Computer Forensics Case Assessment and Triage

- some ideas for discussion

About the author

Harry Parsonage is a Detective Sergeant in the Nottinghamshire Police, England, where he has been practising and managing computer forensics for the last ten years. He has spent most of his 30 years service as a detective during which time he has investigated every type of crime. He also acts as a part-time Computer Forensics Consultant.

Prior to joining the police he had a scientific background and first became involved in computing at university where he learned to program in ALGOL and FORTRAN. Harry graduated with a BSc in Metallurgy and Materials Science and his first graduate job was as a Corrosion Prevention Engineer. He was responsible for managing the corrosion prevention project on the internal surfaces of the steel flood gates of London’s Thames Barrier.

In the Hi Tech Crime arena one of his early cases in 1999 was reported by Steve Gold on Newsbytes as the first worldwide SMS spamming when the Omnipoint SMS gateway in New York was hacked by a Nottingham man who sent a message to thousands of users suggesting they call a telephone number to claim a car they had won, the number belonged to the company which had recently sacked the man. At that time the computer forensics examination was carried out using just Norton Disk Editor but was nevertheless successful and the offender was sentenced to imprisonment.

Harry has written a number of technical papers that have been widely appreciated by forensic practitioners, such as the “Forensic Recovery of Instant Messages from Windows Live Messenger” and “The Meaning of Linkfiles in Forensic Examinations”.

In 2007 his unit was the first in the UK to introduce a software triage process and following the success of the project triage was introduced as a strand of the UK’s Association of Chief Police Officers’ eCrime Strategy.

computerforensics@parsonage.co.uk

Introduction

In 1955, in an article in The Economist, Cyril Northcote Parkinson first suggested Parkinson's Law that "*work expands so as to fill the time available for its completion*". At that time he was referring to public administration but today's corollary to this might be that "*computer forensic examinations expand in proportion to the increase in size of forensic units thus maintaining a significant backlog."*

At present, in 2009, it is commonplace for digital forensic units to have a backlog, several as long as twelve months. Many units have increased in size but have still continued to have a backlog and it is suggested that bringing more staff into a unit will not on its own reduce the backlog of work. This paper discusses how cases submitted to units can be assessed and prioritised, and how software triage can be used to target resources more efficiently.

The author invites discussion on this topic and would welcome any comments on how the issues are dealt with within other units.

What do we consider to be "triage"

A dictionary definition of triage is –

A process for sorting injured people into groups based on their need for or likely benefit from immediate medical treatment. Triage is used in hospital emergency rooms and at disaster sites when limited medical resources must be allocated.

This could be amended slightly so that it is more applicable to digital forensics –

A process for sorting enquiries into groups based on the need for or likely benefit from examination. Triage is used when limited resources must be allocated.

In practical terms this could mean –

- Case Acceptance – an assessment of the submission, does it pass some basic tests.
- Case Prioritisation – a more detailed assessment to put the case in order of priority in a list, or score it with a matrix.
- A simplified automated examination using triage software to identify which item from a group is more likely to render some useful evidence.
- A more detailed examination by an experienced forensic practitioner for the same purpose, e.g. a preview in Encase?

Case Acceptance and Prioritisation

The first step when receiving a case submission is to decide whether or not it meets acceptance criteria. A unit may have a clearly stated acceptance criteria or each case may be judged on an ad hoc basis.

It is useful to have some clear idea of what cases will be accepted, this gives the people making the submissions some guidance and it can be used to some degree to control the volume of work being accepted by the unit.

There are a few factors that could stand alone as case acceptance criteria and be considered first before a detailed case assessment is undertaken, and if the case does not pass those basic tests then there is no point in a detailed assessment. The first factor mentioned below is one which can stand alone as case acceptance criteria. It might be that other parts of the prioritisation factors could be taken out as case acceptance criteria. For example if the only value of the product of an examination will be intelligence then this might be a factor that could mean immediate rejection.

There are other factors which might be considered before carrying out a full assessment. For example, if a submission is so small that it would only take one or two hours of work consider whether it could bypass a detailed assessment. There are often submissions of CDRs, flash memory cards or small USB sticks that could be examined within a short time and it would seem disproportionate to delay such a submission for what could be many months and cause frustration to your internal customers. A small and simple task can sometimes be a refreshing break from a detailed computer examination. These sort of tasks could be undertaken by a member of staff on a lower grade and give them a development opportunity.

