



**The Malicious Exploitation of Information Systems:  
Preventing the Rise of the Insider Threat**

**6-7 November 2008, UCL**

**Issues in the Technologies of  
Digital Investigation**

**Peter Sommer**

**London School of Economics, Open University**

**[peter@pmsommer.com](mailto:peter@pmsommer.com)**

**[p.m.sommer@lse.ac.uk](mailto:p.m.sommer@lse.ac.uk)**



# Incidents

- **Frauds by employees and 3<sup>rd</sup> parties**
- **Contractual disputes**
- **Allegations of failure of duty of care**
- **E-mail and Internet abuse**
- **Breach of confidentiality**
- **Online defamation**
- **Employee / HR disputes**
- **Sexual harassment**
- **Acquisition and storage of child abuse images**
- **Datatheft / Industrial Espionage**
- **Software piracy**
- **Theft of source code**

# Incidents

- Unauthorised access by employees
- Unauthorised access by 3<sup>rd</sup> parties – “hacking”
- Unauthorised data modification – incl viruses and trojans
- Abuse of corporate IT resources for private gain
- Use of corporate IT resources as one stage in a complex criminal act and where a 3<sup>rd</sup> party is victimised
- Use of corporate IT resources for illegal file-sharing
- DoS and DdoS attacks
- “Phishing” and “Pharming” attempts
- Etc etc
- **Requirements of disclosure in civil litigation**

# Incidents

- **Rare, Spectacular Events**
- **Events that occur everywhere to everyone... but still cause panic, distress, loss**
- **High Impact / Low Frequency**
- **High Frequency / Individually, Medium-to-Low Impact**

# Something suspicious is happening in and around your computer systems...

- What do you do?
- Where do you find help?
- How do you assess the investigator market?
- Is the person you want available?
- What are you really asking them to do?
- Is it going to be enough?

# **The Insider Threat: The Investigator's Perspective**

- **What are the suspicions?**
- **How likely is it that the client has mis-interpreted the situation?**
- **What powers do I have?**
  - I start out with no powers, I need to acquire them from the client
- **Now to try and locate evidence ...**

# The Investigator's Perspective

- **Now to try and locate evidence ...**
- **How does the client's organisation work?**
  - What functions does it perform?
  - How do I relate business functions to bits of hardware, software, computer records?
- **Given the suspicions, what should I go for?**
  - Transaction records
  - Emails
  - Web usage
  - Contents of PC, laptop, mobile phone, PDA, memory sticks, etc

# The Investigator's Perspective

- **Are there any restrictions on my access?**
  - Client authorisation as employer
  - Limits on employer's powers
    - Human Rights Act 1998
    - Data Protection Act,
    - Protection from Harassment Act, 1997
    - Regulation of Investigatory Powers Act 2000
      - Telecommunications (Lawful Business Practice)  
(Interception of Communications) Regulations 2000
  - Computer Misuse Act 1990
    - as amended



# The Investigator's Perspective

- Are there any restrictions on my access?
- Penalties for breach of powers:
  - Criminal
  - Abuse of Process
  - Admissibility
  - Harassment
  - Etc etc

# The Investigator's Perspective: Technologies

- **PCs**

- Make reliable complete copy (“forensic image”) and analyse
  - Obvious, visible records, emails, Internet activity
  - Recovery of deleted data
  - Chronologies of activities
- Now standard procedures, products, training
- Imaging can be done covertly over night

File Edit View Tools Help

New Open Save Print Add Device Search Refresh Show Excluded Show Deleted Delete View Email Email/Internet Search To Filter Display

Cases Table Report Gallery Timeline Disk Code

Home Bookmarks Search Hits

Email History WebCache

Secure Storage Keywords

Home Attachments

Email

- Parker's HDD
  - Hotmail
  - Outlook Express
- Clyde's HDD
  - Hotmail
  - Outlook Express
- Fiske
  - Yahoo!
  - Outlook
- Hunter XP
  - Hotmail
  - Outlook Express
  - AOL
    - chaser 1191
      - Incoming/Saved Mail
      - Mail Waiting To Be Sent
      - Mail You've Sent
      - Mail
      - Girls
    - chaser 1191
      - Incoming/Saved Mail
      - Mail You've Sent
      - Mail

