



Forensic IT Trends Survey

September 2002

Fox-IT is an IT security company specialized in three important areas: Forensic IT, IT security and Practical training. Fox-IT was founded 3 years ago and has grown to employ 20 professionals. Fox-IT is known for its personal approach to customers, confidential treatment of sensitive material, delivery of custom products, large expertise, realistic pricing and implementation of large and prestigious projects.

Fox-IT's customers are found in many and varying areas: the police, governmental departments, sports organisations, financial businesses such as banks and insurance companies, lawfirms and notaries. Other areas where security and confidentiality are paramount are continually being added to this list.

EXPERTS IN IT SECURITY

Table of Contents

Table of Contents	2
Preface	3
Forensic IT Investigation Respondents.....	3
Forensic IT Investigation Respondents.....	4
Investigations.....	6
Appendix A: Mailing lists and forums.....	7

Preface

“What are the trends in forensic IT research? Which tools are used? What are the objectives of a forensic IT investigation?”. These questions that we’ve had, led to a small survey that we’ve published on our website, <http://www.fox-it.com/survey>. Our goal was to find out if other forensic IT investigators worldwide, saw the same increase in the number of forensic IT researches and used the same tools.

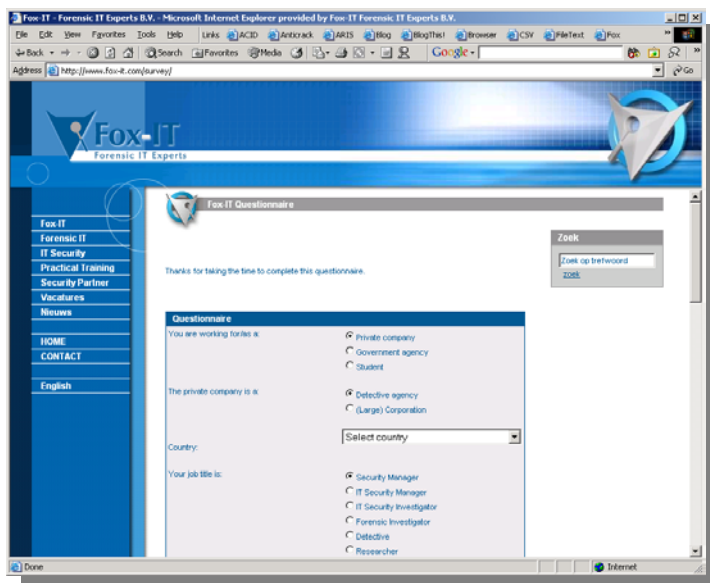
We’ve posted a message to a number of forums and mailing lists that we knew we’re being read by forensic IT investigators (see appendix A). Some moderators rejected our post and claimed it was spam and should not be posted to their list. However, the post clearly stated that the result of our survey was going to be made freely available.

Luckily, some moderators allowed our post and within 2 weeks we got 102 quality responses. More than half of the respondents (66 to be exact) left their email address to be notified when the results would be available.

We received 3 email messages with tips on improving our survey the next time. Next time? Well, in due to the great number of responses, we will hold this survey again next year, using the tips provided by our colleagues.

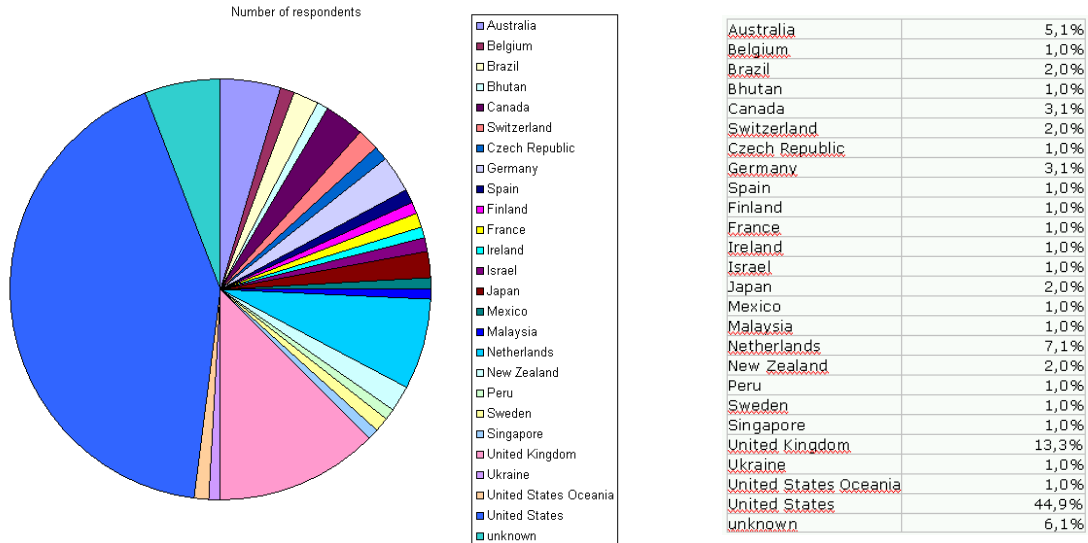
If you are one of the respondents who filled in the survey we’d like to thank you for your time and effort.

