CIT 2011

Evaluation Report

Dr Tom Cockcroft, Canterbury Christ Church University

Introduction

Survey Responses 9

MAC Forensics 10

Post-Preparation Meeting Trainer Evaluation 10

Student Course Evaluation 16

Post-Course Trainer Evaluation 23

Network Forensics 30

Post-Preparation Meeting Trainer Evaluation 30

Student Course Evaluation (by day) 37

SSD Forensics 66

Post-Preparation Meeting Trainer Evaluation 66

Student Course Evaluation (by day) 73

Student Course Evaluation (overall) 91

Post-course Trainer Evaluation 100

**Introduction**

This evaluation was undertaken to establish the extent to which the CIT 2011 newly developed courses satisfied student needs in regards to the acquisition of appropriate knowledge. This is the rationale behind the student-centred aspects of the evaluation.

The CIT 2011 project was also undertaken to develop a set of resources which would be replicable in terms of content delivery and assessment. For this reason, the views of trainers and those involved in course delivery have also been surveyed.

To achieve a fully-rounded evaluation of the pilot process, three surveys were conducted.

**Survey One – Post-Preparation Meeting Trainer Evaluation**

This survey was directed at course trainers. It was used to establish their views regarding the effectiveness of the planning meeting, a week long meeting focusing all aspects of course delivery and assessment.

Trainers were asked;

Did you feel that there was an appropriate gap between the kick-off meeting and the planning meeting?

Did you feel, between the kick-off meeting and the preparation meeting, that you had sufficient contact or support?

Did you feel that the preparation meeting was the correct length?

Did you feel that the team had a sufficient number of trainers?

If there are remaining tasks to be undertaken prior to the delivery of the course, do you feel that you have sufficient time to complete these successfully?

Do you feel that your role in the training delivery has been made clear?

Are you happy with your role in the delivery of the training?

Do you feel that you have been provided with sufficient guidance regarding assessment?

Do you feel that you have been provided with sufficient guidance regarding course design?

Are you happy with the room resources that have been allocated for course delivery and assessment purposes?

Are you happy that all available software and hardware requirements have been agreed?

How satisfied were you with the travel and accommodation arrangements provided by the Project Management Team?

How satisfied were you with the venue facilities provided by the academic partner?

Are there any issues, positive or negative, that you would like to share with us regarding this week’s preparation meeting?

**Survey Two – Student Course Evaluation**

This survey was directed at students who had completed the course. It was used to establish their views regarding the effectiveness of the course in meeting their expectations. Similarly, student’s perceptions of venues and project management were surveyed.

Students were asked;

How helpful did you find the course?

Which session did you feel was the most successful? Why?

Which session did you feel was the least successful? Why?

Can you think of any subjects that could have been addressed in the course which were not covered?

In terms of the combination of practical and theoretical work on the course, would have preferred to see: more practical work, more theoretical work, or no change?

During this course have you learnt skills/acquired knowledge relevant to your workplace?

Will the quality of your work improve as a result of this course?

How satisfied were you with the teaching venue for the course?

How satisfied were you with the accommodation?

How satisfied were you with the way travel and accommodation arrangements were managed?

Would you recommend the training to other colleagues?

Are there any other comments that you would like to make regarding any feature of this course?

**Survey Three – Post-Course Trainer Evaluation**

This survey was directed at trainers who had recently contributed to course delivery. It was used to establish their views regarding the practical aspects of course delivery.

Trainers were asked;

Did you experience any hardware issues whilst delivering the course?

Did you experience any software issues whilst delivering the course?

Did you feel that you had sufficient training/experience to deliver training to an ‘international’ cohort of students?

Do you believe that the assessments worked well as a means of testing student’s knowledge?

Do you believe that the students who attended the course had a sufficient level of knowledge/experience to undertake the course?

Do you believe that the students who attended the course had a sufficient level of the English language to undertake the course?

Having just finished delivering the course, are there any substantial changes you would make to the way the course could be delivered in the future?

Having just finished delivering the course, are there any substantial changes you would make to the content of the course in the future?

If you went through this process again, would you have used your time at the Preparation Meeting differently?

Were you able to stick to the timetable? Did you have to modify it in any way?

Was the venue appropriate for the course?

Did you feel that sufficient support was made available to trainers from the Management Team?

Are there any final points that you would like to make regarding the delivery of the course?

**A note regarding variations in survey style between courses**

There is a small amount of variation in the format and use of the surveys between the different courses that make up this programme. Due to the timing of the courses, the Evaluation Manager was unable to attend them all, so three different individuals created evaluation data, using two different surveying tools. There were some challenges regarding using the VLE (Blackboard/ClicLearn) to deliver the surveys so two publicly available digital surveying tools were used which presented some challenges in respect of different colleagues accessing the Evaluation Manager’s account 9due to the requirement of access to the Evalaution Manager’s private email account).

As a result some variations have occurred;

MAC Forensics – All surveys as described above.