	Name	From	To	Subject	Created	Sent
1	Re: If you love your daughter	billyray150@hotmail.com	Chaser1191@aol.com	Re: If you love your daughter		06/03/02 11:47:39AM
2	Re: Your Daughters Safety Depends on This!!!	billyray150@hotmail.com	Chaser1191@aol.com	Re: Your Daughters Safety Depends on This!!!		06/03/02 10:33:32AM
3	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
4	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
5	Returned mail: User unknown	MAILER-DAEMON@aol.com	Chaser1191@aol.com	Returned mail: User unknown		05/14/02 10:09:32AM
6	Criminal Defense Lawyers - California Criminal...	billyray150b@netscape.net	chaser1191@aol.com	Criminal Defense Lawyers - California Criminal...		05/23/02 07:09:31AM
7	Welcome to My Calendar	AOLMyCalendar@aol.com	chaser1191@aol.com	Welcome to My Calendar		04/18/02 01:11:51PM
8	Re: Next few days	billyray150@hotmail.com	Chaser1191@aol.com	Re: Next few days		04/03/02 08:35:03AM
9	Re: you gotta see this one	billyray150@hotmail.com	Chaser1191@aol.com	Re: you gotta see this one		04/03/02 08:29:34AM
10	Re: Time Test	billyray150@hotmail.com	Chaser1191@aol.com	Re: Time Test		04/03/02 08:28:39AM
11	Re: (no subject)	billyray150@hotmail.com	Chaser1191@aol.com	Re: (no subject)		04/03/02 08:27:47AM
12	Re: xdrive	billyray150@hotmail.com	Chaser1191@aol.com	Re: xdrive		04/03/02 08:26:55AM
13	Re: Instant Messaging	billyray150@hotmail.com	Chaser1191@aol.com	Re: Instant Messaging		04/03/02 08:25:59AM
14	Re: http://www.xdrive.com/page.cfm?name=...	billyray150@hotmail.com	Chaser1191@aol.com	Re: http://www.xdrive.com/page.cfm?name=...		04/03/02 08:25:10AM
15	Re: (no subject)	billyray150@hotmail.com	Chaser1191@aol.com	Re: (no subject)		04/03/02 08:23:52AM
16	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
17	Re: Instant Messaging	billyray150@hotmail.com	Chaser1191@aol.com	Re: Instant Messaging		04/03/02 08:25:59AM
18	Re: xdrive	billyray150@hotmail.com	Chaser1191@aol.com	Re: xdrive		04/03/02 08:26:55AM
19	Delivery Status Notification (Failure)	postmaster@guidancesoftware.com	Chaser1191@aol.com	Delivery Status Notification (Failure)		06/03/02 09:17:30AM
20	Re: Your Daughters Safety Depends on This!!!	billyray150@hotmail.com	Chaser1191@aol.com	Re: Your Daughters Safety Depends on This!!!		06/03/02 10:33:32AM
21	Welcome to My Calendar	AOLMyCalendar@aol.com	chaser1191@aol.com	Welcome to My Calendar		04/18/02 01:11:51PM
22	Re: Next few days	billyray150@hotmail.com	Chaser1191@aol.com	Re: Next few days		04/03/02 08:35:03AM
23	Re: you gotta see this one	billyray150@hotmail.com	Chaser1191@aol.com	Re: you gotta see this one		04/03/02 08:29:34AM
24	Re: Time Test	billyray150@hotmail.com	Chaser1191@aol.com	Re: Time Test		04/03/02 08:28:39AM
25	Re: (no subject)	billyray150@hotmail.com	Chaser1191@aol.com	Re: (no subject)		04/03/02 08:27:47AM

Text Hex Picture Report Console Details Lock 12932/62665

Attachments: NO  
 From: billyray150@hotmail.com  
 To: Chaser1191@aol.com  
 Subject: Re: xdrive

EnScripts Filters Conditions Queries

- Conditions
  - Email Filter Condition
    - To Filter

Case 1\Hunter XP\C\Program Files\America Online 7.0\organize\chaser 1191\AOL Personal Filing Cabinet\Chaser 1191\Mail\Incoming\Saved Mail\Re: xdrive (chaser 1191: PS 29323 LS 29323 CL 29323 SO 000 FO 0 LE 0)





EnCase Version 3 - [Case1.cas]

File Edit View Tools Window Help

New Open Save Add Preview Acquire Back Forward Prev Next Search EScript

Case Bookmarks Keywords 0

Volume D

- ACADEMIC
- Alibhai
- Best Practice
- BThompson
- Cooper

	File Name	Short Name	File Ext	Description	Is Deleted	Is Bookmarked	Last Accessed	Last Written
1	cipr	CIPR		Folder			10/03/01	10/03/01 12:42
2	EIF	EIF		Folder			10/03/01	10/03/01 12:41
3	HnC	HOC		Folder			10/03/01	10/03/01 12:41

Text Hex Report Picture Disk Evidence Lock PS 100630 LS 100630 CL 9077 SO 0 FO 0 LE 1

00100448  
00100480  
00100512  
00100544  
00100576  
00100608  
00100640  
00100672  
00100704  
00100736  
00100768  
00100800  
00100832  
00100864  
00100896  
00100928  
00100960  
00100992  
00101024  
00101056  
00101088  
00101120  
00101152  
00101184  
00101216  
00101248  
00101280  
00101312  
00101344  
00101376  
00101408  
00101440  
00101472  
00101504  
00101536  
00101568  
00101600  
00101632

Text Hex Sector View: 512 BPS

000 ...BeC+C+..CeC+u#..... ..BeC+C+..CeC+U...  
062 ..AF.i.n.a.l...o..d.o.c...yy..yyyyFINAL DOC ..BeC+C+..\*xfav#  
124 ./...Cp.e.n. .G....o.v...d.o.c....yy. -. .O.m...b.u.d.s.a.n.  
186 .. .O..J.e.r.e.m...y. .C.o.r.b...y.n.JEREMY~1DOC .0BeC+C+..Nx  
248 f6'#...Cc...yyyyyy...yyyyyyyyyy...yyyy.h.n. .C.o...l.m.a.n.  
310 s....d.o..O.m.b.u.d...s.a.n. -. ...J.o.OMBUDS~1DOC .WBeC+C+  
372 ..Nxf6\$#.E..C..d.o.c....(yyyyyyyyyy...yyyy.l.v.i.n.d... (e.r.  
434 .B.a.n...g.a..O.m.b.u.d... (s.a.n. -. ...B.a.OMBUDS~2DOC .\_Be  
496 C+C+...xfac#..."

