1

Digital Forensics Laboratories in Operation: How Are Multimedia Data and Devices Handled?

Shujun Li and Anthony T.S. Ho
Department of Computing and Surrey Centre for Cyber Security (SCCS), University of Surrey, Guildford, UK

1.1 Introduction

This chapter looks at the operational side of digital forensics of multimedia data and devices in real-world digital forensics laboratories, especially those run by law enforcement, in order to prepare readers with a proper background for different technical aspects covered in other chapters of this book. The chapter can also be read alone to gain insights about the operational aspect of digital forensic services and practices on multimedia data and devices.

While most digital forensics laboratories handle multimedia data and devices in their everyday operation, the forensic procedures, techniques and tools used often differ from each other due to many factors such as different legislations regulating forensic practices, different digital forensic standards and best practices followed, different structures of the digital forensics laboratories and their parent bodies, etc. We realized that it is difficult to cover too many digital forensics laboratories in different countries in such a short book chapter, so we decide to focus on the following three representative laboratories (two in the United Kingdom and one in China):
Handbook of Digital Forensics of Multimedia Data and Devices

- Digital and Electronics Forensic Service (DEFS), Metropolitan Police Service (known as “the Met” or “the Met Police”, the largest territorial police force in the United Kingdom responsible for policing Greater London excluding the City of London Police area),
- Digital Forensics Team (including an affiliated Audio-Video Team, AV Team), Surrey Police (a medium-sized territorial police force responsible for policing the county of Surrey in the United Kingdom),
- Shanghai Stars Digital Forensic Center (SSDFC), Third Research Institute, Ministry of Public Security, China.

Among the three digital forensics laboratories listed, the Met’s DEFS is the largest one with around 70 technical staff members. The other two are smaller in size but still have a considerably large team (with 14 and 32 technical staff members, respectively). Covering digital forensics laboratories of different sizes highlights how forensic practices of large and smaller law enforcement agencies differ from each other. The third digital forensics laboratory in the list is not an in-house team of a police force, but part of a research institute of the central police authority (Ministry of Public Security) in China. It was selected to cover a different type of digital forensic service providers and also digital forensic practices in a major legislation significantly different from the UK system and the Western systems as a whole. We have not opted to cover any private sector digital forensic service providers because the quality and scope of their services are much more diverse and may not be directly comparable with those provided by law enforcement bodies.

The rest of this chapter is organized as follows. Section 1.2 describes how multimedia data and devices are handled at the Met’s DEFS, with a particular focus on the DEFS’s AV Laboratory (AV Lab) which is the main forensic laboratory handling multimedia data and devices. Sections 1.3 and 1.4 describe different aspects of digital forensic practices on multimedia data and devices at the Digital Forensics Team (including the affiliated AV Team) of Surrey Police (UK) and at the Shanghai Stars Digital Forensic Center (China), respectively. After describing the three digital forensics laboratories, Section 1.5 compares digital forensic practices of the three laboratories to show common features and major differences, which lead to some key observations for future research and possible extension of this chapter. The last section briefly summarizes this chapter. An appendix is given to cover the questions that we asked during our interviews with Surrey Police and the Shanghai Stars Digital Forensic Center in China.

1.2 Digital and Electronics Forensic Service, Metropolitan Police Service, UK

The information about the Digital and Electronics Forensic Service (DEFS) of the Metropolitan Police Service was obtained through a written document provided by staff members of the DEFS. The document was not guided by the authors of the
chapter, but is more a systematic summary from DEFS staff’s point of view on different aspects of their digital forensic practices with a special focus on multimedia data and devices. Further e-mail communications took place after the authors received the written document to clarify unclear issues. The published content of this section was reviewed by the informants.

1.2.1 Background: Metropolitan Police Service

The Metropolitan Police Service (“the Met” hereinafter) is the largest police force in the United Kingdom with around 31,000 police officers, 13,000 police staff, 2,600 Police Community Support Officers (PCSOs) and 5,100 special constables (volunteer police officers) as of May 2014 (Metropolitan Police Service 2014a). It was established in 1829 after the first Metropolitan Police Act was passed (UK Parliament 1829). It is responsible for law enforcement in Greater London (excluding the small region called ‘City of London’ which is the responsibility of the City of London Police), covering a population of 7.2 million (Metropolitan Police Service 2014a). According to the statistics published on its website (Metropolitan Police Service 2014b), there were in total 771,566 notifiable offences in 2012–2013 fiscal year.

1.2.2 Digital and Electronics Forensic Service

The DEFS hereinafter provides the Met with in-house facilities and outsourced services to examine today’s high-tech electronic data and devices. It provides a comprehensive range of services at one location, in its AV, computer, and telephone laboratories. Each of the three laboratories has around 20 members of technical staff. There is also a smaller laboratory for cell site analysis, which has five members of staff. In 2013 the DEFS handled 2,780 cases, leading to an average work load of 3–4 cases per technical staff member per month.

The forensic services provided by the DEFS are guided mainly by in-house standards, the standard operating procedures laid out by the Met and the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence (2011). All laboratories of the DEFS are also actively working towards ISO/IEC 17025 (ISO/IEC 2005) accreditation as required by the UK Forensic Science Regulator in its 2011 ‘Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System’. A more detailed and systematic description on the ACPO guide and other standards and best practice guides can be found in Chapter 2.

Multimedia related forensic services in DEFS are mainly conducted by its AV laboratory (‘AV Lab’ hereinafter), so in the following we will focus on the AV Lab only. Note that some descriptions on the AV Lab also apply to the other three

---

¹ Previous editions of the ACPO guide are titled ‘ACPO Good Practice Guide for Computer-Based Electronic Evidence’. 
laboratories, for example the training and performance evaluation practices and the working environment.

1.2.3 AV Lab: Operational and Procedural Aspects

The AV Lab of the Met’s DEFS is one of the best equipped digital forensics laboratories in the world in terms of both the range and specification of its enhancement tools, and the expertise and experience of its staff. The team is made up of forensic audio and forensic video practitioners, forensic technicians and a number of specialists in areas such as image comparison, CCTV data recovery, audio authenticity and voice comparison.

The AV Lab works with customers across the Met to retrieve, process and analyze all types of audio and video evidence. For complex cases with a lot of digital evidence, the Met’s FOCUS Court Presentation System (Thomas 2010) is sometimes used to assure the maximum impact and accuracy of electronic forensic evidence within the courtroom.

An approved lab form is required for all submissions and the following services are currently available:

• Audio Services
  – Copying – format conversion and decryption, optimal replay
  – Audio enhancement – improving intelligibility and listening comfort
  – Editing – removing redacted passages for disclosure/court, for example ABE interviews
  – Processing – for example voice disguise, level optimization, speed correction and section compilations
  – Audio authenticity analysis – identifying whether a recording has been copied, edited, tampered with or deleted; assessing the provenance of a recording
  – Identification of the time and date of an audio recording through electric network frequency (ENF) analysis
  – Acoustic crime scene evaluation – could person A have heard event B from location C?
  – Voice comparison
  – Repair of broken media

• Video Services
  – Assistance with viewing CCTV/video footage
  – Decoding and conversion of CCTV/video images from either analogue or digital CCTV recorders for court purposes
  – Downloading CCTV from CCTV recorders (DVRs)
  – Court compilations of CCTV/video material
  – Data recovery from corrupted CCTV recordings
  – Production of still images
  – Image comparison
Digital Forensics Laboratories in Operation

- Image enhancement
- Height estimation from images
- Speed estimation of vehicles from CCTV
- Linking an image to a source camera (PRNU analysis)
- Bespoke CCTV playback solutions

In the following, we will look at different operational/procedural aspects of digital forensic practices of the AV Lab.

1.2.3.1 Job Description

Depending on the entry grade, all employees of the AV Lab hold a minimum BTEC² Diploma in Electronic Engineering, but some roles require a degree and/or significant relevant experience. Insistence on electronic/technical engineering qualifications underpins the ability to give evidence in court about the ‘how’s and why’s’ of audio and video recordings. Understanding the fundamental causes of noise, intelligibility degradations and recording-chain impulse response, along with other audio and video engineering issues, enables the specialist to competently explain to a jury what has occurred and the limitations of what can be done to address those problems.

