2010 Report of digital forensic standards, processes and accuracy measurement

Joshua Isaac James, Pavel Gladyshev
{Joshua.James, Pavel.Gladyshev}@UCD.ie

Centre for Cybercrime Investigation
University College Dublin
Belfield, Dublin 4
Ireland

1. Introduction

From December 7th 2010 to December 12th 2010 a survey on *Digital Investigation Process and Accuracy* was conducted in an attempt to determine the current state of digital investigations, the process of examination (examination phases), and how those examinations are being verified as accurate. An online survey was created in English using SurveyMonkey.com[1] (2010), and consisted of 10 questions. Two groups were solicited: a control group from the University College Dublin (UCD) Forensic Computing and Cybercrime Investigation (FCCCI) MSc Programme (2010), and members of the Forensic Focus (FF) (2010) community. The control group consisted of known digital forensic investigators, of which four replies were received. The second group consisted of anonymous replies from the Forensic Focus community. Forensic Focus is a publically accessible online forum and information site on the topic of computer forensics that primarily uses the English language. 28 replies were received from this community, making 32 replies in total. The average responses from the control group were consistent with the average responses from the Forensic Focus community. For the analysis in this paper, all responses will be considered together. The collected survey data can be found in appendix A.

2. Survey Analysis

To determine if trends were sector or region specific, the following questions were asked:

Question 1 was to identify the associated work sector of the respondents.

- **Which of the following best describes your organization?**

1 All graphs created using SurveyMonkey.com

78.1% of respondents claimed to be Law Enforcement, 12.5% claimed to be with a corporate entity, and 9.4% claimed to be contractors. No other sectors were specified, as seen in figure 1.

1. Which of the following best describes your organization?

	Response Percent	Response Count
Corporate	12.5%	4
Law Enforcement	78.1%	25
Contractor	9.4%	3
Education	0.0%	0
Other (please specify)	0.0%	0
answered question		32
skipped question		0

Fig. . Distribution of respondents' by work sector

Question 2 was to identify the region where the respondents were located.

- **What general region best describes your organization's location?**

68.8% or respondents claimed to be from Europe, 21.9% claimed to be from North or South America, 6.3% claimed to be from Asia and South Pacific (ASP), and 3.1% claimed to be from the Middle East and North Africa (MENA) (fig. 2). This distribution is comparable the FF 'members map', with slightly less representation from North and South America. Also FCCCI has slightly more members from Europe than other regions, which could account for some of the over-representation in Europe. Given that the survey was in English and was posted to limited English speaking sources, there is an inherent bias towards English speaking regions. For this reason, any conclusions should be generalized as more relevant to regions where English is the preferred working language e.g. Europe, North America and Australia, rather than a truly global view.

2. What general region best describes your organizations location?			
		Response Percent	Response Count
North/South America		21.9%	7
Europe		68.8%	22
Middle East and North Africa		3.1%	1
Africa		0.0%	0
Asia and South Pacific		6.3%	2
		answered question	32
		skipped question	0

Fig. . Distribution of respondents' by region

The next questions were created to determine an average caseload, and how well departments are keeping up with the workload.

Question 3 was to approximate the number of investigations per month.

- **Approximately how many digital investigations does your department conduct per month?**

43.8% of respondents claimed that 21 or more cases were being conducted per month, 34.4% claimed between 1-10 cases per month, and 21.9% claimed 11-20 cases per month (fig. 3). Each respondent claimed his or her department investigated at least one case per month. The scope of the answers in this question was also found to be too low, resulting in a loss of some specificity above 21 cases.

3. Approximately how many digital investigations does your department conduct per month?			
		Response Percent	Response Count
0		0.0%	0
1-10		34.4%	11
11-20		21.9%	7
21 or more		43.8%	14
		answered question	32
		skipped question	0

Fig. . Approximate number of digital investigations per month conducted per department

Question 4 was to approximate whether each case investigated involved a suspect device such as a computer or cell phone.