Volume D\cryptofiles\cipr



EnCase Version 3 - [Case1.cas]

File Edit View Tools Window Help

New Open Save Add Preview Acquire Back Forward Prev Next Search EScript

Case Bookmarks Keywords 1

Case

- Volume D
  - ACADEMIC
  - Alibhai
  - Best Practice
  - BThompson
  - Cooper
  - CPS Training
  - cryptofiles
  - Darren Guest
  - DTHEFT
  - EU
  - EU Safer Internet
  - FORENS
  - HAKPROGS
  - Howe\_Paul
  - Hussain\_Altaf
    - IL89915
    - New Folder
    - th51nw1004
    - th63beu1020
    - th67beu1002
    - th71nw1000
    - tw36rechw1003
  - IAAC
  - Ibbertson
  - IBM600
  - INFOVAR
  - ISPY
  - JOURNAL
  - LAWFILES
  - LCD Civil Rules

Table Gallery Timeline Report

## EnCase Report

Case: Case1 Page 1

This computer was previewed on 05/13/02 03:11:50PM. The computer system clock read: 05/13/02 03:11:51PM.

**Drive Geometry:**  
Total Size 6.8GB (14,348,817 sectors)

**Volume "Volume D" Parameters**

File System:	FAT32	Drive Type:	Fixed
Sectors Per Cluster:	8	Bytes Per Sector:	512
Total Sectors:	14,348,817	Total Capacity:	7,332,241,408 bytes (6.8GB)
Total Clusters:	1,790,098	Unallocated:	5,792,677,888 bytes (5.4GB)
Free Clusters:	1,414,228	Allocated:	1,539,563,520 bytes (1.4GB)
Volume Name:		Volume Offset:	0
OEM Version:	MSWIN4.1	Volume Serial #:	0000-0000
Heads:	240	Sectors Per Track:	63
Unused Sectors:	3,084,543	Number of FATs:	2
Sectors Per FAT:	13,999	Boot Sectors:	32

Volume D

- ACADEMIC
- Alibhai
  - soans
    - bookmarks
    - Folder Settings
    - PDF
    - ali
    - assists
- ociety - Intellectual Property\_files
  - iec1508\_files
  - Methodology
  - Procedures
    - NCIS
  - Proposals
  - Reliability etc
  - sol wkingpty
  - Shrivenham
- \_files
  - isdn directive
  - RIP
    - House of Commons - Explanatory
    - Note\_files
    - Regulation of investigatory Powers
    - Bill02\_files
  - woolf
  - LCD Civil Rules

Text Hex Report Picture Disk Evidence Lock PS 2004742 LS 2004742 CL 247091 SO 0 FO 0 LE 1

Volume D\ACADEMIC

EnCase Version 3 - [Case1.cas]

File Edit View Tools Window Help

New Open Save Add Preview Acquire Back Forward Prev Next Search EScript

Case Bookmarks Keywords 1

Alibhai  
Best Practice  
BThompson  
Cooper  
CPS Training  
cryptofiles  
Darren Guest  
DTHEFT  
EU  
EU Safer Internet  
FORENS  
ARTICLES  
Biblos  
Book  
Carnivore

	File Name	Is Bookmarked	Last Accessed	Last Written	File Created	Entry Modified
20	Computer Evid...		05/06/02	05/07/97 12:33:10PM	10/16/01 05:35:32PM	
21	CrimLR01.doc		10/16/01	03/29/00 10:52:58AM	10/16/01 05:35:44PM	
22	CrimLR01.exe		02/15/02	11/06/98 05:22:56PM	10/16/01 05:35:38PM	
23	CrimLR01.PDF		10/16/01	10/07/98 11:12:50AM	10/16/01 05:35:44PM	
24	crimlrinv01.doc		10/16/01	01/18/99 11:02:42AM	10/16/01 05:35:44PM	
25	Delhi01.doc		10/16/01	07/28/97 10:03:26AM	10/16/01 05:35:32PM	
26	Delhi02.doc		10/16/01	10/06/99 11:08:44AM	10/16/01 05:35:34PM	
27	Demise_s69.txt		10/16/01	04/03/00 08:15:50PM	10/16/01 05:35:46PM	
28	DIVA.txt		10/16/01	04/03/00 08:17:24PM	10/16/01 05:35:46PM	
29	dload.zip		10/16/01	05/01/98 08:06:48AM	10/16/01 05:35:36PM	

Text Hex Report Picture Disk Evidence Lock PS 2521926 LS 2521926 CL 311739 SO 0 FO 0 LE 1

000000 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441



**EnCase Version 3 - [Case1.cas]**

File Edit View Tools Window Help

New Open Save Add Preview Acquire Back Forward Prev Next Search EScript

Case Bookmarks Keywords 1

- [-] HAKPROGS
- [-] Howe\_Paul
- [+] Hussain\_Altaf
  - [+] IL89915
  - [-] New Folder
  - [-] th51nw1004
  - [-] th63beu1020
  - [-] th67beu1002
  - [-] th71nw1000
  - [-] tw36reclw1003
- [-] IAAC
- [-] Ibbertson
- [-] IBM600
- [-] INFOVAR
- [-] ISPY
- [-] JOURNAL
- [-] LAWFILES
- [-] LCD Civil Rules
- [-] LSE
- [-] NCIS
- [-] PCX
- [-] pmscv\_files
- [-] Powerpoint Present
- [-] Proxim
- [-] QUOTES
- [-] RADIO
- [-] RAWFILES
- [-] RECYCLED