The role requires a broad knowledge of, and interest in, all modern communications and computing technologies with an emphasis on the forensic opportunities offered by their examination. Excellent communication skills and the ability to convey ideas and technical knowledge to police officers and colleagues of all ranks are essential, together with a strong technical understanding of the fundamental principles behind digital devices and the way in which they interoperate with each other and other systems. Staff work on a call out rota, attend crime scenes and give evidence in court.

1.2.3.2 Training

The AV Lab organizes its training program by defining a core skill sets for all lab roles and each staff member’s current status for that knowledge or skill is assessed. This gives both in-house and external training focus for the individual. Elements include externally run foundation courses, internal training with specific software packages such as Avid (formerly known as Digidesign) Pro Tools (Avid Technology, Inc. 2014b), Apple Final Cut Pro (Apple Inc. 2014), and then detail training on the modules within them such as compression/level control, spectral subtraction, etc.

The AV Lab also has internally run courses on more general forensics-related matters such as statement writing, court skills, etc. Internal training is achieved by a mix of group training (e.g. court skills), formal one-to-one training sessions on a particular

---

² BTEC refers to UK’s Business and Technology Education Council, the British body existing between 1984 and 1996, which awarded the vocational qualifications commonly referred to as ‘BTECs’. In 1996, BTEC was merged with the University of London Examination and Assessment Council (ULEAC) to form a new awarding organization Edexcel (Pearson Education Limited) (Edexcel 2014).
topic (e.g. compression) and on-the-job training or specialist shadowing. The new entrant will undergo a full range of teaching from peers and will be carefully shadowed on their early work. The AV Lab fosters a culture of peer review, checking, comparison of techniques and discussion. Even the most experienced specialists will often ask for a second opinion or ideas for alternative approaches. This is never seen as a sign of incompetence but rather aids the dissemination of good practice and innovation.

The Met operates a Performance Development Review system for staff appraisal and development. This is designed to give 6 monthly reviews of an individual’s training requirements, based on performance and his/her future work profile. Objectives are set and reported on for each 6-month period and are based on the needs of the department (e.g. ‘procure and set up a data recovery PC will all relevant tools installed, by March’) and those of the individual (e.g. ‘complete the Met’s diversity strategy training module by December’). Staff’s performance is assessed in a wide range of behaviours, based on the UK’s National Occupational Standards (NOS) (UK Commission for Employment and Skills 2014). Their salaries are however not performance related.

Some equipment vendors and manufacturers run training courses specifically on how to use their products. To date the AV Lab has made little use of these courses as they have emerged relatively recently and staff turnover has been low for many years. However, the AV Lab is not opposed to courses like these as long as they cover the fundamental theory behind the controls being manipulated.

1.2.3.3 Working Environment

It is vital that the working environment is free of any electromagnetic interference especially mobile phone (GSM) interference. A recommended safe distance for mobile phone activity is 10 m. Because the handset handshakes at full power at turn on and turn off, all visitors are expected to turn off their mobile phones or activate ‘flight’ mode before they enter the examination area, and if they are already near the examination area then they will be requested to leave before they change the mode of their phones.

1.2.3.4 Copy Quantities and Formats

When an exhibit is booked in, the officer is informed that he/she will receive back three discs in the format of Compact Disc Digital Audio (CD-DA) (International Electrotechnical Commission 1999) and/or DVD-Video (DVD FLLC 2014) where appropriate. Any agreed variations to this will be noted at the booking. Three enhanced, evidential copies will be produced. One will be a sealed copy and two will be unsealed. If there are a large number of exhibits to be copied or very long running times, then it will also be considered to produce WAV-type files and issue DVD data discs or a hard drive. Included on the copy is a READ-ME document detailing any instructions, copy format types and possible issues.
It is sometimes the case that even following an enhancement the quality of the copied recordings remains poor. In this instance, an unfiltered ‘flat’ copy of the exhibit is produced in addition to the filtered versions and labelled as ‘un-enhanced’.

The exhibit reference numbers assigned to copies are usually in the form of the initials of the forensic audio/video engineer producing the copies, plus an incrementing number that relates to discrete sets of originals, followed by the copy format and then the copy serial number. Each copy reference number should be unique for all submitted recordings relating to a particular operation.

1.2.3.5 Triage

The Police Forensic Liaison Unit (PFLU) acts as a gate keeper for the DEFS service. This PFLU assesses each application for submission before any exhibits arrive in order to winnow out any submissions which are not clearly focused on a specific question, which would cost a disproportionate amount of time to process or which can be reduced or even eliminated in scope through alternative methods of analysis or investigation.

For instance, a mobile phone and a laptop computer may be submitted in order to prove the association between two suspects. If the two suspects are found to be linked through mobile phone contact and text records, there is no need to submit the laptop. For audio it might be that an enhancement is requested to aid transcription of a surveillance probe, but an undercover officer may provide a much better quality version of the same conversation.

One major area of work which requires robust insistence on perfectly completed submission documents is the authorized editing of significant witness interview recordings. Known as ABE (Achieving Best Evidence) interviews (UK Ministry of Justice 2011), these video interviews often require editing to remove references to specific names, addresses and other identifying information. The discussions and negotiations between prosecuting and defence counsel over what will and will not be removed are usually held immediately prior to, or indeed in the middle of, a court hearing. This means that the laboratory is regularly expected to perform edits at very short notice or within tight (and sometimes impossible) timescales, which needs to be carefully handled in the triage process. The ignorance about the time taken for the technical process of capturing, editing and producing these edited versions can lead to frustrations and conflicts so the laboratory has to ensure that its workflow is as efficient as it can be, particularly in this key area.

1.2.3.6 Exhibit Security

Due to the need to protect electronic evidence from being damaged or unintentionally changed, it is crucial for forensic analysts to pay special attention to exhibit security. In the AV Lab, it is required that DVDs and CDs must be played using read-only DVD or CD ROM drives. Writable media such as compact flash cards, hard disks or USB memory sticks must be write protected using a hardware write blocker. In
circumstances where hardware write blocking cannot be used, then software write blocking should be utilized. Details of the write blocking procedure should be recorded in the analyst’s examination notes. In most cases it is not a requirement before an examination to create a forensic copy or duplicate of any source material using a specialized digital forensics software package such as FTK (AccessData Group, Inc. 2014a) or EnCase (Guidance Software, Inc. 2014a), although this may not apply to some types of solid-state storage media.

1.2.3.7 Contemporaneous Notes
In the AV Lab, it is required that all forensic engineers should keep notes of important information about any case such as records of movements and storage of exhibits, instructions from phone calls and emails, etc. The contemporaneous notes should be signed and dated by the engineer conducting the corresponding forensic examination.

Working notes should be made on an examination form with a record of the continuity of the processes and procedures used and include screen shots showing all relevant settings for computer-based signal processing algorithms and where appropriate software versions of plug-in, etc. In addition, the signal chain should be recorded through the whole signal path.

The notes should also include a brief understanding of the instructions and who supplied them from the submission documents so that both the objective(s) and the origin of the forensic work are clear.

1.2.3.8 Evidential Evaluation
Throughout the period working with exhibits, an evidential evaluation of the contents of the recording takes place. The purpose of this evaluation is to inform the investigating police officers of any anomalies found on the recordings and to be in a position to give advice relating to the evidential credibility of the material and offer potential solutions to its shortcomings. Any negative issues arising from the assessment of the submitted evidence regarding evidential quality or authenticity are fed back to the officer in the case (OIC) and technical program unit (TPU).

1.2.3.9 Authentication
The authentication process seeks to establish if a recording is an original and genuine record of the event(s) that took place. This normally means it should be a continuous recording, and should not have been altered or tampered with (i.e. that no information had been added, modified or deleted). This can be approached from a physical level if it is disc/tape based, wrapper level, that is header/file structure and signal level. Ultimately, detection of deliberate tampering may not be possible, however detecting a purported ‘original’ recording is actually some form of copy casts significant doubt on its evidential integrity.
To undertake the procedure one would normally need access to both the original recording and the original recording machine and any equipment used. In addition, a statement from the individual producing the recording should be provided and the statement should cover the equipment used, its means of deployment, and also establish the recording’s evidential chain of continuity.

The authentication process then proceeds in stages as follows:

- Examination and analysis of the original recording and test results.
- Examination and analysis of the original recorder and test results.
- Comparative analysis of the original and test results.
- Production of report and conclusion from the analysis findings.