It is also possible that part of a submission could be given an immediate priority in order to assist the enquiry. For example where there has been some online activity and a suspect's email or IP address has been recorded on a computer it might be useful to preview the computer to recover it so that enquiries can be made with ISPs before the data has been weeded and lost forever. Once this information has been recovered the submission can be prioritised as any other case.

In the same way where a victim or innocent third party has evidence on a computer and the investigating officer is happy to return the original computer to them our practice is to give the imaging of the computer an immediate priority but then return the submission to the queue once that has been done.

The following factors could be considered as criteria for case acceptance and prioritisation.

Is it technically feasible to achieve what has been requested?

This is something that is unlikely to be decided by someone other than a member of the unit, but will normally involve discussion with the submitter to clarify exactly what the request is.

What is the strength of the intelligence to indicate that there is evidence on the items submitted for examination?

This falls into three broad categories,

Direct – someone has seen the evidence on the computer, typically one user of a computer has found that another user has been downloading illicit material, or observed this happen.

Circumstantial – an offence has been committed involving the use of a computer and the IP address check leads to an address where a computer is found. This is often the case in indecent image downloading, online frauds, or hacking.

None – a suspect has been arrested for an offence and there is no evidence to indicate that the computer has been used in connection with the offence but the investigating officer wants to exhaust all possible lines of enquiry by searching a computer for any evidence that might possibly exist.

If the information could have impact, what is the value of the information to the case compared to the cost to recover it?

This comparison will only produce a result which is at some point on a continuous scale and it is for the manager of strategy for the unit to decide at what position on the scale any cut-off point lies. This cut-off point may be moved at times depending on capacity and demand.

The question of value to the case needs to be considered carefully. Not all requests will be able to have any impact on a case. For example there might be a case where someone is arrested for rape, the issue in the case is one of consent, the suspect is in custody when the computer is seized i.e. they have not had opportunity to use it after the incident, the computer has been used for communication between the parties prior to the incident but none of the content is in dispute or goes to the issue of consent. In these circumstances the examination of the computer might provide the detail of the communications and chronology but it is not going to have any impact on the issue of consent. In these circumstances the work required to carry out the examination could be considered to be disproportionate to the value of any result.

The impact can fall into one of the following categories.

a) The evidence on the computer amounts to a defence to or a rebuttal of an allegation.
b) The evidence on the computer constitutes the offence, without which there would be no case. This typically involves offences of possessing and making indecent photographs of children.
c) The evidence on the computer is a significant part of the evidence in the case, typically investigations where the computer has been used to facilitate the offence but there is also evidence elsewhere. This could be a suspect's computer in Computer Misuse Act offences, online fraud, malicious communications, harassment and grooming.
d) The evidence on the computer corroborates other evidence. This might be cases such as sexual offences where there is witness evidence that is supported when a suspect communicates using the computer and indicates knowledge of the age of a victim or lack of consent.
e) The evidence on the computer is peripheral. This is where the evidence sought is not direct evidence of the offence nor corroborates some direct evidence but provides some background information or some other information remote from the offence in order to fill in a biography or lifestyle of a suspect. This may also include cases in which there is sufficient evidence for a realistic prospect of conviction prior to any computer examination.
f) The information sought is not evidence of an offence but is for intelligence purposes only.

Cost of examination

In a public service setting this is a difficult area to manage unless the cases are outsourced against a finite budget, or there is some clearly defined system of charging between departments.

In some areas of the police a department may have a fixed budget for an area of work and has to manage that budget by carefully choosing the volume and cost of goods and services purchased. Once the budget has been spent it is not possible to make any more purchases.

This could be applied in digital forensic units and would seem to be a possible solution to managing the increasing demands made on the units. There is clearly only a finite amount of work that can be done by a group of individuals within a given period of time. Any demands beyond that capability will only result in increased backlogs. This is an area that does not seem to have been successfully addressed in any unit.

It should be possible to calculate how many working hours the unit has available during a given period taking into account abstractions for annual leave, training, sickness, court, etc. Those available working hours could be allocated to the internal customers based on factors such as volume of previous submissions, volumes of particular categories of crime that usually involve computer examinations, or just simply equally amongst all.