Network Forensics – Survey One complete, Survey Two (completed once for each teaching day and one for the exam), No survey Three

SSD Forensics – Survey One complete, Survey Two complete (plus 4 ‘daily’ surveys with less questions), Survey Three.

Despite these variations, the Evaluation Manager believes that the gathered data presents a very effective overview of trainer and student perceptions of the courses, their planning and delivery.

Survey Responses

MAC Forensics

Survey 1 – 4

Survey 2 – 12

Survey 3 – 4

Network Forensics

Survey 1- 3

Survey 2 – Day 1 (18), Day 2 (18), Day 3 (18), Day 4 (17), Day 5 (16)

Survey 3 – n/a

SSD Forensics

Survey 1- 5

Survey 2 – 19. Day 1 (21), Day 2 (18), Day 3 (21), Day 4 (19)

Survey 3 - 2

**Survey Responses**

**MAC Forensics**

**Survey One – Post-Preparation Meeting Trainer Evaluation**

**Survey Two – Student Course Evaluation**

**Which session did you feel was the most successful? Why?**

“Live data acquisition”

“Live forensics and finding Macartifacts”

“Artefacts”

“Mac Artifacts”

“Live Forensics”

“Artifact…showed where to look for important information”

“Command Line Basics…because we’ve learned practical things”

“Command Line Basics, cause it gave you a really good understanding about commands which will be really useful in future investigation”

“Those related to line commands”

“Live data acquisition…to show me something I will really need in the field”

**Which session did you feel was the least successful? Why?**

“Log files”

“Maclogs, too fast many logs”

“Logs…I got lost on the way trying to keep up while looking through log with terminal”

“Operating System…just mainly because the presentation went really fast”

**Can you think of any subjects that could have been addressed in the course which were not covered?**

“Windows Bootcamp”

“’Real’ evidence handling. Just trying the learned new things on some evidence”

“There was too much information…it can’t be covered in 5 days”

“Maybe something related with IPad and IPhones should be included (about the traces they leave in a Mac). i.e. how to analyse an IPhone backup”

**Are there any other comments that you would like to make regarding any feature of this course?**

“Exchange the last day assessments with guided practice exercises”

“Sometimes presentations were rushed through in order to keep the schedule. Therefore some presentations should be shortened. It would be nice if the last hour or two of thursday could be spent on questions from the participants in order to clarify issues or questions that might have come up. This would also help prepare for the assessment. A bit too much focus on command line rather than GUI tools/solutions. A bit more hands-on would be nice although that can be difficult and time consuming due to mixed skill levels”

“a very great THANK YOU!!!! i nice and very interesting course, that must continued, and for the future, if it´s possible - longer time - with more practical working (cases like the last assessment) (learning by doing. maybe an idea for the future, before the curse start, the students, sent specific questions to the curse responsible (maybe one or more answers can be given in the presentations”

“Had a good week but i would have like a little more practical”

“i think the course is good to get basic knowledge about apple HW and mac software. it was also show how to use mac in our work to get most of the information needed in forensic work. I liked the course and it inspired me to use and improve my new mac os knowledge. thank you”

“Just that the all the involved people in this course has really done a great job”

“Maybe it would be useful to have the documentation (presentation, tools, etc..) in advance, so you can prepare classes with time. I will also find useful to have the presentation in paper just to make it easier to takes notes. Thank you for this perfect course”

“It was a great way to get used with some tools for mac forensic”

**Survey Three – Post-Course Trainer Evaluation**

“Not all of them,. But most did. Some did not have interest.”

“Not all students did attend basic forensics courses before. Many of them were lacking basic knowledge in command line use. For next courses a preread material ‘Command line basics’ would be desirable”

“Preread-material “Command Line Basic” is needed, but no substantial changes to the course sessions”

“Not really! Shorter and more goal-directed Reviews could be used to point to the goals”

“I would ask more questions about the lesson to the students and put more examples. In fact I would change some slides to add more examples”

“We had a HDD crash that made us skip the final lesson on Thursday. Otherwise the timetable was good”

“Timetable corrections had to be done because of technical issues belonging to Spotlight and sometimes too long Review Sessions. Had been fixed by skipping less important material”

**Are there any final points that you would like to make regarding the delivery of the course?**

“The assessment could have been done in another way. The questions could have been written down earlier. Perhaps all the trainers need to stay until the final day to help out with the practical”

**Network Forensics**

**Survey One – Post-Preparation Meeting Trainer Evaluation**

**Are there any issues, positive or negative, that you would like to share with us regarding this week’s preparation meeting?**

“I do feel that with five trainers and two course managers who are both involved as trainers, that there are too many involved in each element of the course. This meant that no-one readily accepted responsibility for each section, although I think this was fine tuned at the end of the meeting. There has been minimal contact with the rest of the team in the period between kick-off and preparation. Another thing that has been frustrating in the preparation is that too many people have ideas about other sections, but then are not prepared to become involved in the development or teaching of that section, meaning that one trainer could be left with material that they may find difficult to prepare.”