Table	Gallery	Timeline	Report
<input type="checkbox"/> (13) digisat01...	<input type="checkbox"/> (14) digisat01...	<input type="checkbox"/> (15) diskplats....	<input type="checkbox"/> (16) fatdisk1....
<input type="checkbox"/> (19) hp1.pcx	<input type="checkbox"/> (20) Image2.pcx	<input type="checkbox"/> (21) jmajor.pcx	<input type="checkbox"/> (22) LSELOGO...
<input type="checkbox"/> (25) pacesat0...	<input type="checkbox"/> (26) PMS.PCX	<input type="checkbox"/> (27) PM51.PCX	<input type="checkbox"/> (28) PM5SIG....
<input type="checkbox"/> (31) ukrew.bmp	<input type="checkbox"/> (32) vca.pcx	<input type="checkbox"/> (33) VCAL.PCX	<input type="checkbox"/> (34) VCAR.PCX

Volume D:\PCX\jmajor.pcx



NetAnalysis - Forensic Internet History Analysis - [Massive.net]				
File Filter Exclude Investigate Search Tools Reports View Column Help				
Record URN: 10739				
Type	Last Visited [GMT]	Secondary Date	User	Internet History
FTP	02/16/2002 09:17:14 Sat		Administrator	ftp://dmares.com/pub/nt_32/compare.exe
FTP	02/16/2002 09:17:58 Sat		Administrator	ftp://dmares.com/pub/help_s/compare.hlp
News	05/26/2002 14:07:07 Sun	05/27/2002 06:58:18 Mon	Administrator	news://news.jrsoftware.org/jrsoftware.innosetup
URL	06/01/2002 20:53:55 Sat	06/01/2002 21:53:55 Sat	Administrator	http://www.guidancesoftware.com/cgi/ultimatebb.cgi
File	09/19/2002 19:16:09 Thu		Administrator	file:///D:/NetAnalysis1.14.3/NetAnalysis.vbp
Host	06/01/2002 08:00:43 Sat	06/01/2002 09:00:43 Sat	Administrator	Host: www.guidancesoftware.com
URL	06/01/2002 20:50:12 Sat	06/01/2002 21:50:12 Sat	Administrator	http://www.digital-detective.co.uk
URL	06/01/2002 20:54:16 Sat	06/01/2002 21:54:16 Sat	Administrator	http://www.guidancesoftware.com/cgi/ultimatebb.cgi?ubb=get_profile;u=000000
Host	06/01/2002 08:02:29 Sat	06/01/2002 09:02:29 Sat	Administrator	Host: www.digital-detective.co.uk
URL	06/01/2002 20:48:04 Sat	06/01/2002 21:48:04 Sat	Administrator	http://www.digital-detective.co.uk/cgi-bin/digitalboard/YaBB.pl
Host	06/01/2002 12:53:24 Sat	06/01/2002 13:53:24 Sat	Administrator	Host: www.google.com
News	06/01/2002 13:34:07 Sat	06/01/2002 14:34:07 Sat	Administrator	news://news.mvps.org/ccrp.binaries.examples
Host	06/01/2002 13:34:07 Sat	06/01/2002 14:34:07 Sat	Administrator	Host: news.mvps.org
Host	06/01/2002 13:43:58 Sat	06/01/2002 14:43:58 Sat	Administrator	Host: www2.verisign-direct.com
URL	06/01/2002 20:53:47 Sat	06/01/2002 21:53:47 Sat	Administrator	http://www.guidancesoftware.com/cgi/ultimatebb.cgi?ubb=forum&f=1
Mail	05/21/2002 07:47:22 Tue		Administrator	mailto:craig.wilson@digital-detective.co.uk
Java	05/28/2002 16:50:48 Tue		Administrator	javascript:DoConfirm('Are you sure you want to delete this
Java	05/28/2002 20:44:26 Tue		Administrator	javascript:void(0)
Res	06/01/2002 14:44:08 Sat		Administrator	res://C:\WINNT\System32\shdoclc.dll/dnserror.htm
Help	06/01/2002 18:36:49 Sat		Administrator	mk:@MSITStore:C:\Program%20Files\Microsoft%20Visual%20Stu
Cookie	06/01/2002 20:47:41 Sat		administrator	Cookie: administrator@www.guidancesoftware.com/
Res	06/01/2002 16:49:59 Sat		Administrator	res://C:\WINNT\System32\shdoclc.dll/navcancel.htm
Cookie	06/01/2002 16:52:14 Sat		administrator	Cookie: administrator@webcrawler.com/
URL	06/01/2002 18:42:05 Sat	11/22/2001 02:35:45 Thu	administrator	http://www.google.com/images/res0.gif
URL	06/01/2002 18:42:05 Sat	11/22/2001 02:35:45 Thu	administrator	http://www.google.com/images/res3.gif
URL	06/01/2002 18:42:05 Sat	11/22/2001 02:36:09 Thu	administrator	http://www.google.com/nav_first.gif
URL	06/01/2002 18:42:05 Sat	11/22/2001 02:36:09 Thu	administrator	http://www.google.com/nav_current.gif
URL	06/01/2002 18:42:05 Sat	11/22/2001 02:36:09 Thu	administrator	http://www.google.com/nav_next.gif
Secure	06/01/2002 09:43:23 Sat	05/10/2001 16:07:08 Thu	administrator	https://www.infragistics.com/images/menus/search_off.gif
Secure	06/01/2002 09:43:23 Sat	05/10/2001 16:12:48 Thu	administrator	https://www.infragistics.com/images/menus/cart_off.gif
www.digital-detective.co.uk TAG Type: History Source: Unallocated... Offset: 13969966 URL Records: 103284				