Matthijs van der Wel
Project Manager

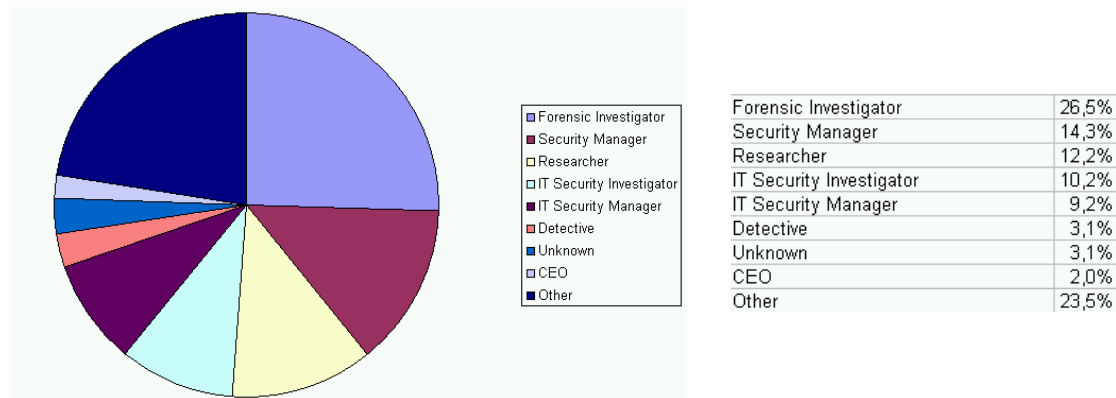


Forensic IT Investigation Respondents

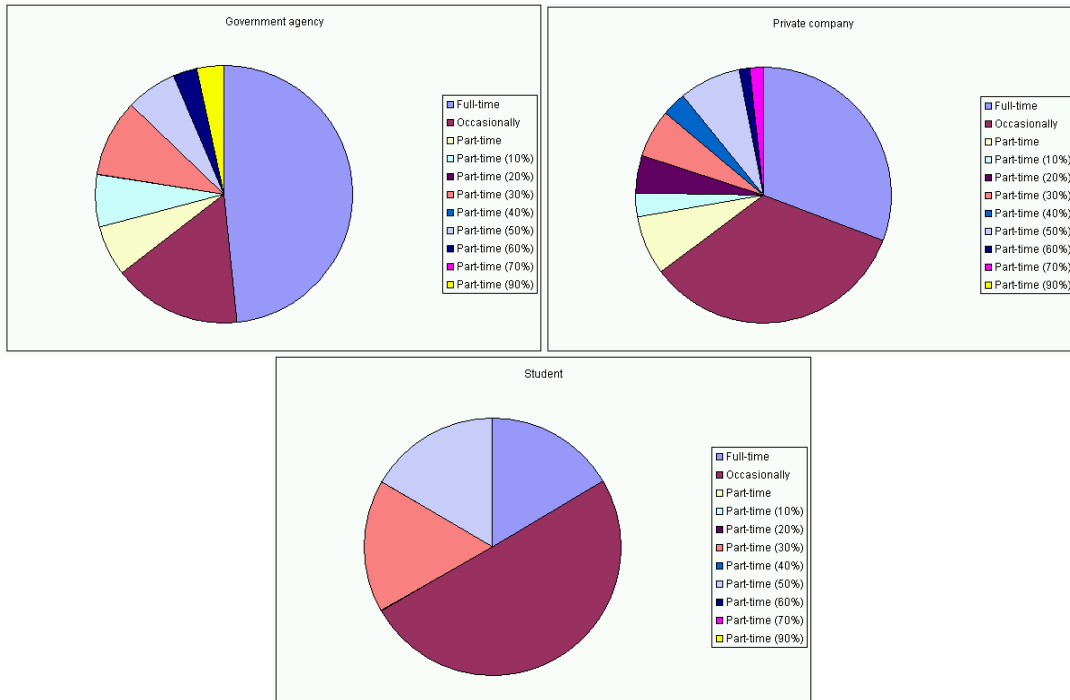
During the first 3 weeks of September 2002 a total of 102 respondents responded to our email message requesting to take part in a survey about forensic IT investigation.