When jobs are submitted to a unit they could be assessed by the manager in order to estimate the time to carry out the examination. In some cases the estimate might be to complete the full examination, in others where it is considered to be a more complex case it could be a staged estimate for parts of the examination.

A process such as this will cause those who use the services of the unit to carefully assess the need for and extent of any examinations. It seems that if there is no restriction on the quantity of submissions that can be requested then those authorising submissions are under no obligation to manage them carefully. There is no incentive to make decisions on whether or not to make a submission based upon the need and risks involved. The introduction of such a system would encourage those using the service of the units to manage their demands.

Where does the particular investigation lie in your organisation's list of priorities?

This is a question to be answered by a manager responsible for strategy in the organisation. The offence under investigation and the status of the suspect are two important factors in considering this question. The offence might be relatively minor but may be one of the organisation's priorities; it may be an acquisitive crime where the value is small compared to the cost of an examination. The suspect may be a member of an Organised Crime Group, a member of your organisation or someone in a public office and these might be considered a higher priority.

It might be worth listing groups of crimes in an order of priority and indicating a position in the list below which an examination will not be considered.

Which case to examine first?

As discussed some of the factors mentioned above to be considered for case acceptance also have an influence in deciding an order of priority for the examinations. It might be that the unit's policy is to accept all cases but to place some so low in the list of priorities that they never get done or are so old as to be stale and would attract an abuse of process argument. It is suggested that this is not a reasonable way to approach the task; it must be wrong to suggest to a victim that their case will be investigated when in actual fact it is so low on the list of priorities that it takes an unreasonable length of time or a decision is made later that it has gone stale. Similarly it must be wrong that a suspect who may well be ultimately innocent has to wait many months to hear that the investigation has ceased without conclusion. Equally where a suspect is taking responsibility for their actions and wants to have their case dealt with expeditiously then it is surely inappropriate to delay that case.

There are two main approaches to prioritisation, one is to make ad hoc judgments based on the experience of the assessor, and another is to use some sort of scoring matrix.

It could be argued that if the ad hoc approach is used then there must be some reasoning behind the judgments such that they could be analysed and put into a matrix.

Another approach that has been used is to deal with urgent cases as a priority and then the remainder are dealt with in date order. Urgent cases might be defined as those where a life is at risk or a child is at risk of serious harm and examining the computer will relieve that risk. The argument for this method is that there is often so little difference between cases that it is impossible to consider one more important than another so they get dealt with in date order. There may be occasions where a case stands out as not fitting the urgent criteria but requires prompt action; such cases can be given an appropriate priority. The advantage of this system is that it minimises time assessing each case.

The various forces that use a matrix system all include common factors in their matrix, some go into more detail than others and some have an "X Factor" where the assessor can add on a large score that significantly increases the priority. This latter point would seem in some respects to defeat the logic of having a matrix; if such factors exist why not include them in the matrix?

There are many factors which are common to each matrix but one which appears to be universally absent is one of cost. The number of items submitted and the complexity of the examination are rarely considered in a matrix but should surely be a key factor on deciding whether or not to accept a case or where it fits in the list of priorities.

If cost is included in the matrix it perhaps needs to have a negative score to offset all the other positive scores, alternatively the cost could be used as a divisor for the score to obtain a ratio of score against cost.

The following are broad headings which could be considered in a scoring matrix.

- Impact/likely value to the case – essential through to intelligence only.
- Cost – the impact of the number of computers and other items to be examined and complexity of examination.
- Type/seriousness of crime.
- Risk of not examining or delaying examination – risk to life, serious sexual assault, financial loss, etc.
- Status of investigation – has someone been arrested, are they in custody or on bail, etc.
- Status of the owner of the computer –person in authority, member of OCG, Level 1 criminal, victim, innocent third party, etc.
- Level of initial intelligence supporting the fact there is some evidence on the computer.

