digital Forensic Process

Analysis

Presentation

These require specialist tools……

Digital Forensic Tools

Types

- Acquisition / Preservation
- “Evidence Finder” / Kiosks
  - ➔ Useful for quick initial searches
- Advanced – bits and bytes
  - ➔ Hidden data
  - ➔ Data recovery
  - ➔ Complex searches
  - ➔ Examinations at fundamental level
- Big Data / eDiscovery

Digital Forensic Tools

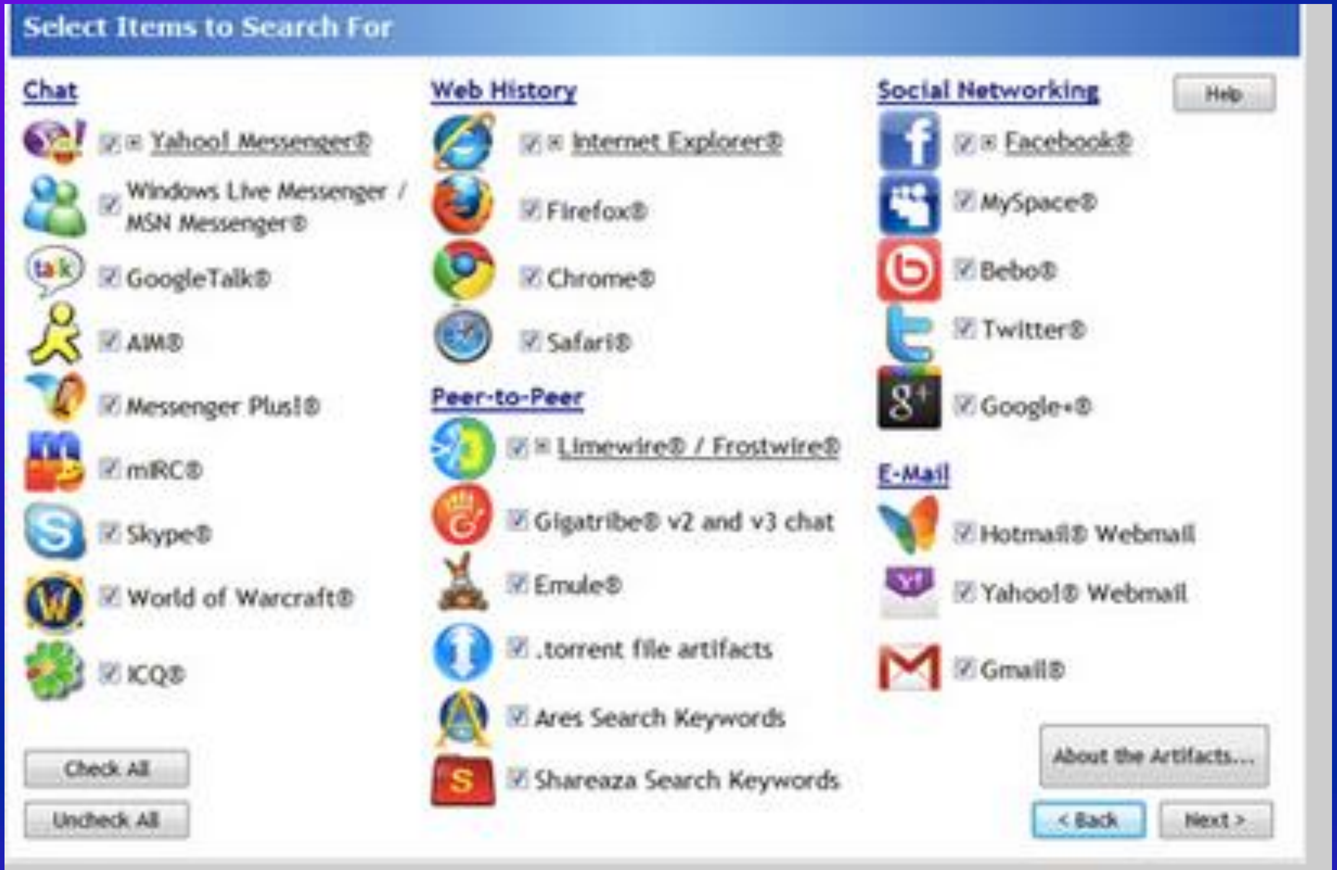
- **Acquisition**
  - Physical / Logical acquisitions
  - Forensic disk imaging
  - Smart phone etc acquisition
  - Big system acquisition
  - Cloud / downloaded social media
- **Preservation**
  - Professional tools usually perform file hashing & create records of their activity

Acquisition

Hardware plus software

Digital Forensic Tools

Evidence Finder Analysis



Select Items to Search For

Chat

- ☑ ⊞ Yahoo! Messenger®
- ☑ Windows Live Messenger / MSN Messenger®
- ☑ GoogleTalk®
- ☑ AIM®
- ☑ Messenger Plus!®
- ☑ mIRC®
- ☑ Skype®
- ☑ World of Warcraft®
- ☑ ICQ®

Web History

- ☑ ⊞ Internet Explorer®
- ☑ Firefox®
- ☑ Chrome®
- ☑ Safari®

Peer-to-Peer

- ☑ ⊞ Limewire® / Frostwire®
- ☑ Gigatribe® v2 and v3 chat
- ☑ Emule®
- ☑ .torrent file artifacts
- ☑ Ares Search Keywords
- ☑ Shareaza Search Keywords