To explain the aforementioned process more clearly, let us look at how authentication is done for audio recordings. Authenticity examination of digital audio material has been used in many cases and has been an ongoing research topic for the AV Lab since around 2000. Various software-based tools have been developed in house to assist with this task.

The initial phase of the examination subjects the recording to critical listening which seeks to establish agreement between the acoustic qualities of the recording and the alleged recording environment and equipment. Critical listening will also identify any key ‘events’ worthy of further analysis such as apparent discontinuities, inconsistencies in the background noise, or acoustic signatures which may indicate manipulation of the recording.

Following critical listening the whole recording and in particular the key events are subjected to waveform analysis which provides a visual display of the audio waveform by means of time/amplitude, frequency/amplitude and dynamic range graphs.

The next stage covers the production of test recordings on the alleged original recording apparatus, made under the same (if possible) or similar conditions and testing of all the various control functions of the recording apparatus. The resulting test recording is then subjected to the same waveform analysis as the original recording above so that a comparative analysis between the original recording results can take place.

Based on the results of the comparative analysis a set of conclusions are derived which aim to either establish the integrity and authenticity of the original recording or question its evidential reliability.

If the recording is in a digital format (e.g. a computer sound file), then further analysis of the digital data can often take place, and this would include consideration of the structure of the file and file header (metadata) present. Examination of the metadata may reveal the recording date/time and duration plus the model of recording used,

---

3 Video recordings can be handled in a similar way although the techniques and tools used will often differ.
similarly absence of the metadata may indicate the file has been produced by digital editing software.

The original recordings are needed because they can be edited with relative ease in digital format nowadays if one has access to a general purpose personal computer (PC) and readily available editing software (many of which are freely available in the public domain).

Even a purportedly original analogue recording may have been copied to a computer, edited or manipulated then recopied back to an analogue recorder. Because of the high quality of many computer systems when dealing with sound material analogue recordings can be presented as the original with in many cases little degradation in quality.

Once material has been copied some of the key audio features of the original can be lost making establishment of its authenticity much harder. This can also be true with regard to the metadata embedded in a digital audio file which could be manipulated by an individual with sufficient knowledge making changes difficult to detect.

The aforementioned authentication process does have limitations. If the original recording is not available to analyze and there is no access to the original recording device (or any knowledge relating to its make, model and means of deployment), one cannot exclude the possibility that the recording has been altered. Examination of a copy of the original recording can be compared to looking at a facsimile of the evidence making it difficult to establish if it is an authentic reproduction of the sound heard, whereas access to the original may tell us a lot more about the evidence gathered.

Where events noted appear to challenge the authenticity of the material, the access to the original recording and an explanation of how it was used to make the recording may help settle questions regarding its integrity. For instance, if there are signal dropouts and noise present on the recording this may be explained by use of a radio link in the signal chain, however if the original equipment only included a cable-connected microphone then another explanation for these artefacts must be sought to ‘prove’ the recording.

1.2.3.10 Audio Enhancement and Processing

Prior to any enhancement/processing taking place, an auditory assessment coupled with FFT (Fast Fourier Transform) analysis of the recording will be undertaken wherever possible. From this evaluation an enhancement strategy will be decided upon. The primary aim of enhancement is to improve the intelligibility of speech or to make the quality of speech more acceptable to the listener.

Degradation can be caused by a number of effects including acoustic noise from background speech, reverberation caused by multiple reflections from a hard surface environment (e.g. in a corridor), electrical interference (e.g. GSM tone injection from a mobile phone), clipping where non-linear distortion is added to the signal through over-driving the signal path, distortion effect from the recording apparatus (i.e. poor quality microphone or over compression by the codec).
The AV Lab is a co-sponsor of the Centre for Law Enforcement Audio Research (CLEAR 2012), a UK Home Office-led 5-year research program which seeks to better understand the effects of filtering on speech intelligibility, transcribers’ performance and developing state-of-the-art algorithms for speech cleaning. The motivation for this sponsorship is to better understand the limitations and opportunities in forensic grade speech enhancement and thus optimize filtering processes and workflows to achieve the ultimate goal of gaining better evidence/intelligence from recordings. Audio filtering has been undertaken for many years by the AV Lab and other forensic labs with the assumption that a corresponding increase in intelligibility must have been attained if a filter setup makes the recording sound ‘better’ to the listener. The AV Lab is questioning this assumption, and working with the other CLEAR consortium members and the academic team to better understand the effects of filtering techniques on intelligibility. The idea is to put enhancement on a more scientific footing—to know more about what the AV Lab is doing with corrupted audio and to avoid unseen pitfalls.

At the heart of the problem is assessment of the enhanced product: how do we know or how do we show that our processes have not degraded the intelligibility of the original signal. Just because we may have applied recognized processes in terms of equipment, techniques and procedures do not guarantee that the ‘wanted’ signal has not been damaged in some way. Intelligibility is assessed on a subjective basis, so without knowing what the original signal should be the results will depend on who is to say one enhancement is better than another.

Less is often more in terms of successful enhancements. If we have a recording that has poor bandwidth and a very low signal-to-noise ratio (SNR), then a speech signal could be so fragile that any form of processing is likely to degrade it further and may be best left in its original form.

1.2.3.11 Video Submissions

Viewing of video material serves as a preliminary assessment of the video exhibits, which may lead to a submission for more complex work such as editing, image comparison, enhancement or data recovery. Common outcomes of viewings include capturing and printing still images, creation of edit lists for court copies and creation of working copies.

Details present in footage can sometimes be enhanced to reveal more information. The capabilities for enhancing video are often very limited, particularly if the original footage is of low quality. Enhancement can range from simply cropping and zooming in on an image, adjusting brightness and contrast or more complex processes such as frame averaging in static components of an image.

If video footage cannot be accessed by conventional means, or has potentially been removed from a device, the officer can submit the exhibit for data recovery. Data recovery is diverse and can include recovering data from damaged media, extracting deleted files, rebuilding corrupt files, reverse engineering video formats and
CCTV systems for playback of footage and extracting time and date information from proprietary file systems. Processes used in data recovery are often developed on an ad hoc, case-by-case basis, as new technology emerges.

1.2.3.12 Statements

Each statement must include the following phrase⁴:

Witness statement
(CJ Act 1967, s.9; MC Act 1980, ss.5A(3) (a) and 5B; MC Rules 1981, r.70)

The aforementioned title is followed by the following:

• The analysts name along with qualifications, occupation and experience
• Company name
• Evidential services lab reference and company lab reference (optional)
• Details of the exhibit including exhibit number and any bag seal numbers
• Brief description of work requested and work carried out
• Details of the copies produced
• Brief description of any enhancement process
• Details of resealing and storage
• Disclosure details, that is ‘A full record of work carried out in this case is available at [company name]. This record will include: documents created at the time of submission; trail documents and original notes of examination’.

1.2.3.13 Basic Quality Assurance Checks

Basic quality assurance checks are required to be performed prior to the case being returned and these include the following:

1. Check that the recorded/noted reference and exhibit numbers matches the submission documents and those referred to in the statement.
2. A peer review of statements must take place.
3. A cursory listen of the final copies to establish correct copied content.
4. A final review of the documentation to pick up any typos, etc.

1.2.4 Selected Forensic Techniques Used by AV Lab

In this section, we give brief descriptions of some selected forensic techniques currently used by the AV Lab staff. This is not a complete list of techniques they use, but a personal selection by the members of staff we got information from.

1.2.4.1 FOCUS Court Presentation System

FOCUS (Thomas 2010) is a bespoke software-based digital evidence viewer and organizer that stores all digital evidence relating to a case in a single place so it can be accessed via an easy-to-navigate front screen. This assists the investigating officer by helping speed up and streamline the presentation of evidence in court. It can be particularly useful in cases with a large quantity, range or complexity of evidence. By improving the quality of court replay systems, the presentation lab provides highly beneficial systems that assist a jury in understanding complex evidence. The system supports the presentation of all electronically held digital evidence, including video, audio, flash, documents, photographs, DVD, 3D immersive imagery, CAD, etc.