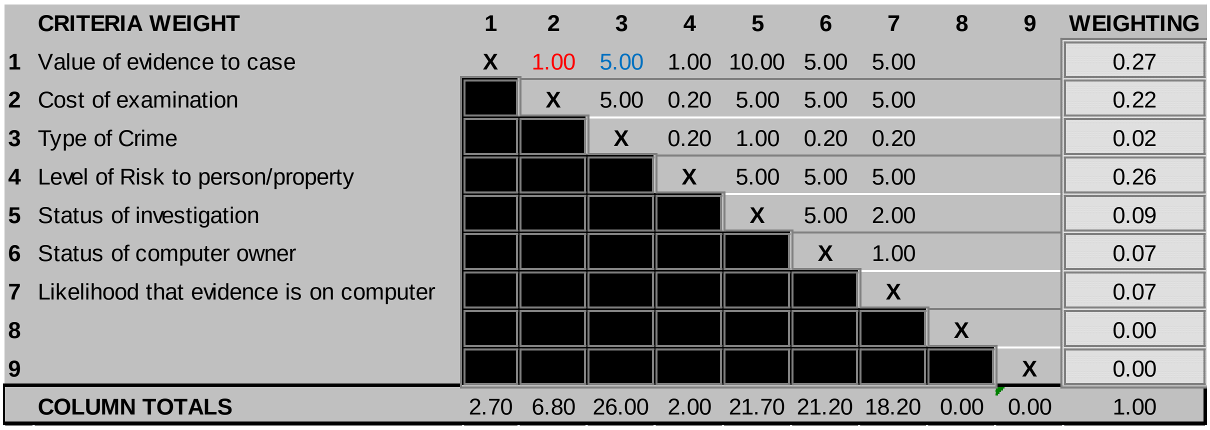
Any factor relevant to an examination will generally fit into one of these headings. It has to be decided how important each of the headings is; are they all equally important or is one or other more important?

In an attempt to make this slightly more scientific a spreadsheet used by TREQ Corporation(1) has been adapted to develop a matrix. The principle of this is that each criterion in a matrix is compared with the others and given a comparative value.

The following values are allocated –

10	MUCH MORE VALUE
5	MORE VALUE
1	EQUAL VALUE
.20	LESS VALUE
.10	MUCH LESS VALUE

This has been done for each of the broad headings above and the following table shows the result.

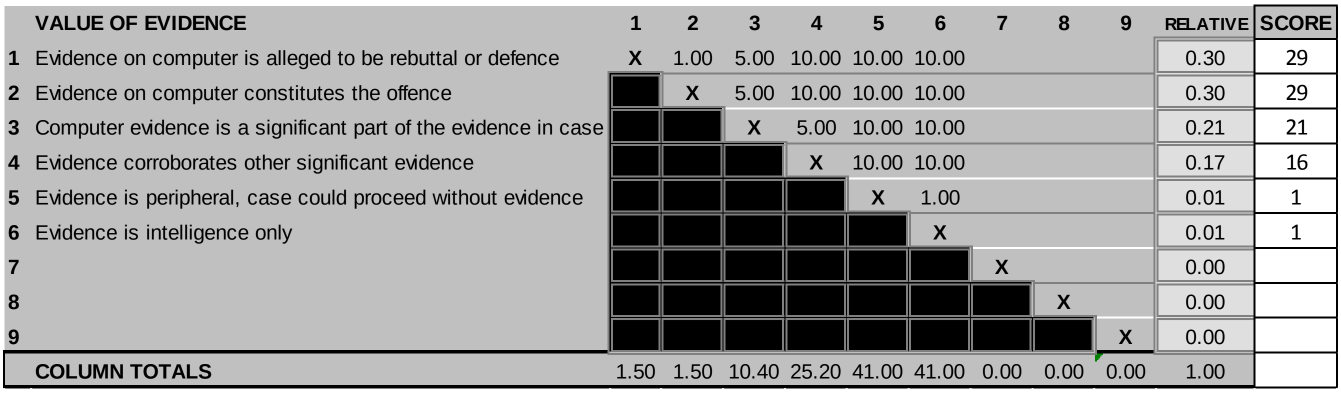


	CRITERIA WEIGHT	1	2	3	4	5	6	7	8	9	WEIGHTING
1	Value of evidence to case	X	1.00	5.00	1.00	10.00	5.00	5.00			0.27
2	Cost of examination	■	X	5.00	0.20	5.00	5.00	5.00			0.22
3	Type of Crime	■	■	X	0.20	1.00	0.20	0.20			0.02
4	Level of Risk to person/property	■	■	■	X	5.00	5.00	5.00			0.26
5	Status of investigation	■	■	■	■	X	5.00	2.00			0.09
6	Status of computer owner	■	■	■	■	■	X	1.00			0.07
7	Likelihood that evidence is on computer	■	■	■	■	■	■	X			0.07
8		■	■	■	■	■	■	■	X		0.00
9		■	■	■	■	■	■	■	■	X	0.00
	COLUMN TOTALS	2.70	6.80	26.00	2.00	21.70	21.20	18.20	0.00	0.00	1.00