# The Investigator's Perspective

- **Main systems**

- Full imaging likely to be technically difficult
- Imaging is easier on a system taken off-line
  - But then the business is no longer functioning
- Partial copying runs risk that it shows an incomplete picture of events
- How far do existing back-up/archiving systems assist?
- How do I limit my examination so as not compromise the rights of third parties?
  - Employees, customers, clients

# The Investigator's Perspective

- **Subsidiary systems**
  - Eg small specialist sub-systems
  - PDAs, laptops, cellphones, memory sticks, media players etc
  - Can we identify?
  - May be disputes over ownership, expectations of privacy
  - Some devices may be technically difficult to examine

# The Investigator's Perspective

- **On-going suspicions: “live” investigations:**
  - Keyloggers
  - Servlets
  - Network monitoring
  - CCTV
  - Human surveillance
  - Background investigations
  - Physical searches

# Technical Support

- **Keyloggers**  
→ hardware



completely invisible for computer operation (pure electronic device)  
No software or drivers required  
Huge 2MB flash memory disk, organized as a FAT file system  
Installs as a flash drive for data retrieve (visible to system as additional disk)  
Super fast data download (up to 100kB/s)  
Quick and easy national layout support  
Compatible with all Low-Speed USB keyboards (including Linux & Mac)

© Peter Sommer, 2008

**LSE**



## Powered Keylogger 2.2 <sup>new</sup>

**Invisibly records computer usage to the smallest detail.**

- ▣ Automatically save the logs to USB Flash Drive <sup>new</sup>
- ▣ Records absolutely all keystrokes and passwords
- ▣ Keylogger invisibly sends logs via e-mail
- ▣ Fully supports the Unicode in contrast to many other keyloggers

**Powered Keylogger** is a driver-based software keylogger that secretly captures keystrokes, mouse clicks and passwords, tracks sent and received emails, monitors Internet activity and logs launched applications. Powered Keylogger is undetectable by a list of firewalls and antivirus software, even anti-spyware/anti-keyloggers won't locate it.



[Download](#)



[More info](#)



[Purchase](#)



## Advanced Keylogger 2.0 <sup>new</sup>

**Records every keystroke to encrypted easy-to-understand logs.**

- ▣ Totally invisible to everyone but you
- ▣ Captures passwords and logins (even Winlogon passwords)
- ▣ Monitors e-mail clients and Internet activity

**Advanced Keylogger** records all computer activity and logs all information so that you can check later what's been done with the computer. You can also secretly receive logs of user's activity to your e-mail.



[Download](#)



[More info](#)



[Purchase](#)

LSE

With the Spector Pro Keylogger, you will be able to:



Capture ev  
(including us



Get the ex:



Capture &



Read ever,



Review ev



See everyt



See every



See every



Quickly fin

## Completely Invisible Stealth Technology



> // ACCESS GRANTED  
PASSWORDS  
ACCOUNTS  
USER NAMES  
EVERYTHING TYPED  
EVERYTHING THEY DO



The most advanced stealth technology available ensures that the Spector Pro keylogger is completely protected from everyone except those with authorized access.

Spector Pro does not appear in the Start Menu, Add/Remove Programs, Task Manager, Running Processes, System Tray, Registry, or on the Desktop – there aren't even any visible files.

"Spector Pro does the BEST  
job of hiding"  
– PC Magazine

"EVERY word they type, EVERY link  
they click, SpectorSoft will be  
watching"  
– InfoWorld Magazine

## Instant Alerts See What They Type and What They View



The Spector Pro keylogger will instantly inform you whenever they type – or even simply VIEW – any "alert words" or phrases that you specify.

Spector Pro continuously looks for alert words in EVERYTHING they type, EVERY web site they visit, ALL chats/Instant Messages and in EACH email sent or received.

EVERY time a keyword is detected, Spector Pro will immediately email you a detailed report of WHEN, WHERE and HOW the keyword was used.