A range of presentation facilities are available, including the following:

- Annotated media, for example arrows on videos highlighting the areas of focus
- Interactive presentations, for example cell site analysis on an Adobe Flash platform
- Map animations – providing street data, geographic and bird’s eye views
- Court replay, management, storyboarding, presentation system facilities and more

The final presentation can be supplied for use in court on CD or DVD or on a hard drive-based system (FOCUS) which contains all evidence types and formats. Presentations of all electronic evidence can then be shown in a professional and easily accessible manner.

1.2.4.2 Electric Network Frequency Analysis

When audio or video is recorded, the mains electrical network frequency (ENF) is often recorded in addition to the wanted audio/video signal. This happens with mains-powered recording equipment but may also occur with battery-powered equipment if it is used in proximity to mains-powered equipment or transmission cables. ENF analysis can thus be used to both determine the date and time of audio/video recordings and to help establish their integrity.

The ENF in the United Kingdom is 50 Hz, but actually varies by small amounts from moment to moment due to variations in the demands placed on the network generators. The generators are synchronized across the network so these small frequency variations are exactly the same across the United Kingdom. Over time, these variations in ENF provide a unique pattern.

The AV Lab has been recording the ENF since 2002 and is able to compare ENF traces found on evidential audio recordings with the ENF database to accurately determine the time and date of recordings.

Comparison of an evidential ENF with the database may also be used in authenticity analysis to establish whether any discontinuities occur with a recording, or whether a recording is a copy.
This technique does have some limitations which include the following:

- ENF analysis only works on digital recordings and certain VHS recordings. Variations in tape speed on analogue recordings mean that the ENF signal is distorted and cannot be used.
- It is much simpler to compare the ENF with an approximate time and date at which the recording is believed to have been made, than to determine when the recording was made without giving any indication of the alleged time and date.
- Generally a recording should be at least two and preferably five minutes long to obtain a reliable ENF result.
- It is not always possible to extract an ENF signal from recordings either because it is not present or because there is too much noise.

The AV Lab co-authored a document for the Forensic Speech and Audio Analysis Working Group (FSAAWG) of the European Network of Forensic Science Institutes (ENFSI) for ENF analysis which was released in 2009.

The AV Lab have developed a set of practitioner competency tests for ENF analysis which should meet the requirements as laid down by the Forensic Regulator (ISO/IEC 17025), and participated in an ENFSI competency test for ENF analysis in 2009.

1.2.4.3 Image Source Identification

Recent research has shown that it is possible to identify the source camera of a digital image based on intrinsic noise patterns called Photo Response Non-Uniformity (PRNU) (Kot and Cao 2013). The AV Lab is actively researching on PRNU-based image source identification (Cooper 2013) and has developed its own source camera identification system. This system allows specific images to be tied to its source cameras (phones/compacts) and casework requiring this form of analysis is on the increase. The AV Lab passed two PRNU source camera identification competency tests run by the Netherlands Forensic Institute (NFI) for the ENFSI Digital Imaging Working Group (European Network of Forensic Science Institutes 2011) in 2010 and 2013.5

1.2.4.4 Challenges

There are a number of challenges identified by the AV Lab staff in the written document the authors received. They are not necessarily a complete list, but can show key areas the research community needs to pay more attention to.

The Met’s DEFS is still dealing with the legacy of the high cost per bit/low storage capacity of earlier generation of digital media where content was ‘thrown away’ in an

---

5 The PRNU source camera identification competency test was devised by Zeno Geradts of the NFI in 2009.
attempt to save space. The compression algorithms used are largely perception-based (i.e. lossy) and may not optimize the reproduction of forensic features.

Image enhancement potential for video material is still limited because of both the recording system and its configuration, for example time lapse capture. Quality of digital AV material is not optimized for forensic purposes such as vehicle identification number (VIN) identification, image comparison and analysis. For video and image compression schemes, lack of resolution, compression artefacts, fields captured instead of full frames and other issues all reduce the effective number of lines for forensic examiners to work with. Audio compression schemes are often optimized for music with a quality level of 16-bit 44 kHz but the actual sound precision can be much less for forensic purposes. On the other hand, there are exaggerated expectations from the general public regarding the precision and capability of digitally stored imagery and sound, so how to manage this is a (not only technical) challenge as well.

Another concern is about anti-forensics which is about manipulations of multimedia evidence by criminals to mislead investigations. There is a greater opportunity for criminals to do so at low cost on readily available equipment (i.e. Adobe Photoshop on digital still images). Access to knowledge to do it is more easily available across the internet. The DEFS and the whole digital forensics community need to continually update their techniques to meet this anti-forensics challenge.

1.2.5 Acknowledgements

The authors would like to thank the following informants from the Met’s DEFS: Paul Groninger (Manager of the AV Lab) and Robin P. How (Senior Manager of the DEFS). The authors would also like to thank Mark A. Stokes, the Head of DEFS, for his help in coordinating the communications between the authors and the DEFS staff for this section.

1.3 Digital Forensics Team (Including Affiliated AV Team), Surrey Police, UK

The information about the Digital Forensics Team (including an affiliated AV Team) of Surrey Police was gathered through a structured interview which took place on 5 July 2013. Some further email communications took place after the interview to get more information and to clarify some unclear issues raised during the interview. The published content of this section was reviewed by the informants.

1.3.1 Background: Surrey Police

Surrey Police is the territorial police force responsible for policing Surrey, one of the so-called ‘home counties’ surrounding London with a population of around 1.1 million (Surrey County Council 2012). The force’s headquarters is in Guildford, the same
town where the University of Surrey is located. Surrey Police originally started with the much smaller Surrey Constabulary (along side with a number of separate borough police forces) since 1851, and gradually evolved into the current county wide force in the 1940s (Surrey Police 2014b). Surrey Police had around 2 000 police officers, over 1 600 police staff, around 200 PCSOs and over 200 special constables as of September 2013 (UK Home Office 2014). Although Surrey Police is much smaller compared with the Metropolitan Police Service, it is a typical medium-sized territorial police force in the United Kingdom in terms of both its size and the population it covers.6 In 2013–2014 fiscal year, there were in total 48 486 notifiable offences (Surrey Police 2014a).

1.3.2 Structure of Surrey Police’s Digital Forensics Team and AV Team

As a smaller police force, Surrey Police does not have a large body for digital forensics like the Met’s DEFS. Instead, it has a medium-sized Digital Forensics Team (‘DF Team’ hereinafter) composed of mainly the following units (as of July 2013):

- A team leader supported by an administrative support officer
- Seven computer forensics analysts
- Five mobile phone forensics examiners

The mobile forensics examiners are assisted by 38 volunteers (detective constables and investigating officers from Guildford, Reigate, Staines police stations—the three largest police stations in Surrey Police) who were trained to do basic forensic analysis on mobile phone cases for triage purpose.

Surrey Police also has a separate AV Team7 which operates independently but is affiliated with the DF Team and under the same management line ‘Forensic Technology Team.’ The AV Team has two technicians focusing fully on multimedia (audio/video) evidence. Occasionally the AV Team passes a submission to the DF Team if the submission is outside its area of work, but normally the two teams do not work with each other directly on submissions.

Although the DF Team does not particularly focus on multimedia data and devices like the AV Team, it routinely handles cases involving multimedia data for cases such as those related to child pornography. Therefore, in this section we cover both the DF Team and the AV Team to give a bigger picture of digital forensics practices at Surrey Police.

---

6 Surrey is the 12th most populated ceremonial county in England out of 48 ones as of mid 2011, and if metropolitan counties and unitary authorities are counted separately Surrey is the 11th most populated county (UK Office for National Statistics 2012).

7 This AV Team is also called the Video Audio Laboratory, but to align with the name of the Digital Forensics Team, we use the former name throughout the whole chapter.
1.3.3 Training and Certification

When recruiting new staff to the DF Team, it is expected that the applicants have gone through the ‘Core Skills in Data Recovery and Analysis’ training course provided by the College of Policing (CoP) (UK College of Policing 2014), but other equivalent training programs and experiences are also counted. However, if a newly recruited staff have not gone through the Core Skills training course, he/she will be asked to attend it, so the CoP training course can be considered as a compulsory qualification. In addition to the CoP training courses, technical staff is normally expected to attend product training programs among which the EnCE (EnCase Certified Examiner) (Guidance Software, Inc. 2014) is of particular importance because Guidance Software’s EnCase Forensics (Guidance Software, Inc. 2014a) is the mostly used digital forensics software toolkit at Surrey Police. Some other training courses include AccessData BootCamp (AccessData Group, LLC 2013) for another important digital forensics toolkit FTK (AccessData Group, Inc. 2014a) used at Surrey Police and courses for general techniques such as internet artefacts, networking technologies, Apple Mac computer forensics, Linux computer forensics, PDA forensics, satellite navigation system forensics, etc.