In line 1 of this table the criterion 1 - “Value of evidence to the case” has been compared to the 2 - “Cost of examination” and it is considered that they are of equal value (=**1.00**) . Next, 1 - “Value of evidence to the case” has been compared to 3 - “Type of Crime” and it is considered that the value of evidence is of more value than the type of crime (**5.00**). The values are entered in line 1 and a reciprocal value is automatically entered in the cells which are blacked out.

The spreadsheet totals all the values and in the final column gives a relative value and these can be used to weight scores from each criterion.

The same process can then be applied to the factors that make up each of the criterion. The following table shows an example for “Value of evidence to the case”.



	VALUE OF EVIDENCE	1	2	3	4	5	6	7	8	9	RELATIVE	SCORE
1	Evidence on computer is alleged to be rebuttal or defence	X	1.00	5.00	10.00	10.00	10.00				0.30	29
2	Evidence on computer constitutes the offence	■	X	5.00	10.00	10.00	10.00				0.30	29
3	Computer evidence is a significant part of the evidence in case	■	■	X	5.00	10.00	10.00				0.21	21
4	Evidence corroborates other significant evidence	■	■	■	X	10.00	10.00				0.17	16
5	Evidence is peripheral, case could proceed without evidence	■	■	■	■	X	1.00				0.01	1
6	Evidence is intelligence only	■	■	■	■	■	X				0.01	1
7		■	■	■	■	■	■	X			0.00	
8		■	■	■	■	■	■	■	X		0.00	
9		■	■	■	■	■	■	■	■	X	0.00	
	COLUMN TOTALS	1.50	1.50	10.40	25.20	41.00	41.00	0.00	0.00	0.00	1.00	

This might appear to be an elaborate process but it is only done initially in order to decide weightings for each criterion, once this has been done it is a simple matter to assess each case by selecting the score in each of the seven broad categories and adding them together. A finished version of the whole matrix is available for download(2) and can be customised with your own criteria.

Who makes the decisions?

Traditionally the digital forensic unit manager has taken on the responsibility for case acceptance and prioritisation. This might be a good approach if a scoring matrix is used as it is likely there will be a consistent use of the matrix.

Alternatively if no matrix is in use this might not be the most appropriate approach. The cases being investigated are the responsibility of the division or department and it makes more sense that they decide which of their investigations have priority over others belonging to them. It also makes sense that if they are to manage the volume, quality and validity of submissions then one person in that division or department should take responsibility for overseeing all of their digital forensic submissions.

A two tier approach could be used –

- The divisional assessor makes an assessment of the case and agrees it is worthy of submission.
- Submission is then passed on to the unit and assessed against case acceptance criteria at the unit.
- If accepted it is listed at the unit as queued work.
- When the unit is ready for further work it asks the divisional assessor to nominate their next job.
- The unit manager goes round the divisions in turn requesting their next job.
- The unit manager only has to prioritise the current jobs which have been nominated by divisions.

Monitoring Results

It is important to capture in a database some key details from each submission, for example the information used to score the matrix –

Value of evidence to case

Cost of examination

Type of Crime

Level of Risk to person/property

Status of investigation

Status of suspect

Likelihood that evidence is on computer

It is also important that the results of any examination are recorded so that this data can be used to influence and justify decisions made in case acceptance and prioritisation.

It is the broad nature of the result not necessarily the detail that will be used for this purpose.

The result could be recorded by category of evidence found –

Evidence of rebuttal or defence

Evidence essential to case

Evidence significant to case

Evidence corroborates other evidence

Evidence peripheral to case

Evidence is intelligence only

No evidence found

It is also useful to capture details of the number type and size of each piece of digital evidence submitted. This can be used to monitor the volume of submissions and support requests for more resources where appropriate.