Social Networking

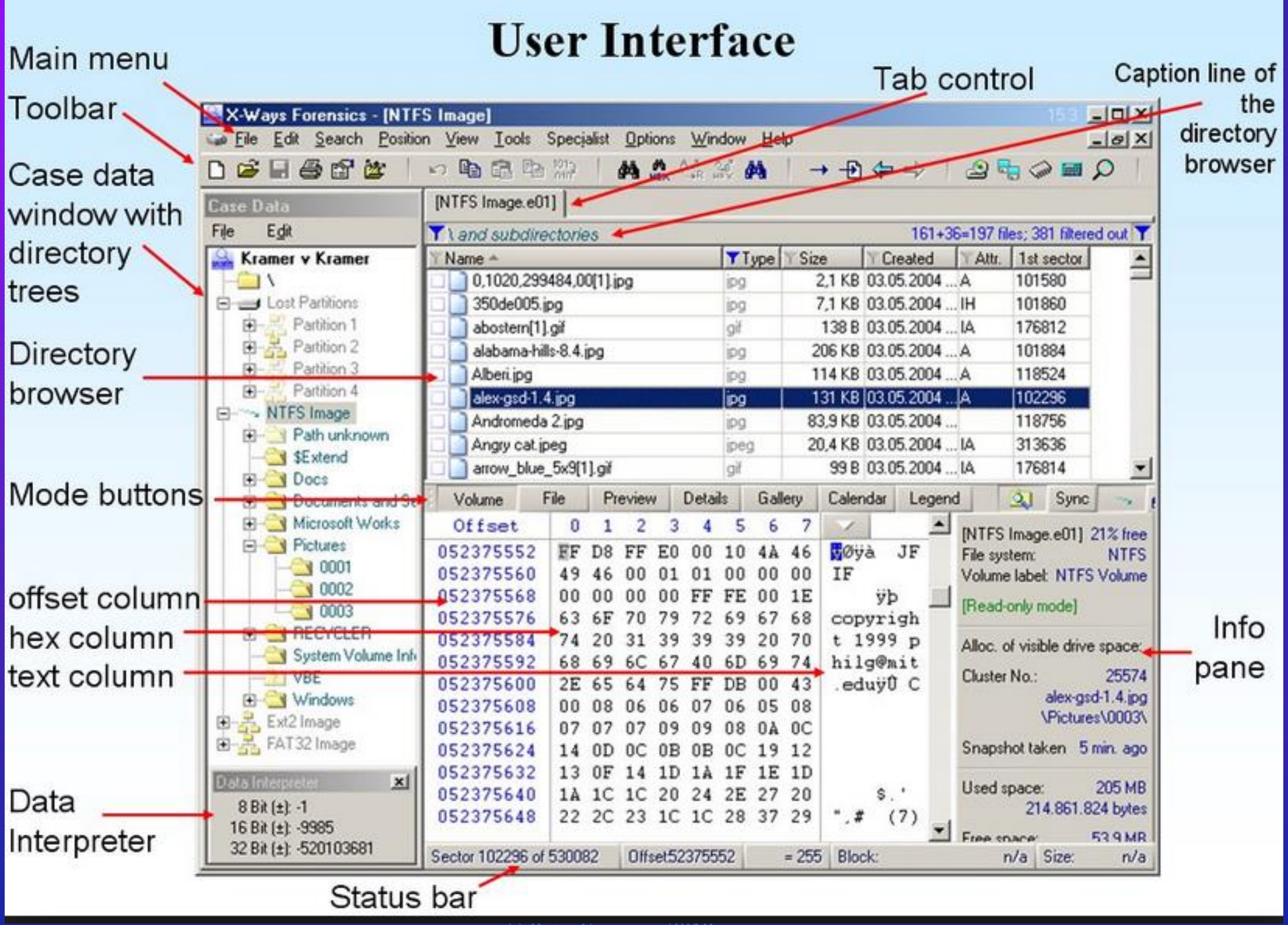
- ☑ ⊞ Facebook®
- ☑ MySpace®
- ☑ Bebo®
- ☑ Twitter®
- ☑ Google+®

E-Mail

- ☑ Hotmail® Webmail
- ☑ Yahoo!® Webmail
- ☑ Gmail®

Digital Forensic Tools

Advanced Analysis



\ and subdirectories

161+36=197 files; 381 filtered out

Name	Type	Size	Created	Attr.	1st sector
0,1020,299484,00[1].jpg	jpg	2,1 KB	03.05.2004 ...	A	101580
350de005.jpg	jpg	7,1 KB	03.05.2004 ...	IH	101860
abostern[1].gif	gif	138 B	03.05.2004 ...	IA	176812
alabama-hills-8.4.jpg	jpg	206 KB	03.05.2004 ...	A	101884
Alberi.jpg	jpg	114 KB	03.05.2004 ...	A	118524
alex-gsd-1.4.jpg	jpg	131 KB	03.05.2004 ...	A	102296
Andromeda 2.jpg	jpg	83,9 KB	03.05.2004 ...		118756
Angry cat.jpeg	jpeg	20,4 KB	03.05.2004 ...	IA	313636
arrow_blue_5x9[1].gif	gif	99 B	03.05.2004 ...	IA	176814

```
 Offset     0  1  2  3  4  5  6  7
052375552  FF D8 FF E0 00 10 4A 46  ÿØÿà  JF
052375560  49 46 00 01 01 00 00 00  IF
052375568  00 00 00 00 FF FE 00 1E      ÿþ
052375576  63 6F 70 79 72 69 67 68  copyrigh
052375584  74 20 31 39 39 39 20 70  t 1999 p
052375592  68 69 6C 67 40 6D 69 74  hilg@mit
052375600  2E 65 64 75 FF DB 00 43  .eduÿÛ C
052375608  00 08 06 06 07 06 05 08
052375616  07 07 07 09 09 08 0A 0C
052375624  14 0D 0C 0B 0B 0C 19 12
052375632  13 0F 14 1D 1A 1F 1E 1D
052375640  1A 1C 1C 20 24 2E 27 20      $.'
052375648  22 2C 23 1C 1C 28 37 29  ",#  (7)
```

[NTFS Image.e01] 21% free
File system: NTFS
Volume label: NTFS Volume
[Read-only mode]

Alloc. of visible drive space:
Cluster No.: 25574
alex-gsd-1.4.jpg
\Pictures\0003\