- **Approximately how many digital investigations per month involve examining a suspect device (computer, cell phone, etc)?**

37.5% claimed that 21 or more cases per month involved a suspect device; another 37.5% claimed only 1-10 cases involved a suspect device; and 25% claimed 11-20 cases per month (fig. 4). When compared to question 3, there is a reduction of suspect devices analyzed vs. the number of cases, but suspect devices are still analyzed the majority of the time. This question does not take into account the number of devices per case.

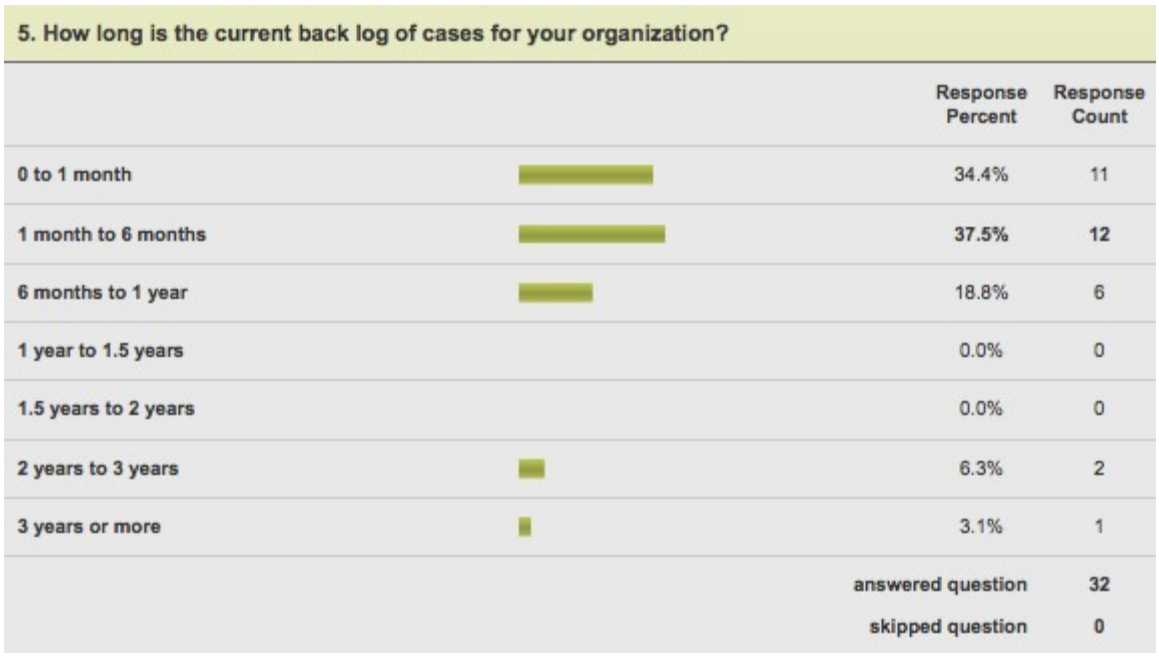
4. Approximately how many digital investigations per month involve examining a suspect device (computer, cell phone, etc)?			
		Response Percent	Response Count
0		0.0%	0
1-10		37.5%	12
11-20		25.0%	8
21 or more		37.5%	12
		answered question	32
		skipped question	0

Fig. . Approximate cases per month involving a suspect device

Question 5 was to determine the current length of case backlog the respondents were experiencing.

- **How long is the current backlog of cases for your organization?**

37.5% responded with 1 month to 6 months, 34.4% responded 0 to 1 month, 18.8% responded 6 months to 1 year, 6.3% responded with 2 years to 3 years, and 3.1% responded with 3 years or more (fig. 5). From these results, 71.9% of respondents have a case backlog between 0 and 6 months. The overall (very approximate) mean is ~9 months. These reported times are similar to those reported in 2004 (EURIM-ippr 2004), and are as much as 1.5 years less than have been recently reported in the US and UK (InfoSecurity 2009; Gogolin 2010; Raasch 2010). There were no responses between 1 year and 2 years.