In order to monitor trends it is useful to monitor the broad type of evidence sought, e.g. documents, pictures, chat, email, internet history, financial records, keywords, etc.

Feedback from the internal customer is another item of information that could be useful. One force requests feedback after finalising cases. The feedback request is a simple choice of positive/neutral/negative and a short optional narrative. The feedback in this force has been generally positive but where there has been negative feedback it has been relating to the delay in having the submission examined. This could be useful in a business case for increased resources.

Points at which a software triage process can be applied

Traditionally computer forensic practitioners have been very conservative when there has been a suggestion that someone other than a fully trained practitioner should become involved in a computer examination. In the UK there appears to be some movement on this position with a gradual acceptance that the volume of work cannot be managed by examining each and every item submitted for examination.

Before using any triage process consideration must be given to the law in your jurisdiction. What responsibilities are placed upon an investigator when conducting a criminal enquiry? It might be that you have a responsibility to conduct all reasonable enquiries which might include a relieving caveat where there are large volumes of information. It might be that case law dictates that you have to consider capturing sufficient evidence to enable the defence to have a reasonable opportunity to examine material which may be exculpatory.

Consider which enquiries if any you are bound in law to do and which could be prejudicial to your case if you don’t. The whole issue of managing the volume of digital forensic examinations is bound closely with managing risk. There is risk involved in allowing probable offenders to carry on offending for 12 months while waiting for a computer examination and there is a risk of missing something by failing to conduct a complete examination; finding the balance is fundamental in any policy on triage.

There are three broad groups of staff that could conduct a software triage –

1) Minimally trained first responder

2) Dedicated local divisional resource with basic training

3) Experienced forensic practitioner

The triage process could be carried out at any of three points in time –

1) At the point of search and seizure

2) On arrival at the local station

3) On submission to the forensic unit

The choice of which resource and at what point the process is undertaken depends upon the level of risk willing to be undertaken by the organisation.

- The less training the user has and the less frequently they carry out a software triage the greater the risk of failure.
- The further from the unit the process is carried out the lesser the control and scrutiny which can be exercised by experienced staff.
- Triage at the point of seizure involves the greatest risk as it is likely to be carried out by the least experienced staff, in a stressful and possibly hostile environment, with a limited time in which to carry out a triage, equipped with the most basic technical knowledge to make difficult judgements.
- Using staff within the unit will have considerably less impact on reducing backlogs than using external staff, but should provide the highest level of confidence.

Choosing a software triage strategy

A strategy will depend very much on the type of work carried out in the unit. It is unlikely that it will be possible to define a blanket policy covering all types of forensic examinations. It is useful to break down the types of work carried out and examine each area to see whether or how a software triage can be best used in each area.

For example, in choosing our strategy we looked at which area of work provided the largest volume of submissions. In any police unit this is probably quite simple as it is likely to be sexual offences, usually involving indecent images of children. In our case this amounted to 60% of our total work; the remainder of work categories were all single figure percentages.

The next consideration was to decide whether trained forensic examiners within the unit would carry out the triage process or if it would be possible to use staff outside the unit with minimal training.

The choice of triage software, ADF Solutions Triage-ID(3), was the key factor in deciding to use staff outside the unit.

In our case the Triage-ID software is configured by trained forensic practitioners within our unit and then used by staff on divisions to conduct triage examinations. The person conducting the examination needs only to perform a simple procedure to set up the search criteria and then ensure the target computer is configured to boot from the Triage-ID CD.

By limiting the use of the triage software to one area of offending it has simplified the use of the software.

The triage software is configured to search for –

1. Indecent images using a large hash set of known images.
2. Indecent images using fuzzy matching of 25,000 known images.
3. Text string search for common terms found in indecent image cases.

The contention is that if these searches are all negative then the likelihood is that the computer has not been used in connection with this type of crime. In any case before a final decision is made the results of the triage are considered in the context of the original intelligence and if there is any doubt a full forensic examination can be conducted.

With one exception explained later it has been stipulated that any results from a triage examination will not to be used as evidence but will be used only as intelligence to assist judgements on how to proceed with an investigation.