**Survey Two – Student Course Evaluation (by day)**

**Monday**

**Which session did you feel was the most successful? Why?**

|  |
| --- |
| “Pretest is very helpfull to know our level of knowlodge” |
| “Entrance Test. Should have been passed in advance, as originally intended.” |
| “Linux session. The session was very understandable and quite easy to follow.” |
| “Hacking Introduction lesson, because this was the first main session to cover  the vectors and types of attacks available.” |
| “The pre-test. It just show how really thin we are, and that we need  continuous education (and self education).” “Linux introduction was quite interesting and refreshing. “ |
| “Basic of security” |
| “Introduction to Linux” |
| “linux session” |
| “The last session (Attacks) was the most successful, because it was not an  introduction. It leads to the main network theme.” |
| “Last session. Because of my own interest.” |
|  |
| “as the first day of the course it was quite good started smooth then geared  up along the day” |
| Linux. Some new stuff. But still to much in too little time.” |
| “All sessions where successful.” |
| “linux because we could discuss it peacefully “ |
| “the linux one” |
| “How hackers work” |

**Which session did you feel was the least successful? Why?**

|  |
| --- |
| “introduction” |
| “Installing Ubuntu. Because there were technical problems and because this is  not a linux course. “  If there is knowledge about the linux operating system needed during the  course, well then make it a necessary fact required to enter the course.” |
| “The exam in the beginning of the day. Because of poor result.” |
| “Introduction to Linux, due to technical issues with the computers it was not  possible to follow the practical exercises.” |
| “last session. a lot of well known theory...” |
| “The Linux lesson was the last successful, because I know Linux quite well.  Every expert should be able to install an Linux distribution and he should know  the basic commands of the shell.” |
| “the final one it was bit fast “ |
| “Hacking theory. Done that during one of OLAF trainings.” |
| “the last one, because i think everyone was tired” |
| “the last one” |
| “Maybe too long sessions, too much information.” |

**Can you think of any subjects that could have been addressed in the course which were not covered?**

|  |
| --- |
| “practis” |
| “Practis” |
| “More Linux practical training. “ |
| “I am missing a practical part.” |

**Are there any other comments that you would like to make regarding any feature of this course?**

|  |
| --- |
| “A little bit too hot. Toilets really interesting...” |
| “Cooler rooms please.” |
| “The classroom is too hot! Maybe too low level, at least first day. I think Linux  knowledge is a must, before entering the course” |

**TUESDAY**

**Which session did you feel was the most successful? Why?**

|  |
| --- |
| “metasploit and nessus” |
| “Practical excersize with Nessus and Metasploit. Because the material was  very interesting and I managed to follow it and understand it and I will be able  to use it in the future.” |
| “Infrastructure Attack-very nice demonstration of capatibilities of open source  programs... even usable in law enforcement manner.” “Network intrusion Investigation Methodology-That is quite useful to know  how to prepare our collected data in form of evidence.” |
| “wireshark session, it's useful at work” |
| “The one with de rabbit game, because it was a practical trainning, in which  we identified for ourself the vulnerabilities. “ |
| “Logfileanalysis” |
| “Logs. Where to find logs and how to use them.” |
| “practical use of nessus and metasploit, because network forensics has to do  with vulnerabilities” |
| “Regular expresions” |
| “wireshark” |
| “first, metasploit” |
| “grep session” |
| “Linux logs, search.” |
| “The Metasploit "hacking" was very nice but also Anders URL-tampering  was really interesting” |
| “grep cause it can be used in very different ways” |
| “First session.” |
| “The GREP was the most successful, due to the interaction levels with the  class.” |

**Which session did you feel was the least successful? Why?**

|  |
| --- |
| “The one with logs. Too much theory, and less practice, according that there  are so many linux command to remember, that the effect is almost zero if isn't  followed by a good practice work.” |
| “The logfile theme, it was not depth enough. There has to be a practical  exercise on a real case, to see how manipulating data is investigated.” |
| “regex, because regex is a general concept that has not specifically to do with  network forensics” |
| “regex. it was dificult. but impposible” |
| “Hacking - interesting but not very practical from the forensic point of view” |
| “None but it is a problem that the computers language is in german/french.  I also think that many people in the class never finished todays excercises” |
| “the pratical due to techinical fault but yet again i could follow the lesson” |
| “Last session. Too much regular expressions.” |
| “The start of the session on TCP/IP, man in the middle although it contained  useful information was presented out of order, it felt jumpy.” |

**Can you think of any subjects that could have been addressed in the course which were not covered?**

|  |
| --- |
|  |
|  |
| “Preparing collected data in form of evidence - best practice of EU members countries – experiences” |
| “How to investigate logfile manipulations. “ |
| “practice on attacks and how they function” “analyzing captured network traffic” “analyzing real world log files” |
| “Let the computers be ready for the class, not like usually we must install and fix some on the way” |
| “more practical excerices from linux” |
|  |
|  |