5. How long is the current back log of cases for your organization?

	Response Percent	Response Count
0 to 1 month	34.4%	11
1 month to 6 months	37.5%	12
6 months to 1 year	18.8%	6
1 year to 1.5 years	0.0%	0
1.5 years to 2 years	0.0%	0
2 years to 3 years	6.3%	2
3 years or more	3.1%	1
answered question		32
skipped question		0

Fig. . Approximate distribution of case backlog times

The following questions were to determine common standards and guidelines, as well as analysis techniques.

Question 6 was to determine what standards or guidelines are commonly used in the digital forensic process. The respondent could have chosen multiple answers.

- **What are the main standards or guidelines your organization uses to ensure quality forensic processes?**

58.1% claimed their standard operating procedure (SOP) was developed in-house, 35.5% claimed to use standards from the National Institute of Standards and Technology (NIST), 29% claimed to use standards from the Association of Chief Police Officers (ACPO), 19.4% claimed to use International Organization for Standardization (ISO) standards, 9.7% claimed to use other standards, such as European Cybercrime Training and Education Group (ECTEG) operating procedures, and guidelines from the Nederlands Forensisch Instituut [Netherlands Forensic Institute] (NFI), and 6.5% used standards from the International Association of Computer Investigative Specialists (IACIS). One respondent declined to answer, making the total respondents 31. The data would suggest that the majority of departments are developing their own SOP, but are also implementing other standards to supplement. NIST (US based) and ACPO (UK based) were the most popular after in-house developed SOP.

6. What are the main standards or guidelines your organization uses to ensure quality forensic processes?

	Response Percent	Response Count
National Institute of Standards and Technology (NIST)	35.5%	11
International Organization for Standardization (ISO)	19.4%	6
International Association of Computer Investigative Specialists (IACIS)	6.5%	2
Association of Chief Police Officers (ACPO)	29.0%	9
Developed in-house	58.1%	18
Other (please specify) Show Responses	9.7%	3
answered question		31
skipped question		1

Fig. . Standards commonly used in digital investigation processes

Question 7 was to determine if any preliminary analysis is done before an in-depth analysis.

- **Is a preliminary analysis (preview) of a suspect computer conducted before an in-depth analysis?**

40.6% of respondents claimed that a preliminary analysis was done sometimes (49% or less), 28.1% claimed a preliminary analysis was done most of the time (50% or more), 21.9% claimed a preliminary analysis was never done, and 9.4% always conduct a preliminary analysis (fig. 7). The data suggests that choosing to conduct a preliminary analysis very much depends on the case, which is consistent with claims by (Casey, Ferraro et al. 2009) that “case management… involves tailoring forensic examination of digital evidence to the type of crime or case under investigation”. In some cases, such as a murder investigation, a preliminary analysis may not be conducted. This could account for why the majority of responses were ‘sometimes’ instead of ‘most of the time’. This question did not consider the types of cases being investigated or departments the respondents were involved with.

7. Is a preliminary analysis (preview) of a suspect computer conducted before an in-depth analysis?			
		Response Percent	Response Count
Always		9.4%	3
Most of the time (50% or more)		28.1%	9
Sometimes (49% or less)		40.6%	13
Never		21.9%	7
		answered question	32
		skipped question	0

Fig. . Graph of how often a preliminary analysis is conducted before an in-depth analysis

Question 8 was to determine how often on scene triage or preview techniques are used.

- **Does your department use on scene triage or preview techniques?**

41.9% of respondents claimed on scene preview or triage was conducted sometimes (49% or less), 29% claimed preview was never conducted, 19.4% claimed preview was done whenever possible, and 9.7% claimed on scene preview was done whenever possible (fig. 8). One respondent declined to answer, making the total respondents 31. The responses are similar to question 7, with more respondents either attempting on scene preview or not previewing at all.