**Alerts are sent to your office,  
home, cell phone or wherever you  
want!**

"This is one slick piece of technology"  
– US News & World Report

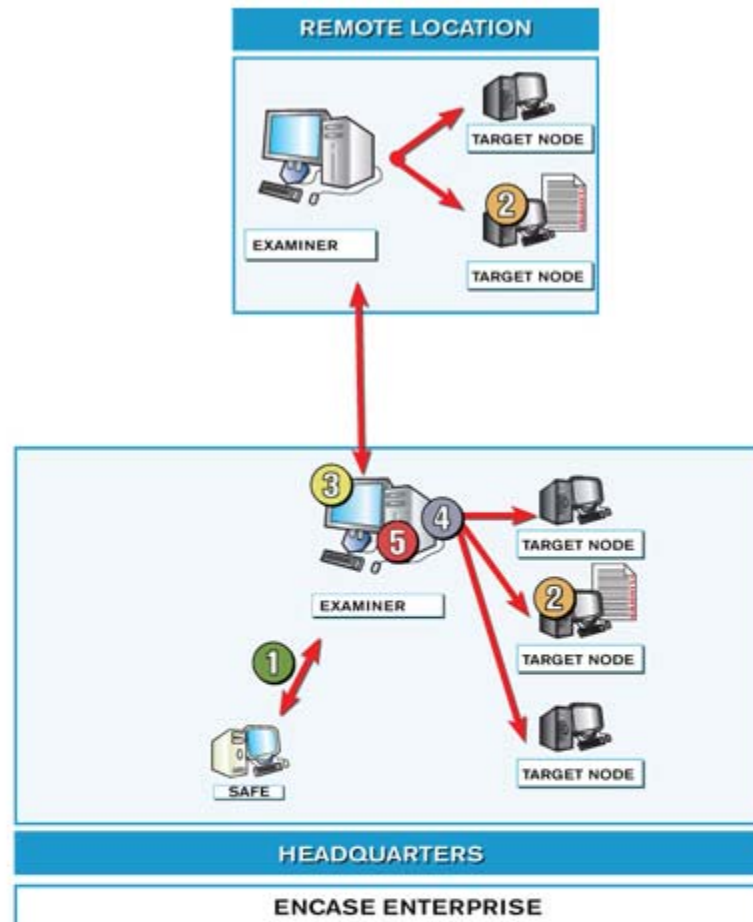
LSE



# Tech

- **Servlets**

- Eg EnCase Enterprise
- Applied on a forensic exam



- 1 Examiner logs into safe for authentication and authorization
- 2 Examiner sends request to target node to snapshot volatile data or to preview drive
- 3 Examiner analyzes/reviews forensic or volatile data from target node
- 4 Analyze further or acquire image
- 5 Generate reports

# Network Surveillance

Wireshark (Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.24	Broadcast	ARP	who has 192.168.0.13? Tell 192.168.0.24
2	2.811077	192.168.0.28	192.168.0.1	DNS	standard query A news.bbc.co.uk
3	2.830511	192.168.0.1	192.168.0.28	DNS	standard query response CNAME newswww.bbc.net.uk A 212.58.22
4	2.831483	192.168.0.28	212.58.226.20	TCP	2147 > http [SYN] Seq=0 Ack=0 win=65535 Len=0 MSS=1460
5	2.851870	212.58.226.20	192.168.0.28	TCP	http > 2147 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1412
6	2.851957	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
7	2.852877	192.168.0.28	212.58.226.20	HTTP	GET / HTTP/1.1
8	2.887300	212.58.226.20	192.168.0.28	TCP	http > 2147 [ACK] Seq=1 Ack=641 win=7040 Len=0
9	2.894571	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
10	2.894610	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
11	2.894638	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=641 Ack=1449 win=65535 Len=0
12	2.915530	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
13	2.917217	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
14	2.917283	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=641 Ack=4273 win=65535 Len=0
15	2.918863	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
16	2.938667	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
17	2.938718	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=641 Ack=7097 win=65535 Len=0
18	2.940375	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]

Frame 1 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: 192.168.0.24 (00:05:1b:00:4f:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 05 1b 00 4f 14 08 06 00 01  .....O.....
0010  08 00 06 04 00 01 00 05 1b 00 4f 14 c0 a8 00 18  .....O.....
0020  00 00 00 00 00 00 c0 a8 00 0d 00 00 00 00 70 02  .....p.....
0030  40 00 c8 53 00 00 02 04 05 b4 00 00              @..S....
  
```

# External Logs

- **System Logs**
- **Web Logs**
- **Intrusion Detection System Logs**
- **Anti-Virus Logs**
- **ISP Logs**
  - **RADIUS**
  - **Web-Logs**

**Subject to  
DPA/ RIPA  
authorisation  
and/or  
consent!**

# Squid Logs

```
1007949021.553      86 192.168.0.103 TCP_MEM_HIT/200 6947 GET http://us.a1.yimg.c
om/us.yimg.com/i/ww/m5v6.gif graeme NONE/- image/gif
1007949022.484     4374 192.168.0.103 TCP_MISS/200 22349 GET http://www.yahoo.com/
graeme DIRECT/64.58.76.223 text/html
1007949022.884       74 192.168.0.103 TCP_HIT/200 4043 GET http://us.a1.yimg.com/u
s.yimg.com/a/ya/yahoo_promotions/fp2.gif graeme NONE/- image/gif
1007949027.488     4418 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/i/us/auc/b/auc16_1.gif graeme NONE/- -
1007949028.056     4569 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/us/sh/pr/hol01/rib.gif graeme NONE/- -
1007949028.059     4604 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/us/sh/pr/hol01/bow.gif graeme NONE/- -
1007949028.061     4544 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/space.gif graeme NONE/- -
1007949028.063     4346 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/i/sh/h99/holly.gif graeme NONE/- -
1007949028.065     4258 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/a/an/anchor/shopping/ads/new37/dell.gif graeme NONE/- -
1007949029.233     1163 192.168.0.103 TCP_MISS/302 148 GET http://www.yahoo.com/r/
m1 graeme DIRECT/64.58.76.227 -
1007949032.096       73 192.168.0.103 TCP_HIT/200 1365 GET http://us.i1.yimg.com/u
s.yimg.com/i/us/pim/maillogin.gif graeme NONE/- image/gif
1007949032.324     3089 192.168.0.103 TCP_MISS/200 12044 GET http://mail.yahoo.com
:[]
```