Most of the respondents are working in the USA and UK. Of all respondents, most of them are working as a Forensic Investigator (26,5%), Security Manager (14,3%) or Researcher (12,2%). The job titles mentioned as 'other' each have one respondent and are: Criminal Investigator, CSO, CTO, Detective Sergeant, Head of Forensic Computing Services, Information Systems Security Officer, Internal Auditor, IT Manager & Forensic Investigator, IT Manager, LAN/WAN Analyst, Lawyer, Network Administrator, Network Security Analyst, Risk Management Coordinator, Security Consultant, Security Specialist, Senior Forensic Technology Manager, Software Engineer, Support Specialist, Systems Administrator, Tech Support Repp, Technical Director and Webmaster.



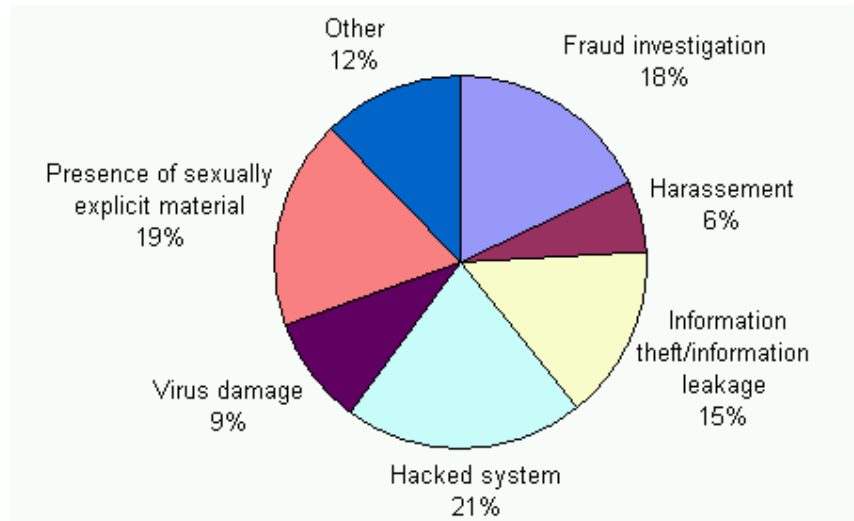
The respondents working for a government agency, usually work full-time on forensic IT investigations. Most of the students only perform forensic IT investigations occasionally.



Government agency		Private company		Student	
<i>Forensic IT is done:</i>	<i>Total</i>	<i>Forensic IT is done:</i>	<i>Total</i>	<i>Forensic IT is done:</i>	<i>Total</i>
Full-time	15	Full-time	20	Full-time	1
Occasionally	5	Occasionally	22	Occasionally	3
Part-time	2	Part-time	5	Part-time	0
Part-time (10%)	2	Part-time (10%)	2	Part-time (10%)	0
Part-time (20%)	0	Part-time (20%)	3	Part-time (20%)	0
Part-time (30%)	3	Part-time (30%)	4	Part-time (30%)	1
Part-time (40%)	0	Part-time (40%)	2	Part-time (40%)	0
Part-time (50%)	2	Part-time (50%)	5	Part-time (50%)	1
Part-time (60%)	1	Part-time (60%)	1	Part-time (60%)	0
Part-time (70%)	0	Part-time (70%)	1	Part-time (70%)	0
Part-time (90%)	1	Part-time (90%)	0	Part-time (90%)	0