The two technicians of the AV Team are both Certified Forensic Video Technicians (CFVT) through the Law Enforcement and Emergency Services Video Association International, Inc. (LEVA International, Inc. 2014). This is however not a formal requirement to be certified as a CFVT although it has proved very beneficial in practice.

1.3.4 Standard Procedure

Regarding the standard procedure, both the DF and the AV Teams are following mainly the ACPO Good Practice Guide for Digital Evidence (Association of Chief Police Officer of England, Wales & Northern Ireland 2011). In the reports of both the DF and AV teams, it is stated that ACPO guidelines are followed, which can normally make sure judges will accept the results. The AV Team also follows the guidelines defined by ACPO and/or the former Home Office Scientific Development Branch (HOSDB)8 on multimedia evidence especially on CCTV evidence and digital imaging (Home Office Scientific Development Branch 2010).

Similar to the case of the Met’s DEFS, the DF Team and the AV Team will need to pass the ISO/IEC 17025 (ISO/IEC 2005) lab accreditation required by the UK Forensic Science Regulator (2011). As of June 2014, Surrey Police is still in the planning phase for this task.

---

8 The HOSDB was renamed to the Centre for Applied Science and Technology (CAST) in April 2011 (Professional Security Magazine 2011).
1.3.5 Routine Tasks Involving Multimedia Data and Devices

The AV Team is mainly handling video and audio footage on different kinds of storage media such as DVDs, CDs, SD cards, USB sticks, DVR CCTV recorders, VHS tapes, dictaphones and compact cassettes. All submissions come via Surrey Police’s Submissions Department which ensures that each submitted exhibit is security sealed, that the submission form has been correctly completed, and that continuity signatures on the exhibit are up to date. The average work load for the whole team is around 50 cases per week, and the most common type of multimedia data is video (around 80%), followed by still images and audio (around 10% each). The routine tasks conducted mainly include

- copying and enhancing video sequences onto DVD (Video), CD or VHS videotape,
- copying and enhancing of audio onto CD or cassette,
- exporting/download of video data from CCTV digital video recorders,
- enhancement and printing of still images from video,
- editing video and/or audio,
- highlighting and/or masking of persons or items in video sequences,
- decoding of multiplex-encoded videotapes,
- recovery of data from corrupt or damaged discs, and
- repairing damaged media.

The DF Team does not have a focus on multimedia data and devices, but it is common to encounter multimedia data and devices. For computer forensics cases (over 100 TB in 2013), it is estimated that around 80% of them involve some kind of multimedia data. For mobile phone forensics cases (around 5000 and 1500 before and after triage) the percentage is around 40%. The multimedia data and devices include audio files, digital still images, digital video clips, CDs, DVDs, digital tapes, digital cameras, digital audio recorders, video camcorders, GPS devices, PDAs, etc. Among all the multimedia data, digital still images are more common than video and audio files, which is partly because video and audio files are often processed by the AV Team and cases with the DF Teams are often about still images (e.g. child pornography cases).

1.3.6 Submission Formats

For this section we discuss the AV Team only because the cases of the DF Team is much broader.

For video submissions, the AV Team needs to provide the results in DVD video format for court. Referring to instructions on the submission form, the technicians normally use screen grabber software to digitize the relevant analogue footage which is then authored to DVD Video and sometimes they have to play the footage from the PC direct to a DVD recorder via composite/S-Video cables. Sometimes the AV Team is asked to grab still images from CCTV footage and print them or burn them to CD.
For audio submissions, the AV Team provides them in Audio CD format for court, for which the technicians usually create WAV files first and then convert them to Audio CD.

After the CD or DVD is made, the technician then duplicates it as required by the standard procedure and uses a disc printer to print a label onto the disc. If the submission is for court, then one of the copies would be sealed and the technician handling the case will include a statement. The job is then returned to the Submissions Department.

1.3.7 Triage

For the DF Team, mobile forensics cases go through a triage process where 38 trained volunteering officers first conduct some basic-level forensic analysis to identify cases requiring more advanced analysis by the forensic examiners of the AV Team. All triage officers focus on file systems only, but not on file content because the latter would require the triage officers to have more advanced skills. The whole process is coordinated by the administrative support officer of the DF Team. Computer forensics cases do not have a triage process, but are prioritized by the computer forensic analysts of the team.

The AV Team does not have a triage process for cases it receives, either. Normally cases are processed in the order they are received, unless a submission is authorized as urgent by a senior police officer.

1.3.8 Software and Hardware Tools Used for Handling Multimedia Data

The DF Team is mainly using EnCase scripts to extract multimedia files from storage media which mostly depend on signatures in file headers. Other software tools that are sometime used include C4ALL (also known as C4P – Categorizer for Pictures) developed by the Ontario Provincial Police Technological Crime Unit\(^9\) in Canada (Ontario Provincial Police Technological Crime Unit 2010), ZiuZ VizX2 (ZiuZ B.V. 2014), Digital Detective’s Blade (Digital Detective Group Ltd 2014) and Microsoft PhotoDNA Microsoft (2013). The DF Team also uses the open-source software tool VLC player to extract frames from video sequences and crop regions of interests if needed.

The AV Team uses various PCs and audio/video players to play audio and video footage. For CCTV there are hundreds of different formats so it is often the case that proprietary player software has to be installed to play a piece of CCTV footage. When such software is not included on the disc, the AV Team technicians will try to download player software from the manufacturer’s website. The AV Team technicians also often edit CCTV to show just the relevant footage, for example they often create a sequence where a suspect is ‘followed’ from camera to camera rather than showing each camera separately in its entirety and sometimes they are asked to highlight or blur out areas of

\(^9\) http://www.e-crime.on.ca/.
the picture. The AV Team uses mainly Avid Media Composer (Avid Technology, Inc. 2014a) and Sony Vegas (Sony Creative Software, Inc. 2014) to edit the footage.

1.3.9 Cases Involving Encryption and Child Pornography

Such cases are mainly handled by the DF Team. Cases involving encrypted files are not common, and probably less than 10% but occasionally cases involving a lot of encrypted files are encountered. In those cases, some software tools for password cracking are normally used such as AccessData PRTK (AccessData Group, Inc. 2014b) which uses distributed computing and GPU. There are also special software tools developed for cracking passwords on Apple iOS and Blackberry devices.

The DF Team handles a lot of child pornography cases. There are two sub-teams for handling such cases: online abuse materials and computer-based analysis. The process can be partly automated using the software tool C4ALL (Ontario Provincial Police Technological Crime Unit 2010) because it has a hash (traditional hashing) database of child pornography pictures. The DF Team realized that perceptual hashing (Monga 2005) (hashing methods robust to benign signal processing operations that do not change the perceptual content of the processed image) will be helpful for handling those cases but it has not been used yet.

1.3.10 Cases Involving Source Device Identification

The DF Team had cases where the sources of digital images need identifying which were handled by looking into the EXIF metadata which is unfortunately prone to manipulation. Advanced techniques like PRNU-based camera source identification have not been used by Surrey Police yet but will be welcomed by the DF Team. There were some cases about source printer identification as well which were handled by looking into the computer spool files. There were two cases about counterfeiting printed documents, one about a banking statement and the other on an ID card, which were analyzed by looking at the material and typos.

1.3.11 Challenges

In our interview with staff members of Surrey Police, only a few challenges were highlighted. We understand this was due to their concerns on more practical issues.

For the DF Team, perceptual hashing seems to be the major technique still missing from existing digital forensics tools, and they feel other multimedia forensic techniques will be very helpful as well. The DF Team members also feel that HD videos cause trouble because of the lack of tools supporting the new format. A similar issue exists for mobile phone forensics because tools are normally updated only once a quarter, but new models of mobile phones are released much more frequently and more new brands/models are emerging in the market.
For the AV Team, one major challenge is the lack of a software tool that can play all types of CCTV footage and output the results to DVD. Currently there seems to be only one product in this space, Siraview (Sira Defence & Security Ltd 2014), but it is not a complete solution yet although the AV Team is indeed using it.