```
lwn.net/images/sp.gif
H lwn.net/images/linuxpower2.png
lwn.net/images/narrow.png
lwn.net/images/eklektixsm.png
stats.lwn.net/1pixtrans.gif
lwn.net/2002/0214/security.php3
lwn.net/images/security.png
```

(96.03% to 100.00%) 60.00% Fri Feb 15 08:48 2002

| h = help

LSE

# Forensic Readiness Plan

## Why have plan?

- To reduce costs and panic
- External consultants will have to “learn” the business
- Lawyers will have to identify admissibility and privilege issues on the spot
- Can also be used for other legal situations, eg internal disciplinary disputes, routine transaction disputes, to aid law enforcement

# Forensic Readiness Programs

## Essentially:

- Based on threat analysis / scenario development
- Requires identification of potential evidence / disclosure requirements – and plan for their formal production
- Results in a proper Contingency Plan – which is tested and kept up-to-date

# 7-step Forensic Readiness Plan

## Identify:

- **the main likely threats/ legal challenges faced by your organisation**
- **what sorts of evidence / disclosure you are likely to need if you have to proceed to civil or criminal litigation**
- **what you will need to do to meet various regulatory and compliance requirements**
- **how far you may have that material already**
- **what you will need to do to secure additional essential material**

# 7-step Forensic Readiness Plan

- the management, skills and resources implications for your organisation
- turn the results into an action plan – which will need regular revision as the organisation and its ICT infrastructure develops.



# **7-step Forensic Readiness Plan**

**The Good News:**

**quite a bit of the work may already have been  
carried out elsewhere in the organisation....**

**.....Disaster Recovery / Business  
Contingency Plans**

# Business Contingency Plans

- **Preparation against disaster:**
  - Fire
  - Flood
  - Terrorism
  - Denial of access
  - Computer failure
  - Etc etc