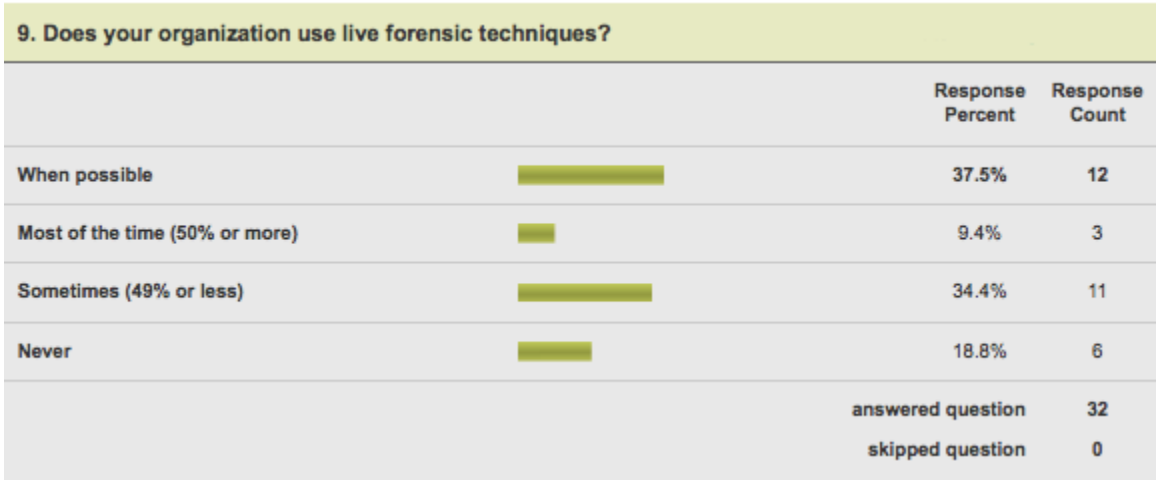
8. Does your department use on scene triage or preview techniques?			
		Response Percent	Response Count
Whenever possible		19.4%	6
Most of the time (50% or more)		9.7%	3
Sometimes (49% or less)		41.9%	13
Never		29.0%	9
		answered question	31
		skipped question	1

Fig. . Graph of how often on scene preview or triage is conducted

Question 9 was to determine how often live forensic techniques are used.

- **Does your organization use live forensic techniques?**

37.5% of respondents claimed they use live forensics when possible, 34.4% use live forensics sometimes (49% or less), 18.8% claimed to never use live forensics, and 9.4% claimed to use live forensics most of the time (50% or more) (fig. 9). When compared to question 8, live forensics is used more often than on scene preview or triage, but not in every possible case.



9. Does your organization use live forensic techniques?

	Response Percent	Response Count
When possible	37.5%	12
Most of the time (50% or more)	9.4%	3
Sometimes (49% or less)	34.4%	11
Never	18.8%	6
answered question		32
skipped question		0

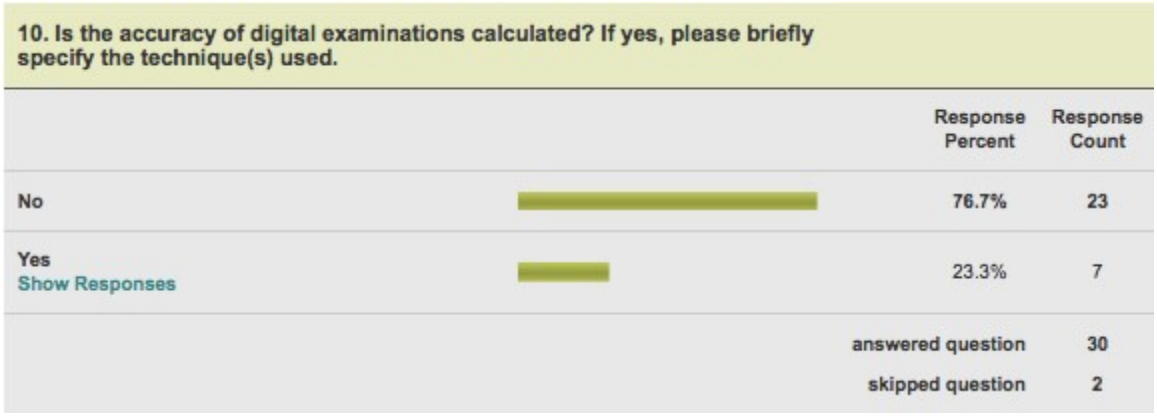
Fig. . Graph of how often live forensics techniques are used

Question 10 was intended to determine the interpretation of ‘accuracy’ in digital examinations. It was expected that each respondent would have a different interpretation of what it means for an examination to be accurate. The word ‘calculated’ was chosen to determine if their definition of accuracy could be measured.