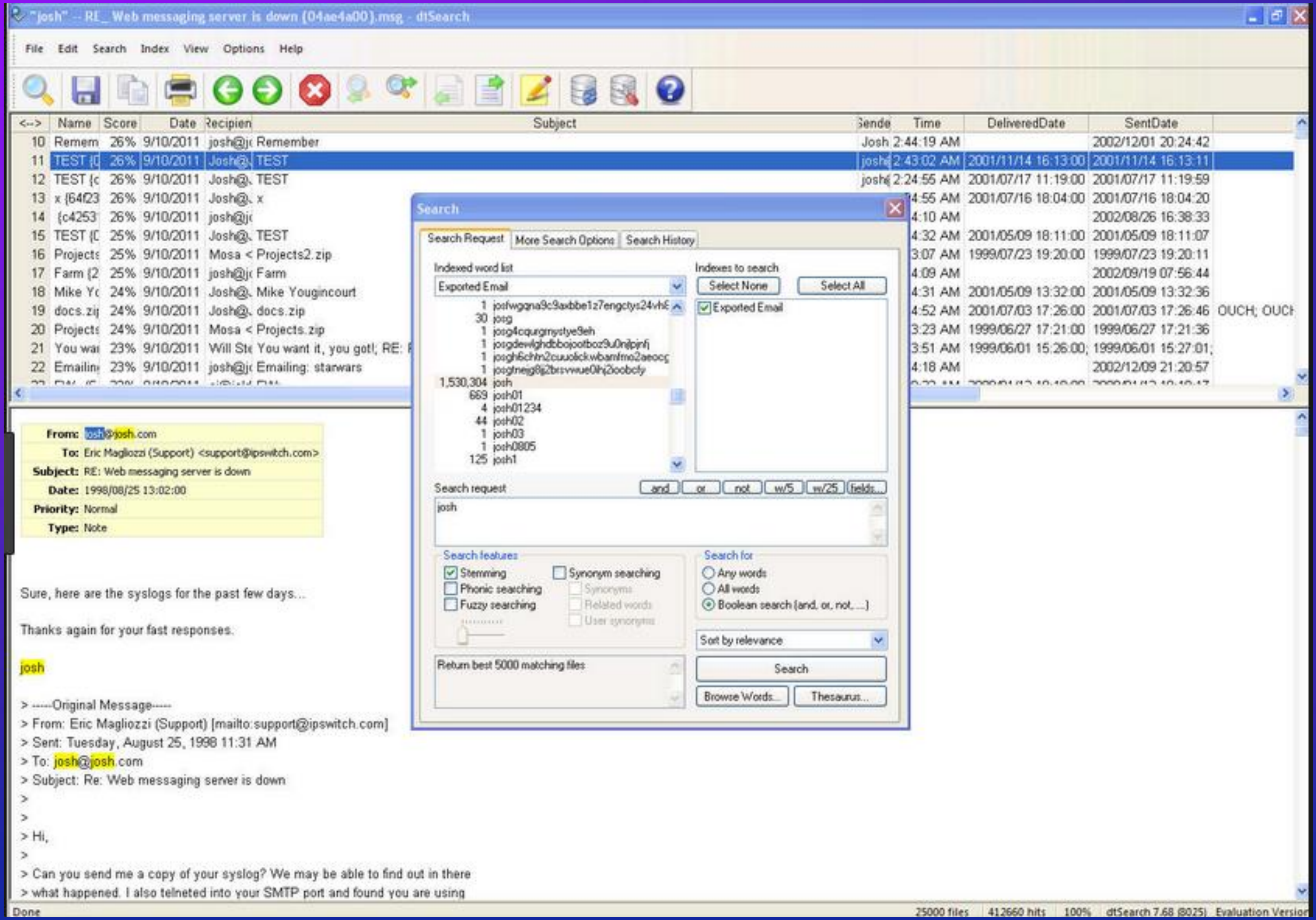
Snapshot taken 5 min. ago

Used space: 205 MB
214.861.824 bytes
Free space: 53.9 MB

Sector 102296 of 530082 | Offset52375552 | = 255 | Block: n/a | Size: n/a

Digital Forensic Tools

Keyword search - Boolean



<-->	Name	Score	Date	Recipien	Subject	Sende	Time	DeliveredDate	SentDate	
10	Remem	26%	9/10/2011	josh@jc	Remember	Josh	2:44:19 AM		2002/12/01 20:24:42	
11	TEST {0	26%	9/10/2011	Josh@.	TEST	joshe	2:43:02 AM	2001/11/14 16:13:00	2001/11/14 16:13:11	
12	TEST {c	26%	9/10/2011	Josh@.	TEST	joshe	2:24:55 AM	2001/07/17 11:19:00	2001/07/17 11:19:59	
13	x {64f23	26%	9/10/2011	Josh@.	x		4:55 AM	2001/07/16 18:04:00	2001/07/16 18:04:20	
14	{c4253	26%	9/10/2011	josh@jc			4:10 AM		2002/08/26 16:38:33	
15	TEST {C	25%	9/10/2011	Josh@.	TEST		4:32 AM	2001/05/09 18:11:00	2001/05/09 18:11:07	
16	Projects	25%	9/10/2011	Mosa <	Projects2.zip		3:07 AM	1999/07/23 19:20:00	1999/07/23 19:20:11	
17	Farm {2	25%	9/10/2011	josh@jc	Farm		4:09 AM		2002/09/19 07:56:44	
18	Mike Yc	24%	9/10/2011	Josh@.	Mike Yougincourt		4:31 AM	2001/05/09 13:32:00	2001/05/09 13:32:36	
19	docs.zij	24%	9/10/2011	Josh@.	docs.zip		4:52 AM	2001/07/03 17:26:00	2001/07/03 17:26:46	OUCH; OUCH
20	Projects	24%	9/10/2011	Mosa <	Projects.zip		3:23 AM	1999/06/27 17:21:00	1999/06/27 17:21:36	
21	You wai	23%	9/10/2011	Will Ste	You want it, you got!; RE: F		3:51 AM	1999/06/01 15:26:00;	1999/06/01 15:27:01;	
22	Emailin	23%	9/10/2011	josh@jc	Emailing: starwars		4:18 AM		2002/12/09 21:20:57	

Indexed word list

Exported Email

1	josfwggna9c9axbbe1z7engctys24vh6
30	josg
1	josg4cqurgmystye9eh
1	josgdewlghdbbojootboz9u0njlpjnfj
1	josgh6chtn2cuuolickwbamfmo2aeocg
1	josgtneig8ij2brsvwue0ihj2ioobcfy
1,530,304	josh
669	josh01
4	josh01234
44	josh02
1	josh03
1	josh0805
125	josh1

Indexes to search

☑ Exported Email

Search request

josh

Search features

☑ Stemming
□ Phonic searching
□ Fuzzy searching
□ Synonym searching
□ Synonyms
□ Related words
□ User synonyms

Search for

○ Any words
○ All words
● Boolean search (and, or, not, ...)