The software triage strategy has been adopted in four distinct areas of work –

Sex Offender Management Teams

In the England and Wales persons convicted of certain sex offences can be placed on the Sex Offender Register. Police forces usually have dedicated units whose responsibility it is to manage these offenders whilst on the Register; this usually entails regular visits to the offender's home address. There are occasions when the officers visiting the sex offender might want to conduct a brief examination of a computer during the visit.

The officers have been trained to use the triage software to conduct this brief search. The search cannot take very long, perhaps an absolute maximum of 30 minutes, and the software can be configured (by the forensic team) to target specific areas of the computer to limit the time taken. The search could be based on the experience of the forensic practitioner targeting common areas which generally produce positive results, based on the offender's previous history of offending, or based on specific current intelligence.

The benefit of this method is that the officer carrying out the search can do so with limited training and knowledge of computer forensics but the search can be carefully targeted using the knowledge and experience of a trained forensic practitioner. The search can also be carefully crafted so that it will be completed within a limited period of time.

Child Abuse Investigations

It is not unusual in a case of a contact sexual abuse investigation that the offender owns and uses a computer. Often it would be a consideration for the officer in the case to request an examination of the suspect's computer in order to conduct a thorough investigation. However where the offence under investigation does not involve the use of a computer and there is no direct evidence of the use of the computer in connection with some offence it is difficult to justify the use of the limited resources of the digital forensic unit to examine the computer.

Members of the Child Abuse Investigation Unit have been trained to use the triage software and in these circumstances they can conduct a triage examination of any recovered computer. Where there is a positive result the computer can be referred for a full forensic examination.

Where the offences under investigation do include the allegation of some indecent images the likelihood is that a full forensic examination will not be completed before the investigating officer has to attend a child protection case conference. In these cases they can conduct a triage examination of the computer and attend a case conference with some intelligence and be in a position where the case conference can come to more informed decisions.

Identifying computers for full examination from multiple submissions

Multiple seizures of computers from one address have become commonplace, it is not unusual to see seizures of up to ten computers for a single case of an indecent image investigation. The team conducting the majority of these online investigations within the force have been trained to use the triage software. In all cases they triage the computers seized in order to identify those which contain indecent images and only those computers identified are submitted for a full examination.

Full prosecution using just triage results

With the agreement of the CPS we have introduced a practice whereby a suspect can be cautioned or prosecuted based on the result of a triage examination in a limited set of circumstances -

- The intelligence indicates that the case is one of simple possession of indecent images.
- The suspect's computer has been triaged and indecent images have been found.
- The images found have been put to the suspect in interview and they have made unequivocal admissions as to culpability.

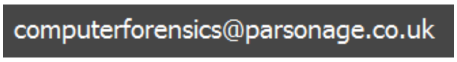
It is accepted that in some cases the full extent of the offending of the suspect might not be revealed but it is suggested that the benefits of this process outweigh the risks. The suspect will be dealt with considerably quicker and thus be on the Sex Offenders Register being monitored.

The first conviction using this process was achieved on 5th August 2008 and the counsel who prosecuted commented in a post trial advice, "I understand that this is the first case to be concluded which involved the use of the new Triage tool. The efficiency of it is most impressive – in this case I note the examination occurred on 5th June 2008 and within 2 months the Defendant has pleaded guilty and has been sentenced."

Results of the triage strategy

In the ten months following the introduction of this triage strategy the number of computers waiting to be examined reduced from 254 to 139, the length of the backlog went down from twelve months to seven months. There has been a positive response from all the divisional staff who have been trained to use it; the fact that they have been empowered to do something they have not previously been able to do has reduced considerably the frustrations felt as a result of backlogs in forensic examinations.

I welcome feedback, comments and discussion on the content of this paper. I would be particularly interested to hear from anyone who has developed a system of costing and charging for services within a public service setting.



computerforensics@parsonage.co.uk

1. **II, Edward D. Carpenter.** Prioritization Matrix. *SixSigma.* [Online] [Cited: 17th June 2009.] http://europe.isixsigma.com/library/content/c060529a.asp .

2. **Parsonage, Harry.** *Computer Forensics Miscellany.* [Online] June 2009. http://computerforensics.parsonage.co.uk.

3. *ADF Solutions Inc.* [Online] http://www.adfsolutions.com/triageid.php.