- **Is the accuracy of digital examinations calculated? If yes, please briefly specify the technique(s) used.**

76.7% of respondents claimed that the accuracy of digital examinations is not being calculated, while 23.3% claimed accuracy was being calculated (fig. 10). Two respondents declined to answer, making the total respondents 30. The majority of respondents that replied yes (4 out of 7) also claimed that accuracy was verified by peer review, followed by hashing the evidence (2 out of 7). Please see appendix A for more information. From the data, accuracy of a digital examination is most commonly interpreted as verification of the

findings by review. No mention was given to ‘calculation’ i.e. a formula for objective measurement.



10. Is the accuracy of digital examinations calculated? If yes, please briefly specify the technique(s) used.

	Response Percent	Response Count
No	76.7%	23
Yes	23.3%	7
Show Responses		
answered question		30
skipped question		2

Fig. . The percentage of respondents claiming to calculate accuracy of digital examinations

3. General Analysis

- Of the respondents, North and South America reported the largest number of investigations with 57% of respondents claiming 21 or more investigations per month, while 50% of respondents in ASP and 41% of respondents in Europe claimed 21 or more per month.
- All corporate and contractor respondents reported backlogs of 0 to 1 month regardless of region and caseload.
- European Law Enforcement (LE) reported the longest backlogs with 18% claiming backlogs of over 1 year. The next longest was ASP LE with 50% of the respondents claiming backlogs of 6 months to 1 year.
- 100% of ASP LE claimed backlogs of 1 month to 1 year; 100% of North/South American LE and 100% of MENA LE claimed backlogs of 1 month to 6 months; and 88% of European LE claimed backlogs of 1 month or more.
- 100% of LE respondents claiming case backlogs greater than 2 years selected *only* NIST as the used guidelines. Alternatively, 100% of corporate that selected *only* NIST as the used guidelines claimed case backlogs of 0 to 1 month.
- 80% of LE that selected *only* that their SOP was developed in-house (no additional standards) reported case backlogs of 1 month to 6 months.
- LE with longer backlogs were more likely to conduct a preliminary analysis before an in-depth analysis.
- 71% of corporate and contractor respondents conducted preliminary analysis more than half the time, and were also the

only respondents to report always (42%) conducting a preliminary analysis.
- The length of the case backlog was more of an indicator as to whether a preliminary analysis would be done than the amount of cases per month.
- Unlike preliminary analysis, respondents with longer backlogs were not more likely to use on scene preview or triage.
- 83% of respondents that used on scene preview or triage whenever possible claimed a backlog of 0 to 1 month as compared to only 11% of respondents who claimed to never use on scene preview.
- The use of live forensic techniques does not appear to correlate to the number of cases per month or case backlog.

4. Conclusions

The data provided gives insight into the current state of digital investigations. It has been shown that organizations are using many different standards, and most are developing their own SOP. Whether this works for the department or not, it indicates that there is a considerable amount of duplicated effort worldwide. Concerning case backlogs, the overall backlog time appears to not be as long as has previously been reported. The use of on scene preview or triage appears to have a positive effect on case backlog, but only 18% of those who use on scene preview or triage – and 16% who use preliminary analysis – claimed to attempt to verify the accuracy of investigations. It appears that some improvements can still be made with current digital investigation methods; however, further research needs to be done concerning the types of cases being investigated and the resources available. By comparing responses from corporate and law enforcement, and considering their traditional differences (budget and case types), both budget and case types appear to be factors in backlog and used preliminary analysis.

Acknowledgments

Thank you to the UCD Forensic Computing and Cybercrime Investigation group as well as the Forensic Focus community for your participation.

Bibliography

[1] Casey, E., M. Ferraro, et al. (2009). "Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence*." Journal of forensic sciences 54(6): 1353-1364.