**Are there any other comments that you would like to make regarding any feature of this course?**

|  |
| --- |
| “A/C :)” |
| “The themes could be less, but they should be more deeper. I want to learn  some specialities, that do not everybody knows. Experienced and older  examiners should show their tricks.” |
| “focus on network forensics instead of covering basics of e.g. linux and regex.” |
| “all equipment are in German. it's realy ...” |
| “To many information in too little time. QandA suffers. Practical suffers.” |
|  |
|  |
|  |

**WEDNESDAY**

**Which session did you feel was the most successful? Why?**

|  |
| --- |
| “egrep” “funny and interesting to find sth in log files” |
| “Logs, it was very helpful to refresh knowledge of raw search.” “IP & DNS, very well explained and demonstrated.” |
| “The morning session with Linux commands because I managed to exercise  these commands.” |
| “Linux lesson from this morning, because it was more practical than the last  days, with examples and good explanations.” |
| “the RegEx-presentation and MarcoÅ› one” |
| “no one” |
| “The lession about dns. Because its a network theme. But it was not enough  time to understand all topics. Too much time to test. Too less time for  explanation.” |
| “skype one cause it can be used quite easily once back home” |
| “Using web browser to send data to the server.” |
| “actual log file analysis with real log files” |
| “Skype geolocation” |
| “regex session, server side attack - amazing, but very quick “ |
| “Skype. New information, practical use, cool tool” |
| “The Skype IP-demo. Very interesting and useful” |
| “Skype” |
| “The actual investigating a network intrusion, through log files.” |
| “Skype user geolocation, because i need it at work” |

**Which session did you feel was the least successful? Why?**

|  |
| --- |
| “The practical exercise with evidence file because it was rather too fast and  not quite understandable for me.” |
| “Hacking lesson with Anders! Despite the fact he's good in what he's doing, it  was so many thing regarding a sensible domain (hacking a webpage), that I  hadn't enough time to think and understand every command that he had  done.” |
| “The skype lession, because I dont need it at work. “ |
| “cross site scripting the instructor was not well prepared to deliver the lesson” |
| “xss, too short, not very understandable” |
| “XSS” |
| “cross site scripting attack - she doesn't understand what is she talking  about...” |
| “Cross Scripting. Short, not very indepth. “ |
| “Margarita’s session” |
| “First one” |
| “Am I on a network investigation course? or how to break into things course?  The grep although good, had too much time spent on it.” |
|  |

**Can you think of any subjects that could have been addressed in the course which were not covered?**

|  |
| --- |
| “A daily repetition.” |
| “better teach what to actually look for in log files, what log files to look for in  the case of web servers, mails, system logs, ...” “how can one detect whether a system is compromized or not, what to look  for ...” |
| “gut” |
| “server side attacks needs more time “ |
| “more cross scripting, php, sql injection theory” |
| “More actual investigating! “ |

**Are there any other comments that you would like to make regarding any feature of this course?**

|  |
| --- |
| “more practis” |
| “A daily repetition.” |
| “For the next course, important to have common languages and settings for  the computers and software. Perhaps also a outline of the name of every  session so it is easier to relate to them and the teacher” |
| “By MORE PRACTICAL work, more relevant practical.” “Again a lot of the day has been spent setting up software or systems.” |

**THURSDAY**

**Which session did you feel was the most successful? Why?**

|  |
| --- |
| “Practical exercise with inserting trojan. Because I didn't come across this  theme in the past!” |
| “hacking games” |
| “Suspicious files - very simple and educational overwiev of tools and  procedures, which will help us to investigate malware.” |
| “Hacking and SIP - practical use, usefull tools and info.” |
| “SIP lesson because it were discussed new things, which are very popular in  cybercrime world today!” |
| “SIP, new protocol for me.” |
| “RAT” |
| “About SIP and pbx:es. I have never worked with them earier. However, all  sessions were very interesting!!!” |
| “Darkcomet –RAT” |
| “it was a good over all today all the session could be usefull one way or an  other” |
| “Successful? The sessions today where we were actually looking at  investigating a network attack and the talking about what we are looking for  in relation to suspect files. These are relevant to the forensic investigation of  a typical network attack.” |
| “Investigators Methodology - very helpful.” |

**Which session did you feel was the least successful? Why?**

|  |
| --- |
| “break times” |
| “1. Suspicious file analysis, because this is not a network theme. 2. SIP cracking, because I will not need it for my work as forensic examiner.” |
| “SIP” |
| “SIP” |
| “compared to the other maybe the sip one” |
| “Least successful would be controlling a trojan, I cannot see how being trained  to use Trojans in so much detail is any use for investigating the malware on the  machine. It was weighted far too much for setting one up and very very little  towards identifying one on a system.” |

**Can you think of any subjects that could have been addressed in the course which were not covered?**

|  |
| --- |
| “repetition of the last day” |
| “Practical staff” |
| “sql-injections” |
| “so maybe some future trends” |
| “Quite a few, too many for this box.” |
| “more methodology of how to exactly to, how to proceed and than - in a second part - what tools to use.” |