Sort by relevance

Return best 5000 matching files

From: josh@josh.com
To: Eric Magliozzi (Support) <support@ipswitch.com>
Subject: RE: Web messaging server is down
Date: 1998/08/25 13:02:00
Priority: Normal
Type: Note

Sure, here are the syslogs for the past few days...

Thanks again for your fast responses.

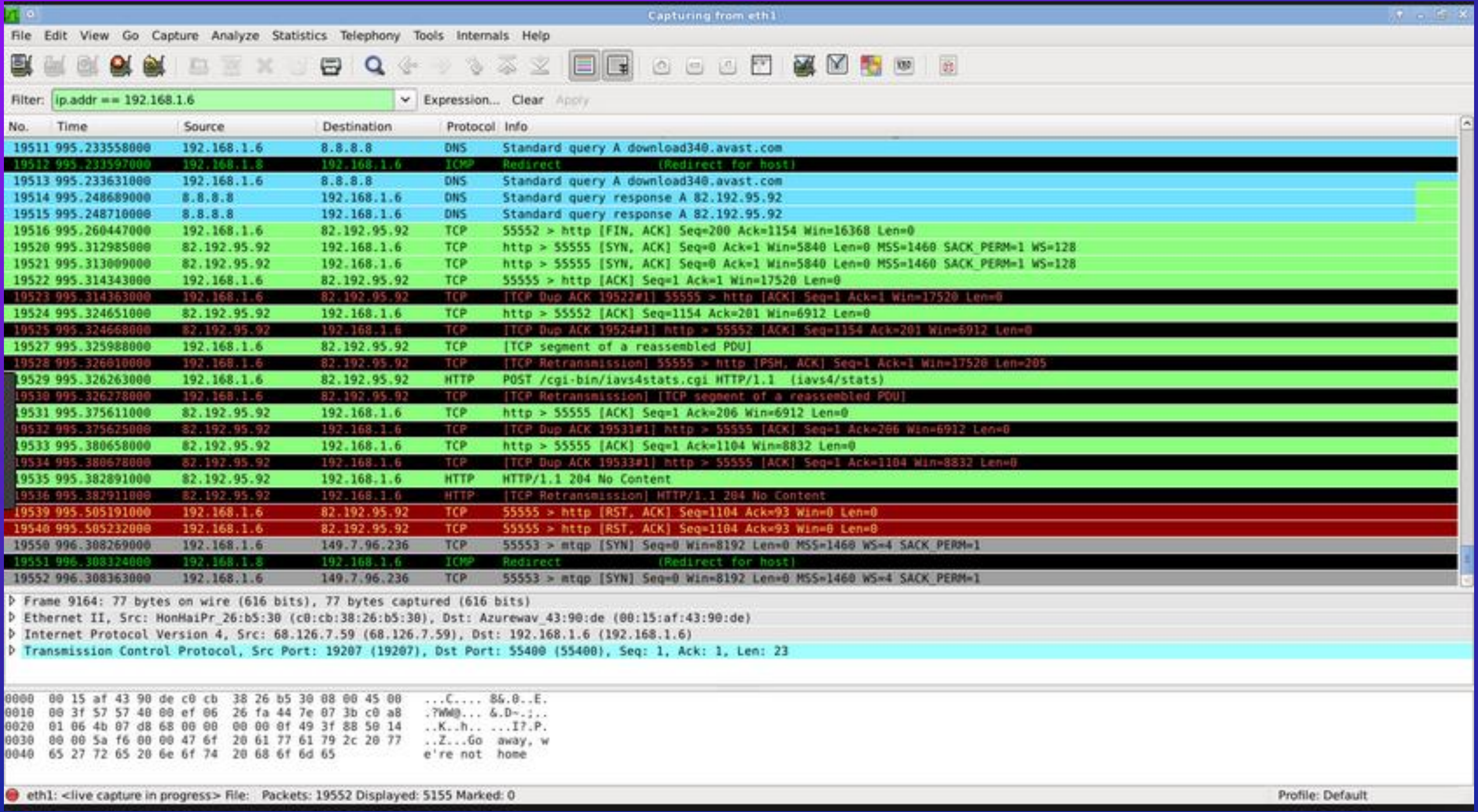
josh

> -----Original Message-----
> From: Eric Magliozzi (Support) [mailto:support@ipswitch.com]
> Sent: Tuesday, August 25, 1998 11:31 AM
> To: josh@josh.com
> Subject: Re: Web messaging server is down
>
>
> Hi,
>
> Can you send me a copy of your syslog? We may be able to find out in there
> what happened. I also telneted into your SMTP port and found you are using

Done | 25000 files | 412660 hits | 100% | dtSearch 7.68 (8025) | Evaluation Version