Investigations

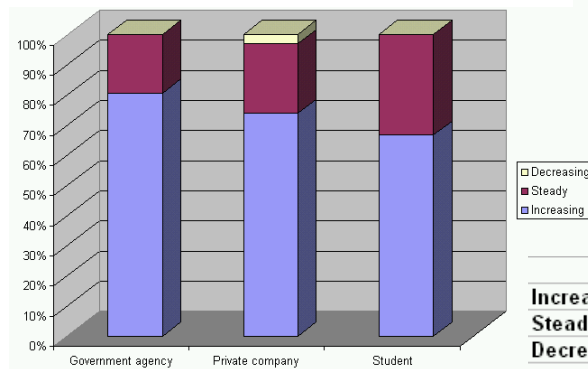
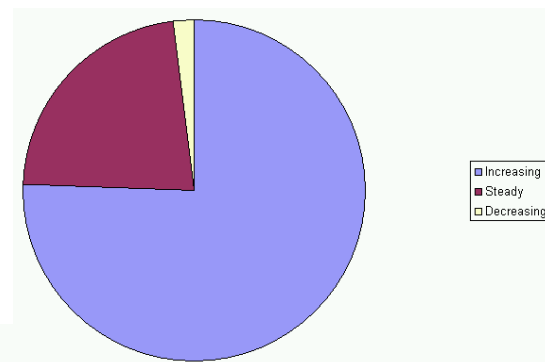
Why do we perform forensic IT investigations?



Among the 'other' the respondents mentioned: Administrative, Child Pornography, Civil Discovery, Commercial dispute, Coordination with other CERTs, Counterfeit, Counterfeit software, DDoS, Deception/Theft, Drug Investigations, Drug related, Electronic discovery, Employee\'s for profit Bus. on Gov. owned Equip., Employees setting up competing businesses, File System Monitoring, Homicide/murder, IDS Monitoring, Illegal resource allocation, Intellectual Property (civil), Intrusion Detection, Lost data, Murder, Narcotics, Non-categorized threat, Other, Other employee misconduct, Research, Research and Patching, Special requirements from customers, Using employer time, equipment to run other business and Wrongful termination.

Compared to one year ago, most of the respondents have seen an increase in the number of forensic IT investigations.

The respondents working for a government agency have seen the largest number of increase. Only 2 respondents working for a private company have experienced a decrease.

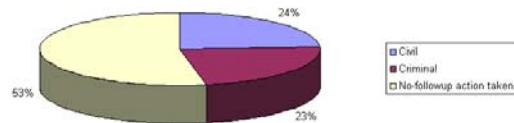


	Government agency	Private company	Student
Increasing	25	48	4
Steady	6	15	2
Decreasing	0	2	0

The expectation that the number of forensic IT investigations will continue to rise is shared by 73 percent of the respondents. Only 2 percent of the respondents think the number of investigations will decrease and 27 percent think the number will stay more or less the same.