**Are there any other comments that you would like to make regarding any feature of this course?**

|  |
| --- |
|  |
|  |
| “There should be an repetition of the last day on the morning.” |
| “trainers are very motivated and skilled - which is good - and I say this  regarding the whole week. Its just that the first two days covered - in my  opinion - topics that should be entry requirements for  this course. This includes espacially basics on linux and regular expression. The  course should be more focused on what the title says: network forensics.  Analyzing logs ... analyzing break-ins ... analyzing traces on client and server  systems ... analyzing network traffic ... “ |

**FRIDAY**

**How did you find the final exam?**

|  |
| --- |
| “There where questions from easy to hard, but it's normal, considering that  this wasn't a basic trainning! “ |
| “I think it was what we expected. It wasn't too easy or too hard.” |
| “a good over all exam about everything it was mention during this week.  although personally i would aviod question about something it was mention  very briefly “ |
| “The final exam was a challenge, this is because questions in there were from  presentations that were hurried or rushed. Not all presentations were made  available to the students. “ “Some of the questions were badly worded, that I wouldn't be surprised if  some of the students struggled to understand them.” |
| “Yes, we will se by the results. I think it was moderate.” |
| “Depends from section to section. Medium level.” |
| “It was hard because we did not have much time to prepare, but for a user that maybe  works some time in Network investigation field, then I belive that the test was  simple.” |
| “medium.” |
| “The final exam was very funy. Most of questions was not exactly  understandable. I do not know, bud I think that this exam was for network  forensic cours, not for hi level english test. The questions was writen for the  native speaker english peoples. I think, that the questions must be  understandable and on good tecnical language... bud newer mind all  finisht.” |
| “Pretty hard. So many information needed.” |
| “A bit hard. There were questions that I have never heard before” |
| “approximatl 40 questions are easy but others hard” |
| “quite hard, the questions was kind of ambigous. “ |
| “It was hard. The english phrases are not so simple to understand. “ “On some questions it is hard to receive the meaning of the questions. “ |
| “ok - but the chaos caused by the disassembling at the last 30 minutes was not  acceptable” |
| “It was okay. There have been several easy questions (e.g. Linux), but also  some to think about and to have a close look (e.g. RegEx). Good “ “mixture, but yes, there has not been much (if any) time to have a look at the  course materials this week.” |

**Did you find the final exam reflected the course well?**

|  |
| --- |
| “I strongly believe that all the aspect discused at the course were covered!” |
| “Yes it did. Questions were about main issues of every class.” |
| “Yes” |
| ‘”It reflected the course well in relation to the level of organisation. I hope the  results will show that people will not have remembered everything (due to  the majority of the material being covered so quickly) and had no material  available as revisions.” |
| “It reflected the course but suprisingly reffered to the material that was  covered briefly (ex. XSS)” |
| “Yes” |
| “ I think that yes.” |
| “yes” |
| “No, because this was, lika I sayd not technical examp, and English (language)  examp.” |
| “Pretty much. “ |
| “Yes. It aims to be given extra effort of the participians” |
| “yes” |
| “Yes” |
| “Yes it reflects, but nobody should have to know ports of a software or things  like that.” |
| “yes” |
| “Yes I think so, because all (or almost all) topics that were discussed during the week  were also part of the test.” |