Digital Forensic Tools

Advanced Analysis – Network Traffic


Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: ip.addr == 192.168.1.6

```
No.   Time          Source         Destination    Protocol Info
19511 995.233558000 192.168.1.6    8.8.8.8        DNS      Standard query A download340.avast.com
19512 995.233597000 192.168.1.8    192.168.1.6    ICMP     Redirect              (Redirect for host)
19513 995.233631000 192.168.1.6    8.8.8.8        DNS      Standard query A download340.avast.com
19514 995.248689000 8.8.8.8        192.168.1.6    DNS      Standard query response A 82.192.95.92
19515 995.248710000 8.8.8.8        192.168.1.6    DNS      Standard query response A 82.192.95.92
19516 995.260447000 192.168.1.6    82.192.95.92   TCP      55552 > http [FIN, ACK] Seq=200 Ack=1154 Win=16368 Len=0
19520 995.312985000 82.192.95.92   192.168.1.6    TCP      http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521 995.313009000 82.192.95.92   192.168.1.6    TCP      http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522 995.314343000 192.168.1.6    82.192.95.92   TCP      55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523 995.314363000 192.168.1.6    82.192.95.92   TCP      [TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524 995.324651000 82.192.95.92   192.168.1.6    TCP      http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525 995.324668000 82.192.95.92   192.168.1.6    TCP      [TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527 995.325988000 192.168.1.6    82.192.95.92   TCP      [TCP segment of a reassembled PDU]
19528 995.326010000 192.168.1.6    82.192.95.92   TCP      [TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529 995.326263000 192.168.1.6    82.192.95.92   HTTP     POST /cgi-bin/iavs4stats.cgi HTTP/1.1  (iavs4/stats)
19530 995.326278000 192.168.1.6    82.192.95.92   TCP      [TCP Retransmission] [TCP segment of a reassembled PDU]
19531 995.375611000 82.192.95.92   192.168.1.6    TCP      http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532 995.375625000 82.192.95.92   192.168.1.6    TCP      [TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533 995.380658000 82.192.95.92   192.168.1.6    TCP      http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534 995.380678000 82.192.95.92   192.168.1.6    TCP      [TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535 995.382891000 82.192.95.92   192.168.1.6    HTTP     HTTP/1.1 204 No Content
19536 995.382911000 82.192.95.92   192.168.1.6    HTTP     [TCP Retransmission] HTTP/1.1 204 No Content
19539 995.505191000 192.168.1.6    82.192.95.92   TCP      55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540 995.505232000 192.168.1.6    82.192.95.92   TCP      55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550 996.308269000 192.168.1.6    149.7.96.236   TCP      55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551 996.308324000 192.168.1.8    192.168.1.6    ICMP     Redirect              (Redirect for host)
19552 996.308363000 192.168.1.6    149.7.96.236   TCP      55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
```

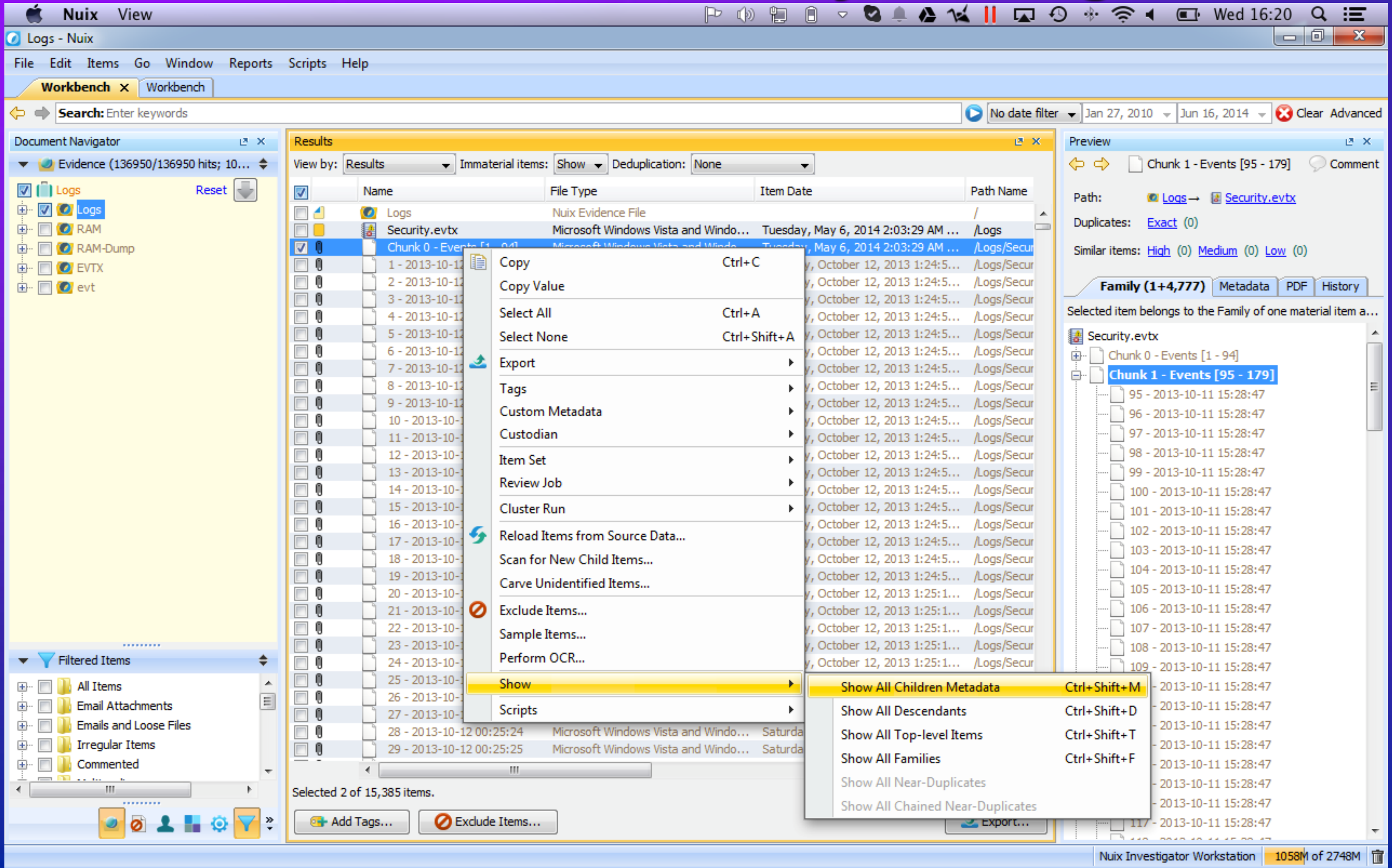
```
▷ Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
▷ Ethernet II, Src: HonHaiPr_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewav_43:90:de (00:15:af:43:90:de)
▷ Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)
▷ Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23
```

```
0000  00 15 af 43 90 de c0 cb  38 26 b5 30 08 00 45 00   ...C.... 8&.0..E.
0010  00 3f 57 57 40 00 ef 06  26 fa 44 7e 07 3b c0 a8   .?WW@... &.D~.;..
0020  01 06 4b 07 d8 68 00 00  00 00 0f 49 3f 88 50 14   ..K..h.. ...I?.P.
0030  00 00 5a f6 00 00 47 6f  20 61 77 61 79 2c 20 77   ..Z...Go  away, w
0040  65 27 72 65 20 6e 6f 74  20 68 6f 6d 65            e're not  home
```

eth1: <live capture in progress> File: Packets: 19552 Displayed: 5155 Marked: 0 Profile: Default