# Business Contingency Plans

- **Tells organisation what to do:**
  - Emergency Priorities
  - Team that will act / Reporting Responsibilities
  - Migrated offices, locations
  - Migrated people
  - Migrated ICT
  - PR for customers, clients, investors, bankers, public-at-large etc

# Business Contingency Plans

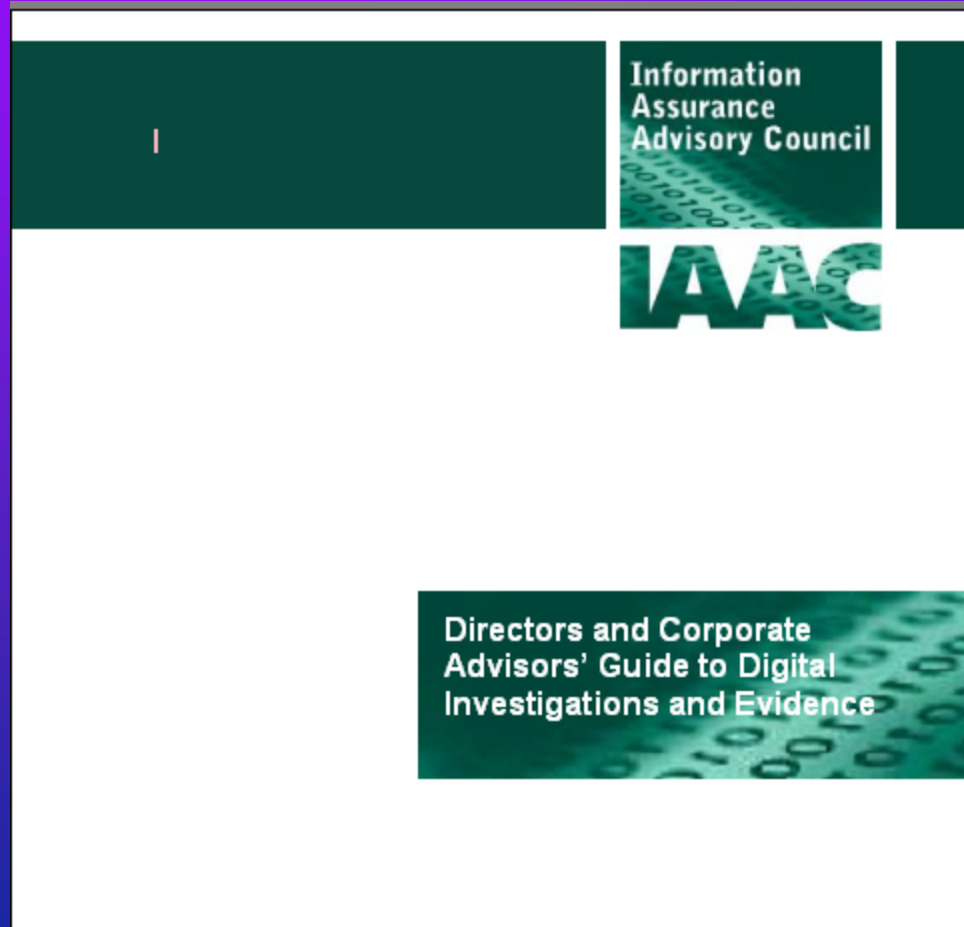
## Research, Design

- Business Analysis
  - to determine priorities (it's too expensive to restore everything instantly)
- Relation of business processes to specific ICT resources, hardware, software, communications links; availability of back-up
- Detailed plan for who does what when
- Emergency Response Team
- Internally published Plan
- Frequent Testing and Revision

# Forensic Readiness Plan: Additional Requirements

- Legal / Regulatory requirements
- Analysis of back-up plans
  - Incremental / complete
- Specific Data Retention / Destruction requirements
- Decisions about mode of disclosure
  - Electronic, print-out, extents, etc
- Witness to explain systems, material produced, testify to reliability and completeness

# Guide to Digital Investigations and Evidence



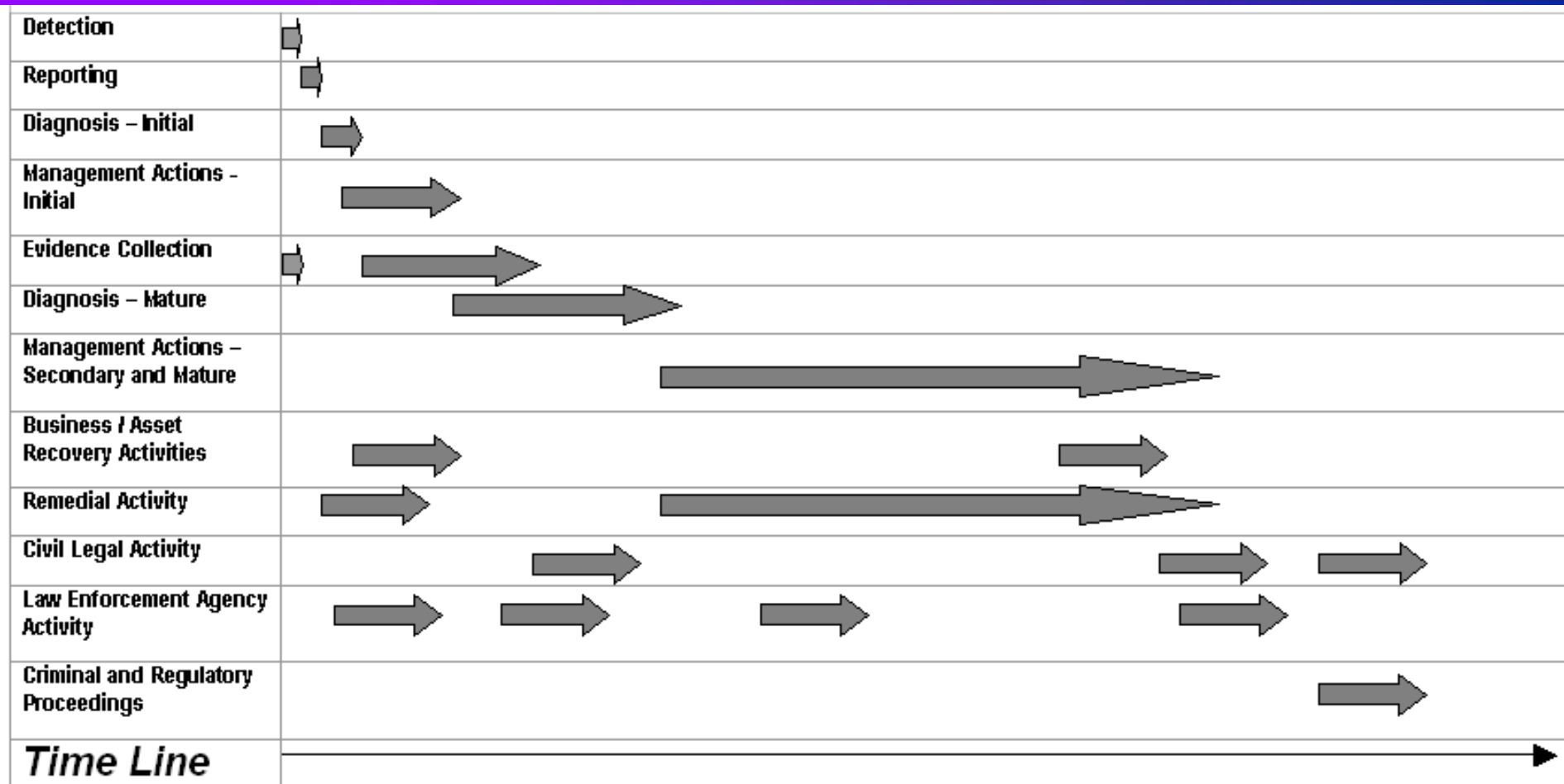
**First published  
2005; new edition  
due**

**[www.iaac.org](http://www.iaac.org)**

# Life-cycle of incidents



Computer Incident Management  
Life Cycle





# Remedial Activity

- The final “prize” from having a FRP:
- Closing the Loop / Learning the Lessons
- *Although the FRP is aimed at legal outcomes, after any event you will have a detailed explanation of what went wrong*
- *Should lead to precise remedial actions*



**The Malicious Exploitation of Information Systems:  
Preventing the Rise of the Insider Threat**

**6-7 November 2008, UCL**

**Issues in the Technologies of  
Digital Investigation**

**Peter Sommer**

**London School of Economics, Open University**

**[peter@pmsommer.com](mailto:peter@pmsommer.com)**

**[p.m.sommer@lse.ac.uk](mailto:p.m.sommer@lse.ac.uk)**