**Are there any comments that you would like to make regarding any feature of this course?**

|  |
| --- |
| “This kind of course should be done more often, because only in that we, we,  as law enforcement, can perform ourselfs. I this way, we can deal better with  the new cybercrime attack, which are more and more often!” |
| “I have nothing to complain. I know you didn't have a time to prepare the  computers while last weekend and that's why we had some problems with  time. Instructors were good and I liked the way they teach. Overall I am very pleased I had  a change to be here. This is not just a learning the new things it's also to make  new contacts.”  “You did a good job !!!” |
| “it was a good over course especially when considering that still is a pilot  course in certa my personal idea regards some small imporvements would be  better planning in terms of time and equipment....regards time try to do the  most relvent aspect and not compress everything its quailty Vs quatity  personal i prefer quailty then a brief describtion about nearly everything....  in terms of equipment i suggest a basic common english OS would have help  after all its not touch typing course... Finally i must admit during this  weekthere were instances where i ended up pondering whether the course  iam doing was Malware Investiation or Network some clear border should be  made...... Finally a small add on to this course would be a small presentation about future trends. what Police officer would meet in the near by future. it would give that extra cherry on the cake for the course could fit quite easily as smooth ending too” |
| “The course in the future needs to be more structured. As a student I felt that  lessons were happening far too quickly with too many "technical dificulties".  With presentations rushed to fit to a timescale that was falling behind  Everyday” “Some subjects we spent far too long covering compared with others that were more  appropriate to the course name being cut short.” “Machines not working in general, having to set up virtual machines or  download them wasting more time, rather than being pre-set up on the  machines ready to be used.” “Material should have been given to us prior to the final exam that would  have enabled us all to revise to a level that the exam was set.” “In summary the venue was good, although at times it was very warm which  made it at times dificult to concentrate.” “The teachers were all friendly and approachable towards the end of the week  they had bonded with the class. At the start of the week, the majority of the  teachers failed to introduce themselves and give a background to them, they  were just a face. As I have said as the week progressed this did change.” |
| “About the course: In compare to other courses organized by BKA, I felt the lack of: 1. Schedule - I think students could get a leflet with all the subjects for each  day, when the course starts, etc. It would also help in evaluating each day  because after whole day I cant even state what the subjects where.  2. Timing - No time for practicals, so It is also hard to raise the discussion  because you know that it will slow down everything, leaving everybody even less time.  3. Using French browser with German OS set to english regional settings and German  keyboard is sometimes challanging and causes software issues. :)   4. Lack of AC makes your brain melt :)”  “Thank you for all your efforts to get the things running and going, it was really a fruitfull  week. “ |
|  |
| “Just a little bit too much info's in a little time. “ |
|  |
| “With this incredable organisation, if teachers put in material more practical  details, and on tests they try to guide the students, not to confuse them - this  will be the best course that I see. Organisation was the best, themes to, but ...  we must learn, not to guest ... |
| The course was too short for the amount the information provided.” |
| “There should be more step by step examples “ |
| “it is so hard course.” “there are alotof diffirent topics” “we need to practice at home” |
| “Sometimes a bit unstructured. I really miss a agenda/schedule so I know what  sessions were called. Overall, each instructor did a really good work and had interesting  presentations.” “Ljuban=l33t!” |
| “There should be a repetition of the day before. To keep the important themes  in mind.” |
| “the staff was zealous” “the course was partially unstructured” “disgusting restrooms” |
| “Overall, this was a good course with really motivated and compentent  trainers. And I know that there is a lot of preparative work necessary,  regarding both content and organization, to set up such a course.  So thank you very much for your engagement.”  “I still think, that less basics should be covered in this intermediate(!) course,  especially regarding the first two days (e.g. linux and RegEx basics). The  course should be more focused on real log analysis, what to find in the logs,  real network traffic analysis, what to find in there. Not only teach what files to  look for or how to sniff a networt, but go into far more deep into the details  that are interesting and important for us as investigators: what to look for in” |

**SSD Forensics**

**Survey One – Post-Preparation Meeting Trainer Evaluation**

**Are there any issues, positive or negative, that you would like to share with us regarding this week’s preparation meeting?**

|  |
| --- |
| “time between preparation meeting and actual course is too long. it would be  better to have another meeting inbetween. it was a great idea to meet in the  castle, so we all gotta stick together and nobody disappeared in his room.” |
| “Working in the group facility we got more work done than in a hotel, so  accommodation was very good.” |

**Survey Two – Student Course Evaluation (by day)**

**Day 1**

**Are there any comments you would like to make regarding Day 1?**

“Please provide slides along with the presentation…it is a better way to follow the course and make notes (rather additional notes than writing down what’s on the slides)”

“It is a hard thing to remember all the offset positions. It would be much easier to follow with a scheme of it”

“Talking about FAT/NTFS structures, MBR, MFT, offsets etc. without the paper is a little useless, there are too many things to remember and write down. It should be at least an electronic version (i.e. doc file) that contains all offsets, names, identifiers. Without it, it will be a painful review”.

“I need an handout”

“Day 1 was a good repetition of material that has been covered in previous ECTEG courses. As this is an advanced course, I think a lot of previous knowledge should be expected from the participants. Still I think it is needed to get everyone up to speed by having the first day as a reminder”

“The FAT and NTFS par tis very complex to having a look in 8 hours course. I think we will spent more time in that subjects or maybe people come to course refreshing their knowledge”

“I have very positive comments on the tutor’s preparation of the subject. Although it was a fairly complex subject the tutors delivered the lectures very professionally”

“I think it’s necessary a handbook or some papers with the information we must study”

I’d like to get the material about ntfs and fat and numbering”

“A little bit more hands on. I know the FAT/NTFS parts are really theoretical stuff but try to build some more hands on, or maybe a little bit more breaks.

“It was a very good idea to cover partitioning and NTFS as enhanced learning as to what I had forgotten since previous courses. Access to pdf material would have been beneficial to take way for revision”  
“Day 1 session could have a prerequisite to save time for media repair sessions”

“I would like to get material beforehand so that I could concentrate more on what the teacher is saying and less on taking notes. Also maybe Day 1 is just a bit too little for FAT, NTFS and numbering systems”

“I hae taken par tin numbering sessions that were explained in clearer way but this was a small problem”  
“Day 1 was another repeat of basics. Maybe it should be a prerequisite in order to get into the subject (SSD/Flash) as soon as possible”

“If possible the native English speaking lecturer might try and loose a little bit of the accent. I know it’s very hard but sometimes it’s hard for the student to follow”

“There should be more time for NTFSA and FAT sessions, especially for NTFS”