Digital Forensic Tools

Advanced Analysis – Big Data



Search: Enter keywords

Jan 27, 2010 – Jun 16, 2014

Evidence (136950/136950 hits; 10…

- ☑ Logs
  - ☑ Logs
  - □ RAM
  - □ RAM-Dump
  - □ EVTX
  - □ evt

Filtered Items:

- □ All Items
- □ Email Attachments
- □ Emails and Loose Files
- □ Irregular Items
- □ Commented

View by: Results Immaterial items: Show Deduplication: None

☑	Name	File Type	Item Date	Path Name
□	Logs	Nuix Evidence File		/
□	Security.evtx	Microsoft Windows Vista and Windo…	Tuesday, May 6, 2014 2:03:29 AM …	/Logs
☑	Chunk 0 - Events [1 - 94]	Microsoft Windows Vista and Windo…	Tuesday, May 6, 2014 2:03:29 AM …	/Logs/Secur
□	1 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	2 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	3 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	4 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	5 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	6 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	7 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	8 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	9 - 2013-10-12		y, October 12, 2013 1:24:5…	/Logs/Secur
□	10 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	11 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	12 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	13 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	14 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	15 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	16 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	17 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	18 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	19 - 2013-10-		y, October 12, 2013 1:24:5…	/Logs/Secur
□	20 - 2013-10-		y, October 12, 2013 1:25:1…	/Logs/Secur
□	21 - 2013-10-		y, October 12, 2013 1:25:1…	/Logs/Secur
□	22 - 2013-10-		y, October 12, 2013 1:25:1…	/Logs/Secur
□	23 - 2013-10-		y, October 12, 2013 1:25:1…	/Logs/Secur
□	24 - 2013-10-		y, October 12, 2013 1:25:1…	/Logs/Secur
□	25 - 2013-10-			
□	26 - 2013-10-			
□	27 - 2013-10-			
□	28 - 2013-10-12 00:25:24	Microsoft Windows Vista and Windo…	Saturda	
□	29 - 2013-10-12 00:25:25	Microsoft Windows Vista and Windo…	Saturda	

Selected 2 of 15,385 items.

Chunk 1 - Events [95 - 179]

Path: Logs → Security.evtx

Duplicates: Exact (0)

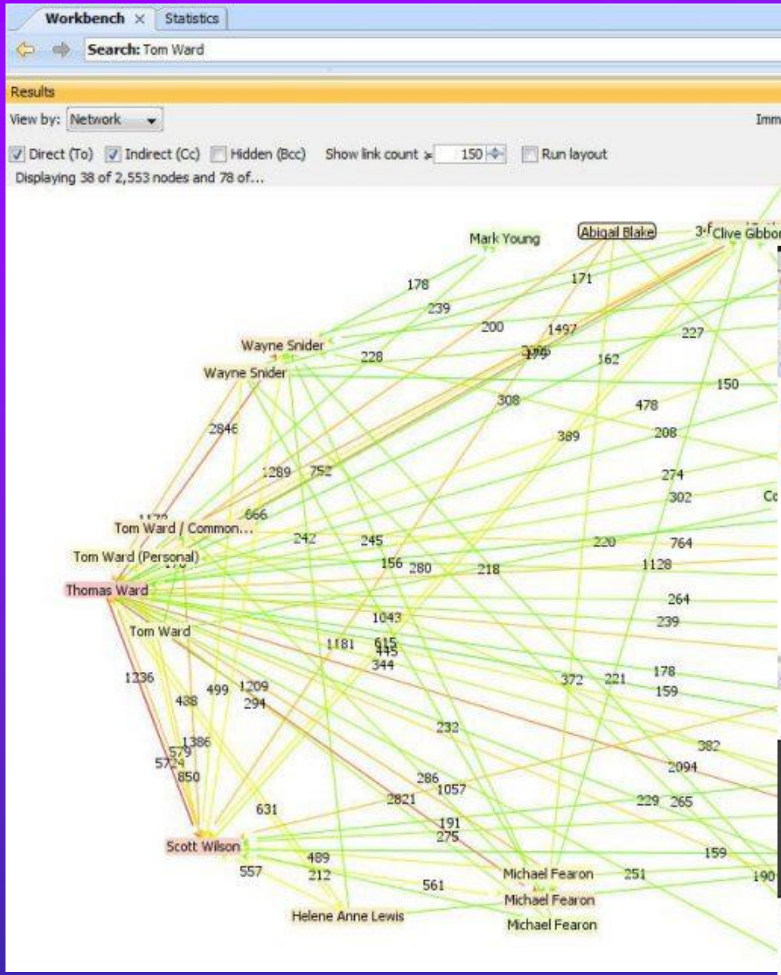
Similar items: High (0) Medium (0) Low (0)

Selected item belongs to the Family of one material item a…

- Security.evtx
  - Chunk 0 - Events [1 - 94]
  - Chunk 1 - Events [95 - 179]
    - 95 - 2013-10-11 15:28:47
    - 96 - 2013-10-11 15:28:47
    - 97 - 2013-10-11 15:28:47
    - 98 - 2013-10-11 15:28:47
    - 99 - 2013-10-11 15:28:47
    - 100 - 2013-10-11 15:28:47
    - 101 - 2013-10-11 15:28:47
    - 102 - 2013-10-11 15:28:47
    - 103 - 2013-10-11 15:28:47
    - 104 - 2013-10-11 15:28:47
    - 105 - 2013-10-11 15:28:47
    - 106 - 2013-10-11 15:28:47
    - 107 - 2013-10-11 15:28:47
    - 108 - 2013-10-11 15:28:47
    - 109 - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 2013-10-11 15:28:47
    - 117 - 2013-10-11 15:28:47