[2] EURIM-ippr. (2004). "EURIM - IPPR E-Crime Study: Partnership Policing for the Information Society." Third Discussion Paper.

Retrieved 23 Nov., 2010, from http://www.eurim.org/consult/e-crime/may_04/ECS_DP3_Skills_040505_web.htm.
[3] ForensicFocus. (2010). "Fornesic Focus: Computer Fornesic News, Information and Community." Retrieved 12 Dec., 2010, from http://www.forensicfocus.com.
[4] Gogolin, G. (2010). "The Digital Crime Tsunami." Digital Investigation 7(1-2): 3-8.
[5] InfoSecurity. (2009, 08 July). "Digital forensics in a smarter and quicker way?" Info Security Retrieved 25 Sept., 2010, from http://www.infosecurity-magazine.com/view/2473/digital-forensics-in-a-smarter-and-quicker-way.
[6] Raasch, J. (2010, 12 July). "Child porn prosecutions delayed by backlog of cases." Retrieved 25 Sept., 2010, from http://www.easterniowanewsnow.com/2010/07/12/child-porn-prosecutions-delayed-by-backlog-of-cases/.
[7] SurveyMonkey. (2010). "SurveyMonkey." Retrieved 12 Dec., 2010, from http://surveymonkey.com.
[8] UCDCCI. (2010). "Forensic Computing and Cybercrime Investigation (FCCCI) MSc Programme." Retrieved 12 Dec., 2010, from http://cci.ucd.ie/content/online-forensic-computing-and-cybercrime-investigation-msc-programme.

Appendix

Appendix A. Table of Survey Questions and Answers

1. Which of the following best describes your organization?	2. What general region best describes your organizations location?	3. Approximately how many digital investigations does your department conduct per month?	4. Approximately how many digital investigations per month involve examining a suspect device (computer, cell phone, etc)?	5. How long is the current backlog of cases for your organization?
Contractor	Europe	21 or more	21 or more	0 to 1 month
Law Enforcement	Europe	21 or more	21 or more	1 month to 6 months
Law Enforcement	Europe	21 or more	21 or more	6 months to 1 year
Law Enforcement	North/South America	21 or more	21 or more	1 month to 6 months
Law Enforcement	Europe	11-20	11-20	1 month to 6 months

Contractor	North/South America	1-10	1-10	0 to 1 month
Law Enforcement	Europe	21 or more	21 or more	6 months to 1 year
Corporate	North/South America	11-20	11-20	0 to 1 month
Law Enforcement	Europe	21 or more	21 or more	3 years or more
Law Enforcement	Europe	1-10	1-10	2 years to 3 years
Law Enforcement	North/South America	21 or more	21 or more	1 month to 6 months
Law Enforcement	Europe	1-10	1-10	1 month to 6 months
Law Enforcement	Europe	1-10	1-10	1 month to 6 months
Law Enforcement	Asia and South Pacific	21 or more	21 or more	6 months to 1 year
Law Enforcement	Europe	1-10	1-10	1 month to 6 months
Law Enforcement	Middle East and North Africa	1-10	1-10	1 month to 6 months
Law Enforcement	Asia and South Pacific	11-20	11-20	1 month to 6 months
Law Enforcement	Europe	11-20	11-20	6 months to 1 year
Law Enforcement	Europe	21 or more	21 or more	0 to 1 month
Law Enforcement	Europe	1-10	1-10	0 to 1 month
Corporate	North/South America	21 or more	21 or more	0 to 1 month
Corporate	North/South America	1-10	1-10	0 to 1 month
Corporate	Europe	11-20	11-20	0 to 1 month
Law Enforcement	Europe	21 or more	1-10	6 months to 1 year
Law Enforcement	Europe	1-10	1-10	0 to 1 month
Law Enforcement	Europe	21 or more	21 or more	6 months to 1 year
Law Enforcement	Europe	11-20	11-20	1 month to 6 months
Law Enforcement	Europe	1-10	11-20	2 years to 3 years
Law Enforcement	Europe	21 or more	21 or more	0 to 1 month
Law Enforcement	Europe	1-10	1-10	1 month to 6 months
Contractor	Europe	11-20	1-10	0 to 1 month
Law Enforcement	North/South America	21 or more	11-20	1 month to 6 months