**Day Two**

**Are there any comments you would like to make regarding Day 2?**

“Maybe a little too confusing about interleaving. Maybe explain all the controller functions before data recovery. It was on the middle of paper reviews, and forensics issues”

“A very nice day and materials”

“A little complex but that is only due to my own lack of knowledge. Instructors very knowledgeable in this area. Very interesting and practicals were good to illustrate the diversity of SSD”

“There should be more extended tests to compare the results and maybe some kind of more precise monitoring software which will generate stats for each action”

“For people that never worked with SSDs it was a lot of input (e.g. all new vocabulary and techniques) but I think tis will settle as the next days a lot of vocabulary gets repeated and knowledge gets deepened”

“The lectures were easier to follow with the material that was provided”

“Very good day but the subject was a little complicated”

“Very good day! Really useful with the post-its. Visualization helps a lot”

**Day Three**

**Are there any comments you would like to make regarding Day 3?**

“manipulating PC3K would help to understand but it’s expensive…Maybe more example of rebuilding dumps (from simple ones to more complicated) could have improve comprehension”

“I think it is important to actually show students the advantages of the chip-off/pc 3000 method e.g. show the logical files on a thumbdrive using just EnCase and then reading out the chip including the data from the write amplification, the data that has not been trimmed yet, etc. Because it seems to me now that the students are kind of scared because of the complex work and they cannot really see the advantages on the other hand side”

“After lunch we had a practical session but it was very tiring to follow a demonstration of PC3K. It would have been better for us students to have more hands on. I think that when it is a practical session we do more than just 1 or 2 exercises. Overall, it was ok but it was a stressful thing for a whole day listening to non native speaking lectures (which are very good) but for us students it was hard cause sometimes we had to do double translation to understand”

“This part of the course is more complex than the others. So I mean that it could be interesting to spend more time, and obtain more documents about this part”

“Very interesting and quite complex in particular the work on PC 3000. Well presented showing excellent trainer knowledge”

“Interesting day. Focus on Flash media and PC3K could have been done earlier and extended. Otherwise it might be necessary to call the module ‘Flash Media Repair – Basic’. More practice and rebuilding could be suitable”

“Please provide presentation before the actual lesson to make it easier to take notes or follow the course. Is there a w ay to provide each student with hands on the used software (PC3000)? Just watching is good but doing it is better”

“I think it was a little difficult to learn in a 8 hours class”

“Paper powerpoint was again very good to understand. Next time use a beamer with a higher resolution or put 2 beamers (split screen). It’s not easy to understand PC3000 if you can’t do it on your own even how good the teacher is. Some things you have to do on your own”

**Day Four**

**Are there any comments you would like to make regarding Day 4?**

“it would be nice to see desoldering and reassembly of a SASD drive. And it would also be important to actually see the contents of invalid flagged pages and see the positive impact of write amplification for forensics. So until now we have seen how chip off can help us with damaged media but we could not see the benefits of having maybe more data on an SSD due to write amplification just by using chip off”

“It will be a great thing to see a whole process working: take apart a USB stick, chip off, read chip, and recover data from it”

“Good choice to let students do hands on on a chip off. Since it is an SSD course I would have expected to have some chip off of SSD as well. Overall, half a day of Filesystems should be enough…rather spend more time on the reading of flash memory chips and the different things to to until you can reconstruct a filesystem”

“Excellent idea in showing live practicals in chip off and PC 3000 to demonstrate theory”

“Overall, it was one of the best days. The only dent in the day is the exam and that not enough time to desoldering the chips cause only 1 equipment and sometimes the chips took a lot of time”

“Could have been possible to ask for participants to bring their own PC3K to have more hands on”

“A very good practical day”

“The ‘hands on’ part was really great! It’s better to learn through practice instead of theory but theory is a must after all”

**Survey Two - Student Course Evaluation (overall)**

**Which session did you feel was the most successful? Why?**

“121205\_8.2 looking at the SA (LR)\_2”

“PC3K”

“SSD Practical”

“SSD Forensics Issues”

“SSD GC and TRIM”

“How intereter the memorys and theory about SSD, as well as refreshing about partitions”

“Practical sessions”

“SSD and NAND Theory. It’s actually interesting”

“The hands-on for th soldiering”

“SSD Forensic Issues – it’s a new topic”

“Practical Lesson for chip-off”

“SSD Techniques and Forensic, Understanding memory image. Looking at the SA and Techniques and Forensic Issues. I think so because it is very important to know how something is working, then how it stores data and just then how to read the data”~

“The session explaining how data sent by the OS is being transformed by the controller before it is placed on the memory chips. It gave a good understanding of what takes place, and how and why we need to do the steps in reverse to decode an image”

“SSD Techniques and Forensic Issues. Provided the framework for all subsequent sessions”

“Read & Write process of Flash Memory, structure of flash memory, reconstrucing filesystem”

“Practical dump rebuilding”

“the session on how SSD and Flash store the data cause this was a subject totally new to me”

“Practical Flash Media Storage Repair”

“PC 3000. I had never seen that. Also the part when they say that you can’t carve on a SSD when TRIM is on.”