rensic Tools

alysis – Big Data



Workbench × Statistics

Search: Tom Ward

Results

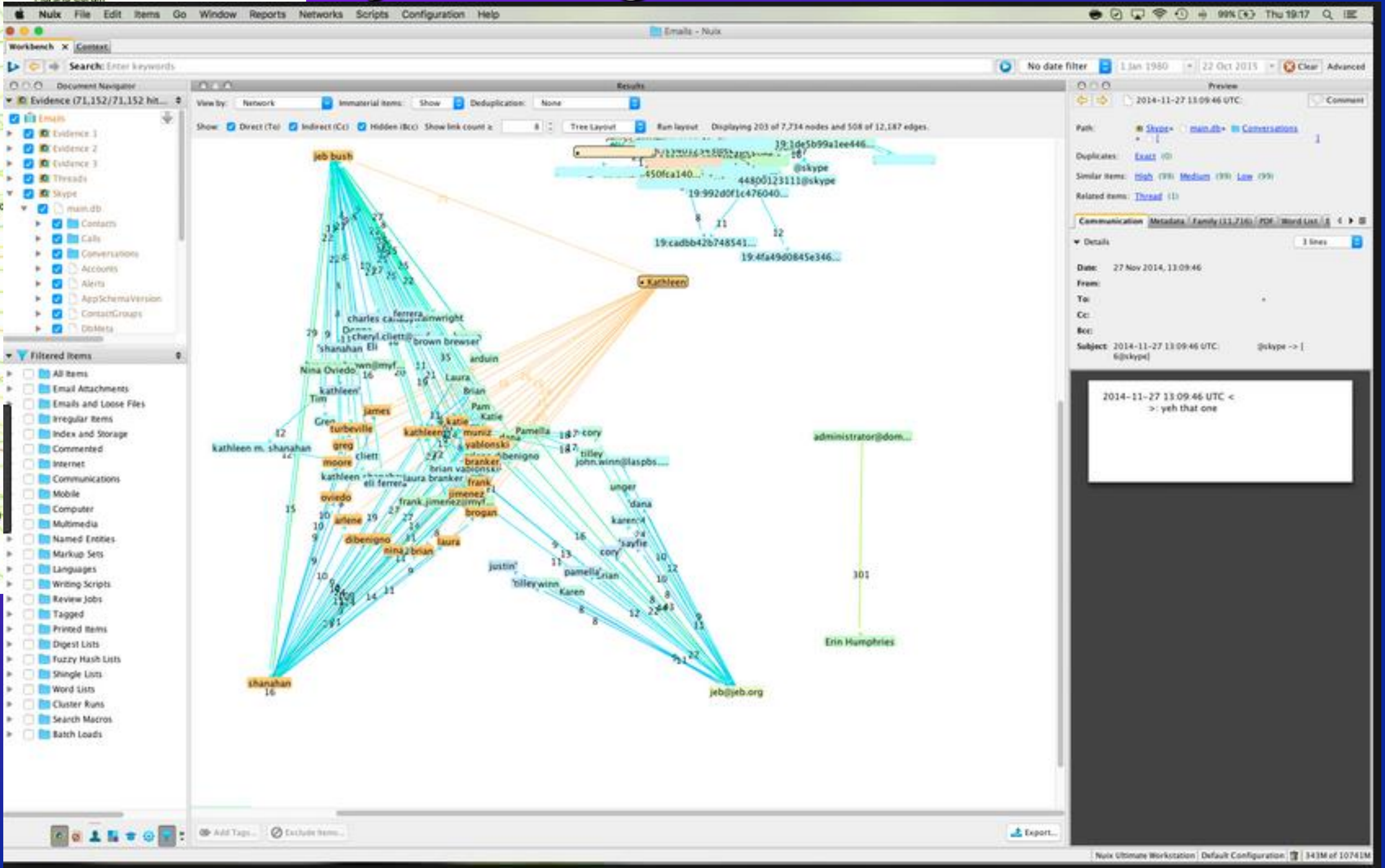
View by: Network

Immaterial items: Show

Deduplication: MD5

☑ Direct (To) ☑ Indirect (Cc) □ Hidden (Bcc) Show link count ≥ 150 □ Run layout

Displaying 38 of 2,553 nodes and 78 of…



Search: Enter keywords

No date filter 1 Jan 1980 22 Oct 2015 Clear Advanced

Results

View by: Network Immaterial items: Show Deduplication: None

Show: ☑ Direct (To) ☑ Indirect (Cc) ☑ Hidden (Bcc) Show link count ≥ 8 Tree Layout Run layout Displaying 203 of 7,734 nodes and 508 of 12,187 edges.

Preview

2014-11-27 13:09:46 UTC:

Path: Skype › main.db › Conversations

Duplicates: Exact (0)

Similar items: High (99) Medium (99) Low (99)

Related items: Thread (1)

Communication Metadata Family (11,716) PDF Word List

Details

Date: 27 Nov 2014, 13:09:46

From:

To:

Cc:

Bcc:

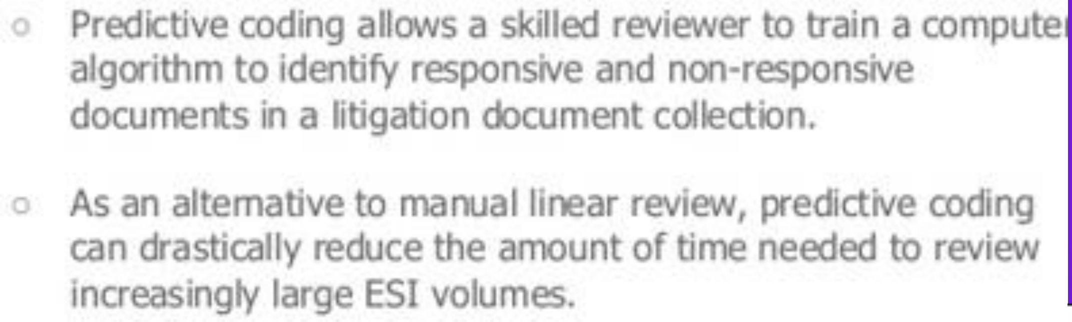
Subject: 2014-11-27 13:09:46 UTC: @skype -> |