1.3.12 Acknowledgements

The authors would like to thank the following interviewees and informants from Surrey Police: Jill Wheeler (Forensic Technology Team Leader), Garry England (member of the DF Team) and David Lawrence (Principal Technician of the AV Team). The authors would also like to thank Jill Wheeler for her help in coordinating the whole information gathering process.

1.4 Shanghai Stars Digital Forensic Centre, Third Research Institute of China’s Ministry of Public Security

The information about the Shanghai Stars Digital Forensic Centre (‘SSDFC’ hereinafter) in China was gathered through its official websites, a written document provided by the Director of SSDFC, and a structured interview which took place on 5 July 2013. Some further email communications took place after the interview to get more information and to clarify some unclear issues raised during the interview. The published content of this section was reviewed by the informants.

1.4.1 Background: Third Research Institute of China’s Ministry of Public Security

The institute was founded in 1978 and is one of 15 research organizations directly managed by the Ministry of Public Security of China. Its main research areas include information and network security, Internet of Things (IoT), special operations communications, illegal drugs control, anti-terrorism and explosion protection, image processing and transmission, and public security protection techniques. It has around 1700 members of staff including over 1300 researchers among which more than 500 have a doctoral or a master’s degree. In 2005 the institute passed the ISO 9001 quality management test (ISO 2008) (Third Research Institute of Ministry of Public Security 2014).

10 The Shanghai Stars Digital Forensic Centre’s official website is http://www.stars.org.cn/, but there is another website http://202.127.0.199/ which provides some supplementary information to the first one.

11 The other nine research institutes are First Research Institute, Forensic Analysis Center (formerly known as Second Research Institute), Fourth Research Institute, Traffic Management Research Institute, Southern Research Institute, Disc Production Source Identification Center, four fire research institutes and four police dog research organizations (one research institute and three dog bases conducting research activities). There are several universities and colleges conducting research activities as well, but they are not counted in the 15 research organizations.
1.4.2 Background: Related Legislations and Regulations

In China, only certified persons and bodies can provide forensic services as laid out in China’s NPC (National People’s Congress) Standing Committee’s Decision regarding Management of Judicial Appraisals (National People’s Congress Standing Committee, People Republic of China 2005). According to how the certification is done for digital forensic services, there are two types of service providers: those serving police forces and certified by the Ministry of Public Security, and those open to the public and certified by the Ministry of Justice. Although following different regulations and certification processes, both types of digital forensic service providers abide by the same basic laws, technical standards and procedures, digital forensic hardware and software equipment, so their expert reports are considered technically equivalent.

1.4.3 Overview of SSDFC

The SSDFC was created by the Third Research Institute of China’s Ministry of Public Security and certified by the Shanghai Judicial Bureau (the provincial branch of the Ministry of Justice in Shanghai) in 2007. It provides forensic services on digital data and AV material to law enforcement agencies, law offices, other bodies in public and private sectors, and natural persons as well (as permitted by the certification it received from the Ministry of Justice). The SSDFC is one of the leading service providers nationwide on forensic analysis of digital data and AV material, and the first one passing both lab accreditation and metrology accreditation by national accreditation authorities.

The SSDFC currently has 32 certified digital forensics experts including 15 experts with a senior professional title (associated researcher or researcher) of the Third Research Institute (Shanghai Stars Digital Forensic Center 2014a). Some digital forensics experts of the SSDFC are members of different technical committees in the digital forensics field and have received awards at both provincial and national levels. Digital forensics experts of SSDFC also conduct research in digital forensics, and they publish research papers at national and international venues. The SSDFC also has several forensic analysis assistants. All digital forensics experts are required to go through annual training organized by the Shanghai Judicial Bureau and the SSDFC.

---

12 There is no official translation of the document’s title and the word ‘Judicial Appraisals’ is not an accurate translation of the original Chinese word, which actually covers judicial appraisals, authentication, forensic examination, etc.
13 The Ministry of Public Security is the central administration of police forces in China.
14 These two titles are direct translations from Chinese. Their seniority is actually close to associate professor and full professor, respectively, as in universities.
1.4.4 Services Provided

The SSDFC provides a variety of digital forensic services mainly in two categories: forensic analysis of digital data, and forensic analysis of audio/video data and devices. There is no internal allocation of digital forensics experts to the two categories, but there are two appointed experts who are in charge of the two categories, respectively. In addition to the two normal categories of services, digital forensics experts of the SSDFC also provide other services such as field inspection, court expert witnesses, printed documents inspection and consultancy.

The SSDFC’s forensic services on audio/video data and devices including mainly the following (Shanghai Stars Digital Forensic Center 2014c):

- Forensic analysis of audio and video material such as denoising, restoration, enhancement and feature extraction
- Identification of languages, persons or objects in audio and video material
- Content analysis of languages and images in audio and video material
- Authentication of audio and video material including event (e.g. start and end) detection and forgery detection
- Speaker authentication from audio material
- Identification of audio and video recording devices such as brands, models, vendors, manufacturing sites, and also identification of the source device of audio and video material
- Forensic analysis and examination of audio and video material on the Web
- Forensic comparison of audio and video material to determine if the sample under analysis is a pirate copy
- Preservation of audio and video material on read-only storage media.

1.4.5 Procedure

Different from in-house digital forensics laboratories run by law enforcement agencies, the SSDFC is open to any legal bodies and natural persons, so it gets cases directly from their customers who provide digital evidence and requirements of the wanted forensic analysis.15 The customer receives two copies of the expert report and the SSDFC keeps a third copy for archival purpose (Shanghai Stars Digital Forensic Center 2014b). Each case is normally handled by two digital forensics experts who either work independently or jointly. One of the two digital forensics experts has more responsibilities and will be the person who appears in court as the expert witness (if required).

For the digital forensic process itself, the SSDFC follows international and national standards, and also its own in-house best practices for each type of digital evidence.

---

15 In-house digital forensics laboratories of law enforcement agencies in China mainly focus on crime scene investigations and simple digital forensics cases. Complicated digital forensics cases are normally outsourced to independent digital forensics laboratories like the SSDFC.
In 2009 the SSDHC passed the ISO/IEC 17025 lab accreditation test (ISO/IEC 2005). In 2014 it passed the ISO/IEC 17043 test (ISO/IEC 2010), becoming the first proficiency testing provider (on digital forensics) in China’s public security (police) system.

The national standards followed by the SSDFC include national standards published by China’s Standardization Administration and General Administration of Quality Supervision, Inspection and Quarantine (GB/T series), industrial standards published by Ministry of Public Security (GA/T series), forensics-related specifications published by Ministry of Justice (SF/Z series), and lab accreditation standards published by the China National Accreditation Service for Conformity Assessment (CNAS-CL series). All the first three standard series cover digital forensics in general and also forensic analysis of AV data and systems. There are also a large number of standards about forensic imaging and photography. For more details about different standards, readers are referred to Chapter 2 of the book.

1.4.6 Workload and Typical Cases

In 2013 the average workload of digital forensics experts of the SSDFC was around 20 cases per person. Most cases can be completed within 30 working days, but some special cases may require up to 60 working days. Since the workload is not very heavy, the SSDFC does not have a triage process, but will prioritize cases based on customers’ needs.

Around 10% of all cases involved multimedia data and devices such as recorded speech, music, digital images in computers and mobile phones, digital video sequences (including movie and TV programs), computer-generated pictures, multimedia discs, digital cameras and camcorders, sound recording devices, GPS devices, and so on. The SSDFC also perform speaker comparison and identification based on recorded speech.

The SSDFC had cases where the authenticity of multimedia data was validated. There are national standards for digital forensics experts to follow for such tasks (GA/T and SF/Z standards).

All digital forensics experts of SSDFC are technically qualified to do forensic photographs, but the SSDFC has a dedicated forensic photographer for such tasks.