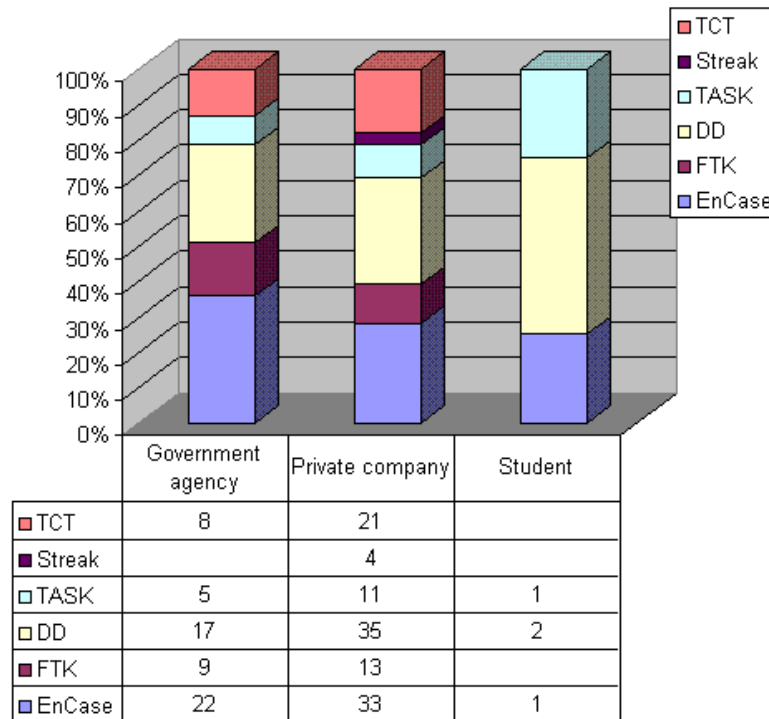
Prosecution

On most of the investigations no follow-up action is taken. More than half of the investigations do not lead to a trial or law suit. Just 24 percent of the investigations leads to civil law suit and just 23 percent to a criminal law suit.



Tools

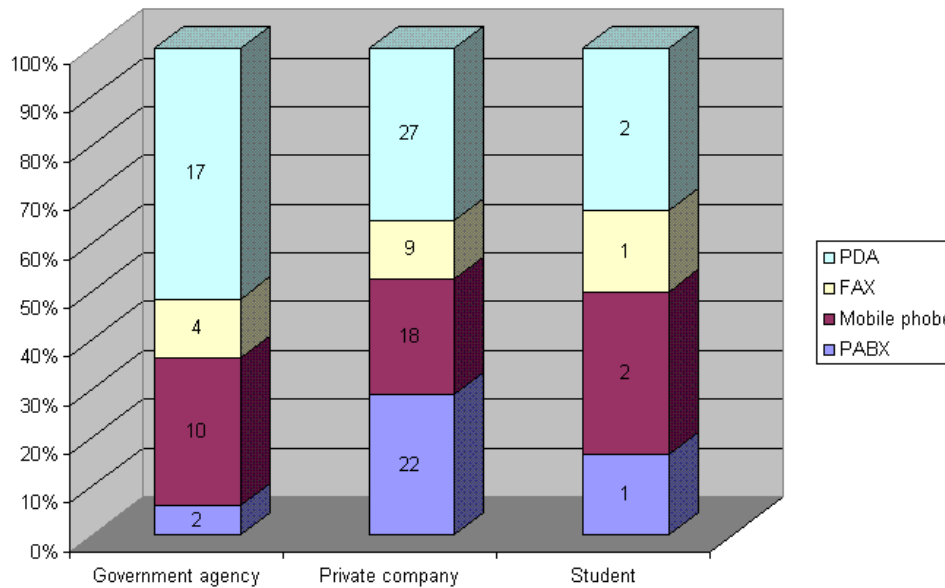
There are many tools used in Forensic IT investigations. Some are tools especially created to aid Forensic experts, some are standard editors or operating system tools.



Encase is overall the most used tool with over half of the respondents using it. Another popular tool is DD with 54 users among the respondents. Most of the Encase and DD users are private companies. The percentage of Encase users is highest in Government agencies and TCT is relatively used more often by private companies. Most used among the other tools the respondents use are Safeback (4), NTi tools suite (3), ProDiscover DFT (3), NetAnalysis (2) and Ghost (2).

Information sources

Intercepting network traffic is a very important technique for forensic IT investigators. Over 67 percent of the respondents have gathered evidence by intercepting network traffic in the course of an investigation. Other (digital) sources that are used are mobile phone, PABX, Fax and PDA. Next to intercepting network traffic the PDA is the most used digital source in forensic investigations.



Respondents also used sources like speech recorder, chipcards, Entry security system, printer and Digital CCTV in an investigation.

Appendix A: Mailing lists and forums

We've posted the following message to the following mailing lists and forums:

Message

Hi,

What are the trends in forensic IT reseach? Which tools are used? What are the objectives of a forensic IT investigation?

In order to answer these questions, we've put together a small survey and placed it on our website. The purpose of this anonymous survey is to write a report which will be freely available.

May we please ask a moment of your time (a couple of minutes) to point your browser at:

<http://www.fox-it.com/survey/>

Thanks in advance for your time and effort.

Matthijs van der Wel
Project Manager
Fox-IT Forensic IT Experts
Rijswijk (ZH), The Netherlands

Mailing lists and forums

- linux_forensics@yahoogroups.com
- forensics@securityfocus.com
- <http://www.digitaldetective.co.uk/forum>
- InternetCrime-L@yahoogroups.com