2014-11-27 13:09:46 UTC <
>: yeh that one

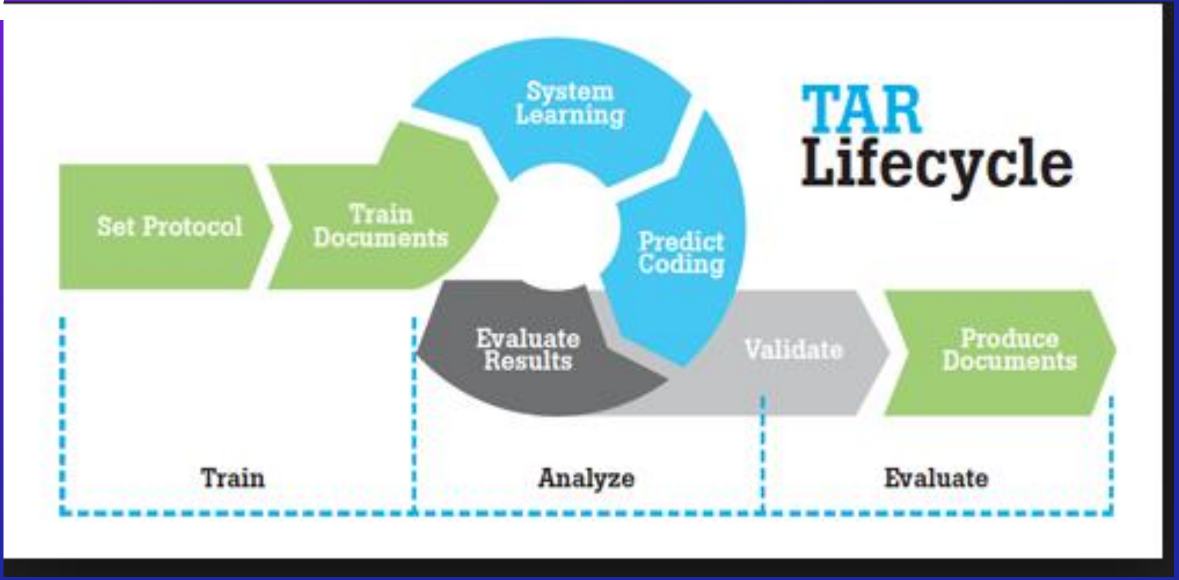
Nuix Ultimate Workstation | Default Configuration | 343M of 10741M

Digital Forensic Tools

Advanced Analysis – Big Data



- Predictive coding allows a skilled reviewer to train a compute algorithm to identify responsive and non-responsive documents in a litigation document collection.
- As an alternative to manual linear review, predictive coding can drastically reduce the amount of time needed to review increasingly large ESI volumes.



"Artificial Intelligence"
Machine Learning

Emerging Challenges

- Capture from Social Media
  - ➔ Facebook, Instagram, etc etc
- Acquisition of evidence from Cloud services
  - ➔ Stored data / Data being processed / where are they located?
- Acquisition from “Dark Web” and other hidden services
- What evidence is there from the Internet of Things?
  - ➔ Many IoT devices are “dumb” – you may have to find their controller
- How would you test an Artificial Intelligence (AI) system you suspected had “misbehaved”?
- Covert investigation & acquisition (law enforcement & intelligence agencies)

Emerging Challenges

- Forensic Science standards – how do we protect the courts from “bad” forensic evidence?
- Some standards for traditional forensic science – ISO 17025 – but this is about the adequacy of laboratories and the tools they use
- In digital forensics:
  - ➔ Fast-changing environment means tools are being constantly updated
  - ➔ DF tools are multi-faceted and complex
  - ➔ Much of the work of experts is in reconstructing events – but ISO 17025 does not directly measure individual expertise and competence
- In the UK: pre-trial meetings between opposing experts

Legal Aspects

- Civilian Powers
- Law Enforcement / Intelligence Agency Powers

Legal Aspects

Civilian Powers

- Powers to investigate your own systems
  - ➔ Usually not difficult
- Powers to investigate your own staff
  - ➔ Depends on employment contract, human rights, data protection
- Powers to investigate a potential external threat
  - ➔ May involve committing a crime
- Powers to acquire evidence from third parties (voluntarily)
  - ➔ Usually not difficult but there may be Data Protection issues
- Powers to acquire evidence from third parties (who don’t want to co-operate)
  - ➔ Court order!

Legal Aspects

Law Enforcement / Intelligence Agency Powers

What types of warrant / authorisation ?

- Powers to seize computers / devices
- Powers to require production of files etc
- Powers to intercept
- Powers to acquire communications data
  - ➔ Who called whom, when, for how long, from which location, which IP address, what internet application – but *NOT* content
- Powers to "hack" (equipment interference, network compromise / exploitation)

Legal Aspects

Some problems

- Civilian:
  - ➔ Disclosure / Discovery
  - ➔ Privacy / Data Protection
  - ➔ Commercial secrets
- Law enforcement agencies
  - ➔ Disclosure of collected evidence
  - ➔ Disclosure of sensitive methods
- Intelligence Agencies
  - ➔ Disclosure of sensitive methods
  - ➔ Concealment of discovered vulnerabilities (the “equities” problem)

Legal Aspects

Evidence from overseas

- Law enforcement
  - Joint investigations
  - Letters of request
  - Mutual Legal Assistance Treaties (MLATs)
  - Trans-jurisdictional Production Orders legislation (to come?)
  - International cyber police (sovereignty?)
- Civilians
  - Overseas businesses will need to comply with their local laws – privacy, free speech etc etc
  - Starting proceedings in foreign courts is expensive and may not be productive

7-step Forensic Readiness Plan

Identify:

- the main likely threats faced by your organisation
- what sorts of evidence you are likely to need if you have to proceed to civil or criminal litigation
- how far you may have that evidence already
- what you will need to do to secure additional essential evidence
- legal issues
- the management, skills and resources implications for your organisation

Peter Sommer

peter@pmsommer.com

www.pmsommer.com