1.4.7 Software and Hardware Tools Used

Software tools used by digital forensics experts of the SSDFC include EnCase (Guidance Software, Inc. 2014a), Recover My File (GetData Pty Ltd 2014), X-Ways Forensics (X-Ways Software Technology AG 2014), Adobe Audition (Adobe Systems Inc. 2014) (for audio forensics), Adroit Photo Forensics (Digital Assembly, LLC 2014) (for photo evidence handling), the Chinese edition of IMIX IMPRESS (IMIX Vision

16 What the SSDFC passed is actually a national standard CNAS-CL03 (China National Accreditation Service for Conformity Assessment 2010), which is effectively equivalent to the ISO/IEC 17043:2010 standard (ISO/IEC 2010).
Support Systems 2014)\(^{17}\) (for forensic image/video restoration and enhancement), VS-99 Computer Speech Processing Workstation (also known as voice print meter) (Beijing Yangchen Electronic Technology Company 2014) (for speaker recognition), etc. The SSDFC also uses password cracking software to break encrypted files and is currently planning to use Microsoft PhotoDNA software (Microsoft 2013) to detect child pornography images automatically. Most software tools are running under Microsoft Windows platform.

The SSDFC is also supported by the rest of the Third Research Institute of China’s Ministry of Public Security to develop bespoke software tools for handling special file formats, extracting data from network streams and uncommon digital devices such as GPS.

### 1.4.8 Challenges

A number of challenges were identified by staff of SSDFC in the written document provided.

#### 1.4.8.1 Standardization Lagging behind IT Technology Development

The rapid development of IT technologies has led to the emergence of new digital devices, storage media, software and hardware tools, and networking protocols. By contrast, the development of digital forensics standards would normally take a long time and actions cannot be taken before any new technology and the corresponding forensic solution becomes available. How to improve the efficiency of digital forensics standardization activities is a key challenge in this field.

#### 1.4.8.2 Preservation of Digital Evidence Compatible with Electronic Signature Law

Digital evidence in its original format is normally prone to manipulation, so it must be preserved following a forensically sound process to make it admissible to the court according to China’s Electronic Signature Law (China National People’s Congress Standing Committee 2004). Therefore, digital forensics standards must consider the problem of how to preserve digital evidence so that the expert reports can be accepted in court.

#### 1.4.8.3 Diverse Storage Media and Device Interfaces

In a digital forensic analysis process, various types of storage media (e.g. floppy disks, CDs, hard disks, USB sticks, MMC/SD/CF storage cards and SIM cards) and device interfaces (e.g. IDE, SATA, SAS, SCSI, fibre channel, USB, Firewire and ISO/IEC

\(^{17}\) The Chinese edition has a different name ‘Imaging Doctor’.
need to be handled effectively by using proper hardware devices and to follow forensically sound procedures and methods.

1.4.8.4 Data Loss in Live Forensics

Forensics of live systems (live forensics) can change the status of the live system such as volatile memory, processes, network communications, which can in turn influence extraction of digital evidence and even the results of the digital forensic analysis. This influence normally differs from system to system. Therefore, different live forensic methods and standard procedures are needed for various operating systems and devices.

1.4.8.5 Reverse Engineering and Binary Code Comparison

In cases involving malicious code, destructive computer program, commercial secrets, digital rights violation, reserve engineering and/or binary code comparison are often required. This can be very complicated to do due to different computer architectures, CPU instruction sets, results produced by different advanced programming languages compilers, operating systems, and run-time environments. To help handle such cases, standard methods and procedures are needed for reverse engineering and binary code comparison.

1.4.8.6 Cloud Forensics

In digital forensics cases involving data stored in the cloud, it becomes very challenging to extract and preserve data due to the difficulties of localizing data. In addition, data in cloud is not necessarily stored physically on a single physical server, but could distribute on many servers which are physically located in different countries and regions. This means that it can be extremely difficult to collect complete data for digital forensic analysis. Even if complete data collection is possible, the huge amount of data stored in cloud requires a lot of more computations. The complexity of data in the cloud can also raise concerns on the originality, integrity and reproducibility of digital evidence extracted, thus making it less admissible in court. More research is needed on this topic to provide information for standard methods and procedures on cloud forensics.

1.4.9 Acknowledgements

The authors would like to thank the following interviewees and informants from the Shanghai Stars Digital Forensic Center: Dr. Bo Jin and Dr. Hong Guo who are the Director and Director Assistant of the Center, respectively.

1.5 Discussions

Looking at the descriptions of the three digital forensics laboratories covered earlier, we can see a common feature shared among them: they all separate cases involving
Digital Forensics Laboratories in Operation

forensic analysis of audio and video material from ‘normal cases’ involving more ‘traditional’ digital forensics such as computer forensics and mobile phone forensics. Although not all laboratories have a separate internal group focusing on audio and video forensic analysis (e.g. the SSDFC in China does not have a separate group), they all offer separate services on audio and video forensic analysis. This fact has its root in separate standards and best practice guides on audio and video forensic analysis in some countries such as in China (specific standards for audio, image and video processing) and in the United States (a separate working group on digital imaging, SWGIT), and can be understood based on the fact that very different techniques (e.g. audio and image processing/analysis) are needed for audio and video forensic analysis, while traditional digital forensics are more focused on computer architectures, file systems and specific software/hardware tools.

It is however common for a computer and mobile forensic examiner to use advanced multimedia file carving tools such as Digital Assembly’s Adroit Photo Forensics (Digital Assembly, LLC 2014) and X-Ways Forensics (X-Ways Software Technology AG 2014) to recover digital images and video sequences out of a disk image, although those tools are based on advanced image analysis techniques (which however are not necessarily what users of the tools need to know). The boundary between the two classes of cases is not always a clear cut especially when digital still images are involved. It is common that child pornography cases are normally handled by computer and mobile forensic examiners rather than image/video forensic analysis experts in the AV team of a digital forensics laboratory because it involves more file carving than signal processing tasks. Multimedia devices are also lying between the boundary: when file extraction or recovery is the actual task, they are normally handled by computer and mobile forensic examiners, but if some level of content analysis is required they are often handled by the AV team.

There are three interesting observations in our interviews and communications with the three digital forensics laboratories covered. The first observation is about forensic photography. Although the SSDFC has a dedicated forensic photographer and all their experts are trained for this task, this topic is not covered by the two UK laboratories but more with other departments/teams of the police forces. Although we did not attempt to cover any forensic photography team, we are aware that forensic photography share many techniques with image and video forensic analysis especially image enhancement. The second observation is about relationship between biometrics and digital forensics. Biometric techniques such as fingerprint and face recognition (and even DNA matching) are almost only considered ‘non-digital’ forensic services although the whole process is nearly fully digitized except for the first step (data capturing). This is however not surprising because fingerprint and face recognition have been handled routinely by traditional forensic laboratories even before the systems become fully digitized and manual inspection/matching is still sometimes required even in the digital era for difficult cases or false positive/negative cases identified through other evidence. The third observation is about the use of
photogrammetry in (digital) forensic analysis. We noticed only the AV Lab of the Met’s DEFS is conducting some photogrammetric analysis (height and speed estimation). Surrey Police’s DF and AV Teams did not have cases requiring such analysis, and when asked about how they would handle such cases they said they would outsource the task. The SSDFC in China did not handle such cases and they did not do research on this topic either. This is also not surprising because of the same reason as in the biometrics case: photogrammetry is independent of the digitization process, and it has existed for long time before digital cameras and camcorders were invented, so it may be seen as a more traditional ‘non-digital’ forensic technique. For the last two observations, we refer the readers to another two chapters of the book which cover the use of biometrics and photogrammetry in digital forensics.

Comparing the three digital forensics laboratories covered in this chapter, we can see clear differences between the two in-house laboratories of local police forces and the SSDFC which is a public-facing laboratory (even though it is managed by a law enforcement research institute). The in-house laboratories are more driven by the needs of the law enforcement bodies they serve and focus on what are the most important tasks (also simpler or more routine tasks), but public-facing laboratories have to provide a broader range of services and be able to handle more complicated cases. This is reflected from the fact that all digital forensics experts of the SSDFC can do both computer/mobile and AV forensics (and even forensic photography). During the interview with the SSDFC, the two interviewees mentioned that local police forces in China also have their in-house digital forensics teams, but they normally handle crime scene investigations and simple forensic analysis but outsource complicated cases to external laboratories like the SSDFC. Surrey Police has the same strategy since it has a smaller digital forensics team, but the Met’s DEFS seems to be less concerned about this probably because it is large enough to cover nearly everything on its own.