6. What are the main standards or guidelines your organization uses to ensure quality forensic processes?	7. Is a preliminary analysis (preview) of a suspect computer conducted before an in-depth analysis?	8. Does your department use on scene triage or preview techniques?	9. Does your organization use live forensic techniques?	10. Is the accuracy of digital examinations calculated? If yes, please briefly specify the technique (s) used.
International Organization for Standardization (ISO)	Sometimes (49% or less)	Sometimes (49% or less)	When possible	Yes - By peer review (technical), then by QA process (non technical)
Association of Chief Police Officers (ACPO)	Sometimes (49% or less)	Sometimes (49% or less)	Sometimes (49% or less)	No
International Organization for Standardization (ISO)	Most of the time (50% or more)	Most of the time (50% or more)	Sometimes (49% or less)	No
National Institute of Standards and Technology (NIST), Developed in-house	Sometimes (49% or less)	Sometimes (49% or less)	Sometimes (49% or less)	No
Developed in-house	Sometimes (49% or less)	Never	When possible	No
Developed in-house	Always	Sometimes (49% or less)	Never	No
NIST, ISO, In-house	Most of the time (50% or more)	Sometimes (49% or less)	Sometimes (49% or less)	No
In-house	Always	Whenever possible	Most of the time (50% or more)	No
National Institute of Standards and Technology (NIST)	Sometimes (49% or less)	Sometimes (49% or less)	When possible	No
National Institute of Standards and Technology (NIST)	Most of the time (50% or more)	Sometimes (49% or less)	When possible	No
Developed in-house	Never	Never	Sometimes (49% or less)	No
Developed in-house	Never	Never	Sometimes (49% or less)	No
NIST. ISO	Never	Never	Never	Yes - 2 technical correctings by other experts of

				the domain
Developed in-house + additional standards	Sometimes (49% or less)	Sometimes (49% or less)	Sometimes (49% or less)	Yes - Work is vet through by supervisor before releasing the examination result to the Investigators.
IACIS, In-House	Sometimes (49% or less)	Never	When possible	No
N/A	Sometimes (49% or less)	Sometimes (49% or less)	Sometimes (49% or less)	N/A
IACIS, ACPO	Sometimes (49% or less)	Sometimes (49% or less)	When possible	Yes - images hashed after acquisition
ACPO, Developed in-house	Most of the time (50% or more)	Most of the time (50% or more)	Never	Yes - don't get the question
Association of Chief Police Officers (ACPO)	Never	N/A	Sometimes (49% or less)	No
ISO, In-house	Never	Sometimes (49% or less)	Most of the time (50% or more)	No
National Institute of Standards and Technology (NIST)	Always	Whenever possible	When possible	No
National Institute of Standards and Technology (NIST)	Most of the time (50% or more)	Sometimes (49% or less)	Never	Yes - MD5 Hash values calculated of evidence and image
NIST, ACPO, In-House	Sometimes (49% or less)	Whenever possible	When possible	No
ACPO, Developed in-house	Sometimes (49% or less)	Never	Sometimes (49% or less)	No
NFI, Developed in-house	Most of the time (50% or more)	Whenever possible	When possible	N/A
Developed in-house	Sometimes (49% or less)	Sometimes (49% or less)	When possible	No
Developed in-house	Most of the time (50% or more)	Whenever possible	When possible	No

National Institute of Standards and Technology (NIST)	Most of the time (50% or more)	Most of the time (50% or more)	When possible	No
ACPO, ECTEG SOP	Never	Never	Never	No
NIST, ISO	Never	Never	Never	Yes - 2 technical verifications of all the analysis
ACPO, Developed in-house	Most of the time (50% or more)	Whenever possible	Most of the time (50% or more)	No
NIST, ACPO, In-House	Sometimes (49% or less)	Never	Sometimes (49% or less)	No