**Which session did you feel was the least successful? Why?**

“121202\_numbering\_systems\_121031(LR)\_Ready”

“Many people had problems with file systems”

“The first PC3000 test”

“Partitions and File Systems. It’s not necessary to keep in mind all those bits and pieces. It’s enough to have a paper in front of the eyes with all the bits decoded. In my opinion, the first day session was a waste of time. All we need to know from first day - that we need to search for some patterns in the physical dump – FAT NTFS FILE.”

“Numbers and partitions. I prefer more theory about SSD and NAND”

“There should have been possibilities shown to actually find deleted data from write amplification which we could not have found with our regular techniques”

“NTFS understanding”

“May be the sessions about FAT and NTFS because there was not enough time to learn everything and to get the idea of how it works”

“NTFS theory was delivered in a ‘dry’ manner by the teacher, without much hands on work for the students. Especially compared to the earlier session where we tested and saw for ourselves what happens to a disk when you partition it and format it”

“Demo of PC3000, because it is unlikely that I will get to use this software”

“Filesystem – too long, basic stuff/only half a day is more than enough time on that matter…since you do not refer to it as much later in the course as expected”

“Filesystems explanation (another repeat of basics)”

“PK3000 not for not being boring or not interesting, but it would have been much more interesting with some hands on by the students”

“First day sessions (not really used afterwards except maybe MBR”

“FAT/NTFS…basic stuff that everybody MUST know, before going to a course like this”

Can you think of any subjects that could have been addressed in the course which were not covered?

“More information about the content of the SA”

“Refreshing about recovering HDD”

“Desoldering and reconstruction of SSD drives additionally to usb/sd cards”

“more practical lessons with PC3000”

“How does the full disk encryption works with SSD”

“chip-off SSD, kind of a practice guide on when chip off will bring which additional data, more in-depth on trim”

“I expected a higher level of lessons. SSD part concerned only TRIM command. I expected more practice, more example about SSDs recovery”

“Practical exercises. Actually few manipulates the media repair. Could have been lots of exercises with participants or ACE licenses”

“Game console. Also a chip from a SSD with TRIM on”

**Are there any other comments that you would like to make regarding any feature of this course?**

“Prepare papers and documentation for the students and will be fine”

“I think all trainers know the topic very well and had a very good way of presenting a difficult topic…I would have preferred however if the course material was provided beforehand, although I do understand this was a pilot course and material may not have been conclusive”

“Thanks for useful trainings”

“The trainers did a really great job!”

“The course was really great. I’ve learnt a lot of things which will be useful in my work”

“Perhaps don’t advertise it as an SSD forensics course. It is in fact a more general flash memory course, which is fine, but then let’s call it what it is”

“Enjoyable course thanks”

“Issues like ppt, screen resolution, timing should be cleared beforehand. Gaming consoles are of much interest...unfortunately that part didn’t take place

“As this course is intermediate, maybe skip basics and focus on flash recovery through PC3K (students could bring their own). Or use tools such as pda.jar to emulate PC3K so everyone can think on the dumps. Anyway the course was interesting because trainers are well qualified. So I could learn sometimes more at coffee breaks”

“They will help me cause now I have a better understanding of SSDs but it will be very difficult to implement these techniques> Reasons vary from job related issues up to financial problems up to legal. To spend 3000 Euro on a software that is not 100% guarantee to yield results, it will be very difficult to obtain the funding. Legaly, we can not ‘destroy’ evidence to obtain information if we can not guarantee that we will have positive results”

“The course was very interesting but was sometimes maybe too much a show. Practical examples were not covered enough whereas some points were too covered (TRIM, filesystems, etc). Maybe an online pretraining material could be issued to avoid wasting some precious time”

“International courses are always very god, because you will hear things and issues from other countries, that will help you during your daily work”

**Survey Three – Post-Course Trainer Evaluation**

“outdated notebooks. The projector quite bad, not bright enough and there should have been a second one”

“MS Office 2010 was missing”

“The assessment was too easy to test the knowledge – if we’d provided a harder one, 30-40% of them would have failed”

“It was open book exam”

“but not all. 5 students weren’t experienced enough”

“some 5 people had little knowledge”

“only 2-4 students had bigger problems in understanding and talking”

“some people had problems (at least 3-5)”

“leaving on Friday morning is a bad idea, if the course should take 5 days. Last day is totally lost for lessons”

“more software dongles, better projector or one laptop per table with teamviewer to show what trainer is doing at his laptop”

“more practical lessons”

“But maybe it is better to have two (maybe shorter) meetings for preparations. One should definitely be in the near of the site for the course”

“Friday was lost due to early travels. The notebooks of the participants had to be prepared for transport on Thursday, so on Friday no lessons possible”

“some material was cut out”

“less flies would have been nice”

Did you feel that sufficient support was made available to trainers from the Management Team?