When comparing the two digital forensics laboratories in the United Kingdom and the one in China, we also noticed a clear difference in the standard procedures they follow. Neither of the the UK laboratories have passed the required ISO/IEC 17025 lab accreditation test yet, although they both are preparing for it, but the SSDFC in China passed the ISO/IEC 17025 lab accreditation test in 2009 (just 2 years after its establishment in 2007) and the more advanced 17043 test as a proficiency test provider in 2014. In the United Kingdom the ACPO Good Practice Guide for Digital Evidence (Association of Chief Police Officer of England, Wales & Northern Ireland 2011) seems to be the only one followed by most in-house laboratories of police forces, although some digital forensic service providers in private sector have passed the ISO/IEC 17025 test (CCL-Forensics Ltd. 2014; Forensic Telecommunications Services Ltd. 2015). While the United Kingdom does not have any national standards

---

18 Some private-sector digital forensic service providers in the United Kingdom also passed some other relevant ISO tests such as ISO 9001 (ISO 2008) for general quality management and ISO/IEC
on digital forensics yet, a large number of national standards have been published by different governmental bodies on digital evidence and forensics including audio and video forensic analysis since many years ago. The ISO standards-based lab accreditation test and the proficiency test required are also more established in China. For a more detailed description on standards and best practice guides in digital and multimedia forensics, readers are referred to Chapter 2 of this book.

Although this chapter only covers three digital forensics laboratories in two nations (the United Kingdom and China), many observations can be generalized to other nations such as the US. Note that the United Kingdom and China are representatives of two most widely adopted law systems in the world (the common law system and the civilian law system), so we expect they reflect more about practices in their respective law systems. For instance the civilian law systems tend to depend more on established laws and regulations rather than important cases, which may explain why China has more standards, while the United Kingdom has more or less only one best practice guide. Despite the possibility to generalize the observations in this chapter to other nations following the two common law systems, we call for caution when readers want to apply such generalizations to their own nations. We plan to cover more digital forensics laboratories from more other nations on the website of this book. The main targets include the United States, more European and Asian nations, Russia, Canada, Australia, New Zealand, major Latin American nations like Brazil and Mexico, South Africa and some major African nations, and also Islamic nations some of which follow a complete differently law system. It will be of interests to look at some very special regions such as Hong Kong, Macau and Taiwan.19

One encouraging fact we noticed is that many new multimedia forensic techniques developed in research community have been used and some are even standardized in China. It is also interesting to see the Met’s DEFS and the SSDFC are both actively conducting research themselves by publishing papers at research venues. The SSDFC is also involved in organization of research events such as scientific conferences (Shanghai Stars Digital Forensic Center 2013). While the use of multimedia forensic techniques are more known to people in digital forensics field or the wider information security field (which are both more in computer science and engineering), researchers working in multimedia forensics are less informed because they are often from a signal processing background (which belongs to electronic engineering more than computer science). One of the motivations of the book is to fill the gap between digital forensics and multimedia forensics fields so that people in the two fields can work together more often and more effectively to meet the real-world needs of digital forensics laboratories.

---

19 We use ‘Taiwan’ as this is the mostly used term in academia without any particular political position. Depending on the political positions of readers, they should interpret this word as the ‘Republic of China’, ‘Taiwan, People Republic of China’ or ‘Taiwan (Republic of China)’ or any other terms more acceptable to them.

27001 (ISO/IEC 2013) for information security management (CCL-Forensics Ltd. 2014; Forensic Telecommunications Services Ltd. 2015).
Regarding the challenges identified by the three digital forensics laboratories, we can see the most common challenge is the diversity of media storage, file formats and device models, which require digital forensics software and hardware tools to be updated more frequently. This is a challenge more for software developers and less so for researchers, although research on reconfigurable software frameworks such as the MPEG Reconfigurable Video Coding (RVC) standard (ISO/IEC 2011) may find opportunities. The three digital forensics laboratories are less converged on other challenges, but some important areas for further research are highlighted which include live forensics, cloud forensics, binary code analysis, anti-forensics, perceptual hashing, advanced image enhancement techniques. More standardization activities are also mentioned by staff of the SSDFC, which is also a concern of the UK Forensic Science Regulator as laid out in its Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System (UK Forensic Science Regulator 2011).

1.6 Summary
This chapter samples three digital forensics laboratories in two nations (the United Kingdom and China) to reflect how multimedia data and devices are handled in real-world digital forensics laboratories in the context of more general digital forensics. The focus is more on the operational side, but some key techniques used and main technical challenges are also covered so that readers can have a better understanding on the positions of those multimedia forensic techniques covered in real world. A comparison of the three digital forensics laboratories has allowed us to discuss some key observations and led to some future research directions. The content of this chapter will be further enriched by supplemental material on the book’s website where we plan to cover more digital forensics laboratories from other nations.

1.A Appendix: Questionnaires for Interviewing Surrey Police and Shanghai Stars Digital Forensic Centre
In this appendix, we give the questionnaires we used to interview staff of Surrey Police and the Shanghai Stars Digital Forensic Centre. Some questions were changed slightly to reflect different contexts of the two digital forensics laboratories.

• What is the structure of your digital forensic team? Do you have a single unit or is it composed of a number of independent groups who are working together?
• What is the current size of your digital forensic team? How many of them are technical examiners, and how many have been certified as qualified forensic examiners? What training courses do you require technical staff to attend?
• What is the average workload of your forensic technical staff? What is the percentage of cases involving multimedia data and devices?
• What types of multimedia data and devices have you encountered in your forensic practice?
• What are the percentage of digital audio, images and videos you normally handle?
• Do you have a triage process for forensic cases? If so, how do you handle multimedia data and devices in such a process?
• Do you have a separate forensic photography team and how do you work with them? Are you using digital cameras for photographing all crime scenes or do you still use optical ones? What are the requirements of cameras used for forensic photography? Could you mention a few models of cameras you are currently using?
• How often do you outsource forensic analysis of multimedia data and devices to other digital forensic labs? If so how many cases go to other police forces and how many go to independent forensic experts in the private sector?
• How do you work with other digital forensic laboratories run by law enforcement?
• What is the standard procedure you are following for general forensic analysis? Are there any guidelines tailored for multimedia data and devices (like those defined by US Scientific Working Group on Imaging Technology (SWGIT))?
• What are the software and hardware tools you use to extract multimedia files from storage media and carve deleted files? What are the challenges of multimedia file carving from your point of view?
• How often do you encounter encrypted multimedia files? Are they always related to child pornography? Do you have a way to automate detection of (child) pornography materials?
• What software and hardware tools are you routinely using to analyze multimedia data and devices? If you have to process raw data to enhance the chance of extracting evidence, what do you know to make the results reproducible and admissible to the court?
• Do you have to often edit multimedia data to make it more understandable to the court? If so, what principles do you follow and what tools do you normally use?
• Do you often need to measure physical properties of persons and objects in digital images and videos? If so what software tools do you normally use and what are the challenges of making the result forensically sound (i.e. admissible to the court)?
• Do you work on cases where biometric data (e.g. face images, fingerprints, recorded speech for speaker recognition) are processed? What software (and hardware) tools do you use to handle biometric data?
• Have you encountered cases where you needed to identify (camera or scanner) sources of digital images and videos? If so, how did you handle those cases?
• Have you encountered cases where you needed to identify sources of recorded digital audio files? If so, how did you handle those cases?
• Have you encountered cases where you needed to identify sources of printed documents (possibly scanned)? If so, how did you handle those cases?
• Have you encountered cases where you needed to authenticate printed documents (i.e. if one piece of paper or printed document is indeed the one claimed)? If so, how did you handle those cases?

• Have you encountered cases where you needed to identify possibly forged digital multimedia files (speech, images, videos)? If so, how did you handle those cases?

• Have you encountered cases where you needed to differentiate computer-generated multimedia data from recorded ones from real world? If so, how did you handle those cases?

• Have you encountered cases where you needed to know what had happened during the whole processing chain of multimedia data (e.g. an seemingly uncompressed image was actually JPEG compressed)?

• Have you encountered cases where suspects or criminals seemed to have employed some anti-forensic techniques to make your work harder? If so are these cases related to multimedia data?

• Do you feel that existing software and hardware tools are sufficient for you to perform your work on multimedia data and devices? If not, what functionalities are missing from existing tools?

• Do you have any other information you feel useful for our book and our research on multimedia forensics in general?

References


Monga V 2005 Perceptually based methods for robust image hashing, PhD thesis. The University of Texas at Austin, Austin, TX.


